Global Scientific JOURNALS
GSJ: Volume 12, Issue 8, August 2024, Online: ISSN 2320-9186
www.globalscientificjournal.com

Computational Forensics and Cybersecurity

Mahmood S. Mahmood [1] Raghad y. Yahaa [2*]

[1] College of Science - University of Mosul, Mosul- Iraq, mahmoodsubhy1981@uomosul.edu.iq

[2*]College of Science - University of Mosul, Mosul – Iraq , raghadyy283@gmail.com

Abstract

The spread of the Internet has led to an increase in cybercrime, so it has become necessary to track malicious activities online to protect operations in law enforcement, national security and citizen protection. As a result, computer forensics has become important, law enforcement agencies and legal entities have realized the importance of IT professionals, and computer forensics has become a daily part of the investigation process. From a law enforcement perspective, it is difficult to find today a case that is not related to computer technology.

Computational forensics is the applied science of investigation and analysis techniques in collecting and maintaining evidence from a particular computer in a manner appropriate to be adopted as evidence in court. Computational forensics aims to conduct an organized investigation while maintaining the documentation of the evidence to find out exactly what happened in the digital world.

keyword: - Computer Forensics, Preserving Evidence, Cybersecurity, Data Recovery, Criminal Evidence.

1- Introduction

Computer forensics, also known as digital forensics or cyber forensics, combines computer science and legal forensics to collect digital evidence in acceptable manner for a court of law by identifying, collecting and storing evidence from an electronic device using technology and investigative techniques. Computer forensics is more important in the increasingly digitally connected world daily, and digital evidence management is critical mater for solving cybercrime and recovering important and compromised data, especially with the rise in cybercrime, according to Insurance Information Institute statistics, which means serious economic costs for individuals and companies[Ref].

With computers and other data collection devices frequently used everywhere, digital evidence – and the forensic process used to collect, preserve and investigate it – is becoming more important in resolving crimes and other legal issues.

2- Computational Forensics

The goal of computer forensics is to investigate evidence trail with the help of electronic media and to recover material on digital devices by conducting a systematic investigation and maintaining a documented chain of evidence to find out exactly what happened on the computer and who is responsible[Ref].

Computer crime can be defined as activity or issue related to computers represented by the misuse of the computer, by using the computer to commit a crime or that the computer itself is the target of the crime and the victim is a security incident .The task of the computer forensic investigator is to collect, examine and protect this evidence using computer forensic techniques to collect and maintain data while containing and eliminating the threat, ensuring that the appropriate guard chain is followed and that valuable evidence is not changed or destroyed. By the same way law enforcement officials comb crime scenes for evidence from personal computers, servers, mobile phones, tablets, and electronic storage devices helps discover important information that can help solve cases, bring criminals to justice and protect victims. [.1]

The legal action is taken from DFIR (Digital Forensics and Incident Response) team use to reconstruct cybersecurity incidents from start to finish to find out what have been happen and how it happened, the extent of the damage and how similar attacks can be avoided in future, Computational forensics, which is a fairly new specialty, focuses on computer security. [2].

3- Why is computer forensics important?

Like physical evidence at crime scenes, collecting and properly handling digital evidence is important as computational forensics and digital evidence play a crucial role in a wide range of issues, especially as everything has gone digital and the internet has almost everyone overnight in the age of technology. In response to these new frontiers of cybercrime, law enforcement agencies needed a system to investigate and analyze electronic data, so then computer forensics was born. Computer forensics is defined as the science of collecting, examining, interpreting, reporting and submitting electronic evidence related to computers, starting with cybercrime, intellectual property theft, phishing, data theft, network breaches, and illegal transactions such as electronic payment, hacking bank accounts and cyber stalking. [3] Having well-managed and secure data can help streamline the forensic process if that data is investigated. Forensic investigators use a many techniques and applications to examine digital copies of compromised devices. They search hidden folders and Unallocated disk space for copies of deleted, encrypted, or corrupted files. Any evidence found in the digital version is carefully documented in the results report and verified using the original device in preparation for legal proceedings involving discovery, or actual litigation. [1].

For big data, they can also adopt applications of the cloud, computer forensic analysis has been used to find information related to the penetration of the system or network, which is known as cloud forensics for the database, it has become necessary to retrieve and analyze

the data or metadata in the databases by examining the information contained in the databases, and then using these discoveries to identify and prosecute the perpetrators. In addition, they can use digital forensics experts and processes to facilitate data recovery in the event of a system or network failure due to a natural or other disaster. [4].

