Training Course on Industrial IoT (IIoT) Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This highly specialized training course is meticulously designed for digital forensic investigators, cybersecurity professionals, operational technology (OT) security teams, and incident responders working within critical infrastructure, manufacturing, and other industrial sectors. As the Industrial Internet of Things (IIoT) rapidly integrates sensors, actuators, smart devices, and advanced analytics into SCADA (Supervisory Control and and Data Acquisition) and ICS (Industrial Control Systems) environments, the attack surface expands dramatically, exposing vital industrial processes to sophisticated cyber threats. Training Course on Industrial IoT (IIoT) Forensics provides the advanced knowledge and hands-on techniques required to acquire, preserve, analyze, and interpret digital evidence from these complex, often proprietary, and safety-critical IIoT ecosystems, which are paramount for uncovering the root cause of cyber-physical incidents, production disruptions, intellectual property theft, and sabotage.

The curriculum delves into the unique architectural considerations of IIoT, focusing on the convergence of IT and OT networks, the diversity of IIoT edge devices, and the intricacies of industrial communication protocols (e.g., Modbus, OPC UA, DNP3). Through intensive practical labs, simulated industrial control environments, and real-world attack scenarios, participants will gain proficiency in identifying relevant data sources, extracting device logs, network traffic, firmware, controller logic, and historical sensor data, and correlating evidence across heterogeneous systems. The course emphasizes forensically sound methodologies and strict adherence to safety protocols, regulatory compliance (including Kenya's Data Protection Act 2019), and chain of custody for evidence collected from live industrial systems, empowering graduates to effectively investigate incidents, ensure operational continuity, and secure the backbone of modern industry.

Programme Curriculum

Training Course on Industrial IoT (IIoT) Forensics

Introduction

This highly specialized training course is meticulously designed for digital forensic investigators, cybersecurity professionals, operational technology (OT) security teams, and incident responders working within critical infrastructure, manufacturing, and other industrial sectors. As the Industrial Internet of Things (IIoT) rapidly integrates sensors, actuators, smart devices, and advanced analytics into SCADA (Supervisory Control and and Data Acquisition) and ICS (Industrial Control Systems) environments, the attack surface expands dramatically, exposing vital industrial processes to sophisticated cyber threats. Training Course on Industrial IoT (IIoT) Forensics provides the advanced knowledge and hands-on techniques required to acquire, preserve, analyze, and interpret digital evidence from these complex, often proprietary, and safety-critical IIoT ecosystems, which are paramount for uncovering the root cause of cyber-physical incidents, production disruptions, intellectual property theft, and sabotage.

The curriculum delves into the unique architectural considerations of IIoT, focusing on the convergence of IT and OT networks, the diversity of IIoT edge devices, and the intricacies of industrial communication protocols (e.g., Modbus, OPC UA, DNP3). Through intensive practical labs, simulated industrial control environments, and real-world attack scenarios, participants will gain proficiency in identifying relevant data sources, extracting device logs, network traffic, firmware, controller logic, and historical sensor data, and correlating evidence across heterogeneous systems. The course emphasizes forensically sound methodologies and strict adherence to safety protocols, regulatory compliance (including Kenya's Data Protection Act 2019), and chain of custody for evidence collected from live industrial systems, empowering graduates to effectively investigate incidents, ensure operational continuity, and secure the backbone of modern industry.

Course Duration

5 Days

Course Objectives

1. Understand the architecture and security models of Industrial IoT (IIoT) and Operational Technology (OT) environments.
2. Identify unique digital evidence sources within IIoT systems, including edge devices, controllers, historians, and gateways.
3. Perform forensically sound data acquisition from diverse IIoT devices and industrial control components (PLCs, RTUs, HMIs).

4. Analyze industrial communication protocols (e.g., Modbus TCP/IP, OPC UA, DNP3) for anomalies and malicious commands.
5. Investigate cyber-physical incidents and attacks impacting industrial processes (e.g., unauthorized control changes, physical damage).
6. Extract and interpret controller logic (ladder logic, function block diagrams) for evidence of tampering or malicious modification.
7. Analyze historian databases and time-series data for anomalies indicative of compromise or data manipulation.
8. Identify vulnerabilities and attack surfaces specific to IIoT devices and OT networks.
9. Reconstruct complex incident timelines by correlating evidence from IT, OT, and IIoT data sources.
10. Navigate safety-critical considerations and the potential impact of forensic actions on live industrial processes.
11. Comply with data privacy regulations (e.g., Kenya Data Protection Act 2019) and industry standards when handling IIoT data.
12. Utilize specialized forensic tools and platforms tailored for IIoT/OT environments.
13. Generate comprehensive forensic reports for IIoT investigations, suitable for legal, regulatory, and internal purposes.

