IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Digital Forensic And Role Of Computers In Digital Forensic

[1] Shraddha Vedre, [2]Waman Parulekar
[1]MCA Intern, [2]Assistant Professor, Guide
[12] Department of MCA
[12] Finolex Academy of Management and Technology, Ratnagiri

Abstract: Nowadays digitalization is increasing very fast, all the organizations and individuals are taking benefit of digitalization in their working process. For that purpose, we need a digital system which helps us to perform various tasks within less time. Also, for our entertainment purpose we use social networking site. There is nothing wrong in this, but we should take care while handling social network and our systems because as the digitalization is growing the rate of crime is increases. So should install some software which prevents cyber-attack. We should aware what types of methods are available when any attack is done. So basically, this paper will focus on digital forensics and computer role in it, which will help us when attack is happened.

Index Terms **– digital forensic, role of computers, cybercrime, cyber-attack, types of digital forensic**

I. ABSTRACT

Nowadays digitalization is increasing very fast; all the organizations and individuals are taking benefit of digitalization in their working process. For that purpose, we need a digital system which helps us to perform various tasks within less time. Also, for our entertainment purpose we use social networking site. There is nothing wrong in this, but we should take care while handling social network and our systems because as the digitalization is growing the rate of crime is increases. So should install some software which prevents cyber attack. We should aware what types of methods are available when any attack is done. So basically, this paper will focus on digital forensics and computer role in it, which will help us when attack is happened.

II. INTRODUCTION

The study is to examine the importance of the Digital Forensics & Role of Computers in Digital Forensics. As we see growth of internet, social media cybercrime is also growing explosively. So, the response to those cybercrimes the field of digital forensics is emerged. Basically digital forensics is the branch of forensics science which mainly focus on the carefully investigation and recovery of the evidence or material found in the devices related to the cybercrime. The digital forensics not only include data in your desktop or laptop, mobile but also include data which is transmitted in private network The term digital forensics was first used as computer forensics. Digital forensics is used to solve crimes, whether they be physical crimes or digital crimes.

The goal of this process is to preserve any evidence in its most original form while performing investigation. The main aim of digital forensics is to present a structured inspection while arranging a documented series of proof and evidence to find out completely what happened on the digital device. With the growing importance of computer security today and the seriousness of cybercrime, it is important for computer professionals to understand the technology that is used in digital forensics. This paper will discuss the need for digital forensics to be practiced in an effective and legal way.

Definition of Digital forensics: " Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery, investigation, examination and analysis of material found in digital devices, often in relation to mobile devices and computer crime."- Wikipedia

The term digital forensics was first Known as computer forensics science. Then it has extended to cover the examination of any device that can be mobile, laptop, desktop or any electronic device which store advance information. This paper focus on the history of digital forensics, types of digital forensics, objective & process of digital forensics, also describes the computer tools which use in digital forensics.

III. LITERATURE REVIEW

A. Digital forensic research: Current state of art-Shriram Raghavan

This research paper focused on the digital forensics' importance. The digital forensic process is multi-staged which involves the collection of digital proof from one of multiple crime scenes, called as evidence acquisition [1]. This is followed up by digital forensic examination of the contents of the evidence using forensic toolkits which gives different levels of abstractions to data. This process also discovers hidden, deleted, lost data form devices and detect and detect and decrypt encrypted data. Using the software support the metadata can be extracted for analysis purpose. The digital forensic analysis covers the realm of analyzing data to understand the set of possible explanations and associated logical sequences of events which explain the state of data in digital evidence [1]. Digital forensic process modeling has attempted to provide overall growth to the area by proposing new theories and principles for the development of methodologies and forensics tool in the digital investigation process. The overall taxonomy is illustrated in this paper. The author provides the detail information about digital forensics and need of digital forensics.

