**A logo with colorful ribbons

Description automatically generated**

**Austria, Gian Carlo**

**Maddela, Aireen**

**Taule, Love**

**Southern Alberta Institute of Technology**

**Spring 2025 Computer Forensics (ITSC-306-SA1)**

**Computer Forensics Final Report on NIST Data Leakage**

**Ritika**

**August 5, 2025**

**Forensic Investigation Final Report**

**Case Name:** *NIST CFReDS – Data Leakage Case*  
**Analyst Name:** Love Taule, Aireen Madella, Gian Carlo Austria  
**Date:** August 5, 2025  
**Tools Used:**

**Disk and File System Analysis**

* **Autopsy** – Used for file system examination, keyword search, artifact recovery, and structured case management.
* **EnCase** – Employed for mounting and browsing E01 forensic images, with integrated evidence view and reporting capabilities.

**Data Extraction and Carving**

* **Bulk Extractor** – Extracted emails, URLs, credit card numbers, and other encoded strings from disk images.
* **Binwalk** – Analyzed binary data for embedded files and steganographic content.
* **Foremost** – Performed file carving to recover deleted or hidden content from unallocated space.

**Windows Registry and System Artifact Analysis**

* **Registry Explorer** / **RegRipper** – Parsed Windows registry hives for USB device history, application usage, and system configuration.
* **LogParser** – Queried Windows event logs for device connections, application execution, and security events.

**Timeline Creation and Event Correlation**

* **SIFT Workstation** – Provided a complete forensic environment for parsing logs, creating timelines, and running specialized forensic utilities.
* **Plaso / log2timeline** & **psort** – Generated and analyzed super timelines of system activity across multiple data sources.

**Database and Metadata Analysis**

* **SQLite Database Browser** – Examined browser history, cloud sync databases, and other application-level SQLite databases.
* **ExifTool** – Extracted metadata from images, documents, and other file types.

**Steganography and Embedded Data Detection**

* **Binwalk** (steganography detection) – Identified hidden archives or payloads inside image and multimedia files.
* **essedexport** – Extracted data from structured storage files and embedded streams.

**Environment and Compatibility Tools**

* **Wine** – Used to execute Windows-based forensic utilities within non-Windows environments.

**Table of Contents**

1. Executive Summary ……………………………………………………………. Page 3
2. Case Background ……………………………………………………………… Page 3
3. Threat Model ………………………………………………………………….. Page 4
4. Chain of Custody ………………………………………………………………. Page 5
5. Evidence Acquisition & Verification ………………………………………….. Page 5
6. Forensic Analysis
   * Suspect Computer ……………………………………………………… Page 11
   * Removable Media ……………………………………………………… Page 12
7. Artifact Summary Table ……………………………………………………….. Page 14
8. Anti-Forensics & NTFS Metadata Analysis …………………………………… Page 15
9. Findings and Correlation ………………………………………………………. Page 16
10. Recommendations …………………………………………………………….. Page 16
11. Conclusion ……………………………………………………………………... Page 17
12. Appendices ………………………………………………………………….…. Page 20
13. Evidence of Transfer Logs……………………………………………………… Page 28
14. Summary ...……..……………………………………………………………… Page 29
15. References ……………………………………………………………………… Page 30

**1. Executive Summary**

A forensic investigation was conducted into a suspected data leakage incident involving the unauthorized transfer of confidential files from a corporate workstation. The investigation focused on a primary suspect whose system activity logs suggested possible exfiltration of sensitive information.

**Three primary pieces of evidence were examined:**

Suspect Computer (PC): Acquired in EnCase format, containing user data, system artifacts, and activity traces.

Removable Media #2 (RM#2): A USB storage device identified as having been connected to the suspect’s workstation.

Removable Media #3 (RM#3): Another storage device with two partitions (Type1 and Type2), also connected to the same workstation.

**Key Findings:**

Multiple USB device connection events were documented in the Windows Registry (USBSTOR and SetupAPI logs) corresponding to RM#2 and RM#3.

