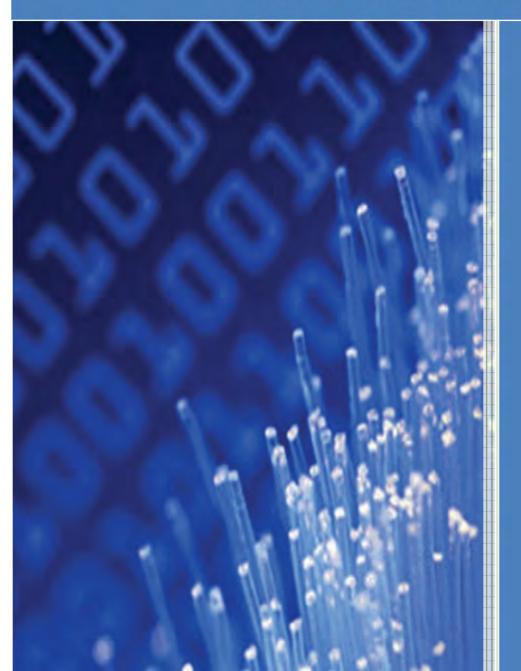


Mesa County Colorado Voting Systems

# **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  | L |
|--|---|
| Introduction   | ; |
| Legal References   | 5 |
| Forensic Examination and Analysis Report   | 7 |
| Forensic Analysis  | 3 |
| System Identification  | 3 |
| Authenticity and Chain of Custody  | ) |
| FINDINGS   | L |
| Overview of System Data Sources  | L |
| Server Disk Partition Structure Overwritten12                                    | 2 |
| Website Server Log Files Missing   | 5 |
| Server Microsoft SQL Server Installation Log Files Missing                       | 7 |
| Server Microsoft SQL Server Log Files Missing                                    | ) |
| EMS Server Dell Server Updates Missing   | ) |
| Server 'Administrator' WebCache Log Files Overwritten                            | 2 |
| Server 'emsadmin' WebCache Log Files Overwritten                                 | 3 |
| Server SQL Server Management Studio (SSMS) Log Files Overwritten                 | 5 |
| Server CBS Log Files Overwritten   | 5 |
| Server Election Databases Missing  | 7 |
| Server Event Logs Missing/Overwritten  | ) |
| Server System Users are Missing  | L |
| Server Virtual Directories Log Files Missing                                     | 2 |
| Server Windows Defender Log Files Missing/Overwritten                            | 3 |
| Server List of .log files in Before Image that were Deleted                      | ļ |
| Significant Number of Logfiles Missing   | 5 |
| List of .evtx Event Log Files deleted  | 5 |
| Analysis Summary   | Ĺ |
| Conclusion   | L |
| Appendix A. Deleted ".log" files after Dominion Trusted Build update             | 2 |
| Appendix B. Supporting Documentation: File details and hash sets for screenshots | L |
| Appendix C. Microsoft EVENT log files  | 2 |
| Appendix D. List of Figures  | 5 |
| Appendix E. 2002 Voting Systems Standards (VSS)                                  | 7 |

# **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<sup>1</sup> 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

<sup>&</sup>lt;sup>1</sup> 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 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<sup>2</sup>.

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:

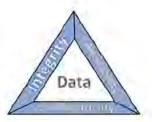
- Engineering systems with a focus on security
- Building systems to meet published high-security standards and applicable regulations
- Patching systems to ensure that vulnerabilities are removed
- Securing networks to ensure highly controlled access
- Logging of all communications, processes, access, 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:

<sup>&</sup>lt;sup>2</sup> 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
```

```
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.

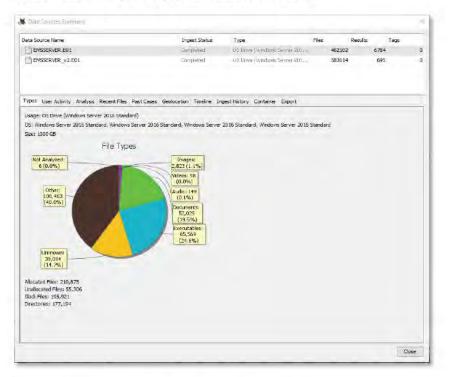
# AUTHENTICITY AND CHAIN OF CUSTODY

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

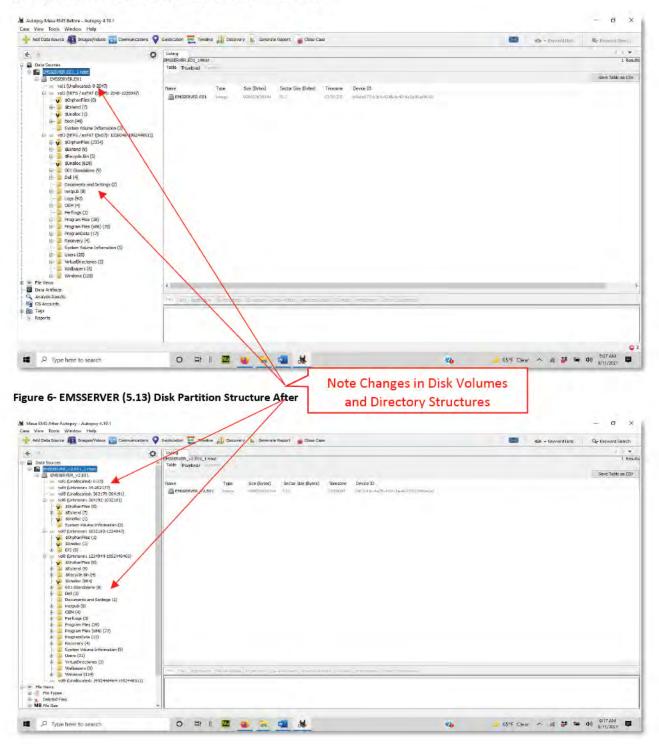


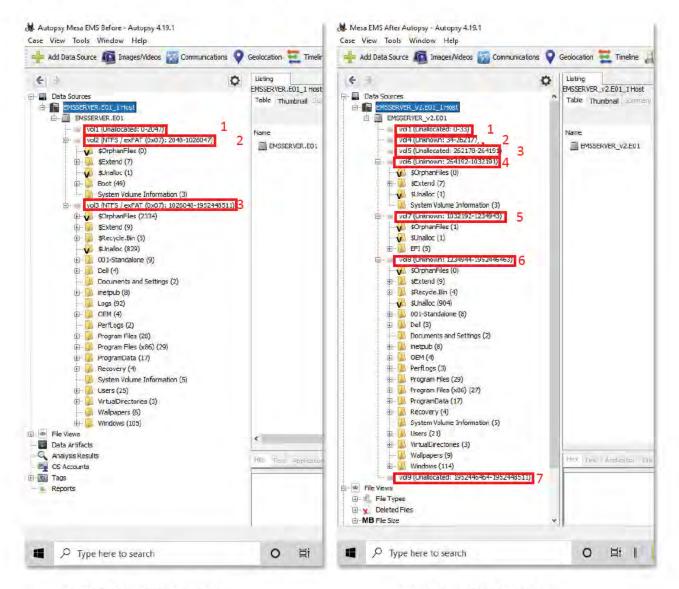
#### Figure 4 - EMS Server (5.13) System Data Sources After



**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





**Before Dominion Update** 

After Dominion Update

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

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

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

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

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

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

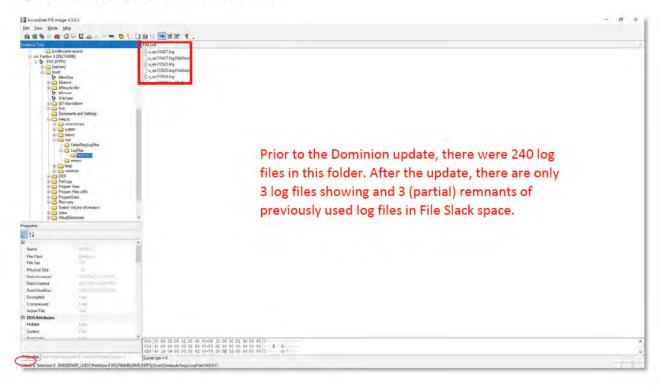
Special forensic software is required to access file slack space, and the data it contains are partial remnants of previous system data. This data may be of use in forensic investigation, and forensic tools often identify it. File Slack is identified here for clarity and better understanding of these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

# Website Server Log Files Missing

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

| 9         m.c.l.a.         u.e.10101109/FARIAL         u.e.20001109         0.0000109  | 2004-0j         u,u21022.koj         u,u21022.koj           2004-0j         u,u21022.koj         u,u21012.koj           2004-0j         u,u21022.koj         u,u21012.koj           2004-0j         u,u21022.koj         u,u21011.koj           2004-0j         u,u21022.koj         u,u21012.koj           2004-0j         u,u21022.koj         u,u210102.koj           2004-0j         u,u21012.koj         u,u21012.koj           2004-0j         u,u21012.koj  |
|--|--|
| Image: Source of Source  | 2004-0j         u,u21022.koj         u,u21022.koj           2004-0j         u,u21022.koj         u,u21012.koj           2004-0j         u,u21022.koj         u,u21012.koj           2004-0j         u,u21022.koj         u,u21011.koj           2004-0j         u,u21022.koj         u,u21012.koj           2004-0j         u,u21022.koj         u,u210102.koj           2004-0j         u,u21012.koj         u,u21012.koj           2004-0j         u,u21012.koj  |
| <ul> <li>L. C. 1981 Logi</li> <lil. 1981="" c.="" logi<<="" td=""><td>Dittligs/Felder.     U.v.210122.prietlick:       Dittligs/Felder.     U.v.210121.prietlick:       Dittligs/Felder.     U.v.210121.prietlick:       Dittligs/Felder.     U.v.210121.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210011.prietlick:       Dittligs/Felder.     <td< td=""></td<></td></lil.></ul>  | Dittligs/Felder.     U.v.210122.prietlick:       Dittligs/Felder.     U.v.210121.prietlick:       Dittligs/Felder.     U.v.210121.prietlick:       Dittligs/Felder.     U.v.210121.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210111.prietlick:       Dittligs/Felder.     U.v.210011.prietlick:       Dittligs/Felder. <td< td=""></td<>  |
| Summary Street         Control Log Predictor         Co  | 2004g         U.g.2022.20.g.Felleck         U.g.21001.6.g           2005g/Holick         U.g.21001.6.g         U.g.21001.6.g           2005g/Holick         U.g.21001.6.g         U.g.21001.6.g           2016g/Holick         U.g.21001.6.g         U.g.2101.6.g           2016g/Holick   |
| ibin         u.e.*9925.5.g         u.e.*9925.5.g <td>2001.gp/Atlack     U_u.21022.tog       2001.gp/Atlack     U_u.21022.tog       2101.gp/Atlack     U_u.21002.tog       <td< td=""></td<></td>   | 2001.gp/Atlack     U_u.21022.tog       2001.gp/Atlack     U_u.21022.tog       2101.gp/Atlack     U_u.21002.tog       2101.gp/Atlack     U_u.21002.tog <td< td=""></td<>   |
| Picuba film         u.e.1955.bag / Elskick         u.e.20001.bg/ Patiskick         u.e.20001.bg/ Patiskick <td>1016g         0.4770223.bg/Feldick         0.47101116g/Feldick           1016g/Feldick         0.4721023.bg/Feldick         0.4721031.bg/Feldick           1016g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g         0.4721031.bg/Feldick         0.4721031.bg/Feldick</td> | 1016g         0.4770223.bg/Feldick         0.47101116g/Feldick           1016g/Feldick         0.4721023.bg/Feldick         0.4721031.bg/Feldick           1016g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g/Feldick         0.4721031.bg/Feldick         0.4721031.bg/Feldick           1116g         0.4721031.bg/Feldick         0.4721031.bg/Feldick   |
| # Since<br># Since  | 2016.gr#dkik u.u.2013.kg<br>2016.gr#dkik u.u.2   |
| # #40.000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.0000             # #40.00000             # #40.00000             # #40.00000             # #40.00000             # #40.00000             # #40.00000             # #40.00000             # #40.0000000             # #40.0000000             # #40.000000   | 2110g     U.u.20123Apj/Kelick     U.u.201201Apj/Kelick       2110g/Kelick     U.u.201201Apj/Kelick       2110g     U.u.201201Apj/Kelick   |
| U. C. 1990/Ling         U. C. 1990   | 211.bg/Faller     u.x.21002.bg       211.bg/Faller     u.x.21002.bg       214.bg/Faller     u.x.21002.bg       214.gg/Faller     u.x.21012.bg       214.gg/Faller     u.x.21012.bg       214.gg/Faller     u.x.21012.bg       214.gg/Faller     u.x.21012.bg       214.gg/Faller     u.x.21012.bg <t< td=""></t<>  |
| Bit         Dut         U. (#19021169/3616x         U. (#19021169/3616x<   | 1946.bg        200000 kg Radicak        200000 kg Radicak           1958.gg        200000 kg Radicak        200000 kg Radicak           1958.gg        200000 kg Radicak        200000 kg Radicak           1958.gg        2000000 kg Radicak        200000 kg Radicak           1958.gg        2000000 kg Radicak        2000000 kg Radicak           2016.gg        2000000 kg Radicak        2000000 kg Radicak           2024.gg        2000000 kg Radicak        2000000 kg   |
| u.e.19002.teg         u.e.1900   | 114.16g/Felder       0.47.1002.0g         115.16g       0.47.0022.0g         115.16g       0.47.0022.0g         115.16g       0.47.0022.0g         115.16g       0.47.0022.0g         115.16g       0.47.0022.0g         115.16g       0.47.0022.0g         115.16g       0.47.0025.0g         115.11g       0.47.0025.0g  |
| Adm.dopie         u.e.10001ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c4         u.e.0011ap.2463c4         u.e.00011ap.2463c4         u.e.00011ap.2463c  | 115.4g   |
| u.e.190014pg/stablak         u.e.19001   | Dibig         U.a.21003.tog           Dibig/Fidlack         U.a.21004.tog           Dibig/Fidlack         U.a.2004.tog           Dibig/Fidlack         U.u.2004.tog           Dibig/Fidlack         U.u.2004.tog           Dibig/Fidlack         U.u.2004.tog           Dibig/Fidlack         U.u.2004.tog   |
| Import         e=10004.bg         c=00011.bg         e=00011.bg         e=000011.bg         e=00001.bg         e=00011.bg         e=00011.bg         e=00011.bg         e=00001.bg         e=00011.bg         e=00001.bg         e=000001.bg         e=000001.  | 2146.gb746kdx     1, c_a210503,cp746dbck       2214.gb746kdx     1, c_a210504,cp746dbck       2224.gb746kdx     1, c_a210504,cp746dbck       2224.gb746kdx     1, c_a210504,cp746dbck       2246.gb746kdx     1, c_a210504,cp746dbck       2146.gb746kdx     1, c_a210504,cp746dbck       104.gb746kdx     1, c_a210514,cp746dbck       105.gb746kdx     1, c_a210514,cp746dbck  |
| import         u.e.10003.kg         u.e.20031.kg/4564.kg  | 201-bg   |
| implementation   | 211.bg/Fieldet         u.a.21003.cbg/Fieldet           222.bg/Fieldet         u.a.21003.cbg/Fieldet           222.bg/Fieldet         u.a.21003.cbg/Fieldet           224.bg/Fieldet         u.a.21003.cbg/Fieldet           224.bg/Fieldet         u.a.21003.cbg/Fieldet           224.bg/Fieldet         u.a.21003.cbg/Fieldet           224.bg/Fieldet         u.a.21003.cbg/Fieldet           224.bg/Fieldet         u.a.21003.cbg/Fieldet           214.bg/Fieldet         u.a.21003.cbg/Fieldet           214.bg/Fieldet         u.a.21003.cbg/Fieldet           216.bg/Fieldet         u.a.21013.cbg/Fieldet           216.bg/Fieldet         u.a.21013.cbg/Fieldet           216.bg/Fieldet         u.a.21013.cbg/Fieldet           216.bg/Fieldet         u.a.21013.cbg/Fieldet  |
| Image: State in the s  | 222ag<br>222ag<br>222ag<br>222ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22ag<br>22 |
| Image:         u.e.17022.5g         0.002013 kg/staffald         u.e.10203.5g/staffald         u.e.10203.5g/staffald         u.e.10203.5g/staffald         u.e.10203.5g/staffald         u.e.10215.5g/staffald         u.e.10215.5g/staffal  | 2224g/Feldet         u.w.21093.op/Feldet           224eg/Feldet         u.w.21093.op/Feldet           224eg/Feldet         u.w.21093.op/Feldet           224eg/Feldet         u.w.21093.op/Feldet           214eg/Feldet         u.w.21093.op/Feldet           164g/Feldet         u.w.21093.op/Feldet   |
| image         ext3003.bsp         ext3003.bsp <td< td=""><td>224.6g         L_u.21092.6g           224.6g         L_u.21092.6g           224.6g         L_u.21092.6g           224.6g         L_u.21009.6g           224.6g         L_u.21009.6g           224.6g         L_u.21009.6g           224.6g         L_u.21009.6g           224.6g         L_u.21001.6g           224.6g         L_u.21001.6g</td></td<>  | 224.6g         L_u.21092.6g           224.6g         L_u.21092.6g           224.6g         L_u.21092.6g           224.6g         L_u.21009.6g           224.6g         L_u.21009.6g           224.6g         L_u.21009.6g           224.6g         L_u.21009.6g           224.6g         L_u.21001.6g  |
| iii weekd         U. RT 1903.169         U. RT 1903.1   | 204-gr Findex         u_a21000 a.gr Andraky           2014 gr Findex         u_a21000 a.gr Andraky           2014 gr Findex         u_a21000 a.gr Andraky           105 gr Findex         u_a21010 a.gr Andraky           105 gr Findex         u_a21010 a.gr Andraky           106 gr Findex         u_a21011 a.gr Andraky           107 Jag         u_a21011 a.gr Andraky           107 Jag         u_uz20111 a.gr Andraky   |
| ing         u_en1002.hg         u_en2002.hg/m64.kd   | 171 Mag         III, and 2008 Mag           121 Mag         III, and 2008 Mag           124 Mag         III, and 2008 Mag           124 Mag         IIII, and 2008 Mag           124 Mag         IIII, and 2008 Mag           124 Mag         IIIII, and 2008 Mag           124 Mag         IIIII, and 2008 Mag           124 Mag         IIIIIIIIIII Age/Middled           125 Mag         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII   |
| Image: Solution of   | 171 Mag         III, and 2008 Mag           121 Mag         III, and 2008 Mag           124 Mag         III, and 2008 Mag           124 Mag         IIII, and 2008 Mag           124 Mag         IIII, and 2008 Mag           124 Mag         IIIII, and 2008 Mag           124 Mag         IIIII, and 2008 Mag           124 Mag         IIIIIIIIIII Age/Middled           125 Mag         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII   |
| Princips         U_ext1002.big         U_ext002.big         U_ext0002.big         U_ext0002.big<   | 1211.6g/Ficklet         1_4_2/20100.6g/Ficklet           105.hg        2020101.2g/Ficklet           105.hg        2020101.2g/Ficklet           105.hg        2020101.2g/Ficklet           105.hg        2020101.2g/Ficklet           105.hg        2020101.2g/Ficklet           105.hg        2020101.2g/Ficklet           105.hg/Ficklet        2020101.2g/Ficklet           105.hg/Ficklet        2020101.2g/Ficklet           105.hg/Ficklet        2020101.2g/Ficklet  |
| Program Fer         Uner1002 high         Uner1002 h   | 104.log (u.a.2013b.log<br>Voltog (u.a.2013b.log Fildeke<br>105.log / u.a.2013b.log Fildeke<br>106.log (u.a.2013b.log Fildeke<br>107.log (u.a.2017b.log<br>107.log (u.a.2017b.log<br>u.a.2017b.log Fildeke  |
| Image: Text still         u.e.x10003.big         u.e.x1003.big         u.e.x10003.big         u.e.x1003.big         <  | 165 kg ] u.e.2010 tag pilotag<br>Stongarataka (u.e.art001 tag pilotag<br>166 kg ] u.e.2010 tag pilotag<br>Kitag Jilataka (u.e.2017 tag pilotag<br>167 kg u.e.2017 tag pilotag  |
| Image: State State Strategy         U.v. 19103 hog  | 180 ng/matteria<br>180 ng   |
| Appen Vision Konstein         u.m.19107.hgg         u.m.00027.hgg         u.m.00027.hgg         u.m.00027.hgg         u.m.00027.hgg         u.m.00027.hgg         u.m.10028.hgg  | 166/ig<br>166/ig2011topFileIck<br>167/ig2011topTileIck<br>167/ig2011topTileIck<br>167/ig2011topTileIck   |
| Pres         u.,ex101034/g         UL.9002716/64/84         u.9000016/64/84         UL.9000016/64/84         UL.9000016/84         UL.900  | 108/ing/ie/Sek ( u.e.201072.eg<br>107/eg<br>109/ag/ie/Siek ( ) u.e.201013.bg/ie/Siek   |
| Topic         U_v.nt 111/55.00         U_v.nt 1111/55.00         U_v.nt 111/55.00  | 107 Jug u_ex210315.bg<br>107 Jug FileSlade [] u_ex210315.bg FileSlade  |
| His         U.e. N110556 pileback         U.e. N010566 pileback         U.e. N100566   | 107 Jug FileSlack [] u_ex210315.log.FileSlick  |
| 1         u.e.***********************************  |  |
| u_ex1911725.pg U_ex2002.14g U_ex2001145.pg U_ex2001145.pg U_ex2001145.pg U_ex2001145.pg U_ex2001145.pg U_ex2001145.pg U_ex20021145.pg U_ex20021145.pg U_ex20021145.pg U_ex20021145.pg U_ex20021145.pg U_ex2002145.pg U_e   |  |
| pen numeri u.e.1911-Ling u.e.2005.ing u.e.20   | 100.ling.FileSlack u.e.210154.log  |
| nem u u en 1991 Sug u en 2001 Sug u en 2001 Sug u en 2001 Sug u en 2003  |  |
| e Class u en 1911/25.log u en 2001/15.gc u en 2001/15.gc u en 2011/25.log  |  |
| stine u_extractiongu_extractiongu_extractions_pressure u_extractiong_restraction_u_extractions_restraction_u_ext   |  |
| after a strategy where a strategy where a strategy where   |  |
|  | n13.log.hie5kis u_u_m210531.log  |
|  |  |
|  | 114 Jog FileSlick 1 u. w210432 log FileSlick   |
| te Created u_ex201024.log u_ex200616.logFileStack u_ex200029.logFileStack u_ex200  |  |
| teModified u.ex2011243og3ileStack u.ex206173og u.ex201102.jog u.ex201  |  |
|  | 205.leg.HieSixxL_e210406.bg  |
| morested (   |  |
| u.ex2002243og u.ex2002243og u.ex200  | 200Jog-FelSlark u_w210407.pg   |
| u_ex20526.log u_ex201226.log u_ex201111.log u_ex2010.  |  |
| u_ex200227.Jog u_ex200524.JogFileSlack u_ex201115.logFileSlack u_ex201   | 209 Jog FileSlack u_ek210409 Jog   |
| ujerzniczskieg ujerzniczskieg ujerzniczskieg ujerzniczskieg ujerzniczskieg   |  |
|  |  |
| ptern Fase   | 210.log.5ile5le3u_e210412.bg   |
| 20 10 00 00 00 00 00 00 00 00 00 00 00 00  | 210.log.5ie5kek 🔄 u_e210412.log  |
| 10 10 00 00 01 28 00 00 00 00 00 00 00 00 00 00 00 00 00   | 223 lag FileSteck un a 210412 lag  |

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



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

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

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

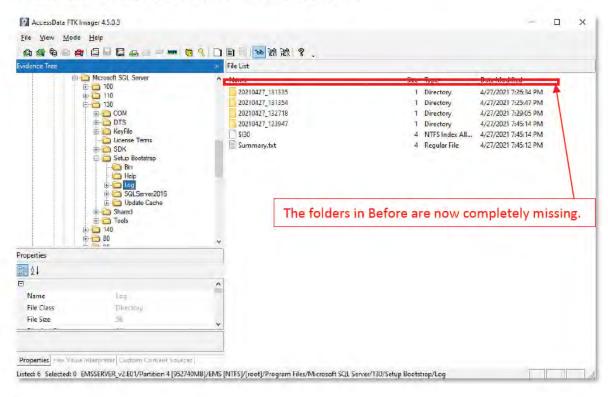
This log data is required to verify that the election system was not accessed by an external, unauthorized device, but due to the specific and unusual installation method for a critical computing system, chosen by Dominion Voting Systems and endorsed by the CO Secretary of State, these critical data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

## Server Microsoft SQL Server Installation Log Files Missing

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

| idence Tree   | File List   |   |  |
|---|---|---|--|
| Morosoft Analysis Services     Morosoft Help Viewer     Morosoft SOL Server     Morosoft SOL Server | <ul> <li>A term</li> <li>20190610_12025T</li> <li>20190610_120209</li> <li>20190610_1358007</li> <li>5100</li> <li>5100</li> <li>Summary.txt</li> </ul> | 1 Directory<br>1 Directory<br>1 Directory<br>4 NTES Index All<br>4 Regular File | D. M. J.C. J<br>6/10/2019 6:50-48 PM<br>6/10/2019 6:15:56 PM<br>6/10/2019 6:55:01 PM<br>6/10/2019 6:55:01 PM<br>6/10/2019 6:54:59 PM |
| perties   | ×   |   |  |
| žţ  |   |   |  |
| Name Log<br>File Class Direcardy<br>File Size 35  | •   |   |  |
| United State St.  | ~   |   |  |

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



**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.

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.

| AccessData FTK Insager 3-1.2.0<br>a View Mode Help   |  |   |  |    |
|--|--|---|--|----|
|  |  |   |  |    |
| > ≤ + + + + + + + + + + + + + + + + + +  |  |   |  |    |
| ience Tree 🔅 🖉   | le List  |   |  |    |
| align     a      | Datatorie LandingPage<br>Summany JMSSERVER 201006<br>Setting: LandingPage.xmFile<br>Setting: LandingPage.thfiRSLek<br>Detail.LandingPage.thfiRSLek<br>Detail.LandingPage.thfiRSLek<br>Stati<br>Vort - 2015-00-10 12:103112 Stpt  |   |  |    |
| Held     Hernet Excitor     How Manual Avalues Servers     Monosof Held Vener     Mono      | <pre>(01) 2019-06-10 12/03/02 51p;<br/>(02) 2019-06-10 12/03/02 51p;<br/>(03) 2019-06-10 12/03/02 51p; Completed Action: ProcessFeatureConfigFileArguments, returned True<br/>(03) 2019-06-10 12/03/02 51p; Completed Action: ProcessFeatureConfigFileArguments<br/>(03) 2019-06-10 12/03/02 51p; Completed Action: ProcessFeatureConfigFileArguments<br/>(03) 2019-06-10 12/03/02 51p; Completed Action: VolidateSetting3AgainstScenario<br/>(04) 2019-06-10 12/03/02 51p; Completed Action: VolidateSetting3AgainstScenario<br/>(05) 2019-06-10 12/03/02 51p; Completed Action: FinalCalculateSetting3AgainstScenario<br/>(05) 2019-06-10 12/03/02 51p; Completed Action: FinalCalculateSettingsAgainstScenario, returned True<br/>(05) 2019-06-10 12/03/02 51p; Completed Action: FinalCalculateSettingsAgainstScenario, returned True<br/>(05) 2019-06-10 12/03/02 51p; Completed Action: FinalCalculateSettingsAgainstScenario, returned True<br/>(02) 2019-06-10 12/03/02 51p; Completed Action: FinalCalculateSettings, returned True<br/>(02) 2019-06-10 12/03/02 51p; Completed Action: FinalCalculateSettings, returned True<br/>(03) 2019-06-10 12/03/02 51p; Completed Action: KxequteSectingsAfile=ExX:=nsionsLoaded, returned True<br/>(03) 2019-06-10 12/03/02 51p; Completed Action: KxequteSectingsAfile=ExX:=nsionsLoaded, returned True<br/>(03) 2019-06-10 12/03/02 51p; Completed Action: LoadingFage<br/>(04) 2019-06-10 12/03/02 51p; Loading page action<br/>(05) 2019-06-10 12/03/03 51p; Completed Action: LoadingFage, returned True<br/>(05) 2019-06-10 12/03/03 51p; Completed Action<br/>(05) 2019-06-10 12/03/04 51p;<br/>(05) 2019-06-10 12/05/04 51p;<br/>(05) 2019-06-</pre> |   |  |    |
|  | (01) 2019-06-10 12:50:40 Slp: Sco: Attempting to open registry subkey SOFTWARE/Microsoft/SCMClient   |   |  |    |
| tom Content Sources  | (01) 2019-06-10 12:50:40 Slp: Sco: Attempting to get registry value MachineId  |   |  |    |
| dence: i le System (Fath (File Options -   | (01) 2019-06-10 11:50:10 S1p: Soc: Attempting to create base registry key HKEY LOCAL MOCHINE, machine<br>(01) 2019-06-10 11:50:10 S1p: Soc: Attempting to open registry subrey Software/Microsoft/Hicrosoft SQL Server/100<br>(01) 2019-06-10 11:50:10 S1p: Soc: Attempting to get registry value CarcomerTeedBack<br>(01) 2019-06-10 12:50:10 S1p: Soc: Attempting to get registry value EncoleFroeRecorting  |   |  |    |
| Lot. Remove Remove BI Licenstinace   | (01) 2019-06-10 12:50:40 Slp: SetupTelemetry: Telemetry has an active session with 2 events.   |   |  |    |
| outles Hen Value Investment Custom Content Sources   | *  |   |  | 2  |
| I have not a second sec | am Fies/Microsoft SOL Servier/130/Setup Bootstrap/Log/2019)610_120251/Detail LandnsPape.txt  |   | NU                                       | 0. |
| activenesities and a faster supplies for usall from hereb  |  |   | 1- | m  |
| C Type here to search  | O LH 🚨 💁 🔍 🚾 🐂 💶 🤐 🖉   | ~ | 12:07 4M<br>Freday<br>9/10/2021          | 5  |

