VOLUME 2 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

UNDERSTANDING THE ISSUES OF SCIENTIFIC EVIDENCE IN DIGITAL FORENSICS

- Shivansh Gupta[1]

ABSTRACT

Numerous Scholars predicted that perhaps the 21st century will bring in a great technological revolution around the world. If we look at all this carefully, we could see that those scholars were correct: we are indeed living in the digital revolution era. Transitions in technological improvements have transformed human civilization throughout history and now have continued to move it further.Experts have historically argued whether technology is a blessing or indeed a burden. Some see it as a blessing, as the digital era has undeniably transformed many people's lives and jobs. The digital world, on the other hand, has generated problems for those who see it as a curse. The worrisome surge in cyberattacks has now become a major area of concern for cyber experts, since the digital world's technological advancements bait more criminals, making it harder for our legal system to keep track of it. Since we humans have become so dependent on technology, a significant surge in the cyber or digital criminal actions was supposed to follow the stratospheric surge in the usage of information and communication technologies by nearly every individual in countries today. In the past, Digital forensics specialists had to deal with much more difficult obstacles when looking for digital evidence in the case. Several technical solutions are available to assist authorities in their search for evidence however, present problems in digital forensic investigations do exist. Authorities must follow the established legal processes while retrieving and analysing data via electronic devices in order for digital forensics to be lawfully admissible as evidence. Digital forensic technologies developed well before the period of digital forensics are usually obsolete and incapable of assessing the tactics employed in some kind of information systems investigation. The legislation's struggle to keep up with the technical changes could restrict any use of digital forensics evidence in legal proceedings in the future. This research paper aims to analyze a few of the legal problems of

[1] Student at VIPS Delhi

the digital forensics inspection process, even the validity of electronic evidence in legal proceedings of law, and also the problems that an evidence collection investigator faces.

Keywords: -

Digital forensics, Law, Technology, cyber, evidence, digital crime

INTRODUCTION

Digital forensics, commonly referred to as computer forensics,is just a process of determining a scientifically examine approach for cybersecurity threats and offences. In the present age of digitalization, it is indeed a fundamental requirement both for legislation and commerce.Digital forensics is a branch of locating, conserving, inspecting, and analysing digital data while verifying techniques and presenting that electronic evidence at trial to answer some legal concerns about crimes and assaults[2]. It is indeed a technique for locating evidence on electronic content such as a computer, smartphone or wireless gadgets, websites, or the internet. This provides the investigative section with advanced techniques and services to help them fix challenging electronic cybercrimes. The computer forensic staff will support the team of investigators in analysing, inspecting, identifying, and preserving potential data stored on various electronic devices. In a nutshell, digital forensics is the art of combining science and law to solve legal issues.It implies that digital forensics probes must adhere to strict guidelines which take into account industrial and organizational standards along with applicable legislation. Since many judicial systems around the globe are precedent-based, cyber forensics detectives follow a set of processes while gathering and reviewing potential data in an effort to avert legal difficulties while submitting relevant proof at trial. Virtual or technological offenses, especially throughout the internet have grown commonplace. They leave a web presence, break laws and produce fresh guidelines for the criminal justice system, lawyers, and security officers as well as legal teams. In the matter entitled *Bharat Jatav v. State of Madhya Pradesh*,[3] Justice Anand Pathak of the Madhya Pradesh High Court raised certain serious digital forensics hurdles, by stating that: -

"*Forensic Sciences does not mean only DNA report or Blood Sampling or FSL report as it goes much beyond and if we wish to march with time, then Society and State agencies have to be well equipped with technologies. When Artificial Intelligence, Robotics, and Drone*

[2]PriyaPedamkar, what is Digital Forensics? | Types of Digital Computer Forensics, EDUCBA. Available at: <https://www.educba.com/what-is-digital-forensics/> [Accessed 16 February 2022].
[3]Bharat Jatav v. State of Madhya PradeshMCRC NO.17346 of 2021

Technologies are knocking at the doors, then policymakers or stakeholders cannot place the "Rule of Law" or "Adjudication Process" at the mercy of archaic method of investigation and prosecution. Police investigation and prosecution in Courts cannot lie at the altar of statement of witnesses alone but it should be based upon a scientific way of investigation and Police Officers, Public Prosecutors, and Trial Judges ought to be well equipped with the subjects and tools of Forensic Sciences."[4]

Digital forensics has evolved into a critical tool for detecting and resolving computer-assisted and other types of crime. However, when it comes to actual execution, such digital intelligence investigative methodologies confront a number of obstacles.

