ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE

VOLUME I AND ISSUE I OF 2023

APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2

Published by

Institute of Legal Education

https://iledu.in

ADMISSIBILITYAND PRESERVATION OF DIGITAL EVIDENCE

AUTHOR - POKALA NEHA, STUDENT AT DAMODARAM SANJIVAYYA NATIONAL LAW UNIVERSITY

Best Citation - POKALA NEHA, ADMISSIBILITYAND PRESERVATION OF DIGITAL EVIDENCE, *ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE (ILE JEVJ)*, 1 (1) of 2023, Pg. 1-7, APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2.

Abstract

Digital evidence plays an important role in today's world. Everything is related to technology, this helps us to complete our work smartly and in less time. After covid, the use of digital devices has taken a rise. However, the technology is being misused and many crimes such as credit card crime, cybercrimes, hacking, etc are increasing. All these crimes are often committed with the help of systems or digital devices, due to which the judiciary has also identified the need for accepting the digital device as admissible evidence. One must remember that digital evidences can easily be tampered, so they require special care in preserving and collection of digital evidences. This article contains the steps taken by the judiciary to make the digital evidence admissible in court of law, importance of digital evidence, need for preservation of digital evidence, types of digital evidence, changes brought in Indian Evidence Act and Information Technology Act and landmark judgments relating to admissibility of digital evidence. Section 65B of Evidence Act deals with the admissibility of evidence. Now a days, almost every public place has Camera's and even in residential areas also people are fixing cameras for safety purposes. Mobile phones are one of the important evidence to know the details about the individual, details of those persons whom the individual is meeting, talking, chatting. Mails, messages, CC Tv footage, DVD, CD, etc are important digital evidences. Admissibility of digital evidence will helps the police to fasten the process of investigation and courts to deliver the justice quickly. Preservation of digital evidence plays an important role in making the evidence admissible in court. The article mentions the steps which are required to preserve the digital evidences.

KEYWORDS - Digital Evidence, Admissibility, Preservation, Indian Evidence Act, Information Technology Act

I. Introduction

Technology plays an important role in today's world, and government has taken steps to digitization. The use of digital technology has became a necessity. The use of technology is definitely a gift for development, however, the technology can also be misused and it is being used for the purpose of committing the crimes. digitization helps the investigation process. Digital evidences are volatile in nature and can easily be tampered, deleted, destroyed. There is a need to preserve the digital evidences in a proper environment, so that the evidences can be accepted in the courts. Judiciary and legislature has identified the need for making the digital evidence admissible in court of law. Most of the digital evidences are only corroborative piece of evidences but not substantive piece of evidences.

The concept of admissibility and preservation of digital evidence plays an important role in today's world in solving the crimes and delivering the justice. It is important to note that the digitization has a huge impact on man kind and it helps in the process of investigation. I choose this topic to understand the importance of admissibility of digital evidence, to know the importance of preservation of digital evidence,

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME I AND ISSUE I OF 2023
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

to analyze the sections relating to admissibility of digital evidences and to analyze the case laws relating to preservation and admissibility of digital evidence. In this article I will explain about the digital evidences, types of digital evidences, admissibility of digital evidence, preservation of digital evidence, case laws which explains about the admissibility and preservation of digital evidences.

II. Digital Evidences

Section 3 of Indian Evidence Act defines evidence as oral, documentary, primary, secondary type of evidences. Oral evidences are the evidences which are oral in nature, documentary evidences are those which are in written form and includes digital evidences. Primary evidences are the evidences which are original in nature, original records. Secondary evidence means production of computer-output of the contents of the electronic record. When it becomes impossible to bring the original device, then the same can be bought before the court in the form of print out, by copying or storing in any electronic device. Primary evidences are more admissible than secondary evidences. Secondary evidences are only admissible when it fulfills the conditions prescribed under section 65B of Indian Evidence Act.

Digital evidence is defined as "information stored or transmitted in binary form that may be relied on in court." It is mainly associated with the crimes which are related to digital world such as cyber crimes, credit card fraud, etc. There are volatile in nature, so, the collection and preservation of digital evidences plays an major role and the same needs to be done carefully, by following all the precautions.

"Electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines" - Section 79A of the Information Technology Act, 2000.

Section 2(k) of Information Technology Act "Computer resource" means computer, computer system, computer network, data, computer data base or software.

- **Types of digital evidences**

Volatile evidences - memory, files, running process and network connections are considered as volatile evidences.

Non-volatile evidences - CD, DVD, Hard drives, RAM, Archive media, Cache and USB storage are considered as non-volatile evidences.

The digital evidence includes voice mail messages, database, programme, operating systems and other information stored in computer.

Computer - generated output - these are not reiterating human declarations such as Automated telephone call records, computer-enhanced photographic images, computerized test-scoring.

