Unit 1: Computer Forensics and Its Significance

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The relevance of cyber forensics
- The concept of cyber forensics
- The various tools used in the implementation of cyber forensics

1.2 INTRODUCTION

The concept of cyber forensics is relatively new in India. The advent of high-speed broadband and mobile internet network at affordable rates has made internet highly accessible to people. However, the improving infrastructure has also contributed to a rise in cyber crimes in India.[82]

[82] Armstrong, I (2002) Computer Forensics Detecting the Imprint. SC Magazine

Cyber forensic is the tool which is employed to detect cybercrimes and to prevent cybercrimes before the crime is committed.

1.3 RELEVANCE OF CYBER FORENSICS

In the case of traditional crimes, the investigating agency visits the crimes scene and collects evidence through various means such as collecting various objects of interest from the crime scene, interacting with the witnesses to the crime, etc. Thus, there is a sense of tangibility to a crime which takes place in the physical world.

However, in the case of cyber crime, the said act is devoid of the same sense of physicality. Since a cybercrime takes place using a computer or such other devices from a remote location, the methods used to detect a traditional crime cannot be employed. One must also remember that since a majority of people are not as well versed with cyberspace, i.e. the notional environment in which communication over computer networks take place, detecting cyber crimes is way more difficult than that of traditional crimes.

Using cyber forensics, the investigating agency is able to gather the evidence pertaining to the commission of cybercrime, including the identity of the perpetrator. The chief objective of cyber forensics is to obtain evidence using various techniques which can be used to make a case before the court of law. A number of cyber crimes such as phishing, hacking, fraud, cyber espionage, cyber terrorism are investigated with the help of cyber forensics. It can be said that without employing the necessary measures afforded by cyber forensics, a number of crimes would have remained unproved and inconclusive.[83]

An important example of the effectiveness of cyber forensics is the BTK serial killer case. From 1974 to 1991 a number of murders took place in Kansas, the United States of America which were suspected to have been committed by a serial killer. However, the investigating authorities were unable to find the culprit behind the killings. In 2004, the investigating agencies started receiving a number of communications from the perpetrator. Some of these communications were sent on a floppy drive. On examination of the floppy disk by cyber forensic experts, it was

[83] Sadiku, Matthew & Tembely, Mahamadou & Musa, Sarhan. (2017) Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering

found that a Microsoft Word document had been deleted from the floppy drive. By analysing the metadata related to the Word document, the investigating agency were able to determine the identity of the perpetrator and the said evidence was considered by the courts while finding Dennis Rader guilty of committing the murders.

1.4 THE CONCEPT OF CYBER FORENSICS

In order to connect to the cyberspace, a user requires to connect to the internet through an Internet Service Provider (ISP). In order to connect to the internet, a user utilises a dial up connection / broadband connection or a mobile network.[84] Thus, in order to obtain evidence, an investigation agency can gather evidence from the following sources:

- The user's computer;
- The servers of the ISP used by the user

Computers maintain data related to the files used by the user in the form of logs. Even if the data is deleted, the logs related to such data is stored in the hard drive through swap files, memory dumps and other unallocated spaces in the hard drive.

Further, when accessing websites, the information is cached in the machine accessing the website. The Oxford Learners Dictionary defines a "cache" as a part of computer's memory that stores copies of data that is often needed while a program is running. "Caching" stores the data related to the web page on the hard drive of the computer.

ISPs maintain logs of the websites visited by users availing internet services through its portals including the IP address and machine ID (Mac ID) of the user.

Using various techniques of cyber forensics, an investigation agency can gather evidence to prove that a machine has been used by the user to commit a cyber crime.

1.5 VARIOUS TOOLS OF CYBER FORENSICS

Before dealing with the various techniques of cyber forensics, it is pertinent to discuss the legal framework.[85]

[84] Mandia, Prosise, Pepe Incident Response & Computer Forensics Second Edition. McGraw-Hill 2003

[85] US Department of Justice Computer Crime and Intellectual Property Section, Criminal Division. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. July 2002 NIJ Electronic Crime

Section 76 in The Information Technology Act, 2000 ("**IT Act**") deals with confiscation of data.[86]

> ***76. Confiscation***.*-Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:*
>
> *Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.*

Further Section 77A of the IT Act provides for compounding of offences committed under the IT Act.

