© October 2025 | IJIRT | Volume 12 Issue 5 | ISSN: 2349-6002

# Mobile Forensics and Investigation Techniques: Addressing Delays and Digital Challenges in Davanagere

Ms. Pooja Kencharaddi[1] and Mr. Mahadevaraddy Hosalli[2]

[1]Postgraduate Student, Department of Criminology and Forensic Science, Davanagere University, Karnataka, India

[2]Postgraduate Student, Department of Criminology and Forensic Science, Davanagere University, Karnataka, India

***Abstract*—The exponential growth of internet usage in India, with 886 million internet users as of 2024, has simultaneously increased in reporting of cybercrimes. This study examines the investigation of cybercrime in Davanagere. Mobile forensics relates to the recovery of digital evidence and data from mobile devices. The tools and techniques are used by the Cybercrime, Economic, and Narcotics (CEN) Police Station in Davanagere, such as IMEI, IMSI, Tower ID, CDR, Tower dump, SDR, CAF, and IPDR. These telecommunications help to collect digital evidence in cybercrime investigations. The officers are facing difficulty in getting IPDR or CDR from the service provider, limited access to technical infrastructure, an encrypted communication platform, insufficient specialized training, and data overload. This leads to delays in cases and causes backlogs. The finding underscores the importance of investing in training, infrastructure, and collaboration with telecom operators.**

***Index Terms*—Cybercrimes, mobile forensics, CEN (Cybercrimes, Economics, and Narcotics), Davanagere**

## I. INTRODUCTION

In this digital era, cybercrimes are rapidly increasing in India. The number of internet users has been increasing day by day. According to the IAMAI and Kantar report, India had 886 million active internet users as of 2024. It simultaneously creates a scope of mobile forensics. Mobile forensics is a branch of digital forensics relating to the recovery of digital evidence and data from a mobile device using accepted methods. The process of mobile forensics involves the stages of identification, collection, analysis, reporting, and presentation. In Davanagere, a fast-growing urban district in Karnataka. The internet users has increased over the past five years. Its impact on cybercrime reporting cases. The report of cybercrime cases in the CEN police station in Davanagere from 2020 to 2024 is 416 cases. The reported cybercrimes are a matrimony case, phishing, cyber stalking, and cyber bullying. The police officers are using several techniques, like network evidence or telecommunication evidence. The telecommunication evidence, like IMEI, IMSI, Tower ID, SDR, CAF, Tower Dump, and IPDR. The investigation officer frequently delays because of technical barriers like encrypted messaging platforms and limited training in specialized forensic tools.

Procedures to be Carried Out Before Starting the Crime Investigation:

- And the results can be achieved fast [related to time] and with high accuracy, so that time consumption can be avoided, as the result further damages can be controlled and the mislead in cases can be avoided compared to traditional investigation.
- Easy to monitor remotely and doesn't require the mandatory conditions like ground work and face-to-face interrogation.

Step 01:

Step 02:

1. Planning: - Before starting any case investigation planning plays an important role, as it includes thinking, decision making, getting of ideas, setting of team, instructions, roles and responsibility like collection of evidence / data said to be Technical or Non – Technical such as Aadhar, PAN card, Bank details, list of active MOB, on ground information from public and other Proof of Identification (POI).
2. Implementation / Execution: - A proper execution or an implementation will cause a direct impact on the case work, for example: - A cell ID in CDR or Tower dump gets changes by a network operator, so that a CDR or Tower dump should be analysed within a given time.

## II. OBJECTIVES

1. To explore mobile forensic investigation practice in Davanagere.
2. To identify delays and challenges faced by law enforcement.

## III. RESEARCH METHODOLOGY

Research Design: Descriptive research
Area of the research: Davanagere
Sample of the study: Primary data
Sample size: 5 officers in CEN Police Station, Davanagere
Data collection tool: Interview with CEN Police Station officers

## IV. RESULT AND DISCUSSION

A. Tools and techniques for investigating cybercrimes in Davanagere: -

1. IMEI: International Mobile Equipment Identity

- IMEI is a unique number for identifying a device on a mobile network.
- To know your IMEI of your handset, dial *#06# on your keypad.
- The mobile number which having two IMEIs represents that the mobile has two SIM slots/a Dual handset.
- An IMEI number includes the Make, Model, and Serial number of the device (website: imei.info).

