8. The **Cleaning your PC...** wizard appears. Observe the progress bar and wait for it to complete.
9. After the cleaning completes, the **Your PC is feeling fresh!** wizard appears, as shown in the screenshot.

Figure 4.4.7: Cleaning complete wizard

You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.

10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.

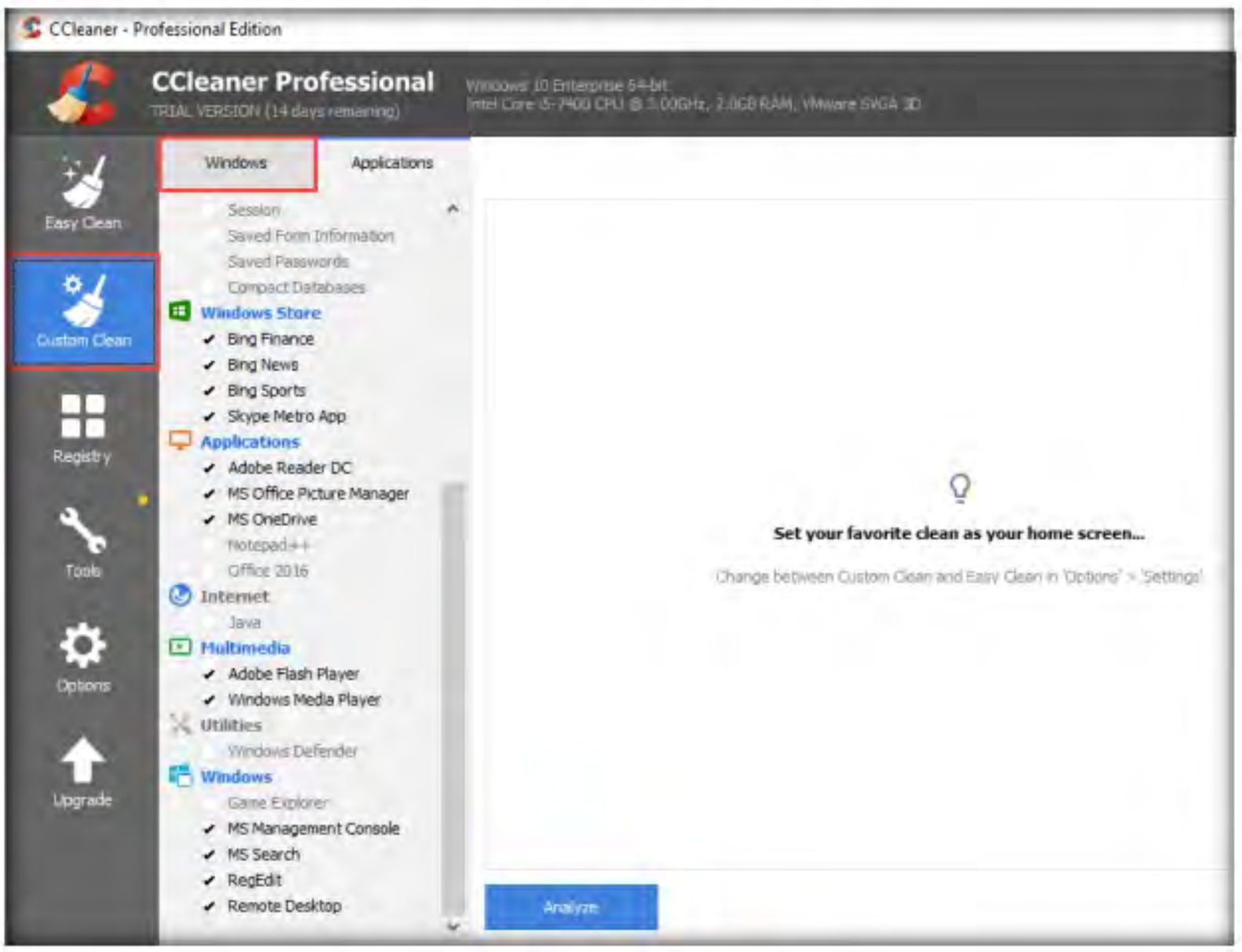


Figure 4.4.8: Custom Clean option

11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Malware Threats

Module 07

Malware Threats

Malware is malicious software that damages or disables computer systems and gives limited or full control of those systems to the malware creator for theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, and other software.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Malware poses a major security threat to information security. Malware writers explore new attack vectors to exploit vulnerabilities in information systems. This leads to ever more sophisticated malware attacks, including drive-by malware, "maladvertising" (or "malvertising") and advanced persistent threats. Although organizations try hard to defend themselves using comprehensive security policies and advanced anti-malware controls, the current trend indicates that malware applications are targeting "lower-hanging fruit"; these include unsecured smartphones, mobile applications, social media, and cloud services. This problem is further complicated, because of the challenges faced during threat prediction.

Assessing an organization's information system against malware threats is a major challenge today, because of the rapidly changing nature of malware threats. One needs to be well-versed in the latest developments in the field and understand the basic functioning of malware to select and implement the controls appropriate for an organization and its needs.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively select security controls to protect your information assets from malware threats.

Lab Objectives

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform malware analysis to determine the origin, functionality, and potential impact of a given type of malware
- Detect malware

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine

- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 180 Minutes

Overview of Malware

With the help of a malicious application (malware), an attacker gains access to stored passwords in a computer and is able to read personal documents, delete files, display pictures, or messages on the screen, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft and password stealing.

Programmers develop malware and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Lab Tasks

Note: Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

Attackers, as well as ethical hackers or pen testers, use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Gain Access to the Target System using Trojans	√	√	√
	1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan	√		√
	1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs		√	√
	1.3 Create a Server using the ProRat Tool		√	√
	1.4 Create a Trojan Server using Theef RAT Trojan		√	√
2	Infect the Target System using a Virus	√		√
	2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System	√		√
3	Perform Static Malware Analysis	√	√	√
	3.1 Perform Online Malware Scanning using VirusTotal	√		√
	3.2 Perform a Strings Search using BinText	√		√
	3.3 Identify Packaging and Obfuscation Methods using PEid		√	√
	3.4 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer		√	√
	3.5 Identify File Dependencies using Dependency Walker		√	√
	3.6 Perform Malware Disassembly using IDA and OllyDbg	√		√
4	Perform Dynamic Malware Analysis	√	√	√
	4.1 Perform Port Monitoring using TCPView and CurrPorts	√		√
	4.2 Perform Process Monitoring using Process Monitor	√		√
	4.3 Perform Registry Monitoring using Regshot and jv16 PowerTools		√	√
	4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)		√	√
	4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol		√	√

	4.6 Perform Installation Monitoring using Mirekusoft Install Monitor		√	√
	4.7 Perform Files and Folder Monitoring using PA File Sight		√	√
	4.8 Perform Device Drivers Monitoring using DriverView and Driver Booster		√	√
	4.9 Perform DNS Monitoring using DNSQuerySniffer		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Gain Access to the Target System using Trojans

A computer Trojan is a program with malicious or harmful code contained inside apparently harmless programming or data in such a way that the program can gain control and cause damage such as ruining the file allocation table on the hard disk.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Attackers use digital Trojan horses to trick the victim into performing a predefined action on a computer. Trojans are activated upon users' specific predefined actions, like unintentionally installing a piece of malicious software or clicking on a malicious link, and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and cause potentially immense damage. For example, users could download a file that appears to be a movie, but, when opened, it unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

Trojan horses work on the same level of privileges as victims. For example, if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks), once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase its level of access, even beyond the user running it. If successful, the Trojan could use the increased privileges to install other malicious code on the victim's machine.

An expert security auditor or ethical hacker needs to ensure that the organization's network is secure from Trojan attacks by finding machines vulnerable to these attacks and making sure that anti-virus tools are properly configured to detect such attacks.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Lab Objectives

- Gain control over a victim machine using the njRAT RAT Trojan
- Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs
- Create a server using the ProRat Tool
- Create a Trojan server using Theef RAT Trojan

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- njRAT RAT Trojan located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**
- SwayzCryptor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Crypters\SwayzCryptor**
- ProRat Tool located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**
- Theef located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Lab Duration

Time: 45 Minutes

Overview of Trojans

In Ancient Greek mythology, the Greeks won the Trojan War with the aid of a giant wooden horse that the Greeks built to hide their soldiers. The Greeks left the horse in front of the gates of Troy. The Trojans, thinking that it was a gift from the Greeks that they had left before apparently withdrawing from the war, brought the horse into their city. At night, the hidden Greek soldiers emerged from the wooden horse and opened the city's gates for their soldiers, who eventually destroyed the city of Troy.

Thus, taking its cue from this myth, a computer Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and cause damage such as ruining the file allocation table on your hard disk.

Lab Tasks

TASK 1

Gain Control over a Victim Machine using the njRAT RAT Trojan

Here, we will use the njRAT Trojan to gain control over a victim machine.

Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks.

Note: The versions of the created client or host and appearance of the website may differ from what it is in this lab. However, the actual process of creating the server and the client is the same, as shown in this lab.

Note: In this lab task, we will use the **Windows 10** (**10.10.10.10**) virtual machine as the attacker machine and the **Windows Server 2016** (**10.10.10.16**) virtual machine as the victim machine.

1. Turn on the **Windows 10** and **Windows Server 2016** victim machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.

Figure 1.1.1: Login window

TASK 1.1

Launch njRAT Trojan

The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. The **njRAT GUI** appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click **Start**.
5. In this lab, the default port number **5552** has been chosen.

Figure 1.1.2: njRAT GUI along with a njRAT pop-up

TASK 1.2

Create a Malware

6. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.

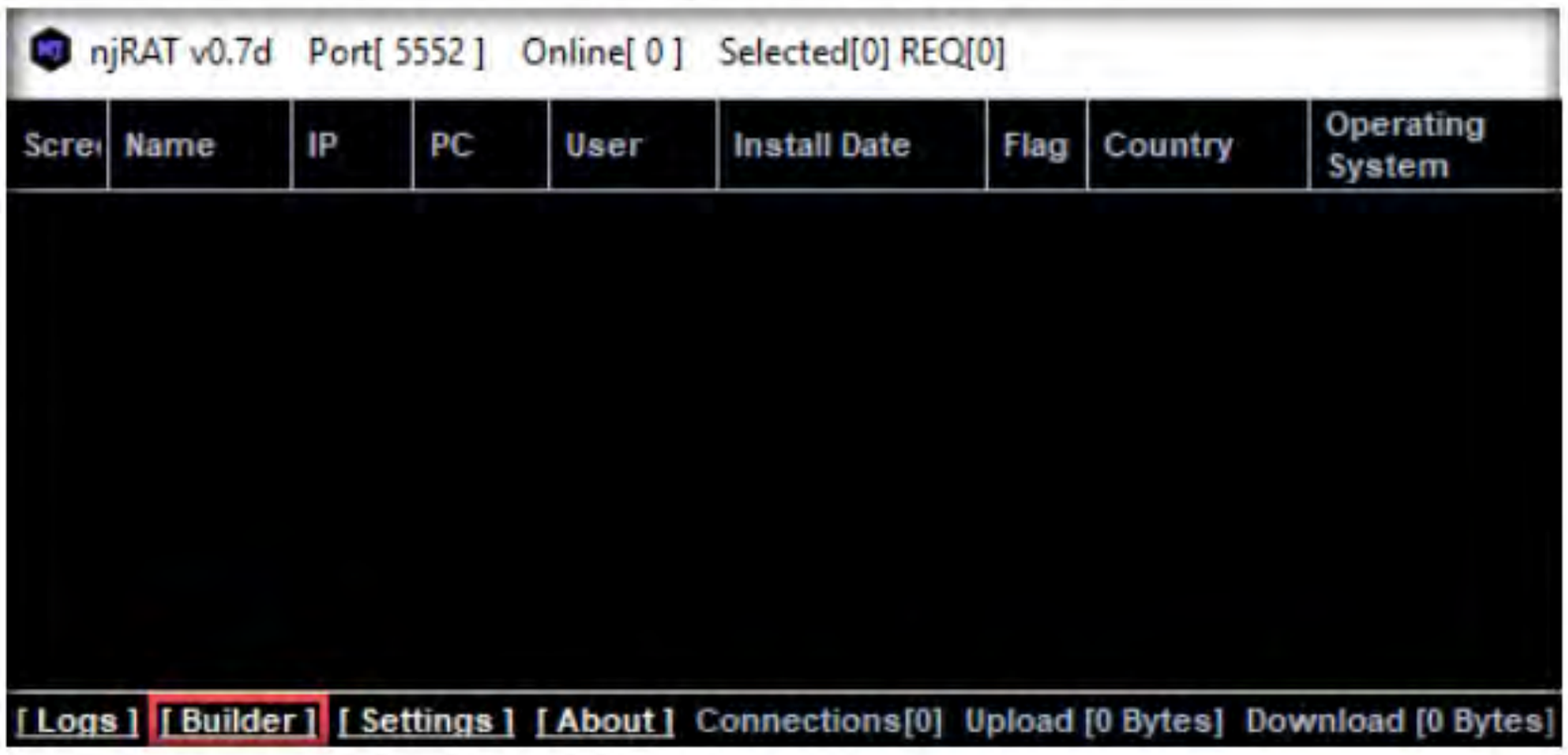


Figure 1.1.3: njRAT GUI

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

7. The **Builder** dialog-box appears; enter the IP address of the **Windows 10** (attacker machine) virtual machine in the **Host** field, check the options **Copy To StartUp** and **Registy StarUp**, leave the other settings to default, and click **Build**.

