CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC)
THIRUVANANTHAPURAM, KERALA

A MINOR PROJECT REPORT ON

"Integrating CSI Linux for Real-Time Forensics on Windows 11 Virtual Machines"

SUBMITTED TOWARDS THE

PG-DCSF August 2025

BY

Group Number - 04

Harshit Shrivastav	PRN:250260940012
Harsh Patidar	PRN: 250260940011
Nimisha Goyal	PRN: 250260940019
Anurag Dadhich	PRN: 250260940005
A V Yashwanth	PRN: 250260940037

Under The Guidance Of

Mr. Jayaram	Mr. Hiron Bose
Co-Ordinator	Project Guide

Table of contents

Table of Contents

ABSTRACT

This project presents a comprehensive approach to live forensic analysis in a virtualized environment, focusing on a Windows 11 virtual machine (VM) as the target system and employing CSI Linux as the investigative platform. The live forensics process began with the use of the **dumplt** utility within the Windows 11 VM to capture a raw memory image (.raw file). This memory dump was subsequently analysed in CSI Linux using the **Volatility3** framework, leveraging multiple plugins to extract, examine, and interpret forensic artifacts such as running processes, loaded modules, network connections, and user activity.

In addition to memory analysis, a forensic disk image of the Windows 11 VM was acquired using **FTK Imager**, resulting in an EnCase image format (.E01 file). This disk image was then subjected to deeper forensic analysis within CSI Linux using Autopsy, enabling file system exploration, recovery of deleted files, timeline analysis, and artifact extraction crucial for understanding system state and user actions.

By integrating memory and disk forensic techniques and applying industry-standard tools across both Windows and Linux platforms, this project demonstrates effective methodologies for live incident response and evidence preservation in virtualized Windows environments. The workflow documented here bridges the gap between volatile memory acquisition and persistent storage examination, offering a robust toolkit and repeatable process for forensic investigators confronting modern digital crime scenes involving virtualized infrastructures.

INTRODUCTION

With the rapid proliferation of virtualized environments and increased reliance on digital systems, the need for effective digital forensic techniques has never been greater. Modern organizations run critical applications and services within virtual machines (VMs), making them prime targets for cyberattacks and security incidents. Investigating breaches or suspicious activities in such environments requires adaptation and the integration of specialized forensic tools and methodologies.

This project focuses on the real-time forensic acquisition and analysis of a Windows 11 virtual machine (VM), utilizing CSI Linux as the investigative platform. Live forensics—collecting and analysing data from a system while it is running—provides invaluable insights into volatile information such as running processes, network connections, and other in-memory artifacts that are lost when a system is powered down. The process offers a crucial advantage in incident response by capturing system state at the time of investigation.

The investigation was structured into two main stages: memory forensics and disk forensics. Using the **dumplt** utility, a raw memory dump of the Windows 11 VM was acquired, then imported into CSI Linux. Volatility3, a state-of-the-art memory analysis framework, was employed to scan the image with various plugins, extracting information on process execution, open network ports, loaded drivers, and user activity.

For persistent data examination, a forensic disk image (.E01 format) was created from the Windows 11 VM using **FTK Imager**. This image was subsequently analysed with **Autopsy** on CSI Linux, allowing for recovery and examination of files, timelines, user artifacts, and hidden or deleted evidence.

By integrating memory and disk forensic techniques, and employing industry-standard tools across both Windows and Linux environments, this project demonstrates a practical, end-to-end approach for live forensic investigation in contemporary virtualized settings.

SCOPE AND OBJECTIVE

1.1 Scope

The scope of this project encompasses the practical application of digital forensic methodologies to a virtualized Windows 11 environment, using CSI Linux as the primary investigative platform. The work covers both live (volatile memory) and post-mortem (disk image) forensic acquisition and analysis, demonstrating a multi-layered approach that is relevant in contemporary cyber incident response scenarios. The project methodology includes:

- Acquiring volatile memory from a live Windows 11 VM using the dumplt tool and analysing it under CSI Linux.
- Leveraging Volatility3 plugins within CSI Linux to extract in-depth forensic information from the memory dump.
- Creating a forensic disk image (.E01 format) of the Windows 11 VM using FTK Imager on the target system.
- Performing comprehensive post-mortem analysis of the disk image with Autopsy on CSI Linux.
- Documenting findings and presenting a workflow that can be replicated for similar forensic investigations in virtualized infrastructures.

1.2 Objectives

The main objectives of this project are as follows:

1. To demonstrate and document the process of live memory acquisition from a running Windows 11 virtual machine.
2. To utilize the Volatility3 framework to extract and interpret critical forensic artifacts from the captured memory image, such as running processes, network connections, user sessions, and loaded modules.
3. To perform forensic acquisition of the virtual machine's disk in E01 format, preserving its integrity using industry-standard tools.
4. To analyse the acquired disk image with Autopsy, identifying and recovering file system artifacts, deleted data, and timeline information related to user and system activity.
5. To showcase the effectiveness of open-source and commercial forensic tools when used in conjunction for comprehensive digital investigations.
6. To develop a structured, repeatable workflow for live and post-mortem forensic analysis within virtual machine environments.

7. To highlight the importance of volatile and persistent data analysis in forming a complete investigative perspective during live incident response.

Through the achievement of these objectives, the project aims to equip digital forensic practitioners and students with practical techniques and an integrated workflow for investigating contemporary Windows systems deployed as virtual machines.

1.3 Methodology

This project adopted a systematic, multi-phase methodology to conduct live forensics on a Windows 11 virtual machine (VM) using CSI Linux as the investigative platform. The process was designed to capture both volatile (memory) and non-volatile (disk) data, enabling comprehensive digital forensic analysis. The major phases are outlined below:

1. Environment Preparation

- **Setup of Virtual Lab**: A Windows 11 VM was configured as the target system where normal user activities were performed. CSI Linux, a specialized digital forensic distribution, was set up as the analysis environment on a separate VM.
- **Networking**: Both VMs were placed on the same virtual network to facilitate secure evidence transfer.

2. Live Memory Acquisition

- **Dumplt Tool Utilization**: The windows11vm was imaged using the dumplt memory tool, executed with administrative privileges to obtain a raw memory dump (.raw file) without altering the system state.
- **Data Integrity**: MD5/SHA1 hash values were computed and recorded immediately after acquisition to ensure the evidence remained untampered throughout the investigation.

3. Memory Analysis with Volatility3

- **Transfer of Dump**: The memory dump was securely copied from the Windows 11 VM to CSI Linux for further investigation.
- **Volatility3 Framework Application**: The raw memory image was loaded into Volatility3. A suite of plugins was systematically run, including those for process enumeration, network connections, loaded drivers, DLL listings, and user sessions.
- **Documentation**: Key findings, such as suspicious processes or anomalous network connections, were documented for evidence and reporting.

4. Forensic Disk Acquisition

- **FTK Imager Usage in Windows11VM**: FTK Imager was installed and used to capture a complete disk image of the target VM. The image was saved in EnCase E01 format for compatibility with forensic analysis tools and preservation of metadata.
- **Verification**: Integrity verification (hashing) was performed to confirm successful, error-free imaging.

5. Post-Mortem Disk Analysis in CSI Linux

- **Transfer of Disk Image**: The E01 file was sent from the Windows 11 VM to CSI Linux, ensuring hashes matched on both source and destination.
- **Autopsy Tool Examination**: Autopsy was used to load and analyze the E01 disk image. Investigative modules within Autopsy enabled examination of the file system, recovery of deleted files, timeline reconstruction, and artifact extraction (such as browser history, event logs, and user activity).

6. Evidence Management and Documentation

- **Evidence Handling**: Chain-of-custody protocols were maintained throughout acquisition, transfer, and analysis.
- **Report Generation**: All command-line actions, findings, hash values, and screenshots were compiled into a structured forensic report, ensuring transparency, repeatability, and admissibility in legal contexts.

7. Workflow Integration

- **Correlating Memory and Disk Findings**: Results from Volatility3 and Autopsy were cross-referenced to draw comprehensive conclusions about system usage, compromise vectors, and user actions.
- **Process Repeatability**: The methodology was designed to be repeatable for similar future investigations involving both memory and disk forensics in virtualized environments.

Through this rigorous methodology, the project demonstrates an effective workflow for live and post-mortem forensic investigation—leveraging open-source and commercial tools to ensure thorough evidence acquisition, reliable analysis, and clear documentation suitable for both academic and professional settings.

PHASES OF DIGITAL FORENSICS

1. Identification

- **Goal:** Recognize and determine the potential sources of digital evidence relevant to an investigation.
- **Key Activities:** Locating devices and storage media (computers, servers, mobile devices, external drives, cloud data) that may store information linked to the incident. All identified devices are documented and secured to prevent any change or loss of data.

2. Preservation

- **Goal:** Safeguard the integrity of digital evidence.
- **Key Activities:** Isolating, securing, and preserving data using forensic techniques. This frequently involves creating forensic images (exact digital replicas) of the original media, using write blockers and specialized tools to avoid modifying evidence. All actions are carefully documented to maintain chain of custody.

3. Collection

- **Goal:** Acquire digital evidence in a manner that maintains its integrity and allows for proper analysis.
- **Key Activities:** The actual acquisition phase, where digital information is extracted from devices—commonly via bit-for-bit imaging or live data capture for volatile memory. This phase may also include careful documentation and secure storage or transportation of evidence to a laboratory for further work.

4. Analysis

- **Goal:** Systematically examine the acquired data to uncover relevant facts, reconstruct events, and support or refute hypotheses related to the investigation.
- **Key Activities:** Using forensic analysis tools and methods (such as keyword searches, recovery of deleted data, examination of logs, reverse steganography, data carving, and timeline generation) to uncover evidence of suspicious or criminal activities. Findings are carefully correlated and interpreted.

5. Documentation and Reporting

- **Goal:** Record the investigative process and communicate findings in a manner that is clear and can stand up in legal or organizational settings.

