

ANDERSON COUNTY CIRCUIT COURT
ANDERSON TENNESSEE

2022 SEP 20 PM 12:06
FILED AC CIRCUIT COURT

BETTY JANE AYERS,
DAVID RUSSELL AYERS, and
SARAH WALKER BRUUN, as residents of and registered voters in Anderson and
Bradley Counties, Tennessee, pro se
Plaintiffs,

v.

Case No. C2LAD108

TRE HARGETT, Secretary of State of the State of Tennessee,
MARK STEPHENS, Administrator, Anderson County Election Commission,
HERBERT H. SLATERY III, Attorney General and Reporter for the State of
Tennessee,
JANET M KLEINFELTER, Deputy Attorney General for the State of Tennessee,
DAVID KUSTOFF, Congressman,
JIM COOPER, Congressman,
STEVE COHEN, Congressman,
MARSHA BLACKBURN, Senator, and
BILL HAGERTY, Senator,
Defendants

**COMPLAINT, MOTIONS FOR EMERGENCY ORDERS OF
TEMPORARY/PERMANENT RESTRAINING ORDER AGAINST THE USE
OF ELECTRONIC VOTING MACHINES & TO PRESERVE ALL VOTING
RECORDS FROM 2020 ELECTIONS, MOTION FOR EMERGENCY
HEARING ON THIS MATTER WITHIN 10 DAYS OF SERVICE OF
SUMMONS**

BETTY JANE AYERS, DAVID RUSSELL AYERS, and SARAH WALKER
BRUUN, pro se, come now with this Complaint against TRE HARGETT, Secretary
of State of the State of Tennessee, MARK STEPHENS, Administrator, Anderson
County Election Commission, HERBERT H. SLATERY III, Attorney General and
Reporter for the State of Tennessee, JANET M KLEINFELTER, Deputy Attorney
General for the State of Tennessee, for unconstitutional actions taken outside the
scope of their jobs and outside of the laws of our State and U.S. Constitutions,
actions which include the failure to discontinue the use of electronic voting

machines for which we gave them abundant and sworn evidence which shows these machines are easily able to be accessed and our votes switched, thus

disenfranchising the Constitutional right of suffrage of the people of Tennessee, and for their failure to address claims in their entirety as presented herein. They were

all given this evidence and failed to act upon it by ridding our state of these

compromised voting machines, or "impure ballot boxes," as is their duty per their

sworn oaths to uphold the Constitution of the State of Tennessee and the United

States of America, and additionally, this Writ of Quo Warranto is brought against

DAVID KUSTOFF, Congressman, JIM COOPER, Congressman, STEVE COHEN,

Congressman, MARSHA BLACKBURN, Senator, and BILL HAGERTY, Senator for

their failure to vote to send the vote back to the States to be re-certified on January

6, 2021, after receiving Attachments G and H, described below, which was an act of

treason in light of the content of the evidence they were given, as they allowed a

man they knew We the People had not elected to be sworn in as President. We bring

this Complaint demanding they immediately resign and face prosecution under the

law, or contact this Court for a date of hearing on this matter within seven days of

receipt of Summons and Complaint if they wish to refute the evidence.

When bringing a petition such as this, we the people, as individual members

of the public have standing as citizens and taxpayers under common law. We the

people have this right of redress per the U.S. Constitution, and the charge to

reestablish justice within the first paragraph of our US Constitution, and justice has

been lost in this matter. In our state, all power is inherent in the people of

Tennessee, all free governments are founded on our authority, and we the people have a right to alter, reform, or abolish the government in such manner as we think proper: *Tennessee Constitution, ARTICLE I. Declaration of Rights. Section 1. That all power is inherent in the people, and all free governments are founded on their authority, and instituted for their peace, safety, and happiness; for the advancement of those ends they have at all times, an unalienable and indefeasible right to alter, reform, or abolish the government in such manner as they may think proper. 2*

Section 2. That government being instituted for the common benefit, the doctrine of nonresistance against arbitrary power and oppression is absurd, slavish, and destructive of the good and happiness of mankind.

Secretary Hargett and Administrator Stephens have both failed to uphold the law of our Tennessee Constitution first and *only*, as they are charged here:

Tennessee Constitution Section 4. That no political or religious test, other than an oath to support the Constitution of the United States and of this state, shall ever be required as a qualification to any office or public trust under this state. Section 5. The elections shall be free and equal, and the right of suffrage, as hereinafter declared, shall never be denied to any person entitled thereto, except upon a conviction by a jury of some infamous crime, previously ascertained and declared by law, and judgment thereon by court of competent jurisdiction."

Plaintiffs have multiple times presented the evidence herein of compromised voting machines which are robbing us of our Constitutional right to vote to both

Secretary Hargett and Administrator Stephens, but they both refuse to cease using the electronic voting machines. We have given them notice that we do not consent to the use of these electronic voting machines, but they and their counsel still refuse to cease using them in our state. Our Constitution is clear: there is no other law besides our Constitution that they have to obey in their jobs, and they have clearly acted outside the Constitution in this matter and against the Constitution in this matter.

Plaintiff Ayers told DAG Kleinfelter that in light of the evidence, she (and by extension our Attorney General) should be representing us in this matter, not opposing us, but she would not, and told Plaintiff Ayers she would be filing a motion to dismiss the former case. Again, Plaintiffs discovered they were likely filed in the wrong court, and filed a notice of voluntary dismissal, and now refile in what we pray is the proper Court.

STATEMENT OF GROUNDS FOR FILING IN THIS COURT

As this matter involves both County and State government officials and Constitutional issues of the disenfranchisement of our right of suffrage at both county and state levels, and the failure of our county and state government officials to uphold their oaths of office, and our Tennessee legislative members' failure to protect the purity of our ballot box and to take steps as per their oaths and powers under the law to protect us from known threats against the purity of our ballot box, and to ensure the integrity of each of our votes, and involves actions from some individuals that amount to treason, and this Court holds venue for county and state

issues, this Court is believed to be the proper venue under both the Tennessee State Constitution Article 1, § 5, and Article IV, §1, ¶2, and the 14th Amendment to the U.S. Constitution, the Elections Clause (Art. I, § 4, cl. 1).¹ As mentioned above, unbeknownst to them at the time, Plaintiffs likely errantly filed this matter in the wrong court, the United States District Court Eastern District Of Tennessee, Knoxville Division, on 8/25/2022, but filed a Notice of Voluntary Dismissal of Defendants on 9/16/2022 when they became aware they were likely filed in the wrong Court. In the duration of that filing and in conferring per our Order to Confer, then-Defendants Mark Stephens and Tre Hargett (and thus the Attorney General and his assistant, the Deputy Attorney General who had filed a notice of appearance as counsel for Tre Hargett) were served via certified mail and email with a demand for the preservation of the entirety of 2020 voting records for all counties in Tennessee, and notification was given to the Deputy Attorney General Kleinfelter via emails during our order to confer, to advise her client to preserve these records even if we were filed in the wrong court. Additionally, the Attorney General (AG) and Deputy Attorney General (DAG) were given all evidence previously filed in this matter when they filed as attorney for their client, Tre Hargett, the Secretary of State, and Plaintiff advised DAG Kleinfelter during the email "meet and confer" that they (Secretary of State and Attorney General and his office) should be representing *we the people* in this matter, not opposing us, but Ms. Kleinfelter informed us, regarding our suit against her client Secretary of State Tre

¹ Plaintiffs have attached affidavits with name, full address, and telephone numbers as they are not attorneys who can easily redact private information from the body of this filing.

Hargett, that our "claims under the Tennessee Constitution are barred by sovereign immunity²" and then filed to dismiss Plaintiffs' former suit after we "met and conferred." As in footnote 2 and other places, the law clearly supports that neither Secretary Hargett nor our Attorney General nor our Deputy Attorney General have a right to act outside the law of our Tennessee and U.S. Constitutions. They swore an oath to the Tennessee Constitution upon taking their jobs, and as they are now acting against the Constitution and against We the People in this matter, all

refusing to remove the electronic voting machines for which we have presented

evidence to them and are presenting that evidence- and even more evidence now-

that it cannot be guaranteed that these machines can't be electronically accessed

and votes flipped- and thus it can't be guaranteed that the outcome of the vote is

who we the people voted for, thus robbing we the people of our Constitutional right

of suffrage, Plaintiffs have added our Tennessee Attorney General and his Deputy

Attorney General as Defendants in our Writ, for their refusal to investigate the very

serious evidence they were given, and their failure to uphold their oath to the TN &

² Our Secretary of State is forcing we the people to use machines for which we have given him evidence that proves these machines are able to be accessed and votes switched, thus threatening our Constitutional right of suffrage. His failure to act to protect our right of suffrage per our Constitution is an action not in keeping with the State, which removes his "sovereign immunity" *If government officials attempt to enforce an unconstitutional law, sovereign immunity does not prevent people whom the law harms from suing those officials in their individual capacity for injunctive relief. This is because they are not acting on behalf of the state in this situation. "The attempt of a State officer to enforce an unconstitutional statute is a proceeding without authority of, and does not affect, the State in its sovereign or governmental capacity, and is an illegal act, and the officer is stripped of his official character and is subjected in his person to the consequences of his individual conduct. The State has no power to impart to its officer immunity from responsibility to the supreme authority of the United States." Ex parte Young, 209 U.S. 123 (1908)*

US Constitutions and to protect the Constitutional right to vote of we the people of Tennessee. They have refused to investigate the multiple sworn affidavits of known threats to our right of suffrage which were presented to both of them in the former case, and are presented herein, and which, again, are now further strengthened with two more sworn testimonies from Mr. Clint Curtis- one at a hearing before the U.S. Senate, and another in the form of a sworn affidavit, all as follows:

STATEMENT OF CLAIM

1. As demonstrated herein, the methods by which elections at the local, state, and Federal levels in Tennessee were conducted in 2020 and are being conducted in 2022 cannot be shown to provide the fair elections guaranteed to every citizen under the U.S. and Tennessee Constitutions, per the 14th Amendment to the U.S. Constitution, the Elections Clause (Art. I, § 4, cl. 1), Art. I, § 5, and Article IV, §1, ¶2 of the Tennessee Constitution.

2. A cryptographic security risk inherent in all voting machines by design, a Trapdoor mechanism described in Exhibit A, (Attached, Declaration of Terpsehore Maras³, Exhibit A, pages 1-37,) makes the output of votes shown in reported election results impossible to reconcile with the ballot inputs, except under a full paper ballot visual inspection and re-count of all paper ballots cast. For ease of the Court while reading Exhibit A, refer to Exhibit B (Attached, Exhibit B, "List of

³ Ms. Maras served in the U.S. Navy and as a private government contractor, overseeing election operations in over 47 foreign countries wherein election results were flipped using the techniques described, which were then employed upon the United States, as related in her affidavit

abbreviations/explanations for reference in Ms. Maras' affidavit," pages 1-3) for a list of abbreviations used in Exhibit A, and their definitions.

3. Tennessee's voting systems possess the capability to be accessed by the internet, as demonstrated and sworn to by Tore Maras in the aforementioned Exhibit A, as well as in Exhibit C, hyperlink here [Fraction Magic – WEICU](#)⁴ (written link & description on Attachment also titled Exhibit C, page1,) which is a video of Bennie Smith, Shelby County, TN Election Commissioner/Secretary. Bennie Smith also appears in this video, Exhibit D, "Bennie Smith with Bev Harris/BlackBoxVoting" [Fraction Magic - Detailed Vote Rigging Demonstration - YouTube](#)⁵, (also Attached as Exhibit D, one page, description with written web site) and in Bennie Smith's attached affidavit, (Exhibit E, pages 1-12,) all of which affirm our voting machines have the ability to be accessed using the internet and our votes switched. This is also attested to not only of Tennessee's, but all the United States' voting machines, by Maria Zack in this video at a hearing before the Kansas Senate: (Exhibit F here as hyperlink next line, but also attached as Exhibit F with the written link and one page description <https://rumble.com/vxw1te-maria-zacks-earth-shattering-testimony-kansas-senate-hearing-mirrored.html>.⁶) Maria Zack's testimony is accompanied by this affidavit from the referenced Italian Attorney, (see Exhibit G, one page,) and this accompanying article (see Exhibit H, 6 pages.)

Plaintiffs believe our Tennessee U.S. Senators, Marsha Blackburn and Bill Hagerty, and US Congressmen David Kustoff, Jim Cooper, and Steve Cohen, were given Exhibits G and H by then-President Trump's attorney before the January 6, 2021 vote; yet still voted on January 6, 2021 NOT to return the vote they now knew to be fraudulent back to the States for re-certification, which is an act of treason, as they knowingly allowed a man they knew for certain we the people did not elect to

⁴ Full link here <https://weicu.org/fraction-magic> if hyperlink doesn't work

⁵ Full link here <https://www.youtube.com/watch?v=Fob-AGgZn44> if hyperlink doesn't work

⁶ Full link here <https://rumble.com/vxw1te-maria-zacks-earth-shattering-testimony-kansas-senate-hearing-mirrored.html> if hyperlink doesn't work

be sworn in as President of the United States. We demand they immediately resign and face prosecution or come to a hearing in this Court to refute this evidence and testimony from our witnesses.

Additionally, the machines used in Hamilton County, Tennessee, are Dominion ImageCast machines, like those used in Mesa County, Colorado, and for which County Clerk Tina Peters for Mesa County, Colorado, had forensic audit reports done for this past election and which show the machines were infiltrated and votes switched (see Exhibit I hyperlink here for all three reports: Election Reports - Tina Peters for Colorado — Tina Peters for Colorado⁷ or Exhibit I Report 1, 85 pages, Exhibit I Report 2, 146 pages, and Exhibit I Report 3, 87 pages.)

Plaintiffs spoke with Administrator Stephens of Anderson County, who did agree to preserve and not to destroy 2020 voting records in any form, but he would not agree to switch to voting on paper when presented the majority of the evidence presented herein, which proves that our machines can be infiltrated, and votes switched. Plaintiffs attempted two times to obtain current EAC certification certificates for Anderson County, Tennessee's voting machines from Administrator Stephens, but upon last request were told he did not have it, to "get that from the state." Other than an update to a non-Anderson County machine, the Hart ECO 1512 Clerical Verity Duo's Certificate on 2/4/22, no further EAC certification of Tennessee's electronic voting machines exists past that which exists in the state records of July 12, 2021, hyperlinked here 20210712_SECMinutes.pdf (tnsosgovfiles.com)⁸ titled "Minutes State Election Commission Meeting July 12, 2021." In that report's list of "Approved Voting Machines"- January 11, 2021 which begins on page 8, it can be seen that Anderson County's voting machines, the Hart Intercivic Model No. eslate 3000 does not appear on page 10 of this report, which lists the approved Hart machines. Additionally, despite multiple emails, phone calls to, and two hand-deliveries of our emails with most of the evidence presented herein (with the

⁷ Full link here <https://www.tinapetersforcolorado.com/election-reports> hyperlink doesn't work

⁸ Full link here https://sos-prod.tnsosgovfiles.com/s3fs-public/document/20210712_SECMinutes.pdf if hyperlink doesn't work

exception of the Mesa County Colorado links above which we did not yet have, and the other two additions mentioned above, still to come, below) with questions to Secretary Tre Hargett over a period of three weeks, he has failed to answer or address any of our questions or concerns in any manner.⁹ Plaintiffs can find no EAC certification for Anderson County's voting machines in any minutes/reports of the State Election Commission Meetings, we therefore feel Anderson County machines and possibly many others throughout the state are and have not been EAC certified per HAVA law in 2018, 2020, or for the upcoming elections, yet Tennessee took HAVA funding in 2018, 2019, and 2020, which is a violation of Section 231 of the federal statutes of HAVA PUBLIC LAW 107-252—OCT. 29, 2002, codified at 52 U.S.C. 20901 to 21145, according to the Department of Justice's site The Help America Vote Act Of 2002 (justice.gov)¹⁰, rules of which they state they enforce in the second category on their page. The manual for HAVA, Section 231 "EAC Voting System Testing and Certification Program Manual," is available here, Cert.Manual.4.1.15.FINAL.pdf (eac.gov)¹¹ where it can be seen on page 1, *No. 1, 1.2. "Authority. HAVA requires that the EAC certify and decertify voting systems. Section 231(a)(1) of HAVA specifically requires the EAC to "... provide for the certification, de-certification and re-certification of voting system hardware and software by accredited laboratories." The EAC has the sole authority to grant certification or withdraw certification at the Federal level, including the authority to grant, maintain, extend, suspend, and withdraw the right to retain or use any certificates, marks, or other indicators of certification."*

Given the number of machines in use in Tennessee, it is highly likely that some were either connected to the Internet or transmitted data that manipulated votes, denying some in Tennessee our right of suffrage per Article 1, § 5 of the Tennessee Constitution. The probability of changing the votes after the machines read the ballots or have votes punched in is too high to leave such a critical part of the

⁹ Plaintiffs will gladly submit documentation of all these letters and phone calls if the Court wishes.

¹⁰ Full link here <https://www.justice.gov/crt/help-america-vote-act-2002> if hyperlink doesn't work

¹¹ Full link here https://www.eac.gov/sites/default/files/eac_assets/1/28/Cert.Manual.4.1.15.FINAL.pdf if hyperlink doesn't work

foundation of the United States, free and fair elections, to the intentions of foreign and domestic bad actors who would sway election results at all levels, local, state, and Federal. Evidence supporting the complete depravity of the entirety of our voting system is growing greatly each day. Administrator Stephens told us that “there isn’t time to enact a paper voting system” and said he would continue using the machines in response to our requests to eliminate all electronic voting and move to paper ballots only. Lack of time to correct these matters is no excuse to continue in depriving the citizens of Tennessee of the matters voiced herein. We must make the time to address these issues, even if time must be made by delaying elections,

and we include herein that the Supreme Court, on August 21, 2022, upheld the right for a State to halt an election until fraudulent matters are corrected: (See exhibit J [hyperlink here Supreme Court Halts Georgia Election Until New System Is Created \(conservativebrief.com\)](#)¹² or written link and description on attached Exhibit J, 4 pages) and see also Exhibit K [hyperlink here Georgia elections for two PSC seats again delayed by U.S. Supreme Court ruling - Georgia Recorder](#)¹³ or written link and description (on attached Exhibit K.)

4. Retention of the November 2020 election data beyond the September 2022 required period is critical to verifying the 2020 election results and to ensuring the fairness of all future elections.

5. Until an in-person, paper ballot, day-of-election voting process is re-established, with results reported immediately after the voting period ends, Americans cannot have any level of confidence that the reported results of any elections accurately reflect the votes cast.

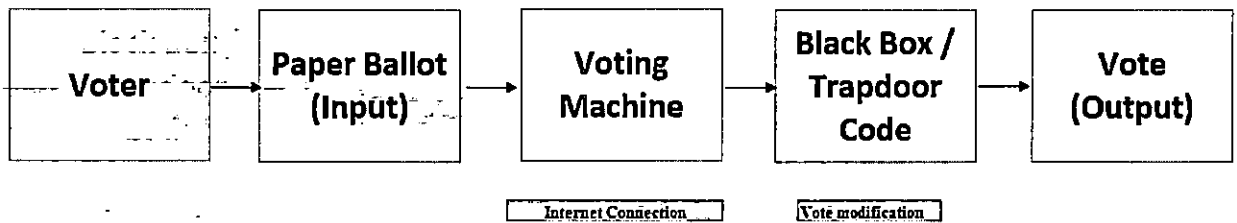
¹² Full link here https://conservativebrief.com/created-65771/?utm_source=CB&utm_medium=ABC if hyperlink doesn't work

¹³ Full link her <https://georgiarecorder.com/brief/georgia-elections-for-two-psc-seats-again-delayed-by-u-s-supreme-court-ruling/> if hyperlink doesn't work

6. Before and during the November 2020 election, neither of the two Voting System Testing Laboratories (“VSTLs”) typically accredited by the Election Assistance Commission (“EAC”) had current un-expired accreditations. Therefore, with no valid Federally approved VSTLs, there could be no such VSTL approval of Tennessee’s voting systems for the November 2020 election. (see Exhibit A)

7. Time is of the essence since the 22-month election data retention requirement expires relative to the November 2020 election in early September of 2022.

8. The following diagram illustrates the simplified election process and the claims raised here; the critical piece is the “Black Box / Trapdoor Code”, which is undetected by design and can be used, as Exhibit A shows, to completely remove the link between the ballot inputs and “vote” outputs:



II. PARTIES

9. Plaintiffs are residents and registered voters of the State of Tennessee.

10. Defendant Hargett is named in his official capacity. Defendant Hargett is the Secretary of State for the State of Tennessee. Defendant Stephens is named in his official capacity. Defendant Stephens is the Administrator of the Anderson County Election Commission, County of Anderson, Tennessee.

III. JURISDICTION AND VENUE

11. Plaintiff incorporates the foregoing paragraphs as if set forth in full herein.

12. It is believed this Court has personal jurisdiction as this Court handles the County, State and Federal election matters in this case.

13. It is believed this Court has subject matter jurisdiction over these civil claims regarding election machines. Plaintiffs ask this Court for leniency under pro se law as regards legal terms, form, citation or lack thereof, and use instead its power under the Constitutional right of redress of We the People and pro se law for fashioning a remedy fit for the severity of the facts presented herein.

14. Venue is proper because Defendants perform their official duties in the County of Anderson and the State of Tennessee, the latter affecting every County therein.

15. Tennessee elections were conducted in 2020 and are planned to be conducted in 2022 in a manner that cannot ensure that each vote cast is counted as cast. The voting systems and equipment used in the November 2020 election, and to be used in the November 2022 elections in Tennessee are manufactured by five companies: Hart, MicroVote, Unisyn, ES&S and Dominion, and can be found here at the Tennessee Secretary of State's web site link: (Exhibit L link: Voting Systems by County (07-2022).pdf ([tnsosgovfiles.com](https://sos.gov/files.com)¹⁴) or the same list, attached as Exhibit L, 3 pages, Tennessee Voting Systems by County.)

16. All voting systems in use in Tennessee and the United States, now and in 2020, are subject to tampering through a Trapdoor mechanism inherent in all election systems. This Trapdoor mechanism is described in detail in Exhibit A,

¹⁴ Full link here https://sos-prod.tnsosgovfiles.com/s3fs-public/document/Voting%20Systems%20by%20County%20%2807-2022%29.pdf?VersionId=IQxujfCbugOUDwGg6vO_q7UBXRxi.fFe if hyperlink doesn't work

affidavit of Terpsehore Maras, filed under penalty of perjury on December 1, 2020 in case #2:20-cv-01771-PP Feehan v. Wisconsin Elections Commission (2:20-cv-01771) District Court, E.D. Wisconsin.

17. The key aspect and summary of the sometimes-technical affidavit Exhibit A, in layman's terms, is its paragraph 61: "Hence, you can't prove anyone manipulated anything. The TRAP DOOR KEY HOLDERS can offer you enough to verify to you what you need to see without revealing anything and once again indicating the inability to detect manipulation. ZERO PROOF of INTEGRITY OF THE VOTE."

18. The problem with verifying that any voting machine system gives a fair outcome, where the votes output are identical to the votes input, is that due to the trapdoor mechanism it is impossible to prove that the election was fair. All of this is the responsibility of the Secretary of State, but he refuses to respond.

19. It is also impossible to prove that the election was unfair, but the burden is on the State to prove that its systems are not only capable of conducting, but in fact, conducted, a fair election. This is an impossibility, as Exhibit A demonstrates. Extensive evidence exists, presented herein, that voting machine systems used in Tennessee have the capability to connect to the internet, and given the number of machines in use, it is extremely improbable that no machines were connected to the internet in the November 2020 election and that none were accessed through trapdoor, or wired or wireless external networks.

20. Exhibit A further explains the Federal Help America Vote Act of 2002 ("HAVA") provides for the accreditation of voting systems by Voting Systems Testing Laboratories ("VSTLs") and requirements for EAC certification. States can opt out, but Tennessee applied for and received 2018 through 2020 HAVA funding, despite lack of EAC certification and/or expired VSTL certification on the EAC certificates; rendering EAC certification null and void under federal law. See amounts Tennessee received in 2020 on (attached exhibit M, Report 1, pages 4, 8, 13 & 16 of the report "THE U.S. ELECTION ASSISTANCE COMMISSION 2020 GRANT EXPENDITURE REPORT July 2021), and see pages 4, 6 and 10 for 2019

funds Tennessee received (on attached Exhibit M 2019 EAC Annual Grant Expenditure Report,¹⁵ Report 2, 11 page report, see pages 4,6, and 10) and see (attached Exhibit M, Report 3, pages 4, 6, and 8 of 2018 HAVA Grants Expenditure Report) for HAVA funds received in 2018, but as related prior to this and in Exhibit A, EAC certification is a requirement for a state to legally receive HAVA funding, and no EAC certification has been provided this year when Plaintiffs asked, nor can certification or valid certification be found for these years in question- again, against federal statutes. Additionally, see amounts Tennessee received in Grant Expenditure Report Fiscal Year 2018 in Report 2, 15 pages, and lastly in Exhibit M see:2020 Grant Expenditure Report July 2021, 17 pages.)

Curiously, and likely against the law, on pages 2 and 3 of the minutes of our Tennessee State Election Committee Meeting for April 13, 2020, several members of the Committee made motions and voted to suspend the rules for approval of voting machines, which was actually a suspension of federal law, which is likely beyond the scope of this committee's power: [hyperlink here](https://sos-tn.gov-files.tnsosfiles.com/20200413_SECMinutes.pdf), 20200413_SECMinutes.pdf (tnsosfiles.com)¹⁶ - see Page 2 and part of 3 on following pages:

¹⁵ Full link here [https://www.eac.gov/sites/default/files/paymentgrants/expenditures/2019 EAC Annual Grant Expenditure Report.pdf](https://www.eac.gov/sites/default/files/paymentgrants/expenditures/2019_EAC_Annual_Grant_Expenditure_Report.pdf) if hyperlink doesn't work

¹⁶ Full link here https://sos-tn.gov-files.tnsosfiles.com/20200413_SECMinutes.pdf if hyperlink doesn't work

Old Business

- NONE

New Business

- **Hart InterCivic - Alli Fick, Certification Project Manager**

Alli Fick, Certification Project Manager for Hart InterCivic made the presentation before the commission. (See attached presentation provided by Hart InterCivic.)

- **Verity Voting 2.4 (Modification to Verity 2.3)**

Commissioner Blackburn made a motion to suspend the rules for certification of voting machines due to Covid-19, and to approve Hart InterCivic Verity Voting 2.4, seconded by Commissioner Wallace. The motion to approve Verity Voting 2.4 was unanimously approved. (Aye votes: Barrett, Blackburn, Duckett, McDonald, Wallace, Wheeler and Younce; No votes: None; Abstention: None.)

- **De Minimis Change to Verity 2.3**

Commissioner McDonald made a motion to suspend the rules for certification of voting machines due to Covid-19, and to approve the De Minimis changes to Verity 2.3, seconded by Commissioner Barrett. The motion to approve the De Minimis change to Verity Voting 2.3 was unanimously approved. (Aye votes: Barrett, Blackburn, Duckett, McDonald, Wallace, Wheeler and Younce; No votes: None; Abstention: None.)

- **Dominion – Ian Piper, Director of Certification**

Ian Piper, Director of Certification for Dominion made the presentation before the commission. (See attached presentation provided by Dominion Voting.)

- **Democracy Suite - 5.5B (Modification to Democracy Suite – 5.5)**

Commissioner Barrett made a motion to suspend the rules for certification of voting machines due to Covid-19, and to approve the modification changes of Democracy Suite 5.5 to Democracy Suite 5.5B, seconded by Commissioner McDonald. The motion to approve the Democracy Suite 5.5B was unanimously approved. (Aye votes: Barrett, Blackburn, Duckett, McDonald, Wallace, Wheeler and Younce; No votes: None; Abstention: None.)



Commissioner Wallace made a motion to suspend the rules for certification of voting machines due to Covid-19, and to approve the ECO 100630 Central Scanner to the Cannon COTS scanner, seconded by Commissioner Duckett. The motion to approve the central scanner was unanimously approved. (Aye votes: Barrett, Blackburn, Duckett, McDonald, Wallace, Wheeler and Younce; No votes: None; Abstention: None.)

21. On page 28 of the **Staff Report to Members of the Tennessee**

Advisory Commission on Intergovernmental Relations, December 2018 issue:

web link here: Tennessee's Election Security: A Staff Update (tn.gov)¹⁷ they

indicated their concerns about “a number of potential vulnerabilities in election

infrastructure,” they listed their concerns and listed some measures taken, but

stated “**more needs to be done,**” and made no effort to protect us from the

vulnerabilities they admitted they knew about. Linked above, but included here for

ease of the Court:

“Despite the progress on communication and improvements to the security of our election process, the Committee remains concerned about a number of potential vulnerabilities in election infrastructure.

• Voting systems across the United States are outdated, and many do not have a paper record of votes as a backup counting system that can be reliably audited, should there be allegations of machine manipulation. In

¹⁷ Full link her https://www.tn.gov/content/dam/tn/tacir/2018-publications/2018_Elections.pdf if hyperlink doesn't work

addition, the number of vendors selling machines is shrinking, raising concerns about supply chain vulnerability.

o Paperless Direct Recording Electronic (DRE) voting machines— machines with electronic interfaces that electronically store votes (as opposed to paper ballots or optical scanners)—are used in jurisdictions in 30 states and are at highest risk for security flaws. Five states use DREs exclusively.

• Many aspects of election infrastructure systems are connected to and can be accessed over the internet. Furthermore, systems that are not connected to the internet, such as voting machines, may still be updated via software downloaded from the internet.

These potentially vulnerable systems include some of the core components of U.S. election infrastructure, including systems affiliated with voter registration databases, electronic poll books, vote casting, vote tallying, and unofficial election night reporting to the general public and the media.

Risk-limiting audits are a best practice to mitigate risk.

• Vendors of election software and equipment play a critical role in the U.S. election system, and the Committee continues to be concerned that vendors represent an enticing target for malicious cyber actors. State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of many of these vendors, and while the

Election Assistance Commission issues guidelines for Security, abiding by those guidelines is currently voluntary.

Summary of SSCI Recommendations

The Senate Select Committee on Intelligence has examined evidence of Russian attempts to target election infrastructure during the 2016 U.S. elections. The Committee has reviewed the steps state and local election officials have taken to ensure the integrity of our elections and agrees that U.S. election infrastructure is fundamentally resilient. The Department of Homeland Security, the Election Assistance Commission, state and local governments, and other groups have already taken beneficial steps toward addressing the vulnerabilities exposed during the 2016 election cycle, including some of the measures listed below, but more needs to be done.” . . .

On page 3 of *The Tennessee Advisory Commission on Intergovernmental Relations’ Legislative Update, June 15, 2022*

Memorandum; link here: [Tab 4 Legislative Update \(tn.gov\)](#),¹⁸ it can be seen they reported that the 112th General Assembly considered election security matters; a topic they had previously studied since 2007, but failed to make any rulings to protect the vote of we the people of Tennessee against these known internet vulnerabilities—linked above, but included below for ease of the Court:

¹⁸ Full link is https://www.tn.gov/content/dam/tn/tacir/commission-meetings/2022june/2022June_Tab4LegisUpdate_Memo.pdf if hyperlink can't be used

“Elections

*The 112th General Assembly considered a variety of bills related to election security, a topic the Commission has studied previously, both in its 2007 staff report, *Trust but Verify: Increasing Voter Confidence in Election Results*, and in a 2018 staff report, *Tennessee’s Election Security: A Staff Update*. Both of these reports recommended that the state adopt voting machines that allow for voter-verifiable paper audit trails. This year the General Assembly did pass Senate Bill 2558 by Jackson and House Bill 2331 by Bricken, which requires that every voting machine used by a county election commission produce a voter-verifiable paper record by default, rather than just have the capability of doing so. The law requires voting machines meet this standard by January 1, 2024. The 112th General Assembly considered but did not pass two similar bills, Senate Bill 687 by Gilmore and House Bill 689 by Beck, along with Senate Bill 2113 by Yarbrow and House Bill 2239 by Freeman. The General Assembly also considered Senate Bill 1865 by Jackson and House Bill 1883 by Rudd, which would have required the secretary of state to conduct forensic audits of at least five counties after every statewide election, starting in 2024. And Senate Bill 2617 by Niceley and House Bill 2827 by Parkinson would have conditioned the use of voting machines to the approval of the local governing body.”*

22. As shown above, our Tennessee Legislature has been aware of the threat to the security of our elections, but has failed to enact the numerous requirements as to procedure and safeguards as required in Article 1, § 4 and §5, Election Clauses of our Constitution:

“State authority to regulate the times, places, and manner of holding congressional elections has been described by the Court as “embrac[ing] authority to provide a complete code for congressional elections ...; in short, to enact the numerous requirements as to procedure and safeguards which experience shows are necessary in order to enforce the fundamental rights involved.” Smiley v. Holm, 285 U.S. 355, 366 (1932.)

23: Despite Plaintiffs asking Mark Stephens, Anderson County’s Election Commission Administrator many times to provide the certification for our county’s voting machines; he could and/or would not provide such, the last time telling us to contact the state for certification. Plaintiffs contacted Secretary of State Tre Hargett multiple times via email; phone, affirmed hand-delivery of these emails by two of his assistants; and made follow-up inquiry phone calls, but our Secretary of State failed to answer any questions in any manner- he has not returned any phone call or email over the three-week period prior to this filing. Because elections happen in mere weeks, we the people therefore assert our right to redress as per the Constitution and now ask this Court for an emergency Temporary Restraining Order against the use of all electronic voting machines in Tennessee until this matter is fully investigated and remedied.

24. In particular, the model of voting machines used by Anderson County, Tennessee, the Hart Intercivic Model No. eslate 3000, Serial No AOB1 A7 US Patent # 6,250,548B1, appears to lack EAC certification as it has not been given when requested by Administrator Stephens, and Secretary Hargett refuses to answer, and Plaintiffs cannot find that model on the State of Tennessee Department of State Division of Elections' Approved Voting Machines – January 11, 2021, nor is it on the list of Approved Voting Machines Currently in Use or Marketed in Tennessee as of July 7, 2021. Regardless of machine type, the attached sworn affidavits and forensic reports from Ms. Maras, Mr. Smith, Ms. Zack, and Ms. Peters, all demonstrate and *prove* how most, if not all of the voting machines on the two Tennessee State lists above or on Exhibit J have been and are able to be infiltrated and thus our voting results have been compromised.

25: Plaintiffs have shown with attached evidence that our electronic voting machines are compromised, likely in totality, across our state and have shown that our legislative members have failed in their duty to provide for safeguards in this matter. We have shown that our legislation was aware of these electronic threats, but kept parking bills in committee, and passed no legislation to protect us from these known threats. For our legislative members to knowingly fail to protect our vote(s) from being subverted is a violation of the oaths they swore to uphold in both our State Constitution and our Constitution as per Amendment XIV, § 3 of our Constitution:

“No person shall be a Senator or Representative in Congress, or elector of President and Vice-President, or hold any office, civil or military, under the United States, or under any State, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any State legislature, or as an executive or judicial officer of any State, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof. But Congress may by a vote of two-thirds of each House, remove such disability.” Askance for consideration of these very serious matters is made in the demands herein for their failure to protect against the known subversion of our vote.

26. We have additionally shown how many of our machines are and were not certified for this election, nor the 2020 and 2018 elections, according to EAC standards, yet our state took HAVA funding in 2018 and 2020, likely in violation of Federal Statutes. Likewise, our Secretary of State, Tre Hargett, has failed to act on our behalf in this matter despite multiple notifications.

27. In the list of approved voting machines included in the 7-19-2018 *Minutes of the State Election Commission Meeting*, beginning page 158 of hyperlink [Exhibit N 20180709_SECMinutes.pdf \(tnsosfiles.com\)](#)¹⁹ (copy of which is Attached, 3 pages in Exhibit N), please note Anderson County’s voting machine, the Hart InterCivic Model No. eslate-3000 is not included on this list and does not appear to be certified, as one Plaintiff has combed through the minutes and verified that no EAC certification exists, in keeping with what is attested in Exhibit A- the VSTL certifications are expired for all of the EAC certificates presented, rendering the EAC certificates invalid for all the states’ voting machines, leaving the machines uncertified per HAVA standards, and the state in violation of federal statutes for receiving HAVA funding without valid EAC certification.

28. The Supreme Court of the United States has recognized that the right to vote consists of not only casting a ballot, but having that vote counted

¹⁹ Full link here https://sos-tn.gov-files.tnsosfiles.com/20180709_SECMinutes.pdf if hyperlink doesn't work

accurately, as it was cast.

29. "We regard it as equally unquestionable that the right to have one's vote counted is as open to protection by Congress as the right to put a ballot in a box." *See United States v. Mosley, 238 U.S. 386 (1915)*

30. "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *See Wesberry v. Sanders, 376 U.S. 17 (1964)*

31. "No one would deny that the equal protection clause would . . . prohibit a law that would expressly give certain citizens a half-vote and others a full vote. . .

[T]he constitutionally guaranteed right to vote and the right to have one's vote counted clearly imply the policy that state election systems, no matter what their form, should be designed to give approximately equal weight to each vote cast. . .

[A] state legislature cannot deny eligible voters the right to vote for Congressmen and the right to have their vote counted." *See Reynolds v. Sims, 377 U.S. 563*

(1964), citing Colegrove v. Green, 328 U.S. 549, 328 U.S. 569-571

32. By utilizing voting machines subject to the Trapdoor mechanism described in Exhibit A, Tennessee has deprived its voters of the capability of knowing that their vote was accurately counted.

33. In further support of all the above, attached is the transcript of the

sworn Senate testimony of computer programmer Clint Curtis in 2004, in which he affirmed the content of all the above attached affiant's affidavits- our election

machines can be accessed at any time, and our votes switched at will. See Exhibit O

for written transcript and written link to the testimony, here is the link to watch it:

<https://rumble.com/v1h6lwn-clinton-eugene-curtis-elections-have-been-stolen-using-machine-algorithms-s.html>

34. Attached is the affidavit of Clint Curtis, in which, again, he affirms all above affidavits. See Exhibit P, 4 pages.

DEMAND FOR JUDGMENT

A) Plaintiff repeats and re-alleges every allegation contained in the foregoing paragraphs as if fully plead herein.

B) Considering the above and attached, Plaintiffs have clearly shown that our vote has the means to be disenfranchised and will continue to be in danger of such if continued use of electronic machines is allowed. Therefore, Plaintiffs demand the order of a full forensic audit and investigation of Tennessee's November 2020 election results, data and electronic machines, and additionally demand an immediate order for the preservation of all 2020 election data and records be they electronic, non-paper, electronic machinery or attachments, printers or accessories of any kind or any other form for the 2020 election, as this data is critical to election integrity and is scheduled to be destroyed in mere days. A full audit of the November 2020 election data would show whether any voting system in any County in Tennessee was connected to the internet by the hidden trapdoor mechanism outlined in Exhibit A. Preservation of this data is critical to election integrity. Irreparable harm will be suffered if these records are destroyed, as there will be no way to prove the integrity of our vote.

C) Plaintiffs make demand for an emergency temporary/permanent

injunction restraining order against the use of any electronic voting equipment or method in the State of Tennessee until this investigation is complete.

C) Plaintiffs make demand for an order that all future elections in Tennessee be conducted using the paper ballot method described in Exhibit A, and that a method such as hourly repetitive public service announcements on Tennessee's television news stations and a variety of radio stations throughout the entirety of the state be put in place to make a state-wide call for volunteers to make this happen. Our citizens will undoubtedly answer and once again live up to what we are famous for.

E) Demand is made to order Defendant Hargett or his successor to re-tabulate the results of every county in Tennessee for the 2020 elections, using our state's volunteers to verify each vote from ballot results from every electronic machine with each voter, then tabulate and compare that result to the 2020 tabulations to assure the integrity of each and every outcome, and decertify any 2020 election result if new, verified results do not match what was tabulated for the 2020 elections.


F) Demand is made for this Court to take action as per the law to legally and rightfully address the actions/lack of action of Defendants and each State Election Committee and Legislative Member who failed to act, as was their duty, to protect our vote when told multiple times of these threats, who made motion to suspend federal rules and lower the standard of protection of the integrity of our

vote , and who failed to pass waiting legislative protection against these known threats to our vote and left the legislation parked, because to knowingly fail to act, and to knowingly proceed to participate in any way with the subversion of the vote of the people is a serious matter. We the people can fill the seats of any vacancies left in these elected seats, until elections can be held. For any named Defendant who chooses to refute this evidence instead of resign, Demandant must contact the Clerk for date and time of hearing, Clerk must sign subpoenas for Plaintiffs, and we demand this Court hold a hearing within ten days of service of Summons. We the people have the right to alter or abolish any government that goes against its original foundation and then reset it back on its original foundation, and we Plaintiffs, members in good standing of We the People now make motion of this Court for all the above.²⁰

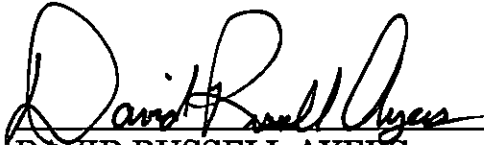
G) Askance is made for any other relief as this Court deems just and proper in this matter.

²⁰²⁰ The Constitution is the supreme law of the land. *"A law repugnant to the Constitution is void."* *Marbury v Madison* 1803.

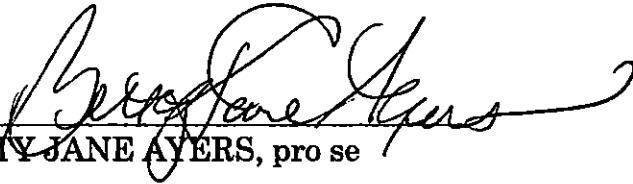
Further, these affiants sayeth naught.



SARAH WALKER BRUUN, pro se



DAVID RUSSELL AYERS, pro se



BETTY JANE AYERS, pro se

Plaintiff Names and Addresses

2022 SEP 21 PM 4:19
FILED AC CIRCUIT COURT

Betty Jane Ayers, pro se
162 Wade Lane
Oak Ridge, TN 37830
865-243-5217

David Russell Ayers, pro se
162 Wade Lane
Oak Ridge, TN 37830
865-243-5047

Sarah Walker Braun, pro se
405 Hartan Rd SE
Cleveland, TN 37323
206-436-9169

Defendants are welcome to
serve Betty Ayers and she
will send papers to the others.

Betty Ayers

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
ANDERSON COUNTY

SARAH ELIZABETH MORANO
DAVID RUSSELL AYERS and
BETTY JANE AYERS, in their personal capacities
as residents of and registered voters in Anderson County
Plaintiffs,

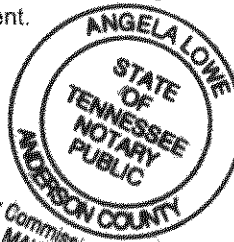
v. Case Number To Be Assigned

TRE HARGETT, in his official capacity as
Secretary of State of the State of Tennessee, and
MARK STEPHENS, in his official capacity as
Administrator, Anderson County Election Commission
Defendants

**Re: COMPLAINT, MOTIONS FOR EMERGENCY ORDERS OF TEMPORARY
RESTRAINING ORDER AGAINST THE USE OF ELECTRONIC VOTING MACHINES
& TO PRESERVE ALL VOTING RECORDS FROM 2020 ELECTIONS**

Betty Jane Ayers, a resident of the State of Tennessee, County of Anderson, Personally
appeared before me _____ (Name of Officer.)
_____ (Official Capacity of Officer.) regarding the above
captioned matter and makes this her statement and General Affidavit upon oath and
affirmation of belief and personal knowledge that the matters, facts and things set forth
in the above captioned case are true and correct to the best of her knowledge, and that
this matter is presented with no ill intent.



Signature



Notary Public Acknowledgment

Tennessee Anderson SEAL
State of County of

I hereby certify that Betty Jane Ayers (Name) appeared before me on
this 20th day of September, 2022 and signed this form in my presence.


Notary Public Signature

05-28-2025
My Commission Expires (Date)

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
ANDERSON COUNTY


SARAH ELIZABETH MORANO
DAVID RUSSELL AYERS and
BETTY JANE AYERS, in their personal capacities
as residents of and registered voters in Anderson County
Plaintiffs,

v. Case Number To Be Assigned

TRE HARGETT, in his official capacity as
Secretary of State of the State of Tennessee, and
MARK STEPHENS, in his official capacity as
Administrator, Anderson County Election Commission
Defendants

**Re: COMPLAINT, MOTIONS FOR EMERGENCY ORDERS OF TEMPORARY
RESTRAINING ORDER AGAINST THE USE OF ELECTRONIC VOTING MACHINES
& TO PRESERVE ALL VOTING RECORDS FROM 2020 ELECTIONS**

David Russell Ayers, a resident of the State of Tennessee, County of Anderson,
Personally appeared before me _____ (Name of
Officer,) _____ (Official Capacity of Officer.) regarding
the above captioned matter and makes this his statement and General Affidavit upon
oath and affirmation of belief and personal knowledge that the matters, facts and things
set forth in the above captioned case are true and correct to the best of his knowledge,
and that this matter is presented with no ill intent.



Signature



Notary Public Acknowledgment

Tennessee Anderson SEAL
State of County of

I hereby certify that David Russell Ayers (Name) appeared May 28, 2025 My Commission Expires
this 20th day of September, 2022 and signed this form in my presence.


Notary Public Signature 05-28-2025
My Commission Expires (Date)

CERTIFICATE OF SERVICE

Plaintiff filed the attached Complaint in person at the Clerk's Office of the

**ANDERSON COUNTY CIRCUIT COURT
ANDERSON TENNESSEE**

Plaintiffs have also served this Complaint upon the following defendants via USPS or FEDEX certified mail:

Secretary Tre Hargett, Business Office
312 Rosa L. Parks Avenue 6th Floor, Snodgrass Tower
Nashville, TN 37243-1102 615-741-2819

Administrator Mark Stephens
100 North Main Street, Room 207
Clinton, TN 37716-3683 865-457-6238

Herbert H. Slatery III, Attorney General and Reporter for the State of Tennessee,
P.O. Box 20207 Nashville, TN 37202-0207 Telephone: (615) 741-3491

Janet M Kleinfelter, Deputy Attorney General for the State of Tennessee,
P.O. Box 20207 Nashville, TN 37202 (615) 741-7403

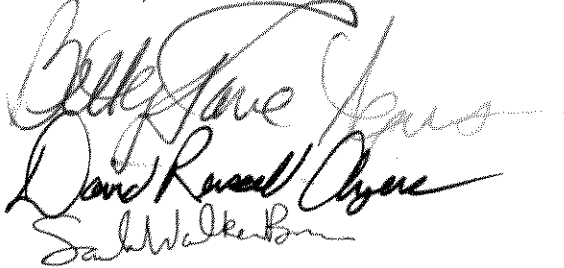
David Kustoff, Congressman,
5900 Poplar Avenue Suite 202 Memphis, TN 38119 901-682-4422

Jim Cooper, Congressman,
1536 Longworth HOB Washington, DC 20515 202-225-4311

Steve Cohen, Congressman, Odell Horton Fed Bldg 167 North Main Street, Suite
369 Memphis, TN 38103 901-544-4131

Marsha Blackburn, Senator, 800 Market Street Suite 121 Knoxville, TN 37902
865-540-3781

Bill Hagerty, Senator, 3322 West End Avenue Suite 120
Nashville, TN 37203 615-736-5129



9-20-22

Betty Jane Ayers, Plaintiff, pro se
David Russell Ayers, Plaintiff, pro se
Sarah Walker Bruun, Plaintiff, pro se

DATE

Exhibit A

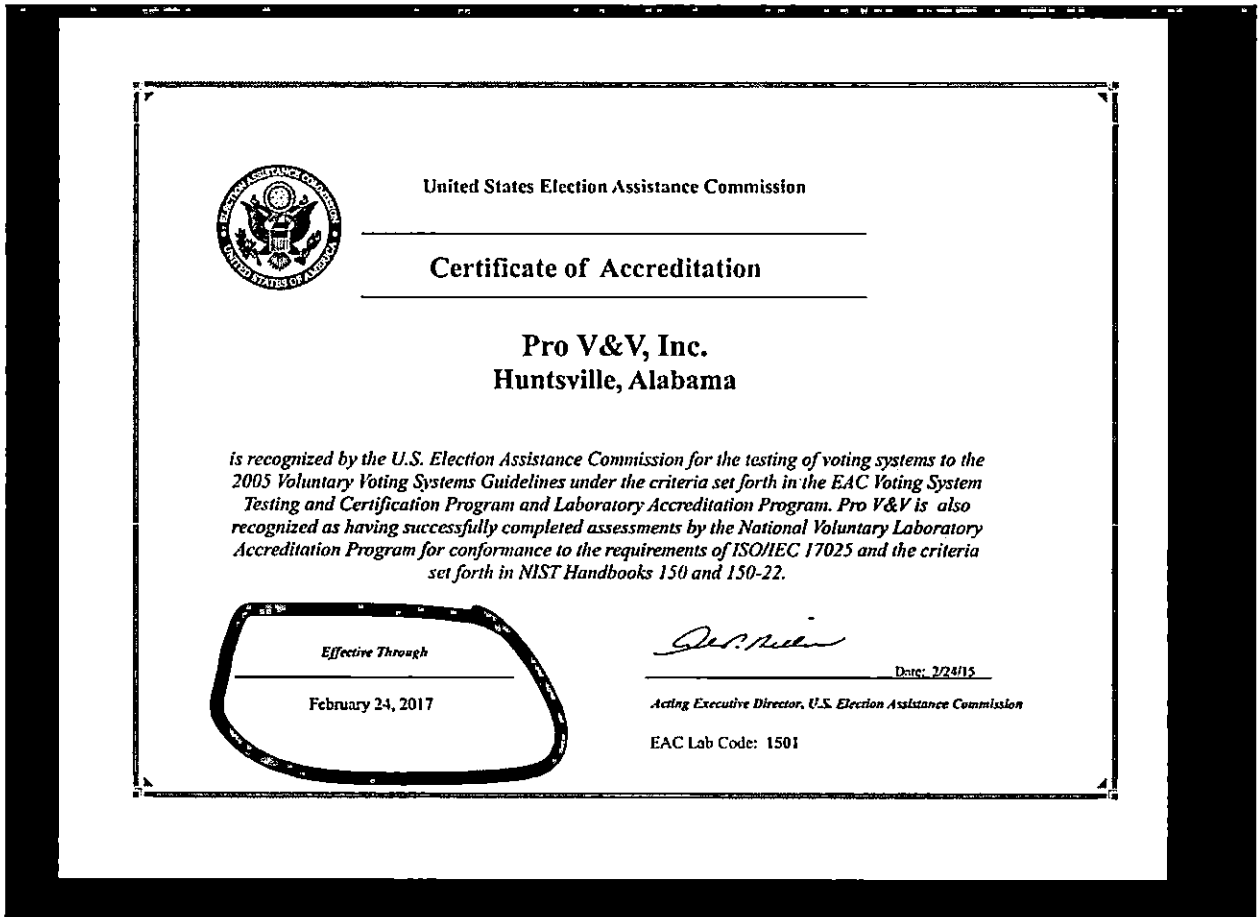
37 pages

Declaration of [REDACTED]

Pursuant to 28 U.S.C Section 1746, I, [REDACTED], make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I have been a private contractor with experience gathering and analyzing foreign intelligence and acted as a LOCALIZER during the deployment of projects and operations both OCONUS and CONUS. I am a trained Cryptolinguist, hold a completed degree in Molecular and Cellular Physiology and have FORMAL training in other sciences such as Computational Linguistics, Game Theory, Algorithmic Aspects of Machine Learning, Predictive Analytics among others.
3. I have operational experience in sources and methods of implementing operations during elections both CONUS and OCONUS
4. I am an amateur network tracer and cryptographer and have over two decades of mathematical modeling and pattern analysis.
5. In my position from 1999-2014 I was responsible for delegating implementation via other contractors sub-contracting with US or 9 EYES agencies identifying connectivity, networking and subcontractors that would manage the micro operations.
6. My information is my personal knowledge and ability to detect relationships between the companies and validate that with the cryptographic knowledge I know and attest to as well as evidence of these relationships.
7. In addition, I am WELL versed due to my assignments during my time as a private contractor of how elections OCONUS (for countries I have had an assignment at) and CONUS (well versed in HAVA ACT) and more.
8. On or about October 2017 I had reached out to the US Senate Majority Leader with an affidavit claiming that our elections in 2017 may be null and void due to lack of EAC certifications. In fact Sen. Wyden sent a letter to Jack Cobb on 31 OCT 2017 advising discreetly pointing out the importance of being CERTIFIED EAC had issued a certificate to

Pro V & V and that expired on Feb 24, 2017. No other certification has been located.



9. Section 231(b) of the Help America Vote Act (HAVA) of 2002 (42 U.S.C. §15371(b)) requires that the EAC provide for the accreditation and revocation of accreditation of independent, non-federal laboratories qualified to test voting systems to Federal standards. Generally, the EAC considers for accreditation those laboratories evaluated and recommended by the National Institute of Standards and Technology (NIST) pursuant to HAVA Section 231(b)(1). However, consistent with HAVA Section 231(b)(2)(B), the Commission may also vote to accredit laboratories outside of those recommended by NIST upon publication of an explanation of the reason for any such accreditation.

United States Department of Commerce
National Institute of Standards and Technology



Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200978-0

Pro V&V
Huntsville, AL


*is accredited by the National Voluntary Laboratory Accreditation Program for specific services,
listed on the Scope of Accreditation, for:*

Voting System Testing

*This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017.
This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality
management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).*

2020-03-26 through 2021-03-31
Effective Dates




For the National Voluntary Laboratory Accreditation Program

10.

11. VSTL's are VERY important because equipment vulnerabilities allow for deployment of algorithms and scripts to intercept, alter and adjust voting tallies.
12. There are only TWO accredited VSTLs (VOTING SYSTEM TEST LABORATORIES). In order to meet its statutory requirements under HAVA §15371(b), the EAC has developed the EAC's Voting System Test Laboratory Accreditation Program. The procedural requirements of the program are established in the proposed information collection, the EAC Voting System Test Laboratory Accreditation Program Manual. Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants. The procedural requirements of this Manual will supersede any prior laboratory accreditation requirements issued by the EAC. This manual shall be read in conjunction with the EAC's Voting System Testing and Certification Program Manual (OMB 3265-0019).



MICHIGAN

<i>State Participation:</i>	Requires Testing by an Independent Testing Authority. MI requires that voting systems are certified by an independent testing authority accredited by NASED and the board of state canvassers.
<i>Applicable Statute(s):</i>	"An electronic voting system shall not be used in an election unless it is approved by the board of state canvassers ... and unless it meets 1 of the following conditions: (a) Is certified by an independent testing authority accredited by the national association of state election directors and by the board of state canvassers. (b) In the absence of an accredited independent testing authority, is certified by the manufacturer of the voting system as meeting or exceeding the performance and test standards referenced in subdivision (a) in a manner prescribed by the board of state canvassers." <u>MICH. COMP. LAWS ANN § 168.795a</u> (2009).
<i>Applicable Regulation(s):</i>	MI does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State accepts requests from persons/corporations wishing to have their voting system examined. The requestor must pay the Secretary of State an application fee of \$1,500.00, file a report listing all of the states in which the voting system has been approved and any reports that these states have made regarding the performance of the voting system. The Board of State Canvassers conducts a field test involving Michigan electors and election officials in simulated election day conditions. The Board of State Canvassers shall approve the voting system if it meets all of the state requirements. <u>MICH. COMP. LAWS ANN § 168.795a</u> (2009).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> <u>http://www.michigan.gov/sos/0,1607.7-127-1633_8716_45458--,00.html</u>



WISCONSIN

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. WI requires that its voting systems receive approval from an independent testing authority accredited by NASED verifying that the voting systems meet all of the recommended FEC standards.
<i>Applicable Statute(s):</i>	“No ballot, voting device, automatic tabulating equipment or relating equipment and materials to be used in an electronic voting system may be utilized in this state unless it is approved by the board [of election commissioners].” <u>WIS. STAT.ANN. § 5.91</u> (West 2009).
<i>Applicable Regulation(s):</i>	“An application for approval of an electronic voting system shall be accompanied by all of the following ... [r]eports from an independent testing authority accredited by the national association of state election directors (NASED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission.” <u>WIS. ADMIN. CODE GAB § 7.01</u> (2009).
<i>State Certification Process:</i>	The Board of Election Commissioners accepts applications for the approval of electronic voting systems. Once the application is completed, the vendor must set up the voting system for three mock elections using; (1) offices, (2) referenda questions and (3) candidates. A panel of local election officials can assist the Board in the review of the voting system. The Board conducts the test using a mock election for the partisan primary, general election, and nonpartisan election. The Board may also require that the voting system be used in an actual election as a condition of the approval. <u>WIS. ADMIN. CODE GAB §§ 7.01, 7.02</u> (2009).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://elections.state.wi.us/section.asp?linkid=643&locid=47



GEORGIA

State Participation: Requires Federal Certification. GA requires that its voting systems are tested to EAC standards by EAC accredited labs and certified by the EAC.

Applicable Statute(s): “Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any voting machine may request the Secretary of State to examine the machine. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any voting machine previously examined and approved by him or her. Before any such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination; provided, however, that in the case of a request by ten or more electors the examination fee shall be \$ 250.00. The Secretary of State may, at any time, in his or her discretion, reexamine any voting machine.” GA CODE ANN. § 21-2-324 (2008).

Applicable Regulation(s): “Prior to submitting a voting system for certification by the State of Georgia, the proposed voting system’s hardware, firmware, and software must have been issued Qualification Certificates from the EAC. These EAC Qualification Certificates must indicate that the proposed voting system has successfully completed the EAC Qualification testing administered by EAC approved ITAs. If for any reason, this level of testing is not available, the Qualification tests shall be conducted by an agency designated by the Secretary of State. In either event, the Qualification tests shall comply with the specifications of the *Voting Systems Standards* published by the EAC.” GA. COMP. R. & RES. 590-8-1-.01 (2009).

State Certification Process: After the voting system has passed EAC Qualification testing, the vendor of the voting system submits a letter to the Office of the Secretary of State requesting certification for the voting system along with a technical data package to the certification agent. An evaluation proposal is created by the certification agent after a preliminary view of the Technical Data Package and sent to the vendor. Any additional EAC ITA testing identified in the evaluation proposal is arranged by the vendor and the certification agent will perform all other tests identified in the evaluation proposal. The certification agent submits a report of their findings to the Secretary of State. Based on these findings the Secretary of State will make a final determination on whether to certify the voting system. GA. COMP. R. & RES. 590-8-1-.01 (2009).

Fielded Voting Systems: *[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].*
<http://www.sos.georgia.gov/Elections/>



PENNSYLVANIA

- State Participation:** Requires Testing by a Federally Accredited Laboratory. PA requires that its voting systems are approved by a federally recognized independent testing laboratory as meeting federal voting system standards.
- Applicable Statute(s):** “Any person or corporation owning, manufacturing or selling, or being interested in the manufacture or sale of, any electronic voting system, may request the Secretary of the Commonwealth to examine such system if the voting system has been examined and approved by a federally recognized independent testing authority and if it meets any voting system performance and test standards established by the Federal Government.” 25 PA. CONS. STAT. ANN. Code § 3031.5 (West 2008).
- Applicable Regulation(s):** PA does not have a regulation regarding the federal certification process.
- State Certification Process:** The Secretary of State examines voting systems, upon request, once the voting systems have received approval by a federally recognized independent testing authority. The person(s) requesting the examination of the voting system are responsible for the cost of the examination. After the examination, the Secretary of State issues a report stating whether or not the voting systems are safe and compliant with state and federal requirements. If the voting systems are deemed safe and compliant by the Secretary of State then the systems may be adopted and approved for use in elections by each county through a majority vote of its qualified electors. 25 PA. CONS. STAT. ANN. Code §§ 3031.5, 3031.2 (West 2008).
- Fielded Voting Systems:** *[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].*
<http://www.votespa.com/HowtoVote/tabid/74/language/en-US/Default.aspx>



ARIZONA

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. AZ requires that its voting systems are HAVA compliant and approved by a laboratory that is accredited pursuant to HAVA.
<i>Applicable Statute(s):</i>	“On completion of acquisition of machines or devices that comply with HAVA, machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with HAVA and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to HAVA.” <u>ARIZ. REV. STAT. § 16-442(B)</u> (2008).
<i>Applicable Regulation(s):</i>	AZ does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State appoints a committee of three people that test different voting systems. This committee is required to submit their recommendations to the Secretary of State who then makes the final decision on which voting system(s) to adopt. <u>ARIZ. REV. STAT. § 16-442(A) and (C)</u> (2008).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> <u>http://www.azsos.gov/election/equipment/default.htm</u>

17.

18. **Pro V& V and SLI Gaming** both lack evidence of EAC Accreditation as per the Voting System Testing and Certification Manual.

19. Pro V& V is owned and Operated by Jack Cobb. Real name is Ryan Jackson Cobb. The company ProV&V was founded and run by Jack Cobb who formerly worked under the entity of Wyle Laboratories which is an AEROSPACE DEFENSE CONTRACTING ENTITY. The address information on the EAC, NIST and other entities for Pro V& V are different than that of what is on ProV&V website. The EAC and NIST (ISO CERT) issuers all have another address.

The screenshot shows a web browser window with the URL <https://eac-legacy.ac-admin.com/Testing-equipment/Testing-system-test-laboratories-v&v/>. The page features a search bar with 'SEARCH' and 'CLEAR' buttons. Below the search bar, the heading 'Accredited Labs' is displayed, followed by '2 results found. Page 1 of 1'. Two lab entries are listed:

- Pro V&V**
700 Boulevard South
Suite 102
Huntsville, AL 35802
Status: Accredited
Program Manager: Jack Cobb, President
Phone: 256-713-1111
[Learn More >](#)
- SLI Compliance, a Division of Gaming Laboratories International, LLC**
4720 Independence Street
Wheat Ridge, CO 80033
Status: Accredited
Program Manager: Traci Mappa, Director of Operations
Phone: 303-422-1566
[Learn More >](#)

On the right side of the page, there are several promotional boxes:

- Frequently Asked Questions**
- Manuals and Forms**
- Test and Certification Blogs**
- DO YOU HAVE QUESTIONS?**
Send your questions to us at info@provv.com or click the button below to contact us.
[Contact Us](#)
(Click to email to your table)
- REGISTER TO VOTE!**
Use the National Mail Voter Registration Form to register to vote, update your registration information with a new name or address, or register with a political party.
Note: If you wish to vote absentee and are a uniformed service member or family member or a citizen living outside the U.S., contact the Federal Voting Assistance Program to register to vote.
[Register Today](#)

The screenshot shows a contact form on the ProV&V website. The URL is www.provv.com/contact/. The form includes the following fields:

- Your Name (required)
- Your Email (required)
- Subject
- Your Message

On the right side of the form, the contact information for Pro V&V is provided:

- Pro V&V
- 6705 Odyssey Drive NW
- Suite C
- Huntsville, AL 35806
- Office: 256-713-1111
- Fax: 256-713-1112

At the bottom of the form is a 'Send' button. Below the form, the copyright notice reads: © 2020 Pro V&V, Inc. All rights reserved.

20. VSTLs are the most important component of the election machines as they examine the use of COTS (Commercial Off-The-Shelf)
21. “Wyle became involved with the testing of electronic voting systems in the early 1990’s and has tested over 150 separate voting systems. Wyle was the first company to obtain accreditation by the National Association of State Election Directors (NASD). Wyle is accredited by the Election Assistance Commission (EAC) as a Voting System Testing Laboratory (VSTL). Our scope of accreditation as a VSTL encompasses all aspects of the hardware and software of a voting machine. Wyle also received NVLAP accreditation to ISO/IEC 17025:2005 from NIST.” Testimony of Jack Cobb 2009
22. COTS are preferred by many because they have been tried and tested in the open market and are most economic and readily available. COTS are also the SOURCE of vulnerability therefore VSTLs are VERY important. COTS components by voting system machine manufacturers can be used as a “Black Box” and changes to their specs and hardware make up change continuously. Some changes can be simple upgrades to make them more efficient in operation, cost efficient for production, end of life (EOL) and even complete reworks to meet new standards. The key issue in this is that MOST of the COTS used by Election Machine Vendors like Dominion, ES&S, Hart Intercivic, Smartmatic and others is that such manufacturing for COTS have been outsourced to China which if implemented in our Election Machines make us vulnerable to BLACK BOX antics and backdoors due to hardware changes that can go undetected. This is why VSTL’s are VERY important.
23. The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAILABLE and HOUSED on the HARDWARE. This is a vulnerability. Exporting system reporting using software like Crystal Reports, or PDF software allows for vulnerabilities with their constant updates.
24. As per the COTS hardware components that are fixed, and origin may be cloaked under proprietary information a major vulnerability exists since once again third-party support software is dynamic and requires FREQUENT updates. The hardware components of the computer components, and election machines that are COTS may have slight updates that can be overlooked as they may be like those designed that support the other third -party software. COTS origin is important and the US Intelligence Community report in 2018 verifies that.
25. The Trump Administration made it clear that there is an absence of a major U.S. alternative to foreign suppliers of networking equipment. This highlights the growing dominance of

Chinese manufacturers like Huawei that are the world's LARGEST supplier of telecom and other equipment that endangers national security.

26. China, is not the only nation involved in COTS provided to election machines or the networking but so is Germany via a LAOS founded Chinese linked cloud service company that works with SCYTL named Akamai Technologies that have offices in China and are linked to the server that Dominion Software.

28 046 Madrid

Asian offices

Akamai Technologies - India
111, Brigade Court
Koramangala Industrial Area
Bangalore 560 095, India

Telephone: 91-80-575-99222
Fax: 91-80-575-99209
Regional Manager: Stuart Spiteri

Akamai Technologies - China
Suite 1560, 15th Floor
NCI Tower
12A Jianguomenwai Avenue
Chaoyang District,
Beijing 100022
China

Telephone: 86-10-8523-3097
Fax: 86-10-8523-3001
Regional Manager: Stuart Spiteri

Akamai Japan K.K.
The Executive Centre Japan K.K.
15F Tokyo Ginko Kyokai building
1-3-1 Marunouchi, Chiyoda-ku, Tokyo 100-0005

Telephone: 81-3-3216-7200 (Centre)
81-3-3216-7300 (Akamai direct)
Fax: 81-3-3216-7390 (Centre)
Regional Manager: Stuart Spiteri

Akamai Technologies - Singapore
Akamai, Regus Centre, 36-01 UOB Plaza 1
80 Raffles Place
Singapore 048624
 Driving directions

Telephone: +65 6248 4614
Fax: +65 6248-4501
Regional Manager: Stuart Spiteri

Akamai Technologies - Australia and New Zealand
201 Sussex St
Tower 2, Level 20
Sydney, NSW 2000, Australia
info@au.akamai.com

Telephone: 61 2 9006 1325
Fax: 61 2 9475 0343
Regional Manager: Stuart Spiteri

pft.gov resolves to 4.30.228.74. According to our data this IP address belongs to Level 3 Communications and is located in Alexandria, Virginia, United States. Please have a look at the information provided below for further details.

4.30.228.74

ISP/Organization

Level 3 Communications

Location

Alexandria 22304, Virginia (VA), United States (US)

Latitude

38.8115 / 38°48'41" N

Longitude

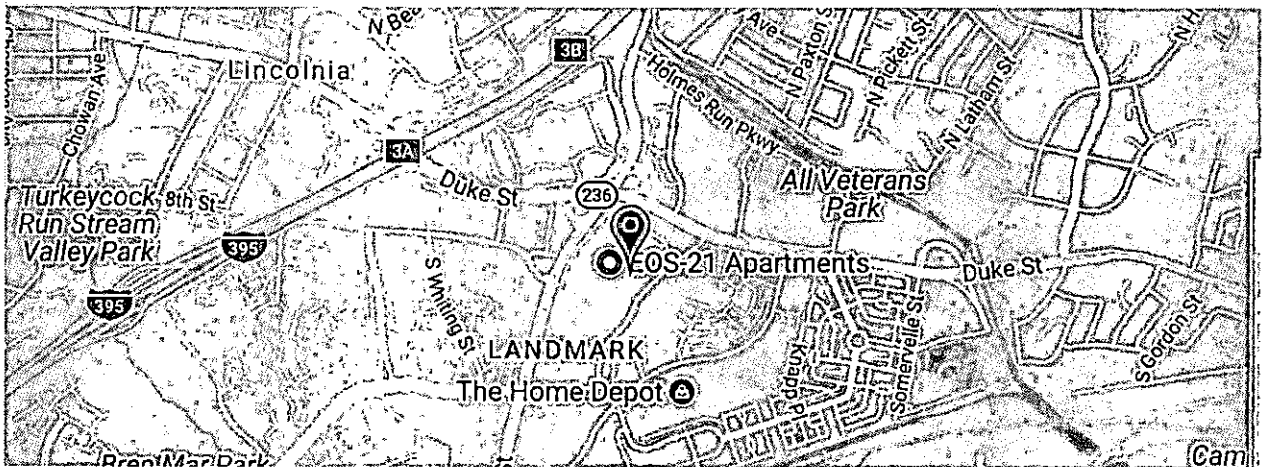
-77.1285 / 77°7'42" W

Timezone

America/New_York

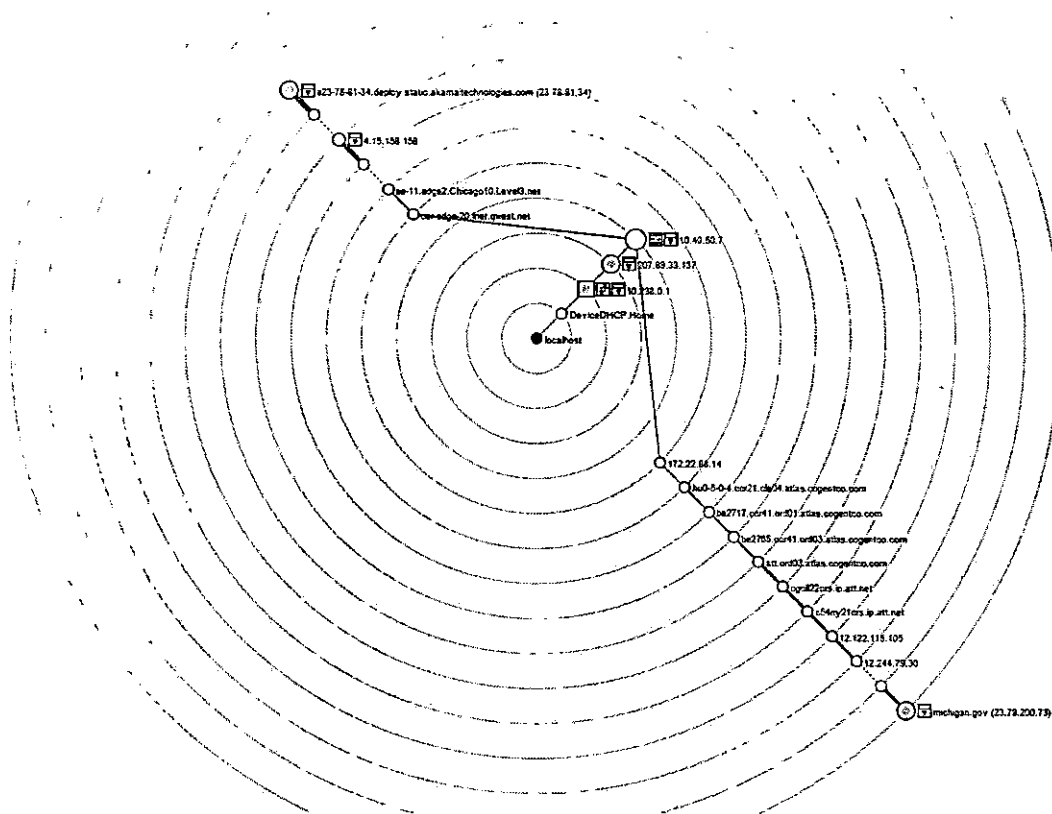
Local Time

Thu, 12 Jul 2018 19:27:40 -0400

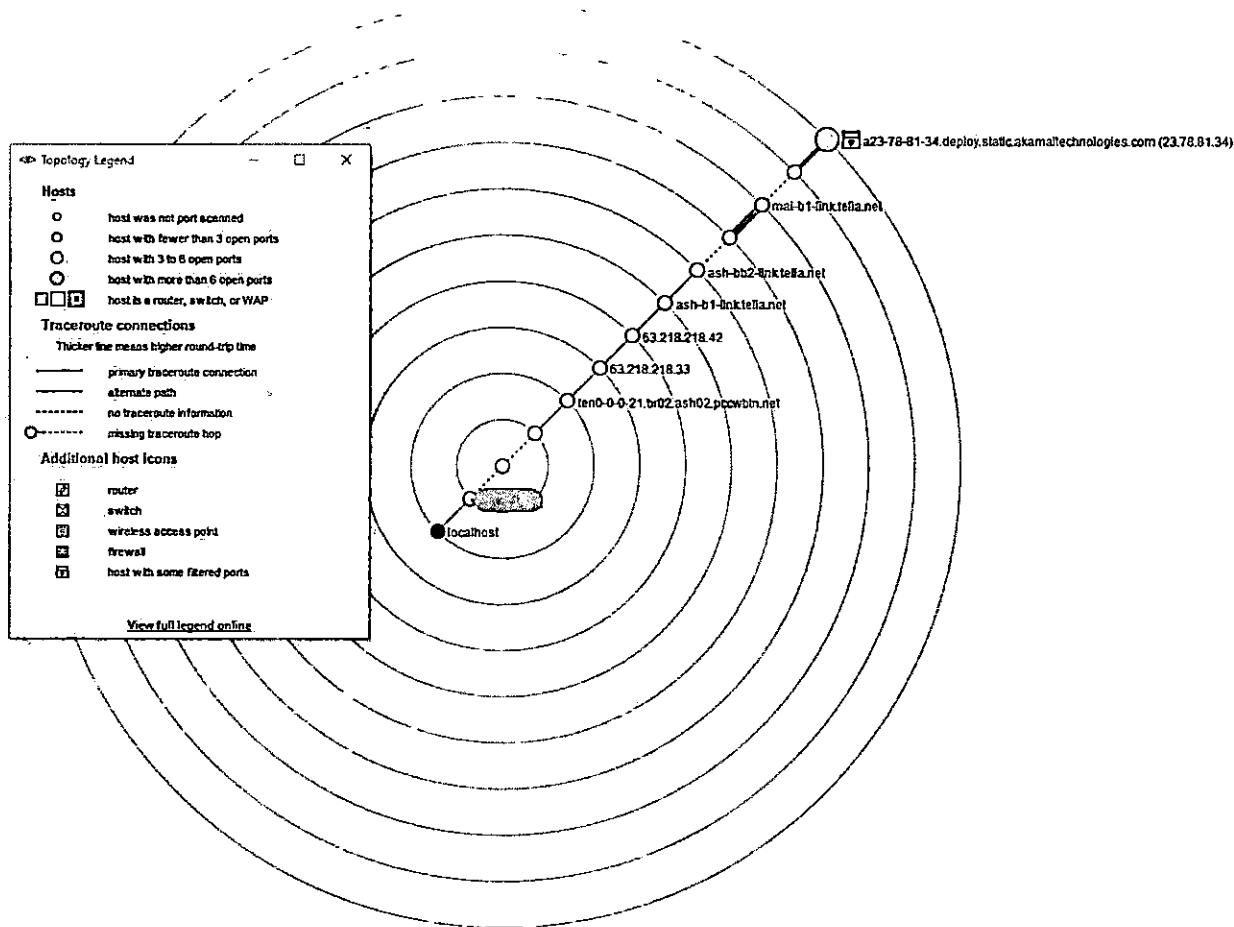


27.

28. L3 Level Communications is federal contractor that is partially owned by foreign lobbyist George Soros. An article that AP ran in 2010 – spoke out about the controversy of this that has been removed. [\(LINK\)](#) “As for the company’s other political connections, it also appears that none other than George Soros, the billionaire funder of the country’s liberal political infrastructure, owns 11,300 shares of OSI Systems Inc., the company that owns Rapiscan. Not surprisingly, OSI’s stock has appreciated considerably over the course of the year. Soros certainly is a savvy investor.” Washington Examiner re-write.



29.



30.

31. **L-3 Communication Systems-East** designs, develops, produces and integrates communication systems and support equipment for space, air, ground, and naval applications, including C4I systems and products; integrated Navy communication systems; integrated space communications and RF payloads; recording systems; secure communications, and information security systems. In addition, their site claims that MARCOM is an integrated communications system and The Marcom® is the foundation of the Navy's newest digital integrated voice / data switching system for affordable command and control equipment supporting communications and radio room automation. The MarCom® uses the latest COTS digital technology and open systems standards to offer the command and control user a low cost, user friendly, solution to the complex voice, video and data communications needs of present and future joint / allied missions. Built in reliability, rugged construction, and fail-safe circuits ensure your call and messages will go through. Evidently a HUGE vulnerability.

32. Michigan's government site is thumped off Akamai Technologies servers which are housed on **TELIA AB** a foreign server located in Germany.
33. Scytl, who is contracted with AP that receives the results tallied BY Scytl on behalf of Dominion – During the elections the AP reporting site had a disclaimer.
AP – powered by SCYTL.

Advertisements		Basic Tracking Info	
Domain:	Michigan.gov	[What's Lookup - Domain Country - Domain To IP]	
IP Address:	23.78.81.34	[IP Blacklist Check]	
Reverse DNS:	34.81.78.23.in-addr.arpa		
Hostname:	a23-78-81-34.deploy.static.akamaitechnologies.com		
	a12-67.akam.net >> 184.26.160.67		
	a11-66.akam.net >> 84.53.139.66		
	a1-35.akam.net >> 193.108.91.35		
Nameservers:	a5-66.akam.net >> 95.100.168.66		
	a18-64.akam.net >> 95.101.36.64		
	a24-65.akam.net >> 2.16.130.65		
Location For an IP: Michigan.gov			
Continent:	North America (NA)		
Country:	United States 🇺🇸 (US)		
Capital:	Washington		
State:	Unknown		
City	Unknown		
Location:	Unknown		
ISP:	Akamai Technologies		
Organization:	Akamai Technologies		
AS Number:	AS1299 Telia Company AB		
something went wrong!	something went wrong!		
Geolocation on IP Map		Time Zone: America/North_Dakota/Center	
		Local Time:	13:48:46
		Timezone	-21600
		GMT offset:	-21600
		Sunrise / Sunset:	07:27 / 17:12
Extra Information for an IP: Michigan.gov			
Continent	Lat/Lon:	46.07305 / -100.546	
Country	Lat/Lon:	38 / -98	
City Lat/Lon:	(37.751) / (-97.822)		
IP Language:	English		

34. “Scytl was selected by the Federal Voting Assistance Program of the U.S. Department of Defense to provide a secure online ballot delivery and onscreen marking systems under a program to support overseas military and civilian voters for the 2010 election cycle and beyond. Scytl was awarded 9 of the 20 States that agreed to participate in the program (New York, Washington, Missouri, Nebraska, Kansas, New Mexico, South Carolina, Mississippi and Indiana), making it the provider with the highest number of participating States.” PDF
35. According to DOMINION : 1.4.1 Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-A consists of 2 types, custom and commercial off the shelf (COTS). COTS applications were verified to be pristine or were subjected to source code review for analysis of any modifications and verification of meeting the pertinent standards.
36. The concern is the HARDWARE and the NON – ACCREDITED VSTLs as by their own admittance use COTS.
37. The purpose of VSTL’s being accredited and their importance in ensuring that there is no foreign interference/ bad actors accessing the tally data via backdoors in equipment software. The core software used by ALL SCYTL related Election Machine/Software manufacturers ensures “anonymity” .
38. Algorithms within the area of this “shuffling” to maintain anonymity allows for setting values to achieve a desired goal under the guise of “encryption” in the trap-door.
39. The actual use of trapdoor commitments in Bayer-Groth proofs demonstrate the implications for the verifiability factor. This means that no one can SEE what is going on during the process of the “shuffling” therefore even if you deploy an algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : “The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system”
40. **Key Terms**
41. **UNIVERSAL VERIFIABILITY:** Votes cast are the votes counted and integrity of the vote is verifiable (the vote was tallied for the candidate selected) . **SCYTL FAILS UNIVERSAL VERIFIABILITY** because no mathematical proofs can determine if any votes have been manipulated.
42. **INDIVIDUAL VERIFIABILITY:** Voter cannot verify if their ballot got correctly counted. Like, if they cast a vote for ABC they want to verify it was ABC. That notion clearly discounts the need for anonymity in the first place.

43. To understand what I observed during the 2020 I will walk you through the process of one ballot cast by a voter.
44. STEP 1 |Config Data | All non e-voting data is sent to ScytI (offshore) for configuration of data. All e-voting is sent to CONFIGURATION OF DATA then back to the e-voting machine and then to the next phase called CLEANSING. CONCERNS: Here we see an “OR PROOF” as coined by mathematicians – an “or proof” is that votes that have been pre-tallied parked in the system and the algorithm then goes back to set the outcome it is set for and seeks to make adjustments if there is a partial pivot present causing it to fail demanding manual changes such as block allocation and narrowing of parameters or self-adjusts to ensure the predetermined outcome is achieved.
45. STEP 2|CLEANSING | The Process is when all the votes come in from the software run by Dominion and get “cleansed” and put into 2 categories: invalid votes and valid votes.
46. STEP 3|Shuffling /Mixing | This step is the most nefarious and exactly where the issues arise and carry over into the decryption phase. Simply put, the software takes all the votes, literally mixes them a and then re-encrypts them. This is where if ONE had the commitment key- TRAPDOOR KEY – one would be able to see the parameters of the algorithm deployed as the votes go into this mixing phase, and how algorithm redistributes the votes.
47. This published PAPER FROM University College London depicts how this shuffle works. In essence, when this mixing/shuffling occurs, then one doesn’t have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes when mixed.

48.

Background - ElGamal encryption

- Setup: Group \mathcal{G} of prime order q with generator g
- Public key: $pk = y = g^x$
- Encryption: $\mathcal{E}_{pk}(m; r) = (g^r, y^r m)$
- Decryption: $\mathcal{D}_x(u, v) = vu^{-x}$
- Homomorphic:

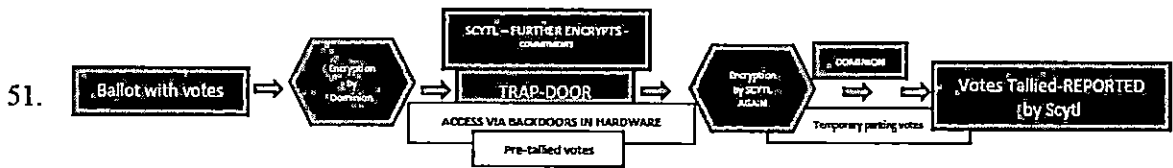
$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(M; R) = \mathcal{E}_{pk}(mM; r + R)$$

- Re-encryption:

$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(1; R) = \mathcal{E}_{pk}(m; r + R)$$



49. When this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes.
50. When the votes are sent to ScytI via Dominion Software EMS (Election Management System) the Trap Door is accessed by ScytI or TRAP DOOR keys (Commitment Parameters).



52. The encrypted data is shifted into ScytI's platform in the form of ciphertexts – this means it is encrypted and a key based on commitments is needed to read the data. The ballot data can only be read if the person has a key that is set on commitments.
53. A false sense of security is provided to both parties that votes are not being “REPLACED” during the mixing phase. Basically, ScytI re-encrypts the ballot data that comes in from Dominion (or any other voting software company) as ciphertexts. ScytI is supposed to prove that votes A, B, C are indeed X, Y, Z under their new re-encryption when sending back the votes that are tallied coding them respectively. This is done by ScytI and the Election Software company that agrees to certain

“Generators” and therefore together build “commitments.”

```
public CommitmentParams(final ZpSubgroup group, final int n) {
    group = group;
    h = GroupTools.getRandomElement(group);
    commitmentlength = n;
    g = GroupTools.getVectorRandomElement(group,
    this.commitmentlength);
}

// from getRandomElement(group)
Exponent randomExponent = ExponentTools.getRandomExponent(group.getQ());
return group.getGenerator().exponentiate(randomExponent);
```

54. ScytI and Dominion have an agreement – only the two would know the parameters. This means that access is able to occur through backdoors in hardware if the parameters of the commitments are known in order to alter the range of the algorithm deployed to satisfy the outcome sought in the case of algorithm failure.
55. Trapdoor is a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able change the value of the commitments however it likes. In other words, ScytI or anyone that knows the commitment parameters can take all the votes and give them to any one they want. If they have a total of 1000 votes an algorithm can distribute them among all races as it deems necessary to achieve the goals it wants. (Case Study: Estonia)

Commitment_{CRYPT} = CM_c

Scyll sets commitment - simple math ↓

$$CM_c(\vec{a}; r) = H \left[\prod_{i=1}^n G_i^{a_i} \right]$$

$$CM_c(\vec{a}; r) = H \left[r + \sum_{i=1}^n (a_i - z_i) e_i \right] \prod_{i=1}^n H_i^{z_i e_i}$$

$$CM_c(\vec{a}; r) = CM_c(\vec{z}; r')$$

$$r' = r + \sum_{i=1}^n e_i (a_i - z_i)$$

56.

57. Within the trapdoor this is how the algorithm behaves to move the goal posts in elections without being detected by this proof . During the mixing phase this is the algorithm you would use to

“reallocate” votes via an algorithm to achieve the goal set.

??

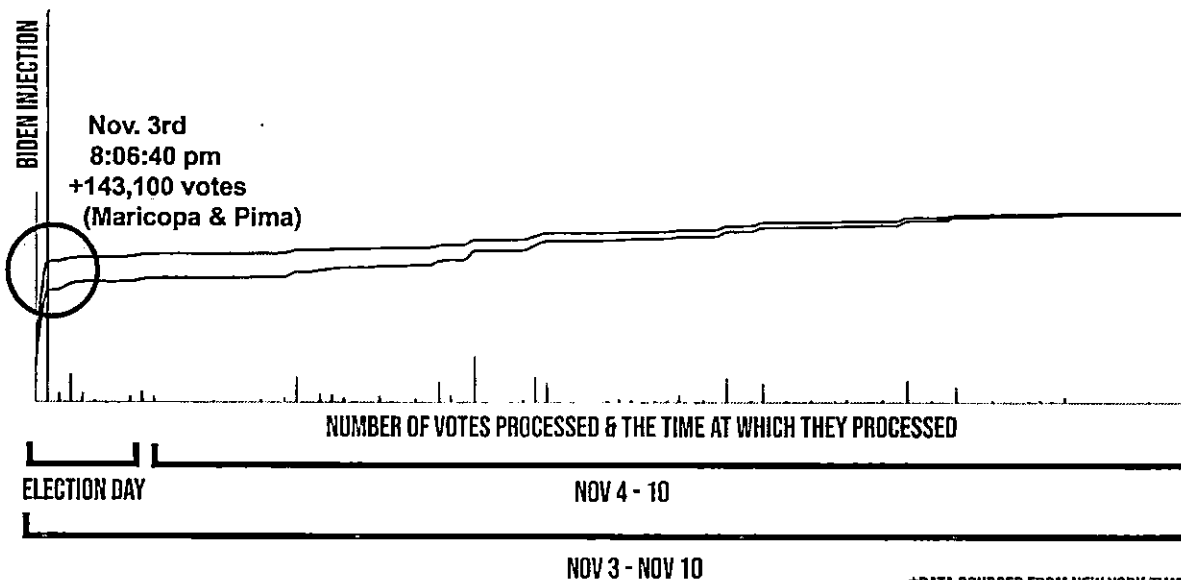
$C_1 = E_{pk}(1; \rho_1) \quad C_1 = E_{pk}(M_1; \rho_1 + \rho'_1)$
 $C_2 = E_{pk}(1; \rho_2) \quad C_3 = E_{pk}(M_3; \rho_2 + \rho'_3) \leftarrow \text{changing vote}$
 $C_3 = E_{pk}(1; \rho_3) \quad C_3 = E_{pk}(M_3; \rho_3 + \rho'_3)$

giving vote to C_3 rather than C_2 .

58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that the randomness is applied and used to generate the tally vote ciphertext. Thus in this case, Scytl who is the mixer can collude with their vote company clients or an agency (-----) to change votes and get away with it. This is because the receiver doesn't have the decryption key so they rely solely on Scytl to be *honest* or free from any foreign actors within their backdoor or the Election Company (like Dominion) that can have access to the key.
59. In fact, a study from the University of Bristol made claim that interference can be seen when there is a GREAT DELAY in reporting and finalizing numbers University of Bristol : How not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios
60. “Zero-knowledge proofs of knowledge allow a prover to convince a verifier that she holds information satisfying some desirable properties without revealing anything else.” David Bernhard, Olivier Pereira, and Bogdan Warinschi.

61. Hence, you can't prove anyone manipulated anything. The TRAP DOOR KEY HOLDERS can offer you enough to verify to you what you need to see without revealing anything and once again indicating the inability to detect manipulation. **ZERO PROOF of INTEGRITY OF THE VOTE.**
62. Therefore, if decryption is challenged, the administrator or software company that knows the trap door key can provide you proof that would be able to pass verification (blind). This was proven to be factually true in the case study by The University of Melbourne in March. White Hat Hackers purposely altered votes by knowing the parameters set in the commitments and there was no way to prove they did it – or any way to prove they didn't.
63. IT'S THE PERFECT THREE CARD MONTY. That's just how perfect it is. They fake a proof of ciphertexts with KNOWN "RANDOMNESS". This rolls back to the integrity of the VOTE. The vote is not safe using these machines not only because of the method used for ballot "cleansing" to maintain anonymity but the EXPOSURE to foreign interference and possible domestic bad actors.
64. In many circumstances, manipulation of the algorithm is NOT possible in an undetectable fashion. This is because it is one point heavy. Observing the elections in 2020 confirm the deployment of an algorithm due to the BEHAVIOR which is indicative of an algorithm in play that had no pivoting parameters applied.
65. The behavior of the algorithm is that one point (B) is the greatest point within the allocated set. It is the greatest number within the A B points given. Point A would be the smallest. Any points outside the A B points are not necessarily factored in yet can still be applied.
66. The points outside the parameters can be utilized to a certain degree such as in block allocation.
67. The algorithm geographically changed the parameters of the algorithm to force blue votes and ostracize red.
68. Post block allocation of votes the two points of the algorithm were narrowed ensuring a BIDEN win hence the observation of NO Trump Votes and some BIDEN votes for a period of time.

ARIZONA "FIXING" THE VOTE



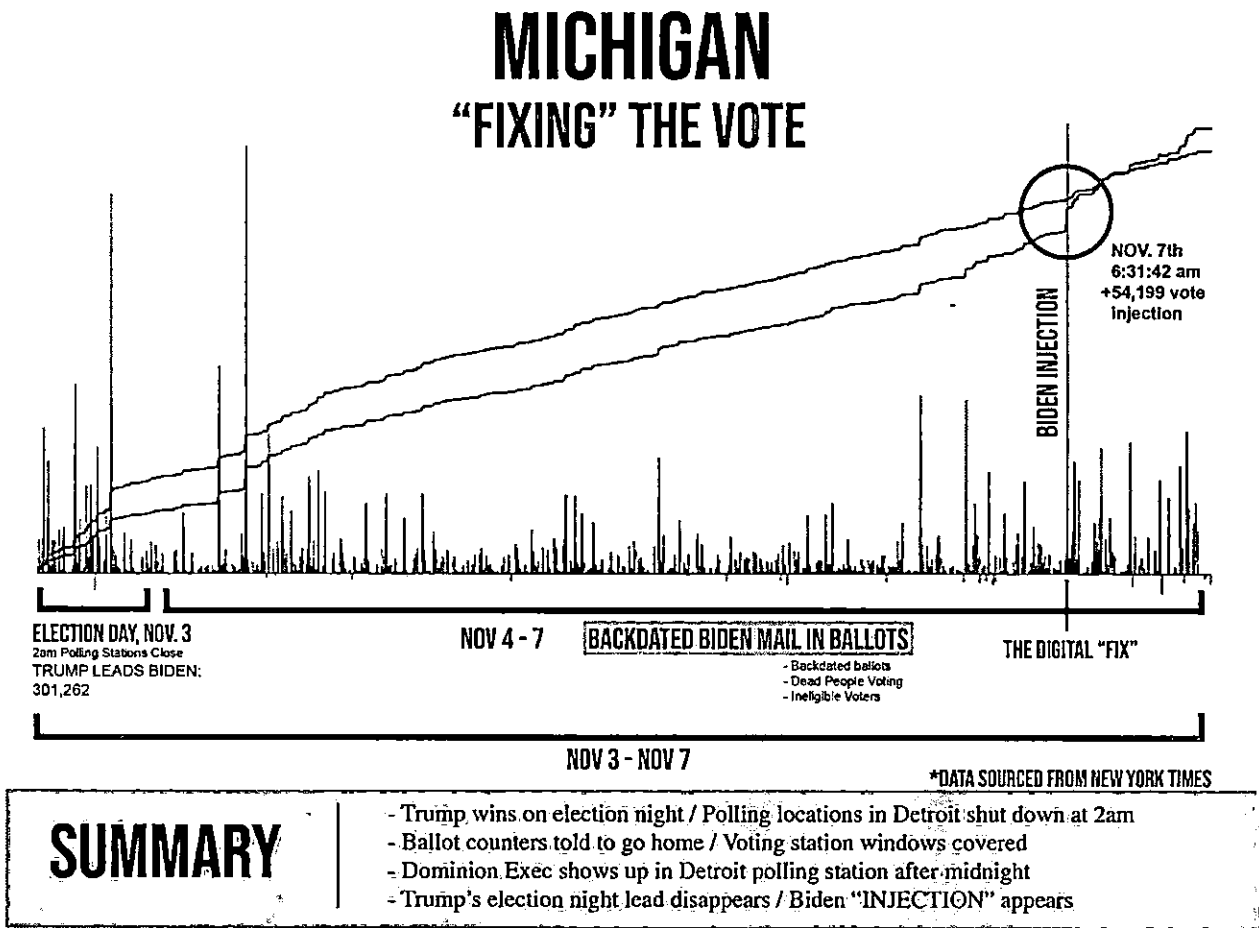
*DATA SOURCED FROM NEW YORK TIMES

SUMMARY

- Mathematical evidence of the seeding "injection" of votes at the beginning
- A spike means that a large number of votes were injected into the totals.
- A normal vote pattern would look like a natural progression – smooth without extreme jumps

69.

70. Gaussian Elimination without pivoting explains how the algorithm would behave and the election results and data from Michigan confirm FAILURE of algorithm.



71. The "Digital Fix" observed with an increased spike in VOTES for Joe Biden can be determined as evidence of a pivot. Normally it would be assumed that the algorithm had a Complete Pivot. Wilkinson's demonstrated the guarantee as :

$$\frac{\|U\|_{\infty}}{\|A\|_{\infty}} \leq n^{\frac{1}{2} \log(n)}$$

72.

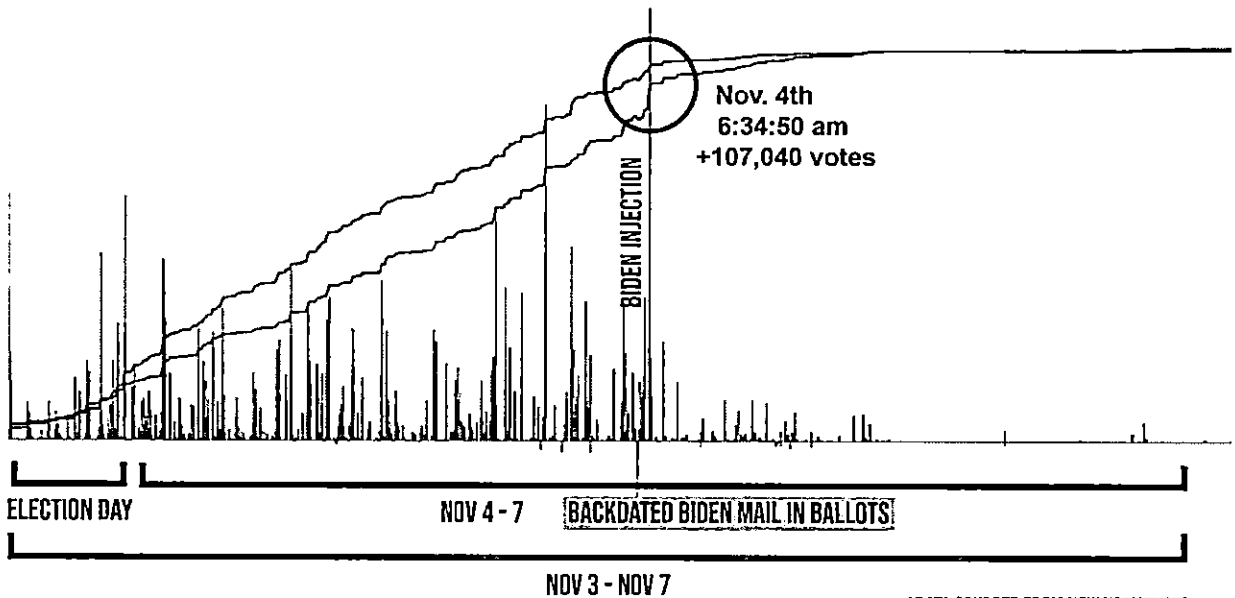
73. Such a conjecture allows the growth factor the ability to be upper bound by values closer to n. Therefore, complete pivoting can't be observed because there would be too many floating points. Nor can partial as the partial pivoting would overwhelm after the "injection" of votes. Therefore, external factors were used which is evident from the "DIGITAL FIX"

74. Observing the elections, after a review of Michigan's data a spike of 54,199 votes to Biden. Because it is pushing and pulling and keeping a short distance between the 2 candidates; but then a spike, which is how an algorithm presents; - and this spike means there was a pause and an insert was made, where they insert an algorithm. Block spikes in votes for JOE BIDEN were NOT paper

ballots being fed or THUMB DRIVES. The algorithm block adjusted itself and the PEOPLE were creating the evidence to BACK UP the block allocation.

- 75. I have witnessed the same behavior of the election software in countries outside of the United States and within the United States. In -----, the elections conducted behaved in the same manner by allocating BLOCK votes to the candidate “chosen” to win.
- 76. Observing the data of the contested states (and others) the algorithm deployed is identical to that which was deployed in 2012 providing Barack Hussein Obama a block allocation to win the 2012 Presidential Elections.
- 77. The algorithm looks to have been set to give Joe Biden a 52% win even with an initial 50K+ vote block allocation was provided initially as tallying began (as in case of Arizona too). In the am of November 4, 2020 the algorithm stopped working, therefore another “block allocation” to remedy the failure of the algorithm. This was done manually as ALL the SYSTEMS shut down NATIONWIDE to avoid detection.

GEORGIA “FIXING” THE VOTE



*DATA SOURCED FROM NEW YORK TIMES

SUMMARY

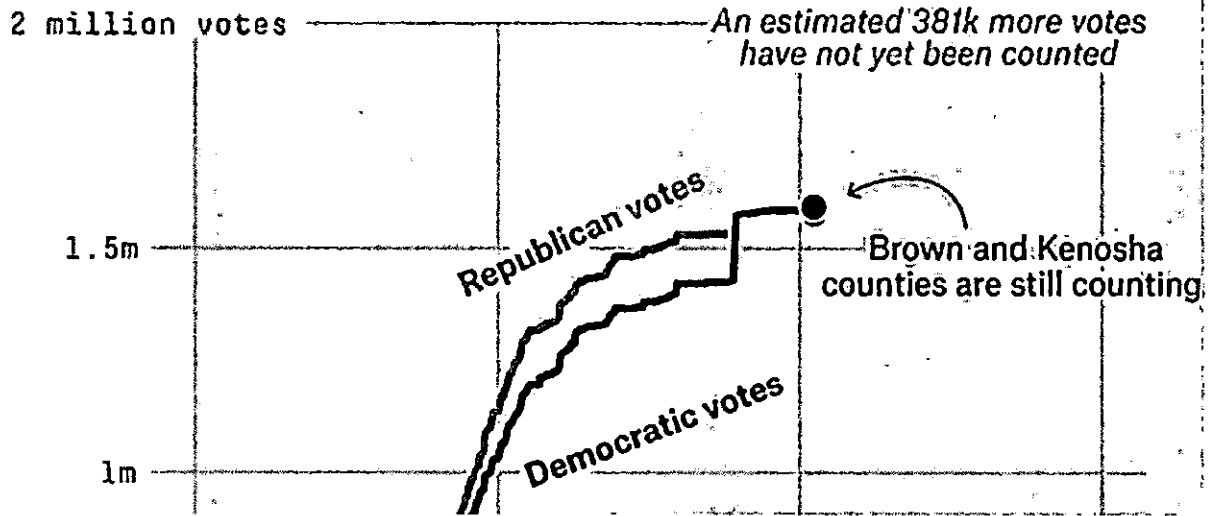
- The spike on the morning of Nov. 4 resulted in a net increase of 107,040 to Biden's total.
- A spike means that a large number of votes were injected into the totals
- A normal vote pattern would look like a natural progression – smooth without

- 78.
- 79. In Georgia during the 2016 Presidential Elections a failed attempt to deploy the scripts to block allocate votes from a centralized location where the “trap-door” key lay an attempt by someone using

the DHS servers was detected by the state of GA. The GA leadership assumed that it was "Russians" but later they found out that the IP address was that of DHS.

80. In the state of Wisconsin, we observed a considerable BLOCK vote allocation by the algorithm at the SAME TIME it happened across the nation. All systems shut down at around the same time.

Total presidential votes for each party so far, with 89 percent of Wisconsin's expected vote counted as of 6:23 a.m on Nov. 4



81.

82. In Wisconsin there are also irregularities in respect to BALLOT requests. (names AND address Hidden for privacy)

F	G	H	V	W	X	Y	AB	AC	AD	AE	AG	AH	AI	AJ	AK	AL	AM
Active	Registered	Military	Brown County	11/01/2020	Online	Military	Official	Active	Not Returned	Online			11/01/2020				
Active	Registered	Regular	Brown County	10/23/2020	Voted in Person	Regular	Official	Active	Returned	Voted in Person			10/23/2020	10/23/2020			
Active	Registered	Military	Brown County	11/01/2020	Online	Military	Official	Active	Not Returned	Online			11/01/2020				
Active	Registered	Regular	Brown County	11/01/2020	Online	Regular	Official	Active	Returned	Mail			11/01/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/01/2020	Email	Regular	Official	Active	Returned	Mail			11/01/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/01/2020	Email	Regular	Official	Active	Returned	Mail			11/01/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular	Official	Active	Returned	Voted in Person			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular	Official	Active	Returned	Voted in Person			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular	Official	Active	Returned	Voted in Person			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular	Official	Active	Returned	Voted in Person			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular	Official	Active	Returned	Voted in Person			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Received in Person	Hospitaliz	Official	Active	Returned	Appointed Agent			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Email	Hospitaliz	Official	Active	Returned	Appointed Agent			11/02/2020	11/02/2020			
Active	Registered	Military	Brown County	11/02/2020	Mail		Official	Active	Returned	Appointed Agent			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Mail	Regular	Official	Active	Returned	Appointed Agent			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Mail	Regular	Official	Active	Returned	Appointed Agent			11/02/2020	11/02/2020			
Active	Registered	Military	Brown County	11/02/2020	Online	Military	Official	Active	Not Returned	Online			11/02/2020				
Active	Registered	Military	Brown County	11/02/2020	Online	Military	Official	Active	Not Returned	Online			11/02/2020				
Active	Registered	Regular	Brown County	11/02/2020	Online	Regular	Official	Active	Not Returned	Online			11/02/2020				
Active	Registered	Military	Brown County	11/02/2020	FPCA	Military	Official	Active	Returned	Mail			11/02/2020	11/02/2020			
Active	Registered	Military	Brown County	11/02/2020	FPCA	Military	Official	Active	Returned	Mail			11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/01/2020	Voted in Person	Regular	Official	Inactive	Returned	Voted in Person			11/01/2020	11/01/2020			
Active	Registered	Military	Brown County	11/01/2020	Mail	Military	Certification Insufficient	Federal Absent	Active	Returned, to be Rejected	Mail		11/01/2020	11/01/2020			
Active	Registered	Military	Brown County	11/01/2020	Mail	Military	Certification Insufficient	Federal Absent	Active	Returned, to be Rejected	Mail		11/01/2020	11/01/2020			
Active	Registered	Military	Brown County	11/01/2020	Online	Military	Official	Active	Not Returned	Mail			11/01/2020				
Active	Registered	Regular	Brown County	11/03/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											
Active	Registered	Regular	Brown County	11/04/2020	Online	Regular											

83.

91. Right before the ----- elections it was alleged that CyberBerkut a pro-Russia group infiltrated --- central election computers and deleted key files. These actions supposedly rendered the vote-tallying system inoperable.
92. In fact, the KEY FILES were the Commitment keys to allow Scytl to tally the votes rather than the election machines. The group had disclosed emails and other documents proving that their election was rigged and that they tried to avoid a fixed election.
93. The elections were held on May 25, 2014 but in the early AM hours the election results were BLOCKED and the final tally was DELAYED flipping the election in favor of -----.
94. The claim was that there was a DDoS attack by Russians when in actual fact it was a mitigation of the algorithm to inject block votes as we observed was done for Joe Biden because the KEYS were unable to be deployed. In the case of -----, the trap-door key was “altered”/deleted/ rendered ineffective. In the case of the US elections, representatives of Dominion/ ES&S/ Smartmatic/ Hart Intercivic would have to manually deploy them since if the entry points into the systems seemed to have failed.
95. The vote tallying of all states NATIONWIDE stalled and hung for days – as in the case of Alaska that has about 300K registered voters but was stuck at 56% reporting for almost a week.
96. This “hanging” indicates a failed deployment of the scripts to block allocate remotely from one location as observed in ----- on May 26, 2014.
97. This would justify the presence of the election machine software representatives making physical appearances in the states where the election results are currently being contested.
98. A Dominion Executive appeared at the polling center in Detroit after midnight.
99. Considering that the hardware of the machines has NOT been examined in Michigan since 2017 by Pro V& V according to Michigan’s own reporting. COTS are an avenue that hackers and bad actors seek to penetrate in order to control operations. Their software updates are the reason vulnerabilities to foreign interference in all operations exist.
100. The importance of VSTLs in underrated to protect up from foreign interference by way of open access via COTS software. Pro V& V who’s EAC certification EXPIRED on 24 FEB 2017 was contracted with the state of WISCONSIN.
101. In the United States each state is tasked to conduct and IV& V (Independent Verification and Validation) to provide assurance of the integrity of the votes.
102. If the “accredited” non-federal entities have NOT received EAC accreditation this is a failure of the states to uphold their own states standards that are federally regulated.
103. In addition, if the entities had NIST certificates they are NOT sufficing according the HAVA ACT 2002 as the role of NIST is clear.
104. Curiously, both companies PRO V&V and SLI GAMING received NIST certifications OUTSIDE the 24 month scope.

105. PRO V& V received a NIST certification on 26MAR2020 for ONE YEAR. Normally the NIST certification is good for two years to align with that of EAC certification that is good for two years.



106.

107. The last PRO V& V EAC accreditation certificate (Item 8) of this declaration expired in February 2017 which means that the IV & V conducted by Michigan claiming that they were accredited is false.

108. The significance of VSTLs being accredited and examining the HARDWARE is key. COTS software updates are the avenues of entry.

109. As per DOMINION'S own petition, the modems they use are COTS therefore failure to have an accredited VSTL examine the hardware for points of entry by their software is key.

*Compact Flash Cards	<u>***SanDisk Ultra:</u> SDCFHS-004G SDCFHS-008G <u>RiData:</u> CFC-14A RDF8G-233XMCB2-1 RDF16G-233XMCB2-1 RDF32G-233XMCB2-1 <u>SanDisk Extreme:</u> SDCFX-016G SDCFX-032G <u>SanDisk:</u> SDFAA-008G	Memory device for ICP and ICE tabulators.
*Modems	Verizon USB Modem Pantech UMW190NCD USB Modem MultiTech MT9234MU CellGo Cellular Modem E-Device 3GPUSUS AT&T USB Modem MultiTech GSM MTD-H5 Fax Modem US Robotics 56K V.92.	Analog and wireless modems for transmitting unofficial election night results.

110.

111. For example and update of Verizon USB Modem Pantech undergoes multiple software updates a year for it's hardware. That is most likely the point of entry into the systems.

112. During the 2014 elections in ---- it was the modems that gave access to the systems where the commitment keys were deleted.

113. SLI Gaming is the other VSTL "accredited" by the EAC BUT there is no record of their accreditation. In fact, SLI was NIST ISO Certified 27 days before the election which means that PA IV&V was conducted without NIST cert for SLI being valid.

United States Department of Commerce
National Institute of Standards and Technology



Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200733-0

SLI Compliance
Wheat Ridge, CO

*is accredited by the National Voluntary Laboratory Accreditation Program for specific services,
listed on the Scope of Accreditation, for:*

Voting System Testing

*This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017.
This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality
management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).*

2020-10-07 through 2020-12-31
Effective Dates



[Signature]
For the National Voluntary Laboratory Accreditation Program

- 114.
115. In fact SLI was NIST ISO Certified for less than 90 days.
116. I can personally attest that high-level officials of the Obama/Biden administration and large private contracting firms met with a software company called GEMS which is ultimately the software ALL election machines run now running under the flag of DOMINION.
117. GEMS was manifested from SOE software purchased by SCYTL developers and US Federally Funded persons to develop it.
118. The only way GEMS can be deployed across ALL machines is IF all counties across the nation are housed under the same server networks.
119. GEMS was tasked in 2009 to a contractor in Tampa, Fl.
120. GEMS was also fine-tuned in Latvia, Belarus, Serbia and Spain to be localized for EU deployment as observed during the Swissport election debacle.
121. John McCain's campaign assisted in FUNDING the development of GEMS web monitoring via WEB Services with 3EDC and Dynology.

**SCHEDULE B-P
ITEMIZED DISBURSEMENTS**

Use separate schedule(s) for each category of the Detailed Summary Page

FOR LINE NUMBER: (check only one) PAGE 7358 / 8595

<input checked="" type="checkbox"/> 23	<input type="checkbox"/> 24	<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27a
<input type="checkbox"/> 27b	<input type="checkbox"/> 28a	<input type="checkbox"/> 28b	<input type="checkbox"/> 28c	<input type="checkbox"/> 29

Any information copied from such Reports and Statements may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes, other than using the name and address of any political committee to solicit contributions from such committee.

NAME OF COMMITTEE (in Full)
JOHN MCCAIN 2008, INC.

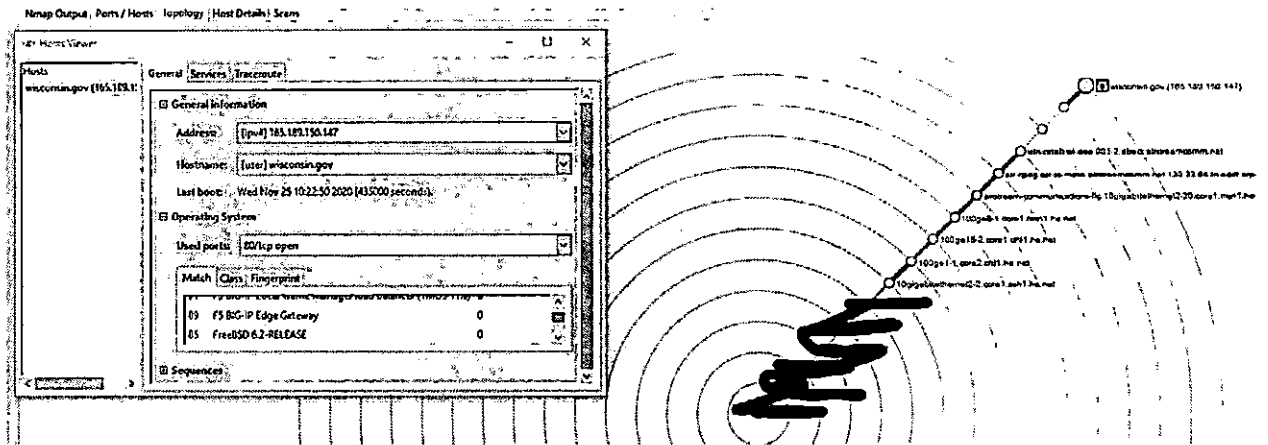
Full Name (Last, First, Middle Initial) A. 3EDC LLC		Date of Disbursement MM / DD / YYYY 03 / 17 / 2008
Mailing Address 211 NORTH UNION ST STE 200		Transaction ID: SB23.10515
City ALEXANDRIA	State VA	Zip Code 22314
Purpose of Disbursement WEB SERVICE	Candidate Name	Amount of Each Disbursement this Period 399916.09
Office Sought: <input type="checkbox"/> House <input type="checkbox"/> Senate <input type="checkbox"/> President	Disbursement For: 2008 <input checked="" type="checkbox"/> Primary <input type="checkbox"/> General <input type="checkbox"/> Other (specify) ▼	Category/Type
State: District:		
Full Name (Last, First, Middle Initial) B. A FARE EXTRAORDINAIRE		Date of Disbursement MM / DD / YYYY 03 / 17 / 2008
Mailing Address 2035 MARSHALL		Transaction ID: SB23.10049
City HOUSTON	State TX	Zip Code 77098
Purpose of Disbursement FACILITY RENTAL/CATERING	Candidate Name	Amount of Each Disbursement this Period 23697.69
Office Sought: <input type="checkbox"/> House <input type="checkbox"/> Senate <input type="checkbox"/> President	Disbursement For: 2008 <input checked="" type="checkbox"/> Primary <input type="checkbox"/> General <input type="checkbox"/> Other (specify) ▼	Category/Type
State: District:		
Full Name (Last, First, Middle Initial) C. ADMINISTAFF		Date of Disbursement MM / DD / YYYY 03 / 05 / 2008
Mailing Address PO BOX 203332		Transaction ID: SB23.10117
City HOUSTON	State TX	Zip Code 77216
Purpose of Disbursement INSURANCE	Candidate Name	Amount of Each Disbursement this Period 483.68
Office Sought: <input type="checkbox"/> House <input type="checkbox"/> Senate <input type="checkbox"/> President	Disbursement For: 2008 <input checked="" type="checkbox"/> Primary <input type="checkbox"/> General <input type="checkbox"/> Other (specify) ▼	Category/Type
State: District:		
Subtotal Of Receipts This Page (optional).....		424097.46
Total This Period (last page this line number only).....		

122.

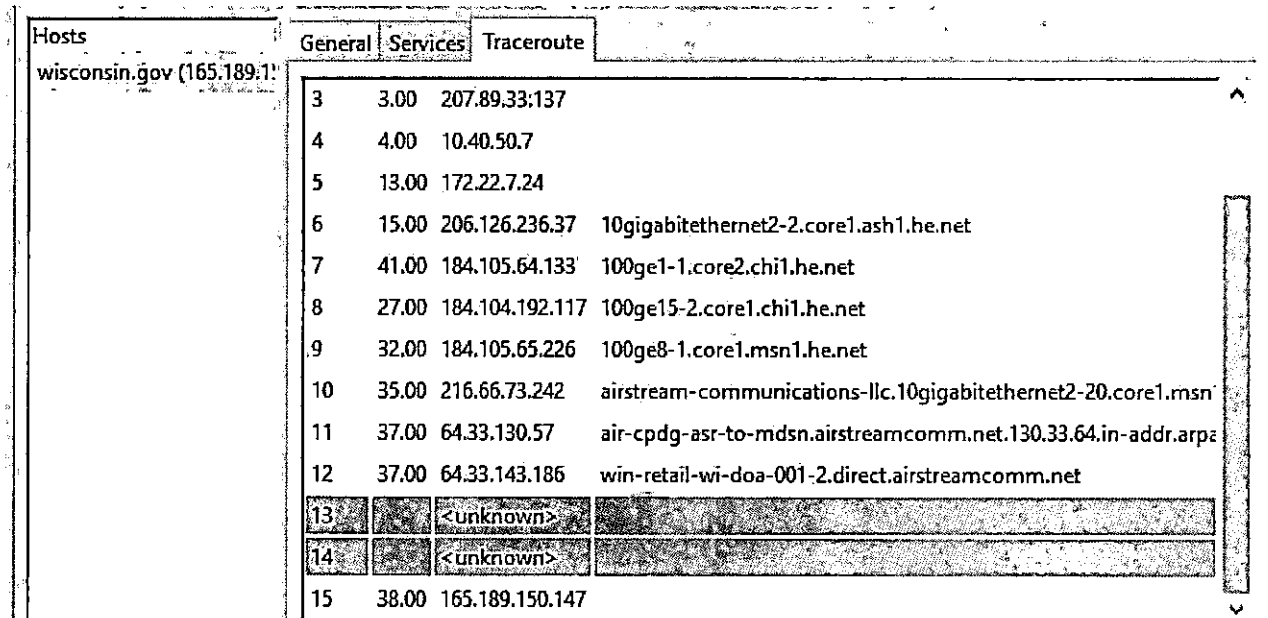
123.

124. AKAMAI Technologies services SCYTL.

- 125. AKAMAI Technologies Houses ALL foreign government sites. (Please see White Paper by Akamai.)
- 126. AKAMAI Technologies houses ALL .gov state sites. (ref Item 123 Wisconsin.gov Example)



- 127.
- 128. Wisconsin has EDGE GATEWAY port which is AKAMAI TECHNOLOGIES based out of GERMANY.
- 129. Using AKAMAI Technologies is allowing .gov sites to obfuscate and mask their systems by way of HURRICANE ELECTRIC (he.net) Kicking it to anonymous (AKAMAI Technologies) offshore servers.



- 130.
- 131. AKAMAI Technologies has locations around the world.
- 132. AKAMAI Technologies has locations in China (ref item 22)
- 133. AKAMAI Technologies has locations in Iran as of 2019.
- 134. AKAMAI Technologies merged with UNICOM (CHINESE TELECOMM) in 2018.
- 135. AKAMAI Technologies house all state .gov information in GERMANY via TELIA AB.

136. In my professional opinion, this affidavit presents unambiguous evidence:
137. That there was Foreign interference, complicit behavior by the previous administrations from 1999 up until today to hinder the voice of the people and US persons knowingly and willingly colluding with foreign powers to steer our 2020 elections that can be named in a classified setting.
138. Foreign interference is present in the 2020 election in various means namely,
139. Foreign nationals assisted in the creation of GEMS (Dominion Software Foundation)
140. Akamai Technologies merged with a Chinese company that makes the COTS components of the election machines providing access to our electronic voting machines.
141. Foreign investments and interests in the creation of the GEMS software.
142. US persons holding an office and private individuals knowingly and willingly oversaw fail safes to secure our elections.
143. The EAC failed to abide by standards set in HAVA ACT 2002.
144. The IG of the EAC failed to address complaints since their appointment regarding vote integrity
145. Christy McCormick of the EAC failed to ensure that EAC conducted their duties as set forth by HAVA ACT 2002
146. Both Patricia Layfield (IG of EAC) and Christy McCormick (Chairwoman of EAC) were appointed by Barack Hussein Obama and have maintained their positions since then.
147. The EAC failed to have a quorum for over a calendar year leading to the inability to meet the standards of the EAC.
148. AKAMAI Technologies and Hurricane Electric raise serious concerns for NATSEC due to their ties with foreign hostile nations.
149. For all the reasons above a complete failure of duty to provide safe and just elections are observed.
150. For the people of the United States to have confidence in their elections our cybersecurity standards should not be in the hands of foreign nations.
151. Those responsible within the Intelligence Community directly and indirectly by way of procurement of services should be held accountable for assisting in the development, implementation and promotion of GEMS.
152. GEMS ----- General Hayden.
153. In my opinion and from the data and events I have observed ----- with the assistance of SHADOWNET under the guise of L3-Communications which is MPRI. This is also confirmed by us.army.mil making the statement that shadownet has been deployed to 30 states which all

happen to be using Dominion Machines.

FAIRFAX, Va. -The Virginia National Guard's Bowling Green-based 91st Cyber Brigade completed the nationwide rollout of its ShadowNet enterprise solution July 19, 2019, with the integration of the 125th Cyber Protection Battalion into the solution's virtual private network. ShadowNet is a custom-built private cloud-based out of the brigade's data center in Fairfax, Virginia, that uses VPN connectivity to provide its aligned units with 24-hour, seven-days-a-week remote access to critical cyber training at both the collective and individual levels. The brigade successfully integrated its three other cyber protection battalions - the 123rd, 124th, and 126th Cyber Protection Battalions - into the ShadowNet platform last January.

"I'm extremely proud to announce that the Soldiers of the 91st Cyber Brigade have completed the construction and rollout of ShadowNet, a world-class enterprise solution designed to propel operational innovation in the field of cyber training," said Col. Adam C. Volant, commander of the 91st Cyber Brigade. "ShadowNet will allow us to leverage the expertise of cyber professionals across our four cyber protection battalions to build Soldier-centric programs and collective training environments that deliver breakthroughs in exercise complexity and cost efficiency. Its robust

OCTOBER 26, 2020
U.S. Army STAND-TO! | Army Readiness Training

SEPTEMBER 12, 2019
September 2017 Nominative Sergeant's Major Assignments

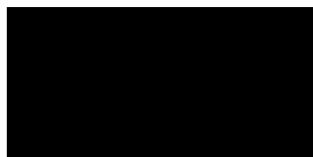
SEPTEMBER 12, 2019
DA ANNOUNCES ROTATIONAL DEPLOYMENTS

154. Based on my research of voter data – it appears that there are approximately 23,000 residents of a Department of Corrections Prison with requests for absentee ballot in Wisconsin. We are currently reviewing and verifying the data and will supplement.

23231	23231	Hansen	Luann	M		(262)994-9050
23232	23232	Neberman	John	C		(262)994-9050
23233	23233	Reynolds	Devi	J		(262)994-9050
23234	23234	Rieckhoff	Kathryn	Susan		(262)994-9050
23235	23235	Edwards	Mark	Landon		(262)994-9050
23236	23236	Pfeiffer	Joseph	Patrick		(262)994-9050
23237	23237	Hines	Dianna	K		(262)994-9050
23238	23238	Beachem	Janice	F		(262)994-9050
23239	23239	Blackstone	Thomas	Wayne		(262)994-9050
23240	23240	Braun	Patricia	Ann		(262)994-9050
23241	23241	Smith	Raymond	L		(262)994-9050
23242	23242	Meyer	Steven	R		(262)994-9050
23243	23243	Vincent	Herbert			(262)994-9050
23244	23244	Guajardo	Juan	P		(262)994-9050
23245	23245	Wallace	Kirk	R		(262)994-9050
23246	23246	Kaplan	Bernard	L		(262)994-9050
23247	23247	Bahrs	Michelle	M		(262)994-9050
23248	23248	Shattuck	Elizabeth	L		(262)994-9050
23249	23249	Munoz	Rosalio	S	JR	(262)994-9050
23250	23250	Strunk	Amy	C		(262)994-9050
23251	23251	Schendel	Michael	P	JR	(262)994-9050
23252	23252	Mack	Kimberly	N		(262)994-9050
23253	23253	Spikes	Debra	A		(262)994-9050
23254	23254	Busarow	Suzanne	M		(262)994-9050
23255	23255	Oliver	Timmy			(262)994-9050
23256	23256	Wember	Jimmy	Dean		(262)994-9050
23257	23257	Kosterman	Michael	Richard		(262)994-9050
23258	23258	Szaradowski	Paul	M		(262)994-9050
23259	23259	Oliver	Dale			(262)994-9050
23260	23260	Derango	Nancy			(262)994-9050
23261	23261	Smith	Arthur	J		(262)994-9050 SMITH24.3059@YAHOO
23262	23262	Brown	Michael	Edward		(262)994-9050

155.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge.
Executed this November 29th, 2020.

A large black rectangular redaction box covering the signature area.A small black rectangular redaction box covering the name of the declarant.

List of abbreviations/explanations for reference in Ms. Maras' affidavit*

OCONUS (chiefly military) Acronym of outside [the] contiguous United States; i.e. Alaska, Hawaii, the US territories, and all other countries.

CONUS (chiefly military) Continental United States

9 EYES A surveillance alliance of the 5 Eyes countries of Australia, Canada, New Zealand, United Kingdom, & United States, plus Denmark, France, Netherlands, and Norway.

HAVA The Help America Vote Act (HAVA) of 2002 was passed by the United States Congress to make sweeping reforms to the nation's voting process. HAVA addresses improvements to voting systems and voter access that were identified following the 2000 election. HAVA requires that the EAC (see below) provide for the accreditation and revocation of accreditation of independent, non-federal laboratories qualified to test voting systems to Federal standards. Generally, the EAC considers for accreditation those laboratories evaluated and recommended by the National Institute of Standards and Technology (NIST) pursuant to HAVA Section 231(b)(1). However, consistent with HAVA Section 231(b)(2)(B), the Commission may also vote to accredit laboratories outside of those recommended by NIST upon publication of an explanation of the reason for any such accreditation. Per HAVA, a state's voting machines must be certified EAC for a state to receive funding.

NIST National Institute of Standards and Technology, US Department of Commerce. NIST's portfolio of services for measurements, standards, and legal metrology provide solutions that ensure measurement traceability, enable quality assurance, and harmonize documentary standards and regulatory practices.

EAC The U.S. Election Assistance Commission (EAC) was established by the Help America Vote Act of 2002 (HAVA). The EAC is an independent, bipartisan commission charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration. The EAC also accredits testing laboratories and certifies voting systems, as well as audits the use of HAVA funds.

VSTL Voting System Test Laboratory-- developed by the EAC to assure voting systems meet statutory requirements under HAVA. Participation is voluntary, but states receiving HAVA funds are required to have their voting systems certified according to HAVA statutory requirements.

ISO CERT is the International Organization for Standardization – It's an independent, international organization that produces various standards spanning throughout the business sector that help improve and ensure quality, efficiency, consistency, and safety of operations and their consequent products and services. It is important to note, **ISO cannot certify you themselves**. ISO develops the standards, but the certification process is performed by external certification bodies and ISO cannot certify a company or organization directly.

COTS Commercial Off-The-Shelf. COTS are the source of vulnerability, therefore VSTLs are VERY important.

NASED National Association of State Election Directors

NVLAP National Voluntary Laboratory Accreditation Program -The National Voluntary Laboratory Accreditation Program provides third-party accreditation to testing and calibration laboratories in response to legislative actions or requests from government agencies or private-sector organizations. NVLAP-accredited laboratories are assessed against the management and technical requirements published in the International Standard, ISO/IEC 17025:2017.

PDF Portable Document Format, standardized as ISO 32000, is a file format developed by Adobe in 1992 to present documents, including text formatting and images, in a manner independent of application software, hardware, and operating systems.

EOL end of life

SCYTL Scytl Election Technologies S.L.U. is a Spanish provider of electronic voting systems and election technology. Founded in 2001 in Barcelona, its products and services are used in elections and referenda across the world. Scytl is owned by Paragon Group. Scytl is one of the largest election services companies, as is its competitor Dominion Voting Systems

LAOS officially the Lao People's Democratic Republic, is a socialist state and the only landlocked country in Southeast Asia.

Akamai Technologies an American content delivery network, a cybersecurity, and cloud service company, providing web and Internet security services. About Us: We make life better for billions of people, billions of times a day. Every day, billions of people connect with their favorite brands to shop online, play games, share ideas, manage money, and so much more. They may not know it, but Akamai is there, powering and protecting life online

UNIVERSAL VERIFIABILITY: Votes cast are the votes counted and integrity of the vote is verifiable (the vote was tallied for the candidate selected)

INDIVIDUAL VERIFIABILITY: Voter cannot verify if their ballot got correctly counted.

Trapdoor a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able change the value of the commitments however it likes, i.e.: a backdoor, a concealed means of bypassing security to gain access to a restricted part of a computer system.

DHS The Department of Homeland Security– the DHS has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector.

DDoS attack A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices(see below). From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

IoT devices any nonstandard computing device that connects wirelessly to a network and has the ability to transmit data

IV&V Independent Verification and Validation: Verification and validation (V&V) performed by an organization that is technically, managerially, and financially independent of the development organization

SOE standard operating environment: a specific computer operating system and collection of software that an IT department defines as a standard build

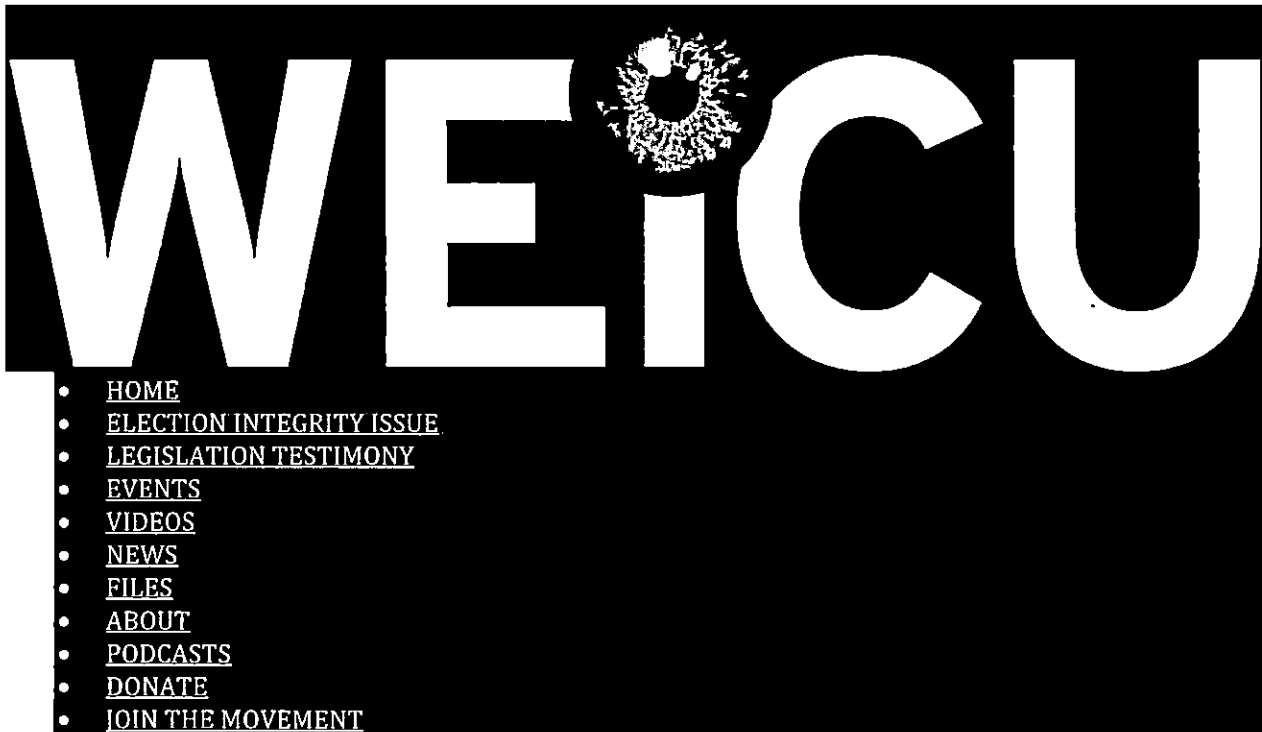
IG Inspector General

*Definitions obtained from Ms. Maras’ affidavit as well as the from the first 2 or 3 internet browser result links for each term, such as Wikipedia, Mirriam Webster, or the term’s web page. This is made for ease of understanding and reference for the repeated use of abbreviations while reading this 37 page affidavit.

EXHIBIT C – a video demonstrating how our machines are compromised, by computer programmer and current Shelby County Election Commissioner/Secretary Bennie Smith:

Web link for video is in body of filing, found on the 4th line of point

#3. <https://weicu.org/fraction-magic> - (appears as Fraction Magic – WEiCU when web-linked)



FRACTION MAGIC

Bennie Smith Explains Fraction Magic

Bennie Smith is the programmer who (with election integrity icon Bev Harris) discovered Fraction Magic.

Tamborine Borrelli of WEiCU talks to Bennie about cyber security issues in WA state pertaining to 3 separate incidences within the 11/3/2020 general election. Among these breaches was a ransomware attack on Lincoln County. Bennie discusses how that could have opened a door to an unsecure election that he , as a sitting election commissioner would not have certified.

Bennie demonstrates how fraction magic works in real time and more importantly how an election could be taken in 5 seconds flat....undetected. He also addresses the “Air Gap Myth” which most election officials have as a false sense of election security.

Exhibit D: is a hyperlink that appears in the body of filing on the 5th line of Point #3:

Fraction Magic - Detailed Vote Rigging Demonstration - YouTube - here is the web site:

<https://www.youtube.com/watch?v=Fob-AGgZn44> and description:

Fraction Magic - Detailed Vote Rigging Demonstration

364,776 views

Oct 31, 2016

6.6K

Dislike

Share

Save



Bev Harris

3.06K subscribers

Subscribe

A real-time demo of the most devastating election theft mechanism yet found, with context and explanation. (See also: Jordan Robertson of Bloomberg Business analyzes Fraction Magic in its Cyber Security Segment: <http://www.bloomberg.com/news/videos/...> and Cover Story in Bloomberg Businessweek <https://www.bloomberg.com/features/20...>)

This demonstration uses a real voting system and real vote databases and takes place in seconds across multiple jurisdictions. Over 5000 subcontractors and middlemen have the access to perform this for any or all clients. It can give contract signing authority to whoever the user chooses. All political power can be converted to the hands of a few anonymous subcontractors. It's a product. It's scalable. It learns its environment and can adjust to any political environment, any demographic. It runs silently, invisibly, and can produce plausible results that really pass for the real thing.

SHOW LESS

AFFIDAVIT

1. I am Bennie Smith, a resident of Memphis, Tennessee – which is located in Shelby County.
2. I serve as an appointed Shelby County Election Commissioner where I am one of a five-member governing body charged with an oath to ensure the integrity of the electoral process.
3. Shelby County is the largest county in Tennessee with over 590,000 registered voters.
4. I am also a Software Engineer, who has had my skills tested at the highest levels with large corporations including Hilton, ABB and Fedex. (CV Attached in Exhibit I).
5. I became involved in election integrity as a citizen and have been involved in promoting election transparency since 2014.
6. Most recently, I have been responsible for evaluating the three (3) major election vendors in Shelby County to replace our aging election equipment through our County Request for Proposal (RFP) process.
7. This government procurement decision is achieved through a thorough purchasing process and a considerable amount of due diligence.
8. I have evaluated the claims made in Michelle Tassinari's affidavit regarding how more than half of the State of Massachusetts equipment creates and stores records in connection to elections. From Tassinari's affidavit, I understand thirty-seven (37) municipalities in Massachusetts use ES&S equipment referred to as DS200, which is a precinct scanning component.
9. This DS200 has a very similar methodology in how it processes digital ballot images to the Dominion voting equipment – ImageCast, which I understand is used in 175 additional towns/cities in Massachusetts.

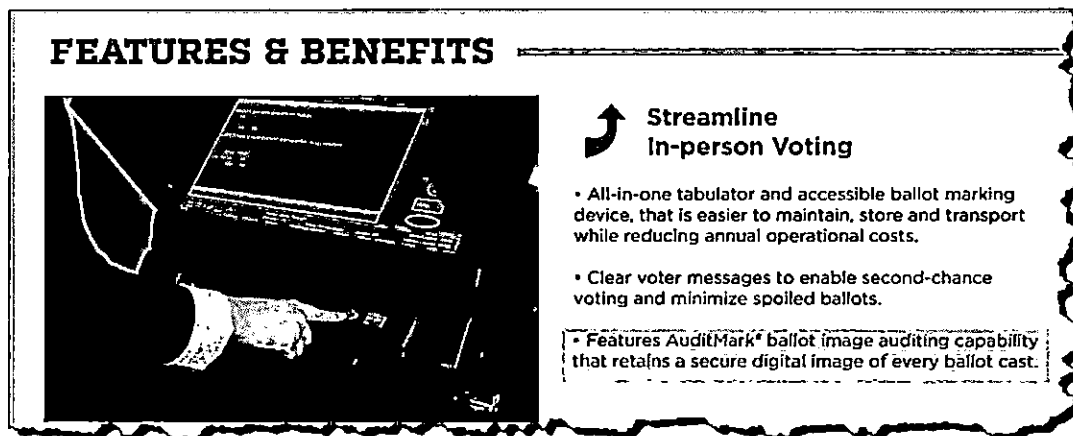
BALLOT IMAGES ARE GENERATED, AND ARE INDISPENSABLE
TO ELECTRONIC VOTING SYSTEMS

10. In Paragraph 9 of the Tassinari affidavit, I encountered the following statement: *“Voting equipment used in Massachusetts does not create or store ballot images.”*

11. On page 2 of the marketing brochure from Dominion for its voting systems, Exhibit II, in its features and benefits section, openly declares that their equipment creates and stores ballot images.

Specifically, it states:

“• Features AuditMark® ballot image auditing capability that retains a secure digital image of every ballot cast.”



12. As an Election Commissioner in Shelby County, I evaluated the responses to the RFP from Dominion, which emphasized that creating and storing ballot images was a core-patented function of how the system operates. It is not realistic to think they would go through creating a proprietary AuditMark® solution, and then have none of its customers use it.

13. The ballot images are processed in the Results Tally and Reporting (RTR) component of the Dominion system, as detailed in *Dominion's Democracy Suite® EMS Results Tally and Reporting User Guide* in Exhibit III, to create the data needed for vote tabulation. Vote tabulation consists of two major sub-systems: I. Acquisition and pre-processing of the ballot images, done by the computer; and, II. Human adjudication of those ballot images that need to be reviewed, which are performed by bi-partisan election officials, and the tabulation of the valid ballot images done by the computer. **In order to do execute these two activities, ballot images must exist.**
14. The first sub-system enables the Acquisition and Pre-Processing of the vote, and demands these basic processes:
- a. Scanning the paper ballot to generate a ballot image that is stored
 - b. Processing and interpreting the ballot image to determine if voter selections are valid. For example, a ballot image can be found to be invalid if the voter selected two candidates in a vote for one race e.g. someone selects Biden and Trump for President of the United States.
 - c. Accepting or rejecting the paper ballot submission based on the processing and interpreting of the ballot image. If the ballot image is invalid, the paper ballot is rejected, and the voter is given the paper ballot back to correct.
15. To reiterate, without ballot images, none of the processes in 15a, 15b, 15c can occur during the acquisition and pre-processing steps; meaning without ballot images, there can be no election using the ImageCast technology.
16. These processes (above in 15) must happen using the ballot image because the pre-processing algorithms first run against the ballot images to determine if the ballot is filled out correctly. If it is not, then the paper ballot is sent back to the voter to correct. If it is correct, then the ballot image is

run through additional image processing algorithms that execute a series of grids and timing marks to calculate where the selections are on the scanned ballot.

