IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

ADVANCING CRIMINAL INVESTIGATIONS THROUGH DIGITAL FORENSIC: AN IN-DEPTH EXPLORATION OF CONTEMPORARY TECHNNIQUES AND CHALLENGES.

- Shivani[1]

- Dr. Sugandha Passi[2]

ABSTRACT

Digital forensics is a crucial component of contemporary criminal investigations and legal proceedings, serving as a linchpin for the acquisition, scrutiny, and protection of electronic evidence from diverse digital devices. This abstract emphasizes the role of digital forensics in augmenting criminal inquiries and offers an insightful assessment of its integration into the legal system, recognizing modern methods and hurdles.

Commencing with an introduction that underscores the importance of digital forensics, this paper highlights its benefits, including evidence preservation, fortifying public safety, national security, and the determination of culpability in criminal cases. The central aim of this paper is to uncover the techniques and challenges associated with digital forensics in criminal investigations, encompassing data acquisition for proving cybercrimes.

Furthermore, the paper scrutinizes the obstacles faced by digital forensics, categorized into two key areas: technical and legal. Lastly, it explores future prospects in digital forensics in the context of criminal investigations, encompassing advancements such as enhanced data analysis, the integration of machine learning and artificial intelligence, online dispute resolution (ODR), and AI-driven "robot lawyers." The utilization of artificial intelligence emerges as a significant opportunity, promising streamlined and fortified processes for digital forensics.

Keywords: digital forensics, criminal investigation, evidence collection, data analysis, cybercrime, electronic evidence, legal proceedings, evidence admissibility, digital fraud, digital devices.

[1]Student of LL.M (criminal law) at University Institute of legal studies (UILS) of Chandigarh and Author of the Research paper titled as *"ADVANCING CRIMINAL INVESTIGATIONS THROUGH DIGITAL FORENSICS: AN IN-DEPTH EXPLORATION OF CONTEMPORARY TECHNEQUES AND CHALLENGES"* made under the guidance of Asst. Prof. Sugandha Passi"

[2] *Assistant Professor* at University Institute of legal studies (UILS) of Chandigard University of and Co-Author-cum-supervisor of the Research Paper titled as *"ADVANCING CRIMINAL INVESTIGATION THROUGH DIGITAL FORENSICS: AN IN-DEPTH EXPLORATION OF CONTEMPORARY TECHNEQUES AND CHALLENGES"*

1.Introduction

> "***Technology has become a double- edged sword in the world of crime. As it aids criminals, so too can it be harnessed to bring them justice."-Timothy Good***

Digital forensics is a subset of forensic science focused on enhancing, investigating, examining, and analyzing materials retrieved from digital devices, often pertaining to computer crime and mobile devices[3]. According to *McKemmish* [4]digital forensics centers around recognizing, obtaining, conserving, scrutinizing, and presenting digital evidence stored electronically. Electronic evidence is a component in almost all criminal activities, with digital forensics playing a crucial role in aiding law enforcement investigations.[5] Various devices, such as laptops, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and others, can be employed for the collection of electronic evidence.[6] The primary objectives of digital forensic are collecting information from electronic evidence, modify it into useful intelligence, and provide the findings to the prosecution.to make sure findings are admissible in court, make use of established forensic techniques in the all procedures.[7]

Thus, Digital forensics involves preserving, identifying, extracting, investigating, and documenting computer evidence suitable for legal proceedings. This scientific discipline focuses on discerning evidence across digital platforms like servers, networks, mobile phones, and computers. Equipping forensic teams with advanced techniques and tools, it aids in solving complex cases related to digital forensics.[8]

1.1 Digital Forensic: concepts and foundation

The Technical Committee of the Digital Forensic Research Workshop (DFRWS)[9] has articulated the definition of digital forensic science as follows:

"*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital DFRWS evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned options." -DERWS,2001*

[3] Carrier, B (2001). "Defining digital forensic examination and analysis tools". *International journal of digital evidence.* 1:2003. *cite*citeseerx.ist.psu.edu

[4] McKemmish R (1999) what is forensic computing? Trends and issues in crime and issues in crime and justice, vol. 188 Australian Institute of Criminology, Canberra, 1-6. ISBN 0-642-24102-3

[5] Lim, Nena, "Digital Forensic Certification Versus Forensic Science Certification" (2008). *annual ADFSL Conference on Digital Forensics, Security and Law.8.*

[6] Nelson, B., Phillips, A., Enfinger, F., and Steuart, C (2005) Guide to Computer and Intrusion Forensics, Artech House, Norwood, MA.

