Training Course on Advanced Android Device Forensics and Data Extraction

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 intensive training course delves into the cutting-edge methodologies and advanced techniques for Android mobile forensics and digital evidence extraction. Participants will gain unparalleled expertise in navigating the complexities of modern Android operating systems, bypassing security mechanisms, and performing deep-dive data recovery from a wide array of devices, including locked and encrypted smartphones. Through hands-on labs and real-world case studies, this program equips digital forensic professionals with the skills to effectively investigate cybercrime, conduct incident response, and present court-admissible evidence from Android devices.

Training Course on Advanced Android Device Forensics and Data Extraction focuses on unearthing hidden and deleted data, analyzing intricate app artifacts, understanding file system nuances, and leveraging both commercial and open-source forensic tools. With the rapid evolution of Android security and new challenges like mobile malware analysis and cloud-synced data, this course provides the critical knowledge and practical experience necessary to stay ahead in the dynamic field of digital investigations. Graduates will be proficient in advanced data carving, SQLite database analysis, and developing custom scripts for automated artifact recovery, empowering them to tackle even the most challenging mobile forensic scenarios.

Programme Curriculum

Training Course on Advanced Android Device Forensics and Data Extraction

Introduction

This intensive training course delves into the cutting-edge methodologies and advanced techniques for Android mobile forensics and digital evidence extraction. Participants will gain unparalleled expertise in navigating the complexities of modern Android operating systems, bypassing security mechanisms, and performing deep-dive data recovery from a wide array of devices, including locked and encrypted smartphones. Through hands-on labs and real-world case studies, this program equips digital forensic professionals with the skills to effectively investigate cybercrime, conduct incident response, and present court-admissible evidence from Android devices.

Training Course on Advanced Android Device Forensics and Data Extraction focuses on unearthing hidden and deleted data, analyzing intricate app artifacts, understanding file system nuances, and leveraging both commercial and open-source forensic tools. With the rapid evolution of Android security and new challenges like mobile malware analysis and cloud-synced data, this course provides the critical knowledge and practical experience necessary to stay ahead in the dynamic field of digital investigations. Graduates will be proficient in advanced data carving, SQLite database analysis, and developing custom scripts for automated artifact recovery, empowering them to tackle even the most challenging mobile forensic scenarios.

Course Duration

10 Days

Course Objectives

1. Master advanced data acquisition techniques for diverse Android devices, including physical and logical extractions from locked and encrypted phones.
2. Perform in-depth Android file system analysis, identifying critical artifacts within YAFFS2, F2FS, and other modern file systems.
3. Utilize cutting-edge forensic tools and methodologies for comprehensive app artifact analysis and database parsing.
4. Effectively bypass Android screen locks and encryption mechanisms to access critical digital evidence.
5. Conduct mobile malware analysis on Android devices, identifying malicious applications, their behaviors, and network communications.
6. Recover and reconstruct deleted and hidden data from Android devices using advanced data carving and SQLite forensic analysis.
7. Analyze cloud-synced data and its forensic implications for Android user activity and evidence correlation.

8. Develop Python scripting skills for automating forensic tasks and extracting unparsed data from complex Android artifacts.
9. Understand and apply anti-forensics detection techniques used by perpetrators on Android platforms.
10. Generate forensically sound reports and present expert testimony based on robust Android digital evidence.
11. Investigate location-based services and geolocation data from Android devices for timeline reconstruction.
12. Adapt forensic strategies to keep pace with Android OS updates and emerging security features.
13. Implement chain of custody principles and best practices for preserving the integrity of Android digital evidence.

Organizational Benefits

1. Enhanced Incident Response Capabilities: Rapidly respond to and investigate cyber incidents involving Android devices, minimizing breach impact.
2. Improved Evidence Collection & Admissibility: Ensure proper collection, preservation, and analysis of Android data, leading to stronger, court-admissible evidence.
3. Reduced Investigation Timelines: Equip teams with advanced techniques and tools to expedite complex Android forensics cases.
4. Mitigated Legal and Financial Risks: Proactively identify and address potential data breaches and intellectual property theft originating from mobile devices.
5. Strengthened Cybersecurity Posture: Gain insights into Android vulnerabilities and attack vectors to enhance overall organizational security.
6. Optimized Resource Utilization: Maximize the effectiveness of existing forensic tools and personnel through advanced skill development.
7. Increased Investigative Success Rates: Improve the ability to uncover critical evidence from even the most challenging Android devices.
8. Compliance with Regulatory Standards: Ensure forensic practices align with legal and industry compliance requirements.
9. Professional Development & Retention: Invest in employee skills, fostering a highly competent and motivated digital forensics team.
10. Proactive Threat Intelligence: Leverage forensic findings from Android devices to develop better proactive threat detection strategies.

Target Participants

- Digital Forensic Examiners
- Law Enforcement Professionals
- Cybersecurity Analysts

- Incident Response Team Members
- IT Security Professionals
- e-Discovery Specialists
- Military and Intelligence Personnel
- Corporate Investigators
- Legal Professionals (involved in digital evidence)
- Security Consultants

Course Outline

Module 1: Foundations of Advanced Android Forensics (Introduction to Android Forensics)

- Understanding Android Architecture & Security Model
- The Android Boot Process & Storage Mechanisms
- Legal & Ethical Considerations in Mobile Device Forensics
- Forensic Readiness & Incident Preparation for Android Devices
- **Case Study**: Analyzing a basic Android data breach scenario.

