Training Course on Mobile Malware Forensics and Analysis

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 is designed to equip digital forensic professionals and cybersecurity analysts with the critical skills and in-depth knowledge required for mobile malware forensics and advanced threat analysis. Participants will delve into the intricacies of both Android and iOS malware, learning to identify, analyze, and reverse engineer malicious applications that target mobile devices. Training Course on Mobile Malware Forensics and Analysis focuses on understanding the latest mobile malware trends, including banking Trojans, spyware, ransomware, and sophisticated APTs, providing hands-on experience with static and dynamic analysis techniques to uncover their malicious capabilities and impact.

Through a blend of theoretical instruction and intensive practical labs, this program empowers investigators to effectively conduct malware incident response, extract compromised data, and develop actionable threat intelligence. Participants will master the use of industry-standard forensic tools and reverse engineering platforms, enabling them to dissect mobile malware, understand its communication protocols, and attribute attacks. This course is essential for anyone on the front lines of mobile security, seeking to defend against the ever-evolving landscape of mobile cyber threats and protect critical organizational assets.

Programme Curriculum

Training Course on Mobile Malware Forensics and Analysis

Introduction

This specialized training course is designed to equip digital forensic professionals and cybersecurity analysts with the critical skills and in-depth knowledge required for mobile malware forensics and advanced threat analysis. Participants will delve into the intricacies of both Android and iOS malware, learning to identify, analyze, and reverse engineer malicious applications that target mobile devices. Training Course on Mobile Malware Forensics and Analysis focuses on understanding the latest mobile malware trends, including banking Trojans, spyware, ransomware, and sophisticated APTs, providing hands-on experience with static and dynamic analysis techniques to uncover their malicious capabilities and impact.

Through a blend of theoretical instruction and intensive practical labs, this program empowers investigators to effectively conduct malware incident response, extract compromised data, and develop actionable threat intelligence. Participants will master the use of industry-standard forensic tools and reverse engineering platforms, enabling them to dissect mobile malware, understand its communication protocols, and attribute attacks. This course is essential for anyone on the front lines of mobile security, seeking to defend against the ever-evolving landscape of mobile cyber threats and protect critical organizational assets.

Course Duration

10 Days

Course Objectives

1. Identify and classify the latest mobile malware families and their common attack vectors across Android and iOS.
2. Perform forensically sound acquisition of mobile devices suspected of malware infection, preserving critical evidence.
3. Conduct static analysis of mobile malware samples (APKs, IPAs), extracting crucial metadata, permissions, and string artifacts.
4. Execute dynamic analysis of mobile malware in a controlled environment, monitoring its behavior, network traffic, and file system interactions.
5. Utilize disassemblers and decompilers (e.g., Ghidra, IDA Pro, Jadx) for reverse engineering mobile malware binaries.
6. Analyze obfuscation and anti-analysis techniques employed by mobile malware to evade detection and hinder reverse engineering.
7. Investigate mobile banking Trojans and credential stealers, understanding their methods for financial fraud.
8. Dissect mobile spyware and stalkerware, identifying data exfiltration mechanisms and surveillance capabilities.

9. Understand ransomware attacks on mobile devices, including their encryption methodologies and recovery challenges.
10. Develop YARA rules and other signatures for proactive detection and identification of mobile malware.
11. Reconstruct the infection chain and attack timeline of mobile malware incidents.
12. Generate comprehensive malware analysis reports and contribute to actionable threat intelligence on mobile threats.
13. Implement mobile endpoint detection and response (EDR) principles for proactive defense against mobile malware.

