Foundations of CHFI (Forensic Mindset)

What is CHFI?

CHFI focuses on **identifying, preserving, analyzing, and presenting digital evidence** in a legally admissible manner.

Closely aligned with:

- Digital Forensics and Incident Response (DFIR)
- MITRE ATT&CK

Core Forensic Principles

1. **Integrity Preservation**
    - Use hashing (MD5/SHA256)
    - No alteration of evidence
2. **Chain of Custody**
    - Who handled evidence, when, how
3. **Repeatability**
    - Another investigator must reach same conclusion
4. **Documentation**
    - Every step logged

CHFI Process (Deep Dive)

Standard Forensic Lifecycle

1. Identification

- Detect incident source
- Example: Suspicious outbound traffic

2. Preservation

- Isolate system (NOT power off blindly)
- Capture volatile memory

3. Collection

- Disk imaging (bit-by-bit)
- Log acquisition

4. Examination

- Data filtering, extraction

5. Analysis

- Timeline creation
- Attack reconstruction

6. Reporting

- Legal-grade documentation

Evidence Types

Type	Example	Importance
Volatile	RAM, processes	High (lost quickly)
Non-volatile	HDD, SSD	Persistent
Network	PCAP	Attack tracing
Logs	SIEM, firewall	Correlation

CHFI Tactics & Techniques (Core Section)

A. Attacker Tactics (Mapped to MITRE ATT&CK)

Tactic	Objective	Example
Initial Access	Entry point	Phishing
Execution	Run payload	PowerShell
Persistence	Maintain access	Registry run keys
Privilege Escalation	Gain admin	Exploit
Defense Evasion	Avoid detection	Log clearing
Credential Access	Steal creds	Mimikatz
Lateral Movement	Spread	SMB
Exfiltration	Data theft	DNS tunneling

B. Forensic Techniques (Investigator View)

1. Disk Forensics

- File carving
- Deleted file recovery
- Metadata analysis

Tools:

- Autopsy
- FTK

2. Memory Forensics

- Process analysis
- Malware detection in RAM

Tools:

- Volatility

Key commands:

- pslist
- netscan
- malfind

3. Network Forensics

- Packet inspection
- Session reconstruction

Tools:

- Wireshark
- tcpdump

4. Log Analysis

- Event correlation
- Timeline building

Sources:

- Windows Event Logs
- Firewall logs
- SIEM alerts

5. Malware Forensics

- Static analysis
- Dynamic sandboxing

Tools:

- IDA Pro
- Cuckoo Sandbox

CHFI Investigation Tactics (Operational)
Key Investigator Tactics
Timeline Analysis

- Build sequence of events

- Correlate logs + file timestamps

Artifact Correlation

- Registry + Prefetch + Logs

IOC vs IOA

Type	Description	Limitation
IOC	Known signature	Easily bypassed
IOA	Behavior-based	More reliable

Anti-Forensics (Critical Topic)

Attackers use:

- Log deletion
- File wiping
- Encryption
- Timestamp manipulation

Investigator counter:

- Journal recovery
- Shadow copies
- Memory analysis

Case Study (Realistic Scenario)

Scenario: Banking Malware Incident

Step-by-step investigation:

1. Alert triggered (SIEM)
2. Suspicious PowerShell detected
3. Memory captured
4. Volatility shows injected process
5. Network logs show C2 communication
6. Disk reveals persistence via registry

Outcome:

- Identified malware family
- Determined data exfiltration
- Produced legal report

Practical Lab (Hands-on)

Lab 1: Memory Forensics

Objective:

Detect malicious process

Steps:

1. Capture RAM (DumpIt)

2. Run:
   volatility -f memdump.raw pslist
   volatility -f memdump.raw malfind
3. Identify suspicious process

Lab 2: Disk Analysis
Objective:
Recover deleted files
Steps:
1. Load image in Autopsy
2. Analyze:
   - File system
   - Deleted files
   - Web artifacts

Lab 3: Network Analysis
Objective:
Find data exfiltration
Steps:
1. Open PCAP in Wireshark
2. Filter:
   dns || http
3. Detect suspicious domain

Reporting & Legal Considerations

Report Structure

- Executive Summary
- Methodology
- Findings
- Evidence
- Conclusion

Legal Aspects

- Evidence admissibility
- Documentation integrity
- Expert witness role

Core Forensic Principles

1. Integrity Preservation (Evidence Integrity)

Concept: Evidence must remain **bit-for-bit identical** to its original state. Any modification—intentional or accidental—can render it inadmissible.

