MESA COUNTY
CLERK & RECORDER

Board of County Commissioners

SEP 17 2021

CONFIDENTIAL LEGAL DOCUMENTS
EXEMPT FROM COLORADO OPEN RECORDS ACT

Hon. Janet Rowland, Chair, Board of County Commissioners
Scott McInnis, County Commissioner
Cody Davis, County Commissioner
544 Rood Avenue
Grand Junction, CO 81501

RE: Forensic Report No. 1 on EMS Server Images

Dear Commissioners:

Enclosed is the first report from the cybersecurity experts who have analyzed thoroughly the two 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 election. Because the report documents a substantial amount of data destruction during the May 25 "Trusted Build" conducted by the Secretary of State's office and the vendor, I wanted to get this in your hands immediately.

I just received this report today. From my review of the executive summary, it does appear that my concerns were more than justified. As you know, the legal duty to preserve election records falls solely to me and my office. "Extensive" amounts of data required to be preserved were instead destroyed, and done in a way that was totally beyond my control or knowledge. Among other things, these deletions would preclude a forensic audit of the last election. Thanks to the pre-Trusted Build image I had commissioned in May, these data have been preserved, in full compliance with my obligations under federal and state law, preserving the integrity of our county's election record archive and permitting a forensic audit if one were conducted.

According to this report, the forensic examination has determined that this system and procedures "cannot meet the certification requirements of the State of Colorado and should not have been certified for use in the state." Obviously, this is highly relevant to any decision whether to continue to use these systems in our county. You already know of my opposition to continued use of these systems, which prevent me from discharging the duties of my office and the requirements of the law.

The experts conducting the forensic analysis are apparently issuing additional reports in the near future, and of course I will promptly deliver these to you. In the meantime, I would welcome a discussion of these findings and the proper course forward for our county to preserve the integrity of our elections.

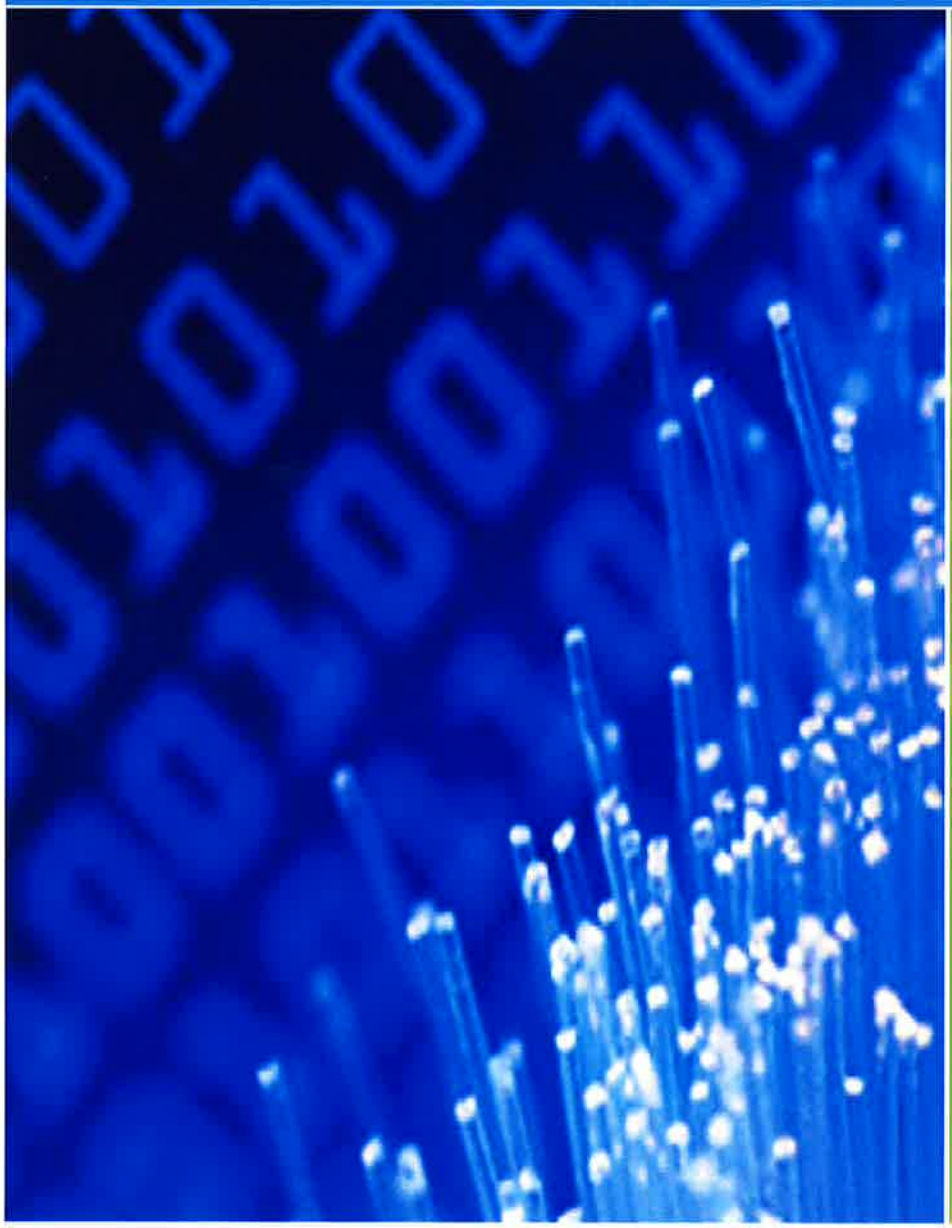
Very truly yours,

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

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

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 examination[1] 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 Electon 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 more[2].

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 cofiguration 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-CO 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

Overview of System Data Sources

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

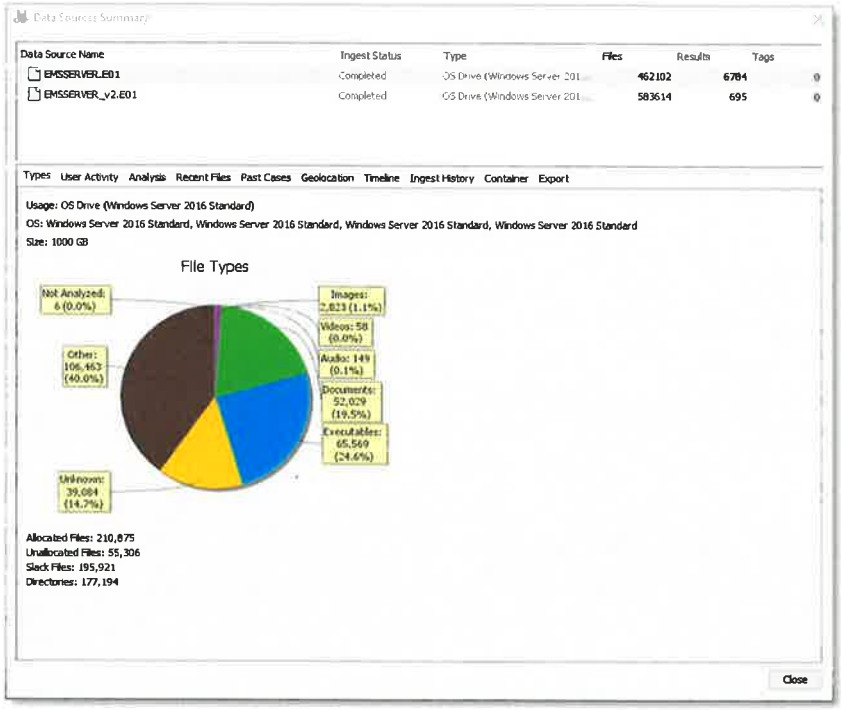
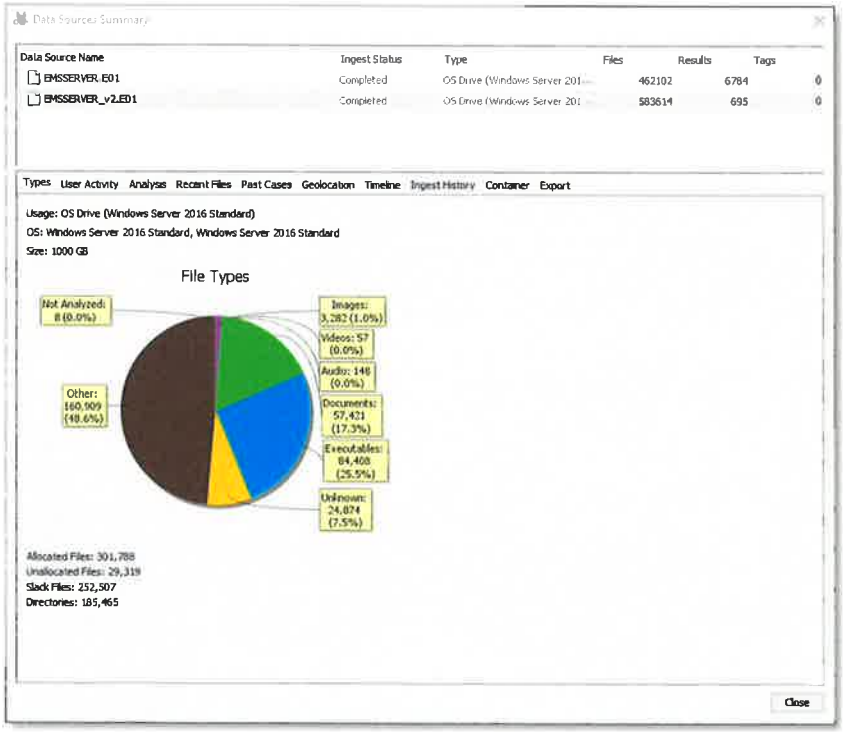


Figure 4 - EMS Server (5.13) System Data Sources After



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

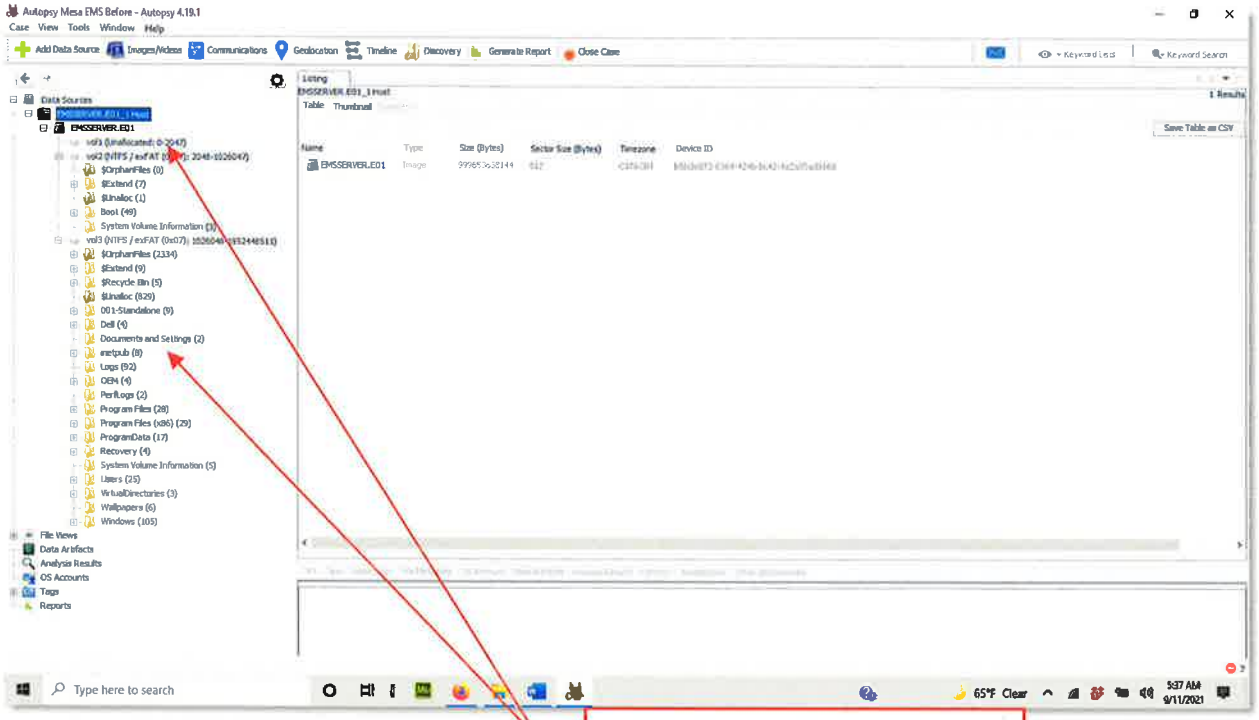


Figure 6- EMSSERVER (5.13) Disk Partition Structure After

Note Changes in Disk Volumes and Directory Structures

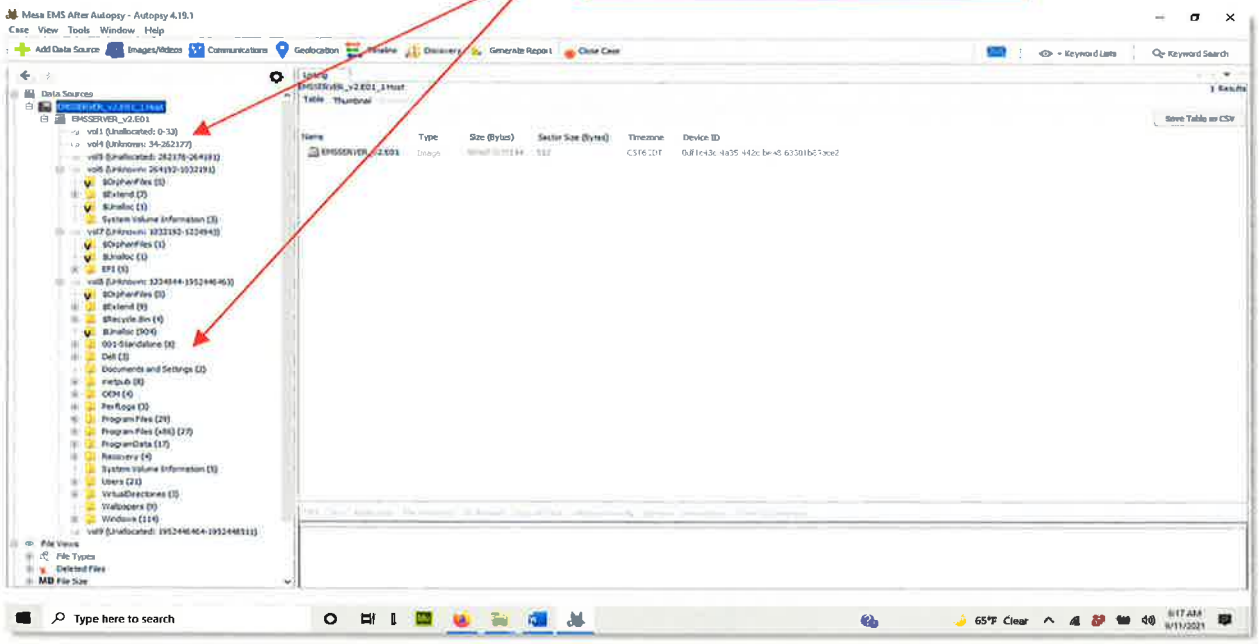
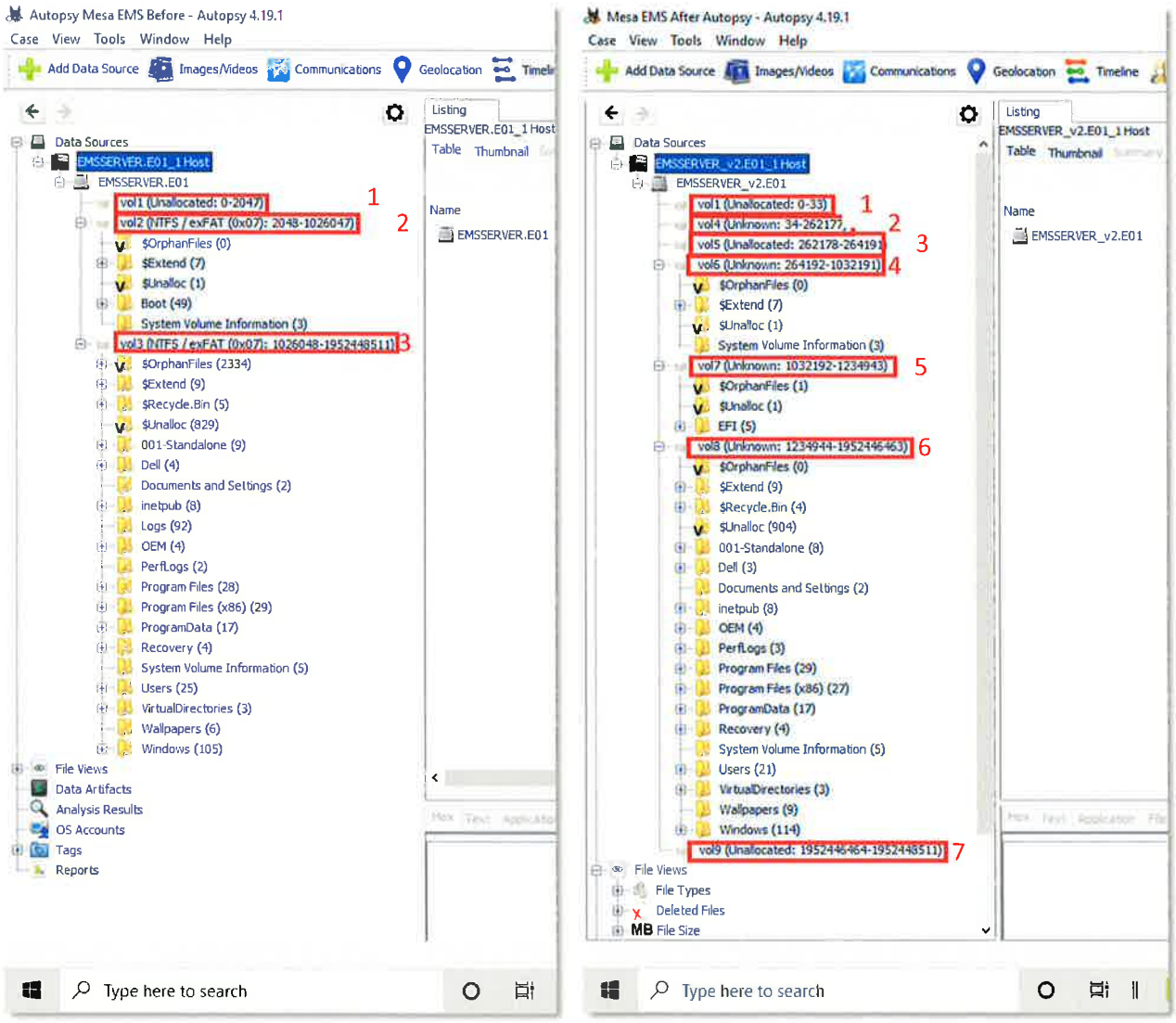


Figure 7 - Server Disk Partition and Directory Changes



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.

