Training Course on IoT Device Forensics, Data Acquisition from Edge Devices

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$2,200 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This specialized training course delves into the complex and rapidly evolving field of IoT device forensics, focusing specifically on data acquisition from edge devices. Participants will gain critical expertise in navigating the diverse architectures, proprietary operating systems, and often unconventional data storage methods of Internet of Things (IoT) devices. Training Course on IoT Device Forensics, Data Acquisition from Edge Devices provides hands-on experience with advanced techniques for forensically sound data extraction from a wide array of IoT categories, including smart home devices, industrial IoT (IIoT) sensors, wearables, and connected vehicles, empowering digital forensic professionals to uncover crucial evidence in cybercrime investigations, incident response, and product liability cases.

The program emphasizes low-level data recovery methods, including firmware extraction, chip-off techniques, JTAG/UART interfacing, and memory forensics, alongside analysis of cloud-connected IoT data and associated mobile applications. With the explosive growth of IoT deployments and the increasing threat surface they present, this course is essential for anyone seeking to master the challenges of digital evidence collection from these ubiquitous devices. Graduates will be proficient in identifying critical IoT artifacts, understanding communication protocols, and generating robust forensic reports that stand up to legal scrutiny in the dynamic landscape of IoT security and investigations.

Programme Curriculum

Training Course on IoT Device Forensics, Data Acquisition from Edge Devices

Introduction

This specialized training course delves into the complex and rapidly evolving field of IoT device forensics, focusing specifically on data acquisition from edge devices. Participants will gain critical expertise in navigating the diverse architectures, proprietary operating systems, and often unconventional data storage methods of Internet of Things (IoT) devices. Training Course on IoT Device Forensics, Data Acquisition from Edge Devices provides hands-on experience with advanced techniques for forensically sound data extraction from a wide array of IoT categories, including smart home devices, industrial IoT (IIoT) sensors, wearables, and connected vehicles, empowering digital forensic professionals to uncover crucial evidence in cybercrime investigations, incident response, and product liability cases.

The program emphasizes low-level data recovery methods, including firmware extraction, chip-off techniques, JTAG/UART interfacing, and memory forensics, alongside analysis of cloud-connected IoT data and associated mobile applications. With the explosive growth of IoT deployments and the increasing threat surface they present, this course is essential for anyone seeking to master the challenges of digital evidence collection from these ubiquitous devices. Graduates will be proficient in identifying critical IoT artifacts, understanding communication protocols, and generating robust forensic reports that stand up to legal scrutiny in the dynamic landscape of IoT security and investigations.

Course Duration

10 Days

Course Objectives

1. Identify and classify diverse IoT device architectures and their impact on forensic acquisition strategies.
2. Perform forensically sound data acquisition from various IoT edge devices, including both volatile and non-volatile memory.
3. Execute firmware extraction techniques from IoT devices for static analysis and artifact identification.
4. Utilize JTAG, UART, and SPI protocols for direct memory access and data extraction from IoT embedded systems.
5. Conduct chip-off forensics on non-standard IoT memory components where traditional methods fail.
6. Analyze IoT communication protocols (e.g., MQTT, CoAP, Zigbee, Bluetooth Low Energy) for forensic insights.

7. Investigate cloud-connected IoT data and associated mobile/web applications for comprehensive evidence collection.
8. Recover and interpret critical forensic artifacts from IoT device storage, including logs, configuration files, and user data.
9. Identify vulnerabilities and attack vectors specific to IoT devices through forensic analysis.
10. Develop custom scripts (Python) for parsing proprietary IoT data formats and automating artifact extraction.
11. Reconstruct user activities and device timelines based on evidence extracted from IoT devices.
12. Generate comprehensive forensic reports detailing findings from IoT device investigations for legal proceedings.
13. Apply chain of custody principles and best practices for preserving the integrity of IoT digital evidence.

