International Journal of Safety and Security Engineering
Vol. 14, No. 1, February, 2024, pp. 217-223
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Cybersecurity Through Live Forensic Investigation of Remote Access Trojan Attacks using FTK Imager Software

Ritzkal[1*], Ade H. Hendrawan[1], Ridwan Kurniawan[1], Alief J. Aprian[1], Dewi Primasari[1], M. Subchan[2]

[1] Informatics Engineering, Universitas Ibn Khaldun, Kota Bogor 16162, Indonesia
[2] Information System, Universitas Muhammadiyah Banten, Banten 15720, Indonesia

Corresponding Author Email: ritzkal@ft.uika-bogor.ac.id

https://doi.org/10.18280/ijsse.140121

Received: 4 January 2024
Revised: 30 January 2024
Accepted: 3 February 2024
Available online: 29 February 2024

Keywords:
malware analysis, digital forensics, kali Linux, information systems security, Metasploit framework, keylogging, remote access trojan, penetration testing

ABSTRACT

This study discusses using FTK Imager software for live forensic investigations in order to track and analyze Remote Access Trojan assaults. In addition to helping organizations safeguard their assets and data against harmful cyberattacks, our research aims to improve computer system security. The knowledge of the presence of the Remote Access Trojan virus, notwithstanding its removal, is the advantage of this research. Installation of Kali Linux, forensic analysis using FTK Imager, and the development and usage of viruses are all part of this study methodology. The process included installing Kali Linux as a platform for the creation and execution of viruses, identifying and analyzing the presence of viruses using FTK Imager, and identifying and analyzing Remote Access Trojan attacks using disk and memory forensic analysis techniques. The research findings indicate that as soon as the target opens the generated virus, the executor gains complete access to the target machine. This allows the executor to follow the target around and record everything it does. As a forensic investigation tool, FTK Imager must be installed on the target in order to detect the virus that the executor developed. The target will thus find it simpler to use memory forensics or disk forensics to look for files created by the executor. describes how to use FTK Imager software to observe and analyze Remote Access Trojan assaults for use in real-world forensic investigations.

1. INTRODUCTION

As per Kelrey and Muzaki's publication, the National Cyber and Crypto Agency (BSSN) of Indonesia saw a 300% surge in cyberattacks via Remote Access Techniques (RAT) in 2022 as compared to the preceding year. In Indonesia, there were 5,874 recorded RAT attacks in 2022 [1]. In the current digital era, data and computer system security has become increasingly important. The increase of cyberattacks, such as Remote Access Trojan (RAT) assaults, highlights how crucial it is to safeguard important systems and data [2, 3]. An attacker can remotely access and take control of a computer or network without the owner's knowledge thanks to a kind of malicious software called a Remote Access Trojan (RAT) [4, 5].

A Remote Access Trojan, or RAT, is essentially a software entity that seeks to remotely take over complete control of an infected system in order to accomplish goals relating to system penetration, unlawful monitoring, and data theft. The benefit that the executor will have from being aware of the victim's actions when the target opens the virus might be the driving force behind RAT assaults in this investigation. such is when the intended recipient inputs their account and password [6, 7]. They are frequently employed in a range of cyberattack scenarios, including as information gathering, system assaults, manipulation, surveillance, and taking advantage of security flaws that are already in place. These factors make RAT attack detection and analysis essential to preserving system and data security [8-10].

Live forensic investigation is one method for the investigation, prevention, and identification of cyber threats in real time [11]. In this context, "live forensic investigation" refers to a technique that allows for the instant acquisition of digital evidence from an operating system without interfering with its operation. This enables security experts to instantly detect current assaults and take appropriate action. For instance, the FTK imager's disk forensic and memory forensic analysis tools were used in this study to examine the existence of Remote Access Trojan infections. Memory forensics records the data that disk forensics analyzes, and the two disciplines work together continuously. The RAT infection will continue to be recognized even if data is erased by the system or destroyed [12, 13].

FTK Imager is one of the forensic tools that security professionals use to gather and analyze digital evidence [14]. The application is capable of taking and analyzing live screenshots of the operating system. This makes it possible for security professionals to check into dubious activity and search for signs of trojan assaults using remote access or other unlawful activity. The goal of this study is to learn more about the use of live forensic investigation, and the primary tool for monitoring and evaluating Remote Access Trojan assaults is the FTK Imager software. Therefore, by bettering computer

system security, this research will help businesses better safeguard their assets and data against malevolent cyberattacks.