[7] Innovations of digital forensics *available at*: https://www.interpol.int (last visited on oct.15,2023)

[8] Lawrence Williams, "what is digital forensics*? available at*: https://www.guru99.com/digital-forensics.htm (last visited on 15 oct.2023)

[9] DFRWS Technical Committee (DFRWS) (2001) A road for digital forensic research: DFRWS Technical Report. DTR-T001-01 FINAL

1.2. Scope of digital forensics in India: The scope of digital forensics is extensive, involving the analysis of data from devices like computers, cellphones, networks, and media storage to detect criminal activities or misuse. This scope has grown due to the increasing use of digital technology in both corporate settings and everyday life. Various forms of digital forensics require in-depth analysis of data from different sources to uncover evidence of criminal behavior.

The Digital forensics encompasses several key areas of application. It is integral to cybercrime investigation, where it aids in the collection of evidence related to cybercrimes. In corporate investigations, it helps probe security issues, intellectual property theft, and various threats. In legal proceedings, both civil and criminal, digital forensic experts preserve, analyze, and present digital evidence in court. Privacy and data protection rely on secure handling of sensitive information, with digital forensics used to investigate data breaches and privacy violations. Professionals in this field also undergo training and research to stay current, aiding in cyber theft investigations and court evidence analysis. The scope of digital forensics evolves to address the demands of an increasingly digital world, driven by technological advancements and escalating cyber threats.[10]

2. Importance of digital forensics in modern crime investigation

Digital forensics holds a critical position in contemporary criminal investigations due to the widespread integration of technology in various criminal activities. Its significance lies in its ability to unearth, scrutinize, and safeguard electronic evidence, ultimately aiding law enforcement in solving crimes and bringing offenders to justice. There are several key reasons underlining the critical role of digital forensics in modern criminal investigations:

2.1 Evidence collection and preservation: Digital forensics plays a pivotal role in the organized and methodical collection and preservation of electronic evidence from a range of devices, including computers, tablets, phones, and other digital media. Maintaining the integrity and admissibility of evidence in a court of law is ensured when it is collected in a methodically sound forensic manner.[11]

2.2 Identification and Acknowledgment: Digital forensics plays a crucial role in identifying suspects by tracing their digital activities, footprints, and cyber connections. By analyzing digital evidence, investigators can attribute actions to specific individuals, offering essential data for criminal profiling and the identification of suspects. [12]

[10] Scope of cyber forensics *available at*: https://forensicsciencepublicdeskindia.wordpress.com (last visited on 15 Oct. 2023)
[11] The Power of Cyber Forensics in Solving Crimes at *available* on https://www.salvationdata.com (last visited on Oct. 16, 2023)

[12] *Ibid.*

2.3 Crime reconstruction: Digital forensics enables the reconstruction of incidents, timelines, and the sequence of activities associated with a crime. Scrutinizing digital artifacts such as emails, messages, files, and transaction records aids in comprehending the premeditation, planning, execution, and concealment of the crime. [13]

2.4 Alibi verification: This process involves investigators confirming the authenticity of an alibi, which is a claim made by a suspect or witness to establish their presence at a different location during the time of a crime.[14] Alibi agencies, also known as alibi networks, utilize electronic records to substantiate or refute alibis. Timestamps, GPS data, and digital communications are instrumental in establishing the whereabouts of individuals at the time of the crime, making an 'alibi' a potent tool in establishing innocence.

2.5 Detection of cybercrimes: In the contemporary era, a significant portion of criminal activities transpires in the digital domain. Digital forensics plays a crucial role in the detection and investigation of cybercrimes, encompassing activities such as hacking digital devices, identity theft, fraud, cyberbullying, and more.[15]

2.6 Support for traditional investigations: In the case of conventional crimes such as homicides, drug trafficking, financial fraud, assault, and burglary, digital forensics assists in uncovering digital evidence that can establish connections crucial for resolving the case.[16]

2.7 Provisions of legal admissible evidence: The Indian Evidence Act outlines provisions for the admissibility of digital evidence in court, making it legally acceptable when forensic protocols and standards are adhered to during collection. Proper handling and thorough documentation of digital evidence enhance its credibility and acceptance within the judicial system.[17]

2.8 Public safety and national security: Digital forensics plays a crucial role in investigating digital activities and communications, allowing law enforcement to identify potential threats to public safety, peace, and national security. Digital forensics aids in the prevention and response to acts of terrorism, cyber-intelligence activities, and other threats to security. [18]

2.9 Efficiency and accuracy: Digital forensic tools and standardized methodologies enable investigators to process large volumes of digital data more effectively, efficiently, and accurately than traditional methods. This eliminates unnecessary time and resource wastage, which is inherent in more time-consuming conventional approaches.

