Unit 1: Computer Forensics and the Process of Confiscation

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- Concept of computer forensics
- Techniques in computer forensic
- Preserving Computer Evidence

1.2 INTRODUCTION

The term ***'computer forensic'*** was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1191. It is a branch of forensic science which is devised to identify local preserve of extract digital information from the computer system to produce and store evidence of the cybercrime before the law court.[117] Dr Clifford Stall, an astronomer and professor in the University of Berkeley has defined - computer forensic, as that branch of forensic science wherein cybercrime investigation and analysis techniques are applied to determine potential legal evidence in a computer environment. Internet-related forensics broadly cover three areas, namely (i) computer forensics, (ii) cyber forensics, and (iii) software forensics.

Cyber forensics plays a crucial role in solving crimes. The collection of forensic evidence serves an important key role that sometimes it is the only way to establish or exclude any case between suspect and victim or crime scene, eventually to establish a final verdict. As Internet technologies associate with us into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted which helps in the investigation process.

1.3 CONCEPT OF COMPUTER FORENSIC

An individual uses his computer to connect the internet via an ***Internet Service Provider (ISP)*** by using either a dial-up connection or a leased line/broadband/ mobile network facility.[118]

There are two levels at which evidence of Internet usage exists:

a) Individual Level
   - On an individual's own computer, computer system or computer network.
   - On the websites assessed by the individual using his own computer, computer system or computer network and

b) ISP Level

[117] Rohas N, "Understanding Computer Forensics", Asian school of cyber law, 2009
[118] Cyber Forensics and Indian Approach
<http://ptlb.in/cfrci/?p=15>

- On the service of an individual's ISP.

1.4 COLLECTING EVIDENCE AT INDIVIDUAL'S LEVEL

Computers usually store text, graphic, image files, e-mails messages etc. in the hard disk during its routine use. User may keep on deleting the unwanted material regularly to free up disk space. Similarly, Chat rooms, Internet Relay Chat (IRC), Internet telephony sessions are real-time discussions happening on the Internet; it is optional for the user to maintain logging files of these sessions.[119]

Caching means copying of a web page/site and storing that copy for the purpose of speeding up subsequent access. It ensures that the load on the servers of origin will be reduced as they can be accessed from the cached servers. With the help of browser software, a user can retrieve any web page from the computer's cache memory rather than going back to the original source site. From the legal standpoint, the information saved in a web-browser cache whether or not intentionally retained constitutes ***'possession'.***

1.5 COLLECTING EVIDENCE AT ISP LEVEL

Logs maintained by the ISPs of the users using dial-up/leased line/ broadband/mobile-Internet connections to connect to ISP indicate the time and duration of Internet usage/connectivity along with the IP address. It will corroborate other types of evidence that has already been gathered during the investigation. Admissibility of such evidence cannot be questioned as it clearly highlights not only the time and duration of computer's Internet usage/connectivity but also the fact that during a specific time period, the user's computer had been working as a sort of *'computer network'*. It is important to note that ISPs under the licensing conditions are collecting traffic data in the form of IP addresses, machine IDs (Mac ids), date and time (of communication), size of data (received/sent) and other related information.

[119] Cyber Forensic Investigation Solutions in India Are Needed <http://ptlb.in/cfrci/?p=9>

1.6 PROCESS OF CYBER FORENSIC

- As soon as the crime is reported and is registered with the police, the investigation starts and data is collected from the place of crime/computer system and is examined using forensic techniques.[120]
- The computer system seized is examined thoroughly to find out the digital data which can act as evidence.
- Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password-protected files, log files, system files etc.
- After all the information is gathered from the computer system the original form of evidence is recovered. It must very importantly be kept in mind that never to harm the originally recovered data while applying forensics.
- Create a mirror image of the original evidence using a different mechanism like bitstream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for the investigation.
- Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.
- Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

1.7 PROBLEMS WITH PRESERVING COMPUTER EVIDENCE

Preserving evidence is not an easy task.[121] There exist both human and technical barriers to the evidence gathering mechanism. One must be aware of such limitations:

- Some of the facilities within the browsers to save WWW pages to the hard disk are imperfect- as it may save the text but not the associated images.

[120] Cyber Forensics
<http://www.cyberlawsindia.net/computerforensics1.html>
[121] Sadiku, Matthew & Tembely, Mahamadou & Musa, Sarhan. (2017) Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering

- In case of some very complex pages, involving *'frames'* and *'templates'*, there could be a perceptible difference in what is seen on screen and what is saved on the hard disk.
- The method used to save a file to the hard disk may not carry any individual labelling, which shows where and when it was obtained. The problem with such saved files is that they could be easily modified or forged.
- It is difficult to tell when a specific page was last acquired due to the browser cache facility. Thus if one examines a whole series of cached pages, it is not easy to pinpoint which page came first and which later.
- It should not be forgotten that many ISPs use proxy servers to speed up the delivery of popular pages. Thus a user of such an ISP may not be sure that what he has received on his computer is the latest version from the source computer (website) as opposed to an earlier cached version held by his ISP.

