

MOBILE FORENSICS IN CYBERCRIME INVESTIGATION: LEGAL AND TECHNICAL CHALLENGES IN INDIA

by

ADV. SANGHARSH P. BORHADE

B.Sc. L.L.B. D.L.L & L.W.

Practicing advocate at Pune and Shirur District and Session Court

ABSTRACT

The rapid growth of smartphones has changed the nature of criminal investigation because mobile phones are no longer used only for calling and messaging. Modern smartphone may contain photographs, videos, WhatsApp conversations, e-mails, call records, location information, social media activity, internet history, financial transactions, documents, passwords, application data and other information which may become important in a criminal investigation. Therefore mobile devices have become one of the most important sources of digital evidence in cybercrime as well as in conventional crimes having a digital component. Mobile device forensics is concerned with the scientific recovery, preservation, acquisition, examination, analysis and reporting of information from mobile devices in a manner which maintains the reliability and integrity of the evidence.

In India the increasing importance of mobile forensic evidence has created both legal and technical questions. The Bharatiya Sakshya Adhiniyam, 2023 now provides the principal statutory framework for electronic and digital records. Sections 61 to 63 specifically deal with electronic records and their admissibility. The Bharatiya Nagarik Suraksha Sanhita, 2023 also introduces important provisions relating to search and seizure through audio-video electronic means and electronic modes of criminal proceedings. At the same time, constitutional rights under Articles 20(3) and 21, particularly privacy and protection against compelled self-incrimination, must be considered during forensic examination.

The major difficulty is that digital evidence can be easily altered, deleted, encrypted, remotely destroyed or transferred to cloud servers. A mobile phone may also contain information belonging not only to the accused but also to family members, friends, victims and unrelated third parties. Therefore, investigation cannot be based merely on taking possession of a mobile phone. Proper seizure, preservation, forensic imaging, extraction, hashing, documentation, examination and presentation before the court are necessary.

Indian courts have gradually developed principles concerning electronic evidence. Decisions such as Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal established important principles regarding electronic records under the earlier Evidence Act. These principles remain relevant while understanding the transition to Sections 61–63 of the Bharatiya Sakshya Adhiniyam, 2023. Recent Supreme Court jurisprudence has also continued to emphasise the importance of admissibility and proper proof of electronic evidence.

This paper critically studies mobile forensics in India from both technical and legal perspectives. It examines the forensic process, difficulties involving locked and encrypted devices, deleted and cloud data, chain of custody, admissibility, privacy, expert evidence and institutional limitations. It argues that effective mobile forensic investigation requires cooperation between investigating officers, forensic experts, prosecutors and courts, together with standardised procedures and continuous technological training.

Keywords: Mobile Forensics, Cybercrime, Digital Evidence, Smartphone, Electronic Evidence, Bharatiya Sakshya Adhiniyam, BNSS, Chain of Custody, Encryption, Privacy, Cyber Investigation.

1. INTRODUCTION

The mobile phone has become one of the most information-rich devices in modern society. A smartphone is not simply a communication instrument. It functions as a camera, computer, payment instrument, navigation device, diary, social media platform, storage device and personal identity device. As a result, almost every important activity of a person may leave some digital trace on a mobile device.

The same technological development which provides convenience to ordinary users has also created new opportunities for criminals. Cybercriminals use mobile phones for phishing, identity theft, online cheating, cyberstalking, ransomware, unauthorised access, financial fraud, circulation

of illegal material and communication with other offenders. Mobile devices can also provide evidence in traditional crimes such as murder, kidnapping, extortion, cheating and organised crime.

Mobile forensics is therefore an important branch of digital forensics. It involves the recovery and analysis of data stored in or associated with a mobile device while maintaining forensic integrity. The process is not limited to opening a phone and looking at photographs or messages. A forensic examination may involve logical extraction, physical acquisition, analysis of application databases, recovery of deleted information, examination of metadata, location information, call records and other associated data.

The evidentiary importance of mobile phones also creates serious legal concerns. Digital information can be copied without obvious physical changes. A screenshot may not reveal whether a conversation was edited, message may have been deleted from the device but remain available on another device or server. Location information may be generated automatically. Applications may store information in different formats and cloud services may operate from jurisdictions outside India.

