ISSN 2347 - 3983
Volume 12. No.2, February 2024
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter011222024.pdf
https://doi.org/10.30534/ijeter/2024/011222024

Cyber Sleuths: The Transformative Role of Computers in Forensic Analysis

Raksha[1], Ramyashree[2], Ranjith R Ganiga[3], S Vishwesh Nayak[4]
[1] Department of Computer Science and Engineering, AIET, India, rakshaacharya1102@gmail.com
[2] Department of Computer Science and Engineering, AIET, India, ramyasuvarna522@gmail.com
[3] Department of Computer Science and Engineering, AIET, India, ranjithganiga2119@gmail.com
[4] Department of Computer Science and Engineering, AIET, India, vishweshnayak43@gmail.com

Received Date: December 25, 2023 Accepted Date: January 24, 2024 Published Date : February 07, 2024

ABSTRACT

This document highlights the importance of computers in the field of digital forensics. As the world progresses towards digitalization, various industries are increasingly recognizing the advantages of incorporating digital processes into their operations. Digitalization facilitates efficient and rapid workflows, and it can be achieved through the use of computers or systems. To perform digital forensic tasks, the installation of specific forensic software tools on a computer is essential. This enables faster and more streamlined procedures. For instance, computers played a significant role in expediting COVID-19 testing through positive forensic tests in 2020. The utilization of computers greatly simplifies the testing process.

Key words: Computer science, Digital world, Forensic world, Authenticate evidence, Bankruptcy, Security, Investigation.

1. INTRODUCTION

Digital forensics has emerged as the prevailing method of presenting medical information in court. The fundamental objective of virtual forensics is to meticulously document and decipher chains of evidence, ensuring a well-informed investigation[1]. The evolution of virtual devices has been a remarkable advancement for successive generations. It is imperative to continually update digital forensics systems. Forensic intelligence is founded on the principle that every perpetrator leaves behind a trace[2]. Moreover, items are intricately interconnected and communication between them leaves behind a trail, enabling the connection of fraudsters to criminal activities through evidence obtained from the crime scene. [3].

2. HISTORY

Hans Gross, a prominent figure in criminal investigation, revolutionized the field by utilizing the technical eye in the late 19th century[1]. This groundbreaking approach paved the way for future advancements in forensic science. Fast forward to 1932, when the FBI established a dedicated laboratory to enhance their agents' forensic capabilities. This move was prompted by the International Law Enforcement Conference on Computer Evidence, highlighting the growing importance of technology in criminal investigations. A significant milestone occurred in 1978 with the enactment of the Florida Computer Crime Act, marking the first formal investigation of virtual offenses. Francis Galton's groundbreaking study on fingerprints in 1998 further elevated the field of fingerprint analysis[1]. Finally, in 2010,[2] Simson Garfinkel explored the intricacies of virtual exploration, adding another dimension to the evolving landscape of forensic science.

3. OBJECTIVE

The major targets encompass right here are:

A. Develop crime scene reports in a manner that ensures the integrity and tamper-proof nature of virtualevidence received.
B. Aid in identifying commonalities between targeted individuals and the main perpetrators involved in criminal activities.
C. Provide assistance in locating, recovering, and securely storing laptops and personal records, enablinginspection firms to present you as credible witnesses incourt proceedings.
D. Retrieve deleted documents and files from virtual media to validate and authenticate evidence in support of investigations.
E. This shows you outline the proof rapidly, and can help you approximate the capability effect of the malicious motion at the victim.
F. Generating a laptop forensic element thatoffers entire info at the exploration process.
G. To preserve the proof following collection of custody is needed.
H. All the steps are followed during digital forensic are show in below figure 1.

