



# OFFENSIVE MOBILE MALWARE ANALYSIS

Expert-Led Cybersecurity Training · Beginner to Advanced

## COURSE OVERVIEW

The Offensive Mobile Malware Analysis course is designed to give a proper understanding of malware threats aimed at iOS and Android platforms. With a focus on mobile OS internals, attack vectors, and security mitigations, this course provides hands-on experience and practical insights. The curriculum begins with an in-depth exploration of iOS and Android architectures, focusing on their security features and platform specific APIs. Participants gain a comprehensive understanding of the challenges posed by modern mobile malware, including obfuscation, anti-detection techniques, and exploit delivery. The course covers sandboxing and the attack surface available from a sandboxed app, and later also discusses creation of jailbreaks and exploits. It also offers a comprehensive insight into reversing Objective-C, Swift, Java, Kotlin and Smali code, as well as native Android and iOS binaries.

The curriculum also covers advanced Frida techniques, such as custom tracing, profiling, and advanced memory inspection, with practical application in real-world scenarios. Through case studies of prominent malware like Operation Triangulation, LightSpy, Predator (Cytrox), Gold Digger, BingoMod, SpyMax v3, and Crocodilus and several custom malware samples designed for the course, the course sheds light on reverse engineering, advanced forensics techniques, and extracting and analyzing forensic artifacts. It concludes with insights into future research opportunities.

This course prepares you for the **Certified Mobile Malware Reverse Engineer (CMMRE)** certification exam, a hands-on assessment specifically designed to test your ability to reverse engineer, and analyze complex real-world malwares found in mobile applications.

## KEY LEARNING OBJECTIVES

- ARM Instruction set (includes updates from ARMv9)
- iOS and Android Security Model
- Setting up your own Malware Research Environment
- Corellium for Malware Research
- Understand how jailbreaks and exploits are written
- Reversing Objective-C, Swift, Java, Kotlin, and Smali code
- Reversing Native Android and iOS Binaries
- Frida for Runtime Analysis
- Advanced Frida Techniques (Agent-Based Architecture, Advanced Memory Inspection, Custom Tracing and Profiling, Inspecting Real-world applications using Frida; includes Objection/r2frida updates)
- Case Study of Public Malware (Operation Triangulation, LightSpy, Gold Digger, BingoMod, Crocodilus, etc)
- Case Study of Custom Malware designed for the course
- iOS and Android Forensics Techniques
- Inspecting Crash Logs
- Extraction and Analysis of Forensic Artifacts
- Conclusion and Future Research
- Become a Certified Mobile Malware Reverse Engineer (CMMRE)

## WHY SHOULD YOU TAKE THIS COURSE?

This is a completely hands-on course designed for beginners and intermediate students. Instead of just slides, attendees will get a chance to reverse engineer custom, and real-world Mobile malware. For the Onsite and Virtual sessions, the attendees will be provided with Cloud-based Corellium labs for performing the hands-on iOS and Android exercises without the need to carry physical phones. The slack channel is created before the course for the students so that they can be adequately prepared in terms of hardware and software before the class.





## WHO SHOULD ATTEND?

This course is designed for malware researchers, reverse engineers, penetration testers, mobile developers, or anyone passionate about learning more about the internals of mobile malware.

## HARDWARE/SOFTWARE REQUIREMENT

- Laptop with 8+ GB RAM and 40 GB hard disk space
- Students will be provided with access to Linux cloud instances
- Students will be provided with access to Corellium for iOS hands-on and as such do not need to carry iOS devices
- Administrative access on the system

Detailed Course Setup instructions and Slack access will be sent a few weeks prior to the class.

