Training Course on Mobile Application Forensics and Data 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 comprehensive training course provides digital forensic professionals with the advanced skills and methodologies required for mobile application forensics and in-depth data analysis. Participants will learn to navigate the intricate landscape of both Android and iOS application ecosystems, focusing on extracting, parsing, and interpreting critical digital evidence embedded within these applications. The curriculum covers a wide array of app types, from messaging apps and social media platforms to financial applications and cloud-synced data, equipping investigators to uncover hidden user activities, communications, and data trails for cybercrime investigations and incident response.

Training Course on Mobile Application Forensics and Data Analysis emphasizes hands-on practical exercises and real-world case studies, enabling participants to master techniques for bypassing app-specific encryption, recovering deleted application data, analyzing SQLite databases, and utilizing both commercial and open-source forensic tools. With the exponential growth of mobile app usage and the increasing complexity of app data storage, this course is crucial for anyone involved in digital investigations, e-discovery, or mobile security. Graduates will be proficient in artifact correlation, timeline reconstruction, and presenting forensically sound findings derived from challenging mobile application data.

Programme Curriculum

Training Course on Mobile Application Forensics and Data Analysis

Introduction

This comprehensive training course provides digital forensic professionals with the advanced skills and methodologies required for mobile application forensics and in-depth data analysis. Participants will learn to navigate the intricate landscape of both Android and iOS application ecosystems, focusing on extracting, parsing, and interpreting critical digital evidence embedded within these applications. The curriculum covers a wide array of app types, from messaging apps and social media platforms to financial applications and cloud-synced data, equipping investigators to uncover hidden user activities, communications, and data trails for cybercrime investigations and incident response.

Training Course on Mobile Application Forensics and Data Analysis emphasizes hands-on practical exercises and real-world case studies, enabling participants to master techniques for bypassing app-specific encryption, recovering deleted application data, analyzing SQLite databases, and utilizing both commercial and open-source forensic tools. With the exponential growth of mobile app usage and the increasing complexity of app data storage, this course is crucial for anyone involved in digital investigations, e-discovery, or mobile security. Graduates will be proficient in artifact correlation, timeline reconstruction, and presenting forensically sound findings derived from challenging mobile application data.

Course Duration

10 Days

Course Objectives

1. Master advanced data acquisition techniques specific to mobile applications, including logical and file system extractions of app data.
2. Perform in-depth SQLite database forensics for mobile applications, including recovery of deleted records and journal analysis.
3. Analyze and interpret application-specific artifacts from popular messaging, social media, and productivity apps on both Android and iOS.
4. Effectively bypass app-level encryption and obfuscation techniques to access hidden or protected data.
5. Conduct mobile app malware analysis to identify malicious behaviors and data exfiltration attempts.
6. Recover and reconstruct deleted application data using advanced carving and data recovery methodologies.

7. Investigate cloud-synced application data, understanding acquisition methods and jurisdictional challenges.
8. Develop custom scripts (Python) for automated parsing and analysis of unique or complex mobile app data structures.
9. Reconstruct user timelines and activity patterns by correlating data from multiple mobile applications.
10. Understand app-specific storage mechanisms and their implications for forensic analysis (e.g., SharedPreferences, Plist files, Realm databases).
11. Generate forensically sound reports detailing findings from mobile application data analysis for legal proceedings.
12. Adapt investigative strategies to keep pace with rapid mobile app updates and evolving data formats.
13. Apply digital evidence preservation best practices specifically for mobile application data.

Organizational Benefits

1. Enhanced Investigative Depth: Uncover deeper insights and hidden evidence from mobile applications, leading to more successful investigations.
2. Improved Data Recovery Rates: Increase the ability to recover critical data from complex and often encrypted mobile app environments.
3. Reduced Investigation Costs: Equip internal teams with specialized skills, minimizing reliance on expensive external forensic services.
4. Strengthened Incident Response: Enable faster and more effective response to cyber incidents involving mobile application data breaches or misuse.
5. Better Compliance & Risk Management: Proactively identify and address potential data privacy violations or regulatory non-compliance related to mobile app data.
6. Optimized Resource Allocation: Efficiently utilize forensic tools and personnel by focusing on high-value mobile app data.
7. Evidence Admissibility: Ensure that mobile app data is collected, analyzed, and presented in a forensically sound manner suitable for legal contexts.
8. Proactive Threat Intelligence: Extract valuable threat intelligence from mobile app malware or exploited vulnerabilities.
9. Increased Employee Proficiency: Foster a highly skilled and adaptable digital forensics team capable of handling modern mobile challenges.
10. Protection of Intellectual Property: Safeguard sensitive company data potentially stored or exfiltrated via mobile business applications.

Target Participants

- Digital Forensic Examiners
- Cybersecurity Analysts
- Incident Response Team Members

- Law Enforcement Investigators
- e-Discovery Professionals
- Internal Auditors and Corporate Investigators
- Mobile Security Specialists
- Malware Analysts
- Network Security Engineers (with forensic interest)
- Legal Professionals (involved in digital evidence)

Course Outline

Module 1: Introduction to Mobile Application Forensics (App Forensics Fundamentals)

- Overview of Mobile Operating Systems (Android & iOS) relevant to apps
- Mobile Application Architecture and Data Storage Principles
- Legal & Ethical Considerations in Mobile App Investigations
- Understanding App Sandboxing and Permissions
- **Case Study**: Initial assessment of an unknown application's data footprint.

Module 2: Android Application Data Acquisition (Android App Data Extraction)

- Methods for Acquiring Android Application Data (Logical, File System, Physical)
- Accessing Rooted vs. Non-Rooted Device App Data
- Utilizing ADB Commands for App-Specific Data Pulls
- Commercial Tools vs. Open-Source Approaches for Android Apps
- **Case Study**: Extracting data from a common Android social media app.

