



A Gateway to all Post Graduate Courses

An MHRD Project under its National Mission on Education through ICT (NME-ICT)



Subject: **Law**

Production of Courseware

e- Content for Post Graduate Courses



Paper : **Information and Communication Technology**

Module : **Digital evidence-broad principle**



ज्ञान-विज्ञान विमुक्तये



Role	Name	Affiliation
Principal Investigator	Prof. (Dr.) Ranbir Singh	Vice Chancellor, National Law University, Delhi
Co-Principal Investigator	Prof. (Dr.) G.S. Bajpai	Registrar, National Law University Delhi
Paper Coordinator	Dr. Aparajita Bhatt	Assistant Professor, National Law University Delhi
Content Writer/Author	Ms. Mrunal Dattatraya Buva	Visiting Faculty, Indian Law Institute, New Delhi
Content Reviewer	Prof. S.K. Verma	Prof. S. K. Verma (Ex-Dean), Faculty of Law, Delhi University, Former Director, Indian Law Institute, New Delhi

Description of Module

Items	Description of Module
Subject Name	Law
Paper Name	Information and Communication Technology
Module Name/Title	Digital Evidence- Broad Principles
Module Id	X
Objectives	To understand the broad principles with respect to recognition, admissibility, and mode of proof and appreciation of digital / electronic evidence in India.
Prerequisites	Digital Evidence, IT Act 2000 and 2008, Indian Evidence Act, Banker`s Book Evidence Act, concept of Cyber Forensic
Key words	Digital Evidence, Electronic Evidence, Indian Evidence Act, 1872, IT Act 2000, IT Act 2008, admissibility, appreciation, cyber forensics,



Module Overview:

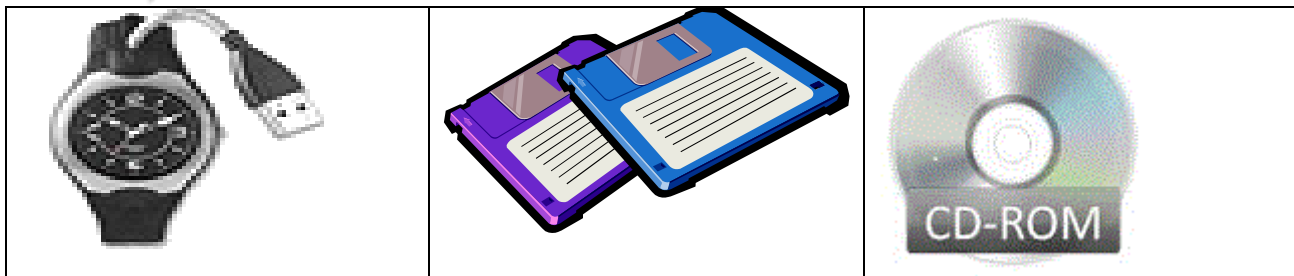
This module provides detailed discussion about the topic of digital evidence- broad principles with special reference to Indian Cyber Law. The module begins with the introduction of the topic. Chapter two to four of this module contains the discussion about the legislations and amendments with regard to digital/ electronic evidence and the development concept of digital/ electronic evidence in India, the principles of admissibility of digital/ electronic evidence, legal provisions relating to the proof of Admissibility of digital Evidence as prescribed in the Indian law etc. The fifth chapter highlights the standard of proof of digital/electronic evidence and appreciation of digital/ electronic evidence as lay down by the Indian Judiciary. Whereas, the sixth chapter talks about the Cyber forensic process, Steps involved and care should be taken while collecting the digital evidence. The last chapter of this module concludes the topic and provides some findings and solutions to the issues involved.

1. INTRODUCTION

Now days the societal communication happens through the transfer of thoughts form physical world to electronic world. The virtual world revolves around the use of information and communication technological devices such as computers, mobile phones, printers, digital cameras etc. Unlike, real world, the virtual world, causes many opportunities for the commission of offences, such as phishing, identity theft, child pornography and hacking etc. Electronic information is often relevant in proving or disproving a fact or fact at issue, the information that constitutes evidence before the court.

