

Foundational Concepts of Digital Evidence

MSCS630: Cybercrime Investigation and Digital Evidence

Dr. Mouatez Karbab



أكاديمية جوعان بن جاسم للدراسات الدفاعية
Joaan Bin Jassim Academy for Defence Studies

October 2, 2026



Outline

- 1 The Order of Volatility
- 2 The Three States of Digital Data
- 3 File Structure: Data, Metadata, and Signatures
- 4 Modern and Emerging Evidence Sources



Introduction to Foundational Concepts of Digital Evidence I

Chapter Objectives

- Put evidence sources in the order of volatility.
- Explain why the most volatile data is collected first.
- Tell data in transit, in use and at rest apart.
- Name the collection method for each state of data.
- Separate a file's content from its metadata.
- Read MACB timestamps on common file systems.
- Identify a file by its signature, not its extension.
- List where smart-device, cloud and disappearing-message evidence survives.

Why This Matters

- Knowing the nature of digital evidence helps you find the right information.
- It also prevents you from accidentally destroying it.





Volatility and Live Response I

Definition: Volatility

- How easily data can be lost or changed.
- Volatile data can vanish at power-off or on a state change [4].
- Volatility decides the order in which you collect data.
- Especially during a *live response*: investigating a computer still turned on.

The Rule

- **Collect the most volatile evidence first.**
- Ignoring the order can lose important data forever.



Why Pulling the Plug Destroys Evidence I

- First instinct at a scene: pull the power cord to save the disk.
- That one action can destroy a large amount of information.
- A running computer changes state every second.
- **Random Access Memory (RAM):** short-term memory of what the system does now.
- RAM holds running programs, network connections and decrypted data.
- All of it disappears when the power is turned off.



Real-World Scenario: The Hasty Shutdown I

Real-World Scenario: The Hasty Shutdown

- Company data leak; first responder finds the affected computer.
- Responder cuts the power to take the machine to the lab.
- At that moment all data in RAM is erased.
- Lost: *fileless malware*, software that runs only in memory, never saved to disk.
- Lost: the active connection to the attacker's server.
- Lost: a list of other affected computers on the network.
- Disk analysis later shows only a normal operating system.
- The malware was designed to save no files to disk.
- Volatile memory not collected first: a solvable case became unsolvable.
- Evidence to identify the attacker and the attack's scale is gone.
- With an encrypted disk, power-off also discards the only unlocked key copy.



Ordering Evidence from Most to Least Volatile I

- Order of Volatility: a clear guide for collecting evidence.
- Data ordered from most temporary to least temporary.
- Collect first whatever would be lost first [6].
- Seven tiers: typical survival time and collection method for each.



Terms Used in the Volatility Tiers I

- **Process table:** lists all running programs.
- **Address Resolution Protocol (ARP) cache:** maps Internet Protocol (IP) addresses to physical device addresses.
- **Routing table:** shows how the computer sends network traffic.
- **RAM:** richest volatile source on a live system; treated below as *data in use*.
- **Swap space / pagefile:** disk area for memory not used often.
- Swap sits on disk but is overwritten so often it counts as volatile.
- **Disk:** main source of *data at rest*.
- **Dead-box forensics:** analysis of a computer that is turned off.
- **Unallocated space:** disk area used by no active file; may hold old deleted file parts.
- Central processing unit (CPU) registers and cache (tier 1) change too fast to collect directly.
- **Network-attached storage (NAS):** storage device connected to a network (tier 7).



The Order of Volatility I

	Tier	Examples	Typical lifetime	How it is collected
1	CPU registers and cache	Values the processor is working on now	Nanoseconds	Not collected directly in practice
2	Network and process state	Routing table, ARP cache, process table, kernel statistics	Seconds to minutes	Trusted live-response commands run from external media
3	System memory (RAM)	Running programs, open connections, decrypted data, encryption keys	Until power-off	Memory acquisition tool writing a memory image to external media
4	Swap space and temporary files	Pagefile, swap partition, program temporary files	Minutes to days, overwritten in use	From the disk image, or copied live
5	Disk (HDD, SSD)	User files, system files, logs, unallocated space	Until overwritten or trimmed	Forensic imaging through a write-blocker
6	Remotely logged data	Central log server, firewall logs, cloud activity logs	Set by retention policy	Export from the log server, or legal process to the provider
7	Archived media and backups	Backup tapes, external drives, NAS, cloud backups	Months to years	Imaging or copying the backup media

Table: The order of volatility. From most to least volatile, adapted from Request for Comments (RFC) 3227

[4]. The RFC places memory in the same tier as network and process state, and lists physical configuration and



The Order of Volatility II

network topology between remote logs and archival media. Lifetimes are typical, not guaranteed: a busy system overwrites swap within minutes, and a retention policy can delete remote logs within days.

