Registry Forensics for Windows Systems Training Course

Professional Development Training Course Outline

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

Course Introduction

Introduction

The Windows Registry, often described as the "brain" of the Windows operating system, is an indispensable repository of critical system and user activity data. In the realm of digital forensics and incident response, a deep understanding of Registry forensics is paramount for uncovering crucial evidence of malicious activity, user behavior, and system configurations. Training Course on Registry Forensics for Windows Systems provides a comprehensive deep dive into the intricate structure and volatile nature of the Windows Registry, equipping participants with the advanced techniques and tools necessary to extract, interpret, and validate forensic artifacts for robust investigations.

This course moves beyond basic Registry exploration, focusing on advanced artifact analysis, timeline reconstruction, and identifying persistence mechanisms used by attackers. Through a blend of theoretical knowledge and extensive hands-on labs, attendees will learn to navigate various Registry hives, decipher complex data structures, and leverage both open-source and commercial forensic software to piece together the narrative of an incident. By mastering Registry forensics, professionals will significantly enhance their ability to detect insider threats, analyze malware infections, and support legal proceedings with irrefutable digital evidence.

Programme Curriculum

Registry Forensics for Windows Systems Training Course

Introduction

The Windows Registry, often described as the "brain" of the Windows operating system, is an indispensable repository of critical system and user activity data. In the realm of digital forensics and incident response, a deep understanding of Registry forensics is paramount for uncovering crucial evidence of malicious activity, user behavior, and system configurations. Registry Forensics for Windows Systems Training Course provides a comprehensive deep dive into the intricate

structure and volatile nature of the Windows Registry, equipping participants with the advanced techniques and tools necessary to extract, interpret, and validate forensic artifacts for robust investigations.

This course moves beyond basic Registry exploration, focusing on advanced artifact analysis, timeline reconstruction, and identifying persistence mechanisms used by attackers. Through a blend of theoretical knowledge and extensive hands-on labs, attendees will learn to navigate various Registry hives, decipher complex data structures, and leverage both open-source and commercial forensic software to piece together the narrative of an incident. By mastering Registry forensics, professionals will significantly enhance their ability to detect insider threats, analyze malware infections, and support legal proceedings with irrefutable digital evidence.

Course Duration

10 Days

Course Objectives

Comprehend the architecture and fundamental principles of the Windows Registry.

Accurately locate and acquire Registry hive files from live and dead systems.

Utilize specialized Registry forensic tools for efficient data extraction and parsing.

Analyze the SAM hive to reconstruct user account information, login times, and password hashes.

Examine the SECURITY hive for system-wide security settings and policies.

Investigate the SOFTWARE hive to identify installed programs, operating system details, and network configurations.

Interpret the SYSTEM hive for system boot information, service configurations, and control sets.

Uncover user activity through NTUSER.DAT analysis, including opened files, typed URLs, and search queries.

Decipher USRCLASS.DAT for user-specific settings, ShellBags, and application usage.

Reconstruct USB device connection history and associated user activities.

Identify malware persistence mechanisms leveraging Registry run keys, services, and scheduled tasks.

Perform timeline reconstruction using Registry timestamps to establish event sequences.

Generate forensically sound reports detailing Registry findings for legal and technical audiences.

Organizational Benefits

Enhanced Incident Detection: Quicker identification of malicious activity and system compromises.

Improved Forensic Investigations: Deeper insights into user actions and attacker methodologies.

Strengthened Insider Threat Detection: Ability to proactively identify and respond to internal malicious activities.

Effective Malware Analysis: Pinpointing malware persistence and impact through Registry artifacts.

Reduced Recovery Time: Faster and more accurate incident response leads to quicker system restoration.

Compliance with Regulations: Ensuring adherence to data handling and investigative standards.

Stronger Legal Defensibility: Producing admissible digital evidence for legal proceedings.

Cost Savings: Reducing reliance on external forensic experts for Windows-based investigations.

Proactive Security Posture: Understanding Registry vulnerabilities to improve system hardening.

Valuable Threat Intelligence: Deriving actionable intelligence from Registry artifacts to enhance security controls.

Target Audience

Digital Forensics Analysts

Incident Responders

Cybersecurity Analysts

Law Enforcement Investigators

IT Security Professional

System Administrators with Security Responsibilities

Security Operations Center (SOC) Analysts

e-Discovery Professionals

Internal Audit Professionals

Malware Analysts

Course Outline

Module 1: Introduction to Windows Registry Forensics

- **What is the Windows Registry?** Structure, purpose, and its role in digital investigations.
- **Registry Hives & Files:** Understanding the physical location and logical organization of hives.
- **Importance in Forensics:** Why the Registry is a goldmine for evidence.
- **Forensic Soundness & Acquisition:** Best practices for preserving Registry integrity.
- **Case Study:** Overview of a real-world incident solved primarily through Registry analysis.

Module 2: Registry Acquisition Techniques

- **Live Acquisition of Hives:** Using built-in tools like reg save and forensic tools.
- **Offline Acquisition from Disk Images:** Extracting hives from forensic disk images.
- **Volume Shadow Copies (VSCs):** Leveraging VSCs for historical Registry data.
- **Memory Forensics & Registry:** Extracting Registry data from volatile memory.
- **Case Study:** Acquiring Registry hives from a running, compromised server.

