# Training Course on Advanced IoT Security and Forensic Challenges

Professional Development Training Course Outline

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

## Course Introduction

The rapid proliferation of Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity, transforming industries from healthcare to manufacturing and smart cities. However, this expansive **IoT ecosystem** simultaneously introduces a complex **cybersecurity threat landscape**, demanding advanced expertise in **IoT security**, **data privacy**, and **digital forensics**. As **Industrial IoT (IIoT)** and consumer devices become increasingly integrated into critical infrastructure and daily life, understanding and mitigating **vulnerabilities** and responding effectively to **cyber incidents** are paramount to safeguarding sensitive data, ensuring operational continuity, and maintaining public trust.

Training Course on Advanced IoT Security and Forensic Challenges provides a comprehensive deep dive into the **cutting-edge challenges** and **next-generation solutions** in securing IoT environments and conducting thorough **IoT forensic investigations**. Participants will gain **hands-on experience** with **industry-leading tools** and methodologies, learning to identify, analyze, and remediate diverse **IoT attacks**. From **firmware analysis** and **network traffic inspection** to **cloud security** and **legal compliance**, this program equips professionals with the **practical skills** and **strategic insights** necessary to defend against evolving threats and become **sought-after experts** in the critical domain of **advanced IoT security and forensics**.

## Programme Curriculum

**Training Course on Advanced IoT Security and Forensic Challenges**

**Introduction**

The rapid proliferation of Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity, transforming industries from healthcare to manufacturing and smart cities. However, this expansive **IoT ecosystem** simultaneously introduces a complex **cybersecurity threat landscape**, demanding advanced expertise in **IoT security**, **data privacy**, and **digital forensics**. As

**Industrial IoT (IIoT)** and consumer devices become increasingly integrated into critical infrastructure and daily life, understanding and mitigating **vulnerabilities** and responding effectively to **cyber incidents** are paramount to safeguarding sensitive data, ensuring operational continuity, and maintaining public trust.

Training Course on Advanced IoT Security and Forensic Challenges provides a comprehensive deep dive into the **cutting-edge challenges** and **next-generation solutions** in securing IoT environments and conducting thorough **IoT forensic investigations**. Participants will gain **hands-on experience** with **industry-leading tools** and methodologies, learning to identify, analyze, and remediate diverse **IoT attacks**. From **firmware analysis** and **network traffic inspection** to **cloud security** and **legal compliance**, this program equips professionals with the **practical skills** and **strategic insights** necessary to defend against evolving threats and become **sought-after experts** in the critical domain of **advanced IoT security and forensics**.

**Course Duration**

10 days

**Course Objectives**

1. Understand the evolving **IoT threat landscape**, including **zero-day exploits**, **botnets**, and **ransomware attacks** targeting connected devices.
2. Implement robust **device authentication**, **firmware hardening**, and **secure boot** mechanisms for embedded systems.
3. Analyze and secure prevalent **IoT protocols** like MQTT, CoAP, Zigbee, and LoRaWAN against **eavesdropping** and **tampering**.
4. Design and deploy **micro-segmentation**, **Zero Trust architectures**, and **network intrusion detection systems (NIDS)** for IoT networks.
5. Secure **IoT cloud platforms**, **data storage**, and API integrations against **data breaches** and unauthorized access.
6. Enforce **GDPR**, **HIPAA**, and other regulatory compliance frameworks for **sensitive IoT data** .
7. Develop and execute comprehensive **IoT incident response plans**, from **detection** to **recovery** and **post-mortem analysis**.
8. Acquire, preserve, and analyze **forensic artifacts** from diverse IoT devices, including **wearables**, **smart home devices**, and **industrial sensors**.
9. Conduct in-depth **malware analysis** specific to IoT platforms, identifying **attack vectors** and **payloads**.
10. Utilize **specialized IoT forensic tools** and techniques for **memory forensics**, **file system analysis**, and **network forensics** in IoT contexts.
11. Navigate the legal complexities, **chain of custody**, and **expert witness testimony** related to IoT cybercrime.
12. Address unique **IIoT security challenges**, including **OT/IT convergence**, **critical infrastructure protection**, and **SCADA security**.
13. Integrate **security-by-design** principles throughout the **IoT software development lifecycle (SDLC)**.

**Organizational Benefits**

- Proactive defense against sophisticated **IoT cyber threats**, reducing the risk of **breaches**, **data loss**, and **operational disruption**.
- Adherence to evolving **data privacy regulations** (e.g., GDPR, CCPA) and industry standards, minimizing legal and financial penalties.

