Network Forensics and Incident Response for Cybercrime 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

As cybercriminal activities escalate in complexity and frequency, Network Forensics and Incident Response have become critical components of digital security strategies. This cutting-edge course provides cybersecurity professionals, law enforcement agents, and IT personnel with advanced skills in identifying, analyzing, and mitigating cybercrime using digital footprints and forensic methodologies. Through hands-on labs, real-world simulations, and expert case studies, participants will learn how to detect, contain, and respond to sophisticated cyber attacks such as ransomware, phishing campaigns, DDoS attacks, and insider threats.

Training Course on Network Forensics & Incident Response for Cybercrime addresses key cyber challenges, covering malware reverse engineering, packet analysis, forensic acquisition, legal compliance, and threat intelligence integration. Participants will emerge as proactive responders and forensic analysts equipped to safeguard sensitive data, enhance organizational resilience, and align with global cybersecurity standards like NIST, ISO 27035, and GDPR. This course is essential for those aiming to lead digital investigations or improve cyber defense infrastructures in high-stakes environments.

Programme Curriculum

Network Forensics and Incident Response for Cybercrime Training Course

Introduction

As cybercriminal activities escalate in complexity and frequency, Network Forensics and Incident Response have become critical components of digital security strategies. This cutting-edge course provides cybersecurity professionals, law enforcement agents, and IT personnel with advanced skills in identifying, analyzing, and mitigating cybercrime using digital footprints and forensic methodologies. Through hands-on labs, real-world simulations, and expert case studies, participants will learn how to detect, contain, and respond to sophisticated cyber attacks such as ransomware, phishing campaigns, DDoS attacks, and insider threats.

Network Forensics and Incident Response for Cybercrime Training Course addresses key cyber challenges, covering malware reverse engineering, packet analysis, forensic acquisition, legal compliance, and threat intelligence integration. Participants will emerge as proactive responders and forensic analysts equipped to safeguard sensitive data, enhance organizational resilience, and align with global cybersecurity standards like NIST, ISO 27035, and GDPR. This course is essential for those aiming to lead digital investigations or improve cyber defense infrastructures in high-stakes environments.

Course Objectives

1. Understand the principles of network forensics and cybercrime analysis.
2. Apply packet sniffing and traffic analysis to detect intrusions.
3. Conduct digital evidence collection in compliance with legal protocols.
4. Utilize Wireshark, TCPDump, and other forensic tools for investigation.
5. Detect and respond to ransomware and phishing attacks.
6. Examine insider threats through log correlation and endpoint forensics.
7. Implement effective incident response frameworks (NIST, SANS).
8. Master live memory acquisition and volatile data preservation.
9. Perform malware analysis and behavior monitoring.
10. Develop incident reporting and breach documentation protocols.
11. Integrate threat intelligence in forensic investigations.
12. Analyze historical cybercrime cases to extract forensic insights.
13. Prepare for cyber forensic certifications (GCFA, CHFI, CCFP).

Target Audiences

1. Cybersecurity Analysts
2. Digital Forensic Investigators
3. Law Enforcement and Military Cyber Units
4. IT Security Managers
5. Risk and Compliance Officers
6. Network Administrators
7. Information Systems Auditors
8. Cybersecurity Students and Educators

Course Duration: 10 days

Course Modules

Module 1: Introduction to Network Forensics

- Definition and scope of network forensics
- Differences between network and computer forensics
- Importance in the digital age
- Challenges in network evidence collection
- Common tools used
- **Case Study:** 2021 Colonial Pipeline cyberattack

Module 2: Legal & Ethical Considerations

- Chain of custody and admissibility of digital evidence
- Cybercrime laws and international cooperation
- GDPR and HIPAA compliance
- Ethical dilemmas in digital investigations
- Policy development for IR

