



Cybercrime Case Investigation and Digital Policing Training Course

31 January – 4 February 2027
Johannesburg

Cybercrime Case Investigation and Digital Policing Training Course

Ref: 766_158299 **Date:** 31 January – 4 February 2027 **Location:** Johannesburg **Fees:** 4500 Euro

Overview

Cybercrime Case Investigation and Digital Policing Training Course is a five-day intermediate course for digital policing officers, cybercrime investigators, analysts, and public-sector incident staff who leave with a Cybercrime Case Development File. Participants structure case intake, harm framing, online trace triage, investigative hypotheses, victim and platform coordination, lawful preservation, documentation, escalation, and handover. The course separates case development from laboratory forensic examination and enterprise incident response. Agile Leaders Training Center develops cybercrime case investigation practice.

Who Should Attend

- Digital policing functions responsible for receiving and developing online crime cases
- Cybercrime investigation functions responsible for hypotheses and investigative actions
- Law-enforcement analysis functions responsible for organizing digital traces
- Victim-support functions responsible for statements, harm, and safeguarding coordination
- Public-sector incident functions responsible for lawful escalation and interagency handover

The course assumes participants can document cases and follow authorized procedures, and leaves out laboratory imaging, device extraction, malware analysis, covert operations, and certification preparation.

Departments and Industries

The course supports departments and industries that investigate or coordinate cyber-enabled crime.

- Cybercrime units, digital policing, and criminal investigation
- Public prosecution liaison and electronic evidence coordination
- Financial crime and fraud investigation
- Telecommunications and online service provider liaison
- Public services, education, and victim-support functions

Learning Objectives

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

- Apply a structured cybercrime case-intake method
- Analyze harm, actors, accounts, events, and online traces
- Build testable investigative hypotheses and action plans
- Use lawful preservation and platform-request planning records
- Evaluate evidence continuity and case-document quality



- Build a Cybercrime Case Development File

Course Agenda

Day 1: Frame the Cybercrime Case

- Cybercrime Report Intake and Triage Form
- Offense, Harm, and Urgency Framing Matrix
- Victim and Witness Safeguarding Checklist
- Case Scope and Jurisdiction Question Set
- Initial Action and Referral Decision Tree

Day 2: Organize Online Traces

- Account, Device, and Service Relationship Map
- Online Event Timeline Construction Method
- Electronic Trace Relevance Classification Card
- Source Reliability and Corroboration Matrix
- Trace Preservation Priority Register

Day 3: Develop Investigative Hypotheses

- Actor, Means, Motive, and Opportunity Canvas
- Competing Hypothesis Comparison Table
- Investigative Question and Action Log
- Evidence Gap and Dependency Map
- Case Direction Review Gate

Day 4: Coordinate Evidence and Handover

- Platform Preservation Request Planning Sheet
- Service Provider Liaison Record
- Electronic Evidence Continuity Log
- Interagency Escalation and Responsibility Map
- Prosecutor-Ready Case Handover Index

Day 5: Practice Digital Case Development

- Exercise: Triage a Cybercrime Report
- Exercise: Build an Online Trace Timeline
- Exercise: Test Competing Investigative Hypotheses
- Exercise: Prepare Preservation and Handover Records
- Capstone: Cybercrime Case Development File

Practical Exercises

The course uses suggested activities based on payment fraud, account abuse, online harassment, and service disruption cases.

- Suggested activity: classify a report by harm, urgency, safeguarding need, and referral path.
- Suggested activity: map accounts, services, communications, and events into an online trace timeline.
- Suggested activity: compare hypotheses against supporting, conflicting, and missing evidence.
- Suggested activity: assemble preservation, continuity, coordination, and handover records into a case file.

FAQs

Who suits cybercrime case investigation training, and what does it assume?

Digital policing officers, cybercrime investigators, analysts, and public-sector incident staff suit the training; it assumes participants can document cases and follow authorized procedures.

How does cybercrime case investigation differ from digital forensic laboratory training?

Cybercrime case investigation structures reports, hypotheses, online traces, coordination, preservation, and handover, while laboratory training concentrates on technical acquisition, processing, examination, and reporting from devices or media.

What should a cybercrime case-intake record contain?

A case-intake record should contain the report source, alleged conduct, harm, affected people and services, urgency, safeguarding needs, available traces, preservation risks, jurisdiction questions, immediate actions, and referral decision.

How should investigators build cybercrime hypotheses?

Investigators should connect actors, means, motive, opportunity, accounts, devices, services, and events, then compare each hypothesis against supporting, conflicting, and missing evidence before selecting further actions.

What belongs in a cybercrime case handover?

A case handover should contain scope, chronology, hypotheses, action history, evidence index, continuity records, preservation activity, victim coordination, provider liaison, outstanding requests, legal considerations, risks, and recommended next actions.



Conclusion

Participants take back a Cybercrime Case Development File connecting intake, harm framing, trace maps, hypotheses, preservation actions, continuity records, and handover materials. It changes fragmented digital reports into a structured investigative workflow. The file supports defensible decisions, clearer coordination, protected evidence, and case transfer without duplicating laboratory forensic work.