

Android Mobile Artifacts: A Treasure Trove of Digital Evidence in Crime Investigation

Nagendar Rao Koppolu

Inspector of Police (In-charge State Cyber Vertical), Telangana Police Department, Hyderabad

Abstract: Every action performed by the user on a mobile device leaves a trail. Phone call records, location details, recorded media, browser history, emails, text messages leave footprints. It contains a sizeable amount of evidence if the device is involved in a crime. Nowadays, most crimes involve mobile phones either as a tool or a target. Data extracted from these devices can be used as forensic evidence, an essential component in crime investigation. This paper discusses the evolution of mobile phones and their operating systems and potential evidence traces, important artifacts for investigation. This paper also briefs each step guided to perform mobile forensic analysis.

Keywords: Mobile Forensics, Digital Forensics, Forensic Investigation, Mobile Artifacts

1. INTRODUCTION

Mobile devices can make and receive telephone calls, send and receive messages, access the internet, etc., using radio frequency while being mobile (in movement) within a mobile service zone. Mobile devices establish a connection to mobile operators through mobile signal towers installed across the service zone. These mobile signal towers, in turn, connect to PSTN (public switched telephone network) [2]. Mobile devices are called cell phones or cellular phones because the networks are divided into various cells to signal the end-user devices better.

Mobile devices or cell phones provide multiple services: wireless telephone communication, text messaging, emails, MMS, Internet access, photography, and other applications. Mobile phones are also called smartphones because they provide multiple additional features to the end-user and their fast data processing capabilities. Over time, mobile phones have evolved from 1G to 5G, providing high-speed broadband internet connectivity and mobile telephony. As a result, Mobile device usage has become a part of our life over the last two decades.

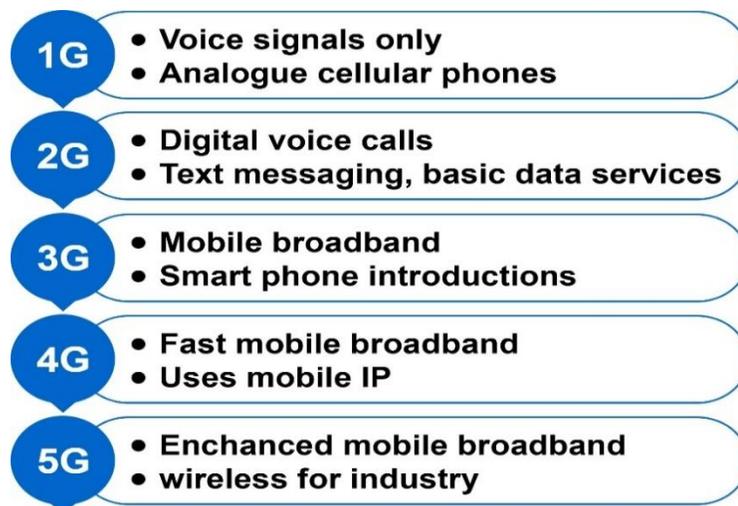


Fig - 1: Evolution of mobile technologies

The evolution of mobile phones includes everything from voice and video communication, messaging to MMS and emails, photography to gaming, personal use applications to business applications, wireless communication to internet access [3]. Advancements in mobile phone technology-facilitated criminals to use mobile phones to commit criminal activities [5]. At the same time, the plethora of new smartphones, improvements in technology, and high-security standards made the smartphone investigation critical. Therefore, standard procedures need to be followed during an investigation to maintain the integrity of

evidence [4]. The investigating officer must know the different acquisition methods and the complexities involved while handling the digital data during analysis. Here, the accessibility of data depends on the operating system, security features, and the make and model of the device.

Mobile Operating System:

Mobile Operating system (OS) manages a mobile device's hardware and software resources, input and output commands, memory utilization for efficient communication [4]. The OS is a base on which applications are loaded for usage. Android and iOS are the most widely used mobile operating systems in the market today.

2. Android OS

Google's Android operating system (OS) was initially developed with Linux kernel. Android can be defined as a software program stack with a set of software subsystems useful for the functioning of mobile devices. This stack includes a working system, middleware based on Java programming, and critical apps such as accessing the internet using a browser and a contact manager [5].

The main reasons for Android popularity are-

- a) *Free*: Android is a free OS because many smartphone vendors use Android OS on their phones.
- b) *Open-Source*: Android is an open-source system, and it is under continuous development.
- c) *Customizable*: Android is easily customizable. Users can easily customize the operating system according to their requirements.
- d) *Apps*: Over 2 million apps are available in the google play store to download and install on the android device.

2.1 Android architecture:

The android architecture contains a different number of components to support any android device needs. Android software contains an open-source Linux Kernel with several C/C++ libraries exposed through application framework services. Linux Kernel provides the main functionality of the operating system and Dalvik Virtual Machine (DVM) provides a platform for running an android application [1].

The main components of the android architecture are:

- Applications
- Application Framework
- Android Runtime
- Platform Libraries
- Linux Kernel

The android architecture is depicted graphically, with various primary components and their sub-components:

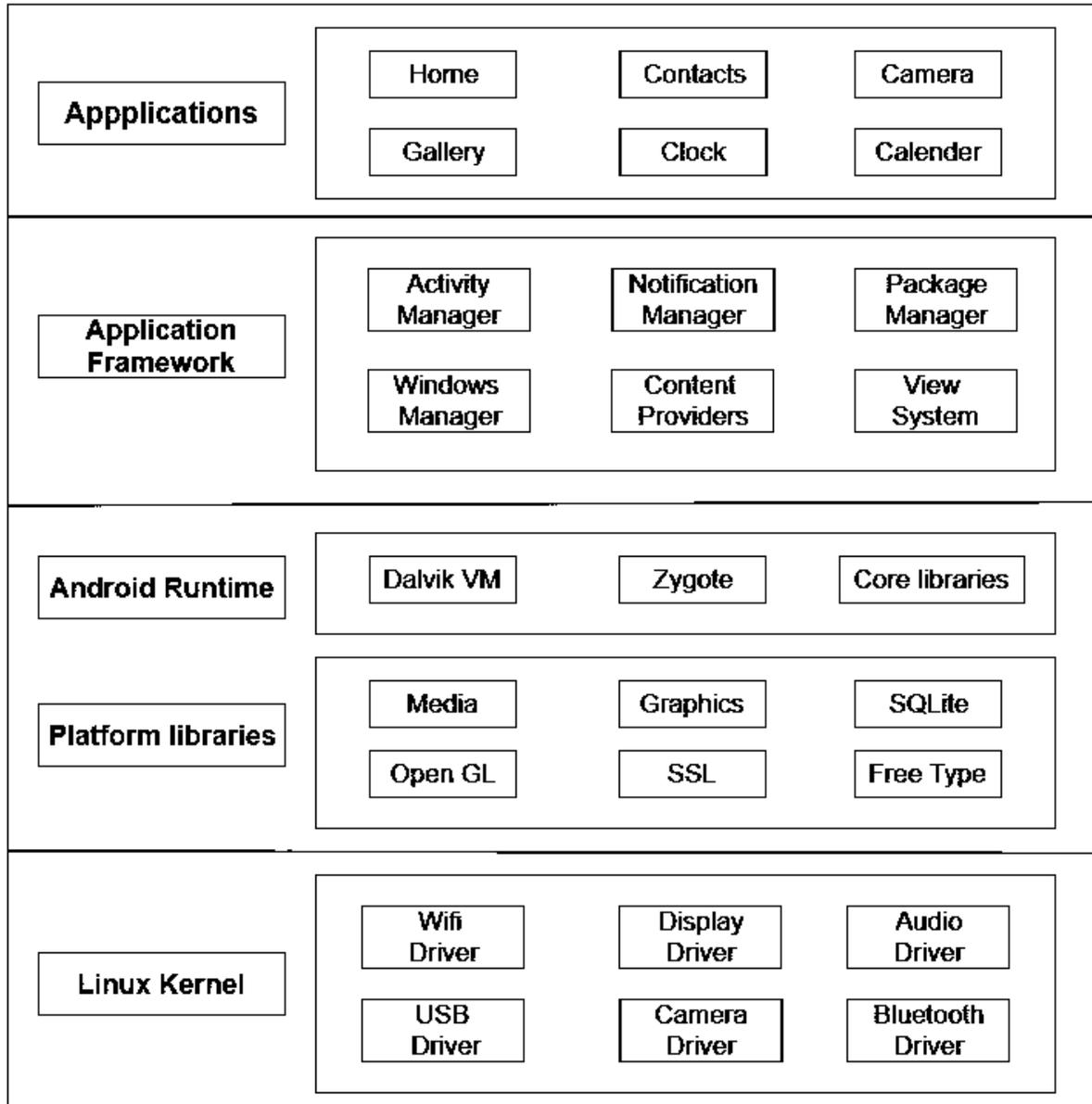


Fig - 2: Android five-layered architecture (Source: <https://www.geeksforgeeks.org/android-architecture/>)

2.1.1 Applications:

Applications are on the top layer of android design. This layer presents pre-installed applications such as home, contacts, camera, display, and outsider applications such as travel applications, games, etc., are shown on this layer. It works in the Android run time with the assistance of the classes and administrations given by the application structure [6].

