Training Course on Advanced USB Device 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

USB devices, ubiquitous in both personal and professional environments, have become critical vectors for data exfiltration, malware propagation, and insider threat activities. As adversaries grow more sophisticated, so too must the techniques employed by digital forensic investigators. Training Course on Advanced USB Device Forensics moves beyond basic artifact collection, focusing on the intricate forensic analysis of USB devices to uncover hidden data, reconstruct complex timelines, and link activity to specific users. Participants will delve into the nuances of various USB device types, their associated file systems, and the subtle digital footprints they leave behind on connected systems, enabling them to extract maximum intelligence from these often-overlooked sources of evidence.

This intensive program emphasizes cutting-edge techniques for dealing with encrypted USB drives, anti-forensic measures, and the challenges of recovering data from damaged or overwritten devices. Through hands-on labs and real-world USB forensics case studies, attendees will master advanced data carving, registry analysis, and the correlation of numerous system artifacts to build compelling investigative narratives. Equip yourself with the expertise to transform seemingly insignificant USB traces into pivotal evidence, significantly enhancing your organization's capability in cybercrime investigation, data breach response, and intellectual property protection.

Programme Curriculum

Training Course on Advanced USB Device Forensics

Introduction

USB devices, ubiquitous in both personal and professional environments, have become critical vectors for data exfiltration, malware propagation, and insider threat activities. As adversaries grow more sophisticated, so too must the techniques employed by digital forensic investigators. Training Course on Advanced USB Device Forensics moves beyond basic artifact collection, focusing on the intricate forensic analysis of USB devices to uncover hidden data, reconstruct complex timelines, and link activity to specific users. Participants will delve into the nuances of various USB device types, their associated file systems, and the subtle digital footprints they leave behind on connected systems, enabling them to extract maximum intelligence from these often-overlooked sources of evidence.

This intensive program emphasizes cutting-edge techniques for dealing with encrypted USB drives, anti-forensic measures, and the challenges of recovering data from damaged or overwritten devices. Through hands-on labs and real-world USB forensics case studies, attendees will master advanced data carving, registry analysis, and the correlation of numerous system artifacts to build compelling investigative narratives. Equip yourself with the expertise to transform seemingly insignificant USB traces into pivotal evidence, significantly enhancing your organization's capability in cybercrime investigation, data breach response, and intellectual property protection.

Course Duration

10 Days

Course Objectives

1. Deep Dive into USB Device Anatomy: Understand the physical and logical structures of diverse USB devices (flash drives, external HDDs, mobile devices as USB, etc.).
2. Master Advanced Registry Forensics: Extract and interpret granular USB connection and usage artifacts from the Windows Registry (USBSTOR, MountPoints2, SetupAPI logs).
3. Analyze System Log Files for USB Activity: Identify and parse relevant entries in Windows Event Logs, Prefetch files, and Superfetch for device usage patterns.
4. Perform Comprehensive File System Analysis: Uncover hidden or deleted data on USB devices using advanced techniques for FAT, NTFS, exFAT, and HFS+ file systems.
5. Conduct Data Carving & File Recovery: Utilize specialized tools and methodologies to recover fragmented or overwritten files from USB storage.
6. Investigate Anti-Forensic Techniques: Detect and counter methods used to erase, conceal, or obfuscate USB usage traces and data.
7. Reconstruct Timelines of USB Activity: Correlate timestamps from multiple artifacts to create precise chronological sequences of device connection, data transfer, and execution.

8. Analyze Shortcut Files (LNK) & Jump Lists: Extract critical information about recently accessed files and folders related to USB devices.
9. Examine ShellBags & UserAssist Artifacts: Gain insights into user interaction with USB-connected folders and applications.
10. Address Encrypted USB Devices: Explore methods and challenges of analyzing BitLocker, VeraCrypt, and other encrypted USB storage.
11. Leverage Automated USB Forensic Tools: Utilize and customize advanced commercial and open-source tools for efficient and thorough USB artifact analysis.
12. Integrate USB Forensics into Broader Investigations: Understand how USB evidence complements network, memory, and endpoint forensics for holistic case building.
13. Present Defensible USB Forensic Findings: Prepare detailed, clear, and legally sound reports based on complex USB device analysis for court or internal proceedings.

