International Journal of Engineering, Science and Mathematics
Vol. 11 Issue 07, July 2022,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Forensic Foresight: A Comparative Study of Operating System Forensics Tools

Author Info

Chaitanya Krishna Suryadevara

Department of Information Systems

Wilmington University

Chaitanyakrishnawork123@gmail.com

Abstract

Digital forensics plays a pivotal role in modern investigations, aiding in the extraction and analysis of digital evidence from various computing environments, including operating systems (OS). This research paper presents a comprehensive comparative analysis of OS forensics tools, aiming to evaluate their capabilities, features, and effectiveness in assisting digital forensic experts. Through an exhaustive examination of a diverse range of OS forensics tools, this study seeks to provide valuable insights for practitioners, researchers, and law enforcement agencies. Our analysis covers key aspects such as data acquisition methods, compatibility with different OS environments, ease of use, speed, and reliability of the tools. We also consider the robustness of each tool in handling various file systems, encryption, and anti-forensic techniques. Furthermore, this research examines the adaptability of these tools to evolving OS architectures and their potential for automated forensic procedures. By conducting rigorous testing and benchmarking, we offer a comprehensive comparison of both open-source and commercial OS forensics solutions, shedding light on their strengths, weaknesses, and suitability for different forensic scenarios. The findings of this comparative analysis aim to assist forensic investigators in making informed decisions when selecting OS forensics tools for their investigations. Additionally, it provides a basis for future development and improvement of digital forensic tools, ensuring that they remain effective in the face of evolving operating system technologies and security measures.

Keywords: digital forensics, operating system, forensics tools, comparative analysis, data acquisition, compatibility, file systems, encryption, anti-forensic techniques, benchmarking, automated procedures, open-source, commercial solutions, investigative decision-making, security measures.

Introduction

Digital forensics has become an indispensable field in contemporary investigations, facilitating the extraction and examination of digital evidence from a wide array of computing environments, particularly operating systems (OS). The proliferation of technology and the digitalization of information have heightened the importance of OS forensics tools as critical assets for forensic practitioners. These tools serve as the gateways to uncovering crucial information hidden within the digital artifacts of an operating system. This research paper embarks on a comprehensive journey through the realm of OS forensics tools, with the overarching aim of providing an evaluative and comparative analysis. The objective is to assess the capabilities, features, and overall effectiveness of these tools in the context of digital forensic investigations. In doing so, we endeavor to offer insights and guidance to practitioners, researchers, and law enforcement agencies navigating the complex landscape of OS forensics.

Our investigation scrutinizes a diverse spectrum of OS forensics tools, ranging from those available as open-source solutions to their commercially developed counterparts. The examination encompasses pivotal aspects such as data acquisition methods, compatibility with varying OS environments, ease of usability, speed, and the reliability of results produced by each tool. Furthermore, we explore the resilience of these tools in the face of challenges posed by different file systems, encryption mechanisms, and anti-forensic tactics.

In an ever-evolving technological landscape, we also investigate the adaptability of these tools to keep pace with changing OS architectures and their potential for streamlining forensic procedures through automation. Rigorous testing and benchmarking procedures are employed to establish a comprehensive comparison, allowing us to delineate the strengths, weaknesses, and contextual suitability of these OS forensics solutions.

This research endeavors to assist forensic investigators in making informed decisions when selecting OS forensics tools tailored to their specific investigative needs. Furthermore, it lays the foundation for ongoing advancements and enhancements in the realm of digital forensic tools, ensuring their continued efficacy in the face of evolving operating system technologies and ever-heightening security measures. The following sections of this paper delve into a detailed examination of OS forensics tools, uncovering their unique characteristics and contributions to the field of digital forensics.

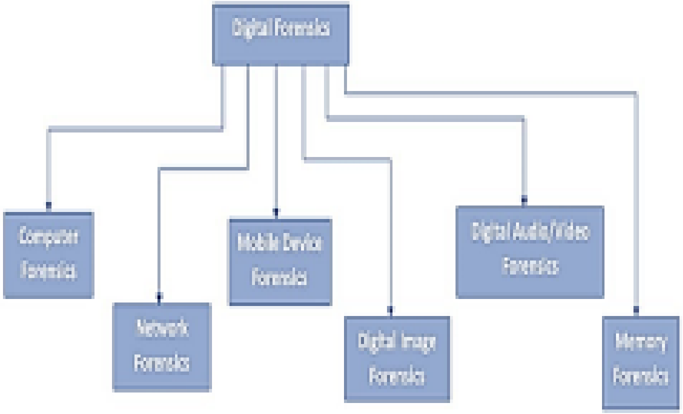


Fig. 1. Types of Digital forensics

Digital forensics encompasses various specialized branches, each focused on different aspects of digital evidence collection, analysis, and investigation. Here are some common types of digital forensics:

1. **Computer Forensics:** This is perhaps the most well-known branch of digital forensics. It involves the investigation of computer systems, including desktops, laptops, servers, and other digital devices, to uncover evidence related to cybercrimes, data breaches, hacking, and unauthorized access. Computer forensics experts analyze file systems, logs, and memory to retrieve information.
2. **Mobile Device Forensics:** With the proliferation of smartphones and tablets, mobile device forensics has become essential. This branch deals with extracting and analyzing data from mobile devices, including call logs, text messages, emails, GPS data, and app usage. It's crucial for cases involving mobile-related crimes, such as cyberbullying, drug trafficking, or missing persons.

3. **Network Forensics:** Network forensics focuses on investigating network traffic data to detect and analyze security incidents, cyberattacks, and unauthorized activities. This involves monitoring and analyzing network packets, logs, and traffic patterns to reconstruct events and identify intrusions or data breaches.
4. **Malware Analysis:** Malware forensics experts analyze malicious software (malware) to understand its functionality, origins, and impact. They dissect malware samples to determine how they infect systems, propagate, and communicate with command and control servers. This information is vital for preventing and mitigating cyber threats.
5. **Digital Media Forensics:** This branch is concerned with the analysis of digital multimedia content, such as images, audio recordings, and videos, to uncover evidence related to crimes like child exploitation, copyright infringement, and tampering with digital media. Digital media forensics experts use specialized tools to verify the authenticity and integrity of media files.
6. **Cloud Forensics:** As more data and applications migrate to the cloud, cloud forensics has emerged as a critical field. It involves investigating cloud service providers and their infrastructure to retrieve digital evidence stored in remote servers. Cases involving data breaches, data loss, or cybercrimes in cloud environments fall under this category.
7. **IoT (Internet of Things) Forensics:** IoT forensics deals with digital evidence from interconnected smart devices and sensors. It includes the investigation of data generated by IoT devices like smart home appliances, wearables, and industrial sensors. This field is becoming increasingly important as IoT adoption continues to grow.
8. **Memory Forensics:** Memory forensics experts analyze the volatile memory (RAM) of a computer or device to extract information that may not be available on disk. This can include active processes, passwords, encryption keys, and other valuable data that may provide insights into ongoing cyber incidents.
9. **Incident Response and Digital Triage:** While not strictly a type of digital forensics, incident response and digital triage involve the initial steps taken to assess and respond to security incidents. This includes identifying and containing threats, preserving evidence, and minimizing damage during the early stages of an investigation.

These are some of the primary types of digital forensics, but the field continues to evolve as technology advances. Specialization within these areas and the development of new subfields are common as digital forensic experts adapt to emerging challenges in the digital realm.

1. LITERATURE REVIEW

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.

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.

Table 1 Literature Review Table

Author	**Title and Description**
Nisarg Trivedi and Dhruv Patel	- Title: Autopsy Forensics Browser - Description: Discusses Autopsy, a Windows-based open-source digital forensics software for event diagnosis, including installation, data analysis, and features.
Vedanta Kapoor et. al	- Title: Principles of Digital Forensics - Description: Explores digital forensics principles, various investigation teams, cybercrimes, and tools, including a comparative analysis of available tools.
B. V. Prasanthi	- Title: Digital Forensics Tools and Frameworks - Description: Explores different digital forensics branches, frameworks, and popular tools used for crime investigation, highlighting their specific applications.
Shaweta Sachdeva et al.	- Title: In-depth Analysis of Digital Forensics Tools - Description: Provides a detailed analysis of online tools for digital forensics and security faults, covering various phases of the data analytics process.
Jarno Baselier	- Title: OSForensics in Digital Forensics - Description: Focuses on OSForensics, a suite of tools for digital forensics, covering installation, features, and its advantages over competitors.

2. Forensic Analysis Tools

2.1 Autopsy

It is a GUI-based digital forensics tool that permits the user to explore hard disk drives and PDAs. It contains a module architecture that enables the user to find supplemental applications or support unique Python or Java projects. This tool contains localized email records and conversations and assists a sizable number of users all around the world. Autopsy is used by law enforcement and business inspectors to examine what happens on a computer. In fact, the user may use it to restore photos from the memory card of their camera. The term "autopsy" refers to the process of investigating the disk's contents after consumption. The most popular types of data conceptual by ingesting are used in digital forensic investigation, which keeps a strategic distance from the necessity to physically carry out the tasks.

