Training Course on Advanced Mobile OS Vulnerabilities for 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 plunges into the critical domain of advanced mobile operating system (OS) vulnerabilities, specifically tailored for digital forensic practitioners, cybersecurity researchers, and elite incident response teams. As mobile devices, particularly smartphones, are the epicenter of modern digital lives, they are also prime targets for sophisticated attacks, including zero-day exploits, malware, and advanced persistent threats (APTs). Training Course on Advanced Mobile OS Vulnerabilities for Forensics moves beyond standard mobile forensics, equipping participants with the cutting-edge knowledge and hands-on skills to identify, analyze, and leverage complex OS-level vulnerabilities to achieve deeper data extraction and a more complete forensic picture, even from locked, encrypted, or compromised devices.

The curriculum provides an in-depth exploration of the internal architectures of both iOS and Android operating systems, focusing on their security models, common vulnerabilities (e.g., kernel exploits, privilege escalation, sandbox escapes), and the methods attackers use to exploit them. Through intensive practical labs, reverse engineering exercises, and analysis of real-world exploits, attendees will gain proficiency in techniques such as JTAG, Chip-Off, advanced logical extractions via exploited interfaces, and memory forensics specific to mobile environments. The course emphasizes the ethical and legal implications of leveraging such vulnerabilities for forensic purposes, ensuring participants operate within legal boundaries while pushing the frontiers of digital evidence recovery in an ever-evolving threat landscape.

Programme Curriculum

Training Course on Advanced Mobile OS Vulnerabilities for Forensics

Introduction

This highly specialized training course plunges into the critical domain of advanced mobile operating system (OS) vulnerabilities, specifically tailored for digital forensic practitioners, cybersecurity researchers, and elite incident response teams. As mobile devices, particularly smartphones, are the epicenter of modern digital lives, they are also prime targets for sophisticated attacks, including zero-day exploits, malware, and advanced persistent threats (APTs). Training Course on Advanced Mobile OS Vulnerabilities for Forensics moves beyond standard mobile forensics, equipping participants with the cutting-edge knowledge and hands-on skills to identify, analyze, and leverage complex OS-level vulnerabilities to achieve deeper data extraction and a more complete forensic picture, even from locked, encrypted, or compromised devices.

The curriculum provides an in-depth exploration of the internal architectures of both iOS and Android operating systems, focusing on their security models, common vulnerabilities (e.g., kernel exploits, privilege escalation, sandbox escapes), and the methods attackers use to exploit them. Through intensive practical labs, reverse engineering exercises, and analysis of real-world exploits, attendees will gain proficiency in techniques such as JTAG, Chip-Off, advanced logical extractions via exploited interfaces, and memory forensics specific to mobile environments. The course emphasizes the ethical and legal implications of leveraging such vulnerabilities for forensic purposes, ensuring participants operate within legal boundaries while pushing the frontiers of digital evidence recovery in an ever-evolving threat landscape.

Course Duration

10 Days

Course Objectives

1. Understand the advanced security architectures of iOS and Android operating systems (e.g., Secure Enclave, SELinux, TrustZone).
2. Identify and categorize common mobile OS vulnerabilities including kernel bugs, privilege escalation flaws, and sandbox bypasses.
3. Perform deep-level physical acquisitions using techniques like JTAG, Chip-Off, and eMMC/eMCP direct access from non-responsive or locked devices.
4. Analyze mobile OS kernel memory dumps for indicators of compromise (IOCs) and rootkits.
5. Leverage discovered vulnerabilities (e.g., bootloader exploits, sideloading flaws) to bypass device locks and encryption for forensic acquisition.
6. Conduct firmware analysis and reverse engineering of mobile OS components to identify hidden artifacts and malicious modifications.
7. Investigate zero-day exploits affecting mobile operating systems and their impact on data integrity.

8. Trace and analyze mobile malware persistence mechanisms and data exfiltration techniques at the OS level.
9. Decipher proprietary encryption schemes and secure boot mechanisms prevalent in modern mobile devices.
10. Develop custom tools and scripts (Python, IDA Pro scripting) for automated analysis of mobile OS artifacts and exploited data.
11. Perform live forensic acquisition from running mobile devices via exploited debugging interfaces.
12. Understand the legal and ethical considerations of utilizing advanced exploitation techniques for forensic purposes, especially concerning data privacy (e.g., Kenya Data Protection Act).
13. Generate expert-level forensic reports detailing complex mobile OS vulnerability exploitation and data recovery processes.

