Training Course on Data Extraction from Damaged Mobile Devices

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$2,200 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This highly specialized training course is meticulously designed for digital forensic investigators, law enforcement personnel, cybersecurity experts, and incident responders who face the daunting challenge of extracting critical digital evidence from physically damaged, water-damaged, or non-functional mobile devices. In high-stakes investigations, from criminal cases and corporate espionage to data breaches and fraud, crucial evidence often resides on mobile phones that have been subjected to extreme conditions, rendering traditional logical or file system extractions impossible. Training Course on Data Extraction from Damaged Mobile Devices provides the cutting-edge knowledge and intensive hands-on skills required to bypass conventional limitations, perform low-level hardware interventions, and recover vital data when all other methods fail.

The curriculum delves deep into the internal architecture of mobile devices, focusing on memory technologies (eMMC, UFS, NAND Flash), board-level components, and test points (JTAG, ISP). Through extensive practical labs, micro-soldering exercises, and real-world damaged device scenarios, participants will master techniques for Chip-Off acquisition, In-System Programming (ISP) data dumps, and advanced repair methods to bring damaged devices to a state where data can be extracted. The course emphasizes forensically sound procedures, strict adherence to chain of custody, and safety protocols when dealing with damaged electronics. It also addresses the legal and ethical considerations (including Kenya's Data Protection Act 2019) of intrusive data recovery, ensuring that all recovered evidence is legally admissible, verifiable, and ethically handled, empowering investigators to unlock crucial intelligence from even the most compromised mobile devices.

Programme Curriculum

Training Course on Data Extraction from Damaged Mobile Devices

Introduction

This highly specialized training course is meticulously designed for digital forensic investigators, law enforcement personnel, cybersecurity experts, and incident responders who face the daunting challenge of extracting critical digital evidence from physically damaged, water-damaged, or non-functional mobile devices. In high-stakes investigations, from criminal cases and corporate espionage to data breaches and fraud, crucial evidence often resides on mobile phones that have been subjected to extreme conditions, rendering traditional logical or file system extractions impossible. Training Course on Data Extraction from Damaged Mobile Devices provides the cutting-edge knowledge and intensive hands-on skills required to bypass conventional limitations, perform low-level hardware interventions, and recover vital data when all other methods fail.

The curriculum delves deep into the internal architecture of mobile devices, focusing on memory technologies (eMMC, UFS, NAND Flash), board-level components, and test points (JTAG, ISP). Through extensive practical labs, micro-soldering exercises, and real-world damaged device scenarios, participants will master techniques for Chip-Off acquisition, In-System Programming (ISP) data dumps, and advanced repair methods to bring damaged devices to a state where data can be extracted. The course emphasizes forensically sound procedures, strict adherence to chain of custody, and safety protocols when dealing with damaged electronics. It also addresses the legal and ethical considerations (including Kenya's Data Protection Act 2019) of intrusive data recovery, ensuring that all recovered evidence is legally admissible, verifiable, and ethically handled, empowering investigators to unlock crucial intelligence from even the most compromised mobile devices.

Course Duration

10 Days

Course Objectives

1. Assess and classify types of physical damage to mobile devices and their impact on data accessibility.
2. Understand the internal components and memory architectures of modern smartphones (eMMC, UFS, NAND, CPU).
3. Perform board-level diagnostics to identify damaged components hindering data access.
4. Execute forensically sound Chip-Off procedures to extract memory chips from damaged PCBs.
5. Utilize In-System Programming (ISP) techniques to acquire data from non-removable eMMC/UFS chips.

6. Apply JTAG and UART interfaces for debugging and data extraction from damaged devices.
7. Conduct micro-soldering techniques for repairing damaged PCBs and establishing test point connections.
8. Recover data from water-damaged and burnt mobile devices using specialized cleaning and repair methods.
9. Handle and read raw memory dumps obtained from Chip-Off and ISP acquisitions.
10. Decrypt and reassemble raw data from encrypted memory chips for analysis.
11. Troubleshoot common issues encountered during damaged device data extraction.
12. Document the damaged device acquisition process meticulously for legal admissibility and chain of custody.
13. Adhere to safety protocols and data privacy regulations (e.g., Kenya's Data Protection Act 2019) throughout the extraction process.