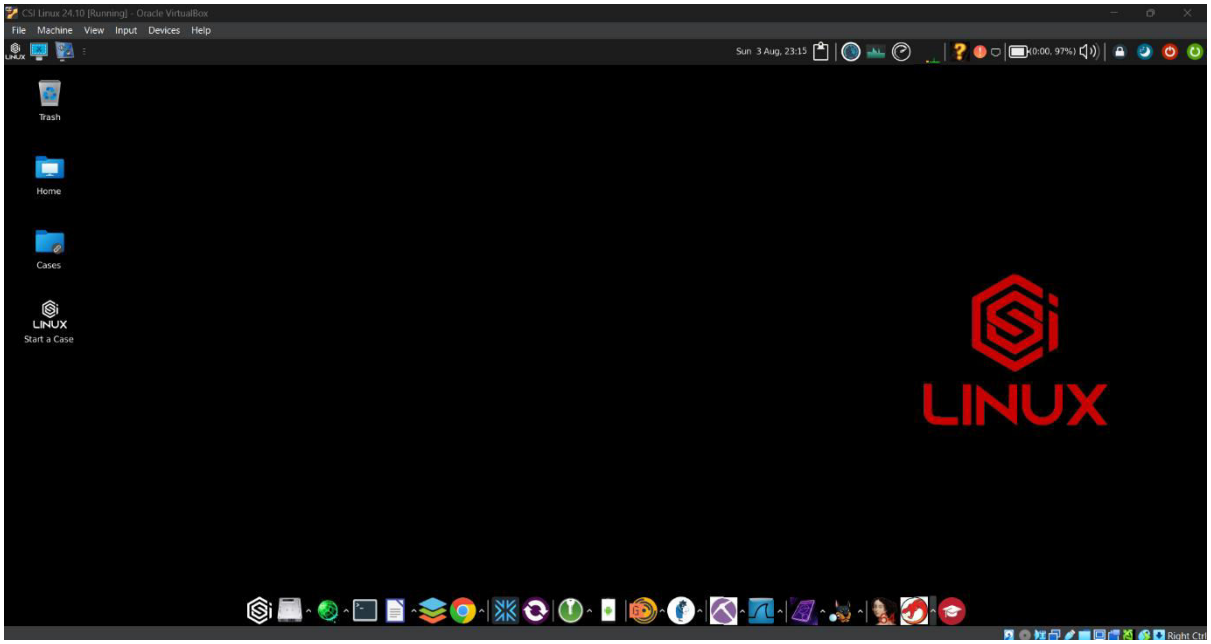
- **Key Activities:** Creating thorough documentation throughout each phase, including all tools, actions, and findings. The final report synthesizes the results, methodologies, conclusions, and recommendations for stakeholders such as management, law enforcement, or court proceedings.

6. Presentation (Sometimes Combined with Reporting)

- **Goal:** Present findings to decision-makers, courts, or other stakeholders.
- **Key Activities:** Delivering evidence and expert testimony, answering questions, and defending the findings in formal proceedings if necessary.

Phase	Main Activities
Identification	Locate devices/sources, recognize relevant evidence
Preservation	Secure and isolate evidence, prevent alteration, create forensic images
Collection	Acquire (image/copy) evidence, ensure proper handling, maintain chain of custody
Analysis	Examine and interpret evidence using forensic tools and advanced investigative methods
Documentation	Record every step, method, and result for transparency and repeatability
Presentation	Communicate findings and methods to courts, management, or relevant authorities

CSI LINUX :



LIVE FORENSICS:

Step Number	Action
1	Add the **DumpIt application** to a USB drive.
2	Plug the USB drive into the **Windows 11 VM**.
3	Open the DumpIt application on the Windows 11 VM to **create the memory dump file**.
4	Once the file is created, **eject the USB drive** from the Windows 11 VM.
5	Plug the USB drive into the **CSI Linux VM**.
6	Copy the memory dump file to the **home directory** on the CSI Linux system.
7	Open a **terminal** on CSI Linux.
8	Start the **Volatility 3 tool** from the terminal.
9	**Analyze the memory dump file** using various Volatility 3 plugins and scans.
10	The analysis is complete when the **output is generated** and reviewed.

DISK FORENSICS:

Step Number	Action	Description
1	**Run FTK Imager on Windows 11 VM**	Launch the FTK Imager software on the target virtual machine to begin the imaging process.
2	**Generate E01 File**	Use FTK Imager to create a forensic disk image (E01 file), which is an exact, bit-for-bit copy of the source drive.
3	**Copy E01 File to CSI Linux VM**	Transfer the generated E01 file from the Windows 11 environment to your CSI Linux analysis machine.
4	**Add File to Autopsy Tool**	Open Autopsy on your CSI Linux VM and create a new case, adding the E01 file as a data source.
5	**Run Scan**	Configure and run the ingest modules in Autopsy to process the data source. This includes file type identification, hash lookups, and keyword searching.
6	**Display All Files**	After the scan is complete, Autopsy will display the file system, deleted files, and other extracted artifacts for review.
7	**Analyze Files**	Manually examine the files and artifacts of interest. Tag relevant items, review timelines, and investigate user activity.
8	**Generate Report**	Use Autopsy's reporting feature to create a detailed report of your findings, including tagged items and notes.
9	**Done**	The process is complete once the report is generated and the investigation is concluded.

VOLATILITY 3

Volatility3 is an advanced open-source framework for analyzing volatile memory (RAM) images, available in CSI Linux for both Windows and Linux memory forensic investigations

Overview of Volatility3

• **Purpose:** Extract digital artifacts from memory dumps, including running processes, hidden malware, network activity, and loaded modules12.

• **Usage Context:** Useful for incident response, intrusion detection, malware analysis, and full forensic investigations within CSI Linux

Basic Workflow

1. Open Terminal in CSI Linux

Navigate to the memory image location.

2. List Available Plugins

```
bash
python3 vol.py --help
```

or for Windows plugins:

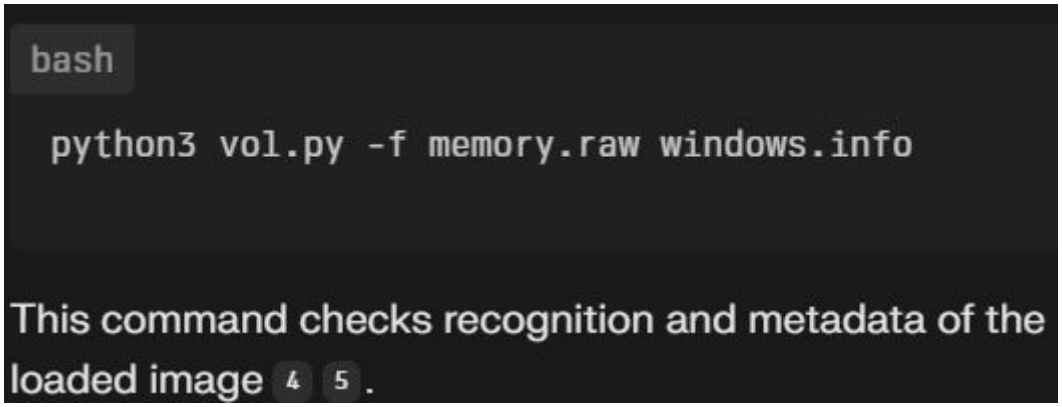
```
bash
python3 vol.py --help | grep windows
```

or for Linux plugins:

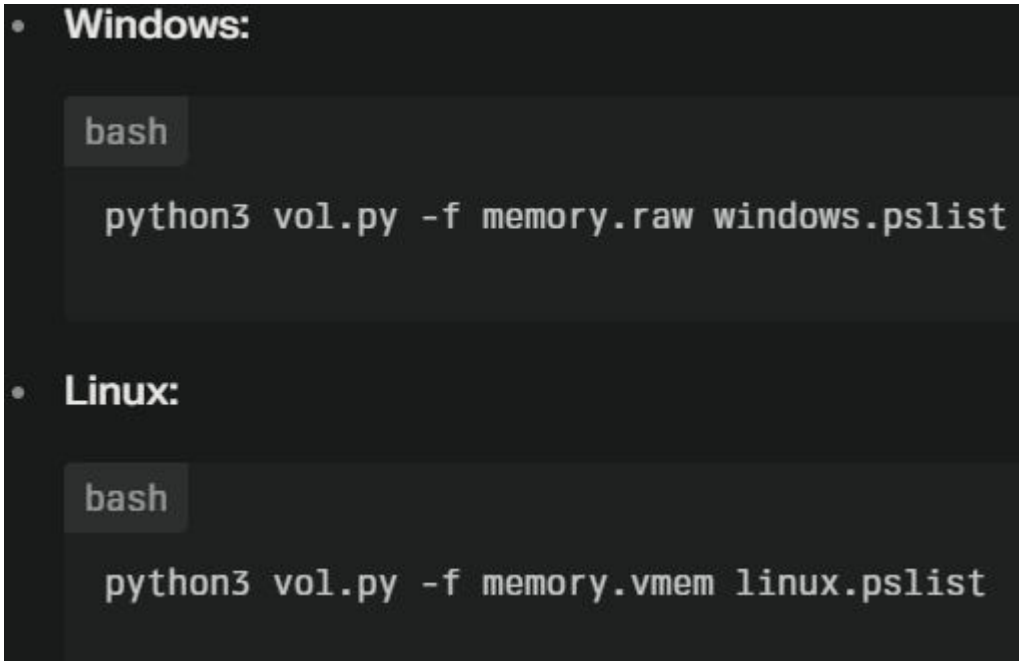
```
bash
python3 vol.py --help | grep linux
```

3. Collect Memory Info

Example for Windows memory image:

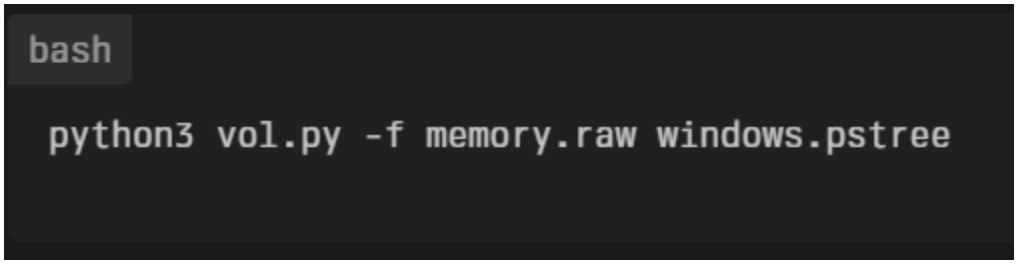


4. List Running Processes



Lists all processes captured at the time of the dump, helping to spot suspicious activity

5. Process Tree View



Visualize parent-child process relations—useful for spotting process injection or anomalous parent/child links

6. Active Network Connections

- **Linux:**

```bash
python3 vol.py -f memory.vmem linux.netconnections
```

- **Windows:**

```bash
python3 vol.py -f memory.raw windows.netscan
```

Shows established/active network connections—helpful in uncovering malware communications

7. Extract Command Histories

- **Linux:**

```bash
python3 vol.py -f memory.vmem linux.bash
```

- **Windows:**

```bash
python3 vol.py -f memory.raw windows.cmdline
```

Exposes bash or cmd.exe command history used on the target at the time of the dump

8. Dumping Process Memory

```bash
python3 vol.py -f memory.raw windows.proc_dump --dump-dir /path/to/save
```

Dumps memory content of all or a specific process for further analysis (like malware extraction or reverse engineering).

9. Listing Loaded Modules (DLLs/Drivers)

```bash
python3 vol.py -f memory.raw windows.dlllist
python3 vol.py -f memory.raw windows.driverscan
```

Lists all DLLs and drivers, revealing injected libraries or unauthorized drivers (malware indicators)

Task	Plugin / Command Example
Info about memory file	`python3 vol.py -f memory.raw windows.info`
List running processes	`python3 vol.py -f memory.raw windows.pslist`
Process tree	`python3 vol.py -f memory.raw windows.pstree`
Network connections	`python3 vol.py -f memory.raw windows.netscan`
Bash/cmd history	`python3 vol.py -f memory.raw windows.cmdline / linux.bash`
Dump process memory	`python3 vol.py -f memory.raw windows.proc_dump --dump-dir ./dumpDir`
List DLLs/Drivers	`python3 vol.py -f memory.raw windows.dll / windows.driverscan`

AUTOPSY

Autopsy is a powerful, user-friendly open-source digital forensic platform included in CSI Linux. It supports the analysis of disk images—such as those acquired in E01 or raw format with FTK Imager—and offers a comprehensive suite for post-mortem examinations of filesystems, user activity, deleted files, timelines, and artifacts.

