PRACTICAL MOBILE FORENSICS

Expert-Led Cybersecurity Training · Beginner to Advanced

COURSE OVERVIEW

This course is designed to equip participants with the necessary skills and knowledge to navigate the complexities of mobile device security, data acquisition, analysis, and reporting focusing on both the iOS and Android platforms.

The course covers the fundamentals of mobile forensics, exploring topics such as the evolution of mobile forensics, the challenges specific to iOS forensics, and dissecting the iOS operating system to understand its internals, filesystem structure, and security mechanisms. Participants will gain insights into user authentication, encryption, data protection, and establishing a robust workflow for seizure, identification, preservation, acquisition, analysis, validation, and reporting of mobile device data. Moving on to data acquisition from iOS devices, participants will learn about various acquisition methods including logical, physical, and filesystem acquisitions. Practical demonstrations will include logical acquisitions using several open source and commercial tools, as well as filesystem acquisitions using public Bootrom exploits and agent-based full filesystem acquisition techniques. In the iOS Data Analysis section, participants will get a walkthrough of forensic tools like Cellebrite Physical Analyzer, Magnet AXIOM, and open-source tools like Apollo, iLEAPP, and iOS Triage for analyzing evidence, decoding data, and extracting common iOS artifacts. Topics such as pattern-of-life forensics, location data analysis, connectivity data analysis, email and messaging forensics, as well as media forensics for photos, videos, and audio files will be explored in depth.

8KSEC

Transitioning to Android, the course covers understanding Android architecture, security features, filesystem structure, and Android forensic setup and pre-data extraction techniques. Participants will learn about Android data extraction techniques including manual extraction, logical extraction, ADB pull extraction, ADB backup extraction, physical extraction, and imaging techniques using tools like Autopsy. In the Android Data Analysis and Recovery section, participants will learn about analyzing and extracting data from Android image files using tools like Autopsy, and understand how to recover deleted files, contacts, and messages, and analyzing Android apps, malware, and reverse engineering techniques.

Additionally, participants will be introduced to advanced concepts such as the TAXII protocol for threat intelligence sharing, the use of Custom IOCs (Indicators of Compromise) for identifying threats specific to mobile environments, and leveraging tools like the Mobile Verification Toolkit (MVT) for mobile app verification and security assessment.

KEY LEARNING OBJECTIVES

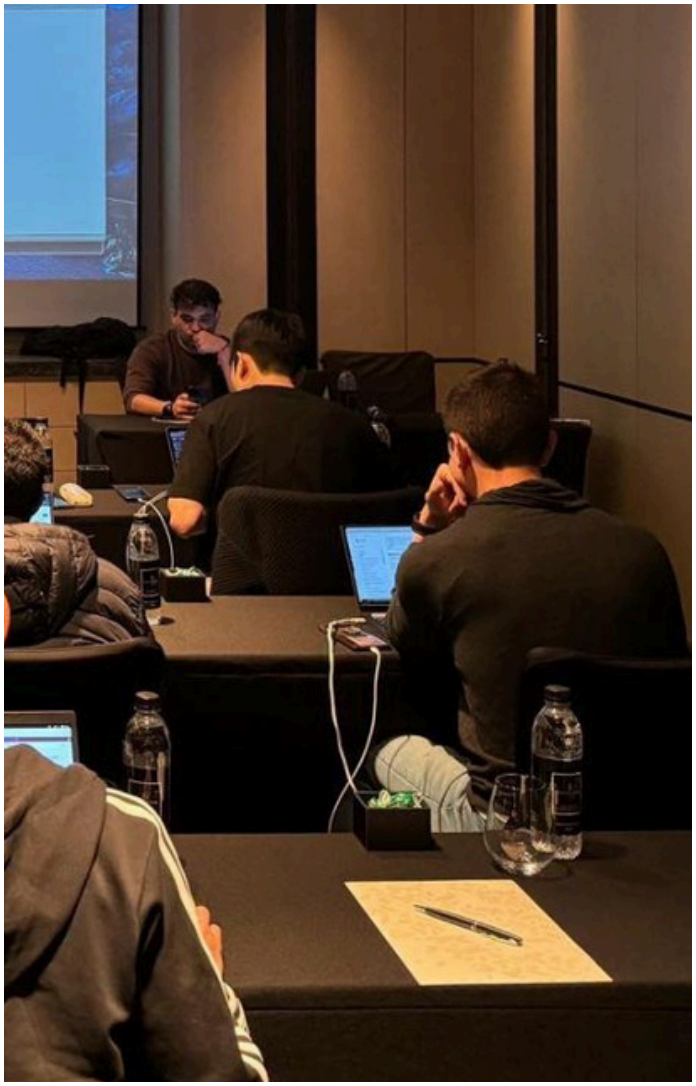
- Mobile Device Security Principles
- Android and iOS Internals
- Android and iOS Security Mitigations
- Mobile Forensics Fundamentals
- iOS Data Acquisition Techniques
- iOS Data Analysis Tools and Methods
- Advanced iOS Forensic Techniques
- Android Architecture and Security Features
- Android Data Extraction Methods
- Android App Analysis and Reverse Engineering
- Hands-On Practice with Practical Labs and Tools

WHO SHOULD ATTEND?

