International Journal in Management and Social Science
Volume 08 Issue 05, May 2020 ISSN: 2321-1784 Impact Factor: 6.178
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

COMPUTER FORENSIC INVESTIGATION PROCESS AND JUDICIAL RESPONSE TO THE DIGITAL EVIDENCE IN INDIA IN LIGHT OF RULE OF BEST EVIDENCE

Nilima Prakash,
Advocate, Punjab and Haryana High Court
Dr. Roshni Duhan,
Department of Laws, B.P. S Women University, Khanpur Kalan, Sonipat

Introduction

The use of science to investigate the facts in court of law is known as Forensic. In the present time, almost every crime is investigated with the help of forensic science and this science is used as evidence to prove the guilt or defend the accused. The forensic evidence includes Physical evidence such as bullets, fire arms and Medical evidence such as blood and DNA. The term Computer forensics includes the acquisition, examination and reporting of information which is found in computers along with networks that pertain to an investigation civil or criminal as well. The computer contains all the materials left whether it is deleted files or registry entries. The traces which are left by someone can be restored easily. As we all are living in the era of modern devices and internet, the role of Cyber forensic investigation comes into picture due to certain problems attached with the internet. The Internet is a significant problem for legal investigations. The prime issue is related to jurisdiction, The crimes such as scams, fraud, phishing and other relevant crimes are enabled due to global internet. It is very easy for a criminal sitting in one country to commit a crime against a person in another country, Due to such complexities and dynamic nature of the Net, a site on the Internet used to perpetrate a crime one day may be different or lost on another day, With regard to the origin of Cyber Forensics, nothing is clear i.e. when did it came into existence. However, this is a certain fact that with the evolution of Computer Science, the crimes relating to computers also started committing. Hence, it can be clearly opined that cyber forensics has been evolved when reporting of incidents of cybercrimes started; as to gather evidences from the target computer and the Internet. Although Internet is a universal abstract, even then, internationally, there is not even a single unanimously accepted document providing standards practices, nor is there a generally accepted governing body for this field. The marks of the need of cyber forensics can be traced back to 1980. The beginning of 1980 saw the need for the techniques to deal with the crimes committed by/against the computers. In 1984, for the first time, a Computer Crime Unit was organized by the United Kingdom. Later, in the same year the United States of America also established a Magnetic Media Program through its department of Federal Bureau of Investigation. India enacted its first legislation only in 2000 with the introduction of Information Technology ACT, 2000. Later, the relevant other legislations were also amended as per the need of the hour.

***Corresponding Author**

Computer Forensics and Computer Investigation Process

Computer Forensics is simply the application of computer investigation and analysis techniques in the interests of determining legal evidences. It mainly deals with the issues relating to the analysis of computer media or computer system for digital evidence in relation to the perpetration of cyber crime. The computer forensics can also be described as "the autopsy of a computer hard disk drive" due to the specialized tools and techniques. Judd Robbins, a prominent computer forensics investigator, defines computer forensics as ―the application of computer investigation and analysis techniques within the interests of determining potential legal evidence[1].

According to **Steve Hailey of Cyber security Institute**[2], computer forensics is ―The preservation, identification, extraction, interpretation, and documentation of computer evidence, to incorporate the principles of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found[3]. There is a proper cyber investigation process which is need to be followed while collecting the cyber evidences. The purpose of a Forensic Computing Investigation is to investigate criminal conduct committed by the use of a computer or other electronic device. The Computer Investigation Process is to be followed by the 4 steps which can be described as under:

1**. Collection and Preservation of Evidence:**

The primary step which is followed by investigator in cyber forensic process is determining the appropriate tool along with some other relevant factors such as type of computer, purpose of use of computer and network used in committing the crime etc. The investigator, or crime scene technician, collects the evidence. The collection procedures vary depending on the type of digital device, and the public and private resources where digital evidence resides such as computers, phones, social media etc. for different digital forensics practices pertaining to multimedia, video, mobile. Law enforcement agencies have standard operating procedures that detail the steps to be taken when handling digital evidence on mobile devices, Internet-enabled objects, the cloud and social media platforms. Unique constraints that could be encountered during the investigation should be identified. For instance, cybercrime investigators could encounter multiple digital devices, operating systems, and sophisticated network configurations which can require specialized knowledge, variations in collection procedures, and assistance in identifying connections between systems and devices (e.g., a topology of networks). However, the manner in which an investigator obtains the data should be complete, yet minimizes the interference with the target data. Such data may simply be printed and copied. Although, this may result in alterations to the meta data associated with

the target data, which may create vulnerabilities. Therefore, most common techniques are adopted to obtain forensic data. These tools and techniques may be;

a) Software Imaging Tools
b) Hardware Imaging Devices
c) Imaging Validation Tools
d) Write Protection Tools

2. Extraction of Evidence

Evidence is extracted from the seized digital devices at the forensic laboratory i.e., static acquisition. At the forensics laboratory, digital evidence should be acquired in a manner that preserves the integrity of the evidence by ensuring that the data is unaltered and that too in a forensically sound manner. To achieve this, the tools and techniques used to acquire digital evidence must prevent alterations to the data or when this is not possible, at least minimize them. The tools and techniques which are used for this particular purpose of extracting evidence should be valid and reliable[4].The limitations of these tools and techniques should be identified and considered before their use. The US National Institute of Standards and Technology has a searchable digital forensics tools database with tools with various functionalities (e.g., cloud forensics tools, among others). There are two types of extraction performed: physical and logical. Physical extraction involves the look for and acquisition of evidence from the situation within a digital device where the evidence resides, like the disk drive of a computer. A physical extraction may be conducted using keyword searches based on terms provided by the investigator, file carving and by examining unallocated space i.e., space available on a system because it was never used or because the information in it was deleted and partition which separates segments of the hard drive from each other. Logical extraction involves the look for and acquisition of evidence from the situation it resides relative to the filing system of a Computer Operating System, which is employed to keep track of the names and locations of files that are stored on a storage medium such as a hard disk. The type of logical extraction conducted depends on the digital device, filing system, applications on the device and OS. A logical extraction involves the acquisition of knowledge from active and deleted files, file systems, unallocated and unused space, and compressed, encrypted, and password protected data. The following tools are used for extraction of evidence:

a) Hidden Data Recovery Tools
b) Known File Filtering
c) Encryption Identification Tools
d) Password Recovery Tools
e) Steganography Detection Tools
f) Virus Detection Capabilities

3. **Examination of Evidence**

The digital forensics process also involves the examination and interpretation of digital evidence (analysis phase), and therefore the communication of the findings of the analysis (reporting phase). During the analysis phase, digital evidence is extracted from the device, data is analysed and events are reconstructed. Before the analysis of the digital evidence, the digital forensics analyst within the laboratory must be told of the objectives of the search, and given some background of the case and the other information that was obtained during the investigation which will assist the forensics analyst during this phase (e.g., IP address or MAC addresses)[5]. Various sorts of analyses are performed counting on the sort of digital evidence sought, like network, filing system, application, video, image, and media analysis. Files are analysed to determine their origin, and when and where the data was created, modified, accessed, downloaded, or uploaded, and the potential connection of these files on storage devices too. Generally, there are four types of analyses that can be performed on computers:

a) time-frame analysis
b) ownership and possession analysis
c) application and file analysis
d) data hiding analysis

The time-frame analysis seeks to create a timeline or time sequence of actions using time stamps (date and time) that led to an event or to determine the time and date a user performed some action. This analysis is performed to attribute a crime to a perpetrator or at the very least attribute an act that led to a crime to particular individual. The ownership and possession analysis is used to determine the person who created, accessed or modified files on a computer system. For instance, this analysis may reveal a picture of kid sexual assault material (i.e., the "representation, by whatever means, of a toddler engaged in real or simulated explicit sexual activities or representation of the sexual parts of a toddler for primarily sexual purposes[6]. This piece of information alone is not enough to prove ownership of child sexual abuse material. Further evidence is required to prove this like exclusive use of the pc where the fabric was found. The application and file analysis is performed to examine applications and files on a computer system to determine the perpetrator's knowledge of and intent and capabilities to commit cybercrime.

