Training Course on Commercial Forensic Tool Utilization

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

In the demanding field of digital forensics and incident response, the effective use of commercial forensic tools is paramount for achieving comprehensive investigations and ensuring legal defensibility. Training Course on Commercial Forensic Tool Utilization is meticulously designed to equip professionals with expert-level proficiency in leveraging industry-leading proprietary software solutions. Participants will gain deep practical experience with powerful platforms that offer integrated workflows, advanced automation, and validated methodologies, crucial for tackling sophisticated cyber threats, complex data breaches, and high-stakes legal cases.

This intensive program focuses on hands-on application of top-tier commercial tools, enabling participants to streamline evidence acquisition, perform in-depth artifact analysis, conduct efficient data recovery, and generate professional, court-ready reports. Beyond technical mastery, the course emphasizes the strategic advantages these tools provide in expediting investigations, improving organizational resilience, and strengthening cybersecurity posture. By mastering these commercial platforms, attendees will become invaluable assets, capable of delivering forensically sound results and contributing significantly to an organization's overall risk management and compliance efforts.

Programme Curriculum

Training Course on Commercial Forensic Tool Utilization

Introduction

In the demanding field of digital forensics and incident response, the effective use of commercial forensic tools is paramount for achieving comprehensive investigations and ensuring legal defensibility. Training Course on Commercial Forensic Tool Utilization is meticulously designed to equip professionals with expert-level

proficiency in leveraging industry-leading proprietary software solutions. Participants will gain deep practical experience with powerful platforms that offer integrated workflows, advanced automation, and validated methodologies, crucial for tackling sophisticated cyber threats, complex data breaches, and high-stakes legal cases.

This intensive program focuses on hands-on application of top-tier commercial tools, enabling participants to streamline evidence acquisition, perform in-depth artifact analysis, conduct efficient data recovery, and generate professional, court-ready reports. Beyond technical mastery, the course emphasizes the strategic advantages these tools provide in expediting investigations, improving organizational resilience, and strengthening cybersecurity posture. By mastering these commercial platforms, attendees will become invaluable assets, capable of delivering forensically sound results and contributing significantly to an organization's overall risk management and compliance efforts.

Course Duration

10 Days

Course Objectives

1. Master advanced data acquisition techniques using leading commercial forensic imagers.
2. Conduct comprehensive file system analysis (NTFS, APFS, Ext4) with commercial forensic suites.
3. Perform in-depth memory forensics using dedicated commercial tools like Magnet RAM Capture and EnCase.
4. Analyze complex network traffic and derive actionable intelligence with commercial network forensic platforms.
5. Utilize commercial tools for robust mobile device forensics, extracting data from diverse mobile operating systems.
6. Execute efficient email and communication analysis using specialized commercial forensic modules.
7. Identify and interpret critical operating system artifacts (Windows, macOS, Linux) with advanced parsing capabilities.
8. Leverage commercial tools for effective malware triage and analysis within a forensic context.
9. Recover fragmented, hidden, and encrypted data using sophisticated commercial carving and decryption features.
10. Generate defensible forensic reports and courtroom-ready documentation using integrated reporting functionalities.
11. Apply commercial tool features for automated workflow optimization and case management.
12. Investigate cloud environments and retrieve evidence using commercial cloud forensic connectors.

13. Stay abreast of new features and updates in commercial forensic software to maintain cutting-edge skills.

Organizational Benefits

1. Accelerated Investigations: Rapidly process and analyze large volumes of data.
2. Enhanced Accuracy & Reliability: Leverage validated, robust toolsets for forensically sound results.
3. Reduced Manual Effort: Automate repetitive tasks, freeing up investigator time.
4. Improved Case Management: Centralized platforms for tracking evidence and progress.
5. Stronger Legal Defensibility: Generate reports that meet stringent legal and regulatory standards.
6. Comprehensive Data Coverage: Access to broader data types and platforms (e.g., cloud, mobile).
7. Increased Investigative Depth: Uncover hidden artifacts and complex relationships in data.
8. Specialized Capabilities: Access to features for advanced scenarios like encryption bypass, specific application analysis.
9. Standardized Workflows: Ensure consistency across investigations within the organization.
10. Competitive Advantage: Equip teams with the industry-standard tools and expertise.

Target Participants

- Experienced Digital Forensic Examiners
- Senior Incident Response Specialists
- Law Enforcement Digital Crime Units
- Corporate Security Investigators
- eDiscovery Professionals
- IT Security Architects and Managers
- Cyber Threat Intelligence Analysts
- Fraud Investigators with digital components
- Legal Professionals requiring in-depth digital evidence understanding
- Consultants specializing in cybersecurity and forensics

Course Outline

Module 1: Introduction to Commercial Forensic Tool Ecosystem

- **Overview of Commercial Tools:** EnCase, FTK, Magnet AXIOM, Cellebrite.
- **Licensing & Deployment Models:** On-premise, cloud, enterprise considerations.

- **Comparative Analysis:** Strengths and weaknesses of leading commercial solutions.
- **Workflow Integration:** How commercial tools fit into an overall DFIR process.
- **Case Study:** Selecting the appropriate commercial toolset for a complex corporate investigation.

Module 2: Advanced Data Acquisition with Commercial Imagers

- **Forensic Imaging Best Practices:** Bit-stream vs. logical, write-blockers.
- **EnCase Imager Deep Dive:** Acquisition of live and dead systems, E01 format.
- **FTK Imager Pro Features:** Targeted acquisition, custom content imaging.
- **Remote Acquisition Techniques:** Utilizing commercial tools for remote data collection.
- **Case Study:** Performing forensically sound remote acquisition from a suspected insider threat's laptop.

