

# 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

<b>1</b>	<b>Introduction and Problem Statement</b>	<b>2</b>
1.1	What is ransomware? . . . . .	2
1.2	Why is forensic analysis critical? . . . . .	2
1.3	Scope and objectives of your project . . . . .	2
<b>2</b>	<b>Implementation details</b>	<b>2</b>
2.1	Environment setup . . . . .	2
2.2	Simulated attack description . . . . .	3
2.3	Step-by-step forensic investigation . . . . .	4
2.4	Tools used and how . . . . .	9
<b>3</b>	<b>Challenges</b>	<b>13</b>
3.1	Environment Setup Issues . . . . .	13
3.2	Ransomware Execution Safety . . . . .	13
3.3	Tool Compatibility . . . . .	13
<b>4</b>	<b>Conclusion and Future Improvements</b>	<b>14</b>
4.1	Summary of Findings . . . . .	14
4.2	Limitations . . . . .	14
4.3	Suggestions for Future Improvements . . . . .	14

# 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.

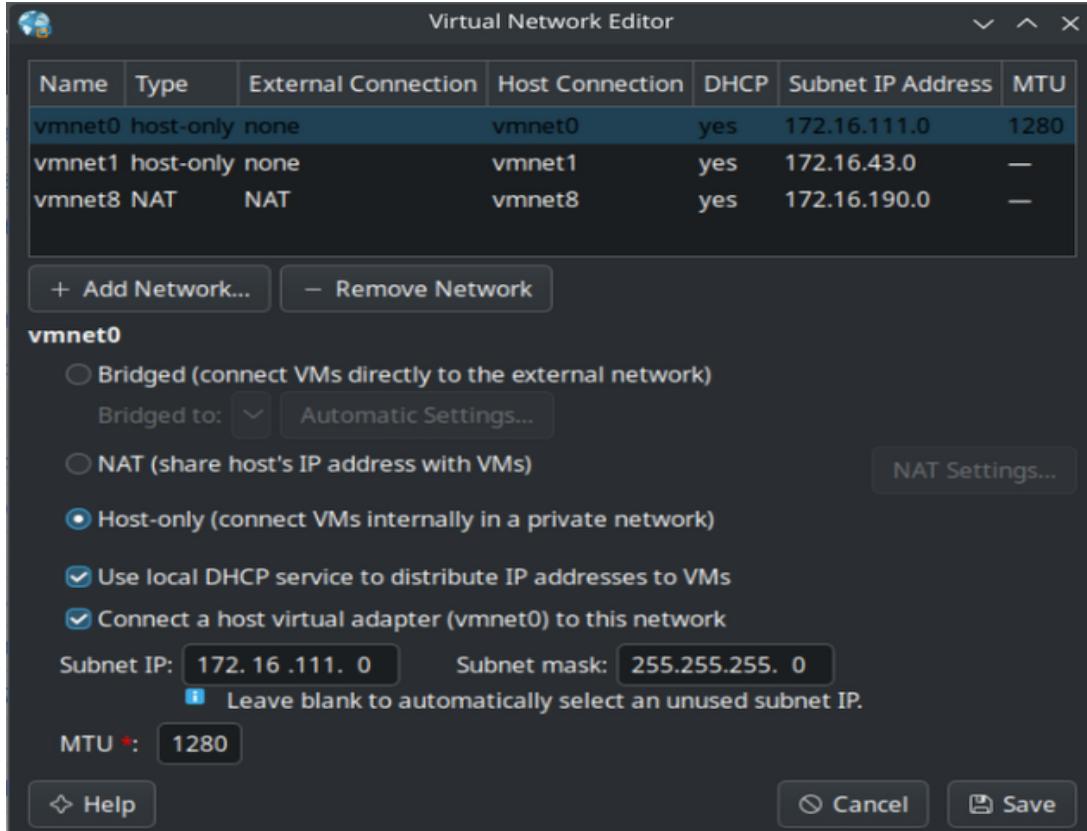


Figure 1: VM Host Only

## 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.

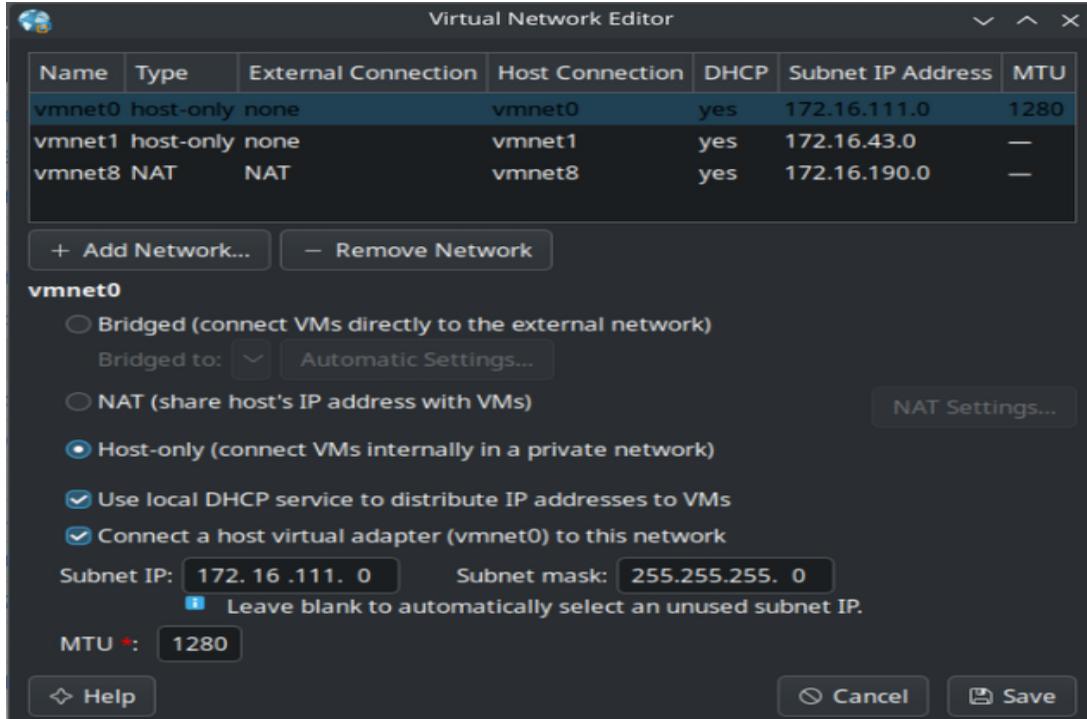


Figure 3: VM Host Only

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.

