ADAMA SCIENCE AND TECHNOLOGY UNIVERSITY

School of Electrical Engineering and Computing

Department of Software Engineering

Course: Digital Forensic

Individual Assignment

Student Name: Ameha Seyoum

ID: UGR/22559/13

Date: March 16, 2025

Submitted to: Dr. Dereje Regassa

Table of Contents

Answers to the Exercises:

1. Explain the difference between acquiring live data or acquiring a forensic image of a powered-down system. What are the complications and impacts of collecting live data versus creating a forensic image of a powered-down system's data?

Live Data Acquisition:

- Involves collecting volatile data from a running system, such as RAM contents, active network connections, and running processes.
- **Advantages:** Captures real-time activities, including malware behavior and encryption keys.
- **Disadvantages:** Alters system state, introduces risk of tampering, and requires specialized tools.

Forensic Imaging of a Powered-Down System:

- Involves creating a bit-by-bit copy of a storage device without modifying data.
- **Advantages:** Provides a legally defensible copy, prevents alteration, and maintains integrity.
- **Disadvantages:** Does not capture volatile memory data, running processes, or network activity.

Complications and Impacts:

- Live acquisition may be necessary for investigating active attacks but is more complex.
- A forensic image is more reliable in court but may lack critical evidence from active sessions.

2. Imagine an NTFS file system that was formatted with the cluster size specified as 8Kb(8192bytes). If a single-byte file was created, how many null bytes would be written to the sector? What would happen to the additional seven sectors in the cluster, and what might they contain?

Null Bytes Written to the Sector:

- NTFS allocates space in clusters (8KB = 8192 bytes).
- If a 1-byte file is created, the remaining **8191 bytes** in the cluster are filled with null (zero) bytes unless the system uses file compression.

Fate of the Additional Seven Sectors in the Cluster:

The remaining sectors may contain:

- **Slack Space:** Residual data from previously deleted files.
- **Unallocated Data:** Information that could be recovered by forensic tools.
- **Hidden Data:** If an attacker intentionally hides information in slack space.

3. Explain what a partition is and where hidden data could be placed intentionally by a technically apt individual.

Partition Definition:

- A partition is a logical division of a storage device, managed by a file system (e.g., NTFS, FAT32, EXT4).

Hidden Data Placement:

- **Hidden Partitions:** Creating an unallocated partition that is not visible to standard file explorers.
- **Slack Space:** Storing small amounts of hidden data in unused portions of allocated clusters.
- **Alternate Data Streams (ADS):** Hiding data within NTFS attributes without appearing in file listings.
- **Bad Sectors Marking:** Using low-level disk manipulation to store data in sectors marked as "bad."
- **Steganography in File System Metadata:** Embedding data within disk structures that remain unnoticed.

4. On an NTFS file system, there can be more than one attribute of a given type. Explain theoretically where someone can hide data for an executable file in a legitimate system configuration file using the behavior of the filesystem attributes.

- NTFS allows multiple attributes of a given type for a file.

Hiding Data in Attributes:

- **Alternate Data Streams (ADS):** Storing hidden executable content behind a legitimate file using file.txt:hidden.exe.
- **Extended Attributes:** Adding metadata-like information that may contain encoded data.
- **Security Descriptors:** Embedding hidden information within permission attributes.

Example:

- An attacker could store a malicious payload inside the ADS of a legitimate system file (config.sys) without modifying its visible size.

5. NTFS maintains at least two attributes with MACE(modified, accessed, created, and entry modified) times for every file and directory on the system. Explain the two attributes and describe the differences in how the timestamps on these attributes can be updated.

Two Main Attributes That Track Timestamps:

1. **Standard Information Attribute (SIA):**
    - Stores Modified, Accessed, Created, and Entry Modified times.
    - Gets updated automatically by system actions.
2. **File Name Attribute (FNA):**
    - Contains another timestamp set for directory entries.
    - Less frequently modified, can retain timestamps even if the SIA changes.

Difference in Timestamp Updates:

- Renaming a file updates the **FNA** but not necessarily the **SIA**.
- Some forensic tools compare SIA and FNA timestamps to detect tampering.

6. Can deleted files be recovered from EXT file systems? Explain some of the challenges for recovery.

Yes, but with Challenges:

EXT file systems use **journaling**, which makes file recovery difficult because metadata is overwritten quickly.

Key Challenges:

- **Metadata Overwrite:** Inodes (file descriptors) are cleared when files are deleted.
- **Fragmentation:** Large files may be spread across the disk, making reconstruction harder.
- **Journal Cleanup:** Data may be erased due to file system maintenance.

Possible Recovery Methods:

- ✓ Using forensic tools like **extundelete** and **Photorec**.
- ✓ Extracting data from unallocated space or journal records.

7. Explain why an attacker may use applications, such as WinRAR, to stage data for theft. What artifacts could an examiner look for in memory and virtual memory in order to determine if an attacker used WinRAR and derive the attacker's password?

Why Attackers Use WinRAR:

- Compressing stolen files into a single archive reduces size and detection risk.
- Password protection adds an extra layer of obfuscation.
- Splitting large files into multiple smaller parts hides them from monitoring tools.

Artifacts to Look for in Memory & Virtual Memory:

- **Running Processes:** Checking for WinRAR.exe execution.
- **Recently Opened Files:** Searching for compressed archives.
- **Memory Dump Analysis:** Extracting plaintext passwords cached in RAM.
- **Shellbag & Prefetch Files:** Identifying user activity related to compressed files.
- **Registry & Event Logs:** Tracking when WinRAR was executed and which files were accessed.

8. A single date or time on a system can be unreliable, given the many ways that they can be manipulated or even updated through the normal course of the operating system's functions. What type of analysis can be used to corroborate the accuracy of an event's timestamp? What other evidence might be identified from this technique?

Why a Single Timestamp is Unreliable:

❖ System functions, user actions, and malware can manipulate timestamps.

Techniques to Corroborate Timestamp Accuracy:

✓ **Timeline Analysis:** Cross-referencing file system logs, registry changes, and network logs.
✓ **Log Correlation:** Comparing timestamps from multiple sources like Windows Event Logs and application logs.
✓ **Hash Comparison:** Ensuring file integrity by checking cryptographic hashes.
✓ **Additional Evidence That Can Be Identified:**
✓ **File Manipulation Attempts:** Identifying mismatches in different timestamp records.
✓ **User Activity Traces:** Correlating login sessions with suspicious file modifications.
✓ **Malware Execution:** Linking changes in system timestamps with known attack patterns.

Additional Evidence That Can Be Identified:

✓ **File Manipulation Attempts:** Identifying mismatches in different timestamp records.
✓ **User Activity Traces:** Correlating login sessions with suspicious file modifications.
✓ **Malware Execution:** Linking changes in system timestamps with known attack patterns.