

Digital Forensics Report

Name: Ahonsi Vincent Oluwafeyikunayomi

Case: Forensic Analysis of Disk Image

Date: March 2025

Report Type: Academic Project – Controlled
Lab Environment

Introduction

A new digital forensics case was set up to analyze a forensic disk image. The case was managed with “Autopsy”, a digital forensics tool, while “Case Note” was used to record contemporaneous notes securely. The Evidence image of the computer identified as belonging to a Steve, evidence item Image1.E01_1 Host and Image1.E01_280952 Host, was the subject of a request to perform a digital forensics analysis. To maintain continuity and integrity, the image was handled according to best practices. Hash values were calculated before and after analysis to verify data integrity and a writing block method was implemented to prevent alteration of data.

The report was written by Ahonsi Vincent Oluwafeyikunayomi, a digital forensics examiner, the investigation revealed evidence suggesting the intent of the user, Steve, to engage in drug trafficking, possession and sale.

Case management

- **Tools Utilized during investigation**

The forensics investigation was conducted using industry standard tools to guarantee accuracy, dependability and adherence to best procedures. The main tool for disc image analysis was Autopsy, an open-source digital forensics platform. It made facilitate the recovery of deleted files, keyword searches, timeline reconstruction, and the extraction of critical artifacts such as browser history and cached data. Additionally, steganography analysis tools were employed to examine images for hidden data that could indicate covert communication or concealed evidence. Given the potential use of stenography in illicit activities, these tools were crucial in detecting anomalies within digital media files.

Throughout the investigation, contemporaneous note-taking software were used to ensure transparency and keep appropriate documentation. These digital tools recorded observations, timestamps and methodologies in secure and verifiable means, supporting a clear chain of custody. Proper documentation is essential in forensic investigation to ensure that all findings are admissible in legal proceedings and can withstand scrutiny. By leveraging these tools in conjunction with established methodologies, the investigation was conducted efficiently and in compliance with industry best practices.

- **Continuity and integrity**

Maintaining continuity and integrity of evidence was a fundamental aspect of the forensics process. Every step, from acquisition to analysis and reporting, was meticulously documented to ensure that the evidence remained untampered. To achieve this, hash values were generated at the time of evidence acquisition and subsequently re-verified after analysis to confirm that no modification had occurred. The use of cryptographic hash functions such as MD5 and SHA-256 allowed for the verification of data integrity, ensuring that all files and disk images remained unchanged throughout the investigation