Thus, mobile forensic investigation must balance two requirements. First, investigators must be capable of obtaining relevant digital evidence before it disappears or becomes inaccessible. Secondly, the investigation must respect the rights of the accused and other persons whose private information may be contained in the device.

The legal framework in India has changed significantly after the introduction of the Bharatiya Sakshya Adhiniyam, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023. Section 61 of the BSA recognises the legal effect of electronic and digital records, subject to Section 63, while Section 62 provides the special evidentiary framework for electronic records.¹

The present study therefore examines mobile forensics as an intersection of technology, criminal investigation, evidence law and constitutional rights.

2. MEANING, NATURE AND SCOPE OF MOBILE FORENSICS

¹ The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–62 (India).

Mobile forensics can broadly be understood as the scientific process of identifying, collecting, preserving, acquiring, examining, analysing and reporting digital information obtained from a mobile device and its associated sources.

The term includes smartphones, tablets and, depending upon the investigation, associated wearable devices and other connected devices. Modern mobile forensic investigation may also involve SIM cards, memory cards, connected computers, cloud accounts, application servers and network-related information.

2.1 Communication Data

This may include call logs, SMS messages, instant messages, e-mails, contact lists and communication-related metadata. Applications such as WhatsApp, Telegram, Signal and other communication platforms may contain significant evidence depending on the case.

2.2 Multimedia Data

Photographs, videos, voice recordings and screenshots can provide direct or circumstantial evidence. Metadata may sometimes provide information concerning creation time, modification, device and location.

2.3 Application Data

Applications often maintain databases and log files. Banking applications, payment applications, social media applications, browsers and other services may contain useful investigative information.

2.4 Location Information

GPS information, Wi-Fi connections, cell tower information and application-generated location data can potentially assist in reconstructing the movements of a device. However, location information must not automatically be treated as conclusive proof of a person's physical presence because the device and its user may not always be the same person.

2.5 Deleted and Residual Data

Deletion from a visible application does not necessarily mean immediate destruction of every underlying digital trace. Depending upon the operating system, application, storage technology and forensic method, remnants may sometimes be recoverable.

2.6 Cloud-Associated Evidence

Modern phones often synchronise information with cloud services. Consequently, the evidence may not be physically located only on the seized device. Investigators may need lawful access to associated accounts or service-provider information.

This methodology is useful in understanding that forensic investigation must be a controlled scientific process rather than an informal inspection of a phone.

3. ROLE OF MOBILE FORENSICS IN CYBERCRIME INVESTIGATION

Mobile forensic evidence play an important role in establishing both the occurrence of a cybercrime and the connection between individuals, devices and digital activities.

For example, in online financial fraud case, a mobile device may contain messages with the victim, banking application records, screenshots of transactions, OTP-related messages, contact numbers, e-mails and browser history. In a cyberstalking case, repeated messages, calls, social media accounts and location-related information may become relevant.

In cases involving online cheating, investigators may examine payment applications, UPI records, e-mails and communication history. In cases involving identity theft, information concerning SIM cards, accounts and devices can become important.

Mobile forensics can also assist in reconstructing a sequence of events. The investigator may compare timestamps from different sources and create a timeline. For example, a message may be sent at one time, a payment made later and a device located in another area at a particular period. When properly authenticated, these separate pieces of evidence can assist the court in understanding the prosecution story.

However, mobile forensic evidence should normally be considered together with other evidence. A contact saved in a phone does not itself prove a criminal relationship. A photograph stored in a device does not necessarily establish who created it. A mobile number being associated with a device does not automatically establish who physically operating the device at a particular time.

Therefore, forensic interpretation must be careful and contextual.

The importance of electronic evidence has been recognised by the Supreme Court. In *Tomaso Bruno v. State of Uttar Pradesh*, the Court observed increasing relevance of electronic evidence and the need for scientific investigation in the technological environment.²

Mobile forensic evidence can therefore perform several functions:

- identification of suspects;
- identification of victims;
- reconstruction of communication;
- establishing timelines;
- linking persons with accounts or devices;
- identifying financial transactions;
- establishing digital relationships;
- locating relevant files;
- recovering deleted information where technically possible; and
- corroborating oral, documentary and physical evidence.