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

# Server Microsoft SQL Server Log Files Missing

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

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

| ccessData Fik Image   |  |   |                   |  |  |
|-----------------------|--|---|-------------------|--|--|
| Jam Work Re           |  |   |                   |  |  |
| 6 % - 6 G             | 3 V C 🚓 🖛 🔞 🤋  |   |                   |  |  |
| nce Tree              |  | r Me List   |                   |  |  |
| 001                   | Acrosoft Asalysis Services   | * Name  | Size Type         | Date Modified  |  |
|                       | Manasaft Help Verwer   |   | 11.               |  |  |
|                       | Manual SOL Gener   | EFRORLOG  | 10 HIPS TODER HIT | 3/23/2421 3/2/133 Pm   |  |
|                       | 100  |   | 112 Regular File  | 5/23/2021-600:17 AM  |  |
| 34                    | 011  | ERRORLOG.1  | 52 Repular File   | 3/30/2021 52542 PM   |  |
|                       | 130  | ERROR_06.2  | 64 Regular File   | 3/30/2021 L19/01 PM  |  |
|                       | 3.80   | ERROR OG.2.FieSlack   | 1 FileSlack       | 100 ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (  |  |
|                       | 90   | ERRORLOG.3  | 62 Repulse Frie   | 3/18/2021 #56:43 PM  |  |
|                       | Client SDK   | ERRORLOG.3.FileSlack  | 3 File Slack      | and the second se  |  |
|                       | MSRS13 MSSQLSERVER   | ERRORLOG.4  | 289 Regular File  | 3/18/2021 4:51:53 PM   |  |
| 14 C                  | MSSQL13 MSSQLSERVER  | EFRON OGAFieSlack   | 4 File Sleck      |  |  |
| - 7                   | MSSQL  | EFRORIOG.5  | 132. Regular File | 1/5/2021 (1:40:53 PM   |  |
|                       | Backup   | CEROILOG.S.FieSlack   | 1 File Slack      |  |  |
|                       | E DATA   | ERRORLOG &  | 39 Regular File   | 1/5/2021 15:37/07 PM   |  |
|                       | inda hata  | K ERRORLOG 6  | 19 Regular File   | 6/11/2019 4:37:35 PM   |  |
|                       | 3083   | K ERNORLOS.6  | 18 Kezular File   | 8/23/2019 1:18:04 PM   |  |
|                       | Log  | K EROLOGA   | 18 Regular File   | 6/12/2010-324-42 PM  |  |
|                       | Horosoft Vaual Study 10.0  | K ERROR OGS   | 18 Regular File   | 6/11/2019 1:56-46 PM   |  |
|                       | Norosoft, NET  | K EFROILOGS   | 18 Regular File   | 6/10/2019 8:54:51 PM   |  |
| 10 Ga 5               |  | K ERROR OG.6  | 20 Regular File   | 6/25/2019 3/42 11 PM   |  |
| 80                    | Reference Assemblies   |   |                   |  |  |
|                       | Innatal Information<br>Mindows Defender  | KI ERROALOGA  | 24 Regular File   | 6/26/2019 9:43:15 PM   |  |
|                       | Nedova Nal   | K EPROPLOG.6  | 47 Regular File   | 6/25/2019 0.14/28 PM   |  |
|                       | Andows Nedia Player  | K) EEROLDG &  | 17 ReputerFile    | 9.4/2019 8.17:57 PKA   |  |
|                       | Windows Multimedia Natiom  | K) ERRORLOG.6   | 50 Regular File   | 9/3/2019 634:40 PM   |  |
|                       | Windows NT   | ERRORLOG/LFieSlack  | 2 File Slack      |  |  |
|                       | Windows Photo Viewer   | EKROFLOG Friedack   | 17 File Slack     | the state of the second s |  |
|                       | Mindows Pottable Devices   | K HkEngineEventfile_0_131046664709830000.xet  | 68 Regular File.  | 6/10/2019 6:54:47 PM   |  |
|                       | Nindows Server<br>Nindows Sdebar   | K Hklinginal/ventlite_0_113046864914560000.ver  | 60 Regular File   | 6/10/2010 NOG-38 PM  |  |
|                       | undows police.   | K HkEngineEvent/ide_0_132046675163990000.xel  | 69 Regular File   | 6/10/2019 1/29/17 PM   |  |
| bes                   |  | K HkEngineEventFile_0_132046687325650000.xel  | 69 Regular File.  | 6/10/2019 135:14 PM  |  |
| 1                     |  | K HkEngineEventFile_0_132046697802720000ukl   | 69 Regular File   | 6/10/2019 8:00:03 PM   |  |
|                       |  | K HkEngineEventfile_0_13/046704106230000.vef  | 59 Regular File   | 6/10/2019 &01/07 PM  |  |
|                       |  | HitergineEventfile_0_133046706065430000+al  | 60 Reputer File   | 6/10/2010 A 25-16 PM   |  |
| inne                  | Log  | K) HkEngineEventFile_0_13096720404950000.rel  | 69 Regular File   | 6/10/2019 847;39 PM  |  |
| e Class               | (Second Second S | K HkEngineEventfile () 132046733900110000.ref   | 69 Repulse File   | 6/10/2019 254:51 PM  |  |
| e Size                | -  | K) HkEngineEventFile 0, 13(0474151/3380000.ref  | 69 Regular File   | 6/11/2019 3:56:46 PM   |  |
| ysical Size           |  | K HkEngineEventFile 0, 13/0474233(9920000.ref   | 69 Regular File   | 6/11/2019 4:37:35 PM   |  |
| te Accessed           | and the second s | K) H&EngineEventFile_0_132040477215610000.ref   | 60 Regular File   | 6/12/2019 9/24/42 PM   |  |
| ste Created           |  | K) H&EngineEventhile_0_112059551715410000.ad.   | 69 Regular File   | 6/3/2019 #36/25 PM   |  |
|                       |  | K HkEngineEventhile 0 132059555238010000.rd   | 69 Regular File   | 6/23/2019 (18:04 PM  |  |
| ate Modified          | in the local state of the state | K) HkEngineEventFile_0_13205955228010000448   | 69 Regular File   | 6/25/2019 818204 PM  |  |
| repted                | - Lines  |   |                   |  |  |
| ompressed             | Tolog  | K HkEngineEventFile_0_130099672724750000uel   | 69 Regular File   | 6/25/2019 8:42:11 PM   |  |
| tual File             | (Name)   | K] H&EngineEventFile_0_12059690813590000.rel  | 69 Regular File   | 6/26/2019 8:43 15 PM   |  |
| ternate Data Stream ( | Court  | K Hkänginefventille_0_132060595517260000.ref  | 69 Regular File   | 6/26/2019 R56/32 PM  |  |
| 25 Attributes         |  | K HkEngineEvent/ile_0_132060600440540000uel   | 69 Regular File   | 9/3/2019 624-a0 PM   |  |
| idden                 |  | K] HkEngineEventFile_0_132120087613370000.xel   | 69 Regular File   | 9/4/2019 837:57 9%   |  |
|                       | hing.  | Tint  |                   | a labolation of the state  |  |
| nteri                 | - Final-   | 000 30 00 00 00 00 00 00 00 00 00 00 00   |                   |  |  |
|                       |  | 010 10 00 00 10 18 01 00 00-00 10 00 00 01 00 00 00 00 00   |                   |  |  |
|                       |  | 020 B4 25 00 00 00 00 10 05-76 00 58 00 01 00 00 00 8   | x Z               |  |  |
| erties Her fulligrene | centre Contine Commit Source   | Cursor pos = 0  |                   |  |  |
|                       |  | The second se |                   |  |  |

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

| See de Bauer e S              |  |                                    |  |  |
|-------------------------------|--|------------------------------------|--|--|
| Norosoft Avalyse Services     | Ale List   |                                    | Date Modified  |  |
| Si Co Norosoft Hilp Viewer    | n Name   | Size Type                          | Liste Modified   |  |
| 🗐 😋 Marplott SQL Server       | EXXORCOD   | 18 Kegulai Por                     | SIZE/ZOZI EXHIUT PM  |  |
| ÷ 110                         | TERIOR OG 1  | 72 Regular File                    | 5/26/2021 049-51 PM  |  |
| 8 🔄 130                       | TERRORIOG2   | 20 Regular File                    | 5/25/2021 h/27/30 PM   |  |
| iii 🛄 140                     | ERRORLOG.3   | t8 Regular File                    | 5/25/2021 8:26:49 PM   |  |
| + - 40                        | ERRORLOG.3.FileSlack   | 3 File Slack                       | 100 C 100  |  |
| ili 🔛 Clere SDK               | TERRÓRLOG.4  | 18 Reputer File                    | 5/25/2021 6-14-16 FM   |  |
| MSRS13 MSSQLSERVER            | CRROILOGA Fieslack   | 3 File Slack                       | and a stand of the   |  |
| MSSQL33.MSSQLSERVER           | ERRDRLOG 3   | 13 Regular File                    | 5/25/2021 6:03:05 PM   |  |
| Backup                        | ERRORLOG 5.FileStack   | 3 File Slack                       | AND DESCRIPTION OF A DE |  |
| a 📥 Deve                      | ERRONLOGA  | 21 Regular File<br>30 Regular File | 4/29/2021 7:24:47 PM<br>4/29/2021 3:29:10 PM   | File sizes are different file dates are  |
| DATA.                         | ERROR OG & Fieldack  | 4 File Slack                       | ACCOUNT #29:10 DO  | File sizes are different, file dates are |
| 2801                          | ERRORLOG FileSack  | 15 File Slack                      |  |  |
|                               | HkEngneEventfile U 1326426278990000xel   | 19 Reputer File                    | #/27/2021 1344:56 PM   | different. Original files have been      |
| Morceoft Visual Studie 10.0   | HitEngineEventfile 0, 132640262718990000.vel.FileSlick   | 4 File Slack                       | STRUCTURE CONTRACTOR   | different, original files have been      |
| Horosoft NET                  | HkEngineEventfile 0 112640261049570000.vet   | 69 Reputer File                    | #27/2021 1:57/01 PM  |  |
| Peference kasembles           | HkEngneEventFile_0_132640263049570000.xet.FileSlack  | .4 File Stack                      |  | replaced with new. Previously 116 files, |
| Chanatal Information          | HkEngineEventFile_0_132640271414290000.xel   | 69 Regular File                    | 4/27/2021 8:18:19 PM   |  |
| 🗟 🔛 Windexes Dafander         | HkEngineEventFile_0_132640271414290000.xet.FileSlack   | of The Stack                       | A CONTRACT OF  | now only 71 files.                       |
| a C Windows Nat               | Hkdingineliventile_0_132640283058110000.ver  | 69 Regular File                    | 4/27/2021 b10-44 PM  | now only 71 mes.                         |
| Stinding Millimolds Rollom    | HkEngineEventHite_0_132640283058110000.vel/HeShick   | 4 File Stack                       | and and a strength   |  |
| 🕸 😂 Windows NT                | HkEngineEventFile_0_132640284500100000.xel   | 60 Regular File                    | 4/27/2021 8:28:40 PM   |  |
| Windows Ploto Varies          | H&EngineEventFile_0_132540284500100000.xelFileSlack  | 4 File Slack<br>60 Ringular File   | 4/27/2021 10:46:27 144   |  |
| (i) Windows Server            | Hitergreet ventrice_0_132640290475680000.vel.hteSlack  | 4 Sie Slack                        | 4/27/202110/49/27114   |  |
| 1 - O Windows Sdebar          | HitmaineEventille 0.132641143400590000.rel   | 69 Regular File                    | 4/28/2021 9:48:53 PM   |  |
| e                             | HkErigineEventFile_0_132641143400590000.vel.FileSluck  | 4 File Stack                       |  |  |
|                               | HitEngneEventFile 0, 132641837510080000+el   | 09 Reputer File                    | 4/29/2021 3/29/11 PM   |  |
|                               | Hild opined ventilite_0_112641237510053000 vel FileSlack   | 4 Bie Stack                        | a sector and a sector and  |  |
|                               | HkEngineEventlide_0_132641838755850000.xef   | 69 Regular File                    | 4/29/2021 to08:43 PM   |  |
| terre transmission            | HkEngineEventFile_0_132641838713850000.net FileStack   | 4 File Stack                       | and an and a   |  |
|                               | Hktngnetventrile_0_152041956409950000.es   | CO Fegular File                    | A/29/20217:14:45 PM  |  |
|                               | HkEngineEventFile_0_132641934419950000uel.FileSlack  | 4 File Slack                       |  |  |
| Accessed Botcom (Mail/194     | HkEngineEventfile_0_132641974049000000.vef<br>HkEngineEventfile_0_132641974049000000.vel.FiteSlack   | 69 Rigular File<br>4 File Slack    | 4/29/2021 7:24:47 PM   |  |
|                               | HkEngineEventFile_0_1325479740400000.xel   | 69 Regular File                    | 5/25/2021 5/03/05 PM   |  |
| Created Hit Council Advict Ma | HkEngineEventhie_0_1326439520416000034   | 09 Regular File                    | 5/23/2021 6:14 16 PM   |  |
|                               | HkEngineEventFile_0_112664195230450000.xel.FileElack   | 4 File Slack                       | - Stankt Litz (Bird)   |  |
| igted Fain                    | HkEngineEventFile 0 132664402014470000.xet   | 69 Regular File                    | 5/25/2521 0:26/49 PM   |  |
| pressed in-                   | HkEngineEventFile_0_132664402014470000.xel FileSlack   | 4 File Slack                       |  |  |
| ul File                       | HkEngineEventfile_0_132654480136440000.vel   | 69 Regular File                    | 5/25/2021 8:27:30 PM   |  |
| nate Data Stream Count        | HEEngineEcentrile, 0, 133664400118440000.vel FileSteek   | 4 File Shack                       | and the second second  |  |
| Attributes                    | HkEngineEventFile_0_133664481965020000.xer   | 69 Regular File                    | 5/26/2021 Ib49:51 PM   |  |
| ten Iv-                       |  | A States                           |  |  |
| in Ear                        | 100 30 50 50 00 00 01 00 00 00-10 10 00 00 00 00<br>100 10 20 50 50 50 01 00 00-50 01 00 00 00 00<br>100 20 20 20 00 00 00 00 00 00 00 00 00 0 | 00 ···· P···· P····                |  |  |

### EMS Server Dell Server Updates Missing

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

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

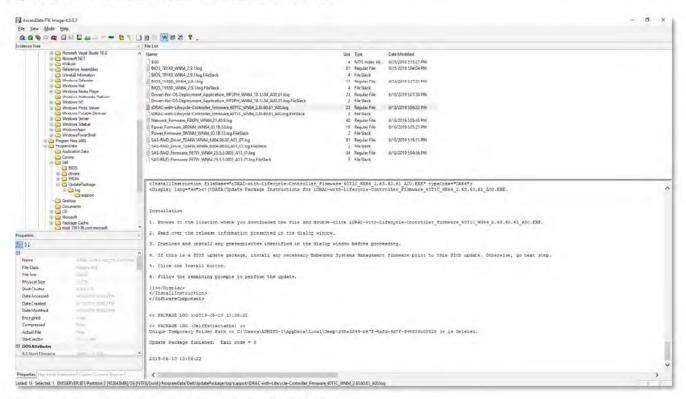


Figure 16 - EMS Server (5.13) Dell Server Update Files After

|   | nlo                             |  |                       |                        |   |
|---|---------------------------------|--|-----------------------|------------------------|---|
|   |                                 | 0 m  |                       |                        |   |
| Sence Tree  |                                 | · Nets   |                       |                        |   |
|   | Vindows Multimedia Platform     | ^ Name   | Size Type             | Date Nodified          |   |
| IN CON  | Vindows NT                      |  |                       |                        |   |
|   | Undowe Posts Varuer             | 1895   |                       | 5/25/2121 6:10:11 PM   |   |
|   | Whitewas Portable Devices       | BI01_9FG65_NN64_2.12.1_01.log  | 17 RegularFile        | 4/27/2821 5:03:40 PM   |   |
|   | Vindows Server                  | BIO1_H5DVH_WN64_212.1.log  | 14 RegularFile        | 3/25/2021 6:06:56 PM   |   |
|   | Vindows Edicbar<br>Vindows/laps | DIDS_HISDVH_WHISH_212.1Ling/TileSlack  | 3 File Sleck          |                        |   |
|   | Vindows/ower/Shell              | Chipset_Driver_4576M_WW64_10.1-18243.8188_445_02.log   | 339 RegularFile       | 4/29/2021 7-22-04 PM   |   |
| HI CO Progra  | win Their (190)                 | Chipset_Driver_45TGM_WN64_10.1.18243.8188_A/5_02.logFileSlack  | 2 File Slack          | and an and the second  |   |
| 🖯 🛄 Proga   |                                 | IDRAC-with-Lifecycle-Controller_Firmware_DPVIR_WN64,2.75.100.75_A00.log  | 33 RegularFile        | 5/25/2021 6/08/19 PM   | Sizes, Dates/Times are different.   |
|   | polication Data                 | DRAC-with-Lifecycle-Controller_Firmware_DPVIR_WN64_2.75.10075_A00.log.FileSlack  | 4 File Slack          |                        | oneos, bacco, nines are anterent  |
|   |                                 | Network_Dimer_284/6_W1464_20.0.0_400.log   | 75 RegularFile        | 5/25/2321 6/09/36 PM   | and the second se   |
|   | diven.                          | Network, Driver, 28416, WN64, 20.0.0, A0Ulog, FileStack  | 2 File Slack          |                        | These Log Files have been   |
|   | Farmure                         | Network_Driver_49X84_WN64_21.80.3_218.0.169.2_01.log   | 51 RegularFile        | 4/27/2021 5:03:17 PM   | the set of |
| WC  | Updati/Package                  | Network_Driver_49x34_WN64_31.80.3_218.0.169.2_01.log_FileSlack   | 2 File Steck          |                        | 1 1 11 110 1100 1101  |
|   | i 📥 100                         | Network, Firmware, 23WP1_WN64, 20.0.16, 400.log  | 49 RegularTile        | 5/25/2121 & 10:15 PM   | replaced with different files.  |
|   | 😂 aupport                       | Network_Firmware_70MIN_WIN64_21.60.16.log  | 43 Regularfile        | 4/27/2821 SIDE IS PM   | the second s  |
|   | Nesktop<br>Nocuments            | Network_Firmware_7CM1N_WN64_21.60.16.log_FileStack   | 2 File Slack          |                        |   |
|   |                                 | Power Fermulare SR08M, WN64.00.18.13.log   | 748 RegularFile       | 4/27/2121 5:06/6 PM    |   |
| 10 0 1  |                                 | Power_Firmware_P0F3V_WN64,00.18.83/log   | 263 RegularFile       | 5/25/2021 6:10:46 PM   |   |
| # 😂 h   | ackage Cache                    | Power_Firmware_P0F3V_WIN64.00.18.83/log_FileSack   | 2 File Stack          |                        |   |
|   | ngid 1991-OS.com microsoft      | SAS-RAID_Diver_T244W_W145i;6.604.0b.00_AU1;07.Jog  | 20 RegularFile        | \$/25/2016-11:19 PM    |   |
|   | oftwareDatribution<br>but Meru  | SAS-RAID_Dever_T244W_WN64_6.604.06.00_AD1_07.log_FieSlack  | 3 File Slack          |                        |   |
|   | emplates                        | SAS-RAID_Firmware_WRFIV_WN64_25.5.8.0001_A16.log   | 67 RegularFile        | 5/25/2121 6:12-17 094  |   |
| B-C3 (  | ISOPhrumi                       | SAS-RAID_Firmware_WRF3Y_WN64_25.58.0001_A16.log_FireStack  | Z File Stack          |                        |   |
|   | ISO Shand                       |  |                       |                        |   |
| III Ca Recti  |                                 | <ol> <li>follow the remaining prompts to perform the update.]]&gt;</li> </ol>  | ets                   |                        |   |
| System<br>Users   | in Volume Information           |  |                       |                        |   |
| (i) 🖸 Vitus   | Deectores                       | <pre><display lang="en"><!-- (CDATA)Sixes:</pre--></display></pre>   |                       |                        |   |
| serties   |                                 | - Fixed at issue that caused sluggish iDRAC VI performance while   |                       |                        |   |
| 21  |                                 | - Fixed at issue where UEF310060 and PGR1006 messages are logged   | intermittently durin  | d post repoors.        |   |
| 24  |                                 | Enhancemeste:  |                       |                        |   |
|   |                                 | A - N/Ajj>c/Display>   |                       |                        |   |
| Larre   | address and printing to Santan  |  |                       |                        |   |
| He Class  | magnitur fing-                  | <pre><importantinfs 10="" driv<br="" en="" home="" support="" url#*http:="" us="" www.com=""><display labg="en"><!--!CDATAINA!!--></display></importantinfs></pre>   | ers/DriversDecalls7dr | iverId=DPVOR=>         |   |
| lie Sze   | 10 8180                         | <td></td> <td></td> <td></td>  |                       |                        |   |
| Physical Size   | 17 MA                           | <criticality value="1"></criticality>  |                       |                        |   |
| Rest Chester  | in har                          | <display lang="en"><!-- [CDATA[Recommended=The service provider</td--><td>recommends applying</td><td>this undate during you</td><td>ir next scheduled update cycle. The update contains feature enhancements or chan</td></display> | recommends applying   | this undate during you | ir next scheduled update cycle. The update contains feature enhancements or chan  |
| late Accessed   | A Private Private Quarter       | c/Criticality>   |                       |                        |   |
|   | And American Containing         |  |                       |                        |   |
|   |                                 |  |                       |                        |   |
| Inte Created  | V: toolt maynet                 | << PACKAGE LOG >>2021-05=25 12:05:16   |                       |                        |   |
| ateModified   | Andre,                          |  |                       |                        |   |
| ste Modified<br>norypted  | Talka.                          | << FACKAGE LOG (SelfExtractable) >>  |                       |                        |   |
| øte Modified<br>ncrypted<br>ompressed   |                                 | Unique Temporary Folder Path <c c:\use:s\emsadmin\appdata\local\<="" td=""><td>Temp/34e315Da-9121-40</td><td>08-bf7a-ea0915458183 &gt;</td><td>&gt; is Deleted.</td></c>   | Temp/34e315Da-9121-40 | 08-bf7a-ea0915458183 > | > is Deleted.   |
| ste Modified<br>httppted<br>ompressed   | 1.4                             | londer there country as the lost   |                       |                        |   |
| ateModified<br>ncrypted<br>ompressed<br>ctual File  |                                 |  |                       |                        |   |
| ateModified<br>norppted<br>iompressed<br>ictual File<br>tart Sector   | 104                             | Update Paskage finished. Exit code = 1   |                       |                        |   |
| ateModifier<br>ncrypted<br>ompressed<br>ctual file<br>tart Sector<br>IOS Attributes                                   | 104                             | Update Parkage finished. Exit code = 1   |                       |                        |   |
| ete Modifiei<br>norypted<br>ompressed<br>ctual file<br>tart Sector<br>OS Attributes                                   | 104                             | Update Parkage finished. Exit code = 5<br>2021-05-21 12:00:15  |                       |                        |   |
| Nate Modified<br>norppted<br>compressed<br>cottual filie<br>cart Sector<br><b>XOS Attributes</b><br>A Struct Filenome | 104                             | ~  |                       |                        |   |

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 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.

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

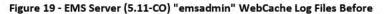


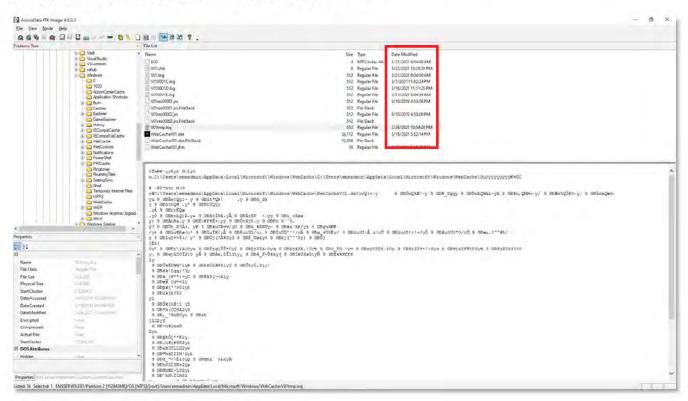
| file Siew Mode B                       | 5elp                     |  |   |
|--|--------------------------|--|---|
| 0000                                   | 000 a 8 1                | 1 61 163 28 28 9   |   |
| idence Tree                            |                          | Field  |   |
|  |                          | A Name Size Type   | DateModified  |
|  | III C PlayReady          | D \$20 4 NTFS index  |   |
|  | H Co Wedners             | V01zhk I Regula File   | 6/17/2020 14:51:53 AM   |
|  | D Windows                | V01.log 512 Kegular File   | 6/17/2020 7-2020 PM   |
|  | 1033                     | K voltoooc.tog Dia Regular File  | 0/10/2019 4:51/20 PM  |
|  | ActionCense/Cache        | V01000A.log 512 Regular File   | 5/22/2020 12-13-13 AM   |
|  | Final AppCache           | Vo10008.log 512 Regular File   | 5/33/2020 12-42-14 4AM  |
|  | in the further shortends | V01000C.log 512 Regular File   | 6/9/2020 12:51:35 AM  |
|  | Gaches                   | V01Hs00001/js 512 Regular File   | 6/10/2019 45610 PM  |
|  | (i) 😋 Suphaw             | V01es00001,es.FileSlack 512 File Slack 512   | 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2   |
|  | E-CameExplorer           | V01es00002,rs 512 Regular File   | 6/10/2019-4:56:10 PM  |
|  | ECorpatieche             | V01es00002,es.FileStack 512 FileStack 512  |   |
|  | (i) 🙆 ECompatilaCache    | V01tmp.log 512 Regular File  | 5/18/2020 10.21:12 PM   |
|  | EDownloadPlatory         | WebCacheV01.dat 26,112 Regular File  | 6/17/080 74600 PM   |
|  | ili Ca NetCache          | WebCacheVOLdat.Fildlack 12,236 File Slack  |   |
|  | H- Votifications         | WebCacheVOL/Im 16 Regular File   |   |
|  | W Carrificache           |  |   |
|  | C Ringtones              | and and and a start and a star       |   |
|  | Roaming Tales            | E as the second s  |   |
|  | - Ded                    | w xC:\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\C:\Users\Administ   | rator/AppData/Local/Microsoft/Windows/WebCashe/Buy9999999991%141018 V('h)%ek1   |
|  | Temporan internet files. | Surger (Manual Administration) 2pp2 ata (Local Minstor ft (Singleys) MatCashe (MatCashe (MatCash       | igbaba av marbinisteren-ujab, num yvyvyvyvyvyvataes.es.is Bistelt. Bus ,me  |
|  | UPPS                     | 9999999999999999Åfr.nlepall *F(6(`)C[' № 6be(€ ~ '*G(E)'É(4F€,-  |   |
|  | WebCache                 | -yyiyyyyyyyyyyial.nngc_d(H(A#21)   |   |
|  | B MnX                    | A.b.#[#1 1 #RIT(12](22#*-*14k.mem 2009000000000000000000.yahon.seawok.no   |   |
|  | E 🎦 Windows Schebar      | 99979999999999994ar.com.nodari TIB UŽA[* ÅgX*,be(E% *U[S{*Å[4JE[<br>%999999999999999999999994ar.nosi I(V( 1]* ¥  | spisze+ JAJAAMAAAAAAAAaa visigi   |
|  | Windows/ept              | 20b4(#A 6 , *[(Y), 46(4WA-A(4b, 461))))))))))))))))))))))))))))))))))))  | as' Vitabee( o a *) ((saa)asex-1(abe  |
|  | 🗉 🖾 Microsof Corporation |  | A(eb,600299999999999999992Ade,noez '[T(1PG]' 00066,be(KA H F *a[[P()(1FCA-A(eb,oS 979   |
| perties                                |                          | <pre>&gt; \GPE5-f(eb,990+9999999999999999994Ase.mojestorget )(hift)' = df99,be(ef<br/>9999999999994Ase.mole )s(1(=0)' = saleberet = "g(s(*0)ase1=""""""""""""""""""""""""""""""""""""</pre>  | <pre>g *k[i(c-\s362-2[ebs*3s3 y99999999999999996arg.nolaviz ]1(*(GY\* 'i)*sbe(02 *m(ki'<br/>g *k[i(c-\s362-2[ebs*3s3 y99999999999999996arg.nolaviz ]1(*(GY\* 's10))</pre> |
| 21                                     |                          | yyyyyyyyyyyydwork.noise ppiirw0," wddobefei ""g(p["0,4361-<br>4:9999999999999994de.nomorebytes ix(p[0-\" "4  | <pre>[eb_iegts33333333333333333333334ro'uomedbrolecc 1(1(#)/, eqei'pelet # _aidi#1/#AAEl-1[ep'up</pre>  |
|  |                          | a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy))))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy)))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy)))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy)))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy))))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy))))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy)))))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy)))))))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy)))))))))))))<br>a stbills & a "y(w(a4-\cLES-S(eb5g=e yppy))))))))))))))))))))))))))))))))))  | Argebe(ES a 1 *//y/i5iic1e0-0/eb611*B pppppppppppppppppppppbet.socb-box ////1*3/*   |
| Name                                   | attempter                | 33333333333333333334amu.mushunhum1/10A7/. B5(Shm(60 u -1)175/6B60-0[   | theilingyyyyyyyyyyyyyyhah.mous 6111'1'' İnsae(60 ~1(8-\4060-0(86.4e2 y)yyyyyyyyyyhde.m  |
| He Gass                                | Annual trans             | 99999999999999999999999999999999999999   | <pre>lebssAssyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy</pre>  |
| Tile Sze                               | and store                |  | 2[6532(4)999999999999999999999999999999999999   |
| Physical Size                          |                          | 9991999999999994com.noracoant (#10,4\" "ay1,be(te # "@(\$11\sN6e-e)  |   |
| tart Cluster                           | Contraction .            | 00000000000000000000000000000000000000   |   |
|  |                          | yyyyyyyyyyyydaam.navelfeed -(8: L*)* 661,be(68 Lf *(*(8)Q>000  | xY MnN+\LHKe-e(en,zx  |
| Nate Accessed                          | The father of American   |  | <pre>(e880f16 gggggggggggggggggggggggggggggggggggg</pre>  |
| Nate Created                           | # 10.0019 #HE.10.0041    | 1.* 08*806(00  *)(%(*))D00-6(000089979999999999999999999999999999999   | A( (_**)' *sequee(co **) pypypypypypypypiorg.nippool A(-(12)'   |
| late Modified                          | 2.1av260010011.1.1 ext-  | 999199999999994se.nukenet A(*)m X/* 1*486be(60 **A(A) ZA(10E+  | (ep.0A'93999999999999292001.null %(A(.sC/*AF'pe(cAC'y(.(E/:tec-e(ep)b .35)  |
| ncripted                               | Tring-                   | 99999999999999999999990m.nuvini *9(0(,0)" DV08be(# 0 8 *2(0(020)/s96-  | <pre>(#FEAKT 553353353353353353545454 #(0:02+), FEADPELE &lt; D #F15(DD2)FEE-16D'#32</pre>  |
| ompressed                              | Talat                    | 99999999999999999999999999999999999999   | Ebe(E ' h %4(8(h))48E-[eb8*40=999999999999999994dk.nwwd )et*(h4)' 404*8be(E 1   |
| ctual File                             | 73.00                    | 22239299999999999999999999999999999999   |   |
|  |                          | 1034 - (6p0(02 3333333333333333350cm'ulaurec .e(0(6), Os(upe(4   | _ 02. "e(e(02n)42"C   |
|  |                          |  |   |
|  | 1000                     | <pre>public control co</pre> | (10*,be(c a = ~1(1(*o)\$554 - (cb8\$52  |
| tart Sector<br>XOS Attributes<br>Edden |                          | wine mists - tenters Allallallalaugerminityed Tiot ol.   | restructs =   |
| OS Attributes                          |                          | 99999999999999999998k.co.svip 8(1(#1)' >25656(@ * "A(1(*D)4D@  |   |
| OS Attributes                          |                          | AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA   |   |

