Digital Forensics and eDiscovery for Windows/Linux Training Course

Professional Development Training Course Outline

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

Course Introduction

In today's hyper-connected world, digital evidence is paramount in legal, corporate, and cybersecurity investigations. The exponential growth of Electronically Stored Information (ESI) across Cloud Computing and IoT devices presents unprecedented challenges and opportunities. This intensive training program delivers vendor-agnostic, platform-specific expertise in conducting forensically sound investigations on both Windows and Linux operating systems. Participants will master the end-to-end eDiscovery Reference Model (EDRM) process, from legal hold and defensible data collection to advanced artifact analysis and expert report generation, ensuring regulatory compliance in an era dominated by Advanced Persistent Threats (APTs) and complex data environments.

Digital Forensics and eDiscovery for Windows/Linux Training Course is designed to transition participants from foundational concepts to advanced forensic techniques and proactive incident response strategies. We focus on practical, hands-on lab exercises utilizing industry-leading forensic toolkits like FTK, EnCase, Volatility, and open-source Linux utilities, coupled with real-world case studies covering insider threats, ransomware, and intellectual property theft. By integrating the principles of computer forensics, network forensics, and eDiscovery, this course prepares a new generation of investigators to maintain the Chain of Custody and deliver admissible evidence crucial for modern litigation and security operations.

Programme Curriculum

Digital Forensics and eDiscovery for Windows/Linux Training Course

Course Introduction

In today's hyper-connected world, digital evidence is paramount in legal, corporate, and cybersecurity investigations. The exponential growth of Electronically Stored Information (ESI) across Cloud Computing and IoT devices presents unprecedented challenges and opportunities. This intensive training program delivers

vendor-agnostic, platform-specific expertise in conducting forensically sound investigations on both Windows and Linux operating systems. Participants will master the end-to-end eDiscovery Reference Model (EDRM) process, from legal hold and defensible data collection to advanced artifact analysis and expert report generation, ensuring regulatory compliance in an era dominated by Advanced Persistent Threats (APTs) and complex data environments.

Digital Forensics and eDiscovery for Windows/Linux Training Course is designed to transition participants from foundational concepts to advanced forensic techniques and proactive incident response strategies. We focus on practical, hands-on lab exercises utilizing industry-leading forensic toolkits like FTK, EnCase, Volatility, and open-source Linux utilities, coupled with real-world case studies covering insider threats, ransomware, and intellectual property theft. By integrating the principles of computer forensics, network forensics, and eDiscovery, this course prepares a new generation of investigators to maintain the Chain of Custody and deliver admissible evidence crucial for modern litigation and security operations.

Course Duration

5 days

Course Objectives

1. Master Forensically Sound data Acquisition and Preservation across Windows and Linux environments.
2. Navigate and analyze complex NTFS and Ext4/Btrfs file systems for hidden and deleted data.
3. Execute proficient Windows Artifact Analysis including Registry, Event Logs, and Jump Lists.
4. Perform Linux-Specific forensic analysis of shell histories, log files, and system daemons.
5. Conduct Memory Forensics to recover volatile data like running processes and encryption keys.
6. Understand and apply the complete Electronic Discovery Reference Model (EDRM) for litigation readiness.
7. Identify and track Advanced Persistent Threats (APTs) and Malware persistence mechanisms.
8. Implement effective Legal Hold procedures and manage Electronically Stored Information (ESI) defensibly.
9. Investigate data associated with modern communication methods, including Ephemeral Messaging and Collaboration Platforms
10. Apply Cloud Forensics principles for data collection from IaaS, PaaS, and SaaS environments.
11. Utilize Technology Assisted Review (TAR) and data analytics for large-scale eDiscovery matters.
12. Generate Expert Witness Reports and articulate technical findings clearly for legal proceedings.
13. Uphold Ethics, Privacy (GDPR, CCPA), and the Admissibility of Digital Evidence in court.

Target Audience

1. Cybersecurity Analysts and Incident Responders
2. IT/System Administrators
3. Legal and Compliance Professionals
4. Digital Forensic Examiners.
5. Law Enforcement and Government Agency Investigators.
6. Internal Auditors and Corporate Fraud Investigators.
7. Risk Management Professionals.
8. Students or Career Changers.

Course Modules

Module 1: Foundations of Digital Evidence & EDRM

- The Digital Forensics Investigation Process and methodologies.
- Legal & Ethical Frameworks.
- Understanding and implementing the Legal Hold and Preservation phases of EDRM.
- The difference between forensically sound imaging and logical data collection.
- Core concepts of hashing, data integrity, and evidence validation.
- Case Study: The Legal Hold Failure.

Module 2: Windows Artifact Analysis and Volatile Data

- System Acquisition.
- Deep-dive into the Windows Registry for user activity, execution history, and device connection.
- Analyzing system and application-specific artifacts.
- File System Forensics.
- Memory Forensics.
- Case Study: The C-Level Data Leak.

Module 3: Deep Dive into Linux Forensics

- Linux System Acquisition.
- Analyzing common Linux file systems.
- Investigating user activity.
- Linux System Logs.
- Rootkit and Malware detection on Linux systems.
- Case Study: Compromised Web Server.

Module 4: Network and Cloud Forensics

- Network Packet Analysis.
- Log File Analysis.
- Cloud Forensics.
- Email Forensics.
- Virtual Machine (VM) Forensics.
- Case Study: Cloud Account Hijack.

Module 5: Mobile and Advanced Data Recovery

- Mobile Device Forensics Overview.
- Data Carving and File Recovery from unallocated space.
- Encrypted Drive Analysis.
- Database Forensics.
- Timeline Construction.
- Case Study: Fraudulent Financial Transactions.

Module 6: Incident Response and Malware

- The full Incident Response Lifecycle.
- Ransomware Investigation.
- Introduction to Static and Dynamic Malware Analysis techniques.
- Containment and Eradication Strategies across Windows and Linux endpoints.
- Developing an effective Threat Hunting strategy using forensic artifacts.
- Case Study: The Multi-Stage Ransomware Attack.

Module 7: EDiscovery Workflow and Analytics

- Advanced Processing and Filtering of ESI.
- Keyword Searching and Concept Searching best practices for effective document review.
- Technology Assisted Review.
- Data Production Formats.
- Managing data privacy and cross-border discovery challenges.
- Case Study: High-Stakes Antitrust Litigation.

Module 8: Reporting, Testimony, and Future Trends

- Structuring a **Defensible Forensic Report**.
- Preparing for **Expert Witness Testimony** and handling Daubert/Frye challenges.
- **Automation** in Forensics and eDiscovery workflows.
- Emerging Trends.
- Ethical challenges in digital investigation and professional development paths.
- **Case Study:** Challenging Evidence Admissibility.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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