Organizational Benefits

1. Enhanced Insider Threat Detection: Quicker identification of data exfiltration and unauthorized device usage.
2. Improved Data Breach Investigations: Pinpoint the source and scope of data breaches involving USB devices.
3. Stronger Intellectual Property Protection: Better capability to detect and prove theft of confidential information.
4. Accelerated Incident Response: Rapidly identify and analyze malicious USB-borne threats.
5. Reduced Litigation Risk: Provide robust, admissible digital evidence in legal proceedings.
6. Proactive Security Posture: Insights gained from USB forensics can inform and strengthen organizational security policies.
7. Comprehensive Digital Evidence Collection: Ensure no critical evidence from USB devices is overlooked.
8. Increased Investigative Efficiency: Streamlined processes for USB artifact analysis.
9. Upskilled Forensic Team: Elevate the expertise of internal cybersecurity and forensic staff.
10. Compliance & Audit Readiness: Demonstrate adherence to data handling and security policies.

Target Participants

- Digital Forensic Examiners
- Incident Responders
- Law Enforcement Investigators
- Cybersecurity Analysts
- Fraud Investigators
- E-Discovery Specialists
- IT Security Managers
- Internal Audit Professionals

- Legal Professionals (with technical interest)
- Threat Intelligence Analysts

Course Outline

Module 1: Foundations of USB Forensics & Device Recognition

- **Introduction to USB Device Forensics:** Scope, importance, and common scenarios.
- **USB Device Architecture:** Understanding USB standards (2.0, 3.0, C), device classes, and data transfer modes.
- **Identifying USB Devices:** Physical identification, device enumeration, and vendor/product IDs.
- **Windows USB Artifacts Overview:** Introduction to key registry keys, logs, and files.
- **Case Study: Unmasking an Unknown USB Device**

Module 2: Advanced Windows Registry Analysis for USB

- **USBSTOR Key Deep Dive:** Extracting device identifiers, serial numbers, and first/last connection times.
- **MountedDevices Key Analysis:** Identifying drive letters and volume GUIDs associated with USB devices.
- **SetupAPI Logs (setupapi.dev.log):** Analyzing device installation and removal events, timestamps.
- **User Profile Hives (NTUSER.DAT):** Locating USB usage traces within individual user contexts.
- **Case Study: Reconstructing USB Device Insertion History**

Module 3: System Log Files & Event Tracing for USB Activity

- **Windows Event Logs (System, Security, Microsoft-Windows-DriverFrameworks-UserMode/Operational):** Identifying USB insertion/removal events, error codes.
- **Prefetch & Superfetch Files (.pf, .db):** Detecting execution of programs from USB devices.
- **SRUM (System Resource Usage Monitor) Artifacts:** Analyzing resource usage by processes run from USB.
- **Windows.old & Recycle Bin Analysis:** Recovering deleted files and user activities related to USB.
- **Case Study: Linking USB Device Connection to Malware Execution**

Module 4: File System Forensics on USB Devices

- **FAT/FAT32 Forensics:** Understanding directory structures, clusters, and deleted file recovery.
- **NTFS Forensics:** MFT analysis, $LogFile, $UsnJrnl, and advanced data recovery.
- **exFAT & HFS+ Considerations:** Unique challenges and techniques for non-Windows file systems on USB.
- **File Carving Techniques:** Recovering data fragments from unallocated space on USB drives.
- **Case Study: Recovering Deleted Files from a USB Flash Drive**

Module 5: Shortcut Files (LNK) & Jump Lists Analysis

- **LNK File Structure & Interpretation:** Extracting target paths, volume information, and timestamps for files accessed on USB.

- **Jump List Analysis (AutomaticDestinations, CustomDestinations):** Discovering recently opened documents and applications from USB devices.
- **Correlating LNK/Jump List data with USBSTOR:** Linking file access to specific connected devices.
- **Automated Parsers for LNK/Jump Lists:** Utilizing tools for efficient artifact extraction.
- **Case Study: Identifying Files Copied To/From a USB Device**