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

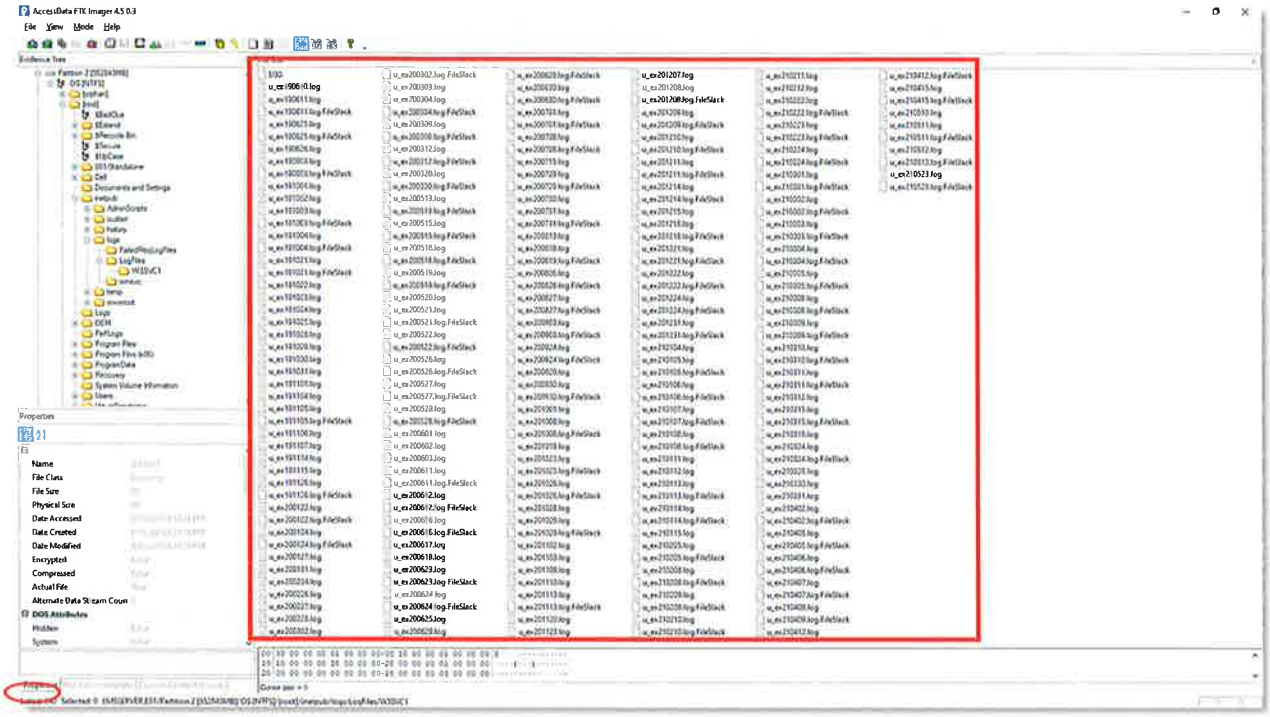
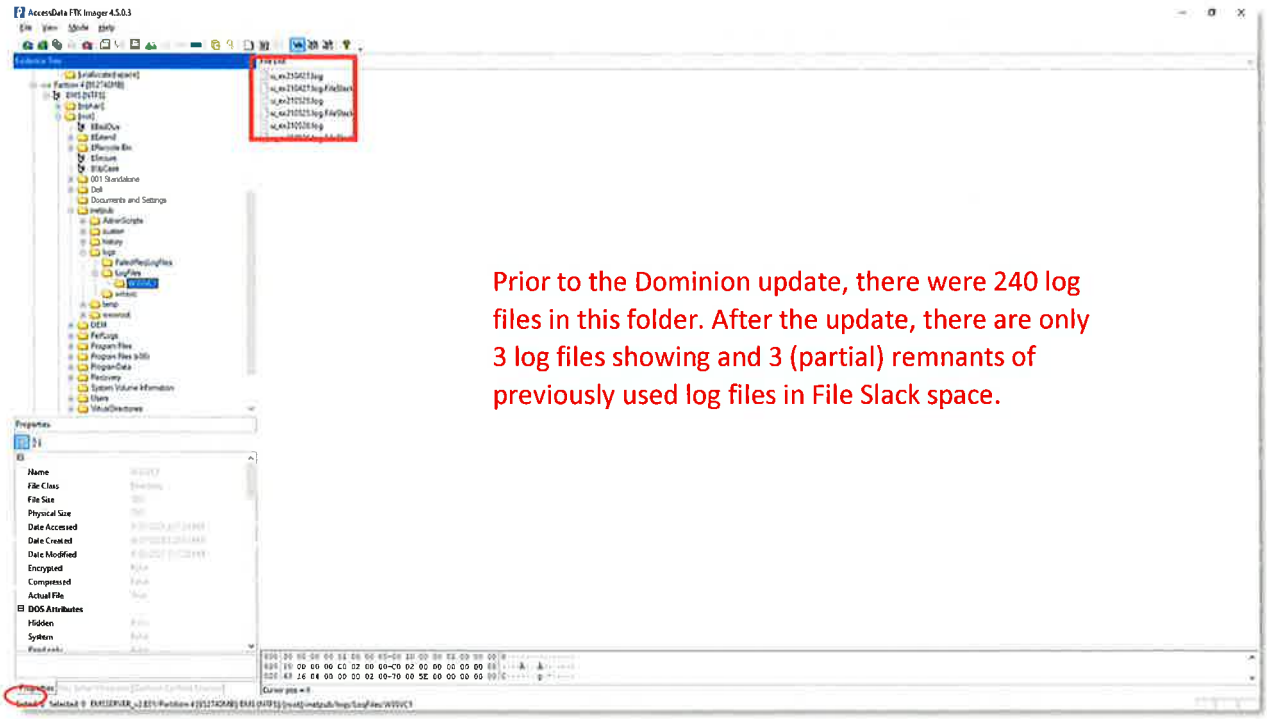


Figure 9 - EMS Server (5.13) Web Server Log Files After



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.

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

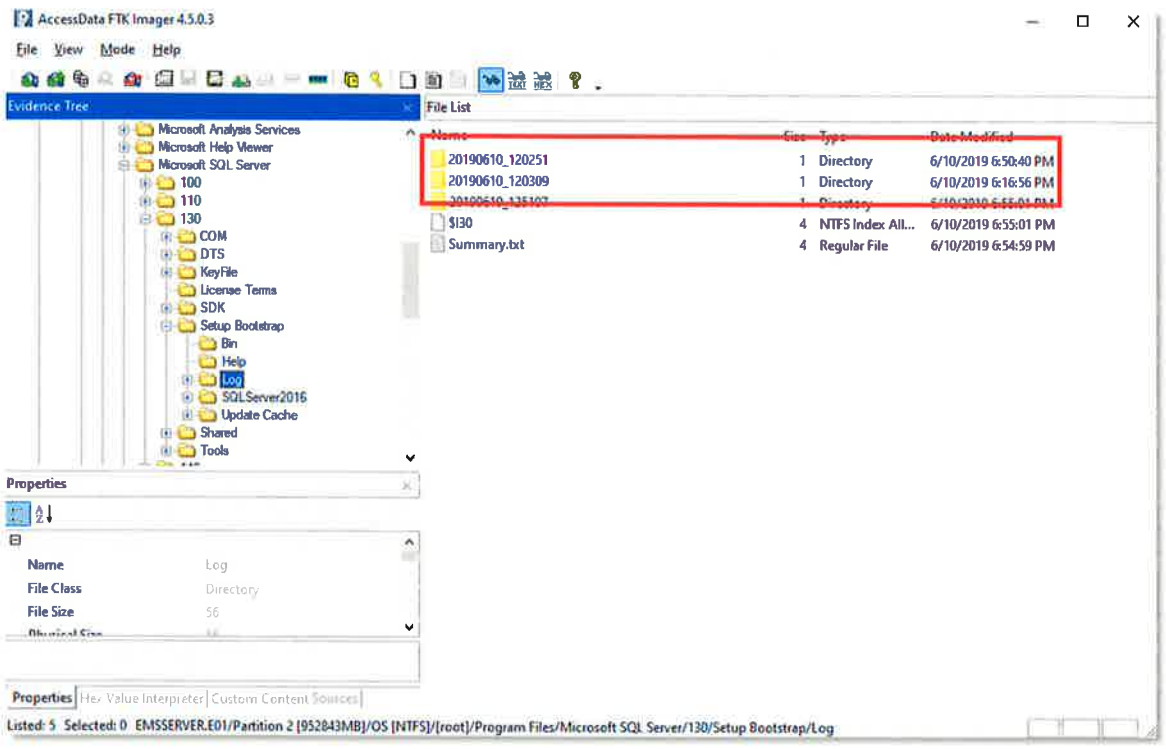
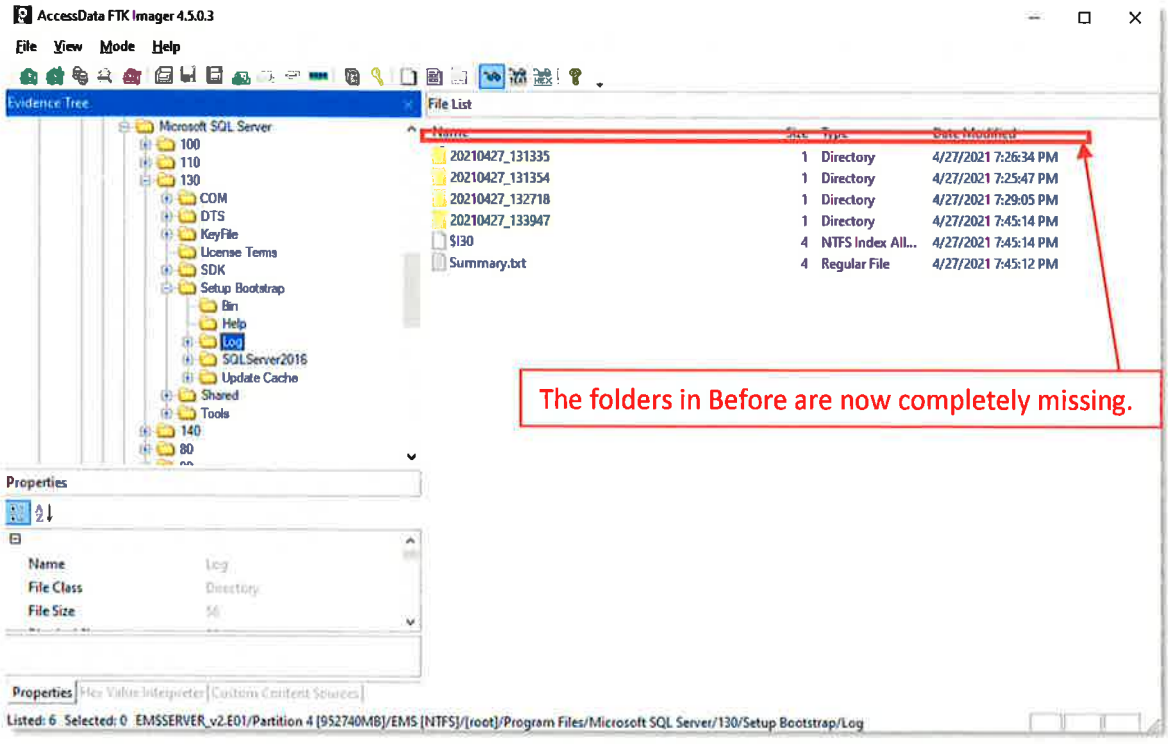


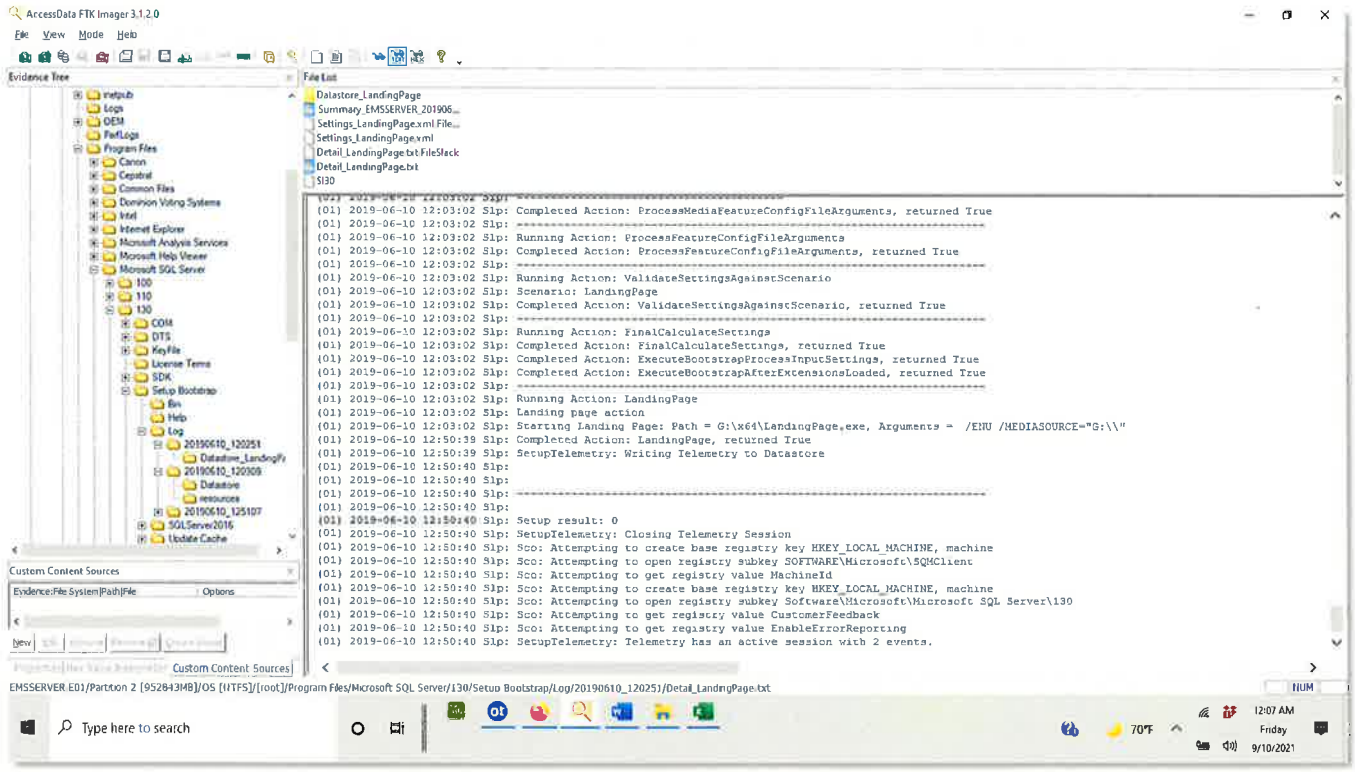
Figure 11 - EMS Server (5.13) MS SQL Server Installation Log Files After



