Page 1717 - 1731 **DOI:** *http://doi.one/10.1732/IJLMH.25898*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 1

2021

Digital Evidences in Investigation of Cyber Offences in India: An Analytical Study

DR. SHIV RAMAN[1] AND MS. NIDHI SHARMA[2]

ABSTRACT

In the present Digital World, new technologies and new inventions are taking place and many more technological developments are under process. The Computer based technology is used for enhancing the modern life everywhere including education, commercial sectors and Govt. organizations etc. It ensures the efficiency and productivity. On the other side 'the excessive dependence' over the technology is the root cause of the Cyber Criminal for committing unlawful and unethical activities with the use of computer and Internet. The Collection and compilation of Digital evidence from the computer and IT based devices is the most challenging job for all investigating agencies in India. The investigation and collection of evidences from computer requires expertise, special knowledge and skill, which is lacking in most technical-personnel's of our country.

Nowadays India has developed as favorite nucleus for the Cyber Criminals, especially hackers and other malevolent users, which use the Internet as a tool for Cyber crimes. The rising trend of Cyber crimes includes Cyber-spamming, hacking, Cyber stacking including theft, phishing etc. Now the time has come for the Indian Police to overhaul and reform investigating methodology for a successful prosecution of Cyber cases in India. Indian traditional system of policing and criminal investigation, is still conducting in old ways of extracting, gathering information and obtaining confession by beating. The Police force is still untrained of modern methods of criminal investigation, which needs special skill for managing and operating highly sophisticated technologies.

Keywords: *Forensic, Digital, Investigation, E- evidence etc.*

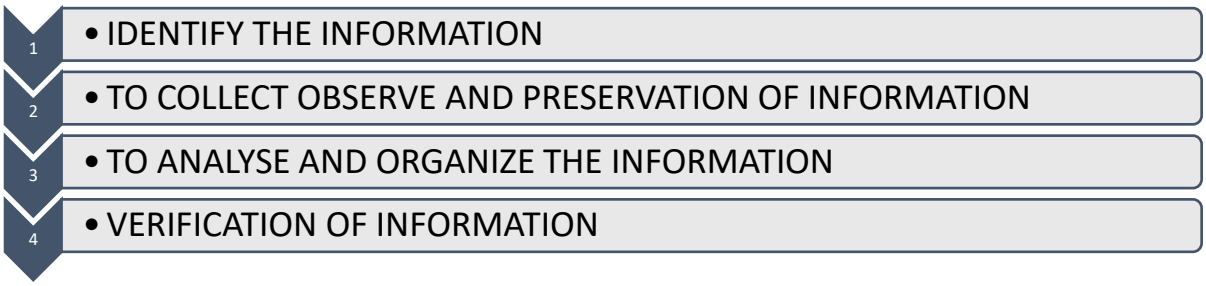
I. INTRODUCTION

The advancement of technology produces a challenge and threat to the traditional ways of collection and generation of evidences. The digital evidences are intangible in nature which is coupled with fragile. The vulnerable structure of internet posed inherent obstacles in collections and preservations of digital evidences. Due to the lacking of adequate technical-

[1] Author is an Assistant Professor at Amity Law School Amity University Haryana, India.
[2] Author is an Assistant Professor at Amity Law School Amity University Haryana, India.

 [ISSN 2581-5369]

legal skills and proficiency in collection of such evidences led to a hike in the Cyber crimes in India. Further Cyber forensics is measured for the use of investigative and analytical techniques to collect, identity& examination and produce evidence or information which is magnetically encoded or stored. The basic objective of the Cyber forensics is to perform a structured investigation while maintaining a chain of documentary evidence to find out exactly what happened on a Computer and identity of the real accused. This task is undertaken by the Cyber Analysts by the use of appropriate forensics tools and technical knowledge to recover electronic evidences according to the rules of evidence and made it to be admissible before the court of law. There are four major tasks undertaken by Cyber Analysts, working with digital evidences:



II. DIGITAL EVIDENCES AND INDIAN LEGAL FRAMEWORK

India & whole world is fascinated by the technological world. The '***Digital India Information technology Campaign'*** give equal opportunities to all to use and access information, data storage, analyze the use of Internet. This E- revolution increase the reliance on e-means of communications, e-commerce and use of data storage devices. It raised the need of transformation of existing IT laws and rules of evidence both in civil and criminal cases. A mass digital information and Cyber crimes in relation with it compelled the Indian Law to incorporate the legal provision for the application of digital evidence.