It may be expressed as follows in light of these issues: How is it possible for a Remote Access Trojan to be made in order to target computer users? Even after the virus has been erased or eliminated by the computer, how can I find evidence of its existence?

One way to get around the aforementioned issues is to learn how to make a Remote Access Trojan by using Linux times version 2022.4, from conception to implementation, and how to use the FTK Imager application as a digital forensic tool to locate evidence of hacking activities. The purpose of this study is merely to identify the presence of the Remote Access Trojan virus, even in cases when the infection has been either manually or automatically eliminated by the system.

2. RESEARCH METHODS

The four steps of this research include preparation, planning, implementation, and outcomes, as shown in Figure 1.

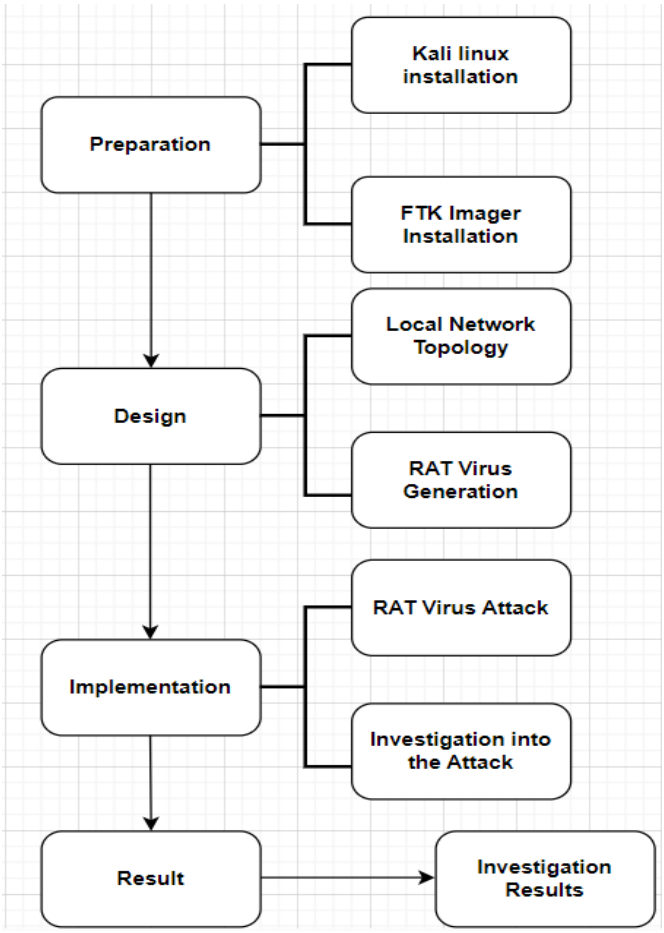

Figure 1. Research methods

a). Preparation

(1) Kali Linux installation

To develop and execute the virus, the first step is to install Kali Linux on a virtual machine. The installation of Kali Linux as a platform for virus creation and execution, along with the use of FTK Imager to discover the presence of the virus, are the preparatory steps for this research.

(2) FTK imager installation

The FTK Imager program is then installed to facilitate hands-on forensic investigation techniques. The purpose of this FTK Imager program is to detect the type of malware targeting the target machine when a virus is executed on it [15].

b). Design

(1) Local network topology

When creating the network topology, the goal is to monitor the target's behavior when connected to a local area network that has a malware execution device. Utilizing FTK imager software to conduct live forensic investigations and monitor and evaluate Remote Access Trojan attacks during the design, network topology, and system, design phases.

(2) RAT virus generation

It uses virtual machines to produce viruses, and the development of malicious software uses a Remote Access Trojan type of attack that attempts to test computer systems for vulnerabilities [16, 17].

c). Implementation

(1) RAT virus attack

Conducted penetration tests for the Remote Access Trojan virus by using file sharing functions to distribute it and offering victims the lure of downloading and running malware files that have embedded images.

(2) Investigation into the attack

The next step in the investigation process is to determine what type of malware infected the target machine after the target ran the infection [18, 19].

2.1 Result investigation

The result stage is the last stage. Findings drawn from the steps of developing the Remote Access Trojan virus, delivering it to the target, and identifying the type of attack fall under this stage. In particular, this step offers a thorough explanation of the efficacy of the virus as well as the analysis process to find the infection on the computer by using the FTK Imager program.

