

ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN: 2583-6323 (Online)

Copyright © 2024 - 25

THE EVOLUTION OF E- EVIDENCE IN INDIAN CRIMINAL LAW AND ITS IMPACT ON DIGITAL FORENSICS BY AI AND MACHINE LEARNING

AUTHOR'S NAME – Kausik Maitra.

AFFILIATION OF AUTHOR - Assistant Professor, Department of Cyber Science & Technology Brainware University, Ex – Assistant Programmer, Technical Forensic Unit CBI, Govt. of india.

Received 14 November 2024; Accepted 16 November; Published 20 October 2024.

ABSTRACT:

This paper examines the evolution of electronic evidence (e-evidence) in Indian criminal law and its profound impact on digital forensics [2]. As technology continues to advance rapidly, the Indian legal system has had to adapt to address the challenges and opportunities presented by digital evidence. Electronic Evidence i.e. Digital Evidence is "any probative information stored or transmitted in digital form that to a court case may use at trial as admissible, authentic, complete, reliable and believable. This study traces the historical development of e-evidence legislation, analyzes current legal frameworks, and explores the implications for digital forensic practices in India. Nowadays societal communication happens through the transfer of thoughts from the physical world to the electronic world.[1] The virtual world revolves around information and communication technological devices such as computers, mobile phones, printers, digital cameras, etc. Unlike, the real world, the virtual world, causes many opportunities for the commission of offenses, such as phishing, identity theft, child pornography, hacking, etc[2]. In the Indian parliament, The Bharatiya Sakshya Adhiniyam (BSA), 2023 passed to supersede the Indian Evidence Act, 1872 and aims to make the judicial system more efficient, fair, and technology-enabled. This bill gives us more to reassess and significantly enhance the current investigative procedures involving digital forensic evidence in India, particularly by integrating international standards[3]. AI systems involve multiple contributors with different persons doing different tasks such as collating and analyzing data, training AI models, developing model techniques and algorithms, testing and evaluating AI

[1] Neha Haldhar, Electronic Evidence And Its Admissibility In Indian Courts, B&B Associates LLP (Nov. 9, 2024, 8:00 P.M.), https://bnblegal.com/article/electronic-evidence-and-its-admissibility-in-indian-courts/.

[2] Pathshala, https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/Law/07._Information_and_communication_technology_/10._Digital_evidence-broad_principle/et/7566_et_10_ET.pdf (last visited Nov. 9 2024)

[3] Brijesh Singh, Digital Evidence: Effective implementation of the new criminal laws in India., Linked in (Nov. 9, 2024, 8:05 P.M.), https://www.linkedin.com/pulse/digital-evidence-effective-implementation-new-criminal-brijesh-singh-sf4ce.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

models, etc. AI / ML enable applications help to identify patterns and signatures that can be used to detect and prevent future attacks potential threats and illegal activity. Policymakers may need to arrive at a more adaptive legal framework to address the unique authentication challenges posed by AI-generated evidence.[4]

Keywords: Evidence Act, IT Act 2000, Electronic Evidence, Digital Evidence, Bharatiya Sakshya Adhiniyam

1. Introduction

The digital age has transformed the landscape of criminal investigations and prosecutions. In India, as in many countries, the legal system has had to evolve to accommodate the increasing prevalence of electronic evidence. The introduction of three new criminal laws in India—the Bhartiya Nyaya Sanhita (BNS), Bhartiya Nagarik Suraksha Sanhita (BNSS), and Bhartiya Sakshya Adhiniyam (BSA)—marks a significant transformation in the legal landscape, particularly concerning digital forensics. These laws, effective from July 1, 2024, aim to modernize the criminal justice system by integrating technology at all stages of legal proceedings. This paper aims to provide a comprehensive overview of how Indian criminal law has adapted to the challenges posed by e-evidence and the consequent effects on digital forensics. Digital artifacts provide to collection of digital data that are large, complex, and heterogeneous datasets. In this context AI and machine learning algorithms can process large volumes of data much faster and more efficiently than humans, enabling investigators to quickly identify potential evidence and leads. AI models [4] to generate reliable and verifiable digital evidence [5] by historical dataset, the assumption that cognitive methodologies used in big data analysis[5] will succeed when applied to Digital Forensic [6] analysis has fuelled a decade-long surge of research into the application of AI in Digital Forensic. Evidence is of two types: oral and documentary. The definition of documentary evidence has been amended to include all documents that are generated by computers, such as emails, database records, and logs. Digital Signatures are also under documentary evidence and can be used to sign and

[4] Rutuja Pol, Can India's New Evidence Act Address The Challenges Posed By Artificial Intelligence?, the secretariat (Nov. 9, 2024, 8:10 P.M.), https://thesecretariat.in/article/can-india-s-new-evidence-act-address-the-challenges-posed-by-artificial-intelligence.

[5] Springer Link, https://link.springer.com/content/pdf/10.1007/s13218-022-00763-9.pdf (last visited Nov. 9, 2024).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

authenticate electronic documents and records. The term 'electronic records' has been given the same meaning as assigned to it in the IT Act, which provides, 'data, record or data generated, image or sound stored, received or sent in the form of electronically.

Digital Revolution in a Nutshell			
1980s	**1990s**	**2000s**	**2010 and onwards**
Personal Computer	Internet / World Wide Web	Mobile Phones	App Development
Transaction Processing	E-Commerce	Technology Enabled Services	Cloud Computing
Data Processing	Telecommunication & Broadcasting	Internet Banking	Drone Technology
			Smart Communication Devices and Mobile Platforms

Table: 1 Digital Revolution

 Overview of Digital Forensics' new legal framework in India: The BSA expands the definition and admissibility of electronic records, treating them with the same validity as traditional paper records. This includes emails, server logs, and other digital communications. In this new framework during search and seizure, the scope of audio-video recording is listed as seized items with witness signature under clause 105.[6] The official will take video photography while collecting forensic evidence under clause 176(3). Clause 176(1) provides an opportunity for an audio-video recording of any statement made during the police investigation[7]. Clause 63 of the Indian Evidence Act deals with secondary evidence, it provides certified copies of documents, Counterparts of documents as against the parties who did not execute them Oral accounts of the contents of a document given by some person who has seen it. While clause 2(d) of BSA defines documents to also include 'electronic or digital records'. These clauses are made transparent and accountable as evidence gathering, and a safeguard against irregularities and manipulation.[13,14,15]

[6] Ministry of home affairs, https://bprd.nic.in/uploads/pdf/SOP%20of%20Audio-Video%20Recording%20for%20Scene%20of%20Crime%20(1).pdf (last visited Nov.9, 2024).
[7] Rahul Tripathi, New criminal laws hinge on technology and forensic throughout all stages, economic times (Nov. 9, 2024, 8:15 P.M.), https://economictimes.indiatimes.com/news/india/new-criminal-laws-hinge-on-technology-and-forensic-throughout-all-stages/articleshow/111412388.cms.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

 The Role of Evidence Collection: The proliferation of computers and the influence of Information technology in human lives and the storage of information in digital form required amendments to Indian law to include the provisions regarding the appreciation of digital evidence. In 2000, the Indian Parliament enacted the Information Technology Act, 2000 (IT Act), which brought in corresponding amendments to existing Indian statutes to make digital Evidence admissible. The IT Act is based on the UNCITRAL Model Law [26] on Electronic Commerce and, apart from providing amendments to the Indian Evidence Act, 1872 (Evidence Act), the Indian Penal Code, 1860, and the Banker's Book Evidence Act, 1891, mainly [27] Recognizes transactions that are carried out by means of electronic data interchange and other means of electronic communications. India's legal framework has recently undergone significant changes with the following ways to aim for transparency and modernize.