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

| le Liew Mode   | Selp   |  |   |  |  |
|--|--|--|---|--|--|
| 0.00   | 3484   | 1 10 14 10 10 10   |   |  |  |
| Annes Tree   |  | File list  |   |  |  |
|  | Profilescontention     Profilescontentio  | Part H           A Marte           and           101,6h           101,6h           10100016g           101000016g           101000016g | Site Type<br>4 VTTS tolex.01<br>8 regular File<br>512 Regular File<br>513 Regular File<br>514 Regular File<br>515 Regular File<br>515 Regular File<br>516 Regular File<br>517 Regular File<br>518 Regular File<br>518 Regular File<br>519 Regular File<br>519 Regular File<br>510 Regular File<br>510 Regular File<br>511 Regular File<br>512 Regular File<br>513 Regular File<br>513 Regular File<br>514 Regular File<br>515 Regular File<br>515 Regular File<br>515 Regular File<br>516 Regular File<br>517 Regular File<br>518 Regular File<br>519 Regular File<br>510 Regular File<br>510 Regular File<br>511 Regular File<br>512 Regular File<br>513 Regular File<br>514 Regular File<br>514 Regular File<br>515 Regular File<br>515 Regular File<br>515 Regular File<br>516 Regular File<br>517 Regular File<br>518 Regular File<br>518 Regular File<br>519 Regular File<br>519 Regular File<br>510 Regular File<br>510 Regular File<br>511 Regular File<br>512 Regular File<br>513 Regular File<br>514 Regular File<br>514 Regular File<br>515 Regular File<br>516 Regular File<br>517 Regular File<br>518 Regular File<br>519 Regular File<br>519 Regular File<br>510 Regular File<br>510 Regular File<br>510 Regular File<br>510 Regular File<br>511 Regular File<br>512 Regular File<br>513 Regular File<br>514 Regular File<br>514 Regular File<br>515 Regular File<br>516 Regular File<br>517 Regular File<br>518 Regular File<br>518 Regular File<br>519 Regular File<br>519 Regular File<br>510 | Defe Modified<br>4/27/2007 6:10-04 PM<br>4/27/2007 6:10-04 PM<br>4/27/2007 6:10-04 PM<br>4/27/2007 6:10-05 PM<br>4/27/20 | All the Before files have been<br>replaced with new files,<br>replacing the originals and<br>therefore making it impossible<br>or nearly impossible to recover.        |
| perties  |  | 2 voltmp.log   | 512 Regular File  | 4/27/2021 6:10:05 PM   |  |
| §1<br>Narr#<br>File Class<br>File Size   | ed torgang<br>Nagatar Kas<br>Kasata  | WebCacheV01.da     WebCacheV01.da     WebCacheV01.da     WebCacheV01.da     WebCacheV01.jm      EL = #E  | 20,112 Regular File<br>12,256 File Stack<br>16 Regular File   | 4/27/2021 61340 PM   |  |
| Physical Size<br>Start Cluster<br>Date Accessed<br>Date Modified<br>Incripted<br>Compressed<br>Actual File<br>Inservent<br>DOS Attributes<br>Actual Size | NAL IN<br>1912/2014<br>Very Very Landon PM<br>Reference PM<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prove<br>Prov | γ0<br>ΤΟ ΤΟ Τ   | и на на пределата на  | SE<br>SE<br>SE<br>SE<br>SE<br>SE<br>SE<br>SE<br>SE<br>SE   | U*EIN&**U/USEIN&(,U/U/EÉX&&-U*U*EIN**,U*USEUN&(/U,U/EÉX&*U/U,USEIN&ŠIU-U*EJN&*2000<br>E-N#(=U/U/E-X***U_USE2N&\$U*U*E,N#(3U*U/E*X***U*U*USE3SUEU*E+N**U*DEDN#(3U5U/E*) |

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





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

| Ble Siew Mode H | telo.  |   |   |  |  |                    |   |           |
|-----------------|--|---|---|--|--|--------------------|---|-----------|
|                 | 98840 03 D   | Da la bai bai ba  |   |  |  |                    |   |           |
|                 |  | File List   |   |  |  |                    |   |           |
| ndence Tree     |  |   |   |  |  |                    |   |           |
|                 | PlayPeady  | Name  | Size Type   | Date Modified  |  |                    |   |           |
|                 | (ii) 💭 SOL Sarvar Managamari Shu   | \$110   | 4 NTFS index AlL  | 4/27/2921 6:59:33 PM   |  |                    |   |           |
|                 | H 🖸 Vat  | V01.chk   | 8 RegularFile   | 5/26/2021 11:40.39 PM  |  |                    |   |           |
|                 | III Carlos Vaual Studio<br>Carlos VSCommon   | V01.log<br>V010066.log  | 512 RegularFile<br>512 RegularFile  | 5/26/2021 4:18:20 PM<br>4/27/2021 6:59:30 PM                               |  |                    |   |           |
|                 | E 🔄 vetub  | V010007.lcg   | 512 RegularFile   | 4/27/2921 6:59:30 PM   |  |                    |   |           |
|                 | 🗠 🧰 Windows.   | V010008.leg   | 512 RegularFile   | 4/27/2921 6:59:30 PM   |  |                    |   |           |
|                 | ActionCenterCache  | V010009.leg   | 512 RegularFile   | 4/27/2121 6-59:30 PM   |  |                    |   |           |
|                 | lopication Shortsub  | VUNDOGA.log   | 512 RegularFile   | 4/27/2021 6:59:30 PM   |  |                    |   |           |
|                 | au Ca Dum  | V010008.log   | 512 RegularFile   | 4/27/2021 6:59:30 PM   |  |                    |   |           |
|                 | - Caches   | V01000C.log   | 512 RegularFile   | 4/27/2021 6:59:30 PM   |  |                    |   |           |
|                 | Bano Explorer  | V01000D.log   | 512 RegularFile   | 4/27/2121 6:59:30 PM   |  |                    |   |           |
|                 | GameExplorer     History   | V01000E.log   | 512 RegularFile   | 4/27/2021 6-59-30 PM   |  |                    |   |           |
|                 | ECompatCache   | V0H000F.leg   | 512 RegularFile   | 4/27/2121 6:59-30 PM   |  |                    |   |           |
|                 | I ECompatilityCache  | Wowdord.leg   | 512 RegularFile   | 4/27/2821 0:59ED PM  |  |                    |   |           |
|                 | PerCache     PerCookes   | 0110011.log   | 512 RegularFile   | 4/27/2021 6:59:30 PM   |  |                    |   |           |
|                 | iii iii iiii iiiiiiiiiiiiiiiiiiiiiiiii   | V0h00h2.log   | 512 ReputarFile   | 4/27/2021 # 59-30 PM   |  |                    |   |           |
|                 | (a) CoverShell   | V01/0013.log  | 512 RegularFile   | 4/27/2021 6/59:30 PM   |  |                    |   |           |
|                 | III Cache  | V0100014.log  | 512 RegularFile   | 4/27/2921 6:59:30 PM   |  |                    |   |           |
|                 | - Ringtone's<br>- Caming Ties  | V010015.leg   | 512 RegularFile   | 4/27/2321 6/59/33 PM   |  |                    |   |           |
|                 | el Contraction de la contracti | V01es00001.jes  | 512. RegularFile  | 4/27/2021 6:16:14 PM   |  |                    |   |           |
|                 | Shell  | V01ee00001.rc.FileSlack   | 512 File Slack<br>512 RegularFile   | 4/27/2321 6:16:14 PM   |  |                    |   |           |
|                 | Temporary Internet Nes   | V01/es00002,es.FileSlack  | 512 File Slack  | ALL TEACTOR FOR THE FIRE   |  |                    |   |           |
|                 | WebCache   | I voltenplog  | 512 ReputerFile   | 4/27/2021 6:59:30 PM   |  |                    |   |           |
|                 | E-Ca WnX   | WebCacheV01.dat   | 26,112 RegularFile  | 5/26/2321 11:40:54 PM  |  |                    |   |           |
|                 | 🐵 🔁 Windows Sidebar 🛛 🛸  | Webl'as haven Editars   | 18 784 File Clark   | and a set of the set of the  |  |                    |   |           |
|                 | ,  | WebCacheV01.jfm   | 16 RegularFile  | 5/26/2021 4:18/20 PM   |  |                    |   |           |
| pete.           |  | 647-6677617+ Ca yec:/Users/EHSADRIN/AppDat  |   |  |  |                    | - 100 - 10  |           |
| 21              |  | COyOC:\Users\EMSALNIN\AppData\Local\Microso   |   |  |  |                    |   | 11-38h30  |
|                 | ~  | 99999999999999999Åca.goldenhost gBo8Ttúå(€  | •"se,be[61 Xt 's'rBpB't   |  |  |                    | and the second second                             |           |
| Plame           | Viti Berlio Adra   | Witten-sleptel. AAAAAAAAAAAAAAAAAAAAAA  |   | 'LBLBLL eller-wieb, a  |  |                    |   |           |
| File Class      | fergular Par   | 7991979999999999999Aco,rognhaugen uB#Situe(€<br>999199999999999Aco,vizards vBuBatyi)€ | <pre>re.belfY pt st'vStExt 1 BC;~;( *s0.be(C; it_st'xSvE_t)</pre>                                 | to,0a  |  |                    |   |           |
| File Sze        | States -   | 51ft5-51eb0pud99999999999999Aau.com.westmea   |   | teits : t'zlubt0:Ft -  | Leps - Bayyyyyyyyyyyyyyyaaa.                                   | .sensebridge (ByDt | - dia #   | speix     |
| Physical Size   |  | 999199999999999999Acom.popvitzin )B(Bst01@  |   | adleey/yyyyyyyyyyyAccm.zeph  | yrecordline 5)B 5916   | *e##82#(@*         | -t "E"@5-B't)2Ee-e[tb                             |           |
| Start Chuster   |  | DES-S[ebi-Ehyppypypypypypypame.plurr #E.Bot<br>#16                                    | (6 *hž 3bě(68 Ut at "StBat)<br>L6 - (*b Nm pryvyvyvyvyvácom.unappy66 "                            | (€ - [eb. béh?9999999999994h   | <pre>set.webpinoytanbayan %B#Bas<br/>su .u*"B*B.ui)F@u-s</pre> | ti€ •hel           | j,be[€ èt ét:ŠE'Bét]<br>99999999998ti.zmarta •B'B | 13E*-*    |
| Date Accessed   | -aretopolitikostod Web   |   | <pre>iii)30 - (eb. im ///////////////////////////////////</pre>                                   | sis u j€ •m2,bel€  | an 'm. n. n. n'n) sen-s  | steetnen 23333     | ANALANANALA . THULLA . 8.8                        | RYG 728   |
| DateCreated     | L'UNITA COMPANYA DIA   | 9999999999999999Anet.nu-pogodi ™B-BDu31€  | •p8; bel€ Hu Pu*85*EPu5)P€,[e   | b, fup91999999999999Acon.medm  | askt24 (B#BPu7)@   | ·puf,belf.         | Tu \u*a58B\u9)NE*-*[e                             | the same  |
| Date Modified   | 3/x7/1971 653.01 844   | 999199999999999Ådk.dhedegaard B.S.\ar)€   | <pre>•gipibe(f) 'u hz*28eThu =)sf"-"[</pre>   | eb,Ieg   |  |                    | the second of the second                          |           |
| Encrypted       | fina   | yyyjyyyyyyyyyaca.schlachter 758hu?)€  |   | the dippyyyipyyyyyyyyyace.sos  |  |                    | tu's5 MCu*ElSC+++(tb,p*q)?<br>be(CA 'u +u*=5*5+u* |           |
| Encrypted       | Think  | 99999999999999999Acom.621422 #858>u530<br>9999999999999999941.lp-support B+844(10     | • = 20,856 [C_2 'u *u*=B=B*u40) (CA=A]<br>• = = = = = = = = = = = = = = = = = = =                 | <pre>(b. %6s)999999999999992de.zaid<br/>(b. %s 97999999999999920Ach)</pre> |  | *a8', be(eA        | Tu Oue ** BB: yh ** B&Bbu                         |           |
|                 |  | 99999999999999999Åca.tannerryan "BiSaug)€   | ·uyo.belth au lu* B*Blu+1)J#A-Al  | 60585V   |  |                    |   |           |
| Actual File     | That   | 99999999999999999\$acm.meganreel uB*Biuk)€  | .vissbe(CA du su'gs Bsu,m)ICE-E(  | 4b, ( 6v)99999999999992Åx92. sou   | thernlights SuBsuo!€   | *vőł, bejez        | üu γ⁺,B{Bv-q}≫C-Ç[tb                              | Beatw 1   |
| StartSector     | 1.5008-50  | 99999999999999999999999999999999999999  | <ul> <li>i'sbe(EI</li> <li>ifNone(EI</li> <li>v dv'fBAEdv5')PEI-I(</li> </ul>                     |  | .regitz EBCBars")@   | ·) 28. be(#1       | hy py ESEBpye-1HEE-91                             | Tabar     |
| DOSAttributes   |  | yyyyyyyyyyyyyainja.consola ChARKvti€<br>yyyjyyyyyyaio.3queens EBEBpv'-1€              | <ul> <li>E299616E FA (A, E29620A2, )LE1-11</li> <li>INUDE101 (A, GA, E29620A2, )LE1-11</li> </ul> |  | redros reforme le  | .ist, belet        | us ba. corobae. 1HER-21                           | Tappy.    |
| Halden          | 1000   | yyytyyyyyyyyyyänet.be9455 ISEn(+())€<br>yyytyyyyyyyyyänö.youpark CS×SAv.*)€           | <ul> <li>crose(c) cv 'v'Ists'vs)rco-o(c</li> <li>crose(c) cv 'v'Ists'vs)rco-o(c</li> </ul>        | 18 ' 979999999999999An1  | .paypro IBIR'vi?i@   | ·. speleo          | @v "v'08fB"v9.) reò-ò[                            | leptoy    |
|                 |  | 99919999999999909Åbr.com.zxe (B0BDv/-1€   | 15be165 0v 0v 00000v2+1900-01   | 455%c 01000000000000000  | .bliker YBÛBÜr0s)€   | ·03866160          | Av ev bSUBevils) NEU-DI                           | (LADS #14 |

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]   |                    |
|--------------|----------------|---|--------------------|
| Entryld 🦂    | ContainerId    | Url   | AccessedTime       |
| @1           | 15             | :2020060820200615: DVSAdministrator@:Host: This PC  | 132368189382665280 |
| 0 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] |             |  |                    |  |  |  |  |  |
|--|-------------|--|--------------------|--|--|--|--|--|
| Entryld 🛛                                | ContainerId | Uni  | AccessedTime       |  |  |  |  |  |
| 01                                       | 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 |  |  |  |  |  |
| 05                                       | 18          | :2021051820210519: emsadmin@file://emsserver/nas/2020%20Mesa%20County%20General/Results/Tabulator00004/Batch2003/1_1_4_2003_DETAIL.DVD.txt     | 132658342689478943 |  |  |  |  |  |
| 0.6                                      | 18          | :2021051820210519: emsadmin@:Host: emsserver   | 132658342689478943 |  |  |  |  |  |
| 07                                       | 18          | :2021051820210519: emsadmin@file://emsserver/nas/2020%20Mess%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.

# Server SQL Server Management Studio (SSMS) Log Files Overwritten

## **Purpose:** These log files track the installation of the SQL Server Management Studio, which is used to get into the backend of the election databases.

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

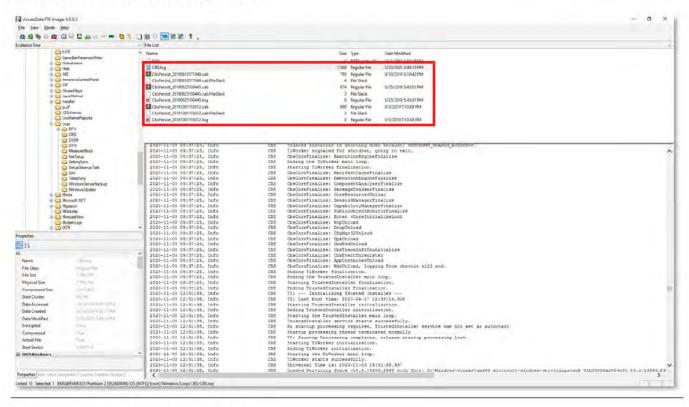
|  | Heb   |   |
|--|---|---|
| 14904  |   | 前 网络龙 ? .   |
| fence Tree   |   |   |
|  | Accluse     Accluse     Accluse     Accluse     Accluse     Accluse     ConnectedEversePation     Boost     ConnectedEversePation     Boost     ConnectedEversePation     Boost     ConnectedEverse     ConnectedEverse     ConnectedEverse     ConnectedEverse     ConnectedEverse   | Stot         Stot <th< th=""></th<>   |
|  | Jiceles Tickebeld/Siller     Kibeld/Siller     Kibeld/Siller     Kibeld/Siller     Kibeld/Siller     Missiller     Missille | <pre></pre>   |
| renties  |   | CommandLine: ************************************   |
| 41   |   | KSI (s) (BC:04) [12:56:57:021]: Note: 1: 2203 2: C:\Windows\Installer\inprogressinstallinfo.ipi 3: -2147287038  |
| 2.9  |   | KSI (# (50:04) [12:56:57026]] 355:412:50:200 for this transaction.<br>KSI (# (50:04) [12:56:7026]] 35:417:420 for the former Wintersort/Windows/CurrentVersion/Policies/Explorer 3:2  |
| Name   | LOW SALE FOR STREET,  | M31 (a) (BC:44) (12:65:75)(37); File will have security applied from OpCode,  |
| The Case   | Energy and to real to the   | KSI (8) (BC:04) (12:56:57:035): SOFTWARE RESTRICTION POLICY: Terifying package> 'C:\ProgramData\Package Cache\(70144EEA-6000-91ED-SD00-SCCEFF225ED4)v14.0.500.272\x84\SQL3ysCirTypes.msi  |
| File Sce   | Arthurs   | KSI (#) (BC:04) [A:04:057030]; SOTTAMEE KSTRUCTION FOIGUT: C:)FF00gamEnts/Feckage Canchy/T0449E8-4000-ALD-FD0D-BC57723094/94.0.590.373 X8415G2gytCirtypes.mai is # sigitatius<br>KSI (#) (BC:04) [A:107:01966]; SOTTAMEE KSTRUCTION FOIGUT: C:)FF00gamEnts/Fackage Canchy/T0449E8-4000-ALD-FD0D-BC57723094/94.0.500.373 X8415G2gytCirtypes.mai is # sigitatius  |
| hysical Size   | 444.178   | MSI (s) (8C:74) [12:57:05:961]: MSCOREE not loaded loading copy from system32   |
| art Cluster  | the second se   | Not (#) (#C104) [11071051965]1 End distog jot enabled   |
| ite Accessed   | Long 2015 Function Bank   | HSI (#) (EC:04) [12:057:061965]; Original parkage =>> C:Vibrogrumbds4)Package Caeth(Vior)10048EA+000+4CID-6D00-BCCHFF2258D4)v14.0.500.272(x)4\SQLDysClrTypes.msi<br>HSI (#) (EC:04] [12:057:061965]; Package verter unning from =>> C:VibrogrumLinstallerJab2fA.msi   |
| ate Created  | 6 TOTOLO DI MONTRA  | HbT (m (BC:04) [1215]:00:569]: APPCONPAT: Comparing score property overrides found.   |
| te Modified  | 1.000000.00104.044  | KEI (#) (BC:C4) [12:57:01:545]: APPCOMPAT: looking for appcompts database entry vith ProductCode "(70144BEA-6000-41ED-8DD0-8CC9FF225BD4)".<br>KEI (#) (SC:041 [12:57:01:5458]: APPCOMPAT: looking for appcompts database.   |
| crypted  | have:   | NGI (# [SC149] [12:57:05:760]: AFFCONVAT: so matching reductCode found in database.<br>NGI (# [SC149] [12:57:06:770]. Hawhing publicly value "Jamaformatherupus" is 1   |
| impressed  | Exten.  | MSI (s) (SC104) [12:57:08:975]: Machine policy value 'DisableTatch' is 0  |
| tual File  | Jag   | KII (s) (6C:54) [1:07:00:975] Nachane policy value "AllowLockdownRatch' is 0<br>MSI (s) (6C:54) [1:07:01:975] Nachane policy value "DisableIMAsculus" is 0  |
|  | VI PLASSA   | MII (a) (BC:44) [11:07/05:971] Hechine policy waite "Dismbled/Watching" is 0<br>MII (a) (BC:44) [12:07/05:971]; Machine policy waite "Dismbled/Watching" is 0   |
|  |   | MSI (#) (BC:C4) [12:57:05:976]: APECCRPAT: looking for apprompt database entry with FroductCode */70144EEA-6000-41ED-5DDD-5CCSPF125BD4 *.   |
| tart Sector  |   |   |
| tart Sector<br>IOS Attributes                        |   | HET (m (BC/FN) [10:57:01:57.6]; ABCONBET; so matching TechantOcde found in depakes.   |
| Start Sector<br>DOS Attributes<br>1.1. Stort Edename | AUGULTIN Schertificuus  | HET en (BCF4) [1517101574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (a) (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) [151701574]; DECOUDET: Un methang TrebunCode Rund in Asphane.<br>El (BCF4) |

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

|              |  | ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●  |
|--------------|--|--|
| dence Tree   | NET VI 5   |  |
|              | Afin     Afin | Stot         Stot <th< th=""></th<>  |
|              | Generation     Generation     Generation   | MSI (m. (50/170) [13/64/02/178]: ****** Runfugitaei<br>************************************  |
|              | <ul> <li>ToorDecReput:</li> <li>Tomp</li> <li>Tomp</li> <li>B636e84 2183-to 7665e80cf</li> </ul>   | Commandation: Co   |
|              | Constant Sectors  | <pre>sts (or (Solin) [1]4460217917] dotated accurate maked.<br/>Sts (or (Solin) [1]4460217917] dotated maked.<br/>Sts (or (Solin) [1]446021795] Lotated maked.<br/>Sts (or (Solin) [1]446021795] Lotated maked.<br/>Sts (or (Solin) [1]446021795] Analysis maked.<br/>Sts (or (Solin) [1]446021795] Analysis maked maked.<br/>Sts (o</pre> |
| 200          | - WHE  | Comparing  |
| rentres      |  | di (a) (dčić) (livietojiše): Machine policy velue "DisableVarinstalis" is 0  |
| 51           |  | 881 (a) (SCIC) [13:46:02:815]: Note: 1: 2203 2: C:\Windows\Isstaller\inprogressinstallinfo.ipi 3: -2147287038  |
| 24           |  | HSI (a) (50:10) [13:46:02:03:0] SIXetRestorPoint skipped for this transaction. HSI (a) (50:10) [13:46:02:03:0] Rest (a) 14:10 a) Rest_ONDERT (ART).edvert/UserstutVersturtVe   |
| lame         | Internet internet  | MSI (s) (SC:1C) [13:46:02:522]; File will have security applied from OpCode.   |
| de Casi      | Paristen I m.  | KIT (#) (EC:10) [31:46:02:83]; SOTTAKER REFRICTION POLICY: Yesfying package ->> 'C:ProgramBat/Package Cabb/(YO144BEA-000-4)(ED-800-0CCHF2328(H)/914.0.500.2724(H)/92(L)/92(H)/92(  |
| le Sze       | dia 162  | HSI (#) (SCID) [13446:02:894]: SOTTALSE RESTRICTON POLICY: C:\ProgramBata Package Cashe\/70144HEL-600-HED-HDD-HDD-HDD-HDD-HDD-HDD-HDD-HDD-HDD  |
| voicel Size  | data 170   | KSI (#) (8CilC) [13:46:02:894]: MSCOREE not loades loading copy from system32  |
| art Cluster  |  | IET (m. (KC)(D) (1)(4)(4)(2)(8)(9)) End dialog not weakled<br>XSI (m. (SC)(C) (1)(4)(4)(2)(8)(9)) (2)(2)(3)(3) Antibal Datases — > C)(Froetreperts)Fackback (200-8)(2)(8)(3)(3)(3)(3)(3)(3)(3)(3)(3)(3)(3)(3)(3)   |
| te Accessed  | A protein visit, and   | RSI (#) (SC:(C) (13:46:02:899): Package we're running from => C:\Windows\Installer\9f3d4.mai   |
| te Created   | Arrested would also  | MEE (# (#C)(C) [11:46:02/405]; AMPCONDAT/ Compatibility mode preparty contrides found.   |
| e Modified   | 3.07052 Table 244  | KST (#) (SC:10) [12:46:02:9031 AFFCCMFAT: looking for uppcompat database entry with ProductOde "70144HEA-600-4LEC-BDO-DCCSFF228DG4".<br>KST (#) (SC:10) [12:46:02:9031 AFFCCMFAT: looking for uppcompat database.  |
| hatqqu       | Press  | MST (m. (40:10) [13:44:03:408): Nachine policy value 'Transformafecure' is 1   |
| repressed    | Free   | MST (a) (40:110) [13:46:02:900]: Machine policy value "Disablefatch" is 0<br>MST (a) (40:11) [13:46:02:900]: Machine policy value "AllowitedownFatch" is 0   |
| tual File    |  | KSI (s) (GCIC) [13:96:02:90]: Machine policy Value "AllowLorddownBach" is 0<br>KSI (s) (GCIC) [13:96:02:90]: Machine policy Value "AllowLorddownBach" is 0   |
| ut jector    | CONTRACT (   | KSI (s) (8C:1C) [13:46:02:909]: Machine policy value 'DisableflyWeightPatching' is D   |
| DS Attribute |  | MSI (#) (8C(1C) [13:46:02:909]: ADBCOMBAT: looking for sppcompat database entry with ProductCode *(70144EEA-6020-41ED-8DE0-8CCSFE228ED4)*.   |
| Short Filena |  | HII (# (#C:CC) [13:46:02:909] ADPCOMPAT: no matching ProductCode found in database.<br>HII (# (#C:CL) [13:46:02:909] Tamaforma are no accuse.  |
|              |  | HSI (a) (HCIC) [13:46703:90]: PROFERTY CHANK: Adding HelicopileLocation property. Its value is "Ci/Owert/MERAINIAgbiaski/coal/Semei/eup/a886-deup.EUD 202104733447" 0; 202399<br>HSI (a) (HCIC) [13:46703:90]: Tomman Liney HSITASKI/A Adding/HelicopileCoal-SystCI/YOP/erute REMOT/Feed/Distance/HSITASKI/A Adding/HelicopileCoal-SystCI/YOP/erute REMOT/Feed/Distance/HSITASKI/A Adding/HelicopileCoal-SystCI/YOP/erute REMOT/Feed/Distance/HSITASKI/A Adding/HelicopileCoal-SystCI/YOP/erute REMOT/Feed/Distance/HSITASKI/A Adding/HelicopileCoal-SystCI/YOP/erute REMOT/Feed/Distance/HSITASKI/A Adding/HelicopileCoal-SystCI/YOP/erute REMOT/Feed/Distance/HSITASKI/A Adding/HelicopileCoal-HSITASKI/A ding/HelicopileCoal-HSITASKI/Adding/HelicopileCoal-HSIT   |
|              |  | Vet la tentra tratagontenta montente dentere destantente tratagonte ta untos en tistentes ententententes e   |