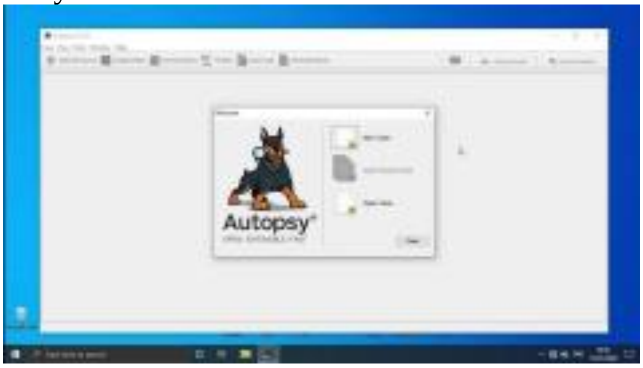


Fig. 2. Autopsy Forensic Tool

2.1.1 Features of Autopsy:

● Timeline analysis: helps in identifying activity by displaying framework events

in a graphical connection point. ● Registry analysis: utilizes RegRipper to

differentiate recently accessed archives and USB devices.

- Keyword Search: Using text extraction and record-checking modules, users may uncover records that include certain phrases and discover common articulation patterns.

● Email Analysis: Like Thunderbird, email analysis can also parse MBOX design messages.

2.2 OS Forensics

OS Forensics is a toolbox that provides a tonne of information on how a machine is used and the files that are stored on it. Users may absolutely manage their tasks and projects with OSForensics. Operating system forensics allows users to monitor what their children are doing on the system and enlist legal experts in the investigation. The application can be easily installed on computer memory. It helps the user to find particular documents on the computer, recover deleted data, keep track of activity, or create a report with specialized information about the machine.It is also quite simple to use, which is fortunate because there is no documentation for the complexities. There is a rare scenario that a user ever has to examine a computer completely, in that scenario OS forensics could be the best tool that can help. Operating System Forensics is essentially a thorough investigation of all devices, and its user interface syncs well. It may also be set up on a USB storage device.

Fig. 3. OSForensics Tool

2.2.1 Features of OSForensics Tool:

- Discover forensic evidence faster: In OSForensics, we find documents quicker, by searching by filename, size, and time. The zoom online search tool may be used to browse document objects in email files from Mozilxla, Thunderbird, and Outlook, and that's only the beginning. Erased records can be looked at and recuperated. Data of the framework is gathered. Recuperation of secret words from internet browsers and finding and uncovering stowed-away regions in the hard disk.

- Manage the digital investigation Case: The executives give the user the authority to total and plan results. HTML case reports provide a summary of the conclusions and information users have concerning a case. Drive imaging is utilized for making/reestablishing a precise duplicate of a stockpiling gadget and remaking raid clusters from individual disk pictures.Operating system forensics can be introduced on a USB streak drive for additional versatility and to keep a protected log of the specific exercises completed throughout the examination.

2.3 DFF (Digital Forensics Framework)

A digital forensics framework is open-source computer forensics programming. It is utilized both by proficient and non-master individuals to accumulate, moderate, and con-cede digital proof without compromising frameworks and data rapidly and without any problem. It is used to compile, moderate, and concede digital proof without jeopardizing systems and data by both experts and non-specialists. Its order line interface empowers to perform digital examination from a distance and accompanies regular functionalities accessible in like manner system like finish, undertakings the executives, and globing or console easy routes. The digital forensic framework may also launch a number of scripts to automate repeated tasks. High-level users and engineers may also preplan their investigation using a digital forensic framework directly from a Python mediator.