2.1.2 Application framework

Application Framework gives a few significant classes which are utilized to make an Android application. It provides a general idea for hardware access and helps manage the UI with application resources [7]. Generally, it provides the services with the help of which we can create a particular class and make that class helpful for the Applications creation. With the assistance of a framework, we can make a specific class and make that class accommodating for the Application creation.

2.1.3 Application runtime

Application Runtime consists of central libraries and Dalvik virtual machine (DVM); it provides the base for the application framework and starts the android application with the help of the central libraries. Like Java Virtual Machine (JVM), Dalvik Virtual Machine (DVM) is a register-based virtual machine for Android. The central library empowers android applications to execute the standard JAVA or Kotlin programming language.

2.1.4 Platform libraries

The Platform Libraries incorporates different C/C++ central libraries and Java-based libraries. For instance, Media, Graphics, Surface Manager, OpenGL, etc., offers help for android improvement [4].

The following is the brief of some core android libraries available:

1. The Media library supports record and playback of audio and video file formats.
2. The surface manager is responsible for managing access to the touch screen display subsystem.
3. SGL and OpenGL are both useful for 2D and 3D graphics.
4. Web-Kit is an open-source web browser engine to process and display web content and simplify page loading.
5. SSL (Secure Sockets Layer) is a communication technology to establish an encrypted link between a web client and a web server.

2.1.5 Linux Kernel

Linux Kernel is the heart of Android. It deals with each of the accessible drivers, such as camera drivers, Bluetooth, sound, memory, etc., which are required during the runtime. The features of the Linux kernel are:

- Security: The Linux kernel handles the security between the application and the system.
- Memory Management: Kernel handles memory management effectively by monitoring all the running apps and freezing or closing unused ones.
- Process Management: Kernel manages the process and allocates resources to processes.
- Network Stack: handles the network communication.
- Driver Model: Kernel ensures that the Operating system and application works properly on the device. Hardware manufacturers are responsible for building their drivers into the Linux Kernel.

2.2 Features of Android Operating System:

The Android operating system has the following features:

- *Near Field Communication (NFC)*: NFC allows electronic devices to interact and share data across very short distances easily. The main aim here is to develop a payment alternative that is more convenient than carrying credit cards or cash.
- *Alternate Keyboards*: Android supports multiple keyboard applications and makes them easy to install through the play store. E.g., SwiftKey, Mint keyboard.
- *Infrared Transmission*: Android operating system supports controlling other devices like home appliances using android devices with a built-in infrared transmitter.
- *No-Touch Control*: Android app Wave Control helps users to control their phones without touching the screen, using only gestures.
- *Automation*: Apps like tasker and automate can automate various tasks on android devices. One can automate any aspect of their android device. It can automatically change device settings like enabling or disabling Bluetooth, Wi-Fi, NFC, or performing actions like sending SMS, email-based on the device's location, time of day, or any other trigger event set by the user.
- *Wireless App Downloads*: Downloading an app to a mobile device does not need a computer to be connected; apps can be downloaded directly to the device using the play store.
- *Custom Home Screens*: the main screen users view after unlocking their android device is the home screen. The home screen can be customized by adding new shortcuts to installed apps, webpages, widgets. Users can also change the home screen using third-party themes on android devices.

- *Widgets*: widgets provide information on the home screen itself instead of opening the App itself. Android widgets can display information from weather apps, music players, or productivity tools like calendars, notes, or email notifications that remind us of upcoming events [9].
- *Custom ROMs*: Android being an Open-Source Operating System, it can be customized as per one's requirement. A customized version of the Android Operating System by individual developers is called a custom ROM. Generally, custom ROMs are created to enhance the usability or provide specific functionality missing in the OEM software.
- *Ultra-data saver mode*: Mobile data consumption can be reduced by compressing and limiting individual applications' data usage.

Android Version with New Features are added in the following Table:

Table- 1: Android release versions

Version Name	Key User Features Added
Android 1.0 (Apple pie)	Download and update apps via android market, camera support, google maps, YouTube application, web browser.
Android 1.1 (Banana Bread)	Show and hide numeric keyboard in caller application, ability to save MMS attachments.
Android 1.5 (Cupcake)	Bluetooth, soft keyboard with keyword predictions, record/watch videos.
Android 1.6 (Donut)	Gesture work turn-by-turn navigation
Android 2.0, 2.0.1, 2.1 (Eclair)	HTML, digital zoom, live wallpapers, updated UI, Microsoft exchange support
Android 2.2 (Froyo)	Speed improvements, apps installation to the expandable memory, upload file support in the browser, animated GIFs
Android 2.3, 2.3.3, 2.3.4, 2.3.5, 2.3.6, 2.3.7 (Gingerbread)	There are social networking features, near field communication on support, native VoIP/SIP support, video call support, voice, and video chats with google talk.
Android 3.0, 3.1, 3.2, 3.2.1, 3.2.2, 3.2.4, 3.2.6 (Honeycomb)	Updated 3D UI, customizable home screen, recent application viewing, media/picture transport protocol, google talk video chat, google eBooks, private browsing, HTTP live streaming, media sync from SD card
Android 4.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4 (Ice cream sandwich)	Lock screen actions, email app support, facial recognition, better voice recognition, smoother screen rotation
Android 4.1, 4.1.1, 4.1.2, 4.2, 4.2.1, 4.2.2, 4.3 (Jellybean)	Voice search, accessibility: gesture mode, enabled home screen rotation, lock screen widgets, multi-user for tablets, dial pas auto-complete, 4k resolution support,
Android 4.4, 4.4.1, 4.4.2, 4.4.3, 4.4.4 (KitKat)	Screen recording, enhanced notification access, new translucent system UI
Android 5.0, 5.0.1, 5.0.2, 5.1 (Lollipop)	Multiple SIM support, device lock protection if misplaced, quick settings: shortcuts to join Wi-Fi networks or control Bluetooth devices
Android 6 (Marshmallow)	USB Type-C support, fingerprint authentication and support, app permission management updates
Android 7.0, 7.1, 7.1.1, 7.1.2 (Nougat)	Daydream virtual reality mode, night light, option to enable fingerprint swipe down gesture, battery usage alerts

2.3

Android 8.0, 8.1 (Oreo)	PIP with resizable window, auto light and dark themes, show battery in quick settings for devices connected via Bluetooth
Android 9 (pie)	User interface updates, richer message notification, power option now has a screenshot button biometric authentication can now be disabled only once.
Android 10	Require permission to access location or files in the background, access system settings directly from apps using floating panel, dark theme, gesture navigations
Android 11	5G app support, screen recording, better permission settings

Android Partitions:

Android uses multiple partitions to organize files and folders in the device, and directories represent partitions. Mainly six partitions are used by Android devices, and each partition has its functionalities. Other partitions differ in each model, such as sd card, sd-ext, etc.

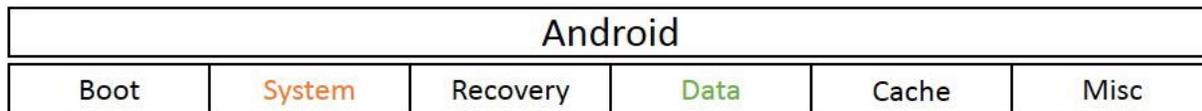


Fig - 3: Android Partitions

2.3.1 /boot

Boot partition of the Android device that includes the Android kernel and ramdisk. The device cannot boot without this partition. This partition should only be wiped if a new Android ROM is being installed immediately.

