DIGITAL FORENSICS AND LAW: EVIDENTARY CHALLENGES IN THE CYBERCRIME PROSECUTIONS

Uddandi Kavya Sri, BBA LL.B. (Hons); GITAM School of Law, GITAM (deemed to be University)

ABSTRACT

The current era is recognized as technological because of advanced technological development globally. There are numerous advantages due to technology and the internet nowadays. Everyone is dependent on technology and the internet to know anything new. As technology develops, there is a vast increase in cybercrimes. Every coin has sides; in the same way, every product will have pros and cons. The development of technology is also giving rise to many cybercrimes like hacking, deepfakes, phishing, Mishing, etc., and new kinds of cybercrimes are evolving daily. The traditional method of investigation and the judicial practices are not effective enough to find the culprit and evidence to convict the offender. Little attention is given to digital Forensics, which result from the shift in the investigative and the judicial practices or methods to prosecute and convict the offender of the cybercrimes. The digital Forensics is the new concept in the legal system; it has some core evidentiary challenges and gaps within the legal and forensic protocols. This paper focuses on the analysis of the evidentiary challenges and its protocols over the digital Forensics and provides some suggestions or recommendations for the effective incorporation of the digital Forensics in the cybercrime prosecutions.

Keywords: Digital Forensics; Cybercrimes; Evidentiary Challenges; Hacking; Deepfakes; Cybercrime prosecutions; Cybercrime Investigations.

INTRODUCTION

In the current lifestyle of the people, the technology became an intrinsic part of our daily life. The human's dependence on the technology increasing day to day which resulting in the cybercrimes. Everything will have two sides with pros and cons. In the same way, the technological development and advancement have both pros and cons whereas the general public use technology to make their work life style ease with the technical assistance and to learn the new things but the offenders or the criminals are using or exploiting the technology to commit various crimes which are termed and recognized as the cybercrimes like financial frauds, deepfakes, terrorism etc[1]., The Forensics has a great importance in the legal system. The Forensics are used in the two parts of a crime; they are crime investigation and the criminal proceedings. Whenever, a crime happened, the Forensics plays a pivotal role in finding the accused of the crime like fingerprints, footprints, blood samples, DNA samples etc., In the same the digital Forensics plays a crucial role in the cybercrimes. The digital forensics are utilized in the cybercrime's investigation procedures. The digital tools like log analysis, network traffic scrutiny; malware destructions and data recovery techniques are used in the cybercrime investigations, which can be termed as the digital forensic tools[2]. As mentioned above, the concept of the digital Forensics evolved from the traditional forensic technology or science which addresses the unique challenges for the digital evidence of the crimes. In the early 2000s, the digital Forensics are completely focused on addressing the Self-contained PC[3] and the Connected or linked PC[4]. As the development is started, the focus of the digital Forensics is extended its scope and included the evidence recovery from any electronic device which had a storage space in it, resulted in removal of the role of digital Forensics from the investigation of the computerized crimes to the all kinds of the cybercrimes[5]. . As the development is started, the focus of the digital forensics is extended its scope and included the

[1] Naeem Allah Rakho, "Cybercrimes and Law: Addressing the Challenges of Digital Forensics in Criminal Investigations" < https://www.scielo.org.mx/scielo.php?pid=S1870-05782024000100023&script=sci_arttext> accessed 1st October, 2025.
[2] Rafifah Syaakirah; Luthfiyah Syifa; Iskandar Muda, "DIGITAL FORENSIC INVESTIGATION IN CYBERCRIMECASES: CASE STUDIES AND RECOMMENDATIONS" http://upubscience.com/upload/20250114142628.pdf accessed 1st October, 2025.
[3] The Self-contained PC is also called as the Standalone PC which refers to the computer which can be worked without any internet connectivity (independent).
[4] Connecter or Linked PC refers to the computer which can be worked through the connection of the internet.
[5] David Mugisha, "ROLE AND IMPACT OF DIGITAL FORENSICS IN CYBER CRIME INVESTIGATIONS" (March, 2019) https://www.researchgate.net/profile/David-Mugisha/publication/331991596_ROLE_AND_IMPACT_OF_DIGITAL_FORENSICS_IN_CYBER_CRIME_INVESTIGATIONS/links/5c9a2f38299bf11169486413/ROLE-AND-IMPACT-OF-DIGITAL-FORENSICS-IN-CYBER-CRIME-INVESTIGATIONS.pdf accessed 1st October, 2025.

evidence recovery from any electronic device which had a storage space in it, resulted in removal of the role of digital forensics from the investigation of the computerized crimes to the all kinds of the cybercrimes.

