Elevating Cybersecurity: Live Forensic Analysis of Remote Access Trojans with FTK Imager

Author: Sunny thakur

ABSTRACT

This study examines the use of FTK Imager software for conducting live forensic investigations aimed at tracking and analyzing Remote Access Trojan (RAT) attacks. Our research seeks to enhance computer system security and assist organizations in safeguarding their assets and data against malicious cyber threats. A key contribution of this study is the understanding of the Remote Access Trojan virus's presence, even after its removal.

The methodology involves installing Kali Linux as a platform for virus creation and execution, utilizing FTK Imager for forensic analysis, and developing and employing various viruses. The process includes setting up Kali Linux, identifying and analyzing the presence of viruses using FTK Imager, and applying disk and memory forensic analysis techniques to investigate RAT attacks.

The findings reveal that once the target activates the generated virus, the executor gains full access to the target machine, allowing them to monitor and record all activities. To effectively detect the virus developed by the executor, FTK Imager must be installed on the target system.

This enables the use of memory and disk forensics to facilitate the search for files created by the executor.

This study illustrates how FTK Imager can be employed as a forensic investigation tool to observe and analyze Remote Access Trojan attacks, providing insights for real-world forensic applications.

Table of Contents

1. INTRODUCTION

According to a publication by Kelrey and Muzaki, the National Cyber and Crypto Agency (BSSN) of Indonesia reported a staggering 300% increase in cyberattacks utilizing Remote Access Techniques (RAT) in 2022 compared to the previous year, with 5,874 recorded RAT attacks in the country. In today's digital landscape, the security of data and computer systems has become increasingly vital. The rise in cyberattacks, particularly Remote Access Trojan (RAT) assaults, underscores the urgent need to protect critical systems and sensitive data.

A Remote Access Trojan (RAT) is a type of malicious software that enables an attacker to gain unauthorized remote access and control over a computer or network without the owner's knowledge. Essentially, a RAT is designed to assume full control of an infected system to achieve objectives related to system penetration, unauthorized surveillance, and data theft. The executor's advantage lies in their ability to monitor the victim's actions, particularly when sensitive information, such as usernames and passwords, is input by the target. RATs are commonly employed in various cyberattack scenarios, including data gathering, system manipulation, surveillance, and exploiting existing security vulnerabilities. Thus, detecting and analyzing RAT attacks is crucial for maintaining system and data security.

Live forensic investigation represents a proactive approach to investigating, preventing, and identifying cyber threats in real time. This method allows for the instant acquisition of digital evidence from an operating system without disrupting its ongoing operations, enabling security experts to promptly detect active threats and respond effectively. For this study, the FTK Imager's disk and memory forensic analysis tools are utilized to investigate the presence of Remote Access Trojan infections. Memory forensics complements disk forensics, as it records data that can be analyzed later, ensuring that RAT infections can be identified even if the system deletes or destroys evidence.

FTK Imager is a prominent forensic tool used by security professionals to collect and analyze digital evidence. The software can capture and analyze live screenshots of the operating system, allowing security professionals to investigate suspicious activities and search for indicators of Trojan attacks or other illicit actions. This study aims to explore the application of live forensic investigation, with a focus on using FTK Imager to monitor and evaluate Remote Access Trojan assaults. By enhancing computer system security, this research intends to assist organizations in better protecting their assets and data against malicious cyberattacks.