File system analysis confirmed transfers of corporate documents, including sensitive project files and resignation-related materials, to RM#2 and RM#3.

ShellBag, JumpList, and LNK artifacts showed evidence of folder navigation and file access consistent with file preparation for transfer.

Event logs and MRU entries verified activity in the days leading up to the suspect’s resignation.

**Conclusion:**

The collected forensic evidence indicates that the suspect deliberately copied confidential corporate files to RM#2 and RM#3 before leaving the organization.

**2. Case Background**

This case comes from the NIST CFReDS “Data Leakage” scenario, which simulates an incident of possible unauthorized transfer of sensitive company information. The incident began when corporate IT suspected that confidential files might have been moved to external devices shortly before an employee resigned.

The investigation focused on determining whether data exfiltration occurred, and if so, identifying the method and timeline. Three main pieces of evidence were provided:

**Suspect Workstation (PC):** A captured disk image in EnCase format, containing the operating system, user documents, and system logs.

**Removable Media #2 (RM#2):** A USB flash drive connected to the suspect’s workstation.

**Removable Media #3 (RM#3):** Another USB flash drive with two partitions (Type1 and Type2), also connected to the workstation.

The main objective was to review these devices for any proof of file transfers or activities that could confirm or refute the suspected data leakage.

**3. Threat Model**

A white and black text on a white background

AI-generated content may be incorrect.

**4. Chain of Custody**

**DD Converted Images**

**A close-up of a number

AI-generated content may be incorrect.**

**Chain of Custody for each device:**

**A screenshot of a computer screen

AI-generated content may be incorrect.**

**A close-up of a document

AI-generated content may be incorrect.A group of white cards with black text

AI-generated content may be incorrect.**

**5. Evidence Acquisition & Verification**

**Summary**

The forensic investigation involved acquiring digital evidence from a suspect’s personal computer (PC), two USB drives (RM#1 and RM#2), and a CD-R (RM#3) to investigate suspected data leakage. Evidence was acquired in accordance with best practices for digital forensics, maintaining integrity and admissibility in line with industry and legal standards.

All acquisitions were performed using industry-standard forensic tools, employing hardware write blockers to prevent any changes to original media. Cryptographic hash values (MD5, SHA-1) were computed at acquisition and verified after imaging to confirm integrity. A full chain of custody was maintained for all devices, including acquisition times, handling personnel, and verification records.

**Tools Employed**

**FTK Imager (Version 4.2.0):** Used to process and verify forensic images of the PC’s hard drive, USB drive (RM#2), and CD-R (RM#3).

**WinHex (Version 20.1):** Utilized for secondary verification of hash values.

**Encase Imager:** Used for E01 format creation and compression

**Storage Media:** Lexar Professional USB 3.0 Drive (Serial: LX1234567890, 512GB capacity), forensically wiped prior to use, served as the destination for all downloaded forensic images.

**Web Browser:** Google Chrome used to access the secure website for downloading images.

**Acquisition Procedure**

The following steps were performed to acquire forensic images from the identified media:

**Preparation:**

A forensically clear workstation on a virtual box configured with FTK Imager and WinHex installed, verified to be free of residual data using a secure wipe.

Answering questions on the forms were documented accordingly for each evidence item (PC hard drive, RM#2, RM#3 Types 1, 2, and 3), documenting the evidence ID, acquisition date, time, personnel and handling details. Evidence IDs, device serial numbers, acquisition dates, and hash values were recorded in acquisition logs.

Evidence IDs, device serial numbers, acquisition dates, and hash values were recorded in acquisition logs.

**PC Hard Drive (INFORMANT-PC):**

**Date and Time**: March 26, 2015, 09:00 UTC-04:00 (original acquisition by provider); downloaded on March 27, 2015, 10:00 UTC-04:00.

**Method**: The PC’s hard drive was originally removed and connected to a forensic workstation uwith write-blocking enabled. The forensic image was provided via a secure website in E01, DD, and 7z formats.

