ISSN NO: 2770-4491
Date of Publication:10-04-2023

Static and Live Digital Forensics, along with practical examples of tools used for each approach.

Nurbek Nasrullayev
Nurafshon Branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent region, Uzbekistan
Homidov Qudratillo Hamza ugli
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
Tuyboyov Oybek Valijonovich
Associate professor of the department of Mechanical Engineering,
Tashkent State Technical University, Tashkent, Uzbekistan
Djurayev Musurmon Avlakulovich
Associate professor of the department of Mechanical Engineering,
Tashkent State Technical University, Tashkent, Uzbekistan

Abstract: The field of digital forensics involves examining and analyzing data, with computers being a primary means of communication that investigators can use to gather relevant information. Forensic analysis can be conducted in either a static or live mode. While the traditional static approach may provide incomplete evidence, live analysis tools offer a more precise and consistent view of current and previous processes. Certain critical system-related data stored in volatile memory cannot be effectively retrieved with static analysis techniques. This paper provides a brief overview of both static and live analysis methods and outlines various tools and techniques utilized in digital forensic analysis.

Keywords: Cybersecurity, Digital Forensics, Static Forensic, Live Forensic, Memory Forensic.

I. Introduction

In recent decades, there has been a significant shift in people's technology preferences, with many adopting modern technologies. Digital media such as PCs, PDAs, laptops, mobiles, and other devices are frequently used for communication. The internet has become a primary means of communication, but it also presents risks of cyber and malware attacks, leading to damage such as data theft and malicious system activities [1-5]. Those responsible for detecting and preventing such attacks must update their skills and procedures to minimize their impact.

Crimes committed with the use of computers can range from the illegal transfer or download of digital files, such as illegal weapons plans or child pornography, to the unauthorized downloading of copyrighted music. Such crimes can also involve fraud or theft related to branded computer hardware, valuable software, applications, or other intellectual property [6-9]. Digital forensics experts investigate the defendant's computer files to determine the source of pirated or illegal files, software, or applications.

Cell phones hold personal information, and digital forensics experts can retrieve vital data related to a person's contacts and communications by examining their digital cell phone records, along with telephone billing records and other digital data sources such as ATM and credit card records.

Digital forensics pertains to data files, software, computer operations, and electronic files stored on other technology-based storage devices such as PDAs, digital cameras, and mobile phones. The aim of forensic science is to utilize digital evidence to recreate and identify suspects, analyze or diagnose victim machines, and investigate criminal or civil court evidence. In computer forensics, experts use techniques and investigation methods to preserve evidence and gather data from computing devices. The primary objective is to conduct an organized investigation while maintaining evidence integrity to determine what occurred on the computing devices and who is responsible. Digital forensic analysis comprises various processes such as data acquisition, analysis, and evidentiary presentation of data. It is commonly performed in live and static modes. In the traditional static approach, the system is analyzed forensically after taking a memory dump and

ISSN NO: 2770-4491
Date of Publication:10-04-2023

shutting down the system. In contrast, live digital forensic analysis involves gathering, analyzing, and presenting evidentiary data using different forensic tools while the victim system remains running. The aim of this paper is to discuss the different techniques utilized in both live and static digital analysis.

II. Analysis Methods with Tools

Static Analysis. In traditional digital forensics, the focus is on examining a duplicate or copy of a disk to extract the memory contents, such as deleted files, web browsing history, file fragments, network connections, opened files, and user login history. This process generates a timeline that provides a partial or summary static view of the activities performed on the victim system before it was shut down. In static analysis, various software and hardware tools, such as Fundl and RegCon, are utilized for memory dumping and sorting of evidentiary data for analysis and presentation purposes. Forensic data is collected using different external devices, including USBs, external hard drives, CDs, and DVDs, and then brought into the forensic lab for investigators to perform various operations or steps to forensically analyze the evidentiary data.

Table 1. Tools for Static analysis

No	Tool Name	Description	Operation system
1.	Registry Recon	The purpose of this tool is to reconstruct the Windows registries from any location on a hard drive and then parse them for thorough analysis.	Windows
2.	EnCase	In static digital forensic investigation mode, this tool is utilized to collect and examine memory dumps.	Windows
3.	FTK (Forensic Toolkit)	This tool is utilized to conduct digital analysis and organize the evidential data in an indexed format.	Windows
4.	SafeBack	This tool is utilized to collect and analyze evidence, as well as create a backup of digital evidentiary data.	Windows
5.	HashKeeper	A software application utilized for the storage of signatures of file hashes in a database.	Windows

Live Analysis. The field of live forensic analysis presents new challenges such as non-interactive analysis and data snapshots. To address these challenges, new data models and user interface designs are needed.