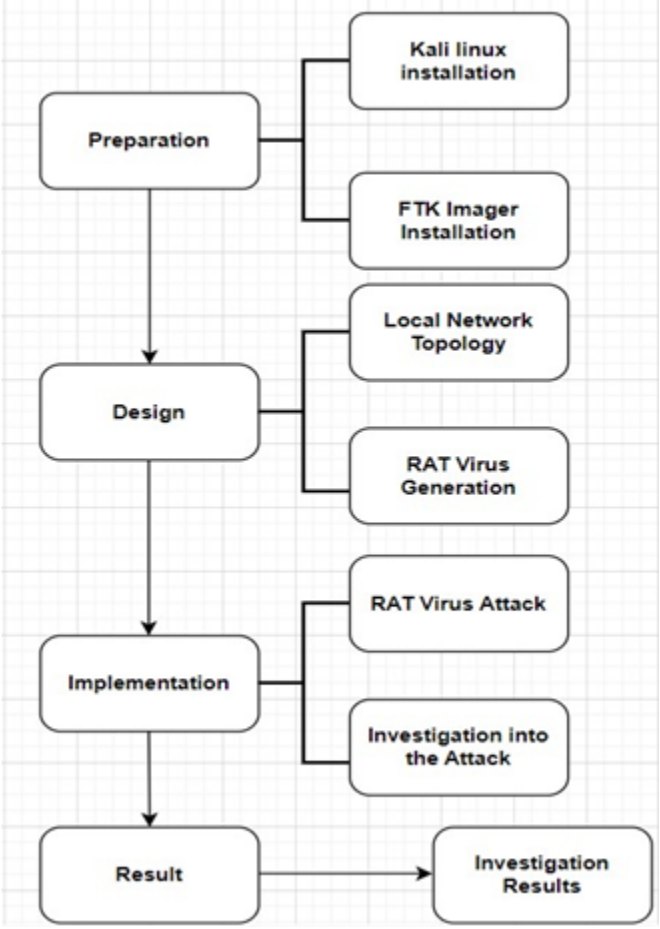
In light of these issues, this study poses the following questions: How can a Remote Access Trojan be created to target computer users? Furthermore, how can one detect evidence of its existence even after the virus has been removed or eliminated by the system?

To address these questions, this study will explore the process of creating a Remote Access Trojan using Linux version 2022.4, from conception to implementation, and demonstrate how to utilize the FTK Imager application as a digital forensic tool to locate evidence of hacking

activities. The primary goal is to identify the presence of the Remote Access Trojan virus, even in cases where the infection has been manually or automatically eradicated by the system.

2. RESEARCH METHODS

This research is structured into four key steps: Preparation, Planning, Implementation, and Outcomes, as illustrated in Figure 1.



a) Preparation

1. **Kali Linux Installation**
   The first step involves installing Kali Linux on a virtual machine. This platform serves as the environment for developing and executing the Remote Access Trojan (RAT) virus. The installation of Kali Linux, combined with the use of FTK Imager, establishes the groundwork for detecting the presence of the virus.
2. **FTK Imager Installation**
   Following the Kali Linux setup, the FTK Imager software is installed to enable hands-on forensic investigation techniques. FTK Imager is crucial for detecting the specific type of malware that targets the machine when the virus is executed.

b) Design

1. **Local Network Topology**
   The design phase focuses on creating a network topology to monitor the target's behavior when connected to a local area network containing a malware execution device. During this phase, FTK Imager is utilized for live forensic investigations, enabling the monitoring and evaluation of Remote Access Trojan attacks.
2. **RAT Virus Generation**
   Utilizing virtual machines, this phase involves producing viruses through the development of malicious software based on the Remote Access Trojan attack model. The purpose is to test computer systems for vulnerabilities.

c) Implementation

1. **RAT Virus Attack**
   Penetration tests are conducted using the Remote Access Trojan virus. This involves leveraging file-sharing functions to distribute the virus, enticing victims to download and execute malware files disguised as embedded images.
2. **Investigation into the Attack**
   Following the execution of the infection, the next step is to investigate the type of malware that has infected the target machine.

2.1 Result Investigation

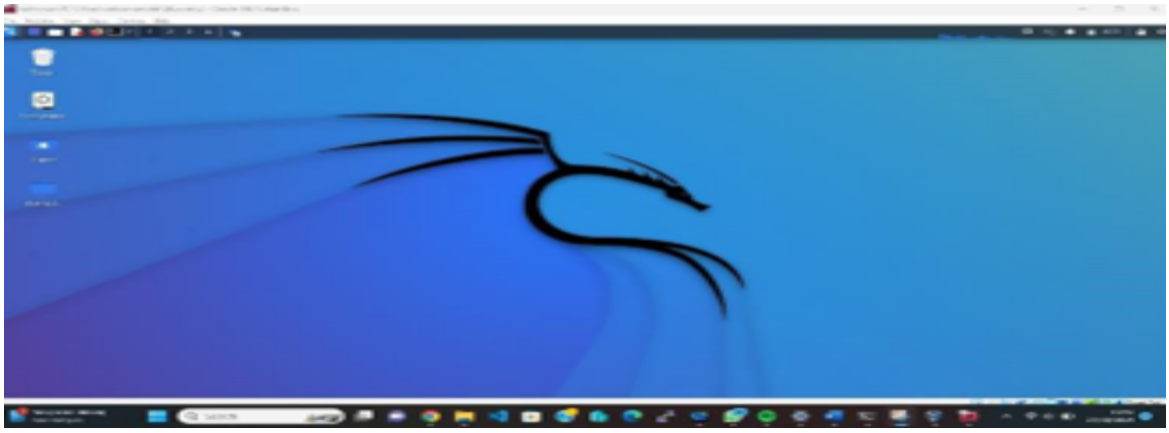
The final stage, Result Investigation, encompasses the findings derived from the process of developing the Remote Access Trojan virus, delivering it to the target, and identifying the nature of the attack. This phase provides a comprehensive analysis of the virus's effectiveness and details the process used to detect the infection on the computer through the FTK Imager software.