Its usefulness, however, depends upon proper collection and authentication.

4. MOBILE DEVICES AS SOURCES OF DIGITAL EVIDENCE

A mobile device can contain both user-created information and automatically generated information. User-created information includes messages, photographs, videos, documents, notes and recordings. Automatically generated information may include metadata, system logs, application records, location information and device identifiers.

4.1 Call Records

Call history may provide information about incoming and outgoing calls. However, the handset record and telecom provider's Call Detail Records are different sources and may require separate legal processes for obtaining them.

² *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.

4.2 Messages and Chats

Messages may be stored locally, remotely or both. Applications may use end-to-end encryption, which creates additional forensic difficulties. The investigator must also establish whether the recovered communication is complete and authentic.

4.3 Photographs and Videos

Images and videos may contain metadata. Metadata can sometimes indicate creation or modification information, but metadata itself must be interpreted cautiously because it can be altered or lost during transfer.

4.4 Browser and Search History

Browser history may help establish internet activity. Cached files, downloads and cookies may also provide investigative leads.

4.5 Social Media Evidence

Social media applications can contain profiles, messages, posts, photographs, videos and account-related information. Investigators should distinguish between information recovered directly from a device and information obtained from the service provider.

4.6 Financial and Payment Information

UPI applications, SMS alerts, banking applications, e-mails and screenshots may help reconstruct transactions. Forensic evidence from the mobile device should preferably be corroborated with records obtained from banks or service providers through lawful procedures.

4.7 Location Evidence

Location information can be obtained from several sources. GPS, cell-site information, Wi-Fi records and application data may not provide identical results. A forensic examiner should therefore explain the source, accuracy and limitations of the location information.

The wide variety of data available from mobile devices demonstrates why mobile forensic examination requires specialised expertise rather than ordinary inspection.

5. MOBILE FORENSIC INVESTIGATION PROCESS

A reliable mobile forensic investigation generally follows a sequence of controlled steps.

5.1 Identification

The first stage is identification of the relevant device or devices. Investigators should record the make, model, colour, serial number, IMEI where available, SIM information, memory cards and visible physical condition. The condition of the device at seizure should be documented. Photographs and contemporaneous records can help demonstrate its original condition.

5.2 Preservation

Preservation is critical because mobile devices can receive new information, automatically synchronise with cloud services or be remotely wiped.

The investigator must therefore consider network isolation, battery status and device condition. However, improper handling can itself alter evidence. Forensic personnel should use appropriate procedures rather than experimenting with the device.

5.3 Seizure and Documentation

The seizure should be documented carefully. The chain of custody should begin from the time the device is taken into possession.

The investigator should record:

- date and time of seizure;
- location;
- person from whom seized;
- device description;
- IMEI/serial number;
- SIM details;
- physical condition;
- whether the device is switched on or off;
- visible notifications, where lawfully and safely documented;
- packaging;
- person responsible for transportation; and

- subsequent transfer to the forensic laboratory.

5.4 Acquisition

Acquisition means obtaining forensic data from the device. Different levels of acquisition may be possible. Manual acquisition involves interaction with the device through its interface. Logical acquisition obtains accessible files and data through appropriate interfaces. File-system acquisition provides a deeper level of access to files and directories. Physical acquisition seeks a more comprehensive representation of device storage where technically possible. The appropriate method depends upon the device, operating system, security configuration and forensic tool.

5.5 Examination

The extracted information is examined for relevant material. Investigators may search for keywords, dates, contacts, files, applications, locations and other information.

5.6 Analysis

Analysis is different from extraction. It involves interpretation of recovered information and development of a meaningful timeline or relationship between data points.

5.7 Reporting

The forensic expert should explain the methodology used, the device examined, the data recovered, the tools used, relevant limitations and conclusions.

NIST's mobile-forensics framework specifically identifies preservation, acquisition, examination, analysis and reporting as core stages.³

The forensic report should be sufficiently clear that another qualified examiner can understand and, where possible, reproduce the methodology.

