Certified Computer Forensics Training Course: Investigate & Secure Digital Evidence

12 – 16 July 2027
Amsterdam

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Certified Computer Forensics Training Course: Investigate & Secure Digital Evidence

Ref: 103600303_99212 **Date:** 12 – 16 July 2027 **Location:** Amsterdam **Fees:** 6500 Euro

Course Overview:

The Certified Computer Forensics Training Course: Investigate & Secure Digital Evidence is designed to equip professionals with the necessary skills to analyze, investigate, and secure digital evidence in legal and corporate environments. With the rise of cybercrime, digital forensics has become an essential practice for identifying security threats, recovering lost data, and preventing unauthorized system access. This course covers computer forensics, cyber forensics, digital forensics, forensic investigation, and cybersecurity forensics to provide participants with hands-on training in analyzing cyber threats and legal aspects of digital evidence.

Through this program, participants will gain expertise in cybercrime investigation, data breach analysis, network forensics, and cyber threat intelligence to strengthen organizational security postures. The course provides practical knowledge on mobile forensics, cloud forensics, and encryption techniques to help professionals handle sophisticated cyberattacks. By the end of this course, attendees will have a deep understanding of digital forensic tools and techniques, enabling them to conduct forensic investigations and assist in cybersecurity incident response.

Target Audience:

- IT Security Professionals
- Cybersecurity Analysts
- Digital Forensics Investigators
- Law Enforcement Officers
- IT Managers & Compliance Officers
- Legal & Risk Management Professionals

AGILE LEADERS
Training Center

Targeted Organizational Departments:

- IT Security & Cybersecurity Teams
- Risk & Compliance Departments
- Fraud Investigation Units
- Law Enforcement & Legal Teams
- Corporate IT & Digital Asset Protection Teams

Targeted Industries:

- Financial Services & Banking
- Law Enforcement & Government Agencies
- Healthcare & Pharmaceuticals
- Telecommunications & IT Services
- E-Commerce & Retail

Course Offerings:

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

- Understand the role of computer forensics, digital evidence, and cybercrime investigation in cybersecurity.
- Implement network forensics techniques to detect and mitigate security incidents.
- Conduct forensic investigations using industry-leading tools and methodologies.
- Apply legal aspects of computer forensics in corporate and law enforcement settings.
-

Identify and recover compromised or lost data through data breach analysis.

Training Methodology:

This training course follows an interactive approach, combining case studies, hands-on lab exercises, and real-world cybercrime scenarios to enhance learning. Participants will be introduced to digital forensic tools and techniques, along with role-playing exercises and group discussions to encourage collaboration. Expert instructors will guide attendees through cyber forensic analyst job roles and best practices for securing digital assets. Assessments, feedback sessions, and simulations will ensure that participants can confidently apply their knowledge in practical settings.

Course Toolbox:

- Course Workbook & Study Guides
- Digital Forensic Tools Overview
- Case Study Scenarios & Investigative Exercises
- Legal & Compliance Reference Materials
- Online Resources & Practical Checklists

AGILE LEADERS
Training Center

Course Agenda:

Day 1: Introduction to Computer Forensics

- Topic 1: Understanding digital forensics and its role in cybersecurity
- Topic 2: The importance of digital evidence in forensic investigations
- Topic 3: Key forensic tools and techniques used in cybercrime investigation
- Topic 4: Steps in a forensic investigation and chain of custody procedures
- Topic 5: Legal and ethical considerations in computer forensics
- Reflection & Review: Discuss the day's key takeaways and address questions

Day 2: Conducting a Forensic Investigation

- Topic 1: Cybersecurity incident response and forensic analysis
- Topic 2: Data breach analysis and digital forensic investigation techniques
- Topic 3: How to extract digital evidence from computers and networks
- Topic 4: Network forensics: analyzing logs, traffic, and intrusion attempts
- Topic 5: Case study: Investigating a real-world cybercrime scenario
- Reflection & Review: Group discussion on investigation findings

AGILE LEADERS
Training Center

Day 3: Advanced Digital Forensic Techniques

- Topic 1: Cyber forensic analyst job roles and responsibilities
- Topic 2: Mobile forensics and investigating smartphones, tablets, and IoT devices
- Topic 3: Role of encryption in digital forensics and decryption methods
- Topic 4: Data recovery in forensic investigations: best practices and tools
- Topic 5: Cloud forensics and cyber investigation challenges
- Reflection & Review: Key learnings and case study discussions

Day 4: Legal Aspects and Reporting

- Topic 1: Computer forensics for law enforcement and corporate security
- Topic 2: Importance of forensic tools in cyber investigations
- Topic 3: Ethical principles in digital forensics and compliance standards
- Topic 4: Preparing digital forensic reports for legal proceedings
- Topic 5: Cyber forensics career opportunities and professional certifications
- Reflection & Review: Mock trial or report presentation exercise

AGILE LEADERS
Training Center

Day 5: Computer Forensics and Practical Application

- Topic 1: Investigating hacking incidents with forensics
- Topic 2: How to analyze cybercrime evidence and identify attack vectors
- Topic 3: Best computer forensics certification pathways and career planning
- Topic 4: How to prevent cybercrime using forensic techniques
- Topic 5: Final assessment and hands-on forensic investigation simulation
- Reflection & Review: Recap of key learnings and course conclusion

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

No formal prerequisites are required. However, a basic understanding of IT security, cybersecurity principles, or law enforcement processes is beneficial for participants.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is structured to last approximately 4-5 hours, including interactive exercises and Q&A sessions. The total course duration is 20-25 hours spread over five days.

How does this course prepare me for a career in digital forensics?

This course equips participants with technical skills, forensic tools, and investigative techniques required to pursue roles in cyber forensics, network forensics, law enforcement, and security analysis. It also provides insights into industry-recognized certifications.

How This Course is Different from Other Computer Forensics Courses:

The Certified Computer Forensics Training Course stands out from other similar programs by offering a comprehensive, hands-on approach to digital forensics. Unlike generic cybersecurity courses, this course delves deep into forensic investigation, cybercrime investigation, and legal compliance, providing participants with real-world case studies and hands-on forensic exercises.

AGILE LEADERS
Training Center

This course covers network forensics, mobile forensics, and cloud forensics, ensuring participants gain expertise in multiple digital environments. It also emphasizes the legal and ethical aspects of digital forensics, helping learners understand compliance requirements for corporate and law enforcement investigations.

Additionally, the course offers guidance on digital forensic certifications, cyber forensics career opportunities, and industry best practices, preparing participants for job roles such as cyber forensic analyst, digital forensic investigator, and forensic security specialist. By combining interactive exercises, simulations, and expert-led discussions, this course ensures participants leave with practical, applicable forensic skills that can be used immediately in their work environments.