Lecture: Chapter 2 – Essential Technical Concepts

Practical Digital Forensics (2023)

Authors: A. Bhardwaj & K. Kaushik
Purpose: To provide a foundational understanding of computing concepts essential for digital forensics investigations.

1. Introduction

A digital forensic investigation requires a strong understanding of fundamental computing concepts. Forensic examiners must know how computers store, process, and represent data, as well as how digital files are structured and how storage media work. This knowledge ensures that digital evidence is acquired, preserved, and analyzed accurately without data loss or tampering.

This chapter explores key technical areas:

- Number systems and encoding
- File structure and metadata
- Hashing for evidence verification
- System memory and storage
- File systems and slack space
- Cloud computing environments
- IP addressing basics

These topics form the technical foundation necessary for forensic professionals to locate, recover, and analyze digital evidence in a forensically sound manner.

2. Number Systems in Computing

Computers represent and manipulate data using different number systems. Understanding these systems is essential for interpreting raw data, file headers, and memory addresses.

2.1 Decimal (Base-10)

- The decimal system is the one we use in daily life.
- It contains ten digits: 0–9.
- Each position represents a power of 10.

  - Example: 4,567 = (4 × 10^3) + (5 × 10^2) + (6 × 10^1) + (7 × 10)

2.2 Binary (Base-2)

- Computers operate in binary, using only **0** and **1**.
- Each binary digit is called a **bit**; 8 bits = 1 byte.
- Binary values represent electrical signals: 0 (off) and 1 (on).
  - Example: 1101 = (1 × 8) + (1 × 4) + (0 × 2) + (1 × 1) = **13**

Understanding binary helps forensic analysts interpret raw data and memory dumps.

2.3 Hexadecimal (Base-16)

- Used to simplify binary representation.
- Contains 16 symbols: 0–9 and A–F.
- Commonly used in memory addresses, file signatures, and hash values.
  - Example: **0x1A** = (1 × 16) + (10) = **26**

Hexadecimal is a more compact مضغوط form of binary and frequently appears in forensic analysis tools and raw data.

2.4 Base64 Encoding

- Represents binary data as ASCII text.
- Used for transmitting binary files (e.g., images, email attachments) over text-based protocols.
- Example: The phrase "Many hands make light work" encoded in Base64 becomes TWFueSBoYW5kcyBtYWtlIGxpZ2h0IHdvcmsu.

Forensic analysts must recognize Base64-encoded data to decode hidden or transferred content.

3. Character Encoding Schemas

Computers use encoding schemes to convert binary data into readable text.

3.1 ASCII (American Standard Code for Information Interchange)

- Uses 7 bits to represent 128 characters (letters, digits, punctuation).
- Example: Letter **A** = 65 in decimal = 01000001 in binary.
- Limitation: Cannot represent all international characters.

3.2 Unicode

- Global standard for encoding text across all languages.
- Common formats:
    - **UTF-8**: Variable-length encoding; backward-compatible with ASCII.
    - **UTF-16** and **UTF-32**: Fixed-length encodings for broader symbol sets.
- Essential in forensic investigations involving multilingual متعددة اللغات data.

4. File Carving and File Structures

4.1 File Carving نحت الفايل

- **Definition**: Recovering files based on content rather than file system metadata.
- Used when file tables are missing, corrupted, or deleted.
- Identifies files using **headers** (beginning bytes) and **footers** (ending bytes).
- Example: A JPEG file starts with FFD8 and ends with FFD9.

Forensic use: Recover deleted images or documents from unallocated space.

4.2 File Structure

A typical file consists of:

- **Header**: Identifies file type (magic number).
- **Body**: The actual data.
- **Footer**: Indicates end of file.

Note: File extensions (e.g., .docx) can be changed to mislead investigatorsتضليل المحققين , but headers reveal true type.

Forensic tools like **Hex Editors** (wxHexEditor, PSPad, Free Hex Editor Neo) allow inspection تفتيشof file headers.

5. Digital File Metadata

5.1 Definition

Metadata is **data about data** — additional information stored with a file describing its properties.

5.2 Common Metadata Elements

- Author name
- Creation and modification dates
- Device name or ID
- GPS coordinates (for images)
- Software used
- File size and type

5.3 Importance in Forensics

Metadata reveals:

- When and where a file was created or modified.
- Which device or user created it.
- Possible tampering (e.g., altered timestamps).