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



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

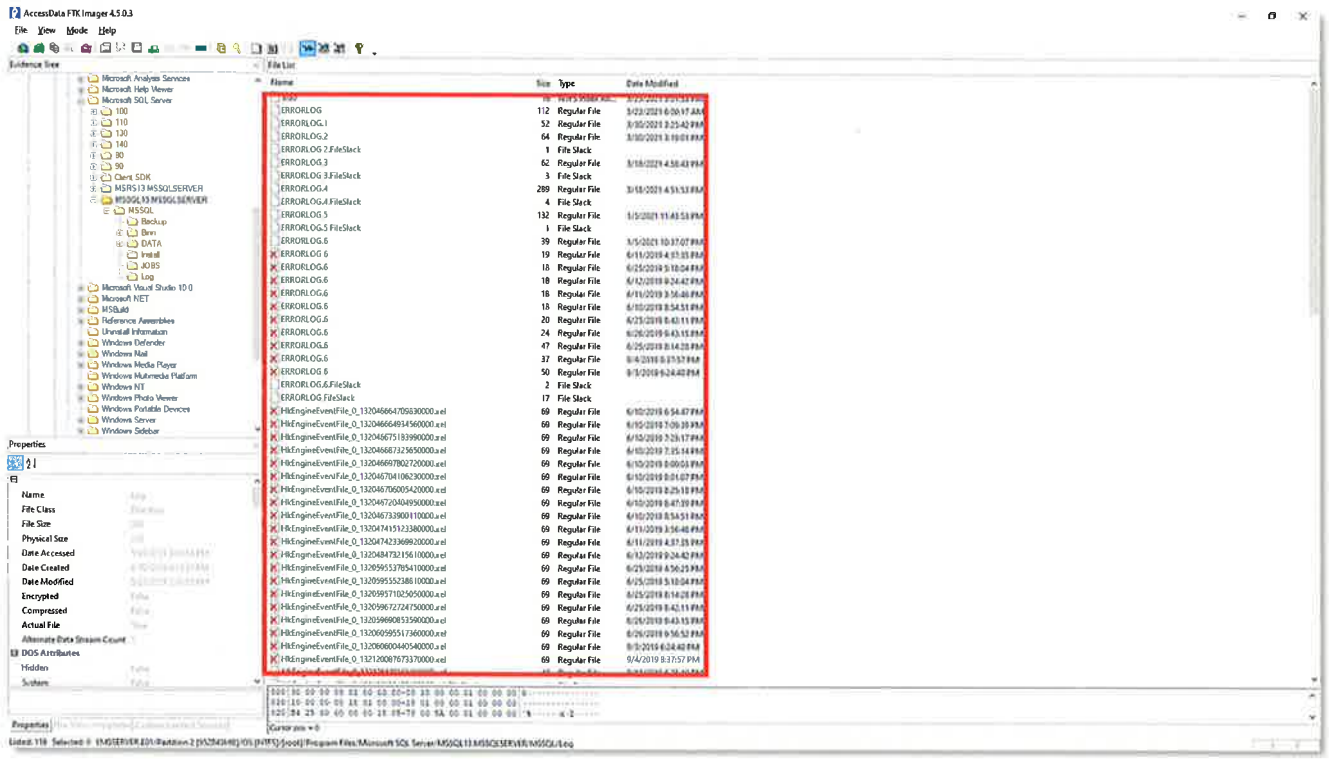
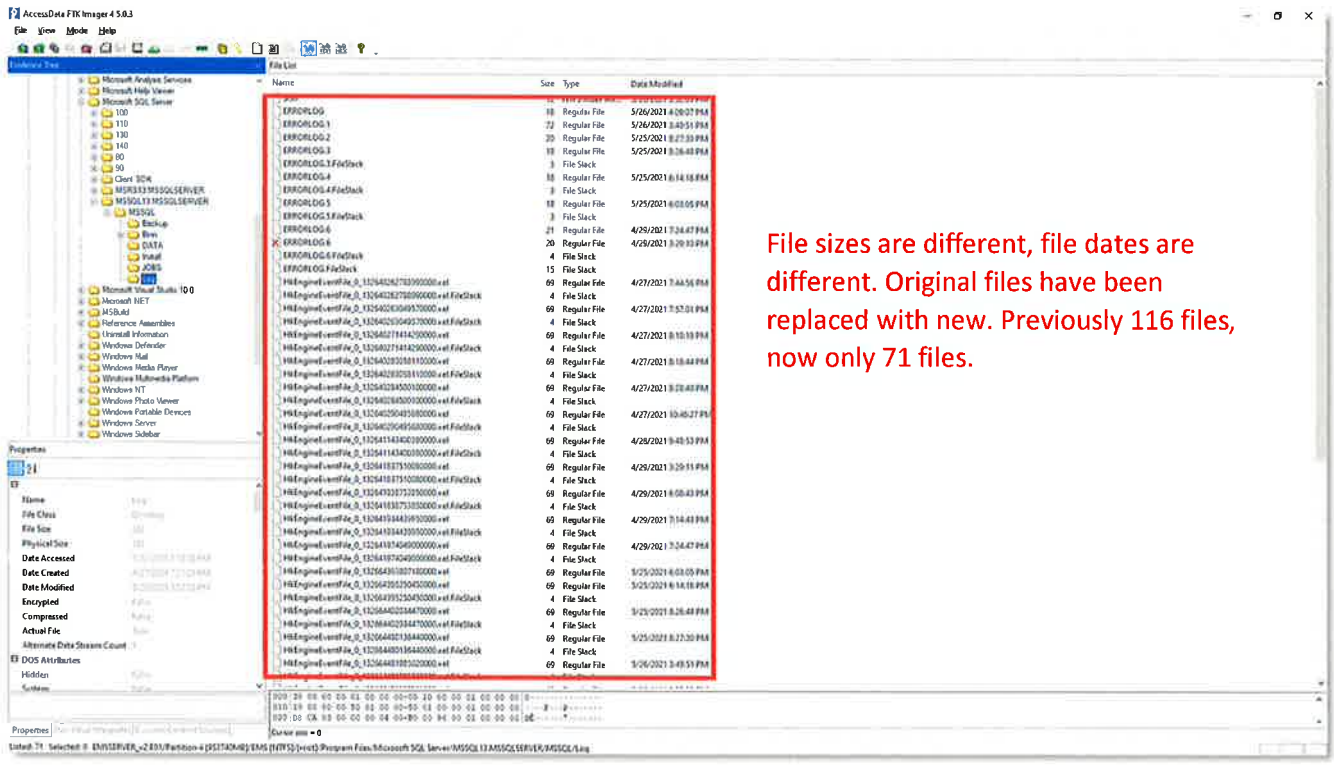


Figure 14 - EMS Server (5.13) SQL Server Log Files After



File sizes are different, file dates are different. Original files have been replaced with new. Previously 116 files, now only 71 files.

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

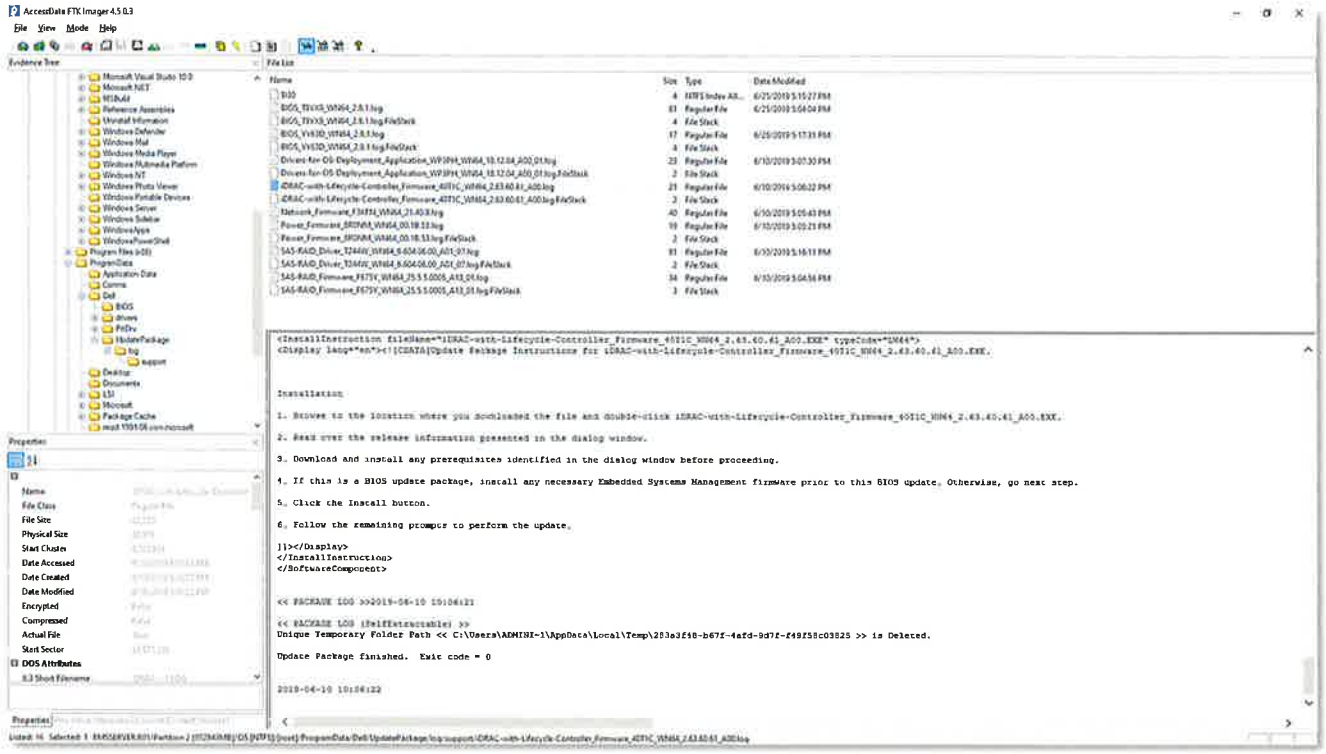
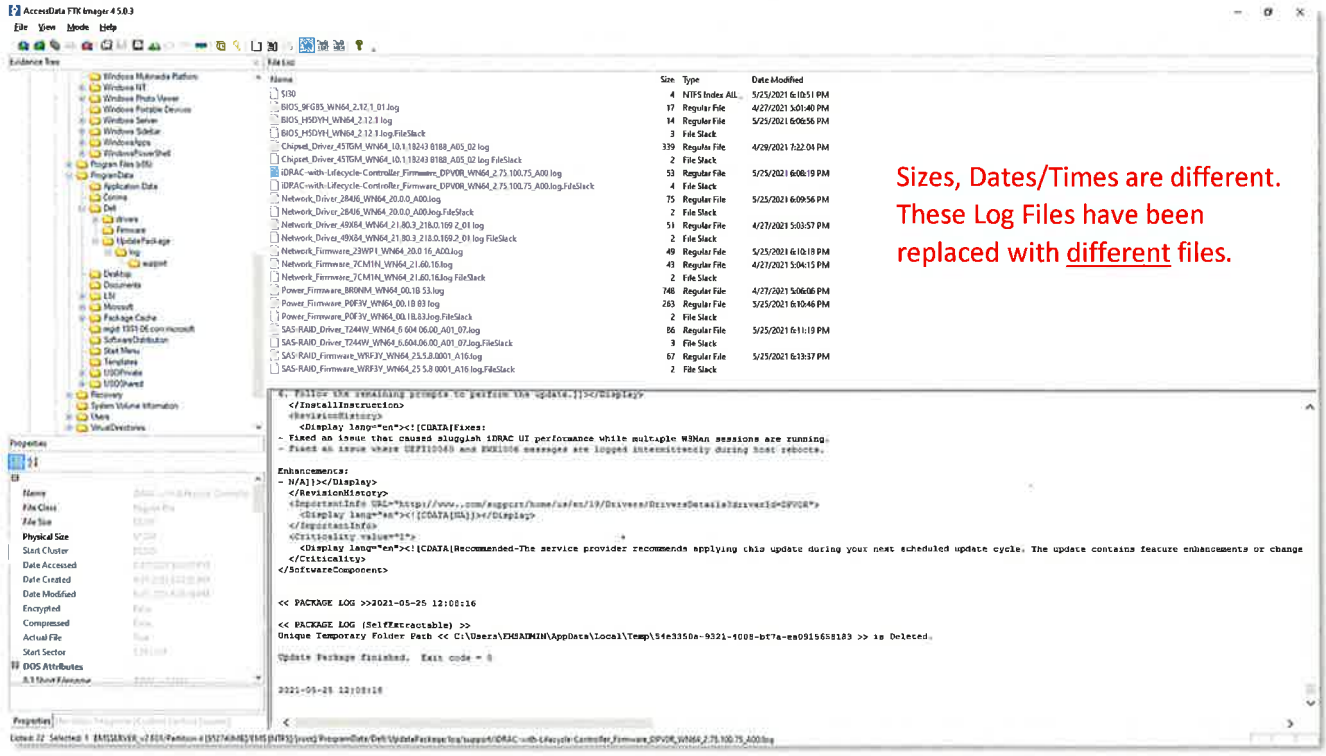


Figure 16 - EMS Server (5.13) Dell Server Update Files After



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

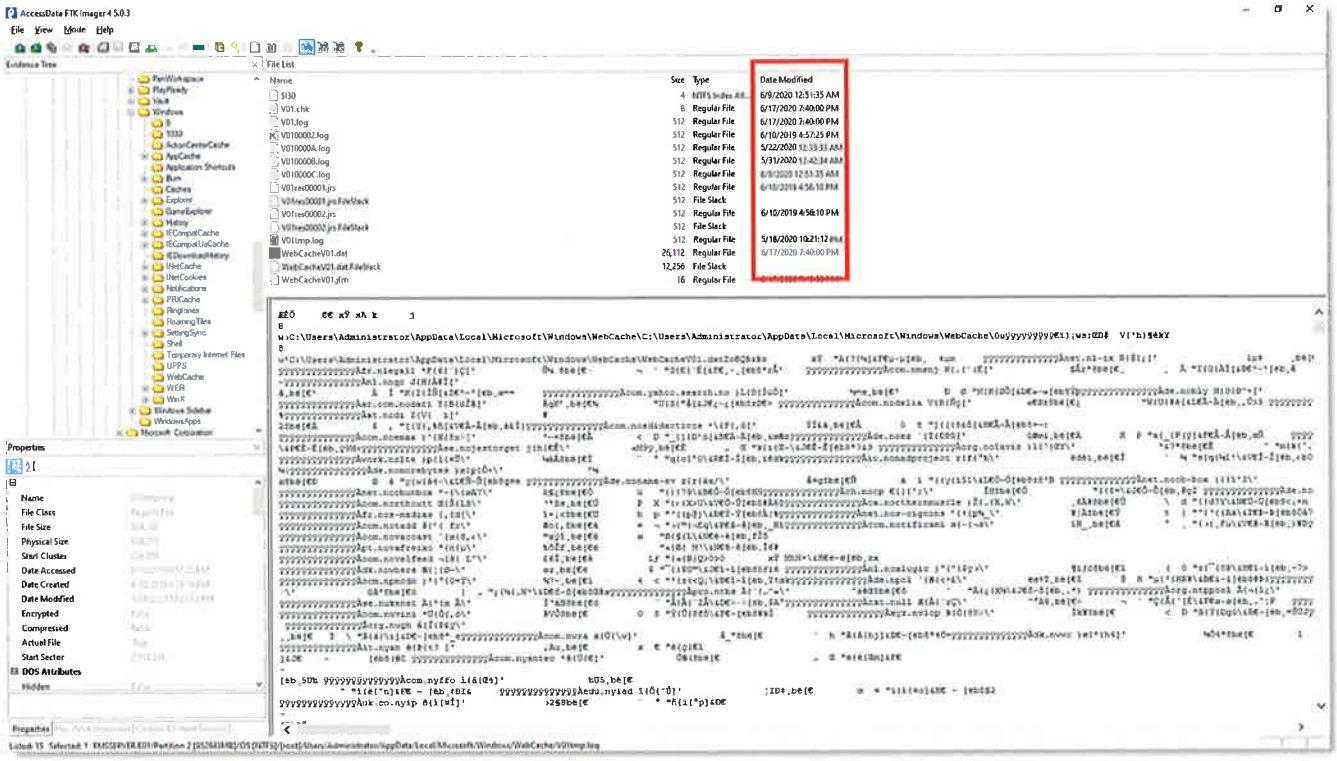
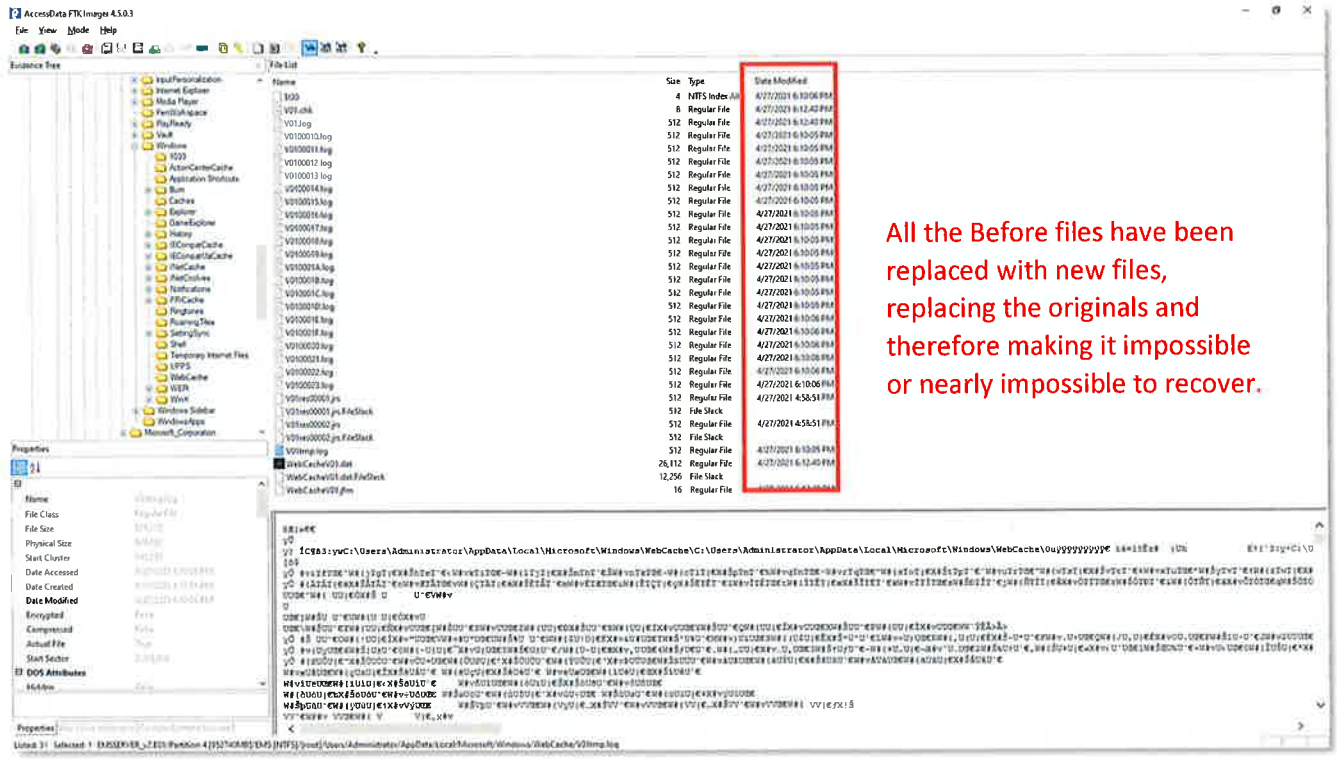