Organizational Benefits

1. Unprecedented Data Access: Gain the ability to extract data from previously inaccessible or highly secure mobile devices.
2. Enhanced Incident Response: Accelerate the investigation of advanced mobile cyberattacks, including zero-day and APTs.
3. Proactive Threat Intelligence: Develop internal expertise to analyze sophisticated mobile exploits and understand emerging threats.
4. Reduced Reliance on External Expertise: Bring highly specialized and costly mobile forensic capabilities in-house.
5. Improved Success Rates: Increase the likelihood of recovering crucial evidence from challenging mobile forensic cases.
6. Strengthened Cybersecurity Posture: Understand mobile OS weaknesses to better secure organizational mobile assets and BYOD policies.
7. Faster Time to Resolution: Decrease the time required for complex mobile investigations, leading to quicker legal or operational outcomes.
8. Strategic Advantage: Position the organization at the forefront of mobile digital forensics capabilities.
9. Compliance Adherence: Ensure advanced data acquisition techniques are executed within strict legal and ethical boundaries.
10. Expert Witness Development: Cultivate personnel capable of providing expert testimony on highly technical mobile OS vulnerabilities and exploit forensics.

Target Participants

- Experienced Mobile Forensic Examiners
- Digital Forensic Researchers
- Cybersecurity Incident Responders
- Penetration Testers specializing in Mobile Devices

- Advanced Law Enforcement Cybercrime Units
- Government Intelligence Analysts
- Reverse Engineers (Malware Analysts)
- Mobile OS Security Developers
- E-Discovery Specialists dealing with highly secured devices
- Threat Intelligence Analysts focusing on mobile platforms

Course Outline

Module 1: Mobile OS Architecture & Security Models (Advanced Mobile OS Internals)

- Deep Dive into iOS and Android Kernel Architecture
- Understanding Mobile OS Security Layers (Sandboxing, ASLR, DEP, SELinux, Secure Enclave)
- Mobile Boot Process and Secure Boot Mechanisms
- Introduction to ARM Assembly and Mobile Exploitation Primitives
- **Case Study**: Deconstructing the boot process of a modern Android device.

Module 2: Advanced Data Acquisition Techniques (Deep Mobile Data Extraction)

- Principles of Physical Acquisition: JTAG, Chip-Off, and eMMC/eMCP Techniques
- In-System Programming (ISP) for Data Access
- NAND Flash Memory Structures and Data Carving
- Bypassing Lock Screens and Encryption at the Hardware Level
- **Case Study**: Performing a Chip-Off acquisition on a non-responsive mobile device.

Module 3: Mobile Bootloader & Firmware Exploitation (Bootloader Exploits for Forensics)

- Understanding Mobile Bootloaders (e.g., iBoot, Qualcomm PBL, EDL Mode)
- Identifying and Leveraging Bootloader Vulnerabilities for Forensic Access
- Analyzing and Dumping Mobile Device Firmware
- Techniques for Flashing Custom Firmware for Forensic Purposes (with ethical considerations)
- **Case Study**: Utilizing a known bootloader vulnerability to gain read access to a locked iOS device.

Module 4: Kernel-Level Forensics & Rootkits (Mobile Kernel Forensics)

- Introduction to Mobile OS Kernel Exploits (Privilege Escalation)
- Analyzing Kernel Memory Dumps for Hidden Processes and Rootkits
- Detecting Kernel-Level Modifications and Integrity Violations
- Using Kernel Debuggers for Live Forensic Analysis
- **Case Study**: Identifying a kernel-mode rootkit on a rooted Android device.

Module 5: Sandbox Escapes & Inter-Process Communication (IPC Forensics)

- Understanding Mobile OS Sandboxing Mechanisms and Their Limitations
- Techniques for Identifying and Exploiting Sandbox Escapes
- Analyzing Inter-Process Communication (IPC) Mechanisms for Data Exfiltration Pathways
- Forensic Analysis of Mobile Application Sandboxes
- **Case Study**: Tracing a malicious app's attempt to escape its sandbox and access sensitive data.

Module 6: Mobile Malware & APT Analysis (Advanced Mobile Malware Analysis)

- Deep Dive into Mobile Malware Families (e.g., Pegasus, Chrysaor, NSO Group exploits)
- Static and Dynamic Analysis of Mobile Malware Samples
- Identifying Malware Persistence Mechanisms on Mobile OS
- Tracing Data Exfiltration Routes and Command & Control (C2) Communication
- **Case Study**: Performing a reverse engineering analysis of a suspicious Android APK for malicious intent.

