INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 4 | Issue 1 Art. 5

2025

Examining the Role of Digital Forensics in Strengthening Cybercrime Investigations in India

Arshiya Banu R and Jyotirmoy Banerjee

Recommended Citation
Arshiya Banu R and Jyotirmoy Banerjee, *Examining the Role of Digital Forensics in Strengthening Cybercrime Investigations in India*, 4 IJHRLR 58-68 (2025).
Available at www.humanrightlawreview.in/archives/.

Examining the Role of Digital Forensics in Strengthening Cybercrime Investigations in India

Arshiya Banu R and Jyotirmoy Banerjee

LLM Student, Amity Law School, Amity University, Bengaluru.
Assistant Professor, Amity Law School, Amity University, Bengaluru.

Manuscript Received	Manuscript Accepted	Manuscript Published
28 Dec. 2024	31 Dec. 2024	03 Jan. 2025

ABSTRACT

In today's digital era, the technological advancement has started dominating in every field because it has been easily accessible to the public and they can get access to everything at one place and further it has become a part of day-to-day life. This dependence on technological advancement has led to an increase in computer and internet related crimes, and it has made it more difficult to find cyber criminals because the place of operation and action of cybercrime are from a different place, and this ends up being difficult in tracing such cyber criminals. The cyber-crime has increased in every field because their platform of committing the crime is completely different, and the general investigation process does not cover the concept of cyber-crime and this brings up the need and necessary of digital forensics as this is the process of collecting digital evidence without infringing the privacy and to maintain the integrity of evidence to make it admissible in court. In simple terms, digital forensics is also a part of forensic science, and this is used to investigate cybercrimes. There are many challenges in collecting digital evidence, and a major issue faced during this digital forensic is that they have to use encrypted data which may end up in violation of data privacy and further need to deal with legal and jurisdictional issues. Despite all this challenges digital forensic has created a new path to help in investigation of cybercrime. This paper focuses on the concept of challenges of digital forensic during investigation of cybercrime and its role in creating impact of such investigation and further it deals with the legal issues during admissibility in court as evidence.

KEYWORDS

Digital Forensic, Cybercrimes, Investigation, Digital Fraud, Digital Evidence.

INTRODUCTION

In recent years, the use of technology has advanced significantly which gave a rise to cybercrimes and this inspired the need for advanced criminal investigation method across the Nation. Digital forensics is the important part for the cyber investigation and digital evidence. The cybercrimes like hacking, phishing, identity theft, digital financial fraud and so on are the modern complex crimes which requires investigation to be done in the modern ways with advanced technology and digital forensic is one such kind of crime investigation[1].

In India, legal provisions in respect of Cybercrimes are defined under Information Technology act, 2000 and it has gone through several amendments to regulate every advanced cybercrime but still it has certain shortcomings and grey areas which need to be regulated and further the concept of digital forensic hasn't been recognised. In recent times, the need of digital forensic for the crime investigation has increased and at the same time it faces a biggest challenge, that is admissibility of digital evidence in the court room.

Digital forensic means the use of forensic methods to collect necessary data to examine the digital information to comply with the legal process. This method is used mostly in the criminal investigation as it helps in revealing the important information of an investigation especially in the cyber space along with the source of such information which makes it more efficient to be admissible in the court.

The criminal Justice system knows the need and necessity of digital forensic but still they fail to implement this tool during cybercrime investigation as it faces many challenges because there is no formal regulation for digital forensic in the Indian Legal system. Other major legal issue in regards to the digital forensic is the privacy of an Individual which may be violated during the collection of data and the misuse of these technologies by the police system. This tool is mainly used to investigate in regards of technological crime and to provide solutions for the same.

Digital forensic is an important tool for investigating the

[1] Indian Journal of Law and Legal Research, *Critical Analysis of Forensic Science In Effective Administration Of Criminal Justice System In India*, IJLLR (2024).

evidence of cybercrimes especially hacking and every other computer related crime which the data of an individual is stored. During the investigation process it includes the how to recover the deleted file, and different way to track a criminal through the IP address and to find the geographical location from where he commits such crime. But the Indian legal system lacks in experience in relation to criminal investigation and fails to maintain standardized policies and procedures in relation to digital evidence.

