Network Forensics and Incident Response 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

In today’s rapidly evolving digital threat landscape, Network Forensics and Incident Response (NFIR) has become a vital discipline for cybersecurity professionals, IT teams, and government security agencies. With the surge in ransomware attacks, data breaches, and nation-state cyber espionage, organizations must be equipped with proactive skills and forensic intelligence to detect, analyze, mitigate, and recover from network-based incidents. Training Course on Network Forensics & Incident Response blends theoretical foundations with hands-on simulations using real-world cyber-attack case studies.

The course provides learners with cutting-edge tools, practical strategies, and tactical frameworks for responding to cyber threats in real time. Using industry-leading platforms, participants will gain comprehensive skills in packet analysis, log correlation, malware tracking, and incident lifecycle management, essential for any modern-day cybersecurity analyst, SOC engineer, or digital investigator. Whether combating insider threats or tracking external attackers, this course is designed to foster deep investigation capabilities and actionable response planning.

Programme Curriculum

Network Forensics and Incident Response Training Course

Introduction

In today’s rapidly evolving digital threat landscape, Network Forensics and Incident Response (NFIR) has become a vital discipline for cybersecurity professionals, IT teams, and government security agencies. With the surge in ransomware attacks, data breaches, and nation-state cyber espionage, organizations must be equipped with proactive skills and forensic intelligence to detect, analyze, mitigate, and recover from network-based incidents. Network Forensics and Incident Response Training Course blends theoretical foundations with hands-on simulations using real-world cyber-attack case studies.

The course provides learners with cutting-edge tools, practical strategies, and tactical frameworks for responding to cyber threats in real time. Using industry-leading platforms, participants will gain comprehensive skills in packet analysis, log correlation, malware tracking, and incident lifecycle management, essential for any modern-day cybersecurity analyst, SOC engineer, or digital investigator. Whether combating insider threats or tracking external attackers, this course is designed to foster deep investigation capabilities and actionable response planning.

Course Objectives

1. Understand the fundamentals of network forensics and its role in cyber threat intelligence.
2. Learn to detect and investigate malicious network activity using modern tools.
3. Perform real-time incident response and log analysis during attacks.
4. Master techniques in packet sniffing, deep packet inspection, and session reconstruction.
5. Analyze malware-infected traffic and extract Indicators of Compromise (IOCs).
6. Conduct forensic timeline reconstruction using network logs and packet captures.
7. Apply threat hunting methodologies to proactively uncover hidden threats.
8. Use SIEM tools for log correlation and alert prioritization.
9. Establish and follow incident response playbooks based on industry standards (NIST, SANS).
10. Build and report actionable forensic evidence for legal and compliance use.
11. Understand network protocol behaviors for anomaly detection and pattern matching.
12. Integrate automated response systems with manual investigation techniques.
13. Conduct post-incident reviews and recommend mitigation strategies.

Target Audiences

1. Cybersecurity Analysts
2. Security Operations Center (SOC) Engineers
3. IT Security Managers
4. Incident Response Teams
5. Digital Forensics Professionals
6. Government & Law Enforcement Cyber Units
7. Network Administrators
8. Ethical Hackers & Penetration Testers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Network Forensics

- Definition and scope of network forensics
- The role of forensics in cybersecurity
- Key terminologies and frameworks
- Differences between digital and network forensics
- Tools overview (Wireshark, TCPdump, Tshark)
- **Case Study:** Identifying rogue access points in a corporate network

Module 2: Networking Fundamentals for Forensics

- OSI model and data flow review
- TCP/IP protocols and forensic importance
- Packet structures and dissection
- Protocol behavior during attacks
- Common network devices and logs
- **Case Study:** Analysis of an internal DNS poisoning attack

Module 3: Capturing Network Traffic

- Packet sniffing tools and configuration
- Network taps and SPAN port usage
- Traffic filters and capture best practices
- Storage and retention policies
- Encryption considerations in traffic capture
- **Case Study:** Capture and decode command & control traffic

