E- EVIDENCE AND COMPUTER FORENSICS: AN ANALYSIS OF THEIR LEGAL FRAMEWORK AND ADMISSIBILITY UNDER THE IT ACT, 2000 AND INDIAN EVIDENCE ACT, 1872

Neha Nandwani & Vishal Tanwar, Manav Rachna university

ABSTRACT

In the era of computer, most of the information is stored in digital form in different devices such as computer, communication device such as cell phone, digital voice recorder, digital camera, and digital video cameras etc. The use of computer forensic and electronic evidence has become increasingly prevalent in legal proceedings and investigations. This research paper aims to provide the overview of the role and significance of electronic evidence and computer forensics and admissibility under the information technology Act 2000 and the Indian evidence act.

Keywords: e- evidence, computer forensic, digital evidence, information technology act, Indian evidence act

Introduction

Computer forensic has becomes very important as the world becomes increasingly digitally connected. It is a field of digital forensics that focuses on the identification, collection, and storing evidence from an electronic device. E-evidence is any information which is stored or transmitted in digital form. This includes emails, text messages, documents, photos, videos, computer logs, social media posts, and other type of digital data. Computer forensics and electronic evidence are essential in various legal contexts, including criminal investigations, civil litigation, intellectual property disputes, fraud investigations, and cyber security incidents. They play a crucial role in establishing the authenticity, integrity, and admissibility of digital evidence and help to uncover the truth to support the administration of justice.

The IT Act has been instrumental in addressing the legal aspects of computer forensics and electronic evidence in India. It has provided a legal framework for the recognition, admissibility, and investigation of electronic evidence to handle and prosecute the cybercrimes.

Computer 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.[1] It is also known as digital forensic. The purpose of computer forensics techniques is to search, preserve and analyse information on computer systems to find potential evidence. A computer forensic examination may prove when a document first appeared on a computer or e-device, when it was last edited, when it was last saved and which user carried out these actions.

Computer forensics is used both in criminal as well as civil prosecution. In ***civil prosecution*** change, alteration in information or stealing of information, can be proved by e-evidence. In ***criminal prosecution***, there are various areas of crimes or dispute where computer forensics is applied such as cyber contravention, intellectual property theft, employment disputes, fraud

[1] Tech target website- What is Computer Forensics (Cyber Forensics)? (techtarget.com)

investigation, forgeries, bankruptcy investigations, inappropriate email and internet use in the work place and regulatory compliance.

types of computer forensics:

1. **disk forensics**- it deals with extracting raw data from the primary or secondary storage of the device by searching active, modified or deleted files.

2. **email forensics-**the recovery and analysis of schedules and contracts contains in email platform.

3. **Malware forensics**- walking through code to find malicious programs and analyzing their payload.

4. **Memory forensics**- receiving the data stored in a computer memory.

Digital evidence or E-evidence

The information technology act deals with various aspects of electronic governance, cybersecurity and electronic commerce. It provides provisions for the admissibility, authenticity, and integrity of electronic evidence. section 79A of the IT (Amendment) Act, 2008 define electronic evidence as any information of probative value that is either stored, or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines. According to section 2(1)(t) of the IT Act[2], the term "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer-generated micro fiche. The e-evidence not only include evidence found in computers but may also extend to include evidence on digital devices such as, telecommunication or electronic multimedia devices. The e-evidence can be found in emails, digital photographs, ATM transaction logs, word processing, documents, instant message, histories, filed saved from accounting programs, spreadsheets, internet browser history databases, contents of computer memory, computer backups, digital video or audio files.

[2] Information Technology Act, 2000

Usage of computer forensic to find e-evidence

Computer forensic has been used to find e-evidence in legal cases that involves the identification, collection, preservation, analysis and presentation of digital evidence. there are various cases where computer forensic is used as evidence:

Dr. Mrs. Nupur talwar V. state of Uttar Pradesh & Anr[3]

Arushi-hemraj murder case, this high profile case from 2008 involved the murder of a teenage girl, arushi talwar and her family's domestic helper, hemraj banjade, in Noida, Uttar Pradesh. Digital forensics played a crucial role in examining the computer and mobile phone records of the victims and suspects, analyzing call logs, text messages, and internet browsing history to find key evidence.

Pratim alias peter mukherjea V. Union of India And Anr[4]

The Sheena bora murder case, which came to light in 2015, involved the murder of sheena bora, the daughter of media executive Indrani mukerjea. Digital forensic played a important role in this case, as the investigation involved analyzing mobile phone records, call data, text messages, and email communications. The digital evidence helped in establishing the relationships between the individuals involved, reconstructing the timeline, and providing crucial evidence against the accused.

Muder of shraddha walker[5]

The sharadhha murder case, where her boyfriend, aaftab poonawala cut the body into 35 parts, stored it in their refrigerator and dumped pieces in isolated locations over a period of time. The e-evidence that can gathered from mobile phones, other electronic gadgets, bank transactions provided evidence against the accused.

Legal provision of Computer forensic and e-evidence in India

Computer forensic and electronic evidence are addressed under both the information

[3] (1984) 2 SCC 627
[4] 19 january 2018
[5] Delhi Murder: Mumbai youth Aaftab threw body parts of Shraddha everyday in Chhatarpur forest hoping animals would eat them (freepressjournal.in) free press journal

technology act and the Indian evidence act. The IT Act[6] has incorporated **section 79A** which empowers the central government to appoint any department, body or agency as examiner of electronic evidence for providing expert opinion on electronic form of evidence before any court or authority.

