Electronic evidence and its challenges

By Dr. Swarupa Dholam

Abstract :

This article begins with meaning of electronic evidence and some related concepts. The first hindrance while dealing with electronic evidence is to understand the meaning of some technical terms frequently used in technological world. A digital evidence specialist can make a range of digital evidence available from a computer. Further part of article provides an outline of some types of electronic evidence. There are a number of discreet elements that accompany the collection and handling of digital evidence. Therefore, this article includes certain guidelines for handling digital evidence. Further, section of this article is on analysis of digital evidence because failure to assess the digital evidence can lead to false assumptions. Challenges to the authenticity of electronic evidence is also included. List of case laws helps to observe the developments in focusing the issue of electronic evidence by judiciary.

Introduction :

Today, virtually every crime has an electronic component in terms of computers and electronic technology being used to facilitate the crime. Computers used in crimes may contain a host of evidence related to the crime, whether it is a conventional crime or a terrorist act. In light of this, judicial officers should not become complacent with individuals or their environment simply because the crime may involve a computer. Judiciary should provide assurance to litigants, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. The influence of electronic media has been spread over all branches of society including law and the judiciary.

Maintaining the integrity of electronic evidence throughout the process of investigation and trial presents different problems from the handling of traditional physical or documentary evidence. Some common problems are greatly exacerbated by the complexity of networked computers. This article does not address the unique issues resulting from networked environments but focuses on selected issues of maintaining the integrity of information taken from stand-alone electronic media. Electronic documents are easy to manipulate: they can be copied, altered, up-dated, deleted (deleted does not mean expunged) or intercepted.

The judge must be able to understand and appreciate that the information obtained from the media is a true and accurate representation of the information originally contained in the media irrespective of whether the acquisition was done entirely by law enforcement or in part or entirely by a civilian witness or victim.

This article does not contain interpretation of any existing law. But it gives idea to interpret those provisions related to electronic evidence.

What is meant by electronic evidence :

The type of evidence that we are dealing with has been variously described as 'electronic evidence', 'digital evidence' or 'computer evidence'.

The word digital is commonly used in computing and electronics, especially where physical-world information is converted to binary numeric form as in digital audio and digital photography.

Definitions of digital evidence include 'Information of probative value stored or transmitted in binary form; and 'Information stored or transmitted in binary form that may be relied on in court. While the term 'digital' is too wide, as we have seen the use of 'binary' is too restrictive, because it only describes one form of data.

> Electronic evidence : data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.

This definition has three elements. First, it is intended to include all forms of evidence that is created, manipulated or stored in a product that can, in its widest meaning, be considered a computer, excluding for the time being the human brain. Second, it aims to include the various forms of devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition will include any form of device, whether it is a computer as we presently understand the meaning of a computer; telephone systems, wireless telecommunications systems and networks, such as the Internet; and computer systems that are embedded into a device, such as mobile telephones, smart cards and navigation systems. The third element restricts the data to information that is relevant to the process by which a dispute, whatever the nature of the disagreement, is decided by an adjudicator, whatever the form and level the adjudication takes. This part of the definition includes one aspect of admissibility – relevance only – but does not use 'admissibility' in itself as a defining criteria, because some evidence will be admissible but excluded by the adjudicator within the remit of their authority, or inadmissible for reasons that have nothing to do with the nature of the evidence – for instance because of the way it was collected. The last criteria, however, restricts the definition of electronic evidence to those items offered by the parties as part of the fact finding process.

Meaning of some technical terms :

The first hindrance while dealing with electronic evidence is to understand the meaning of some technical terms frequently used in technological world. It is every important to understand the function of machine and its operating procedure.

