Training Course on App Store Forensics and Malicious App Analysis

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 specialized training course is meticulously designed for digital forensic investigators, cybersecurity analysts, mobile security researchers, and incident response teams tasked with navigating the complex landscape of app store ecosystems and combating malicious mobile applications. With billions of apps available on platforms like Google Play Store and Apple App Store, and a growing threat of repackaged malware, adware, banking Trojans, and sophisticated spyware, the ability to effectively analyze these applications for forensic artifacts and malicious intent is paramount. Training Course on App Store Forensics and Malicious App Analysis provides the advanced knowledge and hands-on techniques required to extract, reverse engineer, and analyze digital evidence from mobile devices, cloud platforms, and application binaries, crucial for uncovering cybercrime, intellectual property theft, data breaches, and other security incidents.

The curriculum delves into the inner workings of both Android (APK) and iOS (IPA) application packages, exploring their file structures, code obfuscation techniques, and common persistence mechanisms. Through extensive practical labs, dynamic and static malware analysis, sandboxing, and mobile forensics tool utilization, participants will gain proficiency in identifying relevant data sources, extracting user activity logs, sensitive data (e.g., credentials, contacts), network communications, and obfuscated malicious code. The course also critically addresses the significant privacy implications of app data collection and the complex legal frameworks (including Kenya's Data Protection Act 2019) governing app store data acquisition and analysis, ensuring that all investigative practices are forensically sound, legally admissible, and ethically compliant, empowering investigators to combat the evolving threat of malicious mobile applications.

Programme Curriculum

Training Course on App Store Forensics and Malicious App Analysis

Introduction

This specialized training course is meticulously designed for digital forensic investigators, cybersecurity analysts, mobile security researchers, and incident response teams tasked with navigating the complex landscape of app store ecosystems and combating malicious mobile applications. With billions of apps available on platforms like Google Play Store and Apple App Store, and a growing threat of repackaged malware, adware, banking Trojans, and sophisticated spyware, the ability to effectively analyze these applications for forensic artifacts and malicious intent is paramount. Training Course on App Store Forensics and Malicious App Analysis provides the advanced knowledge and hands-on techniques required to extract, reverse engineer, and analyze digital evidence from mobile devices, cloud platforms, and application binaries, crucial for uncovering cybercrime, intellectual property theft, data breaches, and other security incidents.

The curriculum delves into the inner workings of both Android (APK) and iOS (IPA) application packages, exploring their file structures, code obfuscation techniques, and common persistence mechanisms. Through extensive practical labs, dynamic and static malware analysis, sandboxing, and mobile forensics tool utilization, participants will gain proficiency in identifying relevant data sources, extracting user activity logs, sensitive data (e.g., credentials, contacts), network communications, and obfuscated malicious code. The course also critically addresses the significant privacy implications of app data collection and the complex legal frameworks (including Kenya's Data Protection Act 2019) governing app store data acquisition and analysis, ensuring that all investigative practices are forensically sound, legally admissible, and ethically compliant, empowering investigators to combat the evolving threat of malicious mobile applications.

Course Duration

10 Days

Course Objectives

1. Understand the architecture and security models of major mobile app stores (Google Play, Apple App Store) and alternative distribution channels.
2. Identify diverse types of malicious mobile applications (e.g., adware, spyware, banking Trojans, ransomware, cryptominers) and their attack vectors.
3. Perform forensically sound data acquisition from mobile devices to extract app-related artifacts.
4. Conduct static analysis of mobile application packages (APKs, IPAs) to identify suspicious code, permissions, and manifest declarations.

5. Perform dynamic analysis of malicious applications using sandboxing environments and emulators to observe their real-time behavior.
6. Reverse engineer obfuscated Android (Dalvik bytecode) and iOS (Objective-C/Swift) applications to understand their functionality.
7. Extract and interpret application-specific data, including databases, preferences, cache files, and encrypted content.
8. Analyze network traffic generated by mobile applications to identify command-and-control (C2) communications or data exfiltration.
9. Identify indicators of compromise (IOCs) and unique signatures of known and unknown malicious mobile apps.
10. Reconstruct user activity timelines related to app installation, usage, and suspicious interactions.
11. Navigate data privacy regulations and legal considerations (e.g., Kenya's Data Protection Act 2019) pertaining to mobile app data.
12. Utilize specialized mobile forensic tools, disassemblers, and decompilers for malicious app analysis.
13. Generate comprehensive forensic reports detailing malicious app analysis findings for legal or incident response purposes.