17. The ballot images, results files and audit logs are records generated by the ImageCast system and are stored on two compact flash drives for redundancy. In the pre-processing, the ballot images are marked with the AuditMark® technology, and are used to create a Cast Vote Record (CVR) from each ballot image. The CVR contains the results from a single ballot image. The CVRs are aggregated to produce the List Vote Record (LVR) also known as the results file, which contains the results of processing multiple valid ballot images.
18. The second sub-system, the EMS, enables the human adjudication of those ballot images that need to be reviewed by bi-partisan election officials. **If Tassinari is taken at her word, what it means is that any ballot images that needed human adjudication would never be presented to election officials, and those votes would never be counted! They would simply disappear.**
19. The EMS also performs computer tabulation using the valid ballot images and result files. Furthermore, the creation and storage of ballot images is so essential to the core design that Dominion in their RFP submission, stated the following:
“The ImageCast Central stores ballot images by scanned batches. The scanned ballot images are migrated to the Election Management System through computer networking or removable media. As with results data from any precinct scanners in use for an election, Results Tally and Reporting is the portion of the EMS that processes the images to provide tabulation and operational reports to the jurisdiction” (page 26 of RFP submitted by Dominion to Shelby County, see Exhibit IV)
20. In their response to Shelby County’s RFP, Dominion also highlighted as a security benefit of their ImageCast system, *page 94-98 of the RFP’s Question 26, in Exhibit V*, that three files are created by the machine: the results file, the ballot images, and audit logs, in order to ensure that the electronic

data matches the paper ballot, so it can be used to **recreate and audit an entire election, without having to resort to the paper ballots.**

21. The retention of results file, ballot images, and audit logs are critical to ensuring election integrity

22. The User Manual states:

2.4.5 Results Auditing. In most cases, after Election Results are processed, an audit is initiated to examine the system operation in more detail. The first step when performing an audit is to look up the list of scanned ballot images and the log files based on specific criteria. All audit record entries include a time-and-date stamp. The generation of audit record entries will not be terminated or altered by program control or the intervention of any person. The physical security and integrity of the record are maintained at all times.

23. The system also provides Export capabilities to archive and curate all data from an entire election:

- *Export Audit Images: Export audit images to the Results directory on NAS [Network Attached Storage]. – Show Export Log: Show log on export activity in Notepad format.*

24. Moreover, the User's Manual also provides the *Best Practices* of how to handle the Ballot Images

*CHAPTER 6: IMPORTING ELECTION RESULTS Election results (including the scanned ballot images and log files) are stored on the Removable Media and can be stored on local file system or on the NAS. Each file type (result files, **ballot images** and log files) may be imported together or separately. This allows for the flexible management of results after the election occurs. **Since ballot images take a significant amount of time to import, your jurisdiction may decide that they are imported after the results have been completely tallied. Result and log files, however, take only a few seconds to load. Tasks covered in this section:***

Figure 6-3: Load Results dialog 8. It is possible to load the result files, ballot images, and log files separately. For instance, If you want to load ballot images, you need to enable Load Ballot Images and make sure that other checkboxes under Actions are cleared.

25. In closing, the ImageCast does not function with out the “Image” – the ballot image - that was Cast. It is completely antithetical to its name and existence. In fact, the calling card – the unique selling proposition - of Dominion’s ImageCast – “Image” “Cast” - is this ability, which is patented, to mark ballot images, and to be able to provide Election Commissioners like myself with audit capabilities based on evidence and a secure chain of custody for certification while assuring election integrity.
26. What is possible, however, is to choose to discard the ballot images, by not transferring them into the EMS to preserve as a permanent record, during or after tabulation. In such an event, there still would be a record created in the log files documenting that ballot images were not elected to be retained.
27. If one reads the features section of the User’s Manual, the entire system’s core function operates using a digital ballot image, which is generated for adjudication and tabulation.

ONGOING DUE DILIGENCE OF REVIEW OF ERIC COOMER’S
TESTIMONY FURTHER CLARIFIES THE USE OF BALLOT IMAGES

28. As a part of my ongoing due diligence of evaluating Dominion’s electronic voting systems, I also reviewed the 766-page transcript of Eric Coomer’s testimony given on September 10, 2020 relative to the case in the District Court in the Northern District of Georgia, *Curling v. Raffensperger*, 17-CV-2989-AT.
29. Mr. Coomer is the Director of Product Strategy and Security for Dominion Voting Systems.

30. Mr. Coomer’s entire transcript can be viewed at here: <https://coalitionforgoodgovernance.sharefile.com/share/view/sb251b27a09d4ec99> .

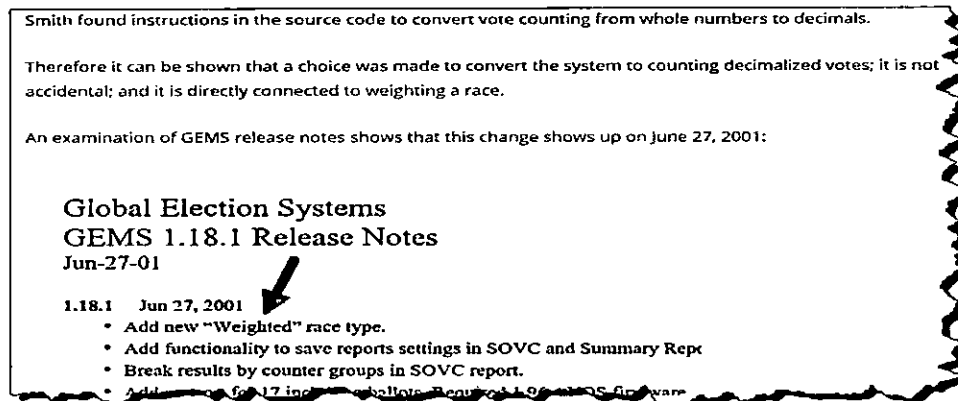
31. These statements of fact from Mr. Coomer concerning ballot images are provided to this Court:

Question	Answer
So does that mean that both precinct and central count scanners create digital ballot images?	That's correct.
And precinct scanners save -- they have the capacity to save those ballot images; correct?	Both devices do, yes.
Okay. And whether or not they save the ballot images is governed by tabulator settings; is that right?	Yes. There is a setting that can determine that.
So if you -- in a precinct scanner when ballot images are set to be saved, the scanner saves those to the compact flash memory card; right?	Correct. It actually saves them to two compact flash. So we have redundant storage.
<p>ICP = ImageCast Precinct (Digital Scanner)</p> <p>I'll turn to the ICP scanners and tabulation of hand-marked paper ballots. What does the ICP read when a hand-marked paper ballot is placed into the scanner?</p>	<p>Regardless of whether it is hand-marked or the QR ballot, the scanners first take a digital image of both sides of the ballot. In the case of hand-marked paper ballots, it looks for various artifacts that are included on the printed ballot. These are referred to as things like long corner marks and the timing marks. You can see those in any of the ballot representations that have been presented. That is used to essentially orient the image so that then we can apply our image processing algorithms. We use those corner marks to orient the image. We use the timing marks, essentially set up a grid to define where the specified voting target locations are. And then our image recognition analyzes those target areas and looks for -- essentially calculates the percentage fill of those areas to determine whether it is a mark or not -- a selected choice or not.</p>

32. Mr. Coomer’s testimony provides the details of ballot image processing and their indispensable use.

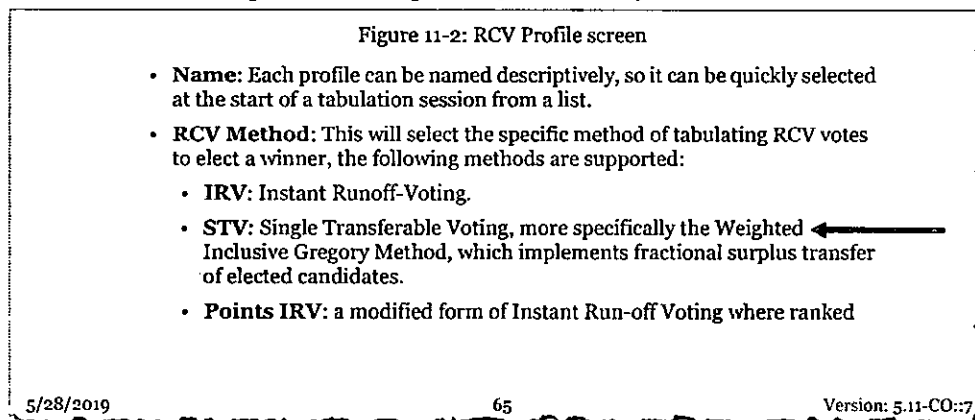
WEIGHTED RACE

33. In 2014, I discovered the weighted election feature in the GEMS Election Management System release notes of 2001. GEMS is owned by Dominion and still in use in Shelby County and many other jurisdictions. GEMS was also operated in the entire state of Georgia until 2019 (though serviced by ES&S) until its new generation technology was implemented.



34. I can demonstrate how destructive this feature is as its function is the absolute removal of one person, one vote.

35. The current name of this feature appears to be the STV Ranked Choice Voting method, as documented in 2019 User's Manual, and clearly indicates a "Weighted" method, "which implements fractional surplus transfers of elected candidates." Counter to Ms. Tassinari's assertion, it is safe to say the vendor knows their capabilities, especially since they documented it in their User Manual.



CONCLUSION

36. Paragraph 9 of the Tassinari affidavit - "*Voting equipment used in Massachusetts does not create or store ballot images.*" – is incompatible with the documented function of electronic voting systems, in which ballot images are necessary to conduct elections.
37. It is indisputable that digital ballot images are records that are generated and stored by the ImageCast system. Moreover, with such a necessary and indispensable component to operate, tabulate, audit, adjudicate an election, there is a Federal requirement that this information be retained.

Signed under pains and penalties of perjury,



Bennie Smith

273 Colbert Street West, Collierville, TN 38017

December 15, 2020

EXHIBIT I - CV

BENNIE J. SMITH

273 Colbert Street West • Collierville, TN 38017 • Mobile: 901.213.6883 • Email: benniejsmith@outlook.com

ELECTION EXPERIENCE**DEMOGRAPHIC AND TURNOUT ANALYTICS**

Consult with numerous candidates and campaigns for the offices of: Governor, Senate, Congress, District Attorney, Sheriff, City/County Mayor, Judge, Juvenile/Criminal/Circuit/City/County Clerk, County Commission, Assessor of Property, State House/Senate, City Council, School Board using a proprietary micro-targeting application and predictive analytics method to forecast voter turnout.

ELECTION INTEGRITY (BLOOMBERG) AND RESEARCH

CYBER SECURITY SEGMENT	(How to Protect Against Election Day Hacking)	NOVEMBER 2016
COVER STORY IN BUSINESSWEEK	(The Computer Voting Revolution Is Already Crappy, Buggy, and Obsolete)	OCTOBER 2016
ELECTION SYSTEM RESEARCH SERIES	(blackboxvoting.org: Fraction Magic)	MAY 2016

SUMMARY OF QUALIFICATIONS

An experienced professional with extensive technical skills, financial and business acumen including: Project Management • Visual Studio • Visual Basic • SSIS • Oracle • PL/SQL • VBA • HTML5 • SQL • ASP • ADO • CSS • SQL Server • T/SQL • BI • Essbase • 6Sigma • TM1 • Reporting • Power BI • Spotfire • C#, VB.NET • Process Improvement and Automation • Database Development • RDBMS • SDLC • Ability to interpret and apply practical solutions to business problems • Strong analytical problem solving and organizational skills

WORK EXPERIENCE

CONSULTANT	DECEMBER 2019 – CURRENT	Memphis, TN
------------	-------------------------	-------------

SMATSOFT LLC

Custom web applications and visualizations, financial prediction models to analyze streaming revenue potential, forecasting and audits.

- Developed royalty payment application to process allocation and contract rules for artists, distributors and music labels.
- Financial modeling, KPI Dashboards, Backend Data modeling to analyze music trends and future streaming potential.

HR DATA ANALYST	DECEMBER 2018 – DECEMBER 2019	Memphis, TN
-----------------	-------------------------------	-------------

FEDEX EXPRESS

Develop analytical visualizations and web applications for the HR Analytics and Innovation Department to measure Safety, Training, QDM (Quality Driven Management) performance, Retention opportunities, turnover rates and the FedEx LiFE program statistics.

- Developed dashboards to identify demographic indicators and KPI metrics to analyze and reduce costs associated with safety
- Created a training journey application to function as an onboarding tool combining multisource training through a dashboard
- Developed web applications to manage talent, relocations, officers and directors, pay equity reviews (diversity and seniority)

FINANCIAL ANALYTICS MANAGER	MARCH 2018 – NOVEMBER 2018	Memphis, TN
-----------------------------	----------------------------	-------------

ABB

Financial Analysis & Reporting, Inventory, Cost Savings, Process Improvement, Statistics, Implement Actionable Analytics.

- Created a budget, cost center and P&L analysis workflow and reporting method for finance controllers and executives.
- Completed Green Belt Training and Implemented a Freight Cost savings project to save 1m+ in overpaid charges.
- Created a Net Price Variance model to examine pricing trends and identify over 60m in unused pricing logic.

SR. ANALYST – BUSINESS ANALYTICS COE	JUNE 2016 – FEBRUARY 2018	Memphis, TN
--------------------------------------	---------------------------	-------------

Thomas & Betts/ABB

Serve as an internal consultant/liaison to various groups within finance and IT. Combine business and technical knowledge to provide innovative practical solutions, processes improvement and document best practices within the business analytics.

- Created mass allocation tool to distribute 2 billion+ in product line targets by region, sales office and distributor saving 3.5m.
- Created a daily detail merge tool to pull global sales, auto generate analysis charts, and reports, agent commissions reporting.
- Created an inventory analysis tool to pull all US usage history giving visibility to 20m in excess or obsolete inventory.

APPLICATION DEVELOPER	OCTOBER 2010 – MAY 2016	Memphis, TN
-----------------------	-------------------------	-------------

Thomas & Betts/ABB

Interface with departments and plants to develop custom applications, business intelligence reports, dashboards, Cognos cubes, crystal reports, SSIS packages, Oracle/SQL Server views to standardize and streamline quantitative analysis and consolidate efforts.

- Coordinate with various departments to gather requirements, make automation recommendations and develop IT Solutions.
- Create custom applications to implement process automation for Electrical Finance, Global Supply Chain and individual plants.
- ETL data warehouse collection from various sources, enforce data integrity, automate data collection, and optimize reporting.

CORPORATE REVENUE ANALYST	MARCH 2007 – MAY 2010	Memphis, TN
---------------------------	-----------------------	-------------

Hilton Worldwide

Support the Corporate Revenue Management department by developing custom applications and business intelligence reports to maximize revenue and market share, analyze demand factors; forecast business levels; identify pricing strategies and trends.

- Created statistical diagrams, charts and new reports to analyze and validate revenue management strategies.
- Created and maintained monthly consolidated reports for Regional Directors of Revenue Management Vice Presidents.
- Custom reports for Regional Directors, Senior and Area Vice Presidents, Global Heads, Portfolio reports for the President.

Contract Work for the following companies:

- International Paper • Custom application development to calculate machine production metrics.
- First Tennessee Bank • Custom VBA Applications for consumer lending, audits and underwriting, to manipulate and retrieve mainframe home loan origination data, audit home loans and HELOCS based on lending rules, guidelines and requirements.

SR. PROGRAMMER ANALYST

APRIL 2001 - APRIL 2003

Memphis, TN

Associated Softworks

Worked as liaison between elected officials and IT, system testing and development and maintenance of City Applications such as:

- Traffic Violations Bureau, Mayor's Citizens Service Center, Solid Waste, Property Maintenance, Internal Affairs (IAB, ISB)
- Housing Inspection, Carts Public Works, etc. User maintenance, Server maintenance (SQL, NT)
- BA: City Court Clerk Court System Replacement, Internal Affairs (New Case Management System), Traffic Violations Bureau system enhancements. Data migration for City annexations.

Exhibit F – Maria Zack’s testimony before Kansas Senate

Web address: <https://rumble.com/vxw1te-maria-zacks-earth-shattering-testimony-kansas-senate-hearing-mirrored.html>

Maria Zack's Earth Shattering Testimony - Kansas Senate Hearing (Mirrored)

Red Pill 2020 Published March 19, 2022 18,016 Views



SUBSCRIBE

12K

SHARE

459

rumbles

EMBED

Maria Zack releases never before heard information on the 2020 election. What happened in 2020? What happened to the Italian witnesses? Who benefits from election INSECURITY? Italy, China, Satellites and more.

GENERAL AFFIDAVIT

Aff VI pg 1 of 1

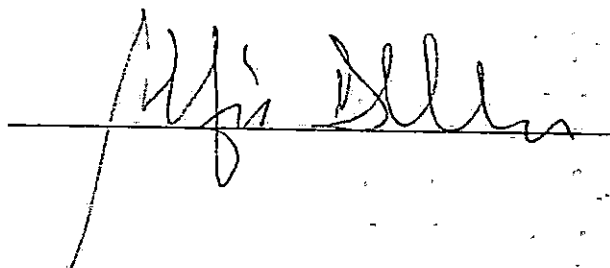
Region of Lazio
Country of Italy

I, Prof Alfio D'Urso, Advocate/Lawyer, of Via Vittorio Emanuele, Catania, 95131 Italy, do hereby provide the following affidavit of facts as conveyed in several meetings with a high level army security services official:

Arturo D'Elia, former head of the IT Department of Leonardo SpA, has been charged by the public prosecutor of Naples for technology/data manipulation and implantation of viruses in the main computers of Leonardo SpA in December 2020. D'Elia has been deposed by the presiding judge in Naples and in sworn testimony states on 4 November 2020, under instruction and direction of US persons working from the US Embassy in Rome, undertook the operation to switch data from the US elections of 3 November 2020 from significant margin of victory for Donald Trump to Joe Biden in a number of states where Joe Biden was losing the vote totals. Defendant stated he was working in the Pescara facility of Leonardo SpA and utilized military grade cyber warfare encryption capabilities to transmit switched votes via military satellite of Fucino Tower to Frankfurt Germany. The defendant swears that the data in some cases may have been switched to represent more than total voters registered. The defendant has stated he is willing to testify to all individuals and entities involved in the switching of votes from Donald Trump to Joe Biden when he shall be in total protection for himself and his family. Defendant states he has secured in an undisclosed location the backup of the original data and data switched upon instruction to provide evidence at court in this matter.

I hereby declare and swear the above stated facts have been stated in my presence.

DATED this 6th day of January 2021 at Rome, Italy.



General Affidavit

Editorial | Foreign | Election Fraud | Italy | The Effort to Take Out Trump

- Editorial
- Foreign

Conte, Leonardo SpA and the U.S. Embassy behind the Election Data Switch fraud to take out Trump

Italy and Conte played a key role in the international cyber plot to take out Trump. Leonardo Finmeccanica's Cyber Warfare satellites are among the means used -

January 5, 2021
8341

by Riccardo Corsetto



Riccardo Corsetto
Director L'UNICO

"The Italian Government and Prime Minister Guisepppe Conte are directly involved in the electoral fraud that affected the American elections leading to Joe Biden's pending illegal victory." According to US investigative sources working here in Italy since 18 November 2020, it was the US Embassy in Rome who coordinated the data manipulation of votes cast for President Trump to Joe Biden, with the technical complicity of Leonardo SpA, a company that is 31% owned by the Italian Government and generates more than half of its multi billion USD annual revenue from its US based subsidiary. Leonardo DRS whose chief executive officer, William Lynn III, was formerly the undersecretary of

defense during the Clinton Administration. Leonardo DRS is actively pursuing a public listing on the NYSE in 2021.



Leonardo SpA, formerly known as Finmeccanica underwent a name change in January 2017. According to individuals who carried out the data switch operation under the direction of US intelligence officials in the American Embassy, they utilized one of Leonardo's advanced military spec (cyber warfare) satellites to transmit manipulated votes back to Frankfurt servers and on to the United States, as reported by the journalist Cesare Sacchetti. **Leonardo S.p.A.** it is the largest industrial company in Italy and is active in the fields of defense, aerospace and cyber security. The largest shareholder is the Italian Ministry of Economy and Finance, which owns a share of approximately 31%.

Leonardo-Finmeccanica merged the activities of previously controlled companies such as AgustaWestland, Alenia Aermacchi, Selex ES, OTO Melara and Wass. Leonardo is the tenth largest defense company in the world and the third largest in Europe with revenues from the defense sector representing 68% of its annual revenue. The company is listed on the FTSE MIB index of the Milan Stock Exchange. The company is structured in five operational divisions: Helicopters, Aircraft, Aerostructures, Electronics and Cyber Systems for Security and information. In Fiscal Year 2020, the US Government awarded nearly \$1B in cyber security, intelligence and defense contracts to Leonardo SpA.

The former chairman of Leonardo is Gianni De Gennora who left Leonardo in May 2020.

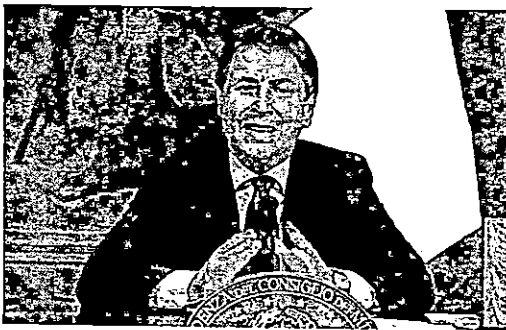


Leonardo SpA Chief Executive Officer Alessandro Profuma, a former banker who in October 2020 was condemned for the scandal of Banca di Monte Paschi di Siena. Alessandro Profumo was appointed by the Gentiloni Government and reconfirmed by Prime Minister Giuseppe Conte. The same Profuma was recently sentenced to six years for banking irregularities by Italian courts.

One of the board of directors of Leonardo SpA (2017) was Professor Guido Alpa, a former law partner of Giuseppe Conte in Rome.

Prime Minister Giuseppe Conte in recent days had been the subject of press articles about plans to establish private intelligence agencies.

The involvement of the Italian Government through Leonardo SpA



The President of the Council - Prime Minister Giuseppe Conte

The Conte Government is believed to have played a key role in the international coup that would have compromised President Donald Trump's reelection.

Switzerland has recently come under heavy accusation of complicity in the alleged cyber coup, as claimed by Neal Sutz, a Swiss-American blogger, who denounced Switzerland's active role in US presidential fraud.

Scylt, Swiss software linked to Dominion Voting Machines

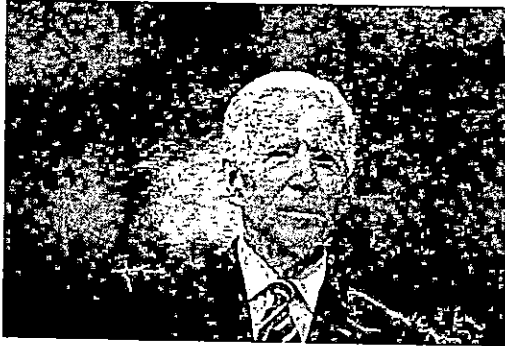
It all starts with Scylt, denounced Neal Sutz, a software purchased by the Swiss national postal service, which is directly implemented in Dominion Voting Machines at the center of the US election scandal, directly linked to the tycoon George Soros.

According to Sutz, Switzerland never informed the Trump Administration of the serious flaws in the Scylt software, well known to the Swiss Government, and added that it had evidence of the plot that President Trump's lawyers would acquire.

According to local sources with direct knowledge of these events reporting to *Nations in Action*, the US nonprofit for election integrity and public governance transparency, the manipulated data was transmitted from Frankfurt to Rome via the US Embassy in via Veneto, according Rome the central role in the alleged international election plot to overturn the ballots cast by American citizens for the next President of the United States thereby creating a constitutional crisis.

On the night of 3 November (in the United States) – approximately 8 o'clock in the morning Italian time – the counting of votes was simultaneously suspended in a number of key battleground states, as shown by some official videos taken from the closed circuit of the Atlanta polling station and which we have documented extensively in this newspaper.

At that point while the fraud was already widely initiated, the Leonardo SpA IT hackers realized that "Trump stood above Biden for a very large and *unexpected number of votes*" so much so that manipulation was in vain and not enough to make him lose.



U.S. President-Elect Joe Biden

Sicilian born Igzanio Moncada, CEO of FATA SpA, a wholly owned subsidiary of Leonardo SpA, is believed to be a bridge between some secret services and the Italian Beijing Business Association, the Italian Iran Business Association and the Italian Qatar Business Association. It has been stated that Moncada may be a key figure in the eight month planning of the election hacking in Italy.

Senior US Embassy personnel in Italy reportedly gave the order to act, coordinating the hacking and developing "new algorithms", states a key witness of the fraud, to secure a win for the democrat candidate **Joe Biden**.

The role of the US Embassy in Rome



The US Ambassador to Italy, Lewis Eisenberg

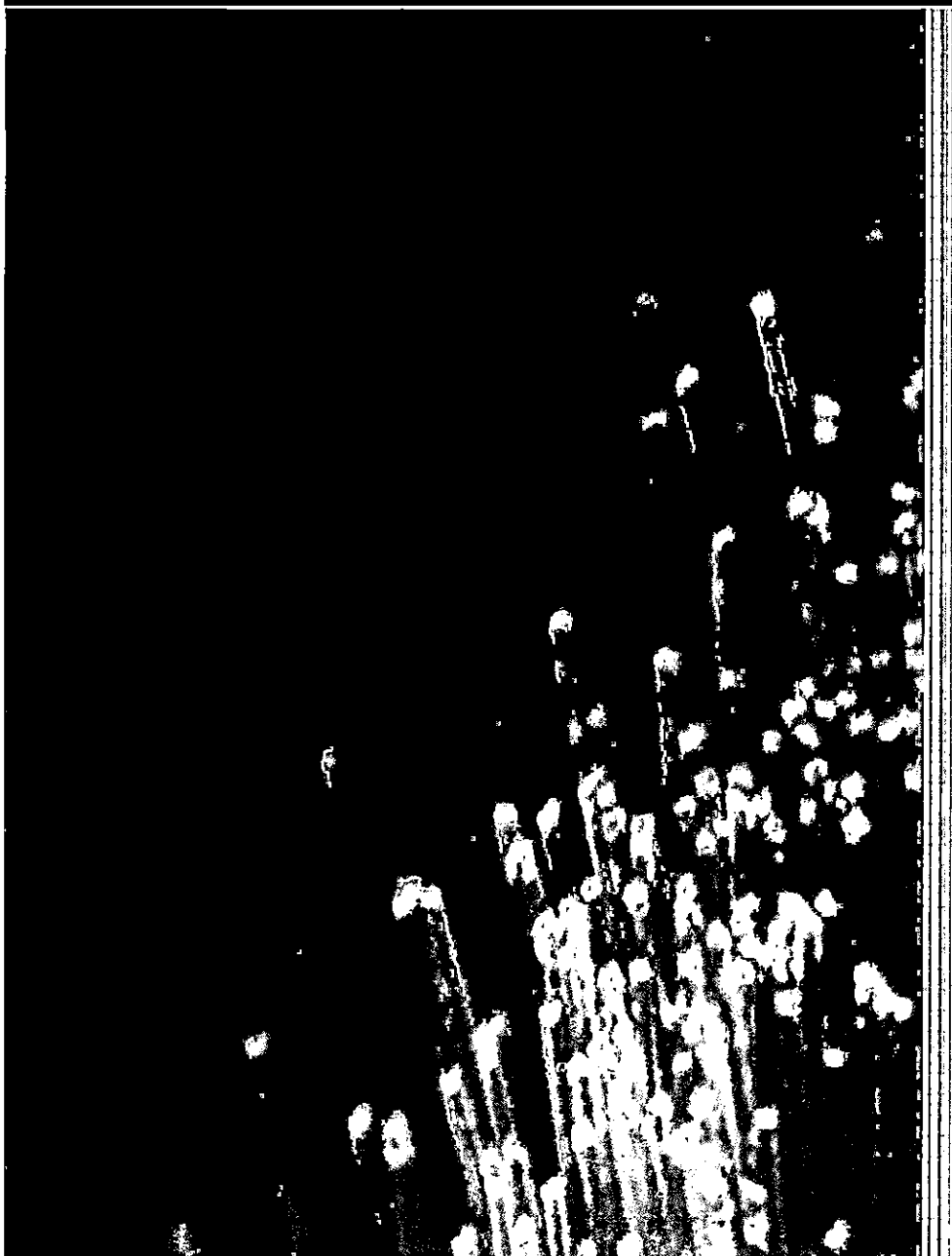
We would not advance this story if it had not come from a former member of the world's largest cyber warfare aerospace and defense conglomerate based in Italy. The US Ambassador to Italy is **Lewis Eisenberg**, very critical of President Trump's military disengagement in the world and who is very close to the neo-Zionist lounges connected to the Goldman circuit.

Three senior officials from the US intelligence community, landed at Leonardo da Vinci Airport in Fiumicino several days prior to the November 3rd 2020 election in the US. According to a former CIA agent, the three intelligence operatives were housed at the U.S. Embassy in Via Veneto to coordinate hacking operations during election count suspension from November 3-4.



**Mesa County
Colorado
Voting Systems**

**Report #1 with
Forensic Examination and Analysis**



September 2021

Mesa County, Colorado, Voting Systems

**Report #1 with
Forensic Examination and Analysis**

15 September 2021

Table of Contents

Executive Summary	1
Introduction	3
Legal References.....	5
Forensic Examination and Analysis Report	7
Forensic Analysis	8
System Identification.....	8
Authenticity and Chain of Custody	10
FINDINGS	11
Overview of System Data Sources	11
Server Disk Partition Structure Overwritten.....	12
Website Server Log Files Missing	15
Server Microsoft SQL Server Installation Log Files Missing.....	17
Server Microsoft SQL Server Log Files Missing	19
EMS Server Dell Server Updates Missing.....	20
Server 'Administrator' WebCache Log Files Overwritten.....	22
Server 'emsadmin' WebCache Log Files Overwritten	23
Server SQL Server Management Studio (SSMS) Log Files Overwritten.....	25
Server CBS Log Files Overwritten	26
Server Election Databases Missing.....	27
Server Event Logs Missing/Overwritten	29
Server System Users are Missing	31
Server Virtual Directories Log Files Missing.....	32
Server Windows Defender Log Files Missing/Overwritten.....	33
Server List of .log files in Before Image that were Deleted.	34
Significant Number of Logfiles Missing	35
List of .evtx Event Log Files deleted	36
Analysis Summary	41
Conclusion.....	41
Appendix A. Deleted ".log" files after Dominion Trusted Build update.....	42
Appendix B. Supporting Documentation: File details and hash sets for screenshots	61
Appendix C. Microsoft EVENT log files.....	62
Appendix D. List of Figures.....	76
Appendix E. 2002 Voting Systems Standards (VSS)	77

EXECUTIVE SUMMARY

This report documents initial findings in an ongoing forensic examination of the voting systems of Mesa County, Colorado, used in the November, 2020 General Election. These voting systems represent a portion of overall election systems infrastructure, and this report is limited to the findings of an ongoing investigation. The findings in this report were prepared by the cyber forensic expert retained to advise the County Clerk pursuant to her duties as the county's Chief Election Official as part of the impacted parties' legal team.

Federal law requires the preservation of election records – which includes records in electronic or digital form – for twenty-two months after an election. Colorado law requires the preservation of election records for an additional three months beyond the Federal requirement. The obligation to ensure the integrity of elections and that all election records are preserved pursuant to federal and state law falls to the elected Clerk & Recorder. This report, the first of several, is based on examination of the data obtained from forensic images of the Dominion Voting System EMS server last used in Mesa County for the November, 2020, election, images taken in furtherance of the preservation requirements of federal and state law. Based upon information received by the Clerk's office from various sources in early 2021, the Clerk became concerned that the voting system modifications might jeopardize these preservation and other legal requirements under the responsibility of the County Clerk. For this reason the Clerk ensured a full backup of election records from the County voting systems, both before and after the software modification performed by the vendor and the Secretary of State on May 25-26, 2021, just six months after the November, 2020, election.

Forensic examination¹ found that election records, including data described in the Federal Election Commission's 2002 Voting System Standards (VSS) mandated by Colorado law as certification requirements for Colorado voting systems, have been destroyed on Mesa County's voting system, by the system vendor and the Colorado Secretary of State's office. Because similar system modifications were reportedly performed upon county election servers across the state, it is possible, if not likely, that such data destruction in violation of state and federal law has occurred in numerous other counties.

The extent and manner of destruction of the data comprising these election records is consequential, precluding the possibility of any comprehensive forensic audit of the conduct of any involved election. This documented destruction also undermines the conclusion that these Colorado voting systems and accompanying vendor and Colorado Secretary of State-issued procedures could meet the requirements of Colorado and Federal law, and consequently vitiates the premise of the Colorado Secretary of State certification of these systems for use in Colorado.

Two backup images, using forensic imaging methods, were obtained from the Dominion Voting Systems (DVS) Democracy Suite (D-Suite) Election Management System (EMS) Standard Server in Mesa County, Colorado. The first image was made of that EMS Standard Server in the D-Suite 5.11-CO version configuration, as used in the November, 2020 election. The second image was of the configuration of the EMS Standard Server in the D-Suite 5.13 version configuration, following the modification of the EMS Standard Server by a combined team of DVS vendor personnel and Colorado Secretary of State staff. The forensic information provided in this report is presented using screenshots from forensic analysts' systems running industry-standard forensics software tools. The report includes "before" and "after" screenshots from the forensic tool that shows the differences between the two backup images.

The forensic examination found that numerous logfiles had been deleted or overwritten. These logfiles are required to reconstruct the function of and events taking place on the the voting systems, and based upon information

¹ Many individuals and organizations, some public officials, have made recent claims that no audit performed nor examination conducted on elections or computer-based election systems can be legitimate or credible unless the examiners are "election experts" or accredited election auditors. There is no such thing as an "accredited election auditor," nor are there Federal standards or procedures to credential election auditors.

provided by legal counsel, must, by law, be preserved. By comparing filenames in the two images (before and after the Dominion update on May 25-26, 2021), examination and analysis identified a total of 28,989 files that were deleted. During a software update, some replacement of program files and their related content is normally expected. However the examination found that 695 log and event log files necessary for the determination of election integrity were deleted.

Based upon information provided by legal counsel, Colorado law (Colorado Revised Statute (CRS) § 1-5-601.5) requires that, prior to use in Colorado elections, electronic and computer-based voting systems be certified by the Colorado Secretary of State. This certification is based on the systems' compliance with the requirements of the Federal Election Commission's 2002 Voting System Standards (VSS), verified by their testing by a Federally-accredited (by vote of the U.S. Election Assistance Commission (EAC)) Voting System Testing Lab (VSTL). While several iterations of newer Voluntary Voting System Guidelines (VVSG) have been issued by the EAC, Colorado's statutory requirement is for compliance with 2002 VSS, which states:

"Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation."

The relevant sections of the VSS are cited in Appendix E.

These statutory requirements establish that voting systems are required to generate and preserve, as critical to the ability to determine and reproduce the conditions and details of election conduct using these systems, logfiles of all system functions, including normal activity, connectivity, file and data access, operator- and automated-processes, and errors. Logfiles are critical to the ability to detect improper operation, including the ability to detect malicious intrusions as well as other improper activities and conditions, and configuration changes that could enable alteration of the actual vote count.

Assuming this information to be correct, this forensic examination found that a substantially large number of these requirements have not been met. This examination also found that destruction of critical logfiles has occurred. This destruction is not incidental or minor but is extensive.

The purpose of this initial report is to document these findings and present preliminary evidence demonstrating unacceptable conduct and system defects revealed by the examined images, as necessary for the Chief Election Official to discharge her statutory obligations. The facts and resultant findings support the conclusions that:

- 1) Election-related data explicitly required to be preserved, as stated in the 2002 VSS criteria referenced in this section, have been destroyed in violation of Federal and State law, and
- 2) Due to non-compliance with the 2002 VSS requirements, these voting systems and accompanying vendor-provided, Colorado Secretary of state-approved procedures cannot meet the certification requirements of the State of Colorado, and should not have been certified for use in the state.

Comprehensive investigation is required to determine whether these critical failures are the result of malicious intent or negligence, and to what extent the systems may have been compromised or subjected to unauthorized access or operation prior to, during, and after election use. That comprehensive investigation *is beyond the scope of this report*. Subsequent reports will address these issues in detail.

Evidence supporting all of these findings is documented in this report.

Introduction

Election officials, including Secretaries of State, are obligated by law to ensure the integrity of all elections, including the transparency required for citizens to verify that integrity themselves. Modern electronic voting systems are marketed as an efficient solution to streamline the voting process and allow for automated collection, tabulation, and reporting of election results, but the efficiency they promise comes at a cost.

The necessary measures and safeguards to ensure the integrity of the systems and their operation against a severe, mounting and ever-evolving threat from sophisticated nation-state and non-nation-state actors are so complex and dynamic as to outpace the limited capabilities and resources of our government, at all levels. While minimal security safeguards may be within government capacity, modern computer-based voting systems are extremely complex and difficult to secure, even for cybersecurity experts, and since voting systems are not under the direct control of the Federal government's top security experts, any government assurances about the sufficiency of those safeguards can serve only to mislead citizens and policy-makers. Even critical defense systems, relentlessly monitored and defended by highly-trained teams using costly, sophisticated tools, are at risk and are frequently compromised, sometimes before procurement. Earlier generations of voting systems relied on simple, human-scale safeguards, for example "air gaps"—that is—to have no wired network connection to the system. But miniaturized wireless communication technologies and networks have proliferated, with billions of wireless devices installed or in use, and malicious actors have developed sophisticated attacks to bypass air gaps, compromise every kind of hardware, firmware, and software, often before they even come into customer or user possession, and to move laterally through networked systems, often undetected. Supply-chains for these systems, from the initiation of the design of integrated circuits and electronic components, most manufactured overseas with little U.S. insight or oversight, through the fabrication, testing, assembly, integration, and operation of these complex composite systems, are vulnerable and untrustworthy for critical functions of government and lucrative economic and national security targets. For all these reasons logfiles, such as those that have been deleted by the Dominion "Trusted Build" update must be preserved to document the complete operation of the computer system and voting applications, and to be able to verify the authenticity, integrity and accuracy of the vote.

The feature size of individual circuits in the chipsets and components of our voting system computers is at the nanoscale, smaller than the smallest known virus particle, and less than 3/10,000ths of the width of a human hair. So we have lost the ability, if we ever had it, to visually verify what is really happening, even at the physical level, in our computer-based voting system. Regardless of how the systems appear to be configured to authorized users and poll-watchers, the functionality and connectivity in these computers can be enabled and modified remotely and wirelessly, or by the introduction of embedded codes on scanned paper, or triggered by specific unforeseeable and indiscernible predetermined software and hardware conditions, or by specific timing events, or by geographic location, or by the proximity of other devices or combinations of any of these means.

For example, some Colorado voting systems ordered as specified by the voting system vendors, from foreign manufacturing and assembly facilities, have included "Integrated Dell Remote Access Controllers (IDRAC)," which are designed to allow "out-of-band" remote management of those systems, meaning that the computers are explicitly equipped to be controlled by remote automated programs or by individuals other than those logged in locally. Through the IDRAC, voting systems might have any aspect of their Basic Input/Output System (BIOS), operating system, or applications controlled or modified, including the addition and deletion of user accounts, the enabling of communications components like wireless networking cards, and the modification, installation, removal or configuration of software and settings. Like the inclusion of multi-band wireless networking cards, similarly specified and ordered for Colorado voting systems by the vendor, there is no excuse or rational justification for the inclusion of components like these, and the fact that the entirety of U.S. voting system regulatory processes and institutions can apparently neither detect, note, nor address these gross vulnerabilities eviscerates the notion that our computer-based voting systems have been secured.

Faced with incredible miniaturization, the importance of logfiles which are records of operation of a computer system, are more important than ever in managing this technology. When the computer is part of a national critical infrastructure, these operational records become essential, not only for troubleshooting or security alone, but for the integrity of the system itself as a component of the National Critical Infrastructure.

For the purposes of this document and ensuing discussion, two terms are defined to differentiate and clarify the evidentiary findings. *Election Data* is all information regarding Ballot Design, Ballot Marking, Electronic scanning of completed ballots, interpretation of the intention of each voter's choice, including human, machine generated or programatic adjudication in the event that the election system is unable to determine conclusively the correct vote input from any specific ballot, tabulation of the actual vote including the databases used to actually contain the raw vote totals, scanned ballot images and Voter Registration and Voter identification information associated with any specific election, as well as the actual vote totals. This includes a complete record of any realtime changes in databases resident in the cloud such as voter registration data. *Election-Related Data* includes all of the computer log and configuration data that document the complete configuration state and operation of the entire computer system and infrastructure upon which Election Software is executed, as well as the operating system of devices that store log and election data such as Network Attached Storage (NAS). Also included in Election-Related data are logs and configuration of network Routers, Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, and other network security devices, including VPNs and more².

Both Election Data AND Election-Related Data must be preserved as "Election Records" under the law, and this is broadly addressed in both the 2002 VSS and the EAC's successor versions of VVSG.

Securing computer systems is a non-trivial task. It involves a litany of processes, including, but not limited to:

- Engineering systems with a focus on security
- Building systems to meet published high-security standards and applicable regulations
- Patching systems to ensure that vulnerabilities are removed
- Securing networks to ensure highly controlled access
- Logging of all communications, processes, access, system modifications
- Auditing of systems and logs regularly to ensure ongoing compliance
- Adequate training and certification for engineers, administrators, and system users
- Adherence to Industry Best Practices, for example, emphasis on password strength and configured security and group policies

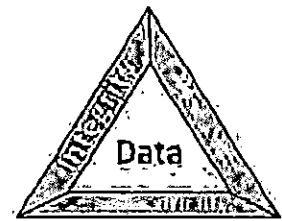
These, among other measures, will help to ensure what is known as the CIA triad. The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability, as follows:

² Log and configuration examination of not only the computer system(s) but also all network systems are critical to forensic examination. Compromise of any unrelated information (e.g. plain-text configuration data containing normally-encrypted passwords) can be easily prevented, so long as simple, quick forensic examiner and cyber professional industry standards are used to obfuscate private and sensitive data from the network device files.

Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity – guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity

Availability – ensuring timely and reliable access to and use of information



Failure in any of the three pillars can and generally will result in a compromise of the system. Failure in the integrity component can have dire consequences for public perception, election results, the future of our government and our country.

Industry-standard forensics analysis tools were applied to the forensic examination.

Information was forensically evaluated using backup images taken from a Mesa County Election server configured for DVS D-Suite 5.11-GO on Sunday, May 23, 2021, before its modification by Dominion Voting Systems and the Colorado Secretary of State to DVS D-Suite 5.13, and again on Wednesday, May 26, 2021, after the update had been applied. This server was the primary system that was used to process election data in Mesa County for the 2020 general election. The EMS server configuration and administrative standards were prepared by Dominion Voting Systems (DVS), running a combination of COTS and proprietary DVS software, and certified for use by the Colorado Secretary of State. Our conclusions include determining that this system not only failed to meet any reasonable standard or statutory requirement for cybersecurity but was also subject to removal of critical information (data destruction):

Our findings include serious irregularities that resulted in the loss of data integrity on the server, including election data and election-related data.

LEGAL REFERENCES

Several Federal and Colorado state legal standards apply to the preservation and definition of election records, applicable to the data generated by and resident on voting systems. Beginning with 52 USC §20701, retention and preservation of records and papers by officers of elections; deposit with custodian; penalty for violation, which states:

Every officer of election shall retain and preserve, for a period of twenty-two months from the date of any general, special, or primary election of which candidates for the office of President, Vice President, presidential elector, Member of the Senate, Member of the House of Representatives, or Resident Commissioner from the Commonwealth of Puerto Rico are voted for, all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election, except that, when required by law, such records and papers may be delivered to another officer of election and except that, if a State or the Commonwealth of Puerto Rico designates a custodian to retain and preserve these records and papers at a specified place, then such records and papers may be deposited with such custodian, and the duty to retain and preserve any record or paper so deposited shall devolve upon such custodian. Any officer of election or custodian who willfully fails to comply with this section shall be fined not more than \$1,000 or imprisoned not more than one year; or both.

In addition to 52 USC §20701, multiple sections of Colorado Revised Statutes (CRS) appear applicable, including:

CRS 1-5-601.5. Compliance with federal requirements (Effective until July 1, 2022)

All voting systems and voting equipment offered for sale on or after May 28, 2004, shall meet the voting systems standards that were promulgated in 2002 by the federal election commission. At his or her discretion, the secretary of state may require by rule that voting systems and voting equipment satisfy voting systems standards promulgated after January 1, 2008, by the federal election assistance commission as long

as such standards meet or exceed those promulgated in 2002 by the federal election commission. Subject to section 1-5-608.2, nothing in this section shall be construed to require any political subdivision to replace a voting system that is in use prior to May 28, 2004.

CRS 1-7-802. Preservation of election records

The designated election official shall be responsible for the preservation of any election records for a period of at least twenty-five months after the election or until time has expired for which the record would be needed in any contest proceedings, whichever is later. Unused ballots may be destroyed after the time for a challenge to the election has passed. If a federal candidate was on the ballot, the voted ballots and any other required election materials shall be kept for at least twenty-five months after the election.

1-13-716. Destroying, removing, or delaying delivery of election records

(1) No person shall willfully destroy, deface, or alter any ballot or any election records or willfully delay the delivery of any such ballots or election records, or take, carry away, conceal, or remove any ballot, ballot box, or election records from the polling location or drop-off location or from the possession of a person authorized by law to have the custody thereof, or aid, counsel, procure, advise, or assist any person to do any of the aforesaid acts.

(2) No election official who has undertaken to deliver the official ballots and election records to the county clerk and recorder shall neglect or refuse to do so within the time prescribed by law or shall fail to account fully for all official ballots and other records in his charge. Informality in the delivery of the ballots and election records shall not invalidate the vote of any precinct if such records are delivered prior to the canvassing of the votes by the county board of canvassers.

(3) Any person who violates any provision of this section is guilty of a misdemeanor and, upon conviction thereof, shall be punished as provided in section 1-13-111.

And several sections of the Code of Colorado Regulations appear applicable, including:

8 CCR 1505-1, Rule 21, 21.4.2: All voting systems must meet the requirements of the 2002 Voting Systems Standards, parts 5 – 7 of article 5 of title 1, CRS, as amended, and this Rule 21.

FORENSIC EXAMINATION AND ANALYSIS REPORT

FORENSIC ANALYSIS

SYSTEM IDENTIFICATION

The server that was analyzed is capable of operating on a small local area network (LAN). The network consists of several systems, including servers and workstations running in a non-virtualized environment. The server that we evaluated was named EMSSERVER. It is running the Microsoft Windows Server 2016 Standard operating system.

The forensic evaluation and reviews were based upon a forensic image archive collected from the Mesa County Dominion EMS Server. The Before and After forensic images were collected from the same server and same hard drive, as documented below, from the actual acquisition. The serial number of the hard drive shown in each collection data set verifies the data origin to be the same physical device.

Figure 1 – EMS Server (5.11-CO) Image Attributes Before

```
Created By AccessData® FTK® Imager 4.2.0.13

Case Information:
Acquired using: ADI4.2.0.13
Case Number: 052321
Evidence Number: 00003
Unique description: EMSSERVER

-----

Information for F:\EMSSERVER\EMSSERVER:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 121,534
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 1,952,448,512
[Physical Drive Information]
Drive Model: DELL PERC H730 Adp SCSI Disk Device
Drive Serial Number: 00222e64128c016e1d004fc54220844a
Drive Interface Type: SCSI
Removable drive: False
Source data size: 953344 MB
Sector count: 1952448512
[Computed Hashes]
MD5 checksum: 3d7cf05ca6e42db765bf5c15220c097d
SHA1 checksum: eab06a7ea23586de2746b9142461717e075f5c9f

Image Information:
Acquisition finished: Sun May 23 2021
Segment list:
F:\EMSSERVER\EMSSERVER.E01
```

Figure 2 - EMS Server (5.13) Image Attributes After

Created By AccessData® FTK® Imager 4.2.0.13

Case Information:

Acquired using: ADI4.2.0.13
Case Number: 052621
Evidence Number: 00002
Unique description: EMSSERVER_v2

Information for E:\Mesa\EMSSERVER_v2:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 121,534
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 1,952,448,512

[Physical Drive Information]

Drive Model: DELL PERC H730 Adp SCSI Disk Device

Drive Serial Number: 00222e64128c016e1d004fc54220844a

Drive Interface Type: SCSI

Removable drive: False

Source data size: 953344 MB

Sector count: 1952448512

[Computed Hashes]

MD5 checksum: 52861d5a7750ab535a9d5f7277469c10

SHA1 checksum: 1bf8f22edb37f72bb29428a591046a1f64279a3f

Image Information:

Acquisition finished: Wed May 26 2021

Segment list:

E:\Mesa\EMSSERVER_v2.E01

Two backup images were obtained, using forensic imaging methods, from the Dominion Voting Systems (DVS) Democracy Suite (D-Suite) Election Management System (EMS) Standard Server in Mesa County, Colorado. The first image was made of that EMS Standard Server in the D-Suite 5.11-CO version configuration, as used in the November, 2020 election on May 23, 2021. The second image was of the configuration of the EMS Standard Server in the D-Suite 5.13 version configuration, following the modification of the EMS Standard Server by a combined team of Dominion Voting System vendor personnel and Colorado Secretary of State (SecState) staff, on May 26, 2021. A forensic image (forensic copy) is a bit-by-bit, sector-by-sector duplicate of a physical storage device using specialized hardware and software; it is a much more comprehensive representation of the state and configuration of the imaged system than could be obtained using simple file backup methods. The images include all files, folders, and unallocated, free, and slack space. These forensic images include not only all the files visible to the server operating system but also deleted files and fragments of files left in the slack and free space but every digital bit of data present on the storage medium, in this case, a SCSI hard disk. When forensic images are acquired, a hash function, also known as a Message Digest, is computed. This hash can be used at any time to validate the integrity of the image to ensure that it has not been edited, modified, or changed in any way. The hash function result from the acquisition of data appears in the text above but also appears inside each respective archive and authenticates the data by demonstrating that it has not changed since it was acquired.

These two images were evaluated to gather technical information, including the integrity of the data stored on the system. No effort was made to reverse-design, de-compile or reverse-engineer the Dominion software. Configuration, which is relevant to the operation of the system, was examined to determine whether improper settings could allow undesirable results and were found to contain such errors. Results relevant to this investigation are documented below. Additional supporting documentation can be found in the appendixes. They include directory listings for many of the directories seen in the screenshots and contain complete filenames, full path names where the files are located, and file hashes.

We have included screenshots that can be used to review and verify these findings. These screenshots were obtained from the forensic images of the Dominion server.

AUTHENTICITY AND CHAIN OF CUSTODY

Digital chain of custody is the record of preservation of digital evidence from collection to presentation in the court of law. This is an essential part of the digital investigation process. The chain of custody is probative that the digital evidence presented to the court remains as originally collected, without tampering. The two images analyzed in this report were obtained through AccessData FTK Imager 4.2.0.13. The serial number on the EMS Server drive on both images match, thus establishing that both images were taken from the same physical drive. I have reviewed the documented chain of custody for both images and have determined that the chain of custody is complete from the forensic operator utilizing FTK Imager through the source from which I directly received these images. (Because of the pending civil litigation and criminal investigation, the written documentation remains in the custody of counsel for later introduction in court proceedings and thus cannot be released as part of this report.) Further confirmation that these are genuine images from the Mesa County EMS Server has been provided by the Colorado Secretary of State's office. See:

<https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2021/PR20210817MesaCounty.html>

FINDINGS

Overview of System Data Sources

Figure 3 – EMS Server (5.11-CO) System Data Sources Before

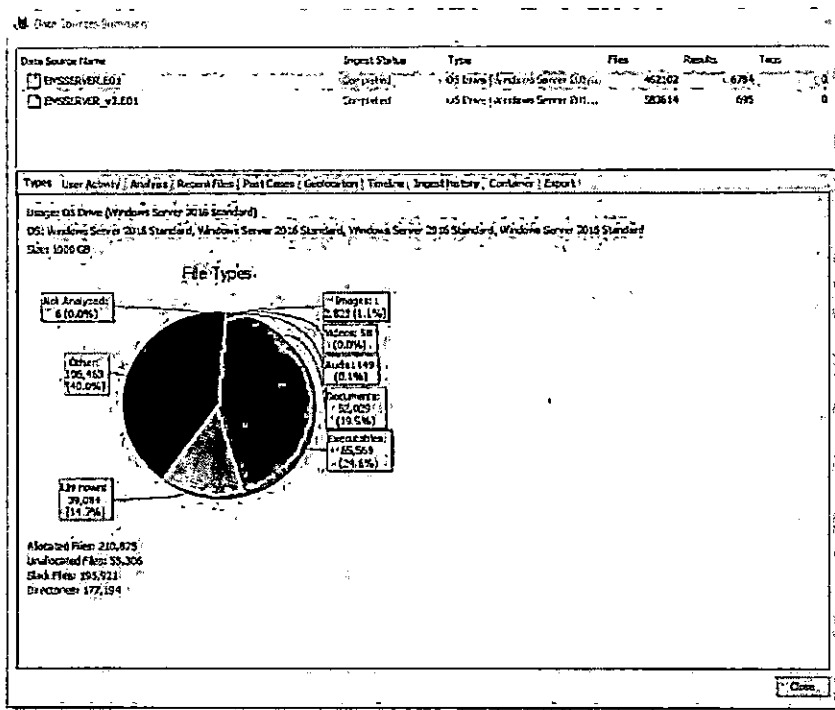
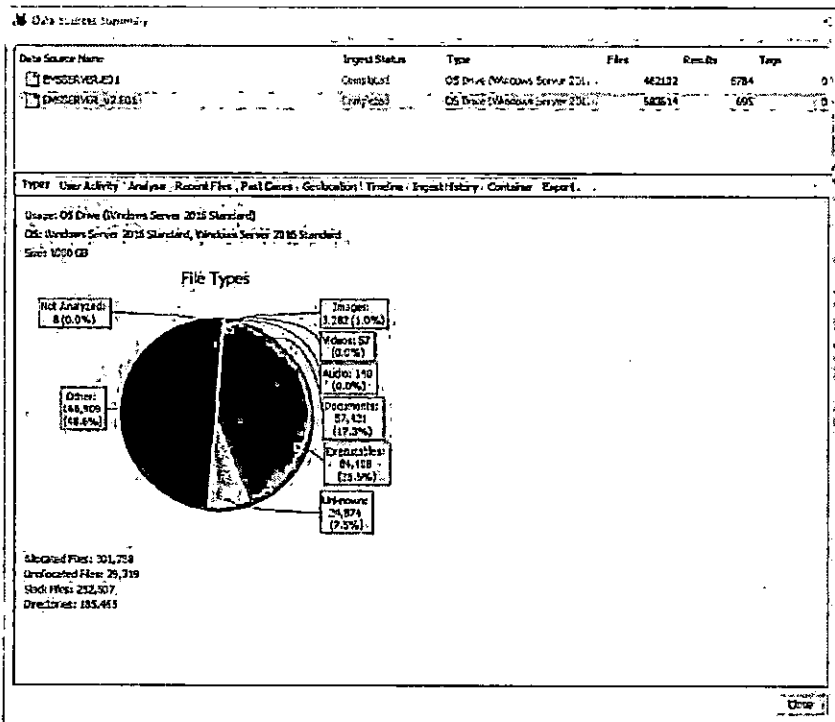


Figure 4 - EMS Server (5.13) System Data Sources After



Server Disk Partition Structure Overwritten

Purpose: The disk partition structure is the structure of how the hard drive is divided up.

Figure 5 - EMSSERVER (5.11-CO) Disk Partition Structure Before

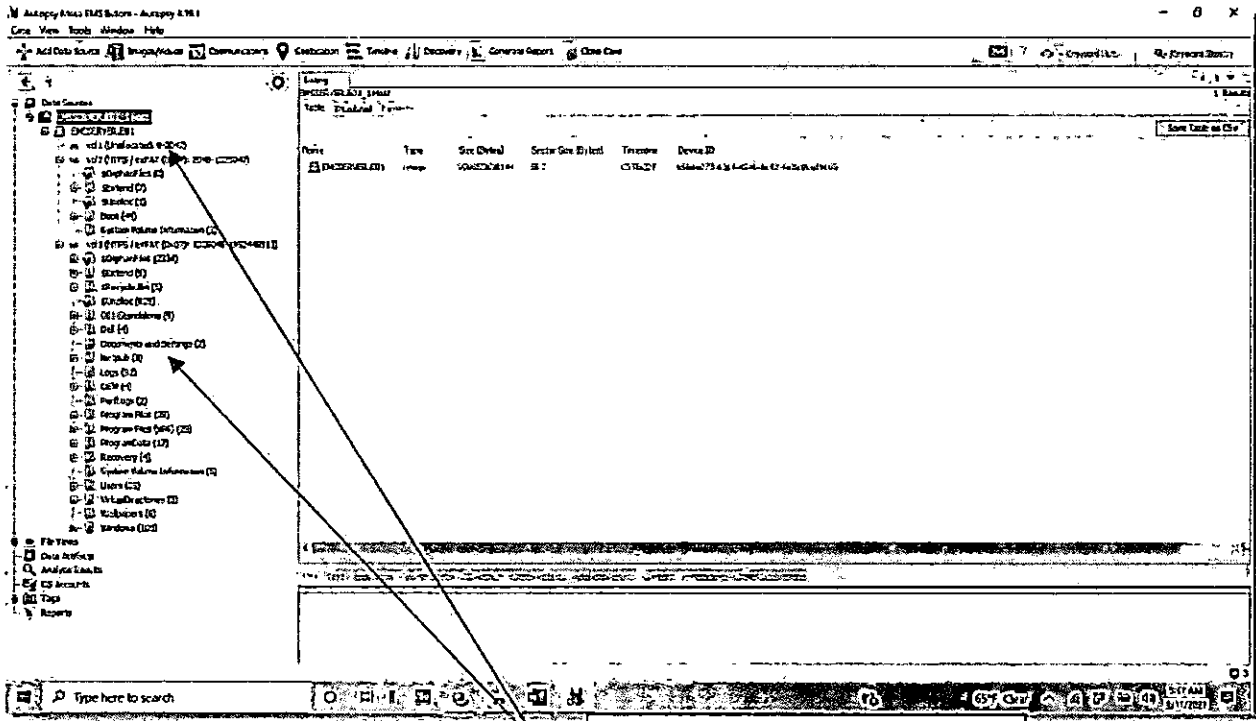


Figure 6 - EMSSERVER (5.13) Disk Partition Structure After

Note Changes in Disk Volumes and Directory Structures

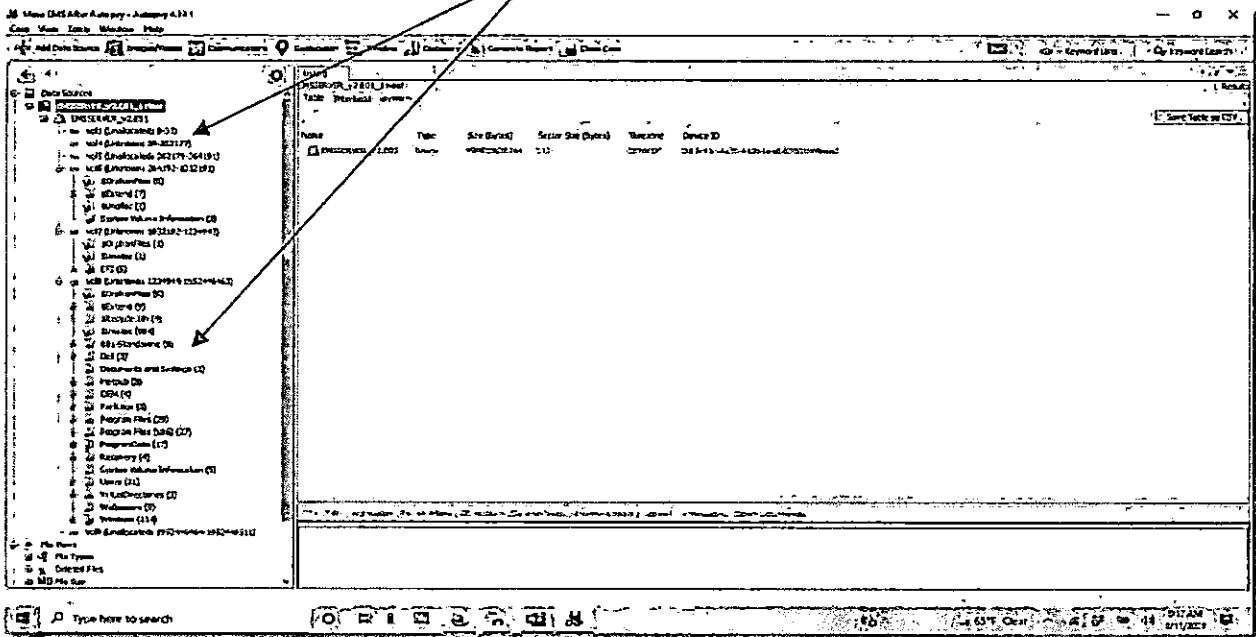
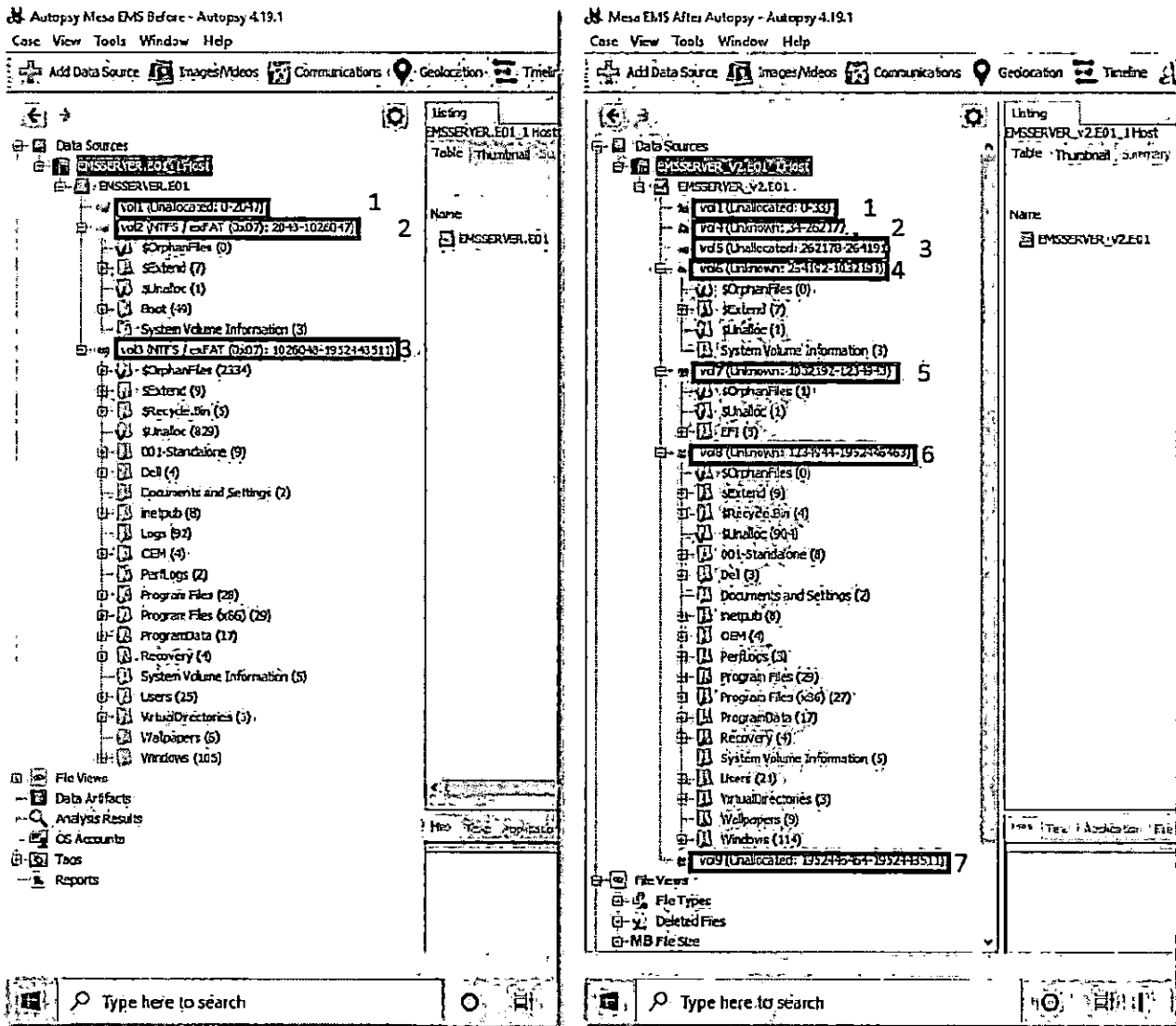


Figure 7 - Server Disk Partition and Directory Changes



Before Dominion Update

After Dominion Update

Computer hard disk drives are data storage devices that must be prepared before use – specifically, they must be partitioned into logical disk volumes and then formatted. Partitioning a hard disk drive is the equivalent of scoring horizontal and vertical rule lines onto blank paper, and then numbering each line, preparing that paper for the orderly recording and look-up of information. A disk is partitioned to organize information into sets of related data. A partition creates a logical drive, C:, D:, E:, etc., that the Master Boot Record (MBR) or Globally Unique Identifier (GUID) Partition Table, which are like maps of the partitioned and formatted memory storage locations on the hard drive, can then use to write and read stored data.

Creation of such a partition, if previous partitions are not preserved, destroys the “map” of underlying data and data locations when the partition is formatted. The previous partition data is then only recoverable by forensic techniques, and is vulnerable to complete destruction if overwritten by data stored according to the new partition “map.” Note that in the before image above, each disk partition (labeled “volX,” e.g. “vol1,” for “volume”) is identified together with the addresses of the beginning block and ending block for each volume.

By comparing the images, it is evident that the disk was re-partitioned, reformatted, and the previous data map completely destroyed by overwriting it with new data, rendering the prior data (mostly) unrecoverable.

Forensic examination of the system can reveal remnants of deleted data. When a computer deletes a file, it does not erase the data; it merely changes the first character of the filename to a non-printable character recognized by software that accesses the disk. This first character tells the operating system to no longer display the file as it is marked as a deleted file, and the space occupied by the disk is marked as reusable.

Each block on the disk is the smallest unit of disk space that can be used. The size of all blocks on the disk are determined when the disk is formatted. The smallest disk block size in common use is 512 bytes. Even if a file only occupies 50 bytes of disk space, the entire 512 byte block is marked as "in use".

If a file of 500 bytes is written to the disk, it occupies one block of disk space, with the last 12 bytes (on a newly formatted disk) each containing the numeric value zero (0). If this file is then deleted, and a file of 50 bytes is written to the same disk block, the first 50 bytes of the block contain the new file, and the next remaining 450 bytes of the disk block contain the data from the deleted file that previously occupied the disk block (followed by the 12 null (0) bytes of data). This data remnant is referred to as "File Slack Space" and is defined as any previous remnant data that remains on the disk and is not accessible via the operating system nor allocated as an accessible file.

Special forensic software is required to access file slack space, and the data it contains are partial remnants of previous system data. This data may be of use in forensic investigation, and forensic tools often identify it. File Slack is identified here for clarity and better understanding of these data.

Website Server Log Files Missing

Figure 8 - EMS Server (5.11-CO) Web Server Log Files Before

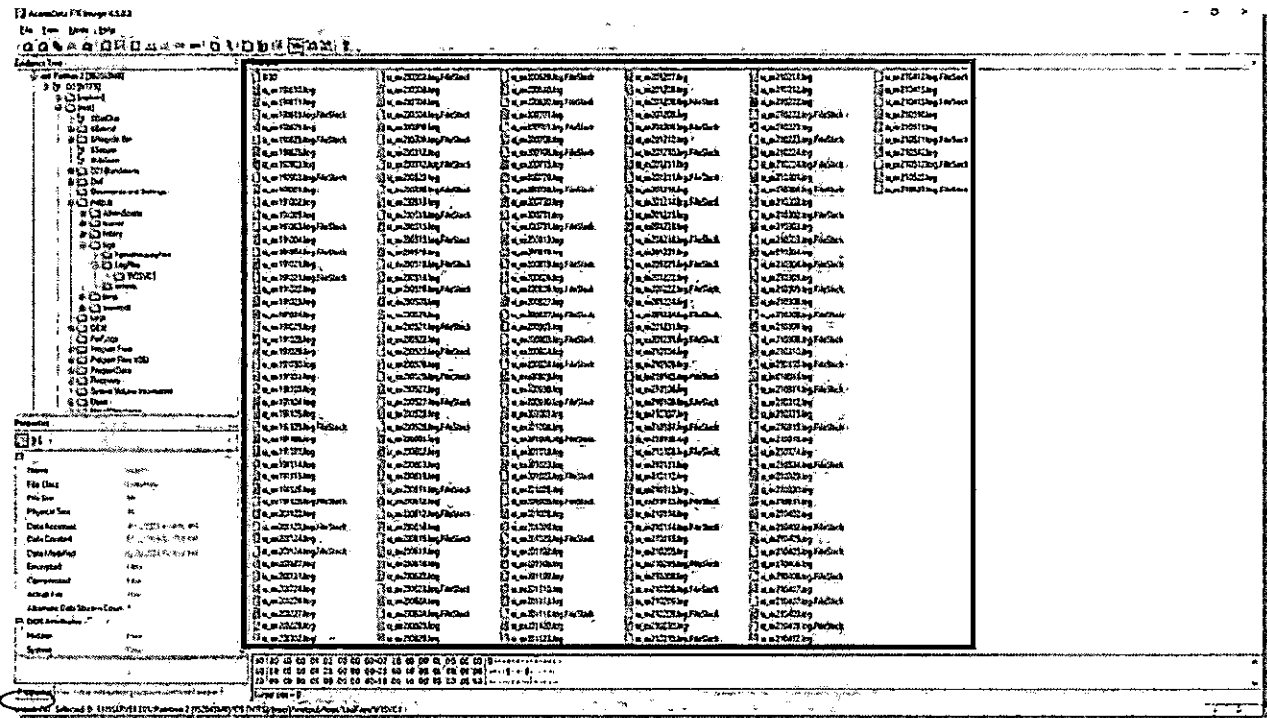
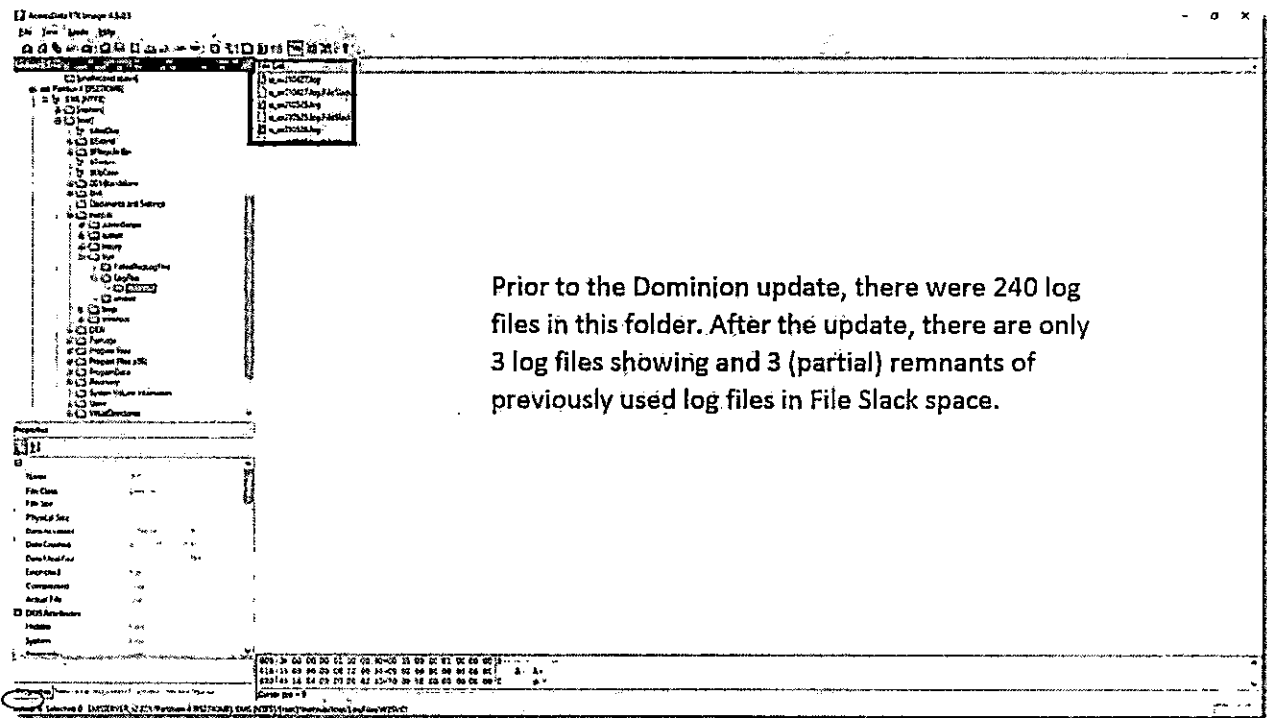


Figure 9 - EMS Server (5.13) Web Server Log Files After



Prior to the Dominion update, there were 240 log files in this folder. After the update, there are only 3 log files showing and 3 (partial) remnants of previously used log files in File Slack space.

A web server provides information to external web clients (via "web browser" software) using the HyperText Transfer Protocol (HTTP). This information can include both read and write access to databases and static presentation of information.

Some software system designs utilize an Ethernet network interface that is essentially an internal connection to itself, known as a *loopback* interface. Thus the presence of a Web Server, by itself, does not indicate a connection to an external ethernet interface. However, such an external connection may be indicated by the data within web server logs, which are stored by default in Microsoft operating systems with Microsoft Internet Information Services (IIS) installed, in a "logs" subfolder to the "inetpub" folder. That log data would include information regarding what web pages and data were accessed and whether it was accessed from within the server (loopback) or via an external network connection.

In these before and after views of the same web server directories, it is clear that the web server logs have been destroyed by or during the Dominion/CO Secretary of State DVS D-Suite 5.13 modification.

This log data is required to verify that the election system was not accessed by an external, unauthorized device, but due to the specific and unusual installation method for a critical computing system, chosen by Dominion Voting Systems and endorsed by the CO Secretary of State, these critical data files with election-related data have clearly been destroyed on the Mesa County EMS Standard Server.

Server Microsoft SQL Server Installation Log Files Missing

Purpose: The Database Management System that is used to hold actual ELECTION DATA – votes from each ballot. These log files contain information detailing the installation events of SQL Server.

Figure 10 - EMS Server (5.11-CO) MS SQL Server Installation Log Files Before

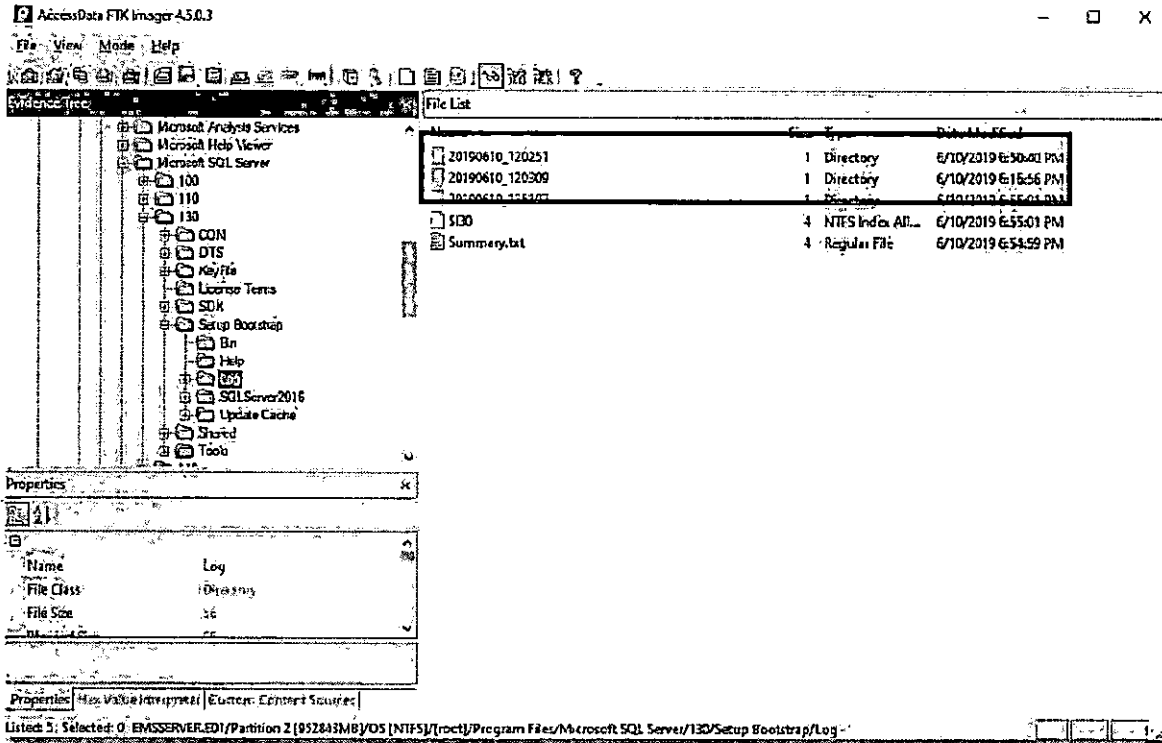
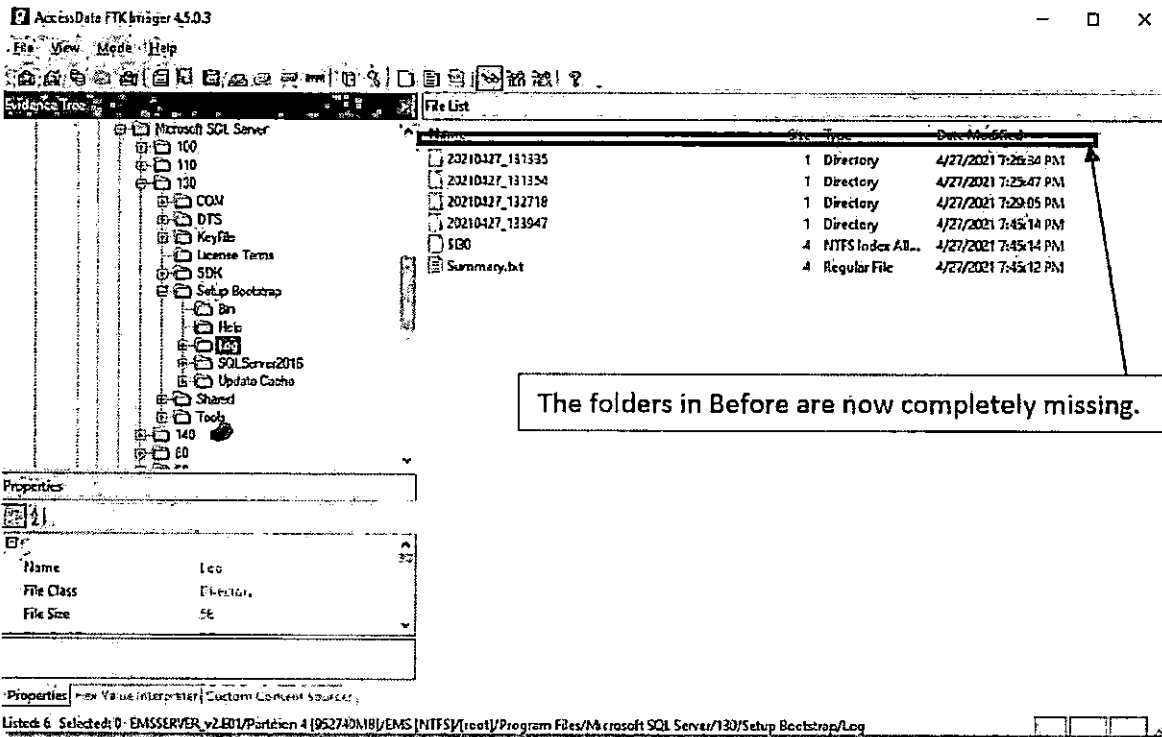


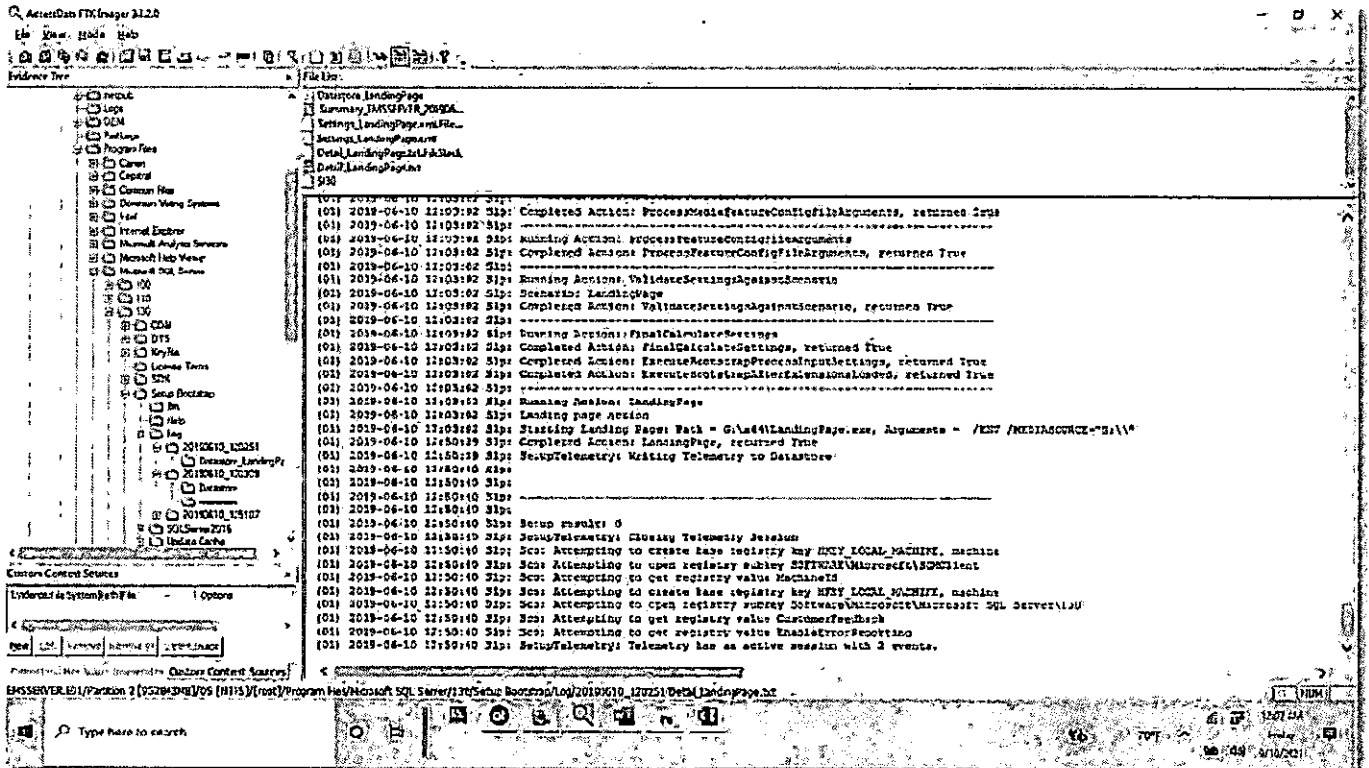
Figure 11 - EMS Server (5.13) MS SQL Server Installation Log Files After



These log files were created by installing the SQL Server Database Management System software and contain data regarding the Initial installation of the software. In a full forensic investigation, these data are part of the information that investigators require to determine a baseline from which can be determined what changes were made, by whom, when the changes were made, and much more on a system with properly configured log recording. Therefore, these data are Election Related as they document not only the configuration but its changes and are relevant to the Integrity of the election.

Figure 12 is an example of log content from the initial software setup. It tells us what (Microsoft) software executes, where data is stored (the G: drive), and it shows us what Registry values have been set during the installation. These are valuable should an investigation of an illegal computer intrusion occur, as they provide a record of the initial configuration during such an investigation.

Figure 12 - Example of Log File Content from EMS Server (5.11-CO) Before



Server Microsoft SQL Server Log Files Missing

Purpose: These log files keep track of events that occur within the SQL Server that manages the election databases.

Figure 13 - EMS Server (5.11-CO) SQL Server Log Files Before

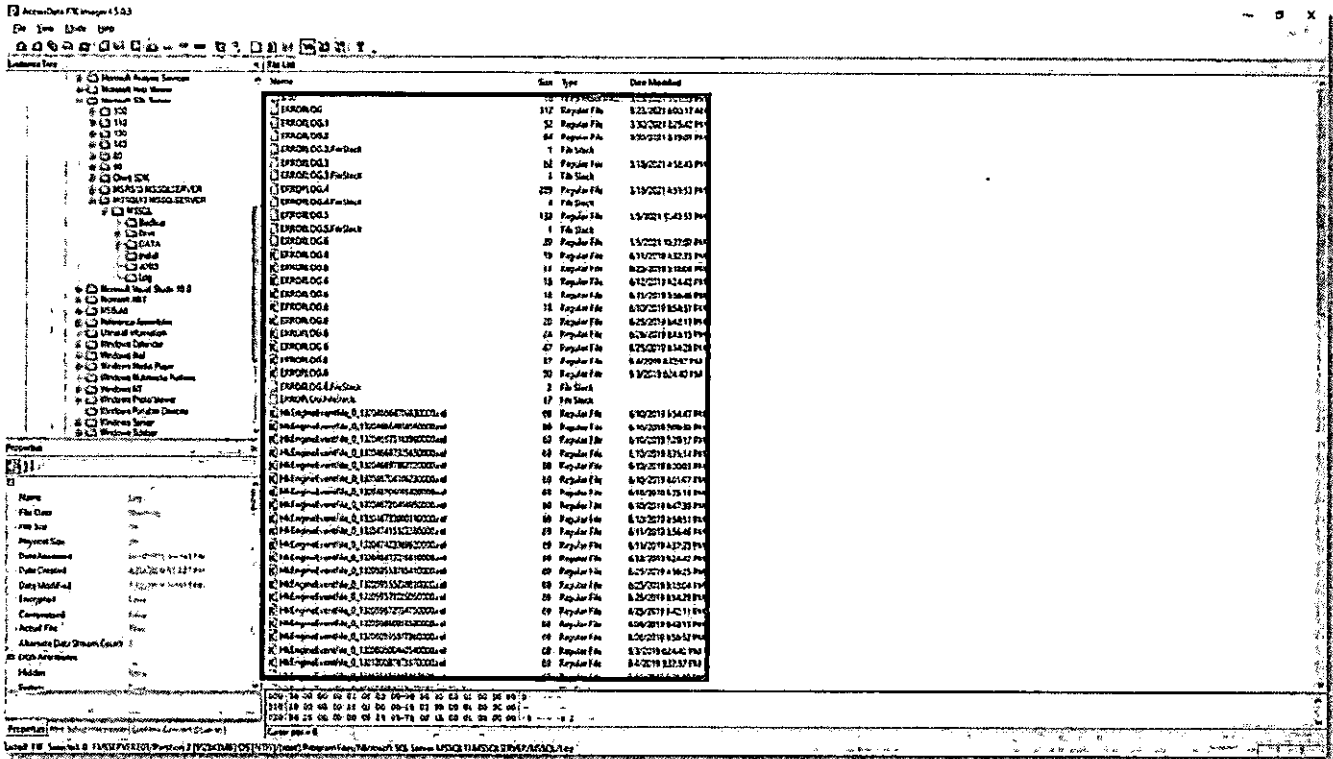
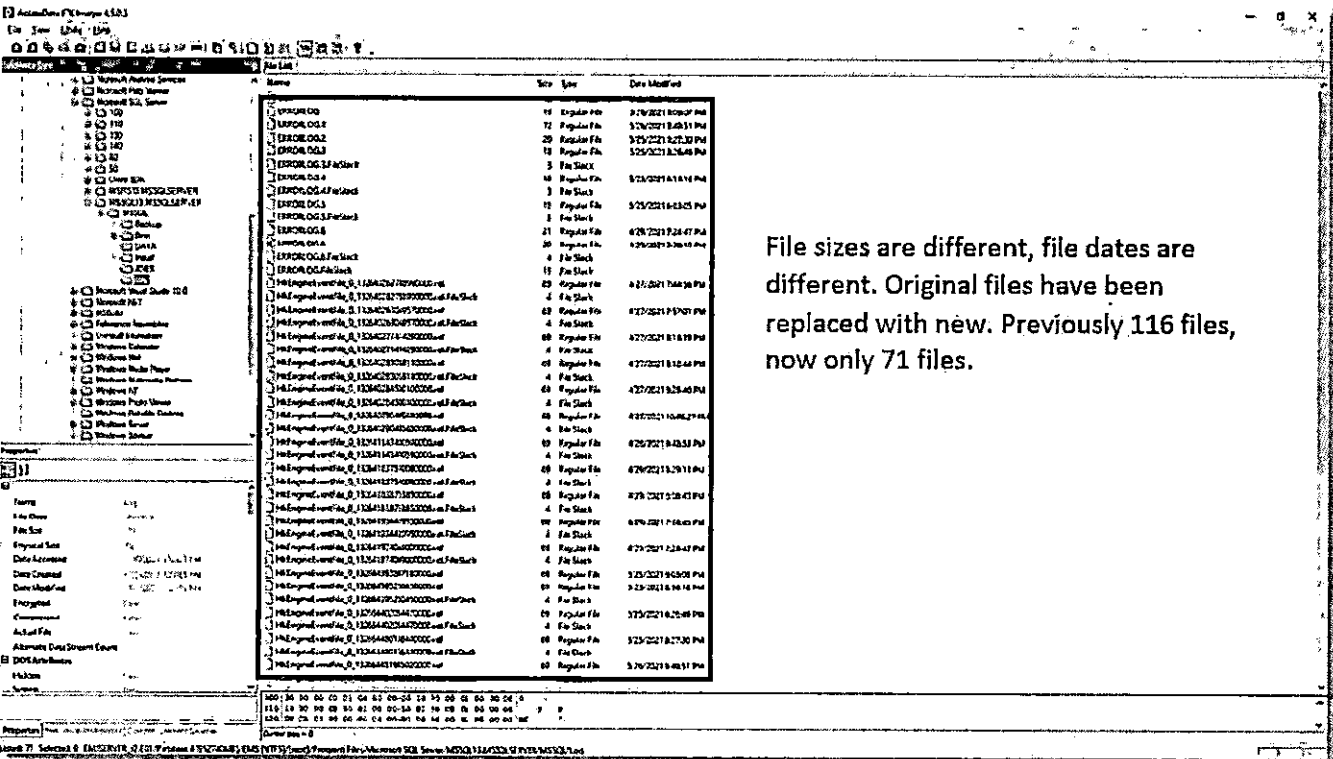


Figure 14 - EMS Server (5.13) SQL Server Log Files After



EMS Server Dell Server Updates Missing

Purpose: These log files track installation of updates made to the various components of the servers, including updates to software for a remote-access card.

Figure 15 - EMS Server (5.11-CO) Dell Server Update Files Before

Name	Size	Type	Date Modified
BIOS			
BIOS_Flash_Package_2.11.11.11.11	4	NTFS Index Attr.	6/25/2016 1:53:17 PM
BIOS_Flash_Package_2.11.11.11.11.11	63	Regular File	6/25/2016 12:04:56 PM
BIOS_Flash_Package_2.11.11.11.11.11	4	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	17	Regular File	6/25/2016 8:06:58 PM
BIOS_Flash_Package_2.11.11.11.11.11	1	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	133	Regular File	6/25/2016 7:22:56 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	53	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	4	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	73	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	11	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	40	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	42	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	203	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	203	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	26	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	17	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	

Figure 16 - EMS Server (5.13) Dell Server Update Files After

Sizes, Dates/Times are different. These Log Files have been replaced with different files.

Name	Size	Type	Date Modified
BIOS			
BIOS_Flash_Package_2.11.11.11.11.11	4	NTFS Index Attr.	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	17	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	14	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	1	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	133	Regular File	6/25/2016 7:22:56 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	53	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	4	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	73	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	11	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	40	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	42	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	203	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	203	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	
BIOS_Flash_Package_2.11.11.11.11.11	26	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	17	Regular File	6/25/2016 6:08:01 PM
BIOS_Flash_Package_2.11.11.11.11.11	2	File Stub	

Several log files of great importance to an investigation are shown in Figure 16. The SAS RAID firmware and drivers logs tell us about the functionality of hard disk controllers (RAID is an acronym for Redundant Array of Independent Disks) and about this storage redundancy's physical capability. Network Firmware logs tell us which hardware devices were updated with new firmware, and the version allows us to trace back to its network (and possibly Internet) functionality. The application of iDRAC controller firmware may indicate the presence of a special hardware controller intended to permit complete remote control of the computer system. This iDRAC controller is often used when a data center must be located an inconvenient distance away from its owner and/or operators, or for example, when such a computer might be physically located at an Internet Service Provider's secure data center. The iDRAC controller permits a remote user to remotely turn on the power to the server, reboot it, access administrative control functions, and make changes to the server, *OUTSIDE THE CONTROL, or even the awareness, of the local computer operator and its operating system.* Among the changes possible via an iDRAC are changes to the BIOS (Basic I/O System) including those firmware settings that include the computer Clock, boot device order, which disks or other data storage devices are used to boot the computer, and some other computer capabilities.

Take note of what files remain following the update.

Not only are the files in an entirely different directory, but the file modification dates have changed, and more importantly, these logs are for DIFFERENT versions of the software, and the previous logs have been overwritten.

Physical examination of the EMS computer system is required to verify the presence or absence of an iDRAC controller, however it is highly irregular for update software to install updates to software for a hardware device that has not been installed.

Server 'Administrator' WebCache Log Files Overwritten

Purpose: These log files store information about websites visited, files opened, etc.

Figure 17 - EMS Server (5.11-CO) Administrator WebCache Log Files Before

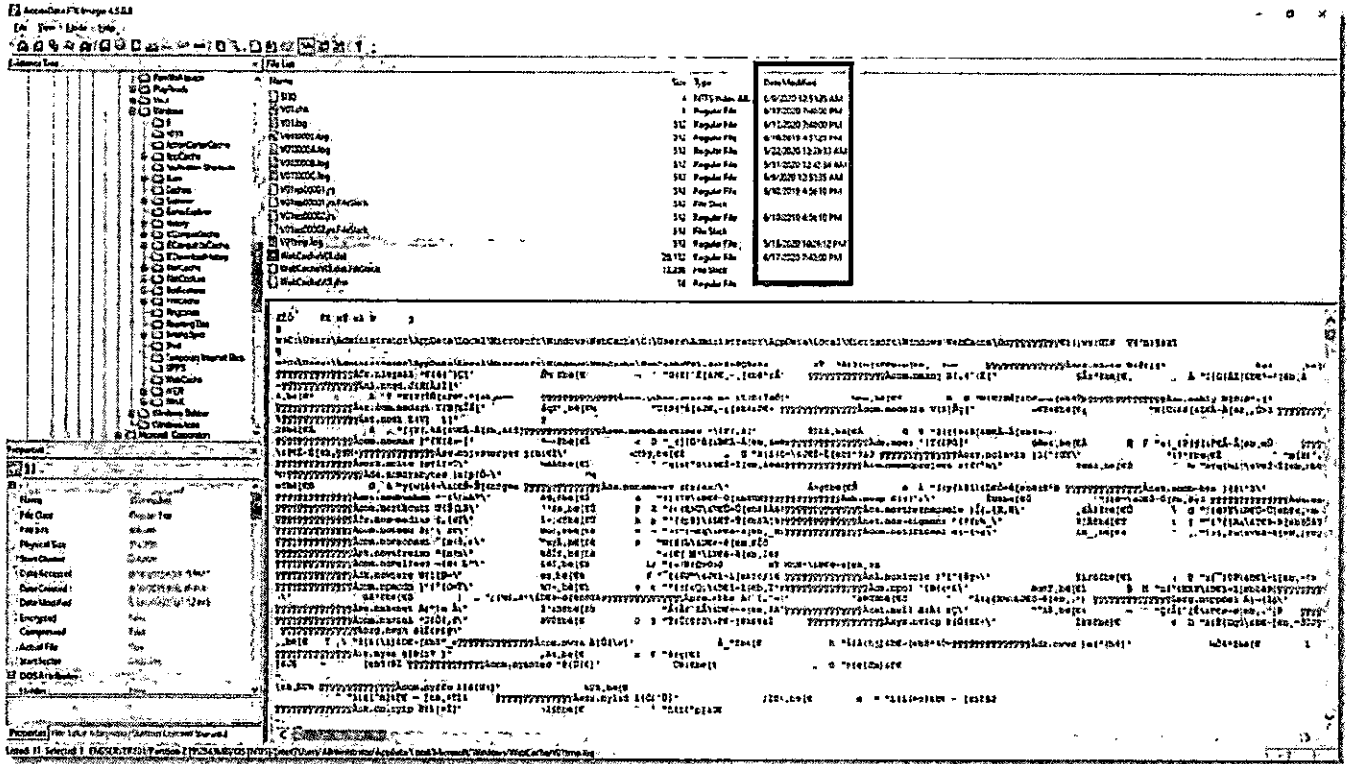
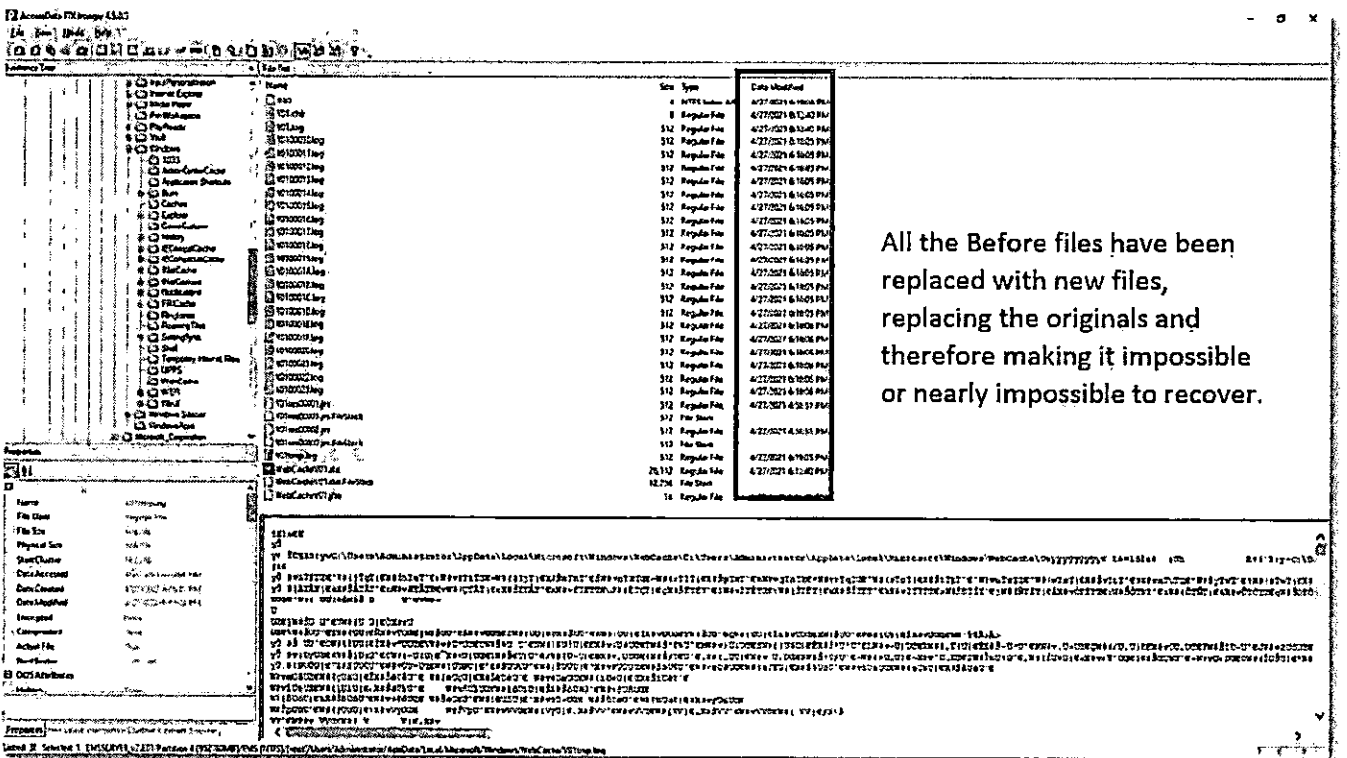


Figure 18 - EMS Server (5.13) Administrator WebCache Log Files After



All the Before files have been replaced with new files, replacing the originals and therefore making it impossible or nearly impossible to recover.

Server 'emsadmin' WebCache Log Files Overwritten

Purpose: These log files store information about websites visited, files opened, etc.

Figure 19 - EMS Server (5.11-CO) "emsadmin" WebCache Log Files Before

Name	Date Modified
WebCache01.log	5/23/2011 10:28:30 PM
WebCache02.log	5/23/2011 10:28:30 PM
WebCache03.log	5/23/2011 10:28:30 PM
WebCache04.log	5/23/2011 10:28:30 PM
WebCache05.log	5/23/2011 10:28:30 PM
WebCache06.log	5/23/2011 10:28:30 PM
WebCache07.log	5/23/2011 10:28:30 PM
WebCache08.log	5/23/2011 10:28:30 PM
WebCache09.log	5/23/2011 10:28:30 PM
WebCache10.log	5/23/2011 10:28:30 PM
WebCache11.log	5/23/2011 10:28:30 PM
WebCache12.log	5/23/2011 10:28:30 PM
WebCache13.log	5/23/2011 10:28:30 PM

Figure 20 - EMS Server (5.13) "emsadmin" WebCache Log Files After

The WebCache log files have been overwritten. IF the computer has been used on the Internet or with ANY webserver (even one on the local network, including this computer's OWN webserver), these WebCache files indicate the connections that were sought, as well as files that were opened. These may provide *critical* evidence that the system has been connected to a network, including networks that have access to the Internet. THESE ARE NOT the same files in the before and after images. They have been deleted and replaced.

Here is a small subset of some of the information that was found on the Before image in these WebCache log files::

Figure 21 - EMS Server (5.11-CO) Webcache Log File Content Before

EntryId	ContainerId	Url	AccessedTime
1	15	:2020060820200615: DVSAdministrator@:Host: This PC	13236818938265280
2	15	:2020060820200615: DVSAdministrator@file:///C:/Users/Administrator/Desktop/DVS%20Adjudication%20%20Key.pfx	132368189382821518

For instance, the above log file entry seems to show a DVS Adjudication Encryption Key was accessed, where it was stored and accessed from, and when it was accessed:

Figure 22 - EMS Server (5.11-CO) Webcache Log File Content Before - II

EntryId	ContainerId	Url	AccessedTime
1	18	:2021051820210519: emsadmin@file:///P:/Logs	132658341190420467
2	18	:2021051820210519: emsadmin@:Host: This PC	132658341190576330
3	18	:2021051820210519: emsadmin@file:///P/	132658341190732829
4	18	:2021051820210519: emsadmin@file:///F:/Logs/5_18_21.evtx	132658341410603691
5	18	:2021051820210519: emsadmin@file://emsserver/nas/2020%20Mes%20County%20General/Results/Tabulator/00004/Batch2003/1_1_4_2003_DETAIL.DVD.txt	132658342689478943
6	18	:2021051820210519: emsadmin@:Host: emsserver	132658342689478943
7	18	:2021051820210519: emsadmin@file://emsserver/nas/2020%20Mes%20County%20General/Results/Tabulator/00004/Batch2003/Images/00004_02003_000001.tif	132658342760262058

In addition, the above log file entry seems to show several interesting files (a windows 'evtx' log file being opened from an external attached USB flash drive, and a ballot detail file and even a ballot image from Batch 2003 being opened from a Network Attached Storage device)

Without a forensic Before image prior to a Dominion 'Update', this type of potentially critically-important forensic information could be, and likely would be, lost forever.

Server SQL Server Management Studio (SSMS) Log Files Overwritten

Purpose: These log files track the installation of the SQL Server Management Studio, which is used to get into the back-end of the election databases.

Figure 23 - EMS Server (5.11-CO) SSMS Log Files Before

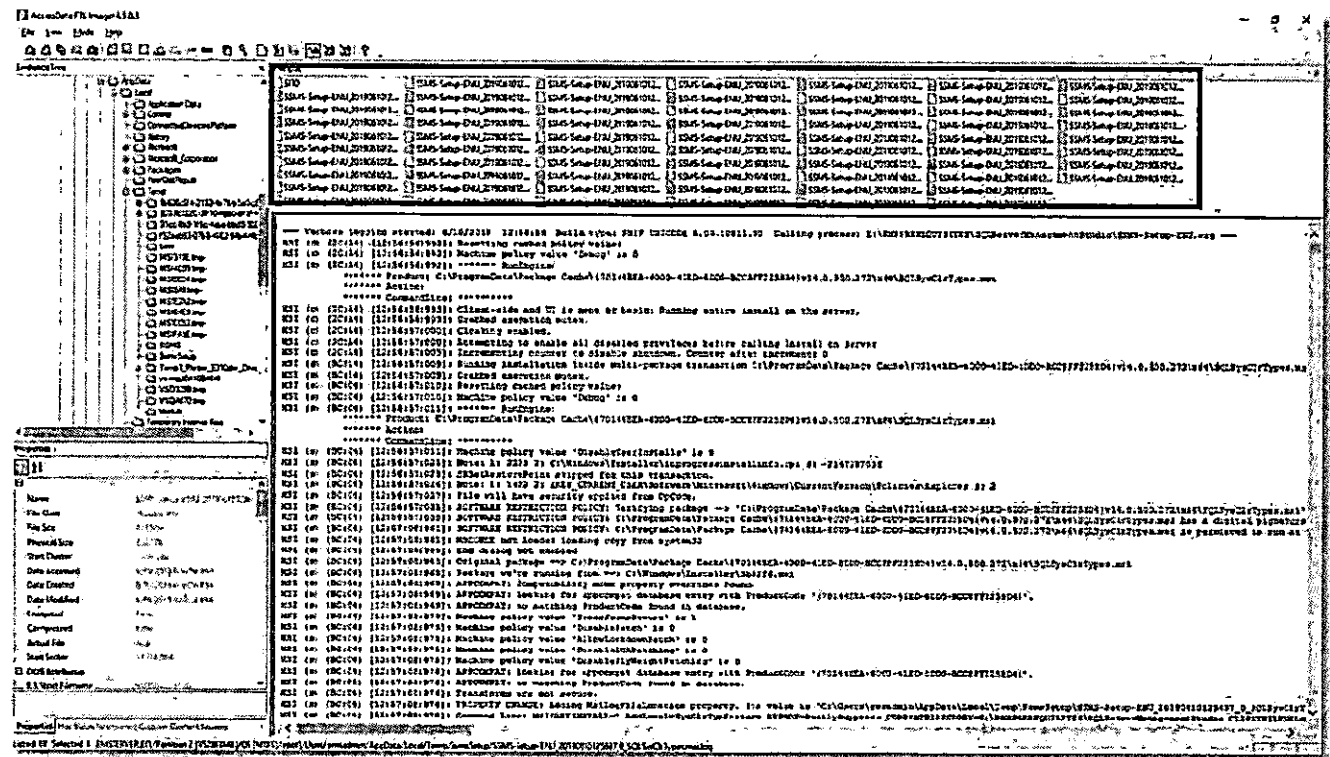
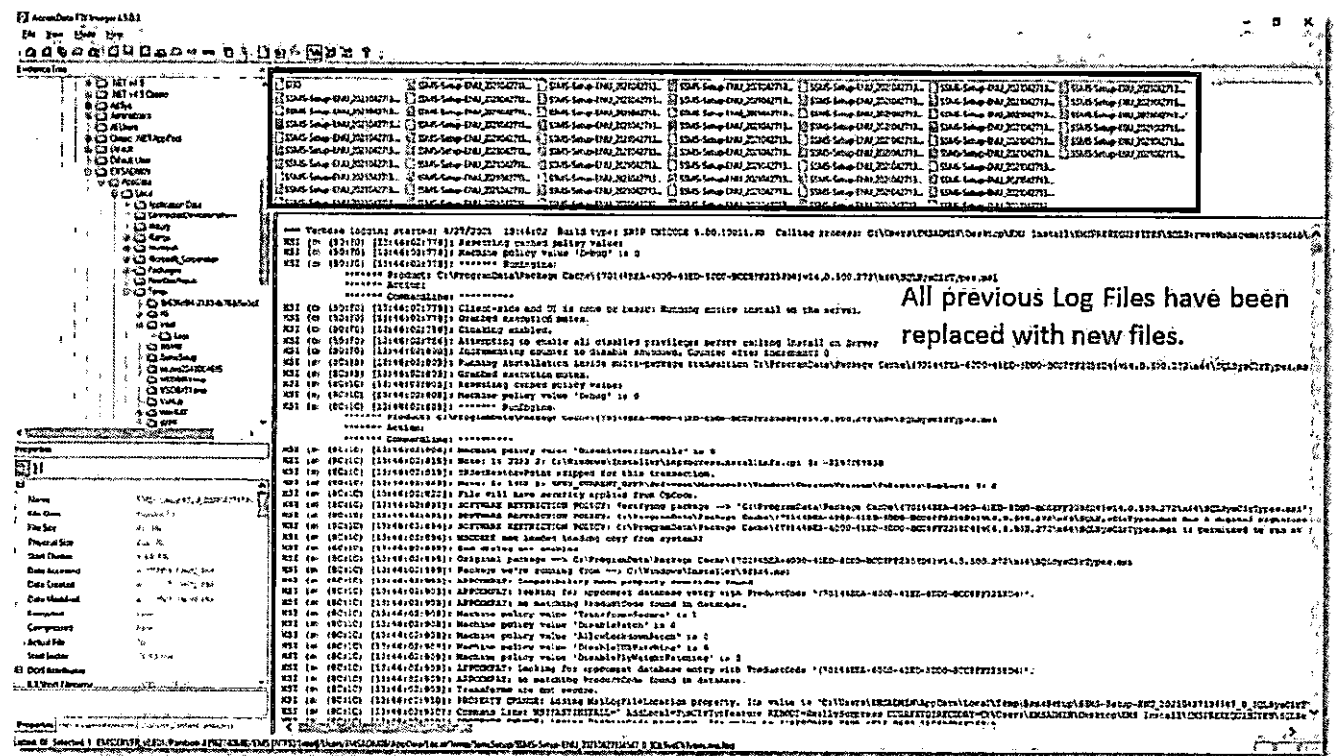


Figure 24 - EMS Server (5.13) SSMS Log Files After



Server CBS Log Files Overwritten

Purpose: These Log Files contain detailed information about installed updates. They could contain evidence of changes to the server that would cause decertification of the system.

Figure 25 - EMS Server (5.11-CO) CBS Log Files Before

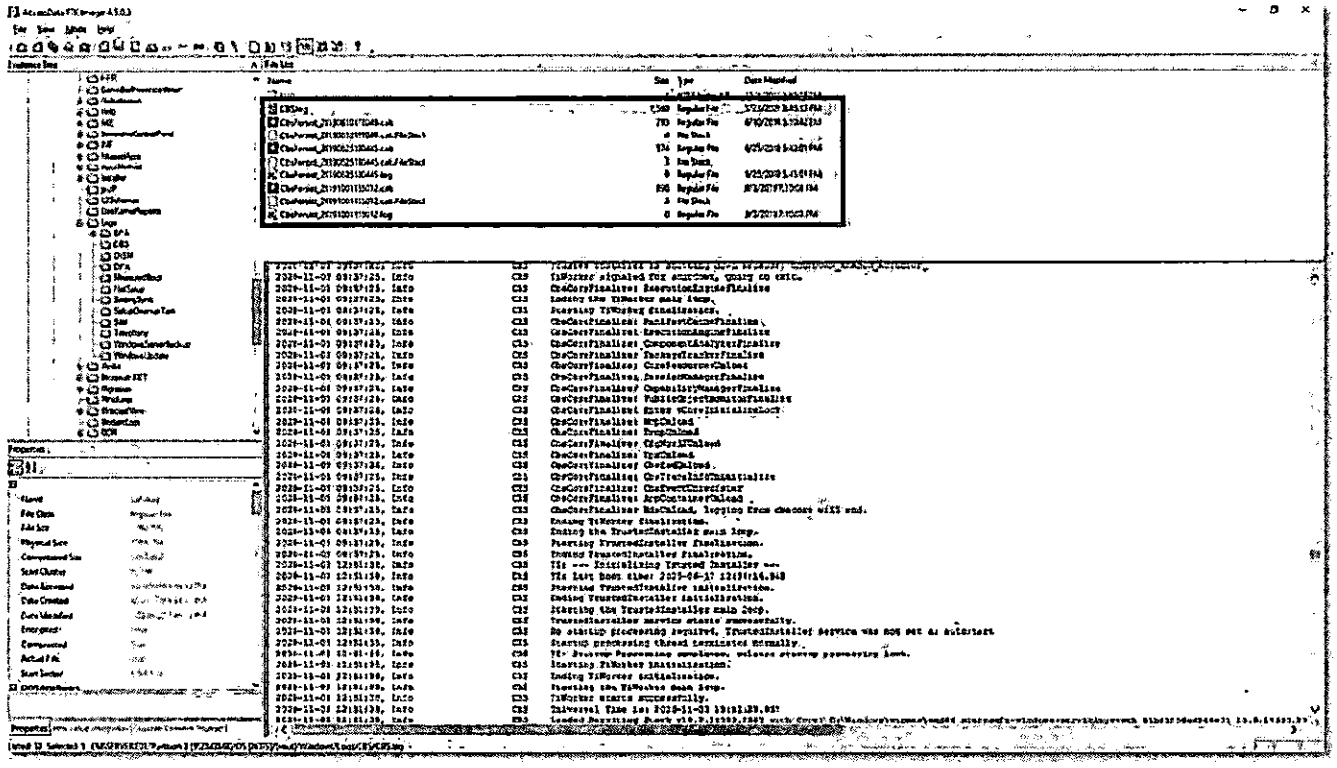
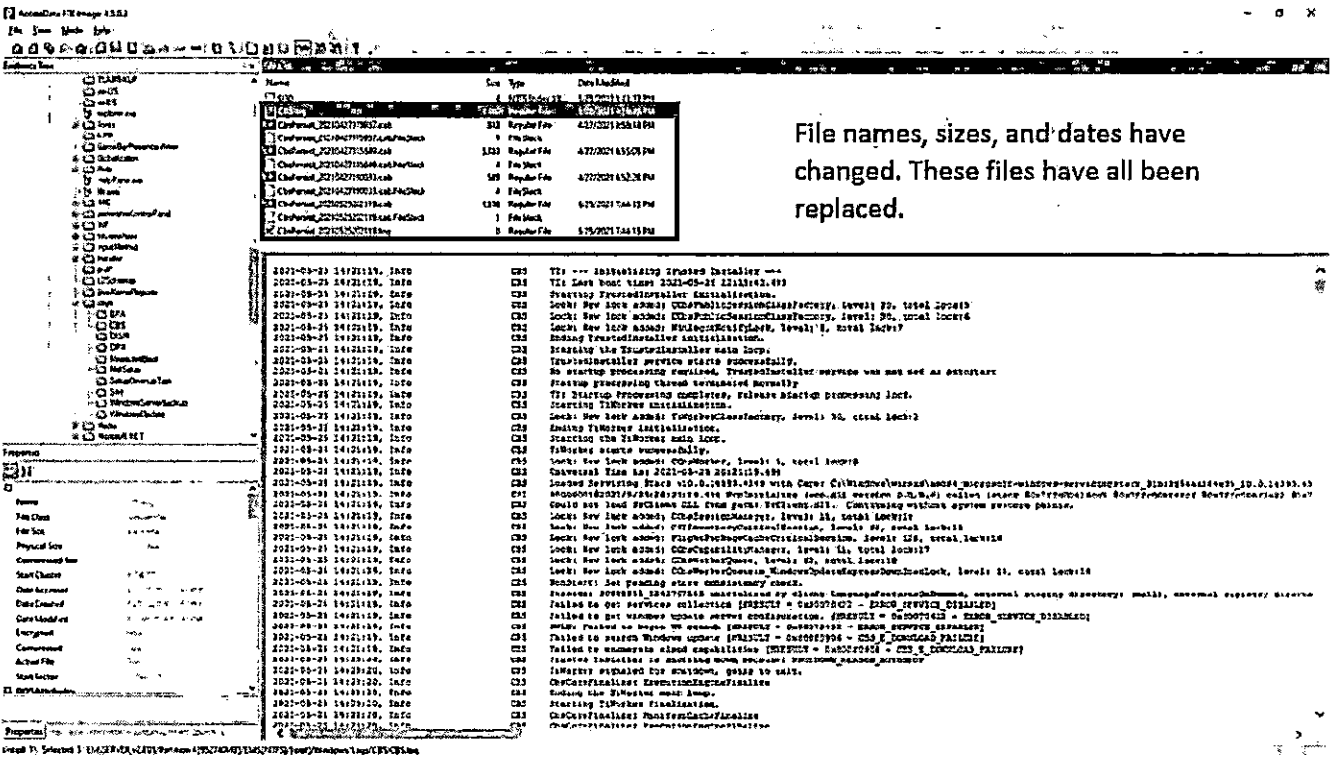


Figure 26 - EMS Server (5.13) CBS Log Files After



File names, sizes, and dates have changed. These files have all been replaced.

Server Election Databases Missing

Purpose: This folder holds all the databases (votes, information regarding batches, when they were processed, how many were processed, who they were processed by, and much more). There are also multiple extra databases that contain information regarding ballot adjudication.

Figure 27 - EMS Server (5.11-CO) Election Databases Before

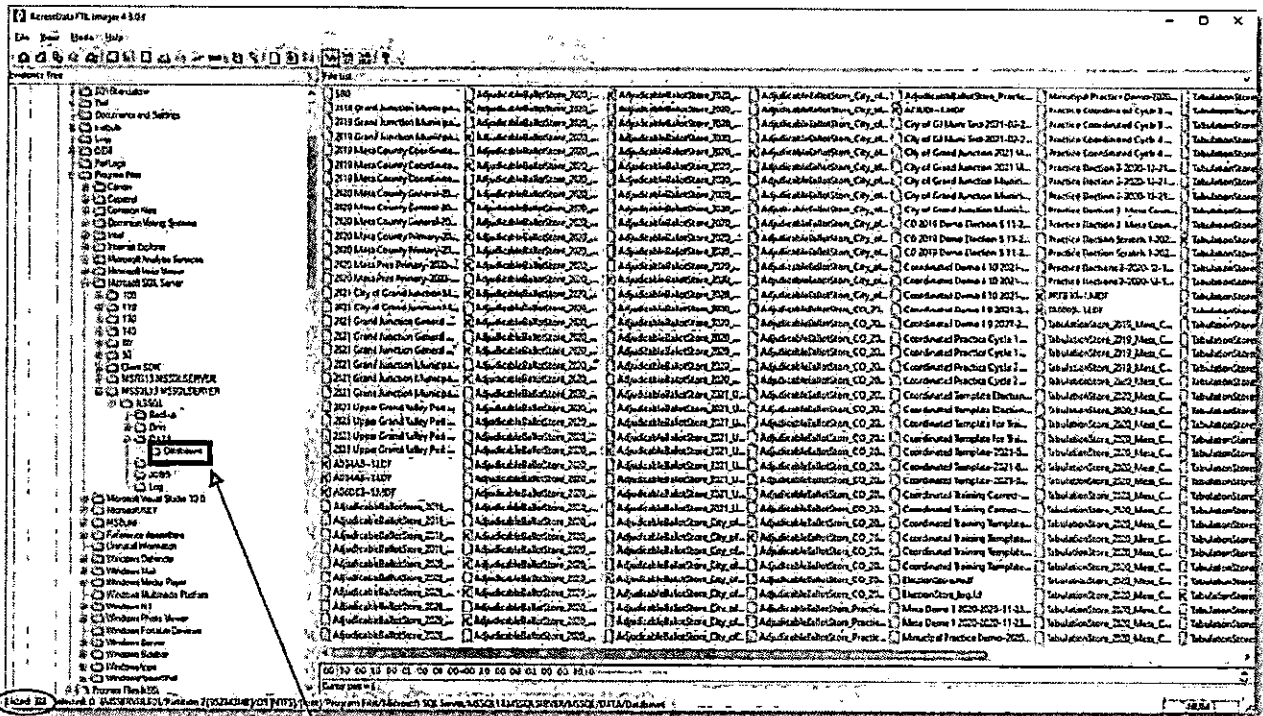
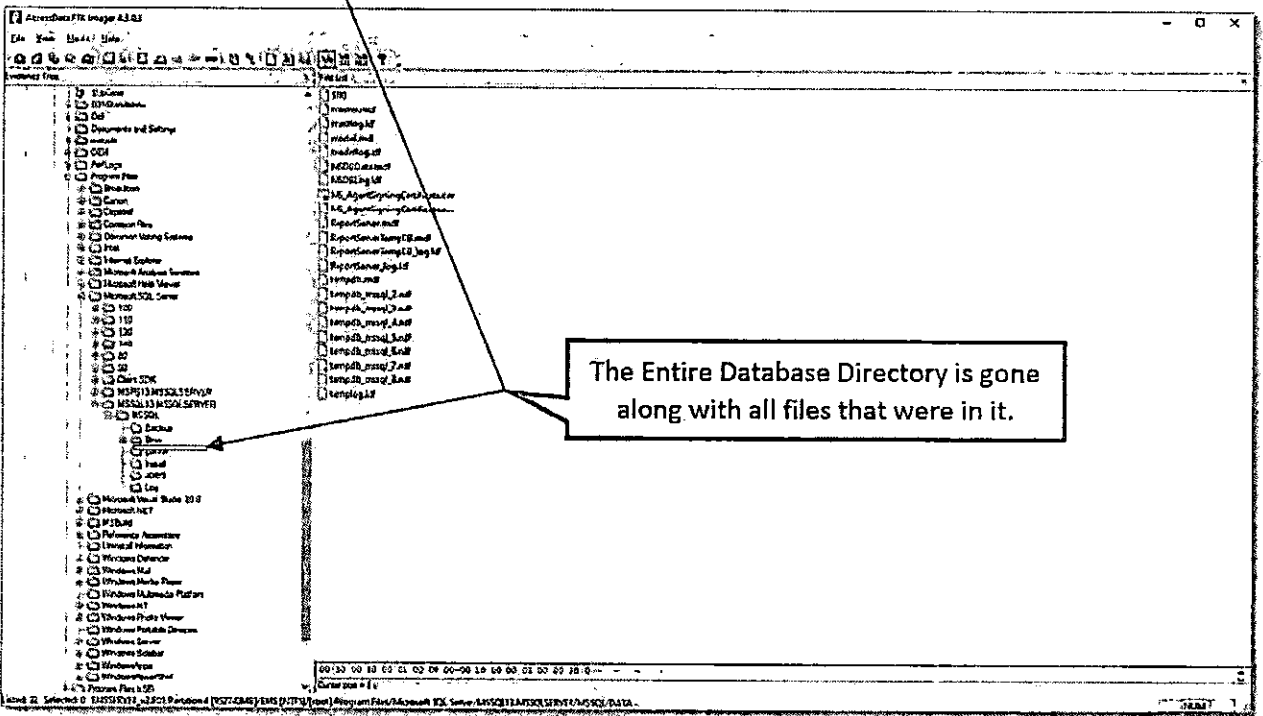


Figure 28 - EMS Server (5.13) Election Databases After



Server DHCP Log Files Missing/Overwritten

Purpose: DHCP Log Files can show evidence regarding computers or other devices being connected to the network.

Figure 29 - EMS Server (5.11-CO) DHCP Log Files Before

The screenshot shows a File Explorer window with the following table of files:

Name	Size	Type	Date Modified
dhcp.log	1	Directory	5/29/2021 9:42:30 PM
dhcp.log	1	NFS Index Allocation	5/29/2021 9:43:38 PM
dhcp.log	1	NFS Indexed Library Stream	5/29/2021 9:43:58 PM
dhcp.log	10	Regular File	5/29/2021 9:43:45 PM
dhcp.log	120	Regular File	5/29/2021 9:43:54 PM
dhcp.log	0	Regular File	5/29/2021 9:43:57 PM
dhcp.log	0	Regular File	5/29/2021 9:43:58 PM
dhcp.log	1	File Stack	5/14/2021 9:30:42 AM
dhcp.log	0	Regular File	5/29/2021 9:43:57 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	11	File Stack	5/29/2021 9:43:58 PM
dhcp.log	8	Regular File	5/29/2021 9:43:57 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	8	Regular File	5/29/2021 9:43:58 PM
dhcp.log	8	Regular File	5/29/2021 9:43:58 PM
dhcp.log	12	Regular File	6/28/2019 9:43:28 AM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	8	Regular File	5/29/2021 9:43:58 PM
dhcp.log	4	Regular File	5/29/2021 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	1	Regular File	5/29/2021 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	4	Regular File	5/15/2021 9:43:58 PM
dhcp.log	3	Regular File	6/18/2019 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	4	Regular File	5/29/2021 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	3	Regular File	6/18/2019 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	4	Regular File	5/29/2021 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	3	Regular File	5/29/2021 9:43:58 PM
dhcp.log	4	Regular File	5/15/2021 9:43:58 PM
dhcp.log	3	Regular File	6/29/2019 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM

Figure 30 - EMS Server (5.18) DHCP Log Files After

The screenshot shows a File Explorer window with a callout box containing the text: "The Number of Files, Dates, and Sizes are Different. They have all been replaced." The table below represents the files shown in the window:

Name	Size	Type	Date Modified
dhcp.log	1	Directory	5/29/2021 10:11:31 PM
dhcp.log	1	NFS Index Allocation	5/29/2021 10:11:31 PM
dhcp.log	1	NFS Indexed Library Stream	5/29/2021 10:11:31 PM
dhcp.log	10	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	120	Regular File	5/29/2021 10:11:31 PM
dhcp.log	0	Regular File	5/29/2021 10:11:31 PM
dhcp.log	7	Regular File	4/29/2021 9:43:58 PM
dhcp.log	2	File Stack	5/29/2021 9:43:58 PM
dhcp.log	1	File Stack	5/29/2021 9:43:58 PM
dhcp.log	8	Regular File	5/29/2021 10:11:31 PM
dhcp.log	3	Regular File	4/29/2021 9:43:58 PM
dhcp.log	1	File Stack	4/29/2021 9:43:58 PM
dhcp.log	2	File Stack	4/29/2021 9:43:58 PM
dhcp.log	2	File Stack	5/29/2021 9:43:58 PM
dhcp.log	2	Regular File	5/29/2021 9:43:58 PM
dhcp.log	3	Regular File	5/29/2021 9:43:58 PM
dhcp.log	3	Regular File	5/29/2021 10:11:31 PM
dhcp.log	8	Regular File	5/29/2021 9:43:58 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM
dhcp.log	1024	Regular File	5/29/2021 10:11:31 PM

The Number of Files, Dates, and Sizes are Different. They have all been replaced.

Server Event Logs Missing/Overwritten

Purpose: These Dominion Log Files keep track of election/project-related activity. The Windows Server event logs outside the red box keep track of much of the activity on the server.

Figure 31 - EMS Server (5.11-CO) Event Logs Before

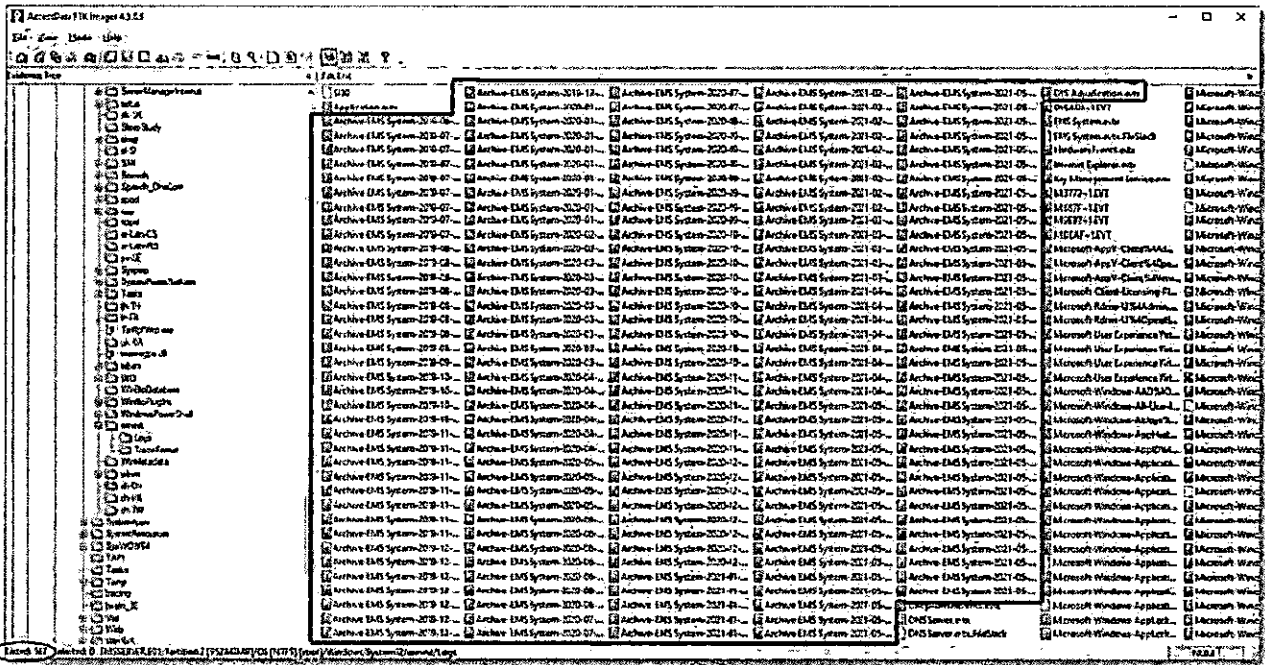
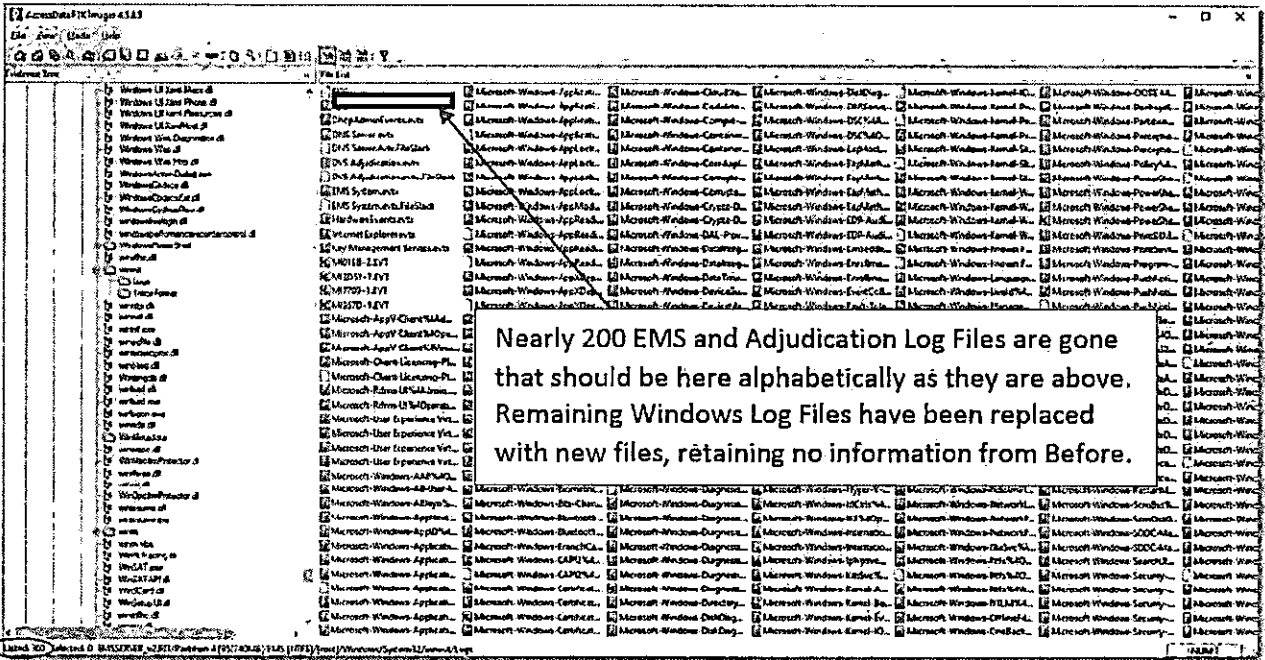


Figure 32 - EMS Server (5.13) Event Logs After



Below are some screen shots of the kind of Election-Related information (such as cast vote records, audit marks, image retrievals, result file loads, etc.) in the EMS Archive Logs that are missing After the Dominion Update:

Figure 33 - Examples of Election Data Missing After Update

The figure displays four screenshots of EMS Archive Logs, each showing a list of events and a detailed view of a specific event. The events are categorized by level (Information) and source (EMS User Log). The detailed views show the command executed and the result of the operation.

Screenshot 1 (Top Left): Archive EMS System 2020-10-21-03:24:37-573. Number of events: 1371. The event list shows multiple 'Information' level events from 'EMS User Log' with 'Event ID' 0 and 'Task C...' 'None'. The detailed view for Event 0 shows the command: `GetSingleCastVoteRecordCommand (execution duration: 16ms): Cast vote record for tabulator '4', batch '2099' and session '2' successfully retrieved.`

Screenshot 2 (Top Right): Archive EMS System 2020-10-21-03:24:37-573. Number of events: 1371. The event list shows multiple 'Information' level events from 'EMS User Log' with 'Event ID' 0 and 'Task C...' 'None'. The detailed view for Event 0 shows the command: `AppendAuditMarkImageCommand (execution duration: 203ms): Audit mark for tabulator '4', batch '2099' and session '77' successfully entered.`

Screenshot 3 (Bottom Left): Archive EMS System 2020-11-05-17:16:37-197. Number of events: 21,157. The event list shows multiple 'Information' level events from 'EMS User Log' with 'Event ID' 0 and 'Task C...' 'None'. The detailed view for Event 0 shows the command: `GetCastVoteRecordImageCommand (execution duration: 19ms): Image for tabulator '10', batch '4341' and session '47' successfully retrieved.`

Screenshot 4 (Bottom Right): Archive EMS System 2020-11-05-17:16:37-197. Number of events: 21,157. The event list shows multiple 'Information' level events from 'EMS User Log' with 'Event ID' 0 and 'Task C...' 'None'. The detailed view for Event 0 shows the command: `LoadResultsCommand (execution duration: 4572ms): Result file '1_170_4343_DETAIL.DVD' was loaded successfully.`

Server System Users are Missing

Purpose: These folders store the information for each user account on the server.

Figure 34 - EMS Server (5.11-CO) System Users Before

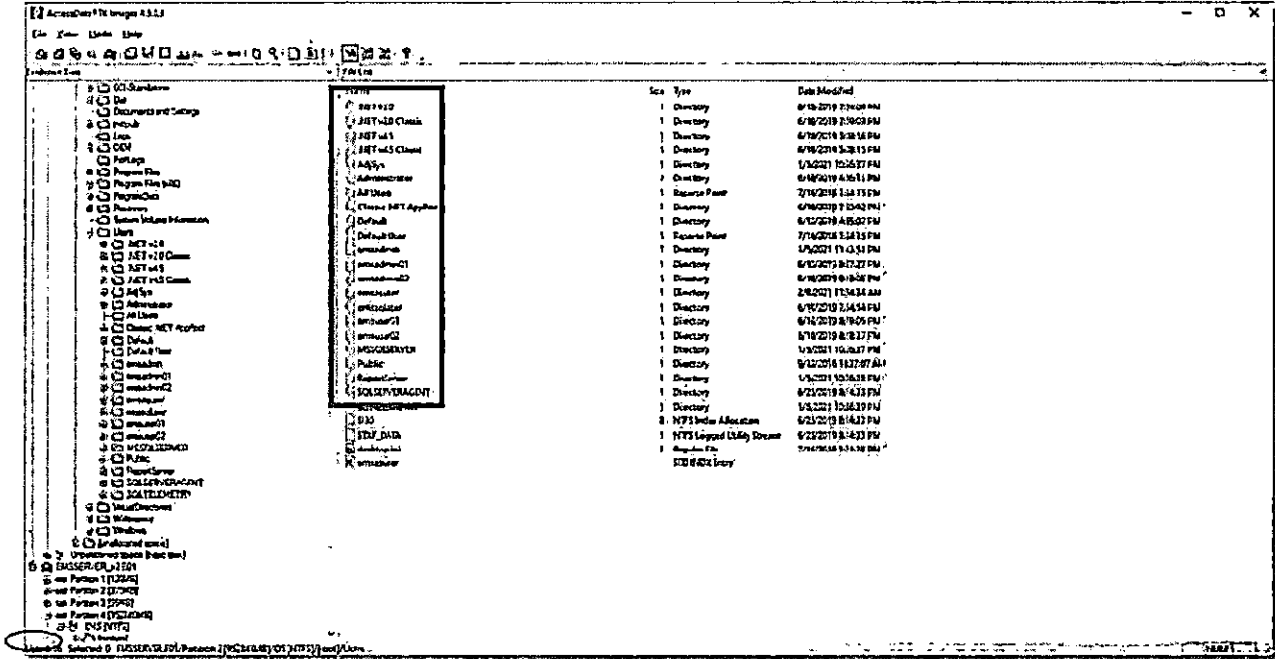
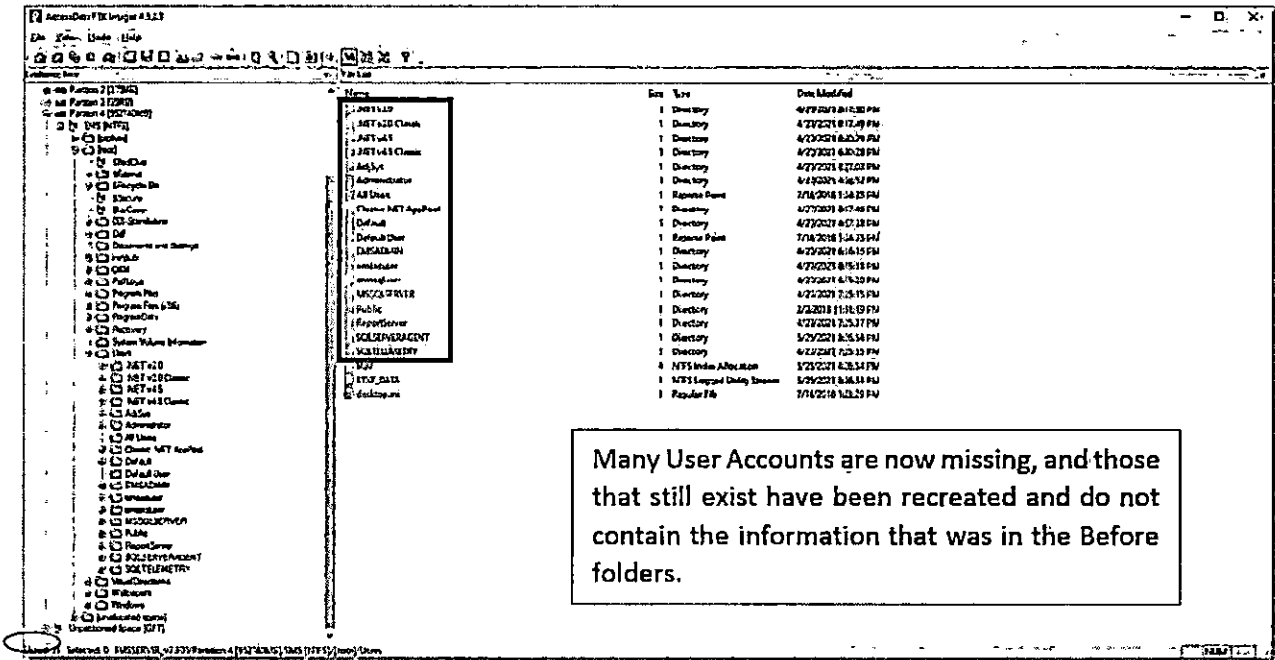


Figure 35 - EMS Server (5.13) System Users After



Server Virtual Directories Log Files Missing

Purpose: These are the Log Files that contain information, warnings, and errors relating to the Website Server as the server processes election projects that have been set up.