Organizational Benefits

1. Unlocking Critical Evidence: Recover data from devices previously considered inaccessible, resolving complex cases.
2. Expanded Investigative Capability: Bring high-value, specialized data recovery skills in-house.
3. Reduced Reliance on External Labs: Decrease costs and turnaround times by performing advanced recovery internally.
4. Enhanced Incident Response: Accelerate data recovery from devices crucial to ongoing cyber security incidents or fraud investigations.
5. Improved Case Resolution: Provide vital evidence to prosecutors, legal teams, or internal stakeholders for successful outcomes.
6. Protection of Sensitive Data: Recover data from damaged devices that might contain critical organizational or personal information.
7. Increased Success Rates: Significantly improve the chances of data recovery from severely damaged devices.
8. Strategic Advantage: Position the organization at the forefront of advanced digital forensics.
9. Compliance with Legal Standards: Ensure all complex data extraction methods adhere to legal and ethical guidelines.
10. Expert Witness Development: Cultivate personnel capable of providing expert testimony on highly technical data recovery methods.

Target Participants

- Digital Forensic Examiners (Intermediate to Advanced)
- Mobile Device Forensic Specialists
- Law Enforcement Digital Evidence Units
- Cybercrime Investigators
- Incident Response Teams

- Hardware Reverse Engineers
- Data Recovery Professionals
- Military and Intelligence Analysts
- Product Security Engineers (Hardware/Firmware)
- Laboratory Technicians responsible for forensic data acquisition

Course Outline

Module 1: Mobile Device Architecture for Forensics (Hardware Fundamentals)

- Overview of Mobile Phone Components: Motherboard, CPU, Memory (eMMC, UFS, NAND), Peripherals
- Understanding Data Storage Mechanisms and Memory Controllers
- Differences between Android and iOS Hardware Architectures
- Common Points of Failure in Physically Damaged Devices
- **Case Study**: Identifying the key components on a disassembled smartphone PCB.

Module 2: Damage Assessment and Initial Triage (Damage Assessment)

- Classifying Types of Physical Damage (Water, Impact, Fire, Bend)
- Initial Safety Protocols for Damaged Devices
- Visual Inspection and Microscopic Examination
- Determining Feasibility of Data Extraction based on Damage
- **Case Study**: Assessing a water-damaged phone to determine the best recovery approach.

Module 3: Introduction to Chip-Off Forensics (Chip-Off Basics)

- Principles and Applications of Chip-Off Acquisition
- Identifying Suitable Memory Chips for Extraction (BGA, LGA)
- Tools and Equipment for Chip Removal (Hot Air Station, Rework Station, Soldering Iron)
- Best Practices for Safe Chip Desoldering to Prevent Damage
- **Case Study**: Practicing safe component removal on a sacrificial PCB.

Module 4: Chip Preparation and Reading (Chip Handling & Reading)

- Cleaning and Reballing BGA Chips for Data Acquisition
- Using Specialized Chip Readers and Adapters
- Understanding Raw Data Dumps from Memory Chips
- Verification of Chip Read Integrity (Hashing)
- **Case Study**: Preparing and reading a removed eMMC chip using a forensic reader.

Module 5: In-System Programming (ISP) Forensics (ISP Acquisition)

- Principles and Advantages of ISP over Chip-Off
- Identifying ISP Test Points (TPs) on Mobile Phone PCBs
- Connecting to ISP Points (Soldering, Probing)
- Utilizing ISP Tools (e.g., Easy JTAG Plus, UFI Box) for Data Acquisition
- **Case Study**: Performing an ISP acquisition on a smartphone with a broken screen.

Module 6: JTAG & UART Forensics (JTAG & UART)

- Understanding JTAG (Joint Test Action Group) and UART Interfaces
- Identifying JTAG Test Access Ports (TAPs)
- Using JTAG Devices (e.g., RIFF Box, Z3X JTAG) for Data Extraction
- Communicating via UART for Console Access and Bootloader Manipulation
- **Case Study**: Connecting to a device via JTAG to bypass a lock or extract data.