The issues in computer forensics can indeed be classified into three categories, as per Fahdi, Clarke, and Furnell (2013) that are: -

- Technical Challenges
- Legal Challenges
- Resource Challenges

TECHNICAL CHALLENGES

Electronics are becoming much more common around the world culture, and their structure, design, performance, and purpose continuously developing as a result. As whenever technologies progress, the overall crime incidence grows in parallel, since it is so widely available that anyone can take advantage of it. Emerging innovations give rise to new sorts of cybercrime.Professionals in computer forensics apply investigative techniques to gather proof against perpetrators. Nevertheless, it is not fair to say that only ethical digital forensics experts are always updated with new technologies; As technology advances, criminals are also becoming cleverer, by adopting anti-forensic measures.Anti-forensics tactics are instruments used by cybercriminals to hide, distort, or remove the records of committed crimes. Anti-forensics is indeed a practice that is viewed as a big issue in the realm of digital forensics.

Anti-forensic methods include encryption, data concealment in storage space, and the covert channel. Whereinencryption is a method of scrambling data. Only an authorised individual with the encryption credentials to decrypt the data records could decrypt and obtain the

[4]Sharma, D., Sharma, D. and Sharma, D., 2022. MP HC | Much to be done in the field of Forensic Sciences and its use in Administration of Justice and Legal Education; Court draws attention towards pendency of matters | SCC Blog. SCC Blog. Available at: <https://www.scconline.com/blog/post/2021/09/07/forensic-sciences/> [Accessed 16 March 2022].

details.[5]Perpetrators can utilise this to disguise their heinous actions and critical information about them.

These perpetrators generally employ program code and applications to suppress bits of data within the memory mechanism in an unseen format.Also discussing about covert channel, it is indeed a telecommunication application that provides an intruder to get around security mechanisms and conceal information on the network. This is exploited by the perpetrator to hide his access to the hacked machine. When it comes to technical problems in digital forensics, there are plenty more issues than these three, such as cloud-based actions, achieving data, absence of expertise and skills, steganography, and so on.

LEGAL CHALLENGES

In the sphere of law, digital forensics serves a critical part. It is because the sources of proof gathered throughout the investigations are used by the court of law. This proof can be relevant to either civil or criminal law, but it is usually tied to criminal justice. In addition, digital forensics is often employed in matters of theft of intellectual property, labor conflicts, insolvency probes, and scam inquiry, among other things.[6]

As we saw previously, there are technical problems associated with advancements in computer forensics similarly there are legal challenges that might often outnumber the other challenges. Such as there are numerous cases in which the current legislation takes a cautious approach and therefore does not recognize each part of digital forensics, also sometimes presenting potential data is much more challenging than collecting it. For most circumstances, the cyber police department misses the essential data to qualify as well as the ability to detect a potential origin of proof. Digital data frequently confronts the law because of its authenticity, where the lack of adequate standards and the lack of adequate justifications of the facts and gatherings results in the case being rejected.[7]

Several judicial frameworks around the globe limit court's ability to hear disputes which come under their jurisdictions. In cases that involve computer forensics, the criminal perpetrator's jurisdiction might vary from the legal authority where the necessary data is

