International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 10 Issue 5, September-October, 2022, Impact Factor: 7.326

A Critical Analysis of Admissibility and Relevancy of Digital/Electronic Evidence

Nutan Rai[1], Kaustubh Thakur[2]

[1,2] BBA LLB 5th Sem/3rd Year, Kalinga University

ABSTRACT

"Innocent until proven guilty" is a basic principle of law in various democratic countries. In accordance with this, evidence is the most prominent term to get the outcome/results of particular trials or proceedings. Evidence, is a term which tries to prove a point or an element of the case to Judge or Jury. Being the duty of both prosecutor and accused to prove their parts, prosecutor has to prove that without any reasonable doubt accused has committed an offence whereas accused has to prove his point that he had not committed any offence, instead the other party is trying to implicate him. In accordance with evidences, there are numerous types of evidences, but considering today's modern era with full of technologies, specially Information Technologies, even the focuses of various countries have been shifted towards digitalization. Even, India has also shifted it's focus towards the agenda of "Digital India". This modern perspective of Digital world has enabled even legal fields to approach towards digitalization by establishing e-courts. As of courts are approaching digitalization, the repetitive question that arises regarding evidence is that whether the involvement of e-evidence or electronic record in both civil and criminal matters is admissible in the court of law or not? However, the admissibility and relevancy of e-evidence or electronic records are subjected to some conditions laid down in evidence act after the amendments made in Indian Evidence Act, 1872 and Information Technology Act, 2000. Here in this research paper, the author has tried to deal not only with the issues associated with admissibility of various types of digital evidences or electronic records (tape recorded conversations, E-mails, CD, Mobiles, etc) but also with the procedures and conditions regarding admissibility and relevancy of digital evidences in accordance of case laws and interpretations of USA, UK, and India by exploring the role of Cyber Forensics and Expert's opinions in this regard. In this paper, relevancy and admissibility of E-Evidence is examined separately to evaluate the evidentiary value to that extent where court should appreciate the E-Evidences to be treated as conclusive proof of any fact in issue.

Keywords: Evidence, digital evidence, IT act, prosecutor, accused, offence, electronic records, Cyber Forensics

RESEARCH PROBLEM

Today's modern era with the broader perspective of digitalization has numerous terms of problems associated with it. Talking about crimes, it has also expanded to the levels of digitalization through involvement of various digital equipments (computers, mobile phones, etc) or through information provided in electronic form associated with Information and Communication Technologies and crimes associated with it can be termed as cyber crimes. Information or facts related to crimes is provided in both stored and transmitted manner to prove a fact in court of law is known as electronic evidence. Thus, evidence is often found & collected in context of trials and proceedings, of both civil & criminal matters in electronic or digital form from digital communication services or digital storage media. Evidence in electronic form serves the same purpose as traditional evidence but with certain concerns and agreements, especially during its collection, so as to prove its validity and make it admissible in the court of law. But despite the advantages of digital evidences, it is also associated with various disadvantages while proving its evidentiary value due to its nature of continuous advancement in modern technologies, or knowledge of various skills to many activities like duplicating, editing, replacing and even hampering of its quality associated with electronic records but these is not the end, the risk associated with digital evidence or electronic records is also due to regulations on admissibility and relevancy of e-evidence under Indian Evidence Act, Information Technology Act and

various other statutes and so as to analyze and study thoroughly through this paper named as "Forensic Analysis of Admissibility and relevancy of E-evidence, a part of documentary evidence".

Research Questions

Q.1 Whether judicial admission by the opposite party as to the electronic record dispenses with formal proof and compliance of Section 65B of the Indian Evidence Act?
Q.2 Whether an electronic document used as primary evidence under section 62 of the Evidence Act is admissible as evidence without meeting the conditions of section 65-B of the Evidence Act?
Q.3 Challenges associated with electronic or digital evidence?
Q.4 How far certification of every particular evidence is necessary?

Objectives

There are numerous problems associated with the digital evidences or electronic records due to its nature and regulations which can hamper the end results of any trials and proceedings of criminal and civil matters. Thus, considering this context of problematic conditions of E-Evidence, this research paper aims to provide some guidance for answering the various questions related to issues of digital evidence with the help of forensic analysis and a temporary review on the meaning of e-evidence, regulations of admissibility and relevancy of e-evidence in court of law, judicial view on admissibility of e-evidence, analysis of supreme court held landmark cases and Interpretations of India, USA and UK, and to present some self-thoughts on the regulations of admissibility and relevancy of E-Evidence.

Hypothesis

Section 65B of the Indian Evidence Act is "not obstante clause" which overrides the general law on secondary evidence given under section 63 and 65 of Indian Evidence Act. The section 63 and 65 of Indian Evidence Act does not apply to the e-evidences or electronic records but is fully governed by section 65A and 65B of Indian Evidence Act, 1872. The only option left to prove the electronic records or e-evidences is to produce the records originally in front of court as primary evidence under section 62 or it's copy using secondary evidence under section 65A and 65B of IEA. But keeping the fact in mind that while producing the e-evidence, every particular e-evidences or electronic records must be issued by certificates to have highly factual evidentiary value of it and make it admissible in court of law.

