

Digital Forensics Investigation Operations Course

16 – 20 May 2027
Chicago

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Digital Forensics Investigation Operations Course

Ref: 430_134804 **Date:** 16 – 20 May 2027 **Location:** Chicago **Fees:** 12000 Euro

Overview

Digital Forensics Investigation Operations Course is a one-week professional course for investigators, compliance, internal audit, security operations, legal support, and incident response teams, who leave with a Digital Investigation Case File. Participants control digital evidence preservation, chain of custody, forensic imaging, artifact examination, timeline reconstruction, analysis documentation, and defensible reporting. Agile Leaders Training Center delivers this digital forensics investigation course.

Who Should Attend

- Teams responsible for internal, fraud, misconduct, or security investigations
- Functions responsible for digital evidence preservation and custody
- Audit and compliance teams responsible for evidence-based reviews
- Security operations teams responsible for incident investigation support
- Legal support teams responsible for reviewing technical evidence and reports

The course assumes participants handle investigation records or technology incidents and leaves out offensive hacking and certification exam preparation.

Departments and Industries

The course supports functions that preserve, examine, document, and report digital evidence across sectors.

- Internal audit, compliance, and corporate investigations
- Banking, insurance, and professional services
- Technology, telecommunications, and security operations
- Healthcare, education, and public services
- Legal, human resources, and incident response functions

Learning Objectives

By the end of this course, participants will be able to:

- Apply a controlled digital investigation scoping process
- Use evidence preservation and chain-of-custody controls
- Build an acquisition plan and verify forensic images
- Analyze file-system artifacts and reconstruct event timelines
- Evaluate findings, limitations, and alternative explanations
- Create a defensible digital investigation case file

AGILE LEADERS
Training Center

Course Agenda

Day 1: Investigation Scope and Evidence Control

- Digital Investigation Intake and Scope Brief
- Evidence Source and Custodian Map
- ISO/IEC 27037:2012 Evidence Handling Lifecycle
- Digital Evidence Risk and Priority Matrix
- Investigation Authority and Boundary Record

Day 2: Preservation and Acquisition

- Digital Evidence Preservation Plan
- Chain-of-Custody Evidence Register
- Volatile and Nonvolatile Data Decision Tree
- Forensic Imaging Acquisition Worksheet
- Hash Verification and Integrity Log

Day 3: Examination and Triage

- Forensic Copy Examination Workflow
- File-System Artifact Triage Matrix
- Deleted and Hidden Data Review Method
- User Activity Artifact Correlation Table
- Examination Notes and Tool Output Register

Day 4: Analysis and Reporting

- Event Timeline Reconstruction Method
- Evidence-to-Hypothesis Analysis Matrix
- Finding Confidence and Limitation Record
- Peer Review and Quality Control Checklist
- Defensible Digital Forensics Report Structure

Day 5: Digital Investigation Case Practice

- Exercise: Investigation Scope Review
- Exercise: Evidence Preservation and Custody Test
- Exercise: Forensic Image Integrity Challenge
- Exercise: Artifact and Timeline Analysis
- Capstone Digital Investigation Case File

Practical Exercises

The course includes the following suggested activities:

- Suggested activity: define investigation questions, boundaries, sources, and preservation priorities for a workplace case
- Suggested activity: document evidence transfer and verify a forensic image against recorded hash values
- Suggested activity: correlate file-system and user activity artifacts into an event timeline
- Suggested activity: prepare findings, limitations, and supporting exhibits for technical and nontechnical reviewers

Frequently Asked Questions

Who suits the Digital Forensics Investigation Operations Course?

It suits investigation, compliance, audit, security operations, legal support, and incident response teams and assumes experience with investigation records or technology incidents.

How does digital forensics investigation differ from incident response?

Digital forensics investigation preserves and examines evidence to answer defined questions, while incident response focuses on containing disruption, restoring services, and coordinating operational recovery.

Why is chain of custody important in digital forensics investigation?

Chain of custody records who controlled evidence, when transfers occurred, what actions were performed, and how evidence integrity was maintained throughout the investigation.

How are forensic images verified during digital evidence examination?

Forensic images are verified by recording and comparing hash values, documenting acquisition conditions, preserving the source, and examining a controlled working copy.

What is the main output of digital forensics investigation operations?

The main output is a Digital Investigation Case File containing scope, evidence records, acquisition details, integrity checks, examination notes, timelines, findings, limitations, and a defensible report.

Conclusion

Participants take back a Digital Investigation Case File and supporting evidence-control artifacts. These products replace fragmented technical notes with a traceable record of scope, custody, acquisition, examination, analysis, and findings. They also clarify evidence integrity, review points, limitations, and the basis for defensible reporting.