Android Mobile Device Forensic Investigation

for Cyber Crime Analysis

Name: -Deepanshu Semwal
FIELD: -BTECH CSE CYBER SECURITY
YEAR: -2026

***Disclaimer:**
This project uses only publicly available data for educational purposes. No unauthorized access or illegal activity was performed.

Self-Declaration

I, **Deepanshu Semwal**, hereby declare that this project entitled **"***Android Mobile Device Forensic Investigation for Cyber Crime Analysis***"** is my original work and has been carried out by me as a **self-initiated project**. This project is based on my own research, learning, and understanding of concepts related to **cybersecurity, digital forensics, and online investigation**.

I further declare that this project has not been submitted previously to any university, institution, or organization for the award of any degree, diploma, or certification. All the information, data, and references used in this project have been properly acknowledged wherever applicable.

I take full responsibility for the authenticity and originality of the content presented in this project.

Name: Deepanshu Semwal
Course: B.Tech (CSE – Cybersecurity)
Date: 03-JANUARY-2026

Acknowledgement

I would like to express my sincere gratitude to my respected faculty members for their guidance and support during the completion of this self-initiated project. Their academic input and encouragement helped me in understanding and applying the concepts related to digital forensics and cyber investigation.

This project was carried out as a self-learning initiative inspired by the objectives and learning framework in the field of Cyber security. Through this work, I was able to enhance my research, analytical, and technical skills, particularly in the area of cybersecurity and online investigation.

I am also thankful to my friends and peers for their motivation, discussions, and support throughout the project work. Lastly, I would like to express my heartfelt gratitude to my parents and family for their constant encouragement, patience, and moral support, which played an important role in the successful completion of this project.

Name: Deepanshu Semwal
Course: B.Tech (CSE – Cybersecurity)
Project Type: Self-Initiated Project
Academic Year: *2026*

Table of Contents

• Abstract

- Smartphones are now the **primary source of digital evidence** in cyber-crime investigations.
- Android dominates the global market, making it the most common target for fraud, phishing, harassment, and identity theft.
- This project simulates a forensic investigation of an Android device, covering:
    - Evidence identification
    - Preservation
    - Extraction
    - Examination
    - Analysis
    - Reporting
- The methodology aligns with **IFSO standards** and emphasizes **legal admissibility** of digital evidence.

• Introduction

- **Digital Forensics**: The science of collecting, preserving, analysing, and presenting digital evidence in a legally admissible manner.
- **Mobile Forensics**: A branch of digital forensics focusing on smartphones and tablets.
- **Why Android?**

  Open-source → easier for attackers to exploit.

  Largest user base worldwide.

  Stores sensitive data: banking apps, chats, call logs, location history.

- **Challenges:**

i. Encryption and app sandboxing.

ii. Deleted data recovery.

iii. Variety of devices and OS versions.

- **Goal of Project**: To demonstrate forensic methodology on Android devices in a simulated academic environment.

• Objectives of the Project

The primary objectives of this academic project are:

1. To understand and implement the **standard operating procedures (SOPs)** for Android mobile device forensic investigation.
2. To **identify, preserve, and collect** volatile and persistent digital evidence from an Android smartphone using forensically sound methods.
3. To perform **in-depth analysis** of extracted mobile artifacts (SMS, call logs, app data, system files) to reconstruct events and establish links in a simulated cybercrime case.
4. To gain hands-on experience with **industry-recognized forensic tools and techniques** for logical and file system acquisition.
5. To comprehend the **legal, ethical, and chain-of-custody requirements** essential for maintaining the integrity and admissibility of digital evidence in legal proceedings.

• Case Scenario (Simulated)

A victim, "Mr. A," reports to the authorities that he has been receiving a series of suspicious SMS messages purporting to be from his bank, urging him to click on a link to "update his KYC details." Upon clicking, he was redirected to a fraudulent website mimicking his bank's portal, where he entered his login credentials. Subsequently, he noticed multiple unauthorized transactions from his account. Mr. A's Android smartphone (a device running Android 11) is identified as the primary vector of the attack and is seized as evidence. The forensic investigation aims to:

- Confirm the presence and content of the **phishing SMS**.
- Identify any **malicious applications** that may have been installed.
- Examine **browser history** for the fraudulent URL.
- Recover any **related communication** (e.g., WhatsApp messages coordinating the fraud).
- Establish a **timeline of events** using system logs and file metadata.