Table Analysis: Reading the Volatility Tiers I

- Tiers 1 to 4 are lost at power-off or within minutes.
- Tier 1 is not collected in practice; tier 2 needs trusted commands from external media.
- Tier 3 (RAM) is captured as a memory image before shutdown.
- Tier 5 onward survives power-off and is imaged or exported.
- Lifetimes are typical: busy systems overwrite swap in minutes.
- Retention policies can delete remote logs within days.



Hands-On: Planning a Live Response Order I

Objective

- Turn the volatility tiers into a collection plan for a running server.

Prerequisites

- Table 1 and the hasty shutdown scenario.

Steps

- 1 List every evidence source on the running server in the scenario.
- 2 Assign each source to its tier in Table 1.
- 3 Order the sources from tier 2 to tier 7.
- 4 Write the collection method next to each source.
- 5 Mark the point at which power-off becomes acceptable.



Hands-On: Planning a Live Response Order II

Expected Outcome

- Network and process state first, memory image next, disk image after shutdown.
- Remote logs and backups requested in parallel, before retention deletes them.

Common Pitfalls

- Imaging the disk before capturing RAM.
- Forgetting that encryption keys live only in memory.



Section 1: Assessment (1/3) I

Question 1

The core rule of the order of volatility?

- A. Collect the largest evidence source first.
- B. Collect the most volatile evidence first.
- C. Collect disk evidence before memory.
- D. Collect remote logs before local data.



Section 1: Assessment (1/3) - Answer I

Question 1

The core rule of the order of volatility?

- A. Collect the largest evidence source first.
- B. Collect the most volatile evidence first. (✓)
- C. Collect disk evidence before memory.
- D. Collect remote logs before local data.

Explanation:

- Collect first whatever would be lost first [6].



Section 1: Assessment (2/3) I

Question 2

Why did the hasty shutdown make the case unsolvable?

- A. The disk was damaged by the power cut.
- B. The write-blocker was missing.
- C. The fileless malware existed only in RAM.
- D. The remote logs were deleted.



Section 1: Assessment (2/3) - Answer I

Question 2

Why did the hasty shutdown make the case unsolvable?

- A. The disk was damaged by the power cut.
- B. The write-blocker was missing.
- C. The fileless malware existed only in RAM. (✓)
- D. The remote logs were deleted.

Explanation:

- Malware, attacker connection and victim list were all in memory.
- The disk showed only a normal operating system.



Section 1: Assessment (3/3) I

Question 3

Why does swap space count as volatile though it sits on disk?

- A. It is erased at every boot by design.
- B. It is overwritten very often.
- C. It is stored in CPU cache.
- D. It is never written to disk.



Section 1: Assessment (3/3) - Answer I

Question 3

Why does swap space count as volatile though it sits on disk?

- A. It is erased at every boot by design.
- B. It is overwritten very often. (✓)
- C. It is stored in CPU cache.
- D. It is never written to disk.

Explanation:

- A busy system overwrites swap within minutes (tier 4).



Outline

- 1 The Order of Volatility
- 2 The Three States of Digital Data
- 3 File Structure: Data, Metadata, and Signatures
- 4 Modern and Emerging Evidence Sources



Where Data Is and What State It Is In I

- The order of volatility says *when* to collect each kind of data.
- To know *how*, know where the data is and its state.
- All digital data is in one of three states.
- **Data in transit, data in use, data at rest.**
- Each state requires different tools and collection methods.
- Data moves between states as it is loaded, saved and sent.
- In transit: network tap or SPAN port; in use: memory image; at rest: forensic image.



Data in Transit: Definition and Characteristics I

Definition: Data in Transit

- Data currently moving from one place to another.
- Usually over a network: a company local area network (LAN) or the internet.
- Most important quality: it is temporary.
- Not captured while moving means lost forever.
- Like a phone call: you must listen at that exact moment.