1.8 VARIOUS BRANCHES OF DIGITAL FORENSICS

Digital Forensics has a very wide scope.[122] The branches of digital forensics are as follows:

a) Disk Forensics

Disk Forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, FireWire devices, CD, DVD, Flash drives, Floppy disks etc.

b) Printer Forensics

Printed material is a direct accessory to many criminals and terrorist acts. In addition, printed material may be used in the course of conducting illicit or terrorist activities. In both cases, the ability to identify the device or type of device used to print the material in question would provide a valuable aid for law enforcement and intelligence agencies.

c) Network Forensics

Network forensics is a branch of digital forensics that focuses on the monitoring and analysis of network traffic. Network forensics is the process of gathering and examining raw data of

[122] I. Resendez, P Martinez, and J Abraham, "An Introduction to Digital Forensics," June 2014, <https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics>

network and systematically tracking and monitoring the traffic of the network to make sure of how an attack took place.

Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time. Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary. Security professionals routinely use such tools to analyze network intrusions not to convict the attacker but to understand how the perpetrator gained access and to plug the hole.

It also helps to investigate offences after the event, determine how they occurred and identify the party or parties responsible. A digital forensic investigator will gather network based evidence from a particular computing device in the network so that it can be presented in court, conducting a thorough digital investigation and building a documented chain of evidence.

d) Mobile Device Forensics

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Mobile phones, especially those with advanced capabilities, are a relatively recent phenomenon, not usually covered in classical computer forensics. Cell phones vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. Developing an understanding of the components and organization of cell phones is a prerequisite to understanding the criticalities involved when dealing with them forensically. Similarly, features of cellular networks are an important aspect of cell phone forensics, since logs of usage and other data are maintained therein. Cell phone forensics includes the analysis of both SIM and phone memory, each requires a separate procedure to deal with.

It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.

e) Database Forensics

Database forensics is a branch of digital forensics relating to the forensic study following the normal forensic process and applying investigative techniques to database contents and metadata. Cached information may also exist in a servers RAM requiring live analysis techniques.

A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify the actions of a database user. Alternatively, a forensic examination may focus on identifying transactions within a database system or application that indicate evidence of wrongdoing, such as fraud.

Third-party software tools which provide a read-only environment can be used to manipulate and analyze data. These tools also provide audit logging capabilities which provide documented proof of what tasks or analysis a forensic examiner performed on the database.

f) Digital Music Device Forensics

Large storage capacities and personal digital assistant (PDA) functionalities have made the digital music device a technology that should be of interest to the cyber forensic community. The digital music revolution has also seen the digital music device become a common household item. It is only a short time until they too make a natural progression into the criminal world. This progression has already begun. Some of the hard-drive-based devices have capacities upwards of 60GB. With this much storage space for music, developers have branched out and included features like a calendar and contact book (Apple iPod-Music and more). These devices are simply a portable hard drive and have the ability to store other types of files besides music; such as documents or pictures.

An employee could take sensitive information by using the capabilities of a digital music device. Suspects could potentially store critical evidence on these types of devices. It must be determined if current frameworks of cyber forensic science are applicable and to what extent current guidelines can be applied to digital music device forensics.

g) Scanner Forensics

A large portion of digital image data available today is created using acquisition devices such as digital cameras and scanners. While cameras allow digital reproduction of natural scenes,

scanners are used to capture hardcopy art in more controlled scenarios. For a forensic approach, a non-intrusive scanner model identification, which can be further extended to authenticate scanned images is a necessity.

Using only scanned image samples; a robust scanner identifier should determine the brand/model of the scanner used to capture individual scanned images. A proposal for such a scanner identifier is based on statistical features of scanning noise. Scanning noise of the images can be done from multiple perspectives, including image denoising, wavelet analysis, and neighbourhood prediction, and obtain statistical features from each characterization. The same approach can be extended to digital cameras and other imaging devices. The most significant challenge is that ***"analytical procedures and protocols"*** are not standardized nor do practitioners and researchers use the standard terminology.

The technology change will result in new devices emerging in the digital world. Whenever a new digital device enters the market a forensic methodology has to evolve to deal with it. This phenomenon will expand the field of device forensics.

h) PDA Forensics

In the modern era, Personal Digital Assistants (PDAs) are getting immensely popular. They are no longer meagre electronic devices holding personal information, appointments and address book. Modern PDAs are hybrid devices integrating wireless, Bluetooth, infrared, WiFi, mobile phone, camera, global positioning system, basic computing capabilities, Internet etc., in addition to the standard personal information management features.

Investigating crimes involving PDAs are more challenging than those involving normal computers. This is mainly because these devices are more compact, battery-operated and store data in volatile memory. A PDA is never really turned off as long as it has sufficient battery power. Evidence residing in PDA is of highly volatile in nature. It can be easily altered or damaged without getting noticed. In order to collect such evidence and ensure its admissibility in a court of law, sound forensic techniques and a systematic approach are needed. A standard forensic model for PDAs, which provides an abstract reference framework is particularly important in digital crime investigations. In addition to law enforcement officials, such a model can also benefit IT auditors, information security

experts, IT managers and system administrators, as often they are the first responders related to any sort of computer crime in an organization.