THE COMPUTER :

The term 'computer' is often used generically to describe almost any form of processing unit. However, not all devices are appropriately termed a computer. For the purposes of this text, a computer can be defined in terms of a set of characteristics that illustrate how it functions. This account is sometimes called an input-processing-output model :

(a) It receives an input of some sort, by way of a local file, mouse, keyboard or through a communication channel (such as a network connection).
(b) It processes the information.
(c) It produces an output to a local file or a printer, for instances.
(d) It must be able to store information.
(e) It must be able to control what it does.

DATA STORAGE :

The increasingly varied ways of storing computer data and the variety of storage contexts means that locating relevant data as prospective evidence may not be a simple matter. Data may be stored locally to a computing device, such as on the hard disk, DVD or CD-ROM, but may also be stored on removable storage devices such as flash drives, memory sticks, or micro memory devices (as commonly found in smart phones). Of concern to many digital investigators is the difficulty inherent in locating and obtaining access to data legally that is stored remotely from an individual's computer, such as on a remote network or 'cloud' facility.

DATA FORMATS :

Computer data may be broadly classified into binary data, where the information is handled as a number represented in binary form, and text data, including alpha, numeric and punctuation data. Text can be entered into the computer by a range of methods :

(a) The typing of letters, numbers and punctuation, mainly when using the keyboard.
(b) Scanning a page with an image scanner and converting the image into data by using optical character recognition ('OCR') software.
(c) Using a bar code. The bar code represents alphanumeric data. The bar code is read with an optical device called a wand. The scanned code is converted into binary signals, enabling a bar code translation component to read the data.
(d) Reading the magnetic stripe on the back of a credit card.
(e) Voice data, where a person speaks into a microphone capable of recording the sounds. This form of data, as well as video data, is encoded in binary form.
(f) Recent developments in software and signal processing mean that speech to text is a further possibility. In this instance, the user speaks into a microphone that is connected to the computer and a dedicated software application analyses the input signal and converts this to a textual representation of the spoken words.

Internet applications such as email and the World Wide Web often manage the encoding and conversion of data from one format to another in order to facilitate easy network transfer and convenience of presentation to the user.

COMPUTER STORED AND COMPUTER GENERATED :

Computer-stored evidence includes documents and other records that were created by a human being and that just happen to be stored in electronic form. Examples include word processing files, e-mail messages, and Internet chat room messages. This kind of evidence may raise both authentication and hearsay issues. Computer- generated

evidence consists of the direct output of computer programs. Examples include the login record of an Internet Service Provider, automated telephone call records, and automatic teller receipts. These records do raise authentication issues but are not properly regarded as hearsay because they are not the statement of a person. Finally, some records may contain a combination of computer-stored and computer-generated evidence. For example, a financial spreadsheet contains both the input data that originated from a person and the output of the computer program. Such evidence therefore presents both kinds of issues. Another category of evidence, computer-generated evidence prepared for trial, also presents distinct issues, and is discussed below.

METADATA :

Metadata is, essentially, data about data. In electronic documents, metadata tends to be information that is hidden from the replication of the text as viewed on a screen. Physical documents can be subject to intensive scrutiny, and the data contained on the document can be analysed in great detail.

Types of evidence available on a computer :

A digital evidence specialist can make a range of digital evidence available from a computer. This section provides an outline of some types of evidence that can be gleaned.

FILES AND LOGS :

A wide range of application software is used on a computer, including programs that enable a user to prepare spreadsheets, databases, text documents, graphic files, multimedia and presentations. The files themselves include digital evidence, as do system logs. A great deal of data can be retrieved, depending on the method of storage, the media it is stored on and how the device manages data storage.

DOCUMENTS AND FILES CREATED OR MODIFIED BY THE USER :

Files containing text can be searched for keywords; forensic tools can then be used to view the 'metadata' : that is, the data that describes or interprets the meaning of data. The metadata can include information such as the storage location of the file on the disk, the last user to modify the file, and the date and time the file was originally created.