This study mainly focuses on evaluating digital forensic in criminal investigation by concentrating on regulations and the precedent. In further aims at the gaps of digital forensic in the existing legal systems and provides solution and recommendations to enhance the use of this technology in the investigation of the criminal justice system.

UNDERSTANDING DIGITAL FORENSICS

Digital forensic is a part of an investigation into computer crimes, and is a subfield of forensic science that involves locating, gathering, analysing, and reporting any valuable digital data on digital devices. Digital forensics also includes the process of identification, preservation, and presentation of digital evidence. Digital forensic has become as one of the most important factors in this technological investigation for extracting the necessary data from the available computer networks. At the same time, an ethical issue has arisen, that is recovering the deleted data from a computer and analysing hard drives is considered as a violation of privacy of an Individual and further it included authentication of digital signatures[2].

- ***Definition of Digital Forensic***

  Digital forensic can be defined as "*A practice of identifying, recovering, and analysing electronic data to uncover and interpret critical information". The primary goal is to maintain the integrity of evidence, preserving it in its original state. This process involves a detailed, methodical investigation, including the collection, identification, and validation of digital data to accurately reconstruct past events. While digital forensics is most commonly employed in legal proceedings, it can also be applied in various other contexts such as cybersecurity or*

[2] Hemlata B. Patil & Dr Anjula Chowbe, An Examination of Digital Evidence and Its Relevance for Indian Forensic, 30 Educational Administration: Theory and Practice 6445 (2024), https://www.kuey.net/index.php/kuey/article/view/3013 (last visited Dec 14, 2024).

corporate investigations"[3]

The science of recovering and examining data from digital sources in such a way that is admissible in the court of law. It further involves the identification, preservation, extraction, and documentation of electronic data to support an investigation. This definition emphasizes both the technical and legal aspects of digital forensics, highlighting the importance of ensuring that digital evidence is handled properly for it to be usable in legal proceedings[4].

The process of locating, protecting, evaluating, and presenting digital evidence in a way that complies with the law is known as digital forensics. It involves the application of specialized techniques to recover, interpret, and authenticate data from electronic devices, with the aim of supporting legal, regulatory, or investigative outcomes. This definition emphasizes the scientific and investigative aspects of the discipline, with a particular emphasis on ensuring the integrity and legal validity of the evidence[5].

- ***Evolution of Digital Forensic***

The evolution of digital forensics has been closely interconnected to the rapid development of technology in India. In 1980s, the use of computers was increased, and that brought the need for investigators to recognize the value of digital data in solving crimes. In early days, digital forensic focused on simple data recovery from CD's and hard drives. In 1990s, the personal computers and the internet started dominating the society, and that resulted in the need of digital forensics which has expanded to include investigations of email and everything related to internet and network. In 2000s, the rise of mobile phones and social media has introduced new challenges, requiring specialized tools and techniques for extracting data from mobile devices and cloud storage. In today's generation, digital forensics covers a broad range of technologies, like cloud computing and plays a critical role in criminal investigations of cybercrime, cybersecurity, and corporate security[6].

[3] EC-Council, *What Is Digital Forensics |Phases of Digital Forensics | EC-Council*, Cybersecurity Exchange (Mar. 6, 2024), https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics.
[4] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (Third edition ed. 2011).
[5] Forensic Computer Crime Investigation, (Thomas A. Johnson ed., 2005)
[6] Mark Pollitt, *A History of Digital Forensics*, 337 3 (Kam-Pui Chow & Sujeet

- ***Types of Digital Forensic***

Digital forensics evaluates certain branches, each focusing on a different aspect of electronic data investigation. Electronic communications, such as emails and instant messaging, can provide crucial direct evidence of criminal intent or involvement, while social media posts and online interactions often reveal connections between suspects or help support alibis. Digital forensic techniques enable investigators to recover deleted or archived data, offering valuable insights into a suspect's activities. In a court of law, the importance of evidence cannot be overstated, as establishing facts is critical. Data from electronic devices can be sourced from two main categories:

- ***Volatile Data***

Volatile data in digital forensics refers to information stored temporarily in a computer's memory, which is lost when the device is powered off or rebooted. This type of data is crucial in investigations because it often contains real-time or recent activity, such as active processes, network connections, system configurations, or contents in RAM. Volatile data can provide immediate insights into a suspect's actions, including running applications, logged-in users, and communication history. However, since it disappears once the system loses power, volatile data is highly time-sensitive and requires quick acquisition during an investigation. Capturing this data is a vital step in digital forensics, especially when investigating cybercrimes, as it can offer critical evidence that is not stored on persistent storage devices like hard drives.

- ***Non-Volatile Data***

Non-volatile data in digital forensics refers to data that is permanently stored on a device, remaining intact even when the power is turned off. This type of data is typically found on hard drives, solid-state drives (SSDs), flash memory, ROM, CDs, and DVDs. Non-volatile data is essential in forensic investigations as it contains critical information, including files, documents, system logs, and application data, which can be used to reconstruct events or actions taken by a suspect. Unlike volatile data, non-volatile data is not time-sensitive and can be accessed at any point during an investigation, making it a crucial component for long-term evidence preservation. In digital forensics, non-volatile data can be analysed to uncover

Shenoi eds., 2010), http://link.springer.com/10.1007/978-3-642-15506-2_1 (last visited Dec 14, 2024).

valuable insights, such as deleted files, browsing history, or hidden data, helping to build a stronger case in both criminal and civil investigations[7].

Digital evidence plays an essential role in forensics investigations, particularly in the context of cybercrime, where devices like smartphones, smartwatches, smart TVs, and gaming consoles can provide critical information. When gathering digital evidence, forensic experts must ensure that it meets five key criteria, such as, it must be admissible, authentic, complete, reliable, and believable. In case of failure of any one this criterion then digital evidence may be failed to pass the admissible test in court of law.

LEGAL FRAMEWORKS GOVERNING DIGITAL FORENSICS

The evolving legal framework surrounding digital forensics is highlighted in recent reforms such as the BNSS[8], and this act emphasizes the importance of digital forensic evidence in modern law enforcement. Further this legislation evaluates the importance of collecting and utilizing digital forensic evidence to combat increasingly sophisticated criminal activities, especially cybercrimes. As technology advances and crimes become more complex, the role of digital forensics has become crucial in solving cases. Following are the key provisions in relation to digital forensic.

This section allows police officers to record the statements of identifiers during test identification parades using audio-video technology, especially if the identifier is mentally or physically disabled. This provision ensures that all statements are documented in a way that is legally admissible, even in cases involving individuals who may struggle with traditional identification processes[9]. This provision mandates that all police searches and seizures be recorded using audio-video technology. This includes the documentation of any place searched or items seized during law enforcement operations. Along with the seizure list, the recorded footage must be forwarded to the relevant judicial authority promptly. This provision ensures transparency and accountability in the investigative process, especially when dealing with digital forensic evidence that may be tampered with

[7] CISOMAG, *What Is Digital Evidence and Why Is It Important in 2021?* CISO MAG | Cyber Security Magazine (Sep. 28, 2021), https://cisomag.com/what-is-digital-evidence-and-why-its-important-in-2021/ (last visited Dec 14, 2024).
[8] BNSS, 2023.
[9] BNSS, 2023, Section 53.

or contested in court[10].

This section requires that evidence from rape victims to be recorded at their home or another preferred location, preferably by a female police officer and in the presence of a parent, guardian, or social worker. This provision aims to protect the dignity and privacy of the victim while also ensuring that the evidence is preserved, potentially through audio-video recording methods. This helps maintain the integrity of evidence in sensitive cases, which may include digital content such as text messages, images, or emails[11]. This provision mandates that forensic evidence to be collected at crime scenes for offenses punishable by seven years or more of imprisonment. This provision is essential for ensuring that digital forensic evidence such as data from computers, mobile devices, or other electronic equipment is properly preserved and can be used in court to prove the involvement of a suspect[12].