Enhanced Digital Forensics

The new laws emphasize the importance of digital forensics in modern investigations. This includes:

Cybercrime Investigations: With the rise in cybercrimes, digital forensics has become crucial. The new framework ensures that digital evidence, such as data from computers, smartphones, and other electronic devices, is collected and preserved correctly.

Chain of Custody: Maintaining a clear chain of custody for digital evidence is essential to ensure its admissibility in court.[8] The new laws provide detailed guidelines on how to handle and document digital evidence. [16,17]

Audio-Visual Recording

The mandatory use of audio-visual recording during search and seizure operations aims to:

Increase Transparency: By recording these operations, the process becomes more transparent, reducing the chances of tampering or misconduct.

Enhance Accountability: Law enforcement officers are held accountable for their actions during these operations, as the recordings can be reviewed if any disputes arise.

Forensic Evidence Collection

Forensic evidence plays a critical role in solving crimes. The new framework includes:

[8] Vanshika Shukla, THE ADMISSIBILITY OF DIGITAL EVIDENCE: CHALLENGES AND FUTURE IMPLICATIONS, the law bridge (Nov. 9, 2024, 8:15 P.M.), https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-Shukla-CLRJ.pdf.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Mandatory Forensic Collection: For serious crimes, it is now mandatory to collect forensic evidence from the crime scene. This includes DNA samples, fingerprints, and other physical evidence.

Use of Technology: Advanced technologies, such as 3D crime scene reconstruction and automated fingerprint identification systems, are being integrated into the evidence collection process.

Expert Testimony

The scope of expert testimony has been broadened to include:

Diverse Fields: Experts from various fields, such as digital forensics, psychology, and medicine, can now provide testimony. This ensures that the court has access to specialized knowledge relevant to the case.

Improved Standards: The standards for qualifying as an expert witness have been updated to ensure that only individuals with the necessary expertise and credentials can testify.

Inclusive Legal Language

The new laws have also modernized the language used in legal documents to be more inclusive and understandable:

Clarity and Precision: Legal terms have been updated to be clearer and more precise, making it easier for all parties involved to understand the legal proceedings.

Inclusivity: The language has been made more inclusive, particularly concerning individuals with mental illnesses, ensuring that their rights are protected and respected

 Emergence of AI and ML in Forensics: Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being used in the field of digital forensics to assist in investigations and improve the accuracy and efficiency of forensic analysis. Here are a few examples of how AI and ML are being used in forensics:

Pattern Recognition: AI and ML algorithms can be trained to recognize patterns in large volumes of data, such as images, audio, and text, enabling faster and more accurate identification of relevant evidence.

Image Analysis: AI and ML techniques can be used to enhance and analyze images, such as faces and license plates, to assist in criminal investigations.

Natural Language Processing: AI and ML algorithms can analyze and interpret large volumes of text data, such as emails and social media posts, to identify potential evidence and leads.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Forensic Data Analysis: ML algorithms can be used to analyze forensic data, such as network traffic and malware, to identify patterns and relationships that may indicate criminal activity.

Predictive Analytics: AI and ML can be used to analyze large volumes of data to identify patterns and predict future events, such as potential cyber-attacks or fraud.

Digital Forensic Investigation Tools: Many digital forensic investigation tools are incorporating AI and ML to automate routine tasks, such as data extraction and analysis, freeing up human investigators to focus on more complex tasks.

Data Visualization: AI and ML [9,10] can be used to create visualizations of forensic data, such as timelines and networks, to help investigators identify patterns and relationships.

Dark Web Analysis: AI and ML techniques can be used to analyze data from the dark web, such as forums and marketplaces, to identify potential threats and illegal activity.

Cyber Threat Intelligence: AI and ML can be used to analyze large volumes of cyber security data, such as malware and intrusion alerts, to identify potential threats and vulnerabilities in real time.

Forensic Cryptography: AI and ML techniques can be used to crack encryption and decode hidden messages in digital evidence, assisting in criminal investigations.

Biometric Analysis: AI and ML can be used to analyze biometric data, such as fingerprints and facial features, to identify individuals involved in criminal activity.

2. Learning Outcome of Digital Forensics by AI and Machine Learning:

As e-evidence becomes increasingly prevalent and important in India's criminal justice system, the use of AI and machine learning in digital forensics is expected to have several potential outcomes, including

- Greater Efficiency: AI and machine learning [12] can automate many of the tedious and time-consuming tasks involved in digital forensics, such as data extraction and analysis, enabling investigators to work more efficiently and effectively.
- Improved Accuracy: AI and machine learning algorithms can analyze large volumes of data and identify patterns and relationships that may be difficult for human investigators to detect, leading to more accurate and reliable evidence.[9]
- Enhanced Investigation: By analyzing data from multiple sources, such as social media, surveillance footage, and mobile devices, AI and machine learning can help

[9] Pub Med Central, https://pmc.ncbi.nlm.nih.gov/articles/PMC10517477/ (last visited Nov. 9, 2024).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

investigators build a comprehensive picture of a crime scene or incident, enabling them to identify suspects and uncover hidden connections.

- Expanded Capabilities: AI and machine learning can enable investigators to analyze new types of evidence, such as biometric data and blockchain transactions, expanding the scope and effectiveness of digital forensics.
- Enhanced Security: AI and machine learning can be used to identify and prevent cyberattacks, fraud, and other types of criminal activity, improving the security of digital evidence and protecting the privacy of victims and witnesses. [11]
- Ethical Challenges: The use of AI and machine learning in digital forensics raises several ethical concerns, such as algorithmic bias, privacy violations, and the potential for abuse by law enforcement agencies[10].
- New Legal Challenges: The emergence of new types of evidence and new investigative techniques may pose new legal challenges, such as how to define and regulate the use of AI and machine learning in criminal investigations.

Data Collection Technique for AI / ML

A varied and representative dataset [1] including a range of scenarios and digital evidence types is necessary for building and training an AI model for digital forensics. To develop an effective data collection technique for digital evidence in AI systems, we should consider a comprehensive approach that ensures the integrity, authenticity, and admissibility of the collected data.