Research Methodology

Considering the terms, admissibility and relevancy of E-Evidence and its analysis through forensic tools, this research paper had followed descriptive and exploratory method with few aspects of statistical data and relevant reference from landmark judgments that are cited in order to shed light on the problems arising in regulations on the admissibility and relevancy of E-Evidence in Indian Courts.

LITERATURE REVIEW

(1) **Principles of the law of Evidence by Dr. Avtar Singh** is a very helpful to study about electronic evidence (a part of documentary evidence) in detail having concerns of every single legal terms associated with digital or electronic evidence or can say electronic records.
(2) **The Law of Evidence amended by Criminal Law (Amendment) Act, 2013 by batuk lal** is also a descriptive book to be referred for the study of analysis of admissibility and relevancy of e-evidence as a part of documentary evidence serving same purpose as traditional evidences.
(3) **Research Paper of SSRN, "Admissibility of E-Evidence in India"** is one of the fine paper to study about E-Evidence in summarized manner.
(4) **Anvar vs. Basheer and the New (old) Law of Electronic Evidence by The Centre for Internet and Society**- in this I got the brief history of Evidence Law by mentioning the principles of admissibility which will help the readers to understand and appreciate the true meaning and applications of Supreme Court rulings, which the true spirit and also talks about how e-evidence can be presented in court.
(5) **"Electronic Evidence and its authenticity in forensic evidence"**, is also a fine research paper to study about the forensic analysis of electronic evidences or electronic records.

INTRODUCTION

This present scenario or the era of 21st century is encountering huge advancements in modern technologies not just in India but also all over the world. The use of various devices like computers, mobile phones, etc., has made relaxation in many of the humanized actions by not restricting it to the recognized or established organizations or institutions but also giving opportunity to the individuals for its use and is quoted as "Cyber-World" leading to expansion of technologies. The

proliferation of Information Technology gives immense rise to Cyberspace in which internet offers people to access all information, data storage, analysation, etc, using advanced technology. This intense dependence on electronic means of communication, commerce, and warehousing information in digital form has certainly created the need to transform Information Technology statutes. Considering legal terms, law of evidence has changed immensely in recent years with numerous types of evidence deemed to be admissible in the court of law through amendments in the existing legislations. The expansion of computers and the influence of Information Technology on society have lead to necessary collection and storage of data or information in digital form by making changes to provisions of Indian Law for evaluation of E-Evidence. It is different from hard copy in such a manner that rules of documentary evidence must be re-examined[1]. Thus, Information Technology Act, 2000 and its amendments are based on United Nations Commissions on International Trade Law (UNCITRAL) and made admissibility of e-evidence viable in India, by legitimizing and encouraging electronic commerce in the global marketplace and amending the Indian Evidence Act, 1872 to include provisions on E-Evidence. Under the evidence law primary evidence has to be proved under section 64 while secondary evidence is to be proved under section 65. The primary evidence is that type of evidence which has highest factual certainty in questions whereas any evidence excluded from primary evidence is called as secondary evidence. The burden of proof to demonstrate the admissibility of secondary evidence rests with the party presenting the evidence. Section 65 of Indian Evidence Act requires that E-Evidence must be proved in accordance with the provisions of section 65B which was added by the virtue of schedule II of Information Technology Act regarding the admissibility of E-Evidence by establishing that any information contained in an electronic document is admissible as evidence by meeting the conditions of section 65B (2) to 65B (5). Therefore, each piece of e-evidence must be accompanied by a certificate issued after the checklist provided in section 65B. With the changes in law, the Indian courts have developed various landmark case laws regarding the use of e-evidence as Judges too demonstrate its knowledge including understandings of admissibility of e-evidence and interpretations of the laws regarding how electronic evidence can be submitted in the court of law.

MEANING OF EVIDENCE

The term evidence is derived from a Latin word "Evidere" which means to show clearly or to discover or to proof something. Evidence, it is the most prominent term in the trials and proceedings of civil and criminal matters, so as to decide the adjudications or can say judgments in the favor of either parties. It's objectives is to: (1) find out the facts of the particular case (2) provide justice (3) note the exact evidentiary value of the witnesses. There are many types of evidences such as oral evidence, documentary evidence, hearsay evidence, etc. Thus, according to the section 3 of Indian Evidence Act, 1872, evidence means and include- (1) all statements which the court permits or requires to be made before it by witnesses, in relation to matters of facts under inquiry, such statement are called oral evidence. (2) all documents including electronic records produced for the inspection of the court, such documents are documentary evidence[2].