Organizational Benefits

1. Expanded Investigative Scope: Equip teams to investigate incidents involving the rapidly expanding universe of IoT devices.
2. Enhanced Data Recovery: Improve the ability to extract crucial evidence from specialized and often custom IoT hardware.
3. Proactive Risk Mitigation: Identify security vulnerabilities in deployed IoT devices before they are exploited.
4. Improved Incident Response: Accelerate the response to security breaches originating from or involving IoT devices.
5. Compliance & Regulatory Adherence: Ensure forensic capabilities meet evolving data privacy and security regulations for IoT.
6. Protection of Critical Infrastructure: Safeguard operational technology (OT) and industrial control systems (ICS) from IoT-related threats.
7. Reduced Litigation Risk: Provide robust, admissible evidence for product liability cases or disputes involving IoT devices.
8. Cost Savings: Build in-house expertise, reducing reliance on expensive external specialists for IoT forensics.
9. Competitive Advantage: Stay ahead in the digital forensics field by mastering emerging technologies.
10. Actionable Threat Intelligence: Extract valuable intelligence on IoT malware and attack methodologies.

Target Participants

- Digital Forensic Examiners
- Cybersecurity Incident Responders
- Hardware Reverse Engineers

- Embedded Systems Developers (with security focus)
- Industrial Control Systems (ICS) Security Professionals
- Law Enforcement Cybercrime Units
- Product Security Teams
- Security Researchers
- Red Team / Penetration Testers
- E-Discovery Specialists

Course Outline

Module 1: Introduction to IoT Ecosystems & Forensics (IoT Forensics Fundamentals)

- Overview of IoT Device Categories and Architectures (Edge, Fog, Cloud)
- Unique Challenges of IoT Forensics vs. Traditional Digital Forensics
- IoT Communication Protocols: MQTT, CoAP, Zigbee, Z-Wave, BLE, Wi-Fi, Cellular
- Legal, Ethical, and Privacy Considerations in IoT Investigations
- **Case Study**: Identifying the forensic scope of a smart home intrusion.

Module 2: IoT Device Identification & Triage (IoT Device Triage)

- Methods for Identifying IoT Device Components and Chipsets
- Initial Triage of IoT Devices: Volatile Data & Live Acquisition
- Safe Power-Down Procedures and Evidence Preservation for IoT
- Understanding Device States (Active, Standby, Off) and Their Impact
- **Case Study**: Triaging a suspected compromised IP camera.

Module 3: Firmware Extraction & Analysis (IoT Firmware Forensics)

- Techniques for Extracting Firmware from IoT Devices (OTA, Hardware Exploits)
- Analyzing Firmware Structures and File Systems (SquashFS, JFFS2, UbiFS)
- Identifying Configuration Files, Credentials, and Embedded Data
- Using Tools like Binwalk, Firmware Mod Kit (fmk) for Firmware Dissection
- **Case Study**: Extracting and analyzing firmware from a smart thermostat to find hardcoded credentials.

Module 4: JTAG/UART/SPI Forensics (IoT Embedded Forensics)

- Understanding JTAG, UART, and SPI Interfaces on IoT Devices
- Identifying Test Points and Pinouts for Debugging and Data Extraction
- Using Bus Pirates, Logic Analyzers, and JTAG Adapters for Access
- Extracting Data from Flash Memory via Embedded Debug Interfaces
- **Case Study**: Connecting via UART to a smart light bulb to extract command logs.

Module 5: Chip-Off Forensics for IoT Devices (IoT Chip-Off)

- Introduction to Chip-Off Techniques for Data Extraction from BGA/eMMC/NAND
- Considerations for De-Soldering and Handling Sensitive Components
- Using NAND/eMMC Readers and Adapters for Raw Data Access
- Reconstructing File Systems from Raw Chip Dumps
- **Case Study**: Performing a chip-off acquisition from a damaged drone's flight controller.

Module 6: IoT Memory Forensics (IoT Memory Analysis)

- Volatile Memory Acquisition from Running IoT Devices (if possible)
- Analyzing RAM Dumps for Running Processes, Network Connections, and Keys
- Identifying Firmware Running in Memory
- Challenges and Limitations of Memory Forensics on Resource-Constrained IoT
- **Case Study**: Extracting network connection details from a live IoT gateway's memory.

Module 7: IoT Communication Protocol Analysis (IoT Protocol Forensics)

- Deep Dive into MQTT, CoAP, and HTTP/HTTPS for IoT Communication
- Sniffing and Analyzing Zigbee and Z-Wave Traffic
- Bluetooth Low Energy (BLE) Packet Analysis for IoT Devices
- Identifying IoT-Specific Data Formats and Payloads
- **Case Study**: Analyzing MQTT traffic from a smart sensor to identify data transmission patterns.