Data in Transit: Examples and Packet Capture I

Examples

- Packets carrying Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) payloads.
- Web requests over Hypertext Transfer Protocol (HTTP) or its encrypted form HTTPS.
- Voice over IP (VoIP) conversations.
- Application programming interface (API) calls between microservices.
- File transfers.
- **Packet:** small unit of data sent over a network.

Data in Transit: Examples and Packet Capture II

Packet Capture (Packet Sniffing)

- Network card in *promiscuous mode*: captures all traffic passing through it.
- Not only traffic sent to the investigator's computer.
- On a switched network, place the card where traffic flows.
- Use a Switched Port Analyzer (SPAN) mirror port or an inline network tap.
- Promiscuous mode alone sees little more than broadcast traffic [18].
- Standard tools: **Wireshark** (graphical) and **tcpdump** (command line) [7].



- ```
http.request.method == "POST"
```

- Shows only packets of HTTP POST requests.
- POST: method browsers use to send form data to a server.
- Works only for plain HTTP.
- HTTPS shows connection metadata, not form contents, without session keys.



# Data in Use: Definition and Characteristics I

## Definition: Data in Use

- Data the CPU is processing or that is stored in RAM.
- The operating system and programs constantly create, change and read it.
- Main goal of a *live acquisition*: collecting data from a running computer.
- Shows the computer's current state.
- Like data in transit, very volatile; lost at power-off.



# Data in Use: Examples and Memory Imaging I

## Examples

- List of running processes.
- Open documents not yet saved to disk.
- Active chat sessions and clipboard contents.
- Most important: *cryptographic keys* that unlock an encrypted disk.

## Collection: The Memory Image

- **Memory image:** exact bit-for-bit copy of physical memory.
- Machine must stay on; captured during live response.
- Small trusted tool run from external media.
- Windows: WinPmem or Magnet RAM Capture.
- Linux: AVML or LiME [15].
- Tool writes one memory-image file, hashed as soon as written.
- Live response is covered in detail in Chapter 6.



# Data at Rest: Definition and Acquisition I

## Definition: Data at Rest

- Data saved on a storage device, like a hard drive.
- Remains on the device without power.
- The most stable type of data.

## Examples

- Documents, photos, videos, database files, emails.
- Operating system files and program files.
- Hard disk drives (HDDs), solid-state drives (SSDs), USB flash drives, memory cards, backups.



# Data at Rest: Definition and Acquisition II

## Acquisition

- Unchanged at power-off: collected carefully and repeatedly, not urgently.
- **Forensic imaging:** exact bit-for-bit copy of the whole device.
- Taken through a write-blocker; the original is never altered [5].
- Post-mortem acquisition is covered in Chapter 6.



# Hands-On: Filtering Form Submissions in a Capture I

## Objective

- Isolate HTTP form submissions in a recorded packet capture.

## Prerequisites

- Wireshark installed; any capture containing plain HTTP traffic.

## Steps

- 1 Open the recorded capture in Wireshark.
- 2 Enter the display filter below and apply it.
- 3 Open one matching packet and read the form fields.
- 4 Repeat on HTTPS traffic and note what is visible.

```
http.request.method == "POST"
```





## Section 2: Assessment (1/3) I

### Question 1

On a switched network, what does promiscuous mode alone capture?

- A. All traffic on every switch port.
- B. Little more than broadcast traffic.
- C. Only encrypted traffic.
- D. Only traffic from the default gateway.



## Section 2: Assessment (1/3) - Answer I

### Question 1

On a switched network, what does promiscuous mode alone capture?

- A. All traffic on every switch port.
- B. Little more than broadcast traffic. (✓)
- C. Only encrypted traffic.
- D. Only traffic from the default gateway.

### Explanation:

- A SPAN port or network tap is needed [18].



## Section 2: Assessment (2/3) I

## Question 2

Which item of data in use is the most important to capture?

- A. Clipboard contents.
- B. Cryptographic keys for an encrypted disk.
- C. The list of installed programs.
- D. The desktop wallpaper.



## Section 2: Assessment (2/3) - Answer I

### Question 2

Which item of data in use is the most important to capture?

- A. Clipboard contents.
- B. Cryptographic keys for an encrypted disk. (✓)
- C. The list of installed programs.
- D. The desktop wallpaper.

### Explanation:

- Keys exist only in memory; without them the disk may stay locked.



