Training Course on Investigating Insider Threats with Digital Forensics

Professional Development Training Course Outline

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

Course Introduction

Introduction

Insider threats represent one of the most insidious and damaging risks to any organization. Unlike external attacks, they originate from individuals with authorized access – employees, contractors, or partners – who misuse their privileges, intentionally or unintentionally, leading to data exfiltration, intellectual property theft, sabotage, or fraud. Digital forensics is the cornerstone of effectively investigating these elusive threats. Training Course on Investigating Insider Threats with Digital Forensics is meticulously designed to equip digital forensic investigators, incident responders, and security professionals with the advanced methodologies and practical skills to identify, collect, preserve, analyze, and report on digital evidence specifically related to insider threat incidents. Participants will learn to navigate the complexities of corporate systems, uncover hidden digital footprints, and reconstruct the complete timeline of malicious activity, transforming raw data into actionable intelligence and legally admissible evidence.

This comprehensive program delves into the unique challenges of insider threat investigations, including the nuances of data acquisition from live systems, the analysis of user behavior anomalies, the detection of anti-forensic techniques, and the critical interplay between technical evidence and human resources considerations. Through extensive hands-on labs, real-world case studies, and the application of industry-leading forensic tools, attendees will gain expertise in examining endpoints, servers, network traffic, cloud services, and mobile devices for indicators of insider risk. By the end of this course, you will be proficient in proactively identifying potential threats, responding effectively to incidents, and building robust, legally defensible cases against those who betray trust from within.

Programme Curriculum

Training Course on Investigating Insider Threats with Digital Forensics

Introduction

Insider threats represent one of the most insidious and damaging risks to any organization. Unlike external attacks, they originate from individuals with authorized access – employees, contractors, or partners – who misuse their privileges, intentionally or unintentionally, leading to data exfiltration, intellectual property theft, sabotage, or fraud. Digital forensics is the cornerstone of effectively investigating these elusive threats. Training Course on Investigating Insider Threats with Digital Forensics is meticulously designed to equip digital forensic investigators, incident responders, and security professionals with the advanced methodologies and practical skills to identify, collect, preserve, analyze, and report on digital evidence specifically related to insider threat incidents. Participants will learn to navigate the complexities of corporate systems, uncover hidden digital footprints, and reconstruct the complete timeline of malicious activity, transforming raw data into actionable intelligence and legally admissible evidence.

This comprehensive program delves into the unique challenges of insider threat investigations, including the nuances of data acquisition from live systems, the analysis of user behavior anomalies, the detection of anti-forensic techniques, and the critical interplay between technical evidence and human resources considerations. Through extensive hands-on labs, real-world case studies, and the application of industry-leading forensic tools, attendees will gain expertise in examining endpoints, servers, network traffic, cloud services, and mobile devices for indicators of insider risk. By the end of this course, you will be proficient in proactively identifying potential threats, responding effectively to incidents, and building robust, legally defensible cases against those who betray trust from within.

Course Duration

10 Days

Course Objectives

1. Define Insider Threat Archetypes: Distinguish between malicious, negligent, and compromised insiders, understanding their motivations and common attack patterns.
2. Master Digital Evidence Collection for Insider Incidents: Safely acquire data from endpoints, servers, cloud services, and mobile devices with chain of custody integrity.
3. Perform Advanced User Activity Analysis: Analyze login/logout times, application usage, file access, print activity, and external device connections for suspicious behavior.
4. Investigate Data Exfiltration Paths: Identify methods and evidence of data theft via USB devices, cloud storage, email, network shares, and unsanctioned applications.

5. Analyze Web Browse & Communication Forensics: Reconstruct online activities, search queries, and communication patterns (email, chat, social media) for intent and context.
6. Detect Anti-Forensic & Evasion Techniques: Uncover attempts to delete logs, encrypt data, use secure deletion tools, or manipulate timestamps to hide insider activity.
7. Examine System & Application Logs: Deeply analyze Windows Event Logs, application logs, security appliance logs, and SIEM data for insider threat indicators.
8. Conduct Network Traffic Analysis for Insider Threat: Identify unusual network connections, data flows, and protocol anomalies indicative of covert communication or data transfer.
9. Utilize User Behavior Analytics (UBA) Artifacts: Integrate insights from UBA systems and endpoint detection and response (EDR) tools into forensic investigations.
10. Trace Privilege Abuse & Escalation: Uncover evidence of unauthorized access attempts, privilege escalation, and lateral movement within internal systems.
11. Assess Cloud & Hybrid Environment Insider Threats: Acquire and analyze data from SaaS applications, cloud storage, and hybrid identity systems for insider activity.
12. Develop Comprehensive Investigative Plans: Formulate a strategic approach to insider threat investigations, integrating technical forensics with HR and legal considerations.
13. Generate Legally Defensible Forensic Reports: Produce clear, detailed, and admissible reports outlining insider threat findings, methodologies, and conclusions.