Dataset Category	Description	Use Cases	Data Types	Privacy
Digital Case Datasets for Forensics	Datasets from real-world digital forensic cases, including proof from verified investigations. Can include hard drive images, network logs, and other artifacts	Forensic analysis, evidence validation	Hard drive images, logs	Privacy and regulatory requirements must be followed

[10] National Academies Press, https://nap.nationalacademies.org/read/11896/chapter/11 (last visited Nov. 9,2024).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Dataset Category	Description	Use Cases	Data Types	Privacy
	gathered during investigations.			
Datasets for Incident Response	Malware samples, system logs, and network traffic logs from simulated or actual incidents. Information gathered from events like malware outbreaks, network attacks, and data breaches	Incident response training, identifying security breaches	Malware samples, logs	Privacy considerations in handling sensitive incident data.
Forensic Memory Analysis Collections	Collections of memory dumps from different operating systems. Used to train models examining volatile memory for indications of malicious behavior	Identifying malware in volatile memory, enhancing forensic capabilities	Memory dumps	Privacy concerns related to the content of memory dumps.
Datasets of Malware	Groups of malware samples and accompanying metadata. Used to train models that identify and categorize various forms of malware.	Malware detection, understanding malware behavior	Malware samples	Privacy concerns, especially if malware samples contain sensitive information.
Device Datasets for IoT	Digital evidence datasets derived from Internet of Things (IoT)	Investigating IoT-related incidents	IoT device data	Privacy concerns related to data

www.abhidhvajlawjournal.com
The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Dataset Category	Description	Use Cases	Data Types	Privacy
	devices, including wearables and data from smart homes.			from personal IoT devices.
Social Media Collections	Information gleaned from social networking platforms, such as messages, posts, and exchanges between users.	Analyzing online threats, cyberbullying investigations	Social media content	Privacy considerations, respecting user confidentiality, and legal standards.
Datasets for Email Communication	Email conversation datasets containing headers, body information, and attachments.	Searching for evidence in email correspondences	Email communication data	The privacy of email content and user information must be protected.
Datasets for Deepfake Detection	Datasets specifically curated for training deepfake image and video detection models, comprising potential manipulated media content found in digital investigations.	Detecting and mitigating the risks associated with deepfake technology	Deepfake images and videos	Privacy concerns, especially if the deepfake content involves individuals.
Phishing Sets	Groups of phishing websites, email campaigns, and related materials. Used to teach models how to identify and categorize phishing attempts.	Phishing attack detection, enhancing cybersecurity measures	Phishing websites and emails	Privacy considerations, especially when analyzing phishing emails.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Dataset Category	Description	Use Cases	Data Types	Privacy
Databases of Forensic Images	Datasets including pictures of storage media and digital equipment. Used in developing models that can identify and evaluate various storage device kinds.	Identifying storage devices in forensic investigations	Forensic images	Privacy concerns related to the content of forensic images and equipment

Table 2. Summarizes the Study of Various Data Set

Historical Context

2.1 Pre-Digital Era

The pre-digital era in India, particularly before the enactment of the Indian Evidence Act of 1872, [25] was characterized by a legal framework [24] that primarily relied on physical documentation, eyewitness accounts, and expert testimony for criminal and civil cases, aimed to standardize and codify evidence laws in India. Prior to this, courts followed English law principles in urban areas and varied local practices in rural regions that included Mohammedan law. This framework was influenced by colonial practices and lacked provisions for the evolving technological landscape.

Types of Evidence before Digitalization

- Oral Evidence: Testimonies from witnesses were paramount. The credibility of witnesses played a crucial role in judicial outcomes.
- Documentary Evidence: Written documents, such as contracts and official records, were essential. However, their authenticity often requires additional verification processes.
- Forensic Evidence: Although not formally recognized in the Evidence Act until later amendments, forensic methods like fingerprint analysis were sometimes utilized based on judicial discretion

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

- Eyewitness Testimony: Eyewitness testimony was a key form of evidence in India's legal system, particularly in criminal cases, and was often relied upon to establish facts and support claims.
- Confessions: Confessions were often used as evidence in criminal cases, although their reliability was sometimes questioned due to concerns about coercion and lack of legal representation.
- Photographic Evidence: Photographs and other visual evidence were commonly used to document crime scenes, injuries, and other relevant information.
- Expert Testimony: Expert testimony, such as from forensic scientists, medical professionals, and technical experts, was often used to provide specialized knowledge and insight in legal proceedings.

2.2 Early Recognition of Electronic Evidence

Before the IT Act, Indian law did not have specific provisions for electronic evidence, leading to challenges in admissibility and authentication. Courts had to use traditional principles of documentary evidence, which were not always well-suited to digital records. Courts had to rely on the Indian Evidence Act, of 1872 and general principles of law to deal with electronic evidence. Courts had to rely on the Indian Evidence Act, of 1872 and general principles of law to deal with electronic evidence.

Best Evidence Rule: The original document must be produced in court. Since electronic records were intangible and often had no physical "original," this posed a problem for admissibility.

Authentication: For electronic records to be accepted, they had to be authenticated, typically by the party seeking to rely on them. However, without specific provisions in the law, it was often challenging to prove the authenticity of electronic records.

The Indian legal system faced several challenges in dealing with cybercrime and electronic evidence before the Information Technology Act, 2000 (IT Act) was passed. [19,20][11]

Lack of a Legal Framework: There were no provisions for the use of digital signatures or the validation of digital documents.

[11] Tania Islam, Indian Legal System In Dealing With Cybercrime, Lawoctopus (Nov. 9, 2024, 8:20 P.M.), https://www.lawctopus.com/academike/indian-legal-system-cybercrime/.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Chain of Custody Issues: There was uncertainty about how to maintain and verify the integrity of electronic records over time.

No Guidelines for Authentication: The courts had no clear standards for verifying the authenticity of electronic evidence.

Slow Response to Cybercrime: The police and other law enforcement agencies often lack the expertise and resources to respond quickly and effectively to cybercrime incidents, which could lead to the loss of valuable evidence.

3. Legislative Developments

3.1 The Information Technology Act, 2000

This section deals with the principles governing the admissibility of electronic evidence within the legal framework of the Indian law of evidence[12]. In the year 2000, Parliament enacted on October 17, 2000, the Information Technology Act 2000 (IT to allow for the admissibility of digital evidence evidence which amended the India n Evidence Act 1872 (IEA), the Indian Penal Code, 1860 (IPC) and the Banker's Book Evidence Act 1891. To make the electronic evidence admissible, the definition of 'evidence' has been amended to include electronic records. The term 'electronic records provides for data, record or data generated, image [7,8] or sound stored, received, or sent in an electronic form or microfilm or computer-generated records.[13] The Information Technology Act, of 2000 [22] represents a significant step towards modernizing India's legal framework in response to digital advancements. By providing a structured approach to electronic transactions and cybercrime regulation, it lays the groundwork for a secure and efficient digital economy in India. The IT Act originally comprised 94 sections, divided into 13 chapters and 2 schedules. Over time, certain sections have been amended or omitted to adapt to evolving technological landscapes.

Major Provisions

Digital Signatures: The Act recognizes digital signatures as valid for authentication purposes, ensuring secure online transactions.[14]

Cybercrime Definitions: It outlines various offenses such as hacking, identity theft, and publishing obscene materials electronically.

[12] Pathsala, https://www.lawctopus.com/academike/indian-legal-system-cybercrime/ (last visited Nov.9, 2024).
[13] Id. At 1807.
[14] Legalstix, https://www.legalstixlawschool.com/blog/Information-Technology-Act-2000 (last visited Nov.9, 2024).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Controller of Certifying Authorities (CCA): The Act establishes a regulatory body to oversee the issuance of digital signatures.