3. RESULT

a). Preparation

According to the study methodology presented, the use of FTK Imager software for live forensic investigation to monitor and analyze Remote Access Trojan attacks will take place in four stages: planning, designing, implementing, and analyzing the findings. Installation of Kali Linux as a platform for the creation of a Remote Access Trojan virus illustrated in Figure 2 below will be the outcome addressed.

Based on Figure 2, many of the IT and security solutions available on Kali Linux may seem complicated to the average user. A large number of its capabilities are aimed primarily at network research and security testing. Many cutting-edge technologies for network security, hacking, and penetration testing are available in Kali Linux. Its strength in the field of IT security is demonstrated by this [20].

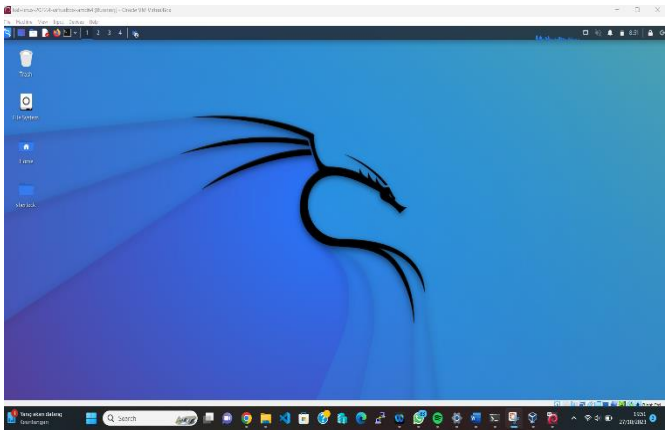

Figure 2. Kali Linux desktop

In Figure 3, cybercrime investigators often use this method to collect digital evidence from a device. Professionals in the field of digital forensics use it extensively due to its dependability and investigative skills. FTK Imager is helpful in various digital investigation scenarios due to its capabilities, which include file viewing, metadata viewing, and file searching. Even for forensic novices, FTK Imager's user-friendly graphical user interface makes the process of viewing digital evidence simple [21].

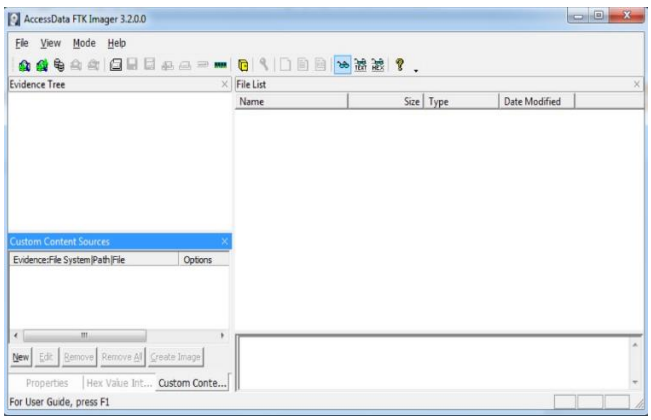

Figure 3. FTK imager

b). Design

Before attacking the target machine, the executor must understand the network path that he follows in order to develop a Remote Access Trojan virus. This may be done by installing Linux several times and using FTK imager as a live forensic research tool. As seen in Figure 4, the executor will connect to the same network segment as the intended network. Communicating with the target will be simpler for the executor as a result.

In Figure 4, The logical topology describes the IP Address addressing in the network structure built by researchers in the CSN Lab, and the local network structure connected to the network center of the Ibn Khaldun University Bogor Rectorate Building, the user or laptop used for scanning is connected to the HS-NCC wireless Access Point, and the HS-NCC Access Point is connected to Swich 02 Cisco SF 100-24 port 10/100, and likewise on the PC client in the CSN Lab room is connected to Switch 03 (PC LAB CSN) Cisco SF 100-24 port 10/100, then switch 03 is connected to Switch 02 (FT CENTER).