Organizational Benefits

1. Proactive Threat Detection: Identify and analyze emerging malicious mobile applications before they cause significant damage.
2. Enhanced Incident Response: Accelerate the investigation and containment of mobile malware incidents.
3. Improved Mobile Security Posture: Understand the attack surface of mobile applications to strengthen organizational defenses.
4. Reduced Financial & Reputational Risk: Minimize losses from data breaches, fraud, and intellectual property theft via malicious apps.
5. Strengthened Compliance: Ensure data handling during investigations adheres to privacy laws (e.g., Kenya Data Protection Act).
6. In-House Expertise: Develop a specialized team capable of advanced mobile application threat intelligence and forensics.
7. Better Vendor Risk Management: Assess the security posture of third-party mobile applications used within the organization.
8. Actionable Intelligence: Provide valuable insights to development and security teams for building more secure applications.
9. Robust Litigation Support: Produce admissible evidence for cases involving mobile app-related cybercrime or intellectual property infringement.

10. Protection of User Data: Safeguard sensitive personal and organizational data from malicious app exploitation.

Target Participants

- Digital Forensic Investigators
- Mobile Security Analysts
- Malware Analysts / Reverse Engineers
- Cybersecurity Incident Responders
- Mobile Application Developers (with a security interest)
- Penetration Testers (Mobile Focus)
- Law Enforcement (Cybercrime Units)
- Fraud Examiners (Mobile Payments Focus)
- Quality Assurance / QA Engineers (Security Testing)
- Product Security Teams

Course Outline

Module 1: Mobile App Ecosystems & Threat Landscape (App Store Basics & Threats)

- Overview of Mobile App Stores (Google Play, Apple App Store, Third-Party)
- Mobile Application Distribution and Installation Mechanisms
- Overview of Mobile Malware Types (Adware, Spyware, Ransomware, Trojans, Backdoors)
- Recent Trends in Malicious Apps and App Store Vulnerabilities
- **Case Study**: Analyzing a recent Android banking Trojan campaign distributed via a third-party app store.

Module 2: Mobile Device Data Acquisition for App Forensics (Mobile Device Data)

- Logical Acquisition for App Data (ADB, iTunes Backups, iOS File System Dump)
- Physical Acquisition for Deeper App Data (JTAG, Chip-Off, ISP)
- Cloud Data Acquisition (Google Drive Backups, iCloud) relevant to apps
- Preserving Device State and App Data Integrity
- **Case Study**: Acquiring a full file system dump from an Android device suspected of running a malicious app.

Module 3: Android Application Package (APK) Analysis (Android App Analysis)

- APK File Structure: `AndroidManifest.xml`, DEX files, Resources, Libraries
- Decompiling DEX to Smali/Java (e.g., Jadx, Apktool)
- Analyzing `AndroidManifest.xml` for Permissions, Services, and Activities
- Identifying Key Entry Points and Components
- **Case Study**: Decompiling a suspicious APK to examine its manifest file for excessive permissions.

Module 4: iOS Application Package (IPA) Analysis (iOS App Analysis)

- IPA File Structure: Executable, Info.plist, Resources, Frameworks
- Decrypting Encrypted iOS Applications
- Analyzing `Info.plist` for Permissions and Capabilities
- Understanding Code Signing and Sandboxing in iOS
- **Case Study**: Analyzing an IPA file to identify its entitlements and capabilities.

Module 5: Static Malware Analysis Techniques (Static Analysis)

- Code Review for Malicious Patterns and Obfuscation
- String Analysis for URLs, APIs, and Sensitive Keywords
- Permission Analysis and Anomaly Detection
- Use of Static Analysis Tools (e.g., Androguard, MobSF, Frida)
- **Case Study**: Using a static analysis tool to find suspicious API calls in an Android app's code.