According to Black's Law Dictionary, evidence is "something that tends to prove or disprove the existence of an alleged fact."¹ Electronic evidence, for the purpose of this paper, may simply be defined as a piece of evidence generated by some mechanical or electronic processes. It inculcates but not restricted to e-mails, text documents, spreadsheets, images, graphics, database files, deleted files, data back-ups, located on floppy disks, zip disks, hard drives, tape drives, CD-ROMs, PDAs, cellular phones², microfilms, pen recorders and faxes etc (as mentioned in table 1 below).







As far as Indian Law of Evidence is concerned, the main issue of the 13- 14 year old Evidence Act 1872 [is that it did not have specific provisions recognizing admissibility and appreciation of digital evidence]. Substantially, it was not at par with modern technological development. Hence, to recognize transactions that are carried out through electronic data interchange and other means of electronic communication, law was *required* to be amended.



¹ Black's Law Dictionary, 8th Edition, Page 595

² Computer Forensic & Electronic Discovery Services *available at*

<http://www.setecinvestigations.com/resources/fags.php> accessed on 15th March 2012 at 12 am.

<p>Pendrive</p> 	<p>Floppy Discs</p> 	<p>CD-ROM</p> 
<p>Celluler Phone</p> 	<p>Microchips</p> 	<p>ZIP DISK</p> 
<p>Hard Drive</p>	<p>PDA</p>	<p>Tape drive</p>

(Table 1: Describing Examples of digital/ e- evidence)
(Source: Google Images)

1.1 Learning Outcome:

Learning outcome of this module would be:

- To know the legislations and amendments therein with regard to digital/ electronic evidence
- To understand the development concept of digital/ electronic evidence
- To learn Principles of admissibility of digital/ electronic evidence
- To know the Proof of Admissibility
- To find Standard of proof of digital/electronic evidence
- To identify Appreciation of digital/ electronic evidence by the Court
- To discover Cyber forensic process

2. Enactment of IT Act, 2000 and Amendments with reference to digital evidence:

This section deals with the principles governing admissibility of electronic evidence within the legal framework of the Indian law of evidence. In the year 2000, Parliament enacted the Information Technology Act 2000 (IT Act) to allow for the admissibility of digital evidence³, which amended the Indian Evidence Act 1872 (IEA), the Indian Penal Code, 1860 (IPC) and the Banker's Book Evidence Act 1891. In order to make the electronic evidence admissible, the definition of 'evidence' has been amended to include electronic records⁴. The term 'electronic records'⁵ provides for data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche. The

³ The IT Act is based on the United Nations Commission on International Trade Law (UNCITRAL)' Model Law on Electronic Commerce , 1996.

⁴ Section 3(a) of *infra* note 14

⁵ Sec. 2(1) (t)



term “Electronic form”⁶ means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device; whereas the term “Information”⁷ includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film, or computer generated micro fiche.

2.1 Legislative Mandate: Mode of Proof and Admissibility of Electronic Evidence under IEA

Now, let us see the provision of Indian Evidence Act to see what our statute says on the issue of mode of proof of electronic evidence.

2.1.1 Admissions:

Now, the term ‘admission’⁸ includes a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or of relevance. Section 22A provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic record produced is in question.

2.1.2 Statement as Part of Electronic Record:

When any statement is part of an electronic record⁹ the evidence of the electronic record must be given as the court considers it necessary in that particular case to understand fully the nature and effect of the statement and the circumstances under which it was made. This provision deals with statements that form part of a longer statement, a conversation or part of an isolated document, or statements that are contained in a document that forms part of a book or series of letters or papers.

2.1.3. Admissibility of electronic evidence:

Section 5 of the Evidence Act provides that evidence can be given regarding only facts in issue or of relevance. Whereas, section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B, Section 65B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record, i.e., the contents of a document or communication printed on paper that has been stored, recorded and copied in optical or magnetic media produced by a computer output, is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set out in Section 65B (2) to (5) are satisfied. Section 136 empowers a judge to decide on the admissibility of the evidence.

2.1.4 Conditions for the admissibility of electronic evidence:

Before a computer output is admissible in evidence, the following conditions as set out in Section 65(B) (2) must be fulfilled:

- (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

⁶ Sec. S.2(1)(r)

⁷ Sec..2(1)(v)

⁸ Section 17 of the Evidence Act, 1872

⁹ Section 39 of the Evidence Act



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 (4) provides that in order to satisfy the conditions set out above, a certificate of authenticity signed by a person occupying a responsible official position is required, which must identify the electronic record containing the statement; describe the manner in which it was produced; give such particulars of any device involved in the production of the electronic record by a computer and deals with any of the matters to which the conditions for admissibility relate.¹⁰

1.1.5 Presumptions Regarding Electronic Evidence:

A fact which is relevant and admissible need not be construed as a proven fact. The judge must appreciate the fact in order to conclude that it is a proven fact. The exception to this general rule is the existence of certain facts specified in the Evidence Act that can be presumed by the court as mentioned below:.

