Advanced Digital Evidence Acquisition and Preservation Training Course

Professional Development Training Course Outline

Category	Criminology	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected world, the landscape of cybercrime and digital incidents is constantly evolving, demanding highly specialized skills in digital forensics and incident response. Training Course on Advanced Digital Evidence Acquisition & Preservation is meticulously designed to equip professionals with cutting-edge techniques for digital evidence acquisition and forensically sound preservation. Participants will delve into advanced methodologies, tools, and best practices to effectively handle complex digital investigations, ensuring the integrity and admissibility of crucial evidence in legal and corporate settings.

This program goes beyond foundational concepts, focusing on live acquisition, cloud forensics, mobile device forensics, and anti-forensics countermeasures. Through practical, hands-on labs and real-world case studies, attendees will master the art of extracting, analyzing, and documenting digital artifacts from diverse sources, including enterprise networks, IoT devices, and encrypted systems. By the end of this course, participants will possess the expertise to confidently navigate challenging digital crime scenes, mitigate data breaches, and contribute significantly to organizational cyber resilience and threat intelligence.

Programme Curriculum

Advanced Digital Evidence Acquisition and Preservation Training Course

Introduction

In today's interconnected world, the landscape of cybercrime and digital incidents is constantly evolving, demanding highly specialized skills in digital forensics and incident response. Advanced Digital Evidence Acquisition and Preservation Training Course equips professionals with cutting-edge techniques for digital evidence acquisition and forensically sound preservation. Participants will delve into advanced methodologies, tools, and best practices to effectively handle complex digital investigations, ensuring the integrity and admissibility of crucial evidence in legal and corporate settings.

This program goes beyond foundational concepts, focusing on live acquisition, cloud forensics, mobile device forensics, and anti-forensics countermeasures. Through practical, hands-on labs and real-world case studies, attendees will master the art of extracting, analyzing, and documenting digital artifacts from diverse sources, including enterprise networks, IoT devices, and encrypted systems. By the end of this course, participants will possess the expertise to confidently navigate challenging digital crime scenes, mitigate data breaches, and contribute significantly to organizational cyber resilience and threat intelligence.

Course Duration

5 Days

Course Objectives

Master advanced digital evidence acquisition techniques for diverse platforms, including volatile memory and cutting-edge storage.

Implement forensically sound preservation strategies to maintain data integrity and chain of custody in complex scenarios.

Conduct in-depth cloud forensics investigations, addressing unique challenges of distributed data and legal jurisdictions.

Perform mobile device forensics on various operating systems, extracting critical data from smartphones and tablets.

Effectively counter anti-forensics techniques employed by sophisticated adversaries.

Utilize open-source and commercial forensic tools for efficient evidence processing and analysis.

Analyze network traffic and logs for indicators of compromise (IOCs) and attack attribution.

Recover and interpret deleted and hidden data from compromised systems and storage media.

Develop robust incident response plans that integrate advanced digital forensics methodologies.

Apply legal and ethical considerations to digital investigations, ensuring evidence admissibility in court.

Generate comprehensive and defensible forensic reports for diverse stakeholders.

Explore emerging trends in digital forensics, including AI-driven analysis and blockchain investigations.

Enhance cybersecurity posture through proactive identification and analysis of digital threats.

Organizational Benefits

1. Enhanced Incident Response Capabilities: Faster and more effective responses to cybersecurity incidents and data breaches.
2. Reduced Legal and Financial Risk: Improved evidence handling ensures admissibility in legal proceedings, minimizing potential liabilities.
3. Improved Data Breach Containment: Quicker identification and isolation of compromised systems, limiting damage.
4. Strengthened Compliance: Adherence to regulatory requirements for data handling and incident reporting.
5. Proactive Threat Intelligence: Ability to derive actionable intelligence from forensic investigations to prevent future attacks.

6. Protection of Intellectual Property: Efficiently investigate and mitigate cases of trade secret theft and corporate espionage.
7. Increased Cyber Resilience: Building an internal capacity to defend against and recover from sophisticated cyber threats.
8. Optimized Resource Utilization: Empowering internal teams to conduct thorough investigations, reducing reliance on external consultants.
9. Enhanced Employee Skillset: Cultivating a highly skilled workforce proficient in cutting-edge digital forensics.
10. Reputation Management: Demonstrating a strong commitment to security and integrity in the face of cyber incidents.

