Educational Administration: Theory and Practice
2024, 30(5), 6445-6452
ISSN: 2148-2403
https://kuey.net/

Research Article

An Examination Of Digital Evidence And Its Relevance For Indian Forensic

Hemlata B. Patil[1*], Dr. Anjula Chowbe[2]

[1*]Research Scholar, University: Sandip University School of Law.
[2]Guide, University: Sandip University School of Law.

***Corresponding Author:** Hemlata B. Patil
*Research Scholar, University: Sandip University School of Law.

Citation: Hemlata B. Patil et al. (2024), Dr. Anjula Chowbe. An Examination Of Digital Evidence And Its Relevance For Indian Forensic, *Educational Administration: Theory and Practice*, 30(5), 6445-6452. Doi: 10.53555/kuey.v30i5.3013

ARTICLE INFO

ABSTRACT

The digital technology revolution has been unprecedented and far more rapid than any other revolution, including the industrial, agricultural and nuclear revolutions. Due largely to advancements in digital technology, the world has shrunk to the size of a global village in the last decade. Businesses, individuals, and communities have only just begun to nurture the legitimate and beneficial potential of the quickly evolving and immensely powerful digital technology that is driving economic growth. Digital computer systems and networks are becoming increasingly important to the cultural practises of people all over the world. Many countries' governments now use digital methods of administration to keep up with the times. In an effort to hasten the country's progress, the Indian government has recently launched the 'Digital India' campaign to encourage the usage of digitalization in our day-to-day lives as well. With its meteoric rise, digitalization has become the backbone of administration, trade, private life, and corporate communications. Researcher in this article briefs about the challenges faced during the investigation process and getting the evidence admissible in the court, Comparative analysis of India and USA, types of evidence, etc. However, criminal investigation and trial had only made slight progress in that domain by enacting the Information Technology Act and amending several laws and codes such as Code of Criminal Procedure and the Indian Evidence Act. needs.

Keywords: Digital Technology, Information Technology Act, crime investigation.

Introduction

Rapid technology has made digital evidence has as an integral part of modern criminal investigations. The acceptance and use of digital evidence in the legal system in India has evolved significantly. This critical review aims to explore the strengths, weaknesses and implications of digital evidence and its forensic value in the Indian context, with reference to relevant literature and case studies. The value that electronic means have added to human existence is immeasurable. If the electronic records meet the requirements of the Indian Evidence Act, the Indian judicial system will accept them as evidence. The availability of digital technology eventually leads to misuse by anti-social or unscrupulous persons, much like other cultural revolutions that have crept in to impact our lives. In contrast to legitimate enterprises, governments, and citizens, criminal organisations have been quick to use the amazing potential of this cutting-edge technology. As a result, the number of crimes involving technology has skyrocketed. Criminals today use the internet and other digital tools to facilitate the commission of both familiar and novel crimes.

Historical Background on Indian Evidence Law

The Indian Evidence Act, 1872, stands as one of the cornerstones of the Indian legal system, which determines the admissibility and relevance of evidence in court proceedings in order to appreciate the importance of this act, it is necessary to trace its history in detail to trace its origins, development and impact on the Indian justice system. The objective of this comprehensive review is to provide a historical context of the Indian law of evidence, trace its development and enduring relevance in contemporary legal practice.

Colonial Origins and Parliamentary Careers

Indian law of evidence dates back to British colonial times, where the law of evidence in India was a mixture of indigenous customs, Islamic law and principles borrowed from English common law but British influence a it extended its establishment of the legal system in India to... the need for an integrated and transparent set of rules

The codification of the law of evidence in India was stimulated by the recommendation of the First Indian Law Commission, under the chairmanship of Lord Macaulay. The Commission recognized the need to standardize the rules of evidence The Commission recognized the necessity of standardizing rules of evidence to ensure fairness, efficiency, and consistency in the administration of justice[1]. Consequently, the Indian Evidence Act was drafted and subsequently enacted in 1872, marking a significant milestone in the development of India's legal framework [2].