3. RESULTS

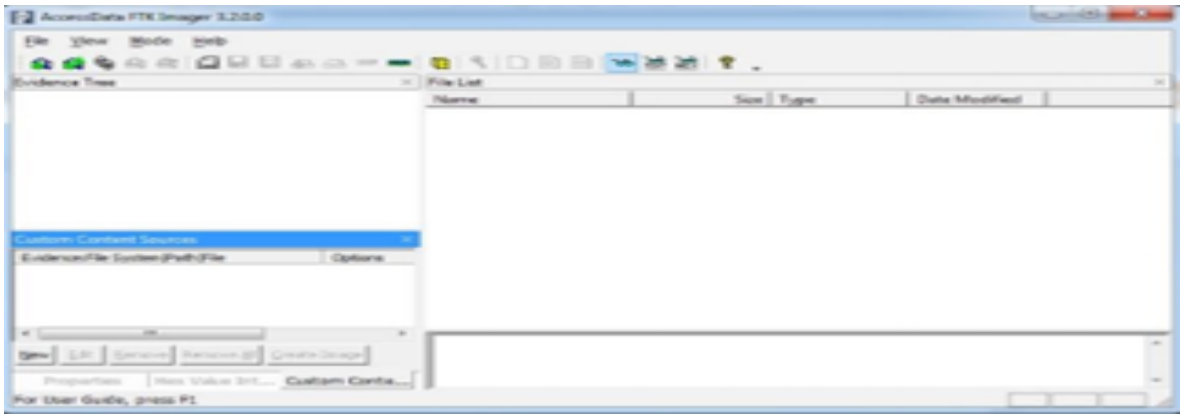
a) Preparation

In accordance with the outlined study methodology, the use of FTK Imager software for live forensic investigation to monitor and analyze Remote Access Trojan attacks proceeds through the four stages: Planning, Designing, Implementing, and Analyzing Findings. The installation of Kali Linux as a platform for creating the Remote Access Trojan virus, illustrated in Figure 2 below, will be the primary outcome addressed.

Figure 2 highlights that many IT and security solutions available on Kali Linux may appear complex to the average user. A significant portion of its capabilities is tailored primarily for network research and security testing. Kali Linux offers a suite of advanced technologies for network security, hacking, and penetration testing, underscoring its strength in the field of IT security.



In Figure 3, cybercrime investigators often utilize FTK Imager to collect digital evidence from devices. This tool is extensively used by professionals in the field of digital forensics due to its reliability and investigative capabilities. FTK Imager proves valuable in various digital investigation scenarios, offering features such as file viewing, metadata analysis, and file searching. Its user-friendly graphical interface simplifies the process of viewing digital evidence, making it accessible even to forensic novices.