Figure 18 - EMS Server (5.13) Administrator WebCache Log Files After



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

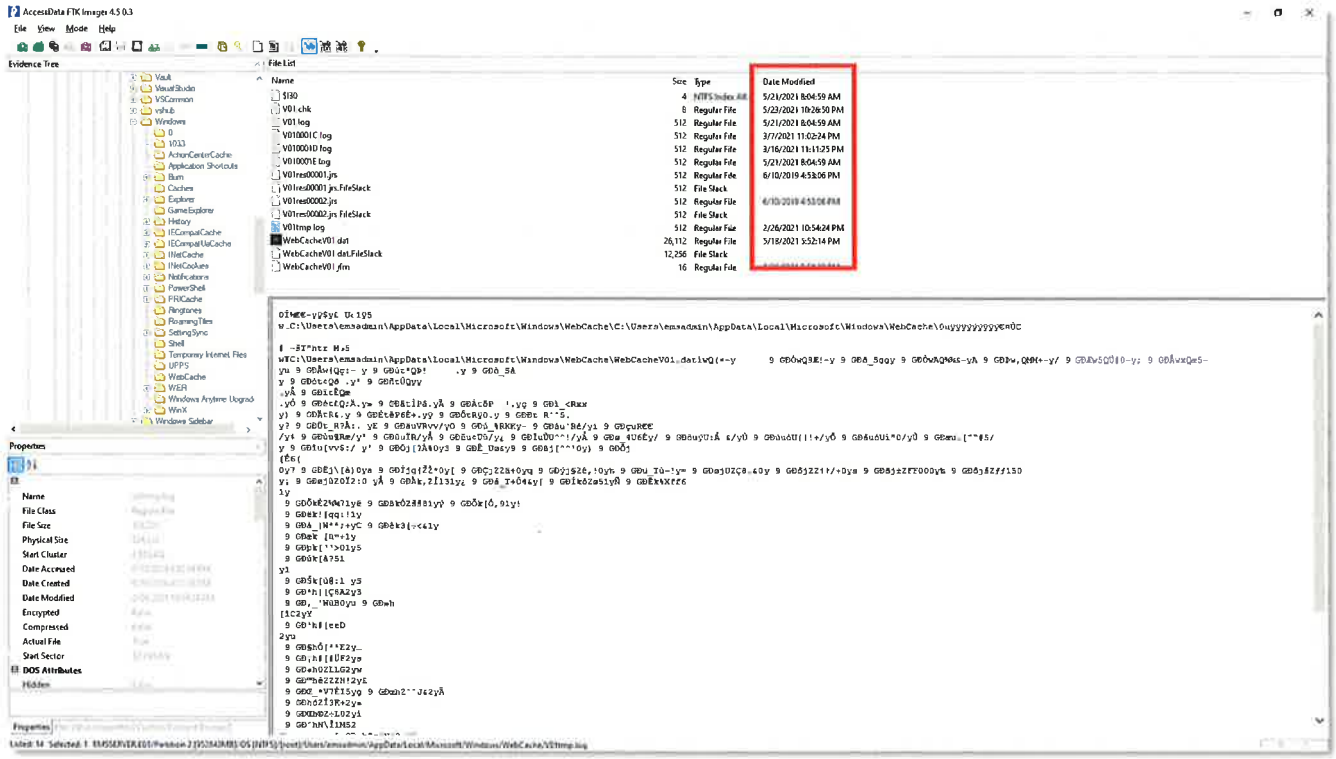
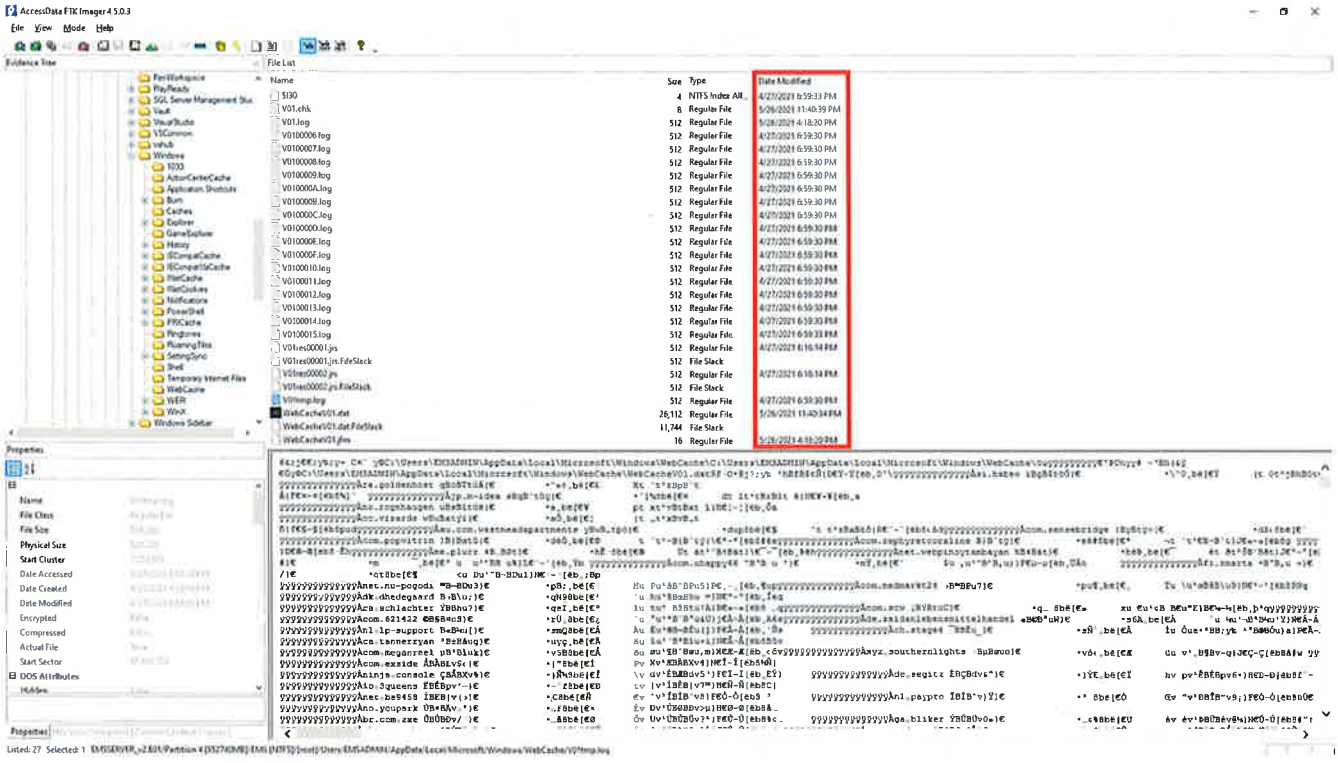


Figure 20 -EMS Server (5.13) "emsadmin" WebCache Log Files After



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

Container_15 [Table ID = 49, 25 Columns]

EntryId	ContainerId	Url	AccessedTime
1	15	:2020060820200615: DVSAdministrator@:Host: This PC	132368189382665280
2	15	:2020060820200615: DVSAdministrator@file:///C:/Users/Administrator/Desktop/DVS%20Adjudication%202%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

Container_18 [Table ID = 39, 25 Columns]

EntryId	ContainerId	Url	AccessedTime
1	18	:2021051820210519: emsadmin@file:///F:/Logs	132658341190420467
2	18	:2021051820210519: emsadmin@:Host: This PC	132658341190576330
3	18	:2021051820210519: emsadmin@file:///F:/	132658341190732829
4	18	:2021051820210519: emsadmin@file:///F:/Logs/5_18_21.evtx	132658341410603691
5	18	:2021051820210519: emsadmin@file://emsserver/nas/2020%20Mesa%20County%20General/Results/Tabulator00004/Batch2003/1_1_4_2003_DETAIL.DVD.txt	132658342689478943
6	18	:2021051820210519: emsadmin@:Host: emsserver	132658342689478943
7	18	:2021051820210519: emsadmin@file://emsserver/nas/2020%20Mesa%20County%20General/Results/Tabulator00004/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.

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

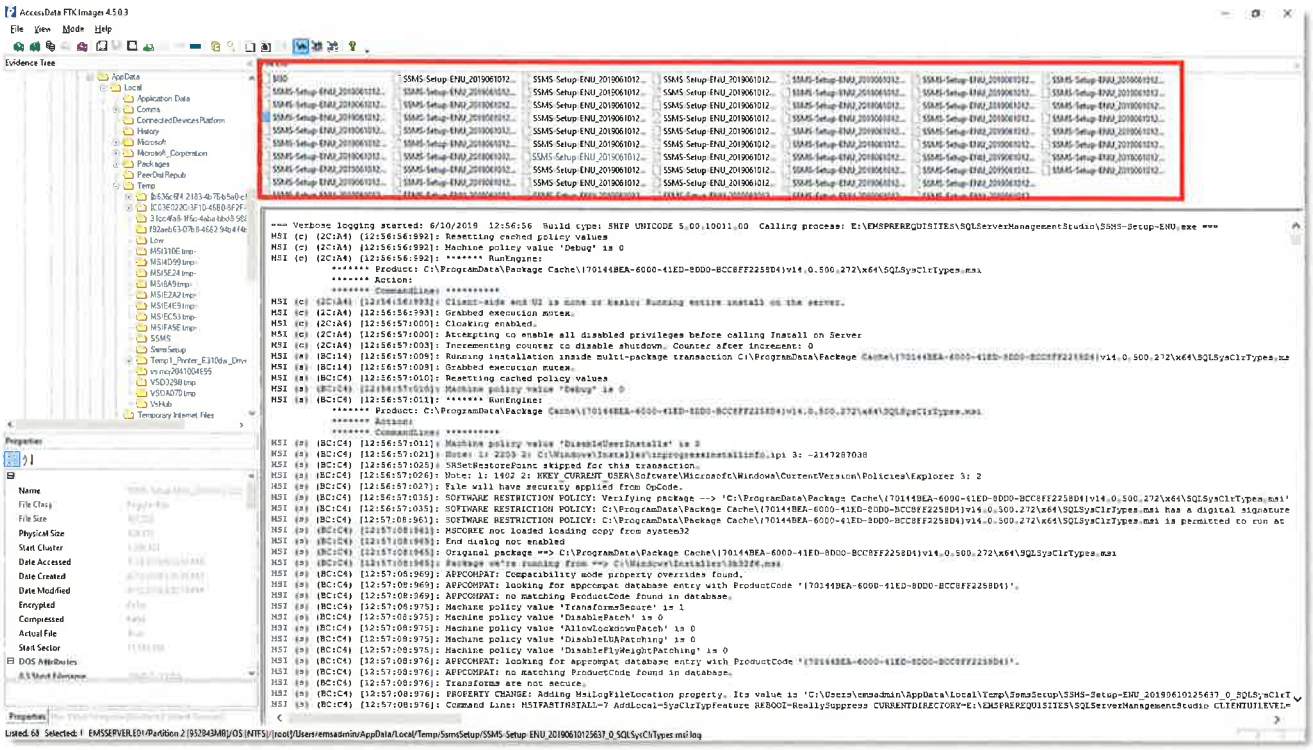
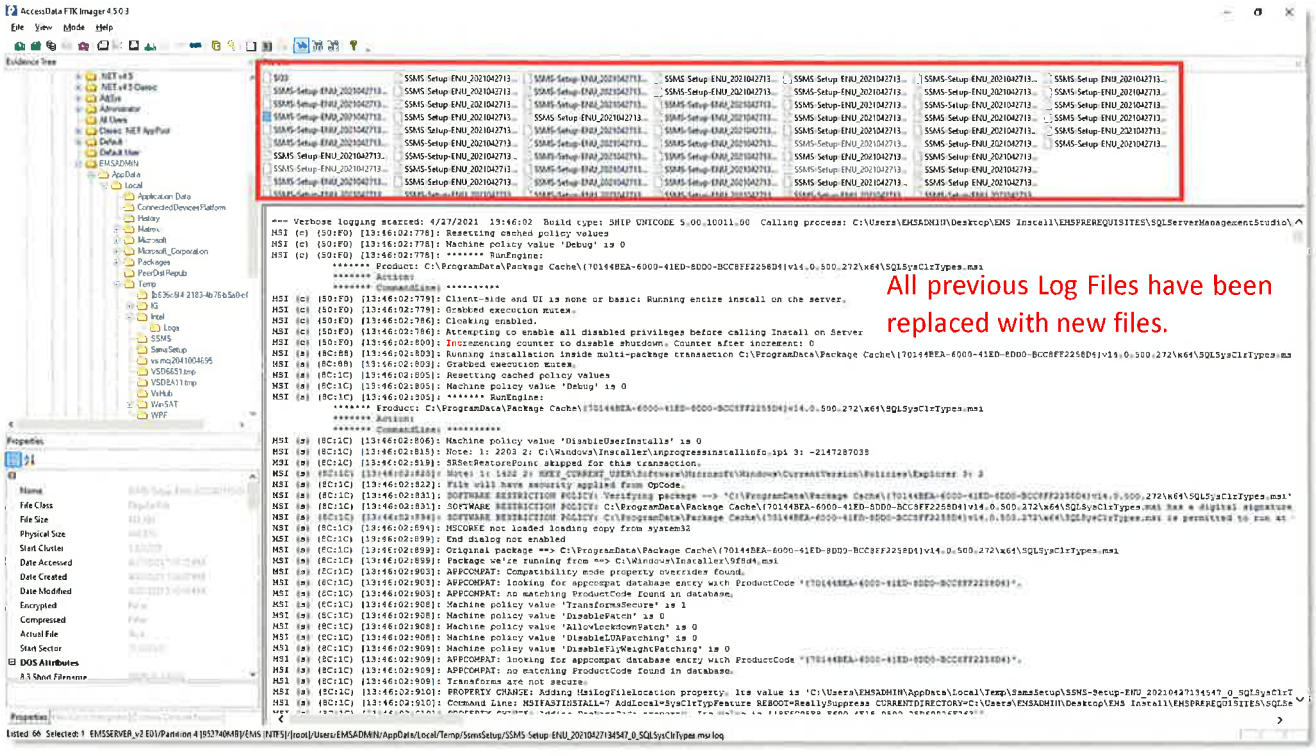


Figure 24 - EMS Server (5.13) SSMS Log Files After



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

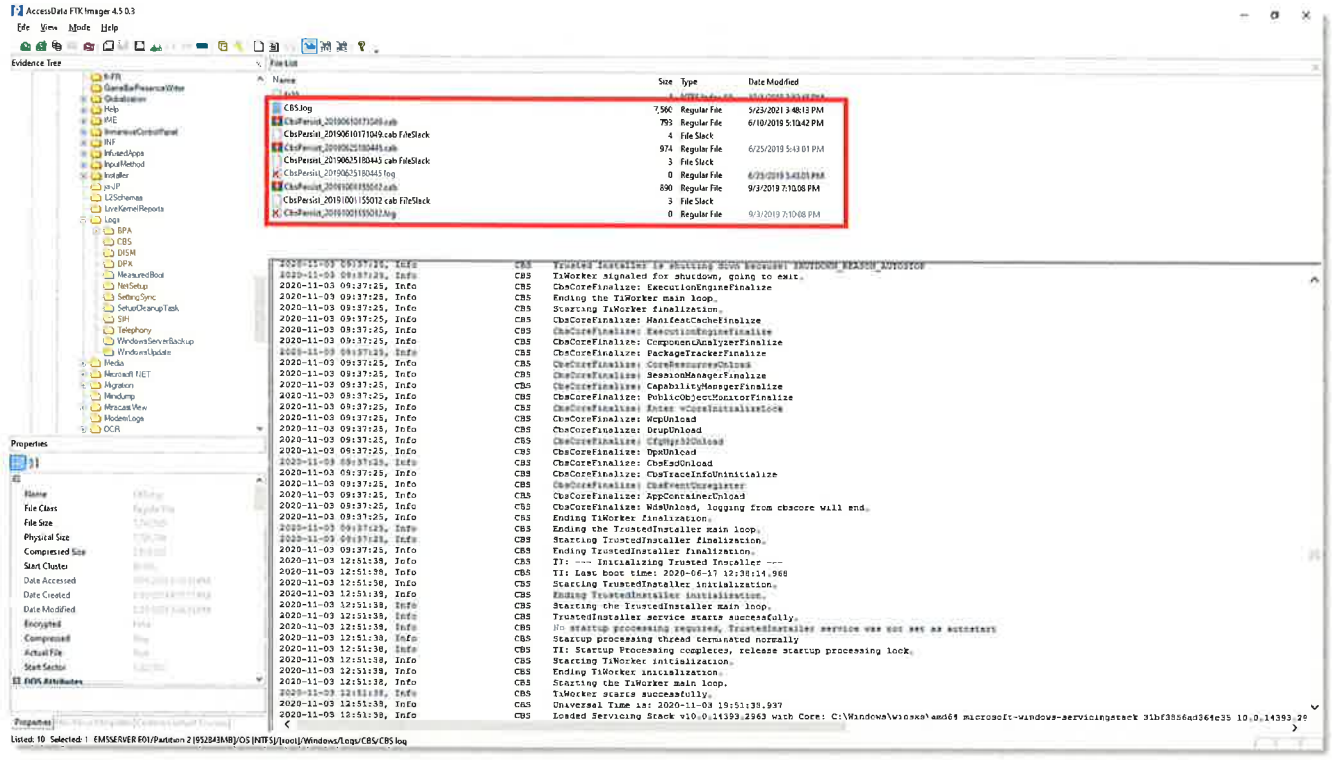
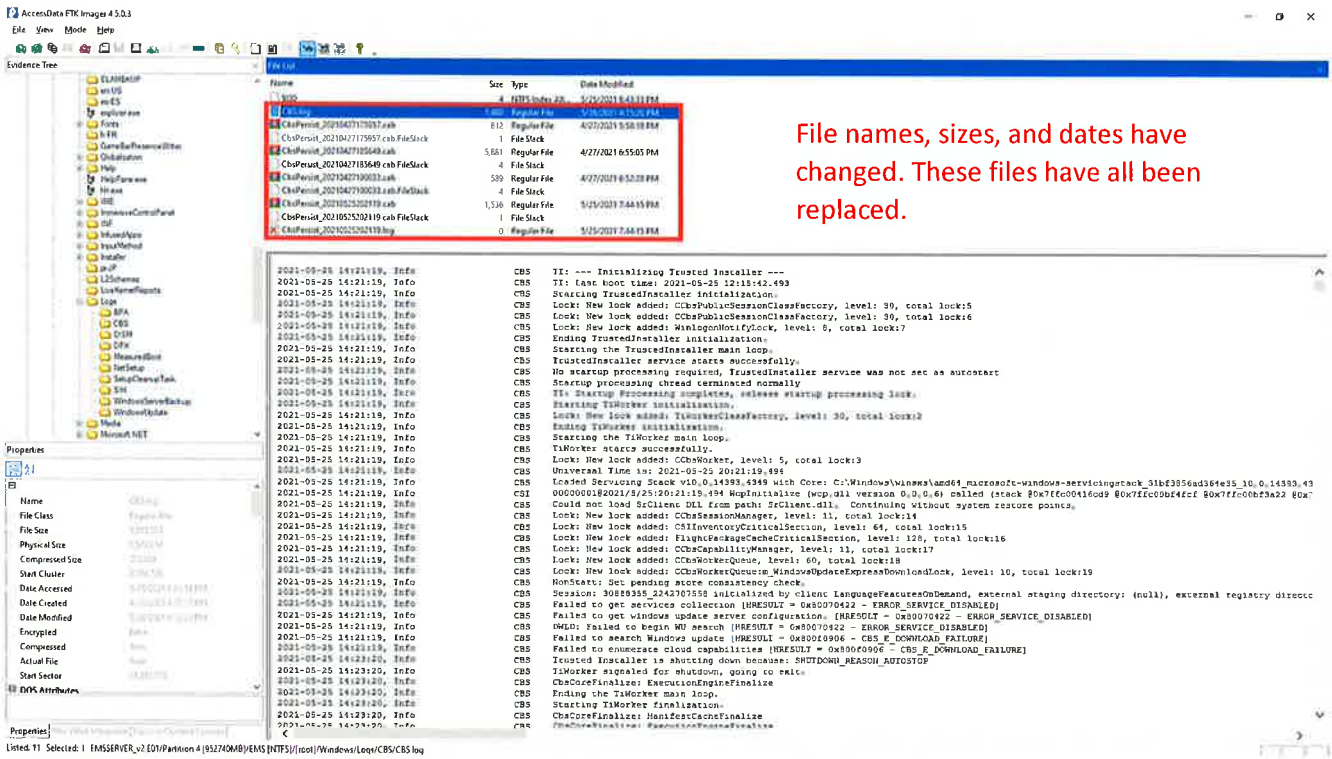