The Information Technology Act, 2000

Under the information technology act 2000, e-records can be used as e-evidence. The act gives wide meaning of electronic record and it includes electronic data in any form such as videos or voice messages simple email or short message (SMS), or multimedia message (MMS) or other information or data in any electronic forms. It means data stored in communication device such as cell phone can also be used as e-evidence. the information technology has made it easy to communicate and transmit data in various forms from a simple personal computer or a mobile phone or other kinds of devices. The Information Technology Act, 2008 has recognized various forms of communication devices and defines a communication device **under section 2 (ha)** of the act means cell phones personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image. Therefore, any e-evidence whether stored in any other device such as computer, digital camera, digital video camera or communication device etc.

The legal validity of e-record is under **section 4 of IT Act, 2000** which states that where any law provides that information or any other manner shall be in writing or in the type written or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed ton have been satisfied if such information or matter is –

- rendered made available in an electronic form; and
- accessible so as to be usable for a subsequent reference

E-evidence has same validity as that of documentary evidence under IT Act.

Indian Evidence Act, 1872

The definition of evidence in **section 3**, the interpretation clause of the act[7] states that evidence

[6] IT (amendment) act,2008
[7] Indian Evidence Act,1872

means *"all documents including electronic records produced for the inspection of the court"* and such evidence is called documentary evidence. Under the Indian Evidence Act, electronic evidence is recognized and governed by section 65 A and 65B. This section provides guidelines for the admissibility of electronic evidence in legal proceedings.

Section 65 A: section 65 A of the Indian evidence Act deals with the admissibility of the electronic records. It states that information contained in electronic records shall be deemed to be a document and admissible as evidence, if the following conditions are satisfied:

- The electronic record is produced from the computer or any other electronic device.
- The computer or electronic device is used for storing the information.
- The information is stored in any form such as printout, optical or magnetic media, or any other form capable of being reproduced.

Section 65B: section 65B of the Indian Evidence Act provides additional requirements for the admissibility of electronic evidence. It states that any information contained in an electronic record i.e. printed on a paper, stored, record or copied in optical or magnetic media, and produced by a computer during a regular course of business shall be deemed to be a document and admissible as evidence. section 65B requires that electronic evidence be accompanied by a certificate, issued by a person in charge of a computer system, affirming its authenticity.

Judicial response to e-evidence

Amitabh Bagchi Vs Ena Bagchi[8]

The Calcutta High Court analyzed section 65 A and 65 B of Indian Evidence Act and upheld that the physical presence of the person in Court may not be required for purpose of adducing evidence and the same can be done to the e medium like video conferencing. The Court stated that section 65A and 65B provide provisions for evidences relation to electronic records and admissibility of electronic records which includes video conferencing.

[8] AIR 2003 SC 2053

Anvar P.V V. P.K. Basheer[9]

The supreme court in the landmark case provided the admissibility of electronic evidence under 65B of the Indian evidence act. The court held that electronic evidence such as electronic documents or CDs, should be accompanied by a certificate in accordance with section 65B(4) of the act.

State of Delhi vs Mohd. Afzal[10]

It was held that electronic records are admissible as evidence. if someone challenges the accuracy of a computer evidence or electronic record on the ground of misuse of system or operating failure or interpolation, then the person challenging it must prove the same beyond reasonable doubt.

Jagjit singh v state of Haryana[11]

In this case, voice recording on CD was accepted as evidence. A member of Haryana SLA gave interview to various news channels i.e; zee news television channel, aaj tak television channel and the Haryana news of Punjab today television channel. The speaker of the legislative assembly of the state of Haryana disqualified him for defection. The court stated that the electronic evidence placed on record was admissible.

Suggestions

computer forensics and electronic evidence are rapidly evolving fields. In this regard, there is a need of providing proper training to law enforcement agencies in handling cyber related evidence and application of sections of evidence law while presenting such evidence in court. There is also need to spread awareness that while submitting evidence to police or courts, it is mandatory to submitted with a certificate under section 65 B (4) of the and Indian Evidence Act so the Court takes cognizance and read it as a primary evidence. It is essential to stay updated on the latest technological advancements, forensic techniques, and legal developments related to electronics evidence.

[9] 2014 10 SCC 473
[10] 2003 (3) JCC 1669
[11] 2006 (11) SCC 1

Conclusion

The Information technology act, 2000 has played a commendable role in addressing issues related to computer forensic and electronic evidence in India. The act was enacted to provide legal recognition and facilitate e-commerce, e-governance, and electronic transactions. Computer forensics serves as a vital tool in the discovery and presentation of electronic evidence in civil and criminal cases. It ensures that digital evidence is collected, analyzed, and presented in a manner that meets legal requirements, thereby assisting in the administration of justice. The information technology act, 2000 amendment is based on the united nations commission on international trade law (UNCITRAL) model law. The IT Act and Indian evidence act has permitted admissibility of digital evidence in various devices such as computer, communication device, digital voice recorder, digital cameras, digital video cameras etc.