The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 9 | September 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Role of Digital Forensics Under Criminal Justice Delivery System in India

Surbhi Gupta

Research Scholar, Sardar Patel Subharti Institute of Law, Swami Vivekanand Subharti University, Meerut (India). Email, adv.guptasurbhi@gmail.com.

Dr. Prem Chandra

Associate Professor, Sardar Patel Subharti Institute of Law, Swami Vivekanand Subharti University, Meerut (India). Email, premchandra1979@gmail.com.

DOI : https://doi.org/10.5281/zenodo.17314843

ARTICLE DETAILS

Research Paper

Accepted: 19-09-2025

Published: 10-10-2025

Keywords:

digital forensics, cyber-crimes, electronic evidence, investigation, digital law, digital fraud.

ABSTRACT

A Digital Forensic continues to play an important role in Indian criminal investigation system. Digital Forensic help to investigate of cybercrimes. During criminal investigation court faced many types of challenges for collection of Digital evidences, like: encrypted data, violation of data privacy and many more. For all the type of challenges Digital Forensic science has created new path to help in criminal investigation. Therefore, there is an urgent need to develop electronic evidences in forensic science to keep pace with various types of crimes, collect evidence and search for criminals. Many of the various methodologies, modern tools and technologies have found their way into a forensic field designed on the basic of forensics principles. The digital branch of forensic science is witnessing fast development in criminal investigation processes, forensic tools used, and all the various types of evidences. In this modern era, it is very important for forensic researchers to become aware of the new advancement technologies in the developed society and understand the requirement of the future. The past decade has witnessed significantly technological advancement to aiding during a digital investigation. This paper introduced the important role of Digital forensic under criminal investigation and

different types of Forensic data collection come under the branches of digital forensic. Due the large use of computers networks and mobile service, digital forensics becomes more important in law enforcement. Based on Doctrinal research methodology, which analyze the various issues, related roles and development of Digital Forensic evidence and analyzing forensic branches in India?

INTRODUCTION

In advance Indian technology and accessibility of modern gadget in use have remarkably options of various criminal investigations all around the International and National countries. Also, Digital forensic is a co-feature or branch of forensic science. The Cyber-crimes like hacking, digital forensics fraud, phishing, identity theft and in the modern World when digital crimes committed with the new techniques, it requires investigation related Forensic science to be done with the advanced technology and Digital Forensics tools one of such kind of crime investigation. After the Cyber-crimes occurs the criminal print a trace which show or identify in large critical identification needed to prove the intention of the criminal and the cyber-crime using evidence, it can be identify by Digital forensic tools or cyber forensic tool. In 21st century it crosses the whole criminal investigation system in India, from the criminal spot scene to the decision of the courtroom. Its structured policies, emerging threat, offers a range of capabilities and increasing public safety. Digital forensic challenged daily with new changes in technology and the invention in which they can be misused.

DIGITAL FORENSICS

The important goal of Digital Forensic is to figure out what happened, when it happened and who did it. Digital forensics means the application of new technologies, various methodologies to collect actual data to examine the digital information to comply with the legal process. In the advancement of the new methodologies the Indian criminal justice system knows the need and requirement of Digital forensic but still they fail to implement the legal framework. There are many challenges faced by the agencies regarding to the Digital forensics is the privacy of an individual which may be violated using the collection of Cyber data and the misuse of new technologies by the Judiciary system.

Digital forensic is also the fast procedural of collection and analyzing the digital evidences which is admissible in the Indian courts. As in new or modern society continues to believe more on computer devices and cloud computing technologies, individual continue to believers of online network percentage

of modern devices which includes Tablets, Mobile phones, IOT devices and many more. Digital forensics has many formats or resources that forensic experts can be use in investigation as digital evidence for reach final conclusion and increasing range of many criminal strategies, which includes data violations, Cyber-attack etc.

