Swanirman Sunirmit Publications of Research Volume 4, Issue 1-March 2024 | [2024-25]
ISSN [Online]: 2583-2654

A Cyber Security Evaluation of Digital Forensics

(Editorial article)

Prof (Dr) D David Neels Ponkumar
Professor/ECE,Vel Tech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi, Chennai.

Abstract: Computer forensics, another name for digital forensics, is a broad discipline that includes individuals of many backgrounds. Network forensics, database forensics, mobile forensics, cloud forensics, memory forensics, and data/disk forensics are just a few of the forensic disciplines that fall under the umbrella of digital forensics. The exponential increase in cyber risks and assaults, as seen by recent data and analytics, calls for the necessity for forensic professionals and researchers to automate processes in the cyber world. The area of digital forensics has challenges because of the fast rise in data volume since it is closely linked to recovering information and data carving. Furthermore, the daily rise in malware causes the forensic sector to deteriorate. This document offers researchers and users an overview of forensics and its many fields, anti-forensic methods, and an assessment of the field's present state.

Keywords: Computer Forensics, Digital Forensics, Network Forensics, Database Forensics, Mobile Forensics, Cloud Forensics, Memory Forensics, And Data/Disk Forensics

I. INTRODUCTION

"Digital forensics" [1], often referred to as "digital forensic science" [2], is a subset of forensic science that focuses on the identification, search, seizure, preservation, and cycle of criminal investigation using digital data. Although this industry dates back to the early 1980s, wide area networks and multi-user, multitasking operating systems gave rise to a revolution in the mid-1990s. In the beginning, forensics was only used to look into unauthorized access to data, but it gradually grew to include financial fraud, child pornography, malware and virus production, cyberattacks, and other crimes. With the rise in cyberattacks and threats, one of the most significant areas in the security sector is digital forensics. A recent KPMG cybercrime research [3] states that in 2016, 72% of Indian firms were the target of cyberattacks, resulting in 63% of financial losses and 55% of sensitive data being taken, which damaged 49% of their reputation. In 2009, there were 2.3 million malware; by 2016, there were 430 million, or 1.1 million new malware created per day, according to a Symantec Corp. study [4]. The issues listed above only make up one facet of digital forensics; the other is data recovery, or finding lost data. Data may be found on hard drives, mobile phones, databases, GPS units, IOT, and high-tech electrical gadgets [5]. Data can be found in both raw and multimedia forms. The task of forensic investigators has become more difficult as data shredding and destruction methods have developed alongside secure data storage and retrieval technologies. This essay's main objectives are to educate readers about cyber threats, cyberattack targets, the results of these attacks, anti-forensic techniques, and, lastly, user-focused defense strategies against cyberattacks.

As the Internet becomes more and more integrated into daily life, we are getting closer to making use of both new and current online possibilities. Cyber forensics is a distinct field that offers opportunities for detecting, storing, evaluating, and presenting digital evidence in a way that is compliant with the law. "Relating to the use of science or technology in the investigation and establishment of facts or evidence in

ISSN [Online]: 2583-2654

a court of law," is how the American Heritage Dictionary defines forensics.

In cyber forensics, computer media must be identified, recorded, and interpreted to be used as evidence or to reconstruct the crime scene. The process of locating, gathering, safeguarding, evaluating, and presenting computer-related evidence in a way that a court will find acceptable is known as computer forensics [6]. Computer forensics has expanded into some related fields more recently, giving birth to some terms6 including cyber forensics, email forensics, digital forensics, data forensics, system forensics, network forensics, forensics analysis, corporate forensics, proactive forensics, etc.

Cyber forensics is the study of how and what went wrong. System forensics is carried out on separate computers. To identify the origins of security breaches, network forensics collects and analyzes network events. Website forensics is another name for the same procedure used on the internet. The major in data forensics focuses on both volatile and nonvolatile data analysis. In proactive forensics, prospective evidence is actively and consistently gathered continuously. It is a kind of continuing forensics. When conducting a forensic investigation, one or more emails are the subject of email forensics shown in Fig 1.