- **Case Study:** Facebook–Cambridge Analytica breach

Module 3: Packet Capture and Traffic Analysis

- Introduction to Wireshark and TCPDump
- Protocol dissection (HTTP, DNS, SMTP, FTP)
- Identifying anomalies and malicious traffic
- Flow analysis and filtering techniques
- Real-time vs post-event analysis
- **Case Study:** Detection of APT attack through traffic patterns

Module 4: Intrusion Detection & Prevention Systems

- Role of IDS/IPS in network forensics
- Signature vs anomaly-based detection
- Integration with SIEM tools
- Event correlation and alerting
- Incident validation and escalation
- **Case Study:** Use of Snort in detecting SQL injection attempts

Module 5: Malware and Payload Analysis

- Reverse engineering basics
- Behavioral and static analysis
- Sandboxing environments
- Signature extraction
- Payload detection techniques
- **Case Study:** WannaCry ransomware behavior investigation

Module 6: Insider Threat and Endpoint Forensics

- Identifying internal breaches
- Forensic imaging and endpoint data acquisition
- USB device tracking and data exfiltration
- Log and access control analysis
- Data Loss Prevention (DLP) tools
- **Case Study:** Snowden and NSA data leak analysis

Module 7: Cloud and Virtual Environment Forensics

- Challenges in cloud evidence collection
- AWS and Azure logging mechanisms
- Snapshots and disk imaging in cloud
- Role of hypervisors and virtual disks
- Legal considerations in cloud IR
- **Case Study:** Capital One AWS misconfiguration breach

Module 8: Incident Response Lifecycle

- Preparation and planning
- Detection and analysis
- Containment, eradication, and recovery
- Lessons learned and reporting
- Creating a CSIRT (Computer Security Incident Response Team)
- **Case Study:** Uber data breach incident response analysis

Module 9: Threat Intelligence Integration

- Threat feeds and analysis tools
- Indicators of Compromise (IOCs)
- Use of MITRE ATT&CK and STIX/TAXII
- Automating threat detection
- Linking TI to forensics workflows
- **Case Study:** SolarWinds supply chain attack

Module 10: Wireless Network Forensics

- Wireless sniffing and packet capture
- WEP/WPA cracking and analysis
- Rogue access point detection
- MAC spoofing investigations
- Mobile and IoT traffic forensics
- **Case Study:** Marriott Wi-Fi data breach

Module 11: Log Management and SIEM Analysis

- Centralized log collection tools
- Syslog, NetFlow, and application logs
- Event correlation techniques
- Setting up dashboards and alerts
- Use of ELK stack and Splunk
- **Case Study:** SIEM analysis in a ransomware attack

Module 12: Live Forensics & Memory Acquisition

- Importance of volatile data
- Tools for RAM imaging (FTK Imager, Volatility)
- Memory artifact extraction
- Analyzing running processes and open ports
- Challenges in live forensics
- **Case Study:** Fileless malware detection through memory dump

Module 13: DNS and Email Forensics

- Tracing spoofed emails and phishing attempts
- SPF, DKIM, and DMARC checks
- DNS tunneling detection
- Email header analysis
- Forensic investigation of webmail providers
- **Case Study:** Business Email Compromise (BEC) forensic response

Module 14: Reporting and Documentation

- Building comprehensive incident reports
- Technical vs executive summaries
- Maintaining chain of evidence
- Templates and IR documentation formats
- Regulatory reporting (GDPR, PCI-DSS)
- **Case Study:** Equifax breach reporting framework

Module 15: Certification Prep & Mock Forensic Challenge

- Overview of GCFA, CHFI, CCFP exams
- Practice questions and simulation

- Building a forensic lab setup
- Group-based forensic scenario challenge
- Skill assessment and feedback
- **Case Study:** Mock IR simulation of a real-world corporate breach

Training Methodology

- Interactive presentations and real-time demonstrations
- Hands-on labs using industry-standard tools
- Group-based forensic analysis exercises
- Simulation of live attack environments
- Expert-led case study discussions
- Evaluation through quizzes, practicals, and scenario-based tests

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
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