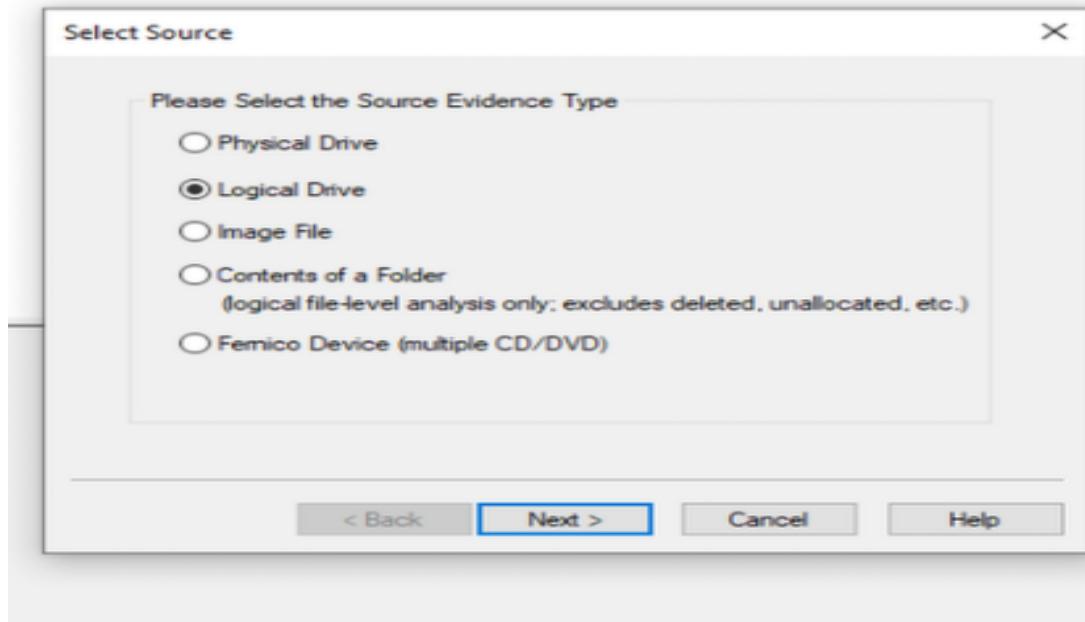


Figure 5: Select Source on FTK Imager

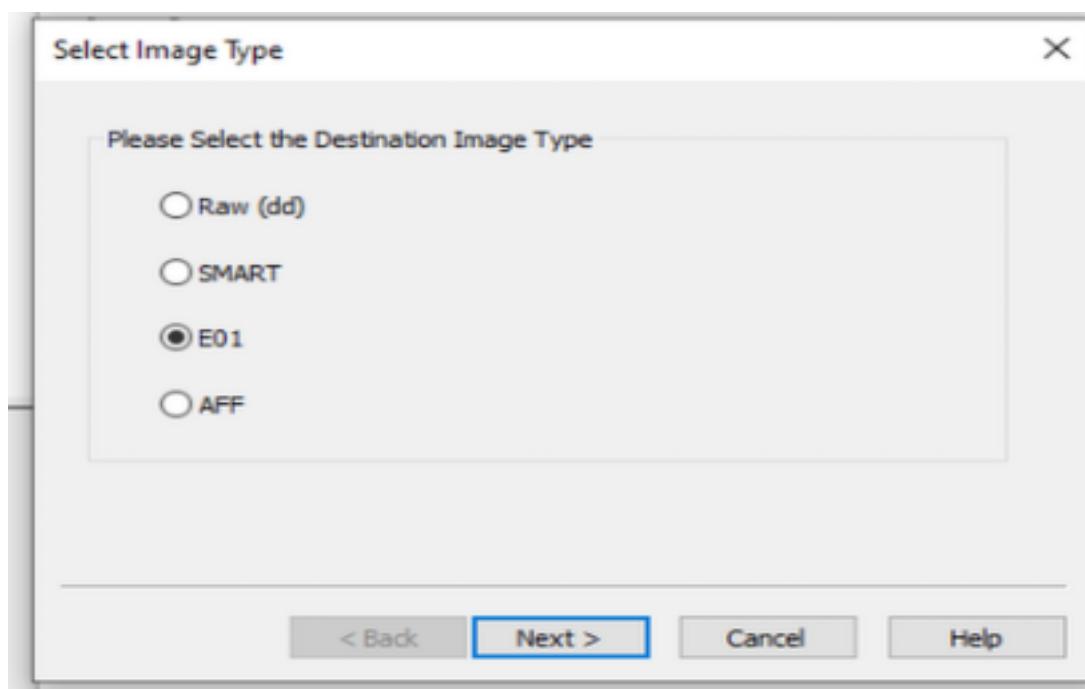


Figure 6: Select Image Type on FTK Imager

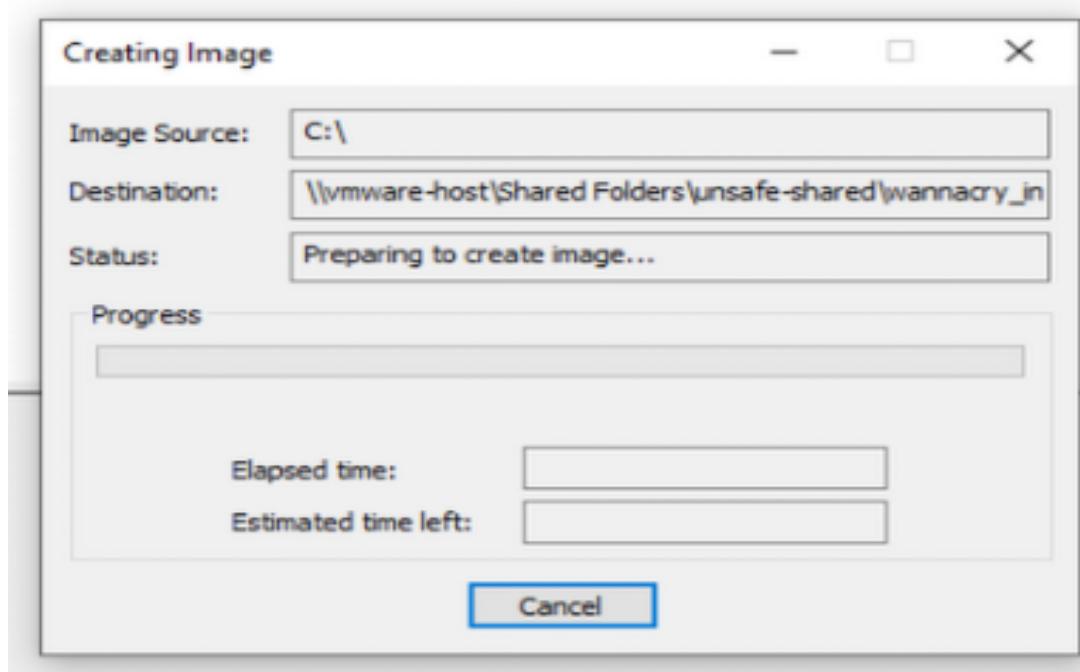


Figure 7: Creating Image on FTK Imager

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



Figure 8: Autopsy

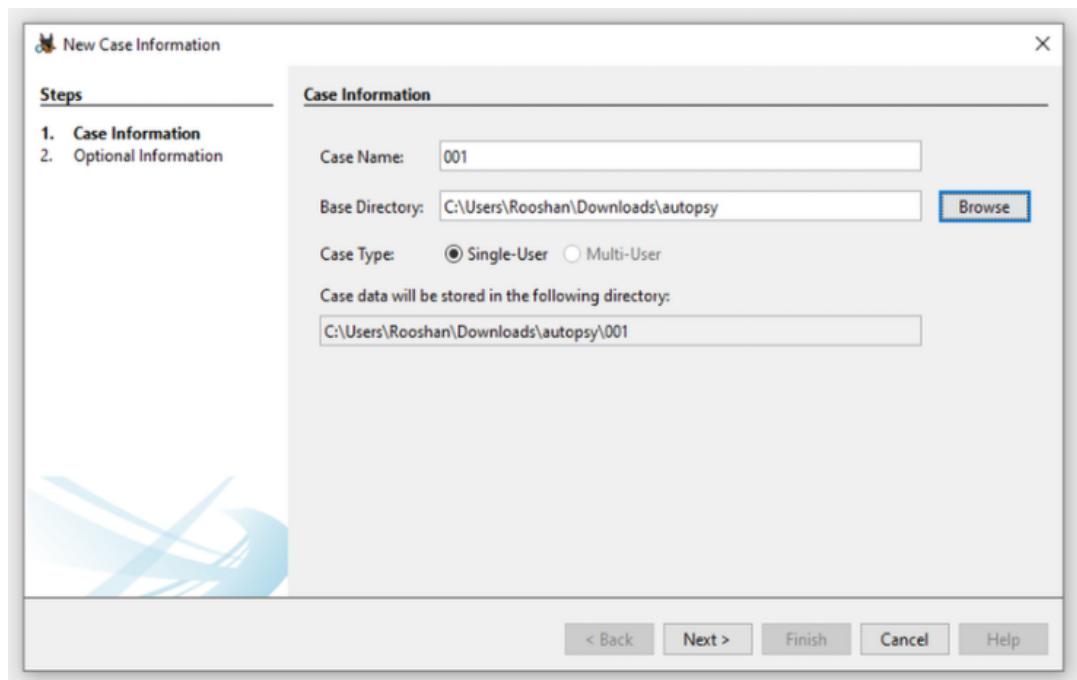


Figure 9: Case Name

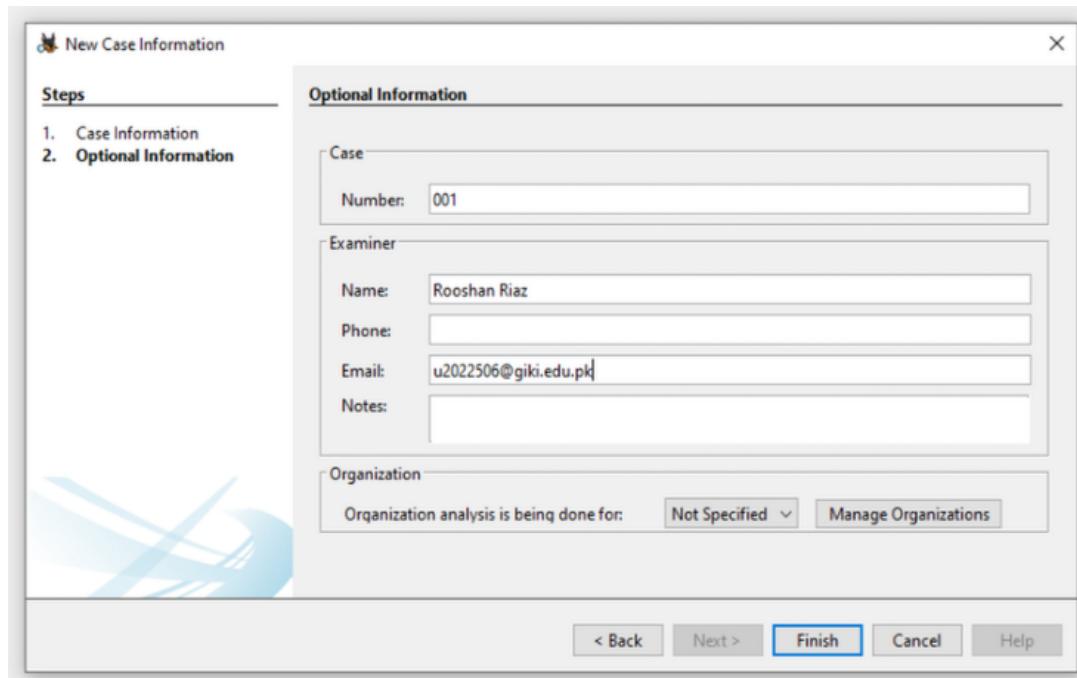