Hash Verification

- **Chain of custody**

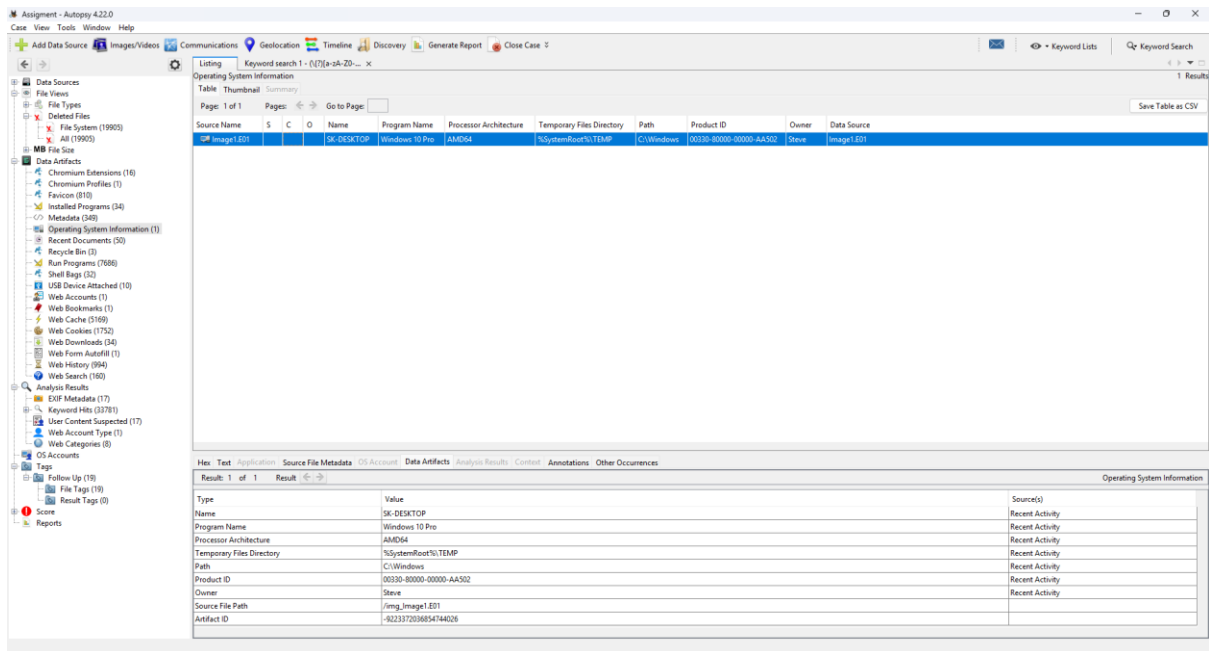
To monitor how digital evidence was handled and moved, an uninterrupted chain of custody was upheld. All forensics copies were stored in as secure environment, and every access or modification was logged. To ensure that all analyses were performed on forensics duplicates rather than the original evidence, write-blocking techniques were used to avoid any unmeant or deliberate data tampering.

Evidence analysis

The evidence item Image1.E01_1 Host and Image1.E01_280952 Host, was examined on 21/03/25 to 23/03/25. Analysis of the forensic disk image revealed the presence of eight partitions, structured with a combination of NTFS and FAT32 file systems. The primary partition, which contained the Windows operating system, was formatted in NTFS, Whereas supplementary partitions retained user data, system recovery files and possible unallocated space that can harbor leftover artifacts.

1. Operating system

The installed operating system was identified as “Windows 10 Pro” with 2/10/2024 recorded as the acquisition date. System metadata indicates that the installation has remained unaltered since that date.