OBJECTIVES OF THE STUDY:

- To distinguish the considerable evidentiary challenges encountered during acquiring, salvation and presenting of the digital evidence in the cybercrime proceedings.
- To analyze the efficiency and the limitations of the existing legal and forensic methodologies in the cybercrimes.
- To suggest some legal reforms and practices which might help in improving the methodologies in the admissibility of the digital evidence in the cybercrime proceedings.

SCOPE OF THE STUDY:

The scope of the paper "Digital Forensics and the Law: Evidentiary Challenges in Cybercrime Prosecutions" embraces a thorough analysis on the technical, procedural legal aspects which are included in the authentication, acquiring, examination, conservation and presentation of the digital evidence in the cybercrime cases. It focuses on the interconnection and distinction between the modern technology in the investigations and the legal prosecutions which administer admissibility of the digital evidence in the prosecution of the cybercrimes in India. Besides, the paper analyses the complexities with in the technical development and the diversity in the advance anti-forensic tactics by the criminals and the cross-border cooperation issues to implement the cyber laws to prevent the crimes. This paper strictly focuses on the distinction of the evidentiary challenges at different stage of the case and proceedings along with the examination of the legal limitations and efficiency of the forensic methodologies in the crime solving and the justice delivering.

SIGNIFICANCE:

The study has its own significance of the critical analysis of the forensic especially the digital Forensics which is considered to be a backbone for the investigations and the prosecutions of the cybercrimes which are rapidly expanding due to the technological advancement and the

development now. The cybercrimes don't leave any kind of the physical evidentiary traces where the only hope of the crime investigation is the digital Forensics, which is important and ensures the gathering, authentication, safeguarding and the presentation of such digital evidence to have successful prosecutions in justice delivery.

HYPOTHESIS:

The advancement and development of the technology is a reason for the limitation in the admissibility of the digital evidence by the court in the cybercrime prosecutions or proceedings.

RESEARCH QUESTIONS:

- What are the technical and procedural limitations and challenges in admissibility of the digital evidence in the cybercrime proceedings by the court?
- How the existing forensic methodologies manage the implications of the authenticity and integrity?
- What kind of the reforms or systems are essential to connect gaps between the Forensics and the legal admissibility and its requirements?

RESEARCH METHODOLOGY:

The doctrinal research is made for the study especially on the standards with respect to the admissibility of the digital Forensics in the legal systems along with the gaps within the admissibility as well. The present research draws on the information from books, journals, articles and other internet sources. The research paper uses the Bluebook model as its reference style.

FUNDAMENTALS OF DIGITAL FORENSICS

Digital Forensics which are also popularly known as the cyber-Forensics[6]. The digital Forensics are a part of science especially the forensic science which especially concentrates on the investigations and the examinations of the electronic devices such as the computers,

[6] "Impact of the forensics in Modern Crime Scene Investigations" (24 February, 2025) https://post.edu/blog/impact-of-digital-forensics-in-modern-crime-scene-investigations/ accessed 04th October, 2025.

laptops, smartphones etc., to gather the evidences for the purpose of solving the cybercrimes[7]. This science (digital Forensics) helps in addressing the legal issues as the law and the science are interconnected to each other in some aspects but the validity of any kind of the scientific evidence depending on the admissibility by the court of law. The digital Forensics has great importance as it helps in the following activities such as:is science (digital forensics) helps in addressing the legal issues as the law and the science are interconnected to each other in some aspects but the validity of any kind of the scientific evidence will be depending on the admissibility by the court of law[8]. The digital forensics has great importance as it helps in the following activities such as:

Data collection: To collect the digital evidence in a crime, it is very important to depend on the technical expert in the digital Forensics. They use various methods to retrieve the information from the electronic devices. The process of data collection is very crucial step because it will be the clue giving step of the case where the case might go on the right or wrong track which might result in change of the justice delivery. The forensic specialists are very specific with respect to the tools and the software for collecting the digital evidence to be precise and prevent the data alterations after the collecting the data which have serious consequences. to be precise and prevent the data alterations after the collecting the data which have serious consequences[9].