Figure 10: Case Number

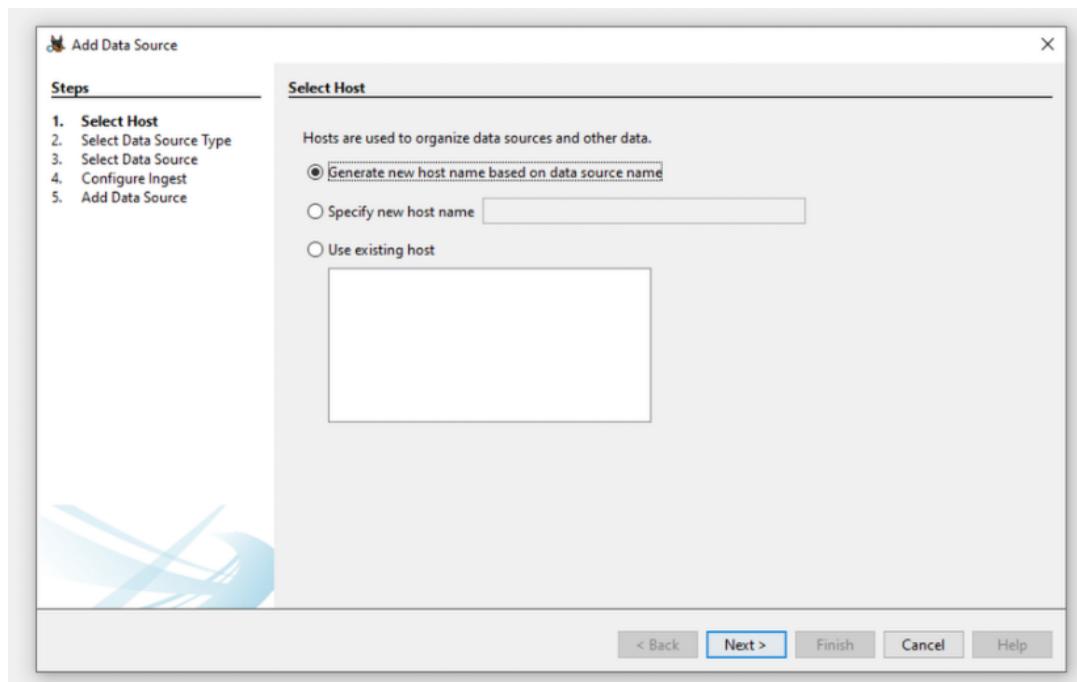


Figure 11: Select Host

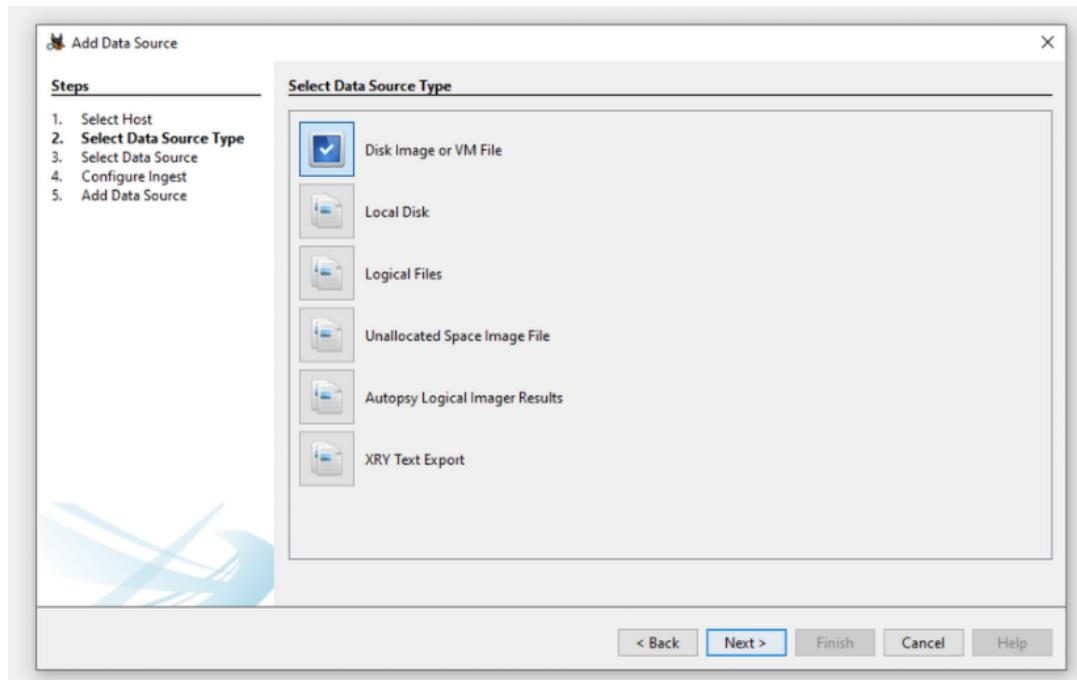


Figure 12: Add Data Source Type

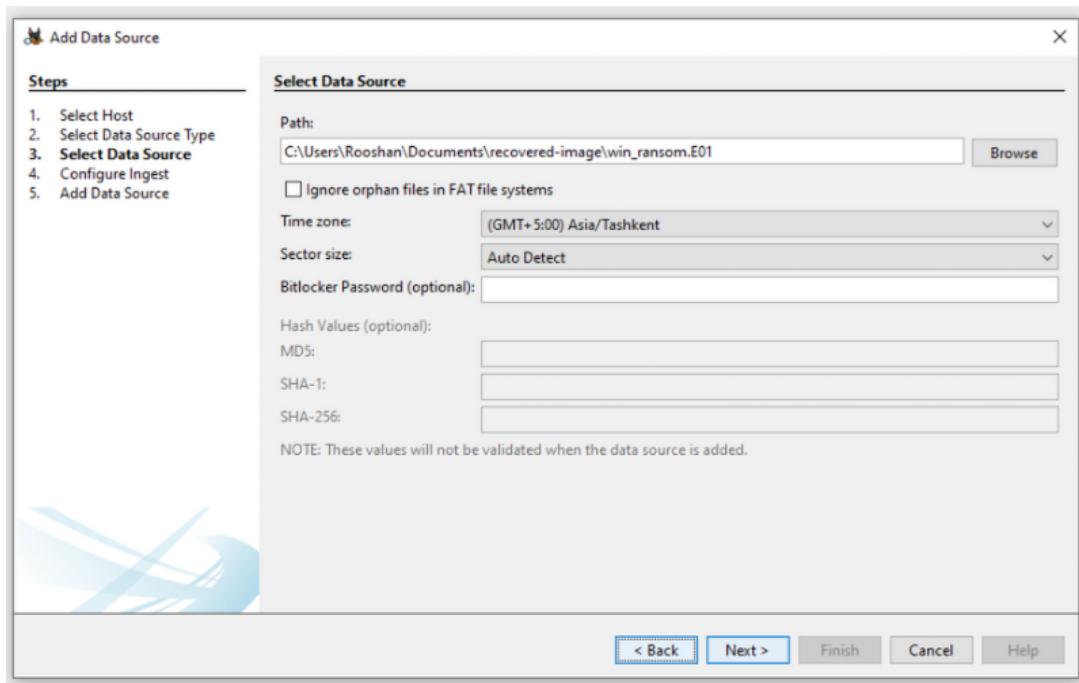


Figure 13: Select Data Source



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.

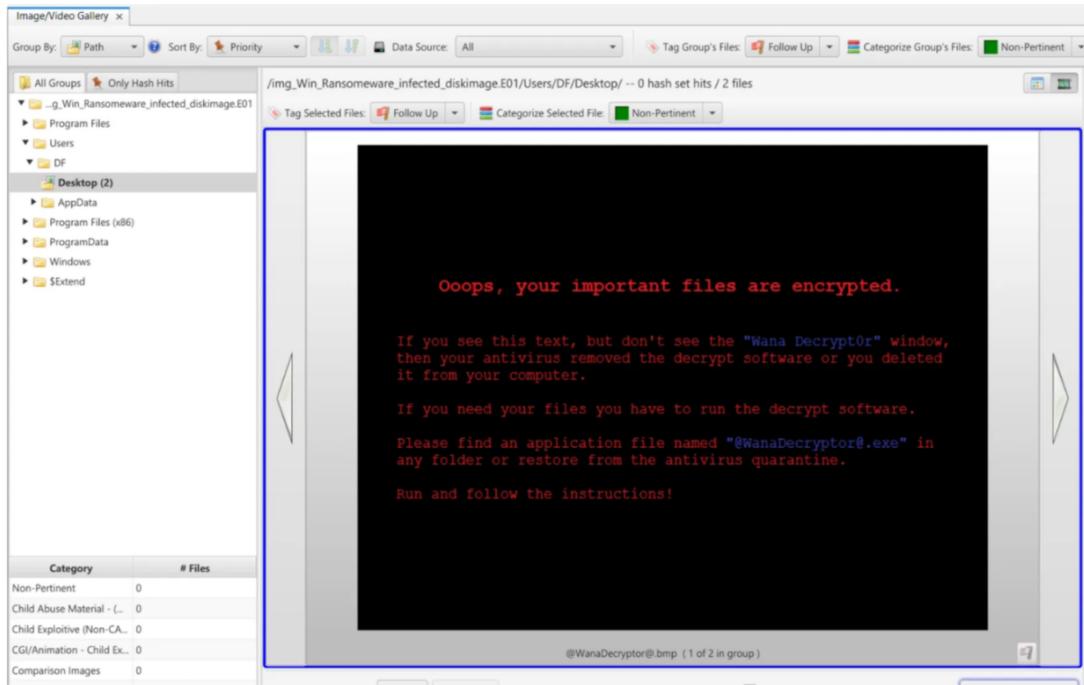


Figure 15: Image Gallery

The screenshot shows the Autopsy Forensic Browser interface. The left sidebar shows various data sources and file types, including 'File Types' (e.g., Images, Videos, Audio, Archives, Databases, Documents, Executable, DLLs, BAT files, CMD files, COM files), 'MB File Size', and 'Data Artifacts' (e.g., Chromium Extensions, Installed Programs, Operating System Information, Recent Documents, Run Programs, Shell Bags, USB Device Attached, Web Bookmarks, Web Cache, Web Cookies, Web Downloads). The main pane displays a table of files found, with 'WannaDecryptor.exe' highlighted. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. The bottom pane shows an 'Analysis Results' section with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, and others. A detailed view of the file '7z.exe' is shown, stating 'This program cannot be run in DOS mode.'