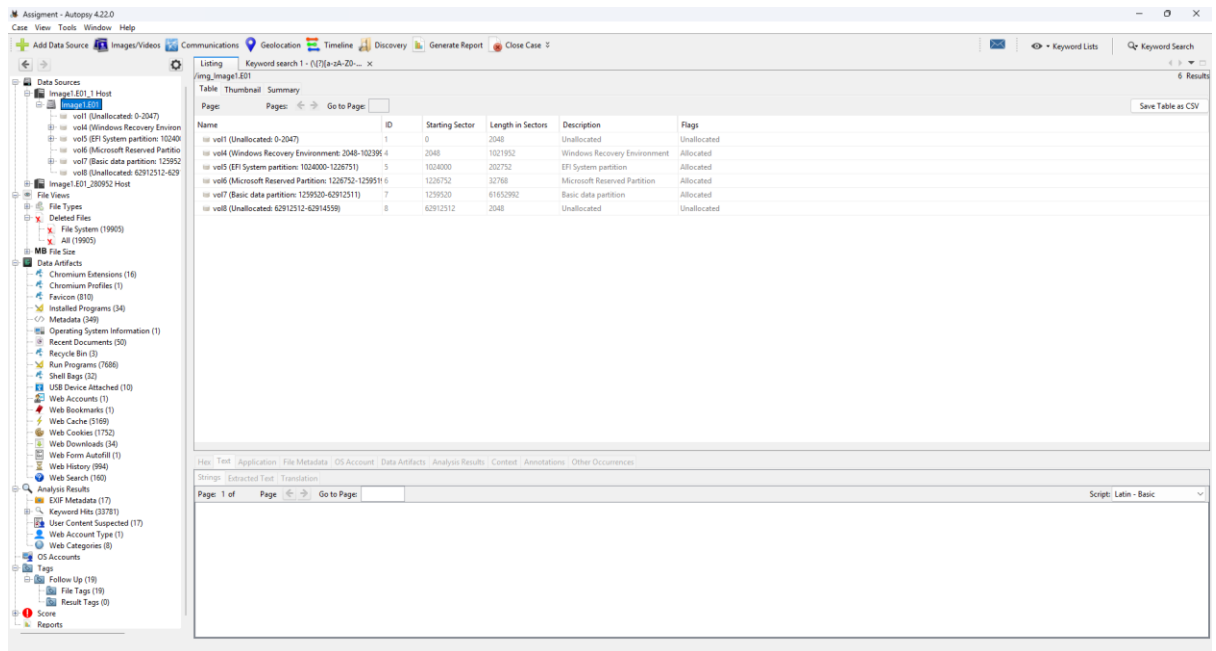


Operating System

2. Disk partition

The forensic analysis of the disk structure revealed that the storage device contained eight partitions, each serving distinct functions within the system. The partitions were identified and analyzed to determine their contents, file system, and potential relevance to the investigation. The eight partitions are as follows:

- Partition 1: Vol 1(Unallocated Spaces: 0-2047)
- Partition 2: Vol 4(Windows Recovery Environment: 2048-1023999)
- Partition 3: Vol 5(EFI System Partition: 1024000-1226751)
- Partition 4: Vol 6(Microsoft Reserved Partition: 1226752-1259519)
- Partition 5: Vol 7(Basic data partition: 1259520-62912511)
- Partition 6: Vol 8(Unallocated: 62912512-62914559)