2.3.2 /system

Android GUI and all the system applications that come pre-installed along with the ROM. This partition contains the entire Android OS except for the kernel and the RAM disk. Wiping this partition will remove Android OS from the device, and the device can only boot into recovery or bootloader mode to install a new ROM [10].

2.3.3 /recovery

It can be considered an alternative boot partition that can perform device recovery if the Android ROM is corrupt or wiped and performs maintenance operations like taking a backup of the Android partitions or restoring the data to the device.

2.3.4 /data

It is also referred to as User data partition. This partition contains the user's data like contacts, SMS, multimedia files, settings, and Android applications. This partition will be wiped when a factory reset is performed. This partition is crucial for retrieving evidence for the investigator.

2.3.5 /cache

Stores frequently accessed data related to the apps installed on android devices. This data is not critical for the Android device's performance or the apps installed, and it can be wiped as and when needed.

2.3.6 /misc

It contains miscellaneous system settings like carrier, region, USB connection configuration in the form of on/off switches. This partition is crucial for the device's functionality and should not be wiped.

2.3.7 /sdcard

It is the internal storage of the android device. It stores all the user media like images, audio, video, documents, app data. This partition is crucial for retrieving evidence for the investigator.

2.4 Android File System

The File system is used to define how data is stored and retrieved on the device. Android uses Linux kernel with support for many file systems. Each file system is an implementation of VFS (Virtual File System). The investigator should understand the most important of them. The Android File Systems are divided into Flash Memory File Systems and Media Based File Systems [1].

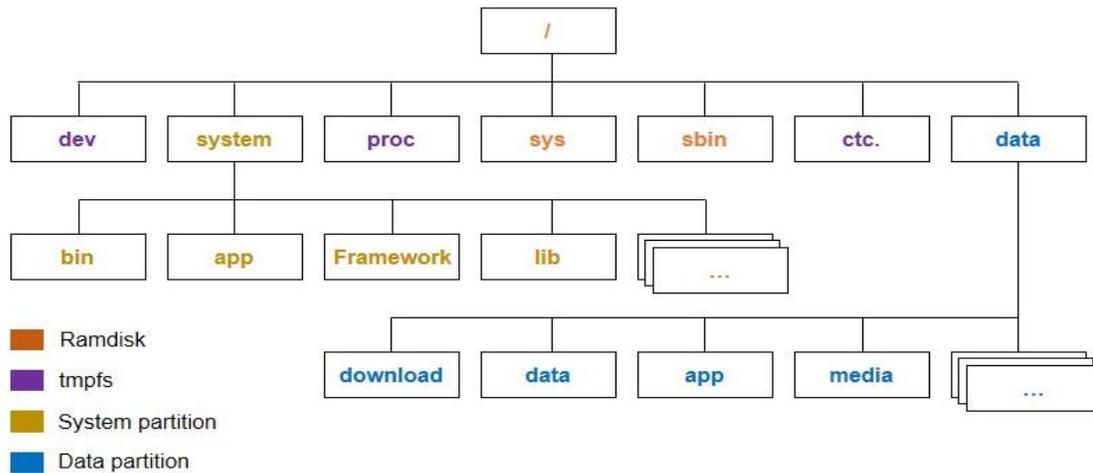


Fig - 4: Android File System

3. Mobile Storage

Mobile artifacts are stored in different locations of the device. Preservation and extraction of data from the memory locations need to be done with care using write-protected equipment to maintain the integrity of the data; every bit of data is valuable during the investigation; therefore, the following data containers should be analyzed [4].

3.1 Subscriber identity module (SIM)

SIM card stores crucial data like phone number, location, user identity, contact lists and stored messages for GSM cellular subscribers.

3.2 Cloud Storage

Cloud storage is free and can be accessed anytime; once a device logged in using Google ID or Apple ID, a dedicated amount of space is given to the user. It can be used for storing multimedia content, application-related backups, synchronize newly added content. Nowadays, most of the data is stored in cloud space, analyzing cloud data has become a significant challenge for investigators.

3.3 Mobile Phone Internal Memory (NAND Flash)

Most of the Mobile artifacts are found in the internal memory of the mobile phone. The internal memory of a mobile phone is also called primary, and it has direct access to the processor. NAND-type flash memory, usually non-volatile, is used in mobile devices. Data about applications, contact list, call history, media files; all the data is stored in NAND flash of the phone; the investigator's honeypot will investigate NAND flash.

3.4 Mobile Phone External Memory (SD and MicroSD card)

The external memory of a mobile phone is also called a secondary memory, and the mobile phone's processor does not directly access it. Still, it uses the input/output channels to access the secondary memory. Usually, this space is used as an expandable memory slot, and it changes according to the manufacturer. Multimedia artifacts and mobile backups can be found in the external memory of the mobile phone. In some instances, the external memory card data can be in encrypted form. In that case, insert the memory card into another device and decrypt it with the password key in another phone. An investigator must not make changes to the original device, so it is always suggestible to use an alternative phone to unlock the encryption on-chip level [1].

4. Android Forensic and Mobile Artifacts

Android forensics is dependent on the degree of access provided by a device, which defines the level or depth of data that an investigator may retrieve. An Android operating system offers two levels of user access control: rooted access and non-rooted access. Because the Android operating system does not provide users administrative or root access, devices are produced with non-root access [3].

Forensic Investigation needs in-depth recovery of artifacts for complete analysis. A rooted device allows total extraction of user data as well as access to the system partition. The system partition stores complete application knowledge, computer storage, and system files. For a non-rooted user, folders like partitions and system folders are hidden with no user access.

Root Checker may be a straightforward application that lets us check if the device is rooted in a matter of seconds. This suggests that Root Checker does not facilitate rooting the device; however, it merely informs its state.

Mobile artifacts are the traces, or the footprints left behind by the criminal unconsciously or accidentally, that are important proof throughout the investigation procedure. Each action performed on a mobile leaves a print because the criminal is unaware that it helps the investigating officer (IO) induce a deeper understanding of the criminal activity.

Artifacts extracted from the mobile devices vary from device to device based on the make and model, OS version, and most significantly, whether it's a smartphone or a keyboard (feature) phone. These artifacts are sensitive, and even tiny changes will tamper with the data in them. To avoid such things, digital devices should be confiscated as early as possible, and there are possibilities of information being overwritten if the device is not handled correctly.

Table - 2: Mobile Artifacts that can be extracted from Feature phones

List	Artifacts
Hardware	Make and model, IMEI number, serial number
User-created	Contact list, SMS and MMS (sent, received, drafted, deleted), calendar, Notes
Device created	Call logs (dialled, received, missed, deleted)

Table - 3: Mobile Artifacts that can be extracted from a smartphone

List	Artifacts
Hardware	Make and model, IMEI number, serial number
User-created	Contact list, SMS & MMS (sent, received, drafted, deleted), calendar, notes, media files (photos and videos), maps, voice recordings
Device created	Call logs (dialled, received, missed, deleted)
Internet artifacts	Online accounts, browser data, social media content, emails, etc.,
Installed application data	Chat logs, parallel apps, e-commerce application data, etc.,

4.1 Important Directories & Files for Mobile artifacts:

/data/data - Apps data is generally installed in a subdirectory of this folder. For example, the default Android web browser is named com.Android.browser, the data files of this App are stored at /data/data/com.Android.browser.

SQLite is an open-source database format that is very widely used for structured data storage by many apps. SQLite databases are a rich source of forensic data. The SQLite files used by the apps are generally stored at /data/data/<ApplicationPackageName>/databases.

1. **Contact Artifact:** Information related to contacts can be found in Contacts2.db database file which is located at below path:
/data/data/com.Android.providers.contacts/databases/contacts2.db
2. **Call History Artifact:** Information related to incoming, outgoing, and missed calls can be found in calllog.db database file which is located at below path:
/data/data/com.Android.providers.contacts/databases/calllog.db
3. **SMS/MMS Artifacts:** Information related to text messages can be found in mmssms.db database file, which is located at below path:
/data/data/com.Android.providers.telephony/databases/mmssms.db
4. **SIM Artifact:** Information related to SIM can be found in the telephony.db database file, which is located at below path:
/data/data/com.android.providers.telephony/databases

Contains data for all SIM cards used in the device, including the ICCID, phone number (if it was stored on the SIM), and the MCC/MNC, which can be used to identify the network provider.