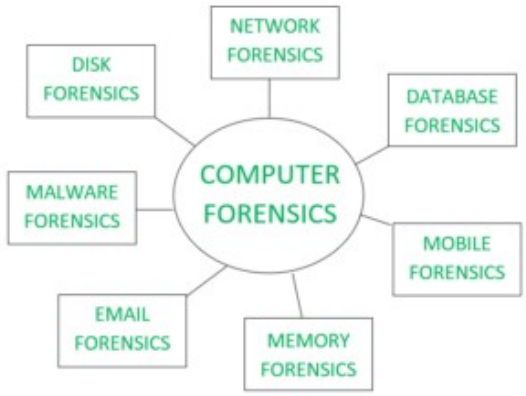

Fig 1: Architecture for cyber forensics

1.1 Background

As opposed to being a mere compilation of several forensic disciplines, digital forensics encompasses a wide range of subjects and approaches. When it comes to storing and retrieving data, methods like data mining, AI, deep learning, algorithms, and architectural frameworks are used. Knowledge of hardware architectures, kernel-level debugging, and mobile forensics which include, among other things, Android programming are all part of memory forensics [7]. Members come from all walks of life and work in fields as diverse as those just described, including forensic science, police enforcement, assault, victim, and corporation court. The multi-faceted intricacy of digital forensics stems from the fact that it crosses over into many other domains, technologies, and occupations.

II. IMPACT OF DIGITAL FORENSICS

Data forensics, cloud forensics, memory forensics, and android/mobile forensics are all subfields that make up the digital forensics domain. While digital forensics has been around for 30 years, cloud forensics [8] as well as mobile forensics [9] was just introduced a decade ago.

2.1 Forensics of the Cloud

Between 2005 and 2009, the phrase "cloud forensics" was coined. In the beginning, the study scope was very limited since there were only a few cloud suppliers accessible.
As time went on in the mid-13s, studies in this area skyrocketed, but there were still many unanswered concerns. Forensic as a service is still missing from this area of study, which causes problems in the forensic sector [10]. Second, cloud servers are not readily accessible to forensic professionals (Fig. 2).

ISSN [Online]: 2583-2654

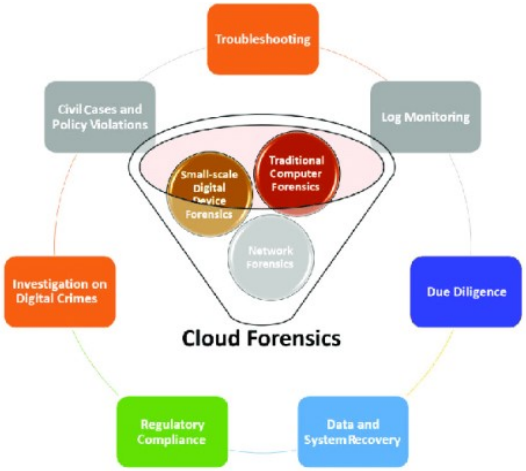

Fig 2: Forensics of the Cloud

2.2 Forensics for Mobile Devices

Mobile forensics began in 2000 with the introduction of new Motorola phones that operated on Java mobile versions. With the advancement of Android and Windows OSes, the number of mobile phones in use has significantly risen in recent times. Android phones function as little computers, allowing users to do significant tasks directly on the device. Mobile forensics is crucial in the forensic field compared to other areas. Over the last two years, several android forensic tools have been created, and commercial tools have also been made accessible (Fig. 3). However, a significant limitation of this sector is the challenge forensic investigators have in separating the internal storage of the mobile device from the operating system.

The graph's decline is due to the rapid development of new mobiles with diverse architectures and operating systems, which has rendered existing technologies inadequate for collecting data from these new devices.

Fig 3: Forensics for Mobile Devices

2.3 Forensic Analysis of Memory

The field of memory forensics is famous in the forensics community.