[13] *Ibid.*
[14] Indian evidence Act, 1872[act no. 1 of 1872] Ss.11
[15] *Supra* note 11
[16] *Ibid.*
[17] *Ibid.*
[18] *Ibid.*

2.10 Crime prevention and deterrence: The deterrent effect of digital forensics serves as a preventive measure, dissuading individuals from participating in criminal activities online. They are aware that their actions can be traced and potentially used against them, which acts as a strong deterrent.[19]

3. Scientific evidence and the criteria for its admissibility:

The admissibility of scientific evidence in India, particularly after the ***Selvi v. State of Karnataka case,*** has been a subject of debate.[20],In the case where the Supreme Court discussed the admissibility of scientific evidence, it expressed the dilemma as follows:

"In criminal cases, the reliability of scientific evidence is intricately linked to various aspects of the right to a fair trial, including the burden of proving guilt beyond a reasonable doubt and the defendant's right to present a defense. It is essential to note that these requirements have long been acknowledged as integral to 'personal liberty' under Article [21] of the constitution. Therefore, it is informative to delve into the admissibility of scientific evidence."[21]

Utilizing forensic science for scientific investigations is significantly more robust, dependable, and productive compared to a criminal justice system primarily reliant on eyewitness accounts. Leaving a victim's fate to the discretion of eyewitnesses is not ideal. Various branches of forensic science, such as DNA analysis, ballistics, fingerprinting, toxicology, and others, offer much greater reliability than the testimony of ordinary witnesses within the criminal justice system. In this era of advanced technology, it is imperative to establish legal foundations that encompass both scientific principles and legal principles. In the case of ***Dharma Deo Yadav Vs. State of U.P.,*** the Supreme Court ruled:[22] "The criminal justice system in this country is facing a critical juncture. Often, reliable and credible witnesses to crimes hesitate to testify in court, and even hardened criminals manage to escape the reach of the law. Additionally, reliable witnesses for the prosecution sometimes turn hostile due to intimidation, fear, and various other reasons. Consequently, law enforcement agencies must explore alternative methods to enhance the quality of investigations, primarily through the collection of scientific evidence. In this era of science and technology, we must establish legal foundations that are firmly rooted in both science and law. The practices and principles that have been relied upon in the past are now seen as needing to give way to innovative and creative approaches if we are to salvage our criminal justice system. With the emergence of new types of crimes and their increasing sophistication, traditional methods and tools have become outdated. Oral testimony is susceptible to various vulnerabilities, such as the power of observation, external influences, forgetfulness, and more, while forensic evidence is immune to these weaknesses."

[19] *Supra* note 11
[20] AIR 2010 SC 1974
[21] AIR2010 SC 1974, 5
[22] (2014) 5 SCC 509' 28

In ***Dow Jones & Company Inc. v Gutnick,***[23] the Australia's High Court determined that in defamation cases, an online article is considered published at the moment it is downloaded and read. As a result, an Australian businessman was granted the right to pursue a defamation lawsuit in Australia regarding an article originally published in the United States and posted on the internet.

4. Modern techniques used in digital forensics:

Digital evidence plays a vital role in investigations and legal proceedings, encompassing various areas such as data theft, network breaches, online fraud, identity theft, as well as violent and white-collar crimes. Digital forensics specialists are tasked with gathering, analyzing, and deciphering this evidence. While the 21st century's technological advancements have brought us numerous digital devices that enhance our lives, they also present challenges for modern digital forensics analysts due to the unique characteristics of these devices.

