Mobile Device Forensics Evidence Training Course

21 – 25 June 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Mobile Device Forensics Evidence Training Course

Ref: 753_223971 **Date:** 21 – 25 June 2027 **Location:** Addis Ababa **Fees:** 4500 Euro

Overview

Mobile Device Forensics Evidence Training Course is a one-week intermediate course for digital forensics practitioners, incident responders, investigators, security analysts, mobile-device administrators, and legal support functions who leave with a Mobile Evidence Examination File. Participants connect lawful authority, evidence preservation, acquisition strategy, Android and iOS artifacts, application and communication evidence, timeline analysis, validation, and reporting through traceable case decisions. Agile Leaders Training Center develops mobile device forensics evidence practice.

Who Should Attend

- Digital evidence functions responsible for acquiring and examining mobile-device data
- Incident response functions responsible for preserving devices and supporting investigations
- Investigation functions responsible for connecting device artifacts to case questions
- Mobile administration functions responsible for device states, backups, and synchronized data
- Legal and audit support functions responsible for evidence records and review readiness

The course assumes participants handle security evidence, device records, or investigative procedures at work, and leaves out exploit development, passcode bypass instruction, certification preparation, and legal advice.

Departments and Industries

The course supports departments and industries that examine mobile evidence for authorized investigations and incident response.

- Digital forensics and incident response
- Cybersecurity operations and internal investigations
- Legal, audit, and compliance support
- Financial services and telecommunications
- Healthcare, industrial operations, and digital services

Learning Objectives

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

- Apply authorization, preservation, and chain-of-custody controls to mobile evidence
- Compare logical, file-system, backup, external-media, and cloud acquisition options
- Analyze Android and iOS artifacts against defined case questions
- Build communication, application, location, and activity timelines
- Evaluate tool output through validation and peer review
- Build a Mobile Evidence Examination File with defensible findings

Course Agenda

Day 1: Authorize and Preserve Mobile Evidence

- Examination Authority and Scope Record
- Device State and Scene Documentation Sheet
- Evidence Identifier and Chain-of-Custody Log
- Powered-On and Powered-Off Preservation Decision Tree
- Network Isolation and Evidence Integrity Checklist

Day 2: Plan and Validate Acquisition

- Logical, Backup, and File-System Acquisition Matrix
- External Media and Synchronized Source Map
- Device Model, Operating System, and Access Profile
- Acquisition Tool Testing and Validation Record
- Extraction Method Rationale and Exception Log

Day 3: Examine Android Evidence

- Android Storage and Application Artifact Map
- Call, Message, Contact, and Account Correlation Sheet
- Browser, Location, and Media Metadata Review
- Application Database and Timestamp Interpretation Method
- Android Finding Verification Worksheet

Day 4: Examine iOS and Connected Evidence

- iOS Backup and File-System Artifact Map
- Application, Communication, and Notification Evidence Review
- Cloud, Computer, Wearable, and Synchronization Source Register
- Cross-Source Timeline and Attribution Matrix
- Finding Limitation and Alternative Explanation Test

Day 5: Practice Mobile Evidence Reporting

- Exercise: Preserve and Document a Mobile Device Scenario
- Exercise: Select and Justify an Acquisition Strategy
- Exercise: Correlate Android and iOS Artifact Timelines
- Exercise: Validate Findings and Record Limitations
- Capstone: Mobile Evidence Examination File

Practical Exercises

The course uses suggested activities based on financial services, telecommunications, healthcare, industrial operations, and digital services.

- Suggested activity: record authority, device state, isolation choices, and chain of custody for a seized handset.
- Suggested activity: compare acquisition options and document the selected method, validation checks, and exceptions.
- Suggested activity: correlate application, communication, location, and media artifacts into a case timeline.
- Suggested activity: prepare findings, limitations, peer-review notes, and a traceable examination report.

FAQs

Who suits mobile device forensics evidence training, and what does it assume?

Digital evidence, incident response, investigation, security analysis, mobile administration, legal, and audit support functions suit the course; it assumes experience with security evidence, device records, or investigative procedures.

How does mobile device forensics training differ from general digital forensics training?

Mobile device forensics training concentrates on handset states, mobile operating systems, application artifacts, synchronized sources, acquisition choices, and device-specific validation, while general digital forensics spans a broader range of computers, storage, networks, and cloud systems.

How should a mobile evidence acquisition method be selected?

A mobile evidence acquisition method should be selected by comparing authority, device state, operating system, access conditions, available tools, required artifacts, risk of alteration, validation options, and documented case needs.

AGILE LEADERS
Training Center

Why must mobile forensics tool output be validated?

Mobile forensics tool output must be validated because parsers can omit, mislabel, or misinterpret artifacts; examiners should compare source data, timestamps, alternative tools or methods, and peer-review findings where appropriate.

What belongs in a Mobile Evidence Examination File?

A Mobile Evidence Examination File contains authority and scope, device condition, custody records, acquisition rationale, validation results, artifact notes, timelines, findings, limitations, review records, and a report that traces conclusions to evidence.

Conclusion

Participants take back a Mobile Evidence Examination File that connects authority, preservation, acquisition, analysis, validation, and reporting. It changes disconnected tool output into a traceable examination record. The file supports reviewable findings, explicit limitations, controlled handovers, and consistent case communication.