Training Course on Printer and Peripheral Device Forensics

Professional Development Training Course Outline

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

Course Introduction

Introduction

In the increasingly interconnected digital landscape, printers and peripheral devices – often overlooked in traditional digital forensic investigations – are emerging as critical sources of evidentiary data in cybercrime, intellectual property theft, and insider threat scenarios. These devices, from networked printers and multifunction devices (MFDs) to scanners, external hard drives, and USB hubs, can retain a wealth of information about user activity, document content, and network connections. Training Course on Printer and Peripheral Device Forensics is designed to equip digital forensic professionals with the in-depth knowledge and practical techniques to forensically examine these often-underutilized sources. Participants will master methods to extract, analyze, and interpret data remnants from the internal storage, logs, and associated system artifacts of a wide array of peripheral devices, transforming them into valuable digital evidence.

This intensive program will delve into the unique challenges of peripheral device forensics, including volatile memory acquisition, proprietary data formats, and the nuances of correlating data across disparate device types. Through hands-on labs and real-world case studies, attendees will learn to recover print job metadata, scanned document images, connected device histories, and network activity traces. By the end of this course, you will possess the advanced skills to conduct thorough investigations involving printers, scanners, and other peripherals, significantly enhancing your ability to uncover crucial evidence, reconstruct events, and build strong, legally defensible cases in any digital investigation.

Programme Curriculum

Training Course on Printer and Peripheral Device Forensics

Introduction

In the increasingly interconnected digital landscape, printers and peripheral devices – often overlooked in traditional digital forensic investigations – are emerging as critical sources of evidentiary data in cybercrime, intellectual property theft, and insider threat scenarios. These devices, from networked printers and multifunction devices (MFDs) to scanners, external hard drives, and USB hubs, can retain a wealth of information about user activity, document content, and network connections. Training Course on Printer and Peripheral Device Forensics is designed to equip digital forensic professionals with the in-depth knowledge and practical techniques to forensically examine these often-underutilized sources. Participants will master methods to extract, analyze, and interpret data remnants from the internal storage, logs, and associated system artifacts of a wide array of peripheral devices, transforming them into valuable digital evidence.

This intensive program will delve into the unique challenges of peripheral device forensics, including volatile memory acquisition, proprietary data formats, and the nuances of correlating data across disparate device types. Through hands-on labs and real-world case studies, attendees will learn to recover print job metadata, scanned document images, connected device histories, and network activity traces. By the end of this course, you will possess the advanced skills to conduct thorough investigations involving printers, scanners, and other peripherals, significantly enhancing your ability to uncover crucial evidence, reconstruct events, and build strong, legally defensible cases in any digital investigation.

Course Duration

5 Days

Course Objectives

1. Identify Forensically Relevant Data Sources: Pinpoint where critical evidence resides within printers, scanners, and other peripheral devices.
2. Master Printer Forensic Techniques: Extract and analyze print job queues, spool files, internal hard drive data, and device logs from networked and local printers.
3. Perform Scanner Forensic Analysis: Recover scanned document images, metadata, and user activity logs from standalone scanners and MFDs.
4. Investigate External Storage Devices: Conduct in-depth forensic examinations of external hard drives, SSDs, and USB flash drives, including deleted file recovery.
5. Analyze USB Hub & Device Connectivity: Reconstruct USB device connection histories and data transfer activities from system artifacts.

6. Acquire Volatile Peripheral Data: Safely capture and analyze volatile memory and live system data related to peripheral device usage.
7. Handle Proprietary Formats: Understand and parse proprietary data formats used by specific peripheral manufacturers.
8. Correlate Cross-Device Artifacts: Link evidence from peripheral devices with host system logs and network traffic for comprehensive investigations.
9. Detect Anti-Forensic Measures: Identify and overcome techniques used to obscure or destroy data on peripheral devices.
10. Manage Networked Peripheral Evidence: Acquire and analyze data from network-attached printers, NAS devices, and IoT peripherals.
11. Understand Firmware Forensics: Recognize the potential for malicious firmware on peripheral devices and its forensic implications.
12. Apply Legal & Ethical Considerations: Adhere to legal standards and ethical guidelines specific to peripheral device evidence collection and analysis.
13. Generate Actionable Forensic Reports: Produce clear, concise, and defensible reports detailing findings from peripheral device investigations.

Organizational Benefits

1. Enhanced Data Exfiltration Detection: Improved ability to detect and prove unauthorized data removal via printing or external storage.
2. Stronger Insider Threat Investigations: Deeper insights into employee misuse of company assets through peripheral device activity.
3. Comprehensive Digital Evidence Collection: Ensures no stone is left unturned, maximizing evidence recovery in complex cases.
4. Reduced Investigation Timelines: Efficient techniques for extracting valuable data from often-overlooked sources.
5. Improved Compliance & Audit Trails: Better understanding of data flow and usage patterns within the organization.
6. Protection of Intellectual Property: Enhanced capability to identify and prosecute IP theft facilitated by peripheral devices.
7. Proactive Security Policy Development: Insights from investigations can inform and strengthen peripheral device usage policies.
8. Cost Savings in Litigation: Stronger evidence leads to better legal outcomes and potentially avoids protracted disputes.
9. Upskilled Forensic Team: Equips staff with specialized knowledge in a growing area of digital forensics.
10. Resilience Against Cyber Threats: Better understanding of peripheral vectors used in malware delivery or data breaches.

