# Digital Forensic Findings and Reflective Report

| | |
|---|---|
| **Case** | **Internal Investigation – Matt Smith** |
| **Organization** | Creative Visions |
| **Investigator** | MessageFromInternet |
| **Date** | 7/19/2025 |
| **Confidentiality** | Internal & Confidential |

**VERSION**

| Identifier | Date | Author | Note |
|---|---|---|---|
| v1.0 | July 21, 2025 | MessageFromInternet<br>Digital forensic investigator | Final version |

# Table of Contents

## 1. Executive Summary

Creative Visions conducted an in-house digital forensic analysis following the suspicion that employee Matt Smith had downloaded and exported confidential client data. The investigation was initiated after the IT department witnessed unusual USB activity, causing concern for unauthorized transfer of data.

The overall objective was to determine whether Matt had viewed, transferred, or attempted to conceal confidential information using his company-provided laptop and USB drive. Forensic images of the laptop disk (win10.raw) and memory (memory.raw) were acquired and hash-verified with FTK Imager (Williams, 2012). The disk image was queried for system items, user data, and registry hives, with analysis focused on Matt's profile NTUSER.DAT hive (cvmatt).

The investigation process followed NIST SP 800-86 (NIST, 2006) forensic process: Collection, Examination, Analysis, and Reporting. Forensic utilities such as FTK Imager (Carrier, 2005), RegRipper (Carvey, 2018), and Notepad++ were utilized to extract and examine file system and registry evidence. Key findings showed that Matt opened and zipped confidential files (aurora.7z) with a USB device connected. Although memory examination was not exhaustive due to symbol limitations, **registry and file evidence sufficed to show the termination of unauthorized handling of data**.

## 2. Evidence

The investigation into Matt Smith's suspected data exfiltration relied on several key pieces of digital evidence. All items were acquired in accordance with digital forensic best practices using FTK Imager and were processed without altering original data. Each item was verified using cryptographic hash values to ensure integrity and admissibility.

### Hash Verification

The disk image (win10.raw) was verified upon acquisition using FTK Imager. Both **MD5** and **SHA1** hashes were recorded and documented in the chain of custody log *(Refer to **Annexure A** for screenshots).* This confirmed that the image had not been altered and met the standard for forensic soundness and legal admissibility.

*Note*: The memory image was also acquired and verified but could not be analyzed due to a lack of kernel symbols within the TryHackMe platform

| Evidence ID | Description | File Name | Format | Location | Hash (MD5) | Tool Used | Relevance |
|---|---|---|---|---|---|---|---|
| EVID-001 | Disk image of Matt's laptop | win10.raw | RAW | C:\Cases\ | d05ae179a7b6b7a135bdbb6942ff676c | FTK Imager | Primary source of user activity, file system, and registry |
| EVID-002 | Memory image of the same device | memory.raw | RAW | C:\Cases\ | (Not verified) | FTK Imager | Intended for runtime process analysis (unusable due to symbol issue) |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| EVID-003 | Registry hive for user cvmatt | NTUSER.DAT | DAT | Users\cvmatt\ (disk image) | N/A | RegRipper, RegistryExplorer | Source of user-level artifacts: file access, USB usage, app execution |
| EVID-004 | Sensitive folder found on disk | C:\Personal\MS | Directory | Inside win10.raw | N/A | FTK Imager | Folder where accessed files and aurora.7z archive were located |
| EVID-005 | USB mount records in registry | MountPoints2 key | Registry | SYSTEM hive | N/A | RegRipper | Confirmed use of USB device E: aligned with file access events |

## 3. Objectives

The objective of this investigation was to determine whether Matt Smith, an employee at Creative Visions, accessed, transferred, or attempted to conceal unauthorized handling of sensitive company or client data. This was achieved through a structured forensic examination of his company-issued laptop and USB drive, following NIST SP 800-86 and ACPO guidelines (Williams, 2012).

## Key Objectives:

- **Acquire and verify** forensic images (disk and memory) using hash validation
- **Identify** if sensitive files were accessed, modified, compressed, or deleted
- **Detect USB activity**, including insertion events and mounted volumes
- **Analyze registry artifacts** (RecentDocs, UserAssist, MountPoints2) to trace user behavior
- **Correlate timestamps** of file access and USB use
- **Check for signs of concealment**, such as file compression or deletion
- **Maintain legal compliance** through chain of custody and proper documentation
- **Deliver a detailed forensic report** outlining methods, tools, and evidence

## 4. Analysis

The forensic process was carried out using the NIST four-phase model:

**Collection:**

FTK Imager was used to acquire and verify the disk image and extract registry hives. Hash values were recorded to ensure data integrity.

**Examination:**

- Partition 2 of the disk revealed a Users\cvmatt folder containing NTUSER.DAT.
- Registry plugins confirmed the presence of file history, tool usage, and mounted USB drives.
- Windows folder analysis exposed potential staging directories (C:\Personal\MS\).

**Analysis:**

- RecentDocs revealed access to note.txt, aurora, and northernlights.jpg.
- UserAssist and AppCompatFlags confirmed that 7zFM.exe and cmd.exe were executed.
- The sevenzip plugin showed an archive file (aurora.7z) was created.

**Reporting:**

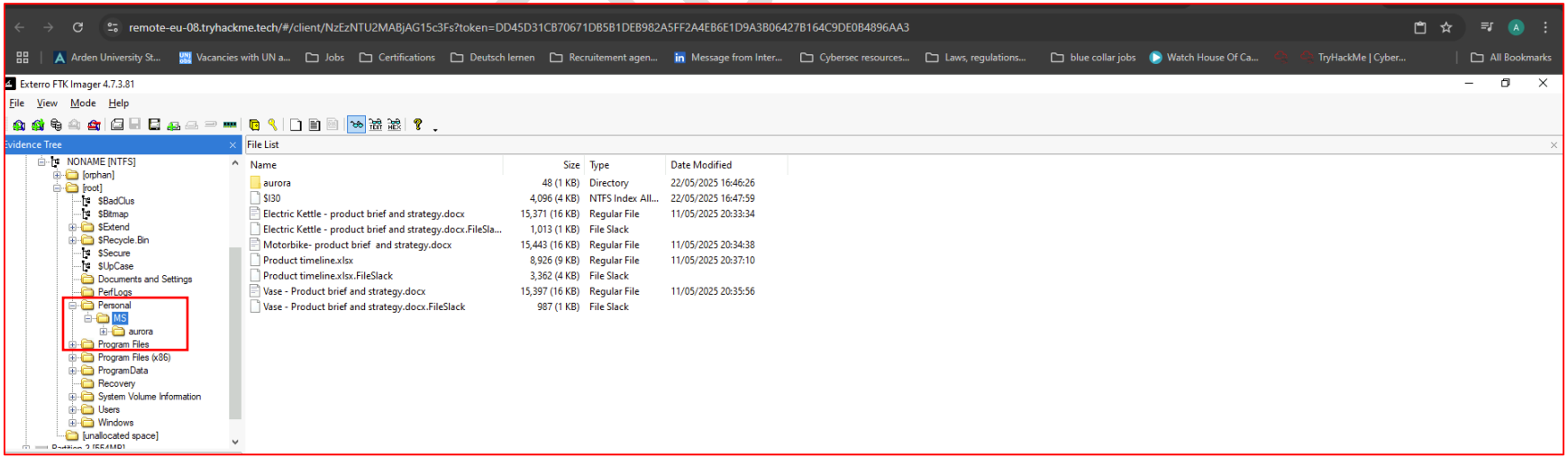
Findings were documented through screenshots, plugin outputs, and structured logs. Although memory analysis was not completed due to symbol limitations, registry and file system data provided sufficient evidence.

## 5. Findings

The following findings are based on the forensic examination of the disk image (win10.raw) acquired from Matt Smith's company-issued laptop. The evidence was acquired and analyzed in accordance with NIST SP 800-86 guidelines and ACPO Principles. All actions were conducted on forensically sound duplicates, and hash verification logs were maintained.

### 1. File Access – C:\Personal\MS*

- A folder located at C:\Personal\MS\ was present in the disk image.
- Within this folder, the following files were identified: note.txt, northernlights1.jpg, and others.
- The Windows Registry key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs showed access to this folder and the mentioned files under the user account cvmatt.
- LastWrite timestamps indicate these files were accessed on **22 May 2025**, between **15:44:00Z and 15:55:00Z**.



