IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, April 2023

Role of Computer in Digital Forensics

Devanshi Mishra[1], Aniket[2], Ashima Mehta[3]
UG Student, Department of Computer Science and Information Technology[1]
UG Student, Department of Computer Science Engineering[2]
Head of department, Department of Computer Science Engineering[3]
Dronacharya College of Engineering, Gurugram, Haryana, India

Abstract: *The report is built around how computers are used in digital forensics. Today, as digitalization spreads quickly, all businesses and people are utilising technology to improve how they conduct business. For that reason, we require a digital system that enables us to complete a variety of jobs more quickly. We also utilise social networking sites for amusement There is nothing wrong with this, but we should exercise caution when using social media and our systems because crime rates are rising as digitalization grows. In order to avoid cyber attacks, software should be installed. When an attack is conducted, we should be aware of the various methods that are available. For instance, in 2020, the use of computers will be too beneficial for the Covid-19 positive forensics test.*

Keywords: Computer, Digital world, Forensic world, cyber-attack, role of computers

I. INTRODUCTION

The study is to examine the importance of the Role of Computers in Digital Forensics Cybercrime on social media is expanding rapidly along with the internet. Therefore, the field of digital forensics has emerged in reaction to those cybercrimes. Essentially, digital forensics is the area of forensic science that focuses on thoroughly examining and recovering any evidence or materials discovered on devices used in cybercrime. Data from your mobile device, desktop computer, laptop, and private network are all included in digital forensics. Computer forensics was the original usage of the term "digital forensics." In order to fully understand what occurred on the digital device, the major goal of digital forensics is to present a methodical examination while organizing a documented chain of proof and evidence. Given the gravity of cybercrime today and the increasing importance of computer security, it is crucial for computer professionals to comprehend the technologies employed in digital forensics. When two objects are related to one other and then moved between them, forensics is predicated on the idea that each criminal leaves a mark behind. This means that a criminal can be connected to a crime by marks evidence brought in from the crime scene. [1-4].

History:

- (1847-1915) Hans Gross, the first person uses the technical study for criminal inquiry purposes.
- Since 1990, what we known as digital forensics was generally termed 'computer forensics'.
- In 1932, the FBI builds a laboratory to provide the facility of forensics to the agents. The main motive of the event is called the International Law Enforcement Conference on Computer Evidence.
- In 1978, the digital offense was first investigated in the Florida Computer Crime Act.
- In 1998, best known for was great work and intelligence is Francis Galton. Galton first managed the recorded study of fingerprints [1].
- In 2010, Simson Garfinkel recognized a topic on facing digital exploration.

II. OBJECTIVE

The main objectives include here are:

- Creating a plan at a potential crime scene that enables you to ensure that the digital evidence obtained is not corrupted.
- It is able to help to retrieve, explores, and maintain computer and acquainted data in such a manner that it favors the inspection agency to represent them as witnessed in a court.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, April 2023

- Retrieving removed files and dispelled documents from digital media to substance the proof and authenticate them.
- This suggests you define the evidence rapidly, and permit you to approximate the potential impression of the malicious action on the victim.
- 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.
- Helps to efficiently tracks down cyber criminals from anywhere in the world

III. PROCESS OF DIGITAL FORENSICS

FIG : PROCESS OF DIGITAL FORENSICS

The digital forensics operation is a recognized factual and forensics action used in digital forensics inspection. Digital Forensics operation has the following five basic steps:

- **Identification:** It is the primary phase in a digital forensic activity. The Identification operation largely comprises things such as what proof is present, where it is amassed, and finally how it is gathered (in which arrangement). It identifies prospective sources of applicable evidence as well as key conservator and position of data. Computerized storage media can be personal Mobile phones, computers, PDAs, etc.
- **Preservation:** In this second stage date is isolated, secured, and preserved [2]. 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. It involves preventing individuals from applying the electronic appliance so that the digital confirmation is not gratified.
- **Analysis:** At the moment, inspection agents restore particles of data and also draw conclusions established on witness found [3]. Although, it might be taking enough repetitions of examination to assist a special crime thesis. A thoroughly systematic search of proof is connecting to the event being explored.
- **Documentation:** In this phase, the History of all the detectable data must be designed. Firstly, documents are based on demonstrating technique and methodology. It supports in regenerating the crime scene and evaluating

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, April 2023

it. It includes proper evidence and documentation of the crime scene along with snapshots and crime-scene retailing.