Note: In this lab, the IP address of the **Windows 10** virtual machine is **10.10.10.10**. This IP address might vary in your lab environment.

njRAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

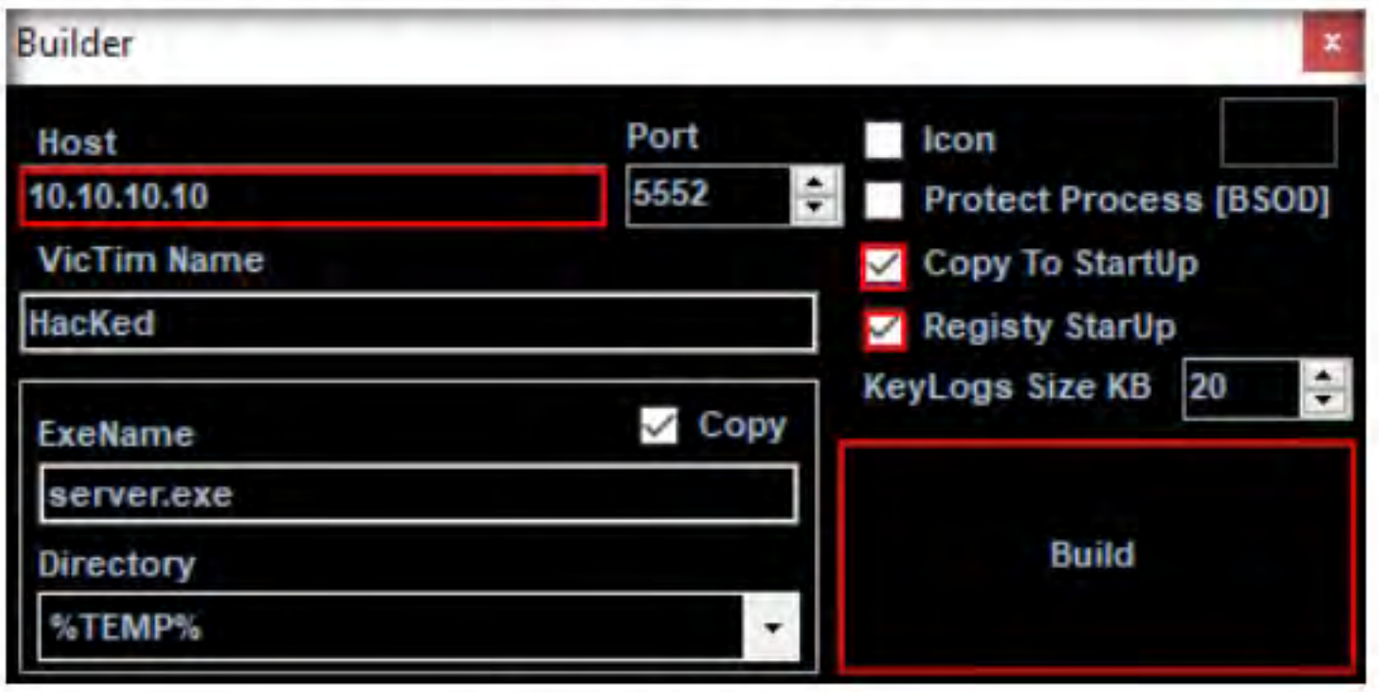


Figure 1.1.4: Builder dialog-box

8. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.
9. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.

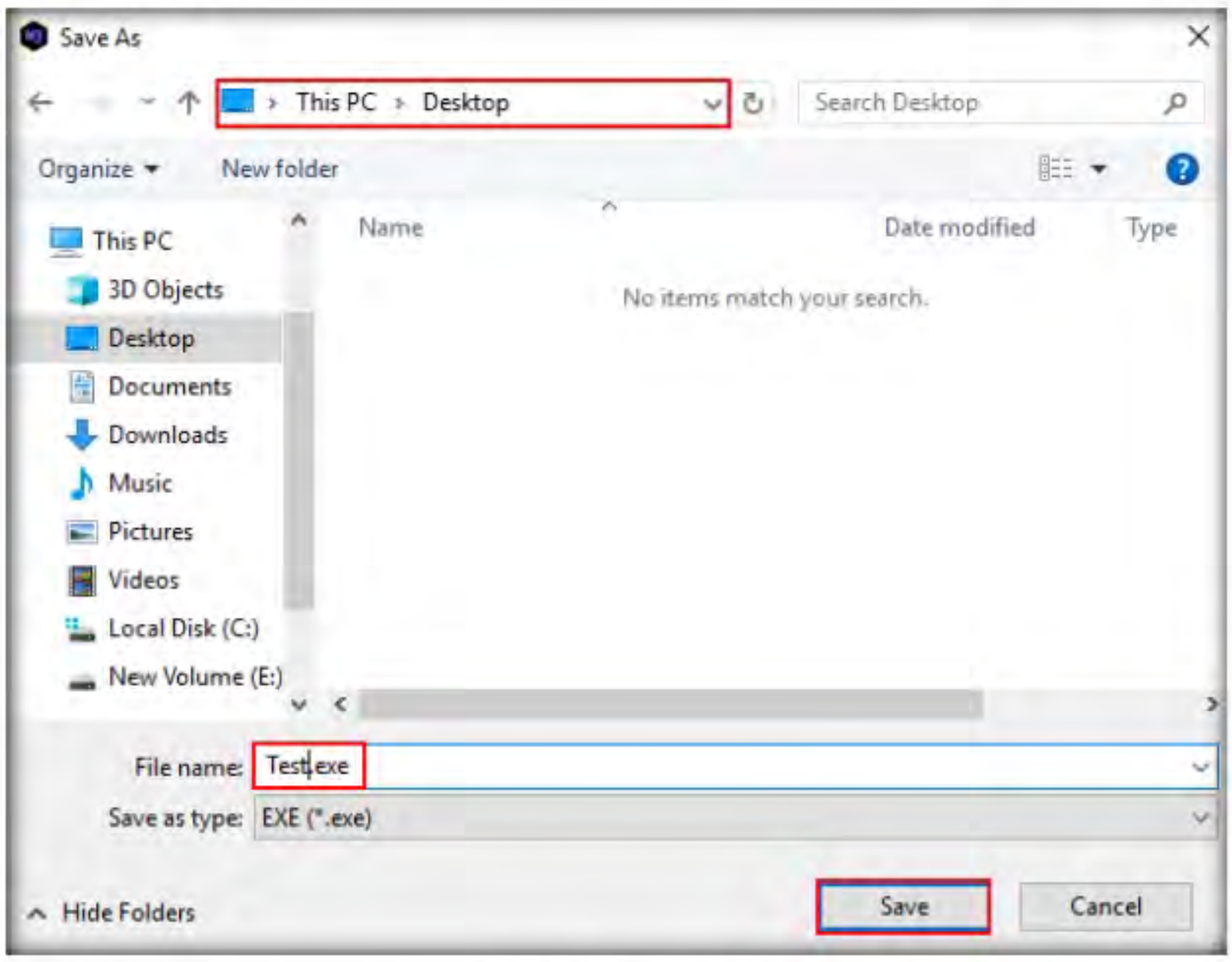


Figure 1.1.5: Save As dialog box

10. Once the server is created, the **DONE!** pop-up appears; click **OK**.

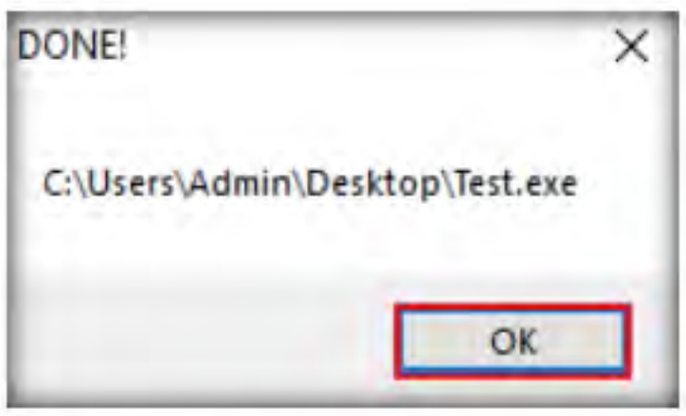


Figure 1.1.6: Server created successfully

11. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

Note: In this lab, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.

TASK 1.3

Execute the Server on Windows Server 2016

12. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

13. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2016**.
14. Here, you are acting both as an **attacker** who logs into the **Windows 10** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2016** virtual machine and downloads the server.
15. Double-click the server (**Test.exe**) to run this malicious executable.

Figure 1.1.7: Executing the server

16. Switch back to the **Windows 10** virtual machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 10** establishes a persistent connection with the victim machine, as shown in the screenshot.

Figure 1.1.8: Connection established successfully

TASK 1.4

Manipulate Files on Victim Machine

17. Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
18. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.
19. Right-click on the detected victim name and click **Manager**.