Technical Mechanism: Hashing

Primary control: cryptographic hashing via Hash Function

Key algorithms:

- MD5 (legacy, fast, collision-prone)
- SHA-256 (forensic standard)

Forensic Workflow

1. Acquire evidence (disk image / RAM)
2. Generate hash (before analysis)
3. Store securely
4. Re-hash after transfer/analysis
5. Compare values

✔ Match = integrity preserved

✘ Mismatch = evidence compromised

Practical Example
sha256sum disk_image.dd
Output:
3f2a...9c8b disk_image.dd

Risks & Controls

Risk	Control
Accidental modification	Write blockers
Malware tampering	Offline acquisition
Weak hashing	Use SHA-256 or stronger

Key Insight: Integrity is not assumed, it is **mathematically proven**.

2. Chain of Custody (CoC)
A **chronological, auditable trail** documenting:

- Who handled evidence
- When
- Why
- Under what conditions

Structure of Chain of Custody

Field	Description
Evidence ID	Unique identifier
Description	Device/file details
Collected by	Investigator name
Date/Time	Timestamp
Location	Where collected
Transfer logs	Every handoff recorded

Lifecycle Flow

Collection → Packaging → Transport → Storage → Analysis → Court
Each stage must be logged.

Example Entry

Step	Person	Action	Time
1	Analyst A	Collected laptop	10:00
2	Analyst B	Received for imaging	11:30

Legal Importance

- Ensures **evidence admissibility in court**
- Prevents defense claims like:
  - "Evidence was tampered"
  - "Unauthorized access occurred"

Best Practices

- Tamper-evident bags
- Digital signatures
- Restricted access logs
- Time synchronization (NTP)

Key Insight: Without CoC, even **perfect evidence becomes useless** in legal proceedings.

3. Repeatability (Reproducibility)

Concept

Another independent investigator must be able to:

- Follow the same steps
- Use the same data
- Reach the same conclusion

Technical Requirements

✔ **Standardized Procedures**

- Imaging method (bit-by-bit)
- Tool configuration

✔ **Tool Consistency**

Example tools:

- Autopsy
- Volatility

Example Scenario

Investigator A:

- Extracts deleted file
- Finds malware

Investigator B:

- Uses same image + tool
- Must retrieve same file + result

❌ **What Breaks Repeatability?**

- Missing steps in documentation
- Tool version mismatch
- Non-deterministic scripts
- Live system analysis (without snapshot)

Scientific Analogy

Repeatability aligns with:

- Experimental reproducibility in science
- Auditability in compliance frameworks

Key Insight: Forensics is not just analysis—it is **defensible science**.

4. Documentation (Forensic Reporting Discipline)

Concept

Every action taken must be:

- Recorded
- Timestamped
- Justified

What to Document

1. Acquisition Details

- Device info
- Hash values
- Tools used

2. Analysis Steps

- Commands executed
- Filters applied
- Findings

3. Observations

- Suspicious artifacts
- Anomalies

4. Decisions

- Why certain paths were taken

Sample Entry

Date: 2026-04-18 10:30
Action: Memory dump acquired using DumpIt
Hash (SHA-256): abc123...
System State: Live, suspected malware activity

Report Structure

1. Executive Summary
2. Scope
3. Methodology
4. Findings
5. Evidence (hashes, logs)
6. Conclusion

Common Pitfalls

Issue	Impact
Incomplete logs	Weak case
No timestamps	Non-verifiable
Tool not mentioned	Non-repeatable

Advanced Practice

- Use **automated logging tools**
- Maintain **forensic notebooks**
- Version control for scripts

Key Insight: If it's not documented**, it did not happen** (legally and professionally)**.**

Final Synthesis (Exam/Interview Ready)

Principle	Core Control	Risk if Ignored
Integrity	Hashing	Evidence invalid
Chain of Custody	Audit trail	Legal rejection
Repeatability	Standard process	Non-defensible findings
Documentation	Detailed logs	Investigation collapse

Standard Forensic Lifecycle (Deep Dive)

This lifecycle is not linear, instead it is **iterative and evidence-driven**, tightly coupled with Digital Forensics and Incident Response (DFIR).

1. Identification (Detection & Scoping)

Objective

Detect that **something abnormal has occurred** and define:

- Scope (which systems?)
- Nature (malware, insider threat, breach?)

Techniques

✔ **Log Monitoring**

- SIEM alerts (failed logins, anomalies)
- Firewall/IDS triggers

✔ **Behavioral Detection (IOA-based)**

- Suspicious PowerShell execution
- Unusual outbound traffic

Aligned with:

- MITRE ATT&CK (Initial Access, Execution)

Real-Life Use Case (Banking)

Scenario:

A bank SOC detects:

- Repeated outbound traffic to unknown IP (Russia-based)
- DNS queries every 5 seconds

Identification outcome:

- Possible **Command & Control (C2) communication**

Key Challenges

- False positives
- Alert fatigue
- Lack of context

Key Insight: Identification is about **signal vs noise discrimination**.