Figure 36 - EMS Server (5.11-CO) Virtual Directory Log Files Before

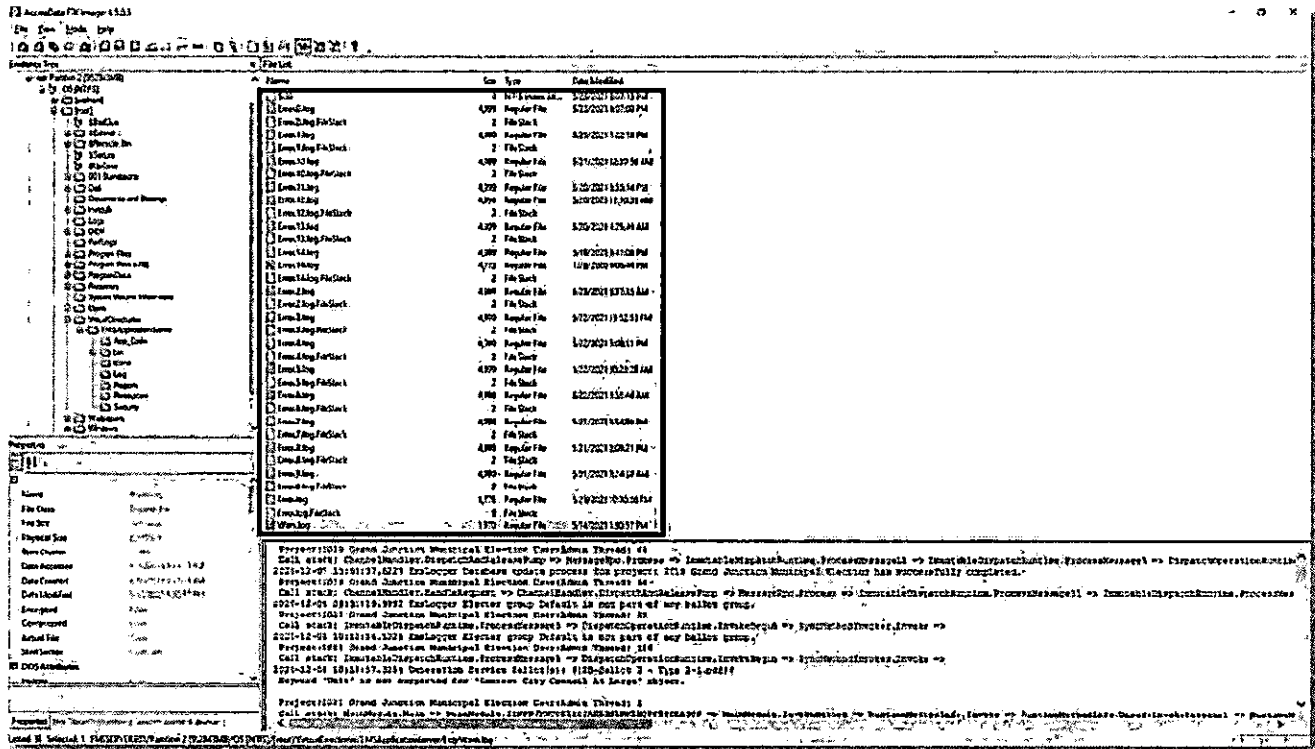
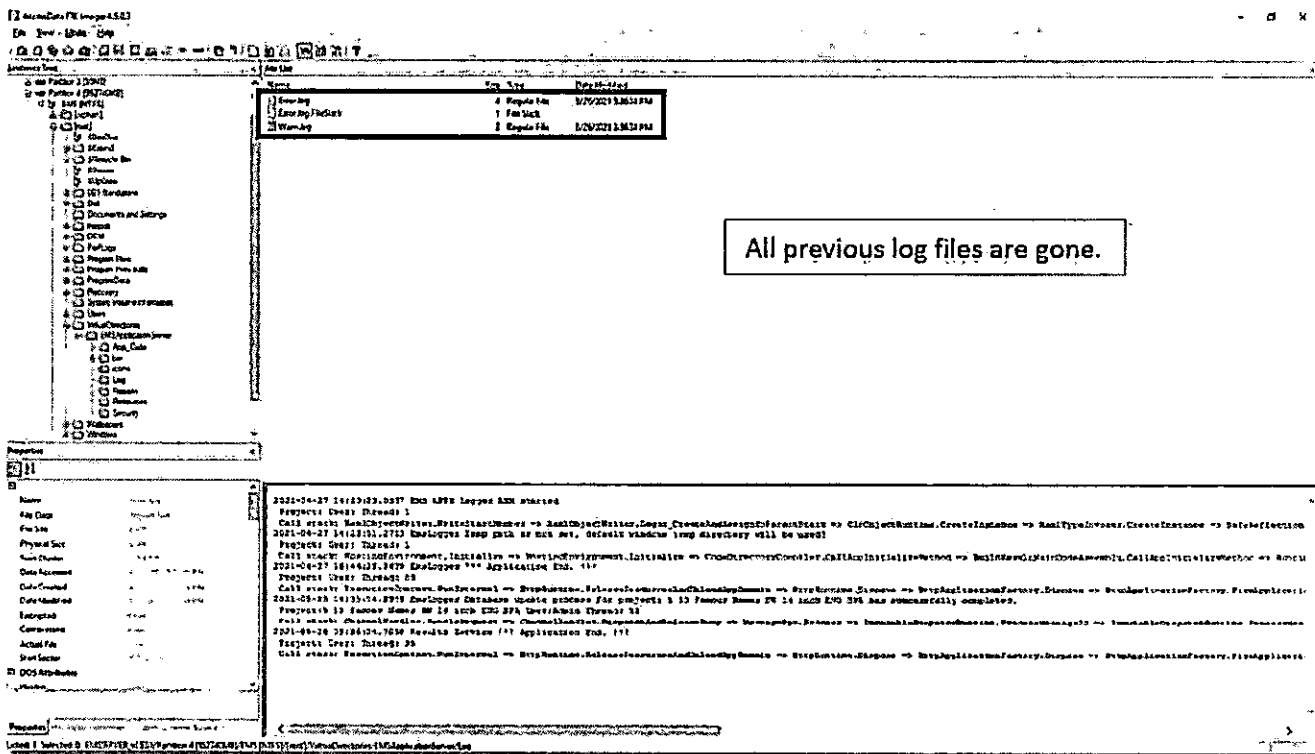


Figure 37 - EMS Server (5.13) Virtual Directory Log Files After



Server Windows Defender Log Files Missing/Overwritten

Purpose: These log files keep track of the activity of the built-in Anti-Virus software.

Figure 38 - EMS Server (5.11-CO) Windows Defender Log Files Before Dominion Update:

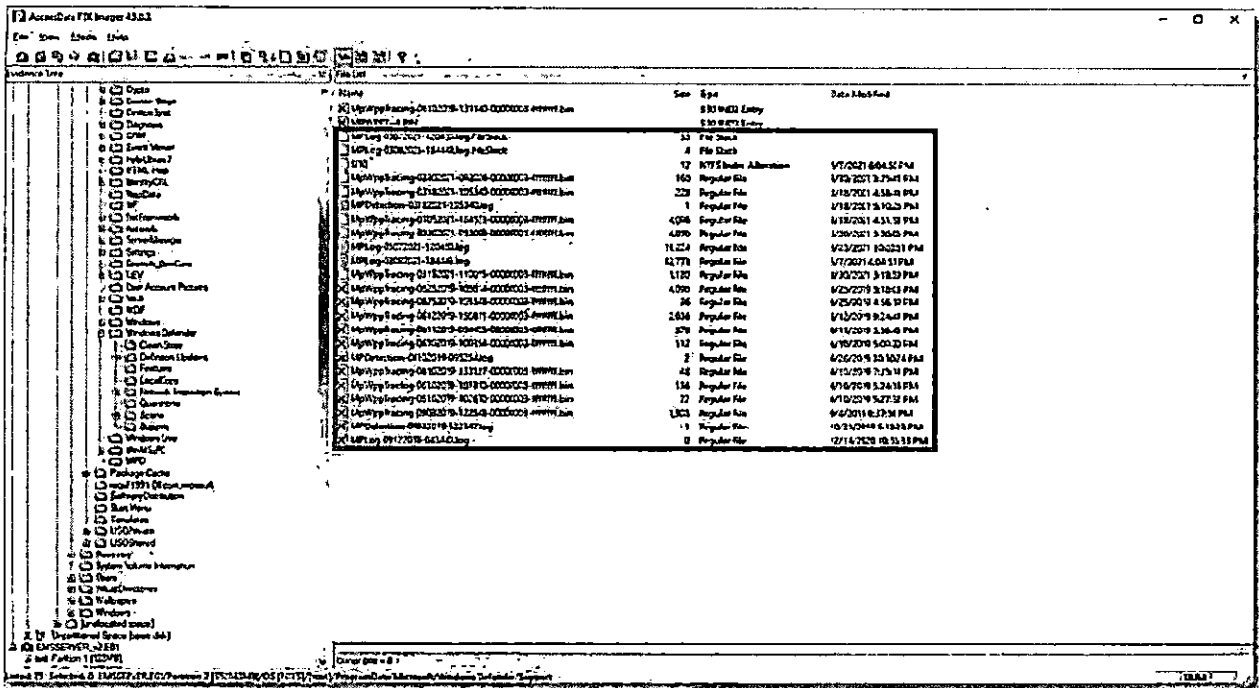
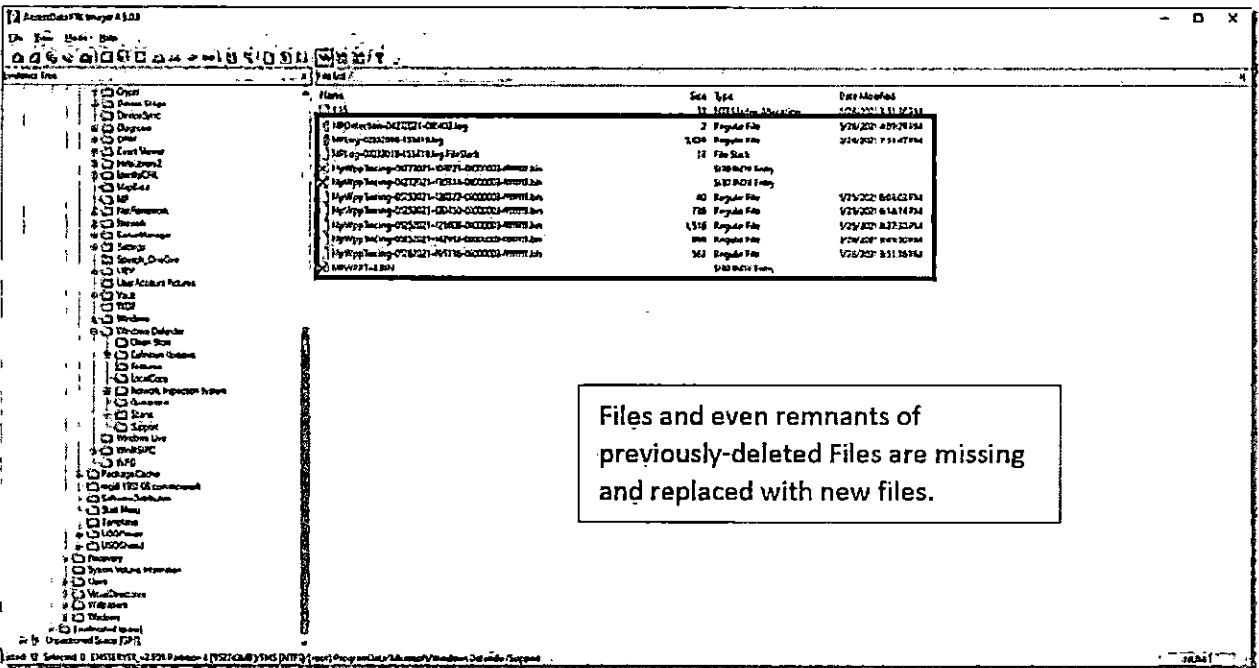


Figure 39 - EMS Server (5.13) Windows Defender Log Files After



Server List of .log files in Before Image that were Deleted.

This list that follows this paragraph is a comparison of the Before and After forensic images of the Mesa County EMS Server. It is a comparative list of files that were deleted – either deliberately erased or overwritten with disregard for the preservation of these files, some of which contain ELECTION RELATED data.

Each line in the image below is the full path listing to each one of the 807 files that end with the word ".log" found on the EMS Server before the Dominion update was applied.

The Color code shows what happened to them After Dominion's update. Of all the files on the server Before the update – files highlighted in Green are still present on the server after the update, while files highlighted in light red have been overwritten and are deleted and not present in the image taken After the update.

Figure 40 - EMS Server Before/After .log File Comparison List

The image shows a large table with multiple columns and rows. The table is mostly obscured by heavy black redaction marks, but some text is visible in the lower right quadrant. The visible text includes file paths and names, such as "C:\Program Files\Microsoft Office\Office12\Excel.exe" and "C:\Program Files\Microsoft Office\Office12\Word.exe". The table appears to be a comparison list of .log files, with columns for file paths and status indicators.

List of .evtx Event Log Files deleted

Figure 41 - EMS Server (5.11-CO) List of .evtx Event Log Files Before

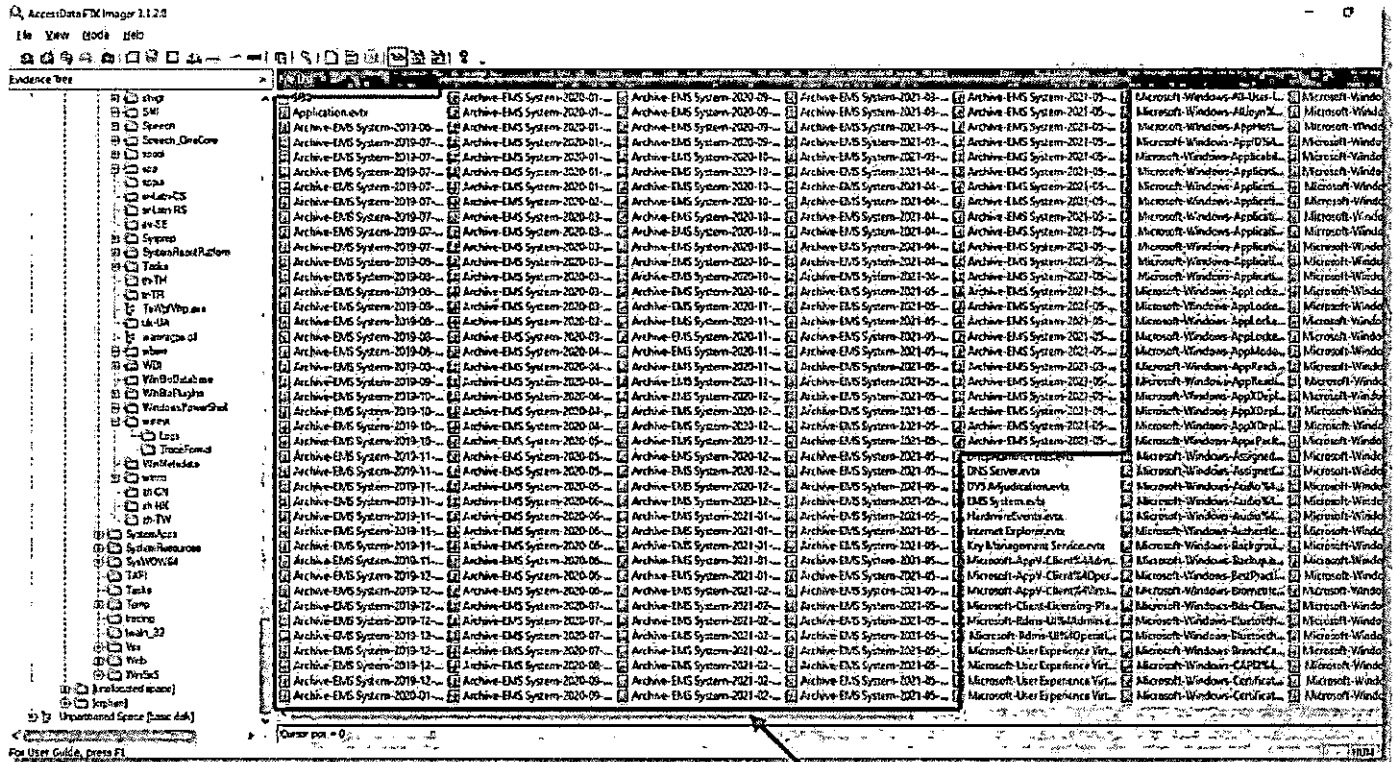
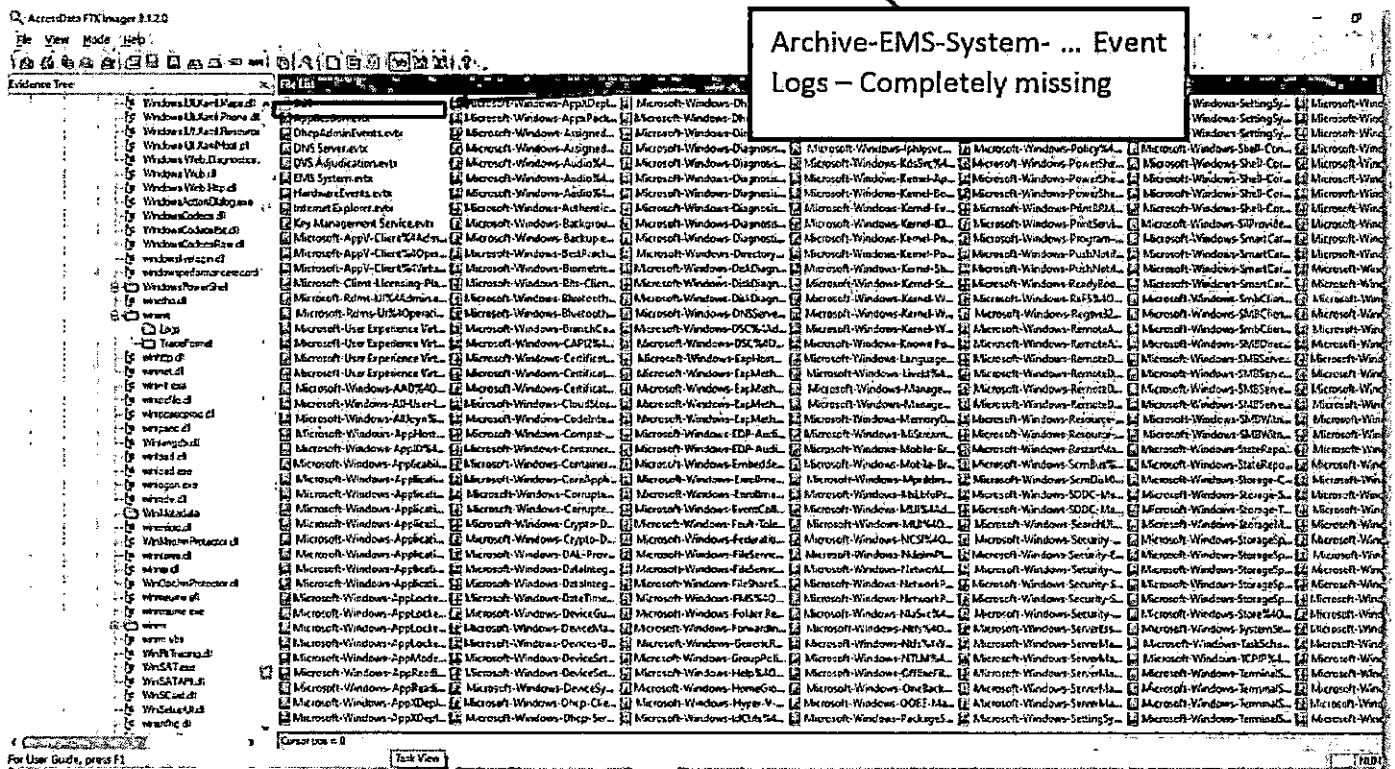


Figure 42 - EMS Server (5.13) List of .evtx Event Log Files After



This list that follows this paragraph is a comparison of the Before and After forensic images of the Mesa County EMS Server. It is a comparative list of files that were deleted – either deliberately erased or overwritten with disregard for the preservation of these files, some of which contain ELECTION RELATED data. A readable list is in Appendix C.

Each line in the image below is the full path listing (e.g., comparison of file names, not content) to each one of the 580 files that end with the word ".evtx" found on the EMS Server before the Dominion update was applied. 190 Event Log Files were deleted.

The Color code shows their status After Dominion's update. Of all the files on the server Before the update – files highlighted in Green are still present (although possibly changed) on the server after the update, while files highlighted in light red have been overwritten and are deleted and not present in the image After the update.

Logs\Microsoft-Windows-Kernel-WHEA%4Errors.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4
Logs\Key Management Service.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VDRVROOT%4Op
Logs\Application.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VHDM:Operatio
Logs\HardwareEvents.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment
Logs\Internet Explorer.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment
Logs\Microsoft-Client-Licensing-Platform%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-International%4O
Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MUI%4Operatio
Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MUI%4Admin.evt
Logs\Microsoft-Windows-AppReadiness%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall
Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-IP\psvc%4Opera
Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4C
Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%4
Logs\Microsoft-Windows-Containers-Wcifs%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%4
Logs\Microsoft-Windows-Containers-Wcnfs%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ApplicationResou
Logs\Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Client-Licensing-Platform%4
Logs\Microsoft-Windows-Crypto-DPAPI%4BackupKeySvc.evtx	Windows\System32\winevt\Logs\System.evtx
Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx	Windows\System32\winevt\Logs\Application.evtx
Logs\Microsoft-Windows-DeviceSetupManager%4Admin.evtx	Windows\System32\winevt\Logs\Security.evtx
Logs\Microsoft-Windows-DeviceSetupManager%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Dhcpv6-Client%4
Logs\Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.evtx	Windows\System32\winevt\Logs\Windows PowerShell.evtx
Logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx	Windows\System32\winevt\Logs\Key Management Service.evtx
Logs\Microsoft-Windows-Dhcpv6-Client%4Admin.evtx	Windows\System32\winevt\Logs\Internet Explorer.evtx
Logs\Microsoft-Windows-Hyper-V-Guest-Drivers%4Admin.evtx	Windows\System32\winevt\Logs\HardwareEvents.evtx
Logs\Microsoft-Windows-International%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Wcmsvc%4Opera
Logs\Microsoft-Windows-AppReadiness%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Program-Compat
Logs\Microsoft-Windows-Kernel-IO%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Client%4Ad
Logs\Microsoft-Windows-Kernel-EventTracing%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
Logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WinRM%4Operat
Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defend
Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defend
Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4Devic
Logs\Microsoft-Windows-Known-Folders-API-Service.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4Actfor
Logs\Microsoft-Windows-Liveld%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceManagemt
Logs\Microsoft-Windows-MUI%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Power%4I
Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Boot%4Or
Logs\Microsoft-Windows-MUI%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%4
Logs\Microsoft-Windows-NCSI%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-PnP%4Cor
Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ShimEngin
Logs\Microsoft-Windows-Ntfs%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4Operatio
Logs\Microsoft-Windows-Ntfs%4WHC.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
Logs\Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VolumeSnapshot
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-IO%4Oper
Logs\Microsoft-Windows-SettingSync%4Debug.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4
Logs\Microsoft-Windows-Kernel-PnP%4Configuration.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4
Logs\Microsoft-Windows-SettingSync%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall
Logs\Microsoft-Windows-Shell-Core%4ActionCenter.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall
Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NCSI%4Operatio
Logs\Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WinINet-Config%4
Logs\Microsoft-Windows-Shell-Core%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4E
Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4E
Logs\Microsoft-Windows-SMBClient%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupMan
Logs\Microsoft-Windows-SmbClient%4Security.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupMan
Logs\Microsoft-Windows-SMBServer%4Audit.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wcifs
Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wcnf
Logs\Microsoft-Windows-SMBServer%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4O

Logs\Microsoft-Windows-SMBServer%4Security.evtx
Logs\Microsoft-Windows-SMBWitnessClient%4Admin.evtx
Logs\Microsoft-Windows-SMBWitnessClient%4Informational.evtx
Logs\Microsoft-Windows-StateRepository%4Operational.evtx
Logs\Microsoft-Windows-StateRepository%4Restricted.evtx
Logs\Microsoft-Windows-TaskScheduler%4Maintenance.evtx
Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx
Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
Logs\Microsoft-Windows-Store%4Operational.evtx
Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
Logs\Microsoft-Windows-User Profile Service%4Operational.evtx
Logs\Microsoft-Windows-UserPnp%4ActionCenter.evtx
Logs\Microsoft-Windows-UserPnp%4DeviceInstall.evtx
Logs\Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx
Logs\Microsoft-Windows-Wcmsvc%4Operational.evtx
Logs\Microsoft-Windows-Windows Defender%4Operational.evtx
Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx
Logs\Microsoft-Windows-WinNet-Config%4ProxyConfigChanged.evtx
Logs\Microsoft-Windows-Winlogon%4Operational.evtx
Logs\Microsoft-Windows-WinRM%4Operational.evtx
Logs\Setup.evtx
Logs\Windows PowerShell.evtx
Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx
Logs\System.evtx
Logs\Security.evtx
Windows\System32\winevt\Logs\Setup.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-02-27-12-21-20-622.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-11-20-46-32-189.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-06-30-13-45-03-347.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-08-02-26-04-899.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-30-19-26-37-188.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-04-08-05-33-867.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-30-16-29-10-602.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-15-15-07-04-381.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-02-02-52-11-569.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-19-00-10-16-214.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-26-22-08-42-827.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-11-22-05-26-089.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-23-04-20-21-835.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-26-12-11-25-223.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-15-07-09-24-325.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-04-04-35-23-707.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-07-21-05-41-859.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-18-19-18-33-633.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-23-20-20-681.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-07-22-53-09-400.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-09-05-03-069.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-03-17-30-918.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-02-11-09-22-083.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-15-51-43-896.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-19-15-04-259.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-28-04-14-58-545.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-06-04-10-43-774.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-24-00-59-56-063.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-08-17-03-22-249.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-10-09-23-03-203.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-06-16-37-56-482.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-02-15-06-36-403.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-07-05-51-17-641.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-06-06-07-29-506.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-27-06-12-01-889.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-14-02-20-35-061.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-16-20-09-20-723.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-26-09-07-58-407.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-08-10-16-08-709.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-26-06-16-16-735.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-21-16-36-38-559.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-03-08-53-17-828.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-23-15-37-23-347.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-13-00-00-07-540.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-21-03-24-37-573.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-15-03-31-17-842.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-10-01-06-03-529.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Servi
Windows\System32\winevt\Logs\Microsoft-Windows-Lived%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-SMBClient%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Con
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Sec
Windows\System32\winevt\Logs\Microsoft-Windows-Logon%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-SettingsSync%4O
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4De
Windows\System32\winevt\Logs\Microsoft-Windows-DateTimeControl
Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders A
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Acti
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4App
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Log
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment
Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-RunTi
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-I
Windows\System32\winevt\Logs\Microsoft-Windows-Store%4Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification
Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification
Windows\System32\winevt\Logs\Microsoft-Windows-TWinUI%4Opera
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe
Windows\System32\winevt\Logs\Microsoft-Windows-Security-SP2-UX-
Windows\System32\winevt\Logs\Microsoft-Windows-BackgroundTaskI
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-A
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-A
Windows\System32\winevt\Logs\Microsoft-Windows-Forwarding%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-A
Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaus
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScal
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScal
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Schedt
Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Con
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Connecte
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-M
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-ClassNP
Windows\System32\winevt\Logs\Microsoft-Windows-RestartManager
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PLA%4
Windows\System32\winevt\Logs\Microsoft-Windows-CAP12%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-WindowsUpdate
Windows\System32\winevt\Logs\Microsoft-Windows-Nlasvc%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Ad
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PCW%4
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Storport
Windows\System32\winevt\Logs\EMS System.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application Serve
Windows\System32\winevt\Logs\Microsoft-Windows-Application Serve
Windows\System32\winevt\Logs\OVS Adjudication.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CloudStorageWiz
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Operational
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Virtual Appli
Windows\System32\winevt\Logs\Microsoft-Rdms-UI%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Rdms-UI%4Operational.evt
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizat
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizat
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizat
Windows\System32\winevt\Logs\Microsoft-Windows-AAO%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-All-User-Install-A
Windows\System32\winevt\Logs\Microsoft-Windows-AllJoyn%4Operat
Windows\System32\winevt\Logs\Microsoft-Windows-AppHost%4Admi
Windows\System32\winevt\Logs\Microsoft-Windows-AppID%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-ApplicabilityEngi
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4EXE
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4MS
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac
Windows\System32\winevt\Logs\Microsoft-Windows-AppXPackaging%4
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccess%4
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccess%4
Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Capture

Windows\System32\winevt\Logs\Archive-EMS System-2019-11-25-05-09-12-916.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-22-13-12-21-043.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-06-08-06-21-993.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-05-17-16-37-197.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-23-08-11-827.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-17-01-19-18-484.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-01-39-07-647.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-04-12-10-17-214.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-12-02-56-47-489.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-07-26-54-297.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-04-04-03-42-737.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-16-16-31-58-059.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-21-12-09-41-781.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-28-14-04-05-771.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-12-22-02-14-487.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-13-18-05-49-770.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-17-19-10-01-322.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-05-14-13-33-324.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-13-10-56-695.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-28-22-08-50-835.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-17-11-04-36-787.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-05-00-03-39-390.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-12-10-09-10-333.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-20-40-41-039.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-24-11-15-42-872.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-18-17-48-53-388.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-09-10-14-15-715.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-31-11-01-47-908.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-27-08-29-08-399.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-14-23-29-04-158.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-24-21-04-12-832.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-21-04-04-25-803.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-01-07-15-340.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-14-18-29-08-151.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-11-21-02-29-740.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-03-11-33-19-283.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-19-20-02-44-037.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-28-20-58-32-283.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-16-03-02-57-774.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-01-21-14-15-340.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-08-12-31-149.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-22-17-12-11-701.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-05-45-04-636.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-05-12-32-06-091.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-26-13-42-04-162.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-16-14-59-42-045.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-23-13-23-46-471.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-18-23-53-08-392.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-13-14-26-512.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-27-17-59-53-690.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-20-09-29-41-350.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-20-07-59-19-878.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-31-02-47-11-038.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-29-23-11-26-924.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-09-05-29-49-411.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-26-06-11-56-096.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-00-00-39-858.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-18-58-50-004.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-28-08-06-44-934.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-11-14-07-34-718.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-15-07-27-29-016.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-04-17-16-43-223.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-24-22-45-04-435.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-20-18-16-33-823.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-18-12-49-02-987.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-13-08-24-43-079.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-22-12-08-49-154.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-30-02-15-24-619.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-22-17-53-50-782.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-11-17-12-21-460.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-18-20-12-44-811.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-02-14-34-04-967.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-07-10-51-04-386.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-11-05-09-09-286.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-31-12-27-41-741.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-22-20-55-04-936.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Playbac
Windows\System32\winevt\Logs\Microsoft-Windows-Authentication U
Windows\System32\winevt\Logs\Microsoft-Windows-Backup.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-BestPractices%4A
Windows\System32\winevt\Logs\Microsoft-Windows-Biometrics%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-BthLE
Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-MTPE
Windows\System32\winevt\Logs\Microsoft-Windows-BranchCacheSMF
Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServic
Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService
Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService
Windows\System32\winevt\Logs\Microsoft-Windows-Compat-Apprais
Windows\System32\winevt\Logs\Microsoft-Windows-CoreApplication
Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRec
Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRec
Windows\System32\winevt\Logs\Microsoft-Windows-DAL-Provider%4A
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceGuard%4C
Windows\System32\winevt\Logs\Microsoft-Windows-Devices-Backgro
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSync%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Netw
Windows\System32\winevt\Logs\Microsoft-Windows-DirectoryService
Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnostic%4
Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnostic%4D
Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticRe
Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Admin.ev
Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-EapHost%4Opera
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Sim
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Tls
Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-Regul
Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-TCB%
Windows\System32\winevt\Logs\Microsoft-Windows-EmbeddedAppl
Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentPolicy
Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentWebS
Windows\System32\winevt\Logs\Microsoft-Windows-EventCollector%4
Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-H
Windows\System32\winevt\Logs\Microsoft-Windows-FederationService
Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Serv
Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Serv
Windows\System32\winevt\Logs\Microsoft-Windows-FileShareShadow
Windows\System32\winevt\Logs\Microsoft-Windows-FMS%4Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-Folder Redirectio
Windows\System32\winevt\Logs\Microsoft-Windows-NdisMiniPlatform%
Windows\System32\winevt\Logs\Microsoft-Windows-GenericRoaming
Windows\System32\winevt\Logs\Microsoft-Windows-Help%4Operatio
Windows\System32\winevt\Logs\Microsoft-Windows-Hyper-V-Guest-D
Windows\System32\winevt\Logs\Microsoft-Windows-IdCtrls%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-IdCtrls%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-International-Reg
Windows\System32\winevt\Logs\Microsoft-Windows-KdsSvc%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Apphel
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-EventTrac
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel.WDI%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-LanguagePackSet
Windows\System32\winevt\Logs\Microsoft-Windows-ManagementToc
Windows\System32\winevt\Logs\Microsoft-Windows-ManagementToc
Windows\System32\winevt\Logs\Microsoft-Windows-MemoryDiagnosti
Windows\System32\winevt\Logs\Microsoft-Windows-MiStreamProvid
Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadban
Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadban
Windows\System32\winevt\Logs\Microsoft-Windows-Mprddm%4Oper
Windows\System32\winevt\Logs\Microsoft-Windows-MSLbfProvider%
Windows\System32\winevt\Logs\Microsoft-Windows-NetworkLocation
Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProvider
Windows\System32\winevt\Logs\Microsoft-Windows-NtLm%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-OfflineFiles%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-OneBackup%4De
Windows\System32\winevt\Logs\Microsoft-Windows-OCBE-Machine-L
Windows\System32\winevt\Logs\Microsoft-Windows-PackageStateRo

Windows\System32\winevt\Logs\Microsoft-Windows-DNSServer%4Audit.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-10-23-29-48-856.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-18-12-10-49-482.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-09-02-13-32-58-546.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-29-19-12-25-021.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Audit.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-Wired-AutoConfig%4
Windows\System32\winevt\Logs\Microsoft-Windows-Workplace Join%4Ad
Windows\System32\winevt\Logs\Microsoft-Windows-WPD-ClassInstaller%
Windows\System32\winevt\Logs\Microsoft-Windows-WPD-CompositeClass
Windows\System32\winevt\Logs\Microsoft-Windows-WPD-MTPClassDrive
Windows\System32\winevt\Logs\SMSApi.evtx

Analysis Summary

Analysis of the Mesa County Dominion Voting Systems EMS server identified that extensive deletion of both election data and election-related data, comprising election records which must and should have been preserved under Federal and Colorado law, has occurred either as a result of or coincident with the vendor's and CO Secretary of State's modification of the system from version 5.11-CO to 5.13. This deleted data is critical to any effort to reconstruct events taking place on the voting systems, and to determine if unauthorized access or operation of the voting systems took place.

Furthermore, the EMS server application logging functions are configured to "Overwrite events as needed" if arbitrarily-selected file storage sizes are exceeded, which could predictably and likely has resulted in the systematic, automated deletion of logfile content comprising election-related data.

This systemic deletion of logfile data requires additional investigation.

CONCLUSION

This forensic examination found that significant election record preservation requirements under the 2002 VSS and Federal and state law HAVE NOT BEEN MET and further that destruction of Election-Related Data, specifically critical logfiles, has occurred. This destruction is not incidental or minor but is *highly significant*.

These findings have been demonstrated in this report and evidence has been presented demonstrating *conclusively to both computer systems experts as well as legal professionals and the general public at large* that the facts in these findings support the conclusions that:

- 1) Election-related data and election data explicitly required to be preserved, as described in the 2002 VSS criteria referenced in this section, HAS BEEN DESTROYED IN VIOLATION OF THE LAW, and
- 2) The specific configuration settings of the server examined lead to the understanding that Certification Requirements for Voting Systems have likely not been met despite this system having been certified and thereby approved for use in Colorado by the Colorado Secretary of State.

Further investigation is required to determine the full scope of non-compliance with legal mandates for voting systems and election records, and whether the non-compliance is deliberate or simply negligent.

APPENDIX A. DELETED ".LOG" FILES AFTER DOMINION TRUSTED BUILD UPDATE

Deleted files are highlighted in light red. Files highlighted in green are still present in the server image.

inetpub\logs\LogFiles\W3SVC1*_ex210406.log
inetpub\logs\LogFiles\W3SVC1*_ex200903.log
inetpub\logs\LogFiles\W3SVC1*_ex191021.log
inetpub\logs\LogFiles\W3SVC1*_ex191101.log
inetpub\logs\LogFiles\W3SVC1*_ex201028.log
inetpub\logs\LogFiles\W3SVC1*_ex191025.log
inetpub\logs\LogFiles\W3SVC1*_ex191023.log
inetpub\logs\LogFiles\W3SVC1*_ex200522.log
inetpub\logs\LogFiles\W3SVC1*_ex191126.log
inetpub\logs\LogFiles\W3SVC1*_ex200819.log
inetpub\logs\LogFiles\W3SVC1*_ex191028.log
inetpub\logs\LogFiles\W3SVC1*_ex210104.log
inetpub\logs\LogFiles\W3SVC1*_ex191022.log
inetpub\logs\LogFiles\W3SVC1*_ex200625.log
inetpub\logs\LogFiles\W3SVC1*_ex210211.log
inetpub\logs\LogFiles\W3SVC1*_ex201008.log
inetpub\logs\LogFiles\W3SVC1*_ex191114.log
inetpub\logs\LogFiles\W3SVC1*_ex200826.log
inetpub\logs\LogFiles\W3SVC1*_ex210223.log
inetpub\logs\LogFiles\W3SVC1*_ex210224.log
inetpub\logs\LogFiles\W3SVC1*_ex210205.log
inetpub\logs\LogFiles\W3SVC1*_ex210318.log
inetpub\logs\LogFiles\W3SVC1*_ex200520.log
inetpub\logs\LogFiles\W3SVC1*_ex201208.log
inetpub\logs\LogFiles\W3SVC1*_ex210407.log
inetpub\logs\LogFiles\W3SVC1*_ex191030.log
inetpub\logs\LogFiles\W3SVC1*_ex191031.log
inetpub\logs\LogFiles\W3SVC1*_ex191106.log
inetpub\logs\LogFiles\W3SVC1*_ex191105.log
inetpub\logs\LogFiles\W3SVC1*_ex191029.log
inetpub\logs\LogFiles\W3SVC1*_ex191104.log
inetpub\logs\LogFiles\W3SVC1*_ex200730.log
inetpub\logs\LogFiles\W3SVC1*_ex210512.log
inetpub\logs\LogFiles\W3SVC1*_ex201103.log

inetpub\logs\LogFiles\W3SVC1\u_ex191107.log
inetpub\logs\LogFiles\W3SVC1\u_ex191115.log
inetpub\logs\LogFiles\W3SVC1\u_ex200929.log
inetpub\logs\LogFiles\W3SVC1\u_ex200930.log
inetpub\logs\LogFiles\W3SVC1\u_ex200813.log
inetpub\logs\LogFiles\W3SVC1\u_ex210523.log
inetpub\logs\LogFiles\W3SVC1\u_ex200127.log
inetpub\logs\LogFiles\W3SVC1\u_ex200224.log
inetpub\logs\LogFiles\W3SVC1\u_ex201023.log
inetpub\logs\LogFiles\W3SVC1\u_ex200618.log
inetpub\logs\LogFiles\W3SVC1\u_ex210212.log
inetpub\logs\LogFiles\W3SVC1\u_ex200302.log
inetpub\logs\LogFiles\W3SVC1\u_ex200124.log
inetpub\logs\LogFiles\W3SVC1\u_ex200303.log
inetpub\logs\LogFiles\W3SVC1\u_ex210303.log
inetpub\logs\LogFiles\W3SVC1\u_ex200227.log
inetpub\logs\LogFiles\W3SVC1\u_ex201113.log
inetpub\logs\LogFiles\W3SVC1\u_ex201214.log
inetpub\logs\LogFiles\W3SVC1\u_ex201218.log
inetpub\logs\LogFiles\W3SVC1\u_ex200528.log
inetpub\logs\LogFiles\W3SVC1\u_ex201222.log
inetpub\logs\LogFiles\W3SVC1\u_ex200131.log
inetpub\logs\LogFiles\W3SVC1\u_ex210105.log
inetpub\logs\LogFiles\W3SVC1\u_ex201221.log
inetpub\logs\LogFiles\W3SVC1\u_ex200228.log
inetpub\logs\LogFiles\W3SVC1\u_ex200304.log
inetpub\logs\LogFiles\W3SVC1\u_ex200518.log
inetpub\logs\LogFiles\W3SVC1\u_ex210302.log
inetpub\logs\LogFiles\W3SVC1\u_ex200715.log
inetpub\logs\LogFiles\W3SVC1\u_ex200624.log
inetpub\logs\LogFiles\W3SVC1\u_ex210113.log
inetpub\logs\LogFiles\W3SVC1\u_ex200519.log
inetpub\logs\LogFiles\W3SVC1\u_ex200320.log
inetpub\logs\LogFiles\W3SVC1\u_ex210106.log

inetpub\logs\LogFiles\W3SVC1\u_ex210222.log
inetpub\logs\LogFiles\W3SVC1\u_ex210412.log
inetpub\logs\LogFiles\W3SVC1\u_ex200827.log
inetpub\logs\LogFiles\W3SVC1\u_ex200673.log
inetpub\logs\LogFiles\W3SVC1\u_ex210210.log
inetpub\logs\LogFiles\W3SVC1\u_ex200617.log
inetpub\logs\LogFiles\W3SVC1\u_ex200515.log
inetpub\logs\LogFiles\W3SVC1\u_ex200731.log
inetpub\logs\LogFiles\W3SVC1\u_ex201001.log
inetpub\logs\LogFiles\W3SVC1\u_ex201215.log
inetpub\logs\LogFiles\W3SVC1\u_ex200521.log
inetpub\logs\LogFiles\W3SVC1\u_ex210111.log
inetpub\logs\LogFiles\W3SVC1\u_ex200526.log
inetpub\logs\LogFiles\W3SVC1\u_ex200601.log
inetpub\logs\LogFiles\W3SVC1\u_ex200612.log
inetpub\logs\LogFiles\W3SVC1\u_ex210115.log
inetpub\logs\LogFiles\W3SVC1\u_ex210112.log
inetpub\logs\LogFiles\W3SVC1\u_ex210107.log
inetpub\logs\LogFiles\W3SVC1\u_ex200616.log
inetpub\logs\LogFiles\W3SVC1\u_ex210209.log
inetpub\logs\LogFiles\W3SVC1\u_ex210409.log
inetpub\logs\LogFiles\W3SVC1\u_ex200630.log
inetpub\logs\LogFiles\W3SVC1\u_ex200708.log
inetpub\logs\LogFiles\W3SVC1\u_ex200701.log
inetpub\logs\LogFiles\W3SVC1\u_ex210511.log
inetpub\logs\LogFiles\W3SVC1\u_ex200924.log
inetpub\logs\LogFiles\W3SVC1\u_ex201019.log
inetpub\logs\LogFiles\W3SVC1\u_ex201029.log
inetpub\logs\LogFiles\W3SVC1\u_ex201109.log
inetpub\logs\LogFiles\W3SVC1\u_ex201123.log
inetpub\logs\LogFiles\W3SVC1\u_ex201026.log
inetpub\logs\LogFiles\W3SVC1\u_ex201120.log
inetpub\logs\LogFiles\W3SVC1\u_ex201209.log
inetpub\logs\LogFiles\W3SVC1\u_ex201102.log

inetpub\logs\LogFiles\W3SVC1\u_ex210301.log
inetpub\logs\LogFiles\W3SVC1\u_ex210330.log
inetpub\logs\LogFiles\W3SVC1\u_ex210329.log
inetpub\logs\LogFiles\W3SVC1\u_ex210402.log
inetpub\logs\LogFiles\W3SVC1\u_ex210114.log
inetpub\logs\LogFiles\W3SVC1\u_ex210108.log
inetpub\logs\LogFiles\W3SVC1\u_ex210405.log
inetpub\logs\LogFiles\W3SVC1\u_ex210310.log
inetpub\logs\LogFiles\W3SVC1\u_ex210311.log
inetpub\logs\LogFiles\W3SVC1\u_ex210304.log
inetpub\logs\LogFiles\W3SVC1\u_ex210315.log
inetpub\logs\LogFiles\W3SVC1\u_ex210309.log
inetpub\logs\LogFiles\W3SVC1\u_ex210331.log
inetpub\logs\LogFiles\W3SVC1\u_ex210415.log
inetpub\logs\LogFiles\W3SVC1\u_ex210510.log
inetpub\logs\LogFiles\W3SVC1\u_ex190903.log
inetpub\logs\LogFiles\W3SVC1\u_ex190625.log
inetpub\logs\LogFiles\W3SVC1\u_ex190610.log
inetpub\logs\LogFiles\W3SVC1\u_ex190611.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\VC10Redist_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\VC10Redist_Cpu32_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\VSHelp_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\SqlSupport_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_tools_extensions_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_tools_extensions_loc_Cpu64_1033_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_common_core_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\conn_info_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\conn_info_loc_Cpu64_1033_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_batchparser_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_engine_core_shared_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_common_core_loc_Cpu64_1033_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\RsFx_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_engine_core_inst_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\SqlDom_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_engine_core_shared_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_engine_core_inst_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_diag_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_rs_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_dmf_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_dmf_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_xevent_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\smo_extensions_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\smo_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_xevent_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\smo_extensions_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_rs_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sqlincl_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\msodbcsql_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\smo_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\tsqllangsvc_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\dacfx_Cpu32_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\SqlSqmShared_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\SqlWriter_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\SqlBrowser_Cpu32_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\SqlSupport_KatmaiRTM_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_tools_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_120309\sql_tools_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\msodbcsql_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\SqlWriter_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\SqlBrowser_Cpu32_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\SqlSqmShared_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_common_core_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_rs_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_common_core_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_rs_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_engine_core_inst_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_engine_core_shared_loc_Cpu64_1033_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\RsFx_Cpu64_1.log

Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\SqlDom_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_engine_core_shared_Cpu64_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\sql_engine_core_inst_loc_Cpu64_1033_1.log
Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190610_125107\MSSQLSERVER\SqlSupport_Cpu64_1.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_09_2021_00_02_18.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_03_18_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_20_2021_00_02_42.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_19_2021_00_02_39.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_17_2021_00_02_35.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_03_18_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_23_2021_00_02_48.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_22_2021_00_02_47.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_16_2021_00_02_33.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_13_2021_00_02_26.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_12_2021_00_02_24.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_15_2021_00_02_30.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_10_2021_00_02_20.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_11_2021_00_02_22.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_21_2021_00_02_45.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_18_2021_00_02_37.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_05_14_2021_00_02_28.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_01_05_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_03_30_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_03_30_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_09_03_2019_12_25_51.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_06_26_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_06_26_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_06_25_2019_10_55_56.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_06_25_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_06_25_2019_10_58_23.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_06_25_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\ReportServerService_06_12_2019_15_08_21.log
Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_06_12_21.log
ProgramData\Dell\UpdatePackage\log\support\BIOS_Y63D_WN64_2.9.1.log

ProgramData\Dell\UpdatePackage\log\support\SAS-RAID_Driver_T244W_WN64_6.604.06.00_A01_07.log
ProgramData\Dell\UpdatePackage\log\support\Drivers-for-OS-Deployment_Application_WP3PH_WN64_18.12.04_A00_01.log
ProgramData\Dell\UpdatePackage\log\support\Power_Firmware_8R0NM_WN64_00.1B.53.log
ProgramData\Dell\UpdatePackage\log\support\SAS-RAID_Firmware_F675Y_WN64_25.5.5.0005_A13_01.log
ProgramData\Dell\UpdatePackage\log\support\Network_Firmware_F3KFN_WN64_21.40.9.log
ProgramData\Dell\UpdatePackage\log\support\iDRAC-with-Lifecycle-Controller_Firmware_40T1C_WN64_2.63.60.61_A00.log
ProgramData\Dell\UpdatePackage\log\support\BIOS_T9YX9_WN64_2.9.1.log
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy\Act
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy\Act
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.AccountsControl_10.0.14393.0_neutral_cw5n1h2txyewy\ActivationStore
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.AccountsControl_10.0.14393.0_neutral_cw5n1h2txyewy\ActivationStore
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.BioEnrollment_10.0.14393.0_neutral_cw5n1h2txyewy\ActivationStore.c
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.BioEnrollment_10.0.14393.0_neutral_cw5n1h2txyewy\ActivationStore.c
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.LockApp_10.0.14393.0_neutral_cw5n1h2txyewy\ActivationStore.dat.LO
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.LockApp_10.0.14393.0_neutral_cw5n1h2txyewy\ActivationStore.dat.LO
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Apprep.ChxApp_1000.14393.0.0_neutral_neutral_cw5n1h2txy
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Apprep.ChxApp_1000.14393.0.0_neutral_neutral_cw5n1h2txy
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.AssignedAccessLockApp_1000.14393.0.0_neutral_neutral_cw5
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.AssignedAccessLockApp_1000.14393.0.0_neutral_neutral_cw5
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.CloudExperienceHost_10.0.14393.0_neutral_neutral_cw5n1h2
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.CloudExperienceHost_10.0.14393.0_neutral_neutral_cw5n1h2
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2txyewy\Activat
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2txyewy\Activat
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.SecondaryTileExperience_10.0.0.0_neutral_cw5n1h2txyewy\
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.SecondaryTileExperience_10.0.0.0_neutral_cw5n1h2txyewy\
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.14393.0_neutral_neutral_cw5n1h2t
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.14393.0_neutral_neutral_cw5n1h2t
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.XboxGameCallableUI_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy\
ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.XboxGameCallableUI_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy\
ProgramData\Microsoft\Windows\AppRepository\Packages\windows.immersivecontrolpanel_6.2.0.0_neutral_neutral_cw5n1h2txyewy\Activat
ProgramData\Microsoft\Windows\AppRepository\Packages\windows.immersivecontrolpanel_6.2.0.0_neutral_neutral_cw5n1h2txyewy\Activat
ProgramData\Microsoft\Windows\AppRepository\Packages\Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore.c
ProgramData\Microsoft\Windows\AppRepository\Packages\Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore.c
ProgramData\Microsoft\Windows\AppRepository\Packages\Windows.PrintDialog_6.2.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat

ProgramData\Microsoft\Windows\AppRepository\Packages\Windows.PrintDialog_6.2.0.0_neutral_neutral_cw5n1h2bxyewy\ActivationStore.dat

ProgramData\Microsoft\Windows Defender\Scans\History\Service\History.Log

ProgramData\Microsoft\Windows Defender\Scans\History\Service\Unknown.Log

ProgramData\Microsoft\Windows Defender\Support\MPLog-03082021-184449.log

ProgramData\Microsoft\Windows Defender\Support\MPLog-05072021-120450.log

ProgramData\Microsoft\Windows Defender\Support\MPDetection-03182021-105340.log

ProgramData\Microsoft\Windows Defender\Support\MPLog-09122016-043440.log

ProgramData\Microsoft\Windows Defender\Support\MPDetection-09032019-122547.log

ProgramData\Microsoft\Windows Defender\Support\MPDetection-06102019-095254.log

ProgramData\Package Cache\02A26E554FBB4232ACD36E70D09F2C7893D399CD%\localappdata%\temp\Ssm
DB65F37EB5E9}_001_kb3095681.log

ProgramData\Package Cache\02A26E554FBB4232ACD36E70D09F2C7893D399CD%\localappdata%\temp\SsmsSetup\VS2015KB3095681Update

ProgramData\Package Cache\444C320629FA}_001_kb3095681.log

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB%\localappdata%\temp\SsmsSetup\VS2015_003_RoslynLa

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB%\localappdata%\temp\SsmsSetup\VS2015_004_vsta_lan

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB%\localappdata%\temp\SsmsSetup\VS2015_001_vsta_slp

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB%\localappdata%\temp\SsmsSetup\VS2015_002_RoslynLa

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB%\localappdata%\temp\SsmsSetup\VS2015_000_vsta_lsc

ProgramData\Package Cache\5E6157D16EC044A823B2FD2C030ED6DEC2E997E%\localappdata%\temp\SsmsSetup\VSTA2015_001_vsta_hösti

ProgramData\Package Cache\5E6157D16EC044A823B2FD2C030ED6DEC2E997E%\localappdata%\temp\SsmsSetup\VSTA2015_002_vsta_finalli

ProgramData\Package Cache\5E6157D16EC044A823B2FD2C030ED6DEC2E997E%\localappdata%\temp\SsmsSetup\VSTA2015_000_vsta_hösti

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_018_Msi_B

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_020_Msi_B

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_032_vs_iso

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_019_Msi_B

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_021_sdk_t

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_004_vcRun

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_005_vcRun

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_006_vcRun

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_003_vcRun

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_007_vs_vsl

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_008_vsbslr

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_009_vsbslr

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301%\localappdata%\temp\SsmsSetup\VS2015IsoShell_010_netfx

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_011_netfx

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_012_netfx

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_013_netfx

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_014_netfx

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_015_netfx

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_017_MSI-B

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_022_sdk_t

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_023_sqlsys

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_024_share

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_025_help3

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_026_Bliss

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_027_Bliss

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_030_vs_mi

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_031_vs_mi

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_033_vs_iso

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_029_vs_mi

System Volume Information\tracking.log

Users\NET.v2.0\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\NET.v2.0\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\NET.v2.0\ntuser.dat.LOG1

Users\NET.v2.0\ntuser.dat.LOG2

Users\NET.v2.0 Classic\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\NET.v2.0 Classic\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\NET.v2.0 Classic\ntuser.dat.LOG1

Users\NET.v2.0 Classic\ntuser.dat.LOG2

Users\NET.v4.5\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\NET.v4.5\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\NET.v4.5\ntuser.dat.LOG1

Users\NET.v4.5\ntuser.dat.LOG2

Users\NET.v4.5 Classic\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\NET.v4.5 Classic\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\NET.v4.5 Classic\ntuser.dat.LOG1

Users\NET.v4.5 Classic\ntuser.dat.LOG2

Users\AdjSys\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\Ad\Sys\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\Ad\Sys\ntuser.dat.LOG1
Users\Ad\Sys\ntuser.dat.LOG2
Users\Administrator\AppData\Local\ConnectedDevicesPlatform\CDPTTraces.log
Users\Administrator\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log
Users\Administrator\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log
Users\Administrator\AppData\Local\Microsoft\Windows\SettingSync\metastore\edbtmp.log
Users\Administrator\AppData\Local\Microsoft\Windows\SettingSync\metastore\edb00001.log
Users\Administrator\AppData\Local\Microsoft\Windows\SettingSync\metastore\edb00002.log
Users\Administrator\AppData\Local\Microsoft\Windows\SettingSync\metastore\edb.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V010000B.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V01tmp.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V01.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V0100002.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V010000A.log
Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V010000C.log
Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\Temp\StructuredQuery.log
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2bxewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2bxewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2bxewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2bxewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2bxewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2bxewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2bxewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2bxewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2bxewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Windows.MiracastView_cw5n1h2bxewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Windows.MiracastView_cw5n1h2bxewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2bxewy
Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2bxewy\Settings\settings.dat.LOG1
Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2bxewy\Settings\settings.dat.LOG2
Users\Administrator\AppData\Local\Temp\IpsigStub.log
Users\Administrator\AppData\Local\Temp\Wmsetup.log
Users\Administrator\AppData\Local\TileDataLayer\Database\EDBtmp.log
Users\Administrator\AppData\Local\TileDataLayer\Database\EDB00002.log
Users\Administrator\AppData\Local\TileDataLayer\Database\EDB.log
Users\Administrator\ntuser.dat.LOG1
Users\Administrator\ntuser.dat.LOG2
Users\Classic.NET.AppPool\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\Classic.NET.AppPool\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\Classic.NET.AppPool\ntuser.dat.LOG1
Users\Classic.NET.AppPool\ntuser.dat.LOG2
Users\Default\NTUSER.DAT.LOG2
Users\Default\NTUSER.DAT.LOG1
Users\emsadmin\AppData\Local\ConnectedDevicesPlatform\CDPTraces.log
Users\emsadmin\AppData\Local\Microsoft\Internet Explorer\ie4unit-UserConfig.log
Users\emsadmin\AppData\Local\Microsoft\Internet Explorer\ie4unit-ClearIconCache.log
Users\emsadmin\AppData\Local\Microsoft\SQL Server Management Studio\14.0\ComponentModelCache\Microsoft.VisualStudio.Default.catalog
Users\emsadmin\AppData\Local\Microsoft\Windows\SettingSync\metastore\edbtmp.log
Users\emsadmin\AppData\Local\Microsoft\Windows\SettingSync\metastore\edb00001.log
Users\emsadmin\AppData\Local\Microsoft\Windows\SettingSync\metastore\edb00002.log

Users\emsadmin\AppData\Local\Microsoft\Windows\SettingSync\metastore\edb.log
Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\V010001C.log
Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\V010001D.log
Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\V010001E.log
Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\V01.log
Users\emsadmin\AppData\Local\Microsoft\Windows\WebCache\V01tmp.log
Users\emsadmin\AppData\Local\Microsoft\Windows\Windows Anytime Upgrade\Upgrade.log
Users\emsadmin\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\emsadmin\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\Temp\StructuredQuery.log
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB\edb.log
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB\edbtmp.log
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB\edb00006.log
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB\edb00007.log
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB\edb00008.log
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Windows.MiracastView_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Windows.MiracastView_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy
Users\emsadmin\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat.LOG1
Users\emsadmin\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat.LOG2
Users\emsadmin\AppData\Local\Temp\{92aeb63-07b8-4662-94b4-f4bccba37ec}\baseutils.log
Users\emsadmin\AppData\Local\Temp\SSMS\SSMS_20190610_131541566_PID2136_logFile.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_32_sql_ssms_loc_x64_loc.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_3_DACFramework.msi.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_4_SQLServerBestPracticesPolicies.msi.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_5_TSqLanguageService_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_6_sql_diag_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_7_adalsql_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_22_sql_as_oledb_x86.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_23_sql_common_core_x86.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_24_sql_common_core_loc_x86.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_30_sql_ssms_extensions_loc_x86.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_31_sql_ssms_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_33_sql_tools_connectivity_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_18_smo_extensions_loc_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_2_msodbcsql.msi.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_8_conn_info_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_9_conn_info_loc_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_0_SQLSysClrTypes.msi.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_1_sqlncli.msi.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_10_sql_batchparser_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_11_sql_xevent_x64.log
Users\emsadmin\AppData\Local\Temp\SSMS-Setup\SSMS-Setup-ENU_20190610125637_12_sql_xevent_loc_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_13_sql_is_scale_management_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_14_sql_is_scale_management_loc_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_15_sql_dmf_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_16_sql_dmf_loc_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_17_smo_extensions_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_19_smo_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_20_smo_loc_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_34_sql_tools_connectivity_loc_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_21_sql_as_oledb_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_35_ssms_rs_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_36_ssms_as_x64.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_29_sql_ssms_extensions_x86.log
Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_37_SsmsPostInstall_x64.log
Users\emsadmin\AppData\Local\Temp\VSD3298.tmp\install.log
Users\emsadmin\AppData\Local\Temp\VSDA070.tmp\install.log
Users\emsadmin\AppData\Local\Temp\VsHub\Microsoft.VisualStudio.ExtensionManager.HubServiceModule-kitajpem.rgb.log
Users\emsadmin\AppData\Local\Temp\SqlSetup_1.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_amd64_20190610120224_000_vcRuntimeMinimum_x64.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_amd64_20190610120224_001_vcRuntimeAdditional_x64.log
Users\emsadmin\AppData\Local\Temp\SqlSetup.log
Users\emsadmin\AppData\Local\Temp\StructuredQuery.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_amd64_20190610120224.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610120041.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610120041_0_vcRuntimeMinimum_x86.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610120041_1_vcRuntimeAdditional_x86.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_amd64_20190610120118.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_amd64_20190610120118_0_vcRuntimeMinimum_x64.log
Users\emsadmin\AppData\Local\Temp\wmssetup.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_amd64_20190610120118_1_vcRuntimeAdditional_x64.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610120157.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610120157_000_vcRuntimeMinimum_x86.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610120157_001_vcRuntimeAdditional_x86.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610125911.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_amd64_20190610125911.log

Users\emsadmin\AppData\Local\Temp\dd_vcrist_ amd64_20190610125912.log
Users\emsadmin\AppData\Local\Temp\dd_vcrist_x86_20190610130115.log
Users\emsadmin\AppData\Local\Temp\MpSigStub.log
Users\emsadmin\AppData\Local\TileDataLayer\Database\EDB.log
Users\emsadmin\AppData\Local\TileDataLayer\Database\EDBtmp.log
Users\emsadmin\AppData\Local\TileDataLayer\Database\EDB00003.log
Users\emsadmin\Documents\EMS\Log\Debug.log
Users\emsadmin\Documents\EMS\Log\Info.log
Users\emsadmin\ntuser.dat.LOG1
Users\emsadmin\ntuser.dat.LOG2
Users\emsadmin01\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\emsadmin01\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\emsadmin01\ntuser.dat.LOG1
Users\emsadmin01\ntuser.dat.LOG2
Users\emsadmin02\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\emsadmin02\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\emsadmin02\ntuser.dat.LOG1
Users\emsadmin02\ntuser.dat.LOG2
Users\emssasuser\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\emssasuser\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\emssasuser\ntuser.dat.LOG1
Users\emssasuser\ntuser.dat.LOG2
Users\emssqluser\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\emssqluser\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\emssqluser\ntuser.dat.LOG1
Users\emssqluser\ntuser.dat.LOG2
Users\emssuser01\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\emssuser01\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\emssuser01\ntuser.dat.LOG1
Users\emssuser01\ntuser.dat.LOG2
Users\emssuser02\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\emssuser02\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\emssuser02\ntuser.dat.LOG1
Users\emssuser02\ntuser.dat.LOG2

Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\MSSQLSERVER\ntuser.dat.LOG1
Users\MSSQLSERVER\ntuser.dat.LOG2
Users\ReportServer\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\ReportServer\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\ReportServer\ntuser.dat.LOG1
Users\ReportServer\ntuser.dat.LOG2
Users\SQLSERVERAGENT\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\SQLSERVERAGENT\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\SQLSERVERAGENT\ntuser.dat.LOG1
Users\SQLSERVERAGENT\ntuser.dat.LOG2
Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Users\SQLTELEMETRY\ntuser.dat.LOG1
Users\SQLTELEMETRY\ntuser.dat.LOG2
VirtualDirectories\EMSApplicationServer\Log\Error.4.log
VirtualDirectories\EMSApplicationServer\Log\Error.log
VirtualDirectories\EMSApplicationServer\Log\Error.12.log
VirtualDirectories\EMSApplicationServer\Log\Error.14.log
VirtualDirectories\EMSApplicationServer\Log\Error.5.log
VirtualDirectories\EMSApplicationServer\Log\Error.8.log
VirtualDirectories\EMSApplicationServer\Log\Error.0.log
VirtualDirectories\EMSApplicationServer\Log\Error.11.log
VirtualDirectories\EMSApplicationServer\Log\Error.10.log
VirtualDirectories\EMSApplicationServer\Log\Error.9.log
VirtualDirectories\EMSApplicationServer\Log\Error.3.log
VirtualDirectories\EMSApplicationServer\Log\Error.6.log
VirtualDirectories\EMSApplicationServer\Log\Error.7.log
VirtualDirectories\EMSApplicationServer\Log\Error.2.log
VirtualDirectories\EMSApplicationServer\Log\Error.1.log
VirtualDirectories\EMSApplicationServer\Log\Error.13.log
VirtualDirectories\EMSApplicationServer\Log\Warn.log
VirtualDirectories\EMSApplicationServer\Log\Error.14.log

Windows\appcompat\Programs\Amcache.hve.LOG1
Windows\appcompat\Programs\Amcache.hve.LOG2
Windows\assembly\GAC_MSIL\System.IO.Log
Windows\assembly\NativeImages_v2.0.50727_32\System.IO.Log
Windows\assembly\NativeImages_v2.0.50727_64\System.IO.Log
Windows\assembly\NativeImages_v4.0.30319_32\System.IO.Log
Windows\assembly\NativeImages_v4.0.30319_64\System.IO.Log
Windows\debug\sammul.log
Windows\debug\PASSWORD.LOG
Windows\debug\NetSetup.LOG
Windows\Dell\UpdatePackage\log\BrcmSetup.log
Windows\INF\setupapi.dev.log
Windows\INF\setupapi.setup.log
Windows\Logs\CBS\CBS.log
Windows\Logs\CBS\CbsPersist_20191001155012.log
Windows\Logs\CBS\CbsPersist_20190625180445.log
Windows\Logs\DISM\dism.log
Windows\Logs\DPX\setupact.log
Windows\Logs\DPX\setuperr.log
Windows\Logs\SetupCleanupTask\setuperr.log
Windows\Logs\SetupCleanupTask\setupact.log
Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.SqlServer.TransferLoginsTask
Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.SqlServer.TransferLoginsTaskUI
Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualStudio.Dialogs
Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualStudio.ImageCatalog
Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualStudio.ProductKeyDialog
Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualStudio.Text.Logic
Windows\Microsoft.NET\assembly\GAC_MSIL\System.IO.Log
Windows\Microsoft.NET\Framework\v2.0.50727\ngen.log
Windows\Microsoft.NET\Framework\v4.0.30319\ngen.log
Windows\Microsoft.NET\Framework\v4.0.30319\ngen.old.log
Windows\Microsoft.NET\Framework\v4.0.30319\ngen.old.log
Windows\Microsoft.NET\Framework64\v2.0.50727\ngen.log
Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log

Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.old.log
Windows\Panther\UnattendGC\setupact.log
Windows\Panther\UnattendGC\setuperr.log
Windows\Panther\DDACL.sys.log
Windows\Panther\cbs.log
Windows\Panther\setupact.log
Windows\Panther\setuperr.log
Windows\Performance\WinSAT\winsat.log
Windows\security\database\edb.log
Windows\security\database\edbtmp.log
Windows\security\logs\scesetup.log
Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG1
Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG2
Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpCmdRun.log
Windows\ServiceProfiles\NetworkService\debug\NetSetup.LOG
Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG2
Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG1
Windows\SoftwareDistribution\DataStore\Logs\edb00222.log
Windows\SoftwareDistribution\DataStore\Logs\edb00227.log
Windows\SoftwareDistribution\DataStore\Logs\edb00223.log
Windows\SoftwareDistribution\DataStore\Logs\edb00224.log
Windows\SoftwareDistribution\DataStore\Logs\edb00225.log
Windows\SoftwareDistribution\DataStore\Logs\edb0022A.log
Windows\SoftwareDistribution\DataStore\Logs\edb0022C.log
Windows\SoftwareDistribution\DataStore\Logs\edb0022D.log
Windows\SoftwareDistribution\DataStore\Logs\edb00230.log
Windows\SoftwareDistribution\DataStore\Logs\edb.log
Windows\SoftwareDistribution\DataStore\Logs\edbtmp.log
Windows\SoftwareDistribution\DataStore\Logs\edb00226.log
Windows\SoftwareDistribution\DataStore\Logs\edb0022B.log
Windows\SoftwareDistribution\DataStore\Logs\edb00228.log
Windows\SoftwareDistribution\DataStore\Logs\edb00229.log
Windows\SoftwareDistribution\DataStore\Logs\edb0022E.log
Windows\SoftwareDistribution\DataStore\Logs\edb0022F.log

Windows\SoftwareDistribution\ReportingEvents.log

Windows\System32\catroot2\edb00018.log

Windows\System32\catroot2\edb0001B.log

Windows\System32\catroot2\edb0001C.log

Windows\System32\catroot2\edb0001D.log

Windows\System32\catroot2\edb.log

Windows\System32\catroot2\edb00013.log

Windows\System32\catroot2\edb00014.log

Windows\System32\catroot2\edb00015.log

Windows\System32\catroot2\edb00016.log

Windows\System32\catroot2\edb00017.log

Windows\System32\catroot2\edb00019.log

Windows\System32\catroot2\edb0001A.log

Windows\System32\catroot2\edbtimp.log

Windows\System32\config\RegBack\SECURITY.LOG1

Windows\System32\config\RegBack\SECURITY.LOG2

Windows\System32\config\RegBack\SOFTWARE.LOG1

Windows\System32\config\RegBack\SOFTWARE.LOG2

Windows\System32\config\RegBack\SYSTEM.LOG1

Windows\System32\config\RegBack\SYSTEM.LOG2

Windows\System32\config\RegBack\DEFAULT.LOG1

Windows\System32\config\RegBack\DEFAULT.LOG2

Windows\System32\config\RegBack\SAM.LOG1

Windows\System32\config\RegBack\SAM.LOG2

Windows\System32\config\BBI.LOG1

Windows\System32\config\BCD-Template.LOG

Windows\System32\config\DEFAULT.LOG2

Windows\System32\config\ELAM.LOG1

Windows\System32\config\SAM.LOG2

Windows\System32\config\SECURITY.LOG2

Windows\System32\config\DEFAULT.LOG1

Windows\System32\config\DRIVERS.LOG1

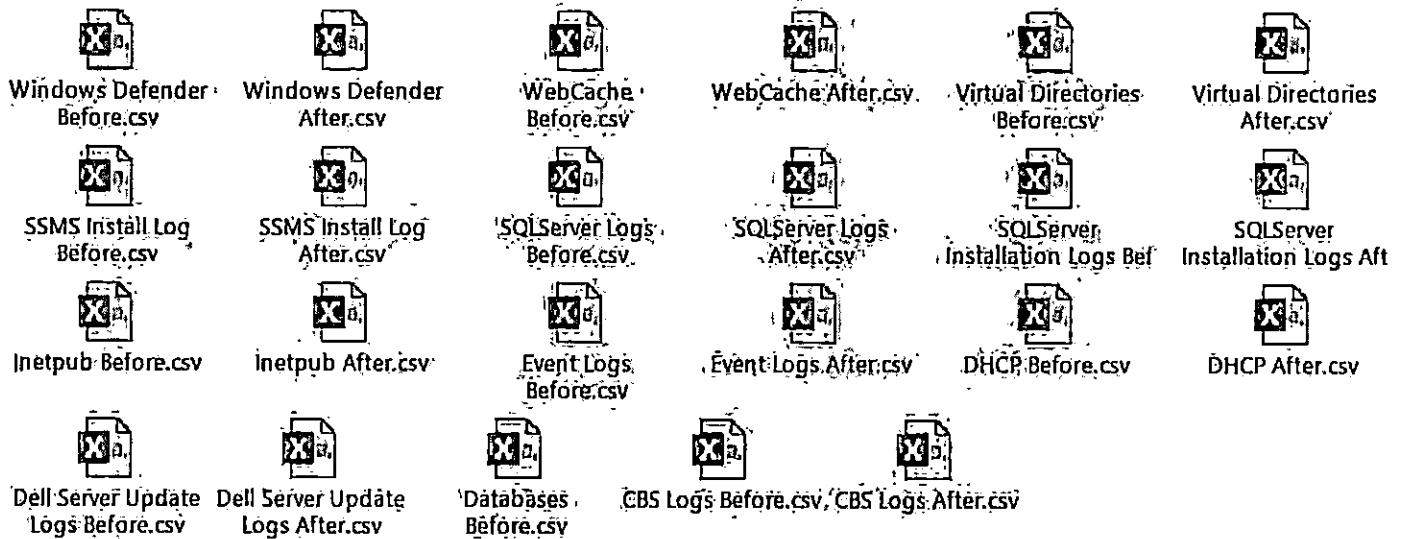
Windows\System32\config\SAM.LOG1

Windows\System32\config\COMPONENTS.LOG2

Windows\System32\config\SECURITY.LOG1

APPENDIX B. SUPPORTING DOCUMENTATION: FILE DETAILS AND HASH SETS FOR SCREENSHOTS

The files below provide integrity data for the graphic screenshots in this document. Each comma-separated-variable (csv) file listed here contain the file name with its full path (e.g., directory structure) and message digest hash values (MD5 and SHA1 algorithms). Due to the length of the data contained in these files, they are provided in a compact disc (CD) addendum to this report.



APPENDIX C. MICROSOFT EVENT LOG FILES

Files in this list were ALL present in the EMS Server Before image. Files listed in RED were deleted or overwritten. Significantly, from their filenames alone, they are OBVIOUSLY Election-Related Records, "Archive-EMS-System-..."

Logs\Microsoft-Windows-Kernel-WHEA%4Errors.evtx
Logs\Key Management Service.evtx
Logs\Application.evtx
Logs\HardwareEvents.evtx
Logs\Internet Explorer.evtx
Logs\Microsoft-Client-Licensing-Platform%4Admin.evtx
Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx
Logs\Microsoft-Windows-AppReadiness%4Admin.evtx
Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx
Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx
Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx
Logs\Microsoft-Windows-Containers-Wcifs%4Operational.evtx
Logs\Microsoft-Windows-Containers-Wcnfs%4Operational.evtx
Logs\Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx
Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx
Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx
Logs\Microsoft-Windows-DeviceSetupManager%4Admin.evtx
Logs\Microsoft-Windows-DeviceSetupManager%4Operational.evtx
Logs\Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.evtx
Logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx
Logs\Microsoft-Windows-Dhcpv6-Client%4Admin.evtx
Logs\Microsoft-Windows-Hyper-V-Guest-Drivers%4Admin.evtx
Logs\Microsoft-Windows-International%4Operational.evtx
Logs\Microsoft-Windows-AppReadiness%4Operational.evtx
Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx
Logs\Microsoft-Windows-Kernel-IO%4Operational.evtx
Logs\Microsoft-Windows-Kernel-EventTracing%4Admin.evtx
Logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx
Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx
Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx
Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx
Logs\Microsoft-Windows-Known Folders API Service.evtx
Logs\Microsoft-Windows-Liveld%4Operational.evtx
Logs\Microsoft-Windows-MUI%4Admin.evtx
Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx
Logs\Microsoft-Windows-MUI%4Operational.evtx
Logs\Microsoft-Windows-NCSI%4Operational.evtx
Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx

Logs\Microsoft-Windows-Ntfs%4Operational.evtx
Logs\Microsoft-Windows-Ntfs%4WHC.evtx
Logs\Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx
Logs\Microsoft-Windows-SettingSync%4Debug.evtx
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
Logs\Microsoft-Windows-Kernel-PnP%4Configuration.evtx
Logs\Microsoft-Windows-SettingSync%4Operational.evtx
Logs\Microsoft-Windows-Shell-Core%4ActionCenter.evtx
Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx
Logs\Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx
Logs\Microsoft-Windows-Shell-Core%4Operational.evtx
Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx
Logs\Microsoft-Windows-SMBClient%4Operational.evtx
Logs\Microsoft-Windows-SmbClient%4Security.evtx
Logs\Microsoft-Windows-SMBServer%4Audit.evtx
Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx
Logs\Microsoft-Windows-SMBServer%4Operational.evtx
Logs\Microsoft-Windows-SMBServer%4Security.evtx
Logs\Microsoft-Windows-SMBWitnessClient%4Admin.evtx
Logs\Microsoft-Windows-SMBWitnessClient%4Informational.evtx
Logs\Microsoft-Windows-StateRepository%4Operational.evtx
Logs\Microsoft-Windows-StateRepository%4Restricted.evtx
Logs\Microsoft-Windows-TaskScheduler%4Maintenance.evtx
Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx
Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
Logs\Microsoft-Windows-Store%4Operational.evtx
Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
Logs\Microsoft-Windows-User-Profile-Service%4Operational.evtx
Logs\Microsoft-Windows-UserPnp%4ActionCenter.evtx
Logs\Microsoft-Windows-UserPnp%4DeviceInstall.evtx
Logs\Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx
Logs\Microsoft-Windows-Wcmsvc%4Operational.evtx
Logs\Microsoft-Windows-Windows Defender%4Operational.evtx
Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx
Logs\Microsoft-Windows-WinNet-Config%4ProxyConfigChanged.evtx
Logs\Microsoft-Windows-WinLogon%4Operational.evtx
Logs\Microsoft-Windows-WinRM%4Operational.evtx
Logs\Setup.evtx
Logs\Windows PowerShell.evtx

Logs\Microsoft-Windows-Firewall-With-Advanced-Security\Firewall.evtx
Logs\Microsoft-Windows-WMI-Activity\Operational.evtx
Logs\System.evtx
Logs\Security.evtx
Windows\System32\winevt\Logs\Setup.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-02-27-12-21-20-622.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-11-20-46-32-189.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-06-30-13-45-03-347.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-08-02-26-04-899.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-30-19-26-37-188.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-04-08-05-33-867.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-30-16-29-10-602.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-15-15-07-04-381.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-02-02-52-11-569.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-19-00-10-16-214.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-26-22-08-42-827.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-11-22-05-26-089.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-23-04-20-21-835.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-26-12-11-25-223.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-15-07-09-24-325.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-04-04-35-23-707.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-07-21-05-41-859.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-18-19-18-33-633.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-23-20-20-681.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-07-22-53-09-400.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-09-05-03-069.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-03-17-30-918.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-02-11-09-22-083.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-15-51-43-896.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-19-15-04-259.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-28-04-14-58-545.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-06-04-10-43-774.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-24-00-59-56-063.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-08-17-03-22-249.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-10-09-23-03-203.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-06-16-37-56-482.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-02-15-06-36-405.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-07-05-51-17-641.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-06-06-07-29-506.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-27-06-12-01-889.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-14-02-20-35-061.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-16-20-09-20-723.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-26-09-07-58-407.evtx

Windows\System32\winevt\Logs\Archive-EMS System-2020-07-08-10-16-08-709.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-26-06-16-16-735.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-21-16-36-38-559.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-03-08-53-17-828.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-10-23-15-37-23-347.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-13-00-00-07-540.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-21-03-24-37-573.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-15-03-21-17-842.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-10-01-06-03-529.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-25-05-09-12-916.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-22-13-12-21-043.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-06-08-06-21-993.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-05-17-16-37-197.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-23-08-11-827.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-17-01-19-18-484.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-01-39-07-647.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-04-12-10-17-214.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-12-02-56-47-489.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-07-26-54-297.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-04-04-03-42-737.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-16-16-31-58-059.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-21-12-09-41-781.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-28-14-04-05-771.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-12-22-02-14-487.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-13-18-05-49-770.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-17-19-10-01-322.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-05-14-13-33-324.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-13-10-56-695.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-28-22-08-50-835.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-17-11-04-36-787.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-05-00-03-39-390.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-12-10-03-10-333.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-20-40-41-039.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-24-11-15-42-872.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-18-17-48-53-388.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-09-10-14-15-715.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-31-11-01-47-908.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-27-08-29-08-399.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-14-23-29-04-158.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-24-21-04-12-832.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-21-04-04-25-803.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-01-07-03-50-651.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-14-18-29-08-151.evtx

Windows\System32\winevt\Logs\Archive-EMS System-2021-05-11-21-02-29-740.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-03-11-33-19-283.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-19-20-02-44-037.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-28-20-58-32-283.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-16-03-02-57-774.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-01-21-14-15-340.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-08-12-31-149.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-22-17-12-11-701.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-05-45-04-636.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-05-12-32-06-091.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-26-13-42-04-162.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-16-14-59-42-045.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-23-13-23-46-471.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-18-23-53-08-392.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-13-14-26-512.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-27-17-59-53-690.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-20-09-29-41-350.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-20-07-59-19-878.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-31-02-47-11-038.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-29-23-11-26-924.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-09-05-29-49-411.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-26-06-11-56-096.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-00-00-39-858.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-18-58-50-004.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-28-08-06-44-934.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-11-14-07-34-718.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-15-07-27-29-016.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-04-17-16-43-223.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-24-22-45-04-435.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-20-18-16-33-823.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-18-12-49-02-987.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-13-08-24-43-079.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-22-12-08-49-154.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-30-02-15-24-619.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-22-17-53-50-782.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-11-17-12-21-460.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-18-20-12-44-811.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-02-14-34-04-967.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-07-10-51-04-386.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-11-05-09-09-286.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-31-12-27-41-741.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-22-20-55-04-936.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-01-03-27-07-105.evtx

Windows\System32\winevt\Logs\Archive-EMS System-2021-04-09-17-04-07-509.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-09-07-12-48-391.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-11-00-11-12-292.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-12-21-57-907.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-03-08-03-17-087.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-18-13-07-673.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-08-27-17-53-57-312.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-30-01-16-19-620.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-19-51-20-073.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-02-24-44-262.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-23-57-17-682.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-08-20-31-15-022.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-21-34-01-652.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-02-16-11-00-907.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-10-17-14-18-337.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-16-31-18-634.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-17-35-55-190.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-10-17-26-50-697.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-08-21-07-21-169.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-22-01-49-473.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-15-41-56-864.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-14-16-397.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-25-20-742.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-33-50-215.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-46-57-607.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-17-20-24-507.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-07-23-24-216.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-14-51-41-139.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-04-06-37-355.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-09-54-24-839.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-14-52-50-172.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-06-37-33-489.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-03-16-22-000.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-19-02-14-166.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-00-50-01-529.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-01-35-37-340.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-14-00-17-879.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-17-23-46-597.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-20-37-42-553.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-09-03-54-186.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-10-43-31-360.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-04-55-44-339.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-22-18-50-801.evtx

Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-19-47-50-347.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-06-34-10-708.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-02-28-13-043.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-21-29-43-807.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-00-46-23-325.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-18-09-30-390.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-14-03-47-942.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-11-36-14-332.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-11-32-36-872.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-08-16-00-636.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-05-48-27-189.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-12-25-20-731.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Operational.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-19-09-27-36-681.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Security.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-23-03-48-10-012.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-14-17-50-17-089.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-22-06-31-22-632.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-03-10-49-41-423.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%4FilterNotifications.evtx
Windows\System32\winevt\Logs\DhcpAdminEvents.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-26-00-51-55-728.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-07-05-09-14-598.evtx
Windows\System32\winevt\Logs\DNS Server.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DNSServer%4Audit.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-10-23-29-48-856.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-18-12-10-49-482.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-09-02-13-32-58-546.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-29-19-12-25-021.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Audit.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Maintenance.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-VDRVROOT%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-VHDMP-Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-International%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-MUI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-MUI%4Admin.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSe
Windows\System32\winevt\Logs\Microsoft-Windows-Iphlpsvc%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.ev
Windows\System32\winevt\Logs\Microsoft-Client-Licensing-Platform%4Admin.evtx
Windows\System32\winevt\Logs\System.evtx
Windows\System32\winevt\Logs\Application.evtx
Windows\System32\winevt\Logs\Security.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcpv6-Client%4Admin.evtx
Windows\System32\winevt\Logs\Windows PowerShell.evtx
Windows\System32\winevt\Logs\Key Management Service.evtx
Windows\System32\winevt\Logs\Internet Explorer.evtx
Windows\System32\winevt\Logs\HardwareEvents.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Wcmsvc%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant
Windows\System32\winevt\Logs\Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.e
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WinRM%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4DeviceInstall.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4ActionCenter.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Ad
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%4Restricted.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-PnP%4Configuration.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-IO%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4Errors.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-NCSI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupManager%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupManager%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wclfs%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wcnfs%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Service%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-LiveId%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBClient%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Security.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Winlogon%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4Debug.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DateTimeControlPanel%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API Service.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4ActionCenter.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-DeploymentProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Store%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TWinUI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Inventory.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-BackgroundTaskInfrastructure%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-MultiMachine%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-MultiMachine%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Forwarding%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-MgmtProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScan%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScan%4CrashRecovery.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-ManagementAgent%4WHC.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-ClassPnP%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-RestartManager%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PLA%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CAPI2%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-NlaSvc%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PCW%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Storport%4Operational.evtx
Windows\System32\winevt\Logs\EMS System.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application Server-Applications%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Application Server-Applications%4Operational.evtx
Windows\System32\winevt\Logs\DVS Adjudication.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CloudStorageWizard%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-AppV-Client%4Virtual Applications.evtx
Windows\System32\winevt\Logs\Microsoft-Rdms-UI%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Rdms-UI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualization-Agent Driver%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualization-App Agent%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualization-IPC%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualization-SQM Uploader%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AAD%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-All-User-Install-Agent%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AllJoyn%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppHost%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppID%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ApplicabilityEngine%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4EXE and DLL.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4MSI and Script.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Packaged app-Deployment.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Packaged app-Execution.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AppxPackaging%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccess%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccessBroker%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4CaptureMonitor.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4PlaybackManager.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-Authentication User Interface%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Backup.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-BestPractices%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Biometrics%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-BthLEPrepairing%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-MTPEnum%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-BranchCacheSMB%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServices-Deployment%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServicesClient-Lifecycle-System%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServicesClient-Lifecycle-User%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Compat-Appraiser%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CoreApplication%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRecovery-Client%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRecovery-Server%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DAL-Provider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceGuard%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Devices-Background%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSync%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripted%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripted%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-ScriptedDiagnosticsProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Networking%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DirectoryServices-Deployment%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnostic%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticDataCollector%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticResolver%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EapHost%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-RasChap%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-RasTls%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Sim%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ttls%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-Regular%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-TCB%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EmbeddedAppLauncher%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentPolicyWebService%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentWebService%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-EventCollector%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-Heap%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-FederationServices-Deployment%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-ServerManager-EventProvider%4Admin.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-ServerManager-EventProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-FileShareShadowCopyProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-FMS%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Folder-Redirection%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-NdisImPlatform%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-GenericRoaming%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Help%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Hyper-V-Guest-Drivers%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-IdCtrls%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-IKE%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-International-RegionalOptionsControlPanel%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-KdsSvc%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ApphelpCache%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-EventTracing%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WDI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-LanguagePackSetup%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ManagementTools-RegistryProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ManagementTools-TaskManagerProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-MemoryDiagnostics-Results%4Debug.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-MiStreamProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadband-Experience-Parser-Task%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadband-Experience-SmsRouter%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Mprddm%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-MsLbfoProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-NetworkLocationWizard%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-NTLM%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-OfflineFiles%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-OneBackup%4Debug.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-OOBE-Machine-DUI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PackageStateRoaming%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagnostic.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionRuntime%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionSensorDataService%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-User Control Panel%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Policy%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell-DesiredStateConfiguration-FileDownloadManager%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PrintBRM%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-PrintService%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ReFS%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Regsvr32%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and Desktop Connections%4Admin.evtx

Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and Desktop Connections%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-RemoteFX-Synth3dvs%4Admin.e
Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.ev
Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Resolver%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ScmBus%4Certification.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ScmDisk0101%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SearchUI%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Security-Audit-Configuration-Client%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Security-EnterpriseData-FileRevocationManager%4Operati
Windows\System32\winevt\Logs\Microsoft-Windows-Security-Netlogon%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-GenuineCenter-Logging%4Operational.ev
Windows\System32\winevt\Logs\Microsoft-Windows-Security-UserConsentVerifier%4Audit.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ServerEssentials-Deployment%4Deploy.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-ConfigureSMRemoting%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azure%4Debug.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azure%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SilProvider%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-Audit%4Authentication.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-DeviceEnum%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-VCARD-Module%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-VCARD-Module%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBDirect%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClient%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClient%4Informational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Tiering%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StorageManagement%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Driver%4Diagnostic.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Driver%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-SpaceManager%4Diagnostic.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-SpaceManager%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-SystemSettingsThreshold%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TCP/IP%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-ClientUSBDevices%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-ClientUSBDevices%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-PnPDevices%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-PnPDevices%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.ev
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operati

Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-ServerUSBDevices%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-ServerUSBDevices%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-SessionBroker-Client%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-SessionBroker-Client%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TZSync%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-TZUtil%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-UAC%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-UAC-FileVirtualization%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-User-Device-Registration%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-User-Loader%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-VerifyHardwareSecurity%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Volume%4Diagnostic.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-VPN-Client%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-VPN%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WFP%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Win32k%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Winsock-WS2HELP%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Wired-AutoConfig%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-Workplace-Join%4Admin.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WPD-CompositeClassDriver%4Operational.evtx
Windows\System32\winevt\Logs\Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx
Windows\System32\winevt\Logs\SMSEAPI.evtx

APPENDIX D. LIST OF FIGURES

Figure 1 – EMS Server (5.11-CO) Image Attributes Before	8
Figure 2 - EMS Server (5.13) Image Attributes After	9
Figure 3 – EMS Server (5.11-CO) System Data Sources Before	11
Figure 4 - EMS Server (5.13) System Data Sources After	11
Figure 5 - EMSSERVER (5.11-CO) Disk Partition Structure Before.....	12
Figure 6- EMSSERVER (5.13) Disk Partition Structure After	12
Figure 7 - Server Disk Partition and Directory Changes.....	13
Figure 8 - EMS Server (5.11-CO) Web Server Log Files Before.....	15
Figure 9 - EMS Server (5.13) Web Server Log Files After	15
Figure 10 - EMS Server (5.11-CO) MS SQL Server Installation Log Files Before	17
Figure 11 - EMS Server (5.13) MS SQL Server Installation Log Files After	17
Figure 12 - Example of Log File Content from EMS Server (5.11-CO) Before	18
Figure 13 - EMS Server (5.11-CO) SQL Server Log Files Before	19
Figure 14 - EMS Server (5.13) SQL Server Log Files After	19
Figure 15 - EMS Server (5.11-CO) Dell Server Update Files Before	20
Figure 16 - EMS Server (5.13) Dell Server Update Files After	20
Figure 17 - EMS Server (5.11-CO) Administrator WebCache Log Files Before.....	22
Figure 18 - EMS Server (5.13) Administrator WebCache Log Files After	22
Figure 19 - EMS Server (5.11-CO) "emsadmin" WebCache Log Files Before	23
Figure 20 -EMS Server (5.13) "emsadmin" WebCache Log Files After	23
Figure 21 - EMS Server (5.11-CO) Webcache Log File Content Before.....	24
Figure 22 - EMS Server (5.11-CO) Webcache Log File Content Before - II	24
Figure 23 - EMS Server (5.11-CO) SSMS Log Files Before	25
Figure 24 - EMS Server (5.13) SSMS Log Files After.....	25
Figure 25 - EMS Server (5.11-CO) CBS Log Files Before	26
Figure 26 - EMS Server (5.13) CBS Log Files After	26
Figure 27 - EMS Server (5.11-CO) Election Databases Before.....	27
Figure 28 - EMS Server (5.13) Election Databases After	27
Figure 29 - EMS Server (5.11-CO) DHCP Log Files Before	28
Figure 30 - EMS Server (5.13) DHCP Log Files After	28
Figure 31 - EMS Server (5.11-CO) Event Logs Before	29
Figure 32 - EMS Server (5.13) Event Logs After.....	29
Figure 33 - Examples of Election Data Missing After Update.....	30
Figure 34 - EMS Server (5.11-CO) System Users Before	31
Figure 35 - EMS Server (5.13) System Users After	31
Figure 36 - EMS Server (5.11-CO) Virtual Directory Log Files Before	32
Figure 37 - EMS Server (5.13) Virtual Directory Log Files After	32
Figure 38 - EMS Server (5.11-CO) Windows Defender Log Files Before Dominion Update:.....	33
Figure 39 - EMS Server (5.13) Windows Defender Log Files After	33
Figure 40 - EMS Server Before/After .log File Comparison List.....	34
Figure 41 - EMS Server (5.11-CO) List of .evtx Event Log Files Before.....	36
Figure 42 - EMS Server (5.13) List of .evtx Event Log Files After	36

APPENDIX E. 2002 VOTING SYSTEMS STANDARDS (VSS)

The 2002 VSS explicitly states:

"2.2.4.1 Common Standards

To ensure system integrity, all system shall:

...

g. Record and report the date and time of normal and abnormal events;

h. Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.)

i. Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator; and

J. Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.

Furthermore, in 2.2.5.3, COTS (Commercial Off-The-Shelf) General Purpose Computer System Requirements, the 2002 VSS states:

Further requirements must be applied to COTS operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations (or "PCs"), including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these COTS systems is vulnerable to unintended effects from other user sessions, applications, and utilities, executing on the same platform at the same time as the election software.

"Simultaneous processes" of concern include unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted.

First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.

Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.

Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.

And, in 4.3 Data and Document Retention, the 2002 VSS states:

All systems shall:

- a. Maintain the integrity of voting and audit data during an election, and for at least 22 months thereafter, a time sufficient in which to resolve most contested elections and support other activities related to the reconstruction and investigation of a contested election; and
- b. Protect against the failure of any data input or storage device at a location controlled by the jurisdiction or its contractors, and against any attempt at improper data entry or retrieval.

And the 2002 VSS states, in 4.4.3 In-Process Audit Records:

In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain:

- a. Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:
 - 1) The source and disposition of system interrupts resulting in entry into exception handling routines;
 - 2) All messages generated by exception handlers;
 - 3) The identification code and number of occurrences for each hardware and software error or failure;
 - 4) Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing;
 - 5) Other exception events such as power failures, failure of critical hardware components, data transmission errors, or other type of operating anomaly;
- b. Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to: Diagnostic and status messages upon startup;
 - 2) The "zero totals" check conducted before opening the polling place or counting a precinct centrally;
 - 3) For paper-based systems, the initiation or termination of card reader and communications equipment operation; and
 - 4) For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e., each voter's transaction as an event). This data can be compared with the publiccounter for reconciliation purposes;
- c. Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors; and
- d. System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed.

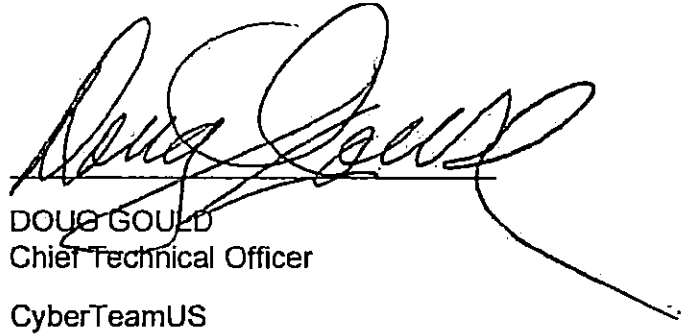
And section 6.5.5, Shared Operating Environment, in the the 2002 VSS states:

Ballot recording and vote counting can be performed in either a dedicated or nondedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data. Systems that use a shared operating environment shall:

- a. Use security procedures and logging records to control access to system functions;
- b. Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well;
- c. Controlled system access by means of passwords, and restriction of account access to necessary functions only; and
- d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources.

The foregoing Forensic Examination and Report was prepared by me and I am responsible for its content.

This 15th day of September, 2021.



DOUG GOULD
Chief Technical Officer
CyberTeamUS

Doug Gould Biography

Doug Gould is an expert in Cyber Security with more than 40 years' experience in the field. Doug retired from AT&T after 31 years, where he served as Chief Cyber Security Strategist. He currently serves as Chief Technical Officer at CyberTeamUS.



Doug began at AT&T with Bell Laboratories, serving in the Semiconductor Laser Development department and later in the Bell Lab's Security Group, as a delegate to the Bell Labs' Unix Systems

Subcommittee, was an early pioneer in the field of Computer Forensics and won a Bell Labs Innovation Award. At AT&T he designed the security architecture for one of the largest states in the US, consulted with cabinets of the nations' largest corporations and designed the first healthcare network fully compliant with Healthcare Information Exchange standards. Outside AT&T, he has overseen security for a US Government Agency and has solved major cases for the FBI and Secret Service; he has served as an Officer of the Court as a forensic expert and has been an expert witness in landmark cybersecurity cases. He designed security architectures for DoD networks including some of the most sensitive areas of the Government. Doug has owned and led several professional services firms in the Information Security field. He served on the NC Council for Entrepreneurial Development and has consulted with many companies about the complex integration of business and technology.

Doug is the past president of Eastern North Carolina InfraGard, the public-private partnership between the nation's critical infrastructure operators and the US Intelligence community.

Doug's background is at the Master's level in Electrical Engineering, Computer Science, Computer Security and Business Administration.

He is a subject matter expert in:

- Strategic Enterprise Security
- Security Architecture & Design (including network Micro-Segmentation)
- Security Governance
- Risk Management

- Security Device Technologies (Firewalls, IDS/IPS, DLP, SIEMs, Encryption, VPNs, Unified Threat Management, etc., Enterprise, Remote and Cloud)
- Information Forensics (Computer & Network Forensics)
- Public Key Infrastructures
- Identity and Access Management
- Authentication, Authorization and Access Control (incl Biometrics)
- Regulatory Compliance
- Physical Security (Threat Assessment/Risk Analysis, TSCM, Access Control, Counterterrorism & Counterintelligence, facility and site protection)
- Business Continuity & Disaster Recovery Planning
- Response & Recovery Strategy
- Threat Intelligence
- Intelligence Analysis

Doug served as Chief Information Security Officer at the World Institute for Security Enhancement, has written advanced security courses, developed advanced security methodologies and has taught government, private sector professionals and law enforcement agents information security, computer forensics, advanced computer forensic sciences and Technical Surveillance Countermeasures (TSCM).

Doug holds numerous certifications in security including the CISSP and Certified Anti-Terrorism Specialist (CAS), as well as numerous instructor certifications in security.

Doug currently serves as Chief Technical Officer at CyberTeamUS.

He is a Vietnam-era US Navy Veteran where he worked in Electronic Warfare and Electronic Intelligence.

Doug is an invited conference speaker.

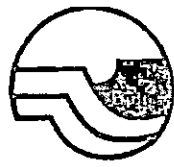
Doug Gould Forensic Addendum

Major Forensic Cases

- 1986 – Disclosure of National Security Information
Discovered a leak of highly classified information and was able to identify the perpetrator within a group of 15 people. The FBI and US Naval Investigative Service brought this to resolution.
- Early 1990's – US Secret Service investigation, "Mothers of Doom" hacker case
At USSS Evidence Lab, in response to a request for assistance from USS SA Jack Lewis, performed evidence recovery and identified 800 pages of evidence, invalidating immunity of a suspect's testimony in a proffer session.
- Late 1990's – Interpath, a North Carolina Internet Service Provider (ISP)
This ISP was a tier-1 (top level) provider infected with Stacheldraht malware. Investigated the live (running) server and identified that all evidence on disc had been deleted. The only remaining evidence was a running program in memory, which was recovered. This case changed the Best Practice in Forensics – no longer is the first step necessarily removing the power. Had that been done no evidence would remain in this case.
- Late 1990's – As senior security administrator for the US EPA, investigated a complaint from the White House of computer intrusions and discovered an international attack involving 4 countries. Wrote monitoring and tracking software to capture the perpetrator online, brought together the FBI, Royal Canadian Mounted Police (RCMP), Scotland Yard and Deutsche Bundespost in a live investigation tracking the intruder resulting in an arrest in Germany.
- South Carolina – A Public Works supervisor accused of violation of county policy was fired and brought countersuit. Forensic investigation recovered 4 3" thick binders of evidence showing sexual misconduct. Countersuit dismissed.
- Discovered Al Qaida attack plans targeting US Soil. Working with the FBI, the perpetrator, who was a foreign citizen in the US. Arrest made within 48 hours and the attack was thwarted.
- Mid-2000's – Florida vs. Rabinowicz – in a case where possession of contraband was the only element of proof, stipulated that the contraband was authentic and present. I proved forensically that the defendant was not technically in possession of the evidence and that evidence was planted. Qualified as an expert witness and provided expert testimony in this case.
- Mid-2000's – Identified a leak of national security from Oak Ridge National Laboratory involving chemical weapon information using forensic analysis and was able to identify the perpetrator. DSS responded and resolved the case.
- Mid-2000's – Investigated sabotage of a health industry contractor. The systems administrator had been fired and sabotaged the system. Solved the case and the administrator went to prison.

Instructor of Forensics

- Taught Forensics and Advance Forensic Techniques to State Law Enforcement, Military and major corporate customers at the World Institute for Security Enhancement.
- Taught Technical Surveillance Countermeasures (TSCM) course for government and industry at the World Institute for Security Enhancement.
- Wrote the entire course and taught the entire CISSP curriculum at Able Information Systems.



MESA COUNTY
CLERK & RECORDER

Hon. Janet Rowland
Board of County Commissioners
544 Rood Ave. Grand Junction, CO

March 1, 2022

RE: Forensic Report No. 2 on EMS Server Images

Dear Commissioner Rowland:

Enclosed is the second report, in electronic and hard copy form, from the cybersecurity experts who have continued to analyze the forensic images of the drive of the DVS Democracy Suite Election Management System in my office which we used for the management of the 2020 general election and the 2021 City Council Election. As you know, I had these images taken to preserve election records and help determine whether the county should continue to utilize the equipment from this vendor. Because the enclosed report reveals shocking vulnerabilities and defects in the current system, placing my office and other county clerks in legal jeopardy, I am forwarding this to the county attorney and to you so that the county may assess its legal position appropriately. Then, the public must know that its voting systems are fundamentally flawed, illegal, and inherently unreliable.

From my initial review of the report, it appears that our county's voting system was illegally certified and illegally configured in such a way that "vote totals can be easily changed." We have been assured for years that external intrusions are impossible because these systems are "air gapped," contain no modems, and cannot be accessed over the internet. It turns out that these assurances were false. In fact, the Mesa County voting system alone was found to contain thirty-six (36) wireless devices, and the system was configured to allow "any computer in the world" to connect to our EMS server. For this and other reasons—for example, the experts found uncertified software that had been illegally installed on the EMS server—our system violates the federal Voting System Standards that are mandated by Colorado law.

As the county officer elected to manage our elections in accordance with the law, I cannot hide behind the Secretary of State's certification of the Democracy Suite system and ignore the numerous and profound deficiencies revealed in this report. As the experts point out, the Secretary of State's certification itself was unlawful, based as it was on testing performed by an unaccredited lab, a lab that missed 100% of the security issues that render the system unusable, uncertifiable, and illegal. The county must reassess its recently-renewed lease agreement and consider its legal options immediately. We cannot continue to use this equipment. Please respond once you have read the enclosed report.

Very truly yours

A handwritten signature in black ink, appearing to read "Tina M. Peters".

Tina M. Peters

Tina M. Peters

Mesa County Clerk & Recorder

200 S. Spruce Street | Grand Junction, CO 81501

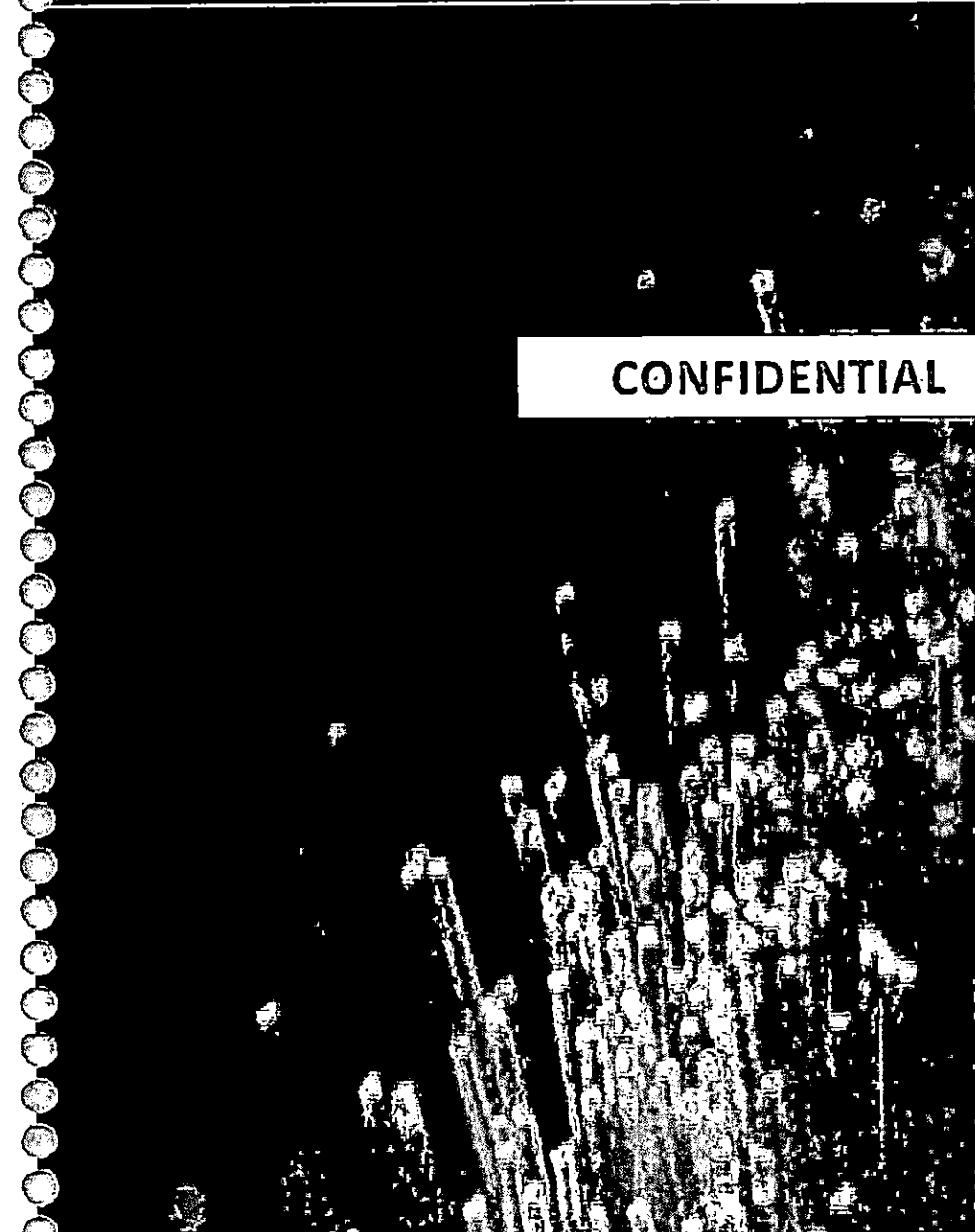
Tina.Peters@MesaCounty.US Office(970) 244-1714 Cell (970) 812-2610



**Mesa County
Colorado
Voting System**

**Report #2
Forensic Examination and Analysis Report**

CONFIDENTIAL



February 28, 2022

Table of Contents

Executive Summary 1

Critical Discoveries 1

 Most Significant Findings: The Voting System is Not Secure, Violates Security Standards Required By State and Federal Law 2

 “Back-Door” found in Voting System; Uncertified Software Invalidates Voting System Certification ... 2

 Capability to Easily “Flip” Election Results Demonstrated 3

 Voting System Components Manufactured and Assembled in China and Mexico 3

 Voting System Presents an Immediate threat and is Dangerous to use in the upcoming 2022 election3

Key Findings 5

 Analysis Summary: Compliance of Mesa County, Colorado, DVS D-Suite systems with the law 7

Examination Methodology 15

FORENSIC ANALYSIS..... 19

System identification 19

Authenticity 21

Chain of Custody..... 21

 Tools Used..... 22

TEST PREPARATION 22

Finding 1: 25

EXAMINATION OBJECTIVE 1: 34

Finding 2: 51

Finding 3: 52

Finding 4: 52

EXAMINATION RESULT 1 52

EXAMINATION OBJECTIVE 2: 53

Finding 5: 68

Finding 6: 75

EXAMINATION RESULT 2: 75

EXAMINATION OBJECTIVE 3: 76

EXAMINATION RESULT 3: 89

Conclusion..... 92

Appendix A. Compliance Requirements 96

Federal Election Commission 2002 Voting Systems Standards (VSS) 96

APPLICABILITY 96

 VSS V1, 1.6, page 1-13: 96

 VSS V1, 2.1, page 2-19: 97

 VSS V1, 2.2, page 2-20: 97

DATA RETENTION..... 98

Election Record Definition, Scope and Content 98

 VSS V1, 4.4.3, page 4-84: 98

Security Requirements for Voting Systems 100

 VSS V1, 6.1, page 6-93: 100

 VSS V1, 6.2, page 6-96: 101

 VSS V1, 6.2.2, page 6-97: 101

Appendix B. Database Fundamentals 104

Appendix C. IP ADDRESSING FUNDAMENTALS 107

Appendix D. Nation-State Cyber Attack Capabilities 109

 Introduction 109

 Moonlight Maze..... 110

 Stuxnet..... 110

 Operation Titan-Rain 111

 Operation Aurora..... 111

 2020 US Government Attack 112

 Summary..... 112

Appendix E. Security Considerations for SQL Server Installations 113

Appendix F. C.R.S. 1-5-608.5..... 115

Appendix G. C.R.S. 1-5-615 117

Appendix H. Man in the middle attack..... 119

Appendix J. Forensic Imaging Technology 121

Appendix K. Accessing a Computer Without a Password..... 126

 Finding a password 126

 Cracking a password 126

 Rainbow Tables..... 127

 Bypassing a password 127

 Exploitation of Services..... 127

Intel Active Management Technology (AMT) and Management Engine (ME) 128

Dell Integrated Remote Access Controller (iDRAC) 129

Strengthening Access Security..... 129

APPENDIX L. Supply Chain Security Threat and Foreign Manufacturing..... 131

Appendix M. Colorado Secretary of State Press Release 133

Doug Gould Biography..... 137

Table of Figures

Figure 1 - SSMS Installation Date on Mesa County EMS server 12

Figure 2 - Mesa County, Colorado EMS server (5.11-CO) Forensic Image Attributes..... 20

Figure 3 - Test Workstation and Dominion EMS server 23

Figure 4 - Installed Microsoft Software 25

Figure 5 - SQL Server 2016 Configuration Manager 26

Figure 6 - SQL Server 2016 Configuration Manager – Network Protocols enabled..... 27

Figure 7 - TCP/IP Properties..... 30

Figure 8 - TCP/IP Properties of SQL Server, attached to port 1433 the standard (default) port. 31

Figure 9 - SQL Server Properties 32

Figure 10 - Encryption is enabled but No Encryption Certificate is configured 33

Figure 11 - SQL Server Management Studio (SSMS) software showing in the EMS server Start Menu 34

Figure 12 - SSMS is installed and starting on the EMS server system..... 35

Figure 13 - Logging in to the SQL Server using SQL Server Management Studio..... 36

Figure 14 - SSMS enables direct access to the internal databases to anyone logged in to the EMS server. 37

Figure 15 - Databases from many prior elections are fully accessible 38

Figure 16 - Additional databases used in previous elections 39

Figure 17 - Internal database tables, including ones with counted votes are accessible 40

Figure 18 - Menu Option to Select the Top 1000 rows 41

Figure 19 - Accessing the Ballot Choice database table 42

Figure 20 - Test to determine if the Ballot Choice Table can be edited to easily flip the votes 43

Figure 21 - Candidate settings for Trump 44

Figure 22 - Candidate settings for Biden 45

Figure 23 - Pulling up the results report prior to attempting the alteration 46

Figure 24 - Run Stored Procedure to pull up a report of Presidential Electors..... 47

Figure 25 - Retrieved Vote Totals 48

Figure 26 - Candidate number for Trump modified 49

Figure 27 - Candidate number for Biden modified..... 50

Figure 28 - Vote totals retrieved again after modification..... 51

Figure 29 - Accessing port 1433 with Telnet 53

Figure 30 - The EMS server network interface appears to answer a connection to port 1433 54

Figure 31 - EMS server has the 'Windows Firewall' enabled 55

Figure 32 - Windows Firewall Custom SQL entry is enabled 57

Figure 33 - SQL port 1433 is allowed. 58

Figure 34 - Access to the SQL database standard port is allowed from ANY IP ADDRESS worldwide..... 59

Figure 35 - No additional IP address restrictions or permissions..... 60

Figure 36 - Test Workstation, 192.168.100.150, and EMS, 192.168.100.10, are on the same subnet 61

Figure 37 - Mesa EMS server is responding to network ping test..... 62

Figure 38 - Telnet connectivity test from separate computer not part of the Dominion system 63

Figure 39 - Telnet to EMS server port 1433 (SQL) succeeds 64

Figure 40 - SSMS access test from separate computer not part of the DVS D-Suite system..... 65

Figure 41 - Log In to the server..... 66

Figure 42 - From a separate Windows 10 computer EMS server database access has been obtained..... 67

Figure 43 - From a separate Windows computer, the databases can be accessed and reports run..... 68

Figure 44 - SSMS permits database Edit..... 69

Figure 45 - EMS server Database view from a separate computer not part of the DVS D-Suite system 70

Figure 46 - SSMS permits us to edit the databases 71

Figure 47 - "internalMachined" for Trump is now changed back to a 2. 72

Figure 48 - Candidate data for Biden from previous change 73

Figure 49 - Candidate data for Biden changed back to original 74

Figure 50 - The vote choice was remotely changed back to its original state 75

Figure 51 - Network scanner installed on cellphone..... 76

Figure 52 - IP address for the EMS server found via wireless connection and iPhone app..... 77

Figure 53 - Scanner Results..... 78

Figure 54 - SQL Access Functionality 79

Figure 55 - SQL Pro Capabilities..... 80

Figure 56 - Making an SQL Connection..... 81

Figure 57 - iPhone Connection to Dominion EMS Database 82

Figure 58 - Databases listing, Continued 83

Figure 59 - Database Table Listing..... 84

Figure 60 - Database Access 85

Figure 61 - Executing a Database Query..... 86

Figure 62 - Table Data..... 87

Figure 63 - A script to change the vote data 88

Figure 64 - Script Results 89

Figure 65 - Small Wireless Device Surreptitiously Installed (internally) on a Computer Motherboard 90

Figure 66 - DVS Compliance Statement..... 102

Figure 67 - Man In The Middle Attack..... 119

Figure 68 - Illustrative Hard Disk Components..... 121

Figure 69 - Disk Track and Sector illustration 122

EXECUTIVE SUMMARY

This report documents findings in an ongoing forensic examination of images of the hard drives¹ of the Dominion Voting System (DVS) Democracy Suite (D-Suite) version 5.11-CO Election Management System (EMS) server of Mesa County, Colorado. The DVS D-Suite EMS server in that configuration was used for all elections held in 2020 and through May 2021, including the November, 2020 General Election, and the April, 2021 Grand Junction Municipal Election. This voting system represents a portion of the overall election system infrastructure in Mesa County and the State of Colorado. This report is limited to a subset of the findings of an ongoing investigation. Report #1 is incorporated by reference.² The findings in this report were prepared by me as a consultant to the legal team representing Tina Peters, the Mesa County Clerk and Recorder, pursuant to her statutory duties as Mesa County's Chief Election Official.

Critical Discoveries

This report details the following critical discoveries regarding Mesa County's voting system:

- Uncertified software installed, rendering the voting system unlawful for use in elections.
- Does not meet statutorily mandated Voting System Standards (VSS) and could not have been lawfully certified for purchase or use.
- Suffered systematic deletion of election records (audit log files required by Federal and State law to be generated and maintained), which, in combination with other issues revealed in this report, creates an unauditible "back door" into the election system.
- Violates Voting Systems Standards ("VSS") which expressly mandate prevention of the ability to "change calculated vote totals." This report documents this non-compliance from the logged-in EMS server, from a non-DVS computer with network access, and from a cell phone (which may be possible if any of the 36 internal wireless devices in voting system components are deliberately or accidentally enabled and a password is obtained).
- Mandatory VSS "System Auditability" required features are disabled.
- Is configured with 36 wireless devices, which represent an extreme and unnecessary vulnerability, and which may be exploited to obtain unauthorized access from external devices, networks, and the Internet.
- Is configured through firewall settings to allow any computer in the world to connect to the Election Management System (EMS) server.
- Uses only a Windows password with generic userIDs to restrict and control access.
- Contains user accounts with administrative access that share passwords, subverting VSS-required user accountability and action traceability controls.
- Uses a self-signed encryption certificate which exposes the system to the risk of undetected compromise or alteration.

¹ A forensic image of a hard drive is a bit-for-bit copy of the user accessible data storage area residing on the data storage mechanism used by the computer system; it is every byte of data accessible to the computer or user. For a complete discussion of this definition, see Appendix J.

² Report No.1 was issued on September 15, 2021 and can be downloaded at <https://standwithtina.org/>.

Most Significant Findings: The Voting System is Not Secure, Violates Security Standards Required By State and Federal Law

The most significant findings include the conclusive determination, based on testing, that the voting system is not secure and protections have not been implemented in accordance with the requirements of the Federal Election Commission's 2002 Voting System Standards (VSS) (see Appendix A). Those Standards constitute a mandatory minimum requirement for a voting system to be certified and used under Colorado law. Given the fundamental flaws in the security design and configuration of this system, there is no conceivable interpretation under which this voting system could be considered secure.³ The fact that it was tested and certified for use vitiates claims of competency and trustworthiness of the entire regime of testing and certification being used, of truthfulness of testing and certification statements, of competency of the Colorado Secretary of State's office, and of the validity of any election results obtained from the voting system as used in any jurisdiction.

"Back-Door" found in Voting System; Uncertified Software Invalidates Voting System Certification

The combination of unauthorized software installed in the EMS server in 2017 (still present in violation of law in 2021), the failure to employ security mechanisms already built into the system and required by VSS, and the obliteration of mandatory audit logs (destruction of both election records and evidence of access to the EMS server) that Federal and State law require be preserved, create a "back-door" to the EMS server that is only partially protected by a simple password, with no preserved audit records. The existence of uncertified software violates the certification of the voting system and makes the use of the voting system in an election illegal. Indeed, University of Michigan Professor J. Alex Halderman,⁴ a recognized computer science expert on electronic voting systems, testified under oath⁵ that components of this Dominion Voting System ("DVS") are highly vulnerable to attack and that the system he examined is used in 16 other states, including Colorado. In his declaration he states under oath that this vulnerability in the Dominion voting system can be used to "steal votes", and requests the federal court allow him to give the Critical Infrastructure Security Agency (CISA) immediate access to his report detailing his findings.⁶ The findings in this report agree with Professor Halderman's finding that the system can be used to steal elections.

³ Even the Center for Internet Security (CIS) recognizes the need for these controls in their Handbook for Election Infrastructure Security: <https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf>. The National Institute of Standards and Technology (NIST), which chaired the development of the Voting Systems Standards extensively recommends the fundamental security principle of "Least Privilege" that has been ignored in the configuration of the EMS.

⁴ Professor of Computer Science & Engineering, University of Michigan, Director, University of Michigan Center for Computer Science and Society, Director, Michigan CSE Systems Lab, <https://jhalderm.com/>.

⁵ Declaration of J. Alex Halderman, *Curling et al. v. Raffensperger et al.*, 1:17-cv-02989-AT, Docket No. 1177-1, (ND Ga.).

⁶ *Id.*

A password was not necessary to access this EMS server.⁷ There are many mechanisms by which a server can be exploited and administrative access obtained without a password; the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) has identified over eight hundred of these admin-access vulnerabilities⁸ (among hundreds of thousands of other vulnerabilities) since its inception in 2005, and the Common Vulnerabilities and Exposures (CVE) program operated by MITRE Corp. lists nearly 170,000 computer vulnerabilities⁹ that are *publicly known* since its inception in 1999.

Capability to Easily "Flip" Election Results Demonstrated

Tests demonstrate the vote totals can be easily changed, commonly known as "flipping the election,"¹⁰ in this critical Election Management System server. The VSS directs voting systems vendors, like DVS, to address this specific risk¹¹ but based on the software contained on the EMS that was analyzed, the vendor has not done so here. Further, the obliteration of audit trails (logs) on the EMS server makes it extraordinarily difficult (and maybe impossible) to forensically determine whether any external connection allowing unauthorized access to the voting system, wireless or wired, occurred before, during or after the elections.

This report describes the absence of legally required security features on the voting system and then demonstrates only a few examples of the many possible methods by which it is possible to change calculated vote totals and alter the results of an election as consequence of those security failures.

Voting System Components Manufactured and Assembled in China and Mexico

The Mesa County EMS server used through May 2021 (serial number 4NV1V52) was assembled in Mexico, and its motherboard was manufactured in China. It is well understood that foreign manufacture or assembly exposes the components to the risk of compromise through the installation of foreign-controlled access devices during manufacture in the reported supply-chain attack.¹²

Voting System Presents an Immediate threat and is Dangerous to use in the upcoming 2022 election

The tests conducted in this report demonstrate and document three test intrusions into the DVS Election Management System server using popular, commercially available software that allows easy access to vulnerable election records. Given even momentary access, a person with only moderate computer skills

⁷ The Mesa County Co. DVS D-Suite 5.11-CO server was forensically restored in a virtual environment, and a common password reset/bypass technique was used. See Appendix K. Also see www.gaverifiedvoting.org/pdf-litigation/20200819-785_2-Declaration-Alex-Halderman.pdf

⁸ https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=administrative+access&search_type=all&isCpeNameSearch=false

⁹ <https://www.cve.org/>

¹⁰ The switching of calculated vote totals in an election has been identified in 2 other jurisdictions: Fulton County, Pennsylvania, and Antrim County, Michigan. See <https://rumble.com/embed/vjr2u6/?pub=dw7pn> which documents testimony of the Fulton County finding.

¹¹ "Changing the calculated vote totals," VSS, Volume 1, section 6.1, page 6-93. See Appendix A.

¹² <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>; See Appendix L for discussion.

can perform such an intrusion. It is not possible to reconcile these massive security failures with the obvious requirements for such an important piece of critical infrastructure. In combination with mandatory audit records being deleted in violation of state and federal laws that require their preservation, and in violation of evidence preservation orders for active legal cases ¹³, this EMS server presents an immediate threat to election integrity, with potential grave consequence to Colorado and the Nation by allowing the unauthorized alteration of election results.

The threat is immediate because 2022 election processes are already underway with primary elections imminent, and many jurisdictions will use these systems, and citizens' electoral franchise will be at risk, if citizens and public officials are not warned.

The initial installation and continued presence of uncertified software (Microsoft SQL Server Management Studio) in the Mesa County EMS Server is a violation of law. However, the tests conducted for this report clearly demonstrate that it is not the SSMS software alone that enabled illegal access to and modification of election databases and scanned ballot images. The state certifying this software on a chronically insecure system does not remedy the system's chronic insecurity – it only obfuscates one problem (insecurity) with another (improper testing and certification).

In contrast to the testing and certification of DVS D-Suite 5.11-CO, the current certification in Colorado of DVS D-Suite 5.13 includes SSMS, but tests conducted in this examination demonstrate conclusively that the EMS system is insecure both with, and without, SSMS.

¹³ Log files and other auditable records of normal and abnormal activity on computer-based voting systems are not only election records which must be preserved for 22 months according to Federal law, and 25 months according to Colorado law, they also represent evidence that is subject to document preservation requirements in existing civil litigation and, foreseeable, for future civil and criminal cases.

Key Findings

Six Key Findings in this report are:

1. The Mesa County EMS server used in the 2020 General Election had Microsoft SQL Server Management Studio 17 installed in May 2017. This software is not listed on the official test and certification report nor on the vendor's application to the Colorado Secretary of State for certification of DVS D-Suite version 5.11-CO signed by "Nick Ikonomakis," VP, Engineering [Dominion Voting Systems], dated 6/6/2019. As it was not listed, tested, or certified, the unauthorized installation of this software violates and renders illegal the certification of the election system, and its use in an election.

2. The inclusion of unauthorized and uncertified Microsoft SQL Server Management Studio software, as configured, allows the bypassing of Dominion Voting Systems' software and enables any data in the vote databases to be changed. For example, using the uncertified Microsoft SQL Server Management Studio software, it is a quick and simple task to "flip" the vote (change calculated vote totals, demonstrated herein by changing only two values in the database to flip tens of thousands of votes).

3. With the addition of a wireless access device (added to the test to emulate the presence of multiple wireless devices that exist on Mesa County's DVS hardware), the insecure configuration of the Mesa County EMS server allowed the editing and changing of the calculated vote totals using a standard iPhone. Wireless access, whether enabled accidentally or enabled/added deliberately (even in secret) to a voting system network, enables intrusion, attack, and compromise of any electronic voting system. The security configuration of the EMS server was wholly inadequate to prevent such intrusions. Thirty-six wireless access devices were identified built-in to the Mesa County DVS D-Suite system components, as documented by Dell and the Secretary of State's equipment inventory.

But, due to the DVS-specified configuration of the EMS, and the Secretary of State-approved procedures that overwrite audit records¹⁴ – by mandating that the EMS server "overwrite" log files "as needed," and further, during the Secretary of State's so-called "Trusted Build" update which overwrote the EMS server, both in violation of federal and state laws - it is at best, extremely difficult to determine from EMS server audit log data how or even whether the wireless connections were used during or affecting Mesa County's elections.

4. The exceptionally poor security configuration of the EMS server's operating system, firewall, and the improper and inadequate configuration of the SQL Server database management system

¹⁴ Approved, by certifying vendor supplied information. CRS-1-5-620 states that the vendor provides documentation including manuals to the Secretary of State, and any information not on file with and approved by the Secretary of State shall not be used in an election.

CONFIDENTIAL

(DBMS) enabled access to the election databases and the alteration of vote totals using freely available, non-DVS and non-Microsoft database app downloaded and installed onto on a cell phone.

5. The Colorado Secretary of State's certification of DVS D-Suite version 5.11-CO for use throughout the state of Colorado was illegal,¹⁵ given the overwhelming number of VSS compliance violations found within the EMS server, which undermine the credibility of the claimed testing, technical competency of the testing lab, and the Secretary of State's certification.

6. The Mesa County, Colorado EMS server as used in elections including the 2020 General Election, and the April 2021 Grand Junction Municipal Election, has been shown to be insecure and grossly misconfigured such that it could not prevent unauthorized access to the election database or, as explicitly required by the VSS, prevent "changing the calculated vote totals" (demonstrated using an exact forensic replica of the system). This constitutes a material violation of the VSS requirements. It was possible to access the EMS server and change only 2 numbers in the database to completely reverse the Mesa County election 2020 Presidential election results stored on the EMS server. If this was done during the election, the EMS server would have then reported the changed vote totals as its authentic result.

¹⁵ The Colorado Secretary of State's certification of both DVS D-Suite 5.11-CO and 5.13 were also apparently illegal under state law, given that testing by a federally accredited testing lab is prerequisite for certification under Colorado law, and the Secretary's certifications both relied upon testing by an unaccredited voting system testing lab.

Analysis Summary: Compliance of Mesa County, Colorado, DVS D-Suite systems with the law

Four Key Objectives for this assessment are:

1. To determine whether implemented security capabilities comply with the 2002 Voting System Standards (VSS), mandatory under Colorado law;
2. To determine whether the results of an election stored on the EMS server can be altered by any person with physical access to the logged-in EMS server,
3. To determine whether the results of an election stored on the EMS server can be altered by any person using even a non-Dominion computer directly or indirectly connected to the EMS server network, and
4. To determine whether the results of an election stored on the EMS server can be altered by any person using a device such as a cell phone wirelessly connected to the EMS server network.

It is recommended that this report be viewed on a computer. Some of the screen images may be difficult to read when printed on paper, but viewed on a computer they can be expanded (zoomed in) and are easily read.

Documented in this report is a series of tests conducted as part of the examination to evaluate a few aspects of the security compliance¹⁶ of the Mesa County, Colorado DVS D-Suite version 5.11-CO EMS server, and the findings from that examination. These tests were limited to the EMS server. The EMS server receives and stores ballots in the form of electronic ballot images and cast vote records (CVR) from each ballot optically scanned into ImageCast Central (ICC) scanning/tabulation machines, and tabulates the results of the election. The images, CVRs, tabulated results and all system log files that document every aspect of system state, access, and operation are critical election records. The EMS server is one of the most critical components of the voting system and the security of its election records is of paramount importance.

The examination began with no pre-conceived assumptions about vulnerabilities and security. An identical copy of the Mesa County EMS server hard drive image¹⁷ was mounted and tested to exactly replicate the conditions of use during elections conducted between the installation of version 5.11-CO in 2019 and its replacement on May 25, 2021. The identified uncertified SSMS software component was installed earlier and very likely presented this same security weakness since its installation in 2017, but the scope of the tests in this report only addresses the 2019-2021 period. The computer-based voting system is extraordinarily complex and requires skill, knowledge, and diligence to configure securely. Despite being custom-ordered and then configured by the vendor, the critical nature of voting systems and the extreme importance of securely configuring these computer-based systems requires that voting systems be tested by competent cybersecurity professionals to determine their vulnerability. Colorado law requires only that

¹⁶ The evaluation identified critical weaknesses in the system and this report documents those findings. A comprehensive evaluation of every possible defect is beyond the scope of this report; the investigation is ongoing.

¹⁷ An identical copy of the Logical drive image, mounted within an Oracle VirtualBox virtual environment.

CONFIDENTIAL

they be tested by a laboratory accredited by the U.S. Election Assistance Commission (EAC) and the results certified by the Colorado Secretary of State.

The DVS application to the Colorado Secretary of State for certification of DVS D-Suite 5.11-CO represents that this system "meets the requirements of the Colorado Secretary of State Election Rules (8 CCR 1505-1)" (which specify that all voting systems in Colorado must meet the requirements of the 2002 VSS).¹⁸ This includes documentation of the "minimum services needed for the successful, secure and hardened operation of the voting system" and "contains security measures for all systems, software, devices (upload, download, and other programming devices) that act as connectors and any additional recommended security measures." While this provision of law addresses documentation to be provided, it is also necessarily required that the documentation be truthful and accurate. A forensic examination of this system, and tests performed in this examination, clearly show that these requirements are not met; the system is not secure and certainly not hardened against unauthorized access.

Testing confirmed that an outside party could use a separate computer as well as a cell phone, with publicly available and widely used free software (none of which were part of the DVS D-Suite), to easily change election results. The obliteration of audit trails on the EMS server by DVS and the Secretary of State personnel during the "trusted build" process diminished the ability to forensically determine whether any network connections (including wireless connections or intrusions) were made to the EMS server. Thirty-five wireless devices were identified on the DVS D-Suite system, including the ImageCast Voter Activation (ICVA) computer, serial number 2DX0Z52, ordered on August 16, 2015 by DVS for use in Mesa County. It was ordered by DVS configured with a Dell Wireless 1560 internal wireless adapter, providing both 2.4GHz and 5GHz (dual band) Wi-Fi and Bluetooth connectivity to and through that ICVA computer. In total, Mesa County was provided thirty-five D-Suite components with wireless capability installed: Dell Latitude 7450 computers providing ICVA functionality, serial nos. 8GX0Z52, 8JX0Z52, BCX0Z52 with Dell Wireless 1560 modules, and Dell Optiplex 9030 ImageCast Central (ICC) systems, serial nos. H4B4T52, H4G0T52, H4JBT52, and H4L9T52 with Dell Wireless modules. A Dell E310DW wireless printer was configured as the EMS server's default printer, with IP address 192.168.100.11, bringing the total number of wireless devices to thirty-six. Wireless device encryption can be easily broken,¹⁹ and the vulnerabilities are online and in the Computer Vulnerabilities and Exposures (CVE) database.²⁰ A demonstration video of this intrusion is also available.²¹ Twenty-eight (28) tablets, provided by DVS as ICX devices in the D-Suite system, include

¹⁸ https://web.archive.org/web/20201018013640/https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule21.pdf

¹⁹ Vulnerability: <http://www.dell.com/support/kbdoc/en-us/000125799/wi-fi-security-protocol-key-re-installation-attack-krack-impact-status-on-dell-products>; Published and freely available code to implement the attack: <https://www.joe0.com/2017/11/11/kali-linux-virtualbox-instructions-for-testing-wi-fi-devices-against-wpa2-key-reinstallation-attack-krack-attack/>

²⁰ <http://cve.mitre.org/> : CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088. This attack is against the WPA2 encryption protocol and all wireless devices, regardless of manufacturer, are impacted.

²¹ <http://www.krackattacks.com/>, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, Vanhoef and Piessens, <https://papers.mathyvanhoef.com/ccs2017.pdf>

CONFIDENTIAL

wireless capability. The prior expert analysis and testimony of Professor Halderman further confirms the vulnerability of these Dominion ICX components to malicious attack and compromise by an outside party.²²

Because of the extraordinary nature of the "back-door" identified and because internal wireless devices were included as part of the DVS D-Suite system used in Mesa County, I added a wireless access device to the server network during testing to properly replicate the actual hardware used in Mesa County. This enabled determination of whether the system vulnerabilities could be exploited with the more limited capabilities of a mobile device. This report describes testing that demonstrates how easily the design and configuration of this voting system allows this type of exploitation.²³

The tests in this report first demonstrate that any person with physical access to the logged-in EMS system can change the election database results (calculated vote totals), with²⁴ or without²⁵ a userID and password, on the Mesa County EMS before, during, or after the election by using a few mouse clicks. By itself, the ability of any user to modify election database totals illustrates the voting system's non-compliance with VSS and Colorado law. The tests also demonstrate that if the voting system has any external connection for even a moment, a person anywhere in the world can change the election database results on the EMS server with a few mouse clicks. This is an extraordinary danger to election integrity.

The protection offered by use of passwords is further weakened by the fact that different userIDs created on the EMS server share the same password.²⁶ Shared passwords were also reported in the Maricopa, Arizona forensic audit.²⁷ Rudimentary security protocol demands that each userID must have its own unique password. The sharing of password across accounts renders ineffective individual accountability for actions by a user (each assigned a specific userID, required for access control mandated by VSS and the ability of audit trails to identify fraudulent activity). This renders the system noncompliant with VSS requirements. VSS mandates, among other things, that the system: (1) "establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized; (2) protect the system from intentional manipulation and fraud, and from malicious mischief"; and (3) identify fraudulent or erroneous changes to the system."²⁸ Other jurisdictions have learned that they do not have control of their voting systems but the vendor, Dominion Voting Systems, has the administrative passwords and, therefore,

²² www.gaverifiedvoting.org/pdf-litigation/20200819-785_2-Declaration-Alex-Halderman.pdf

²³ The VSS expressly identifies the prevention of this type of manipulation in its security objectives for voting systems, VSS Volume 1, section 6.1, page 6-93, excerpted in Appendix A.

²⁴ I accessed the EMS server with and without a password. I was able to guess the password, and separately used a well-known password bypass technique, both methods were successful and I gained access to a copy of the EMS server in an Oracle VirtualBox environment.

²⁵ Passwords are easily bypassed, and knowledge of a specific password is not required, since access can be obtained without a password. See Appendix K.

²⁶ Thirty different userIDs on the Mesa County EMS server were found to share an identical password. Two of those accounts were enabled and active.

²⁷ Maricopa County Forensic Election Audit, Volume III, section 6.5.2.1.3

²⁸ (VSS V1, 6.1, page 6-93, see Appendix A).

CONFIDENTIAL

control.²⁹ Mesa County's DVS EMS server has an administrator account installed specifically for Dominion Voting Systems' use.³⁰ In light of the legal and security responsibilities in the administration of elections, allowing a vendor (in this case DVS) to maintain administrator access to the voting system is inexplicable, as is the exclusion of local election officials from control over their own elections.

The names of account userIDs on Mesa County's EMS server, created during the installation of DVS D-Suite 5.11-CO, are generic. Generic account userIDs were also found in the Maricopa, Arizona audit.³¹ This finding in Arizona strongly suggests that it is a DVS practice to use generic userIDs and the same userIDs are likely used on every DVS election system in the USA. As one of the two components of required authentication (userID and password), this is an extraordinary compromise of security, as it is likely that once a userID from one state is known, it may be known for *all* states.

The examination found that the EMS server network was active and in use; the Ethernet network interface was found to be enabled, an IP address was found to be assigned, and election databases and ballot images were found to be stored on the EMS 'NAS' disk drive. The drive was shared to the connected network.³² Any representation that the EMS server was not connected to a network is false. The transmission control protocol / Internet protocol (TCP/IP) port that supports direct back-end database access on the EMS server was found to be unprotected by anything other than Windows authentication (a common userID and a shared password) and any person who gains unauthorized access will have full access to ballot images and the tabulated vote databases, in violation of the 2002 VSS.

The tests conducted in this examination found the system to be insecure and also ensured that no protections that might otherwise have secured the system were overlooked by the examination process. No advanced security penetration techniques were needed; the initial access to the operating system (i.e., "login") was performed both by guessing the password as well as by using well-known and easy to find password bypass techniques. The unauthorized and uncertified Microsoft SQL Server Management Studio software³³ ("SSMS") on the EMS server was run and access to the SQL server databases on the EMS server, which should be highly restricted, was granted without restriction or challenge. This same access has been found in other forensic examinations of virtually identical DVS D-Suite voting systems used in at least two other states.³⁴ A non-Microsoft, non-DVS software application that supports SQL database access was also used (from an iPhone) and access to Mesa County EMS server election databases was obtained, allowing

²⁹ Maricopa County Forensic Election Audit, Volume III, section 6.5.3.1.3. See also <https://www.westernjournal.com/az-audit-exclusive-election-systems-password-hasnt-changed-2-years-shared-time/>.