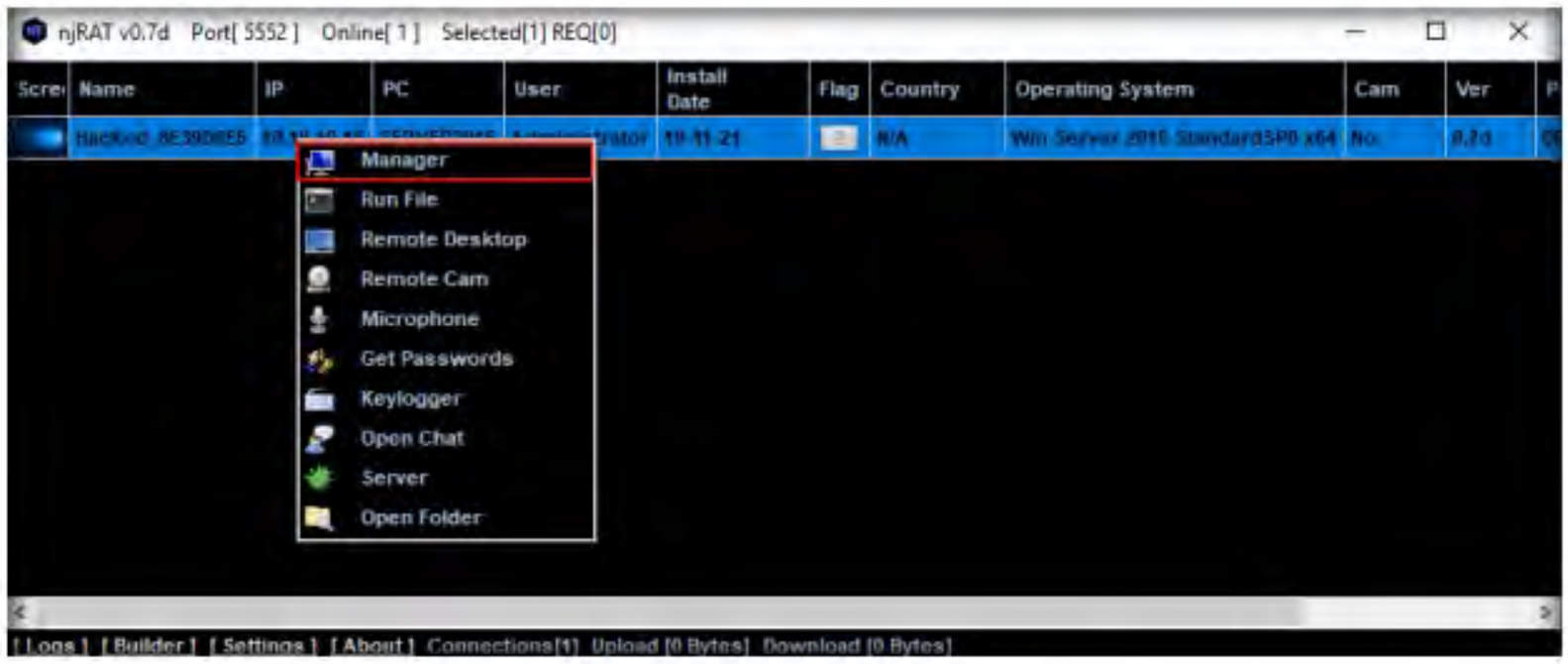


Figure 1.1.9: Managing the victim machine

20. The **manager** window appears with **File Manager** selected by default.

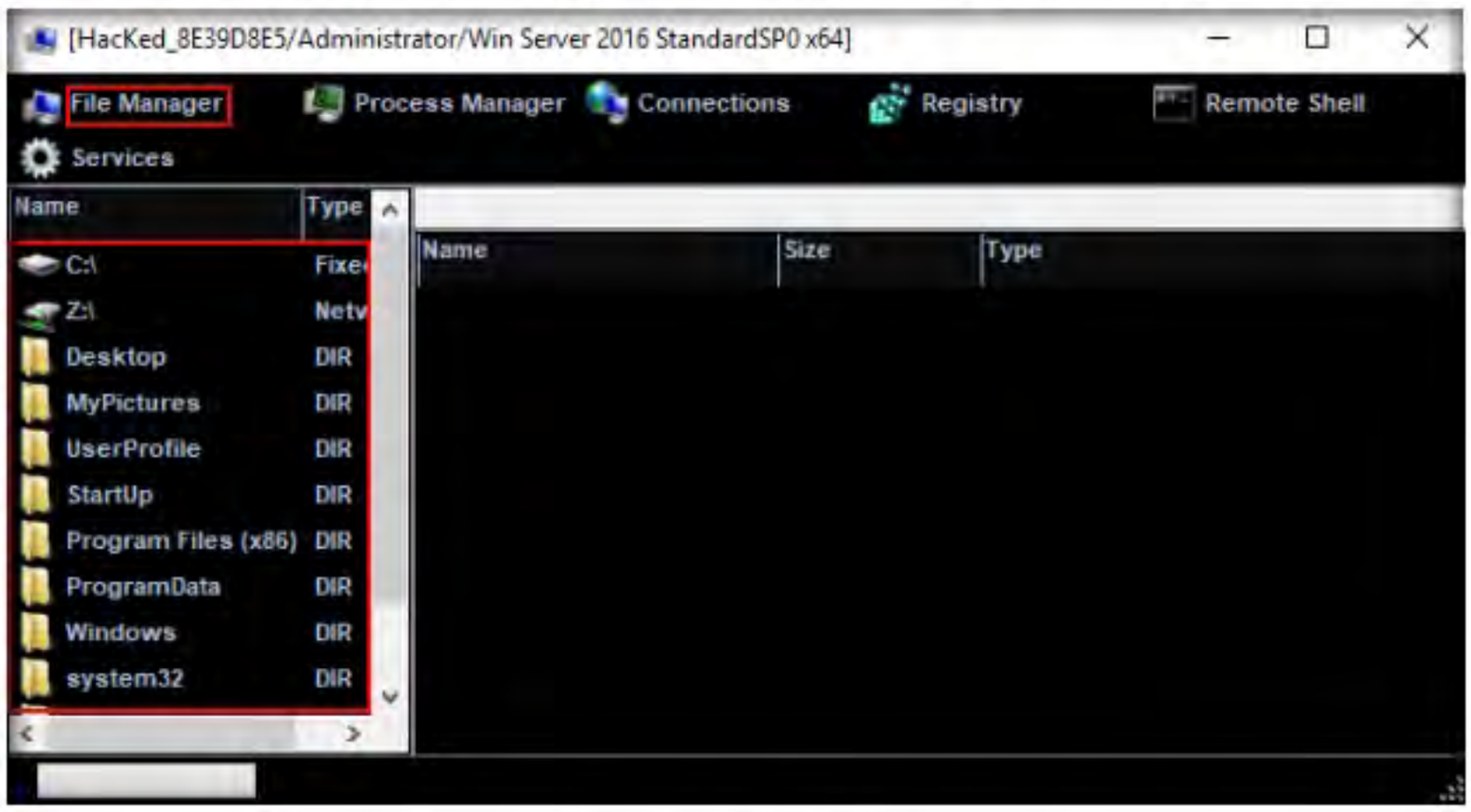


Figure 1.1.10: Manager window

21. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

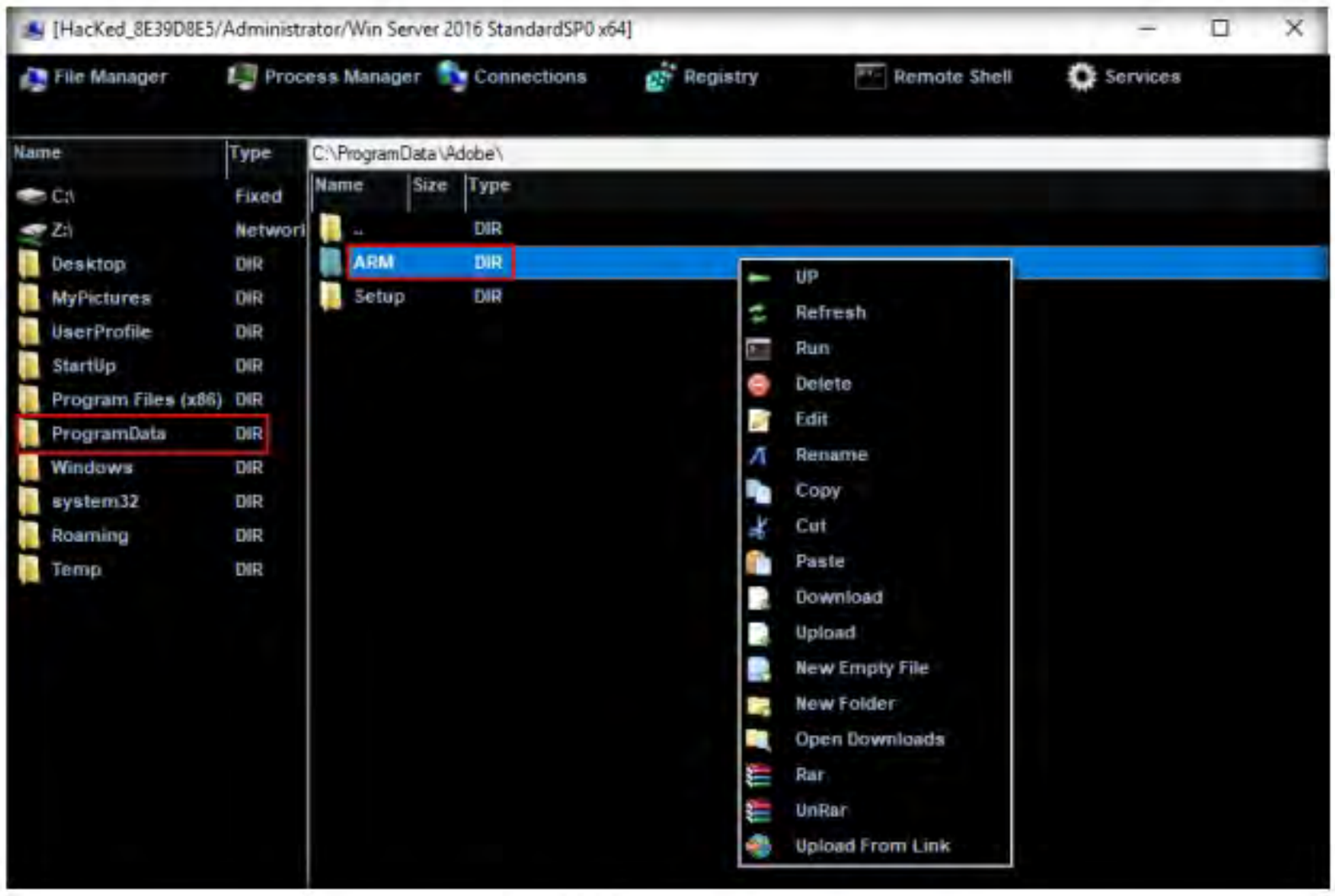


Figure 1.1.11: Accessing directories

TASK 1.5

Manage the Processes

22. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as **Kill**, **Delete**, and **Restart**.

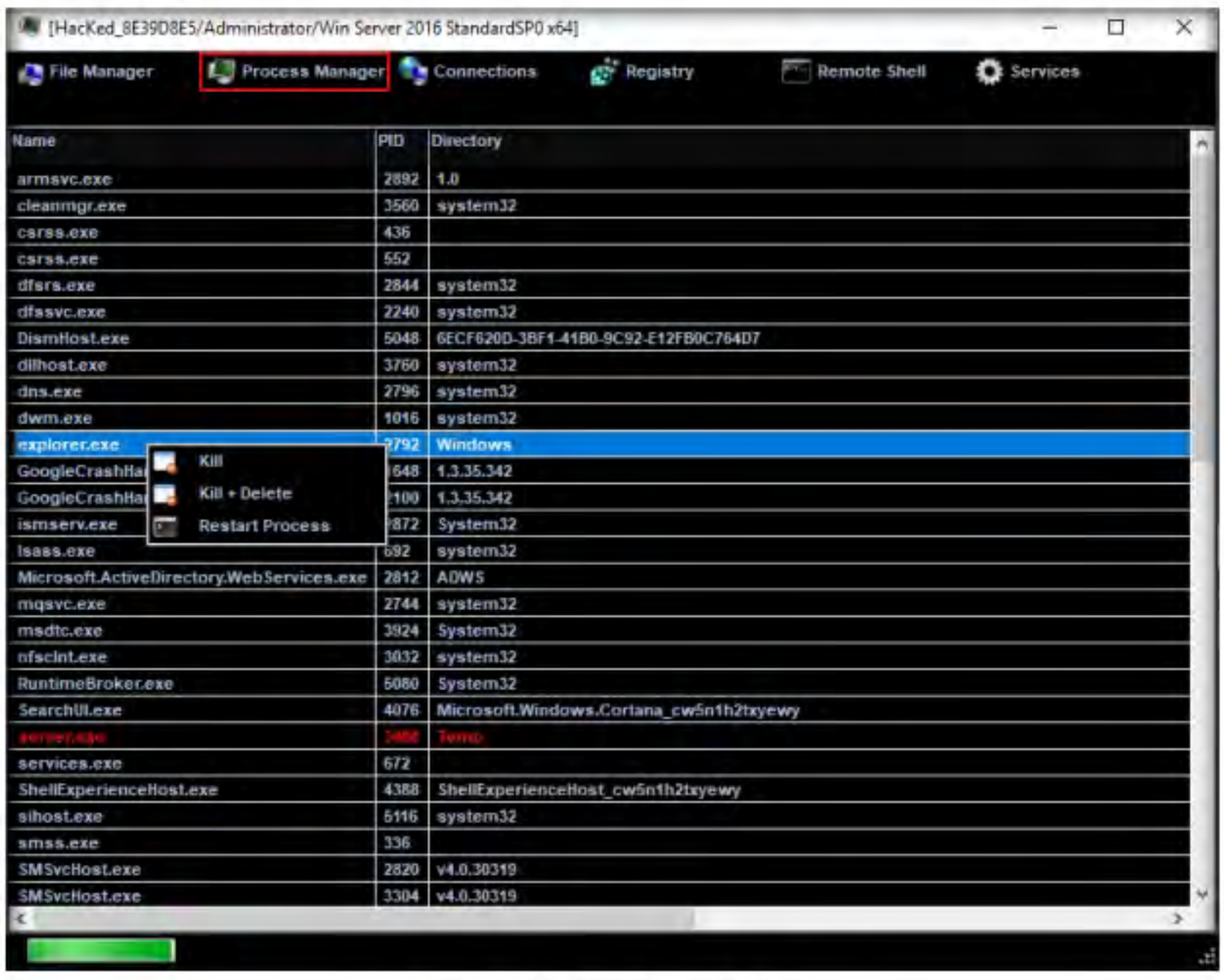


Figure 1.1.12: Process Manager Section

TASK 1.6

Manage the Connections

23. Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.

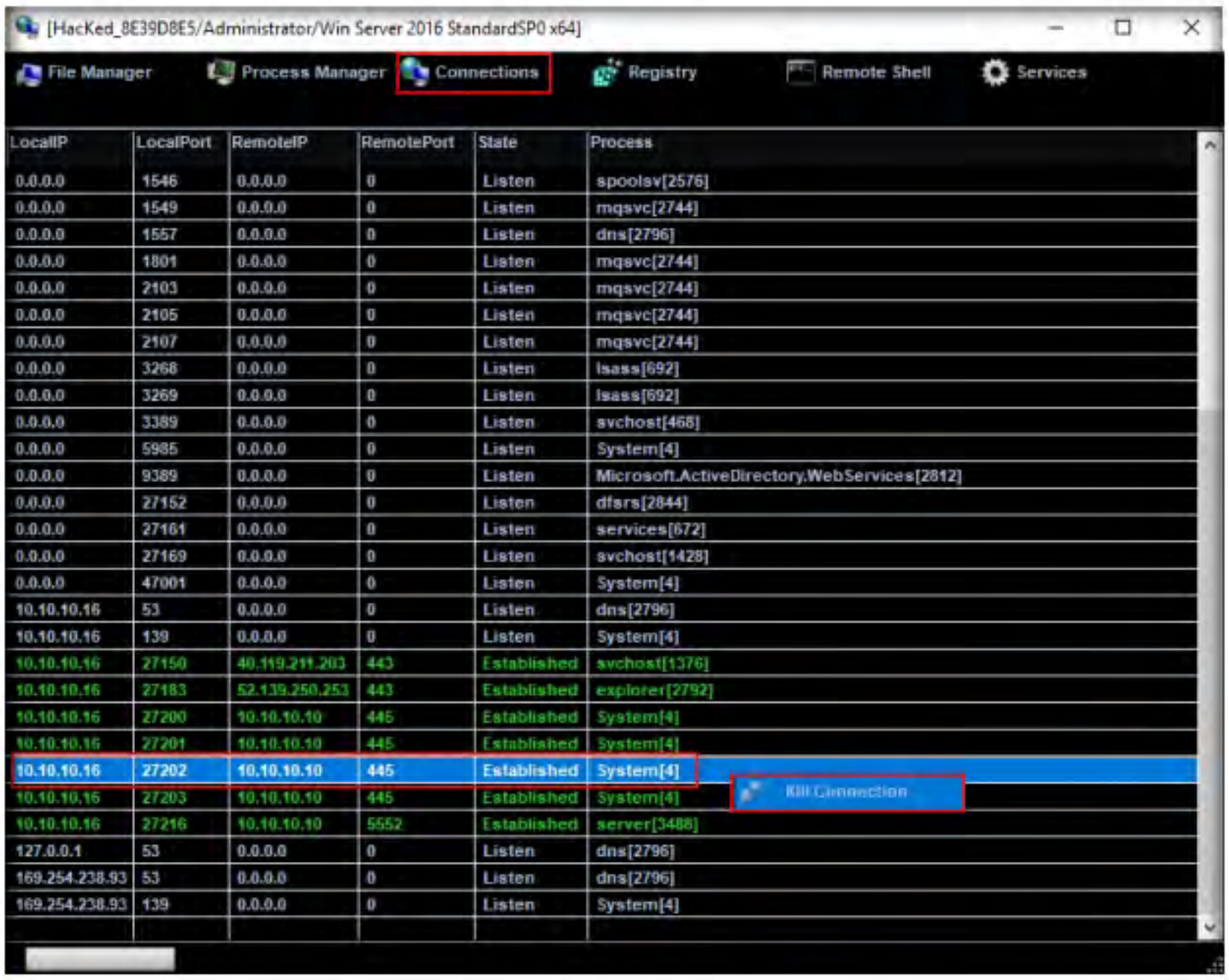


Figure 1.1.13: Managing connections

TASK 1.7

Manage the Registries

24. Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.
25. A few options appear for the files; you can use these to manipulate them.