Figure 1: Digital Forensic Cycle

4. PROCESS OF DIGITAL FORENSICS

Digital forensic operations have become widely recognized and adopted as standard practice for conducting investigations in the digital realm. The Figure 2 shows process of digital forensic. These operations encompass a comprehensive set of procedures designed for digital forensic examination[2]. The process of digital forensics typically encompassesfive fundamental steps, which include:

4.1 Identification:

The Identification operation holds paramount importance in virtual forensic activities. This stage primarily deals with identifying the available evidence, its collection location, and the methods employed during the collection process. It involves identifying potential sources of pertinent evidence and determining the custodian and integrity of the data. Computerized storage media such as personal mobile phones, computers,[4] PDAs, and similar devices are commonly encountered in this context. In this below figure 2 show the process of digital forensics.

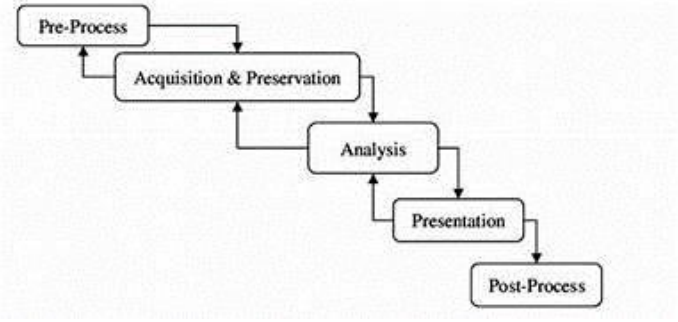

Figure 2: Process of digital forensic

4.2 Preservation:

It is a function that automatically saves the data that c an be used. Currently, information is classified or clas sified [2]. It includes supporting people through the u se of digital devices by making virtual authentication unnecessary.

4.3 Analysis:

Now, the auditors correct the rest of the documents and draw conclusions based on eyewitnesses [3]. However, there should be sufficient checks to help complete a particular criminal record. Research evidence correlates very well with the research period.

4.4 Documentation:

During this phase, a comprehensive record of statistical data is generated. The information is derived from various methodologies and presentation techniques. Its purpose is to enhance crime analysis and enable effective comparisons. This record includes vital evidence and information pertaining to the crime scene, accompanied by photographs and a repository of crime scene details.

4.5 Presentation:

In this final stage, the work of explaining, summarizing and clarifying the message takes place. Digital forensics refers to more than simple tasks such as data collection, processing and disclosure. This is an ongoing science andneeds updating, so a forensic scientist must be a scientist before entering the digital forensics field.

5. DIGITAL FORENSIC TYPES

Digital forensics is break up into particular sub-branches regarding the inspection of diverse sorts of evidence. Figure 3 shows types of digital forensic.

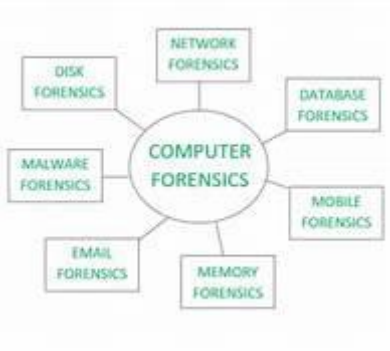

Figure 3: Types of Digital forensic

A. Mobile Forensics:

This stage primarily deals with the examination and analysis of cell phones and other mobile devices. In contemporary times, mobile phones have become the most common form of digital evidence found at crime scenes, as they serve as a convenient and abundant source of information. The process involves retrieving and extracting vital data, including call logs, SIM contacts, incoming and outgoing messages (MMS/SMS), multimedia files,chat records, documents, and network- related information[4].

B. Computer Forensics:

It is called the sub-department of virtual forensics. It in particular operates instances connected to statistics saved withinside the laptop gadgets[3].
The intention of laptop forensics battle is to discover and describe the existing circumstance of virtual proof saved into gadgets like laptops, computers, garage gadgets, and different digital gadgets.

C. Network Forensics:

It in particular offers with instances interconnected to pc community policy[2]. This community site visitors may be LAN or WAN.