## WHAT WILL THE STUDENT GET?

- An attempt to Certified Mobile Malware Reverse Engineer (CMMRE) certification exam
- Certificate of completion for the Training program
- Source code for custom malwares
- All Frida Scripts used during the course
- Students will be provided with access to Corellium for iOS and Android hands-on for the duration of the course
- Students will be provided access to cloud instances for the duration of the course
- Slack access for the class and after for regular mobile security discussions

## PREREQUISITE KNOWLEDGE

- Working knowledge of cybersecurity and pentesting fundamentals
- Working knowledge of Malware analysis fundamentals on any platform
- Basic working knowledge of Android and iOS platforms
- Basic Linux skills and command-line proficiency
- Understanding of fundamental programming concepts and looping structures in at least one higher-level language (Java, Kotlin, Objective-C, Swift, C, C++, or similar)
- Basic ARM/AARCH64 binary assembly and exploitation knowledge is recommended, but not required

# COURSE SYLLABUS

## Module 1: Introduction to Reverse Engineering in iOS and Android

- Key Concepts and Terminologies
- Introduction to Hopper/Ghidra
- Introduction to the ARM 64 instruction set
- Disassembling methods
- Modifying assembly instructions
- Deciphering Mangled Swift Symbols
- Identifying Native Code
- Understanding the Program flow
- Identifying Cross-Platform mobile frameworks

## Module 2: Intro to iOS Security

- iOS security model
- App Signing, Sandboxing, and Provisioning
- iOS App Groups
- Primer to latest iOS security
- Xcode Primer
- Address Sanitizer
- Exploring the iOS filesystem
- What's in a Code Signature?
- Entitlements explained
- How Sandboxing works on iOS
- Sandbox profiles
- Setting up lldb for Debugging
- lldb basic and advanced usage
- Setting up the testing environment
- Jailbreaking your device
- What's in a Rootless Jailbreak?
- Jailbreak Bootstraps
- Sideloaded apps
- Binary protection measures
- Decrypting IPA files
- Self-signing iOS binaries

## Module 3: Intro to Android Security

- Android Security Architecture
- Extracting APK files from Google Play
- Understanding Android application structure
- Signing Android applications
- Understanding Android ADB
- Understanding the Android file system
- Permission Model Flaws
- Attack Surfaces for Android applications

## Module 4: Frida in-depth

- Overview of Frida and its capabilities
- Setting up the Frida environment
- Frida usage and commands
- Frida-trace and handlers
- Frida hooking techniques
- Frida on native code
- Frida memory manipulation techniques
- Analyzing messaging apps using Frida
- Invoking custom functions with Frida

## Module 5: Advanced Data Handling Techniques

- Introduction to Objective-C and Swift
- Reversing Objective-C, Swift, Kotlin and Java Binaries
- Reversing Obfuscated Code
- Reversing malicious iOS daemons
- Inspecting IPC traffic
- Understanding different stages of a Malware
- Device Acquisition techniques

- Using Custom IOCs
- Case Study of Public iOS Malware
- Process of Android Apps Engineering
- Reverse Engineering for Android Apps
- Smali Learning Labs
- Examining Smali files
- Smali vs Java
- Dex Analysis and Obfuscation
- Reversing Obfuscated Android Applications
- Case Study of Popular Android Malwares
- Patching Android Applications
- Android App Hooking
- Understanding the Program flow
- Identifying Cross-Platform mobile frameworks

## Module 6: Static and Dynamic analysis

- Proxying iOS and Android Traffic
- Introduction to Certificate Transparency
- Exploiting Local Storage
- Exploiting Weak Cryptography
- Multiple Manual and Automated Root Detection and Bypass Techniques
- Analyzing Proguard, DexGuard, and other Obfuscation Techniques
- Multiple Manual and Automated SSL Pinning Bypass techniques

## Module 7: Conclusion, Future Trends, and Challenges

- Inspecting Crash Logs
- Extraction and Analysis of Forensic Artifacts
- Introduction to the Mobile Verification Toolkit (MVT) for mobile app verification and security assessment.
- Using MVT for analyzing mobile apps, identifying vulnerabilities, and performing security assessments.
- Hands-on practice with MVT tools and techniques for mobile security assessment.
- Engaging in practical labs and case studies of Public Malwares.
- Identifying Malware artifacts from Filesystem and Backups





### *About the company*

8kSec is a foremost cyber security research company offering exceptional training and consulting services to aid clients in enhancing their security stance. Our experts possess extensive experience in delivering specialised cybersecurity training and consulting to several commercial and defence organisations across the United States, Europe, and the Middle East and North Africa region.

### *Get in touch*

[8kSec.io](https://8ksec.io)

[trainings@8ksec.io](mailto:trainings@8ksec.io)

