SCHOOL OF COMPUTER SCIENCE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN, UTTARAKHAND

DIGITAL FORENSICS

ASSIGNMENT FILE - 2

(2024-2025)

For

Vth Semester

Submitted To:
Prof. Subhranil Das
Assistant Professor S.S.
[Vth Semester]
School of Computer Sciences

Submitted By:
Mr. Akshat Negi
500106533(SAP ID)
R2142220414(Roll No.)
B.Tech. CSF (Batch-1)

ASSIGNMENT FILE – 3

1. Explain the differences between memory forensics and hardware forensics. Discuss how these two types of forensic analysis differ in terms of purpose, methods of acquisition, and challenges faced by forensic investigators.

1. Differences Between Memory Forensics and Hardware Forensics

Memory forensics and hardware forensics are both crucial components of digital forensics, yet they differ significantly in purpose, methods of acquisition, and the challenges faced by investigators.

- **Purpose**:
    - **Memory Forensics**: Primarily focuses on volatile data (data lost when a device is powered off) within a system's memory (RAM). It aims to capture live activity, such as running processes, network connections, and unsaved data, which can provide insights into current system usage and possible malicious activity.
    - **Hardware Forensics**: Concentrates on non-volatile data, usually stored on physical storage devices such as hard drives, SSDs, USB drives, and other forms of physical media. This type of forensic analysis is often used to recover deleted files, analyze file structures, and identify artifacts left behind on the storage medium.
- **Methods of Acquisition**:
    - **Memory Forensics**: Involves using specialized tools (like FTK Imager, Volatility, and Redline) to capture an image of the live memory. The process usually requires the system to be in a running state, as RAM contents disappear upon shutdown.
    - **Hardware Forensics**: Uses disk imaging tools (like EnCase, FTK, or dd) to create an exact replica of the storage device, allowing investigators to analyze it without altering the original evidence. Imaging can be done when the device is offline, making it less likely to alter the data.
- **Challenges**:
    - **Memory Forensics**: One of the biggest challenges is that memory is volatile; any power interruption or system restart erases data. Investigators must work quickly to capture the memory state. Additionally, live system acquisition can potentially modify the contents of memory, affecting evidence integrity.
    - **Hardware Forensics**: Challenges include dealing with encryption and large data storage capacities, which can prolong the imaging process and make the analysis more time-intensive. Furthermore, investigators must ensure no data is modified during acquisition, which requires careful handling of write-blocking tools.

2.Describe the role of file system traces in digital investigations on Windows systems. Include in your explanation how date-time stamps and metafiles can aid forensic analysts in determining the history of file access and modifications.

2. Role of File System Traces in Digital Investigations on Windows Systems

File system traces are essential in Windows-based forensic investigations as they help analysts reconstruct user actions, such as file creation, access, modification, and deletion.

- **Date-Time Stamps**: Windows file systems (e.g., NTFS) record multiple timestamps for each file, including creation, modification, access, and entry modification timestamps (often abbreviated as MACB—Modified, Accessed, Changed, Birth). These timestamps allow investigators to establish a timeline of events, potentially revealing when a file was last accessed or altered, which can indicate user activity and usage patterns.
- **Metafiles**: Metafiles, such as the Master File Table (MFT) in NTFS, store critical metadata about files and directories. The MFT holds information like file paths, size, timestamps, and data fragments. By analyzing these details, forensic analysts can identify deleted files and determine their original locations. Additionally, metafiles like $LogFile in NTFS maintain records of recent changes, aiding in the reconstruction of file history even if attempts to delete or obfuscate have occurred.
- **Usage in Forensic Analysis**: Combining date-time stamps and metafile data enables forensic analysts to trace the history of file access and changes, essential for investigating unauthorized access, verifying alibis, or identifying attempts to tamper with files. Tools like EnCase, Autopsy, and FTK are frequently used to parse and interpret these traces.

3. List and elaborate on the main steps involved in the memory forensics process. Provide an overview of each step, including acquisition, analysis, and the challenges associated with memory forensics.

3. Main Steps in the Memory Forensics Process

Memory forensics involves a sequence of steps to capture, analyze, and interpret volatile data from a live system. Each step is essential to preserving and understanding the memory state of the system under investigation.

- **Acquisition**:
    - The acquisition process involves capturing an image of the system's RAM, using tools that minimize disruption to the live system state. Examples include DumpIt, FTK Imager, or Redline. During acquisition, investigators should take precautions to avoid altering memory contents, as even minor changes can impact the data integrity. Memory dumps are saved in a standard format (e.g., raw or .mem file) for later analysis.
- **Analysis**:
    - Analysis involves examining the memory dump to uncover relevant information. This includes identifying active processes, open network connections, loaded drivers, and registry entries. Tools like Volatility or Recall can help parse these elements. Investigators may look for malicious processes, hidden modules, or suspicious activity patterns, often correlating memory data with other artifacts from the disk or network.
- **Challenges in Memory Forensics**:
    - Memory forensics presents several challenges, such as ensuring data integrity in a live environment and dealing with the large size of memory dumps, which can complicate analysis. Additionally, encryption and advanced obfuscation techniques used by attackers make it difficult to interpret certain portions of memory. Analysts must stay up-to-date with current anti-forensic techniques that aim to hide or scramble malicious activity within memory.

By following these steps, forensic analysts can extract valuable information from a system's volatile memory, providing insight into active or recent activities that might not be preserved on disk.