

GENESIS ITU

Digital Forensics Fundamentals

Course Textbook & Student Workbook

A college-style foundation in digital evidence, investigation process, and professional reporting — designed as the natural next step after SOC Analyst training.

Zarco AI Systems LLC · Genesis ITU

Clean · Practical · Professional

How to Use This Book

This workbook is written for students who already understand basic security operations: alerts, logs, and the idea of incident response. Digital forensics goes deeper. It teaches you how to collect and examine digital evidence in a way that is careful, documented, and suitable for real investigations.

Read each chapter in order. When you see a definition, learn it formally — the same language employers and reports use. Complete the pause-and-review prompts before moving on. Labs use only practice images and your own systems. Never examine another person's device without proper authorization.

This course does not teach you how to break into systems. It teaches you how to investigate lawfully and report truthfully after an incident or under proper authority.

Table of Contents

Chapter 1 — What Digital Forensics Is

Chapter 2 — Legal Authority, Ethics, and Scope

Chapter 3 — Chain of Custody and Evidence Integrity

Chapter 4 — Acquisition and Imaging

Chapter 5 — File Systems, Deleted Data, and Metadata

Chapter 6 — Timeline Analysis

Chapter 7 — Memory Forensics Fundamentals

Chapter 8 — Network and Log Forensics

Chapter 9 — Malware Triage and Safe Handling

Chapter 10 — Reporting, Testimony Mindset, and Career Path

Appendix A — Glossary

Appendix B — Starter Tool List

Appendix C — Report Template Outline

Chapter 1 — What Digital Forensics Is

Digital forensics is the disciplined process of identifying, preserving, collecting, analyzing, and presenting digital evidence. The goal is not curiosity. The goal is reliable facts that can support decisions — in a security investigation, a workplace case, or a legal proceeding.

Digital forensics

The application of scientific and investigative methods to digital data in order to preserve, recover, analyze, and present evidence in a manner suitable for a court or other formal review.

Digital evidence

Information of probative value that is stored or transmitted in binary form, including files, logs, memory contents, network captures, and device artifacts.

DFIR

Digital Forensics and Incident Response — the combined practice of investigating security incidents and handling digital evidence with forensic discipline.

How forensics differs from everyday troubleshooting

A help-desk technician may reboot a machine to fix a problem. A forensic examiner treats that same machine as a possible crime scene. Rebooting can destroy volatile evidence in memory. Opening a file can change timestamps. Good intentions are not enough; process protects the truth.

The forensic process (high level)

- **Identification** — What systems and data may hold relevant evidence?
- **Preservation** — Prevent alteration of original evidence.
- **Collection / acquisition** — Create forensic copies under controlled methods.
- **Examination / analysis** — Recover and interpret artifacts on working copies.
- **Presentation** — Report findings clearly, with methods and limitations stated.

SOC analysts often perform the first two or three steps in light form: noticing an alert, isolating a host, and preserving logs. Full forensics extends that work with imaging, deeper recovery, and formal reporting.

***Pause and review.** In your own words, explain how digital forensics differs from ordinary troubleshooting. Name the five high-level process stages.*

Lab — Mindset check

- Write three actions a technician might take that could destroy or alter evidence.
- Write three actions a forensic examiner would take instead.
- Keep this note for Chapter 3 (chain of custody).

Chapter 2 — Legal Authority, Ethics, and Scope

Technical skill without authority is not investigation — it can be a violation of law or policy. Before you touch a system, you must know why you are allowed to do so and how far your permission goes.

Authorization

Permission, granted by law, policy, or the rightful owner, to perform a defined investigative action on a system or data set.

Scope

The agreed or ordered boundaries of an investigation: which devices, accounts, time ranges, and data types are included — and which are not.

Unauthorized access

Accessing a system, account, or data without legal or organizational permission. Good intent does not automatically make access lawful.

Common lawful contexts

- Your own devices and accounts for learning (lab images preferred).
- Employer-owned systems under written incident response or acceptable-use policy.
- Client engagement under a signed agreement.
- Law enforcement acting under warrant, consent, or other lawful process.

