Unit 2: Overview of Digital Records and Cyber Forensics

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- Define digital records, its types and characteristics
- Forensic Science and Definition of Cyber Forensics
- Key Elements and Classification of Cyber Forensics

- Know how Cyber Forensics is used by investigating officer

1.2 INTRODUCTION TO DIGITAL RECORDS

In the current era of digitalisation, use of technology to transfer the paper-based information into digital information is very much common with every organisation. Technological advancement has made this change easier through different means. Digitalised information does not only give us the ease of access but also better storage in comparison with paper-based data. But digitalisation is not only limited to convert information from traditional way to technological way. Whatever new data is getting generated, gather and created is directly getting digitalised and it leads to new concepts like big data because the number of digital records is increasing tremendously day by day.[13]

The information residing in computing devices is in the form of 0's and 1's, this is also known as the mother tongue of computers (binary). All the information is nothing but the combination of digits (0's and 1's) hence we call them digital. Whatever the information is being stored in the digital format is been accessed with the help of software in human understandable form. Together this digital information is called as digital records. This digital information is mainly stored in different storage devices in different formats.

1.3 DEFINITION AND SCOPE

Digital record is the information which is mainly stored in computing devices in the form of 0's and 1's.

Digital record is a form of electronic record which is electronically generated or stored in different storage devices.

[13] The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010

Digital record is also defined as a record created or maintained by means of digital computer technology which includes records that are born digital or have undergone conversion from a non-digital format.[14]

It is a record which is maintained in a coded numeric format that can be accessed using a combination of hardware and software which translates them into text or images which can be comprehended by the human eye.

1.4 CHARACTERISTICS AND TYPES

The information in the form of digital records correctly reflects certain characteristics

- ***Confidentiality***

  Confidentiality refers to only the authorized person could have access to the information. It is also equivalent to the privacy of data. In simple language, confidentiality is the measures undertaken to prevent sensitive information from reaching to wrong people while making sure the right people can access it.

  Example: Data encryption, User ID-Passwords etc.[15]

- ***Availability***

  Availability simply means the information should be available in required format whenever needed. That means protecting the information from intentional as well as non-intentional loses. It is making sure that information is available for use all the time.

  Example: Performing hardware repairs, troubleshooting operating system issues, enough bandwidth availability preventing bottlenecks etc.

- ***Integrity***

  Integrity means maintaining the state of the information constant throughout its lifecycle. It also means consistency accuracy and trustworthiness of the data. The information should not change in transit also, it should be protected from alteration by unauthorized people.

- ***Authenticity***

[14] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016

[15] Forensic Examination of Digital Evidence: A Guide for Law Enforcement

The authenticity of the information mainly involves proof of identity. Which means it is the assurance that the information is from the source it claims to be from. Authentication is used to verify authenticity.

- ***Reliability***

  A reliable record is the one whose content is full, accurate and trustworthy. Reliable records are mainly used for interpretation and conclusion.

- ***Usability***

  It is the characteristic is recorded which mainly addresses further use of the digitally stored information. It is the record which should be located, retrieved and interpreted.

TYPES OF DIGITAL RECORDS

Based on the type of information, Digital records are classified as follows:

- ***Image File***

  This record mainly contains still images in the form of photographs. These images are stored in a variety of data formats such as JPEG (Joint Photographic Experts Group), TIFF (Tagged Image File Format), GIF (Graphic Interchange Format) etc.[16]

- ***Text File***

  This digital record mainly consists of different type of text which includes Tables, Databases, and Logs etc. These digital records also contain File format like .DOC, .PPT, .XLS, .PDF (Portable Document Format).

- ***Audio File***

  In this type of digital records, the sound is recorded which can be originally produced from analogue or digital formats. The audio files have several characteristics like Sampling Frequency, Bit-depth, Mono or Stereo. The examples of audio files are.WAV, MP3 etc.

- ***Video File***

  Video file is nothing but moving images recording which can be synced with audio. Pixel array, Frame rate per second, Aspect Ratio, Bit Rate, High Definition are important

[16] Arkfeld, M R (2002-2006), Electronic Discovery and Evidence. Law Partner Publishing, LLC. Phoenix, Arizona

characteristics of video files. The examples of video files are .AVI (Audio Video interleave), .MXF (Material Exchange Format), .WMV (Windows Media File) etc.

- ***Mark-up Language***

  This file format mainly contains embedded instruction for displaying the content over the website. This file is responsible for the text and graphical representation of the information over the World Wide Web. Examples of these files are .HTML (HyperText Mark-up Language), .XML (Extensible Mark-up Language) etc.

