Digital Forensics(CY-341)

Project Report

Forensic Analysis of Ransomware Attack

Group Members

1. Shameer Awais (2022428)
2. Rooshan Riaz (2022506)
3. Yasir Khan (2022455)
4. Naqi Raza (2022574)

Submission Date: 04/05/2024

Ghulam Ishaq Khan Institute of Engineering Sciences and Technology

Contents

1 Introduction and Problem Statement

1.1 What is ransomware?

The WannaCry ransomware attack, one of the most notorious in recent history, hit the world in May 2017. It spread rapidly, affecting over 200,000 computers across 150 countries, including critical infrastructure such as the UK's National Health Service. The malware exploited a vulnerability in the SMB protocol, which had a patch available months before the attack. Using the EternalBlue exploit, which was leaked by the NSA, WannaCry spread swiftly through networks.

This project focuses on conducting a forensic analysis of the WannaCry attack using tools such as Autopsy for disk forensics and Volatility for memory analysis.

1.2 Why is forensic analysis critical?

Forensic analysis is essential in identifying the methods used by attackers, discovering the indicators of compromise (IoCs), and understanding the impact of the ransomware on infected systems. This process aids in strengthening cybersecurity measures and improving incident response protocols.

1.3 Scope and objectives of your project

The objective of this project was to set up an isolated environment, execute WannaCry, and analyze its behavior using forensics tools. The analysis focuses on:

- Disk forensics using Autopsy to locate encrypted files and identify the malware's traces.
- Memory forensics using Volatility to track in-memory processes and uncover real-time ransomware activities.
- Identifying key Indicators of Compromise (IoCs) for future ransomware detections.

2 Implementation details

2.1 Environment setup

The analysis was conducted in a controlled environment using a Windows 10 virtual machine (VM) that was isolated from external systems to prevent the spread of the ransomware. Windows Defender and SmartScreen protection were disabled to allow the ransomware to execute.

The VMware Virtual Network Editor displays three networks: vmnet0 (host-only, subnet 172.16.111.0), vmnet1 (host-only), and vmnet8 (NAT), with DHCP enabled and non-standard MTU settings. Host-only mode isolates VMs internally, while NAT shares the host's IP. This setup supports secure, private VM environments for testing or development.

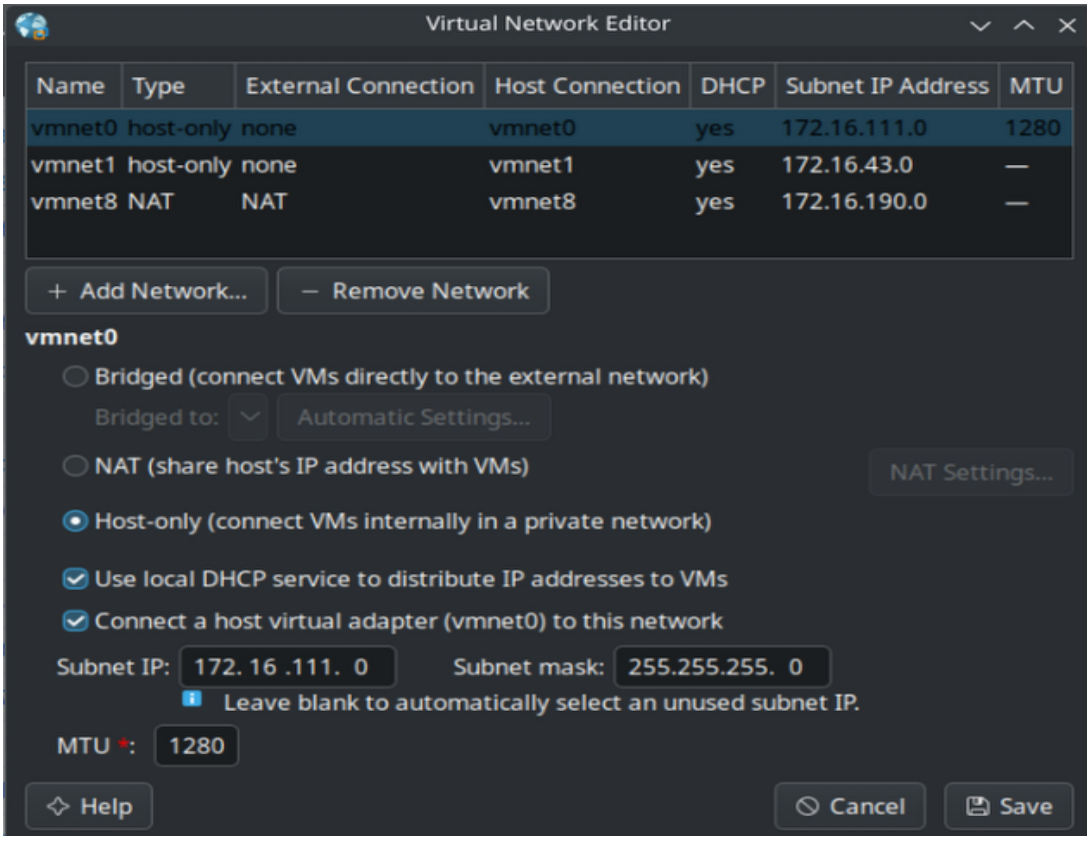

Figure 1: VM Host Only

2.2 Simulated attack description

The WannaCry ransomware was downloaded and executed in the isolated environment, replicating the conditions of a real-world attack. This simulation was necessary to gather forensic data without compromising any live systems.