- Rapid and effective **cyber incident management**, minimizing downtime and reputational damage.
- Safeguarding **industrial control systems (ICS)**, **smart city infrastructure**, and sensitive consumer data.
- Demonstrating a commitment to **IoT security excellence**, fostering trust with customers and partners.
- Preventing costly **cyberattacks** and reducing the financial impact of successful breaches.
- Cultivating an in-house team of highly skilled **IoT security specialists** and **digital forensic investigators**.

**Target Audience**

1. Cybersecurity Professionals
2. Digital Forensics Investigators and Law Enforcement
3. IoT Developers and Solution Architects
4. OT/ICS Security Engineers
5. Penetration Testers and Ethical Hackers
6. IT/OT Managers and Risk Officers
7. Compliance and Legal Professionals dealing with IoT data
8. Cloud Security Specialists

**Course Outline**

**Module 1: Introduction to Advanced IoT Security & Forensics**

- Deep Dive into the IoT Ecosystem: Devices, Protocols, Platforms, and Applications.
- Understanding the Unique IoT Attack Surface and Threat Landscape (2025 Trends).
- Fundamentals of IoT Security Principles: Confidentiality, Integrity, Availability, Privacy.
- Introduction to Digital Forensics Methodologies in IoT Contexts.
- **Case Study:** The Mirai Botnet and its impact on IoT device security.

**Module 2: IoT Device Security: Hardware & Firmware Analysis**

- IoT Device Architecture, Components, and Attack Vectors at the Hardware Level.
- Firmware Extraction Techniques (JTAG, UART, SPI, NAND) and Analysis.
- Reverse Engineering IoT Device Firmware for Vulnerability Identification.
- Secure Boot, Trusted Platform Modules (TPM), and Hardware Security Modules (HSM) in IoT.
- **Case Study:** Analyzing a compromised smart camera firmware for backdoor discovery.

**Module 3: IoT Communication Protocol Security**

- In-depth analysis of common IoT protocols: MQTT, CoAP, Zigbee, Z-Wave, Bluetooth, LoRaWAN.
- Vulnerabilities and Attack Scenarios specific to each protocol.
- Implementing Secure Communication: TLS/DTLS, End-to-End Encryption, Message Integrity.
- Network Traffic Analysis for IoT (Packet Capture, Protocol Decryption).
- **Case Study:** Exploiting a vulnerable MQTT broker to manipulate smart home devices.

**Module 4: IoT Network Security & Segmentation**

- Designing Secure IoT Network Architectures: Segmentation, VLANs, Firewalls.
- Implementing Zero Trust Principles in IoT Environments.

- Intrusion Detection/Prevention Systems (IDS/IPS) for IoT Networks.
- Securing IoT Gateways and Edge Devices.
- **Case Study:** Segmenting an IIoT network to prevent lateral movement after an initial compromise.

**Module 5: IoT Cloud & Platform Security**

- Understanding Cloud Architectures for IoT (PaaS, IaaS, SaaS) and associated risks.
- Securely Integrating IoT Devices with Cloud Platforms (AWS IoT, Azure IoT Hub, Google Cloud IoT Core).
- API Security for IoT Applications and Cloud Services.
- Data Storage Security in the Cloud: Encryption at Rest and In Transit.
- **Case Study:** Investigating a data breach originating from a misconfigured IoT cloud platform.

**Module 6: IoT Data Privacy, Governance & Compliance**

- Regulatory Landscape: GDPR, CCPA, HIPAA, NIS Directive, and IoT.
- Data Minimization, Pseudonymization, and Anonymization Techniques for IoT Data.
- Privacy-by-Design Principles in IoT Development.
- Consent Management and User Rights in IoT Data Collection.
- **Case Study:** Ensuring GDPR compliance for a smart healthcare monitoring system.

**Module 7: Advanced IoT Malware Analysis & Reverse Engineering**

- Types of IoT Malware (Botnets, Ransomware, Worms) and their characteristics.
- Static and Dynamic Malware Analysis Techniques for ARM/MIPS architectures.
- Disassembly and Debugging of IoT Malware Binaries.
- Indicators of Compromise (IOCs) and Threat Intelligence Sharing.
- **Case Study:** Deconstructing a new variant of IoT botnet malware and identifying its C2 infrastructure.