EVOLUTION OF DIGITAL FORENSICS

The evolution of Digital forensic has been closely interconnected to the fast development of techniques in India. In 1980's the use of networks of computer was increased, and that need brought for investigators to recognize the value of Digital networks in solving crimes. This led to origin of the computer forensic as in a different category such as FBI's Magnetic Media Program (1984), Computer Analysis and Response Team (CART) and early forensic software tools. In 1990's personal computer network stared dominating the society, and resulted the need of Digital forensic has enlarge everything related to the networks' and internet.

This century brought rapid growth in digital forensic with (IOCE) International organization on computer evidence (1995), standardized protocols and expansion beyond computer device. In modern Era 2000's the rise of laptops, mobile phones have introduced new challenges, requiring new technologies for extracting data from Cloud storage, artificial intelligence, and various devices. And still continue to evolve new technologies of Digital forensics for helping investigators can solve complex crimes and collect Digital evidences. In present generation, D.F covers a broad range of tools and technologies like cloud computing, Encase, memory analysis, file carving tools, memory forensics and many more. In our modern Indian context, the need of legal acceptance of Digital crimes and digital evidences started in the new era of the Information technology Act (IT) act 2000. After amendments and the essential provisions of "Bhartiya Nyay Sanhita 2023" and "Bhartiya Sakshiya Adhiniyam2023" has been provisional in dealing with Digital forensics, Cyber-crime and electronic evidences. Bhartiya Nagrik Suraksha Sanhita (BNSS), 2023, this new law highlights the role of audio-video technology in police investigations, including recording searches and seizure processes.

MAIN BRANCHES OF DIGITAL FORENSICS

Computer Forensics: Digital forensics or computer Forensics science helps to investigate digital storage evidence and computers devices. It also includes identification of Digital device to recover, identify, preservation, analyzing and presenting facts or opinion related searched information. Computer forensics fields also use common laws principles and technologies to recover device.

Mobile devices forensics: This branch highlights firstly or primarily on recollection and collecting Digital evidences from Mobile devices, also searching many devices with the help of internal and external memory or communicating functionally, such as mobile devices, PDA services, GPS Devices and tablets.

Network Forensics: Network forensics branch helps to finding monitors, registrations, and analyzing networks functioning. Network devices are fast and top dynamic, evenly volatile, or once transmitting, it is gone. Actually, it also means of many new network devices Forensics is continuing proactive criminal investigation proceedings.

Database Forensics: Databases forensics branch includes reporting the access of the devices and helps the criminal investigating related changes happens time to time. It can apply database forensics to various purposes. Additionally, your database forensics analysis also focused on time stamps legislation with the up to date time of a row in relational device base. These types of criminal investigating help to investigator test the database for reliability and clarify the action of an actual Database.

STEPS IN THE DIGITAL FORENSICS INVESTIGATION PROCESS

The National Institute of Standard and Technology (NIST) highlight main four steps which are as follows:

1. **Data Collection**: Recognize the digital techniques or media storage collection relevant data, relevant digital identification and metadata of the digital criminal investigation. After identify the coolected data, they also preserve the accurate copies or applied rest of the criminal investigation.
2. **Examiniation**: After collection data from web browser history, chats, remote storage, deleted space, accessible disk, operating system cashe, investigator can examine all the copies of data. Examination of the data during trial fall into second step of the digital forensics procedure. It is connected to the reliability of evidences digital information of the forensic criminal investigation.
3. **Data analysis**: Forensic investigator uses various methodogies and digital forensics tools to remove data of device from Digital evidence. Analysts can also refer exclusive or open source forensic tools to finding button to mendates threats actions.
4. **Reporting of data**: Once the analysts investigating is complete, then the forensic experts can create a formal and realiable document of report that highlights their relevant finding, involving what happened and who may be possible, It is a last step addopted during the trial of the court proceedings.

TYPES OF DIGITAL EVIDENCE

It is an important step in the Digital forensics process. It includes collection data from various sources, like mobile devices, computers networks, storage media, while assuring the integrity of the digital evidence. After all, collection of various types of digital evidences then investigator required various tools and techniques to be used in their process.

