Training Course on Advanced Embedded System 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

Introduction

This highly specialized training course is meticulously crafted for digital forensic investigators, cybersecurity researchers, reverse engineers, and incident response teams confronting the unique and intricate challenges of advanced embedded system forensics. From the ubiquitous IoT devices, smart appliances, and wearables to industrial control systems (ICS), automotive ECUs, and critical infrastructure components, embedded systems are at the core of modern technology, yet they present a distinct and often opaque landscape for forensic analysis. Training Course on Advanced Embedded System Forensics provides the cutting-edge knowledge and intensive hands-on skills required to acquire, preserve, and analyze digital evidence directly from the hardware and firmware of these specialized devices, crucial for uncovering firmware tampering, sophisticated malware, intellectual property theft, and cyber-physical attacks.

The curriculum delves deep into the low-level architectures of embedded systems, exploring microcontroller internals, various memory technologies (NAND, NOR, eMMC, SPI Flash), JTAG/SWD debugging interfaces, and custom communication protocols. Through extensive practical labs, firmware reverse engineering exercises, hardware analysis techniques (e.g., Chip-Off, ISP), and vulnerability exploitation for forensic access, participants will master methodologies to bypass security features, recover deleted data, and analyze proprietary file systems, even from physically damaged or non-responsive devices. The course also critically examines the ethical and legal complexities (including Kenya's Data Protection Act 2019) of performing invasive forensics on embedded systems, ensuring that all acquired evidence is forensically sound, legally admissible, and ethically compliant, empowering investigators to extract vital intelligence from the most challenging digital artifacts.

Programme Curriculum

Training Course on Advanced Embedded System Forensics

Introduction

This highly specialized training course is meticulously crafted for digital forensic investigators, cybersecurity researchers, reverse engineers, and incident response teams confronting the unique and intricate challenges of advanced embedded system forensics. From the ubiquitous IoT devices, smart appliances, and wearables to industrial control systems (ICS), automotive ECUs, and critical infrastructure components, embedded systems are at the core of modern technology, yet they present a distinct and often opaque landscape for forensic analysis. Training Course on Advanced Embedded System Forensics provides the cutting-edge knowledge and intensive hands-on skills required to acquire, preserve, and analyze digital evidence directly from the hardware and firmware of these specialized devices, crucial for uncovering firmware tampering, sophisticated malware, intellectual property theft, and cyber-physical attacks.

The curriculum delves deep into the low-level architectures of embedded systems, exploring microcontroller internals, various memory technologies (NAND, NOR, eMMC, SPI Flash), JTAG/SWD debugging interfaces, and custom communication protocols. Through extensive practical labs, firmware reverse engineering exercises, hardware analysis techniques (e.g., Chip-Off, ISP), and vulnerability exploitation for forensic access, participants will master methodologies to bypass security features, recover deleted data, and analyze proprietary file systems, even from physically damaged or non-responsive devices. The course also critically examines the ethical and legal complexities (including Kenya's Data Protection Act 2019) of performing invasive forensics on embedded systems, ensuring that all acquired evidence is forensically sound, legally admissible, and ethically compliant, empowering investigators to extract vital intelligence from the most challenging digital artifacts.

Course Duration

10 Days

Course Objectives

1. Understand the architecture and memory organization of diverse embedded systems (microcontrollers, SoCs, FPGAs).
2. Identify and leverage hardware debugging interfaces (e.g., JTAG, SWD, UART) for forensic data extraction.
3. Perform physical data acquisition from embedded memory chips using Chip-Off and In-System Programming (ISP) techniques.
4. Conduct firmware extraction and reverse engineering to analyze proprietary code, configurations, and hidden artifacts.

5. Analyze custom embedded operating systems (e.g., RTOS, bare-metal) and their unique forensic characteristics.
6. Investigate firmware tampering, malicious implants, and rootkits in embedded devices.
7. Extract and interpret device logs, sensor data, and command history from IIoT and consumer embedded devices.
8. Identify vulnerabilities in embedded bootloaders and secure boot processes for forensic bypass.
9. Decipher proprietary data formats and communication protocols used by embedded systems.
10. Reconstruct incident timelines by correlating evidence from embedded devices with network and cloud artifacts.
11. Develop custom tools and scripts (Python, Ghidra/IDA Pro scripting) for automated embedded forensic analysis.
12. Navigate the legal and ethical considerations of performing invasive forensics on embedded systems, including Kenya's Data Protection Act.
13. Generate comprehensive forensic reports detailing complex embedded system investigations for expert testimony.

