Aurelia: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia
E-ISSN: 2964-2493 P-ISSN: 2962-0430
Vol. 4 No. 1 January 2025

# Utilizing Capa in Kali Linux for Wannacry Malware Identification and Analysis

**Pritiy Singgam[1] Afifah Naila Nasution[2] Pedro Stella Mario Meyar Waruwu[3]**
Computer Science Department, Faculty of Mathematics and Natural Sciences, Universitas Negeri Medan, Indonesia[1]
Mathematic Department, Faculty of Mathematics and Natural Sciences, Universitas Negeri Medan, Indonesia[2,3]
Email: pritymirota@gmail.com[1]

**Abstract**
Purpose: This study aims to analyze the WannaCry ransomware using Kali Linux and the Common Access Platform Assistant (CAPA) method to provide a deeper understanding of the malware's attack tactics, capabilities, and behaviors. Methods/Study design/approach: The research was conducted by installing CAPA version 7.4.0 downloaded from GitHub, followed by file extraction and access permission configuration. The WannaCry malware was obtained from the "thezoo" repository on GitHub, extracted, and analyzed using CAPA commands in the Linux terminal. The analysis results were presented in tables showing the malware's tactics, techniques, and behaviors. Result/Findings: The analysis revealed that CAPA effectively identified various tactics and techniques used by WannaCry, confirming its classification as malware. Validation through antivirus services indicated that 68 out of 72 services flagged the file as malicious, emphasizing the importance of robust cybersecurity measures. Novelty/Originality/Value: This study offers new insights into the working mechanisms of WannaCry ransomware and highlights the effectiveness of the CAPA method in malware analysis. The findings contribute to a better understanding of cybersecurity threats and provide valuable information for professionals in the field to enhance defense strategies against malware.
**Keywords:** WannaCry Ransomware, Malware Analysis, Kali Linux, Common Access Platform Assistant (CAPA), Cybersecurity



## INTRODUCTION

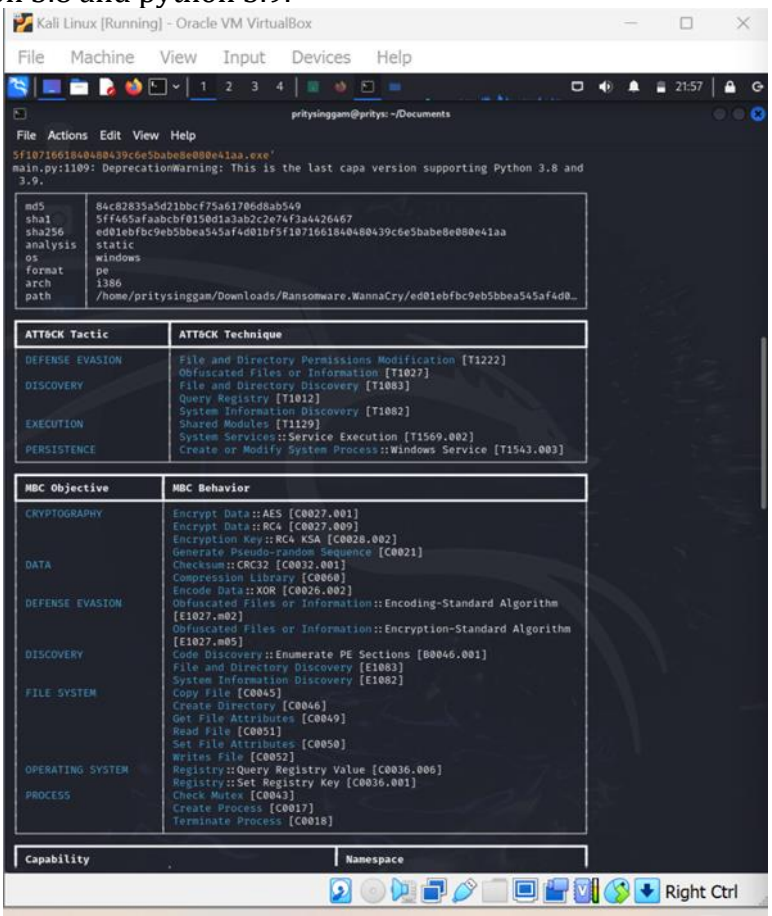
Kali Linux is the world's most powerful and popular penetration testing platform, used by security professionals in a wide range of specializations, including penetration testing, forensics, reverse engineering, and vulnerability assessment. The advancement of computer and Internet technology has changed our lives, and it has revolutionized the way organizations conduct businesses. However, technological evolution and digitization have given rise to cybercriminal activities. The growing threat of cyberat tacks on critical infrastructure, data centers, private/public, defense, energy, government, and financial sectors pose a unique challenge for everyone from an individual to large corporations. These cyberat tacks use malicious software (also known as Malware) for financial theft, espionage, sabotage, intellectual property theft, and political motives. Symantec's Internet Security Theart Report on the infection of malicious software attacks that use cryptographic techniques that threaten to publish a victim's data or permanently block access with a ransom or so-called ransomware continues to increase, and in May 2017 a new ransomware was identified that encrypts data, as well as makes copies of itself and gives time to pay, warning that the victim's files will be deleted. This type of ransomware is known as wannacry.