Ethics for the professional examiner

Collect only what the scope requires. Do not browse personal content for curiosity. Separate facts from opinions in reports. Protect privacy of uninvolved parties. Refuse pressure to alter findings. If you are unsure whether you have authority, stop and ask legal, HR, or a supervisor.

Pause and review. List two situations where you would have authority to examine a system, and two where you would not. What is scope, and why does it matter?

Chapter 3 — Chain of Custody and Evidence Integrity

Evidence is only as strong as the story of how it was handled. Chain of custody is that story in written form.

Chain of custody

A chronological record documenting the seizure, custody, control, transfer, analysis, and disposition of evidence, showing who had it, when, and what was done.

Integrity (of evidence)

The property that evidence has not been altered in an undocumented way from the time of acquisition through analysis and presentation.

Cryptographic hash

A fixed-length value computed from data (for example SHA-256) used to detect change. Matching hashes before and after a copy support a claim that the copy is identical to the source at the bit level for practical purposes.

Practical rules

- Prefer working on forensic images, not original media, whenever possible.
- Hash original or image at acquisition; record the hash in the custody log.
- Document every person who receives the evidence and every tool used.
- Store media securely; limit access to those with a need.
- If something goes wrong (dropped drive, failed copy), document it honestly.

In a SOC setting you may not seize physical drives every day, but the same discipline applies to log exports, packet captures, and disk snapshots: label them, hash them, and record who handled them.

Pause and review. Define chain of custody. Why do investigators hash an image after acquisition? What should you do if a copy fails halfway?

Lab — Hash practice

- On your own lab file, compute a SHA-256 hash (certutil, sha256sum, or HashCalc).
- Copy the file and hash the copy. Confirm they match.
- Change one byte in a third copy and hash again. Confirm they differ.
- Write the commands and results in your notebook.

Chapter 4 — Acquisition and Imaging

Acquisition is the controlled creation of a forensic copy of digital media or data. The ideal is a bit-for-bit image of the source, taken in a way that minimizes change to the original.

Forensic image

A bit-stream or sector-level copy of a storage device or partition, often stored in formats such as raw (dd) or E01, used as the working source for examination.

Write blocker

Hardware or software that allows read access to storage media while preventing writes, protecting the original evidence during acquisition.

Volatile data

Information that exists in temporary storage (especially RAM) and is lost when power is removed or the system is rebooted.

Order of volatility (concept)

Some evidence disappears quickly. A common teaching order from most to least volatile includes: CPU registers and cache, memory (RAM), network state, running processes, disk, then backups and archives. In incident response, teams often capture memory and critical logs before shutting a system down.

Acquisition principles

- Document the device: make, model, serial, condition, time zone if known.
- Use write blocking when acquiring from original disks.
- Record tool name, version, and operator.
- Verify the image with hashing.
- Label and store the original and the image separately.

Pause and review. What is a forensic image? What is a write blocker for? Why might an IR team capture memory before pulling the power plug?

Lab — Imaging awareness

- Install FTK Imager or a comparable free imager in your lab environment.
- Create an image of a small USB stick you own (or a practice VM disk).
- Record the hash of the image.
- Do not use workplace or other people's devices for practice.

Chapter 5 — File Systems, Deleted Data, and Metadata

Understanding how operating systems store files helps you find what users and attackers leave behind — including data they thought was deleted.

File system

The method an operating system uses to organize and store files on media (examples: NTFS, APFS, ext4, FAT32).

Metadata

Data about data — such as timestamps, file size, ownership, and permissions — that can support timeline and attribution analysis.

Unallocated space

Storage areas not currently assigned to active files; may still contain recoverable remnants of deleted files until overwritten.

Deleted does not always mean gone

When a user deletes a file, many systems remove directory entries or mark clusters as free rather than immediately wiping content. Until those areas are reused, forensic tools may recover file contents or fragments. Solid-state drives and modern secure-delete features can change this picture — always state limitations in your report.

Timestamps to understand

MAC times (modified, accessed, created) and similar fields vary by file system and tool. Time zone and clock skew matter. A professional report states how times were interpreted and whether the system clock was reliable.