Module 7: Advanced Soldering and Rework Techniques (Advanced Rework)

- Micro-Soldering Fundamentals for Mobile Device Repair
- Replacing Damaged Connectors, Flex Cables, and Components
- Board Repair Techniques for Broken Traces and Pads
- Best Practices for Heat Management and Flux Application
- **Case Study**: Repairing a damaged USB charging port or battery connector.

Module 8: Data Recovery from Water Damaged Devices (Water Damage Recovery)

- Principles of Water Damage and Corrosion Effects
- Disassembly and Cleaning Procedures (Ultrasonic Cleaner, Isopropyl Alcohol)
- Drying Techniques and Corrosion Removal
- Repairing Corroded Traces and Components
- **Case Study**: Restoring power to a water-damaged phone to attempt logical extraction.

Module 9: Data Recovery from Burnt/Impact Damaged Devices (Severe Damage Recovery)

- Challenges of Data Recovery from Severely Burnt or Shattered Devices
- Identifying Intact Components for Targeted Extraction
- Specialized Techniques for Handling Fragile PCBs and Memory Chips
- Risks and Limitations of Extreme Damage Recovery
- **Case Study**: Assessing a phone with extensive impact damage to identify recoverable memory.

Module 10: Analyzing Raw Memory Dumps (Raw Data Analysis)

- Interpreting Raw Binary Data from Chip-Off/ISP Dumps
- Identifying File System Structures within Raw Dumps
- Using Hex Editors and Disk Imaging Tools for Analysis
- Carving for Known File Types and Artifacts
- **Case Study**: Manually identifying picture file headers within a raw memory dump.

Module 11: File System Reconstruction & Decryption (File System Reconstruction)

- Reconstructing Mobile File Systems (EXT4, F2FS, APFS) from Raw Data
- Understanding Flash Translation Layers (FTL) and Wear Leveling Implications
- Decrypting Encrypted Data (e.g., Full Disk Encryption, File-Based Encryption)
- Using Forensic Software to Parse Reconstructed File Systems
- **Case Study**: Reassembling a file system from an eMMC dump and Browse its contents.

Module 12: Bypassing Device Security for Data Extraction (Security Bypass)

- Understanding Bootloader Locks and Secure Boot Mechanisms
- Exploiting Vulnerabilities for Forensic Access (where applicable and ethical)
- Dealing with Password-Protected and Encrypted Devices
- Legality and Ethics of Bypassing Security in Forensics
- **Case Study**: Exploring methods to gain access to a locked device for data acquisition.

Module 13: Specialized Tools & Equipment (Forensic Tooling)

- Overview of Commercial Chip-Off/ISP/JTAG Equipment
- Essential Micro-Soldering Tools and Supplies
- Data Converters and Adapters for Memory Chips
- Software for Raw Data Analysis and File System Reconstruction
- **Case Study**: Setting up a workstation with necessary hardware and software for damaged device recovery.

Module 14: Documentation and Reporting for Damaged Devices (Documentation & Reporting)

- Detailed Documentation of Damage Assessment and Repair Steps
- Maintaining an Enhanced Chain of Custody for Intrusive Methods
- Explaining Complex Technical Procedures in Forensic Reports
- Addressing Risks and Limitations in Findings
- **Case Study**: Documenting the complete process of data recovery from a water-damaged device for an official report.

Module 15: Legal, Ethical & Future Trends (Legal, Ethical & Future)

- Legal Considerations for Damaged Device Forensics (e.g., Consent, Warrants)
- Ethical Dilemmas and Responsibilities in Intrusive Data Recovery
- **Compliance with Kenya's Data Protection Act 2019** for recovered sensitive data
- Emerging Technologies and Challenges in Damaged Device Forensics (UFS, Advanced Encryption)

- **Case Study**: Discussing the ethical implications of attempting data recovery on a device that might be destroyed in the process.

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.
- Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
03 Aug 2026	14 Aug 2026	Online	$2,200
10 Aug 2026	21 Aug 2026	Online	$2,200
17 Aug 2026	28 Aug 2026	Online	$2,200
24 Aug 2026	04 Sep 2026	Online	$2,200
31 Aug 2026	11 Sep 2026	Online	$2,200
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskills.com | Website: www.fineskills.com