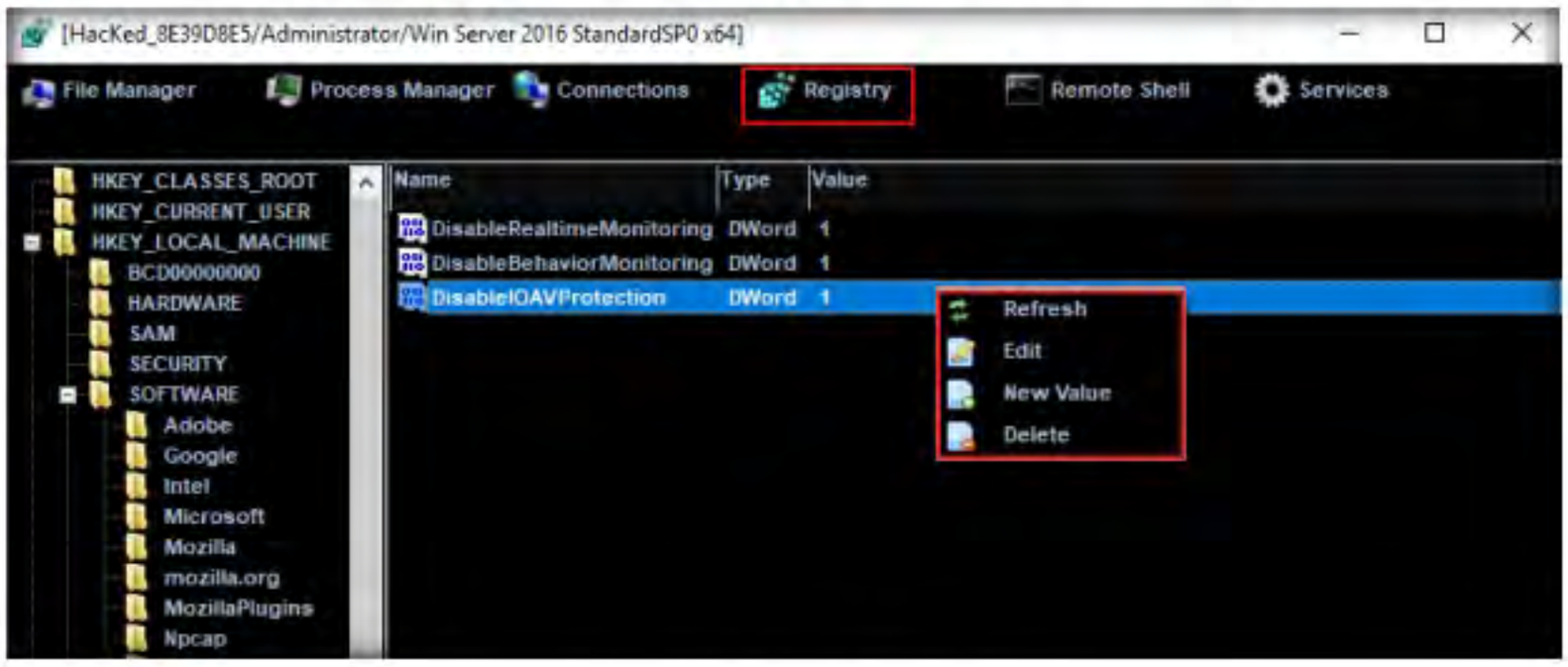


Figure 1.1.14: Managing Registries

TASK 1.8

Launch a Remote Shell

26. Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2016**).
27. Type the command **ipconfig/all** and press **Enter**.

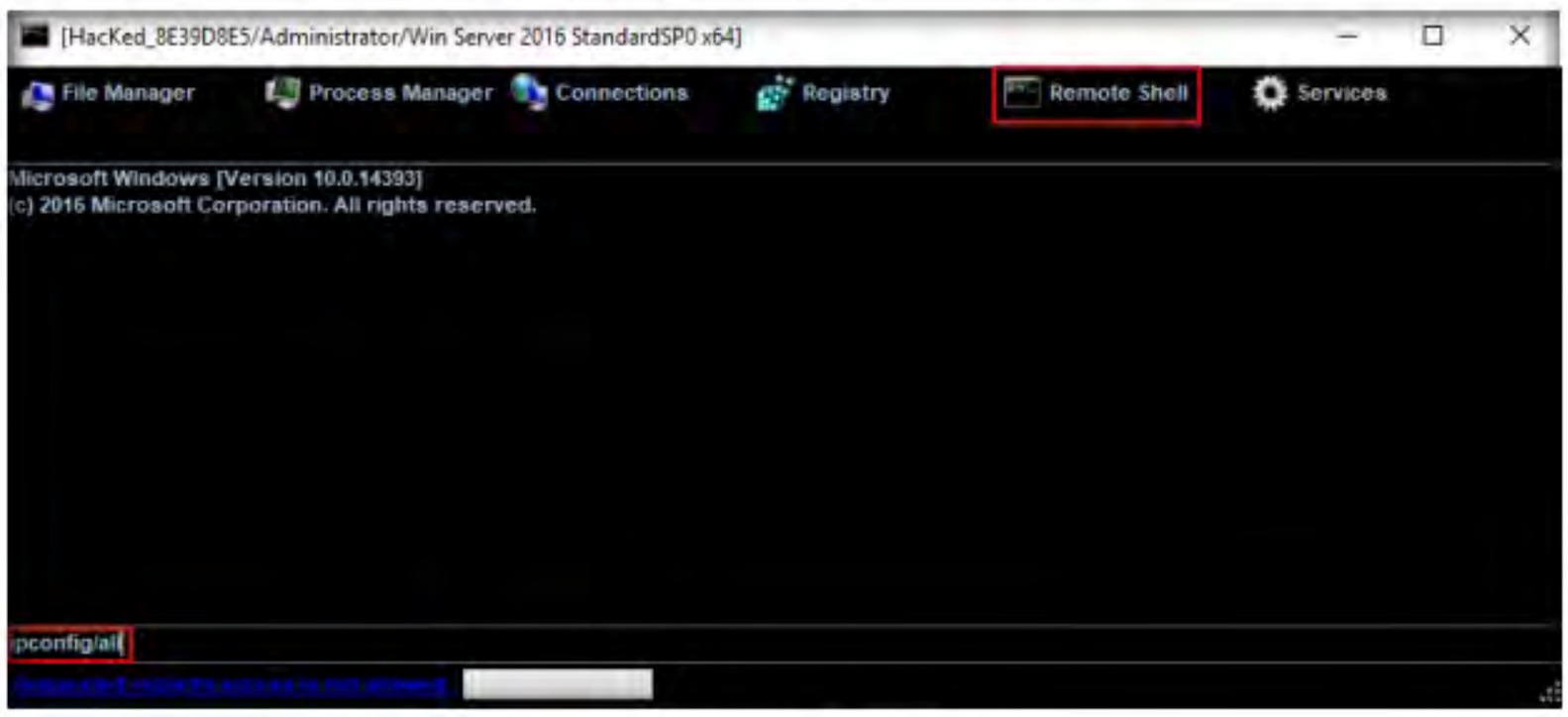


Figure 1.1.15: Launch a Remote Shell

28. This displays all interfaces related to the victim machine, as shown in the screenshot.

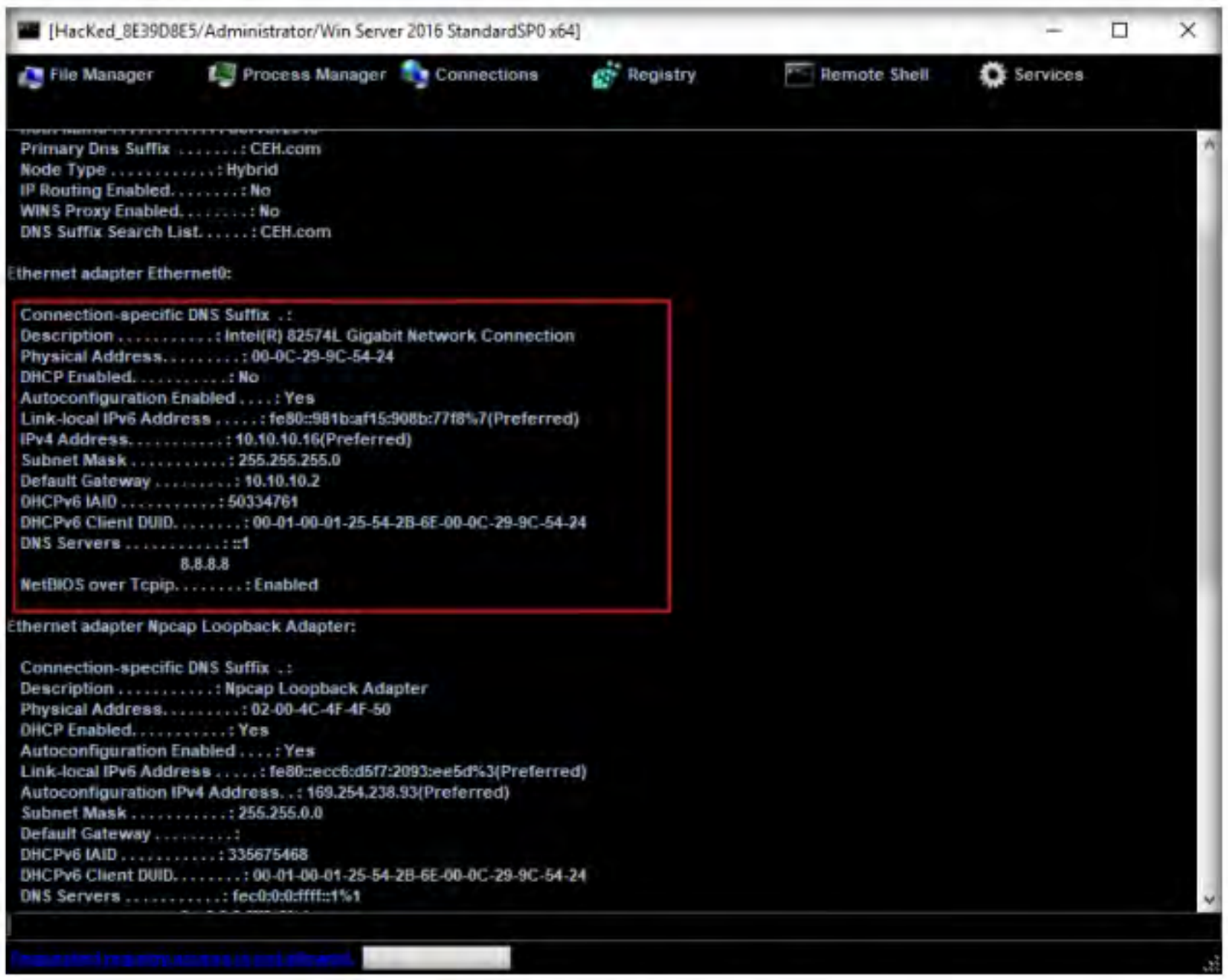


Figure 1.1.16: Launch a Remote Shell

29. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.

30. In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.
31. Close the **Manager** window.
32. Now, right-click on the victim name, click **Run File**, and choose an option from the drop-down list to execute scripts or files remotely from the attacker machine.