Pause and review. Define metadata and unallocated space. Why can deleted files sometimes still be recovered? Name one reason timestamps can mislead an analyst.

Lab — Autopsy first look

- Download a practice disk image from a known training source (Digital Corpora, NIST, or similar).
- Open it in Autopsy.
- Locate at least one deleted or interesting file and note its metadata.
- Screenshot or note tool version for your records.

Chapter 6 — Timeline Analysis

A timeline organizes events in order so the story of an incident becomes visible: when malware landed, when a user logged in, when data left the network.

Timeline analysis

The process of collecting timestamped artifacts from multiple sources and arranging them chronologically to reconstruct sequence of activity.

Artifact

A piece of digital data that indicates user or system activity (for example a prefetch file, browser history entry, logon event, or scheduled task).

Building a useful timeline

- Pull times from disk artifacts, logs, and network data when available.
- Normalize time zones to a single reference (often UTC) and note local offsets.
- Cross-check: does the same event appear in more than one source?
- Mark gaps and uncertainties rather than inventing connections.
- Focus on events relevant to the scope — not every file touch on the system.

SOC analysts already build light timelines from SIEM alerts. Forensics extends that skill with host artifacts that never made it into the SIEM.

Pause and review. *What is timeline analysis for? Why normalize to UTC? What should you do when two sources disagree about a time?*

Chapter 7 — Memory Forensics Fundamentals

Memory forensics examines the contents of RAM. It is essential when attackers use fileless techniques, inject code into legitimate processes, or leave keys and payloads only in memory.

Memory dump

A snapshot of volatile memory (RAM) captured for analysis, often including process lists, network connections, and loaded modules at a point in time.

Fileless malware

Malicious activity that minimizes or avoids writing traditional executable files to disk, relying instead on memory, scripts, or legitimate system tools.

Why SOC teams care

An alert may show suspicious PowerShell. The disk image may look clean. A memory dump can reveal the real command line, injected modules, or active command-and-control connections. Memory and disk analysis complement each other.

Starter analysis questions

- What processes were running?
- Which processes have unexpected network connections?
- Are there signs of code injection or hollowed processes?
- What commands appear in command-line arguments?

Tools such as Volatility are commonly taught for this work. Always analyze dumps in an isolated lab environment.

Pause and review. *What is a memory dump? Give one example of a question memory analysis can answer that disk analysis might miss.*

Lab — Volatility orientation

- Install Volatility 3 in your lab.
- Obtain a sample memory dump from a training source.
- List processes and note anything unusual for a baseline Windows or Linux dump.
- Record the plugin or command you used and one finding.

Chapter 8 — Network and Log Forensics

Not all evidence lives on a single laptop. Network captures and centralized logs often prove when data moved, which hosts talked, and whether an attacker reached critical systems.

PCAP

Packet capture file containing recorded network traffic for later analysis (commonly opened in tools such as Wireshark).

Log correlation

Comparing events from multiple log sources (firewall, endpoint, identity, application) to form a single coherent incident narrative.

Practical focus areas

- DNS queries that reveal command-and-control domains.
- Unusual outbound connections on rare ports.
- Authentication failures followed by success from a new location.
- Large transfers to external storage or cloud accounts.

Preserve original log exports and PCAPs with the same hashing and custody habits you use for disk images. Note sensor time sync issues.

Pause and review. *What is a PCAP? Name two log or network artifacts that often appear in incident timelines.*

Lab — Wireshark basics

- Open a public sample PCAP in Wireshark.
- Filter for DNS or HTTP.
- Identify one conversation and write source, destination, and purpose if clear.
- Export a short note for your lab journal.

Chapter 9 — Malware Triage and Safe Handling

Forensic examiners sometimes must handle suspicious files. The priority is safety of the lab, accuracy of the analysis, and clear documentation — not speed for its own sake.

Malware triage

An initial, controlled assessment of a suspicious sample to determine type, basic behavior indicators, and whether deeper reverse engineering is required.

Isolated lab

A restricted environment (often a virtual machine without sensitive production access) used to examine untrusted code safely.

