HANDS-ON VIRTUAL LAB COURSE

Digital Forensics Essentials

From Evidence to Courtroom

Practical digital-evidence literacy for law enforcement and legal professionals. Understand what digital forensics is, how it works, and how it holds up in court — through plain-language instruction, real-world case studies, and hands-on labs in a safe virtual environment. No technical background required.

12	22–26	19	Tier 1	Zero
MODULES	HOURS OF INSTRUCTION	HANDS-ON LAB EXERCISES	FOUNDATIONAL LEVEL	SETUP — LABS RUN ONLINE

FOUR MODERN EVIDENCE DOMAINS

Digital evidence is no longer just computer files. This course goes deep on the four domains investigators encounter most — each explored through guided, hands-on exercises with industry-standard forensic tools.

Mobile Devices

Smartphones and tablets: extraction levels, app data, encryption challenges, and cloud-linked evidence.

Video Evidence

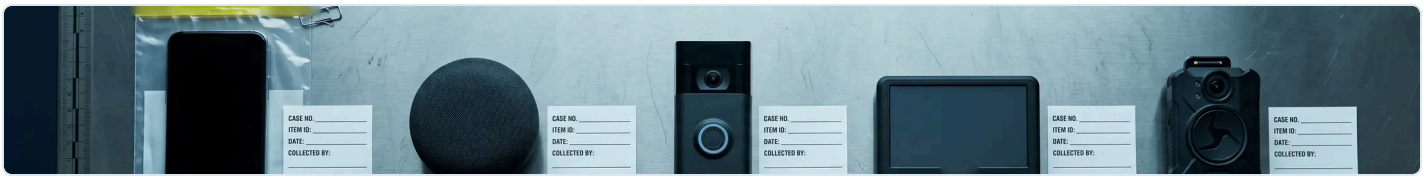
CCTV, body cameras, and dashcams: metadata analysis, timestamps, and proving footage hasn't been altered.

IoT & Smart Devices

Smart speakers, video doorbells, and home automation: what they record and where the data actually lives.

Vehicle & Location Data

License plate readers, GPS tracking, cell tower analysis, and the legal standards that govern them.



Plus — AI & emerging technology: deepfake detection, AI-assisted evidence analysis, and the ethical and admissibility questions raised by AI-generated content.

WHO THIS COURSE IS FOR

Built for every professional who touches digital evidence — from the first officer on scene to the attorney arguing admissibility.

- Patrol Officers & First Responders
- Detectives & Investigators
- Prosecutors
- Defense Attorneys
- Judges & Magistrates
- Forensic Paralegals
- Legal Tech & eDiscovery Professionals
- Fraud & Insurance Investigators
- Aspiring Forensics Students

WHY DFE-101

Plain-Language Instruction

Technical concepts explained for legal audiences — no computer science degree needed.

Grounded in Real Case Law

Landmark decisions — *Carpenter*, *Daubert*, *Frye* — woven throughout the course.

Courtroom-Ready Skills

Warrant templates, authentication procedures, and a courtroom simulation exercise.

Digital Forensics Essentials: From Evidence to Courtroom

DFE-101

WHAT YOU'LL LEARN

- ✓ Explain what digital forensics is and why it matters in modern investigations
- ✓ Apply the legal frameworks governing digital evidence — Fourth Amendment, ECPA, SCA
- ✓ Draft warrant language for smartphones, cloud services, IoT devices, and location data
- ✓ Anticipate common defense challenges to digital evidence — and how to mitigate them
- ✓ Identify digital evidence across mobile, video, IoT, and location-data domains
- ✓ Follow proper first-responder protocols for digital evidence at a crime scene
- ✓ Evaluate how digital evidence is authenticated and presented in court
- ✓ Assess the impact of AI and deepfakes on digital evidence reliability

COURSE MODULES

1. Introduction to Digital Forensics
2. The Digital Evidence Landscape
3. Legal Frameworks for Digital Evidence
4. First Responder Protocols
5. Mobile Device Evidence
6. Video Evidence
7. IoT and Smart Device Evidence
8. Vehicle Tracking and Location Data
9. Drafting Warrants for Digital Evidence
10. AI & Emerging Technology in Forensics
11. Digital Evidence in the Courtroom
12. Comprehensive Review & Case Simulation

LEARN BY DOING

Guided Labs

Step-by-step exercises with expected outputs and progressive hints — build skills with confidence on your first pass.

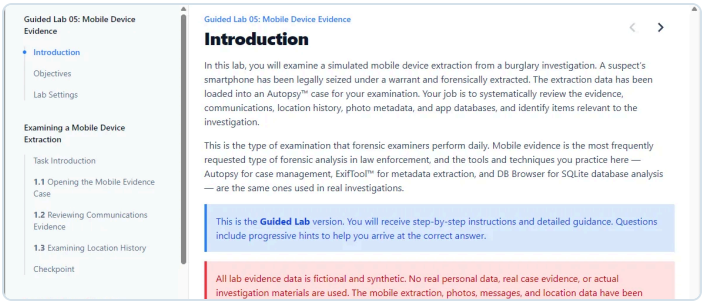
Applied Labs

The same scenarios with the training wheels off — high-level objectives that verify you can work independently.

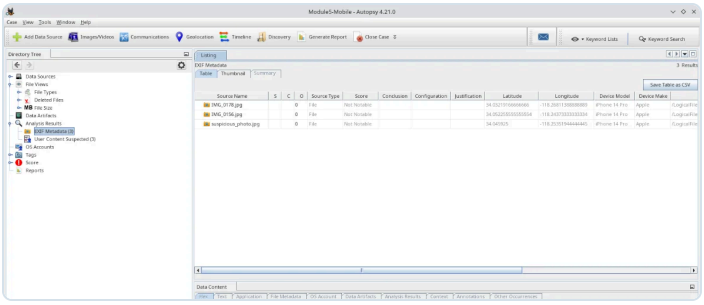
Capstone: The Riverside Case

An end-to-end simulated investigation spanning mobile, video, IoT, and location evidence — automatically graded.

Industry-standard tools, pre-installed and ready: Autopsy, ExifTool, MediaInfo, VLC, DB Browser for SQLite, GIMP, and a full Linux forensic workstation — all in a fully sandboxed virtual lab. Nothing to install, nothing to break.



Guided lab instructions, right in the browser



Autopsy examining evidence in the virtual lab

CERTIFICATION & FRAMEWORK ALIGNMENT

MAPS TO FOUNDATIONAL OBJECTIVES FROM

- IACIS CFCE
- ISFCE CCE
- CompTIA Security+ (SY0-701)
- GIAC GCFE
- EC-Council CHFI

ALIGNED WITH INDUSTRY FRAMEWORKS

- NICE Workforce Framework
- NIST SP 800-86
- SWGDE Standards
- DOJ Electronic Evidence Guidance

Prerequisites — just the basics. No prior technical or forensics experience required. If you can navigate a desktop, open files, and use a web browser, you're ready. Familiarity with the criminal justice system helps, but isn't required.

All product names, logos, and brands are property of their respective owners. All lab evidence data is fictional.