Figure 2: Ransomware Alert

2.3 Step-by-step forensic investigation

1. Set up a Windows 10 virtual machine and disconnected it from the network.

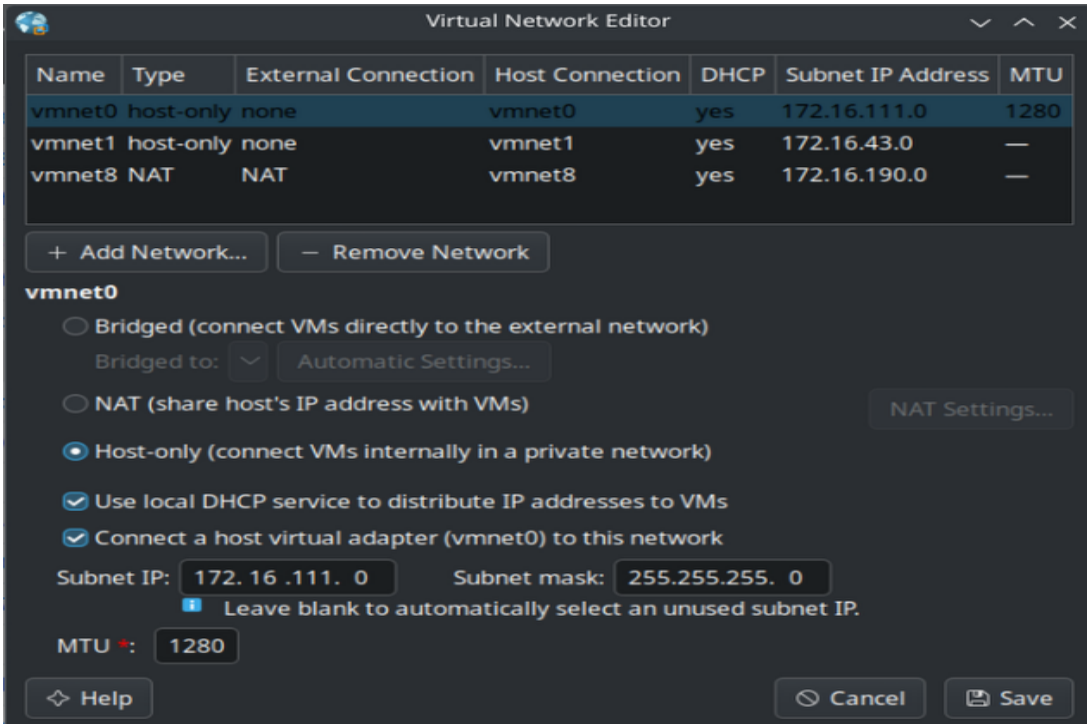

Figure 3: VM Host Only

2. Disabled Windows Defender and SmartScreen protection.

3. Downloaded and executed the WannaCry ransomware.

Figure 4: Ransomware Alert