MEANING OF DOCUMENTARY EVIDENCE

The provisions related to the documentary evidence are provided under *Chapter-V of the Indian Evidence Act, 1872*. *Section 3* of the Act defines the term "Document" "as any matter which is expressed or described on any substance by means of letters, figures or remarks or by more than one means and which can be used for recording the matter. Generally, the most common document which we have to deal with is described by letters. The documents are written in any language of communication such as Hindi, English, Urdu etc. The documents produced before the court as evidence are the documentary evidence and there must be primary or secondary evidence to prove the contents of the documents"[3]. Primary evidence has been defined under *section 62 of the Indian Evidence Act* and it means the original document when itself produced before the court for the inspection whereas the secondary evidence has been defined under *section 63 of the Act* as the certified copy of the evidence or copy of original documents by including the oral accounts given by a person about the contents of the document who has himself seen it.

MEANING OF ELECTRONIC EVIDENCE

In this Cyber-World era, the usage of computers is not just restricted to established organizations or institutions but also to every individual at the swipe of a finger. However, the virtual world unlike the real world creates several approaches for the commission of cyber offences such as phishing, child pornography, identity theft, hacking, etc. As there is a constant rise in the dependency on electronic means of communications, e-business and storing of information in digital form, the need for transformation of the law relating to the information technology as well as rules of admissibility of electronic evidence in

[1] Innovative Health group Inc vs Calgary Health Region 2008, ABCA 2019 (CanLII)(madam Justice Conrad)
[2] Meaning given under Indian Evidence Act,1872
[3] Wani, M. Afzal, Journal of Indian Law Institute 53, no.3 (2011): 530-33. Accessed, March 22, 2021.doi:10.2307/4514873

both civil and criminal matters has widened. The term 'Electronic Evidence' signifies a piece of evidence generated by some mechanical or electronic processes which is often relevant in proving or disproving a fact or fact at issue, the information that constitutes evidence before the court. Electronic Evidence is commonly known as Digital evidence. The forensics experts or the Examiner of Electronic Evidence have the ability to recover the data which is stored in electronic devices or systems and after their examination it can be made admissible before the Court proceedings. As the electronic records are more vulnerable to alteration, transposition, tampering, excision etc., without the presence of any such safety measures, it can lead to distortion of justice if the entire proceeding is based on electronic evidence. The legitimacy of the e-documents being arguable for the reason that they are susceptible to be tampered with, the agencies which conducts investigation of such e-documents are struggling with the problem of admissibility of such electronic evidence. Accordingly, the Information Technology Act, 2000 which is formulated on the basis of United Nations Commissions on International Trade (UNCITRAL) Model Law on Electronic Commerce was amended to allow the admissibility of digital evidence and also brought amendments to Indian Evidence Act, 1872, the Indian Penal Code, 1860 and the Banker's Book Evidence Act, 1891. The amendments carried out in these acts provides the legislative structure for transactions which take place in the electronic world. But it is accompanied with differences categorized such as CD,DVD, hard drive/memory map data, website data, social media communication, email, snapshot of chat messages, SMS/MMS and computer generated document poses unique issues and challenges for proper theme and authentication to various set of views. In this research paper, examiner of electronic evidence in nexus with the other statutory provisions with respect to the admissibility of electronic evidence has been analyzed.

MEANING OF ELECTRONIC RECORD/DOCUMENT UNDER INFORMATION TECHNOLOGY ACT, 2000

Electronic record Complies with section 2 (t) of the Information Technology Act, 2000, of a broader connotation is given to an electronic document. Section 2 (t) defines" electronic record " in the sense of data, record or generated data, image or it's stored, received or transmitted in electronic or microfilm format or computer generated microfilm"[4]

Legal recognition of Electronic Record u/s 4 of the IT Act
When a law provides this information or any other question written, typed or printed, and then nothing against nothing contained in said law, it is considered that this requirement has been Please, when such information or elements:
(a) Are displayed or available in an electronic form; and
(b) Accessible for use by another reference

ELECTRONIC EVIDENCE AND INDIAN EVIDENCE ACT, 1872

Apparently, when comparing electronic evidence to the conventional or traditional form of evidence, it has been seen that the evaluation of the electronic evidence in order to check its authenticity requires specialized and expert training in the field of cyberspace, the methodology used for its investigation and the analysis of facts, figures, or particulars kept or recovered from any electronic device for it to be admissible before the court of law. The Indian Evidence Act which has been amended as a consequence of Section 92 of the Information Technology Act, 2013, includes the addition of the words "electronic record" in the definition of evidence, thereby permitting admissibility of the electronic evidence. Regarding Section 59, which incorporates "documentary evidence", for the words "contents of documents" the words "contents of documents or electronic records" have been substituted. In addition to this Section 65A & 65B were inserted by way of amendment to provide for the admissibility of electronic evidence. Further, Section 79A of the IT Act has expanded the scope of Section 45 of the Indian Evidence Act. Section 45 of the IEA provides for Opinion of experts. By virtue of Section 45, any expert called to give opinion on "electronic form evidence" will be relevant in accordance with the Indian Evidence Act, 1872. Also, a separate Section i.e., Section 45A has been inserted by way of amendment in the year 2009 to specifically make the Opinion of Examiner of Electronic Evidence relevant before the court of law.