Overview of Autopsy

- **Function:** Forensic analysis of disks, partitions, and filesystems.
- **Supported Formats:** Handles E01, raw/dd, and many other disk image types generated by FTK Imager and similar tools.
- **Modules:** Built-in modules for extracting web history, documents, installed programs, event logs, email, registry hives, user actions, and more.

Basic Workflow in CSI Linux

1. Launching Autopsy

- Open Autopsy from the CSI Linux applications menu or by running autopsy in a terminal.

2. Creating a New Case

- Click **"Create New Case"** and fill in case details (case name, base directory, examiner name).

3. Adding a Data Source

- Select **"Add Data Source"**.
- Choose **"Disk Image or VM File"**.
- Browse and select your acquired **E01** (EnCase) or **raw/dd** disk image from the forensic acquisition phase.
- Autopsy will verify and process the selected image.

4. Configuring Ingest Modules

- Autopsy automatically suggests various ingest modules—select relevant options (file analysis, hash lookup, keyword search, web artifacts, email, recent activity, etc.) depending on your analysis goals.
- Click **"Next"** and Autopsy will begin analysis.

5. Exploring Evidence

Once ingest is underway or complete, navigate through the left-side tree:

- **File System:** Browse directories, recover deleted files, flag hidden/executable/malicious files.
- **Recent Activity:** Quickly see user activity (USB insertions, document access, executed programs).
- **Web Artifacts:** Analyze browser history, downloads, cookies, and cached files.
- **Communications:** Extract emails, chat logs, and IM data if present.
- **Event Logs:** Inspect Windows log files for login activity, errors, and system changes.
- **Keyword Search:** Use built-in or custom wordlists to sweep for suspicious content.

6. Reporting and Documentation

- Use Autopsy's integrated **Report** feature to export findings in HTML, Excel, or custom report formats.
- Document paths to evidence items, hash values, and timelines for legal or organizational processes.

Common Tasks and Examples

Task	Where to find/What to do
Browse files and folders	Evidence tree > File System
Recover deleted files	Evidence tree > File System > "Deleted Files"
View web browsing history	Evidence tree > Web Artifacts > Browsers (e.g., Chrome, Edge, Firefox)
Analyze timelines of activity	Evidence tree > Timeline
Search for keywords	Keyword Search tab
Examine registry, artifacts	Evidence tree > Extracted Content > Registry, Activity
Prepare and export report	Tools/Actions > Generate Report

RESULTS

VOLATILITY 3

Process & Thread Analysis:

Lists active processes by walking the EPROCESS list.

```
12:15:19 csi@csi ~/volatility3
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.pslist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xd207df0fd040  148     -       N/A     False   2025-05-02 02:49:58.000000 UTC  N/A     Disabled
84      4       Registry        0xd207df1eb080  4       -       N/A     False   2025-05-02 02:49:52.000000 UTC  N/A     Disabled
396     4       smss.exe        0xd207e25e3080  2       -       N/A     False   2025-05-02 02:49:58.000000 UTC  N/A     Disabled
556     544     csrss.exe       0xd207e3713140  10      -       0       False   2025-05-02 02:50:02.000000 UTC  N/A     Disabled
628     544     wininit.exe     0xd207e3bbc080  3       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
644     620     csrss.exe       0xd207e3bc6140  17      -       1       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
696     620     winlogon.exe    0xd207e3c020c0  5       -       1       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
760     628     services.exe    0xd207e3c24100  6       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
784     628     lsass.exe       0xd207e3c380c0  10      -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
888     760     svchost.exe     0xd207e3c7b080  14      -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
916     628     fontdrvhost.ex  0xd207e3cb01c0  6       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
924     696     fontdrvhost.ex  0xd207e3cb21c0  6       -       1       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
1020    760     svchost.exe     0xd207e3e520c0  11      -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
516     760     svchost.exe     0xd207e3e800c0  5       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
```

Lists active threads and their information

```
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.threads
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  PID     TID     StartAddress    StartPath       Win32StartAddress       Win32StartPath  CreateTime      ExitTime

0xd207df106200  4       12      0xf800749ab660  -       0xf800749ab660  -       N/A     1600-11-03 12:00:27.000000 UTC
0xd207df0aa040  4       16      0xf800749257a0  -       0xf800749257a0  -       N/A     1600-11-03 12:00:27.000000 UTC
0xd207df11b080  4       20      0xf800749257a0  -       0xf800749257a0  -       N/A     1600-11-03 12:00:27.000000 UTC
0xd207df0c5080  4       24      0xf800749acf50  -       0xf800749acf50  -       N/A     1600-11-03 12:00:27.000000 UTC
0xd207df194080  4       28      0xf800749acf50  -       0xf800749acf50  -       N/A     1600-11-03 12:00:27.000000 UTC
0xd207df0a2080  4       40      0xf80074e38c50  -       0xf80074e38c50  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df109480  4       48      0xf80074987a20  -       0xf80074987a20  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df074080  4       52      0xf80074995a00  -       0xf80074995a00  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df091200  4       56      0xf80074995a00  -       0xf80074995a00  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df1b6080  4       60      0xf8007498cde0  -       0xf8007498cde0  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df102080  4       64      0xf8007498dcd0  -       0xf8007498dcd0  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df171080  4       68      0xf8007498efc0  -       0xf8007498efc0  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df1c7080  4       72      0xf800749aa1b0  -       0xf800749aa1b0  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df12c080  4       76      0xf80074e304d0  -       0xf80074e304d0  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df1da080  4       80      0xf8007498bb80  -       0xf8007498bb80  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df10b080  4       96      0xf800749adf80  -       0xf800749adf80  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df10d080  4       100     0xf800749adf80  -       0xf800749adf80  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df146080  4       108     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df153080  4       120     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df157080  4       124     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df159080  4       128     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df15d080  4       132     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df162080  4       136     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df166080  4       140     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df168080  4       144     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df16c080  4       148     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df16e080  4       152     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df175080  4       156     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df177080  4       160     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df17d080  4       168     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df187080  4       172     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df189080  4       176     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
0xd207df18d080  4       180     0xf80074d23e60  -       0xf80074d23e60  -       2025-05-02 02:49:52.000000 UTC  1600-11-03 12:00:27.000000 UTC
```

Scans memory for hidden or terminated processes.

```
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.psscan
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

1500    760     svchost.exe     0xd207df133080  8       -       0       False   2025-05-02 02:50:04.000000 UTC  N/A     Disabled
1584    760     svchost.exe     0xd207df15a080  11      -       0       False   2025-05-02 02:50:04.000000 UTC  N/A     Disabled
1432    760     svchost.exe     0xd207df17c080  1       -       0       False   2025-05-02 02:50:04.000000 UTC  N/A     Disabled
84      4       Registry        0xd207df1eb080  4       -       N/A     False   2025-05-02 02:49:52.000000 UTC  N/A     Disabled
1728    760     MpDefenderCore  0xd207e13d2080  5       -       0       False   2025-05-02 03:02:23.000000 UTC  N/A     Disabled
9056    760     svchost.exe     0xd207e16c20c0  8       -       0       False   2025-05-02 02:52:09.000000 UTC  N/A     Disabled
396     4       smss.exe        0xd207e25e3080  2       -       N/A     False   2025-05-02 02:49:58.000000 UTC  N/A     Disabled
8280    760     svchost.exe     0xd207e2fd70c0  1       -       0       False   2025-05-02 02:51:44.000000 UTC  N/A     Disabled
556     544     csrss.exe       0xd207e3713140  10      -       0       False   2025-05-02 02:50:02.000000 UTC  N/A     Disabled
628     544     wininit.exe     0xd207e3bbc080  3       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
644     620     csrss.exe       0xd207e3bc6140  17      -       1       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
696     620     winlogon.exe    0xd207e3c020c0  5       -       1       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
760     628     services.exe    0xd207e3c24100  6       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
784     628     lsass.exe       0xd207e3c380c0  10      -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
888     760     svchost.exe     0xd207e3c7b080  14      -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
916     628     fontdrvhost.ex  0xd207e3cb01c0  6       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
924     696     fontdrvhost.ex  0xd207e3cb21c0  6       -       1       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
1080    696     dwm.exe 0xd207e3d14080  17      -       1       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
1072    696     LogonUI.exe     0xd207e3d15100  0       -       1       False   2025-05-02 02:50:03.000000 UTC  2025-05-02 02:50:37.000000 UTC  Disabled
1100    760     svchost.exe     0xd207e3d1c080  1       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
1224    760     svchost.exe     0xd207e3dbe080  2       -       0       False   2025-05-02 02:50:04.000000 UTC  N/A     Disabled
1244    760     svchost.exe     0xd207e3dc50c0  10      -       0       False   2025-05-02 02:50:04.000000 UTC  N/A     Disabled
1272    760     svchost.exe     0xd207e3dd1080  3       -       0       False   2025-05-02 02:50:04.000000 UTC  N/A     Disabled
7844    7488    msedgewebview2  0xd207e3dfd080  15      -       1       False   2025-05-02 02:55:34.000000 UTC  N/A     Disabled
1020    760     svchost.exe     0xd207e3e520c0  11      -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
516     760     svchost.exe     0xd207e3e800c0  5       -       0       False   2025-05-02 02:50:03.000000 UTC  N/A     Disabled
```

DLLs & Modules:

Lists loaded DLLs for each process

```
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.dlllist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

396     smss.exe        0x7ff7d8f00000  0x30000 smss.exe        \SystemRoot\System32\smss.exe   2025-05-02 02:49:59.000000 UTC  Disabled
396     smss.exe        0x7ffa735f0000  0x217000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2025-05-02 02:49:59.000000 UTC  Disabled
556     csrss.exe       0x7ff67f1e0000  0x7000  csrss.exe       C:\Windows\system32\csrss.exe   2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa735f0000  0x217000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa706c0000  0x19000 CSRSRV.dll      C:\Windows\SYSTEM32\CSRSRV.dll  2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa706a0000  0x16000 basesrv.DLL     C:\Windows\system32\basesrv.DLL 2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70680000  0x15000 winsrv.DLL      C:\Windows\system32\winsrv.DLL  2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70ea0000  0x3d3000        kernelbase.dll  C:\Windows\SYSTEM32\kernelbase.dll      2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa71280000  0xc4000 kernel32.dll    C:\Windows\SYSTEM32\kernel32.dll        2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70650000  0x25000 winsrvext.dll   C:\Windows\SYSTEM32\winsrvext.dll       2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70ad0000  0x26000 win32u.dll      C:\Windows\system32\win32u.dll  2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa73100000  0x29000 GDI32.dll       C:\Windows\system32\GDI32.dll   2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70c70000  0x122000        gdi32full.dll   C:\Windows\SYSTEM32\gdi32full.dll       2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70850000  0x111000        ucrtbase.dll    C:\Windows\SYSTEM32\ucrtbase.dll        2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70970000  0x9a000 msvcp_win.dll   C:\Windows\system32\msvcp_win.dll       2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa72530000  0x1b1000        USER32.dll      C:\Windows\system32\USER32.dll  2025-05-02 02:50:02.000000 UTC  Disabled
556     csrss.exe       0x7ffa70640000  0xe000  sxssrv.DLL      C:\Windows\system32\sxssrv.DLL  2025-05-02 02:50:03.000000 UTC  Disabled
556     csrss.exe       0x7ffa704d0000  0xa3000 sxs.dll C:\Windows\system32\sxs.dll      2025-05-02 02:50:03.000000 UTC  Disabled
556     csrss.exe       0x7ffa72be0000  0xb1000 ADVAPI32.dll    C:\Windows\system32\ADVAPI32.dll        2025-05-02 02:50:03.000000 UTC  Disabled
556     csrss.exe       0x7ffa73050000  0xa7000 msvcrt.dll      C:\Windows\system32\msvcrt.dll  2025-05-02 02:50:03.000000 UTC  Disabled
556     csrss.exe       0x7ffa723c0000  0xa7000 sechost.dll     C:\Windows\SYSTEM32\sechost.dll 2025-05-02 02:50:03.000000 UTC  Disabled
556     csrss.exe       0x7ffa72d80000  0x114000        RPCRT4.dll      C:\Windows\system32\RPCRT4.dll  2025-05-02 02:50:03.000000 UTC  Disabled
556     csrss.exe       0x7ffa70820000  0x28000 bcrypt.dll      C:\Windows\SYSTEM32\bcrypt.dll  2025-05-02 02:50:03.000000 UTC  Disabled
```