# 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

| ile Siew M   | lade Belp  |  |                    |   |   |
|--|--|--|--------------------|---|---|
|  | a a l C  | 1 1 10 10 20 20 21 .                                     |                    |   |   |
| dence Tree   |  | S FileList   |                    |   |   |
|  | ELAMERUP   | A Name   | Size Type          | Date Modified   |   |
|  | 🖾 e-US   | 1 6130   | 4 NTIS Index       |   |   |
|  | ants<br>to replace on  | III Citatee  | 1.00 Heather File  |   |   |
|  | al lores   | CbsPersist_20210427115957.cab                            | 512 Regular File   | 4/27/2021 558:18 PM   | with the second s |
|  | L + 100  | Costenior_20210427115937.ceb.fileSteck                   | 1 FileSlack        |   | File names, sizes, and dates have   |
|  | GameBarPlesenceWitter  | CbsPerust 20210427115649.cab                             | 5.001 Regular File | + 427/2021 655:05 PM  |   |
|  | ii 🛄 Gobalization  | CbsPensist 20210427115649.cab.FileSlack                  | 4 FileSlack        | Contraction of the light  | abayred These files have all hear   |
|  | to HelpPane site   | CbsPersist_20210427190033.cab                            | 589 Regular File   | e 4/27/2021 6/52/28 PM  | changed. These files have all been  |
|  | - 15 Ho exe  | CbsPensist_20210427190033.cab.FileSlack                  | A File Slack       | A State of the second se | and the second se |
|  | III CO ME  | CbsPersist_20210525202119.cab                            | 1530 Regular File  | <ul> <li>5/25/2021 T/44(15 PM</li> </ul>  | replaced.   |
|  | III California InterarveControlPanel   | CbsPersist_20210525202119.cab.FileStack                  | 1 FileSlack        |   | replaced  |
|  | til C titured Apos   | CbsRemist_20210525202119.log                             | 0 Repular File     | e 5/25/2021 1544:15 PM  |   |
|  | 🔅 🙆 nputMethod   |  |                    |   |   |
|  | 🗄 😂 installer  |  |                    | and the second designed and the second  |   |
|  | Carlena (25chema)  | 2021-05-23 14:21:19, info<br>2021-05-25 14:21:19, info   |                    | TI: Initializing Trusted<br>TI: Last boot time: 2021-05-2   |   |
|  | DiveKemelReports   | 2021-05-25 14:21:19, Info                                |                    | Starting TrustedInstaller int   |   |
|  | Lif Cal Loga   | 2021-05-25 14:21:19, Info                                | C88                | Lock: New Lock added: CCD#Pub   | SicSessionClassFactory, level: 30, total lock:5   |
|  | C BPA  | 2021=05=23 14:21:19, Info                                |                    |   | licSessionClassFactory, level: 30, total lock:6   |
|  | CBS<br>DISM  | 2021-05-25 14:21:19, info<br>2021-05-25 14:21:19, info   |                    | lock: New lock added: Winlogo<br>Ending TrustedInstaller inits  | sNotifiLock, level: 8, total lock: 7  |
|  | DPx  | 2021-05-25 14:21:19, Info                                |                    | Starting the TrustedInstaller   |   |
|  | MeasuredBoot   | 2021-05-25 14:21:18, info                                | -C83               | TrustedInstaller service star   | ta successfully.  |
|  | I Nel Selup  | 2021-05-25 14:21:19, Info                                |                    |   | d, TrustedInstaller service was not set as abtostart  |
|  | SetupCeanupTask  | 2021-05-25 14:21:19, Info<br>2021-05-25 14:21:19, Info   |                    | Startup processing thread ter   | minated normally  |
|  | WindowsServerBackup  | 2021-05-25 14:21:19, info                                |                    | Starting TiWorker initializat   |   |
|  | - WindowsUpdate  | 2021-05-25 14:21:19, Info                                | C3.5               |   | rClassTactory, level: 30, total lock:2  |
|  | R Contract NET   | 2021-05-25 14:21:19, Info                                |                    | Ending TiWorker initializatio   |   |
| 1 1  | IN: MERCARON, NE 1   | 2021-05-25 14:21:19, Info<br>2021-05-21 14:21:19, Info   |                    | Starting the TiWorker main 10<br>TiWorker starts successfully.  |   |
| perties  |  | 2021+05-25 14:21:10, into                                |                    | Lock: Sev lock added: COsNor  |   |
| 21   |  | 2021-05-25 14:21:19, Info                                | CBS                | Universal Time is: 2021-05-21   | 1 20:21:19.494  |
|  |  | 2021-05-21 14:21:19, info                                |                    |   | 14393.4349 with Core: C:\Windows\wiraxs\ami64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.14393.4  |
| Name   | Office and the second s | 2021-05-28 14:21:18, 3nfo<br>2021-05-28 14:21:19, Info   |                    |   | NA Meminimiziative (wep.dl) version 0.0.0.6) called (stark #0x7ff000416od) #0x7ff000414fof #0x7ff000hf1a22 #00<br>from path: SrClient.dll. Continuing without system restore points.  |
| File Class   | increase in the  | 2021-05-28 14:21:19, Info                                |                    |   | sionManager, level: 11, total kock:14   |
| Hit Set  | 10.000   | 3031-08-21 14:31:18, Info                                | est                | laaks flew lask addeds Cffines  | staryCrisicalSection, isrei: 68, sonal locksit.   |
| Physical Size  | 100.00   | 2021-05-25 14:21:19, info                                |                    |   | <pre>%skageCacheCriticalSection, jevel: 126, tytel lock:16</pre>  |
| orrowessed 5   |  | 2021-05-25 14:21:19, info<br>2021-05-25 14:21:19, info   |                    |   | MbilityManager, level: 11, total lock:17<br>MarQueve, level: 60, notal lock:18  |
| art Cluster  | ADP NOT  | 2021-05-25 14:21:19, Info                                |                    |   | Bergueses Herder 60, sonal lockilo<br>Bergueses WindowsfoldsteffapressfownloadLock, level: 10, sotal lockil9  |
|  |  | 2021-05-25 14:21:19, Info                                | C88                | SonStart: Set pending store of  | whalstency check.   |
| Date Accesses  |  | 2021-05-25 14:21:19, Into                                |                    |   | initialized by client LanguageFeature#OnDemand, external staging directory: (mull), external registry direct  |
| Jate Crested   | -statements with   | 2021-05-25 14:21:19, Info<br>2021-05-25 14:21:19, Info   |                    |   | <pre>tion (HRESULT = 0x80070422 - ERROR_SERVICE_DISALED) server configuration. (HRESULT = 0x80070412 - ERROR SERVICE DISABLED)</pre>  |
| late Modified  |  | 2021-05-20 14:21:19, info<br>2021-05-20 14:21:19, info   |                    |   | server contiguration. [mesoul = menoyoux - manual service bisable]  |
| Encrypted  | Teles  | 2021-05-25 14:21:19, info                                | -C35               | Thiled to search Windows upda   | tte [HRISULT = 0x800f0906 - CBS_E_DONNLOAD_FAILURE]   |
| Compressed   | (here)   | 2021-05-25 14:21:10, Info                                |                    |   | abilities (HEESULT + Dx800f0906 - CB3_E_DONNLOAD_PAILURE)   |
| Actual File  | 200  | 2021-05-25 14125:20, INFO                                |                    |   | I SOWN RECENTET SHUTDOWN MEASON AUTOIDOP  |
| Start lector   | 71.58E T/H   | 2021-05-23 14:23:20, info<br>2021-05-23 14:23:20, info   |                    | TiWorker signaled for stundes<br>ObsCoreFinalize: ExecutionEnd  |   |
| DOSAH-Ibul   | -  | 4 2021-05-25 14:23:20, into<br>2023-05-25 14:23:20, into |                    | Ending the TiMorket main loop   |   |
|  |  | 2021-05-23 14:23:20, info                                | CBS                | Starting TiWorker finalization  |   |
|  |  | 2021-05-25 14:23:20, Info                                | CBS                | ChaCoreFinalize: ManifestCach   | *Finalize   |
| and the second s | inter-management Cardmin-Prevent (Second)  | 2021-05-25 14:21:20, ThFn                                | 19.4               | ChaCoveFinalizet ExecutionEnd   | Inerital tak  |

#### 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 (5.1 | 1-CO) Election Databases Before |
|-----------------------------|---------------------------------|
|-----------------------------|---------------------------------|

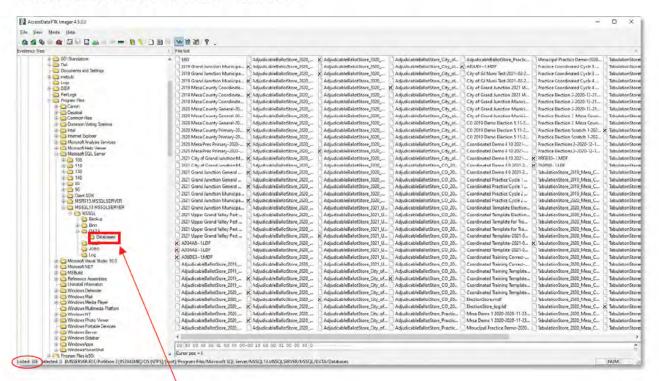
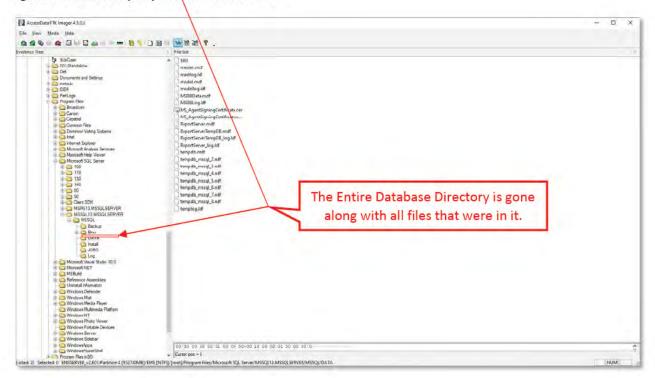


Figure 28 - EMS Server (5.13) Election Databases After

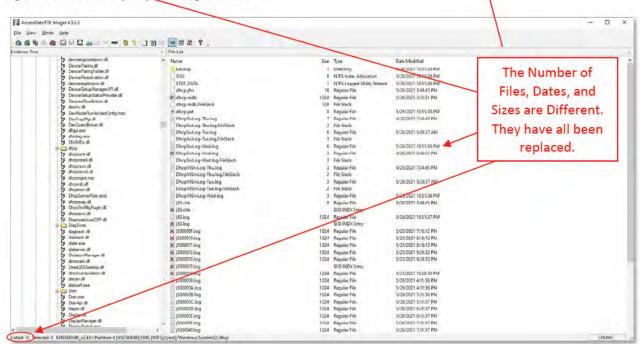


Server DHCP Log Files Missing/Overwritten

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

| AccessDate FTK Imager | 4.5.6.3                             |                                |                              |  | - 0   |  |
|-----------------------|-------------------------------------|--------------------------------|------------------------------|--|-------|--|
| e giew Mode Help      |                                     |                                |                              |  |       |  |
|                       | 00                                  |                                |                              |  |       |  |
|                       |                                     |                                |                              |  |       |  |
| lence Tree            |                                     | File List                      |                              |  |       |  |
|                       | bg-8G A                             | Name                           | Size Type                    | Date Modified  |       |  |
| 41 😋                  |                                     | Dacktap                        | 1. Directory                 | 3/23/2027 955:39 PM  |       |  |
|                       | Bherops<br>CatRoot                  | 5130                           | 8 NTFS Index Allocation      | 5/23/2021 9:33:59 PM   |       |  |
|                       | catnot2                             | STXF DATA                      | 1 NTFS Logged Utility Stream | 5/23/2021 9(33:59 PM   |       |  |
| 14                    | cngieyhelperdi                      | dhep.jfm                       | 16 Regular File              | 8/30/2021 3/35/41 PM   |       |  |
|                       | CodeIntegrity                       | Pc dbcn.mdb                    |                              | 3/30/2021 3:03:04 PM   |       |  |
|                       |                                     |                                | 1024 Regular File            | sy sty coch station PM   |       |  |
| 0-00                  | cortig                              | dhcp.mdb.FileSlatk             | 128 Fole Stack               |  |       |  |
|                       | Configuration                       | 14 dhop.pat                    | 0 Regular File               | 5/23/2021 9:13:59 PM   |       |  |
|                       | 4+62                                | DhepSed.og.Feilog              | D Dagutar File               | 5/22/2021 640-01 AM  |       |  |
|                       | da-GK                               | DhcpSnLog-Frilag-FileSlack     | 1 File Stack                 |  |       |  |
|                       | DDfe                                | DhepSeiLog-Men.log             | 0 Regular File               | 5/11/2021 6:00:42 AM   |       |  |
|                       | de dE                               | DhcpSoLog-Mon.log-FieSlack     | 1 File Slack                 |  |       |  |
|                       | 🗀 telekup                           | DiscpSisting-Setling           | 8 Regular File               | 5/21/2021 6:00:06 AM   |       |  |
|                       | dhorngmi.me-                        | DhipSotog Sadag FileSlack      | 1 FileSlack                  |  |       |  |
|                       | dhaymb dil                          | DhcpSwipg-Sunlog               | 6 Regular File               | 5/21/2021 6:00:06 AM   |       |  |
| 19                    | direimin di                         | DhopSnLog-SunJog-FileSlack     | 11 File Stack                |  |       |  |
|                       | DhosServerRole and                  | DhcpSrvLog-ThuJog              | 8 Regular File               | 5/21/2021 6/0:57 AM  |       |  |
|                       | dhoyshap.dll                        | DhcpSivLog-Thulog.FileSlack    | 1 File Slack                 | A R LEVE C WINDOW PART   |       |  |
| 10                    | DhouSer/MigPuger dll<br>choasavo dl | DhcpSr/Log-Tue.log             | D Reputar Pile               | 5/19/2021 boltx47 AM   |       |  |
|                       |                                     |                                |                              | 6/11/2019 4:37:34 PM   |       |  |
| 60                    | DiagSycs                            | X DhopSellog-Tue.log           | 6 Regular File               |  |       |  |
| 63                    | Dan                                 | X DhepSelog-Tunlog             | 12 Regular File              | 6/26/2019 5:24:26 AM   |       |  |
| 1                     | dist.ince                           | DhcpSivLog-Tue.log.FikSlack    | 1 File Slack                 | A Report of the State of the St |       |  |
|                       | dnoord exe                          | DhcpSnLog-Wed.log              | 0 Regular File               | 5/20/2021 600:52 AM  |       |  |
|                       | drangint misc.                      | X DhcpSnLog-Wed.log            | 4 Regular File               | 6/12/2019 9:04:41 PM   |       |  |
|                       | drangi dil                          | DhcpSr/Log-Wed.log.FileSlack   | 1 File Slack                 |  |       |  |
| -9                    | draperi di                          | DhepViSniteg-frideg            | 4 Regular File               | 5/23/2021 6/06/01 AM   |       |  |
|                       | downlevel                           | DhcpVtSrvLog-fri.log.FieStack  | 1 File Stack                 |  |       |  |
| 1900                  |                                     | DhipViSryLog-Mon.log           | 4 Regular File               | 5/10/2021 6:00-42 AM   |       |  |
| 100                   | Driver Store                        | X DhopViSrvLog-Monilog         | 3 Regular Elle               | 5/10/2019 8:54:50 PM   |       |  |
|                       | dec<br>el-GR                        | DhcpVtSn/Log-Mon.logFileSlact  | 1 File Stack                 |  |       |  |
| 2                     |                                     | DhicpVtSrvLog-Sac.log          | 4 Regular File               | 5/23/2021 6/0.06 AM  |       |  |
|                       | en-GB                               | DhcpV(SrvLog-Set.log.FileSlack | 1 File Sleck                 | and the state of t |       |  |
| 65                    |                                     |                                |                              | 5/23/2021 6:00:06 AM   |       |  |
| 9                     | es                                  | DhcpVtSrvLog-Sun.log           | 3 Regular File               | SY 29/2021 COUCUD ANY  |       |  |
| 00                    |                                     | DhcpVrtSrvLog-Sun.log.HieSlack | 2 File Slack                 | and  |       |  |
| 0                     | ed-NX                               | DhcpVtSrvLog-Thu.log           | A Regular File               | 5/21/2021 500:57 AM  |       |  |
|                       | et ett.                             | DhcpVtSrvLog-Thu.log.fileSlack | T File Stack                 | A CONTRACTOR OF  |       |  |
|                       |                                     | DhcpVISrvLog-Tue.log           | -4 Regular File              | 5/19/2021 5:00:47 AM   |       |  |
| 3                     | fr                                  | K DiscpVrSext.og-fue.log       | 3 Regular File               | 6/26/2019 544-26 AM  |       |  |
|                       | #5"1 ¥                              | DhcpVtSrvLog-Tue.logJileSlack  | 1 File Stack                 |  | (NUM) |  |

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



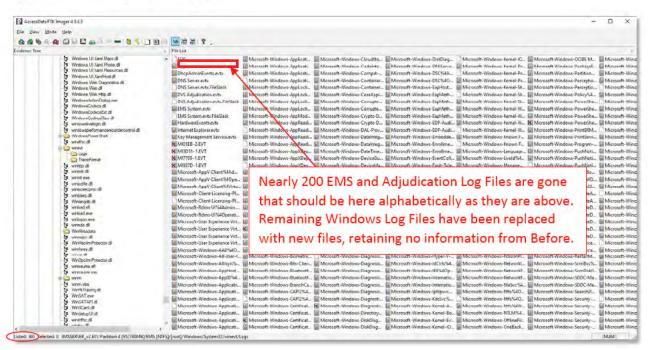
### Server Event Logs Missing/Overwritten

**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

| AccessData H | TK Imager 4.5.0.5                                      |                           |                                   |                             |                             |                              | 1.7                            | 0. >           |
|--------------|--|---------------------------|-----------------------------------|-----------------------------|-----------------------------|------------------------------|--------------------------------|----------------|
| Sie Ser 18   | ode Help   |                           |                                   |                             |                             |                              |                                |                |
|              |  | D                         |                                   |                             |                             |                              |                                |                |
|              |  |                           |                                   |                             |                             |                              |                                |                |
| vidense Tree |  | H FikLot                  |                                   |                             |                             |                              |                                |                |
|              | 8: CanerManageristemai                                 | * 5130                    | Archive-EMS System-2019-12        |                             |                             |                              | DVS Adjudication.exts          | Microsoft-     |
|              | Hi Sala  | Application e.t.          | Arekine-EMIS System-2020-01-      | Arthive-EMS System-2020-07: | Archive EMS System-2011-02  | Archive EMS System 2021-05   | C DVSADJ-1EVT                  | Microsoft.     |
|              | - sk-9K<br>SteepStudy                                  | Archive-EMS System-2019   | -06 Archive-EMS System-2020-01    | Aschive-EMS System-2020-08  | Archive-EMS System-2011-02  | Archive-EMS System-2021-05   | EMS System.evtx                | Microsoft-     |
|              | a sieep study  | Archive-EMS System-2019   | -07 Archive-FMS System-2020-01    | Archive-EMS System-2020-09  | Archive-EMS System-2001-02  | Archive-EMS System-3021-05   | EMS System.evtx.FleSiack       | Microseft-     |
|              | 🔾 #S   | Archive-EMS System-2019   | -07 Archive-FMS System-2020-01    | Archive-EMS System-2020-09  | Archive EMS System-2001-02  | Archive-EMS System-3021-05   | i Hardware Vents evtr          | Microseft-     |
|              | IN CONTRACTOR  | Archive-EMS System-2019   | -07 Jachive-EMS System-2020-01    | Archive-EMS System-2020-09  | Archive-EMS System-2001-02  | Archive-EMS System-3021-05-  | Internet Explorer.exts         | Microsoft-     |
|              | in Co Speech   | Arubice ENS System-2019   | 07 Archive EMIS System 2020-01    | Anthive TMS System 2020-09  | Anthree EMIC Sustem-2001-02 | Archive-EMS System -3021-05- | Key Management Service-exter   | Microsoft-     |
|              | Speech_OneCore   |                           | -07 Archive-EMS System-2020-01    |                             |                             |                              | C M3773-1EVT                   | Microseft-     |
|              | ik 😂 sposi   |                           | -07 Archive-EMS System-2020-01    |                             |                             |                              | M667F-LEVT                     | Microsoft-V    |
|              | 100 BODA   |                           | -07 Archive-EMS System-2020-01    |                             |                             |                              | CIM9607-1EVT                   | Microsoft-V    |
|              | ar-Lath-CS   |                           | -07 Archive-EMS System-2020-02    |                             |                             |                              | MBEAF-LEVT                     | Microsoft-     |
|              | anLativRS  |                           | -08 Archive-EMS System-2020-03    |                             |                             |                              | Mcrosoft-AppV-Clent%4/d        |                |
|              | E su SE  |                           | -08 Archive-EMS System-1020-03    |                             |                             |                              | Mcrosoft-AppV-Cient%40pe       |                |
|              | E C Sysperep   |                           | -08 Archive-EMS System-2020-03    |                             |                             |                              | Mcrosoft-AppV-Cient%/Virtu.    |                |
|              | p 🛄 System/Reset/Nation/                               |                           | -08 Archive-EMS system-2020-03    |                             |                             |                              | Mcrosoft-Client-Licensing-PL.  |                |
|              | (i) 🥁 Tasks  |                           |                                   |                             |                             |                              |                                |                |
|              | C th TH  |                           | -08 🕍 Archive-EMS System-2020-03  |                             |                             |                              | Mcrosoft-Rdms-U%/Admin         |                |
|              | TaWofWip.exe   |                           | -08 Archive-EMS System-1020-03    |                             |                             |                              | Mcrosoft-Rdms-U%40penti        |                |
|              | C uk-lk  |                           | -08 📓 Archive-EMS System-2020-03  |                             |                             |                              | Mcrosoft-User Experience Virt. |                |
|              | -b warregos (B   |                           | 08 🔙 Archive EMS System 2020-03   |                             |                             |                              | Merosoft User Experience Virt. |                |
|              | e wben   | Archive-EMS System-2019   | -09 MArchive-EMS System-2020-03   | Archive-EMS System-2020-10  | Archive-EMS System-2021-04  | Archive-EMS System-2021-05   | Mcrosoft-User Experience Virt. | . 📓 Microseft- |
|              | IRI 🕒 WO   | Archive-EMS System-2019   | - 10 📓 Archive-EMS System-2020-04 | Archive-EMS System-2020-11  | Archive-EMS System-2021-04  | Archive-EMS System-2021-05   | Mcrosoft-User Experience Virt. | . K Microseft- |
|              | 🗂 WinBioDatabase                                       | Archive-EMS System-2019   | -10 Archive-EMIS System-2020-04   | Archive-EMS System-2020-11  | Archive-EMS System-2021-04  | Archive-EMS System-3021-05   | Mcrosoft-Windows-AAD%40_       | . Microseft-!  |
|              | 🕖 🤐 WritioFlughs                                       | Archive-EMS System-2019   | -10 📓 Archive-EMS System-2020-04  | Archive-EMS System-2020-11  | Archive-EMS System-2021-05  | Archive-EMS System-2021-05   | Mcrosoft-Windows-All-User-L    | Microseft-     |
|              | 1 WindowsPowerShell                                    | Archive-EMS System-2019   | -10 📓 Archive-EMS System-1020-04  | Achive-EMS System-2020-11+  | Archive-EMS System-2021-05+ | Archive+EMS System+2021+05   | Mcrosoft-Windows-Alboyn%       | Microseft-     |
|              | i i i i i i i i i i i i i i i i i i i                  | Archive-EMS System-2019   | -11 Archive-EMS System-2020-04    | Archive-EMS System-2020-11  | Archive-EMS System-2021-05  | Archive-EMS System-2021-05-  | Mcrosoft-Windows-AppHest       | Microseft-     |
|              | TraceFormat  | Archive-EMS System-2019   | -11 Archive-EMS System-2020-04    | Archive-EMS System-2020-11- | Archive EMS System-20/1-05- | Archive-EMS System-2021-05-  | Mcrosoft-Windows-AppiD164      | Microsett-     |
|              | WiniAetadata   |                           | -11 Archive-EMS System-2020-05    |                             |                             |                              | Mcrosoft-Windows-Applicabi.    |                |
|              | 🗊 😋 winmi  |                           | -11 Archive-EMS System-2020-05    |                             |                             |                              | Mcrosoft-Windows-Applicati     |                |
|              | - Calicon  |                           | -11 Archive-EMS System-2020-05    |                             |                             |                              | Mcrosoft-Windows-Applicati     |                |
|              | 21-11K   |                           | -11 Archive-EMS System-2020-05    |                             |                             |                              | Mcrosoft-Windows-Applicati.    |                |
|              | the TW   |                           | -11 Archive-EMS System-2020-06    |                             |                             |                              | Mcrosoft-Windows-Applicati     |                |
|              | 🗈 🛄 Systemstagia                                       |                           | -11 Archive-EMS System-2020-00    |                             |                             |                              | Mcrosoft-Windows-Applicati     |                |
|              | System Resources     System Resources     System O/064 |                           | 12+ Archive-EMS System-2020-06    |                             |                             |                              |                                |                |
|              | TAPI   |                           |                                   |                             |                             |                              | Mcrosoft-Windows-Applicati.    |                |
|              | Tanks  |                           | 12 Archive-EM5 System 2020-06     |                             |                             |                              | Mcrosoft Windows Applicati.    |                |
|              | H-Ca Temp  |                           | -12 Archive-EMS System-2020-06    |                             |                             |                              | Mcrosoft-Windows-Applicati.    |                |
|              | tracing.   |                           | 12 📓 Archive EM5 System 2020-06   |                             |                             |                              | Mcrosoft Windows Applicati     |                |
|              | twain_32   |                           | -12 📓 Archwe-EMS System-2020-06   |                             |                             |                              | Mcrosoft Windows Applicati     |                |
|              | (E) 🔁 Ves  |                           | 12 Archive-EMS System 1020-07     |                             |                             | DNS Server.eitx              | Mcrosoft Windows AppLeck.      |                |
|              | Web Web  | Archive-EMIS System -2019 | 12 Archive-EMS System-2020-07     | Archive-EMS System-2021-01  | Archive EMS System-2001-05  | DNS Server et x FileSlock    | Mcresoft-Windows-AppLeck       | Microsoft-     |