3.2 The Information Technology (Amendment) Act, 2008

The Information Technology (Amendment) Act, 2008 was a significant amendment to the IT Act, 2000, [21] which aimed to enhance the security and confidentiality of electronic records and data, prevent cybercrime, and facilitate the collection and preservation of electronic evidence. IT (Amendment) Act, 2008 has introduced clause 43A – "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns controls or operates is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damaged by way of compensating to the person so affected" to protect the privacy of consumers/customers/citizens.[15] Key points about this amendment:

1. Purpose: It was enacted to address issues related to cybercrime, electronic commerce, and digital signatures that were not adequately covered in the original act.
2. Key additions:
    - Introduced provisions for cybercrime offenses like cyberstalking, identity theft, and phishing.
    - Added sections on child pornography and cyberterrorism.
    - Expanded the definition of computer networks to include mobile devices.
3. Data protection: Introduced rules for the protection of sensitive personal data and information.
4. Intermediary liability: Clarified the liability of intermediaries (like ISPs and social media platforms) for third-party information or data they host.
5. Electronic evidence: Strengthened provisions related to electronic evidence and its admissibility in court.
6. Penalties: Increased penalties for various cybercrimes and introduced new offenses.[16]

[15] Nishith Desai, ANALYSIS OF THE NEW DATA PROTECTION LAW PROPOSED IN INDIA, Nishithdesai (Nov. 9, 2024, 8:20 P.M.), https://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA%20Hotline/Analysis_of_the_new_Data_Protection_Law_Dec2419.pdf

[16] Shreyansh Pandey, IT Act 2000 vs IT amendment act, 2012, legalvidhiya (Nov. 9, 2024, 8:20 P.M.), https://legalvidhiya.com/information-technology-act-2000-vs-information-technology-amendment-act-2012/.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

7. Regulatory bodies: Empowered various regulatory bodies to frame rules and regulations under the Act.

8. Implementation: The Act came into force on October 27, 2009.

Some key provisions of the IT Amendment Act, of 2008 include:

- Amendment of Section 43: The amendment enhanced the penalties for damage to computers and data, and added new offenses, such as identity theft, phishing, and cyber-squatting.
- Amendment of Section 66: The amendment increased the punishment for hacking, tampering with computer source code, and transmitting viruses.
- Amendment of Section 67: The amendment enhanced the punishment for obscene and indecent content on the internet, and expanded the scope to include transmission of such content through any electronic medium.
- Amendment of Section 69: The amendment provided for the interception, monitoring, and decryption of electronic communications for national security and public safety.
- New Section 72A: The amendment introduced a new provision prohibiting the disclosure of personal information without the individual's consent.
- Amendment of Section 79: The amendment introduced the concept of safe harbor for intermediaries, providing them immunity from liability for content hosted on their platforms provided they comply with the due diligence requirements under the Act.
- New Section 69B: The amendment empowered the Central Government to issue directions for blocking access to any information through any computer resource in the interest of sovereignty, security, defense, and public order.[17]

3.3 The Information Technology (Amendment) Act, 2021

The Information Technology (Amendment) Rules, 2021 were introduced by the Indian government as an amendment to the Information Technology Rules, 2011, to strengthen the regulation of social media platforms, digital news websites, and online streaming services. It refers to updates made to India's Information Technology (IT) Act, 2000,[23] to address the dynamic nature of technology, internet regulation, and digital rights. The amendments were mainly focused on enhancing oversight of digital platforms, data protection, and preventing

[17] The Information Technology Act, 2000, 4, No. 21, act of Parliament, 2000 (India).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

misuse of social media, particularly in light of rising incidents like cyberbullying, misinformation, and the need for accountability in the digital sphere.

Key Provisions and Highlights:

• Intermediary Guidelines and Digital Media Ethics Code: The amendment introduced stricter rules for social media platforms, online streaming services, and news websites, making it mandatory for them to: Establish a grievance redressal mechanism[18]. Appoint officers like a Chief Compliance Officer (CCO), Nodal Contact Officer, and Grievance Officer to handle content issues. Ensure traceability of messages for law enforcement purposes in cases of serious offenses.

• Increased Regulation of Social Media Platforms: The act classified social media intermediaries into two categories—social media intermediaries and significant social media intermediaries. The latter, due to their scale, faced stricter requirements. They were required to: Enable identification of the "first originator" of messages if needed for investigating crimes. Remove flagged content within 36 hours.

• Content Moderation and Takedown: Platforms were asked to take down offensive content related to child sexual abuse, threats to India's security, or misinformation within a specific time frame. An appeals process was introduced for users to challenge content removal decisions.

• Digital Media and OTT Platforms: For online streaming services, a self-regulatory code of ethics was mandated, where a body would monitor compliance and handle grievances about content.

• Data Protection and Privacy: Though not a complete data protection law, the amendment enhanced user privacy by holding platforms accountable for the collection, processing, and use of personal data.

• Increased Penalties for Cybercrimes: The amendments also introduced heavier fines and penalties for cybercrimes, including hacking, identity theft, and cyberbullying, with a focus on ensuring justice for victims and accountability for offenders.

3.4 Information Technology Amendment Rules, 2023

The 2023 IT Rules Amendment refers to changes made to India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These amendments

[18] Sanjay Kanojia, Explainer: Why India's new rules for social media, news sites are anti-democratic, unconstitutional, Scroll (Nov. 9, 2024, 8:20 P.M.), https://scroll.in/article/988105/explainer-how-indias-new-digital-media-rules-are-anti-democratic-and-unconstitutional.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

were introduced in October 2023 and are significant for their impact on social media platforms, online content, and digital news media. Here are the key points about this amendment:

• Fact-checking unit: One of the most controversial aspects is the establishment of a government fact-checking unit. This unit has the authority to flag content as "fake," "false," or "misleading," particularly concerning the central government's business.

• Content removal: Social media platforms are required to remove content flagged by this unit within 36 hours.

• Due diligence: The amendment places additional due diligence requirements on social media intermediaries.

• AI-generated content: The rules address concerns about AI-generated misinformation, requiring platforms to be more vigilant about such content.

• User rights: Platforms are required to respect users' constitutional rights, including the freedom of speech and expression.

• Grievance redressal: The amendment strengthens the grievance redressal mechanism for users.

• Transparency: There's an increased emphasis on transparency reports from social media platforms.

• Critical response: Some have criticized the amendments as potentially infringing on free speech and giving too much power to the government to control online narratives.

• Legal challenges: The rules have faced legal challenges, with some cases pending in Indian courts at the time of my last update.

• Impact on digital news: The rules also affect digital news media, requiring them to adhere to certain guidelines and potentially remove content flagged by the fact-checking unit.

These amendments have sparked significant debate in India about the balance between regulating online content and protecting free speech. Supporters argue they're necessary to combat misinformation, while critics worry about potential misuse and censorship.

4. Bhartiya Sakshya Adhiniyam, 2023 for E-Evidence

The Bharatiya Sakshya Adhiniyam (BSA), also known as the Indian Evidence Bill, is a proposed legislation in India that aims to replace the existing Indian Evidence Act of 1872. This new law aims to streamline, modernize, and simplify the presentation and interpretation of evidence in Indian Judicial.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

• Purpose: The BSA is intended to modernize and update India's evidence laws to better align with current technological advancements and societal changes.