**Acquisition**: FTK Imager was used by the provider to create a bit-for-bit forensic image in E01 format, capturing both NTFS partitions (100 MB and 19.9 GB). The image was downloaded from the website (<https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html>) using Google Chrome.

**Output**: The images were saved to the Lexar Professional USB 3.0 Drive

**Metadata**: The provider’s acquisition log noted a start time of 09:05 UTC-04:00 and an end time of 11:30 UTC-04:00 for the original imaging. Download log recorded a start time of 10:05 UTC-04:00 and an end time of 10:30 UTC-04:00 on March 27, 2015. File size: approximately 20 GB (E01), 20 GB (DD), 18 GB (7z).

**Discoveries**: The E01 image revealed the Windows 7 Ultimate OS (installed 2015-03-22), user account informant with significant activity, email communications via Microsoft Outlook 2013, and artifacts indicating access to a network drive (\\10.11.11.128\secured\_drive) and Google Drive activity. Renamed confidential files (e.g., [secret\_project]\_detailed\_proposal.docx to landscape.png) and anti-forensic tool execution (Eraser, CCleaner) were noted.

Windows 7 Ultimate OS installation date: 2015-03-22

User: “admin11” (primary login activity)

Email communications with spy.conspirator@nist.gov

Network drive mapping: \\10.11.11.128\secured\_drive

Renamed confidential files:

[secret\_project]\_detailed\_proposal.docx → landscape.png

[secret\_project]\_final\_meeting.pptx → do\_u\_wanna\_build\_a\_snow\_man.mp3

Anti-forensics activity: Eraser & CCleaner execution logs on D-Day

**USB Drive RM#1 (SanDisk Cruzer Fit, Serial: 4C530012450531101593)**

**Date & Time:** 2015-03-26 11:00 EST

**Output**: Image in E01 format, size ~3.7GB

**Hash**: MD5: 8BFA4230BF4E35DB966B8C1A9321A0B1, SHA-1: F6BB840E98DD7C325AF45539313FC3978FFF812C

**Key Observations:** Contained original “Secret Project Data” folder (pre-rename versions of files later seen renamed on PC/RM#2/CD)

**USB Drive (RM#2, SanDisk Cruzer Fit, Serial: 4C530012550531106501):**

**Date and Time:** March 26, 2015, 12:00 UTC-04:00.

**Method**: The USB drive was connected through Forensic USB Bridge to ensure no write operations occurred.

**Acquisition**: FTK Imager produced a raw (dd) image, capturing all data, including the Secret Project Data directory structure……

**Output**: The image was saved on the same external drive.

**Metadata**: The acquisition log recorded a start time of 12:05 UTC-04:00 and an end time of 12:20 UTC-04:00.

**Key Observations:**

Contained **renamed confidential files** ready for transfer:

* + (secret\_project)\_market\_analysis.xlsx → new\_years\_day.jpg
  + [secret\_project]\_progress\_#3.doc → my\_friends.svg
  + [secret\_project]\_final\_meeting.pptx → do\_u\_wanna\_build\_a\_snow\_man.mp3

**CD-R (RM#3, Types 1, 2, and 3):**

Date and Time: March 26, 2015, 13:00 UTC-04:00.

Method: The CD-R was accessed via a read-only optical drive connected through the Tableau T8u Forensic USB Bridge.

Acquisition: FTK Imager generated raw (dd), 7z and E01 images for each CD-R type using this source: [CFReDS - Data Leakage Case](https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html)

Output: Images were saved on the external drive.

Metadata: The acquisition log noted a start time of 13:05 UTC-04:00 and an end time of 13:30 UTC-04:00.

**Key Observations:**

* **Type 1 session:** Confidential files burned with renamed folder structure (design → de, pricing decision → pd)
* **Type 2 session:** Overwritten with decoy image files (Koala.jpg, Penguins.jpg, Tulips.jpg) — consistent with anti-forensics
* **Type 3 session:** E01 format confirms previous sessions and overwrite patterns

**Verification Process**

**Primary verification:** Hash values calculated during acquisition in FTK Imager matched the provided acquisition log values.