Computer- stored declarations - these are reiterating data that has been entered in computer such as accounting records, invoices, charts, graphs, and summaries.

The digital evidences which can be collected for the purpose of investigation are files, E-mails, photos, videos, web server, web history, cell phone, record of cell signal history, etc.

Evidences can be collected by using digital means such as Lie detector test or polygraph test, brain mapping test.

III. Admissibility of digital evidence

Admissibility makes the evidence collected, utilized for the purpose of serving the justice. The digital evidence which is collected through lie detector test, brain mapping test is considered as corroborative piece of evidence but not substantive piece of evidence. Illegal search and collection of evidence will not make the collected evidence inadmissible. **Section 65A of Indian Evidence Act and 65B of Indian Evidence Act**

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME I AND ISSUE I OF 2023
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

Deals with the admissibility of digital evidence. The electronic record is documentary evidence. The question arises whether call recording, voice notes and other electronic records of similar nature falls under oral evidence or documentary evidence? such type of evidences can also be converted into readable form with the help of software. So the same should be considered as electronic record as there are in binary form. A Person making a certificate under Section 65B must be a competent and capable person and must occupy a responsible official position.[1]

The electronic records are considered as valid evidence when the same was obtained from a computer when it was used to store information on regular basis, if information was given by a person who has the lawful authority over the computer, if the information is derived from other source which is regularly fed into the computer, when the computer is in working condition then electronic records are not affected, the Information is derived from such information fed into the computer in the ordinary course of the said activities.[2] These are the few conditions which are required to be satisfied to make the digital evidence admissible. Both primary and secondary type of evidences has admissible value in the court, but the value depends in the way, the evidences are being submitted to the court. If the original digital evidences are being submitted then the value of admissibility will be relatively higher than the one which are submitted by copying from the original system. If the evidence is being submitted as secondary form of evidence, then in such case the certificate under section 65B of Evidence Act is mandatory. If the evidences is in the form of audio and video recording then in such case the original recordings will have the greater admissible value and if the copied version of those recordings are submitted then the recordings must be accompanied with the certificate and must comply the conditions which are prescribed in section 65B of Indian Evidence Act.

Mobile phones are one of the significant evidences. The data of calls, emails, messages are important digital evidences. Producing mobile phone itself has more evidenciary value than submitting the copy of chats, call records, etc. With respect to admissibility of evidence in court of law, the primary evidences has more value than secondary and it is compulsory to produce a certificate proving the authenticity of the evidences, the evidence must comply the conditions prescribed under section 65B of the Act.

Section 65B(4) provides that a **certificate** attesting the following should be given: "A statement identifying the electronic record, A statement describing how the electronic record was produced, Details of the device that produced that electronic record to show it was created by a computer, Statements related to matters enumerated in Section 65B(2) of the Indian Evidence Act, 1872, A statement stating that the subject matter of certificate is to the best of the knowledge and belief of the person stating it, Should be signed by a person having the official position of that device or management of that device." The certificate should be produced by a person, who is occupying a responsible official position. The digital evidences are volatile, latent, time sensitive, easily destructible. So, it is very important to make sure that the evidence which is being submitted in the court is real and authentic. The admissibility mainly depends upon the originality of the device submitted and the certificate which is being issued by the officer proving the authenticity of the evidence.

IV. Preservation of Digital Evidence

Digital evidences play a significant role in Criminal Justice system. Technology has become a part of our life and it helps to solve

[1] Rohan Jain, Admissibility of Electronic Record in India, Manupatra, <https://articles.manupatra.com/article-details/Admissibility-of-Electronic-Record-in-India> (Last accessed on 10 June 2023).
[2] Ajay Bhargava, Aseem Chaturvedhi, Karan Gupta, Shivank Diddi, Use of Electronic Evidence in Judicial Proceedings, Mondaq <https://www.mondaq.com/india/trials-amp-appeals-amp-compensation/944810/use-of-electronic-evidence-in-judicial-proceedings> (Last accessed on 12 June 2023).

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME I AND ISSUE I OF 2023
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

the crimes easily. However, it is well known fact that the digital evidences are volatile and can easily be tampered, destroyed. It is one of the main reasons, why initially digital evidences were not considered as admissible evidences. Preservation of the digital evidences is an crucial step, which needs to be done carefully without any negligence.