2. Preservation (First Response – Critical Phase)

Objective

Ensure evidence is:

- Not altered
- Not destroyed
- Legally defensible

Techniques

✔ **System Isolation**

- Remove from network (NOT shut down immediately)

✔ **Capture Volatile Data**

- RAM (critical!)
- Running processes
- Network connections

Tools:

- DumpIt
- FTK Imager

Real-Life Use Case

Scenario: Banking Trojan infection

Wrong action:

- Immediately shutting down system → lose RAM evidence

Correct action:

- Capture memory → detect fileless malware

Critical Risks

Mistake	Impact
Power off system	Lose volatile evidence
Continue normal use	Evidence overwritten
No isolation	Attack spreads

Key Insight: Preservation decisions often **determine investigation success or failure.**

3. Collection (Evidence Acquisition)

Objective

Acquire **forensically sound copies** of data.

Techniques

✔ **Disk Imaging (Bit-by-bit)**

- Full disk clone (including deleted space)

✔ **Log Collection**

- OS logs
- Application logs
- Network logs

Integrity Control

Use hashing via:

- SHA-256

Tools

- FTK Imager
- EnCase

Real-Life Use Case
Scenario: ATM fraud investigation
Collected:

- ATM machine disk image
- Transaction logs
- CCTV timestamps

Common Issues

- Partial collection (missed logs)
- Live system contamination
- Lack of hashing

Key Insight: Collection must be **complete, verified, and reproducible**.

4. Examination (Data Processing & Extraction)

Objective
Filter and extract **relevant artifacts** from massive datasets.

Techniques

✔ **File System Analysis**

- Deleted files
- Hidden partitions

✔ **Artifact Extraction**

- Browser history
- Registry keys
- Prefetch files

Tools

- Autopsy
- Sleuth Kit

Real-Life Use Case

Scenario: Insider data theft

Findings:

- USB usage logs
- Recently accessed confidential files
- File copy traces

Challenges

- Large data volume (TBs)
- Encrypted data
- Obfuscation

Key Insight: Examination is about **reducing noise into meaningful artifacts.**

5. Analysis (Correlation & Reconstruction)

Objective

Transform extracted data into:

- **Timeline**
- **Attack narrative**
- **Attribution (if possible)**

Techniques

✔ **Timeline Analysis**

- File timestamps
- Log correlation

✔ **Attack Reconstruction**

- Entry → Execution → Persistence → Exfiltration

Aligned with:

- MITRE ATT&CK

Tools

- Volatility
- Wireshark

Real-Life Use Case
Scenario: SWIFT fraud attempt
Findings:

1. Phishing email delivered malware
2. Malware created persistence
3. Credentials stolen
4. Unauthorized SWIFT transaction initiated

Full attack chain reconstructed

Challenges

Issue	Impact
Missing logs	Incomplete timeline
Time desync	Incorrect sequence
False correlation	Wrong conclusion

Key Insight: Analysis converts **data → intelligence → evidence.**

6. Reporting (Legal & Executive Communication)

Objective

Produce **clear, defensible, and actionable report**.

Structure

1. Executive Summary

- Business impact
- High-level findings

2. Technical Details

- Evidence
- Methodology
- Tools used

3. Timeline

- Step-by-step attack flow

4. Conclusion & Recommendations

- Root cause
- Preventive measures

Legal Requirements

- Evidence admissibility
- Chain of custody proof
- Expert witness readiness

Real-Life Use Case

Scenario: Regulatory reporting (Bangladesh Bank)

Report includes:

- Breach scope
- Financial impact
- Control gaps
- Remediation plan

Common Mistakes

Issue	Impact
Too technical	Management confusion
Too vague	Weak legal case
Missing evidence	Non-admissible

Key Insight: A great investigation is useless without a **clear, defensible report**.

Example: Banking Malware Attack

Phase	What Happened
Identification	SOC detects abnormal DNS traffic
Preservation	System isolated, RAM captured
Collection	Disk + logs acquired
Examination	Malware artifacts extracted
Analysis	Attack chain reconstructed
Reporting	Legal + regulatory report submitted

Reporting & Legal Considerations

1. Forensic Report Structure (Deep Explanation)

A forensic report must satisfy **two audiences simultaneously**:

- **Management (non-technical)**
- **Legal authority (technical + evidentiary rigor)**

1. Executive Summary

Purpose

Translate complex investigation into **business impact + decision insight**.

Must Answer

- What happened?
- How severe?
- What is the impact (financial, operational, reputational)?
- What actions are required?

Real-Life Example (Bank)

"A malware infection led to unauthorized credential access. No financial loss occurred, but **3 systems were compromised**, posing a high risk to SWIFT operations."