## Section 2: Assessment (3/3) I

### Question 3

The standard acquisition method for data at rest?

- A. Packet capture on a SPAN port.
- B. A memory image from external media.
- C. Forensic imaging through a write-blocker.
- D. Copying user folders with the file manager.



## Section 2: Assessment (3/3) - Answer I

### Question 3

The standard acquisition method for data at rest?

- A. Packet capture on a SPAN port.
- B. A memory image from external media.
- C. Forensic imaging through a write-blocker. (✓)
- D. Copying user folders with the file manager.

### Explanation:

- Bit-for-bit copy; original never altered [5].



# Outline

- 1 The Order of Volatility
- 2 The Three States of Digital Data
- 3 File Structure: Data, Metadata, and Signatures**
- 4 Modern and Emerging Evidence Sources



# Files Carry Layers of Information I

- Most evidence at rest is stored as files.
- A file is more than what you see when you open it.
- Every file has several layers useful to an investigation.
- Key distinction: the content (data) versus information *about* the file (metadata).

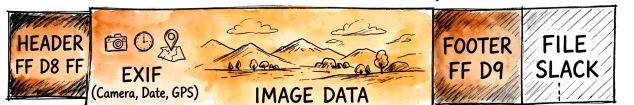




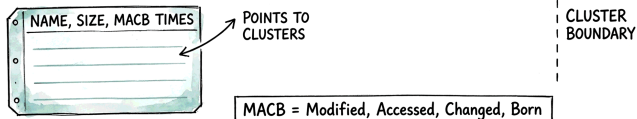
# Metadata Inside and Outside a JPEG File I

- Inside the file: header signature, Exchangeable Image File Format (EXIF) block, footer.
- After the footer: file slack up to the cluster boundary.
- In the file system record: name, size and MACB times, pointing to the clusters.

## 1. INSIDE THE FILE (The Bytes on Disk)



## 2. OUTSIDE THE FILE (The File System Record)



The signature and EXIF metadata travel inside the file.

Name and MACB times are kept by the file system, outside the file.





# MACB Timestamps Across Three File Systems I

|   | Meaning                      | NTFS (\$SI)          | ext4                  | APFS     | Normally updated by                          |
|---|------------------------------|----------------------|-----------------------|----------|----------------------------------------------|
| M | Content last modified        | Modified             | mtime                 | Modified | A write to the file's content                |
| A | Content last read            | Accessed             | atime                 | Accessed | A read, subject to the last-access policy    |
| C | Metadata record last changed | \$MFT entry modified | ctime (inode change)  | Changed  | A rename, permission change or content write |
| B | Created on this volume       | Created              | crtime, shown by stat | Created  | File creation; a copy gets a new B time      |

**Table: MACB timestamps across three file systems.** NTFS times are those of the \$STANDARD\_INFORMATION (\$SI) attribute, whose record lives in the Master File Table (MFT); APFS field names follow the Apple File System Reference [1]. The same letter can name a different event on each file system; on ext4 the C time is the inode change time, not a creation time. Last-access updates are often delayed or switched off for performance (`relatime` on Linux [17], `NtfsDisableLastAccessUpdate` on Windows [12]), so check the system's setting before relying on an A time.

# Table Analysis: Reading MACB Times I

- NTFS times come from the \$STANDARD\_INFORMATION (\$SI) attribute in the Master File Table (MFT).
- APFS field names follow the Apple File System Reference [1].
- The same letter can name a different event per file system.
- On ext4, C is the inode change time, not creation.
- A copy gets a new B time.
- Last-access updates are often delayed or off for performance.
- Linux: `relatime` [17].
- Windows: `NtfsDisableLastAccessUpdate` [12].
- Check the system's setting before relying on an A time.





# Practical Demo: Extracting GPS with ExifTool I

- **ExifTool:** command-line tool to read, write and edit metadata in many file types.
- Get latitude and longitude from a photo [9]:

```
exiftool -gpslatitude -gpslongitude image.jpg
```

## Limits

- Coordinates place the device that took the photo, not necessarily the suspect.
- EXIF can be edited; ExifTool itself can write it.
- Corroborate before relying on it.



# File Signatures (Magic Numbers) I

- Extensions (.jpg, .pdf, .docx) are just part of the name.
- A user can easily change them to hide what a file is.
- Correct identification: the **file signature**, or *magic number*.
- Specific byte sequence at the start (header), sometimes the end (footer).
- The sequence identifies the file's format.
- Forensic tools search for signatures, even when the extension is wrong.
- Three common examples follow [11].



