Training Course on Network 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

In the evolving digital threat landscape, Network Device Forensics has become an indispensable part of cybersecurity investigations. Organizations depend on routers, switches, and firewalls for seamless communication and protection, making these network devices a prime target for cyberattacks. Training Course on Network Device Forensics equips cybersecurity professionals, network engineers, and IT investigators with the skills to analyze, interpret, and investigate digital artifacts within critical infrastructure components. The course highlights the importance of deep-packet inspection, firmware analysis, configuration audits, and log correlation to uncover indicators of compromise and persistent threats.

This course is designed with the latest forensic techniques, industry best practices, and compliance standards such as NIST, ISO 27001, and MITRE ATT&CK. It prepares learners to recognize malicious behaviors hidden within network traffic, retrieve and preserve logs from routers and firewalls, and trace back attacks using network telemetry. From device-level evidence acquisition to chain-of-custody documentation, participants will learn to support both internal security operations and legal proceedings with defensible forensic analysis.

Programme Curriculum

Training Course on Network Device Forensics

Introduction

In the evolving digital threat landscape, Network Device Forensics has become an indispensable part of cybersecurity investigations. Organizations depend on routers, switches, and firewalls for seamless communication and protection, making these network devices a prime target for cyberattacks. Training Course on Network Device Forensics equips cybersecurity professionals, network engineers, and IT investigators with the skills to analyze, interpret, and investigate digital artifacts within critical infrastructure components. The course highlights the importance of deep-packet inspection, firmware analysis, configuration audits, and log correlation to uncover indicators of compromise and persistent threats.

This course is designed with the latest forensic techniques, industry best practices, and compliance standards such as NIST, ISO 27001, and MITRE ATT&CK. It prepares learners to recognize malicious behaviors hidden within network traffic, retrieve and preserve logs from routers and firewalls, and trace back attacks using network telemetry. From device-level evidence acquisition to chain-of-custody documentation, participants will learn to support both internal security operations and legal proceedings with defensible forensic analysis.

Course Objectives

1. Understand the fundamentals of network forensics and packet-level analysis.
2. Identify forensic artifacts from router logs and switch memory dumps.
3. Apply deep-packet inspection (DPI) techniques to detect anomalies.
4. Analyze and correlate firewall logs to reconstruct attack paths.
5. Perform configuration file audits for security misconfigurations.
6. Conduct firmware reverse engineering to detect tampering.
7. Develop strategies for incident response and threat attribution.
8. Implement network monitoring and logging best practices.
9. Create forensic reports for internal audits and legal evidence.
10. Use open-source and commercial tools for device forensics.
11. Understand compliance with GDPR, HIPAA, and NIST standards.
12. Utilize SIEM integration for correlating network data.
13. Demonstrate chain of custody and data integrity in forensic investigations.

Target Audience

1. Cybersecurity Analysts
2. Network Engineers
3. IT Auditors
4. Incident Response Teams
5. Law Enforcement Cyber Units
6. Digital Forensics Investigators
7. Penetration Testers
8. Compliance and Risk Officers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Network Device Forensics

- Overview of routers, switches, and firewalls
- Importance of network device forensics in cybersecurity
- Forensic challenges and limitations
- Device evidence identification and preservation
- Legal implications and chain of custody
- **Case Study**: Investigating unauthorized access via a compromised home router

Module 2: Router Forensics Techniques

- Router architecture and OS (Cisco IOS, Juniper JunOS)
- Log extraction and analysis (Syslog, NetFlow)
- NVRAM and RAM forensic analysis
- Identifying rogue configurations and firmware tampering
- Command history reconstruction and user tracking
- **Case Study**: Detecting data exfiltration through router backdoor

Module 3: Switch Forensics and Data Flow Analysis

- VLANs and switch traffic behavior
- MAC address table analysis
- Spanning Tree Protocol (STP) exploitation
- Port mirroring for evidence acquisition
- ARP cache and session hijacking detection
- **Case Study**: Tracing lateral movement across internal VLANs

Module 4: Firewall Log Analysis and Policy Audits

- Firewall types (stateful, stateless, NGFW)
- Log interpretation (deny/allow rules, connection logs)
- Auditing ACLs and NAT configurations
- Detecting rule manipulation and bypass techniques
- Identifying port scanning and DDoS attempts
- **Case Study**: Rule misconfiguration allowing unauthorized SSH access

Module 5: Packet Capture and Deep-Packet Inspection

- Capturing live traffic with tcpdump, Wireshark, Zeek
- Session reconstruction and protocol decoding
- Filtering malicious payloads
- SSL/TLS inspection techniques
- Encrypted traffic analysis using metadata
- **Case Study**: Analyzing packet captures from a suspected phishing campaign

Module 6: Firmware Forensics and Reverse Engineering

- Extracting firmware from network devices
- Static and dynamic firmware analysis
- Identifying embedded backdoors
- Tools: Binwalk, Ghidra, Firmware Mod Kit
- Firmware signature validation and integrity check
- **Case Study**: Dissecting a trojanized firmware image

Module 7: SIEM Integration and Threat Attribution

- Correlating device logs with SIEM (Splunk, ELK)
- Threat intelligence enrichment
- MITRE ATT&CK mapping of behaviors
- Timeline reconstruction of incidents
- Identifying threat actors and TTPs
- **Case Study**: Cross-device analysis of a targeted ransomware attack

Module 8: Reporting, Documentation, and Legal Readiness

- Creating admissible forensic reports
- Documentation standards and templates
- Presenting findings to legal and management teams
- Maintaining evidence integrity and timelines
- Handling subpoenas and legal disclosure
- **Case Study**: Preparing a forensic report for law enforcement submission

Training Methodology

- Interactive labs with real-world traffic and logs

- Step-by-step tool demonstrations (CLI and GUI-based)
- Case-based discussions with evidence walkthroughs
- Group exercises simulating real-world forensic investigations
- Downloadable templates and forensic report formats
- Knowledge assessments and practical scenarios at the end of each module

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
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
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