Common Mistakes

- Too technical (C2, DLL injection jargon)
- Too vague ("incident occurred")

Best Practice
Write it as if addressing:

- CEO
- Board Risk Committee

2. Methodology

Purpose
Explain **how the investigation was conducted**, ensuring:

- Transparency
- Repeatability
- Legal defensibility

Components

- Acquisition method (disk imaging, RAM capture)
- Tools used:
  - FTK Imager
  - Autopsy
- Hashing approach:
  - SHA-256
- Analysis techniques (timeline, artifact correlation)

Real-Life Example
"A bit-by-bit disk image was acquired using FTK Imager. Integrity was verified using SHA-256 hashing. Memory was analyzed using Volatility."

Risk if Missing

- Defense can claim:
  - "Unreliable process"
  - "Evidence manipulated"

Key Insight: Methodology proves your work is **scientifically and legally valid**.

3. Findings
Purpose
Present **what was discovered**, clearly and objectively.

Content Includes

- Malware presence
- Unauthorized access
- Suspicious activities
- Timeline of attacker actions

Structure

Finding	Description	Evidence
Malware detected	Trojan found in system32	File hash
Unauthorized login	Admin login at 3 AM	Event log

Real-Life Example

"Analysis revealed a PowerShell-based fileless malware establishing persistence via registry run keys."

Critical Rule

- **No assumptions**
- Only **evidence-backed statements**

Key Insight

Findings must be:

- **Objective**
- **Traceable to evidence**

4. Evidence

Purpose

Provide **verifiable proof** supporting findings.

Types of Evidence

- Disk images
- Memory dumps
- Log files
- Network captures (PCAP)

Integrity Assurance

Maintained via: Hash Function

Evidence Presentation Format

Evidence ID	Type	Hash	Description
E-01	Disk Image	abc123	User laptop
E-02	RAM Dump	def456	Captured memory

Real-Life Example

"Evidence E-03 (memory dump) revealed an injected process communicating with external IP 185.x.x.x."

Common Pitfalls

Issue	Impact
Missing hash	Evidence invalid
No labeling	Confusion
Poor storage	Tampering risk

Key Insight: Evidence is the **foundation of legal truth**.

5. Conclusion
Purpose
Provide **final assessment + actionable recommendations.**

Should Include

- Root cause
- Impact summary
- Risk level
- Recommended controls

Real-Life Example
"The breach originated from a phishing email exploiting user awareness gaps. Immediate implementation of EDR and user training is recommended."

Avoid

- Introducing new findings
- Emotional language

Key Insight
Conclusion bridges **technical findings → business decisions**.

2. Legal Considerations (Deep Dive)

1. Evidence Admissibility

Concept

Evidence must be accepted in court—otherwise investigation fails legally.

Requirements

- ✔ Relevance
- ✔ Authenticity
- ✔ Integrity
- ✔ Proper acquisition

Legal Risk

If violated:

- Case dismissed
- Evidence rejected

Real-Life Example

A bank fraud case fails because:

- Disk image was taken **without write blocker**

Defense argument:

"Evidence could have been altered"

Key Insight: Technical correctness ≠ legal admissibility**, both *must align.***

2. Documentation Integrity

Concept

All documentation must be:

- Accurate
- Complete
- Tamper-proof

Includes

- Investigation logs
- Chain of custody
- Analysis notes

Protection Techniques

- Digital signatures
- Access control
- Time synchronization

Real-Life Example

If timestamps mismatch:

- Attack timeline becomes invalid
- Legal credibility drops

Risks

Issue	Impact
Missing logs	Weak case
Edited records	Legal rejection
Time inconsistency	Timeline collapse

Key Insight: Documentation is **evidence about evidence.**

3. Expert Witness Role

Concept

Investigator may need to testify in court as an expert.

Responsibilities

- Explain technical findings in simple terms
- Defend methodology
- Validate evidence integrity

Required Skills

Skill	Importance
Technical depth	High
Communication	Critical
Legal awareness	Essential

Real-Life Example

Court question:

“How can you prove this file was not altered?”

Expected answer:

- Explain hashing
- Show matching hash values
- Reference acquisition process

Common Failure Points

- Overuse of jargon
- Inconsistent statements
- Lack of documentation

Key Insight

An expert witness must be:

- **Technically correct**
- **Legally credible**
- **Clearly understandable**

Final Synthesis

Area	Core Purpose	Failure Impact
Executive Summary	Business clarity	Misinformed decisions
Methodology	Legal defensibility	Evidence challenged
Findings	Fact reporting	Misinterpretation
Evidence	Proof	Case collapse
Conclusion	Action guidance	No remediation
Admissibility	Legal acceptance	Case dismissed
Documentation	Audit trail	Credibility loss
Expert Witness	Court validation	Weak testimony