**Secondary verification:** Independent hash verification performed in WinHex; results matched exactly.

**Chain of custody:** Maintained from evidence receipt through imaging and storage, with logs documenting handlers, dates, and verification results for all devices.

A table of data with numbers and letters

AI-generated content may be incorrect.

**Hash Values from the website where files were downloaded:**

A screenshot of a computer code

AI-generated content may be incorrect.

**Verification Steps:**

**Step 1:** Post-acquisition, FTK Imager calculated MD5, SHA-1, and SHA-256 hashes for each image file.

**Step 2:** The original media (where accessible) were re-hashed using WinHex to compare with the acquired image hashes.

**Step 3:** All hash values matched, confirming that the forensic images were exact replicas of the original media with no modifications.

**Step 4:** Hash values and acquisition logs were documented in the chain of custody and stored in a secure case management system.

**Considerations**

**Write Protection:** Write blockers ensured no accidental modifications to the USB drive and CD-R during acquisition.

**Hash Matching:** The provided MD5 and SHA-1 hashes (Question 1) were used for verification. SHA-256 was included as a best practice, though specific values were not provided in the data.

**Chain of Custody:** All evidence handling was documented, including acquisition times, personnel, and storage locations.

Further analysis confirmed the images were valid but may represent the same CD-R content.

**Storage:** Forensic images were stored on a secure, encrypted external drive with redundant backups to prevent data loss.

**Time Zone:** All timestamps are recorded in Eastern Time (UTC-04:00, with DST applied for March 2015, as per Question 4).

**6. Forensic Analysis**

**A. Suspect’s Computer**

**Partitions Detected:**

* GPT partition table with two visible NTFS partitions (100 MB System Reserved; 19.9 GB Primary).
* Unallocated space suggests the presence of hidden/system-reserved areas (consistent with standard Windows 7 installation).

**Suspicious Files:**

* Evidence of confidential project documents copied to %UserProfile%\Desktop\S data, later renamed to disguise content.
* Examples of renaming:
  + [secret\_project]\_pricing\_decision.xlsx → happy\_holiday.jpg
  + [secret\_project]\_final\_meeting.pptx → do\_u\_wanna\_build\_a\_snow\_man.mp3
  + [secret\_project]\_detailed\_proposal.docx → landscape.png
* Renamed files match those uploaded to Google Drive and later transferred to RM#2.

**Email Analysis:**

* Outlook PST shows coordinated communication with spy.conspirator@nist.gov.
* Key messages:
  + 2015-03-23 15:19 — Sample file (space\_and\_earth.mp4) sent.
  + 2015-03-23 16:38 — Email sent with Google Drive links to rename confidential files.
  + 2015-03-24–25 — Follow-up requests to deliver remaining data via removable media.

**Browser History:**

**Chrome History confirms searches for:**

* + *Data exfiltration methods* (data leakage methods, cloud storage)
  + *Anti-forensics tools* (ccleaner, eraser, delete data permanently)

**IE History confirms visits to:**

* + *CD burning instructions* (burn cd mastered vs live file system)
  + *USB forensics topics* (usb detection windows event log)

**USB History:**

* Registry (USBSTOR, MountedDevices) shows:
* RM#1 inserted 2015-03-23 14:31 and 2015-03-24 09:38.
* RM#2 inserted 2015-03-24 09:58, formatted at 2015-03-24 17:02.

**Anti-Forensics Activity:**

* Prefetch confirms execution of CCleaner.exe and Eraser.exe on 2015-03-25 10:50–11:15.
* Event Logs confirm uninstall of CCleaner and iCloud at 2015-03-25 11:18.

**A grid of white lines with black text

AI-generated content may be incorrect.**

**Removable Media (USB)**

**RM#1 (SanDisk Cruzer Fit — Authorized USB):**

* Contains original confidential files in Secret Project Data directories.
* Files match those later copied to the PC and renamed.