Module 3: iOS Application Data Acquisition (iOS App Data Extraction)

- Methods for Acquiring iOS Application Data (Logical, File System, Full Dumps)
- Accessing Jailbroken vs. Non-Jailbroken Device App Data
- Leveraging iTunes/Finder Backups for App Data
- Commercial Tools and Checkm8-based Exploits for iOS Apps
- **Case Study**: Acquiring data from an iOS messaging application.

Module 4: SQLite Database Forensics for Apps (App Database Forensics)

- In-depth Structure of SQLite Databases in Mobile Apps
- Recovering Deleted Records and Tracing WAL (Write-Ahead Logging) Files
- Interpreting SQLite Journal Files for Transaction History
- Advanced SQL Queries for Targeted Data Extraction from Apps
- **Case Study**: Reconstructing deleted chat messages from a mobile banking app.

Module 5: Common Application Artifacts Analysis (Popular App Artifacts)

- Analysis of Messaging App Artifacts (WhatsApp, Telegram, Signal, iMessage)
- Forensic Examination of Social Media App Data (Facebook, Instagram, TikTok)
- Understanding Browser App Forensics (Chrome, Safari, Firefox Mobile)
- Extracting Data from Email Clients and Productivity Apps
- **Case Study**: Correlating user activity across multiple communication apps.

Module 6: Cloud-Synced Application Data (Cloud App Forensics)

- Investigating Cloud Backups and Synchronized App Data (Google Drive, iCloud)
- Challenges of Cloud Data Acquisition: Legal, Technical, and Jurisdictional
- Identifying App-Specific Cloud Storage and Associated Metadata
- Best Practices for Preserving Cloud-Based App Evidence
- **Case Study**: Tracing synced notes and documents from a cloud-enabled productivity app.

Module 7: Advanced Application Data Parsing (App Data Parsing Techniques)

- Understanding and Parsing Plist Files (iOS), SharedPreferences (Android), and XML files
- Analyzing JSON and Protobuf Structures within App Data
- Techniques for Dealing with Obfuscated or Encrypted App Data
- Custom Parsers and Data Transformation for Complex Structures
- **Case Study**: Developing a custom parser for a niche mobile game's data.

Module 8: Mobile Application Malware Analysis (App Malware Forensics)

- Identifying Signs of Malicious Mobile Applications
- Static and Dynamic Analysis of Android APKs and iOS IPAs
- Detecting Data Exfiltration and Command & Control (C2) Communication
- Understanding Mobile Rootkits and Ransomware Affecting Apps
- **Case Study**: Analyzing a suspected malicious banking app for suspicious behavior.

Module 9: App-Specific Encryption & Decryption (App Encryption Forensics)

- Overview of App-Level Encryption Implementations
- Techniques for Bypassing or Decrypting App-Specific Protections
- Utilizing Device Keychains and Secure Enclaves for Data Access
- Dealing with Secure Messaging App Encryption Challenges
- **Case Study**: Attempting to decrypt protected data from a secure communication app.

Module 10: Digital Wallets & Financial App Forensics (Financial App Forensics)

- Investigating Mobile Payment Apps (Apple Pay, Google Pay, M-Pesa)
- Analyzing Cryptocurrency Wallet Applications and Transaction Traces
- Extracting Data from Banking Apps and Financial Service Providers
- Understanding Security Features and Forensic Limitations of Financial Apps
- **Case Study**: Tracing transactions through a mobile payment application.

Module 11: Gaming & Entertainment App Forensics (Gaming App Forensics)

- Extracting User Data from Mobile Gaming Applications
- Analyzing In-App Purchases, Achievements, and Game State Data
- Investigating Cheating and Fraud within Mobile Games
- Understanding Data Storage in Online Multiplayer Games
- **Case Study**: Analyzing game data to prove a user's activity in an online game.

Module 12: Location-Based & IoT App Forensics (Location App Forensics)

- Extracting and Interpreting Location Data from Mapping and Ride-Sharing Apps
- Analyzing Data from Smart Home and IoT Device Control Apps
- Correlating App-Generated Location Data with System Logs
- Privacy Concerns and Legal Implications of Location Data
- **Case Study**: Using a ride-sharing app's data to trace a suspect's route.

Module 13: Timeline Reconstruction & Data Correlation (Timeline Analysis Mobile Apps)

- Building Comprehensive User Timelines from Multiple App Artifacts
- Correlating Data Across Different Mobile Devices and Accounts
- Identifying Gaps and Inconsistencies in App-Generated Data
- Tools and Methodologies for Visualizing Correlated App Data
- **Case Study**: Reconstructing a full day's activities based on multiple mobile app logs.

Module 14: Automated Analysis & Scripting (Automated App Forensics)

- Introduction to Forensic Automation for Mobile Applications
- Developing Python Scripts for Recurring App Data Parsing Tasks
- Integrating Custom Scripts with Commercial Forensic Platforms
- Leveraging Open-Source Libraries for Efficient App Data Processing
- **Case Study**: Automating the extraction of specific data from a frequently updated app.

Module 15: Reporting & Presenting App Forensic Findings (App Forensic Reporting)

- Best Practices for Documenting Mobile Application Forensic Examinations
- Crafting Clear and Concise Reports for Technical and Non-Technical Audiences
- Admissibility of Mobile App Data as Digital Evidence
- Preparing for and Delivering Expert Witness Testimony on App Forensics
- **Case Study**: Creating a comprehensive forensic report for a mobile app-related incident.

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.
- Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 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