This area has its roots in the very beginnings of computer forensics. Here, "memory" refers to a wide variety of storage media, including read-only memory, flash devices, non-removable memory (found in mobile phones and tablets), and random access memory. The field of live memory forensics has seen a lot of study, although there are still certain obstacles (Fig. 4).

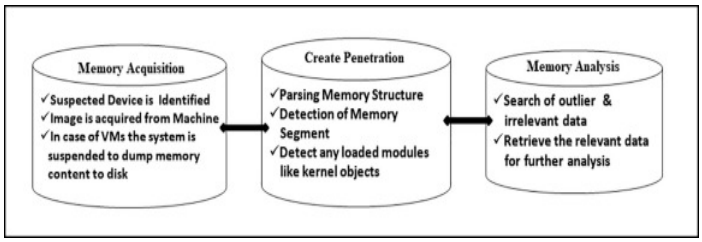

Fig 4: Forensic analysis of memory

2.4 Disk and Digital Forensics

Despite disk forensics' early 1990s inception, 2012–2014 saw a flurry of activity in the field. The subsequent collapse of the graph was due to insufficient data forensic tools. Data forensics had a little gap in its research when big data [11] first

ISSN [Online]: 2583-2654

appeared in the forensics industry. There is a lot of activity right now in data forensics with massive datasets that are either homogenous or heterogeneous. In the realm of data processing and connection, several issues remain unsolved [12]. The accompanying graphs (Fig. 5) illustrate the prevalence of research in these areas.

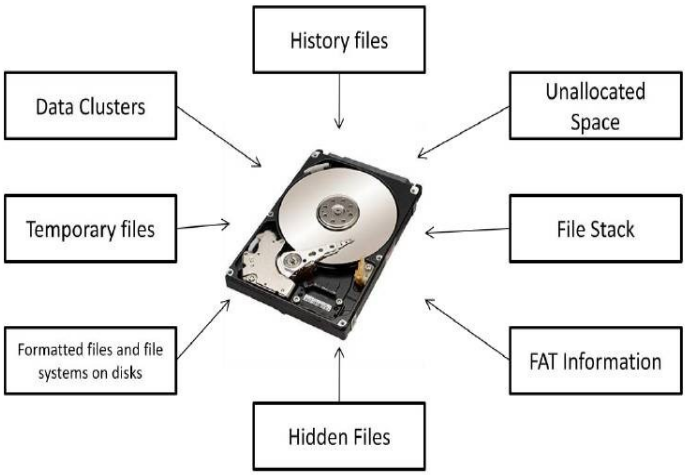

Fig 5: Disk and Digital Forensics

III. EXPERTISE IN FORENSIC AND ANTI-FORENSIC METHODS

The purpose of digital forensics is to track out the perpetrator by recovering, identifying, and analyzing data. Data that has been formatted, destroyed, or shredded may still be recovered by forensic processes across domains; hence, anti-forensics [13] aims to erase data, leaving no sign of deletion in the form of a log file, text file, or temporary internet file. Over the last 30 years, a plethora of forensic technologies have become accessible across all forensic disciplines. Also created were anti-forensic technologies, which aided criminals and attackers but hindered forensic professionals due to the overwhelming amount of data they had to process. Still, there aren't many solutions out there that can handle all the domains. Software like Encase, Caine's forensic tools, Oxygen's forensic suite, and many more are examples of forensic applications.