[5]Official Blog of E-mail Examiner Software. 2022. Challenges Facing in Digital Forensic Evidence Finding Process. Available at: < https://www.mailxaminer.com/blog/current-challenges-in-digital-forensics-investigations/#:~:text=%20The%20different%20challenges%20faced%20in%20digital%20forensics,Blockchain%20Revolution%207%20Ransomware%208%20Cloud-Based%20More%20 > [Accessed 16 March 2022].
[6]IlakkiyaKamaraj,Enhelion Blogs. 2022. Role of Digital Forensics in Law - Enhelion Blogs. Available at: <https://enhelion.com/blogs/2020/11/20/role-of-digital-forensics-in-law/> [Accessed 18 March 2022].
[7]CISO MAG | Cyber Security Magazine. 2022. Challenges and Applications of Digital Forensics. Available at: <https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/> [Accessed 18 March 2022].

stored. In order to be fully acceptable, electronic evidence should comply with the recognized legal norms of evidence in a given jurisdiction.

Talking about privacy, which is a fundamental human right, can indeed be complicated in digital forensics. Most countries' privacy rules, especially article 12 of the UN Declaration on Human Rights, acknowledge the right to privacy, that safeguards persons from unjustified searches and seizures. Because search and seizure are the very first step in a computer forensic examination, a poor technique might have a damaging effect on the evidence's validity. As a result, forensics experts must check that they do not trespass on the accused's privacy throughout their searches and also that appropriate legal procedures are in place in addition to a court order.

Digital data is inherently delicate and can quickly lose its worth if it is not acquired, stored, and safeguarded properly and promptly. This can be easily deleted or edited with a single tap. As a result, it is critical that data protection be handled immediately in the process of investigation. To really be credible, the investigation team had to be able to display in court that the data had not been tampered with in any manner and it can be relied to be genuine. There are much more concerns that are being litigated, but only some of them have been mentioned above.

RESOURCE CHALLENGE

Since digital forensics is much more vulnerable than tangible proof, this could rapidly disintegrate as the amount of crimes rises. As a result, the duty of analysing such a vast amount of data falls on a digital forensic specialist. Forensic professionals utilize several techniques to assess the legitimacy of the data in order to make the investigation process faster and more vulnerable, but interacting with all these instruments is a barrier in itself. Below are some of the resource constraints that have been highlighted.

Such as technological advancements, learning digital data has become much more challenging due to sudden changes in technology such as computer systems, software systems, and equipment. The latest models of the operating system really aren't supported by earlier models, and software engineers have not provided any primitive adapters, which have legal implications.

Coming upon copying and quantity, digital papers security, accessibility, and validity are all simply exploited. Broad networking, as well as the web, combine to build a global platform

that enables information to be transferred across territorial limits. The convenience with which people may communicate and the access to digital documents has increased the quantity of information, making it more complex to identify genuine and useful material.

LAWS RELATED TO DIGITAL FORENSICS IN INDIA

The Indian government has adopted a number of laws that allow digital evidence to carry out their tasks with specific privileges in order to reduce the occurrence of electronic crimes. The Indian Evidence Act of 1872 and even the Information Technology Act of 2000 contain the primary laws governing digital forensics. Some of the laws have been discussed below: -

Digital data have been added to the concept of "Evidence". The term "Documentary Evidence" has indeed been expanded to embrace all documents provided for court review, even electronic information evidence is defined under section 3 of the Evidence Act of 1872.[8] Digital shreds of evidence can be used instead of documentation. According to section 4 of the Information Technology (Amendment) Act, 2008.[9]

The IT Act defines "data, document or information produced, picture or audio preserved, obtained or sent in a digital system or microfilm or computer- generated microfiche. The term "admission" i.e in section 17 of the Indian Evidence Act has been broadened to incorporate any verbal, photographic, or digital remark that implies a conclusion to almost any truth at dispute or of consequence.[10]

The Indian Evidence Act has been amended to include a fresh provision i.e section 22-A that addresses the admissibility of spoken proof concerning the information of digital data. Oral statements about the facts of digital data are not essential until the authenticity of the digital data obtained is in question, according to the law.