***(Note: This is a simulated case study created for academic purposes. All data used is synthetic, generated in a lab environment with no connection to real individuals or incidents.)**

• Evidence Identification

Based on the case scenario, the following potential digital evidence is identified on the seized Android device for examination:

a) **SMS and MMS messages:** For phishing message content, sender numbers, and timestamps.

b) **Call logs:** To identify any suspicious calls from unknown numbers around the time of the incident.

c) **WhatsApp chat data:** A potential channel for fraud coordination or social engineering.

d) **Images and videos:** Screenshots of banking apps, transaction alerts, or images containing sensitive information.

e) **Browser history:** To locate the visited fraudulent phishing URL and search history related to banking or fraud.

f) **Installed applications:** To identify the presence of malicious apps, fake banking apps, or remote access tools.

g) **Device information and system logs:** Critical for context, including:

- **Device Identity:** IMEI, serial number, model, phone number (to link device to user/carrier).
- **System State:** OS version, root status, screen lock status, last boot time.
- **Account Information:** Google account(s) logged in, which can link the device to a specific individual and cloud data.
- **Network & Connectivity:** WIFI SSIDs historically connected to, Bluetooth pairings (to place the device in a location).
- **Usage Statistics (**usage stats**):** Detailed logs showing which applications were in the foreground/background and for how long, crucial for creating an activity timeline.
- **Event Logs:** Records of app installations/uninstallations, screen on/off events, and battery state changes.

• Evidence Preservation

Immediate preservation actions are taken to prevent evidence tampering or remote wiping:

- The device is immediately isolated from all networks: **Airplane mode is enabled**, and the device is placed inside a **Faraday bag** to block all cellular, Wi-Fi___33, Bluetooth, and NFC signals.
- Physical examination is conducted to document the device's make, model, condition, and any connected peripherals (SIM, SD card).
- If the device is on, its state is documented (screen locked/unlocked, running apps). It is kept powered on to prevent activation of lockout mechanisms. If off, it is **not powered on** without proper isolation equipment.
- A **forensic hash (MD5/SHA-1/SHA-256)** of the acquired data image is calculated and documented to serve as a digital fingerprint, proving the evidence's integrity from the point of acquisition.
- A detailed **Chain of Custody (CoC) form** is initiated, recording every person who handles the device, the date, time, and purpose of handling, ensuring evidence integrity is legally verifiable.
- The core principle of **"no write" operations** is followed; the examiner's tools and methods must not alter the original data on the device.

• Evidence Collection Methodology

1 Logical Acquisition

Using **Android Debug Bridge (ADB)** with appropriate authorization (e.g., USB debugging enabled on the device), a logical extraction was performed. This method extracts files and folders accessible to the user without rooting the device. Data acquired includes:

- Contacts, SMS/MMS databases.
- Call log records.
- Media files (photos, videos) in standard directories.
- Application data folders for installed apps (subject to app-level encryption and permissions).

2 File System Acquisition

A more comprehensive extraction was performed to obtain a lower-level view. Using ADB and backup features or forensic tools, a file system dump was acquired. This provides access to:

- System directories (/data/system/, /data/log/).

- Application databases and shared preferences files.
- File system metadata (timestamps).
- Deleted data remnants from unallocated space (if the file system image is complete). The resulting **forensic image (e.g.,** .dd **or** .bin **file)** is mounted as a read-only drive in the analysis workstation.

• Tools Used

All tools were used in an isolated, offline lab environment for academic simulation:

- **Autopsy (The Sleuth Kit):** Primary forensic platform for analysing the acquired forensic image. Used for file system browsing, keyword searching, hash filtering, timeline analysis, and report generation.
- **FTK Imager:** Employed for creating forensic disk images of external SD cards (if present) and verifying image integrity via hash verification.
- **Android Debug Bridge (ADB):** Command-line tool for communicating with the Android device, enabling backup operations, and pulling files for logical acquisition.
- **SQLite Database Browser:** Used to manually examine and query the internal structure of application databases (e.g., mmssms.db, calllog.db, wa.db for WhatsApp) extracted from the device, allowing for recovery of deleted records and complex SQL queries.
- **HxD Hex Editor:** For low-level examination of specific files and searching for raw data patterns.

• Examination and Analysis

The forensic image was loaded into **Autopsy** for systematic examination:

- **Keyword Searches:** Searches were conducted for terms like "bank," "KYC," "update," "OTP," "transaction," the victim's bank name, and common phishing phrases.
- **Timeline Analysis:** File system timestamps (MAC times) and log entries were consolidated to create a visual timeline of device activity, correlating SMS receipt times with browser sessions and app usage.
- **Artifact Carving:** Tools within Autopsy were used to carve and reconstruct files from unallocated space.
- **Database Analysis:**

    - The mmssms.db was examined, revealing the full content, phone number, and timestamp of the phishing SMS.
    - The browser history database was queried, confirming a visit to the fraudulent URL with a timestamp shortly after the SMS was received.
    - The usage stats database was parsed, showing the messaging app and browser app were active in sequence, supporting the victim's statement.
- **Application Analysis:** The list of installed apps (packages.xml) was reviewed. No obvious malicious APK was found, indicating a **web-based phishing attack** rather than a malware-based one.