When it comes to criminal digital evidences, it can be related anything from devices, logs and all types of images, video recordings, archives, replicate data, duplicate storage, metadata, residual files, and even devices which stored or hidden inside a devices RAM, as long as they all are related as part of mindset for a digital criminal investigation in Indian judiciary system.

Logs: logs belong to the eyesight device data types category, in which could be anything from: os logs, database logs, Gmail logs, Software logs, networking logs, door accessing record, android logs, IP logs, data server logs, and fingerprinting device. To successfully conducting various logs forensic, the main and prior key is a log forensic expert should be knowingly about various logs of such kind is that can be automatically and directly placed on the logs and devices, either by various kind of technological software that is downloaded or by cooperating system itself. At the accordance of time, system logs or software can also contain a data of identification about the access data and security mistakes as warnings and notification.

Video recordings and images: These types of digital forensics evidences, video recordings or footage can be directly classified as the visible or eyesight data evidence type, as like video logs. There are many types of digital evidences which includes in this evidence category, involves video recording on mobile device, CCTV footages, digital camera footage and many more.

Archives: Archives evidences are regular files reachable directly from the device explorer, they also fall into a visible data type group. Like: zip/rar/similar files, software, databases, backups, etc. They can also create all logs of exactable file format, in which regulate anything from, videos, images, text messages, documents, sources items, or even any other hidden archives. In the same process of investigation, these produce as a large source of digital evidence that can contains data in many fields' relevance to breach of the criminal case in hand.

Active data: This is specified to as accurate data and also, it's an insight or visible device types. In the popular content editors related Microsoft word often recover temporary devices on hard drives. Additionally, various operating system or software could create many types of related files like: Gmail

clients, images viewer, word processor, scanning, archives etc. The main believers to accuracy about this digital evidence is that Cyber criminals related are often smarter to hide, delete or manipulate the accuracy and originals, but sometimes cyber criminals forget to erase the actual files that sort behind the operating systems.

Metadata: Metadata evidence falls into an invisible evidence type's field because it is urgently requiring special software to be competent to visual. An images or photo files on a hard drive could contain additionally devices relating the files identification where the images were captured, otherwise as knowingly as EXIF data. This device of data also connected to the device and revealing the data affirmation such as: where the spot of images was taken, what type of lenses was used during the proceedings, the cameras brands and models, coloring profile and many more.

Residual DATA: Residual data is like to recover the deleted or overwritten data. It is not type of visible data, it considers as unseen data or device type. If any person deletes a data from device, then data is still present there. That all formatting data the chances of being overwritten by any other device or data, which is reliable if there, are many hard drives is running out. It is very beneficiary evidence if someone wants to recover deleted data from device by using DRS by Salvation data, not only deleted data but also corrupted or manipulated data.

Volatile data: This type of data is unwritten type of disk itself; hence it belongs to the unseen or invisible data or device type. The RAM requires checking and detecting them, volatile data for obvious reasons the data of device is circulated off, neither, it can be lost permanently. Volatile data can be tricky specifically analyzing and often necessary forensic RAM imaging its content in the actually or original state.

Replicant data: Replicant data is an invisible data type. Where there is the evidence list, the replicant data came into force. There are many incidents when various software types can drop temporary backups and many directories to stop the unblessed or unfortunate scenario of lost devices. Examples of this data includes: web cache and cookies, temporary directories, data blocks, memory etc. It is helpful digital forensic evidence for examine and collection the crucial details, in case to hide incriminating evidence by formatting the important files, replicant data can be used source of evidence to prove their guilt.

LEGAL FRAMEWORKS GOVERNING DIGITAL FORENSICS

The evolving of legal framework surrounding digital Forensics in highlighted in recent reforms such as the BNS, BNSS ns BSA, and these acts emphasizes the importance of the Digital forensics' evidences in modern law enforcement. Following are the main provisions in relation to Digital Forensics.