SYSTEM AND PROGRAM FILES :

A system file in computing is a critical computer file without which a computer system may not operate correctly. These files may come as part of the operating system, a third-party device driver or other sources. Specific example of system files include the files with .sys filename extension in MS-DOS and Windows, the *System suitcase* on Mac OS and the files located in sys, the root folder of the Linux file system, sysfs.

Program Files is the directory name of a standard folder in Microsoft Windows operating systems in which applications that are not part of the operating system are conventionally installed. Typically, each application installed under the 'Program Files' directory will have a subdirectory for its application-specific resources.

TEMPORARY FILES AND CACHE FILES :

When a computer connects to the Internet, a range of information is recorded and retained in different locations, including a list of the websites that have been visited. Temporary files of websites that have been visited are stored in cache folders.

DELETED FILES :

File systems keep a record of where data are located on a disk. The way data are stored will differ, depending on the operating software and the architecture of the method used to allocate blocks of storage for files. In simple terms, the location of data on a disk is controlled by a file system.

NETWORKS :

Gone are the days when most computers stood alone on a desk. The majority of computers are now connected, or are intermittently connected, to some form of network. The trials left by the assortment of logs and files in computers can produce digital evidence in abundance, including use of email, connecting to the Internet and viewing websites, and the transfer of files between computers. Other sources of digital evidence can be obtained from server.

Types of network -

(a) *Internet* - The Internet is a global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link several billion devices worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to-peer networks for file sharing.

(b) *Corporate intranets* - An intranet, usually run by a large organisation, is a network that is based on the Internet protocols. In Principle, an intranet is only available to members, employees or others with authorisation to enter it and use the information contained on the intranet.

(c) *Wireless networking* - Wireless networking is also known as Wi-Fi meaning wireless fidelity.

(d) *Cellular networks* - The technology that enables devices to transfer data between a computer and a cellular telephone, and between cellular telephones, is developing rapidly.

(e) *Dial-up* - Occasionally, computers are still connected to the Internet by means of the traditional copper telephone line.

DATA DESTRUCTION :

Data destruction is the most obvious and most widely discussed anti-forensics measure, and has created a considerable legal and technological debate. Unlike a physical object or piece of paper that can be destroyed effectively, it is much more difficult to obliterate a document in electronic format. All a user does when they click the 'delete' icon on a computer is, in general terms, remove the pointer to the data. The document or data remains, and it is possible to retrieve this data in certain circumstances, even if it is partly overwritten.

FALSIFYING DATA :

Tampering with evidence is not new. An early example of erasing part of a tape recording and re-recording part of a conversation occurred.

Such attempts to adduce fraudulent evidence before a court are rare, but increasing. However, it is conceivable, given the ease with which electronic data is so easily manipulated and altered, that attempts will be made in the future to falsify and alter documents before a trial takes place.

HIDING DATA :

Tampering with and destroying data work best when the criminal no longer needs the data. For possession crimes such as the possession of illegal images, this is not possible. Hiding the data rather than destroying or altering it therefore, becomes an important objective. Cryptography is the best known anti-forensic method to hide data from third parties.

Guidelines for handling digital evidence :

A number of guidelines, papers and other projects have been undertaken and published in relation to the collection and handling of digital evidence, and the digital forensic community has argued for a global response to the issue. As with any other form of evidence, there are a number of discreet elements that accompany the collection and handling of digital evidence.

Step 1. Identifying digital evidence :

Evidence discovered in digital format may be the first sign that something is wrong. For instance, a security administrator to a bank might consider an investigation may be needed where the intrusion detection system sets off an alarm, or where the email logs indicate that a particular member of staff is receiving an excessive number of emails during a day or over an extended period.

In such a case, the source and reliability of the information needs to be assessed, which requires an investigation into the facts.

Step 2. Gathering digital evidence :

Once it has been established that it is necessary to seize or gather evidence in digital format, a further set of procedures should be in place to guide the digital evidence specialist in respect to the scene itself, including the identification and seizure of the evidence if necessary.