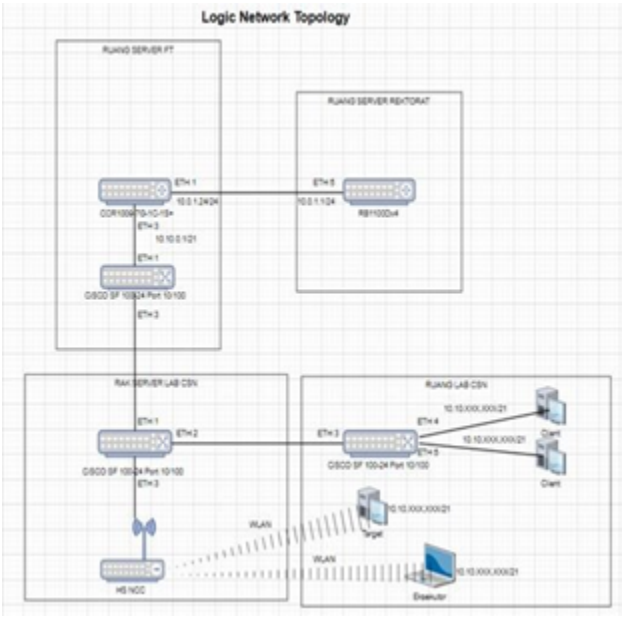


b) Design

Before launching an attack on the target machine, the executor must understand the network path followed to develop a Remote Access Trojan virus. This is achieved by installing Linux multiple times and employing FTK Imager as a live forensic research tool. As illustrated in Figure 4, the executor connects to the same network segment as the intended target, facilitating communication.

Figure 4 presents the logical topology of the IP addressing scheme in the network structure established by researchers in the CSN Lab. The local network is connected to the network center of the Ibn Khaldun University Bogor Rectorate Building. The scanning device, or laptop, is linked to the HS-NCC wireless access point, which in turn connects to Switch 02 (Cisco SF 100-24) via port 10/100. Additionally, a client PC in the CSN Lab room is connected to Switch 03

(PC LAB CSN), also a Cisco SF 100-24, on port 10/100. Switch 03 is connected to Switch 02 (FT CENTER) to form a cohesive network.



In the faculty server room, Switch 02 connects to the CCR1009-7G-1C-1S+ router, which is assigned a local IP of 10.10.0.1/21 and serves as the DHCP server for IP addressing on the CSN Lab network with an address range of 10.10.XXX.XXX/21. From the CCR1009-7G-1C-1S+ router, interface 01, with IP 10.0.1.24/24, connects to the RB1100Dx4 router in the rectorate server room, which has an IP of 10.0.1.1/24.

To generate the payload for the attack, the `msfvenom` command is used to create a reverse TCP Meterpreter payload in executable format for Windows 64-bit, saved as "Articles.pdf". When executed on the victim's machine, this Windows executable creates a reverse shell that connects back to IP address 10.10.7.227 on port 4444.

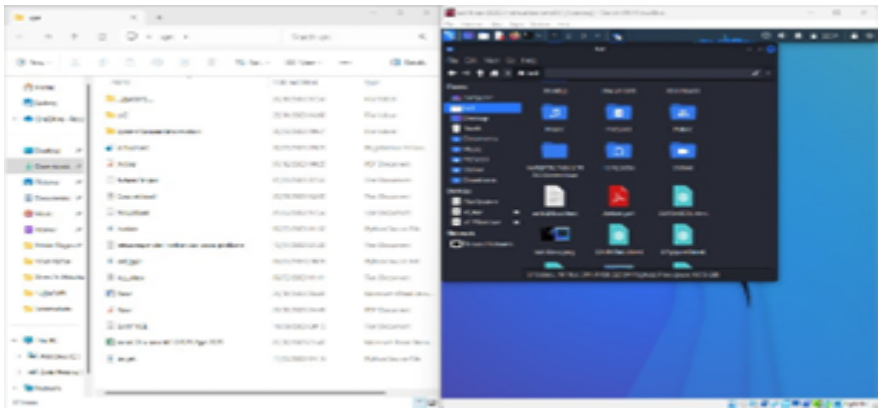
In Figure 5, To initiate the attack against the target, this step

spreads the Remote Access Trojan infection . 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

Once the executor has created a Remote Access Trojan (RAT) infection, data exchange with the target will occur as shown in Figure 6. The executor lures the victim into opening a viral file, thereby gaining complete access to the target machine.

In Figure 6, the attack was executed against a Windows 11 Home Single Language (version 22H2) using the Kali Linux operating system (version 2022.4). When the target executes a malicious file disguised with a PDF extension, the executor obtains full control over the target computer, allowing for actions such as downloading, deleting, editing, and uploading files. This poses significant risks, especially if careless individuals inadvertently execute the virus. The executor can easily deceive the target into opening the infected file by appending an `.exe` extension to the PDF.



In Figure 7, the `msfconsole` serves as the main console interface for the Metasploit Framework. This interface enables users to interact with and execute Metasploit modules directly from the command line. Some command-line functions of `msfconsole` are summarized in Table 1.

In summary, a reverse TCP payload, specifically designed for Windows x64 systems, is configured with this command. Once the Windows x64 target is successfully exploited, the Meterpreter is installed, establishing a reverse TCP connection back to the attacker.