As per Section 45A, During a proceeding if the need arises as to formation of an opinion by the Court on any matter which pertains to any information communicated or stored in any computer resource or in any other electronic or digital form, the opinion which is given by an Examiner of Electronic Evidence mentioned under Section 79A of the Information Technology Act, 2000 is a relevant fact. The explanation clause supplemental to section 45A states that the Examiner of Electronic Evidence is an expert for the purpose of this Section. In the matter of *Tulip Lab Pvt. Ltd v. Mr. Henrik Uffe Jensen*, the Delhi High Court had opined that, "NASSCOM is requested to appoint an expert to look into the data furnished by the defendants in support of the contention that the plaintiff may be indulged in spamming…."[5]

[4] Information Act, 2000, section 2(t) and section 4
[5] Research paper of SSRN, "Admissibility of e-evidence in India".

ADMISSIBILITY OF ELECTRONIC EVIDENCES

Section 65A of the Indian Evidence Act has been incorporated with the intention to prove the contents of electronic records in conformity with the provisions of Section 65B of the Indian Evidence Act. Thus, Section 65B of the Evidence Act specifies the procedure for justifying any documentary evidence by way of an electronic record. Section 65B states that, Despite the other provisions of the Evidence Act, any information which is contained in electronic record i.e., engraved on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be considered to be a document, if it fulfils the conditions prescribed under this section 65B (2) to (5) in connection with the information and the computer in question, shall be admissible in any civil or criminal proceeding without the directive to present the evidence by producing the original document.

CONDITIONS FOR THE ADMISSIBILITY OF ELECTRONIC EVIDENCES UNDER SECTION 65B, 65B (1)(2)(3)(4) OF INDIAN EVIDENCE ACT

Cases in which secondary evidence relating to documents may be given.— Secondary evidence may be given of the existence, condition or contents of a document in the following cases: —

(a) when the original is shown or appears to be in the possession or power — of the person against whom the document is sought to be proved, of any person out of reach of, or not subject to, the process of the Court, or of any person legally bound to produce it, and when, after the notice mentioned in section 66, such person does not produce it;
(b) when the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest;
(c) when the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;
(d) when the original is of such a nature as not to be easily movable;
(e) when the original is a public document within the meaning of section 74;
(f) when the original is a document of which a certified copy is permitted by this Act, or by any other law in force in [India][6] to be given in evidence;
(**g)** when the originals consist of numerous accounts or other documents which cannot conveniently be examined in Court and the fact to be proved is the general result of the whole collection.

In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible.
In case (b), the written admission is admissible.
In case (e) or (f), a certified copy of the document, but no other kind of secondary evidence, is admissible.
In case (g), evidence may be given as to the general result of the documents by any person who has examined them, and who is skilled in the examination of such documents.

[7]**[65A Special provisions as to evidence relating to electronic record** — The contents of electronic records may be proved in accordance with the provisions of section 65B.

65B. Admissibility of electronic records. —
Section 65B(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Section 65B (2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: —

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

[6] Subs. By Act 3 of 1951, s.3 and the Schedule, for "the States".
[7] Ins. By Act 21 of 2000, s. 92 and the Second Schedule (w.e.f.17-10-2000).

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Section 65B(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) By a combination of computers operating over that period; or
(b) By different computers operating in succession over that period; or
(c) By different combinations of computers operating in succession over that period; or
(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

Section 65B(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, —

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

Section 65B (5) For the purposes of this section, —
(a) Information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
Explanation. —For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.]

MODE TO PROVE ELECTRONIC RECORDS UNDER SECTION 65A OF INDIAN EVIDENCE ACT, 1872

Section 65A of the Indian Evidence Act is a special provision providing mode of proving and making e-evidence admissible in court. It says, "Contents of electronic records may be proved in accordance with the provisions of section 65B10." In general words, electronic record may be proved, if compliance of section 65B is made. In exceptional cases, the content of electronic records can be tested. Section 65B has been complied with this means that the content of that document can be tested on the basis of a simple certificate. Now it's up to the court to see what document can be proved during certification according to section 65B of the Indian Evidence Act. For Example: System log-in data record. It may be proved by certification under section 65B of the IEA. Term may be used, so it is not obligatory. It depends on the circumstances, the court may request for better evidence. Section 65A of the Evidence Act creates Electronic evidence law; the content of electronic documents may be tested in accordance with the provisions of section 65B.20 The section performs the same function for electronic records as the section 61 done for supporting documents: create a separate procedure, distinguishes itself from the simple oral testimony procedure.