³⁰ Account names are withheld in this report to protect the security of the system, since an account name and a password are literally the only things protecting this system.

³¹ Maricopa County Forensic Election Audit, Volume III, section 6.5.2.1.3

³² Dominion misleadingly refers to this as "NAS." It is not. NAS stands for Network-Attached Storage. This storage was found not to be network-attached, but instead, "direct-attached," and is thus a DAS instead of a NAS.

³³ D:\Program Files (x86)\Microsoft SQL Server\140\Tools\Binn\ManagementStudio\Ssms.exe.

³⁴ Analysis of the Antrim County, Michigan November 2020 Election Incident, J. Alex Halderman, March 26, 2021, p.10; September 24, 2021, Presentation of Ben Cotton entitled *Arizona Senate Audit, Digital Findings*, slide 13.

changes to the calculated vote totals. Testing shows conclusively that the voting system was not secure and that protections required by law were not enabled.

Report #1 documented the destruction of system log files that voting systems are required to generate and preserve in order to comply with federal and Colorado law.³⁵) Those critical election records would be necessary to allow a forensic examiner to identify whether any changes to the election databases were made, and when and how they occurred. This system did not preserve those election records,³⁶ in violation of federal and Colorado law. This failure was a direct result of the system configurations and technical guidance as directed by Dominion and mandated by the Colorado Secretary of State for all counties using D-Suite version 5.11-CO EMS servers. The installation of the voting system software update (called the "Trusted Build") by the Secretary of State, assisted by DVS personnel, in all DVS-equipped Colorado counties further overwrote and eradicated most records necessary to perform a forensic audit of the affected elections.

As a direct result of the destruction of those election records (in the form of log files that provide an audit trail required by law to be preserved), any examiner, much less a non-expert public official, will find it difficult if not impossible to determine conclusively that the voting systems have not been tampered with or operated in an unauthorized manner. Destruction of those election records prevents detection and/or confirmation that the vulnerabilities identified in this report were not exploited to alter election results.

A full, independent forensic audit should be conducted in any jurisdiction that used this system, given the extraordinary insecurity and non-compliance of this voting system with both legal standards and industry-recognized best practices and the failure of the existing testing and certification regime to detect those conditions,. Such an audit should include every component of the voting system, all electronic logs, removable media, and escrowed source code. Cast paper ballots should be examined for authenticity and then recounted in order to have confidence that the tabulated vote count matches the paper ballots. Because of the obliteration of audit trail data, audit techniques which rely upon small, statistical sampling of results (so-called "risk-limiting audits") are not reliable. No person can trust any result obtained from this system in any election in which it was used due to the extreme insecurity of this voting system.

Although this examination addresses the local Mesa County, Colorado election results stored on the Mesa County EMS server, similar destruction of election records and the security weaknesses that enabled it are

³⁵ Appendix A, VSS, Retention Requirement

³⁶ If not for the action of the Mesa County Clerk, who forensically preserved the Mesa County election records by backup of EMS server hard drive, the auditable record of the partial EMS server log files that remained from the November 2020 General Election and the April 2021 Grand Junction Municipal Election would have been destroyed by the Secretary of State's action and direction. That destruction of election records by DVS and the Secretary of State would have precluded a forensic audit of those elections and prevented the exposure of the voting system vulnerabilities as they existed in the November 2020 general election and the April 2021 Grand Junction Municipal Election. Failure to meet statutory-security compliance requirements would have been hidden from both public officials and the public. Neither the Secretary of State nor DVS instructed election officials to properly preserve these critical electronic records prior to these destructive "updates" and instead instructed them only to preserve ballot images and related election project files.

CONFIDENTIAL

highly likely to have occurred across Colorado and possibly other jurisdictions. The configuration of the system is required to be tested by EAC-accredited testing labs, controlled through certification by the Colorado Secretary of State, and specified by Dominion Voting Systems (DVS), so it is almost certain this system is used throughout Colorado, and it is likely very similar, if not identical to systems used in other states.

Examination of the EMS server found that unauthorized Microsoft SQL Server Management Studio software³⁷ ("SSMS") was installed on 5/17/2017 at 06:49:44 AM. Given that the "trusted build" process was used in 2019 and overwrote all previous data on the Mesa County EMS server, SSMS must have been installed by DVS on its golden image of the D-Suite system; if it were installed by Mesa County staff, the installation date could not have preceded the DVS installation date of D-Suite 5.11-CO in 2019. SSMS remained installed on Mesa County's EMS server through the backup imaging conducted in May 2021. That software was present on the 5.11-CO EMS server but not listed on the Certification Application or testing report for the DVS D-Suite 5.11-CO system. This failure of the manufacturer to meet, the voting system testing lab to verify, and the Colorado Secretary of State to ensure that minimum Federal Voting System Standards were met, as required by law, is inexcusable and grossly violates industry standards. Only after this software was noted in an expert report, dated December 13, 2020, and submitted in connection with a widely publicized vote switching controversy in Antrim County Michigan involving DVS D-Suite systems, did DVS submit an application for certification for version 5.13-CO, dated Jan. 13, 2021 which listed SSMS as an installed software component.³⁸

Name	File Ext	Logical Size	Category	File Created
SSms.exe	exe	720,632	Executable	05/17/17 06:49:44 AM (-4:00 Eastern Daylight Time)

Figure 1 - SSMS Installation Date on Mesa County EMS server

The Colorado Secretary of State should have been aware that this separate software component (a completely separate download from Microsoft) was required to be listed on the application for certification, tested by a federally-accredited lab, and certified. The addition of MS SQL Server Management Studio is not necessary to the election process, and allows any party with access to the EMS server to alter cast ballots, tallies, databases, ballots, and audit records with up to full administrative permission.

Examination revealed fundamental flaws within the security configuration of the Mesa County Election Management System (EMS) server used in the November 2020 general election and the April 2021 Grand Junction municipal election that show conclusively that this voting system and its software, as delivered by Dominion Voting Systems and certified by the Colorado Secretary of State, is uncertifiable under Colorado law because it contains unauthorized, untested and uncertified software in violation of the law, is configured in a manner that violates mandatory VSS and industry best-practice security standards, allows "intentional manipulation and fraud" that the VSS standard prohibits, and fails to log system events and preserve audit trails required by VSS in a manner that makes determination of election integrity extremely difficult, and maybe impossible.

³⁷ D:\Program Files (x86)\Microsoft SQL Server\140\Tools\Binn\ManagementStudio\SSms.exe.

³⁸ See Antrim Michigan Forensics Report, Allied Security Operations Group, December 13, 2020.

CONFIDENTIAL

Nationwide, various election officials have denied qualified third-party investigators the access to election system equipment including logs, network and security equipment configurations, and network diagrams, that might allow the detection of unauthorized access and operation of voting systems. This report demonstrates why this is a dangerous development because the denial of access prevents the discovery of the full extent of the failure of election security and election records integrity.

The techniques used in this report employ basic network troubleshooting techniques that can readily be executed by persons with minimal skills. In fact, software found to be already installed on the EMS server (Microsoft SQL Server Management Studio was downloaded and installed on the test workstation, while Fing and SQL Pro from the Apple App Store were installed on an iPhone). In each instance, the software was launched and access was granted. It was so simple that calling the test an “attack” is almost inappropriate, since standard publicly-available software was used without modification and connection was made in an industry standard manner to the default port assigned for SQL databases.³⁹ The server had no security implemented other than userID and password, and even that is easily bypassed.⁴⁰ In this case it was not a smart examiner but the exceptionally insecure configuration of the voting system that was at fault in failing to meet the requirements of law. That exceptionally insecure configuration is an open invitation to the average hacker, and indeed almost anyone with basic skills, to be able to change election results.

But it is not the average “hacker” or even cyber-criminals that provide the greatest threat to election integrity. While it has been stressed that these *relatively simple* intrusions could be done by anyone with a reasonable understanding of networks, the fact is that nation-state adversaries have long attacked and subverted the critical infrastructure of the United States,⁴¹ as documented in Appendix D. The extreme sophistication of these nation-state actors' cyber threat capabilities has persisted for decades, evolved far beyond the knowledge of the average citizen, and the history of publicly-known attacks document it beyond question. Malicious actors, including foreign nation-states, our most capable and persistent adversaries, already know how to subvert insecure systems, like this election infrastructure.

The evidence of foreign interest in our voting systems is too important to bury in a footnote: four (4) Korean students, at 2 different Korean universities, authored the paper [A Study of Vulnerabilities in E-Voting System](https://www.researchgate.net/publication/315040247_A_Study_of_Vulnerabilities_in_E-Voting_System), Xing Shu Li, Hyang ran Lee, Malrey Lee and Jae-young Choi, *Advanced Science and Technology Letters Vol.95 (CIA 2015)*, pp.136-139, https://www.researchgate.net/publication/315040247_A_Study_of_Vulnerabilities_in_E-Voting_System. Section 2 discusses “hybrid election systems” that are exactly what the Dominion Democracy Suite elections systems are.

Continued suppression of the knowledge of this system's extreme security failures, long known to foreign nation-states and others, does not further the security of critical infrastructure election systems – indeed, elections have taken place and are ongoing while these known security failures have been left unaddressed.

³⁹ The standard port for SQL database access is 1433. When this port is found open, it is obvious that it provides access to a database system. The port number can and should be reassigned to another number to improve security, making the discovery of database access more difficult, and is an example of multi-layered “Defense in Depth.”

⁴⁰ Appendix K.

⁴¹ <https://www.whitehatsec.com/blog/2020-election-security-the-urgent-need-to-address-vulnerabilities-in-voting-systems/>

CONFIDENTIAL

For example, in his September 21, 2021 Declaration, Professor Halderman attached an email string with CISA dated August 18-19, 2021, wherein he requested that the federal district court allow him to immediately provide his sealed expert report to CISA because of the threat posed to the election systems in sixteen states—including Colorado—by DVS machines with ICX software that can be used to “steal votes.” In that August, 2021, exchange, CISA agreed to receive Halderman’s expert report detailing these security failures. However, even though Professor Halderman testified in his Declaration that this threat was “urgent,” and that it would take “months” to fix these “critical vulnerabilities,” CISA inexplicably waited to even seek Prof. Halderman’s report until more than five months had passed—to January 21, 2022.⁴² The voting systems Halderman described as critically vulnerable were used in the November, 2021, elections in the U.S., including in Colorado. Thus, the suppression of knowledge of security failures has indeed harmed election security and facilitates continued malfeasance.

The security and configuration of the equipment images examined to date leaves no doubt that our voting systems are dangerously insecure, and renders absurd any claim of election integrity.

This examination has demonstrated the ability for any individual to change the calculated vote totals in the internal database tables used in an actual election, bypassing any Dominion Voting System software security and access controls, with no record preserved in log files that are meant to comprise an audit trail of election records. It demonstrates how trivially election results data can be tampered with and even changed completely by someone with physical access to the EMS server, or by using a non-DVS computer attached to the network, or even by using a cell phone or mobile device if wireless access has by any means been enabled on the network.

⁴² Statement of Interest [by CISA], *Curling et al. v. Raffensperger et al.*, 1:17-cv-02989-AT, Docket No. 1269-1 (filed February 10, 2022), (ND Ga.).

EXAMINATION METHODOLOGY

Description of the Examined System

The voting systems used in Mesa County, Colorado, like other systems used across the state and the nation, are made by Dominion Voting Systems (DVS). Many of these voting systems are comprised of an industry-standard computer⁴³ that uses a Microsoft operating system and a combination of proprietary Dominion application software and non-proprietary, commercially available software. This provides a foundation for election-related functions including creating election projects, defining ballots, capturing and storing the election data in a secure database management system, tabulating and counting the votes, and reporting election results.

The Mesa County Election Management System (EMS) server runs on the Microsoft (MS) Windows Server 2016 operating system, and it employs a database management system known as Microsoft SQL Server (SQL Server). The security of the server depends largely upon the proper configuration of the operating system, network, and the SQL Server.

The design of the voting system includes the functional capability to adjudicate ballots that the computer cannot accurately interpret. Adjudication, in this regard, means nominally, that a person sits in front of a computer terminal, a ballot image is shown on the screen, and this person chooses the option that they feel the voter intended to choose. Adjudication is facilitated by a software application that runs on the EMS system (part of the DVS software) and, normally on one or more Adjudication workstations. If unauthorized code is executed on the EMS system, including on Adjudication workstations or other DVS workstations authorized to be connected to the EMS server, or if an unauthorized user is accessing or has accessed an Adjudication workstation, the adjudication function may be executed to adjudicate ballots without the intervention or knowledge of any authorized operator.

This process requires that the EMS server (which stores and provides access to the election databases and ballot images) be connected to a network. While necessary for the adjudication function to work in the present design of the voting system, this design requirement significantly raises the risk of abuse, especially considering the failure to implement required security.

The Mesa County election director at the time reported that the D-Suite 5.11-CO network consisted of a single network switch connecting only specifically-designated components of the voting system, including the EMS server, adjudication workstations, an EMS server client workstation hosting the Election Event Designer (EED) software, and a Network Attached Storage (NAS) file server.⁴⁴ DVS documents the connection of these systems in their manuals. Therefore, while the EMS server may not have been directly connected to the Internet (it is impossible to rule out, without access to all logs which should have been generated and preserved), it was connected to other computers via a network to allow specific voting system devices to communicate with each other. These other computers must be fully examined to assure

⁴³ An "industry-standard" computer is comprised of common components (motherboard, bus, memory, processors, communications, input/output ports) in a common architecture, e.g., the type of computers one purchase in big box stores and find in use in a home-use or business setting, running office productivity and web-browsing software.

⁴⁴ The term Network Attached File Server is, in this case, a misnomer. DVS uses the term NAS, however it is a shared disk drive on the EMS server itself. In this report, I may use the term synonymously, but there is a difference that will be noted where relevant.

that no connection to external devices or networks (including the Internet) occurred, because connection to other computers exposes the EMS server to a common "Island-Hopping attack,"⁴⁵ which is where every device attached to the EMS network may have a direct or indirect path to and from a device or network outside of the election network, providing a path for an attacker's movement through networked devices to the target. For example, the computers in a home are typically all connected to each other via a wired and/or wireless network, and because the home router is connected to the internet, all devices in that home also have a path to the internet.

The voting system network (based on DVS manuals, EMS server image information, and election official input) was reproduced, both with a virtual network environment and again with a physical Ethernet network composed of cables and a small desktop network switch, to allow the network connection of a Test Workstation used in this report. This configuration was used to test access to the EMS server by a person sitting in front of the EMS server, and again to test access to the EMS server by even a non-Dominion computer that connects to this network. To test whether access from a device with more limited capability such as a mobile phone was possible, a wireless access device was added to the network to simulate the hardware used in Mesa County and the enabling, through misconfiguration or malicious action, of one or more of these wireless devices to provide access, even temporarily. Because I did not physically see or examine the original setup of the voting system network in the Mesa County facility, and due to the destruction of log data by both improper configuration and the overwriting of log files, it is not possible to provide conclusive forensic verification that the voting system was not connected to unauthorized external networks or devices, including wireless devices.⁴⁶ It should be noted that seven internal wireless adapters, and twenty-eight wireless-equipped ICX devices, were ordered as components of the Mesa County DVS D-Suite system, as supplied by DVS. In addition, a Dell E310DW wireless-capable network printer was configured as the default printer on the Mesa County EMS server. This brings the total number of wireless access devices to a total of thirty-six devices.

The EMS server has a software firewall. The purpose of having a firewall is to address the risk of access to the EMS server from all unauthorized devices, users, networks, methods, ports, Internet Protocol (IP) addresses or groups of addresses, and during specific time periods. However, a firewall must be specifically configured (programmed) to perform these functions. One risk of a software firewall is that all users with administrative access can change its programming because it resides on the EMS server; a separate hardware firewall device with its own non-shared password mitigates this risk. Per the VSS and required

⁴⁵ In an Island-Hopping attack, a threat actor gains access to a target computer remotely, through other, connected computers or devices. E.g., a target computer (which we'll call "A") is connected to computer or device "B" (e.g., a network printer). Computer or device "B" is connected to computer or device "C" and computer/device "C" is connected to computer/device "D". It is not necessary that they all be connected in a single physical network. In fact, most modern computers have one or more wireless communications devices; such a wireless capability could allow the access that enables an Island-hopping attack. It is not necessary that the connection be of long duration. The attacker might enter and compromise computer "D" from the global Internet over a wireless connection, determine that computer "C" is connected, break-in to computer "C," move through its connection to computer "B," and finally to computer "A" (which is may be particularly vulnerable if there is an assumed trusted relationship/connection between computers "B" and "A." This chain of connection and intrusions ultimately allows the complete compromise of the target computer.

⁴⁶ More detail will be provided in a subsequent forensic report.

by Colorado Law,⁴⁷ risks that must be addressed by a voting system include “Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals.” The EMS server firewall was found to be programmed specifically to permit access to back-end database services, enabling access to vote data and vote totals⁴⁸ on the Mesa County EMS server from ANY IP-address, globally, at any time. This configuration fails to meet requirements in the law, as well as every industry best practice recommendation for firewall rule configuration.

SQL Server, a database management system (DBMS), installed and used on the EMS server (which stores and manages the election databases) is accessible using any software tool supporting connection to SQL Server, employing Windows Authentication. One of the most common and freely available tools is known as Microsoft SQL Server Management Studio (“SSMS”). SSMS is free and available to download from Microsoft from any internet connection. In this examination it was downloaded from Microsoft, installed on the test workstation, and in a matter of minutes, used to easily and directly access the back-end election database and change any data in it. Searching the internet for ‘how to install SQL server management studio,’ the first result was: <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15>, which walks anyone through installing the software while other readily-accessible online videos walk even a novice through the installation.

But even that is not required for anyone with physical access to the EMS server, because SSMS software was found already installed on the Mesa County EMS server image. This software is not on the list of certified software for DVS D-Suite 5.11-CO nor reasonably expected on a voting system, due to the vulnerability it introduces. This addition in itself violates the stated certification of the voting system.

Software (SSMS) that allows direct access to the back end of the election results database and allows changing vote totals was found installed and functional on the Mesa County EMS server. The software firewall, that could have severely restricted access, was programmed instead to allow access from anywhere in the world. Although the VSS does not specifically address firewall configuration, it does specify addressing this kind of risk, and the firewall, supplied by Microsoft as part of the computer operating system could have and should have been programmed to limit access, at a minimum to only those Mesa County devices required to connect to the EMS server (the few other DVS D-Suite computers and devices necessary could be restricted by their specific IP addresses, for example). Such a configuration would also prevent the wireless access demonstrated by my tests and documented in this report, by disallowing its connection, had the firewall been used to control this database access (port 1433, or an alternate port, explained later in this document). However, given the presence of internal wireless devices as part of the DVS D-Suite system, a properly configured firewall rule on the EMS server that restricted access from only other Dominion devices on that network still may not prevent unauthorized access from occurring through the individually-authorized yet wireless-capable devices.⁴⁹ Possibly most alarming, I found a firewall rule that allows global (from anywhere in the world) access, is not supplied by Microsoft, and must have been explicitly created. Allowing global access is extraordinarily irresponsible, particularly given that SSMS

⁴⁷ See VSS Volume 1, section 6.1.

⁴⁸ This firewall could have prevented access but instead specifically allowed it.

⁴⁹ This means that the security implemented on every one of these connected devices must be as strong as that of the server that holds and tabulates ballots.

CONFIDENTIAL

enables direct access to the vote data. This dangerous combination constitutes what is commonly known as a “back door” into the voting system, and together with deleted audit trails presents an undetectable path for unauthorized access to, and illegal manipulation of, election data. The failure of the software firewall is not the only access control that was misconfigured. Access control mechanisms in the DBMS itself failed to prevent the access demonstrated in these relatively simple tests.

It must be emphasized that this test was done on a virtual replica of the Mesa County EMS server, created from an image of that EMS server’s hard drive, and not on the actual in-use election system.⁵⁰

For all practical purposes, the term “Mesa County EMS server” is used to mean the logical image⁵¹ of the Mesa County EMS server recreated from the forensic, integrity-controlled Encase Forensic Archive of the actual Mesa County EMS server. The original forensic image of the system was obtained using Access Data’s Forensic Tool Kit Forensic Imaging software. Access Data is an industry-standard forensic software vendor. I had no access to the actual Mesa County EMS server hardware and have relied upon forensic images of that server furnished by legal counsel to create a virtual replica of the EMS server.

Access was attempted and established to the (replica) EMS server to determine the degree to which the EMS server was secured in accordance with legally-mandated VSS standards. The results were alarming. It was found that the SQL Server databases on the Mesa County EMS server were unprotected, beyond a simple password that can be bypassed.⁵² While many potential security restrictions were possible, it was found that surprisingly few were implemented. The SQL Server software on the EMS server was set up with a Windows Firewall with Advanced Security features, however, an explicit firewall rule on the EMS server allowed access directly to the SQL election databases back-end from any IP address in the world.

Security settings relevant to the SQL Server and access to the databases were examined. A subsequent report will address the comprehensive security implementation. This report focuses upon the EMS server’s failure to protect the election databases and the ease with which they can be accessed by any bad actor to change election results.

⁵⁰ A forensic image of a hard drive is a bit-for-bit copy of the user accessible data storage area residing on the data storage mechanism used by the computer system. For a complete discussion of this definition, see Appendix J.

⁵¹ The exact view of disk storage data as seen by the EMS server computer.

⁵² Appendix K.

FORENSIC ANALYSIS

SYSTEM IDENTIFICATION

The Mesa County, Colorado EMS server analyzed in this report is capable of operating on a local area network (LAN). The network consists of several systems, including servers and workstations. The server that was evaluated was named EMSSERVER. It is running the Microsoft Windows Server 2016 operating system.

The forensic evaluation and reviews were based upon a forensic image⁵³ archive collected from the Mesa County EMS server. The forensic image of the EMS server examined in this work was collected on May 23, 2021, before the Secretary of State staff, assisted by DVS personnel, installed their "Trusted Build" software update, as documented below. The serial number of the hard drive shown in the collection data set verifies the data origin to be the physical device.

The backup image was obtained, using forensic imaging methods (an AccessData FTK Imager), from the DVS D-Suite EMS Standard Server, version 5.11-CO, in Mesa County, Colorado, as used in the November, 2020 election. The acquisition data are presented in Figure 2.⁵⁴

⁵³ A forensic image (forensic copy) is a bit-by-bit, sector-by-sector duplicate of a physical storage device's user accessible storage area using specialized hardware and software. To be technically accurate, hard drives contain a "service area" that is not accessible by the user or the Operating system, nor by forensic software; this service area is accessed by the drive's internal controller. The service area is used by the firmware in the disk drive to identify defects in the media introduced during manufacture as well as those identified during operation. Making a perfect magnetic storage platter would be prohibitively expensive thus they are made to be fault tolerant, and the defective areas are simply skipped by using a defect-map. Forensic imaging is a much more comprehensive representation of the state and configuration of the imaged system than could be obtained using simple file backup methods. Forensic Imaging copies data from the subject data storage media without altering the original data in any way. The image includes all files, folders, and unallocated, free, and slack space as well as copies of internal Microsoft files that are protected from access during a normal backup (including the MS "Registry database" and other protected files). These forensic images include not only all the files visible to the server operating system but also deleted files and fragments of files left in the slack and free space as well as every digital bit of data present on the storage medium. When multiple disks are configured into a Redundant Array of Independent Disk (RAID) array, the RAID controller provides a "logical view" of every bit on the media to provide a sector-by-sector bit-for-bit copy of the storage medium; this permits, for example, the use of two identical disk storage devices to provide double the space of a single device, or two devices configured as mirror images of each other to provide failure redundancy. While there are many different configurations for RAID subsystems, a RAID subsystem provides the exact same view of the storage medium and data access to a forensic imaging process as it does to the computer in which it is installed.

⁵⁴ To the extent that personal identifying information was identified in Figure 2, it has been removed. This in no way affects the accuracy of the findings in this report or the evidence.

Created By AccessData® FTK® Imager 4.2.0.13

Case Information:

Acquired using: ADI4.2.0.13

Case Number: 052321

Evidence Number: 00003

Unique description: EMSSERVER

Information for F:\EMSSERVER\EMSSERVER:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 121,534

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 1,952,448,512

[Physical Drive Information]

Drive Model: DELL PERC H730 Adp SCSI Disk Device

Drive Serial Number: 00222e64128c016e1d004fc54220844a

Drive Interface Type: SCSI

Removable drive: False

Source data size: 953344 MB

Sector count: 1952448512

[Computed Hashes]

MD5 checksum: 3d7cf05ca6e4 2db765bf5c15220c097d

SHA1 checksum: eab06a7ea23586de2746b9142461717e075f5c9f

Image Information:

Acquisition finished: Sun May 23 2021

Figure 2 - Mesa County, Colorado EMS server (5.11-CO) Forensic Image Attributes

AUTHENTICITY

When forensic images are acquired, a hash function⁵⁵ is computed. This hash function is far more than a checksum, despite the "checksum" reference in Error! Reference source not found.. The mathematical complexity of the hash function is sufficient such that there is only an infinitesimally small probability that any two different source files can produce the same resultant hash.⁵⁶ This hash can be used at any time to validate the integrity of the image to ensure that it has not been edited, modified, or changed in any way. The hash function result from the acquisition of data appears in the text above but also appears inside each respective archive and authenticates the data by demonstrating it has not changed since it was acquired. Moreover, two different hash functions (MD5 and SHA-1) are in the image and have never been shown to be simultaneously compromised in the same attack.

The hash function results were compared and match the data from the original collection of the forensic image. This provides the greatest mathematical assurance possible that the data in the forensic image examined is a true, authentic and unaltered copy of the original disk data.

Further confirmation that these are genuine images from the Mesa County EMS server has been provided by the Colorado Secretary of State's office. See:

<https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2021/PR20210817MesaCounty.html>⁵⁷

Chain of Custody

Digital chain of custody is the record of preservation of digital evidence from collection to presentation in the court of law. This is an essential part of the digital investigation process. The chain of custody is probative that the digital evidence presented to the court remains as originally collected, without tampering. The image analyzed in this report was obtained through AccessData FTK Imager 4.2.0.13.

⁵⁵ A hash function is a mathematical algorithm that converts an input (e.g., the bits of a file, or all the files on the hard drive) of arbitrary or variable length into an encrypted output of a fixed length. The purpose of the hash in this case, is to create a "signature" for the file or hard drive, such that any other party at any other time, can compute the hash of the file, files or hard drive and confirm that they are identical, because the hash outputs match.

⁵⁶ While the SHA-1 128-bit algorithm has been found possible to compromise, the attack required 9,223,372,036,854,775,808 computations of the algorithm. This is the equivalent of 6,500 years of single-CPU computations or 110 years using today's modern Graphics Processing Units (as used in mining cryptocurrency). This attack required the use of two specifically-designed different files that produce the same hash, created by expert mathematicians explicitly for this purpose. Such an attack may be within the capability of a Nation-State or by spending an enormous amount on cloud computing. In its application as a sophisticated checksum, the effort to change an original dataset into a specific altered dataset with the same hash would present astronomical difficulty much greater than the 9.2 quintillion (quintillion means $\times 10^{18}$) computations in the attack referenced here, would require extraordinary resources, financing and would be exceptionally difficult to conceal. The likelihood of this occurring is infinitesimally small. The likelihood of this occurring undetectably is virtually zero. The probability of two different message digest algorithms being simultaneously fooled is nearly impossible and has never been shown to be possible.

⁵⁷ Reproduced in Appendix M.

I have reviewed the documented chain of custody for the image and have determined that the chain of custody is complete from the forensic operator utilizing FTK Imager through the source from which I directly received these images. (Because of the pending civil litigation and criminal investigation, the written documentation remains in the custody of counsel for later introduction in court proceedings and thus is not included as part of this report.)

Tools Used

The initial forensic image was acquired using Access Data FTK Imager. Once acquired, Encase Forensic was used to maintain forensic integrity of the archive. Autopsy, Encase Forensic, FTK Imager and Oracle VirtualBox were used to analyze the image. All findings were verified with Encase Forensic examination of the integrity-controlled forensic image.

TEST PREPARATION

The Mesa County EMS server forensic image was used to recreate a complete and exact replica of the Mesa County EMS server's software, operating system, and even boot code, which was then launched in an Oracle VirtualBox⁵⁸ virtual computer environment for the examination. This technology is commonly used in software development and testing. This exact replica was used for this examination.

The image was evaluated to gather technical information, including the integrity of the data stored on the system. No effort was made in this analysis to reverse-design, de-compile, or reverse-engineer the compiled binary Dominion Voting System software. Operating system configuration relevant to the operation of the system as well as DBMS configuration was examined. Results relevant to this investigation are documented.

Screenshots are presented that can be used to review and verify these findings and provide step-by-step instructions to reproduce and validate these results. The security of the system has been compromised by the vendor, the Voting System Testing Lab and the Secretary of State's unlawful certification that the system meets all the requirements in law, and exacerbated by false statements that voting systems are safe, secure and have strong integrity. These test results verify the fact. These screenshots were obtained from the mounted forensic images of the EMS server. These results can be reproduced by anyone.

While many of the EMS server settings can be determined from operating system configuration records, it is much easier and far more understandable to view the same information with the Microsoft applications designed for this purpose. The software that serves as the host for the DVS D-Suite voting system applications is the intellectual property of Microsoft, e.g., Windows, SQL Server, and SSMS. The configuration values, or "settings," are determined by the end user, in this case DVS or the Secretary of State of Colorado, but are not proprietary. These are the settings that must be examined, as part of a comprehensive examination, when a voting system is tested for certification.

⁵⁸ The VirtualBox environment provides all of the resources that a server provides, including central processing units (CPUs) and network interfaces. Virtual means that many of the functions normally executed by dedicated computer hardware are instead performed in software, and the interfaces present on the original server are emulated by the host computer's interfaces. None the less, a virtual environment allows us to operate an operating system and application programs *as though* they were running on the actual server hardware.

The security of the entire voting system depends on the totality of all the hardware and software, *combined with* the configuration settings and records of system activity preserved in system log files. Similarly, the security of a home depends not just on having 3 doors and 21 windows, but also whether each of them are locked, as well as whether each of them are monitored on video (equivalently, access being logged) and whether they are each monitored by an alarm system.

The design of the system can be more secure or less secure, inherently, just as a house with 1 door and 1 window is more secure than a house with 10 doors and 20 windows. But voting system testing labs (VSTL) are explicitly required to check and verify these critical settings.

Below are presented screenshots from two different computers used in the testing environment. Each step is explained in detail so that one can easily follow along.

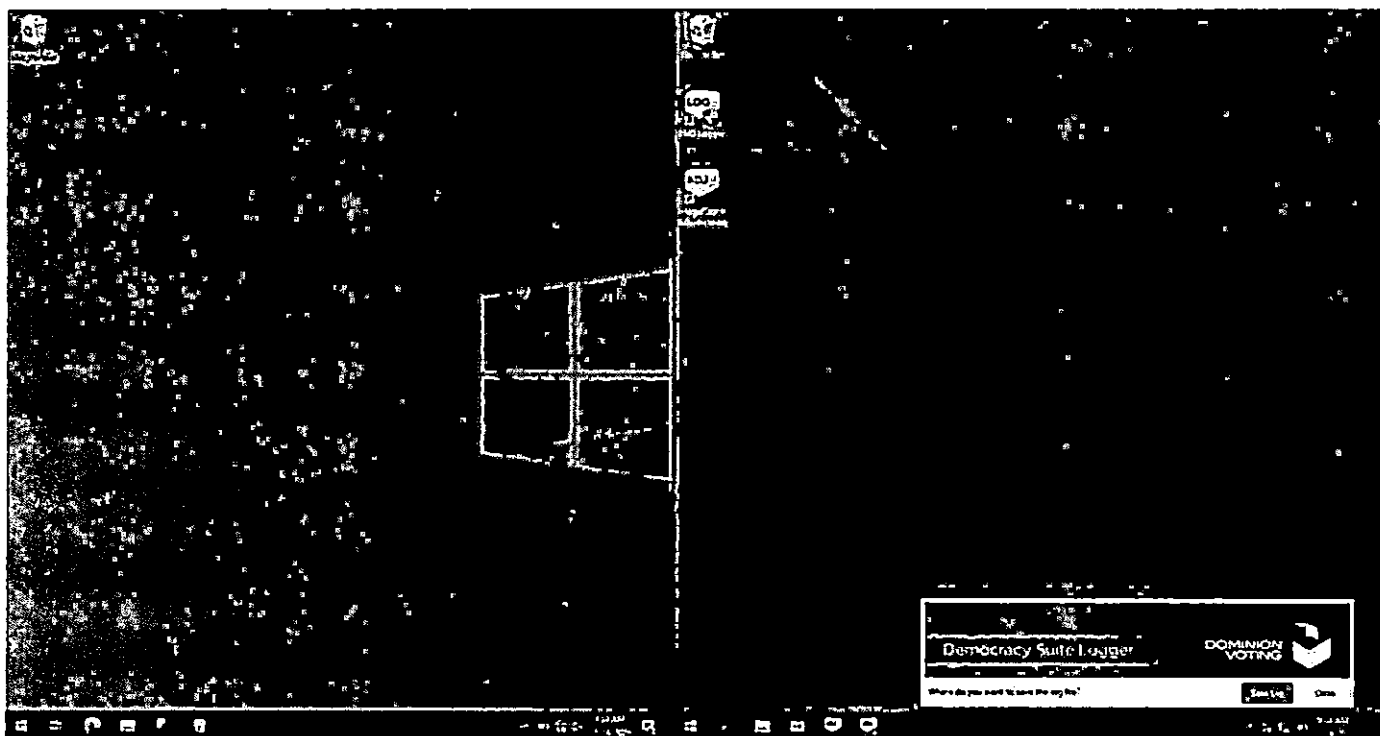


Figure 3 - Test Workstation and Dominion EMS server

On the left side in blue is the Test Workstation running the Microsoft Windows 10 operating system that was used as part of testing. On the right side in red, the emulated Mesa County EMS server, from the EMS Server image, is displayed. The EMS server operating system is Windows Server 2016 and is configured exactly as it was when the image was taken on May 23, 2021. These computers are connected to the same network⁵⁹ for testing.

⁵⁹ The EMS server has its IP address assigned as 192.168.100.10, just as it was while in operation in Mesa County. The Windows 10 computer is also set up on the same 192.168.100.0/24 network just as any device could have been connected at Mesa County. The figures shown in this report are taken from two “virtually” connected virtual

CONFIDENTIAL

Both systems are hosted in Oracle VirtualBox virtual environments on an isolated virtual network (emulated within VirtualBox) for the first test – these two computers⁶⁰ are the only computing devices connected to this virtual network.

The tests were repeated a second time using a physical network connection from a stand-alone test workstation with Windows 10 (within a separate Oracle VirtualBox instance, for forensic sterility) connected by Ethernet cable to a Netgear GS108 gigabit network switch, and then to the VirtualBox instance of the Mesa County EMS server's host computer.

This implementation, and testing with a physical network, together, exactly mimics the functionality of the Mesa County EMS server because it is running the exact operating system and application software, identically configured because it is an exact copy created from the integrity-controlled forensic image. Thus, its response and security controls are identical and well-suited for examination in this manner.

The Mesa County EMS network was connected to other components of the EMS D-Suite, but these components neither participate in, nor could prevent the accesses demonstrated in this test (if not compromised and exploited). They are, with respect to the conclusions of these tests, irrelevant, notwithstanding the possible additional data paths to external networks they may offer in either direction.

environments on a single computer, but the results were verified and duplicated using two different computers and a physical network and network switch, i.e., the test's connection between the two systems made no difference on the results obtained.

⁶⁰ The reference to "Computers" in this paragraph specifically refers to the operational system comprised of electrical computing devices which perform identical functions and the software installed and configured to operate those devices. For example, an Intel i7 Central Processing Unit (CPU) performs identically on every computer motherboard provided that all of its features are properly included in the electrical design of the motherboard. The main characteristic of a computer is determined by the Operating System, its configuration, and the application software and its configuration. Thus it is entirely appropriate to examine the Operating system, application software and their respective configurations to understand the computer system's operational capability and function. The reference to the software as "computers" is intended to describe the software's purpose, capability and functionality as used in Mesa County as a computer system, not to a specific device.

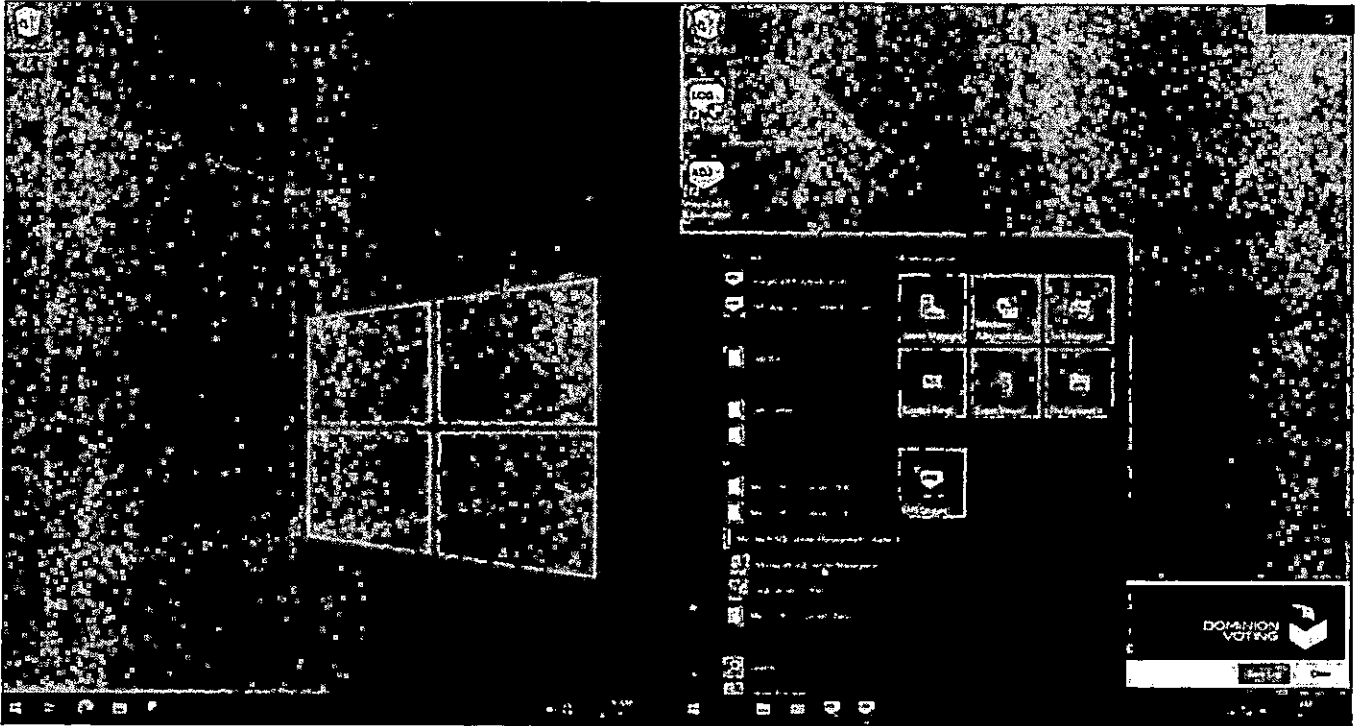


Figure 4 - Installed Microsoft Software

As the Dominion EMS server was examined, the installed Microsoft SSMS software was found listed on the Start Menu.

The presence of SSMS software on the EMS server was unexpected because it enables direct access to the EMS server databases, bypassing the DVS application software. Properly-designed software developed with security in mind would strictly require all database access of any kind (including backup and maintenance) to go through security/tracking/auditing components as part of the design.

The very dangerous side effect of having or allowing Microsoft SSMS software on a voting system is that it can enable surreptitious access to the voting database and is a concern if it is configured to allow such access. Therefore, it is necessary to examine the EMS server's entire software configuration.

Finding 1: The Mesa County EMS system used in the 2020 General Election had Microsoft SQL Server Management Studio 17 installed as configured by Dominion Voting Systems. This software is not listed on the official test report or application for certification. As it was not tested, the unauthorized installation of this software violates and renders illegal the certification of the voting system for use in an election.

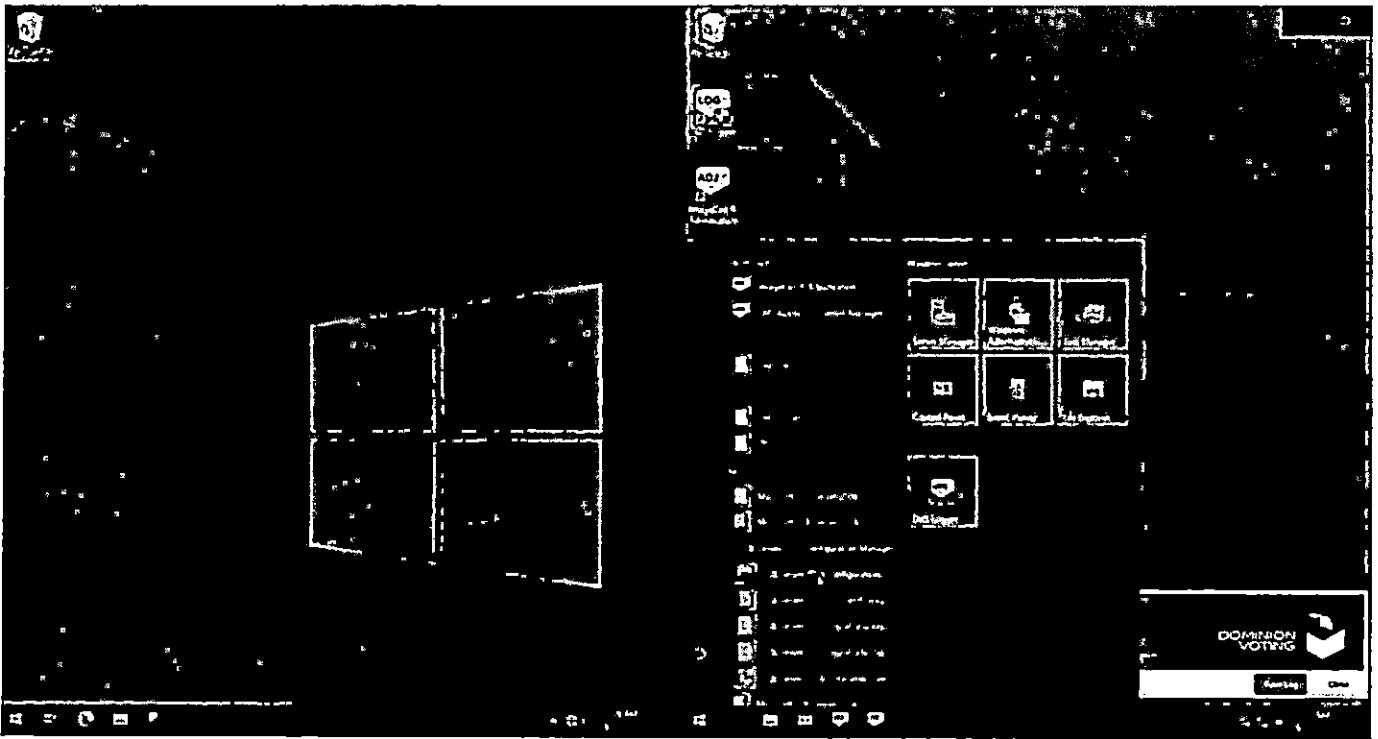


Figure 5 - SQL Server 2016 Configuration Manager

To determine how the SQL Server is configured and whether unfiltered and uncontrolled access is permitted, I examined its configuration through the software application provided by Microsoft entitled "SQL Server 2016 Configuration Manager" as shown in Figure 5.

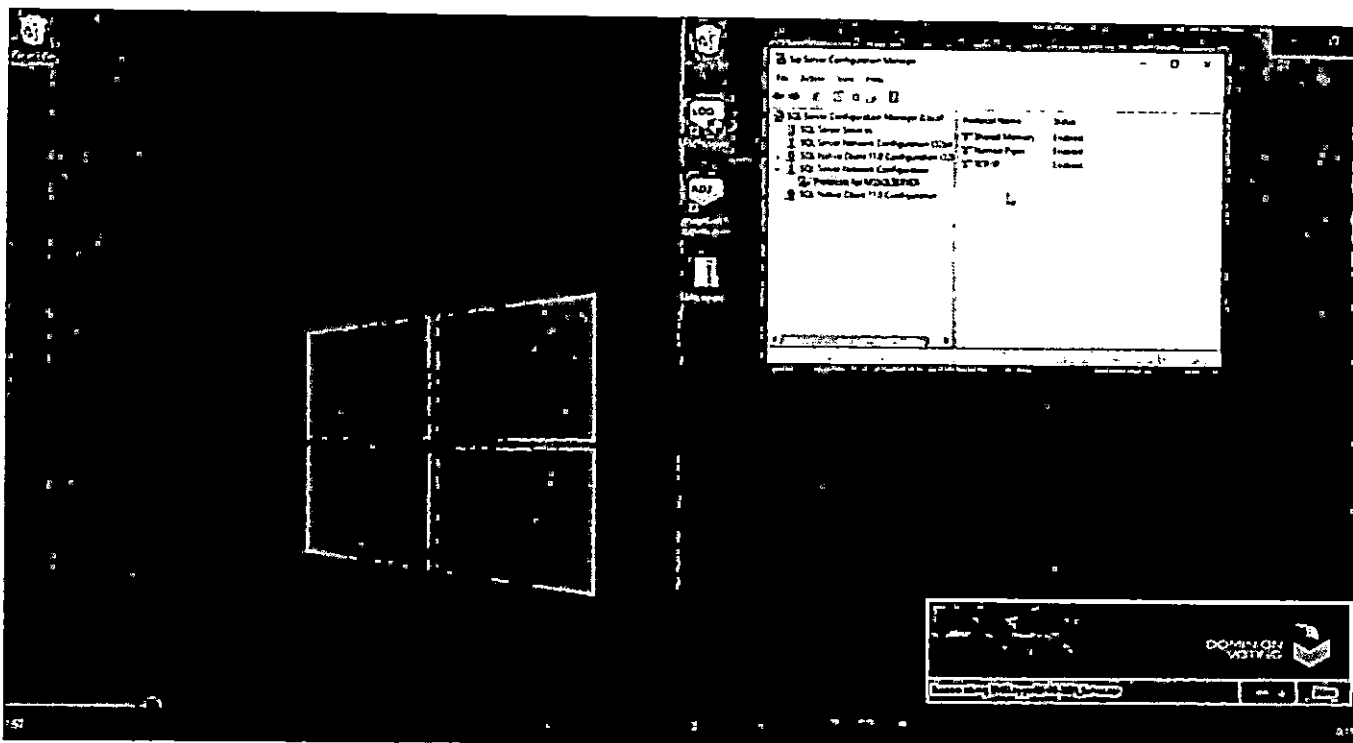


Figure 6 - SQL Server 2016 Configuration Manager – Network Protocols enabled

All three of three possible SQL server protocols were left “Enabled,” providing pathways to the database above what are required for operation. These extra pathways can severely reduce system security.

Under the SQL Server “Network Configuration” the menu item is selected titled “Protocols for MSSQLSERVER” that shows that more protocols are enabled than should be, especially for a “secure” system. While one of these may be necessary, all three being enabled presents an unwarranted risk.

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled

Microsoft states, in its SQL server documentation⁶¹ that:

“To enhance security, SQL Server disables network connectivity for some new installations. Network connectivity using TCP/IP is not disabled if you are using the Enterprise, Standard, Evaluation, or Workgroup

⁶¹ <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/default-sql-server-network-protocol-configuration?view=sql-server-ver15>

CONFIDENTIAL

edition, or if a previous installation of SQL Server is present. For all installations, shared memory protocol is enabled to allow local connections to the server.”

For an election management system, it is entirely inappropriate and irresponsible to enable Shared Memory or TCP/IP access over an unsecured network connection, and particularly careless and irresponsible to enable these together with “Named Pipes.” Shared Memory access permits an intruder to install malicious software and to execute arbitrary commands with full administrative privileges if exploited. Given the exceptionally minimal protection implemented on this server, if any connection were made to a network that provides a path to the Internet⁶² by the EMS system, any other computer connected to the Ethernet network would be granted access to the TCP/IP ports⁶³ enabled by the EMS server and a hostile party would be able to penetrate and alter the EMS server.⁶⁴ In the examined state of the EMS server, if this network *or any computer connected to this network* were connected to the internet either directly or indirectly, by wire or wireless, a hostile party *anywhere in the world* would be able to penetrate and alter the EMS server, including altering actual election records, like tabulated vote databases.

A computer system configured in this manner should never be used in any critical infrastructure or high security environment and, as a voting system, should be immediately decertified and those responsible for creating and selling such system investigated.

While multiple security mechanisms exist within a Microsoft Windows 2016 server, including the Microsoft Windows Defender firewall, SQL database permission restrictions, Operating System security Policy, Group Security Policy, file access control lists, and much more,⁶⁵ some were configured not to protect the server but instead to allow all “local” and “remote” access. Tests conducted in this examination demonstrate that not only are those explicit programmed settings misconfigured, but that no other security mechanisms within the installed hardware and software prevented the ability to access and change election data, or even to provide any warning of such drastic and consequential access.

⁶² Given the exceptionally large number of wireless devices in this election infrastructure (thirty-six), particularly in the context of the plethora of improper security configuration mistakes made in this installation, examination of every device in the infrastructure including the wireless printer must be undertaken before the network can be considered secure; absent appropriate systems log data, such a determination might not be possible.

⁶³ TCP/IP networks identify computer systems by their IP (Internet Protocol) address. TCP/IP further identifies the specific service (email, file transfer, database access, etc.) to be used on the destination computer using a port number transmitted within the beginning of the packet (in its header). Standards identify the assignment of port numbers to specific services, for example, web browsing uses port 80, encrypted web browsing uses port 443, email uses port 25, and database access using the Structured Query Language (SQL) uses port 1433. There are 65,536 available port numbers. Ports 0 through 1,023 are assigned to commonly used services/protocols, 1,024 through 49,151 are sometimes registered to a specific service, and those remaining are available for dynamic use (e.g., as needed). One can conceptually think of these ports in the same way we think of channels on cable TV – each is associated with specific content.

⁶⁴ For example, see CVE 2018-8273, CVE 2021-1656, CVE 2020-0618 at <http://cve.mitre.org> and Microsoft Knowledgebase KB 4073225 regarding the “Meltdown” and “Spectre” vulnerabilities presented by the “management engine” back door in every CPU manufactured since 2007 whether Intel, AMD or ARM processors.

⁶⁵ See the US Department of Defense Security Technology Implementation Guides (STIGs), at <http://public.cyber.mil>

There is a great misunderstanding about intrusion into computer systems. Many people conceive of it as depicted by Hollywood, where an intrusion takes several minutes or significantly longer. While this makes for good drama, it is not realistic at all. In the real world, malicious actors – particularly hostile nation-states, e.g., China, Russia, North Korea and Iran to name a few, have extremely sophisticated cyberwar capabilities. They are capable of intruding and *altering data* in a matter of less than a few seconds and they engage in persistent cyber operations to penetrate and compromise supply chain, industrial base, trusted vendors, academia, and government offices which might someday afford access.

Intrusion can be accomplished without a direct connection to the target computer. In the case of a voting system, using the example of an Adjudication Workstation connected via wired Ethernet to the EMS, if the Adjudication workstation has a wireless (Wi-Fi) interface, such a connection might be automatically connected to external devices and networks without the EMS or Adjudication workstation operator ever noticing it, especially since all laptops today have both wired Ethernet and Wi-Fi interfaces which might enable an Island-Hopping attack. Thirty-six (36) wireless devices were identified in the Mesa County DVS D-Suite system (e.g., on the DVS D-Suite ICVA computers and ICX tablets and one Dell E310DW wireless printer, with IP address 192.168.100.11, set as the default printer on the EMS server). Any other connected device, including a printer like the one installed on the Mesa EMS infrastructure,⁶⁶ creates an increase in this risk exposure. This is why an Internet connection in any device or computer, even several connections removed, is so extremely dangerous to critical systems. To mitigate this risk, the US Department of Defense (DoD) maintains special closed networks for sensitive information, which are forbidden to have internet connections or connection to any system with an internet connection.

Appendix D lists some of the more notable nation-state cyber-attacks as well as a link to an online video of one cyberattack that completely destroyed a power generation facility. Adversaries constantly scan and probe every computer on the internet, and through those computers, other devices and computers not directly connected to the internet, to identify weakness well in advance of the need for an attack. Today's attacks occur very quickly, in a matter of seconds.

⁶⁶ At Bell Laboratories in the 1980's, printers that used the Postscript language were exploited (to leverage their computational power) in this manner because they were the first to have a bi-directional communication connection (e.g., able to talk back to the host computer, over a network). Today's printers all have this capability and present a risk of being a component of an Island-Hopping attack.

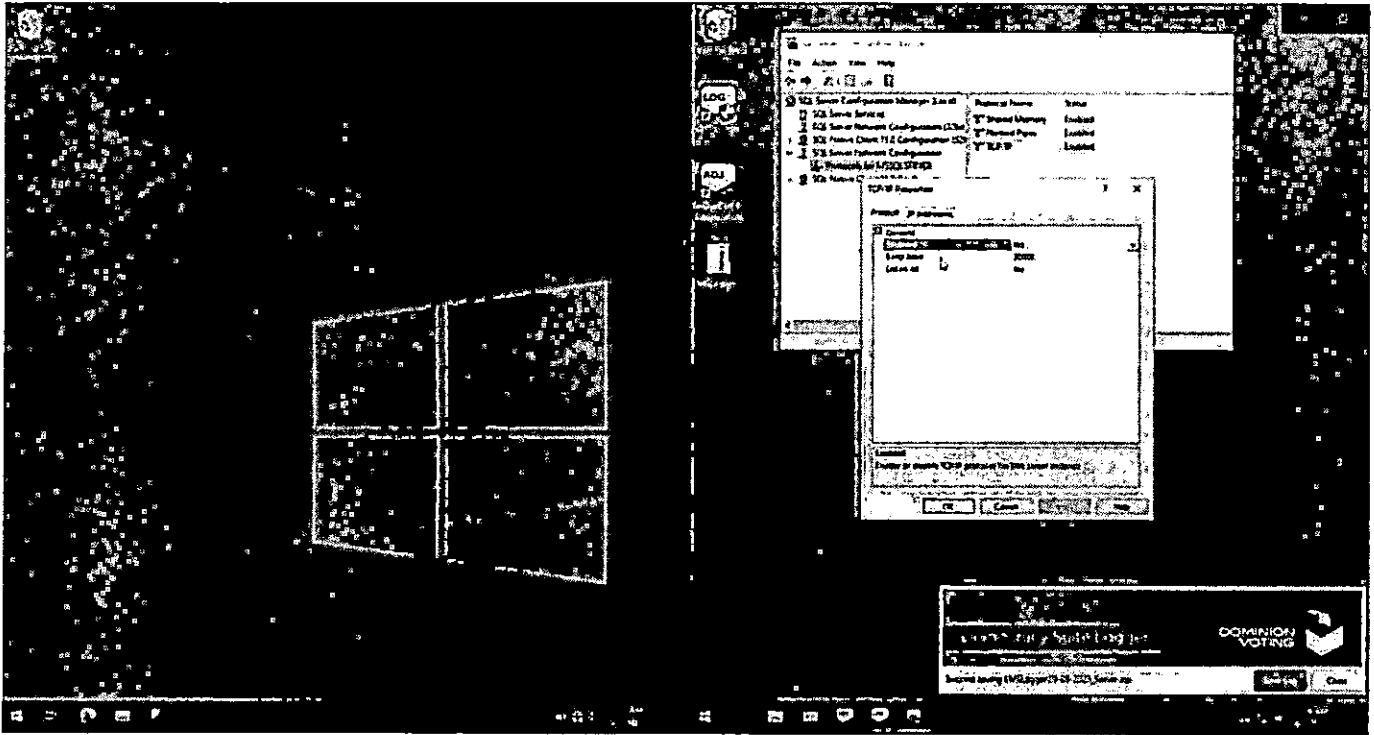


Figure 7 - TCP/IP Properties

The TCP/IP protocol setting in Figure 7 has "Enabled" set to "Yes" on Mesa County's EMS Server, and the configuration setting above has the parameter "Listen All" set to "yes" indicating that the SQL Server will listen on every network connection. More detail for the TCP/IP protocol is in Figure 8.

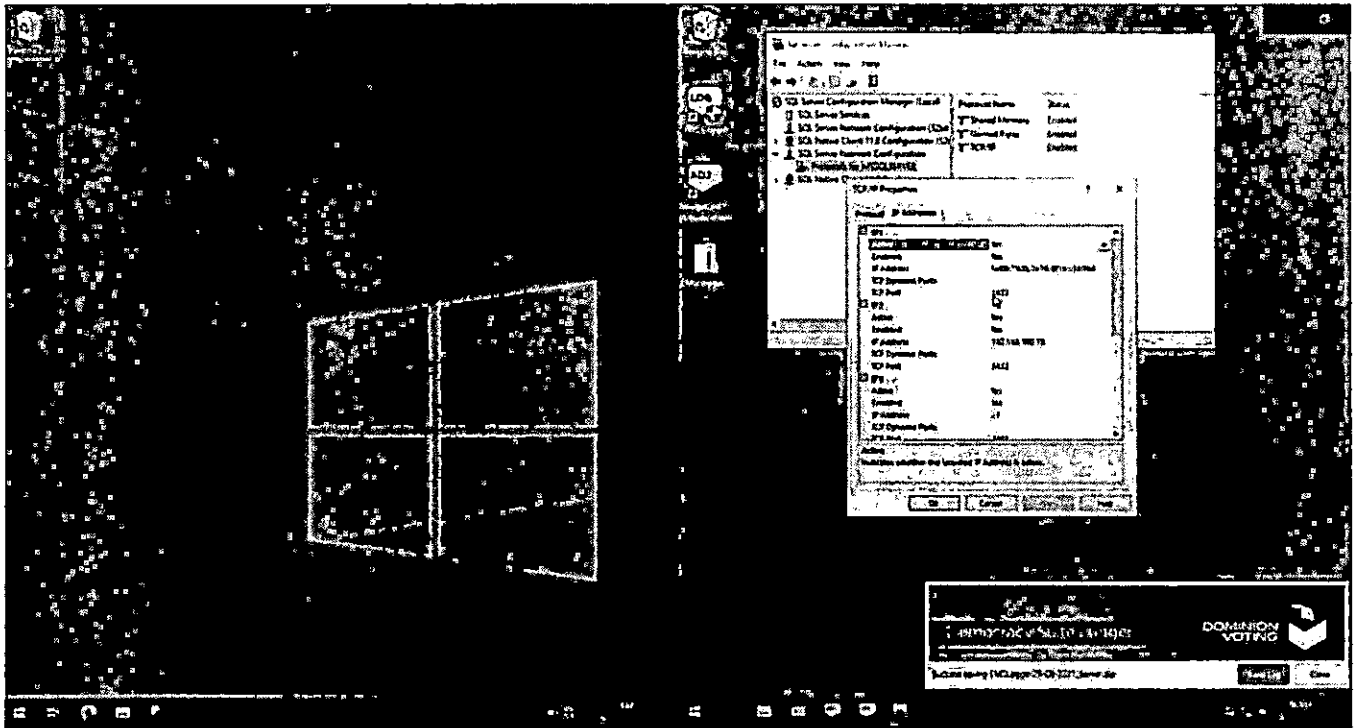


Figure 8 - TCP/IP Properties of SQL Server, attached to port 1433 the standard (default) port.

Figure 8 shows the SQL server is bound to and active on all Ethernet interfaces. This allows multiple electronic pathways to the server over multiple network connections should someone connect a cable into that jack. Also important to note is the default port number 1433 being used, instead of a more secure alternate port.

IP2 shows the IPv4 address 192.168.100.10, an IP address assigned to be used by the Mesa County EMS server. For a discussion of IP addressing fundamentals, see Appendix C. IP Addressing Fundamentals.

The Mesa County EMS server is a Dell PowerEdge T630 server, serial number 4NV1V52, and has 3 Ethernet interfaces (or Network Interface Cards (NICs)) – 2 of them assigned to the computer itself and one assigned to a separate controller (the iDRAC, Integrated Dell Remote Access Controller) which can be used to allow remote control of the computer including power-on, power-off and privileged access to the computer, via this integrated remote access controller (iDRAC). The interfaces accessed via the Server Configuration Manager (shown in these Figures) are those IP addresses assigned to the computer and do not include the interface assigned to the iDRAC.

A conclusive determination that these IP addresses had a connection to another network, even the Internet, is not possible without examining the physical system, as well every other device connected to the network. Most network firewall/router devices use translation (network address translation, NAT, or port address translation, PAT) and most computers/devices with multiple network interfaces (Wi-Fi, and wired Ethernet, for example) can be compromised to implement an Island-Hopping attack (using malicious software that provides translation, even though standards may prohibit it).

Absent a full forensic examination of all network and computing devices, it can be challenging to factually conclude that connection to the global Internet was, or was not, present and in operation. Given that

network systems are designed to support Internet connectivity, other evidence (including the alteration, addition or exclusion of votes, or data in log files, for example – See Report #1) must be considered, may be the only artifacts that enable detection or conclusive determination, and may indicate a probability that such a connection may have been in use.

I was told that when this exact copy (forensic image) of the Mesa County EMS server was taken, the Mesa County EMS server was connected to a (wired) computer network via its Ethernet interface. Configuration data forensically extracted from the EMS server, including some log remnants and registry configuration data validate this information about the connection to a network.

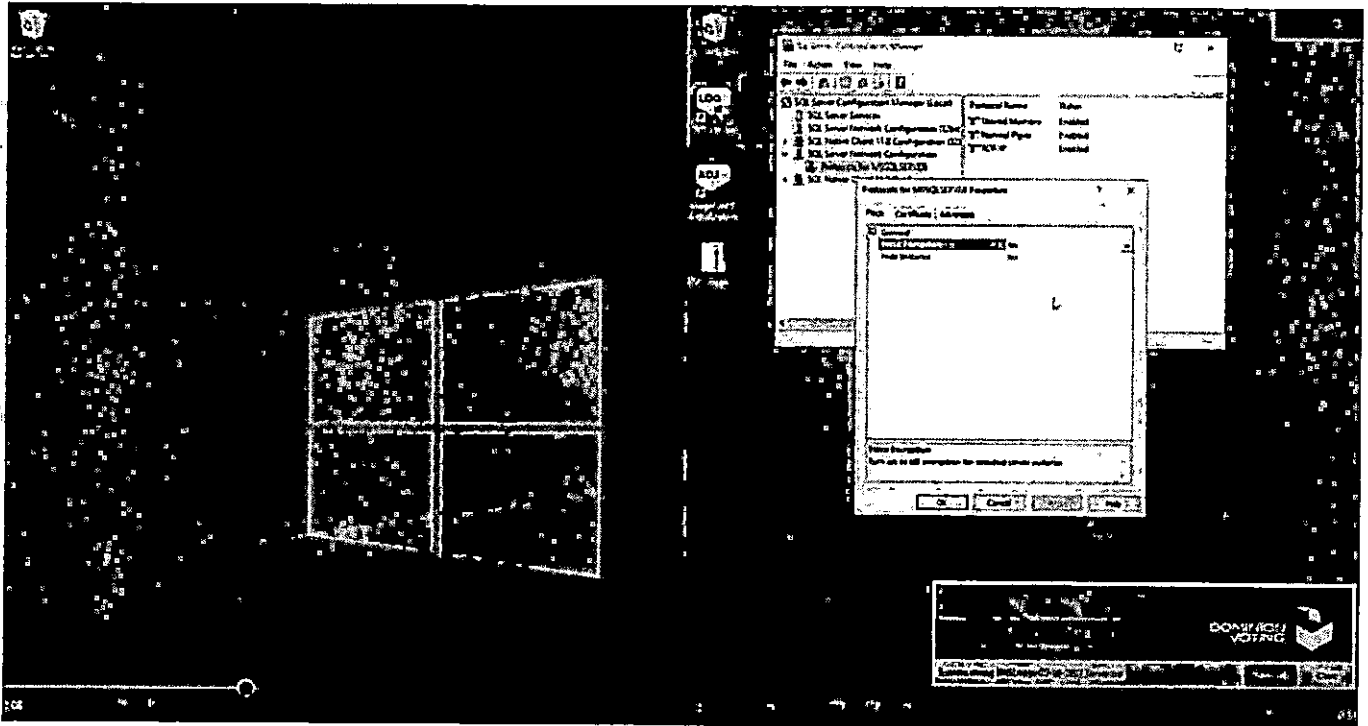


Figure 9 - SQL Server Properties

The SQL Server service is configured to force network communication to be encrypted. This is an expected configuration; however, it is crippled by what was found next.

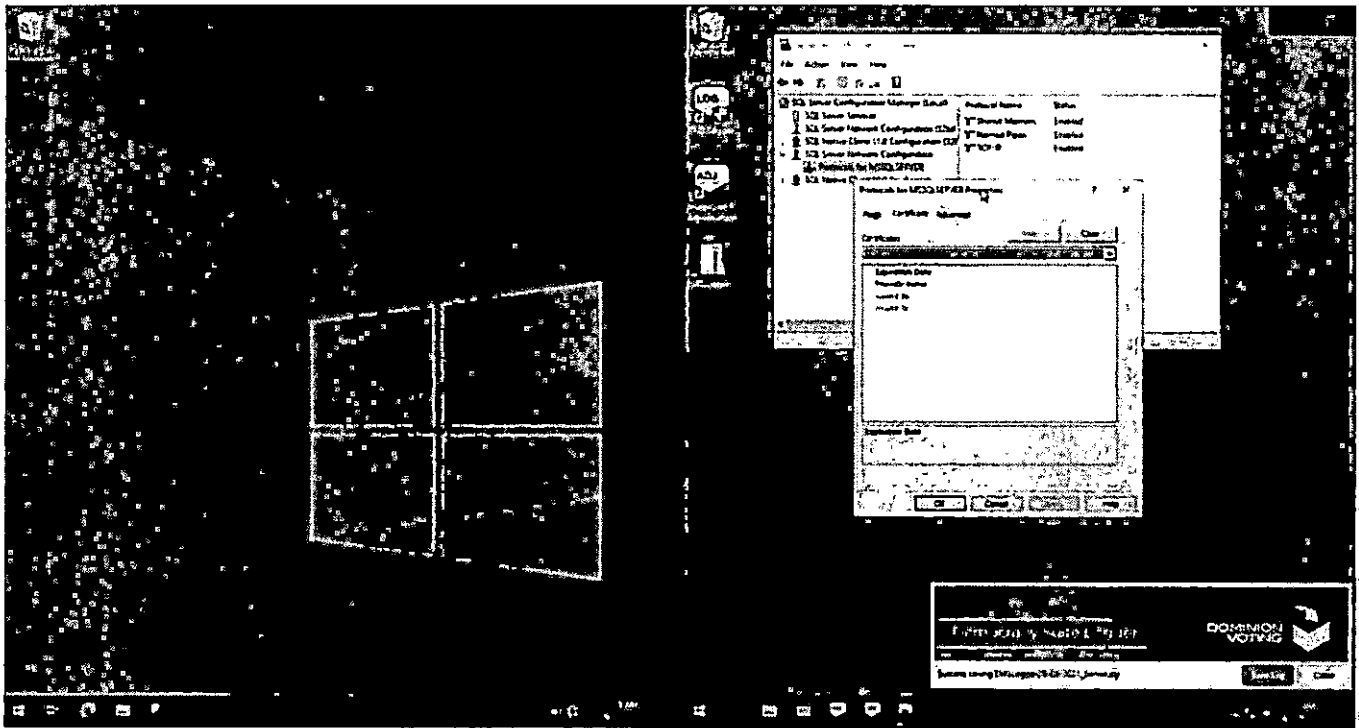


Figure 10 - Encryption is enabled but No Encryption Certificate is configured

No encryption certificate is configured, which causes the server to use a 'self-signed' certificate that is extremely vulnerable to a common man-in-the-middle attack. This means that the communication to and from the voting database itself could be intercepted, viewed, and changed, without detection.

A man-in-the-middle attack is explained in Appendix H.

The SQL Server Documentation directly provided by Microsoft clearly states "Self-signed certificates do not guarantee security. The encrypted handshake is based on NT LAN Manager (NTLM). It is highly recommended that you provision a verifiable certificate on SQL Server for secure connectivity. Transport Security Layer (TLS) can be made secure only with certificate validation." (<https://docs.microsoft.com/en-us/sql/relational-databases/native-client/features/using-encryption-without-validation?view=sql-server-2016>)

CONFIDENTIAL

EXAMINATION OBJECTIVE 1:

Determine whether calculated vote totals can be altered by anyone with physical access to the logged-in EMS server.

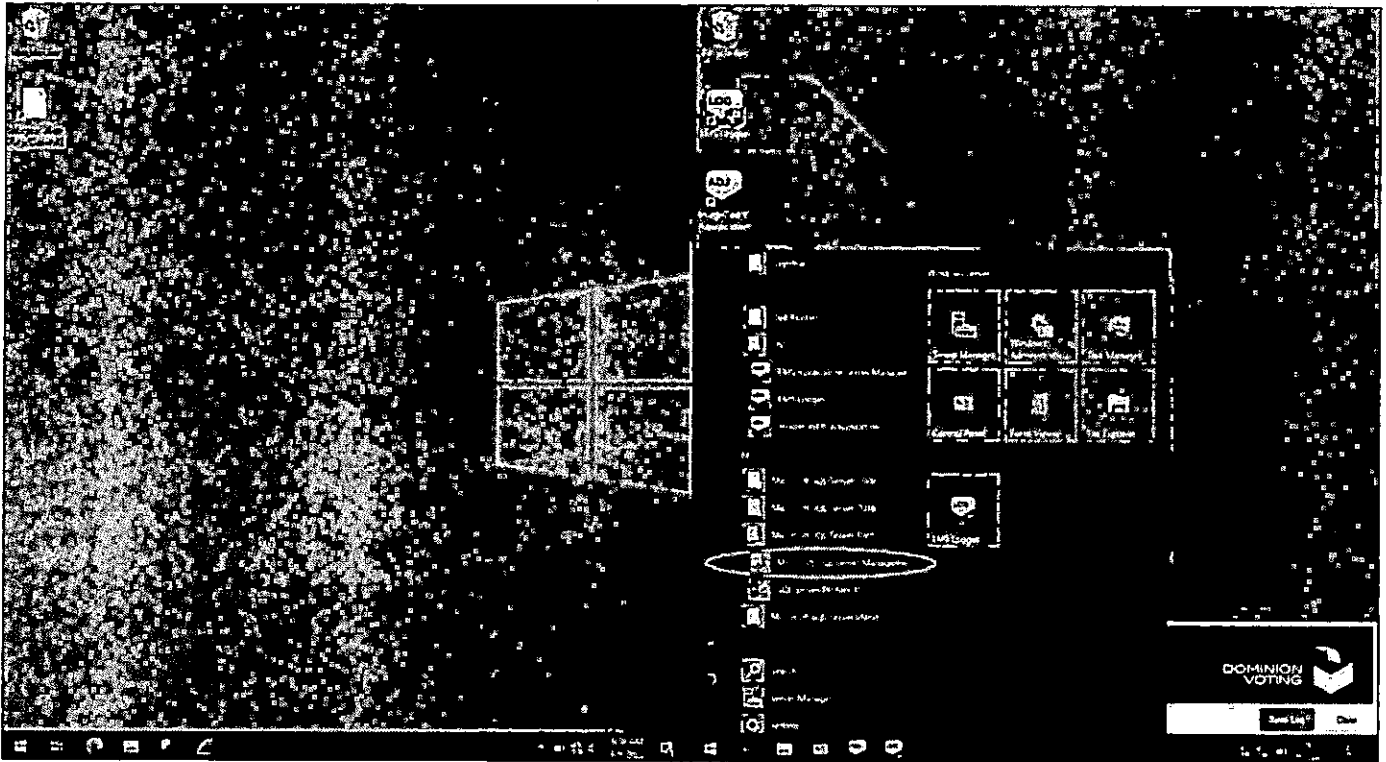


Figure 11 - SQL Server Management Studio (SSMS) software showing in the EMS server Start Menu

Microsoft SQL Server Management Studio (SSMS) allows direct back-end access to and manipulation of SQL Server databases. Figure 12 shows this software is found already installed on the EMS Server.

The VSS explicitly prohibits voting systems from allowing any users to change calculated vote totals, or an individual vote, or to compromise ballot security; the VSS also mandates the retention of all audit trails for 22 months specifically to enable detection of civil rights violations or intentional manipulation and fraud, and to support litigation and prosecution. SSMS enables that prohibited ability, as demonstrated in this test.

The Mesa County EMS was protected by only a (Windows authentication) password, as this test demonstrates. The use of a password alone is not secure; this fact is taught routinely in training for the board certification "Certified Internet Systems Security Professional" (CISSP), emphasizing the principle of "Defense in Depth," e.g., multiple layers of security.

Passwords are compromised often.⁶⁷ As early as 1985, the US Government published, in its "rainbow series" of security publications from the DoD, the "Green book"⁶⁸ guide to password management. While the password management recommendations in the guide are considered obsolete today, its appendices explain the mathematical calculation for the probability that a password can be guessed based on the complexity of the password, how often the password is changed, and the speed with which a computer can execute those guesses. Today's computer processor execution speed (CPU clock rate) is 5,000 times faster than computers were in 1985. Today's gaming home computers are 5 times faster than the fastest computer in the world was in 1985,⁶⁹ and systems used for crypto-mining may be as much as 100 times faster than that fastest 1985 computer.

Password insecurity alone presents an extreme and unacceptable risk.

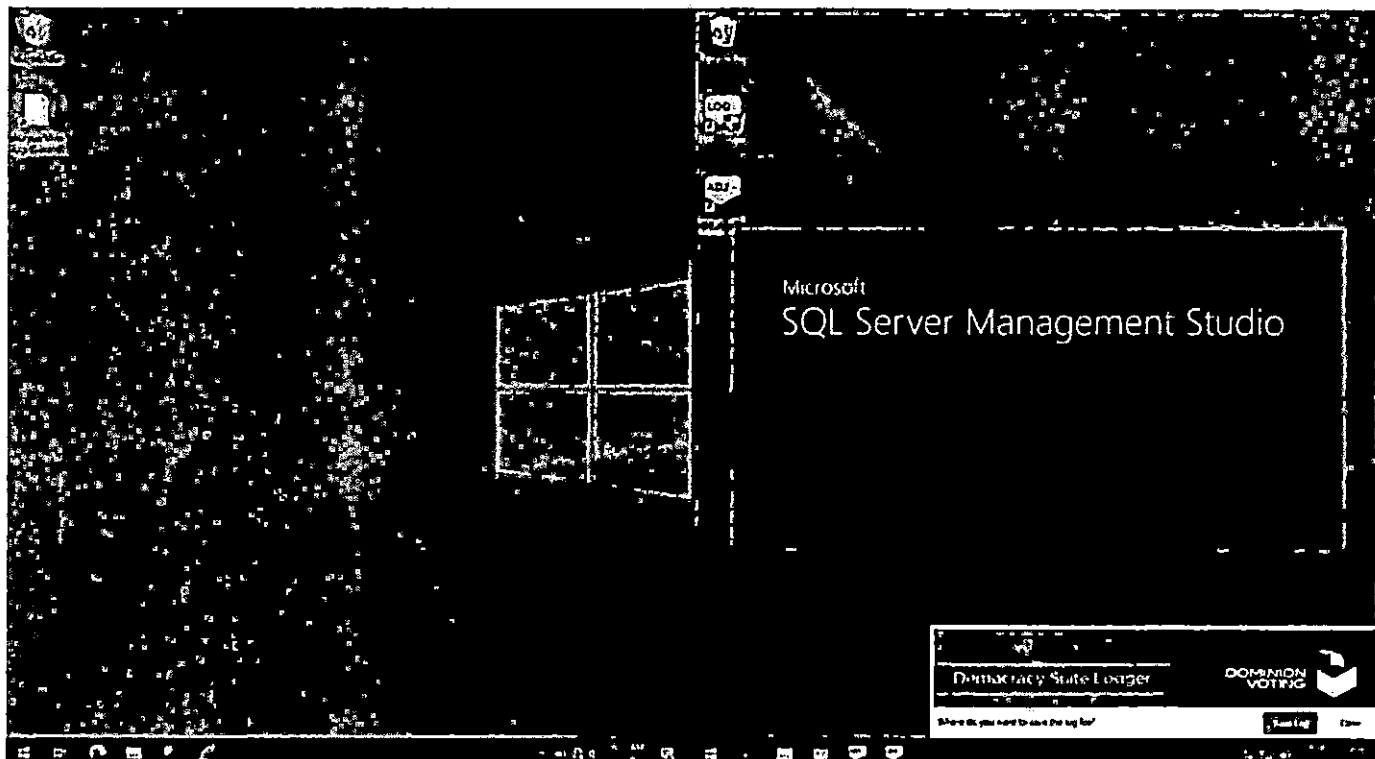


Figure 12 - SSMS is installed and starting on the EMS server system.

The SSMS starts up without any problem or warning when a user clicks on it.

⁶⁷ Accounts in public media support this fact. These are only several of many such references: <https://www.westernjournal.com/az-audit-exclusive-election-systems-password-hasnt-changed-2-years-shared-time/> and <https://www.csoonline.com/article/3266607/1-4b-stolen-passwords-are-free-for-the-taking-what-we-know-now.html>

⁶⁸ <https://csrc.nist.gov/CSRC/media/Publications/white-paper/1985/12/26/dod-rainbow-series/final/documents/std002.txt>

⁶⁹ A Cray X/MP supercomputer operated at a clock speed of 1 GHz, or 1 billion clock cycles per second in 1985, while the first home PC clock speed was typically 1MHz.

Not only can SSMS be used on a separate computer, not part of the DVS system, to directly access the back-end server databases, it can be used directly by any person with physical access to the logged in server itself (screen, keyboard, and mouse), such as rogue election staff, cleaning staff, etc.

In addition to bad-actors from outside the election staff, any individual election staff worker that has access to a logged-in EMS server also is allowed the ability to go directly into the back-end of the database and add votes, change votes, delete votes, swap votes, and countless other alterations, bypassing all DVS application software. Even an honest individual could accidentally allow data to be changed without their knowledge in a matter of seconds by innocently attaching a USB flash drive with hidden programming/malware on it.

Anyone with unrestricted physical access and knowledge of the userID can make similar changes without even a password, if the standard user account is left logged-in. Someone with advanced security knowledge can access the system without a password, as I was easily able to do.

In this test the Microsoft SQL Server Management Studio is used to demonstrate unauthorized access to the election databases. However, the use of Microsoft SSMS is not even required – a popular piece of software manufactured by SQL Pro (e.g., non-Microsoft software) is shown in the third test in this report, to provide the same access from the more limited computing power of a mobile phone.

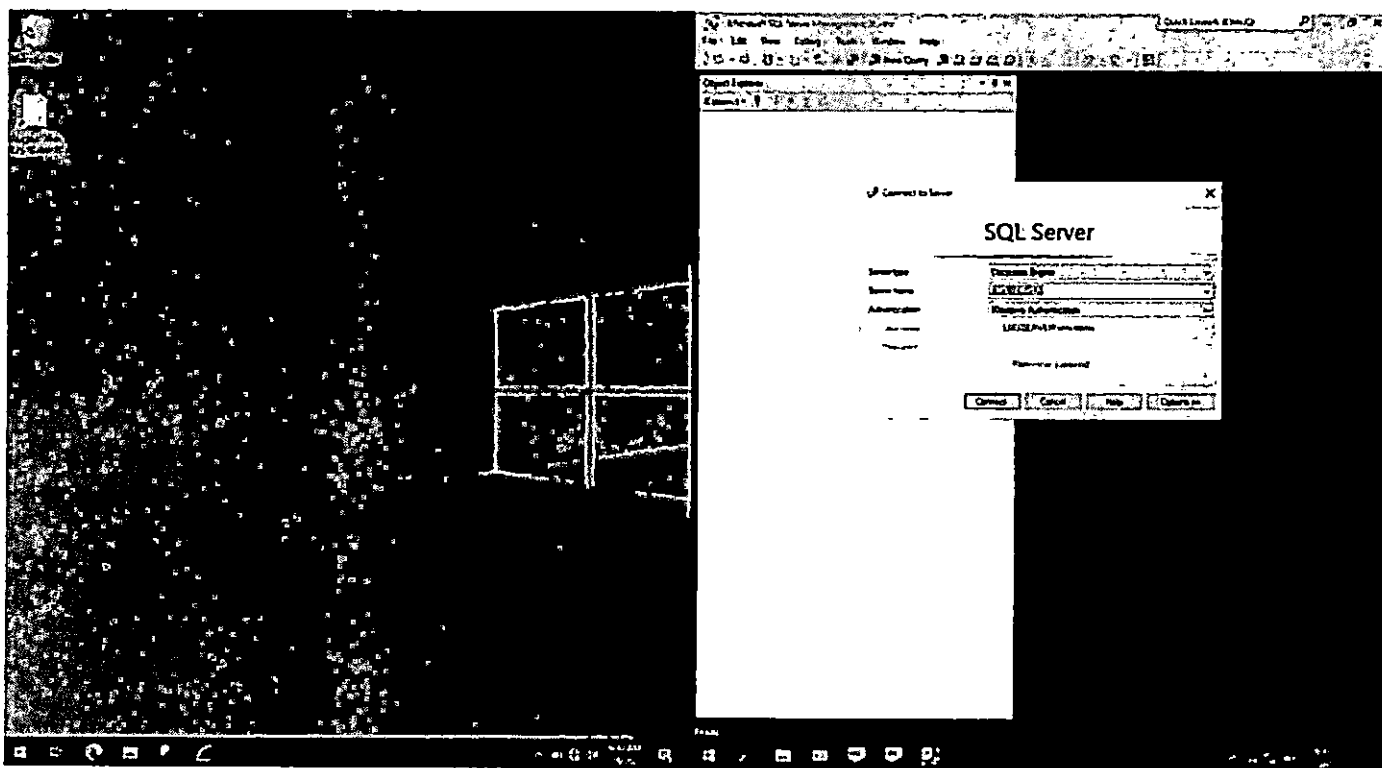


Figure 13 - Logging in to the SQL Server using SQL Server Management Studio

When SQL Server Management Studio (SSMS) first starts, connection entries are already pre-filled-out. The user doesn't need to type a username or password, and needs only to click the 'Connect' button to get into the back-end databases.

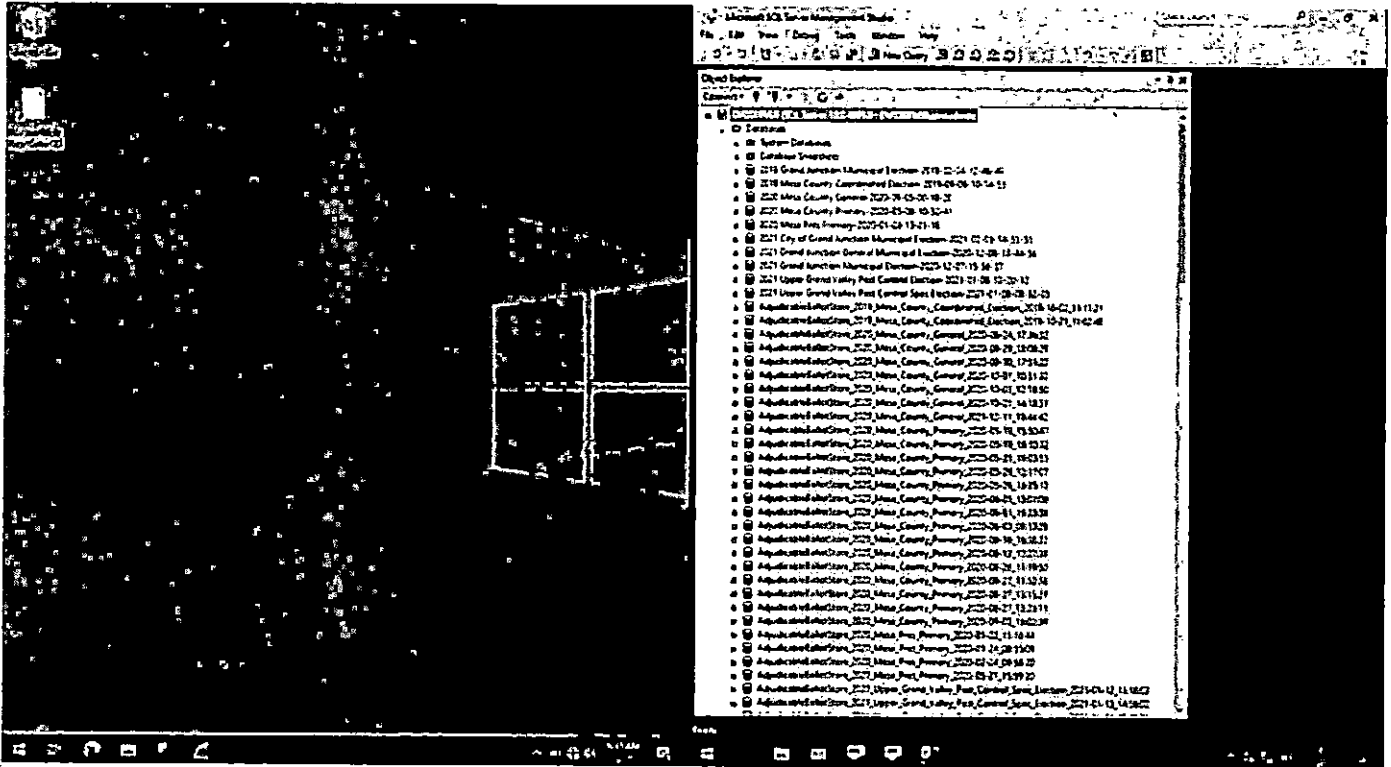


Figure 14 - SSMS enables direct access to the internal databases to anyone logged in to the EMS server

After clicking 'Connect,' and then the '+' sign next to 'Databases' all the internal databases are shown to be accessible. It took only four clicks of the mouse to get here into the back-end of the voting databases.

One of the many election databases that are shown is from the 2020 US General Election. The US Presidential Primary of 2020, among many others, can also be seen.

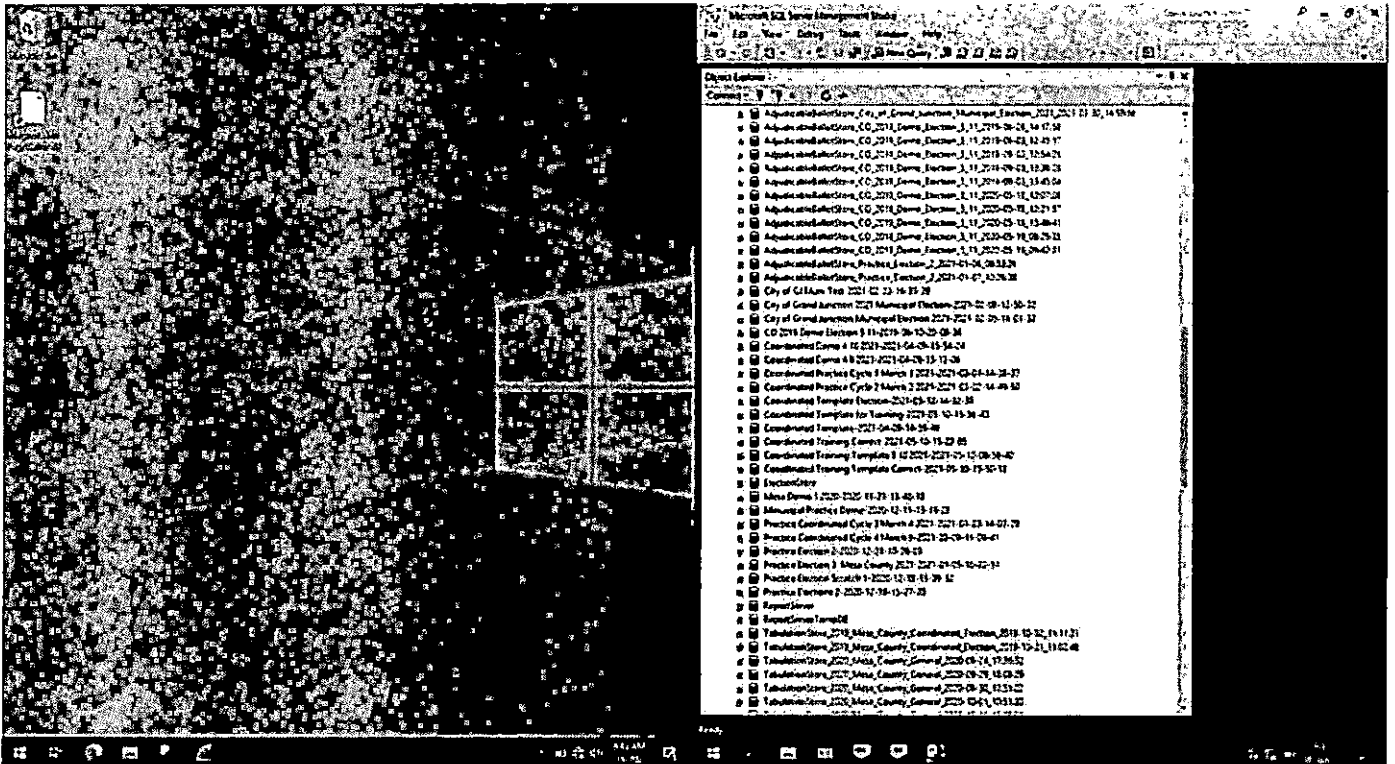


Figure 15 - Databases from many prior elections are fully accessible

Here can be seen accessible many elections from the City of Grand Junction, Mesa County, as well as adjudication and tabulation databases from many of these elections.

The presence of databases from previous elections on the EMS server, provide a rich library of information that can be used to understand and identify potential vulnerabilities in the EMS. While these records are required to be retained, they should be maintained off- system, securely archived, inaccessible to the EMS or any user.

The presence of prior election databases on the EMS server also offers an extensive and convenient repository for copy and paste modifications of election data, not only for the 2020 election but for any prior listed election as well.

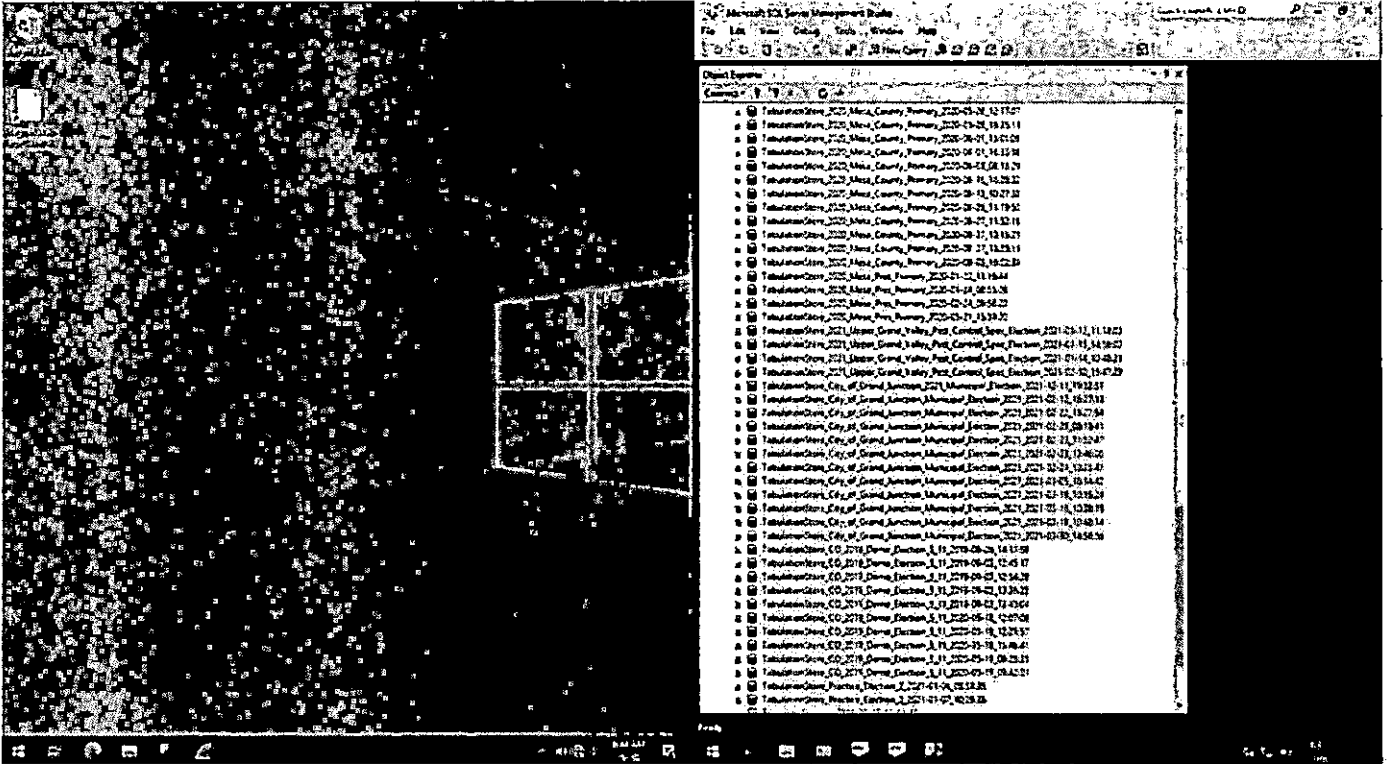


Figure 16 - Additional databases used in previous elections

Many TabulationStore databases are shown here, including even a TabulationStore for the Upper Grand Valley Pest Control Special Election.

Figure 16 is a continuation of the list in Figure 15, demonstrating that far more than one screen of databases are accessible.

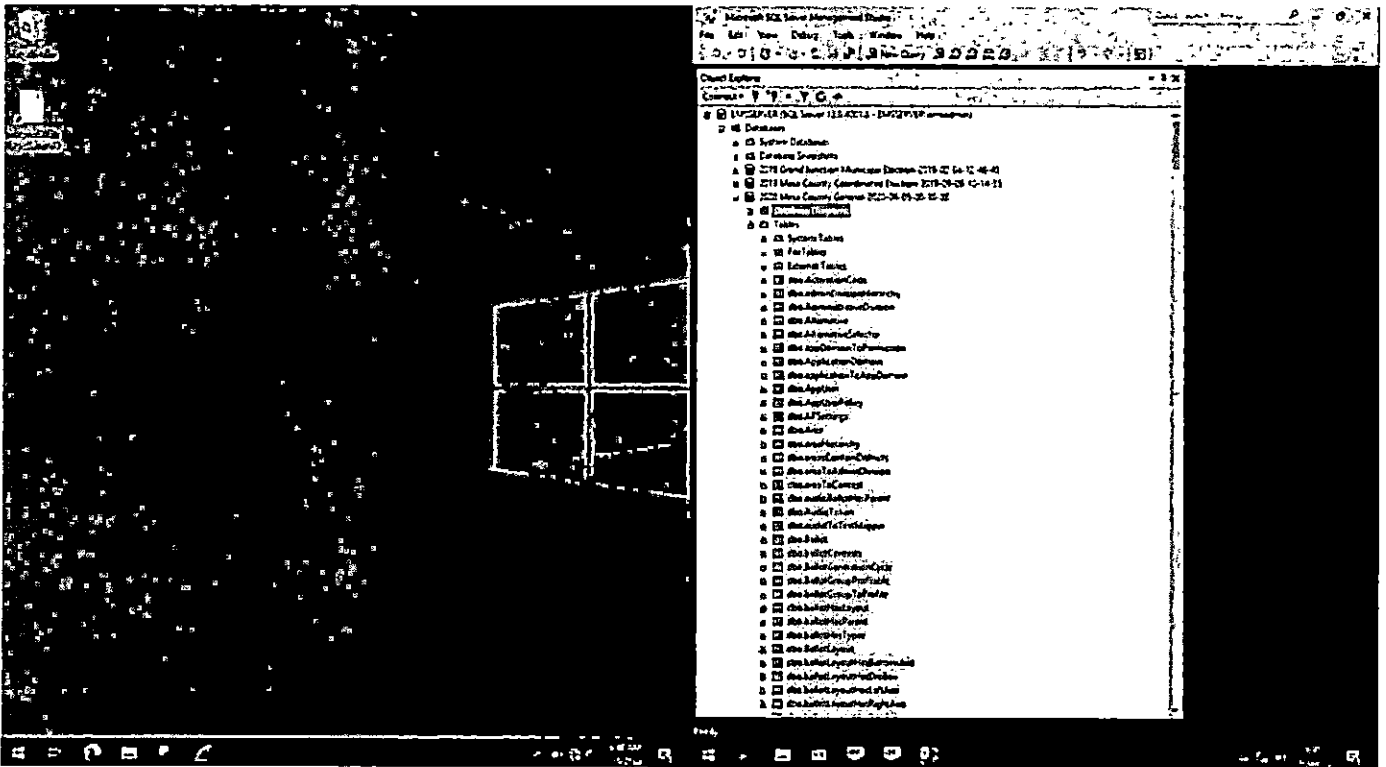


Figure 17 - Internal database tables, including ones with counted votes are accessible

The '+' sign next to the 2020 Mesa County General database was selected, followed by the '+' sign next to 'Tables.' A list of all internal database tables for the 2020 Mesa County General database is now shown. Nothing has stopped me from accessing this. Not a single warning has shown on screen.

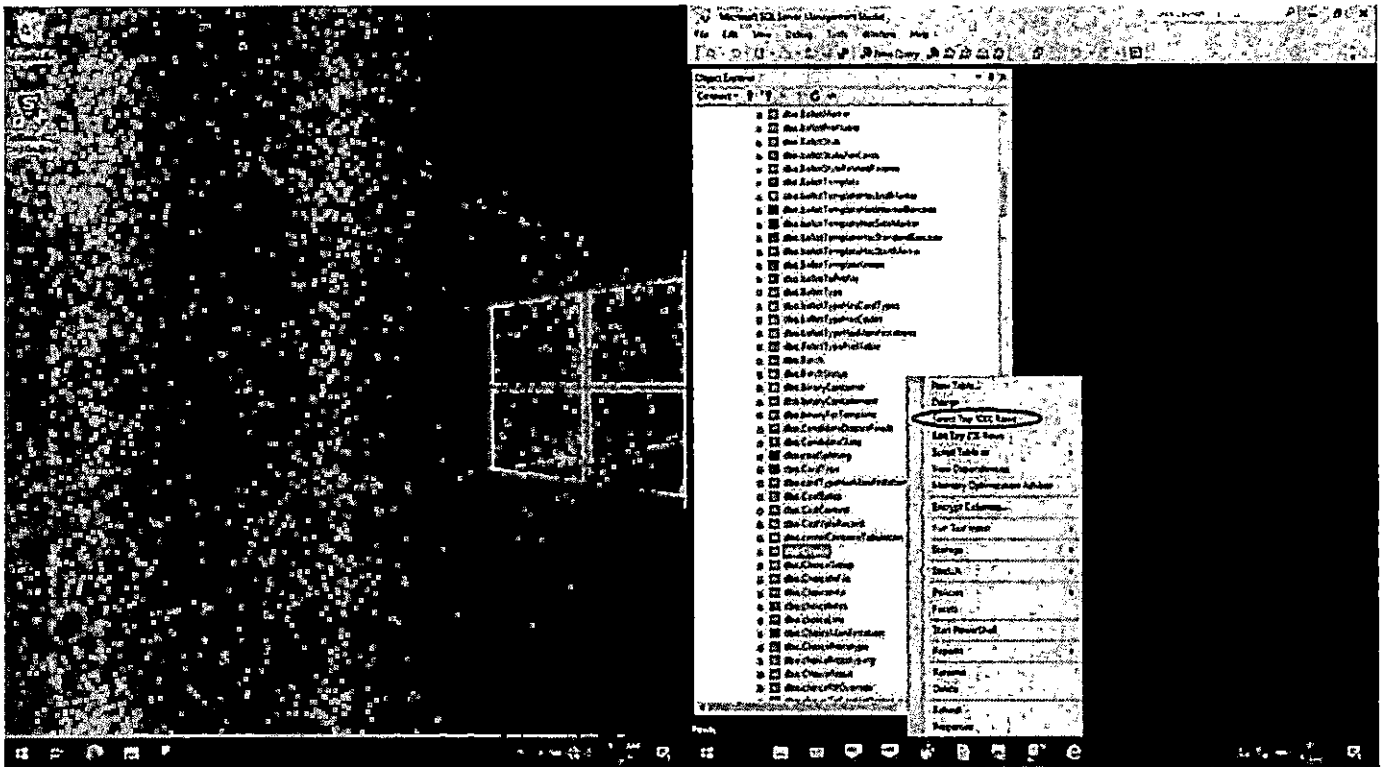


Figure 18 - Menu Option to Select the Top 1000 rows

As an example, one of the tables, 'dbo.Choice,' was selected by scrolling down and right-clicking, then choosing 'Select Top 1000 Rows' by clicking on that option. This instructs the database server to show me the top 1000 rows in the database table.

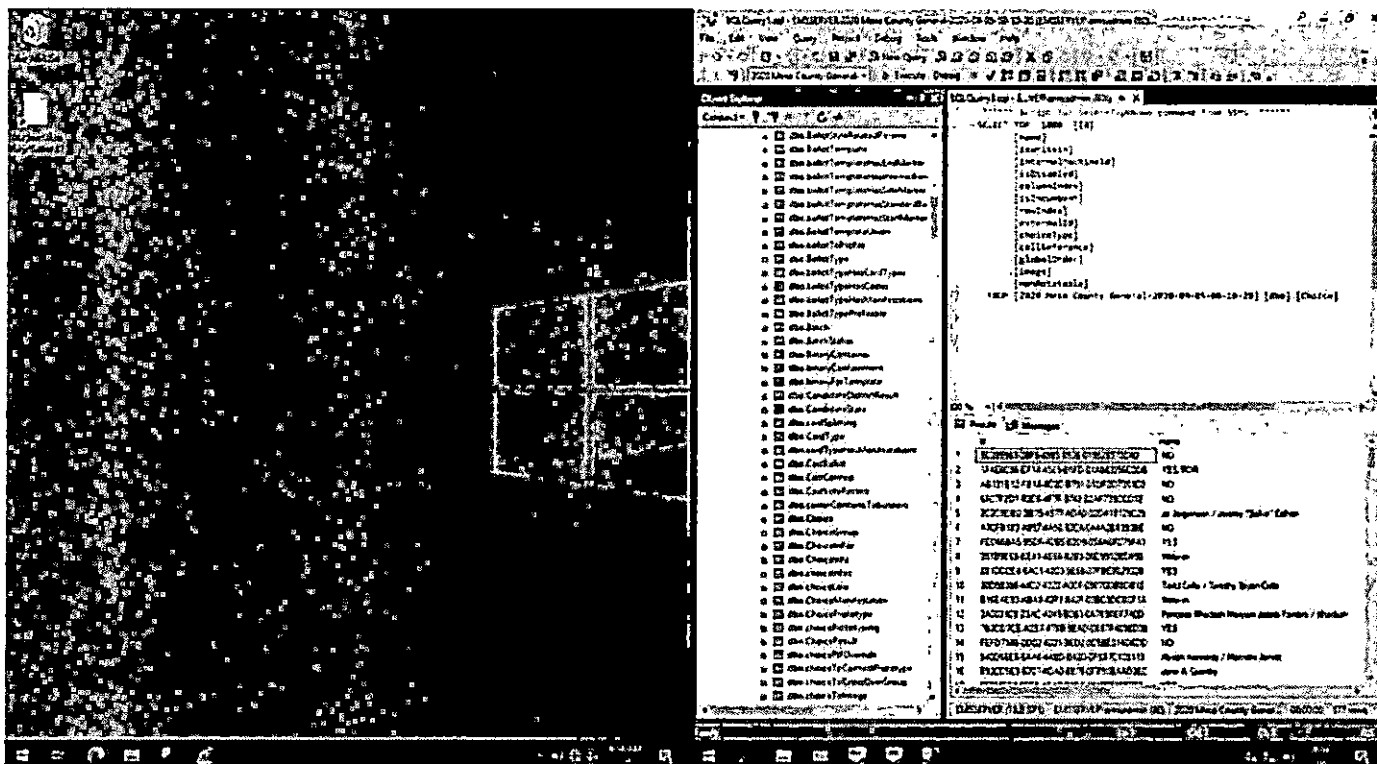


Figure 19 - Accessing the Ballot Choice database table

I was able to easily open the Ballot Choice database table. The computer retrieved all 177 rows of data from this table in the database. This corresponds to 177 different ballot choices in the election. I have still not been blocked, nor has the system provided any warning that anyone is directly accessing the voting database.

Each election “contest” is defined, together with candidates and the rules for voting, e.g., “pick one, pick two, pick three, etc.,” depending on the specific item, for example, commissioners of a town, and the number of seats open in this specific election.

On the right side of the screen in the upper right pane is displayed the SQL Query (SQL program script) that is automatically filled-out by SSMS. The user merely just needs to know how to click the mouse button. The automated query shown is used to retrieve data (the top 1000 rows), and the data columns listed that will be retrieved are also shown. On the bottom right pane the response from the request is shown. The first two columns display on screen (‘id’ and ‘name’) but the scroll bar allows one to scroll to the right to see the remaining 12 columns.

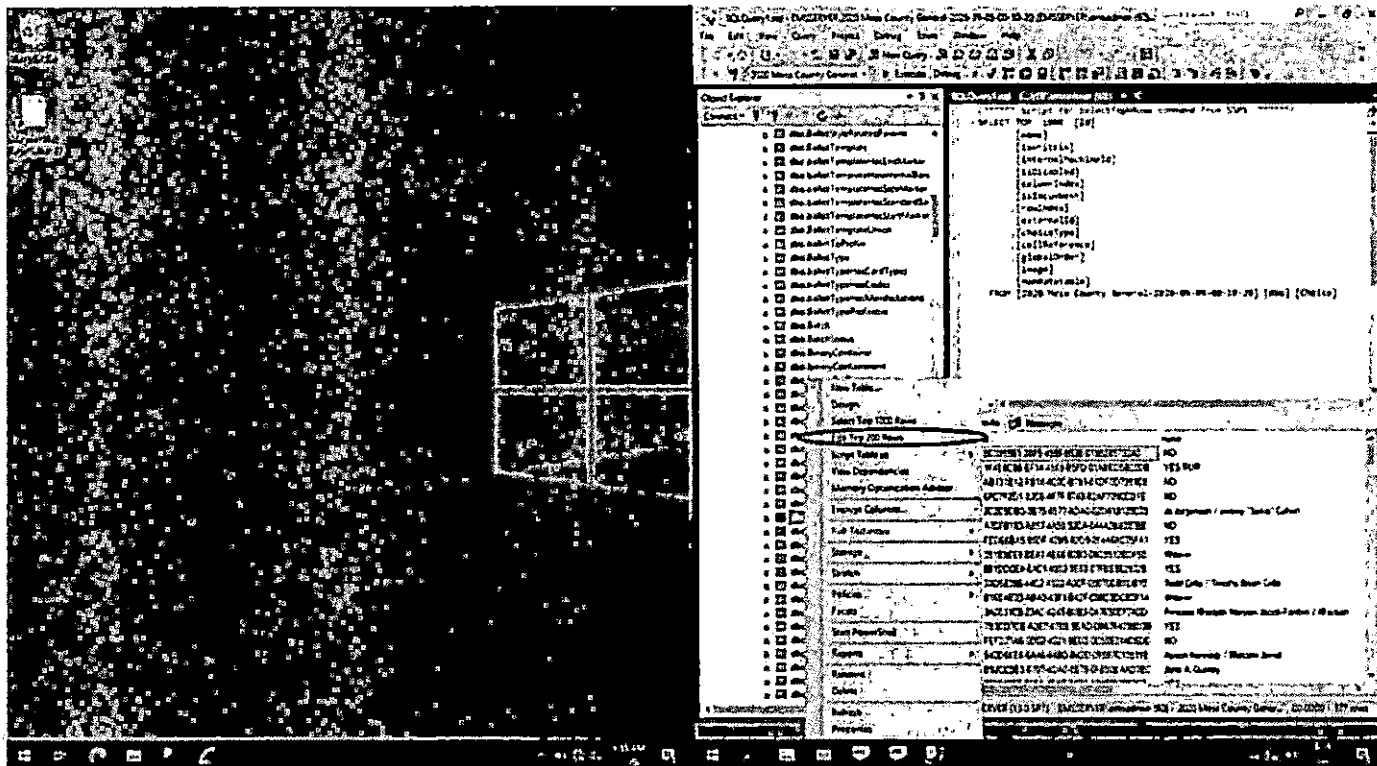


Figure 20 - Test to determine if the Ballot Choice Table can be edited to easily flip the votes

I now right-click the table again and select the menu option to Edit the Top 200 rows of the database to determine if it will also allow me to directly alter the data.

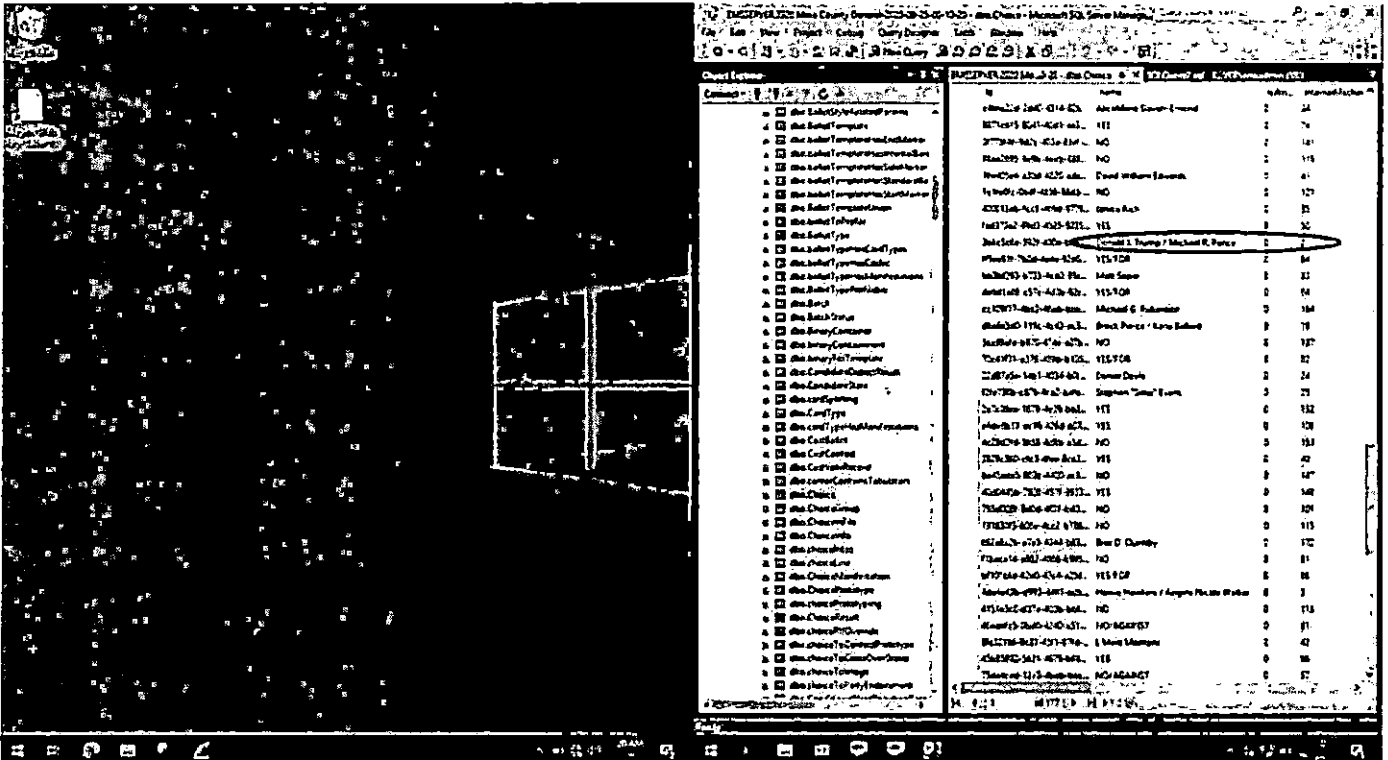


Figure 21 - Candidate settings for Trump

The computer responds to the request and shows all 177 rows of this Choice table in a spreadsheet-like display. Note here that the Choice 'Donald J. Trump / Michael R. Pence' has an internalMachinelid of '2'.

Note the first four columns are:

- Id – A unique identifier to identify the particular choice.
- Name – The 'title' of the choice on the ballot.
- isWritein – Possibly used to signify if a particular choice is a write-in field.
- internalMachinelid – Another unique identifier to identify a particular choice used to produce reports.

The internalMachinelid parameter is an indirect reference to the counted vote for candidates. Because the reference is indirect (i.e., a number rather than a key index that is common to the candidate's identity throughout the database), the reference can be easily changed, flipping the vote, and is extraordinarily difficult to identify. In database design, this is an example of bad design practice that breaks the "referential integrity" of the database and enables the potentially malicious action demonstrated here.

InternalMachined	Name	Value
28	Joseph R. Biden	YES
27	Joe Biden	NO
75	Joe Biden	NO
34	Joe Biden	YES
177	Joe Biden	NO
55	Joe Biden	NO
123	Joe Biden	YES
102	Joe Biden	YES
97	Joe Biden	NO
46	Joe Biden	NO
131	Joe Biden	NO
25	Joe Biden	NO
140	Joe Biden	YES
151	Joe Biden	NO
137	Joe Biden	NO
128	Joe Biden	NO
36	Joe Biden	YES
78	Joe Biden	YES
119	Joe Biden	YES
114	Joe Biden	NO
29	Joe Biden	NO
27	Joe Biden	NO
52	Joe Biden	YES
72	Joe Biden	YES
123	Joe Biden / Kamala D. Harris	1
79	Joe Biden	NO
138	Joe Biden	YES
25	Joe Biden	NO
125	Joe Biden	NO
79	Joe Biden	NO
123	Joe Biden	NO
40	Joe Biden	NO
123	Joe Biden	NO

Figure 22 - Candidate settings for Biden

The 'Joseph R. Biden / Kamala D. Harris' choice has an internalMachined of '1.'

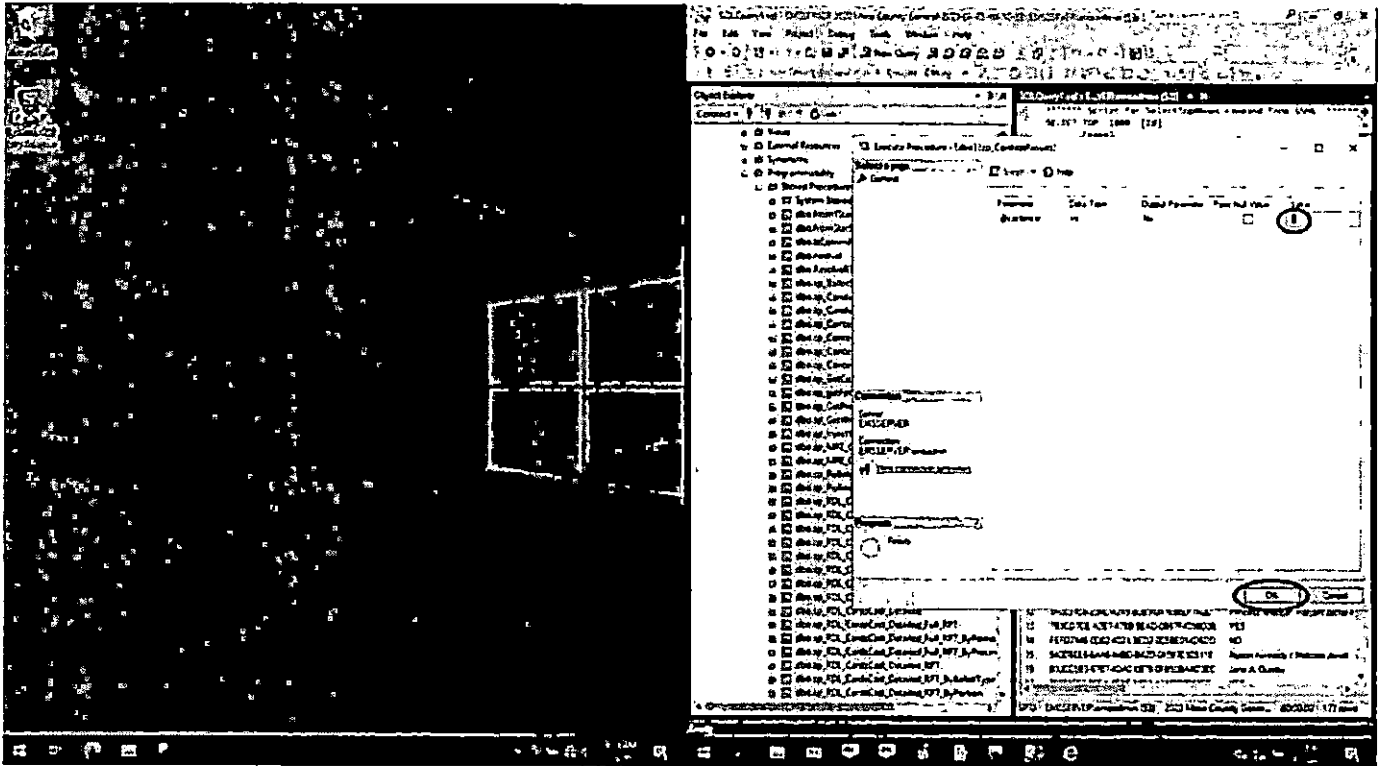


Figure 24 - Run Stored Procedure to pull up a report of Presidential Electors

The computer then prompts for which ContestId to query. A '1' to signify the Presidential Electors is entered, then 'OK' is clicked.

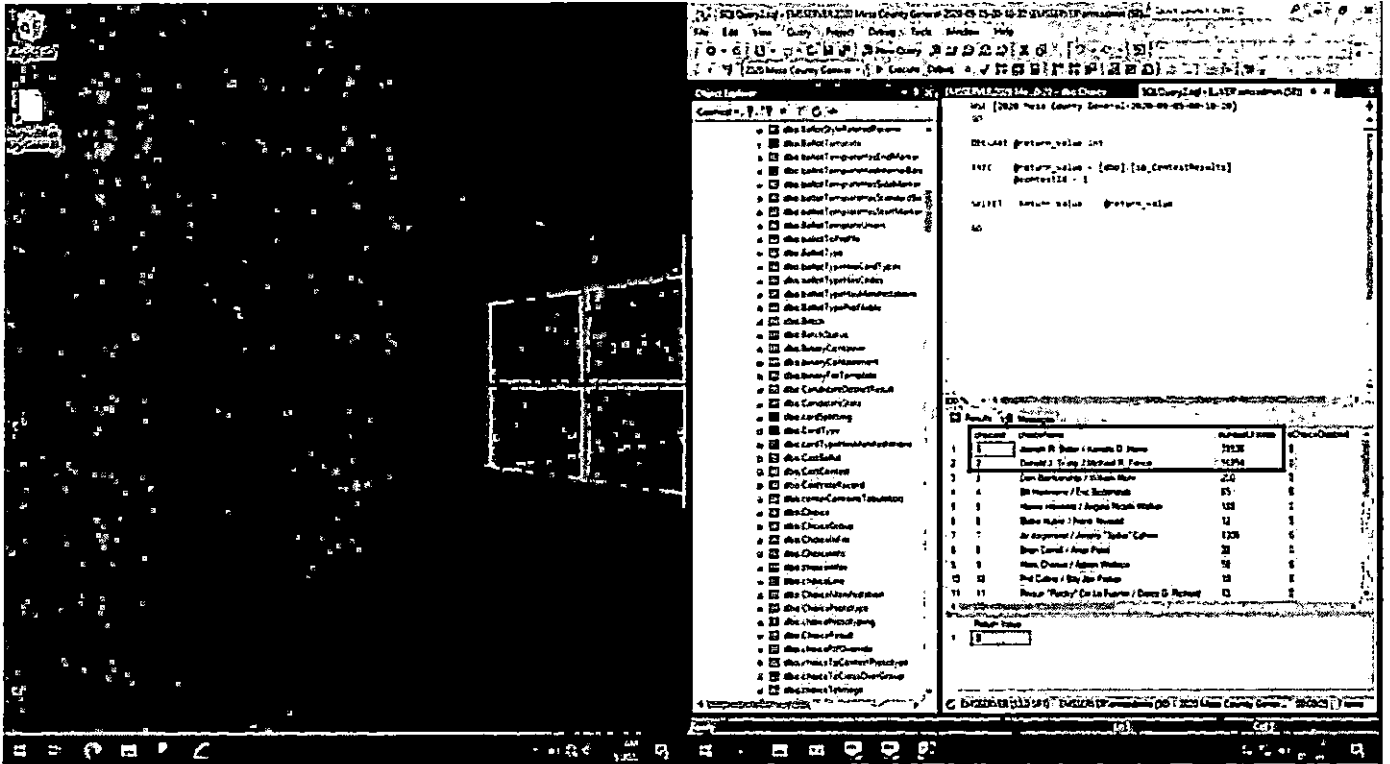


Figure 25 - Retrieved Vote Totals

This report shows the total number of votes for the Presidential contest:

'Joseph R. Biden / Kamala D. Harris' as having 31,536 votes, and

'Donald J. Trump / Michael R. Pence' as having 56,894 votes.

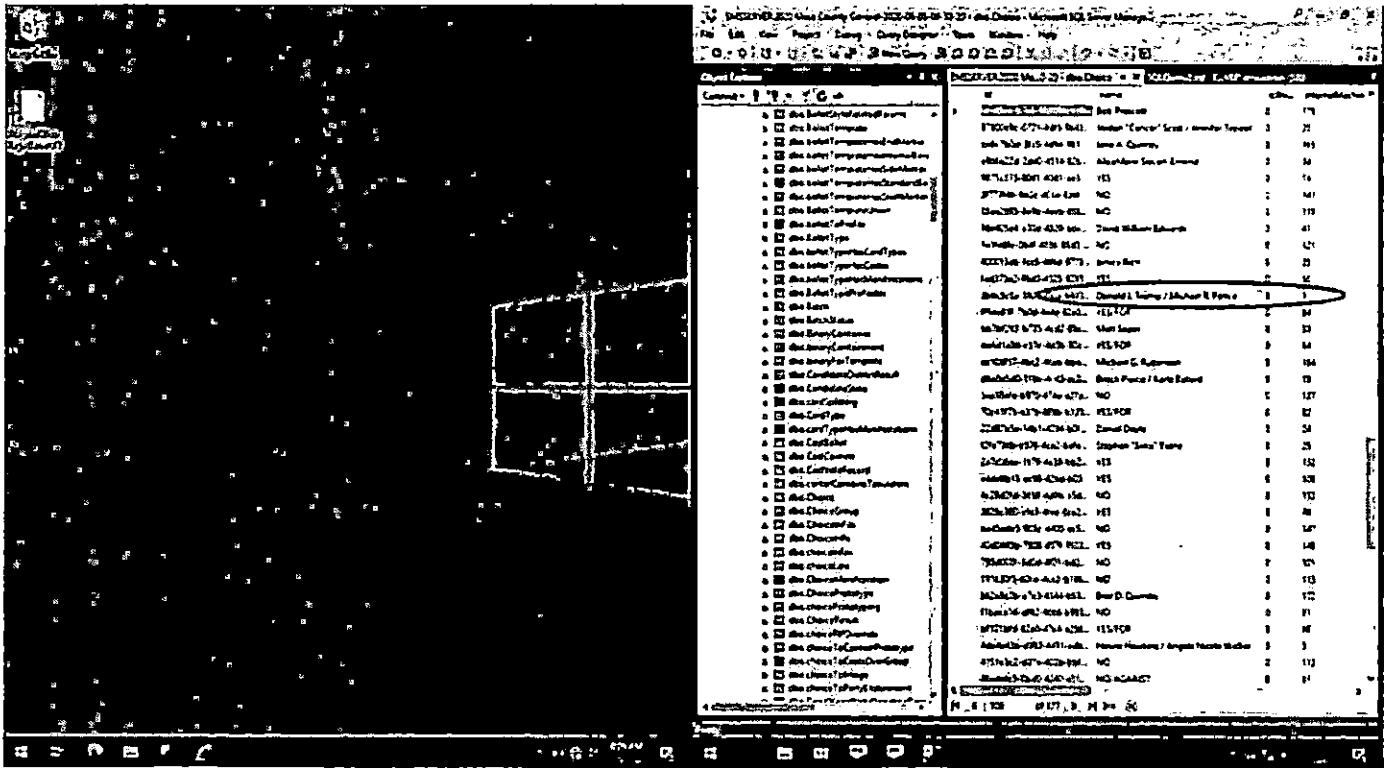


Figure 26 - Candidate number for Trump modified

Here, I change the Trump 'internalMachinelD' from a '2' to a '1.' The SQL Server Management Studio allows the change without any hesitation or warning that a crucial piece of data was changed. The lack of good design and very poor referential integrity allows this.

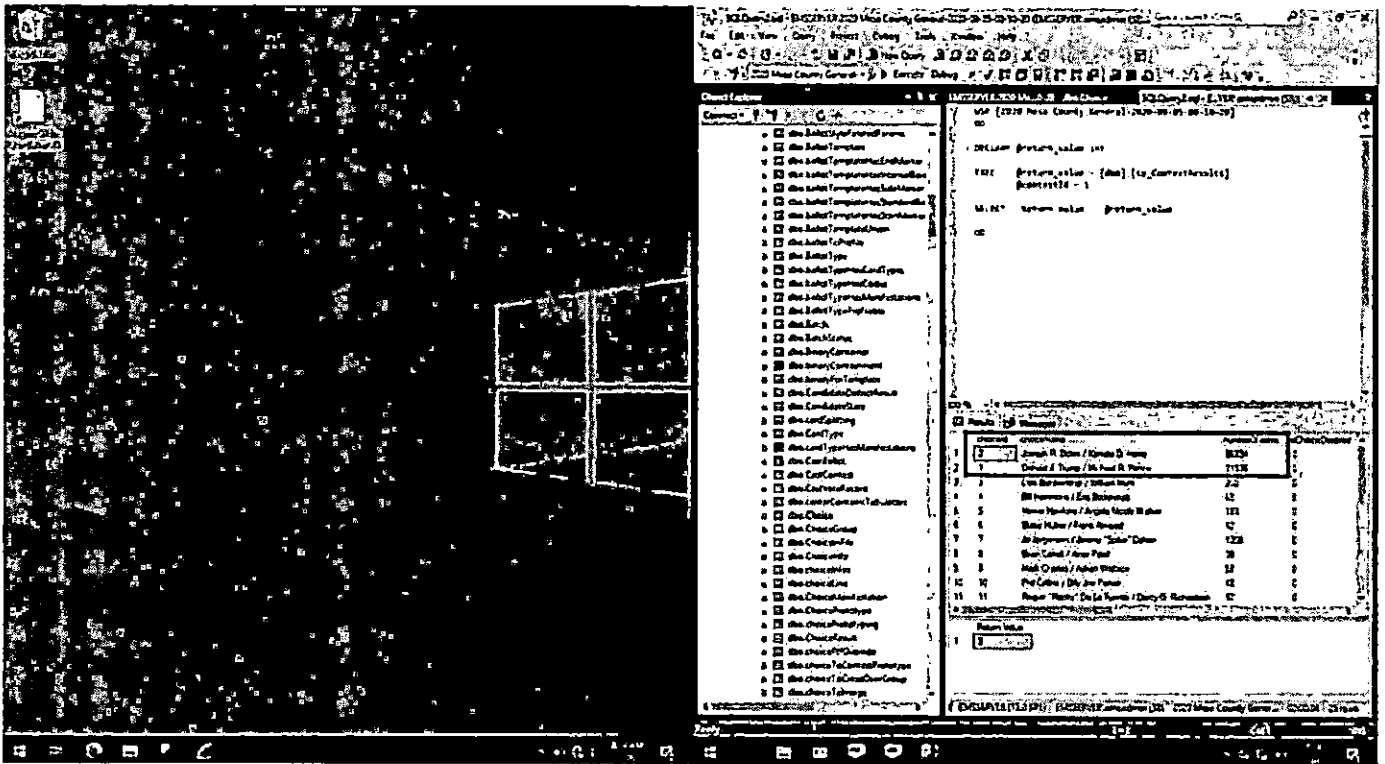


Figure 28 - Vote totals retrieved again after modification.

Making only these two small changes, which can be done in under a minute by an individual sitting in front of the voting system server, resulted in a flip of 25,358 votes. This demonstrates the ease with which someone can completely alter the results of the election on this EMS server with only a few mouse clicks and 2 keypresses on the keyboard with the software that is built-in to this voting system. This is only one in countless ways election data could be altered.

When the stored procedure is executed to retrieve the vote totals again, the vote totals for Biden now show 56,894 and the total for Trump shows 31,536.

By changing only two values in the election database in less than a minute, I have flipped 25,358 votes, completely changing the vote total results in the election database. The change was made using Microsoft SSMS software already residing on the EMS server, without needing to enter any additional password, and without a warning about the risk of changing this information.

Finding 2: The existence and use of unauthorized and uncertified Microsoft SQL Server Management Studio (found on the EMS server in Mesa Co. and in other counties around the country), allows and facilitates the bypass of Dominion Voting Systems' software to alter calculated vote totals in the election database by anyone with physical access to the logged-in EMS server.

It is important to understand how easily this was done, and therefore how quickly such a change can be made. It was not necessary to change the 88,430 votes in the database, but rather only two index values, the internalMachineld values, to completely flip the result of this county's votes.

Finding 3: It is a simple task to flip votes and therefore very easy to do quickly.

Finding 4: The insecurity of the Mesa County EMS server, in concert with unauthorized, uncertified software, allowed the alteration of the election result, flipping the vote from one candidate to another, with trivial difficulty.

Let us also distinguish the claim being made here:

It is not asserted in these findings that this 'Vote Flipping' was performed on this server during the 2020 election, but rather the design and configuration of the system permits it, and due to the extraordinary lack of security and the unauthorized, uncertified software installed on the system, the voting system itself was, and is, completely uncertifiable and wholly unsafe to use for any election.

To be explicitly clear, this demonstration is about the lack of security and the access that insecurity and unauthorized software allows, and it is explicitly not about the vote totals in any election from this server. The lack of efficient logging and the destruction of the required log files prevent any assertion to the contrary in this analysis.

Whether votes were 'flipped' using this process, or the countless other ways that could be used, requires examination of computer system logs and database logs, and other data, and will be separately addressed. In this finding, it is demonstrated that it is possible, and that the defects in the security and certification of the system are extraordinary and far beyond simple errors and omissions.

Examination Result #1

Vote totals can be altered by anyone with physical access to the logged-in EMS server.

EXAMINATION OBJECTIVE 2:

Determine whether the calculated vote totals can be altered by any person using a non-Dominion computer directly or indirectly connected to the EMS server network.

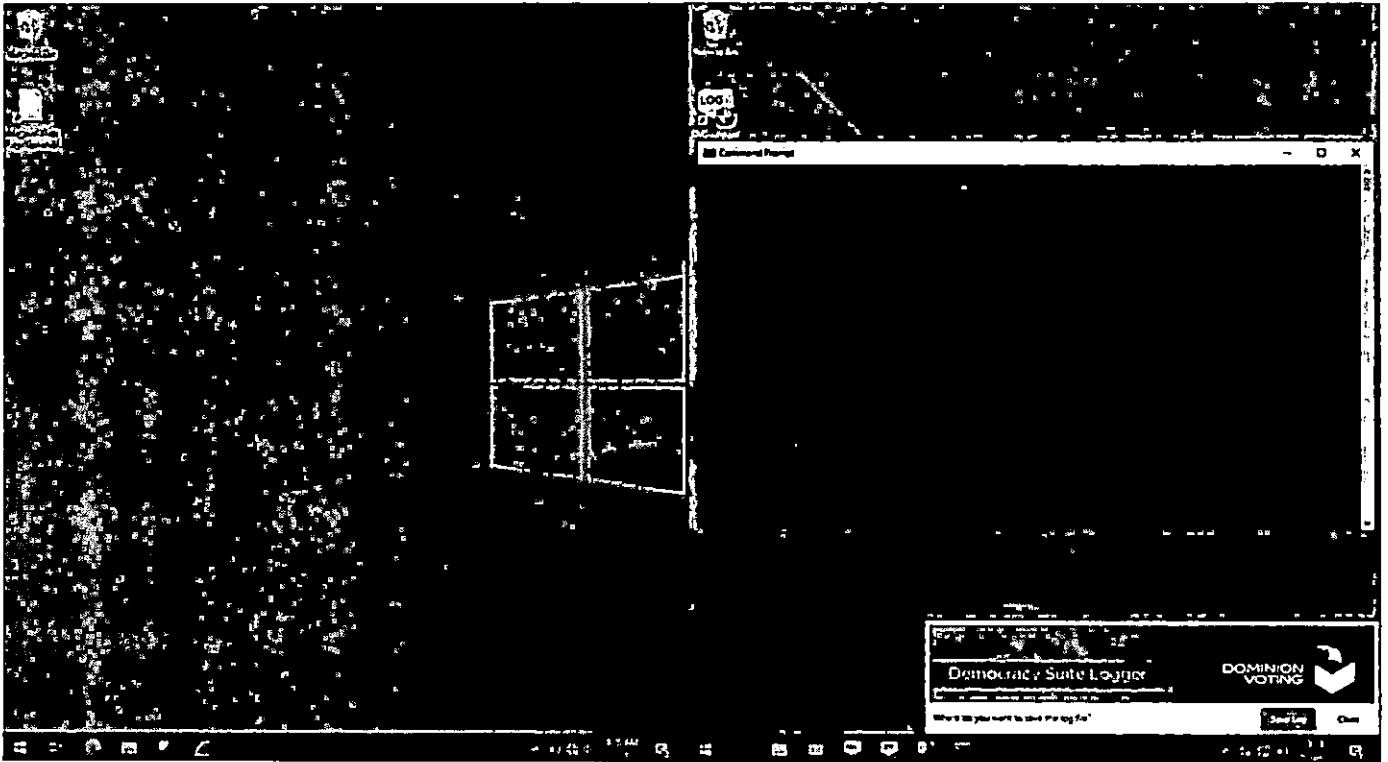


Figure 29 - Accessing port 1433 with Telnet

The telnet command is used to test to see if direct network connection to the database port is possible.

'Telnet' is a common network diagnostic tool used by IT and Cybersecurity professionals for communicating with a telnet server, and other text-based TCP services.

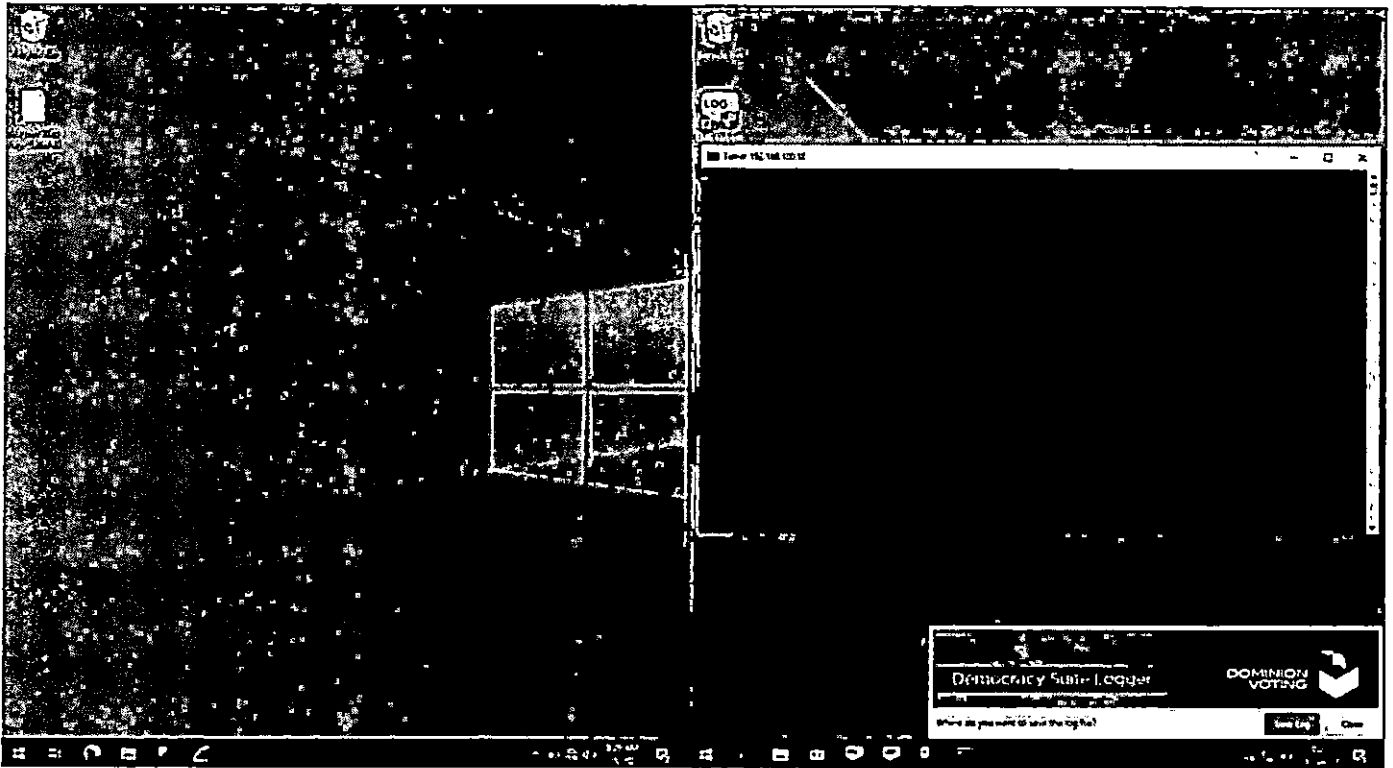


Figure 30 - The EMS server network interface appears to answer a connection to port 1433

The blank window with the cursor in the top left indicates that the connection was indeed successful, and the database service is now waiting for input.