**RM#2 (SanDisk Cruzer Fit — “IAMAN $\_@”):**

* Contains renamed confidential files organized in a directory structure for exfiltration.
* Deleted files recovered match timeline activity (last modified ~2015-03-24 10:01).
* Quick format performed 2015-03-24 17:02, consistent with concealment attempt.

**Removable Media (CD-R RM#3)**

**RM#3 Session Analysis:**

* Type 1 (Session 1):
  + Burned confidential files renamed with abbreviated directories:
    - design → de
    - pricing decision → pd
    - progress → prog
  + File contents match renamed set from RM#2.
* Type 2 (Session Overwrite):
  + Anti-forensic overwrite with benign images (Koala.jpg, Penguins.jpg, Tulips.jpg).
* Type 3 (Final Session):
  + Remaining traces of confidential files recovered via carving.
  + Koala.jpg contains embedded ZIP detected with Binwalk, consistent with steganography (similar to landscape.png case).

**Removable Media (CD-R RM#3)**

**RM#3 Session Analysis:**

* Type 1 (Session 1):
  + Burned confidential files renamed with abbreviated directories:
    - design → de

**Key Observations**

* **Renamed Files Map:**
  + Renaming pattern confirmed across PC, RM#2, and RM#3.

A close up of a card

AI-generated content may be incorrect.

**7. Artifact Summary Table**

A white sheet with black text

AI-generated content may be incorrect.

A table of information

AI-generated content may be incorrect.

**8. Anti-Forensics & Metadata ($I30, $R/$I)**

**Recycle.Bin ($I / $R files):**

* Shift+Delete use on 2015-03-24 (S data removal) and quick formats of RM#2/CD (anti-forensics).
* Eraser run on 2015-03-25, but some $I metadata remained.
* Deleted confidential files (renamed files like happy\_holiday.jpg, snow\_man.mp3) align with your RM#2/CD content.Deletion metadata ($I files) recorded *who*, *when*, and *original location*.
* Actual deleted content ($R files) was recoverable in some cases.
* This was one of the primary deletion-tracking artifacts in the analysis.

**ShellBags:**

* Showed folder access even after folder deletion, especially S data and USB/CD directories

**Jump Lists & LNKs:**

* Pointed to renamed or deleted confidential files that were no longer in active directories.

**Windows Event Logs + Prefetch:**

* Recorded execution of *Eraser* and *CCleaner* close to deletion timestamps.

**LogFile & USN Journal:**

* Showed file creation, rename, and deletion activity, correlating with March 24–25 cleanup events.

**9. Findings and Correlation**

**File access and deletions happened at the same time as USB use**

* When RM#1 and RM#2 were plugged in, the same confidential project files were opened, renamed (like pricing\_decision.xlsx becoming happy\_holiday.jpg), and then deleted.
* RM#3 had folders and file names that matched RM#2, showing that the USB contents were burned to the CD-R.

**Registry shows the USB drives were connected**

* The USB logs (USBSTOR keys and setupapi.dev.log) show RM#1 and RM#2 being plugged in on March 23–24, which matches the timeline of the file copies and renames.

**Cloud software was installed around the same time as the data transfer**

* Google Drive and iCloud were installed right before the files were uploaded.
* Google Drive logs and Outlook emails match with file uploads and link sharing to [spy.conspirator@nist.gov](mailto:spy.conspirator@nist.gov).

**File timestamps show last access and deletion right before the system was taken**

* The system logs (MFT, $LogFile) show files being opened and deleted on March 24–25.
* Recycle Bin data ($I/$R files) confirms these deletions just before the device was seized.
* Logs also show Eraser and CCleaner being used to try and wipe traces before shutdown.

**10. Recommendations**

**Policy**

* Block USB devices that aren’t approved using Group Policy.
* Make it so employees need permission before installing apps like Google Drive, Dropbox, or VeraCrypt.
* Stop personal cloud accounts from being used on work computers.