It is important not to permit anybody to disturb the hardware or the network, or work on a computer that is liable to being seized and retained, and it is admissible that the police officers that are engaged in searching for digital evidence should be properly trained.

Data can be deleted on a remote server or cloud storage before it can be secured.

There are two fundamental principles in relation to copying digital evidence that a digital evidence specialist should be aware of :

(a) The process of making the image should not alter the original evidence. This means that the appropriate steps should be taken to ensure that the process used to take the image should not write any data to the original medium.

(b) The process of copying data should produce an exact copy of the original. Such a reproduction should allow the specialist to investigate the files in the way they that existed on the original medium.

Step 3. Preserving digital evidence :

Digital evidence in particular needs to be validated if it is to have any probative

value. A digital evidence specialist will invariably copy the contents of a number of disks or storage devices, in both criminal and civil matters. To prove the digital evidence has not been altered, it is necessary to put in place checks and balances to prove the duplicate evidence in digital format has not been altered since it was copied. The method used to prove the integrity of data at the time the evidence was collected is known as an electronic fingerprint. The electronic fingerprint uses a cryptographic technique that is capable of being associated with a single file, a floppy disk or the entire contents of a hard drive. As digital evidence is copied, so a digital evidence specialist should use software tools that are relevant to the task.

Step 4. The chain of custody :

However, the chain of custody, in both civil and criminal matters, should be considered very carefully in respect to digital evidence. The reason or taking particular care with digital evidence is because it is easy to alter. It is necessary to demonstrate the integrity of the evidence and to show it cannot have been tampered with after being seized or copied. There is another reason for being meticulous about ensuring the chain of evidence is correctly recorded. In a case involving a number of items of hardware and more than one computer, it will be necessary to ensure there is a clear link between the hardware and the digital evidence copied from the hardware. In this respect, the record should address such issues s who collected the evidence; how and where it was collected; the name of the person who took possession of the evidence; how and where it was stored; the protection afforded to the evidence while in storage; and the names of the people that removed the evidence from storage, including the reasons for removing the evidence from storage.

Step 5. Transporting and storing digital evidence :

Consideration should be given to the methods by which any hardware and digital evidence is transported and stored. Computers need to be protected from accidentally booting up; consideration should be taken to ensure that hardware is clearly marked to prevent people from using the equipment unwittingly; and loose hard drives, modems, keyboards and other such materials should be placed in anti-static or aerated bags. Storage conditions should be appropriate. Hardware and digital evidence should be protected from dirt, humidity, fluids, extremes of temperature and strong magnetic fields. It is possible for data to be rendered unreadable if the storage media upon which the digital evidence is contained are stored in a damp office or overheated vehicle during the summer.

Analysis of digital evidence :

A digital evidence specialist is not only required to obtain and copy digital evidence that has a high probative value, but must also provide an analysis of the evidence. The analysis of the evidence will involve reviewing the text of the data, and the attributes of the data. This exercise may also include, but will not be limited to, looking for and recovering deleted files, and other data that may be hidden on the disk, checking logs for activity and checking unallocated and slack space for residual data. Failure to assess the digital evidence can lead to false assumptions.

TOOLS :

A digital evidence specialist will not only, ideally, require an in-depth knowledge of

the operating system they are to investigate, but they will also need to use a number of proprietary tools in the performance of their investigation and analysis of digital evidence. The types of took they use will depend on the operating system (Windows, Unix, Macintosh) they are required to look at, and whether they are investigating a network, hand held devices, embedded systems or wireless networks.

COPYING THE HARD DRIVE :

Before entering a computer, it is essential that the investigator is familiar with the underlying operating systems, files systems and applications. By understanding the file systems, the digital evidence specialist will be aware of how information is arranged, which in turn enables them to determine where information can be hidden, and how such information can be recovered and analysed. In order to establish answers to questions such as : 'who might have had access to a computer or system'; 'which files they would have been able to look at', and 'whether it was possible for an unauthorised outsider to obtain access to the computer from the Internet', the digital evidence specialist should understand the nature of user accounts and profiles, and the control mechanism that determines which files a user is permitted to gain access to once they are logged on to a system.