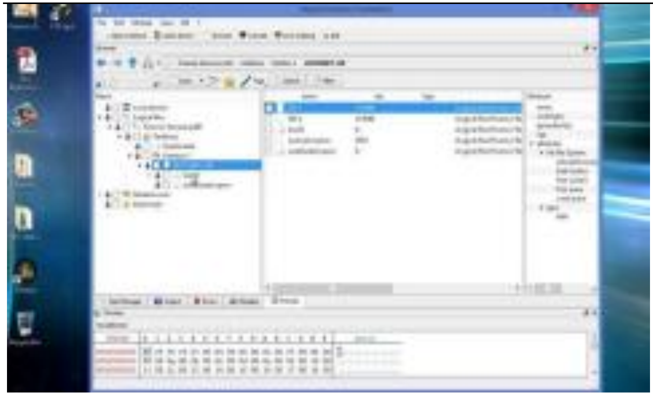


Fig. 4. DFF Forensic Tool

2.4 Wireshark

Wireshark is a free open-source parcel analyzer. It is used for network damage, testing, programming and association convention progress, and education. With this tool, we can view every package on the network and gauge the high level of traffic in our company. Every OS is compatible with Wire Shark, and it has a user-friendly interface in GUI contexts. Wire shark is the world's most appropriate organization analyzer. This is an extremely useful asset that gives organization and upper-layer conventions data about the data caught in an organization.

A network bundle analyzer is a monitoring tool used to look within an organization link to see what's going on. One of the best sniffers anyone could expect to discover is being developed as a free, high-quality sniffer called WireShark. It includes amazing components and a great graphic user interface that has been properly developed and produced do. It is supported by Windows, MAC OS X, and frameworks built on Unix. This amazing sniffer Wireshark has channels, a diversity of codes, and numerous perspectives that enable users to inspect individual bundles and delve deeply into network data. Wireshark may be used to analyze a large program's network traffic, sweep the traffic stream on the network, or track out network problems.

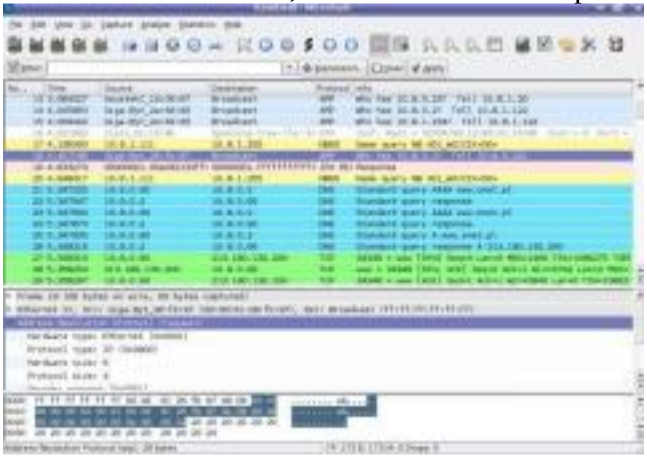


Fig. 5. Wireshark Tool

2.5 TrueCrypt

An encryption tool called TrueCrypt is available as freeware and is open source. It can encrypt a package, the entire stockpiling device, or create a virtual fragmented disk inside a document. It has full disk encryption and is a multi-stage open-source record of documents. Additionally, it has the ability to arrange a fragmented hard disk section on a smaller encrypted record that is clearly visible to any disk administrator. It provides advanced encryption without any problems. Additionally, it offers "on-the-fly encryption," which means that after entering the right password, we don't need to rely on bulky papers to decode the information, showing that the data are readily available. TrueCrypt protects very sensitive personal and corporate classified data. To prevent unauthorized access to legitimate data, it employs document encoding and package encryption.

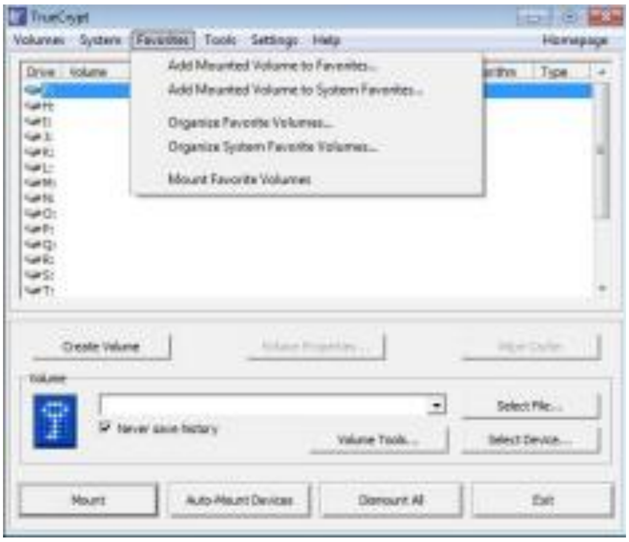
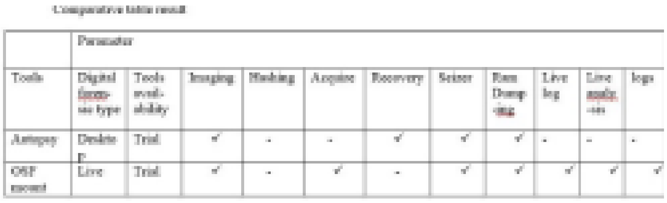