2.1.5.1 Gazettes in electronic form:

Under the provisions of Section 81 A of the Evidence Act, the court presumes the genuineness of electronic records purporting to be from the Official Gazette or any legally governed electronic record, provided that the electronic record is kept substantially in the form required by law and is produced from proper custody.¹¹

2.1.5.2 Electronic agreements:

Section 84A¹² provides for the presumption that a contract has been concluded where the parties' digital signatures are affixed to an electronic record that purports to be an agreement.

2.1.5.3 Secure electronic records and digital signatures:

Section 85B of the Evidence Act provides that where a security procedure has been applied to an electronic record at a specific time, the record is deemed to be a secure electronic record from such time until the time of verification. Unless the contrary is proved, the court is to presume that a secure electronic record has not been altered since obtaining secure status. The provisions relating to a secure digital signature are set out in Section 15 of the IT Act. It is presumed that by affixing a secure digital signature the subscriber intends to sign or approve the electronic record. In respect of digital signature certificates (Section 8 of the Evidence Act) , it is presumed that the information listed in the certificate is correct, with the exception of information specified as subscriber information that was not verified when the subscriber accepted the certificate.

¹⁰ Indian Evidence Act, 1872 (as amended in 2000)

¹¹ *Ibid*

¹² *Supra note 12*



2.1.5.4 Electronic messages:

Under section 88A, it is presumed that an electronic message forwarded by a sender through an electronic mail server to an addressee corresponds with the message fed into the sender's computer for transmission. However, there is no presumption regarding the person who sent the message.¹³

2.1.5.5 Five-year old electronic records:

The provisions of Section 90A of the Evidence Act makes it clear that where an electronic record is produced from the custody which the court considers to be proper and purports to be or is proved to be five years old, it may be presumed that the digital signature affixed to the document was affixed by the signatory or a person authorized on behalf of the signatory. An electronic record can be said to be in proper custody if it is in its natural place and under the care of the person under whom it would naturally be. The same rule also applies to evidence presented in the form of an electronic copy of the Official Gazette.

3. Changes to Banker's Book Evidence Act, 1891:

Now, the definition of 'banker's book' under Section 2(3) includes the printout of data stored on a floppy disc or any other electro-magnetic device. Section 2A provides that the printout of an entry or a copy of a printout must be accompanied by a certificate stating that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager, together with a certificate from a person in charge of the computer system, containing a brief description of the computer system and the particulars of its safeguards.¹⁴

3.1 What is permissible as evidence?

A certified copy of any entry in a banker's book shall in all legal proceedings be received as evidence of the original entry itself (Section 4)

3.2 Is banker's book in electronic form?

Any record 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 {Section 2(3)}.

3.3 How a certified copy of electronic record be obtained? {Section 2(8)}

–A copy obtained through mechanical process can be certified, if it is a certified by the principal accountant or the manager of the bank.

–A printout containing a certificate in accordance with Section 2A.

3.4 Nature of certificate for a copy obtained through mechanical process:

–A certificate from principal accountant or manager of the branch that the mechanical or other process adopted to obtain the copy has ensured the accuracy of the copy.

–Authenticity certificate from principal accountant or branch manager, and

–Certificate from person- in-charge of computer system regarding safeguard to protect computer system

¹³ *Supra note 12*

¹⁴ The Bankers Book Evidence Act, 1891 as amended in 2000



4. Changes in Indian Penal Code, 1860:

With the adoption of the IT Act, 2000, a number of offences were introduced under the provisions of the First Schedule of the IT Act, and amended the Indian Penal Code (IPC) with respect to offences for the production of documents that have been amended to include electronic records. The range of additional offences includes absconding to avoid the production of a document or electronic record in a court (section 172, IPC); intentionally preventing the service of summons, notice or proclamation to produce a document or electronic record in a court (section 173, IPC); intentionally omitting to produce or deliver up the document or electronic record to any public servant (section 175, IPC); fabricating false evidence by making a false entry in an electronic record or making any electronic record containing a false statement, intending the false entry or statement to appear in evidence in judicial proceedings (sections 192 and 193, IPC); the destruction of an electronic record of a person's secrets or destroys an electronic record, or obliterates or renders illegible the whole or part of electronic record with an intention of preventing the record from being produced or used as evidence (section 204, IPC); making any false electronic record (section 463 and 465, IPC)¹⁵