6. TECHNICAL CHALLENGES IN MOBILE FORENSICS

Mobile forensic investigation faces several technical obstacles.

6.1 Passwords and Screen Locks

³ Ayers, Brothers & Jansen, supra note 1.

Modern devices may be protected by PINs, passwords, biometric authentication or other security systems. A locked device may significantly restrict forensic access.

Investigators should not assume that a forensic tool will always defeat the security of a modern smartphone. Compatibility varies between devices and operating-system versions.

6.2 Encryption

Full-device encryption and application-level encryption can prevent access to data without the appropriate authentication credentials or technical method.

Encryption is a legitimate security measure for users, but it creates a significant challenge when investigators are lawfully attempting to obtain evidence.

6.3 Secure Hardware

Modern smartphones increasingly use hardware-backed security mechanisms. Security keys may be stored in protected hardware, making traditional extraction techniques ineffective.

6.4 Deleted Data

Deleted data may or may not be recoverable. Modern flash storage and operating systems may use mechanisms such as encryption and garbage collection which can make traditional recovery methods unreliable.

6.5 Cloud Storage

Important data may exist outside the physical device. Cloud synchronisation may mean that deleting information from the handset does not necessarily delete it from every server, while the reverse may also occur.

7. LEGAL FRAMEWORK GOVERNING MOBILE FORENSIC EVIDENCE IN INDIA

The legal framework concerning mobile forensic evidence is primarily connected with evidence law, criminal procedure, information technology law and constitutional rights.

The Bharatiya Sakshya Adhiniyam, 2023 is particularly important. Section 61 provides that electronic or digital records cannot be denied admissibility merely because they are electronic or

digital, subject to Section 63. Section 62 states that contents of electronic records may be proved according to Section 63.⁴

Section 63 provides the specific conditions relating to admissibility of electronic records. The statutory Schedule also provides a certificate format and contains provisions concerning identification of the electronic record, device information and hash values.⁵

This is particularly significant for mobile forensic evidence because the evidence may be extracted from a mobile device and presented through another medium such as a storage device, printout or forensic report.

The transition from Section 65-B of the Indian Evidence Act to Section 63 of the BSA is important. Earlier Supreme Court decisions interpreting Section 65-B therefore remain valuable for understanding foundational concepts, but practitioners must apply the current statutory language of the BSA to proceedings governed by the new law.

The Information Technology Act, 2000 also remains relevant to electronic records and cyber offences. Section 79A provides for notification of an Examiner of Electronic Evidence, which is relevant to expert opinion concerning electronic evidence.

Section 530 of the BNSS also recognises electronic modes for trials, inquiries, evidence and related proceedings.⁶

Therefore, the current framework is not limited to the admissibility of digital evidence. It also concerns the manner in which evidence is collected, preserved and presented.

8. ELECTRONIC EVIDENCE AND ADMISSIBILITY UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

The central question in mobile forensic litigation is not simply whether information was recovered from a phone. The court must determine whether the material is relevant, authentic, legally admissible and sufficiently reliable.

⁴ The Bharatiya Sakshya Adhinyam, No. 47 of 2023, §§ 61–63 (India).

⁵ Id. § 63 & Schedule.

⁶ Id. § 530.

Under the earlier Evidence Act, the Supreme Court's decision in *Anvar P.V. v. P.K. Basheer* established that electronic records produced as secondary evidence were subject to the special requirements of Section 65-B.⁷

The three-Judge Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* reaffirmed the importance of the statutory certificate for electronic evidence under Section 65-B and clarified several practical aspects concerning production of the certificate.⁸

Under the present BSA, Section 63 performs the central role in admissibility of electronic records. The Schedule to the Act is particularly important because it contemplates information concerning the source device and hash value. The statutory format specifically identifies mobile devices among the possible sources of electronic records.⁹

8.1 Importance of Hash Values

A hash value is a digital fingerprint of data. If the same data is processed using the same hashing algorithm, the resulting hash value should correspond to that data. In forensic practice, hashing can help demonstrate that a forensic copy has not been altered after acquisition.

However, a hash value does not by itself prove that the underlying information is true. It assists in establishing integrity of the digital file or image. Authenticity, relevance, authorship and evidentiary meaning require additional proof.