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

| hive-EMS Sys  | N  |   |   |   |  |   | Event D Task   |                      |
|---|--|---|---|---|--|---|--|----------------------|
| /el   | Date and Time  | Source  | EventID Task C  | - Love  | Date and Time  | Source  | Event ID Task C  |                      |
| Information   | 10/20/2020 4:55:01 PM  | EMS User Log  | 0 None  | (i) Information   | 10/20/2020 4:55:01 PM  | EMS User Log  | 0 None   |                      |
| nformation  | 10/20/2020 4:54:46 PM  | EMS User Log  | 0 None  | ()Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:44 PM  | EMS User Log  | 0 None  | (1) Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:44 PM  | EMS User Log  | 0 None  | (1)Information  |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:44 PM  | EMS User Log  | 0 None  | (1) Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:44 PM  | EMS User Log  | 0 None  | (1) Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:37 PM  | EMS User Log  | 0 None  | 15 Information  | 10/20/2020-4:54:37 PM  | EMS lise Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:37 PM  | EMS User Log  | 0 None  | (1) Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:37 PM  | EMS User Log  | 0 None  | (i)Information  |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:37 PM  | EMS User Log  | 0 None  | (1) Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:31 PM  | EMS User Log  | 0 None  | (1)Information  | 10/20/2020 4:54:31 PM  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:31 PM  | EMS User Log  | 0 None  | (1)Information  | 10/20/2020 4:54:31 PM  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:28 PM  | EMS User Log  | 0 None  | (1) Information   | 10/20/2020 4:54:28 PM  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:28 PM  | EMS User Log  | 0 None  | (1) Information   | 10/20/2020 4:54:28 PM  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:28 PM  | EMS User Log  | 0 None  | (1)Information  | 10/20/2020 4:54:28 PM  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:16 PM  | EMS User Log  | 0 None  | (1) Information   | 10/20/2020 4:54:16 PM  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:13 PM  | EMS User Log  | 0 None  | (1) Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:12 PM  | EMS User Log  | 0 None  | (1)Information  |  | EMS User Log  | 0 None   |                      |
|   |  |   | 0 None  | (1) Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:12 PM  | EMS User Log  |   | ()Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:12 PM  | EMS User Log  | 0 None  | ()Information   |  | EMS User Log  | 0 None   |                      |
| formation   | 10/20/2020 4:54:01 PM  | EMS User Log  | 0 None  | *   | AW LOCK LOCK HEARDT P M  | and user cog  | v raune  |                      |
| 0, EMS Use  | rLog   |   |   | ¥ Event 0, EMS U  | er Log   |   |  |                      |
|   |  |   |   | General Det   | inc. I   |   |  |                      |
| neral Detail  | S  |   |   | general Det   | ans  |   |  |                      |
| attend to a   | Note Barrielle   | 1   |   | Angeneites  | titMarkTolmageCommand //   | verution duration, 202.   | ms): Audit mark for tabulator '4, batch '  | 2005 and section 177 |
| ietSingleCast<br>uccessfully r  |  | ecution duration: 16m   | is): Cast vote record for tabulator '4, batch '2096'  | and session '8' Appendiau<br>successfull  |  | Account adrauon: 2031   | may mode many for tabulator is, batch  | road and separate in |
| oscessiony r  | SALLS TSMI   |   |   |   |  |   |  |                      |
|   |  |   |   |   |  |   |  |                      |
|   |  |   |   |   |  |   |  |                      |
|   |  |   |   | in the second   |  |   |  |                      |
| g Name:   | EMS System   |   |   | Log Name:   | EMS System   |   |  |                      |
| urce:   | EMS User Log   | Logged:   | 10/20/2020 4:54:44 PM   | Source:   | EMS User Log   | Logged:   | 10/20/2020 4:54:37 PM  |                      |
| ent ID;   | 0  | Task Catego   | ny: None  | Event ID:   | 0  | Task Category   | n None   |                      |
| vel:  | Information  | Keywords:   | Classic   | Level:  | Information  | Keywords:   | Classic  |                      |
| en  | N/A  | Computer  | EMSSERVER   | User  | N/A  | Computer  | EMSSERVER  |                      |
| Cade  | 0.4  | comparen.   | CHROCHART   | OnCode:   |  |   | a trade to a t   |                      |
|   |  |   |   |   |  |   |  |                      |
|   | and an and a second  |   |   |   | stinger Europhics during the   |   |  |                      |
| lore Informat   | tion: Event Log Online He  |   | autoria 24.457  |   | ation: Event Log Online He   |   | NAME: 21 157   |                      |
| iore Informat   | stem-2020-11-05-17-16-:  | 37-197 Number of  |   | Archive: EMS :  | iystem-2020-11-05-17-16  | 37-197 Number of e  |  |                      |
| ive-EMS Sys   | stem-2020-11-05-17-16-3<br>Date and Time   | 37-197 Number of<br>Source  | Event ID Task C   | Archive-TMS:  | system 2020-11-05-17-16<br>Date and Time   | 37-197 Number of e<br>Source  | Event ID Task C  | _                    |
| ore Informat<br>ive-EMS Sys<br>of ormation  | stem-2020-11-05-17-16-<br>Date and Time<br>11/3/2020 8:58:46 PM  | 87-197 Number of<br>Source<br>EMS User Log  | Event ID Tesk C<br>D None   | Archive TMS:<br>Level<br>@Information   | ystem 2020-11-05-17-16<br>Date and Time<br>11/3/2020 8:58:21 PM  | 37-197 Number of a<br>Source<br>EMS User Log  | Event ID Task C<br>0 None  | _                    |
| ore Informat<br>ive-EMS Sys<br>if<br>oformation<br>oformation   | tem-2020-11-05-17-16-<br>Date and Time<br>11/3/2020 8-58:46 PM<br>11/3/2020 8-58:45 PM   | 87-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>Ø Nane<br>Ø None   | Archive-TMS   | ystem-2020-11-05-17-16<br>Date and Time<br>1 11/3/2020 8:58:21 PM<br>1 11/3/2020 8:58:06 PM  | 37-197 Number of a<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None  |                      |
| ore Informat<br>ive-EMS Sys<br>if<br>oformation<br>oformation   | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 8-58-46 PM<br>11/3/2020 8-58-46 PM<br>11/3/2020 8-58-46 PM   | 87-197 Number of<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>0 None<br>0 None<br>0 None   | Archive-IMS (<br>Level<br>Dinformatio<br>Dinformatio  | System 2020-11-05-17-16<br>Date and Time<br>1 11/3/2020 8:58:21 PM<br>11/3/2020 8:58:50 PM<br>11/3/2020 8:57:55 PM   | 37-197 Number of e<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None  | -                    |
| ore Informat<br>ive-EMS Sys<br>if<br>iformation<br>iformation<br>iformation   | stem=2020-11-05-17-16=3<br>Date and Time<br>11/3/2020 8-58-45 PM<br>11/3/2020 6-58-45 PM<br>11/3/2020 8-58-45 PM<br>11/3/2020 8-58-45 PM   | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>0 None<br>0 None<br>0 None<br>0 None   | Archive-IMS2<br>Level<br>Informatio<br>Informatio<br>Informatio   | ystem-2020-11-05-17-16<br>Date and Time<br>11/3/2020 8:58:21 PM<br>11/3/2020 8:58:52 PM<br>11/3/2020 8:57:55 PM<br>11/3/2020 8:57:55 PM  | 37-197 Number of e<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None<br>0 None  | _                    |
| ore Informat<br>we-EMS Sys<br>I<br>formation<br>formation<br>formation<br>formation   | Item-2020-11-05-17-10-3<br>Date and Time<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-6 PM<br>11/3/2020 8:58-36 PM  | 57-197 Number of<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None   | Archive-TMS:<br>Level<br>() informatio<br>() Informatio<br>() Informatio<br>() Informatio<br>() Informatio  | ystem-2020-11-05-17-16<br>Date and Time<br>11/3/2020 8:58:21 PM<br>11/3/2020 8:58:06 PM<br>11/3/2020 8:57:55 PM<br>11/3/2020 8:57:55 PM  | 37-197 Number of c<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None  | -                    |
| ore Informat<br>we-EMS Sys<br>I<br>formation<br>formation<br>formation<br>formation   | stem=2020-11-05-17-16=<br>Date and Time<br>11/3/2020 8-58-45 PM<br>11/3/2020 6-58-45 PM<br>11/3/2020 8-58-45 PM<br>11/3/2020 8-58-45 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None<br>O None<br>O None<br>U None<br>U None   | Archive-IMS:<br>Level<br>@Informatio<br>Dinformatio<br>@Informatio<br>@Informatio   | System 2020-11-05-17-16<br>Date and Time<br>11/3/2020 858-21 PM<br>11/3/2020 85-55 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM  | 37-197 Number of c<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None  | -                    |
| ore Informat<br>ver EMS Sys<br>I<br>formation<br>formation<br>formation<br>formation<br>formation   | Item-2020-11-05-17-10-3<br>Date and Time<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-6 PM<br>11/3/2020 8:58-36 PM  | 57-197 Number of<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None   | Archive-EMSS<br>Level<br>@Informatio<br>@Informatio<br>@Informatio<br>@Informatio<br>@Informatio  | ystem 2020-11-05-17-16<br>Date and Time<br>1 11/3/2020 835821 PM<br>11/3/2020 83606 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM   | 37-197 Number of e<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None  | -                    |
| ve-EMS Sys<br>I<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | tem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 6:58:46 PM<br>11/3/2020 6:58:46 PM<br>11/3/2020 6:58:36 PM<br>11/3/2020 6:58:36 PM<br>11/3/2020 6:58:36 PM  | Source<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None<br>O None<br>O None<br>U None<br>U None   | Archive-IMS:<br>Level<br>@Informatio<br>Dinformatio<br>@Informatio<br>@Informatio   | ystem 2020-11-05-17-16<br>Date and Time<br>1 11/3/2020 835821 PM<br>11/3/2020 83606 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM   | 37-197 Number of c<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None  | -                    |
| ve-EMS Sys<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | tem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 0-584-6 PM<br>11/3/2020 0-584-6 PM<br>11/3/2020 0-584-6 PM<br>11/3/2020 0-584-6 PM<br>11/3/2020 0-584-6 PM<br>11/3/2020 0-584-5 PM<br>11/3/2020 0-584-5 PM  | 57-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None   | Archive-EMSS<br>Level<br>@Informatio<br>@Informatio<br>@Informatio<br>@Informatio<br>@Informatio  | ystem 2020-11-05-17-16<br>Date and Time<br>11/3/2020 83-821 PM<br>11/3/2020 83-535 PM<br>11/3/2020 8-57-55 PM<br>11/3/2020 8-57-55 PM<br>11/3/2020 8-57-55 PM<br>11/3/2020 8-57-55 PM<br>11/3/2020 8-57-55 PM  | 37-197 Number of e<br>Source<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None  |                      |
| ve-EMS Sys<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation  | tem-2020 - 11 - 05 - 17 - 16 -<br>Date and Time<br>11/3/2020 B 50:46 PM<br>11/3/2020 B 50:46 PM<br>11/3/2020 B 50:36 PM<br>11/3/2020 B 50:36 PM<br>11/3/2020 B 50:36 PM<br>11/3/2020 B 50:34 PM<br>11/3/2020 B 50:34 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None   | Archive-EMS:<br>Level<br>Binformatic<br>Binformatic<br>Binformatic<br>Binformatic<br>Binformatic<br>Binformatic<br>Binformatic  | system: 2020-11-05-17-16<br>Date and Time<br>11/3/2020 85-821 PM<br>11/3/2020 85-55 PM<br>11/3/2020 85-755 PM  | 37-197 Number of c<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tack C.,.<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None   |                      |
| ve-EMS Sys<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 0-5846 PM<br>11/3/2020 0-5846 PM<br>11/3/2020 0-5846 PM<br>11/3/2020 0-5846 PM<br>11/3/2020 0-5843 PM<br>11/3/2020 0-5843 PM<br>11/3/2020 0-5843 PM<br>11/3/2020 0-5843 PM   | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>D None<br>O None<br>O None<br>O None<br>D None<br>O None<br>O None<br>O None<br>O None<br>O None   | Archive-IMSC<br>Level<br>@Informatio<br>Dinformatio<br>Dinformatio<br>Dinformatio<br>Dinformatio<br>Dinformatio<br>Dinformatio<br>Dinformatio<br>Dinformatio  | ystem 2020-11-05-17-16<br>Date and Time<br>11/3/2020 8/58/21 PM<br>11/3/2020 8/58/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/35 PM<br>11/3/2020 8/57/35 PM  | 37-197 Number of o<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None<br>0 None  |                      |
| ve-EMS Sys<br>terministics<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation  | tem-2020 - 11 - 05 - 17 - 16 -<br>Date and Time<br>11/3/2020 B 50:46 PM<br>11/3/2020 B 50:46 PM<br>11/3/2020 B 50:36 PM<br>11/3/2020 B 50:36 PM<br>11/3/2020 B 50:36 PM<br>11/3/2020 B 50:34 PM<br>11/3/2020 B 50:34 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>D None<br>O None<br>O None<br>O None<br>D None<br>D None<br>O None<br>O None<br>O None<br>O None<br>O None   | Archive-IMS2<br>Level<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio   | ysterm 2020-11-05-17-16<br>Date and Time<br>11/3/2020 83:821 PM<br>11/3/2020 85:365 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:725 PM<br>11/3/2020 85:725 PM  | 37-197 Number of e<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 None  |                      |
| ver EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | tem-2020 - 11 - 05 - 17 - 16 -<br>Date and Time<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:36 PM<br>11/3/2020 B 58:36 PM<br>11/3/2020 B 58:34 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>D None<br>O None<br>O None<br>O None<br>D None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None   | Archive-IMSI<br>Level<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio   | system: 2020-11-05-17-16<br>Date and Time<br>11/3/2020 85-821 PM<br>11/3/2020 85-826 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-725 PM   | 37-197 Number of a<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Tack C.,.<br>0 None<br>0 None   |                      |
| ve-EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | stem: 2020-11-05-17-16-<br>Date and Time<br>11/2/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM   | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>D None<br>O None<br>O None<br>O None<br>D None<br>D None<br>O None   | Archve-FMSI<br>Level<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio  | ystem 2020-11-05-17-16<br>Date and Time<br>11/3/2020 858/21 PM<br>11/3/2020 858/25 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85755 PM<br>11/3/2020 85725 PM<br>11/3/2020 85725 PM<br>11/3/2020 85725 PM<br>11/3/2020 85725 PM<br>11/3/2020 85725 PM  | 37 197 Number of e<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 None  |                      |
| ve-EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 8:584-6 PM<br>11/3/2020 8:584-6 PM<br>11/3/2020 8:584-6 PM<br>11/3/2020 8:584-6 PM<br>11/3/2020 8:584-6 PM<br>11/3/2020 8:584-6 PM<br>11/3/2020 8:584-7 PM<br>11/3/2020 8:5845-7 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None<br>O None<br>O None<br>U None<br>U None<br>O None<br>O None<br>O None<br>U None<br>O None<br>O None<br>O None<br>O None<br>O None   | Archive-IMSI<br>Level<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio   | ysterm 2020-11-05-17-16<br>Date and Time<br>11/3/2020 853621 PM<br>11/3/2020 85362 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM  | 37-197 Number of a<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  |                      |
| ve-EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation  | stem-2020 - 11 - 05 - 17 - 16 -<br>Date and Time<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:36 PM<br>11/3/2020 B 58:36 PM<br>11/3/2020 B 58:34 PM<br>11/3/2020 B 58:35 PM<br>11/3/2020 B 57:55 PM<br>11/3/2020 B 57:55 PM   | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>D None<br>O None<br>O None<br>O None<br>D None<br>D None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None   | Archive-EMSI<br>Level<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio   | system 2020-11-05-17-16<br>Date and Time<br>11/3/2020 85-821 PM<br>11/3/2020 85-825 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM   | 37-197 Number of o<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 None  |                      |
| vec EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation  | stem: 2020-11-05-17-16-<br>Dete and Time<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55854 PM<br>11/3/2020 55854 PM<br>11/3/2020 55854 PM<br>11/3/2020 55854 PM<br>11/3/2020 5555 PM<br>11/3/2020 55755 PM<br>11/3/2020 55755 PM  | S7-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>D None<br>O None<br>O None<br>O None<br>D None<br>D None<br>O None<br>O None<br>D None<br>D None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None<br>O None   | Archive-IMSI<br>Level<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio   | system 2020-11-05-17-16<br>Date and Time<br>11/3/2020 85-821 PM<br>11/3/2020 85-825 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM<br>11/3/2020 85-725 PM   | 37 197 Number of o<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  |                      |
| ver EMS Sys<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | tem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 95845 PM<br>11/3/2020 95755 PM<br>11/3/2020 95755 PM<br>11/3/2020 95755 PM<br>11/3/2020 95755 PM<br>11/3/2020 95755 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U Nane<br>O None<br>O None<br>O None<br>U None<br>U None<br>O None<br>O None<br>O None<br>U None<br>O None   | Archive-EMS3<br>Level<br>I Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio   | ystem 2020-11-05-17-16<br>Date and Time<br>11//2/2020 853/21 PM<br>11/3/2020 853/25 PM<br>11/3/2020 853/55 PM<br>11/3/2020 853/55 PM<br>11/3/2020 853/55 PM<br>11/3/2020 853/55 PM<br>11/3/2020 853/55 PM<br>11/3/2020 853/25 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  |                      |
| ver EMS System<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | stem-2020 - 11-05-17-16-<br>Dete and Time<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:46 PM<br>11/3/2020 B 58:36 PM<br>11/3/2020 B 58:34 PM<br>11/3/2020 B 58:35 PM<br>11/3/2020 B 57:55 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>D None<br>O None<br>O None<br>O None<br>D None<br>D None<br>O None   | Archive-IMSI<br>Level<br>I informatio<br>I informat   | ystem 2020-11-05-17-16<br>Date and Time<br>11/3/2020 85-821 PM<br>11/3/2020 85-821 PM<br>11/3/2020 85-755 PM<br>11/3/2020 85-725 PM  | 37-197 Number of o<br>Source<br>EMS User Log<br>EMS User Log  | Event ID         Tack C           0         None   |                      |
| vec EMS System<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation  | stem-2020-11-05-17-16-<br>Date and Time<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55755 PM  | S7-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>D None<br>O None<br>O None<br>O None<br>D None<br>D None<br>O None   | Archive-TMS:<br>Level<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformati   | ysterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 83-821 PM<br>11/3/2020 85-355 PM<br>11/3/2020 85-352 PM<br>11/3/2020 85-352 PM<br>11/3/2020 85-35 PM<br>11/3/2020 85-35 PM<br>11/3/2020 85-35 PM<br>11/3/2020 85-364 PM<br>11/3/2020 85-46 PM<br>11/3/2020 85-64 PM   | 37-197 Number of c<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 |                      |
| ver EMS System<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | tem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 9584-5 PM<br>11/3/2020 95755 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None<br>O None<br>O None<br>U None<br>O None   | Archive-EMS:<br>Level<br>I informatio<br>I informat   | System 2020-11-05-17-16<br>Date and Time<br>11//2/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85352 PM<br>11/3/2020 85352 PM<br>11/3/2020 85352 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85457 PM<br>11/3/2020 85457 PM<br>11/3/2020 85457 PM<br>11/3/2020 85451 PM<br>11/3/2020 85451 PM<br>11/3/2020 85451 PM<br>11/3/2020 85451 PM<br>11/3/2020 85451 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID         Tack C           0         None   |                      |
| ver EMS System<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | stem-2020-11-05-17-16-<br>Date and Time<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55755 PM  | S7-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tesk C<br>D None<br>O None<br>O None<br>O None<br>D None<br>D None<br>O None   | Archive-TMS:<br>Level<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformatice<br>Chiformati   | System 2020-11-05-17-16<br>Date and Time<br>11//2/2020 8/58/21 PM<br>11/3/2020 8/58/25 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/55 PM<br>11/3/2020 8/57/25 PM<br>11/3/2020 8/5/25 PM<br>11/3/2020 8/5/25 PM<br>11/3/2020 8/5/25 PM<br>11/3/2020 8/5/25 PM  | 37-197 Number of c<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 |                      |
| vec-EMS System<br>I formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation   | tem-2020-11-05-17-16-2<br>Date and Time<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55836 PM<br>11/3/2020 55836 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55755 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None   | Archive-EMS:<br>Level<br>I informatio<br>I informat   | System 2020-11-05-17-16<br>Date and Time<br>11//2/2020 8/58/21 PM<br>11/3/2020 8/58/25 PM<br>11/2/2020 8/57/55 PM<br>11/2/2020 8/57/55 PM<br>11/2/2020 8/57/55 PM<br>11/2/2020 8/57/55 PM<br>11/2/2020 8/57/55 PM<br>11/2/2020 8/57/55 PM<br>11/2/2020 8/57/25 PM<br>11/2/2020 8/5/25 PM<br>11/2/2020 8/5/25 PM<br>11/2/2020 8/5/25 PM<br>11/2/2020 8/5/25 PM<br>11/2/2020 8/5/25 PM   | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID         Tack C           0         None   |                      |
| ore Information<br>wee EMIS System<br>if demation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formatio  | tem-2020-11-05-17-16-2<br>Date and Time<br>11/3/2020 55845 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55845 PM<br>11/3/2020 55835 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55755 PM<br>11/3/2020 55725 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None   | Archive-EMSC<br>Level<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio | System 2020-11-05-17-16<br>Date and Time<br>11//2/2020 858-21 PM<br>11/3/2020 858-25 PM<br>11/3/2020 85755 PM<br>11/3/2020 85725 PM<br>11/3/2020 85647 PM<br>11/3/2020 85641 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID         Tack C           0         None   |                      |
| ore Information<br>wee EMIS System<br>if demation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formatio  | tem-2020-11-05-17-16-2<br>Date and Time<br>11/3/2020 55845 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55845 PM<br>11/3/2020 55835 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55755 PM<br>11/3/2020 55725 PM  | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None   | Archive-EMS:<br>Level<br>I informatio<br>I informat   | System 2020-11-05-17-16<br>Date and Time<br>11//2/2020 858-21 PM<br>11/3/2020 858-25 PM<br>11/3/2020 85755 PM<br>11/3/2020 85725 PM<br>11/3/2020 85647 PM<br>11/3/2020 85641 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID         Tack C           0         None   |                      |
| Iver EMS Systems<br>Information<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>afor   | stem-2020-11-05-17-16-<br>Date and Time<br>11/3/2020 95844 PM<br>11/3/2020 95844 PM<br>11/3/2020 95844 PM<br>11/3/2020 95844 PM<br>11/3/2020 95834 PM<br>11/3/2020 95835 PM<br>11/3/2020 95835 PM<br>11/3/2020 95735 PM<br>11/3/2020 95725 PM<br>11/3/200 95725 PM<br>11/3/200 | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event D Task C<br>0 None<br>0 N | Archive-IMS3<br>Level<br>I Informatio<br>I I Informatio<br>I I I I I I I I I I I I I I I I I I I  | System 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85351 PM<br>11/3/2020 85546 PM<br>11/3/2020 85546 PM<br>11/3/2020 85546 PM<br>11/3/2020 85546 PM<br>11/3/2020 85546 PM   | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  | Isuccessfully.       |
| Ince Information<br>ince EMIS System<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>informat  | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-36 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:57-55 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/200 8:57-                     | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>U None<br>O None   | Archive-IMS3<br>Level<br>I Informatio<br>I I Informatio<br>I I I I I I I I I I I I I I I I I I I  | Sterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85365 PM<br>11/3/2020 85365 PM<br>11/3/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID         Tack C           0         None   | I successfully.      |
| Iver EMS Systems<br>Information<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>aformation<br>afor   | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-36 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:57-55 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/200 8:57-                     | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event D Task C<br>0 None<br>0 N | Archive-IMS3<br>Level<br>I Informatio<br>I I Informatio<br>I I I I I I I I I I I I I I I I I I I  | Sterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85365 PM<br>11/3/2020 85365 PM<br>11/3/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  | Isuccessfully.       |
| ere Information<br>iver EMIS Systemation<br>of emation<br>of ema  | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-36 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:57-55 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/200 8:57-                     | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event D Task C<br>0 None<br>0 N | Archive-IMS3<br>Level<br>I Informatio<br>I I Informatio<br>I I I I I I I I I I I I I I I I I I I  | Sterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85365 PM<br>11/3/2020 85365 PM<br>11/3/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  | I successfully.      |
| ere Information<br>iver EMIS Systemation<br>of emation<br>of ema  | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-36 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:57-55 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/200 8:57-                     | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event D Task C<br>0 None<br>0 N | Archive-IMS3<br>Level<br>I Informatio<br>I I Informatio<br>I I I I I I I I I I I I I I I I I I I  | Sterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85365 PM<br>11/3/2020 85365 PM<br>11/3/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  | I successfully.      |
| Ince Information<br>ince EMIS System<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>information<br>informat  | stem-2020-11-05-17-16-3<br>Date and Time<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-46 PM<br>11/3/2020 8:58-36 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:58-34 PM<br>11/3/2020 8:57-55 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/2020 8:57-57-50 PM<br>11/3/200 8:57-                     | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event D Task C<br>0 None<br>0 N | Archive-EMSC<br>Level<br>Chiformatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio  | Sterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85365 PM<br>11/3/2020 85365 PM<br>11/3/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  | Isuccessfully.       |
| ere Information<br>iver EMIS Systemation<br>of emation<br>of ema  | tem-2020-11-05-17-16-2<br>Date and Time<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55846 PM<br>11/3/2020 55836 PM<br>11/3/2020 55836 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55834 PM<br>11/3/2020 55755 PM<br>11/3/20 | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event D Task C<br>0 None<br>0 N | Archive-IMS3<br>Level<br>I Informatio<br>I I Informatio<br>I I I I I I I I I I I I I I I I I I I  | Sterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85352 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85325 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85365 PM<br>11/3/2020 85365 PM<br>11/3/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Task C<br>0 None<br>0 None  | I successfully.      |
| ore Information<br>www.EMS System<br>Information<br>of emation<br>of emation<br>o   | stem: 2020-11-05-17-16-<br>Dete and Time<br>11/3/2020 558-45 PM<br>11/3/2020 55755 PM<br>11/3/2020 55725 P   | SI-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event (D Tesk C<br>0 None<br>0  | Archive-EMSC<br>Level<br>Chiformatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio<br>Informatio  | System 2020-11-05-17-16<br>Date and Time<br>11/3/2020 85362 PM<br>11/3/2020 85365 PM<br>11/3/2020 85755 PM<br>11/3/2020 85725 PM<br>11/3/2020 85647 PM<br>11/3/2020 85548 PM<br>11/3/2020 85548 PM<br>11/3/2020 85548 PM   | 37 197 Number of o<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Tack C<br>0 None<br>0 None  | I successfully.      |
| ver EMS System<br>I demation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>forma  | Atem-2020-11-05-17-16-3 Date and Time 11/3/2020 6584-6 PM 11/3/2020 65854-6 PM 11/3/2020 65855 PM 11/3/2020 65755 PM 11/3/2020 65751 PM 11/3/200 11/3/200 65751 PM 11/3/200 11   | S7-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>0 None<br>0 None   | Xrchive-IMSS<br>Level<br>I Informatio<br>I Informat   | Sterm 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85321 PM<br>11/3/2020 85305 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85355 PM<br>11/3/2020 85325 PM<br>11/3/2020 85326 PM<br>11/3/2020 85546 PM  | 37 197 Number of a<br>Source<br>EMS User Log<br>EMS User Log  | Event ID         Task C           0         None   | I successfully.      |
| vec EMS System<br>in formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>for  | stem-2020-11-05-17-16-3 Date and Time 11/3/2020-9584-6 PM 11/3/2020-9584-7 PM 11/3/2020-9584-7 PM 11/3/2020-9584-7 PM 11/3/2020-95755 PM 11/3/2020-95725 PM 11/3/200 11/3/200 11/3   | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event ID Task C<br>D None<br>O None   | Archive-EMSC<br>Level<br>Carlot Level<br>Carlot Informatio<br>Carlot Informatio   | System 2020-11-05-17-16<br>Date and Time<br>11//2/2020 85320 PM<br>11//2/2020 85325 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85352 PM<br>11//2/2020 85352 PM<br>11//2/2020 85352 PM<br>11//2/2020 85355 PM<br>11//2/2020 85365 PM<br>11//2/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Tack C<br>0 None<br>0 | successfully.        |
| vec EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>format | stem: 2020-11-05-17-16-<br>Date and Time<br>11/3/2020 558-45 PM<br>11/3/2020 5575 PM<br>11/3/2020 55755 PM<br>11/3/2020 55725 PM   | SI-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event (D) Task C<br>0 None<br>0 | Archive-TMS:<br>Level<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio | istem 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85:821 PM<br>11/3/2020 85:306 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:725 PM<br>11/3/2020 85:745 PM<br>11/3/2020 85   | 37 197 Number of o<br>Source<br>ENS User Log<br>ENS User Log<br>EN  | Event ID         Tack C           0         Nome   | I successfully.      |
| vec EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>format | stem-2020-11-05-17-16-3 Date and Time 11/3/2020-9584-6 PM 11/3/2020-9584-7 PM 11/3/2020-9584-7 PM 11/3/2020-9584-7 PM 11/3/2020-95755 PM 11/3/2020-95725 PM 11/3/200 11/3/200 11/3   | 37-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event (D) Task C<br>0 None<br>0 | Archive-IMSS<br>Level<br>I formatio<br>I informatio<br>I I informatio<br>I informat   | System 2020-11-05-17-16<br>Date and Time<br>11//2/2020 85320 PM<br>11//2/2020 85325 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85355 PM<br>11//2/2020 85352 PM<br>11//2/2020 85352 PM<br>11//2/2020 85352 PM<br>11//2/2020 85355 PM<br>11//2/2020 85365 PM<br>11//2/2020 85546 PM  | 37-197 Number of e<br>Source<br>ENS User Log<br>ENS User Log  | Event ID Tack C<br>0 None<br>0 | Fsuccessfully.       |
| vec EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>format | stem: 2020-11-05-17-16-<br>Date and Time<br>11/3/2020 558-45 PM<br>11/3/2020 5575 PM<br>11/3/2020 55755 PM<br>11/3/2020 55725 PM   | SI-197 Number of<br>Source<br>EMS User Log<br>EMS User Log  | Event (D) Task C<br>0 None<br>0 | Archive-TMS:<br>Level<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio<br>informatio | istem 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85:821 PM<br>11/3/2020 85:306 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:725 PM<br>11/3/2020 85:75 PM<br>11/3/2020 85:75 PM<br>11/3/2020 85:75 PM<br>11/3/2020 85 | 37 197 Number of o<br>Source<br>ENS User Log<br>ENS User Log<br>EN  | Event ID         Tack C           0         Nome   | Fsuccessfully.       |
| ve-EMS Systemation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formation<br>formati | stem: 2020-11-05-17-16-<br>Date and Time<br>11/3/2020 558-45 PM<br>11/3/2020 5575 PM<br>11/3/2020 55755 PM<br>11/3/2020 55725 PM   | 37-197 Number of<br>Source<br>EMS User Log<br>EMS Use | Event (D) Task C<br>0 None<br>0 | Archive-IMS3     Level     Control Contro Control Control Control Control Control   | istem 2020-11 05-17-16<br>Date and Time<br>11/3/2020 85:821 PM<br>11/3/2020 85:306 PM<br>11/3/2020 85:755 PM<br>11/3/2020 85:725 PM<br>11/3/2020 85:75 PM<br>11/3/2020 85:75 PM<br>11/3/2020 85:75 PM<br>11/3/2020 85 | 37-197 Number of a<br>Source<br>ENS User Log<br>ENS U | Event ID         Tack C           0         Nome   | I successfully.      |