- **Presentation:** In this last phase, the operation of outline and summarization and clarification of opinions is done. In this last step process of summarization of conclusions is done. Digital Forensics not only means simple activity like collect, process, and presents the data. It is all about the current research and also needs to up-to-date, therefore one forensics needs to be a scientist first then after he can be able to join the digital forensics field.

IV. DIGITAL FORENSIC TYPES

Digital forensics is split into specific sub-branches relating to the inspection of various types of evidence.

1. **Mobile forensics**: It mainly deals with confirmation related to mobile phones and other mobile devices. Most superiorly now a day's mobile phones are the most usual digital evidence found at crime scenes and phones are the most convenient source of evidence. It supports to restore important information like call logs, SIM contacts, incoming, and MMS/SMS, images, videos, audio, chats, documents, and network information. In this evidence is recovered from mobile phones, smartphones, SIM cards PDAs, game consoles and tablets.
2. **Computer Forensics:** It is known as the sub-branch of digital forensics. It mainly operates cases linked to data stored in the computer devices. The goal of computer forensics conflict is to find out and describe the present condition of digital evidence stored into devices like laptops, computers, storage devices, and other electronic devices
3. **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. This network traffic can be LAN or WAN.
4. **Database Forensics:** It is also a sub-branch that is connecting the review and inspection of the database and the review and inspection of the database and their metadata. This also handles cars linked to the database.
5. **Digital Image Forensics:** In digital image forensics, images that have been received digitally are extracted and analysed in order to verify their authenticity by retrieving the image file's metadata and learning more about its past.
6. **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.
7. **Live Forensics:** Most probably it contends with the examination and survey of cases related to a live scenario. It helps to maintain the confirmation of having any changes.
8. **Email Forensics:** It deals with the retrieval of emails, as well as deleted emails and contact details. Also, investigate spam mails.

V. IMPORTANCE OF FORENSIC KNOWLEDGE

orensics is so much important for justifying anyone. It plays a significant role in law & justice. It helps to provide proper justice to the victim and also supports to catch and punish criminals or culprits. The knowledge of forensics investigation process, techniques and methods provide advantages to an investigator that entire evidence is correctly gathered and gives to maintain authentication, integrity when legal and technical forensics investigation procedure ignored correctly then following problems arise:

- Demolish the proof of the justice system.
- Proof not being acceptable in court due to authenticity and integrity issues.
- Important and useful evidence being destroyed or compromised.

VI. COMPUTER ROLE IN DIGITAL FORENSICS

The need for assistance in recovering data that can be used as a proof is growing as the difficulty of enforcing the law increases, thus the field of PC criminology will only become more in demand. More than ever, this expanding field of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, April 2023

study needs IT specialists skilled in this type of information recovery for law implementation. As technology advances, criminal activity likewise rises. 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 procedure, known as anti-forensics approach, is a significant difficulty in the field of digital forensics. 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 material they find, including surfing history, documents, and even metadata, may subsequently be used by the prosecution to build a case against the defendant. 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. The investigator will gather the information needed to solve the crime case by tracing the digital footprints. 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 locate the source of security breach, retrieve deleted or hidden material, decipher passwords, etc. Investigation begins once the data carving procedure, which entails cloning a disc, is completed to preserve evidence in its original form. 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.

VII . COMPUTER FORENSICS TOOL

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 needs to be used. FTK manager is free software. It can be used to create disk images which can be analysed 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

As mobile forensics become more important, acquiring a mobile-specific forensic tool can be beneficial. The finest commercial tool for mobile forensics is Cellebrite UFED, which works with many different platforms and has unique tools for analysing mobile devices.