Module 6: ShellBags & UserAssist for User Interaction

- **ShellBags Analysis:** Reconstructing user navigation and folder access on USB devices, including previously connected network shares.
- **UserAssist Key Forensics:** Revealing executed programs and accessed folders, often including those on USB.
- **Correlating ShellBags/UserAssist with System Timestamps:** Building a timeline of user interaction.
- **Forensic Tooling for ShellBags and UserAssist:** Utilizing specialized parsers.
- **Case Study: Uncovering Hidden Folder Access on a USB External Drive**

Module 7: Browser, Email & Application Forensics for USB Interactions

- **Web Browser History & Downloads:** Tracing files downloaded to or from USB devices.
- **Email Client Artifacts:** Investigating attachments saved from/to USB, or sent from files on USB.
- **Application-Specific Logs:** Analyzing logs from applications that interact with external storage.
- **Cloud Sync Client Artifacts:** Evidence of data transferred to/from cloud via USB-connected devices.
- **Case Study: Tracing Data Exfiltration via Web Uploads from USB**

Module 8: Addressing Encrypted & Protected USB Devices

- **BitLocker To Go Forensics:** Understanding encryption, recovery keys, and acquisition challenges.
- **VeraCrypt/TrueCrypt Analysis:** Identification of encrypted containers and potential decryption strategies.
- **Other Encryption Solutions:** Overview of hardware-encrypted USB drives and proprietary software.
- **Challenges of Brute-Forcing & Password Recovery:** Limitations and ethical considerations.
- **Case Study: Attempting Data Recovery from an Encrypted USB Drive**

Module 9: Anti-Forensic Techniques & Evasion

- **Data Wiping & Shredding:** Detecting and recovering from secure deletion utilities.
- **Steganography on USB Devices:** Identifying hidden data within innocent-looking files.
- **USB Anti-Forensic Tools:** Analyzing tools designed to erase USB connection traces.
- **Forensic Countermeasures:** Techniques to bypass or mitigate anti-forensic attempts.
- **Case Study: Unmasking a Data Wiping Operation on a USB Stick**

Module 10: Damaged & Physically Impaired USB Devices

- **Physical Damage Assessment:** Identifying types of damage and their impact on data recovery.

- **Chip-Off Forensics (Introduction):** Overview of advanced techniques for physically extracting data from NAND flash.
- **Monolith Devices:** Challenges and specialized approaches for integrated USB controllers.
- **Professional Data Recovery Services:** When and how to engage external expertise.
- **Case Study: Recovering Data from a Partially Damaged USB Drive**

Module 11: Linux & macOS USB Forensics

- **Linux USB Artifacts:** /var/log, .bash_history, udev rules, and device files.
- **macOS USB Artifacts:** Unified logs, com.apple.usbd logs, .DS_Store, and fseventsd logs.
- **Cross-Platform Artifact Correlation:** Combining evidence from different operating systems.
- **Open-Source Tools for Linux/macOS USB Forensics:** Utilizing specific utilities.
- **Case Study: Investigating a USB Device Used on a Linux Workstation**

Module 12: Advanced USB Forensic Tooling

- **Commercial Forensic Suites (Magnet AXIOM, EnCase, FTK):** Deep dive into USB artifact parsing capabilities.
- **Specialized USB Forensic Tools (USB Detective, USBLogView, RegRipper plugins):** Focused utilities for specific artifacts.
- **Scripting for USB Forensics (Python, PowerShell):** Automating artifact extraction and analysis.
- **Developing Custom Parsers:** Creating scripts for unique or obscure USB artifacts.
- **Case Study: Efficiently Processing Multiple USB Device Images**

Module 13: Timeline Reconstruction & Correlation

- **Developing a Comprehensive Timeline:** Integrating USB connection times with file access, execution, and user activity.
- **UTC vs. Local Time Concerns:** Handling time zone discrepancies in evidence.
- **Timeline Analysis Tools:** Using Supertimeline, TimeSketch, and custom scripts for visualization.
- **Correlating USB Events with Network & System Activity:** Building a holistic picture of the incident.
- **Case Study: Building a Chronology of a Data Theft Incident involving USB**

Module 14: Legal Considerations & Expert Reporting

- **Legal Admissibility of USB Evidence:** Ensuring chain of custody, integrity, and foundational requirements.
- **Ethical Considerations:** Data minimization, privacy, and scope of investigation.
- **Crafting Expert Reports for USB Forensics:** Structure, clarity, and defensibility.
- 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

Start Date	End Date	Location	Price
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