Training Course on Mobile Payment System Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This specialized training course is meticulously designed for digital forensic investigators, financial crime units, cybersecurity professionals, fraud examiners, and regulatory bodies grappling with the escalating complexities of mobile payment system forensics. In Kenya, and globally, mobile money platforms like M-Pesa have revolutionized financial transactions, but their rapid adoption has also made them a prime target for sophisticated financial fraud, SIM swap attacks, account takeovers, phishing schemes, and money laundering. Training Course on Mobile Payment System Forensics equips participants with the critical knowledge and hands-on techniques required to acquire, preserve, analyze, and interpret digital evidence from mobile devices, cloud platforms, and backend systems involved in mobile payment ecosystems, enabling effective investigation and prosecution of mobile payment fraud.

The curriculum delves into the intricate mechanisms of mobile money platforms, digital wallets, QR code payments, and peer-to-peer (P2P) transfers, exploring the various layers of data generation from the mobile device itself to network operator logs and payment gateway records. Through extensive practical labs, simulated fraud scenarios, and real-world case studies specific to the Kenyan context (e.g., M-Pesa fraud patterns), participants will master methodologies to extract transaction histories, device fingerprints, application data, communication logs, and associated metadata. The course also critically emphasizes adherence to forensically sound principles, chain of custody, and compliance with local regulations like Kenya's Data Protection Act 2019 and financial services laws, ensuring that all collected evidence is legally admissible and ethically handled, empowering investigators to combat the evolving landscape of mobile payment fraud effectively.

Programme Curriculum

Training Course on Mobile Payment System Forensics

Introduction

This specialized training course is meticulously designed for digital forensic investigators, financial crime units, cybersecurity professionals, fraud examiners, and regulatory bodies grappling with the escalating complexities of mobile payment system forensics. In Kenya, and globally, mobile money platforms like M-Pesa have revolutionized financial transactions, but their rapid adoption has also made them a prime target for sophisticated financial fraud, SIM swap attacks, account takeovers, phishing schemes, and money laundering. Training Course on Mobile Payment System Forensics equips participants with the critical knowledge and hands-on techniques required to acquire, preserve, analyze, and interpret digital evidence from mobile devices, cloud platforms, and backend systems involved in mobile payment ecosystems, enabling effective investigation and prosecution of mobile payment fraud.

The curriculum delves into the intricate mechanisms of mobile money platforms, digital wallets, QR code payments, and peer-to-peer (P2P) transfers, exploring the various layers of data generation from the mobile device itself to network operator logs and payment gateway records. Through extensive practical labs, simulated fraud scenarios, and real-world case studies specific to the Kenyan context (e.g., M-Pesa fraud patterns), participants will master methodologies to extract transaction histories, device fingerprints, application data, communication logs, and associated metadata. The course also critically emphasizes adherence to forensically sound principles, chain of custody, and compliance with local regulations like Kenya's Data Protection Act 2019 and financial services laws, ensuring that all collected evidence is legally admissible and ethically handled, empowering investigators to combat the evolving landscape of mobile payment fraud effectively.

Course Duration

5 Days

Course Objectives

1. Understand the architecture and operational flows of various mobile payment systems (e.g., mobile money, digital wallets, NFC payments).
2. Identify key digital evidence sources in mobile payment fraud investigations across devices, networks, and backend systems.
3. Perform forensically sound data acquisition from mobile devices (smartphones, feature phones) relevant to payment activities.
4. Extract and analyze transaction logs, payment receipts, and balance information from mobile payment applications.

5. Investigate SIM swap fraud by analyzing device history, network operator logs, and account activity.
6. Identify and interpret indicators of compromise (IOCs) related to phishing, social engineering, and malware targeting mobile payment users.
7. Analyze application-specific data from popular mobile money apps (e.g., M-Pesa, Airtel Money) for forensic artifacts.
8. Understand tokenization and encryption mechanisms in mobile payments and their forensic implications.
9. Trace fund transfers and recipient details across mobile payment networks.
10. Utilize specialized forensic tools and techniques for mobile device and financial data analysis.
11. Navigate regulatory compliance requirements and data privacy laws (e.g., Kenya's Data Protection Act 2019) in mobile payment investigations.
12. Reconstruct fraudulent transaction timelines and establish patterns of activity.
13. Generate comprehensive forensic reports suitable for law enforcement, financial institutions, and court proceedings.

Organizational Benefits

1. Enhanced Fraud Detection & Prevention: Develop capabilities to identify and mitigate sophisticated mobile payment fraud schemes.
2. Improved Financial Crime Investigation: Equip teams with specialized skills to investigate mobile money-related offenses effectively.
3. Reduced Financial Losses: Minimize financial impact from fraudulent transactions, chargebacks, and account takeovers.
4. Strengthened Compliance: Ensure adherence to local financial regulations and data protection laws (e.g., Kenya's Data Protection Act).
5. Faster Incident Response: Accelerate the response and resolution of mobile payment security incidents.
6. Protection of Customer Trust: Demonstrate a commitment to securing customer funds and data in mobile payment ecosystems.
7. Actionable Threat Intelligence: Gain insights into emerging mobile payment fraud trends and attack methodologies.
8. Optimized Resource Allocation: Efficiently utilize forensic tools and personnel in high-volume mobile payment fraud cases.
9. Robust Litigation Support: Produce legally admissible evidence for prosecuting mobile payment fraud cases.
10. Competitive Advantage: Position the organization as a leader in securing and investigating digital financial services.