Module 7: Zero-Day Exploit Identification & Impact (Zero-Day Mobile Forensics)

- Methodologies for Identifying Undisclosed (Zero-Day) Mobile OS Vulnerabilities
- Analyzing Publicly Disclosed Zero-Day Exploits and Their Forensic Implications
- Detecting Traces of Zero-Day Exploitation on Compromised Devices
- Responding to Mobile Devices Affected by Zero-Day Attacks
- **Case Study**: Investigating a device suspected of being compromised by a zero-click iOS exploit.

Module 8: Advanced iOS Forensics & Security (Deep iOS Forensics)

- iOS File System Analysis (APFS) and Secure Enclave Interaction
- Keychain Data Extraction and Decryption Techniques
- Advanced iMessage and Safari Data Forensics
- Analyzing iOS System Logs for Security Events and Anomalies
- **Case Study**: Extracting and analyzing encrypted keychain data from an unlocked iOS device.

Module 9: Advanced Android Forensics & Security (Deep Android Forensics)

- Android File System Analysis and SELinux Enforcement
- User Data Encryption (FBE/FDE) and Decryption Challenges
- Advanced SQLite Database Analysis for Android Apps
- Analyzing Android System Logs (logcat) for Malicious Activities
- **Case Study**: Overcoming File-Based Encryption (FBE) to extract data from an Android device.

Module 10: Memory Forensics on Mobile Devices (Mobile RAM Forensics)

- Techniques for Acquiring RAM Dumps from Live Mobile Devices
- Analyzing Mobile Memory Dumps for Volatile Artifacts (Processes, Network Connections, Credentials)
- Identifying In-Memory Exploits and Shellcode
- Tools and Methodologies for Mobile Memory Analysis
- **Case Study**: Extracting in-memory artifacts from a suspect's rooted Android phone.

Module 11: Network & Protocol Analysis on Mobile (Mobile Network Forensics)

- Capturing and Analyzing Mobile Device Network Traffic (Wi-Fi, Cellular)
- Identifying Suspicious Connections and C2 Traffic
- Decrypting TLS/SSL Traffic from Mobile Applications
- Investigating VPN Configurations and Proxy Settings on Mobile OS
- **Case Study**: Detecting a malicious app's C2 communication by analyzing network traffic captures.

Module 12: Anti-Forensic Techniques & Evasion (Mobile Anti-Forensics Countermeasures)

- Common Anti-Forensic Techniques on Mobile Devices (Data Wiping, Encryption, Root Cloaking)
- Methods for Detecting and Counteracting Anti-Forensic Measures
- Data Carving and Fragment Recovery from Heavily Modified Devices
- Advanced Persistence and Stealth Techniques Used by Attackers
- **Case Study**: Recovering partially wiped data from a mobile device after a factory reset attempt.

Module 13: Custom Scripting & Tool Development (Mobile Forensic Automation)

- Introduction to Python for Mobile Forensic Automation
- Scripting for Automated Data Parsing and Artifact Extraction
- Leveraging APIs for Programmatic Interaction with Forensic Tools
- Building Custom Utilities for Niche Mobile Forensic Challenges
- **Case Study**: Developing a Python script to automatically parse a proprietary log format from a specific mobile app.

Module 14: Legal, Ethical & Reporting Considerations (Advanced Mobile Forensic Ethics)

- Advanced Legal Challenges in Mobile OS Vulnerability Exploitation (Warrants, Consent)
- Ethical Guidelines for Conducting Invasive Mobile Forensics
- Impact of Data Protection Acts (Kenya Data Protection Act 2019) on Advanced Mobile Forensics
- Crafting Expert-Level Forensic Reports for Complex Mobile OS Findings
- **Case Study**: Discussing the ethical implications of using a zero-day exploit to gain access to a suspect's phone.

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

- Forensics of 5G Devices and Edge Computing
- Investigating Next-Gen Mobile OS (e.g., Fuchsia OS, specialized IoT OS)
- AI/ML in Mobile Forensics: Opportunities and Limitations
- The Impact of Quantum Computing on Mobile Device Encryption
- **Case Study**: Predicting forensic challenges and solutions for a hypothetical AI-powered mobile device.

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.
- 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