Basic Principles and Policies

The Indian Evidence Act 1872 contains a set of principles and rules governing the presentation and examination of evidence in court proceedings. Its core program covers a wide range of issues including evidence interpretation, witness competence, weight of evidence and witness evaluation

Presumption of innocence, the fundamental principle of the Indian Evidence Act, places the burden of proof beyond reasonable doubt on the prosecution to prove guilt Besides, the Act provides rules for admitting it and limited consideration of oral and documentary evidence to ensure a fair and impartial testing procedure

Development and Change

A significant amendment to the Indian Evidence Act and in 2002 added electronic evidence as a separate category. This study demonstrated the growing importance of digital technology in today's legal context and sought to address the challenges associated with the admissibility and authenticity of electronic evidence in court[3]

Influence and legacy

The Indian Evidence Act has had a profound impact on the Indian legal system, governing the conduct of trials, presentation of evidence and determination of outcome. Insistence on impartiality, transparency and fairness has helped to build the credibility and integrity of the Indian judiciary.

Digital Evidence is Important in Indian Criminal Trials

This important study examines the importance of digital evidence in Indian criminal trials, and in enhancing investigations, establishing guilt or innocence and the impending process of criminal activities Through an examination of relevant law, case law and scholarly literature focusing on the process, the aim of this discussion is to clarify the importance of digital evidence in Indian law.

Activities in the digital realm leave digital traces such as file fragments, activity logs, timestamps, metadata, and so on – may be deemed to be of value, for any number of reasons.

They may be useful as evidence in establishing the origins of a document or piece of software, for legal purposes in determining the activities of the parties involved in a criminal case, or even as a resource for cyber-criminals looking to reconstruct information or identifying credentials on their victims. The prolific usage of electronic devices such as smartphones and computers, humongous amount of data generated from these. As such, there can be an expectation within almost any investigation for the need to identify digital evidence.

If identified, collected and analysed in a forensically sound manner, electronic evidence can prove crucial to the outcome of criminal, civil and cooperate investigations.[4]

---

[1] https://www.legalserviceindia.com/legal/article-7229-historical-background-of-evidence-law-in-india-with-special-reference-to-the-indian-evidence-act-1872.html

[2] Sarkar, S. (2013). Law of Evidence: The Indian Evidence Act, 1872. LexisNexis.

[3] Gandhi, B. (2007). Law of Evidence in India: A Critical Commentary on Indian Evidence Act, 1872. Universal Law Publishing.

[4] https://nja.gov.in/Concluded_Programmes/2021-22/P-1271_PPTs/1.Digital%20Forensics%20Collection,%20Presservation%20and%20Appreciation%20of%20Electronic%20Evidence.pdf

The role of digital evidence in criminal investigations

Performing digital forensics can be an expensive proposition involving licenses, equipment and significant personnel costs. Demonstrating cost effective return on investment is crucial to securing command staff buy in. Funding these efforts can involve a complicated mix of local, state and federal budgets, and this can be particularly challenging for smaller departments. Regional models and other forms of collaboration can help, provided officers know where to turn for help.

Advanced digital evidence training is not yet part of the core curriculum for police academies, yet officers of all levels of experience may have contact with digital evidence that is sufficient to affect the resolution of the case. For example: training can improve the preservation of evidence[5].

Digital evidence includes many types of electronic data, including emails, text messages, social media posts, Internet browsing histories, and electronic documents. In Indian criminal trials, digital evidence is an important tool for law enforcement agencies, providing valuable information about criminal activities, such as cybercrime, financial fraud, terrorism and intellectual property a they steal[6]

Digital evidence often provides an up-to-date record of events, making it easier to reconstruct timelines and identify suspects. Additionally, digital evidence can corroborate or refute witness testimony, strengthening its relevance to circumstances and establish patterns of behaviour crucial for building a compelling case [7].