4. **Organisation of Evidence**

Evidence preservation seeks to guard digital evidence from modification. The integrity of digital evidence should be maintained in each phase of the handling of digital evidence. First responders, investigators, crime scene technicians, and digital forensics experts must

demonstrate, wherever possible, that digital evidence was not modified during the identification, collection, and acquisition phase. The ability to do so depends on the digital device e.g., computer and mobile phones and circumstances encountered by them (e.g., need to quickly preserve data). To demonstrate this, a chain of custody must be maintained. The chain of custody is "the process by which investigators preserve the crime (or incident) scene and evidence throughout the life cycle of a case. It includes information about who collected the evidence, where and the way the evidence was collected, which individuals took possession of the evidence, and once they took possession of it". After collecting and documenting the evidence either by forensic imaging or by storing it in other devices like USBs, hard drives etc., the evidence is packaged, labelled, tagged and is updated in the evidence database. Once the digital evidence is seized, orders of the competent court could also be sought to retain the seized properties or send the digital evidence for forensic analysis. In cases where the owners of the property approach the court for the discharge of the impounding properties, the IO should send a forensic imaged copy of the seized property instead of the first material seized for smoother investigation. However, the organization of digital evidence is critical to any investigation. Hence, it is quite necessary that an investigator must be able to take a piece of evidence and determine how it fits in the larger framework of the case. In most cases involving digital evidence, it is really easy for the investigator to become swamped by so much data that it is hard to decipher the key pieces of information. With proper case management and information chaining, the investigator can brief his search to the sources of key evidence. There are different tools which are used by the investigator for organisation of evidence. These are as follows:

A. **Link Analysis Tool:**

For the right direction investigation, not just the collection of evidence necessary but understanding that how each piece relates to each-other is also important. So, the Link Analysis Tool comes into play. This tool allows the investigator to get a better understanding of the case and could result in solving the case much faster. With the help of this tool, an investigator can draw associations between disparate pieces of evidence and make it effective and presentable in court.

B. Network Forensics:

As the name suggests, the collection of digital evidence in a network environment is termed as Network Forensics. There are several complications to a cyber investigation when a network is involved. These complications can hamper the investigator and require special training to complete the investigation process complete. Network Forensic also involve, 'the reconstruction of events on a client network deduced from the clues at hand'[7]. In this regard, LAN (Local Area Network),WAN (Wide Area Network) and ETHERNET[8] play a vital role in the networking system.

C. Intrusion Detection System Analysis:

An intrusion detection system is designed to inspect all in-bound network activity that may indicate a network attack, record the event, notify the appropriate security administrators of suspicious events and take some action to block activities from the concerned source.

D. Incident Forensics:

It involves the investigation of a compromise or attack that has occurred on a system. After the attack, there are two approaches: active system analysis[9] and inactive system analysis[10]. The active system analysis requires processing steps before the standard computer forensic methodology is applied. On the other hand, the inactive system analysis requires the same basic methodology associated with the computer forensic process, with a different set of objectives being the identification and recovery of modified system files and processes.

