

No. 121

CYBERSECURITY

Digital Forensics

Collecting and analysing digital evidence the right way



oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 121

Digital Forensics

Collecting and analysing digital evidence the right way

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Digital Forensics
Collecting and analysing digital evidence the right way

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product and tool names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What digital forensics is 5
2 Uses 6
3 Principles 7
4 The forensic process 8
5 Order of volatility 9
6 Chain of custody 10
7 Legal considerations 11
8 Roles 12
9 First responder do's and don'ts 13

PART II · SOURCES OF EVIDENCE

10 Computers and disks 15
11 File systems 16
12 Windows artifacts 17
13 macOS and Linux 18
14 Memory forensics 19
15 Network forensics 20
16 Email evidence 21
17 Mobile devices 22
18 Cloud forensics 23
19 Logs 24
20 Microsoft 365, Google Workspace and SaaS 25

PART III · ANALYSIS

21 Timelines 27
22 Malware triage 28
23 The limits of attribution 29

FREE SAMPLE · ojayo.com

24 Investigating business email compromise 30
25 Tools 31
26 Anti-forensics 32
27 AI and automation 33
28 Reporting 34
29 Presenting findings 35

PART IV · IN PRACTICE

30 Forensics in incident response 37
31 Forensic readiness 38
32 Building a practice lab 39
33 Careers 40
34 Common mistakes 41
35 Ethics 42
36 A worked example 43
37 Bringing it together 44
Checklists 45
Glossary 46
Further reading 47

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Digital forensics is the science of collecting, preserving and analysing digital evidence so that it can answer questions reliably: What happened? When? Who was involved? What data was affected? It supports incident response, internal investigations, insurance claims and court cases.

This book introduces digital forensics for beginners. It explains core principles such as preservation and chain of custody, where evidence lives on computers, in memory, on networks, phones and in the cloud, how analysts build timelines, and how findings are reported. It focuses on legitimate investigations by authorized people.

What this book covers

- What digital forensics is and the principles that make evidence trustworthy.
- The forensic process from identification to reporting.
- Disk, memory, network, email, mobile and cloud evidence.
- Common artifacts, timelines and tools.
- Forensics in incident response, legal considerations and forensic readiness.

Who this book is for

- **Security analysts and incident responders** starting out.
- **IT staff** who may need to preserve evidence.
- **Students** considering a forensics career.
- **Managers** who commission investigations.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–9): what forensics is, uses, principles, the process, order of volatility, chain of custody, legal considerations, roles, and first responders.
- **Part II — Sources of evidence** (Chapters 10–20): computers and disks, file systems, Windows artifacts, macOS and Linux, memory, network, email, mobile, cloud, logs, and SaaS platforms.
- **Part III — Analysis** (Chapters 21–29): timelines, malware triage, attribution limits, a business email compromise investigation, tools, anti-forensics, AI and automation, reporting, and presenting findings.
- **Part IV — In practice** (Chapters 30–37): forensics in incident response, readiness, labs, careers, common mistakes, ethics, a worked example, and a plan.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in a real investigation.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on law and screens

Rules on evidence and privacy differ between countries; seek legal advice before investigations involving people or legal action. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what digital forensics is and the principles that make digital evidence reliable.

FREE SAMPLE · ojayo.com

CHAPTER 1

What digital forensics is

Forensics answers questions with evidence.

A definition

Digital forensics applies scientific methods to identify, preserve, collect, analyse and report on digital evidence in a way that is reliable and repeatable.

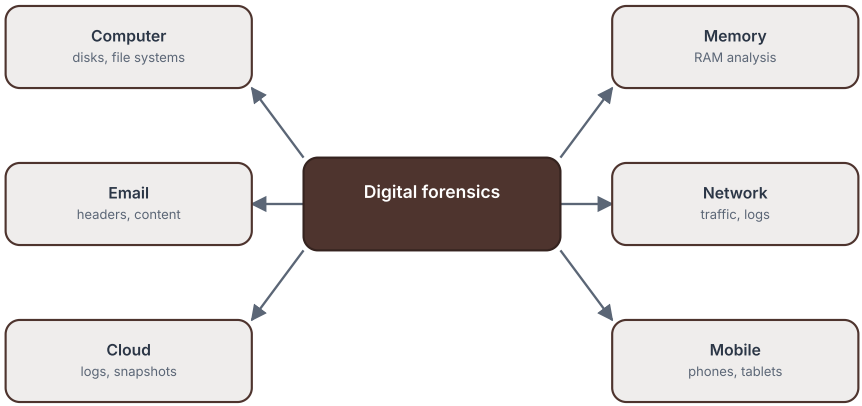


Figure 1.1 Branches of digital forensics

Evidence everywhere

Almost every action leaves digital traces: log entries, file timestamps, registry changes, network records, cloud audit trails, messages.

> **KEY IDEA**
> The goal is not just to find answers but to be able to prove them.

FREE SAMPLE · ojayo.com

CHAPTER 2

Uses

Forensics supports many kinds of investigation.

- **Incident response**: how attackers got in and what they did.
- **Data breach assessment**: what data was accessed, for notification decisions.
- **Internal investigations**: policy violations, fraud, data theft by insiders.
- **Litigation and e-discovery**: evidence for legal disputes.
- **Law enforcement**: criminal cases.
- **Insurance**: supporting claims.

FREE SAMPLE · ojayo.com

CHAPTER 3

Principles

A few principles make evidence trustworthy.

- **Preserve the original**: work on copies, not the original evidence.
- **Document everything**: who, what, when, how.
- **Verify integrity**: use cryptographic hashes to prove evidence has not changed.
- **Be repeatable**: another examiner should reach the same result.
- **Stay objective**: follow the evidence, including what contradicts your theory.

Hashes prove integrity

```
import hashlib

def sha256_of(path, chunk_size=1024 * 1024):
    h = hashlib.sha256()
    with open(path, "rb") as f:
        while chunk := f.read(chunk_size):
            h.update(chunk)
    return h.hexdigest()
```

If the hash of a copy matches the hash of the original, they are identical.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics (you are reading this)
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Digital Forensics

Enjoyed it? The full book has 52 pages and 37 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.