B. Digital forensic And Its Analysis Tools

In this paper, author examined distinctive forensics tools used for analysis security flows in digital forensics and also the detailed review of cyber forensics. Digital evidence can also be obtained from the data structure locate in memory by using different tools. The new process model is selected to collect essential evidence quickly and investigate the crime immediately. The Stepwise Forensic Process Model presents the stepwise and in-situ approach provides incident identification, recovery, analysis. The SFPM suggest a new investigational model for selecting the target and analyzing the relevant evidences only [2]. It is based on the crime scene situation and is done on purpose to quickly selecting and investigating the system, to overcome the limitations of the traditional forensic model.

Due to rapid increase in number of internet users across the world the frequency of cybercrime or digital attacks has quickly increased. Therefore, the need to decide effective methodologies and develop well organized tools to detect these criminal attacks timely.

In this paper author examined different tools which is used to perform digital forensic analysis. It includes forensic analysis of encrypted drives, disk analysis, memory analysis. Also provides the provisional study of tools regarding cyber forensics analysis.

IV. PROBLEM DEFINITION

With the rise in use of internet and technology, the increase in cybercrime is inevitable. Like in real life, people who use electronic devices like mobile, laptop, desktop etc. leave behind different footprints, traces and marking. This virtual or digital traces could be file fragments, activity logs, timestamps, metadata and so on. Digital forensics is new forensic science that involves finding of evidence from devices like laptop, desktop, mobile phones or public and private networks. Forensic teams identify, investigate, examine and preserve the digital evidence and present it in the court. Whether data has been compromised by a cyber-attack or files encrypted by ransom ware, data forensic experts can help to determine how the attack took place, what the damages were, and in many cases, who is attacker [3]. If any person or organization was recently victim of cyber attack, then it may be difficult for them to decide what action should be taken. So, the knowledge of digital forensic process will help them to find right way. Also knowing digital forensic tool will help you to know what your job is in case of cyber attack.

V. OBJECTIVE/SCOPE

It helps to identify, analyze and preserve digital devices and public and private networks related materials in such manner that it helps any agency for investigation and present those materials as proof in court of low, means to produce the evidence in the court, which can help to punish the criminal. With the help of computer tools, finding of cybercriminal done within lower time. Designing procedure or techniques at the suspected crime scene which will help to ensure that the digital evidence obtained is no corrupted. It helps you to recognize the proof very fast Helps you to identify the evidence very fast and also allows you to estimate the future impact of the malicious activity on the victim. To produce a computer forensic report which include a complete report on the investigation process. Recover lost, hidden or deleted data from system where the attack took place to prosecute criminal. Helps to efficiently tracks down cyber criminals from anywhere in the world. To save person's or organization's money and valuable time.

VI. METHODOLOGY

Research design- The study is to examine the importance of the Digital Forensics & Role of Computers In Digital Forensics. Knowledge of cybercrime is necessary for every one and if any person or organization was recently the victim of cyberattack, it may be difficult to decide what next course of action should be. Knowledge of digital forensics can lead you in the direction to understand what information was compromised, what action should be taken next.

Data collection- it began using reading articles on digital forensics. Articles includes all information about digital forensics and its importance. Also, I refer some research papers related digital forensics. Also, I found information on website which was very helpful to further study.

VII. ANALYSIS & FINDINGS

A. History Of Digital Forensic

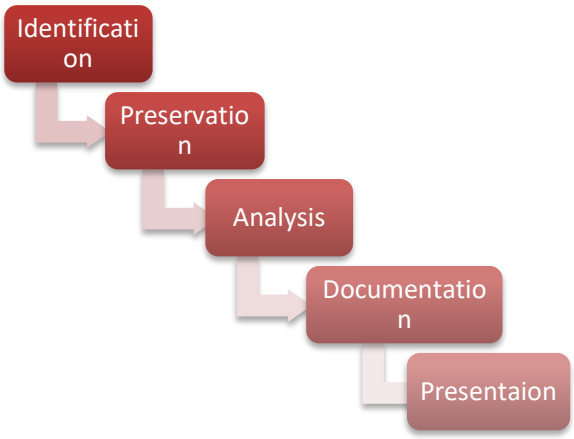
Until the 1990 the term digital forensics was known as computer forensics and the low of enforcement officers were the first computers forensic technicians. As the most documentation happened digitally, the area of concern for low of enforcement was data storage. Analyzing the Documentation was very long task for the officers so in this situation the FBI launched the first magnet media program in 1984, which was the first digital forensics program. After one year under the guidance of John Austen the metropolitan Police set up the computer crime unit in UK.