The current state of anti-forensic techniques:

1. Strategies for encrypting and decrypting data, often known as steganography
2. Software Developers
3. Bootable Drives and Live CDs
4. Online infrastructure
5. S.M.A.R.T. method for hard drives
6. Kernel access denied

IV. DISCUSSIONS FOR COMPARATIVE ANALYSIS

Every day, security measures are tightened, yet there have also been security breaches. Both forensic and anti-forensic instruments are in the works at the same time. Ransomware, injections of SQL queries, and spear phishing attacks are among the worst threats and assaults, and despite several security companies developing novel technologies and applications, there are not yet effective methods available to prevent them. Cybercrime statistics show an alarming increase in assaults every day, which makes many businesses and professionals afraid to fall victim. Many scholars are interested in forensics, but the field has not been able to meet expectations. When it comes to putting forensics into practice, researchers and examiners still face significant obstacles, such as cloud forensics and android forensics [14]. The need for a multi-tool that can handle various architectures and operating systems is the second big obstacle for mobile forensics [15]. Correlating the enormous amounts of big data [16, 17] and automated methods inside it is difficult for researchers in disk/data forensics.

V. CONCLUSION

Following a short introduction to forensics in the context of the cyber world, this article has covered cyber-attacks, different kinds of cyber threats, the extent of current research in the digital forensic sector, and various strategies used in forensics and anti-forensics. Testing the effectiveness of criminal justice toolkits when combined with anti-forensic techniques, conducting live analysis with test cases, and setting up various professional tools in Windows and Linux

ISSN [Online]: 2583-2654

environments using various critical test cases are all areas that could use more research. The development and deployment of a cross-platform integrated forensic tool is also part of the ongoing effort.

REFERENCES

[1]. Raghavan, S. (2013). Digital forensic research: current state of the art. CSI Transactions on ICT, 1(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7.

[2]. Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. Advances in Digital Forensics V, 17–36. https://doi.org/10.1007/978-3-642-04155-6_2.

[3]. Information Systems Audit and Control Association (ISACA) (2021). State of Cybersecurity 2020. Available: https:// www.isaca.org/state-of-cybersecurity-2020.

[4]. Finance Online (2022). 2022/2023 Cybersecurity trends. Available:

[5]. https://financesonline.com/cybersecurity-trends

[6]. F. Casino, et al, (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access.

[7]. H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, G. B. Wills, "Security, cybercrime and digital forensics for IoT," in Principles of Internet of things (IoT) ecosystem: Insight paradigm, Springer, Cham, 2020, pp. 551-577.

[8]. D. Paul-Joseph, J. Norman, "An analysis of digital forensics in cyber security," in First International Conf. on Artificial Intelligence and Cognitive Computing, Singapore: Springer, 2019, pp. 701-708.

[9]. V. Kumar&M. L. Garg, "Predictive analytics: A review of trends and techniques," International Journal of Computer Applications, vol. 182, no. 1, pp. 31-37, 2018.

[10]. J. H. Addae, X. Sun, D. Towey, M. Radenkovic, "Exploring user behavioral data for adaptive cybersecurity." User Modeling and User-Adapted Interaction, vol. 29, no. 3, 701-750, 2018.

[11]. N. Al Mutawa, J. Bryce, V.N. Franqueira, A. Marrington, &J.C. Read, "Behavioural digital forensics model: Embedding behavioral evidence analysis into the investigation of digital crimes," Digital Investigation, vol. 28, pp. 70-82, 2019.

[12]. W. Petherick, "Forensic victimology assessments in child abuse and neglect cases," in Child Abuse and Neglect, Academic Press, 2019, pp. 135-149.

[13]. R.Y. Patil, &M.A. Ranjanikar, "A new network forensic investigation process model," in Mobile computing and sustainable informatics, Singapore: Springer, 2002, pp. 139-146.

[14]. A.M. Balogun, T. Zuva. "Criminal profiling in digital forensics: Assumptions, challenges and probable solution," in 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), 2018, pp. 1-7.

[15]. D. Möller., Cybersecurity in digital transformation: Scope and applications. New York: Springer, 2020.

[16]. E. Holder, E.O. Robinson, K. Rose. "Electronic crime scene investigation: An on-the-scene reference for first responders," US Department of Justice Office of Justice Programs, 810, 2009.

[17]. M. Reith, C. Carr, G. Gunsch, "An examination of digital forensic models," International Journal of Digital Evidence, vol. 3, no. 3), pp. 1-12, 2002.