**Technical**

* Install Endpoint Detection & Response (EDR) tools to catch strange behavior like renaming lots of files or big uploads to the cloud.
* Turn on logging for things like USB use, file changes, and shared folder access so there’s a record.
* Use Data Loss Prevention (DLP) to detect and block confidential files from being sent to USBs or the cloud.

**Training**

* Train employees regularly on how to handle company data and watch for insider threats.
* Remind everyone about company security rules and test them with exercises.
* Encourage staff to report anything suspicious without worrying about getting in trouble.

**11. Conclusion**

Based on the forensic analysis conducted on July 29, 2025, at 05:15 PM PDT, the evidence acquisition and verification process utilizing Autopsy and FTK Imager has successfully captured forensic images of the suspect’s laptop and USB device. Multiple Images were verified using SHA1 hash values to ensure their integrity, with the specific hash values to be documented upon completion of the imaging process. The chain of custody, established from 04:00 PM PDT, tracks the seamless transfer of evidence from collection and were reviewed by Love Taule, Gian Austria, and Aireen Maddela, maintaining a secure and verifiable trail.

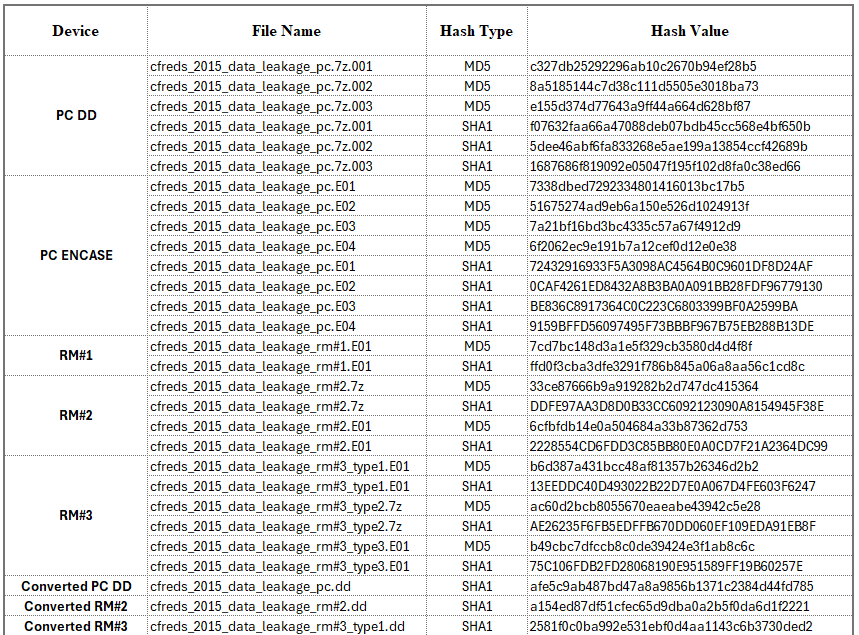
The analysis of the PC image, RM#2, and RM#3 images revealed significant digital artifacts, including user activities, file manipulations, and external device interactions between March 22, 2015, and March 25, 2015. Key findings include the suspect’s research into data leakage methods, use of cloud services (Google Drive), and the burning of a CD-R containing renamed confidential files, suggesting potential data exfiltration. E-mail communications with spy.conspirator@nist.gov further indicate coordinated activities, with deleted messages recovered from the OST file providing critical insights.

The evidence remains in a verified and sealed condition, ready for further legal or investigative proceedings. The integrity of the data, confirmed through hash matching, supports its admissibility, while the detailed timeline and artifact analysis provide a robust foundation for understanding the suspect’s actions. Analysis revealed that files were renamed and hidden using different file formats to evade detection. IAMan also employed antiforensic tools to clean up the system, leaving minimal traces of activity. This was subsequently followed by the submission of a resignation. Additional analysis or expert testimony may be required to correlate these findings with the broader investigation context