Digital evidences and its types

Electronic communications, such as emails and instant messaging, can provide direct evidence of criminal intent or complicity. Social media posts and online interactions can reveal connections between suspects or support alibis. Additionally, digital forensic techniques allow investigators to access deleted or archived data, providing valuable insights into the activities of suspects[8]

In a court of law, evidence is of supreme importance; it is crucial to establish facts. Data or relevant information from electronic devices is pulled from two types of sources.

- **Volatile or non-persistent**: Hard disks and removable devices are a few examples of volatile data devices, which means that data is not accessible when they are unplugged from the computer. Further, data can be deliberately erased or wiped from these devices, to destroy evidence. Of course, Volatile also refers to memory that relies on power to store its contents, such as RAM chips. When the power is switched off, the memory contents are lost.
- **Non-volatile, which is persistent:** Persistent data is stored permanently in memory, and a loss in power doesn't erase its content. For example, data stored in flash memory, ROM (Read-only memory), CD/ DVD, or tape.

Forensics investigation is incomplete without digital evidence. Digital data or information stored in electronic devices are associated with e-crime – another word for cybercrime. In the digitalization era, every Internet-enabled electronic device like a smartwatch, smart TV, video game console etc., can be a key component in gathering information to crack a case.

Additionally, the five rules of gathering digital evidence that every forensic expert should keep in mind are that digital evidence should be: admissible, authentic, complete, reliable, and believable. Hence, skilled individuals trained in this field need to handle and preserve the digital evidence[9].

Legal Framework for Digital Evidence

Existing law and judicial precedents govern the admissibility and handling of digital evidence in Indian criminal trials. The Indian Evidence Act, 1872, provides a framework for the admissibility and evaluation of evidence, including digital evidence. Under the Act, digital evidence must meet certain criteria to be considered admissible, including relevance, authenticity and reliability.[10]

In addition, the Information Technology (IT) Act, 2000, and subsequent amendments establish specific provisions for cybercrime and admissibility of electronic evidence This act empowers law enforcement agencies to collect digital evidence, preserved and prosecuted to ensure that perpetrators of digital crimes are held accountable under the law[11]

---

[5]https://www.iacpcybercenter.org/investigators/digital-evidence/understanding-digital-evidence/
[6]Indian Evidence Act, 1872
[7]Agarwal, S. P. (2016). The Indian Evidence Act, 1872: With Exhaustive Case Law. Eastern Book Company.
[8]State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
[9]https://cisomag.com/what-is-digital-evidence-and-why-its-important-in-2021/
[10]Information Technology (IT) Act, 2000.
[11]Sharma, N. (2019). Law of Evidence: Principles and Practices. Universal Law Publishing.

Types of Cybercrime

There are several different forms of cybercrime; the majority of cybercrime is carried out with the aim of gaining financial benefit for the perpetrators, though the methods by which cybercriminals want to be compensated vary. The following are examples of various forms of cybercrime;
Cyber Extortion is a crime that involves a cyberattack or threat of a cyberattack, as well as a demand for money to stop the attack. The ransomware attack is one form of cyber extortion. The intruder gains access to a company's databases and encrypts all of the company's records and information — something of value — rendering the data unavailable until a ransom is charged. This is generally in the form of a cryptocurrency, such as bitcoin (Tanimoto, Kakuta, Sato and Kanai, 2015).

Crypto-jacking is a form of attack in which scripts are used to mine cryptocurrencies in browsers without the user's permission. Crypto-jacking attacks can include the victim's computer being infected with cryptocurrency mining software. However, if the user's browser has a tab or window open on the malicious site, many attacks rely on JavaScript code that performs in-browser mining. There is no need to install malware because the in-browser mining code is executed when the affected page is loaded[12].

Demanding situations and concerns

An essential task is the rapidly evolving generation, which calls for law enforcement and prison professionals to be aware about emerging trends and trends in digital forensic techniques further to reality and integrity digital evidence may be called into question, specifically in cases concerning tampering, hacking, or facts breaches.
Moreover, judges commonly scrutinize the admissibility of digital evidence in courtroom, and judges check the credibility and relevance of such proof on a case-by using-case foundation
From electronic communications, social media activities to forensic information, virtual proof presents valuable insights. However, continued efforts to decorate judicial capacity, support criminal frameworks and foster collaboration among stakeholders are needed to meet the challenges related to virtual evidence Through the adoption of virtual technology and adopting excellent practices in digital forensics, India can make sure powerful use of digital proof.