Digital &Electronic form of evidences has turn into an omnipresent part of Cyber investigations with the objective to extend further than computer-explicit crime. Regular touch with digital devices in all facade of life produces so called ***'digital exhaust'*** that can yield significant clues about relations, locality, and target of both of, victims and accused. The source of digital evidence may not easy to identify as a computer or cell phone found at the sight. Vehicle navigation systems, video game consoles and other networked devices can also contain exceptionally important data. Similarly, online user accounts without any physical connection to a crime scene can produce important information about offline actions. The recognition and preservation of digital evidence is just one junction with the lifecycle of a criminal investigation. Technical skills and infrastructure must be premeditated

 [ISSN 2581-5369]

in advance. The coordination with other functionaries of the criminal justice system such as prosecutors, defense attorneys and judges are also crucial for a successful prosecution.[3] The IT Act, 2000 and its amendments are based on United Nations Commission on International Trade Law (UNICITRAL), the model law on Electronic Commerce. The IT Act, 2000 was amended to allow the admissibility of digital evidences.

(A) Origin of Electronic Evidence

In the year 1984, the FBI first time started to use the term 'Computer evidence'. Then in year 1991, anew term- "Computer Forensics" was invented. In year 2000 India passed a new Act to deal with Cyber Law issues was passed and named as- Information Technology Act, 2000.

(B) Meaning of Digital Evidence/ E- Form of Evidence:

Section 79A of the Information Technology Act, 2000 defines the meaning of Electronic form of Evidence as- *"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, and digital fax machines.*[4]

The another meaning of E- evidence or digital evidence is- "*any probative information stored or transmitted in digital form, which a person can use in Court at trial……..It is an information of probative value which is stored or transmitted in binary form"*[5]

The term Evidence is confined not only to that found on Computer but also extended to evidence in digital devices such as E- multimedia or telecommunication devices, E-mails, Digital photographs, ATM transactions logs, E- documents, Word- processing, histories, Instant message, E- accounting programs, Spread- sheets, Internet browser, Computer memory, Computer printer, Computer back-ups, digital Videos or audio files, Mobile data, Virtual games/ Multimedia etc.[6]So there are three elements in the definition those are:

1. It includes all form of digital storage devices.
2. It include all form of digital information (data) stored in.
3. It restrict only to the relevant data or information.

---

[3] International Association Chief of Police, *Cybercrime Investigation*, LAW ENFORCEMENT CYBER CENTER, (Jan. 30, 2021, 11:04 AM), https://www.iacpcybercenter.org/officers/cyber-crime-investigations/

[4] Justice K.N.Basha 2009, Detection of Cyber Crime and Investigation . (Jan. 29, 2021, 10:04 AM), https:// www.tnsja.tn.nic.in/article/Cyber Crime by KNBJ.pdf

[5] Dubey V. Admissibility of electronic evidence: an Indian perspective. Forensic Res Criminol Int J. 2017;4(2):58-63. DOI: 10.15406/frcij.2017.04.00109

[6] Karnika Seth, *Evidentiary Value Of Sms, Mms And E-Mail, (Jan.25,2021,12.00AM)* EVIDENTIARY VALUE OF SMS, MMS AND E-MAIL, http://www.karnikaseth.com/evidentiary-value-of-sms-mms-and-e-mail.html

(C) Location of Digital and Electronic Evidences:

Generally the evidences can be found on hard disks/drives. The hard drive contains both ***Volatile*** and ***Nonvolatile*** data. The Volatile may be disappeared whenever we shut down or power off the computer system whereas Nonvolatile data stored or preserved in hard disk of system. Theseevidences may be found in hard drive in various forms like in form of files saved or created by the user e.g. spread- sheet, image, video, audio or document file, email, or calendars, files protected by the user either encrypted or password protected, files created by the computer like. Log file, hidden or back- up files and other data area e.g. Meta data.