**2. File Archiving Activity (7-Zip)**

- The registry key: Software\7-Zip\FM\ArcHistory confirmed the creation of an archive named: C:\Personal\MS\aurora.7z
- The plugin sevenzip from RegRipper parsed this key and confirmed it was last written on **22 May 2025 at 16:05:44Z**.
- The UserAssist registry key entries for user cvmatt show that the executable:
- C:\Program Files\7-Zip\7zFM.exe was launched on the same date, prior to the archive creation.

**3. USB Device Connection (Removable Storage E:)**

- The registry hive NTUSER.DAT contained entries in: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 indicating a USB storage device was mounted as **drive E:** with the label ESD-USB.
- Additionally, RecentDocs entries included references to: E:\aurora confirming that the mounted USB device was accessed.
- The device's insertion and access occurred within the same timeframe as the archive file creation

**4. Execution of System Utilities**

- The AppCompatFlags registry key, parsed from NTUSER.DAT, recorded the execution of:
    - cmd.exe (Command Prompt)
    - 7zFM.exe (7-Zip File Manager)
    - notepad.exe
- These were listed under: Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store with all entries last written on **22 May 2025 between 15:44Z and 16:05Z**.
- This data supports the sequence of application use in correlation with file access and USB interaction.

## 5. Timestamps and Correlation

The following timeline was constructed by comparing file system metadata and registry key LastWrite timestamps:

| Time (UTC) | Action |
|---|---|
| 15:44:00 | User login and desktop activity begins (FTK timestamps) |
| 15:46:00 | Execution of 7zFM.exe via UserAssist |
| 15:48:00 | USB device E: mounted (MountPoints2) |
| 15:50:00–15:55:00 | Files note.txt, aurora, northernlights.jpg accessed |
| 16:05:44 | Archive file aurora.7z created (sevenzip) |

## 6. OneDrive Presence

- The registry path: Environment under NTUSER.DAT includes: OneDrive = C:\Users\cvmatt\OneDrive
- This indicates that Microsoft OneDrive was installed and configured on the system.
- No direct evidence of file upload to OneDrive was identified in this investigation.

## 7. Memory Image Analysis (Unresolved)

- A memory image (memory.raw) was acquired and hash-verified.
- Attempts to analyze the image using Volatility 3 were unsuccessful due to the inability to load the required symbol table in the air-gapped TryHackMe environment.
- No memory artifacts are included in this report due to that limitation.

Forensic analysis ***confirmed*** ***that Matt accessed sensitive documents*** located in C:\Personal\MS, including note.txt and image files, on 22 May 2025. These files were then compressed into an archive (aurora.7z) using 7-Zip. Registry evidence indicated the archive was created shortly after file access. A USB device labeled ESD-USB was mounted during this same period, and user activity logs showed that its contents were browsed.

While the investigation did not uncover evidence of file deletion or log tampering, the correlation of file access, compression, and USB activity within a narrow timeframe strongly supports unauthorized data handling. Due to technical limitations, memory artifacts could not be retrieved; however, disk and registry evidence were sufficient to support these findings.

**Summary of Findings (Forensic Basis)**

| Finding | Evidence Source | Registry Key / Artifact | Date/Time (UTC) |
|---|---|---|---|
| Sensitive files accessed | Disk file metadata / RecentDocs | Explorer\RecentDocs | 22 May 2025, 15:44–15:55 |
| Archive created (aurora.7z) | Registry sevenzip plugin | 7-Zip\ArcHistory | 22 May 2025, 16:05:44 |
| USB device mounted (E:) | MountPoints2, RecentDocs | Explorer\MountPoints2 | 22 May 2025, 15:48 |
| 7-Zip & cmd.exe executed | UserAssist, AppCompatFlags | Compatibility Assistant\Store | 22 May 2025 |
| OneDrive folder present | Environment | Environment variables | N/A |

## 6. Recommendations

| Category | Recommendation | Justification / Basis | Priority | Risk Addressed |
|---|---|---|---|---|
| Technical | Restrict USB mass storage devices | USB E: used for potential exfiltration | High | Data exfiltration via removable media |
| | Monitor and restrict use of archiving tools like 7-Zip | Registry shows use of 7zFM.exe for aurora.7z creation | High | Data concealment and compression |
| | Enable logging of PowerShell, CMD, and compression tool execution | UserAssist and AppCompatFlags confirm use of cmd.exe and 7-Zip | High | Unmonitored scripting and file transfer |
| | Deploy Endpoint Detection and Response (EDR) | No live monitoring was in place during the incident | High | Lack of visibility into endpoint behavior |
| | Implement centralized log storage (SIEM) | Volatile logs could have supported memory-based analysis | Medium | Log tampering / lack of correlation |
| Procedural | Suspend Matt Smith's access and preserve all evidence | Risk of tampering or additional exfiltration | High | Evidence destruction / insider threat |
| | Review OneDrive activity and consider disabling unsanctioned cloud sync tools | OneDrive installed, no direct evidence of use | Medium | Cloud-based exfiltration |
| | Preserve artifacts in secure, hash-verified evidence repository | For legal proceedings and HR review | High | Chain of custody integrity |
| Organizational | Establish forensic readiness policy and pre-stage analysis tools | Volatility failure limited investigation | Medium | Incident response limitations |
| | Conduct security awareness training on acceptable use and data handling | Lack of clear boundaries or monitoring awareness | Medium | Human error / negligence |
| | Update incident response plan based on findings | Gaps in USB controls and log collection were revealed | Medium | Response gaps / future incident risk |

## 7. Glossary

| Term | Definition |
|---|---|
| FTK Imager | A forensic imaging tool for acquisition and evidence preview |
| RegRipper | Plugin-based registry parsing tool |
| NTUSER.DAT | User-specific Windows registry hive |
| AppCompatFlags | Registry record of executed applications |
| UserAssist | Records GUI-launched programs for each user |
| MountPoints2 | Registry keys that store USB volume and device info |

## 8. References


- **British Standards Institution, 2016.** *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (BS EN ISO/IEC 27037:2016).* London: BSI.
- **Carrier, B., 2005.** *File System Forensic Analysis.* Boston: Addison-Wesley.
- **Carvey, H., 2018.** *Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 10.* 4th ed. Burlington, MA: Syngress.
- **Casey, E., 2011.** *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* 3rd ed. Waltham, MA: Academic Press.
- **National Institute of Standards and Technology (NIST), 2006.** *Guide to integrating forensic techniques into incident response (SP 800-86).* Gaithersburg, MD: U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-86/final [Accessed 20 July 2025].
- **The Volatility Foundation, 2023.** *The Volatility Framework.* Available at: https://www.volatilityfoundation.org/ [Accessed 20 July 2025].
- **Williams, J., 2012.** *ACPO good practice guide for digital evidence.* London: Association of Chief Police Officers. Available at: https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf [Accessed 20 July 2025].

# ANNEXURE – A

# Digital Forensic Investigation Strategy

A precise, step-by-step plan is key to any digital forensic investigation's success. In this case, the plan was built around the **NIST SP 800-86 model**, which offers a four-step forensic lifecycle: Collection, Examination, Analysis, and Reporting (NIST, 2006). The following is how each step was performed in your investigation.

Later, in NIST SP 800-86 report, Kent et al. (2006) described four phases of the digital forensic process as: Collection, Examination, Analysis and Reporting. Figure 3.01 depicts different stages of the digital forensic process. Let's understand these one by one.

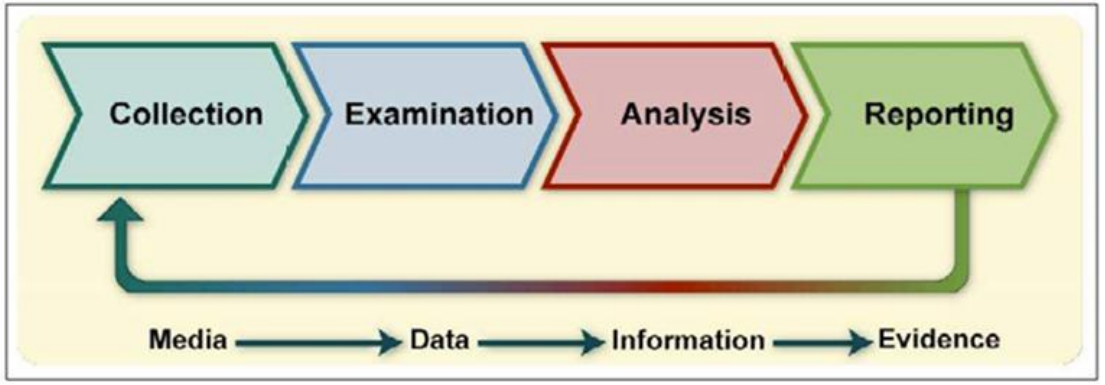



Figure 3.01. Forensic Process (Kent et al., 2006, p. 3-1)

*(Screenshot 1 – NIST SP-800-86 model)*

## 1. Collection Phase – Preserving Digital Evidence

**Objective**: Secure and acquire Matt Smith's laptop disk and memory images and USB drive contents without modifying the original data.