Example:
IMEI → 9113151016113580
Type Allocation Code (TAC) → 91131510
Serial number → 1613580

2. IMSI: International Mobile Subscriber Identity

IMSI stands for International Mobile Subscriber Identity. It's a unique number that Mobile Network Operators (MNOs) use to recognize individual subscribers, and it's a key component of a Subscriber Identity Module (SIM) profile.
Example:


*Figure 1 Example for IMSI*

IMSI: → 404909309739988
MNC (Mobile Network Code) → 404
Serial number → 90
MCC (Mobile Country Code) → 9309739988

3. CGI/ CELL ID/ TOWER ID:

- A Cell ID / Tower ID / CGI (Cell Global Identity), all these technical terms relate to the Tower.
- Parallel example for the Cell ID concept.

Example: - Vehicle Registration RTO


*Figure 2 Vehicle Registration RTO*

IND - India
KA – Karnataka (state)
04 – Bangalore (district)
JQ – Vehicle serial number issued
5657 – The Number includes all the information about the vehicle

<u>Functioning of the Mobile tower or the Network:</u>

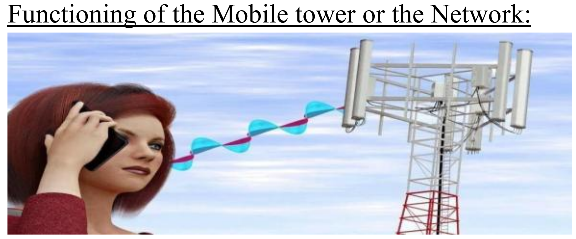

Figure 3 Functioning of the Mobile tower and the Network

A cell site, cell tower, or cellular base station is a cellular-enabled mobile device site where antennas and electronic communications equipment are placed (typically on a radio mast, tower, or other raised structure) to create a cell, or adjacent cells, in a cellular network. The raised structure typically supports an antenna and one or more sets of transmitter/receiver transceivers, digital signal processors, control electronics, and a GPS receiver for timing.

- The major role of a cell tower is to mount antennas for "Transmitting and Receiving Radio Frequency" signals to/from" mobile cell phones or devices.
- A Cell Tower covers a Total 360° further It is divided into 3 sectors, where each sector covers 120°, and each sector will have a Cell ID.

Knowing about Azimuth Angle:

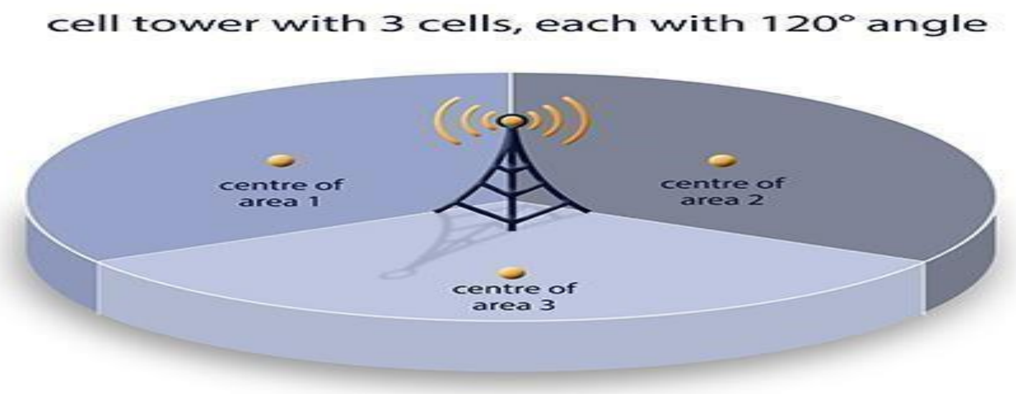


*Figure 4 Azimuth angle*

4. SDR & CAF:

SDR: Subscriber Detail Record.

- It is provided by the network operators to law enforcement agencies.
- It includes information like Name, address, DOB, proof of identification number like Aadhaar number, voter ID number, and alternate phone number of persons, which is provided during the purchase of a SIM card.
- In this SDR, every data helps the IO get some links to the cases.

Example: - By getting an Aadhaar number, we can get a phone number connected to that Aadhaar.