Organizational Benefits

1. Enhanced Threat Detection: Proactively identify and respond to sophisticated mobile malware threats targeting the organization.
2. Reduced Incident Response Time: Expedite the analysis and containment of mobile malware incidents, minimizing potential damage.
3. Improved Data Protection: Safeguard sensitive organizational and user data from exfiltration by malicious mobile applications.
4. Strengthened Mobile Security Posture: Gain deep insights into mobile attack vectors to fortify mobile device security policies and infrastructure.
5. Effective Proactive Defense: Develop custom signatures and intelligence to prevent future mobile malware infections.
6. Compliance with Security Regulations: Ensure forensic practices align with industry standards and legal requirements for incident handling.
7. Cost Savings: Reduce reliance on external mobile malware analysis services by building in-house expertise.
8. Actionable Threat Intelligence: Contribute to internal and external threat intelligence feeds, aiding broader cybersecurity efforts.
9. Protection of Brand Reputation: Mitigate risks associated with mobile malware compromising company-owned devices or applications.
10. Skill Development & Retention: Invest in highly specialized training for security personnel, increasing their value and commitment.

Target Participants

- Malware Analysts
- Digital Forensic Investigators
- Cybersecurity Incident Responders
- Reverse Engineers
- Security Operations Center (SOC) Analysts
- Threat Intelligence Analysts
- Mobile Application Developers (with security focus)

- Penetration Testers (mobile)
- IT Security Professionals
- Law Enforcement Cybercrime Units

Course Outline

Module 1: Introduction to Mobile Malware & Ecosystems (Mobile Malware Fundamentals)

- Overview of Mobile Operating Systems (Android & iOS) Security Models
- Evolution of Mobile Malware: Historical Context and Current Landscape
- Types of Mobile Malware: Trojans, Spyware, Ransomware, Adware, Rootkits, Worms
- Mobile Malware Distribution Methods and Infection Vectors (Side-loading, App Stores, Phishing)
- **Case Study**: Analyzing a common mobile adware campaign.

Module 2: Mobile Malware Acquisition & Preservation (Malware Acquisition Mobile)

- Forensic Acquisition Techniques for Infected Mobile Devices (Logical, File System, Physical)
- Isolation of Infected Devices (Faraday Bags, Network Isolation)
- Creating Forensically Sound Images of Compromised Devices
- Preservation of Mobile Malware Samples and Associated Artifacts
- **Case Study**: Acquiring data from an Android device suspected of a new banking Trojan.

Module 3: Setting Up a Mobile Malware Analysis Lab (Malware Analysis Lab Setup)

- Virtualization Technologies for Safe Malware Analysis (VMware, VirtualBox)
- Android Emulators and iOS Simulators for Dynamic Analysis
- Network Configuration for Malware Sandboxing (INetSim, Burp Suite)
- Essential Tools for Static and Dynamic Mobile Malware Analysis
- **Case Study**: Configuring a secure and isolated environment for Android malware execution.

Module 4: Static Analysis of Android Malware (Android Malware Static Analysis)

- Decompiling Android APKs (Jadx, APKTool, Bytecode Viewer)
- Analyzing AndroidManifest.xml for Permissions and Components
- Examining DEX Files and Smali Code for Malicious Functionality
- Identifying Suspicious Strings, URLs, and IP Addresses
- **Case Study**: Static analysis of an Android banking Trojan's APK.

Module 5: Dynamic Analysis of Android Malware (Android Malware Dynamic Analysis)

- Running Android Malware in a Sandbox Environment (Cuckoo Sandbox, Mobile Sandboxes)
- Monitoring Network Traffic (Wireshark, Burp Suite, Fiddler)
- Analyzing API Calls and System Interactions (Frida, Xposed)
- Observing File System Changes and Dropped Files
- **Case Study**: Observing the real-time behavior of an Android spyware sample.

Module 6: Static Analysis of iOS Malware (iOS Malware Static Analysis)

- Analyzing iOS IPA Files and Application Bundles
- Examining Info.plist and Entitlements for iOS App Permissions
- Reverse Engineering iOS Binaries (Objective-C, Swift) with Ghidra/IDA Pro
- Identifying Suspicious Libraries and Frameworks

- **Case Study**: Static analysis of a suspected iOS surveillance app.