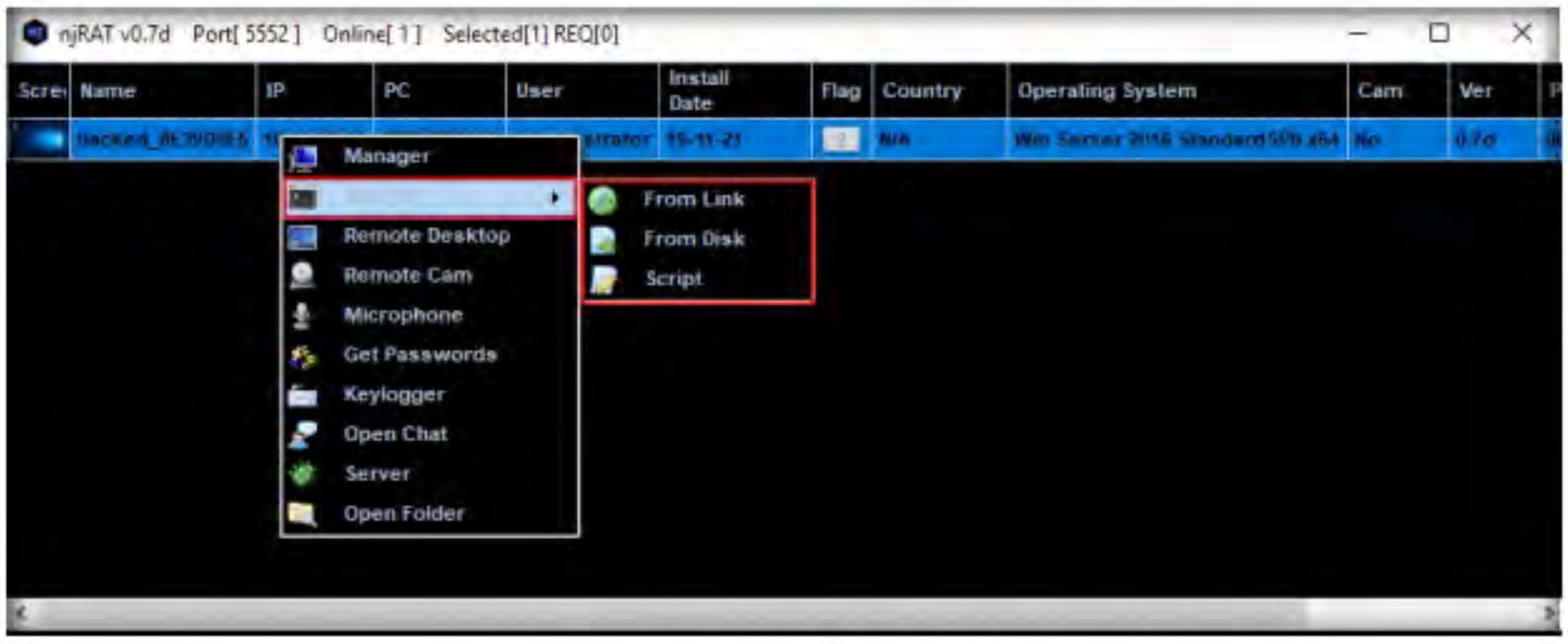


Figure 1.1.17: Launch a Remote Shell

TASK 1.9

Launch a Remote Desktop Connection

33. Right-click on the victim name, and then select **Remote Desktop**.

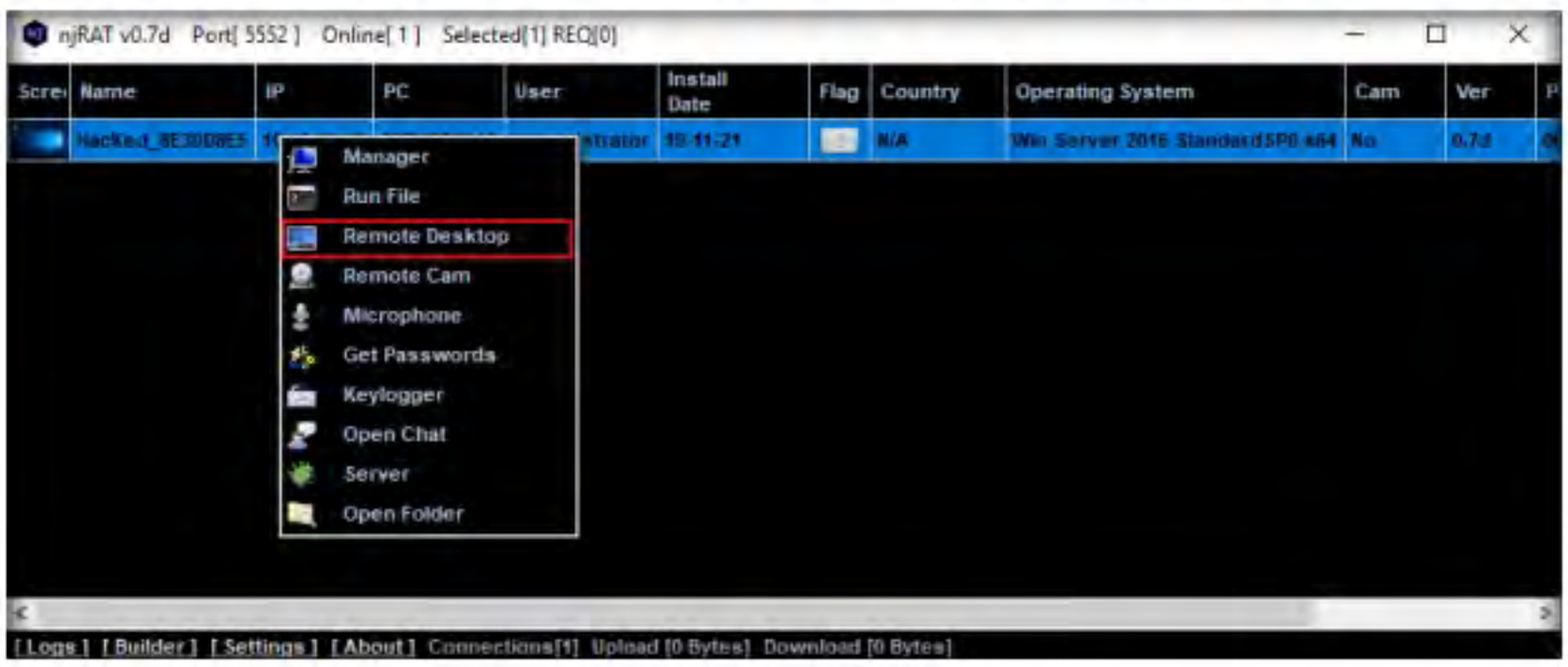


Figure 1.1.18: Launching a Remote Desktop Connection

34. This launches a remote desktop connection without the victim's awareness.
35. A **Remote Desktop** window appears; hover the mouse cursor to the top-center area of the window. A down arrow appears; click it.

Figure 1.1.19: Remote Desktop window

36. A remote desktop control panel appears; check the **Mouse** option.

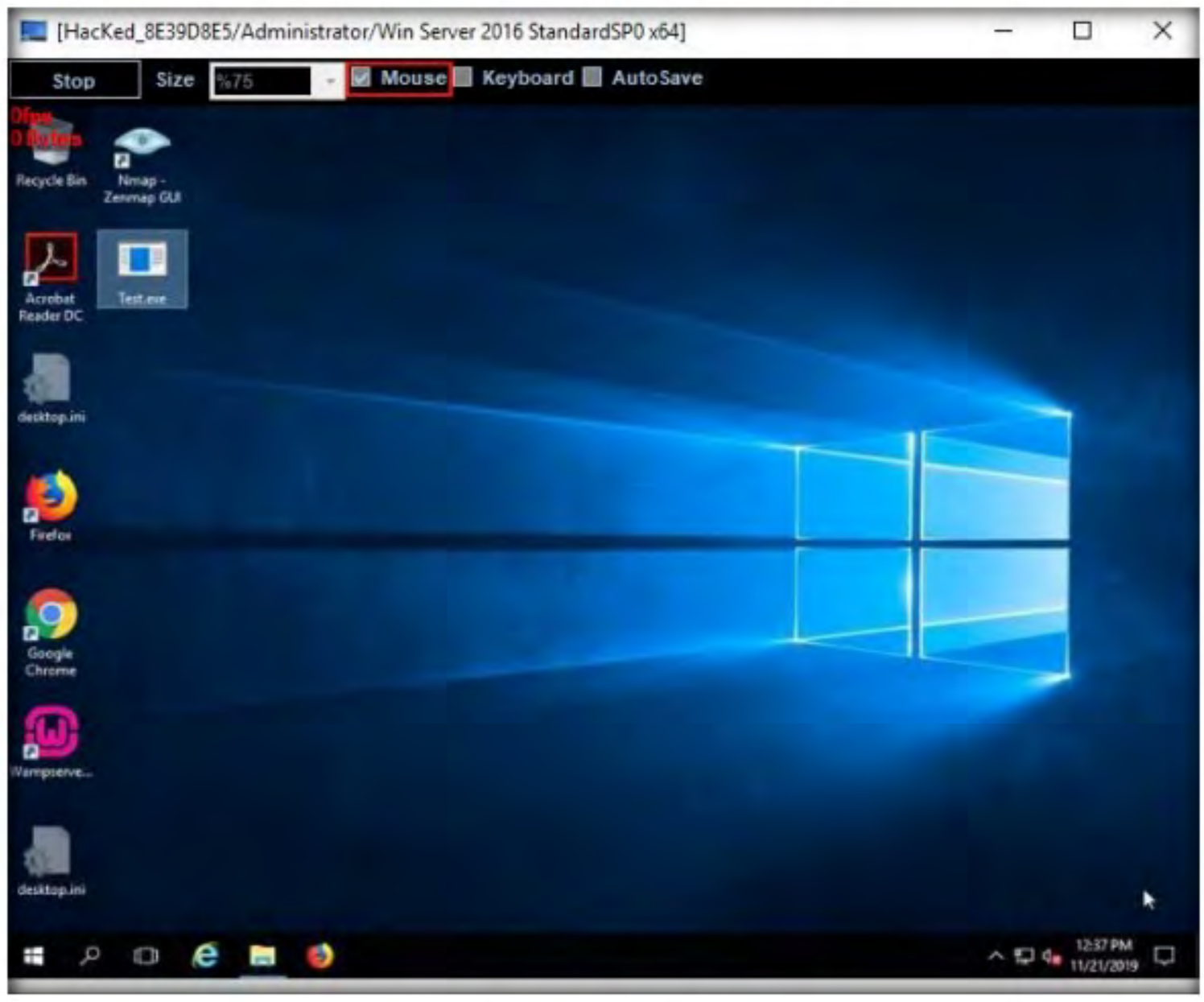


Figure 1.1.20: Remote Desktop Control Panel

37. Now, you will be able to remotely interact with the victim machine using the mouse.

Note: If you want to create any files or write any scripts on the victim machine, you need to check the **Keyboard** option.