Gossip related to SDR and cheating: - No company [CDR analysers software companies] or any other organization will provide the SDR except the network operator, only to LEA, if it is a police complaint, can be filed against the company for leaking the data, as it's against the privacy and policy.

CAF: Customer Application Form.

- It's a form that includes complete biodata of a customer while taking a SIM card.
- The same data is provided as SDR to LEA.
- But includes some more information, like a picture of a person.

Example: - If a person "A" is holding a phone number and if it gets disconnected over a period of time same phone number will be given to another person, let's call it person "B". At the time, by using CAF, you can get to know the time period of person "A" who used the same phone number.

Procedure for Requesting the Technical Data:

- Register a Complaint by Adding the Technical data to the complaint copy collected during the investigation under FIR/Case No.
- Send the signed Compliant Copy / FIR to the District Unit office (DPO).
- Procedure followed by DPO or DCP office for getting in return data (CDR, Tower Dump, IPDR, ILD) from network operator for the given technical data given by IO (shown in below block diagram below).
- Each Unit office will be appointed by a Nodal officer (SP or DCP) to negotiate with the Network operator Nodal officer.

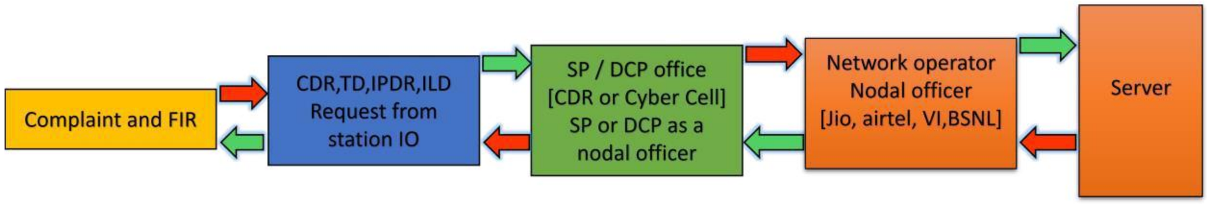


*Figure 5 Procedure for requesting technical data*

5. CDR: Call Detail Record

- Call Detail Record (CDR) is the detailed record of all the telephonic calls that pass through a telephone exchange or any other telecommunications equipment.
- The CDR is maintained by the concerned telephone exchange and contains call details such as date of call, time of call, duration of call, cell ID, destination number, IMEI, and IMSI, etc.

CDR Data Analysis in Case Investigation:

- Study the Case first.
- Get to know whether the CDR obtained is a Raw or an Analysed one.
- If it's a raw CDR, analyse it as per your convenience [MS Excel or CDR software].
- Go with the reports like: -
  - ➢ Movements of a CDR person based upon Cell ID or Tower ID Change.
  - ➢ Maximum Calls v/s Maximum Duration.
  - ➢ Common Number.
  - ➢ Call Lists (Ex, Last Called Numbers).
  - ➢ Call Type (if Call Forwarded).