Relevancy and Admissibility of Digital Evidence and Rule of Best Evidence

The law of evidence has long been guided by the rule of "best evidence" which is considered to have two basic prototypes: a) avoidance of hearsay and b) production of primary evidence. These rules are believed to weed out infirm evidence and produce only that which cannot reasonably be doubted. In light of the Indian Evidence Act, 1872, this will be understood as only an individual who has himself perceived the very fact being proved can depose with reference to it, and not someone who has received the information second hand. Similarly, where a document is to be wont to prove some extent, the first should be produced in court, and not a replica or photograph or the other reproduction of the same, not even statements regarding the contents by someone who has seen it. For any reproduction of a press release or document is lower on the rung of authenticity than the first, giving opportunities for fraud or fabrication. Under the Indian Evidence Act, any substance on which matter has been expressed or described are often considered a document, as long as the aim of such expression or description is to record the matter. Electronic records are defined within the Information Technology Act, 2000 as any data, record or data generated, any image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. An electronic record is often safely included under such a definition because matter is recorded on the pc as bits and bytes, which are the digital equivalent of figures or marks. Computer records were widely considered to be hearsay statements since any information retrieved from a computer would consist of input provided by a human being. Thus, be it a word document containing statements written by one party, or an image of a missing person generated by the computer based on inputs given to it, all such records will be hearsay. An electronic document would either involve documents stored during a digital form, or a print out of an equivalent. What is recorded digitally may be a document, but can't be perceived by

an individual not using the pc system into which that information was initially fed. Thus, if music composer A mixed certain tunes on his computer, and another composer, B, wanted to sue him for copyright violation, B wouldn't have access to the digital records on A's computer. Even though such a document are often imprinted onto a magnetic base, like a compact disk (CD), it might still require access to A's computer. A document containing a print out of computer records, though a document lato sensu, are often perceived by anybody. Whenever the print out of such documents is taken, it amounts to Secondary evidence as per the strict provisions of Indian Evidence Act. In India, this attitude has come with a change after the amendment to the Evidence Act in 2000. Sections 65A and 65B were introduced into the chapter concerning documentary evidence. Section 65A provides that contents of electronic records could also be admitted as evidence if the standards provided in Section 65B is complied with. Section 65B provides that shall be considered documents, thereby making it primary evidence, if the pc which produced the record had been regularly in use, the knowledge fed into the computer was a part of the regular use of the PC and the PC had been operating properly. It further provides that each one computer output shall be considered as being produced by the pc itself, whether it had been produced directly or indirectly, whether with human intervention or without. This provision does away with the concept of computer evidence being hearsay. Thus, with the amendments introduced into the statute, electronic evidence in India is not any longer either secondary or evidence, but falls within the simplest evidence rule i.e. the Rule of Best Evidence.

Judicial Response to the Digital Evidence in India

This is the rule of law that for any piece of evidence to be introduced in court, it must meet certain standards of legal permissibility that allow the court to receive and consider it. Manifestly speaking, one of the prime considerations before evidence is considered to be admissible, its relevance to the matter at issue. Lets' have a look upon certain case laws which prove that admissibility of digital evidence in India has been warmly accepted.

From the beginning we find in a very popular case of **Twentieth century Film Fox Corporation v. NRI Film Production Association (Pvt) Ltd.**[11] in which the Hon'ble Court observed the conditions which must be complied in order to authenticate the video conferencing. The suggested conditions are:

i) Before a witness is examined in terms of the audio-video with as is to file an affidavit duly verified before a notary or a judge that the person who is shown as the wItness is the same person who is about to depose on the screen. A copy is to be made available to the opposite side.

ii) The person who examines the witness on the screen is also supposed to file on undertaking before examination along with a copy to the opposite counsel/party with regard to identification.

iii) The witness has to be examined during working hours of Indian court and oath is to be administered through the media.

iv) The witness should not plead any innocence on account of time difference between Indian and United States of America.

v) The learned judge is to record such remarks as is material regarding the demeanour of the witness on the screen.

vi) Before examination of the witness. a set of plaint, written statement and other documents must be sent so that the witness becomes acquainted with the document and an acknowledgement is to filed before the court in this regard.

There is another case of **State v. Navjot Sandhu**[12], popularly known as **Parliament Attack Case,** which led to the conviction of the Respondent under various provisions of the Indian Penal Code, 1860 and the Prevention of Terrorism Act, 2002. One of the pieces of evidence relied by the prosecution and subsequently forming the basis of conviction was the call records of the accused. The Hon'ble Supreme Court held that printouts taken from the computers/servers by mechanical process and authorized by a responsible official of the service providing Company are often given into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts supported his personal knowledge. This would make the call records admissible. The Supreme Court went further on to state that regardless of the compliance of the wants of Section 65B of the Evidence Act which may be a provision regarding handling of admissibility of electronic records, there is no bar to adduce secondary evidence under the other provisions of the Evidence Act, namely Sections 63 and 65[13].