Data recovery: The data recovery must be speed from the electronic devices is the one of the best uses of the digital or computer forensics. The speed data recovery is utmost important to handle the digital evidence and the Forensics[10].

Accurate Data Analysis: The data which is collected and recovered by the technical expert is detailly analyzed to provide the investigators with some insights which would become a breakthrough for their investigations. The modern forensic methods make the investigators to gather more evidence might be the physical and digital from different sources mobiles and network logs and more. These analyses support in the legal proceedings to draw a decision

[7] Annie Badman, "What is Digital Forensics? https://www.ibm.com/think/topics/digital-forensics accessed on 04th October, 2025.
[8] "Digital Forensics in cyber security" (23 July, 2025) https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/ accessed on 4th October, 2025.
[9] Kavya Shree and Apoorva Shree, "DIGITAL FORENSICS IN LAW ENFORCEMENT: IMPORTANCE AND CHALLENGES" https://www.ijlra.com/details/digital-forensics-in-law-enforcement-importance-and-challenges-by-kavyashree-r-apoorva-sri-a-r accessed 04th October, 2025.
[10] Ibid.

based on the strong evidence produced or presented before court of law[11]. support in the legal proceedings to draw a decision based on the strong evidence produced or presented before court of law.

- **Digital Forensics and Cyber Security**

  Every person will have an idea over the concept of the digital Forensics concentrates on the criminal investigations like cybercrimes but the knowledge of the interconnection between the digital Forensics and the cybersecurity is very rare. The cyber security is branch of the investigative department which addresses or concentrates on the investigations of the cybercrimes. The cyber security uses multiple kinds of the digital Forensics to deal with the cybercrimes and the crucial information found out and the other electrical evidence like data recovered will be presented before court of law as evidence. The digital Forensics are used by the cyber security for the purpose of following: cybercrimes and the crucial information found out and the other electrical evidence like data recovered will be presented before court of law as evidence[12]. The digital forensics are used by the cyber security for the purpose of following:

  - To find the root cause behind the cyberattacks and cyber crimes.
  - To protect the digital evidence gathered before the sensitivity of such evidence is exploited.
  - To track the traces or footprints of the hacker and to identify the tools or the software used by the hackers for the crime.
  - To ensure the data or the information is safe.
  - To identify the supporting network for the illegal access.
  - To trace the origin of the offender or hacker through the login activities or the

[11] Kavya Shree and Apoorva Shree, "DIGITAL FORENSICS IN LAW ENFORCEMENT: IMPORTANCE AND CHALLENGES" https://www.ijlra.com/details/digital-forensics-in-law-enforcement-importance-and-challenges-by-kavyashree-r-apoorva-sri-a-r accessed 04th October, 2025.
[12] "Digital Forensics in cyber security" (23 July, 2025) https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/ accessed on 4th October, 2025.

tools.

❖ **Digital Forensics and Forensic Accounting**

The intersection between the digital Forensics and the forensic accounting is very important and crucial to deal with the financial fraud which is also considered as a cybercrime. The professionals in the either fields will collaborate with each other in order to reveal the complex financial fraud schemes through the technology. The forensic accounting professional deal with the improper and suspicious transactions by the individual or the company etc., in the either fields will collaborate with each other in order to reveal the complex financial fraud schemes through the technology. The forensic accounting professional deal with the improper and suspicious transactions by the individual or the company etc[13].,

❖ **Types of Digital Forensics**

The digital Forensics have various stages and kinds of the technics and methods to do the crime investigation which is used in different kinds of cases. To combat the various kinds of cybercrimes, the cybersecurity uses the different digital forensic technics to specific cybercrime. The kinds of the digital Forensics are as follows: different digital forensic technics to specific cybercrime[14]. The kinds of the digital forensics are as follows:

A. **Computer forensics:** The branch or the wing of the digital Forensics includes the examination of the computers in order to identify, analyze and gather the evidence of the cybercrime. The computer forensics is field where the investigative methods are techniques are used for the forementioned purposes especially from the computer devices.