Figure 26 - EMS Server (5.13) CBS Log Files After



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

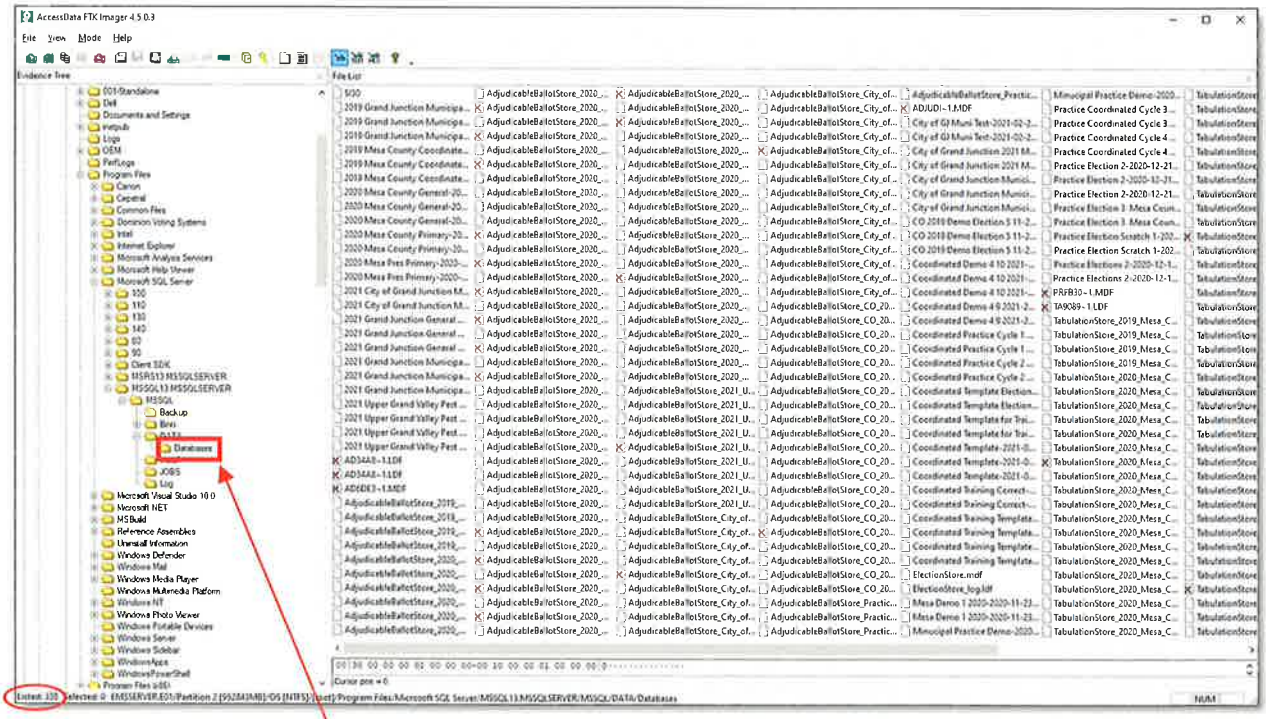
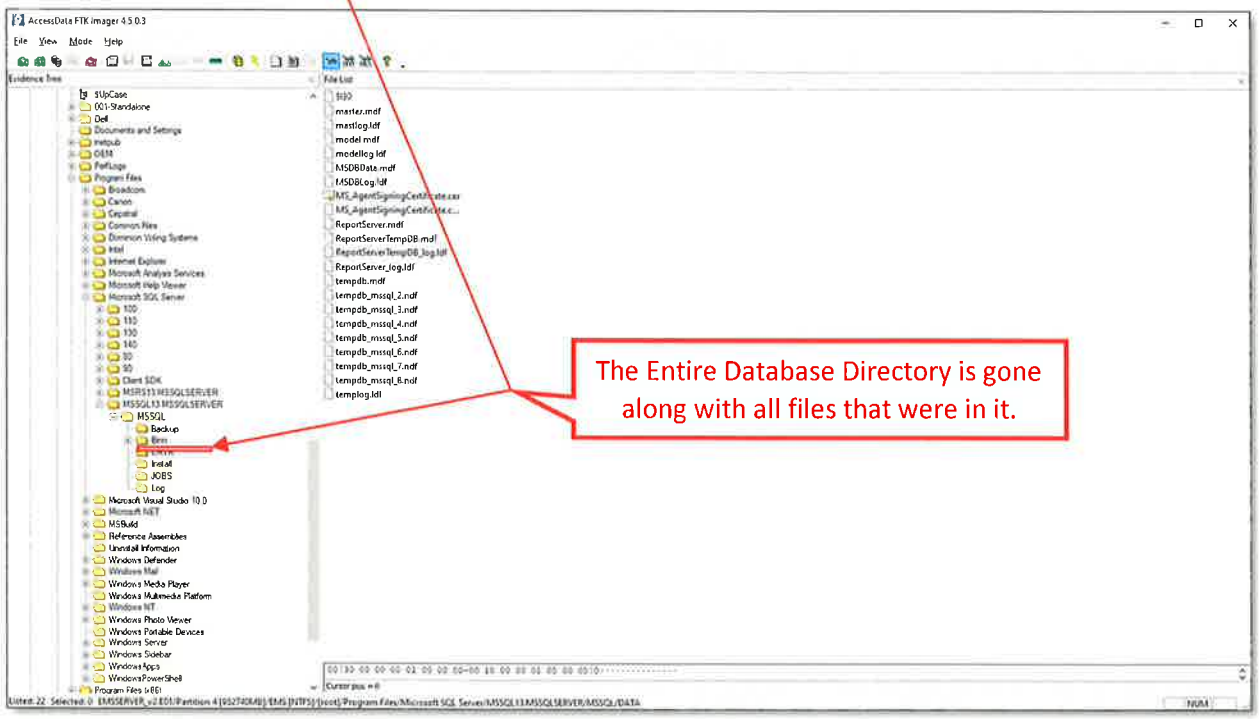


Figure 28 - EMS Server (5.13) Election Databases After



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

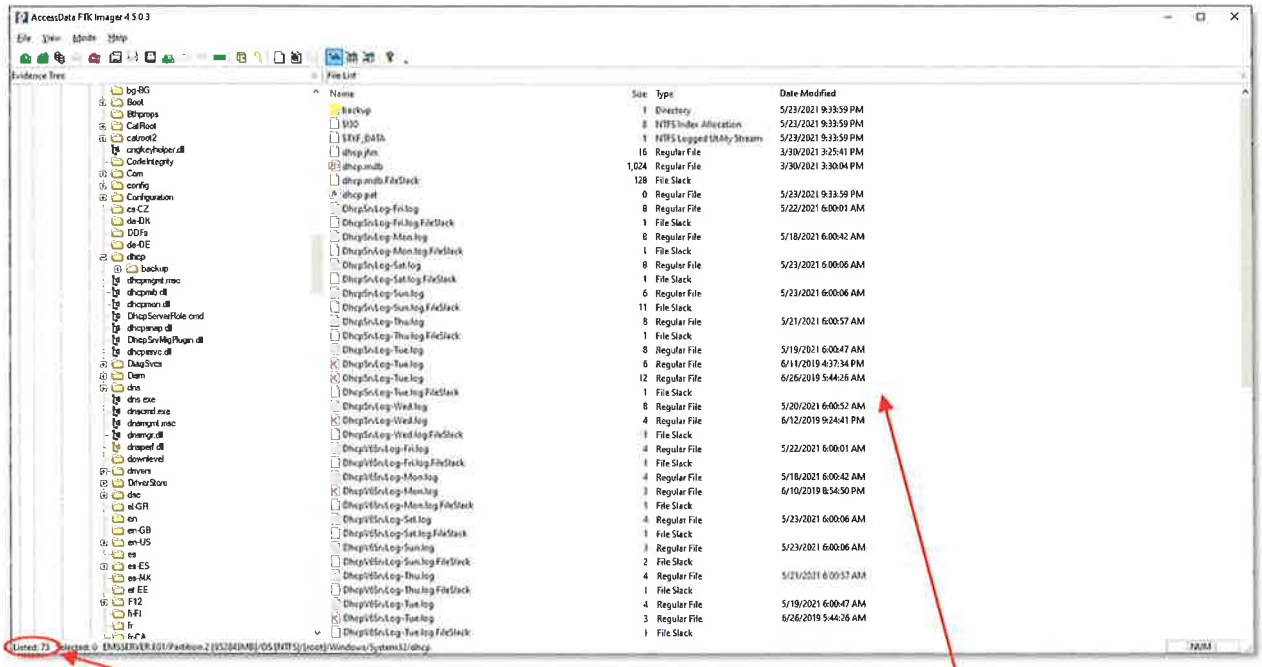
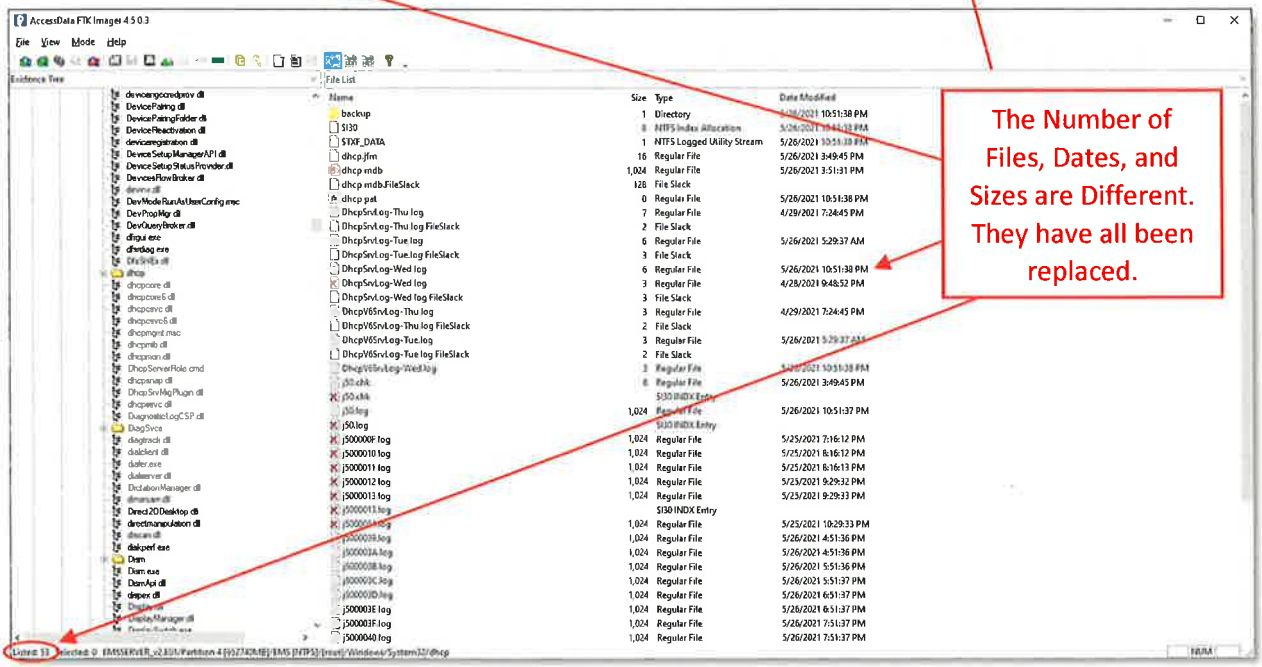


Figure 30 - EMS Server (5.13) DHCP Log Files After



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

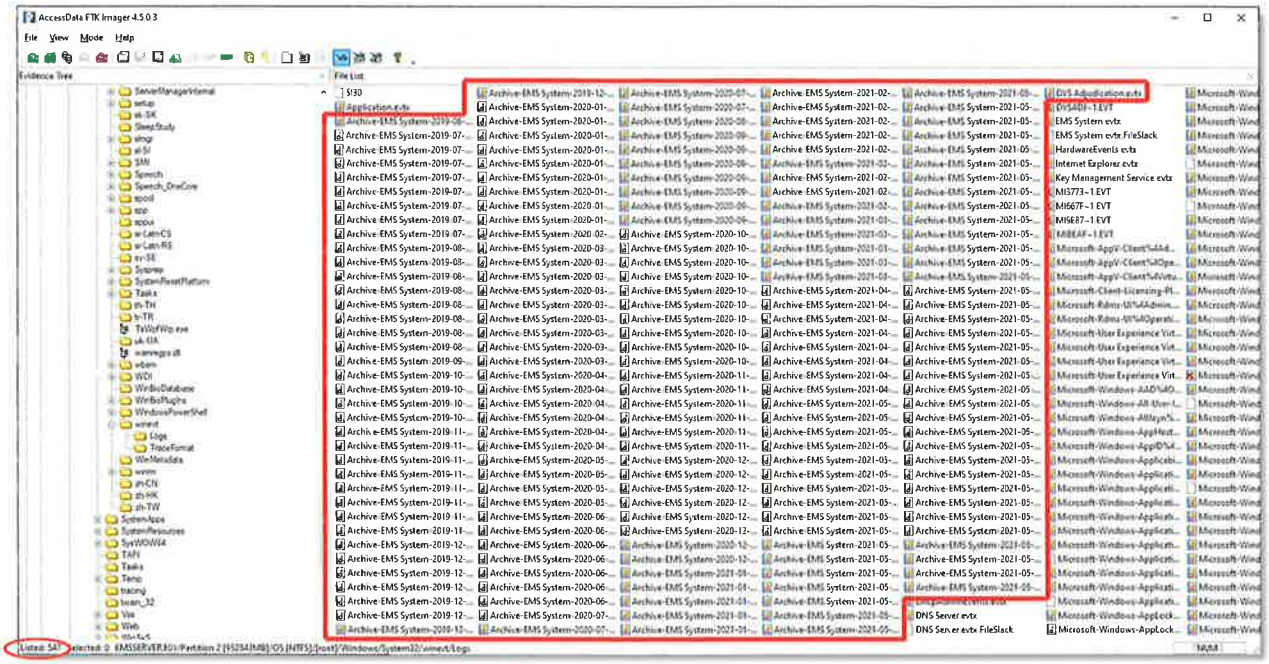
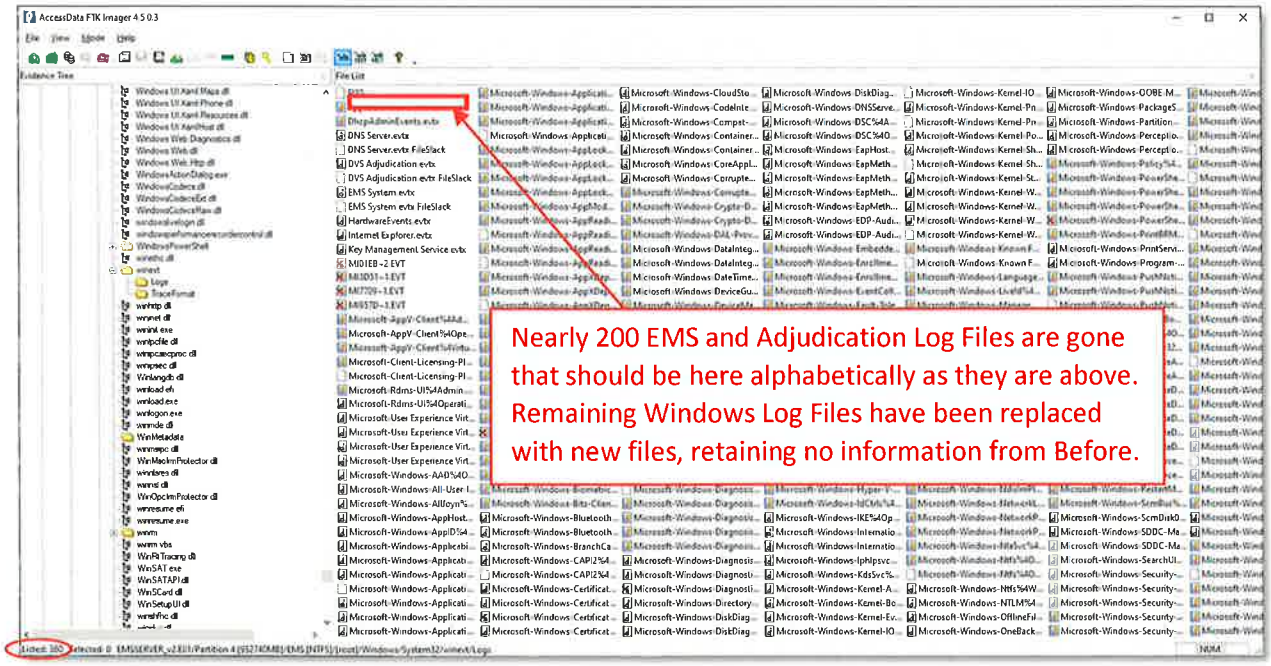
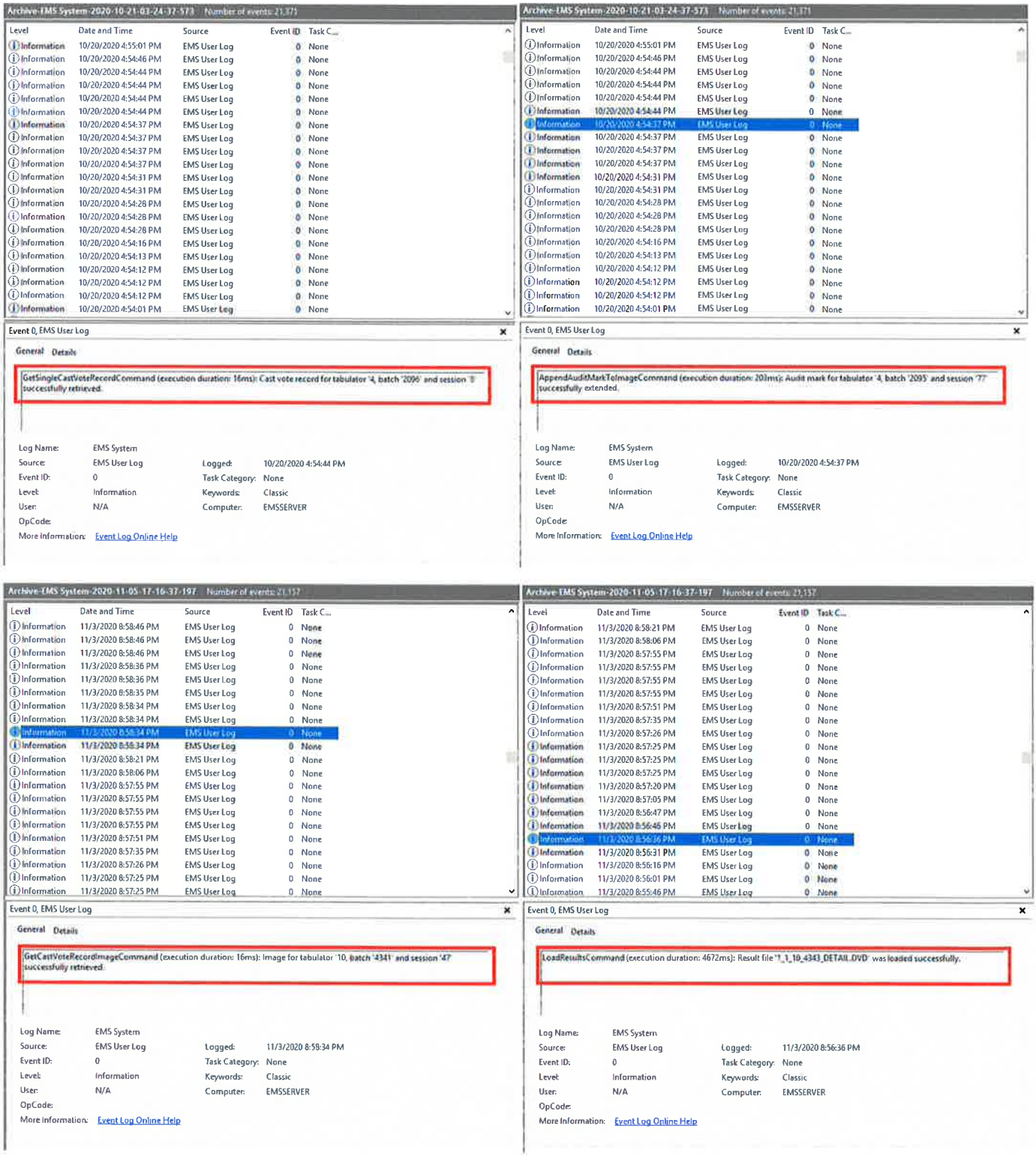