Organizational Benefits

1. Unprecedented Access to Evidence: Recover crucial data from previously inaccessible or highly specialized embedded devices.
2. Enhanced Incident Response: Accelerate the investigation of sophisticated cyber-physical attacks targeting embedded systems.
3. Proactive Threat Intelligence: Develop internal expertise to analyze embedded malware and emerging vulnerabilities.
4. Reduced Reliance on External Expertise: Bring highly specialized and costly embedded forensic capabilities in-house.
5. Improved Success Rates: Increase the likelihood of recovering critical evidence from challenging embedded device cases.
6. Strengthened Product Security: Understand embedded system weaknesses to better secure proprietary products and intellectual property.
7. Faster Time to Resolution: Decrease investigation timelines for incidents involving embedded systems.
8. Strategic Advantage: Position the organization at the forefront of advanced embedded systems security and forensics.
9. Compliance Adherence: Ensure advanced data acquisition techniques comply with legal and ethical standards (e.g., Kenya Data Protection Act).
10. Expert Witness Development: Cultivate personnel capable of providing expert testimony on highly technical embedded system forensics.

Target Participants

- Experienced Digital Forensic Investigators
- Cybersecurity Incident Responders
- Hardware Reverse Engineers
- Firmware Analysts / Malware Reverse Engineers
- IoT Security Researchers
- Industrial Control Systems (ICS) / OT Security Professionals
- Automotive Cybersecurity Specialists
- Government Intelligence and Law Enforcement Units
- Embedded Systems Developers (with a security interest)
- Product Security Engineers (Hardware/Firmware)

Course Outline

Module 1: Embedded Systems Architecture & Memory (Embedded Hardware Fundamentals)

- Introduction to Microcontrollers, Microprocessors, and SoCs
- Types of Embedded Memory: NOR Flash, NAND Flash, eMMC, SPI Flash, EEPROM, RAM
- Memory Mapping and Address Spaces in Embedded Systems
- Understanding Embedded Operating Systems (RTOS, Bare-Metal, Linux Embedded)
- **Case Study**: Deconstructing the memory layout of a common IoT development board.

Module 2: Physical Acquisition Techniques (Hardware Data Extraction)

- Principles of Chip-Off Forensics for Embedded Memory
- In-System Programming (ISP) for Direct Memory Access
- JTAG/SWD Debugging Interfaces for Data Extraction
- Device Disassembly and Component Identification
- **Case Study**: Performing a Chip-Off acquisition on a consumer drone's flight controller.

Module 3: Firmware Extraction & Analysis (Firmware Forensics)

- Methods for Firmware Extraction (JTAG, SPI Programmer, UART, Exploit-based)
- Identifying Firmware Formats and Structures
- Tools for Firmware Analysis: Binwalk, Firmware Mod Kit (fmk)
- Dissecting Bootloaders and Kernel Images
- **Case Study**: Extracting and unpacking the firmware from a smart router.

Module 4: Embedded File Systems & Data Recovery (Embedded File System Forensics)

- Common Embedded File Systems (UBIFS, JFFS2, YAFFS2, cramfs)
- Challenges of Wear Leveling and Flash Translation Layers (FTL)
- Recovering Deleted Data from Embedded Flash Memory
- Carving for Artifacts in Raw Memory Dumps
- **Case Study**: Recovering deleted logs from a smart home hub's flash memory.

Module 5: Firmware Reverse Engineering (Embedded Code Analysis)

- Introduction to ARM Assembly and MIPS Assembly
- Using Disassemblers/Decompilers: Ghidra, IDA Pro for Firmware Analysis
- Identifying Functions, Variables, and Control Flow in Embedded Binaries

- Patching Firmware for Forensic Access or Debugging
- **Case Study**: Reverse engineering a firmware function responsible for device authentication.

Module 6: Bootloader & Secure Boot Forensics (Bootloader Exploitation)

- Understanding Embedded Bootloaders (e.g., U-Boot, RedBoot, custom bootloaders)
- Analyzing Secure Boot Chains and Trust Anchors
- Identifying and Leveraging Bootloader Vulnerabilities for Forensic Access
- Bypassing Secure Boot for Firmware Modification/Extraction
- **Case Study**: Exploiting a known bootloader vulnerability in an industrial control device.