4. Used FTK Imager to acquire both disk and memory images.

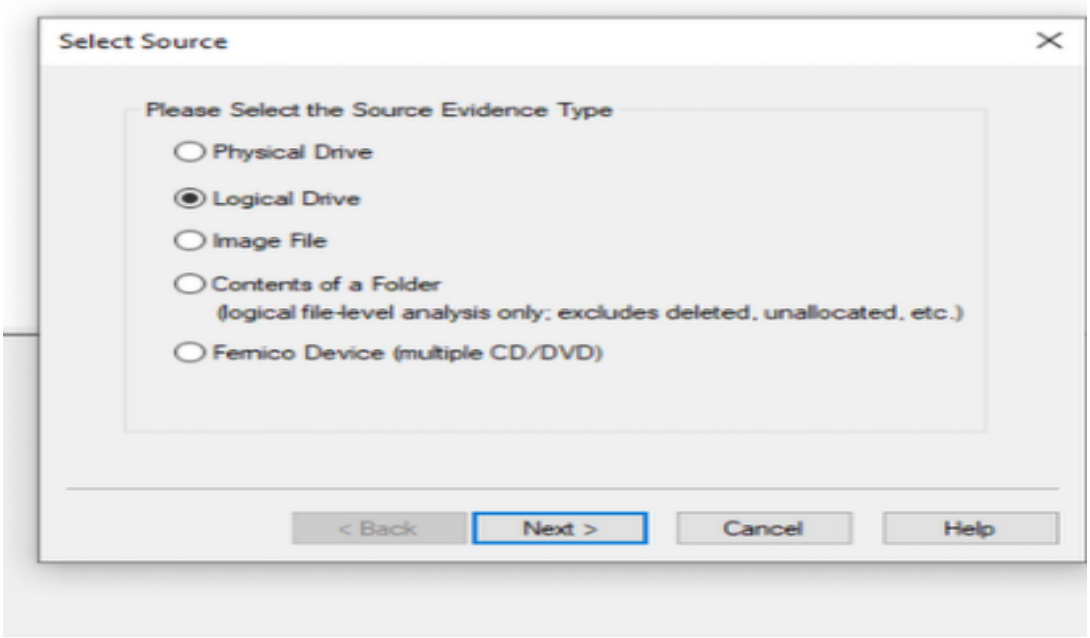

Figure 5: Select Source on FTK Imager

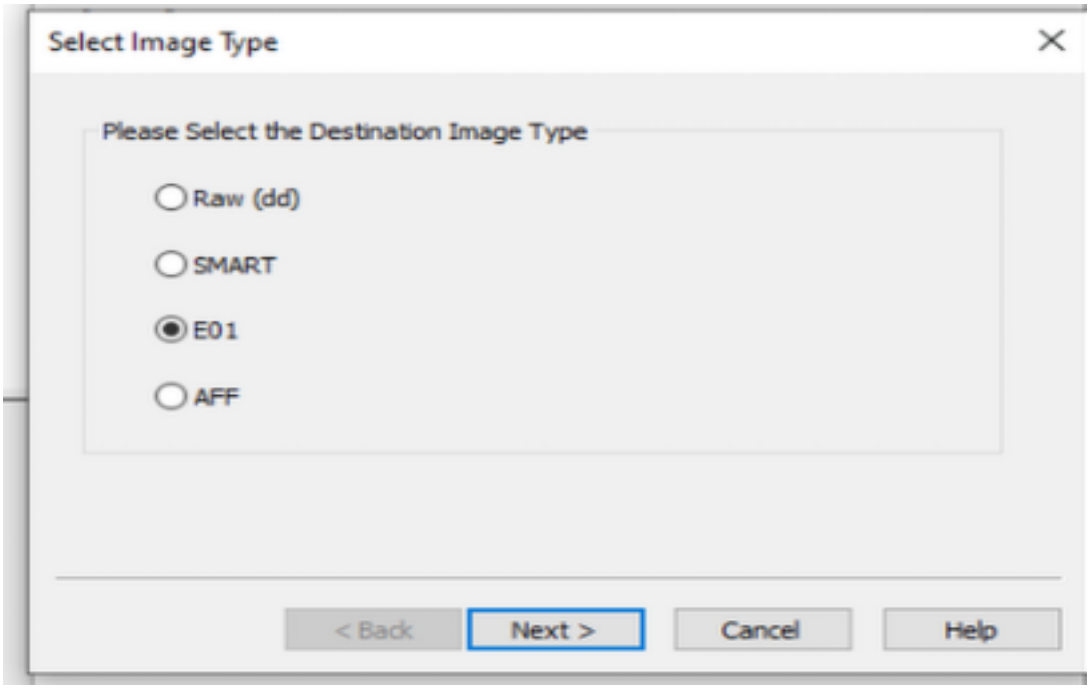

Figure 6: Select Image Type on FTK Imager

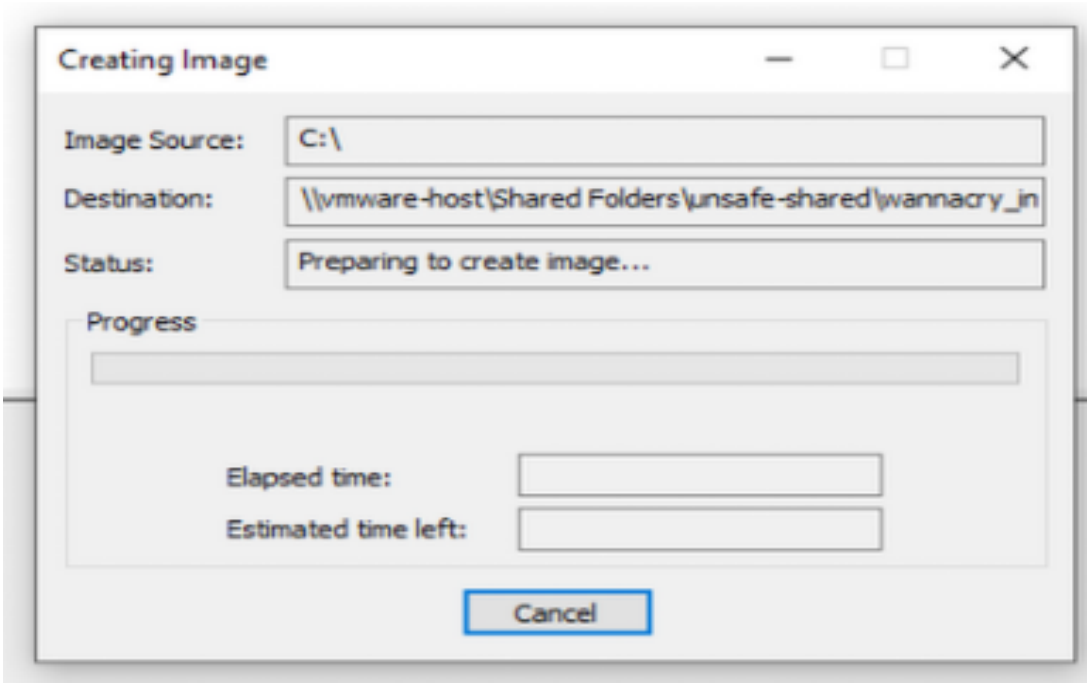

Figure 7: Creating Image on FTK Imager

