iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47346

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

A Comparative Analysis of OS Forensics Tools

Manjot Kaur Bhatia[1], Palak Gambhir[2], Shefali Sinha[3], Saksham Kumar Singh[4]
[1, 2, 3, 4] *Jagan Institute of Management Studies, Sec-5, Rohini, Delhi-110085*

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 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].

©IJRASET: All Rights are Reserved

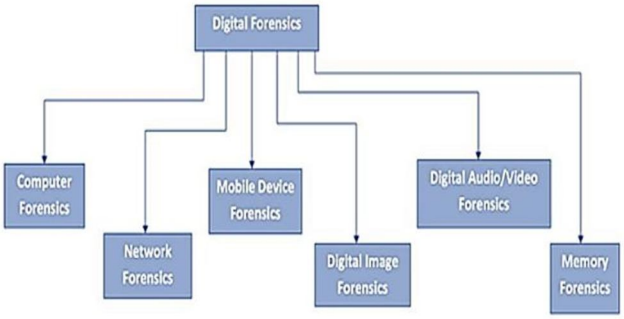


Fig. 1. Types of Digital forensics

Digital forensics is an ever-evolving science with many sub-disciplines. Some of these subdomains are:

1) *Network Forensics:* Digital forensics includes observing computer organizations and examining traffic to assemble data, proof, or the beginning of cyber-attacks. Digital forensics concerning cyber-attacks includes dissecting the idea of assaults by zeroing in on the assailant's action.[4]
2) *Database Forensics:* Database forensics is concerned with the forensic investigation of databases and the data they store. Usually, computer forensics examiners investigate databases to see who got to the database and what moves were made during a particular time to decide on actions or exchanges. Questionable interpretation. They can recuperate erased data.
3) *Remote Forensics:* Wi-fi networks are worthwhile passage focuses for programmers. Remote forensics manages the assortment of data sent over remote organizations through remote switches, remote passages, wi-fi switches, and other wi-fi transmissions. Computer forensics experts frequently filter remote organizations to distinguish malevolent or unapproved gadgets, malware, interruptions, or contaminated gadgets.
4) *Disk Forensics:* Drive creation is the most common way of separating data from capacity media like hard drives, pen drives, memory cards, and so on. Computer forensics experts utilize their insight and experience supplemented with forensic apparatuses, innovation, and methods to recuperate data from gadgets, even in basic circumstances. Genuinely or intelligently harmed.[5]
5) *Cloud Forensics:* Cloud forensics is the use of forensic examination standards and techniques in a cloud climate. This frequently gets very confounded as the data can be spread across a few cloud servers, which thusly can be situated in various actual areas and, surprisingly, in various nations. While carrying out digital forensic examinations on such a conveyed dataset can be tested, experienced computer forensic specialists possess the ability to handle the errands.
6) *Mobile Forensics:* Mobile forensics includes inspecting and dissecting cell phones to recuperate put away data, for example, contacts, logs, instant messages, sound and video records, messages, perusing data, area data, web-based entertainment messages, and that's just the beginning. Time as gadgets become refined handheld gadgets with expanding usefulness and data stockpiling limits.[4]
7) *Email Forensics:* Email forensics manages to recuperate and investigate the source and content of messages, including erased messages, schedule sections, and contacts, and that's just the beginning. Computer forensics examiners regularly dissect email headers, server logs, email sources, and email connections, from there, the sky is the limit. To examine email-related violations.
8) *Desktop Forensics:* Computer forensics is concerned with the assortment, protection, examination, and show of proof tracked down on computers and related stockpiling gadgets. Computer forensics specialists completely inspect the items away from gadgets, hard drives, messages, archives, and different documents. They likewise dive into metadata and furthermore remove stowed-away or erased data.[5]