Target Audience

1. Digital Forensics Investigators
2. Incident Response Team Members
3. Cybersecurity Analysts
4. Law Enforcement Professionals
5. Legal Professionals involved in cybercrime cases
6. IT Security Managers
7. Auditors and Compliance Officers
8. System Administrators with security responsibilities
9. Consultants specializing in cybersecurity and forensics
10. e-Discovery Professionals

Course Outline

Module 1: Foundations of Advanced Digital Forensics

- **Deep Dive into Digital Evidence:** Volatility, Locard's Exchange Principle, and types of digital artifacts.
- **Advanced Forensic Readiness:** Proactive measures and organizational preparation for incident response.
- **Legal & Ethical Frameworks:** Evolving legal precedents, privacy concerns, and expert witness testimony.
- **Forensic Tool Ecosystem:** In-depth review of industry-leading commercial and open-source tools.
- **Case Study: Enterprise Data Breach Initial Response:** Analyzing the critical first hours of an advanced persistent threat (APT) incident.

Module 2: Advanced Data Acquisition & Imaging

- **Live System Acquisition Techniques:** Memory forensics, process analysis, and volatile data collection.
- **Disk Imaging Beyond Basics:** Handling advanced file systems, RAID, and encrypted volumes.
- **Network Forensics Data Capture:** Packet capture, flow analysis, and deep packet inspection for threat hunting.
- **Cloud Environment Acquisition:** Navigating legal and technical challenges in IaaS, PaaS, and SaaS environments.
- **Case Study: Insider Threat Investigation:** Acquiring data from a live employee workstation without detection.

Module 3: Mobile Device Forensics & IoT

- **Smartphone Forensics (iOS & Android):** Advanced extraction techniques for locked and encrypted devices.
- **IoT Device Forensics:** Acquiring data from smart devices, industrial control systems, and connected vehicles.
- **Wearable Technology & Drone Forensics:** Specialized challenges and solutions for emerging digital evidence sources.
- **Data Carving & File System Unallocated Space:** Recovering fragmented and deleted data from mobile devices.
- **Case Study: Mobile Malware Analysis:** Tracing the spread and impact of mobile ransomware through forensic artifacts.

Module 4: Anti-Forensics & Evasion Techniques

- **Understanding Anti-Forensic Methodologies:** Data wiping, steganography, encryption, and artifact manipulation.
- **Detecting & Countering Evasion:** Techniques for identifying and bypassing anti-forensic tools.
- **Encrypted Volume Analysis:** Strategies for accessing and decrypting seized data.
- **Live System Tampering Detection:** Identifying attempts to hide or destroy evidence during live investigations.
- **Case Study: Ransomware Attack Disguise:** Uncovering hidden data and attacker methodologies despite anti-forensic measures.

Module 5: Advanced Artifact Analysis

- **Registry & Log File Analysis:** Deep dive into Windows, Linux, and macOS system artifacts.
- **Browser Forensics & Web Activity:** Tracing user activity, online communications, and dark web interactions.
- **Email & Messaging Forensics:** Advanced techniques for extracting and analyzing digital communications.
- **Malware Analysis & Reverse Engineering:** Identifying malware families and their functionalities from forensic images.
- **Case Study: Corporate Espionage:** Analyzing digital artifacts to reconstruct the timeline and method of data exfiltration.

Module 6: Network Forensics & Threat Hunting

- **Advanced Network Packet Analysis:** Deep dive into protocols, anomalies, and covert channels.
- **Intrusion Detection System (IDS) & Security Information and Event Management (SIEM) Log Analysis:** Correlating events for comprehensive incident reconstruction.
- **Wireless Network Forensics:** Investigating Wi-Fi attacks and unauthorized access.
- **Cloud Network Security Forensics:** Tracing activity and data flow within cloud infrastructures.

- **Case Study: Advanced Persistent Threat (APT) Campaign:** Using network artifacts to identify attacker infrastructure and command-and-control.

Module 7: Reporting & Expert Testimony

- **Crafting Comprehensive Forensic Reports:** Structure, content, and legal considerations.
- **Data Visualization for Forensics:** Presenting complex findings clearly and concisely.
- **Preparing for Expert Witness Testimony:** Courtroom procedures, direct examination, and cross-examination strategies.
- **Admissibility of Digital Evidence:** Understanding Daubert and Frye standards in various jurisdictions.
- **Case Study: Mock Courtroom Scenario:** Presenting forensic findings and undergoing simulated cross-examination.

Module 8: Emerging Trends & Future of Forensics

- **AI & Machine Learning in Forensics:** Automated analysis, anomaly detection, and predictive capabilities.
- **Blockchain Forensics:** Tracing cryptocurrency transactions and smart contract analysis.
- **Quantum Computing & Its Impact on Forensics:** Future challenges and opportunities.
- **Cyber-Physical Systems & ICS Forensics:** Investigating incidents in critical infrastructure.
- **Case Study: Future of Cybercrime & Forensics:** Discussing hypothetical scenarios and evolving investigative techniques.

Training Methodology

This training course will employ a blended learning approach incorporating:

- Interactive lectures and presentations
- Hands-on exercises and case studies
- Individual and group simulation projects
- Discussions and knowledge sharing
- Practical application of simulation software
- Real-world examples and industry best practices

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com **or call** *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com