This section allows the police officers to record witness statements using audio-video technology at their discretion. This provision is especially beneficial when dealing with vulnerable witnesses or those unable to appear physically due to distance, health, or fear of intimidation. The use of audio-video technology ensures that witness testimonies are accurately documented and can be used as valid evidence in court[13].

These sections empower authorities to use audio-video technology for the examination of witnesses in warrant cases, which can be conducted at state-designated locations. This provision facilitates the gathering of witness testimony in cases where in-person presence is not feasible. It also ensures that testimony is preserved for future use in court, maintaining the integrity of the witness's statements[14].

This section permits the examination of the accused through electronic means, such as video conferencing. This is particularly important for ensuring the fair treatment of the accused, especially in cases where physical transportation might pose security risks, or the accused cannot be present due to illness, distance, or other factors. The use of electronic examination ensures that the legal process continues without delays while maintaining transparency[15].

[10] BNSS, 2023, Section 105.
[11] BNSS, 2023, Section 176(1) cl. 1.
[12] BNSS, 2023, Section 176 cl. 3.
[13] BNSS, 2023, Section 180 cl. 3.
[14] BNSS, 2023, Section 265.
[15] BNSS, 2023, Section 306.

This provision allows for the collection of various forensic samples under a magisterial order. These samples include fingerprints, voice samples, signatures, and handwriting. In the digital age, these samples may also include biometric data, digital fingerprints, and voice recordings that are used in digital forensic investigations. By expanding the range of forensic samples, this section enables a more comprehensive approach to identifying and linking suspects to crimes, especially in cybercrime investigations[16].

The above provisions provide a modern and comprehensive legal framework that enhances the role of digital forensics in law enforcement. By ensuring the proper handling and recording of forensic evidence through audio-video technology, these reforms are crucial in addressing the challenges posed by modern, tech-driven crimes. However, for successful implementation the police official needs to have skilled personnel, proper infrastructure, and a careful approach to privacy concerns while recording information and collecting data.

CHALLENGES OF DIGITAL FORENSICS IN CRIMINAL INVESTIGATION

The use of digital forensics as an investigatory tool has become essential in modern criminal investigations in India. However, there are several challenges related to its technical, legal, procedural, and ethical aspects that affect the effectiveness and impartiality of criminal investigations. These challenges need to be addressed to improve the application of digital forensics in the Indian legal system.

- ***Technical Challenges***

  Digital forensics in India faces significant technical challenges that complicate criminal investigations. One of the foremost issues is encryption, particularly end-to-end encryption used in messaging applications like WhatsApp. When data is encrypted, investigators cannot access it without the decryption key, making it nearly impossible to retrieve vital information needed for cases, especially in cybercrimes and terrorist activities.

- ***Legal and Procedural Challenges***

  On the legal and procedural front, challenges arise in the admissibility of digital evidence in courts. Compliance with Section 63[17], which requires the certification of electronic

[16] BNSS, 2023, Section 349.
[17] BSA, 2023.

records, is often difficult to achieve. Jurisdictional issues or the lack of availability of the original source of the data can create significant hurdles in certifying evidence.

- ***Ethical Concerns in Digital Forensics***

Ethical concerns in digital forensics are becoming increasingly significant, particularly in the context of privacy rights. Every citizen has the right to privacy[18]. Investigators may unintentionally access personal data during a digital forensics investigation that is unrelated to the crime being investigated, potentially violating privacy rights. Therefore, there is a pressing need for a strong ethical framework, alongside robust legal standards and technical procedures, to ensure that digital forensics is applied effectively and justly.