II. 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.

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. FORENSIC ANALYSIS TOOLS

A. 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.[11] 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.

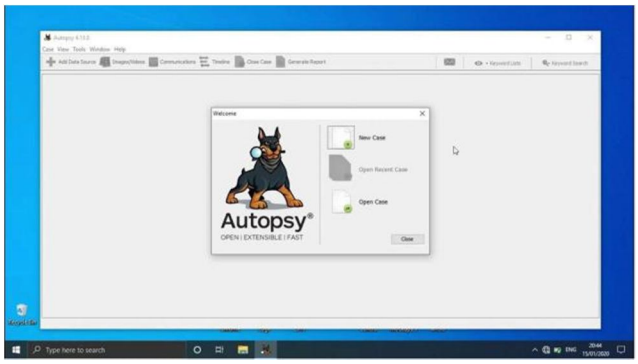


Fig. 2. Autopsy Forensic Tool 3.1.1 Features of Autopsy:

1) Timeline Analysis: helps in identifying activity by displaying framework events in a graphical connection point.
2) Registry Analysis: utilizes RegRipper to differentiate recently accessed archives and USB devices.
3) Keyword Search: Using text extraction and record-checking modules, users may uncover records that include certain phrases and discover common articulation patterns.[11]
4) Email Analysis: Like Thunderbird, email analysis can also parse MBOX design messages.
5) Web Artifacts: helps to identify client action by extracting web action from regular applications.
6) LNK file analysis finds other approaches and helps to report them.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. OSForensics

OSForensics 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.[12,13] 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 3.2.1 Features of OSForensics Tool:

1) *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.
2) *Determine Suspicious Behavior and Files:* It compares and synchronizes records using the md5, SHA-1, and SHA-256 hashes. One can create drive markings and contrast them with distinctive contrasts.[11] Document watcher that can show streams, hex, text, pictures, and metadata. Email watcher that can show messages straightforwardly from the chronicle. Peruse web programs and catch online substances for disconnected proof administration. To identify the time and frequency of uses that have been active on the system, and therefore recorded by the OS's preference.
3) *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.[12] 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.

C. 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.[11,13] 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.

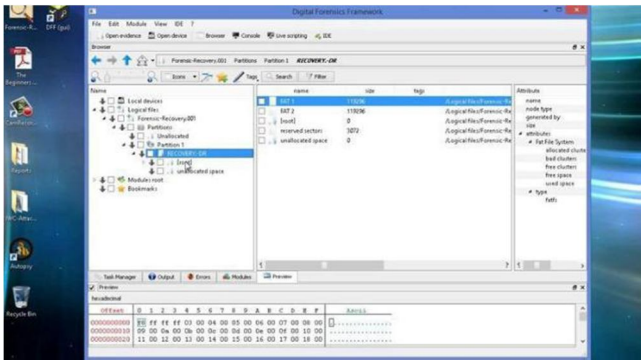


Fig. 4. DFF Forensic Tool

D. 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.

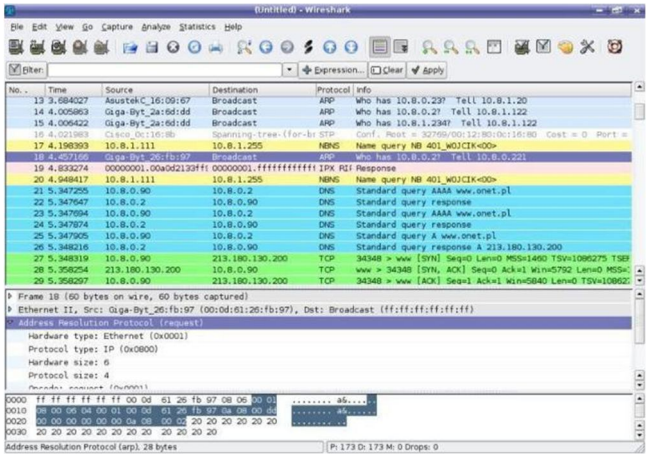


Fig. 5. Wireshark Tool

E. 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.[11] To prevent unauthorized access to legitimate data, it employs document encoding and package encryption.