Module 6: Dynamic Malware Analysis & Sandboxing (Dynamic Analysis)

- Setting up Android Emulators and iOS Simulators for Analysis
- Using Mobile Sandboxes (e.g., Anubis, AnyRun, custom setups)
- Monitoring File System Changes, Registry Access, and Process Activity
- Network Traffic Capture and Analysis during App Execution
- **Case Study**: Running a suspected spyware app in a sandbox to observe its data exfiltration attempts.

Module 7: Reverse Engineering Mobile Application Code (Code Reverse Engineering)

- Introduction to Dalvik Bytecode and ARM Assembly
- Using Disassemblers/Decompilers (Ghidra, IDA Pro) for Android and iOS
- Identifying Anti-Analysis Techniques (Anti-debugging, Anti-emulation, Code Packing)
- Bypassing Simple Obfuscation Techniques
- **Case Study**: Reversing a small malicious function within an Android application to understand its purpose.

Module 8: Data Storage Forensics (App Data Storage)

- Analyzing SQLite Databases within Mobile Applications
- Extracting and Interpreting Shared Preferences, Plist Files, and XML Data
- Recovering Deleted Application Data
- Understanding Secure Storage Mechanisms (Keystores, Secure Enclave)
- **Case Study**: Extracting and analyzing a SQLite database from a messaging app to recover chat history.

Module 9: Network Communication Analysis (Network Artifacts)

- Capturing and Analyzing Network Traffic (Wireshark, Burp Suite) from Mobile Devices
- Identifying Command-and-Control (C2) Traffic and Data Exfiltration Channels
- Decrypting HTTPS Traffic from Mobile Apps (SSL Pinning Bypass)
- Analyzing DNS Queries and IP Connections
- **Case Study**: Intercepting and analyzing encrypted traffic from a banking Trojan to its C2 server.

Module 10: User Activity & Timeline Reconstruction (User Activity Forensics)

- Correlating App Usage Logs with Device Timestamps
- Reconstructing User Interactions within Applications
- Identifying App Installation and Uninstallation Events
- Tracing App Downloads from Official and Third-Party Sources

- **Case Study**: Building a timeline of a user's interaction with a fraudulent app, from download to suspicious activity.

Module 11: Malicious App Persistence Mechanisms (App Persistence)

- Understanding Rootkits and Bootkits in Mobile Environments
- Analyzing Auto-Start Mechanisms, Background Services, and Broadcast Receivers
- Detecting Code Injection and Hooking Techniques
- Identifying Privileged Access and Exploits
- **Case Study**: Identifying how a malicious app maintains persistence on a rooted Android device.

Module 12: Mobile Payment App Forensics (Payment App Focus)

- Analyzing Mobile Payment Application-Specific Data (Transaction Logs, Receipts)
- Investigating In-App Purchase Fraud and Payment Card Skimming
- Identifying Indicators of Banking Trojans and Financial Malware
- Tracing Fund Transfers via Mobile Wallets
- **Case Study**: Forensic analysis of an Android banking app to find evidence of credential theft.

Module 13: App Store Policy & Review Process (App Store Security)

- Understanding App Store Submission Guidelines and Review Processes
- How Malicious Apps Bypass App Store Protections
- Reporting Malicious Apps and Collaboration with App Stores
- The Role of Automated Scans and Human Review
- **Case Study**: Analyzing a case where a malicious app successfully infiltrated an official app store.

Module 14: Legal, Ethical & Reporting (Legal & Reporting)

- Legal Frameworks for Mobile App Investigations (Search Warrants, Subpoenas)
- Data Privacy Laws in Kenya (**Kenya Data Protection Act 2019**) and their Impact on App Forensics
- Chain of Custody for Mobile App Evidence

- Crafting Comprehensive Forensic Reports for Law Enforcement and Legal Proceedings
- **Case Study**: Discussing the legal implications of analyzing user data from a malicious app, ensuring compliance with Kenyan privacy laws.

Module 15: Emerging Threats & Future of App Forensics (Future Trends)

- AI/ML in Mobile Malware and Anti-Forensics
- Forensics of Decentralized Apps (dApps) and Blockchain-based Apps
- Analysis of Mobile IoT Apps and Wearable App Forensics
- Automated Malicious App Detection and Analysis Platforms
- **Case Study**: Exploring the challenges of analyzing a malicious decentralized application.

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 practi

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

Start Date	End Date	Location	Price
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