Figure 16: Listing of Files

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

1960	764	RuntimeBroker	0xd083061c50c0	5	-	1	False	2025-05-04 08:38:38.000000 UTC	N/A
7264	568	svchost.exe	0xd083045260c0	2	-	0	False	2025-05-04 08:38:45.000000 UTC	N/A
8156	764	RuntimeBroker	0xd08304550300	1	-	1	False	2025-05-04 08:38:49.000000 UTC	N/A
6212	764	ApplicationFrm	0xd083063f7340	8	-	1	False	2025-05-04 08:38:50.000000 UTC	N/A
1916	764	MWAHHost.exe	0xd083063f6080	25	-	1	False	2025-05-04 08:38:50.000000 UTC	N/A
8440	568	svchost.exe	0xd0830673240	3	-	0	False	2025-05-04 08:38:53.000000 UTC	N/A
6692	568	OneDrive.exe	0xd083068d1080	25	-	1	True	2025-05-04 08:39:00.000000 UTC	N/A
8952	1996	audiogd.exe	0xd083064e4080	5	-	0	False	2025-05-04 08:39:03.000000 UTC	N/A
1976	568	SgrmBroker.exe	0xd08305ce62c0	7	-	0	False	2025-05-04 08:39:22.000000 UTC	N/A
8668	568	svchost.exe	0xd08306675300	1	-	0	False	2025-05-04 08:39:22.000000 UTC	N/A
8628	568	svchost.exe	0xd08305a0a080	9	-	0	False	2025-05-04 08:39:22.000000 UTC	N/A
8780	568	svchost.exe	0xd083065c10c0	8	-	0	False	2025-05-04 08:39:22.000000 UTC	N/A
1604	568	svchost.exe	0xd08305859240	7	-	1	False	2025-05-04 08:39:23.000000 UTC	N/A
7880	2704	msedge.exe	0xd083057d1080	0	-	1	False	2025-05-04 08:40:00.000000 UTC	2025-05-04 08:41:52.000000 UTC
8036	7880	msedge.exe	0xd08305591080	0	-	1	False	2025-05-04 08:40:01.000000 UTC	2025-05-04 08:41:52.000000 UTC
7956	764	TextInputHost	0xd0830669d080	10	-	1	False	2025-05-04 08:40:25.000000 UTC	N/A
1716	568	svchost.exe	0xd083060d8340	2	-	0	False	2025-05-04 08:43:24.000000 UTC	N/A
488	568	svchost.exe	0xd08304ca7080	2	-	0	False	2025-05-04 08:45:16.000000 UTC	N/A
7248	3576	chrome.exe	0xd083060d0080	0	-	1	False	2025-05-04 08:45:19.000000 UTC	2025-05-04 08:46:06.000000 UTC
8592	568	svchost.exe	0xd083043ad080	3	-	0	False	2025-05-04 08:46:09.000000 UTC	N/A
7684	764	dllhost.exe	0xd08303ef4080	7	-	1	False	2025-05-04 08:48:02.000000 UTC	N/A
5132	568	svchost.exe	0xd0830507e080	3	-	0	False	2025-05-04 08:48:05.000000 UTC	N/A
9132	568	svchost.exe	0xd083068d080	1	-	0	False	2025-05-04 08:48:30.000000 UTC	N/A
2868	568	svchost.exe	0xd0830569a080	4	-	0	False	2025-05-04 08:48:59.000000 UTC	N/A
6828	568	svchost.exe	0xd08305753080	3	-	0	False	2025-05-04 08:48:59.000000 UTC	N/A
6648	2704	WannaCrypt0r.e	0xd083049be080	7	-	1	True	2025-05-04 08:49:43.000000 UTC	N/A
2320	6648	@WanaDecryptor	0xd08304ac0800	2	-	1	True	2025-05-04 08:49:46.000000 UTC	N/A
2336	2320	taskhsvc.exe	0xd08304c2f080	2	-	1	True	2025-05-04 08:49:47.000000 UTC	N/A
4696	2336	conhost.exe	0xd08305179080	4	-	1	False	2025-05-04 08:49:47.000000 UTC	N/A
2156	988	msedge.exe	0xd08304d20080	0	-	1	False	2025-05-04 08:50:01.000000 UTC	2025-05-04 08:50:03.000000 UTC
3604	2704	@WanaDecryptor	0xd082ff77f080	1	-	1	True	2025-05-04 08:50:09.000000 UTC	N/A
		Disabled							