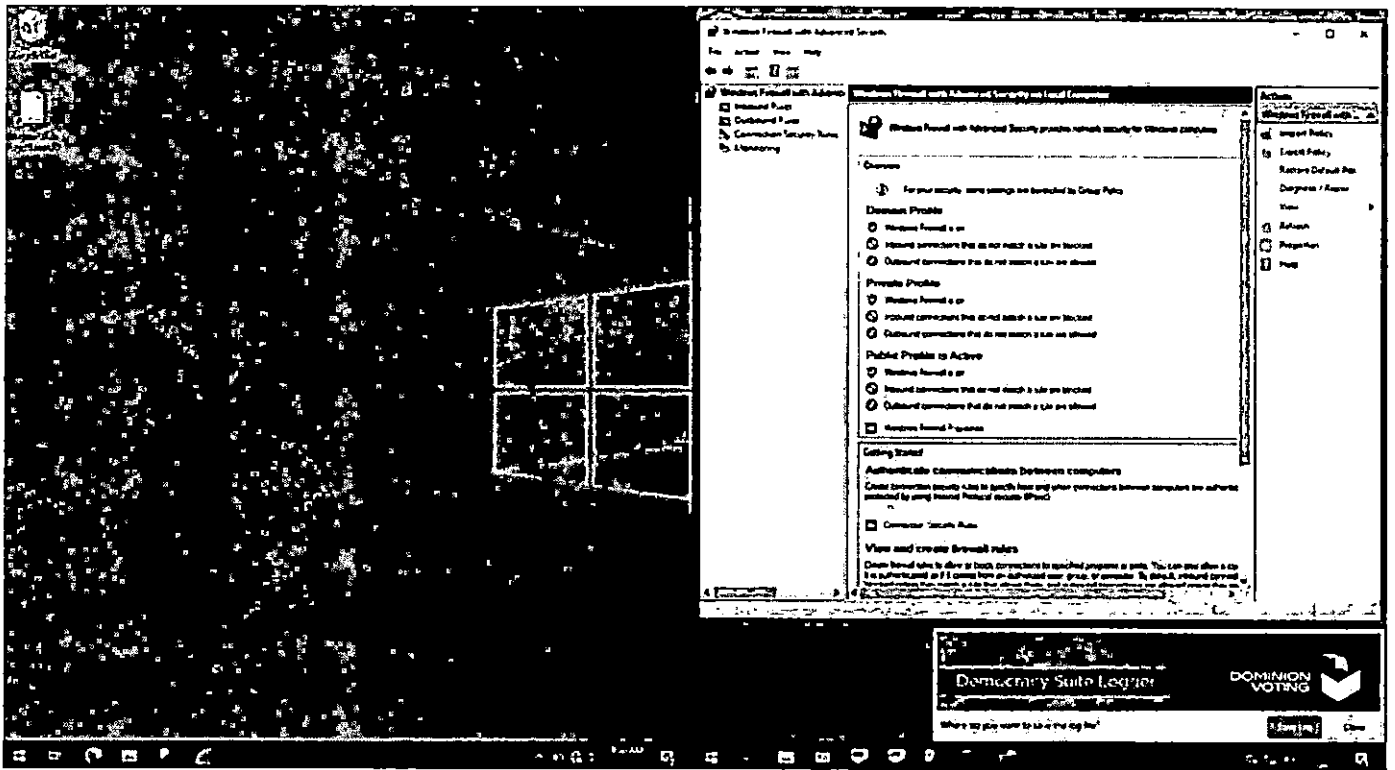


Figure 31 - EMS server has the 'Windows Firewall' enabled

Because it was trivial to connect directly to the database server on port 1433, the firewall was then checked to see if it was enabled on the server. This figure shows that the Windows Firewall with Advanced Security is installed and enabled, however the configuration of the firewall must now be examined to see why it allowed this activity.

The Mesa County EMS server contained firewall software, but it is the specific configuration of the firewall that is unsafe. In this screenshot, the firewall is shown to be enabled. For each profile ("Domain," "Private," and "Public"), the settings are the same:

- Windows Firewall is on. <- GOOD
- Inbound connections that do not match a rule are blocked <- GOOD, but requires further inspection.
- Outbound connections that do not match a rule are all allowed. <- RECKLESS FOR A 'SECURE' SYSTEM

Before going further, it is important to understand what a Firewall is and how it operates. A Firewall is a device that evaluates computer traffic on a network, and based on rules, allows or denies each specific connection. The rules in most common firewalls contain:

- the source IP address,
- source port number,
- Internet Protocol number,
- destination IP address,
- destination port number,

CONFIDENTIAL

- (Some firewall rules may contain dates and times, for example Monday to Friday 8 am to 5 pm),
- the action to Allow the connection,
- Block the connection,
- Drop the connection, and
- whether to log the connection.

Typically, the rule base is evaluated from top to bottom in order, and the first rule that matches the connection is applied (and the rest of the rule base is skipped). For ANY connection that did not match previously – it is blocked by the Firewall.

It is notable that outbound connections that do not match a rule are set as “Allowed” in this EMS server. For a critical infrastructure voting system, such a configuration is completely reckless. Per VSS⁷⁰ and industry best practices systems that require connection should be explicitly specified, and no other outbound connections should be allowed. One of the reasons for such a requirement is that many internet addresses contain malicious software that can be downloaded and installed, sometimes automatically, depending on how they are accessed. The existence of such malicious software has given rise to an entire Anti-Virus and Anti-Malware industry.

⁷⁰ VSS Volume 1, sections 6.4 and 6.4.2

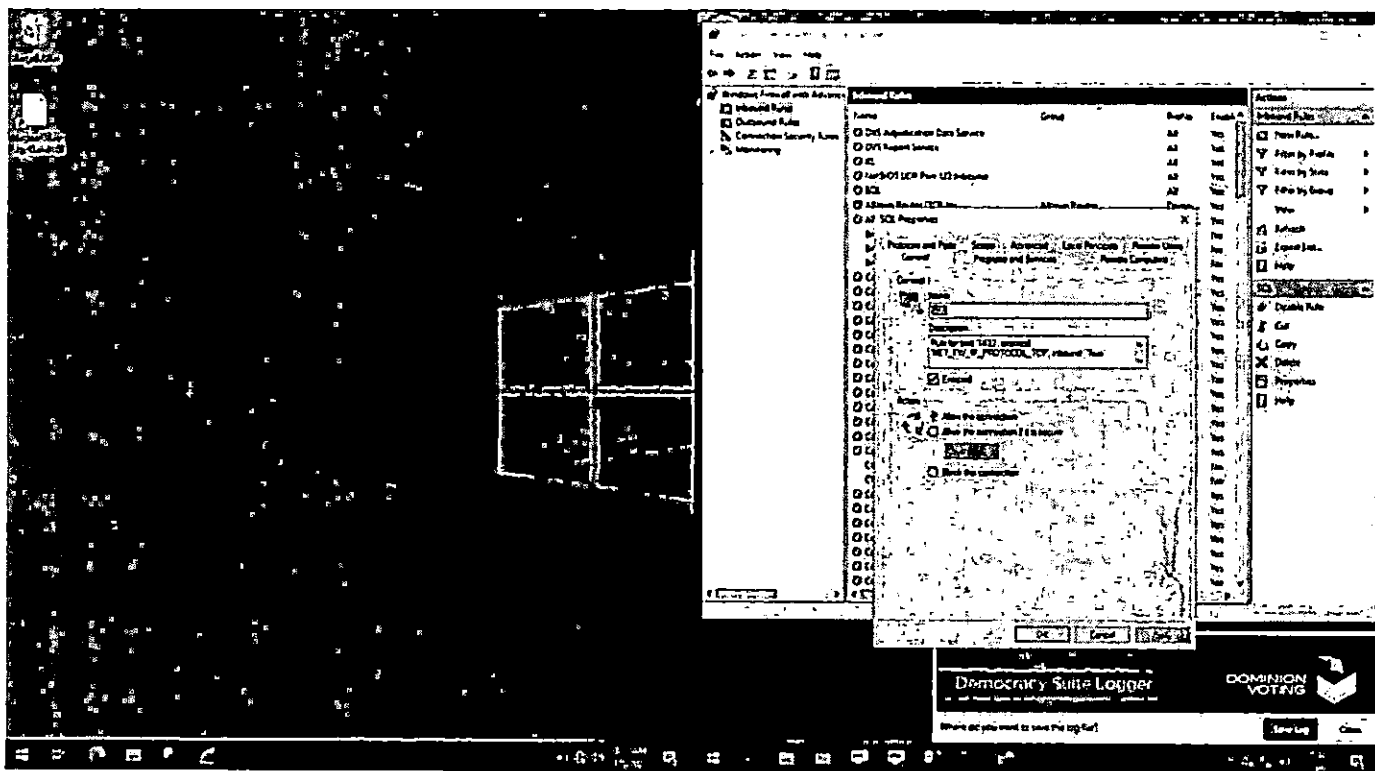


Figure 32 - Windows Firewall Custom SQL entry is enabled

Within the Windows Firewall, a custom firewall rule was found for the SQL service. This rule is not created by Microsoft; it must have been created by another means. The content of the 'SQL' rule is examined and shows the rule is "Enabled," and set to "Allow the connections". Note, the option titled 'Allow the connection if it is secure' just below the chosen option is available however not selected. This means again, the vendor had the option and opportunity to make the system configuration more secure, and neglected to or chose not to, and the individuals involved in the certification either did not check or ignored the vulnerability.

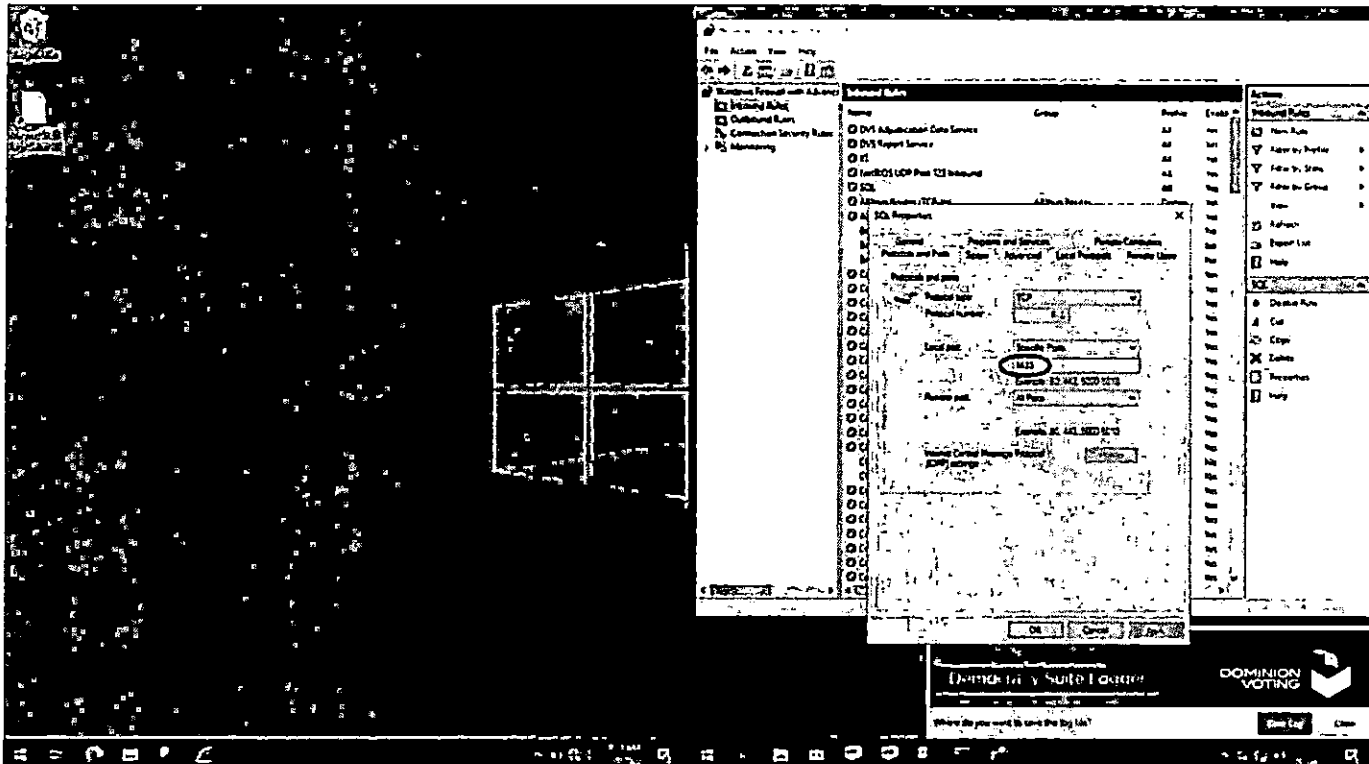


Figure 33 - SQL port 1433 is allowed.

The commonly-known default SQL Service, TCP port 1433 is specifically allowed by this firewall rule.

The port number selected for SQL database access could have been changed so that probing of the computer implicitly revealed less information. This is a recommended technique for high security networks where it is intended that the discovery of systems be disallowed; there are many other recommendations to be followed to truly harden the security of an operating system and its applications.

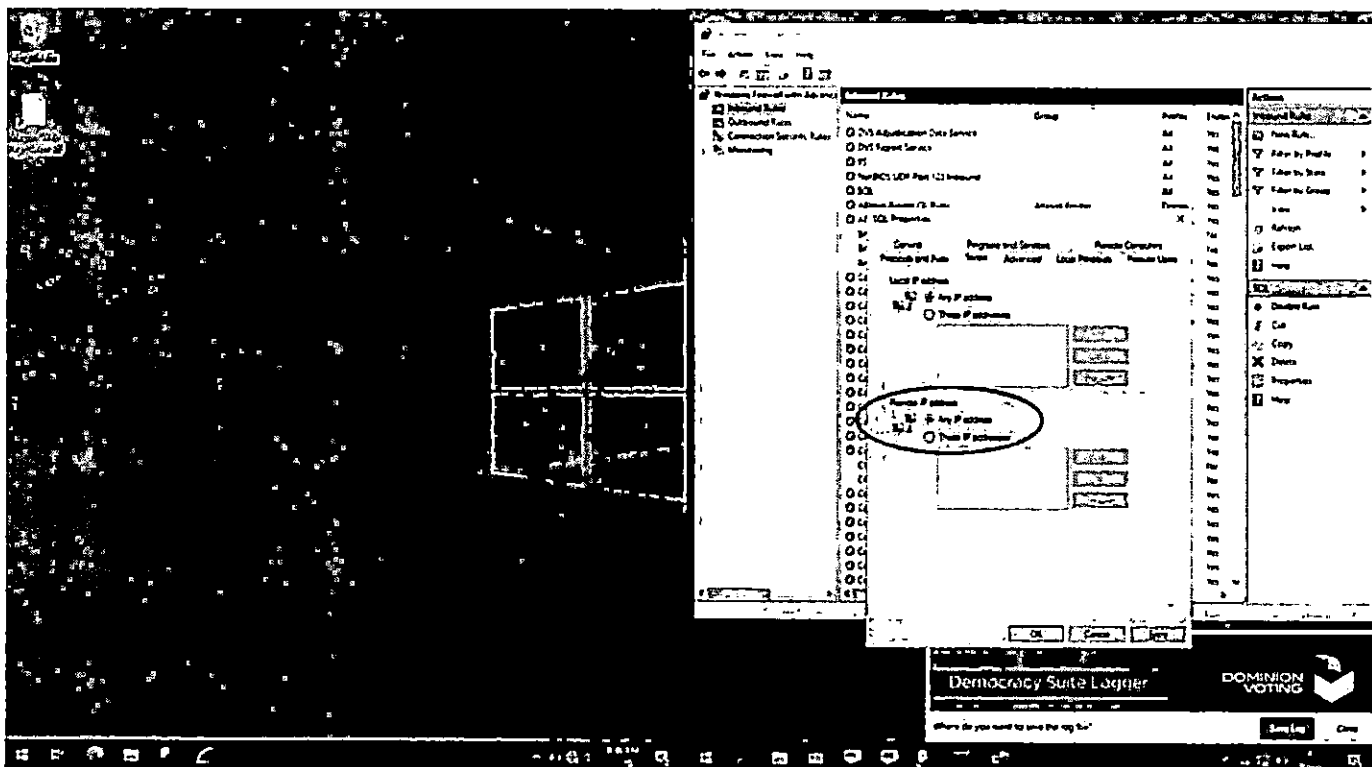


Figure 34 - Access to the SQL database standard port is allowed from ANY IP ADDRESS worldwide.

The IP address of the requesting computer is shown here as 'Remote IP address.' This rule is programmed to allow 'Any IP address' to connect to this port. Any IP address applies to any IP address anywhere in the world.

The ability to make the server more secure has been included by Microsoft and made easy to implement in the graphical user interface (GUI), specifically by allowing for the specification of Remote IP addresses to be accepted (which would exclude all those not explicitly listed). Microsoft documentation states:

"Any computer (including computers on the Internet): Not recommended. Any computer that can address your computer to connect to the specified program or port. This setting might be necessary to allow information to be presented to anonymous users on the internet, but increases your exposure to malicious users. Enabling this setting can allow Network Address Translation (NAT) traversal."

The option to specify a list of IP addresses is present in the GUI, "These IP addresses:" but is not selected.

Again, DVS had the option and opportunity to make the system configuration more secure, and neglected to or chose not to, and the individuals involved in the testing and certification either did not check or ignored the vulnerability.

Instead, they configured the option that Microsoft states is "Not recommended" and "increases your exposure to malicious users."

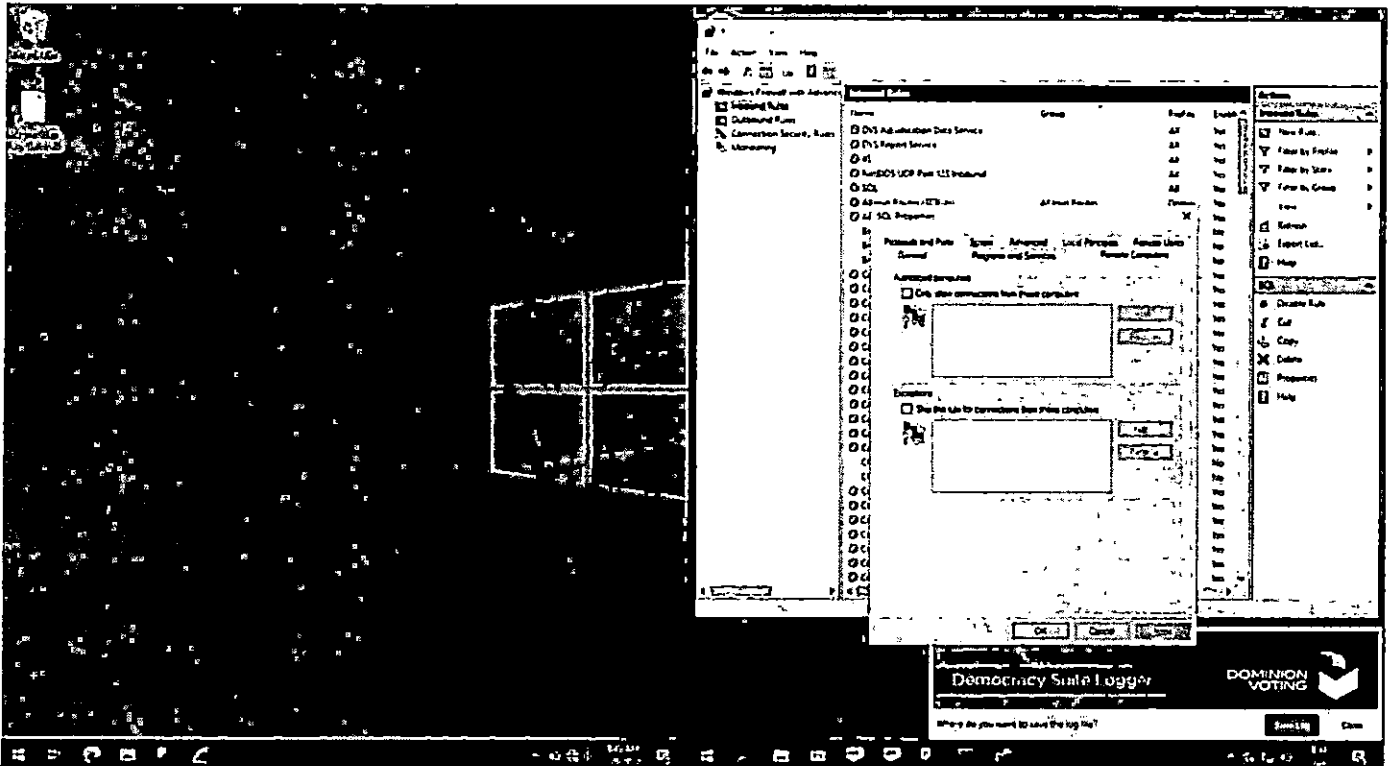


Figure 35 - No additional IP address restrictions or permissions

No restrictions are in place on the firewall that require authentication or integrity-protected communication on the network. The vendor could have specified as “Authorized computers” only those computers and devices deployed within the DVS D-Suite 5.11-CO voting system configuration in Mesa County, and excluded any and all other computers and devices in the world. But the vendor does not restrict that communication and, again, neither the voting system testing lab nor the Secretary of State staff took note or action regarding that neglect of a required security setting. For such a ‘secure’ critical system (“critical infrastructure,” according to the U.S. Government), there is no excuse for this lack of security to help guarantee integrity of each citizen’s vote.

It is possible to restrict access to a designated set of computers and even ensure that the connections are authenticated and integrity-protected. The functionality for this is built-in to the operating system, had the voting system vendor chosen to configure it. This safeguard of network traffic authentication and integrity-protection is available, but unused by DVS in this image of the Mesa County EMS server configuration.

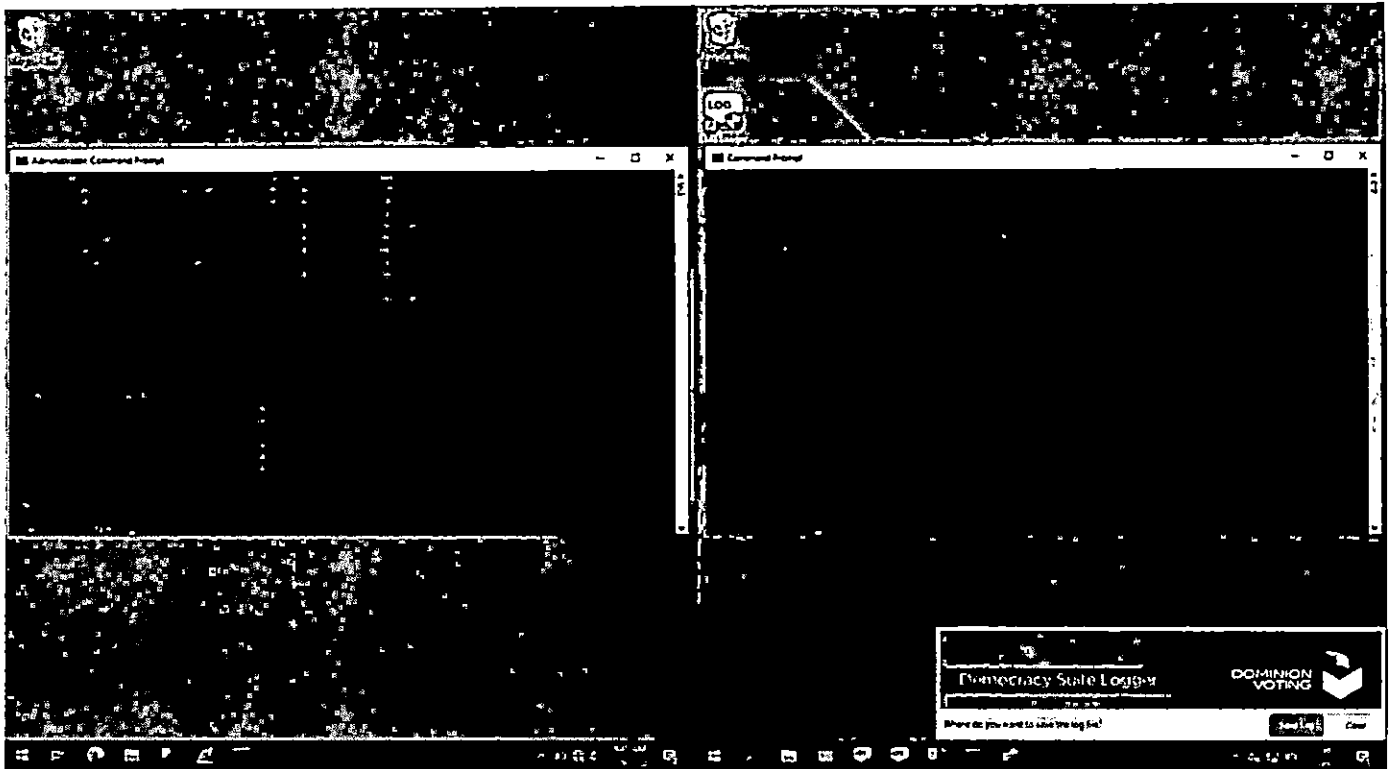


Figure 36 - Test Workstation, 192.168.100.150, and EMS, 192.168.100.10, are on the same subnet

This is demonstrating that the IP address for the Test Workstation on the left is on the same subnet as the IP address for the EMS Server on the right.

This address configuration shows that the test workstation and the EMS server are configured on the same subnetwork, i.e., "subnet," e.g., they should be able to connect to each other if there is not something restricting them from doing so. If they were not on the same subnetwork, a router would be required but is unnecessary in this examination for the finding demonstrated here.

Testing the connection from an external Test Workstation tests the totality of the EMS server configuration and assures that claims of being able to connect from a separate computer not part of the DVS system are valid. Specifically, this test assures that no additional countermeasures or configuration of the EMS server are overlooked in arriving at this conclusion.

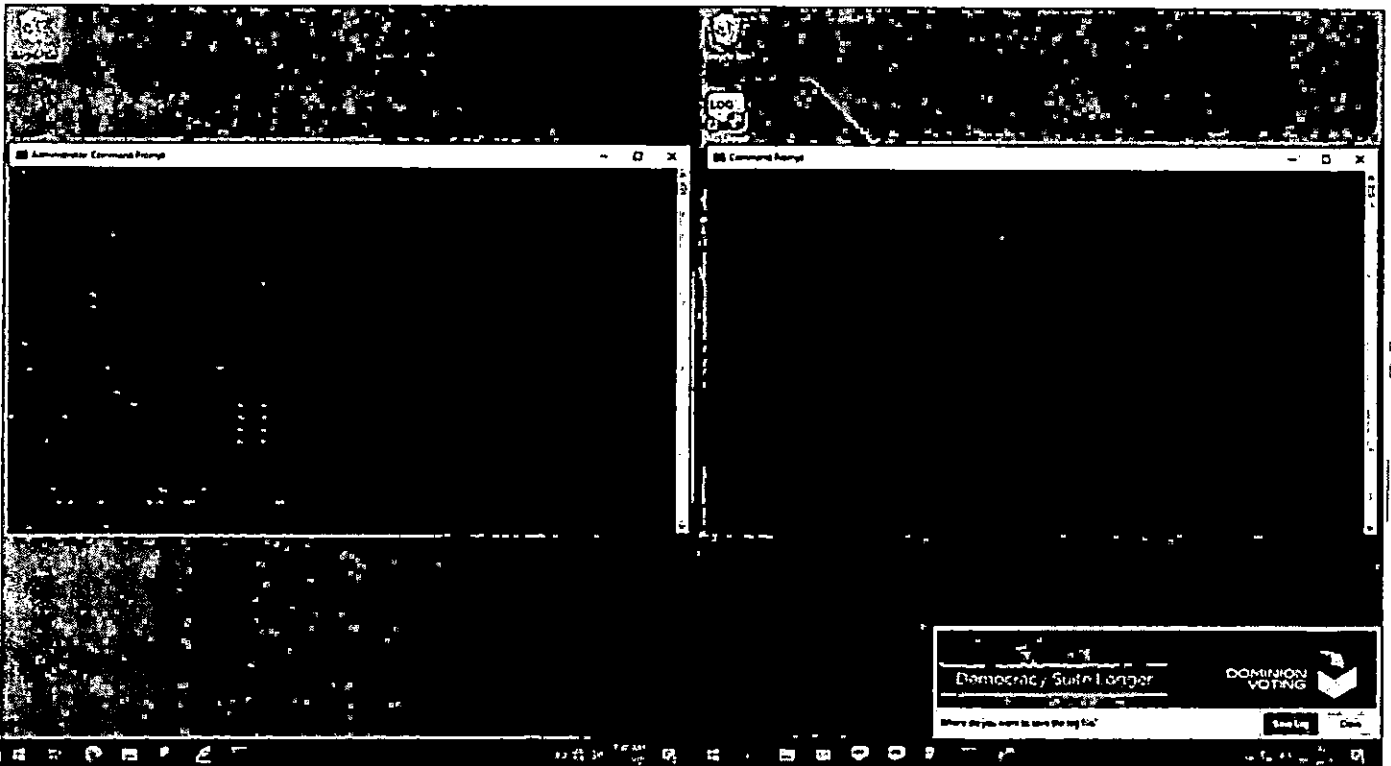


Figure 37 - Mesa EMS server is responding to network ping test.

'Ping' is another common diagnostic utility being used to determine if the EMS server on the right responds to the request from the Test Workstation on the left. All 4 responses were received by the Test Workstation from the EMS server, in response to the 4 requests sent by the Test Workstation.

In a properly highly secured network, one would expect the Internet Control Message Protocol (ICMP) request to be disallowed on the EMS server, in order to help prevent the unauthorized or malicious discovery of the DVS D-Suite network structure of devices and addresses.

This test demonstrates the lack of such restriction: the EMS server responded to the request.

The ping test uses Internet Control Message Protocol (ICMP) and transmits an "echo request" to the echo service on a remote computer. The remote computer responds and the original computer records the time it took to return the request. This is commonly used to determine if a device with a particular IP address is present on a network. This test demonstrates that the Test Workstation is connected to the EMS server across the network.

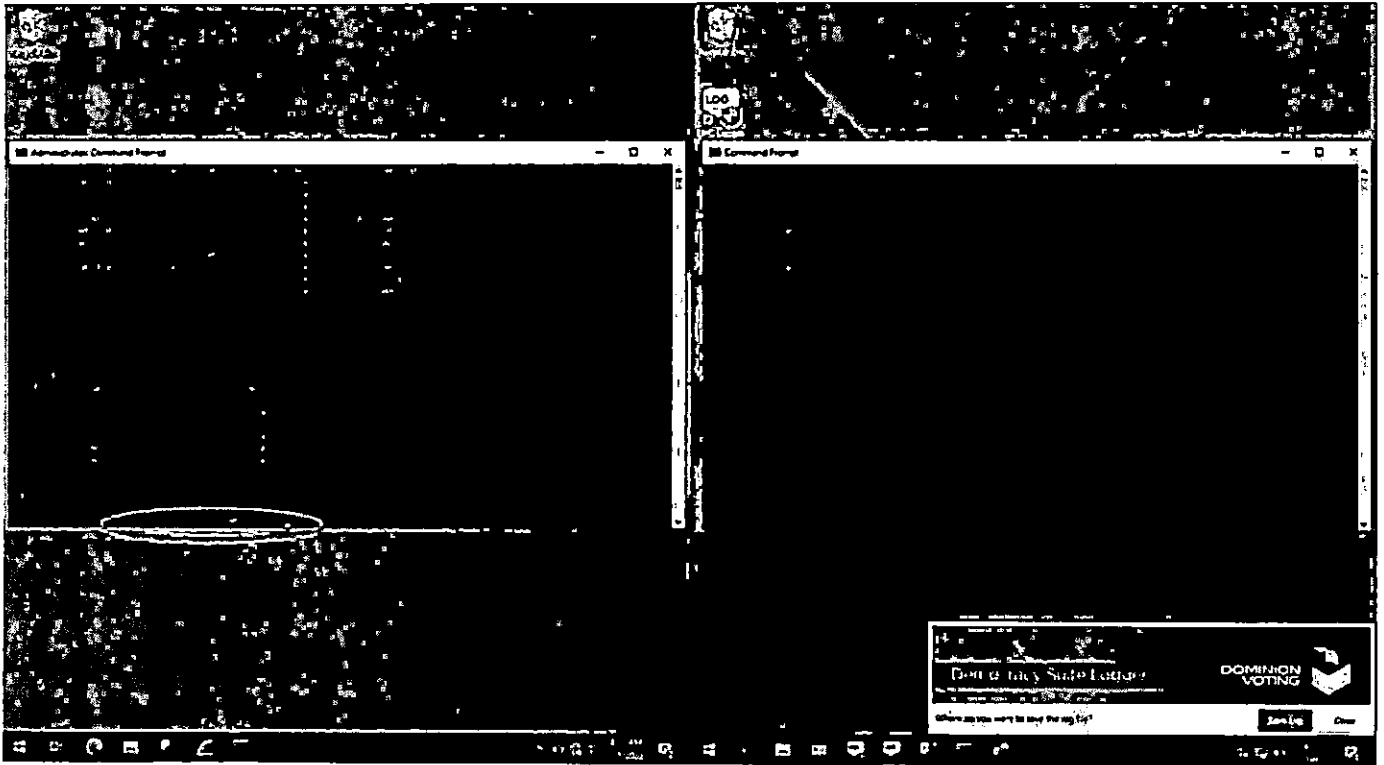


Figure 38 - Telnet connectivity test from separate computer not part of the Dominion system

The same 'Telnet' command (as in Figure 28) is used to see if the commonly-known default configured SQL Server port of 1433 on the EMS server at 192.168.100.10 can be connected to this alternate non-DVS D-Suite system.

Having established that the test workstation can connect to the server IP address, the Telnet command is used to test the connection to the EMS server's SQL service. Previously this connection was attempted from the EMS server to itself. The connection from the Test Workstation, a separate computer not part of the DVS D-Suite system, is attempted here.

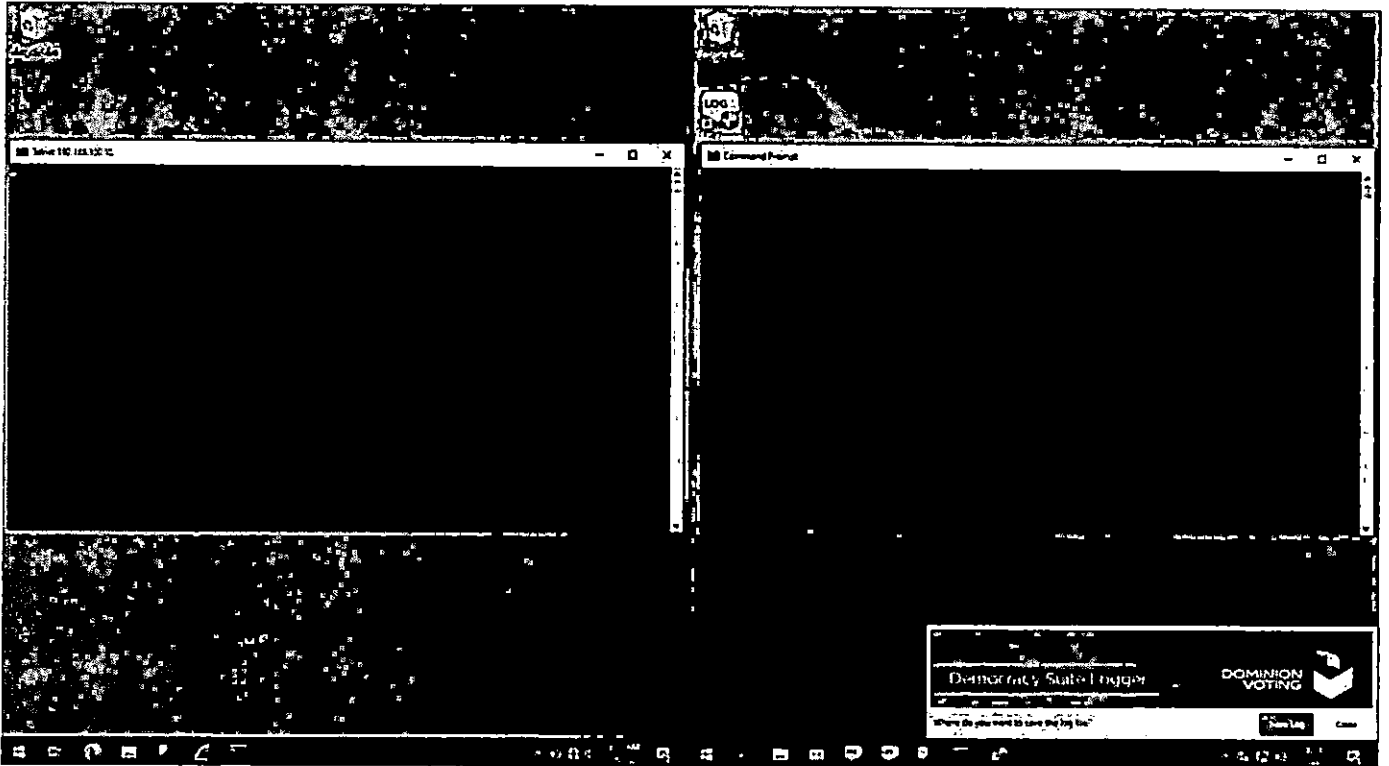


Figure 39 - Telnet to EMS server port 1433 (SQL) succeeds

Just as when this same test was run on the EMS server itself, the connection to the SQL Server port 1433 on the EMS server is successful from the Test Workstation.

The Telnet utility from the Test Workstation is able to connect to the EMS server showing, as in the Telnet test from the server to itself, that the SQL database service port is operating and listening for connections, and accessible from a non-DVS D-Suite computer.

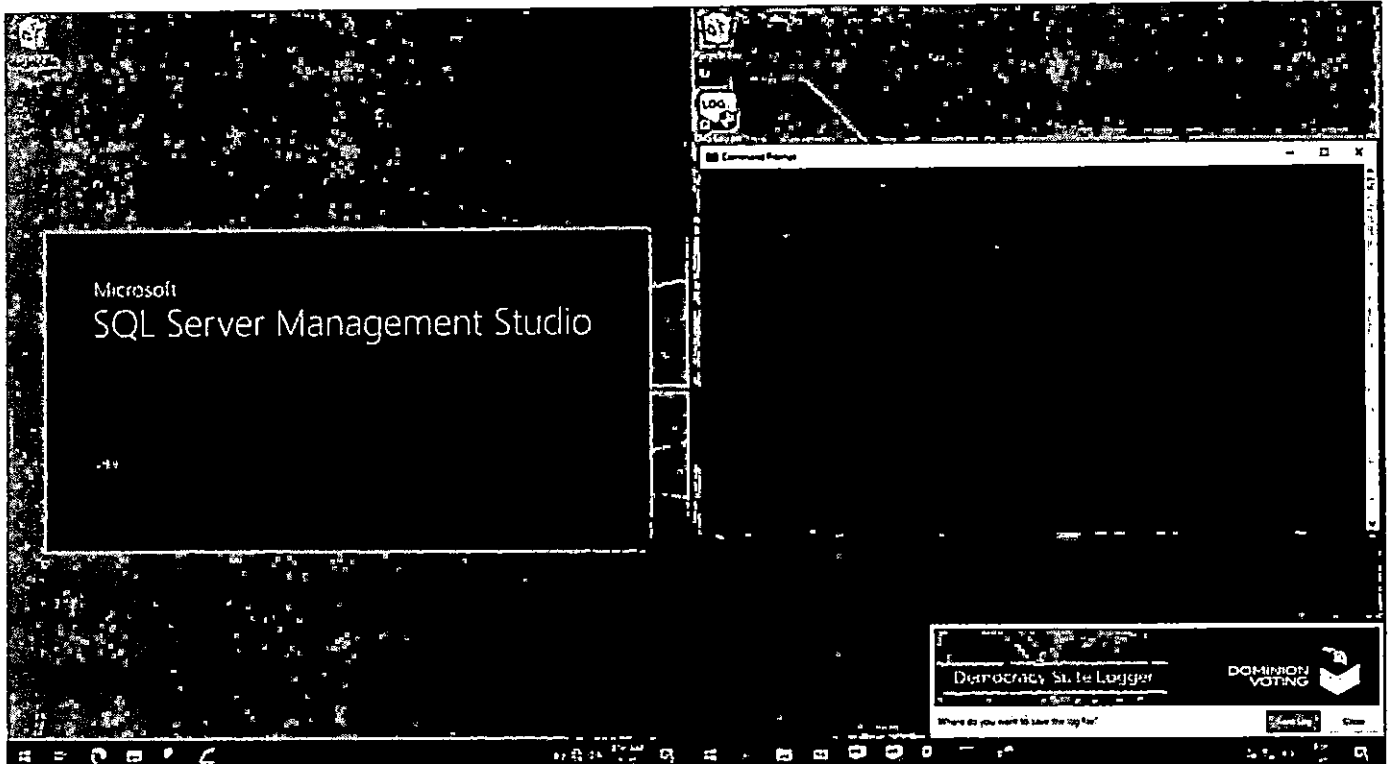


Figure 40 - SSMS access test from separate computer not part of the DVS D-Suite system

SSMS is downloaded from Microsoft and installed on the Test Workstation. Here, it is started, just as it was on the EMS server previously.

Anyone could do this by following the simple directions found with an Internet search for 'how to download SQL server management studio.' There are also many videos on the internet that walk even a novice through doing so.

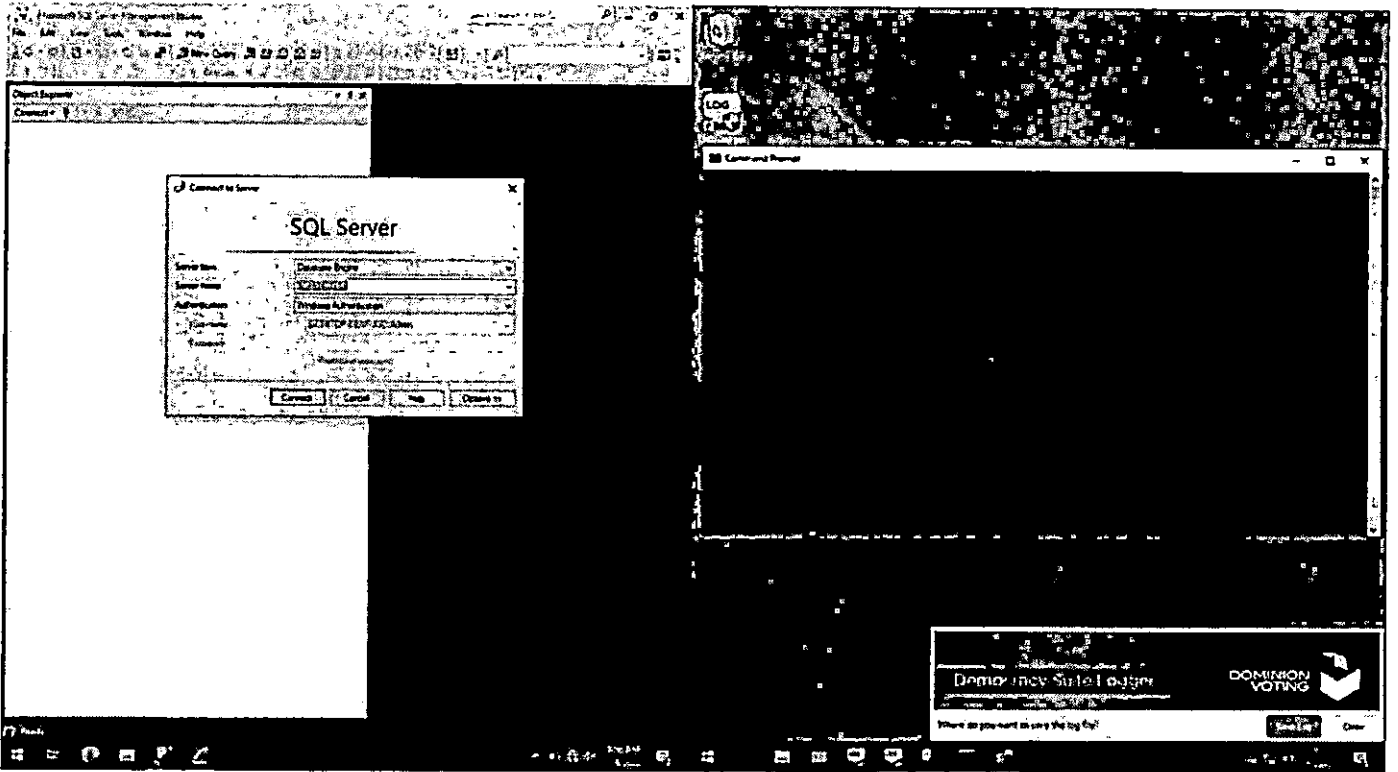


Figure 41 - Log In to the server

A user account was created on the Test Workstation using the same username and password that was used to log in to the EMS server on the right. SQL Server Management Studio was started and the same computer name 'EMSSERVER' was typed into the 'Server name' field on the Test Workstation.

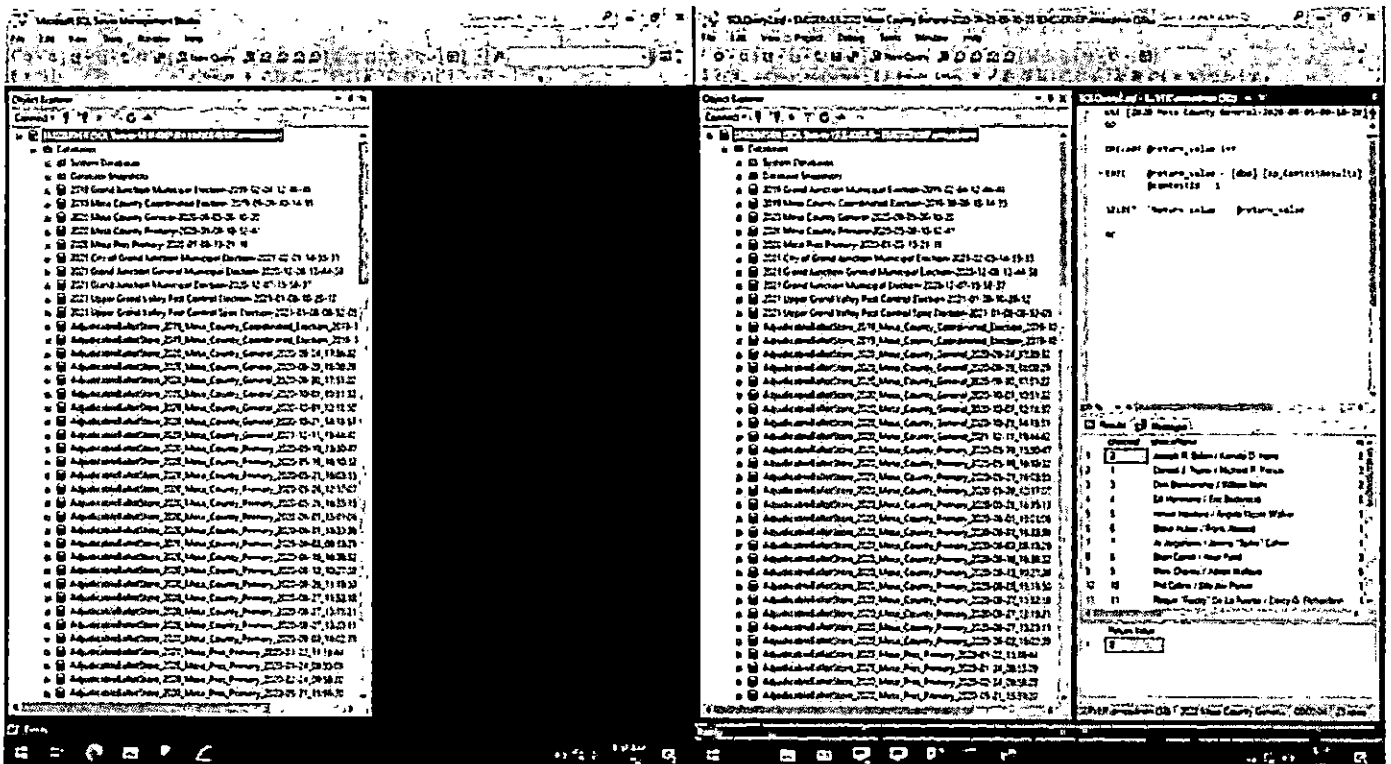


Figure 42 - From a separate Windows 10 computer EMS server database access has been obtained.

After clicking 'Connect,' SQL Server Management Studio connected successfully without so much as a warning. Clicking on the '+' next to Databases reveals the same list of databases available on the EMS server itself, accessible from the Test Workstation.

In Figure 42 I have obtained access to the EMS server from a separate computer not part of the Dominion system and can see election databases. On the left side of the screenshot, the display from the test workstation is shown and on the right side of the screenshot the display from the EMS server is shown. Both systems show the same databases listed. Remote access (i.e., from a separate computer not part of the Dominion system) to the database has been obtained by the Test Workstation.

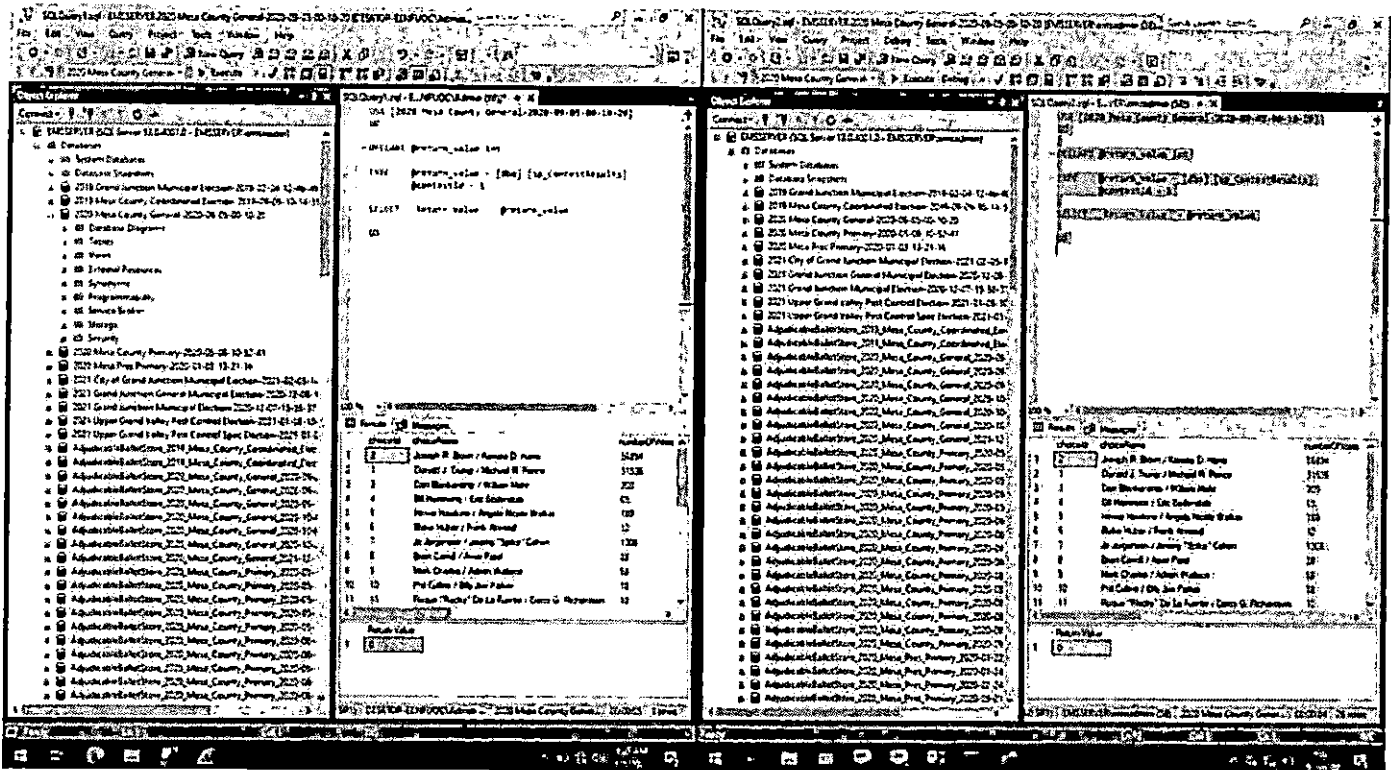


Figure 43 - From a separate Windows computer, the databases can be accessed and reports run.

To confirm this is the data directly from the EMS server, the same report is run on both systems. They both report identical information from the database.

The results display the database in the altered state in which it was left, showing the flipped 56,894 votes for Biden and 31,536 for Trump from the test illustrated in Figure 28.

Finding 5: The security configuration of the Mesa County EMS server permitted access to election data and records from a separate computer not part of the DVS D-Suite system.

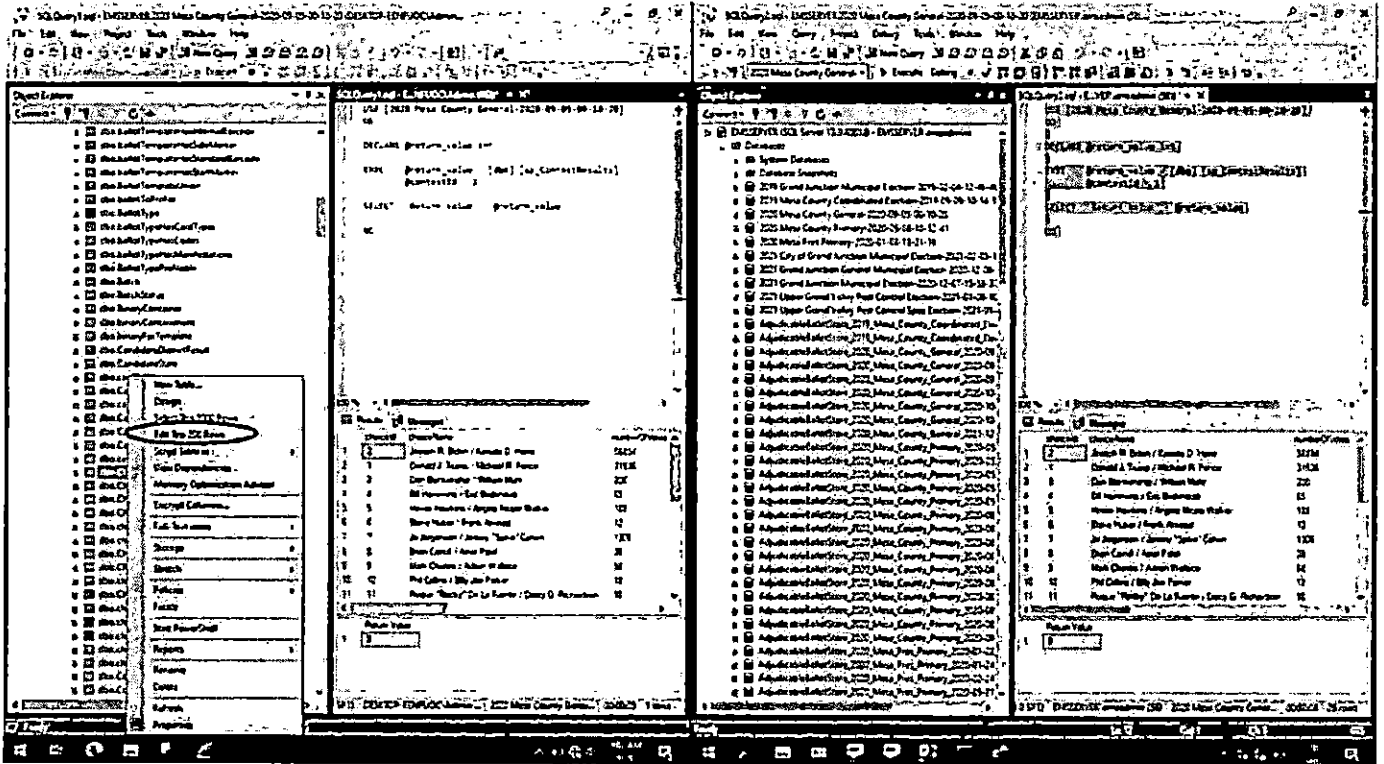


Figure 44 - SSMS permits database Edit

I again right-click on the 'dbo.Choice' table and then select 'Edit Top 200 Rows'.

As previously shown via the EMS server itself, using Microsoft SSMS on a separate computer, not part of the DVS system, access was gained to the same data and the same operations performed as if it was done on the EMS server itself.

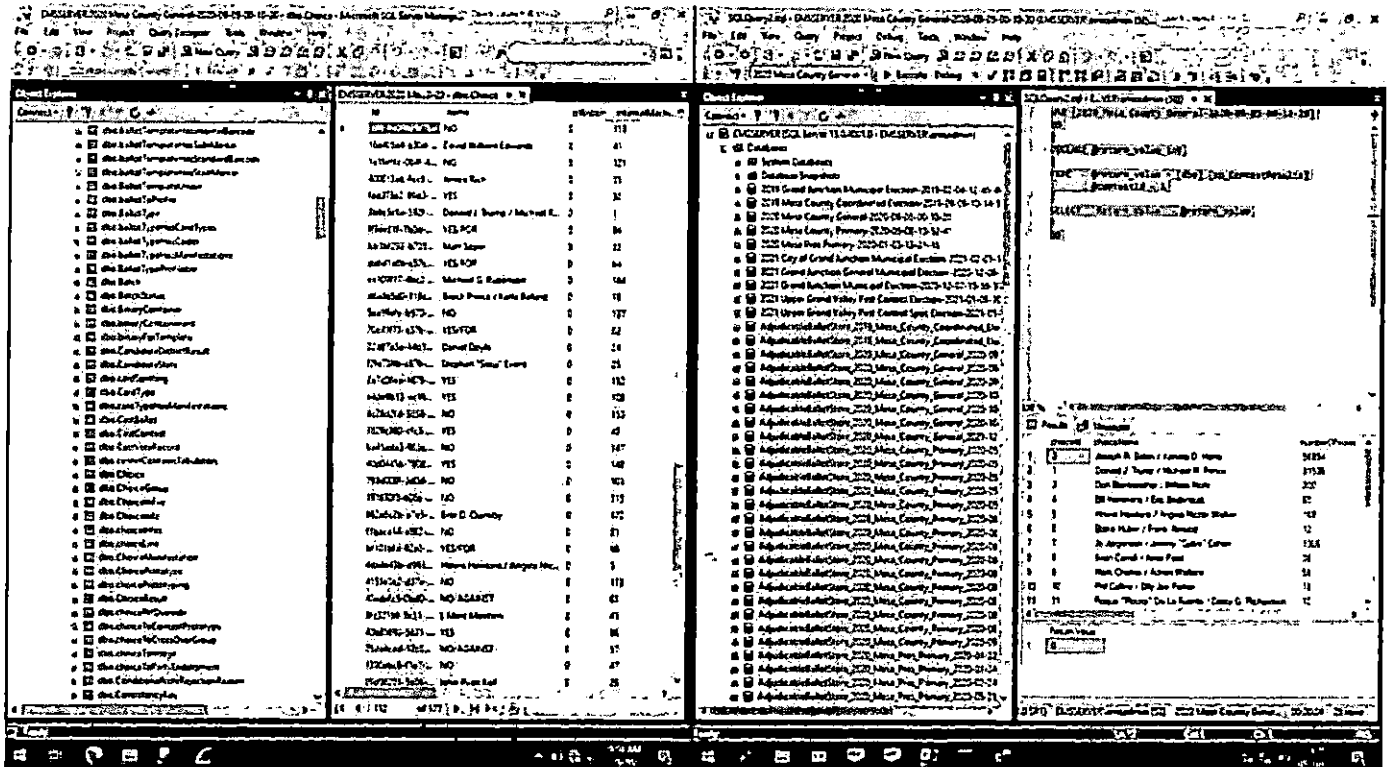


Figure 45 - EMS server Database view from a separate computer not part of the DVS D-Suite system

SSMS shows the same table in the same format as it did on the EMS server.

In Figure 45 the top 200 rows of the election database are available for editing using SSMS running on the Test Workstation to access the Mesa County EMS server across the network. The internalMachIneld for Biden is still '2' and for Trump it is still '1' from the previous alteration in Examination Objective 1 (Figure 26).

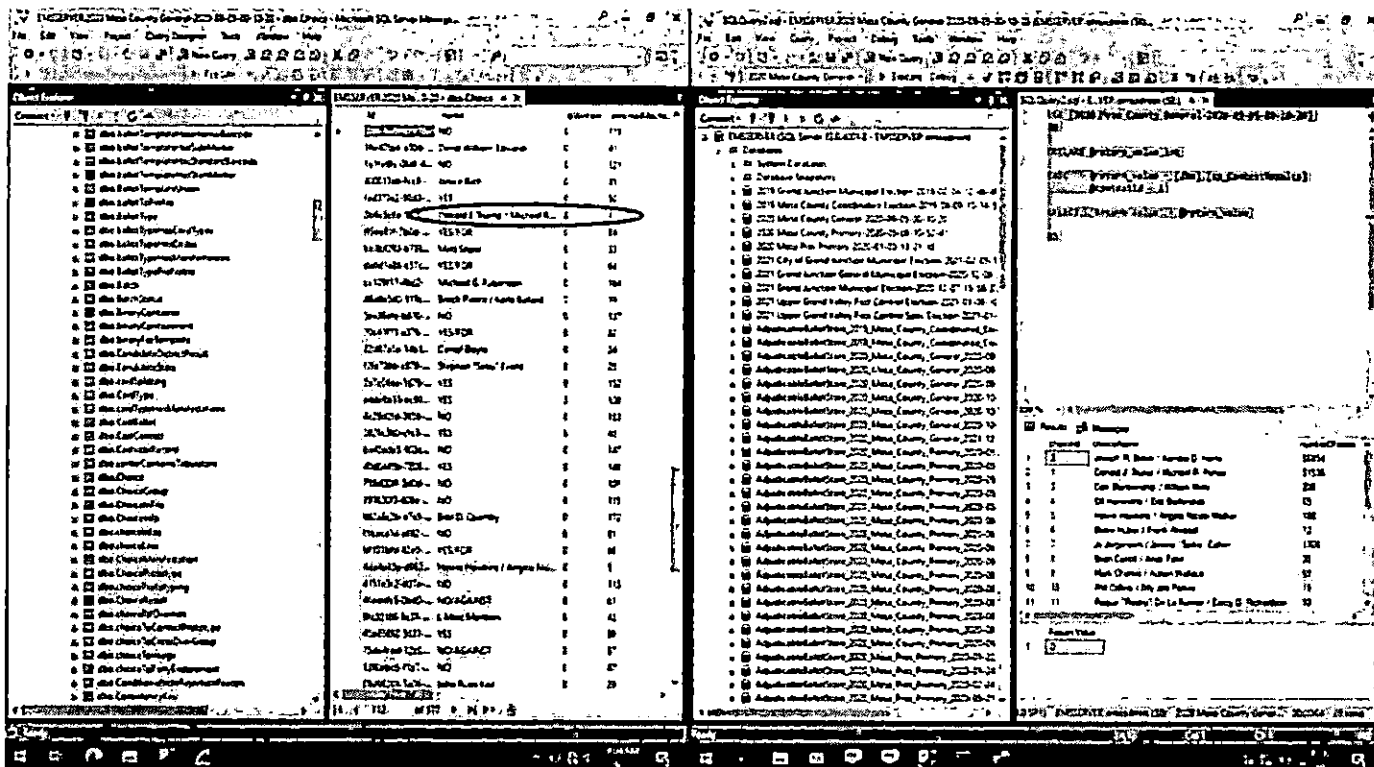


Figure 46 - SSMS permits us to edit the databases

A successful attempt to edit the election database on the EMS server, from the Test Workstation, is made to reverse the changes made earlier, thereby altering them back to the original results. Note the current setting of internalMachineld for Trump is '1.'

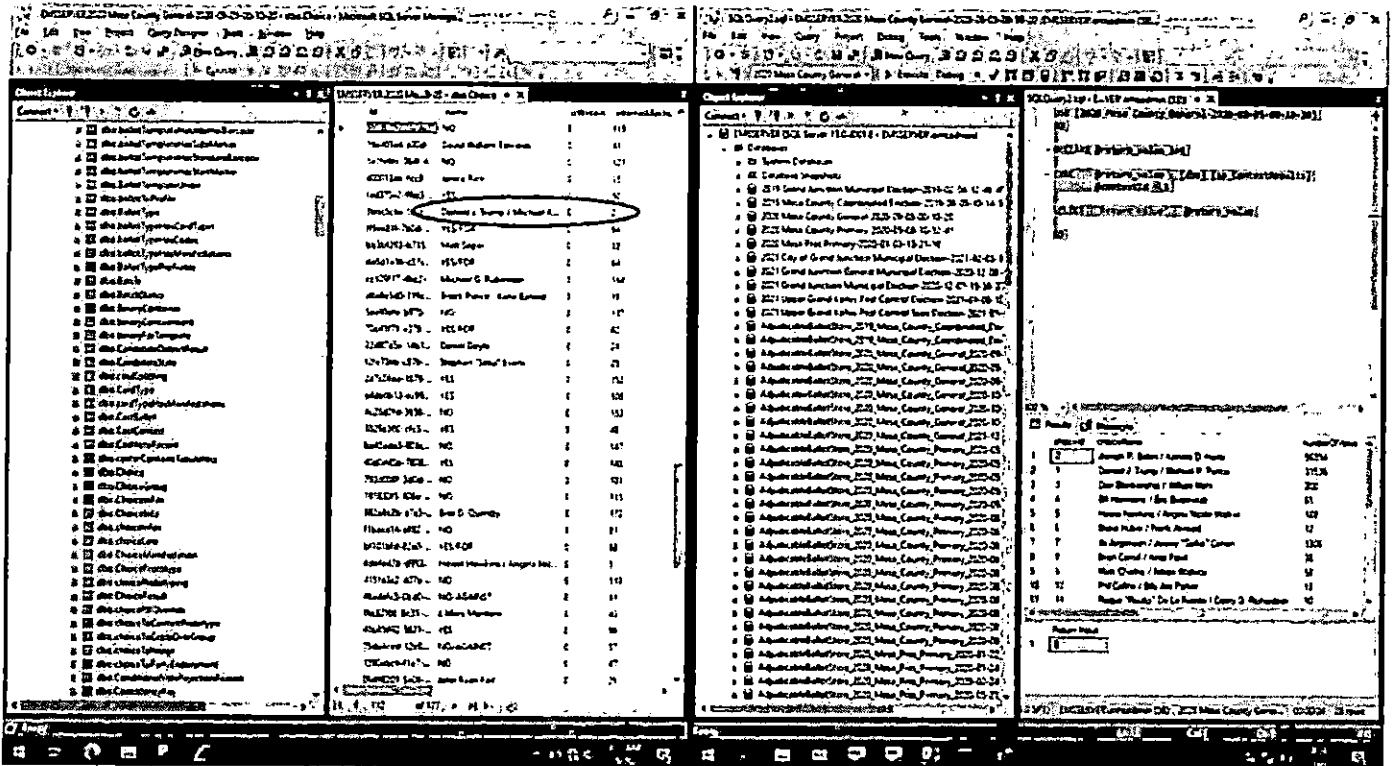


Figure 47 - "internalMachinelD" for Trump is now changed back to a 2.

The "internalMachinelD" for Trump is changed back to "2." The database server allows this alteration from the Test Workstation without any error or warning.

The screenshot displays a Microsoft Access database window with a table of candidate data. The table has columns for 'id', 'name', 'election', and 'internalMachined'. The entry for 'Joseph R. Biden / Kamala D. H.' is circled in red, showing an 'internalMachined' value of '2'. Other candidates listed include 'Kamala Harris', 'Bernie Sanders', and 'Elizabeth Warren'. To the right, a 'Queries' pane shows a list of queries, and a 'Results' pane displays a list of names and numbers.

id	name	election	internalMachined
1000001	Kamala Harris	NO	7
1000002	Bernie Sanders	YES	14
1000003	Elizabeth Warren	NO	15
1000004	Joe Biden	YES	123
1000005	Joe Biden	YES	102
1000006	Joe Biden	NO	67
1000007	Joe Biden	NO	49
1000008	Joe Biden	NO	13
1000009	Joe Biden	NO	21
1000010	Joe Biden	YES	142
1000011	Joe Biden	NO	13
1000012	Joe Biden	NO	15
1000013	Joe Biden	NO	125
1000014	Joe Biden	YES	36
1000015	Joe Biden	YES	78
1000016	Joe Biden	YES	112
1000017	Joe Biden	NO	111
1000018	Joe Biden	NO	27
1000019	Joe Biden	NO	28
1000020	Joe Biden	YES	12
1000021	Joe Biden	YES	73
1000022	Joe Biden	NO	123
1000023	Joe Biden	NO	42
1000024	Joe Biden	NO	144

Figure 48 - Candidate data for Biden from previous change

The current "internalMachined" for Biden is still "2", in the election database on the EMS server, as changed earlier from the EMS server.

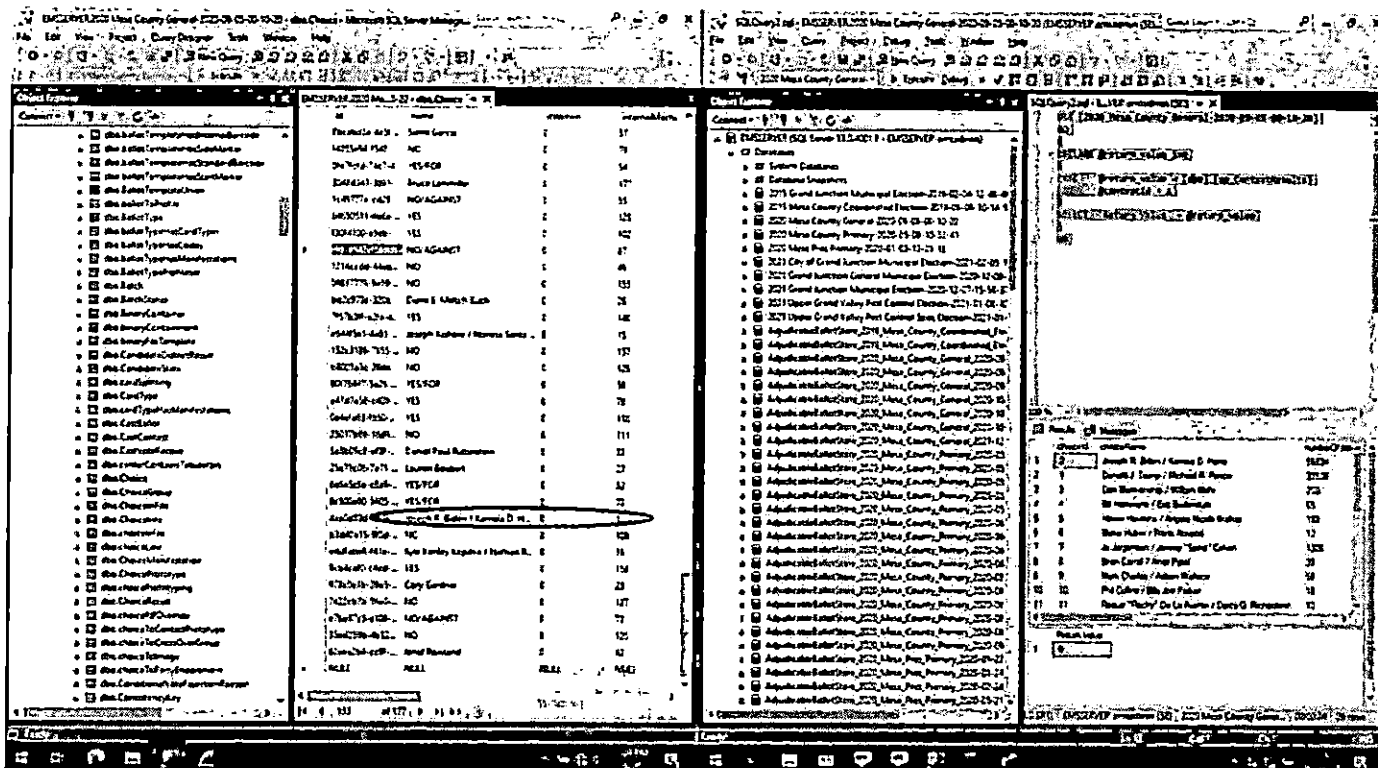


Figure 49 - Candidate data for Biden changed back to original

I next change, from the Test Workstation, the "internalMachinelD" for Biden in the election database on the EMS server back to "1", its original value. There is again no error or warning given.

As one can see, this alteration of the voting database was also successful. The system has been restored to the state in which it was found prior to making the first alteration of the voting system database.

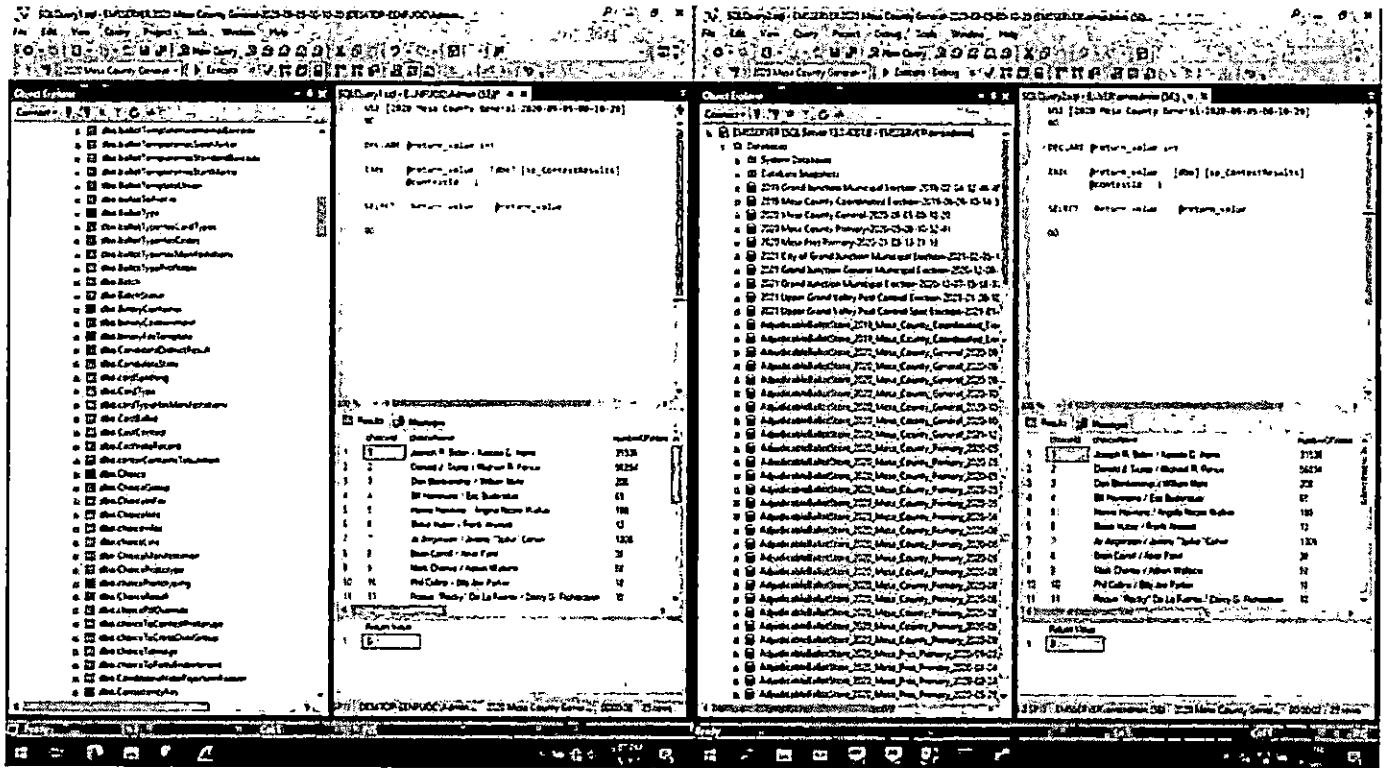


Figure 50 - The vote choice was remotely changed back to its original state

The alterations of the vote totals in the election database on the EMS server also succeeded from a separate computer not part of the DVS D-Suite system. Queries were executed both from the Test Workstation and on the EMS server, and both results again show that it is possible by anyone with physical access to a Dominion Computer or any part of the voting system network to alter the entire election result on the EMS server by changing only two values, with knowledge nearly anyone could attain by using Google and watching one or more YouTube videos.

The query is run on both systems to show that the database results have changed back.

Finding 6: The Mesa County EMS server containing the 2020 General Election vote results has been shown to be insecure and grossly misconfigured such that it allows unrestricted access to the election database and enables changing calculated vote totals from a separate computer not part of the DVS D-Suite system with nothing more than the knowledge of a password. It was possible to access the EMS server and, by changing only 2 numbers in the database, completely alter the election results in Mesa County for the 2020 Presidential election.

EXAMINATION RESULT 2:

The election results database CAN be altered by any person using a non-DVS D-Suite computer directly or indirectly connected to the EMS server network.

EXAMINATION OBJECTIVE 3:

Determine whether the calculated vote totals of an election can be altered by any person using a cell phone or mobile device wirelessly connected to the EMS server network.

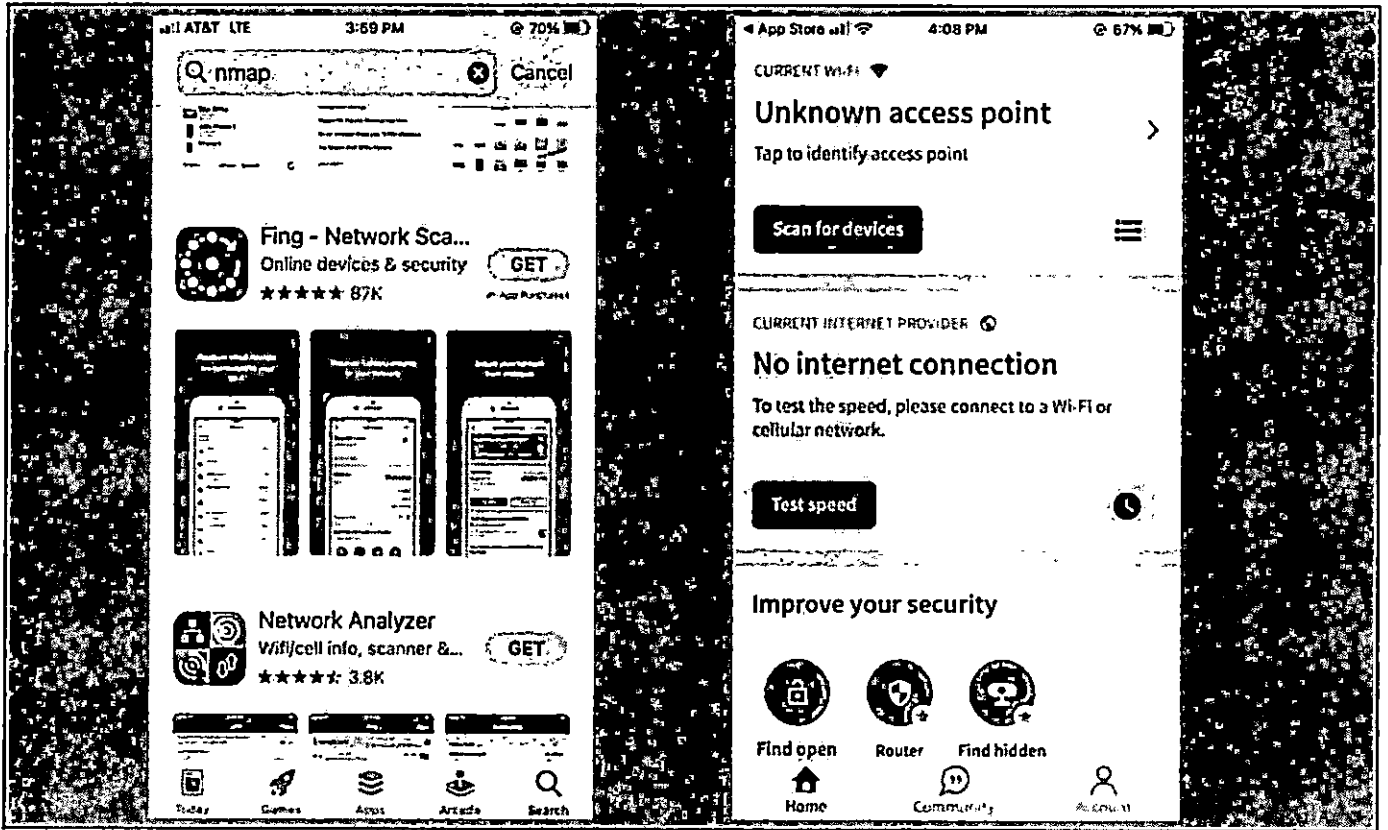


Figure 51 - Network scanner installed on cellphone

An iPhone was connected to the same network, wirelessly, using a common wireless router purchased at a retail store. A router such as this could be plugged in and hidden anywhere on the DVS D-Suite network, or the same functionality could be inserted electronically via common hacking into any device on the network with a wireless card, including network printers and network scanners. As discussed earlier, thirty-five (35) devices of the existing DVS-supplied equipment already had a built-in wireless card or device installed, as well as a wireless-capable printer, so this could have easily been done without attaching any devices outside the system components. The Apple App Store was searched and a common network scanner 'Fing' was easily found. As one can see, 'Fing' has already been downloaded over 87,000 times. In the image on the right, 'Fing' was run and the option 'Scan for Devices' was selected.

Previously an Island-Hopping attack was described. For such an attack to occur, a connection to a different network is used.

This part of the examination was carried out to determine whether the system could have been accessed wirelessly using the more limited capabilities of a mobile device (a cell phone in this test). Thirty-five (35) wireless devices were identified within the Mesa County DVS D-Suite system. In order to perform this part

of the examination it was necessary to mimic the actual MESA hardware, so a wireless access point was connected to the VirtualBox test system that was running the actual software of the Mesa County EMS server via a host-based network interface card.

If any wireless device gains access to any device connected to the EMS infrastructure (as was demonstrated here), including the inadvertent enabling of even a laptop wireless interface (typically performed by a single button press on the keyboard of a laptop, or by preprogrammed, triggered activation of internal code on the device, or by remote command from an actor with access to the device), such an attack could easily occur.

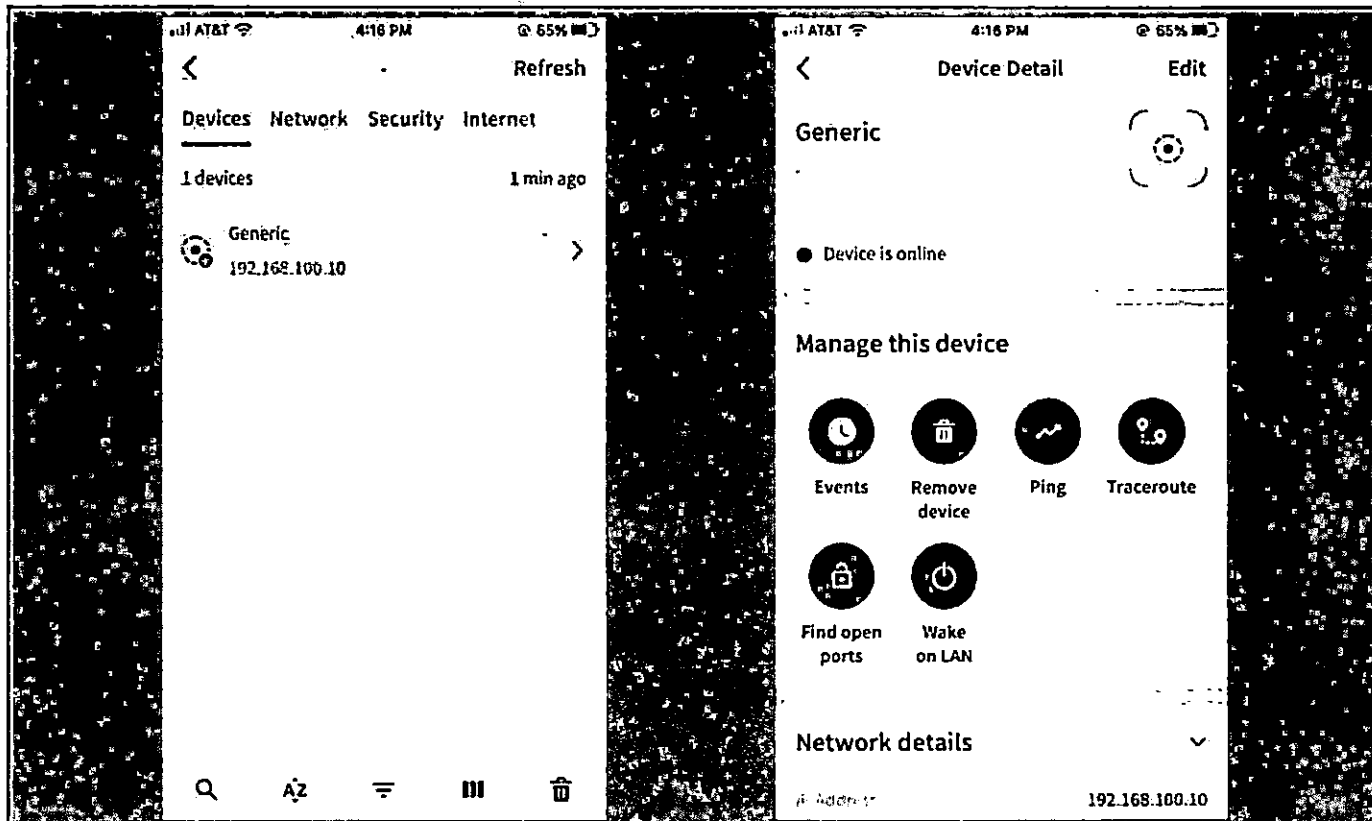


Figure 52 - IP address for the EMS server found via wireless connection and iPhone app

On the left, the network scanner immediately finds the IP address for the EMS Server and displays the IP address (192.168.100.10). The device is selected, and on the right, the phone app presents more options. I then selected "Find open ports."

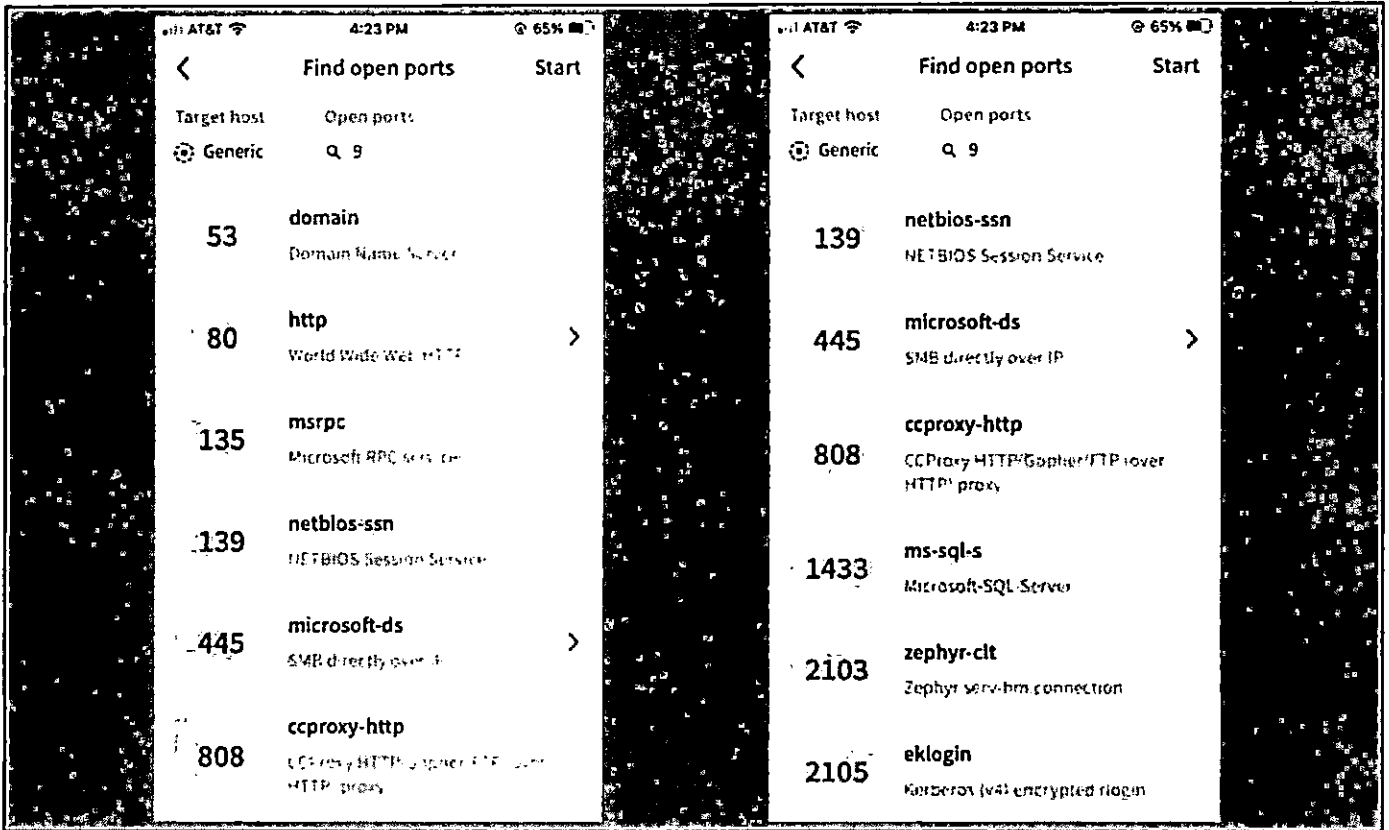


Figure 53 - Scanner Results

The iPhone app lists all the ports that it sees open on the EMS server. Port “1433”, which the app indicates is associated with “Microsoft-SQL-Server,” is immediately detected.

In Figure 53, left, one can see the first 6 of the 9 open ports on the EMS server with a wireless access point connected. On the right, scrolling down the screen reveals the remainder of the 9 open ports identified. The SQL service port, 1433, has been identified as operating and configured on this device.

Using the method recommended by CIS (Nmap⁷¹), a device that offers the Microsoft SQL Service has been identified. This uses standard networking software that many IT professionals and most IT Security professionals are very familiar with.

Whether such an exploitation of technology is performed with the single-response ping command or by using a more powerful tool like Nmap, the discovery of a network connected device on the same network segment has been accomplished.

⁷¹ Network Mapper (Nmap) is a tool for network exploration or security auditing, frequently used by cybersecurity penetration testers to find live / operating devices and hosts on networks, perform port scanning, detect operating systems and versions in use, and ping networks and subnetworks to diagram potential and available communication paths.

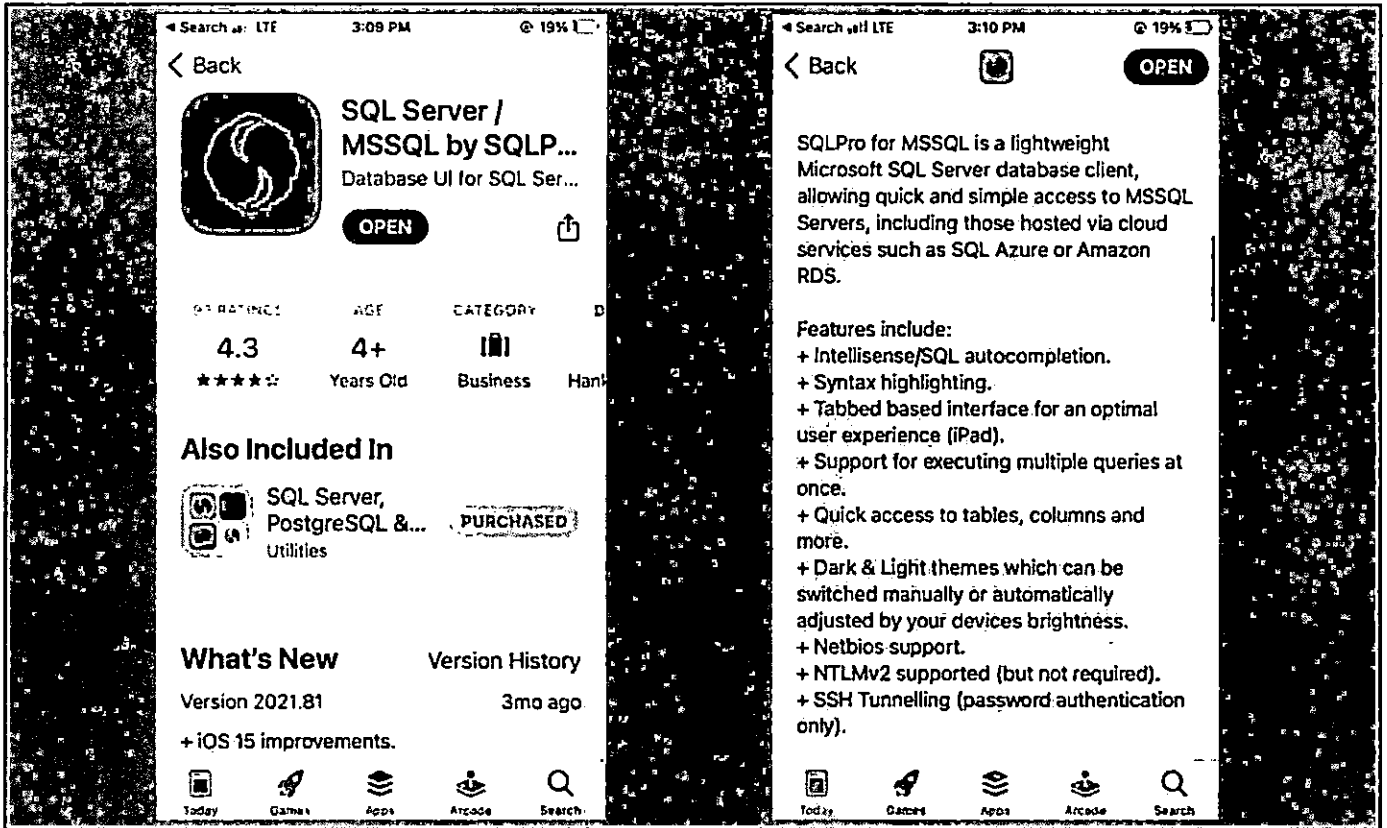


Figure 54 - SQL Access Functionality

Returning to the Apple App Store, a search for 'SQL Server' finds another app, 'SQL Server by SQLPro'. The description shows that it is a Microsoft SQL Server database client.

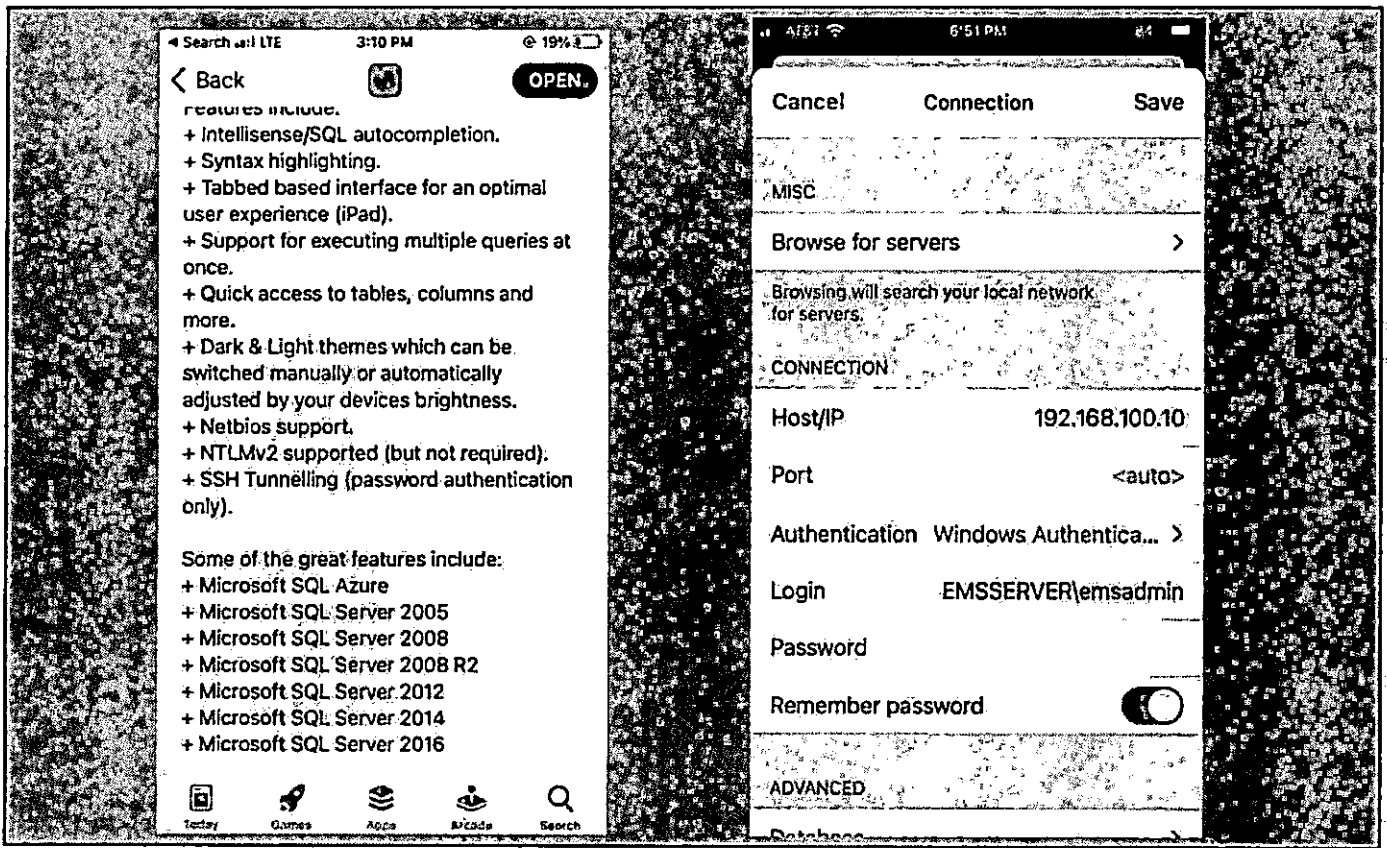


Figure 55 - SQL Pro Capabilities

On the left, the app description shows that it supports Microsoft SQL Server 2016, which is the exact version used by the EMS server. On the right, we use the same IP address, username, and password applied from the iPhone app as previously used to access the EMS server, physically sitting in front of its screen.

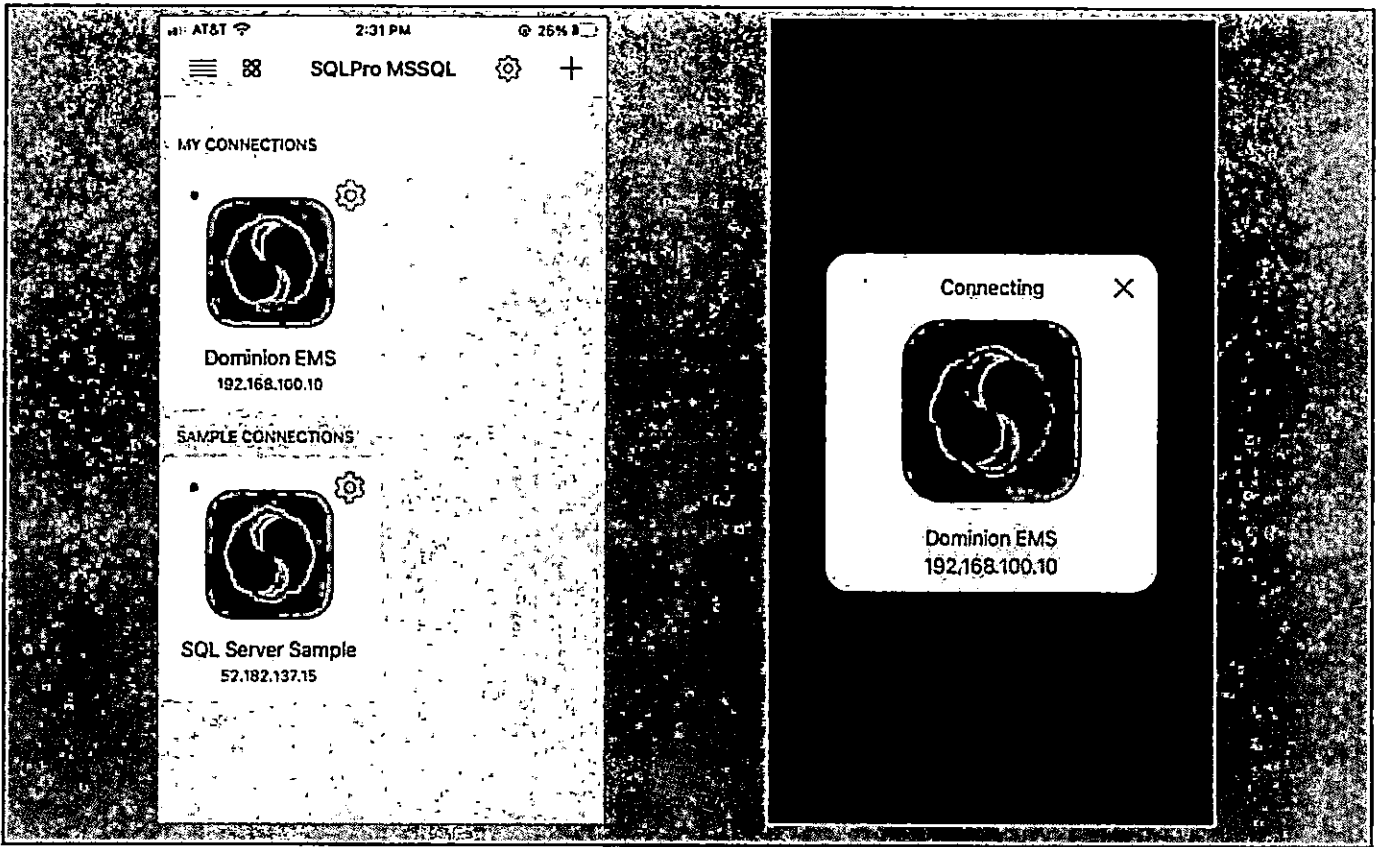


Figure 56 - Making an SQL Connection

The left image shows the configured connection to the EMS server. The right image shows the iPhone connecting directly to the database on the EMS server.

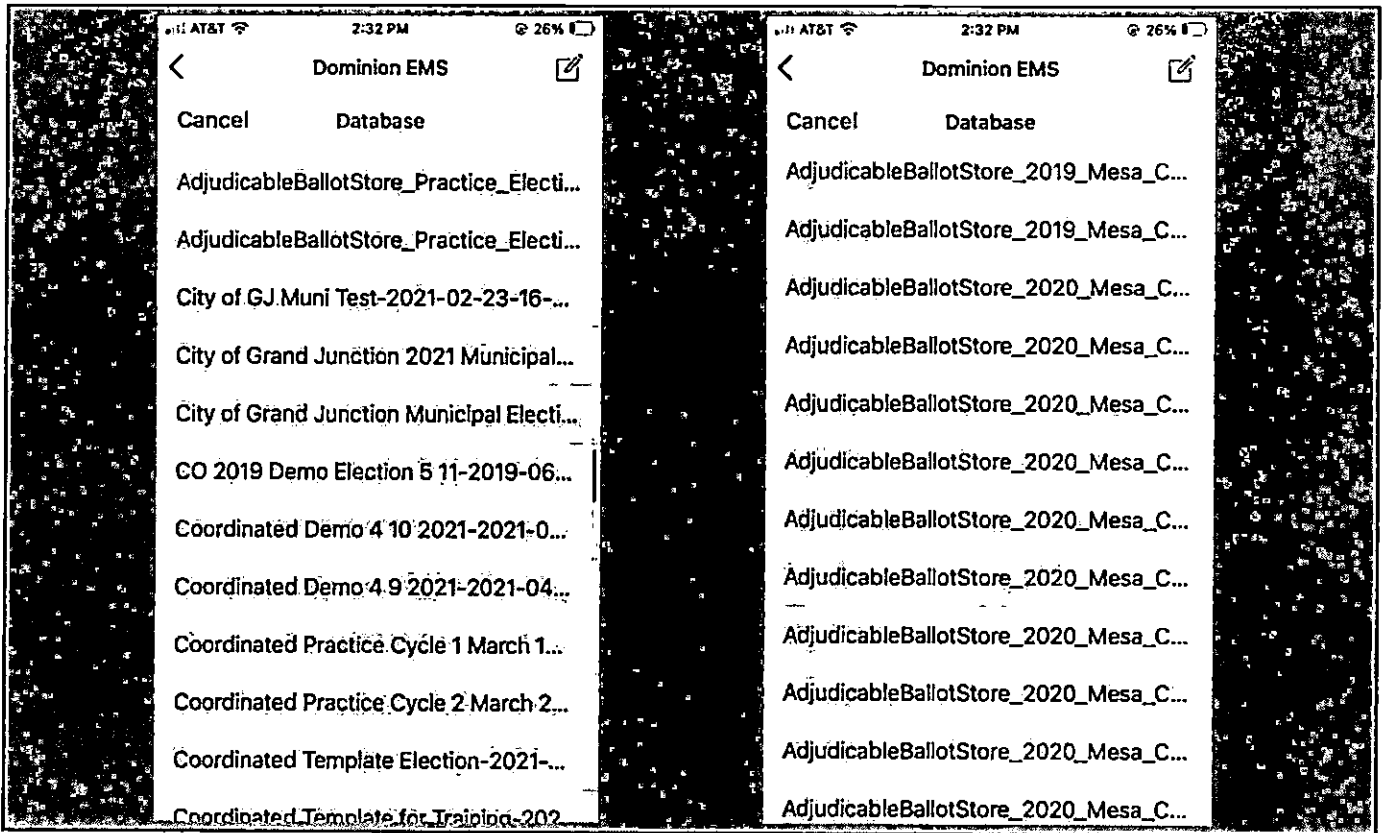


Figure 57 - iPhone Connection to Dominion EMS Database

After a second, the app lists all the voting system databases, just like it did on both the EMS server and on the Test Workstation.

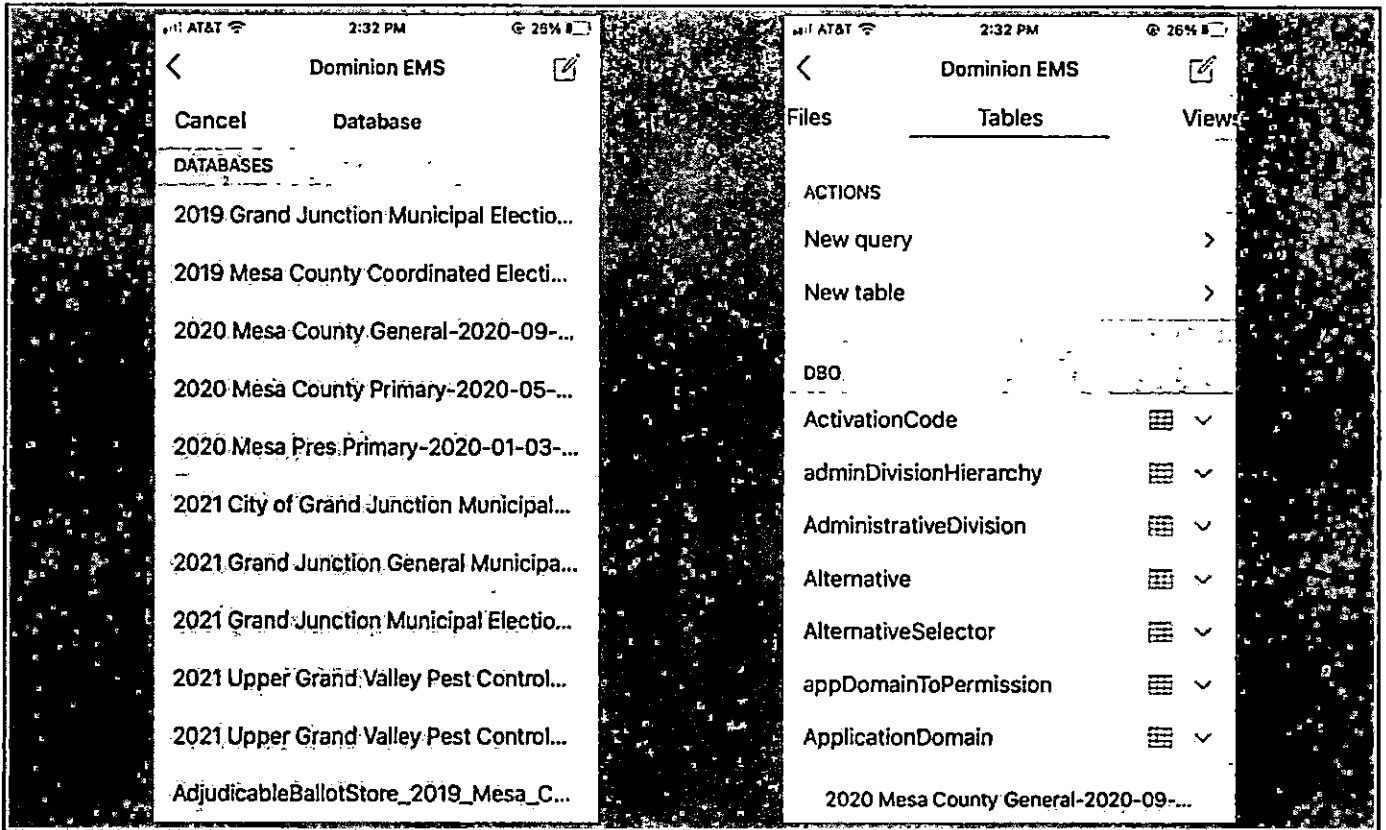


Figure 58 - Databases listing, Continued

Multiple Tabulation Store databases are shown on the left. Next, the 2020 Mesa County General election was chosen from the top of the list, and the image on the right shows the resulting screen, listing the tables in that particular database. So far, the examiner has not been denied access or even experienced a warning of any kind.

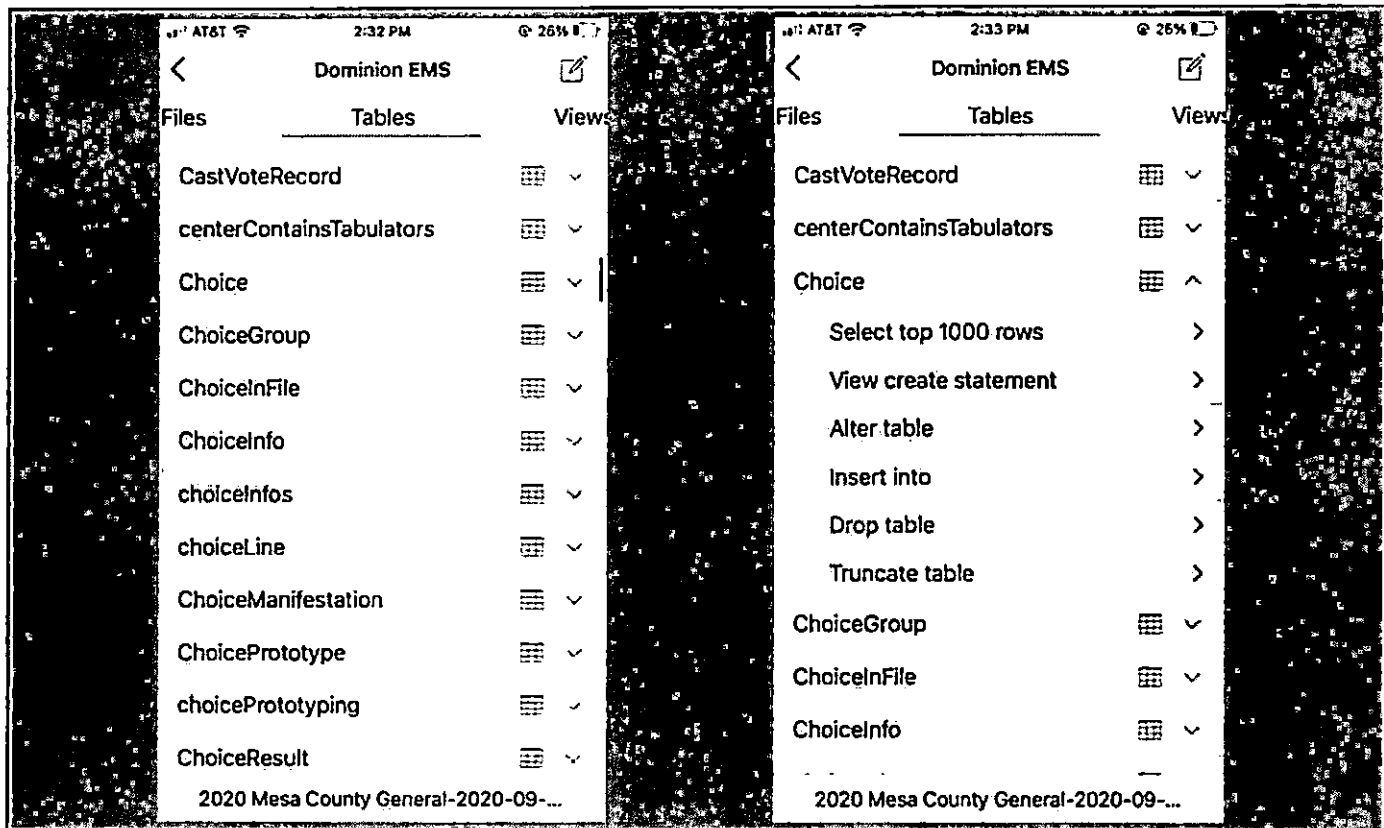


Figure 59 - Database Table Listing

On the left, one sees the same 'Choice' table as was seen on the EMS server and Test Workstation (where it was called 'dbo.Choice'). On the right, 'Choice' table is selected resulting in the options as shown. I selected 'Select top 1000 rows'.

Note that the "drop table" command would delete the table entirely, while the "truncate table" command would shorten the table, and if applied to a table containing actual vote data, would delete some of those votes.

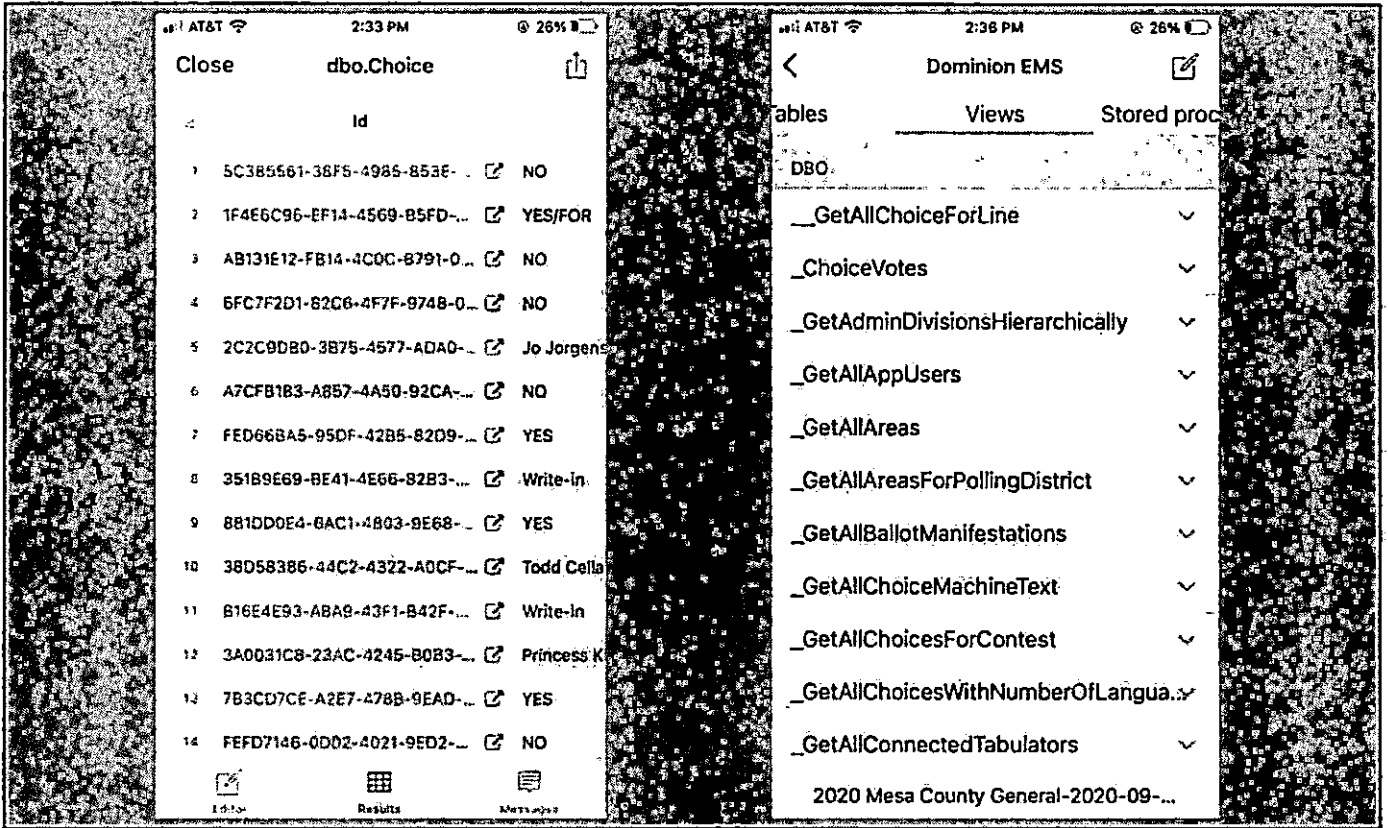


Figure 60 - Database Access

On the left, one sees the top 177 rows in the 2020 Mesa County General database, along with the choices listed as shown by both the EMS server and the Test Workstation. On the right, 'Views' at the top menu was then selected to pull up the database views from the EMS server.

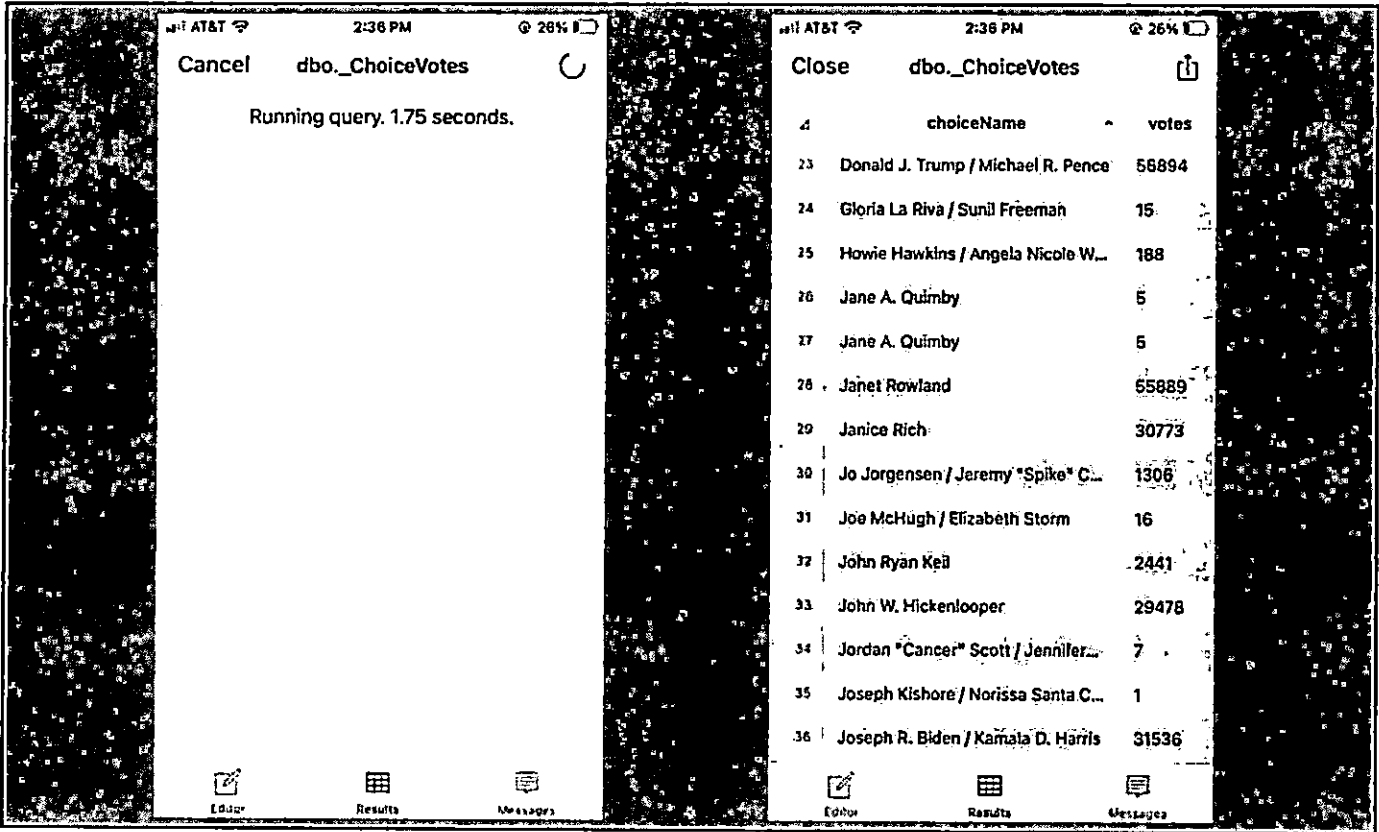


Figure 61 - Executing a Database Query

The _ChoiceVotes view was selected. On the left, one sees that it took 1.75 seconds to pull up all the votes for each choice in the election. The result of that query is shown on the right.

id	name	isWritein	internalMachineld
23	Donald J. Trump / Michael R. Pence	0	2
24	Gloria La Riva / Sunil Freeman	0	17
25	Hovie Hawkins / Angela Nicole W...	0	5
26	Jane A. Quimby	0	171
27	Jane A. Quimby	0	165
28	Janet Rowland	0	42
29	Janice Rich	0	35
30	Jo Jorgensen / Jeremy "Spike" C...	0	7
31	Joe McHugh / Elizabeth Storm	0	18
32	John Ryan Keil	0	29
33	John W. Hickenlooper	0	22
34	Jordan "Cancer" Scott / Jennifer...	0	20
35	Joseph Kishore / Norissa Santa C...	0	15
36	Joseph R. Biden / Kamala D. Harris	0	1

Figure 62 - Table Data

The left and right images demonstrate the effect of scrolling to the right, to display all the columns. All the columns in this table can be viewed without being denied or without any type of warning.

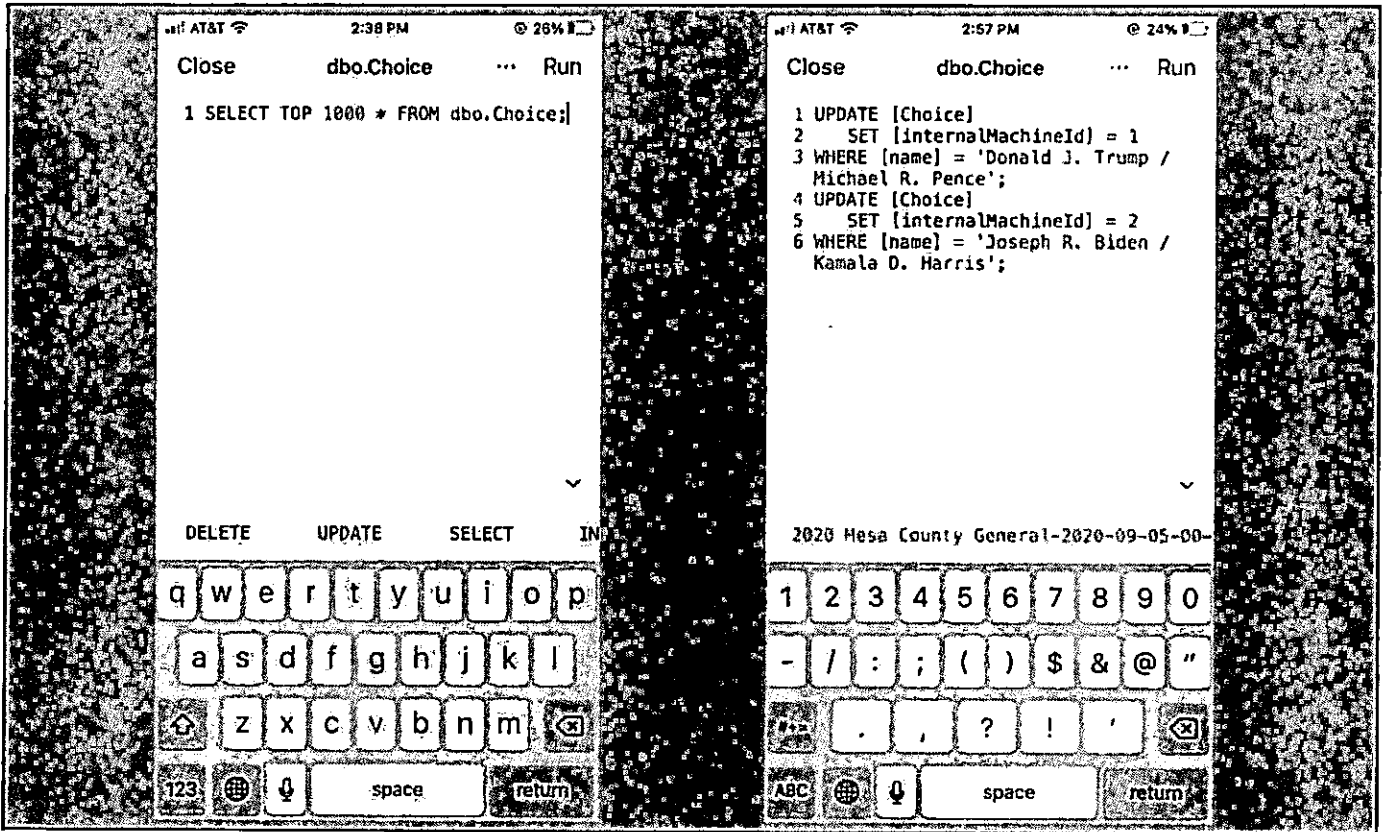


Figure 63 - A script to change the vote data

The left image shows the default query that asks for the SQL Server to send the top 1000 rows from the dbo.Choice table. The instructions on the image on the right were then typed in. What they do is very simple: They update the Choice table by setting the internalMachineId to '1' for 'Donald J. Trump / Michael R. Pence,' and setting the internalMachineId to '2' for the entry with 'Joseph R. Biden / Kamala D. Harris' in it. This is the same type of change that was made by hand on both the EMS server and the Test Workstation earlier in this report.

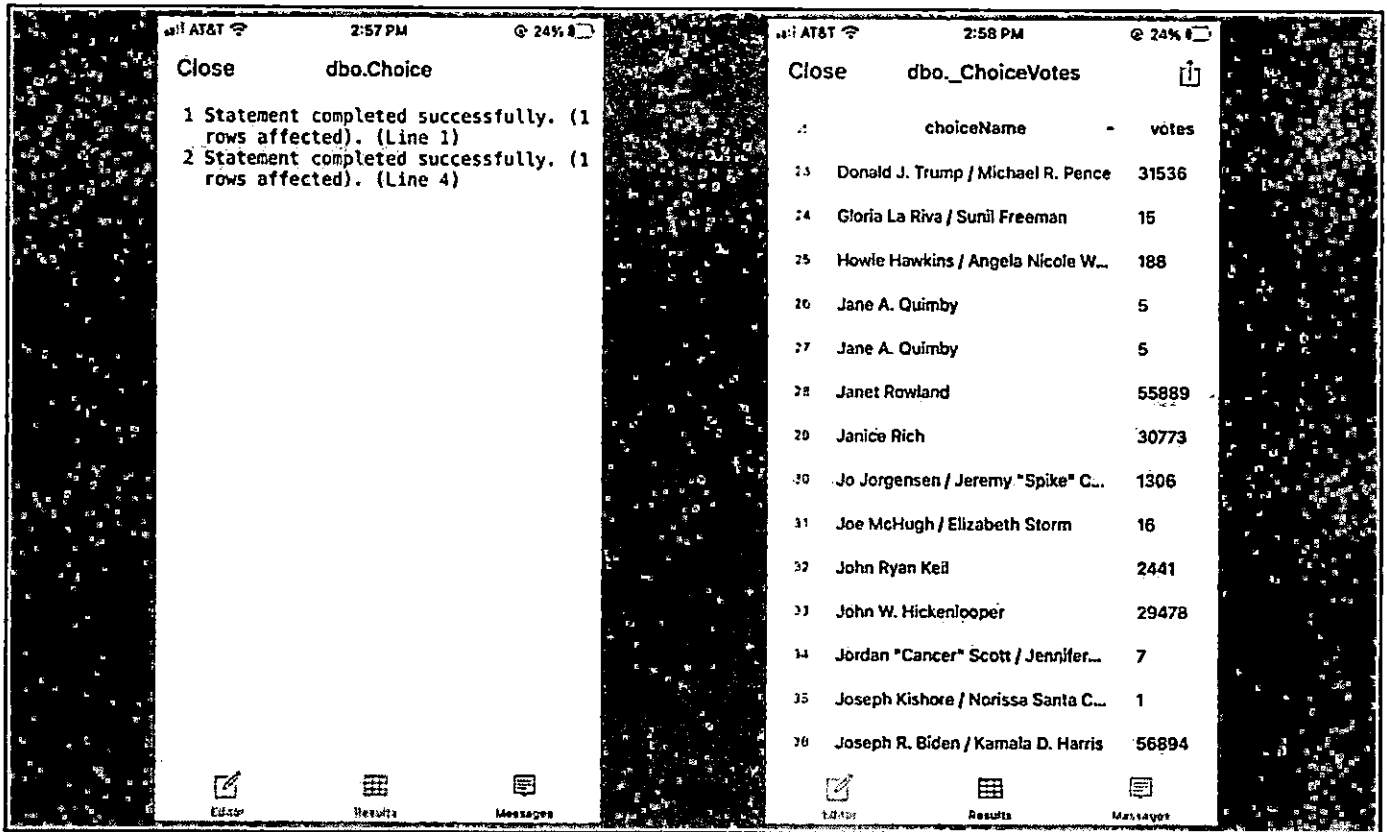


Figure 64 - Script Results

The image on the left shows the typed instructions were executed and the EMS server reported that each instruction was completed successfully, affecting one row each. On the right, the `_ChoiceVotes` view is run again to see that once again the election results were flipped from Trump to Biden, using a basic iPhone with an app downloaded from the App Store that anyone could install and use.

EXAMINATION RESULT 3:

The calculated vote totals in an EMS server database can be altered by any person using the more limited capabilities of a mobile device wirelessly connected to the EMS server network.

For the iPhone test, while a wireless device was added to the network to allow this demonstration to occur, it's alarming that's all it took to accomplish this, especially since thirty-six devices in the Mesa DVS hardware had wireless cards installed. Anyone could purchase a wireless device like this online or at most computer or office supply stores, attach it inside the voting center, and use one of the easy to guess or well-known passwords on the system (or obtain it from the Darkweb,⁷² or access the iDRAC remote control server, or use DVS-published default passwords, etc.), could sit out in the parking lot and change any part of the database before, during, or after an election. More dangerous, since thirty-six devices in the DVS D-Suite System were configured with a wireless card, the same abuse could be committed by someone with basic computer networking skills,⁷³ given wireless access to the EMS server is completely insecure, exposed to access, protected by only a Windows password, despite many additional protections being available. As an example, a Dell Wireless 1560 internal wireless adapter was identified in the specified configuration on the DVS D-Suite ImageCast Voter Activation (ICVA) computer that is part of the Mesa County DVS D-Suite system. A skilled individual could easily get away with this same unauthorized access and much more with almost any modern cell phone, iPhone or Android, Mac, or PC. Wireless capability is very small today, easily fitting inside a small USB device, which could even be inserted in an internal port, invisible to County officials, allowing for the surreptitious connection of the capability in such a manner that only highly trained specialists would be able to find it. Figure 65 depicts such a miniaturized wireless USB device, which could be installed without notice on a motherboard of the type used by D-Suite EMS servers (shown).

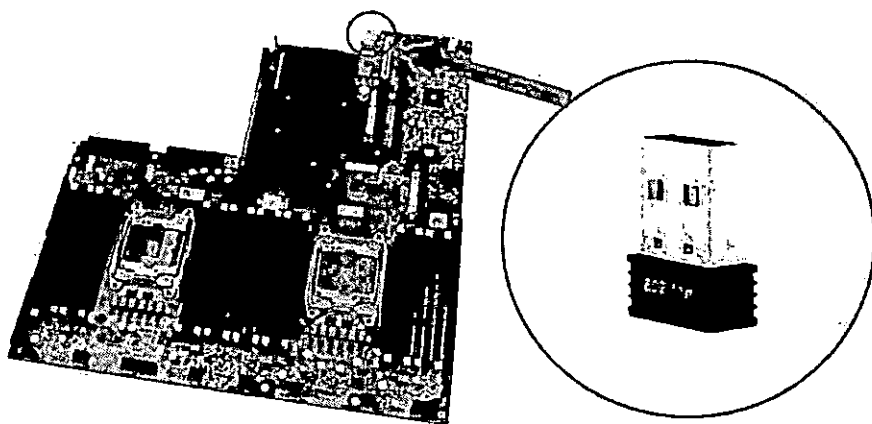


Figure 65 - Small Wireless Device Surreptitiously Installed (internally) on a Computer Motherboard

The result of this examination demonstrates that an attack is possible using a wireless device connected in any one of a multitude of ways. It was possible to perform network scanning using industry standard tools on a common Apple iPhone.

⁷² The Darkweb is a clandestine, encrypted, anonymized webserver infrastructure characterized by extensive criminal activity including trafficking in computer access credentials (passwords) as well as many other criminal activities. Access to the Darkweb is only available through use of The Onion Router (TOR) which hides and renders untraceable (to most searches and searchers) the IP address and location of its users. Content on the Darkweb is hidden from the general Internet to facilitate criminal activity.

⁷³ <https://papers.mathyvanhoef.com/ccs2017.pdf>, <http://www.krackattacks.org/>

CONFIDENTIAL

It must be noted that the methods used here are well described in publicly-available, commonly-known literature. Cybersecurity industry guides⁷⁴ describe the Nmap application specifically to identify connections to the network. Nmap uses the ICMP 'echo request' command, just as our previous check did using the 'ping' command. Nmap is capable of executing many echo requests in parallel to more rapidly identify the devices connected to a network than the single-request ping program can, and Nmap tests all of the port numbers configured to be tested, for each IP address being tested.

The report in this examination does not reveal any secret tradecraft, or compromise election security; the techniques used in this examination are common among IT professionals. Unfortunately, there is very little security in this voting system, to begin with.

This examination demonstrates how the use of wireless networking can be easily exploited and documents the risk presented using one example. Given the ease with which it can be implemented if wireless devices are enabled (e.g., by an accidental button press on a laptop), it is important to acknowledge the risk so that future elections can be properly protected. To assure integrity of the infrastructure, computing devices with wireless network capability must not be used because wireless networking can be easily enabled by accident (or maliciously). Additionally, certification under VSS absolutely required steps to have been taken within the voting system design and implementation that secure the system from accidental or malicious connections to other networks. The fact that these steps were not taken casts doubt on the credibility and competence of the vendor, the certification authority, the certification testing lab, and the institutions responsible for the testing lab accreditation program.

Making use of the broadband modem inside the cell phone, it may be possible to create a connection from the internet directly into the electronic voting system, bypassing all County firewalls and security, allowing someone to command and control it from anywhere in the world.

This would be completely undetectable by election officials, and most, if not all forensic experts.

While critics may assert that it has not yet been proven that any wireless device was connected to the Mesa County systems and operating prior, during, or after the election, the fact is that wireless devices were installed in Mesa County DVS systems, and critics cannot prove those devices were not operating and exploited. The required compliance standards were created explicitly to provide such proof, yet the features that enable compliance were disabled. Due to the illegal disabling of logging mechanisms, configured overwriting of logs, and the failure to preserve the log data (in violation of the law) that would either show tampering and fraud or support claims of the integrity of the election, it cannot be proven that the election was free of intrusion and tampering (See Report #1).

⁷⁴ <https://attack.mitre.org/techniques/T1046/>

CONCLUSION

An ongoing forensic examination of the Mesa County EMS server, version 5.11-CO, provided by DVS revealed the overwriting of critical log data and election records, the misconfiguration of logging functions, and the failure to preserve required election records in Report #1.

In this Report #2, the examination has conclusively shown and demonstrated the ability to access election records from a separate computer, not part of the DVS D-Suite system, the ability to edit the election database, and the ability to change calculated vote totals to alter the election results on the Mesa County EMS server entirely, "flipping" the winner of an election contest in the jurisdiction from one candidate to another.

The Key Objectives for this report were answered by this examination:

1. To determine whether D-Suite-implemented security requirements comply with the 2002 Voting System Standards (VSS)
 - a. Uncertified software was used on the system rendering the certification of the entire system and all elections conducted with it, Invalid.
 - b. Security protections required by law were almost completely absent
 - i. Other than a userID and an easily guessed or bypassed password, no authentication was required
 - ii. The firewall rule for access to the election database, ballots and results was unrestricted to any IP address in the world
 - iii. Together with the firewall rule, Microsoft SQL Server Management Studio (SSMS) enabled complete access to the entire election databases – not just to the 2020 election but to the elections of June 2019 through May 25, 2021.
 - iv. A self-signed encryption certificate was used introducing the potential for a man-in-the-middle attack
 - v. Thirty-five wireless devices (802.11, Wi-Fi) were installed inside election equipment and an additional wireless device was identified in a connected printer
 - vi. Any or all of these wireless devices could have connected to the Internet via the building wireless facilities
 - vii. "Purging" (deletion) of critical Audit Log data, as specified by DVS and directed by the Secretary of State⁷⁵, destroyed all records of connection to the Internet or elsewhere, all record of user activity, including programs run by these users, errors, and any record of the addition or deletion of votes and the alteration of election results.
 - c. EACH of the compliance failures identified in 1.a. and 1.b. above are clear violations of the law.

⁷⁵ The TDP associated with the "trusted build" process is promulgated by the Secretary of State. CRS 1-5-620 States that the vendor provides manuals and documentation and that any information not on file with and approved by the Secretary of State shall not be used in an election.

2. To determine whether the results of an election, stored on the EMS server, can be altered by any person with physical access to the logged-in EMS server,
 - a. Any person with physical access to the logged-in EMS server can change the calculated vote totals on the EMS server.
3. To determine whether the results of an election stored on the EMS server, can be altered by any person using even a non-Dominion computer directly or indirectly connected to the EMS server network.
 - a. Any person using even a non-DVS computer directly or indirectly connected to the EMS server network can change the calculated vote totals on the EMS server.
4. To determine whether the results of an election stored on the EMS server, can be altered by any person using a device such as a cell phone wirelessly connected to the EMS server network.
 - a. Any person using a device such as a cell phone wirelessly connected to the EMS server network can change the calculated vote totals on the EMS server.

Examination of wireless vulnerability required that a wireless device be connected to the EMS server network and demonstrated that such a device when connected is capable of allowing uncontrolled access to and alteration of an election database on the EMS server.

