THE ADMISSION OF DIGITAL EVIDENCE AND ITS VALIDITY IN THE COURT OF LAW

Author: *K. Pramod Kumar Reddy, III year of B.A.,LL.B.(Hons.) from Alliance University, Alliance school of Law, Bangalore, Karnataka.*

Co-author*: Mutaman Amir Ahmed Abdullah, III year of B.A.,LL.B.(Hons.) from Alliance University, Alliance school of Law, Bangalore, Karnataka*

ABSTRACT

Law enforcement is constantly competing with criminals in the use of new technology, requiring the advancement of technologies to scan digital devices for relevant information in a cohesive manner. Another, even more important, aspect of this race is the development of a modern forensics approach that incorporates the forensic study of all types of digital crime scene investigations. When an offence involving an electronic device, such as a smartphone, is brought to a criminal court, the defence must establish a technique to assert beyond a reasonable doubt that the suspect is guilty of the crime. As the information and communications infrastructure market progresses, digital evidence is becoming more relevant in legal proceedings. Since cybercrimes and computer-facilitated crimes are increasingly transnational, the digital forensic process and digital evidence handling must be streamlined to ensure that the digital evidence collected is admissible in legal proceedings. The transnational admissibility of digital evidence is further complicated by the differing legal views on evidence in various jurisdictions. This technique is largely reliant on the findings of the forensic analyst or Digital Forensic Investigator, who is tasked with looking for traces of evidence in the exhibits. This paper provides an analysis of digital evidence, as well as specific challenges related to digital evidence, major types of evidence in the legal system, the enforceability of digital evidence in the judicial system, and how evidence is represented in the courtroom.

Keywords: Digital Forensic, Digital Evidence, Admissibility, Challenges, Judiciary.

INTRODUCTION

The world is advancing towards the digital era where the internet has become a big necessity in the everyday lives of people, with the increase in users, the internet has become a place where people can get a different kind of things for their purpose or work (either in the positive form or in the negative form). Because of that many users, the internet has provided cyberspace with the help of IT (Information Technology) to allow those internet users to grow. With the help of that cyberspace, people have become more dependent on the internet. When this came up in the big picture a lot of users of the internet used cyberspace to commit wrongs like hacking and many more.

To prove these kinds of crimes which are done on the internet, the investigation has to be done, but clearly, it can't be done physically, so it means it needs to be done on the computer on which that crime has been committed and that evidence has to be submitted in the court and even those can't be submitted physically, so even the evidence has to be presented digitally in front of the court. There have been many thoughts on, what if those pieces of evidence are distorted and are then presented in the court of law. To prevent this kind of issue the court has come up with different procedures to validate those evidence for admitting those evidence in the court of law. A few of those for validating are expert opinion, etc. For all of these being included the Indian Evidence Act, 1872, and Indian Penal Code, 1860. The Indian Evidence Act, 1872 is amended on different things such as admissibility, expert opinion, etc. on digital evidence, and the Indian penal code, 1860 is amended on penalties and punishments on the distortion of that digital evidence. But now, digital evidence is not only used for cyber-related crimes but is also in normal cases. Some of those are CD, Recording, Digitally written statements, etc., and many more. Right now the investigation on this kind of digital crimes has exposed many cases within the Indian Territory

DIGITAL FORENSICS

Before we get into the evidence part we need to understand the meaning of Digital forensic[1]. Digital forensics is a branch of the forensic sciences that deals with the investigation and

[1] Legalserviceindia.com. 2021. *Future of Digital Forensics in India: An Analysis*. [online] Available at: <http://www.legalserviceindia.com/legal/article-4896-future-of-digital-forensics-in-india-an-

recovery of evidence of a crime that is done in cyberspace or on any other digital platform. The Forensic is now extended even to Civil cases. The discipline has emerged completely in the 21st century. This discipline is used to refute the hypothesis in the court of law which is in support of the case. Digital forensic is divided into different parts:

1. Computer Forensic.
2. Mobile Forensic.
3. Network Forensic.
4. Data analysis Forensic.
5. Database Forensic.

1. **Computer Forensic:** This kind of forensic is done to investigate computers, embedded systems, static memories, etc. The origin of this kind of forensic was in the 2006 case of Sharon Lopatka of northern California where the killer's torture and death fantasies were recorded on the email of the killer.

2. **Mobile Forensic:**

The forensic investigation in mobile is done on communications, location, etc. For example, in the case of the murder of Meredith Kercher, the accused Patrick Lumumba was punished after the investigation in his mobile revealed SMS Data, which was used against the accused to convict him and punish him for the murder.

3. **Network Forensic:**

This type concentrates on monitoring and collecting network traffic on the computer for information relating to a cyber-crime.

4. **Data analysis forensic:**

This forensic is conducted when a crime is related to financial fraud, where this analyse and examine structured data.

analysis.html#:~:text=Digital%20Forensics%20is%20defined%20as,
phone%2C%20server%2C%20or%20network.>

5. **Database forensic:**

Examining done on databases and metadata, to recover relevant information.