This course is for penetration testers, mobile developers or anyone keen to learn mobile application security.

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 follow along with the hands-on forensic exercises by the instructors. 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. 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.



PREREQUISITE KNOWLEDGE

- Working knowledge of cybersecurity and pentesting fundamentals
- Basic working knowledge of iOS and Android 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)
- Working knowledge of Forensic acquisition skills is recommended, but not required

WHAT WILL THE STUDENTS GET?

- Certificate of completion for the Training program
- Huge list of good reads and articles for learning mobile device forensics
- Source code for All 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 (Live On-site & Virtual Training only)
- Students will be provided access to cloud instances for the duration of the course (Live On-site & Virtual Training only)
- Slack access for the class and after for regular mobile security discussions (Live On-site & Virtual Training only)

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 (Live On-site & Virtual Training only)

8KSEC

COURSE SYLLABUS

Module 1: Introduction to Mobile Device Security

- Overview of mobile device security principles and challenges.
- Introduction to mobile forensics and its importance in digital investigations.

Module 2: iOS Forensics Fundamentals

- Evolution of mobile forensics and the new golden age for iOS forensics.
- Understanding the iOS operating system, filesystem structure, and security mechanisms.
- Challenges specific to iOS forensics and methods to overcome them.
- iOS Code Signing, Encryption, and Sandboxing
- The APFS Filesystem
- iOS Kernel Security Measures
- iOS daemons
- IPC Mechanisms in iOS
- Intro of the WebKit framework
- The libimobildevice framework
- Introduction to mvt (Mobile Verification Toolkit)
- iOS Keychain

Module 3: Data Acquisition from iOS Devices

- Understanding acquisition methods such as logical, physical, and filesystem acquisitions.
- Hands-on practice with tools like Cellebrite UFED, Elcomsoft iOS Forensic Toolkit, Bootrom exploits such as checkm8 (for legacy A11 and earlier devices / iPhone X and older), and modern acquisition methods including palera1n and agent-based techniques for filesystem acquisition on newer devices.
- Performing logical and filesystem acquisitions on iOS devices.
- Important files in an iOS device

Module 4: iOS Data Analysis and Tools

- Differences between encrypted and unencrypted backups
- Working with iOS backups
- Introduction to forensic tools like Cellebrite Physical Analyzer, Magnet AXIOM, Sumuri Recon, and iOS Triage, alongside open-source tools like Apollo, iLEAPP, ALEAPP, and RLEAPP.
- Analyzing iOS artifacts such as emails, messages, call logs, location data, and media files.
- Using custom scripts and tools for iOS data analysis and verification.

Module 5: Advanced iOS Forensic Techniques

- Exploring advanced topics in iOS forensics, including pattern-of-life forensics and connectivity data analysis.
- Introduction to the TAXII protocol for threat intelligence sharing in the mobile environment.
- Leveraging Custom IOCs for identifying threats specific to iOS devices.
- Forensic implications of iOS Lockdown Mode on acquisition and analysis workflows.
- Advanced Data Protection (ADP) for iCloud: end-to-end encryption impact on cloud acquisition, key management, and recovery options.
- Identifying Lockdown Mode and ADP status on a target device or account.

8KSEC

Module 6: Android Forensics and Security

- Understanding Android architecture, security features, and filesystem structure.
- Android forensic setup, pre-data extraction techniques, and data acquisition methods.
- Analyzing Android apps, malware, and reverse engineering techniques
- Android permission model, SELinux, Sandboxing
- IPC mechanisms in Android
- The Android Keystore

Module 7: Android Forensic Setup and Data Extraction Techniques

- Setting up a forensic environment for Android analysis and data extraction.
- Installing necessary software, Android platform tools, and creating virtual Android devices.
- Exploring various data extraction techniques including manual extraction, logical extraction, ADB pull extraction, and physical extraction.
- Hands-on practice with tools like SQLite Browser, ADB backup extraction, and Autopsy for analyzing and recovering Android data.

Module 8: Android App Analysis and Malware Detection

- Analyzing widely used Android apps such as Facebook, Telegram, WhatsApp and Google Chrome for retrieving data.
- Techniques for reverse engineering Android applications including extracting APK files, reverse engineering steps, and identifying Android malware.
- Understanding types of Android malware, how they spread, and techniques for malware detection and analysis.

Module 9: Mobile Verification and Security Assessment

- 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.

Module 10: Practical Labs and Case Studies

- Engaging in practical labs and case studies to apply learned concepts and techniques.
- Analyzing real-world scenarios, conducting investigations, and reporting findings.
- Developing skills in mobile device security, forensics, and incident response through hands-on exercises.

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
trainings@8ksec.io