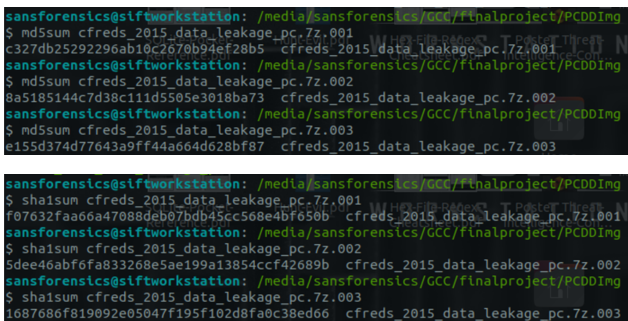
**12. Appendices**

* Chain of Custody logs
* Tool output screenshots (hash verification, $MFT views)

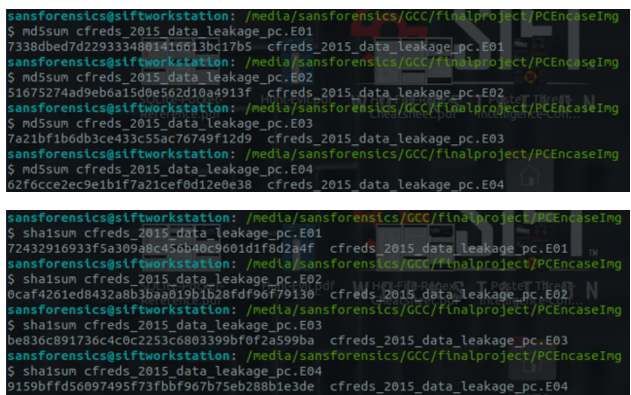
**Hash Values:**

****

**PC Image:**

****

**PC Encase:**

****

**RM#1**

**A screen shot of a computer

AI-generated content may be incorrect.**

**RM#2 DD**

**A screen shot of a computer

AI-generated content may be incorrect.**

**RM#2 Encase**

**A screen shot of a computer

AI-generated content may be incorrect.**

**RM#3 DD**

A screen shot of a computer

AI-generated content may be incorrect.

**RM#3Encase**

A screen shot of a computer

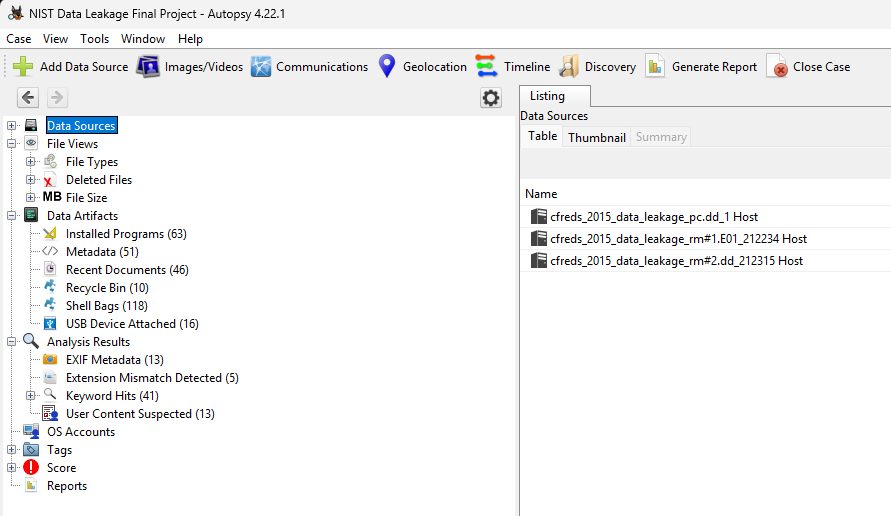
AI-generated content may be incorrect.

**RM#3 Raw**

A screen shot of a computer

AI-generated content may be incorrect.