Advantages

In the Indian criminal system, digital evidence offers many blessings. First, it provides a fact that may not be in conventional forms of evidence, including electronic files, emails, social media pastime, metadata and this expanded proof enhances the investigative manner, and strengthens cases that go to trial. Second, virtual proof is regularly hard to adjust or adjust if proper forensic procedures are accompanied, contributing to reliability and authenticity Third, virtual forensic gadgets and technology have turn out to be increasingly state-of-the-art, allowing investigators to get better and examine data from numerous virtual gadgets effectively.

Challenges:

Despite its advantages, digital evidence in India also has significant challenges. A key issue is the lack of a standardized protocol framework for handling and examining digital evidence in law enforcement agencies and forensic laboratories This consistency can make a difference in the admissibility and reliability of digital evidence in court.[13] Furthermore, the rapid pace of technological advancement poses challenges for forensic professionals, who must constantly update their skills and equipment to keep pace with new developments. Lack of clear guidelines and standards for authenticating digital evidence, particularly in the context of electronic communications, social media posts and digital documents.[14]
Another challenge is addressing privacy and data security issues in the collection and use of digital evidence. As digital technologies become increasingly prevalent in everyday life, concerns about unauthorized access, modification, or misuse of personal data pose significant legal and ethical dilemmas [15]. Balancing the need for effective law enforcement with the protection of individual rights and privacy rights remains a critical area of concern.[16]

---

[12] https://www.researchgate.net/publication/360919194_Role_of_Digital_Forensic_in_solving_cyber_crimes

[13] Singh, S., & Mishra, D. (2019). An Overview of Digital Forensic Investigations in India. International Journal of Computer Sciences and Engineering, 7(1), 199-203.

[14] Chand, A. K., & Prakash, S. (2021). Admissibility of Electronic Evidence in India: Issues and Challenges. International Journal of Advanced Legal Research, 3(2), 44-51.

[15] Swarup, S., & Oberoi, R. (2021). Challenges and Opportunities in Digital Forensics: An Indian Perspective. International Journal of Advanced Research in Computer Science, 12(1), 43-48

[16]. Mittal, S., & Jha, S. (2020). Privacy Concerns and Digital Evidence: A Critical Analysis. Journal of Indian Law and Society, 11(2), 34-46.

Implications for the prison device, the increased reliance on virtual evidence has a sizeable impact at the Indian prison machine. On the one hand, using virtual proof has facilitated the research and prosecution of cybercrime, monetary fraud and other digital crimes. It has additionally contributed to greater transparency and performance within the judicial process, enabling quicker resolution of cases.

Comparative Analysis of Digital Evidence in USA

Judges' interpretations of the legality and importance of electronic evidence Digital proof is accepted in trial courts in the United States. Digital evidence includes things like digital images, social media posts, computer-generated data, computer-stored documents, webpage content, etc. Electronic interactions, such as emails, are also included[17]. In the Lorraine v. Markel American Insurance Company case, Judge Grimm announced a verdict on the admissibility of electronic evidence[18]. This concept relates to whether or not electronic evidence is accepted. A detailed examination of the following components is necessary: the protagonist must handle any hearsay difficulties with the electronic evidence; the relevancy of the evidence is evaluated; correctness; originality; authenticity; and whether duplicate supporting secondary evidence is required.

These include determining whether the statement is one made by the declarant and, if it is hearsay, deterring it from being used as evidence[19].