D. Database Forensics:

This sub-department serves as a bridge between database evaluation, inspection, and metadata assessment. It is responsible for managing database-related tasks, including the handling of associated vehicles.

E. Live Forensics:

It is common to encounter situations where a review and case study are conducted based on real-life scenarios. Such studies are essential for preserving evidence and confirming any modifications or changes that may have occurred.

F. Email Forensics:

This specific department is tasked with the retrieval ofemails, including those that have been deleted, as well as extracting contact information related to these emails.

G. Examples of uses:

In digital research business associations insuch cases,

- Compliance issues.
- Fraud investigations
- Bankruptcy investigations
- Internet and email inefficiencies
- Fraud investigations
- Industry solutions
- Controversial solutions.

6. SIGNIFICANCE OF FORENSICKNOWLEDGE

Forensic science holds significant importance in ensuring justice for individuals. It plays a crucial role in the realm of law and justice, aiding in the pursuit oftruth and enabling the capture and punishment of criminals or wrongdoers. Familiarity with forensic investigation procedures, techniques, and methods provides investigators with the advantage of gatheringand presenting evidence in a manner that upholds authenticity, integrity, and credibility[5]. Without adhering to appropriate legal and technical investigative procedures, various issues can arise, leading to potential complications.

- Tear off evidence from the judicial system.
- Evidence not admissible in court due to issues of authenticity and integrity.
- The destruction or compromise of crucial and valuable evidence can have a significant impact.

7. SIGNIFICANCE OF COMPUTERSN IN DIGITAL FORENSICS

Forensic computer work will increase as the need to help recover data that can be used as evidence becomes increasingly difficult for law enforcement. According to Forbes magazine, in 2015 it was IT professionals and that wasthe only IT score category that was established. This position even changes the nature of modal and dominion legal authorization to unravel the examples and cause irreparable consequences.

8. COMPUTER FORENSICS TOOL

Computer forensics relies on the utilization of diverse software tools, administered by skilled investigators. These experts are responsible for executing operations such as identifying encrypted files, employing industry- leading techniques. Common tasks encompass routine activities like file recovery, deletion, and password retrieval from raw data. While the primary function of computer forensics is data recovery, its significance lies in enabling investigators to process and analyze this information, providing solutions to resolve cases and reach informed judgments.

9. DIGITAL FORENSICS CHALLENGES

Digital Forensics faces many ultimatums. Figure 4 shows challenges of digital forensics

A. High Volume and Speed:

The challenges posed by the storage, collection, and processing of vast amounts of information in forensic contexts have persistently emerged, further compounded by the widespread availability and commercialization of digital data.

B. Explosion of Complexity:

The evidence pertaining to a single server can be scattered across various virtual or physical locations, including cloud resources, social networks, and storage units linked to private networks[3].Consequently, assembling the evidence accuratelyand comprehensively requires additional expertise, time, and specialized tools. Certain complex tasks are expedited through the utilization of computer forensic tools. The utilization of these tools streamlines the process and aids in swiftly performing intricate tasks associated with evidence extraction and analysis [3-8].

C. The Emergence of Forensic Techniques:

Precautions include methods of encryption, obfuscation, and obfuscation, including data archiving. In any case, a collaboration between generalization skills, cybercrime research, and evidence gathering is fundamental to building discreet cases that meet the requirements of the law[7]. So security professionals need the best tools to find.

D. Legitimacy:

In the modern era, organizations and institutions have become increasingly complex and virtualized. They often extend their intricate operations to the edge, utilizing technologies like cloud computing, or entrust certain responsibilities to external entities, such as in the case of infrastructure-as-a-service (IaaS) or software-as-a-service (SaaS) models[8].