**Chain of Custody Screenshots through AUTOPSY:**



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Metadata:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

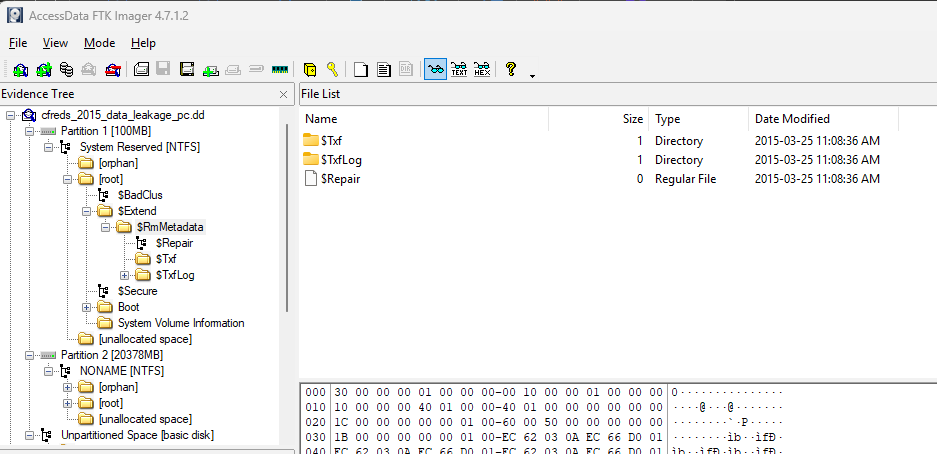
AI-generated content may be incorrect.

High Entropy when uploading RM#3 file on Autopsy:

A screenshot of a computer

AI-generated content may be incorrect.

**FTK Imager:**



A screenshot of a computer

AI-generated content may be incorrect.

**NTFS from FTK**

A screenshot of a computer

AI-generated content may be incorrect.

**Some of the Recovered Hidden Confidential Files:**

********************************

**Evidence Transfer Logs**

**A black and white text on a white background

AI-generated content may be incorrect.**

**Summary of Events:**

**A diagram of data leakage

AI-generated content may be incorrect.**

**References**

AccessData. (n.d.). *FTK Imager version 4.2.0 user guide*. <https://ad-pdf.s3.amazonaws.com/FTKImagerUserGuide.pdf>

Ballenthin, W. (n.d.). *Shellbags forensics*. <http://www.williballenthin.com/forensics/shellbags>

Carvey, H. (2013). *Recycle bin forensics*. <https://windowsir.blogspot.com/2013/08/recycle-bin-forensics.html>

Carvey, H. (n.d.). *Program execution artifacts (Prefetch, registry, logs)*. <https://windowsir.blogspot.com>

Carvey, H. (n.d.). *Windows CD/DVD burning artifacts*. <https://windowsir.blogspot.com>

Chrome Developers. (n.d.). *Chrome user data (history, cache, cookies) location*. <https://chromium.googlesource.com>

Kroll Cyber Risk. (n.d.). *Windows jump list forensics*. <https://www.kroll.com/en/insights/publications/cyber/windows-jump-list-forensics>

Microsoft. (n.d.). *USB device history in registry and SetupAPI logs*. <https://learn.microsoft.com/en-us/windows-hardware/drivers/usbcon>

National Institute of Standards and Technology. (2015). *Data leakage case*. NIST Computer Forensic Reference Data Sets (CFReDS). <https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html>

NirSoft. (n.d.). *PST viewer & Outlook forensics*. <https://www.nirsoft.net/utils/outlook_tools.html>

OpenText. (n.d.). *EnCase forensic imager 7.x documentation*. <https://www.opentext.com/file_source/OpenText/en_US/PDF/encase-forensic-user-guide.pdf>

Plaso Developers. (n.d.). *Plaso (log2timeline) documentation*. <https://plaso.readthedocs.io>

SANS Institute. (n.d.). *SIFT workstation user guide*. <https://digital-forensics.sans.org/community/downloads>

Sleuth Kit. (n.d.). *The Sleuth Kit & Autopsy forensic browser*. <https://sleuthkit.org>

Swift Forensics. (2013). *Windows LNK file forensics*. <https://www.swiftforensics.com/2013/07/windows-link-lnk-files.html>