Mobile Forensics in Financial Fraud Analysis

Shubham Ganji , Smita Kulkarni Pai
Computer Engineering Department
MGM's College of Engineering and Technology, Kamothe, Navi Mumbai

Abstract : Mobile forensics, a critical component of digital forensics, is essential for investigating and analyzing digital evidence pertinent to financial fraud security. This guide delineates key steps and methodologies, with a focus on device identification, secure data extraction, password decryption, cloud and deleted data analysis, timeline reconstruction, network and geolocation analysis, app and social media investigations, and comprehensive reporting. The operational process involves acquiring mobile devices, analyzing file systems for financial data, extracting and decoding relevant information, verifying findings,collaborating with network forensics for broader insights, and presenting conclusive results. Mobile forensics plays a pivotal role in uncovering evidence for financial crimes, ranging from fraudulenttransactions to data breaches, where mobile devices serve as critical tools. Specialized techniques in mobileforensics contribute significantly to meticulous and successful investigations aimed at mitigating financial fraud risks.

Keywords- Mobile Forensics, Data, Analysis, Extraction, Evidence, Financial fraud.

I. INTRODUCTION

Digital forensics, often referred to as computer forensics, is the process of collecting, analyzing, and preserving electronic evidence in a manner that maintains its integrity for investigative or legal purposes. Digital forensics involves the examination of digital devices, storage media, and electronic data to uncover, interpret, and document evidence relevant to financial fraud cases or cybersecurity incidents targeting financial systems [1].

Digital forensics encompasses a broad range of activities, including:

- **Data Recovery:** Retrieving data from storage devices compromised by financial fraud activities, including deleted transactions, altered records, or intentionally concealed information [3].

- **Evidence Preservation:** Ensuring the integrity and admissibility of digital evidence related to financial fraud by meticulously following established procedures, securing digital evidence, and maintaining a detailed chain of custody [3].

- **Analysis of Digital Artifacts:** Analyzing digital artifacts related to financial transactions, including records, logs, metadata, and system traces, to reconstruct fraudulent events and identify perpetrators [3].

- **Malware Analysis:** Analyzing malicious software designed to target financial systems or manipulate financial data, understanding its behavior, functionality, and impact on financial transactions, and identifying methods used by fraudsters to compromise financial systems [3].

- **Incident Response:** Coordinating the response to financial fraud incidents by swiftly identifying the scope and impact of fraudulent activities, implementing measures to contain the breach, and collaborating with relevant stakeholders to mitigate further risks and prevent future occurrences of financial fraud [3].

Subtypes of Digital Forensics include-

- **Network Forensics:** Investigating network traffic, logs, and communication patterns to uncover security breaches, unauthorized access, or malicious activities targeting financial systems, such as unauthorized fund transfers or data exfiltration [2].

- **Mobile Forensics:** Analyzing mobile devices for financial data related to fraudulent transactions, including call records, messages, banking app activities, and geolocation information to link devices to financial fraud schemes [2].

- **Database Forensics:** Database forensics examines digital evidence in databases to uncover unauthorized access, breaches, and fraud using techniques like SQL queries and log analysis, crucial for maintaining data integrity and prosecuting cybercrimes [2].

II. STEPS / METHODS / HOW IT WORKS :

Step/Method	Need	Methods	How It Works
Device Identification	- Identify the specific mobile device to tailor forensic procedures accordingly.	- Utilize forensic tools that can identify the make, model, and operating system version of the mobile device.	**- Mobile forensic software often provides detailed device information during the initial scanning process.**
	- Different mobile operating systems and device models may require different forensic techniques.	- Analyze device information from system files and metadata.	**- Examination of system files, metadata, and device settings can reveal crucial details about the device.**
Seizure and Isolation	- Ensure the preservation of the device's state for accurate forensic analysis.	- Use physical methods to seize the device without altering its content.	**- Forensic specialists use tools like Faraday bags to isolate mobile devices and prevent them from connecting to networks.**
	- Prevent remote tampering or data wiping to maintain the integrity of evidence.	- Isolate the device from networks to prevent any remote interference.	**- Seizure involves securing the device in a way that minimizes the risk of physical damage or data alteration.**
Documentation and Chain of Custody	- Establish a clear record of the device's condition and any physical damage.	- Document the device's physical condition, includingany signs of damage or manipulation.	**- Digital photographs, written descriptions, and documentation software can record the device's condition.**
	- Maintain a documented chain of custody to ensure the admissibility of evidence in court.	- Use digital signatures, timestamps, and secure storage to maintain a chain of custody.	**- Chain of custody logs track the movement and handling of the device from seizure to analysis.**
Data Extraction	- Retrieve relevant data from the mobile device for forensic examination.	- Employ mobile forensic tools capable of extracting data from different types of mobile devices.	**- Forensic software communicates with the mobile device, accessing and copying data for analysis.**
	- Extract various types of data, such as call logs, messages, contacts, and multimedia files.	- Follow established procedures to ensurethe integrity of extracted data.	**- Extraction methods vary, including physical acquisition (bit-by-bit copying) and logical acquisition (focused on specific data types).**
Password and PIN Decryption	- Gain access to protected information on the mobile device.	- Use forensic tools that support password cracking or work with manufacturers to legally access locked devices.	**- Forensic tools attempt to guess or systematically test passwords until the correct one is found.**
	- Overcome security measures to retrieve critical evidence.	- Employ techniques like brute force attacks or leveraging vulnerabilities to decrypt passwords.	**- Collaboration with device manufacturers may involve lawful access methods, such as obtaining encryption keys.**