Target Participants

- Digital Forensic Examiners
- Incident Responders
- Cybersecurity Analysts
- Law Enforcement Investigators
- IT Auditors
- Security Operations Center (SOC) Analysts
- Data Loss Prevention (DLP) Specialists
- Fraud Investigators
- Legal Professionals (with technical interest)
- System Administrators with security responsibilities

Course Outline

Module 1: Introduction to Peripheral Device Forensics

- **The Evolving Threat Landscape:** Why peripheral devices are crucial evidence sources.
- **Categories of Peripheral Devices:** Printers, scanners, external storage, input devices, USB hubs, etc.
- **Forensic Challenges:** Data volatility, proprietary formats, data dispersion.
- **Legal & Ethical Foundations:** Consent, scope, chain of custody for peripherals.
- **Case Study: Insider Data Theft via External Hard Drive**

Module 2: Printer Forensics: Data & Artifacts

- **Printer Types & Data Storage:** Laser, inkjet, MFDs, internal storage (HDD/SSD).
- **Print Spooling & Spool Files (.SPL, .SHD):** Acquisition and analysis of print job content.
- **Printer Logs & Metadata:** Job history, user, date/time, network connections.
- **Hidden Data (Yellow Dots, Watermarks):** Manufacturer tracking codes and their forensic significance.
- **Case Study: Tracing a Leaked Document to a Specific Printer**

Module 3: Printer Forensics: Acquisition & Analysis

- **Live Acquisition from Networked Printers:** Techniques for accessing internal web interfaces and storage.
- **Physical Acquisition of Printer Storage:** Safely removing and imaging internal hard drives/SSDs.
- **Analyzing Printer Firmware:** Identifying versions and potential malicious modifications.
- **Tooling for Printer Forensics:** Utilizing specialized software and scripts.
- **Case Study: Investigating a Printer-Based Data Exfiltration Scheme**

Module 4: Scanner Forensics & Multifunction Devices (MFDs)

- **Scanner Capabilities & Data Remnants:** Imaging units, internal memory, document feeders.
- **Recovering Scanned Documents:** Locating and extracting images and associated metadata.
- **MFD Logs & Audit Trails:** Fax logs, scan-to-email/network logs, user activity.
- **Forensic Acquisition from MFDs:** Challenges and techniques for data extraction.
- **Case Study: Uncovering Scanned Confidential Documents**

Module 5: External Storage Device Forensics (Beyond USB Drives)

- **Advanced USB Flash Drive Forensics:** Review of deep dive techniques, anti-forensics.
- **External Hard Drives & SSDs:** Full disk imaging, partition recovery, deleted data.
- **Network Attached Storage (NAS) Forensics:** Acquiring data from shared storage, logging.
- **Memory Cards (SD, MicroSD) & Digital Camera Forensics:** Image/video recovery, metadata.
- **Case Study: Investigating Mass Data Copying to an External SSD**

Module 6: USB Connectivity & Hub Forensics

- **USB Device Enumeration & Identification:** Hardware IDs, Vendor/Product IDs (VID/PID).
- **Windows Registry & System Log Artifacts:** Deep dive into USBSTOR, MountPoints2, SetupAPI logs for connection history.
- **USB Hub Analysis:** Understanding how hubs impact device connectivity traces.
- **Correlating USB Activity with User Sessions:** Linking device usage to specific users and timestamps.
- **Case Study: Reconstructing USB Device Usage on a Compromised Workstation**

Module 7: Volatile Data & Live Analysis for Peripherals

- **Memory Forensics for Peripheral Interaction:** Capturing and analyzing RAM for active processes related to peripherals.
- **Live System Data Collection:** Capturing volatile artifacts (e.g., open files, network connections) linked to peripheral use.
- **Spooler Service & Print Queue Analysis (Live):** Real-time monitoring and acquisition.
- **Network Traffic Analysis for Peripherals:** Identifying print jobs or data transfers over the network.
- **Case Study: Live Acquisition to Catch an Ongoing Data Exfiltration**

Module 8: Reporting, Best Practices & Emerging Trends

- **Integrating Peripheral Evidence:** Incorporating findings into comprehensive forensic reports.
- **Legal Defensibility & Expert Testimony:** Presenting peripheral device evidence in court.
- **Developing Organizational Policies:** Mitigating risks associated with peripheral device usage.
- **Future of Peripheral Forensics:** IoT devices, smart home peripherals, and advanced tracking.
- **Case Study: A Hybrid Incident Combining Printer, USB, and Network Evidence**

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.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	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

Start Date	End Date	Location	Price
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