Module 8: Cloud-Connected IoT Data Forensics (Cloud IoT Forensics)

- Investigating IoT Platform Cloud Services (AWS IoT, Azure IoT Hub, Google Cloud IoT Core)
- Acquiring Data from Cloud-Hosted IoT Databases and Logs
- Analyzing Mobile and Web Applications Connected to IoT Devices
- Legal and Jurisdictional Challenges in Cloud IoT Data Acquisition
- **Case Study**: Retrieving historical data and user commands from an Alexa account.

Module 9: IoT Data Artifact Analysis (IoT Artifact Analysis)

- Identifying and Interpreting Logs, Event Timestamps, and Configuration Files
- Analyzing SQLite Databases and Other Data Stores on IoT Devices
- Extracting User Activity, Sensor Readings, and Device State Information
- Recovering Deleted Data and Unallocated Space on IoT Storage
- **Case Study**: Reconstructing a timeline of door sensor events from a smart home hub's logs.

Module 10: IoT Vulnerabilities & Attack Vectors (IoT Security Forensics)

- Common IoT Vulnerabilities (Weak Credentials, Insecure Updates, Open Ports)
- Forensic Indicators of IoT Device Compromise
- Analyzing Exploited Vulnerabilities and Attack Traces
- Understanding IoT Botnets and DDoS Attacks
- **Case Study**: Investigating an IoT device compromised by the Mirai botnet.

Module 11: Industrial IoT (IIoT) & SCADA Forensics (IIoT Forensics)

- Specific Challenges of Forensics in Operational Technology (OT) Environments
- Data Acquisition from PLC, RTU, and SCADA Systems (where applicable to IoT)
- Analyzing Protocols like Modbus, DNP3, and OPC UA in an IoT Context
- Impact of Compromised IIoT Devices on Critical Infrastructure
- **Case Study**: Analyzing logs from an IIoT sensor connected to a manufacturing line.

Module 12: Vehicle IoT & Telematics Forensics (Connected Car Forensics)

- Data Sources in Connected Vehicles (Infotainment, ECU, Telematics Units)
- Methods for Acquiring Data from OBD-II Ports and Vehicle Buses (CAN bus)
- Analyzing GPS Data, Trip Logs, and User Profiles from Connected Cars
- Forensic Challenges of Modern Vehicle Architectures
- **Case Study**: Extracting trip history from a vehicle's infotainment system.

Module 13: Wearable & Health IoT Forensics (Wearable Forensics)

- Data Acquisition from Smartwatches, Fitness Trackers, and Health Monitors
- Analyzing Biometric Data, Activity Logs, and Location Information
- Understanding Synchronization with Mobile Apps and Cloud Services
- Privacy Considerations in Wearable Device Investigations
- **Case Study**: Analyzing fitness tracker data to corroborate a user's alibi.

Module 14: Custom Parsing & Scripting for IoT (IoT Forensic Scripting)

- Introduction to Python for IoT Forensic Automation
- Developing Scripts to Parse Proprietary IoT Data Formats
- Automating Firmware Analysis and Artifact Extraction
- Leveraging Open-Source Tools and Libraries for IoT Forensics
- **Case Study**: Writing a Python script to parse custom log files from a smart appliance.

Module 15: Reporting & Presenting IoT Forensic Findings (IoT Forensic Reporting)

- Best Practices for Documenting IoT Device Examinations
- Crafting Clear and Defensible Forensic Reports for IoT Investigations
- Admissibility of IoT-Generated Digital Evidence
- Preparing for and Delivering Expert Witness Testimony in IoT Cases
- **Case Study**: Drafting a comprehensive forensic report for an IoT-related privacy breach.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
10 Aug 2026	21 Aug 2026	Online	$2,200
17 Aug 2026	28 Aug 2026	Online	$2,200
24 Aug 2026	04 Sep 2026	Online	$2,200
31 Aug 2026	11 Sep 2026	Online	$2,200
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200
28 Sep 2026	09 Oct 2026	Online	$2,200

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskills.com | Website: www.fineskills.com