



## Editorial

---

### Mobile Forensics in India: Opportunities, Challenges, and the Road Ahead

From being a basic communication tool, the mobile phone has developed into a potent storehouse of social, professional, and personal information. Mobile devices have become essential to daily life in India, as smartphone usage has rapidly increased not only among urban, but also among rural populations. As a result, one of the most important aspects of modern forensic inquiry is **mobile forensics**, which is the scientific extraction, analysis, and interpretation of data from mobile devices. It is an essential instrument in the Indian criminal justice system because of its applicability in criminal investigations, cybercrime, terrorism, financial fraud, and civil litigation.

The exponential increase in digital crimes is the main reason why mobile forensics has become so popular in India. Mobile communication systems are increasingly used in crimes like terrorism, organized criminal coordination, online financial fraud, cyberstalking, and disinformation operations. Important investigation leads are frequently found in call logs, communications, application data, geolocation data, multimedia files, and cloud-based backups. The growing reliance of Indian courts on digital evidence highlights the necessity of strong forensic techniques and legally acceptable evidence processing.

Mobile forensic investigations in India function within a complicated legal framework. The gathering and admissibility of digital evidence are governed by the **Information Technology Act, 2000**, the **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023**, and the **Bharatiya Sakshya Adhinyam (BSA), 2023** (especially Sections 62 and 63). A significant ethical and constitutional component has been introduced by the historic ruling that acknowledged the right to privacy as a basic right. Investigators now have to weigh proportionality, legal authorization, and respect for individual privacy against the requirement of gathering digital evidence. Any procedural error runs the danger of excluding evidence and undermining public confidence.

Mobile forensics in India confronts several structural and operational obstacles despite its increasing significance. One significant obstacle is the rapid growth of technology. Strong encryption, secure bootloaders, proprietary hardware designs, and regular operating system updates frequently surpass the capability of forensic equipment. Investigators have to deal with encrypted chat apps, locked devices, and cloud-based data kept outside of national borders. These difficulties are made worse by limited access to sophisticated forensic software, particularly in smaller forensic labs and district-level units.

Another significant concern is the **lack of standardized protocols and uniform training**. While central agencies and premier forensic laboratories may possess advanced infrastructure and skilled personnel, capacity at the state and district levels remains uneven. Inadequate training can lead to improper data extraction, contamination of evidence, or failure to maintain a proper chain of custody. Such deficiencies not only weaken

prosecutions but also raise serious ethical concerns regarding the integrity of forensic practice.

The admissibility of mobile forensic evidence in Indian courts depends heavily on **methodological transparency and expert credibility**. Courts increasingly scrutinize how data was acquired, whether tools used were reliable, and whether procedures adhered to established forensic principles. This highlights the urgent need for **accreditation of forensic laboratories**, validation of tools, and development of national guidelines specific to mobile forensics. Collaboration between forensic scientists, legal experts, and policymakers is essential to ensure that scientific rigor aligns with legal requirements.

Looking ahead, the future of mobile forensics in India lies in **capacity building, research, and ethical governance**. Investment in indigenous forensic tool development can reduce dependence on expensive foreign software and enhance data security. Regular training programs, certification courses, and microcredentials can help create a skilled workforce capable of addressing emerging challenges. Equally important is the integration of ethical frameworks that emphasize privacy protection, minimal intrusion, and accountability.

In conclusion, mobile forensics is now situated in India at the nexus of ethics, law, and technology. The effectiveness of delivering justice will be greatly impacted by the forensic system's capacity to adjust as mobile devices continue to influence criminal activity. To ensure that technology is a tool of truth rather than a source of ethical and legal controversy, mobile forensic capabilities must be strengthened while respecting constitutional principles.

**Dr Shankar M Bakkannavar**  
Editor – in – Chief