Training Course on Mobile Malware Analysis (Android and iOS)

Professional Development Training Course Outline

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

Course Introduction

As mobile devices continue to dominate personal and enterprise computing, they have become prime targets for sophisticated cyberattacks. With the rise in Android and iOS malware campaigns, there's an urgent demand for cybersecurity professionals equipped with advanced mobile malware analysis skills. Training Course on Mobile Malware Analysis (Android and iOS) empowers participants with practical, hands-on knowledge to detect, analyze, reverse-engineer, and mitigate mobile malware threats targeting both Android and iOS platforms. Using real-world scenarios, dynamic analysis tools, and forensic frameworks, learners will gain deep insight into how threat actors exploit mobile ecosystems and how to stay ahead of evolving attack vectors.

This course focuses on trending cyber threats such as spyware, trojans, ransomware, adware, and zero-day mobile exploits. Participants will learn how to leverage tools like Frida, MobSF, JADX, Ghidra, Hopper, and dynamic sandboxing environments. With the mobile threat landscape expanding rapidly due to BYOD (Bring Your Own Device) policies and mobile banking, mastering mobile malware analysis is essential for incident response teams, forensic investigators, ethical hackers, and security architects. This intensive course will enable participants to develop effective countermeasures and proactively protect mobile infrastructures.

Programme Curriculum

Training Course on Mobile Malware Analysis (Android and iOS)

Introduction

As mobile devices continue to dominate personal and enterprise computing, they have become prime targets for sophisticated cyberattacks. With the rise in Android and iOS malware campaigns, there's an urgent demand for cybersecurity professionals equipped with advanced mobile malware analysis skills. Training Course on Mobile Malware Analysis (Android and iOS) empowers participants with practical, hands-on knowledge to detect, analyze, reverse-engineer, and mitigate mobile malware threats targeting both Android and iOS platforms. Using real-world scenarios,

dynamic analysis tools, and forensic frameworks, learners will gain deep insight into how threat actors exploit mobile ecosystems and how to stay ahead of evolving attack vectors.

This course focuses on trending cyber threats such as spyware, trojans, ransomware, adware, and zero-day mobile exploits. Participants will learn how to leverage tools like Frida, MobSF, JADX, Ghidra, Hopper, and dynamic sandboxing environments. With the mobile threat landscape expanding rapidly due to BYOD (Bring Your Own Device) policies and mobile banking, mastering mobile malware analysis is essential for incident response teams, forensic investigators, ethical hackers, and security architects. This intensive course will enable participants to develop effective countermeasures and proactively protect mobile infrastructures.

Course Objectives

1. Understand the mobile threat landscape for Android and iOS platforms.
2. Perform static and dynamic analysis of mobile malware samples.
3. Use reverse engineering tools like JADX, Ghidra, Hopper, and IDA Pro.
4. Analyze mobile spyware, trojans, and ransomware behavior.
5. Identify zero-day mobile vulnerabilities and exploit methods.
6. Extract indicators of compromise (IOCs) from infected mobile devices.
7. Decompile Android APKs and analyze iOS IPA files.
8. Explore sandboxing and emulation techniques for dynamic malware testing.
9. Conduct memory forensics and behavioral profiling of mobile apps.
10. Integrate threat intelligence feeds into mobile malware investigations.
11. Use Frida and Objection for runtime instrumentation and hooking.
12. Examine malicious code obfuscation and anti-analysis techniques.
13. Build custom incident response strategies for mobile threats.

Target Audience

1. Cybersecurity Analysts
2. Incident Response Teams
3. Mobile App Developers
4. Ethical Hackers
5. Penetration Testers
6. Digital Forensic Investigators
7. Threat Intelligence Professionals
8. Security Architects

Course Duration: 5 days

Course Modules

Module 1: Introduction to Mobile Malware Ecosystems

- Overview of Android and iOS security architecture
- Common mobile threat vectors
- Categories of mobile malware
- Current attack trends
- Regulatory & compliance concerns
- *Case Study: Pegasus Spyware – A Deep Dive into Mobile Surveillance*

Module 2: Android Malware Basics

- APK structure and permissions
- Android app component analysis
- Common Android malware techniques

- Risky APIs and malware entry points
- Understanding manifest files
- *Case Study: Joker Malware Analysis*

Module 3: iOS Malware Basics

- iOS file system and sandboxing
- IPA structure and provisioning profiles
- Jailbreaking and iOS threat exposure
- iOS malware delivery methods
- Common exploits in iOS versions
- *Case Study: XCodeGhost – iOS Supply Chain Attack*

Module 4: Static Malware Analysis

- APK/IPA unpacking tools
- Decompiled code inspection with JADX & Hopper
- Signature-based detection
- File system artifact analysis
- Recognizing malicious behaviors in code
- *Case Study: Triada Trojan Static Breakdown*

Module 5: Dynamic Malware Analysis

- Sandboxing and emulation techniques
- Using MobSF for dynamic testing
- Real-time behavior monitoring
- Hooking and instrumentation basics
- Runtime analysis with Frida and Objection
- *Case Study: Analyzing Obfuscated Spyware in Emulated Environments*

Module 6: Reverse Engineering Android Apps

- Using JADX, Ghidra, and IDA Pro
- Disassembling DEX and ODEX files
- String extraction and control flow analysis
- Analyzing code obfuscation patterns
- Identifying C&C communication
- *Case Study: Unpacking and Reversing AndroRAT*

Module 7: Reverse Engineering iOS Apps

- Decrypting and disassembling IPA files
- Analyzing Mach-O binaries
- Leveraging Hopper and Radare2
- Symbol recognition and code paths
- Detecting iOS-specific obfuscation
- *Case Study: In-depth Forensics of a Banking Trojan*

Module 8: Mobile Memory Forensics

- Capturing volatile memory on Android and iOS
- Extracting sensitive data from memory dumps
- Identifying injected malicious code
- Investigating malicious runtime processes
- Leveraging tools like Volatility for mobile

- *Case Study: Memory Forensics of a Remote Access Trojan (RAT)*

Training Methodology

- Hands-on lab sessions with Android and iOS emulators
- Real malware sample analysis and reverse engineering
- Instructor-led demonstrations and tool walkthroughs
- Group discussions and team-based exercises
- Interactive quizzes and knowledge checkpoints
- Final capstone project with evaluation

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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