# Common File Signatures I

| File type          | Header (hex) | As text         | Footer (hex)                     |
|--------------------|--------------|-----------------|----------------------------------|
| JPEG image         | FF D8 FF     | (not printable) | FF D9                            |
| PDF document       | 25 50 44 46  | %PDF            | ends with %%EOF (25 25 45 4F 46) |
| Windows executable | 4D 5A        | MZ              | none                             |

**Table: Common file signatures.** A JPEG header continues with a fourth byte that names the variant, commonly E0 for the JPEG File Interchange Format (JFIF) or E1 for EXIF, so a carver matches on the first three bytes only. The text column shows the header bytes as American Standard Code for Information Interchange (ASCII) characters where they are printable.



# Table Analysis: Signature Mismatch I

- JPEG's fourth header byte names the variant: E0 (JFIF) or E1 (EXIF).
- A carver therefore matches JPEG on the first three bytes only.
- PDF and executable headers are readable as ASCII.

## Warning Sign

- Extension does not match signature: a warning sign.
- It can mean a user tried to hide the file.



# The Concept of Data Carving I

- Deleting a file usually removes only its pointer.
- **Pointer:** the file-system part that locates the file.
- The space is marked as unallocated (defined in Section 1).
- On a hard disk the data stays until a new file overwrites it.
- **Data carving:** recovering files from unallocated space by known signatures [8].

## Solid-State Drives

- The window is short on SSDs.
- The OS sends TRIM for freed blocks; the drive erases them in the background.
- Carving an SSD often recovers little [3].

## How a Carver Works

- 1 Scan raw data for a header from Table 3.
- 2 Copy from there until the matching footer or a size limit.
- 3 Recovers files even when all file-system metadata is gone.



# The Concept of Data Carving II

- Widely used carvers: **Foremost, Scalpel, PhotoRec.**



# Illustrative Case: A Recovered Planning Document I

## Illustrative Case: A Recovered Planning Document

- Homicide investigation; examiners recover a deleted spreadsheet.
- It sets out an attack plan weeks before the attack.
- Metadata ties it to the suspect's user account.
- Metadata dates it before the crime.
- Prosecutors use it to argue premeditation.

## Lesson for the Examiner

- One recovered document, dated and attributable, can outweigh any volume of undated material.





# Hands-On: Checking a File Signature Against Its Extension II

## Expected Outcome

- ff d8 ff, 25 50 44 46 and 4d 5a headers.
- The renamed file is flagged as a mismatch.

## Common Pitfalls

- Matching on all four JPEG bytes and missing EXIF variants.
- Trusting the operating system's file-type icon.



# Section 3: Assessment (1/3) I

## Question 1

On ext4, what does the C time record?

- A. File creation.
- B. Inode (metadata) change.
- C. Last content read.
- D. Last copy to another volume.



# Section 3: Assessment (1/3) - Answer I

## Question 1

On ext4, what does the C time record?

- A. File creation.
- B. Inode (metadata) change. (✓)
- C. Last content read.
- D. Last copy to another volume.

## Explanation:

- The same letter names different events per file system [5].



# Section 3: Assessment (2/3) I

## Question 2

The correct way to identify a file's real type?

- A. Its extension.
- B. Its icon.
- C. Its header signature.
- D. Its size.



## Section 3: Assessment (2/3) - Answer I

### Question 2

The correct way to identify a file's real type?

- A. Its extension.
- B. Its icon.
- C. Its header signature. (✓)
- D. Its size.

### Explanation:

- Extensions are part of the name and easy to change [11].



# Section 3: Assessment (3/3) I

## Question 3

Why does carving an SSD often recover little?

- A. SSDs have no unallocated space.
- B. TRIM lets the drive erase freed blocks in the background.
- C. SSD files carry no signatures.
- D. Carvers cannot read flash memory.



## Section 3: Assessment (3/3) - Answer I

### Question 3

Why does carving an SSD often recover little?

- A. SSDs have no unallocated space.
- B. TRIM lets the drive erase freed blocks in the background. (✓)
- C. SSD files carry no signatures.
- D. Carvers cannot read flash memory.

### Explanation:

- Freed blocks are erased soon after deletion [3].



