Training Course on Windows Server 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

Windows Servers form the backbone of most enterprise IT infrastructures, hosting critical applications, databases, and user data. Consequently, they are prime targets for sophisticated cyberattacks, making Windows Server forensics an indispensable skill for modern incident responders and digital forensic investigators. Training Course on Windows Server Forensics is meticulously designed to equip professionals with the deep technical expertise required to effectively investigate security breaches, insider threats, and data exfiltration incidents on Windows Server operating systems. Participants will learn to navigate the complexities of server environments, analyze high-volume log data, uncover stealthy persistence mechanisms, and reconstruct attack timelines with unparalleled precision, transforming raw data into actionable digital evidence.

This comprehensive program delves beyond basic workstation forensics, focusing on server-specific artifacts, Active Directory forensics, cloud-integrated server environments, and the nuances of large-scale data acquisition from critical production systems. Through intensive hands-on labs, real-world breach simulations, and advanced tooling, attendees will master techniques for correlating disparate server logs, identifying lateral movement, analyzing memory dumps from compromised servers, and understanding the intricate interplay between on-premises and hybrid cloud server components. Elevate your forensic capabilities to effectively respond to the most challenging server compromise investigations and safeguard your organization's most valuable digital assets.

Programme Curriculum

Training Course on Windows Server Forensics

Introduction

Windows Servers form the backbone of most enterprise IT infrastructures, hosting critical applications, databases, and user data. Consequently, they are prime targets for sophisticated cyberattacks, making Windows Server forensics an indispensable skill for modern incident responders and digital forensic investigators. Training Course on Windows Server Forensics is meticulously designed to equip professionals with the deep technical expertise required to effectively investigate security breaches, insider threats, and data exfiltration incidents on Windows Server operating systems. Participants will learn to navigate the complexities of server environments, analyze high-volume log data, uncover stealthy persistence mechanisms, and reconstruct attack timelines with unparalleled precision, transforming raw data into actionable digital evidence.

This comprehensive program delves beyond basic workstation forensics, focusing on server-specific artifacts, Active Directory forensics, cloud-integrated server environments, and the nuances of large-scale data acquisition from critical production systems. Through intensive hands-on labs, real-world breach simulations, and advanced tooling, attendees will master techniques for correlating disparate server logs, identifying lateral movement, analyzing memory dumps from compromised servers, and understanding the intricate interplay between on-premises and hybrid cloud server components. Elevate your forensic capabilities to effectively respond to the most challenging server compromise investigations and safeguard your organization's most valuable digital assets.

Course Duration

5 Days

Course Objectives

1. Master Windows Server Architecture: Understand the core components and forensic implications of Windows Server operating systems (2012, 2016, 2019, 2022).
2. Conduct Forensically Sound Server Acquisition: Safely acquire full disk images, memory dumps, and targeted artifacts from live and dead Windows Servers.
3. Perform Advanced Event Log Analysis: Deeply analyze security, system, application, and specialized logs for indicators of compromise (IOCs) and attack narratives.
4. Investigate Active Directory Compromises: Uncover evidence of unauthorized access, privilege escalation, and lateral movement within Active Directory environments.
5. Analyze Server Registry Hives: Extract critical system configuration, installed software, and user activity artifacts from server registry hives.
6. Examine Server File Systems: Recover deleted files, analyze NTFS metadata, and identify hidden data streams on server volumes.

7. Conduct Memory Forensics on Servers: Analyze large memory dumps to identify malicious processes, injected code, and network connections.
8. Detect Persistence Mechanisms: Identify and analyze various techniques attackers use to maintain access on compromised servers (e.g., Scheduled Tasks, Services, WMI).
9. Trace Lateral Movement & Pivoting: Follow the trail of an attacker moving between servers and endpoints within an enterprise network.
10. Automate Server Artifact Collection: Leverage scripting (PowerShell) and forensic tools for efficient and scalable data collection from multiple servers.
11. Investigate Web Server & Database Compromises: Analyze IIS, Apache, SQL Server, and other application-specific logs for breach indicators.
12. Address Cloud-Integrated Server Forensics: Understand forensic challenges and acquire evidence from hybrid server environments utilizing Azure AD, AWS EC2, or GCP.
13. Generate Comprehensive Forensic Reports: Produce detailed, technical, and legally defensible reports outlining server compromise investigations.

Organizational Benefits

1. Accelerated Incident Response: Rapidly identify, contain, and eradicate threats impacting critical server infrastructure.
2. Minimized Breach Impact: Reduce downtime and data loss by efficiently responding to server compromises.
3. Enhanced Security Posture: Proactive identification of vulnerabilities and misconfigurations leading to server exposures.
4. Improved Compliance & Audit Readiness: Demonstrate robust investigative capabilities for regulatory compliance.
5. Stronger Insider Threat Detection: Uncover evidence of malicious activity by internal actors on servers.
6. Better Root Cause Analysis: Pinpoint the exact entry points and attack methodologies used to compromise servers.
7. Reduced Litigation Risk: Produce high-quality, admissible digital evidence for legal proceedings.
8. Optimized Security Investments: Maximize the effectiveness of existing security tools and processes through enhanced forensic understanding.
9. Skilled Internal Workforce: Develop in-house expertise to handle complex server-side investigations independently.
10. Protection of Critical Business Assets: Safeguard intellectual property, customer data, and core operational systems.