• Findings

The forensic analysis corroborated the victim's complaint and yielded the following key findings:

1. **SMS Evidence:** A specific SMS from an unknown number (+91XXXXXX) was identified, containing a phishing link, received on [Simulated Date & Time].
2. **Browser Evidence:** The browser history contained an entry for the exact phishing URL, accessed approximately 2 minutes after the SMS was received. The URL was analysed and found to be a non-secure (HTTP) site with a domain name masquerading as the legitimate bank.
3. **Timeline Correlation:** The usage stats and event logs confirmed the "Messages" app was active at the time of the SMS, followed immediately by the "Chrome" browser app, creating a coherent sequence of events.
4. **No Malicious App Found:** The investigation did not find evidence of a malicious application install, focusing the attack vector on SMS phishing (smishing).
5. **Device Context:** The device was not rooted, had a screen lock enabled, and was logged into the victim's personal Google account, strengthening the attribution of activity to the device owner.

• Legal Aspects

The investigation was conducted with strict adherence to legal protocols:

- **Information Technology Act, 2000:** The acts fall under relevant sections:

    - **Section 43:** Damage to computer/computer system (unauthorized access).
    - **Section 66C:** Identity theft (using the victim's banking password).
    - **Section 66D:** Cheating by personation using computer resources (impersonating the bank).
- **Indian Penal Code, 1860:**
    - **Section 419:** Punishment for cheating by personation.
    - **Section 420:** Cheating and dishonestly inducing delivery of property (fraudulent transactions).
- **Chain of Custody:** The maintained CoC form provides a legally auditable trail for the evidence.
- **Admissibility:** The use of forensically sound methods, hash verification, and detailed documentation ensures the digital evidence meets the standards of **Section 65B of the Indian Evidence Act, 1872**, for admissibility in electronic form.

• Conclusion

This project successfully demonstrates that Android mobile forensic investigation is a **critical, multi-disciplinary process** essential for solving cybercrimes. By applying a structured methodology—from isolation and preservation to deep artifact analysis—investigators can uncover a compelling digital narrative. The simulated case confirmed the phishing attack vector, provided concrete evidence (SMS, URL), and established a trustworthy timeline. The project underscores that technical proficiency must be coupled with **rigorous procedural discipline** and **legal awareness** to transform raw device data into credible, court-admissible evidence. As criminals increasingly exploit mobile platforms, the role of systematic mobile forensics will only grow in importance for law enforcement and cybersecurity professionals.

• Future Scope

The field of mobile forensics continues to evolve, presenting several areas for future work:

- **Advanced Tool Development:** Overcoming challenges posed by **device encryption**, **hardware security modules (e.g., Titan M)**, and locked bootloaders.
- **Cloud Forensics Integration:** Expanding investigations to include data synchronized with **Google Drive, iCloud, WhatsApp Web/Desktop, and other cloud services**, which often hold critical evidence not stored locally.

- **IoT and Wearable Forensics:** Extending methodologies to companion devices like smartwatches, fitness trackers, and IoT hubs that contain complementary data.
- **AI & Machine Learning Assisted Analysis:** Implementing AI to automate the parsing of massive datasets, identify hidden patterns in communication, detect anomalies in app behaviour, and predict potential evidence locations, thereby reducing analyst time and human error.

➢ References

- **Books & Standards:**
  - "Android Forensics: Investigation, Analysis and Mobile Security for Google Android" by Andrew Hoog.
  - NIST Special Publication 800-101 Rev. 1, "Guidelines on Mobile Device Forensics."
  - National Institute of Justice (NIJ), "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors."
- **Legislation:**
  - The Information Technology Act, 2000 (India).
  - The Indian Evidence Act, 1872 (Amended).
  - The Indian Penal Code, 1860.
- **Academic & White Papers:**
  - Research papers from journals like *Digital Investigation*, *Journal of Forensic Sciences*.
  - Technical white papers from Cellebrite, Oxygen Forensics, and Magnet Forensics.
- **Online Resources:**
  - Android Developers Documentation (for file system structure).
  - Forensics Wiki for tool and technique references.
  - Official documentation for Autopsy, ADB, and SQLite.

*** Disclaimer:** ***This report documents a project conducted in a simulated, academic environment. All data was artificially generated for educational purposes. The methodologies described are for learning and should be applied in real investigations only by trained professionals under appropriate legal authority.***