Training Course on Advanced Wireless Attack Forensics

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 landscape, wireless networks are increasingly targeted by cybercriminals exploiting vulnerabilities in Wi-Fi, Bluetooth, ZigBee, and other wireless communication protocols. Training Course on Advanced Wireless Attack Forensics is specifically designed to equip cybersecurity professionals, digital forensic analysts, and network investigators with the latest tools, skills, and methodologies required to detect, analyze, and respond to sophisticated wireless-based cyberattacks. This course emphasizes hands-on investigations, RF spectrum analysis, and post-incident data recovery techniques, offering learners real-world scenarios and AI-enhanced forensic analysis.

As IoT and mobile-first infrastructures expand, so do the vectors of exploitation. This course bridges the knowledge gap by exploring emerging wireless attack surfaces, such as rogue access points, Evil Twin attacks, and signal spoofing, and combining them with advanced forensic frameworks to reconstruct intrusions, assess damage, and produce court-admissible evidence. By the end of the course, learners will be well-equipped to navigate complex attack environments and respond proactively with cutting-edge forensic methods.

Programme Curriculum

Training Course on Advanced Wireless Attack Forensics

Introduction

In today’s hyper-connected digital landscape, wireless networks are increasingly targeted by cybercriminals exploiting vulnerabilities in Wi-Fi, Bluetooth, ZigBee, and other wireless communication protocols. Training Course on Advanced Wireless Attack Forensics is specifically designed to equip cybersecurity professionals, digital forensic analysts, and network investigators with the latest tools, skills, and methodologies required to detect, analyze, and respond to sophisticated wireless-based cyberattacks. This course emphasizes hands-on investigations, RF spectrum analysis, and post-incident data recovery techniques, offering learners real-world scenarios and AI-enhanced forensic analysis.

As IoT and mobile-first infrastructures expand, so do the vectors of exploitation. This course bridges the knowledge gap by exploring emerging wireless attack surfaces, such as rogue access points, Evil Twin attacks, and signal spoofing, and combining them with advanced forensic frameworks to reconstruct intrusions, assess damage, and produce court-admissible evidence. By the end of the course, learners will be well-equipped to navigate complex attack environments and respond proactively with cutting-edge forensic methods.

Course Objectives

1. Understand the forensic principles behind wireless attack vectors.
2. Analyze RF spectrum data for wireless intrusion detection.
3. Detect and respond to Evil Twin and rogue AP threats.
4. Utilize open-source and commercial wireless forensics tools.
5. Apply AI-assisted anomaly detection in wireless traffic.
6. Execute ZigBee, Bluetooth, and Wi-Fi attack reconstructions.
7. Investigate MAC spoofing and address obfuscation techniques.
8. Recover digital evidence from compromised wireless devices.
9. Interpret logs from wireless intrusion detection systems (WIDS).
10. Use Geolocation and triangulation to trace attackers.
11. Conduct legal and policy-compliant wireless forensics.
12. Prepare forensic reports for litigation and internal reviews.
13. Simulate real-world wireless breach scenarios for team readiness.

Target Audience

1. Digital Forensics Investigators
2. Cybersecurity Analysts
3. Network Security Engineers
4. Incident Response Teams
5. Wireless Security Researchers
6. Law Enforcement Cyber Units
7. Penetration Testers & Ethical Hackers
8. IoT Security Consultants

Course Duration: 10 days

Course Modules

Module 1: Fundamentals of Wireless Forensics

- Wireless communication protocols overview
- Types of wireless attacks and vulnerabilities
- Forensic challenges in wireless environments
- Capturing volatile wireless evidence
- Chain-of-custody best practices
- **Case Study**: Tracing a rogue Wi-Fi hotspot in a hospital network

Module 2: Wi-Fi Attack Lifecycle and Forensics

- Packet sniffing and analysis with Wireshark & Kismet
- Deauthentication attacks and data capturing
- Identifying and isolating Evil Twin networks
- WPA/WPA2/WPA3 cracking overview
- Wireless artifact analysis techniques
- **Case Study**: Forensic breakdown of a university dorm Evil Twin attack

Module 3: Bluetooth Attack Forensics

- Overview of Bluetooth vulnerabilities
- Tools for Bluetooth scanning and sniffing (e.g., Ubertooth)
- Detection of Bluejacking and Bluesnarfing
- Device pairing analysis
- Log correlation from mobile forensics
- **Case Study**: Theft of corporate data via Bluetooth headset hijack