VIEWING THE DATA :

When the digital evidence has been copied, the data can be viewed physically or logically. To view data physically, such as the files and the properties associated with them, it is necessary to view the directory through a tool.

RECOVERING DATA :

Increasing numbers of people delete the contents of their hard drives in computers in anticipation of legal action or after legal action has begun.

There are several techniques that can be used to recover data that has been deleted. This can be done manually or using tools, depending on the complexity of the problem faced.

PASSWORDS AND ENCRYPTION :

A number of tools are available that are capable of removing passwords, and bypassing or recovering them. Some tools are available to guess passwords if the encryption keys are small enough, and where it is not possible to defeat a password, it is sometimes possible to search for unencrypted versions of the data in other areas of the hard disk.

Challenges to the authenticity of electronic evidence can include :

1. a claim that the records were altered, manipulated or damaged between the time they were created and the time they appear in court as evidence;
2. the reliability of the computer program that generated the record ;may be questioned;
3. the identity of the author may be in dispute: for instance, the person responsible for writing a letter in the form of a word processing file, SMS or email may dispute they wrote the text, or sufficient evidence has not been adduced to demonstrate the nexus between the evidence and the person responsible for writing the communication;
4. the evidence from a social networking website might be questioned as to its

reliability;

5. it might be agreed that an act was carried out and recorded, but at issue might be that the party introducing the evidence has failed to prove that where others might have access to a device (such as a mobile telephone), there was no proof to show that the message was directed to a particular person; or
6. whether the person alleged to have used their PIN, password or clicked the 'I accept' icon was the person that actually carried out the action.
7. The data on local area networks, and whether there is a need to obtain an image of the complete network, if this is possible. If an image of each computer comprising the network is taken, the issue with networked computers is to demonstrate who had access to which computers at what time, and whether this access is audited. The security mechanisms in place on the network will be an important consideration when proving authenticity.
8. Data from the Internet is also subject to problems, because reliance may be placed on data obtained from remote computers, the computer of an investigator, and perhaps intercepted evidence. With the increased use of cloud computing where data is stored on 'server farms', accessible via the Internet, obtaining a copy of the data may be subject to contractual restrictions, or the data may be stored in another jurisdiction, which in turn may mean it will be necessary to take local legal advice in relation to the obtaining of the data.
9. Where data is being updated constantly, such as transactional data-bases, or websites that are continually updated, this poses problems, as the relevant evidence is point-in-time, which may be extremely difficult to obtain.
10. Authentication of information on social media sites presents its own unique set of issues. Firstly, it can be difficult to establish the author of the document, because social media sites often have a number people writing to the one page. Secondly, proving the identity of an author can be difficult, since it is still possible to create an internet profile without having to prove identity.

Points to be considered which may help in dealing with electronic evidence :

The abovsaid challenges can be dealt after some general investigative questions are answered. These are important questions regarding a crime involving computers and electronic evidence, which can be kept in mind while dealing with such evidences. They are as follows:

A. Use or operating part of machine :

- ✓ Where is the computer's electronic media (compact disks, floppy disks, thumb drives, etc) stored?
- ✓ When and where was the computer obtained? Was it new or used?
- ✓ Who has access to the computer hardware and software?
- ✓ If other people have access to the computer, hardware or software can they access everything on the computer or only certain files, folders or programs?
- ✓ How many people use the computer? Who are they and for how many times ?
- ✓ Whose fingerprints might be found on the electronic media?

B. About User :

- ✓ What are the user names on the computers? And What programs are used by

each computer user?

- ✓ What is the level of computer experience of each computer user?
- ✓ Does the computer require a user name and password? What are they?