The Federal Rules of Evidence, namely Rules 401 and 402, address logical relevance. Demonstrating that evidence tends to support or contradict any truth that is pertinent to the choice of action is not as difficult as one might think[20]. Federal regulations specify that electronic evidence must pass the same logical relevance standard as traditional evidence.
Federal Rule of Evidence Rule 403 tackles prejudiced bias by emphasising the "pragmatic relevance" requirement. "Unfair prejudice" describes a too strong inclination to judge often, though not always based on feelings[21].
As per rule 403, electronic evidence is not admitted

1. If the contents or language of the evidence is offensive.
2. If the evidence has animation and exists, the possibility that the accurate act cannot be ascertained by the jury.
3. Summarises extensive electronic writings, recordings, or images under Rule 1006.
4. It may not be accurate or dependable[22].

[17] Michael D. Gifford, Admitting Electronic Evidence in Federal Court: I've Got All This Evidence Data – Now What Do I Do With It? AM. B. ASS'N, 2 (2008), http://www.abanet.org/labor/basics/elist/papers/lied.pdf. https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf

[18] Lorraine, 241 F.R.D. 534, https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf

[19] STEPHEN MASON AND ALLISON STANFIELD, AUTHENTICATING ELECTRONIC EVIDENCE, ELECTRONIC EVIDENCE, 193 – 261.(2017) University of London Press; Institute of Advanced Legal Studies, URL: https://www.jstor.org/stable/j.ctv512x65.14 https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf

[20] Shiv N.S. Scope of Electronic Evidence in India: A Comparative Study (UK, USA & Canada) 24 Supremo Amicus [227] (2021) https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf

[21] FED. R. EVID. 403 https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf

[22] GOODISON, SEAN E., ROBERT C. DAVIS, AND BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE. 1 – 32, Santa Monica, CA: RAND Corporation,2015. https://www.rand.org/pubs/research_reports/RR890.html or https://www.jstor.org/stable/10.7249/j.ctt15sk8v3.1 https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf

USA

a. Legal concerns Legislators need to alter their legislation in light of technological advancements in order to address issues with digital evidence. To determine the legal requirements for the chain of custody and admissibility, law enforcement must focus on the courts and prosecutors while creating the regulations.
b. Issue with Search and Seizure irrational Under some circumstances, the Fourth Amendment forbids government agents from conducting searches or seizures. Before beginning the search, the authorities must obtain a search warrant. The warrantless search is authorised if the relevant party gives their approval. When making an arrest and to keep the evidence from being destroyed, limited searches can also be carried out. Horton v California[23], electronic evidence storage is not permitted by this rule. There are two stages to gathering evidence with a search warrant.

- The initial step is to seize the split that contains the information. According to the courts, the first seizure may need to be quite wide and contain a lot of data that isn't covered by the search warrant.
- Consequently, the need for the specific information included in the evidence makes the second stage—examination—extremely vital. An analysis is conducted on the files found on the confiscated device. Further information that falls outside the current scope can be found during such an activity[24].

The United States Congress has created several legislation to strike a balance between the importance of the Fourth Amendment and the need for criminal inquiry. There are four codes that are significant to digital evidence.

A judge with adequate cause can issue an order that authenticates the inspection by enforcing the law. If the government tries to listen in on communications without a judicial warrant. This may have legal or criminal ramifications, as well as the concealment of evidence. The Pen Registers and the Trap and Trace Device Statute restrict the acquisition of metadata from telephone and Internet communications[25].

Research gaps and future instructions

The current research is on the admissibility of digital evidence in Indian courts addresses the need for complete suggestions and satisfactory practices to make sure reliability, accuracy and relevance. Future studies ought to focus on developing standardized structures for collecting, maintaining, and imparting digital proof, taking into account the unique traits of virtual information units.
Additionally, there may be a need for interdisciplinary studies that bridges the gap between law, engineering, and forensic technological know-how. Collaborative efforts regarding criminal professionals, digital forensics professionals, and generation experts can assist meet the complex demanding situations posed by way of virtual proof and realise effective felony frameworks and procedural safeguards so that it will be achieved.
In addition, studies must take a look at the effect of rising technology along with blockchain, artificial intelligence and the Internet of Things (IoT) on the popularity and authenticity of virtual proof To apprehend how those technologies have an effect on the reliability and integrity of virtual information maintained, is important to make sure the accuracy and equity of checking out in the virtual age.