Fig. 6. TrueCrypt Forensic Tool

For the key inference, a few combinations of hash and encryption computations are used. TrueCrypt is the tool that helps to encrypt the data. This method is replicated from one storage disk to another storage disk when we clone from a TrueCrypt disc. At that stage, data got decoded and temporarily stored in memory. Decoded data is always temporarily kept in RAM by TrueCrypt; it is never saved to a disk. In any case, the volume's data collection is already encoded before it is mounted.

3. COMPARATIVE ANALYSIS RESULTS



Comparative table result

	Parameter										
Tools	Digital forensic type	Tools availability	Imaging	Hashing	Acquire	Recovery	Seizer	Ram Dumping	Live log	Live analysis	logs
Autopsy	Desktop	Trial	✓	-	-	✓	✓	✓	-	-	-
OSF mount	Live	Trial	✓	-	✓	-	✓	✓	✓	✓	✓

Fig. 7. Comparative Analysis Results

4. RESEARCH CHALLENGES

With the huge advancement of computer innovations over the last ten years, the use of innovation has been characterized as both great and terrible. While certain individuals use innovation to develop things to help humanity, hoodlums likewise use innovation to accomplish their own objectives. One of the primary issues is that when an innovation is created to recognize and research hoodlums, there is one more method that assists lawbreakers with concealing themselves. This is a gigantic test forensics officials face today. Not at all like numerous different wellsprings of actual proof, digital proof is not difficult to change, eliminate or stow away, perhaps without leaving tracks that could distinguish the lawbreaker. So, hostile to forensics has turned into a significant test for digital forensics. The various challenges that occur during forensics include:

A. Encryption

Encryption is the cycle of scrambling data that must be decoded and perused by somebody who has the right deciphering key. Encryption is utilized to stow away or make the proof mixed up on the compromised framework.

In 2007, an occurrence happened when US customs tracked down youngster erotic entertainment on Canadian resident and legitimate us occupant Sebastian Boucher's pc. The pc was seized as evidence, and he was accused of shipping the porn across borders. The issue seemed when inspectors attempted to open the implicating drive z and figured out that it was a pretty good privacy scrambled holder. Albeit a forensic copy of the hard drive was made after the closure of the journal, the inspector couldn't open the scrambled compartment.

Attackers use a variety of encryption methods, and in order to make the data useable, experts must decode the encrypted data. It is time-consuming, and occasionally the data that has been scrambled cannot be read.

B. Steganography

Steganography is an encryption strategy that can be utilized alongside cryptography as an extra-secure technique in which to safeguard data.". Steganography is a technique that may be used to hide any data inside of a record transporter without altering its outside appearance. This steganography is used by attackers to hide their secret data (payloads) inside the hacked framework. The expert must identify this hidden data while analyzing computer infractions in order to unearth the information for further reference.

C. Undercover Channel

An Undercover communication channel, sometimes known as a hidden channel, allows attackers to hide information from the organization and perhaps evade interruption detection methods. Regularly, an organisation convention is picked, and its header is changed to spill messages between assailants, taking advantage of the way that a couple of fields of the header are adjusted during transmission.". Assailants utilize these secrets directly to keep a secret association between the assailant and the compromised framework. It is less recognizable.

D. Data concealing away space

Attackers hide some data inside volume sections and make it impossible for the regular framework commands and projects to find them. It complicates and prolongs the assessment, and occasionally, the validity of the data might be disputed. Perhaps the most well-known method of obscuring data away from the computer is a rootkit.

As per Microsoft (2014), malware architects use rootkits to stow away malware inside casualties' pcs. It is exceptionally difficult to distinguish rootkits and most computer clients don't have the foggiest idea about how to eliminate these rootkits. Client mode rootkits are equipped for stowing away "processes, records, framework drivers, network ports, and even framework administrations".

E. Remaining Data Wiping

Data cleanup for leftovers is yet another name for remaining data wiping. A few hidden cycles are operating without the attacker's information at the time the attacker uses a computer to accomplish his goal. However, a shrewd attacker can avoid this risk by removing the tracks left by his machine and making the structure appear as though it hasn't been used for that purpose.

