Training Course on Wireless Network Forensics and Security Incident Investigation

Professional Development Training Course Outline

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

Course Introduction

In today's hyper-connected digital world, wireless networks serve as the foundation of modern communication infrastructure. As the demand for mobility and seamless data transmission continues to grow, so too does the complexity and vulnerability of wireless systems. Cybersecurity threats, including unauthorized access, rogue access points, and man-in-the-middle attacks, increasingly target wireless environments. Training Course on Wireless Network Forensics and Security Incident Investigation is designed to equip cybersecurity professionals, IT administrators, and digital forensic investigators with the technical and analytical skills necessary to uncover, analyze, and respond to wireless threats effectively.

Through a hands-on, in-depth curriculum, participants will learn to apply cutting-edge wireless forensics tools, interpret wireless packet captures, identify intrusions, and respond to incidents using industry best practices. The course integrates real-world case studies, interactive labs, and practical scenarios to ensure participants can perform comprehensive investigations into security breaches involving Wi-Fi, Bluetooth, and emerging wireless protocols. Stay ahead in the cybersecurity race with this powerful course focused on wireless defense, threat detection, and incident response.

Programme Curriculum

Training Course on Wireless Network Forensics and Security Incident Investigation

Introduction

In today's hyper-connected digital world, wireless networks serve as the foundation of modern communication infrastructure. As the demand for mobility and seamless data transmission continues to grow, so too does the complexity and vulnerability of wireless systems. Cybersecurity threats, including unauthorized access, rogue access points, and man-in-the-middle attacks, increasingly target wireless environments. Training Course on Wireless Network Forensics and Security Incident Investigation is designed to equip cybersecurity professionals, IT administrators, and digital forensic investigators with the technical and analytical skills necessary to uncover, analyze, and respond to wireless threats

effectively.

Through a hands-on, in-depth curriculum, participants will learn to apply cutting-edge wireless forensics tools, interpret wireless packet captures, identify intrusions, and respond to incidents using industry best practices. The course integrates real-world case studies, interactive labs, and practical scenarios to ensure participants can perform comprehensive investigations into security breaches involving Wi-Fi, Bluetooth, and emerging wireless protocols. Stay ahead in the cybersecurity race with this powerful course focused on wireless defense, threat detection, and incident response.

Course Objectives

1. Understand wireless network architecture and 802.11 standards.
2. Identify and mitigate wireless-specific vulnerabilities.
3. Analyze wireless traffic using Wireshark and Aircrack-ng.
4. Implement wireless security protocols including WPA3 and EAP.
5. Detect rogue access points and spoofed MAC addresses.
6. Apply wireless packet sniffing and decryption techniques.
7. Perform full-scale wireless penetration testing.
8. Conduct thorough post-incident forensics investigations.
9. Understand Bluetooth, Zigbee, and IoT wireless threats.
10. Investigate Wi-Fi phishing attacks and Evil Twin APs.
11. Develop and document wireless incident response playbooks.
12. Integrate wireless forensics with SIEM and SOC environments.
13. Prepare forensic reports that are legally admissible in court.

Target Audience

1. Cybersecurity Analysts
2. Network Engineers
3. Incident Response Teams
4. IT Security Consultants
5. Forensic Investigators
6. Wireless Network Administrators
7. SOC & NOC Professionals
8. Penetration Testers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Wireless Network Forensics

- Overview of wireless technologies and topologies
- Understanding RF spectrum and frequencies
- Evolution of 802.11 standards
- Wireless network components and communication flow
- Key terminologies in wireless forensics
- **Case Study:** Investigating a campus-wide rogue AP incident

Module 2: Wireless Security Protocols & Encryption

- WEP, WPA, WPA2, WPA3 overview
- Encryption methods and key exchange mechanisms
- Wireless authentication types
- Protocol vulnerabilities and exploits
- Understanding EAP, PSK, and RADIUS

- **Case Study:** Breaking weak encryption in an enterprise setting

Module 3: Wireless Threat Landscape

- Common wireless attacks (DoS, MITM, Evil Twin)
- Role of wireless in APTs and malware delivery
- Threat modeling for wireless networks
- Bluetooth, Zigbee, and IoT attack surfaces
- Physical layer and RF jamming threats
- **Case Study:** Bluetooth skimming at a retail store