• Comprehensive revision: It represents a complete overhaul of the evidence law framework in India, which has been largely unchanged since the colonial era.

• Digital evidence: One of the major focuses is on incorporating provisions for digital and electronic evidence, recognizing the increasing importance of such evidence in modern legal proceedings.

• Admissibility of evidence: The bill aims to clarify and update rules regarding the admissibility of various types of evidence in court.

• Expert testimony: It includes updated provisions on the use of expert testimony in court proceedings.

• Privacy concerns: The proposed law attempts to balance the need for evidence collection with the privacy rights of individuals.

• Scientific advancements: It incorporates considerations for new scientific methods of evidence collection and analysis, such as DNA testing.

• Language: The bill is being drafted in simple, accessible language to make it more understandable to the general public.

• Consultation process: The development of the BSA has involved consultations with various stakeholders, including legal experts, judges, and law enforcement agencies.

• Timeline: As of my last update, the bill was still in the drafting and consultation phase. It had not yet been introduced in the parliament for debate and passage.

• Controversies: Like many significant legal reforms, the BSA has been the subject of debate among legal scholars and practitioners regarding its potential impacts on the justice system.

4.1 Key Additions and Alterations

• Incorporation of Digital and Electronic Evidence Provisions

Recognition of E-Evidence: One of the key reforms includes a greater focus on the admissibility and handling of digital evidence. Provisions will likely streamline how electronic records, including data from digital devices, social media, and online platforms, are admitted as evidence in court.

Section 65B Revisions: The rules around the certification of electronic records under Section 65B of the Indian Evidence Act may be revised, either to simplify the process of obtaining the

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

necessary certification or to introduce more flexibility, reducing the burden on litigants and making it easier to present digital evidence in court.

• Strengthening of Witness Protection and Testimonies

Protection of Vulnerable Witnesses: There could be provisions to strengthen the protection of vulnerable witnesses, such as those involved in sensitive cases (e.g., sexual offenses, human trafficking). The use of video conferencing and anonymity for witnesses in such cases may become more streamlined.

Perjury Penalties: Increased penalties for false testimony or perjury may also be incorporated, helping to enhance the integrity of witness testimonies.

• Clarification on the Burden of Proof and Presumptions

Revisions to the Burden of Proof: The Act might introduce clearer rules around the burden of proof, especially in cases involving digital and circumstantial evidence. This would ensure that litigants better understand their responsibilities in presenting valid evidence.

Presumptions in Specific Cases: New presumptions in favor of certain types of evidence, like government-maintained records or certified electronic evidence, could simplify the litigation process.

• Expanding Admissibility of Evidence

Simplified Admission Procedures: The rules of admissibility might be simplified, with fewer procedural hurdles in accepting evidence related to digital communications, electronic media, and forensic evidence.

DNA and Forensic Science: The BSA may expand provisions relating to DNA evidence and forensic science, making such evidence more central in criminal investigations and trials.

• Strengthening the Chain of Custody

Provisions aimed at ensuring the integrity of evidence from collection to presentation in court (the "chain of custody") will likely be updated. This is especially relevant for digital evidence which is easily alterable or destructible. Courts will likely need stricter procedures for tracking and maintaining the integrity of electronic records.

• Modernization of Language and Terminology

The Bharatiya Sakshya Adhiniya could see a modernization of the terminology used in evidence law, replacing archaic language with more contemporary legal terms. This will improve the readability and application of the law, making it easier for legal professionals and litigants to understand the provisions.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

• Introduction of Data Privacy Considerations

Given the rising importance of data privacy in the digital age, the new Act may include provisions aimed at balancing the need for evidence with individuals' privacy rights. This could be particularly relevant in cases involving the seizure and analysis of digital devices, such as mobile phones or computers.

• Increased Use of Technology in Legal Proceedings

The BSA will likely encourage the use of technology in legal processes, such as through electronic submissions of evidence or virtual hearings. This would aim to enhance the efficiency and accessibility of the legal system, especially in light of the pandemic-era shift toward digital courts.

• Reform of Documentary Evidence Rules

The reforms may seek to streamline documentary evidence rules, especially in the context of electronic documents. This would involve aligning the legal treatment of digital documents with that of physical documents to ensure both are treated equally in court.

• New Provisions for Interrogations and Confessions

The Bharatiya Sakshya Adhiniya may introduce updated regulations around the admissibility of confessions and interrogations, particularly in the context of digital recordings. These rules would ensure that interrogations recorded electronically follow appropriate procedures for use in criminal trials.

• Gender-Sensitive Provisions

New gender-sensitive provisions may be added, ensuring that victims of gender-based violence are better protected in court proceedings. This includes protecting the dignity and privacy of victims when presenting evidence related to sexual offenses.

4.2 Comparison of the Bharatiya Sakshya Adhiniyam, 2023, and the Indian Evidence Act, 1872

1. The Indian Evidence Act, of 1872 contained 3 Parts and 11 Chapters

2. The Bharatiya Sakshya Adhiniyam, 2023 Contains 4 Parts, 12 Chapters and a Schedule

3. The Indian Evidence Act, of 1872 had a total of 167 sections whereas The Bharatiya Sakshya Adhiniyam, 2023 contains 170 sections

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.



Chart 1: Bharatiya Sakshya Adhiniyam, 2023

5. Available Research Datasets for Digital Forensics

Dataset	Description	Source
Network Forensics Datasets UNSW-NB15 Dataset	A comprehensive network traffic dataset for intrusion detection systems. Contains both normal and attack network behaviors, including DoS, exploits, fuzzers, and worms.	UNSW-NB15 Dataset
CICIDS2017 Dataset	Network traffic dataset for intrusion detection system (IDS) evaluation. Benign and common attack traffic, including brute force, DoS, DDoS, web attacks, and infiltration.	Canadian Institute for Cybersecurity
Malware Analysis Datasets Microsoft Malware Classification Challenge (BIG 2015)	A large dataset of malware samples for classification. 9 classes of malware, with both binary and disassembled versions.	Kaggle
Android Malware Dataset (AMD)	A large collection of Android malware samples. Over 24,000 samples, were categorized by malware family. Over 24,000 samples, were categorized by malware family.	AMD Project
NSL-KDD Dataset	An improved version of the KDD Cup 1999 dataset, used for intrusion	NSL-KDD Dataset

www.abhidhvajlawjournal.com
The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Dataset	Description	Source
	detection and training machine learning models to detect network attacks.	
CICIDS 2017 (Canadian Institute for Cyber Security Intrusion Detection Evaluation)	A modern dataset with up-to-date network traffic logs containing both benign and malicious traffic is ideal for machine learning experiments in network forensics.	CICIDS 2017
Phishing Websites Dataset	A dataset containing features of phishing and legitimate websites, which can be used to build machine learning models for detecting phishing attacks.	Phishing Websites Dataset

Table: Available Research Datasets for Digital Forensics

6. Case Studies of Digital Forensic

Visualizing and Reasoning about Presentable Digital Forensic Evidence with Knowledge Graphs

• Digital forensics is the process of examining and interpreting data from digital devices in order to find out what happened.