Target Participants

- Digital Forensic Investigators
- Financial Crime Investigators (Banks, Telcos, Mobile Money Operators)
- Fraud Analysts and Examiners
- Law Enforcement Agencies (DCI, Cybercrime Units, Banking Fraud)
- Cybersecurity Incident Responders (Financial Sector)
- Anti-Money Laundering (AML) Specialists
- Internal Auditors (Financial Institutions)
- Risk Management Professionals (Fintech, Mobile Money)
- Regulatory Compliance Officers
- Legal Professionals specializing in Financial Crime

Course Outline

Module 1: Mobile Payment Ecosystem & Fraud Landscape (Mobile Payment Fundamentals)

- Overview of Mobile Payment Systems: Mobile Money, Digital Wallets, QR Payments, P2P transfers
- Key Players: Mobile Network Operators (MNOs), Banks, Payment Service Providers (PSPs), Merchants, Users
- Common Mobile Payment Fraud Types: SIM Swap, Phishing, Account Takeover, Social Engineering, Malware
- Regulatory Environment for Mobile Payments in Kenya (Central Bank of Kenya, CAK)
- **Case Study**: Analyzing a common M-Pesa phishing scam in Kenya.

Module 2: Mobile Device Forensics for Payments (Device Data Extraction)

- Forensically Sound Acquisition from Smartphones (Android, iOS) and Feature Phones
- Extracting Mobile Payment Application Data: SQLite Databases, Preferences, Logs
- Analyzing SMS, Call Logs, and Contacts for Communication Patterns
- Device Fingerprinting and Hardware Identifiers for Device Linkage
- **Case Study**: Recovering deleted M-Pesa transaction SMS messages from an Android device.

Module 3: Mobile Payment Application & Wallet Forensics (App Data Analysis)

- Deep Dive into Popular Mobile Money Apps (e.g., M-Pesa, Airtel Money): Data Storage, Encryption
- Analyzing Digital Wallet Contents: Tokens, Card Details (if applicable), Transaction History
- Reverse Engineering Application Data Formats for Unparsed Artifacts
- Understanding Application Updates and Their Impact on Forensics
- **Case Study**: Extracting and parsing the internal database of a common mobile money app to find hidden transaction records.

Module 4: Network & Backend System Forensics (Network & Backend Forensics)

- Analyzing Mobile Network Operator (MNO) Logs: Call Detail Records (CDRs), SIM Change History
- Investigating Payment Gateway Logs and Transaction Processing Records
- Cloud-Based Data: Account Backups, Synchronized App Data relevant to payments
- Correlating On-Device Data with Network and Backend Records
- **Case Study**: Using MNO SIM swap logs to confirm a fraudulent account takeover.

Module 5: Transaction Analysis & Fraud Patterns (Transaction & Fraud Analysis)

- Detailed Analysis of Mobile Payment Transaction Data: Amounts, Dates, Times, Parties, Status
- Identifying Anomalous Transaction Patterns and Fraud Indicators
- Tracing Fund Movements Across Multiple Accounts and Entities
- Leveraging Financial Analytics Tools for Large Dataset Review
- **Case Study**: Tracing the flow of laundered funds through a series of mobile money transactions.

Module 6: SIM Swap & Account Takeover Investigations (SIM Swap Forensics)

- Understanding the Mechanics of SIM Swap Attacks
- Evidence Sources for SIM Swap Investigations: Telco Records, Device Changes, Login Anomalies
- Reconstructing the Timeline of a SIM Swap Incident
- Mitigation and Prevention Strategies for SIM Swap Fraud
- **Case Study**: Forensic investigation of an account takeover facilitated by a SIM swap.

Module 7: Malware, Phishing & Social Engineering (Mobile Payment Security)

- Identifying Malware on Mobile Devices Targeting Payment Apps
- Analyzing Phishing and Smishing (SMS Phishing) Attacks for Mobile Payments
- Investigating Social Engineering Tactics Used to Defraud Users
- Extracting Evidence from Compromised Messaging Apps or Emails
- **Case Study**: Analyzing a mobile device infected with banking trojan malware targeting mobile payment credentials.

Module 8: Legal, Regulatory & Reporting (Legal & Compliance)

- Legal Frameworks for Financial Crime Investigations in Kenya (e.g., Proceeds of Crime and Anti-Money Laundering Act, Banking Act)
- Compliance with **Kenya's Data Protection Act 2019** on financial data privacy
- Chain of Custody for Mobile Payment Evidence
- Preparing Comprehensive Forensic Reports for Law Enforcement and Regulatory Bodies
- **Case Study**: Preparing a forensic report on a mobile money fraud case, highlighting adherence to the Kenya Data Protection Act.

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 *+254724527104*

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
03 Aug 2026	07 Aug 2026	Online	$1,100
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100

Start Date	End Date	Location	Price
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100

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

Register Online Now

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