F. Tail obfuscation-going after the apparatuses

The most well-known strategy is the obscurity of the well-spring of the assault. Here, the assailant involves bogus data to deceive the specialist .In this manner now and again the examiner could miss a few data that have forensic worth.

5. CONCLUSION

Various individuals across the globe have proposed various strategies for distinguishing imitations. Different approaches to altering pictures are talked about above in this paper. As from the above conversation, the inactive methods or visually impaired imitation identification is liked over dynamic procedures as dynamic strategies require the first picture alongside the manufactured picture. In any case, with uninvolved recognition methods history of the picture isn't by any stretch of the imagination required. This element is detached method makes it extremely renowned. Crooks are turning out to be increasingly more fit for doing falsifications with various procedures. They utilize different strategies all at once altogether not to be identified by accessible fraud discovery procedures. Right now, accessible advances to identify fabrications are not programmed and the majority of the apparatuses expect humans to work. Computerizing these devices is a truly extreme undertaking to be achieved in not so distant future.

In this paper, we analyzed particular forensic apparatuses utilized for breaking down security blemishes in digital forensics and the point-by-point survey of digital forensics. The data structure that is located in memory may also be used to get digital proof using a variety of devices. The new cycle model is chosen to quickly acquire urgent proof and investigate the situation. The Stepwise Forensic

The data structure that is located in memory may also be used to get digital proof using a variety of devices. The new cycle model is chosen to quickly acquire urgent proof and investigate the situation. The stepwise forensic process model demonstrates an in-situ method that provides occurrence-recognizable evidence, recovery, and analysis. The SFPM suggests a brand-new investigative paradigm for selecting the aim and, as it were, breaking down the key confirmations. To surpass the limitations of the conventional forensic model, it is planned to quickly pick and assess the framework depending on the circumstances surrounding the crime scene.

The network parcel analyzer is focused on network research analysis, the evolution of correspondent norms, and in education. It detects network traffic as well as a distinct increase in traffic in our company. The sophisticated forensic tools are supposed to collect and analyze data throughout the forensic investigation, but they are also anticipated to spot any errors or conflicts that may have occurred during execution.

Because of the quick expansion in the number of Internet clients across the world, the recurrence of digital assaults has expanded. In this way, the need to devise successful systems and foster proficient apparatuses to conveniently recognize these assaults. In this paper, we have analyzed various devices for performing digital forensic examinations. This examination gives a temporary investigation of the instruments concerning the digital forensic examination.

6. REFERENCES

1. R.S Khalaf and A. Varol, ”Digital Forensics: Focusing on Image Forensics,” 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-5, doi: 10.1109/ISDFS.2019.8757557

2. G Maria Jones; S Godfrey Winster, ”An Insight into Digital Forensics: History, Frameworks, Types and Tools,” in Cyber Security and Digital Forensics: Challenges and Future Trends, Wiley, 2022, pp.105-125, doi: 10.1002/9781119795667.ch6

3. H. Majed, H. N. Noura, and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," 2020 8th International Symposium on Digital Forensics and Security (IS-DFS), 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116399

4. O. M. Adedayo, ”Big data and digital forensics,” 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016, pp. 1-7, doi: 10.1109/IC-CCF.2016.7740422

5. Refaces. (2022, January 18). What is Digital Forensics: Process, tools, and types: Computer Forensicsoverview. RecFaces. Retrieved from https://recfaces.com/articles/digital-forensics

6. K. U. Maheshwari and G. Shobana, "The State of the art tools and techniques for remote digital forensic investigations," 2021 3rd International Conference on Signal Processing and Communication (ICPSC), 2021, pp. 464-468, doi: 10.1109/ICSPC51351.2021.9451718.

7. L. Chen, L. Xu, X. Yuan and N. Shashidhar, "Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges," 2015 International Conference on Computing, Networking and Communications (ICNC), 2015, pp. 1132-1136, doi: 10.1109/ICCNC.2015.7069509.

8. K. S. Singh, A. Irfan and N. Dayal, "Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 584-590, doi: 10.1109/ISCON47742.2019.9036214.

9. K. Ghazinour, D. M. Vakharia, K. C. Kannaji and R. Satyakumar, "A study on digital forensic tools," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017, pp. 3136-3142, doi: 10.1109/ICPCSI.2017.8392304.

10. A. Al-Sabaawi, "Digital Forensics for Infected Computer Disk and Memory: Acquire, Analyse, and Report," 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020, pp. 1-7, doi: 10.1109/CSDE50874.2020.9411614.