• Identification, collection, examination, [24] and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data[19]

• The importance of digital forensic evidence

• Evidence is the key to proving someone is guilty or innocent of the actions they have been charged

• Testifying in court as an expert

• Digital forensic professionals need to present and interpret evidence to various audiences

Approach: Presentable Digital Forensic Evidence (PreDIE) based on Knowledge Graph

• Representing digital forensic evidence in Digital Forensic Knowledge Graph (DFKG)

• It puts evidence information in context via linking and the semantic metadata of evidence as well as describes how digital examiners interact with evidence

• Different than Web Ontology Language: describing and exchanging static metadata of entities

[19] Digital Forensics in the Cloud, https://apps.dtic.mil/sti/pdfs/ADA590911.pdf (last visited Nov. 9, 2024).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

• DFKG supports the criteria of PreDIE

• Authenticity: A piece of digital forensic evidence is proven to be genuine and not a forgery.

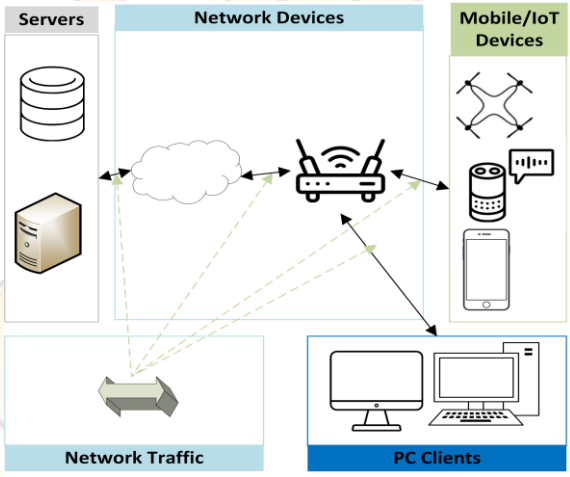
• Integrity: A piece of digital forensic evidence should not have been tampered with.

• Validity: The validity of evidence means that a tool used in forensic examination meets standards.

• Credibility: The credibility of evidence demonstrates a forensic examiner who will be responsible for the discovery or interpretation of artifacts

• Relevance: Evidence is relevant if it has any tendency to make a fact more or less probable than it would be without the evidence and the fact is of consequence in determining the action[20]

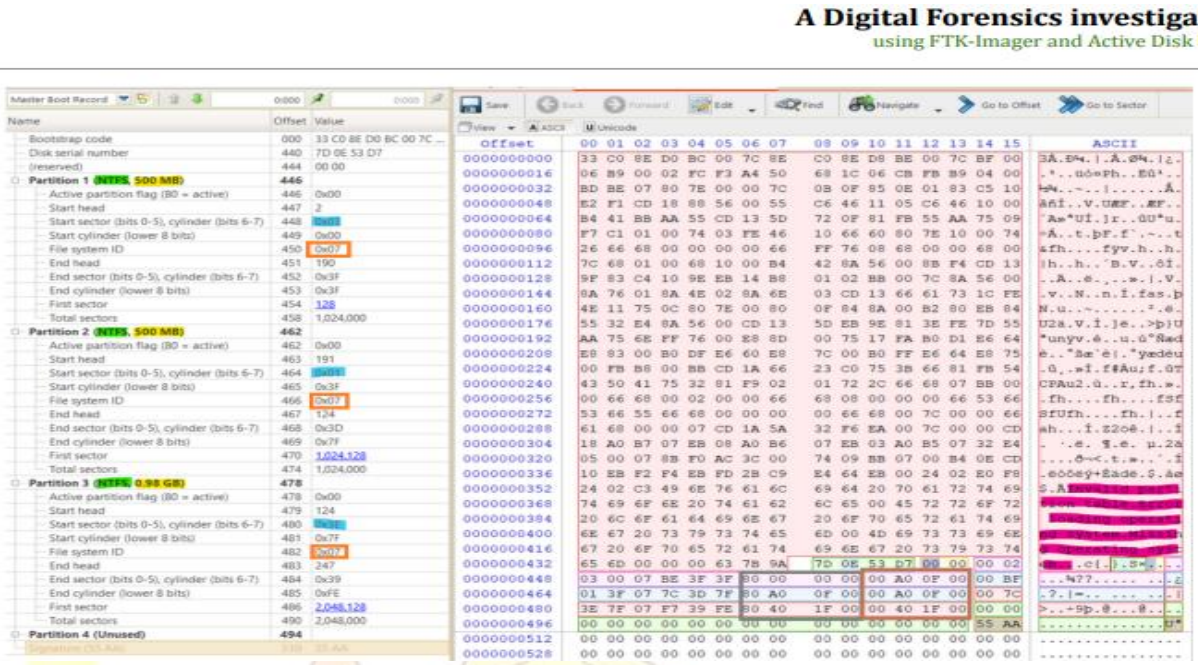
• Digital Forensic Knowledge Graph (DFKG): Cyber Case Descriptive Objects (CCDO), Cyber Forensic Observable Objects (CDOO), Cyber Forensic Domain Objects (CFDO).



Picture 1: Digital Forensic Knowledge Graph

[20] Law Indiana edu, https://law.indiana.edu/instruction/tanford/b723/04relev/R401.pdf (last visited Nov.9, 2024).

www.abhidhvajlawjournal.com
The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

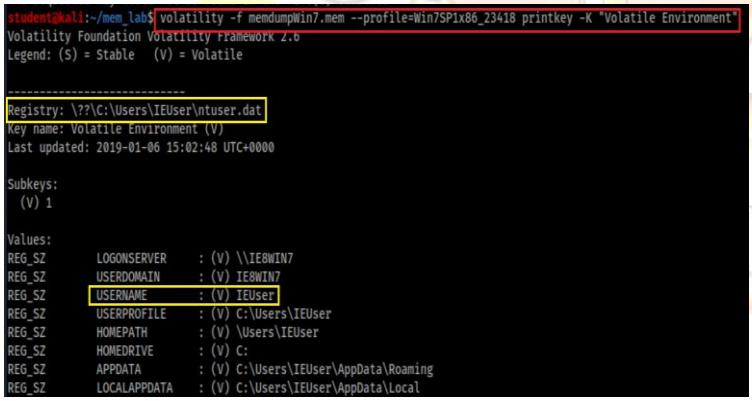


Picture 2: FTK Imager

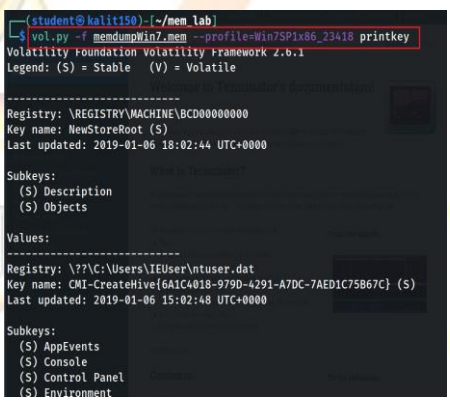
Memory Forensics (Memory and Memory Dump)

A memory dump is a process that takes all information in RAM and writes it to a storage drive in case of an application or system crash known as a core dump, and blue screen of death (BSOD) in Windows-based computers.

