Training Course on SIM Card and Carrier-Based Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This specialized training course provides digital forensic investigators, law enforcement personnel, and cybersecurity analysts with the essential skills to conduct SIM card forensics and leverage carrier-based data for investigations. In an increasingly connected world, mobile communications are central to almost every digital investigation. Training Course on SIM Card and Carrier-Based Forensics delves into the intricate data artifacts stored on Subscriber Identity Modules (SIM cards), including contacts, SMS messages, call logs, and network-specific information, as well as the wealth of information accessible through Mobile Network Operator (MNO) records, such as Call Detail Records (CDRs), cell tower data, and subscriber information. Participants will learn forensically sound techniques for extracting and analyzing this critical evidence, which is vital for cybercrime investigations, fraud detection (e.g., SIM swapping), human trafficking cases, and accident reconstruction.

The curriculum emphasizes hands-on acquisition methods using specialized SIM card readers and forensic tools, alongside an in-depth understanding of the legal processes required to obtain data from telecommunications providers in Kenya and internationally. Participants will explore the structure of SIM card file systems, delve into the intricacies of analyzing CDRs for timeline reconstruction and location analysis, and understand the privacy implications and legal frameworks (e.g., Kenya Data Protection Act 2019) governing such sensitive data. Graduates will emerge with the advanced capabilities to effectively integrate SIM card and carrier data into comprehensive digital investigations, providing invaluable intelligence for attribution, profiling, and evidence presentation in court.

Programme Curriculum

Training Course on SIM Card and Carrier-Based Forensics

Introduction

This specialized training course provides digital forensic investigators, law enforcement personnel, and cybersecurity analysts with the essential skills to conduct SIM card forensics and leverage carrier-based data for investigations. In an increasingly connected world, mobile communications are central to almost every digital investigation. Training Course on SIM Card and Carrier-Based Forensics delves into the intricate data artifacts stored on Subscriber Identity Modules (SIM cards), including contacts, SMS messages, call logs, and network-specific information, as well as the wealth of information accessible through Mobile Network Operator (MNO) records, such as Call Detail Records (CDRs), cell tower data, and subscriber information. Participants will learn forensically sound techniques for extracting and analyzing this critical evidence, which is vital for cybercrime investigations, fraud detection (e.g., SIM swapping), human trafficking cases, and accident reconstruction.

The curriculum emphasizes hands-on acquisition methods using specialized SIM card readers and forensic tools, alongside an in-depth understanding of the legal processes required to obtain data from telecommunications providers in Kenya and internationally. Participants will explore the structure of SIM card file systems, delve into the intricacies of analyzing CDRs for timeline reconstruction and location analysis, and understand the privacy implications and legal frameworks (e.g., Kenya Data Protection Act 2019) governing such sensitive data. Graduates will emerge with the advanced capabilities to effectively integrate SIM card and carrier data into comprehensive digital investigations, providing invaluable intelligence for attribution, profiling, and evidence presentation in court.

Course Duration

5 Days

Course Objectives

1. Understand the structure and file system of SIM cards (MF, DF, EF) and their data storage capabilities.
2. Perform forensically sound acquisition of data directly from SIM cards using specialized readers.
3. Extract and analyze contacts, SMS messages, and call logs stored on SIM cards, including deleted entries.
4. Interpret network-specific data (IMSI, ICCID, MCC, MNC) from SIM cards for subscriber identification.

5. Understand the types of Call Detail Records (CDRs) available from Mobile Network Operators (MNOs) and their forensic value.
6. Initiate and manage the legal process for obtaining CDRs and other carrier-based data from MNOs in Kenya.
7. Analyze CDR data to reconstruct communication patterns, call frequencies, and associated metadata.
8. Utilize cell tower data (Cell ID, GPS coordinates) from CDRs for approximate location analysis and timeline reconstruction.
9. Investigate SMS and MMS message content from carrier records for evidentiary purposes.
10. Identify and analyze SIM swapping fraud indicators using both SIM card and carrier data.
11. Understand voicemail forensics and the process of acquiring and analyzing voicemail recordings.
12. Apply data protection principles (e.g., Kenya Data Protection Act 2019) and ethical considerations to SIM card and carrier-based investigations.
13. Generate comprehensive forensic reports combining SIM card and carrier data for legal admissibility.

Organizational Benefits

1. Expanded Investigative Scope: Access crucial evidence from SIM cards and mobile network operators, augmenting device-level forensics.
2. Improved Case Resolution: Uncover vital communication, location, and subscriber data for complex criminal and civil cases.
3. Enhanced Fraud Detection: Strengthen capabilities in investigating telecommunications fraud, especially SIM swapping.
4. Accurate Accident/Incident Reconstruction: Utilize call and location data to accurately reconstruct timelines of events.
5. Compliance with Legal Mandates: Ensure all data acquisition from carriers adheres to strict legal and regulatory requirements.
6. Reduced Investigative Bottlenecks: Expedite investigations by understanding the process of obtaining and analyzing carrier data.
7. Cost Savings: Develop in-house expertise, reducing reliance on external specialists for carrier-based investigations.
8. Actionable Intelligence: Generate intelligence on communication patterns, network usage, and suspicious activities.
9. Strengthened Evidence Admissibility: Learn best practices for maintaining chain of custody and presenting SIM/carrier data in court.
10. Protection of Critical Assets: Aid in securing accounts compromised via SIM-related attacks.