Module 7: Dynamic Analysis of iOS Malware (iOS Malware Dynamic Analysis)

- Running iOS Malware on Jailbroken Devices or Emulators
- Monitoring Network Connections and Data Exfiltration
- Intercepting API Calls and Runtime Behavior (Frida, Cycript)
- Analyzing Process Memory and Loaded Modules
- **Case Study**: Observing data exfiltration attempts from an iOS malware sample.

Module 8: Mobile Banking Trojans & Financial Malware (Mobile Banking Malware)

- Characteristics and Attack Methods of Mobile Banking Trojans (e.g., Mamont, Anubis, Cerberus)
- Overlay Attacks and SMS Interception Techniques
- Identifying Phishing and Social Engineering Lures
- Strategies for Extracting Stolen Financial Data
- **Case Study**: Dissecting a banking Trojan's code to understand its overlay injection.

Module 9: Mobile Spyware & Stalkerware Analysis (Mobile Spyware Analysis)

- Detecting Covert Surveillance Applications
- Analyzing Call Recording, SMS Logging, and Location Tracking Functionality
- Identifying Remote Control and Data Exfiltration Mechanisms
- Forensic Artifacts Left by Spyware Applications
- **Case Study**: Analyzing an Android stalkerware app's data collection methods.

Module 10: Mobile Ransomware & Cryptojacking (Mobile Ransomware Forensics)

- Understanding Mobile Ransomware Encryption Techniques
- Identifying Ransom Demands and Communication Channels
- Strategies for Data Recovery from Encrypted Mobile Devices (if possible)
- Recognizing Cryptojacking Malware on Mobile Devices
- **Case Study**: Analyzing a mobile ransomware sample's encryption routine.

Module 11: Advanced Obfuscation & Anti-Analysis Techniques (Malware Anti-Analysis)

- Code Obfuscation (e.g., ProGuard, DexGuard) and Deobfuscation Techniques
- Anti-Debugging and Anti-Emulator Measures
- Polymorphic and Metamorphic Mobile Malware
- Bypassing Anti-Analysis Protections
- **Case Study**: Deobfuscating a packed Android malware sample.

Module 12: Mobile Malware Persistence & Rootkits (Mobile Malware Persistence)

- Understanding Mobile Malware Persistence Mechanisms (Boot-time, App Permissions)
- Analyzing Rootkits and Kernel-Level Compromises on Mobile Devices
- Detecting Privilege Escalation Exploits
- Identifying Modified System Files and Processes
- **Case Study**: Investigating how a mobile rootkit maintains persistence on a device.

Module 13: Attribution & Threat Intelligence (Mobile Threat Intelligence)

- Correlating Malware Samples with Known Threat Actors and Campaigns
- Developing YARA Rules for Mobile Malware Detection

- Contributing to and Leveraging Public Threat Intelligence Platforms
- Understanding Malware Triage and Scoring Methodologies
- **Case Study**: Developing YARA rules to detect a specific family of mobile spyware.

Module 14: Mobile Malware Incident Response (Mobile Malware Incident Response)

- Steps for Responding to a Mobile Malware Infection
- Containment, Eradication, and Recovery Strategies
- Post-Incident Analysis and Lessons Learned
- Communication and Reporting during a Mobile Malware Incident
- **Case Study**: Simulating a mobile malware incident response scenario.

Module 15: Future Trends in Mobile Malware (Future Mobile Malware)

- AI/ML in Mobile Malware Development and Detection
- Targeting of IoT Devices via Mobile Platforms
- Exploiting Supply Chain Vulnerabilities in Mobile Apps
- Evolution of Zero-Click Exploits and Advanced Persistent Threats (APTs)
- **Case Study**: Discussing the potential impact of a hypothetical AI-driven mobile malware.

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.org or call *+254724527104*

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.

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