Cloud Forensics	- Investigate data stored in cloud services associated with the mobile device.	- Use credentials obtained from the device or legal means to access cloud accounts.	**- Forensic specialists log in to cloud accounts using obtained credentials to access synced data.**
	- Extract relevant information from cloud backups and synced data.	- Extract and analyze data from cloud storage services.	**- Extracted cloud data is then analyzed alongside on-device data for a comprehensive overview.**
Deleted Data Recovery	- Recover information that has been intentionally or unintentionally deleted from the mobile device.	- Use forensic techniques to recover deleted files or fragments.	**- Specialized tools and methods focus on the recovery of data from unallocated space or deleted file remnants.**
	- Analyze remnants of deleted files to reconstruct the user's activities.	- Analyze the device's file system to identify traces of previously deleted data.	**- Examination of file system structures helps identify locations where deleted data may persist.**
Timeline Reconstruction	- Establish a chronological order of events based on extracted data.	- Utilize timeline analysis tools to create a visual representation of events.	**- Timeline reconstruction involves arranging extracted data chronologically to understand the order of activities.**
	- Understand the sequence of user activities on the mobile device.	- Correlate timestamps from various artifacts to reconstruct a coherent timeline.	**- Correlation of timestamps from different sources helps create an accurate timeline.**
Network Analysis	- Examine network-related data to identify connections and communication with external entities.	- Analyze network logs and communication patterns.	**- Forensic tools and network analysis software help identify connections and communication patterns.**
	- Investigate the mobile device's interactions with Wi-Fi, Bluetooth, and cellular networks.	- Examine Wi-Fi, Bluetooth, and cellular data to track the device's movements.	**- Examination of network-related artifacts provides insights into the device's interactions with external entities.**
Geolocation Analysis	- Determine the geographic locations visited by the mobile device.	- Extract and analyze GPS data to pinpoint the device's locations.	**- GPS data extracted from the device provides latitude and longitude coordinates.**
	- Map the device's movements over time using location-based information.	- Utilize mapping tools to visualize the device's movements.	**- Mapping tools convert location data into visual representations, allowing investigators to track the device's movements.**
App and Social Media Analysis	- Investigate applications and social media interactions on the mobile device.	- Use forensic tools to analyze app data and extract relevant information.	**- Forensic specialists focus on app-specific data structures to extract messages, posts, and user interactions.**
	- Extract messages, posts, and user interactions from relevant apps.	- Explore communication patterns within social media apps.	**- Analysis of app data provides insights into the user's online activities.**
Reporting	- Compile a comprehensive report summarizing the findings of the mobile forensic analysis.	- Organize findings into a structured and clear report.	**- The report serves as acomprehensive document detailing theentire forensic process and its outcomes.**
	- Present relevant information, artifacts, and conclusions for use in legal proceedings.	- Include details such as the methodology, results, and expert opinions.	**- It provides a clear narrative for legal professionals, offering valuable insights into the digital evidence.**

Acquisition of Mobile Device	- Acquire data from the mobile device for forensic analysis.	- Physical acquisition involves obtaining a bit-by-bit copy of the device's storage.	**- Physical acquisition requires specialized tools and direct access to the device's storage.**
	- Choose appropriate acquisition methods based on the nature ofthe investigation.	- Logical acquisition focuses on extracting specific data using the device's operating system.	**Logical acquisition focuses on extracting specific data using the device's operating system.**
Analysis of File Systems	- Examine the file system structure to understand data storage mechanisms.	- Analyze file system metadata, directories, and file allocation tables.	**- Examination of file system structures helps forensic specialists locate and categorize data.**
	- Identify locations where different types of information are stored on the mobile device.	**- Use forensic tools to understand the organization of data within the file system.**	

III. CASE STUDY :

In 2018, the Enforcement Directorate (ED) of India launched a high-profile investigation into a financial fraud involving Nirav Modi and Punjab National Bank (PNB). The case centered on fraudulent issuance of Letters of Undertaking (LoUs) and illicit fund transfers amounting to billions of rupees. The fraud was initially uncovered during a routine internal audit conducted by PNB officials, prompting swift action by the ED [4].

The ED's forensic team played a crucial role in the investigation, conducting a meticulous analysis of seized mobile devices belonging to key individuals implicated in the scam [4]. Through advanced forensic techniques, including data extraction and analysis of call records, text messages, emails, and financial transactions, the team unearthed compelling evidence of fraudulent activities. This included evidence of unauthorized LoUs, elaborate money laundering schemes orchestrated by Nirav Modi and his associates, and collusion among corrupt PNB officials [5].

Armed with the incriminating evidence obtained through mobile forensics, the ED pursued legal action against Nirav Modi, his associates, and several PNB officials involved in the fraud. The subsequent legal proceedings resulted in convictions, extradition proceedings against Nirav Modi, and significant penalties for the perpetrators [5]. The Nirav Modi-PNB fraud case exemplifies the critical role of mobile forensics in uncovering complex financial crimes and ensuring accountability, underscoring the importance of robust investigative measures in safeguarding the integrity of India's financial system [5].

IV. CONCLUSION :

In conclusion, the effective application of Mobile forensics in financial fraud security is indispensable for uncovering evidence, prosecuting perpetrators, and safeguarding the integrity of financial systems. Through rigorous investigative efforts and the integration of digital forensic findings into legal proceedings, authorities can achieve accountability, deter fraudulent activities, and uphold the rule of law in combating financial fraud.

V. REFERENCES :

[1] Digital Forensics by Dr. Neelakshi Jain and Dr. Dhananjay Kalbande. Wiley Publications .

[2] https://www2.deloitte.com/us/en/pages/advisory/articles/forensic-analytics-in-fraud-investigations.html

[3] https://www.business-standard.com/about/what-is-pnb-scam

[4] https://www.kroll.com/en/insights/publications/forensic-data-analysis-of-mobile-devices

[5] https://en.wikipedia.org/wiki/Punjab_National_ Bank_Scam