Target Participants

- Digital Forensic Examiners
- Law Enforcement Officers (e.g., Cybercrime Units, Fraud Investigators)
- Telecommunications Fraud Analysts
- Cybersecurity Incident Responders
- Corporate Investigators
- E-Discovery Specialists
- Legal Professionals (prosecutors, defense attorneys)
- Internal Auditors
- Intelligence Analysts
- Mobile Network Operator Security Teams

Course Outline

Module 1: Introduction to SIM Cards & Carrier Data (SIM Card Forensics Fundamentals)

- Overview of Mobile Communication Technologies (GSM, UMTS, LTE, 5G)
- Role and Structure of the Subscriber Identity Module (SIM Card)
- Types of Data Stored on a SIM Card (IMSI, ICCID, Contacts, SMS)
- Introduction to Mobile Network Operator (MNO) Data and its Forensic Value (CDRs, Subscriber Info)
- **Case Study**: Examining a standard SIM card to identify basic subscriber information.

Module 2: SIM Card Data Acquisition & Preservation (SIM Card Data Extraction)

- Forensically Sound Removal and Handling of SIM Cards
- Using SIM Card Readers and Forensic Tools for Data Extraction
- Logical vs. Physical Acquisition from SIM Cards
- Recovering Deleted Data from SIM Card EEPROM
- **Case Study**: Acquiring contacts and SMS messages from a feature phone SIM card.

Module 3: SIM Card Data Artifact Analysis (SIM Card Artifacts Analysis)

- Detailed Analysis of Phonebook Entries (ADN, FDN, LND)
- Interpreting SMS Message Structures and Content on SIM Cards
- Examining Call Log Entries Stored on the SIM
- Understanding Service Provider Name (SPN) and Network Parameters
- **Case Study**: Analyzing timestamps on SIM-stored SMS to establish communication timelines.

Module 4: Understanding Call Detail Records (CDRs) (CDR Data Forensics)

- Components of a Call Detail Record (Date/Time, Origin/Destination Numbers, Duration, Cell ID)
- Types of CDRs: Voice, SMS, Data Sessions
- Data Retention Policies of Mobile Network Operators in Kenya
- Requesting and Interpreting Raw CDR Data Files
- **Case Study**: Analyzing a CDR for a specific date to identify all inbound and outbound calls.

Module 5: Location Data from Mobile Carriers (Cell Site Analysis)

- Principles of Cell Site Analysis: How Mobile Devices Connect to Towers
- Interpreting Cell ID (CID) and Location Area Code (LAC) Data in CDRs
- Using Cell Tower Data for Approximate Geographic Location
- Limitations and Accuracy of Cell Site Analysis for Location Forensics
- **Case Study**: Plotting a suspect's approximate location over time using multiple cell tower handoffs from CDRs.

Module 6: Investigating Carrier-Based Communications (Telecom Data Investigation)

- Analyzing SMS/MMS Content from Carrier Records (where available)
- Understanding Data Session Records (IP addresses, Data Volume)
- Voicemail Forensic Analysis: Acquisition and Authentication Challenges
- Correlating Carrier Data with On-Device and Cloud Data
- **Case Study**: Reconstructing a full communication narrative from combined CDR and on-device SMS data.

Module 7: SIM Swapping & Telecom Fraud Forensics (SIM Swapping Forensics)

- Understanding the Mechanics and Impact of SIM Swapping Fraud
- Identifying Indicators of Compromise (IOCs) in Carrier Records (e.g., sudden SIM change, suspicious account activity)
- Investigating Mobile Money Fraud and its Link to SIM-Based Attacks
- Collaboration with Mobile Network Operators in Fraud Investigations
- **Case Study**: Analyzing carrier logs to identify a fraudulent SIM swap event and associated account takeovers.

Module 8: Legal & Ethical Considerations in Carrier Forensics (Telecom Data Legal)

- Navigating Legal Frameworks for Accessing Telecom Data (Warrants, Court Orders in Kenya)
- Adherence to the **Kenya Data Protection Act 2019** regarding subscriber privacy.
- Ensuring Chain of Custody for SIM and Carrier-Based Evidence
- Ethical Implications of Accessing and Using Sensitive Communications Data
- **Case Study**: Discussing the legal process and privacy considerations when requesting historical location data from Safaricom.

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.com or call *+254769199797*

Certification

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

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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