Figure 32 - EMS Server (5.13) Event Logs After



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



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

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

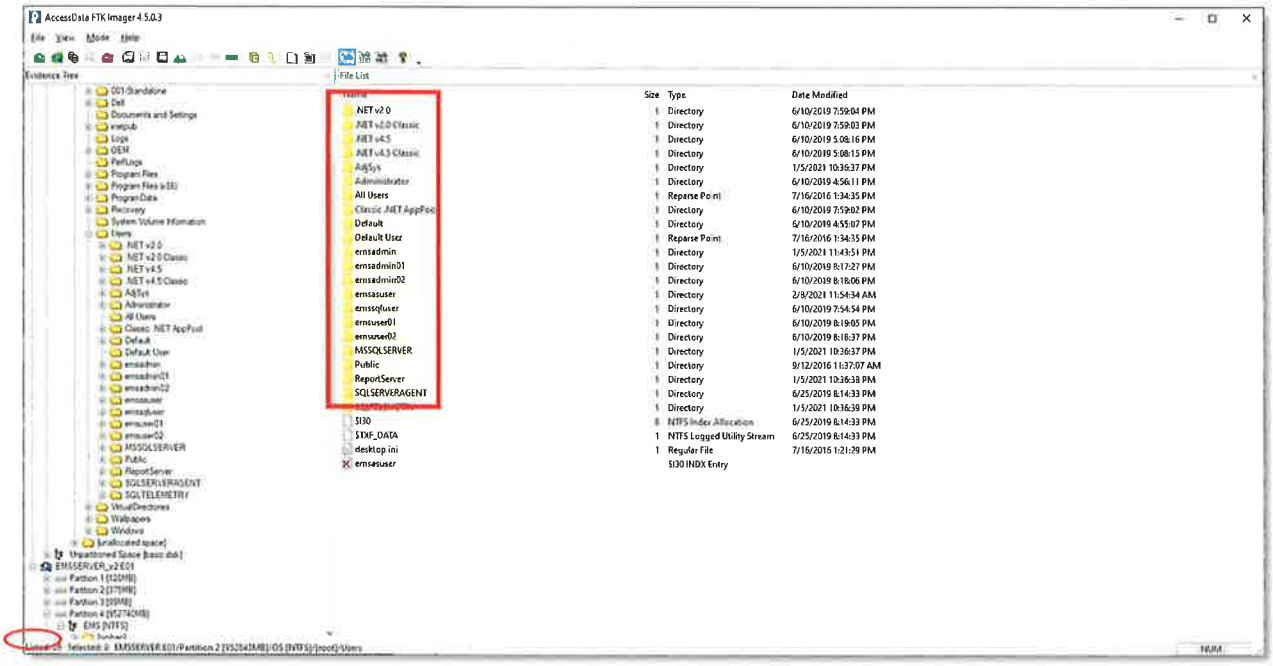
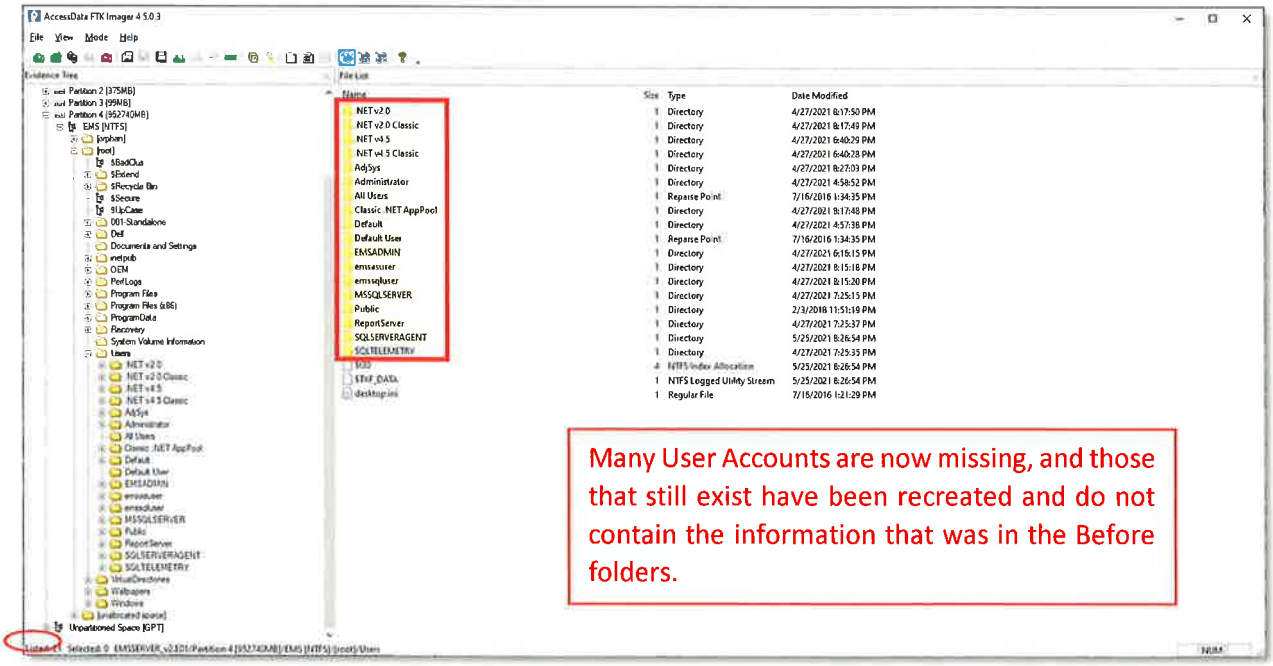


Figure 35 - EMS Server (5.13) System Users After



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

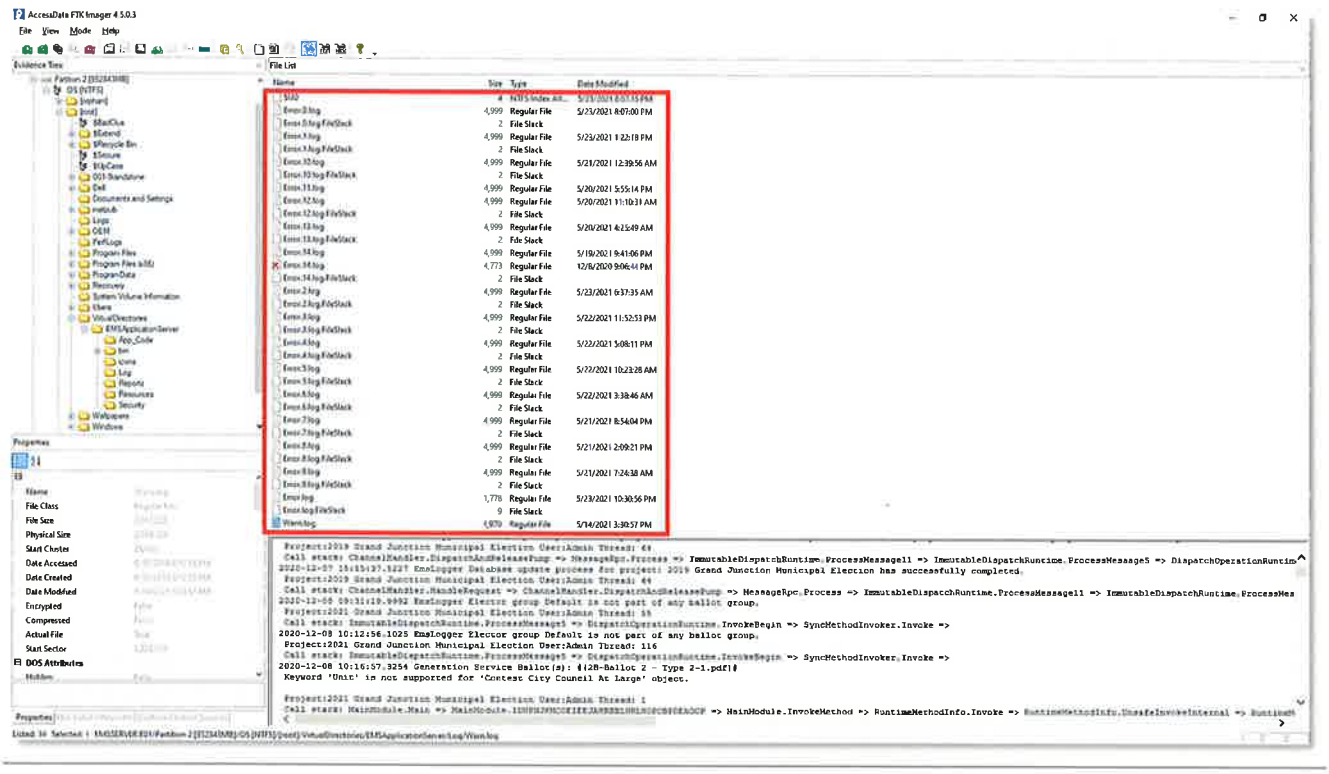
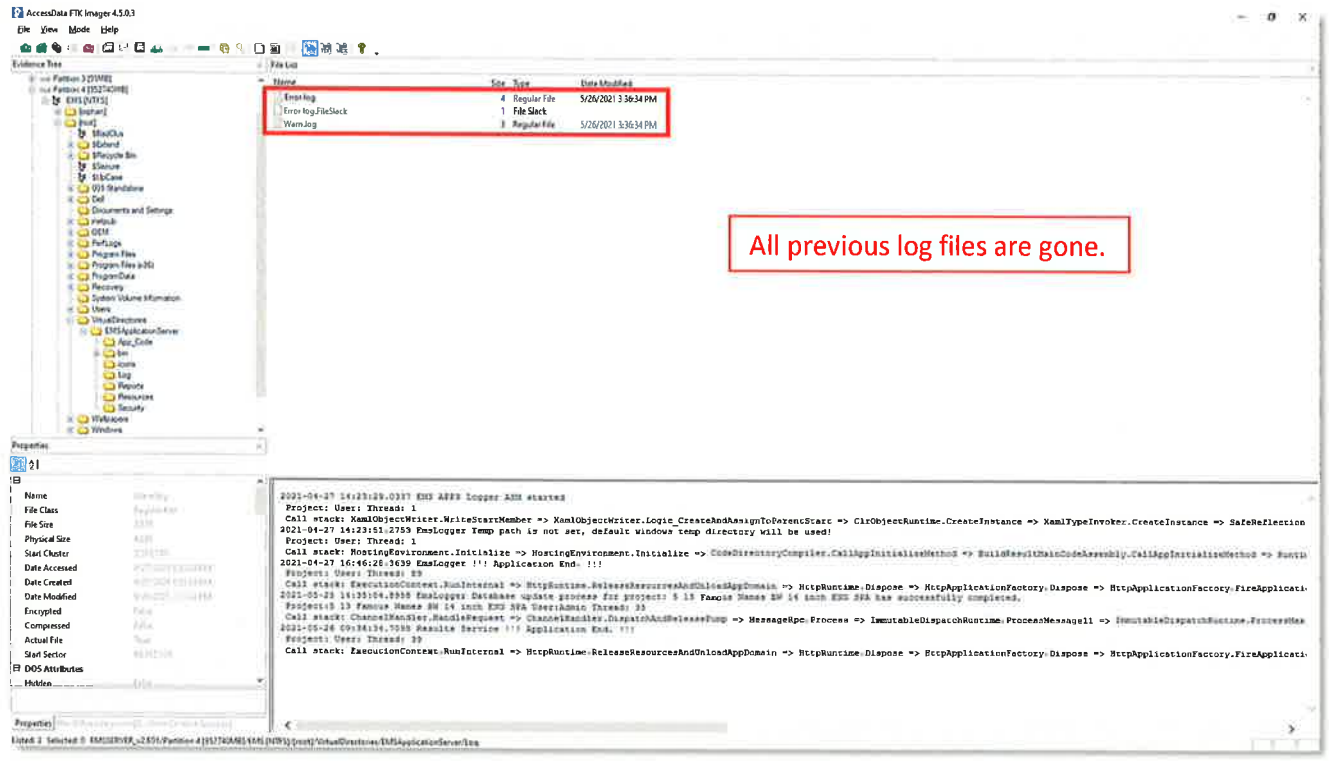


Figure 37 - EMS Server (5.13) Virtual Directory Log Files After



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:

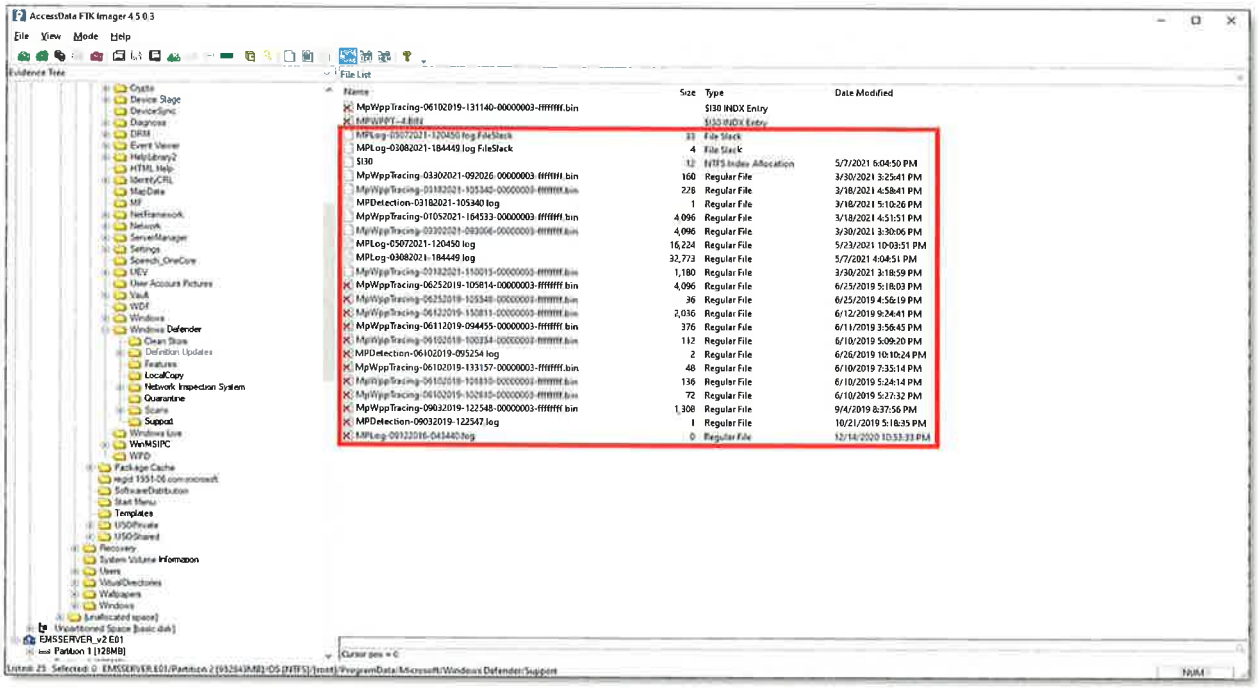
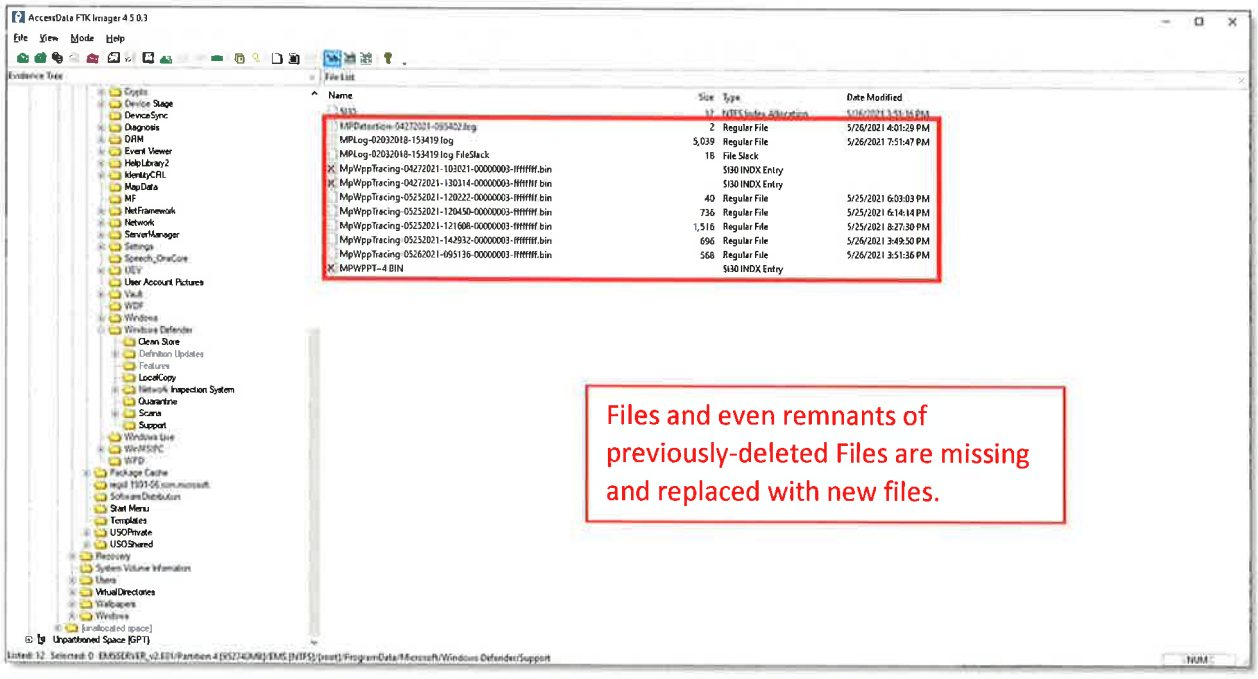


Figure 39 - EMS Server (5.13) Windows Defender Log Files After



Files and even remnants of previously-deleted Files are missing and replaced with new files.