Investigation: Understand the Suspect and Accounts, Understand the Suspect's PC, Network Forensics, Investigate Command History, Investigate the Suspect's USB, Investigate Internet Explorer History, Investigate File Explorer History Timeline Analysis



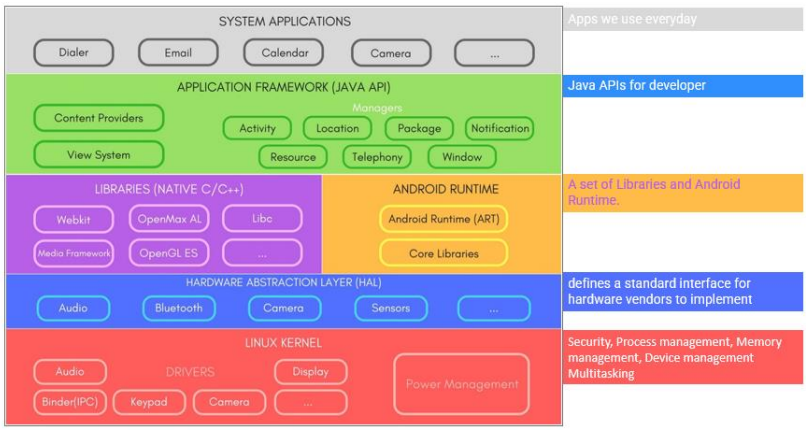
Picture 3: Who was using the device?



Picture 4: Show all registry keys

Android Devices

www.abhidhvajlawjournal.com
The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.



Picture 5: List all app names and package ID

IoT Forensic

This appears to be a new subfield of digital forensics that poses significant privacy concerns. It entails the forensic examination of IoT devices such as smart devices (lights, doorbells, speakers, cameras, home appliances, etc.) and connected systems (e.g., in smart cities). IoT forensics [18] evidence can be used to corroborate claims made in court. For example, data retrieved from smart doors can be utilized to confirm the presence of a suspect in a particular location at a certain time.

Printer Forensics

Printer forensics is crucial for identifying the devices used to print materials related to criminal or terrorist activities. Forgers often use digital scanners and printers to create counterfeit currency and documents. By analyzing printed documents, forensic experts can identify unique characteristics of printers and even differentiate between devices of the same model. This helps law enforcement agencies trace counterfeit materials back to specific printers.

Investigating Emails

- Email Forensics [3] refers to analyzing and recovering email messages and other information related to email accounts for criminal investigations, litigation, and compliance.
- Data Acquisition: The first step in email forensics is to acquire the relevant data, including email messages, attachments, and other metadata, from the email server, desktop computers, laptops, or mobile devices.
- Forensic Analysis: The data is then analyzed using specialized software tools and techniques to extract and reconstruct the email messages and other relevant information.

www.abhidhvajlawjournal.com
The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

7. Challenges and Considerations

Technical Complexity: Collecting and preserving digital evidence requires specialized skills and tools. Law enforcement agencies must be equipped with advanced technology and trained personnel to handle digital forensic tasks effectively.

Cloud Storage: The rise of cloud storage necessitates navigating challenges in accessing and analyzing remotely stored data. Gathering evidence from the cloud involves legal procedures, coordination with service providers, and potential jurisdictional complexities.

Chain of Custody: Maintaining the chain of custody is critical for evidence admissibility in court. Hardware-related challenges arise during the secure transfer and storage of digital devices while preserving evidence integrity.

Privacy Concerns: The increased reliance on digital evidence raises significant privacy issues. There is a need for stringent protocols to protect individuals' data while conducting investigations.

Awareness and Training: There is a critical need for widespread training among law enforcement officials, legal practitioners, and the public regarding the new laws and effective digital evidence-handling practices.

Bias and Accuracy: AI systems can inherit biases present in training data, leading to inaccurate results or wrongful conclusions. Continuous monitoring and refinement of algorithms are necessary to mitigate these risks.

Internet of Things (IoT) Devices: The proliferation of IoT devices generates vast data volumes. Investigating these devices demands expertise in their unique architectures, communication protocols, and data storage mechanisms.

Physical Device Access: Obtaining access to locked or password-protected devices, particularly mobile phones and encrypted hard drives, poses significant hurdles for cyber forensic investigations.

8. Future Trends

Emerging Technologies

- Advances in AI and ML Algorithms: How the future development of more sophisticated algorithms could further enhance forensic investigations.
- Integration with Emerging Technologies: The potential for combining AI with technologies such as block chain and quantum computing to improve evidence integrity and security.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

- Collaborative Frameworks: The role of collaboration between law enforcement agencies, technology companies, and academic institutions in advancing AI and ML use in digital forensics.
- Collection and Annotation of Events Filtering Datasets: With the ubiquity of smartphone and camera devices, the number of events recorded and consequently, the volume of data generated surpasses the human ability to analyze it. These models help to promise future direction in reducing the need for annotated data.
- Forensic Artefact: XAI (Explainable Artificial Intelligence) libraries are software tools that aim to make the inner workings of AI models more transparent and understandable. And relevant domain experts to analyze the end-to-end solution and identify discrepancies that may result in sub-optimal performance relative to the objectives required. It is designed based on 1) data analysis, 2) model evaluation, and 3) production monitoring. AI functions contain
    - Decision Trees which are a graphical representation of a series of decisions, where each branch represents a possible outcome. In the context of XAI, decision trees can be used to illustrate the steps taken by an AI model to arrive at a decision or prediction.,
    - LIME (Local Interpretable Model-Agnostic Explanations): LIME is an open-source software tool that can be used to explain the predictions of machine learning models by decomposing them into small, interpretable components.[21]
    - Anchors: Anchors are a visual tool for explaining the behavior of machine learning models by highlighting a set of examples that are most similar to the input data.
    - Rule Lists: Rule lists are a human-readable representation of machine learning models that can be used to explain the logic behind the model's predictions.

[21] Tushar Khot, Daniel Khashabi, Kyle Richardson, Peter Clark, Ashish Sabharwal, Text Modular Networks: Learning to Decompose Tasks in the Language of Existing Models, Cornell University (Nov.9, 2024, 8:30 P.M.), https://arxiv.org/abs/2009.00751.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

