



Legal Research Development

An International Refereed e-Journal

ISSN: 2456-3870, Journal home page: <http://www.lrdjournal.com>

Vol. 07, Issue-II, Dec. 2022



COMPUTER FORENSIC - A NEW BRANCH OF FORENSIC SCIENCE AND CYBER CRIME

Bhawana Saxena^{a,*}, 

^a Ph.D. Scholar(Law), Govt. M.L.B. College of Excellence, Gwalior, Jiwaji University, Gwalior, Madhya Pradesh (India).



KEYWORDS

Computer forensic, forensic examiner, cyber-crime, electronic evidence, Computer forensic experts, array of methods, ISP (Internet Service Provider).

ABSTRACT

Computer forensic is also known as digital forensic. The computer forensic examiner or expert works with other law enforcement agencies make a unit. As the information technology increases its resources for the advancement of society, digital crimes or cyber-crimes are also increases at very rapid speed simultaneously. This is a very great loss of our technological privileges. To curb cyber-crime there is need of an anti-cyber-crime professionals or examiners, experts and other law enforcement officials they assist to each other in investigation of cyber-crime. Section 79 A of The Information Technology Act 2000, provides provisions for examiner of electronic records and gives power to Central Government to appoint any department, body or agency of Central or State Government as an examiner of Electronic Evidence. Now days, there is a great need of computer forensic examiner or expert to mitigate or diminish cyber-crimes. Generally a case of cyber-crime cannot be resolved to some extent, without the assistance of computer expert or forensic examiner or expert. Several crimes like child pornography and forgery or fraud in online transaction are required forensic examination of evidence.

Introduction

Forensic science is an integral part of administration of criminal justice system. Computer forensic is a new branch of forensic science. It is also known as digital forensic. Forensics generally means the use of science and technology to establish facts in Courts of law. It includes scientific collection, examination, analysis then presentation of results in the basis of information retrieved from computer and its storage media, in such a way that it can be used as a potential legal evidence.¹ The evidences so furnished will be in some electronic form called "electronic records" but several times, it becomes difficult to test the veracity of such evidences, in absence of expert. Here comes the role of computer forensic or cyber forensic (Expert). In other words Forensic analysis of electronic/digital records is similar to analysis of human anatomy (postmortem of human body), which is required to establish proofs against real person or property before the court.

Aim of computer forensic

The aim of computer forensic is to assist the court in reaching a conclusion regarding produced data as evidence. Can draw on an array of method to discover data present in a computer system or to restore /recover/retrieve deleted, encrypted or damaged file information exists in computer system. The information procreates during the course of examination and analysis of data would assist in the investigation of crime and deposition in the court law.

Forensic analysis of computer or digital evidence

Computer forensic experts or examiner use an array of methods to get information held in computer system or discover deleted, damaged and encrypted or password protected data that stored in computer system. After analysis of collected data the information generated during

examination would become helpful in investigation of crime and deposition of courts of law.

Array of method

Technically an array is a data structure that contains a group of elements (values or variables) and those elements are all of same data type called string or integer. Arrays related to set of values can be easily sorted or searched. An array is used to store a collection of data. In simple words it is a pre-defined programs used to store or retrieve collection of data.

The whole process of collection, examination, extraction, analysis and then presentation consist of several steps. The last step 'presentation' is the documentation and reporting of the analysis. The documentation and reporting is the sum up of forensic investigation (search and seizure) and examination. Such report assist the investigator, prosecution and to the court in reaching to conclusion of the case. The steps which the forensic examiner followed during investigation and forensic examination of a case, be described herein as²-

Step1: The first step is Acquisition of evidence. It includes acquisition from seized computer, equipment's used, hardware and software used, network including ISP (Internet Service Provider) and from the on crime site.

Step2: The second step is security of digital evidence according to the guidelines of the department. As we know the digital evidence is delicate in nature. It can be easily distorted and spoiled, so make copies of hardware and software configurations to the examiner's computer after that verification of operation of the examiner's computer system is needed.

Step 3: The third step includes the protection of static and magnetic

Corresponding author


*E-mail: bhawana.rose@gmail.com (Bhawana Saxena).

DOI: <https://doi.org/10.53724/lrd/v7n2.3>

Received 20th Oct. 2022; Accepted 30th Nov. 2022

Available online 20th Dec. 2022

2456-3870/©2022 The Journal. Publisher: Welfare Universe. This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

 <https://orcid.org/0000-0003-0490-2039>



fields by disassemble the case of computer configuration.

Step 4: The fourth step includes the identification of storage devices including internal, external or both and then get separated them from the system.

Step 5: The fifth step includes making of copies of all the internal storage devices and hardware configuration, which also includes condition of the drive like (size, model, jumper setting, location etc) and copies of internal components like video card, sound card, network card, memory card, Media access control (MAC) and Personnel Computer Memory Card International Association cards (PCMCIA).

Step 6: The sixth step is the disconnection of storage devices from back from the power supply and from data cable and motherboard to prevent the damage of data.

Step 7: The seventh step is "Control boot". The forensic examiner get back configuration from the suspect's device through 'control boots' process then they perform a controlled boot function to capture CMOS/BIOS information.

CMOS- is a Secondary metal oxide semiconductor chip used to store Bios configuration.

While BIOS, stand as (Basic Input Output System). It is a set of routines stored in read only memory that enables a computer to start the operating system and to communicate with various devices in the system such as disk drive, keyboard, monitor, printer and communication port.