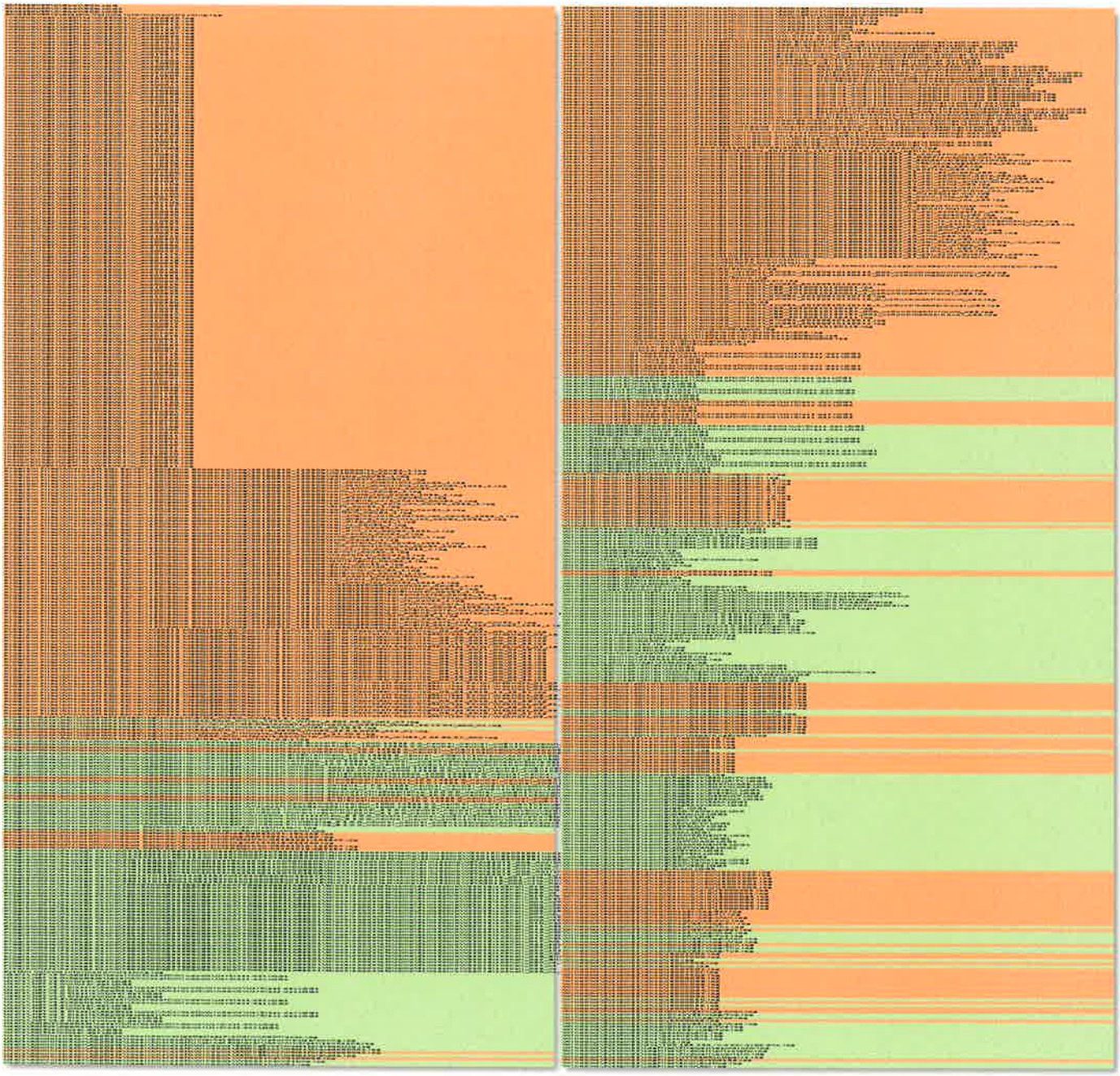
Server List of .log files in Before Image that were Deleted.

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



Significant Number of Logfiles Missing

The dataset from which this spreadsheet was created was extracted from the EnCase images of the original evidence on the hard drives of the EMS Server and had a traceable chain of custody. While the images above are too small to be readable, the entire content of this list is reproduced in Appendix A.

Of the original 807 ".log" files on the EMS Server before Dominion's update, only 302 remain, and 505 ".log" files have been deleted or overwritten.

Of the files *that remain*, the forensic examination has not yet verified whether the content of these files (which have the same filename and Path – e.g., in the same directories) is unchanged. The files that have been deleted DO include files that constitute Election Records and are subject to Federal and State data retention laws.

This list is only 807 files, and the text size is so small that the content is barely readable. The list of files has been broken down into small subsets because the number of files on the entire server totals 363,321 files, many of which are provided by Microsoft as part of the Windows Server 2016 operating system and its associated application programs and are not Election Related and do not contain actual Election Data.

List of .evtx Event Log Files deleted

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

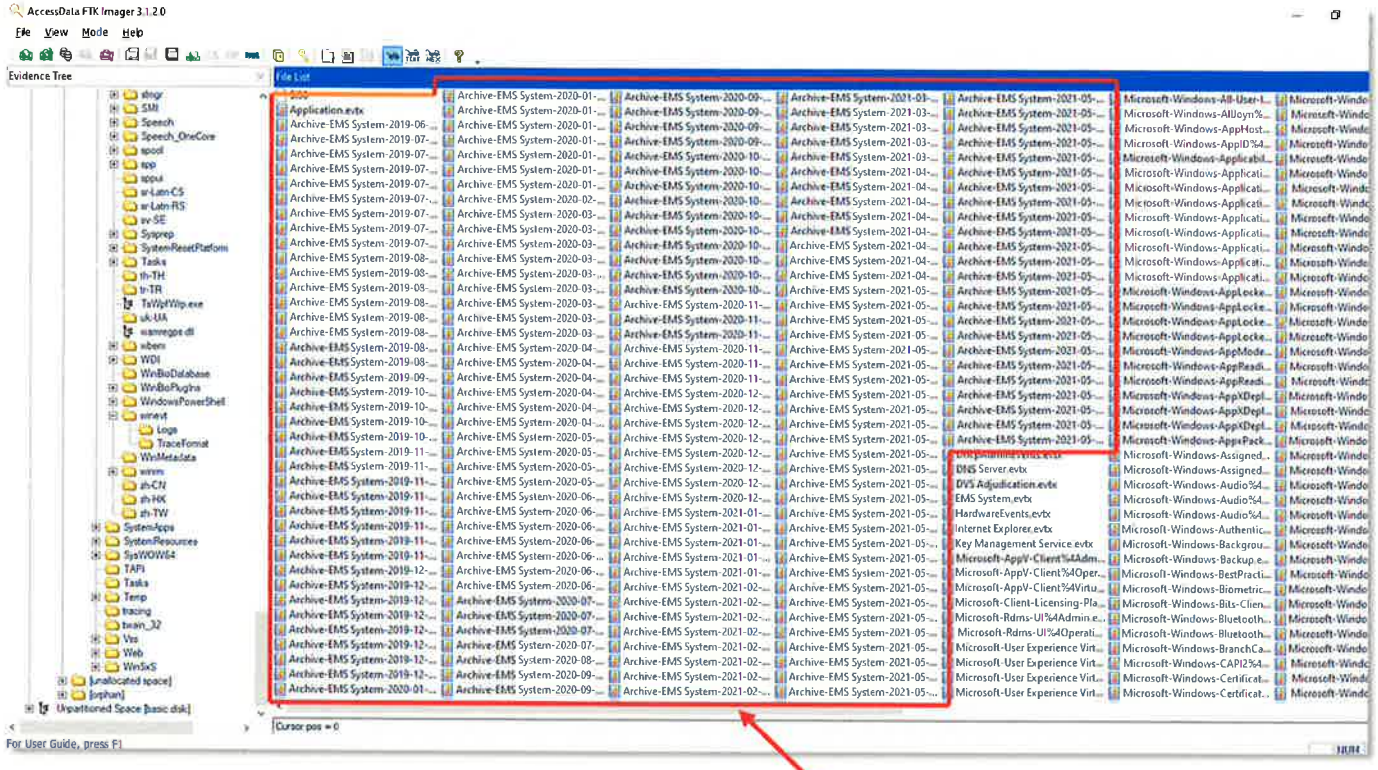
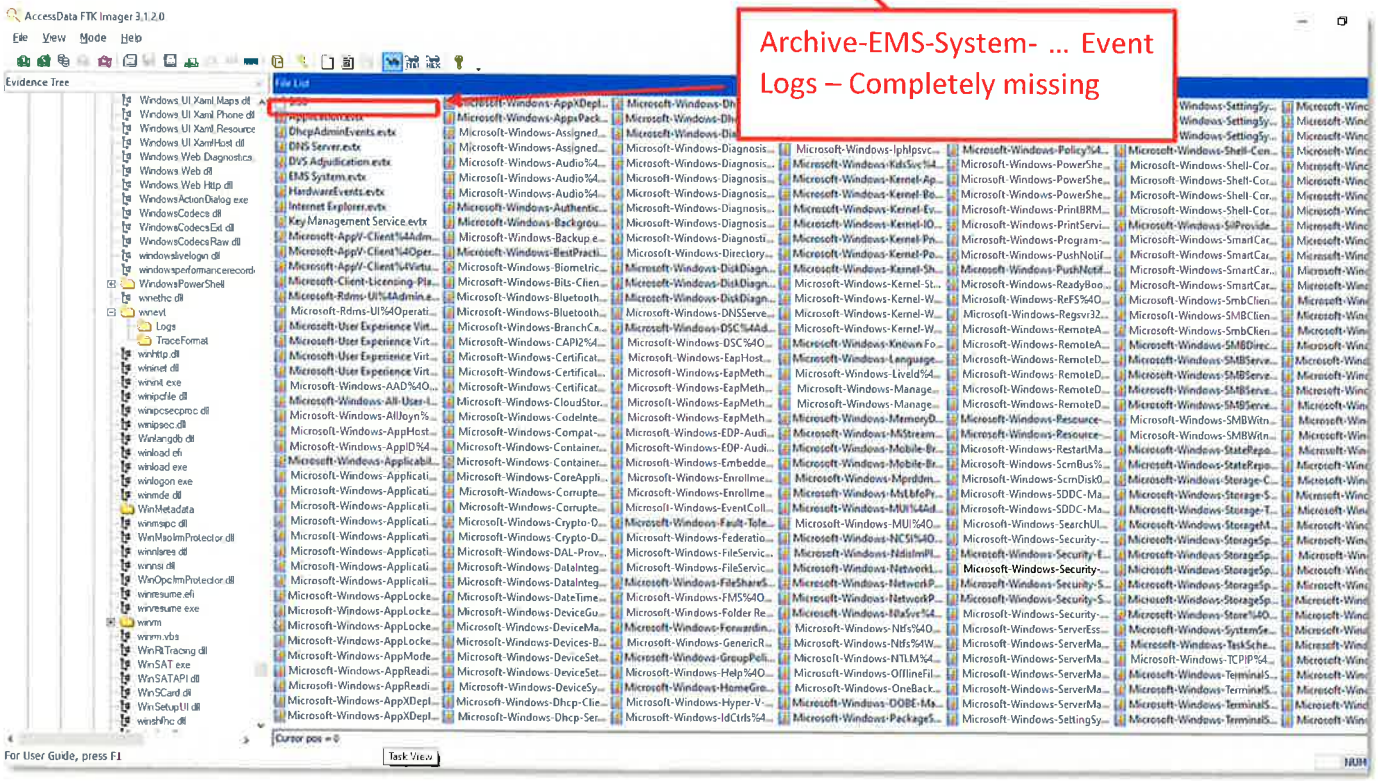


Figure 42 - EMS Server (5.13) List of .evtx Event Log Files After



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., comparision 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-VHDMP-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%4Operation
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 Firewal
Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Iphlpsvc%4Opera
Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4O
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-Exper
Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Program-Compati
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%4Actior
Logs\Microsoft-Windows-LiveId%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceManageme
Logs\Microsoft-Windows-MUI%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Power%4T
Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Boot%4Op
Logs\Microsoft-Windows-MUI%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%
Logs\Microsoft-Windows-NCSI%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%
Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-PnP%4Cor
Logs\Microsoft-Windows-Ntfs%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ShimEngin
Logs\Microsoft-Windows-Ntfs%4WHC.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4Operation
Logs\Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VolumeSnapshot-
Logs\Microsoft-Windows-SettingSync%4Debug.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-IO%4Oper
Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4(
Logs\Microsoft-Windows-Kernel-PnP%4Configuration.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4E
Logs\Microsoft-Windows-SettingSync%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4(
Logs\Microsoft-Windows-Shell-Core%4ActionCenter.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewal
Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NCSI%4Operatior
Logs\Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WinINet-Config%
Logs\Microsoft-Windows-Shell-Core%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4(
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-Wcnfs
Logs\Microsoft-Windows-SMBServer%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4Op

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-WinINet-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-2019-12-02-15-06-36-405.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\Microsoft-Windows-User Profile Servi
Windows\System32\winevt\Logs\Microsoft-Windows-LiveId%4Operatic
Windows\System32\winevt\Logs\Microsoft-Windows-SMBClient%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Con
Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Secu
Windows\System32\winevt\Logs\Microsoft-Windows-Winlogon%4Oper
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4De
Windows\System32\winevt\Logs\Microsoft-Windows-DateTimeControl
Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders Al
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%4Logo
Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment
Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runtir
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-D
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%4Operat
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Exper
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Exper
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Exper
Windows\System32\winevt\Logs\Microsoft-Windows-Application-Exper
Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-I
Windows\System32\winevt\Logs\Microsoft-Windows-BackgroundTaskIn
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-M
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-M
Windows\System32\winevt\Logs\Microsoft-Windows-Forwarding%4Op
Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-M
Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaus
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScan
Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScan
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Schedu
Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Cont
Windows\System32\winevt\Logs\Microsoft-Windows-Shell-ConnectedA
Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-M
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4
Windows\System32\winevt\Logs\Microsoft-Windows-Storage-ClassPnP
Windows\System32\winevt\Logs\Microsoft-Windows-RestartManager%
Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PLA%4
Windows\System32\winevt\Logs\Microsoft-Windows-CAPI2%4Operatic
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\DVS 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 Virtualizati
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizati
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizati
Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizati
Windows\System32\winevt\Logs\Microsoft-Windows-AAD%4Operation
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%4MSI
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac
Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac
Windows\System32\winevt\Logs\Microsoft-Windows-AppxPackaging%
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccess%
Windows\System32\winevt\Logs\Microsoft-Windows-AssignedAccessB
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\Microsoft-Windows-Audio%4Operati
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-22-13-12-21-043.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Playbac
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-06-08-06-21-993.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Authentication U
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-05-17-16-37-197.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Backup.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-23-08-11-827.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-BestPractices%4(
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-17-01-19-18-484.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Biometrics%4Ope
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-01-39-07-647.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Ope
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-04-12-10-17-214.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-BthLE
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-12-02-56-47-489.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-MTPE
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-07-26-54-297.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-BranchCacheSME
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-04-04-03-42-737.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServic
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-16-16-31-58-059.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServic
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-21-12-09-41-781.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServic
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-28-14-04-05-771.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Compat-Appraise
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-12-22-02-14-487.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CoreApplication%
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-13-18-05-49-770.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRec
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-17-19-10-01-322.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRec
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-05-14-13-33-324.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DAL-Provider%4(
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-13-10-56-695.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceGuard%4C
Windows\System32\winevt\Logs\Archive-EMS System-2019-11-28-22-08-50-835.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Devices-Backgrou
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-17-11-04-36-787.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSync%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-05-00-03-39-390.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-12-10-03-10-333.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-20-40-41-039.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-24-11-15-42-872.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Netw
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-18-17-48-53-388.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DirectoryServices
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-09-10-14-15-715.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnostic%4
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-31-11-01-47-908.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticDa
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-27-08-29-08-399.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticRe
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-14-23-29-04-158.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Admin.evt
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-24-21-04-12-832.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Operation
Windows\System32\winevt\Logs\Archive-EMS System-2019-12-21-04-04-25-803.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapHost%4Opera
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-01-07-03-50-651.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-14-18-29-08-151.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-11-21-02-29-740.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Sim
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-03-11-33-19-283.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ttls
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-19-20-02-44-037.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-Regul
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-28-20-58-32-283.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-TCB%
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-16-03-02-57-774.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EmbeddedAppLa
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-01-21-14-15-340.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentPolicy
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-08-12-31-149.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentWebS
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-22-17-12-11-701.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-EventCollector%4
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-05-45-04-636.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-H
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-05-12-32-06-091.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FederationServic
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-26-13-42-04-162.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Serv
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-16-14-59-42-045.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Serv
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-23-13-23-46-471.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FileShareShadow
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-18-23-53-08-392.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-FMS%4Operation
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-13-14-26-512.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Folder Redirectio
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-27-17-59-53-690.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NdisImPlatform%
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-20-09-29-41-350.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-GenericRoaming%
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-20-07-59-19-878.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Help%4Operatio
Windows\System32\winevt\Logs\Archive-EMS System-2020-01-31-02-47-11-038.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Hyper-V-Guest-D
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-29-23-11-26-924.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-IdCtrls%4Operati
Windows\System32\winevt\Logs\Archive-EMS System-2020-03-09-05-29-49-411.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-IKE%4Operationa
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-26-06-11-56-096.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-International-Reg
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-00-00-39-858.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-KdsSvc%4Operat
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-18-58-50-004.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ApphelpC
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-28-08-06-44-934.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-EventTrac
Windows\System32\winevt\Logs\Archive-EMS System-2020-04-11-14-07-34-718.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WDI%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-15-07-27-29-016.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-LanguagePackSet
Windows\System32\winevt\Logs\Archive-EMS System-2020-07-04-17-16-43-223.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ManagementTod
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-24-22-45-04-435.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ManagementTod
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-20-18-16-33-823.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MemoryDiagnost
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-18-12-49-02-987.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MiStreamProvide
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-13-08-24-43-079.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadbar
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-22-12-08-49-154.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadbar
Windows\System32\winevt\Logs\Archive-EMS System-2021-03-30-02-15-24-619.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Mprddm%4Oper
Windows\System32\winevt\Logs\Archive-EMS System-2020-05-22-17-53-50-782.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-MsLbfoProvider%
Windows\System32\winevt\Logs\Archive-EMS System-2020-06-11-17-12-21-460.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NetworkLocation
Windows\System32\winevt\Logs\Archive-EMS System-2021-01-18-20-12-44-811.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProvider
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-02-14-34-04-967.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-NTLM%4Operati
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-07-10-51-04-386.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-OfflineFiles%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-11-05-09-09-286.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-OneBackup%4De
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-31-12-27-41-741.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-OOBE-Machine-D
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-22-20-55-04-936.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PackageStateRoa