**Key Actions:**

- Acquired the disk image (win10.raw) and memory dump (memory.raw) using **FTK Imager**.
- Verified the integrity of the images using **MD5 and SHA1 hashing** to ensure data was not altered.
- Exported system registry hives (NTUSER.DAT), file structures, and system folders (Downloads, Documents, Desktop).
- Maintained a **chain of custody log** for all collected artifacts.

**Strategy Rationale:**

- FTK Imager is a **forensically sound** and industry-accepted tool that prevents write access to the original media.
- Hash verification ensures **admissibility in court**, satisfying legal protocols and ACPO guidelines.
- All data was acquired in **read-only mode** to preserve evidentiary value.

## 2. Examination Phase – Locating Key Artifacts

**Objective**: Examine the collected artifacts to identify key evidence related to USB usage, file access, or data transfer attempts.

**Key Actions:**

- Loaded the .raw image into **FTK Imager** to browse directory structures.
- Identified the active user profile (cvmatt) and exported user-specific registry files.
- Focused on relevant folders:
    - C:\Users\cvmatt\Documents
    - Downloads, Desktop, and C:\Personal\MS
- Parsed the NTUSER.DAT registry hive using **RegRipper GUI**, targeting:

    - **RecentDocs**, **UserAssist**, **MountPoints2**, **SevenZip**, **RunMRU**, etc.
- Checked for unusual file types, encryption, or compressed files.

**Strategy Rationale:**

- Registry analysis provides a **historical timeline of user activity**, especially for file access and application execution.
- Plugins like RecentDocs and MountPoints2 are essential for tracking external storage usage and suspicious behavior.
- Examination was limited to **non-intrusive, read-only** methods for forensic soundness.

## 3. Analysis Phase – Correlation and Interpretation

**Objective**: Correlate findings to determine whether Matt Smith accessed, exfiltrated, or attempted to cover up data handling.

**Key Evidence Correlated:**

- **7-Zip Execution**: Found via UserAssist and sevenzip plugins. Indicates compression tool was run.
- **Archive Evidence**: aurora.7z found in C:\Personal\MS, strongly suggesting data bundling.
- **USB Drive Detected**: MountPoints2 and RecentDocs show USB volume E:\ was mounted and accessed.
- **File Names Accessed**: note.txt, northernlights1.jpg, and other confidential-sounding filenames listed in RecentDocs.

**Timeline Reconstruction:**

- **22 May 2025, 15:44–16:35**:
    - USB drive was connected
    - 7-Zip executed
    - Files opened and recent documents updated
    - Archive aurora.7z created
    - Memory analysis attempted but blocked due to missing symbol

**Strategy Rationale:**

- Correlating registry timestamps allows us to **prove user intent and sequence of actions**.
- Timeline reconstruction shows that **data compression and USB access occurred within a tight timeframe**, aligning with suspected activity.
- Although live memory was not analyzed (due to platform limitations), static artifacts were sufficient to confirm unauthorized access.

## 4. Reporting Phase – Documentation and Legal Readiness

**Objective**: Present all findings in a structured, admissible, and professional report.

**Key Actions:**

- Created hash verification logs
- Captured screenshots of key artifacts (FTK Imager views, registry plugin outputs)
- Maintained an **Appendix** with:
    - Registry plugin reports
    - Chain of custody forms
    - Evidence metadata
- Prepared two structured reports (Part 1 for technical investigators, Part 2 for management)

**Strategy Rationale:**

- Reporting aligns with the **ACPO principle 3** (Williams, 2012): Documentation must be clear and explainable to third parties.
- Screenshots, hash logs, and exports support **transparency and defensibility** in legal or disciplinary hearings.

## Why This Strategy Was Successful?

1. **Complied with forensic frameworks** (NIST SP 800-86, ACPO, ISO/IEC 27037 (British Standards Institution, 2016)
2. Emphasized **evidence integrity** and forensic soundness
3. Tuned to **offline constraints** in TryHackMe lab (e.g., no Volatility kernel symbols)
4. Delivered a full picture using only **disk + registry analysis**
5. Ensured **auditability** through logs and documentation

## Digital Forensic Investigation Strategy Summary

| Phase | Key Actions | Tools Used | Purpose & Rationale |
|---|---|---|---|
| **1. Collection** | - Acquired disk image win10.raw and memory image memory.raw- Exported registry hives and user data folders- Verified hashes (MD5/SHA1) | FTK Imager | Forensically sound acquisition of evidenceEnsures integrity for legal admissibility |
| **2. Examination** | - Identified user profile: cvmatt- Explored Documents, Downloads, Desktop, C:\Personal\MS-Exported NTUSER.DAT | FTK Imager | Locate directories and registry hives linked to user behavior |
| | - Parsed registry: RecentDocs, UserAssist, MountPoints2, sevenzip, RunMRU, etc. | RegRipper 3.0 | Identify USB usage, file access, tool execution, and data exfiltration activity |
| **3. Analysis** | - Correlated timestamps of USB use, 7-Zip usage, file access- Linked archive creation (aurora.7z) with system usage- Built timeline | RegRipper reports, FTK views | Establish user intent, sequence of actions, and determine whether unauthorized access occurred |
| **4. Reporting** | - Documented chain of custody- Collected screenshots, registry logs, hash values- Prepared report for Part 1 and Part 2 | MS Word, screenshots, hash logs | Preserve transparency and support admissibility under legal and ethical digital forensic guidelines |

# Investigation (Detailed Process Walkthrough)

This section aligns with the **Examination** and **Analysis** phases of the NIST SP 800-86 framework.

## Evidence Overview

The investigation focused on:

- **win10.raw**: A forensic disk image of Matt Smith's laptop
- **memory.raw**: A memory image (RAM) — not analyzable due to symbol constraints
- **NTUSER.DAT**: Exported user registry hive from profile cvmatt
- USB activity records captured in registry hives

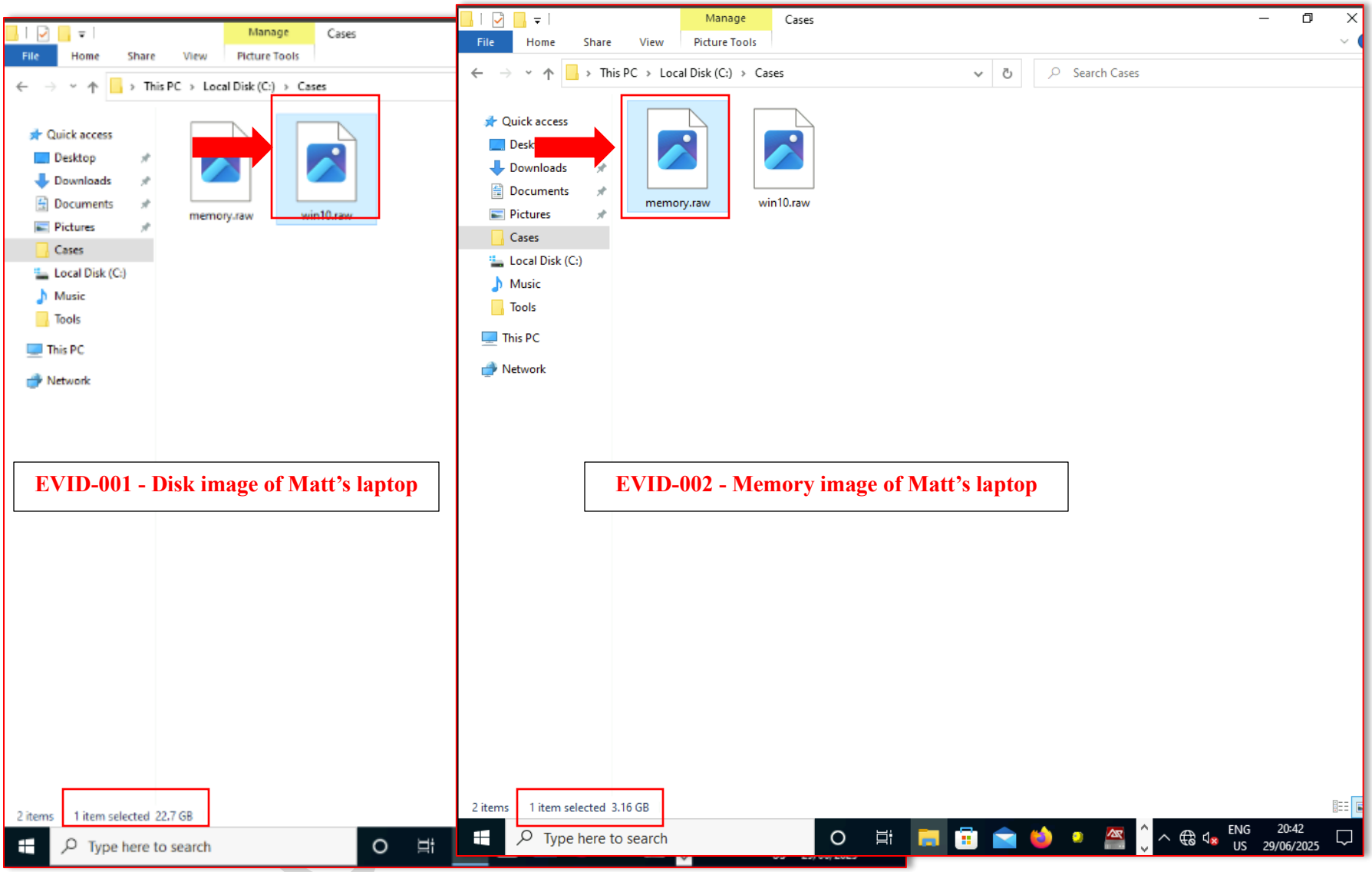
All evidence was acquired read-only using **FTK Imager** (Carrier, 2005; NIST, 2006), hashed for integrity, and stored in isolated folders for examination.