5. Implications through Judicial Decisions

Despite the admissibility of electronic records in evidence, the courts are finding it difficult to cope up with the issue of integrity and authenticity of the electronic evidence to attach weight to it.

5.1 Admissibility of printout prior to IT Act:

In TADA COURT (MUMBAI) –Bombay Bomb Blast Case regarding Sanjay Dust's call records, the court observed that the print-outs are not a copy of the magnetic tape because the tape by itself cannot be termed as a document. It does not fall within the definition of a document under section 3 of Indian Evidence Act. It was, therefore, ruled that the print-outs were primary evidence.

5.1.1 Admissibility

In *State of Gujarat v. Shailendra Kamal Kishor Pande & Ors.*,¹⁶ the Supreme Court held that the CD itself is primary and direct evidence admissible. For consideration of the CD as evidence, it has to be proved that the same has been prepared and preserved safely by independent authority like police. In another case, *M/s V. S. Lad and Sons v. The State of Karnataka & Ors.*,¹⁷ even the 'satellite sketches' produced in support of allegations was held admissible for evidence. It would be appropriate to mention that the Hon'ble Supreme Court in the case of *P. Padmanabh v. M/s Syndicate Bank Ltd*¹⁸ disbelieved the extract of the transaction in the ATM machine for want of compliance with the provisions of Sec. 65 B (4) of the Indian Evidence Act and held thereby that unless *clear admission of malfunctioning of either ATM machine or computer.....provisions of section 65B cannot be pressed into service by plaintiff*".

¹⁵ Karia D. Tejas, Digital Evidence: An Indian Perspective, 5 Digital Evidence and Electronic Signature Law Review 214 (2008)

¹⁶ 2008 CRI.L.J. 953

¹⁷ 2009 CRI.L.J. 3760

¹⁸ AIR 2008 Karnataka 42



In *M/s. P. R. Transport Agency v. Union of India*¹⁹ it was held that the acceptance of the tender, communicated by the respondents to the petitioner by e-mail, will be deemed to be received by the petitioner at Varanasi or Chandauli, where the petitioner has his place of business. In *Nestle S.A. and Anr v. Essar Industries and Ors.*²⁰ the plaintiffs sought to prove the electronic data already on record and the updated electronic data under Sub-section 1 of Section 65B after complying with the provisions of Sub-section 4 by filing affidavit of an officer accompanied by the requisite certificate

5.2 Tape Recordings

The Supreme Court of India in the case of *Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdass Mehra*²¹ has observed that tape recorded speeches constitute a document as defined by section 3 of the Evidence Act, which stand on the same footing as photographs, and they are admissible in evidence on satisfying certain conditions with respect to identification, accuracy and relevancy of the voice recording.

Thus prior to the amendment, the court used to fall back upon on the basic provisions to decide the admissibility and value of such record.

Following are the judicial trends, after the amendment regarding admissibility and appreciation of digital evidence has been done in to the Indian Evidence Act, 1872.

5.3 Search and seizure

In the matter of *State of Punjab v Amritsar Beverages Ltd*²², it was held that the proper course of action for officers in such circumstances was to make copies of the hard disk or obtain a hard copy, affix their signatures or official seal on the hard copy and furnish a copy to the dealer or person concerned. ”

5.4 Evidence Recorded On CD

In *Jagjit Singh v State of Haryana*²³, it was held that the electronic evidence placed on record was admissible and upheld the reliance placed by the speaker on the recorded interview when reaching the conclusion that the voices recorded on the CD were those of the persons taking action.