# Outline

- 1 The Order of Volatility
- 2 The Three States of Digital Data
- 3 File Structure: Data, Metadata, and Signatures
- 4 Modern and Emerging Evidence Sources



# Evidence Beyond Computers and Servers I

- States of data and file structures apply wherever data is stored.
- Digital evidence is no longer only on computers and servers.
- Connected devices and online services add new places to find evidence.



# IoT Devices as Evidence Sources I

## Definition: Internet of Things (IoT)

- Network of physical devices with sensors and software.
- They connect to the internet to send and receive data.
- Each device can be a source of digital evidence.

## Examples

- Smart speakers: voice commands and queries.
- Smart watches, fitness trackers: location, steps, heart rate.
- Smart home hubs, thermostats: occupancy, temperature changes.
- Vehicle infotainment: GPS routes, phone connections.
- Home security cameras: video stored locally or in the cloud.



# IoT Forensic Challenges and Opportunities I

## Challenges

- Non-standard file systems and data formats.
- Small amounts of volatile storage.
- Most important data often sent to the cloud.
- The device alone may not give a complete picture [14].

## Opportunities

- Combined device data builds a detailed timeline.
- Movements, conversations and daily routines.
- Can support or contradict an alibi.
- Only once sensor accuracy and the device's user are established.



# Cloud Storage as an Evidence Source I

- More user data now lives in the cloud, not on local devices.
- Google Drive, Dropbox, iCloud, Microsoft OneDrive.
- Evidence may persist on provider servers after the user deletes it locally [10].
- Obtaining it requires legal process on the provider, such as a warrant.
- That takes time and may involve several countries' laws.



أكاديمية جوعان بن جاسم للدراسات الدفاعية  
Joosin Bin Jassem Academy for Defence Studies

- 

# Investigating Ephemeral Messaging II

## File-Based Encryption

- On such phones unallocated space is rarely productive.
- iPhone: each file has its own key, wrapped in file metadata [2].
- Once that metadata is gone, encrypted remnants cannot be decrypted.



# Hands-On: Mapping Remnants of a Disappearing Message I

## Objective

- List every place a deleted ephemeral message might still survive.

## Prerequisites

- The remnant list and the file-based encryption caveat from this section.

## Steps

- 1 Take a scenario: a threat sent by Snapchat between two phones.
- 2 List the sender-side remnant locations.
- 3 List the recipient-side locations, including screenshots.
- 4 Add cloud backups and the provider's servers.
- 5 For each, note the legal process or acquisition it needs.

# Hands-On: Mapping Remnants of a Disappearing Message II

## Expected Outcome

- A ranked list: other device, backups, database and log, notifications.

## Common Pitfalls

- Planning to carve unallocated space on an encrypted phone.
- Ignoring the other party's device.



# Section 4: Assessment (1/3) I

## Question 1

Why may analysing only an IoT device give an incomplete picture?

- A. IoT devices never store data.
- B. They often send their most important data to the cloud.
- C. Their data is always encrypted.
- D. They cannot be imaged.



## Section 4: Assessment (1/3) - Answer I

## Question 1

## Why may analysing only an IoT device give an incomplete picture?

- A. IoT devices never store data.
- B. They often send their most important data to the cloud. (✓)
- C. Their data is always encrypted.
- D. They cannot be imaged.

Explanation:

- Small local storage, data held by the cloud service [14].



## Section 4: Assessment (2/3) I

### Question 2

Where can deleted messages survive inside the messaging app?

- A. Only in the app's icon cache.
- B. In the database's free pages and write-ahead log.
- C. In the CPU registers.
- D. Nowhere; deletion is immediate.



## Section 4: Assessment (2/3) - Answer I

## Question 2

## Where can deleted messages survive inside the messaging app?

- A. Only in the app's icon cache.
- B. In the database's free pages and write-ahead log. (✓)
- C. In the CPU registers.
- D. Nowhere; deletion is immediate.

Explanation:

- The log holds recent changes before they merge [16].



# Section 4: Assessment (3/3) I

## Question 3

Why is carving rarely productive on an iPhone?

- A. iPhones use magnetic storage.
- B. Each file has its own key; remnants cannot be decrypted once metadata is gone.
- C. iPhones have no unallocated space.
- D. Apple forbids forensic tools.



## Section 4: Assessment (3/3) - Answer I

### Question 3

Why is carving rarely productive on an iPhone?