In live digital forensics, information is collected, analyzed, and reported while the compromised system remains operational. The tools used for live digital forensic analysis can provide a clearer view of information such as memory dumps, running processes, open network connections, and unencrypted versions of encrypted files. These types of memory contents cannot be properly obtained through static analysis. Live analysis ensures consistency and integrity of forensic data. The information gathered through live analysis can be used to produce forensic evidence or to illustrate the activities and actions performed by the user, either directly or via remote login on the compromised system.

Table 2. Tools for Live analysis

No	Tool Name	Description	Operation system
1.	SIFT (SANS Investigative Forensics Toolkit)	SIFT is utilized to conduct digital forensic investigations across various operating systems.	Ubuntu
2.	EPRB (Elcomsoft Password Recovery Bundle)	This set of tools is employed for conducting digital analysis on systems that are encrypted, as well as for recovering passwords and decrypting data.	Windows

ISSN NO: 2770-4491
Date of Publication:10-04-2023

3.	The Sleuth Kit	The toolkit offers both graphical user interface (GUI) and command line interface (CLI) options for conducting digital forensic analysis on both Unix and Windows systems.	Unix/Windows
4.	COFEE (Computer online forensic evidence extractor)	COFEE is utilized for live extraction and analysis of forensic data.	Windows
5.	OCFA (Open Computer Forensics Architecture)	This is a tool that utilizes a command line interface to conduct distributed computer forensics and analyze digital media. It is commonly employed in digital forensic laboratories.	Linux
6.	OS Forensics	This software is utilized to conduct examinations on various types of digital data, including email, files, images, and web browsers.	Windows
7.	Forensic Assistant	This tool is utilized to examine the actions executed by a user on the internet, such as sending and receiving emails, working on documents and instant messaging, as well as browsing the web.	Windows
8.	bulk extractor	This tool is utilized to retrieve phone numbers, email addresses, URLs, and other identified objects.	Windows, Linux
9.	IRCR (Incident Response Collection Report)	This tool gathers real-time forensic information from various sources such as command history, computer, network connections, active processes, open ports, registry startup records, and system event logs.	Windows
10.	Intella	This tool is utilized for the examination and investigation of digital data, cell phones, and emails.	Windows
11.	CMAT(Compile Memory Analysis Tool)	This tool retrieves data from memory dumps and also identifies malware.	Windows
12.	WFT (Window Forensic Toolkit)	This toolkit is utilized for conducting digital forensic analysis on memory, system data, file and directory timestamps, user information, current processes, port numbers, and network configurations.	Windows

Live vs Static Analysis. Static analysis is a conventional method of digital forensics in which investigators analyze data that is at rest, such as the contents of a hard drive. This involves shutting down the computer systems to prevent any further damage to the data. However, in recent years, there has been a growing emphasis on live system analysis due to the fact that many recent attacks do not leave any evidence on the hard drive but only in the computer's memory. Additionally, the increasing use of cryptographic storage and keys makes it necessary to study the information while the system is still running to prevent the loss of information. This paper discusses both live and static forensic techniques and how they work together with traditional methods to meet forensic requirements. It covers the various types of information that can be collected and how evidence can be analyzed from a live machine, as well as the techniques used for static disk analysis.

Table 3. Tools for both(Static/Live) analysis

No	Tool Name	Description	Operation system
1.	Digital Forensics Framework	DFF is employed as both a digital investigation tool and a development platform for both live and static analysis.	Windows/ Linux/ Mac OS

ISSN NO: 2770-4491
Date of Publication:10-04-2023

2.	PTK Forensics (Programmers Toolkit)	This framework has a graphical user interface (GUI) and is used for both static and live analysis.	LAMP
3.	The Coroner's Toolkit	This is a command-based tool for conducting forensic analysis on Unix systems via a command-line interface.	Unix
4.	X-Way Forensics	This tool is a versatile Win Hex editor that can be used for both static and live analysis.	Windows
5.	CAINE (Computer Aided investigative environment)	This is a command line interface that can be used for both distributed and standalone computer forensics.	Linux
6.	Net Intercept	It is used to analyze transitory information	Appliance
7.	WireShark	This tool is employed to capture and analyze network packets.	Windows/Mac/Linux

III. Key Challenges And Related Works

The domain of live forensic analysis poses fresh obstacles such as non-interactive analysis and data snapshots, necessitating the creation of new data models and user interface designs. However, there is a risk that the analysis tools loaded into the RAM may also alter the memory contents, leading to erroneous analysis outcomes. This challenge can be surmounted by using appropriate tools and techniques for live digital forensic analysis. Moreover, there may be cases where analysis needs to be carried out without disrupting the system's functionality, so that the system can continue to perform its intended tasks while being analyzed digitally.