In *Anvar P.V. v. P.K. Basheer and others*²⁴, the appellant sought the direction to set aside the election of the elected candidate on account of corrupt practice and produced CDs which were made after recording the speeches, songs and announcements using other instruments and by feeding them into a computer. It was held that since the CDs produced were not certified, the same were not admissible as secondary evidence. While, deciding the admissibility of the secondary evidence pertaining to electronic evidence, the 3-judge bench of R.M. Lodha, CJ and Kurian Joseph and R.F. Nariman, JJ overruled the ruling of the Court in *State (NCT of Delhi) v. Navjot Sandhu*²⁵, to that extent. The bench noted that the Court in the aforementioned case omitted to take note of Sections 59 and 65A of the Evidence Act, 1872 and hence erred in holding that that irrespective of the compliance with the requirements of Section 65B, which is a

¹⁹ AIR 2006 ALLAHABAD 23

²⁰ I.A.No.3427/2005 in CS(OS) No.985/2005

²¹ AIR 1975 SC 1788

²² 2006 IndLaw SC 3911

²³ AIR2007SC590

²⁴ CIVIL APPEAL NO. 4226 OF 2012, DOD: 18.09.2014

²⁵ AIR 2005 SC 3820



special provision dealing with admissibility of the electronic record, there is no bar in adducing secondary evidence, under Sections 63 and 65 of the Evidence Act, of an electronic record.

While, overruling the legal position as to electronic evidence as laid down in *Navjot Sandhu Case*, the Apex Court, applying the principle of *generalia specialibus non derogant* (special law will always prevail over the general law), held that the evidence relating to electronic record being a special provision, the general law on secondary evidence under Section 63 read with Section 65 of the Evidence Act shall yield to the same.

5.5 Admissibility of Intercepted Telephone Calls

The case of *State (NCT of Delhi) v Navjot Sandhu*²⁶ (overruled), dealt with the proof and admissibility of mobile telephone call records. A submission was made on behalf of the accused that no reliance could be placed on the mobile telephone call records, because the prosecution had failed to produce the relevant certificate under Section 65B(4) of the Evidence Act. The Supreme Court concluded that *a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records.*

In the matter of *Ravi Kant Sharma and Ors. v. State*²⁷ It was held that call details record is not a direct computer printout of the data available in the computers/servers of the telephone company. As the telephone data has been tampered with, it cannot be relied upon to base conviction of the accused persons.

5.6 Examination of a Witness by Video Conference

In *State of Maharashtra v Dr Praful B Desai*²⁸, the court allowed the examination of a witness through video conferencing. Again, in *Amitabh Bagchi v. Ena Bagchi*²⁹, it was held by the court that the Sections 65A and 65B provide provisions for evidences relating to admissibility of electronic records, and it includes video conferencing.

5.7 Digital Signatures

In *Bodala Murali Krishna v.Smt. Bodala Prathima*³⁰ the court held that, "... Sections 67-A and 73-A were introduced as regards proof and verification of digital signatures. As regards the presumption to be drawn about such records, sections 85-A, 85-B, 85-C, 88-A and 90-A were added. ***These provisions are to recognize the electronic records and digital signatures, as admissible pieces of evidence...***"

²⁶ *ibid*

²⁷ 2011 V AD (Cr.) 75

²⁸ AIR 2003 SC 2053

²⁹ AIR 2005 Cal 11

³⁰ 2007(2)ALD 72



5.8 Deleted Files on Hard Disk



*Dharambir v. Central Bureau of Investigation*³¹ the judgment significantly notes 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 retain information which indicates that some text or file in any form was recorded on it at one time and subsequently removed. By use of software programmes it is possible to find out the precise time when such changes occurred in the hard disc. To that extent even a blank hard disc which has once been used in any manner, for any purpose will contain some information and will therefore be an electronic record.”

5.9 Admissibility of SMS:

*In Rohit Vedpaul Kaushal v. State of Maharashtra*³² the Bombay High Court, after examining the SMS messages sent by the accused held: “ that some of the SMS sent by the accused certainly fall within the scope of Section 67 of the IT Act ”

5.10 Email as E-Evidence

*In Mrs. Nidhi Kakkar v. Munish Kakkar*³³, the issue before the court was whether; text of emails produced in Court was admissible evidence. It was held by the hon`ble court that if person produced text of information generated through computer, it should be admissible in evidence, provided proof was tendered in a manner brought through Evidence Act. Printed version produced by wife that contained text of what was relevant for case was held as admissible.