Module 4: ZigBee and IoT Wireless Forensics

- ZigBee architecture and attack surfaces
- IoT forensic acquisition strategies
- Firmware extraction and analysis
- ZigBee sniffing with KillerBee
- Investigating sensor spoofing
- **Case Study**: Compromise of smart lighting in a smart office setup

Module 5: Rogue Access Points & MAC Spoofing

- Identification of rogue APs
- MAC address spoofing techniques
- Tools: Aircrack-ng suite and Fluxion
- Correlating logs to pinpoint device origin
- Evidence preservation for MAC-hopping attackers
- **Case Study**: Financial fraud enabled by MAC spoofing at a public café

Module 6: RF Spectrum Analysis

- Using Software-Defined Radio (SDR)
- Signal strength triangulation
- Detecting unusual RF signals
- Interference and jamming analysis
- Legal considerations for RF capture
- **Case Study**: Detection of hidden surveillance RF devices in a boardroom

Module 7: Wireless Intrusion Detection Systems (WIDS)

- Deploying and configuring WIDS
- Interpreting detection logs and alerts
- Behavioral anomaly analysis
- Custom WIDS rule configuration
- Integration with SIEM systems
- **Case Study**: Real-time detection of ARP spoofing on a public Wi-Fi network

Module 8: Post-Incident Forensic Analysis

- Triage methods for wireless breaches
- Artifact carving from mobile and IoT devices
- Correlation of wireless and endpoint data
- Using timeline analysis tools
- Reporting for law enforcement
- **Case Study**: Forensic reconstruction of a 24-hour Wi-Fi attack timeline

Module 9: Legal and Ethical Considerations

- Jurisdictional limitations in RF forensics

- Admissibility of wireless digital evidence
- Privacy law implications in wireless investigations
- Documentation for legal scrutiny
- Working with law enforcement and legal teams
- **Case Study**: Courtroom analysis of evidence in a Wi-Fi intrusion case

Module 10: Advanced Wireless Sniffing Tools

- Airgeddon, Wifite, and other advanced tools
- Combining hardware and software tools
- Channel hopping and focused scans
- Hidden SSID detection
- Metadata capture and use in investigations
- **Case Study**: Covert surveillance using Airgeddon in a corporate espionage scenario

Module 11: AI in Wireless Forensics

- Introduction to ML models for anomaly detection
- Training AI to identify signal irregularities
- Real-time AI-based WIDS
- Behavioral profiling of wireless devices
- AI-assisted pattern recognition in wireless attacks
- **Case Study**: Detection of multi-stage Wi-Fi breach using anomaly-based AI model

Module 12: Wireless Forensics for IoT Devices

- Common forensic challenges with smart devices
- Device identification and network mapping
- Extracting logs from IoT platforms
- Correlating sensor data with intrusion timestamps
- Reverse engineering custom firmware
- **Case Study**: Smart thermostat breach investigation in a smart home

Module 13: Cloud & Remote Wireless Device Investigations

- Investigating cloud-managed wireless systems
- Correlation of cloud logs with local wireless evidence
- VPN obfuscation techniques and detection
- Forensics on remote Wi-Fi extenders
- Tracking wireless activity via cloud dashboards
- **Case Study**: Multi-location wireless intrusion traced through cloud dashboard logs

Module 14: Wireless Forensics Reporting

- Structure and components of forensic reports
- Visualizations for wireless evidence
- Data presentation best practices
- Report generation automation tools
- Stakeholder-based reporting
- **Case Study**: Presenting wireless forensic findings to a non-technical executive team

Module 15: Capstone Project and Simulation

- End-to-end wireless breach simulation
- Incident response and evidence collection
- Team-based forensic report creation

- Real-time triage under pressure
- Peer review and feedback sessions
- **Case Study**: Simulated airport Wi-Fi attack with forensic investigation presentation

Training Methodology

- **Hands-on Labs**: Practical exposure using industry-grade tools and real scenarios
- **Case-Based Learning**: Each module concludes with real-world forensic case analysis
- **Group Discussions & Simulations**: Enhancing peer learning and situational handling
- **Instructor-led Demos**: Live sessions for advanced tools and wireless setups
- **Assessment & Capstone**: Interactive assessments and final simulation-based evaluation
- **Comprehensive Resource Kit**: Access to scripts, software, datasets, and checklists

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