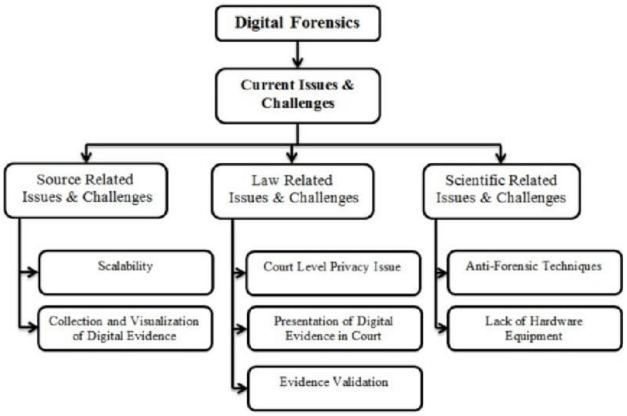

Figure 4: Challenges of Digital Forensics

E. Privacy Investigations:

These days, humans are spending plenty of time with the net and percentage numerous recollections of lifestyles, basically via online casual agencies or web-primarily based totally lifestyles destinations[6]. It allows to locate and collect all statistics to make an assault that maltreats a client's safety additionally it is connected with numerous issues whilst computing is appended [6].

F. Improvements of Standards:

The examinations of the front-line cybercrimes may also require coping with statistics in a cooperative manner or using redistributed ability and calculation. Accordingly, a middle development for the automated criminology community could be the development of suitable trendy preparations and deliberations[8].

10. ADVANTAGES OF DIGITAL FORENSICS

We are now discussing the benefits of digital forensics. Here is the

- If the company's computer system or network is suitable, it can help the company present important information.
- A company cyber criminals are punished in court by giving evidenceagainst them.
- Cybersecurity develops precautions against theft or destruction of computer software, hardware, and information related to them.
- Identify and extract convincing risk criteria from the dataset for further analysis.
- The ability to reduce or eliminate sampling problems is an important benefit of criminal records.

11. DISADVANTAGES OF DIGITALFORENSICS

- Most investigators do not have appropriate technical knowhow in the field of investigation.
- One result, they can no longer be able to publish the desired end result of all cases.
- Request to persuade and authenticate evidence. Practice will go to prison Creating virtual files and defensive statistics is too expensive .Digital evidence receives in court.

12. CONCLUSION

After careful consideration and analysis, we have reached the consensus that digital forensics holds immense significance in our society. The evidence in question extends beyond the confines of a single server and is distributed across various physical and virtual locations, including cloud resources, social networks, and storage units linked to private networks. This highlights the importance and utility of digital forensics in accessing and analyzing evidence from these diverse sources[9].Digital forensics has come a long way in the past few decades, evolving to meet the challenges posed by technological advancements and the increasing rate of cybercrimes. The development of models and frameworks has provided a structured approach to digital forensic investigations, ensuring the integrity and admissibility of digital evidence in legal proceedings.

However, the field of digital forensics continues to face challenges in keeping up with the rapidly changing technology
landscape. The need for standardization, scientific research, and collaboration between different stakeholders is crucial for advancing the field and ensuring the reliability and effectiveness of digital evidence in solving crimes. As the digital landscape continues to evolve, digital forensic experts must stay informed and adapt their methodologies and techniques to address emerging challenges[9]. By doing so, they can continue to uncover valuable digital evidence that plays a critical role in modern-day criminal investigations.

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, Integrateddigital forensic process model.*Computers & Security*, *38*, 103- 115. (2016).

[7] SM.Mohammad Security and Privacy Concerns of the 'Internet of Things' (IoT) in IT and its Help in the Various Sectors across the World International Journal of Computer Trends and Technology (IJCTT) – Volume 68 Issue 4 –April 2020. Available at SSRN: https://ssrn.com/abstract=3630513(April 4,2020).

[8] F. B. Cohen, *Digital forensic evidence examination*. Livermore: Fred Cohen &Associates. (2016).

[9] S. R.Selamat, R.Yusof and S.Sahib, Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, *8*(10), 163-169.(2008).