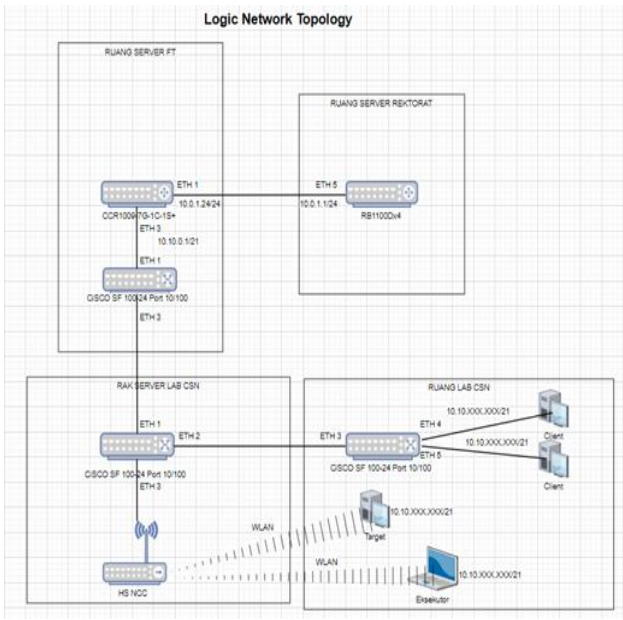

Figure 4. Logic network topology

Cisco SF 100-24 port 10/100, then switch 02 is connected to Switch (FT CENTER) Cisco SF 100-24 port 10/100 in the faculty server room and the ft center switch is connected to the CCR1009-7G-1C-1S+router with local IP 10.10.0.1/21 and dhcp server for IP addressing on the CSN Lab network with dhcp server 10.10.XXX.XXX/21. Then from the CCR1009-7G-1C-1S+router on interface 01 with IP 10.0.1.24/24 connected to the RB1100Dx4 router in the rectorate server room with IP 10.0.1.1/24.

The msfvenom command is used to generate the reverse_tcp meterpreter payload for windows 64 bit in executable format and save it in the "Articles.pdf" file [22]. The command will generate a Windows executable meterpreter reverse shell which when run on the victim will connect back to IP 10.10.7.227 on port 4444 [23].

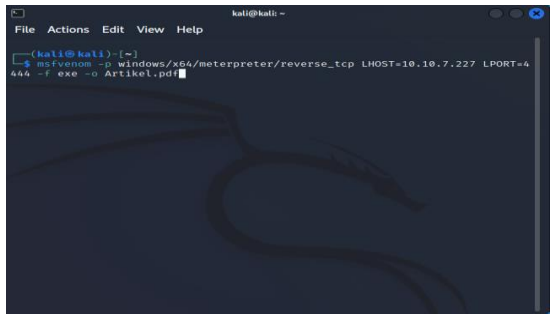

Figure 5. Virus generation

In Figure 5, To initiate the attack against the target, this step spreads the Remote Access Trojan infection [24]. The next stage is for the executor to instruct the target on how to access the prepared file, after moving the virus file by modifying the .exe extension into a PDF extension.

c). Implementation

The executor will exchange data with the target in Figure 6 below once it has created a Remote Access Trojan infection. By approaching the target with a bait, the executor can get complete access to the target machine by tricking the victim

into opening the viral file.

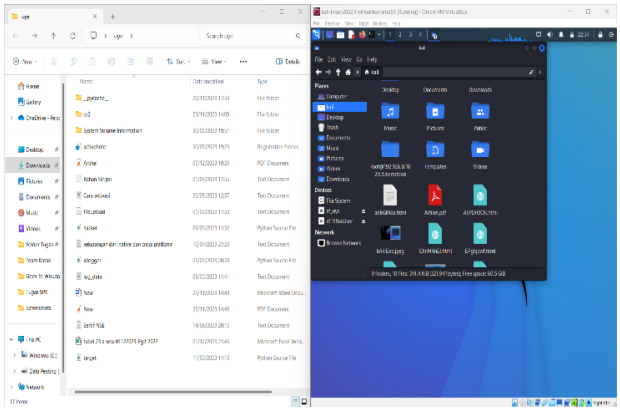

Figure 6. Virus transfer

In Figure 6, Using file sharing, the attack was conducted against Windows 11 Home Single Language version 22H2 using the Kali Linux operating system, version 2022.4. Once the target executes a malicious file with a PDF extension, the executor will have full access to the target computer and can download, delete, edit and upload files as needed. If used improperly by careless people, this may be dangerous. The executor will easily trick the target into opening the file containing the virus by simply adding the .exe extension file into the PDF.

In Figure 7, Msfconsole is the main console interface for the Metasploit Framework [25]. It allows users to interact with and execute Metasploit modules from the command console. Some of the command line functions of msfconsole are listed in Table 1.

In short, a reverse TCP payload advanced meterpreter intended for Windows x64 computers is configured with this command. The meterpreter will be installed and a reverse TCP connection will be established to the attacker when the Windows x64 target is successfully exploited [26].

In Figure 8, The executor will have full access to the files generated by the executor (virus) once the target opens the virus. To determine if the virus created by the executor is viable, the executor will use this console to perform a penetration test on the target machine. During the test run, the executor will track the actions performed by the target using Kali Linux tools. The executor will display the actions performed by the target on the website on the console when the target enters the login and password to access the uika learning website portal. so that the executor knows the target's password and login [27].