5. **Download Artifacts:** Information related to files downloaded from internet can be found in downloads.db database file which is located at below path:
/data /data/com.android.providers.downloads/databases/ downloads.db
6. **WhatsApp Artifacts:** Information about WhatsApp contacts can be found in the wa.db database file which is located at below path:
/data/com.whatsapp/databases/ wa.db
Information about chat messages on WhatsApp can be found in the msgstore.db database file, which is located at below path: /data/com.whatsapp/databases/ msgstore.db
7. **Facebook Artifacts:** Information about Facebook user profile can be found in prefs_db database file which is located at below path:
/data/data/com.facebook.katana/databases/prefs_db
Information about Facebook users' friends can be found in the contacts_db2 database file which is located at below path:
/data/data/com.facebook.katana/databases/contacts_db2
Information about messages on Facebook can be found in the threads_db2 database file which is located at below path:
/data/data/com.facebook.katana/databases/threads_db2

8. *Multimedia Artifacts - EXIF Metadata:*

Exif stands for Exchangeable image file format. Exif was created by the Japan Electronic Industries Development Association (JEIDA), and it specifies the formats for pictures, sounds, and supportive tags employed by digital cameras, smartphones. Data is found in many files, including JPEG, TIFF, MOV, WAV, and others. Exif data is data kept with the digital file invisible to the viewer. The data embedded among every photograph will cover a broad spectrum of data. The information contained in every picture is:

- a. **Date and Time:** Most digital cameras can record the current date and time.
- b. **Physical Location:** GPS-enabled cameras, particularly smartphones, will geotag photographs with actual GPS coordinates wherever the photo was taken.
- c. **Dimensions:** Image resolution, compression, breadth, and height (measured in pixels).
- d. **Variable Camera Settings:** Together with the shutter speed, exposure time, aperture size, distance, metering mode, ISO speed, and camera orientation (rotation) when the photograph was taken and whether or not a flash was used.
- e. **Fixed Camera data:** Like the build, model, serial variety, and if a lens was used, it should conjointly store data concerning the lens furthermore.
- f. **Thumbnail:** A smaller version of the first image is kept for fast viewing on the camera's digital display screen, file managers, and photograph manipulation software package.

Additional data that may be available with the photograph when it's been taken include:

- Description:* Text describing what the photograph was concerning.
- Keywords:* A photograph might be labelled with keywords for looking out later.
- Copyright data:* Photographers and Stock Photography websites need to shield their pictures to add copyright data to the image.
- Image Manipulation information:* Once a picture is modified from its original state, image manipulation software package, the software package manufacturer could insert their meta-information distinguishing what software package created the changes and UN agency made the changes.

5. How can investigators use retrieved Mobile artifacts for investigation purposes?

5.1 Mobile Device information:

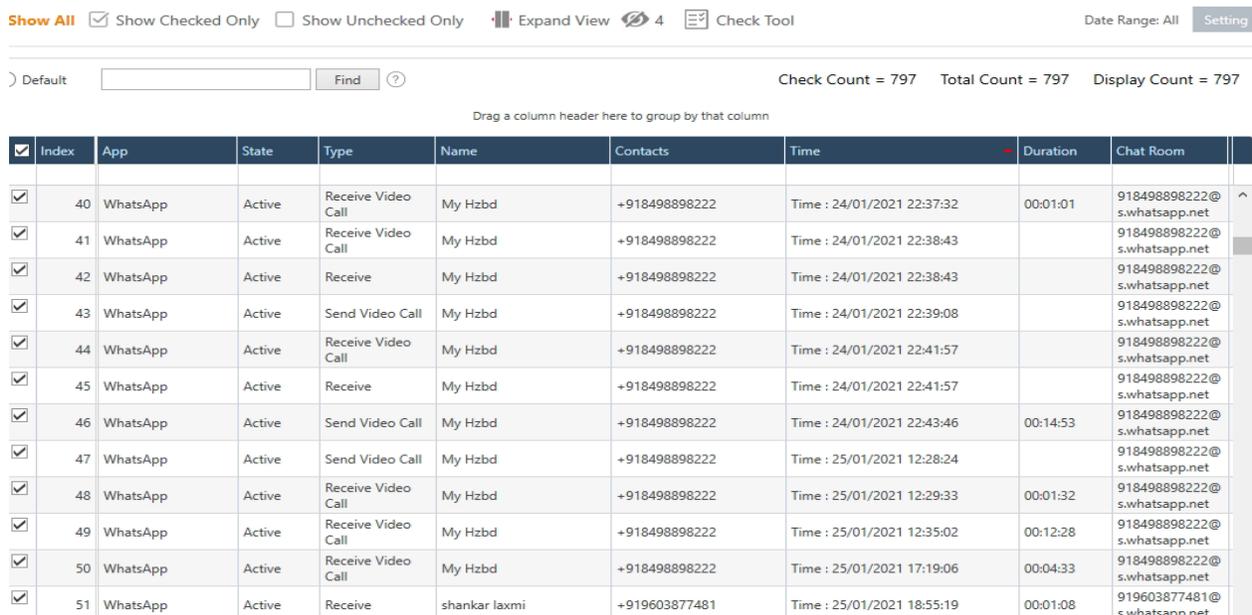
IMEI (International Mobile Station Equipment Identity) number is a number that identifies a device when it connects to a cellular network. If the phone has two SIM slots, it will have two IMEI numbers, one for each. The main purpose of the IMEI number is to identify the mobile device on the cellular network to prevent theft. Like computer MAC-address, IMEI number is hard-coded into the mobile, so nobody can modify them without damaging the device.

There are multiple ways to get the IMEI number from a mobile device. The easiest way to check the IMEI number on your phone is to open your keypad and then type *#06#, and it will immediately show your IMEI number on the mobile device screen. Another method to retrieve the IMEI number is to go to "Settings -> About Phone -> Status -> IMEI Information."

When a complaint regarding a stolen mobile device has been given to the service provider, they can blocklist the IMEI Number and trace it out. There are many websites similar to imei.info, where we can get exact specifications and information about the mobile device by entering the IMEI number of the device. On a website like imeipro.info, we can enter an IMEI number to check whether your phone has been blacklisted/reported as lost or stolen.

5.2 Application and communication data:

We use various Instant messaging and social media platforms like WhatsApp, Facebook, Linked In, Uber, Dropbox, and mobile dating applications where we share our data. Those applications can capture our contacts, call logs, messages, chats, emails, and social media account details. An investigator may use the above information to track down a person's relatives, friends, acquaintances, and adversaries. Investigators can use the information to build a network of a person's "close acquaintances," which can help investigate people's involvement.



Index	App	State	Type	Name	Contacts	Time	Duration	Chat Room
40	WhatsApp	Active	Receive Video Call	My Hzbd	+918498898222	Time : 24/01/2021 22:37:32	00:01:01	918498898222@s.whatsapp.net
41	WhatsApp	Active	Receive Video Call	My Hzbd	+918498898222	Time : 24/01/2021 22:38:43		918498898222@s.whatsapp.net
42	WhatsApp	Active	Receive	My Hzbd	+918498898222	Time : 24/01/2021 22:38:43		918498898222@s.whatsapp.net
43	WhatsApp	Active	Send Video Call	My Hzbd	+918498898222	Time : 24/01/2021 22:39:08		918498898222@s.whatsapp.net
44	WhatsApp	Active	Receive Video Call	My Hzbd	+918498898222	Time : 24/01/2021 22:41:57		918498898222@s.whatsapp.net
45	WhatsApp	Active	Receive	My Hzbd	+918498898222	Time : 24/01/2021 22:41:57		918498898222@s.whatsapp.net
46	WhatsApp	Active	Send Video Call	My Hzbd	+918498898222	Time : 24/01/2021 22:43:46	00:14:53	918498898222@s.whatsapp.net
47	WhatsApp	Active	Send Video Call	My Hzbd	+918498898222	Time : 25/01/2021 12:28:24		918498898222@s.whatsapp.net
48	WhatsApp	Active	Receive Video Call	My Hzbd	+918498898222	Time : 25/01/2021 12:29:33	00:01:32	918498898222@s.whatsapp.net
49	WhatsApp	Active	Receive Video Call	My Hzbd	+918498898222	Time : 25/01/2021 12:35:02	00:12:28	918498898222@s.whatsapp.net
50	WhatsApp	Active	Receive Video Call	My Hzbd	+918498898222	Time : 25/01/2021 17:19:06	00:04:33	918498898222@s.whatsapp.net
51	WhatsApp	Active	Receive	shankar laxmi	+919603877481	Time : 25/01/2021 18:55:19	00:01:08	919603877481@s.whatsapp.net

Fig - 5: Application and Communication Artifacts extracted from a smartphone

5.3 Multimedia:

If a criminal has taken a photo or video during or after a crime, any recorded Geodata can help forensic investigators pinpoint the crime scene's exact location. It is one of the most valuable pieces of information stored within the metadata of a digital photo. Suppose a kidnapper sends police a digital image of their captive as proof of life or record a ransom video with demands. Photo or video recorded with a GPS-enabled phone or camera will help the police quickly determine the exact GPS coordinates and helps in arresting the kidnapper.