- A. iPhones use magnetic storage.
- B. Each file has its own key; remnants cannot be decrypted once metadata is gone. (✓)
- C. iPhones have no unallocated space.
- D. Apple forbids forensic tools.

### Explanation:

- File-based encryption wraps each key in the file's metadata [2].



# Conclusion: Key Takeaways I

- **Volatility:** decides what to collect first.
- **Three states:** in transit, in use, at rest decide how to collect it.
- **Files:** metadata and signature often say more than content.
- **Emerging sources:** smart devices, cloud accounts, disappearing-message apps widen the search.
- Copies and remnants of the same data often survive somewhere else.

## Next Step

Apply these concepts to acquiring evidence from live and powered-off systems.



## References I

- [1] Apple Inc.  
Apple file system reference, 2020.
- [2] Apple Inc.  
*Apple Platform Security*, 9 2022.  
Published periodically.
- [3] Graeme B. Bell and Richard Boddington.  
Solid state drives: The beginning of the end for current practice in digital forensic recovery?  
*Journal of Digital Forensics, Security and Law*, 5(3), 2010.
- [4] D. Brezinski and T. Killalea.  
Guidelines for evidence collection and archiving.  
RFC 3227, IETF, 2 2002.
- [5] Brian Carrier.  
*File System Forensic Analysis*.  
Addison-Wesley Professional, Boston, MA, 2005.



# References II

- [6] Eoghan Casey.  
*Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.*  
Academic Press, San Diego, CA, 3rd edition, 2011.
- [7] Laura Chappell.  
*Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide.*  
Chappell University, 2nd edition, 2012.
- [8] Simson L. Garfinkel.  
Carving contiguous and fragmented files with fast object validation.  
*Digital Investigation*, 4:2–12, 2007.  
Proceedings of the Seventh Annual DFRWS Conference.
- [9] Phil Harvey.  
Exiftool by phil harvey.  
Software Website, 2024.  
Accessed on August 2, 2025.



# References III

- [10] Martin Herman, Michaela Iorga, Ahsen Michael Salim, Robert Jackson, Mark Hurst, Ross Leo, Richard Lee, Nancy Landreville, Anand Kumar Mishra, Yien Wang, and Rodrigo Sardinas.  
NIST cloud computing forensic science challenges.  
Technical Report NIST IR 8006, National Institute of Standards and Technology, 2020.
- [11] Gary C. Kessler.  
GCK's file signatures table, 2025.  
Accessed on October 2, 2026.
- [12] Microsoft.  
fsutil behavior.  
Microsoft Learn, Windows Commands reference, 2026.  
Accessed on October 2, 2026.
- [13] Snap Inc.  
When does Snapchat delete Snaps and Chats?  
Snapchat Support, 2026.  
Accessed on October 2, 2026.



# References IV

- [14] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis.  
A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues.  
*IEEE Communications Surveys & Tutorials*, 22(2):1191–1221, 2020.
- [15] Joe Sylve.  
Lime - linux memory extractor.  
GitHub repository, 2012.  
The canonical source code repository for the LiME tool.
- [16] The SQLite Project.  
Write-ahead logging, 2026.  
Accessed on October 2, 2026.
- [17] The util-linux project.  
mount(8) — linux manual page.  
man7.org, 2026.  
Accessed on October 2, 2026.

# References V

[18] The Wireshark Foundation.  
CaptureSetup/Ethernet.  
Wireshark Wiki, 2026.  
Accessed on October 2, 2026.



# Acronyms and Terminology II

**Data Carving** The process of recovering files from a storage medium by searching for known file signatures in the raw data, often used on unallocated space where deleted files may reside.

**Data in Transit** Data that is actively moving across a network, from one point to another. It is highly volatile and must be captured as it moves or it will be lost.

**Data in Use** Data that is actively being processed by a computer's CPU or that resides in its volatile memory (RAM).

**Dead-box Forensics** The analysis of a computer or digital device that has been powered off. This process primarily focuses on examining data at rest.

**Digital Remnants** Traces or fragments of data that remain on a device even after a user or application has attempted to delete them.

**Ephemeral Messaging** A type of communication where messages are designed to be automatically deleted after being viewed, such as in apps like Snapchat or Signal.

**EXIF** Exchangeable Image File Format: A standard for storing metadata within image files. This data can include the camera model, date, time, and GPS coordinates of where the photo was taken.

