

Introduction to Digital Forensics

Introduction to Digital Forensics

Key concepts, processes, and best practices for investigating digital evidence.

1. What Is Digital Forensics?

Aspect	Description
Definition	The scientific method of identifying, preserving, analyzing, and presenting digital evidence from computers, mobile devices, networks, and other electronic media.
Goal	Reconstruct events, determine the truth of an incident, and provide admissible evidence for legal or disciplinary actions.
Scope	Includes computers, smartphones, tablets, servers, cloud services, IoT devices, removable media, and network traffic.
Legal Context	Governed by statutes (e.g., Computer Fraud and Abuse Act, GDPR), chain of custody rules, and evidentiary standards (relevance, authenticity, reliability).

2. Core Principles

1. **Integrity** – Preserve the original data unchanged (use write blockers, hash verification).
 2. **Authenticity** – Prove that the evidence is what it claims to be (hash values, timestamps).
 3. **Reliability** – Follow repeatable, documented procedures; use validated tools.
 4. **Chain of Custody** – Record every person who handles the evidence, when, where, and why.
 5. **Legal Admissibility** – Ensure compliance with jurisdiction-specific rules (e.g., Daubert, Frye standards).
-

3. The Digital Forensics Process (Four-Stage Model)

1. Identification

- Determine potential sources of evidence (devices, accounts, cloud services).
- Prioritize based on volatility (RAM > network traffic > hard drives > backups).

Introduction to Digital Forensics

2. Preservation

- Isolate the device (air?gap, power?down, or live acquisition if needed).
- Create a forensic image (bit?for?bit copy) using tools such as FTK Imager, dd, or EnCase.
- Calculate and record cryptographic hash (MD5, SHA?1, SHA?256) for original and image.

3. Analysis

- **File System Examination** – locate hidden, deleted, or altered files; recover metadata.
- **Timeline Reconstruction** – correlate timestamps (MAC times, log entries, registry keys).
- **Keyword & Pattern Searches** – use regex, hash sets (NSRL), or YARA rules.
- **Memory Analysis** – extract processes, network connections, encryption keys (Volatility, Rekall).
- **Network Forensics** – parse PCAP files, reconstruct sessions (Wireshark, NetworkMiner).
- **Application?Specific Artifacts** – browsers, email clients, instant messengers, cloud sync folders.

4. Presentation

- Document findings in a clear, chronological report.
- Include methodology, tools, hash values, screenshots, and expert opinion.
- Prepare for testimony: be ready to explain technical details to non?technical audiences.

4. Types of Digital Evidence

Category	Typical Sources	Common Artifacts
Computer Forensics	Desktops, laptops, servers	File system, registry, event logs, system restore points
Mobile Forensics	Smartphones, tablets	Call logs, SMS, app data, GPS traces, SIM card info

Introduction to Digital Forensics

Category	Typical Sources	Common Artifacts
Network Forensics	Routers, firewalls, IDS/IPS	Packet captures, flow records, VPN logs
Cloud Forensics	SaaS, IaaS platforms	API logs, storage buckets, virtual machine snapshots
IoT Forensics	Smart cameras, wearables	