38. On completing the task, close the **Remote Desktop** window.

39. In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on them and track voice conversations.

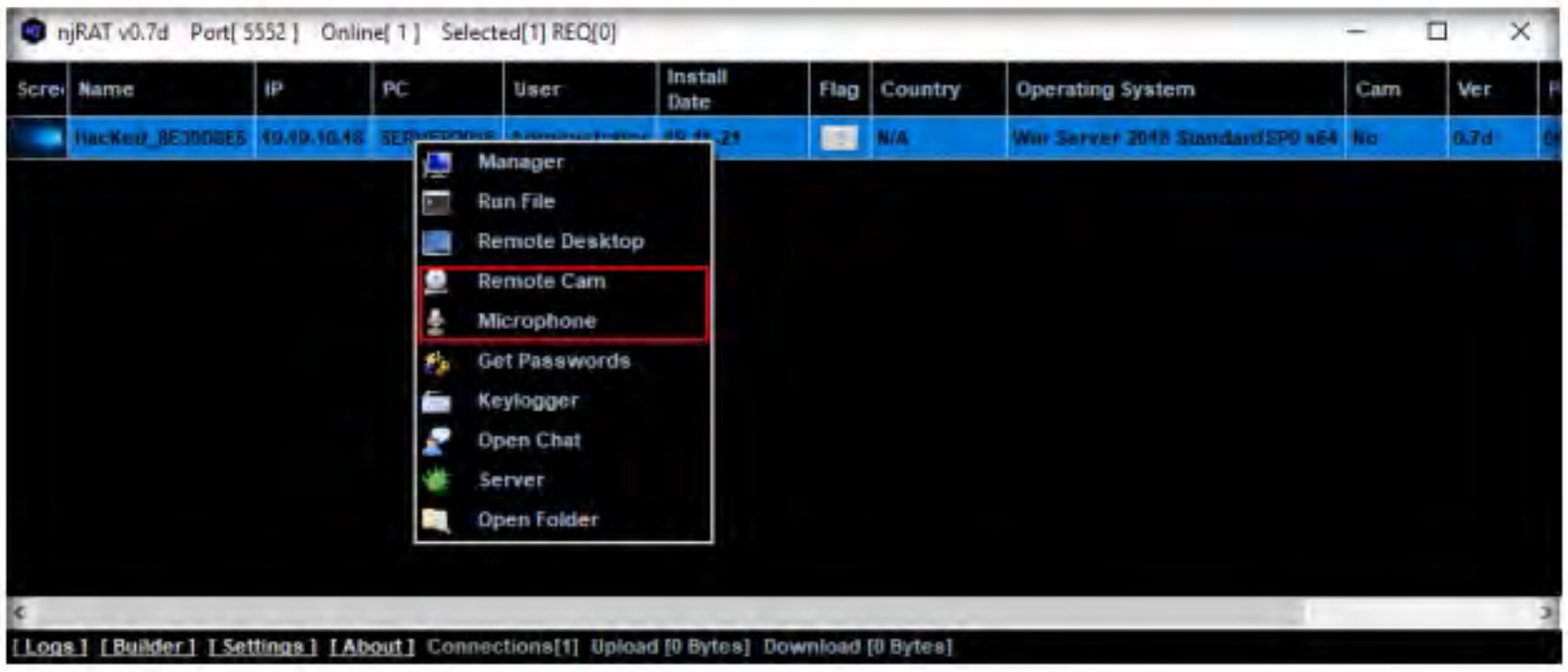


Figure 1.1.21: Accessing Remote Cam and Microphone

TASK 1.10

Perform Key Logging

40. Switch to the **Windows Server 2016** virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.

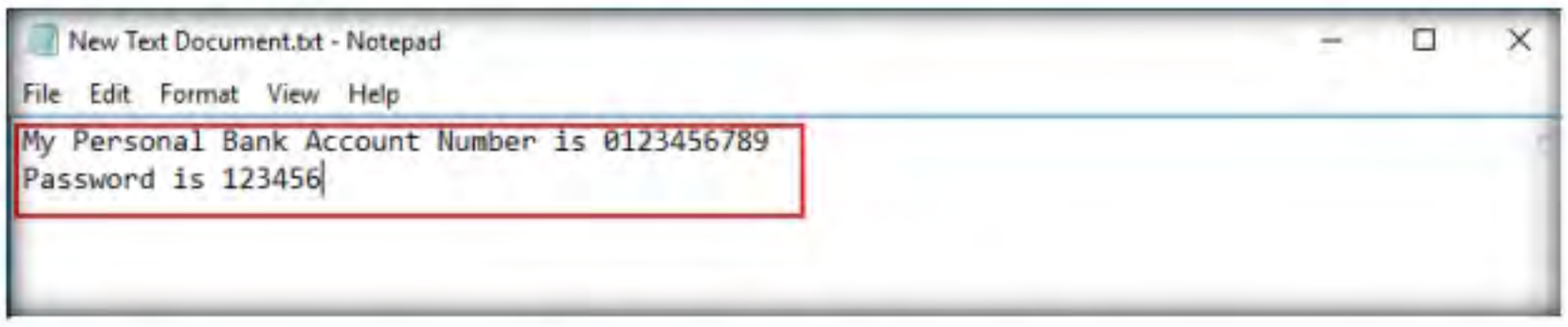


Figure 1.1.22: Entering Sensible Information

41. Switch back to the **Windows 10** virtual machine, right-click on the victim name, and click **Keylogger**.

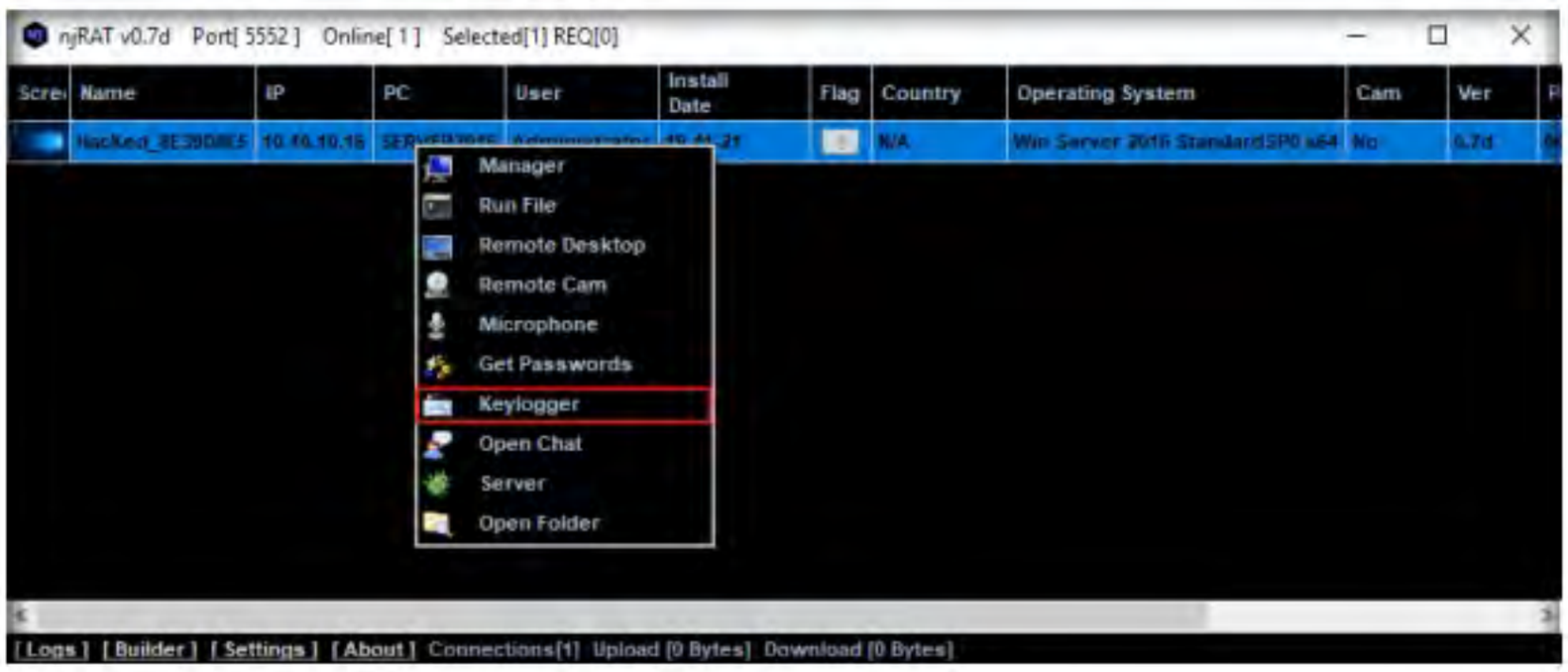


Figure 1.1.23: Launching Keylogger

42. The Keylogger window appears; wait for the window to load.
43. The window displays all the keystrokes performed by the victim on the **Windows Server 2016** virtual machine, as shown in the screenshot.

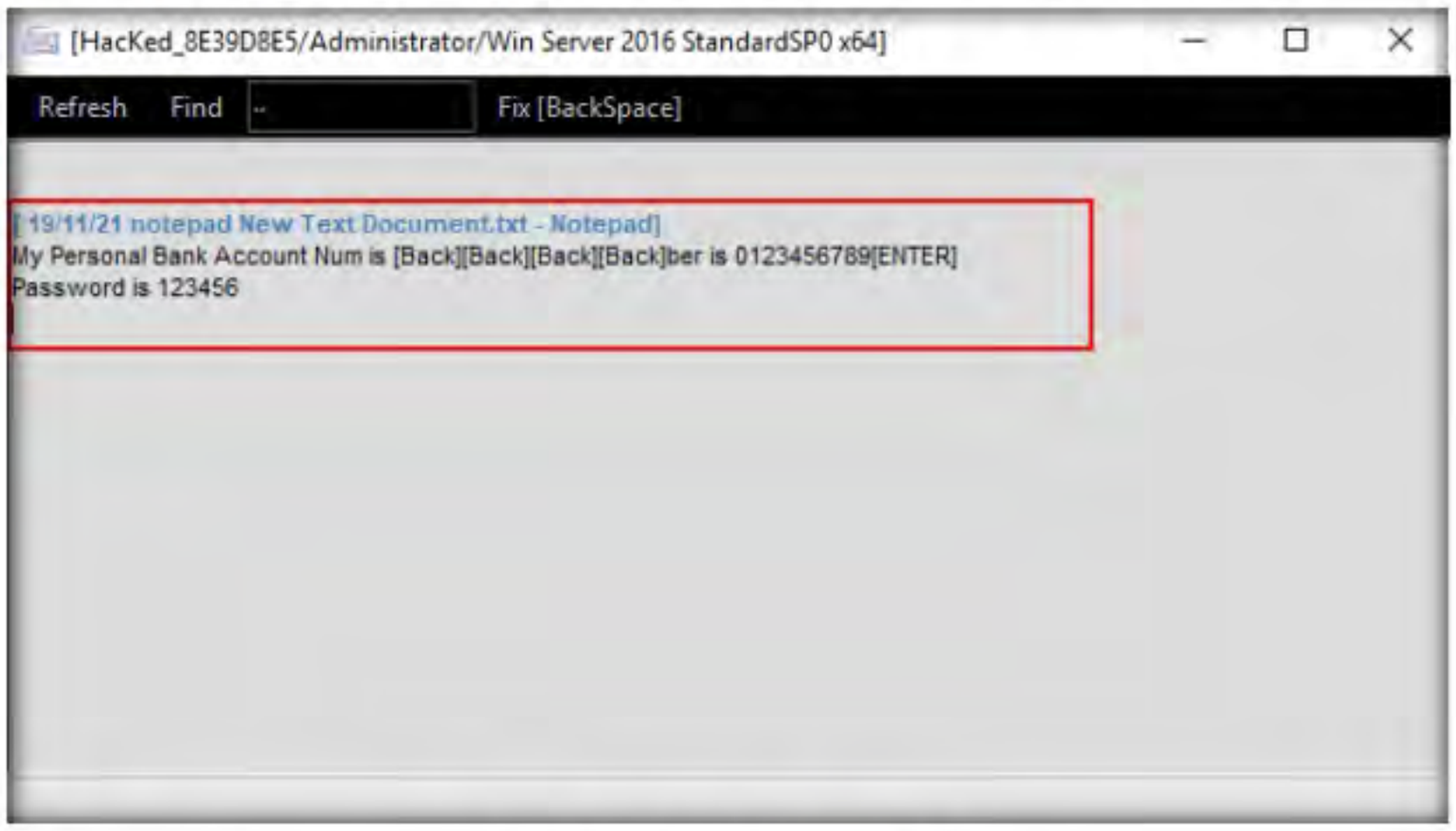


Figure 1.1.24: Keystrokes logged by njRAT

44. Close the **Keylogger** window.
45. Right-click on the victim name, and click **Open Chat**.

TASK 1.11

Chat with the Victim

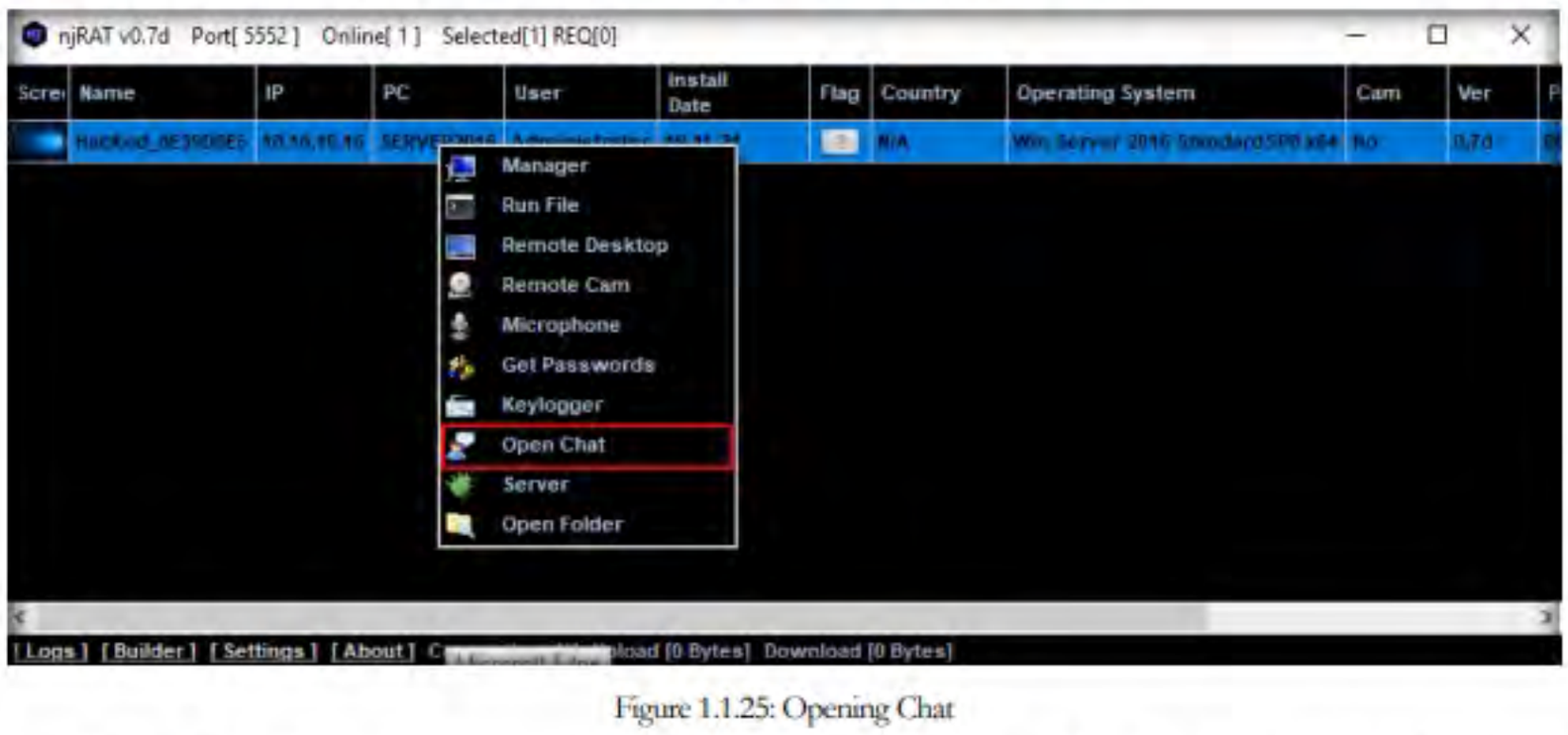


Figure 1.1.25: Opening Chat

46. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.

Figure 1.1.26: Entering a nickname

47. A chat box appears; type a message, and then click **Send**.

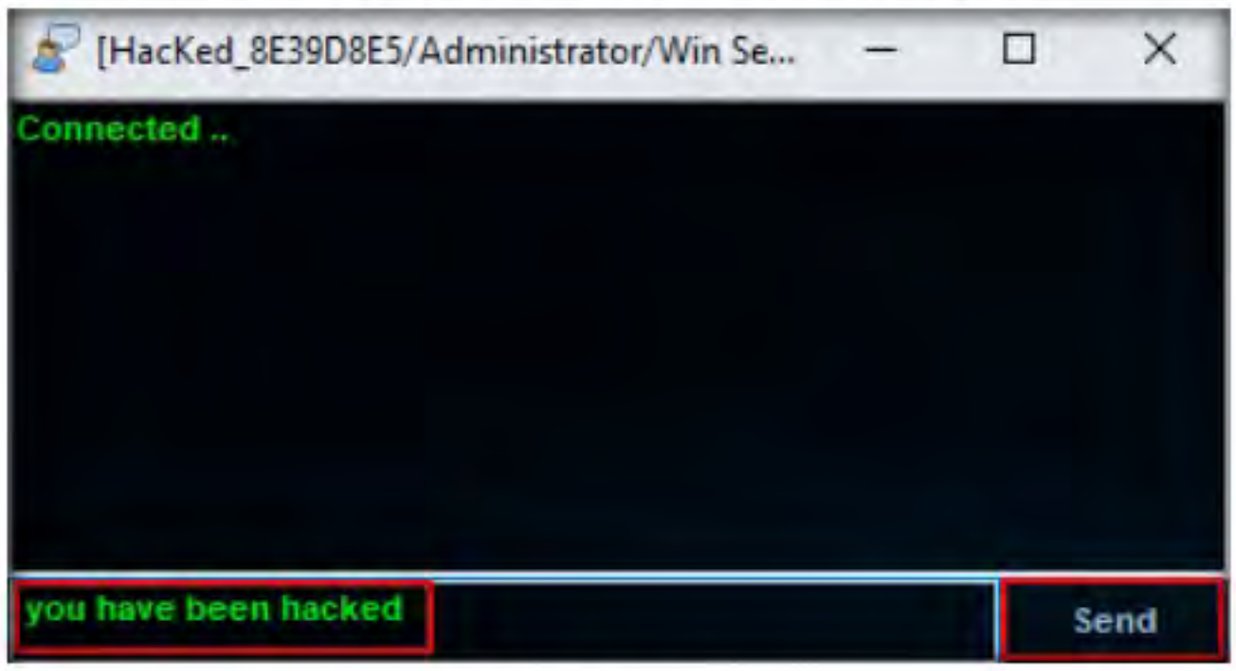


Figure 1.1.27: Typing a message

48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2016**), as demonstrated in the screenshot.