Like their counterparts in the field of legal investigation, computer forensic investigators need to be experts not only in searching for digital evidence but also in collecting and processing it to ensure its credibility and admissibility in court. Forensic investigators typically follow standard procedures, which vary depending on the context of the criminal investigation, or the device being investigated. [5]. The first step is to identify devices or storage media that may contain data, information sought by investigators, or other digital elements relevant to the investigation. These devices are collected and placed in a forensic laboratory or another secure facility to follow protocol and help ensure data recovery is properly restored. Computer forensics investigations in computer forensics use a range of techniques that are known to experts. Some common techniques include: .[6]

Reverse Hide Information Forensic experts create an image, or partial copy, of the data to be saved The process of trying to hide data within any type of digital file or message is called reverse hiding information if a cybercriminal hides important information within an image or digital file, as computer forensic experts examine the parts of the message or the contents of the file. They then store both the image and the original safely to protect them from alteration or destruction. Experts collect two types of data: persistent data, stored on the device's local hard drive, and volatile data, located in memory or in transit (for example, logs, cache, and random access memory (RAM). Volatile data should be cautious because is ephemeral and can be lost if the device is turned off or power is lost and is investigated on the digital version. They may also use publicly available information for forensic purposes, such as social media posts or Fees recorded in the payment application for the purchase of illegal products or services displayed on the website. [7].

furthermore, **Recover Deleted Files**, this technique involves recovering files or parts deleted by someone - whether accidentally or deliberately - or by a virus or malware by searching the computer system and memory for parts of files that have been partially deleted in one place but left traces elsewhere on the device. The analysis looks at volatile data as part of the forensic imaging process, which is often stored in cache or RAM. Many of the tools used to mine volatile data require a computer in a forensic laboratory to maintain the legitimacy of the evidence. [8]

And, **Drive Analysis**, forensic investigators analyze the image to identify relevant digital evidence. This technique involves analyzing data across multiple computer drives, linking them to information, and cross-referencing them to clarify similarities and provide context by comparing events from one computer to another and detecting anomalies Investigators use specialized techniques including direct analysis, the running device is analyzed from within the operating system using system tools on the computer, which is known as memory forensics for computer RAM (RAM) and/or cache. The analysis looks at volatile data This helps determine the cause of abnormal computer traffic, scans network packets and logs to identify suspicious activities, reconstructs the timeline compiles a chronology of events based on decryption timestamps, breaks encryption to access protected data, which is known as network forensics. Finally,

malware forensics, which involves analyzing and sifting code to identify malicious software such as viruses, Trojans, or ransom ware, and analyzing their payload. [7].

4- Cyber Security

The Academy of International Law was established in 1995 to reduce crime, combat terrorism, share knowledge and experience. In 1997 the Scientific Working Group on the Creation of Digital Evidence (SWGDE) develop standards for forensic medicine in the training and development by courses and programs in the field of digital forensics. Computational forensics is closely related to cybersecurity. However, computer forensics is concerned with retrieving data from the device in order to detect evidence of criminal activity, and is not interested in preventing cybercrime, such as cybersecurity. The results of computer forensics information that are revealed can help inform cybersecurity professionals about how to prevent cybercrime in the future..[4].

With cybercrime spreading throughout the network which costs users and institutions billions of dollars, cyber forensics is an inevitable and extremely important factor that not only threatens cyberterrorism organizations, but also harms people's lives through online drug promotion, militancy, etc. Technology has encouraged criminals to shift from physical crime to cybercrime, by accessing email and access to corporate and institutional computer networks and opening doors to malware and more complex cyberattacks. [4]

Therefore, it is critical to expand the scope of cyber forensics due to the increase in cybercrime According to the National Crime and Justice Research Council (NCRB), cybercrime doubled from 2016 to 2018, and is expected to quadruple than it currently is. This demonstrates the importance of law enforcement in solving cybercrime and cyber experts facing various cyber forensics challenges as it helps us combat hostilities by identifying the primary culprits. Evidence collected during investigations helps cybersecurity professionals locate hackers, cybersecurity professionals use a set of IT skills and thus protect the information within the system and protect the system's ability to operate and do their job, cybersecurity professionals use many different types of tools to protect the networks and the information they contain:.[9][6] Some of the tools they use include:

- **Web Application Firewalls (WAF)** A web application firewall monitors and filters traffic to and from websites, helping to keep your data safe from intrusions and secure it. Using scanning tools to protect financial and personal information and identifying vulnerabilities such as encryption issues, misconfigurations, missing patches, and vulnerabilities.
- **Vulnerability scanners** is a proactive approach that scan networks and software to identify vulnerabilities that an Internet hacker can exploit. Vulnerability screening is a vital part of the overall approach to IT risk management by security teams.
- **Penetration testing tools** is a term for cybersecurity that refers to a simulation series of cyberattacks in order to find security vulnerabilities. Its tools are used by cybersecurity professionals to carry out permissible breaches on

their own systems in order to detect vulnerabilities to help them make strategic decisions and prioritize reform actions.

- **Malware detectors** Malware can steal or encrypt data, in contrast, malware detectors review websites and programs to see if they are infected with malware and pose a threat.
- **Password protection tools** Password security tools help identify weak passwords, autofill saved passwords, or create passwords to help keep devices secure. [10]

Finally, it can be said that cybersecurity as a system is primarily concerned with preventing cybercrime, as hackers with their offensive skills are trying to actively work in order to test the strengths of the network, search for weaknesses and suggest how to improve them.

5- Cybersecurity and Criminal Evidence

With the world's increasing reliance on digital technology for the basic functions of life, technological advances, the increase in our online activities, and the increase in cybercrime, cybersecurity focuses on prevention. While computer forensics is all about recovery and reaction, cybersecurity is proactive and reactive, focusing on preventing and detecting cyberattacks, as well as responding to and addressing cyberattacks. Computer forensics is almost entirely interactive, starting to work in the event of a cyberattack Or a crime [11]. But computer forensics investigations often provide valuable information that cybersecurity teams could be used. Despite their differences, both aim to protect data, software, networks, and other digital assets. [11]

Cybersecurity helps prevent cybercrime from occurring, while computer forensics helps recover data when an attack occurs and also helps identify the culprit behind the crime by accelerating the processing of cyber threats while ensuring that any relevant digital evidence is not compromised to simplify the response to threats while preserving evidence against cybercriminals. Computer forensics, cybersecurity, and incident response help achieve an integrated workflow that can help security teams stop cyber threats faster while also preserving digital evidence that may be lost in light of the urgent need to mitigate threats. [12]

- The importance of cyber forensics is:

1- Cyber forensics helps gather important digital evidence to track down the criminal regardless of whether he is in physical reality as well as maintain computer integrity.

2- Electronic devices store huge amounts of data that the average person fails to see, a lot of information collected by modern devices, for example, computers in cars constantly collect information about when the driver brakes and changes speed without the

driver's knowledge. However, this information can be crucial in resolving a legal issue or crime, which is critical in cyber forensics.

3- It is useful for innocent people to prove their innocence through evidence collected online.

4- Digital evidence is not only useful in solving digital world crimes such as data theft, network breaches, and illegal online transactions but is used to solve real-world physical crimes, such as burglary, assault, murder, etc. [13]

- The scope of cyber forensics

The role of cyber forensics experts is becoming more important nowadays. Cyber forensics enables specialists to remotely examine any crime scene by collecting, preservation, processing and analyzing digital evidence, information stored or transmitted in binary form. Such evidence can be found on the computer's hard drive or mobile phone by reviewing browsing history, email logs or digital tracking. Get a digital copy of the system, which may lead to mixing the file with the files already on the computer, and using the following tools [3]: -

• **Replica authentication and confirmation:** The identification phase is the first step in the cyber forensics analysis process after the files are copied, experts verify that the copied data is exactly as consistent as it exists in the real system such as details about the parties involved, the nature of the crime, when and where it occurred, and the methods used. This helps the forensic investigator collect data in a criminally sound manner, by following standards and best practices recognized by the U.S. National Institute of Standards and Technology.