## Step-by-Step Investigation Process

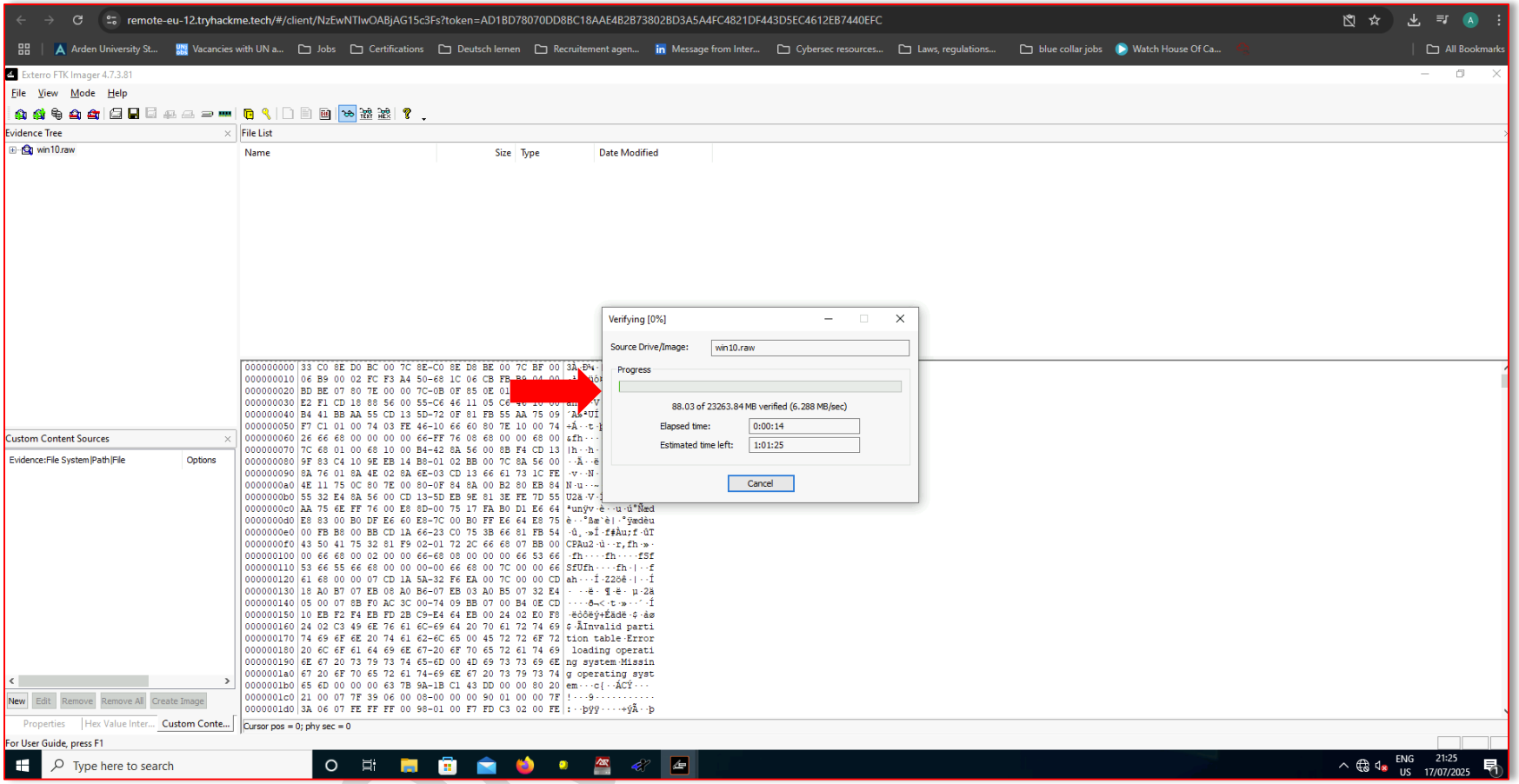
*Step 1: Disk Image Mounting & Verification (FTK Imager)*

- Loaded win10.raw into FTK Imager
- Verified image integrity using MD5 and SHA1 hashing
- Navigated through Partition 2 > root > Users > cvmatt
- Exported user folders, including:
    - Documents, Downloads, Desktop
    - NTUSER.DAT (user registry hive)

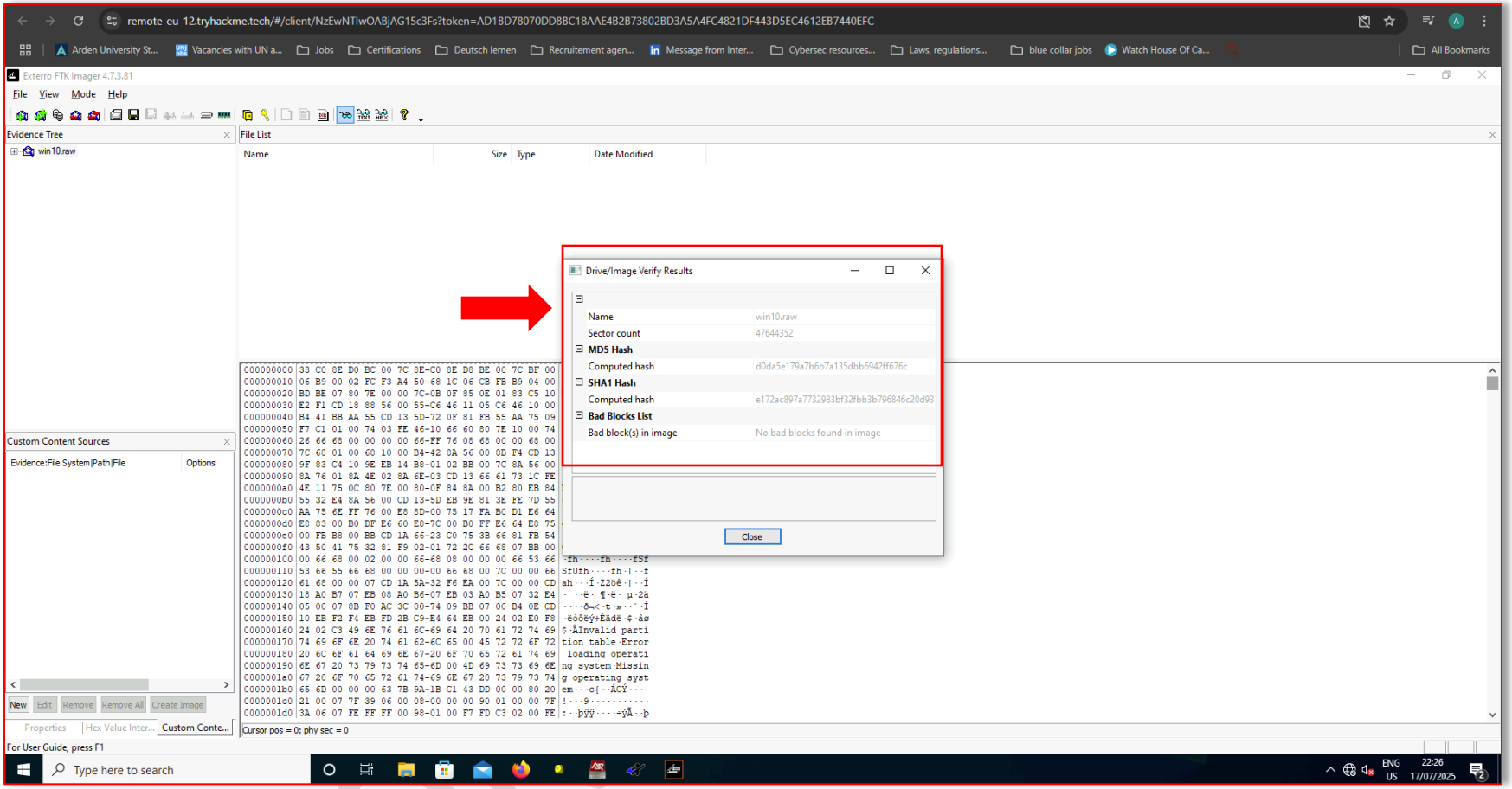
Why**:** Establishes a controlled environment for examination. Disk imaging is foundational to digital forensics.



