IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DIGITAL FORENSICS' ROLE IN CYBER CRIME

[1] R.SURESH , [2] Dr. A.DEVENDRAN, [3] Dr.V.N.RAJAVARMAN

[1]Research scholar, [2]Research Supervisor, [3]Co- Supervisor

[1,2,3] Department of Computer Science

[1]Dr. M.G.R Educational and Research Institute, Chennai, India.

Abstract: In the digital era, people of different ages i.e. from children to elders are using smart phones, laptops, tablets, and other cyber gadgets for their day-to-day activities. Though it simplifies and makes our lifestyle easier, it also leads mankind to many problems. This is because, if some people use these gadgets for their own good purpose, others use them for their own selfish motive and in fact misuse these gadgets thereby becoming cybercriminals. These cybercriminals can be classified as Hackers, Phishers, and Ransom Artists; who are involved in digital crime and create many problems for the public. These problems are rectified by the digital forensics department. Forensic science includes a branch called digital forensics. It collects and explores evidence from digital devices. This paper focuses on the introduction about "Digital Forensics and Digital Crimes".

***Index Terms* - Digital forensics -cyber forensics - forensic science - network forensic- computer forensics**

I. INTRODUCTION

Cell phones, tablets, game consoles, laptops, and desktop computers are just a few examples of the digital devices that have become indispensable in today's culture. As these gadgets become more prevalent in our daily lives, there is a danger that information obtained from them could be used for illegal purposes. Thus, the digital forensics department established by the government finds cybercriminals and protects the digital device users without occur any loss.

Here, Forensics is the method for gathering, analyzing, and presenting evidence to the court using scientific understanding. [1]. Digital forensics is the application of forensic technology that makes use of systematic information to accumulate, analyze, file, and present digital evidence associated with computer crime in a criminal court docket. The vital goal of knowing what was done when it was done, and who did it. [2]. The term "cybercrime" (sometimes known as "digital crime") refers to the use of computers and networks for criminal purposes, such as the dissemination of computer viruses, cyberbullying, and improper fund transfers.

II. OBJECTIVES OF DIGITAL FORENSICS

The goal of digital forensics is to find and recover legal evidence, discover data leaks within an organisation, access potential damage from a data breach, present the evidence in court, and lastly, provide a framework for expert testimony in court [2]. To facilitate or hasten the reconstruction of criminal events, digital evidence is derived from digital sources [5].

III. DIGITAL FORENSICS CHARACTERISTICS

Digital forensics is typically used to describe the identification and prevention of cybercrime. Given that they both focus on digital events, they are both relevant to digital security. Because it emphasises preventative measures, digital forensics is more responsive than digital security. [3]. Computer forensics, email forensics, storage forensics, network forensics, and mobile forensics are the five subfields of digital forensics. In the relentless area, file sharing through network settings is the focus of illegal activity. Mobile forensics, a brand-new industry subset of digital forensics, is focused on protecting evidence from mobile devices. [4].

IV. DIGITAL CRIME

Cybercrime is another term for the digital crime. Cybercrime is any crook interest that entails a laptop, networked tool, or community. While most cybercrimes are executed with a view to generating profit for the cybercriminals, a few cybercrimes are done towards computer systems or gadgets without delay to harm or disable them. Others use computers or networks to unfold malware, unlawful information, pix, or other substances. Some cybercrimes do both i.e., goal computers to infect them with a computer virus, which is then unfolded to different machines and on occasion, complete networks. A number one impact of cybercrime is economic. Cybercrime can include many distinct styles of profit-pushed criminal hobby, inclusive of ransom ware assaults, e-mail, and net fraud, and identity fraud, as well as attempts to souse, borrow economic accounts, credit playing cards, or other price cards facts. Cybercriminals may additionally target a man or woman's non-public statistics or corporate information for theft and resale [6]. Phishing, Harassment, Ransomware, online Prostitution, Child Pornography & Solicitation, Account Hacking, etc., are some examples of cybercrime.