5. Analyzed the disk and memory images using Autopsy and Volatility.

Figure 8: Autopsy

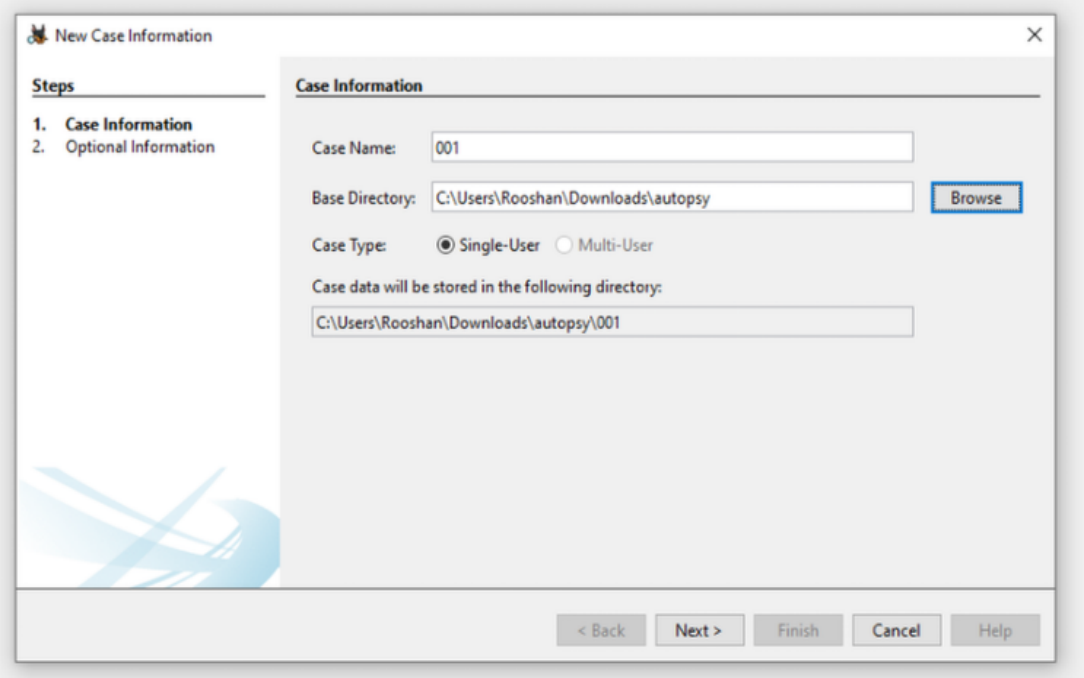

Figure 9: Case Name

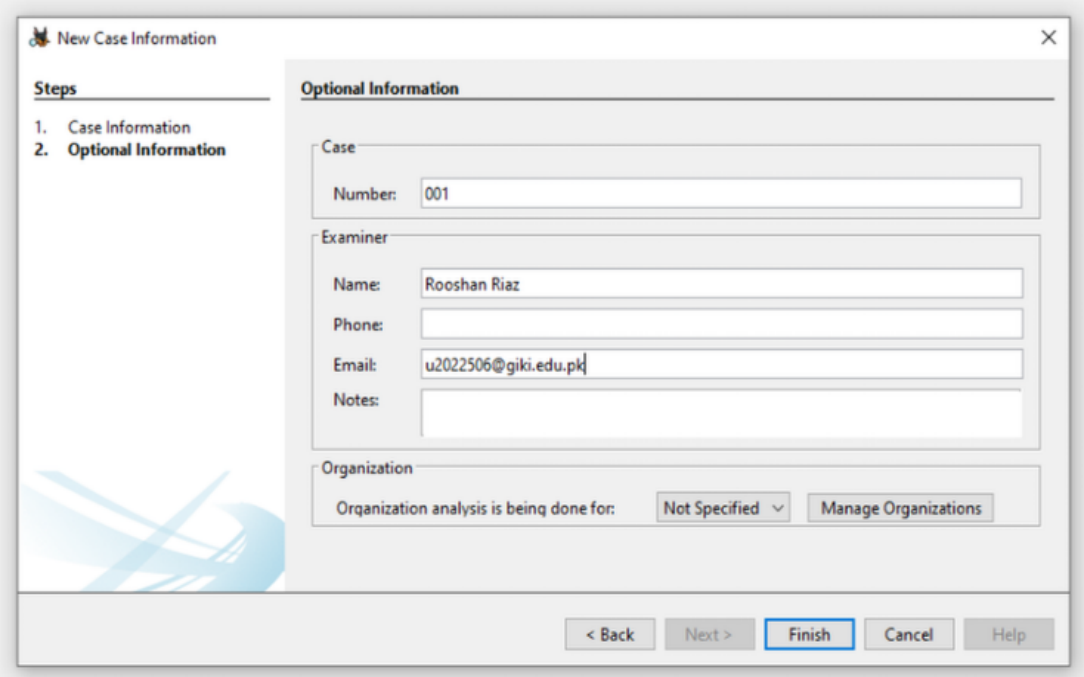

Figure 10: Case Number

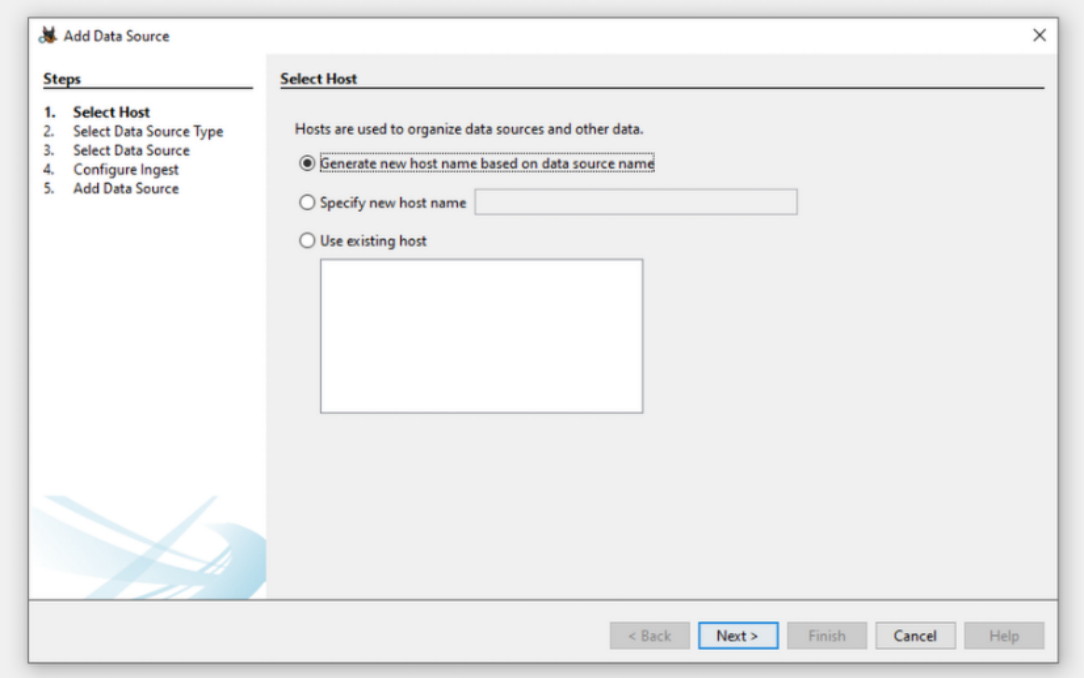

Figure 11: Select Host

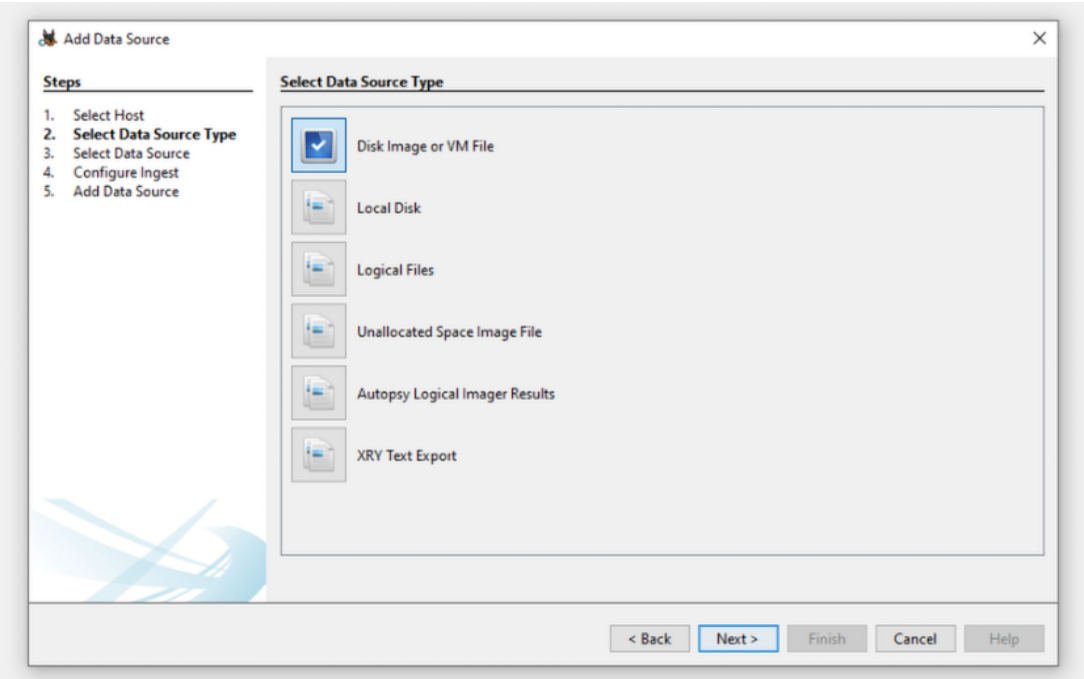

Figure 12: Add Data Source Type