TYPES OF ELECTRONIC EVIDENCES WITH ITS ADMISSIBILITY AND EVIDENTIARY VALUE UNDER INDIAN EVIDENCE ACT

Information Technology Act, 2008 defines electronic records; it covers a wide range of formats in which data can be produced. DVD, CD, pen drives, telephonic recordings, hard drives, e-mails, pictures, video recordings, sound recordings, etc. are a few of them. Each of the above electronic records formats deals with a variety of different conditions relating to their evidentiary value and admissibility in a court of law.

Evidence in the form of as DVD, CD, Hard-Drive, chip, Memory Chip, Pen Drive: Above electronic records are admissible as primary as well as secondary evidence. The value evidence depends on how and in what manner the electronic records have been submitted to the court i.e. if these electronic records are submitted as it is then those have more value without any doubt but if you want to submit their copied version on other similar or different device then you have to comply with the conditions precedent under Sec. 65b of the Indian Evidence Act and get the certificate for its admission in the court.

Audio and Video Recordings: These electronic records are admissible if they are submitted in original i.e. original audio or video recordings are the valid and authentic source of electronic evidence and not the copied version. Their copied version records on other similar or different device have to comply with the conditions precedent under Sec 65B of the Indian Evidence Act and get the certificate for its admission in the court.

Evidence generated through mobile phone in the form of media, calls and email: Email: It is recognized as a valid and authentic source of evidence. Generally, e-mails are submitted through print outs attached with the certification of u/s 65B of the Indian Evidence Act. Media and calls generated through mobile phone: Nowadays, Mobile phones are very useful electronic device and very resourceful. It helps from tracing location, capturing videos & pictures, recording calls to many other electronic resources which aids the judicial and investigating system to get valuable evidence. Mobile phone's electronic records are admissible if they are submitted in original i.e. mobile itself which contains the primary source of media and calls. Their copied version records on other similar or different device have to comply with the conditions precedent under sec. 65B of Indian Evidence Act and get the certificate for its admission in the court.

MEANING OF CYBER FORENSICS

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Computer forensics -- which is sometimes referred to as *computer forensic science* -- essentially is data recovery with legal compliance guidelines to make the information admissible in legal proceedings. The terms *digital forensics* and *cyber forensics* are often used as synonyms for computer forensics.

Digital forensics starts with the collection of information in a way that maintains its integrity. Investigators then analyze the data or system to determine if it was changed, how it was changed and who made the changes. The use of computer forensics isn't always tied to a crime. The forensic process is also used as part of data recovery processes to gather data from a crashed server, failed drive, reformatted operating system (OS) or other situation where a system has unexpectedly stopped working.

Types of computer forensics

There are various types of computer forensic examinations. Each deals with a specific aspect of information technology. Some of the main types include the following:

- **Database forensics.** The examination of information contained in databases, both data and related metadata.
- **Email forensics.** The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.
- **Malware forensics.** Sifting through code to identify possible malicious programs and analyzing their payload. Such programs may include Trojan horses, ransomware or various viruses.
- **Memory forensics.** Collecting information stored in a computer's random access memory (RAM) and cache.

- **Mobile forensics.** The examination of mobile devices to retrieve and analyze the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.
- **Network forensics.** Looking for evidence by monitoring network traffic, using tools such as a firewall or intrusion detection system.

Techniques forensic investigators use

Investigators use a variety of techniques and proprietary forensic applications to examine the copy they've made of a compromised device. They search hidden folders and unallocated disk space for copies of deleted, encrypted or damaged files. Any evidence found on the digital copy is carefully documented in a finding report and verified with the original device in preparation for legal proceedings that involve discovery, depositions or actual litigation. Computer forensic investigations use a combination of techniques and expert knowledge. Some common techniques include the following:

- **Reverse steganography.** Steganography is a common tactic used to hide data inside any type of digital file, message or data stream. Computer forensic experts reverse a steganography attempt by analyzing the data hashing that the file in question contains. If a cybercriminal hides important information inside an image or other digital file, it may look the same before and after to the untrained eye, but the underlying hash or string of data that represents the image will change.
- **Stochastic forensics.** Here, investigators analyze and reconstruct digital activity without the use of digital artifacts. Artifacts are unintended alterations of data that occur from digital processes. Artifacts include clues related to a digital crime, such as changes to file attributes during data theft. Stochastic forensics is frequently used in data breach investigations where the attacker is thought to be an insider, who might not leave behind digital artifacts.
- **Cross-drive analysis.** This technique correlates and cross-references information found on multiple computer drives to search for, analyze and preserve information relevant to an investigation. Events that raise suspicion are compared with information on other drives to look for similarities and provide context. This is also known as *anomaly detection*.
- **Live analysis.** With this technique, a computer is analyzed from within the OS while the computer or device is running, using system tools on the computer. The analysis looks at volatile data, which is often stored in cache or RAM. Many tools used to extract volatile data require the computer in to be in a forensic lab to maintain the legitimacy of a chain of evidence.
- **Deleted file recovery.** This technique involves searching a computer system and memory for fragments of files that were partially deleted in one place but leave traces elsewhere on the machine. This is sometimes known as *file carving* or *data carving*.

