Training Course on Bypassing Mobile Device Locks for Forensic Access

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 is specifically designed for digital forensic investigators, law enforcement professionals, and cybersecurity experts who require forensic access to locked mobile devices. In today's digital landscape, modern smartphones and tablets are increasingly secured with complex passcodes, patterns, biometric locks, and full-disk encryption, often rendering traditional logical acquisitions insufficient. Training Course on Bypassing Mobile Device Locks for Forensic Access provides cutting-edge knowledge and hands-on techniques to overcome these sophisticated security measures, enabling the acquisition, preservation, and analysis of critical digital evidence from devices that would otherwise remain inaccessible.

The curriculum covers a comprehensive range of lock bypass methodologies for both iOS and Android platforms, including bootloader exploits, hardware-based attacks (e.g., Chip-Off, ISP, JTAG), software vulnerabilities, and advanced logical bypasses. Participants will gain practical experience with industry-standard forensic tools and specialized hardware, learning to navigate the intricate security architectures, encryption mechanisms, and anti-forensic techniques employed by device manufacturers. Emphasizing forensically sound procedures and strict adherence to legal and ethical guidelines (including Kenya's Data Protection Act), this course ensures that all acquired evidence is admissible in court, empowering investigators to unlock the full potential of mobile devices as sources of intelligence in cybercrime investigations, internal security breaches, and complex litigation.

Programme Curriculum

Training Course on Bypassing Mobile Device Locks for Forensic Access

Introduction

This intensive training course is specifically designed for digital forensic investigators, law enforcement professionals, and cybersecurity experts who require forensic access to locked mobile devices. In today's digital landscape, modern smartphones and tablets are increasingly secured with complex passcodes, patterns, biometric locks, and full-disk encryption, often rendering traditional logical acquisitions insufficient. Training Course on Bypassing Mobile Device Locks for Forensic Access provides cutting-edge knowledge and hands-on techniques to overcome these sophisticated security measures, enabling the acquisition, preservation, and analysis of critical digital evidence from devices that would otherwise remain inaccessible.

The curriculum covers a comprehensive range of lock bypass methodologies for both iOS and Android platforms, including bootloader exploits, hardware-based attacks (e.g., Chip-Off, ISP, JTAG), software vulnerabilities, and advanced logical bypasses. Participants will gain practical experience with industry-standard forensic tools and specialized hardware, learning to navigate the intricate security architectures, encryption mechanisms, and anti-forensic techniques employed by device manufacturers. Emphasizing forensically sound procedures and strict adherence to legal and ethical guidelines (including Kenya's Data Protection Act), this course ensures that all acquired evidence is admissible in court, empowering investigators to unlock the full potential of mobile devices as sources of intelligence in cybercrime investigations, internal security breaches, and complex litigation.

Course Duration

10 Days

Course Objectives

1. Identify and understand various mobile device lock mechanisms (PIN, Pattern, Password, Biometric, Full-Disk Encryption).
2. Perform forensically sound acquisition from locked iOS and Android devices, distinguishing between Before First Unlock (BFU) and After First Unlock (AFU) states.
3. Utilize bootloader exploitation techniques to bypass device locks and gain forensic access.
4. Execute hardware-based data extraction methods such as Chip-Off, In-System Programming (ISP), and JTAG for locked or damaged devices.
5. Leverage known software vulnerabilities and exploits to achieve logical bypasses for specific OS versions.
6. Understand and overcome File-Based Encryption (FBE) and Full-Disk Encryption (FDE) on locked devices.
7. Employ physical extraction techniques to bypass lock screens and recover encrypted data.

8. Analyze the security architecture of both iOS (Secure Enclave) and Android (TrustZone, Keymaster) in relation to lock bypass.
9. Apply ethical hacking methodologies in a controlled forensic environment to simulate real-world bypass scenarios.
10. Navigate the legal and ethical implications of bypassing mobile device locks, ensuring compliance with Kenya's Data Protection Act.
11. Utilize commercial and open-source forensic tools specialized in lock bypass and data decryption.
12. Develop custom scripts (Python) for automating aspects of lock bypass or data decryption.
13. Generate comprehensive forensic reports detailing lock bypass procedures and the integrity of acquired evidence.