Module 4: Tools for Wireless Forensics

- Overview of Wireshark, Kismet, Aircrack-ng
- Wireless sniffers and adapters
- Open-source wireless security tools
- Packet capture and analysis basics
- Real-time monitoring and alerting tools
- **Case Study:** Using Aircrack-ng to detect WPA2 handshake leaks

Module 5: Wireless Traffic Analysis

- Understanding wireless packet structure
- Identifying normal vs. malicious patterns
- Filtering and tagging suspicious frames
- MAC address spoofing detection
- Radiotap headers and meta-information
- **Case Study:** Analyzing de-authentication attacks in a hotel

Module 6: Rogue Device Detection

- Types of rogue devices (routers, sniffers, repeaters)
- Behavioral profiling for device detection
- Signal strength triangulation
- Vendor and MAC OUI lookup
- Automated rogue AP alerts
- **Case Study:** Locating a rogue AP in a government office

Module 7: Bluetooth & IoT Forensics

- Bluetooth protocol layers and vulnerabilities
- Sniffing and capturing Bluetooth traffic
- Zigbee forensic analysis overview
- IoT device fingerprinting
- Bluetooth Low Energy (BLE) forensic tools
- **Case Study:** Investigating compromised smart locks via BLE

Module 8: Incident Response for Wireless Breaches

- Wireless incident detection techniques
- Containment and eradication protocols
- Log analysis and correlation
- Preservation of wireless evidence
- Legal and organizational escalation procedures
- **Case Study:** Coordinated response to university-wide network breach

Module 9: Wireless Penetration Testing

- Penetration testing frameworks (PTES, OWASP)
- Conducting wireless vulnerability scans
- Performing handshake captures and cracking
- Testing for Evil Twin and MITM attacks
- Documenting test results for stakeholders
- **Case Study:** Ethical hacking of public café Wi-Fi

Module 10: Post-Breach Forensics

- Steps for comprehensive forensic investigation
- Timeline reconstruction and event correlation
- Deep packet inspection (DPI) techniques
- Evidence preservation and chain of custody
- Recovery and reporting
- **Case Study:** Legal defense using forensic Wi-Fi evidence

Module 11: Legal Considerations in Wireless Forensics

- Jurisdictional laws and compliance (GDPR, HIPAA)
- Admissibility of wireless evidence
- Chain of custody and legal documentation
- Ethical hacking and consent boundaries
- Data protection and privacy obligations
- **Case Study:** Courtroom analysis of Wi-Fi intrusion evidence

Module 12: Wireless Network Hardening

- Security configuration best practices
- Device-level hardening and updates
- Intrusion prevention systems (IPS) for wireless
- Segmenting guest and internal networks
- Using VLANs and ACLs in Wi-Fi environments
- **Case Study:** Securing hospital wireless infrastructure

Module 13: Threat Hunting in Wireless Environments

- Proactive monitoring strategies
- Integrating wireless data with SIEM
- Building wireless attack detection rules
- Behavioral analytics and anomaly detection
- Creating threat hunting playbooks
- **Case Study:** Threat hunt reveals insider misuse of corporate Wi-Fi

Module 14: Advanced Wireless Attack Techniques

- Advanced spoofing and sniffing tools
- Side-channel attacks and RF hacking
- Using drones for wireless attacks
- Multi-vector attack chaining (e.g., BLE + Wi-Fi)
- Payload delivery through wireless beacons
- **Case Study:** Attack simulation on smart city infrastructure

Module 15: Capstone Project & Simulation

- Group simulation of wireless breach investigation
- Realistic scenario with live attack traces

- Forensic analysis, threat identification, and reporting
- Team presentations of findings
- Peer and instructor feedback
- **Case Study:** Full incident lifecycle for a simulated enterprise breach

Training Methodology

- Interactive instructor-led sessions
- Real-world case studies and simulations
- Hands-on labs with forensic tools
- Group-based penetration testing exercises
- Guided report writing and peer review activities

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