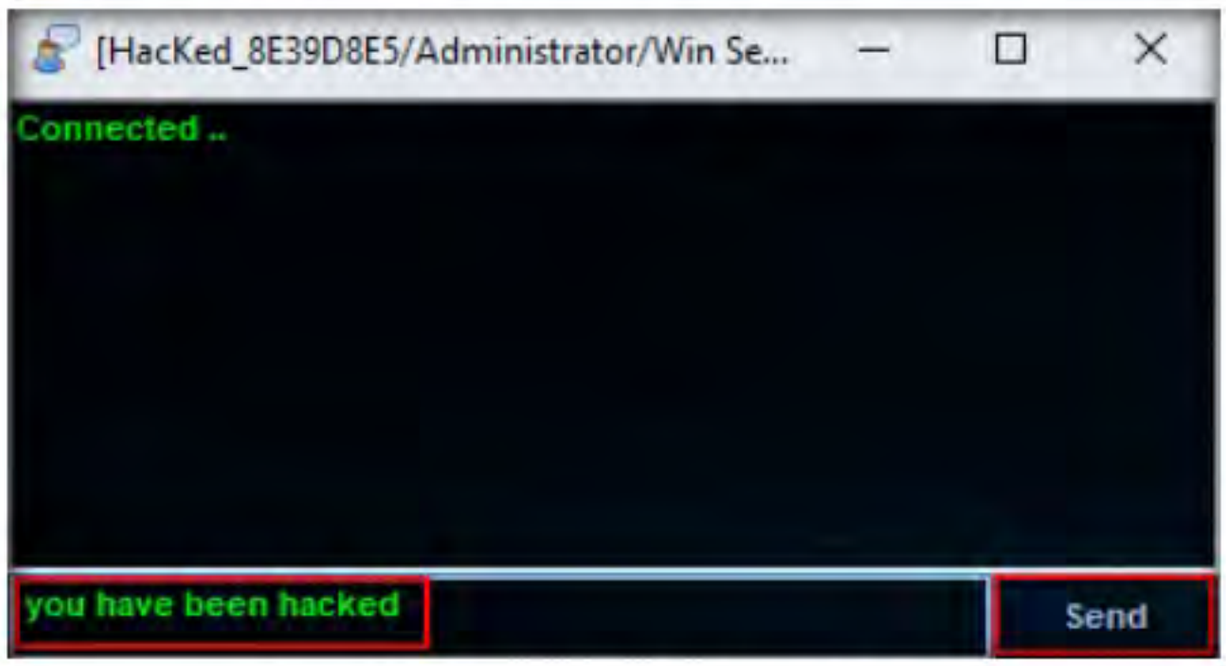


Figure 1.1.28: Message displayed on the victim's desktop

49. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.

50. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2016**, as the machine is shut down in the process of restarting.

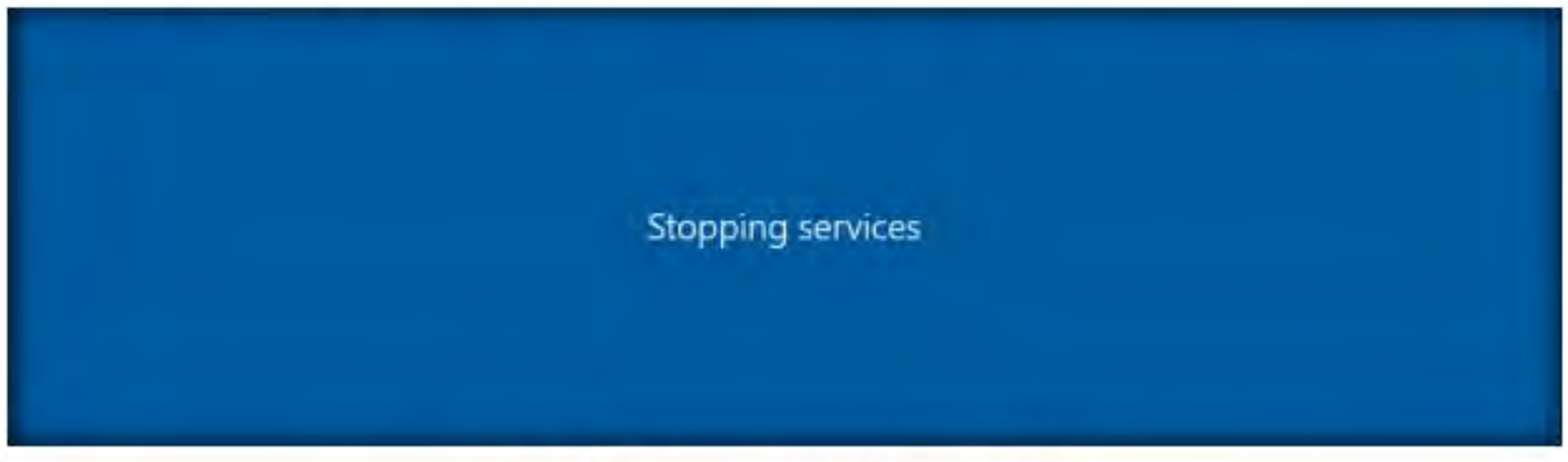


Figure 1.1.29: Shutting down the victim machine

51. Switch back to the attacker machine (**Windows 10**); you can see that the connection with the victim machine is lost.

Figure 1.1.30: Connection closed in njRAT GUI

52. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.

Note: It might take some time to establish a connection with the victim.

Figure 1.1.31: Logging in to victim machine

Figure 1.1.32: Connection established automatically

53. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.

54. On completion of this lab, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
55. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.
56. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.
57. Turn off the **Windows Server 2016** virtual machine.

TASK 2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 2.1

Scan a Malicious File with VirusTotal

1. Turn on the **Windows Server 2016** virtual machine
2. In the **Windows 10** virtual machine, open any web browser (here, **Google Chrome**), enter the URL **https://www.virustotal.com** in the address bar, and press **Enter**.
3. The **VirusTotal** main analysis site appears; click **Choose file** to upload a virus file.

At present, numerous anti-virus software programs have been configured to detect malware such as Trojans, viruses, and worms. Although security specialists keep updating the virus definitions, hackers continually try to evade or bypass them. One method that attackers use to bypass AVs is to "crypt" (an abbreviation of "encrypt") the malicious files using fully undetectable crypters (FUDs). Crypting these files allows them to achieve their objectives, and thereby take complete control over the victim's machine.

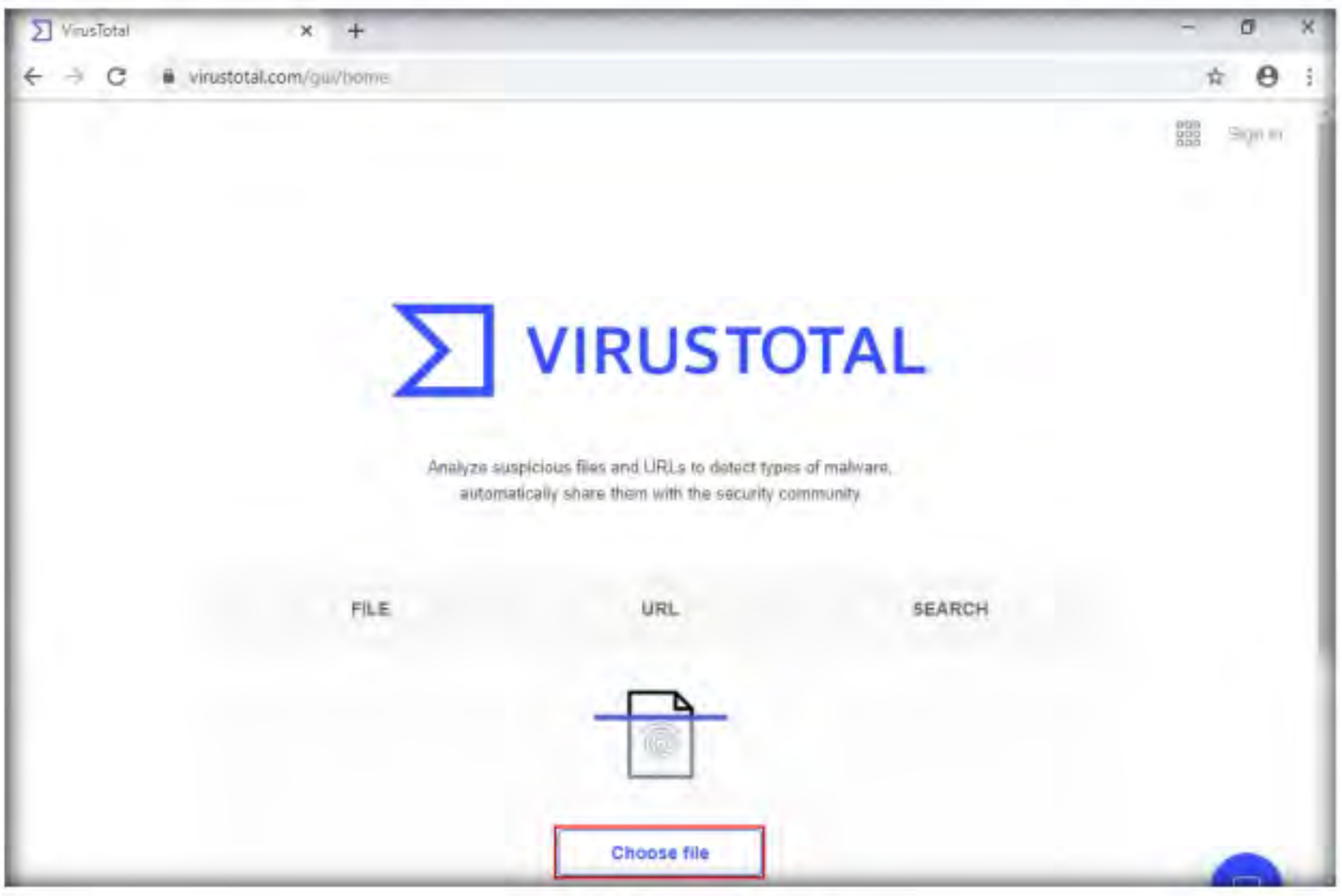


Figure 1.2.1: VirusTotal webpage

4. An **Open** dialog box appears; navigate to the location where you saved the malware file **Test.exe** in the previous lab (**Desktop**), select it, and click **Open**.

