Disk Forensics

Disk Imaging

- Definition: Disk imaging is **the process of creating an exact, bit-by-bit copy of a storage device (like a hard drive or SSD) to capture all data, including hidden, deleted, and residual data in unallocated space**.
- Importance: Imaging **preserves the original evidence** while enabling **forensic analysis on the copy**, maintaining the integrity of the original data.
- Best Practice: Create a verified, write-protected image using a forensic tool, such as **FTK Imager or EnCase**, and calculate hash values (e.g., MD5, SHA-256) to ensure data integrity.

Filesystems

- Filesystems organize and store data on a disk, and understanding them helps investigators interpret data and locate evidence more effectively.
- Common Filesystems
    - **NTFS (New Technology File System)**: Used in **Windows**; supports security features like ACLs (access control lists), encryption, and journaling, which help in tracking file access, ownership, and modification.
    - **ext2/3/4 (Extended Filesystem)**: Common in **Linux**. Ext3 and ext4 support journaling, which logs file operations, making it easier to recover data after crashes or power failures.
    - **APFS (Apple File System)**: Used in **macOS**; includes advanced features like encryption, snapshots, and space sharing. Encryption and snapshots require specialized techniques to analyze but can reveal historical data changes.

Logs

- Purpose: Logs provide a **record of system, application, and user activity**, offering valuable insight into incidents.
- Key Log Types:
    - **Windows Event Logs**: Stored in .evtx format, these logs include:
        - Security Logs: Record login attempts, user access, and security changes.
        - System Logs: Track system-level events, including errors and warnings.
        - Application Logs: Log events from installed applications, useful for application-specific incidents.
    - **Unix System Logs**: Commonly stored in /var/log/, they include:
        - auth.log: Authentication attempts, including logins and SSH connections.
        - syslog: General system events, useful for tracking processes and system errors.
        - dmesg: Kernel-level messages, helpful for analyzing hardware and system startup issues.
    - Application Logs: Application-specific logs like web server logs (e.g., Apache, Nginx) and database logs track detailed user interactions, errors, and performance.

Data Recovery (Carving)

- Definition: **Carving is a method to retrieve deleted or fragmented files by identifying data patterns and reconstructing files without relying on file system metadata**.
- Process: Tools scan for specific file signatures (e.g., PDF, JPEG headers) to retrieve data that may have been deleted or partially overwritten.
- Value in Forensics: Carving enables recovery of remnants from unallocated space, which can yield critical evidence even after files have been deleted.

Forensic Tools

- **plaso / log2timeline**
  - Purpose: Plaso, which builds on log2timeline, **automates timeline creation by parsing multiple log types and system metadata, organizing events chronologically**.
  - Forensics Value: Useful for building a comprehensive event timeline, helping to identify sequences of user actions and system events leading up to and following an incident. Plaso is especially effective for correlating data across multiple sources.
- **FTK Imager**
  - Purpose: FTK Imager is **a free forensic tool primarily for creating disk images but also enables previewing and exporting evidence**.
  - Forensics Value: FTK Imager allows investigators to **create forensic disk images** in formats like E01 or raw, verify data integrity with hashing, and extract specific files or folders as needed.
- **EnCase**
  - Purpose: EnCase is **a commercial, industry-standard tool widely used in digital forensics for disk imaging, analysis, and evidence documentation**.
  - Forensics Value: EnCase enables in-depth disk analysis, including file system parsing, keyword searching, email analysis, and detailed reporting. Its comprehensive features and reliability make it widely accepted in legal settings and complex investigations.

Practical Application in Disk Forensics

- **Disk Imaging** captures **a bit-for-bit copy, preserving data integrity**.
- **Filesystem Knowledge** enables better interpretation of stored and deleted data.
- **Logs** provide a record of system, application, and user actions.
- **Data Recovery** through Carving allows recovery of deleted data for analysis.
- Tools like **Plaso, FTK Imager, and EnCase** streamline investigation, documentation, and reporting, enabling investigators to gather and interpret evidence effectively.

Summary

Together, these methods and tools form the core of disk forensics, helping forensic experts systematically uncover digital evidence and reconstruct event timelines accurately.