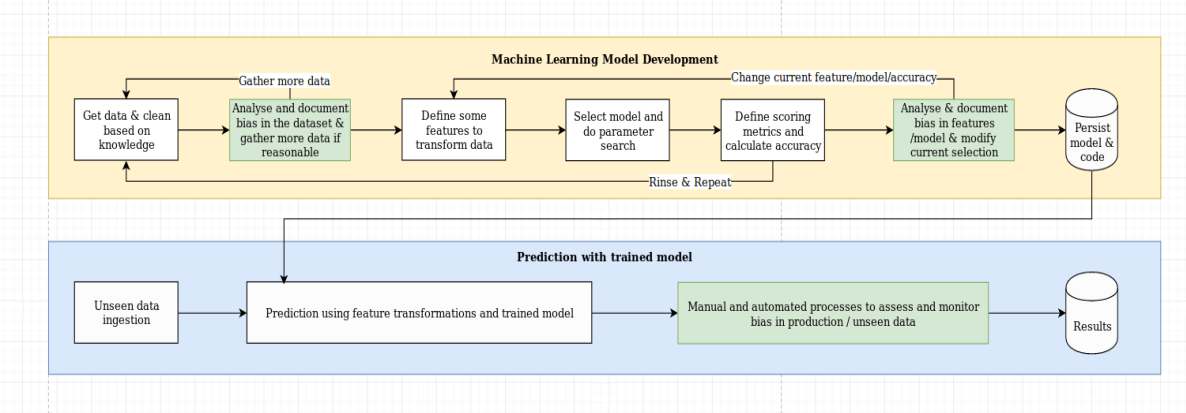


Chart 2: Explainable Artificial Intelligence Model

9. CONCLUSION:

The evolution of e-evidence in Indian criminal law has been marked by significant legislative and judicial developments. While substantial progress has been made in adapting the legal framework to the digital age, challenges remain. The field of digital forensics continues to evolve in response to these legal changes and technological advancements. As India moves forward, it is crucial to maintain a balance between effective law enforcement, admissibility of digital evidence, and protection of individual rights in the digital sphere. The integration of digital forensics into India's new criminal laws represents a critical step towards modernizing the justice system. By leveraging technological advancements, these laws aim to streamline judicial processes, enhance citizen protection, and ensure that justice is served efficiently in an increasingly digital world. However, addressing challenges related to public awareness, infrastructure, and privacy will be essential for realizing the full potential of these reforms.

Author's contributions

The single "Kaushik Maitra" author contributed significantly towards the final make-up of the paper. Conceptualization; Data curation; Formal analysis; Literature review and Methodology; Supervision; Writing-original draft; Writing-reviewing and editing

Acknowledgment Statement

I would like to thank Working in the Technical Forensic Unit, Central Bureau of Investigation, Govt. Of India. Their commitment to the cause and their expertise in the field of Digital forensic collection and analysis has been instrumental in completing this study. Additionally, we extend our heartfelt thanks to the Central Forensic Lab and the Department of Cyber Science & Technology of Brainware University involved in the study for their participation & trust and make a positive impact on Digital Forensic Investigation under the Indian legal framework.

Declaration of Competing Interest:

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding:

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.[22]

Ethical Approval:

Research involving Human Participants and/or Animals: This article does not contain any studies with human participants or animals performed by any of the authors.

[22] Zahra Mokhtari, Health-related quality of life in Iranian patients with type 2 diabetes: An updated meta-analysis study, Strath prints (Nov.9, 2024, 8:33 P.M.), https://strathprints.strath.ac.uk/65727/1/Mokhtari_etal_DMS_2018_Health_related_quality_of_life_in_Iranian_patients.pdf.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

References:

1. Bhatt VH (2010) A Data Mining Approach for Data Generation and Analysis for Digital Forensic Application. IACSIT 2(3):313–319
2. Yannikos Y et al (2014) Data corpora for digital forensics education and research. In: IFIP International conference on digital forensics, pp 309–325
3. Bogawar P, Bhoyar K (2016) A novel approach for the identification of writing traits on email database. In 2016 1st India International Conference on Information Processing (IICIP) 1-6
4. Morovati K, Kadam S (2019) Detection of phishing emails with email forensic analysis and machine learning techniques. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(2):98-107, 2019
5. Gobel T, Schafer T, Hachenberger J, Turr J, Harald B (2020) A Novel approach for generating synthetic datasets for digital forensics. Adv Digit Forensic XVI, IFIP ACT 589:73–9
6. Reith M, Carr C, Gunsch G (2002) An examination of digital forensic models. Int J Digit Evid 1(3):1–12
7. Casey E (2011) Digital evidence and computer crime 3rd Edition. Forensic Science, computers, and the Internet. Academic Press. eBook ISBN: 9780080921488
8. Ferreira S, Antunes M, Correia M (2021) A dataset of photos and videos for digital forensics analysis using machine learning processing. Data 6(8):87
9. Sammut C, Webb G (2010) Mean absolute error. Encyclopedia of Machine Learning, 652
10. Steel C et al (2022) Technical behavior of child sexual exploitation material offenders. J Dig Forensic Secur Law 17(1):2
11. Sunde N, Dror I (2019) Cognitive and Human Factors in Digital Forensics: Problems, Challenges, and the way Forward. Digit Investig 29:101–108
12. Doowon J (2020) Artificial intelligence security threat, crime, and forensics: taxonomy and open issues. IEEE Access 8:184560–184574
13. Rohan Jain, Admissibility of Electronic Record in India, MANUPATRA, (June 13, 2023, 1:28 PM) https://articles.manupatra.com/articledetails/Admissibility-of-Electronic-Record-inIndia

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

14. Devang Chhatrapati, Arun B. Prasad, Electronic Evidence-Admissibility and Authentication: A Judicial Perception of Apex Court of India, researchgate, (June 13, 2023, 7:30 PM) https://www.researchgate.net/publication/353581175_Electronic_EvidenceAdmissibility_and_Authentication_A_Judicial_Perception_of_Apex_Court_of_India
15. Dubey V (2017), "Admissibility of Electronic Evidence: An Indian Perspective", Forensic Research & Criminology International Journal, 4(2) 2017.
16. S V N Adarsh, B A S Ajeena, A log-based strategy for fingerprinting and forensic investigation of online cybercrimes International Conference on Interdisciplinary Advances in Applied Computing (ICONIAAC '14), volume 7, p. 1 - 5 Posted: 2014
17. Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Science International, 231(1-3), 284-295.
18. Atzori, L., Lera, A., & Morabito, G. (2010). The Internet of Things: A Survey. Computer Networks, 54(15), 2787-2805.
19. Prakash Nilima, Duhan Roshni, Computer forensic investigation process and judicial response to the digital evidence in India in light of the rule of best evidence, Indian journal, Online ISSN: 2321-1784.Published online: 2020 May 04, Volume: 8, Issue: 5
20. Amit Kumar Das, Types of Jurisdictions, WRITINGLAW.COM, Aug 8, 2023 10 Types or Kinds of Jurisdiction of Indian Courts (writinglaw.com)
21. Singh, S., & Mishra, D. (2019). An Overview of Digital Forensic Investigations in India. International Journal of Computer Sciences and Engineering, 7(1), 199-203.
22. 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
23. Mittal, S., & Jha, S. (2020). Privacy Concerns and Digital Evidence: A Critical Analysis. Journal of Indian Law and Society, 11(2), 34-46.
24. MANINDRA SINGH HANSPAL, Navigating Legal Changes in BNS, BNSS, and BSA, 2023: A New Era for Women's Safety in India, INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION, ISSN 2581-9453, Vol. 6 Iss 4;
25. Agarwal, S. P. (2016). The Indian Evidence Act, 1872: With Exhaustive Case Law. Eastern Book Company

26. Kamshad Mohsin and Dr. K. B. Asthana, Digital Forensics in Law: Unravelling the Challenges and Advancements, International Journal of Forensic Research, ISSN: 2767-2972
27. Turner, P. (2005) 'Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)', Digital Investigation, 2(3), pp. 223–228.

ABHIDHVAJ LAW JOURNAL