Bhartiya Nyaya Sanhita, 2023

This section highlights the use of *document* which includes electronic and digital record, or which may be used, as relevant evidence of that related matter.

This provision defines the act jeopardize honors and sovereignty, unity and integrity of our India, whoever knowingly or purposely spoken either words, written or by signals, and *by electronic communication* or by use of financial mean, excites or attempts to excite, or promote and encourage vibes of separatist activity's or unity and integrity of our India.

This provision or section highlights the launching the enmity between various branches of religion, race, and residence, place of birth, language etc, and these acts prejudicial to dignity of maintenance of consonance included or *through electronic communication.*

This section explains Extortion, *threatens by sending emails* or messages through an electronic device to give such type of committed extortions or give him money.This main provision *related record of forgery* in the courtroom of Public register etc, involves whoever forges a false papers or any electronic records, purporting to be a records or an identity document issuing by the Government or proceeding or trial of in a court.

Bhartiya Nagrik Suraksha Sanhita, 2023

This section allows officers of Police to record and maintain the statement of identifiers during examination of identification parades by using audio video techniques, mainly if the identifier is physically or mentally disabled person. This section also ensures that the statement of the legal documents is legally admissible, even in individually related cases who may struggle traditional identifier processes.

This provision specifies that all police investigators can be recorded with using audio video techniques. This also involves the documentation of such places inquiries and item seized during operations of Law enforcement. Along with this the list of recorded footage must forwarded to the judicial authority. So, this provision ensures the accountability and transparency in the criminal investigation process, especially dealing with cases related digital forensic evidence that can be tampered or contested in the court room.

This provision requires related evidence from Rape victim to be recorded at their work place, home, or other proffered location, by a female police officer also in the presence of their Guardian, parents and

any social worker (if any). Mainly the aim of this provision is to protect the privacy and dignity of rape victim and also ensuring that the evidences are preserved. Which can be includes Digital content as like text messages, emails or images.

This important section mandates that the criminal cases which has punishment of seven years imprisonment or more of imprisonment, essential play a role of forensic science in such types of cases. Also, this section is mandates for ensuring that the digital evidences such like mobile devices, data collection from computers, or many others digital equipment is preserved and also used in trial of the court.

This section permits the officers to record witness's statement with the help of audio video techniques at their discretion. Actually, this provision is especially beneficial while dealing with the vulnerable witnesses or those people who is unable to appear physically because of health issue, due to long distance or any other fear of intimidation.

This provision allows the examination and identification of the accused through the digital electronic means, as alike video conferencing. This section ensures the fair and reliable trial for the accused, mainly cases related where Physical transportation can pose of security risks, or accused is unable to present in the courtroom due to any reason.

This section provides the collection of various Forensic samples which falls under a Magistrate order. These types of samples include signatures, fingerprints, and handwriting and voice notes. In the new Digital age, these types of samples may also include voice recordings, biometric data and Digital fingerprints, that are also used in investigation related Digital forensics.

The admissibility and reliability of evidence in Indian courts depends to the originality of Digital evidence and relevancy of the offer in Indian justice system. **(Bhartiya Shakshya Adhiniyam, 2023)** BSA describes the process proof of electronic evidence. This provision explains that a certificate stating how the electronic record was made, the identity of that device and declaration by the making person of electronic record. In *State* ***(NCT of Delhi) v. Navjot Sandhu (2005)****:* The Supreme Court of India held that the reliability and admissibility of Electronic record, ruling they can be acceptable without a certificate under provision 65B (4) of the Indian Evidence Act.