Organizational Benefits

1. Reduced Insider Threat Risk: Proactive identification and mitigation of internal threats, safeguarding critical assets.
2. Minimized Financial & Reputational Damage: Prevent data breaches, intellectual property theft, and system sabotage.
3. Enhanced Incident Response Capability: Rapid and effective response to suspected insider incidents.
4. Stronger Compliance Posture: Meet regulatory requirements for data protection and incident reporting.
5. Improved Data Loss Prevention (DLP): Insights from forensics inform and strengthen DLP policies and tools.
6. Better Employee Training & Awareness: Case studies enhance security awareness and policy adherence.
7. Increased Investigative Efficiency: Streamlined processes for complex insider threat investigations.
8. Robust Legal & HR Support: Provides concrete evidence for disciplinary actions or legal prosecution.
9. Protection of Intellectual Property: Safeguard trade secrets and proprietary information from internal compromise.
10. Cultivation of a Security-Conscious Culture: Fosters an environment where vigilance against insider risks is prioritized.

Target Participants

- Digital Forensic Investigators
- Incident Response Team Members
- Cybersecurity Analysts (SOC Tier 2/3)
- Insider Threat Program Managers
- Compliance Officers
- Human Resources Professionals (with security interest)
- Legal Counsel (involved in digital investigations)
- IT Auditors
- Security Operations Managers
- Network Security Engineers

Course Outline

Module 1: Introduction to Insider Threats & Digital Forensics Fundamentals

- **Defining Insider Threats:** Malicious, negligent, compromised insiders, and their motivations.
- **Impact of Insider Threats:** Data exfiltration, sabotage, fraud, espionage.
- **The Role of Digital Forensics:** How forensics supports insider threat investigations.
- **Legal & Ethical Considerations:** Privacy, monitoring policies, chain of custody.
- **Case Study:** Overview of a high-profile insider data breach.

Module 2: Insider Threat Indicators & Behavioral Analysis

- **Technical Indicators:** Unusual login times, data access, application usage.
- **Behavioral Indicators:** Disgruntlement, policy violations, suspicious personal finances.
- **User Activity Monitoring (UAM) & User Behavior Analytics (UBA):** Integrating logs and alerts.
- **Contextual Analysis:** Combining technical and non-technical clues.
- **Case Study:** Correlating UBA alerts with suspicious digital activity.

Module 3: Endpoint Forensics for Insider Threats (Windows)

- **Windows Artifacts Deep Dive:** Registry hives (NTUSER.DAT, SAM, SYSTEM), Event Logs.
- **User Profile Analysis:** Recent documents, jump lists, shellbags, prefetch files.
- **Application Usage & Installation:** Program execution, software installations/uninstalls.
- **External Device Connectivity:** USB device history, connected peripheral artifacts.
- **Case Study:** Reconstructing user activity on a suspect Windows workstation.

Module 4: Data Exfiltration Analysis: Endpoint & Network

- **USB Device Forensics:** Recovering deleted files, analyzing USB history.
- **Cloud Storage & File Sync Services:** Identifying uploads to personal cloud accounts.
- **Email & Messaging Client Forensics:** Analyzing mailboxes, chat logs for data transfers.
- **Network Share Activity:** Tracing data copied to/from network drives.
- **Case Study:** Tracing exfiltrated sensitive documents via a USB drive.

Module 5: Email & Internet Activity Forensics

- **Email Header Analysis:** Identifying sender, recipient, and routing for suspicious emails.
- **Web Browser Forensics:** History, cache, cookies, downloads, search queries.
- **Social Media & Webmail Analysis:** Extracting data from online platforms.
- **Proxy & VPN Usage Detection:** Identifying attempts to hide online activity.
- **Case Study:** Uncovering communications with a competitor via personal email.