Figure 8 illustrates that the executor gains full access to the files generated by the virus once the target opens the malicious file. To assess the effectiveness of the virus, the executor conducts penetration testing on the target machine. During this test, the executor tracks the target's actions using Kali Linux tools. When the target enters their login credentials to access the UIKA learning website portal, the executor displays these actions in real time on the console, allowing them to capture the target's password and login information.

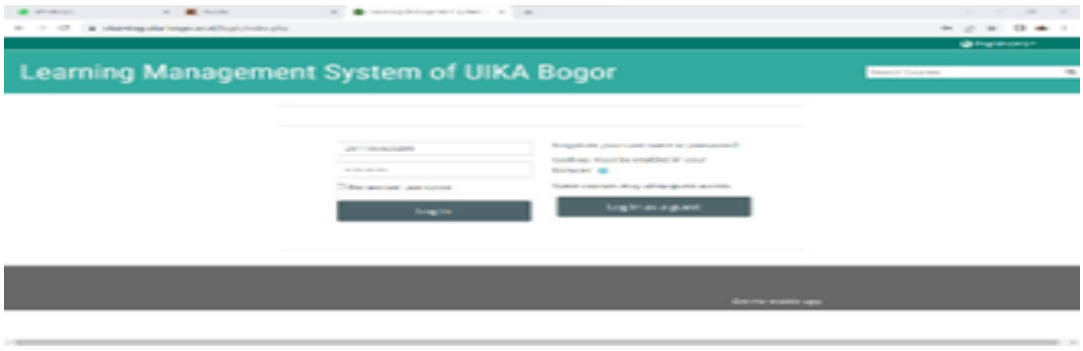


Table 1. Explanation of Virus Startup Command Line

No.	Command Line	Function
1	Exploit	Loads the Metasploit exploit module, which is code designed to exploit vulnerabilities or bugs to execute a payload.
2	Multi	Indicates a multi-exploit handler, which can work with any payload and supports multiple targets by default.

3	Handler	A component that manages communication with the payload after it has been uploaded to the target.
4	Set LHOST	Defines the IP address for the payload to connect back to; `10.10.7.227` indicates the attacker's listening interface.
5	Set LPORT	Specifies the TCP port for the reverse connection; `4444` is commonly used, but others like `80`, `443`, or `22` can also be utilized.
6	Set payload	Configures the payload to be used in the exploit.
7	Windows/x64	Indicates that the payload targets the 64-bit Windows operating system.
8	Meterpreter	Refers to the Metasploit Meterpreter payload, which is an advanced payload designed for post-exploitation control.
9	Reverse_tcp	Specifies the reverse connection technique using the TCP protocol, where the exploited Windows target connects back to the attacker.

d) Result Investigation

The target activity results will be logged in the Kali Linux operating system, as depicted in Figure 9, after monitoring the target's actions using the keyscan tool. The logged data includes information from keyboards and other input devices connected to the target computer. A forensic assessment of the infected target laptop can be conducted using the methods outlined in Figures 10 and 11, facilitating the detection of any infections present.

In Figure 9, the `keyscan_start` and `keyscan_dump` commands are valuable features of the Metasploit Framework within Kali Linux that enable keylogging on the target. It is crucial to note that this keylogging method is strictly for research purposes, intended to assess the effectiveness of a virus generated and authorized by the appropriate parties. The function of the command line is detailed in Table 2.

Figure 9. Virus Execution

During the investigation phase of the Remote Access Trojan incident, this research identified the presence of malicious software on the victim's computer system. The perpetrator had created malware intended to operate on the target machine. Consequently, the presence of malicious software is tracked using digital forensic tools such as FTK Imager. There are two primary methods for identifying malicious software on a system.

e) Disk Forensics

In Figure 10, FTK Imager serves as the forensic investigation tool used in this analysis. By examining forensic memory and drives, the file generated by the executor is visible in the image above due to disk forensics techniques applied by FTK Imager. This file enabled the executor to access the target machine. Disk forensics focuses on the collection, organization, and analysis of digital evidence from storage media, including hard drives, USB flash drives, CDs, DVDs, and more. This discipline is often referred to as computer forensics or digital forensics.

