International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions

***[1]N Satyanandam, [2]Shravani Cheripally, [3]Veldi sriya**
*[1] Associate Professor, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, India
*[2,3] Students, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 01 April 2023
Published: 21 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
513-518

ABSTRACT

The internet is expanding at a breakneck pace, as the number of crimes perpetrated using or against computers. The area of computer forensics has arisen in reaction to the rise of computer crime. Computer forensics is the meticulous collection and examination of electronic evidence that not only analyses the damage to a computer because of an electronic attack but also recovers lost data from such a system to convict a criminal. As a result, the standard forensic process that is required after an electronic attack involves collecting evidence from a computer system, analyzing, and presentation of the collected evidence in court. Forensics deals primarily with the recovery and analysis of latent evidence. The growth of digital forensics has substantially increased the requirement for effective tools. There are several tools available today which are used to investigate the OS of a given computer. The purpose of this paper is to compare OS forensics tools by evaluating their ease of use, functionality, performance, and product support and documentation. This research will provide a brief comparative analysis of two widely used OS forensic tools-OSForensics and autopsy based on various contradictory factors.

Keywords: OSForensics, digital forensics, autopsy, data forensics, computer forensics

I. INTRODUCTION

Applying inspection and analysis methods to obtain and preserve data from the relevant computer device in a form that is appropriate for presenting in court is known as digital forensics. Digital forensics does a thorough investigation while maintaining a recorded chain of evidence to ascertain precisely what may be found on a computer system and who was responsible for it. Examiners and analysts now routinely employ digital forensics technologies [1]. In general, forensic analysts adhere to the following guidelines: investigators create a digital duplicate of the device's storage media after physically isolating it to ensure that it cannot be unintentionally contaminated. The original media is kept in a safe or another secure

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

location once it has been duplicated in order to preserve its condition. To investigate the copy, analysts employ several strategies and recovery applications forensic tools, looking for clones of erased, encrypted, or corrupted information in invisible folders and free disk space. Digital forensics is a crucial tool for resolving computer- related crimes including phishing and financial crimes as well as crimes against individuals where a computer may contain evidence. The forensic examination of a computer's data leak is known as memory forensics. Investigation of sophisticated computer assaults that are covert enough to not leave data on the machine's hard drive is its main use. In forensics, evidence is gathered, examined, and presented to the courts utilizing experimental knowledge. The retrieval and evaluation of evidence are the main topics covered by forensics. Evidence can come in a variety of shapes and sizes, including DNA evidence discovered in blood stains, fingerprints left on a window, and data on a hard drive. The process of gathering and analyzing data from networks, computer systems, storage devices, and wireless transmission in a form that is acceptable as evidence in a court of law is known as computer forensics [2]. Data gathering, authentication, and analysis are the three primary phases of computer forensic investigation. Making a bitwise duplicate of the disc is the main step in the data-gathering process. By comparing the duplicate with the original checksum, authentication establishes that the copy being used for analysis is a precise replica of the data on the original disc. If typical forensic techniques are unable to recover lost data, the user may be able to extract the data utilizing a more sensitive device, although this is seldom done because of the high cost of the required equipment. The main purpose of computer forensics is to gather electronic evidence for use in investigations. To use this knowledge in the prosecution of a crime, the evidence must be properly and lawfully gathered. Finding evidence of several crimes resulting in the trade secret theft using computer and network forensics techniques. Computer and network forensics aim to provide sufficient proof so that offenders can be effectively punished. For instance, evidence relating to child pornography, fraudulent transactions, drug or forgery records, or murder may be discovered during a criminal investigation. In civil processes, it is possible to find evidence of private and professional documents that pertain to fraud, harassment, or divorce. Professionals in computer network forensics aren't solely employed by attorneys. Insurers may need computer network forensics technology to find evidence to reduce the amount paid for claims. Additionally, anyone can employ computer network forensics to back up sexual harassment or other tort claims [3].