Practical Issues with the Digital Evidence: Digital evidence tends to be more voluminous, can be easily modified, altered, difficult to destroy, potentially more expensive and more readily available.

(D) Definition of Evidence in Indian Law:

The amended definition of 'Evidence' includes 'E- record' (Sec. 3(a) of Indian evidence Act, 1872). The evidences are of two kinds- Oral or documentary. The new amended definition of documentary evidence is inclusive of e- record for the inspection of court. The term E- record has the same meaning as given to it in Sec. 2(1)(t) of Information Technology Act, 2000 which provides-

'data, record or data generated, image or sound stored, received or sent in E- form or Micro film or Computer-generated Micro fiche.[7]

(E) **Nature of Digital Evidence - *Primary or Secondary*:**

In the Indian Evidence Act, 1872, we can prove the contents of the documents either by Primary or by Secondary Evidence. The provision of Sec. 62 defines 'Primary evidence' as- 'when the document itself produced for the inspection of the Court'. And 'Secondary Evidence' in Sec. 63(2) as- 'certified copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies'.

In the case of ***State v. Navjot Sandhu***, it was held that- *'It is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the court. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service providing company can be led in evidence through a witness who can identify the signatures of the certifying officer or otherwise speak of the facts based on his personal knowledge. Irrespective of the*

[7]Sec. 2(1)(t) "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;.. IT Act, 2000. http://www.dot.gov.in

 [ISSN 2581-5369]

compliance with the requirements of section 65B…. there is no bar to adducing secondary evidence under the other provisions of the Evidence Act……..[8]

Classification of Digital Forensic tools:

We can classify the Digital forensics tools into diverse categories:

- *Internet analysis tools*
- *Database forensics tools*
- *Disk and data capture tools*
- *Email analysis tools*
- *Mobile devices analysis tools*
- *File analysis tools*
- *Registry analysis tools*
- *File viewers*
- *Mac OS analysis tools*
- *Network forensics tools*

There is also a long list of most commonly used tools for cyber forensics. These are as follows:

- *X-Ways Forensics*
- *SANS Investigative Forensics Toolkit – SIFT*
- *Plain Sight*
- *XRY- mobile forensics tool.*
- *HELIX3- is a live CD-based digital forensic suite created to be used in incident response.*
- *Digital Forensics Framework*
- *Open Computer Forensics Architecture (OCFA)*
- *CAINE*
- *Llib forensics*
- *Volatility*
- *Windows SCOPE*

[8]State NCT of Delhi vs. Navjot Sandhu @ Afsan Guru-AIR 2005 SC3 820.

 [ISSN 2581-5369]

- *The Coroner's Toolkit*
- *Oxygen Forensic Suite*
- *Bulk Extractor*
- *Xplico*
- *Cellebrite UFED*
- *EnCase*
- *Registry Recon*
- *The Sleuth Kit*
- *Mandiant RedLine*
- *Computer Online Forensic Evidence Extractor (COFEE)*

2 #Hash Values, a Useful Tool for Examination, Discovery and Authentication of Digital Evidence:

Digital evidence is taking a significant place in civil and criminal cases. The present amended law establishes new parameters regarding the protection and detection of digitally saved information. Now it important to understand- how "hash" values (or hash algorithms) being used it as a significant tool for investigation, discovering and authentication of digital evidences.

Meaning of #Hash Value:

A judicial guide defines "hash value" as: *"A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production."*

#Hash values are used during different phases regarding electronic evidence.

 [ISSN 2581-5369]

1.	*In the computer forensic examination process, a hash value is used to ensure that the examined copy has not been altered. A hash value will be taken of the original hard drive. Under accepted protocols, an image is made of the original. The image is used during the forensic examination to preserve the integrity of the original. A hash value is taken of the imaged copy before any examination. If the values are the same, then the copy is treated the same as the original. If the values are different, then the integrity of the copy is called into question. At the end of the forensic examination, a third value is commonly taken. The three hash values (original hard drive, imaged hard drive before the examination, and imaged hard drive after the examination) must match.*
2.	*#Hash values can be used to authenticate evidence introduced in court. Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication.*
3.	*#Hash values may be used during the discovery process.* [9]

(F) EVIDENTIARY VALUE OF E- EVIDENCE AND MODES OF PROOF:

Under the following head we can examine & analyze the modes of proof andAdmissibility of digital evidence and legislative arrangements made in this regards which area as follows:

Admission of Facts/ Statements:

The term 'admission' is inclusive of both oral and documentary or digital form of statements, which can be suggest a inference to any facts in issue or relevant fact. Again Sec. 22A of the Act prohibits the oral admission regarding the contents of E- records are not relevant the question in issue is reading the genuineness.