Figure 17: WannaDecryptor

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

PS C:\Users\Rooshan\Downloads\volatility3-develop\volatility3-develop> python.exe .\vol.py -f memdump.mem windows.info	Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished	
Variable Value	
Kernel Base 0xf8016cc00000	
DTB 0x1ad000	
Symbols file:///C:/Users/Rooshan/Downloads/volatility3-develop/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb/89284D0cA6ACC827489A448D5AF9290B-1.json.gz	
Is64Bit True	
IsPAE False	
layer_number 0 WindowsIntel32e	
memory_layer 1 Filelayer	
KdVersionBlock 0xf8016d80f3a0	
Major/Minor 15.19041	
MachineType 34404	
KeNumberProcessors 2	
SYNTHETIC 2025-05-04 08:56:01+00:00	
NtSystemRoot C:\Windows	
NtProductType NtProductWinNt	
NtMajorVersion 10	
NtMinorVersion 0	
PE MajorOperatingSystemVersion 10	
PE MinorOperatingSystemVersion 0	
PE Machine 34404	
PE TimeStamp Fri May 20 08:24:42 2101	
PS C:\Users\Rooshan\Downloads\volatility3-develop\volatility3-develop> python.exe .\vol.py -f memdump.mem windows.pslist	
Volatility 3 Framework 2.26.2	
Progress: 100.00 PDB scanning finished	
PID PPID ImageFileName Offset(V)	Threads Handles SessionId Wow64 CreateTime ExitTime
4 0 System 0xd082ff669040 122 - N/A False 2025-05-04 08:37:16.000000 UTC N/A Disabled	
92 4 Registry 0xd082ff65e0800 4 - N/A False 2025-05-04 08:37:12.000000 UTC N/A	
304 4 smss.exe 0xd0830276a040 2 - N/A False 2025-05-04 08:37:16.000000 UTC N/A	
416 404 csrss.exe 0xd0830263b140 10 - 0 False 2025-05-04 08:37:18.000000 UTC N/A	
492 404 wininit.exe 0xd08303544080 1 - 0 False 2025-05-04 08:37:19.000000 UTC N/A	
512 484 Csrss.exe 0xd0830356f140 12 - 1 False 2025-05-04 08:37:19.000000 UTC N/A	
568 492 services.exe 0xd083035ec200 10 - 0 False 2025-05-04 08:37:19.000000 UTC N/A	
604 492 lsass.exe 0xd083031c1e200 9 - 0 False 2025-05-04 08:37:19.000000 UTC N/A	
616 484 winlogon.exe 0xd08303c11080 6 - 1 False 2025-05-04 08:37:19.000000 UTC N/A	
752 616 fontdrvhost.ex 0xd083025ce340 5 - 1 False 2025-05-04 08:37:19.000000 UTC N/A	
748 492 fontdrvhost.ex 0xd08303543080 5 - 0 False 2025-05-04 08:37:19.000000 UTC N/A	
764 568 svchost.exe 0xd08303d91240 16 - 0 False 2025-05-04 08:37:19.000000 UTC N/A	
864 568 svchost.exe 0xd083025cd300 13 - 0 False 2025-05-04 08:37:19.000000 UTC N/A	
920 568 svchost.exe 0xd08303e68240 5 - 0 False 2025-05-04 08:37:19.000000 UTC N/A	

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  0xd08305da7560 0x8  Event 0x1f0003  -
6648  WannaCrypt0r.e  0xd08306aa9c50 0x1c  MmCompletionPacket 0x1  -
6648  WannaCrypt0r.e  0xd083050983c0 0x10  IoCompletion 0x1f0003  -
6648  WannaCrypt0r.e  0xd0830443fa00 0x14  ThreadPoolFactory 0xf00ff  -
6648  WannaCrypt0r.e  0xd08305ea8d50 0x18  IRTimer 0x100002  -
6648  WannaCrypt0r.e  0xd08306aa9d230 0x1c  WaitCompletionPacket 0x1  -
6648  WannaCrypt0r.e  0xd083058df40 0x20  IRTimer 0x100002  -
6648  WannaCrypt0r.e  0xd08306aa9cef0 0x24  WaitCompletionPacket 0x1  -
6648  WannaCrypt0r.e  0xd0830509b90 0x28  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xd0830509b90 0x2c  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xd0830509b90 0x30  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xa88b6cd7a9c0 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  0xd08305d40e0 0x44  Event 0x1f0003  -
6648  WannaCrypt0r.e  0xa88b6cd7a9c0 0x48  Directory 0x3  KnownDlls32
6648  WannaCrypt0r.e  0xd08305da77e0 0x4c  Event 0x1f0003  -
6648  WannaCrypt0r.e  0xd08305da77e0 0x50  MmCompletionPacket 0x1  -
6648  WannaCrypt0r.e  0xd083050a8500 0x54  IoCompletion 0x1f0003  -
6648  WannaCrypt0r.e  0xd08304614060 0x58  ThreadPoolFactory 0xf00ff  -
6648  WannaCrypt0r.e  0xd083059e6b60 0x5c  IRTimer 0x100002  -
6648  WannaCrypt0r.e  0xd083059e6b60 0x60  WaitCompletionPacket 0x1  -
6648  WannaCrypt0r.e  0xd083059e6b60 0x64  IRTimer 0x100002  -
6648  WannaCrypt0r.e  0xd083059e6b60 0x68  WaitCompletionPacket 0x1  -
6648  WannaCrypt0r.e  0xd083059e6b60 0x70  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xd083059e6b60 0x74  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xa88b6cd7a9c0 0x78  Directory 0x3  KnownDlls32
6648  WannaCrypt0r.e  0xd08305da7c60 0x7c  Event 0x1f0003  -
6648  WannaCrypt0r.e  0xd08308851dd0 0x80  Event 0x1f0003  -
6648  WannaCrypt0r.e  0xd083050ab990 0x88  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xd08304cae20 0x90  Mutant 0x1f0001  SM0:6648:168:WilStaging_02
6648  WannaCrypt0r.e  0xd08304cae20 0x94  Directory 0x1  BaseNamedObjects
6648  WannaCrypt0r.e  0xd083050ab990 0x98  Semaphore 0x1f0003  SM0:6648:168:WilStaging_02_p0
6648  WannaCrypt0r.e  0xd083050ab990 0x9c  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xd083050ab990 0xa0  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xd083050ab990 0xa4  ThreadPoolFactory 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  0xd083050ab1d0 0xb8  EtwRegistration 0x804  -
6648  WannaCrypt0r.e  0xd083050abfd0 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.