Investigators can also track a stolen camera online using the camera's serial number, stored in the metadata when photos are taken from that camera and are uploaded to the internet. Further, Investigators might obtain the owner's information from the manufacturers via the make, model, and serial number they gathered from the photo metadata.

Table Gallery Check Count = 2,011 Total Count = 2,017 Display Count = 2,017

○ Default Find ?

Drag a column header here to group by that column

<input type="checkbox"/>	Index	App	State	Attr	Type	File Path	File Name	Preview	File Time
<input checked="" type="checkbox"/>	226	Default	Active	Normal	MPEG	/media/0/Android/data/in.mohalla.sharechat/files/videoCache/9	1927.98854.1616583887763.v3.exo	1927.98854.1616583887763.v3.exo	Modify Time : 24/03/2021 16:34:47 Access Time : 24/03/2021 16:34:47 Change Time : 24/03/2021 16:34:47 Play Time : 00:00:00
<input checked="" type="checkbox"/>	227	Default	Active	Normal	MPEG	/media/0/Android/data/in.mohalla.sharechat/files/videoCache/9	2016.63279.1616584181391.v3.exo	2016.63279.1616584181391.v3.exo	Modify Time : 24/03/2021 16:39:41 Access Time : 24/03/2021 16:39:41 Change Time : 24/03/2021 16:39:41 Play Time : 00:00:00
<input checked="" type="checkbox"/>	228	Default	Active	Normal	MP4	/media/0/Android/data/in.mohalla.sharechat/files/videoCache/9	1728.0.1616312474380.v3.exo		Modify Time : 21/03/2021 13:11:41 Access Time : 21/03/2021 13:11:14 Change Time : 21/03/2021 13:11:41 Play Time : 00:00:33
<input checked="" type="checkbox"/>	229	Default	Active	Normal	MP4	/media/0/Android/data/in.mohalla.sharechat/files/videoCache/9	1902.0.1616583609243.v3.exo	1902.0.1616583609243.v3.exo	Modify Time : 24/03/2021 16:30:09 Access Time : 24/03/2021 16:30:09 Change Time : 24/03/2021 16:30:09 Play Time : 00:00:58
<input checked="" type="checkbox"/>	230	Default	Active	Normal	MP4	/media/0/Android/data/in.mohalla.sharechat/files/videoCache/9	1909.0.1616583757825.v3.exo	1909.0.1616583757825.v3.exo	Modify Time : 24/03/2021 16:32:37 Access Time : 24/03/2021 16:32:37 Change Time : 24/03/2021 16:32:37 Play Time : 00:00:19
<input checked="" type="checkbox"/>	231	Default	Active	Normal	MPEG	/media/0/Android/data/in.mohalla.sharechat/files/videoCache/9	1905.196737.1616583719465.v3.exo	1905.196737.1616583719465.v3.exo	Modify Time : 24/03/2021 16:31:59 Access Time : 24/03/2021 16:31:59 Change Time : 24/03/2021 16:31:59 Play Time : 00:00:00
<input checked="" type="checkbox"/>	232	Default	Active	Normal	MPEG	/media/0/Android/data/in.mohalla.sharechat/files/videoCache/9	1924.160670.1616583865802.v3.exo	1924.160670.1616583865802.v3.exo	Modify Time : 24/03/2021 16:34:25 Access Time : 24/03/2021 16:34:25 Change Time : 24/03/2021 16:34:25 Play Time : 00:00:00

Fig - 6: Multimedia Artifacts extracted from a smartphone

5.4 Internet history and email:

Criminal mobile device's internet history, internet bookmarks, internet cache, and emails are excellent sources of evidence for the investigator to prove the criminal's crime.

<input checked="" type="checkbox"/>	Index	App	State	Browser	Type	Time	Title	URL
<input checked="" type="checkbox"/>	180	Chrome	Active	Chrome	History	Create Time : 02/03/2021 19:04:24	New Punjabi Song 2021 Viah Ch Gaah (Full Song) Shivjot Ft Gurlej Akhtar Latest Punjabi Songs 2021 - YouTube	https://m.youtube.com/watch?v=oR00Fk_g6Dw
<input checked="" type="checkbox"/>	181	Chrome	Active	Chrome	History	Create Time : 02/03/2021 19:04:28	New Punjabi Song 2021 Viah Ch Gaah (Full Song) Shivjot Ft Gurlej Akhtar Latest Punjabi Songs 2021 - YouTube	https://m.youtube.com/watch?v=oR00Fk_g6Dw
<input checked="" type="checkbox"/>	182	Chrome	Active	Chrome	History	Create Time : 04/03/2021 11:32:42	Watching "made for kids" content - YouTube Help	https://support.google.com/youtube/bin/answer.py?answer=9632097&nohelpkit=1&hl=en
<input checked="" type="checkbox"/>	183	Chrome	Active	Chrome	History	Create Time : 04/03/2021 11:32:42	Watching "made for kids" content - YouTube Help	https://support.google.com/youtube/answer/9632097?nohelpkit=1&hl=en
<input checked="" type="checkbox"/>	184	Chrome	Active	Chrome	History	Create Time : 04/03/2021 18:08:14	Billiard Room - zisgames.com	https://gooleads.g.doubleclick.net/acik?sa=1&ai=C3zheb9RAYLbGO9SQ1Aagp7XYAvLdxxgjsb nmPkMireh3eEFAEg4_uTA2D16uMDoAGNzJ3gAcgBB qkCqKWCXsG2aD6oAwGqBNIBT9DyfbCGBiOUd9r4bN sOUSOJ3MgyI4ndK- iqVVvQFPeaGrEXFULTG0aAYGmt8mQGLR- Js9x7U3BsgEFc- W2RjLWicE8LdJX4a6cKPa1UWVybFzLxKcBL022deKFc PiKULunYaoLmVu5p5bYbDptfArvMmOJ302- yrxveU4wzH-

Fig - 7: Browser Artifacts extracted from a smartphone

5.5 Malware:

Similar to computer systems, mobile devices are also prone to malware attacks. Forensic tools can detect malware on mobile devices. Further, analysis can help uncover the malware's effect on the mobile device and understand if the criminal stole sensitive information from the device or if a third party was monitoring communications. Malware in mobile devices can be found when the physical extraction of the device is taken.

5.6 Backup and cloud data:

Because mobile devices are so portable, the danger of data loss rises if the mobile is stolen, lost, or malfunctions. Many people prefer to backup their device locally (to a PC) or backup their device to a cloud service to mitigate this danger. Using forensic techniques, we can retrieve more information from mobile cloud data than mobile devices as they store older mobile backups. Multiple previous backups may be saved and retrieved utilizing forensic techniques, allowing these backup locations to hold much more information. Massive server farms are commonly used to store this type of information. A criminal might store data on google drive, uses Amazon for massed computing tasks, and communicate through Gmail.

5.7 GPS location data:

For example, when a person is traveling, their mobile device could be connecting to roaming networks, Wi-Fi hotspots, cell site towers, etc. Each of these actions leaves a "footprint" of locations that a person has visited. Such information is precious to an investigation to track the locations of the crime event.

Depending on the device features, modern mobile devices such as smartphones, tablets, and portable navigation systems can save a history of a user's whereabouts for months or even years.

The most frequent source of position data retained in the device memory is information from the Global Positioning System (GPS). The GPS (Global Positioning System) determines the position of a GPS-enabled device by using satellites circling the planet. GPS is more precise than other sources of position data, and this information, including date and time, maybe shown on a map. An investigator can find the GPS location information from a photo's metadata; a video taken using a third-party app or navigation app loaded on the device. It is easy to image and triage the device to look for location data forensically, user settings, installed applications, and metadata if you have access to the device.