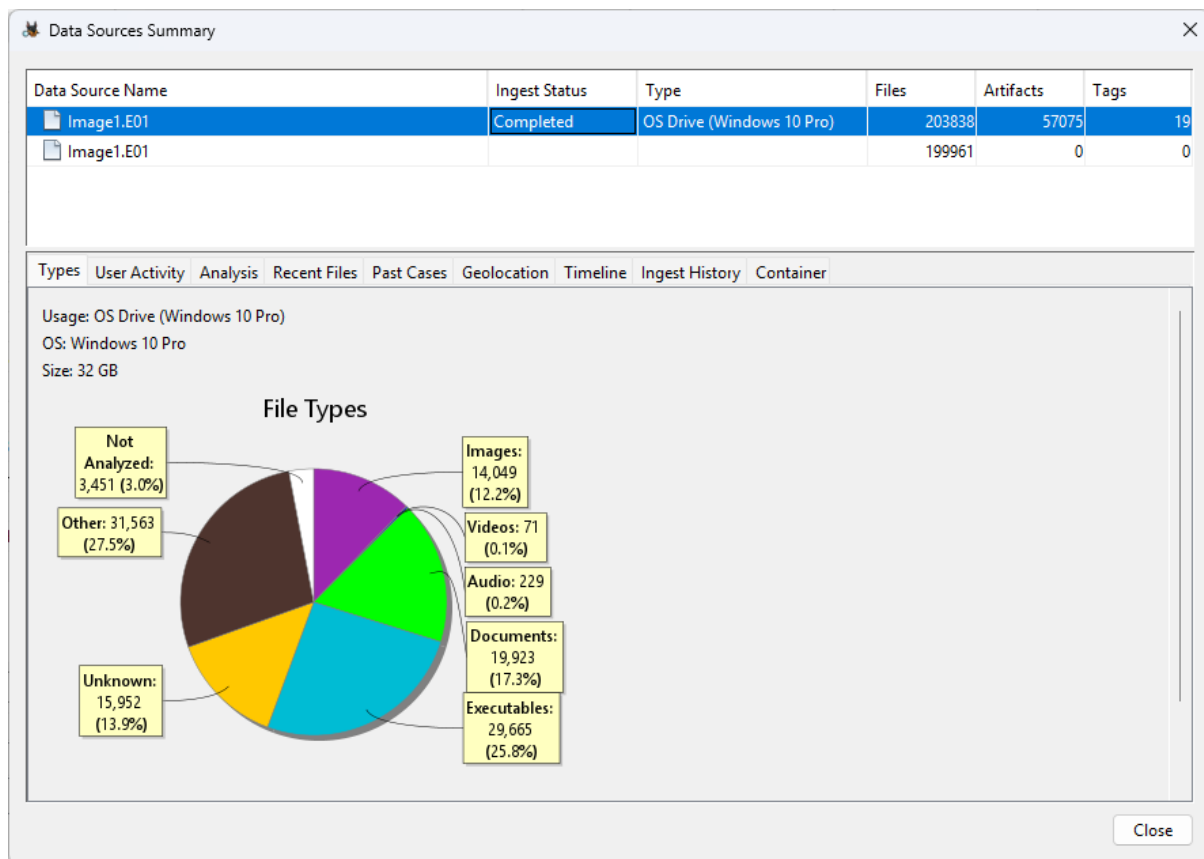
Disk Partition

3. Disk Structure

The disk size was that of 32GB, an analysis on the disk structure was done to retrieve its content and distribution of data on the disk. The disk was separated into the following Sections stored in different areas and data types.

Disk Structure:

- Documents: 19,923(17.3%)
- Executables: 29,665(25.8%)
- Images: 14,049(12.2%)
- Videos: 71(0.1%)
- Audio: 229(0.2%)
- Not Analyzed: 3,451(3.0%)
- Other: 31,563(27.5%)
- Unknown: 15,952(13.9%)



4. Time Zone

Systems time zone settings were also configured to Etc/GMT (UTC +0:00). This setting is inconsistent with the users recorded location-based activity in Australia, suggesting the possibility of manual modification or default configuration at the time of installation.

5. Installed Programs

Analysis of installed programs on the system revealed a range of utility, security and virtualization. Notable installations include:

- TrueCrypt: A disk encryption tool capable of creating encrypted volumes, which may indicate an attempt to secure or conceal sensitive data.
- Image stenography: Software designed for embedding hidden messages or files within images, suggesting possible data obfuscation techniques.
- CCleaner: A system cleaning utility that can remove traces of user activity, potentially affecting forensics recovery efforts.

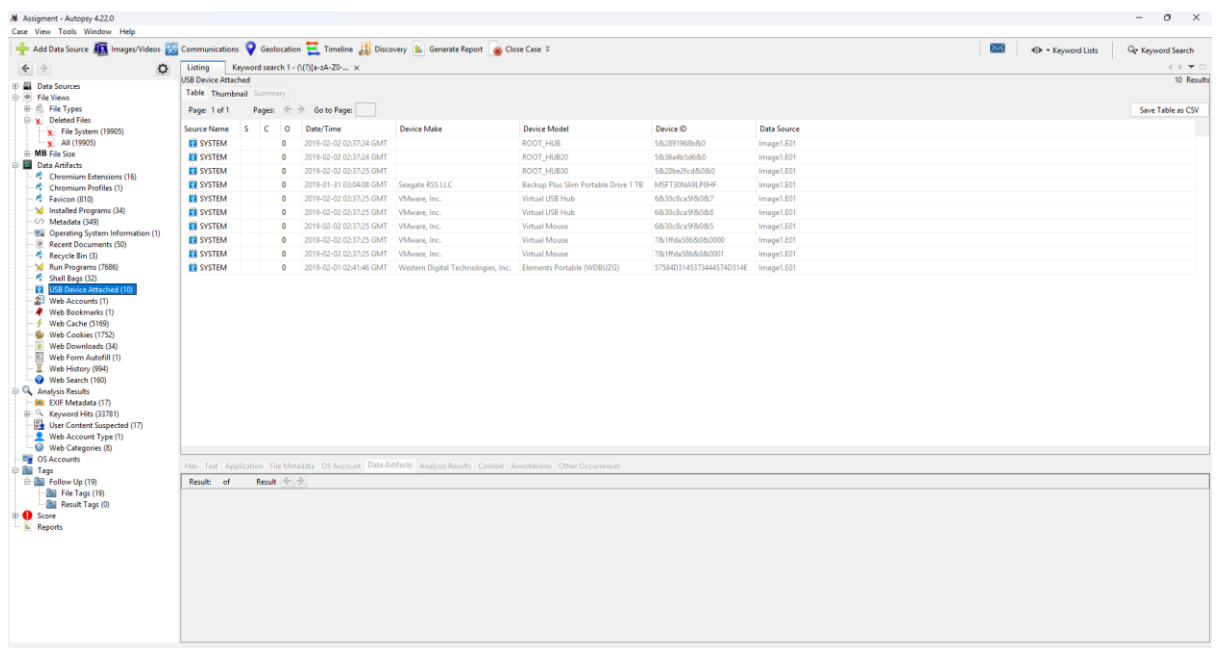
- **VMware Tools:** Indicates the presence of a virtualized environment, which may have been used to isolate activities.

