Lecture: Hard Disks and File Systems

1. Introduction

In digital forensics, understanding how data is stored, structured, and retrieved from storage devices is fundamental. Hard disks and file systems form the backbone of digital evidence collection and analysis. Investigators must understand how files are organized, how operating systems interact with storage, and how deleted or hidden data can be recovered for forensic purposes.

2. Objectives

By the end of this lecture, students will be able to:

- Explain the structure and working of hard disks.
- Describe various file systems (NTFS, FAT, EXT, etc.).
- Understand logical and physical disk structures.
- Identify sources of forensic evidence within disks and file systems.
- Analyze registry files for evidence.

3. Hard Disk Concepts

3.1 Definition

A Hard Disk Drive (HDD) is a non-volatile storage medium that retains data even when the power is off. It consists of spinning platters coated with magnetic material, read/write heads, and a controller for managing data access.

3.2 Structure

- Platters: Circular disks that store data magnetically.
- Tracks: Concentric circles on the platter.
- Sectors: Smallest physical storage units (usually 512 bytes or 4 KB).
- Clusters: Logical groupings of sectors used by the file system.
- Cylinders: Set of tracks aligned vertically across platters.

3.3 Logical Structure

The logical view is how the operating system perceives the disk:

- Partitions: Divisions of the disk (Primary, Extended, Logical).
- File System: Structure for organizing and managing files within a partition.

4. File Systems Overview

A file system defines how data is stored, retrieved, and managed on storage devices. It organizes data into files and directories and maintains metadata.

4.1 Common File Systems

1. FAT (File Allocation Table)
   - Used in older systems and removable drives.
   - Variants: FAT12, FAT16, FAT32.
   - Simple structure but limited file size (4 GB) and partition size.
2. NTFS (New Technology File System)
   - Default in modern Windows systems.
   - Supports large files, file permissions, encryption, and journaling.
   - Key structures: Master File Table (MFT), File Record Segments, and Metadata.
3. EXT (Extended File System)
   - Common in Linux: EXT2, EXT3, EXT4.
   - Supports journaling (EXT3/EXT4), large file sizes, and permissions.
4. HFS+ / APFS (Apple File Systems)
   - Used in macOS.
   - APFS supports snapshots and cloning.
5. exFAT
   - Used for flash drives and cross-platform storage.
   - Larger file support than FAT32.

5. File System Components in Forensics

5.1 Metadata

Stores attributes such as file name, creation date, modification time, permissions, and size.

5.2 Directory Structure

Hierarchical organization of files and folders. Deleted files may still be referenced here until overwritten.

5.3 Slack Space and Unallocated Space

- Slack space: Unused bytes within a cluster; may contain remnants of previous files.
- Unallocated space: Space not currently assigned to any file; can contain recoverable deleted data.

5.4 Journals

Used in journaling file systems to record pending operations; useful for reconstructing recent activities.

6. Hard Disk Forensics

6.1 Goals

- Recover deleted files.
- Identify hidden or encrypted partitions.
- Extract timestamps and metadata.
- Ensure data integrity (hash verification).

6.2 Process

1. Imaging: Create a bit-by-bit copy of the disk using tools (FTK Imager, EnCase, dd).
2. Analysis: Examine partitions, files, and hidden data using forensic tools.
3. Recovery: Use carving and signature analysis to retrieve deleted files.
4. Validation: Compare hash values before and after analysis.

6.3 Tools

- Autopsy/The Sleuth Kit
- FTK Imager

- EnCase
- X-Ways Forensics

7. Windows Registry Analysis

The Windows Registry is a central database that stores system and application settings. It is a rich source of forensic evidence.

7.1 Registry Hives

- SAM – User account info and passwords.
- SYSTEM – Hardware configuration.
- SOFTWARE – Installed applications.
- SECURITY – Security policies.
- NTUSER.DAT – User-specific preferences.

7.2 Evidence in Registry

- User login times.
- Installed programs.
- USB device history.
- Network information.
- Recent documents and searches.

7.3 Tools for Analysis

- RegRipper
- Registry Explorer
- Autopsy (Registry Plugin)

8. Forensic Challenges

- Data Overwriting: Deleted data may be overwritten by new files.
- Encryption and Compression: May obscure يحجب data visibility.
- Anti-Forensics: Use of wiping tools or hidden partitions.
- SSD Wear-Leveling: Makes recovery unpredictable.

9. Conclusion

Understanding hard disks and file systems is crucial in digital forensics. Investigators rely on this knowledge to recover data, analyze evidence, and present findings in a legally admissible manner. Mastery of partition structures, file allocation mechanisms, and registry analysis allows for accurate reconstruction of user activities and system events.

10. Summary Points

- Hard disks store data magnetically using structured layers.
- File systems (FAT, NTFS, EXT) define data organization.
- Forensic analysis includes imaging, examination, and recovery.
- Windows Registry provides vital artifacts for user activity.
- Tools like Autopsy, EnCase, and RegRipper are essential.