Organizational Benefits

1. Enhanced Operational Resilience: Rapidly investigate and recover from cyber incidents impacting critical industrial processes.
2. Improved Cybersecurity Posture: Proactively identify and mitigate vulnerabilities in IIoT and OT systems.
3. Reduced Downtime & Production Loss: Minimize the impact of cyber-physical attacks on industrial operations.
4. Strengthened Incident Response: Develop specialized capabilities for complex IIoT/OT incident triage and analysis.
5. Protection of Intellectual Property: Safeguard proprietary industrial processes and manufacturing secrets from cyber theft.
6. Compliance with Industry Regulations: Ensure forensic practices align with sector-specific security standards and data protection laws (e.g., Kenya Data Protection Act).
7. Cost Savings: Reduce reliance on expensive external IIoT forensic specialists.
8. Actionable Threat Intelligence: Gain insights into unique attack vectors and threat actors targeting industrial environments.
9. Enhanced Safety: Investigate incidents that could lead to physical harm or environmental damage, improving overall safety protocols.
10. In-House Expertise: Cultivate a highly specialized team capable of defending and investigating the most advanced IIoT threats.

Target Participants

- Digital Forensic Investigators (with an interest in OT)
- Cybersecurity Analysts in Industrial Control Systems
- Operational Technology (OT) Security Engineers
- Industrial Incident Responders
- SCADA/ICS Engineers (with a security interest)
- Plant Security Managers
- Critical Infrastructure Protection Specialists
- Industrial Network Administrators
- Threat Intelligence Analysts (Industrial Sector)
- Compliance Officers in Manufacturing/Utilities

Course Outline

Module 1: Introduction to IIoT & OT Ecosystems (IIoT & OT Fundamentals)

- Defining IIoT: Convergence of IT and OT in Industrial Environments
- Architecture of Industrial Control Systems (ICS) and SCADA
- Key IIoT Components: Sensors, Actuators, PLCs, RTUs, HMIs, Gateways
- Unique Challenges of IIoT Forensics: Safety, Uptime, Proprietary Systems
- **Case Study**: Mapping the data flow in a smart factory production line.

Module 2: IIoT Device Data Acquisition & Preservation (IIoT Data Acquisition)

- Forensically Sound Acquisition from IIoT Edge Devices (Sensors, Controllers)
- Data Collection from PLCs and RTUs (online/offline methods)
- Extracting Data from HMI (Human-Machine Interface) Systems
- Challenges of Live vs. Dead Box Forensics in Operational Environments
- **Case Study**: Acquiring firmware and logs from a smart industrial sensor.

Module 3: Industrial Protocol & Network Forensics (Industrial Network Forensics)

- Analysis of Common Industrial Protocols: Modbus TCP/IP, OPC UA, DNP3, Ethernet/IP
- Intercepting and Analyzing Network Traffic within OT Networks
- Identifying Malicious Commands and Anomalous Traffic Patterns

- Segmentation and Network Architecture for Forensic Visibility
- **Case Study**: Detecting a Modbus TCP/IP packet injection attack on a motor control system.

Module 4: PLC & Controller Logic Forensics (PLC Logic Forensics)

- Understanding Programmable Logic Controllers (PLCs) and their Programming Languages (Ladder Logic, Structured Text)
- Extracting and Analyzing PLC Programs and Configuration Files
- Detecting Unauthorized Logic Modifications and Malware in Controllers
- Reconstructing Control Actions and Process Anomalies from PLC Logs
- **Case Study**: Investigating a PLC logic change that caused an unexpected system shutdown.

Module 5: Historian & Time-Series Data Forensics (Historian Data Analysis)

- Role of Historian Databases in IIoT/OT Environments
- Extracting and Analyzing Time-Series Data from Industrial Systems
- Identifying Data Manipulation, Gaps, or Anomalies in Historical Records
- Correlating Process Data with Security Events and User Actions
- **Case Study**: Analyzing historian data to pinpoint when a specific process parameter was altered outside normal operating ranges.

Module 6: Cyber-Physical Incident Investigations (Cyber-Physical Incident Response)

- Understanding Attack Vectors against IIoT/OT (e.g., Ransomware, Insider Threats, Remote Access Exploits)
- Investigating Incidents Leading to Physical Damage or Operational Disruptions
- Root Cause Analysis of Cyber-Physical Attacks
- Containment, Eradication, and Recovery Strategies for IIoT/OT Incidents
- **Case Study**: Forensic analysis of an incident where a cyberattack caused a physical overflow in a water treatment plant.

Module 7: IIoT/OT Forensic Readiness & Tools (IIoT Forensic Readiness)

- Developing Forensic Readiness Plans for Industrial Environments

- Implementing Logging and Monitoring for IIoT Devices and Control Systems
- Overview of Specialized IIoT/OT Forensic Tools and Platforms
- Building Secure Remote Access and Jump Box Environments for Forensics
- **Case Study**: Designing a logging strategy for a new IIoT deployment to enhance forensic visibility.

Module 8: Legal, Regulatory & Emerging Trends (IIoT Legal & Future)

- Legal Obligations and Regulatory Compliance in IIoT/OT Forensics (e.g., NIS 2, ISA/IEC 62443, local regulations like Kenya's Data Protection Act 2019)
- Privacy and Data Handling Considerations for IIoT Data
- Ethical Implications of Investigating Live Industrial Systems
- Future Trends: AI/ML in IIoT Security, Digital Twins, Quantum Computing's Impact on OT
- **Case Study**: Discussing the legal challenges of sharing sensitive IIoT forensic data with external parties under Kenyan law.

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.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now