1.5 ADVANTAGES AND DISADVANTAGES

ADVANTAGES OF DIGITAL RECORDS

- **Easy to gather, store and access**

  Due to the different types of input available, it becomes very easy to collect and store information digitally. Example: Barcode reader, Document scanner, Touch screen etc.[17]

- **Speed**

  Because of high computing power an advanced networking devices, it's becoming faster to transmit, search and processing of the digital information.

- **Cost**

  Cost for overall digital records is comparatively cheaper in many aspects like storage, transmission etc.

- **Multimedia**

  This gives added advantage to represent the information in more presentable and active ways.

DISADVANTAGES OF DIGITAL RECORDS

- **Equipment Cost**

  When an organisation goes paperless there is a huge volume of data which is held on paper have to be converted to digital format. The cost of hardware and software needed

[17] Boucher, K, and Endicott-Popovsky, B (2008), "Digital Forensics and Records Management: What We can Learn from the Discipline of Archiving"

for this holds a substantial amount of money. This infrastructure also becomes obsolete in a relatively short time.

- **Privacy and security issue**

  As digital information increases, the functionality aspect like access and availability, privacy and security decreases reciprocally.

1.6 RELAVENCE TO E-COMMERCE AND E-GOVERNANCE

The digital India programme is a flagship program of the Government of India with a vision to transform India into digitally empowered society and knowledge economy. Information technology Act 2000 mainly addresses the legal recognition of digital records in e-commerce and e-governance.[18]

E-commerce is also known as electronic commerce is the activity of commercial transactions carried through computing and networking devices. E-commerce activity is rapidly growing in India which adds around 6 million new entrants every month. Amazon, Flipkart, Paytm, Snapdeal are few examples of E-commerce companies in India.

E-governance is defined as the use of computing technology and networking across government departments. It mainly involves the conversion of the paper base transaction into digital records. This has bought many projects under digitalisation namely Income Tax, Passport, Land records, Insurance, Visa immigration etc.

1.7 INTRODUCTION TO CYBER FORENSICS

Cyber Forensics is a rapidly growing field of forensics which mainly addresses all sort of digital evidence. Due to the increasing use of technology in everyday life, there are lots of digital records gets generated every now and then in different computing devices. These digital footprints come very handily during the investigation of all sort of criminal activities. Cyber

[18] Richard III GG, Roussev V Next-generation digital forensics Communications of the ACM. 2006 Feb 1;49(2):76-80

forensics gives us an in-depth view and understanding of these digital records in various situations. Hence, cyber forensics is not only used by the government but also private organisations.

1.8 DEFINITION

Cyber Forensics mainly consists of the integration of two terminologies as Cyber and Forensics. Cyber is defined as a space created by interconnected computer devices across the globe. The word cyber refers to digitalisation, the culture of computers and information technology.

Forensic means suitable for use in a court of law. Hence, Cyber forensics is defined as a branch of forensic science which addressed the recovery and investigation of the evidence found in digital devices. It is also sometimes referred to as digital forensics because of the direct relation with digital records.

Cyber forensics is a branch of forensic science which aims at a constructive way of identifying, reserving analysing, recovering and presenting the digital evidence in a court of law.

Cyber forensics is the application of investigation to search, gather and preserve the evidences from computing device in a way that is suitable for presentation in a court of law. CERT (Computer Emergency Response Team) defines cyber forensics as the process of using scientific knowledge for collecting analysing and presenting evidence to the court.

1.9 FORENSIC SCIENCE

Forensic science deals with recovery and analysis of latent evidence. Latent evidence may have different forms right from fingerprints on the glass to DNA evidence recovered from blood stains to the deleted SMS of mobile phones. The main objective of forensic science is to find out what has happened, who is affected, what has been used, how it has been used and who has committed the act. The first objective is to gather all the facts around this. Next objective is to present the data in a manner which is acceptable for the court. Forensic science is the application of science governed by legal standards of admissible evidence and criminal procedures. Forensic scientists are the group of people responsible to carry out the tasks of forensics namely collecting,

preserving and analysing scientific evidence during the course of the investigation. Many times forensic scientist visits the scene of the crime to collect the evidence in a proper forensic manner. Forensic scientist also gets testified as an expert witness in both criminal and civil cases.[19]

In the recent decade, documenting forensic science has become more efficient. Forensic scientists have started using advanced technologies in forensic processes. It has resulted in the accuracy of findings and also helped into logical reasoning of the incident. Unlike other areas of technology, forensic science has made significant growth and contributed to the court proceedings by eliminating all the doubts of prosecution towards the evidence.