LEGAL CHALLENGES IN LANDMARK CASES INVOLVING DIGITAL EVIDENCE IN INDIA

Several landmark cases in India have addressed the legal challenges surrounding the admissibility and reliability of digital evidence, particularly in relation to the Indian Evidence Act, 1872. These cases have helped the legal system in shaping the legal framework for handling electronic evidence, while also highlighting the complexities involved.

In the present case, the judicial interpretation was done in regard to clarifying the legal standards for the admissibility of electronic evidence in India. The Supreme Court upheld the provisions under Sections 65B (1) and (2) of the Indian Evidence Act, currently it is section 63 of BSA[19], which stipulate that digital evidence, including emails and electronic records, must be accompanied by a certificate issued by a person responsible for the relevant computer system. This certificate is essential to prove the authenticity and reliability of digital evidence. The ruling emphasized that electronic evidence must be verifiable and meet the legal requirements for admissibility in court. The court also made it clear that without proper certification, digital evidence could be considered inadmissible. This case established key safeguards for the inclusion of electronic evidence, reinforcing the need for careful handling to maintain its integrity[20].

In this case, the Supreme Court addressed the admissibility of forensic reports involving digital systems. The court recognized the importance of digital forensics in investigating cybercrimes and affirmed that forensic reports could be admitted as secondary

[18] India CONST. art. 21.
[19] The BSA, 2023.
[20] Anwar P.V. v. P.K. Bashir and Others 2014 10 SCC 473.

evidence under Sections 63 and 65 of the Indian Evidence Act, currently Section 58 and 63 as per BSA[21]. This decision highlighted the necessity of following established forensic procedures, such as maintaining the chain of custody when collecting and analyzing digital evidence. By upholding the credibility of digital forensics, the court emphasized the role of forensic experts in ensuring the reliability of electronic evidence in court[22].

This present case is also known as the Parliamentary attack case, this case involved the admissibility of intercepted telephone conversations as evidence. The Supreme Court ruled that telecommunications interceptions are legal, and further provided certain procedural safeguards to be followed. The court laid down guidelines for the lawful interception of communications, including judicial oversight, and stressed the need for confidentiality during such operations. This case was significant in recognizing the evolving nature of digital evidence law in India, where the rights to privacy and a fair trial must be balanced with the need for national security and criminal investigations. The decision highlighted the complexity of handling digital evidence, particularly in the context of telecommunication interceptions, and stressed the importance of ensuring compliance with constitutional principles[23].

These landmark cases illustrate the challenges of handling digital evidence in India's legal system, particularly concerning its admissibility, authenticity, and reliability. As technology advances, the legal framework continues to evolve, ensuring that digital evidence can be effectively utilized in criminal proceedings while respecting fundamental rights such as privacy and fair trial. These rulings have paved the way for clearer guidelines and more sophisticated methods for the collection, analysis, and presentation of digital evidence in court.

ROLE OF DIGITAL FORENSICS IN LANDMARK CRIMINAL CASES IN INDIA

Digital forensics has become a crucial tool in solving high-profile criminal cases in India, playing a dominant role in determining negligence or guilt in various crimes. As technology increasingly integrates into daily life, evidence from electronic devices such as mobile phones, computers, and other gadgets has become central to crime investigations. In cases involving financial fraud, terrorism, cybercrimes, harassment, and even murder, digital

[21] Ibid.
[22] State of Maharashtra v. Dr. Prafull B Desai (2003) 4 SCC 493.
[23] State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.

forensics offers valuable insights that traditional evidence might not provide. Electronic data, including call records, internet activity, and digital footprints, can serve as primary evidence, supporting alibis, confirming witness statements, or disproving false claims by suspects. Several landmark cases in India demonstrate the profound impact of digital forensics on the criminal justice system.

One of the most notable cases where digital forensics played a pivotal role was the Arushi Talwar and Hemraj double murder case[24]. The investigation relied heavily on call detail records and internet browsing history to piece together timelines and verify or challenge statements made by suspects. However, this case also exposed the limitations of digital forensics, as discrepancies in the analysis of electronic evidence led to conflicting conclusions. Ultimately, these inconsistencies contributed to the acquittal of the accused by the Allahabad High Court in 2017. This case highlighted the importance of following best practices and established forensic standards to ensure digital evidence is admissible and reliable in court.