Installation records indicate that the aforementioned programs were last added or modified between September 2018 and February 2019, during a period of active system use. The Presence of encryption and stenography tools is significant, as these applications are commonly associated with data concealment, protection, or unauthorized information exchange. Further examination is required to determine encrypted volumes, or hidden data exists with forensics image.

6. Hardware Devices

Hardware Devices and connected Volumes. System logs reveal the connection of multiple external devices, including USB storage drives and virtual USB hubs. Key finding include:

- **Seagate Backup Plus Slim Portable Drive (1TB, Devices ID: MSFT30NA9LP8HF):** Connected on 31/01/19, potentially used for external data storage or transfer.
- **VMware Virtual USB Hub:** Identified in the logs, further supporting the presence of a virtualized environment.
- **Multiple USB Root Hubs(USB 2.0,3.0):** Logged connections on 02/02/19, indicating active USB device usage.



Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM	0			2019-02-02 02:37:24 GMT	ROOT_HUB	ROOT_HUB	58289198b860	Image1.E01
SYSTEM	0			2019-02-02 02:37:24 GMT	ROOT_HUB20	ROOT_HUB20	5836a4b5a8560	Image1.E01
SYSTEM	0			2019-02-02 02:37:25 GMT	ROOT_HUB30	ROOT_HUB30	5820b2c7c88080	Image1.E01
SYSTEM	0			2019-01-31 03:04:08 GMT	Seagate R35 LLC	Backup Plus Slim Portable Drive 1 TB	MSFT30NA9LP8HF	Image1.E01
SYSTEM	0			2019-02-02 02:37:25 GMT	VMware, Inc.	Virtual USB Hub	6830c3c5f80807	Image1.E01
SYSTEM	0			2019-02-02 02:37:25 GMT	VMware, Inc.	Virtual USB Hub	6830c3c5f80808	Image1.E01
SYSTEM	0			2019-02-02 02:37:25 GMT	VMware, Inc.	Virtual Mouse	6830c3c5f80805	Image1.E01
SYSTEM	0			2019-02-02 02:37:25 GMT	VMware, Inc.	Virtual Mouse	7818da5868080000	Image1.E01
SYSTEM	0			2019-02-02 02:37:25 GMT	VMware, Inc.	Virtual Mouse	7818da5868080001	Image1.E01
SYSTEM	0			2019-02-01 02:41:48 GMT	Western Digital Technologies, Inc.	Elements Portable (WD800JG)	57584031453734445740314E	Image1.E01

Hardware Devices

The Presence of external storage devices, most especially the “Seagate Backup Plus drive”, raises the possibility of additional forensic evidence existing outside the examined disk image. Further investigation may be required to determine the nature of the data transferred through these devices.

7. User Profile

The Primary user account on the system is registered under the name “Steve”. An analysis of the user’s internet activity revealed a mix of general browsing as well as sports related queries but what caused the most concern were the drug related searches.