The Indian Evidence Act sections 65-A and 65-B lay out the requirements for digital reserves to be admissible. Section 65-A stipulates that the information of digital data may indeed be verified in compliance with section 65-B's provision. Section 65-B states that, quite apart from the evidence act, any data included in an electrical gadget is presumed to be a

[8]Legislative.gov.in. 2022. The Indian Evidence Act, 1872 |Legislative Department | Ministry of Law and Justice | GoI. Available at: <https://legislative.gov.in/actsofparliamentfromtheyear/indian-evidence-act-1872> [Accessed 19 March 2022].
[9]Bcasonline.org. 2022. Information Technology (Amendment) Act,2008. Available at: <https://www.bcasonline.org/Referencer2015-16/Other%20Laws/information_technology_act_000.html> [Accessed 19 March 2022].
[10]Linkedin.com. 2022. Electronic Evidence/ Digital Evidence & Cyber Law in India. Available at: <https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali-/> [Accessed 21 March 2022].

documentation and is acceptable without further proof of the original production if the terms imposed forth in section 65-B are met.[11]

Electronic data is defined just like any data of evidentiary significance that is kept or communicated in digital format and comprises computer proof, audio files, video data, mobile phones, and electronic mail, according to section 79A of the IT (Amendment) Act, 2008. This also allows the central administration to nominate any central or local government body or organization as an inspector of digital evidence.[12]

CASE LAWS OF DIGITAL FORENSICS

In the case of *Amitabh Bagchi v. Ena Bagchi*,[13]the jury concluded that an individual's actual appearance in court is not essential for the aim of actually presenting testimony and that the same could be accomplished using virtual meetings, but with proper precautions. Section 65-A and 65-B deal with proof associated with electronic data and their validity, and video calls are included in the term of electronic data.

In *BodalaMurali Krishna v. Smt. BodalaPrathima*[14]the court opined that "The amendments carried to the Evidence Act by introduction of Section 65A and B are in relation to the electronic record. Sections 67A and 73A were introduced as regards to proof and verification of digital signatures. As regards presumption to be drawn about such records, Sections 85A, 85B, 85C, 88A, and 90A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and digital signatures, as admissible pieces of evidence. It is no doubt true that the recording of evidence through the process of video conferencing is not specifically referred to in these provisions."

As far as if in the case of *The State of Maharashtra vs Dr. Praful B. Desai*[15]the Apex court stated that video calls are a scientific and technological innovation that allows people to view, listen, and chat with those who are not physically available with about the same warmth and convenience as if they had been. The judicial necessity for the witness's attendance doesn't really imply real attendance. The court granted video calls for witness investigation and stated that there is no justification why video calling for witness examination should never be an important element of digital data.

[11]Ibid
[12] Ibid 8
[13]Amitabh Bagchi v. EnaBagchi, AIR 2005 Cal 11
[14]BodalaMurali Krishna v. Smt. BodalaPrathima, AIR 2007 AP 43
[15]The State of Maharashtra vs Dr. Praful B. Desai, AIR 2003 SC 2053

In the case of *Dharambir vs Central Bureau of Investigation*[16] the court determined that when section 65-B refers to a digital form generated by a computer, it also refers to a harddrive on which data was saved, was previously preserved, or is currently being kept. There are two stages of a digital database, according to it. One would be the hard drive, which once used, creates a digital database of data about the modifications the hard drive has undergone, material that can be retrieved from the hard drive using a software programme. The live searchable data stored on a hard drive in the format of a text document, audio file, video clip, or even other media is another level of digital records. Accessible data could be transferred or duplicated to some other magnetic or digital equipment, including a CD, Pendrive, or similar technology. Even an empty hard drive with no data that may have been used for storing data could be replicated by creating a clone or mirror image.

In one of the landmark judgements *State (N.C.T. Of Delhi) vs Navjot Sandhu,*[17]This case concerned the validity and verification of mobile phone call logs. While examining the offender's appeal for targeting parliament, the guilty argued that the mobile phone call data could not be relied upon because the prosecution had omitted to present the appropriate certification under section 65-B (4) of the evidence act. The Apex court determined that cross-examination of a capable witness familiar with the computer's operation during the relevant period and the method wherein the call logs printouts were collected was adequate to establish the phone logs.