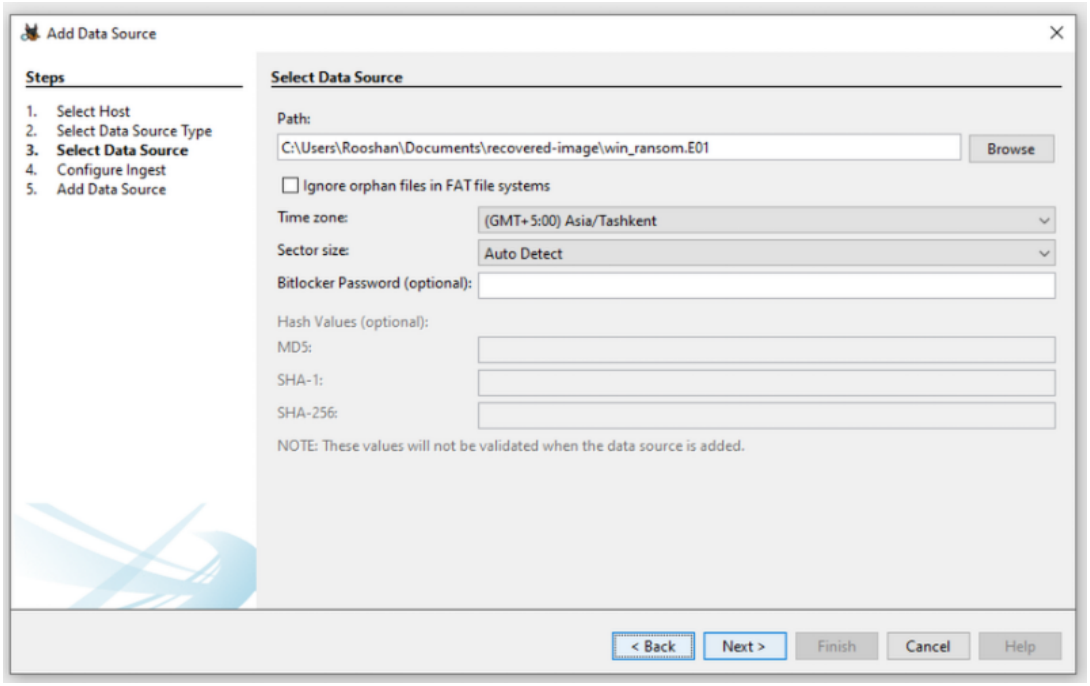

Figure 13: Select Data Source

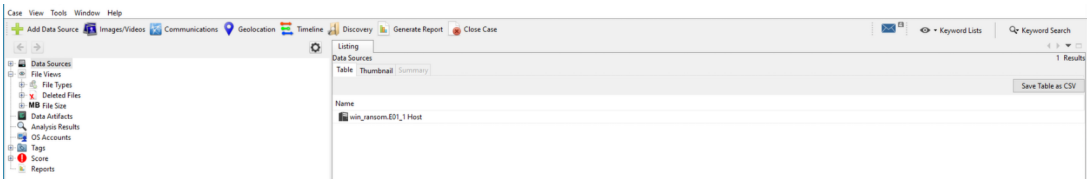

Figure 14: DataSources

6. Identified WannaDecryptor.exe in the executable section and tracked the malicious process.

2.4 Tools used and how

- **FTK Imager**: Acquired disk and memory images from the infected system.