5.11 Supply of documents in Digital form:

*In Ujjal Dasgupta v. State*³⁴ it was held by the High Court of Delhi that “...the accused has right to be provided with the copies of Supply of documents relied upon by prosecution which are in digital form in pen drives and hard discs to the accused...”

5.12 IP Address:

*In Sanjay Kumar Kedia v. Narcotics Control Bureau & Anr.*³⁵, 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

³¹ 148(2008)DLT 289

³² 2007 INDLAW MUM 755

³³ (2011)162PLR113

³⁴ 150 (2008) DLT 60

³⁵ Para 8 and 9 Appeal (crl.) 1659 of 2007, DOD: 03/12/2007



Butalbital. In this situation, Section 79 will not grant immunity to an accused who has violated the provisions of the Act.”

5.13 Pornography Material and Intermediary’s liability

In the case of *Avnish Bajaj v. State*³⁶, it was held by the court that by not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene. The proliferation of the internet and the possibility of a widespread use through instant transmission of pornographic material, calls for a strict standard having to be insisted upon.

5.14 Expert Opinion:

A new section 79A has been added in to the IT Act 2000., which provides that the Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.³⁷

One of the pieces of circumstantial evidence sought to be relied by the prosecution in the *Pramod Mahajan Murder Trial*, learned trial Court of Bombay, dismissed the submission that a SMS is inadmissible as valid evidence, as the practical demonstration was conducted by defense witness, who was “not an expert” as per law.

5.15 E-Evidence whether Primary or Secondary:

Under the Evidence Act, the contents of documents may be proved either by primary or secondary evidence. Section 62 of the Act defines “Primary evidence” as “...the document itself produced for the inspection of the Court”. The Act, also defines, “Secondary Evidence” [section 63(2)] as the “*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 *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 compliance with the requirements of section 65B.... there is no bar to adducing secondary evidence under the other provisions of the Evidence Act...*”

5.16 Aids and Interpretation

³⁶ 116 (2005) DLT 427, also see Sharma Vakul, *Information Technology – Law & Practice* (Universal Law Publishing, 2009).

³⁷ IT Amendment Act 2008



In *Ponds India Ltd. v. Commissioner of Trade Tax, Lucknow*³⁸, it was mentioned by the Hon`ble Court that “Wikipedia, like all other external aid to construction is not an authentic source,”

5.17 Evidence as per Banker`s Book Evidence Act

In *State Bank of India v. Rizvi Exports Ltd* (DRT, Allahabad)³⁹, the SBI had filed a case to recover money from some persons who had taken loans and submitted printouts of statement of accounts maintained in SBI’s computer systems as a part of evidence. The relevant certificates as mandated by the Bankers Books of Evidence Act, had not been attached to these printouts. The Court held that these documents were not admissible as evidence.

6. Cyber Forensic Processes⁴⁰

What is cyber forensics? :

Cyber forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable in any judicial or administrative hearing. Cyber forensic is divergent from traditional branches of forensic science.

Do`s and Don`ts , required to be followed during Cyber forensic processes	
1.	Never work on digital evidence
2.	Do not have a long span
3.	Methodology for analysis is case dependent

Table 1: Describes about the Do`s and Don`ts , required to be followed during Cyber forensic processes

Following are Cyber Forensics Labs where electronic records can be taken for obtaining certificate:

- 3 Labs at Hyderabad
- 1 Lab at Trivandrum
- 1 Lab at CBI, Delhi
- 1 Lab at Himachal
- 1 Lab at Ahmadabad
- 1 Lab at Mumbai

6.1 Six Stages of the Cyber Forensic Process

1. Identification: To know the digital evidence
2. Acquire : logical backup, copy the directories & files of a logical volume, not to capture deleted files, physical backup, i.e., disk imaging/ cloning/mirror image, Exhibit Computer. he Government hard disk is to be used to store the Image of the exhibit HDD. By using Write Protection device, the original hard disk can be free from contamination, The original should be exhibited.

³⁸ (2008) 8 SCC 369

³⁹ II (2003) BC 96

⁴⁰ Pandyalaya Krishnashastry, Power Point Presentation, available at

https://www.dsci.in/sites/default/files/Krishna%20Sastry%20Pendyalaya_cyber%20crime%20_case%20studies.pdf

accessed on 18 Aug 2014 at 5 AM. also see Pandyalaya Krishnashastry, Cyber Cime-digital evidence and Cyber Forensics available at <https://www.wirc-icai.org/material/COMPUTER%20FORENSICS.pdf> accessed on 20 August 2012 at 4 PM.