5. Netwok Analysis: Wireshark

The most well-known and often used tool for network traffic analysis is Wireshark. 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. For analysis, it supports live traffic capture files.

VIII. DIGITAL FORENSIC CHALLENGES

There are lots of ultimatums that are faced by Digital Forensics. These are following as-

- **High volume and speed**: Problems related to storing, acquiring, and processing a lot of information for forensics intentions have been bringing about issues many times, and also are promoted by availability and extensive marketing of digital information.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, April 2023

- **Explosion of complexity**: Evidence is out of control for a single host. This is dispersed among a number of virtual or actual locations, including cloud resources, social networks, and storage units associated with personal networks. Due of this, it takes more knowledge, time, and resources to correctly and totally rebuild the evidence. Some difficult tasks also performed very fast using the techniques of computer forensics tools [3-8].
- **Arise of anti-forensics techniques**: Cautious measures incorporate encryption, jumbling, and shrouding methods, including data stowing away. Collaboration among universal purviews, in any case, researching cybercrime and gathering proof is fundamental in building hermetically sealed cases for law requirement. Security experts require the best research tools for that.
- **Legitimacy**: Present-day foundations are getting mind-boggling and virtualized, regularly moving their multifaceted nature at the outskirt, (for example, in haze figuring) or designating a few obligations to outsiders, (for example, in stage as-an administration systems).
- **Privacy investigations**: Nowadays, people spend a lot of time online and frequently interact with online communities or online life destinations to share their experiences and memories. When computing is added, it aids in the discovery and collection of all data necessary to create attacks that violate client security and is associated with a number of issues [6].
- **Improvement of standards**:Even if our technology is advance, the files are still use to collect, categorized and analysed the data. So technological changes are necessary to upgrade or changes the solution. The examinations of front-line cybercrimes may require handling data in a cooperative way or utilizing redistributed capacity and calculation. Accordingly, a centre advance for the computerized criminology network will be the improvement of appropriate standard arrangements and deliberations.

IX. ADVANTAGES OF DIGITAL FORENSIC

Here, are pros/benefits of Digital forensics

- To create evidence in court that can result in the offender being punished
- To protect the integrity of the computer system
- In the event that their computer systems or networks are compromised, aids the businesses in obtaining crucial information.
- Effectively locates cybercriminals from any location in the world.
- Assists in safeguarding the organization's money and priceless time.
- Enables the extraction, processing, and interpretation of factual material, allowing for the legal demonstration of cybercriminal behaviour.

X. DISADVANTAGES OF DIGITAL FORENSICS

The following are the main cons and drawbacks of using digital forensics.

- Digital evidence accepted into court. But it must be demonstrated that there has been no tampering.
- Electronic record production and storage is a very expensive endeavour.
- Legal professionals need to have substantial computer knowledge and must generate legitimate, persuading evidence. If the digital forensic instrument employed does not meet the required standards, the evidence may be rejected by the justice system in a court of law
- The investigating officer's lack of technical understanding can prevent the desired outcome

XI. CONCLUSION

The discussion leads us to the conclusion that digital forensics is crucial to our culture and has gotten much simpler thanks to computers alone. 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 misuse of their systems. With help of computer the task of finding criminal become very easy. There is new technology which helps the investigators while investigate any case.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, April 2023

REFERENCES

[1]. M.Reith , C.Carr and G. Gunsch, An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12. (2016).

[2]. S.C.Gupta, (2017). Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(1), 118-131

[3]. B.Carrier and E. Spafford, An event-based digital forensic investigation framework. Digital Investigation. (2015).

[4]. B.Martini, An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71-80. (2016).

[5]. B.Carrier, Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence, 1(4), 1-12. (2016).

[6]. M D.Kohn, M.M.Eloff and J. H. Eloff, Integrated digital forensic process model. Computers & Security, 38, 103- 115. (2016).