C. Connection to the net

- ✓ How does the computer have access to the Internet (DSL, Cable, Dial-Up, LAN, etc)?
- ✓ Does the victim or suspect have an e-mail account? Who is the service provider (Yahoo, AOL, Gmail, Hotmail, etc)? And what is the email address ?
- ✓ Which e-mail client (program) does the suspect or victim use?
- ✓ Does the victim or suspect remotely access their computer (can they get into their computer when away from the office or home)?
- ✓ Do any of the users use on-line or remote storage?

D. Deleting data

- ✓ Have any programs been used to "clean" the computer?
- ✓ Does the computer contain encryption software or hard drive wiping utilities?
- ✓ What is the chronology of the access or changes in the data?

E. Investigative Authority

- ✓ Who has investigated the incident and what actions have been taken to identify, collect, preserve, or analyze the data and the devices involved?
- ✓ Who handled the evidence?
- ✓ Document the name and job function (e.g., layperson versus qualified personnel) of each individual who handled the digital evidence. More than one person could be involved in this process.
- ✓ Identify everyone who had control of the digital evidence after it was examined and before it was given to law enforcement.
- ✓ How was the digital evidence collected and stored?
- ✓ Identify any tools or methods used to collect the digital evidence.
- ✓ Determine who had access to the digital evidence after it was collected (anyone with access to the evidence should be considered part of the chain of custody). Account for all storage of data as well.
- ✓ When was the evidence collected? Document the date and time when the evidence was collected (including a reference to time zone if necessary).

Case Law :

In this part of article some case laws, which are explained periodical wise, it helps to observe the developments in focusing the issue of electronic evidence by judiciary. The general case-index also provides an issue wise analysis of the each case. It mainly based on the decision of Hon'ble Supreme Court and Hon'ble High Court of Bombay reported in various journals. Efforts have also been made to present the other High Court's ruling hereby in an index format to have a quick glance and its comparative study.

Sr.	Name of the Case	Citation	Notes
1.	State vs. Mohd. Afzal And Ors.	(2003) DLT 385, 2003(71)DRJ 17	Computer generated electronic records is evidence, admissible at a trial if proved in

	(Parliament attack case)	MANU/DE/1026/ 2003	the manner specified by Section 65B of the Evidence Act.
2.	State vs. Navjyot Sandhu	(2005) 11 SCC 600, AIR 2005 SC 3820 MANU/SC/0465/2005	Merely because a certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65.
3.	Anvar vs. Basheer	AIR 2015 SC 180 MANU/SC/0834/2014	Section 65B of the Evidence Act has been inserted by way of an amendment by the Information Technology Act, 2000. Inasmuch it is a special provision which governs digital evidence and will override the general provisions with respect to adducing secondary evidence under the Evidence Act.
4.	Avnish Bajaj vs. State (Bazee.com case)	2008(105)DRJ 721 MANU/DE/0851/2008	This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.
5.	Som Prakash vs. State Of Delhi	AIR 1974 SC 989 1974 Cri. LJ 784 MANU/SC/0213/1974	In this case Supreme Court has rightly observed that "in our technological age nothing more primitive can be conceived of than denying discoveries and nothing cruder can retard forensic efficiency than swearing by traditional oral evidence only thereby discouraging the liberal use of scientific aids to prove guilt." Statutory changes are needed to develop more fully a problem solving approach to criminal trials and to deal with heavy workload on the investigators and judges.
6.	SIL Import, USA	(1999) 4 SCC 567	In yet another decision in which use of