Path to access the location information is /data/com.google.android.apps.maps/databases

Start Date: 10/6/2018 ~ End Date: 3/28/2021 Search for targets regardless of date information.

○ Default Find ?

Drag a column header here to group by that column

<input checked="" type="checkbox"/>	Index	Type	State	Datetime	Coordinate	Latitude	Longitude	Range
<input checked="" type="checkbox"/>	13	Map	Active			18.9733194	78.7052778	
<input checked="" type="checkbox"/>	14	Map	Active			18.9733194	78.7052778	
<input checked="" type="checkbox"/>	15	Map	Active			18.9703694	78.704925	
<input checked="" type="checkbox"/>	16	Map	Active			18.9692917	78.7052778	
<input checked="" type="checkbox"/>	17	Map	Active			18.9731861	78.7053389	
<input checked="" type="checkbox"/>	18	Map	Active			18.9688889	78.7022556	
<input checked="" type="checkbox"/>	19	Map	Delete	06/10/2018 05:30:37		18.968734	78.705103	
<input checked="" type="checkbox"/>	20	Picture	Active	16/01/2021 00:07:55		18.9733428888889	78.7056350555556	
<input checked="" type="checkbox"/>	21	Media Log	Delete	16/01/2021 00:07:55		18.9733	78.7056	
<input checked="" type="checkbox"/>	22	Media Log	Delete	16/01/2021 00:07:55		18.9733427	78.7056345	
<input checked="" type="checkbox"/>	23	Picture	Unused	16/01/2021 00:08:29		18.9733428888889	78.7056350555556	
<input checked="" type="checkbox"/>	24	Media Log	Delete	16/01/2021 00:08:29		18.9733	78.7056	
<input checked="" type="checkbox"/>	25	Picture	Active	16/01/2021 00:08:46		18.9733428888889	78.7056350555556	
<input checked="" type="checkbox"/>	26	Media Log	Delete	16/01/2021 00:08:46		18.9733	78.7056	
<input checked="" type="checkbox"/>	27	Media Log	Delete	16/01/2021 00:08:46		18.9733427	78.7056345	

Fig - 8: GPS Location Artifacts extracted from a smartphone

5.9 Android general management and accessibility settings

Accessibility Options exist in various shapes and sizes, and many are specific to your device or Android version. There are standard Android Accessibility Option settings, such as TalkBack, text size, captions, and "touch and hold" delay time settings, that you'll find on most mobile devices, but there are many more. Accessibility Options are incorporated in Android for hard-of-hearing folks, have a vision disability, or have any other impairments that make using Android mobile devices more accessible for them. An investigator can look into it and find if a person has any impairment, and they can also reveal how good he is with the usage of the phone.

5.10 Data usage and Battery Usage for Investigator

The android smartphone is likely to have several apps, each of which consumes resources such as battery power and wireless data. Almost every App on your phone needs data to operate, whether it's over WIFI or cellular data; investigators observe which applications use the most data. An investigator can use simple tricks for tracking and finding out app usage stats, which apps are used more frequently, and which App uses the phone's resources.

- Go to Settings
- Go to "Network & internet" > "Data usage" > "Data warning & limit"
- Tap on "App data usage cycle."

Every App consumes some battery power, allowing the investigator to observe which apps use the most battery.

- Start the Settings App and tap "Battery."
- Tap "Battery Usage."

5.11 App Permission

App permissions describe which aspects of your device app will access when using or running in the background. It might be compulsory for some apps to allow the access permission of the camera, location, or media file of the device. Certain apps might not need access to your camera, but they don't work if permission is not allowed. We can provide some app access to mobile device cameras or contacts lists. Some apps will send a notification asking for permission to access the camera or gallery on the phone, and you may choose whether to allow it or not. In the phone's Settings, you can also adjust permissions for a specific app or by permission type.

There are various techniques that an investigator may follow while analyzing mobile applications to evaluate user data. An examination of the SQLite database linked with the App is part of the analysis. For example, Location permission is enabled for a particular App. In that case, the app stores information related to the approximate location of the user device, which can be

based on network provider (i.e., cell towers) or based on GPS. Understanding the permissions connected with an app enables the investigator to understand the types of evidence that may be sought from the service provider and the types of evidence to search for when analyzing the SQLite database.

5.11.1 Types of App Permissions

The following is the list of app permissions, which can be enabled or disabled on the mobile device.

- *Body Sensor permission*: This allows the application to access phone sensors and record data from the sensor.
- *Calendar permission*: This allows the application to access phone Calendar info.
- *Call Logs permission*: This allows the application to view and modify the phone's call history.
- *Camera permission*: This allows the application to access your device's camera and take images or record video using it.
- *Contacts permission*: This allows the application to access the phone's contact list.
- *Location permission*: This allows the application to access the location of your device.
- *Microphone*: This allows the application to access the microphone of your device and to record audio using it
- *Phone*: This allows the application to make and manage phone calls from your device.
- *Physical activity*: This allows the application to access info about your physical activity example like walking, biking, step count, etc., from your device.
- *SMS*: This allows the application to view and send text messages from your device.
- *Storage*: This allows the application to access and use photos, media, and other files from your phone.

6. Investigation procedure

An Investigating Officer (IO) must find what happened, who is involved, how it is done, where and why, answers to all these questions will uncover the crime. An IO must avoid preconceived theories as they might mislead the actual case. The ultimate aim of the IO should be a reconstruction of the crime scene, identifying the suspect and victims (in few cases), and finding the motivation behind the crime using digital evidence.

Proactive steps must be taken if a digital device is a part of a crime scene; the evidential device must be preserved from being tampered with and maintaining evidence integrity. The below steps are part of the proper investigation.

6.1 Immediately place the mobile device in airplane mode basic rule of sound evidence is that the last access date and time must match the seizure date and time. If the network connection is not disabled, there are chances of data overwriting. In some cases, criminals can wipe the data remotely. All this situation leads to tampering of evidence that cannot be submitted to the attorney.

6.2 Document the pin code and user's credentials. After the seizure, IO must make a document and collect as many user credentials as possible because the type of data needed for investigation cannot be known at first. PIN bypass techniques are available, but it is suggestable to document the credentials. Enquire how frequently the criminal backed up the data to the cloud or drives as sometimes cloud data can be a crucial part of the investigation.

6.3 Documentation. IO must document everything by mentioning the seizure date and time, collected device make and model, number of sim slots available. If any external memory cards are present, a vendor of SIM and its unique identity number by taking pictures and video to support the documentation.

6.4 Lab proceedings in the forensic lab are to be followed to extract potentially sound evidence that needs to be submitted in the court of law.

1. *Collection*: The first step in forensics is to collect all the digital devices involved in the crime scene for investigation purposes.
2. *Preservation*: Disabling network connections and working on the original device can change the evidence; therefore, a clone of the actual device should be taken. It is also useful whenever re-investigation happens. The submitted evidence and newly extracted evidence should be a match.
3. *Acquisition*: From the obtained clone, copy data should be extracted in an image file; the image file is nothing but a compressed version of a clone. The following data acquisition methods help in understanding the type of data possible to acquire for investigation

4. *Analysis:* Analysis is looking into the relevant data using an appropriate tool; the specialist should have up-to-date training on the tool and procedure to implement.
5. *Reporting:* Tool gives the evidential report and a handwritten/digitally signed reporting document by mentioning the details from the beginning, following the chain of custody is obtained.

7. Types of Mobile Data Acquisition

Mobile forensics differs from computer forensics in that it poses different obstacles to forensic investigators. Data that may be accessed, saved, and synced across various devices is one of the most difficult forensic difficulties for the mobile platform. Because the data is volatile and may be easily modified or removed from afar, more work is necessary to keep it safe.