1.10 ELEMENT OF CRIME

The legal definition of all crimes contains certain elements. If the government is not able to prove the existence of these elements then the conviction cannot be obtained in a court of law. That means crime can be broken down into elements which should be proved beyond a reasonable doubt by the prosecution. There are three main elements of every crime:

1. ***Criminal Act***

   It is the activity prohibited by law. It is also referred to as conduct which means an action carried out by accuse.

2. ***Criminal Intent***

   It is also called a purpose or state of mind resulted in a criminal act. It is further classified into four categories

- Purposely
- Knowingly
- Recklessly
- Negligently

3. ***Concurrence***

   Concurrence means the occurrence of both the above two elements at the same time.

Apart from these three, there are other elements of crime such as

[19] Carrier B Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence. 2003 Jan;1(4):1-2

- ***Law***

  There must be some law which addresses the act. That may sound obvious but there are certain acts which are objectionable but not criminal. Example Parking a vehicle in front of someone's gate.

- ***Burden of Proof***

  Depending on the case, the allegations or defence made in the court has to be proved beyond a reasonable doubt. The burden of the proof mainly lies with the one who makes certain statements in the court.

- ***Exculpatory Evidence***

  This is an important concept regarding the evidence that proves the accused innocence. In a criminal case, prosecutors have a legal duty to turn over exculpatory evidence to the defence.

1.11 KNOWLEDGE REQUIRED FOR CYBER FORENSICS

Cyber Forensics requires an understanding of various computing and networking concepts.[20] As cyber forensics consists of different technologies related to digital devices, the investigator should have solid background knowledge of the following topics:-

Hardware

On cannot perform forensic analysis without the knowledge of computer paths. That means the investigator should have a working knowledge of motherboard, Processor, Hard Drives, RAM and Expansion slots.

Hard Drives

Hard drives record and store the data in magnetic form on platters. The platters are organised on the spindle with Reading/Write head.

The data is organised as follows

- A sector is a basic unit of data storage on the hard disk which consists of 512 bytes.
- A cluster is a logical group of sectors.

[20] Breeuwsma, Marcel, et al "Forensic data recovery from flash memory." Small Scale Digital Device Forensics Journal 1.1 (2007): 1-17

- Sectors are in turn organised by tracks.

There are four types of hard drives:

1. SCSI- Small Computer System Interface
2. IDE- Integrated Drive Electronics
3. SATA- Serial Advanced Technology Attachment
4. SSD- Solid State Drive

RAM (Random Access Memory)

RAM plays a vital role in a forensic investigation point of view. Sometimes it's important to carry out forensics of running machine. For that, live memory capture is required. That means to take what is currently in RAM. Hence, live memory capture become quite important.

Following are the different types of RAM:

- DRAM (Dynamic RAM)
- SGRAM (Synchronous Graphic RAM)
- PSRAM (Pseudo-Static RAM)
- RLDRAM (Reduced Latency RAM)

Operating System

Operating systems are responsible for different operations on the machine. Cyber forensic approach changes with different operating systems. Hence, detailed knowledge of operating system enhances forensic investigation.[21]

Following are some of the examples of Operating System:

- Windows
- LINUX
- Macintosh
- IOS
- Android

Files and File Systems

The file system is the way through which computer organises data on a disk. Knowledge of file system gives added advantage to the investigator.

Following are some examples of file systems:

[21] SWGDE Best Practices for Computer Forensics, Scientific Working Group for Digital Evidence, Version 2.1

- FAT (File Allocation Table)
- NTFS (New Technology File System)
- EXT (Extended File System)

Networks

Many cybercrimes take place across the network. Strong understanding of the basics of networking helps the forensic investigator to unearth the important findings to different networking devices and related technologies. Hence, it is advised to have the following device and technologies:

Network topologies, Types of the network (LAN, WAN etc), Types of cables, WiFi, Hub, Switch, Router, Networking protocols etc.

1.12 CLASSIFICATION OF CYBER FORENSICS

Cyber forensics is an emerging practice to discover digital evidence through different computing devices and prosecute the criminals in a court of law. These digital footprints spread across multiple gadgets used by criminals. Cyber forensics is classified into many sub-branches depending upon the technology used for the storage of information in different computing devices around us.

Disk Forensics

It is also called as storage device forensics. It mainly deals with extracting information by searching the required data through active and deleted files. This field of forensics also targets unallocated and slack spaces of storage media.

Mobile Device Forensics

This branch mainly addresses forensics of all cellular devices like mobile, tablet, pagers etc. Mobile forensic retrieves the information like address book, call logs, SMS, photos, videos, audios etc.

Network Forensics

It mainly focuses on monitoring and analysing network traffic for the purpose of intrusion detection, information gathering, legal evidence etc. It is one of the proactive forensic investigation techniques. It also includes a log analysis of different networking devices.