Module 2: Advanced Android Data Acquisition Techniques (Android Data Extraction)

- Logical vs. Physical Acquisition: Pros, Cons, and Advanced Scenarios
- Bypassing Screen Locks and Encryption on Newer Android Versions
- JTAG, Chip-Off, and ISP Techniques: When and How to Apply
- Advanced Tool Integration: Cellebrite, Magnet AXIOM, Oxygen Forensics
- **Case Study**: Acquiring data from a modern, locked Android smartphone.

Module 3: Android File System Deep Dive (Android File System Analysis)

- In-depth Analysis of EXT4, F2FS, and YAFFS2 File Systems
- Carving Deleted Files and Unallocated Space on Android Devices
- Understanding Android Partitions: System, Data, Cache, Recovery
- Analyzing Metadata within Android File Systems
- **Case Study**: Recovering deleted images and documents from a formatted Android partition.

Module 4: SQLite Database Forensics on Android (Android Database Forensics)

- Advanced SQLite Analysis for Android Applications
- Recovering Deleted and Orphaned Records from SQLite Databases
- Interpreting WAL (Write-Ahead Logging) Files for Forensic Insights
- Developing Custom SQL Queries for Complex Data Extraction
- **Case Study**: Reconstructing chat conversations from a messaging app's SQLite database.

Module 5: App Artifact Analysis & Reverse Engineering (Android App Forensics)

- Deconstructing Android Applications (APKs) for Forensic Analysis
- Identifying and Analyzing App-Specific Data Structures
- Extracting Data from Obfuscated and Encrypted App Containers
- Understanding App Permissions and Their Forensic Significance
- **Case Study**: Investigating data traces from a cryptocurrency trading app.

Module 6: Mobile Malware Analysis & Reverse Engineering (Android Malware Forensics)

- Identifying Android Malware Signatures and Behaviors
- Static and Dynamic Malware Analysis Techniques
- Decompiling Android Applications for Code Review
- Analyzing Malware Persistence Mechanisms and Command & Control (C2) Communications
- **Case Study**: Dissecting a ransomware sample found on an Android device.

Module 7: Cloud-Based Data & Android Forensics (Cloud Forensics Android)

- Investigating Cloud Backups and Synchronized Data (Google Drive, WhatsApp Cloud)
- Legal Challenges and International Cooperation in Cloud Forensics
- Extracting and Analyzing Data from Cloud Provider Accounts (if legally permissible)
- Understanding the Interplay between On-Device and Cloud Data
- **Case Study**: Tracing user activity across multiple Android devices via cloud synchronization.

Module 8: Network Forensics on Android Devices (Android Network Forensics)

- Analyzing Wi-Fi, Bluetooth, and Cellular Network Connections
- Extracting and Interpreting Network Traffic Logs
- Identifying VPN usage and Tor connections on Android
- Examining Browser History, Downloads, and Web Artifacts
- **Case Study**: Reconstructing a user's web Browse activity and identifying suspicious connections.

Module 9: Location Forensics & Geolocation Data (Android Geolocation Forensics)

- Extracting and Analyzing GPS Data, Cell Tower Locations, and Wi-Fi Hotspots
- Understanding Google Location History and its Forensic Value
- Mapping Location Data for Timeline Reconstruction
- Tools and Techniques for Geolocation Visualization
- **Case Study**: Proving presence at a specific location using Android device data.

Module 10: Advanced Data Carving & File Recovery (Android Data Recovery)

- Deep Dive into Signature-Based and Header-Footer Carving
- Reconstructing Fragmented Files and Data Streams
- Customizing Carving Signatures for New File Types
- Validating Carved Data for Forensic Integrity
- **Case Study**: Recovering critical fragmented video evidence from unallocated space.

Module 11: Anti-Forensics & Countermeasures (Android Anti-Forensics)

- Identifying Data Wiping, Encryption, and Steganography Techniques
- Detecting Rooting, Custom ROMs, and Tampering Attempts
- Analyzing Secure Folders and Private Spaces on Android
- Strategies for Bypassing Anti-Forensic Measures
- **Case Study**: Uncovering attempts to conceal evidence on an Android device.

Module 12: Scripting for Android Forensics (Python Forensics Android)

- Introduction to Python for Forensic Automation
- Developing Scripts for Parsing Custom Artifacts
- Automating Data Extraction and Report Generation
- Leveraging Open-Source Python Libraries for Forensics
- **Case Study**: Writing a Python script to extract specific data from an unusual app.

Module 13: Report Writing & Expert Testimony (Forensic Reporting Android)

- Structuring Comprehensive and Defensible Forensic Reports
- Presenting Technical Findings to Non-Technical Audiences
- Admissibility of Digital Evidence in Legal Proceedings
- Preparing for and Delivering Expert Witness Testimony
- **Case Study**: Drafting a mock forensic report for a complex Android investigation.

Module 14: Emerging Trends & Future Challenges (Future of Android Forensics)

- IoT Device Integration and its Impact on Android Forensics
- AI/ML in Digital Forensics: Opportunities and Challenges
- Privacy Enhancing Technologies (PETs) and Their Forensic Implications
- Forensic Challenges of Foldable Phones and Wearable Devices
- **Case Study**: Discussing the forensic implications of a hypothetical smart home device linked to an Android phone.

Module 15: Practical Capstone Project (Android Forensics Capstone)

- Simulated Real-World Android Forensic Investigation
- Applying All Learned Techniques to a Complex Scenario
- Team-Based Problem Solving and Collaboration
- Presentation of Findings and Recommendations

- **Case Study**: A full-scale, multi-device Android investigation from seizure to reporting.

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.
- Expert-led Q&A sessio

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