Windows\System32\winevt\Logs\Archive-EMS System-2020-07-01-03-27-07-105.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagn
Windows\System32\winevt\Logs\Archive-EMS System-2021-04-09-17-04-07-509.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionRuntin
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-09-07-12-48-391.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionSenso
Windows\System32\winevt\Logs\Archive-EMS System-2020-10-11-00-11-12-292.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-User Control Pan
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-12-21-57-907.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Policy%4Operatic
	Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell-Desir
Windows\System32\winevt\Logs\Archive-EMS System-2020-11-03-08-03-17-087.evtx	FileDownloadManager%4Operational.evtx
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-18-13-07-673.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PrintBRM%4Adm
Windows\System32\winevt\Logs\Archive-EMS System-2020-08-27-17-53-57-312.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-PrintService%4Ac
Windows\System32\winevt\Logs\Archive-EMS System-2020-09-30-01-16-19-620.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-19-51-20-073.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ReFS%4Operatio
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-02-24-44-262.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Regsvr32%4Oper
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-23-57-17-682.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-08-20-31-15-022.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-21-34-01-652.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-02-16-11-00-907.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-10-17-14-18-337.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-16-31-18-634.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-17-35-55-190.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaus
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-10-17-26-50-697.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ScmBus%4Certifi
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-08-21-07-21-169.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ScmDisk0101%4C
Windows\System32\winevt\Logs\Archive-EMS System-2020-12-09-22-01-49-473.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SearchUI%4Oper
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-15-41-56-864.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-Audit-Co
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-14-16-397.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-Enterpri
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-25-20-742.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-Netlogo
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-33-50-215.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-
Windows\System32\winevt\Logs\Archive-EMS System-2021-02-09-17-46-57-607.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Security-UserCon
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-17-20-24-507.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ServerEssentials-
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-07-23-24-216.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-C
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-14-51-41-139.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azur
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-04-06-37-355.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azur
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-09-54-24-839.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SilProvider%4Ope
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-19-14-52-50-172.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-Audit%
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-06-37-33-489.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-Devic
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-03-16-22-000.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-V
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-21-19-02-14-166.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-V
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-00-50-01-529.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SMBDirect%4Adr
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-14-01-35-37-340.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClien
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-14-00-17-879.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClien
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-17-23-46-597.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Tiering%
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-20-37-42-553.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageManager
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-12-09-03-54-186.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-D
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-10-43-31-360.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-D
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-04-55-44-339.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Sp
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-17-22-18-50-801.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Sp
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-13-19-47-50-347.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-SystemSettingsTh
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-06-34-10-708.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TCPIP%4Operatic
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-02-28-13-043.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-18-21-29-43-807.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-00-46-23-325.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-15-18-09-30-390.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-14-03-47-942.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-11-36-14-332.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-16-11-32-36-872.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-20-08-16-00-636.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-23-05-48-27-189.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Archive-EMS System-2021-05-22-12-25-20-731.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TZSync%4Operati
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-19-09-27-36-681.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-TZUtil%4Operatic
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Security.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-UAC%4Operation
Windows\System32\winevt\Logs\Archive-EMS System-2019-07-23-03-48-10-012.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-UAC-FileVirtualiz
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-User Device Regis
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-14-17-50-17-089.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-User-Loader%4Op
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-22-06-31-22-632.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VerifyHardwareS
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-03-10-49-41-423.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Volume%4Diagno
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%4Operational.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VPN-Client%4Ope
Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%4FilterNotifications.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-VPN%4Operation
Windows\System32\winevt\Logs\DhcpAdminEvents.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WFP%4Operation
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-26-00-51-55-728.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Win32k%4Operat
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-07-05-09-14-598.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WindowsSystemA
Windows\System32\winevt\Logs\DNS Server.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Winsock-WS2HEL

Windows\System32\winevt\Logs\Microsoft-Windows-DNSServer%4AudIt.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Wired-AutoConfig%4
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-10-23-29-48-856.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-Workplace Join%4Ad
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-18-12-10-49-482.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WPD-ClassInstaller%4
Windows\System32\winevt\Logs\Archive-EMS System-2019-09-02-13-32-58-546.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WPD-CompositeClass
Windows\System32\winevt\Logs\Archive-EMS System-2019-08-29-19-12-25-021.evtx	Windows\System32\winevt\Logs\Microsoft-Windows-WPD-MTPClassDriver
Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Audit.evtx	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\u_ex210406.log

inetpub\logs\LogFiles\W3SVC1\u_ex200903.log

inetpub\logs\LogFiles\W3SVC1\u_ex191021.log

inetpub\logs\LogFiles\W3SVC1\u_ex191101.log

inetpub\logs\LogFiles\W3SVC1\u_ex201028.log

inetpub\logs\LogFiles\W3SVC1\u_ex191025.log

inetpub\logs\LogFiles\W3SVC1\u_ex191023.log

inetpub\logs\LogFiles\W3SVC1\u_ex200522.log

inetpub\logs\LogFiles\W3SVC1\u_ex191126.log

inetpub\logs\LogFiles\W3SVC1\u_ex200819.log

inetpub\logs\LogFiles\W3SVC1\u_ex191028.log

inetpub\logs\LogFiles\W3SVC1\u_ex210104.log

inetpub\logs\LogFiles\W3SVC1\u_ex191022.log

inetpub\logs\LogFiles\W3SVC1\u_ex200625.log

inetpub\logs\LogFiles\W3SVC1\u_ex210211.log

inetpub\logs\LogFiles\W3SVC1\u_ex201008.log

inetpub\logs\LogFiles\W3SVC1\u_ex191114.log

inetpub\logs\LogFiles\W3SVC1\u_ex200826.log

inetpub\logs\LogFiles\W3SVC1\u_ex210223.log

inetpub\logs\LogFiles\W3SVC1\u_ex210224.log

inetpub\logs\LogFiles\W3SVC1\u_ex210205.log

inetpub\logs\LogFiles\W3SVC1\u_ex210318.log

inetpub\logs\LogFiles\W3SVC1\u_ex200520.log

inetpub\logs\LogFiles\W3SVC1\u_ex201208.log

inetpub\logs\LogFiles\W3SVC1\u_ex210407.log

inetpub\logs\LogFiles\W3SVC1\u_ex191030.log

inetpub\logs\LogFiles\W3SVC1\u_ex191031.log

inetpub\logs\LogFiles\W3SVC1\u_ex191106.log

inetpub\logs\LogFiles\W3SVC1\u_ex191105.log

inetpub\logs\LogFiles\W3SVC1\u_ex191029.log

inetpub\logs\LogFiles\W3SVC1\u_ex191104.log

inetpub\logs\LogFiles\W3SVC1\u_ex200730.log

inetpub\logs\LogFiles\W3SVC1\u_ex210512.log

inetpub\logs\LogFiles\W3SVC1\u_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_ex200623.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\sqlncli_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.l

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_20

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_20

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_20

Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_03_30_20

Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_03_30_20

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_20

Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost_06_26_20

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_20

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_20

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_20

ProgramData\Dell\UpdatePackage\log\support\BIOS_YY63D_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\ActivationStor

ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.AccountsControl_10.0.14393.0_neutral__cw5n1h2txyewy\ActivationStor

ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.BioEnrollment_10.0.14393.0_neutral__cw5n1h2txyewy\ActivationStore.

ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.BioEnrollment_10.0.14393.0_neutral__cw5n1h2txyewy\ActivationStore.

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_cw5n1h2txye

ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Apprep.ChxApp_1000.14393.0.0_neutral_neutral_cw5n1h2txye

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\A

ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.SecondaryTileExperience_10.0.0.0_neutral__cw5n1h2txyewy\A

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\Activati

ProgramData\Microsoft\Windows\AppRepository\Packages\windows.immersivecontrolpanel_6.2.0.0_neutral_neutral_cw5n1h2txyewy\Activati

ProgramData\Microsoft\Windows\AppRepository\Packages\Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore.

ProgramData\Microsoft\Windows\AppRepository\Packages\Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore.

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_cw5n1h2txyewy\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\02A26E554FBB4232ACD36E70D09F2C7893D399CD\%localappdata%\temp\Ssms
444C320629FA}_001_kb3095681.log

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB\%localappdata%\temp\SsmsSetup\VSTALS2015_003_RoslynLa

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB\%localappdata%\temp\SsmsSetup\VSTALS2015_004_vsta_lan

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB\%localappdata%\temp\SsmsSetup\VSTALS2015_001_vsta_lslp

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB\%localappdata%\temp\SsmsSetup\VSTALS2015_002_RoslynLa

ProgramData\Package Cache\4F812BBB2BE7E30CED293F8A229A5410D70DE6DB\%localappdata%\temp\SsmsSetup\VSTALS2015_000_vsta_lscc

ProgramData\Package Cache\5E6157D16EC044A823B2FD2C030ED6DECD2E997E\%localappdata%\temp\SsmsSetup\VSTA2015_001_vsta_hostir

ProgramData\Package Cache\5E6157D16EC044A823B2FD2C030ED6DECD2E997E\%localappdata%\temp\SsmsSetup\VSTA2015_002_vsta_finaliz

ProgramData\Package Cache\5E6157D16EC044A823B2FD2C030ED6DECD2E997E\%localappdata%\temp\SsmsSetup\VSTA2015_000_vsta_hostir

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_vsbsln

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell_009_vsbsln

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_netfxc

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\AdjSys\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\AdjSys\ntuser.dat.LOG1

Users\AdjSys\ntuser.dat.LOG2

Users\Administrator\AppData\Local\ConnectedDevicesPlatform\CDPTraces.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_cw5n1h2txyewy\Settings\settings.dat.LOG2

Users\Administrator\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\Administrator\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy\Settings\settings.dat.LOG2

Users\Administrator\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\Administrator\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2

Users\Administrator\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\Administrator\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat.LOG2

Users\Administrator\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\Administrator\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG2

Users\Administrator\AppData\Local\Packages\Windows.MiracastView_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\Administrator\AppData\Local\Packages\Windows.MiracastView_cw5n1h2txyewy\Settings\settings.dat.LOG2

Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy

Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat.LOG1

Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat.LOG2

Users\Administrator\AppData\Local\Temp\MpSigStub.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\ie4uinit-UserConfig.log

Users\emsadmin\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log

Users\emsadmin\AppData\Local\Microsoft\SQL Server Management Studio\14.0\ComponentModelCache\Microsoft.VisualStudio.Default.catalo

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\f92aeb63-07b8-4662-94b4-f4bcccba37ec\baseutils.log

Users\emsadmin\AppData\Local\Temp\SSMS\Ssms_20190610_131541566_PID2136_logFile.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_32_sql_ssms_loc_x64_Loc.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_3_DACFramework.msi.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_4_SQLServerBestPracticesPolicies.msi.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_5_TSqlLanguageService_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_6_sql_diag_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_7_adalsql_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_22_sql_as_oledb_x86.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_23_sql_common_core_x86.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_24_sql_common_core_loc_x86.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_30_sql_ssms_extensions_loc_x86.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_31_sql_ssms_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_33_sql_tools_connectivity_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_18_smo_extensions_loc_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_2_msodbcsql.msi.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_8_conn_info_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_9_conn_info_loc_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_0_SQLSysClrTypes.msi.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_1_sqlncli.msi.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_10_sql_batchparser_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\SSMS-Setup-ENU_20190610125637_11_sql_xevent_x64.log

Users\emsadmin\AppData\Local\Temp\SsmsSetup\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\VSD329B.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_vcredist_amd64_20190610120224_000_vcRuntimeMinimum_x64.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_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_vcredist_amd64_20190610120224.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_x86_20190610120041.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_x86_20190610120041_0_vcRuntimeMinimum_x86.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_x86_20190610120041_1_vcRuntimeAdditional_x86.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_amd64_20190610120118.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_amd64_20190610120118_0_vcRuntimeMinimum_x64.log

Users\emsadmin\AppData\Local\Temp\wmsetup.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_amd64_20190610120118_1_vcRuntimeAdditional_x64.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_x86_20190610120157.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_x86_20190610120157_000_vcRuntimeMinimum_x86.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_x86_20190610120157_001_vcRuntimeAdditional_x86.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_x86_20190610125911.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_amd64_20190610125911.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_amd64_20190610125912.log

Users\emsadmin\AppData\Local\Temp\dd_vcredist_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\emsasuser\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\emsasuser\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\emsasuser\ntuser.dat.LOG1

Users\emsasuser\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\emsuser01\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\emsuser01\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\emsuser01\ntuser.dat.LOG1

Users\emsuser01\ntuser.dat.LOG2

Users\emsuser02\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

Users\emsuser02\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2

Users\emsuser02\ntuser.dat.LOG1

Users\emsuser02\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\sammui.log

Windows\debug\PASSWD.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\DDACLSys.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\edbtmp.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

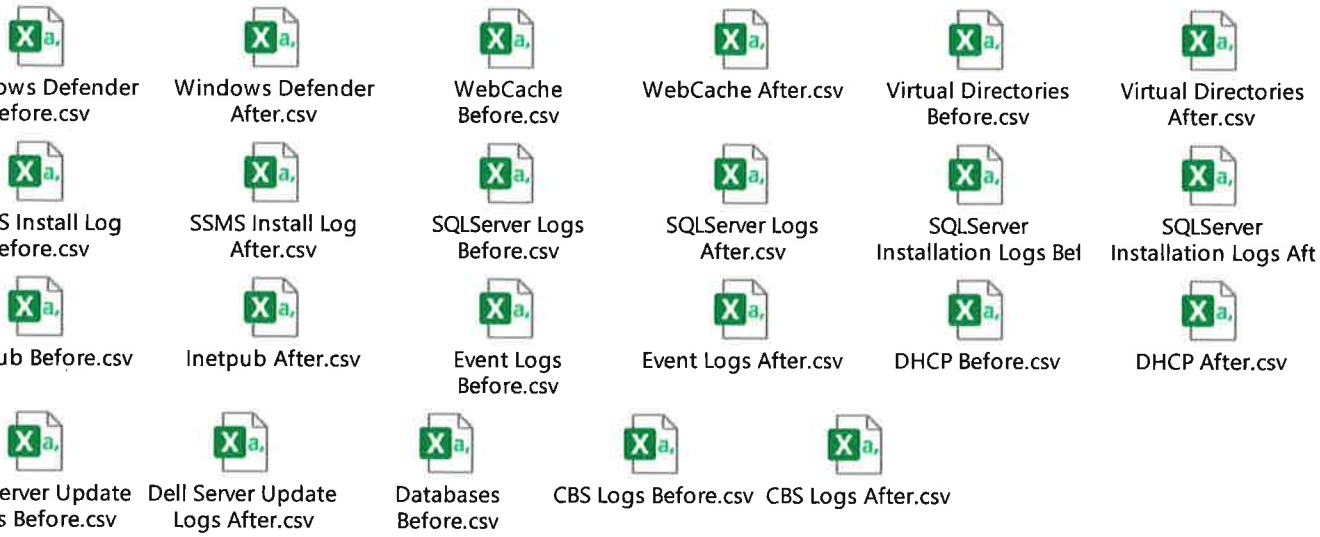
Windows\System32\config\SAM.LOG1

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-LiveId%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-WinINet-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-2019-12-02-15-06-36-405.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%4Adr
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-Wcifs%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-Troublesh
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.ev
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.e
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.
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.ev
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.e
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-FileDownloadMana
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-Synth3dvsc%4Admin.e
Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evt
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.evt
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-TCPIP%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.evt
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operation

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\SMSApi.evtx

APPENDIX D. LIST OF FIGURES

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 electon 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 secton 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.