**Module 8: IoT Incident Response & Forensics Readiness**

- The IoT Incident Response Lifecycle: Preparation, Detection, Containment, Eradication, Recovery, Post-Incident Activity.
- Building an IoT Forensics Toolkit and Lab Environment.
- Forensics Readiness Planning for IoT Deployments.
- Establishing a Secure Chain of Custody for IoT Evidence.
- **Case Study:** Developing an incident response plan for a smart factory suffering a ransomware attack.

**Module 9: IoT Device Forensics: Acquisition & Preservation**

- Challenges of IoT Data Acquisition: Limited Storage, Volatile Memory, Non-Standard Filesystems.
- Physical Acquisition Techniques: Chip-off, JTAG, Memory Dumping.
- Logical Acquisition Methods: API Calls, Cloud Data Extraction, Network Traffic Capture.
- Handling Encrypted IoT Devices and Data.
- **Case Study:** Extracting evidence from a smart speaker involved in a criminal investigation.

**Module 10: IoT Data Forensics: Analysis & Reconstruction**

- Analyzing File Systems of Embedded Devices (SquashFS, YAFFS2, JFFS2).
- Memory Forensics for IoT Devices (Volatility Framework for ARM/MIPS).

- Log Analysis and Event Correlation across diverse IoT devices and platforms.
- Reconstructing Timelines and User Activity from IoT Data.
- **Case Study:** Reconstructing events from a smart home hub after a suspected intrusion.

**Module 11: IoT Network Forensics**

- Advanced Network Traffic Analysis for IoT Protocols (Wireshark, Tshark).
- Identifying Anomalous Traffic Patterns and Malicious Communications.
- Deep Packet Inspection for IoT-Specific Payloads.
- Attribution Techniques for IoT Cyberattacks.
- **Case Study:** Tracing the source of a DDoS attack launched from a compromised IoT fleet.

**Module 12: Industrial IoT (IIoT) Security & Forensics**

- Specific Security Challenges in OT/ICS Environments and IIoT.
- SCADA System Vulnerabilities and Attack Methodologies.
- Securing PLC, RTU, and HMI Devices.
- Forensic Investigation in Industrial Control Systems.
- **Case Study:** Analyzing a cyberattack on a critical infrastructure (e.g., power grid) involving IIoT devices.

**Module 13: Legal & Ethical Aspects of IoT Forensics**

- Legal Frameworks for Digital Evidence in IoT.
- Rules of Evidence and Admissibility in Court.
- Expert Witness Testimony and Report Writing for IoT Forensics.
- Ethical Considerations in IoT Investigations (Privacy, Data Handling).
- **Case Study:** Presenting forensic findings from a drone-related incident in a legal setting.

**Module 14: Emerging Threats & Advanced Defenses in IoT**

- AI/ML in IoT Security: Anomaly Detection, Predictive Analytics.
- Blockchain for Secure IoT Transactions and Data Integrity.
- Quantum-Resistant Cryptography for Future IoT Security.
- Supply Chain Security for IoT Devices.
- **Case Study:** Exploring the use of blockchain for secure firmware updates in a large IoT deployment.

**Module 15: Building a Secure IoT Ecosystem & Future Trends**

- Implementing Security-by-Design and Privacy-by-Design throughout the IoT Lifecycle.
- Threat Modeling for IoT Systems.
- Continuous Monitoring and Vulnerability Management for IoT.
- Future of IoT Security: Edge Computing, 5G, and Digital Twins.
- **Case Study:** Developing a comprehensive security roadmap for a smart city initiative.

**Training Methodology**

This training course employs a highly interactive and practical methodology designed for maximum knowledge retention and skill development. It combines:

- **Instructor-Led Presentations:** Clear and concise explanations of complex concepts.
- **Hands-on Labs:** Practical exercises using industry-standard tools and simulated IoT environments. Participants will work with real or emulated IoT devices (e.g., Raspberry Pi, ESP32) for practical scenarios.

- **Real-world Case Studies:** In-depth analysis of past IoT security incidents and forensic investigations to illustrate concepts.
- **Live Demos:** Demonstrations of attack techniques and defense mechanisms.
- **Group Discussions & Collaborative Activities:** Fostering peer learning and problem-solving.
- **Q&A Sessions:** Addressing participant queries and clarifying doubts.
- **Capture The Flag (CTF) Challenges:** Optional competitive exercises to reinforce skills.
- **Capstone Project:** A comprehensive project to apply learned skills to a realistic IoT security or forensics scenario.

**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.** 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 |
| **28 Sep 2026** | 09 Oct 2026 | Physical | $3,000 |

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **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