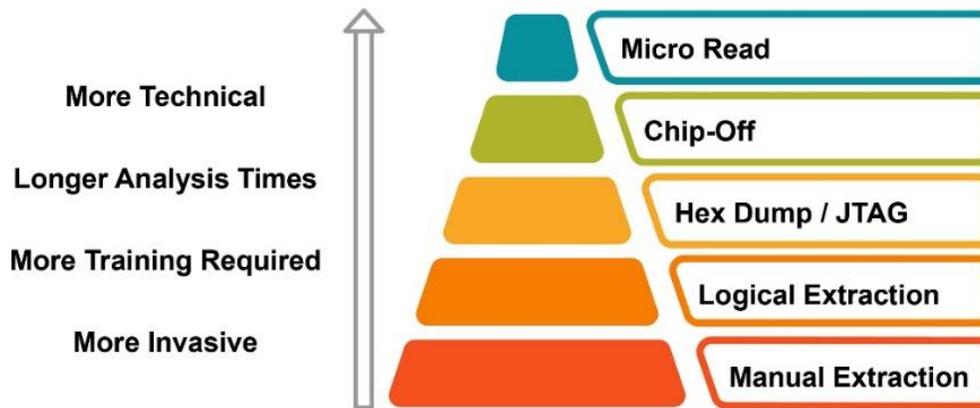


Fig - 9 : Types of Mobile Data Extraction Method

7.1 Manual Acquisition:

Not recommended, but in critical conditions must be used once after all other methods are not working. In this procedure, a screenshot or a picture or video of the device content is taken. Data can also be collected by connecting the mobile device to a computer. This method is a time-consuming process, and there is a high probability of human error, i.e., accidentally deletion or modification of data during data acquisition. Tools used for manual acquisition are Project-A-Phone, Fernico ZRT, EDEC Eclipse, etc.



Fig - 10: EDEC Eclipse 3 Pro kit

7.2 Logical Acquisition:

Logical Acquisition Technique extracts allocated data by accessing the file system (directly or indirectly). The mobile device and the forensic PC must be connected via USB cable. The forensic computer delivers commands to the mobile device, mobile responds with data from its memory. Logical Data Acquisition Technique extracts allocated data by accessing the file system (directly or indirectly). The forensic tool directly accesses the files present in internal

memory; such direct access helps extract the database (DB) files, log files, and system files present. This kind of extraction helps get a complete file system structure and full access to DB files (SMS, MMS, notes, calendar); in a few instances, Logical extraction can also retrieve deleted data. The logical acquisition cannot recover deleted files data from the unallocated space. All Mobile forensic tools support logical extraction.

7.3 Physical Acquisition:

Bit to bit copy of physical storage which means data that resides outside active user data and DB files like media content (images, videos, audio), an application installed, geographic location information, and emails, and it also helps in getting more amount of deleted data. Physical Acquisition recovers allocated and unallocated (deleted or obsolete) data. It is the most expensive and efficient type of acquisition method but less supported. Investigator can retrieve all information saved in the device. For example, if a culprit has stored data on an upcoming event in a calendar and deleted it, the investigator can recover the same information.

7.4 Software Based - Physical Acquisition:

MTK Chipset and EDL Mode on Qualcomm are well-known hacks used by Mobile Forensic Tools for Physical Extraction. In this method, forensic software exploits the device vulnerabilities, runs on the devices with root access, and provides a complete physical image of data partitions. It is the way to retrieve deleted information (i.e., data from deleted records and deleted files) but with limited support. Requires advanced skill knowledge for this method and also depends upon the vendor/model of the device. This method is intrusive (i.e., rooting of phone and bootloader bypass/replacements on the mobile phone). It will not work on the latest android version/devices as encryption remains an issue.

7.4.1 Hardware-Based - Physical Acquisition

7.4.1.1 JTAG Acquisition:

The JTAG interface is generally used to communicate with the processor for testing during the device production process. This method allows investigators to acquire device data from a smartphone non-invasively. This method involves specially designed hardware connected to a specific port. i.e., Test Access Ports (TAPs) on the mobile device, allowing data from the smartphone's NAND or NOR flash memory chips to travel through them and directly to the system, creating a raw memory dump of the device's contents.



Fig - 11: Types of JTAG Connection Cable to Mobile phone

This method requires high skill knowledge of disassembling the device, shouldering, etc. JTAG ports are not available on the latest smartphone device; this method is supported on selected devices. JTAG pin configuration depends upon the vendor and model of the device. Data extracted using method encryption on the device remains an issue.

7.2.1.2 Chip Off Acquisition: The chip-off acquisition involves physically removing the mobile device's flash memory. Using specialized tools and techniques, the investigator disassembles the device and removes the flash memory from the circuit board. Once the flash module is removed, it is placed into a specialized component to read memory modules.

A chip-off examination is invasive, and once the chip is removed from the device, the chip would need to be re-balled and then reinstalled into the device to operate as it had previously. This process is highly labor-intensive and equally expensive.

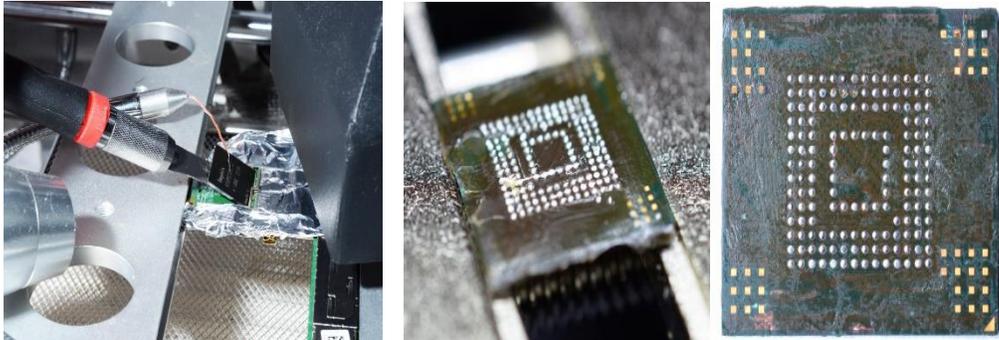


Fig - 12: Removing Chip from Mobile phone & EMMC Chip

7.4.2 Micro Read:

This approach manually captures a general view of the memory chip via the lenses of an electron microscope and evaluates data on the chip, especially the physical gates. An electron microscope is used to rebuild the chip contents by reading each gate's status separately.

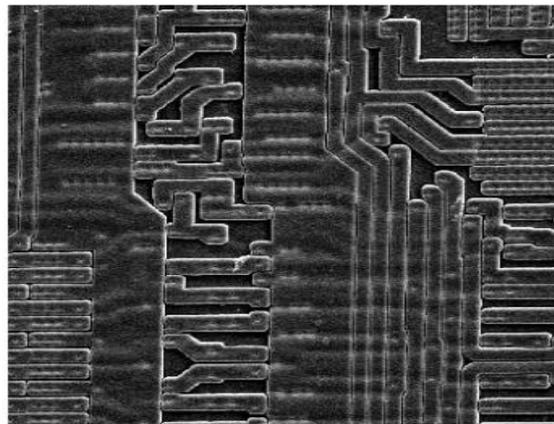


Fig -13: Micro Read – CHIP using Electron Microscope.

This procedure entails deciphering and displaying data stored on memory chips. The researchers study the physical gates on the chips with a high-powered electron microscope, then transform the gate level into 1s and 0s to get the ASCII code. The procedure is costly and time-consuming. It also necessitates a thorough understanding of hardware and file systems.

8. Mobile forensics tools:

Given the importance of forensics in today's data-driven society, this paper discusses the necessity to investigate the many mobile Device forensic technologies accessible. This paper aims to perform a comparative analysis of the various commercial and open-source mobile device forensic tools concerning predefined software parameters and employ a cross-device and test-driven approach. The test scenarios are structured to assess whether the selected tools possess a holistic one while responding to threats and techniques of the digital realm. Following are the Mobile forensics tools that are used by Investigators:

1. Cellebrite UFED 4PC / Touch 2 (www.cellebrite.com)
2. MSAB XRY Office (www.msab.com)

3. Oxygen Forensic Detective (www.oxygen-forensic.com)
4. MOBILedit (<https://www.mobiledit.com>)
5. SPF Pro (www.salvationdata.com)
6. Magnet Axion Mobile (www.magnetforensics.com)
7. MD-Next, MD-Red (www.hancomgmd.com)
8. ADF Mobile Device Investigator (www.adfsolutions.com/mobile-device-investigator)
9. Paraben E3:DS (paraben.com/digital-forensic-tools-5)
10. Final Mobile Forensics (www.finaldata.com/mobile)

9. Mobile forensic Challenges:

When a digital device is involved in a crime scene, and if an investigator has to visit the location, he should carry a camera and a tool kit to seize the evidence. Depending on the type of crime, an investigator must decide if to make a live acquisition or hold the evidence and take it to the lab for further analysis. Digital evidence from mobile devices is typically difficult to gather for law enforcement and forensic investigators. Some of the causes are as follows:

9.1 Unlocking Phone:

There can be several barriers and challenges to mobile phone forensic; phones are frequently protected with a passcode, preventing an investigator from accessing the data. Most phones include an optional security feature that deletes data if an incorrect passcode had entered many times. So, brute force attempts to unlock the phone by entering every conceivable combination of passcodes is potentially dangerous. In other circumstances, a user aware that they are under investigation may try to delete or remotely erase data to conceal or destroy evidence. If the device had synced to the cloud, one can see and update synced info on all devices, such as bookmarks, history, passwords, and other settings. Once sign-in automatically to Gmail, YouTube, Search, and other Google services such as media files, saved calendar dates, contact information, messages, apps installed, documents saved can all be retrieved. If the investigator signed in before turning on sync, they would stay signed in. If a criminal changes his device, he can still get access to synced information in case of his device seizure. For an investigator to have access to his cloud data, it can be google drive or his iCloud; cloud forensic extraction will pull all the data in case of physical device damage.