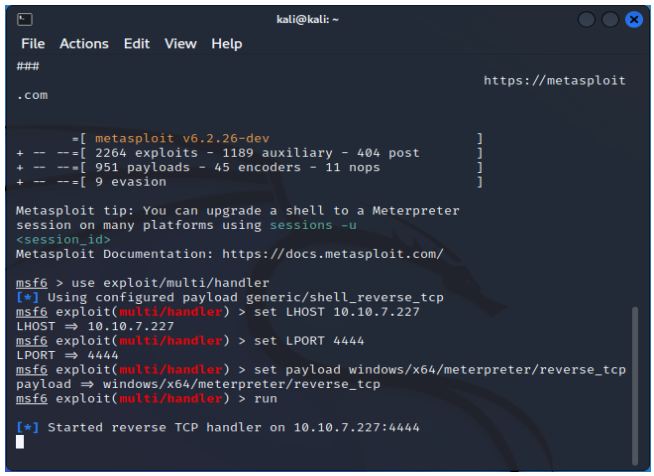

Figure 7. Use of msfconsole

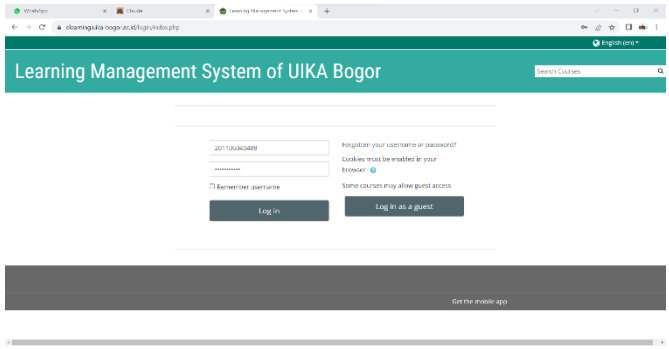

Figure 8. Target activity

Table 1. Explanation of virus startup command line

No.	Command Line	Function
1	Exploit	This specifies that we load the Metasploit exploit module. An exploit is code that takes advantage of a vulnerability or bug to execute a payload.
2	Multi	It shows a multi exploit handler, which means it can be used with any payload and supports multiple targets by default.
3	Handler	A handler is a component that "handles" the interaction and communication with the payload that has been uploaded to the target after being exploited. The handler captures connections back from the payload.
4	Set LHOST	LHOST serves to determine the IP address where the payload will connect. The value 10.10.7.227 in LHOST means that the attacker has an interface with that IP address. LHOST is the "home" or destination endpoint that will be used to listen to the reverse shell payload's reverse connection.
5	Set LPORT	LPORT defines the TCP port that will be used to listen to the reverse connection of the reverse shell payload. The value 4444 is a commonly used port, but you can also use other ports such as 80, 443, 22, etc. LPORT the destination port where the reverse shell payload listener will wait for a TCP connection from the target after the payload is executed.
6	Set payload	This is the command to configure what payload to use in the exploit.
7	Windows/x64	This section specifies the payload targeted for the Windows operating system 64-bit (x64) platform.
8	Meterpreter	This is the Metasploit meterpreter payload, which is a very feature-rich advanced payload for post-exploitation control.
9	Reverse_tcp	It specifies the meterpreter's reverse connection technique using the TCP protocol. Reverse TCP means the exploited Windows target will connect back to the attacker.

d). Result investigation

The results of the target activity will be logged in the Kali Linux operating system, as seen in Figure 9 below, after the target activity being monitored using the keyscan tool. Keyboards and other devices that are plugged into a laptop or computer are the results that are shown. A forensic assessment of the virus-affected target laptop may be carried out using the methods shown in Figures 10 and 11. This will simplify the process of determining whether the infection is present.

In Figure 9, The keyscan_start and keyscan_dump commands are useful features in the Metasploit Framework on Kali Linux that are used to perform keylogging on a target. It is important to emphasize that the usage of this keylogging approach is just for research purposes, to evaluate if a virus that has been generated and approved by the appropriate parties is suitable enough to be tracked down [28]. The command line above whose function is attached in Table 2.