V. THE DIGITAL FORENSICS PROCESS IN DIGITAL CRIME

In the area of digital crime, digital forensics will be crucial in identifying offenders. Detection, Protection, Investigation, Documentation, and Presentation are all steps involved in digital forensics. This is seen in fig. 1.

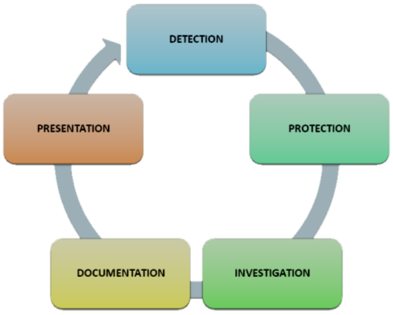

Fig -1 Process of Digital Forensics.

5.1 DETECTION

In the forensic procedure, it is the initial stage. The identification method specifically takes into account information like what evidence is delivered, where it is finally preserved, and how it is saved and in which format. Desktop computers, smart phones, and other digital devices are examples of digital media. [7]

5.2 PROTECTION

This section focuses on protecting data from unauthorized access, securing it, and preserving it [8]. It also addresses how to prevent people from using digital devices altogether.

5.3 INVESTIGATION

In this stage, investigators piece together bits of data and make inferences based mostly on the evidence gathered. However, it could take numerous rounds of analysis to support a particular crime theory [16].

5.4 DOCUMENTATION

In this approach, a document holds all the information that is currently displayed is desired. It enables evaluating and rebuilding the scene of a crime. It entails accurate crime scene documenting, including tracing the site, drafting, and photography.

5.5 PRESENTATION

This final step involves the process of summarizing and clarifying conclusions. However, it needs to be stated in everyday language without using technical terms. The specific information should be cited in all abstracted terminology.

VI. TOOLS USED FOR DIGITAL FORENSIC INVESTIGATIONS

There is a variety of tools employed for virtual forensics in crimes involving our internet environment due to the different of computer crimes. The most often utilized equipment for this cause is briefly discussed in the following subsections. [10].

6.1 MEMGATOR

MemGater is a memory document evaluation device that automates the extraction of information from a reminiscence report and compiles a file for the investigator. MemGator brings collectively some of the equipment together with the Volatility Framework, Scalpel File Carver, and AESKeyFinder into the most effective application.

6.2 GALLETA

It is a forensics tool that examines the cookie files created by Microsoft Internet Explorer (MSIE). It separates the report's subjects so that they can be loaded into a spreadsheet.

6.3 ETHREAL

The open-source software tool Ethreal is widely used in the community as a packet analyzer. Live network packets are captured by it. It displays the information contained in the headers of every protocol used during the transmission of the packets that were captured. According to user preferences, it filters the packets [9].

6.4 PASCO

A command-line tool that investigators can use to study Internet Explorer facts saved in an index.dat report. Pasco parses the record and outputs the consequences to an area-delimited document. An investigator can then load this record into spreadsheet software to view the information.

6.5 RIFIUTI

This device is a Recycle Bin Forensic Analysis Tool and it recovers any currently deleted documents. Rifiuti is an open supply released beneath the liberal Free BSD license.

6.6 NMAP

A free and open-source network scanner is Nmap (Network Mapper). Nmap sends packets and then analyses the answers to find hosts and services on a computer network. A few functions are provided by Map for investigating laptop networks, including host finding, issuer detection, and functional device detection [12].

VII. DIFFICULTIES WITH DIGITAL FORENSIC INVESTIGATIONS IN CYBERCRIME

One of the goals of this essay is to offer open-ended research questions for the reader's benefit, so enhancing research in this fascinating area. A number of concerns have started to be looked into and examined in the following subsections.

7.1 INCONSISTENCY IN DATA VIEW

It is frequently discovered that the content visualised in cyberspace does not always correlate to the identical preserved copy on the disc, which can cause forensic analysis to produce confusing or even incorrect conclusions. This opens up a window for research into how we will approach the issue and what techniques, resources, innovations, etc., could be used to decrease its consequences [10].