B. **Mobile Forensics:** Mobile device forensics is also a branch or a wing in the digital Forensics where the investigative techniques are used to retrieve or

[13] "Impact of the forensics in Modern Crime Scene Investigations" (24 February, 2025) https://post.edu/blog/impact-of-digital-forensics-in-modern-crime-scene-investigations/ accessed 04th October, 2025.
[14] Ibid.

recover the data from the mobiles, smart watches and GPS devices etc., as evidence.

C. **Network forensics:** The network forensics addresses the network activities of the offenders like the internet usage, messages, emails, IP addresses etc.,

D. **Database forensics:** This wing of the digital forensics concerns on the investigation and examination of the activities in the database like the changes made to the information or data, to investigate the crime[15].

❖ **Digital Forensics and Investigation Procedure**

The cybersecurity surely uses the digital forensic science in the crime investigations especially in the cybercrimes in the data collection and the digital evidences of the case[16]. The cybersecurity has a specific procedure in the data collection and the evidence in the cybercrime cases as follows:

Step 1: Request of forensic: The request for digital Forensics shall be made within the case investigation which consists of the purpose, scope and methods of Forensics to be used. It gives a clear outline to continue the investigation of the crime.

Step 2: Extraction: This is considered as a most crucial step in the investigating procedure of the cybercrime where the forensic experts will be preparing the testing procedures in the clear documentation step by step to provide as evidence. In this step, the experts will extract or retrieve the data relevant to the offender or offender's activities from the electronic devices like files, deleted data, the transmission of the data, network usage and data etc.,

Step 3: Identification: The experts try to identify and find the relevant data to the retrieved data from the devices which gives a clear understanding of the data and prevent the investigators from misleading in the investigation procedure.

[15] "Digital Forensics in cyber security" (23 July, 2025) https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/ accessed on 4th October, 2025.
[16] Jia-Rong Sun; Mao-Lin Shih; Min-Shiang Hwang, "A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure" http://ijns.jalaxy.com.tw/contents/ijns-v17-n5/ijns-2015-v17-n5-p497-509.pdf accessed on 4th October, 2025.

Step 4: Analysis: The relevant data which is identified in the previous step will be analyzed to find the evidence which are hidden or erased in the electronic device which is seized by the investigators in the procedures. In this step, the expert will try to find out the person who created it and the alterations made to the data by him like alteration in the documents or photos or videos and also to whom the data is transmitted.

Step 5: Forensic report: The forensic expert after the analysis of the data gives a detailed report over their findings in the cases along with the proper chain of clues along with the tools and techniques used to identify the data. The proper documentation of the report is made to produce as evidence before court of law.

Step 6: Case level analysis: The final analysis shall be made by reviewing the findings of information and the evidence which helps in the drawing the final conclusions of the investigators in the case[17].

- **Role of digital forensic experts in the Investigations**

The role of the forensic expert is very crucial in the investigations of the cybercrimes. The scope of the cybercrimes is increasing rapidly from day to day in the current era. The reason behind it might the development of the technology in this era. Now, the cybercrimes are the biggest threat to the world as the technological development is taking place where the internet usage took part in the personal life an individual. It has a massive effect on the society where a single cyber-attack would lead to the financial loss and integrity; the IPR infringement and loss of the national defence information in certain cases. The fact is that the technology also brings the positive changes in the society like spreading the essential information which help the people but it is also misused by the people for their personal use or benefit. The digital forensic experts will deal with the finding of the traces of the offenders or the criminals in the cybercrimes through their forensic techniques or methods in retrieving the evidences like the network logs, creator of cyber threat links or the fraudulent links, the alteration of the original data and the transmission of the data. These can be done by the forensic experts by using the certain digital forensic tools namely: Autopsy; Disc manager; Cyber

[17] "Digital Forensics in cyber security" (23 July, 2025) https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/ accessed on 4th October, 2025.