Organizational Benefits

1. Unprecedented Access to Evidence: Recover critical data from previously inaccessible locked mobile devices.
2. Enhanced Investigative Success: Drastically increase the likelihood of solving complex cases by unlocking vital digital clues.
3. Faster Incident Response: Reduce investigation timelines by efficiently bypassing device locks and acquiring data.
4. Reduced Reliance on External Services: Build in-house expertise for specialized mobile device unlocking, saving significant costs.
5. Proactive Threat Mitigation: Understand mobile device vulnerabilities to better secure organizational assets.
6. Improved Evidence Admissibility: Ensure all lock bypass procedures are forensically sound and legally compliant.
7. Increased Efficiency: Optimize the use of forensic tools and resources by understanding their advanced capabilities.
8. Competitive Advantage: Position the organization at the forefront of advanced mobile forensics.
9. Compliance Assurance: Train personnel on the latest legal guidelines for accessing locked data, including local regulations in Kenya.
10. Expertise Development: Cultivate highly skilled forensic specialists capable of tackling the most challenging mobile investigations.

Target Participants

- Digital Forensic Examiners
- Law Enforcement Cybercrime Investigators
- Corporate Security Investigators
- Cybersecurity Incident Responders
- Military and Government Intelligence Analysts

- Mobile Phone Reverse Engineers
- e-Discovery Specialists
- Penetration Testers (with a forensic interest)
- Legal Professionals (prosecutors, defense attorneys)
- Mobile Device Repair Technicians (seeking forensic specialization)

Course Outline

Module 1: Mobile Device Lock Mechanisms & Fundamentals (Mobile Lock Overview)

- Types of Mobile Device Locks: PIN, Pattern, Password, Biometric (Fingerprint, Face ID)
- Understanding Full-Disk Encryption (FDE) and File-Based Encryption (FBE)
- Device States: Before First Unlock (BFU) vs. After First Unlock (AFU)
- Introduction to Mobile Device Security Architectures (Secure Enclave, Keymaster, TrustZone)
- **Case Study**: Analyzing the lock screen behavior of a modern Android device.

Module 2: Legal & Ethical Considerations for Lock Bypass (Legal & Ethical Bypass)

- Legal Frameworks for Mobile Device Access (Search Warrants, Court Orders in Kenya)
- Consent Requirements vs. Compelled Decryption
- Admissibility of Evidence from Bypassed Devices
- Ethical Implications of Using Vulnerabilities for Forensic Purposes
- **Case Study**: Discussing the legal implications of attempting to bypass an iPhone's passcode under Kenyan law.

Module 3: Non-Invasive & Logical Bypass Techniques (Logical Bypass Methods)

- Leveraging USB Restricted Mode bypasses (if applicable to OS version)
- Exploiting Backup Passwords and Lockdown Files (iTunes/Finder Pairing Records)
- Utilizing Emergency Call Features or Accessibility Options for Limited Access
- ADB and Fastboot Commands for Android Locked Devices (where applicable)
- **Case Study**: Using a lockdown file to create a backup from a locked iPhone.

Module 4: Android Device-Specific Bypass Techniques (Android Lock Bypasses)

- Google Account Bypass (Android 5.0 Lollipop and older)
- ADB Pull for Specific Files (requires debugging enabled and older Android versions)
- Custom Recovery (TWRP) & ADB Sideloading for Pattern/PIN Reset
- Flashing Custom Firmware (Rooting for Forensic Access)
- **Case Study**: Bypassing an Android pattern lock using the TWRP recovery method.

Module 5: iOS Device-Specific Bypass Techniques (iOS Lock Bypasses)

- Checkm8 Bootrom Exploit for Older A-series iPhones (DFU Mode Physical Acquisition)
- GrayKey and Similar Tools for Passcode Brute-Forcing
- Leveraging Forensic Toolkits for Logical Extractions from Locked iOS Devices (if in AFU)
- Understanding USB Restricted Mode and its Countermeasures
- **Case Study**: Using a DFU mode exploit to gain physical access to an older iPhone for data extraction.

Module 6: Hardware-Based Acquisition: Chip-Off (Chip-Off for Locked Devices)

- Principles of Chip-Off Forensics for Mobile Devices
- De-soldering Techniques for eMMC, eMCP, and NAND Chips
- Using Chip Readers and Adapters for Raw Data Extraction
- Reassembling File Systems from Raw Chip Dumps
- **Case Study**: Performing a simulated Chip-Off acquisition on a severely damaged, locked smartphone.