7.2 DESIGN ORIENTED BY EVIDENCE

The forensics technologies of today were initially developed to look into digital evidence unrelated to cases. In other words, the tested proof helps with the inquiry process but doesn't address any problems with our online environment. In addition, the vast bulk of this technology exclusively handles offences done against computers, not, say, a person [13].

7.3 TECHNOLOGY GAP

Sadly, the generational divide between cybercriminals and the prevention tools and software kits is skewed heavily in their favour. This demonstrates the value of investigating security software programme tactics and equipment to close this gap, which is unavoidable [14].

7.4 TECHNICAL CHALLENGES

The two demanding situations faced in a virtual forensic investigation are complexity and amount. The complexity hassle refers to the statistics accumulated being at the lowest stage or in raw format. Non-technical human beings will find it tough to understand such information.

7.5 LEGALDEMANDING SITUATIONS

Digital evidence can be tampered with effortlessly, now and again, even with no lines. It is common for modern computer systems to have more than one gigabyte-sized disk. Burning a CD-ROM is no longer sufficient to capture and freeze digital evidence. Since the proof was not frozen before beginning documents, important evidence has been ruled invalid.

VIII. CONCLUSION

In this paper, I am try to speak about the function of digital forensics in preventing cybercrimes become furnished. Throughout the paper, numerous essential elements, functions, and technologies were offered and uttered. It is observed that there may be a big hole between the currently available digital forensics equipment and the premier utility of the digital forensics concept. This commentary was investigated within the sections of this paper. Based on that, some important concerns have been highlighted to provide areas for cutting-edge research aiming to decorate digital forensics implementation and research manner, especially for cybercrimes. Although the contemporary hole among the found out era and virtual forensic equipment is massive, it still may be lessened with the aid of supporting the research on this course.

IX. REFERENCES

[1] Sammons, John. *The basics of digital forensics: the primer for getting started in digital forensics*. Elsevier, 2012.

[2] Hassan, Nihad A. "Introduction: Understanding digital forensics." *Digital Forensics Basics*. Apress, Berkeley, CA, 2019. 1-33.

[3] Sadiku, Matthew NO, Mahamadou Tembely, and Sarhan M. Musa."Digital Forensics." *International Journal of Advanced Research in Computer Science and Software Engineering* 7.4 (2017).

[4] Kumari, Noble, and A. K. Mohapatra. "An insight into digital forensics branches and tools." *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*. IEEE, 2016.

[5] Casey, Eoghan, and Aaron Stanley. "Tool review–remote forensic preservation and examination tools." *Digital investigation* 1.4 (2004): 284-297.

[6] https://www.techtarget.com/searchsecurity/definition/cybercrim

[7] Daniel, Larry. *Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom*. Elsevier, 2011.

[8] Centre for Strategic and International Studies.Net Losses: Estimating the Global Cost of Cybercrime. Mission College Boulevard Santa Clara CA, 2014.

[9] Meghanathan, Natarajan, Sumanth Reddy Allam, and Loretta A. Moore. "Tools and techniques for network forensics." *arXiv preprint arXiv:1004.0570* (2010).

[10] Harbawi, Malek, and AsafVarol. "The role of digital forensics in combating Cybercrimes." *2016 4th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, 2016.

[11] Childs, Dave, and Paul Stephens. "An analysis of the accuracy and usefulness of Vinetto, Pasco and Mork. pl." *International Journal of Electronic Security and Digital Forensics* 2.2 (2009): 182-198.

[12] https://en.wikipedia.org/wiki/Nmap

[13] Garfinkel, Simson L. "Digital forensics research: The next 10 years." *digital investigation* 7 (2010): S64-S73.

[14] M. Rogers. Digital Forensics and Cyber Crime. Springer: ICST Institute for Computer Science, Lafayette, USA, pp. 144-220,2012.

[15] https://www.educba.com/what-is-digital-forensics/

[16] https://www.guru99.com/