DIGITAL EVIDENCE

The information or confidential data stored on a computer or electronic device that was obtained by a law enforcement agency as part of a criminal investigation is known as digital evidence. Indian courts have established legal precedents on the use of electronic proof as a result of the reform of the law. Judges have also shown an understanding of the inherent "electronic" existence of testimony, with insight into its admissibility and the application of the statute about how electronic evidence should be brought and filed before the court.

E-crime (Electronic Crime), such as credit card fraud or child pornography, is often associated with digital evidence. In a court of law, forensic responders may use records processed or transferred in binary form on a computer hard disc, a cell phone, or some other electronic device as digital evidence. This material could include the suspects' emails or cell phones, which could be crucial in determining their motive and whereabouts at the time of the crime, as well as the searches they conducted on search engines like Google or YouTube.

There are two types of digital evidence:

1. Non-persistent, or volatile memory: Memory that loses its content when the power is switched off, such as data contained in RAM (semiconductor storage).

2. Non-volatile, i.e., material that does not alter when the power is switched off. Data on a disc, hard drive, CD/DVD, and ROM, for example. Any computer or system that records data, including several modern home gadgets like video game consoles, GPS sports watches, and internet-enabled systems used in home automation, can be searched for the digital proof. Internet searches using open-source intelligence are often used to locate digital documentation (OSINT). Any data file created on an electronic computer is considered digital evidence.

Email, text messages, instant messages, data and records recovered from hard discs, electronic bank transfers, audio and video files are all examples of this. Admissible, true, total, credible, and convincing are the five laws to follow when collecting digital data. Furthermore, there are several forms of digital evidence and those types of evidence can be found: Internet-based, stand-alone computers or devices, and handheld devices.

PROVISIONS RELATING TO ELECTRONIC EVIDENCE

The Indian Evidence Act of 1872 defines evidence as, a) witness testimony, which includes oral testimony, b) photographic evidence, which includes electronic records created for the court's inspection. The term "all documentation produced for the inspection of the Court" was replaced with "all documents including electronic data produced for the inspection of the Court" in Section 3 of the Act. In the case of documentary evidence, the terms "content of papers" have been replaced by "content of documents or electronic archives" in Section 59, and Sections 65A and 65B have been added to incorporate the admissibility of electronic evidence[2]. Traditionally, the general rule of proof has been that straightforward oral evidence, except for records, can be used to prove any facts. As per Section 2(t) of the Information Technology Act, 2000, the wider connotation has been given to an electronic record. Sec 2(t) defines electronic record' as meaning, "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfilm"[3].

The hearsay law states that any oral evidence that is not direct cannot be counted upon until it meets one of the exceptions outlined in sections 59 and 60 of the Evidence Act. In the case of letters, though, the hearsay rule is not as rigid or as clear as it is in the case of oral testimony. Since oral testimony cannot prove the contents of a text, and the document speaks for itself, this is the case. Therefore, if a document is missing, oral testimony cannot be provided as to the validity of the document, and it cannot be matched with the contents of the document. This is because it will violate the hearsay rule (since the document is absent, the truth or accuracy of the oral evidence cannot be compared to the document). Either primary or secondary evidence must be shown to prove the contents of a text.

[2] Dubey V (2017), "Admissibility of Electronic Evidence: An Indian Perspective", Forensic Research & Criminology International Journal, 4(2) 2017.
[3] NCJRS: Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors,2007

Although primary proof of the record is the document itself, it was recognized that there may be circumstances in which primary evidence would not be usable. Thus, to demonstrate the contents of a document, secondary evidence in the form of authenticated copies of the document, copies produced through mechanical methods, and oral accounts of anyone who has seen the document are allowed under section 63 of the Proof Act. As a result, the clause allowing secondary evidence dilutes the hearsay rule's values and is an attempt to reconcile the complexities in ensuring the production of documentary primary evidence while the original is unavailable. Section 65 of the Proof Act specifies when primary evidence of the record is not required, and secondary evidence - as listed in section 63 of the Evidence Act - can be offered. This includes situations when the original document:

1. Is a collection of several documents.
2. Or has been proved by the prejudiced party itself or any of its representatives.
3. Is lost or destroyed.
4. Cannot be easily moved, i.e. physically brought to the court.
5. Is a public document of the state.
6. Can be proved by certified copies when the law narrowly permits.

CHALLENGES[4] ON ADMITTING THE DIGITAL EVIDENCE BY THE INDIAN JUDICIARY

1. A question raised, asking what if the digital evidence is damaged or tampered between the time of when they were found or created to the time of being presented in front of the court of law.
2. The reliability of the digital evidence that is generated by the computer and social media.
3. There can be an identity crisis over the person who wrote a message digitally. For example, A is the person who wrote an email or SMS in a dispute, there is no sufficient evidence to prove that he is the one that wrote the Email or SMS.
4. Let us assume an act was carried where it was recorded, but the person who recorded the act has failed to prove that evidence where the person who is played with is the same person related to the case.