pestudio 9.61 - Malware Initial Assessment - www.winitor.com   c:\users\rooshan\downloads\nrvp.exe (read-only)				
file	settings	about		
└─INR c:\users\rooshan\downloads\nrvp.exe				
└─ indicators (virustotal > score)				
└─ footprints (type = sha256)				
└─ virustotal (score > 24/72)				
└─ dos-header (size > 64 bytes)				
└─ dos-stub (size > 152 bytes)				
└─ rich-header (tooling > Visual Studio 2015)				
└─ file-header (executable > 64-bit)				
└─ optional-header (subsystem > GUI)				
└─ directories (count > 3)				
└─ sections (characteristics > self-modifying)				
└─ libraries (Flag > 1)				
└─ imports (Flag > 2)				
└─ exports (n/a)				
└─ thread-local-storage (n/a)				
└─ .NET (n/a)				
└─ resources (count > 4)				
└─ abc strings (count > 326)				
└─ debug (n/a)				
└─ manifest (size > 368 bytes)				
└─ version (FileDescription > NRVP)				
└─ certificate (n/a)				
└─ overlay (n/a)				
└─ vendor (72/72)				
Antiy-AVL	score (24/72)	undetected	04.05.2025	1
Arcabit		Trojan.Generic.D48AE5C6	04.05.2025	1
Avast		undetected	04.05.2025	1
Avira		undetected	04.05.2025	1
Baidu		undetected	18.03.2019	22:40
BitDefender		Trojan.GenericKD.76211654	04.05.2025	1
Bkav		W64.AIDetectMalware	04.05.2025	1
CAT-QuickHeal		undetected	03.05.2025	2
CMC		undetected	04.05.2025	1
ClamAV		undetected	04.05.2025	1
CrowdStrike		win/malicious_confidence_60% (W)	26.10.2023	557
Cylance		Unsafe	24.04.2025	11
Cynet		undetected	04.05.2025	1
DeepInstinct		MALICIOUS	03.05.2025	2
DrWeb		undetected	04.05.2025	1
ESET-NOD32		undetected	04.05.2025	1
Elastic		undetected	23.04.2025	12
Emsisoft		Trojan.GenericKD.76211654 (B)	04.05.2025	1
F-Secure		undetected	04.05.2025	1
Fortinet		undetected	04.05.2025	1
GData		Trojan.GenericKD.76211654	04.05.2025	1
Google		Detected	04.05.2025	1
Gridinsoft		Malware.Win64.Gen.cl	04.05.2025	1
Ikarus		undetected	04.05.2025	1
Jiangmin		Trojan.Generic.huhzm	03.05.2025	2

Figure 21: Pestudio

- Multiple vendors classify it as a Trojan (e.g., Trojan.GenericKD.76211654 by Bit-Defender, Trojan.Generic.hulvam by Jiangmin).

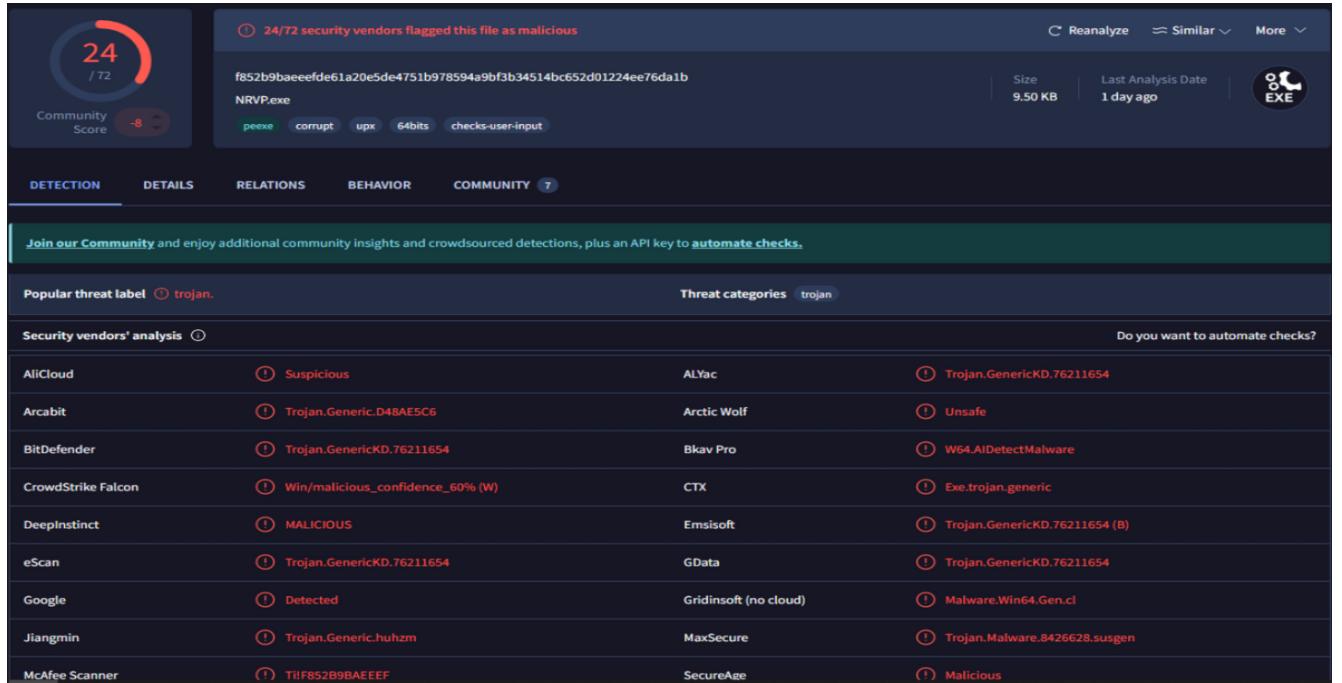


Figure 22: Virus Total

## 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.