Case Laws

Digital proof has end up an increasing number of prominent in Indian regulation, shaping criminal trials and influencing judicial choice-making This complete assessment examines the key troubles in India which have dealt with virtual evidence thru decisions on it and its implications for on the analysis of this discussion The purpose is to offer a survey of the evolving role of virtual evidence in Indian law.

---

[23] Horton v California, 496 U.S. 128 (1990).
https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
[24] 7 Thomson, Lucy L., Scitech Lawyer; Chicago, Mobile Devices: New Challenges For Admissibility Of Electronic Evidence, 9(3), The SciTech Lawyer, 32 - 37 (2013).
https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
[25] 8 GOODISON, SEAN E., ROBERT C. DAVIS, AND BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE. 1 – 32, Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR890.html
https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf

Major Digital Evidence Case Laws in India are cited:

1. Anwar P.V. V. P.K. Bashir and Others: (2014) 10 SCC 473

In this landmark case, the Supreme Court of India dominated on the admissibility and probative price of electronic statistics underneath the Indian Evidence Act, 1872. The court docket held that electronic statistics, emails and digital documents exist, as sections 65b(1) and 65b(2) of the Evidence Act. This provision makes it mandatory for a person in a responsible governmental function to certify electronic evidence in terms of the operation of the applicable tool or the manage of the applicable operation.

The choice clarifies the methods for developing safeguards for the admissibility of digital proof, and emphasizes the importance of authenticity and reliability in virtual data. It installed tips for the verification of digital proof, together with the requirement to produce a certificates beneath section 65B(four) of the Evidence Act to preserve the integrity of digital statistics

2. State of Maharashtra v. Dr. Prafull B Desai : (2003) four SCC 601

In this case, the Supreme Court addressed the admissibility of electronic evidence acquired via forensic evaluation of laptop systems. The court docket recognized the significance of virtual forensics within the investigation of cybercrime and agreed that forensic reports are admissible as secondary evidence under Section 63 and 65 of the Indian Evidence Act.

The decision highlighted the need for forensic experts to follow hooked up techniques and maintain a chain of custody while accumulating and reading virtual evidence. Establishing electronic information emphasised the reliability and trustworthiness of courtroom reports and figuring out perpetrators of cybercrimes.

3. State (NCT of Delhi) v. Navjot Sandhu: (2005) eleven SCC six hundred

In this high-profile case, generally known as the "Parliamentary attack case", the Supreme Court taken into consideration the admissibility of cellphone conversations as proof The court docket confirmed that it is felony to intercept telecommunications in India Telegraph Act, 1885 And underneath the extra provisions meet the want Now it can be admitted in proof, he delivered

The choice highlighted the importance of procedural safeguards and judicial oversight in issuing lets in and sporting out crossings, as well as good enough methods to make sure compliance with constitutional ideas of confidentiality plant. It mounted pointers for the admissibility of intercepted communications in criminal complaints, balancing legislative interests with the rights of individuals to privacy and a truthful trial

This information act is normal of the evolving regulation on virtual evidence in India, addressing complex problems of admissibility, authenticity and reliability Highlights the significance of adapting criminal standards to the virtual age of fact meet, while respecting the principles of equity, transparency and duty in crook prosecution equality

Conclusion

In conclusion, the Indian Evidence Act, 1872, represents a pivotal second inside the development of the Indian felony gadget, formulating guidelines and concepts governing the manufacturing and exam of evidence in court docket court cases Its historical history applicable sheds light at the colonial affects and legislative procedures that formed the Act and subsequent traits.

In end, digital proof holds first rate judicial relevance within the Indian criminal device, offering specific possibilities and challenges. Although virtual proof has revolutionized crook investigations and superior the use of virtual criminal prosecution, it must be dealt with with care and thoroughly analyzed to make sure credibility and admissibility in court Items more suitable to address the challenges associated with virtual proof cation, formalized programs, and encouragement of continuing training and training India can use all to be had digital evidence to maintain justice and conduct cyber so crime is dealt with efficiently.