The purpose and the finding of Key Objective 4 demonstrates that if such a wireless device were connected to the EMS server network, the election results can be accessed and altered surreptitiously. The ease with which wireless technology can be enabled, even by accident, presents an unacceptable risk to critical infrastructure voting systems, especially when combined with the egregious violations of the VSS and the multiple security failures found in this examination. **Wireless encryption is easy to break,⁷⁶ has been broken, documented and demonstrated online.⁷⁷**

The disabling and mis-configuration of numerous security measures as found in this Examination renders this EMS election system unsafe and utterly insecure. Unauthorized software, multiple violations of VSS and consequently Colorado law and the use of an un-accredited testing laboratory made the certification of this system, and its subsequent use in elections, illegal.

The on-going examination found that security provisions on the election equipment were not restricted by IP address but rather the firewall configuration was programmed to allow any IP address from anywhere in the entire World to access the election records with no more than a single and relatively simple password to protect it.

There is nothing secret or novel about the techniques used to demonstrate direct access, access by a non-DVS computer or iPhone access to the election databases. Software accessible to hundreds of millions of people and openly advertised for free download and use was used to demonstrate the extreme insecurity of the voting system.

⁷⁶ <http://cve.mitre.org/>, supra note 18

⁷⁷ <https://papers.mathyvanhoef.com/ccs2017.pdf>, <http://www.krackattacks.org/>

The reason for the insecure configuration of these critical infrastructure-designated voting systems, in contradiction to the vendor's claims⁷⁸ and the Secretary of State's certification, should be determined through appropriate investigation.

The law requires the retention of election records including system logs but this election system is grossly out of compliance with the law. Combined with the overwriting of log files, the systematic disabling of critical logging and numerous security elements disabled or bypassed, creating a "back-door" for malicious actors, this configuration of the Mesa County, Colorado voting system assures that may not be possible to prove the integrity of any election in which this equipment was used. This voting system is not compliant with the law, should never have been used in an election, and cannot be trusted to provide authenticated, reliable election data in any election.

Nearly every point of examination has revealed the most serious deficiencies in both security and configuration.

The claim that "election systems were not connected to the Internet" has been made, however the use of removable media devices, presence of wireless networking components within DVS components, use of the internet for election results reporting and other functions, and the destruction of and non-retention of critical logs prevent the verification that the system was not connected to the internet. The configuration of logging to ensure overwriting of log data resulted in operating system logs not being retained that may have shown any improper activity, had it occurred. Because of this it is not possible, on the basis of election systems log files (that are required to be retained), to prove election tampering or election integrity.

This failure of the voting system to retain log files that could prove election integrity is a most serious violation of certification requirements. The voting system, having not met election certification requirements, could not have been legally authorized for use in an election.

This report has detailed the following critical discoveries in Mesa County's voting system:

- **Uncertified software installed, rendering the voting system unlawful for use in elections.**
- **Does not meet statutorily mandated Voting System Standards (VSS) and could not have been lawfully certified for purchase or use.**
- **Suffered systematic deletion of election records (audit log files required by Federal and State law to be generated and maintained), which, in combination with other issues revealed in this report, creates an unauditible "back door" into the election system.**
- **Violates Voting Systems Standards ("VSS") which expressly mandate prevention of the ability to "change calculated vote totals." This report documents this non-compliance from the logged-in EMS server, from a non-DVS computer with network access, and from a cell phone (which may be possible if any of the 36 internal wireless devices in voting system components are deliberately or accidentally enabled and a password is obtained).**
- **Mandatory VSS "System auditability" required features are disabled.**
- **Is configured with 36 wireless devices, which represent an extreme and unnecessary vulnerability, and which may be exploited to obtain unauthorized access from external devices, networks, and the Internet.**

⁷⁸ See Appendix A. Compliance Requirements.

CONFIDENTIAL

- Is configured through firewall settings to allow any computer in the world to connect to the EMS server.
- Uses only a Windows password with generic userIDs to restrict and control access.
- contains user accounts with administrative access that share passwords, subverting VSS-required user accountability and action traceability controls.
- Uses a self-signed encryption certificate which exposes the system to the risk of undetected compromise or alteration.

This report does not compromise state secrets or election integrity – that has already been done by these multiple violations of law, multiple failures of the vendor, the Voting System Testing Lab and the Secretary of State's improper certification. Nation-state adversaries already know these vulnerabilities exist; it is only the American people that are unaware. No new vulnerabilities are discovered or disclosed in this report; all of them are previously well known in the industry and to professionals.

Immediately pending elections and the complete lack of election integrity presented by this voting system present an extreme danger to our constitutional republic. With elections beginning on a large scale very soon, with the massive security vulnerabilities, the weakness presented by this uncertifiable Voting System, the abject failure of the Voting System Testing Laboratory with expired accreditation and lack of proper oversight by authorities, remediation of these issues before pending elections is not possible.

This DVS election system has been shown non-compliant with the law and has been shown to be uncertifiable. The use of this system in an election was itself a breach of law, and more importantly a breach of public trust with reckless disregard for the right of a free people to choose their government.

APPENDIX A. COMPLIANCE REQUIREMENTS

Standards for election systems are provided by the Federal Election Commission Voting Systems Standards (VSS) and in Colorado, compliance is required with this standard.

The VSS requires access control to prevent or detect access to election systems, ensure that system functions are executable only in the intended manner and order, provide safeguards to prevent tampering, record and report the date and time of normal and abnormal events, maintain a permanent record of all audit data that cannot be modified or overridden, detect and record every event including an error condition that the system cannot overcome, time-dependent or programmed events that occur without the intervention of the voter or a polling place operator, and to protect the system from intentional manipulation and fraud, among many other requirements.

Federal Election Commission 2002 Voting Systems Standards (VSS)

Specific compliance requirements from the 2002 Voting Systems Standards (VSS) documentation are excerpted in this section. The Standards are contained in 2 volumes which together are several hundred pages long, and are published on the Federal Election Commission website as two PDF documents.

Excerpts in this Appendix are cited by VSS Volume, Section and Page number for reference in the first line of each box, followed by text of the VSS. Discussion of these standards follows outside each text box as appropriate.

APPLICABILITY

VSS V1, 1.6, page 1-13:

The Standards apply to all system hardware, software, telecommunications, and documentation intended for use to:

- Prepare the voting system for use in an election;
- Produce the appropriate ballot formats;
- Test that the voting system and ballot materials have been properly prepared and are ready for use;
- Record and count votes;
- Consolidate and report votes;
- Display results on-site or remotely; and
- Maintain and produce all audit information.

In general, the Standards define functional requirements and performance characteristics that can be assessed by a series of defined tests. Standards are mandatory requirements and are designated by use of the term "shall".

All of these functional requirements are important. In this report we focus on aspects of recording and counting votes. Determination of whether the election management system performed with the accuracy and integrity required by these standards requires the audit information be maintained and preserved in accordance with law. The VSS is applicable the DVS D-Suite systems examined and reported upon in this document and in Report #1.

VSS V1, 2.1, page 2-19:

This section contains standards detailing the functional capabilities required of a voting system.

[...]

- **Overall Capabilities:** These functional capabilities apply throughout the election process. They include Security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunication and data retention.

The VSS is written specifying capabilities required at a high level. Detailed implementation methods are not specified but it is clear, for example, that these topics are not to be ignored.

VSS V1, 2.2, page 2-20:

This section defines required functional capabilities that are system-wide in nature and not unique to pre-voting, voting, and post-voting operations. All voting systems shall provide the following functional capabilities:

- Security;
- Accuracy;
- Error Recovery;
- Integrity;
- System auditability;
- Election management system;
- Accessibility;
- Vote tabulating;

The emphasis on all of these functional capabilities together indicates the serious nature of the requirement in this standard. The declaration by the U.S. Government that these systems are part of the national critical infrastructure further reinforces the importance of these capabilities. "Shall provide" indicates the mandatory nature of the requirement. The implementation of a functional security capability does not mean to apply the weakest possible implementation of security, for example.

DATA RETENTION

VSS V1, 2.2.11, page 2-34:

United States Code Title 42, Sections 1974 through 1974e, states that election administrators shall preserve for 22 months "all records and paper that come into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting." This retention requirement applies to systems that will be used at anytime for voting of candidates for Federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector). Therefore, all systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of 22 months thereafter.

[...]

The appropriate state or local authority must preserve all records that may be relevant to the detection and prosecution of federal civil rights or election crimes for the 22-month federal retention period, if the records were generated in connection with an election that was held in whole or in part to select federal candidates.

This requirement is clear. In discussion of retention of "all records that come into their possession" the burden of understanding what a record is, falls on election administrators. In particular this standard specifies that state or local authority must perform the preservation of all records.

Election Record Definition, Scope and Content

VSS V1, 4.4.3, page 4-84:

In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain:

- a. Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:
 - 1) The source and disposition of system interrupts resulting in entry into exception handling routines;
 - 2) All messages generated by exception handlers;
 - 3) The identification code and number of occurrences for each hardware and software error or failure;
 - 4) Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing.

Other exception events such as power failures, failure of critical hardware component, data transmission errors, or other type of operating anomaly;

Documenting computer interrupts is a very detailed requirement, from a computer science perspective it is considered extreme. In normal operation, logs of computer activity typically do not include this level of detail unless the generation of records (logging) is set to the most verbose level for software debugging,

because the volume of log data generated can be extreme. The specification that these records are generated during diagnostic routines as well as during the counting and tallying of the vote, in the same sentence, is illuminating and indicates that the intention of the VSS is that this most extreme level of record be generated especially in the 4th example listed in this standard.

It is instructive to note that this standard specifically enumerates these requirements within the definition of a record, rather than in the section that specifically addresses security:

- System login;
- System access errors;
- File access errors; and
- Physical violations of security as they occur,

One reason that file access errors are included in this definition is that programming and operational errors can result in the creation of errors in stored data (that manifest in file access errors). Another reason is that intruders were well known at the time this standard was written and before, to attempt to destroy evidence of their activities by deleting audit trail records that might tend to incriminate them. Title 18, Sec. 1030 makes unauthorized access to such a computer system a felony.

In other election cases such as the Antrim, Michigan case it is notable that while records of previous elections were preserved and still on the election system, the audit records from the 2020 election were missing; the fact that records were generated and preserved previously but suddenly stopped during a specific event where malfeasance is suspected is significant and indicative of the practice by intruders to delete any record of their activity.

Astronomer Cliff Stoll became famous as an early computer crime investigator and published a book entitled "The Cuckoo's Egg" in which he recognized that computers don't make mistakes – programmers do. As a consequence, he looked at the very records regarding exception handling and errors that are required in this standard, because accounting software on the computer he managed as a grad student reported a 25-cent error in accounting data. Cliff's curiosity and persistence resulted in the discovery of a computer attack where the intruder tried to delete audit records that resulted in the error. The investigation ultimately revealed international espionage and attacks against the US Government that would have gone unnoticed without his analytical search for what he initially assumed was a programming error. As a pattern of evidentiary finding, this history is very useful in understanding computer crime and criminal behavior.

This inclusion of these security-specific requirements in this basic but over-arching definition indicates their importance and that the intent of the standard is for great detail in the generation of these specific security audit records.

Security Requirements for Voting Systems

VSS V1, 6.1, page 6-93:

[...]

Ultimately, the objectives of the security standards for voting systems are:

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized;
- To protect the system from intentional manipulation and fraud, and from malicious mischief;
- To identify fraudulent or erroneous changes to the system; and
- To protect secrecy in the voting process.

The Standards are intended to address a broad range of risks to the integrity of a voting system. While it is not possible to identify all potential risks, the Standards identify several types of risk that must be addressed by a voting system. These include:

- Unauthorized changes to system capabilities for:
 - Defining ballot formats;
 - Casting and recording votes;
 - Calculating vote totals consistent with defined ballot formats; and
 - Reporting vote totals;
- Alteration of voting system audit trails;
- Changing, or preventing the recording of, a vote;
- Introducing data for a vote not cast by a registered voter;
- Changing calculated vote totals;
- Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals; and
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.

This standard is also clear. The first three bullets in the list of objectives are related as previously explained, because intentional manipulation, fraud, malicious mischief and fraudulent or erroneous changes to the system often manifest in records that appear initially to have been accidents, inadvertent mistakes and errors.

The failure of security identified in this report specifically permitted unauthorized changes to the recording of votes in a database, as components of the database that should have been protected were allowed to be altered. A more difficult to find alteration might involve the changing of ballot formats so that a vote for one candidate appeared as a vote for a different candidate, but the access granted by the failure of security access controls allowed full administrative access to the database. The changing of calculated vote totals was specifically demonstrated by the tests in this examination. The data values changed essentially mean "Trump's votes are stored here -> X" and "Biden's votes are here -> Y" and the test switched X and Y.

As presented in Report #1, audit trails were altered (deleted) because the specifically enumerated risk was not addressed as required by this standard.

VSS V1, 6.2, page 6-96:

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability confidentiality and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss, or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

Access control capability was built into the EMS server operating system and into the SQL DBMS but not programmed to be secure and one most egregious finding was that the EMS server was specifically configured to be insecure in defiance to the requirements in this standard and every known industry, government and security best practice, the standards of the National Institute of Standards and Technology (which chaired the committee that produced the VSS), and the DoD Security Technology Implementation Guides.

VSS V1, 6.2.2, page 6-97:

Vendors shall provide a detailed description of all access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples include:

- a. Use of data and user authorization;
- b. Program unit ownership and other regional boundaries;
- c. One-end or two-end port protection devices;
- d. Security kernels;
- e. Computer-generated password keys;
- f. Special protocols;
- g. Message encryption; and
- h. Controlled access security.

Vendors shall also define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.

This standard requires a detailed description to be provided by the voting system vendor, but clearly expects these functional protections to be implemented if the measures are to be documented.

DVS stated on their website⁷⁹ that they are compliant with voting systems standards, including the Voluntary Voting Systems Guidelines (VMSG) as shown in Figure 66. A review of the VSTL test-related documents reveals that the standards tested against were the VMSG standards. By comparing the test plans and reports to the requirements in the VMSG, this is easily assessed.



Dominion Voting Systems is committed to ensuring the security of elections.

We utilize both voluntary and compulsory testing on every one of our systems as part of company and federal/state certification processes. Our Democracy Suite products have been tested and certified by the U.S. Election Assistance Commission (EAC) in accordance with federal Voluntary Voting Systems (VMSG).

Figure 66 - DVS Compliance Statement

The Voluntary Voting Systems Guidelines (VMSG) contain even more explicit and precise definitions of the logging required than do the VSS, and although these are Guidelines that are not explicitly required under Colorado law, DVS makes the claim on their website that they are compliant with them. The 2005 VMSG were a defacto standard for the security of election systems and have been revised several times. The 2005 VMSG specifically requires in section 2.1.5.1 that a number of safeguards and operational requirements be applied. The VMSG excerpt below is *only a small partial list of those requirements*, but for this examination, the finding of key compliance issues is noted in Red following each requirement:

- a. Voting system equipment shall record activities through an event logging mechanism.
FAIL. Log mechanism does exist and records some, but not all activities, even though it overwrites and destroys those records frequently. Logging is not only incomplete but is wholly inadequate.
- b. Voting system equipment shall enable file integrity protection for stored log files as part of the default configuration.
FAIL. Not only have log files not been preserved, but they have been overwritten as indicated in Report #1. Further, the log file size has been set to a very small limit such that the log data is NOT preserved and cannot be recovered historically. Integrity Protection for these log files is not implemented.
- c. The voting system equipment logs shall not contain information that, if published, would violate ballot secrecy or voter privacy or that would compromise voting system security in any way.
FAIL. The log files that remain contain very little information of value in determining the integrity of the election at all; no information was found in the logs that can violate the secrecy of ballots or voter privacy, or that would compromise voting system security, but critical Audit Log data has been deleted (overwritten and in some cases its collection disabled) that is required for an Audit of the system's security, integrity, accuracy, that would identify errors, malicious actions, illegal tampering with ballots and vote totals, intrusions, what programs

⁷⁹ This statement was present on Dominion Voting Systems' website in September, 2020 and has since been removed, however the claim that they comply with voluntary VMSG standards brings this into relevance.

were run, by whom, and their results. Contrary to the law, this is not in compliance – it is just the opposite: voting system security is compromised by the inability to detect malicious activity.

- d. The voting system equipment shall log at a minimum the following data characteristics for each type of event: 1) system ID; 2) unique event ID and/or type; 3) timestamp; 4) success or failure of event, if applicable; 5) User ID trigger the event, if applicable; 6) Resources requested, if applicable.

FAIL. The EMS system does not record this information and in most cases has been configured by the Manufacturer to not log this information.

- e. Voting system equipment shall log all events, including abnormal events.

FAIL. The disabling of logging and the overwriting of log files above a certain size prevent the logging of all events.

- f. Voting system equipment shall ensure that event logging cannot be disabled. Voting system equipment shall implement default settings for secure log management activities, including log generation, transmission, storage, analysis and disposal.

FAIL. The design and configuration of this voting system provides exactly the opposite. Logging has been disabled by design and by the misconfiguration of the operating system such that the required and necessary records are NOT stored.

- g. Voting system equipment shall log clearing of logs and log rotation.

FAIL. The EMS system does not log the clearing of logs or log rotation, nor the overwriting of files (an act of “clearing the logs”). No record of log rotation could be found. In Report #1, the vendor DVS not only overwrote the operating systems and all log data with its “Trusted Build” installation, it designed the installation process to re-format and re-partition the hard disk ensuring that this occurred.

Of particular importance are sections b, d, e, f and g above. Had they been implemented properly and in accordance with the standards as Dominion claims and Customers expect, these log data would have supported conclusions regarding the integrity or the lack of integrity of the election. In both Antrim and Maricopa investigations, the DVS software did not log each modification to each record. Per the VSS, this detail of logging should be not only performed, but retained for 22 months (25 months in Colorado).

Even the Center for Internet Security (CIS) recognizes the need for these controls, among many others, in their Handbook for Election Infrastructure Security.⁸⁰

Given the failure to implement these required and recommended controls, the DVS Democracy Suite version 5.11-CO as provided to the State of Colorado does not possess the required integrity controls as claimed by DVS and required by law. From the evidence presented in this report, this failure of integrity safeguards means that elections held in Colorado using this equipment do not possess the integrity to protect the vote from tampering, or to record access to or modification of the vote.

⁸⁰ <https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf>

APPENDIX B. DATABASE FUNDAMENTALS

This report addresses computerized databases. This Appendix provides a basic understanding of the terms and technology involved to support the reader's understanding of findings in this report.

The voting systems used in Mesa County, Colorado are made by DVS. Many of these voting systems are comprised of an industry-standard computer that uses a Microsoft operating system and Dominion application software that provides a foundation for election related functions including capturing and storing the election data in a database management system, tabulating and counting the vote.

The Mesa County Election Management System (EMS) server runs on the Microsoft Windows Server 2016 operating system, and it employs a database management system known as Microsoft SQL Server. The security of the system depends largely upon the proper configuration of the Operating System and the SQL Server.

There are several types of databases, including relational, non-relational, and object-oriented databases. This discussion will be limited to relational databases because this is the type of database used in the Dominion voting system that is the subject of this forensic examination.

Microsoft SQL Server is a Database Management System (DBMS). A DBMS can contain many databases. Within this Mesa County, Colorado EMS server DBMS are many databases from prior elections, in addition to the 2020 General Election. Each database consists of many tables that can have different purposes. Some are administrative (access permissions for example), some are necessary for the DBMS to function (such as the database of databases, necessary because a DBMS can have multiple databases), and some have operational content related to the purpose of the database. This information is contained in multiple Tables consisting of multiple columns (and multiple rows if not empty). The database of databases (referred to as the DBDB) identifies the users, access permissions, the identity of each table that is contained within each respective database, among other items.

The fundamental components of a relational database are Tables, Rows and Columns. Data are organized in tables. Columns within a table contain specific data types, for example, first name, last name, street address, city, state, etc. Rows within a table each contain an instance of the data, referred to in database science as a tuple. The database is called a relational database because the various tables are *Related* by what is known as a KEY value. The Key value exists in multiple tables and is the item that links or *relates* the data in one table to the data in another table. For example, in a voter database, one reasonable KEY value might be Ballot Number – it would exist in all the associated tables and it becomes possible to retrieve ALL the data about a particular ballot by searching for every row where ballot number equals, for example, 300.

One primary purpose of a database is to return data in response to a request for that data, called a Query. One of the most common computer languages used in modern relational databases is the Structured Query Language (SQL). Structured query language is intended to be readable and understood easily.

An example of an SQL-like query might be to find the address of a person in a database table called "Addresses". Such a query might look like:

```
RETRIEVE(Addresses) address.street.address, address.city, address.state where first.name="John"  
and last.name="Smith"
```

IF the database table has an entry for John Smith, the above query would return the Street Address, City and State for him, *provided that* the user of this database had permission to read this specific Addresses table. While there is a specific order (syntax) for the components of the database command (e.g., a format), the commands are not difficult to understand, and the example here, while similar, is simplified to make it very understandable.

A DBMS implemented in software known as *Microsoft SQL Server* is addressed in this document because it is the DBMS installed and used in the Mesa County Colorado Election Management System server. The function of a DBMS is to organize its tables and rows, to provide a very granular set of permissions to the users of the database, to provide the integrity of the data – specifically to ensure that data cannot be inappropriately altered or deleted, and to control the four basic functions of the database. Four basic functions are implemented in relational databases, with respect to the data contained in its table-rows. Those basic functions are read, write, modify, and delete. The DBMS also supports various types of calculations based on the data in its tables.

One of the features of a DBMS is to very granularly control the permissions within a database. For example, a user might have permission to change the street address within a row, but not be allowed to change the city or state. Normal computer system permissions *without* a DBMS give the user permission to access the entire data set (for example, within a spreadsheet). Thus, the permission settings (e.g., configuration) of a DBMS are critical to its proper functioning and the ability to maintain integrity of the data within the database. These permission settings control who can perform which transactions.

Permissions within a well-controlled database specify which users can read which tables, which users can add data to the table, which users can modify (or update) data in the table, and which users can delete data in a table. Most commonly only the DBMS administrator has all four permissions for any table. It is common for an average user to be able to read and perhaps add data to a table, while changing or deleting data requires a supervisor to perform the task. A computer program (or task) can be assigned permission in the same manner that a user can be, sometimes by creating a user-id that is used only by the program.

There are special tables within a database that are highly restricted. These special tables include the DBDB within the DBMS, the User table within each database, the permissions for each user to each database and database table, and in some cases, the permissions for each user to the columns within each table. These special tables define how the DBMS operates.

It is required that a particular user within a DBMS only be able to alter the data with good reason. One example might be the case of a changed vote. Let's consider, for example, a hand-marked ballot, for simplicity, identified as ballot #300. The identity of the voter is not associated with the ballot number so it is accessed only by its number. The ballot contains circles or squares to be marked to indicate a vote. However, if the ballot marking is not within the lines (within limits), the ballot is marked for adjudication so that a human can then take steps to determine the voter's intent and then store that entry in the database. In this example, the original vote (and the photographic image of the ballot) might be stored in a database table called PendingAdjudication (the table name is an example to illustrate the technology). The Adjudication user should be able to read the data in the PendingAdjudication table, but not change or delete it. The user looks at the ballot image and makes their determination of voter intent and the results are written to a separate table called AdjudicatedVote. The user then has permission to change the value of ONE COLUMN within the PendingAdjudication table (for the specific data row) to indicate Adjudicated or

CONFIDENTIAL

NotAdjudicated. The point of the example is that even in this case, the original data is not deleted, and a separate database table is used to compile the data. The Adjudication user in this example NEVER changes the original data, but the vote that is counted is in the AdjudicatedVote table. Thus, an audit of the complete voter database should show that there is one, and only one, entry for ballot #300, and the decision of the auditor should be available for review and the actions taken should be traceable. A more complex design may even use a separate table all-together to track which items are adjudicated or not.

The design of the database must make sense. In the example above, if the Adjudicator were to be permitted to change the original vote in the PendingAdjudication table, the ability to review their decision would be lost and there would be no way to audit the change, without seeing the before- and after- results. Thus, not only must the configuration of permissions enable those necessary changes but it must protect the integrity of the data and support the ability of the system to be auditable.

There is much not discussed here. For example, the DBMS in a voting application would be expected to check the PendingAdjudication table to make sure that every ballot that was sent to be adjudicated HAD BEEN processed, and that there were no rows with NotAdjudicated remaining, before the tabulation and count of votes had been finalized.

The design of the database and its permissions are only part of the logic required to make such a system work properly. As with the check above to ensure that all votes were adjudicated, there is much additional logic, which should be found within the database processing workflow, to ensure the proper calculations and integrity are maintained throughout the entire voting process.

APPENDIX C. IP ADDRESSING FUNDAMENTALS

There are two versions of Internet Protocol addressing seen in this data. The legacy version of addressing is expressed by four one- to three-digit numbers separated by periods – “X.X.X.X,” where X is an 8-bit number (e.g., has a value of 0-255). Because industry and users throughout the world have exceeded the number of available address numbers, a new address scheme was developed. The legacy address scheme is known as IP version 4 (IPv4) and is 32 binary bits long, while the new scheme is known as IP version 6 (IPv6) and is 128 binary bits long, represented as 8 groups of 4 hexadecimal values (0-9 and A-F) separated by periods (A.B.C.D.E.F.G.H). This solves the problem of running out of IPv4 addresses and provides, by one estimate, more than 1,500 IP addresses for every square meter of Earth’s surface. This explanation is provided because both types of addresses are present in this forensic analysis and it is necessary for the reader to understand the data being presented.

In Figure 8, IP2 shows the IPv4 address 192.168.100.10, the address assigned to be used by the Mesa County EMS server. IP1 shows the IPv6 address FE80::792B:3E74:DF1B:C565%5. This translates to FE80:0000:0000:792B:3E74:DF1B:C565 (the double colon stands for repeated 0 address values), and “zone” 5 (%5) which is essentially the identifier that indicates which IP Network Interface Card (NIC) the address is tied to. While these data reflect the interface capability of the Oracle VirtualBox environment, the IP Address 192.168.100.10 is configured in the stored operating system and when launched here, automatically assumed the same IP address. IPv6 is addressed here for completeness.

The IPv4 address used (192.168.x.x) is a “Private Network” address per Internet Standard RFC-1918 and is NOT directly routable across the Internet. However, firewalls, routers and other network devices use a service called Network Address Translation (NAT) or Port Address Translation (PAT) to convert these private addresses to publicly routable addresses and allow them to be transmitted over the larger Internet. Thus, the use of a private network address assigned to a particular Ethernet interface does not in itself, prevent the computer from accessing the Internet – it becomes necessary to examine all routers, firewalls and other networking equipment to determine whether the computer is capable of *direct* connection to the Internet via a translation mechanism such as NAT or PAT.

For every IPv4 address, the number is split into two parts – the first part of the number is the Network Address and the second part of the number is the Device Address. This is defined by the number of bits assigned to the network address and follows the IP address and a slash “/.” “192.168.100.0/24” indicates the first 24 bits of this binary number constitutes the Network Address and the remaining 8 bits constitute the Device Address. This set of Device Addresses is referred to as a Subnet. For data to leave a subnet, the subnet must have a Default Gateway assigned. When a computing device sends data to an address that is outside the Subnet group of addresses, it sends that data to the Default Gateway address which then *routes* the data onward to its destination.

There are two special Device Addresses: the first value in the Device Address is used to specify the Network Address while the last address in the subnet range is defined as a Broadcast Address and is used to send data to every device in the Subnet. In the address example “192.168.100.0/24,” the first address is 0 and is the Network Address is 255; a broadcast to all 254 device addresses possible on this subnet would be sent to “192.168.100.255.” The first usable address of this subnet is “192.168.100.1,” which is typically used for the Default Gateway address.

CONFIDENTIAL

The IPv6 address used (FE80:x:x:x:x:x:x) is a *link-local* address, which means that it is also not routable across the Internet. The concept of NAT and PAT are not used in IPv6, *with the single exception of using it to translate IPv6 addresses to IPv4 addresses and vice versa* because not all network equipment is capable of using IPv6 (yet). Some legacy network equipment widely in use today is not capable of transporting IPv6.

This link-local (FE80) address is not routable and is not supposed to be translatable from IPv6 to IPv4 and vice versa, however this depends on whether a particular network device vendor has followed the standard when implementing their software. While most vendors have designed their devices properly (network devices would not work properly otherwise), from a scientific and evidentiary perspective, it still remains necessary to forensically examine all connected network devices to ensure that these addresses cannot reach the Internet.

APPENDIX D. NATION-STATE CYBER ATTACK CAPABILITIES

Introduction

The mere idea of advanced Nation-State cyberwarfare capabilities at first blush seems like fantasy straight out of a James Bond film. Yet these attack capabilities are the most sophisticated on the planet. Most countries, including the USA, consider their defensive and offensive cyberwar capabilities to be highly classified. In the USA these are implemented by the National Security Agency, specifically in its Tailored Access Operations (TAO) group according to numerous reports, and in the UK, by the CGHQ. In this appendix, a short synopsis (and bibliography) of several of the more sophisticated cyberattacks are presented, *in particular in support of statements made elsewhere in this document*—specifically, that attacks occur *extremely quickly*, that a USB Thumb Drive can be infected with malicious software which can then infect other computer systems, and that cyberattacks can cause considerable damage. This is a very small sampling of some of the more sophisticated attacks but is illustrative of the advanced sophistication and the pervasive nature of vulnerabilities.

Security experts in the USA also understand and have documented issues with Voting Systems security, in *this report* <https://archive.org/details/6432002-Voting-Village-Report-defcon27/page/n15/mode/2up>. This security conference (Defcon 2019) is often billed as a “hacker” conference, however some of the most renowned security professionals in the world attend it, and the “Voting Village” at Defcon, in the referenced report, is co-chaired by Matt Blaze, Professor of Law and McDevitt Chair for the Department of Computer Science, Georgetown University (and author of many books on the subject). Christopher Krebs, Director of the US Critical Infrastructure Security Agency (CISA) also attended.

In 1984, while working at Bell Telephone Laboratories, I witnessed one of the very first destructive computer viruses. In that era, computer monitors used standard NTSC television signals to present video on a large cathode ray tube “tv screen”. The monitor used a very high voltage (tens of thousands of volts) to cause the electron beam to display a picture. To generate the high voltage, the monitor used a “flyback” transformer, a specific type of high-frequency transformer commonly found in televisions, that took advantage of the 15,575 hertz horizontal scan signal that is part of the NTSC standard video signal. This signal was amplified and fed the primary winding of the transformer. It was found that the video driver circuit card in primitive ‘PCs’ of that era allowed the frequency of the horizontal scan signal to be programmed. When that frequency was programmed to 0 hertz, the electric current through the primary winding of the transformer changed from a rapidly varying signal to a constant “on” state. Since this state exceeded the capability of the transformer, it burned the transformer out, destroying the monitor.

In 2007, DHS and the Idaho National Laboratory ran the Aurora Generator Test to demonstrate vulnerabilities in the electric power grid in the USA.⁸¹ A leaked video⁸² of the attack is widely available on the Internet and shows the complete destruction of a 27 ton, 2.25MW generator by a cyberattack. In this attack, the attackers (part of the US Military) opened the relays of the generator (by remote computer control) long enough for the generator to slip out of synchronization with the power grid, and then reconnected the relays, causing a catastrophic mechanical jolt to the generator. This is the equivalent of driving your car at 70 mph, and while moving at that speed, placing your car into reverse gear. They did

⁸¹ https://en.wikipedia.org/wiki/Aurora_Generator_Test

⁸² <https://youtu.be/LM8kLaJ2NDU>

this three times, as is apparent from the video. The third time was “the charm” as the generator’s diesel engine self-destructs and the room as well as the external exhaust pipe fill with black smoke. The article cited⁸³ includes both the video of the test showing destruction of the generator as well as the original DHS report, released under FOIA.

Adversaries constantly scan and probe every computer on the internet to identify weakness well in advance of the need for an attack. A commercial (i.e., unclassified) example of this scanning is demonstrated by the company Lumeta. During the first Gulf War, noted security expert Bill Cheswick, co-founder of Lumeta, used a common troubleshooting tool (ping) and was able to perform real-time battle-damage assessment by detecting computers that went offline due to active bombing campaigns. Adversaries have discovered their targets well in advance and have pre-programmed attacks ready to launch.

Moonlight Maze

“Moonlight Maze was a 1999 US government investigation into a massive data breach of classified information. It started in 1996 and affected NASA, the Pentagon, military contractors, civilian academics, the DOE, and numerous other American government agencies. By the end of 1999, the Moonlight Maze task force was composed of forty specialists from law enforcement, military, and government. The investigators claimed that if all the information stolen was printed out and stacked, it would be three times the height of the Washington Monument, which is 555 ft (169 m) tall. The Russian government was blamed for the attacks, although there was initially little hard evidence to back up the US accusations besides a Russian IP address that was traced to the hack. Moonlight Maze represents one of the first widely known cyber espionage campaigns in world history. It was even classified as an Advanced Persistent Threat (a very serious designation for stealthy computer network threat actors, typically a nation state or state-sponsored group) after two years of constant assault. Although Moonlight Maze was regarded as an isolated attack for many years, unrelated investigations revealed that the threat actor involved in the attack continued to be active and employ similar methods until as recently as 2016.”⁸⁴

Stuxnet

Stuxnet was an offensive operation, believed to be conducted by the USA and Israel,⁸⁵ to destroy nuclear enrichment centrifuges at Iran’s Natanz enrichment facility,⁸⁶ About 1,000 centrifuges were involved in the enrichment of ‘yellow.cake’ uranium from “fuel grade” for commercial power reactors to “weapons grade” to create nuclear weapons (bombs/missiles).

“Stuxnet was a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran. This worm was an unprecedentedly masterful and malicious piece of code that attacked in three phases. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers. The worm’s authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant.”

⁸³ <https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/>

⁸⁴ https://en.wikipedia.org/wiki/Moonlight_Maze

⁸⁵ <https://www.jpost.com/International/Snowden-US-Israel-created-virus-to-destroy-Iran-nukes-319226>

⁸⁶ <https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/>

“Stuxnet could spread stealthily between computers running Windows—even those not connected to the Internet. If a worker stuck a USB thumb drive into an infected machine, Stuxnet could “worm” its way onto it, then spread onto the next machine that read that USB drive. Because someone could unsuspectingly infect a machine this way, letting the worm proliferate over local area networks, experts feared that the malware had perhaps gone wild across the world.”

“In October 2012, U.S. defense secretary Leon Panetta warned that the United States was vulnerable to a “cyber–Pearl Harbor” that could derail trains, poison water supplies, and cripple power grids. The next month, Chevron confirmed the speculation by becoming the first U.S. corporation to admit that Stuxnet had spread across its machines.”⁸⁷

Operation Titan-Rain

Titan Rain was a series of coordinated computer attacks⁸⁸ on the United States that began in 2003 and originated from Guangdong, China. The attacks are believed to have come from the People’s Liberation Army unit 61398, located at the Lingshui Signals Intelligence Unit on Hainan Island, one of China’s largest military facilities in the South China Sea. This is the same unit responsible for the attack on the Wall Street Journal, which cyber forensics company Mandiant identified as APT-1 (Advanced Persistent Threat–1)⁸⁹.

“An advanced persistent threat (APT) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals.”⁹⁰

Titan Rain is rumored to have stolen as much as 40 Terabytes of US Government secrets. This attack persisted for many years.

Operation Aurora

Operation Aurora was conducted by the People’s Liberation Army of China from mid-2009 through December, 2009.⁹¹

It was a very large scale attack that affected numerous commercial entities including Google, Morgan-Stanley, Adobe Systems, Akamai Technologies, Juniper Networks, and Rackspace who have publicly confirmed that they were targeted. According to reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical were also among the targets. The unit which conducted the attack has been named APT-17.

“The attack was named ‘Operation Aurora’ by Dmitri Alperovitch, Vice President of Threat Research at cybersecurity company McAfee. Research by McAfee Labs discovered that ‘Aurora’ was part of the file path on the attacker’s machine that was included in two of the malware binaries McAfee said were associated

⁸⁷ <https://spectrum.ieee.org/the-real-story-of-stuxnet>

⁸⁸ https://en.wikipedia.org/wiki/Titan_Rain

⁸⁹ <https://www.lawfareblog.com/mandiant-report-apt1>

⁹⁰ https://en.wikipedia.org/wiki/Advanced_persistent_threat

⁹¹ https://en.wikipedia.org/wiki/Operation_Aurora

with the attack. "We believe the name was the internal name the attacker(s) gave to this operation," McAfee Chief Technology Officer George Kurtz said in a blog post."

"According to McAfee, the primary goal of the attack was to gain access to and potentially modify source code repositories at these high-tech, security, and defense contractor companies. '[The software configuration management systems] were wide open,' says Alperovitch. 'No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways—much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting.' "

2020 US Government Attack

In 2020, a massive nation-state attack against many companies and US Government organizations took place.⁹² Initially only the Treasury department and the NTIA were thought to have been attacked. But it turned out that many of the US Government operations including the IRS and even the US Administrative Office of the Courts (which relies heavily on the software SolarWinds) were compromised.

This attack was a supply-chain attack. SolarWinds, a network management system, as many software firms do, periodically releases updates to its software. SolarWinds was broken into and one of its update programs was infected with malware. Because SolarWinds was inappropriately assigned too much trust by its customers, their software updates were white-listed (allowed through the firewall, unchallenged). The attack was in the update.

This is widely regarded as one of the worst attacks in US history for the length of time it lasted (9 months) before detection as well as the impact it had upon affected organizations.

Summary

Nation-States including Russia, China, North Korea, Malaysia, Iran and many others seek to attack the USA's national security, economic, industrial, communications, and financial systems. These attackers are extremely sophisticated and well trained. For example, North Korea has an institute in Pyongyang that teaches cyberwarfare and has been turning out more than 100 graduates every month for well over 15 years. Other Nation-States, including Iran, have sent students to North Korea's school.

This brief history has documented the sophistication of advanced cybersecurity attacks.

Multiple references show that sophisticated attacks can occur by transfer through USB drives, without being detected by the end user.

This history shows how unprotected system configurations have enabled advanced cyberattacks, and how software updates can infiltrate a company's IT operations and take control.

⁹² https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach.

APPENDIX E. SECURITY CONSIDERATIONS FOR SQL SERVER INSTALLATIONS

The following information was taken directly from Microsoft documentation and is provided here to be a reference to basic security considerations related to installations of Microsoft SQL Server. This is relevant as Microsoft SQL Server is the product used in the Dominion EMS.

From Microsoft SQL Server Documentation:

Security is important for every product and every business. By following simple best practices, many security vulnerabilities can be avoided. Below are some security best practices that should be considered both before installing SQL Server and after SQL Server has been installed. Security guidance for specific features is included in Microsoft reference articles for those features.

Before Installing SQL Server:

- Follow these best practices when setting up the server environment:
- Enhance physical security
- Use firewalls
- Isolate services
- Configure a secure file system
- Disable NetBIOS and server message block

Details about these items are provided below.

Enhance Physical Security

Physical and logical isolation make up the foundation of SQL Server security. To enhance the physical security of the SQL Server installation, do the following tasks:

- Place the server in a room accessible only to authorized persons.
- Place computers that host a database in a physically protected location, ideally a locked computer room with monitored flood detection and fire detection or suppression systems.
- Install databases in the secure zone of the corporate intranet and do not connect your SQL Servers directly to the Internet.
- Back up all data regularly and secure the backups in an off-site location.

Use Firewalls

Firewalls are important to help secure the SQL Server installation. Firewalls will be most effective by following these guidelines:

- Put a firewall between the server and the Internet. Enable your firewall. If your firewall is turned off, turn it on. If your firewall is turned on, do not turn it off.
- Divide the network into security zones separated by firewalls. Block all traffic, and then selectively admit only what is required.
- In a multi-tier environment, use multiple firewalls to create screened subnets.
- When you are installing the server inside a Windows domain, configure interior firewalls to allow Windows Authentication.

Isolate Services

Isolating services reduces the risk that one compromised service could be used to compromise others. To isolate services, consider the following guidelines:

- Run separate SQL Server services under separate Windows accounts. Whenever possible, use separate, low-rights Windows or Local user accounts for each SQL Server service.

Configure a Secure File System

Using the correct file system increases security. For SQL Server installations, you should do the following tasks:

- Use the NTFS file system (NTFS). NTFS is the preferred file system for installations of SQL Server because it is more stable and recoverable than FAT file systems. NTFS also enables security options like file and directory access control lists (ACLs) and Encrypting File System (EFS) file encryption. During installation, SQL Server will set appropriate ACLs on registry keys and files if it detects NTFS. These permissions should not be changed. Future releases of SQL Server might not support installation on computers with FAT file systems.
- Use a redundant array of independent disks (RAID) for critical data files.

Disable NetBIOS and Server Message Block

Servers in the perimeter network should have all unnecessary protocols disabled, including NetBIOS and server message block (SMB).

NetBIOS uses the following ports:

- UDP/137 (NetBIOS name service)
- UDP/138 (NetBIOS datagram service)
- TCP/139 (NetBIOS session service)

SMB uses the following ports:

- TCP/139
- TCP/445

During or After Installation of SQL Server

After installation, you can enhance the security of the SQL Server installation by following these best practices regarding accounts and authentication modes:

Service accounts

- Run SQL Server services by using the lowest possible permissions.
- Associate SQL Server services with low privileged Windows local user accounts, or domain user accounts.

Authentication mode

- Require Windows Authentication for connections to SQL Server.
- Use Kerberos authentication.

Strong passwords

- Always assign a strong password to the sa [system administrator] account.
- Always enable password policy checking for password strength and expiration.
- Always use strong passwords for all SQL Server logins.

References:

<https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-sql-server-installation?view=sql-server-ver15>

<https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-sql-server-installation?view=sql-server-2016>

APPENDIX F. C.R.S. 1-5-608.5

1-5-608.5. Electronic and electromechanical voting systems - testing by federally accredited labs - certification and approval of purchasing of electronic and electromechanical voting systems by secretary of state - conditions of use by secretary of state - testing.

(1) A federally accredited laboratory may test, approve, and qualify electronic and electromechanical voting systems for sale and use in the state of Colorado.

(2) (Deleted by amendment, L. 2009, (HB 09-1335), ch. 260, p. 1190, § 4, effective May 15, 2009.)

(3)

(a) If the electronic and electromechanical voting systems tested pursuant to this section satisfy the requirements of this part 6, the secretary of state shall certify such systems and approve the purchase, installation, and use of such systems by political subdivisions and establish standards for certification.

(b) The secretary of state may promulgate conditions of use in connection with the use by political subdivisions of electronic and electromechanical voting systems as may be appropriate to mitigate deficiencies identified in the certification process.

(c) In undertaking the certification required by this section, the secretary of state may consider either procedures used or adopted by county clerk and recorders or best practices recommended by equipment vendors.

(3.5)

(a) [Editor's note: Subsection (3.5) is effective July 1, 2022.] On and after December 31, 2022, if an electronic and electromechanical voting system tested pursuant to this section satisfies the requirements of this part 6 related to the use of the system in an election using instant runoff voting and the rules established by the secretary of state pursuant to section 1-5-616 (1.5), the secretary of state shall certify such system and approve the purchase, installation, and use of such system by political subdivisions in an election using instant runoff voting.

(b) The secretary of state may promulgate conditions of use in connection with the use by political subdivisions of an electronic and electromechanical voting system in an election using instant runoff voting as may be appropriate to mitigate deficiencies identified in the certification process.

(c) In undertaking the certification required by this section, the secretary of state may consider procedures used or adopted by county clerk and recorders or best practices recommended by equipment vendors.

(4) In undertaking the certification required by this section, the secretary of state may request a federally accredited laboratory to undertake the testing of an electronic or electromechanical voting system or may use and rely upon the testing of an electronic or electromechanical voting system already performed by another state or a federally accredited laboratory upon satisfaction of the following conditions:

(a) The secretary of state has complete access to any documentation, data, reports, or similar information on which the other state or laboratory relied in performing its testing and will make such information available to the public subject to any redaction required by law; and

CONFIDENTIAL

(b) The secretary of state makes written findings and certifies that he or she reviewed the information specified in paragraph (a) of this subsection (4) and determines that the testing:

(I) Was conducted in accordance with appropriate engineering standards in use as of the time the testing is undertaken; and

(II) Satisfies the requirements of sections 1-5-615 and 1-5-616 and all rules promulgated thereunder.

(5) In undertaking the certification required by this section, the secretary of state may conduct joint testing with an agency of another state or with a federally accredited laboratory.

History

Source: L. 93:Entire section added, p. 1414, § 57, effective July 1. L. 2004:Entire section amended, p. 1346, § 13, effective May 28. L. 2009:Entire section amended,(HB 09-1335), ch. 260, p. 1190, § 4, effective May 15. L. 2021:(3.5) added,(HB 21-1071), ch. 367, p. 2416, § 3, effective July 1, 2022.

Research References & Practice Aids

Hierarchy Notes:

C.R.S. Title 1

C.R.S. Title 1, Art. 5

State Notes

Research References & Practice Aids

Cross references:

For the legislative declaration contained in the 2004 act amending this section, see section 1 of chapter 334, Session Laws of Colorado 2004.

Colorado Revised Statutes Annotated

Copyright © 2022 COLORADO REVISED STATUTES All rights reserved.

APPENDIX G. C.R.S. 1-5-615

1-5-615. Electronic and electromechanical voting systems - requirements.

(1) The secretary of state shall not certify any electronic or electromechanical voting system unless such system:

(a) Provides for voting in secrecy;

(b) Permits each elector to vote for all offices for which the elector is lawfully entitled to vote and no others, to vote for as many candidates for an office as the elector is entitled to vote for, and to vote for or against any ballot question or ballot issue on which the elector is entitled to vote;

(c) Permits each elector to verify his or her votes privately and independently before the ballot is cast;

(d) Permits each elector privately and independently to change the ballot or correct any error before the ballot is cast, including by voting a replacement ballot if the elector is otherwise unable to change the ballot or correct an error;

(e) If the elector overvotes:

(I) Notifies the elector before the ballot is cast that the elector has overvoted;

(II) Notifies the elector before the vote is cast that an overvote for any office, ballot question, or ballot issue will not be counted; and

(III) Gives the elector the opportunity to correct the ballot before the ballot is cast;

(f) Does not record a vote for any office, ballot question, or ballot issue that is overvoted on a ballot cast by an elector;

(g) For electronic and electromechanical voting systems using ballot cards, accepts an overvoted or undervoted ballot if the elector chooses to cast the ballot, but it does not record a vote for any office, ballot question, or ballot issue that has been overvoted;

(h) In a primary election, permits each elector to vote only for a candidate seeking nomination by the political party with which the elector is affiliated;

(i) In a presidential election, permits each elector to vote by a single operation for all presidential electors of a pair of candidates for president and vice president;

(j) Does not use a device for the piercing of ballots by the elector;

(k) Provides a method for write-in voting;

(l) Counts votes correctly;

(m) Can tabulate the total number of votes for each candidate for each office and the total number of votes for and against each ballot question and ballot issue for the polling location;

(n) Can tabulate votes from ballots of different political parties at the same voter service and polling center in a primary election;

CONFIDENTIAL

(o) Can automatically produce vote totals for the polling location in printed form; and

(p) Saves and produces the records necessary to audit the operation of the electronic or electromechanical voting system, including a permanent paper record with a manual audit capacity.

(1.5) [Editor's note: Subsection (1.5) is effective July 1, 2022.] The secretary of state shall not certify any electronic or electromechanical voting system for use in an election using instant runoff voting unless, in addition to meeting the requirements of subsection (1) of this section, the system meets the requirements and performs the functions required by section 1-7-1003.

(2) The permanent paper record produced by the electronic or electromechanical voting system shall be available as an official record for any recount conducted for any election in which the system was used.

History

Source: L. 2004:Entire section added, p. 1347, § 14, effective May 28. L. 2013:IP(1), (1)(m), (1)(n), and (1)(o) amended,(HB 13-1303), ch. 185, p. 713, § 49, effective May 10. L. 2021:(1.5) added,(HB 21-1071), ch. 367, p. 2417, § 6, effective July 1, 2022.

Research References & Practice Aids

Hierarchy Notes:

C.R.S. Title 1

C.R.S. Title 1, Art. 5

State Notes

Research References & Practice Aids

Cross references:

(1) For the legislative declaration contained in the 2004 act enacting this section, see section 1 of chapter 334, Session Laws of Colorado 2004.

(2) In 2013, the introductory portion to subsection (1) and subsections (1)(m), (1)(n), and (1)(o) were amended by the "Voter Access and Modernized Elections Act". For the short title and the legislative declaration, see sections 1 and 2 of chapter 185, Session Laws of Colorado 2013.

Colorado Revised Statutes Annotated

Copyright © 2022 COLORADO REVISED STATUTES All rights reserved.

APPENDIX H. MAN IN THE MIDDLE ATTACK

In Figure 10, an encryption certificate is not visible. This is due to the fact that an encryption certificate had not been created and assigned. This alone does not indicate the lack of a security encryption certificate, because SQL Server will create a self-signed certificate automatically, as it has done in this case. However, self-signed certificates are known to be insecure and susceptible to common man-in-the-middle attacks. On a voting system, where security should be paramount, this is wholly irresponsible at best.

Despite the direct connection to the back-end of the SQL server is set to be encrypted even in this sub-par fashion, any device with Microsoft SQL Server Management Studio or any other SQL Server client installed that supports the Windows Authentication method can connect to the server provided they have some type of connection (directly or indirectly) to any part of the voting system network, can find the server IP address, a userID and a password. Microsoft SQL Server Management Studio is a free download from Microsoft and does not require any special licensing – anyone can obtain it and use it without restriction. There are also many other SQL Clients that exist for Windows, OS X, iPhone, Android, and others, many that are free to download and use.

The SQL Server Management Studio (SSMS) software used on the Expert's client computer was downloaded directly from Microsoft, and that Expert's client computer had no prior encryption configuration, encryption keys or certificates containing encryption keys – the only things supplied to make the connection to the EMS server were a userID, password, and the IP address of the server.

Detail:

A "Man-In-The-Middle" attack (MITM) is an attack where an eavesdropper intercepts a communication between two parties, and makes each party believe he (or she) is the person they intended to communicate with by impersonating them.

In Figure 67 below, Person A would normally communicate with Person B directly. The attack involves intercepting the communication and impersonating the other party as illustrated by the red arrows and Person C.

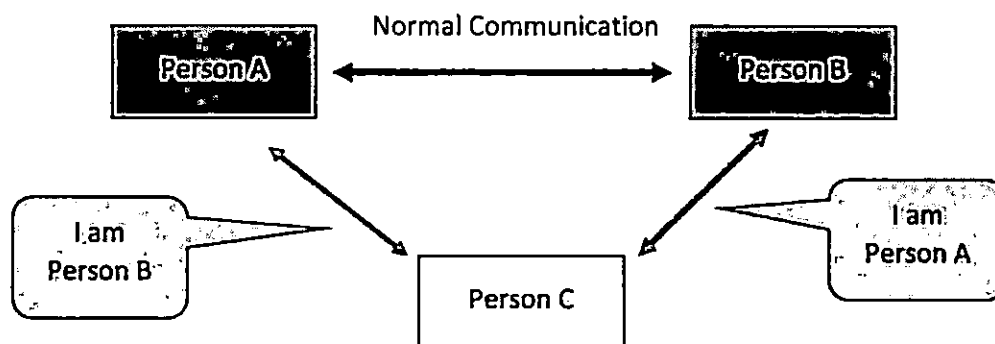


Figure 67 - Man In The Middle Attack

In the MITM attack, Person C can eavesdrop undetected, and can also alter or insert data that the other parties are unaware of. This is often used to steal passwords as well as change information, when the communication is unencrypted.

CONFIDENTIAL

When the communication is encrypted with an encryption certificate, the certificate must be checked to be sure it is authentic and valid. If these checks are not properly performed, the MITM attack becomes possible.

A public Certificate Authority (a commercial service that can be purchased) usually guides the user through the proper certificate checking process when setting up the service. Alternatively, encryption may be setup using a Self-Signed Certificate, however the user is dependent upon their own knowledge and experience, thus Self-Signed Certificates are more prone to human error, oversight, or lack of knowledge of the proper process. If the checks are not properly setup, either method may be subject to this attack method.

While this seems complicated to setup for the average user, devices that perform MITM attacks are commonly available (see the Wi-Fi Pineapple, <https://shop.hak5.org/products/Wi-Fi-pineapple>). Tools such as these are used by cybersecurity professionals to check for the kind of misconfiguration that would allow an MITM attack, with the goal of helping the client fix those security problems, once identified. However, the devices are available for purchase by anyone.

APPENDIX J. FORENSIC IMAGING TECHNOLOGY

In the forensic community, forensic imaging is often referred to as producing a bit-for-bit image of a data storage medium, most of which historically have been hard disk drives. The statement is not quite so simple – as this Appendix explains.

In the figure below, internal components of a hard disk drive are illustrated. The blue disks are the actual 'disk platters', each of which have an upper magnetic media surface and a lower magnetic media surface. Each disk platter is mounted on a center shaft, called a 'spindle' which is connected to a motor that rotates the disks. For each media surface (i.e., where data can be stored) there is an armature (illustrated in black on the right) with a read/write head (in red, at the end of the armature). In this illustration, there are 4 platters with 2 media surfaces each, for a total of 8 surfaces where data can be stored.

As the disk spins, the read/write heads (similar to the heads in a magnetic tape recorder) move over the data and can read and write new data by magnetizing the disk media. These heads actually aerodynamically fly, a micron or so above the disk platter.

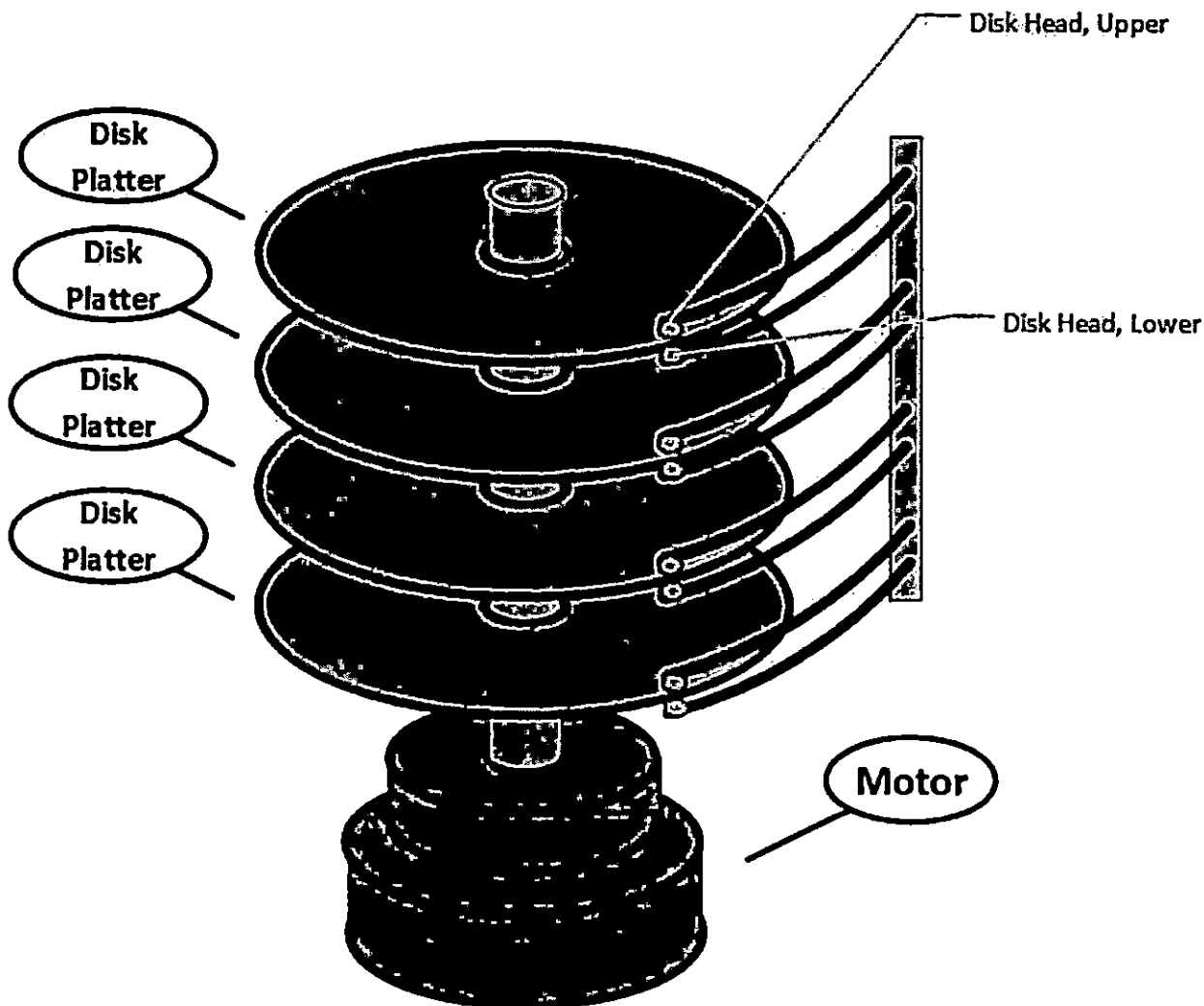


Figure 68 - Illustrative Hard Disk Components

Much like a pizza, each platter surface is divided into sectors (nearly triangular, just as pizza slices are). The surface is further divided into tracks – concentric rings that are smaller and smaller as they move toward the center of the disk. This organization is illustrated in a highly simplified illustration in Figure 67.

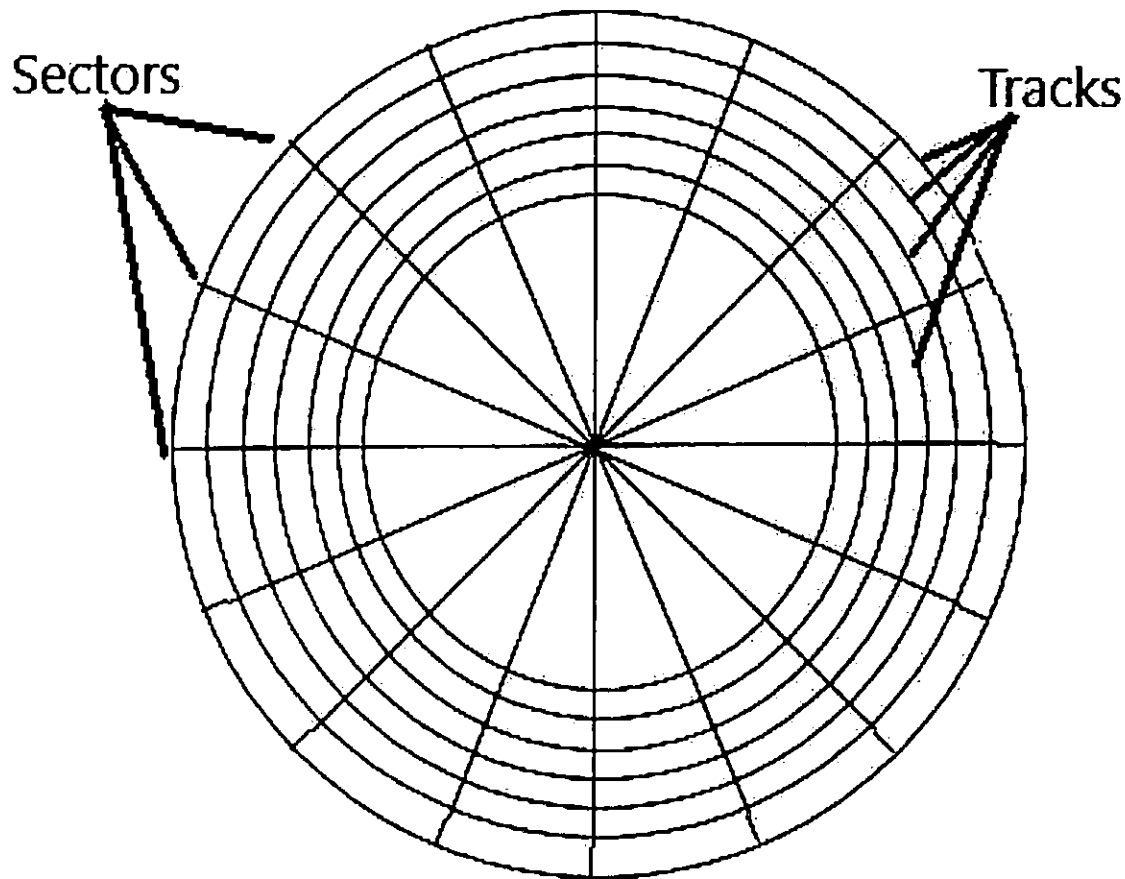


Figure 69 - Disk Track and Sector illustration

In the 1970's, magnetic media was manufactured to have a defect-free surface, but this was prohibitively expensive. Winchester disk technology provided a solution to the high expense. Rather than manufacture a disk media surface that was 100% usable, the manufacture of disk media with a 98% usable surface provided the ability to reduce cost very significantly. This allowed for defective areas on the disk – sectors in which data could not be reliably stored. But this required a scheme to identify these bad areas and ignore them. A map of the disk was developed, from the first sector to the last. As the disk was manufactured, the surface was tested for defects and those sectors with defects were added to the Permanent Defect list, today referred to as the p-list. When the disk is formatted, the disk controller (contained in the disk itself, on its circuit card) will access each physical sector on the disk that is not contained in the p-list, and label that sector with a sequential sector number known as a Logical Block Address (LBA). Obviously the LBA will skip over those sectors in the Defect list. To accommodate the growth of future defects, a list of new bad sectors (to be discovered later in the life of the device) would be added to a Growth List, known as a G-list.

Disk drives are manufactured with more capacity than the end user can access. For example, a 500Gb disk may actually have 580Gb of media storage available. This extra area is known as the Service Area of the disk, and is inaccessible except to the physical disk controller (circuit card that is part of the disk drive itself).

The p-list may be stored in a read-only memory (ROM) on the physical disk controller, or it may be stored in the service area. The g-list is empty at manufacture time and cannot be stored in a ROM but is rather stored in the service area of the disk. The remainder of the service area consists of spare sectors – unused sectors. When a new bad sector is discovered (i.e., a new disk failure) special disk access commands in the disk driver software instruct the disk that a specific logical block is bad and that block is added to the g-list, together with the identity of a spare sector used to replace that sector. The physical disk controller may have replaced physical sector 3921 (LBA 3921) with spare sector 616416, but the new physical storage sector is still addressed by the host computer controller as LBA 3921 because of this mapping. This permits the disk to continue to be used without the computer (and consequently its software) being aware of the replacement sector. If data was unreadable from the damaged sector, the data (file) stored in that location may be damaged and have to be replaced but the disk device still appears, to the computer, to work normally.

Because the sectors in the p-list were defective and never used after manufacture at all, and the g-list sectors were determined after manufacture to be defective, they cannot be read at all. The physical disk controller (built into the drive) has made these p-list and g-list sectors no longer accessible. Spare sectors are also not accessible in the service area of the disk as they are intended to be used as future replacements for active data storage. Finally some physical disk controllers store disk firmware in the service area of the disk but this is neither accessible nor usable to the end user or to the host computer system, but ONLY to the physical disk controller itself.

Thus, there exist data storage areas on a hard drive that have a list of bad sectors, the actual bad sectors themselves that cannot be read, and spare sectors used to repair the drive (and sometimes disk controller firmware). These data storage areas are protected from access to ensure that the drive can be used even though some defects are present from manufacture and others may develop during the lifetime of the drive.

This detail is provided to explain from a scientific perspective that the statement that “every physical bit on a hard drive is accessible and preserved in a forensic image” is true because the logical hard drive, i.e., the total user accessible data area, is what the computer itself and the user are able to access and every bit of data is preserved exactly as it existed at the time of imaging the data. These data in the service area of the data storage system are not accessible to the computer or any user, are not able to be read by forensic software, and they are not copied as part of a forensic image, but they are also not relevant to a forensic analysis of the computer system as none of the data in this service area can be read, written or manipulated without special equipment used by the manufacturer to create the storage device.

The unreadable service area on the drive is not accessible by the computer and does not contain any user accessible data. Even when a bad sector is added to the g-list, the computer does not access the protected service area; it sends a command to the physical disk controller which adds the sector to the g-list and remaps a spare sector in its place.

The remainder of the disk is known as ‘user accessible data area’ and is accessible by the computer system. This user accessible data area is formatted by the computer operating system, Microsoft Windows Server 2016 standard in the case of the Mesa County EMS server, and the data components necessary to create a file system are added to the drive (Master Boot Record, Partition Table, list of free data blocks / sectors, directories and ultimately files containing program and user data). Data in the user accessible data area

can be created, modified, or overwritten. When a file is “deleted” by the operating system, the directory entry is marked indicating that the directory slot is now available to be reused and the sector numbers previously occupied by the file are added back to the list of free data blocks (the free list). The data is not physically deleted from the drive – the drive area is simply marked as available for reuse. When the sectors previously occupied (by for example, data from a photographic image, 1 megabyte in size) are reused by a smaller file, for example, 10,000 bytes of data, the remainder of the original file is still present on the drive and these 990,000 bytes of the photo image in this example can be recovered. Forensic practitioners call this “carving” data from the unallocated disk data, because the boundaries of the previous data are no longer defined and must be discovered by the practitioner to successfully recover the data. These data are fragments of previous files, and while recoverable, are incomplete and sometimes present the forensic analyst with difficulty even determining what kind of data it previously was. Data that has been partially overwritten is not likely recoverable, but the remainder of the data that was not overwritten is able to be recovered. Absent context it may not be possible to draw a conclusion from the data so recovered, however sometimes enough information persists that it supports a conclusion alone or in combination with other data recovered.

All data, and every bit stored in the user accessible data area on the disk drive are captured by a forensic image of the entire disk system and are accessible to the forensic analyst in the forensic image. Thus, for all practical purposes, every possible bit and byte of data on the storage device that is accessible is captured and its integrity preserved such that any modification or alteration of the forensic image is detectable.

The data storage device may be a spinning magnetic disk storage device (hard drive), or it may include Solid State Disks (SSD) or other storage devices and may be in a Redundant Array of Independent Disk (RAID) configuration, in which case the data captured in a forensic image will include every bit of data in the logical hard drive exactly as presented to the computer by the data mass storage subsystem. From an evidentiary point of view, the forensic image captures and preserves every bit and byte of data in the logical view of the physical disk. The forensic imaging software copies all the data that can be accessed by the computer system regardless of whether it is partitioned and formatted or not.

Data that has been completely overwritten is not likely recoverable. “Completely overwritten” means that a sector containing 512 bytes of data is overwritten with 512 bytes of new data (random data in the case of “drive wiping” software). The US Department of Defense considers a file containing classified information (up to the Secret classification) to be adequately destroyed and unrecoverable when overwritten with random data 7 times.

In this examination, the term “hard drive image” refers to this exact data set presented to and operated upon by the computer system. It is a complete set of all data accessible to the computer or computer operator and is an accurate reproduction of ALL of the data on the disk system that can be accessed by the computer under examination.

The original data in the integrity-protected forensic archive cannot be altered, and preserves forensic chain of custody, because this examination used an exact copy of from the original preserved in the forensic archive.

In this Appendix the capability of a forensic image has been explained, with the technical detail of hard drive technology to aid in the understanding that the statement that “every bit and byte of data in the hard

CONFIDENTIAL

drive is captured and preserved", made with reference to the logical view of the data storage medium is technically accurate, and that "every bit and byte of data that can be accessed by a human or a computer operating system IS captured and preserved", integrity controlled and evidentially a complete set of all possible data is preserved and presented in the examination.

APPENDIX K. ACCESSING A COMPUTER WITHOUT A PASSWORD

It is a common belief that a password provides safety as a security mechanism.

In this Appendix I discuss some of the many methods by which password can be bypassed, at a high level. Step-by-step instruction is not provided here. Many books have been published⁹³ and many professional instruction courses and certifications⁹⁴ exist for those in the field who need or desire it and it is not my purpose to repeat that content here.

Finding a password

Many resources exist on the Darkweb⁹⁵ to obtain passwords that have been broken by criminals and are either offered for free or for sale. The article cited discusses 1.4 billion passwords available for free on the Darkweb. US Title 18, section 1029 makes trafficking in passwords or access devices a crime. I did not search the Darkweb for these passwords because trafficking in passwords is a crime, the Darkweb is also full of criminal content, some of which the mere possession of without any intent, is a crime, as well as malware and ransomware, often disguised in innocent-looking webpages. Venturing onto the Darkweb is a good way to lose all your computer data as a consequence of encountering these subversive “traps”.

Method #1 is simply looking up the password. Despite the risk of computer infection or damage, many people do use the Darkweb and this content is available in many cases for free. This risk is so prolific that many services monitor this for you, Norton LifeLock and Identity Force among them, by searching for your credentials on the Darkweb and providing notification if your access has been compromised.

Cracking a password

Passwords, when entered, are encrypted and only the encrypted form of the password is stored. When a person enters a password to login, it is again encrypted and the result is compared to the stored encrypted password. The two encrypted passwords are compared and if they match, access is granted. The encrypted, stored password is *never* decrypted in the process of granting access.

It is possible, once the encrypted stored passwords are obtained, to run various “password cracking” software that tries all conceivable combinations of letters, numbers and symbols until a match between the encrypted stored password and the result under test. The password “cracker” outputs the unencrypted password, once found.

⁹³ <https://www.goodreads.com/shelf/show/penetration-testing>
<https://computingforgeeks.com/best-penetration-testing-books-to-buy>

⁹⁴ Certified Ethical Hacker (CEH) Certification, GPEN, Certified Penetration Tester (CPT), PenTest+, ECSA- EC Council Certified Security Analyst, Certified Expert Penetration Tester (CEPT), Licensed Penetration Tester (LPT), OSCP – Offensive Security Certified Professional, OSCE – Offensive Security Certified Expert
<https://alpinsecurity.com/blog/top-penetration-testing-certifications/>

⁹⁵ <https://www.csoononline.com/article/3266607/1-4b-stolen-passwords-are-free-for-the-taking-what-we-know-now.html>

Rainbow Tables

Encrypting every possible password (called a “brute force” method) requires an extensive amount of computing power and is remarkably slow. To speed this process up, “rainbow tables” have been created. These are tables of encrypted passwords and the corresponding plaintext password allowing the application to simply search the list for a matching entry rather than encrypting every possible combination until a match is found.

Many sources of rainbow tables and the software that uses them exist on the Internet and are readily available.

Bypassing a password

It is possible to bypass a password requirement altogether by using special software on a CD, USB thumb drive or other media or installed by one of many access methods. Security professionals use capabilities like password bypass when a password is forgotten and must be recovered. Microsoft operating systems even include the option to create such a bypass mechanism when the operating system is installed (a password recovery disk). There are many password recovery methods identified on the Internet that perform this function across many different operating systems and are readily available on demand including, specifically, for Microsoft Windows Server 2016 Standard.⁹⁶

Exploitation of Services

Often, in the programming of a computer service, for example, a web server, mistakes and oversights are made in the programming process that leave opportunities for a malicious person to obtain unauthorized access. One such example is the inclusion of “non-printable” characters in an input value (meaning that the included data does not show on a screen). This technique fools the receiving computer into accepting part of the input value as a command that it should execute (a command that means “send me your password file,” for example). There are many different ways to do this, each with their own deep technical explanation (buffer overflow, cross-site scripting, code injection, manipulation of software timing, etc.). There are many penetration testing textbooks that explain the deep technical process and teach how to do this.

These types of mistakes and oversights account for nearly 170,000 identified weaknesses that allow a computer to be attacked. The CVE⁹⁷ system operated by Mitre Corp. has identified 169,169 publicly disclosed vulnerabilities to date. The National Vulnerability Database (NVD⁹⁸) is provided by the National Institute of Technology and Standards (NIST) and contains 808 vulnerabilities that provide full administrative access (between 2005 and the time of this writing). Computer vulnerabilities (weaknesses) are identified nearly daily, and are reported and validated before being published in the CVE or NVD repositories. There exist more vulnerabilities than are publicly known; many are under investigation, not yet validated, while others are known to the US military and intelligence communities and are classified. From these 808 publicly known vulnerabilities, many could be applied to the Mesa County EMS server to grant the type of access demonstrated in this report.

⁹⁶ <https://www.top-password.com/blog/reset-forgotten-windows-server-2016-password/>

⁹⁷ <https://www.cve.org/>

⁹⁸ https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=administrative+access&search_type=all&isCpeNameSearch=false

There are entire suites of software that simplify and automate the capability. Manually performing an exploitation may be a difficult process that requires deep technical knowledge but these automated suites simplify the task making it accessible to a larger population of people. For example, Metasploit can obtain access to a system and return to the user a fully logged-in session with administrative access, allowing the malicious user to do whatever they want to with the system, including stealing or altering data. Kali Linux is an operating system (intended for security professionals to test the security of systems) that contains Metasploit and many dozens of other security tools that can be used to exploit a computer system.

Even passwords (and encryption keys) specific to Dominion Voting Systems have been revealed on the Internet, by no less than the U.S. Election Assistance Commission, and are available online at the time of this writing. One such report with the actual system passwords and encryption keys was published more than 10 years ago and is still available online.

Intel Active Management Technology (AMT) and Management Engine (ME)

Every processor made by Intel since 2008, as well as processors made by AMD and others, incorporate a form of this Management Engine (ME) technology.⁹⁹ This has not been popularized broadly but is a serious concern for all computer systems.

Embedded in the silicon of microprocessors is an independent processor with its own operating system. This processor runs even when the power is off (as long as there is power to the motherboard), and is accessible via the computer's network interface. It provides its own IP address and MAC address and is capable of bypassing the operating system.

Vulnerabilities identified in 2017 were identified as critical.¹⁰⁰ Researchers indicated that it was possible to read passwords from memory (among other things) and completely bypass the Operating System of today's computers. While no exploitation of this capability has been identified that we know of, Nation-States (including our own) would consider the ability to be highly classified – to the point – we would not know about it.

The vulnerabilities are known as Meltdown and Spectre. They are side-channel attacks against systems.¹⁰¹

These vulnerabilities if exploited could provide complete access, undetectably, to a system, even with the computer in a "shutdown" state, as long as the system is plugged in (i.e., power is supplied to the motherboard). This continuous power to the motherboard has long been a feature in modern computer systems and is how the "Wake on LAN" feature is able to function ... it is not that the computer has no power, it just has very low power applied.

⁹⁹ https://en.wikipedia.org/wiki/Intel_Management_Engine

¹⁰⁰ <https://www.intel.com/content/www/us/en/support/articles/000025619/software.html>

¹⁰¹ <https://www.intel.com/content/www/us/en/architecture-and-technology/side-channel-variants-1-2-3.html>

<https://www.intel.com/content/www/us/en/architecture-and-technology/side-channel-variants-3a-4.html>

<https://www.intel.com/content/www/us/en/architecture-and-technology/l1tf.html>

<https://www.intel.com/content/www/us/en/architecture-and-technology/mds.html>

Dell Integrated Remote Access Controller (iDRAC)

Dell offers a capability known as iDRAC on its servers.¹⁰² It is a completely separate processor with its own Ethernet interface, IP and MAC addresses. It is intended to be used on a highly restricted network for “out of band” management of the server, and allows an administrator (or anyone with access¹⁰³) to reboot the system, access and change the BIOS, and alter the system without the motherboard’s processor being able to detect this activity. If you have a server in a data center 30 miles (or more) from your office that needs to be rebooted, and you don’t have staff at this remote location, driving an hour or more just to reboot the system is an impediment to productivity – the iDRAC is intended to provide remote control for just this reason.

The primary computer has no way to detect the use of the iDRAC; if used the primary computer’s audit and system logs would not record it. An iDRAC is intended to permit access to the core computer and its files.

Strengthening Access Security

One technique for strengthening access security is multi-factor authentication. This is an industry-standard practice and recommended by the National Institute of Standards and Technology (NIST) among many other technical and professional organizations.

Many readers will recognize this multi-factor authentication as something you have already used, once you understand what it is. Multi-factor authentication requires identification be verified by techniques in two or more of the three categories:

1. Something you know (a password, special code, birthday, or other identifying number not related to the information you are accessing),
2. Something you have (an access token, a calculator that accepts an input number and returns an encrypted response, a cellphone where you receive a message to authorize the access, etc.), and
3. Something you are (biometric information, a fingerprint, retina scan, iris scan, face recognition, etc.).

Systems that send you a verification code via cell phone SMS message are a good example of the use of multi-factor authentication.

Best practice in access security is to apply the principle of “Defense in Depth,” which is to apply multiple layers of security such that if one fails another serves to protect the system. A “hardened” system requires Defense in Depth, and the proper implementation of multiple security mechanisms, as specified in the DoD Security Technology Implementation Guides (STIGs).

The US Department of Defense employs thousands of military and contractor staff who work full-time on the problem of maintaining sufficient cybersecurity to (hopefully) stay ahead of the threat. Homeland Security maintains a significant cybersecurity division, as does the National Security Agency (NSA) and other parts of the US intelligence community; the Critical Infrastructure Security Agency (CISA) is dedicated to this mission; NIST maintains an entire division for cybersecurity; the DOJ maintains its own capability for the investigation and prosecution of these High-Tech crimes and the High-Tech Criminal Investigator’s Association (HTCIA) provides a public private partnership with their law enforcement counterparts. This is

¹⁰² <https://www.dell.com/support/kbdoc/en-us/000179517/dell-powerededge-how-to-configure-the-idrac-system-management-options-on-servers>

¹⁰³ Note that this document identifies the default iDRAC userID and password as “root” and “calvin”.

CONFIDENTIAL

a gross understatement of the problem and the resources allocated to address it. Part of the mission of the FBI InfraGard program is to maintain a public-private partnership with the civilian operators of US national critical infrastructure to thwart cybercrime and cyber threats against the USA. The US Secret Service maintains an Electronic Financial Crimes Task Force (EFCTF) to pursue financial cybercrimes. The budget for these efforts far exceeds several billion dollars annually.

Yet our election security depends on temporary workers with very minimal training and no requirement for cybersecurity knowledge, training or certification. DoD requires thousands of security professionals. Is our election infrastructure less important?

The ability to obtain access to a computer without a password is a persistent problem and will continue to be because computers are programmed by humans; and humans are not perfect, they make mistakes.

Unfortunately, there are enough nefarious people in the world exploiting these weaknesses for their own benefit, that this problem is not likely to ever end.

APPENDIX L. SUPPLY CHAIN SECURITY THREAT AND FOREIGN MANUFACTURING

The United States is a significant target of espionage from foreign adversaries. According to the US Director of National Intelligence in their Supply Chain Risk Management Best Practices¹⁰⁴ document,

“The U.S. is under systematic assault by Foreign Intelligence Entities (FIEs) who have augmented traditional intelligence operations with nontraditional methods, including economic espionage, supply chain exploitation, and the use of students, scientists, and corporate employees, to collect both classified and unclassified information. The scale of this effort has put entire industries at risk. Specifically, the globalization of supply chains presents a major attack vector, characterized by a complex web of contracts and subcontracts for component parts, services, and manufacturing. FIEs use this complexity to obfuscate efforts to penetrate sensitive research and development programs, steal vast amounts of personally identifiable information (PII) and intellectual property (IP), and insert malware into critical components. Supply chain exploitation, especially when executed in concert with cyber intrusions, malicious insiders, and economic espionage, threatens the integrity of key U.S. economic, critical infrastructure, and research/development sectors.”

With the growth of global competition, industry in the US is driven to source materials, components, and finished goods from other countries where costs are significantly lower. However, FIEs continue to insert operatives into these foreign supply chains to the USA where they might be strategically positioned to infiltrate supplies using espionage techniques, including inserting surveillance devices into manufactured goods.

This activity includes the contamination of manufactured electronic components with surveillance devices that record and retransmit audio, video and computer data to their foreign controllers.

Presidential Executive Orders 13959¹⁰⁵ signed by President Trump declared a National Emergency (Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies) and Presidential Executive Order 14032¹⁰⁶ signed by President Biden continued and expanded that National Emergency, banning investment in listed foreign companies. These include manufacturers like Huawei, China Telecom, cellphone manufacturers and electronics manufacturers that have conducted espionage against the US by means of installing covert surveillance devices in equipment during its manufacture.

Infiltration of the supply chain includes the use of hardware and software alterations to systems. The SolarWinds attack on the US Government involved a software infiltration of the supply chain.¹⁰⁷

¹⁰⁴ <https://www.dni.gov/files/NCSC/documents/supplychain/20190405-UpdatedSCRM-Best-Practices.pdf>

¹⁰⁵ <https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies>

¹⁰⁶ <https://www.federalregister.gov/documents/2021/06/07/2021-12019/addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples>

¹⁰⁷ <https://www.asisonline.org/security-management-magazine/articles/2021/03/spies-in-the-supply-chain/>

CONFIDENTIAL

These alterations of hardware and software are incredibly sophisticated. The alteration of electronic computer chips to plant malicious circuitry¹⁰⁸ in the design of silicon integrated circuits has been demonstrated at the University of Michigan.¹⁰⁹

FBI Director Christopher Wray stated that Chinese spying in the U.S. is so widespread the FBI must launch two counterintelligence investigations a day to counter it.¹¹⁰ China is focused on stealing U.S. technology to increase its capabilities while shortening the research and development time. The FBI currently has over 2,000 active counterintelligence cases related to China.

Bloomberg reported about China's infiltration of the motherboards of Supermicro computers,¹¹¹ manufactured outside the United States and how the insertion of a small chip on the motherboard compromised dozens of companies in the US.

The use of components fabricated, assembled and, or manufactured outside the US, whether furnished as individual parts, assemblies or finished goods, exposes them to the risk of foreign exploitation.

As Bloomberg claimed about the exploitation of Supermicro computers, sourcing components from foreign suppliers presents a supply chain risk that can only be avoided by domestic sourcing.

¹⁰⁸ <https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/>

¹⁰⁹ <https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf>

¹¹⁰ <https://forwardobserver.com/dailysa-fbi-blown-away-by-chinese-spying/>

¹¹¹ <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

APPENDIX M. COLORADO SECRETARY OF STATE PRESS RELEASE



News Release

Media contact
303-860-6903

Annie Orloff
annie.orloff@sos.state.co.us

Steve Hurlbert
steve.hurlbert@sos.state.co.us

State of Colorado
Department of State
1700 Broadway
Suite 550
Denver, CO 80290

Jena Griswold
Secretary of State

Chris Beall
Deputy Secretary of State

Statement from Colorado Secretary of State's Office Regarding an Official Order to Appoint Sheila Reiner and an Advisory Committee to Supervise Mesa County Elections

Denver, August 17, 2021 - Today, the Colorado Secretary of State's office issued an Order to appoint Mesa County Treasurer Sheila Reiner to supervise all conduct of the Mesa County elections and establish a three-person advisory committee including Representative Janice Rich, Ouray Clerk and Recorder Michelle Nauer, and former Secretary of State Bernie Buescher to advise and assist Reiner in her duties.

"The people of Mesa County deserve safe and secure elections. I am confident that with these appointments, voters in Mesa will be able to exercise their constitutional right to have their voices heard in our democracy. As Secretary of State, my top priority is to ensure all election security protocols are followed and to safeguard Coloradans' right to vote and we will continue to conduct the business required of our office to provide oversight, to ensure the integrity of the state's elections," said Colorado Secretary of State Jena Griswold.

"In light of the ongoing investigation into the chain-of-custody and election security protocol breach in Mesa County, the Colorado County Clerks Association supports the Colorado Secretary of State's designation of an interim election official to conduct and oversee elections in Mesa County until the investigation is complete. While unusual, this important step of placing a top-notch election expert in the office will ensure a safe and secure election

CONFIDENTIAL

is conducted for the citizens of Mesa County," said Matt Crane, Executive Director of the Colorado County Clerks Association.

While Department of State staff is continuing to conduct analysis and awaiting additional information, as well as the outcome of a criminal investigation, several facts have prompted substantial concern regarding the ability of the Mesa County Clerk and Recorder's office to execute an election in compliance with statute and rule. Of particular concern:

- Mesa County authorized a non-employee, Gerald Wood, to attend the May 25, 2021 trusted build, in clear violation of Election Rule 20.5.4. The Department has confirmed that this individual was present at the May 25, 2021 trusted build event. The Department has determined that Mesa County Clerk and Recorder employees Belinda Knisley and Sandra Brown participated in facilitating the improper presence of this non-employee during the trusted build event by misrepresenting the individual's employment status and role.
- Footage, both video and photos, was posted online showing the BIOS passwords for Mesa County's voting system. The Department knows from the timestamp on the video and from other evidence that it is likely this sensitive information was filmed and collected during the limited access trusted build installation in Mesa County on May 25, 2021. This meeting was limited only to a minimal number of Department of State staff, voting equipment vendor staff, and three individuals approved to attend by Mesa County: Clerk Tina Peters, Sandra Brown, and Gerald Wood.
- Video surveillance of the Mesa County voting equipment was not continuous and cannot confirm chain of custody of voting equipment. The evidence suggests that an individual in the Mesa County Clerk's office directed Mesa County staff to turn off video surveillance of the voting equipment prior to the May 25, 2021 trusted build. The video surveillance cameras were not turned back on until well after the trusted build had been completed, which is inconsistent with the Department's understanding of the normal course of business practice in Mesa County.
- Two hard drive images from Mesa County election servers were released on the internet during the week of August 9, 2021. Analysis confirms that these images belong to Mesa County hard drives and were created before and after the May 25, 2021 trusted build. The only method to make such copies is to physically access the machines.
- One of the hard drive images is believed to have been taken on Sunday, May 23, 2021. The Department has confirmed that Clerk Peters, Sandra Brown, and Gerald Wood accessed the area where election equipment was stored outside of normal work hours on May 23.

At this time, it is clear that the facts uncovered in the Mesa County Clerk and Recorder's office require that the Secretary of State exercise her authority as Colorado's chief election official pursuant to 1-1-107, C.R.S. to supervise all elections occurring under the authority of Title 1 of the Colorado Revised Statutes in order ensure compliance with all election statutes and rules.

Effective immediately and until revoked by the Secretary of State through subsequent order, Sheila Reiner the Mesa County Treasurer and former Mesa County Clerk will supervise all

CONFIDENTIAL

conduct related to elections occurring under the authority of Title 1 of the Colorado Revised Statutes. The newly formed advisory committee will be responsible for advising and assisting Reiner and will include Representative Janice Rich, Ouray Clerk and Recorder Michelle Nauer, and former Secretary of State Bernie Buescher.

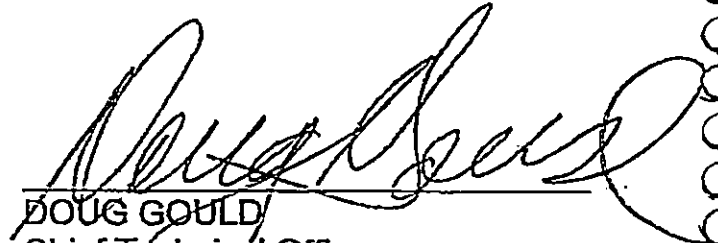
The committee will participate in weekly meetings with Ms. Reiner during the preparation for and execution of an election, unless Ms. Reiner and the committee decide upon another frequency. The committee shall also be permitted to participate in election functions as designated by Ms. Reiner. The Mesa County Clerk and Recorder and staff will take any and all lawful direction from Ms. Reiner and any other Secretary of State designee on any and all election matters.

Given the deadline to purchase, certify, and install trusted build on election equipment before August 31st, a swift appointment was required to ensure safe and secure elections in Mesa County.

#

The foregoing Forensic Examination and Report was prepared by me and I am responsible for its content.

This 28th day of February, 2022.



DOUG GOULD
Chief Technical Officer
CyberTeamUS

Doug Gould Biography

Doug Gould is an expert in Cyber Security with more than 40 years' experience in the field. Doug retired from AT&T after 31 years, where he served as Chief Cyber Security Strategist. He currently serves as Chief Technical Officer at CyberTeamUS.



Doug began at AT&T with Bell Laboratories, serving in the Semiconductor Laser Development department and later in the Bell Lab's Security Group, as a delegate to the Bell Labs' Unix Systems

Subcommittee, was an early pioneer in the field of Computer Forensics and won a Bell Labs Innovation Award. At AT&T he designed the security architecture for one of the largest states in the US, consulted with cabinets of the nations' largest corporations and designed the first healthcare network fully compliant with Healthcare Information Exchange standards. Outside AT&T, he has overseen security for a US Government Agency and has solved major cases for the FBI and Secret Service; he has served as an Officer of the Court as a forensic expert and has been an expert witness in landmark cybersecurity cases. He designed security architectures for DoD networks including some of the most sensitive areas of the Government. Doug has owned and led several professional services firms in the Information Security field. He served on the NC Council for Entrepreneurial Development and has consulted with many companies about the complex integration of business and technology.

Doug is the past president of Eastern North Carolina InfraGard, the public-private partnership between the nation's critical infrastructure operators and the US Intelligence community.

Doug's background is at the Master's level in Electrical Engineering, Computer Science, Computer Security and Business Administration.

He is a subject matter expert in:

- Strategic Enterprise Security
- Security Architecture & Design (including network Micro-Segmentation)
- Security Governance
- Risk Management

- Security Device Technologies (Firewalls, IDS/IPS, DLP, SIEMs, Encryption, VPNs, Unified Threat Management, etc., Enterprise, Remote and Cloud)
- Information Forensics (Computer & Network Forensics)
- Public Key Infrastructures
- Identity and Access Management
- Authentication, Authorization and Access Control (incl Biometrics)
- Regulatory Compliance
- Physical Security (Threat Assessment/Risk Analysis, TSCM, Access Control, Counterterrorism & Counterintelligence, facility and site protection)
- Business Continuity & Disaster Recovery Planning
- Response & Recovery Strategy
- Threat Intelligence
- Intelligence Analysis

Doug served as Chief Information Security Officer at the World Institute for Security Enhancement, has written advanced security courses, developed advanced security methodologies and has taught government, private sector professionals and law enforcement agents information security, computer forensics, advanced computer forensic sciences and Technical Surveillance Countermeasures (TSCM).

Doug holds numerous certifications in security including the CISSP and Certified Anti-Terrorism Specialist (CAS), as well as numerous instructor certifications in security.

Doug currently serves as Chief Technical Officer at CyberTeamUS.

He is a Vietnam-era US Navy Veteran where he worked in Electronic Warfare and Electronic Intelligence.

Doug is an invited conference speaker.

Doug Gould Forensic Addendum

MAJOR FORENSIC CASES

- 1986 – Disclosure of National Security Information
Discovered a leak of highly classified information and was able to identify the perpetrator within a group of 15 people. The FBI and US Naval Investigative Service brought this to resolution.
- Early 1990's – US Secret Service investigation, "Mothers of Doom" hacker case
At USSS Evidence Lab, in response to a request for assistance from USS SA Jack Lewis, performed evidence recovery and identified 800 pages of evidence, invalidating immunity of a suspect's testimony in a proffer session.
- Late 1990's – Interpath, a North Carolina Internet Service Provider (ISP)
This ISP was a tier-1 (top level) provider infected with Stacheldraht malware. Investigated the live (running) server and identified that all evidence on disc had been deleted. The only remaining evidence was a running program in memory, which was recovered. This case changed the Best Practice in Forensics – no longer is the first step necessarily removing the power. Had that been done no evidence would remain in this case.
- Late 1990's – As senior security administrator for the US EPA, investigated a complaint from the White House of computer intrusions and discovered an international attack involving 4 countries. Wrote monitoring and tracking software to capture the perpetrator online, brought together the FBI, Royal Canadian Mounted Police (RCMP), Scotland Yard and Deutsche Bundespost in a live investigation tracking the intruder resulting in an arrest in Germany.
- South Carolina – A Public Works supervisor accused of violation of county policy was fired and brought countersuit. Forensic investigation recovered 4 3" thick binders of evidence showing sexual misconduct. Countersuit dismissed.
- Discovered Al Qaida attack plans targeting US Soil. Working with the FBI, the perpetrator, who was a foreign citizen in the US. Arrest made within 48 hours and the attack was thwarted.
- Mid-2000's – Florida vs. Rabinowicz – in a case where possession of contraband was the only element of proof, stipulated that the contraband was authentic and present. I proved forensically that the defendant was not technically in possession of the evidence and that evidence was planted. Qualified as an expert witness and provided expert testimony in this case.
- Mid-2000's – Identified a leak of national security from Oak Ridge National Laboratory involving chemical weapon information using forensic analysis and was able to identify the perpetrator. DSS responded and resolved the case.
- Mid-2000's – Investigated sabotage of a health industry contractor. The systems administrator had been fired and sabotaged the system. Solved the case and the administrator went to prison.

INSTRUCTOR OF FORENSICS

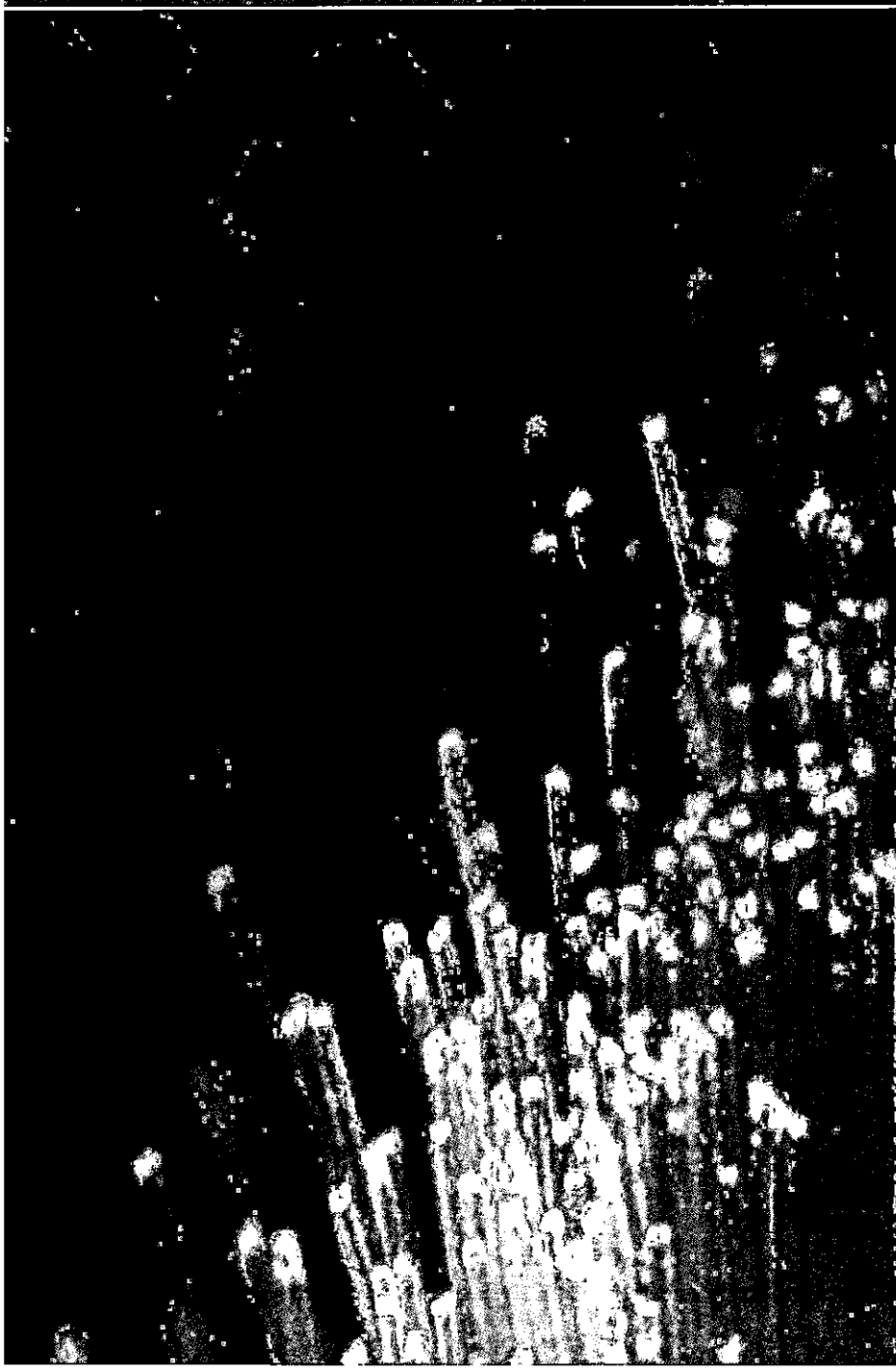
- Taught Forensics and Advance Forensic Techniques to State Law Enforcement, Military and major corporate customers at the World Institute for Security Enhancement.
- Taught Technical Surveillance Countermeasures (TSCM) course for government and industry at the World Institute for Security Enhancement.

Wrote the entire course and taught the entire CISSP curriculum at Able Information Systems.



**Mesa County
Colorado
Voting Systems**

**Report #3
Election Database and Data Process Analysis**



March 19 2022

Table of Contents

Executive Summary	3
Introduction.....	5
Definition of Terms.....	7
Analysis	9
Discussion.....	26
Conclusions.....	28
Appendix A – Batches in Original Adjudication Database.....	31
Appendix B – Batches in New Adjudication Database.....	38
Appendix C – EMS User Log Events in November 2020.....	59
Appendix D – EMS User Log Events in March 2021.....	68
Reference A – Databases and Tables.....	73
Reference B – Scanner Speed	75
Reference C – Scanners Used by Mesa County.....	76
Reference D – Data Movement from Batches to Votes	77

EXECUTIVE SUMMARY

This report documents the findings of an examination of tabulated vote databases based on forensic analysis of the drive image of Mesa County, Colorado's Dominion Voting Systems (DVS) Election Management System (EMS) server. The findings in this report were prepared by the authors as consultants to the legal team representing Tina Peters, the Mesa County Clerk and Recorder, pursuant to her statutory duties as Mesa County's Chief Election Official. The findings provide evidence of potentially unauthorized and illegal manipulation of tabulated vote data during the 2020 General Election and 2021 Grand Junction Municipal Election. Because of this evidence, which led to the vote totals for those elections being impossible to verify, the results and integrity of Mesa County's 2020 General Election and the 2021 Grand Junction Municipal Election are in question.

This analysis was performed using the forensic image of the EMS server, which was backed up before Colorado Secretary of State and DVS overwrote the hard drive with D-Suite version 5.13.

Findings and Implications:

- 1) There was an unauthorized creation of new election databases during early voting in the 2020 General Election on October 21, 2020, followed by the digital reloading of 20,346 ballot records into the new election databases, making the original voter intent recorded from the ballots unknown. In addition, 5,567 ballots in 58 batches did not have their digital records copied to the new database, although the votes from the ballots in those batches were recorded in the Main election database.
- 2) The same unauthorized creation of new election databases occurred during the 2021 Grand Junction Municipal Election on March 30, 2021, followed by the digital reloading of 2,974 ballot records, making the original voter intent recorded on those ballots unknown. In addition, 4,458 ballots in 46 batches did not have their digital records copied to the

new database, although the votes from the ballots in those batches were recorded in the Main election database.

- 3) The absence of secure hash algorithm (.sha) files for each digital ballot image makes the authenticity of each digital ballot image, and the ballot-level record for those ballots, impossible to verify.
- 4) The true total vote count in Mesa County, Colorado cannot be accurately calculated for the 2020 General Election or the 2021 Grand Junction Municipal Election from records in the databases of the county's voting system.
- 5) There is no function or feature on the EMS server that could be executed inadvertently or deliberately by a local election official that would cause this combination of events to occur, especially within the time frame that these events occurred. Given the complex sequence of data manipulations and deletions necessary to produce the digital evidence described in this report, this combination of events could not have been the result of either deliberate or inadvertent actions by those officials.
- 6) Dominion's installation of the Trusted Build update on the EMS in May of 2021, as ordered by the Colorado Secretary of State, destroyed all data on the EMS hard drive, including the batch and ballot records that evidenced the creation of new databases and reprocessing of ballot records described in Findings 1 and 2 above. This destruction of all data by the trusted build is described in the "Mesa County, Colorado Voting Systems Forensic Examination and Analysis Report".
- 7) The fact that such ballot record manipulation has been shown demonstrates a critical security failure with the DVS EMS wherever it is used. The manipulation would not be identifiable to an election official using the voting systems, nor to an observer or judge overseeing the election conduct, much less to citizens with no access to the voting systems; without both cyber and database management system expertise, and

unfettered access to database records and computer log files (many of which were destroyed by the actions of the Secretary of State) from the EMS server, the manipulation would be undetectable.

INTRODUCTION

The use of computerized election management systems is now nearly universal across counties in the United States. While the use of these systems is touted as “efficient”, potentially decreasing manpower costs and time to produce election results, it also greatly reduces the transparency of the election process and exposes our elections to extraordinary vulnerability from both inadvertent and deliberate misconfiguration or misuse. Americans’ right to free and fair elections is inalienable, but that right is infringed by lack of transparency, and by whatever lies behind that opaque curtain.

Without free and fair elections and the transparency to see it for themselves, without relying on the assertions of any other person or organization, Americans’ consent and the legitimacy of our government, at all levels, is in doubt. If Americans’ votes are to be recorded and counted by machines, every aspect of those machines’ operation, configuration, and data must be recorded, immediately available at no cost or administrative burden to citizens and their independent examiners and confirmed 100% accurate through that independent verification. The absence or shortfall of any of those three imperatives (recorded, available, and independently verified) should immediately cause the public to distrust both the purported result from those machines, and also anyone who insists that they accept those results.

Numerous Federal and State laws attempt to safeguard our voting rights and the integrity of our elections. Title 52 USC provides for much of the Federal guidance in this area, and Colorado Revised Statute (CRS) Title 1 covers most of the Colorado state guidance.

- a) 52 U.S. Code § 10307 prohibits any person acting under color of law to “...willfully fail or refuse to tabulate, count, and report...” the vote of any person entitled to vote.

- b) 52 U.S. Code § 10308(a) prescribes penalties for any person depriving or attempting to deprive any person of voting rights under Federal statute.
- c) 52 U.S. Code § 10308(c) prescribes penalties for conspiring to violate or interfere with secured voting rights.
- d) 52 U.S. Code § 20701 mandates the preservation of all election records for 22 months after an election for Federal offices.^{1,2}
- e) 52 U.S. Code § 20702 prescribes penalties for theft, destruction, concealment, mutilation, or alteration of § 20701 election records.
- f) 52 U.S. Code § 21081 requires that voting systems used in elections for Federal office meet the standards of that section, including that the voting system shall produce a record with an audit capacity for such system, and that “the error rate of the voting system in counting ballots...shall comply with the error rate standards established under section 3.2.1 of...” the Federal Election Commission 2002 Voting System Standards (VSS).³
- g) CRS §1-5-601.5 requires that voting systems and equipment in Colorado meet 2002 VSS standards, at minimum.
- h) CRS §1-7-802 requires the preservation of election records for 25 months after elections.
- i) CRS §1-13-111 prescribes penalties for destroying, removing, or delaying delivery of election records.

Title 52 clarifies that the “every officer of election” is responsible for maintaining the election records.

¹ U.S. Department of Justice Publication “Federal Law Constraints on Post-Election ‘Audits’,” July 28, 2021, states that “The materials covered by Section 301 extend beyond ‘papers’ to include other ‘records.’ Jurisdictions must therefore also retain and preserve records created in digital or electronic form.”

² The Federal Election Commission’s 2002 Voting System Standards, the standards of which are mandatory minima for certification of voting systems under Colorado state statute § 1-5-601.5., specifies that a voting system which “...provides access to incomplete election returns and interactive inquiries before the completion of the official count...shall: a. ...be designed to provide external access to incomplete election returns only if that access for these purposes is authorized by the statutes and regulations of the using agency...b. Use voting system software and its security environment designed such that data accessible to interactive queries resides in an external file, or database, that is created and maintained by the elections software under the restrictions applying to any other output report, namely, that: 1) The output file or database has no provision for write-access back to the system. 2) Persons whose only authorized access is to the file or database are denied write-access, both to the file or database, and to the system,” and states that the Standards are “intended to address...risks to the integrity of a voting system...,” including “...Changing calculated vote totals;...” and “Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals;...”

³ 2002 VSS, para 3.2.1 specifies “d. For central-county systems...: Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data...a target error rate of no more than one in 10,000,000 ballot positions.” A ballot position is each and every choice (e.g. a “bubble” which can be marked or filled-in) on a ballot selectable by a voter to convey their voting choices.

Mesa County, Colorado, uses software and hardware provided by DVS and for the 2020 General Election and the 2021 Grand Junction Municipal Election, specifically used “D-Suite 5.11-CO.” The primary voting system EMS server, which contains the raw tabulated vote information used to produce official election reports, makes use of Microsoft SQL Server 2016 databases running on the Microsoft Windows Server 2016 operating system. The forensic image used for the analysis, created on May 23, 2021, has been validated as authentic.

DEFINITION OF TERMS

“Ballot”: Mesa County used two-sided paper ballots in the November 2020 General Election and the 2021 Grand Junction Municipal Election. A ballot is a device used to cast votes in an election. In Colorado, ballots are pieces of paper defining races and issues, and reflecting the choices of individual voters from among the options available for each race and issue. A digital image of each paper ballot is created by the DVS D-Suite voting system during the processing of ballots, as described below, and that ballot image is stored on the designated “NAS (Network Attached Storage device)” of the D-Suite voting system.

“Adjudication”: A term used to describe the process of determining voter intent from a voter’s ballot marks, where ballot markings are ambiguous. According to Dominion’s Democracy Suite Use Procedure Manual, adjudication is “the process of examining voted ballots to determine, and, in the judicial sense, adjudicate voter intent”. In the DVS D-Suite, adjudication refers to the operation and use of a software component called “EMS Adjudication,” and the process of using that software component to manually or automatically interpret voter intent from scanned ballot images, and then to record that interpretation as the record of the vote choices for the affected ballots, in both “result files” and ballot images. Depending on software configuration choices, individual ballot images/result files, entire batches of ballot images/result files, or all ballot images/result files can be subjected to automatic or manual adjudication on the basis of “exceptions” or “outstack conditions” (e.g., “overvotes”, where too many choices are marked for a race or issue; or “marginal marks” when ballot choice ovals are not adequately filled in), or by the arbitrary decision of EMS administrators.

“Manual Adjudication”: Either all ballot images, or individual ballot images, or those from particular batches or tabulators, in which voter intent for any race or issue is flagged by the EMS Adjudication software module as not being determinable (or as having “exceptions”), are, in theory, sent to “Manual Adjudication” stations where officials called “Adjudicators” view the digital images of the ballots and decide the voter’s intent. In this Report we sometimes use the terms “manual adjudication” and “machine adjudication” to clearly distinguish the process of human judging of voter intent from the process of the DVS EMS Adjudication software’s determining of voter intent.

“Adjudication database”: The DVS D-Suite version used in Mesa County during the November 2020 and April 2021 elections maintains a separate SQL Server database, called an “AdjudicableBallotStore,” created by DVS software, for each election which contains records of all batches and ballots scanned into the voting system through ImageCast scanning workstations, and any batch and ballot records manually entered. The database maintains critical information about each batch and ballot, most importantly the ballot Adjudication status and the file location of the ballot image. A batch can have any of the following adjudication statuses in the adjudication system: In-Progress, Read Error, Review, Pending Submission, Submitted, or Submission Error.⁴ Throughout, “Adjudication database.”

“Main election database”: The DVS D-Suite version used in Mesa County during the November 2020 and April 2021 elections maintains a database for each election, called an “ElectionStore” by DVS, which contains information defining an election, including contest, candidate, and ballot definitions as well as aggregated vote information which is used to produce all election reports generated by County officials. Throughout, “Main database.”

“Tabulation database”: The DVS D-Suite version used in Mesa County during the November 2020 and April 2021 elections maintains a database for each election,

⁴ In-Progress batches have been acquired by the system (e.g. through scanning at an ICC) and have ballots being served to clients (Adjudication); Read Error batches are those which encounter errors while being loaded into the system; Review are batches with all ballot adjudication complete, including batches with no adjudication required; Pending Submission are batches submitted to tally, but which have not yet completed that transmission to the tally process; Submitted are batches which have completed the transmission to the tally process; Submission Error are batches that were submitted to the tally process, but which were unsuccessfully submitted.

called a “TabulationStore” by DVS, which contains the timestamps and ballot counts for each batch of ballots, which duplicates that information contained in the Adjudication database. It contains other tables which are not used by Mesa County’s elections. Throughout, “Tabulation database.”

“Reprocessed”: For the purposes of this Report, the term “reprocessed” means that one or more data records which had already been created, presumably by scanning of paper ballots through an ImageCast Central (ICC) workstation, though also technically possible through manual entry of records, within the databases associated with an election, were loaded into the system *again* to a different database, and that this re-loading was not performed in connection within any documented, authorized election-related operations procedure or function. A comparison with the log files of the respective ICC workstations might reveal whether the reprocessed paper ballots were, in fact, rescanned at the ICC, but many of those log files have been destroyed by the Secretary of State’s “Trusted Build.”

ANALYSIS

I. Evidence of ballot record data manipulation – November 2020 General Election

Our analysis shows manipulation, which was neither initiated nor authorized by Mesa County election clerks, of the batches and ballots processed during the first three days of ballot processing in the November 2020 General Election.

The following timeline of events, beginning October 19, 2020, when Mesa County began processing ballots in the General Election, demonstrates this manipulation of ballots.

October 19, 2020 – October 21, 2020, 2:14 PM

On these first three days of ballot counting in Mesa County, up until 2:14 PM on October 21, 2020, 267 batches, consisting of 25,913 ballots, were physically processed (physically scanned on DVS ICC scanners with voters’ choices, in the

form of marks on the ballots, scanned and interpreted by software) through three tabulators, internally identified in the Main database as tabulator IDs 4, 7, and 10. Mesa County election clerks reported no unusual activity or errors encountered during the processing of these 267 batches. The Adjudication database used at this time contains records of all batches with a sequential “load order” of 1 to 267, and other tables within it record the information about each ballot, for instance the time it was entered into the database, the tabulator used, and the adjudication status. Those which were selected for Adjudication have the proper status records indicating that the normal adjudication steps occurred.

The initial 10 batches processed through tabulator 10, containing a total of 941 ballots, had timestamps indicating that they were all entered into the database within 47 seconds (total – not 47 seconds per batch, but 47 seconds for 10 batches). (See Appendix A for a list of the batches and their timestamps in the **original** Adjudication database.) The Canon DR-G1130, which according to purchasing documents and Colorado Secretary of State voting equipment inventories is the model of scanners used by Mesa County (see Reference C and the Colorado Secretary of State website⁵), operates at approximately 100 pages per minute (ppm), duplex, meaning that scanning both sides of each ballot would take no less than 0.01 minutes, which is 0.6 seconds, per ballot. 941 ballots at 0.6 seconds per ballot should have taken a minimum of 564 seconds, or slightly under 9 and a half minutes, a significantly longer interval than 47 seconds, which is physically impossible. Mesa County election clerks were unaware of these batch timestamps, or any issue which could explain them.

October 21, 2020 - 2:14 PM

According to the data contained in the EMS SQL Server Database, new Tabulation and Adjudication databases were created on the EMS server at 12:18:50 PM October 01, 2020. These databases initially contained no data records.

⁵ CO SecState Voting Equipment Inventory at: <https://archive.ph/RQS91>
Page 10 of 87

Figure 1. "Before" Screenshot of Databases on the Mesa EMS Server

	name
1	2020 Mesa County General-2020-09-05-00-10-20
2	AdjudicableBallotStore_2020_Mesa_County_General_2020-10-01_12:18:50
3	TabulationStore_2020_Mesa_County_General_2020-10-01_12:18:50

One Adjudication database and one Tabulation database were listed, with creation times before the counting in Mesa County began on October 19, 2020.

Figure 2. "After" Screenshot of Databases on Mesa EMS Server

	name
1	2020 Mesa County General-2020-09-05-00-10-20
2	AdjudicableBallotStore_2020_Mesa_County_General_2020-10-21_14:18:51
3	TabulationStore_2020_Mesa_County_General_2020-10-21_14:18:51
4	AdjudicableBallotStore_2020_Mesa_County_General_2020-10-01_12:18:50
5	TabulationStore_2020_Mesa_County_General_2020-10-01_12:18:50

Two Adjudication databases ("AdjudicableBallotStore") and two Tabulation databases ("TabulationStore") are now listed, one set of which had creation times before the date and time ballot scanning and tabulation began in Mesa County on October 19, 2020 and the other set of which the EMS server data indicate were created two and a half days *after* ballot scanning and tabulation began.

It has been observed that a clerk giving the EMS system a command to stop and then restart adjudication in an election again creates new Adjudication and Tabulation databases. Mesa County clerks are very certain that they did not initiate any such action in either the November 2020 or the April 2021 elections. Therefore, it is likely that a procedure internal to the DVS software had to perform a stop and restart of the adjudication services in order to perform the batch and ballot manipulation which occurred later (see below).

There are only a few possibilities which would explain how the database copying process was initiated.

1. Direct action by Mesa County personnel

The client application used by election clerks does give them the ability to stop and restart adjudication, which would create the new databases.

However, Mesa County personnel are very clear that they did nothing of the sort and explained that they would only do such a thing in an extreme emergency, as the process would have made the production of legally mandated reports very difficult.

2. Triggered remotely

“Report #2, Forensic Examination and Analysis Report” by D. Gould identifies numerous security vulnerabilities in the DVS EMS server. A signal, or external trigger,⁶ giving instructions to software inside the EMS server could have been sent to and received through any of the open communication ports, or through the port 80 Web Server port, which has been demonstrated to be open on the server and accepting commands via an application programming interface (API).⁷ This signal, along with other information, could have been received via a local network connection (from any device connected to the EMS server’s internal network), from a remote network connection (if the EMS server’s internal network has been bridged to the external internet), or via an internal cellular modem installed in the EMS server. If the EMS Server was connected to a wireless network, it is feasible that even a cell phone outside of the building, but still within the wireless signal radius, could have been used to trigger the events.

This option is plausible but infers a degree of external, time-sensitive control over the DVS equipment in use in Mesa County. This control might

⁶ E.g., an “external trigger” most people are familiar with is the function whereby their smartphone’s wi-fi connection is turned on in response to detecting the proximity of a saved, pre-approved wi-fi network. The external trigger satisfies the criteria of an internal, saved rule for application behavior, and the application then executes the correlated command or function. We likely don’t think of “Do Not Disturb” mode on our smartphones as being similarly controlled by an external trigger, but if our smartphones are configured to “use network time,” meaning the time signal transmitted by the cellular carrier network, then our smartphones’ “Do Not Disturb” mode isn’t turned on at the time we set, per se, but when our cellular carrier tells our phone that the specified time is reached.

⁷ An API is a specification for interaction which allows computer applications to communicate with, make requests to, and issue commands to other computer applications. I.e., API enables machine-machine communication, coordination, and command and control, depending on the permissions and allowable exchanges of the specific API specification.

be considered undesirable by the perpetrators responsible for manipulating the election data, because it was a possibility that any unauthorized network connections, whether they be via standard ethernet, wireless network connection, or cellular modem, could have been discovered during the election period.

3. Algorithmically Triggered

A software algorithm⁸ running inside the DVS computer systems in Mesa County could have made the decision to perform the new database creations and the selected record manipulation which followed based on preprogrammed criteria related to the election results at the time.

Given that this method requires the least amount of external control and monitoring, this option would seem to be the most likely. The decision to copy the Adjudication and Tabulation databases and re-process the ballot records would be made by software running inside the Dominion EMS (or inside another connected machine running Dominion software) based on unexpected voting patterns.

October 21, 2020, 2:30 PM – 2:34 PM

During this time period, 209 out of the original 267 batches (containing a total of 20,346 ballots) were digitally – not physically – loaded into the new Adjudication and Tabulation databases. Specifically, records for batches with load order 2 through 59 were not reloaded and do not appear in the new Adjudication database in any form. The timestamps of the 209 batch records (load order 1 and load orders 60 through 267) show an impossibly short processing time (approximately 4 seconds each) for these batches to have been physically processed into the newly created Adjudication and Tabulation databases. As described above, because of the minimum scanning time of one

⁸ An “algorithm” is simply a set of rules for logical, sequential consideration of inputs (e.g. a contingent variable state, like “the switch is off” or “the switch is on,” or the value of field/memory location “X” is “1” or is “Not 1”) to produce a consistent, expected output. In this case, a simple, hypothetical algorithm might have been something like “IF (‘numberofbatches’>50) AND (‘ElectionProjectActive’=TRUE) AND (‘EMSAdminUserLoggedIn’=FALSE) AND (VOTETOTAL,‘InternalMachineID:01’>VOTETOTAL,‘InternalMachineID:02’) AND (SYSTIME>20201019) AND (SYSTIME<20201103) THEN COPY: BATCHID030010: BATCHID030059 AND INSERTINTO “adjudicableballotstore,” etc.

minute per batch for the Canon DR-G1130 scanner-based tabulator, it is not possible for these 20,346 ballots to have been physically rescanned (i.e., the paper ballots were not reloaded into the scanning hardware), but rather the digital batch and ballot records were directly added to the new Adjudication database. This indicates that the batches could only have been loaded into the newly created Adjudication and Tabulation databases by using software code or a script running within the EMS server. See Appendix B for a list of all batches and their timestamps in the new Adjudication database. See Appendix C for a list of all commands executed prior to and after the database copy, which provides a precise timeline of the effects of those commands on the database copy.

It is important to note that this unauthorized procedure only copied the records of selected batches of ballots, indicating that this was an intentional act.

Below is a screenshot of the beginning of the list of batches recorded in the original Adjudication database, sorted by the order that they were loaded:

Figure 3. List of Batches Recorded in the Original Adjudication Database, Sorted by Load Order

	TabulatorId	BatchId	Category	CvrBatchId	Name	LoadOrder	CreationTime	ModificationTime
1	10	4001	0	1	Tabulator 10 - Batch 4001	1	2020-10-19 12:07:40.850	2020-10-19 12:09:58.200
2	10	4002	0	2	Tabulator 10 - Batch 4002	2	2020-10-19 12:07:44.443	2020-10-20 10:43:25.547
3	10	4003	0	3	Tabulator 10 - Batch 4003	3	2020-10-19 12:07:48.257	2020-10-20 10:43:26.437
4	10	4004	0	4	Tabulator 10 - Batch 4004	4	2020-10-19 12:07:50.960	2020-10-20 10:43:27.423
5	10	4005	0	5	Tabulator 10 - Batch 4005	5	2020-10-19 12:07:53.960	2020-10-20 10:43:28.500
6	10	4006	0	6	Tabulator 10 - Batch 4006	6	2020-10-19 12:08:12.123	2020-10-20 10:43:29.907
7	10	4007	0	7	Tabulator 10 - Batch 4007	7	2020-10-19 12:08:16.137	2020-10-20 10:43:30.953
8	10	4008	0	8	Tabulator 10 - Batch 4008	8	2020-10-19 12:08:20.107	2020-10-20 10:43:32.390
9	10	4009	0	9	Tabulator 10 - Batch 4009	9	2020-10-19 12:08:24.170	2020-10-20 10:43:33.673
10	10	4010	0	10	Tabulator 10 - Batch 4010	10	2020-10-19 12:08:28.233	2020-10-20 10:43:34.703
11	4	2001	0	11	Tabulator 4 - Batch 2001	11	2020-10-19 12:23:35.457	2020-10-20 10:42:50.047
12	4	2002	0	12	Tabulator 4 - Batch 2002	12	2020-10-19 12:30:25.763	2020-10-20 10:42:51.343
13	4	2003	0	13	Tabulator 4 - Batch 2003	13	2020-10-19 12:32:30.137	2020-10-20 10:42:52.470
14	4	2004	0	14	Tabulator 4 - Batch 2004	14	2020-10-19 12:36:19.937	2020-10-20 10:42:52.970
15	4	2005	0	15	Tabulator 4 - Batch 2005	15	2020-10-19 12:43:25.387	2020-10-20 10:42:53.797
16	4	2006	0	16	Tabulator 4 - Batch 2006	16	2020-10-19 13:50:28.623	2020-10-20 10:42:48.593
17	4	2007	0	17	Tabulator 4 - Batch 2007	17	2020-10-19 13:54:18.990	2020-10-20 10:42:54.533
18	4	2008	0	18	Tabulator 4 - Batch 2008	18	2020-10-19 13:58:23.777	2020-10-20 10:42:56.080
19	4	2009	0	19	Tabulator 4 - Batch 2009	19	2020-10-19 14:03:28.847	2020-10-20 10:42:57.673
20	4	2010	0	20	Tabulator 4 - Batch 2010	20	2020-10-19 14:06:33.427	2020-10-20 10:42:58.877
21	4	2011	0	21	Tabulator 4 - Batch 2011	21	2020-10-19 14:10:23.157	2020-10-20 10:42:59.563
22	4	2012	0	22	Tabulator 4 - Batch 2012	22	2020-10-19 14:14:28.253	2020-10-20 10:43:00.360
23	4	2013	0	23	Tabulator 4 - Batch 2013	23	2020-10-19 14:18:33.053	2020-10-20 10:43:00.970
24	4	2014	0	24	Tabulator 4 - Batch 2014	24	2020-10-19 14:22:22.753	2020-10-20 10:43:01.533

Note that there is a sequential order with all load order numbers represented.

Below is a screenshot of the same table in the newly created Adjudication database:

Figure 4. List of Batches in Newly Created Adjudication database

	TabulatorId	BatchId	Category	CvrBatchId	Name	LoadOrder	CreationTime	ModificationTime
1	10	4001	0	1	Tabulator 10 - Batch 4001	1	2020-10-21 14:20:07.257	2020-10-22 10:33:50.593
2	10	4025	0	60	Tabulator 10 - Batch 4025	60	2020-10-21 14:20:26.273	2020-10-22 10:33:51.907
3	4	2036	0	61	Tabulator 4 - Batch 2036	61	2020-10-21 14:20:30.477	2020-10-22 10:31:56.047
4	10	4026	0	62	Tabulator 10 - Batch 4026	62	2020-10-21 14:20:34.430	2020-10-22 10:33:53.330
5	4	2037	0	63	Tabulator 4 - Batch 2037	63	2020-10-21 14:20:39.043	2020-10-22 10:31:56.780
6	10	4027	0	64	Tabulator 10 - Batch 4027	64	2020-10-21 14:20:43.107	2020-10-22 10:33:54.423
7	10	4028	0	65	Tabulator 10 - Batch 4028	65	2020-10-21 14:20:47.370	2020-10-22 10:33:55.703
8	4	2038	0	66	Tabulator 4 - Batch 2038	66	2020-10-21 14:20:51.527	2020-10-22 10:31:57.297
9	4	2039	0	67	Tabulator 4 - Batch 2039	67	2020-10-21 14:20:55.887	2020-10-22 10:31:58.187
10	4	2040	0	68	Tabulator 4 - Batch 2040	68	2020-10-21 14:21:00.060	2020-10-22 10:31:58.860
11	4	2041	0	69	Tabulator 4 - Batch 2041	69	2020-10-21 14:21:04.060	2020-10-22 10:31:59.907
12	10	4029	0	70	Tabulator 10 - Batch 4029	70	2020-10-21 14:21:08.260	2020-10-22 10:33:56.843
13	4	2042	0	71	Tabulator 4 - Batch 2042	71	2020-10-21 14:21:12.747	2020-10-22 10:32:00.593
14	10	4030	0	72	Tabulator 10 - Batch 4030	72	2020-10-21 14:21:16.810	2020-10-22 10:33:57.640
15	4	2043	0	73	Tabulator 4 - Batch 2043	73	2020-10-21 14:21:20.747	2020-10-22 10:32:01.217

While the record of the batch with load order 1 was copied, there is a gap of 58 batches before the second line, which is a record of the batch with load order 60. Batch load order numbers 2 through 59 were *not* copied, effectively deleting them in the new Adjudication database.

The data records describing the batches and the ballots contained within them in the new Adjudication database, specifically the time stamps shown in Appendix B as well as statements by Mesa County election officials, indicate that the paper ballots and batches were not physically re-scanned. Therefore, it appears the process of scanning these ballots was simulated, and the records of the batches and the ballots contained within them were electronically transferred from the original Adjudication database into the new Adjudication database.

For example, below is the sequence of events detailing the processing of batch 4024 (whose ballots and records were *not* copied to the new Adjudication database) and batch 4025 (whose ballots and records were copied to the new Adjudication database). This will illustrate the contrast between copied and uncopied batch and ballot records.

Batch 4024 is recorded in the original Adjudication database as being created at 4:09:34 PM on October 19. It contained 100 ballots and was scanned by tabulator 10. Ten of these ballots from batch 4024 were subsequently manually adjudicated. The manually adjudicated ballot numbers in the batch which were manually adjudicated were 4, 8, 13, 14, 30, 48, 63, 87, 88, and 90. Then, the votes contained on all 100 ballots were recorded in the appropriate tables in the Main database (see Reference A for a list of these tables). When the new Adjudication database was created, no records from Batch 4024 were copied to it, and thus there was no reprocessing or physical rescanning of the ballots. Adjudication history for the 10 ballots which were manually adjudicated was no longer available to the Mesa County clerks, and the original voter intent of these ballots is unknown.

In contrast, Batch 4025 is recorded in the original Adjudication database as being processed at 4:12:23 PM on October 19. This batch contained 99 ballots and was also scanned by tabulator 10. Fourteen of these ballots were subsequently manually adjudicated. The ballot numbers in the batch which were manually adjudicated were 3, 10, 13, 21, 22, 23, 34, 40, 49, 59, 66, 79, 97, and 99. Then, the votes contained on all 99 ballots were recorded in the appropriate tables in the Main database.

After the new Adjudication database was created, a record of Batch 4025 appeared in its tables at 2:20:26 PM on October 21. It is still listed as having 99 ballots and from tabulator 10. In the new Adjudication database, however, only 6 of the batch 4025 ballots (8 less than the first time these batches were entered into the original Adjudication database), were *again* manually adjudicated. The individual ballot numbers were 3, 21, 22, 40, 59, and 66. At this point, the vote records from at least those 6 ballots and possibly all 99 would have been recorded in the appropriate tables in the Main database, replacing the votes which were already in that database from those ballots. Adjudication history for the 14 ballots which were manually adjudicated was no longer available to the Mesa County clerks, and the original voter intent of these ballots is unknown.

The selected batches in the new Adjudication database (batch 1 and batches 60 through 267) appeared in the same serial order that they were loaded into the original Adjudication database, with the same batch numbers, ballot counts, and load order numbers (compare Appendix A and Appendix B).

October 21, 2020, shortly after 2:34 PM

At this point, as reported by Mesa County election officials, some Mesa County adjudication officials began noticing that they were being asked to look at ballots that they had already adjudicated. This is consistent with these ballots and batches being reprocessed in the new Adjudication database. When the new Adjudication database was created, and the selected records described above were copied and reprocessed, there were outstanding ballots from the last set of batches scanned before the event. As some of these ballots were sent to manual adjudication again after the batches were reprocessed, this caused a situation where the same ballot was in the manual adjudication process twice. This caused confusion among the election staff who were assigned the duty of manual adjudication, since when a ballot was adjudicated the second time the master count of adjudicated ballots, which is displayed by the Dominion system and is used by the election clerks to track the overall adjudication process, did not change. This caused the Adjudication officials to assume that there had been an error and, in some cases, to attempt additional manual adjudications of the same ballot with the same unsatisfactory result.

According to several Mesa County election officials, DVS support was contacted at approximately 4PM on the 21st of October, and while the support representative claimed to not have a solution for the issue Mesa County was seeing, that issue ceased soon afterwards. This indicates that DVS may have performed or caused to be performed an operation unknown to Mesa County election officials (and outside of their control) to address this problem which manifested after the unauthorized database manipulation.

Of the 209 batches which were processed twice (batches 1 and 60 through 267), the ballot counts match between the old and new Adjudication database. However, DVS software marked 2,166 ballots for manual adjudication the first time they were processed in the original Adjudication database, but when reprocessed in the new Adjudication database the software marked only 965 ballots for manual adjudication.

The same ballots run through the same hardware and evaluated by the same software should have had the same resulting ballots marked for adjudication, but they did not. This leads to the logical critical conclusion that not all the ballots in the batches processed after the database copy were the same and had the same votes as the ballots in the same batches processed before the database copy. There is no record remaining of the votes originally recorded from the ballots, and therefore there can be no certainty that the votes now recorded are the same. In essence, the chain of custody has been broken for these votes in the database.

The 58 batches which were *not* duplicated in the new Adjudication database must also be seen as suspect, as their chain of custody has also been broken via the fact that no record of them or their adjudication exists in the Adjudication database in use at the end of the election. A clerk wishing to view the adjudication status of a ballot in any of the 58 batches would be unable to do so, as no information about those batches exists in the new Adjudication database.

Thus, all 25,931 ballot records processed before 2:14 PM on October 21, 2020, comprising over 25% of the County's total over the entire election, cannot be verified and should not have been counted.

II. Evidence of Ballot Manipulation – April 2021 Grand Junction Municipal Election

Our analysis shows a nearly identical manipulation of the batches and ballots processed during the first six days of ballot processing in the April 2021 Municipal Election in Grand Junction, Colorado.

The timeline of events beginning March 24, 2021, when Mesa County Election clerks began processing ballots in the 2021 Grand Junction Municipal Election, follows.

March 24, 2021 – March 30, 2021, 2:43 PM

On these first seven days of counting, up until 2:43 PM on March 30, 2021, 88 batches of ballots, consisting of 8,540 ballots, were processed. County Election clerks report no unusual activity or errors encountered *at any time* during the election counting process. The Adjudication database used at this time contains records of all batches with a sequential load order of 1 to 88, and other tables within it record each ballot. Those which were selected for Manual Adjudication (339 in total) have the proper status records indicating the normal adjudication steps occurred.

March 30, 2021, 2:58 PM

According to the data contained in the EMS server, new Adjudication and Tabulation databases were created and registered within the DVS system as the associated databases for the election. As in the circumstance previously described in the early voting period for the November 2020 election, these two databases initially contained no data.

See Appendix D for a list of all commands executed prior to and after the database creation in the April 2021 Municipal Election, which provides a precise timeline of the effects of creating the new databases and copying the batch and ballot records.

It is important to note that this unauthorized procedure copied the records of only selected batches of ballots, indicating that this was an intentional act.

Below is a screenshot of the beginning of the list of batches recorded in the original Adjudication database, sorted by the order that they were loaded:

Figure 5. List of Batches Recorded in the Original Adjudication Database, Sorted by Load Order

TabulatorId	BatchId	Category	CvrBatchId	Name	LoadOrder	CreationTime	ModificationTime
30	3000	0	2	Tabulator 30 - Batch 3000	1	2021-03-24 14:52:58.350	2021-03-29 14:07:57.213
30	3001	0	3	Tabulator 30 - Batch 3001	2	2021-03-24 15:09:05.203	2021-03-29 14:07:57.557
30	3002	0	4	Tabulator 30 - Batch 3002	3	2021-03-24 15:10:53.607	2021-03-29 14:07:57.917
30	3003	0	5	Tabulator 30 - Batch 3003	4	2021-03-24 15:13:57.637	2021-03-29 14:07:58.307
30	3004	0	6	Tabulator 30 - Batch 3004	5	2021-03-24 15:17:01.500	2021-03-29 14:07:58.587
30	3005	0	7	Tabulator 30 - Batch 3005	6	2021-03-24 15:21:03.903	2021-03-29 14:07:58.837
30	3006	0	8	Tabulator 30 - Batch 3006	7	2021-03-24 15:24:05.780	2021-03-29 14:07:56.837
30	3007	0	9	Tabulator 30 - Batch 3007	8	2021-03-24 15:28:55.220	2021-03-29 14:07:59.273
30	3008	0	10	Tabulator 30 - Batch 3008	9	2021-03-24 15:33:59.600	2021-03-29 14:07:59.650
30	3009	0	11	Tabulator 30 - Batch 3009	10	2021-03-24 15:37:03.750	2021-03-29 14:08:00.010
30	3010	0	12	Tabulator 30 - Batch 3010	11	2021-03-29 11:06:24.310	2021-03-29 14:08:00.323
30	3011	0	13	Tabulator 30 - Batch 3011	12	2021-03-29 11:38:04.150	2021-03-29 14:08:00.667
30	3012	0	14	Tabulator 30 - Batch 3012	13	2021-03-29 11:42:52.697	2021-03-29 14:08:01.040
30	3013	0	15	Tabulator 30 - Batch 3013	14	2021-03-29 11:45:56.630	2021-03-29 14:08:01.383
30	3014	0	16	Tabulator 30 - Batch 3014	15	2021-03-29 11:48:00.360	2021-03-29 14:08:01.713
30	3015	0	17	Tabulator 30 - Batch 3015	16	2021-03-29 11:51:03.987	2021-03-29 14:08:02.040
30	3016	0	18	Tabulator 30 - Batch 3016	17	2021-03-29 13:05:52.907	2021-03-29 14:08:02.400
30	3017	0	19	Tabulator 30 - Batch 3017	18	2021-03-29 13:08:56.587	2021-03-29 14:08:02.743
30	3018	0	20	Tabulator 30 - Batch 3018	19	2021-03-29 13:12:00.483	2021-03-29 14:08:03.073
30	3019	0	21	Tabulator 30 - Batch 3019	20	2021-03-29 13:14:04.207	2021-03-29 14:08:03.400
30	3020	0	22	Tabulator 30 - Batch 3020	21	2021-03-29 13:19:53.690	2021-03-29 14:08:03.727
30	3021	0	23	Tabulator 30 - Batch 3021	22	2021-03-29 13:22:57.557	2021-03-29 14:08:04.103
30	3022	0	24	Tabulator 30 - Batch 3022	23	2021-03-29 13:26:01.097	2021-03-29 14:08:04.430
30	3023	0	25	Tabulator 30 - Batch 3023	24	2021-03-29 13:28:04.527	2021-03-29 14:08:04.790
30	3024	0	26	Tabulator 30 - Batch 3024	25	2021-03-29 13:30:53.410	2021-03-29 14:08:05.133
30	3025	0	27	Tabulator 30 - Batch 3025	26	2021-03-29 13:32:57.050	2021-03-29 14:08:05.540
30	3026	0	28	Tabulator 30 - Batch 3026	27	2021-03-29 13:37:01.250	2021-03-29 14:08:05.900
30	3027	0	29	Tabulator 30 - Batch 3027	28	2021-03-29 13:40:05.090	2021-03-29 14:08:06.227
30	3028	0	30	Tabulator 30 - Batch 3028	29	2021-03-29 13:41:53.687	2021-03-29 14:08:06.573
30	3029	0	31	Tabulator 30 - Batch 3029	30	2021-03-29 13:44:57.640	2021-03-29 14:08:06.900

Below is a screenshot of the same table in the newly created Adjudication database, sorted by creation time:

Figure 6. List of Batches in the Newly Created Adjudication Database, Sorted by Creation Time

TabulatorId	BatchId	Category	CvrBatchId	Name	LoadOrder	CreationTime	ModificationTime
30	3047	0	49	Tabulator 30 - Batch 3047	48	2021-03-30 15:00:14.560	2021-03-30 15:25:33.373
30	3048	0	50	Tabulator 30 - Batch 3048	49	2021-03-30 15:00:17.950	2021-03-30 15:25:34.090
30	3050	0	52	Tabulator 30 - Batch 3050	51	2021-03-30 15:00:36.577	2021-03-30 15:25:33.733
30	3054	0	56	Tabulator 30 - Batch 3054	55	2021-03-30 15:00:50.780	2021-03-30 15:03:21.940
20	2000	0	59	Tabulator 20 - Batch 2000	58	2021-03-30 15:01:01.250	2021-03-30 15:03:19.520
20	2002	0	61	Tabulator 20 - Batch 2002	60	2021-03-30 15:01:07.983	2021-03-30 15:03:19.847
20	2003	0	62	Tabulator 20 - Batch 2003	61	2021-03-30 15:01:11.467	2021-03-30 15:03:20.050
20	2004	0	63	Tabulator 20 - Batch 2004	62	2021-03-30 15:01:15.123	2021-03-30 15:03:19.127
20	2005	0	64	Tabulator 20 - Batch 2005	63	2021-03-30 15:01:18.687	2021-03-30 15:03:20.237
20	2006	0	65	Tabulator 20 - Batch 2006	64	2021-03-30 15:01:22.203	2021-03-30 15:03:20.410
20	2008	0	67	Tabulator 20 - Batch 2008	66	2021-03-30 15:01:29.203	2021-03-30 15:03:20.627
20	2009	0	68	Tabulator 20 - Batch 2009	67	2021-03-30 15:01:32.953	2021-03-30 15:03:20.847
20	2010	0	69	Tabulator 20 - Batch 2010	68	2021-03-30 15:01:36.467	2021-03-30 15:03:21.033
20	2011	0	70	Tabulator 20 - Batch 2011	69	2021-03-30 15:01:40.437	2021-03-30 15:03:21.237
20	2012	0	71	Tabulator 20 - Batch 2012	70	2021-03-30 15:01:44.513	2021-03-30 15:03:21.410
20	2013	0	72	Tabulator 20 - Batch 2013	71	2021-03-30 15:01:48.063	2021-03-30 15:03:21.567
20	2015	0	74	Tabulator 20 - Batch 2015	73	2021-03-30 15:01:55.170	2021-03-30 15:03:21.723
20	2016	0	75	Tabulator 20 - Batch 2016	74	2021-03-30 15:01:58.827	2021-03-30 15:03:39.753
20	2018	0	77	Tabulator 20 - Batch 2018	76	2021-03-30 15:02:05.920	2021-03-30 15:03:47.913
20	2019	0	78	Tabulator 20 - Batch 2019	77	2021-03-30 15:02:09.407	2021-03-30 15:03:48.210
20	2020	0	79	Tabulator 20 - Batch 2020	78	2021-03-30 15:02:13.140	2021-03-30 15:03:47.613
20	2021	0	80	Tabulator 20 - Batch 2021	79	2021-03-30 15:02:16.017	2021-03-30 15:03:51.317
20	2023	0	82	Tabulator 20 - Batch 2023	81	2021-03-30 15:02:22.517	2021-03-30 15:04:13.667
20	2024	0	83	Tabulator 20 - Batch 2024	82	2021-03-30 15:02:26.050	2021-03-30 15:04:18.870
20	2025	0	84	Tabulator 20 - Batch 2025	83	2021-03-30 15:02:29.580	2021-03-30 15:04:18.527
20	2026	0	85	Tabulator 20 - Batch 2026	84	2021-03-30 15:02:33.597	2021-03-30 15:04:20.793
10	1001	0	87	Tabulator 10 - Batch 1001	86	2021-03-30 15:02:40.610	2021-03-30 15:04:48.777
10	1002	0	88	Tabulator 10 - Batch 1002	87	2021-03-30 15:02:44.050	2021-03-30 15:04:49.120
10	1003	0	89	Tabulator 10 - Batch 1003	88	2021-03-30 15:02:47.423	2021-03-30 15:04:48.417
10	1000	0	96	Tabulator 10 - Batch 1000	114	2021-03-30 16:04:55.357	2021-03-30 16:17:49.813

March 30, 2021, 3:00 PM – 3:03 PM

During this three-minute time period, records of 42 batches and the 4,082 ballots contained within them, previously processed into the original Adjudication database, were copied into the new Adjudication database. According to the time stamps, the records of the batches appeared in the new Adjudication database in intervals of a fraction of a second between them, much too quickly for the ballots contained in the batches to have been physically scanned (per the maximum scanning speeds discussed above). Mesa County election clerks state that they did not take any action to reprocess or re-scan any batches on that day, nor did they at any time stop and restart the Adjudication software process. Only 39 ballots in these 42 batches went through manual adjudication after being copied to the new database, and database records indicate that the adjudication process was completed successfully on those 39 ballots.