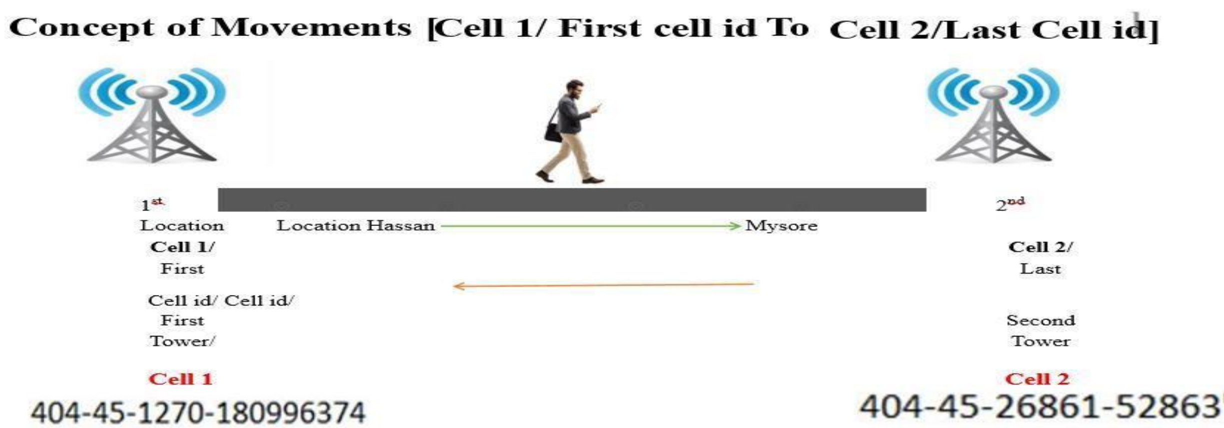


*Figure 6 Concept of movement from Cell 1 to Cell 2*

6. Tower Dump/ Tower CDR:

- Tower dump is a Technical Way or Method that is used during the Investigation process to find out the Phone Number or Mobile Number which is used / active/present at the Offence place when the crime occurred.
- If an accused uses his phone while committing a crime in an offence place, that particular phone number uses the nearby Tower for the service by getting the tower dump data, we need to find out the accused's phone number.

Data required for requesting Tower dump / Tower CDR:

A Cell ID or Tower ID is the key term for obtaining tower dump/tower CDR. The ways of getting Cell ID / Tower ID for Tower dump requisition:

- Traditional Method (making a phone call in the particular crime spot by using a different operator SIM card and getting the cell ID).
- Cell ID Extracting Machine.
- Mobile Applications.

7. IPDR: Internet Protocol Detail Record:

IPDR is the data that is obtained normally during the investigation of there is any Usage of the Internet is done or Internet-based Activities.

Type of IPDR and inputs required:

IPDR that can be provided by the service provider (Ex, Airtel, Jio, Vi, BSNL):

- Mobile Number or Phone number IPDR with Destination IP and without Destination IP (Input: - Mobile Number).
- MEI IPDR (Input: - IMEI Number).
- Public IP-based IPBR (to get the "B" party phone number based upon the "A" side IPDR as input).

IPDR that can be provided by companies like FB and Google:

- Business Record Data (Input: - Account ID): A Simple way to understand the Columns or Data that will be given in the IPDR file from the service provider.
- Public IP: It's an IP assigned to the Service Provider or Network Operator.
- Source or private IP: It's an IP assigned to your device that is using the internet.
- Destination IP: It's an IP which is assigned to the Applications or to the Website that you are using (Ex, Facebook, Google, WhatsApp, etc).