The GRR (Gradual Release of Responsibility) framework proposed by Cohen et al. [10] is a rapid response framework that aims to decrease the investigative effort required per machine. The framework progresses isolated live forensics, by engaging in auditing, secrecy issues, and accessibility. It delivers a secure and accessible platform to enable forensic analysis solutions. One of the key advantages of GRR is that it supports automated analysis for a large enterprise dataset by executing complex queries in a shorter span of time, thus enhancing the investigative capacity. This can help reduce the cost of response and improve the quality of evidence. Another advantage of GRR is that it imposes enterprise procedures as it is capable of scanning corporate digital assets instantaneously. This means that GRR can help to enforce organizational policies, procedures, and best practices related to digital forensics.

Overall, the GRR framework is a useful tool for digital forensics investigations in large organizations. By providing a secure and accessible platform for forensic analysis, GRR can help to reduce the investigative effort required per machine, enhance the investigative capacity, and improve the quality of evidence obtained.

Mrdovic et al. [11] suggest that live analysis of a running system can be useful in obtaining volatile data to understand events that occurred in the past. The advantage of analyzing a live system is that the system state cannot be changed or reversed, making the collected evidence valid. Additionally, volatile memory dumps can be used for offline analysis of live data. The virtual machine created using static data from the memory dump can provide a good picture of the live system when the dump was taken. The investigator can then conduct interactive sessions without violating the integrity of the evidence. This combination of live digital forensics and static analysis offers new possibilities in the virtual environment. When conducting live analysis, it is important to hibernate the system before carrying out any examination. This is the best way to save the volatile memory and system state, and it does not require any changes or additions to the system state. Once the system is hibernated, a secondary storage image is created and can be used for analysis.

Overall, live analysis can be a useful technique in digital forensics investigations, especially when combined with static analysis. By obtaining volatile data from a running system and creating a virtual machine using static data, investigators can gain a better understanding of events that occurred in the past without violating the integrity of the evidence.

Hay et al. [12] discuss the approaches, techniques, and tools of live analysis in both virtual and real environments. As computer technologies become more prevalent, supporting digital forensics tools and techniques become increasingly important for efficiently analyzing related system behavior. To investigate the challenges and progress in live analysis, it is necessary to understand the traditional approach to digital forensics, which involves halting the system and creating a valid copy of the data for analysis of the storage media. Static tools are used to search the storage media for discovering digital evidence. However, static analysis results in an incomplete picture of the event, with limiting factors including process shutdown, encrypted data, and absence of memory content details. In contrast, live analysis collects data from the running system and deals with many of the inadequacies of static analysis. There are many ways to perform live analysis on physical machines, including the use of imported utilities, standard user interface, and modified system. In the case of virtual machines, techniques include interactive logging/replay and live analysis. Each technique has its own advantages and disadvantages, which can contribute to the evolution of live analysis.

Overall, live analysis can be a powerful technique for digital forensics investigations, providing a more complete picture of the event than static analysis alone. As technology continues to advance, it is important for digital forensics tools and techniques to keep pace and adapt to new environments and challenges.

Wang et al. [13] present a computer live forensics model based on physical memory analysis, which can effectively address many challenges faced by live forensics investigations. The authors discuss several issues related to the credibility of live forensics, including the calculation of possible credibility based on the model of memory analysis. This enables validation of the live analysis and minimizes the impact on collected evidence. The outcomes of live forensics on the evidence include the chance of covering key traces by the forensic toolkit and the affected region in digital evidence. Additionally, the model addresses authenticity, integrity, verifying consistency rules, repeatability, applicability, and fault tolerance. By using this model, investigators can effectively analyze digital evidence and maintain the credibility of the analysis. This can be especially important in cases where the evidence collected can impact legal proceedings. The authors' approach helps to ensure that the evidence is valid and reliable, which can be critical to the outcome of the investigation.

Casey et al. [14] discuss how full disk encryption (FDE) can significantly impede digital investigations by preventing access to all digital evidence. When dealing with volume encryption or FDE, simply quitting the use of the evidential system is not a satisfactory technique as all the data on the device becomes inaccessible for forensic examination. To address these challenges, there is a need for more effective competencies to identify and preserve encryption before unplugging the device. Additionally, prosecutors need to prepare search warrants that provide digital investigators with the best opportunity to obtain decrypted data in the field.

FDE has disadvantaged earlier investigations, but there are directions for assembling items at the scene of the crime that might be useful for dealing with encrypted data, as well as performing crime scene forensic acquisitions of live digital forensic systems. These procedures increase the chances of obtaining digital evidence in an unencrypted state or detaining a passphrase or encryption key. To deal with FDE, there are some applicants for drafting and performing search warrants. These warrants can be critical for obtaining access to encrypted data and enabling digital investigators to effectively analyze it.