At the beginning of 1990, s major change tool place because investigators realized that digital forensics need standard techniques, protocols and procedures. So, in 1994 and 1995 the serious fraud office and Inland arrange a series of conferences which is place at police staff college Bramshill, during which the modern British digital methodology was establish.

In 1986, Clifford Stoll, who was a Unix System Administrator at Lawrence Berkeley National laboratory, created the first honeypot trap. In which he planned a for hacker. He gathered 50 computer terminals around his office which was connected with office phone lines.

Iraq and Afghanistan additionally prompted the interest in digital forensics examination. Simultaneously, computerized crime scene investigation assumed a significant part in removing the evidential information from the digital devices assembled by the U.S. troops during the conflict.

B. Process Of Digital Forensic:



Process of digital forensics

1. Identification

Basically, it is first step of digital forensic activity. Identification includes following things What the evidence is, where it is stored and how it is sorted.

2. Preservation

In this second stage date is isolated, secured, and preserved. Investigators does not investigate directly on the original evidence. They make copy of that evidence, stores that copy in other location and then investigate that evidence.

3. Analysis

In this step, investigators reconstruct fragments of data and draw conclusions based on the proof which is found at the device. It might take numerous iterations of examination to support a specific crime theory [4].

4. Documentation

It involves proper documentation of crime scene with sketching, photography and mapping. It help to recreating and reviewing crime scene.

5. Presentation

In this last step process of summarization of conclusions is done. And documents of evidence present in the court.

C. Types Of Digital Forensic:

1. Computer Forensics:

Computer forensics include collection, identification, Preservation and reporting of evidence found on electronic devices like computer, laptops and storage media for investigation and legal proceedings.

2. Network Forensics:

Network forensics include the monitoring, capturing, storing and analysis of activities or events done on public or private network to discover source of security attacks and other problems like virus, worms or malware attacks.

3. Mobile devices Forensics:

In this evidence is recovered from mobile phones, smartphones, SIM cards PDAs, game consoles and tablets.

4. Digital Image Forensics:

In the digital image forensics, the extraction and analysis of digitally received images to validate the authenticity by recovering the metadata of the image file to ascertain its history.

5. Digital Video/Audio Forensics:

In digital video/audio forensics the collection, analysis and evaluation of sound and video recording. In this forensic authenticity of recording is checked if it is in its original form and it has been tampered with either mistakenly or maliciously.

6. Memory forensics:

Memory forensics involves the recovery of evidence from the RAM of laptop or desktop. It is also called and acquisition.

7. Cloud Forensics:

In cloud forensics the investigation done on the crime committed over the cloud and it is an application within in digital forensics.

8. Email Forensics:

Email forensics includes the recovery of deleted emails and contact details. Also, investigate spam mails.

D. Role Of Computers In Digital Forensic:

As a technology develops, crimes and criminal are also increases. To find cybercriminals the term digital forensic is very useful. The digital forensics experts use forensic tools for collecting shreds of evidence against criminals and criminals use such tools for hiding, removing and altering their traces of crime, this process is called anti forensics technique and this is a major challenge in digital forensic world.

When a suspect has been identified and if their personal computer or laptop or cell phone taken as evidence, investigator goes searching for data that is necessary for the investigation. While searching for information they need to be careful to follow procedures of digital forensics. The information that they uncover whether it can be documents, browsing information or even metadata, may then it can be used by prosecution to create case against the suspect. Digital footprint is the information about the person who use the system, like webpages visited by them, their activity status means when they were active and what device they were using. By following the digital footprints, the investigator will retrieve the data to solve the crime case.