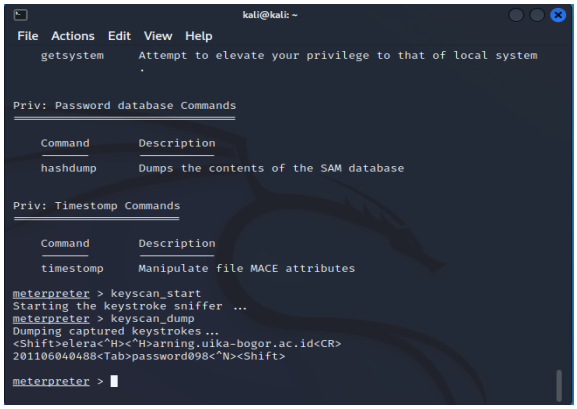

Figure 9. Virus execution

This research found that the victim's computer system had malicious software running on it during the investigation phase of the Remote Access Trojan incident. The perpetrator created malicious software that was intended to run on the intended target. Therefore, the presence of malicious software is tracked using digital forensic tools such as FTK Imager. Locating malicious software on a system can be done using two main methods.

e). Disk forensic

In Figure 10, The forensic investigation tool used in this test is FTK Imager software. By examining forensic memory and drives. The file generated by the executor can be seen in the image above thanks to the use of disk forensics techniques by FTK imager. The executor was able to reach the target machine thanks to the file. Disk forensics is a field of study that focuses on the collection, organization, and analysis of digital evidence relating to storage media, including hard drives, USB flash drives, CDs, DVDs, and more. This field is often also referred to as computer forensics or digital forensics [29].

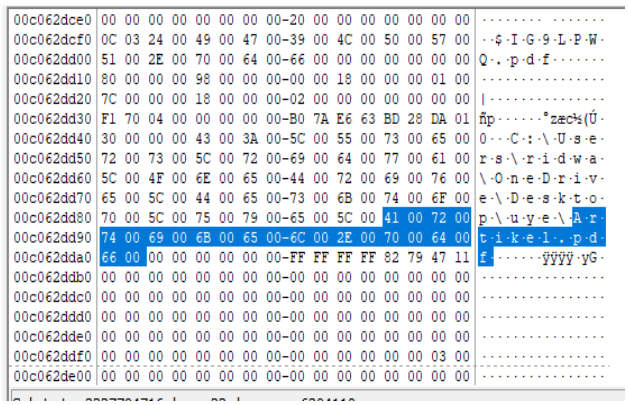

Figure 10. Hard drive storage investigation

f). Memory forensic

In Figure 11, The file generated by the executor can be seen in the image above thanks to the use of memory forensics techniques by FTK imager. After being deleted, the RAT malware file can be found in the following file: Documents \users\ridwa\OneDrive\Desktop\uye\Article.pdf. The executor was able to reach the target machine because of the file. The practice of examining the volatile memory (RAM) of a device to find digital evidence for the investigation of a cybercrime or security incident is known as memory forensic analysis [30]. The analysis must be performed while the device is still operational because volatile memory (RAM) is used to store data that is lost when it is turned off. RAM stores information about open files, open processes, network connections, and so on. Memory forensic analysis can be done for various purposes such as cyber crime investigation, malware analysis, information security incident response, digital forensics, etc. [31].

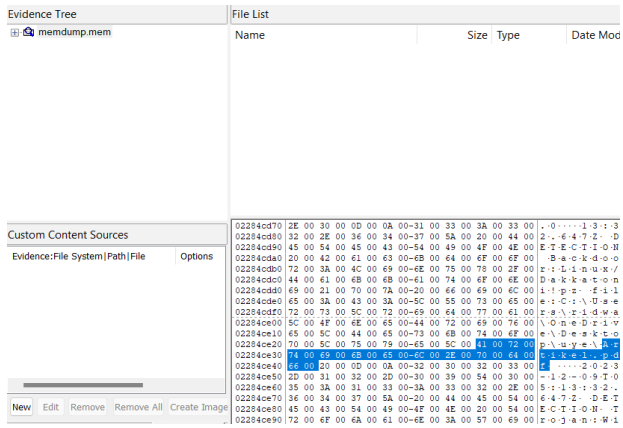

Figure 11. Memory investigation

Table 2. Explanation of virus startup command line

No.	Command Line	Function
1	Keyscan_start	The keylogging procedure on the target starts with this command. Every keystroke the target user makes on the keyboard is captured through keylogging. This command is often used after the target has been successfully compromised in the first place, either by using a Meterpreter session or an exploited reverse shell.
2	Keyscan_dump	This command is used to display or discard all keylog results that have been logged to date after the keylogging process has started. All keystrokes and keyboard inputs made by the target user-including potentially highly sensitive ones such as passwords, private communications, and proprietary information-will be displayed in the results.