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

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

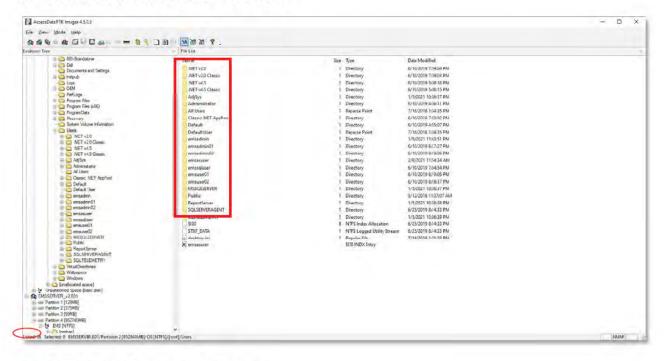
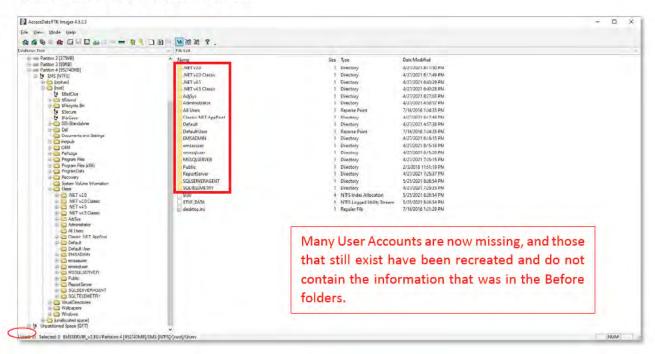


Figure 35 - EMS Server (5.13) System Users After



# 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

| AccessData FIK Image   |   |                            |  |  | - 5   |
|--|---|----------------------------|--|--|---|
| e View Mode H  |   |                            |  |  |   |
| a 44 % ⊂ 48 £  | 998448 - 64   | 日回 医激激激 1 .                |  |  |   |
| dence Tree   |   | 8 File List                |  |  |   |
| - us Patton 2 (9538  | I3MB]   | A Name                     | Size Bype  | Date Modified  |   |
| OS INTEST  |   | \$130                      |  | 523/2021 R07/15 PM   |   |
| (i) 📮 (vekan)  |   | ErrevOllog                 | 4,999 Regular File   | 5/23/2021 b07:00 PM  |   |
| S 18m  | 0.1   | Errou0.tog.FileStack       | 2 File Stack   |  |   |
| 11-C 564   |   | Drost Log                  | 4,999 Regular File   | 5/21/2021 - 22-18 PM   |   |
| 18 😂 \$Per   |   | Erro, 1.log FileSlack      | 2 File Stack   | and the second se  |   |
| 1ª SSec  |   | Error 10.log               | 4.000 Regular File   | 5/21/2021 (2:19:56 AM  |   |
| B 001  |   | Error, 20.log, FileSlack   | 2 File Stack   | and the second se  |   |
| d Del  |   | Error.11.log               | 4999 Reputer File  | 5/20/2021 x55:14 PM  |   |
|  | everyta and Deterings.  | Errout2.tog                | 4,939 Regular File   | 5/20/2021 (1:10/31 AM  |   |
| (i) 💭 Initia   |   | Error, 12.log FleSlack     | 2 File Stack   |  |   |
| Logi   |   | Error, 13.log              | 4999 Reputer File  | 5/20/2021 4:25:49 AM   |   |
| () Cal OCH   |   | Errol, 13.log FileSlack    | 2 File Slack   |  |   |
| III C Prog   |   | Errol 14Jog                | 4,999 Regular File   | 5/19/2021 k41:06 PM  |   |
|  | rain Paga si200   | K trro. 14.log             | 9,773 Regular Free   | 12/8/2020 R06-44 PM  |   |
| ili 😂 Prog   | semData   | Error, 14.log FileSlack    | 2 File Slack   |  |   |
| E Peco   |   | Free.2.log                 | 4999 Repulse File  | 5/29/2021 9:97:35 AM   |   |
| Ti Ca User   | en Volumi Information   | Croc2.log.FileSlack        | 2 File Stack   |  |   |
|  | Directories   | Imp.J.log                  | 4,999 Regular File   | 5/22/2021 (15:52:53 PM   |   |
| 60   | IMSApplicationServer  | C Errol Ling FileSlack     | 2 File Stack   |  |   |
|  | App_Code  | Errou4.tog                 | 4,000 Reputer File   | 5/22/2021 Sole 1T PM   |   |
|  | a bin   | Inout.log.FileSlack        | 2 File Slack   | And the second states of the s |   |
|  | a cons  | Error, Silog               | 4,999 Reputer File   | 3/22/2021 (0:23-28 AM  |   |
|  | Reports   | Error, S. Jog, FileSlack   | 2 File Stack   |  |   |
|  | Aesoupes  | Erreifolog                 | 4999 Regular File  | 5/22/2021 3-38-46 AM   |   |
|  | Securty   | Errol & log FilrSlack      | 2 File Stack   |  |   |
| 🗄 🔁 Wat  | papers .  | Erras 7.5ag                | 4,000 Regular File   | 5.21/2021 3.54/04 PM   |   |
| (i) 😂 West   | lows  | Erros 7.log.FileSlack      | 2 File Slack   |  |   |
| pertis   |   | ErrouB.log                 | 4,999 Require File.  | 5/21/2021 2:09:21 PM   |   |
| 21   |   | Errol & log FileSlack      | 2 File Slack   |  |   |
|  |   | ErrorSilog                 | 4,999 Regular File   | 5/21/2021 1:24 38 AM   |   |
|  |   | Erreifling Fildlack        | 2 Tite Stack   |  |   |
| Name   | Contraction in the local data   | Cirror.log                 | 1,775 Regular File   | 5/23/2021 10:30:56 PM  |   |
| File Class   | Population (14)   | Erroslog,FileStack         | 9 File Slack   |  |   |
| File Size  |   | WanJog                     | 1,970 Regular File   | 5/14/2021 3:30:57 PM   |   |
| Physical Size  | CHIEF   | 12                         |  |  |   |
| Start Cluster  |   | Present 1019 Grand June    | tion Municipal Election Users  | min Theradi 64   | A DECEMBER OF A |
| Date Accessed  | IN HERE OF A REAL PROPERTY OF A |                            |  | essageRpc.Frocess => InsutableDispatchRuntime.ProcessNessag<br>ess for project: 2019 Grand Junction Municipal Election has   | gell => ImmutableDispatuhkuntime.ProcessMessages => Dispatch/perationRunti  |
| Date Created   | and the second second second  |                            | ion Municipal Election User:   |  | a anoneseratel combracad.   |
| DateModified   | AVAID 111 ASSID IN A  | Call stack: ChannelHand    | ler.HandleRequest => ChannelB  | dler.DispatchAndReleasePunp => MessageRpc.Process => Immuta  | ableDispatchRuntime.ProcessNessagel1 => ImmutableDispatchRuntime.ProcessNe  |
| Encripted  | Polar.  | 2020-12-05 09:31:19.9992   | Enslogger Elector group Defe   | t is not part of any ballot group.   |   |
| Compressed   | inter .   |                            | ion Municipal Election Deer  |  |   |
|  |   |                            |  | > DispatchOperationAuntime.InvokeBegin => SyncheshodInvokes<br>t is not part of any ballot group.  | E'ILAOK4 ->   |
| Actual File  | 10.am   |                            | iten Hunicipal Elector Group Ders  |  |   |
| Start Sector   | Lineau  |                            |  | > DispatchOperationRuntime.InvokeBegin => SyncNechodInvoker  | n.Invoke =>   |
| DOS Attributes   |   | 2020-12-00 10:14:57.3254   | Deservice Sallot a)  | #(2B-Ballot 2 - Type 2-1.pdf)#   |   |
| nidom .  | A second  | " Reyword 'Qais' is not at | apported for "Contest City Co  | cil At Large' object.  |   |
|  |   |                            |  | in which a   |   |
|  |   |                            | ion Municipal Election Caer:   |  | umedettodinfy.Invose -> Pantimedethodinfo.UnsafeInvokeInternal -> Pantime   |
| opertes No Tableton  | (and ) seed when  | Call starst Raildordule.   | the state of the s | ALL DESCRIPTION OF THE PROPERTY OF THE PROPERT | cannot cryainity, involv -> vantamente cholinity. Unsattiny oxiinite ini -> pantamente  |
| All second secon | SERVER-E01/Particion 2 (912843MB)   | 11                         |  |  |   |

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

| AccessData FTK ImagerA.<br>e Siew Mode Help   |   |   |  |  |  |  |
|---|---|---|--|--|--|--|
|   | - C   | 1 10 10 10 10 10  |  |  |  |  |
| ince Tree   |   | < file List   |  |  |  |  |
| Pattor 3 (99MB)   |   | n Name  | Size Type  | Date Modified  |  |  |
| Perilign  | i Bin<br>didana<br>didana<br>Rea<br>rea end Settraja<br>Dea<br>7<br>Volume Homatori<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ectore<br>ec | incologi<br>Incologi<br>Weening   | 1 File Slick   | 5/26/221 3 863 PM  | All previous log files are gone.   |  |
| ili 🛆 Waloop<br>ili 🔾 Wedow<br>eties  | in<br>Secution<br>Secution  | * N   |  |  |  |  |
| arre<br>le Class<br>le Sois<br>le Sois<br>et Souker<br>ant Churker<br>ant Churker | Annuary<br>Annuary<br>Altri<br>Altri<br>Altria<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Annuary<br>Ann  | Project: User: Thread: J<br>Call stack: XanDoi scoli<br>2021-04-27 14:02103.2730<br>Call stack: MostingTread<br>Call stack: NostingTread<br>Discourse Thread Scole<br>Project: Dest Thread Scole<br>Project: Disc Thread Scole<br>Project: Disc Thread Scole<br>Project: Disc Thread Scole<br>Project: Dest Thread Scole<br>Project: User: Thread Scole<br>Project: User: Thread Scole<br>Project: User: Thread Scole | lien.Neitedtarthemmen => Xuell<br>Emalogger Temp path is not set<br>Comment.Institute => Nortineff<br>Massager !!! Application End<br>Start.Sunfframmal => Herpfurmin<br>Finaloger Entainase upoble<br>a TM id anch ENG SFA UserAAdu<br>e Hauldebumgat => Channelka<br>Results Service /!! Applicati<br>9. | . default windows temp<br>vyronment.Initialize vo.<br>117<br>us.Belesselseourceskudd<br>bese for project; 5 13 F<br>is Thread: 33<br>wins. Dispatchkaddelesse<br>pp End. 111 | Wholdssignibly restrictions of ChObjectRuntime.CreateInstance => XamiTypeInvokes.Create<br>Interviewy will be used!<br>CodeBitrectoryCompiler_SalikgoInitializeNethod => RunidSewicHairCodeAssembly.Calik<br>IosdSppGomain => NitpRontime.Sispone => NitpApplioximeFectory.Bisgone => NitpAppli<br>Mong => NessageNps.Fectore => PenetableNispataNEurita.Fectory.Bisgone => NitpApplis<br>LeadBpgDomain => RitpRuntime.Dispone => NitpAppliantimeFactory.Bisgone => NitpApplis | rolnizializeMethod => Au<br>nationFactory.FireApplio<br>OlepscokOurtes.Twonese |
| IOS Attributes<br>Edition   |   |   |  |  |  |  |
|   | and and a set house 1   |   |  |  |  |  |

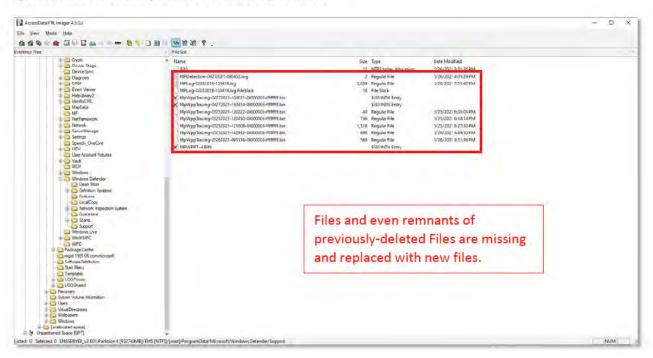
## Server Windows Defender Log Files Missing/Overwritten

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

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

| AccessData FTK Imager 45.0.3                              |  |                          |   | - 0   |
|---|--|--------------------------|---|-------|
| s Yoriv Mode Help   |  |                          |   |       |
| 6846 GHE  | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1  |                          |   |       |
| ince litee  | 2 File Det   |                          |   |       |
| N Copta   |  |                          | a state state   |       |
| Device Stage  | and the second s | Size Type                | Date Modified   |       |
| Device Sysc   | K MpWppfracing-06102019-131140-00000003-######.bin   | \$30 INDX Entry          |   |       |
| b) 🔄 Diagnosa   | X MPWPPT-4.8IN   | \$10 INDX Entry          |   |       |
| 🗄 😋 рим   | MPLog-03072021-120430.log.PiteSlack  | 33 File Slack            |   |       |
| E Event Verwer  | MPLog-03082021-184449.log.F/eSlack   | 4 File Stack             | and the second se |       |
| H Co HelpLExay2   | 3100   | 12 NTES Index Allocation | 1/7/2021 6:04:50 PM   |       |
| HTML Hep<br>) Californity CRL                             | MpWppTracing-033020/1-092026-00000003-(fffffff.bin   | 160 Regular File         | 1/30/2001 3:25:41 PM  |       |
| MapData   | MpWppTracing 031820(1+105340-00000003-HHHHH).bim   | 228 Regular File         | 3/18/2021 4/58/41 PK4   |       |
| MF NF   | MPDetection-03182021-105340Jog   | 1 Regular file           | 5/18/2021 5:10:25 PM  |       |
| 1) Can Net Framework                                      | MpWppfracing-010520/1+164513-00000008-ffffffff.bin   | 4,096 Regular File       | 3/18/2001 4:51:51 PM  |       |
| k) Ca feiterick   | MpWpphacing 03302021-093016-00001003-I/HIMLEin   | 4.050 Regular file       | 3/30/2021 3/30/05 PM  |       |
| k) ServerManager  | MPLog-05072021-120450.log  | 16.224 Regular life      | 5/23/20/1 10:0251 PM  |       |
| 10 🗂 Settanga   | MPLog-07082071-18449Lbg  | 33,773 Regular File      | 5/7/2021 4:04:51 PM   |       |
| Sevenils_DreeCom  |  | 1,180 Regular File       |   |       |
| le 😋 LEV  | MpWppFracing-03182021 110015-00000003-IIIIIIIII.bm   |                          | 5/30/2021 3:18:59 PM  |       |
| User Account Pictures                                     | MpWppTracing-06252019-105514-00000003-fffffffff.bin  | 4,090 Regular file       | 6/25/2019 5:18:03 PM  |       |
| O WDF   | K MpWppTracing-06252019-105548-00000003-fffffffff.bin  | 36 Regular file          | 6/25/2019 4:56:19 PM  |       |
| () C Windows  | MpWppFracing-06122019-150811-00000003-ffffffff.bin   | 2,036 Regular File       | 6/12/2019 9:24:41 PM  |       |
| U City Windows Defender                                   | K) MpWpphacing-06112019-094455-00006003-I/I/I/I/I.bin  | 376 Regular Nec          | 6/11/2019 3:56.45 PM4   |       |
| Clean Store   | MpWppTracing-06102019-100354-00000003-ffffffff.bin   | 132 Regular File         | 6/10/2019 5:09:20 PM  |       |
| Defessor Updates  | MPDetection-06102019-095254/ag   | 2 Regular File           | 6/26/2019 10:10:24 PM   |       |
| C Features  | MpWppfracing-06102019-133117-00000003-ffffffff.bin   | 48 Regular File          | 6/10/2019 7:35/14 PM  |       |
| incallery   | MpWppTracing-06102019-101810-00000003-ffffffff.bin   | 116 Regular file         | 6/10/2019 5:24:14 PM  |       |
| 🗈 🤐 Network Impaction System                              | X MpWppTracing-05102019-102610-00000003-ffffffff.bin   | 72 Regular File          | 6/10/2019 5:27:32 PM  |       |
| Guarantere<br>18 Go Scans                                 | X MpWppTracing 09032019-122548-00000003-###### bin   | 1,508 Regular File       | 9/4/2019 8:37:56 PM   |       |
| Suppon  | MPDetection -00032019-1225472org   | 2 Regular File           | 10/21/2018 5-1835 PM  |       |
| Windows Live  | x MPLog-09122015-043440.log  | 0 Regular File           | 12/14/2020 10:51:33 PM  |       |
| U CO WnMSIPC  | K + tog officion owneddy   | a regulation too         | 10 THE CALL THE DWIDT FIRE  |       |
| CO WPD  |  |                          |   |       |
| 11/ 💭 Package Cache                                       |  |                          |   |       |
| regid 1991 06.com/microsoft                               |  |                          |   |       |
| Software Distribution                                     |  |                          |   |       |
| Tomolates   |  |                          |   |       |
| USOPrivate  |  |                          |   |       |
| it G USOShared  |  |                          |   |       |
| HI CA Reservery   |  |                          |   |       |
| System Volume Information                                 |  |                          |   |       |
| (i) 🚞 (bars   |  |                          |   |       |
| (i) 💭 VitualDirectories                                   |  |                          |   |       |
| 🛞 😂 Walipapere  |  |                          |   |       |
| (a) Windows     (a) Carlocated space                      |  |                          |   |       |
| 1 Unpartitioned Space basic diki                          |  |                          |   |       |
| EMSSERVER +2 E01  | 1  |                          |   |       |
| Parttion 1 [128MB]  | Curror pos = 0   |                          |   |       |
| 2 25 Selected & EMSSERVER.E01/Partition 2 (952843MB/OS [N |  |                          |   | SUM . |

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



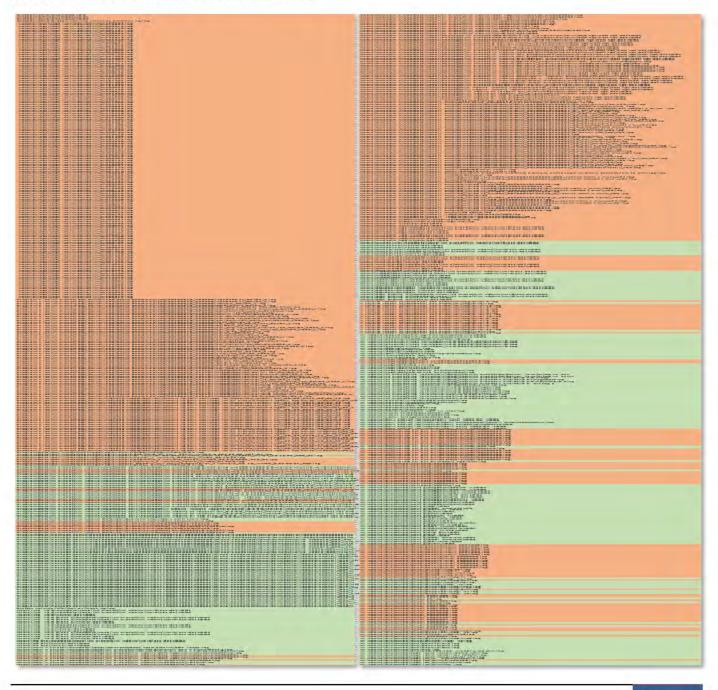
Server List of .log files in Before Image that were Deleted.

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

Each line in the image below is the full path listing to each one of the 807 files <u>that end with the word ".log" found</u> 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