In **Amitabh Bagchi v. Ena Bagchi** [14] the Calcutta High Court also observed the importance of Section 65B of Indian Evidence Act, 1872. Accordingly the Hon'ble Court held that physical presence of a person in court may not be required for the purpose of adducing evidence and the same can be done through other mediums such as video conferencing. Section 65A and 65B provide provisions for evidence relating to electronic records and admissibility of electronic record and it is notable that definition of electronic records includes video conferencing.

While having reading several other judgments passed by other High Courts and Hon'ble Supreme Court we find in **Jagjit Singh v. State of Haryana**[15] that the Speaker of the Legislative Assembly of the State of Haryana disqualified a Member on the ground of defection. The Supreme Court, whilst hearing the matter, also considered the appreciation of digital evidence within the sort of transcripts of digital media including the News Channels. The channels involved were Zee News channel, the Aaj Tak television channel, and the Haryana News of Punjab Today television channel. The court indicated the extent of the relevant digital materials and determined that the electronic evidence placed on the record was admissible, and upheld the reliance placed by the Speaker on the interview recorded on the CDs for reaching the conclusion that the persons recorded on the CDs were equivalent as those taking action and their voices were also identical. This judgment enhanced the role of Digital Evidence in perspectives of Best Evidence Rule also. The prosecution in the case of **The State of Maharashtra and Ors. v. Rajesh and Ors.** [17] relied on the CCTV[18] footage recovered from the petrol pump wherein the

accused had refueled the vehicle. Bharat Petroleum Corporation had given the contract to the Kores India Limited for installation of CCTV Cameras at the premises of petrol pump. Eight numbers of CCTV cameras, Network Video Recorder[19] and monitor, etc. were supplied at their petrol pump by the Kores India Limited. All the cameras were functioning 24×7 hours and in case of any malfunctioning in the system, pump operators had to lodge the complaint to the Bharat Petroleum through the Broma Software. Prosecution affirmatively stated that till date of commission of the said crime there was no occasion to lodge complaint about the malfunctioning of the CCTV cameras and its system installed at their petrol pump. The court observed that there is a revolution in the way the evidence is produced before the court, it makes the systems function faster and more effective and any documentary evidence by way of an electronic record under the Sections 59 and 65A of Evidence Act are often proved only in accordance with the procedure prescribed under Section 65B. The purpose of those provisions is to sanctify secondary evidence in electronic form, generated by a computer. This is to be noted that the Section starts with a non obstante clause. Thus, notwithstanding anything contained within the Evidence Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document as long as the conditions mentioned under Sub-section (2) are satisfied, without further proof. The very admissibility of such a document, i.e., electronic record which is named as computer output, depends on the satisfaction of the four conditions specified in (2) of Section 65B.

Conclusion

Cyber forensics involves the identification, documentation, and interpretation of computer media for using them as evidence and it is the process of identifying, collecting, preserving, analysing and presenting the computer-related evidence in a manner that is legally acceptable by court. Forensic sciences have been developed to ensure that criminals are hunted down and brought to the court of law. This branch of science provides benefits to the society at large. However, Cyber forensics became tougher since new forms and techniques of knowledge storage are continuously being changed and new technologies are being developed. One of the major challenges faced by the investigators and courts is the lack of legal framework. In India after the enactment of Information Technology Act, 2000 subject to satisfaction of the provisions laid down under section 65B and **ratio decidendi** stipulated in **Anwar P.V. v. P.K. Basheer**, amendments in the Indian Evidence Act, 1872 and the Indian Penal Code, 1860, electronic record is admissible evidence. However, the major problem is to jurisdictional issues. The tasks of identifying cyber-criminals and bringing them to justice pose formidable challenges to enforcement agencies across the world and need a degree and timeliness of cooperation that has been until only recently considered difficult, if not impossible, to realize . In India, all electronic records are now considered to be documents, thus making them primary evidence. At an equivalent time, a