FLAWS OR LOOPHOLES IN DIGITAL FORENSICS

There are many loopholes at present associated with digital forensics of which some are listed below: -

VALIDITY AND RELIABILITY OF SCIENTIFIC EVIDENCE

Lack of science-based surety, inadequate study due to limited assets, lack of an ethical code, absence of specialist's credentials, total lack of data sets, and non-availability of inaccuracy percentage facts for all strategies are among the variables that undermine the validity of scientific proof in India.[18]

SHORTAGE OF SPECIALISTS

[16]Dharambir vs Central Bureau of Investigation, 148 (2008) DLT 289
[17]State (N.C.T. Of Delhi) vs Navjot Sandhu, AIR 2005 SC 3820
[18]Ojp.gov. 2022. Available at: <https://www.ojp.gov/pdffiles1/nij/grants/231977.pdf> [Accessed 24 March 2022].

As per estimates, India has only 0.33 forensic professionals for each and every 0.1 million inhabitants, who are responsible for investigating crimes sites and generating conclusions. Nevertheless, the demographic rate of forensics experts in other nations varies based on the burden of criminal cases in multiple nations, ranging from 20 to 50 experts per 0.1 million residents.[19]

VARIOUS LAWS

There is an absence of a particular piece of regulations that encompasses all of the laws pertaining to forensics.

HIGHER NUMBER OF PENDING CASES

The current situation of outstanding matters in 2021 is really no different; 0.7 to 0.8 million matters are projected to be unresolved in India's forensic labs. In such conditions, India's recommendation rate to FSLs is around 10-12% of overall crime reported in multiple areas. This number illustrates not only the lack of infrastructure, as well as the administration's inability to create revolutionary rules that allow disputes to be resolved quickly.[20]

EXPERTISE OF SPECIALISTS

The widening information barrier is yet another potential danger to digital forensics. In a brief span of time, forensic science has advanced dramatically. As a result, there is an immediate need for us to improve their skills of those presently working in this industry to guarantee that they have the experience and skill to conduct forensic studies using the most up to date digital technology. The expertise gap will function as a major constraint to the effectiveness of developing new digital instruments if learning is not prioritised[21].

CONCLUSION

Science has progressed to the point that it may provide significant benefits to its clients in a variety of ways. Perpetrators, on the other hand, employ tech for heinous crimes like fraud, extortion, virus attacks, and so on. As a result, digital forensics serves as the main method to aid in the prevention of cyberattacks by identifying them and serving as proof. As a result, it

[19]Sciencedirect.com. 2022. FSIR | Forensic Science International: Reports | Vol 3, July 2021 | ScienceDirect.com by Elsevier. Available at: <https://www.sciencedirect.com/journal/forensic-science-international-reports/vol/3/suppl/C> [Accessed 25 March 2022].

[20] Ibid

[21]Moore, S., 2022. Challenges in Digital Forensics. News-Medical.net. Available at: <https://www.azolifesciences.com/article/Challenges-in-Digital-Forensics.aspx> [Accessed 31 March 2022].

is extremely important in the legal world. It aids in the detection and prosecution of cybercriminals. It also encourages other businesses and organizations to safeguard their sensitive data. There have been nevertheless, substantial legal considerations that forensic experts must address. Failing to follow the legal requirements governing the collecting and use of forensic data can render the information useless and lead to this being found unacceptable in court, as well as expose examiners to responsibility in lawsuits and testimony. To address the aforementioned difficulties, we need a particular nationwide rule that applies to everyone who is participating in or engaging with such a digital forensic procedure, or who provides any service, instrument, or programme that is used for purposes of research. Current law and also proposed laws established to bridge this issue must be regularly updated to account for evolving developments in modern technologies and also educating court and enforcement agencies officers entrusted with arbitrating matters using digital data. Learning must involve all basic and specialized elements. Without a question, digitalization will continue to advance. As a result, a well-planned digital evidence approach would certainly aid in the prevention of future cybercrimes.