Module 6: Server & Log Forensics in Insider Investigations

- **Windows Server Logs:** Security, System, Directory Service logs for admin activity.
- **Active Directory Forensics:** Account changes, privilege escalation, authentication attempts.
- **File Server Auditing:** Tracking access, modification, and deletion of sensitive files.
- **Database Logs:** Identifying unauthorized queries or data extraction.
- **Case Study:** Investigating a malicious insider's activity on a corporate file server.

Module 7: Network Forensics & Covert Channels

- **Network Traffic Capture & Analysis:** Identifying unusual data flows, protocol anomalies.
- **DNS & ICMP Tunneling:** Detecting data exfiltration over unconventional channels.
- **Web Proxies & VPN Connections:** Tracing outbound connections to anonymizing services.
- **Network Session Reconstruction:** Understanding full data streams between endpoints.
- **Case Study:** Detecting data exfiltration via a DNS covert channel.

Module 8: Cloud & SaaS Forensics for Insider Threats

- **Cloud Service Provider (CSP) Logs:** Audit logs, activity logs from IaaS, PaaS, SaaS.
- **Microsoft 365 / Google Workspace Forensics:** SharePoint, OneDrive, Exchange Online audit trails.
- **Cloud Identity & Access Management (IAM):** Analyzing suspicious login patterns and permission changes.
- **Data Residency & Jurisdiction Challenges:** Legal aspects of cloud data acquisition.
- **Case Study:** Investigating unauthorized access to a cloud-based CRM system.

Module 9: Mobile Device Forensics for Insider Threats

- **Mobile Device Acquisition:** Logical vs. physical extraction, challenges and tools.
- **SMS & Messaging App Forensics:** Recovering communications (WhatsApp, Signal, Telegram).
- **Cloud Sync & Backup Analysis:** Examining mobile data backed up to cloud services.
- **Location Data & Device Activity:** Tracing movements and app usage on mobile devices.
- **Case Study:** Recovering deleted messages from an employee's personal device.

Module 10: Anti-Forensic Techniques & Evasion

- **Data Wiping & Secure Deletion:** Identifying and recovering data from wiped drives.
- **Encryption Detection & Circumvention:** Analyzing encrypted volumes and files.
- **Timestomp & Metadata Manipulation:** Detecting altered file timestamps and properties.
- **Rootkits & Stealthy Malware:** Uncovering hidden processes and files used for covert activity.
- **Case Study:** Countering anti-forensic measures used by a sophisticated insider.

Module 11: Steganography Detection in Insider Threat Cases

- **Principles of Steganography:** Hiding data within images, audio, video, documents.
- **Steganalysis Techniques:** Statistical analysis, visual inspection, specialized tools.
- **Common Steganographic Tools:** Identifying their use and extracting hidden payloads.

- **Covert Channels in Legitimate Protocols:** DNS, HTTP, ICMP.
- **Case Study:** Detecting and extracting hidden data from an image file.

Module 12: Memory Forensics for Insider Threat Context

- **Live Memory Acquisition:** Safely capturing RAM from suspect systems.
- **Volatility Framework:** Analyzing processes, network connections, command history in memory.
- **Extracting Credentials:** Identifying cached passwords and sensitive data in RAM.
- **Detecting In-Memory Malware & Injected Code:** Uncovering stealthy threats.
- **Case Study:** Analyzing a memory dump to reveal active malicious processes.

Module 13: Correlation, Timeline Reconstruction & Attack Attribution

- **Data Normalization & Correlation:** Integrating disparate data sources (logs, artifacts, network).
- **Timeline Analysis Tools:** Building chronological sequences of events.
- **Anomaly Detection & Pattern Recognition:** Identifying deviations from baseline behavior.
- **Attribution & Intent Analysis:** Linking digital evidence to specific individuals and motivations.
- **Case Study:** Building a comprehensive timeline for an insider data exfiltration incident.

Module 14: Report Writing & Legal/HR Considerations

- **Structuring Forensic Reports:** Executive summary, findings, methodology, conclusions, recommendations.
- **Legal Admissibility:**Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Register Online Now

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