The drug related searches contain queries related to drug use and trade more targeted searches include searches for:

- Drug usage and effects.
- Tampering and “cutting of crystals”.
- International drug trade and distribution.

Further Investigation into browser cache and saved shortcuts confirmed searches for “best places to trade drugs”, “international drug routes” and locations such as Eastbourne and Wellington libraries. This aligns with previously retrieved images containing mapped routes, travel documents and cryptic messages, suggesting possible connection between the users research and planned activities.

The Presence of deleted images showing substances consistent in appearance with controlled substances, money and Clothing items featuring symbols and insignia commonly associated with known groups, as well as discussion regarding amyl nitrate and its legal status in Australia, further supports indications that the user may have been researching or preparing for drug-related activities across multiple locations.

Additional analysis of communication records and encrypted storage is necessary to determine the full extent of the user’s involvement.

Findings and conclusions

- The user Steve was identified as the primary user of the forensic image. Internet activity logs show a mixture of general browsing, including sports-related searches, alongside searches related to drug use, tampering and trade. The findings indicate potential involvement in cross-border drug trafficking.
- The forensic image contained eight partitions with a windows 10 pro operating system, acquired on 10/02/24. The systems time zone was set to Etc/GMT, ensuring consistency in time-based evidence correlation.

- A search of the Recycle Bin revealed multiple deleted images showing bundles of currency, packaged substances resembling drugs and clothing associated with organized groups. Metadata analysis determined these files were deleted on 02/02 /19 at 02:48 GMT.
- Analysis of images recovered from the system showed flight tickets and maps with routes drawn on them. A ticket indicated a planned journey from Brisbane (BNE) Airport to Wellington international Airport(WLG) on February 16, 2019, at 08:45 AM, with a return on February 23, 2019, at 5:40pm. Additional images extracted marked locations in Eastbourne, New Zealand, as well as movements tracked from Eastbourne to Wainuiomata, Stokes Valley, and Naenae. One image labelled “Dropoff.jpg”, pinpointed Eastbourne Library as a landmark worthy of attention.
- A keyword search for “drugs” retrieved 85 results, including a file named “data_3”, containing cached Google Chrome search history. The keyword appeared in a search result for “five men charged in Australia with large scale drug supply”.
- Further analysis of “data_3” uncovered a conversation involving IP address 151.101.233.132 regarding amyl nitrate, its effects, its ban in Australia, and support for its use.
- Additional Keyword searches revealed that the user had searched for “international drug routes”, indicating possible research into trafficking pathways.
- A file named “shortcuts” contained Google search shortcuts, including “best places to trade drugs” and searches for Eastbourne, Wellington library and wellington city. These searches may be connected to previously examined images showing mapped routes and locations.
- Installed software included Truecrypt and image stenography, tools commonly used for data encryption and concealing information within images, raising concerns about the users intent to hide or protect sensitive data.
- Connected hardware logs showed multiple USB devices attached to the system, suggesting potential external data transfers that may need further examination.

Based on the forensics findings, the evidence strongly suggests that the user Steve conducted research on drug trade routes, engaged in discussions related to banned substances and exhibited behavior consistent with illicit activities. Further analysis of network logs, USB transfers and hidden files may provide additional context to confirm or refute Steves involvement in drug trafficking and sales.

References

- EclipseForensics (2024). *The Digital Forensic Expert's Playbook: Best Practices and Strategies* - Eclipse Forensics. [online] Eclipse Forensics. Available at: <https://eclipseforensics.com/the-digital-forensic-experts-playbook-best-practices-and-strategies/>.

- Ch, R. and el (2020). *Comprehensive Guide on Autopsy Tool (Windows)*. [online] Hacking Articles. Available at: <https://www.hackingarticles.in/comprehensive-guide-on-autopsy-tool-windows/>.
- Cadosecurity.com. (2024). *How to Handle Digital Evidence: Best Practices*. [online] Available at: <https://www.cadosecurity.com/wiki/how-to-handle-digital-evidence-best-practices>.

Contemporaneous Notes