Triage; Email forensic etc[18]., Without these experts it will be difficult in finding the offenders and prosecute them in the court of law as it need the technological knowledge to go into the hidden websites to find the traces and do the ethical hacking etc.,

DIGITAL EVIDENCE AND ITS ADMISSIBILITY:

The general meaning of the term evidence is the proof of the actions or records of any action or any other relevant information. So, the term digital evidence means the stored or transmission or any collection of any information in a device is itself a proof of the actions before the court of law. The electronic devices or electronics are everywhere around the world. The people around the world are accessing the electronics like computers, mobiles, laptops and internet in the current era which is recognized as the technological era due to its development. The electronic devices and internet are only sources of the digital evidence. The scope of the digital evidence in approximately 1990s are limited to the data in the computers but the technology is developing day by day. Therefore, the scope of the digital evidence is extended to the internet access, computers, laptops, mobile and any other devices which can store the information or data in it. The digital evidence can be in any form like messages, emails, videos, photos, voice recordings.

Admissibility of the digital evidence: The digital Forensics has two dimensions such as the legal considerations and the admissibility of the digital evidence. Now-a-days the usage of the electronic devices by the public to communicate with each other. So, it became common to use the digital evidence in the prosecution of cybercrimes against the criminals. Due to the wide use of the digital devices, the question of the admissibility by the court into the picture because of the various reasons. In general, the digital evidence is admissible by the court in the prosecutions. by the public to communicate with each other. So, it became common to use the digital evidence in the prosecution of cybercrimes against the criminals. Due to the wide use of the digital devices, the question of the admissibility by the court into the picture because of the various reasons. In general, the digital evidence is admissible by the court in the prosecutions[19].

[18] "Digital Forensics in cyber security" (23 July, 2025) https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/ accessed on 4th October, 2025.
[19] "Impact of the forensics in Modern Crime Scene Investigations" (24 February, 2025) https://post.edu/blog/impact-of-digital-forensics-in-modern-crime-scene-investigations/ accessed 04th October, 2025.

The **Information Technology Act, 2000** made the digital records admissible by court through its provisions like **Section 5** which gave a legal recognition to the electronic signatures. Generally, the signature is made by a person for the authentication of the information in the document where the signature means the physical. Through this section the central government declared the electronic signatures as valid according to the standards set by them. **Section 79A** which is added through the **Information Technology Amendment Act, 2008** states that the central government may appoint an examiner to examine the digital signature for the authentication of the expert suggestions in drawing the decision[20].

The **Bhartiya Sakshya Adhiniyam, 2023** made the electronic evidence as the primary evidence as the actual documents produced before the court under **section 57** where as the **section 65B of the Indian Evidence Act, 1872** states that the electronic evidence as the secondary evidence but the actual documents are primary evidence produced before the court and also states that the electronic evidence must be examined by the expert and get the authenticity to produce as evidence before the court against the other party[21]. The same is held in the case of "Tomaso Bruno & Anr vs State Of U.P"[22], In this case the CCTV footage is produced before the court as electronic evidence but the court refused to recognize the evidence as the electronic evidence is not certified by the technical expert under section 65B of the Indian Evidence Act, 1872.

CHALLENGES OF THE DIGITAL FORENSICS:

The evolution of the technology greatly impacts the digital Forensics in the investigations and also posing the unique challenges in its admissibility in the court. the digital environment is dynamic in nature which changes from day to day. The forensic experts and the investigators have to adopt the new techniques or methods along with the new tools to combat the cyber threats and cybercrimes. Due to the advancement in the technology especially Artificial Intelligence (AI) is main threat to the digital Forensics and the cybersecurity. The Artificial intelligence doesn't have the complete human behaviour of the considering the right and wrong in its actions. The criminals are using the AI in committing the cybercrimes in an[23]. The AI

[20] "All about digital Evidence" (23 February, 2024) https://blog.ipleaders.in/all-about-digital-evidence/#What_is_digital_evidence accessed on 5th October, 2025.
[21] "All about digital Evidence" (23 February, 2024) https://blog.ipleaders.in/all-about-digital-evidence/#What_is_digital_evidence accessed on 5th October, 2025.
[22] (2015) 7 SCC 178.
[23] Srinivas Katkuri, "Legal challenges and lacunas in the digital forensics jurisprudence in India" < https://www.lawjournals.org/assets/archives/2024/vol10issue3/10110.pdf> accessed on 5th October, 2025.