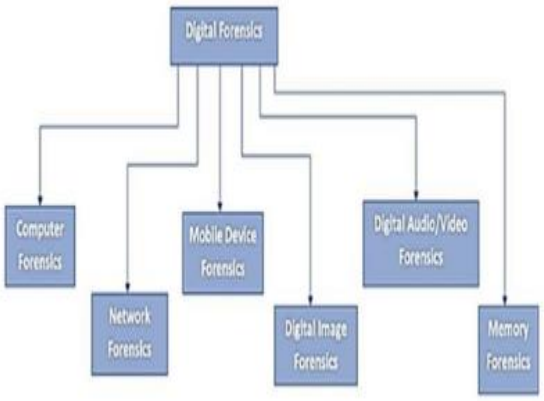

Fig. 1. Types of Digital forensics

II. RELATED WORK

Nisarg Trivedi and Dhruv Patel discussed about the Autopsy Forensics Browser which is a graphical user interface for The Sleuth Kit (TASK). Autopsy is a Windows-based, open-source, and free Source digital forensics software for event diagnosis. In a read- only setting, it is useful for analyzing disc images, local discs, and directories to identify potential reasons for an event. It is intended to be an expandable platform that can accommodate plug-in components from both open-source and proprietary software projects to provide an end-to -end computer forensics solution. This article describes the installation of Autopsy, data

intake, data analysis, and software features in the most recent version.

Vedanta Kapoor et. al explored the principles of digital forensics and discuss the numerous forensics investigation teams that are at their disposal. Additionally, they talk about the many kinds of cybercrimes that occur and the tools that are available to stop them. Additionally, they conducted a comparison analysis of all the tools available based on many aspects, providing the reader with an abstract understanding of which tool to employ for the greatest outcomes. B. V. Prasanthi explored all the different branches of digital forensics and forensics frameworks that are there and reviewed all the popular digital forensics tools available in the market that are in use by various agencies for the purpose of crime investigation. Each tool is made to suit different needs such as Caine is used for virtual forensics, X-Ways Forensics for disk imaging and cloning, Libforensics to develop digital forensics applications and extract info from various sources, etc. Nowadays, every second someone falls victim to cyber -attacks or cyber thefts, and hence Cyber Forensics is indispensable in today's world. Security and scalability are important issues for system[16,17]. Shaweta Sachdeva et al. did an in-depth analysis of the various tools that exist online for performing Digital Forensics and security faults. They have explained in detail all the phases involved in the data analytics process and their significance, starting from the Identification phase, followed by Acquiring phase, the Authentication phase, the Analysis phase, and lastly Presentation phase. In the present scenario, the number of mobile phone and computer users only seems to be increasing, and hence more and more people are falling prey to cyber-attacks and scams. Hence, we cannot underestimate the importance of digital forensics. Jarno Baselier has described all about the tool OSForensics and its application in the field of Digital Forensics. OSForensics is a tool that is a complete suite of tools with different uses. It is used for both live-acquisition and non-live-acquisition forensics. The paper talks about the complete installation process of OSForensics and the steps involved in it, as its striking features make OSForensics stand out and outperform its other competitors in the market. It is very affordable as compared to other software's available in the market and significantly faster. The author has also explained in detail its interface and various components of the software.

III. PROPOSED SYSTEM

Image forgery detection is explained. At first stage in block based copy move forgery detection techniques, an be pre-processed e.g. change from shading to grayscale picture. At that point, the preprocessed picture issub separated into covering squares of size B × B. From every one of the hinders, a one of a kind portrayal as highlight vectors is acquired. At that point, for coordinating procedure these component vectors might be orchestrated strategies, for example, lexicographic arranging, neighbor and so on and some sort of separation measure is utilized between neighboring element vectors, for example, Euclidean Distance. What's more, in conclusion some morphological task is connected with the goal that it identifies the produced locale.