Unlike what was found in the November 2020 General Election records described above, the records for these 42 batches which were copied to the new database do not appear in the new Adjudication database in exactly the same order as they had originally been loaded; 12 batch records are out of order when the records in the original Adjudication database and the new Adjudication database are compared.

No further anomalies are shown in the Adjudication database records during the Election counting process, nor did Mesa County election clerks encounter any unexpected issues.

Of the 42 batches which were processed twice (batches 45 through 49 and 51 through 88), the ballot counts (total number of ballots) match between the old and new Adjudication databases. However, DVS software sent 339 ballots to manual adjudication the first time they were processed in the original Adjudication database, but when reprocessed in the new Adjudication database the software sent just 39 ballots to manual adjudication.

The same ballots run through the same hardware and evaluated by the same software should have had the same resulting ballots marked for adjudication, but they did not. This leads to the logical critical conclusion that not all the ballots in the batches processed after the database copy were the same and had the same votes as the ballots in the same batches processed before the database copy. There is no record remaining of the votes originally recorded from the ballots, and therefore there can be no certainty that the votes now recorded are the same. In essence, the chain of custody has been broken for these votes in the database.

The 46 batches which were *not* duplicated in the new Adjudication database must also be seen as suspect, as their chain of custody has also been broken via the fact that no record of them or their adjudication exists in the Adjudication database in use at the end of the election. A clerk wishing to view the adjudication status of a ballot in any of these 46 batches would be unable to do

so, as no information about these batches exists in the new Adjudication database.

Thus, all 8,540 ballots processed before 2:58 PM on March 30, 2021, comprising over 49% of the total votes in the entire 2021 Grand Junction Municipal Election, cannot be verified and should not have been counted. These 8,540 ballots represent more than twice the winning margin in any of the four City Council races that occurred in this election.

III. Comparison of the November 2020 General Election Findings and the April 2021 Grand Junction Municipal Election Findings

Comparing the above findings for the two elections shows numerous similarities and also critical differences.

Similarities:

- In both elections, a software process running within the DVS system performed an unauthorized creation of new Adjudication and Tabulation databases.
- In both elections, database records of selected batches and of the ballots within those batches were copied into the new databases and were reprocessed.
- In both elections, selected batches were not copied to the new Adjudication and Tabulation databases, making adjudication information invisible to the Mesa County election clerks.

Differences:

- In the November 2020 General Election, records of a sequential series of batches and the ballots contained within them were copied from the original Adjudication and Tabulation databases to the new Adjudication and Tabulation databases, and the batches were copied in the same order as in the original databases. In the April 2021 Grand Junction Municipal Election, records of a non-sequential series of batches and the ballots contained within

them were copied, and they appear in the new Adjudication database in a different order than in the original database.

- In the April 2021 Grand Junction Municipal Election, the EMS User Logs (which show events and commands which were executed) show reference to a batch 89. As there were 88 batches in the original Adjudication database, this would have logically been the next batch received from the scanners. However, no record of a batch with the load order '89' exists in either Adjudication database, and there are missing load orders between 88 and 114 as well.

The similarities lead to the conclusion that the same method was used to alter the database records in both elections.

The differences lead to the conclusion that there is a degree of control in the method used to alter the database records which used parameters unique to each election.

IV. Summary Impact of Above Findings

This manipulation of batch and ballot records described above is significant for three reasons.

First, when the ballots were reprocessed as described above, including re-adjudication, it is logical to conclude that whatever votes had been initially recorded could well have been replaced by the reprocessed votes in the Main election database. The differences in the Manual Adjudication numbers certainly supports this possible conclusion. Thus, this procedure could change votes in the Main database without leaving any evidence to indicate changes had been made, or any way to determine the nature of the changes or what the original vote data was.

Second, the adjudication status (including the timestamps of adjudication events, the results of the adjudication, and the user who performed the

adjudication) of any ballots in the batches not copied to the new Adjudication database would not be viewable through the DVS client software applications.

Third, an examination of the EMS server which was less rigorous than ours would not likely have caught the fact that the Adjudication and Tabulation databases used at the end of the elections were not the same, nor did they contain the same records, as the databases used at the beginning of the elections. This leads to the possible conclusion that some batches and ballots were excluded from the new databases so as to inhibit the possibility of their being audited or examined.

V. Lack of Referential Integrity in DVS Database Tables

Most modern database designs include a concept called “referential integrity.” For example, if you have one table of data that has information about “people,” and another table that has information about “colleges,” you might have a field in an individual record in the “people’s” table that can contain an id, or pointer, to the college he or she attended. Referential integrity, in this case, would mean that if “John Smith’s” record had a pointer to the “University of Pittsburgh”, the system should give an error if you try to remove the item “University of Pittsburgh” from the “colleges” table. It would not allow you to do this action because a field in “John Smith’s” record refers to the college “University of Pittsburgh” and deleting that entry in the “colleges” table makes “John Smith’s” record invalid.

However, some of the DVS Election Management System data structures have no such referential integrity built into them. Therefore, batch records in one database could be deleted without any consequence to records that point to that batch in another database, and without any detection of the error. This lack of referential integrity means that vote or ballot information could easily be added or removed from one part of the database without any warnings or errors occurring in other parts of the database.

It is, for example, possible to change the fields with vote counts in one table of the Main election database without having that change affect any other tables

or cause a referential integrity violation. This is a fundamental and critical breach of sound database design, particularly considering the importance of chain-of-custody and audit trail evidence for the provenance of ballot record and tabulated vote information in a voting system.

Please see Reference D for an example of how the batch and ballot data moves through the various databases and tables in the Dominion EMS.

VI. Digital Ballot Images are Obfuscated and Unverifiable

An attempt was made to investigate the conditions of the digital ballot images to corroborate the findings above. This avenue of research is greatly hindered because the ballot IDs or sequence numbers in the batches are not relatable to their images, not even within the DVS databases themselves. This is an additional example of a lack of referential integrity within the system.

Additionally, the digital ballot images do not have the accompanying “.sha” files which are meant to prove the authenticity of the ballots. Therefore, any findings, including the integrity and authenticity of ballot images, related to the digital ballot images cannot be absolutely validated because there is no proof that the images are the ones created at the time the ballots were first processed.

Finally, code running within the EMS server that has the system access rights to create and alter SQL Server database records could be used to alter the stored digital ballot images themselves. The EMS Adjudication module software already has the capability of altering scanned images and legitimately does so for each manually adjudicated ballot.

DISCUSSION

The events described above show a significant manipulation of a large number of batch, ballot, and vote records in the DVS EMS Database in Mesa County, and there are only a few possible explanations for the manipulation.

1. Human Error

Extensive questioning of Mesa County election clerks has ruled out human error as the reason for the unauthorized creation of election databases on October 21, 2020, followed by reprocessing of 20,346 ballots. These personnel have a strong recollection of the events of October 21, 2020, and because of the timelines established both by their recollection and corresponding database time stamps, it is evident that any and all unusual actions they might have taken on that day were in response to the new database's creation having already occurred, and batch records being copied into the new database, which affected their ability to complete adjudication on some in-process ballots. Similarly, Mesa County election officials have a strong recollection of the events of March 30, 2021. They state that they did not take any steps that would have given rise to the unauthorized creation of new election databases during the 2021 Grand Junction Municipal Election on that day, followed by the reprocessing of 2,974 ballots,.

2. Software Failure

While an error or failure in the DVS EMS server is a possibility, it strains credulity that any error could cause the numerous specific events which are documented above. In particular, the non-sequential reloading of the batches during the 2021 Grand Junction Municipal Election, when compared with the sequential reloading in the November 2020 General Election, makes it inherently impossible for the same error to have caused both chains of events.

However, as noted in the section above labelled "Algorithmically Triggered", the DVS EMS server (or another connected machine running Dominion software) could have been preprogrammed to perform the unauthorized new database creations and the selected record manipulation which followed based on preprogrammed criteria related to the election results at the time. This would be the result of advance planning in the deliberate

design of the software to alter outcomes when unexpected voting patterns were detected.

3. Network Breach or Pre-Installation of Manipulating Software or Algorithm

A device external to the DVS D-Suite network could have connected to the DVS D-Suite and to the EMS server, using the open SQL Server port 1433, open Web Services port 80, or through any other open port directly into the DVS Software. As outlined in “Report #2, Forensic Examination and Analysis Report” by D. Gould, there are numerous flaws in the security of the server, many of which could provide an outside entity with direct access to the SQL Server Database or the Application itself. The DVS D-Suite makes use of “SOAP” messaging protocol API calls through its web server, so malicious procedures could be triggered by simple port 80 access.

As *all* Windows log files which would show these accesses are configured, as specified by DVS manuals published by the Colorado Secretary of State as mandatory technical procedures for County election officials, to keep only a small amount of log entries before they are overwritten, no record of external access to the DVS D-Suite is available in system logs.

Regardless of whether the voting system was connected to an external network or device, even momentarily, or whether a pre-installed software or algorithm was triggered by an external command or complex set of variable conditions, the execution of manipulating software or algorithm could plausibly be responsible for the results described in our findings.

CONCLUSIONS

1. Unauthorized creation of new Tabulation and Adjudication databases occurred during the counting of the November 2020 General Election, along with the selective copying of batch and ballot records from the original databases to the new ones. This manipulation places all 25,913 initial ballots counted into a state where they cannot be validated – some because

it is possible that their vote information was changed, and unverifiable that it was not, and the rest because their “chain of evidence” has been intentionally obfuscated. Even if the count and content of ballot images match the numbers and counts reported by the database, there is no method to validate those ballot images due to missing “.sha” files, which are intended to provide such validation.

2. Unauthorized creation of new Tabulation and Adjudication databases occurred during the 2021 Grand Junction Municipal Election, along with the selective copying of batch and ballot records from the original databases to the new ones. This places all 8,540 initial ballots counted into a state where they cannot be validated – some because it is possible that their vote information was changed and unverifiable that it was not, and some because their “chain of evidence” has been intentionally obfuscated.
3. As we have found evidence that thousands of ballot records have had their validity placed in serious question, none of the election results from the 2020 General or 2021 Grand Junction Municipal Elections in Mesa County can be considered trustworthy. If Mesa County has preserved the respective paper ballots, as they are required to do by law, and those ballots were forensically authenticated with confirmed chain-of-custody from eligible electors to sworn county election officials (not possible retrospectively, nor under current election procedures in Colorado), then a hand-count of paper ballots might support a verifiable, trustworthy conclusion about the county-level results of these two elections.
4. Because the unauthorized methods used to alter batch and ballot-level information described above are available within the DVS EMS server, this system cannot be considered reliable for use in any election. An investigation, involving all physical and cyber evidence, including a source code audit of the exact, verifiable version of all DVS-supplied executable and library files, is necessary to identify the exact software methods used to produce the manipulation and to determine other potential unauthorized actions that the code is able to cause or enable.

5. The Dominion Voting System's database structure stores actual vote information in only one table, in aggregated form, so alterations made to vote counts or candidates in just that table, create a single point of attack or failure for the entire vote reporting process (see Reference D).

**APPENDIX A - BATCHES - ORIGINAL ADJUDICATION DATABASE
(WITH TIME BETWEEN BATCHES) - NOVEMBER 2020 ELECTION**

TabulatorId	BatchId	LoadOrder	Creation Date	Creation Time	Difference from Prior	Ballots
10	4001	1	10/19/2020	12:07:41 PM		100
10	4002	2	10/19/2020	12:07:44 PM	0:00:04	42
10	4003	3	10/19/2020	12:07:48 PM	0:00:04	100
10	4004	4	10/19/2020	12:07:51 PM	0:00:03	100
10	4005	5	10/19/2020	12:07:54 PM	0:00:03	100
10	4006	6	10/19/2020	12:08:12 PM	0:00:18	100
10	4007	7	10/19/2020	12:08:16 PM	0:00:04	100
10	4008	8	10/19/2020	12:08:20 PM	0:00:04	99
10	4009	9	10/19/2020	12:08:24 PM	0:00:04	100
10	4010	10	10/19/2020	12:08:28 PM	0:00:04	100
4	2001	11	10/19/2020	12:23:35 PM	0:15:07	98
4	2002	12	10/19/2020	12:30:26 PM	0:06:50	100
4	2003	13	10/19/2020	12:32:30 PM	0:02:04	100
4	2004	14	10/19/2020	12:36:20 PM	0:03:50	100
4	2005	15	10/19/2020	12:43:25 PM	0:07:05	100
4	2006	16	10/19/2020	1:50:29 PM	1:07:03	100
4	2007	17	10/19/2020	1:54:19 PM	0:03:50	100
4	2008	18	10/19/2020	1:58:24 PM	0:04:05	100
4	2009	19	10/19/2020	2:03:29 PM	0:05:05	100
4	2010	20	10/19/2020	2:06:33 PM	0:03:05	100
4	2011	21	10/19/2020	2:10:23 PM	0:03:50	99
4	2012	22	10/19/2020	2:14:28 PM	0:04:05	100
4	2013	23	10/19/2020	2:18:33 PM	0:04:05	100
4	2014	24	10/19/2020	2:22:23 PM	0:03:50	100
4	2015	25	10/19/2020	2:26:27 PM	0:04:05	100
4	2016	26	10/19/2020	2:30:32 PM	0:04:05	100
4	2017	27	10/19/2020	2:34:23 PM	0:03:51	100
4	2018	28	10/19/2020	2:36:27 PM	0:02:04	33
4	2019	29	10/19/2020	2:40:30 PM	0:04:03	100
4	2020	30	10/19/2020	2:44:20 PM	0:03:51	100
4	2021	31	10/19/2020	2:48:25 PM	0:04:05	99
4	2022	32	10/19/2020	2:51:29 PM	0:03:04	100
4	2023	33	10/19/2020	2:57:21 PM	0:05:52	99
4	2024	34	10/19/2020	2:59:26 PM	0:02:04	100
10	4011	35	10/19/2020	3:05:31 PM	0:06:05	100
4	2025	36	10/19/2020	3:06:20 PM	0:00:49	100
10	4012	37	10/19/2020	3:09:24 PM	0:03:05	100
4	2026	38	10/19/2020	3:10:28 PM	0:01:04	99
10	4013	39	10/19/2020	3:12:33 PM	0:02:04	100

4	2027	40	10/19/2020	3:15:22 PM	0:02:49	100
10	4014	41	10/19/2020	3:16:26 PM	0:01:04	100
4	2028	42	10/19/2020	3:17:33 PM	0:01:07	100
4	2029	43	10/19/2020	3:19:22 PM	0:01:49	25
4	2030	44	10/19/2020	3:22:24 PM	0:03:02	100
10	4015	45	10/19/2020	3:24:29 PM	0:02:04	99
4	2031	46	10/19/2020	3:29:34 PM	0:05:05	100
10	4016	47	10/19/2020	3:30:23 PM	0:00:49	100
4	2032	48	10/19/2020	3:34:28 PM	0:04:05	99
10	4017	49	10/19/2020	3:34:32 PM	0:00:04	100
10	4018	50	10/19/2020	3:40:22 PM	0:05:50	100
10	4019	51	10/19/2020	3:44:26 PM	0:04:05	100
10	4020	52	10/19/2020	3:48:31 PM	0:04:05	99
4	2033	53	10/19/2020	4:00:24 PM	0:11:53	100
10	4021	54	10/19/2020	4:00:43 PM	0:00:19	99
4	2034	55	10/19/2020	4:03:33 PM	0:02:49	100
10	4022	56	10/19/2020	4:03:37 PM	0:00:04	100
10	4023	57	10/19/2020	4:05:26 PM	0:01:49	78
4	2035	58	10/19/2020	4:09:30 PM	0:04:04	100
10	4024	59	10/19/2020	4:09:34 PM	0:00:04	100
10	4025	60	10/19/2020	4:12:24 PM	0:02:50	99
4	2036	61	10/19/2020	4:13:28 PM	0:01:04	100
10	4026	62	10/19/2020	4:15:33 PM	0:02:04	100
4	2037	63	10/19/2020	4:16:22 PM	0:00:49	99
10	4027	64	10/19/2020	4:19:26 PM	0:03:04	100
10	4028	65	10/19/2020	4:22:31 PM	0:03:05	100
4	2038	66	10/19/2020	4:24:20 PM	0:01:50	100
4	2039	67	10/19/2020	4:28:25 PM	0:04:05	100
4	2040	68	10/19/2020	4:32:30 PM	0:04:05	100
4	2041	69	10/19/2020	4:35:22 PM	0:02:52	100
10	4029	70	10/19/2020	4:37:26 PM	0:02:04	100
4	2042	71	10/19/2020	4:41:31 PM	0:04:05	99
10	4030	72	10/19/2020	4:41:35 PM	0:00:04	99
4	2043	73	10/19/2020	4:46:25 PM	0:04:50	100
10	4031	74	10/19/2020	4:49:29 PM	0:03:05	97
10	4032	75	10/19/2020	4:53:34 PM	0:04:05	99
10	4033	76	10/19/2020	4:55:23 PM	0:01:49	100
4	2044	77	10/19/2020	4:57:27 PM	0:02:04	100
10	4034	78	10/19/2020	4:58:32 PM	0:01:04	100
4	2045	79	10/19/2020	5:00:22 PM	0:01:51	99
10	4035	80	10/19/2020	5:03:27 PM	0:03:05	100
10	4036	81	10/19/2020	5:06:31 PM	0:03:05	100
4	2046	82	10/19/2020	5:16:22 PM	0:09:51	99
4	2047	83	10/19/2020	5:18:28 PM	0:02:06	100
10	4037	84	10/19/2020	5:18:32 PM	0:00:04	100

4	2048	85	10/19/2020	5:22:22 PM	0:03:51	99
4	2049	86	10/20/2020	10:05:36 AM	16:43:13	100
4	2050	87	10/20/2020	10:07:25 AM	0:01:49	100
4	2051	88	10/20/2020	10:10:30 AM	0:03:05	99
4	2052	89	10/20/2020	10:13:35 AM	0:03:05	100
4	2053	90	10/20/2020	10:17:26 AM	0:03:51	100
4	2054	91	10/20/2020	10:29:33 AM	0:12:06	100
4	2055	92	10/20/2020	10:32:37 AM	0:03:05	100
4	2056	93	10/20/2020	10:40:29 AM	0:07:51	100
4	2057	94	10/20/2020	10:43:33 AM	0:03:05	100
4	2058	95	10/20/2020	10:50:38 AM	0:07:05	99
4	2059	96	10/20/2020	10:53:28 AM	0:02:49	100
4	2060	97	10/20/2020	10:56:32 AM	0:03:05	100
4	2061	98	10/20/2020	10:59:37 AM	0:03:04	100
4	2062	99	10/20/2020	11:02:27 AM	0:02:50	98
4	2063	100	10/20/2020	11:05:31 AM	0:03:04	100
4	2064	101	10/20/2020	11:08:36 AM	0:03:05	100
4	2065	102	10/20/2020	11:11:26 AM	0:02:50	100
4	2066	103	10/20/2020	11:16:31 AM	0:05:05	100
4	2067	104	10/20/2020	11:19:35 AM	0:03:05	100
4	2068	105	10/20/2020	11:22:40 AM	0:03:05	100
4	2069	106	10/20/2020	11:26:29 AM	0:03:50	99
4	2070	107	10/20/2020	11:30:34 AM	0:04:05	94
4	2071	108	10/20/2020	11:33:38 AM	0:03:04	100
4	2072	109	10/20/2020	11:38:28 AM	0:04:50	100
4	2073	110	10/20/2020	11:43:33 AM	0:05:05	100
10	4038	111	10/20/2020	11:43:37 AM	0:00:04	99
10	4039	112	10/20/2020	11:48:28 AM	0:04:50	100
10	4040	113	10/20/2020	11:50:32 AM	0:02:04	99
4	2074	114	10/20/2020	11:52:36 AM	0:02:04	99
10	4041	115	10/20/2020	11:55:28 AM	0:02:51	100
4	2075	116	10/20/2020	11:56:32 AM	0:01:04	99
10	4042	117	10/20/2020	11:58:36 AM	0:02:04	100
10	4043	118	10/20/2020	12:02:26 PM	0:03:50	100
10	4044	119	10/20/2020	12:05:31 PM	0:03:05	100
4	2076	120	10/20/2020	12:07:35 PM	0:02:04	100
4	2077	121	10/20/2020	12:13:40 PM	0:06:05	100
10	4045	122	10/20/2020	12:13:44 PM	0:00:04	100
4	2078	123	10/20/2020	12:16:34 PM	0:02:50	99
10	4046	124	10/20/2020	12:16:38 PM	0:00:04	100
4	2079	125	10/20/2020	12:19:28 PM	0:02:50	99
10	4047	126	10/20/2020	12:19:46 PM	0:00:19	99
4	2080	127	10/20/2020	12:22:36 PM	0:02:49	99
10	4048	128	10/20/2020	12:22:40 PM	0:00:04	100
4	2081	129	10/20/2020	12:25:30 PM	0:02:50	100

10	4049	130	10/20/2020	12:30:35 PM	0:05:05	100
4	2082	131	10/20/2020	1:08:32 PM	0:37:57	100
10	4050	132	10/20/2020	1:11:37 PM	0:03:05	100
4	2083	133	10/20/2020	1:14:29 PM	0:02:52	100
10	4051	134	10/20/2020	1:14:48 PM	0:00:19	100
4	2084	135	10/20/2020	1:16:37 PM	0:01:49	100
10	4052	136	10/20/2020	1:18:26 PM	0:01:49	100
4	2085	137	10/20/2020	1:20:30 PM	0:02:04	100
10	4053	138	10/20/2020	1:21:35 PM	0:01:04	100
4	2086	139	10/20/2020	1:22:39 PM	0:01:04	100
10	4054	140	10/20/2020	1:27:29 PM	0:04:50	100
10	4055	141	10/20/2020	1:31:34 PM	0:04:05	100
4	2087	142	10/20/2020	1:33:38 PM	0:02:04	98
4	2088	143	10/20/2020	1:37:28 PM	0:03:50	100
10	4056	144	10/20/2020	1:47:34 PM	0:10:06	97
4	2089	145	10/20/2020	1:53:39 PM	0:06:05	100
4	2090	146	10/20/2020	1:58:30 PM	0:04:51	99
10	4057	147	10/20/2020	2:02:35 PM	0:04:05	96
4	2091	148	10/20/2020	2:04:39 PM	0:02:04	100
4	2092	149	10/20/2020	2:07:29 PM	0:02:49	100
10	4058	150	10/20/2020	2:07:47 PM	0:00:18	97
4	2093	151	10/20/2020	2:10:37 PM	0:02:49	100
4	2094	152	10/20/2020	2:14:28 PM	0:03:52	100
4	2095	153	10/20/2020	2:19:33 PM	0:05:05	97
4	2096	154	10/20/2020	2:23:38 PM	0:04:05	99
7	3001	155	10/20/2020	2:26:28 PM	0:02:50	100
7	3002	156	10/20/2020	2:29:32 PM	0:03:05	100
4	2097	157	10/20/2020	2:31:37 PM	0:02:04	100
7	3003	158	10/20/2020	2:32:26 PM	0:00:49	100
7	3004	159	10/20/2020	2:36:31 PM	0:04:05	98
4	2098	160	10/20/2020	2:38:36 PM	0:02:05	100
7	3005	161	10/20/2020	2:39:40 PM	0:01:04	98
4	2099	162	10/20/2020	2:42:29 PM	0:02:49	99
7	3006	163	10/20/2020	2:43:33 PM	0:01:04	100
4	2100	164	10/20/2020	2:46:38 PM	0:03:05	100
7	3007	165	10/20/2020	2:47:27 PM	0:00:49	100
4	2101	166	10/20/2020	2:49:32 PM	0:02:05	100
7	3008	167	10/20/2020	2:51:36 PM	0:02:04	100
4	2102	168	10/20/2020	2:57:29 PM	0:05:53	97
7	3009	169	10/20/2020	2:57:47 PM	0:00:18	95
4	2103	170	10/20/2020	3:00:37 PM	0:02:49	99
7	3010	171	10/20/2020	3:01:41 PM	0:01:04	99
4	2104	172	10/20/2020	3:04:33 PM	0:02:53	99
7	3011	173	10/20/2020	3:04:37 PM	0:00:04	98
4	2105	174	10/20/2020	3:07:28 PM	0:02:51	100

7	3012	175	10/20/2020	3:07:47 PM	0:00:19	100
7	3013	176	10/20/2020	3:10:36 PM	0:02:50	98
4	2106	177	10/20/2020	3:12:41 PM	0:02:04	95
7	3014	178	10/20/2020	3:13:30 PM	0:00:49	100
4	2107	179	10/20/2020	3:21:35 PM	0:08:06	95
7	3015	180	10/20/2020	3:23:39 PM	0:02:04	94
4	2108	181	10/20/2020	3:25:30 PM	0:01:50	100
7	3016	182	10/20/2020	3:25:50 PM	0:00:20	100
7	3017	183	10/20/2020	3:29:39 PM	0:03:50	100
4	2109	184	10/20/2020	3:30:29 PM	0:00:50	94
7	3018	185	10/20/2020	3:35:34 PM	0:05:05	97
7	3019	186	10/20/2020	3:59:43 PM	0:24:09	95
2	1001	187	10/20/2020	4:02:32 PM	0:02:49	75
7	3020	188	10/20/2020	4:03:36 PM	0:01:03	99
7	3021	189	10/20/2020	4:06:40 PM	0:03:04	99
7	3022	190	10/20/2020	4:10:30 PM	0:03:50	99
7	3023	191	10/20/2020	4:13:34 PM	0:03:05	100
7	3024	192	10/20/2020	4:22:40 PM	0:09:06	99
4	2110	193	10/20/2020	4:24:30 PM	0:01:50	98
7	3025	194	10/20/2020	4:26:34 PM	0:02:04	100
4	2111	195	10/20/2020	4:28:38 PM	0:02:04	100
7	3026	196	10/20/2020	4:29:30 PM	0:00:51	100
7	3027	197	10/20/2020	4:34:35 PM	0:05:05	100
7	3028	198	10/20/2020	4:38:39 PM	0:04:05	100
2	1002	199	10/20/2020	4:46:29 PM	0:07:50	21
2	1003	200	10/20/2020	4:56:34 PM	0:10:04	75
2	1004	201	10/20/2020	4:57:37 PM	0:01:03	80
4	2112	202	10/21/2020	9:05:41 AM	16:08:04	99
4	2113	203	10/21/2020	9:07:45 AM	0:02:04	95
4	2114	204	10/21/2020	9:10:35 AM	0:02:50	98
4	2115	205	10/21/2020	9:14:40 AM	0:04:05	96
4	2116	206	10/21/2020	9:18:45 AM	0:04:05	99
4	2117	207	10/21/2020	9:20:34 AM	0:01:49	100
4	2118	208	10/21/2020	9:22:38 AM	0:02:04	100
4	2119	209	10/21/2020	9:28:44 AM	0:06:05	100
4	2120	210	10/21/2020	9:33:35 AM	0:04:51	100
4	2121	211	10/21/2020	9:36:39 AM	0:03:04	100
4	2122	212	10/21/2020	9:39:44 AM	0:03:05	100
4	2123	213	10/21/2020	9:42:35 AM	0:02:51	100
2	1005	214	10/21/2020	9:50:40 AM	0:08:05	68
2	1006	215	10/21/2020	9:54:43 AM	0:04:03	37
2	1007	216	10/21/2020	9:56:45 AM	0:02:02	76
2	1008	217	10/21/2020	10:14:37 AM	0:17:51	14
10	4059	218	10/21/2020	10:16:39 AM	0:02:02	100
10	4060	219	10/21/2020	10:25:45 AM	0:09:06	100

10	4061	220	10/21/2020	10:28:34 AM	0:02:50	100
10	4062	221	10/21/2020	10:32:39 AM	0:04:05	98
10	4063	222	10/21/2020	10:34:43 AM	0:02:04	100
10	4064	223	10/21/2020	10:37:35 AM	0:02:51	100
10	4065	224	10/21/2020	10:40:39 AM	0:03:05	100
10	4066	225	10/21/2020	10:43:44 AM	0:03:05	100
10	4067	226	10/21/2020	10:47:34 AM	0:03:51	99
10	4068	227	10/21/2020	10:51:39 AM	0:04:05	100
10	4069	228	10/21/2020	10:56:44 AM	0:05:05	100
10	4070	229	10/21/2020	10:59:33 AM	0:02:49	100
10	4071	230	10/21/2020	11:02:38 AM	0:03:05	99
10	4072	231	10/21/2020	11:05:42 AM	0:03:05	100
10	4073	232	10/21/2020	11:21:37 AM	0:15:54	100
10	4074	233	10/21/2020	11:27:42 AM	0:06:05	100
10	4075	234	10/21/2020	11:35:47 AM	0:08:06	97
10	4076	235	10/21/2020	11:38:37 AM	0:02:49	100
10	4077	236	10/21/2020	11:41:41 AM	0:03:05	100
10	4078	237	10/21/2020	11:46:46 AM	0:05:05	100
10	4079	238	10/21/2020	11:49:36 AM	0:02:50	100
10	4080	239	10/21/2020	11:53:41 AM	0:04:05	100
10	4081	240	10/21/2020	12:00:46 PM	0:07:05	101
10	4082	241	10/21/2020	12:02:36 PM	0:01:49	100
10	4083	242	10/21/2020	12:05:40 PM	0:03:05	100
10	4084	243	10/21/2020	12:08:45 PM	0:03:05	100
10	4085	244	10/21/2020	12:12:35 PM	0:03:50	100
10	4086	245	10/21/2020	12:15:40 PM	0:03:05	98
10	4087	246	10/21/2020	12:50:37 PM	0:34:57	98
10	4088	247	10/21/2020	12:53:41 PM	0:03:04	95
10	4089	248	10/21/2020	12:55:46 PM	0:02:04	97
10	4090	249	10/21/2020	12:58:35 PM	0:02:50	98
10	4091	250	10/21/2020	1:03:42 PM	0:05:06	95
10	4092	251	10/21/2020	1:08:46 PM	0:05:05	98
10	4093	252	10/21/2020	1:10:37 PM	0:01:50	98
10	4094	253	10/21/2020	1:13:41 PM	0:03:04	95
10	4095	254	10/21/2020	1:16:45 PM	0:03:04	97
10	4096	255	10/21/2020	1:19:35 PM	0:02:50	96
10	4097	256	10/21/2020	1:23:41 PM	0:04:05	95
10	4098	257	10/21/2020	1:28:46 PM	0:05:05	100
10	4099	258	10/21/2020	1:29:34 PM	0:00:49	63
10	4100	259	10/21/2020	1:34:38 PM	0:05:04	100
7	3029	260	10/21/2020	1:50:46 PM	0:16:07	100
7	3030	261	10/21/2020	1:53:37 PM	0:02:51	100
7	3031	262	10/21/2020	1:57:42 PM	0:04:05	100
7	3032	263	10/21/2020	2:00:50 PM	0:03:09	100
7	3033	264	10/21/2020	2:05:40 PM	0:04:50	100

7	3034	265	10/21/2020	2:08:46 PM	0:03:05	100
7	3035	266	10/21/2020	2:11:35 PM	0:02:50	100
7	3036	267	10/21/2020	2:14:40 PM	0:03:05	99

**APPENDIX B - BATCHES - NEW ADJUDICATION DATABASE
(WITH TIME BETWEEN BATCHES) - NOVEMBER 2020 ELECTION**

TabulatorId	BatchId	CvrBatchId	LoadOrder	Creation Date	Creation Time	Difference from Prior	Ballots
10	4001	1	1	10/21/2020	2:20:07 PM		100
10	4025	60	60	10/21/2020	2:20:26 PM	0:00:19	99
4	2036	61	61	10/21/2020	2:20:30 PM	0:00:04	100
10	4026	62	62	10/21/2020	2:20:34 PM	0:00:04	100
4	2037	63	63	10/21/2020	2:20:39 PM	0:00:05	99
10	4027	64	64	10/21/2020	2:20:43 PM	0:00:04	100
10	4028	65	65	10/21/2020	2:20:47 PM	0:00:04	100
4	2038	66	66	10/21/2020	2:20:52 PM	0:00:04	100
4	2039	67	67	10/21/2020	2:20:56 PM	0:00:04	100
4	2040	68	68	10/21/2020	2:21:00 PM	0:00:04	100
4	2041	69	69	10/21/2020	2:21:04 PM	0:00:04	100
10	4029	70	70	10/21/2020	2:21:08 PM	0:00:04	100
4	2042	71	71	10/21/2020	2:21:13 PM	0:00:04	99
10	4030	72	72	10/21/2020	2:21:17 PM	0:00:04	99
4	2043	73	73	10/21/2020	2:21:21 PM	0:00:04	100
10	4031	74	74	10/21/2020	2:21:25 PM	0:00:04	97
10	4032	75	75	10/21/2020	2:21:29 PM	0:00:05	99
10	4033	76	76	10/21/2020	2:21:34 PM	0:00:04	100
4	2044	77	77	10/21/2020	2:21:40 PM	0:00:06	100
10	4034	78	78	10/21/2020	2:21:44 PM	0:00:04	100
4	2045	79	79	10/21/2020	2:21:48 PM	0:00:04	99
10	4035	80	80	10/21/2020	2:21:53 PM	0:00:05	100
10	4036	81	81	10/21/2020	2:21:57 PM	0:00:04	100
4	2046	82	82	10/21/2020	2:22:01 PM	0:00:04	99
4	2047	83	83	10/21/2020	2:22:05 PM	0:00:04	100
10	4037	84	84	10/21/2020	2:22:09 PM	0:00:04	100
4	2048	85	85	10/21/2020	2:22:13 PM	0:00:04	99
4	2049	86	86	10/21/2020	2:22:17 PM	0:00:04	100
4	2050	87	87	10/21/2020	2:22:21 PM	0:00:04	100
4	2051	88	88	10/21/2020	2:22:25 PM	0:00:04	99
4	2052	89	89	10/21/2020	2:22:30 PM	0:00:04	100
4	2053	90	90	10/21/2020	2:22:34 PM	0:00:04	100
4	2054	91	91	10/21/2020	2:22:38 PM	0:00:04	100
4	2055	92	92	10/21/2020	2:22:42 PM	0:00:04	100
4	2056	93	93	10/21/2020	2:22:46 PM	0:00:04	100
4	2057	94	94	10/21/2020	2:22:50 PM	0:00:04	100
4	2058	95	95	10/21/2020	2:22:54 PM	0:00:04	99
4	2059	96	96	10/21/2020	2:22:58 PM	0:00:04	100
4	2060	97	97	10/21/2020	2:23:02 PM	0:00:04	100

4	2061	98	98	10/21/2020	2:23:06 PM	0:00:04	100
4	2062	99	99	10/21/2020	2:23:11 PM	0:00:04	98
4	2063	100	100	10/21/2020	2:23:15 PM	0:00:04	100
4	2064	101	101	10/21/2020	2:23:19 PM	0:00:04	100
4	2065	102	102	10/21/2020	2:23:23 PM	0:00:04	100
4	2066	103	103	10/21/2020	2:23:28 PM	0:00:05	100
4	2067	104	104	10/21/2020	2:23:34 PM	0:00:06	100
4	2068	105	105	10/21/2020	2:23:38 PM	0:00:04	100
4	2069	106	106	10/21/2020	2:23:42 PM	0:00:04	99
4	2070	107	107	10/21/2020	2:23:46 PM	0:00:04	94
4	2071	108	108	10/21/2020	2:23:50 PM	0:00:04	100
4	2072	109	109	10/21/2020	2:23:54 PM	0:00:04	100
4	2073	110	110	10/21/2020	2:23:58 PM	0:00:04	100
10	4038	111	111	10/21/2020	2:24:02 PM	0:00:04	99
10	4039	112	112	10/21/2020	2:24:06 PM	0:00:04	100
10	4040	113	113	10/21/2020	2:24:10 PM	0:00:04	99
4	2074	114	114	10/21/2020	2:24:14 PM	0:00:04	99
10	4041	115	115	10/21/2020	2:24:18 PM	0:00:04	100
4	2075	116	116	10/21/2020	2:24:22 PM	0:00:04	99
10	4042	117	117	10/21/2020	2:24:26 PM	0:00:04	100
10	4043	118	118	10/21/2020	2:24:31 PM	0:00:05	100
10	4044	119	119	10/21/2020	2:24:35 PM	0:00:04	100
4	2076	120	120	10/21/2020	2:24:39 PM	0:00:04	100
4	2077	121	121	10/21/2020	2:24:43 PM	0:00:04	100
10	4045	122	122	10/21/2020	2:24:48 PM	0:00:04	100
4	2078	123	123	10/21/2020	2:24:52 PM	0:00:04	99
10	4046	124	124	10/21/2020	2:24:56 PM	0:00:05	100
4	2079	125	125	10/21/2020	2:25:00 PM	0:00:04	99
10	4047	126	126	10/21/2020	2:25:05 PM	0:00:04	99
4	2080	127	127	10/21/2020	2:25:09 PM	0:00:04	99
10	4048	128	128	10/21/2020	2:25:13 PM	0:00:04	100
4	2081	129	129	10/21/2020	2:25:17 PM	0:00:04	100
10	4049	130	130	10/21/2020	2:25:22 PM	0:00:05	100
4	2082	131	131	10/21/2020	2:25:26 PM	0:00:04	100
10	4050	132	132	10/21/2020	2:25:30 PM	0:00:04	100
4	2083	133	133	10/21/2020	2:25:35 PM	0:00:04	100
10	4051	134	134	10/21/2020	2:25:39 PM	0:00:04	100
4	2084	135	135	10/21/2020	2:25:44 PM	0:00:05	100
10	4052	136	136	10/21/2020	2:25:49 PM	0:00:05	100
4	2085	137	137	10/21/2020	2:25:53 PM	0:00:04	100
10	4053	138	138	10/21/2020	2:25:57 PM	0:00:04	100
4	2086	139	139	10/21/2020	2:26:01 PM	0:00:04	100
10	4054	140	140	10/21/2020	2:26:05 PM	0:00:04	100
10	4055	141	141	10/21/2020	2:26:09 PM	0:00:04	100
4	2087	142	142	10/21/2020	2:26:13 PM	0:00:04	98

4	2088	143	143	10/21/2020	2:26:17 PM	0:00:04	100
10	4056	144	144	10/21/2020	2:26:21 PM	0:00:04	97
4	2089	145	145	10/21/2020	2:26:25 PM	0:00:04	100
4	2090	146	146	10/21/2020	2:26:29 PM	0:00:04	99
10	4057	147	147	10/21/2020	2:26:33 PM	0:00:04	96
4	2091	148	148	10/21/2020	2:26:37 PM	0:00:04	100
4	2092	149	149	10/21/2020	2:26:41 PM	0:00:04	100
10	4058	150	150	10/21/2020	2:26:45 PM	0:00:04	97
4	2093	151	151	10/21/2020	2:26:49 PM	0:00:04	100
4	2094	152	152	10/21/2020	2:26:53 PM	0:00:04	100
4	2095	153	153	10/21/2020	2:26:58 PM	0:00:04	97
4	2096	154	154	10/21/2020	2:27:02 PM	0:00:04	99
7	3001	155	155	10/21/2020	2:27:06 PM	0:00:04	100
7	3002	156	156	10/21/2020	2:27:10 PM	0:00:04	100
4	2097	157	157	10/21/2020	2:27:14 PM	0:00:04	100
7	3003	158	158	10/21/2020	2:27:18 PM	0:00:04	100
7	3004	159	159	10/21/2020	2:27:22 PM	0:00:04	98
4	2098	160	160	10/21/2020	2:27:26 PM	0:00:04	100
7	3005	161	161	10/21/2020	2:27:30 PM	0:00:04	98
4	2099	162	162	10/21/2020	2:27:35 PM	0:00:04	99
7	3006	163	163	10/21/2020	2:27:39 PM	0:00:04	100
4	2100	164	164	10/21/2020	2:27:43 PM	0:00:04	100
7	3007	165	165	10/21/2020	2:27:47 PM	0:00:04	100
4	2101	166	166	10/21/2020	2:27:53 PM	0:00:06	100
7	3008	167	167	10/21/2020	2:27:58 PM	0:00:05	100
4	2102	168	168	10/21/2020	2:28:02 PM	0:00:04	97
7	3009	169	169	10/21/2020	2:28:06 PM	0:00:04	95
4	2103	170	170	10/21/2020	2:28:10 PM	0:00:04	99
7	3010	171	171	10/21/2020	2:28:14 PM	0:00:04	99
4	2104	172	172	10/21/2020	2:28:18 PM	0:00:04	99
7	3011	173	173	10/21/2020	2:28:22 PM	0:00:04	98
4	2105	174	174	10/21/2020	2:28:26 PM	0:00:04	100
7	3012	175	175	10/21/2020	2:28:30 PM	0:00:04	100
7	3013	176	176	10/21/2020	2:28:34 PM	0:00:04	98
4	2106	177	177	10/21/2020	2:28:38 PM	0:00:04	95
7	3014	178	178	10/21/2020	2:28:42 PM	0:00:04	100
4	2107	179	179	10/21/2020	2:28:47 PM	0:00:04	95
7	3015	180	180	10/21/2020	2:28:50 PM	0:00:04	94
4	2108	181	181	10/21/2020	2:28:54 PM	0:00:04	100
7	3016	182	182	10/21/2020	2:28:58 PM	0:00:04	100
7	3017	183	183	10/21/2020	2:29:02 PM	0:00:04	100
4	2109	184	184	10/21/2020	2:29:06 PM	0:00:04	94
7	3018	185	185	10/21/2020	2:29:10 PM	0:00:04	97
7	3019	186	186	10/21/2020	2:29:15 PM	0:00:05	95
2	1001	187	187	10/21/2020	2:29:19 PM	0:00:04	75

7	3020	188	188	10/21/2020	2:29:22 PM	0:00:03	99
7	3021	189	189	10/21/2020	2:29:26 PM	0:00:04	99
7	3022	190	190	10/21/2020	2:29:31 PM	0:00:04	99
7	3023	191	191	10/21/2020	2:29:35 PM	0:00:04	100
7	3024	192	192	10/21/2020	2:29:40 PM	0:00:05	99
4	2110	193	193	10/21/2020	2:29:44 PM	0:00:04	98
7	3025	194	194	10/21/2020	2:29:48 PM	0:00:05	100
4	2111	195	195	10/21/2020	2:29:53 PM	0:00:04	100
7	3026	196	196	10/21/2020	2:29:57 PM	0:00:04	100
7	3027	197	197	10/21/2020	2:30:01 PM	0:00:04	100
7	3028	198	198	10/21/2020	2:30:05 PM	0:00:04	100
2	1002	199	199	10/21/2020	2:30:09 PM	0:00:04	21
2	1003	200	200	10/21/2020	2:30:10 PM	0:00:02	75
2	1004	201	201	10/21/2020	2:30:14 PM	0:00:04	80
4	2112	202	202	10/21/2020	2:30:17 PM	0:00:03	99
4	2113	203	203	10/21/2020	2:30:22 PM	0:00:04	95
4	2114	204	204	10/21/2020	2:30:25 PM	0:00:04	98
4	2115	205	205	10/21/2020	2:30:29 PM	0:00:04	96
4	2116	206	206	10/21/2020	2:30:34 PM	0:00:04	99
4	2117	207	207	10/21/2020	2:30:38 PM	0:00:04	100
4	2118	208	208	10/21/2020	2:30:42 PM	0:00:04	100
4	2119	209	209	10/21/2020	2:30:46 PM	0:00:04	100
4	2120	210	210	10/21/2020	2:30:50 PM	0:00:04	100
4	2121	211	211	10/21/2020	2:30:54 PM	0:00:04	100
4	2122	212	212	10/21/2020	2:30:59 PM	0:00:04	100
4	2123	213	213	10/21/2020	2:31:03 PM	0:00:04	100
2	1005	214	214	10/21/2020	2:31:06 PM	0:00:04	68
2	1006	215	215	10/21/2020	2:31:09 PM	0:00:03	37
2	1007	216	216	10/21/2020	2:31:11 PM	0:00:02	76
2	1008	217	217	10/21/2020	2:31:14 PM	0:00:03	14
10	4059	218	218	10/21/2020	2:31:15 PM	0:00:01	100
10	4060	219	219	10/21/2020	2:31:20 PM	0:00:04	100
10	4061	220	220	10/21/2020	2:31:24 PM	0:00:04	100
10	4062	221	221	10/21/2020	2:31:28 PM	0:00:04	98
10	4063	222	222	10/21/2020	2:31:32 PM	0:00:04	100
10	4064	223	223	10/21/2020	2:31:36 PM	0:00:04	100
10	4065	224	224	10/21/2020	2:31:40 PM	0:00:04	100
10	4066	225	225	10/21/2020	2:31:44 PM	0:00:04	100
10	4067	226	226	10/21/2020	2:31:49 PM	0:00:04	99
10	4068	227	227	10/21/2020	2:31:53 PM	0:00:04	100
10	4069	228	228	10/21/2020	2:31:57 PM	0:00:04	100
10	4070	229	229	10/21/2020	2:32:02 PM	0:00:04	100
10	4071	230	230	10/21/2020	2:32:06 PM	0:00:04	99
10	4072	231	231	10/21/2020	2:32:10 PM	0:00:04	100
10	4073	232	232	10/21/2020	2:32:15 PM	0:00:05	100

10	4074	233	233	10/21/2020	2:32:19 PM	0:00:04	100
10	4075	234	234	10/21/2020	2:32:23 PM	0:00:04	97
10	4076	235	235	10/21/2020	2:32:27 PM	0:00:04	100
10	4077	236	236	10/21/2020	2:32:32 PM	0:00:05	100
10	4078	237	237	10/21/2020	2:32:36 PM	0:00:04	100
10	4079	238	238	10/21/2020	2:32:40 PM	0:00:04	100
10	4080	239	239	10/21/2020	2:32:44 PM	0:00:04	100
10	4081	240	240	10/21/2020	2:32:49 PM	0:00:04	101
10	4082	241	241	10/21/2020	2:32:53 PM	0:00:04	100
10	4083	242	242	10/21/2020	2:32:57 PM	0:00:04	100
10	4084	243	243	10/21/2020	2:33:02 PM	0:00:05	100
10	4085	244	244	10/21/2020	2:33:06 PM	0:00:04	100
10	4086	245	245	10/21/2020	2:33:11 PM	0:00:05	98
10	4087	246	246	10/21/2020	2:33:15 PM	0:00:04	98
10	4088	247	247	10/21/2020	2:33:19 PM	0:00:04	95
10	4089	248	248	10/21/2020	2:33:23 PM	0:00:04	97
10	4090	249	249	10/21/2020	2:33:27 PM	0:00:05	98
10	4091	250	250	10/21/2020	2:33:31 PM	0:00:04	95
10	4092	251	251	10/21/2020	2:33:35 PM	0:00:04	98
10	4093	252	252	10/21/2020	2:33:39 PM	0:00:05	98
10	4094	253	253	10/21/2020	2:33:43 PM	0:00:04	95
10	4095	254	254	10/21/2020	2:33:47 PM	0:00:04	97
10	4096	255	255	10/21/2020	2:33:51 PM	0:00:04	96
10	4097	256	256	10/21/2020	2:33:55 PM	0:00:04	95
10	4098	257	257	10/21/2020	2:33:59 PM	0:00:04	100
10	4099	258	258	10/21/2020	2:34:03 PM	0:00:04	63
10	4100	259	259	10/21/2020	2:34:06 PM	0:00:03	100
7	3029	260	260	10/21/2020	2:34:10 PM	0:00:04	100
7	3030	261	261	10/21/2020	2:34:14 PM	0:00:04	100
7	3031	262	262	10/21/2020	2:34:18 PM	0:00:04	100
7	3032	263	263	10/21/2020	2:34:22 PM	0:00:04	100
7	3033	264	264	10/21/2020	2:34:26 PM	0:00:04	100
7	3034	265	265	10/21/2020	2:34:30 PM	0:00:04	100
7	3035	266	266	10/21/2020	2:34:34 PM	0:00:04	100
7	3036	267	267	10/21/2020	2:34:38 PM	0:00:04	99
7	3037	268	268	10/21/2020	2:34:42 PM	0:00:04	100
7	3038	269	269	10/21/2020	2:39:47 PM	0:05:05	100
7	3039	270	270	10/21/2020	2:45:38 PM	0:05:50	100
7	3040	271	271	10/21/2020	2:48:42 PM	0:03:05	99
7	3041	272	272	10/21/2020	2:51:47 PM	0:03:05	100
7	3042	273	273	10/21/2020	2:55:39 PM	0:03:52	100
7	3043	274	274	10/21/2020	3:03:44 PM	0:08:06	99
7	3044	275	275	10/21/2020	3:08:37 PM	0:04:52	100
7	3045	276	276	10/21/2020	3:15:42 PM	0:07:05	100
7	3046	277	277	10/21/2020	3:25:48 PM	0:10:06	99

7	3047	278	278	10/21/2020	3:30:39 PM	0:04:51	100
7	3048	279	279	10/21/2020	3:33:43 PM	0:03:05	100
7	3049	280	280	10/21/2020	3:39:50 PM	0:06:06	99
7	3050	281	281	10/21/2020	3:42:39 PM	0:02:49	98
7	3051	282	282	10/21/2020	3:45:43 PM	0:03:04	99
7	3052	283	283	10/21/2020	3:49:48 PM	0:04:05	100
7	3053	284	284	10/21/2020	3:52:38 PM	0:02:49	99
7	3054	285	285	10/21/2020	3:56:43 PM	0:04:05	100
7	3055	286	286	10/21/2020	3:58:47 PM	0:02:04	100
4	2124	287	287	10/21/2020	4:06:38 PM	0:07:52	100
4	2125	288	288	10/21/2020	4:08:43 PM	0:02:04	100
4	2126	289	289	10/21/2020	4:11:48 PM	0:03:05	100
4	2127	290	290	10/21/2020	4:19:38 PM	0:07:51	98
4	2128	291	291	10/21/2020	4:23:43 PM	0:04:05	100
4	2129	292	292	10/21/2020	4:27:48 PM	0:04:05	100
4	2130	293	293	10/21/2020	4:30:37 PM	0:02:50	100
4	2131	294	294	10/21/2020	4:35:42 PM	0:05:05	99
4	2132	295	295	10/21/2020	4:39:47 PM	0:04:05	100
4	2133	296	296	10/21/2020	4:44:37 PM	0:04:50	99
4	2134	297	297	10/21/2020	4:47:42 PM	0:03:05	99
4	2135	298	298	10/21/2020	4:51:47 PM	0:04:05	100
4	2136	299	299	10/21/2020	4:55:38 PM	0:03:51	100
4	2137	300	300	10/21/2020	5:00:42 PM	0:05:05	100
4	2138	301	301	10/21/2020	5:03:47 PM	0:03:04	100
4	2139	302	302	10/21/2020	5:06:36 PM	0:02:50	100
4	2140	303	303	10/21/2020	5:09:41 PM	0:03:04	98
4	2141	304	304	10/21/2020	5:12:45 PM	0:03:05	100
4	2142	305	305	10/21/2020	5:17:36 PM	0:04:50	100
4	2143	306	306	10/21/2020	5:24:41 PM	0:07:05	99
10	4101	307	307	10/22/2020	8:33:49 AM		100
10	4102	308	308	10/22/2020	8:41:55 AM	0:08:06	96
10	4103	309	309	10/22/2020	8:49:45 AM	0:07:50	98
4	2144	310	310	10/22/2020	8:50:50 AM	0:01:05	100
4	2145	311	311	10/22/2020	8:53:41 AM	0:02:51	100
10	4104	312	312	10/22/2020	8:56:45 AM	0:03:05	100
4	2146	313	313	10/22/2020	9:01:50 AM	0:05:05	99
4	2147	314	314	10/22/2020	9:08:43 AM	0:06:53	96
4	2148	315	315	10/22/2020	9:13:48 AM	0:05:05	100
10	4105	316	316	10/22/2020	9:14:52 AM	0:01:04	100
10	4106	317	317	10/22/2020	9:20:43 AM	0:05:51	100
4	2149	318	318	10/22/2020	9:21:47 AM	0:01:04	96
10	4107	319	319	10/22/2020	9:24:52 AM	0:03:04	100
4	2150	320	320	10/22/2020	9:29:41 AM	0:04:50	99
10	4108	321	321	10/22/2020	9:30:46 AM	0:01:04	100
4	2151	322	322	10/22/2020	9:32:50 AM	0:02:04	100

10	4109	323	323	10/22/2020	9:35:54 AM	0:03:05	100
4	2152	324	324	10/22/2020	9:39:44 AM	0:03:50	100
10	4110	325	325	10/22/2020	9:40:48 AM	0:01:04	100
4	2153	326	326	10/22/2020	9:43:53 AM	0:03:05	100
10	4111	327	327	10/22/2020	9:44:42 AM	0:00:50	100
4	2154	328	328	10/22/2020	9:46:47 AM	0:02:04	100
10	4112	329	329	10/22/2020	9:48:51 AM	0:02:04	100
4	2155	330	330	10/22/2020	9:52:41 AM	0:03:50	100
10	4113	331	331	10/22/2020	9:52:59 AM	0:00:18	100
4	2156	332	332	10/22/2020	9:55:48 AM	0:02:49	99
10	4114	333	333	10/22/2020	9:56:52 AM	0:01:04	100
4	2157	334	334	10/22/2020	9:58:41 AM	0:01:49	100
10	4115	335	335	10/22/2020	10:00:46 AM	0:02:04	100
4	2158	336	336	10/22/2020	10:01:50 AM	0:01:05	100
4	2159	337	337	10/22/2020	10:04:42 AM	0:02:52	100
4	2160	338	338	10/22/2020	10:09:47 AM	0:05:05	100
4	2161	339	339	10/22/2020	10:12:52 AM	0:03:05	100
4	2162	340	340	10/22/2020	10:15:42 AM	0:02:51	100
10	4116	341	341	10/22/2020	10:18:47 AM	0:03:05	99
4	2163	342	342	10/22/2020	10:20:51 AM	0:02:04	100
10	4117	343	343	10/22/2020	10:20:55 AM	0:00:04	100
10	4118	344	344	10/22/2020	10:24:45 AM	0:03:50	100
10	4119	345	345	10/22/2020	10:28:50 AM	0:04:05	100
4	2164	346	346	10/22/2020	10:31:54 AM	0:03:04	99
10	4120	347	347	10/22/2020	10:32:42 AM	0:00:48	100
10	4121	348	348	10/22/2020	10:36:46 AM	0:04:04	100
4	2165	349	349	10/22/2020	10:37:50 AM	0:01:04	92
10	4122	350	350	10/22/2020	10:41:42 AM	0:03:51	100
4	2166	351	351	10/22/2020	10:44:46 AM	0:03:05	95
10	4123	352	352	10/22/2020	10:46:51 AM	0:02:04	100
4	2167	353	353	10/22/2020	10:52:40 AM	0:05:50	46
4	2168	354	354	10/22/2020	10:57:44 AM	0:05:04	65
4	2169	355	355	10/22/2020	11:08:49 AM	0:11:05	85
4	2170	356	356	10/22/2020	11:09:53 AM	0:01:04	85
4	2171	357	357	10/22/2020	11:11:42 AM	0:01:49	78
2	1009	358	358	10/22/2020	11:21:47 AM	0:10:05	26
2	1010	359	359	10/22/2020	11:22:48 AM	0:01:02	66
2	1011	360	360	10/22/2020	11:26:52 AM	0:04:04	100
2	1012	361	361	10/22/2020	11:28:41 AM	0:01:49	31
4	2172	362	362	10/22/2020	12:22:41 PM	0:54:01	60
4	2173	363	363	10/22/2020	3:01:48 PM	2:39:07	100
4	2174	364	364	10/22/2020	3:07:53 PM	0:06:05	99
4	2175	365	365	10/22/2020	3:12:43 PM	0:04:50	100
4	2176	366	366	10/22/2020	3:16:48 PM	0:04:05	100
4	2177	367	367	10/22/2020	3:18:53 PM	0:02:04	100

4	2178	368	368	10/22/2020	3:21:44 PM	0:02:51	100
4	2179	369	369	10/22/2020	3:26:49 PM	0:05:05	100
4	2180	370	370	10/22/2020	3:31:54 PM	0:05:05	100
4	2181	371	371	10/22/2020	3:37:44 PM	0:05:51	99
4	2182	372	372	10/22/2020	3:40:49 PM	0:03:05	100
4	2183	373	373	10/22/2020	3:43:54 PM	0:03:05	100
4	2184	374	374	10/22/2020	3:46:44 PM	0:02:50	100
10	4124	375	375	10/22/2020	4:19:55 PM	0:33:11	99
10	4125	376	376	10/22/2020	4:35:48 PM	0:15:53	85
10	4126	377	377	10/22/2020	4:37:52 PM	0:02:04	87
10	4127	378	378	10/22/2020	4:39:56 PM	0:02:04	100
10	4128	379	379	10/22/2020	4:42:45 PM	0:02:50	100
10	4129	380	380	10/22/2020	4:45:50 PM	0:03:04	100
10	4130	381	381	10/22/2020	4:48:54 PM	0:03:05	100
10	4131	382	382	10/22/2020	4:54:45 PM	0:05:51	100
10	4132	383	383	10/22/2020	4:57:49 PM	0:03:05	100
4	2185	384	384	10/22/2020	5:03:54 PM	0:06:05	98
4	2186	385	385	10/22/2020	5:06:44 PM	0:02:50	100
4	2187	386	386	10/22/2020	5:13:50 PM	0:07:05	100
4	2188	387	387	10/22/2020	5:18:55 PM	0:05:05	100
4	2189	388	388	10/22/2020	5:21:45 PM	0:02:50	100
4	2190	389	389	10/22/2020	5:24:50 PM	0:03:05	100
4	2191	390	390	10/22/2020	5:31:55 PM	0:07:05	99
4	2192	391	391	10/22/2020	5:36:45 PM	0:04:50	88
4	2193	392	392	10/22/2020	5:40:49 PM	0:04:04	100
4	2194	393	393	10/22/2020	5:43:54 PM	0:03:05	100
4	2195	394	394	10/22/2020	5:46:44 PM	0:02:50	100
4	2196	395	395	10/22/2020	5:49:48 PM	0:03:05	100
4	2197	396	396	10/22/2020	6:01:54 PM	0:12:06	24
4	2198	397	397	10/26/2020	10:25:50 AM		100
4	2199	398	398	10/26/2020	10:27:54 AM	0:02:04	100
4	2200	399	399	10/26/2020	10:30:45 AM	0:02:51	100
10	4133	400	400	10/26/2020	10:32:49 AM	0:02:04	99
4	2201	401	401	10/26/2020	10:33:54 AM	0:01:05	100
10	4134	402	402	10/26/2020	10:36:44 AM	0:02:49	99
4	2202	403	403	10/26/2020	10:37:48 AM	0:01:04	99
10	4135	404	404	10/26/2020	10:40:52 AM	0:03:05	100
4	2203	405	405	10/26/2020	10:43:42 AM	0:02:50	100
10	4136	406	406	10/26/2020	10:44:46 AM	0:01:04	100
4	2204	407	407	10/26/2020	10:46:51 AM	0:02:04	100
10	4137	408	408	10/26/2020	10:48:41 AM	0:01:50	100
4	2205	409	409	10/26/2020	10:49:45 AM	0:01:04	100
10	4138	410	410	10/26/2020	10:51:50 AM	0:02:04	100
2	1013	411	411	10/26/2020	10:53:40 AM	0:01:50	66
10	4139	412	412	10/26/2020	10:55:44 AM	0:02:04	100

2	1014	413	413	10/26/2020	10:58:48 AM	0:03:04	59
10	4140	414	414	10/26/2020	10:58:51 AM	0:00:02	55
2	1015	415	415	10/26/2020	11:02:40 AM	0:03:49	57
2	1016	416	416	10/26/2020	11:04:44 AM	0:02:03	87
2	1017	417	417	10/26/2020	11:06:48 AM	0:02:04	95
2	1018	418	418	10/26/2020	11:09:52 AM	0:03:04	97
2	1019	419	419	10/26/2020	11:12:41 AM	0:02:49	43
10	4141	420	420	10/26/2020	1:13:55 PM	2:01:14	99
10	4142	421	421	10/26/2020	1:17:45 PM	0:03:50	99
10	4143	422	422	10/26/2020	1:24:50 PM	0:07:05	100
10	4144	423	423	10/26/2020	1:28:55 PM	0:04:05	100
10	4145	424	424	10/26/2020	1:31:44 PM	0:02:50	100
10	4146	425	425	10/26/2020	1:34:49 PM	0:03:05	100
10	4147	426	426	10/26/2020	1:41:54 PM	0:07:05	100
4	2206	427	427	10/26/2020	1:42:45 PM	0:00:51	98
10	4148	428	428	10/26/2020	1:45:50 PM	0:03:04	99
10	4149	429	429	10/26/2020	1:49:54 PM	0:04:05	100
10	4150	430	430	10/26/2020	1:53:44 PM	0:03:50	99
4	2207	431	431	10/26/2020	1:56:49 PM	0:03:05	99
4	2208	432	432	10/26/2020	1:59:53 PM	0:03:05	100
4	2209	433	433	10/26/2020	2:02:43 PM	0:02:50	99
4	2210	434	434	10/26/2020	2:05:49 PM	0:03:05	100
4	2211	435	435	10/26/2020	2:08:53 PM	0:03:05	100
10	4151	436	436	10/26/2020	2:27:47 PM	0:18:54	100
10	4152	437	437	10/26/2020	2:30:51 PM	0:03:05	99
10	4153	438	438	10/26/2020	2:34:44 PM	0:03:53	100
10	4154	439	439	10/26/2020	2:38:49 PM	0:04:05	99
10	4155	440	440	10/26/2020	2:41:53 PM	0:03:05	100
10	4156	441	441	10/26/2020	2:50:44 PM	0:08:51	96
10	4157	442	442	10/26/2020	2:53:49 PM	0:03:04	100
10	4158	443	443	10/26/2020	2:56:55 PM	0:03:07	100
10	4159	444	444	10/26/2020	3:00:46 PM	0:03:50	100
10	4160	445	445	10/26/2020	3:03:50 PM	0:03:05	100
7	3056	446	446	10/26/2020	3:12:56 PM	0:09:06	100
4	2212	447	447	10/26/2020	3:13:45 PM	0:00:49	99
7	3057	448	448	10/26/2020	3:15:50 PM	0:02:04	100
4	2213	449	449	10/26/2020	3:16:54 PM	0:01:04	100
4	2214	450	450	10/26/2020	3:19:43 PM	0:02:49	37
4	2215	451	451	10/26/2020	3:26:47 PM	0:07:04	99
4	2216	452	452	10/26/2020	4:40:52 PM	1:14:05	100
4	2217	453	453	10/26/2020	4:44:57 PM	0:04:05	100
4	2218	454	454	10/26/2020	4:48:46 PM	0:03:50	99
4	2219	455	455	10/26/2020	4:52:51 PM	0:04:05	100
4	2220	456	456	10/26/2020	4:54:56 PM	0:02:04	100
4	2221	457	457	10/26/2020	4:59:45 PM	0:04:50	100

4	2222	458	458	10/26/2020	5:03:50 PM	0:04:05	100
4	2223	459	459	10/26/2020	5:06:55 PM	0:03:05	100
4	2224	460	460	10/26/2020	5:09:45 PM	0:02:50	100
4	2225	461	461	10/26/2020	5:12:49 PM	0:03:05	100
4	2226	462	462	10/26/2020	5:15:54 PM	0:03:04	98
4	2227	463	463	10/26/2020	5:21:44 PM	0:05:50	100
4	2228	464	464	10/26/2020	5:30:50 PM	0:09:06	100
4	2229	465	465	10/27/2020	12:58:54 PM		100
4	2230	466	466	10/27/2020	1:04:00 PM	0:05:05	98
10	4161	467	467	10/27/2020	1:06:04 PM	0:02:04	100
4	2231	468	468	10/27/2020	1:07:53 PM	0:01:49	100
10	4162	469	469	10/27/2020	1:08:58 PM	0:01:05	100
4	2232	470	470	10/27/2020	1:12:02 PM	0:03:05	100
10	4163	471	471	10/27/2020	1:12:52 PM	0:00:49	99
4	2233	472	472	10/27/2020	1:14:56 PM	0:02:04	100
10	4164	473	473	10/27/2020	1:16:00 PM	0:01:04	82
4	2234	474	474	10/27/2020	1:19:04 PM	0:03:04	100
10	4165	475	475	10/27/2020	1:19:53 PM	0:00:49	99
4	2235	476	476	10/27/2020	1:21:57 PM	0:02:04	100
10	4166	477	477	10/27/2020	1:23:02 PM	0:01:04	100
4	2236	478	478	10/27/2020	1:24:51 PM	0:01:49	99
2	1020	479	479	10/27/2020	1:30:56 PM	0:06:06	84
2	1021	480	480	10/27/2020	1:35:00 PM	0:04:04	34
2	1022	481	481	10/27/2020	1:38:03 PM	0:03:02	74
2	1023	482	482	10/27/2020	1:38:51 PM	0:00:49	71
4	2237	483	483	10/27/2020	1:49:57 PM	0:11:05	100
4	2238	484	484	10/27/2020	1:53:01 PM	0:03:05	100
4	2239	485	485	10/27/2020	1:55:52 PM	0:02:50	100
4	2240	486	486	10/27/2020	2:01:57 PM	0:06:06	98
4	2241	487	487	10/27/2020	2:06:02 PM	0:04:05	100
4	2242	488	488	10/27/2020	2:07:51 PM	0:01:49	100
4	2243	489	489	10/27/2020	2:14:57 PM	0:07:05	100
4	2244	490	490	10/27/2020	2:18:01 PM	0:03:05	100
4	2245	491	491	10/27/2020	2:20:51 PM	0:02:50	100
4	2246	492	492	10/27/2020	2:24:56 PM	0:04:05	100
4	2247	493	493	10/27/2020	2:29:01 PM	0:04:05	96
10	4167	494	494	10/27/2020	2:29:50 PM	0:00:49	68
4	2248	495	495	10/27/2020	2:30:53 PM	0:01:03	99
10	4168	496	496	10/27/2020	2:31:57 PM	0:01:04	100
4	2249	497	497	10/27/2020	2:35:02 PM	0:03:05	100
10	4169	498	498	10/27/2020	2:35:06 PM	0:00:04	100
4	2250	499	499	10/27/2020	2:38:56 PM	0:03:50	100
10	4170	500	500	10/27/2020	2:41:00 PM	0:02:04	99
4	2251	501	501	10/27/2020	2:42:04 PM	0:01:04	100
10	4171	502	502	10/27/2020	2:44:53 PM	0:02:50	100

4	2252	503	503	10/27/2020	2:45:58 PM	0:01:04	100
10	4172	504	504	10/27/2020	2:48:02 PM	0:02:04	100
4	2253	505	505	10/27/2020	2:49:53 PM	0:01:51	100
4	2254	506	506	10/27/2020	2:54:58 PM	0:05:05	98
4	2255	507	507	10/27/2020	2:59:02 PM	0:04:05	100
4	2256	508	508	10/27/2020	3:01:52 PM	0:02:50	100
4	2257	509	509	10/27/2020	3:08:57 PM	0:07:05	100
4	2258	510	510	10/27/2020	3:16:03 PM	0:07:05	100
4	2259	511	511	10/27/2020	3:22:54 PM	0:06:51	100
4	2260	512	512	10/27/2020	3:25:58 PM	0:03:05	100
4	2261	513	513	10/27/2020	3:30:03 PM	0:04:05	100
10	4173	514	514	10/27/2020	3:31:52 PM	0:01:49	100
10	4174	515	515	10/27/2020	3:37:58 PM	0:06:05	99
4	2262	516	516	10/27/2020	3:39:02 PM	0:01:04	100
4	2263	517	517	10/27/2020	3:44:53 PM	0:05:51	100
10	4175	518	518	10/27/2020	3:45:11 PM	0:00:19	100
10	4176	519	519	10/27/2020	4:06:05 PM	0:20:53	98
10	4177	520	520	10/27/2020	4:09:54 PM	0:03:50	98
10	4178	521	521	10/27/2020	4:13:59 PM	0:04:05	100
10	4179	522	522	10/27/2020	4:18:04 PM	0:04:05	100
10	4180	523	523	10/27/2020	4:21:54 PM	0:03:50	100
10	4181	524	524	10/27/2020	4:25:59 PM	0:04:05	100
4	2264	525	525	10/27/2020	4:27:02 PM	0:01:04	100
10	4182	526	526	10/27/2020	4:28:52 PM	0:01:49	100
4	2265	527	527	10/27/2020	4:29:56 PM	0:01:04	100
10	4183	528	528	10/27/2020	4:32:00 PM	0:02:04	100
4	2266	529	529	10/27/2020	4:32:52 PM	0:00:52	100
10	4184	530	530	10/27/2020	4:35:57 PM	0:03:05	98
4	2267	531	531	10/27/2020	4:42:02 PM	0:06:05	99
4	2268	532	532	10/27/2020	4:49:53 PM	0:07:51	99
4	2269	533	533	10/27/2020	4:54:58 PM	0:05:05	90
2	1024	534	534	10/27/2020	6:54:58 PM	2:00:00	57
7	3058	535	535	10/27/2020	7:01:02 PM	0:06:04	99
4	2270	536	536	10/28/2020	2:03:04 PM		10
4	2271	537	537	10/29/2020	12:58:08 PM		100
4	2272	538	538	10/29/2020	1:01:13 PM	0:03:05	100
4	2273	539	539	10/29/2020	1:08:05 PM	0:06:52	100
4	2274	540	540	10/29/2020	1:12:10 PM	0:04:05	100
4	2275	541	541	10/29/2020	1:17:00 PM	0:04:50	98
4	2276	542	542	10/29/2020	1:21:05 PM	0:04:05	100
4	2277	543	543	10/29/2020	1:24:09 PM	0:03:04	100
4	2278	544	544	10/29/2020	1:30:01 PM	0:05:52	100
4	2279	545	545	10/29/2020	1:36:06 PM	0:06:05	100
4	2280	546	546	10/29/2020	1:40:11 PM	0:04:05	99
4	2281	547	547	10/29/2020	1:44:02 PM	0:03:51	100

4	2282	548	548	10/29/2020	1:48:06 PM	0:04:05	99
4	2283	549	549	10/29/2020	1:54:11 PM	0:06:05	100
4	2284	550	550	10/29/2020	1:56:02 PM	0:01:51	100
4	2285	551	551	10/29/2020	1:59:07 PM	0:03:05	100
4	2286	552	552	10/29/2020	2:02:12 PM	0:03:05	100
4	2287	553	553	10/29/2020	2:09:03 PM	0:06:51	100
4	2288	554	554	10/29/2020	2:13:08 PM	0:04:05	100
4	2289	555	555	10/29/2020	2:19:12 PM	0:06:05	100
4	2290	556	556	10/29/2020	2:22:02 PM	0:02:50	100
4	2291	557	557	10/29/2020	2:25:07 PM	0:03:05	100
4	2292	558	558	10/29/2020	2:36:13 PM	0:11:06	100
4	2293	559	559	10/29/2020	2:38:04 PM	0:01:51	100
4	2294	560	560	10/29/2020	2:40:09 PM	0:02:04	100
4	2295	561	561	10/29/2020	2:45:13 PM	0:05:05	97
4	2296	562	562	10/29/2020	2:49:03 PM	0:03:50	99
4	2297	563	563	10/29/2020	2:51:07 PM	0:02:04	100
4	2298	564	564	10/29/2020	2:54:14 PM	0:03:06	100
4	2299	565	565	10/29/2020	2:57:03 PM	0:02:50	100
4	2300	566	566	10/29/2020	3:00:08 PM	0:03:05	100
2	1025	567	567	10/29/2020	3:16:15 PM	0:16:07	72
2	1026	568	568	10/29/2020	3:17:03 PM	0:00:48	61
2	1027	569	569	10/29/2020	3:23:07 PM	0:06:04	83
2	1028	570	570	10/29/2020	3:25:11 PM	0:02:04	82
2	1029	571	571	10/29/2020	3:27:14 PM	0:02:04	59
2	1030	572	572	10/29/2020	3:33:03 PM	0:05:49	82
2	1031	573	573	10/29/2020	3:34:07 PM	0:01:03	81
2	1032	574	574	10/29/2020	3:35:10 PM	0:01:03	76
2	1033	575	575	10/29/2020	3:37:13 PM	0:02:04	73
2	1034	576	576	10/29/2020	3:41:02 PM	0:03:49	52
4	2301	577	577	10/29/2020	3:45:05 PM	0:04:03	100
4	2302	578	578	10/29/2020	3:48:10 PM	0:03:04	99
4	2303	579	579	10/29/2020	3:52:14 PM	0:04:05	100
4	2304	580	580	10/29/2020	3:55:04 PM	0:02:49	100
4	2305	581	581	10/29/2020	3:59:09 PM	0:04:05	99
4	2306	582	582	10/29/2020	4:04:13 PM	0:05:05	99
4	2307	583	583	10/29/2020	4:07:03 PM	0:02:50	100
4	2308	584	584	10/29/2020	4:11:08 PM	0:04:05	100
4	2309	585	585	10/29/2020	4:13:12 PM	0:02:04	100
4	2310	586	586	10/29/2020	4:17:03 PM	0:03:50	98
4	2311	587	587	10/29/2020	4:20:07 PM	0:03:04	100
4	2312	588	588	10/29/2020	4:23:12 PM	0:03:05	100
4	2313	589	589	10/29/2020	4:26:04 PM	0:02:52	99
4	2314	590	590	10/29/2020	4:32:09 PM	0:06:05	98
4	2315	591	591	10/29/2020	4:38:14 PM	0:06:05	100
4	2316	592	592	10/29/2020	4:41:04 PM	0:02:50	100

4	2317	593	593	10/29/2020	4:49:10 PM	0:08:06	100
4	2318	594	594	10/29/2020	4:52:14 PM	0:03:05	99
4	2319	595	595	10/29/2020	4:56:04 PM	0:03:50	100
4	2320	596	596	10/29/2020	4:59:09 PM	0:03:05	99
4	2321	597	597	10/29/2020	5:01:13 PM	0:02:04	100
4	2322	598	598	10/29/2020	5:07:05 PM	0:05:52	99
4	2323	599	599	10/29/2020	5:11:09 PM	0:04:05	99
4	2324	600	600	10/29/2020	5:14:14 PM	0:03:05	100
4	2325	601	601	10/29/2020	5:16:03 PM	0:01:49	100
4	2326	602	602	10/29/2020	5:20:08 PM	0:04:05	100
4	2327	603	603	10/29/2020	5:22:13 PM	0:02:04	100
4	2328	604	604	10/29/2020	5:25:04 PM	0:02:51	100
4	2329	605	605	10/29/2020	5:30:09 PM	0:05:05	100
7	3059	606	606	10/30/2020	12:37:26 PM		97
7	3060	607	607	10/30/2020	12:41:16 PM	0:03:50	100
7	3061	608	608	10/30/2020	12:45:20 PM	0:04:05	100
7	3062	609	609	10/30/2020	12:50:11 PM	0:04:51	100
7	3063	610	610	10/30/2020	12:55:16 PM	0:05:05	99
10	4185	611	611	10/30/2020	1:16:25 PM	0:21:08	100
10	4186	612	612	10/30/2020	1:20:14 PM	0:03:50	100
10	4187	613	613	10/30/2020	1:23:19 PM	0:03:05	100
10	4188	614	614	10/30/2020	1:27:24 PM	0:04:05	99
10	4189	615	615	10/30/2020	1:30:13 PM	0:02:49	100
10	4190	616	616	10/30/2020	1:37:19 PM	0:07:05	100
10	4191	617	617	10/30/2020	1:40:23 PM	0:03:05	100
10	4192	618	618	10/30/2020	1:43:13 PM	0:02:50	100
10	4193	619	619	10/30/2020	1:48:18 PM	0:05:05	100
10	4194	620	620	10/30/2020	1:51:23 PM	0:03:05	100
10	4195	621	621	10/30/2020	1:54:12 PM	0:02:50	100
10	4196	622	622	10/30/2020	2:04:18 PM	0:10:06	99
10	4197	623	623	10/30/2020	2:07:23 PM	0:03:05	100
10	4198	624	624	10/30/2020	2:13:13 PM	0:05:50	100
10	4199	625	625	10/30/2020	2:22:19 PM	0:09:06	96
10	4200	626	626	10/30/2020	2:25:23 PM	0:03:04	100
10	4201	627	627	10/30/2020	2:28:13 PM	0:02:50	100
10	4202	628	628	10/30/2020	2:31:17 PM	0:03:05	100
10	4203	629	629	10/30/2020	2:34:22 PM	0:03:05	100
10	4204	630	630	10/30/2020	2:41:13 PM	0:06:51	98
10	4205	631	631	10/30/2020	2:44:17 PM	0:03:05	100
10	4206	632	632	10/30/2020	2:47:22 PM	0:03:05	100
10	4207	633	633	10/30/2020	2:51:11 PM	0:03:50	100
10	4208	634	634	10/30/2020	2:54:16 PM	0:03:05	100
10	4209	635	635	10/30/2020	2:57:21 PM	0:03:05	100
10	4210	636	636	10/30/2020	3:00:12 PM	0:02:51	100
10	4211	637	637	10/30/2020	3:03:17 PM	0:03:04	100

10	4212	638	638	10/30/2020	3:06:21 PM	0:03:05	100
2	1035	639	639	10/30/2020	3:09:11 PM	0:02:50	96
10	4213	640	640	10/30/2020	3:09:30 PM	0:00:18	100
2	1036	641	641	10/30/2020	3:11:19 PM	0:01:49	79
10	4214	642	642	10/30/2020	3:12:22 PM	0:01:04	100
2	1037	643	643	10/30/2020	3:14:12 PM	0:01:49	82
2	1038	644	644	10/30/2020	3:16:15 PM	0:02:03	69
2	1039	645	645	10/30/2020	3:18:18 PM	0:02:03	34
4	2330	646	646	10/30/2020	3:25:22 PM	0:07:03	100
10	4215	647	647	10/30/2020	3:27:12 PM	0:01:50	93
4	2331	648	648	10/30/2020	3:30:16 PM	0:03:04	98
10	4216	649	649	10/30/2020	3:35:23 PM	0:05:07	100
4	2332	650	650	10/30/2020	3:38:13 PM	0:02:49	100
10	4217	651	651	10/30/2020	3:38:31 PM	0:00:18	100
4	2333	652	652	10/30/2020	3:47:22 PM	0:08:51	100
10	4218	653	653	10/30/2020	3:48:11 PM	0:00:49	100
4	2334	654	654	10/30/2020	3:51:16 PM	0:03:04	100
10	4219	655	655	10/30/2020	3:53:20 PM	0:02:05	70
4	2335	656	656	10/30/2020	3:55:24 PM	0:02:03	100
10	4220	657	657	10/30/2020	3:57:13 PM	0:01:49	100
4	2336	658	658	10/30/2020	3:59:17 PM	0:02:04	99
10	4221	659	659	10/30/2020	4:00:21 PM	0:01:04	100
10	4222	660	660	10/30/2020	4:03:11 PM	0:02:50	100
4	2337	661	661	10/30/2020	4:04:15 PM	0:01:04	99
10	4223	662	662	10/30/2020	4:07:20 PM	0:03:05	100
10	4224	663	663	10/30/2020	4:10:25 PM	0:03:05	100
4	2338	664	664	10/30/2020	4:11:14 PM	0:00:49	100
4	2339	665	665	10/30/2020	4:17:19 PM	0:06:05	99
4	2340	666	666	10/30/2020	4:22:24 PM	0:05:05	100
4	2341	667	667	10/30/2020	4:27:14 PM	0:04:50	84
4	2342	668	668	10/30/2020	4:32:18 PM	0:05:04	75
4	2343	669	669	10/30/2020	4:37:22 PM	0:05:04	68
10	4225	670	670	11/1/2020	1:56:35 PM		100
10	4226	671	671	11/1/2020	1:59:40 PM	0:03:05	100
10	4227	672	672	11/1/2020	2:01:29 PM	0:01:49	100
10	4228	673	673	11/1/2020	2:04:34 PM	0:03:05	100
10	4229	674	674	11/1/2020	2:09:39 PM	0:05:05	100
10	4230	675	675	11/1/2020	2:12:43 PM	0:03:05	100
10	4231	676	676	11/1/2020	2:17:33 PM	0:04:50	100
10	4232	677	677	11/1/2020	2:22:38 PM	0:05:05	99
10	4233	678	678	11/1/2020	2:26:43 PM	0:04:05	99
10	4234	679	679	11/1/2020	2:29:32 PM	0:02:49	100
10	4235	680	680	11/1/2020	2:32:37 PM	0:03:05	99
10	4236	681	681	11/1/2020	2:35:41 PM	0:03:05	100
10	4237	682	682	11/1/2020	2:38:31 PM	0:02:49	100

10	4238	683	683	11/1/2020	2:44:36 PM	0:06:05	100
10	4239	684	684	11/1/2020	2:51:42 PM	0:07:05	97
10	4240	685	685	11/1/2020	2:54:31 PM	0:02:49	100
10	4241	686	686	11/1/2020	2:57:36 PM	0:03:05	100
10	4242	687	687	11/1/2020	3:00:40 PM	0:03:05	99
10	4243	688	688	11/1/2020	3:05:31 PM	0:04:51	100
10	4244	689	689	11/1/2020	3:07:35 PM	0:02:04	100
7	3064	690	690	11/1/2020	3:14:42 PM	0:07:07	100
7	3065	691	691	11/1/2020	3:17:32 PM	0:02:50	100
7	3066	692	692	11/1/2020	3:20:36 PM	0:03:05	100
7	3067	693	693	11/1/2020	3:24:41 PM	0:04:05	100
10	4245	694	694	11/1/2020	3:35:32 PM	0:10:51	100
10	4246	695	695	11/1/2020	3:38:37 PM	0:03:05	100
10	4247	696	696	11/1/2020	3:41:41 PM	0:03:05	100
10	4248	697	697	11/1/2020	3:45:31 PM	0:03:50	99
10	4249	698	698	11/1/2020	3:49:36 PM	0:04:05	99
10	4250	699	699	11/1/2020	3:51:40 PM	0:02:04	100
10	4251	700	700	11/1/2020	3:54:30 PM	0:02:50	100
10	4252	701	701	11/1/2020	3:57:35 PM	0:03:05	100
10	4253	702	702	11/1/2020	4:00:39 PM	0:03:05	100
10	4254	703	703	11/1/2020	4:02:44 PM	0:02:04	100
10	4255	704	704	11/1/2020	4:05:33 PM	0:02:49	100
10	4256	705	705	11/1/2020	4:12:39 PM	0:07:05	100
10	4257	706	706	11/1/2020	4:15:43 PM	0:03:05	100
10	4258	707	707	11/1/2020	4:19:33 PM	0:03:50	100
10	4259	708	708	11/1/2020	4:24:38 PM	0:05:05	100
4	2344	709	709	11/1/2020	4:27:42 PM	0:03:04	70
10	4260	710	710	11/1/2020	4:27:45 PM	0:00:03	100
10	4261	711	711	11/1/2020	4:30:35 PM	0:02:50	100
4	2345	712	712	11/1/2020	4:32:39 PM	0:02:04	100
10	4262	713	713	11/1/2020	4:33:43 PM	0:01:04	100
10	4263	714	714	11/1/2020	4:36:33 PM	0:02:50	100
10	4264	715	715	11/1/2020	4:38:37 PM	0:02:04	99
10	4265	716	716	11/1/2020	4:42:42 PM	0:04:05	100
4	2346	717	717	11/1/2020	4:45:31 PM	0:02:49	99
10	4266	718	718	11/1/2020	4:46:36 PM	0:01:04	100
4	2347	719	719	11/1/2020	4:48:39 PM	0:02:04	22
10	4267	720	720	11/1/2020	4:51:42 PM	0:03:02	100
10	4268	721	721	11/1/2020	4:54:31 PM	0:02:50	100
2	1040	722	722	11/2/2020	3:06:33 PM		94
2	1041	723	723	11/2/2020	3:06:36 PM	0:00:03	91
2	1042	724	724	11/2/2020	3:06:39 PM	0:00:03	77
2	1043	725	725	11/2/2020	3:06:58 PM	0:00:19	75
2	1044	726	726	11/2/2020	3:07:01 PM	0:00:03	83
2	1045	727	727	11/2/2020	3:07:04 PM	0:00:03	80

2	1046	728	728	11/2/2020	3:07:07 PM	0:00:03	72
2	1047	729	729	11/2/2020	3:07:10 PM	0:00:03	75
2	1048	730	730	11/2/2020	3:07:13 PM	0:00:03	36
2	1049	731	731	11/2/2020	3:07:14 PM	0:00:02	51
2	1050	732	732	11/2/2020	3:07:17 PM	0:00:02	55
2	1051	733	733	11/2/2020	3:07:19 PM	0:00:02	35
2	1052	734	734	11/2/2020	3:07:21 PM	0:00:02	61
2	1053	735	735	11/2/2020	3:07:23 PM	0:00:03	64
2	1054	736	736	11/2/2020	3:07:26 PM	0:00:03	53
2	1055	737	737	11/2/2020	3:07:29 PM	0:00:03	55
2	1056	738	738	11/2/2020	3:07:47 PM	0:00:18	98
10	4269	739	739	11/2/2020	3:07:51 PM	0:00:04	99
2	1057	740	740	11/2/2020	3:08:26 PM	0:00:35	97
10	4270	741	741	11/2/2020	3:08:45 PM	0:00:19	100
2	1058	742	742	11/2/2020	3:10:34 PM	0:01:49	97
2	1059	743	743	11/2/2020	3:12:23 PM	0:01:49	32
10	4271	744	744	11/2/2020	3:13:26 PM	0:01:03	100
2	1060	745	745	11/2/2020	3:17:30 PM	0:04:05	61
2	1061	746	746	11/2/2020	3:19:33 PM	0:02:03	62
2	1062	747	747	11/2/2020	3:20:36 PM	0:01:03	30
10	4272	748	748	11/2/2020	3:22:38 PM	0:02:02	98
10	4273	749	749	11/2/2020	3:26:28 PM	0:03:50	100
4	2348	750	750	11/2/2020	3:28:32 PM	0:02:04	99
10	4274	751	751	11/2/2020	3:29:36 PM	0:01:04	100
4	2349	752	752	11/2/2020	3:31:26 PM	0:01:50	100
10	4275	753	753	11/2/2020	3:32:31 PM	0:01:04	100
4	2350	754	754	11/2/2020	3:34:35 PM	0:02:04	100
4	2351	755	755	11/2/2020	3:36:26 PM	0:01:51	100
10	4276	756	756	11/2/2020	3:37:31 PM	0:01:04	99
4	2352	757	757	11/2/2020	3:40:35 PM	0:03:05	100
10	4277	758	758	11/2/2020	3:40:39 PM	0:00:04	100
4	2353	759	759	11/2/2020	3:44:29 PM	0:03:50	100
10	4278	760	760	11/2/2020	3:45:33 PM	0:01:04	100
4	2354	761	761	11/2/2020	3:50:25 PM	0:04:51	100
10	4279	762	762	11/2/2020	3:50:45 PM	0:00:20	99
10	4280	763	763	11/2/2020	3:54:34 PM	0:03:50	100
4	2355	764	764	11/2/2020	3:55:39 PM	0:01:04	100
4	2356	765	765	11/2/2020	3:58:28 PM	0:02:49	100
10	4281	766	766	11/2/2020	3:59:32 PM	0:01:04	99
4	2357	767	767	11/2/2020	4:02:37 PM	0:03:05	100
10	4282	768	768	11/2/2020	4:02:41 PM	0:00:04	100
10	4283	769	769	11/2/2020	4:05:30 PM	0:02:50	98
4	2358	770	770	11/2/2020	4:06:34 PM	0:01:04	100
10	4284	771	771	11/2/2020	4:12:27 PM	0:05:52	100
10	4285	772	772	11/2/2020	4:14:31 PM	0:02:04	100

10	4286	773	773	11/2/2020	4:19:37 PM	0:05:06	100
7	3068	774	774	11/2/2020	4:21:26 PM	0:01:49	98
10	4287	775	775	11/2/2020	4:22:30 PM	0:01:04	100
10	4288	776	776	11/2/2020	4:25:35 PM	0:03:05	100
7	3069	777	777	11/2/2020	4:27:25 PM	0:01:50	99
7	3070	778	778	11/2/2020	4:32:30 PM	0:05:05	100
7	3071	779	779	11/2/2020	4:42:36 PM	0:10:06	86
7	3072	780	780	11/2/2020	5:06:30 PM	0:23:54	60
2	1063	781	781	11/3/2020	1:58:38 PM		100
2	1064	782	782	11/3/2020	2:01:42 PM	0:03:05	100
2	1065	783	783	11/3/2020	2:07:33 PM	0:05:50	63
2	1066	784	784	11/3/2020	2:08:35 PM	0:01:03	61
2	1067	785	785	11/3/2020	2:12:39 PM	0:04:03	62
2	1068	786	786	11/3/2020	2:14:42 PM	0:02:03	69
2	1069	787	787	11/3/2020	2:19:45 PM	0:05:04	62
10	4289	788	788	11/3/2020	2:24:49 PM	0:05:04	86
2	1070	789	789	11/3/2020	2:26:38 PM	0:01:49	73
10	4290	790	790	11/3/2020	2:26:41 PM	0:00:03	100
2	1071	791	791	11/3/2020	2:28:45 PM	0:02:04	74
2	1072	792	792	11/3/2020	2:29:34 PM	0:00:49	78
10	4291	793	793	11/3/2020	2:29:52 PM	0:00:18	99
2	1073	794	794	11/3/2020	2:31:42 PM	0:01:49	79
10	4292	795	795	11/3/2020	2:32:45 PM	0:01:03	100
2	1074	796	796	11/3/2020	2:34:34 PM	0:01:49	40
10	4293	797	797	11/3/2020	2:35:36 PM	0:01:02	100
10	4294	798	798	11/3/2020	2:37:41 PM	0:02:04	100
2	1075	799	799	11/3/2020	2:40:45 PM	0:03:04	45
10	4295	800	800	11/3/2020	2:42:48 PM	0:02:03	97
10	4296	801	801	11/3/2020	2:44:37 PM	0:01:49	100
2	1076	802	802	11/3/2020	2:46:41 PM	0:02:04	86
2	1077	803	803	11/3/2020	2:48:45 PM	0:02:04	76
2	1078	804	804	11/3/2020	2:54:34 PM	0:05:49	61
10	4297	805	805	11/3/2020	2:57:38 PM	0:03:03	99
2	1079	806	806	11/3/2020	2:58:42 PM	0:01:04	72
2	1080	807	807	11/3/2020	3:00:45 PM	0:02:03	81
10	4298	808	808	11/3/2020	3:01:36 PM	0:00:51	100
2	1081	809	809	11/3/2020	3:02:40 PM	0:01:04	59
10	4299	810	810	11/3/2020	3:04:43 PM	0:02:03	100
10	4300	811	811	11/3/2020	3:07:48 PM	0:03:05	100
10	4301	812	812	11/3/2020	3:10:37 PM	0:02:49	100
7	3073	813	813	11/3/2020	3:11:41 PM	0:01:04	100
10	4302	814	814	11/3/2020	3:13:46 PM	0:02:04	99
7	3074	815	815	11/3/2020	3:14:35 PM	0:00:49	99
10	4303	816	816	11/3/2020	3:16:39 PM	0:02:04	100
7	3075	817	817	11/3/2020	3:17:43 PM	0:01:04	100

10	4304	818	818	11/3/2020	3:18:48 PM	0:01:04	100
7	3076	819	819	11/3/2020	3:20:37 PM	0:01:49	100
10	4305	820	820	11/3/2020	3:21:42 PM	0:01:05	100
7	3077	821	821	11/3/2020	3:23:47 PM	0:02:05	100
10	4306	822	822	11/3/2020	3:24:36 PM	0:00:49	100
10	4307	823	823	11/3/2020	3:26:40 PM	0:02:04	100
7	3078	824	824	11/3/2020	3:27:45 PM	0:01:04	99
10	4308	825	825	11/3/2020	3:30:36 PM	0:02:51	99
7	3079	826	826	11/3/2020	3:32:40 PM	0:02:04	100
10	4309	827	827	11/3/2020	3:33:44 PM	0:01:04	100
7	3080	828	828	11/3/2020	3:35:48 PM	0:02:04	100
7	3081	829	829	11/3/2020	3:41:38 PM	0:05:50	98
10	4310	830	830	11/3/2020	3:41:42 PM	0:00:04	100
7	3082	831	831	11/3/2020	3:45:47 PM	0:04:05	100
10	4311	832	832	11/3/2020	3:47:37 PM	0:01:50	98
7	3083	833	833	11/3/2020	3:49:41 PM	0:02:04	100
10	4312	834	834	11/3/2020	3:50:45 PM	0:01:04	100
10	4313	835	835	11/3/2020	3:54:35 PM	0:03:50	100
7	3084	836	836	11/3/2020	3:55:39 PM	0:01:04	100
7	3085	837	837	11/3/2020	3:58:44 PM	0:03:05	100
10	4314	838	838	11/3/2020	3:58:48 PM	0:00:04	99
7	3086	839	839	11/3/2020	4:03:38 PM	0:04:50	99
10	4315	840	840	11/3/2020	4:03:57 PM	0:00:19	99
10	4316	841	841	11/3/2020	4:07:46 PM	0:03:50	100
7	3087	842	842	11/3/2020	4:08:36 PM	0:00:49	99
10	4317	843	843	11/3/2020	4:10:40 PM	0:02:04	100
10	4318	844	844	11/3/2020	4:12:45 PM	0:02:05	100
7	3088	845	845	11/3/2020	4:16:35 PM	0:03:50	100
10	4319	846	846	11/3/2020	4:16:53 PM	0:00:18	100
10	4320	847	847	11/3/2020	4:19:43 PM	0:02:49	100
7	3089	848	848	11/3/2020	4:21:49 PM	0:02:06	100
10	4321	849	849	11/3/2020	4:22:40 PM	0:00:52	100
7	3090	850	850	11/3/2020	4:25:45 PM	0:03:05	97
7	3091	851	851	11/3/2020	4:28:37 PM	0:02:52	100
7	3092	852	852	11/3/2020	4:34:43 PM	0:06:05	95
10	4322	853	853	11/3/2020	4:37:47 PM	0:03:04	99
7	3093	854	854	11/3/2020	4:38:36 PM	0:00:49	100
7	3094	855	855	11/3/2020	5:11:47 PM	0:33:11	100
7	3095	856	856	11/3/2020	5:14:37 PM	0:02:50	100
10	4323	857	857	11/3/2020	5:44:47 PM	0:30:10	100
10	4324	858	858	11/3/2020	5:47:37 PM	0:02:50	100
10	4325	859	859	11/3/2020	5:55:43 PM	0:08:06	100
10	4326	860	860	11/3/2020	6:01:49 PM	0:06:06	100
7	3096	861	861	11/3/2020	6:11:40 PM	0:09:51	20
10	4327	862	862	11/3/2020	6:11:41 PM	0:00:01	86

7	3097	863	863	11/3/2020	6:48:53 PM	0:37:12	100
7	3098	864	864	11/3/2020	6:51:42 PM	0:02:50	100
7	3099	865	865	11/3/2020	7:19:52 PM	0:28:10	100
10	4328	866	866	11/3/2020	7:20:41 PM	0:00:49	100
7	3100	867	867	11/3/2020	7:24:46 PM	0:04:05	100
10	4329	868	868	11/3/2020	7:25:37 PM	0:00:51	100
7	3101	869	869	11/3/2020	7:27:42 PM	0:02:05	98
10	4330	870	870	11/3/2020	7:34:48 PM	0:07:05	100
7	3102	871	871	11/3/2020	7:35:37 PM	0:00:49	100
10	4331	872	872	11/3/2020	7:49:44 PM	0:14:07	99
7	3103	873	873	11/3/2020	7:50:48 PM	0:01:05	98
10	4332	874	874	11/3/2020	8:05:41 PM	0:14:52	100
10	4333	875	875	11/3/2020	8:09:46 PM	0:04:05	99
2	1082	876	876	11/3/2020	8:16:36 PM	0:06:51	100
2	1083	877	877	11/3/2020	8:17:41 PM	0:01:04	81
2	1084	878	878	11/3/2020	8:19:44 PM	0:02:04	81
10	4334	879	879	11/3/2020	8:23:35 PM	0:03:51	100
10	4335	880	880	11/3/2020	8:27:39 PM	0:04:04	99
2	1085	881	881	11/3/2020	8:29:43 PM	0:02:04	71
10	4336	882	882	11/3/2020	8:30:47 PM	0:01:03	100
2	1086	883	883	11/3/2020	8:31:36 PM	0:00:49	78
10	4337	884	884	11/3/2020	8:37:42 PM	0:06:06	100
2	1087	885	885	11/3/2020	8:38:46 PM	0:01:04	52
2	1088	886	886	11/3/2020	8:40:48 PM	0:02:03	57
10	4338	887	887	11/3/2020	8:40:51 PM	0:00:03	99
2	1089	888	888	11/3/2020	8:41:40 PM	0:00:49	35
2	1090	889	889	11/3/2020	8:44:42 PM	0:03:03	85
10	4339	890	890	11/3/2020	8:44:46 PM	0:00:03	100
2	1091	891	891	11/3/2020	8:46:36 PM	0:01:50	84
10	4340	892	892	11/3/2020	8:47:40 PM	0:01:04	100
2	1092	893	893	11/3/2020	8:48:44 PM	0:01:04	82
2	1093	894	894	11/3/2020	8:50:47 PM	0:02:04	82
10	4341	895	895	11/3/2020	8:50:51 PM	0:00:03	100
2	1094	896	896	11/3/2020	8:51:40 PM	0:00:49	74
10	4342	897	897	11/3/2020	8:53:43 PM	0:02:04	100
10	4343	898	898	11/3/2020	8:56:48 PM	0:03:04	99
2	1095	899	899	11/3/2020	8:58:37 PM	0:01:49	83
10	4344	900	900	11/3/2020	8:59:41 PM	0:01:04	100
2	1096	901	901	11/3/2020	9:01:45 PM	0:02:04	89
10	4345	902	902	11/3/2020	9:02:49 PM	0:01:04	100
10	4346	903	903	11/3/2020	9:08:39 PM	0:05:50	97
10	4347	904	904	11/3/2020	9:13:44 PM	0:05:05	99
10	4348	905	905	11/3/2020	9:17:48 PM	0:04:05	99
10	4349	906	906	11/3/2020	9:20:38 PM	0:02:50	99
7	3104	907	907	11/3/2020	9:24:43 PM	0:04:05	99

10	4350	908	908	11/3/2020	9:27:47 PM	0:03:05	100
7	3105	909	909	11/3/2020	9:28:37 PM	0:00:49	99
7	3106	910	910	11/3/2020	9:32:41 PM	0:04:05	68
10	4351	911	911	11/3/2020	10:13:38 PM	0:40:57	55
10	4352	912	912	11/3/2020	10:16:42 PM	0:03:03	98
10	4353	913	913	11/3/2020	10:22:47 PM	0:06:05	99
10	4354	914	914	11/3/2020	10:25:38 PM	0:02:51	100
10	4355	915	915	11/3/2020	10:28:43 PM	0:03:05	100
10	4356	916	916	11/3/2020	10:31:47 PM	0:03:05	99
10	4357	917	917	11/3/2020	10:34:38 PM	0:02:51	100
10	4358	918	918	11/3/2020	10:37:43 PM	0:03:05	100
10	4359	919	919	11/3/2020	10:40:47 PM	0:03:05	100
10	4360	920	920	11/3/2020	10:43:39 PM	0:02:52	100
10	4361	921	921	11/3/2020	10:45:44 PM	0:02:04	100
10	4362	922	922	11/3/2020	10:48:48 PM	0:03:05	100
2	1097	923	923	11/3/2020	10:50:37 PM	0:01:49	99
2	1098	924	924	11/3/2020	10:53:42 PM	0:03:04	94
10	4363	925	925	11/3/2020	10:55:46 PM	0:02:04	100
10	4364	926	926	11/3/2020	11:00:38 PM	0:04:52	98
10	4365	927	927	11/3/2020	11:03:43 PM	0:03:04	100
2	1099	928	928	11/3/2020	11:04:47 PM	0:01:04	68
10	4366	929	929	11/3/2020	11:06:51 PM	0:02:04	100
10	4367	930	930	11/3/2020	11:09:40 PM	0:02:50	100
2	1100	931	931	11/3/2020	11:10:44 PM	0:01:04	77
10	4368	932	932	11/3/2020	11:11:48 PM	0:01:03	100
2	1101	933	933	11/3/2020	11:15:37 PM	0:03:50	88
10	4369	934	934	11/3/2020	11:15:56 PM	0:00:19	100
10	4370	935	935	11/3/2020	11:18:45 PM	0:02:50	100
2	1102	936	936	11/3/2020	11:19:50 PM	0:01:04	99
10	4371	937	937	11/3/2020	11:20:39 PM	0:00:49	100
2	1103	938	938	11/3/2020	11:21:43 PM	0:01:04	65
2	1104	939	939	11/3/2020	11:22:45 PM	0:01:03	37
2	1105	940	940	11/3/2020	11:27:48 PM	0:05:03	95
2	1106	941	941	11/3/2020	11:28:37 PM	0:00:49	95
7	3107	942	942	11/3/2020	11:37:42 PM	0:09:05	66
2	1107	943	943	11/10/2020	12:58:43 PM		87
2	1108	944	944	11/10/2020	1:01:32 PM	0:02:49	81
2	1109	945	945	11/10/2020	1:03:36 PM	0:02:04	69
2	1110	946	946	11/10/2020	1:08:40 PM	0:05:04	98
2	1111	947	947	11/10/2020	1:15:45 PM	0:07:05	97
2	1112	948	948	11/10/2020	1:27:36 PM	0:11:51	95
2	1113	949	949	11/10/2020	1:28:40 PM	0:01:04	68
2	1114	950	950	11/10/2020	1:30:43 PM	0:02:03	81
2	1115	951	951	11/10/2020	1:37:33 PM	0:06:50	85
2	1116	952	952	11/10/2020	1:40:37 PM	0:03:04	81

2	1117	953	953	11/10/2020	1:42:41 PM	0:02:04	95
2	1118	954	954	11/10/2020	1:44:31 PM	0:01:50	94
2	1119	955	955	11/10/2020	1:54:37 PM	0:10:06	98
2	1120	956	956	11/10/2020	1:56:41 PM	0:02:04	87
2	1121	957	957	11/10/2020	1:58:31 PM	0:01:50	83
2	1122	958	958	11/10/2020	2:01:35 PM	0:03:04	85
2	1123	959	959	11/10/2020	2:02:39 PM	0:01:03	68
7	3108	960	960	11/10/2020	2:13:44 PM	0:11:05	97
7	3109	961	961	11/10/2020	2:21:34 PM	0:07:51	99
7	3110	962	962	11/10/2020	2:24:39 PM	0:03:04	100
7	3111	963	963	11/10/2020	2:33:45 PM	0:09:06	99
7	3112	964	964	11/10/2020	2:39:35 PM	0:05:50	90
7	3113	965	965	11/10/2020	2:45:40 PM	0:06:05	92
7	3114	966	966	11/10/2020	3:43:41 PM	0:58:01	82
2	1124	967	969	11/13/2020	11:38:15 AM		59
7	3115	968	970	11/13/2020	11:38:17 AM	0:00:02	21
7	3116	969	971	11/13/2020	11:38:18 AM	0:00:01	2
7	3117	970	972	11/13/2020	11:38:18 AM	0:00:00	23
7	3118	971	973	11/13/2020	12:59:07 PM	1:20:49	40
2	1125	972	976	11/20/2020	11:47:01 AM		12
7	3119	973	977	11/20/2020	11:53:03 AM	0:06:02	21

APPENDIX C – LOG ENTRIES FROM EMS USER LOG – OCTOBER 2020

Date and Time	Commands / Comments in red
10/21/2020 14:18:01	SubmitBatchCommand (execution duration: 1250ms): Batch 227 - Successfully synchronized results.
10/21/2020 14:18:02	SubmitBatchCommand (execution duration: 1156ms): Batch 226 - Successfully synchronized results.
10/21/2020 14:18:03	SubmitBatchCommand (execution duration: 1297ms): Batch 228 - Successfully synchronized results.
10/21/2020 14:18:05	SubmitBatchCommand (execution duration: 906ms): Batch 229 - Successfully synchronized results.
	The above four commands are the last 4 batches adjudicated before the database copy being written back to the database
10/21/2020 14:18:14	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater then 267).
10/21/2020 14:18:33	LoadResultsCommand (execution duration: 2688ms): Result file '1_1_7_3037_DETAIL.DVD' was loaded successfully.
	The above two statements are the Adjudication Module checking for new Batches, and then loading the DVD file from the NAS for the new one it encountered.
	Note that this batch never made it to the old Adjudication database, it eventually made it to the new one. We are at this point 18 seconds from the database copy.
10/21/2020 14:18:39	GetAdjudicationSupportStatusCommand (execution duration: 16ms): Adjudication status retrieved (Adjudication is enabled)
10/21/2020 14:18:52	GetAdjudicationSupportStatusCommand (execution duration: 0ms): Adjudication status retrieved (Adjudication is enabled)
	This is the only time that this command is seen in the log during the election period, and they happened 12 seconds BEFORE the copy and then again 1 second after.
10/21/2020 14:18:57	GetRelevantOutstackConditionsCommand (execution duration: 31ms): Successfully retrieved relevant outstack conditions
10/21/2020 14:19:26	GetRelevantOutstackConditionsCommand (execution duration: 0ms): Successfully retrieved relevant outstack conditions
	Again, the only time this command is seen, and to me it seems that it involves the new database trying to figure out the current adjudication status
10/21/2020 14:20:06	GetBatchesCommand (execution duration: 1156ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater then 0). Values of CvrSortOrder field for delivered batches are: 1
	This is the Adjudication Module looking for new batches on the NAS drive. As there are currently no batches (the new database was created with no records), it is looking for anything >0
10/21/2020 14:20:07	GetCastVoteRecordsCommand (execution duration: 219ms): Cast vote records for batch '1' successfully retrieved.
	1 Batch was found and retrieved
10/21/2020 14:20:25	GetBatchesCommand (execution duration: 47ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater then 1). Values of CvrSortOrder field for delivered batches are: 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268
	Now the Adjudication module checks for new batches again. Note that the 1st time it found only one, now it finds ALL the rest from 60 - 267 (no sign of 2-59)
10/21/2020 14:20:26	GetCastVoteRecordsCommand (execution duration: 219ms): Cast vote records for batch '60' successfully retrieved.
10/21/2020 14:20:30	GetCastVoteRecordsCommand (execution duration: 312ms): Cast vote records for batch '61' successfully retrieved.

10/21/2020 14:20:34	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '62' successfully retrieved.
10/21/2020 14:20:38	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '63' successfully retrieved.
10/21/2020 14:20:43	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '64' successfully retrieved.
10/21/2020 14:20:47	GetCastVoteRecordsCommand (execution duration: 344ms): Cast vote records for batch '65' successfully retrieved.
10/21/2020 14:20:51	GetCastVoteRecordsCommand (execution duration: 406ms): Cast vote records for batch '66' successfully retrieved.
10/21/2020 14:20:55	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '67' successfully retrieved.
10/21/2020 14:20:59	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '68' successfully retrieved.
10/21/2020 14:21:04	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '69' successfully retrieved.
10/21/2020 14:21:08	GetCastVoteRecordsCommand (execution duration: 359ms): Cast vote records for batch '70' successfully retrieved.
10/21/2020 14:21:12	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '71' successfully retrieved.
10/21/2020 14:21:16	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '72' successfully retrieved.
10/21/2020 14:21:20	GetCastVoteRecordsCommand (execution duration: 297ms): Cast vote records for batch '73' successfully retrieved.
10/21/2020 14:21:24	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '74' successfully retrieved.
10/21/2020 14:21:28	GetCastVoteRecordsCommand (execution duration: 344ms): Cast vote records for batch '75' successfully retrieved.
	The above log entries are the reloading of the batches 60 - 75
10/21/2020 14:21:29	GetCastVoteRecordImageCommand (execution duration: 0ms): Image for tabulator '10, batch '4001' and session '18' successfully retrieved.
	The Adjudication Module begins processing ballots needing adjudication (4001 = batch 1)
10/21/2020 14:21:33	GetCastVoteRecordsCommand (execution duration: 312ms): Cast vote records for batch '76' successfully retrieved.
10/21/2020 14:21:37	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '77' successfully retrieved.
10/21/2020 14:21:44	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '78' successfully retrieved.
10/21/2020 14:21:48	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '79' successfully retrieved.
10/21/2020 14:21:52	GetCastVoteRecordsCommand (execution duration: 375ms): Cast vote records for batch '80' successfully retrieved.
10/21/2020 14:21:56	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '81' successfully retrieved.
10/21/2020 14:22:00	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '82' successfully retrieved.
10/21/2020 14:22:04	GetCastVoteRecordsCommand (execution duration: 266ms): Cast vote records for batch '83' successfully retrieved.
10/21/2020 14:22:09	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '84' successfully retrieved.
10/21/2020 14:22:13	GetCastVoteRecordsCommand (execution duration: 344ms): Cast vote records for batch '85' successfully retrieved.
10/21/2020 14:22:17	GetCastVoteRecordsCommand (execution duration: 281ms): Cast vote records for batch '86' successfully retrieved.
10/21/2020 14:22:21	GetCastVoteRecordsCommand (execution duration: 250ms): Cast vote records for batch '87' successfully retrieved.
10/21/2020 14:22:25	GetCastVoteRecordsCommand (execution duration: 297ms): Cast vote records for batch '88' successfully retrieved.

10/21/2020 14:34:21	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '263' successfully retrieved.
10/21/2020 14:34:25	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '264' successfully retrieved.
10/21/2020 14:34:30	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '265' successfully retrieved.
	The reload is almost complete
10/21/2020 14:34:33	GetCastVoteRecordImageCommand (execution duration: 16ms): Image for tabulator '10, batch '4001' and session '25' successfully retrieved.
	A second ballot from batch 1 goes to adjudication
10/21/2020 14:34:34	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '266' successfully retrieved.
10/21/2020 14:34:38	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '267' successfully retrieved.
	At this point we have reloaded all of the batches from the original database. Time elapsed since copy event: 11 minutes, 47 seconds
	This is 3 seconds (on average) per copied batch, .03 seconds (on average) per ballot.
10/21/2020 14:34:42	GetCastVoteRecordsCommand (execution duration: 234ms): Cast vote records for batch '268' successfully retrieved.
	This is the system actually loading up batch 3037, the last one that was saved before the database copy. (See line 7 above)
	At this point all but 58 batches and their ballots from the original Adjudication database are now copied to the new database

APPENDIX D – LOG ENTRIES FROM EMS USER LOG – MARCH 2021

Date and Time	Command / Comment
03/30/2021 14:57:16	GetCastVoteRecordImageCommand (execution duration: 16ms): Image for tabulator '30, batch '3044' and session '72' successfully retrieved.
	Adjudication Module requesting an image so that it can be adjudicated
03/30/2021 14:57:17	GetBatchesCommand (execution duration: 0ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
03/30/2021 14:57:32	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
03/30/2021 14:57:47	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
03/30/2021 14:58:02	GetBatchesCommand (execution duration: 0ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
	Normal checks for new batches. We are 54 seconds from database copy event
03/30/2021 14:58:41	GetAdjudicationSupportStatusCommand (execution duration: 16ms): Adjudication status retrieved (Adjudication is enabled)
03/30/2021 14:58:57	GetAdjudicationSupportStatusCommand (execution duration: 16ms): Adjudication status retrieved (Adjudication is enabled)
	Like in the November 2020 election these two commands appear right before and right after the copy event.
03/30/2021 14:58:59	GetRelevantOutstackConditionsCommand (execution duration: 47ms): Successfully retrieved relevant outstack conditions
03/30/2021 14:59:15	GetRelevantOutstackConditionsCommand (execution duration: 0ms): Successfully retrieved relevant outstack conditions
	These two commands also were found just after the database copy event
03/30/2021 14:59:52	GetBatchesCommand (execution duration: 156ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 0). Values of CvrSortOrder field for delivered batches are: 45, 46
03/30/2021 14:59:52	GetCastVoteRecordsCommand (execution duration: 406ms): Cast vote records for batch '46' successfully retrieved.
03/30/2021 14:59:56	GetCastVoteRecordsCommand (execution duration: 109ms): Cast vote records for batch '47' successfully retrieved.
	The select batches from the original Adjudication database begin being encountered, although like November 2020, not all at once.
03/30/2021 15:00:14	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 46). Values of CvrSortOrder field for delivered batches are: 48, 49
03/30/2021 15:00:14	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '49' successfully retrieved.
03/30/2021 15:00:18	GetCastVoteRecordsCommand (execution duration: 109ms): Cast vote records for batch '50' successfully retrieved.

03/30/2021 15:00:36	GetBatchesCommand (execution duration: 31ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater then 49). Values of CvrSortOrder field for delivered batches are: 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88
03/30/2021 15:00:36	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '52' successfully retrieved.
03/30/2021 15:00:40	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '53' successfully retrieved.
03/30/2021 15:00:43	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '54' successfully retrieved.
03/30/2021 15:00:47	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '55' successfully retrieved.
03/30/2021 15:00:51	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '56' successfully retrieved.
03/30/2021 15:00:54	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '57' successfully retrieved.
03/30/2021 15:00:58	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '58' successfully retrieved.
03/30/2021 15:01:01	GetCastVoteRecordsCommand (execution duration: 125ms): Cast vote records for batch '59' successfully retrieved.
03/30/2021 15:01:05	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '60' successfully retrieved.
03/30/2021 15:01:08	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '61' successfully retrieved.
03/30/2021 15:01:11	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '62' successfully retrieved.
03/30/2021 15:01:15	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '63' successfully retrieved.
03/30/2021 15:01:19	GetCastVoteRecordsCommand (execution duration: 125ms): Cast vote records for batch '64' successfully retrieved.
03/30/2021 15:01:22	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '65' successfully retrieved.
03/30/2021 15:01:25	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '66' successfully retrieved.
03/30/2021 15:01:29	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '67' successfully retrieved.
03/30/2021 15:01:33	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '68' successfully retrieved.
03/30/2021 15:01:36	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '69' successfully retrieved.
03/30/2021 15:01:40	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '70' successfully retrieved.

03/30/2021 15:01:44	GetCastVoteRecordsCommand (execution duration: 109ms): Cast vote records for batch '71' successfully retrieved.
03/30/2021 15:01:48	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '72' successfully retrieved.
03/30/2021 15:01:51	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '73' successfully retrieved.
03/30/2021 15:01:55	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '74' successfully retrieved.
03/30/2021 15:01:59	GetCastVoteRecordsCommand (execution duration: 109ms): Cast vote records for batch '75' successfully retrieved.
03/30/2021 15:02:02	GetCastVoteRecordsCommand (execution duration: 109ms): Cast vote records for batch '76' successfully retrieved.
03/30/2021 15:02:06	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '77' successfully retrieved.
03/30/2021 15:02:09	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '78' successfully retrieved.
03/30/2021 15:02:12	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '79' successfully retrieved.
03/30/2021 15:02:16	GetCastVoteRecordsCommand (execution duration: 63ms): Cast vote records for batch '80' successfully retrieved.
03/30/2021 15:02:19	GetCastVoteRecordsCommand (execution duration: 109ms): Cast vote records for batch '81' successfully retrieved.
03/30/2021 15:02:22	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '82' successfully retrieved.
03/30/2021 15:02:26	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '83' successfully retrieved.
03/30/2021 15:02:29	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '84' successfully retrieved.
03/30/2021 15:02:33	GetCastVoteRecordsCommand (execution duration: 109ms): Cast vote records for batch '85' successfully retrieved.
03/30/2021 15:02:37	GetCastVoteRecordsCommand (execution duration: 78ms): Cast vote records for batch '86' successfully retrieved.
03/30/2021 15:02:40	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '87' successfully retrieved.
03/30/2021 15:02:44	GetCastVoteRecordsCommand (execution duration: 94ms): Cast vote records for batch '88' successfully retrieved.
03/30/2021 15:02:47	GetCastVoteRecordsCommand (execution duration: 47ms): Cast vote records for batch '89' successfully retrieved.
03/30/2021 15:03:04	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater then 88).

03/30/2021 15:03:19	SubmitBatchCommand (execution duration: 203ms): Batch 63 - Successfully synchronized results.
03/30/2021 15:03:19	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater then 88).
03/30/2021 15:03:19	SubmitBatchCommand (execution duration: 141ms): Batch 59 - Successfully synchronized results.
03/30/2021 15:03:20	SubmitBatchCommand (execution duration: 125ms): Batch 61 - Successfully synchronized results.
03/30/2021 15:03:20	SubmitBatchCommand (execution duration: 78ms): Batch 62 - Successfully synchronized results.
03/30/2021 15:03:20	SubmitBatchCommand (execution duration: 78ms): Batch 64 - Successfully synchronized results.
03/30/2021 15:03:20	SubmitBatchCommand (execution duration: 62ms): Batch 65 - Successfully synchronized results.
03/30/2021 15:03:21	SubmitBatchCommand (execution duration: 109ms): Batch 67 - Successfully synchronized results.
03/30/2021 15:03:21	SubmitBatchCommand (execution duration: 78ms): Batch 68 - Successfully synchronized results.
03/30/2021 15:03:21	SubmitBatchCommand (execution duration: 62ms): Batch 69 - Successfully synchronized results.
03/30/2021 15:03:21	SubmitBatchCommand (execution duration: 94ms): Batch 70 - Successfully synchronized results.
03/30/2021 15:03:21	SubmitBatchCommand (execution duration: 62ms): Batch 71 - Successfully synchronized results.
03/30/2021 15:03:22	SubmitBatchCommand (execution duration: 63ms): Batch 72 - Successfully synchronized results.
03/30/2021 15:03:22	SubmitBatchCommand (execution duration: 62ms): Batch 74 - Successfully synchronized results.
03/30/2021 15:03:22	SubmitBatchCommand (execution duration: 78ms): Batch 56 - Successfully synchronized results.
03/30/2021 15:03:34	GetBatchesCommand (execution duration: 0ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater then 88).
03/30/2021 15:03:40	SubmitBatchCommand (execution duration: 188ms): Batch 75 - Successfully synchronized results.
03/30/2021 15:03:48	SubmitBatchCommand (execution duration: 172ms): Batch 79 - Successfully synchronized results.
03/30/2021 15:03:48	SubmitBatchCommand (execution duration: 125ms): Batch 77 - Successfully synchronized results.
03/30/2021 15:03:48	SubmitBatchCommand (execution duration: 109ms): Batch 78 - Successfully synchronized results.

03/30/2021 15:03:49	GetBatchesCommand (execution duration: 0ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
03/30/2021 15:03:51	SubmitBatchCommand (execution duration: 125ms): Batch 80 - Successfully synchronized results.
03/30/2021 15:04:04	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
03/30/2021 15:04:14	SubmitBatchCommand (execution duration: 203ms): Batch 82 - Successfully synchronized results.
03/30/2021 15:04:18	SubmitBatchCommand (execution duration: 156ms): Batch 84 - Successfully synchronized results.
03/30/2021 15:04:19	SubmitBatchCommand (execution duration: 125ms): Batch 83 - Successfully synchronized results.
03/30/2021 15:04:19	GetBatchesCommand (execution duration: 0ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
03/30/2021 15:04:21	SubmitBatchCommand (execution duration: 156ms): Batch 85 - Successfully synchronized results.
03/30/2021 15:04:34	GetBatchesCommand (execution duration: 16ms): Cast vote record batch list was successfully retrieved (CvrSortOrder greater than 88).
03/30/2021 15:04:48	SubmitBatchCommand (execution duration: 109ms): Batch 89 - Successfully synchronized results.
03/30/2021 15:04:49	SubmitBatchCommand (execution duration: 141ms): Batch 87 - Successfully synchronized results.
03/30/2021 15:04:49	SubmitBatchCommand (execution duration: 156ms): Batch 88 - Successfully synchronized results.
	Like November 2020, the rest of the batches from the original Adjudication database are copied and reprocessed.
	The order, however, is not the same, and there is a referenced to a batch 89 which does not have a record in either Adjudication database.

REFERENCE A – DATABASES AND TABLES

In order to assist other researchers, who may wish to examine these findings or perform additional analysis, here are the most important databases and tables which were used in this analysis.

Main election databases:

November 2020 General Election:

[2020 Mesa County General-2020-09-05-00-10-20]

April 2021 Municipal Election:

[City of Grand Junction-Municipal Election 2021-2021-02-05-16-01-32]

Primary Tables (specifically related to vote totals):

ResultContainer: (Batch level raw vote data)

ResultSplitter: (Vote Data by Polling Location)

ChoiceResult: (Raw aggregated vote data)

CastVoteRecord: (Raw per-ballot list)

Choice: (All Candidates/Choices)

Contest: (All contests in Election)

Tabulator: (All defined tabulators)

Stored Procedures (useful for checking final results):

GetContestResults: Displays current results of any or all contests

GetContestStatistics: Displays stats for any or all contests, including undervotes and overvotes

Adjudication databases:

November 2020 General Election:

[AdjudicableBallotStore_2020_Mesa_County_General_2020-10-01_12:18:50] (before copy)

[AdjudicableBallotStore_2020_Mesa_County_General_2020-10-21_14:18:51] (after copy)

April 2021 Municipal Election:

[AdjudicableBallotStore_City_Of_Grand_Junction_Municipal_Election_2021_2021-03-18_10:48:14] (before copy)

[AdjudicableBallotStore_City_Of_Grand_Junction_Municipal_Election_2021_2021-03-30_14:58:56] (after copy)

Primary Tables:

Batches: Raw batch information

SerializedAdjudicableBallots: Contains one data record for each ballot received.

BallotStatusEvents: Every ballot with Adjudication status. New records for same ballot whenever any change occurs in the status of the ballot.

REFERENCE B – SCANNER SPEED

4.5 Processing Rate

The central scanning device's processing rate also depends on the handling and poll verification activities.

The number of ballots per minute depends on the width or length of the ballot. The following table documents the approximate scanning speed of the ICC scanners.

Scanner	Ballot Size	Pages per Minute (ppm) Scanned
Canon DR-G1130	8.5" x 11"	Approximately 100 ppm, as per Dominion Voting's Quality Assurance test results.
Canon DR-G2140	8.5" x 22"	Approximately 70 ppm, as per Dominion Voting's Quality Assurance test results.
Canon DR-M160II	8.5" x 11"	Approximately 60 ppm, as per Dominion Voting's Quality Assurance test results.

<https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/2-03-ICC-FunctionalityDescription-5-11-CO.pdf>

REFERENCE C – SCANNERS USED BY MESA COUNTY

DESCRIPTION	QTY	UNIT PRICE	EXTENSION
Central Scanning Hardware & Software License			
<i>ImageCast Central Includes:</i>	4	\$18,500	\$74,000
<i>Canon DR-G1130 high speed document scanner.</i>			
- <i>ImageCast® Central Software including third party Kofax VRS 4.5 software.</i>			
- <i>OptiPlex 9020 All-in-One Series with pre-loaded software</i>			
- <i>One (1) iButton Programmer and (1) iButton Key Switch & Cat5 RJ 45</i>			
<i>Cables</i>			
- <i>12 months Hardware Warranty</i>			
- <i>12 months Firmware License</i>			

https://onbase.mesacounty.us/OnBaseAgendaOnline/Documents/Downloadfile/Special_Meeting_1018_Agenda_Packet_8_24_2021_1_00_00_PM.pdf?documentType=5&meetingId=1018&isAttachment=True

REFERENCE D – DATA MOVEMENT FROM BATCHES TO VOTES

Below please find an example of how the data moves through the system from the batch to its votes, and how the ballot level vote data is obfuscated in the process. Blank and irrelevant fields are omitted.

When batch 4025 was received in the Mesa County November 2020 election, the following record was created in the *batches* table of the Adjudication database.

Field	Value
TabulatorId	10
BatchId	4025
Name	Tabulator 10 - Batch 4025
LoadOrder	60
CreationTime	10/21/20 2:20 PM
ModificationTime	10/22/20 10:33 AM
BallotCount	99
HasAdjudicatedBallots	1

After all adjudication tasks were complete, a record exists in the Main election database *ResultContainer* table.

Field	Value
Id	60
containerType	CVR
resultState	Published
batchId	4025
fileName	1_1_10_4025_DETAIL.DVD
tabulatorId	10
CvrSortOrder	60
TimeStamp	10/19/20 4:12 PM

This table serves as a record of each individual batch received, and the *batchId* field (4025 in this case) references the *BatchId* of the Adjudication database's *Batches* table, as shown above. This is the first evidence of a break in referential integrity, as there is no database-level relationship between these two tables. In

other words, the *Batches* record in the Adjudication database can be removed or altered without any warning or error being generated by the database.

Of note also is that the number of ballots which exists in each batch is not a part of the *ResultContainer* table. This makes reconciling the data in the Main election database tables much more difficult.

From here, the information goes to three other tables of interest in the Main election database. The first is *CastVoteRecord*, which contains the ballot-level vote data.

Id	ResultContainerId	RecordId	PrecinctPortionId	IsCurrent	OriginalCvrId	OutstackConditions	BallotTypeId	tabulatorId	batchId
5892	60	1	124	1	NULL	1088	5	10	4025
5893	60	2	103	1	NULL	1088	7	10	4025
5894	60	3	66	0	NULL	256	8	10	4025
5895	60	4	44	1	NULL	1088	3	10	4025
5896	60	5	111	1	NULL	1088	7	10	4025
5897	60	6	63	1	NULL	1088	7	10	4025
5898	60	7	79	1	NULL	0	7	10	4025
5899	60	8	98	1	NULL	0	7	10	4025
5900	60	9	22	1	NULL	1088	3	10	4025
5901	60	10	22	0	NULL	256	3	10	4025
5902	60	11	111	1	NULL	0	7	10	4025
5903	60	12	134	1	NULL	0	7	10	4025
5904	60	13	134	0	NULL	256	7	10	4025
5905	60	14	4	1	NULL	1088	1	10	4025
5906	60	15	100	1	NULL	1088	7	10	4025
5907	60	16	98	1	NULL	1088	7	10	4025
5908	60	17	40	1	NULL	0	1	10	4025
5909	60	18	129	1	NULL	1088	7	10	4025
5910	60	19	124	1	NULL	1088	5	10	4025
5911	60	20	108	1	NULL	0	7	10	4025
5912	60	21	131	0	NULL	5	7	10	4025
5913	60	22	41	0	NULL	1344	1	10	4025
5914	60	23	42	0	NULL	256	1	10	4025
5915	60	24	13	1	NULL	1088	2	10	4025
5916	60	25	42	1	NULL	1088	1	10	4025
5917	60	26	2	1	NULL	0	1	10	4025
5918	60	27	42	1	NULL	0	1	10	4025
5919	60	28	60	1	NULL	0	7	10	4025
5920	60	29	95	1	NULL	0	7	10	4025
5921	60	30	100	1	NULL	1088	7	10	4025

5922	60	31	10	1	NULL	1088	1	10	4025
5923	60	32	117	1	NULL	1088	5	10	4025
5924	60	33	101	1	NULL	0	7	10	4025
5925	60	34	10	0	NULL	256	1	10	4025
5926	60	35	102	1	NULL	1088	7	10	4025
5927	60	36	60	1	NULL	0	7	10	4025
5928	60	37	101	1	NULL	1088	7	10	4025
5929	60	38	7	1	NULL	1088	1	10	4025
5930	60	39	41	1	NULL	0	1	10	4025
5931	60	40	101	0	NULL	1344	7	10	4025
5932	60	41	62	1	NULL	1088	8	10	4025
5933	60	42	46	1	NULL	1088	1	10	4025
5934	60	43	70	1	NULL	0	8	10	4025
5935	60	44	63	1	NULL	1088	7	10	4025
5936	60	45	100	1	NULL	0	7	10	4025
5937	60	46	94	1	NULL	1088	7	10	4025
5938	60	47	101	1	NULL	1088	7	10	4025
5939	60	48	79	1	NULL	1088	7	10	4025
5940	60	49	131	0	NULL	1	7	10	4025
5941	60	50	3	1	NULL	0	1	10	4025
5942	60	51	108	1	NULL	0	7	10	4025
5943	60	52	63	1	NULL	0	7	10	4025
5944	60	53	105	1	NULL	0	7	10	4025
5945	60	54	100	1	NULL	0	7	10	4025
5946	60	55	17	1	NULL	0	3	10	4025
5947	60	56	40	1	NULL	0	1	10	4025
5948	60	57	101	1	NULL	0	7	10	4025
5949	60	58	60	1	NULL	1088	7	10	4025
5950	60	59	22	0	NULL	1	3	10	4025
5951	60	60	134	1	NULL	1088	7	10	4025
5952	60	61	103	1	NULL	1088	7	10	4025
5953	60	62	60	1	NULL	0	7	10	4025
5954	60	63	7	1	NULL	1088	1	10	4025
5955	60	64	52	1	NULL	0	3	10	4025
5956	60	65	100	1	NULL	1088	7	10	4025
5957	60	66	100	0	NULL	256	7	10	4025
5958	60	67	101	1	NULL	0	7	10	4025
5959	60	68	79	1	NULL	0	7	10	4025
5960	60	69	100	1	NULL	0	7	10	4025
5961	60	70	129	1	NULL	1088	7	10	4025
5962	60	71	98	1	NULL	0	7	10	4025
5963	60	72	138	1	NULL	0	7	10	4025
5964	60	73	119	1	NULL	0	7	10	4025

5965	60	74	50	1	NULL	1088	1	10	4025
5966	60	75	102	1	NULL	0	7	10	4025
5967	60	76	100	1	NULL	0	7	10	4025
5968	60	77	22	1	NULL	1088	3	10	4025
5969	60	78	60	1	NULL	1088	7	10	4025
5970	60	79	44	0	NULL	1344	3	10	4025
5971	60	80	101	1	NULL	0	7	10	4025
5972	60	81	111	1	NULL	1088	7	10	4025
5973	60	82	129	1	NULL	0	7	10	4025
5974	60	83	98	1	NULL	1088	7	10	4025
5975	60	84	111	1	NULL	1088	7	10	4025
5976	60	85	34	1	NULL	0	1	10	4025
5977	60	86	35	1	NULL	1088	1	10	4025
5978	60	87	17	1	NULL	0	3	10	4025
5979	60	88	50	1	NULL	1088	1	10	4025
5980	60	89	104	1	NULL	0	7	10	4025
5981	60	90	104	1	NULL	0	7	10	4025
5982	60	91	30	1	NULL	0	1	10	4025
5983	60	92	134	1	NULL	0	7	10	4025
5984	60	93	134	1	NULL	1088	7	10	4025
5985	60	94	101	1	NULL	1088	7	10	4025
5986	60	95	105	1	NULL	1088	7	10	4025
5987	60	96	52	1	NULL	1088	3	10	4025
5988	60	97	105	0	NULL	256	7	10	4025
5989	60	98	100	1	NULL	1088	7	10	4025
5990	60	99	98	0	NULL	1344	7	10	4025
9514	60	3	66	1	5894	0	8	10	4025
9515	60	10	22	1	5901	0	3	10	4025
9516	60	13	134	1	5904	0	7	10	4025
9517	60	22	41	1	5913	1088	1	10	4025
9518	60	23	42	1	5914	0	1	10	4025
9519	60	21	131	1	5912	1092	7	10	4025
9620	60	34	10	1	5925	0	1	10	4025
9621	60	49	131	1	5940	1088	7	10	4025
9622	60	40	101	1	5931	1088	7	10	4025
9623	60	59	22	1	5950	1	3	10	4025
9624	60	66	100	1	5957	256	7	10	4025
9625	60	79	44	1	5970	1088	3	10	4025
9626	60	99	98	1	5990	1088	7	10	4025
9728	60	97	105	1	5988	0	7	10	4025

There is one record for each ballot in batch 4025, and then an additional record for each ballot which went through the manual adjudication process. The *IsCurrent* field indicates which of the two ballot records is the latest one. No timestamp exists in this table to be able to determine the time the ballot data was entered or modified.

Unlike a “Cast Vote Record” file, this table contains no vote information.

Next is *ResultSplitter*. Batch 4025 was separated into 42 rows in this table:

Id	numberOfValid	pollingDistrictId	resultContainerId	numberOfWriteIns	tabulatorId	ballotId
2008	1	30	60	0	10	1
2007	2	104	60	0	10	7
2006	1	35	60	0	10	1
2005	1	34	60	0	10	1
2004	2	50	60	0	10	1
2003	1	119	60	0	10	7
2002	1	138	60	0	10	7
2001	2	52	60	0	10	3
2000	2	17	60	0	10	3
1999	3	105	60	0	10	7
1998	1	3	60	0	10	1
1997	1	94	60	0	10	7
1996	1	70	60	0	10	8
1995	1	46	60	0	10	1
1994	1	62	60	0	10	8
1993	2	7	60	0	10	1
1992	2	102	60	0	10	7
1991	8	101	60	0	10	7
1990	1	117	60	0	10	5
1989	2	10	60	0	10	1
1988	1	95	60	0	10	7
1987	5	60	60	0	10	7
1986	1	2	60	0	10	1
1985	1	13	60	0	10	2
1984	3	42	60	0	10	1
1983	2	41	60	0	10	1
1982	2	131	60	0	10	7
1981	2	108	60	0	10	7
1980	3	129	60	0	10	7
1979	2	40	60	0	10	1
1978	9	100	60	0	10	7

1977	1	4	60	0	10	1
1976	5	134	60	0	10	7
1975	4	22	60	1	10	3
1974	5	98	60	0	10	7
1973	3	79	60	0	10	7
1972	3	63	60	0	10	7
1971	4	111	60	0	10	7
1970	2	44	60	0	10	3
1969	1	66	60	0	10	8
1968	2	103	60	0	10	7
1967	2	124	60	0	10	5

The 99 ballots in batch 4025 are segregated here by polling district number. No vote information appears in this table, and this table links back to its corresponding record in the *ResultContainer* table through the *resultContainerId* field. Again, this table contains no specific vote information for the ballots.

Next is the table *ChoiceResult*. Because of how the records are aggregated, there are over 1,600 records for batch 4025. For brevity, only the first 49 records are displayed.

Id	numberOfVotes	isValid	contestResultId	pollingDistrictId	tabulatorId	resultContainerId	choiceId	partyId
72135	2	1	56749	63	10	60	82	0
72136	1	1	56749	63	10	60	83	0
72137	2	1	56750	63	10	60	88	0
72138	1	1	56750	63	10	60	89	0
72139	2	1	56751	79	10	60	2	0
72140	1	1	56751	79	10	60	1	0
72141	2	1	56752	79	10	60	23	5
72142	1	1	56752	79	10	60	22	2
72143	2	1	56753	79	10	60	27	5
72144	1	1	56753	79	10	60	28	2
72145	2	1	56754	79	10	60	32	5
72146	1	1	56754	79	10	60	31	2
72147	2	1	56755	79	10	60	35	5
72148	1	1	56755	79	10	60	36	2
72149	2	1	56756	79	10	60	38	5
72150	2	1	56757	79	10	60	39	5
72151	1	1	56757	79	10	60	40	2
72152	2	1	56758	79	10	60	42	5
72153	1	1	56758	79	10	60	41	2

72154	3	1	56759	79	10	60	44	0
72155	3	1	56760	79	10	60	46	0
72156	3	1	56761	79	10	60	48	0
72157	3	1	56762	79	10	60	50	0
72158	2	1	56763	79	10	60	74	0
72159	1	1	56763	79	10	60	75	0
72160	3	1	56764	79	10	60	76	0
72161	3	1	56765	79	10	60	78	0
72162	3	1	56766	79	10	60	80	0
72163	2	1	56767	79	10	60	53	0
72164	1	1	56767	79	10	60	52	0
72165	3	1	56768	79	10	60	55	0
72166	2	1	56769	79	10	60	56	0
72167	1	1	56769	79	10	60	57	0
72134	3	1	56748	63	10	60	73	0
72133	1	1	56747	63	10	60	71	0
72132	2	1	56747	63	10	60	70	0
72131	3	1	56746	63	10	60	68	0
72130	2	1	56745	63	10	60	66	0
72129	1	1	56745	63	10	60	67	0
72128	2	1	56744	63	10	60	65	0
72127	1	1	56744	63	10	60	64	0
72126	1	1	56743	63	10	60	63	0
72125	2	1	56743	63	10	60	62	0
72124	1	1	56742	63	10	60	60	0
72123	2	1	56742	63	10	60	61	0
72122	2	1	56741	63	10	60	59	0
72121	1	1	56741	63	10	60	58	0
72120	1	1	56740	63	10	60	57	0
72119	2	1	56740	63	10	60	56	0

This table, the only table which actually has a record of the vote totals used to produce reports, aggregates the votes by polling district and candidate or issue choice. As an example, the fifth line of data specifies that there are two votes for Donald Trump (*choiceId* 2, which references the *internalMachineId* field of the table *Choice*) from polling district 3075539035 – GJ (*pollingDistrictId* 79, which references the *internalMachineId* field of the table *PollingDistrict*).

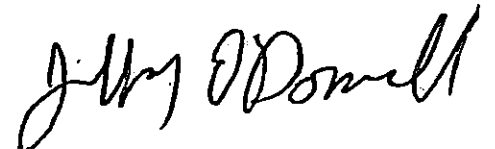
From this table, and the associated tables it links to, all reports are generated. As this is the only table which records vote choices, this is a single point of attack

or failure for the entire vote counting process of the Dominion system. Changes can be made to this table by any process, for instance changing the number of votes or the candidate, would be undetectable as such changes do not affect any other records in any other tables. Nor would such changes require alterations of any other records in any other tables.