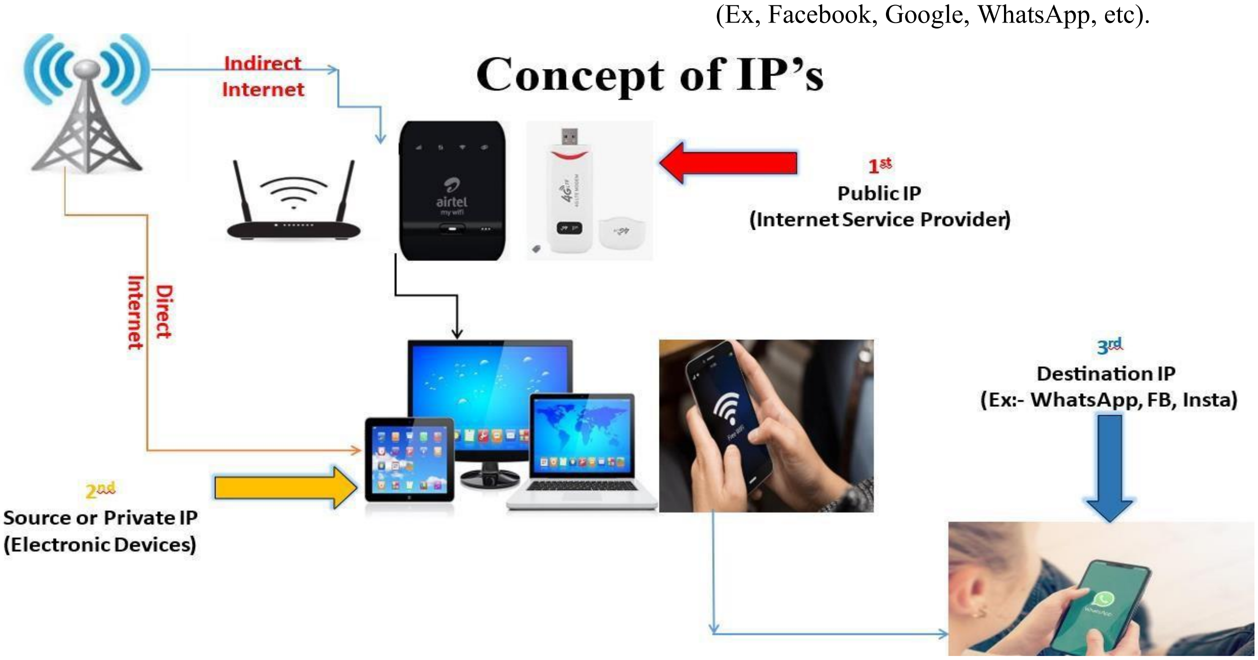


*Figure 7 Concept of IP*

B. Reasons for delaying and challenges investigation of cybercrime in Davanagere:

1. Delay in obtaining IPDR / Technical data from the service provider.
2. Tower dump analysis is delayed due to the large volumes of subscribers' data to filter and match.
3. Lack of specialized training for cybercrime officers.
4. The Internet Protocol Detail Records require approval from SP, the network operator, and the server.
5. Limited access to technical infrastructure in Davanagere.
6. A large volume of data requires more time to analyze.
7. Legal barrier in accessing private subscriber information and cross-border data.
8. Dependency on multiple telecom providers for data collection.
9. Lack of sufficient officers to handle cases.
10. Backlogs in forensic labs for mobile and network data analysis.

Findings:

1. Mobile forensics techniques such as IMEI, IMSI, Tower ID, Tower dump, CDR, SDR, CAF, and IPDR are used in cybercrime investigations in Davanagere.
2. The reporting of cybercrimes is increasing in the CEN Police Station, Davanagere.

3. The dependency on the service provider for IPDR and Tower dump.
4. The lack of specialized training for cybercrime investigating officers.
5. The investigating officers are facing technical barriers, such as an encrypted communication platform and cross-border digital evidence.

Suggestions:
1. Provide regular training for cybercrime investigators.
2. Introduce AI-based software for analysing large datasets.
3. Increase officers in the cybercrime investigation unit to balance the case load.
4. Establish a cyber forensic unit in Davanagere.
5. Develop fast-track protocols with telecom operators to speed up data sharing.

## V. CONCLUSION

The rapid growth of internet users in India. According to the IAMAI and Kantar report, 886 million internet users are in India as of 2024. Cybercrime cases are rapidly increasing in Davanagere. Mobile forensics plays a crucial role in the investigation of cybercrime. It provides digital evidence for investigation. The tools and techniques used by investigators such as IMEI, IMSI, Tower ID, CDR, Tower dump, SDR, CAF, and IPDR. The investigators are facing several problems during the investigation, such as delays in obtaining IPDR from the service provider, analysis of large volumes of data, a lack of specialized training, and limited access to technology. These barriers not only slow down the investigation process but also increase the risk of evidence loss and case backlogs. The strengthening capacity of the cybercrime unit through proper training, recruiting specialized personnel, and establishing cyber forensic laboratories.

## REFERENCES

[1] Elavarasi, M., & Elango, N. M. (2017). Analysis of Cybercrime Investigation Mechanism in India‖. Indian Journal of Science and Technology, 10(40).
[2] Kencharaddi, P., Hosalli, M. (2025). Cybercrimes in Davanagere District: A Study of Local Trends and Case Insights. Internation Journal of innovative Research in Technology, IV (12), 3899-3905.
[3] Smt. Padmashree Gunjeekar, Deputy Superintendent of Police, and Umesh P, Police officer, and other Police officers, CEN Police Station, Davanagere.
[4] Sadiq, M., Iqbal, M., Naveed, K., & Sajad, M. (2016). Mobile devices forensics investigation: process models and comparison. ISJ Theoretical & Applied Science, 1(33), 164-8.
[5] Smt. Uma Prashanth I.P.S., Superintendent of Police, Davanagere.
[6] Internet in India 2024: Kantar_IAMAI Report | IAMAI. (n.d.). https://www.iamai.in/research/internet-india-2024-kantariamai-report