4.1 Digital Vehicle Forensics: Digital vehicle forensics is a valuable tool for uncovering evidence related to modern smart cars, like Tesla, which essentially function as computers on wheels. These vehicles continuously record data that can be detected, analyzed, and are constructed using advanced sensors integrated into the vehicle itself. In general, investigators must gather both physical and digital components, akin to collecting fingerprints, for thorough fingerprint analysis within the field of vehicle forensics. These components aid in collecting crucial evidence necessary for solving complex criminal cases. Even in cases where footage of an incident is compromised or corrupted, contemporary video and digital vehicle forensics tools can still be employed, such as VIP2.0, enable investigators to compute intricate variables pertinent to the case. Forensic tools for vehicles enable the determination of crucial details such as the direction, circumstances, speed, and velocity of the vehicle, all of which contribute to establishing essential evidence.[24]

4.2 Drone forensics-- Contemporary all-digital forensic solutions, such as Salvation Data's Digital Forensic Lab, play a crucial role in tackling diverse criminal activities associated with drone technology. It is imperative not to underestimate the potential misuse of drone technology, which can encompass:

- Unauthorized surveillance[25]
- Espionage[26]
- Voyeurism[27]

[23] (2002) 194 ALR 433.
[24] Vehicle Digital Forensics Services *AT available* on https://techfusion.com (last visited on OCT. 16,2023)
[25] Oxford learner's dictionaries "*Surveillance means the act of carefully watching a person suspected of a crime or a place where a crime may be committed."*
[26] Acc. To wax *espionage* is "*the crime of spying or secretly watching a person, company, government, etc. for the purpose of gathering secret information or detecting wrongdoing, and to transfer such information to another organization or state."*
[27] Acc. To Collins English dictionary "*Voyeurism is the practice of getting sexual pleasure by secretly waiting other people having sex or taking their clothes off."*

- Drug smuggling[28]
- Disrupting airport operations
- Physically attacking innocent civilians

Drones have the potential for use in activities such as espionage, smuggling, and physical attacks.

4.3 Biometrics— Biometric techniques such as face identification, feature identification, face recognition, and fingerprint scans are valuable tools in forensic analysis. By comparing biometric features like facial characteristics and fingerprints to stored data in databases, including information such as age, gender, bone structure, and more, the recognition process can be significantly expedited. Contemporary tools for forensic data analysis possess advanced technological capabilities to extract key features that aid in the identification of individuals, including details related to their eyes, gender, skin attributes, and expressions.[29]

4.4 Social network forensics— Social media forensics is the process of gathering evidence from online platforms to uncover criminal activity. With the widespread use of social media like Facebook, TikTok, WhatsApp, and Snapchat, the number of users is expected to quadruple by 2023. Cyber forensic technology is crucial for analyzing online profiles, revealing connections, and identifying signs of illegal actions. It helps detect illicit transactions, tackle harassment, protect against the release of personal information, and play a significant role in our technology-driven world.[30]

4.5 Geolocation— Digital Device Usage: Nowadays, everyone uses digital devices such as mobile phones on a daily basis, making it relatively simple to track various personal information, including GPS location data and Google Maps timelines, among other details. This information can also be invaluable in investigations, where Digital forensics tools, such as SPR Pro, are utilized to extract photos and other evidence from these devices.[31]

4.6 Cloud forensics— Shams, defines cloud forensics as *"the application of computer forensic principles and procedures in a cloud computing environment"*[32] A significant portion of individuals' data, over 50%, is now stored in the cloud. For those well-versed in cloud forensics technology, this presents an opportunity to analyze cloud-stored data when seeking clues or evidence. However, there are various challenges associated with data recovery, particularly when utilizing iCloud for iPhones. These challenges involve ensuring the admissibility of the collected

[28] Collins English dictionary "*drug is a chemical which is given to people in order to treat or prevent an illness or disease".* And *"Smuggle means if someone smuggles things or people into a place or out of it, they take them there illegally or secretly".*
[29] Monika Saini and Anup Kumar Kapoor*, "Biometric in forensic identification: applications and challenges"* volume 1 journal of forensic medicine.
[30] Vivekananth. P *"The Role of Social Media Forensics in Digital Forensics"* (August 28, 2022)
[31] Christopher Galbraith, Padhraic Smyth, *et.al.,* "Statistical Methods for the Forensic Analysis of Geolocated Event Data" 33 *Forensic Science International: Digital Investigation* (July 2020)
[32] Shams Zawoad and Ragib Hasan. "*Cloud forensics: a meta- study of challenges, approaches, and open problems*". ArXiv preprint arXiv: 1302.6312,2013

evidence in a court of law. When handling evidence of this nature, investigators also have concerns about maintaining the chain of custody and addressing other related issues. [33]