Cybercrime is a growing concern in our society, and it is crucial to have effective prevention methods and technologies in place to address it. With the advancement of technology, cyber criminals are becoming more sophisticated and finding new ways to exploit vulnerabilities in computer systems and networks. As a result, cybersecurity professionals are continuously developing new techniques and tools to protect against these threats [15-18]. Artificial intelligence (AI) is one of the emerging technologies that can be used to enhance cybersecurity. AI can be used to analyze large amounts of data in real-time and identify potential threats. Machine learning algorithms can also be used to learn from previous attacks and detect new patterns of behavior that may indicate an attack is underway. Additionally, AI can be used to automate security tasks, such as monitoring network traffic and responding to potential threats.

Overall, the integration of AI in cybersecurity can provide faster and more accurate detection and response to cyber threats, which is essential in today's digital landscape.

IV. Conclusion

During the data acquisition phase of static and live digital analysis, it is important to ensure that the memory contents are accurate to obtain reliable results. However, it is common for forensic tools used in both static and live analysis to overwrite the data structure of running processes, resulting in inconsistencies in the evidence. Therefore, it is necessary to adopt effective methodologies and appropriate tools to detect attacks easily and minimize alterations in memory contents. This study provides a concise examination of the tools and techniques utilized in both live and static digital forensic analysis.

Reference

1. Rajaboevich, G. S., Baxtiyarovich, N. N., & Salimovna, F. D. (2020, November). Methods and intelligent mechanisms for constructing cyberattack detection components on distance-learning systems. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.
2. Bakhodir, Y., Nurbek, N., & Odiljon, Z. (2019). Methods for applying of scheme of packet filtering rules. International Journal of Innovative Technology and Exploring Engineering, 8(11), 1014-1019.
3. Gulomov, S. R., & Bakhtiyorovich, N. N. (2016, November). Method for security monitoring and special filtering traffic mode in info communication systems. In 2016 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.
4. Malikovich, K. M., Rajaboevich, G. S., & Karamatovich, Y. B. (2019, November). Method of constucting packet filtering rules. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
5. Насруллаев, Н. Б., & Файзиева, Д. С. (2020). Анализ средств службы информационной безопасности в дистанционном обучении. Молодой ученый, (31), 14-18.
6. Baxtiyorovich, N. N., & Ubaydullaevna, H. I. (2019, November). Method of analyzing of antivirus errors when audit provides. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-3). IEEE.
7. Komil, T., & Nurbek, N. (2015). Development method of code detection system on based racewalk algorithm on platform FPGA. In Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE) (p. 278). International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE).
8. Safoev, N., & Nasrullaev, N. (2021, November). Low area QCA Demultiplexer Design. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 01-05). IEEE.
9. Yakubdjanovna, I. D., Bakhtiyarovich, N. N., & lqbol Ubaydullayevna, X. (2020, November). Implementation of intercorporate correlation of information security messages and audits. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
10. Cohen, M. I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the enterprise. digital investigation, 8, S101-S110.
11. Mrdovic, S., Huseinovic, A., & Zajko, E. (2009, October). Combining static and live digital forensic analysis in virtual environment. In 2009 XXII International Symposium on Information, Communication and Automation Technologies (pp. 1-6). IEEE.
12. Hay, B., Bishop, M., & Nance, K. (2009). Live analysis: Progress and challenges. IEEE Security & Privacy, 7(2), 30-37.
13. Wang, L., Zhang, R., & Zhang, S. (2009, December). A model of computer live forensics based on physical memory analysis. In 2009 First International Conference on Information Science and Engineering (pp. 4647-4649). IEEE.
14. Alazab, M., Venkatraman, S., & Watters, P. (2009, June). Digital forensic techniques for static analysis of NTFS images. In Proceedings of ICIT2009, Fourth International Conference on Information Technology, IEEE Xplore.

15. Sherzod Rajaboevich, G., Dilmurod Gulamovich, A., & Nurbek Bakhtiyorovich, N. (2019). Method for determination of the probabilities of functioning states of information of protection on cloud computing. International Journal of Mechanical Engineering and Technology, 10(3).
16. Shakarov, M., Safoev, N., & Nasrullaev, N. (2022). Обеспечение безопасности интернет вещей в промышленности 4.0 с использованием WAF. Research and Education, 1(9), 386-393.
17. Насруллаев, Н., Муминова, С., Сейдуллаев, М., & Сафоев, Н. (2022). Внедрение DMZ для повышения сетевой безопасности веб-тестирования. *Scientific Collection «InterConf»*, (110), 641-649.
18. Rajaboevich, G. S., Baxtiyorovich, N. N., & Komilovich, T. S. (2021, November). A model for preventing malicious traffic in DNS servers using machine learning. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.