• **Ensure that the copied data is criminally acceptable:** This involves establishing a strict chain of custody and using storage procedures. A guard chain is a process that creates a path or record of all actions applied to digital evidence, ensuring that it remains intact throughout the analysis. It is possible to change the format of data as it is copied from a device, resulting in differences in the investigators' operating system and the system from which the data was copied. To avoid this, investigators make sure that the structure remains stable and that the data is criminally acceptable and written to the hard drive in a format that is appropriately used in the computer

• **Recover deleted files**: Cyber forensics experts examine and interpret digital evidence after recovering deleted or corrupted data using specialized tools and techniques

• **Technical report preparation**, preparation of technical, appropriate and easy-to-understand reports as a final step, forensic experts prepare a formal report clarifying their analysis, and share the results of the investigation and any conclusions or recommendations. Although reports vary by case, they are often used to present digital evidence in court, the result of this report is to clearly indicate the

crime, potential perpetrators, innocent individuals and what methods they used to commit the crime, and investigators present their findings in a legal proceeding, where they can be used to determine the outcome. [13,6]

- Skills required for a cyber-forensic investigator

• **Technical competence**: Cybersecurity is a technology-driven field; you are likely to be responsible for correcting errors, regularly updating systems, and delivering real-time protection software. To conduct routine operations, it is essential that cybersecurity professionals be technologically qualified.

• **Beware of details**: To preserve the vital elements of systems, avoid risks and measure potential impact, the investigator must be able to quickly identify problems and on alert to be able to conduct a comprehensive assessment of the infrastructure and the ability to analyze to develop solution methods and build a clear understanding of data in physical environments.

• **Strong communication skills**: A crime scene investigator must be able to examine and explain technical facts to others in depth. [13]

Nowadays, understanding the complexities of cybercrime investigations is more important than ever. From the investigation process to the key players, the tools and techniques involved in the world of cybercrime investigations have become important. By upgrading your cybercrime protection, you can detect relevant threats and prioritize them to prevent any type of attack.

6- Conclusion

Information security is defined as the protection of information assets to ensure integrity, prevent unauthorized access, and detect the existence of modifications or cancellations, for example, breaking into a computer system, while cyber forensics is used to collect and evaluate evidence specific to the computer specified in the investigation, such as hacking and hackers. With the ever-increasing cyber-attacks, cyber forensics is required to address such activities, as computer-related electronic evidence is collected, examined, interpreted, reported and submitted in the name of forensics. Cyber to use recovered data as evidence in criminal trials.

Reference

[1] Fenu, G., & Solinas, F., Computer forensics investigation an approach to evidence in cyberspace, In The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic. 2013, pp. 4-6.
[2] Pande, J., & Prasad, A., Digital forensics, Post-Graduate Diploma in Cyber Security Digital Forensics (PGDCS-06), Uttrakhand Open University, 2016.
[3] Muditha G. Role of Digital Forensic in solving cybercrimes Research, November 2021 , DOI: 10.13140/RG.2.2.18493.95205.
[4] Tmt. U., information security and digital forensics, Chennai 600028.
[5] John S. , Digital Forensics and Incident Response: Digital Forensic Process (Episode 2) ,Published Sep 30, 2023, https://www.linkedin.com/pulse/digital-forensics-incident-response-forensic-process-episode-john.

[6] Mugisha, D., Role and impact of digital forensics in cyber crime investigations. International Journal of Cyber Criminology, 2019, 47(3).
[7] Cyber Forensics , M.Sc. (IT), Institute of Distance and Open Learning , University of Mumbai, - 400 098. Tantia Jogani Industrial Est,p.33.
[8] Naeem A. R., Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, Department of Cyber Law at Tashkent State University of Law, Uzbekistan, 2023.
[9] Cybercrime Investigation Tools and Techniques You Must Know!, https://cybertalents.com/blog/cyber-crime-investigation.
[10] Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C., Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access, 2022, 10, 25464-25493, DOI: 10.1109/ACCESS.2022.3154059.
[11] Arpita Singh Maharana Pratap , Dr S. K. Singh , TECHNOLOGY REVOLUTION GIVES CYBERCRIME A BOOST: CYBER-ATTACKS AND CYBER SECURITY 1 Conference Paper · May 2019
[12] Lucky George , Cyber Law and Forensics , Dr. Ambedkar law university Chennai.
[13] Prasanthi, B. V., Cyber forensic tools: a review, International Journal of Engineering Trends and Technology (IJETT), 2016, 41(5), 266-271, DOI: 10.14445/22315381/IJETT-V41P249.