8.2 Screenshots

A screenshot can be useful, but it should not automatically be treated as equivalent to the original underlying digital record. Investigators should, where possible, preserve the source data and document the manner in which the screenshot was obtained.

8.3 WhatsApp and Similar Chats

⁷ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

⁸ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

⁹ The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63 & Schedule.

A printed WhatsApp conversation, screenshot or exported chat may require proper authentication and compliance with the applicable provisions of the BSA. The investigating agency should preserve the original source and maintain documentation of extraction.

8.4 Call Detail Records

CDRs obtained from a telecom service provider are different from call logs found on a handset. The source and method of production should therefore be clearly established.

The importance of proper electronic-evidence proof was again illustrated by the Supreme Court in *Pooranmal v. State of Rajasthan*, where the Court considered the statutory requirements concerning electronic evidence and referred to the principles laid down in *Anvar P.V.* and *Arjun Panditrao Khotkar*.¹⁰

Thus, mobile forensic evidence must be treated as evidence requiring a legally recognised foundation, not merely as information appearing on a computer screen.

9. SEARCH, SEIZURE AND PRESERVATION UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

Mobile forensic investigation begins before forensic extraction. It begins at the stage of lawful search and seizure.

The investigating officer should have proper legal authority for searching and seizing the device. The circumstances of seizure should be recorded accurately.

Section 105 of the BNSS introduces a significant procedural safeguard by requiring search and seizure processes covered by the provision to be recorded through audio-video electronic means, preferably through a mobile phone.¹¹

This provision has practical significance for digital evidence because it may create a contemporaneous record of the seizure process.

A proper seizure process should ideally identify the device and document its condition. The investigator should avoid unnecessary manipulation of the device. Turning the device on or off,

¹⁰ *Pooranmal v. State of Rajasthan*, 2026 INSC 217 (Mar. 10, 2026).

¹¹ The Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 105 (India).

unlocking it, connecting it to another system or allowing network connectivity may affect the evidentiary state depending upon the circumstances.

Preservation also requires consideration of network connectivity. A connected device may synchronise information, receive new messages or potentially be remotely wiped. At the same time, investigators must follow lawful and technically sound methods of isolation.

9.1 Chain of Custody

Chain of custody refers to the documented history of possession and handling of evidence from seizure until production before the court.

In mobile forensics, the chain should identify:

- who seized the phone;
- who sealed it;
- where it was stored;
- who transported it;
- when it reached the forensic laboratory;
- which examiner opened or examined it;
- what forensic method was used;
- where the forensic image was stored;
- who had access to the extracted data; and
- how the final report was prepared.

A break or unexplained gap in the chain can provide an important basis for challenging the reliability of digital evidence.

The chain of custody is therefore not a mere administrative formality. It forms part of the foundation through which the prosecution seeks to establish that the evidence presented in court is substantially the same evidence that was seized.

10. PRIVACY AND CONSTITUTIONAL CHALLENGES

Mobile phones contain unusually private information. A single device may reveal communications, photographs, relationships, financial transactions, medical information, family details, location history and personal interests.

Consequently, forensic examination may raise serious Article 21 privacy concerns.

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognised privacy as a constitutionally protected right under Article 21 and the broader fundamental-rights framework.¹²

The privacy issue is especially important because a search of a mobile phone may reveal much more information than is necessary to investigate the particular offence.

For example, if a person is investigated for one financial transaction, unrestricted examination of every photograph, private conversation and unrelated document may raise proportionality concerns.

Therefore, investigators should consider:

- legality of the search;
- relevance of the data;
- necessity of accessing particular information;
- proportionality of the intrusion;
- protection of unrelated third-party information; and
- secure handling of extracted data.

10.1 Article 20(3) and Self-Incrimination

Another issue concerns compelled access to information protected by authentication mechanisms. The constitutional protection against compelled self-incrimination under Article 20(3) must be considered carefully where investigators seek passwords, biometric access or other forms of compelled assistance.

The legal position concerning different forms of digital authentication continues to require careful application of constitutional principles to technological developments.