4.7 Fingerprint Forensics— Sir Francis Galton demonstrated the utility of fingerprints in identification, and analyzing the evidence by fingerprints, fingerprints fixed and permanent in nature it is experts can easily identify the perpetrator of the crime by forensic DNA database of potential mathes. Scientists are advancing fingerprint analysis, exploring DNA, amino acids, and explosive residues in prints. This aids cases like Johnson's, using new techniques for prints collected in 1994 to potentially clear the accused. These innovations handle small material quantities (500 nL), making chemical fingerprint analysis feasible, despite lower DNA levels compared to swabs. Tracey Dawson Cruz, a forensic molecular biologist at Virginia Commonwealth University, highlights the ability to extract biological profiles from small samples. Such methods complement traditional pattern analysis, offering deeper insights from fingerprints, even in smudged prints. [34]

4.8 Voiceprint forensics— Just like fingerprints, voiceprints are inherently unique to each individual. By conducting digital forensic analysis on voice recordings, investigators can compare audio samples to determine if the voice in two distinct recordings belongs to the same person. Each individual's voice exhibits distinctive characteristics.[35]

4.9 Malware forensics—Diverse types of malware forensics have emerged, posing significant cyber threats capable of stealing data, taking control of your browser, erasing files, encrypting them, and demanding a ransom for the decryption key.[36]

4.10 Email forensics—This entails scrutinizing emails and their content to determine their authenticity, source, date and time, actual sender, and recipients in a forensically sound manner. The aim is to generate admissible digital evidence suitable for presentation in civil or criminal court proceedings.

4.11 Mobile Forensics: Mobile forensics is a discipline that ensures the protection and preservation of system integrity. This process can be divided into three primary categories: seizure,
acquisition, and examination and analysis. Mobile forensics entails extracting digital evidence from mobile devices using established techniques and methods.[37]

[33] Cloud forensics and the digital forensics *available at:* https://www.appdirect.com (last visited on Oct. 16 2023)
[34] Kerri Jansen, "Fingerprints are more than just patterns; they're chemical identities" *C&en* march 10, 2019
[35] Timblin, Terry "Voiceprints: The Determination of Admissibility," University of Dayton Law Review. 2, No. 1, (1977): Article 8.
[36] Brand, Murray, Villi, Craig; and Woodward, Andrew (2010) "Malware Forensics: Discovery of the Intent of Deception", *Journal of Digital Forensics, Security and law:* Vol. 5: No. 4, Article 2.
[37] Mobile forensics and forensics lab *available at:* https://securityscorecard.com(last visited on 16 Oct. 2023)

4.12 Network forensics— Network Forensics: Network forensics is a discipline that focuses on uncovering and recovering information related to cybercrimes occurring in networked environments. It is defined as the practice of monitoring and analyzing computer network traffic. network

4.13 Memory forensics— Memory forensics stands as a crucial facet of cyber investigation, enabling investigators to pinpoint unauthorized and anomalous activities on a target computer or server. Investigative insights, including running processes, executable files, IP addresses, and other network details, can be gleaned by the investigator. [38]

5. Challenges in Digital Forensics in Criminal Investigation System:

Research and development in the realm of digital forensics face pressing issues, including insufficient resources, coordination gaps, and an insufficient acknowledgment of its significance within the criminal justice system. Digital forensics plays a vital role in investigations and legal proceedings, upholding the principles of justice, especially in cases involving digital evidence. Nevertheless, a multitude of challenges are intertwined with digital forensics in both investigative and courtroom settings, and these challenges can present substantial hurdles in practical application. Broadly, the challenges in digital forensics can be categorized into three primary areas:

5.1 Technical Challenges

In today's era of rapid technological advancement, crimes and criminals have evolved in tandem. Digital forensics experts employ forensic tools to gather evidence against wrongdoers, while these very criminals utilize similar tools to conceal, alter, or erase traces of their activities. This countermeasure within digital forensics is known as "anti-forensics" technique, and criminals have adeptly adapted to it. Here In this section, we will concisely and comprehensibly outline some of the primary technical challenges within the realm of digital forensics.[39]

5.1.1 Data Overload: Picture having a multitude of files and messages on a computer, making it akin to finding a needle in a haystack. Digital investigators frequently encounter an overwhelming amount of information to sift through, a common challenge in digital forensics.

5.1.2 Data Security and Encryption: It's comparable to attempting to unlock a sealed box. At times, the data on a device is concealed or safeguarded by robust security measures, making access difficult. Encryption serves to uphold the privacy between two individuals, but it can also be employed by criminals for less virtuous purposes.

