

Digital Forensics and Incident Response Lab-1

S SHRAVAN KUMAR

PES1UG22CS493

Task-1

Some of the popular open source tools for forensics are :

1. Autopsy

Autopsy is an end-to-end open source digital forensics platform

Autopsy can do File System analysis which can be used to recover and analyze any hidden files and remnants of file fragments

Autopsy sanitizes the files to be analyzed and can analyze the files in many formats.

It allows us to view any meta-data details in the file system

2. SIFT is a comprehensive collection of open-source Digital Forensics Tools and software

It can be used to carry out Disk Forensics

It contains both Sleuth Kit CLI for disk analysis and Autopsy GUI for file system analysis and deleted data recovery

File carving and recovery using Scalpel and Foremost

Memory Forensics can be carried out i.e analysis of DRAM dumps

Can also perform Hash Analysis and Network Forensics, Malware Analysis, Email Analysis and Metadata Extraction

3. Volatility: Volatility is an open source framework designed to analyze

DRAM dumps (it's included as dram analysis tool in SIFT)

It can provide insights on the running processes, Network activity, files in memory, Malware, Current System State and also provide Timeline analysis

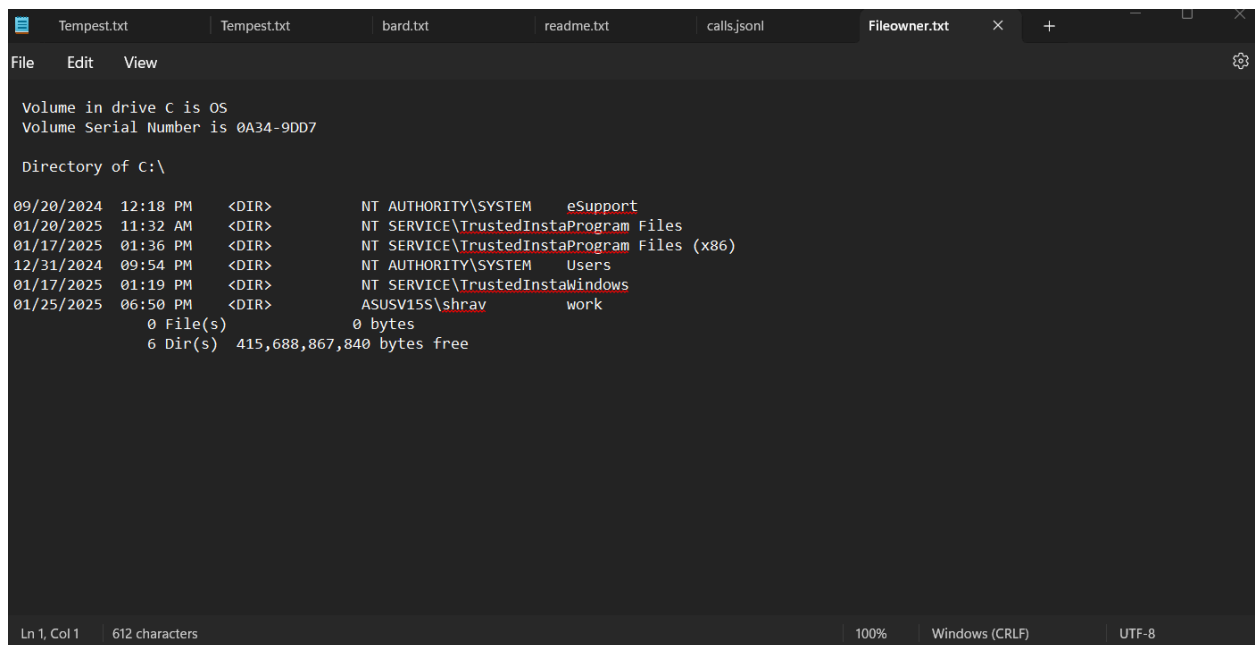
Task-2

```
C:\>md work
```

```
C:\>dir /q > C:\work\Fileowner.txt
```

```
C:\>notepad C:\work\Fileowner.txt
```

```
C:\>notepad C:\work\Fileowner.txt
```