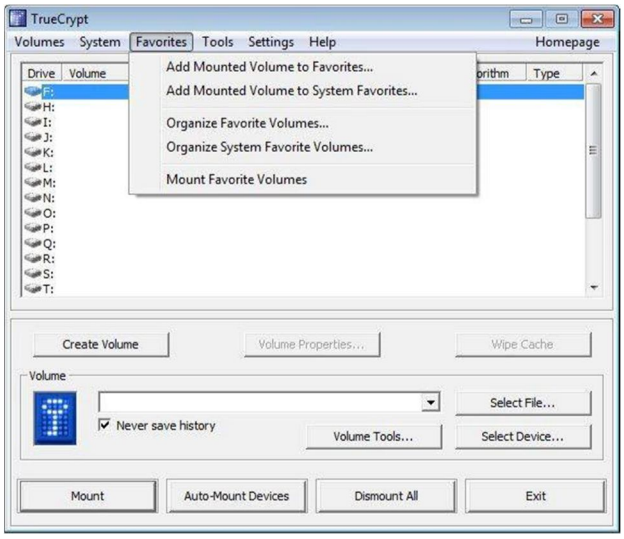


Fig. 6. TrueCrypt Forensic Tool

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. [14] 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.

IV. COMPARATIVE ANALYSIS RESULTS

	Parameter										
Tools	Digital foren-sic type	Tools avail-ability	Imaging	Hashing	Acquire	Recovery	Seizer	Ram Dump -ing	Live log	Live analy -sis	logs
Autopsy	Deskto p	Trial	✓	-	-	✓	✓	✓	-	-	-
OSF mount	Live	Trial	✓	-	✓	-	✓	✓	✓	✓	✓

Fig. 7. Comparative Analysis Results

V. 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.[12]

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.".[13] 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.".[13] 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".[14]

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 (for example bogus email headers, changing record expansions). In this manner now and again the examiner could miss a few data that have forensic worth.

G. Resource Challenges

Depending on the circumstances, the amount of data involved in the case may be huge. In order to spread messages amongst attackers, an organisation convention is frequently chosen and its header modified. This technique makes use of the fact that a few header fields are altered during transmission.[13] Attackers use these secrets to maintain a covert connection between themselves and the compromised system. It is harder to identify.

Likewise, the examiner must review each piece of information that was acquired in order to compile evidence. For the test, a bigger expenditure could be necessary. Time is a constraining factor; thus, it becomes yet another challenging test in the realm of digital forensics. Client exercises are rewritten in the volatile memory in unexpected memory forensics because the data stored in the volatile memory is vaporous. In this way, agents are able to dissect only late material that has been stored in unexpected memory. This minimizes the data's value as evidence in the investigation.[15]

An examiner should make sure that no information is changed or overlooked throughout the examination when collecting data from the source, and the information should be thoroughly obtained.

Data sources that are harmed won't be quickly utilized in examinations. So, it is a significant issue when an examiner finds an important source that isn't usable.