Additionally, there is no way to consistently link a particular vote shown in the *ChoiceResult* table to its original ballot within the batch.

The foregoing Forensic Examination and Report was prepared by us, and we are responsible for its content.

The 19th day of March 2022.



Jeffrey O'Donnell
Chief Information Officer
Ordros Analytics



Walter C. Daugherty
Senior Lecturer Emeritus
Department of Computer Science and Engineering
Texas A&M University

BIOGRAPHY

Jeffrey O'Donnell is a Full Stack software and database developer and analyst. He holds Bachelor's degrees in Computer Science and Mathematics from the University of Pittsburgh.

Over the last 40 years, Mr. O'Donnell has worked and consulted for numerous private sector corporations, including Rockwell International, Westinghouse Electric Nuclear, General Defense, U.S. Steel, Mellon Bank, IOTA 360, and the Penn State Applied Research Laboratory. For several years he also delivered and created computer science curriculum for the Community College of Allegheny County.

For the last two decades, Mr. O'Donnell has developed numerous "big data" analysis systems, including systems to provide short-term stock market investors with new types of research and predictive analytics.

He currently is President of Qest Development, a full-service software consulting and publishing company, and is Chief Information Officer of Ordros Analytics, which specializes in election analytics of all types.

Dr. Walter C. Daugherty is a computer consultant and also Senior Lecturer Emeritus in the Department of Computer Science and Engineering at Texas A&M University. He graduated from Oklahoma Christian University with a degree in mathematics, and then earned master's and doctor's degrees from Harvard University, which he attended on a Prize Fellowship from the National Science Foundation.

As a computer expert he has consulted for major national and international firms, and for government agencies. He helped develop the national computer keyboard standard and invented integrated user training within computer applications as well as various electronic computer interfaces.

As a computer science and engineering teacher and researcher, he has published 26 research articles from over \$2.8 million in funded research projects, plus conference papers and other publications. He taught many areas of computer science and engineering for 37 years (32 years at Texas A&M University), including artificial intelligence, quantum computing, programming and software design, and cyber-ethics.

At Harvard he received the Bowdoin Prize and medal for writing, and in 2015 was named a Distinguished Alumnus of Oklahoma Christian University. He is a life member of the Association for Computing Machinery and American MENSA.

Supreme Court Halts Georgia Election Until New System Is Created (conservativebrief.com)

Supreme Court Halts Georgia Election Until New System Is Created



Carmine Sabia August 21, 2022



Getty Images

Advertisement

OPINION: This article may contain commentary which reflects the author's opinion.

-
-
-
-

The Supreme Court has stepped in on a case involving a Georgia election law that is alleged to harm black voters.

It temporarily stopped an election in Georgia on Friday, reviving the ruling from a federal judge that said that the state had disadvantaged black voters in violation of the Voting Rights Act, The New York Times reported.

In an unsigned order without noted dissents, the justices wrote that an appeals court's reason for staying the judge's ruling — that it had come too close to the election in November — was flawed because state officials had told the judge that there was enough time to make the required adjustments. The Supreme Court vacated the stay and returned the case to the appeals court for reconsideration.

Advertisement

The court's order was an exception to what legal experts say is a growing trend: a near-categorical ban on late changes to state election procedures even when those changes have been ruled necessary to address illegal infringements of the right to vote. But the exception was based on an unusual concession from state officials and therefore may not have larger implications.

The case concerned elections for the Georgia Public Service Commission, which sets utility rates and has five members. A 1998 law divided the state into five districts, with one commissioner representing each. But the commissioners continued to be elected in statewide elections.

About a third of Georgians are Black, but Black voters are in a majority in District 3, which is made up of counties in the Atlanta metropolitan area. Four Black voters from that district sued to challenge statewide elections for commissioners, saying the practice violated the Voting Rights Act by diluting their power to elect candidates of their choice.

Advertisement

The Supreme Court agreed with the appeals court which said that Secretary of State Brad Raffensperger “applied a version of the Purcell principle that respondent could not fairly have advanced himself in light of his previous representations to the district court that the schedule on which the district court proceeded was sufficient to enable effectual relief as to the November elections should applicants win at trial.”

The Secretary of State said he would not “make an appeal based on Purcell.”

“Under the *Purcell* principle, courts should not change election rules during the period of time just prior to an election because doing so could confuse voters and create problems for officials administering the election. The principle takes its name from *Purcell v. Gonzalez*, in which the Supreme Court reversed an October 2006 decision of the U.S. Court of Appeals for the 9th Circuit blocking an Arizona voter ID law during that year’s midterm election,” SCOTUS Blog said.

Advertisement

And last week it was reported that the North Carolina Supreme Court may be set to put the brakes on a constitutional amendment that would require voters to produce a valid ID before casting a ballot.

According to a Friday report, the state’s highest court ruled 4-3 along party lines that the requirement, which was added to the North Carolina constitution in 2018 via amendment, could be invalid because the GOP majorities in the state legislature were allegedly the result of unconstitutional racial gerrymandering.

The high court’s ruling did not overturn the amendment, which voters ratified that year, but the justices did send the case back down to a lower court for further review.

“In the final week of the final regular legislative session preceding the 2018 general election, a General Assembly that was composed of a substantial number of legislators elected from districts that the United States Supreme Court had conclusively determined to have resulted from unconstitutional racial gerrymandering enacted legislation presenting six constitutional amendments to North Carolina voters,” Justice Anita Earls wrote for the Court’s Democrat-appointed majority, *The Daily Wire* reported.

The outlet adds:

The two amendments at issue in the case were the voter ID amendment, as well as another amendment preventing the state income tax from ever being raised above 7%. The amendments were passed by a three-fifths majority of both chambers of the legislature; but the voter ID amendment only passed by two votes in the state House of Representatives and three in the Senate; the tax cap amendment passed by just one vote in the House and four votes in the Senate. In the general election in 2018, both amendments were ratified [by] a majority of voters.

At the same time, a federal court ruling found that nearly 30 legislative districts were illegal racial gerrymanders; 100 of the state's 170 legislative seats had to be redrawn, the Associated Press reported. Judges allowed the state legislators elected in 2016 to serve their two-year terms. But in 2018, using redrawn legislative maps, voters in the state broke Republican supermajorities in both houses, the Raleigh News & Observer added.

State Republican leaders were outraged by the ruling.

Georgia elections for two PSC seats again delayed by U.S. Supreme Court ruling - Georgia Recorder

GEORGIA RECORDER

- GOVERNMENT/POLITICS
- ENERGY/ENVIRONMENT
 - EDUCATION
 - HEALTH
- CRIMINAL JUSTICE
- ELECTION 2022

- ENERGY & ENVIRONMENT
- GOVERNMENT & POLITICS

FOR THE RECORD

Georgia elections for two PSC seats again delayed by U.S. Supreme Court ruling

BY: STANLEY DUNLAP - AUGUST 19, 2022 5:46 PM



A U.S. Supreme Court Aug. 19 ruling went in favor of four Black Georgians suing the state in a voting rights case. The Supreme Court order restores a district court injunction that removes two Public Service Commission elections off of the Nov. 8 ballot. States Newsroom file photo

The U.S. Supreme Court removed two Georgia Public Service Commission races from the Nov. 8 ballot, but left open the possibility for an appeals court to reconsider the five-member board that were ruled discriminatory by a district court judge.

The Supreme Court on Friday ruled that the 11th Circuit Court of Appeals erred last week when it blocked a U.S. District Court injunction to delay the PSC elections until after Georgia lawmakers replaced the district-seat, statewide election process that violates the Voting Rights Act by hindering Black voters' ability to elect their preferred candidates.

The 11th circuit judges can decide if they want to review the case and place the two commission races back onto this fall's midterm election ballot by using a more sound legal argument than claiming the injunction came down too close to the election, the Supreme Court decision said.

In a 2-1 vote last week, the Circuit Court granted the state's emergency motion to proceed with the elections conducted on the same general election featuring high-profile races for governor, secretary of state, and U.S. Senate.

With the ruling by the nation's highest court, the two PSC seats that were up for grabs this year are back on hold as the deadline approaches for the secretary of state's office to have ballots ready ahead of the Oct. 17 early voting period.

Meanwhile, the method Georgians will use to elect state regulators will be decided during the appeal of U.S. District Judge Steven Grimberg's ruling in favor of the four plaintiffs seeking district-level elections that they say increases the chances that Black residents' concerns are heard by commissioners who decide how much Georgia Power and other utilities' charge for electricity and natural gas.

"We are pleased that the Supreme Court took this important step toward ensuring that this November's PSC elections are not held using a method that unlawfully dilutes the votes of millions of Black citizens in Georgia," plaintiff's attorney Nico Martinez said on Friday. "We look forward to presenting the merits of our case on appeal and are confident the district court's well-reasoned decision will ultimately be upheld."

The Supreme Court's order comes a day after a Fulton County Superior Court judge reversed Secretary of State Brad Raffensperger's decision to disqualify Democratic candidate Patty Durand, who was drawn out of District

2 by a GOP-created district map in the 2022 legislative session shortly before candidate qualifying started.

Durand and Libertarian Colin McKinney were set to face Republican Commissioner Tim Echols on the same November ballot as the District 3 race between appointed GOP incumbent Fitz Johnson and Democrat Shelia Edwards.

Despite accounting for more than 30% of the voting-age population, the PSC's majority Black metro Atlanta district has only ever elected one Black commissioner.

Currently, commissioners must live in one of five regional districts but are elected by a statewide vote.

The state has argued that political partisanship is the primary factor determining why the majority of Black voters prefer certain candidates.



Voting Systems by County

County	Manufacturer	System
Anderson	Hart	eSlate
Bedford	MicroVote	Infinity
Benton	Hart	Verity Scan
Bledsoe	Hart	eSlate
Blount	Hart	Verity Touch
Bradley	MicroVote	Infinity
Campbell	Hart	Verity Touch
Cannon	MicroVote	Infinity
Carroll	Hart	eSlate
Carter	MicroVote	Infinity
Cheatham	Unisyn	OpenElect Optical Scan
Chester	ES&S	ExpressVote
Claiborne	Hart	eSlate
Clay	MicroVote	Infinity
Cocke	MicroVote	Infinity
Coffee	ES&S	ExpressVote
Crockett	ES&S	ExpressVote
Cumberland	MicroVote	Infinity
Davidson	ES&S	ExpressVote
Decatur	ES&S	ExpressVote
DeKalb	MicroVote	Infinity
Dickson	ES&S	ExpressVote
Dyer	MicroVote	Infinity
Fayette	MicroVote	Infinity
Fentress	MicroVote	Infinity
Franklin	MicroVote	Infinity
Gibson	MicroVote	Infinity
Giles	MicroVote	Infinity
Grainger	Hart	Verity Scan
Greene	ES&S	ExpressVote

County	Manufacturer	System
Grundy	MicroVote	Infinity
Hamblen	MicroVote	Infinity
Hamilton	Dominion	ImageCast
Hancock	Hart	eSlate
Hardeman	Hart	eSlate
Hardin	ES&S	ExpressVote
Hawkins	MicroVote	Infinity
Haywood	Hart	Verity Duo
Henderson	Hart	Verity Scan
Henry	MicroVote	Infinity
Hickman	Hart	eSlate
Houston	ES&S	ExpressVote
Humphreys	Hart	Verity Touch
Jackson	MicroVote	Infinity
Jefferson	MicroVote	Infinity
Johnson	MicroVote	Infinity
Knox	Hart	Verity Scan
Lake	ES&S	ExpressVote
Lauderdale	MicroVote	Infinity
Lawrence	MicroVote	Infinity
Lewis	Hart	Verity Duo
Lincoln	ES&S	ExpressVote
Loudon	ES&S	ExpressVote
Macon	MicroVote	Infinity
Madison	ES&S	ExpressVote
Marion	Hart	Verity Touch
Marshall	MicroVote	Infinity
Maury	ES&S	iVotronic
McMinn	Hart	Verity Duo
McNairy	ES&S	ExpressVote
Meigs	MicroVote	Infinity with VVPAT
Monroe	Hart	Verity Duo
Montgomery	MicroVote	Infinity
Moore	ES&S	ExpressVote

County	Manufacturer	System
Morgan	Hart	eSlate
Obion	Hart	Verity Touch
Overton	MicroVote	Infinity
Perry	MicroVote	Infinity
Pickett	ES&S	Optical Scan
Polk	Unisyn	OpenElect Optical Scan
Putnam	MicroVote	Infinity
Rhea	Hart	Verity Scan
Roane	ES&S	ExpressVote
Robertson	MicroVote	Infinity
Rutherford	MicroVote	Infinity
Scott	MicroVote	Infinity
Sequatchie	MicroVote	Infinity
Sevier	ES&S	ExpressVote
Shelby	ES&S	AccuVote TSX
Smith	MicroVote	Infinity
Stewart	MicroVote	Infinity
Sullivan	Hart	Verity Scan
Sumner	MicroVote	Infinity
Tipton	MicroVote	Infinity
Trousdale	MicroVote	Infinity
Unicoi	MicroVote	Infinity
Union	MicroVote	Infinity
Van Buren	MicroVote	Infinity
Warren	MicroVote	Infinity
Washington	MicroVote	Infinity
Wayne	MicroVote	Infinity
Weakley	ES&S	ExpressVote
White	Hart	Verity Scan
Williamson	ES&S	ExpressVote
Wilson	ES&S	ExpressVote

THE U.S. ELECTION ASSISTANCE COMMISSION



2020 GRANT EXPENDITURE REPORT

July 2021

ANNUAL GRANT EXPENDITURE REPORT

2020

Overview

The U.S. Election Assistance Commission (EAC) was created by Congress in 2002 to improve the administration of elections for federal offices through funding, guidance, and policy development under the Help America Vote Act of 2002 (HAVA). HAVA provides funding to state and local election districts to support upgrading systems for casting votes, registering voters in statewide voter registration databases, providing provisional voting options, and implementing other improvements to the administration of federal elections, such as training for election officials and poll workers, polling place accessibility improvements, and disseminating information on how and where to vote.

Between 2003 and September 30, 2020, a total of \$4,154,617,623 in federal funds has been awarded to 50 states, the District of Columbia and five U.S. territories (American Samoa, the Commonwealth of Puerto Rico, Guam, the Northern Mariana Islands, and the United States Virgin Islands) hereinafter referred to collectively as states. This total includes \$805 million appropriated by Congress in 2018 and 2020 to improve the administration of federal elections, with an emphasis on security enhancements to election systems as well as \$400 million appropriated by Congress under the CARES Act to respond to the pandemic. The Northern Mariana Islands were first authorized to receive HAVA funds in 2020 through the Consolidated Appropriations Act of 2020.

The 2018 appropriation was the first time since 2010 that the federal government made resources available through HAVA to support federal election improvements. States have reported total expenditures of \$3,670,124,269, or 88 percent of total federal funds and accrued interest, available under Sections 101, 102 and 251 of HAVA. This total includes \$255,252,660 in spending associated with the 2018/2020 Election Security award through September 30, 2020 and \$325,889,204 in CARES ACT funds through December 31, 2020.

Under HAVA, funds are available to the states until fully expended with the exception of the CARES Act funds which could only be spent to respond to the effects of the COVID-19 pandemic on the 2020 election cycle. CARES Act funds were only available for expenditure through December 31, 2020. With the addition of CARES Act funds, this report covers calendar year expenditures for CARES Act grants through December 31, 2020 and fiscal year 2020 expenditures for all other grants.

HAVA Section 101 Funds

In 2003, the EAC disbursed \$349,182,262 to states under Section 101 of HAVA for activities to improve the administration of federal elections. Section 101 funds are the most flexible funds available to states through HAVA for administering and improving federal elections because the funds by law can be deployed without first meeting the requirements of Title III of HAVA. Section 101 funds have been used for a wide range of activities including voter education, developing the State Plan, training poll workers, and securing and storing voting equipment.

Section 101 funds have been used to conduct preliminary planning for statewide voter registration systems and to upgrade and replace county voter registration election management systems for compatibility with new voter registration systems. States have implemented voter education programs and conducted training for election officials and poll workers. Another key result has been making polling places accessible and providing voter materials at polling places in multiple languages.

As of September 30, 2020, states reported total expenditures of \$375,037,682 which includes expenditures of federal funds and accumulated interest over the course of the award. Thirty-five states have spent all their Section 101 funds and interest and another 13 states have spent at least 90 percent of their funds. Most states with remaining funds have designated them for annual maintenance of and enhancements to their statewide voter registration systems. Table 1 provides a full accounting of expenditures by states which reflects 94% of federal funds and interest expended.

Table 1: Section 101 HAVA Funds as of September 30, 2020

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
ALABAMA	\$4,989,605	\$6,795	\$4,823,431	\$172,969
ALASKA*	\$5,000,000	\$772,947	\$5,772,947	\$0
AMERICAN SAMOA*	\$1,000,000	\$66,224	\$1,066,224	\$0
ARIZONA*	\$5,451,369	\$1,010,134	\$6,461,503	\$0
ARKANSAS*	\$3,593,165	\$226,288	\$3,819,453	\$0
CALIFORNIA	\$26,804,708	\$2,351,240	\$27,179,892	\$1,976,056
COLORADO*	\$4,860,301	\$1,056,513	\$5,916,814	\$0
CONNECTICUT*	\$5,000,000	\$682,868	\$5,682,868	\$0
DELAWARE**	\$5,000,000	\$472,080	\$5,467,766	\$4,314
DISTRICT OF COLUMBIA*	\$5,000,000	\$408,108	\$5,408,108	\$0
FLORIDA*	\$14,447,580	\$1,859,810	\$16,307,390	\$0
GEORGIA	\$7,816,328	\$716,814	\$7,816,328	\$716,814
GUAM*	\$1,000,000	\$12,773	\$1,012,773	\$0
HAWAII	\$5,000,000	\$1,370,153	\$5,000,000	\$1,370,153
IDAHO*	\$5,000,000	\$1,807,418	\$6,807,418	\$0

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
ILLINOIS	\$11,129,030	\$1,134,502	\$12,119,472	\$144,060
INDIANA	\$6,230,481	\$1,015,543	\$7,240,335	\$5,689
IOWA*	\$5,000,000	\$690,082	\$5,690,082	\$0
KANSAS	\$5,000,000	\$1,429,453	\$3,959,832	\$2,469,622
KENTUCKY	\$4,699,196	\$1,145,796	\$5,662,619	\$182,373
LOUISIANA*	\$4,911,421	\$935,421	\$5,846,842	\$0
MAINE*	\$5,000,000	\$611,809	\$5,611,809	\$0
MARYLAND*	\$5,636,731	\$551,709	\$6,188,440	\$0
MASSACHUSETTS*	\$6,590,381	\$904,363	\$7,494,744	\$0
MICHIGAN	\$9,207,323	\$1,700,789	\$5,925,637	\$4,982,474
MINNESOTA*	\$5,313,786	\$64,724	\$5,378,510	\$0
MISSISSIPPI*	\$3,673,384	\$443,500	\$4,116,884	\$0
MISSOURI*	\$5,875,170	\$954,107	\$6,829,277	\$0
MONTANA*	\$5,000,000	\$400,061	\$5,400,061	\$0
NEBRASKA*	\$5,000,000	\$998,292	\$5,998,292	\$0
NEVADA*	\$5,000,000	\$452,843	\$5,452,843	\$0
NEW HAMPSHIRE	\$5,000,000	\$1,296,921	\$4,926,544	\$1,370,377
NEW JERSEY**	\$8,141,208	\$650,000	\$8,167,547	\$623,661
NEW MEXICO*	\$5,000,000	\$292,244	\$5,292,244	\$0
NEW YORK	\$16,494,325	\$4,250,045	\$14,825,931	\$5,918,438
NORTH CAROLINA	\$7,887,740	\$757,931	\$8,639,322	\$6,349
NORTH DAKOTA*	\$5,000,000	\$63,997	\$5,063,997	\$0
OHIO*	\$10,384,931	\$426,837	\$10,811,768	\$0
OKLAHOMA*	\$5,000,000	\$353,656	\$5,353,656	\$0
OREGON*	\$4,203,776	\$59,199	\$4,262,975	\$0
PENNSYLVANIA*	\$11,323,168	\$1,301,492	\$12,624,660	\$0
PUERTO RICO	\$3,151,144	\$324,193	\$3,475,152	\$186
RHODE ISLAND*	\$5,000,000	\$140,275	\$5,140,275	\$0
SOUTH CAROLINA	\$4,652,412	\$895,188	\$5,460,763	\$86,837
SOUTH DAKOTA	\$5,000,000	\$2,470,851	\$5,484,012	\$1,986,839
TENNESSEE	\$6,004,507	\$1,072,587	\$7,005,687	\$71,408
TEXAS	\$17,206,595	\$3,800,187	\$20,869,487	\$137,296
U. S. VIRGIN ISLANDS*	\$1,000,000	\$21,806	\$1,021,806	\$0
UTAH*	\$3,090,943	\$560,156	\$3,651,099	\$0
VERMONT*	\$5,000,000	\$580,051	\$5,580,051	\$0
VIRGINIA*	\$7,105,890	\$1,130,578	\$8,236,468	\$0
WASHINGTON*	\$6,098,449	\$259,047	\$6,357,496	\$0
WEST VIRGINIA*	\$2,977,057	\$104,747	\$3,081,804	\$0

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
WISCONSIN*	\$5,694,036	\$978,071	\$6,672,107	\$0
WYOMING	\$5,000,000	\$1,681,819	\$5,574,238	\$1,107,581
Totals	\$348,646,140	\$49,725,036	\$375,037,682	\$23,333,494

The asterisk (*) denotes 35 grants the EAC has closed or is closing. Federal funds and earned interest are fully expended.

The double asterisk (**) identifies grants for which financial data is not current. State needs to file updated data for closeout.

The EAC awarded \$349,182,262. The lower amount received reflects a de-obligation of \$536,122 due to an audit finding.

HAVA Section 101 Election Security Funds

As noted earlier, Congress appropriated \$805 million in 2018 and 2020 to improve the administration of elections for federal office, especially to enhance election technology and make election security improvements. The funding provided states with additional resources to secure and improve election systems. The EAC awarded these funds to the 50 states, the District of Columbia and five U.S. Territories (American Samoa, Guam, the Northern Mariana Islands, Puerto Rico and the U.S. Virgin Islands) through a formula described in Sections 101 and 104 of the Help America Vote Act of 2002 (P.L. 107-252) (HAVA). The Northern Mariana Islands first became eligible for the funds in 2020. To access the funds, states provided a budget and a program narrative describing how they would use them. The EAC requested funding allocations in five main areas:

- Voting Equipment
- Post-Election Auditing
- Voter Registration Systems
- Cyber Security
- Communication

States had the option to describe additional areas for expenditures and several states included funding allocations to improve accessibility for individuals with disabilities, support security training for poll workers and staff and implement software upgrades to equipment to improve security.

The 2020 election cycle, beginning with primaries conducted after March 15, 2020, was severely affected by the COVID-19 pandemic. States rescheduled primaries and focused their attention on ensuring voters could vote safely. Several states reported delays in planned contract activities because state resources were refocused on securing the 2020 election and some major expenditures were delayed until 2021 due to the pandemic. States also reported decreased costs for travel and training because planned activities were conducted remotely. State activities in response to the pandemic are described below in the section on CARES Act expenditures. As of September 30, 2020, states had spent a total of \$255,252,660 or 31.2% of the Election Security funds and interest earned. Table 2 provides state-by-state funds expenditures under the Election Security grants.

Table 2: Section 101 Election Security HAVA Funds as of September 30, 2020

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
ALABAMA	\$13,088,416	\$219,236	\$3,353,653	\$9,953,999
ALASKA	\$6,000,000	\$167,983	\$4,370,858	\$1,797,125
AMERICAN SAMOA	\$1,200,000	\$0	\$451,170	\$748,830
ARIZONA	\$15,860,974	\$291,489	\$8,483,595	\$7,668,868
ARKANSAS	\$9,503,000	\$59,635	\$5,336,664	\$4,225,971
CALIFORNIA	\$73,502,386	\$1,016,738	\$5,535,494	\$68,983,630

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
COLORADO	\$13,476,843	\$343,904	\$1,049,403	\$12,771,344
CONNECTICUT	\$10,876,298	\$100,846	\$5,833,956	\$5,143,188
DELAWARE	\$6,036,503	\$0	\$5,963,519	\$72,984
DISTRICT OF COLUMBIA	\$6,000,000	\$97,124	\$4,487,398	\$1,609,726
FLORIDA	\$40,800,785	\$291,960	\$21,257,468	\$19,835,278
GEORGIA	\$21,907,178	\$30,828	\$7,918,749	\$14,019,257
GUAM	\$1,200,000	\$4,620	\$474,223	\$730,397
HAWAII	\$6,642,675	\$73,321	\$366,052	\$6,349,944
IDAHO	\$6,854,176	\$125,029	\$2,388,077	\$4,591,128
ILLINOIS	\$28,132,931	\$540,850	\$4,485,343	\$24,188,438
INDIANA	\$16,140,537	\$190,781	\$8,816,793	\$7,514,525
IOWA	\$9,786,086	\$164,126	\$2,062,124	\$7,888,089
KANSAS	\$9,308,516	\$103,186	\$19,200	\$9,392,502
KENTUCKY	\$12,265,189	\$35,487	\$5,763,113	\$6,537,563
LOUISIANA	\$12,512,099	\$196,808	\$0	\$12,708,907
MAINE	\$6,643,743	\$105,859	\$277,290	\$6,472,312
MARYLAND	\$15,010,079	\$32,927	\$3,947,074	\$11,095,932
MASSACHUSETTS	\$16,769,740	\$312,458	\$3,624,331	\$13,457,867
MICHIGAN	\$22,760,697	\$463,879	\$2,441,648	\$20,782,928
MINNESOTA	\$14,014,282	\$331,462	\$1,101,579	\$13,244,165
MISSISSIPPI	\$9,521,138	\$160,975	\$8,628,501	\$1,053,612
MISSOURI	\$15,365,191	\$310,918	\$2,549,269	\$13,126,839
MONTANA	\$6,133,534	\$127,483	\$2,315,202	\$3,945,816
NEBRASKA	\$7,422,268	\$201,902	\$1,534,553	\$6,089,617
NEVADA	\$9,083,287	\$147,938	\$1,698,658	\$7,532,567
NEW HAMPSHIRE	\$6,582,632	\$114,044	\$1,858,696	\$4,837,980
NEW JERSEY	\$20,740,674	\$383,461	\$1,398,513	\$19,725,622
NEW MEXICO	\$7,853,131	\$241,198	\$1,572,204	\$6,522,125
NEW YORK	\$41,431,856	\$673,535	\$11,836,838	\$30,268,553
NORTH CAROLINA	\$22,050,678	\$419,907	\$5,266,285	\$17,204,300
NORTH DAKOTA	\$6,000,000	\$21,606	\$0	\$6,021,606
NORTHERN MARIANA ISLANDS	\$600,000	\$0	\$205,137	\$394,863
OHIO	\$25,907,133	\$468,849	\$15,696,584	\$10,679,398
OKLAHOMA	\$11,036,835	\$275,874	\$1,001,673	\$10,311,036
OREGON	\$11,392,028	\$319,199	\$1,571,741	\$10,139,486
PENNSYLVANIA	\$28,651,723	\$488,894	\$25,701,621	\$3,438,996
PUERTO RICO	\$7,818,845	\$0	\$815,165	\$7,003,681
RHODE ISLAND	\$6,216,181	\$71,445	\$2,807,362	\$3,480,263
SOUTH CAROLINA	\$12,833,986	\$230,800	\$3,558,045	\$9,506,740

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
SOUTH DAKOTA	\$6,000,000	\$138,605	\$2,949,445	\$3,189,160
TENNESSEE	\$16,077,419	\$287,344	\$4,221,627	\$12,143,136
TEXAS	\$49,449,808	\$2,054,248	\$20,745,707	\$30,758,348
U.S. VIRGIN ISLANDS	\$1,200,000	\$4,974	\$721,709	\$483,265
UTAH	\$8,714,983	\$151,382	\$1,305,161	\$7,561,204
VERMONT	\$6,000,000	\$91,254	\$1,391,104	\$4,700,149
VIRGINIA	\$19,301,044	\$437,593	\$4,727,727	\$15,010,910
WASHINGTON	\$16,805,722	\$303,369	\$5,818,635	\$11,290,456
WEST VIRGINIA	\$7,666,929	\$49,999	\$3,723,458	\$3,993,470
WISCONSIN	\$14,828,442	\$276,500	\$7,101,301	\$8,003,641
WYOMING	\$6,000,000	\$180,356	\$2,721,962	\$3,458,394
Totals	\$804,978,600	\$13,934,186	\$255,252,660	\$563,660,127

Three states did not request their full allocations. Total unrequested = \$21,400

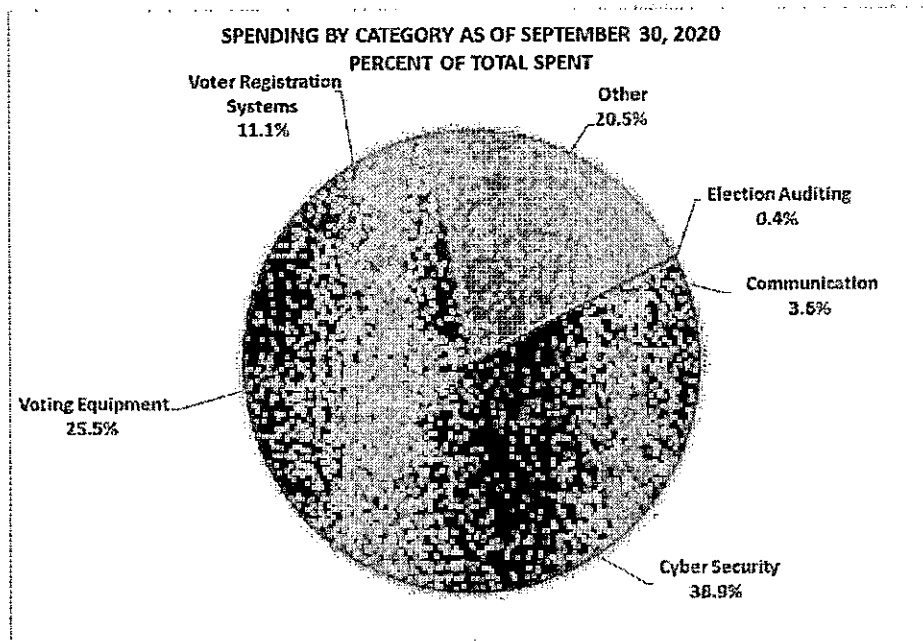
States also report their expenditures by categories they provided in their original program narratives describing how they would spend the funds. Table 3 shows the amounts spent through September 30, 2020 on six main funding objectives. Expenditures by category do not necessarily align with expenditures reported on the financial reports because financial reports include unliquidated obligations.

Table 3: Election Security HAVA Funds by Project Category

Spending by Category as of September 30, 2020		
Project Category	Amount	Percent of Total Spent
Cyber Security	\$95,150,783	38.9%
Voting Equipment	\$61,860,748	25.5%
Voter Registration Systems	\$27,974,457	11.1%
Other	\$51,074,839	20.5%
Communications	\$8,985,191	3.6%
Post-election Auditing	\$1,517,041	0.4%
Total	\$246,563,059	100%

Amounts reported expended by program categories do not include unliquidated obligations included in federal expenditure reports.

Data is unavailable for New Hampshire and North Carolina.



The EAC grants staff's review of state progress reports identified various themes across state activities to enhance election security and improve the administration of federal elections. One common activity between states, irrespective of their relative size or population density, was the choice to spend funds on post-election audits after the November presidential election. Colorado, Georgia, Idaho, Indiana, Iowa, and many other states plan some form of audit with the funds. These audits, which would continue on an ongoing basis, most often take the form of a risk-limiting audit (RLA). RLAs involve storing the paper ballots safely and securely and taking a random sample of a certain number of paper ballots, counting them by hand, and using statistical inference and confidence intervals to determine the success of the vote tallying.

In 2020, states also built their cybersecurity infrastructure by conducting tabletop exercises. Many states and territories employed tabletop exercises to prepare for unforeseen incidents. Tabletop exercises are typically run-in conjunction with an expert or a series of experts on security who can guide staff through the proper response to a security breach or other problematic election incident. States also conducted a wide variety of cybersecurity training for the state chief election official's office and local election officials, covering topics such as cyber hygiene, risk mitigation, information security and election technology, asset management and backup and recovery testing.

States conducted various scans of existing election systems, such as cyber hygiene scans, penetration testing, operating system scanning and risk analysis and vulnerability assessments. Over 20 states worked with the Department of Homeland Security or other security experts to conduct assessments of local election jurisdiction security systems and processes. State progress reports indicated almost 70% of the states focused their activities in 2020 directly on cyber security while 50% of the states also spent funds on

new voting equipment or enhancements to existing voting equipment to increase security. An additional 53% of states replaced or enhanced their voter registration systems to ensure security of the data and to protect against cyberattacks. Many states spent funds in all three areas. Of the states that have spent over 80% of their funds, such as Delaware, Arkansas, Florida and West Virginia, the funds were spent to replace voting equipment that did not provide a paper trail or were allocated to subgrants to local election jurisdictions to address cyber and physical security issues. Four additional states, Georgia, Pennsylvania, South Carolina, and Virginia replaced voting equipment that did not provide a paper trail in advance of the 2020 election.

HAVA Section 101 CARES Act Funds

As noted earlier, Congress appropriated \$400 million in late March 2020 under the CARES Act for states to address the effects of the pandemic on the 2020 election cycle. The EAC streamlined its award process, disbursed the funds to the states shortly after passage of the CARES Act, and alerted them immediately upon passage of the Act that they could expend funds as of March 28, 2020. These additional funds provided much needed resources for states to cover the additional costs for increased absentee or vote-by-mail processes, technology to efficiently request and track mail ballots, safe in-person early or election day voting, and communication to voters about the changes in voting processes due to the pandemic. Almost all states experienced a significant increase in vote-by-mail, which required purchase of secure ballot boxes, high speed scanners and automated letter openers, additional printing of ballots and envelopes, expenditures for postage and return postage, and overtime and hazard pay for state and local employees and poll workers. Many states faced shortages in poll workers and moved quickly to secure personal protective equipment (PPE) for staff, poll workers and voters for the primaries. Traditionally poll workers are senior citizens who were more at risk of serious complications and death from the pandemic. States conducted extensive recruitment efforts to hire additional poll workers.

Federal funds were only available to the states through December 31, 2020 and required a 20% state match. Given state budget crises resulting from the pandemic, a few states did not request the full amount available to them because they could not provide the required match. Two states, Arizona and Oregon, were not able to use any of the funds because of state requirements for legislative approval to use federal funds or state processes that could not be completed in time to take advantage of the funds. Given the short period of time available for use of the federal funds, the EAC adjusted its expenditure reporting period to cover the entire federal fund expenditure period, March 28, 2020 through December 31, 2020. Table 4 below covers the period ending December 31, 2020 and includes expenditures by states for both primaries and the November general election. Many states are still preparing final expenditure reports as local election jurisdictions provide final accounting of expenditures. The data in Tables 4 and 5 contains some estimates that will be reconciled as states complete the review of local expenditures and report on state match.

Table 4: Section 101 CARES Act Funds as of December 31, 2020

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
ALABAMA	\$6,498,674	\$35,318	\$4,376,717	\$2,157,275
ALASKA	\$3,000,000	\$12,350	\$2,366,993	\$645,357
AMERICAN SAMOA	\$600,000	\$0	\$600,000	\$0
ARIZONA	\$7,874,848	\$16,605	\$0	\$7,891,453
ARKANSAS	\$4,719,034	\$3,974	\$1,409,214	\$3,313,794
CALIFORNIA	\$36,485,465	\$0	\$36,485,465	\$0
COLORADO	\$6,691,472	\$52,101	\$6,180,003	\$563,570

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
CONNECTICUT	\$5,400,677	\$108,013	\$5,508,690	\$0
DELAWARE	\$3,000,000	\$0	\$3,000,000	\$0
DISTRICT OF COLUMBIA	\$3,000,000	\$540	\$3,000,540	\$0
FLORIDA	\$20,253,853	\$112,284	\$16,559,031	\$3,807,106
GEORGIA	\$10,875,912	\$0	\$10,875,912	\$0
GUAM	\$600,000	\$0	\$600,000	\$0
HAWAII	\$3,295,842	\$0	\$2,876,851	\$418,991
IDAHO	\$3,404,276	\$11,597	\$3,415,541	\$332
ILLINOIS	\$13,966,097	\$45,535	\$14,011,632	\$0
INDIANA	\$8,013,610	\$6,445	\$8,013,610	\$6,445
IOWA	\$4,859,545	\$10,473	\$4,297,664	\$572,354
KANSAS	\$4,622,500	\$0	\$4,477,003	\$145,497
KENTUCKY	\$6,090,061	\$0	\$5,979,582	\$110,479
LOUISIANA	\$6,212,616	\$3,210	\$6,212,616	\$3,210
MAINE	\$3,299,827	\$14,869	\$974,099	\$2,340,597
MARYLAND	\$7,452,501	\$2,677	\$7,455,178	\$0
MASSACHUSETTS	\$8,325,918	\$12,519	\$8,338,437	\$0
MICHIGAN	\$11,299,561	\$14,676	\$11,314,237	\$0
MINNESOTA	\$6,958,233	\$22,137	\$5,835,588	\$1,144,782
MISSISSIPPI	\$4,728,037	\$20,687	\$1,693,866	\$3,054,858
MISSOURI	\$7,628,763	\$7,824	\$4,030,794	\$3,605,793
MONTANA	\$3,000,000	\$7,563	\$218,221	\$2,789,341
NEBRASKA	\$3,686,252	\$42,826	\$1,611,628	\$2,117,450
NEVADA	\$4,496,720	\$13,318	\$3,863,956	\$646,082
NEW HAMPSHIRE	\$3,269,494	\$11,347	\$3,280,841	\$0
NEW JERSEY	\$10,296,913	\$14,683	\$10,311,596	\$0
NEW MEXICO	\$3,889,527	\$127,647	\$3,889,527	\$127,647
NEW YORK	\$20,567,088	\$13,277	\$20,126,258	\$454,107
NORTH CAROLINA	\$10,947,139	\$0	\$8,339,880	\$2,607,259
NORTH DAKOTA	\$3,000,000	\$1,776	\$3,001,776	\$0
NORTHERN MARIANA ISLANDS	\$600,000	\$0	\$478,908	\$121,092
OHIO	\$12,861,311	\$41,808	\$12,903,119	\$0
OKLAHOMA	\$2,730,486	\$24,555	\$1,226,867	\$1,528,174
OREGON	\$5,656,663	\$32,475	\$0	\$5,689,138
PENNSYLVANIA	\$14,223,603	\$20,107	\$12,538,832	\$1,704,878
PUERTO RICO	\$3,881,359	\$0	\$2,382,774	\$1,498,584
RHODE ISLAND	\$3,022,037	\$0	\$3,022,037	\$0
SOUTH CAROLINA*	\$6,372,386	\$0	\$0	\$6,372,386

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
SOUTH DAKOTA	\$3,000,000	\$55,358	\$350,024	\$2,705,334
TENNESSEE	\$7,982,281	\$7,499	\$7,918,831	\$70,949
TEXAS	\$24,546,841	\$94,215	\$20,859,792	\$3,781,264
U.S. VIRGIN ISLANDS	\$600,000	\$0	\$600,000	\$0
UTAH	\$4,321,708	\$13,517	\$1,848,848	\$2,486,377
VERMONT	\$3,000,000	\$1,782	\$2,106,301	\$895,481
VIRGINIA	\$9,582,344	\$27,537	\$9,609,881	\$0
WASHINGTON	\$8,343,778	\$44,354	\$5,626,093	\$2,762,039
WEST VIRGINIA	\$3,807,691	\$8,231	\$1,522,814	\$2,293,108
WISCONSIN	\$7,362,345	\$4,084	\$7,366,429	\$0
WYOMING	\$3,000,000	\$45,979	\$994,710	\$2,051,269
Totals	\$397,205,286	\$1,167,772	\$325,889,204	\$72,483,854

Asterisk (*) denotes states that have not submitted reports.
Due to state legislature restrictions and timing, Arizona and Oregon could not spend any CARES funds.
Five states did not request their full allocations. Total unrequested = \$2,794,714

States also reported their expenditures by categories designated in the progress report the EAC created for reporting purposes. Table 5 shows the amounts spent through December 31, 2020 in six main funding objectives. While the EAC provided guidance on categorization, expenditures are categorized at each state's discretion. For example, one state may categorize subgrants to purchase or lease voting equipment as "Voting Processes", while another state categorizes similar subgrants as "Other." Where possible the EAC recategorized expenditures that states reported as "Other" into one of the EAC-defined categories. Examples of the kinds of expenditures included in each category are described below.

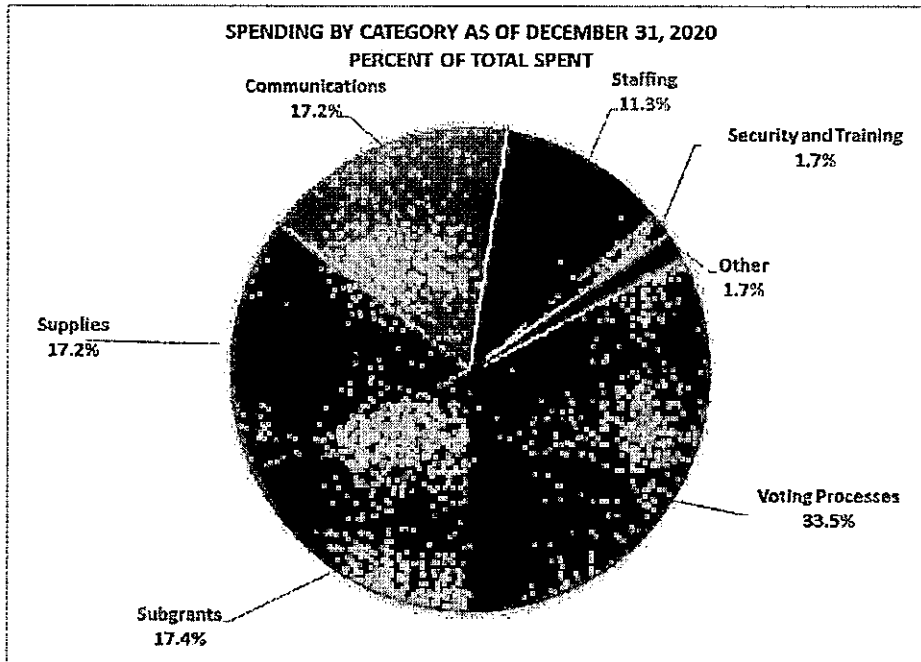
- **Voting Processes:** Additional costs for printing and mailing ballots, high speed scanners, ballot tracking equipment, and ballot drop boxes and leasing of larger polling places to accommodate social distancing.
- **Staffing:** Additional poll workers, election office staff diverted to pandemic response, temporary staff, overtime salary for elections staff, supplemental and/or hazard pay for poll workers.
- **Supplies:** Personal protective equipment, social distancing signage, plexiglass shields, disinfectant, pens and marking devices for one-time use.
- **Security and Training:** Health and safety training of poll workers for sanitation procedures and socially distancing in-person voting.
- **Communications:** Notifying the public of changes to registration, ballot request options, precautions and/or new voting procedures in response to the pandemic.
- **Subgrants:** Funds distributed to local election jurisdictions for costs in any of the categories in states which chose to provide the funds for local purchases instead of statewide purchasing.

- **Other:** Storage and delivery, travel, office expenditures.

Table 5: CARES Act by Expenditure Categories as of December 31, 2020

Expenditure Category	Amount Expended	Percent Expended
Voting Processes	\$92,983,285	33.5%
Subgrants	\$48,306,918	17.4%
Supplies	\$47,856,106	17.2%
Communications	\$47,684,375	17.2%
Staffing	\$31,459,922	11.3%
Security and Training	\$4,716,939	1.7%
Other	\$4,709,306	1.7%
Total	\$277,716,851	100%

Amounts do not include states submitting final reports in June 2021.
 Amounts are estimates in some cases. States are updating progress reports.
 Expended amounts may not include unliquidated obligations reported on FFRs.



HAVA Section 251 Funds - Requirements Payment Grants

Section 251 funds, known as Requirements Payments, were distributed to states using a formula required under HAVA based on a percentage equal to the quotient of the voting age population of each state and the total voting age population of all states. States are required to deposit Section 251 funds in interest-bearing state election accounts and the funds are available until expended. The funds were to be used to:

- Procure voting systems that comply with the requirements of Title III, Section 301 Voting System Standards of HAVA;
- Implement provisional voting (i.e., allowing a voter whose registration status cannot be confirmed at the polling place to cast a provisional ballot);
- Provide information to voters at the polling place such as general information on voting rights;
- Develop and implement a computerized statewide voter registration list; and
- Implement identification requirements for first-time voters who register to vote by mail.

Section 251 funds may also be used for the improvement of the administration of elections for federal office if a state certifies to the EAC that it has either (1) met the requirements of Title III or (2) will not spend more than the amount of the minimum payment applicable to the state on such other activities.

As of September 30, 2020, 22 states reported spending 100 percent of their HAVA Requirements Payment funds (including interest) and another 25 states reported spending 90 percent or more of their funds and interest. States reported cumulative expenditures of \$2,718,310,626 (See Table 6). All but 12 states have less than 10% of their funds remaining. The states with higher percentages include states that had replaced a large portion of their voting equipment just prior to receiving HAVA funds. Those states expect to replace voting equipment in the near future, and their balance of unexpended funds will decrease significantly.

Table 6: Section 251 HAVA Funds as of September 30, 2020

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
ALABAMA	\$40,247,219	\$2,557,534	\$40,436,652	\$2,368,101
ALASKA	\$13,021,803	\$3,461,470	\$15,747,513	\$735,761
AMERICAN SAMOA*	\$2,490,652	\$292,118	\$2,782,770	\$0
ARIZONA**	\$45,516,688	\$4,353,350	\$47,508,539	\$2,361,498
ARKANSAS*	\$24,245,457	\$2,542,278	\$26,787,735	\$0
CALIFORNIA	\$296,305,593	\$46,492,837	\$286,695,564	\$56,102,866
COLORADO	\$38,767,048	\$4,741,500	\$42,972,582	\$535,966
CONNECTICUT*	\$31,109,847	\$7,847,074	\$38,956,921	\$0
DELAWARE**	\$13,021,803	\$1,311,579	\$13,004,721	\$1,328,661
DISTRICT OF COLUMBIA*	\$13,028,257	\$1,935,280	\$14,963,537	\$0
FLORIDA	\$148,633,048	\$24,397,483	\$171,190,236	\$1,840,295
GEORGIA	\$72,641,827	\$905,460	\$68,465,323	\$5,081,964
GUAM*	\$2,319,361	\$48,049	\$2,367,410	\$0

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
HAWAII	\$13,028,257	\$1,193,385	\$12,971,881	\$1,249,761
IDAHO*	\$13,021,803	\$1,267,652	\$14,289,455	\$0
ILLINOIS	\$110,597,147	\$9,213,084	\$118,649,289	\$1,160,943
INDIANA	\$54,440,282	\$2,280,602	\$56,676,561	\$44,323
IOWA*	\$26,645,880	\$1,464,817	\$28,110,697	\$0
KANSAS	\$24,033,425	\$2,518,854	\$26,079,277	\$473,002
KENTUCKY	\$36,919,261	\$5,429,814	\$30,406,135	\$11,942,940
LOUISIANA*	\$39,350,512	\$3,552,964	\$42,903,476	\$0
MAINE	\$13,028,257	\$1,522,838	\$14,551,095	\$0
MARYLAND*	\$47,663,156	\$3,888,041	\$51,551,197	\$0
MASSACHUSETTS	\$58,589,549	\$12,957,409	\$37,766,703	\$33,780,255
MICHIGAN*	\$88,575,455	\$7,735,014	\$96,310,469	\$0
MINNESOTA	\$43,962,194	\$3,764,051	\$47,606,797	\$119,448
MISSISSIPPI	\$25,164,294	\$1,589,078	\$26,741,357	\$12,014
MISSOURI*	\$50,394,880	\$4,268,957	\$54,663,837	\$0
MONTANA*	\$13,028,257	\$618,633	\$13,646,890	\$0
NEBRASKA*	\$15,442,405	\$1,046,168	\$16,488,573	\$0
NEVADA*	\$18,155,632	\$1,272,294	\$19,427,926	\$0
NEW HAMPSHIRE	\$13,028,257	\$2,431,164	\$10,410,561	\$5,048,860
NEW JERSEY*	\$76,360,392	\$5,808,946	\$82,169,338	\$0
NEW MEXICO*	\$15,599,671	\$271,854	\$15,871,525	\$0
NEW YORK	\$172,076,865	\$33,090,178	\$198,174,468	\$6,992,575
NORTH CAROLINA	\$73,460,046	\$7,349,172	\$78,886,117	\$1,923,101
NORTH DAKOTA*	\$13,028,257	\$1,356,359	\$14,384,616	\$0
OHIO *	\$102,069,874	\$6,307,853	\$108,377,727	\$0
OKLAHOMA	\$31,043,081	\$4,322,402	\$31,163,776	\$4,201,707
OREGON	\$31,243,106	\$4,132,436	\$34,533,849	\$841,692
PENNSYLVANIA	\$112,821,809	\$17,063,949	\$128,919,443	\$966,315
PUERTO RICO	\$5,868,252	\$223,389	\$5,649,494	\$442,147
RHODE ISLAND	\$13,028,257	\$485,182	\$13,506,985	\$6,454
SOUTH CAROLINA	\$36,384,617	\$919,428	\$37,121,804	\$182,240
SOUTH DAKOTA	\$13,028,257	\$4,898,802	\$13,028,257	\$4,898,802
TENNESSEE	\$51,877,745	\$7,920,219	\$33,631,819	\$26,166,145
TEXAS*	\$180,251,801	\$12,381,621	\$192,633,426	\$0
U. S. VIRGIN ISLANDS**	\$2,319,361	\$71,884	\$2,319,353	\$71,892
UTAH	\$18,491,597	\$732,340	\$18,589,858	\$634,079
VERMONT	\$12,453,257	\$2,892,693	\$10,084,337	\$5,261,613
VIRGINIA*	\$64,499,288	\$9,562,569	\$74,061,857	\$0

STATE	Amount Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
WASHINGTON	\$52,955,253	\$6,629,712	\$59,295,660	\$289,305
WEST VIRGINIA	\$17,184,961	\$1,228,148	\$17,999,331	\$413,778
WISCONSIN*	\$48,296,088	\$4,367,057	\$52,663,144	\$0
WYOMING*	\$13,028,257	\$1,084,504	\$14,112,761	\$0
Totals	\$2,603,787,596	\$302,001,528	\$2,728,310,626	\$177,478,498

The asterisk (*) denotes grants the EAC has closed or is closing. Federal funds and earned interest are fully expended.

The double asterisk (**) identifies grants for which financial data is not current. State needs to file updated data for closeout.

EAC awarded \$2,603,857,487. The lower amount received reflects a de-obligation of \$69,890 as a result of an audit finding.

Exhibit M
Report 2

15 pages

THE U.S. ELECTION ASSISTANCE COMMISSION



ANNUAL GRANT EXPENDITURE REPORT

FISCAL YEAR 2019

September 20, 2020

ANNUAL GRANT EXPENDITURE REPORT

Fiscal Year 2019

Overview

The U.S. Election Assistance Commission (EAC) was created by Congress in 2002 to improve the administration of elections for federal offices through funding, guidance and policy development under the Help America Vote Act of 2002 (HAVA). HAVA provides funding to state and local election districts to support upgrading systems for casting votes, registering voters in statewide voter registration databases, providing provisional voting options, and implementing other improvements to the administration of federal elections, such as training for election officials and poll workers, polling place accessibility improvements, and disseminating information on how and where to vote.

Between 2003 and September 30, 2019, a total of \$3,632,751,475¹ in federal funds had been awarded to 50 states, the District of Columbia and four U.S. territories (American Samoa, the Commonwealth of Puerto Rico, Guam and the United States Virgin Islands) hereinafter referred to collectively as states. This total includes \$380 million appropriated by Congress in 2018 to improve the administration of federal elections, with an emphasis on security enhancements to election systems. This 2018 appropriation was the first time since 2010 that the federal government made resources available through HAVA to support federal election improvements. States have reported total expenditures of \$3,448,244,244, or 86 percent of total federal funds and accrued interest, available under Sections 101, 102 and 251 of HAVA. This total includes \$92,288,293 in spending associated with the 2018 awards.

Under HAVA, funds are available to the states until fully expended. In 2019, the EAC completed a process to close out expended funds in long-standing grants through September 30, 2018, and carry forward any unexpended funds into new grant amendments. This process allowed states to follow federal grant closeout policy related to record retention. During that process, the EAC conducted final closeouts on 24 Section 101 and 11 Section 251 grants. States had fully expended all federal, state and interest funds under those grants and are no longer required to submit financial and progress reports. EAC amended the grants to carry forward remaining funds for those states that had not fully expended their funds.

¹ This amount includes \$300.3 million in Section 102 funds and \$380 million in 2019 Section 101 Election Security funds.

HAVA Section 101 Funds

In 2003, EAC disbursed \$349,182,262 to states under Section 101 of HAVA for activities to improve the administration of federal elections. Section 101 funds are the most flexible funds available to States through HAVA for administering and improving federal elections because the funds by law can be deployed without first meeting the requirements of Title III of HAVA. Section 101 funds have been used for wide-ranging activities including voter education, developing the State Plan and training poll workers, and securing and storing voting equipment.

Section 101 funds have been used to conduct preliminary planning for Statewide Voter Registration Systems and to upgrade and replace county voter registration election management systems for compatibility with new voter registration systems. States have implemented voter education programs and conducted training for election officials and poll workers. Another key result has been making polling places accessible and providing voter materials at polling places in multiple languages.

As of September 30, 2019, states reported total expenditures of \$365,306,979, which includes expenditures of federal funds and accumulated interest over the course of the award. Thirty states have spent all of their Section 101 funds and interest and another 21 states have spent at least 90 percent of their funds. Table 1 provides a full accounting of expenditures by states which reflect almost 91.6% of federal funds and interest expended.

Table 1: Section 101 HAVA Funds as of September 30, 2019

<u>State</u>	<u>Total 101 Funds Received</u>	<u>Interest Earned</u>	<u>Total Expenditures</u>	<u>Balance of Funds and Interest</u>
ALABAMA	\$4,989,605	\$2,667	\$4,823,431	\$168,841
ALASKA	\$5,000,000	\$1,087,315	\$5,676,414	\$410,901
AMERICAN SAMOA	\$1,000,000	\$66,224	\$1,000,000	\$66,224
ARIZONA	\$5,451,369	\$1,010,134	\$2,095,600	\$4,365,903
ARKANSAS*	\$3,593,165	\$226,288	\$3,819,453	\$0
CALIFORNIA	\$26,804,708	\$2,740,570	\$27,381,278	\$2,164,000
COLORADO	\$4,860,301	\$1,056,513	\$5,916,814	\$0
CONNECTICUT*	\$5,000,000	\$682,868	\$5,682,868	\$0
DELAWARE	\$5,000,000	\$472,080	\$5,467,766	\$4,314
DISTRICT OF COLUMBIA*	\$5,000,000	\$408,108	\$5,408,108	\$0
FLORIDA	\$14,447,580	\$1,859,810	\$14,447,580	\$1,859,810
GEORGIA	\$7,816,328	\$713,171	\$7,816,328	\$713,171
GUAM	\$1,000,000	\$12,773	\$1,012,773	\$0
HAWAII	\$5,000,000	\$1,369,777	\$1,773,535	\$4,596,242
IDAHO*	\$5,000,000	\$1,807,418	\$6,807,418	\$0
ILLINOIS	\$11,129,030	\$1,270,134	\$12,195,182	\$203,982
INDIANA	\$6,230,481	\$938,781	\$7,196,262	-\$27,000
IOWA*	\$5,000,000	\$690,082	\$5,690,082	\$0
KANSAS	\$5,000,000	\$1,400,123	\$3,959,832	\$2,440,292

KENTUCKY	\$4,699,196	\$1,024,965	\$4,699,196	\$1,024,965
LOUISIANA*	\$4,911,421	\$935,421	\$5,846,842	\$0
MAINE	\$5,000,000	\$611,789	\$5,607,822	\$3,967
MARYLAND	\$5,636,731	\$551,709	\$6,188,440	\$0
MASSACHUSETTS*	\$6,590,381	\$904,363	\$7,494,744	\$0
MICHIGAN	\$9,207,323	\$1,684,045	\$9,884,787	\$1,006,581
MINNESOTA*	\$5,313,786	\$64,724	\$5,378,510	\$0
MISSISSIPPI*	\$3,673,384	\$443,500	\$4,116,884	\$0
MISSOURI*	\$5,875,170	\$954,107	\$6,829,277	\$0
MONTANA	\$5,000,000	\$399,279	\$5,310,004	\$89,275
NEBRASKA*	\$5,000,000	\$998,292	\$5,998,292	\$0
NEVADA*	\$5,000,000	\$452,843	\$5,452,843	\$0
NEW HAMPSHIRE	\$5,000,000	\$1,296,921	\$2,463,272	\$3,833,649
NEW JERSEY	\$8,141,208	\$650,000	\$8,791,208	\$0
NEW MEXICO*	\$5,000,000	\$292,244	\$5,292,244	\$0
NEW YORK	\$16,494,325	\$4,102,603	\$15,847,784	\$4,749,144
NORTH CAROLINA	\$7,887,740	\$757,737	\$8,639,321	\$6,156
NORTH DAKOTA*	\$5,000,000	\$63,997	\$5,063,997	\$0
OHIO*	\$10,384,931	\$426,837	\$10,811,768	\$0
OKLAHOMA*	\$5,000,000	\$353,656	\$5,353,656	\$0
OREGON*	\$4,203,776	\$59,199	\$4,262,975	\$0
PENNSYLVANIA*	\$11,323,168	\$1,301,492	\$12,624,660	\$0
PUERTO RICO	\$3,151,144	\$324,190	\$3,474,602	\$732
RHODE ISLAND*	\$5,000,000	\$140,275	\$5,140,275	\$0
SOUTH CAROLINA	\$4,652,412	\$891,665	\$5,312,877	\$231,201
SOUTH DAKOTA	\$5,000,000	\$2,434,031	\$5,049,623	\$2,384,408
TENNESSEE	\$6,004,507	\$1,065,545	\$6,686,421	\$383,631
TEXAS	\$17,206,595	\$3,781,531	\$19,438,981	\$1,549,146
U. S. VIRGIN ISLANDS	\$1,000,000	\$21,806	\$1,000,000	\$21,806
UTAH*	\$3,090,943	\$560,156	\$3,651,099	\$0
VERMONT*	\$5,000,000	\$580,051	\$5,580,051	\$0
VIRGINIA*	\$7,105,890	\$1,130,578	\$8,236,468	\$0
WASHINGTON*	\$6,098,449	\$259,047	\$6,357,496	\$0
WEST VIRGINIA*	\$2,977,057	\$104,747	\$3,081,804	\$0
WISCONSIN	\$5,694,036	\$978,071	\$6,672,107	\$0
WYOMING	\$5,000,000	\$1,662,754	\$5,495,929	\$1,166,825
Total	\$348,646,140	\$50,079,005	\$365,306,979	\$33,418,166

The asterisk (*) denotes grants EAC closed in 2019. Federal funds and earned interest were fully expended. EAC awarded \$349,182,262. The lower amount received reflects a deobligation of \$536,122 as a result of an audit finding.

HAVA Section 101 Election Security Funds

As noted earlier, the Congress provided an additional \$380,000,000 through the Omnibus Appropriations Act of 2018 in March of 2018 to improve the administration of elections for federal office, especially to enhance election technology and make election security improvements. The funding provided states with additional resources to secure and improve election systems. The EAC awarded these funds to the 50 states, the District of Columbia and four U.S. Territories (American Samoa, Guam, Puerto Rico and the U.S. Virgin Islands) eligible to receive them through a formula described in Sections 101 and 104 of the Help America Vote Act of 2002 (P.L. 107-252) (HAVA). To access the funds, states provided a budget and a program narrative describing how they would use the funds. The EAC requested funding allocations in five main areas:

- Voting Equipment
- Post-Election Auditing
- Voter Registration Systems
- Cyber Security
- Communication

States had the option to describe additional areas for expenditures and several states included funding allocations to improve accessibility for individuals with disabilities, support security training for poll workers and staff and implement software upgrades to equipment to improve security. As of September 30, 2019, states had spent a total of \$92,288,293 or 24.3% of the funds, which includes expenditures of federal funds and accumulated interest. Table 2 provides a state-by-state view of funds and expenditures under the 2018 grants.

**Table 2: Section 101 Election Security HAVA Funds as of September 30, 2019
Awarded April 2018**

State	Funds Received	Interest Earned	Expenditures	Balance of Funds and Interest
ALABAMA	\$6,160,393	\$92,697	\$595,528	\$5,657,563
ALASKA	\$3,000,000	\$106,034	\$20,982	\$3,085,053
AMERICAN SAMOA	\$600,000	\$0	\$232,228	\$367,772
ARIZONA	\$7,463,675	\$213,817	\$2,452,425	\$5,225,067
ARKANSAS	\$4,475,015	\$31,614	\$4,475,015	\$31,614
CALIFORNIA	\$34,558,874	\$387,975	\$66,771	\$34,880,079
COLORADO	\$6,342,979	\$167,061	\$592,700	\$5,917,340
CONNECTICUT	\$5,120,554	\$88,431	\$919,703	\$4,289,282
DELAWARE	\$3,000,000	\$0	\$3,000,000	\$0
DISTRICT OF COLUMBIA	\$3,000,000	\$66,864	\$914,698	\$2,152,166
FLORIDA	\$19,187,003	\$53,821	\$17,240,566	\$2,000,258
GEORGIA	\$10,305,783	\$0	\$433,243	\$9,872,540
GUAM	\$600,000	\$2,050	\$62,091	\$539,959

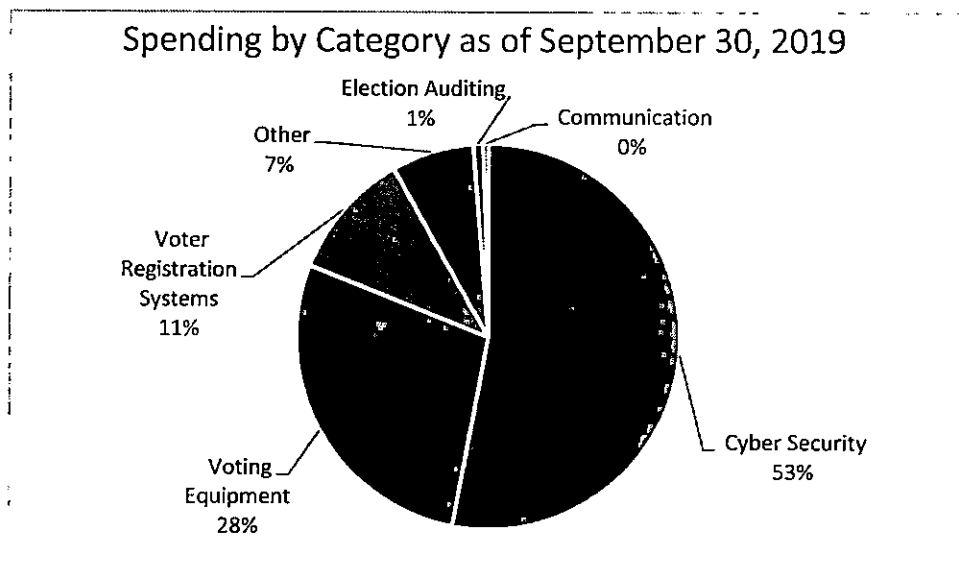
HAWAII	\$3,134,080	\$0	\$0	\$3,134,080
IDAHO	\$3,229,896	\$77,281	\$788,160	\$2,519,017
ILLINOIS	\$13,232,290	\$345,737	\$1,290,619	\$12,287,408
INDIANA	\$7,595,088	\$178,683	\$6,934,989	\$838,782
IOWA	\$4,608,084	\$97,460	\$1,032,782	\$3,672,762
KANSAS	\$4,383,595	\$62,802	\$0	\$4,446,397
KENTUCKY	\$5,773,423	\$35,487	\$3,612,874	\$2,196,036
LOUISIANA	\$5,889,487	\$133,509	\$0	\$6,022,996
MAINE	\$3,130,979	\$60,622	\$31,912	\$3,159,689
MARYLAND	\$7,063,699	\$15,905	\$123,114	\$6,956,490
MASSACHUSETTS	\$7,890,854	\$76,125	\$1,654,651	\$6,312,328
MICHIGAN	\$10,706,992	\$307,366	\$300,615	\$10,713,744
MINNESOTA	\$6,595,610	\$196,892	\$47,169	\$6,745,333
MISSISSIPPI	\$4,483,541	\$86,985	\$1,267,121	\$3,303,405
MISSOURI	\$7,230,625	\$171,417	\$757,418	\$6,644,623
MONTANA	\$3,000,000	\$86,423	\$918,146	\$2,168,277
NEBRASKA	\$3,496,936	\$105,338	\$79,187	\$3,523,087
NEVADA	\$4,277,723	\$80,579	\$603,034	\$3,755,267
NEW HAMPSHIRE	\$3,102,253	\$73,465	\$821,841	\$2,353,877
NEW JERSEY	\$9,757,450	\$234,697	\$375,003	\$9,617,144
NEW MEXICO	\$3,699,470	\$87,881	\$1,545,147	\$2,242,204
NEW YORK	\$19,483,647	\$513,670	\$6,613,982	\$13,383,335
NORTH CAROLINA	\$10,373,237	\$0	\$0	\$10,373,237
NORTH DAKOTA	\$3,000,000	\$8,880	\$0	\$3,008,880
OHIO	\$12,186,021	\$327,847	\$6,125,850	\$6,388,018
OKLAHOMA	\$5,196,017	\$149,882	\$0	\$5,345,899
OREGON	\$5,362,981	\$179,978	\$509,286	\$5,033,673
PENNSYLVANIA	\$13,476,156	\$333,143	\$3,898,769	\$9,910,530
PUERTO RICO	\$3,676,962	\$0	\$589,662	\$3,087,300
RHODE ISLAND	\$3,000,000	\$51,525	\$1,729,753	\$1,321,772
SOUTH CAROLINA	\$6,040,794	\$129,736	\$1,543,465	\$4,627,065
SOUTH DAKOTA	\$3,000,000	\$92,794	\$201,518	\$2,891,277
TENNESSEE	\$7,565,418	\$164,090	\$1,741,666	\$5,987,842
TEXAS	\$23,252,604	\$673,695	\$2,828,492	\$21,097,807
UTAH	\$4,111,052	\$87,114	\$477,977	\$3,720,189
VERMONT	\$3,000,000	\$63,867	\$1,057,597	\$2,006,270
U.S. VIRGIN ISLANDS	\$600,000	\$2,580	\$243,761	\$358,819
VIRGINIA	\$9,080,731	\$186,388	\$1,317,673	\$7,949,446
WASHINGTON	\$7,907,768	\$154,502	\$3,891,533	\$4,170,737
WEST VIRGINIA	\$3,611,943	\$40,496	\$3,587,122	\$65,316
WISCONSIN	\$6,978,318	\$199,584	\$2,661,915	\$4,515,987

WYOMING	\$3,000,000	\$103,117	\$78,540	\$3,024,577
Totals	\$380,000,000	\$7,187,907	\$92,288,293	\$294,899,614

States also report their expenditures by spending categories they provided in their original program narratives describing how they would spend the funds. Table 3 shows the amounts spent through September 31, 2019 on six main funding objectives. Of the states that have spent over 80% of their funds, such as Delaware, Arkansas, Florida and West Virginia, the funds were spent to replace voting equipment that did not provide a paper trail or were allocated to subgrants to local election jurisdictions. Several other states will replace voting equipment in advance of the 2020 election.

Table 3: Election Security HAVA Funds by Project Category

Spending by Category as of September 30, 2019		
Project Category	Amount	Percent of Total Spent
Cyber Security	\$48,858,381	52.9%
Voting Equipment	\$25,893,420	28.1%
Voter Registration Systems	\$9,912,532	10.7%
Other	\$6,420,764	7.0%
Election Auditing	\$769,237	0.8%
Communication	\$429,826	0.5%
Total	\$92,284,160	100%



In 2020 EAC staff reviewed state program narratives and identified some themes across their plans to enhance election security and improve the administration of federal elections. One strong commonality between states, irrespective of their relative size or population density, was the choice to spend funds on

post-election audits. Colorado, Georgia, Idaho, Indiana, Iowa, and many other states plan some form of audit with the funds. These audits, which would continue on an ongoing basis, most often take the form of a risk-limiting audit (RLA). RLAs involve storing the paper ballots safely and securely and taking a random sample of a certain number of paper ballots, counting them by hand, and using statistical inference and confidence intervals to determine the success of the vote tallying.

Another common theme among states in building their cybersecurity infrastructure is the execution of tabletop exercises. New Jersey, New York, Ohio, the U. S. Virgin Islands, and many other states and territories are employing tabletop exercises as a way to prepare for unforeseen incidents. Tabletop exercises are typically run in conjunction with an expert or a series of experts on security who can guide staff through the proper response to a security breach or other problematic election incident.

States also plan to mitigate election-related computer system cyber vulnerabilities identified through Department of Homeland Security or similar scans or assessments of existing election systems, such as:

- Cyber Hygiene Scans
- Penetration Testing
- Social Engineering Testing & Training (i.e. Phishing campaign assessments)
- Database and Operating system scanning
- Risk Analysis and Risk and Vulnerability Assessments
- Asset and network architecture reviews
- System resiliency and redundancy testing
- DDOS Protection
- HTTPS/TLS upgrades
- Two-factor authentication implementation/upgrades
- Intrusion detection and preventions systems

Finally, states are planning a wide variety of cybersecurity training for the state chief election official's office and local election officials. Various entities conduct training activities in these areas:

- Cybersecurity Training
- Information Security & Governance Training
- Cyber Hygiene Training
- Risk Mitigation Training
- Risk and Vulnerability Self-Assessment Training
- Election Technology and Asset Management Training
- Critical Infrastructure Training
- Table Top Exercises
- Social Engineering Training
- Information Operations and Communications Training
- Incident Response, Incident Handling, and Recovery Planning Training
- Vendor Selection and IT Procurement Training
- Election Technology Testing and Auditing Training
- Backup and Recovery Testing and Training

HAVA Section 251 Funds - Requirements Payment Grants

Section 251 funds, known as Requirements Payments, were distributed to states using a formula required under HAVA based on a percentage equal to the quotient of the voting age population of each state and the total voting age population of all states. States are required to deposit Section 251 funds in interest-bearing state election accounts and the funds are available until expended. The funds were to be used to:

- Procure voting systems that comply with the requirements of Title III, Section 301 Voting System Standards of HAVA;
- Implement provisional voting (i.e., allowing a voter whose registration status cannot be confirmed at the polling place to cast a provisional ballot);
- Provide information to voters at the polling place such as general information on voting rights;
- Develop and implement a computerized statewide voter registration list; and
- Implement identification requirements for first-time voters who register to vote by mail.

Section 251 funds may also be used for the improvement of the administration of elections for federal office if a state certifies to EAC that they have either (1) met the requirements of Title III or (2) will not spend more than the amount of the minimum payment applicable to the state on such other activities.

During the closeout process conducted in 2019, the EAC allowed states that had not requested their 2011 funds at that time to do so. To receive the funds, states had to meet the required 5% state match, deposit those funds into the state election funds and review their State Plans to determine if an amendment was needed to access the funds. During that process, 12 states requested those funds representing about \$1,040,000 in additional 25 funds disbursed by the EAC.

As of September 30, 2019, 15 states reported spending 100 percent of their HAVA Requirements Payment funds (including interest) and another 28 states reported spending 90 percent or more of their funds and interest. States reported cumulative expenditures of \$2,698,508,681 (See Table 4). Finally, Table 5 is a state-by-state graph showing the percentage of all HAVA funds and interest remaining unspent as of September 30, 2019. All but 12 states have less than 10% of their funds remaining. The states with higher percentages include states that had replaced a large portion of their voting equipment just prior to receiving HAVA funds. Those states expect to replace voting equipment in the near future and their balance of unexpended funds will decrease significantly.

Table 4: Section 251 HAVA Funds as of September 30, 2019

State	Funds Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
Alabama*	\$40,247,219	\$2,529,448	\$40,436,652	\$2,340,015
Alaska	\$13,021,803	\$3,421,063	\$14,214,587	\$2,228,279
American Samoa	\$2,490,652	\$292,118	\$2,782,770	\$0
Arizona	\$45,516,687	\$4,353,350	\$47,508,539	\$2,361,498
Arkansas*	\$24,245,457	\$2,542,169	\$26,775,820	\$11,806
California	\$296,305,593	\$46,274,099	\$269,843,402	\$72,736,290

Colorado	\$38,767,048	\$4,730,760	\$42,972,582	\$525,227
Connecticut*	\$31,109,847	\$7,847,073	\$38,942,231	\$14,689
Delaware	\$13,021,803	\$1,311,579	\$13,004,721	\$1,328,661
District of Columbia	\$13,028,257	\$1,934,737	\$14,959,924	\$3,070
Florida	\$148,633,048	\$24,327,119	\$164,691,951	\$8,268,216
Georgia	\$72,641,827	\$1,208,012	\$68,462,929	\$5,386,910
Guam	\$2,319,361	\$48,049	\$2,367,410	\$0
Hawaii	\$13,028,257	\$977,446	\$12,829,948	\$1,175,755
Idaho	\$13,021,803	\$1,267,652	\$14,289,455	\$0
Illinois	\$110,597,147	\$9,356,384	\$118,622,450	\$1,331,080
Indiana	\$54,440,283	\$2,280,602	\$56,676,561	\$44,323
Iowa	\$26,645,880	\$1,464,817	\$28,110,697	\$0
Kansas	\$24,033,425	\$2,274,074	\$25,838,952	\$468,547
Kentucky*	\$36,919,262	\$5,180,653	\$30,404,580	\$11,695,334
Louisiana	\$39,350,512	\$3,552,964	\$42,903,476	\$0
Maine*	\$13,028,257	\$1,522,804	\$14,544,406	\$6,656
Maryland	\$47,663,156	\$3,888,041	\$51,551,197	\$0
Massachusetts	\$58,589,550	\$12,526,060	\$32,464,159	\$38,651,451
Michigan*	\$88,575,455	\$7,721,968	\$94,971,678	\$1,325,745
Minnesota	\$43,962,194	\$3,761,498	\$47,570,361	\$153,332
Mississippi*	\$25,164,294	\$1,588,892	\$26,741,357	\$11,829
Missouri	\$50,394,880	\$4,265,288	\$54,176,424	\$483,744
Montana	\$13,028,257	\$618,633	\$13,979,996	\$333,106
Nebraska	\$15,442,405	\$1,046,168	\$16,488,573	\$0
Nevada	\$18,155,632	\$1,272,294	\$19,427,926	\$0
New Hampshire*	\$13,028,257	\$2,431,164	\$10,410,561	\$5,048,860
New Jersey	\$76,360,392	\$5,808,946	\$82,169,338	\$0
New Mexico	\$15,599,671	\$271,854	\$15,871,525	\$0
New York	\$172,076,865	\$33,143,176	\$194,119,725	\$11,100,316
North Carolina*	\$73,460,046	\$7,349,173	\$78,886,117	\$1,923,102
North Dakota	\$13,028,257	\$1,356,359	\$14,384,616	\$0
Ohio	\$102,069,874	\$6,307,853	108377727.3	\$0
Oklahoma*	\$31,043,081	\$4,214,988	\$30,492,597	\$4,765,472
Oregon	\$31,243,106	\$4,085,618	32273780.72	\$3,054,943
Pennsylvania	\$112,821,809	\$16,861,352	\$125,106,929	\$4,576,231
Puerto Rico	\$5,868,252	\$222,622	\$4,584,124	\$1,506,750
Rhode Island*	\$13,028,257	\$485,182	\$13,506,985	\$6,454
South Carolina	\$36,384,617	\$914,189	\$37,121,804	\$177,001
South Dakota	\$13,028,257	\$5,237,852	\$13,435,600	\$4,830,509
Tennessee	\$51,877,746	\$7,506,630	\$33,001,879	\$26,382,497
Texas	\$180,251,801	\$12,381,621	\$192,633,426	\$5

U. S. Virgin Islands	\$2,319,361	\$2,179	\$2,319,361	\$2,179
Utah*	\$18,491,597	\$722,728	\$18,568,105	\$646,220
Vermont	\$12,453,257	\$2,892,693	\$8,765,516	\$6,580,433
Virginia	\$64,499,288	\$9,562,569	\$74,061,857	\$0
Washington	\$52,955,253	\$6,614,605	\$57,242,745	\$2,327,113
West Virginia	\$17,184,960	\$1,218,236	\$17,591,293	\$811,903
Wisconsin	\$48,296,088	\$4,367,057	\$52,663,144	\$0
Wyoming	\$13,028,257	\$1,088,258	\$14,112,761	\$3,754
Total	\$2,603,787,598	\$300,432,717	\$2,680,258,114	\$223,962,201

Asterisk * indicates states that requested and received their 2011 funds in 2019.

EAC awarded \$2,603,857,487. The lower amount received reflects a deobligation of 69,890 as a result of an audit finding.

Negative amounts result from state including some state expenditures as federal.

**Table 5: Remaining HAVA Funds and Interest as of September 30, 2018
(Excludes 2018 Section 101 Funds)**

State	Percent of Funds Remaining
WASHINGTON	5%
WEST VIRGINIA	3%
NORTH CAROLINA	2%
MICHIGAN	2%
PENNSYLVANIA	2%
AMERICAN SAMOA	2%
SOUTH CAROLINA	2%
NEW JERSEY	1%
DISTRICT OF COLUMBIA	1%
COLORADO	1%
TEXAS	1%
WISCONSIN	1%
VIRGINIA	1%
U.S. VIRGIN ISLANDS	1%
MISSOURI	1%
MINNESOTA	0%
IOWA	0%
MARYLAND	0%
MAINE	0%
MISSISSIPPI	0%
ARKANSAS	0%
RHODE ISLAND	0%
CONNECTICUT	0%
INDIANA	0%
MASSACHUSETTS	48%
NEW HAMPSHIRE	41%
TENNESSEE	38%
VERMONT	36%
HAWAII	30%
SOUTH DAKOTA	26%
KENTUCKY	26%
CALIFORNIA	17%
PUERTO RICO	16%
ARIZONA	12%
OKLAHOMA	11%
ALASKA	11%
NEW YORK	8%
ILLINOIS	8%
OREGON	7%
GEORGIA	7%
KANSAS	6%
DELAWARE	6%
WYOMING	6%
ALABAMA	5%
FLORIDA	5%

Exhibit M
Report 3
17 pages

THE U.S. ELECTION ASSISTANCE COMMISSION



GRANT EXPENDITURE REPORT
FISCAL YEAR 2018

April 4, 2019

Overview

The U.S. Election Assistance Commission (EAC) was created by Congress in 2002 to improve the administration of elections for federal offices through funding, guidance and policy development under the Help America Vote Act of 2002 (HAVA).

HAVA provides funding to state and local election districts to support upgrading systems for casting votes, registering voters in statewide voter registration databases, providing provisional voting options, and implementing other improvements to the administration of federal elections, such as training for election officials and poll workers, polling place accessibility improvements, and disseminating information on how and where to vote.

Through September 30, 2018, a total of \$3,628,946,231¹ in federal funds has been awarded to 50 states, the District of Columbia and four U.S. territories (American Samoa, the Commonwealth of Puerto Rico, Guam and the United States Virgin Islands) hereinafter referred to as the “States.” This total includes \$380 million appropriated by Congress in 2018 to support equipment purchases and security enhancements to election systems. This 2018 appropriation was the first time since FY10 that the federal government made resources available through HAVA to support federal election improvements to the administration of federal elections.

States have reported total expenditures of \$3,400,037,361, or 85 percent of total federal funds and accrued interest, available under Sections 101, 102 and 251 of HAVA. This total includes \$30,881,027 in spending associated with the 2018 awards, which took place between April 17 and September 30, 2018 in the run-up to the 2018 election. Chart 4 shows total funds expended excluding the 2018 HAVA Funds.

¹ This includes \$300.3 million in Section 102 funds that were appropriated for the replacement of punch card or lever voting machines in 30 eligible states and \$380 million appropriated in 2018 under Section 101 of HAVA.

HAVA SECTION 101 Funds

In 2003, EAC disbursed \$349,182,267 to states under Section 101 of HAVA for activities to improve the administration of federal elections (see Table 1). As of September 30, 2018, States reported total expenditures of \$359,725,678, which reflects expenditures of federal funds and accumulated interest over the course of the award. Twenty-seven (27) States have spent all of the Section 101 funds and interest and another fourteen (14) States have spent at least 90 percent of the funds. Table 1 provides a full accounting of expenditures by States.

State	Funds Received	Interest Earned	Expenditures	Balance
ALABAMA	\$4,989,605	\$362,297	\$4,821,432	\$530,471
ALASKA	5,000,000	766,742	5,452,122	314,620
AMERICAN SAMOA	1,000,000	66,224	1,000,000	66,224
ARIZONA	5,451,369	1,010,134	2,095,600	4,365,903
ARKANSAS	3,593,165	226,288	3,819,453	0
CALIFORNIA	26,804,708	2,688,888	27,282,272	2,211,324
COLORADO	4,860,306	1,056,513	5,902,689	14,130
CONNECTICUT	5,000,000	682,868	5,682,868	0
DELAWARE	5,000,000	472,080	5,467,766	4,314
DIST. OF COLUMBIA	5,000,000	408,108	5,000,000	408,108
FLORIDA	14,447,580	1,843,679	14,183,307	2,107,953
GEORGIA	7,816,328	698,741	7,816,328	698,741
GUAM	1,000,000	12,773	1,012,773	0
HAWAII	5,000,000	1,369,777	1,687,087	4,682,690
IDAHO	5,000,000	1,807,418	6,807,418	0
ILLINOIS	11,129,030	1,264,381	12,102,242	291,169
INDIANA	6,230,481	938,781	7,196,262	0
IOWA	5,000,000	684,225	5,449,329	234,896
KANSAS	5,000,000	1,310,653	2,916,433	3,394,220
KENTUCKY	4,699,196	1,024,965	4,699,196	1,024,965
LOUISIANA	4,911,421	935,421	5,846,842	0
MAINE	5,000,000	611,679	5,606,021	5,658
MARYLAND	5,636,731	551,709	5,544,137	644,303
MASSACHUSETTS	6,590,381	904,363	7,494,744	0

Table 1 Cont. Section 101 HAVA Funds as of September 30, 2018				
State	Total Section 101 Funds Received	Interest Earned	Expenditures	Balance
MICHIGAN	\$ 9,207,323	\$ 1,662,608	\$9,884,787	\$985,145
MINNESOTA	5,313,786	64,724	5,378,510	0
MISSISSIPPI	3,673,384	443,500	4,116,884	0
MISSOURI	5,875,170	954,107	6,829,277	0
MONTANA	5,000,000	396,018	5,201,133	194,885
NEBRASKA	5,000,000	998,292	5,998,292	0
NEVADA	5,000,000	452,843	5,452,843	0
NEW HAMPSHIRE	5,000,000	1,193,153	2,460,200	3,732,953
NEW JERSEY	8,141,208	650,000	8,167,547	623,661
NEW MEXICO	5,000,000	292,244	5,292,244	0
NEW YORK	16,494,325	3,669,945	15,847,784	4,316,486
NORTH CAROLINA	7,887,740	719,637	9,495,453	0
NORTH DAKOTA	5,000,000	63,997	5,063,997	0
OHIO	10,384,931	426,837	10,811,768	0
OKLAHOMA	5,000,000	353,656	5,353,656	0
OREGON	4,203,776	59,199	4,262,975	0
PENNSYLVANIA	11,323,168	1,301,492	12,624,660	0
PUERTO RICO	3,151,144	324,191	3,467,760	7,575
RHODE ISLAND	5,000,000	140,275	5,140,275	0
SOUTH CAROLINA	4,652,412	886,692	5,300,905	238,198
SOUTH DAKOTA	5,000,000	2,385,195	4,796,646	2,588,549
TENNESSEE	6,004,507	1,047,014	6,279,290	772,232
TEXAS	17,206,595	3,727,371	18,469,359	2,464,607
UTAH	3,090,943	560,156	3,651,099	0
VERMONT	5,000,000	580,051	5,580,051	0
VIRGIN ISLANDS	1,000,000	21,806	1,000,000	21,806
VIRGINIA	7,105,890	1,130,578	7,637,378	599,090
WASHINGTON	6,098,449	259,047	6,357,496	0
WEST VIRGINIA	2,977,057	104,747	3,081,804	0
WISCONSIN	5,694,036	1,796,103	6,426,085	1,064,055
WYOMING	5,000,000	1,628,931	5,409,203	1,219,728
TOTAL*	348,646,145	49,993,116	359,725,678	39,913,583

*Reflects a deobligation of \$536,122 as a result of an audit finding. Total awarded was 349,182,267.

MASSACHUSETTS	\$7,890,854	36,111	\$1,057,216	6,869,749
MICHIGAN	\$10,706,992	54,033	\$0	10,761,025
MINNESOTA	\$6,595,610	36,883	\$0	6,632,493
MISSISSIPPI	\$4,483,541	11,096	\$241,851	4,252,786
MISSOURI	\$7,230,625	31,582	\$224,922	7,037,285
MONTANA	\$3,000,000	16,980	\$0	3,016,980
NEBRASKA	\$3,496,936	19,112	\$23,207	3,492,841
NEVADA	\$4,277,723	\$0	\$13,554	4,264,169
NEW HAMPSHIRE	\$3,102,253	643	\$129,426	2,973,470
NEW JERSEY	\$9,757,450	\$0	\$909	9,756,541
NEW MEXICO	\$3,699,470	9,868	\$807,496	2,901,841
NEW YORK	\$19,483,647	\$0	\$1,702,376	17,781,271
NORTH CAROLINA	10,373,237	\$0	\$0	10,373,237
NORTH DAKOTA	\$3,000,000	1,282	\$0	3,001,282
OHIO	\$12,186,021	54,878	\$129,589	12,111,310
OKLAHOMA	\$5,196,017	19,028	\$0	5,215,045
OREGON	\$5,362,981	39,704	\$2,290	5,400,395
PENNSYLVANIA	\$13,476,156	24,077	\$0	13,500,233
PUERTO RICO	\$3,676,962	\$0	\$0	3,676,962
RHODE ISLAND	\$3,000,000	\$0	\$584,127	2,415,873
SOUTH CAROLINA	\$6,040,794	7,886	\$0	6,048,680
SOUTH DAKOTA	\$3,000,000	30,649	\$0	3,030,649
TENNESSEE	\$7,565,418	0	\$0	7,565,418
TEXAS	\$23,252,604	123,240	\$219,447	23,156,396
UTAH	\$4,111,052	\$0	\$0	\$4,111,052
VERMONT	\$3,000,000	\$30,823	\$843,912	\$2,186,911
VIRGIN ISLANDS	\$600,000	\$0	\$18,775	\$581,225
VIRGINIA	\$9,080,731	\$0	\$0	\$9,080,731
WASHINGTON	\$7,907,768	\$40,504	\$512,533	\$7,435,739
WEST VIRGINIA	\$3,611,943	\$32,157	\$3,611,943	\$32,157
WISCONSIN	\$6,978,318	\$37,118	\$180,090	\$6,835,346
WYOMING	\$3,000,000	\$10,059	\$0	\$3,010,059
TOTAL	\$380,000,000	\$906,728	\$31,412,144	349,494,584

HAVA SECTION 251 Funds

Section 251 funds, known as Requirements Payments, were distributed to States using a formula found in HAVA that is based on a percentage equal to the quotient of the voting age population of each State and the total voting age population of all States. States are required to deposit Section 251 money in interest bearing state election accounts and the funds are available until expended.

As of the September 30, 2018, twenty-eight (28) States reported using 100 percent² of their HAVA Requirements Payment funds (including interest) and another 14 states reported using 90 percent or more of their funds and interest. States reported cumulative expenditures of \$2,698,508,681 (See Table 3).

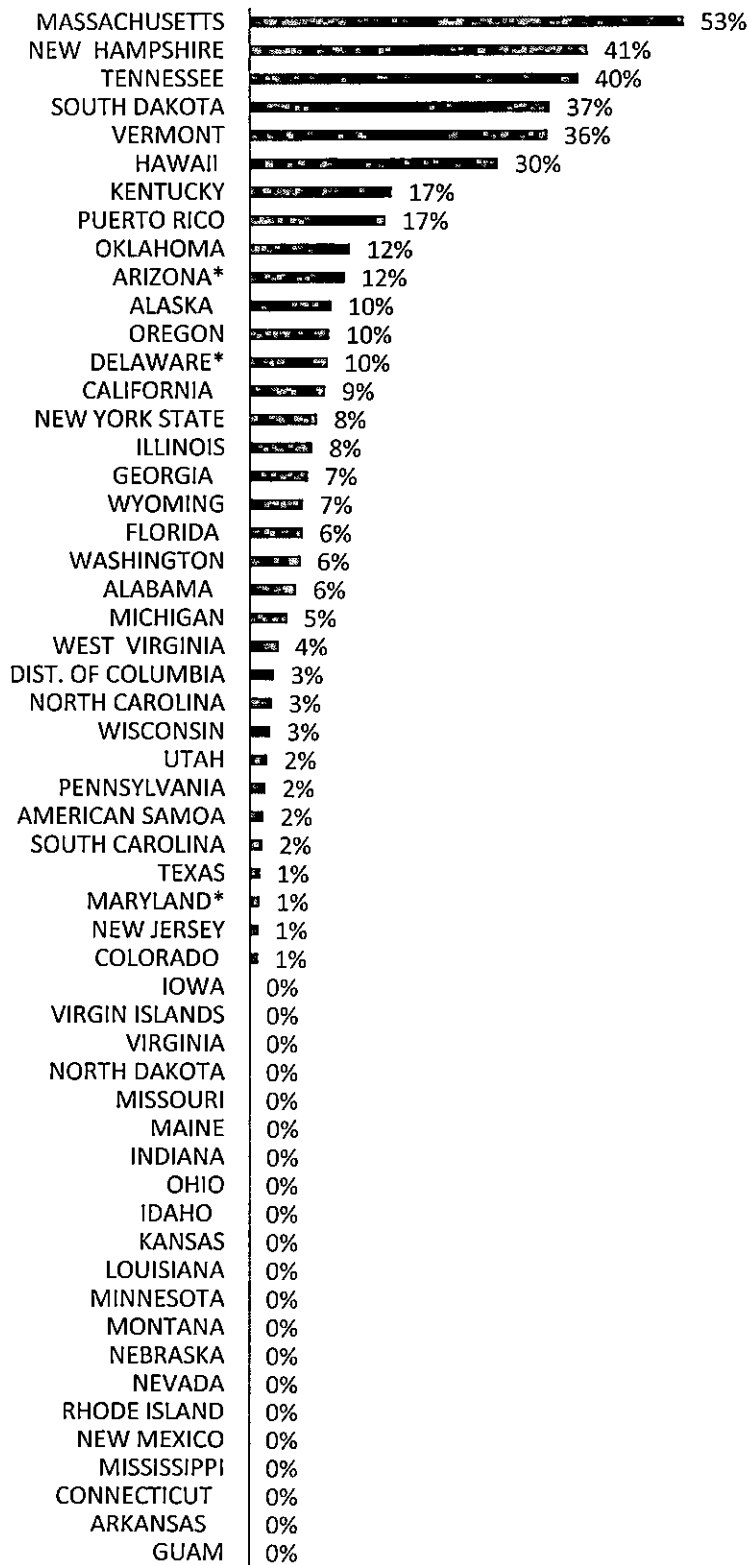
Table 3 Section 251 HAVA Funds as of September 30, 2018

State	Total Section 251 Funds Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
ALABAMA	\$40,227,863	\$2,369,451	\$40,436,616	\$2,160,698
ALASKA	\$13,021,803	\$2,650,959	\$13,843,301	\$1,829,461
AMERICAN SAMOA	\$2,490,652	\$292,118	\$2,782,770	\$0
ARIZONA	\$45,516,688	\$4,353,350	\$47,508,539	\$2,361,498
ARKANSAS	\$24,233,666	\$2,542,154	\$26,775,820	\$0
CALIFORNIA	\$296,305,593	\$44,631,006	\$303,422,823	\$37,513,776
COLORADO	\$38,767,048	\$4,719,210	\$42,972,582	\$513,677
CONNECTICUT	\$31,095,158	\$4,392,980	\$35,488,138	\$0
DELAWARE	\$13,021,803	\$1,930,256	\$13,004,721	\$1,947,338
DISTRICT OF COLUMBIA	\$13,028,257	\$1,922,983	\$14,746,048	\$205,191
FLORIDA	\$148,633,048	\$24,310,937	\$162,028,349	\$10,915,636
GEORGIA	\$72,641,827	\$761,687	\$67,906,200	\$5,497,314
GUAM	\$2,319,361	\$48,049	\$2,367,410	\$0
HAWAII	\$13,028,257	\$977,446	\$12,499,108	\$1,506,595
IDAHO	\$13,021,803	\$1,267,652	\$14,289,455	\$0
ILLINOIS	\$110,593,988	\$9,297,474	\$118,549,567	\$1,341,896
INDIANA	\$54,440,282	\$2,280,602	\$56,676,561	\$44,322
IOWA	\$26,645,880	\$1,464,690	\$28,083,331	\$27,240
KANSAS	\$24,033,426	\$2,222,954	\$30,853,941	\$0
KENTUCKY	\$36,901,642	\$4,794,078	\$34,404,580	\$7,291,139

² States that have over 99% of funds and interest spent are counted as 100% expended for purposes of this report. Actual funds remaining are shown for each state on the chart.

State	Total Section 251 Funds Received	Interest Earned	Total Expenditures	Balance of Funds and Interest
LOUISIANA	\$39,350,512	\$3,552,964	\$42,903,476	\$0
MAINE	\$13,021,803	\$1,522,719	\$14,537,278	\$7,244
MARYLAND	\$47,663,156	\$3,888,041	\$51,527,784	\$23,413
MASSACHUSETTS	\$58,589,549	\$11,498,511	\$28,222,757	\$41,865,303
MICHIGAN	\$88,535,685	\$7,641,697	\$92,435,575	\$3,741,807
MINNESOTA	\$43,962,194	\$3,758,390	\$47,501,444	\$0
MISSISSIPPI	\$25,152,465	\$1,588,892	\$26,741,357	\$0
MISSOURI	\$50,394,880	\$4,255,352	\$54,177,399	\$472,833
MONTANA	\$13,028,257	\$618,633	\$13,979,996	\$0
NEBRASKA	\$15,442,405	\$1,046,168	\$16,488,573	\$0
NEVADA	\$18,155,632	\$1,272,294	\$19,427,926	\$0
NEW HAMPSHIRE	\$13,021,803	\$2,292,595	\$10,173,179	\$5,141,219
NEW JERSEY	\$76,360,392	\$5,808,946	\$81,696,605	\$472,733
NEW MEXICO	\$15,599,671	\$271,854	\$15,871,525	\$0
NEW YORK	\$172,076,865	\$33,085,355	\$193,587,917	\$11,574,303
NORTH CAROLINA	\$73,421,775	\$7,370,242	\$77,418,650	\$3,373,367
NORTH DAKOTA	\$13,028,257	\$1,355,754	\$14,258,148	\$125,863
OHIO	\$102,069,874	\$6,307,853	\$108,377,697	\$0
OKLAHOMA	\$30,200,723	\$4,101,437	\$29,420,654	\$4,881,506
OREGON	\$31,243,106	\$3,988,360	\$31,243,105	\$3,988,360
PENNSYLVANIA	\$112,821,809	\$16,861,352	\$126,737,641	\$2,945,520
PUERTO RICO	\$5,868,252	\$222,622	\$4,503,921	\$1,586,952
RHODE ISLAND	\$13,021,803	\$485,182	\$13,506,985	\$0
SOUTH CAROLINA	\$36,384,617	\$910,483	\$37,121,805	\$173,295
SOUTH DAKOTA	\$13,028,257	\$5,107,330	\$11,373,403	\$6,762,184
TENNESSEE	\$51,877,745	\$6,914,050	\$32,108,378	\$26,683,417
TEXAS	\$180,251,805	\$12,381,621	\$192,633,426	\$0
UTAH	\$18,481,440	\$705,044	\$18,549,134	\$637,350
VERMONT	\$12,453,257	\$2,673,691	\$7,604,787	\$7,522,161
VIRGIN ISLANDS	\$2,319,361	\$2,179	\$2,319,361	\$2,179
VIRGINIA	\$64,449,288	\$9,562,569	\$74,011,857	\$0
WASHINGTON	\$52,995,253	\$6,550,527	\$56,052,533	\$3,493,247
WEST VIRGINIA	\$17,184,961	\$1,183,796	\$17,520,296	\$848,461
WISCONSIN	\$48,296,088	\$3,566,337	\$51,862,425	\$0
WYOMING	\$13,028,257	\$1,079,409	\$13,971,822	\$135,843
Total	\$2,602,749,240	290,662,283	2,698,508,681	194,464,562

Remaining HAVA Funds as of September 30, 2018
 (Excluding New 2018 Grants)



State Plans and Expenditures of 2018 HAVA Funds

Reported Spending as of September 30, 2018		
Category	Amount	Percentage of Total Spent
Cybersecurity	18,283,414	58.2%
Voting Equipment	\$10,658,794	33.9%
Voter Registration System	2,107,074	6.7%
Other	312,093	1.0%
Election Auditing	19,881	0.1%
Communication	27,747	0.1%
Total	\$31,409,003	100%

As noted earlier, on Friday, March 23, 2018, President Donald J. Trump signed the Consolidated Appropriations Act of 2018 into law. The Act included \$380 million in Help America Vote Act (HAVA) funds to improve the administration of elections for Federal office, including to enhance election technology and to make election security improvements, marking the first new appropriation for HAVA funds since FY2010.

The funding provided states with additional resources to secure and improve election systems. States could begin spending funds once they received their notice of grant award on April 17, 2018. However, most states waited until funds were transferred to their state election accounts and many states had to get state legislative approval before spending funds.

States and territories eligible to receive the funds were required to provide a budget and state narrative for how they would be used. The EAC published the narratives and budgets for 48 out of 55 eligible states and territories public on August 21, 2018. Seven remaining states and territories were granted extensions and had their budgets and narratives into the EAC by mid-September 2018. By September 20, 2018, 100 percent of funds had been disbursed to states.

According to these narratives and budgets, the vast majority of states and territories plan to spend their allotted funds within the next two or three years. Each funding recipient was required to file a standard Federal Financial Report and updated program narrative to the EAC by December 31, 2018.

The following is a summary of how states were able to utilize the 2018 HAVA Funds within the first six months of them being made available, based on these Progress and Financial Reports:

- **Alabama** expects to expend the \$6.1 million the state received in 2018 HAVA funds, and the required state match of \$308,020, in FY2019 to make upgrades to and replace voting equipment, mitigate cyber vulnerabilities, establish post-election auditing protocols statewide, continue the provision of the computerized statewide voter registration list for the entire state.
- **Alaska** plans to use its \$3.15 million to replace the state's 20-year old voting system.
- **American Samoa** used a portion of its HAVA funding to repair and restore equipment and election offices damaged during Tropical Cyclone Gita so they would be functional ahead of the 2018 election. Going forward, the territory is planning a complete upgrade of its voter registration system, continuing to provide special needs services to voters with disabilities and increasing its voter outreach efforts.
- **Arizona** funded a comprehensive security assessment of its election systems and provided training to help each of the state's fifteen counties understand the different types of existing

security threats and what support is available. Long-term, the state plans to award election security sub-grants to counties and create an election security position within the Secretary of State's office.

- **Arkansas** established cost-sharing agreements with the counties to replace aging voting equipment. New acquisitions ensure that a paper trail for ballots cast is present in all Arkansas counties and almost 70 percent of Arkansas voters voted on the newly integrated election equipment system in the 2018 Midterm Election. Of the initial \$4,724,225 in funds available through HAVA, Arkansas had only \$44,305 in funds remaining.
- **California** is funding cybersecurity support and training, polling place accessibility, election auditing and vote center implementation through FY2021 at the county level. The state is also using funds to make security enhancements to its centralized voter registration system and personnel costs.
- **Colorado** will use its 2018 HAVA Funds to enhance technology and security in the state's election process, including improving risk-limiting audits and other audits of election-related systems in 2019 and beyond. From April 17, 2018 to September 30, 2018, Colorado expended \$211,124.82 (including \$109,899.80 in 2018 HAVA Funds and earned interest) on Colorado Voting Systems (COVS) training that was necessary to implement a ballot level comparison Risk-Limiting Audit (RLA). An additional \$99,064 was used for Election Preparedness for Infrastructure and Cybersecurity (EPIC) tabletop exercises with county election and IT officials.
- **Connecticut** is purchasing voting equipment, making security enhancements to address cyber vulnerabilities, improving post-election audits and voter registration systems and management, enhancing security training for election officials and improving voting accessibility.
- **Delaware** plans to purchase new voting equipment, including a new voting system with a voter verifiable paper audit trail, an absentee system and an Election Management/Voter Registration system which will move elections from the state's aging mainframe.
- **Florida** plans to use the \$19,187,003 the state received in 2018 HAVA funds for three primary projects. \$15,450,000 will be used to establish an online grant program for 67 county supervisors of elections to enhance election security. \$1,987,003 will be used to establish an online grant program for county supervisors of elections to improve voting accessibility. The remaining \$1,750,000 will be earmarked by the Florida Department of State to implement security enhancements to the state voter registration system, contract a team of cybersecurity specialists to provide support to the state and county supervisor of elections offices, and to fund a voter education campaign to educate voters on how to get ready to register and vote in an election. As of September 30, 2018, \$95,688.91 had already been expended.
- **Georgia** plans to increase election security, simplicity and accessibility by purchasing secure voting devices that produce a voter-verifiable paper ballot. The state will also provide an online sample ballot for all voters, improve its voter registration database, conduct election auditing and testing, and purchase ALBERT sensors, cybersecurity services and new e-poll books.
- **Guam** will use its funds to replace and upgrade voting equipment, perform election auditing, make improvements to its voter registration system, upgrade cybersecurity equipment and provide training.
- **Hawaii** will be utilizing its \$3.1 million in funds to enhance the election cybersecurity infrastructure and update equipment related to the statewide voter registration system, voting equipment and vote counting system. As of September 30, 2018, \$4,310.56 was used to establish telecommunications and network services at Counting and Control Centers during the 2018 Elections and an additional \$77,486.93 was used to hire an Election Information Specialist responsible for enhancing accessibility to elections for voters with disabilities and additional staff to perform duties required to administer elections for federal office.

- **Idaho** plans to use its new HAVA appropriation to hire staff, award sub-grants to voting districts, secure new voting equipment, perform election auditing, acquire a new voter registration system, make cybersecurity improvements and software updates, and provide staff trainings. Thus far, the state has expended \$513,064.10 of both federal funds and interest for acquiring software to deploy security patches across the state network, initial voter registration system upgrades and personnel.
- **Illinois** will use its funding for a cybersecurity information sharing program, hiring a Cyber Navigator/Advisor, providing cybersecurity resources for local election authorities and implementing a statewide network to provide centralized monitoring, mitigation and security services. Thus far, the State Board of Elections has used the funds for relevant equipment and software, Electronic Registration Information Center (ERIC) Association dues and relevant conference and information sharing costs.
- **Indiana** helped counties implement multi-factor authentication systems for accessing voting equipment and conducted cybersecurity training for all county officials during the state's annual election administrators conference. Going forward, the state plans to acquire additional election technology, implement e-poll book vendor network security enhancements, deploy auditable voting systems and perform election night reporting security enhancements.
- **Iowa** conducted cybersecurity training seminars for county auditors and staff and participated in a pilot program for a self-assessment cybersecurity tool. The Secretary of State's Office also implemented two-factor authentication for access to the statewide voter registration system, purchased additional security protections for the state's election night reporting system and partnered with the Department of Homeland Security to conduct two tabletop exercises. Finally, Iowa was able to purchase additional security protections for the state's election night reporting system.
- **Kansas** will use its funds to ensure every voting machine has a voter verifiable paper audit trail, conduct post-election audits after every election, improve the security of the statewide voter registration system, increase cybersecurity efforts at all levels of election administration and create, maintain and train local election officials on a comprehensive security communications plan.
- **Kentucky** used some of its funds during the FY2018 reporting period to acquire Trustwave, cloud-based and managed security services designed to protect data and reduce security risk. The State Board of Elections is in the process of working with Trustwave to install and set up the equipment.
- **Louisiana** will use 2018 HAVA funds and the state match for a new electronic voting system.
- **Maine** plans to upgrade its voting equipment and Central Voter Registration (CVR) system hardware and software, implement election night reporting, cybersecurity software improvements, monitoring and training, and improve ballot security and online training.
- **Maryland** will replace and upgrade voting equipment, perform election audits, upgrade voter registration system servers and software in off-election years and enhance system monitoring activities, mitigating cyber vulnerabilities, refining an incident management plan and providing training. Thus far, the state has spent \$1,302 of its allocated federal funds on statewide tabletop exercises and \$176,139.50 of its state match on Voted Ballot Audits following the 2018 Primary Elections and implementing two-factor authentication and enhancing its virtual private network (VPN) security monitoring.
- **Massachusetts** made network security upgrades for its voter registration system, hired a network security engineer and conducted security training for election staff. The Secretary of State's Office also plans to use funds to acquire new voting equipment, upgrade the state's voter registration system and improve the cybersecurity of its election system.

- **Michigan** is focusing on cybersecurity, information and physical security and providing funding and resources statewide to allow for the completion of detailed election system security assessments at the state, county and local level.
- **Minnesota** is using \$6,925,391 in 2018 HAVA Funds and required state match to strengthen, secure and modernize Minnesota's Statewide Voter Registration System (SVRS); assess the state's data sharing and post-election review/audit process; improve secure information sharing with counties; enhance website security and accessibility and recruit and train election officials. The Secretary of State's Office will also use funds to invest in cybersecurity and information technology upgrades, expand absentee and mail-voting for voters with disabilities and provide sub-grants to local jurisdictions for improved election security and accessibility.
- **Mississippi** is using its funds to upgrade its Statewide Elections Management System, addressing cyber vulnerabilities, implementing post-election auditing and funding certain permissible county expenditures.
- **Missouri** spent most of its allocated 2018 HAVA Funds to implement cybersecurity enhancements that protect against attempts to penetrate the Missouri Centralized Voter Registration System. In September, the state also hosted the National Election Security Summit attended by federal, state and local election authorities to discuss practical ways to mitigate threats and vulnerabilities.
- **Montana** is replacing its statewide voter registration system and funding a 50 percent cost match with counties to purchase new voting equipment. They are also undertaking a major cybersecurity upgrade and hiring election and voter security IT personnel.
- **Nebraska** is using 2018 HAVA Funds to replace voting equipment, implement security upgrades and system enhancements to its voter registration system, install and maintain ALBERT sensors and perform cybersecurity scans and testing. The state is also using this federal funding to train election division staff and county election officials, provide resources for voters with disabilities and put additional security measures in place for election night reporting.
- **Nevada** will use the funds to upgrade voting equipment, provide sub-grants to jurisdictions, evaluate the state's cyber vulnerabilities, expand upon current election auditing practices and procedures, increase voter outreach and training.
- **New Hampshire** is enhancing election technology and making security improvements, improving voting systems and technology, educating voters, training election officials and election workers and improving access for voters with disabilities.
- **New Jersey** plans to make improvements to its cyber and physical security, voter registration system, voting equipment, election auditing, Americans with Disabilities Act compliance and training for election officials. Thus far, the state has expended its 2018 HAVA Funds on a Department of Homeland Security-administered tabletop security training session for county election officials.
- **New Mexico** hired a full-time IT security and compliance administrator whose responsibilities include implementing additional security practices to safeguard sensitive data and election systems and protect against cyber vulnerabilities. The state also purchased scan tabulation systems that feature ballot image capture and audit capabilities.
- **New York** spent approximately \$1.7 million in 2018 on several security initiatives, including a contract with Grant Thornton to conduct a uniform comprehensive risk assessment of every county board of elections. As of September 30, 2018, 22 of 58 assessments were complete. The state contracted another security firm to provide intrusion detection and log monitoring services for all county boards of elections. Additionally, 712 state and county election officials and election vendors have attended security awareness training and all county board of elections officials have attended at least one cybersecurity tabletop exercise training.

- **North Carolina** plans to use its 2018 HAVA funds to modernize their statewide elections information management system, perform election auditing, undergo security assessments, hire a Chief Information Security Officer and implement a Cyber Advisory Panel.
- **North Dakota** is spending its entire 2018 HAVA award and required five percent state match on procuring a paper-based, HAVA-compliant voting system.
- **Ohio** is using its funds to make enhancements to its statewide voter registration system database, provide enhanced cybersecurity for election email accounts, conduct tabletop exercises and training, launch an IT and email support pilot project and conduct post-election audits through 2020.
- **Oklahoma** is purchasing e-poll books and document scanners for local election offices, upgrading its online voter registration system by 2020, providing training for county and state election boards, and ensuring there is a robust plan in place for cyber and physical security.
- **Oregon** is making improvements to the Oregon Elections System for Tracking and Reporting, securing state and local election systems and increasing IT security capacity and voter registration efficiency. The state also plans to build a feature so voters can track their ballot at all stages of the election process, provide public access to campaign finance reports and expand capacity and public visibility.
- **Pennsylvania** is replacing aging voting equipment that is reaching the end of its usable life with new equipment that has a voter verifiable paper audit trail.
- **Puerto Rico** plans to use its 2018 HAVA funds to enhance election cybersecurity and network infrastructure and upgrade Election Day voter registration.
- **Rhode Island** purchased a platform for the Centralized Voter Registration system that encrypts all data within it. The state also purchased another system that monitors for and protects the Centralized Voter Registration System from ransomware. In addition, the state purchased a system that provides real-time analysis of security threats, sends alerts if issues are detected and quarantines devices if there is abnormal activity.
- **South Carolina** is using its \$6 million in 2018 HAVA Funds to harden its security posture and enhance the resilience of its elections.
- **South Dakota** is replacing aging voting equipment, including ballot marking devices and ballot tabulators purchased in 2005, and making cybersecurity upgrades to the statewide voter registration file and election night reporting page.
- **Tennessee** is providing sub-grants to assist counties in the purchase of approved voting systems, making improvements to its voter registration system and providing cybersecurity scans and training for each county election commission office.
- **Texas** worked with its Voter Registration system vendor in 2018 to make security updates to its system, including integration of a standalone portal and data encryption. The state also acquired cybersecurity training and made it available free of charge to all 254 counties in advance of the 2018 election. Prior to the 2018 election, 150 officials attended the training.
- **The U.S. Virgin Islands** is conducting a risk assessment and upgrades to its voting equipment, updating its voter registration system, developing and implementing a cybersecurity plan, and providing cyber risk management training for Board of Elections leadership, staff and vendors.
- **Utah** will purchase new voting equipment, replace the state's voter registration database and implement additional security measures and training for both counties and the state.
- **Vermont** used its 2018 HAVA Funds to replace and upgrade voting equipment, implement post-election audits, mitigate cyber vulnerabilities and provide required cybersecurity training for all town and city clerks in the spring of 2018, prior to the 2018 Midterm Elections. Of the initial \$3,150,000 available through federal appropriations, the required state match and interest, as of September 30, 2018, Vermont had expended \$843,912.28.

- **Virginia** is securing the Department of Elections' infrastructure and developing and implementing security and continuity of operations plans.
- **Washington** has implemented advanced firewall protection for the state's centralized election system and installed an advanced threat detection and prevention appliance. The state also acquired a database storage device on the Voter Registration system that has back-up and recovery capabilities. All equipment and software, with the exception of the database storage device, was in place prior to the 2018 Midterm Election. The state also held cybersecurity training for election officials that is a precursor for a cybersecurity training program individually tailored for each county in the state.
- **Washington, D.C.** has used \$399,400 of its funds to purchase new voting equipment and hire additional staff to increase the number of early voting centers across the District of Columbia, to train election officials and to produce voter education materials. The District of Columbia plans to use its remaining 2018 HAVA Funds to acquire additional equipment, increase maintenance and support, hire a full time cybersecurity expert, hire and train additional poll workers, continue voter education and outreach, and invest in technology to improve all aspects of voter registration and election administration.
- **West Virginia** used its 2018 HAVA funds to establish a grant program available for counties to be awarded funding for election equipment, physical security, cybersecurity and e-poll books.
- **Wisconsin** will address the immediate security needs of the state such as purchasing software, implementing additional security measures to protect the statewide voter registration system, creating federally funded staff positions and hiring additional IT developers. Wisconsin will also collect feedback from local election officials, voters and election partners to determine long-term election security needs.
- **Wyoming** will use the 2018 HAVA funds to replace outdated voting equipment originally purchased in 2005 and enhance the state and county cybersecurity infrastructure.



State of Tennessee
Department of State
Division of Elections

Approved Voting Machines – January 8, 2018

Machine	EAC Certification Number	Date Certified by SEC	Notes
Diebold/Prémier/ES&S Gems 1-18-22	N-1-06-12-12-003	February 15, 2005	This version includes both a DRE and Precinct Optical Scan solution. (Balotar – Ballot on Demand – Certified 10/12/2015) Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
Dominion Voting Democracy Suite 4.0	EAC Certification Number DVS-40-G-10	August 13, 2012	Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
Dominion Voting Democracy Suite 4.14	EAC Certification Number DemSuite4-14	January 13, 2014	Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
Dominion Voting Democracy Suite 4.14-A Democracy Suite 4.14B Democracy Suite 4.14-D	EAC Certification Number DemSuite-4.14-A DVS-DemSuite-4.14B DVS-DemSuite-4.14-D	January 11, 2016	Note: The next review will be required no later than December 1, 2023.
ES&S Unity 2.5	N-1-02-22-22-003	October 11, 2005	This version includes both a DRE and Precinct Optical Scan solution. (Balotar – Ballot on Demand – Certified 10/12/2015) Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
ES&S 3.0.1.1	N-2-02-22-22-006	August 21, 2007	(Balotar – Ballot on Demand – Certified 10/12/2015) Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.

Machine	EAC Certification Number	Date Certified by SEC	Notes
ES&S EVS 5.2.0.0	ESSEVS5200	October 12, 2015	EVS 5.2.0.0 - counties are required to use the DS200 ballot tote bins and ballots must be serially-numbered with a ballot stub. Express Vote Ballot on Demand - approval requires ballots must be serially-numbered with a ballot stub. Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
ES&S EVS 5.2.1.0	ESSEVS5210	January 9, 2017	EVS 5.2.1.0 - counties are required to use the DS200 ballot tote bins and ballots must be serially-numbered with a ballot stub. Express Vote Ballot on Demand - approval requires ballots must be serially-numbered with a ballot stub.
ES&S EVS 5.2.2.0	ESSEVS5220	January 8, 2018	EVS 5.2.1.0 - counties are required to use the DS200 ballot tote bins and ballots must be serially-numbered with a ballot stub. Express Vote Ballot on Demand - approval requires ballots must be serially-numbered with a ballot stub.
Hart InterCivic eSlate System Version 3.4	N-1-04-22-22-003	October 11, 2005	Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
Hart InterCivic eSlate System Version 5.0	N-1-04-22-22-006	July 17, 2007	Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
Hart InterCivic Verity 1.0	HRT-Verity-1.0	December 1, 2015	The next review will be required no later than December 1, 2023.
Hart InterCivic Verity 2.0	HRTVerity2.0	January 8, 2018	
MicroVote Infinity EMS 3.1.0.0	N-1-09-22-22-001	January 17, 2006	Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
MicroVote Infinity EMS 4.0B (Modification)	EAC Certification Number MVTEMS40B	October 8, 2012	Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
MicroVote Infinity 4.1 (Modification)	EAC Certification Number MVTEMS41	July 10, 2017	Infinity 4.1 - Software Upgrade - SEC approved the 4.1 software for existing voting machines.
Unisyn OpenElect 1.0.1	EAC Certification Number: UNS10121966-OE-WI	April 9, 2012	Note: The next review will be required no later than December 1, 2023. Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.

Machine	EAC Certification Number	Date Certified by SEC	Notes
Unisyn OpenElect 1.1	EAC Certification Number: UNS10121966-OE-1.1	June 18, 2012 April 14, 2012	April 14, 2014 – de minimis change Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
Unisyn OpenElect 1.2	EAC Certification Number: UNS10121966-OE-1.2	April 14, 2014	(Ballot on Demand – Certified 7/13/2015) Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.
Unisyn OpenElect 1.3	EAC Certification Number: 04211950-1.3	July 13, 2015	Note: The State Election Commission met on December 1, 2015, and recertified this machine for use in TN. The next review will be required no later than December 1, 2023.

Exhibit ~~1~~ 0

Sworn Senate Testimony by

Computer Programmer Clint Curtis

video link & transcript

7 pages

Video Link: <https://rumble.com/v1h6lwn-clinton-eugene-curtis-elections-have-been-stolen-using-machine-algorithms-s.html>

Video of interview of Mr. Curtis and Senate testimony intermixed: Video Link: <https://www.simpson4auditor.com/post/clinton-curtis-testimony-on-how-elections-have-been-stolen-using-algorithms-since-at-least-2000>

Transcript link: https://www.bradblog.com/?page_id=9437

Transcript of sworn testimony by computer programmer Clint Curtis, before the U.S. HOUSE OF REPRESENTATIVES Democrats of the Judiciary Committee, December 13, 2004, as seen on video above follows below.

For the full compendium of our Clint Curtis/Tom Feeney vote-rigging scandal, which we originally broke on December 6, 2004, please see: <https://BradBlog.com/ClintCurtis>.

Attorney Cliff Arnebeck called Clint Curtis before the Committee, for the purpose of determining if the vote-counting process of the 2004 U.S. General Election in Ohio could have been manipulated by computer.

[Mr. Curtis is sworn in by the court reporter, on-camera, but without sound. Then sound commences.]

CLIFF ARNEBECK: Mr. Curtis, would you please state your full name for the record.

CLINT CURTIS: My name is Clinton Eugene Curtis.

ARNEBECK: And where do you reside?

CURTIS: Tallahassee, Florida.

ARNEBECK: And what is your profession?

CURTIS: I'm a computer programmer.

ARNEBECK: Would you please speak into the microphone so that the audience can hear your testimony.

CURTIS: I'm a computer programmer.

ARNEBECK: Mr. Curtis, are there programs that can be used to secretly fix elections?

CURTIS: Yes.

ARNEBECK: How do you know that to be the case?

CURTIS: Because in October of 2000 I wrote a prototype for present Congressman Tom Feeney, at the company I work for in Oviedo, Florida, that did just that.

ARNEBECK: And when you say, "Did just that," it would rig an election?

CURTIS: It would flip the vote fifty-one forty-nine to whoever you wanted it to go to, and whichever race you wanted it to win.

ARNEBECK: And would that program that you designed be something that elections officials, that might be on county boards of elections, could detect?

CURTIS: They'd never see it.

[Audience: "Hmmm!"]

ARNEBECK: Mr...[Audience speaks "... question again"] Would you answer that question once again?

CURTIS: They would never see it.

ARNEBECK: So how would such a program, a secret program that fixes the election, how could it be detected?

CURTIS: You would have to view it either in the source code, or you'd have to have a receipt, and then count the hard paper against the actual vote total. Other than that, you won't see it.

ARNEBECK: Alright, Mr. Curtis, if you had been asked, you or others with your professional expertise, had been asked to design a protective program, a program that would protect the Ohio elections from against such software to fix the election, could you have done so?

CURTIS: If we'd been asked to make a program that could fix the election? Sure, anybody can do it.

ARNEBECK: No, could you have designed a program, a procedure, a protocol, that would have protected Ohio against this kind of rigging?

CURTIS: No, you have to look at the source code. You have to get, probably, programmers from both, or all, parties to look at the source code, and determine if there's anything in there that shouldn't be there. I mean, it's a simple program, you're adding one, two persons total. It's a hundreds lines of code, tops. There's.. [unintelligible]

ARNEBECK: Are you aware of whether there was any protective action in Ohio against this kind of vote rigging through software?

CURTIS: I don't know.

ARNEBECK: You don't know?

CURTIS: I don't know.

ARNEBECK: You were not asked to assist in the development of any protective system, is that correct?

CURTIS: No I was not.

ARNEBECK: In your op.. uh.. have you reviewed at all the elections results in Ohio?

CURTIS: No I haven't.

ARNEBECK: OK. Given the availability of such vote-rigging software, and the testimony that has been given under oath of substantial statistical anomalies, and gross differences between exit polling data and the actual

tabulated results, do you have an opinion whether or not the Ohio election, the Presidential election, was hacked?

CURTIS: Yes I would say it was. I mean, if you ... have exit polling data that is significantly off from the vote, then it's probably hacked.

ARNEBECK: And your testimony is under oath?

CURTIS: Yes, sir.

ARNEBECK: And the testimony you've given is true?

CURTIS: Yes, sir.

ARNEBECK: Thank you.

[Applause, considerable.]

REP. STEPHANIE TUBBS JONES Congresswoman Waters and I have the same question:

[Curtis is directed: "Back to the podium." Curtis returns to podium.]

REP. STEPHANIE TUBBS JONES What did you say you were asked to prepare?

CURTIS: I was asked by Tom Feeney, he's now Congressman, at that time he was Speaker of the House of Florida; Yang Enterprises' --- which is the company I worked for --- lobbyist; and their corporate attorney. He wore a lotta hats.

REP. STEPHANIE TUBBS JONES And at that time, he was the Speaker of the House of Florida, is that what you said?

CURTIS: Yes.

REP. STEPHANIE TUBBS JONES Ok, thank you.

CONGRESSMAN JERROLD NADLER: You say he was the lobbyist for the voting machine company at the same time he was Speaker of the House?

CURTIS: I don't know what the voting machine company, but he was a lobbyist for Yang Enterprises. We had NASA contracts...

CONGRESSMAN JERROLD NADLER: Yang Enterprises did what, computers?

CURTIS: Computers.

REP. JERROLD NADLER: OK. And he was your lobbyist, your company's lobbyist?

CURTIS:
He was the lobbyist for Yang Enterprises.

REP. JERROLD NADLER: And he asked you to design a code to rig an election?

CURTIS: Yes.

REP. JERROLD NADLER: While he was Speaker of the Florida House?

CURTIS: Yes.

REP. JERROLD NADLER: Was that during, or previous to, the 2000 election?

CURTIS: Yes, October, end of September.

REP. JERROLD NADLER: Did he ever express why he wanted the code to rig an election?

CURTIS: No. I immediately assumed that they were trying to keep you guys from cheating on them.

[Audience laughs.] So I wrote up the documentation of what you would look for in the source code, how you would make sure that you didn't get, you know, taken advantage of, make sure that all voting machines had receipts, because that way you could back count the ones that looked funny.

REP. JERROLD NADLER: By "receipts," you mean a paper trail?

CURTIS: Yes, paper trail. And I handed that in to Mrs. Yang and said, "Here's your report, here's your program." And she said, "You don't understand. We need to hide the fraud in the source, in the source code."

REP. JERROLD NADLER: Hide the fraud, not reveal it?

CURTIS: Not reveal the fraud, "Because we need it to control the vote in South Florida." That's what she it said.

[Audience: "Woh!!"]

REP. JERROLD NADLER: To your knowledge, was this used?

CURTIS: I have no idea, I, I was ready to leave. [Audience/Curtis laugh.] I retired and left the company.

REP. JERROLD NADLER: Your testimony just a moment ago I think you said just before you left in answer to Congresswoman... Jones' question, would you just repeat what you said in reference to the exit polls?

CURTIS: The exit polls should not be significantly different from the vote.

REP. JERROLD NADLER: And if they were, you would conclude what?

CURTIS: I would conclude someone's playing with the vote.

REP. JERROLD NADLER: Not with the exit polls?

CURTIS: That's possible too.

REP. JERROLD NADLER: OK.

CURTIS: Something is definitely skewed.

REP. JERROLD NADLER: Something is skewed in one or the other?

CURTIS: Right. To select which one, you'd have to see where the problem is.

REP. JERROLD NADLER: Let me ask you one further question. Assuming for the moment that such software, that's what you call it? such software to rig a vote, was used, in one or more machines in Ohio or in Florida, could you today detect that, if you looked at the source code?

CURTIS: If you could get the machines, and they had not been patched yet, I mean once they get in and touch 'em, anything could happen. You could also set timers to do that, but then you'd see the timers. Then you'd have to take those machines, decompile 'em, which I couldn't do, but possibly a Microsoft or MIT something, could do, you might, you might, be able to do.

REP. JERROLD NADLER: You might.

CURTIS: Depends on how good they are at destroying what they had.

REP. JERROLD NADLER: Destroying what they had by tampering with the machine afterwards, or by programming it with destroying instruction in the first place?

CURTIS:
Right.

REP. JERROLD NADLER: Either or both?

CURTIS: Either or both. Because since you didn't actually see what's in there. So you don't actually know if the code is running in single executable, or running in various modules. If it's running in modules, you can make the code actually eat itself.

[Audience murmurs, then "Wow!"]

REP. JERROLD NADLER: Let me ask you just one further question. We've been told, I've been told, that people who assume that lots of the election results, a large fraction of the election results in this state may have been affected by computerware fraud in the computer are paranoid, because in order to do that you would have to have access to thousands of machines, and that would be readily detectable. Is that true?

CURTIS: It depends on the technology used. If you did a central tabulation machine that fed in, all you would have to do is set a flag. If you set a flag, the central tabulation machine would then flip your vote.

REP. JERROLD NADLER: So if you, so one person putting in bad code in a central tabulation machine could affect thousands and thousands, or tens of thousands, of votes?

CURTIS: Right. And you could activate it ...

[Congressman Nadler starts to speak, but stops]

CURTIS: ...you could activate it either automatically, or you could make it so that there's code existing on like an automic [?] machine that feeds it, where you would punch it in, it would set the flag, server would receive the flag, and then...

REP. JERROLD NADLER: And if you had a recount ... [unclear] ... no paper trail --- assuming that would happen --- would that be revealable by seeing a discrepancy between what the tabulator, the central tabulator trail [unclear] the individual machines which had not been tampered with, have?

CURTIS: Not if I wrote it.

REP. JERROLD NADLER: Why not?

CURTIS: I would make it match.

REP. JERROLD NADLER: You could work back from the tabulator to the individual machines? So the tabulator would tell the machines to switch their results?

CURTIS: Yes. It talks both ways. You can flip it to do whatever you need.

REP. JERROLD NADLER: And they actually do talk to each other, the machines...?

CURTIS: Yes; once it's hooked up, if it's networked together, they can talk to each other.

REP. JERROLD NADLER: So there's absolutely no assurance whatsoever that anything could be [right?] with these machines?

CURTIS: Absolutely none, unless you look at the source code, and make sure it's safe before it goes out.

REP. JERROLD NADLER: Thank you very much.

[Madam Chair:] Thank you, Congressman Nadler. I know that Congresswoman Waters has questions, and then Senator Miller, and then Congresswoman Stephanie Tubbs-Jones.

REP. MAXINE WATERS: This will only a moment, if you will come back to the uh, microphone.

[Audience laughs]

CURTIS: I'm new at this.

REP. MAXINE WATERS: As you know, there has been a lot of discussion about, I think it was Diebold Company; their relationship to the President, and the administration, and supposedly comments about helping to insure that the President was re-elected. In your world, in your environment, have you heard any of this kind of discussion? Do you know people at Diebold? Do you have any sense of any actions that may have been taken?

CURTIS: Uh, I don't know anything about that at all.

REP. MAXINE WATERS: Thank you.

[Madam Chair calls Dr. Miller]

DR. MILLER: I suspect that people will attack you in terms of your credibility. Could you restate once again your, your credentials.

CURTIS: Uh, I'm a programmer, I worked for NASA, I worked for Exxon Mobil, I worked for um, Florida Department of Transportation, and other elements of my story, because this company, well, let's get into it. Why not? This company also had a NASA contract, and they were basically downloading tons of information, I mean, gigabytes' worth, and handing them off to this little Chinese guy named Henry Nee (?) And, it didn't seem right, and, he was hacking things

I wrote a program for DOT that allowed contractors to send information into DOT, and he was kind of the quality assurance guy for software. He put a wiretapping module into the program that went out to the contractors so that it actually sent everything they sent, back to Yang. So I reported all this, and just last March I think, he was arrested for attempting to send anti-tank missile chips to the capital of Communist China.

If that's correct, this is like a small thing...

Of course I think he only got a hundred dollar fine.

[Audience: HmMMM! HmMMM!]

And no time.

[Audience: Oh God!]

[Madam Chair:] Thank you. Congresswoman Stephanie Tubbs-Jones....

[Audience: long, hearty applause]

We are now going to um go back to the public testimony and...

[End]

Exhibit P

Affidavit of Clint Curtis 4 pages

AFFIDAVIT



1. I, Clint Curtis, swear that the following is true and correct.
2. I was born in Illinois and I am 46 years old. I graduated from college at Illinois State University with a degree in political science history and later started my own company and learned to write computer software programs.
3. In the mid 1990s, I moved to Florida and later got a job with Yang Enterprises (YEI) in Oviedo, Florida in August 1998 as a computer programmer. I became the lead programmer for YEI and had daily meetings with YEI CEO Mrs. Li Woan Yang. At the time, I was a life long registered Republican.
4. In the early fall of 2000, a man came into YEI and was introduced to me as Tom Feeney, future Speaker of the House of Representatives in Florida as well as YEI's corporate counsel and lobbyist.
5. I sat in meetings with Mr. Feeney on at least a dozen occasions over the next several months and we discussed several potential projects to determine their viability. In short, I was the technology adviser to Mr. Feeney on these proposals. After these consultations, Mr. Feeney would advise YEI on how best to procure the contracts for these projects.

6. During a meeting in late September or October of 2000 at YEI, there were four people present including myself, Tom Feeney, Mike Cohen, Mrs. Yang, and to the best of my recollection, two other YEI employees came in and out of the room during the course of the meeting. Mr. Feeney said that he wanted to know if YEI could develop a prototype of a voting program that could alter the vote tabulation in an election and be undetectable. He was very specific in the design and specifications required for this program. He detailed, in his own words, that; (a) the program needed to be touch-screen capable, (b) the user should be able to trigger the program without any additional equipment, (c) the programming to accomplish this remain hidden even if the source code was inspected.

I told him that it would be virtually impossible to hide such code written to change the voting results if anyone were able to review the uncompiled source code. However, if the code were compiled before anyone was allowed to review it then many vote fraud would remain invisible to detection. After further discussion, Mrs. Yang told Mr. Feeney that we would attempt to build a prototype for this program so he could see it, test it, and show it to others. It was my initial belief that Mr. Feeney was interested in such a program because of a concern that Democrats would try to use such a program to steal an election, and he wanted to be able to detect and prevent that if it occurred.

7. Shortly thereafter, as directed, I created the vote fraud software prototype by making a software program where each candidate is represented as an element of



an array of controls. Each candidate is listed in a database, and their number corresponds to where you want them to show up in that array. When the program starts, it reads the database, and takes the number assigned to the candidate and fills in the label with the index that matches that number. That allows the program to work dynamically. It doesn't matter who the candidate is as they have been equated to the index number assigned. From a normal perspective it allows the voter to select the candidate, click on the submit button and the candidate's selected previous vote total is then increased by one.

In the vote fraud prototype that I created things were not what they seemed. Hidden on the screen were invisible buttons. A person with knowledge of the locations of those invisible buttons could then use them to alter the votes of any candidate listed. By clicking the correct order of invisible buttons the candidate selected by the user is compared to other candidates within that same race. If the candidate they selected is leading the race, nothing happens. If the other candidate is leading the race, the vote totals are altered so that the selected candidate is now leading the race with 51% of the vote. The other candidates then share the remaining 49% in exact proportion to the totals they had previously. In the prototype supplied to Feeney, the vote totals showed on the screen. In an actual application, the user would receive no visible clues to the fraud that had just occurred. Since the vote is applied by race, any single race or multiple races can be altered. The supervisors or any other voter would never notice this fraud since no visible sign would appear. Additionally, the procedure could be repeated as many times as was necessary to achieve the desired results. No amount of testing or simulations would expose the fraud as its activation and process is completely invisible to everyone except the person programming the vote fraud routine.

The same procedure could be automated to activate without any user intervention whenever the machine detects a certain pattern of voting. The algorithm could also be altered from hidden keys or triggers that would allow the fraudulent user to manipulate both the margins and percentages of any particular race. In most national elections it is not necessary to win every area.

8: Once I had the software program done, I wrote a report on how a person could see voting manipulation simply by looking at the source code. Any manipulation of the vote and the procedures for flipping the vote would be obvious to a competent programmer. I provided the program to Mr. Hai Lin Nee, the Quality Control person at YEI, and discussed it with him. He approved its distribution.

9: I gave the software program, which was on a CD disc, and the report that was on disc and on paper, to Mrs. Yang. I stressed that she and Mr. Feeney could view the operation of the program and then see how to detect such fraudulent source code so it could be prevented. Conversely, if they allowed blind (already compiled) code to be used (no source code provided) and there were no paper receipts, the votes could be flipped from one candidate to the other without any possible way for the deception to be detected. I explained that this could be done with a touch



screen machine or automatically. She immediately stated, "You don't understand, in order to get the contract we have to hide the manipulation in the source code. This program is needed to control the vote in South Florida." I was shocked that they were actually trying to steal the election and told her that neither I nor anyone else could produce any such program. She stated that she would hand in what I had produced to Feeney and left the room with the software.

10. In my role as a technology advisor at YEI, I was present at subsequent meetings between Mr. Feeney and Mrs. Yang. In several of those meetings, prior to the 2000 election, it became clear to me that Mr. Feeney was well aware that by artificially reducing the margin of victory of the opposition party in areas where they were the strongest, the overall outcome would then favor his candidate. As well, he bragged that he had already implemented "exclusion lists" to reduce the "black vote". He further mentioned that the "proper placement of police patrols could further reduce the black vote by as much as 25%." I didn't know at the time, if Mr. Feeney had meant that as a racial joke or actually part of the plan.
11. Soon thereafter, I resigned from YEI and took another job at the Florida Department of Transportation (FDOT). While there, I discovered some other illegal activities of YEI, who had contracts with FDOT, involving over-billing and defrauding of the State of Florida regarding contracts that I had worked on at YEI. I reported this information to the FDOT Inspector General's office and they began harassing me and another employee, Mavis Georgalis, who had made similar reports and eventually we were both fired by FDOT on the same day. We later filed whistleblower complaints against FDOT. Mrs. Georgalis was successful but mine was filed after the deadline and was dismissed.
12. The IG at the FDOT, Raymond Lemme, pursued some of the allegations I made against YEI, as I had advised him of the information concerning Tom Feeney and the vote-fraud issue, illegal aliens employed by YEI, fallacious over-billing, and a wiretapping module that was placed into a FDOT software program for the document management system. Mr. Lemme continued to meet and talk with me about matters relating to the case after I was fired from FDOT, and in June of 2003, he told me that he had tracked the corruption "all the way to the top," and that the story would break in the next few weeks and I would be satisfied with the results. A few weeks later, on July 1st, Mr. Lemme was found dead with his arm slashed in a hotel room in Valdosta, Georgia.
13. Hai-Lin Nee, the Quality Control manager at YEI, also worked with a company called Azure Systems of Orlando. While at YEI, Mrs. Yang provided Mr. Nee with many gigabytes of downloaded information from NASA projects that YEI was working on, including the Maximo facilities repair maintenance database, which he then took from the premises of YEI. This happened on several occasions. Also, I saw Mrs. Yang send a great deal of internal information to her brother in China, who, she had informed me, had been deported for spying. Wayne Leaders, an investigator for NASA, later confirmed this deportation of Mrs. Yang's brother.



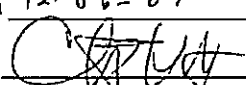
Mr. Leaders was responding to one of my multiple attempts to contact NASA on the YEI matter. I had also made a report to Mr. Leaders regarding a program that I had written for FDOT that allowed for outside contractors to submit documents to FDOT. Between the time I wrote the program and the phase of Mr. Nee's quality assurance, I discovered that Mr. Nee had inserted a wiretapping module into the software that copied all the information bound to FDOT and sent it via the Internet to YEI. I have reason to believe that he also did this with a similar program I had written for NASA.

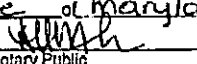
14. In late 2003 or early 2004, I provided information to Detective Rob Pace at the Leon County Terrorist Task Force concerning Hai Lin Nee who I had learned was an illegal Chinese alien. I informed Detective Pace that Mr. Nee was working at YEI on NASA programs. Hai Lin Nee was subsequently arrested by federal officials in Orlando, Florida on or about March 17, 2004 on charges that included sending radar guidance system chips for Hellfire Anti-Tank Missiles to a company in Communist China.

15. I reported much of this information to the FBI, CIA, Homeland Security and Florida Department of Law Enforcement through emails but the only one to respond was Tom Yowell, a Special Agent with the Florida Department of Law Enforcement assigned to the FBI Joint Terrorism Task Force. Mr. Yowell responded via email on November 22, 2004, that YEI was under investigation by another office of the FBI and that if I supplied him with my telephone number and name, he would pass that information to the other office so that they could contact me. I did, but I have not yet heard back from the FBI or Mr. Yowell as of today's date. I have filed a QUITAM, which is still pending, with the State of Florida concerning the over-billing by YEI.

I have never been charged or convicted of any crime although I have been involved with two civil matters. The first is a copyright infringement case dating from 1997. The case was ultimately settled out of court with no finding of wrongdoing by anyone, and with both parties agreeing to pay their own attorneys' fees. The second being a suit that YEI has brought against Mavis Georgalis and me in retaliation for reporting on its illegal activity. The YEI civil suit is still pending and the court eventually required that FDOT to be included as a co-defendant as well because it was the sole owner of the software that Ms. Georgalis and I were falsely accused of having appropriated. YEI employees have so far refused to subject themselves to depositions in that pending case.

I declare under penalty of perjury, pursuant to 28 USC § 1746, that the above is true and correct.

Executed on 12-06-04
Clinton
Clint Curtis 

Subscribed and sworn to before me, in my presence, this
6th day of December, 2004, a Notary Public
in and for the State of Maryland.

Notary Public
My commission expires February 12, 2007