> ***77A. Compounding of Offences****- (1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.*
>
> *Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.*
>
> *Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.*

Scene Investigation – A Guide for First Responders 2001. NHTCU Good Practice Guide for Computer Based Electronic Evidence 2003

[86] IT Act: Offences (Section 65 to 78)
<https://informationtechnologyactindia.blogspot.com/p/offences-section-65-to.html>

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

Section 265B, Code of Criminal Procedure, 1973

265B. Application for plea bargaining *-A person accused of an offence may file an application for plea bargaining in the Court in which such offence is pending for trial.*

The application under Sub-Section (1) shall contain a brief description of the case relating to which the application is filed including the offence to which the case relates and shall be accompanied by an affidavit sworn by the accused stating therein that he has voluntarily preferred, after understanding the nature and extent of punishment provided under the law for the offence, the plea bargaining in his case and that he has not previously been convicted by a Court in a case in which he had been charged with the same offence.

After receiving the application under Sub-Section (1), the Court shall issue a notice to the Public Prosecutor or the complainant of the case, as the case may be, and to the accused to appear on the date fixed for the case.

When the Public Prosecutor or the complainant of the case, as the case may be, and the accused appear on the date fixed under Sub-Section (3), the Court shall examine the accused in camera, where the other party in the case shall not be present, to satisfy itself that the accused has filed the application voluntarily and where-

the Court is satisfied that the application has been filed by the accused voluntarily, it shall provide time to the Public Prosecutor or the complainant of the case, as the case may be, and the accused to work out a mutually satisfactory disposition of the case which may include giving to the victim by the accused the compensation and other expenses during the case and thereafter fix the date for further hearing of the case;

the Court finds that the application has been filed involuntarily by the accused or he has previously been convicted by a Court in a case in which he had been charged with the

> *same offence; it shall proceed further in accordance with the provisions of this Code from the stage such application has been filed under Sub-Section (1).*

Section 265C of Criminal Procedure Code, 1973

> *S. 265C Guidelines for mutually satisfactory disposition In working out a mutually satisfactory disposition under clause (a) of Sub-Section (4) of section 265B, the Court shall follow the following procedure, namely;*
>
> *in a case instituted on a police report, the Court shall issue a notice to the Public Prosecutor, the police officer who has investigated the case, the accused and the victim of the case to participate in the meeting to work out a satisfactory disposition of the case;*
>
> *Provided that throughout such process of working out a satisfactory disposition of the case, it shall be the duty of the Court to ensure that the entire process is completed voluntarily by the parties participating in the meeting;*
>
> *Provided further that the accused may, if he so desires, participate in such meeting with his pleader, if any, engaged in the case;*
>
> *in a case instituted otherwise than on police report, the Court shall issue a notice to the accused and the victim of the case to participate in a meeting to work out a satisfactory disposition of the case;*
>
> *Provided that it shall be the duty of the Court to ensure, throughout such process of working out a satisfactory disposition of the case, that it is completed voluntarily by the parties participating in the meeting;*
>
> *Provided further that if the victim of the case or the accused, as the case may be, so desires, he may participate in such meeting with his pleader engaged in the case.*

To give effect to the content addressed through such aforementioned provisions of the legal framework in the country, there are various techniques implemented that act as tools. Such tools are majorly used for collecting digital evidence related to various limbs of cyberlaw such as disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics.

Disk Forensics Tool aims at addressing concerns arising in association with data recovery, data analysis, tracking senders of emails, analysing forensic registry, extracting forensic thumbnail, etc.

Network Forensics Tool aims at addressing concerns arising in association with analysis of forensic log, tracing sender of emails, analysing network sessions, etc.

Mobile Device Forensics Tool aims at addressing concerns arising in association with the acquisition of software, analysis of mobile phones and smartphones, analysis of mobile devices, analysis of call data records of various service providers, creation of forensic solution for imaging, analysis of sim cards, etc.[87]

Live Forensics Tool aims at addressing concerns arising in association with arriving at software solutions related to acquisition and analysis of volatile data in systems.