Module 3: In-Depth File System Analysis (NTFS, APFS, Ext4) with Commercial Suites

- **Commercial File System Parsers:** How tools interpret MFT, B-trees, inodes.
- **NTFS Artifacts & Timelines:** USN Journal, $LogFile, Volume Shadow Copies with EnCase/FTK.
- **APFS Structures & Recovery:** APFS snapshots, deleted file recovery on macOS.
- **Linux File System Forensics (Ext4):** Block allocation, journaling, and recovery.
- **Case Study:** Reconstructing a detailed timeline of events on a Windows server after a ransomware attack using timeline analysis features.

Module 4: Advanced Memory Forensics with Commercial Solutions

- **Live Memory Acquisition Tools:** Magnet RAM Capture, EnCase Memory Imager.
- **Volatility Integration:** Leveraging commercial tools to integrate with Volatility for deeper analysis.
- **Process and Network Connection Analysis:** Identifying active malware and C2 channels.
- **User Session Reconstruction:** Extracting web history, open files from RAM.
- **Case Study:** Analyzing a live memory dump to identify malicious processes and network indicators of compromise.

Module 5: Network Traffic & Logs Analysis with Commercial Platforms

- **Network Packet Capture & Analysis:** Advanced features of commercial tools for PCAP analysis.
- **Network Flow Data Interpretation:** NetFlow, IPFIX analysis for traffic patterns.
- **Log Management & Correlation:** Integrating SIEM and log data for network investigations.
- **Threat Hunting with Network Data:** Proactive detection of anomalies and attack patterns.
- **Case Study:** Investigating a sophisticated network intrusion by correlating firewall, proxy, and packet data.

Module 6: Windows Operating System Artifacts (Commercial Focus)

- **Windows Registry Forensics:** Advanced parsing and analysis of hive files for user activity.
- **Event Log Analysis:** Comprehensive review of security, system, and application logs.
- **Link Files, Jump Lists, Shellbags:** Detailed analysis of user interactions with files and applications.
- **Browser Forensics Automation:** Extracting and analyzing web activity from popular browsers.
- **Case Study:** Uncovering evidence of data exfiltration through USB devices and cloud storage sync on a Windows endpoint.

Module 7: macOS and Linux Operating System Artifacts (Commercial Focus)

- **macOS Forensic Analysis:** Unified Log, Plist files, quarantine, and application usage.
- **Linux Forensic Artifacts:** System logs, cron jobs, user history, and package management.
- **Commercial Tools for Cross-Platform Analysis:** Leveraging unified interfaces.
- **Identifying Rootkits and Persistence Mechanisms:** Advanced detection on *nix systems.
- **Case Study:** Investigating unauthorized access and privilege escalation on a Linux web server.

Module 8: Mobile Device Forensics with Cellebrite/Magnet AXIOM

- **Mobile Device Acquisition Techniques:** Logical, physical, and file system extraction.
- **Cellebrite UFED/Physical Analyzer:** Deep dive into mobile data extraction and decoding.
- **Magnet AXIOM Mobile:** Comprehensive analysis of smartphone data, apps, and cloud backups.
- **Application Data Analysis:** WhatsApp, Telegram, social media forensics.
- **Case Study:** Extracting and analyzing communication data from a locked suspect mobile device.

Module 9: Email & Communication Forensics (Commercial Tools)

- **Email Header Analysis:** Tracing email origins and identifying spoofing.
- **PST/OST/MBOX File Analysis:** Extracting and analyzing mailboxes for relevant communications.
- **Instant Messaging & Collaboration Tools:** Slack, Teams, Zoom chat forensics.
- **Identifying Phishing & Malware Delivery:** Analyzing embedded links and attachments.
- **Case Study:** Investigating a business email compromise (BEC) incident by analyzing email server logs and user mailboxes.

Module 10: Malware Analysis & Triage with Commercial Integration

- **Malware Sandboxing & Dynamic Analysis:** Integrating commercial tools with sandbox environments.
- **Static Analysis Techniques:** Disassembly, signature matching, and string analysis.
- **Threat Intelligence Feed Integration:** Enriching findings with real-time threat data.
- **Endpoint Detection & Response (EDR) Forensics:** Leveraging EDR data for incident analysis.
- **Case Study:** Triage and initial analysis of a suspected ransomware sample using commercial threat intelligence and sandboxing.

Module 11: Cloud & SaaS Forensics with Commercial Connectors

- **Cloud Service Provider (CSP) Evidence:** AWS, Azure, GCP log and artifact collection.
- **SaaS Application Forensics:** Microsoft 365, Google Workspace, Salesforce investigations.
- **Commercial Cloud Connectors:** Tools for acquiring data from cloud environments.
- **Legal & Privacy Considerations in Cloud Forensics:** Data residency, international laws.
- **Case Study:** Collecting and analyzing audit logs from a compromised Microsoft 365 tenant.

Module 12: Data Recovery & File Carving with Commercial Precision

- **Advanced Data Recovery Algorithms:** Recovering data from corrupted or formatted drives.
- **Commercial File Carving Engines:** Precise recovery of specific file types (images, documents, executables).
- **Reconstructing Fragments:** Techniques for assembling carved data into usable files.
- **Handling Encrypted & Damaged Volumes:** Strategies for accessing challenging data.

- **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
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