VI. 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.

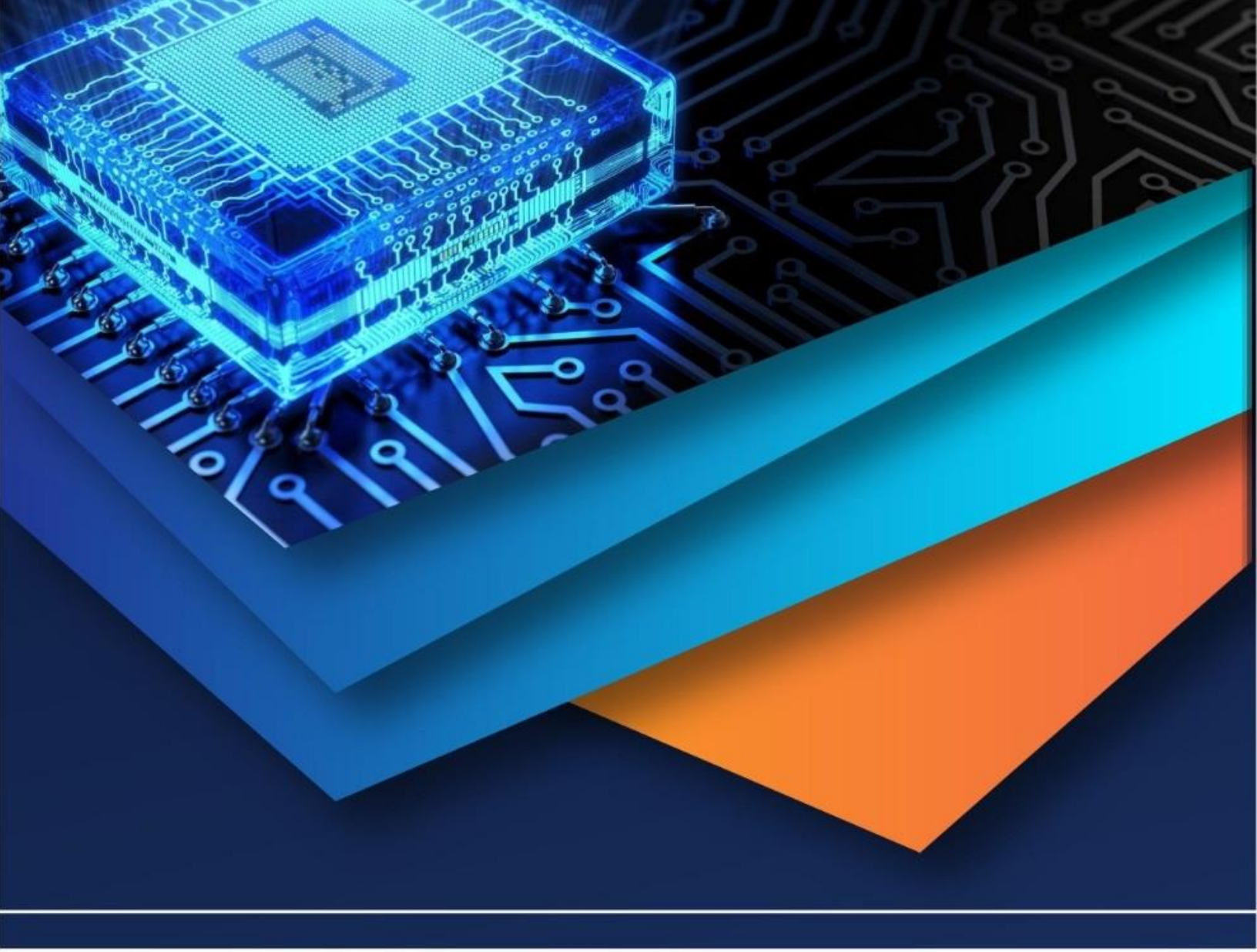
The data structure that is located in memory may also be used to get digital proof using a variety of devices. The new cycle model is chosen to quickly acquire urgent proof and investigate the situation. The stepwise forensic process model demonstrates an in-situ method that provides occurrence- recognizable 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.

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.
[11] Al-Dhaqm et al., "Digital Forensics Subdomains: The State of the Art and Future Directions," in IEEE Access, vol. 9, pp. 152476-152502, 2021, doi: 10.1109/ACCESS.2021.3124262
[12] Y. Adam and C. Varol, "Intelligence in Digital Forensics Process," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-6, doi: 10.1109/ISDFS49300.2020.9116442
[13] V. Fernando, "Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges," 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2021, pp. 1-7, doi: 10.1109/NTMS49979.2021.9432641
[14] P. Bahadur and D. S. Yadav, "Computer forensics-digitized science," 2015 SAI Intelligent Systems Conference (IntelliSys), 2015, pp. 1025-1031, doi: 10.1109/Intel-liSys.2015.7361269

[15] R. Poisel and S. Tjoa, "A Comprehensive Literature Review of File Carving," 2013 International Conference on Availability, Reliability and Security, 2013, pp. 475-484, doi: 10.1109/ARES.2013.62.
[16] Bhatia, M., Muttoo, S. K., & Bhatia, M. P. S. (2011). Secure group communication protocol. Int J Adv Eng Sci Technol, 11(1), 221-225.
[17] Bhatia, M., Muttoo, S. K., & Bhatia, M. P. S. (2013). Secure Requirement Prioritized Grid Scheduling Model. Int. J. Netw. Secur., 15(6), 478-483.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)