[4] Monir M. (2013), Textbook on The Law of Evidence, (9th ed.) Universal Law Publishing.

5. Not being able to prove the person that has allegedly clicked or used the pin or I accept button as the same person that has acted.
6. Data that is retrieved from the Internet is thought of as a problem. As the data from the internet might be not reliable as the evidence can be an intercepted evidence. Another issue is if the information on the cloud is situated in the different jurisdiction of another court, then the evidence should be dealt with by that local jurisdiction.
7. When evidence needed to be obtained from an online database where the data is constantly updated on the time to time basis.
8. The author of a post on social media is a problem to find that person, as that post amounts to a crime. The author of the post is difficult to find as social media has a lot of people as the author who may write on the same thing as the author. So, it will be hard to find the identity of the author.

SUGGESTIONS ON RESOLVING THE CHALLENGES ON THE ADMISSIBILITY OF DIGITAL EVIDENCE

To allow the use of electronic records, the Evidence Act also allows for such presumptions. The court shall assume that any electronic document purporting to be an agreement (containing the parties' electronic signatures) was signed by affixing the parties' digital documents, by Section 85A of the Evidence Act. Similarly, until the opposite is proved, Section 85B of the Evidence Act requires the Courts to assume that the protected electronic record has not been changed after the precise point in time to which the secured status refers. Furthermore, Section 85C of the Evidence Act establishes an assumption as to the authenticity of information found in an electronic signature certificate, while Section 81A establishes a similar presumption for electronic Gazettes.

In addition to electronic records being used as evidence, there has been an increase in the use of electronic media in judicial proceedings for other purposes. Although acknowledging the benefits of social communications such as emails and WhatsApp texts, etc…In commercial litigation and litigation where interim relief is sought, the Supreme Court has encouraged parties and their attorneys to represent the opposing party by email in addition to the regular modes of operation. The Hon'ble Bombay High Court has taken a similar position. Also, service via

WhatsApp has been acknowledged by the Hon'ble Delhi High Court and the Hon'ble Bombay High Court in recent times. To address the problems[5], we need a clear national regulation that applies to anyone that is interested in or deals with a digital forensic investigation, or who provides some service, tool, or programme that is used for investigation purposes. Businesses that manufacture equipment for digital forensic examination must have proper instruction manuals with a thorough description, pros, and cons about the tools, and investigating departments must conduct training and learning programs with their digital forensics officers so that they are familiar with new technology[6]. When experts see an outdated smartphone model or an old operating machine on the crime scene, the mobile or software development providers must have updates relating to outdated technologies so that experts can quickly review and retain data for proof purposes. During an inquiry, investigating offices must still exercise caution.

CONCLUSION

Courts could also determine whether digital evidence was tampered with before, during, or after collection, as well as the reliability of the mechanism that produced it. Virtual investigators may be called to the stand to testify about the original evidence's authenticity, as well as the compilation and processing mechanisms and procedures, as well as to claim that they developed the chain of custody and forensically maintained the records. Proof may be excluded where there is an unexpected breach in the chain of custody. To draw sound conclusions and defend those conclusions and the related facts on the stand, an understanding of the major categories of evidence mentioned above is needed. A digital investigator's findings and evidence may be harmed by a lack of understanding of these principles. At the end of the day, digital prosecutors would deliver their conclusions to a non-technical jury in court. The secret to the success of any presentation is planning, preparation, and more practice. To discuss critical topics, be familiar with all facets of the situation, foresee questions, rehearse responses, and plan visual presentations. While this may take time and effort, bear in mind that someone's liberty could be at risk.

[5] Fahdi, M.L. Clarke, N.L. Furnell, S.M. (2013). Challenges to Digital Forensics: A Survey of Researchers Practitioners Attitudes and Opinions. [Online]. P 1. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6641058 [Accessed 06/22/2017]

[6] Casey, E. (2002). Uncertainty and loss in digital evidence. International Journal of Digital Evidence, 1 (2). Available from http://www.ijde.org/archives/docs/02_summer_art1.pdf

BIBLIOGRAPHY

1. Legalserviceindia.com. 2021. *Future of Digital Forensics in India: An Analysis*. [http://www.legalserviceindia.com/legal/article-4896-future-of-digital-forensics-in-india-an-analysis.]

2. Dubey V (2017), "Admissibility of Electronic Evidence: An Indian Perspective", Forensic Research & Criminology International Journal, 4(2) 2017.

3. NCJRS:Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors,2007

4. Fahdi, M.L. Clarke, N.L. Furnell, S.M. (2013). Challenges to Digital Forensics: A Survey of Researchers Practitioners Attitudes and Opinions.[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6641058 [Accessed 06/22/2017]

5. Monir M. (2013), Textbook on The Law of Evidence, (9th ed.) Universal Law Publishing.

6. Casey, E. (2002). Uncertainty and loss in digital evidence. International Journal of Digital Evidence, 1 (2). Available from http://www.ijde.org/archives/docs/02_summer_art1.pdf