3. Authenticate: If the hash value is justified, the duplicate is authentic. Hash value is an Alpha-numeric number, it's a digital fingerprint. For the acquisition and verification of hash value, the software Md5 is replaced with SHA2 to calculate hash value
4. Analyze: Extract, Process, Interpret
5. Document: *Report should clearly list:* software's used and versions, contain hash results, all storage media numbers, model make, supported by photographs.
6. Testimony: Expert Opinion

6.2 Common Investigation Mistakes

1. Failure to collect and preserve the electronic evidence
 - The electronic files which are part of 'captured' computer, devices or media are isolated in a sanitized environment.
 - The replica/mirror image of the hard disks of computers, which have been seized by the investigating authorities to be deposited with the court.
 - The Hon'ble Court may take an appropriate decision with regard to such replica/mirror image would also be supplied to the accused under s.207 of Cr.P.C.,
2. Failure to label the electronic devices/media etc.
3. Failure to calculate the hash function[or value?] of the collected electronic data.
4. Failure to record details of computer forensic examination(s) in the charge sheet may lead to discharge or even acquittal of the accused.

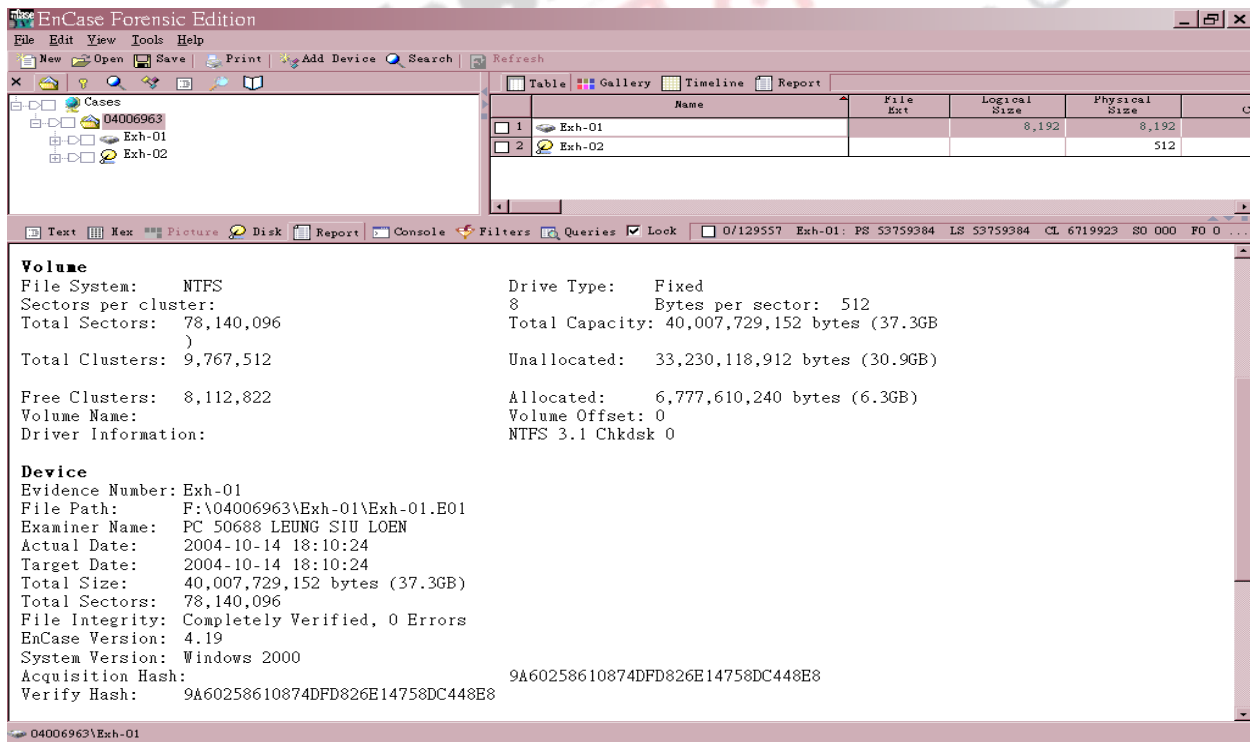
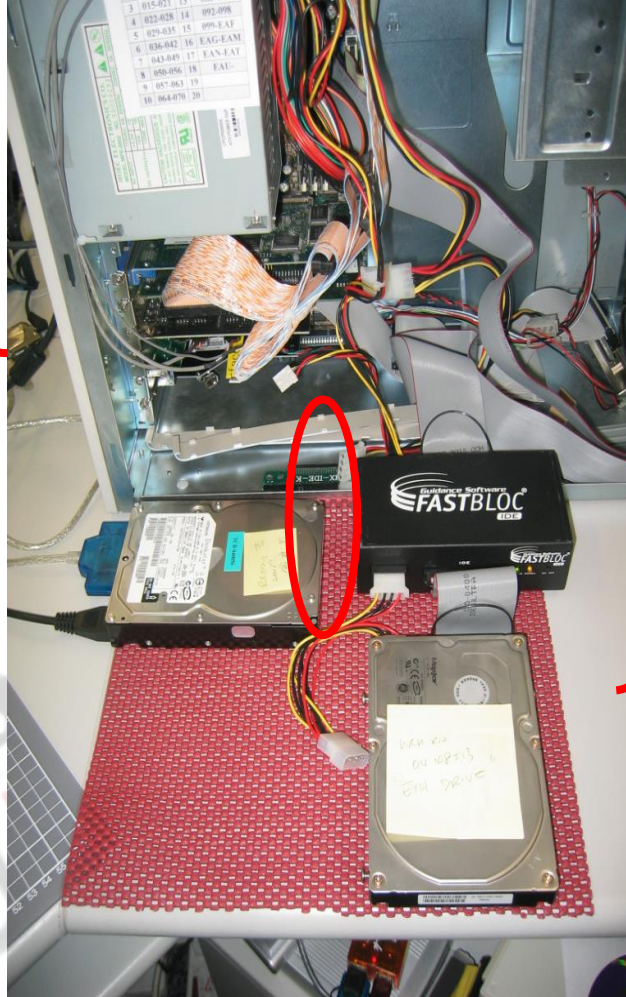