**ExifTool** A powerful command-line tool for reading, writing, and editing metadata (like EXIF data) within a wide variety of file types.



# Acronyms and Terminology III

- File Signature (Magic Numbers)** A unique sequence of bytes at the beginning (and sometimes end) of a file that identifies the true file format, regardless of the file's extension.
- File System** The method and data structure an operating system uses to control how data is stored and retrieved on a storage device like a hard drive.
- Fileless Malware** Malicious software that exists and runs only in a computer's active memory (RAM) without writing itself to the hard drive, making it undetectable in a powered-off system.
- Foremost** A command-line tool used to perform data carving to recover deleted files based on their headers and footers.
- GPS** Global Positioning System: A satellite navigation system. Phones and cameras can write GPS coordinates into a photo's EXIF metadata.
- HDD** Hard Disk Drive: A traditional data storage device that stores data magnetically on rotating platters.
- HTTP** Hypertext Transfer Protocol: The protocol web browsers and servers use to exchange pages and form data. Plain HTTP traffic can be read in a packet capture.
- HTTPS** Hypertext Transfer Protocol Secure: HTTP carried over an encrypted connection. A packet capture shows its connection metadata but not its content unless the session keys are available.

# Acronyms and Terminology IV

**IoT** Internet of Things: The vast network of interconnected physical devices, such as smart watches, security cameras, and home assistants, that collect and exchange data and can serve as sources of digital evidence.

**IP** Internet Protocol: The protocol that addresses and routes packets between networks. The ARP cache links IP addresses to physical device addresses.

**JFIF** JPEG File Interchange Format: A common JPEG variant, identified by the byte E0 after the FF D8 FF header.

**JPEG** Joint Photographic Experts Group: The common compressed image format used by cameras and phones. Its files begin with the bytes FF D8 FF and end with FF D9.

**LAN** Local Area Network: A network that connects computers within one building or site, such as a company office network.

**Live Acquisition** The process of collecting data, particularly from volatile memory (RAM), from a computer while it is still running.

**Live Response** The set of actions an investigator performs on a computer system while it is still powered on, with the primary goal of collecting volatile data before it is lost.



**MAC Times** A set of critical file system metadata timestamps associated with a file, including its Modified, Accessed, Changed (metadata) and Born (created) times, often written MACB.



# Acronyms and Terminology V

- Memory Image** A bit-for-bit copy of the contents of a computer's physical memory (RAM) at a specific point in time.
- Metadata** Data about data. It is information that describes a file's properties, such as its creation date, author, file size, and timestamps, rather than the content of the file itself.
- MFT** Master File Table: The NTFS table holding one record for every file and folder, including the \$SI timestamps.
- NAS** Network-Attached Storage: A dedicated file storage device connected to a network that allows multiple users and devices to store and retrieve data from a central location.
- NTFS** New Technology File System: The standard file system of Microsoft Windows. It keeps MACB timestamps in each file's MFT record.
- Order of Volatility** The fundamental principle in digital forensics that dictates evidence should be collected in order from most volatile (most likely to be lost) to least volatile.
- Packet** A small segment of a larger message that is sent over a computer network.
- Packet Capture (Packet Sniffing)** The act of intercepting and logging data packets as they travel across a digital network.



# Acronyms and Terminology VI

**PDF** Portable Document Format: A document format whose files begin with the ASCII characters %PDF.

**PhotoRec** A file data recovery software tool designed to recover lost files, including video, documents and archives from hard disks, and lost pictures from digital camera memory.

**Promiscuous Mode** A setting for a network interface card (NIC) that allows it to capture all network traffic it can see, not just the traffic addressed to it.

**RAM** Random Access Memory: A computer's volatile, short-term memory where applications, the operating system, and current data are kept for fast access by the processor. Its contents are lost when power is turned off.

**RFC** Request for Comments: A document series published by the Internet Engineering Task Force. RFC 3227 gives guidelines for evidence collection, including the order of volatility.

**Scalpel** An open-source data carving tool that is an overhaul and improvement of the Foremost tool.

**\$SI** \$STANDARD\_INFORMATION: The NTFS attribute that holds a file's main set of MACB timestamps.

**SPAN** Switched Port Analyzer: A switch feature that copies traffic from other ports to one mirror port, so a capture device can see it.





# Thank You!