Target Participants

- Digital Forensic Investigators

- Incident Response Team Leads & Members
- Security Operations Center (SOC) Analysts (Tier 2/3)
- System Administrators with Security Responsibilities
- Cybersecurity Engineers
- Threat Hunters
- IT Auditors
- Network Security Specialists
- Malware Analysts
- Enterprise Architects (involved in security design)

Course Outline

Module 1: Windows Server Architecture & Foundational Forensics

- **Windows Server OS Overview:** Key differences from workstations, server roles (AD, DNS, DHCP, Web).
- **Server Imaging & Acquisition:** Best practices for live vs. dead acquisition, physical vs. logical, tools (FTK Imager, KAPE).
- **Order of Volatility for Servers:** Prioritizing data collection in a live server environment.
- **File Systems on Servers:** Deep dive into NTFS artifacts (MFT, $LogFile, $UsnJrnl).
- **Case Study: Initial Triage of a Potentially Compromised Domain Controller**

Module 2: Event Log Analysis for Server Incidents

- **Advanced Event Log Parsing:** Security, System, Application, PowerShell, Remote Desktop (RDP) logs.
- **Critical Event IDs:** Understanding key indicators for logon failures, account lockouts, process creation, service installations.
- **Log Forwarding & Aggregation:** Analyzing logs from centralized SIEMs (Splunk, ELK Stack, Azure Sentinel).
- **Identifying Anti-Forensic Techniques:** Detecting cleared event logs and log tampering.
- **Case Study: Tracing Brute-Force Attacks and Successful Logons**

Module 3: Active Directory & Domain Controller Forensics

- **Active Directory Fundamentals:** Understanding Domain Controllers, users, groups, GPOs, trusts.
- **AD-Specific Logs:** Directory Service, Replication, and DNS Server logs.
- **Detecting Compromised Accounts:** Kerberos tickets (Golden/Silver Ticket), Pass-the-Hash.
- **Analyzing Group Policy Objects (GPOs):** Identifying malicious policy changes and persistence.
- **Case Study: Investigating a Domain Admin Account Compromise**

Module 4: Server Memory Forensics & Malware Analysis

- **Memory Acquisition from Servers:** Challenges and techniques for large RAM sizes (e.g., WinPmem, DumpIt).
- **Volatility Framework Deep Dive:** Analyzing processes, network connections, loaded modules, injected code from memory dumps.
- **Identifying Malware on Servers:** Rootkits, backdoors, in-memory threats.

- **Extracting Credentials from Memory:** Mimikatz artifacts, LSASS dumps.
- **Case Study: Analyzing a Ransomware Attack Through Memory Forensics**

Module 5: Server Persistence & Lateral Movement Techniques

- **Common Persistence Mechanisms:** Scheduled Tasks, Services, Run Keys, WMI persistence.
- **Lateral Movement Indicators:** PsExec, Remote Desktop Protocol (RDP), SMB shares, WinRM.
- **Service Control Manager & Task Scheduler Analysis:** Detecting malicious service installations and scheduled tasks.
- **Registry Forensics for Server Persistence:** Analyzing HKLM\SYSTEM, HKLM\SOFTWARE hives for unauthorized changes.
- **Case Study: Tracing an Attacker's Lateral Movement Across Servers**

Module 6: Web Server, Database, & Application Forensics

- **IIS Web Server Forensics:** Analyzing W3SVC logs, application pools, configuration files.
- **SQL Server Forensics:** Audit logs, error logs, transaction logs, database integrity checks.
- **Application-Specific Logs:** Analyzing logs from common business applications running on servers.
- **Identifying Web Shells & Backdoors:** Techniques for detecting compromised web applications.
- **Case Study: Investigating a Web Server Defacement and Database Compromise**

Module 7: Cloud-Integrated & Hybrid Server Forensics

- **Forensic Challenges in Hybrid Environments:** Data visibility, shared responsibility, API logging.
- **Azure AD & Hybrid Identity Forensics:** Analyzing Azure AD audit logs, sign-in logs, and PIM for suspicious activity.
- **AWS EC2 & GCP Compute Engine Forensics:** Acquiring and analyzing instance snapshots, CloudTrail, GuardDuty, and GCP Audit Logs.
- **Correlating Cloud & On-Premises Evidence:** Unifying timelines and attacker narratives across hybrid infrastructure.
- **Case Study: Investigating a Lateral Move from On-Premises to Cloud Server**

Module 8: Reporting, Remediation & Forensic Readiness

- **Structuring a Server Forensic Report:** Executive summary, technical findings, recommendations.
- **Presenting Findings to Stakeholders:** Communicating technical details to non-technical audiences.
- **Remediation & Hardening Strategies:** Implementing lessons learned from forensic investigations.
- **Building a Server Forensic Readiness Program:** Proactive logging, data retention, and incident response planning.
- **Case Study: Full Post-Mortem Analysis and Reporting for a Server Breach**

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 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
21 Sep 2026	25 Sep 2026	Online	$1,000

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 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