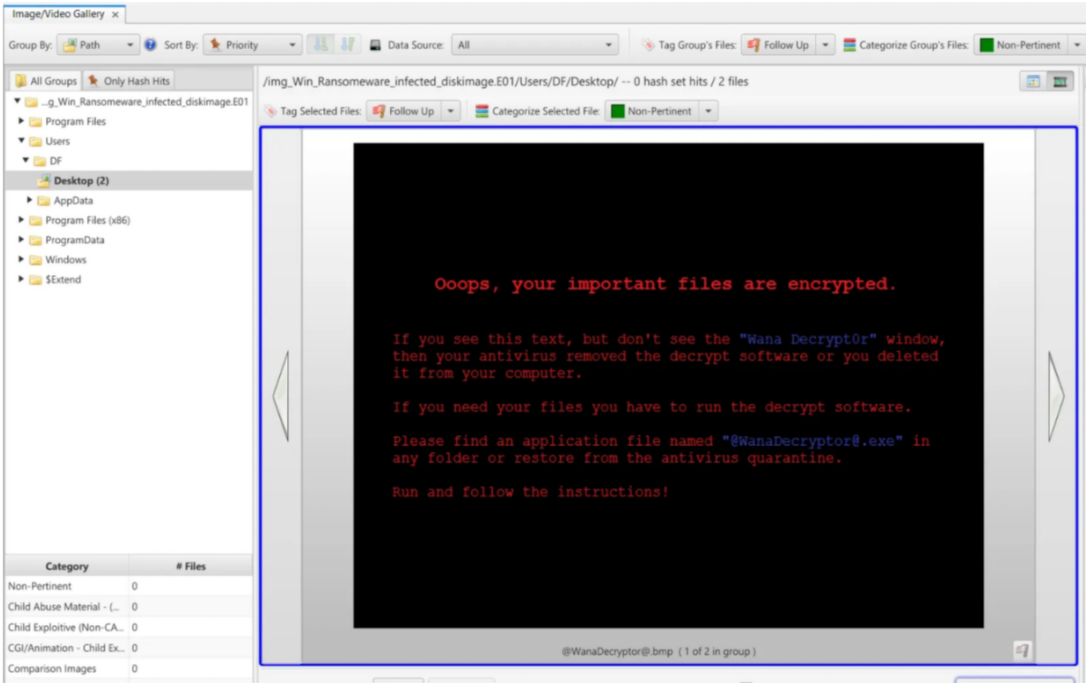

Figure 15: Image Gallery

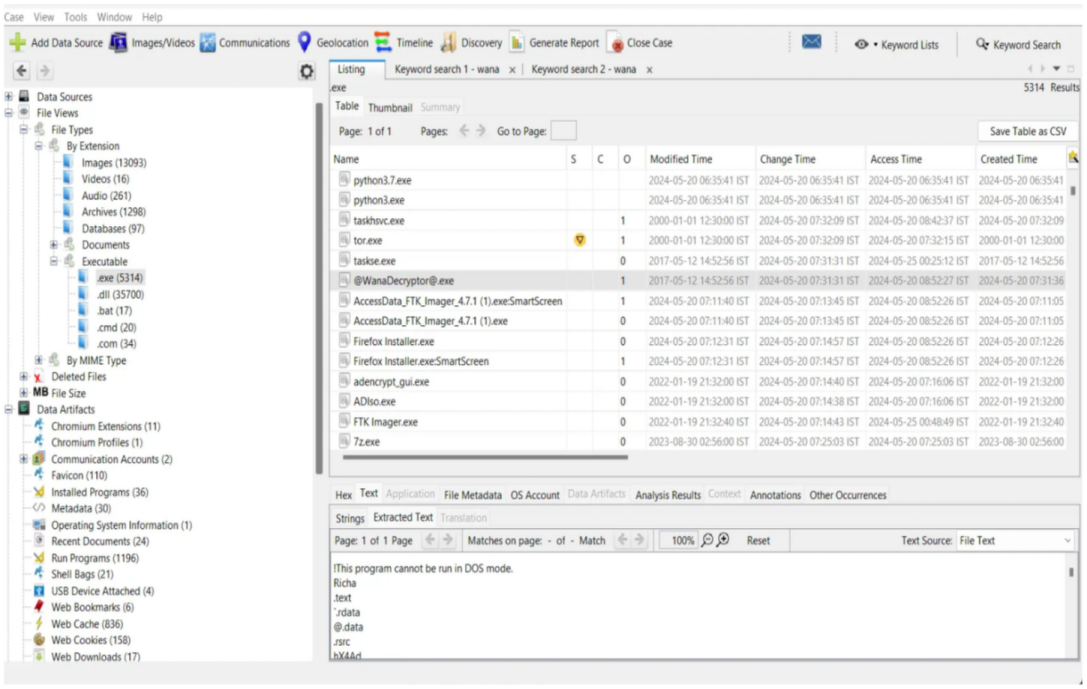

Figure 16: Listing of Files

- **Autopsy**: Analyzed the disk image to find encrypted files and the presence of WannaDecryptor.exe.

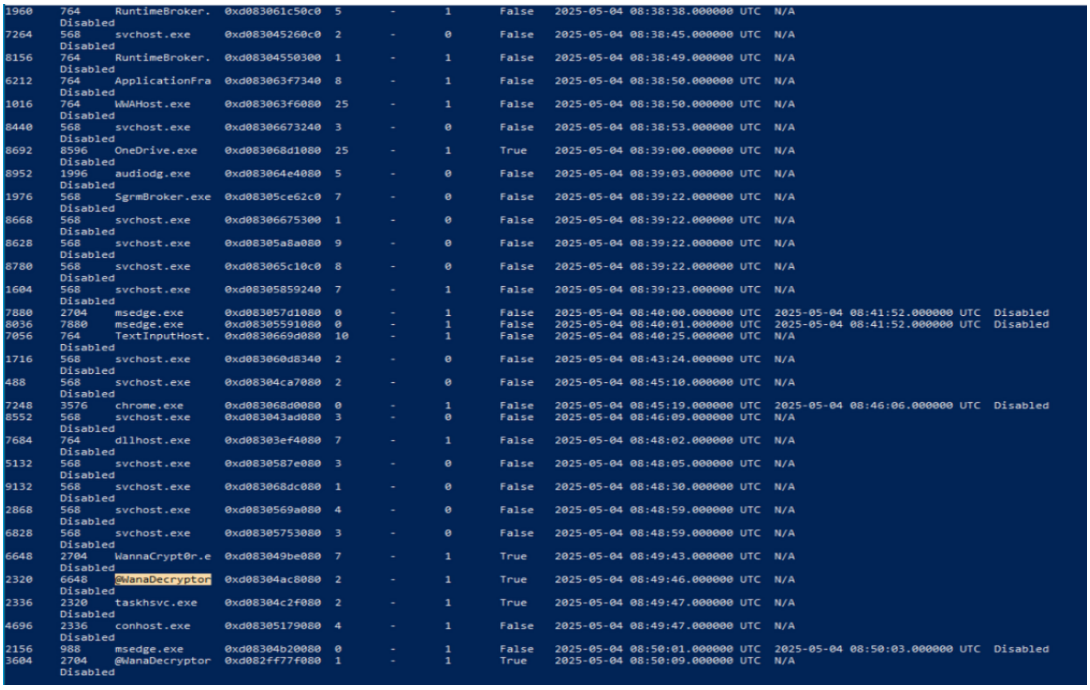

Figure 17: WannaDecryptor

- **Volatility**: Analyzed the memory dump to track processes related to the ransomware, identifying suspicious activity and extracting IoCs.