Another landmark case that evaluated the power of digital forensics was the 2008 Mumbai Terror Attacks[25]. The digital forensic team played a crucial role in convicting Ajmal Kasab, the only terrorist to survive the attack. Investigators used call detail records, emails, and movement data to trace the attackers' communications, linking them to handlers in Pakistan and uncovering the planning behind the attack. The analysis of mobile phones and satellite communication devices was instrumental in identifying the terrorists' network and securing Kasab's conviction on charges of terrorism, murder, and conspiracy. This case illustrated how digital forensics is essential not only in identifying direct perpetrators but also in unravelling the larger networks behind organized crime and terrorism.

In the Nirbhaya Gang Rape case[26] it has demonstrated the need and necessity of digital forensics in solving heinous crimes. The brutal gang rape and murder of a young woman in New Delhi sparked nationwide outrage. Mobile phone records, CCTV footage, and call logs were used to prove the presence of the accused at the crime scene. The combination of digital evidence, along with medical reports and witness testimonies, led to the conviction of the accused, with four individuals sentenced to death. This case highlighted the sophistication of digital forensic tools in

[24] Dr. (Smt.) Nupur Talwar v. State of U.P. and Anr. (1984) 2 SCC 627.
[25] Rajesh Basrur et al., Front Matter, I (2009), https://www.jstor.org/stable/resrep05887.1 (last visited Dec 15, 2024).
[26] Mukesh v. State (NCT of Delhi), (2017) 6 SCC 1.

confirming the presence of suspects and strengthening the evidence presented in court.

These landmark cases examine the transformative role of digital forensics in modern criminal investigations. Whether confirming alibis, exposing terrorist networks, or solving brutal crimes, digital evidence plays a critical role in the pursuit of justice in high-profile cases in India. However, the cases also emphasize the need for accurate and standardized forensic analysis to ensure that digital evidence is reliable, admissible, and effectively utilized in court.

CONCLUSION

Digital forensics has emerged as a cornerstone in advancing criminal investigations in India, especially in tackling the surge of technology-driven crimes. It has proven to be a force multiplier, enabling law enforcement agencies to uncover, analyze, and prosecute offenses more effectively. Despite its potential, the field faces substantial legal, procedural, and technical challenges that hinder its full integration into the criminal justice system.

One of the most pressing concerns is ensuring the admissibility and reliability of digital evidence in courts. Strict procedural compliance, inconsistent evidence handling, and the lack of standardized forensic practices often undermine the credibility of digital evidence. Additionally, technical hurdles such as advanced encryption, data manipulation, and the deployment of anti-forensic tools by criminals create significant barriers to investigations. These challenges are compounded by the rapid evolution of technology, which often outpaces the capability of investigative frameworks.

High-profile cases have showcased the transformative potential of digital forensics, underscoring the need for more rigorous and standardized procedures to ensure the integrity of digital evidence. Strengthening cross-border cooperation in cybercrime investigations, particularly with nations like the US and UK that have advanced forensic practices, can provide India with valuable insights. Furthermore, equipping judges and legal practitioners with training in digital evidence evaluation is critical for ensuring fair adjudication.

To address these challenges, India must prioritize the establishment of uniform forensic protocols and invest in cutting-edge technologies to enhance investigative capabilities. Collaboration between law enforcement, judiciary, and technical experts is essential to create a cohesive framework that supports the effective use of digital forensics. Additionally, raising public

and institutional awareness about the significance of preserving digital evidence can further bolster its role in criminal investigations.

Moreover, the digital forensics holds immense promise for strengthening India's criminal justice system. By evolving legal and procedural frameworks, standardizing forensic processes, and adopting global best practices, India can ensure the credibility and operational efficiency of digital evidence. This approach will not only modernize the justice system but also build public trust in its ability to deliver justice in an increasingly digital world.