## RESEARCH METHODS

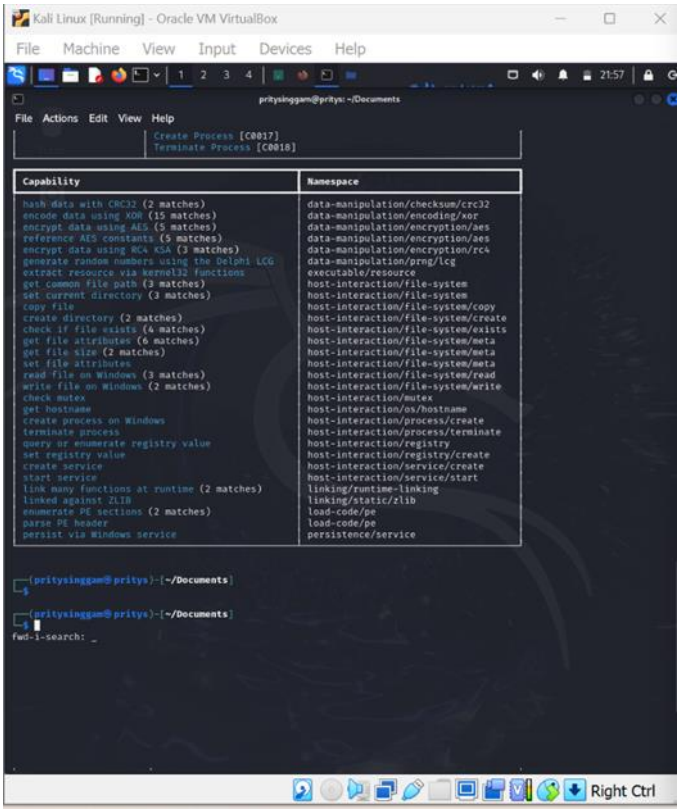
In this research we use kali linux which kali linux functions as an operating system that analyzes malware such as wannacry ransomware with the CAPA (Common Access Platform Assistant) method. The first step is the installation of capa which is downloaded via github, then we use the v7.4.0 release. We extract it first then After extracting we open the terminal then to give access we use the command “chmod += capa”. then enter capa with the command “./capa” then the capa version will come out. To add malware we take it on “thezoo github”, then we can download the desired malware. We took the WannaCry Ransomware. After downloading, we open the file manager and then extract the file, when extracted there will be a password request where the password is “infected”. We enter the command “./capa then drop the malware file that we have extracted. The result that comes out is the WannaCry Ransomware table which contains attack tactics, capabilities and behavior.

## RESEARCH RESULT AND DISCUSSION

Picture 1 and Picutre 2 are the results of testing malware in linux times using capa. The capa is in accordance with what is suggested by the CAPA documentation where the capa we use supports python 3.8 and python 3.9.