Module 4: Log Analysis & Correlation

- Syslog, Windows Event Logs, and NetFlow basics
- Log aggregation tools (Splunk, ELK Stack)
- Log normalization and parsing
- Pattern recognition and anomaly detection
- Correlating logs across multiple systems
- **Case Study:** Log-based detection of brute-force attacks

Module 5: Deep Packet Inspection (DPI)

- Understanding DPI engines
- Identifying payload anomalies
- Malware behavior via DPI
- DPI vs traditional IDS/IPS
- Integration with forensic platforms
- **Case Study:** DPI uncovering hidden data exfiltration

Module 6: Network Intrusion Detection & Forensics

- IDS/IPS architecture and placement
- Open-source IDS tools (Snort, Suricata)
- Alert tuning and signature customization
- Rule writing and traffic inspection
- Signature vs anomaly-based detection
- **Case Study:** Detecting SQL injection using Snort

Module 7: Malware Traffic Analysis

- Identifying malware behavior in network traffic
- Reverse engineering basics
- Malware sandboxing tools
- Static vs dynamic malware analysis
- Tracing callback and beaconing
- **Case Study:** Analyzing ransomware lateral movement

Module 8: Threat Intelligence Integration

- Sources of threat intelligence
- Threat feeds and IOC enrichment
- STIX, TAXII, and MISP integration
- Linking intelligence to forensics
- Intelligence-led incident response
- **Case Study:** Mitigating a phishing campaign using threat intel feeds

Module 9: Incident Response Lifecycle

- NIST/SANS IR framework overview

- Roles and responsibilities in an IR team
- Triage and escalation protocols
- Evidence preservation and chain of custody
- Post-incident reporting best practices
- **Case Study:** Coordinating a cross-department IR simulation

Module 10: Forensic Reporting & Documentation

- Report structure and objectives
- Legal considerations in reporting
- Visualizations using forensic data
- Stakeholder-centric documentation
- Compliance frameworks (HIPAA, GDPR)
- **Case Study:** Preparing legal-grade reports for a data breach

Module 11: Automation in Forensics

- Automating packet analysis and log parsing
- Python for network forensics
- SOAR platforms overview
- Benefits of automation in IR
- Case generation and ticketing integration
- **Case Study:** Automated IOC extraction and alerting pipeline

Module 12: Insider Threat Investigation

- Behavioral analysis and monitoring
- Data exfiltration detection
- Email and file transfer tracking
- Insider threat kill chain
- User behavior analytics (UBA)
- **Case Study:** Catching a privileged user data leak

Module 13: Cloud Forensics & Network Visibility

- Cloud network architecture (AWS, Azure, GCP)
- Cloud-native forensic tools
- Log collection in cloud environments
- SaaS & API traffic monitoring
- Cloud IR challenges and solutions
- **Case Study:** Investigating a misconfigured S3 bucket breach

Module 14: Wireless Network Forensics

- Wireless protocols and vulnerabilities
- Capturing Wi-Fi traffic (Aircrack-ng, Kismet)
- WPA2 cracking and handshake analysis
- Rogue AP detection and mitigation
- Wireless traffic filtering techniques
- **Case Study:** Breach via unauthorized access on a public Wi-Fi

Module 15: Red Team vs Blue Team Simulation

- Offensive vs defensive tactics
- Red team attack simulation
- Blue team detection and response

- Post-exercise debrief and improvement
- Practical exercise and tools comparison
- **Case Study:** Simulated APT attack and full-cycle response

Training Methodology

- Instructor-led theoretical sessions with interactive Q&A
- Real-time hands-on labs and simulations
- Use of open-source and enterprise-grade forensic tools
- Case study walkthroughs based on real-life cyber attacks
- Group activities and team-based forensic exercises
- Pre- and post-assessments to track knowledge retention

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	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
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