Safe handling rules

- Never open unknown samples on your daily-driver or production machine.
- Use isolated VMs; snapshot before analysis; revert after.
- Disable unnecessary network sharing from the lab VM.
- Password-protect or clearly label malware archives when storing samples.
- Record hashes of samples before analysis.

This chapter is triage-level awareness. Full reverse engineering is a specialized career path beyond this fundamentals course.

Pause and review. *Why isolate malware analysis? What should you record before examining a sample?*

Chapter 10 — Reporting, Testimony Mindset, and Career Path

A finding that cannot be explained clearly has limited value. Professional forensics ends in communication: written reports, and sometimes spoken explanation under pressure.

Forensic report

A structured document describing scope, methods, evidence handled, findings, and conclusions, written so a non-specialist decision-maker can understand what was done and what it means — without hiding limitations.

Report structure (recommended)

- Title, author, date, case or ticket reference.
- Scope and authorization summary.
- Evidence inventory (devices, images, hashes, custody notes).
- Tools and versions used.
- Methodology narrative.
- Findings (facts first).
- Conclusions and opinions (clearly labeled as such).
- Limitations and recommendations.
- Appendix: detailed artifacts, screenshots, exports.

Testimony mindset

If you ever explain your work to management, HR, or a legal setting, stick to what you did, what you observed, and what your methods support. Say “I do not know” when you do not know. Do not exaggerate certainty.

Career next steps after this course

- Strengthen SOC/IR experience while practicing lab forensics weekly.
- Build a portfolio of anonymized lab reports (never real victim data).
- Consider certifications such as related CompTIA tracks, then specialist forensics credentials when budget and experience allow (examples often discussed in industry: vendor tool certs, GIAC GCFA, and others — research current requirements).
- Search roles: Digital Forensics Analyst, DFIR Analyst, IR with forensics focus.

Pause and review. List the main sections of a forensic report. What is the difference between a finding and an opinion in your report?

Congratulations on completing Digital Forensics Fundamentals. You now have the vocabulary, process discipline, and starter lab habits to grow from SOC-style triage into structured investigation. Continue practicing only on authorized systems and lab images. Stay precise. Stay honest. Best of luck as you take the next step — you have come a long way, and steady discipline will serve you well.

Appendix A — Glossary

Acquisition

Controlled collection of digital evidence, often by forensic imaging.

Artifact

A data remnant that indicates activity on a system.

Chain of custody

Documented history of evidence handling.

DFIR

Digital Forensics and Incident Response.

Forensic image

Bit-level copy of media used for examination.

Hash

Cryptographic fingerprint used to detect changes in data.

Memory dump

Snapshot of RAM for volatile analysis.

Metadata

Data describing a file or object (times, owner, size, etc.).

PCAP

Saved network packet capture.

Scope

Authorized boundaries of an investigation.

Timeline analysis

Chronological reconstruction of events from artifacts.

Unallocated space

Disk areas not assigned to active files; may hold deleted data.

Volatile data

Data that disappears when power or process state is lost.

Write blocker

Device or software preventing writes to evidence media.

Appendix B — Starter Tool List

Use only in authorized lab environments. Verify download sources and versions yourself.

Autopsy

GUI disk analysis platform built on The Sleuth Kit.

FTK Imager

Imaging and preview tool commonly used for acquisition practice.

Volatility 3

Memory forensics framework.

Wireshark

Network protocol analyzer for PCAP review.

Hash tools

sha256sum, certutil, or HashCalc for integrity checks.

Isolated VM

Virtual machine software for safe malware triage labs.

Appendix C — Report Template Outline

Copy this outline into your own document for lab cases.

1. Case title and reference number
2. Examiner name and date
3. Authorization / scope statement
4. Evidence list (item, description, hash, received from/date)
5. Tools and versions
6. Methods (acquisition, examination steps)
7. Findings (numbered facts)
8. Conclusions (labeled separately from findings)
9. Limitations
10. Recommendations
11. Appendix / exhibits

Genesis ITU · Digital Forensics Fundamentals · Zarco AI Systems LLC
For educational use with authorized lab materials only.