Preservation needs to be done in two stages. One is to preserve the crime scene and all the digital evidences which are present in crime scene until, the forensic department collects the digital evidences. Second stage is to preserve the collected evidence in a secured place, so that it can be submitted in competent court. After reaching to the crime scene, if the investigating officer, finds any digital evidences then the following steps needs to be followed. Do not change the current state of the device, if is on then keep it on or if it is off then leave it as it is. If devices such as mobile phones were found, then in such case keep the device in safe place and do not on the phone. Do not leave the device in unsecured place. Take the photograph of the evidence along with the plug connections, do not insert the digital evidences such as SIM card, Memory card, Pen drive in to any external device. Do not copy or delete the data. Time plays an important with respect to digital evidences, so extra precautions needed to be taken. After collecting the devices, do not put in high temperature places. If any password or fingerprint is protecting the device, then do not open the device as there is danger of losing the data.

Mobile phones, laptop, computers, cameras contain lot of details such as the places which the victim visited recently, people he or she met, call logs, messages, etc. It is necessary to protect the device. The digital evidences can be easily destructible. So, methods such as recovering the deleted data must be adopted by all the officers. Every investigating officer should take the advice of forensic expert while dealing with electronic devices.

V.Methods to preserve the digital evidence and its integrity

The methods which were used by forensic experts to preserve any evidence are drive imaging, Hash values, chain of custody.

Drive Imaging

Before analyzing the evidence from a source, the forensic experts needs to create image of such evidence. Drive imaging is a process in which an analyst will create the bit by bit duplicate image of such evidence. There are few points which needs to be seen while preserving the evidence. The deleted files can be recovered by the experts by using forensic techniques. It should be remembered that the forensic analysis should always be done on a duplicate one but not on original one.

Hash values

It is a unique numerical identifier that can be assigned to files or group of files based standard mathematical algorithm applied to characteristics of data set.[3] New hash value will be generated even if small part of data is altered, added to the original file. The hash value and other metadata will not be visible in normal life explorer window but a forensic analyzer can obtain the hash values. In order to make the evidence admissible in the court the hash value of the duplicate image needs to be same the original one. If there is change in hash value then the digital evidence cannot be accepted by the court.

Chain of custody

After collection of evidence, it is necessary to maintain the chain of custody which means documenting all the steps which were done with respect to the digital evidences. Who has the possession of such digital evidence, on what time the digital evidence has sent to the experts all should be in documentation. The steps which are included in transferring the evidences

[3] Shiv Raman, Nidhi Sharma, Digital Evidences in investigation of cyber offenses in India: An Analytical study, Volume 4 and Issue 1 of 2021, International Journal of Law management & Humanities.

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME I AND ISSUE I OF 2023
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

should be documented. The chain of custody demonstrates that the evidence is in possession since the image is created which means the evidence is preserved. Any lapses in the chain of custody will diminishes the legal value of the evidence.

If the evidence is kept unattended which means it is not preserved properly and the same will decrease the integrity of digital evidence. They needs extra care as they are fragile, time sensitive and can be tampered. The preservation needs to be done with proper care to maintain the integrity and authenticity of digital evidences and precautions needs to be taken while preserving them. The challenges faced while preserving the digital sources are the quantity of material needs to be maintained, high cost, various range of files, changes in availability of hardware, software and other software required for access.[4]

VI. Case Laws

Virendra Khanna v State of Karnataka & Anr[5]

The petitioner had filed a writ petition challenging the interlocutory orders passed by the government, in which the court ordered him to furnish his passwords of his mobile phone and to undergo polygraph test, if he fails to furnish his passwords, email passwords without hearing him or obtained consent. It was contended that furnishing of passwords is against to his right of privacy. There is no mandate under section 53 and 311CrPC which empowers the trial court and violates "article 20(3) and section 161(2) of CrPC".

The court held that the court cannot suo moto can order accused to furnish password but investigating officer can do. The need to search for mobile and laptop arises in two situations. One is when there is "**apprehension that the potential evidence**" which is present in mobile may be destroyed and in "**ordinary course of investigation**". With respect to first situation, it is futile to proceed with search warrant, but by recording the reasons for his belief the officer can proceed with the search without warrant. In second case, it is essential to have search warrant. The court further held providing passport is equivalent to providing signature, hand writing.[6] The evidence procured from mobile cannot by ipso facto proves the guilt.

The court held that it does not violates right to privacy because it falls under exception, in the process of investigation. It however set aside password order and polygraph as the same was issued without warrant and giving hearing.