4. CONCLUSIONS

The four steps of this research methodology are as follows: First, preparation, which involves the installation of FTK Imager and Kali Linux. The first step in building and executing a virus is installing Kali Linux, while the first step in starting a forensic investigation is launching FTK Imager. Next, proceed to the design stage, which includes creating a Remote Access Trojan virus and building a local network topology. Executors will find it easier to identify the path they want to target to deliver the virus if they know the local network topology. Next, perform implementation, which includes investigating and using the Remote Access Trojan virus to launch the attack. Upon transmission of the virus through file sharing, the executor tricks the victim into opening the malicious file. After that, the executor will have full access to the intended laptop or PC. Live Forensic Investigation is used to conduct an investigation of the attack to determine if the infection exists. Digital proof of RAT assaults in the.pdf extension was found in the findings of live forensics. Despite the system's deletion of the virus, FTK Imager demonstrated efficacy in identifying RAT assaults. The primary contribution of this work is a forensic investigation approach that may uncover digital evidence of remote access attacks (RATs) by employing FTK imager.

REFERENCES

[1] Kelrey, A.R., Muzaki, A. (2019). Pengaruh ethical hacking bagi keamanan data perusahaan. Cyber Security dan Forensik Digital, 2(2): 77-81. https://doi.org/10.14421/csecurity.2019.2.2.1625

[2] Nasution, M.A.H., Laksono, A.T. (2020). Investigasi serangan backdoor Remote Access Trojan (RAT) terhadap smartphone. JURIKOM (Jurnal Riset Komputer), 7(4): 505-510. http://dx.doi.org/10.30865/jurikom.v7i4.2301

[3] Aldya, A.P., Widiyasono, N., Setia, T.P. (2019). Reverse engineering untuk analisis malware Remote Access Trojan. Jurnal Edukasi dan Penelitian Informatika, 5(1): 40.

[4] Kara, İ., Aydos, M. (2019). The ghost in the system: Technical analysis of Remote Access Trojan. International Journal on Information Technologies & Security, 11(1): 73-84. https://www.researchgate.net/publication/331980804.

[5] Ardiyasa, I.W., Suwirmayanti, N.L.G.P. (2021). Analisa serangan remote exploit pada jaringan komputer dengan menggunakan metode network forensic. Explore, 11(2): 46-52.

[6] Davaslioglu, K., Sagduyu, Y.E. (2019). Trojan attacks on wireless signal classification with adversarial machine learning. In 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, USA, pp. 1-6. https://doi.org/10.1109/DySPAN.2019.8935782

[7] Tukaral, K., Sheth, R.K. (2019). Sandbox evasive Remote Access Trojan. https://www.ijraset.com

[8] Jiang, W., Wu, X., Cui, X., Liu, C. (2019). A highly efficient Remote Access Trojan detection method. International Journal of Digital Crime and Forensics (IJDCF), 11(4): 1-13. https://doi.org/10.4018/IJDCF.2019100101

[9] Aprilliansyah, D., Riadi, I. (2021). Analysis of Remote Access Trojan attack using android debug bridge. IJID International Journal on Informatics for Development, 10(2): 102-111. https://doi.org/10.14421/ijid.2021.2839

[10] Costales, R., Mao, C., Norwitz, R., Kim, B., Yang, J. (2020). Live trojan attacks on deep neural networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, pp. 796-797.

[11] Setiawan, N. (2022). Metode live forensik untuk investigasi serangan formjacking pada website ecommerce. Jurnal Sistem dan Teknologi Informasi, 7(1): 1-9. https://dspace.uii.ac.id/bitstream/handle/123456789/38731/17917120.pdf?sequence=1&isAllowed=y.

[12] Closser, D., Bou-Harb, E. (2022). A live digital forensics approach for quantum mechanical computers. Forensic Science International: Digital Investigation, 40: 301341. https://doi.org/10.1016/j.fsidi.2022.301341

[13] de Loaysa Babiano, L.F., Macfarlane, R., Davies, S.R. (2023). Evaluation of live forensic techniques, towards Salsa20-Based cryptographic ransomware mitigation. Forensic Science International: Digital Investigation, 46: 301572. https://doi.org/10.1016/j.fsidi.2023.301572

[14] Alshammari, A. (2023). Detection and investigation model for the hard disk drive attacks using FTK imager. International Journal of Advanced Computer Science and Applications, 14(7). https://doi.org/10.14569/IJACSA.2023.0140784

[15] Bhosale, N.P. (2021). Evidence recovery using EnCase and FTK in forensic computing investigation. International Journal of Scientific Research in Computer Science and Engineering, 9(4): 8-13. https://doi.org/10.26438/ijsrcse/v9i4.813

[16] Kaur, J. (2019). Taxonomy of Malware: Virus, worms and trojan. International Journal of Research and Analytical Reviews, 6(1): 192-196. http://ijrar.com/.