Forensic investigators investigate encrypted data using various type of software and tools, also many upcoming techniques that investigators use, depending on the type of cybercrime they are dealing with. Investigators recovers the deleted or hidden files, cracks the passwords, finds the source of security breach. While investigating the data carving process is done which involves the cloning a disk to preserve evidence in its most original form and then the investigation starts. Therefore, the digital forensics software prioritizes data integrity. This can be mined for history of legal activity, encrypted spacing, illegal files, deleted files, track logs.

According to Forbes magazine the number one profession for 2015 was IT, Because IT expertise in law enforcement is not for critical position but one that can change the face of low enforcement with technique.

E. Digital Forensic Tools:

1 .Disk Analysis: Autopsy/Sleuth Kit

Autopsy and Sleuth Kit are the most well-known forensics toolkits in digital forensics. The sleuth kit is command line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI based system that uses the sleuth kit behind the scenes.

2. Image Creation: FTK imager

As autopsy does not have image creation functionality, so another tool need to be used. FTK manager is free software. It can be used to create disk images which can be analyzed using autopsy/sleuth kit.

3. Memory Forensic: Volatility

For analysis of volatile memory, the most well-known and popular tool is volatility. It is open source, free and supports third party plugins. Volatility foundation holds annual contest for users to develop the useful extension to the framework.

4. Mobile Forensic: Cellebrite UFED

A mobile-focused forensic tool might be a useful acquisition as growing importance of mobile forensic. Cellebrite UFED is the best commercial tool for mobile forensics and it supports various platforms and boasts exclusive tools for mobile device analysis.

5.Netwok Analysis: Wireshark

Wireshark is most popular and widely used tool for network traffic analysis. It is free and open source, offers study for many different types of network traffic. Wireshark has easy to use GUI for traffic analysis and include wide range of functionality. It supports live traffic capture files for analysis.

VIII. LIMITATIONS & FUTURE SCOPE

A. High Volume And Speed

Problems related to obtaining, sorting and processing a information for forensics purposes have been causing for at least a decade

B. Explosion of complexity

Evidence is not limited within a single host but it is separated among different physical or virtual locations, like online social networks, cloud resources and personal network. Because of this reason more tools, expertise and time are needed to correctly reconstruct evidence.

C. Development Of Standards

Even if our technology is advance, the files are still use to collect, categorized and analyzed the data. So technological changes are necessary to upgrade or changes the solution.

D. Privacy-preserving Investigations

Nowadays, people bring many aspects of their lives into cyberspace, mainly through social networks and social media sites. Unfortunately, collecting information to reconstruct and locate and attack can violate users' privacy.

E. Legitimacy

Modern Infrastructures are becoming complex and virtualized, often shifting their complexity at the border or delegating some duties to third parties like platform as service frameworks.
Because of increase in data and devices, the digital forensics scope can only expand. And with that expansion drilling into data will be developed. AI will play a key role in this process.

In the field of child sexual exploitation (CSE), AI will be used to prevent investigators from viewing duplicate images of abuse. The benefits of this are two-fold [5].

CONCLUSION

The forensics examination of electronic devices has surely been huge success in the identification of cyber and computer related crime.

Organizations are giving importance on the need to be equipped with appropriate incident management to handle misuser of their systems. And digital forensics is the most important tool in this process.
Computer plays very important role in digital forensics. With help of computer the task of finding criminal become very easy. There are new technology which helps the investigators while investigate any case.

So, throughout the discussion I come to this conclusion that digital forensics Is very important to our society and it has become very easy with the help of computers. So, the role of computers in digital marketing is very important.

REFERENCES

[1]Shriram Raghavan, *Digital Forensics Research: Current state of art*. (Nov 2012)

[2] Review paper on *cyber forensics and its analysis tools.*

[3]https://www.packetlabs.net/posts/digital -forensics

[4]https://www.guru99.com/digital-forensics.html

[5]https://www.cameraforensics.com/blog/2020/02/21/digital-forensics-what-you-need-to-know/index.html

[6]International Journal for research in Applied Science & engineering Technology, Rituparna Das, Mayank Patel *Cyber security for networking sites; issues, challenges, solutions*

[7] Cory Altheide and Hrlen Carvey, *Digital Forensics With Open Source Tools(2011)*