5.1.3 Specialists: Consider digital forensics as akin to solving a complex puzzle. It necessitates specific skills to assemble all the pieces effectively, and not everyone possesses the expertise to do so.

[38] Forensics methods and techniques *available at:* https://www.salvationdata.com (last visited on 16 Oct. 2023)
[39] Challenges in digital forensics *available at:* https://www.forensicfocus.com (last visited on 17 Oct. 2023)

5.1.4 Advancing technology: Much like video games becoming outdated, the tools employed in digital forensics can swiftly become obsolete. Investigators must stay abreast of the most recent technological developments.

5.1.5 Cyberattacks: Visualize someone attempting to break into a house to pilfer evidence. In a similar vein, criminals might endeavor to hack or tamper with digital evidence through cyberattacks.

5.2 Legal challenges

In the realm of digital forensics, the primary legal challenge pertains to the admissibility of evidence in criminal cases. This challenge is particularly relevant when it comes to the collection of evidence through search and seizure of digital equipment. During investigations, strict adherence to legal procedures is imperative when recovering, collecting, and analyzing data from digital systems.

Digital forensics, often referred to as computer forensics, addresses the legal challenge of ensuring that digital evidence is admissible in a court of law. This encompasses the legal issues inherent in the investigative process of computer forensics and the admissibility of digital evidence in court proceedings.[40]

5.2.1 Evidence preservation: it's like keeping a precious item safe. Digital evidence must be preserved carefully to make sure it doesn't get damaged or lost.

5.2.2 Data privacy concerns: think of it like a rulebook. Laws about data privacy can be complex and investigators must follow them when handling personal information. We have also fundamental right under 21 article of the constitutions.[41]

5.2.3 Case jurisdiction: in legal system, Courts are only empowered to adjudicate cases falling within their jurisdiction. The issue of jurisdiction is particularly pertinent in cybercrime cases. , data or information is located in another place or crime is committed in another location, therefore confusion arises between the cases filing jurisdiction. The jurisdiction of local courts does not cover cybercrimes committed by out-of-state offenders that affect the local territory. In such situations, extradition is the necessary process to bring the offender within India's jurisdiction.[42]

[40] Legal issues in computer forensics and digital evidence *available at:* https://www.researchgate.net/publication(last visited on Oct. 17, 2023)

[41] Indian constitution law 1950 Art.21

[42] George Raburu, Lawrence Dinga, "Legal Issues in Computer Forensics and Digital Evidence Admissibility," *international Journal of computer science and Mobile computing IJCSMC*, Vol.9 Issue. 7, July 2020 pg. 86-89

5.2.4 Resource issues: imagine trying to solve a big jigsaw puzzle, but you don't have all the pieces. Sometimes, investigators don't have the right tools or enough money to do their job effectively.

5.2.5 Credibility: think of digital evidence like a story. It needs to be reliable and believable. Sometimes, people question if the evidence is true or not.

6. Legal and ethical consideration: India had several provision or statutes relating to digital forensics for the criminal investigations. Legal field is dynamic in nature or now in advance period of technology to need some verify or analyze the provisions related to digital forensics, here are some of the key provisions and statutes relating to digital forensics in India. But there is no specific legislation make a law relation to digital forensics.

6.1 Information technology act,2000: this act, along with its subsequent amendments, is a significant law governing various aspects of digital transactions and cybercrimes. It provides for the legal framework for the investigation of cybercrimes and the collection of digital evidence.[43]

6.2 Indian evidence act,1872: this act governs the acceptance of evidence in Indian courts, including digital evidence. Section 65B [44] specifically deals with electronic evidence and the conditions for its admissibility.

6.3 The code of criminal procedure, 1973: The Code of Criminal Procedure (CrPC) serves as the procedural law governing the administration of criminal justice in India. It outlines the process of collecting and presenting evidence, including digital evidence, during the course of a criminal investigation and trial.[45]

6.4 Indian penal code,1860: various sections of the IPC deal with offenses related to cybercrimes and other digital activities. These include sections on hacking, identity theft, and online fraud.[46]

6.5 National cyber security policy,2013: while not a statute, this policy outlines the government's approach to cybersecurity and digital forensics, aiming to create a secure and resilient cyberspace evidence.[47]

6.6 The reserve bank of India guidelines: The RBI has issued guidelines and regulations related to the security and digital forensics of financial transactions and banking activities in India.[48]

6.7 The aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act,2016: this law governs the aadhaar system, which is used for digital identification and verification. It includes provisions for the security of aadhaar data and digital transactions.[49]

State-specific laws: some states in india may have their own specific laws and regulations related to digital forensics and cybercrimes.