Novel Guidelines for search and preservation of digital devices

- The investigating officer should be accompanied with forensic expert, the photograph should be taken of the devices including its connections and diagram should be drawn. If the system is off do not power on and if it is on do not off the system.
- The mouse can be moved if any picture appears it should be photographed. Secure the data in RAM, IP address, network connection, MAC address.
- If forensic expert is not available then unplug the laptop and pack them separately in faraday bags, remove its battery. If it cannot be done then shut down it.
- Ascertain whether the device is connected to any remote device or shared network if yes then seize those devices, routers, modems.
- Identify who is using unsecured data and collect the relevant details.
- Prevent the device from coming into contact with any network, wireless

[4] P.J. Rosario Vasantha Kumar, Preservation of E-Resources: Tools & Techniques, Archive.org, <https://archive.org/details/httpsierj.injournalindex> (Last accessed on 11th June 2023).
[5] *Virendra Khanna V State of Karnataka & Anr*, W.P.(GM-RES) 11759 OF 2020 [2021] (Karnataka High Court).
[6] Vinoy Joy, Ganapathy Subbiah, Ruha Shetty, Guidelines For Search & Preservation Of Electronic Devices In Criminal Investigations, Mondaq, <https://www.mondaq.com/india/white-collar-crime-anti-corruption--fraud/1062228/guidelines-for-search--preservation-of-electronic-devices-in-criminal-investigations-far-reaching-decision-by-karnataka-hc> (Last accessed on 9th June 2023).

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME I AND ISSUE I OF 2023
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

communication. Keep the battery full so that the data will not be lost. Remove the sim card and if power is off remove the battery, if not then put the device on aeroplane mode.

- The seized equipment must be kept in safe and in normal temperature.
- While searching, seize the electronic devices such as pen drives, DVD, Hard wares, USB.
- Keep laptop, mobile away from network and search for passwords of them as there is chance to be written in any book, place.
- The documentation must be done from time of entry and completion of search.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[7]

The facts of the case were the election of the appellant was challenged by the opposition candidate on the ground that the submission of nomination papers has happened after the cut off time prescribed by the election commission but the same was accepted by the returning officer. In order to support the contentions they relied upon the video recordings outside the office of returning officer, the same was submitted before court, it shows that the candidate has submitted after the prescribed time. The returning officer did not provide, certificate under "section 65-B(4). The question arises before High court, whether the evidence can be accepted without issuance of certificate which shows the authenticity of the evidence. By relying upon the evidences that the cameras were working properly, recording was done on daily basis, court accepted those evidences. This was challenged by appellant in Supreme court, SC upholding the **Anvar PV V. PK Basheer[8] judgment** and overruling the **Shafhi Mohammed V State of HP[9],** made it clear that the certificate must be mandatory provided as a condition under Sec65 B (4) for admissibility of electronic evidence. If the document produced is original then no need of certificate. The court issued guidelines for the ISPs (internet service providers) and the cell phone companies regarding maintenance of CD records and other records relevant for the purpose of seizure during investigation.

VI. Conclusion

Admissibility of digital evidence and the preservation of digital evidences are two important aspects, which needs to be addressed. New technology must be adopted in order to make sure the collected evidences is stored and preserved properly. Guidelines must be provided with respect to admissibility and preservation of digital evidences. Methods to preserve the digital evidences should be implemented properly. As technology is developing, digital evidences must be given importance as admissible evidences in order to make sure the justice is served quickly.

VII. References

1. RohanJain, Admissibility of Electronic Record in India, Manupatra, <https://articles.manupatra.com/article-details/Admissibility-of-Electronic-Record-in-India> (Last accessed on 10 June 2023).

2. Ajay Bhargava, Aseem Chaturvedhi, Karan Gupta, Shivank Diddi, Use of Electronic Evidence in Judicial Proceedings, Mondaq <https://www.mondaq.com/india/trials-amp-appeals-amp-compensation/944810/use-of-electronic-evidence-in-judicial-proceedings> (Last accessed on 12 June 2023).

3. Shiv Raman, Nidhi Sharma, Digital Evidences in investigation of cyber offenses in India: An Analytical study, Volume 4 and Issue 1 of 2021, International Journal of Law management & Humanities.

4. P.J. Rosario Vasantha Kumar, Preservation of E-Resources: Tools & Techniques, Archive.org, <https://archive.org/details/httpsierj.injournalindex> (Last accessed on 11h June 2023).

[7] Arjun Panditrao Khotkar V. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[8] Anvar PV V. PK Basheer, (2014) 10 SCC 473 .
[9] Shafhi Mohammed V State of HP, (2018) 2 SCC 801 .

5. Vinoy Joy, Ganapathy Subbiah, Ruha Shetty, Guidelines For Search & Preservation Of Electronic Devices In Criminal Investigations, Mondaq, <https://www.mondaq.com/india/white-collar-crime-anti-corruption--fraud/1062228/guidelines-for-search--preservation-of-electronic-devices-in-criminal-investigations-far-reaching-decision-by-karnataka-hc> (Last accessed on 9th June 2023).

6. Virendra Khanna v State of Karnataka & Anr, W.P.(GM-RES) 11759 OF 2020 [2021] (Karnataka High Court).

7. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

8. Anvar PV V. PK Basheer, (2014) 10 SCC 473.

9. Shafhi Mohammed V State of HP, (2018) 2 SCC 801.