JUDICIAL INTERPRETATIONS ON ADMISSIBILITY OF E-EVIDENCE IN INDIA AND USA

Judicial Interpretation on admissibility of e-evidence in India

In a reference related to the interpretation of Section 65B of the Electronic Records Admissibility under Evidence Act of 1872, RF Nariman's three-judge court, S. Ravindra Bhat and V. Ramasubramanian, held that the certificate required under section 65B (4) is a prerequisite for the admissibility of evidence by means of an electronic file, as rightly judged by the three-judge tribunal in Anvar PV v. PK Basheer, (2014) 10 SCC 473, and incorrectly clarified by a divisional bench in Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801. The court further clarified that the certificate required under Section 65B (4) is not necessary if the original document is self-produced or primary in nature qualifying condition mention u/s62.

The Court heard the remission of the order of July 26, 2019, in which, after citing Anvar PV v PK Basheer, (2014) 10 SCC 473 (decision of this court with three judges), it was determined that a sentence of the additional bench in Shafhi Mohammad v. Himachal Pradesh state, (2018) 2 SCC 801 may need to be reconsidered by larger bench of judges. The divisional bench had clarified in the Shathi Mohammad judgment that the requirement of a certificate under Section 64B (4), being procedural, can be relaxed by the Court when the interests of justice justify it, and a circumstance in which the interest of justice would be for the electronic device to be produced by a party that does not own that device, which would prevent that party from obtaining the required certificate.

(1) Anvar P.V. vs. P.K. Basheer & Ors 16

Notwithstanding what we have stated herein in the preceding paragraphs on the secondary evidence of electronic record with reference to Sections 59, 65-A and 65-B of the Evidence Act, if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act, the same is admissible in evidence, without compliance with the conditions in Section 65-B of the Evidence Act"7"

The court also cleared up the confusion surrounding the earlier judgment in the Anvar PV case and ruled that the last sentence in the Anvar PV case that reads: "if an electronic record as such is used as primary evidence u/s 62 of the Law of Evidence... "must be read without the words" by virtue of section 62 of the Evidence Act" These observations are clearly contrary to the provisions of Section 65B, which does not distinguish between "primary" and "secondary" evidence. In doing so, the Court added virtual words to section 65-B to say that the certificate is necessary for secondary tests and not for primary tests. It was also inappropriate to rely on section 62 to reach this conclusion.

Sections 65A and 65B are complete codes, as evidenced by the no-obstruction clause. In addition, Sections 61 to 65 deals with conventional docs i.e. documents that are not generated on an elect while Sections 65-A and B deal with electrical evidence to the repletion of Sections 61 to 65. But the court later said that secondary evidence for the content of the document could also be based on section 65 of the Evidence Act. This statement is manifestly incorrect and contrary to the provisions of section 65B.

Two Supreme Court decisions depart from the position in Anvar (supra). In Tomaso Bruno held by Supreme Court bench of three judges ruled that secondary evidence of the content of a document can be invoked u/s 65. In that judgment, however, the Supreme Court has not invoked section 65B (4), nor of the law established in Anvar case. Instead, the Supreme Court relied on Navjot Sandhu", which was specifically annulled in Anvar case.

(2) NCT of Delhi v. Navjot Sandhu

Subsequently, in Shafhi Mohammad, the Supreme Court ruled that the requirement to present a certificate under section 65B (4) was procedural and not always mandatory. A party not in possession of the device from which the document was produced cannot be required to submit a certificate under section 65B, paragraph 4, which will apply only when a device provides electronic evidence and therefore can provide such a certificate. However, if the person is not in possession of the device, sections 63 and 65 cannot be excluded.

The Supreme Court overruled the judgment held in the case of Tomaso Bruno and Shafhi Mohammad in order to clarify the position of law on admissibility of e-evidence as follows:

- A certificate under section 65B (4) is mandatory and a prerequisite for the admissibility of evidence by means of electronic records.
- There is no need to reconsider the law enshrined in Anvar. The last sentence of paragraph 24 of said judgment, which reads: "if an electronic document as such is used as primary evidence under section 62 of the Evidence Law, it is identical to evidence, without meeting the conditions of section 65) .B of the Evidence Act "should be read without the words" as per section 62 of the Evidence Act".
- The non-obstructive wording of section 65B, paragraph 1, makes it clear that when it comes to information contained in an electronic document. its admissibility and evidence must follow the exercise of section 65B, which is a special provision in this regard and sections 62 and 65 are irrelevant in this regard.
- The requirement of subsection 65B (4) is not necessary if the original document is submitted under sec 62. This can be done by the owner of a laptop, tablet or even a cell phone by going to the witness stand and proving that the device in question, on which the original information was first stored, is owned and/or controlled. for him.. If the computer is on a system or network and it is not possible to physically bring said system or network to court, the only way to provide information in said electronic record is in accordance with Section 65B (1), with the certificate required under the subsection 65B (4).
- Oral evidence cannot be sufficient in lieu of a certificate under Section 65B (4) and a person responsible for a computing device cannot provide evidence, in lieu of the certificate required under section 65B (4),
- If the required certificate has been requested from the interested person or authority and the interested person or authority refuses to issue said certificate or does not respond to said request, the party requesting said certificate may request the court to obtain the certificate' in accordance with the provisions of the Evidence Law", of the Code of Civil Procedure, 1908 and/or of the Code of Criminal Procedure, 1973. Once the request has been submitted to the court and In court orders or orders while the required certificate must be presented by the person to whom you send a subpoena in this regard, the party requesting the certificate has made every effort to obtain the required certificate, the required certificate.
- The court observes that Section 65B does not refer to the stage at which such act must be provided to the court. In Anvar (supra), the Court indicated that said certificate must accompany the electronic file when it is presented as evidence. This requirement applies in cases where the p person who wishes to rely on the electronic record can obtain said certificate. In cases where a deferate is issued or when such a certificate is required and has not been issued by the p 14/18 he court will summon the person mentioned in section 65 B. paragraph 4, and ret to issue the certificate.. (s). This should be done when the electronic record is presented to the court without the required

certificate as evidence. In criminal cases, the court can have the required certificate produced at any stage, as long as as the trial is not over. Although these observations were made in the context of criminal cases, the Court indicated that the foregoing is subject to the exercise of adequate discretion in civil matters.

- Since the certificate can be issued pursuant to section 65B (4) long after the computer has actually produced the electronic record, it is sufficient that the certificate is to the best of the transmitter's knowledge.
- The conditions of sections 65B (2) and 65B (4) must be fulfilled collectively

(3) Sanjaysinh Ramrao Chavan Vs. Dattatray Gulabrao Phalke

The Hon'ble High Court of Delhi, while choosing the charges against denounced in a defilement case watched that since sound and video CDs being referred to are unmistakably forbidden in confirm, hence trial court has incorrectly depended upon them to reason that a solid doubt emerges in regards to solicitors criminally plotting with co-blamed to carry out the offence being referred to. Along these lines, there is no material based on which, it can be sensibly said that there is solid doubt of the complicity of the applicants in commission of the offence being referred to. Ankur Chawla Vs. CBI. The Hon'ble High Court of Calcutta while choosing the acceptability of email held that an email downloaded and printed from the email record of the individual can be demonstrated by ethicalness of Section 65B r/w Section 88A of Evidence Act. The declaration of the observer to do such technique to download and print the same is adequate to demonstrate the electronic correspondence. Abdul Rahaman Kunji Vs. The State of West Bengal. In the ongoing judgment articulated by Hon'ble High Court of Delhi, while managing the acceptability of blocked phone bring in a CD and CDR which were without an endorsement u/s 65B Evidence Act, the court watched that the optional electronic confirmation without authentication u/s 65B Evidence Act is unacceptable and can't be investigated by the court for any reason at all. Jagdeo Singh Vs The State and Ors.

Case Law: Riley Vs California (U.S Supreme Court Judgment)

The Supreme Court held in a unanimous decision by Chief Justice Roberts, that police generally require a warrant in order to search cell phones, even when it occurs during an otherwise lawful arrest. The Chief Justice explained that analogizing a search of data on the cell phone to a search of physical items is akin to "saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from Point A to Point B but little else justified lumping them together." The Court also emphasized that "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple–get a warrant."

EPIC's amicus brief, joined by twenty-four legal scholars and technical experts from the EPIC Advisory Board, was cited twice in the Court's opinion, on pages 20 and 21 and the Court also adopted other portions of the brief without explicit reference. The Court stated:

Mobile application software on a cell phone, or "apps" offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. See Brief for Electronic Privacy Information Center as Amicus Curiae in No. 13-132, p. 9.

Case Law: Lorraine Vs Markel American Insurance Company, 241 F.R.D. 534 (D. Md. May 4, 2007)

Magistrate Judge Paul D. Grimm (United States District Court for the District of Maryland) provided the field with guidance on the admissibility of electronic evidence. In the ensuing years, the case drew comments and criticism from legal scholars. According to the court, when Electronically Stored Information (ESI) is offered as evidence, the following evidentiary rules must be considered: relevancy, authenticity, hearsay, best evidence, and probative value.

Levi-Sachs and Archambault (2008) stated that "Despite the fact that the court provides a general roadmap for admissibility of ESI, the court does not indicate whether more stringent standards are necessary or desirable." Frieden and Murray (2011) believe that the methods for authentication prescribed in Lorrain Vs Markel are similar to those of traditional evidence. They state that though, "certain issues, such as authentication, may be more complicated in the context of electronic evidence, traditional evidentiary principles can be consistently adapted to address questions regarding the admissibility of electronic evidence."