Identifies unlinked modules (indicative of stealthy malware)

```
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.ldrmodules
Volatility 3 Framework 2.26.2
/home/csi/volatility3/volatility3/framework/deprecation.py:28: FutureWarning: This API (volatility3.plugins.win
plugin has been renamed, please call volatility3.plugins.windows.malware.ldrmodules.LdrModules rather than vola
  warnings.warn(

Pid     Process Base    InLoad  InInit  InMem   MappedPath

4       System  0x2190000       False   False   False   \Windows\SysWOW64\ntdll.dll
4       System  0x132821900000  False   False   False   \Windows\System32\ntdll.dll
396     smss.exe        0x7ffa735f0000  True    True    True    \Windows\System32\ntdll.dll
396     smss.exe        0x7ff7d8f00000  True    False   True    \Windows\System32\smss.exe
556     csrss.exe       0x7ffa706c0000  True    True    True    \Windows\System32\csrsrv.dll
556     csrss.exe       0x7ff67f1e0000  True    False   True    \Windows\System32\csrss.exe
556     csrss.exe       0x7ffa70640000  True    True    True    \Windows\System32\sxssrv.dll
556     csrss.exe       0x7ffa704d0000  True    True    True    \Windows\System32\sxs.dll
556     csrss.exe       0x7ffa70360000  True    True    True    \Windows\System32\ServicingCommon.dll
556     csrss.exe       0x7ffa70680000  True    True    True    \Windows\System32\winsrv.dll
556     csrss.exe       0x7ffa70650000  True    True    True    \Windows\System32\winsrvext.dll
556     csrss.exe       0x7ffa706a0000  True    True    True    \Windows\System32\basesrv.dll
556     csrss.exe       0x7ffa71280000  True    True    True    \Windows\System32\kernel32.dll
556     csrss.exe       0x7ffa70970000  True    True    True    \Windows\System32\msvcp_win.dll
556     csrss.exe       0x7ffa70850000  True    True    True    \Windows\System32\ucrtbase.dll
556     csrss.exe       0x7ffa70820000  True    True    True    \Windows\System32\bcrypt.dll
556     csrss.exe       0x7ffa70c70000  True    True    True    \Windows\System32\gdi32full.dll
556     csrss.exe       0x7ffa70ad0000  True    True    True    \Windows\System32\win32u.dll
556     csrss.exe       0x7ffa70ea0000  True    True    True    \Windows\System32\KernelBase.dll
556     csrss.exe       0x7ffa70da0000  True    True    True    \Windows\System32\bcryptprimitives.dll
556     csrss.exe       0x7ffa72be0000  True    True    True    \Windows\System32\advapi32.dll
556     csrss.exe       0x7ffa72530000  True    True    True    \Windows\System32\user32.dll
556     csrss.exe       0x7ffa723c0000  True    True    True    \Windows\System32\sechost.dll
556     csrss.exe       0x7ffa73100000  True    True    True    \Windows\System32\gdi32.dll
556     csrss.exe       0x7ffa73050000  True    True    True    \Windows\System32\msvcrt.dll
556     csrss.exe       0x7ffa72d80000  True    True    True    \Windows\System32\rpcrt4.dll
```

Registry & Configuration:

Prints contents of registry keys

```
12:52:15 csi@csi ~/volatility3
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.registry.printkey
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Last Write Time Hive Offset     Type    Key     Name    Data    Volatile

2025-05-02 08:13:15.000000 UTC  0x930155665000  Key     [NONAME]        A       N/A     False
2025-05-02 06:13:10.000000 UTC  0x930155665000  Key     [NONAME]        MACHINE N/A     False
2025-05-02 02:50:15.000000 UTC  0x930155665000  Key     [NONAME]        USER    N/A     False
2025-05-02 07:28:08.000000 UTC  0x930155665000  Key     [NONAME]        WC      N/A     False
2022-05-07 05:25:15.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        ActivationBroker        N/A     False
2025-04-24 10:46:21.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        ControlSet001   N/A     False
2025-05-02 05:47:23.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        DriverDatabase  N/A     False
2025-05-02 02:49:52.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        HardwareConfig  N/A     False
2022-05-07 05:25:13.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        Input   N/A     False
2022-05-07 06:01:48.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        Keyboard Layout N/A     False
2022-05-07 05:25:13.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        Maps    N/A     False
2025-05-02 03:48:20.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        MountedDevices  N/A     False
2022-05-07 05:25:13.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        ResourceManager N/A     False
2022-05-07 05:25:13.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        ResourcePolicyStore     N/A     False
2025-05-02 02:49:52.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        RNG     N/A     False
2022-05-07 05:25:13.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        Select  N/A     False
2025-05-02 05:47:22.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        Setup   N/A     False
2022-05-07 05:25:13.000000 UTC  0x930155677000  Key     \REGISTRY\MACHINE\SYSTEM        Software        N/A     False
```

Lists registry hives in memory

```
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.registry.hivelist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  FileFullPath    File output

0x930155665000          Disabled
0x930155677000  \REGISTRY\MACHINE\SYSTEM         Disabled
0x9301556a5000  \REGISTRY\MACHINE\HARDWARE       Disabled
0x9301572ab000  \SystemRoot\System32\Config\SOFTWARE    Disabled
0x9301581d0000  \Device\HarddiskVolume1\EFI\Microsoft\Boot\BCD  Disabled
0x930155db6000  \SystemRoot\System32\Config\DEFAULT     Disabled
0x9301584b6000  \SystemRoot\System32\Config\SECURITY    Disabled
0x930158516000  \SystemRoot\System32\Config\SAM Disabled
0x9301586d5000  \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       Disabled
0x9301588be000  \SystemRoot\System32\Config\BBI Disabled
0x9301588e3000  \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Disabled
0x93015a76a000  \??\C:\Users\HSRI\ntuser.dat    Disabled
0x93015a7e2000  \??\C:\Users\HSRI\AppData\Local\Microsoft\Windows\UsrClass.dat  Disabled
0x930158b5b000  \??\C:\Windows\AppCompat\Programs\Amcache.hve   Disabled
0x93015b281000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\MicrosoftWindows.Client.FileExp_1000.22700.1000.0_x64__cw5n1h2txyewy\ActivationStore.dat    Disabled
0x93015b27f000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\MicrosoftWindows.Client.Core_1000.22700.1020.0_x64__cw5n1h2txyewy\ActivationStore.dat      Disabled
0x93015b27c000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\MicrosoftWindows.Client.CBS_1000.22700.1081.0_x64__cw5n1h2txyewy\ActivationStore.dat       Disabled
0x93015b610000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenuExperienceHost_10.0.22621.4249_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat Disabled
0x93015b705000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.UI.Xaml.CBS_8.2404.3001.0_x64__8wekyb3d8bbwe\ActivationStore.dat  Disabled
0x93015b6eb000  \??\C:\Users\HSRI\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\Settings\settings.dat       Disabled
0x93015b77d000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\MicrosoftWindows.Client.WebExperience_525.10401.30.0_x64__cw5n1h2txyewy\ActivationStore.dat Disabled
0x93015b792000  \??\C:\ProgramData\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\S-1-5-21-2024401937-3989158610-945509862-1001\SystemAppData\Helium\Cache\2949f22fc3f6f7e.dat    Disabled
0x93015b794000  \??\C:\Users\HSRI\AppData\Local\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\SystemAppData\Helium\User.dat      Disabled
0x93015b803000  \??\C:\Users\HSRI\AppData\Local\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\SystemAppData\Helium\UserClasses.dat       Disabled
0x93015b806000  \??\C:\ProgramData\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\S-1-5-21-2024401937-3989158610-945509862-1001\SystemAppData\Helium\Cache\2949f22fc3f6f7e_COM15.dat      Disabled
0x93015b80e000  \??\C:\ProgramData\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\S-1-5-21-2024401937-3989158610-945509862-1001\SystemAppData\Helium\Cache\2949f22fc3f6f7e.dat    Disabled
```

Scans memory for registry hives (useful if hivelist fails)

```
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.registry.hivescan
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset

0x93015f2e2000
0x930160c84000
0x93015e228000
0x93016064f000
0x93015f05d000
0x930155db6000
0x9301572ab000
0x93015b870000
0x9301584b6000
0x9301581d0000
0x93015a76a000
0x93015bc20000
0x930155677000
0x93015bc0f000
0x93015efb4000
0x93015c8e2000
0x93016076d000
0x93015e497000
0x9301664fc000
0x93015b705000
0x9301588be000
0x93015f5cd000
0x93015b77d000
0x93015c6ea000
0x93015997e000
```

Network Activity:

Scans for network connections and sockets

```
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.netscan
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xd207df09f470  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1804    svchost.exe     2025-05-02 02:50:04.000000 UTC
0xd207df09f470  TCPv6   ::      49667   ::      0       LISTENING       1804    svchost.exe     2025-05-02 02:50:04.000000 UTC
0xd207df09fb50  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1244    svchost.exe     2025-05-02 02:50:04.000000 UTC
0xd207df09fe10  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1244    svchost.exe     2025-05-02 02:50:04.000000 UTC
0xd207df09fe10  TCPv6   ::      49666   ::      0       LISTENING       1244    svchost.exe     2025-05-02 02:50:04.000000 UTC
0xd207df16cab0  TCPv4   192.168.0.160   26460   146.75.118.172  80      CLOSED  -       -       N/A
0xd207e10c2050  TCPv6   ::1     26439   ::1     3306    ESTABLISHED     -       -       N/A
0xd207e24c4010  TCPv6   2409:4063:4bc4:ac61:40de:4325:924d:37f5 51711   2603:1040:a06:6::2      443     CLOSED  -       -       N/A
0xd207e25c7050  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       1020    svchost.exe     2025-05-02 02:50:03.000000 UTC
0xd207e25c71b0  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2025-05-02 02:50:07.000000 UTC
0xd207e25c71b0  TCPv6   ::      445     ::      0       LISTENING       4       System  2025-05-02 02:50:07.000000 UTC
0xd207e25c7470  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       760     services.exe    2025-05-02 02:50:07.000000 UTC
0xd207e25c7470  TCPv6   ::      49670   ::      0       LISTENING       760     services.exe    2025-05-02 02:50:07.000000 UTC
0xd207e25c75d0  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       760     services.exe    2025-05-02 02:50:07.000000 UTC
0xd207e25c7730  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       628     wininit.exe     2025-05-02 02:50:03.000000 UTC
0xd207e25c7b50  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1804    svchost.exe     2025-05-02 02:50:04.000000 UTC
0xd207e25c7cb0  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2620    spoolsv.exe     2025-05-02 02:50:05.000000 UTC
0xd207e25c7e10  TCPv4   0.0.0.0 80      0.0.0.0 0       LISTENING       4       System  2025-05-02 02:50:07.000000 UTC
0xd207e25c7e10  TCPv6   ::      80      ::      0       LISTENING       4       System  2025-05-02 02:50:07.000000 UTC
0xd207e25c80d0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       784     lsass.exe       2025-05-02 02:50:03.000000 UTC
0xd207e25c8230  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2620    spoolsv.exe     2025-05-02 02:50:05.000000 UTC
0xd207e25c8230  TCPv6   ::      49668   ::      0       LISTENING       2620    spoolsv.exe     2025-05-02 02:50:05.000000 UTC
0xd207e25c84f0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       1020    svchost.exe     2025-05-02 02:50:03.000000 UTC
0xd207e25c84f0  TCPv6   ::      135     ::      0       LISTENING       1020    svchost.exe     2025-05-02 02:50:03.000000 UTC
0xd207e25c8bd0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       784     lsass.exe       2025-05-02 02:50:03.000000 UTC
0xd207e25c8bd0  TCPv6   ::      49664   ::      0       LISTENING       784     lsass.exe       2025-05-02 02:50:03.000000 UTC
```

Security & Malware Detection:

Detects potentially injected code and memory regions

```
❯ python3 vol.py -f /home/csi/HS-20250803-071041.dmp -p windows windows.malfind
Volatility 3 Framework 2.26.2
/home/csi/volatility3/volatility3/framework/deprecation.py:28: FutureWarning: This API (volatility3.plugins.windows.malware.ma
 has been renamed, please call volatility3.plugins.windows.malware.malfind.Malfind rather than volatility3.plugins.windows.mal
  warnings.warn(

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdu
/home/csi/volatility3/volatility3/framework/deprecation.py:105: FutureWarning: This plugin (volatility3.plugins.windows.malfi
. Please ensure all method calls to this plugin are replaced with calls to volatility3.plugins.windows.malware.malfind.Malfin
  warnings.warn(

3444    MsMpEng.exe     0x2c307200000   0x2c30730cfff   VadS    PAGE_EXECUTE_READWRITE  269     1       Disabled        N/A
56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..(
4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H...8....
49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A\][_^
c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 80 61 ...@.....H..H..a
0x2c307200000:  push    rsi
0x2c307200001:  push    rdi
0x2c307200002:  push    rbx
0x2c307200003:  push    rbp
0x2c307200004:  push    r12
0x2c307200006:  push    r13
0x2c307200008:  push    r14
0x2c30720000a:  push    r15
0x2c30720000c:  sub     rsp, 0x28
0x2c307200010:  lea     r15, [rsp]
0x2c307200014:  mov     rbp, rcx
0x2c307200017:  lea     rsi, [rcx + 0x3898]
0x2c30720001e:  jmp     rdx
0x2c307200020:  lea     rsp, [r15 + 0x28]
0x2c307200024:  pop     r15
0x2c307200026:  pop     r14
0x2c307200028:  pop     r13
0x2c30720002a:  pop     r12
0x2c30720002c:  pop     rbp
0x2c30720002d:  pop     rbx
0x2c30720002e:  pop     rdi
0x2c30720002f:  pop     rsi
0x2c307200030:  ret
0x2c307200031:  add     byte ptr [rax], al
```

Scans memory for loaded kernel modules

```
❯ python3 vol.py -f /home/csi/HS-20250803-071041.dmp -p windows windows.modscan
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Base    Size    Name    Path    File output

0xd0846d0698a0  0xf8040b440000  0x6000  hal.dll \SystemRoot\system32\hal.dll    Disabled
0xd0846d06bdd0  0xf8040b450000  0xb000  kdcom.dll       \SystemRoot\system32\kd.dll     Disabled
0xd0846d06c730  0xf8040d000000  0x1047000       ntoskrnl.exe    \SystemRoot\system32\ntoskrnl.exe       Disabled
0xd0846d06cb80  0xf8040b0b0000  0x383000        mcupdate.dll    \SystemRoot\system32\mcupdate_GenuineIntel.dll  Disabled
0xd0846d06cdc0  0xf8040b490000  0x6f000 CLFS.SYS        \SystemRoot\System32\drivers\CLFS.SYS   Disabled
0xd0846d06d010  0xf8040b460000  0x29000 tm.sys  \SystemRoot\System32\drivers\tm.sys     Disabled
0xd0846d06d1e0  0xf8040b500000  0x1b000 PSHED.dll       \SystemRoot\system32\PSHED.dll  Disabled
0xd0846d06d3b0  0xf8040b520000  0xd000  BOOTVID.dll     \SystemRoot\system32\BOOTVID.dll        Disabled
0xd0846d06d570  0xf8040b530000  0x7a000 FLTMGR.SYS      \SystemRoot\System32\drivers\FLTMGR.SYS Disabled
0xd0846d06d750  0xf80410b20000  0x62000 msrpc.sys       \SystemRoot\System32\drivers\msrpc.sys  Disabled
0xd0846d06d930  0xf8040b5b0000  0x2f000 ksecdd.sys      \SystemRoot\System32\drivers\ksecdd.sys Disabled
0xd0846d06db10  0xf80410a00000  0x115000        clipsp.sys      \SystemRoot\System32\drivers\clipsp.sys Disabled
0xd0846d06dd30  0xf8040b5e0000  0x10000 cmimcext.sys    \SystemRoot\System32\drivers\cmimcext.sys       Disabled
0xd0846d06e010  0xf80410b90000  0x16000 werkernel.sys   \SystemRoot\System32\drivers\werkernel.sys      Disabled
0xd0846d06e1f0  0xf80410bb0000  0xc000  ntosext.sys     \SystemRoot\System32\drivers\ntosext.sys        Disabled
0xd0846d06e3c0  0xf80410bc0000  0xfb000 CI.dll  \SystemRoot\system32\CI.dll     Disabled
0xd0846d06e5b0  0xf80410cc0000  0xbe000 cng.sys \SystemRoot\System32\drivers\cng.sys    Disabled
0xd0846d06e780  0xf80410d80000  0xc7000 Wdf01000.sys    \SystemRoot\system32\drivers\Wdf01000.sys       Disabled
0xd0846d06e970  0xf80410e70000  0x13000 WppRecorder.sys \SystemRoot\system32\drivers\WppRecorder.sys    Disabled
0xd0846d06eb50  0xf80410e50000  0x17000 WDFLDR.SYS      \SystemRoot\system32\drivers\WDFLDR.SYS Disabled
0xd0846d06ed20  0xf80410e90000  0xe000  PRM.sys \SystemRoot\System32\DriverStore\FileRepository\prm.inf_amd64_de435dc5c75d64a5\PRM.sys  Disabled
0xd0846d06f010  0xf80410ea0000  0x27000 acpiex.sys      \SystemRoot\System32\Drivers\acpiex.sys Disabled
0xd0846d06f1e0  0xf80410ed0000  0xb8000 ACPI.sys        \SystemRoot\System32\drivers\ACPI.sys   Disabled
0xd0846d06f3c0  0xf80410f90000  0xc000  WMILIB.SYS      \SystemRoot\System32\drivers\WMILIB.SYS Disabled
0xd0846d06f590  0xf80410fa0000  0xb000  msisadrv.sys    \SystemRoot\System32\drivers\msisadrv.sys       Disabled
0xd0846d06f760  0xf80410fb0000  0x8c000 pci.sys \SystemRoot\System32\drivers\pci.sys    Disabled
0xd0846d06f930  0xf80411040000  0x57000 tpm.sys \SystemRoot\System32\drivers\tpm.sys    Disabled
0xd0846d06fcc0  0xf804110b0000  0x86000 intelpep.sys    \SystemRoot\System32\drivers\intelpep.sys       Disabled
0xd0846d070010  0xf80411140000  0x19000 WindowsTrustedRT.sys    \SystemRoot\system32\drivers\WindowsTrustedRT.sys       Disabled
0xd0846d0701f0  0xf80411160000  0x13000 IntelPMT.sys    \SystemRoot\System32\drivers\IntelPMT.sys       Disabled
0xd0846d0703c0  0xf80411180000  0xb000  WindowsTrustedRTProxy.sys       \SystemRoot\System32\drivers\WindowsTrustedRTProxy.sys  Disabled
0xd0846d0705b0  0xf80411190000  0x16000 pcw.sys \SystemRoot\System32\drivers\pcw.sys    Disabled
0xd0846d070770  0xf804111b0000  0x1c000 vdrvroot.sys    \SystemRoot\System32\drivers\vdrvroot.sys       Disabled
0xd0846d070940  0xf80411270000  0xe1000 spaceport.sys   \SystemRoot\System32\drivers\spaceport.sys      Disabled
```

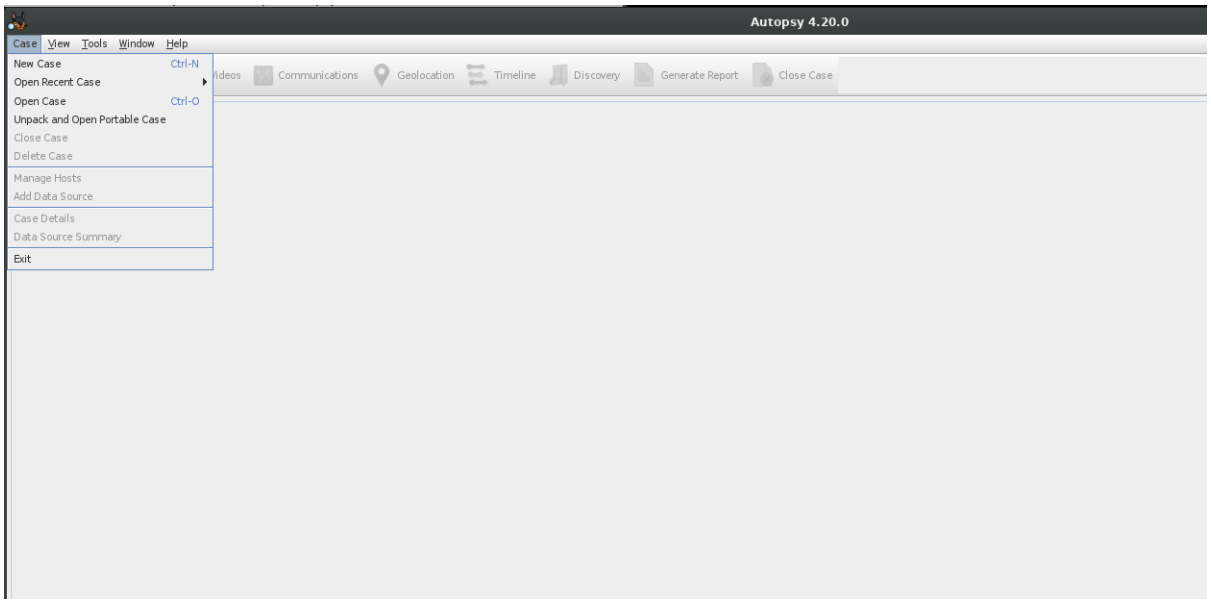
Miscellaneous:

Displays metadata about the memory image (OS, architecture, etc.)