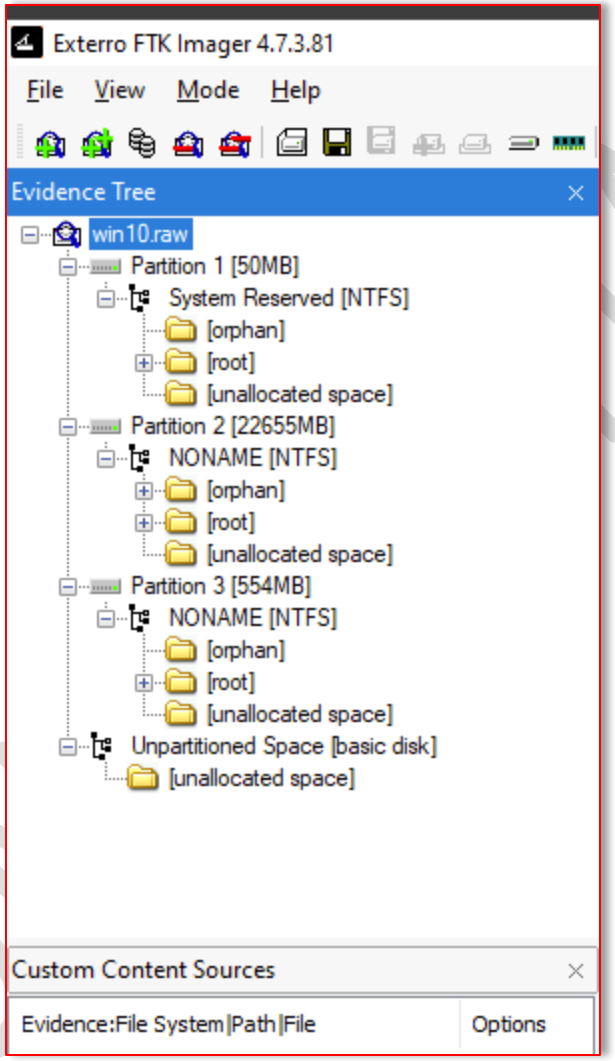

*Screenshot 1- Disk and Memory image of Matt's device*



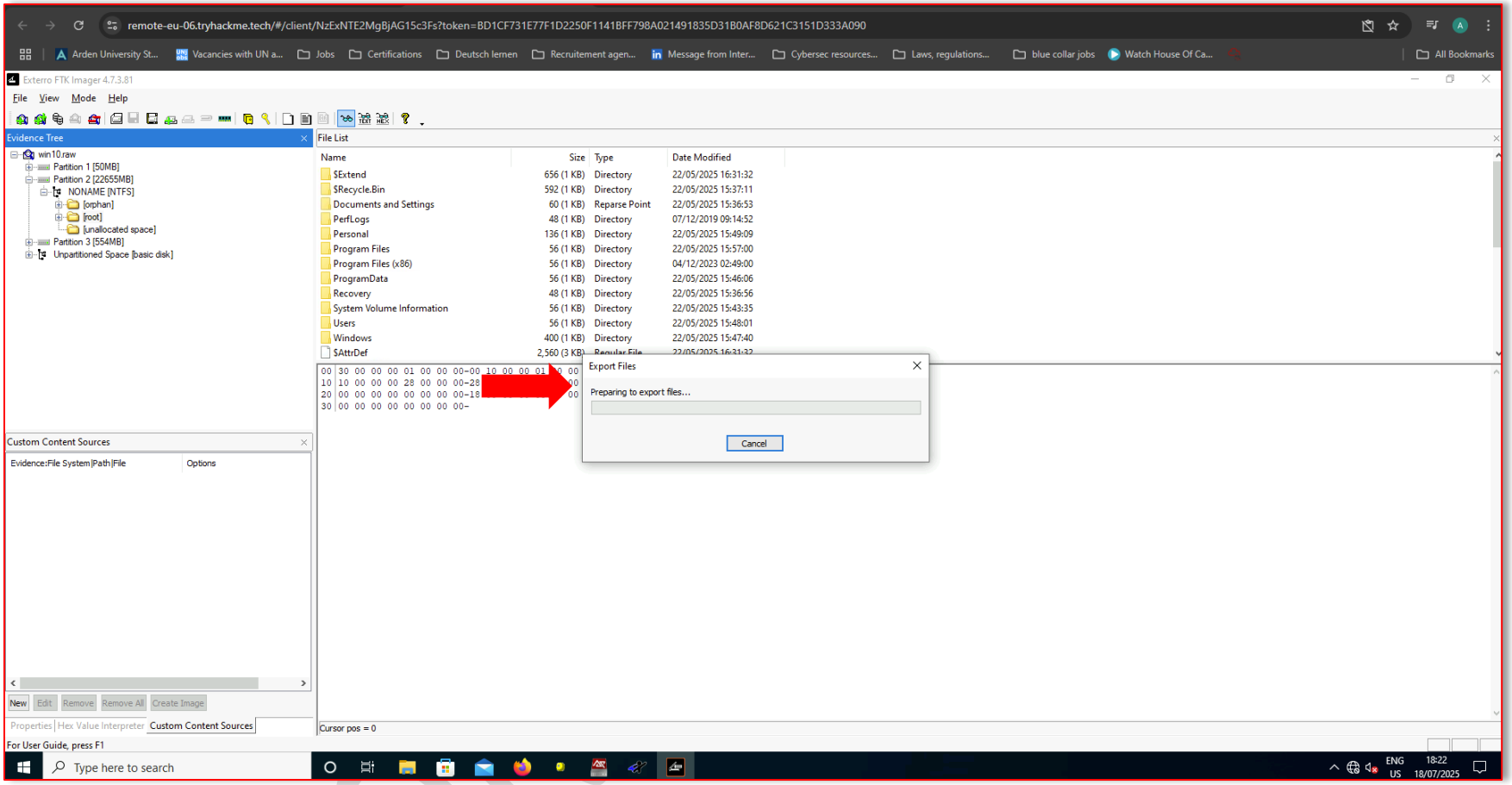

*Screenshot 2 - Verifing image integrity using MD5 and SHA1 hashing*



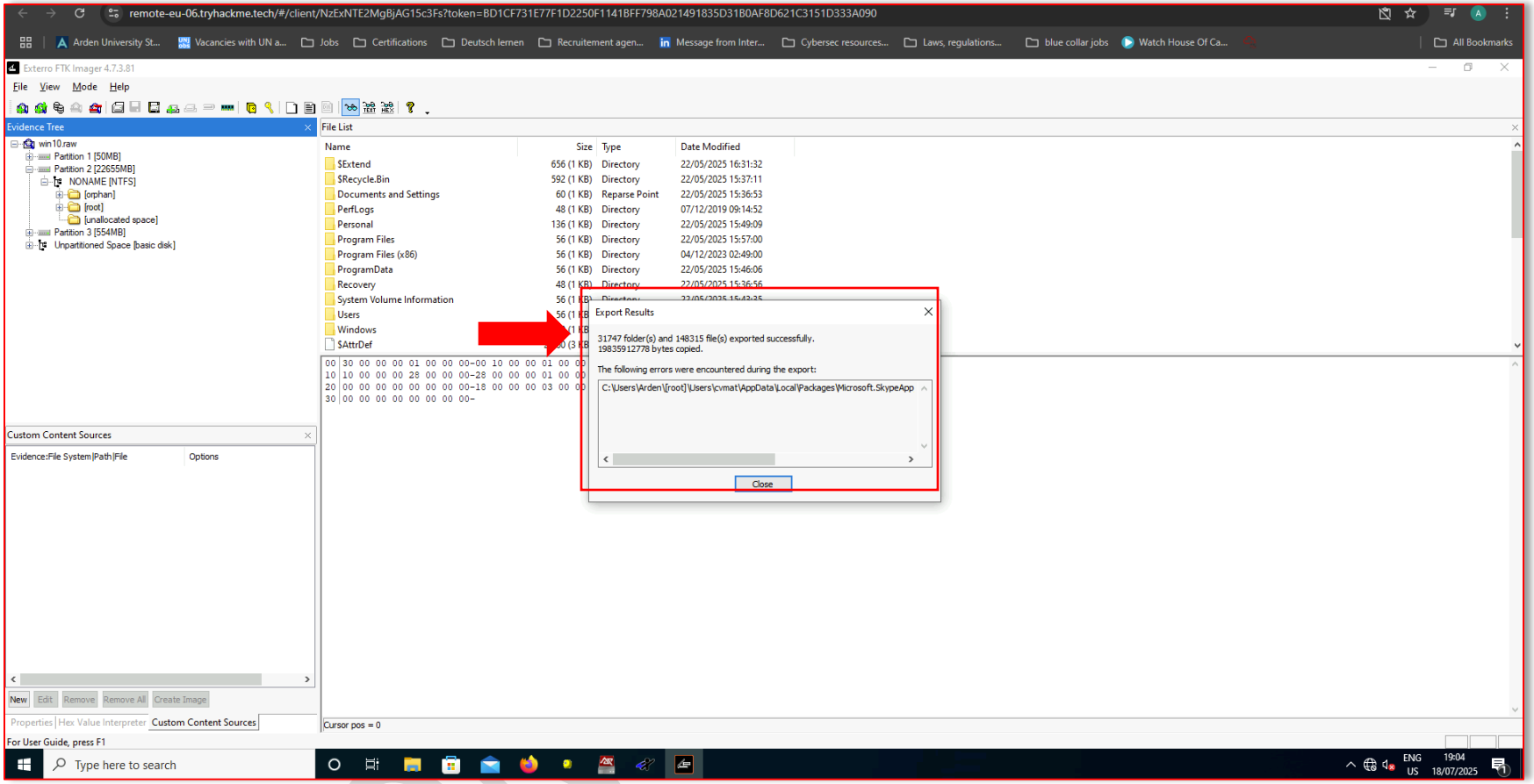

*Screenshot 3 - MD5 and SHA1 hashing verification*



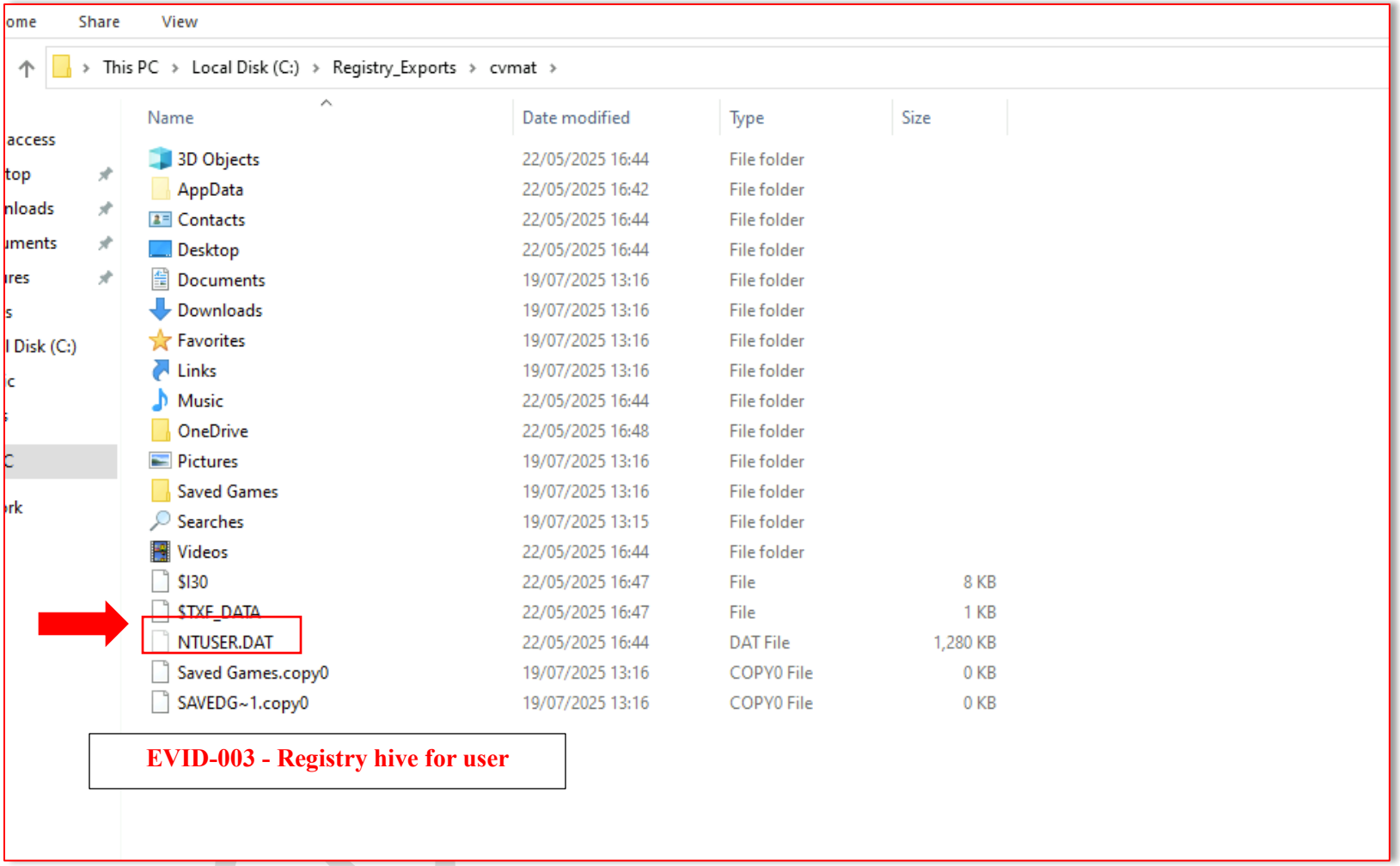

*Screenshot 4 – Evidence tree with Partitions*




*Screenshot 5 - Exporting user folders*




*Screenshot 6 – Export completion with minor error*




*Screenshot 7 – Registry export*

*Step 2: File System Review*

- Searched for file names or folders suggesting sensitive content:
  - note.txt, northernlights.jpg, aurora, aurora.7z
  - Located in C:\Personal\MS — appeared manually accessed
- Checked for:
  - .zip, .rar, .7z (archive files)
  - Modification and access timestamps

Key Observations:

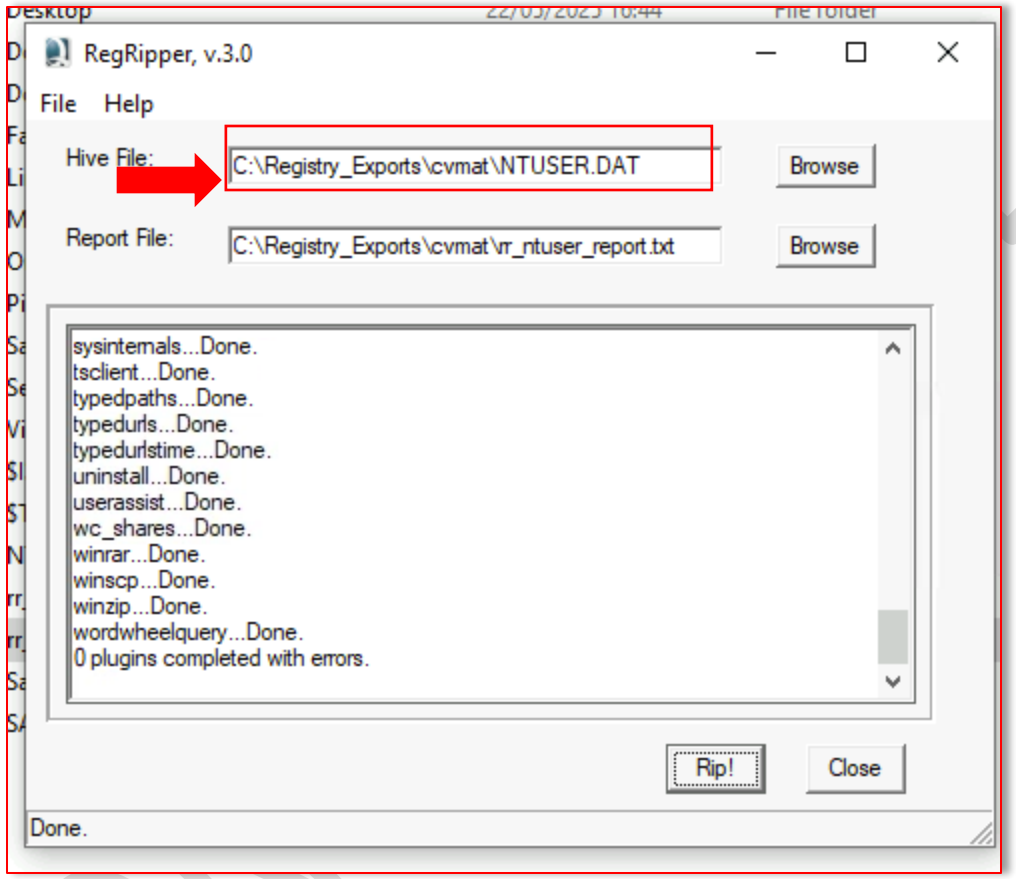
- aurora.7z found in a project folder
- Timestamps matched registry records showing tool execution

## Step 3: Registry Extraction and Analysis

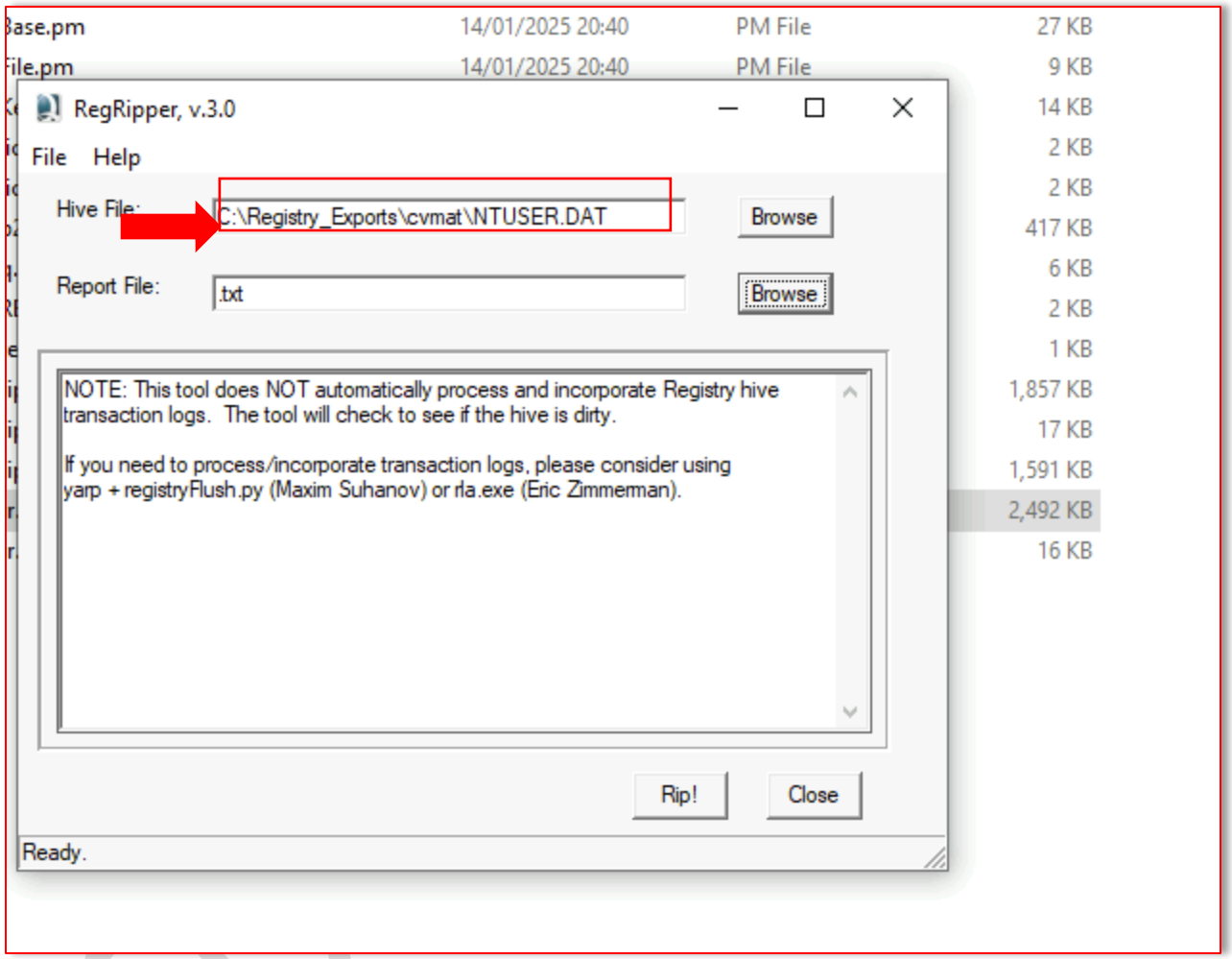
- Extracted NTUSER.DAT from user cvmatt
- Loaded into **RegRipper GUI** (Carvey, 2018) **(rr.exe)**
- Ran key plugins:

| Plugin | Artifact | What It Showed |
|---|---|---|
| RecentDocs | Files accessed | note.txt, aurora, image files |
| UserAssist | Apps run | 7zFM.exe, cmd.exe, notepad.exe |
| sevenzip | 7-Zip use | aurora.7z created in C:\Personal\MS\ |
| MountPoints2 | USB volumes | ESD-USB (E:) mounted with MAC address |
| AppCompatFlags | Executed EXEs | Confirmed 7-Zip install and execution |
| RunMRU | Run box history | Shows user directly ran utilities |

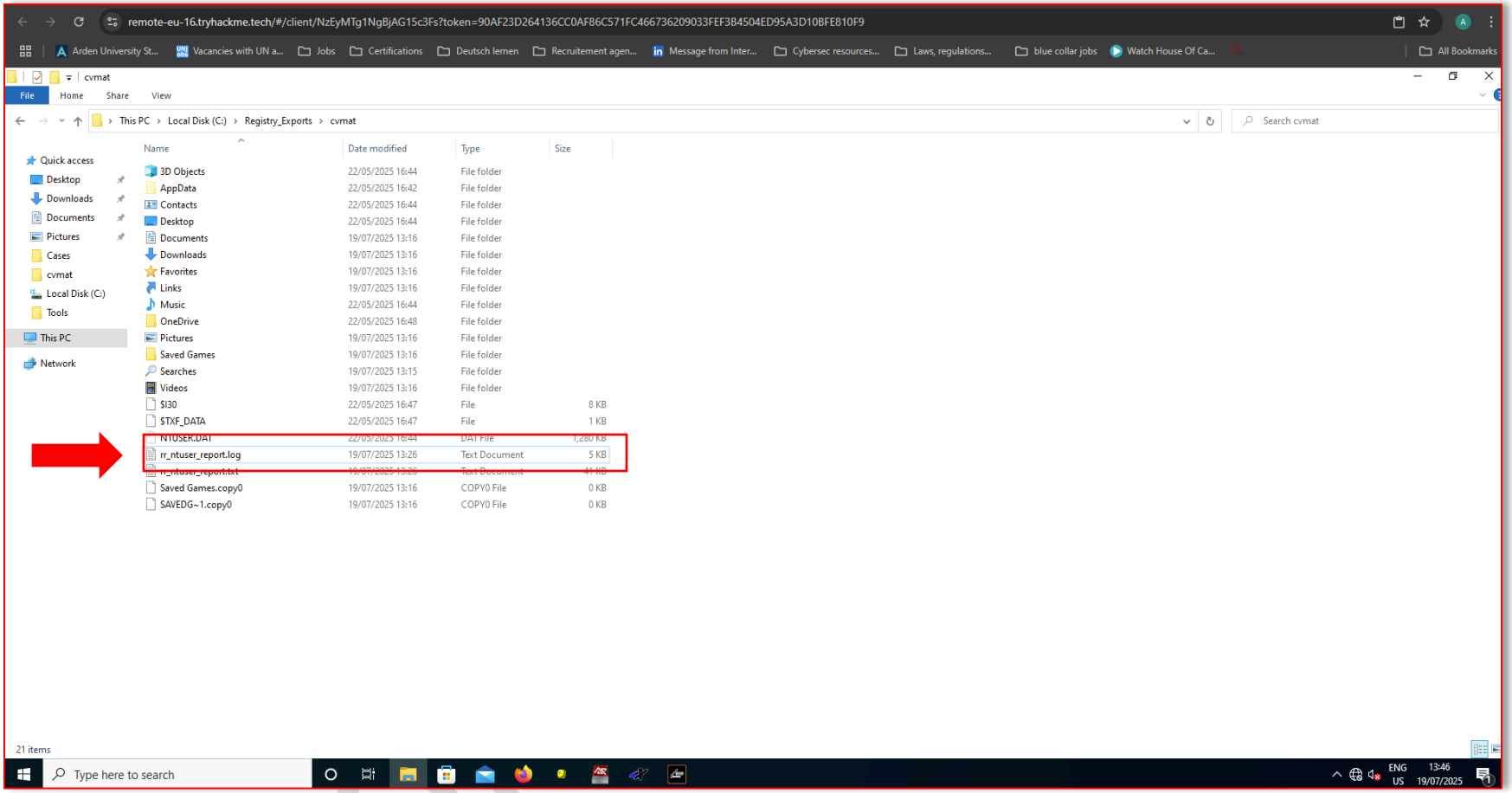
Why Registry Matters: It provides user-level activity logs even if files are deleted.