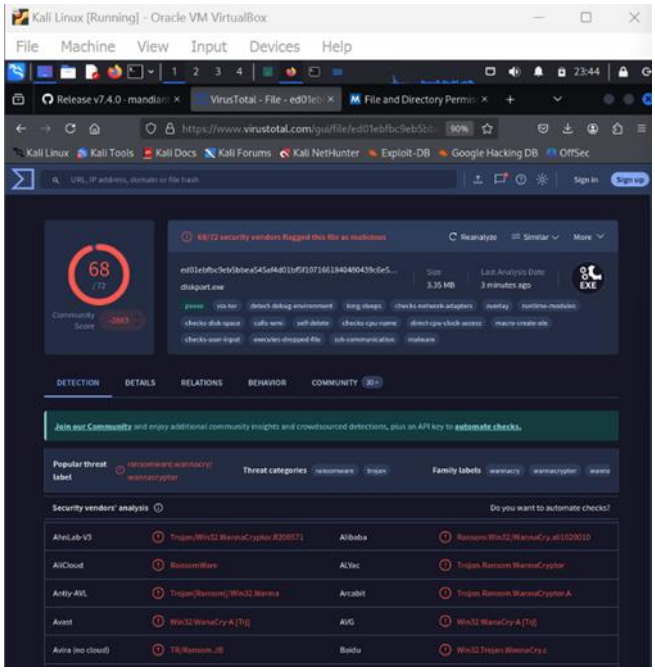



**Picture 1. (Table of Ransomware WannaCry)**

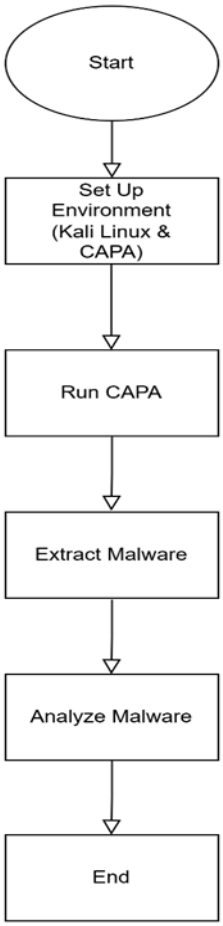



**Picture 2. (Table of Ransomware WannaCry)**

In both tables from Picture 1 and Picture 2 we can see that there are attack tactics and techniques, then MBC Objective and MBC Behavior tables and finally Capabilities and namespaces. The next table of Picture 1.3 is to prove whether the wannacry ransomware is really malware. the results show that 68 out of 72 antivirus services mark this file as malicious or containing a virus.




**Picture 3. (VirusTotal of Ransomware WannaCry)**




## CONCLUSION

This research demonstrates the use of Kali Linux and the Common Access Platform Assistant (CAPA) method to analyze the WannaCry ransomware. Through the installation and implementation of CAPA, the analysis revealed detailed insights into the attack tactics, capabilities, and behaviors associated with WannaCry, and confirmed its classification as malware. In addition, the validation of WannaCry as malware, was reinforced by external evaluations. Of the 72 antivirus services that reported the ransomware as a threat.The majority of them highlighted the malicious nature of the malware and emphasized the importance of strong cybersecurity measures to counter the threat. In summary, this analysis not only provides a deeper understanding of the working mechanism of the WannaCry ransomware, but also highlights the effectiveness of the CAPA technique in malware analysis and provides valuable insights in the field of cybersecurity.

## BIBLIOGRAPHY

Asaad, R. R. (2021). Penetration testing: Wireless network attacks method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7–12.

Konecka, S., Bentyn, Z. (2024). Cyberattacks as Threats in Supply Chains. European Research Studies Journal. (27) 3 : 778-796

Pandey, A. K., et al. (2020). Trends in malware attacks: Identification and mitigation strategies. In Critical Concepts, Standards, and Techniques in Cyber Forensics (pp. 47–60). IGI Global.

Wijaya, A. H., & Fitrani, A. S. (2019). Wannacry identification for computer data security. JICTE (Journal of Information and Computer Technology Education), 3(1), 22–28.