1.9 PROCESS OF CONFISCATION

Section 76 of the Information Technology Act, 2000 highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders or regulations made thereunder are liable to be confiscated.[123]

The proviso to the section further highlights that in case if the person concerned in whose possession, power or control computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device is found, establishes to the satisfaction of the court that he was in no way responsible for any of the contraventions, the adjudicating court not to confiscate such devices, under such circumstances. In such a case, the court may make such other order authorized by this Act, against the person contravening provisions of this Act, rules, orders or regulations made thereunder.

1.10 ADMISSIBILITY OF DIGITAL EVIDENCE

Digital evidence usually takes the form of writing or at least a form which can be analogized to writing, it must be authenticated and satisfy the requirements of the Best Evidence Rule.

The proponent of the evidence need not present testimony by a programmer, but should present some witnesses who can describe how information is processed through the computer and used by the organization.

With regard to hearsay, most courts have dealt with the objection to the introduction of computer records by relying on the business record exception. Such an approach may work for audit logs, provided they satisfy the rule, which might not be the case for

[123] N Kumari and A K Mohapatra, "An insight into digital forensics branches and tools," Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies, 2016

computer records collected as part of an investigation rather than as the result of a routine, periodic process. The following are some guidelines to preserve admissibility of digital evidence:

- Upon seizing digital evidence, action should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

In the case of ***P.V. Anwar v P.K.Basheer,***[124]the Court in ***PARAGRAPH 24 OF ITS JUDGMENT*** held that the electronic evidence which is a primary document can be admitted without producing certificate and there is no obligation to satisfy the condition laid down in Section 65B of the Evidence Act, 1872. If that electronic record satisfies the condition under Section 62 then it can be unequivocally admitted as evidence. The same will not be covered either under Section 65A or 65B of the Evidence Act, 1872. Primary evidence is a ***'document'*** which is defined under Section 3 of Evidence Act, 1872.[125]

1.11 CONCLUSION

Cyber forensics plays a significant role in the criminal justice system as we continue to incorporate a range of technologies into our everyday lives. Evidence of all most the types of crime is increasingly found in digital devices that either the perpetrator or the victim used. As a result of this potential evidence which did not exist in the past, investigators of conventional crimes increasingly need to consider any digital evidence that may be available.

[124] *P V Anwar v P K Basheer* [2014] 10 SCC 473

[125] M Reith, C Carr, and G Gunsch, "An examination of digital forensic models," International Journal of Digital Evidence, vol 1, no 3, Fall 2002

In addition, Security professionals routinely use such tools to analyze network intrusions not to convict the attacker but to understand how the perpetrator gained access and to plug the hole. Data recovery firms rely on similar tools to resurrect files from drives that have been inadvertently reformatted or damaged.

1.12 LET'S SUM UP

In this chapter, we have studied the concept of computer forensic along with how the evidence is collected at each level. We also studied the process of cyber forensic and the problems faced in preserving the evidence. Finally, we ended the discussion with the process of confiscation and admissibility of digital evidence.

1.13 FURTHER READING

- The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010
- Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016
- STANDARD OPERATING PROCEDURE OF DIGITAL EVIDENCE COLLECTION (Digital Forensics Department, CyberSecurity Malaysia)

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber forensics?**

   The term *'computer forensic'* was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1191. It is a branch of forensic science which is devised to identify local preserve of extract digital information from the computer system to produce and store evidence of the cybercrime before the law court.

2. Explain the concept of Computer Forensic?

An individual uses his computer to connect the internet via an ***Internet Service Provider (ISP)*** by using either a dial-up connection or a leased line/broadband/ mobile network facility.

There are two levels at which evidence of Internet usage exists:

a) Individual Level

- On an individual's own computer, computer system or computer network.
- On the websites assessed by the individual using his own computer, computer system or computer network and

b) ISP Level

- On the service of an individual's ISP.

3. Explain the process of cyber forensic?

The process of cyber forensic is as follows:

- As soon as the crime is reported and is registered with the police, the investigation starts and data is collected from the place of crime/computer system and is examined using forensic techniques.
- The computer system seized is examined thoroughly to find out the digital data which can act as evidence.
- Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password-protected files, log files, system files etc.
- After all the information is gathered from the computer system the original form of evidence is recovered. It must very importantly be kept in mind that never to harm the originally recovered data while applying forensics.
- Create a mirror image of the original evidence using a different mechanism like bitstream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for the investigation.

- Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.
- Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

4. What are the various branches of digital forensics?

- Disk Forensics
- Printer Forensics
- Network Forensics
- Mobile Device Forensics
- Database Forensics
- Digital Music Device Forensics
- Scanner Forensics
- PDA Forensics

1.15 ACTIVITY

Explain the different branches of digital forensics with illustrations along with the procedure for admissibility of electronic evidence and case laws with respect to it? (1500-2000 words)