References:

1. https://www.legalserviceindia.com/legal/article-7229-historical-background-of-evidence-law-in-india-with-special-reference-to-the-indian-evidence-act-1872.html
2. Sarkar, S. (2013). Law of Evidence: The Indian Evidence Act, 1872. LexisNexis.
3. Gandhi, B. (2007). Law of Evidence in India: A Critical Commentary on Indian Evidence Act, 1872. Universal Law Publishing
4. https://nja.gov.in/Concluded_Programmes/2021-22/P-1271_PPTs/1.Digital%20Forensics%20Collection,%20Presservation%20and%20Appreciation%20of%20Electronic%20Evidence.pdf
5. https://www.iacpcybercenter.org/investigators/digital-evidence/understanding-digital-evidence/
6. Indian Evidence Act, 1872
7. Agarwal, S. P. (2016). The Indian Evidence Act, 1872: With Exhaustive Case Law. Eastern Book Company.
8. State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
9. https://cisomag.com/what-is-digital-evidence-and-why-its-important-in-2021/

10. Information Technology (IT) Act, 2000.
11. Sharma, N. (2019). Law of Evidence: Principles and Practices. Universal Law Publishing.
12. https://www.researchgate.net/publication/360919194Role_of_Digital_Forensic_in_solving_cyber_crimes
13. Singh, S., & Mishra, D. (2019). An Overview of Digital Forensic Investigations in India. International Journal of Computer Sciences and Engineering, 7(1), 199-203.
14. Chand, A. K., & Prakash, S. (2021). Admissibility of Electronic Evidence in India: Issues and Challenges. International Journal of Advanced Legal Research, 3(2), 44-51.
15. Swarup, S., & Oberoi, R. (2021). Challenges and Opportunities in Digital Forensics: An Indian Perspective. International Journal of Advanced Research in Computer Science, 12(1), 43-48
16. Mittal, S., & Jha, S. (2020). Privacy Concerns and Digital Evidence: A Critical Analysis. Journal of Indian Law and Society, 11(2), 34-46.
17. Michael D. Gifford, Admitting Electronic Evidence in Federal Court: I've Got All This Evidence Data – Now What Do I Do With It? AM. B. ASS'N, 2 (2008), http://www.abanet.org/labor/basics/elist/papers/lied.pdf.https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
18. Lorraine, 241 F.R.D. 534, https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
19. STEPHEN MASON AND ALLISON STANFIELD, AUTHENTICATING ELECTRONIC EVIDENCE, ELECTRONIC EVIDENCE, 193 – 261.(2017) University of London Press; Institute of Advanced Legal Studies, URL: https://www.jstor.org/stable/j.ctv512x65.14
https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
20. Shiv N.S. Scope of Electronic Evidence in India: A Comparative Study (UK, USA & Canada) 24 Supremo Amicus [227] (2021),https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
21. FED. R. EVID. 403,https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
22. GOODISON, SEAN E., ROBERT C. DAVIS, AND BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE. 1 – 32, Santa Monica, CA: RAND Corporation,2015. https://www.rand.org/pubs/research_reports/RR890.html or https://www.jstor.org/stable/10.7249/j.ctt15sk8v3.1,https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
23. Horton v California, 496 U.S. 128 (1990).https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
24. 7 Thomson, Lucy L., Scitech Lawyer; Chicago, Mobile Devices: New Challenges For Admissibility Of Electronic Evidence, 9(3), The SciTech Lawyer, 32 - 37 (2013).https://www.ijlmh.com/wp-content/uploads/ Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf
25. 8 GOODISON, SEAN E., ROBERT C. DAVIS, AND BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE. 1 – 32, Santa Monica, CA: RAND Corporation, 2015.
https://www.rand.org/pubs/research_reports/RR890.html,https://www.ijlmh.com/wp-content/uploads/Comparative-Analysis-of-Digital-Evidence-in-India-and-USA.pdf