# Digital Evidence Collection, Analysis and Presentation Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Criminology | **Duration** | 10 Days |
| **Base Fee** | $3,000 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

In today’s digital age, the proliferation of cybercrime and the increasing use of digital devices in criminal activities necessitate a strong foundation in digital evidence collection, forensic analysis, and data presentation. Training Course on Digital Evidence Collection, Analysis & Presentation is meticulously designed to equip law enforcement professionals, cybersecurity specialists, legal practitioners, and forensic analysts with the essential tools and techniques required to gather, examine, and present digital evidence effectively. Participants will gain in-depth knowledge of chain of custody, data integrity, and digital forensics protocols, ensuring compliance with global standards and legal frameworks.

With an emphasis on emerging technologies and real-world case studies, this course integrates hands-on training with theoretical frameworks to ensure mastery in areas such as incident response, mobile forensics, cloud data retrieval, and courtroom testimony. Whether you are responding to a cybersecurity breach or preparing evidence for prosecution, this course will elevate your skillset and position you as a proficient digital investigator in the fight against cybercrime.

## Programme Curriculum

**Digital Evidence Collection, Analysis and Presentation Training Course**

**Introduction**

In today’s digital age, the proliferation of cybercrime and the increasing use of digital devices in criminal activities necessitate a strong foundation in digital evidence collection, forensic analysis, and data presentation. Digital Evidence Collection, Analysis and Presentation Training Course is meticulously designed to equip law enforcement professionals, cybersecurity specialists, legal practitioners, and forensic analysts with the essential tools and techniques required to gather, examine, and present digital evidence effectively. Participants will gain in-depth knowledge of chain of custody, data integrity, and digital forensics protocols, ensuring compliance with global standards and legal frameworks.

With an emphasis on emerging technologies and real-world case studies, this course integrates hands-on training with theoretical frameworks to ensure mastery in areas such as incident response, mobile forensics, cloud data retrieval, and courtroom testimony. Whether you are responding to a cybersecurity breach or preparing evidence for prosecution, this course will elevate your skillset and position you as a proficient digital investigator in the fight against cybercrime.

**Course Objectives**

1. Understand core concepts of digital forensics and cybercrime investigation.
2. Demonstrate proficiency in data acquisition from digital devices.
3. Apply best practices for preserving digital evidence integrity.
4. Utilize forensic software tools for evidence analysis.
5. Master techniques in mobile device forensics.
6. Identify procedures for cloud-based evidence retrieval.
7. Execute a thorough chain of custody process.
8. Develop skills in incident response and log analysis.
9. Ensure legal admissibility of digital evidence in court procedures.
10. Interpret metadata and digital footprints accurately.
11. Detect and analyze malware-infected systems.
12. Prepare comprehensive digital forensic reports.
13. Deliver compelling and accurate courtroom testimony.

**Target Audiences**

1. Law Enforcement Agencies
2. Digital Forensics Analysts
3. Cybersecurity Professionals
4. Prosecutors & Legal Professionals
5. Intelligence Officers
6. IT Auditors
7. Compliance Officers
8. Criminal Justice Students & Academicians

**Course Duration:** 10 days

**Course Modules**

**Module 1: Introduction to Digital Evidence**

- Definition and types of digital evidence
- Importance in modern investigations
- Legal considerations
- Role of digital forensics in the justice system
- Tools and environments for evidence collection
- **Case Study: The BTK Killer & Floppy Disk Metadata**

**Module 2: Chain of Custody and Evidence Handling**

- Defining chain of custody
- Proper documentation and labeling
- Avoiding contamination
- Secure storage and transportation
- Maintaining evidence integrity
- **Case Study: Enron Email Archive Analysis**

**Module 3: Data Acquisition Techniques**

- Disk imaging and cloning
- Write-blocking technologies
- Live vs. dead acquisition
- RAM acquisition
- Password bypass strategies
- **Case Study: FBI Acquisition of Silk Road Server**

**Module 4: Forensic Tools & Software**

- FTK and EnCase overview
- Autopsy and Sleuth Kit
- X-Ways Forensics
- Open-source vs commercial tools
- Software validation
- **Case Study: Deep Dive into the use of EnCase in Child Pornography Cases**