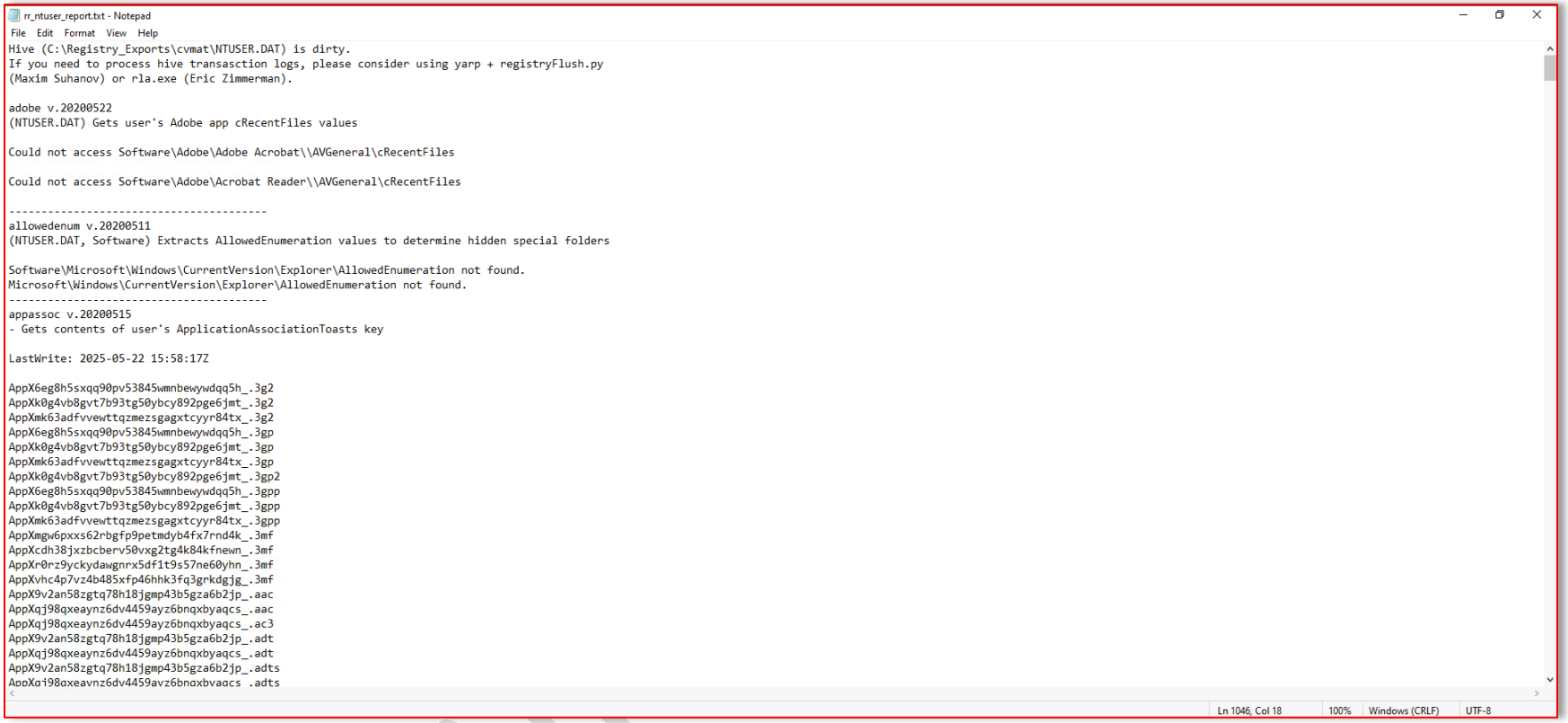

*Screenshot 8 - Extracted NTUSER.DAT from user cvmatt*




*Screenshot 9 – Loading RegRipper for extraction*




*Screenshot 10 – NTUser Report exported .txt and .log file*




*Screenshot 11 – txt file*

## *Step 4: USB Usage Verification*

- MountPoints2 and RecentDocs confirmed:
  - USB device mounted as **E:**
  - Label: ESD-USB
  - MAC: 80:6E:6F:6E:69:63
- File paths in RecentDocs showed user browsing E:\aurora

Why Important: **Shows device access** at the same time **files were compressed.**

### *Step 5: Timeline Correlation (Casey, 2011)*

Used timestamps from:

- Registry (LastWriteTime)
- File system metadata (Modified, Created)
- Program execution history

Reconstructed Timeline (22 May 2025):

| Time (Z) | Action |
|---|---|
| 15:44 | User logs in |
| 15:46 | 7zFM.exe executed |
| 15:48 | USB E: mounted |
| 15:50–16:00 | Files aurora, note.txt accessed |
| 16:02 | Archive aurora.7z appears |
| 16:05–16:35 | UserAssist logs multiple tools uses |
| 16:38 | User logout |

**Conclusion:** USB mounted **after** 7-Zip use and file access — highly indicative of exfiltration intent.

### *Step 6: Memory Analysis (Attempted)*

- Tried to run vol.py (Volatility 3) (The Volatility Foundation, 2023)
- Plugins like windows.info, pslist, cmdline failed due to missing symbol files
- TryHackMe's air-gapped setup prevented symbol download

**Impact:** Live memory artifacts (e.g., clipboard, process memory) not retrieved
**Mitigation:** Relied on registry and disk for full reconstruction

## 3. **Summary of Investigation Steps**

| Step | Tool Used | Output |
|---|---|---|
| Disk Imaging | FTK Imager | win10.raw, hashed |
| File System Review | FTK Imager | Located sensitive files |
| Registry Parsing | RegRipper | Artifacts confirming tool/file usage |
| USB Analysis | RegRipper (MountPoints2) | USB usage logs |
| Timeline Building | Manual synthesis | Matched timestamps from all layers |
| Memory Analysis | Volatility 3 (fail) | Skipped due to symbol restrictions |

# References


- **British Standards Institution, 2016.** *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (BS EN ISO/IEC 27037:2016).* London: BSI.
- **Carrier, B., 2005.** *File System Forensic Analysis.* Boston: Addison-Wesley.
- **Carvey, H., 2018.** *Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 10.* 4th ed. Burlington, MA: Syngress.
- **Casey, E., 2011.** *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* 3rd ed. Waltham, MA: Academic Press.
- **National Institute of Standards and Technology (NIST), 2006.** *Guide to integrating forensic techniques into incident response (SP 800-86).* Gaithersburg, MD: U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-86/final [Accessed 20 July 2025].
- **The Volatility Foundation, 2023.** *The Volatility Framework.* Available at: https://www.volatilityfoundation.org/ [Accessed 20 July 2025].
- **Williams, J., 2012.** *ACPO good practice guide for digital evidence.* London: Association of Chief Police Officers. Available at: https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf [Accessed 20 July 2025].