Module 7: Hardware-Based Acquisition: ISP (In-System Programming Bypass)

- Understanding In-System Programming (ISP) Points on Mobile Device Boards
- Identifying Test Points for Direct Memory Access (eMMC/eMCP)
- Using ISP Adapters and Forensic Box Tools for Data Extraction
- Advantages and Disadvantages of ISP vs. Chip-Off
- **Case Study**: Utilizing ISP points to bypass the lock on a recent Android device.

Module 8: JTAG & eMMC/eMCP Forensics (JTAG & eMMC Forensics)

- Introduction to JTAG for Mobile Device Debugging and Data Access
- Identifying JTAG Pins and Connecting to Target Devices
- Extracting Data from eMMC and eMCP Chips via JTAG/Direct Connection
- Understanding Data Structures on Embedded MultiMediaCard (eMMC)
- **Case Study**: Gaining access to a legacy Android device via JTAG for forensic data extraction.

Module 9: Advanced Encryption Bypass Techniques (Encryption Bypass Methods)

- Understanding Key Derivation Functions (KDFs) and Cryptographic Protection
- Forensic Challenges of Hardware-Backed Encryption (Secure Enclave, TEE)
- Leveraging Passcode Brute-Forcing Tools (e.g., GPU-accelerated cracking)
- Decryption of Encrypted File Systems (FDE/FBE) Post-Acquisition
- **Case Study**: Attempting to brute-force a weak passcode on an encrypted mobile device.

Module 10: Firmware Vulnerabilities for Bypass (Firmware Bypass Exploits)

- Identifying and Analyzing Firmware Vulnerabilities (Bootloader, Baseband, Modem)
- Exploiting Firmware Flaws to Gain Unauthorized Access
- Forensic Implications of Custom ROMs and Modified Firmware
- Tools for Firmware Analysis and Exploitation
- **Case Study**: Investigating a phone that was unlocked using a publicly known firmware exploit.

Module 11: Mobile OS Memory Forensics (Mobile RAM Bypass)

- Acquiring RAM Dumps from Live or Partially Compromised Devices
- Analyzing Volatile Memory for Passcodes, Encryption Keys, and Running Processes
- Identifying In-Memory Exploits and Shellcode
- Tools and Methodologies for Mobile Memory Analysis (e.g., Volatility Framework for Android)
- **Case Study**: Extracting a cached passcode from RAM on an Android device in AFU state.

Module 12: Anti-Forensic Measures & Countermeasures (Anti-Forensics Bypass)

- Common Anti-Forensic Techniques on Mobile Devices (Secure Erase, Data Wiping, Device Destruction)
- Detecting and Mitigating Anti-Forensic Attempts

- Data Carving and Fragment Recovery from Wiped Devices
- Strategies for Dealing with Remote Wipes and Device Lockouts
- **Case Study**: Recovering fragments of data from a mobile device subjected to a factory reset.

Module 13: Commercial Forensic Tools & Their Capabilities (Forensic Tool Bypass)

- Overview of Leading Commercial Mobile Forensic Tools (Cellebrite, MSAB, Oxygen Forensics, Magnet AXIOM)
- Understanding Their Lock Bypass and Data Extraction Features
- Limitations and Success Rates of Commercial Tools for Specific Devices/OS Versions
- Practical Labs Using Selected Commercial Tools for Lock Bypass
- **Case Study**: Using a commercial tool to perform a full file system extraction from a locked device.

Module 14: Custom Scripting & Tool Development (Custom Bypass Scripting)

- Introduction to Python for Mobile Forensic Automation
- Scripting for Automated Lock Screen Bypass Attempts
- Developing Custom Parsers for Decrypted Data
- Leveraging Open-Source Libraries for Low-Level Mobile Device Interaction
- **Case Study**: Writing a Python script to automate brute-force attempts on specific Android lock patterns.

Module 15: Reporting & Presenting Bypassed Evidence (Bypassed Evidence Reporting)

- Best Practices for Documenting Lock Bypass Procedures
- Crafting Clear and Defensible Forensic Reports on Bypassed Devices
- Presenting Complex Technical Findings (e.g., exploit chains) to Non-Technical Audiences
- Addressing Challenges to Admissibility of Evidence from Bypassed Devices in Kenyan Courts
- **Case Study**: Preparing a mock expert report for a case involving data recovered from a hardware-bypassed mobile device.

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 sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

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