Tools of cyber forensics are used and implemented to extract digital evidence that can be used and admitted in courts of law. Since electronic evidence plays a vital and pivotal role in cybercrimes, tools of cyber forensics act as the basis of digital media by allowing anti-forensic techniques to be countered.

The most useful tool used in cyber forensics is the Digital Evidence Search Kit (DESK), which is a machine that law enforcement agents; it further involves the use of a subject machine, which is the device used by the suspect. These two machines communicate with each other using a serial. The DESK system searches for and identifies the keywords in Chinese and/or English using a text pattern file, to locate the words searched for on the subject machine. The DESK function further uses the hash value database that contains fingerprints of certain systems of the file so as to enable verification of file integrity.

The DESK function involves three types of searches:

a Physical Search – This involves performing a search of patterns of individual physical sectors in the storage of the subject machine. Owing to such physical search, evidence of

[87] Bynum, T. (2001) Computer Ethics: Basic Concepts and Historical Overview Stanford Encyclopedia of Philosophy Retrieved 12 January 2007 from
<http:// plato.stanford.edu/archives/win2001/entries/ethics-computer/>

cybercrime stored in unused sectors can be discovered with ease. It further allows locating files independent of the specific file systems.

b Logical Search – This kind of search involves making use of information regarding the file system concerned. A file, which is conceptually a sequence of bytes, is placed in portions of the sequence into different sectors by the file system, in accordance with the logical continuity of the contents thereof.

c Deleted File Search – File deletion, in most file systems, is accomplished by way of modifying only a few bytes of the file system, thereby allowing the content of a deleted file to subsist in the storage system, unless overwritten. Therefore, patterns in deleted files can be traced back until the time that the disk sectors are overwritten by other new files.

1.6 CONCLUSION

Digital forensics is a rapidly advancing field that has many challenges and crosswinds. The opportunities are endless, but they are not for the faint of heart. Frustration is a common partner, so the ability and mentality to press on through is a key characteristic an investigator should have. Someone who needs to be shown how to do everything may want to rethink their career options. A can-do attitude is essential, but the investigator does not need to go it alone. A variety of resources are available to assist, and most of the investigators who have worked through the learning curve to achieve competence are more than eager to help others do the same. Usually, they had others to lean on, so once you reach a level of expertise with the assistance of others, do not forget to return the favor.

1.7 LET'S SUM UP

In this chapter, we studied the significance of computer forensics and its relevancy. We discussed the concept of cyber forensics and finally, ended the discussion with various tools used in cyber forensics and provisions pertaining to it under the Information Technology Act.

1.8 FURTHER READING

- Bell, G., and Boddington, R. (2010). Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? The Journal of Digital Forensics, Security and Law, Vol 5(3).

- De Forest, P. R., Gaensslen, R. E., and Lee, H. C. (1983). Forensic Science: An Introduction to Criminalistics, McGraw-Hill, New York.
- Menn, J. (2010). Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet, PublicAffairs, New York.
- Gogolin, G. (2010). The Digital Crime Tsunami. Digital Investigation, Vol. 7(1-2).
- Kind, S., and Overman, M. (1972). Science against Crime, Aldus Books, London, UK

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of cyber forensic?

Cyber forensic is the tool which is employed to detect cybercrimes and to prevent cybercrimes before the crime is committed.

2) What are the methods/sources that need to be used to obtain evidence in cyber forensic?

In order to obtain evidence, an investigation agency can gather evidence from the following sources:

- The user's computer;
- The servers of the ISP used by the user

3) What is the most important tool in cyber forensic?

The most useful tool used in cyber forensics is the Digital Evidence Search Kit (DESK), which is a machine that law enforcement agents; it further involves the use of a subject machine, which is the device used by the suspect.

4) What are the 3 types of searches under desk function?

The DESK function involves three types of searches:

a Physical Search
b Logical Search
c Deleted File Search

1.10 ACTIVITY

Explain the concept and relevancy of cyber forensics in the present era, along with the various tools that are used to gather evidence and relevant provisions under the I.T. Act? (800-1000 words)