Anwar PV. v. PK Basher (2004): The Supreme Court reversed their decision addressed that the reinstated of certificate requirement for Electronic records, highlights the requirement of a document of certificate under provision 65b of evidence admissibility. Later on in the landmark case ***Arjun Pundit***

Khotkar v. Kailas Kushiro Goyatan : the Supreme Court pointed out that Sec 65B certificate can may be allowed to be proceed later if it is at all impossibilities to obtain the same at the time of filing. The S.C judgment expresses a sensible nature without violating the principles of procedural fairness and legal certainty.

For instance, in ***K.L. Nagadev v. State of Karnataka13***, the High Court of Karnataka overruled the judgment and touches upon a wide topic related the admissibility of Electronic evidences that was collected by storage devices by the investigator, wherein the State had not so much strict about following the related provision of the Indian context like Code of Criminal Procedural, also given under **section 79A' of the 'Information Technology Act, 2000'**, which promote the appointment of government authorized digital related experts that can be reduce or less risks of seizure of digital evidences produce in the courtroom. This type of change related electronic evidence is the heart of judiciary during updated to keep pace with the techniques advancing or the ever-developing facts of computer criminality.

Digital Evidence or electronic evidence is "any significant information storage in digital form that can be a party to a court case may use during trials. **Section 79A of Information Technology Act (Amend. Act, 2008),** defines electronics form evidences as try to proven the actual value that is either covered or transmitted in electronic form and also includes Computer evidences, digital audio recordings, digital video footages, cell-phones, fax machines. Digital Evidence also explains as information and data of valuable investigation that is stored on, received or accepted by an Electronic device. Digital evidences to all types of Crimes involves: Cyber-threats, Cyber-larceny fraud scams, online credit cards, Cyber identity theft, internet Counterfeit, electronic Funds transactions, Cyber harassment, Cyber stalking, Cyber copyright infringement.

The K.S Puttaswamy v. Union of India *case* decided into 2 parts, firstly decided in 2017 related *Right to privacy*, Supreme Court stated that privacy which include the legal right to control personal data and protect it, is an intrinsic part and any seizure of privacy by the state must satisfy a 3 fold test: legality, proportionality, and legitimate aim. Secondly, decided in 2018 related *Aadhaar Act Judgment*, the S.C highlights the issue of Digital surveillance, seizure of privacy was served a larger public interest. Thus, the Supreme Court decided that any inspection of data collection by the non-state or state actors must be proportionate to the aim being pursued.

In the case of ***Nirbhaya Gang Rape case (2012),*** the case refers to the Rape and murder of a young woman in New Delhi. In Nirbhaya case digital evidence and CCTV footage, was played crucial role for identifying and apprehending the suspects. It also support criminal investigation for forensic analysis of

the bus and various physical evidence, the prosecution also relied on forensic evidence, including DNA identification or witness testimonies. This case also showed how the sophistication of Digital forensic technology delivered to help in the inconsistency of the hard to solve modern criminal investigation.

Digital forensics has become a crucial tool in solving crimes in India, but still India has seen a significant surge in digital crimes cases, with an average of *7000 cases reported daily in 2024, marking 113.7% increase compared to previous years, victims lost over 120 Crores to digital frauds in 2024.* The Indian government has taken step to combat digital crimes, including setting up *The National Cyber Crime Reporting Portal (NCCRP) and (ICCCC) The Indian Cyber Crime Coordination Centre (14C).* These agencies have blocked 2.75 lakhs fraudulent phone numbers and prevent potential frauds worth 4000 Crores in 2024.

CHALLENGES IN DIGITAL FORENSICS

Digital forensic in modern criminal investigation faces various challenges, including:

1. **Technical Challenges**: Encrypted data can be very difficult to analyze and access, the complexity of new modern digital system can make it challenging to recognize and identify relevant evidence. Changing in rapid pace of technology can make it very difficult for investors to keep up with the latest tools and techniques in India. And the large volume difficulty of Digital data can make it also challenging to analyze relevant evidence in criminal investigation.
2. **Legal and Procedural Challenges**: Admissibility of Digital evidence must need certain standard to reliability of evidences or to maintain certain chain of custody for Digital evidence is crucial to ensures it admissibility or integrity. In legal jurisdictional issues of digital crimes there is multiple jurisdictions involve, making it challenging to determine which authorities have jurisdictions. Also investigating digital crime often requires International corporations, which can be challenging in Legal proceedings.
3. **Investigative Challenges**: When cases involving large amount of data identifying relevant Digital evidence can be challenging and analyze complex evidences, such as Malware or encrypted data, needs experts' specialists. Investigators also must stay up to date with the new techniques and technologies adopted by the modern criminals, also balancing the needs to gather evidence with protect individual rights and freedoms.
4. **Resources challenges**: Digital forensics resources like specialized equipment and expertise is short supply and Investigators also need of training and expertise to affectivity investigate Digital forensics crime. And Investigators has also resource intensive and limited Budget.

These Challenges highlights the complexities of Digital forensics science in Criminal investigations and requirement for ongoing training, expertise, and equipment's to effectively investigate Digital forensics crimes.

CONCLUSION

The Digital forensics helps immense promise for strengthen India's criminal investigation. By involving legal and procedural framework, India can ensure the legality, credibility and operational efficiency of Digital forensics. A Digital forensic procedure given to the criminal investigators important assistance related gathering digital evidence admissible in the Indian court. Digital evidence must be admissible, authenticated and accurate in order to be accepted in the court. This paper also examined various methods of tools for digital forensics which is used to analyze security frauds. D.E collected from the data structured resides in the important device using several tools. In digital forensics analyses, various tools are not only helping to collect and identify data but they are required to find the mysteries of all the conflict accrues in the execution phase.

REFERENCES

1. Vaibhav M. Agrawal, "Critical Analysis of Forensic Science in Effective Administration of Criminal Justice System in India" Indian Journal of Legal Research 12 (2023): 78.
2. Hem Lata B. Patil, Anjula Chobe, "An Examination of Digital Evidence and Its Relevance for Indian Forensic" Educational Administration Theory and Practice 30 (2024):112.
3. Radhika Verma, "Role of Digital Forensics and Criminal Investigation in India" International journal of research and publication and reviews 5 (2024): 8.
4. Harjinder Singh Lallie, "An Overview of the Digital Forensics Investigation Infrastructure of India" Digital Investigation 9 (2012): 4.
5. Kam-Pui Chow, Advances in Digital Forensics V1 (IFIP International Federation for Information Proceeding) (2010).
6. Mohammed Alkhanafseh, Mohammad Qatawneh and Wesam Almobaideen, "A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a focus on Cloud Forensics" International Journal of Advanced Computer Science and Application 10 (2019): 1.
7. BlueVoyant. "Understanding Digital Forensics: Process, Techniques, and tools." Accessed June 26, 2025. https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools#what-are-the-different-branches-of-digital-forencics.

8. Fedelis Security, “Mastering the Digital Forensics Process: Key steps Explained” (Education Center, 28 Jan 2025) Accessed 1July,2025 https://fidelissecurity.com/cybersecurity-101/learn/digital-forensic-investigation-process.
9. B Nelson, A Phillips, and C Seurat, ”Guide to Computer Forensics and Investigations” (6th edn,Cengage 2019) Accessed 5 July,2025 https://faculty.cengage.com/works/9781337568944
10. Pruthi Ramkanta Hegde, “All about digital evidence” (2024) Page on IPleaders blog. Accessed 6 july,2025.https://blog.ipleaders.in/all-about-digital-evidence/#What_is_digital_evidence
11. Axon, “5 common types of digital evidence (and what you should know about them)” Accessed 8July,2025https://www.axon.com/resources/5-common-types-of-digital-evidence-and-what-you-should-know-about-them
12. Muzammil M, “A Robust Technique of Anti Key Logging Mechanism” (Digital Ecosystem and Technologies Conference. Inaugural IEEE-IES, 2007) DOI:10.1109/DEST.2007.371990. (2007).