It's essential to consult with legal professionals and authorities in india for the most up-to-date information and guidance on digital forensics and its application in criminal investigations in the court proceedings.

[43] Information technology act, 2000 (Act No. 21 of 2000) 9 June, 2000
[44] Indian Evidence Act,1872 (act No.1 of 1872)1 ss. 65B
[45]The code of criminal procedure Act, 1973 (Act No. 2 of 1973)
[46] Indian penal code,1860 (Act No.45 of 1860)
[47] Cyber laws in India *available at:* https://ifflab.org.com (last visited om Oct. 18, 2023)
[48] RBI Guideline on information security *available at:* https://arconnet.com (last visited on Oct. 18, 2023)
[49] Aadhaar act *available at:* https://uidai.gov.in (last visited on Oct. 18, 2023)

7. Future trends and direction in digital forensic:

The future of digital forensics is a dynamic and evolving field, characterized by emerging trends and directions. The rapid pace of innovation and development in this field means that new inventions and advancements are a daily occurrence. Additionally, the proliferation of Internet of Things (IoT) devices has introduced new challenges for digital forensics practitioners.

7.1 Integration into criminal investigation system

- **Legal framework:** governments and legal systems worldwide have adapted by enacting laws and regulations that govern the collection, preservation, and use of digital evidence. These legal frameworks ensure that digital forensic procedures align with due process and privacy rights.
- **Training and education:** law enforcement agencies have invested in training programs and educational initiatives to equip investigators with the skills and knowledge required for digital forensics. This includes understanding the technical aspects of various devices and staying updated with evolving technologies.
- **Specialized units:** many law enforcement agencies now have specialized digital forensic units or collaborate with specialized forensic teams to handle electronic evidence. These units are equipped with state-of-the-art tools and software to conduct comprehensive digital investigations.
- **Public-private partnerships:** collaboration between law enforcement, academia, private sector, and non-profit organizations has become crucial. Public-private partnerships foster information sharing, research, and development of innovative forensic tools and techniques.
- **Technological advancements:** rapid advancements in technology have necessitated continuous innovation within the field of digital forensics. This includes keeping pace with evolving hardware, operating systems, encryption techniques, and network protocols to effectively analyze digital evidence.
- **Artificial intelligence:**[50]The use of artificial intelligence (AI) and machine learning(MI) in digital forensics is an emerging and changing trends in the field. AI and MI technologies are being employed to enhance the efficiency and effectiveness of digital forensic investigations of various ways, like automated data analyze large volumes of data, it is especially beneficial in cases where extensive amount of digital evidence need to be inspected. They can be identifying structure, irregularity, inconsistency and connection that might be challenging for human analysts to detect. This is the most important emerging trend in digital forensics is the use of AI and MI.[51]

The use of AI and MI technology in court investigations aids in profiling suspects, understanding their actions, and discerning between legal and illegal activities. This is especially valuable in criminal investigations. Incorporating

[50] Trends of digital forensics *available at:* https://study.com (last visit on Oct. 18,2023)
[51] Future of digital forensics trends *available at:* https://ts2.space last visit on Oct. 18,2023)

natural language processing is essential for analyzing and preserving text-based evidence, like emails and chat logs. AI assists in anomaly detection within digital data patterns, simplifying the identification of potential criminal evidence. Predictive analysis with MI models can anticipate future cyber threats. Implementing AI in digital forensics streamlines evidence collection and analysis, saving time and resources, and alleviating the court system's burden. In this evolving era, digital forensics is vital for maintaining security and justice. The integration of AI and machine learning in this field offers automation, faster investigations, and the management of large data volumes.[52]

A groundbreaking development is on the horizon as an AI-powered legal assistant, known as the "robot lawyer," prepares to advise a defendant in a US court. Created by DoNotPay, this AI algorithm will function through a smartphone, offering guidance to the defendant via an earpiece during court proceedings. While this experiment showcases the potential of AI in the legal system and seeks to reduce legal expenses, it also raises ethical concerns and the possibility of AI replacing certain legal professions. The integration of AI in the courtroom is a significant step forward, but it brings with it challenges related to bias and transparency.[53]