¹² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

The Supreme Court's decision in *Selvi v. State of Karnataka* is important for understanding the constitutional protection concerning compelled testimonial material and investigative techniques.¹³

The important point is that digital investigation must not be treated as a constitutional-free zone. Technology cannot eliminate fundamental rights.

11. AUTHENTICITY, INTEGRITY AND CHAIN OF CUSTODY

The reliability of mobile forensic evidence depends upon more than technical extraction.

Three concepts are particularly important: authenticity, integrity and continuity of custody.

11.1 Authenticity

Authenticity concerns whether the evidence is what the prosecution claims it to be.

For example, if a message is attributed to a particular accused, the prosecution may need to establish the connection between the account, device, number and accused.

The mere fact that a message appears on a phone may not always establish who authored it.

11.2 Integrity

Integrity concerns whether the data has remained unchanged or whether alterations can be identified.

Hashing is one important technique used for integrity verification. Forensic imaging also assists in preserving the original evidence while examination is conducted on a working copy.

11.3 Continuity

Continuity concerns the history of possession and handling.

If a seized phone passes from police officer to malkhana, then to forensic laboratory, then to examiner and later to court, those transfers should be documented.

11.4 Original Device and Forensic Copy

¹³ *Selvi v. State of Karnataka*, (2010) 7 SCC 263.

A basic forensic principle is to protect the original evidence and conduct examination on a forensic copy where practicable. The examiner should document the acquisition process and maintain the relevant logs.

11.5 Expert Evidence

Mobile forensic evidence can involve technical matters beyond ordinary judicial knowledge. A qualified forensic expert may therefore explain the extraction process, tools, hash values, databases and limitations.

However, expert evidence is opinion evidence. The final determination regarding relevance, admissibility and evidentiary weight belongs to the court.

11.6 Limitations of Forensic Reports

A forensic report should not overstate conclusions.

For example:

Weak conclusion: “The accused definitely sent the message.”

More scientifically cautious conclusion: “The recovered device contained the identified communication associated with the relevant account/number, subject to the limitations recorded in the report.”

The distinction is important because forensic science should present evidence and explain its limitations rather than replace the judicial function.

12. JUDICIAL APPROACH TO ELECTRONIC EVIDENCE IN INDIA

Indian courts have progressively adapted traditional evidentiary principles to electronic evidence.

The earlier judicial history concerning Section 65-B of the Indian Evidence Act demonstrates the difficulties courts initially faced in deciding how electronic evidence should be proved.

In *Anvar P.V.*, the Supreme Court treated Section 65-B as the special statutory framework governing secondary electronic evidence.

In *Arjun Panditrao Khotkar*, the Supreme Court reaffirmed the importance of the certificate requirement and clarified the legal position after considering earlier conflicting decisions.

The Supreme Court has also recognised that technology can provide important evidence in criminal investigation. In *Tomaso Bruno*, the Court emphasised the importance of scientific investigation and electronic evidence.

More recent jurisprudence also demonstrates that courts will scrutinise electronic evidence rather than automatically accepting it. In *Pooranmal*, the Supreme Court considered CDR evidence in the context of the applicable certificate requirement and held that failure to satisfy the required statutory proof affected admissibility.

The judicial approach therefore indicates several principles:

- electronic evidence is legally significant;
- digital evidence requires statutory compliance;
- source and authenticity matter;
- certificates and documentation may be essential;
- forensic methodology is relevant;
- chain of custody must be maintained;
- electronic evidence should be evaluated with the rest of the prosecution evidence; and
- courts must distinguish between the existence of digital information and proof of the fact sought to be established through it.

This approach is particularly important for mobile forensic evidence because smartphones generate extremely large amounts of data. Courts must separate genuinely relevant evidence from information that is merely available.

13. PRACTICAL PROBLEMS AND INSTITUTIONAL CHALLENGES IN INDIA

Although India has developed a legal framework for electronic evidence, practical implementation continues to face difficulties.

13.1 Lack of Trained Personnel

Police officers may understand the investigative importance of a mobile phone but may not have sufficient forensic knowledge to preserve it correctly.

13.2 Limited Forensic Infrastructure

Cyber forensic laboratories require specialised hardware, software and trained personnel. Delays in forensic examination can affect investigation and trial.