Module 3: Core Registry Forensic Tools

- **Registry Editor (RegEdit.exe):** Basic navigation and viewing.
- **Registry Explorer & RegRipper:** Advanced parsing and artifact extraction.
- **Volatility Framework (Registry Plugins):** Analyzing Registry data from memory dumps.
- **Other Specialized Tools:** Overview of various commercial and open-source solutions.
- **Case Study:** Comparing artifact extraction capabilities of different tools on a sample hive.

Module 4: SAM Hive Analysis

- **User Account Information:** Extracting usernames, SIDs, and last login times.
- **Password Hashes (and their limitations):** Understanding the SAM hive's role in password storage.
- **Group Membership & Privileges:** Identifying user and group access levels.
- **Account Creation & Modification Dates:** Tracing user lifecycle events.
- **Case Study:** Identifying unauthorized user accounts and their activities.

Module 5: SECURITY Hive Analysis

- **Security Policies & Settings:** Examining password policies, lockout policies, and audit settings.
- **Domain Information:** Understanding domain membership and associated security configurations.
- **LSA Secrets & Cached Credentials:** Exploring potential sensitive data.
- **Service Account Information:** Identifying accounts used by system services.
- **Case Study:** Discovering a policy misconfiguration exploited by an attacker.

Module 6: SOFTWARE Hive Analysis

- **Installed Programs & Versions:** Identifying software present on the system.
- **Operating System Information:** OS version, build, and installation details.
- **Wireless Network Connections (WLAN):** SSIDs, connection times, and security types.
- **File Associations:** Understanding how file types are handled by the system.
- **Case Study:** Tracing the installation of unauthorized software by an employee.

Module 7: SYSTEM Hive Analysis

- **Control Sets:** Understanding current, default, last known good configurations.
- **Computer Name & Domain Membership:** Identifying system identity.
- **Time Zone & System Time:** Correlating events with accurate timestamps.
- **Services & Drivers:** Identifying legitimate and malicious services.
- **Case Study:** Reconstructing system boot history and identifying abnormal shutdowns.

Module 8: NTUSER.DAT Analysis (User Activity)

- **Most Recently Used (MRU) Lists:** Documents, applications, and search queries.
- **Typed URLs & Internet History (Registry artifacts):** Web Browse activity remnants.
- **UserAssist Key:** Tracking executed applications and their last execution times.
- **RunMRU & OpenSaveMRU:** Files opened/saved through common dialogs.
- **Case Study:** Profiling a user's activity to determine intent in an intellectual property theft case.

Module 9: USRCLASS.DAT & ShellBags

- **ShellBags Forensics:** Understanding folder access history, even for deleted or removable media.
- **Jump Lists & Recent Docs (User Specific):** Identifying recently accessed files and programs.
- **MuiCache:** Application execution and usage statistics.
- **Windows Shell Items:** Various user-interface related artifacts.
- **Case Study:** Using ShellBags to prove access to sensitive network shares.

Module 10: USB Device Forensics through Registry

- **USB Device Connection History:** Identifying connected USB devices and their timestamps.
- **Volume Serial Numbers & Mount Points:** Tracing specific storage devices.
- **Device Classes & Vendors:** Identifying types of connected peripherals.
- **Driver Information for USB Devices:** Understanding device installation.
- **Case Study:** Linking a specific USB drive to data exfiltration from a workstation.

Module 11: Malware Persistence Mechanisms in Registry

- **Run Keys & RunOnce Keys:** Common auto-start locations for malicious executables.
- **Services Key Analysis:** Identifying malicious services configured for persistence.
- **Scheduled Tasks (Registry remnants):** Tracing tasks created for recurring malicious activity.
- **Image File Execution Options (IFEO):** Debuggers and process hijacking.
- **Case Study:** Uncovering how ransomware achieved persistence through Registry modifications.

Module 12: Advanced Registry Artifacts & Timelining

- **ShimCache (AppCompatCache):** Executable execution history and file metadata.
- **AmCache:** Detailed application compatibility and execution data.
- **Background Activity Moderator (BAM) / Desktop Activity Moderator (DAM):** Monitoring background process execution.
- **Prefetch Files (Registry related):** Program execution and associated files.
- **Case Study:** Building a comprehensive timeline of events using multiple Registry artifacts to reconstruct an intrusion.

Module 13: Correlating Registry Data with Other Artifacts

- **Registry & Event Logs:** Cross-referencing Registry changes with system events.
- **Registry & File System Timestamps:** Aligning Registry events with file system activities.
- **Registry & Network Logs:** Correlating Registry entries with network connections.
- **Memory Dumps & Registry:** Enhancing live analysis with memory forensics.
- **Case Study:** Connecting a Registry-based persistence mechanism to network beaconing activity.

Module 14: Practical Registry Investigation Workflow

- **Developing an Investigation Plan:** Integrating Registry analysis into the overall strategy.
- **Tool Selection & Validation:** Choosing the right tools for specific Registry analysis tasks.
- **Automated vs. Manual Analysis:** Balancing efficiency with depth.
- **Handling Large Datasets:** Strategies for managing and analyzing extensive Registry data.
- **Case Study:** End-to-end investigation scenario demonstrating a complete Registry forensics workflow.

Module 15: Reporting & Legal Aspects of Registry Forensics

- **Structuring Forensic Reports:** Presenting Registry findings clearly and concisely.
- **Documenting Chain of Custody:** Ensuring evidence integrity.
- **Visualizing Registry Data:** Graphical representations for easier understanding.
- **Admissibility of Registry Evidence:** Meeting legal standards for court presentation.
- **Case Study:** Preparing a mock expert report based on a Registry investigation, ready for court presentation.

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 c

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

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

Register Online Now

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