blanket rule against hearsay has been created in respect of computer output. These two changes within the stance of the law have created paradigm shifts within the admissibility and relevancy of electronic evidence, albeit certain precautions still being necessary. However, technology has itself provided answers to problems raised by it, and computer forensics make sure that manipulations in electronic evidence show up clearly within the record. Human beings now only got to make sure that electronic evidence being admitted has relevancy to the very fact in issue and is in accordance with the Constitution and other laws of the land

References:

1. Ravi Kumar Jain ―Cyber Forensics: Invstigatin Crimes in the Cyber World‖. Usha (Ed.), Cyber Forensics. Digital Experience, The ICFAI University Press, Hyderabad, 2008, p. 7.
2. Steve Hailey is an Information Technology veteran of thirty years, with twenty-three years of experience developing and delivering technical training. Steve has twenty-seven years of data recovery experience, and has been conducting digital forensic analysis professionally for sixteen years. He is a highly skilled expert witness and dynamic instructor, bringing to bear his combined skills in information security and digital forensic analysis. He currently instructs the information security and digital forensics curriculum at Edmonds Community College in Washington State. Retrieved from http://www.cybersecurityinstitute.biz/experts.htm, on 26/06/2017.
3. S. Hailey, What is Computer Forensics, 2003. Retrieved from http://www.cybersecurityinstitute. biz/forensics.htm, on 26/06/2017
4. NIST, SWGDE Recommended Guidelines for Validation Testing, 2014; US National Institute of Justice, 2007b).
5. (Nelson, Phillips, and Steuart, 2015; SWGDE Best Practices for Digital Evidence Collection, 2018).
6. Article 2, United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography of 2000) on a suspect's device.
7. 'Network Forensics'. CTX Corporation. Available at:http://www.forensics-intl.com/filelist.html.
8. Ethernet is a family of frame - based computer networking technologies for Local Area Networks. It defines a number of wiring and signaling standards for the physical layer, through means of network access at the Media Access Control/ Data Link Layer and a common addressing format.
9. An active system analysis is performed before the shutting down of system
10. Inactive system analysis is the approach of traditional computer analysis

11. AIR 2003 KANT 148.
12. AIR 2005 SC 3820.
13. The Court held that 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 and 65.
14. AIR 2005 Cal 11
15. (2006) 11 SCC 1.
16. See also, Murugesan v. Arumugham and Ors, MANU/TN/1399/2017; Janardhanan Pillai and Ors. v. Salini and Ors, MANU/KE/1671/2016: K. Ramajayam v. The Inspector of Police, MANU/TN/0112/2016; Kamal Patel v. Ram Kishore Dogne, MANU/MP/0050/2016; Abdul Fareed and Ors. v. State of U.P. and Ors, MANU/UP/2212/2016; Ashwani Kumar v. State of Haryana, MANU/PH/1887/2016
17. 2016 (3) Bom. C. R. (Cri) 55, MANU/MH/0660/2016. See also Mohammad Akbar v. Ashok Sahu and Ors, MANU/CG/0405/2016; Nepal Singh v. The State of Tripura, MANU/TR/0233/2016; Radhanath Yadav and Ors. v. State of Assam, MANU/GH/0532/2016; Rakesh Jain v. State of Haryana, MANU/PH/0164/2016
18. Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.
19. A network video recorder (NVR) is a software program that records video in a digital format to a disk drive, USB flash drive, SD memory card or other mass storage device. An NVR contains no dedicated video capture hardware. However, the software is typically run on a dedicated device, usually with an embedded operating system. Alternatively, to help support increased functionality and serviceability, standard operating systems are used with standard processors and video management software. An NVR is typically deployed in an IP video surveillance system. Retrieved from https://en.wikipedia.org/wiki/Network_video_recorder on 06/07/2017 at 15:35 hrs