which is used for the security of the privacy but the offenders using the same technology or AI to commit the offences or cybercrimes. The challenges of the digital Forensics are as follows: digital forensics and the cybersecurity. The Artificial intelligence doesn't have the complete human behaviour of the considering the right and wrong in its actions. The criminals are using the AI in committing the cybercrimes in an easy way. The AI which is used for the security of the privacy but the offenders using the same technology or AI to commit the offences or cybercrimes. The challenges of the digital forensics are as follows:

1. **Encryption**: It is known as the main hurdle or the obstacle in gathering the digital evidence[24]. The encryption is a kind of technique which used for the protection of the data, in includes the process of the message is converted into a code which is not easy to decode to prevent from the unwanted access to such information. Even though it is an important and essential tool to protect the privacy of the individual information, actually it is very hard to do without the decrypting key as it includes the complex algorithms. The offenders are decrypting the codes and accessing the personal information of the public without any decryption key. Although the law taking the assistance of the IT industry to have strong encryption of the data but failing in or other way which is making difficult in balancing the privacy rights and the law enforcements[25].

2. **Data Recovery:** Data recovery which is another challenge in the digital evidence admissibility by court. The data which is a confidential, crucial for the integrity of the state or prosecution of the cybercrime is intentionally is deleted by the cybercriminals to remove the traces of their activities and plans[26]**.** The data recovery one of the main issues before the forensic experts as the forensic methodology is still not advanced to the extent needed now. The techniques which are used by the technical experts are not good enough to retrieve the data which is erased from the cyberworld or cyber environment. Despite of these efforts, there is no guarantee of the data recovery which

[24] "Digital Forensics in cyber security" (23 July, 2025) https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/ accessed on 4th October, 2025.
[25] "Digital Evidence Challenges in Federal Cybercrime Trials" https://federal-criminal.com/computer-crimes/digital-evidence-challenges-in-federal-cybercrime-trials/ accessed on 5th October, 2025.
[26] "Digital Forensics in Cybercrime Investigation" https://ijcat.com/archieve/volume13/issue10/ijcatr13101010.pdf accessed on 5th October, 2025.

is the reason for the question of admissibility of the digital evidence in the court[27].

3. **Jurisdictional Boundaries:** The jurisdiction is the more complex in nature in the concept of the digital Forensics[28]. The cybercrimes in a place might be committed by an offender might belongs to another country which brings in the complexity of the jurisdictional authority. The complexity in gathering the evidence is more and the authenticity of the evidence will be less. might belongs to another country which brings in the complexity of the jurisdictional authority. The complexity in gathering the evidence is more and the authenticity of the evidence will be less[29].

4. **Technical issues:** The evolution of the technology is the main issue in the admissibility of the digital evidence. New kind of the electronic devices are introducing in the market which gives the advantages along with the disadvantages to the people. The growth in the technology, the criminals are finding their new ways in the committing the crime which are making challenging to the cybersecurity in investigating of such crimes as no clues or traces are difficult to find in such cases.

5. **Expert witness and the authenticity:** For admissibility of the digital Forensics, the forensic experts have to provide their testimony regarding the techniques used by them in collecting and analysis of the data. The expert testimony must show the credibility in their evidence and should not be challenged on its reliability by the court. The credibility of the expert is only the big question in prosecution and their techniques as well because of the development in the technology day by day.

6. **Data Manipulation:** The evidence tampering is huge issue to be addressed in the prosecution especially in the cybercrimes. Earlier it is not very easy to tamper the evidence but it is been very easy to do so.

   Polygraphy test: In the early days, the polygraph test is considered to be very authenticate test to get the confession by the offender and produce it as evidence which

[27] "Digital Evidence Challenges in Federal Cybercrime Trials" https://federal-criminal.com/computer-crimes/digital-evidence-challenges-in-federal-cybercrime-trials/ accessed on 5th October, 2025.
[28] "Digital Forensics in Cybercrime Investigation" https://ijcat.com/archieve/volume13/issue10/ijcatr13101010.pdf accessed on 5th October, 2025.
[29] "Digital Forensics in Cybercrime Investigation" https://ijcat.com/archieve/volume13/issue10/ijcatr13101010.pdf accessed on 5th October, 2025.

is also admissible by the court as well. But now, there are many techniques to cheat the polygraph test like control of all kinds of the emotions during the test.