13.3 Encryption and Secure Devices

Strong encryption can make lawful forensic access technically difficult.

13.4 Cloud and Foreign Service Providers

Relevant information may be stored outside India. Obtaining such data may require cooperation with service providers and, in appropriate cases, international legal assistance.

13.5 Privacy of Third Parties

A seized phone may contain private information belonging to persons who are not accused in the case. There must therefore be safeguards against unnecessary disclosure.

13.6 Inconsistent Documentation

Poor documentation at the seizure or forensic stage may later create questions concerning authenticity and chain of custody.

13.7 Dependence on Screenshots

Investigators sometimes rely heavily on screenshots because they are easy to obtain. However, screenshots may not preserve all relevant metadata and underlying information.

The solution is not simply to purchase more forensic software. Institutional capacity must develop together with technology.

14. CRITICAL ANALYSIS, FINDINGS AND SUGGESTIONS

Mobile forensics has become indispensable for modern criminal investigation, but its evidentiary value depends heavily on the quality of the investigation.

One important finding is that collection and preservation are as important as extraction. Even the most advanced forensic software cannot repair evidence that has been improperly handled at the beginning.

Secondly, technical evidence and legal admissibility are different questions. A forensic examiner may successfully recover a WhatsApp conversation, but the prosecution must still establish its relevance, authenticity and admissibility according to law.

Thirdly, the current BSA framework is a major development because it expressly recognises electronic and digital records and provides a statutory framework for their proof. The Schedule accompanying Section 63 is particularly relevant to mobile devices because it contemplates device identification and hash values.

Suggestions

14.1 Standard Operating Procedures

A uniform national SOP for mobile seizure, preservation, extraction and reporting should be developed and regularly updated by the authority.

14.2 Training of Police Officers

Investigating officers should receive practical training concerning mobile, device seizure, network isolation, documentation and preservation.

14.3 Strengthening Forensic Laboratories

Cyber forensic laboratories should be equipped with updated hardware-software and secure evidence-storage systems.

14.4 Independent Tool Validation

Forensic tools should be tested and validated very well, the laboratory should maintain records of tool versions and validation procedures.

14.5 Better Chain-of-Custody Systems

Digital evidence management systems can be used to record each transfer and handling event.

14.6 Protection of Privacy

Investigators should develop procedures for filter of irrelevant personal information and restricting access to unrelated data.

14.7 Forensic Expert Availability

Courts should have access to qualified and more eminent experts who can explain technical evidence without replacing the judicial role.

14.8 Better Prosecutorial Preparation

Prosecutors should understand mobile forensic reports, certificates, hashes and extraction methodology.

14.9 Digital Evidence Protocols for Courts

Courts may benefit from structured protocols for receiving, storage and displaying digital evidence.

14.10 Continuous Legal and Technical Updating

Because mobile technology changes rapidly, forensic standards cannot remain static training and SOPs should be revised periodically.

14.11 International Cooperation

For cloud-based and cross-border evidence, effective cooperation mechanisms along with service providers and foreign authorities should be strengthened.

14.12 Separation of Investigation and Interpretation

Forensic examiners should report what was technically recovered , the limitations of that recovery. Investigators and courts should then draw appropriate legal inferences from the evidence as a whole.

The ultimate objective should be a system where digital evidence is both technically reliable and legally fair.

15. CONCLUSION

Mobile phones have become one of the most important sources of digital evidence in contemporary criminal investigations. The transformation of smartphones from simple communication devices into highly connected personal computers has made them valuable sources of information

concerning communication, location, financial transactions, photographs, videos, applications and online activity.

Mobile forensics is becoming an essential component of modern cybercrime investigation in India. Its effectiveness will depend upon the ability of the criminal justice system to combine technological capability with legal safeguards. Proper seizure, preservation, acquisition, examination, analysis, documentation and presentation are necessary for reliable digital evidence.

The future of mobile forensic investigation in India should therefore focus on scientific reliability, legal admissibility, constitutional protection, trained investigators, validated forensic tools and transparent chain-of-custody procedures. When these elements work together, mobile forensic evidence can significantly assist the criminal justice system while maintaining fairness to the accused and protecting the rights of individuals.