Database Forensics

In many software, information is stored in the form of a database. Hence, database forensics comes very handy in order to retrieve information related to databases. It mainly consists of metadata analysis, timestamp analysis and deleted record recovery of the databases.

Malware Forensics

It mainly deals with investigating and analysing malicious code in the system which may be in the form of Virus, Worm, Trojan, and Rootkit etc.

Email Forensics

This branch of forensics is responsible for recovery and analysis of emails which includes email source investigations, email attachments, contacts and calendar invites of email etc.

Memory Forensics

It aims at collecting and analysing information from system memory in the raw form. The system memory mainly consists of system register, cache and RAM.

Wireless Forensics

It is a subcategory of Network Forensics which targets the methodology and tools required to collect and analyse wireless network traffic data.

1.13 KEY ELEMENTS OF CYBER FORENSICS

Following are the key elements which encompass cyber forensics:

The Identification and Acquisition of Digital Evidence

It is important to have knowledge of possible evidences lying around the crime scene. The cyber forensic investigator should be able to identify the type of information stored in a device and also the format of that data. With the help of this information, the appropriate technology can be decided to extract the evidence. The acquisition process can vary device to device. During the acquisition process, the investigator can acquire the evidence either by creating an image or by cloning the disk.

Preservation of Digital Evidence

This is a critical element of forensic investigation in which the evidence is stored by protecting it against any type of alteration or tampering.

The Analysis of Digital Evidence

This element consists of loading, processing, extracting of the identified evidence. This is the main element of cyber forensics. The extraction produces a binary data which should be analysed and processed to convert it into human-readable form.

The Reporting of Digital Evidence

This element consists of a collection of all the findings stated in such a way that it can be understood by any person. The report should be in very simple terms giving the description of the item mainly findings and conclusion.

Presentation of the Digital Evidence

This element is directly related to the representation to the court of law. The proper representation increases the chances of admissibility of the evidence.

1.14 HOW CYBER FORENSICS HELP INVESTIGATING OFFICER

Discover all files

A casual viewer may not able to view all the files present over the system. Through forensic view, investigator can discover all the files which are present on the system which includes hidden files, password-protected files, encrypted files, hidden files etc.

Data Recovery

Cyber forensics helps into the recovery of the deleted files from the disc. Cyber forensics can also carve overwritten files to extract data to some extent. Data recovery also unearths the files from unallocated or slacks space of the discs.

Keyword Search

Cyber forensics helps to index of the hug information which ultimately helps investigator to find out the relevant evidences effectively and faster.

Timeline Analysis

Cyber forensics can give the proper timeline of the identified evidence with the help of different metadata and event logs of the system. With the help of timeline analysis, the investigator can have detailed knowledge of when particular evidence been created, accessed and used for the crime.

Volatile Evidence Analysis

Forensics of volatile data helps the investigator to know what is currently happening on the system. It can be done by the analysis of RAM and cache memory. This also gives added advantage to monitor live attacks.

Root Cause Analysis (RAC)

Cyber Forensics can help the investigator to identify the root cause of the said crime by complete analysis of the computing devices involved in a particular act.

Despite all above cyber forensics can also be used for some other reasons like

Operational Troubleshooting

Better incidence response and recovery

Log Monitoring

Data Preservation

Business Continuity

Better Vulnerability Detection

1.15 LET'S SUM UP

In this chapter, we have studied the concept of digital records and cyber forensics along with its characteristics, advantages and disadvantages and types. We also studied how it is relevant to e-commerce and e-governance. Finally, we ended our discussion with how cyber forensics can help the investigating officers.

1.16 FURTHER READING

- Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
- Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3rd Edition, Cengage, 2010 BBS.

1.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are digital records?**

Digital record is a form of electronic record which is electronically generated or stored in different storage devices.

2. **What are the different types of digital records?**

Digital records are classified as follows:

- Image File
- Text File
- Audio File
- Video File
- Mark-up Language

3. **What is cyber forensics?**

   Cyber forensics is a branch of forensic science which aims at a constructive way of identifying, reserving analysing, recovering and presenting the digital evidence in a court of law.

4. **What are the different types of cyber forensics?**

Cyber forensics is classified into many sub-branches depending upon the technology used for storage of information in different computing devices around us.

- Disk Forensics
- Mobile Device Forensics
- Network Forensics
- Database Forensics
- Malware Forensics
- Email Forensics
- Memory Forensics
- Wireless Forensics

1.18 ACTIVITY

Briefly explain the meaning of cyber forensics along with its elements that are used in crime scene and its classification? Also, elucidate in what way cyber forensics can help the investigating offices with a case study. (1500 words)