9.2 Damaged Phone: Some phones that undergo cell phone forensics examinations are also physically damaged, often intentionally. Users that want to hide evidence will go a step further than simply deleting data and attempt to destroy devices by smashing them, throwing them in a body of water, or trying to burn them. Sometimes, these physically damaged phones aren't submitted for examination because it is assumed that criminals destroyed them beyond recovery.

9.3 Hardware differences: The market had inundated with several mobile phone models from various manufacturers. Different varieties of mobile phones may be encountered by forensic investigators, each with its extra size, hardware, features, and operating system. In addition, because of the short product development cycle, new models appear often. As the mobile landscape evolves, it's more important than ever for examiners to adapt to all problems and stay current on mobile device forensic procedures across various devices.

9.4 Mobile Security / Encryption: Security mechanisms are implemented into modern mobile platforms to secure user data and privacy. These characteristics operate as a stumbling block during forensic collection and evaluation. Modern mobile devices, for example, include built-in encryption methods from the hardware to the software layers. To retrieve data from the devices, the examiner may need to break past various encryption techniques.

9.5 Lack of resources: Forensic examiners will need the instruments necessary to analyze the variety of mobile phones. An investigator must maintain forensic acquisition equipment such as USB cables, batteries, and chargers for various mobile phones to collect data from those devices.

- 9.6 Anti-forensic techniques:** Anti-forensic strategies arose in response to digital forensics' positive efforts to reduce cyberattacks, making it difficult for cyber forensic professionals to identify perpetrators. It has created challenges for the job of computer investigators. Anti-forensic procedures are based on the principle of erasing or making footprints untraceable. In the lack of prior information, it becomes impossible for forensic investigators to establish any facts. Data concealing and other anti-forensic techniques are obscuring data, safe wiping, data forgery, etc. Such approaches make data retrieval from digital media data nearly tricky; rooting the phone can assist in data retrieval in such circumstances.
- 9.7 Dynamic nature of evidence:** Intentionally or inadvertently, digital evidence can be easily tampered. Browsing an app on the phone, for example, might change the data saved by that App on the device.
- 9.8 Accidental reset:** Mobile phones include capabilities that allow you to reset everything. While mistakenly resetting the device while analyzing it may result in data loss, physical extraction using forensics tools might aid in recovering the data.
- 9.9 Device alteration:** Moving application data, renaming files, and changing the manufacturer's operating system are feasible ways to change devices. In this scenario, the suspect's knowledge and experience should be considered. You won't be able to recover the evidentiary data in such circumstances.
- 9.10 Communication shielding:** Cellular networks, Wi-Fi networks, Bluetooth, and Infrared are all used by mobile devices to connect. Because device communication can modify device data, the investigator should rule out the prospect of additional contact once the device has been seized.
- 9.11 Lack of availability of tools:** Mobile devices come in a variety of models and vendors. One forensic tool would not support all the devices and perform all the necessary functions, so a combination of tools needs to be used. It might be challenging to select the proper tool for a particular phone.
- 9.12 Malicious programs:** Malicious software or malware, such as a virus or a Trojan, might be present on the device. These malicious applications may attempt to propagate to other devices via a wired or wireless link.
- 9.13 Remote unlock/remote erase:** Android owns a tool that helps locate and remotely wipe the stolen phone. Usually, phones get locked through passwords or fingerprints, or patterns to maintain security. Still, criminals are using this feature to delete the evidence from the device after the seizure remotely.

10. Conclusions:

Mobile phones are one of the important sources of information for investigators. The history of mobile phones dates back to few decades. The widespread usage of smartphone devices enabled storing and transferring massive amounts of data that may have been utilized as digital evidence in a forensic investigation. With the help of digital forensic tools, forensic investigators can extract active and deleted mobile artifacts such as SMS, Call registers, Images, Audio, Videos, and Files from mobile devices that investigators can use for further investigation.

Given the many kinds of smartphone devices in the market, extracting digital evidence from these devices may be difficult at times. The extraction of digital evidence from cell phones may be done in a variety of methods. However, prior knowledge of smartphone forensic tools is paramount to a successful forensic investigation. Mobile Forensic tools ensure the integrity of the mobile phone, resulting in non-contamination of evidence.

REFERENCES:

- [1] Webpage: <https://ieeexplore.ieee.org/document/7880238>
- [2] E. Casey, "Digital Evidence and Computer Crime: Forensic Science" in Computers and the Internet, Academic Press, ELSEVIER, 2011.
- [3] A. Chavez, "A jailbroken iPhone can be a very powerful weapon in the hands of an attacker", Project Report Purdue University Calumet 's CIT Department, 2008.

- [4] R. Ayers, S. Brothers and W. Jansen, "Guidelines on Mobile Device Forensics", NIST Special Publication 800-101, May 2014, [online] Available: <http://dx.doi.org/10.6028/NIST.SP.800-101r1>.
- [5] V. L. Thing, K.-Y. Ng and E.-C. Chang, "Live memory forensics of mobile phones", Digital Investigation, vol. 7, no. Supplement, pp. S74-S82, August 2010.
- [6] "The volatility framework: volatile memory artifact", Systems. Volatile, [online] Available: <http://secxplrd.blogspot.in/2011/10/volatility-framework-volatile-memory.html>.
- [7] J. Oh, S. Lee and S. Le, "Advanced evidence collection and analysis of web browser activity", Digital Investigation, vol. 8, pp. S62-S70, August 2011.
- [8] D. Quick and K.-K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges", Digital Investigation, vol. 11, pp. 273-294, 2014.
- [9] M. Kaart and S. Laraghy, "Android forensics: Interpretation of timestamps", Digital Investigation, vol. 11, pp. 234-248, 2014.
- [10] K. Barmpatsalou, D. Damopoulos, G. Kambourakis and V. Katos, "A critical review of 7 years of Mobile Device Forensics", Digital Investigation (2013), vol. 10, pp. 323-349, 2013.
- [11] D. Walnycky, I. Baggili, A. Marrington and J. Moore, "Network and device forensic analysis of Android social-messaging applications", Digital Investigation, vol. 14, pp. S77-S84, 2015.
- [12] F. Karpisek, I. Baggili and F. Breitingner, "WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages", Digital Investigation, pp. 1-9, 2015.
- [13] N. Arce, "WhatsApp Calling For Android and iOS: How To Get It and What To Know", TECHTIMES, March 2015, [online] Available: <http://www.techtimes.com/articles/38291/20150309/whatsapp-calling-for-android-and-ios-how-to-get-it-and-what-to-know.htm>.

AUTHOR'S PROFILE:


Mr. Nagendar Rao Koppolu joined Police Service as Sub-Inspector in the year 1998. He served in Law Enforcement, Bureau of Immigration (IB), Central Bureau of Investigation (CBI) (Anti-Corruption Wing), State Intelligence Department, and State Information Technology Cell. He pursued M.Tech (CSE), M.Sc.(IT), and Criminal Justice Data Analysis (IIT Kanpur). He is a certified Cyber Security Professional and ISO 27001 ISMS Lead Auditor. He co-authored two books on cybercrime. Presently, he is Inspector (in-charge) of State Cyber Vertical, Telangana.