Module 7: Embedded OS & RTOS Forensics (RTOS Forensics)

- Forensic Analysis of Real-Time Operating Systems (RTOS) (e.g., FreeRTOS, VxWorks, Zephyr)
- Extracting Task Information, Kernel Objects, and Memory Allocations
- Analyzing RTOS-specific Logs and Debug Information
- Understanding Context Switching and Interrupt Handling for Incident Reconstruction
- **Case Study**: Analyzing a FreeRTOS memory dump to identify active processes during an incident.

Module 8: Device Logs & Data Artifacts (Embedded Log Analysis)

- Identifying and Extracting Device-Specific Logs (System Logs, Application Logs, Error Logs)
- Parsing Proprietary Log Formats
- Analyzing Sensor Data, Actuator Commands, and Historical Data
- Correlating Device Events with External Stimuli
- **Case Study**: Reconstructing user actions from the logs of a smart thermostat.

Module 9: Custom Protocols & Communication (Embedded Protocol Forensics)

- Reverse Engineering Custom Embedded Communication Protocols (Serial, SPI, I2C, CAN Bus)
- Analyzing Network Traffic from Embedded Devices
- Decrypting Encrypted Embedded Communications
- Tools for Protocol Analysis and Emulation
- **Case Study**: Analyzing CAN bus traffic from a vehicle's infotainment system.

Module 10: Vulnerability & Exploit Analysis (Embedded Vulnerability Forensics)

- Common Vulnerabilities in Embedded Systems (Buffer Overflows, Race Conditions, Authentication Bypass)
- Identifying Exploitation Traces on Embedded Devices
- Analyzing Shellcode and Malware Persistence Mechanisms in Firmware
- Understanding Firmware Update Vulnerabilities
- **Case Study**: Investigating a compromised smart meter for traces of a firmware update attack.

Module 11: Anti-Forensic Techniques in Embedded Systems (Embedded Anti-Forensics)

- Understanding Anti-Forensic Measures (Secure Erase, Self-Destruct Mechanisms, Data Obfuscation)
- Detecting and Counteracting Anti-Forensic Attempts on Embedded Devices
- Data Carving and Fragment Recovery from Wiped or Reset Devices
- Memory Volatility and Its Impact on Evidence Preservation

- **Case Study**: Recovering data from an embedded device designed to wipe its memory upon tamper detection.

Module 12: Forensic Tooling & Automation (Embedded Forensic Tools)

- Overview of Commercial and Open-Source Embedded Forensic Tools
- Using Hardware Tools (Logic Analyzers, Oscilloscopes, Protocol Analyzers)
- Scripting for Automated Data Parsing and Artifact Extraction (Python, Ghidra/IDA Python)
- Building a Dedicated Embedded Forensics Lab Environment
- **Case Study**: Automating the extraction of specific log entries from a large firmware dump using Python scripting.

Module 13: Supply Chain Attacks & Trust (Supply Chain Forensics)

- Investigating Compromises in the Embedded Device Supply Chain
- Detecting Malicious Hardware Components or Firmware Injections
- Analyzing Manufacturing Test Points and Debug Backdoors
- Verifying Firmware Authenticity and Integrity
- **Case Study**: Tracing a suspicious firmware modification to a specific point in the manufacturing supply chain.

Module 14: Legal, Ethical & Reporting Considerations (Embedded Forensics Legal & Ethics)

- Legal Frameworks for Embedded Device Forensics (Warrants, Consent)
- Ethical Guidelines for Conducting Invasive Hardware/Firmware Analysis
- Data Privacy Concerns and Compliance (e.g., **Kenya Data Protection Act 2019**)
- Crafting Expert-Level Forensic Reports for Embedded System Investigations
- **Case Study**: Discussing the ethical dilemma of potentially bricking a device during a Chip-Off operation in a criminal investigation.

Module 15: Emerging Trends & Future Challenges (Future of Embedded Forensics)

- Forensics of Next-Gen IIoT and Smart City Embedded Devices
- AI/ML Integration in Embedded Systems and its Forensic Impact
- Investigating Quantum-Resistant Cryptography in Embedded Devices
- Challenges of Hardware Security Modules (HSMs) and Trusted Execution Environments (TEEs)
- **Case Study**: Predicting future forensic challenges posed by AI-powered edge computing devices.

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.

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
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