CONCLUSION

Digital evidence or electronic record is permitted in India, if it meets the conditions provided under Section 65B. Therefore, the law on the admissibility of digital evidence is very well crystallized. However, one of the concerns that still arise is when, if a secondary electronic record is confiscated from the defendant, obviously the certificate cannot be obtained under 65B (4). Furthermore a question arose, when an electronic document used as primary evidence under section 62 of the Evidence Act is admissible as evidence without meeting the conditions of section 65-B of the Evidence Act? After analysation of the provisions and judgments held by apex court it can be thus conclude that the admissibility of the secondary electronic evidence has to be adjudged within the parameters of Section 65B of Evidence Act and the proposition of the law settled in the recent judgment of the Apex Court and various other High Courts as discussed above. The intention is clear and explicit that if the secondary electronic evidence is without a certificate under section 65B of Evidence Act, it is not admissible and any opinion of the forensic expert and the testimony of the witness in the court of law cannot be looked into by the Indian court. However when an electronic document used as primary evidence under section 62 of the Evidence Act is admissible as evidence without meeting the conditions of section 65-B of the Evidence Act as held by Supreme Court in its various judgments.

The tolerability of the optional electronic confirmation must be decreed inside the parameters of Section 65B of Evidence Act and the suggestion of the law settled in the ongoing judgment of the Apex Court and different other High Courts as examined previously. The suggestion is clear and unequivocal that if the auxiliary electronic confirmation is without an endorsement u/s 65B of Evidence Act, it isn't allowable and any assessment of the criminological master and the testimony of the observer in the official courtroom can't be investigated by the court. In any case, there are few holes which are as yet uncertain as what might be the destiny of the optional electronic confirmation seized from the blamed wherein, the declaration u/s 65B of Evidence Act can't be taken and the denounced can't be made observer against himself as it would be violative of the Article 19 of the Constitution of India. Unmistakably the affirmation of electronic proof is the standard over all locales, as opposed to the avoidance. Alongside preferences, the suitability of electronic records can likewise be unpredictable – albeit a few locales have forced the necessities viewing acceptability as in India.22 It may be, in this manner, upon the 'managers of law', the courts to see that the right proof is displayed and directed to encourage a smooth working of the lawful framework. Sound and educated administration rehearses alongside investigation by the courts must be received to decide if the confirmation satisfies the three basic legitimate prerequisites of validness, dependability and trustworthiness. Ideally, with the Supreme Court having re- characterized the guidelines, the Indian courts will embrace a reliable approach, and will execute every conceivable defend for tolerating and acknowledging electronic confirmation.

BIBLIOGRAPHY

Books & Journals

[1] Anvar v. Basheer and the New (Old) Law of Electronic Evidence - The Centre for Internet and Society http://cisindia.org/internetgovernance/blog/anvarvbasheernewoldlawofelectronicevidence.accessed on 31/03/2020.
[2] http://mja.gov.in/Site/Upload/GR/Title NO.190 (As Per Workshop List title n 0190 pdf)
[3] https://ujala.uk.gov.in/files/15.pdf
[4] Paul, George L. "CANVASSING THE EMERGING LAW OF DIGITAL INFORMATION: STEPHEN MASON'S 'ELECTRONIC EVIDENCE. Jurimetrics, vol. 53, no. 4, 2013, pp. 467-481. JSTOR, www.jstor.org/stable/24395659 Accessed 23 Mar. 2021
[5] Schafer, Burkhard, and Stephen Mason. "The Characteristics of Electronic Evidence." Electronic Evidence, edited by Stephen Mason and Daniel Seng. University of London Press, 2017, pp. 18 35. JSTOR, www.jstor.org/stable/j.ctv512x65.9. Accessed 23 Mar. 2021
[6] Tejaskaria. et al. The Supreme Court of India re-defines admissibility of electronic evidence in India, 12 DEESLR. 33, 36 (2015). Accessed on March 31, 2021. 7. Wani, M. Afzal. Journal of the Indian Law Institute 53, no. 3 (2011): 530-33. Accessed, March 22, 2021. doi:10.2307/45148573.

Cases Referred

[1] Anvar P.V. vs..P.K. Basheer & Ors, (2014) 10 SCC 473
[2] K. Ramajyam v. Inspector of Police (2016) Crl. LI 1542
[3] State (NCT of Delhi) v. NavjotSandhu Afsan GAIR 2005 SC 3820
[4] State vs. Mohd Afzal (2003) 107 DLT 385
[5] Tomaso Bruno and Anr. v. State of Uttar Pradesh
[6] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 80

[7] Barnali Baishya vs State Of U.P. And Anr

Statues

[1] Code of Civil Procedure, 1908
[2] Code of Criminal Procedure, 1973
[3] Indian Evidence Act, 1872
[4] Information Technology Act, 2000.