The screenshot shows a Windows Notepad application window with the file 'Fileowner.txt' open. The text inside the window is the output of the 'dir /q' command, which lists the contents of the C:\ drive. The output includes the volume information for drive C, the directory listing, and the free space on the drive.

```
File Edit View

Volume in drive C is OS
Volume Serial Number is 0A34-9DD7

Directory of C:\

09/20/2024 12:18 PM <DIR> NT AUTHORITY\SYSTEM eSupport
01/20/2025 11:32 AM <DIR> NT SERVICE\TrustedInstaProgram Files
01/17/2025 01:36 PM <DIR> NT SERVICE\TrustedInstaProgram Files (x86)
12/31/2024 09:54 PM <DIR> NT AUTHORITY\SYSTEM Users
01/17/2025 01:19 PM <DIR> NT SERVICE\TrustedInstaWindows
01/25/2025 06:50 PM <DIR> ASUSV15S\shrav work
0 File(s) 0 bytes
6 Dir(s) 415,688,867,840 bytes free

Ln 1, Col 1 612 characters 100% Windows (CRLF) UTF-8
```

Task-3

Chain of Custody

Chain of Custody is a legal document that maintains a trail records the chronological sequence of custody, control and access, transfer of materials which could include either physical or electronic evidences.

It is a proces that has been required for evidence to be shown legally in court. Maintaining a Chain of Custody is essential for forensic scientist working on a specific criminal case. The documentation of evidence is necessar for maintaining a chain of custody because everything that is done or performed on the piece of evidence must be listed and whoever came in contact with that piece of evidence is accountable for whatever happens to it.

This prevents contamination of evidence by officials or from taking a piece of evidence.

Task-4

We shall compare the following Open Source forensics tools:

The Sleuth Kit, Autopsy and Volatility

Sleuth Kit: is a collection of command-line tools that provides a deep, low-level analysis of disk images, supporting a wide range of file systems. It is the backend system for Autopsy

Features/Capabilities of Sleuth Kit:

Disk Imaging, File System Analysis, Data Recovery, Volume and Partition Analysis, MetaData Analysis, Hashing and Integrity Checking.

Autopsy: is a Graphical Interface that uses the Sleuth Kit underneath it. Its a digital forensics tool primarily designed for disk forensics and provides file system analysis , emails, internet history and other data

Key Features are:

File System Analysis, (FAT, NTFS, ext etc.) , Timeline Analysis, Keyword Search, Hash Analysis, Email and Browser artifacts, all the above features in a single GUI based package. It supports File Carving.

Volatility: Volatility is an advanced memory forensics tool used to analyze volatile memory (RAM) dumps. It helps us to understand the state of a system using the primary memory and analyzing the processes running which store memory in the primary and current network activity, malware etc.

Key Features are:

Memory Dump Analysis, Malware Analysis, Process Analysis, Network Forensics, Timeline Creation.

It provides cross platform support, deep memory analysis, forensic logging.

Task 5

The Craigslist Killer

This case involves Philip Markoff, a medical student who, in 2009, used Craigslist to target two women who had advertised their services through the site. He lured them into meeting under the pretense of paying for said services, then robbed and them and fatally shot one of the victim. His crimes involved using anonymous email accounts and other digital means to cover his tracks.

The use of Digital Forensic Tools helped in catching hold of the culprit as Markoff created an anonymous email account to communicate with victims without using his personal identity. Email forensics was employed to identify the true sender of the emails, linking them back to Markoff.

Once Markoff's email communications and IP addresses were traced to him, law enforcement focussed their investigation on his computers and network activity. Markoff's cell phone records were analyzed. Cell tower data can be used to track a person's location through the cell phones they use, which is key in identifying when and where the crimes occurred.