A. Pseudo code for a nonexclusive falsification identification:

Step-1:Input picture
Step-2: pre-preparing
Step-3: square division
Step-4: include extraction
Step-5: include coordinating
Step-6: Detection result

B. Image falsification location strategies:

Duplicate move (Cloning): A duplicate move falsification is made by reordering content inside a similar picture, and conceivably post preparing it. In this period, the recognition of duplicate move imitations has turned out to be a standout amongst the most effectively examined subjects in daze picture

legal sciences. A standout amongst the most well-known assault is duplicate move altering pictures where a district of a picture is replicated starting with one section and is moved then onto the next part in a similar picture. The replicated district can go under various preparing like pivot, scaling, etc.. The altered picture might be controlled utilizing strategies to make it difficult for the human eyes to find the phony [3S]. Picture grafting: Picture splicing is a straightforward procedure that yields and glues locales from the same or separate sources. It is a major advance utilized as a part of computerized photomontage which alludes to glue up created by staying together pictures utilizing computerized instruments, for example, Photoshop [26]. Picture joining is a picture altering strategy to duplicate a piece of a picture and glue it onto another image [17]. Resize: This activity can be utilized to contract or grow the span of a picture or part of a picture utilizing decrease, zooming and scaling strategies.

IV. FORENSIC ANALYSIS TOOLS

The digitalization of the world is getting all the more dominant step by step. So the field of digital forensic is additionally developing extremely quickly. In this segment, we will talk about three digital forensic tools under the irrespective categories:

Network Forensic is the field of Digital criminology where the investigators focus on packets traveling in a network and the details of the computer systems connected to that network.

Following are the tools to test the network forensic applications:

Wireshark

Wireshark is free and analyzer of open source network protocols that empowers the investigator to intelligently browse the computer network data traffic. The author of Wireshark is Gerald Combs and created by the Wireshark group. It catches live information from a network interface. It captures traffic and converts it into a readable arrangement. This makes simple to recognize how much traffic crosses the network, how often and how much latency there is between some hops and so on. Wireshark supports over 2,000 network protocols. Live information is perused from various kinds of the network like IEEE 802.11, Ethernet, PPP (Point-to-Point Protocol) and loopback. Wireshark colors data packets toassist the client by identifying the sorts of traffic.

2. Nmap (Network Mapper)

Nmap is a network scanner used by sending packets and reviewing replies to find host and equipment on a computer network. The developer of Nmap is Gordon Lyon (Fyodor). It identifies the open ports on target hosts and interrogates remote network facilities to determine the name and version number of the application. It also helps to identify the operating system (OS).

NESSUS

Nessus is a vulnerability scanner for open-source networks that uses the normal vulnerabilities and architecture of the exposition. It has a web-based interface that contained a web customer and a simple HTTP server. It does not require any software installation apart from the Nessus server. It can distinguish potential vulnerabilities in the frameworks. It incorporates configuration reviewing, resource profiling, rapid discovery, and delicate information revelation and defenselessness analysis of a security act. It is created by Tenable. Inc.

Xplico

Xplico is a Network Forensic Analysis Tool (NFAT) which is an application that reproduces the acquisition contents conducted with a packet sniffer. It is created by Giauluca Costa and Andrea de Franceshi. The objective of Xplico is to extract web traffic to catch the application's information it contained. It permits simultaneous access by various

investigators. The tool analyzes web packet and catches them to remove and parse certain protocols and return web action, for example, VoIP, email and HTTP. The Xplico framework underpins various protocols with the most steady being: HTTP, ARP, SMTP, PPP, SIP, VLAN, DNS, IPv4, IPv6, TCP, UDP, FTP and so on. To prevent protocol misidentification, every application protocol is recognized using Port Independent Protocol Identification (PIPI).