| Users/Jddministrator/AppData/Local/Microsoft/Windows/WebCache/V010000Log         Win           Users/Jddministrator/AppData/Local/Microsoft/Windows/WebCache/V010000Clog         Win           Users/Jddministrator/AppData/Local/Wincos/Windows/WebCache/V010000Clog         Win           Users/Jddministrator/AppData/Local/Wincos/Windows/Lats.adaLLOG1         Win           Users/Jddministrator/AppData/Local/Wincos/Windows/Lats.adaLLOG2         Win           Users/Jddministrator/AppData/Local/Wincos/Windows/Lats.adaLLOG2         Win           Users/Jddministrator/AppData/Local/Wackages/Microsoft.AM.Dir/okerPlugin_cwfn1h2txyewy/Settings/Lettings.datLOG2         Win           Users/Jddministrator/AppData/Local/Packages/Microsoft.AM.Dir/okerPlugin_cwfn1h2txyewy/Settings/Lettings.datLOG2         Win           Users/Jddministrator/AppData/Local/Packages/Microsoft.Biofnrollment_cwfn1h2txyewy/Settings/Lettings.datLOG2         Win           Users/Jddministrator/AppData/Local/Packages/Microsoft.Biofnrollment_cwfn1h2txyewy/Settings/Lettings.datLOG2         Win           Users/Jddministrator/AppData/Local/Packages/Microsoft.Biofnrollment_cwfn1h2txyewy/Settings/Lettings.datLOG2         Win           Users/Jddministrator/AppData/Local/Packages/Microsoft.Biofnrollment_cwfn1h2txyewy/Settings/Lettings.datLOG2         Win           Users/Jddministrator/AppData/Local/Packages/Microsoft.LockApp_cwfn1h2txyewy/Settings/Lettings.datLOG2         Win           Users/Jddministrator/AppData/Local/Packages/Microsoft.Windows.Aporpc/DrxApp_cwfn1h2txyewy/Settings/Lettings.datLOG   | Vindows/System32LogFiles/Sum/Svc00167.10g Vindows/System32LogFiles/Sum/Svc00167.10g Vindows/System32LogFiles/Sum/Svc00168.10g Vindows/System32LSMI/Store/Machine/SCHEMA.DAT.LOG2 Vindows/System32LSMI/Store/Machine/SCHEMA.DAT.LOG2 Vindows/System32LSyspreps/Panther/USetupact.10g Vindows/System32LSyspreps/Panther/USetupact.10g Vindows/System32LSyspreps/Panther/Setupact.10g Vindows/System32LSystemS2LSpaseulia.10.10g Vindows/System32LSystemS2LSpaseulia.10.10g Vindows/System32LSystemS2LSpaseulia.10.10g Vindows/System32LSpaseulia.10.10g Vindows/System32LSpaseulia.10.10.10g Vindows                               |
|--|--|
| Users\/ddministrator\/AppDats\Local\/Microsoft\Windows\/UsrClass.datLOG1         Will           Users\/ddministrator\/AppDats\Local\/Microsoft\Windows\/UsrClass.datLOG1         Will           Users\/ddministrator\/AppDats\Local\/Microsoft\Windows\/UsrClass.datLOG2         Will           Users\/ddministrator\/AppDats\Local\/Microsoft\Windows\/UsrClass.datLOG2         Will           Users\/ddministrator\/AppDats\Local\/Packages\/Microsoft.AAD.BrokerPlugin_cw6n1h2txyewy\Settings\settings.datLOG1         Will           Users\/ddministrator\/AppDats\Local\Packages\/Microsoft.AAD.BrokerPlugin_cw6n1h2txyewy\Settings\settings\settings.datLOG2         Will           Users\/ddministrator\/AppDats\Local\Packages\/Microsoft.AAD.BrokerPlugin_cw6n1h2txyewy\Settings\settings\settings\settings\datLOG2         Will           Users\/ddministrator\/AppDats\Local\Packages\/Microsoft.AAD.BrokerPlugin_cw6n1h2txyewy\Settings\setting   | Vindows/System32\LogFiles/Sum/Svc00168.log<br>Vindows/System32\LogFiles/Sum/Svc.log<br>Vindows/System32\LogFiles/Sum/Svc.log<br>Vindows/System32\LogFiles/Sum/Svc.log<br>Vindows/System32\LogFiles/Sum/Svc.log<br>Vindows/System32\LogFiles/Sum/Svc.log<br>Vindows/System32\LogFiles/Sum/Svc.log<br>Vindows/System32\System22\System22\System32\Sys          |
| Users\/dministrator\/dppData\Local\/Microsoft\/Windows\/UsrClass.datLOG1         Win           Users\/dministrator\/dppData\Local\/Microsoft\/Windows\/UsrClass.datLOG2         Win           Users\/dministrator\/dppData\Local\/Wicrosoft\/Windows\/UsrClass.datLOG2         Win           Users\/dministrator\/dppData\Local\/Wicrosoft\/Windows\/UsrClass.datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/AbD.BrokerPlugin_cw5n1h2txyewy\Settings\settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/AbD.BrokerPlugin_cw5n1h2txyewy\Settings\settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/RabConterPlugin_cw5n1h2txyewy\Settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/RabConterPlugin_cw5n1h2txyewy\Settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/RabConterPlugin_cw5n1h2txyewy\Settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/RabConterPlugin_cw5n1h2txyewy\Settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/RabConterPlugin_cw5n1h2txyewy\Settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/LockApp_cw5n1h2txyewy\Settings\settings\datLOG2         Win           Users\/dministrator\/dppData\Local\/Package\/Microsoft\/LockApp_cw5n1h2txyewy\Settings\settings\datLOG2         Win  | Vindows/System32\LogFiles/Sum/Svc.log<br>Vindows/System32\MicrosoftProtect/Recovery/Recovery.datLDG1<br>Vindows/System32\MicrosoftProtect/Recovery/Recovery.datLOG2<br>Vindows/System32\MicrosoftProtect/Recovery/Recovery.datLOG2<br>Vindows/System32\MicrosoftProtect/Recovery/Recovery.datLOG2<br>Vindows/System32\MicrosoftProtect/Recovery/Recovery.datLOG2<br>Vindows/System32\MicrosoftProtect/Recovery/Recovery.datLOG2<br>Vindows/System32\MicrosoftProtect/Recovery.datLOG2<br>Vindows/System32\System2\System42\System42\System32\System       |
| Users\/Administrator\/AppData\Local\Packages\Microsoft.Windows\UsrClass.datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw6n1h2txyewy\Settings\settings\settings\datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw6n1h2txyewy\Settings\settings\datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw6n1h2txyewy\Settings\settings\datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.ABD.BrokerPlugin_cw6n1h2txyewy\Settings\settings\settings.datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw6n1h2txyewy\Settings\settings.datLOG1         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw6n1h2txyewy\Settings\settings.datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw6n1h2txyewy\Settings\settings.datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw6n1h2txyewy\Settings\settings.datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw6n1h2txyewy\Settings\settings.datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.LocApp_cw6n1h2txyewy\Settings\settings.datLOG2         Win           Users\/Administrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw6n1h2txyewy\Settings\settings.datLOG2         Win           Users\/Administrator\/AppData  | Vindows\System32\Microsoft\Protect\Recovery\Recovery.dat.L0G1<br>Vindows\System32\Microsoft\Protect\Recovery\Recovery.dat.L0G2<br>Vindows\System32\Microsoft\Protect\Recovery\Recovery.dat.L0G2<br>Vindows\System32\Microsoft\Protect\Recovery\Recovery.dat.L0G2<br>Vindows\System32\Microsoft\Protect\Recovery\Recovery.dat.L0G2<br>Vindows\System32\System32\SMI\Store\Machine\SCHEMA.DAT.L0G1<br>Vindows\System32\System32\System2\Panther\UE\setuper1.0g<br>Vindows\System32\System32\System2\Panther\UE\setuper1.0g<br>Vindows\System32\System32\System32\System2\Panther\setuper1.0g<br>Vindows\System32\System32\System2\Panther\setuper1.0g<br>Vindows\System32\System |
| Users\/dministrator\/dppData\\ucal\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2tsyewy\Settings\set  | Vindows/System32(Microsoft/Protect/Recovery/Bacovery.datL062<br>Vindows/System32(Microsoft/Protect/Recovery.datL062<br>Vindows/System32(Microsoft/MicroRel/CHEMA.DATL061<br>Vindows/System32(SMiCroRel/Machine/SCHEMA.DATL062<br>Vindows/System32(Systerp@inther/lE/Setupact.log<br>Vindows/System32(Systerp@inther/setupact.log<br>Vindows/System32(Systerp@inther/setupact.log<br>Vindows/System32(Systerp@inther/setupact.log<br>Vindows/System32(Syster@inter)@inther/setupact.log<br>Vindows/System32(System32)Sistem82(Sistem82)Sistem32(System32)Sistem32)Sistem32(System32)Sistem32)Sistem32(System32)Sistem32)Sistem32(System32)Sistem32)Sistem32(System32)Sistem32)Sistem32)Sistem32(System32)Sistem32)Sistem32)Sistem32(System32)Sistem32)Sistem32)Sistem32(System32)Sistem32)Sistem32)Sistem32)Sistem32)Sistem32(System32)Sistem3    |
| Users\/dministrator\/AppData\Loca\\Packages\Microsoft.AAD.BrokerPiugin_cw5n1h2txyewy\Settings\settings\satLIOG2         Wii           Users\/dministrator\/AppData\Loca\\Packages\Microsoft.AAD.BrokerPiugin_cw5n1h2txyewy\Settings\settings\satLIOG2         Wii           Users\/dministrator\/AppData\Loca\\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings\settings.dstLIOG2         Wii           Users\/dministrator\/AppData\Loca\\Packages\Microsoft.RccountsControl_cw5n1h2txyewy\Settings\settings.dstLIOG2         Wii           Users\/dministrator\/AppData\Loca\\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.dstLIOG2         Wii           Users\/dministrator\/AppData\Loca\\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.dstLIOG2         Wii           Users\/dministrator\/AppData\Loca\\Packages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Loca\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Lpackages\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Microsoft.Usets\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lpackages\Lp  | Vindows/System32(MaDtc/TraceIdtetraceIog<br>Vindows/System32(MaDtc/MSDTcLDG<br>Vindows/System32(SMI)Store/Machine/SCHEMA.DAT.LDG1<br>Vindows/System32(SMI)Store/Machine/SCHEMA.DAT.LDG2<br>Vindows/System32(Systere)Panther/US/etupaet.log<br>Vindows/System32(Systere)Panther/US/etupaet.log<br>Vindows/System32(Systere)Panther/Setuper.log<br>Vindows/System32(Systere)Panther/Setuper.log<br>Vindows/System32(Systere)Panther/Setuper.log  |
| Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.datLOG1         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.datLOG1         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.BioEnrollmem_cw5n1h2txyewy\Settings\settings.datLOG1         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.BioEnrollmem_cw5n1h2txyewy\Settings\settings.datLOG2         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.BioEnrollmem_cw5n1h2txyewy\Settings\settings.datLOG2         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.BioEnrollmem_cw5n1h2txyewy\Settings\settings.datLOG2         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.BioEnrollmem_cw5n1h2txyewy\Settings\settings.datLOG1         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.UccApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewySettings\settings.datLOG2         Wirit           Users\/ddministrator\/dopData\/Local\/Packages\/Microsoft.Windows.AsignedAccessLocApp_cw5n1h2txyewySettings\settings.datLOG2 <td>Vindows/System32(MsDtc/MSDTCLOG<br/>Vindows/System32(SMtDtre/Machine/SCHEMA.DAT.LOG1<br/>Vindows)System32(SMtDtre/Machine/SCHEMA.DAT.LOG2<br/>Vindows/System32(Sysprep)Panther/UE/setuper1.log<br/>Vindows/System32(Sysprep)Panther/UE/setuper1.log<br/>Vindows/System32(Sysprep)Panther/setuper1.log<br/>Vindows/System32(Sysprep)Panther/setuper1.log<br/>Vindows/System32(Sysprep)Panther/setuper2.log<br/>Vindows/System32(Sysprep)Panther/setuper2.log<br/>Vindows/System32(Sysprep)Panther/setuper2.log</td> | Vindows/System32(MsDtc/MSDTCLOG<br>Vindows/System32(SMtDtre/Machine/SCHEMA.DAT.LOG1<br>Vindows)System32(SMtDtre/Machine/SCHEMA.DAT.LOG2<br>Vindows/System32(Sysprep)Panther/UE/setuper1.log<br>Vindows/System32(Sysprep)Panther/UE/setuper1.log<br>Vindows/System32(Sysprep)Panther/setuper1.log<br>Vindows/System32(Sysprep)Panther/setuper1.log<br>Vindows/System32(Sysprep)Panther/setuper2.log<br>Vindows/System32(Sysprep)Panther/setuper2.log<br>Vindows/System32(Sysprep)Panther/setuper2.log   |
| Users\/dministrator\/AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.datLOG1         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.BioEnrolIment_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.UnckApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.datLOG2         Wii           Users\/dministr  | Vindows/System32\SMI\Store\Machine\SCHEMA.DATLOG1<br>Vindows/System32\SMI\Store\Machine\SCHEMA.DATLOG2<br>Vindows/System32\SysprepDranther\Estupact.log<br>Vindows/System32\SysprepDranther\setupact.log<br>Vindows/System32\SysprepDranther\setupact.log<br>Vindows/System32\                |
| Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2tyvewy\Settings\settings.dat.LOG1         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2tyvewy\Settings\settings.dat.LOG1         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2tyvewy\Settings\settings.dat.LOG1         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.EiloEnrollment_cw5n1h2tyvewy\Settings\settings.dat.LOG1         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.LockApp_cw5n1h2tyvewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.LockApp_cw5n1h2tyvewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.UnckApp_cw5n1h2tyvewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChuApp_cw5n1h2tyvewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChuApp_cw5n1h2tyvewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Local\Packages\Microsoft.Windows.Apprep.ChuApp_cw5n1h2tyvewy\Settings\setting   | Vindows/System32(SMI/Store/Machine/SCHEMA.DATLOG2<br>Windows/System32(Sysrepr0)Panther/US/stupact.log<br>Windows/System32(Sysrepr0)Panther/US/stupact.log<br>Windows/System32(Sysrepr0)Panther/setupact.log<br>Windows/System32(System32(Susrep)Panther/setupact.log<br>Windows/System32(Susrep)Panther/setupact.log   |
| Users/Administrator/AppData/Local/Packages/Microsoft/BioEnrollment_cw5n1h2tyvew/Settings/settings.datLOG2 Wii<br>Users/Administrator/AppData/Local/Packages/Microsoft/BioEnrollment_cw5n1h2tyvew/Settings/settings.datLOG3 Wii<br>Users/Administrator/AppData/Local/Packages/Microsoft/Evideos/Settings/S   | Windows\System32\Sysprep\Panther\E\setupact.log<br>Windows\System32\Sysprep\Panther\E\setupact.log<br>Windows\System32\Sysprep\Panther\setupact.log<br>Windows\System32\Sysprep\Panther\setupact.log<br>Windows\System32\System32\Susprep\Panther\setupact.log<br>Windows\System32\Susprep\Panther\setupact.log  |
| Users\/Administrator\/AppData\Loca\\Packages\MicrosoftLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1         Wii           Users\/Administrator\/AppData\Loca\\Packages\MicrosoftLockApp_cw5n1h2txyewy\Settings\settings\settings.dat.LOG1         Wii           Users\/Administrator\/AppData\Loca\\Packages\MicrosoftLockApp_cw5n1h2txyewy\Settings\settings\settings.dat.LOG1         Wii           Users\/Administrator\/AppData\Loca\\Packages\MicrosoftWindows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Loca\\Packages\MicrosoftWindows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Loca\\Packages\MicrosoftWindows.Asprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.LOG2         Wii           Users\/Administrator\/AppData\Loca\\Packages\MicrosoftWindows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\setti  | Vindows/System32(Sysprep\Panther\/Elsetuperr.log<br>Vindows/System32(Sysprep\Panther\setuperr.log<br>Vindows/System32(Sysprep\Panther\setupacLlog<br>Vindows/System32(Saseutils.log<br>Vindows/SystemResources\Windows.Ul.Logon  |
| Users/Administrator/AppData/Local/Packages/MicrosoftLockApp_cw5n1h2tsyewy/Settings/settings.dat.LOG2 Wii<br>Users/Administrator/AppData/Local/Packages/Microsoft.Windows.Apprep.ChxApp_cw5n1h2tsyewy/Settings/settings.dat.LOG1 Wii<br>Users/Administrator/AppData/Local/Packages/Microsoft.Windows.Apprep.ChxApp_cw5n1h2tsyewy/Settings/settings.dat.LOG2 Wii<br>Users/Administrator/AppData/Local/Packages/Microsoft.Windows.AsjgnedAccessLockApp_cw5n1h2tsyewy/Settings/settings.dat.LOG2 Wii   | Vindows/System32/Sysprep/Panther/setuper.log<br>Vindows/System32/Sysprep/Panther/setuper.log<br>Vindows/System32/Susseutils/og<br>Vindows/SystemResources/Windows.Ull.logon  |
| Users/Vdministrator/AppData/Local/Packages/Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy/Settings/settings.dat.IOG1 Will<br>Users/Vdministrator/AppData/Local/Packages/Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy/Settings/settings.dat.IOG2 Will<br>Users/Vdministrator/AppData/Local/Packages/Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy/Settings/set   | Vindows/System32\Sysprep\Panther\setupacLlog<br>Vindows/System32\baseutis.log<br>Vindows/SystemResources\Windows.UI.Logon  |
| Users/Vdministrator/AppData/Local/Packages/Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy/Settings/settings.dat.LOG2  | Windows\System32\baseutis.Jog<br>Windows\SystemResources\Windows.UI.Logon  |
| Users\Administrator\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.LOG1  | Vindows\SystemResources\Windows.UI.Logon   |
|  |  |
|  |  |
|  | Vindows\SystemResources\Windows.UI.PrintDialog   |
|  | Vindows\Temp\/pksetup-20190625-113536-0.log  |
|  | Vindows\Temp\/pksetup-20190626-162623-0.log  |
|  | Vindows\Temp\MpCmdRun.log  |
| Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings\settings\settings   | Vindows\Temp\silconfig.log   |
|  | Vindows\Temp\ASPNETSetup_00000.log   |
|  | Vindows\Temp\ASPNETSetup_00001.log   |
|  | Vindows\WinSxS\amd64_microsoft-windows-com-dtc-runtime_31bf3856ad364e35_10.0.14393.0_none_46c76e6076b59fe9\MSDTC.LOG   |
|  | Vindows\WinSxS\amd64_tsportalwebpart_31bf3856ad364e35_10.0.14393.0_none_620a5da1064dcfc0\allusers_tswa.log   |
|  | Vindows/WinSxS/poqexec.log   |
|  | Vindows\PFRO.log   |
|  | Vindows\Dtcinstall.log   |
|  | Vindows\/sasetup.log   |
|  | Vindows\setupact.log   |
|  | Vindows/setuper.log  |
|  | Vindows\wsusofflineupdate.log  |
|  | Vindows\Update.log   |
|  | Vindows\lis.log  |
|  | ost Files\/5007CCF.log   |
|  | ost Files\j5007CD0.log   |
|  | ost Files\/5007CD1.log   |
|  | ost Files\j5007CD2.log   |
|  | ost Files\(5007CD0.log   |
|  | ost Files\j5007CD1.log   |
|  | ost Files\(5007CDLlog  |
|  | ost Files (j5007CCD.log<br>ost Files (j5007CCD.log   |
|  |  |
|  | ost Files\j500002F.log<br>ost Files\j500030.log  |
|  |  |
|  | ost Files\j5000031.log   |
|  | ost Files\j5000032.log   |
|  | ost Files\j5000033.log   |
|  | ost Files\/5000034.log   |
|  | ost Files\j5000035.log   |
|  | ost Files\/5000036.log   |
|  | ost Files\j5000037.log   |
| Users\emsadmin\AppData\Local\Microsoft\SQL Server Management Studio\14.0\ComponentModelCache\Microsoft.VisualStudio.Default.catLos   |  |
|  | .ost Files\j5000039.log  |
| Los Los  | ost Files\j500003A.log   |

#### 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.

<u>Of the original 807 ".log" files on the EMS Server before Dominion's update, only 302 remain</u>, 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

| e View Mo  | and the second sec   |   |   |   |
|------------|--|---|---|---|
| lence Tree |  | × FileList  |   |   |
|            | B     Speech       B     Speech       B     spool       B     Sp   | Archive-EMS system:2019-07     Archive-EMS system:2019-07     Archive-EMS system:2019-07     Archive-EMS System:2019-01     Archive-EMS System:2019-01     Archive-EMS System:2019-01     Archive-EMS System:2019-07     Archive-EMS System:2019-07 | Archive-EMS System-2020-01      Archive-EMS System-2021-09      A | Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win |
|            | Taylor(Wing and     Taylor(Wing and     Taylor(Wing and     Wen     WinBolDatabase  | Archive EMS System-2019-08     Archive EMS System-2019-08     Archive EMS System-2019-08     Archive EMS System-2019-08     Archive EMS System-2019-09     Archive EMS System-2019-10   | 💯 Archive-EMS System-2020-04 📓 Archive-EMS System-2020-11 🗑 Archive-EMS System-2021-05 🗑 Archive-EMS System-2021-05 🚺 Microsoft-Windows-AppMode   | Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win<br>Microsoft-Win                  |
|            | B winm     CN     ch   | <ul> <li>Archive-EMS System-2019-11</li> <li>Archive-EMS System-2019-11</li> <li>Archive-EMS System-2019-11</li> <li>Archive-EMS System-2019-11</li> <li>Archive-EMS System-2019-11</li> <li>Archive-EMS System-2019-12</li> <li>Archive-EMS System-2019-12</li> <li>Archive-EMS System-2019-12</li> </ul>  | Archive-EMS System-2020-05      Archive-EMS System-2021-07      rchive-EMS System-2021-07     Archiv   | Microsoft-Wi<br>Microsoft-Wi<br>Microsoft-Wi<br>Microsoft-Wi<br>Microsoft-Wi<br>Microsoft-Wi<br>Microsoft-Wi  |
|            | tecing<br>totaln 32<br>totaln 32<br>tot | Archive-EMS System-2019-12<br>Archive-EMS System-2019-12<br>Archive-EMS System-2019-12<br>Archive-EMS System-2019-12<br>Archive-EMS System-2019-12  | Archive-EMS System-2020-07 Archive-EMS System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetooth,     Archive-EMS System-2020-07 Archive-EMS System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetooth,     Archive-EMS System-2020-07 Archive-EMS System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetooth,     Archive-EMS System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetooth,     Archive-EMS System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetooth,     Microsoft-Uter-EMS-System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetooth,     Microsoft-Uter-EMS-System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetooth,     Microsoft-Uter-EMS-System-2021-02 Archive-EMS System-2021-05 Microsoft-Ridme-UT%/Admin.e., Microsoft-Windows-Bluetoct,     Microsoft-Uter-EMS-System-2021-02 Archive-EMS-System-2021-05 Microsoft-Uter-EMS-System-2021-05 Microsoft-Windows-RidmeX-Ca   | Microsoft-Wi<br>Microsoft-Wi<br>Microsoft-Wi<br>Microsoft-W<br>Microsoft-W<br>Microsoft-W   |

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

| View Mo   | ide <u>H</u> eb               |                                 |                                 |                              | Archive-FMS-S                | ystem Even                         | t   |
|-----------|-------------------------------|---------------------------------|---------------------------------|------------------------------|------------------------------|------------------------------------|---|
| 植物白白      |                               | 8 3 D B B                       | 2                               |                              |                              |                                    |   |
| ence Tree | ×                             | File List                       |                                 |                              | ogs – Comple                 | tely missing                       | the second second   |
| 1 1       | - Mindows Ul Xami Maps di A   |                                 | merosoft-Windows-AppXDepl       |                              | ege compre                   | conf minoring                      | -Windows-SettingSv 🔝 Micros   |
|           | 14 Windows Ul Xam Phone dl    |                                 | Microsoft-Windows-AppxPack.     |                              |                              |                                    | Windows-SettingSy I Micros  |
|           |                               | DhcpAdminEvents.evtx            | Microsoft-Windows-Assigned      |                              |                              |                                    | -Windows-SettingSy. Windows-  |
|           | - Is Windows UI Xam/Host dl   |                                 |                                 |                              | Microsoft Windows Johlnows   | Microsoft-Windows-Policy%4         |   |
| 1         | 1º Windows Web Diagnostics.   |                                 |                                 |                              |                              | Microsoft-Windows-PowerShe         |   |
|           | Windows Web dl                |                                 |                                 |                              |                              | Microsoft-Windows-PowerShe         |   |
|           | g Windows Web Http dl         |                                 |                                 |                              |                              | Microsoft-Windows-PowerShe Mi      |   |
|           | WindowsActionDialog.exe       | Internet Explorer.evtx          |                                 |                              |                              | Microsoft-Windows-PrintBRM         |   |
|           | P WindowsCodecs dl            |                                 | Microsoft-Windows-Backgrou      |                              |                              | Microsoft-Windows-PrintBevil       |   |
|           | WindowsCodecsEt.dl            |                                 | Microsoft-Windows-Backgrou      |                              |                              |                                    | crosoft-Windows-SmartCar Micros   |
|           | WindowsCodecsRaw dl           |                                 |                                 |                              |                              |                                    |   |
|           | 12 windowstwelogin.dl         |                                 | A Microsoft-Windows-BestPracti- |                              |                              | Microsoft-Windows-PushNotif        |   |
|           | windowsperformancerecord      |                                 | Microsoft-Windows-Biometric     |                              |                              | Microsoft-Windows-PushNotif 🛃 Mi   |   |
|           | 🗄 - 🛅 WindowsPowerShel        |                                 | Microsoft-Windows-Bits-Clien_   |                              |                              | 🛃 Microsoft-Windows-ReadyBoo 🛃 Mi  |   |
|           | winethe.dl                    |                                 | Microsoft-Windows-Bluetooth     |                              |                              | Microsoft-Windows-ReFS%40 🚺 Mi     |   |
|           | B-C winevt                    | Microsoft-Rdms-UI%40perati      |                                 | Microsoft-Windows-DNSServe.  |                              | 📓 Microsoft-Windows-Regsvi32 📓 Mi  |   |
|           | Loga                          |                                 | Microsoft-Windows-BranchCa.     |                              |                              |                                    | crosoft-Windows-SmbClien 🔙 Micros   |
|           | - TraceFormat                 | Microsoft-User Experience Virt  | Microsoft-Windows-CAPI2%4       | Microsoft-Windows-DSC%40     | Microsoft-Windows-Known Fo   | 🛃 Microsoft-Windows-RemoteA 📕 Mi   | crosoft-Windows-SMBDirec 🔛 Micros   |
|           | - winhtp.dl                   | Microsoft-User Experience Virt. | Microsoft-Windows-Certificat    | Microsoft-Windows-EapHost    | Microsoft-Windows-Language   | 🛃 Microsoft-Windows-RemoteD 🔣 Mi   | crosoft-Windows-SMBServe 🔠 Micros   |
|           | e winnet.dl                   | Microsoft-User Experience Virt. | Microsoft-Windows-Certificat    | Microsoft-Windows-EapMeth    | Microsoft-Windows-Liveld%4   | 🛃 Microsoft-Windows-RemoteD 📓 Mi   | crosoft-Windows-SMB5erve 🔠 Micros   |
|           | wininit exe                   | Microsoft-Windows-AAD%40        | Microsoft-Windows-Certificat    | Microsoft-Windows-EapMeth.,  | Microsoft-Windows-Manage     | 🗿 Microsoft-Windows-RemoteD 📓 Mi   | crosoft-Windows-SMBServe 🚂 Micros   |
|           | g winipcfile.dl               | Microsoft-Windows-All-User-I_   | Microsoft-Windows-CloudStor     | Microsoft-Windows-EapMeth    | Microsoft-Windows-Manage     | 🚼 Microsoft-Windows-RemoteD 🛃 Mi   | crosoft-Windows-SMBServe 😹 Micros   |
|           | - is whipsecprocidi           | Microsoft-Windows-AllJoyn%      | Microsoft-Windows-CodeInte      | Microsoft-Windows-EapMeth    | Microsoft-Windows-MemoryD    | 🔠 Microsoft-Windows-Resource 🔝 Mi  | crosoft-Windows-SMBWith 🔝 Micros  |
|           | - p winpsec di                | Microsoft-Windows-AppHost       | Microsoft-Windows-Compat        | Microsoft-Windows-EDP-Audi.  | . Microsoft-Windows-MiStream | Microsoft-Windows-Resource 📓 Mi    | crosoft-Windows-SMBWitn   |
|           | 1º Winlangdb.dll              | Microsoft-Windows-AppID%4       | Microsoft-Windows-Container     | Microsoft-Windows-EDP-Audi.  | Microsoft-Windows-Mobile-Br  | Microsoft-Windows-RestartMa_ II Mi | crosoft-Windows-StateRepo 🐺 Micros  |
|           | 🖉 winipad eti                 | Microsoft-Windows-Applicabil    | Microsoft-Windows-Container     | Microsoft-Windows-Embedde.   | Microsoft-Windows-Mobile-Br  | Microsoft-Windows-ScmBus% 🛃 Mi     | crosoft-Windows-StateRepo 🖉 Micros  |
|           | 12 winked.exe                 |                                 | Microsoft-Windows-CoreAppli.    |                              |                              |                                    | rosoft-Windows-Storage-C.   |
|           | - winiogan.exe                |                                 | Microsoft-Windows-Corrupte      |                              | Microsoft-Windows-Msl bfoPr  | Microsoft-Windows-SDDC-Ma          | crosoft-Windows-Storage-S., Micros  |
|           | 12 winmde.dl                  | Microsoft-Windows-Applicati.    | Microsoft-Windows-Corounte      | Microsoft-Windows-EventColl  | Microsoft-Windows-MUISdAd    | Microsoft-Windows-SDDC-Ma., Mi     | crosoft-Windows-Storage-T   |
|           | WinMetadata<br>Ne winmsioc.dl |                                 | Microsoft-Windows-Crypto-D      |                              |                              |                                    | crosoft-Windows-StorageM 👪 Micros   |
|           | S WinMaplmProtector.dl        |                                 | Microsoft-Windows-Crypto-D      |                              |                              |                                    | crosoft-Windows-StorageSp   |
|           | - a winderes.dl               | Microsoft-Windows-Applicati     |                                 |                              |                              | Microsoft-Windows-Security-E       |   |
|           | - is winnel d                 | Microsoft-Windows-Applicati     |                                 |                              |                              | Microsoft-Windows-Security         |   |
|           | -Ta WinOpcimProtector di      | Microsoft-Windows-Applicati     |                                 |                              |                              | Microsoft-Windows-Security-S. Min  |   |
|           | S winnaume efi                | Microsoft-Windows-AppLocke      |                                 | Microsoft-Windows-FMS%40.    |                              | Microsoft-Windows-Security-S       |   |
|           | g winesume exe                | Microsoft-Windows-AppLocke      |                                 | Microsoft-Windows-Folder Re. | Microsoft-Windows-NiaSvc%4-  |                                    | crosoft-Windows-Store%40 @ Micros   |
|           | R-C win                       | Microsoft-Windows-AppLocke      |                                 | Microsoft-Windows-Forder Re. |                              |                                    | crosoft-Windows-State 240 🔐 Microsi<br>crosoft-Windows-SystemSe 🐼 Microsi |
|           | Te warm ubs                   | Microsoft-Windows-AppLocke      |                                 |                              |                              | Microsoft-Windows-ServerMa         |   |
|           | 9 WinRt Tracing.dl            |                                 |                                 |                              |                              |                                    |   |
|           | Ta WinSATexe                  | Microsoft-Windows-AppMode       |                                 |                              |                              | Microsoft-Windows-ServerMa 📓 M     |   |
|           | WinSATAPI.dl                  | Microsoft-Windows-AppReadi      |                                 |                              |                              | Microsoft-Windows-ServerMa 📓 Mi    |   |
|           | WinSCard.dl                   | Microsoft-Windows-AppReadi      |                                 |                              |                              | 🗿 Microsoft-Windows-ServerMa 🔃 Mi  |   |
|           | - WinSetupUI.dl               |                                 |                                 |                              |                              | 🔠 Microsoft-Windows-ServerMa 📓 Mi  |   |
|           | winshing di                   | Microsoft-Windows-AppXDepl      | Microsoft-Windows-Dhcp-Ser      | Microsoft-Windows-IdCtrls%4. | Microsoft-Windows-PackageS   | 🚼 Microsoft-Windows-SettingSy 🛃 Mi | crosoft-Windows-TerminalS 😹 Micros  |

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 <u>that end with the word ".evtx" found on the EMS Server before the Dominion update was applied</u>. 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%  |
|---|--|
| Logs\Key Management Service.evtx  | Windows\System32\winevt\Logs\Microsoft-Windows-VDRVROOT%4C   |
| Logs\Application evtx   | Windows\System32\winevt\Logs\Microsoft-Windows-VHDMP-Operat  |
| Logs\HardwareEvents.evtx  | Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployme  |
| Logs\Internet Explorer.evtx   | Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployme  |
| Logs\Microsoft-Client-Licensing-Platform%4Admin evtx                                | Windows\System32\winevt\Logs\Microsoft-Windows-International%4   |
| 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.e  |
| Logs\Microsoft-Windows-AppReadiness%4Admin.evtx                                     | Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firew   |
| Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx                             | Windows\System32\winevt\Logs\Microsoft-Windows-Iphlpsvc%4Ope   |
| Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted evtx                        | Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4  |
| Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx                              | Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%   |
| Logs\Microsoft-Windows-Containers-Wcifs%4Operational.evtx                           | Windows\System32\winevt\Logs\Microsoft-Windows-AppReadiness%   |
| Logs\Microsoft-Windows-Containers-Wcnfs%4Operational.evtx                           | Windows\System32\winevt\Logs\Microsoft-Windows-ApplicationReso   |
| Logs\Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx | Windows\System32\winevt\Logs\Microsoft-Client-Licensing-Platform   |
| 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%  |
| 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%4Ope   |
| Logs\Microsoft-Windows-AppReadiness%4Operational.evtx                               | Windows\System32\winevt\Logs\Microsoft-Windows-Application-Exp   |
| Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx                                | Windows\System32\winevt\Logs\Microsoft-Windows-Program-Comp  |
| Logs\Microsoft-Windows-Kernel-IO%4Operational.evtx                                  | Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Client%4/  |
| Logs\Microsoft-Windows-Kernel-EventTracing%4Admin.evtx                              | Windows\System32\winevt\Logs\Microsoft-Windows-TerminalService   |
| Logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational evtx                       | Windows\System32\winevt\Logs\Microsoft-Windows-TerminalService   |
| Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx                          | Windows\System32\winevt\Logs\Microsoft-Windows-WinRM%4Oper   |
| Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx                            | Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defen   |
| Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx                       | Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defer   |
| Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx                                | Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4Dev  |
| Logs\Microsoft-Windows-Known Folders API Service.evtx                               | Windows\System32\winevt\Logs\Microsoft-Windows-UserPnp%4Acti   |
| Logs\Microsoft-Windows-LiveId%4Operational.evtx                                     | Windows\System32\winevt\Logs\Microsoft-Windows-DeviceManager   |
| Logs\Microsoft-Windows-MUI%4Admin.evtx  | Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Power%   |
| Logs\Microsoft-Windows-GroupPolicy%40perational evtx                                | Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Boot%40  |
| Logs\Microsoft-Windows-MUI%4Operational.evtx  | Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository   |
| Logs/Microsoft-Windows-NCSI%40perational.evtx                                       | Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository   |
| Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx                             | Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-PnP%4C   |
| Logs\Microsoft-Windows-Ntfs%4Operational.evtx                                       | Windows/System32/winevt/Logs/Microsoft-Windows-Kernel-ShimEng  |
| Logs\Microsoft-Windows-Ntfs%4WHC evtx   | Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4Operatio  |
| Logs\Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx     | Windows/System32/winevt/Logs/Microsoft-Windows-Ntfs%4WHC.ev  |
| Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx                  | Windows/System32/winevt/Logs/Microsoft-Windows-VolumeSnapsh  |
| Logs/Microsoft-Windows-SettingSync%4Debug.evtx                                      | Windows/System32/winevt/Logs/Microsoft-Windows-Volumesnapsin<br>Windows/System32/winevt/Logs/Microsoft-Windows-Kernel-IO%40p |
| Logs/Microsoft-Windows-Sectings/incodeDebug.evo                                     | Windows/System32/winevt/Logs/Microsoft-Windows-CodeIntegrity%  |
| Logs/Microsoft-Windows-Kernel-PnP%4Configuration evtx                               | Windows/System32/winevt/Logs/Microsoft-Windows-Codemcegrity/<br>Windows/System32/winevt/Logs/Microsoft-Windows-Kernel-WHEA%  |
|   |  |
| Logs\Microsoft-Windows-SettingSync%4Operational.evtx                                | Windows/System32/winevt/Logs/Microsoft-Windows-Kernel-WHEA%  |
| Logs\Microsoft-Windows-Shell-Core%4ActionCenter.evtx                                | Windows/System32/winevt/Logs/Microsoft-Windows-Windows Firew   |
| Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx                                 | Windows/System32/winevt/Logs/Microsoft-Windows-NCSI%40perati   |
| Logs\Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx                           | Windows/System32/winevt/Logs/Microsoft-Windows-WinINet-Config  |
| Logs\Microsoft-Windows-Shell-Core%40perational.evtx                                 | Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%   |
| Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx                                 | Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%   |
| Logs\Microsoft-Windows-SMBClient%4Operational evtx                                  | Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupMa   |
| Logs\Microsoft-Windows-SmbClient%4Security.evtx                                     | Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupMa   |
| Logs\Microsoft-Windows-SMBServer%4Audit.evtx  | Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wci  |
| Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx                                 | Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wcr  |
| Logs\Microsoft-Windows-SMBServer%40perational.evtx                                  | Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4   |

