



Forensic Incident Response and Evidence Preservation Training Course

19 – 23 September 2027
Nairobi

Forensic Incident Response and Evidence Preservation Training Course

Ref: 760_157851 **Date:** 19 – 23 September 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Forensic Incident Response and Evidence Preservation Training Course is a five-day intermediate course for incident responders, SOC analysts, forensics practitioners, security operations staff, and investigation coordinators who leave with a Forensic Incident Response Casebook. Participants integrate forensic readiness, volatile-data priorities, evidence preservation, event correlation, containment choices, recovery validation, and defensible handover during active incidents. The course balances operational response speed with evidence integrity. Agile Leaders Training Center develops forensic incident response and evidence preservation practice.

Who Should Attend

- Incident response functions responsible for triage, containment, recovery, and coordination
- Security operations functions responsible for escalating alerts and preserving investigation context
- Digital forensics functions responsible for evidence integrity, analysis, and traceability
- Technology operations functions responsible for system access, restoration, and validation
- Investigation coordination functions responsible for scope, documentation, and handover

The course assumes participants support cybersecurity incidents, monitoring, system administration, or digital investigations, and leaves out criminal prosecution, malware reverse engineering, mobile-device specialization, certification preparation, and exam coaching.

Departments and Industries

The course supports departments and industries that must respond to incidents without losing digital evidence.

- Cybersecurity operations, incident response, and digital investigations
- Information technology, resilience, risk, and internal assurance
- Financial services and healthcare
- Energy, industrial operations, and telecommunications
- Public services, education, and digital platforms

Learning Objectives

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



- Apply incident-response and forensic-readiness decision criteria
- Prioritize volatile, persistent, network, and application evidence
- Use preservation, acquisition, custody, and integrity records
- Analyze indicators and artifacts into a defensible event timeline
- Evaluate containment and recovery actions against evidential impact
- Build a Forensic Incident Response Casebook

Course Agenda

Day 1: Establish Forensic Response Readiness

- NIST SP 800-61 Rev. 3 Response Consideration Map
- NIST SP 800-86 Forensic Integration Lifecycle
- Incident Authority, Scope, and Escalation Matrix
- Forensic Readiness and Evidence Source Register
- Response Role and Chain-of-Custody Assignment

Day 2: Preserve Live Incident Evidence

- Volatile Data Collection Priority Matrix
- System, Network, and Application Evidence Source Map
- Live Acquisition Risk and Feasibility Checklist
- Evidence Integrity and Cryptographic Hash Record
- Preservation, Custody, and Transfer Documentation Pack

Day 3: Triage and Reconstruct Events

- Forensic Triage Question and Hypothesis Board
- Indicator, Artifact, and Source Correlation Matrix
- Timestamp Normalization and Event Sequencing Method
- Cross-System Incident Timeline Reconstruction Board
- Contradiction, Gap, and Evidential Weight Register

Day 4: Balance Containment and Recovery

- Containment Action and Evidence Impact Matrix
- Isolation, Shutdown, and Monitoring Decision Tree
- Eradication Change and Evidence Traceability Log
- Recovery Validation and Residual Indicator Checklist
- Findings, Limitations, and Handover Report Template



Day 5: Practice Forensic Incident Response

- Exercise: Scope an Incident and Assign Evidence Priorities
- Exercise: Preserve Volatile and Persistent Evidence
- Exercise: Reconstruct a Cross-Source Incident Timeline
- Exercise: Defend Containment and Recovery Decisions
- Capstone: Forensic Incident Response Casebook

Practical Exercises

The course uses suggested activities based on financial services, healthcare, energy, telecommunications, and digital platforms.

- Suggested activity: triage an active compromise and rank evidence sources before containment changes the environment.
- Suggested activity: record acquisition, integrity, custody, and transfer decisions for volatile and persistent evidence.
- Suggested activity: correlate system, network, and application artifacts into a timeline with gaps and contradictions.
- Suggested activity: present containment, recovery validation, limitations, and a defensible operational handover.

FAQs

Who suits forensic incident response training, and what does it assume?

Incident response, security operations, digital forensics, technology operations, and investigation coordination functions suit the course; it assumes practical involvement with incidents, monitoring, systems, or digital evidence.

How does forensic incident response differ from general computer forensics training?

Forensic incident response preserves and analyzes evidence while an incident is being contained and recovered, while general computer forensics training focuses more broadly on post-event acquisition and examination of computing artifacts.

Which evidence should forensic incident response preserve first?

Forensic incident response should prioritize evidence by volatility, investigative value, collection feasibility, business impact, legal authority, and the risk that containment or recovery will alter or destroy it.



How should containment decisions protect digital evidence?

Containment decisions should document the action, purpose, timing, affected systems, expected evidence impact, alternatives considered, approvals, preserved data, integrity checks, and resulting changes to the investigation timeline.

How is recovery validated during forensic incident response?

Recovery is validated by checking restored assets, residual indicators, account and access changes, control operation, monitoring coverage, known persistence paths, business functionality, and traceability to the incident findings.

Conclusion

Participants take back a Forensic Incident Response Casebook connecting authority, evidence priorities, preservation, timeline analysis, containment, recovery validation, and handover. It changes competing response and investigation actions into traceable operational decisions. The casebook supports evidence integrity, faster coordination, reasoned tradeoffs, peer review, and defensible communication of findings and limitations.