China has been at the forefront of "Internet courts" since 2017, employing AI-powered non-human judges to enable remote resolution of legal cases. These courts efficiently handle a range of disputes, showcasing AI's potential in the legal system. The introduction of AI judges promises cost savings and quicker decisions, signifying a substantial transformation in the legal arena. Countries like Canada are also exploring AI's role in legal proceedings, emphasizing the need for the legal industry to adapt to evolving expectations.[54]

6. Conclusion and suggestions

The field of advancing criminal investigation through digital forensics presents a dynamic and continually evolving landscape that holds a paramount role in modern law enforcement. The significance of digital forensics in criminal investigations cannot be overstated. In an era where digital devices and technologies are pervasive, these devices aid in the collection, analysis, and preservation of digital evidence during criminal Scrutinize. This, in turn, assists in solving crimes, prosecuting offenders, and ultimately upholding justice in the nation.

This paper outlines key highlights, including mobile forensics, network forensics, cloud forensics, voiceprint forensics, fingerprint forensics, and more, which are of great importance for investigators seeking to uncover digital evidence.

However, as digital forensic techniques progress, they also give rise to new challenges. Digital forensics finds application in various domains, with both national and international legislations encompassing digital media.

[52] Muhammad sarfraz "*cybersecurity threats with new perspectives*"

[53] Ananaya Singh, "World's First 'Robot Lawyer' will Soon Defend Human in court" Jan 9, 2023

[54] Tara Vasdani, "Robot justice: China's use of Internet Court", The *Lawyer's Daily, part of LexisNexis Canada Inc.*

However, it assumes a pivotal role within the legal field. Investigators employ digital or technological tools to gather, analyze, and identify evidence through digital forensics in a process that pertains to both civil and criminal law. The majority of cases involving digital forensics are related to criminal law, and it is predominantly used in the realm of cybercrime, intellectual property theft, fraud investigation, hacking, online banking fraud, and the illicit online sale of goods, among others.

It is crucial to uphold the integrity of digital evidence, making it an essential requirement for proficient forensic analysts. Data privacy and encryption are major concerns in the realm of cybercrime. Furthermore, the widespread use of Internet of Things (IoT) devices and the intricacies of cloud computing environments present additional challenges to investigators.

The advancement of criminal investigations through digital forensics is a vital component of modern law enforcement. Skilled professionals and innovative technologies play a crucial role in facilitating smoother operations within the criminal justice system. These advancements save time and are increasingly harnessing the capabilities of Artificial Intelligence (AI) and Machine Intelligence (MI) to enhance their effectiveness.

REFERENCES

- Innovations of digital forensics *available at*: https://www.interpol.int (last visited on oct.15,2023)
- Lawrence Williams, "what is digital forensics*? available at*: https://www.guru99.com/digital-forensics.htm (last visited on 15 oct.2023)
- DFRWS Technical Committee (DFRWS) (2001) A road map for digital forensic research: DFRWS Technical Report. DTR-T001-01 FINAL
- Scope of cyber forensics *available at*: https://forensicsciencepublicdeskindia.wordpress.com (last visited on 15 Oct. 2023)
- The Power of Cyber Forensics in Solving Crimes at *available* on https://www.salvationdata.com (last visited on Oct. 16, 2023)
- Vehicle Digital Forensics Services *available at:* https://techfusion.com (last visited on OCT. 16,2023)
- Cloud forensics and the digital forensics *available at:* https://www.appdirect.com (last visited on Oct. 16 2023)
- Mobile forensics and forensics lab *available at:* https://securityscorecard.com(last visited on 16 Oct. 2023)
- Forensics methods and techniques *available at:* https://www.salvationdata.com (last visited on 16 Oct. 2023)
- Challenges in digital forensics *available at:* https://www.forensicfocus.com (last visited on 17 Oct. 2023)
- Legal issues in computer forensics and digital evidence *available at:* https://www.researchgate.net/publication(last visited on Oct. 17, 2023)
- Cyber laws in India *available at:* https://ifflab.org.com (last visited om Oct. 18, 2023)
- RBI Guideline on information security *available a:* https://arconnet.com (last visited on Oct. 18, 2023)
- Aadhaar act *available at:* https://uidai.gov.in (last visited on Oct. 18, 2023)
- Trends of digital forensics *available at:* https://study.com (last visit on Oct. 18,2023)
- Future of digital forensics trends *available at:* https://ts2.space last visit on Oct. 18,2023)