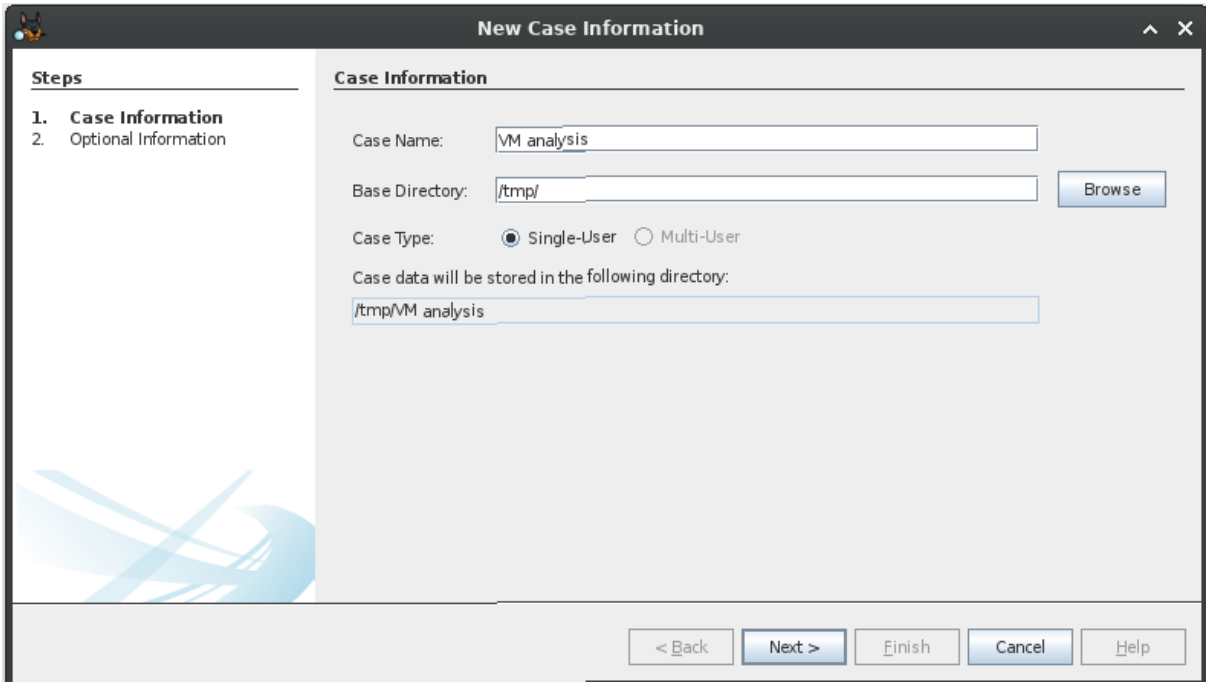
```
12:15:03 csi@csi ~/volatility3
❯ python3 vol.py -f ../HS-20250502-080600.raw windows.info
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf80074600000
DTB     0x1ae000
Symbols file:///home/csi/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/9A3533F8CCC878F8F791BADD952A6EC8-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80075209998
Major/Minor     15.22621
MachineType     34404
KeNumberProcessors      2
SystemTime      2025-05-02 08:11:57+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Tue Aug 24 22:18:17 2077
```

AUTOPSY

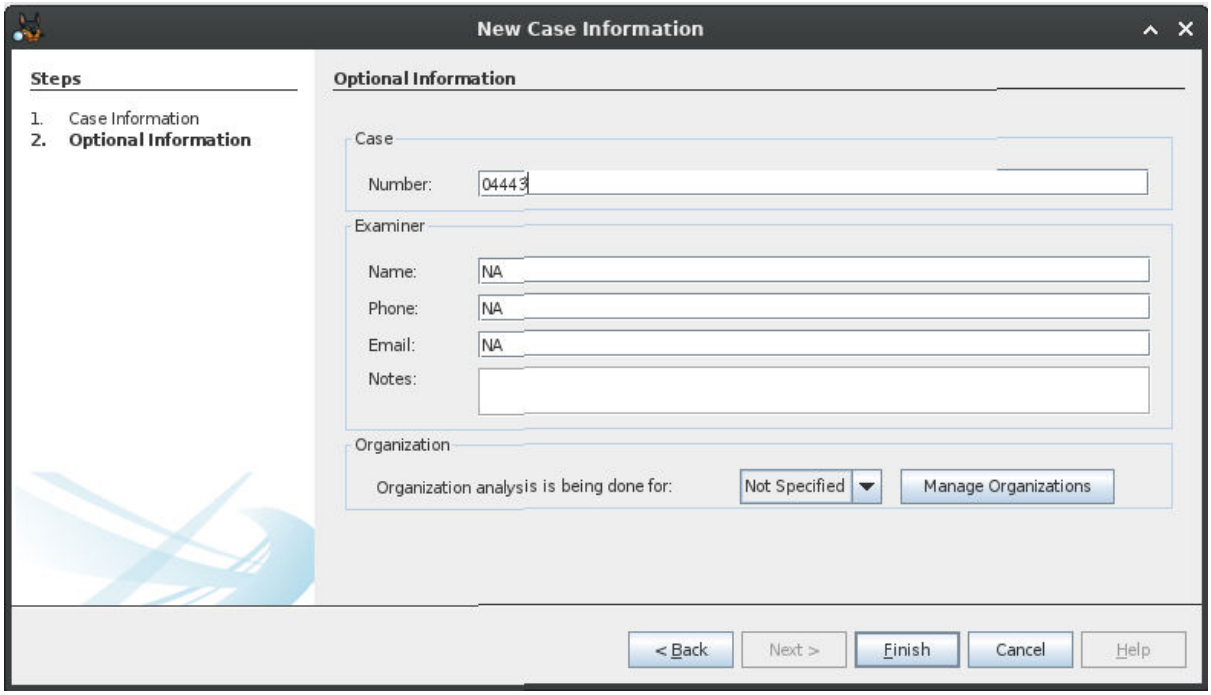
STEP1:



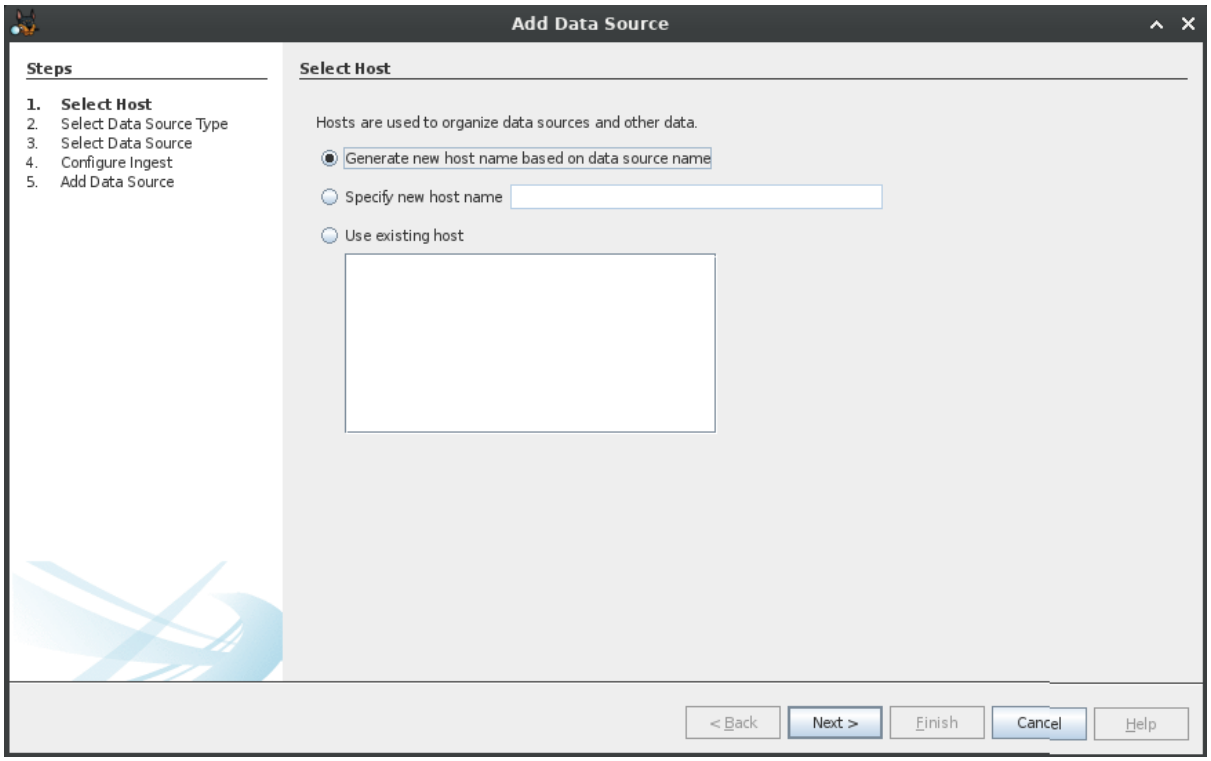
STEP2:



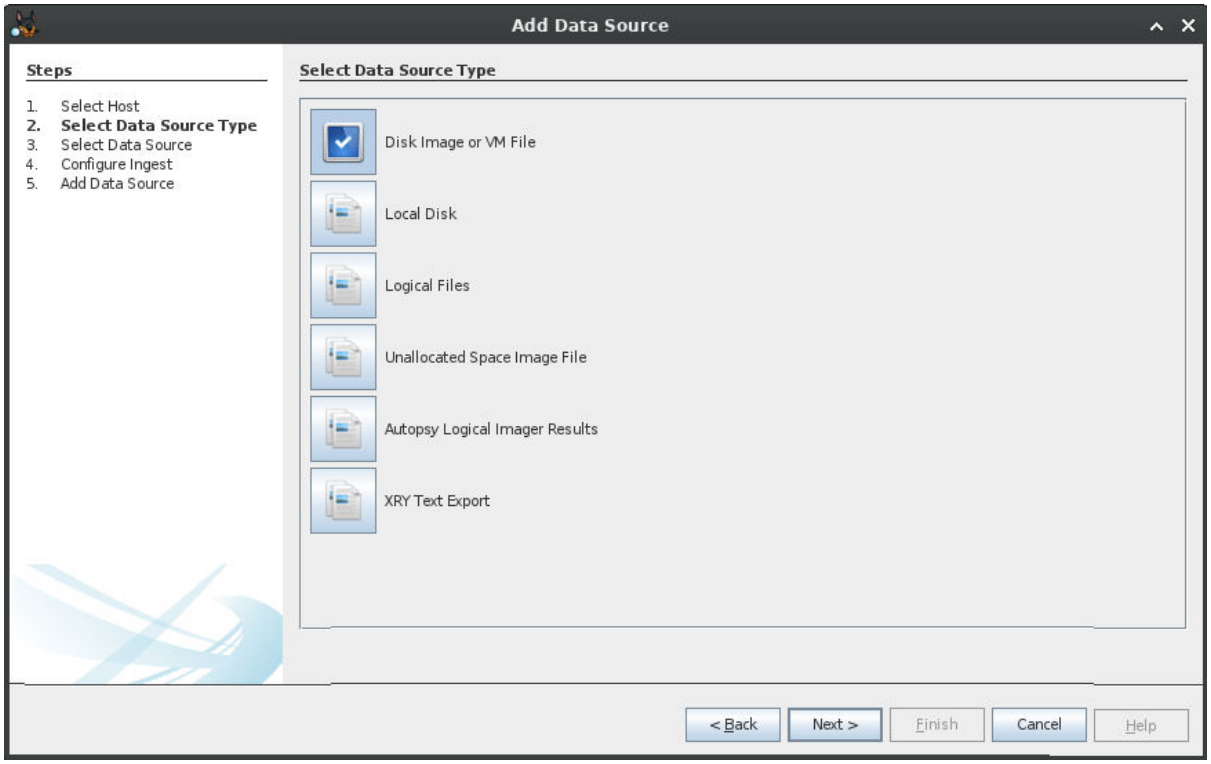
STEP3:


New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 04443
Examiner
Name: NA
Phone: NA
Email: NA
Notes:
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help

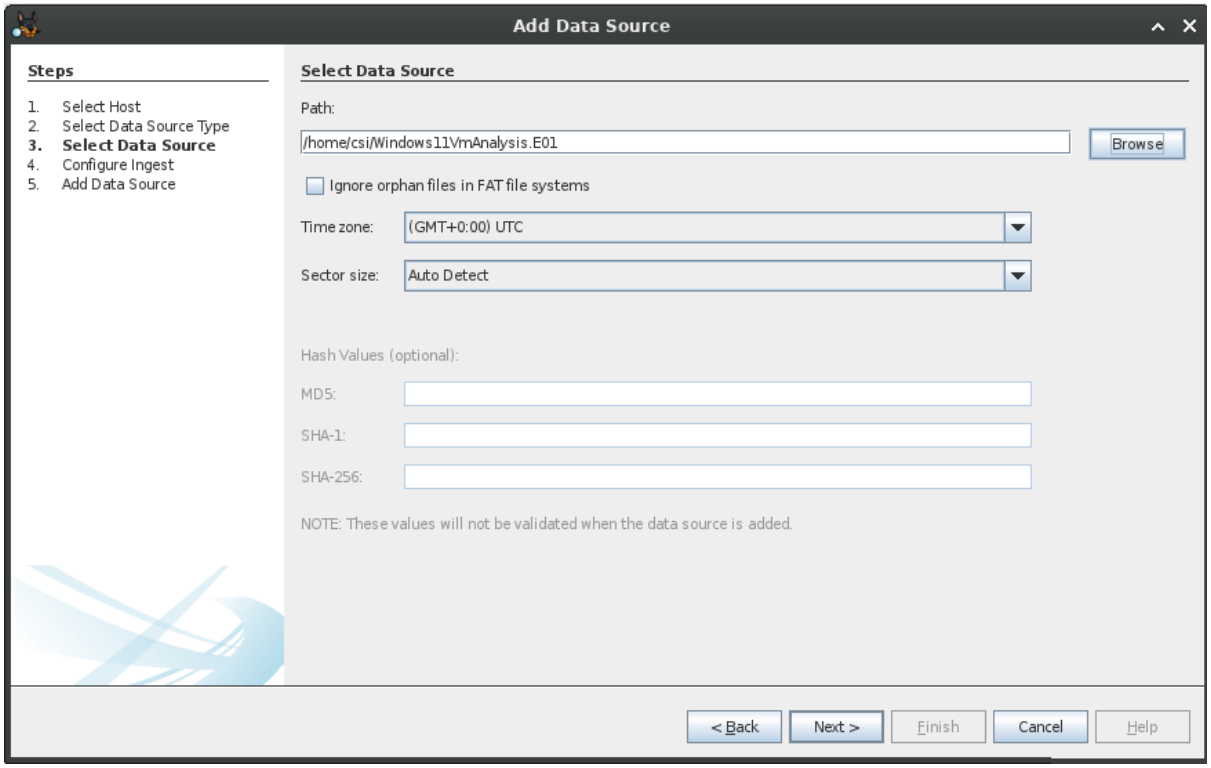
STEP4:


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help

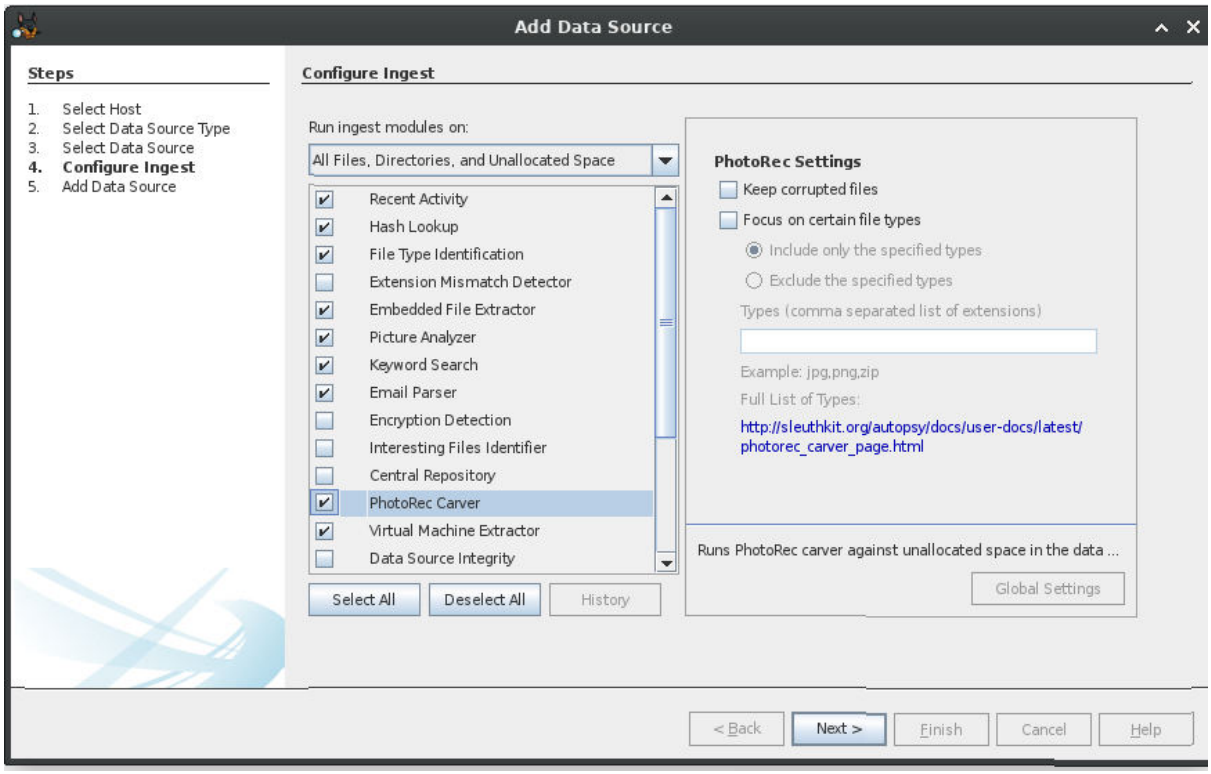
STEP5:


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help

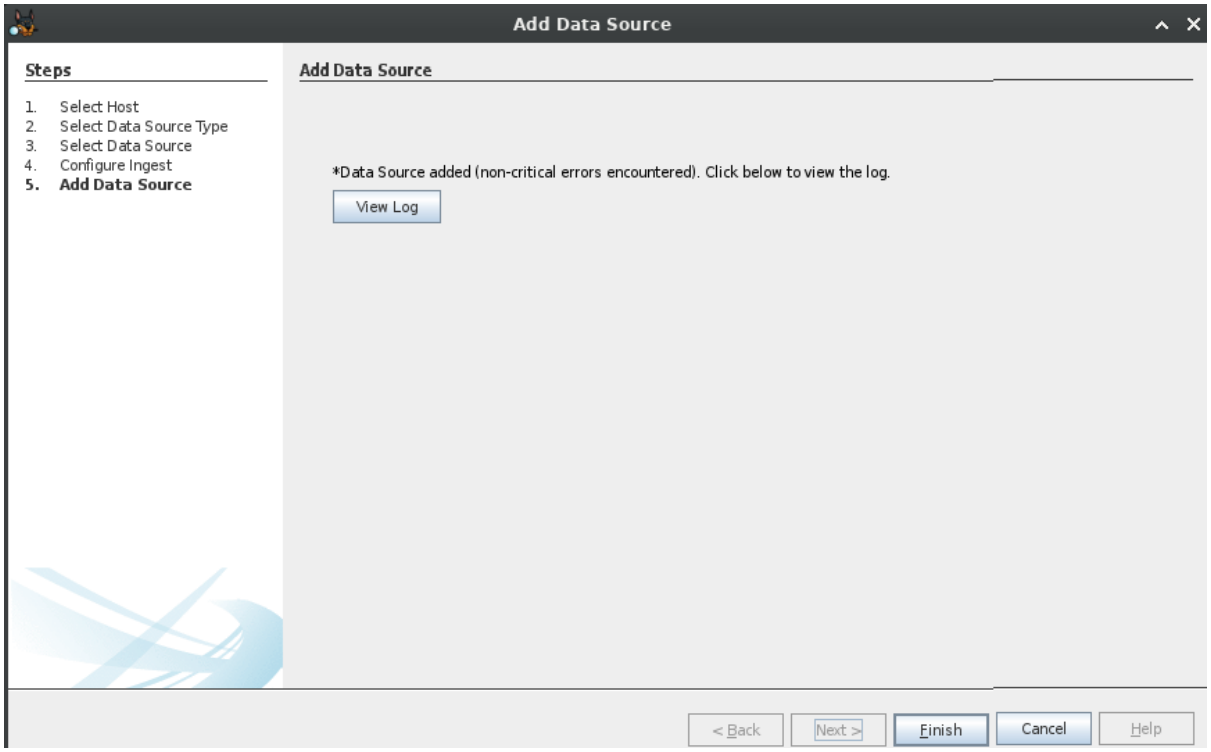
STEP6:


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
/home/csi/Windows11VmAnalysis.E01
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT+0:00) UTC
Sector size:
Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help

STEP7:

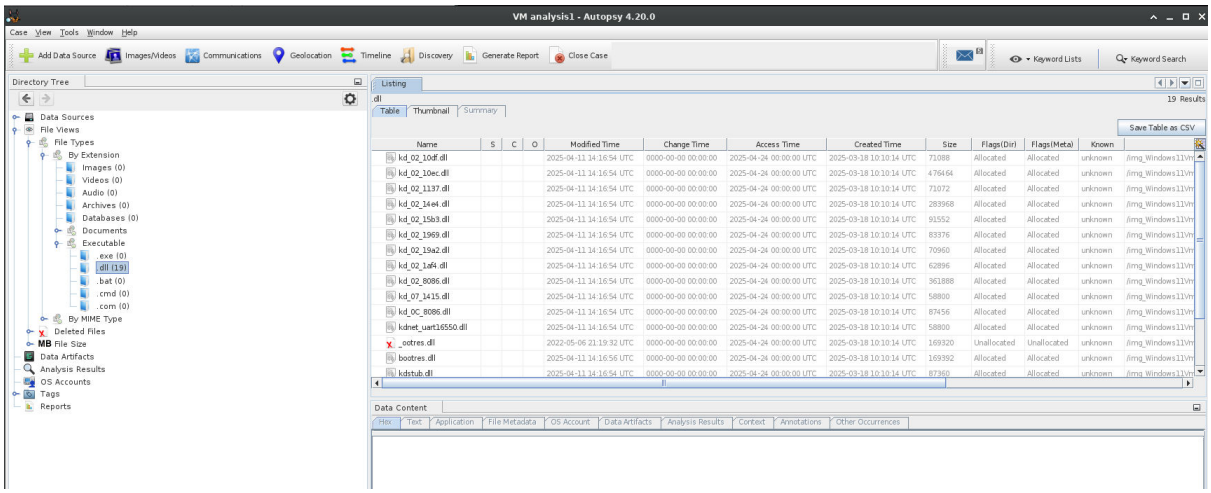

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Select All
Deselect All
History
PhotoRec Settings
Keep corrupted files
Focus on certain file types
Include only the specified types
Exclude the specified types
Types (comma separated list of extensions)
Example: jpg,png,zip
Full List of Types:
http://sleuthkit.org/autopsy/docs/user-docs/latest/photorec_carver_page.html
Runs PhotoRec carver against unallocated space in the data ...
Global Settings
< Back
Next >
Finish
Cancel
Help

STEP8:

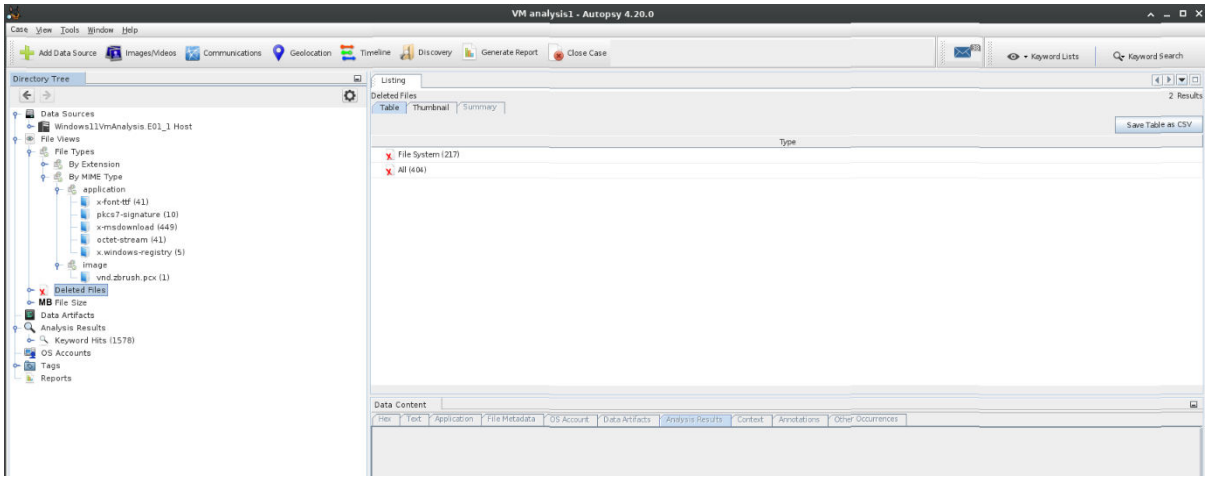

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
*Data Source added (non-critical errors encountered). Click below to view the log.
View Log
< Back
Next >
Finish
Cancel
Help

OUTCOME:

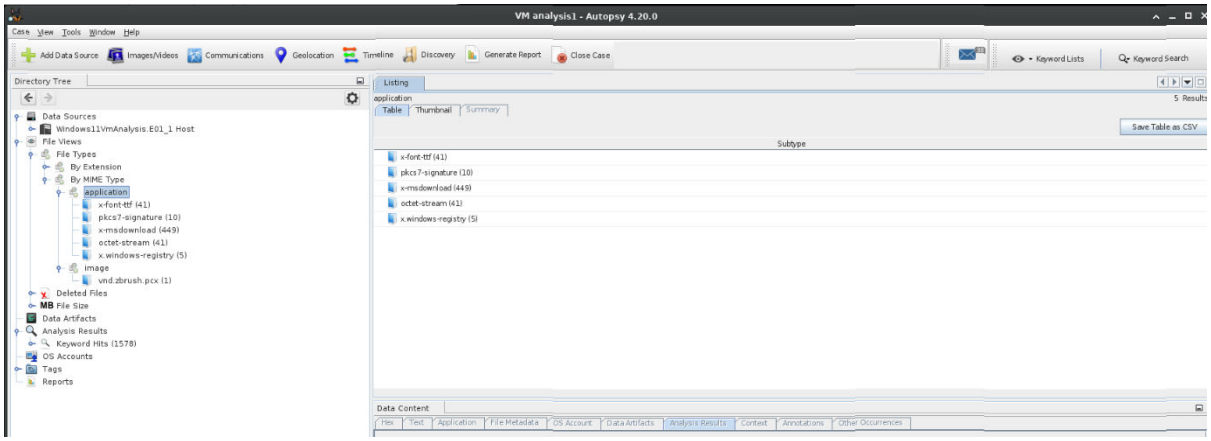
1: The output displays metadata of 21 .dll files within Autopsy, showing their creation, access, modification times and file size, useful for timeline and anomaly analysis in forensic investigations.



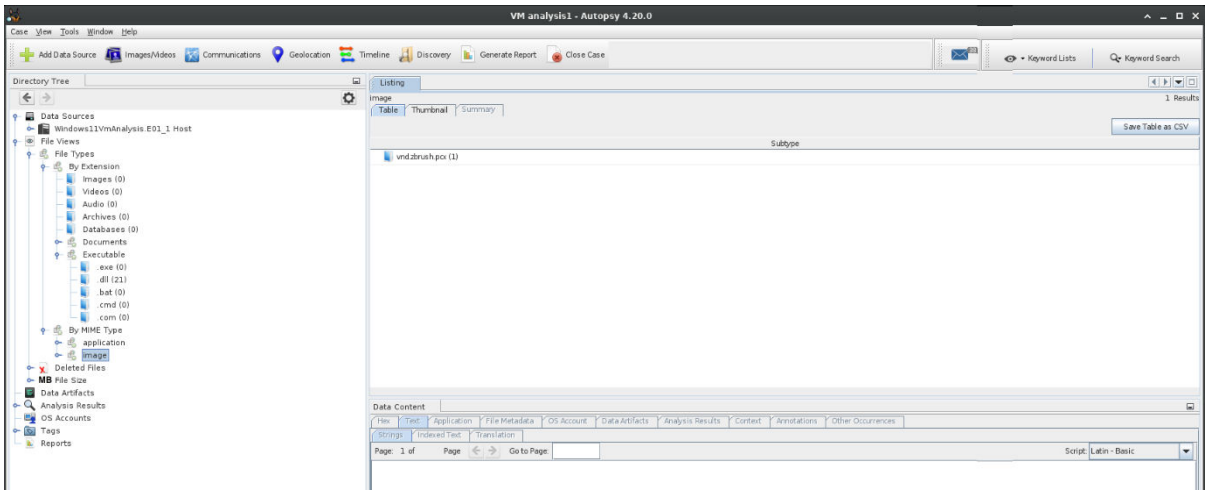
2: The output highlights deleted file evidence from a Windows 11 VM image within Autopsy, useful for recovery and timeline reconstruction in forensic analysis. The Autopsy output shows 404 deleted files that were recovered from the Windows 11 VM image.



3: The output displays Autopsy's MIME-type breakdown of recovered files, totaling 546 files across formats like executables, registry entries, fonts, and certificates — vital for classifying content and prioritizing forensic triage.



4: The output shows Autopsy's file type categorization for the data source, highlighting 1 recovered .pcx image file (vnd.zbrush.pcx) from the Windows11VmAnalysis.E01_1_Host — useful for artifact validation and narrowing file relevance in forensic review.



CONCLUSION

This project systematically demonstrated a complete workflow for live digital forensic investigation within a virtualized Windows 11 environment, utilizing CSI Linux as the analysis platform. Through the structured phases of evidence acquisition, preservation, examination, and reporting, critical insights were achieved into both the volatile (memory) and non-volatile (disk) states of the target system.

The use of the **dumplt** tool enabled the secure capture of a raw memory image from the live Windows 11 VM, preserving volatile artifacts that would otherwise be lost upon shutdown. Comprehensive analysis with **Volatility3** revealed valuable information about running processes, active network connections, and in-memory indicators of compromise, providing a real-time snapshot of system activity during the investigation window.

In parallel, a full disk image in **E01** format was created using **FTK Imager**. Subsequent in-depth analysis with **Autopsy** on CSI Linux enabled the exploration and recovery of file systems, detection of deleted or suspicious files, timeline analysis, and correlation of user behaviour with system artifacts. The integration of memory and disk analysis provided a holistic understanding of the system's state, supporting effective incident response and evidentiary record keeping.

By documenting each phase—tool usage, evidence handling, result interpretation, and reporting—the project not only achieved its investigative objectives but also outlined a practical, repeatable methodology appropriate for both academic and professional digital forensics contexts. The workflow established here reinforces best practices in cross-platform forensic operations, highlights the importance of combining volatile and persistent data analysis, and underscores the synergy of open-source and commercial tools.

In conclusion, this work equips practitioners with a robust approach for investigating security incidents in modern, virtualized environments, ensuring both technical depth and procedural rigor in digital forensic investigations.

REFERENCES

1. CSI Linux Documentation

CSI Linux. (2024). Digital Forensics Operating System. [Available in CSI Linux Help and Documentation Panel]

2. Volatility3 Framework

Volatility Foundation. (2024). Volatility 3 Documentation. https://volatility3.org

3. Autopsy Digital Forensics Platform

Basis Technology. (2024). Autopsy User Guide. https://sleuthkit.org/autopsy/docs/user-docs/

4. FTK Imager

Exterro (AccessData). (2024). FTK Imager User Guide. https://accessdata.com/product-download/ftk-imager-version-4-7-1

5. dumplt Memory Acquisition Tool

"dumplt: Memory Dump Acquisition Tool for Windows". Internal Documentation, 2024.

6. General Digital Forensics Texts

- Carrier, B. (2011). File System Forensic Analysis. Addison-Wesley.

- Casey, E. (2015). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press.

7. Operating System Documentation

Microsoft. (2024). Windows 11 Documentation and Security Guide. https://docs.microsoft.com/en-us/windows/

8. Other Online Resources

Sleuth Kit Wiki. https://wiki.sleuthkit.org

DFIR Community and CSI Linux Forums