[17] Ibrahim, M.R., Thanoon, K. (2022). Quasar Remote Access Trojan feature extraction depending on Ethical Hacking. Technology, 4(1): 58-75. https://doi.org/10.47577/technium.v4i1.5831

[18] Supriyono, A.R., Prayudi, Y. (2018). Live forensics acquisition file sharing samba pada mikrotik router OS. Cyber Security dan Forensik Digital, 1(1): 7-13. https://doi.org/10.14421/csecurity.2018.1.1.1210

[19] Kusuma, G.H.A. (2023). Implementasi volatility dalam mengalanalisa malware pada memory dump. Journal of Informatics and Advanced Computing (JIAC), 4(1): 36-43.

[20] Syahib, M.I., Yasin, M.A., Rauf, B.W. (2023). Pengenalan dan instalasi kali linux untuk langkah awal pengetahuan tentang keamanan sistem informasi. ANOA: Jurnal Pengabdian Masyarakat Fakultas Teknik, 1(02): 32-38. https://doi.org/10.51454/anoa.v1i02.275

[21] Yudhana, A., Riadi, I. (2022). Analisis kinerja perangkat lunak forensic imaging pada sistem operasi linux menggunakan metode static forensic. Insect (Informatics and Security): Jurnal Teknik Informatika, 8(1): 38-47. https://doi.org/10.33506/insect.v8i1.1962

[22] Putra, R.D.L., Mardianto, I. (2019). Exploitation with Reverse_tcp method on android device using metasploit. Jurnal Edukasi dan Penelitian Informatika, 106-112.

[23] Kolli, Y., Mohd, T.K., Javaid, A.Y. (2018). Remote desktop backdoor implementation with reverse TCP payload using open source tools for instructional use. In

2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 444-450. https://doi.org/10.1109/IEMCON.2018.8614801

[24] Vyas, H. (2019). Fully undetectable Remote Access Trojan: Windows. International Journal of Research and Applied Sciences in Engineering and Technology, 7(5): 1886-1890. https://doi.org/10.22214/ijraset.2019.5316

[25] Raj, S., Walia, N.K. (2020, July). A study on metasploit framework: A pen-testing tool. In 2020 International Conference on Computational Performance Evaluation (ComPE), IEEE, pp. 296-302. https://doi.org/10.1109/ComPE49325.2020.9200028

[26] Thomas, S., Scholar, P.G. (2021). Vulnerability testing on rooted android phones using msf venom payloads. In Proceedings of the National Conference on Emerging Computer Applications (NCECA), p. 27. https://doi.org/10.5281/zenodo.5112704

[27] Kuncoro, A.P., Kusuma, B.A. (2018). Keylogger is a hacking technique that allows threatening information on mobile banking user. In 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE), IEEE, Yogyakarta, Indonesia, pp. 141-145. https://doi.org/10.1109/ICITISEE.2018.8721028

[28] Yadav, S., Mahajan, A., Prasad, M., Kumar, A. (2020). Advanced keylogger for ethical hacking. International Journal of Engineering Applied Sciences and Technology, 5: 634-638. http://www.ijeast.com.

[29] Khalid, Z., Iqbal, F., Al-Hussaeni, K., MacDermott, A., Hussain, M. (2021). Forensic analysis of Microsoft Teams: Investigating memory, disk and network. In International Summit Smart City 360. Cham: Springer International Publishing, pp. 583-601. https://doi.org/10.1007/978-3-031-06371-8_37

[30] Shree, R., Shukla, A.K., Pandey, R.P., Shukla, V., Bajpai, D. (2022). Memory forensic: Acquisition and analysis mechanism for operating systems. Materials Today: Proceedings, 51: 254-260. https://doi.org/10.1016/j.matpr.2021.05.270

[31] Yücel, Ç., Koltuksuz, A. (2020). Imaging and evaluating the memory access for malware. Forensic Science International: Digital Investigation, 32: 200903. https://doi.org/10.1016/j.fsidi.2019.200903