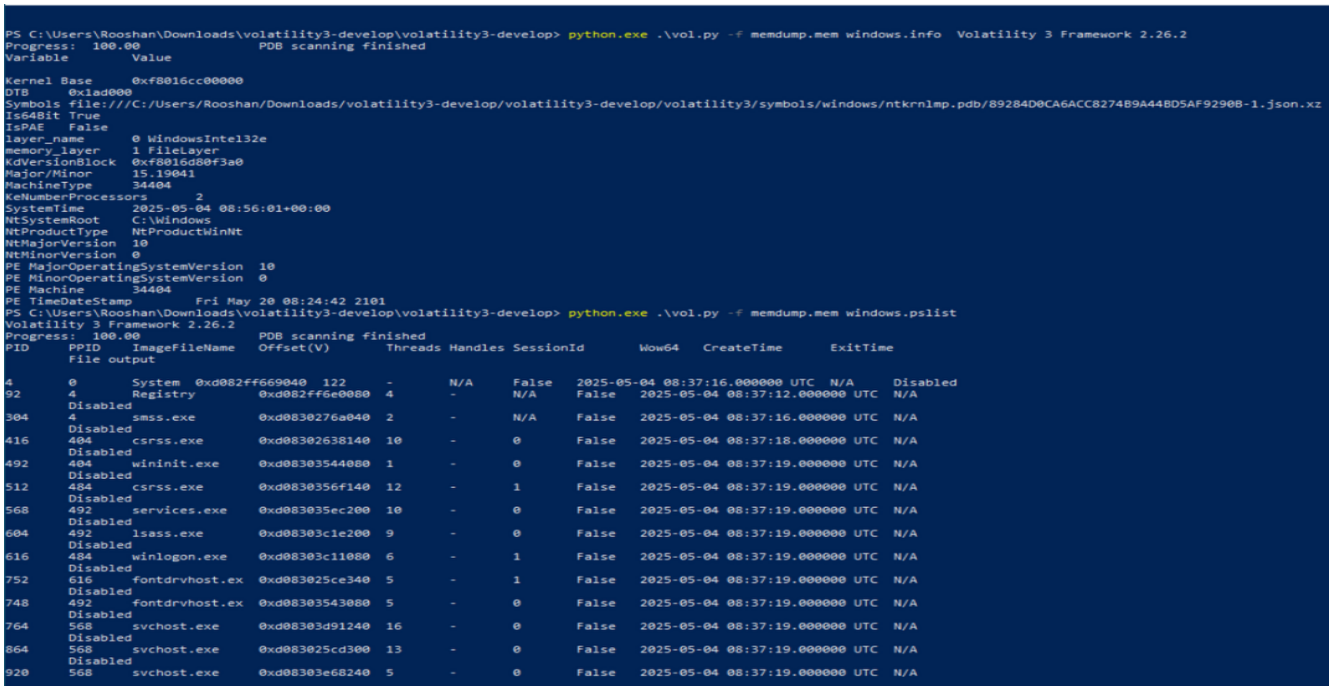

Figure 18: Windows Info

```
PS C:\Users\Rooshan\Downloads\volatility3-develop\volatility3-develop> python.exe .\vol.py -f memdump.mem windows.psscan --pid 3604
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

3604    2704    @WanaDecryptor  0xd082ff77f080  1       -       1       True    2025-05-04 08:50:09.000000 UTC  N/A     Disabled
PS C:\Users\Rooshan\Downloads\volatility3-develop\volatility3-develop>
```

Figure 19: Scanning Process ID: 3604

```
PS C:\Users\Rooshan\Downloads\volatility3-develop\volatility3-develop> python.exe .\vol.py -f memdump.mem windows.handles --pid 6648
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name

6648    WannaCrypt0r.e  0xd08305da7560  0x4     Event   0x1f0003        -
6648    WannaCrypt0r.e  0xd08305da7760  0x8     Event   0x1f0003        -
6648    WannaCrypt0r.e  0xd08306a9c530  0xc     WaitCompletionPacket    0x1     -
6648    WannaCrypt0r.e  0xd083050983c0  0x10    IoCompletion    0x1f0003        -
6648    WannaCrypt0r.e  0xd08304843fa00  0x14    TpWorkerFactory 0xf00ff -
6648    WannaCrypt0r.e  0xd08305e8ad50  0x18    IRTimer 0x100002        -
6648    WannaCrypt0r.e  0xd08306a9d230  0x1c    WaitCompletionPacket    0x1     -
6648    WannaCrypt0r.e  0xd08305e8df40  0x20    IRTimer 0x100002        -
6648    WannaCrypt0r.e  0xd08306a9cef0  0x24    WaitCompletionPacket    0x1     -
6648    WannaCrypt0r.e  0xd0830509bd90  0x28    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd0830509c110  0x2c    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050a5a30  0x30    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xa88b6cd7b740  0x34    Directory       0x3     KnownDlls
6648    WannaCrypt0r.e  0xd08305da7ee0  0x38    Event   0x1f0003        -
6648    WannaCrypt0r.e  0xd08305da7960  0x3c    Event   0x1f0003        -
6648    WannaCrypt0r.e  0xd0830884e270  0x40    File    0x100020        \Device\HarddiskVolume3\Windows
6648    WannaCrypt0r.e  0xd08305da80e0  0x44    Event   0x1f0003        -
6648    WannaCrypt0r.e  0xa88b6cd7a0c0  0x48    Directory       0x3     KnownDlls32
6648    WannaCrypt0r.e  0xd08305da70e0  0x4c    Event   0x1f0003        -
6648    WannaCrypt0r.e  0xd08306a9ac00  0x50    WaitCompletionPacket    0x1     -
6648    WannaCrypt0r.e  0xd083050a8500  0x54    IoCompletion    0x1f0003        -
6648    WannaCrypt0r.e  0xd08304614060  0x58    TpWorkerFactory 0xf00ff -
6648    WannaCrypt0r.e  0xd08305e8e6b0  0x5c    IRTimer 0x100002        -
6648    WannaCrypt0r.e  0xd08306a9dd90  0x60    WaitCompletionPacket    0x1     -
6648    WannaCrypt0r.e  0xd08305e8d280  0x64    IRTimer 0x100002        -
6648    WannaCrypt0r.e  0xd08306a9df30  0x68    WaitCompletionPacket    0x1     -
6648    WannaCrypt0r.e  0xd083050a7b70  0x6c    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050a72b0  0x70    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050aa810  0x74    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xa88b6cd7a0c0  0x78    Directory       0x3     KnownDlls32
6648    WannaCrypt0r.e  0xd08305da7be0  0x7c    Event   0x1f0003        -
6648    WannaCrypt0r.e  0xd08305da7c60  0x80    Event   0x1f0003        -
6648    WannaCrypt0r.e  0xd08308851dd0  0x84    File    0x100020        \Device\HarddiskVolume3\Users\Rooshan\Downloads\WannaCry
6648    WannaCrypt0r.e  0xd083050ab990  0x88    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd08308754390  0x8c    Mutant  0x1f0001        SM0:6648:168:WilStaging_02
6648    WannaCrypt0r.e  0xd08304ca0420  0x90    ALPC Port       0x1f0001        -
6648    WannaCrypt0r.e  0xa88b6cf54c00  0x94    Directory       0xf     BaseNamedObjects
6648    WannaCrypt0r.e  0xd08305b23b10  0x98    Semaphore       0x1f0003        SM0:6648:168:WilStaging_02_p0
6648    WannaCrypt0r.e  0xd083050aab90  0x9c    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050abb50  0xa0    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd08305bc4060  0xa4    TpWorkerFactory 0xf00ff -
6648    WannaCrypt0r.e  0xd083050ab370  0xa8    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050ac170  0xac    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050abc30  0xb0    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050aac70  0xb4    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050ab0d0  0xb8    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050abd10  0xbc    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050abdf0  0xc0    EtwRegistration 0x804   -
6648    WannaCrypt0r.e  0xd083050aa640  0xc4    IoCompletion    0x1f0003        -
```

Figure 20: Windows Handle Process ID: 6648

- Lists mixed results—vendors like Arcabit, BitDefender, and Gridinsoft flag it as a Trojan or generic malware, while others (e.g., Avast, ESET-NOD32) report no detection.