Not only the polygraph, there are many other tests and the digital evidence which are tampered easily by the use of the technology present now[30]. As the advancement in the technology the authenticity in the digital evidence in the legal system is depleting day by day. The forensic investigators have duty to safeguard the evidence which is gathered and stored to preserve them from alterations and follow the strict protocols[31].

CASE LAWS:

Shafi Mohammad v. State of Himachal Pradesh (2018)[32]

In this case, the apex court of India addressed the impact technology in videography and the electronic evidence make the crime investigations and the prosecutions more transparent. The court referred the action plan made by the Ministry of Home Affairs which is giving its suggestion over the videography during the criminal investigation especially in the crime scenes to give a credibility to the report made by the police after the investigation before the court[33]. It is also said that it is time to adopt the videography as effective investigative practice to build the trust among the public on the law enforcement and the administrative procedure like investigations. This decision extended the scope of the section 65B of the Indian Evidence Act, 1872 and states that the video evidence itself is a tamper-proof and credible which does not any sort of the certification[34].

Arjun Panditkar Khotkar Vs Kailash Kishanrao (2020)[35]

The video recordings in the legislative Assembly of the Maharashtra proves that the Arjun Panditkar filed the late nomination which is been alleged on him. The Election commission of India provided the video evidence before the court but failed to provide the proper certification

[30] "Digital Evidence Challenges in Federal Cybercrime Trials" https://federal-criminal.com/computer-crimes/digital-evidence-challenges-in-federal-cybercrime-trials/ accessed on 5th October, 2025.
[31] Supra 32.
[32] (2018) 2 SCC 801.
[33] "All about digital Evidence" (23 February, 2024) https://blog.ipleaders.in/all-about-digital-evidence/#What_is_digital_evidence accessed on 5th October, 2025.
[34] Kavya Shree and Apoorva Shree, "DIGITAL FORENSICS IN LAW ENFORCEMENT: IMPORTANCE AND CHALLENGES" https://www.ijlra.com/details/digital-forensics-in-law-enforcement-importance-and-challenges-by-kavyashree-r-apoorva-sri-a-r accessed 04th October, 2025.
[35] [2020] 7 S.C.R. 180

of the video authenticity which is required under section 65B of the Indian Evidence Act, 1872. The issue raised with respect to the admissibility of the digital evidence produced before the court. Therefore, the supreme court of India ruled that the certification of the authenticity of the digital evidence is mandatory and also held that the video recordings or the photographs which are produced from the original device are exempted from the certificate of authenticity by the experts[36].

CONCLUSION:

The term digital forensics is very essential element in the cybercrime investigations. These Forensics helps in the decoding, retrieving the data, collecting the data, unveiling the network logs which are the essentials in the cybercrime investigations and also have a part in combating the cybercrimes which are increasing rapidly. The digital Forensics is the most complicated process but mostly ensures the reliability and credibility in the courts as the digital evidence to draw the decisions on any case. It is irrespective whether the issue is civil or criminal in nature. The legal frameworks like Information Technology Act, 2000 and the Bhartiya Shakya Adhiniyam, 2023 working in combating the cybercrimes. The landmark supreme court decision in the Arjun Panditrao Khotkar Vs Kailash Kishanrao (2020) brought the strength to the standards of the digital evidence for admissibility in the prosecutions. The importance of the authentication by the forensic also been pronounce. The intersection of the legal and the technical professional like forensic experts is necessary in unveiling the cybercrime which are complex in nature and give validity to the evidence in the court. The drastic evolution of the technology, the digital forensic wing is facing or suffering with many challenges like encryptions, jurisdictional obstacles, data manipulation etc., Subsequently, the digital Forensics is only aid in the solving the crime investigation without any deviations which results in the validity of the digital evidence. The government also have responsibility in this aspect and has to provide certain policies which helps in combating the cybercrimes as well as in educating the public regarding the cybercrimes.

[36] "All about digital Evidence" (23 February, 2024) https://blog.ipleaders.in/all-about-digital-evidence/#What_is_digital_evidence accessed on 5th October, 2025.