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%40perational.evtx Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin evtx Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx Logs\Microsoft-Windows-Store%40perational.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%40perational.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-Liveld%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-SMBClient%4Ope Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Con Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Seci Windows\System32\winevt\Logs\Microsoft-Windows-Winlogon%4Ope 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 A Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Acti Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%40pe Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4App Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Logi Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeploymen Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runti Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-E 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-Expe Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe Windows\System32\winevt\Logs\Microsoft-Windows-Application-Expe Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-Windows\System32\winevt\Logs\Microsoft-Windows-BackgroundTask Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-M Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-N Windows\System32\winevt\Logs\Microsoft-Windows-Forwarding%4Op Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-N Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaus Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScar Windows\System32\winevt\Logs\Microsoft-Windows-DataIntegrityScar Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Schedu Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Cont Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Connected4 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-RestartManager9 Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PLA%4 Windows\System32\winevt\Logs\Microsoft-Windows-CAPI2%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-WindowsUpdate Windows\System32\winevt\Logs\Microsoft-Windows-NlaSvc%4Operati Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%40p Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Ad Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-PCW% 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 Virtualizat Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizat Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizat Windows\System32\winevt\Logs\Microsoft-User Experience Virtualizat Windows\System32\winevt\Logs\Microsoft-Windows-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%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-ApplicabilityEngi Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4EXE Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4MS Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac Windows\System32\winevt\Logs\Microsoft-Windows-AppLocker%4Pac Windows\System32\winevt\Logs\Microsoft-Windows-AppxPackaging% 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\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\Microsoft-Windows-Audio%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-Audio%4Playbac Windows\System32\winevt\Logs\Microsoft-Windows-Authentication U Windows\System32\winevt\Logs\Microsoft-Windows-Backup.evtx Windows\System32\winevt\Logs\Microsoft-Windows-BestPractices%40 Windows\System32\winevt\Logs\Microsoft-Windows-Biometrics%4Op Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Ope Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-BthLEF Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-MTPE Windows\System32\winevt\Logs\Microsoft-Windows-BranchCacheSME Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService Windows\System32\winevt\Logs\Microsoft-Windows-CertificateService Windows\System32\winevt\Logs\Microsoft-Windows-Compat-Appraise Windows\System32\winevt\Logs\Microsoft-Windows-CoreApplication9 Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRed Windows\System32\winevt\Logs\Microsoft-Windows-CorruptedFileRec Windows\System32\winevt\Logs\Microsoft-Windows-DAL-Provider%40 Windows\System32\winevt\Logs\Microsoft-Windows-DeviceGuard%4C Windows\System32\winevt\Logs\Microsoft-Windows-Devices-Backgrou Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSync%4Op Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripte Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Netw Windows\System32\winevt\Logs\Microsoft-Windows-DirectoryServices Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnostic%4 Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticDa Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticRe Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Admin.evt Windows\System32\winevt\Logs\Microsoft-Windows-DSC%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-EapHost%4Opera Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ras Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Sim Windows\System32\winevt\Logs\Microsoft-Windows-EapMethods-Ttls Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-Regula Windows\System32\winevt\Logs\Microsoft-Windows-EDP-Audit-TCB% Windows\System32\winevt\Logs\Microsoft-Windows-EmbeddedAppLa Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentPolicy Windows\System32\winevt\Logs\Microsoft-Windows-EnrollmentWebS Windows\System32\winevt\Logs\Microsoft-Windows-EventCollector% Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-He Windows\System32\winevt\Logs\Microsoft-Windows-FederationServic Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Serv Windows\System32\winevt\Logs\Microsoft-Windows-FileServices-Servic Windows\System32\winevt\Logs\Microsoft-Windows-FileShareShadow Windows\System32\winevt\Logs\Microsoft-Windows-FMS%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-Folder Redirection Windows\System32\winevt\Logs\Microsoft-Windows-NdisImPlatform% Windows\System32\winevt\Logs\Microsoft-Windows-GenericRoaming Windows\System32\winevt\Logs\Microsoft-Windows-Help%4Operatio Windows\System32\winevt\Logs\Microsoft-Windows-Hyper-V-Guest-D Windows\System32\winevt\Logs\Microsoft-Windows-IdCtrls%4Operati Windows\System32\winevt\Logs\Microsoft-Windows-IKE%4Operationa Windows\System32\winevt\Logs\Microsoft-Windows-International-Reg Windows\System32\winevt\Logs\Microsoft-Windows-KdsSvc%4Operat Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ApphelpC Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-EventTrac Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WDI%40p Windows\System32\winevt\Logs\Microsoft-Windows-LanguagePackSet Windows\System32\winevt\Logs\Microsoft-Windows-ManagementToc Windows\System32\winevt\Logs\Microsoft-Windows-ManagementToo Windows\System32\winevt\Logs\Microsoft-Windows-MemoryDiagnost Windows\System32\winevt\Logs\Microsoft-Windows-MiStreamProvide Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadbar Windows\System32\winevt\Logs\Microsoft-Windows-Mobile-Broadbar Windows\System32\winevt\Logs\Microsoft-Windows-Mprddm%4Oper Windows\System32\winevt\Logs\Microsoft-Windows-MsLbfoProvider% Windows\System32\winevt\Logs\Microsoft-Windows-NetworkLocation Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProvider Windows\System32\winevt\Logs\Microsoft-Windows-NTLM%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-OfflineFiles%4Op Windows\System32\winevt\Logs\Microsoft-Windows-OneBackup%4De Windows\System32\winevt\Logs\Microsoft-Windows-OOBE-Machine-D 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\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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-StoreMgr%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%45ecurity.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%45ecurity.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%45ecurity.evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-07-23-03-48-10-012 evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-08-14-17-50-17-089 evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-08-14-17-50-17-089 evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-08-03-10-49-41-423 evtx Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%40perational evtx Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%40perational evtx Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%40perational evtx Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%40perational evtx Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Server%40perational evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-08-26-00-51-55-728 evtx

Windows/system32/winev/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-Partition%4Diagr Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionRuntin Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionSenso Windows\System32\winevt\Logs\Microsoft-Windows-User Control Pan Windows\System32\winevt\Logs\Microsoft-Windows-Policy%4Operatic Windows\System32\winevt\Logs\Microsoft-Windows-Policy%4Operatic FileDownloadManager%4Operational evtx

Windows\System32\winevt\Logs\Microsoft-Windows-PrintBRM%4Adm Windows\System32\winevt\Logs\Microsoft-Windows-PrintService%4A Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%4Op Windows\System32\winevt\Logs\Microsoft-Windows-ReFS%4Operatio Windows\System32\winevt\Logs\Microsoft-Windows-Regsvr32%4Oper Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and Windows\System32\winevt\Logs\Microsoft-Windows-RemoteApp and Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopS Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaus Windows\System32\winevt\Logs\Microsoft-Windows-ScmBus%4Certifi Windows\System32\winevt\Logs\Microsoft-Windows-ScmDisk0101%40 Windows\System32\winevt\Logs\Microsoft-Windows-SearchUI%4Oper Windows\System32\winevt\Logs\Microsoft-Windows-Security-Audit-Co Windows\System32\winevt\Logs\Microsoft-Windows-Security-Enterpri Windows\System32\winevt\Logs\Microsoft-Windows-Security-Netlogo Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-Windows\System32\winevt\Logs\Microsoft-Windows-Security-UserCon Windows\System32\winevt\Logs\Microsoft-Windows-ServerEssentials-Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-C Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azur Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-Azur Windows\System32\winevt\Logs\Microsoft-Windows-SilProvider%4Ope Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-Audit Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-Device Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-1 Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-Windows\System32\winevt\Logs\Microsoft-Windows-SMBDirect%4Adr Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClier Windows\System32\winevt\Logs\Microsoft-Windows-SMBWitnessClier Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Tiering% Windows\System32\winevt\Logs\Microsoft-Windows-StorageManagen Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-D Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-D Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Sp Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Sp Windows\System32\winevt\Logs\Microsoft-Windows-SystemSettingsTh Windows\System32\winevt\Logs\Microsoft-Windows-TCPIP%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices 
Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices Windows\System32\winevt\Logs\Microsoft-Windows-TZSync%4Operat Windows\System32\winevt\Logs\Microsoft-Windows-TZUtil%4Operatic Windows\System32\winevt\Logs\Microsoft-Windows-UAC%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-UAC-FileVirtualization Windows\System32\winevt\Logs\Microsoft-Windows-User Device Regis Windows\System32\winevt\Logs\Microsoft-Windows-User-Loader%40 Windows\System32\winevt\Logs\Microsoft-Windows-VerifyHardwareS Windows\System32\winevt\Logs\Microsoft-Windows-Volume%4Diagno Windows\System32\winevt\Logs\Microsoft-Windows-VPN-Client%4Op Windows\System32\winevt\Logs\Microsoft-Windows-VPN%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-WFP%4Operation Windows\System32\winevt\Logs\Microsoft-Windows-Win32k%40perat Windows\System32\winevt\Logs\Microsoft-Windows-WindowsSystem/ Windows\System32\winevt\Logs\Microsoft-Windows-Winsock-WS2HEL Windows\System32\winevt\Logs\Microsoft-Windows-DNSServer%4Audit.evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-08-10-23-29-48-856.evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-08-18-12-10-49-482.evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-09-02-13-32-58-546.evtx Windows\System32\winevt\Logs\Archive-EMS System-2019-08-29-19-12-25-021.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Audit evtx Windows\System32\winevt\Logs\Microsoft-Windows-Wired-AutoConfig%4 Windows\System32\winevt\Logs\Microsoft-Windows-WPD-ClassInstaller%4 Windows\System32\winevt\Logs\Microsoft-Windows-WPD-CompositeClass Windows\System32\winevt\Logs\Microsoft-Windows-WPD-MTPClassDriver 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 <u>destruction of Election-Related Data</u>, <u>specifically critical</u> <u>logfiles</u>, <u>has occurred</u>. 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.k 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\_2( 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\_2( 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\_2( Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost\_03\_30\_2( Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost\_03\_30\_2( 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\_2( Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\LogFiles\Microsoft.ReportingServices.Portal.WebHost\_06\_26\_2( 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\_2( 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\_2( 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\_2( 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  $\label{eq:programData} Microsoft \\ Windows \\ App \\ Repository \\ Packages \\ Microsoft \\ AD. \\ Broker \\ Plugin \\ 1000.14393.0.0 \\ neutral \\ neutral \\ cw5n1h2t \\ xyewy \\ Action \\ Advised   $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Accounts \\ Control \\ 10.0.14393.0 \\ neutral \\ cw5n1h2txyewy \\ Activation \\ Stores  ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.AccountsControl\_10.0.14393.0\_neutral\_cw5n1h2txyewy\ActivationStor  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Bio Enrollment \\ 10.0.14393.0 \\ neutral \\ cw5n1h2txyewy \\ \\ Activation \\ Store.com \\ com   $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Bio Enrollment \\ 10.0.14393.0 \\ neutral \\ w5n1h2txyewy \\ \\ Activation \\ Store.c \\ Microsoft \\ Micros$ ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.LockApp\_10.0.14393.0\_neutral\_\_cw5n1h2txyewy\ActivationStore.dat.LO ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.LockApp 10.0.14393.0 neutral cw5n1h2txyewy\ActivationStore.dat.LO ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Apprep.ChxApp\_1000.14393.0.0\_neutral\_neutral\_cw5n1h2txy& ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Apprep.ChxApp\_1000.14393.0.0\_neutral\_neutral\_cw5n1h2txy&  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ Assigned \\ Access \\ Lock \\ App_1000.14393.0.0 \\ neutral_neutral_cw5 \\ Nicrosoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ AppRepository \\ Packages \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ AppRepository \\ Packages \\ Windows \\ AppRepository \\ Packages \\ Windows \\ AppRepository \\ Microsoft \\ Windows \\ AppRepository \\ Microsoft \\ Windows \\ AppRepository \\ Windows \\ Microsoft \\ Windows \\ Microsoft \\ Windows \\$  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ Assigned \\ Access \\ Lock \\ App_1000.14393.0.0 \\ neutral_neutral_cw5 \\ Nicrosoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ AppRepositor \\ Microsoft \\ Windows \\ AppRepositor \\ Microsoft \\ Windows \\ W$ ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.CloudExperienceHost\_10.0.14393.0\_neutral\_neutral\_cw5n1h21 ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.CloudExperienceHost\_10.0.14393.0\_neutral\_neutral\_cw5n1h2i  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ Cortana \\ 1.7.0.14393 \\ neutral \\ neutral \\ cw5n1h2txyewy \\ Activat \\ Neutral \\$  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Windows \\ Cortana \\ 1.7.0.14393 \\ neutral \\ neutral \\ cw5n1h2txyewy \\ Activat \\ Neutral \\$  $\label{eq:programData} with the second sec$ 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\_cw5n1h2tb ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost\_10.0.14393.0\_neutral\_neutral\_cw5n1h2tb  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Microsoft \\ Xbox \\ Game \\ Callable \\ UI_1000.14393.0.0\_neutral\_neutral\_cw5n1h2txyewy \\ Name \\ AppRepository \\ Packages \\ Microsoft \\ Xbox \\ Game \\ Callable \\ UI_1000.14393.0.0\_neutral\_neutral\_cw5n1h2txyewy \\ Name \\$  $\label{eq:programData} with the set of the$  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ Activati \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ Activati \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ Activati \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ Activati \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ Activati \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ windows.immersive control \\ panel_{6.2.0.0} \\ neutral_neutral_cw5n1h2t \\ yewy \\ windows.immersive control \\ windows.immersive con$  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ windows. \\ immersive control \\ panel_{6.2.0.0} \\ neutral_cw5n1h2t \\ xyewy \\ Activati \\ advector \\ adve$  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Windows \\ Miracast \\ View \\ 6.3.0.0 \\ neutral \\ neutral \\ cw5n1h2txyewy \\ \\ Activation \\ Store. \\ (a,b) \\ (a$ ProgramData\Microsoft\Windows\AppRepository\Packages\Windows.MiracastView\_6.3.0.0\_neutral\_neutral\_cw5n1h2txyewy\ActivationStore.c  $\label{eq:programData} Microsoft \\ Windows \\ AppRepository \\ Packages \\ Windows \\ PrintDialog \\ 6.2.0.0 \\ neutral \\ neutral \\ cw5n1h2txyewy \\ Activation \\ Store. \\ data \\ respectively  

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 Cache\02A26E554FBB4232ACD36E70D09F2C7893D399CD\%localappdata%\temp\Ssm ProgramData\Package 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\_lsc 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\_E ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015lsoShell\_020\_Msi\_E ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015lsoShell\_032\_vs\_isc ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell 019 Msi E ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell 021 sdk to 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\VS2015lsoShell\_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\_vsbslr ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_010\_netfx\_

ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_011\_netfx\_ ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_012\_netfx\_ ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_013\_netfx\_ ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell 014 netfxc ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell 015 netfx ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_017\_Msi\_E ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_022\_sdk\_to ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_023\_sqlsys ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015lsoShell\_024\_share ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_025\_help3 ProgramData\Package Cache\FE948F0DAB52EB8CB5A740A77D8934B9E1A8E301\%localappdata%\temp\SsmsSetup\VS2015IsoShell\_026\_Bliss\_1 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\VS2015lsoShell\_033\_vs\_isc 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\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  $Users \ Administrator \ AppData \ Local \ Packages \ Microsoft. Accounts \ Control\_cw5n1h2txyewy \ Settings. \\ dat. LOG2$  $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. Bio Enrollment \ cw5n1h2txyewy \ Settings \ settings. \ dat. \ LOG1$  $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. Bio Enrollment \ cw5n1h2txyewy \ Settings \ settings. \ dat. \ LOG2$  $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. \ Lock \ App \ cw5n1h2txyewy \ Settings. \ dat. \ LOG1$ 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  $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. Windows. Apprep. Chx \ App \ _cw \ 5n1h \ 2txy ewy \ Settings \ dat. LOG2$  $Users \ Administrator \ AppData \ Local \ Packages \ Microsoft. Windows. Assigned \ Access \ Lock \ App \ Cw5n1h2txyewy \ Settings. \ dat. \ LOG1$ Users\Administrator\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp\_cw5n1h2txyewy\Settings\settings.dat.LOG2  $Users \ Administrator \ AppData \ Local \ Packages \ Microsoft. Windows. Cloud \ Experience \ Host_cw5n1h2txyewy \ Settings. \ dat. \ LOG1$ 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  $Users \ Administrator \ AppData \ Local \ Packages \ Microsoft. Windows. Cortana \ _cw5n1h2txyewy \ Settings. \ dat. \ LOG1 \ Microsoft. \ Microso$ 

| $Users \ Administrator \ AppData \ Local \ Packages \ Microsoft. Windows. Cortana \ cw5n1h2txyewy \ Settings \ settings. dat. LOG2 \ Microsoft \ Micr$    |
|---|
| $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. Windows. Secondary Tile \ Experience \ cw5n1h2txyewy \ Settings \ dat. LOG1$  |
| $Users \ Administrator \ AppData \ Local \ Packages \ Microsoft. Windows. Secondary Tile \ Experience \ cw5n1h2txyewy \ Settings \ dat. LOG2$   |
| $Users \ Administrator \ AppData \ Local \ Packages \ Microsoft. Windows. \\ Shell \ Experience \ Host \ cw5n1h2txyewy \ Settings \ dat. \\ LOG1 \ Microsoft \ Micr$  |
| $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. Windows. \\ Shell Experience \ Host \ cw5n1h2txyewy \ Settings \ settings. \\ dat. \\ LOG2 \ Microsoft \ Mindows \ Shell \ Experience \ Host \ Shell \$ |
| $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. \ Xbox Game Callable UI\_cw5n1h2txyewy \ Settings \ dat. \ LOG1 \ Microsoft. \ Mic$   |
| $Users \ Administrator \ App Data \ Local \ Packages \ Microsoft. \ Xbox Game Callable UI\_cw5n1h2txyewy \ Settings \ settings. \ dat. \ LOG2 \ Microsoft. \ Micr$   |
| $Users \ Administrator \ App Data \ Local \ Packages \ windows. immersive control panel \ cw 5n1h2txyewy \ Settings \ dat. \ LOG1 \ Marcological \ LOG1 \ Marcological \ Marcol$    |
| $Users \ Administrator \ App Data \ Local \ Packages \ windows. immersive control panel \ cw 5n1h2txyewy \ Settings \ dat. LOG2$  |
| $Users \ Administrator \ App Data \ Local \ Packages \ Windows. Miracast \ View \ cw 5n1h2txyewy \ Settings \ settings. dat. LOG1$  |
| $Users \ Administrator \ App Data \ Local \ Packages \ Windows. Miracast \ View \ cw 5n1h2txyewy \ Settings \ settings. dat. LOG2$  |
| Users\Administrator\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy  |
| $Users \ Administrator \ App Data \ Local \ Packages \ Windows. Print Dialog \ cw5n1h2txyewy \ Settings \ settings. dat. LOG1$  |
| $Users \ Administrator \ App Data \ Local \ Packages \ Windows. Print Dialog \ cw5n1h2tx yewy \ Settings \ settings. \ dat. \ LOG2$   |
| 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  $Users\ensuremath{\mathsf{Users}}\xspace with the set of the$ Users\emsadmin\AppData\Local\Packages\Microsoft.AccountsControl\_cw5n1h2txyewy\Settings\settings.dat.LOG2 Users\emsadmin\AppData\Local\Packages\Microsoft.BioEnrollment\_cw5n1h2txyewy\Settings\settings.dat.LOG1  $Users\ensuremath{\columnwidth} Users\ensuremath{\columnwidth} users\ensuremath{\columnwidth$  $Users\ensuremath{\columnwidth} Users\ensuremath{\columnwidth} Users\ensuremath{\columnwidth$ 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  $Users\ensuremath{\mathsf{Windows}}\ensuremath{\mathsf{AppData}}\ensuremath{\mathsf{Local}}\ensuremath{\mathsf{Packages}}\ensuremath{\mathsf{Microsoft}}\ensuremath{\mathsf{Windows}}\ensuremath{\mathsf{AppData}}\ensuremath{\mathsf{Local}}\ensuremath{\mathsf{Vacal}}\ensuremath{\mathsf{Packages}}\ensuremath{\mathsf{Microsoft}}\ensuremath{\mathsf{Windows}}\ensuremath{\mathsf{AppData}}\ensuremath{\mathsf{Local}}\ensuremath{\mathsf{Vaca$ Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp\_cw5n1h2txyewy\Settings\settings.dat.LOG1  $Users\ ensuremath{scal}\ ens$  $Users \ ensuremath{\mathsf{S}} with \ ensuremath{\mathsf{S}} wit$  $Users\ensuremath{\mathsf{W}} users\ensuremath{\mathsf{W}} users$ ensuremath{\mathsf{W}} users\ensuremath{\mathsf{W}} users\ensuremath{\mathsf{W}} usersensuremath{\mathsf{W}} users\ensuremath{\mathsf{W}} usersensuremath{\mathsf{W}} usersensuremath{\mathsf{W  $Users\ensuremath{\mathsf{Users}}\e$ 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  $Users\enset{enset} Users\enset{enset} users\enset$ Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.Cortana\_cw5n1h2txyewy\Settings\settings.dat.LOG1  $Users\ensuremath{\columnwith}{lines} with the set of   $Users \ ensuremath{shift} users \ ensurema$ Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.SecondaryTileExperience\_cw5n1h2txyewy\Settings\settings.dat.LOG2  $Users\ensuremath{\mathsf{Users}}\ensuremath{\mathsf{Users}}\ensuremath{\mathsf{Local}}\ensuremath{\mathsf{Packages}}\ensuremath{\mathsf{Microsoft}}\ensuremath{\mathsf{Windows}}\ensuremath{\mathsf{Settings}}\ensuremath{\mathsf{Local}}\ensuremath{\mathsf{Vackages}}\ensuremath{\mathsf{Vackages}}\ensuremath{\mathsf{Microsoft}}\ensuremath{\mathsf{Settings}}\ensuremath{\mathsf{Local}}\ensuremath{\mathsf{Vackages}}\ensuremath{\mathsf$ 

Users\emsadmin\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost\_cw5n1h2txyewy\Settings\settings.dat.LOG2  $Users\ensuremath{\mathsf{Users}}\e$  $Users\ensuremath{\mathsf{Users}}\xspace{\constrains} Users\ensuremath{\mathsf{Users}}\xspace{\constrains}\xspace{\co$ 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  $Users\ensuremath{\columnwidth} Users\ensuremath{\columnwidth} Users\ensuremath{\columnwidth$ Users\emsadmin\AppData\Local\Packages\Windows.PrintDialog\_cw5n1h2txyewy  $Users\ensuremath{\coloremath{\mathsf{S}}\ensuremath{\mathsf{S}}\ens$ 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\SSM5-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  |
| 1 |  |

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.



Dell Server Update Dell Server Update Logs Before.csv

Logs After.csv

Databases Before.csv

61

# 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-..."

| 1 | Logs\Microsoft-Windows-Kernel-WHEA%4Errors.evtx                                     |
|---|---|
|   | Logs\Key Management Service.evtx  |
|   | Logs\Application.evtx   |
|   | Logs\HardwareEvents.evtx  |
|   | Logs\Internet Explorer.evtx   |
|   | Logs\Microsoft-Client-Licensing-Platform%4Admin.evtx                                |
|   | Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx |
|   | Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx                                 |
|   | Logs\Microsoft-Windows-AppReadiness%4Admin.evtx                                     |
|   | Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx                             |
|   | Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx                        |
|   | Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx                              |
|   | Logs\Microsoft-Windows-Containers-Wcifs%4Operational.evtx                           |
|   | Logs\Microsoft-Windows-Containers-Wcnfs%4Operational.evtx                           |
|   | Logs\Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx |
|   | Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx                              |
|   | Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx                               |
|   | Logs\Microsoft-Windows-DeviceSetupManager%4Admin.evtx                               |
|   | Logs\Microsoft-Windows-DeviceSetupManager%4Operational.evtx                         |
|   | Logs\Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.evtx        |
|   | Logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx                                      |
|   | Logs\Microsoft-Windows-Dhcpv6-Client%4Admin.evtx                                    |
|   | Logs\Microsoft-Windows-Hyper-V-Guest-Drivers%4Admin.evtx                            |
|   | Logs\Microsoft-Windows-International%4Operational.evtx                              |
|   | Logs\Microsoft-Windows-AppReadiness%4Operational.evtx                               |
|   | Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx                                |
|   | Logs\Microsoft-Windows-Kernel-IO%4Operational.evtx                                  |
|   | Logs\Microsoft-Windows-Kernel-EventTracing%4Admin.evtx                              |
|   | Logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx                       |
|   | Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx                          |
|   | Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx                            |
|   | Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx                       |
|   | Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx                                |
|   | Logs\Microsoft-Windows-Known Folders API Service.evtx                               |
|   | Logs\Microsoft-Windows-Liveld%4Operational.evtx                                     |
|   | Logs\Microsoft-Windows-MUI%4Admin.evtx  |
|   | Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx                                |
|   | Logs\Microsoft-Windows-MUI%4Operational.evtx  |
|   | Logs\Microsoft-Windows-NCSI%4Operational.evtx                                       |
|   | Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx                             |
| - |   |

Logs\Microsoft-Windows-Ntfs%4Operational.evtx Logs\Microsoft-Windows-Ntfs%4WHC.evtx Logs\Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx Logs\Microsoft-Windows-SettingSync%4Debug.evtx Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx Logs\Microsoft-Windows-Kernel-PnP%4Configuration.evtx Logs\Microsoft-Windows-SettingSync%4Operational.evtx Logs\Microsoft-Windows-Shell-Core%4ActionCenter.evtx Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx Logs\Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx Logs\Microsoft-Windows-Shell-Core%4Operational.evtx Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx Logs\Microsoft-Windows-SMBClient%4Operational.evtx Logs\Microsoft-Windows-SmbClient%4Security.evtx Logs\Microsoft-Windows-SMBServer%4Audit.evtx Logs\Microsoft-Windows-SMBServer%4Connectivity.evtx Logs\Microsoft-Windows-SMBServer%4Operational.evtx Logs\Microsoft-Windows-SMBServer%4Security.evtx Logs\Microsoft-Windows-SMBWitnessClient%4Admin.evtx Logs\Microsoft-Windows-SMBWitnessClient%4Informational.evtx Logs\Microsoft-Windows-StateRepository%4Operational.evtx Logs\Microsoft-Windows-StateRepository%4Restricted.evtx Logs\Microsoft-Windows-TaskScheduler%4Maintenance.evtx Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx Logs\Microsoft-Windows-Store%40perational.evtx Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx Logs\Microsoft-Windows-User Profile Service%40perational.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%40perational.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-2020-10-26-06-16-735.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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-VHDMP-Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeploymentServer%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx Windows\System32\winevt\Logs\Microsoft-Windows-International%40perational.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%40perational.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%40perational.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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-WinRM%4Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-IO%40perational.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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx Windows\System32\winevt\Logs\Microsoft-Windows-DeviceSetupManager%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Service%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Liveld%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%40perational.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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Admin.evtx Windows\System32\winevt\Logs\Microsoft-Windows-TWinUI%40perational.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-Troubles Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx Windows\System32\winevt\Logs\Microsoft-Windows-BackgroundTaskInfrastructure%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-MultiMachine%4Admin.evtx Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-MultiMachine%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Forwarding%4Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-ServerManager-MgmtProvider%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Detector%40perational.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%40perational.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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-NlaSvc%4Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%40perational.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%40perational.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%40perational.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%40perational.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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Backup.evtx Windows\System32\winevt\Logs\Microsoft-Windows-BestPractices%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Biometrics%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-BthLEPrepairing%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Bluetooth-MTPEnum%40perational.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%40perational.ev Windows\System32\winevt\Logs\Microsoft-Windows-CertificateServicesClient-Lifecycle-User%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Compat-Appraiser%4Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-CoreApplication%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-DeviceGuard%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Devices-Background%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-DirectoryServices-Deployment%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnostic%4Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-DiskDiagnosticDataCollector%40perational.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%40perational.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%40perational.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%40perational.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%40perational. 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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-ManagementTools-TaskManagerProvider%40perational.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. 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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagnostic.evtx Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionRuntime%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-PerceptionSensorDataService%40perational.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%40perational.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.ev Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Resolver%40perational.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%40perati 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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-VCard-Module%4Admin.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SmartCard-TPM-VCard-Module%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-SpaceManager%4Diagnostic.evtx Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-SpaceManager%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-SystemSettingsThreshold%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-TCPIP%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%4Admin.evtx Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RDPClient%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.ev Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%40peration

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%40perational.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%40perational.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%40perational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Winsock-WS2HELP%4Operational.evtx Windows\System32\winevt\Logs\Microsoft-Windows-Wired-AutoConfig%40perational.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%40perational.evtx Windows\System32\winevt\Logs\SMSApi.evtx

### APPENDIX D. LIST OF FIGURES

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

#### APPENDIX E. 2002 VOTING SYSTEMS STANDARDS (VSS)

The 2002 VSS explicitly states:

"2.2.4.1 Common Standards

To ensure system integrity, all system shall:

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

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

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

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

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

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

"Simultaneous processes" of concern include unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of 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.

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

This \_15th\_day of September, 2021.

DOUG GOULD Chief Technical Officer

CyberTeamUS

## **Doug Gould Biography**

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



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

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

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

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

He is a subject matter expert in:

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

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

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

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

Doug currently serves as Chief Technical Officer at CyberTeamUS.

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

Doug is an invited conference speaker. **EXHIBIT** 

# **Doug Gould Forensic Addendum**

### Major Forensic Cases

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

## Instructor of Forensics

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