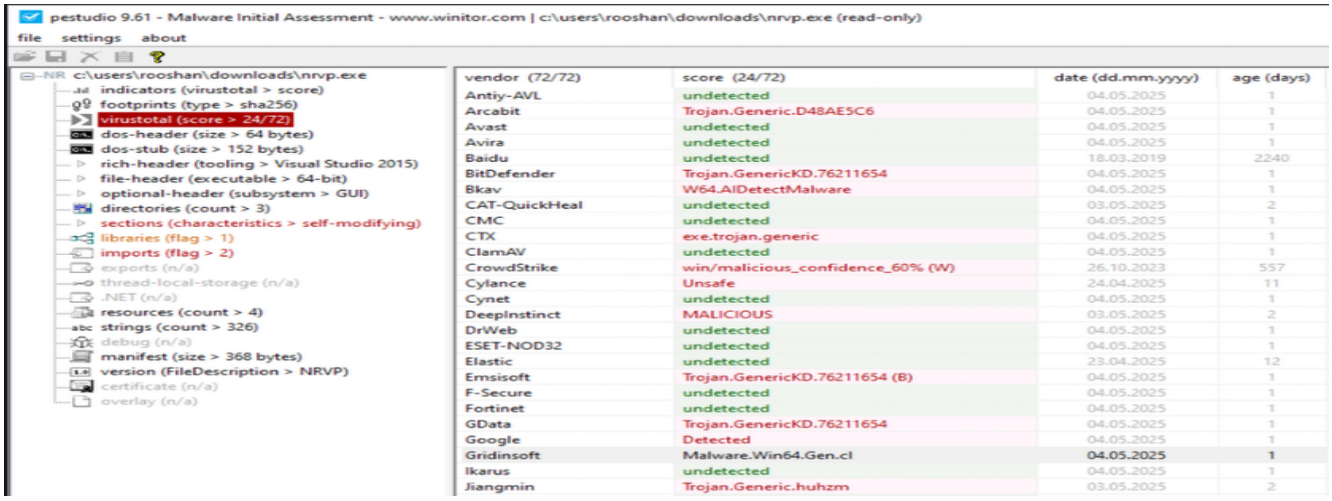

Figure 21: Pestudio

- Multiple vendors classify it as a Trojan (e.g., Trojan.GenericK0.76211654 by BitDefender, Trojan.Generic.hulvam by Jiangmin).

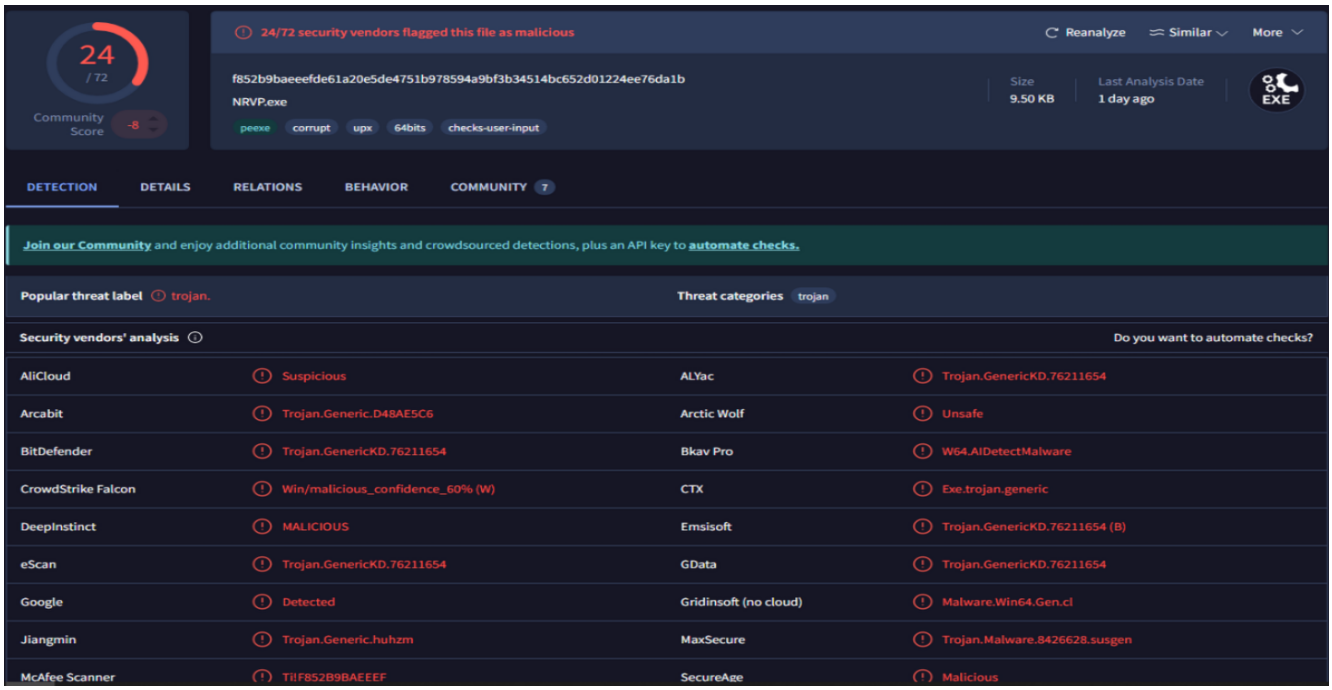

Figure 22: Virus Total

3 Challenges

3.1 Environment Setup Issues

Setting up a secure, isolated environment was crucial to avoid spreading the ransomware. This required strict precautions and ensuring that the VM had no external network connectivity.

3.2 Ransomware Execution Safety

Disabling Windows Defender posed a risk of the ransomware executing undetected. To mitigate this, the VM was isolated, and only the necessary tools were used to analyze the malware.

3.3 Tool Compatibility

Ensuring that the forensics tools like FTK Imager, Autopsy, and Volatility were compatible with the Windows 10 VM was challenging. This required proper configuration and regular updates to the tools.

4 Conclusion and Future Improvements

4.1 Summary of Findings

The forensic analysis revealed the presence of WannaDecryptor.exe in the system, indicating that the ransomware had successfully encrypted the files. Memory forensics revealed that the ransomware used a specific process (or4qtckT.exe) to delete files and propagate across the system.

4.2 Limitations

The main limitation of the project was the inability to test the ransomware in a live environment due to safety concerns. Furthermore, due to the isolated nature of the environment, the attack could not be fully replicated across a larger network.

4.3 Suggestions for Future Improvements

Future improvements could involve conducting the analysis on a larger network of machines to simulate real-world conditions more accurately. Additionally, automating the detection of ransomware using behavioral analysis could enhance proactive defense mechanisms.