Image 1: Describing Cyber Forensic Report⁴¹

⁴¹ *Ibid*

Exhibit Computer

The Government hard disk is used to store the Image of the exhibit HDD



By using right Protection device the original hard disk can be free from contamination

The original

7. Conclusion

Once digital/ electronic evidence is admitted, the presiding officer has to decide what evidential weight to attach thereto. The following cautionary observations of the Law Commission of England are relevant here “if computer output cannot relatively readily be used as evidence in criminal case, much crime would in practice be immune from prosecution. On the other hand, computers are not infallible. They do occasionally malfunction.”⁴³ Though the Indian Evidence Act cannot be withered away in the era of new technological developments, as suitable amendments have been incorporated; the need of the hour is to fill

⁴² Ibid

⁴³ Hon’ble Thiru. Justice Sathasivam P., Supreme Court of India, Appreciation of Evidence including Evidence recorded through Electronic Media for Sessions Cases: Lecture delivered during Training Programme for District Judges Under the aegis of 13th Finance Commission Grant at Tamil Nadu State Judicial Academy on 26.03.2011



the gaps where no law exists and to reduce it into writing where judicial pronouncements have held up the system so far. Therefore one has to be cautious while appreciating digital/electronic records.

Summary

With advent in technology, it was necessary to enact a new law and amend the old law to deal with the issue of cybercrime. Hence by enacting the IT Act, 2000 and amending the statutes such as Indian Evidence Act, 1871, IPC, 1860 and Banker`s Book Evidence Act, 1891, certain provisions are provided to ascertain standard of proof and appreciation of electronic evidence, i.e., evidence in electronic form. For the purpose of admissibility of electronic record, a *three prong test* is important for Prosecution:

1. Document in question is an electronic record,
2. Produced by a computer, and
3. Accompanied by a certificate, fulfilling the conditions laid down S.65 (B)(2)-(B)(4) of the IT Act or proven by way of secondary evidence.

While deciding various cases, Courts have recognized the electronic evidence in various form such as CD`s, emails, tape records, IP address, telephone records etc., So also certain steps are required to be followed and care should be taken while collecting the e-evidence. Although the present law of evidence has been amended, the law will have to be amended as and when required with new technological development.