The Statement forming a part of E- record:

The Sec. 39 of Evidence Act, 1872 made that part evidence of E- record or statement can be given of so much and no more than which the court consider necessary in particular cause to the full understanding of the circumstances under which it was made. It means evidence of statement forming a part of a longer statement of a conversation or part of an isolated document, statement are contained in document that form part of a book or series of letter or papers.

[9] Federal Evidence Blog ,http://federalevidence.com/blog Highlights " Using "Hash" Values In Handling Electronic Evidence I Federal Evidence Review I." Published by Federal Evidence.com.

Electronic/Digital evidence and its admissibility:

The confined mandate of Sec. 5 of Evidence Act, 1872 says that- *'Evidence can be given only regarding facts there are in issue or there relevant, but no other facts'*.The admissibility of facts or things is a question of exclusive judicial scrutiny by the judge in Sec. 136 of Evidence Act, 1872. The Sec. 65A and 65B included in Evidence Act, 1872 after passing of Information Technology Act, 2000. Sec. 65A- provides that, the contents of E- record may be proved in accordance of Sec. 65B.

Sec. 65B provides that- *'Notwithstanding anything contained in an E- record, whether it be the contents of a document or recorded copied in optical or magnetic media produced by a computer also referred to as computer output in the Act, it is deemed to be a document and is admissible in evidence without further proof of the production of the original, providing the conditions set out in Sec. 65B (2)-(5) are satisfied.*

Pre-Conditions for Admissibility of Digital Evidence:

The Sec. 65…… (2) ... (5),Provides the pre conditions for admissibility of Digital evidence which are as follows:

Sec. 65B- Admissibility of electronic records:

(1) *…….*

(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;

(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.

(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.

(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.

(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;

 [ISSN 2581-5369]

(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: *……*

The Presumptions:

Presumption of one fact from the other is the task of court. Generally relevant or admissible fact may not be considered as 'proved facts'. It's a completely a matter of judicial appreciation and scrutiny of judge. In any trial all the facts, things, incidents, transactions cannot explain with true version for facts or circumstances under which those things happened. In that situation court can presume certain fact, things, truncations regarding these can be presumed under Section 114 of Indian Evidence Act, 1872 or under other relevant provisions of other laws. The amendment Evidence Act introduces various judicial presumptions regarding digital evidence. These are:

E- agreements: Sec. 84A provides the presumption regarding a lawful concluded contract, where the parties digitally affixed their signature to an E- record that purports to be an agreement.

Electronic Gazettes: Sec. 81A is regarding the presumption of genuineness of E- record or the official gazette directed by any law, providing the E- record form and produced from proper custody.

Digital Signature & secure E-record: Under Sec. 85B of the IT Act, 2000, the court can presume a secure E- record is unaltered since obtaining secure status where a security procedure is be applied to an e- record at a specific time. Unless contrary is proved. Under Sec. 15 of IT Act, 2000 and Sec. 85C of Indian Evidence Act, 1872, it can be presume that the subscriber intends to sign or approve the E- record when he affixed a secure digital signature.

With regard to the digital signature certificate (Sec. 8 of the Evidence Act, 1872), it is a presumption that information in the certificate is correct along with exception of specified information, was not verified, at the time of acceptance of certificate.

 [ISSN 2581-5369]

E-mails/ Electronic Message: Sec. 88A is about the presumption regarding authenticity of the E- message, not regarding the sender of the message. It is presumed regarding forwarded E- message by a sender through an E- mail server to an addressee corresponds with the message fed into the sender's computer for transmission.