Figure 10. Hard Drive Storage Investigation

f) Memory Forensics

In Figure 11, the file generated by the executor is displayed thanks to memory forensics techniques utilized by FTK Imager. Even after deletion, the RAT malware file can be located at: `Documents\users\ridwa\OneDrive\Desktop\uye\Article.pdf`. The executor accessed the target machine via this file. Memory forensics involves examining a device's volatile memory (RAM) to uncover digital evidence for investigating cybercrimes or security incidents. This analysis must be conducted while the device remains operational because volatile memory (RAM) stores data that is lost once the device is powered off. RAM contains information about open files, processes, network connections, and more. Memory forensic analysis is applicable in various contexts, including cybercrime investigation, malware analysis, information security incident response, and digital forensics.

Figure 11. Memory Investigation

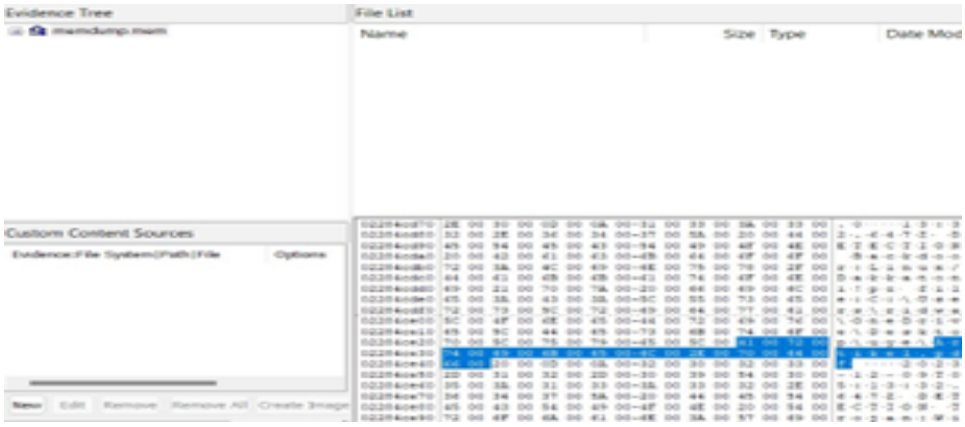


Table 2. Explanation of Virus Startup Command Line

No.	Command Line	Function
1	Keyscan_start	Initiates the keylogging process on the target. Every keystroke made by the target user is captured. This command is typically used after successfully compromising the target through a Meterpreter session or exploited reverse shell.
2	Keyscan_dump	Displays or discards all keylog results captured to date after the keylogging process has begun. It reveals all keystrokes and keyboard inputs made by the target user, including sensitive information such as passwords and private communications.

4. CONCLUSIONS

This research methodology comprises four key steps:

1. **Preparation**: The initial phase involves the installation of FTK Imager and Kali Linux. This step is essential for building and executing the virus, where Kali Linux serves as the platform for creating the Remote Access Trojan (RAT), while FTK Imager is launched to commence the forensic investigation.
2. **Design**: This phase includes the creation of the RAT and establishing a local network topology. Understanding the local network topology allows executors to effectively identify their target paths for delivering the virus, facilitating the attack's success.
3. **Implementation**: In this stage, the RAT is utilized to conduct the attack. The virus is transmitted through file sharing, wherein the executor deceives the victim into opening the malicious file. Once the victim opens the file, the executor gains full access to the targeted laptop or PC.
4. **Investigation**: A live forensic investigation is conducted to ascertain the existence of an infection. Digital evidence of RAT assaults was discovered within a PDF file during this

phase. Even after the system's deletion of the virus, FTK Imager proved effective in identifying the RAT presence.

The primary contribution of this work lies in a forensic investigation approach capable of uncovering digital evidence of remote access attacks (RATs) through the utilization of FTK Imager. This methodology enhances the understanding of RAT behavior and strengthens the forensic investigation process, ultimately contributing to improved cybersecurity practices.

REFERENCES

1. Kelrey, A.R., Muzaki, A. (2019). Pengaruh ethical hacking bagi keamanan data perusahaan. Cyber Security dan Forensik Digital, 2(2): 77-81. Link
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. Link
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. Link
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. Link
7. Tukaral, K., Sheth, R.K. (2019). Sandbox evasive Remote Access Trojan. Link
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. Link
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. Link
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. Link
12. Closser, D., Bou-Harb, E. (2022). A live digital forensics approach for quantum mechanical computers. Forensic Science International: Digital Investigation, 40: 301341. Link
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. Link

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). Link
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. Link