

Open Source Intelligence Investigation and Verification Course

15 – 19 November 2026
Cape town

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Open Source Intelligence Investigation and Verification Course

Ref: 449_264734 **Date:** 15 – 19 November 2026 **Location:** Cape town **Fees:** 4500 Euro

Overview

Open Source Intelligence Investigation and Verification Course is a one-week intermediate-to-advanced course for investigators, intelligence analysts, compliance and fraud teams, security functions, journalists, and researchers, who leave with an auditable OSINT Case File. The course connects lawful investigation planning, open-source discovery, entity resolution, web and social evidence, geolocation, chronology, content verification, collection integrity, analytical assessment, and reporting. Agile Leaders Training Center delivers practical open source intelligence investigation training.

Who Should Attend

- Investigation functions responsible for lawful online inquiries and evidence documentation
- Intelligence functions responsible for source discovery, assessment, and analytical reporting
- Compliance and fraud functions responsible for due diligence, alerts, and case escalation
- Corporate security functions responsible for threat, incident, and integrity inquiries
- Journalism and research functions responsible for verifying public claims and digital content
- Assurance functions responsible for reviewing investigation methods and records

The course assumes participants already conduct research, investigations, due diligence, or evidence review and leaves out hacking, credential abuse, malware, covert access, and jurisdiction-specific legal advice.

Departments and Industries

The course supports departments that conduct lawful online investigations and assess publicly available information across public-interest and commercial settings.

- Investigation, intelligence, security, and fraud departments
- Compliance, due diligence, risk, and internal-audit functions
- Newsrooms, research organizations, and civil-society teams
- Financial services, insurance, and professional-services organizations
- Technology, telecommunications, logistics, and platform businesses
- Legal support, corporate affairs, and reputation-risk functions

Learning Objectives

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

- Apply a lawful OSINT investigation cycle
- Use search, archive, and source-discovery methods
- Build identity, entity, and relationship assessments
- Analyze imagery, location, chronology, and online claims
- Evaluate source reliability, evidence integrity, and analytical confidence
- Build an auditable OSINT Case File

Course Agenda

Day 1: Investigation Scope and Controls

- OSINT Investigation Cycle and Decision Map
- Question, Hypothesis, and Collection Plan
- Lawful Source and Ethical Boundary Checklist
- Investigator Safety and Exposure Risk Register
- Case Log and Audit Trail Standard

Day 2: Discovery and Entity Resolution

- Advanced Search Operator Query Matrix
- Web Archive and Change Timeline Method
- Public Record and Domain Evidence Register
- Identity Attribute and Alias Resolution Grid
- Entity Relationship and Network Mapping Canvas

Day 3: Content Verification and Location

- Source Provenance and Reliability Assessment
- Reverse Image and Video Search Workflow
- Visual Landmark and Geolocation Evidence Sheet
- Timestamp, Shadow, and Chronology Analysis
- Claim Corroboration and Contradiction Matrix

Day 4: Evidence and Analytical Reporting

- Digital Collection and Preservation Record
- Metadata Relevance and Limitation Checklist
- Evidence Integrity and Handling Log
- Competing Hypotheses Analysis Table
- Confidence Statement and Intelligence Report Template

Day 5: OSINT Investigation Practice

- Suggested Exercise: Investigation Plan and Safety Review
- Suggested Exercise: Search, Archive, and Entity Resolution
- Suggested Exercise: Image, Location, and Chronology Verification
- Suggested Exercise: Evidence and Confidence Assessment
- Capstone Exercise: Auditable OSINT Case File

Practical Exercises

The course uses suggested activities to connect investigation questions, public sources, verification evidence, and defensible findings.

- Suggested activity: convert a case question into hypotheses, collection priorities, ethical limits, and a traceable case log.
- Suggested activity: resolve aliases and entities across public web, archive, domain, and social evidence.
- Suggested activity: test imagery, location, time, provenance, and contradictory claims before reaching a finding.
- Suggested activity: assemble collected evidence, alternative explanations, confidence judgments, and reporting records into the capstone file.

FAQs

Who suits open source intelligence investigation training, and what does it assume?

Open source intelligence investigation training suits professionals who already conduct research, casework, due diligence, verification, or evidence review and need a repeatable lawful online investigation method.

How does OSINT investigation training differ from digital forensics training?

OSINT investigation training works with lawfully accessible public information, while digital forensics training focuses on acquiring and examining devices, systems, or stored data under separate technical and legal controls.

How is source reliability evaluated in an OSINT investigation?

Source reliability is evaluated through provenance, access path, independence, consistency, corroboration, motive, context, technical limitations, and the distinction between what the source shows and what the analyst infers.

How do geolocation and chronology support online investigation verification?

Geolocation and chronology test where and when content was created by comparing landmarks, terrain, shadows, weather, transport, archived pages, timestamps, and independent reference material.

AGILE LEADERS
Training Center

What makes an OSINT Case File auditable?

An OSINT Case File is auditable when it records questions, searches, sources, collection times, preserved items, verification steps, analytical alternatives, confidence judgments, limitations, and reporting decisions.

Conclusion

Participants take back an auditable OSINT Case File containing plans, search records, entity maps, verification sheets, preserved evidence, hypothesis tests, confidence statements, and findings. The file changes scattered online material into a traceable investigation record. It supports reviewable decisions, transparent limitations, and consistent reporting.