Presumption regarding 5 Year old E- record: Sec. 90A is regarding the presumption of an E- record produced from the proper custody and purports to be or proved to be of five years old, that the digital signature affixed to document, was affixed by the signatory or authorized person of signatory.

Amendments made in Banker's Book Evidence Act, 1891:

The amended definition of 'banker's book' now includes the printout of data stored in disk or floppy or other electro- magnetic device as:

***Sec. 2(3) "bankers' books**" include ledgers, day-books, cash-books, account-books and all other records used in the ordinary business of the bank, whether these records are kept in written form or stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism, either onsite or at any offsite location including a back-up or disaster recovery site of both.*

Sec. 2(8) of the Act allows to obtain the certified copy of E- record be obtained. The provision says:

Sec. 2(8): "certified copy" means when the books of a bank,—

(a) *Consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of S**ection 2A**.*

(b) *a printout of any entry in the books of a bank stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such printout as a copy of such entry and such printout contains the certificate in accordance with the provisions of S**ection 2A.***

Further **Sec. 4** of the Banker's Book Evidence Act, 1891 amended to give permission admissibility of E- evidences. It says:

Sec. 4- Mode of proof of entries in banker's books

Subject to the provisions of this Act, a certified copy of any entry in a bankers book shall in all legal proceedings be received as prima facie evidence of the existence of such entry, and

shall be admitted as evidence of the matters, transactions and accounts therein recorded in every case where, and to the same extent as, the original entry itself is now by law admissible, but not further or otherwise[10].

Amendments introduced in Indian Penal Code, 1860:

A large number of Section & amendments were introduced in Indian Penal Code, 1860 after the passing,in Schedule First of Information Technology Act, 2000. These amendments were regarding production of documents, summons, and fabrication of evidence, false entry, and false statement; intentionally prevent the production of documents or other record before court, fabrication of false record to *include* the E- records. The following is the list of Sections of Indian Penal Code, 1860:

Sec. 172	Absconding to avoid service of summons or other proceeding.
Sec. 173	Knowingly preventing service of summons or other proceeding, or preventing publication thereof.
Sec. 175	Intentional omission to produce document or electronic record to public servant by person legally bound to produce it
Sec. 192	Fabrication of false evidence.
Sec. 193	Punishment for giving or fabricating false evidence.
Sec. 204	Intentionally destruction of document or electronic record to prevent its production as evidence.
Sec. 463	Forgery of documents and the evidences.
Sec. 465	Punishment for forgery.

Judicial Implications on Digital Evidence through Judicial Pronouncements:

Recording of Evidence n CDs:

In the matter of ***Jagjit Singh vs., State of Haryana(2006) 11 SCC 1***, The Haryana Legislative assembly Speaker disqualified a Member on the ground of defection. The Supreme court of India while hearing, considered and appreciated the digital form of evidence in form of

[10] https://lawyerslaw.org/the-bankers-book-evidence-act-1891/

transcripts of E- media including Aaj Tak, Zee News and Haryana News etc. and indicated the extent in paragraph no, 25 of the judgment.

Intercepted Phone Calls and its admissibility:

In the matter of ***State (NCT of Delhi) vs. Navjot Sandhu, (2005) 11 SCC 600***, an appeal was filed against the conviction held in Indian Parliament Attack on Dec, 13, 2001. In this case the apex court accepted the proof of mobile telephone calls and location tracking details.

Evidentiary Value of Video Conferences:

In the case of ***State of Maharastra vs. Dr. Praful B Desai (AIR 2003 SC 2053)***

The main issue in this case was- Whether a witness can be examines by mean of E-conferencing? The SC observed that due to advancement of science and technology, which permits live conversation with visibility with someone who is or cannot be physically present with that facility then a live E- testimony of witness can be taken with due care and caution.

Data Protection Law, Abhinav Srivastva case, Polularly known as AADHAR case:

The UIDAI entrusted with the duty of AUA (Authentication User Agency)to give certain Aadhaar enabled services by authenticating the Aadhaar card holder. They obtain data from the CIDR via ASA (Aadhaar Service Agency).