	vs. Exim Aides Exporters, Bangalore	MANU/SC/0312/1999	available technology has been given a real boost, the Supreme Court held that "Technological advancement like fascimile, Internet, e-mail, etc. were in swift progress even before the Bill for the Amendment Act was discussed by Parliament. So when Parliament contemplated notice in writing to be given we cannot overlook the fact that Parliament was aware of modern devices and equipment already in vogue."
7.	Grid Corpn. Of Orissa Ltd. vs. AES Corpn.	2002 AIR (SC) 3435	In this the Supreme Court has ruled in favour of technology and it held that "When an effective consultation can be achieved by resort to electronic media and remote conferencing it is not necessary that the two persons required to act in consultation with each other must necessarily sit together at one place unless it is the requirement of law or of the ruling contract between the parties." In this case the contention was that the two arbitrators appointed by the parties should have met in person to appoint the third arbitrator.
8.	State of Maharashtra vs. Dr. Praful B Desai	MANU/SC/0268/2003 (2003) 4 SCC 601	The Supreme Court held that video-conferencing could be resorted to for the purpose of taking evidence of a witness. In that case, one party was seeking direction of the court to take evidence of a witness residing in the United States of America. Though a lower court had ordered such evidence to be taken with the help of video-conferencing, the concerned High Court struck down that order on the grounds that the law required the evidence to be taken in the presence of the accused. The Appeal Bench of the High Court upheld the said latter order. The Supreme Court struck down the High Court order by stating that recording of evidence satisfies the object of Section 273 of the Code of Civil Procedure that evidence be recorded in

			the presence of the accused. In explaining the benefits of video-conferencing the Court observed that "In fact the Accused may be able to see the witness better than he may have been able to if he was sitting in the dock in a crowded Court room. They can observe his or her demeanour. In fact the facility to play back would enable better observation of demeanour. They can hear and rehear the deposition of the witness."
9.	Sanjaysinh Ramrao Chavan vs. Dattatray Gulabrao Phalke	MANU/SC/0040/ 2015	Relying upon the judgment of Anvar P.V. supra, while considering the admissibility of transcription of recorded conversation in a case where the recording has been translated, the Supreme Court held that as the voice recorder had itself not subjected to analysis, there is no point in placing reliance on the translated version. Without source, there is no authenticity for the translation. Source and authenticity are the two key factors for electronic evidence.
10.	Ankur Chawla vs. CBI	MANU/DE/2923/ 2014	The Hon'ble High Court of Delhi, while deciding the charges against accused in a corruption case observed that since audio and video CDs in question are clearly inadmissible in evidence, therefore trial court has erroneously relied upon them to conclude that a strong suspicion arises regarding petitioners criminally conspiring with co-accused to commit the offence in question. Thus, there is no material on the basis of which, it can be reasonably said that there is strong suspicion of the complicity of the petitioners in commission of the offence in question.
11.	Abdul Rahaman Kunji vs. The State of West Bengal	MANU/WB/0828/ 2014	The Hon'ble High Court of Calcutta while deciding the admissibility of email held that an email downloaded and printed from the email account of the person can be proved by virtue of Section 65B r/w Section 88A of Evidence Act. The

			testimony of the witness to carry out such procedure to download and print the same is sufficient to prove the electronic communication.
12.	Jagdeo Singh vs. The State and Ors.	MANU/DE/0376/ 2015	In the recent judgment pronounced by Hon'ble High Court of Delhi, while dealing with the admissibility of intercepted telephone call in a CD and CDR which were without a certificate u/s 65B Evidence Act, the court observed that the secondary electronic evidence without certificate u/s 65B Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever.

Ref. :

1. Burkhard Schafer and Stephen Mason, The characteristics of electronic evidence in digital format, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013.
2. George R. S. Weir and Stephen Mason, The source of Digital Evidence, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013.
3. Manish T. Karia and Tejas D. Karia, India, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013.
4. Stephen Mason and Andrew Sheldon, Proof : The investigation, collection and examination of digital evidence, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013.
5. Stephen Mason, Authenticating Digital Data, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013.
6. U.S. Department of Homeland Security, United state secret services, Best Practices for Seizing Electronic Evidence, (downloaded on 1.8.2015 from www.crime-scene-investigator.net)