Tools for metadata analysis:

- **ExifTool**
- **MediaInfo**
- **XnView**
- **GIMP**
- **PDF Metadata Editor**

Forensic analysts often extract metadata to reconstruct event timelines and user actions.

6. Timestamp Analysis

Files contain three major timestamps:

- **Created** – when the file was first generated.
- **Modified** – last change to the content.
- **Accessed** – last time it was opened or viewed.

By comparing timestamps, investigators can build activity timelines. Some suspects may alter timestamps; forensic tools can detect inconsistencies and reveal tampering.

7. Hash Analysis

7.1 Definition

A **hash** is a unique, fixed-length string derived from file content using a cryptographic algorithm. Used to verify **integrity** and **authenticity** of digital evidence.

7.2 Common Algorithms

- **MD5** (Message Digest)(128-bit)
- **SHA-1** (Secure Hash Algorithm)(160-bit)
- **SHA-256** (256-bit)

7.3 Applications in Forensics

- Validate evidence before and after acquisition.
- Identify duplicate or known files using hash databases.
- Detect file tampering or corruption.

7.4 Tools

- **HashMyFiles** (NirSoft)
- **Febooti Hash & CRC**
- **Windows PowerShell**:
- Get-FileHash filename -Algorithm SHA256

Hashes are like **digital fingerprints**; if the file changes, its hash changes.

8. System Memory

8.1 Types

1. **Volatile Memory** – Data lost when power is off
   - Example: **RAM (Random Access Memory)**
2. **Non-Volatile Memory** – Data retained after power-off
   - Examples: **ROM**, **Hard Drives**, **Flash Drives**
   -

8.2 RAM

- Temporarily stores data of running programs.
- Contains:
  - Active processes
  - Browser history
  - Passwords
  - Decrypted data
- Crucial ضروري for live forensic analysis (e.g., malware running in memory).

Types of RAM:

- **D(Dynamic)RAM** – requires constant refresh
- **S(Static)RAM** – faster, used in CPU cache

8.3 ROM

- Stores firmware (e.g., BIOS).
- Non-editable during normal operations.
- Types:
  - **PROM** – programmable once
  - **EPROM** – erasable with UV (ultraviolet) light
  - **EEPROM** – erasable electronically

9. Secondary Storage

9.1 Hard Disk Drives (HDD)

- Magnetic storage with spinning platters.
- Data stored in **tracks**, **sectors**, and **clusters**.
- **Slack space**: unused area in clusters that may contain remnants of deleted files.

9.2 Solid State Drives (SSD)

- Flash-based, faster, no moving parts.

- Limited write cycles but improving over time.
- Used in modern laptops and forensic workstations.

9.3 Backup Storage

- External drives, USBs, optical discs, cloud storage.
- May contain older versions or backups of incriminating data.

10. File Systems

Define how data is stored and retrieved on storage media.

File System	Platform	Features
FAT32	Windows, portable devices	Simple, lacks security
NTFS	Windows default	Supports permissions, journaling
EXT4	Linux	Stable, supports large volumes
HFS+/APFS	macOS	Efficient, supports snapshots

Understanding file systems is vital for identifying deleted files, slack space, and hidden data.

11. Slack Space

- **Definition:** The unused portion within a file cluster.
- **Significance:** May contain fragments of previous files.
- **Use in Forensics:** Recover remnants بقاياof deleted data.
- **Tool:** Disk Slack Checker (Karen’s Power Tools).

12. Cloud Computing Environments

Forensics must adapt to cloud-based storage and services.

12.1 Service Models

1. **SaaS (Software as a Service)** – e.g., Gmail, Office 365
2. **PaaS (Platform as a Service)** – e.g., Azure App Services

3. **IaaS (Infrastructure as a Service)** – e.g., AWS EC2

Challenges:

- Jurisdiction issues
- Data ownership
- Remote acquisition

13. Networking Concepts

IP Addressing

- Unique identifier for network devices.
- **IPv4** – 32-bit (e.g., 192.168.1.1)
- **IPv6** – 128-bit, supports more devices.

Forensic significance:

- Identify source/destination of communications
- Track network-based crimes

14. Recommended Tools

Purpose	Tools
File Carving	Scalpel, PhotoRec
Metadata Analysis	ExifTool, MediaInfo
Hashing	HashMyFiles, PowerShell
Memory Acquisition	FTK Imager, Magnet RAM Capture
File System Analysis	Autopsy, Sleuth Kit