The Accused recognized vulnerabilities presented in e-hospital android app (online reservation arrangement for booking doctor/hospital arrangements). He designed his own mobile app that can connect to e-hospital app at the backend and grant e-KYC services to the users. The e-KYC generate an OTP(one time password)to the user (only individual person having access to his registered mobile number can view the demographic information).This offence is concerned with unauthorized contact to AUA and given the authentication and e-KYC API services in unauthorized manner.The above was held the violation of the section 29(2) of the Aadhaar Act, 2016 and provisions of IT Act 2000.

Search and Seizure:

In the case of ***State of Punjab vs, Amritsar Beverages Ltd. 2006 Ind Law SC 3911,*** it was judicially madeclear by the findings that the proper course of actions for the officers in such case was to prepare the copies of the hard disk or obtain a hard copy, affixed with the signatures along official seal on it, And also furnish a copy to the dealer or to the concerned person.

Deleted Files on Storage devices:

In case of ***Dharambir v. Central Bureau of Investigation*,148(2008)DLT 289**, the apex court in the judgment considerably observed that, *even if the hard disc is restored to its original position of a blank hard disc by erasing what was recorded on it, it would still seize information which identified that some text or file in any form was recorded on it at one time and consequently removed. With the use of software programmes it is probable to find out the specific time when such changes occurred in the hard disc. To that extent even a blank hard disc which has once been used in any mode, for any objective, will contain some information and will therefore be an electronic record."*[11]

SMS and Its evidentiary value:

In case of ***Rohit Vedpaul Kaushal v. State of Maharashtra,* 2007 INDLAW MUM 75**, the High Court of Bombay, Maharashtra, after exploring the SMS messages sent by the accused to the victim, it was held that- SMS sent by the accused undoubtedly go down inside the scope of Section 67 of the IT Act, hence admissible.

Evidentiary Value of IP Addresses:

In the matter of ***Sanjay Kumar Kedia v. Narcotics Control Bureau & Anr***. Para 8 and 9 Appeal (crl.) 1659 of 2007, DOD: 03/12/2007, it was held by the court that *"the Xponse Technologies Ltd and Xponse IT Services Pvt. Ltd were not acting merely as a network service provider but were actually running internet pharmacy and dealing with prescription drugs like Phentermine and Butalbital. In this situation, Section 79 will not grant immunity to an accused who has violated the provisions of the Act."*[12]

Evidentiary Value of Electronic mails:

In case of ***Nidhi Kakkar v. Munish Kakkar*(2011)162PLR113**, the main question before the court was- Whether e-mail text brought before court, is admissible as an evidence or not?

After the examination the provision of Evidence Act, 1872 and IT Act, 2000-it was observed that if person produced text of information generated through computer or any digital device, it should be permissible in evidence, if the sufficient proof was tendered in a way brought through Evidence Act. The printed edition created by wife that enclosed the text of what was significant for case was held as admissible.

[11]CRL.M.C.1775 of 2006, CRL.M.C. 1980 of 2006, CRL.M.C. 6476 of 2006, CRL.M.C. 203 of 2007, CRL.M.C. 3626 of 2007, CRL.M.C. 3657 of 2007, W.P. (CRL.) No. 1393 of 2007

[12] Sanjay Kumar Kedia v. Narcotics Control Bureau & Anr. Para 8 and 9 Appeal (crl.) 1659 of 2007, DOD: 03/12/2007

Liability of intermediary for Pornography or Restricted Contents:

In the leading case of- ***Avnish Bajaj v. State*, 116 (2005) DLT 427**, it was observed by the Apex court that- in absence of suitable content filters, that can detect the words in the inventory or the pornographic material that was being offered for sale or exhibiting, then website will have risk of being imputed to it the information that such thing was in fact obscene. The creation of the internet and the likelihood of a widespread use through instantaneous transmission of pornographic material, calls for a stringent standard are in need to be brought.

III. CONCLUSION

Cyber forensics and e-discovery are two crucial areas that have gained tremendous importance in the modern day technology crimes investigations. It is difficult to imagine a cyber crime investigation without the use of e-discovery and cyber forensics. These legislative changes and the courts' positive approach to recognizing and appreciating digital evidence indicate that India is making progress with respect to the admissibility and appreciation of digital evidence. However, it still has a long way to go if it intends to keep pace with global developments.

*****

 [ISSN 2581-5369]