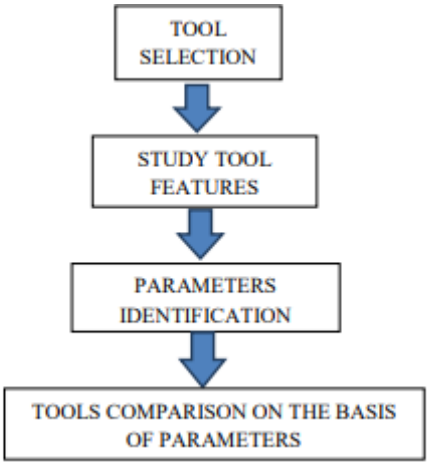

Fig.2 Flow Chart of Strategy

V. CONCLUSION

Digital forensics is a multi-disciplinary and inter-disciplinary field encompassing diverse disciplines such as criminology, law, ethics, computer engineering, and information and communication technology (ICT), computer science, and forensic science. It is the process of uncovering and interpreting electronic data so as to preserve any evidence in its most original form. Although the field of digital forensics is still young, increased awareness of DF has drawn many to this developing field. It is going through a transition from a relatively obscure tradecraft to a scientific field that needs to be continuously held to higher standards. Several next generation forensic analysis systems are under development. Colleges and universities around the world have started to offer courses in DF in the information security curriculum at undergraduate and graduate levels. The Digital Forensic Research Workshop (DFRWS) has contributed more than any other organization to research and development in digital forensics. It has organized annual open workshops devoted to digital forensics since 2001 [9].

VI. REFERENCES

[1]. Mayank Lovanshi and Pratosh Bansal, "Comparative Study of Digital Forensic Tools" in Springer Nature Singapore, 2019.

[2]. KhalequeMdAashiq Kamal, Mahmoud Alfadel and Munawaran SaiyaraMunia, "Memory Forensic Tools: Comparing Processing Time and left Artifacts on volatile memory", International workshop on Computational Intelligence (IWCI), 2016.

[3]. S. McCombie amd M. Warren, "Computer Forensic: An issue of definition", 1st Australian Computer, Network and Information Forensics Conference, 2003.

[4]. Phillip D. Dixon, "An Overview on computer Forensics", IEEE, December 2005.

[5]. Pratima Sharma, Kirti Jain, Bharti Nagpal and Tanvi, "REGEX: An Experimental Approach for Searching in Cyber Forensic", IEEE Conference, March 2017.

[6]. VarshakarbhariSanap and Vanita Mane, "Comparative Study and Digital Forensic Tools", International Journal of Computer Applications, ICAST 2015.

[7]. Priyanka Dhaka and Rahul Johari, "CRIB: Cyber Crime Investigation, Data Archival and analysis using Big Data Tool", ICCCA 2006.

[8]. Ed Crowley, "Information System Security Curricula Development", ACM, October 2003.

[9]. Matthew C. Stamm, Min Wu and K.J .Ray Liu, "Information Forensics: An Overview of the First Decade", IEEE Access, May 2013.

[10]. HamdaBariki, Mariam Hashmi and Ibrahim Baggili, "Defining a Standard of Reporting Digital Evidence Items in Computer Forensic Tools", Institute of Computer Sciences, Social Informatics and Telecommunication Engineering, 2011.

[11].Charles Lim, Meily, Micsen and HerryAhmadi, "Forensic Analysis of USB Flash Drives in Educational Environment", IEEE, 2014.
[12].Ahmed Ghafarian, "Forensic Analysis of Cloud Computing Services", Science and information conference, 2015.
[13].GouthamiVelakanti and Aditya Katuri, "Enhancement of existing tools and Techniques for Computer Forensic Investigation", International journal of computer science and information technologies, Vol. 5, No.1, pp. 161-164, 2014.
[14].Leonardo Carvajal, CihanVarol and Lei Chen, "Tools for Collecting Volatile Data: A survey Study", IEEE 2013.
[15].https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

Cite this article as :

N Satyanandam, Shravani Cheripally, Veldi sriya, "Emotion based Music Recommendation System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.513-518, March-April-2023.