**Module 5: File System Analysis**

- FAT32, NTFS, and EXT file systems
- Hidden partitions and volumes
- Slack space analysis
- File recovery techniques
- Volume shadow copies
- **Case Study: Analysis of Deleted Files in a Corporate Fraud Case**

**Module 6: Metadata and Log Files**

- Understanding file metadata
- Email and document metadata
- Operating system logs
- Browser and internet history
- Time-stamp anomalies
- **Case Study: Watergate Scandal & Metadata Timeline Reconstruction**

**Module 7: Email and Web Forensics**

- Webmail vs. client-based email
- Email headers and attachments
- Identifying phishing and spoofing
- Internet activity logs
- Social media data collection
- **Case Study: Email Tracking in Corporate Espionage**

**Module 8: Mobile Device Forensics**

- Android and iOS architecture
- Data acquisition techniques
- App data and location tracking
- SIM card and cloud sync artifacts
- Locked devices and bypass methods
- **Case Study: Phone Data in Domestic Violence Investigation**

**Module 9: Network Forensics**

- Packet sniffing and traffic analysis
- Intrusion detection systems

- Firewall and router logs
- VPN and proxy tracing
- Wi-Fi forensic techniques
- **Case Study: Tracing Cyber Attack on Financial Institution**

**Module 10: Malware Analysis**

- Types of malware
- Behavior and static analysis
- Sandbox environment usage
- Malware signature extraction
- Identifying rootkits and backdoors
- **Case Study: Analysis of WannaCry Ransomware**

**Module 11: Cloud Forensics**

- Cloud service providers and jurisdiction
- Cloud storage evidence collection
- Data synchronization and deletion
- Cloud-specific tools
- Challenges in chain of custody
- **Case Study: Dropbox Metadata in Insider Threat Investigation**

**Module 12: Virtual Machines & Digital Artifacts**

- Identifying virtual environments
- Artifacts in VMware and VirtualBox
- Memory and snapshot analysis
- VM escape and rootkits
- Hypervisor logs
- **Case Study: Hacking Investigation via VM Deployment**

**Module 13: Report Writing and Documentation**

- Structuring a forensic report
- Writing technical findings in layman's terms
- Attaching exhibits and appendices
- Addressing limitations
- Presenting reproducible findings
- **Case Study: Report Format for Cyber Harassment Case**

**Module 14: Courtroom Presentation of Evidence**

- Rules of digital evidence admissibility
- Expert witness testimony tips
- Presenting technical info to jury
- Handling cross-examination
- Visual evidence presentation tools
- **Case Study: Expert Witness Role in FBI vs. Apple Case**

**Module 15: Ethics, Privacy & Legal Framework**

- Ethical obligations of forensic examiners
- Data protection laws (e.g., GDPR, HIPAA)
- Search warrant and consent issues
- International cooperation challenges

- Ethical dilemmas in corporate forensics
- **Case Study: Privacy Concerns in Facebook Data Leak Investigation**

**Training Methodology**

- Interactive lectures with real-world demonstrations
- Hands-on lab sessions using forensic tools
- Group-based scenario workshops and mock investigations
- Case study analysis for each module
- Quizzes and knowledge checks for reinforcement
- Final capstone project and presentation

**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.

**e.** One-year post-training support Consultation and Coaching provided after the course.

**f.** Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

## Upcoming Scheduled Sessions

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **07 Sep 2026** | 18 Sep 2026 | Physical | $3,000 |
| **14 Sep 2026** | 25 Sep 2026 | Physical | $3,000 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $3,000 |
| **28 Sep 2026** | 09 Oct 2026 | Physical | $3,000 |

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **05 Oct 2026** | 16 Oct 2026 | Physical | $3,000 |
| **12 Oct 2026** | 23 Oct 2026 | Physical | $3,000 |
| **19 Oct 2026** | 30 Oct 2026 | Physical | $3,000 |
| **26 Oct 2026** | 06 Nov 2026 | Physical | $3,000 |

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

**Register Online Now**

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