Step 8: The eighth step includes 'Examination of evidence'. The examination of evidence involves extraction and analysis of digital evidence. The getting of recovered data from the device is called 'extraction' and analysis is the elucidation of the recovered data and after that it will be placed in a resolving format. The process of extraction includes identification and recovery of data at physical level like drives but it does not include file system, as well as identification and recovery of data at logical level. The file system extraction is the logical extraction like extraction from installed operating system(s), file system(s), and/or application(s) and extraction of name and size of the files, date and time, file location, extraction of the unallocated space, extraction of password- protected, encrypted and compressed data, recovery of deleted files, extraction of file slack. Logical extraction involves analysis of extracted data.

Step 9: The Ninth and the last step of forensic examination is the 'analysis of extracted data'. It interprets the extracted data to determine their significance to the case. Such analysis involved Data hiding analysis, time frame analysis, time frame analysis and owner and possession analysis.

Documentation and reporting of the results by the forensic examiner:

After the analysis of digital records, the forensic examiner reduced his results in writing such process is called documentation and reporting. Documentation is an ongoing process throughout the examination of

digital records or evidences. It must contain complete and accurate results of the examination, consistent with departmental policies and the specifics of writing of reports will also be suggested under departmental policies.

Sensitiveness of electronic evidences

The electronic evidences are so sensitive and their storing or keeping needs special care and materials those investigating officers or teams are proposed to be seized needs careful handling. The floppies and hard disk are magnetic media that are extremely sensitive. The hard disk is the most critical part of the computer as it contains the entire data and must be imperatively handled with due care. A simple carrying of floppy by putting it in bags or pocket may damage it and its data therefore an anti-static wristband is required to be worn before starting of search and seizure operations. A CD or Compact Disk, is an optical media and is very delicate by its outer structure it can be break by its roughly usage but it is less sensitive as compared to other storing Medias because these are based on semi-conductor technology.

The following guidelines were proposed by the Computer Analyses and Research Team of FBI Hqrs Lab, Washington DC are useful, to be followed by the investigators.³

1. An anti-static plastic material must be used only for wrapping media or equipment while the magnetic media like hard disk and others must not be wrapped in plastic cover due to the risk of static electric discharge.
2. All the parts of the computer system when get separated they must be packed separately and each part must be properly labeled.
3. The label having a restricted note like 'restricted to x-rays and magnetic fields' must be affixed.
4. All hardware materials even registers, papers (loose papers also), documents, manuals and maps etc. found on site must not be touched by bare hands and use card board boxes for their packing.
5. Use gloves to preserve latent fingerprints for examination during investigation.
6. Ensure the removal of power supply from all devices and standing apart network connection properly from the system.
7. In case of searching of cases related to pornography (including child pornography), ensure the seizure of cameras, possible available other sources like printing and scanning devices and hard copies of photos if found available on crime site or else.

Conclusion

It is concluded that forensic examiner or expert plays an important role in preventing and controlling cyber-crime. Acquisition and examination of digital records and after that their examination and analysis is a complex process. Normally educated investigator officials cannot get success on cyber-crime without taking assistance of forensic examiner or experts. The Information technology (IT) infrastructure is

a very complex structure. The Information Technology Act 2000 is not in-depth to fall down cyber-crimes from India, as the technology grows for the betterment of society, the anti-social personalities with mal intention and aiming also grow with rapid speed. The law Enforcement agencies of India are not competent to handle and tackle their new inventions and experiments due to the lack of scientific and technical knowledge of Information technology (IT) infrastructure. The information technology is entirely a complex model we cannot recognize its functionality by bare eyes. The Indian Government is required to make more strong laws, rules, regulations and policies with an objective to diminish online crimes from society. Punishment provisions must also be required deterrent especially in case of child pornography. As we came to know from above discussion this field is purely technical and scientific field, hence required scientific experts as law enforcement agencies during investigation process especially in searching, seizing and analysis process of digital evidences. The Indian Government is required to make a separate unit of only Information Technology and computer science professionally educated law enforcement officials and make such education as primary requisition, at the time of their selection and appointment procedure. Today, almost at many places the law enforcement officials are belong to a simple educated field, they passed the competitive exam and get selection and appointment as law enforcement officials, bearing a charge of investigation of digital crime, as working force /officials. Therefore a question will always arise how do they work? Government

should make a separate post for IT professionals only to be worked as a digital crime or cyber-crime investigator or examiner and forensic expert, as law enforcement officials. Their work will be a team work under the guideline of government and concerning department or body, with a similar motive to resolve the case and fall down its growth from the society. Periodic training of those officials must be made compulsory for their up-dating. In every state there should be a separate cyber Cell which exclusively investigate cyber-crimes. Since cyber-crimes are of technical nature, all the police officers whether constable or sub-inspector rank or new comers there should be a compulsory or special training system to deal such crimes.

Suggestion

1. The government needs to make cyber centers in every district and village area.
2. The government needs to establish a healthy law enforcement system to handle and tackle their new inventions and experiments
3. The government needs to establish a healthy scientific and technical knowledge of Information technology (IT) infrastructure.
4. The Indian Government must make a separate unit of only Information Technology and computer science.

Endnotes

¹ Agrawal, S.C.,(2002), CBI Bulletin, A Central Bureau Of Investigation Publication,Vol.10(1):15-23.

² Forensic Examination of Digital Evidence: A Guide for Law Enforcement <https://www.ojp.gov/pdffiles1/nij/199408.pdf> (Last Seen 10th Oct. 2022)

³ Kaul, R.,(1996),CBI Bulletin, A Central Bureau Of Investigation Publication,Vol.4(1):6-10.