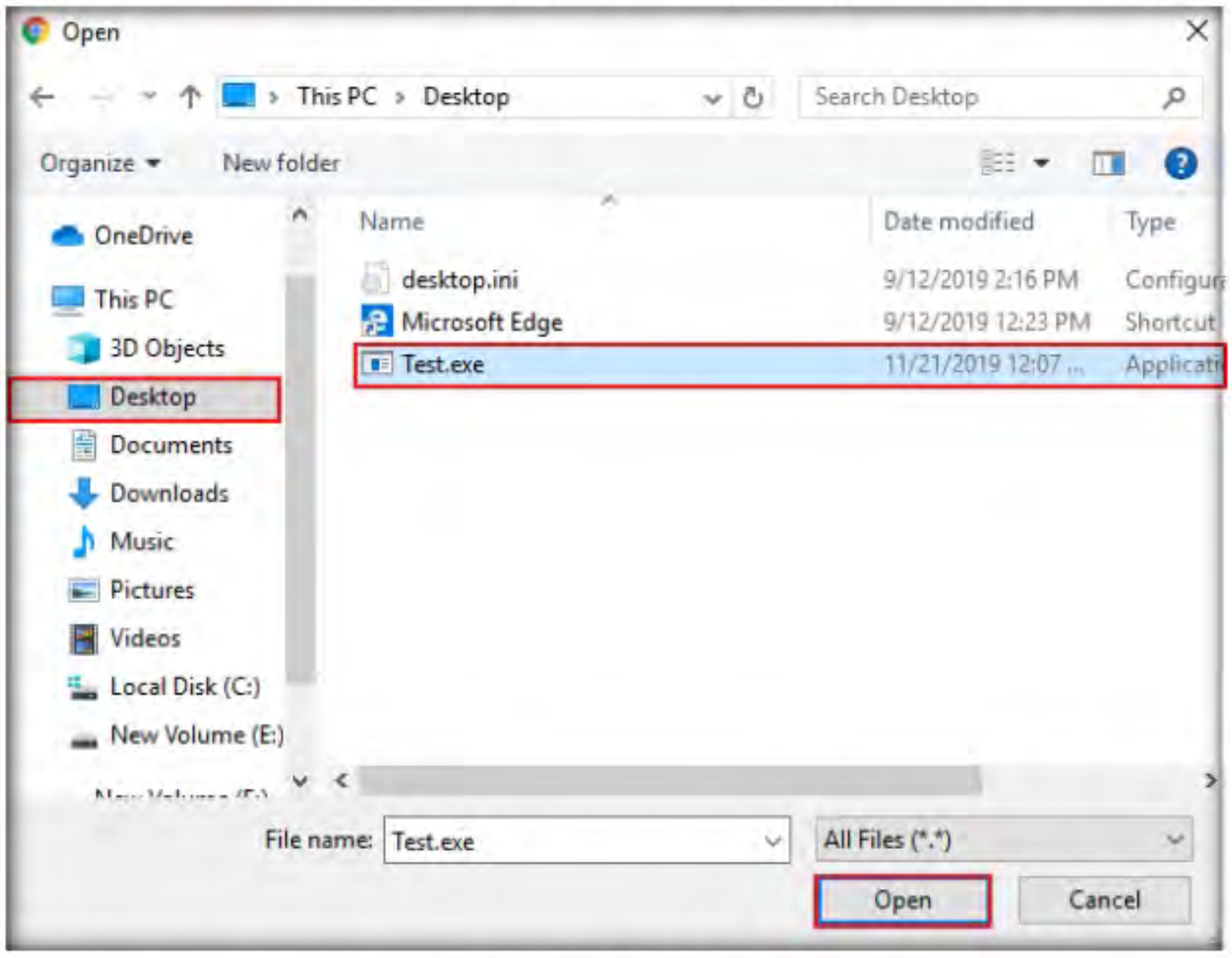


Figure 1.2.2: Open dialog box

5. Click **Confirm upload** on the **VirusTotal** page.

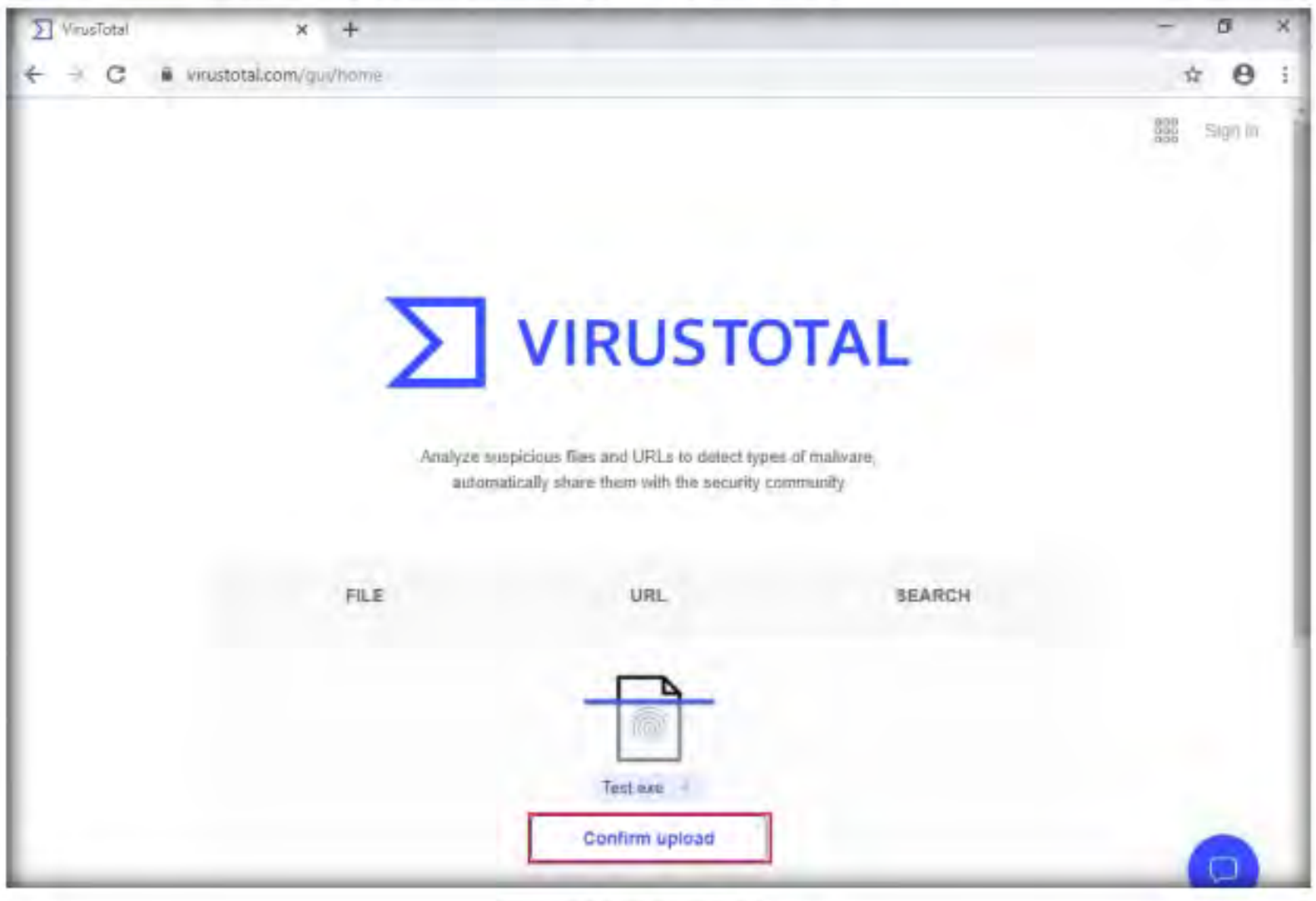


Figure 1.2.3: Uploading Malware

6. The **VirusTotal** uploads the file, scans it with the various anti-virus programs in its database, and displays the scan result, as shown in the screenshot.

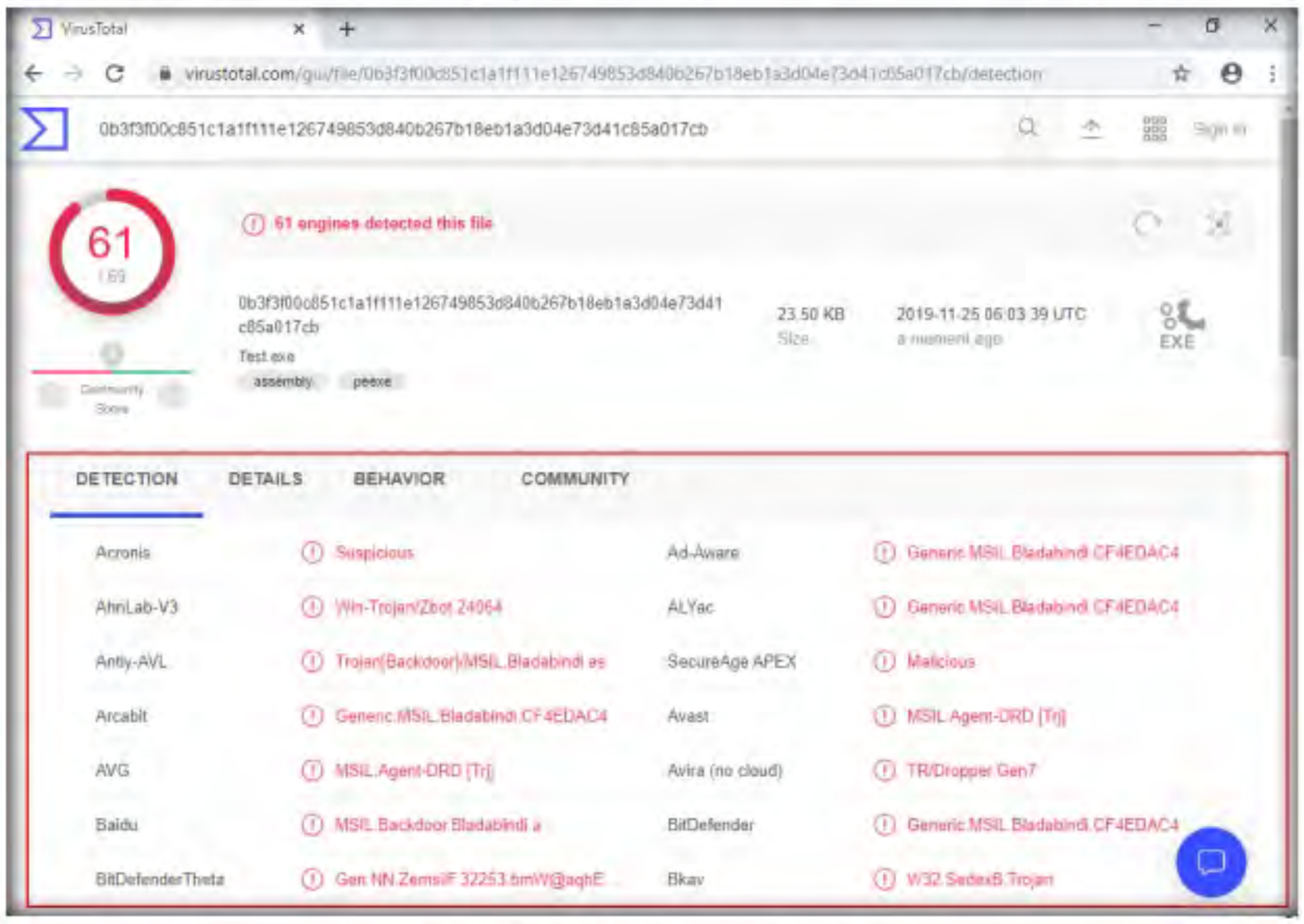


Figure 1.2.4: File detected by various anti-viruses

7. You can see that **61** out of **69** anti-virus programs have detected **Test.exe** as a malicious file. Minimize the web browser window.

Note: The detection ratio might vary in your lab environment.

TASK 2.2

Crypt a Trojan Using SwayzCryptor

8. Go to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Crypters\SwayzCryptor** and double-click **SwayzCryptor.exe**.
9. The **SwayzCryptor** GUI appears; click ... below **File** to select the Trojan file.

Figure 1.2.5: Uploading the malicious file in SwayzCryptor

10. The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.

Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses. SwayzCryptor is an encrypter (or "crypter") that allows users to encrypt their program's source code.

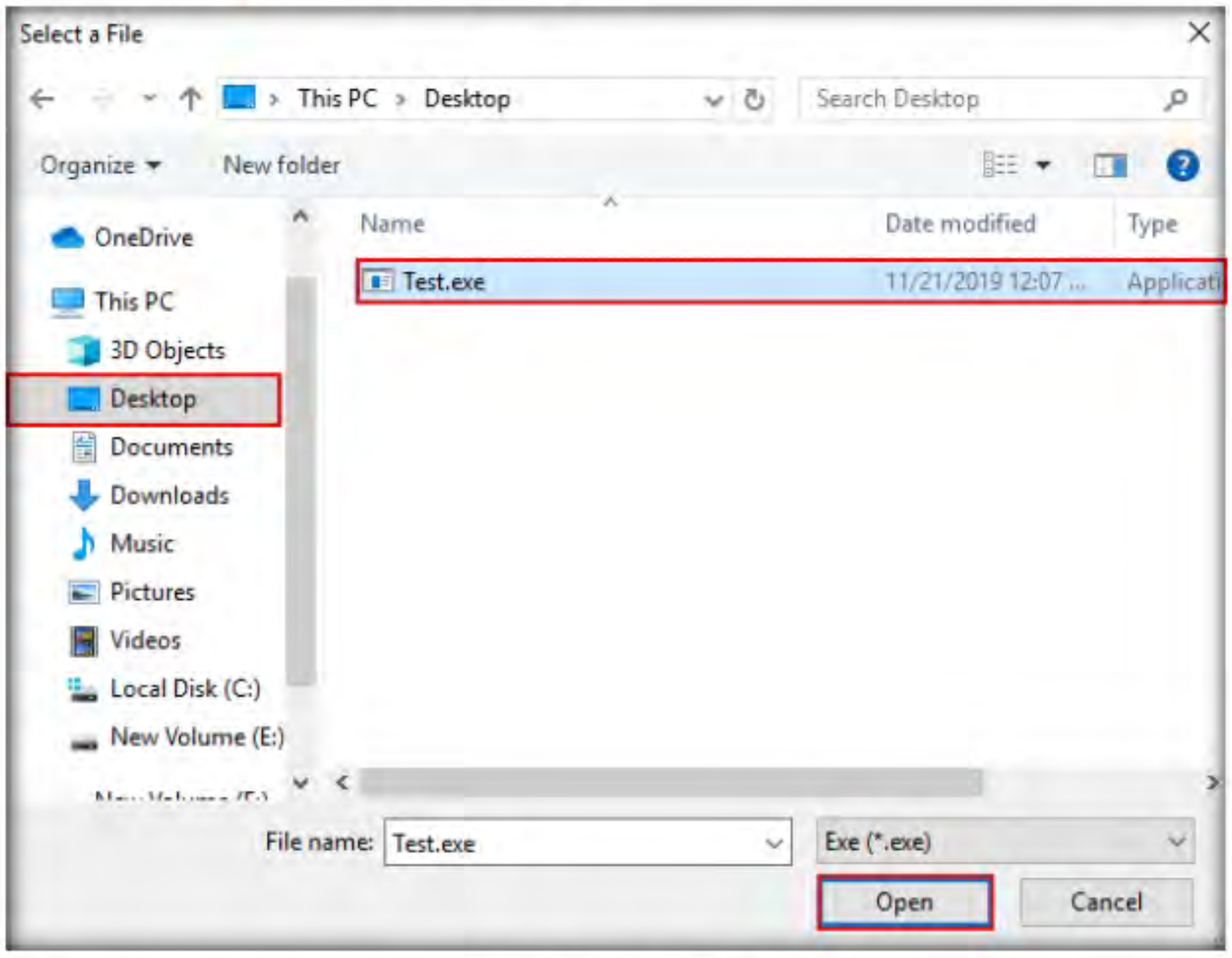


Figure 1.2.6: Selecting the File

11. Once the file is selected, check the options **Start up**, **Mutex**, and **Disable UAC**, and then click **Encrypt**.

Figure 1.2.7: Configuring options

12. The **Save File** dialog-box appears; select the location where you want to store the crypted file (here, **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.

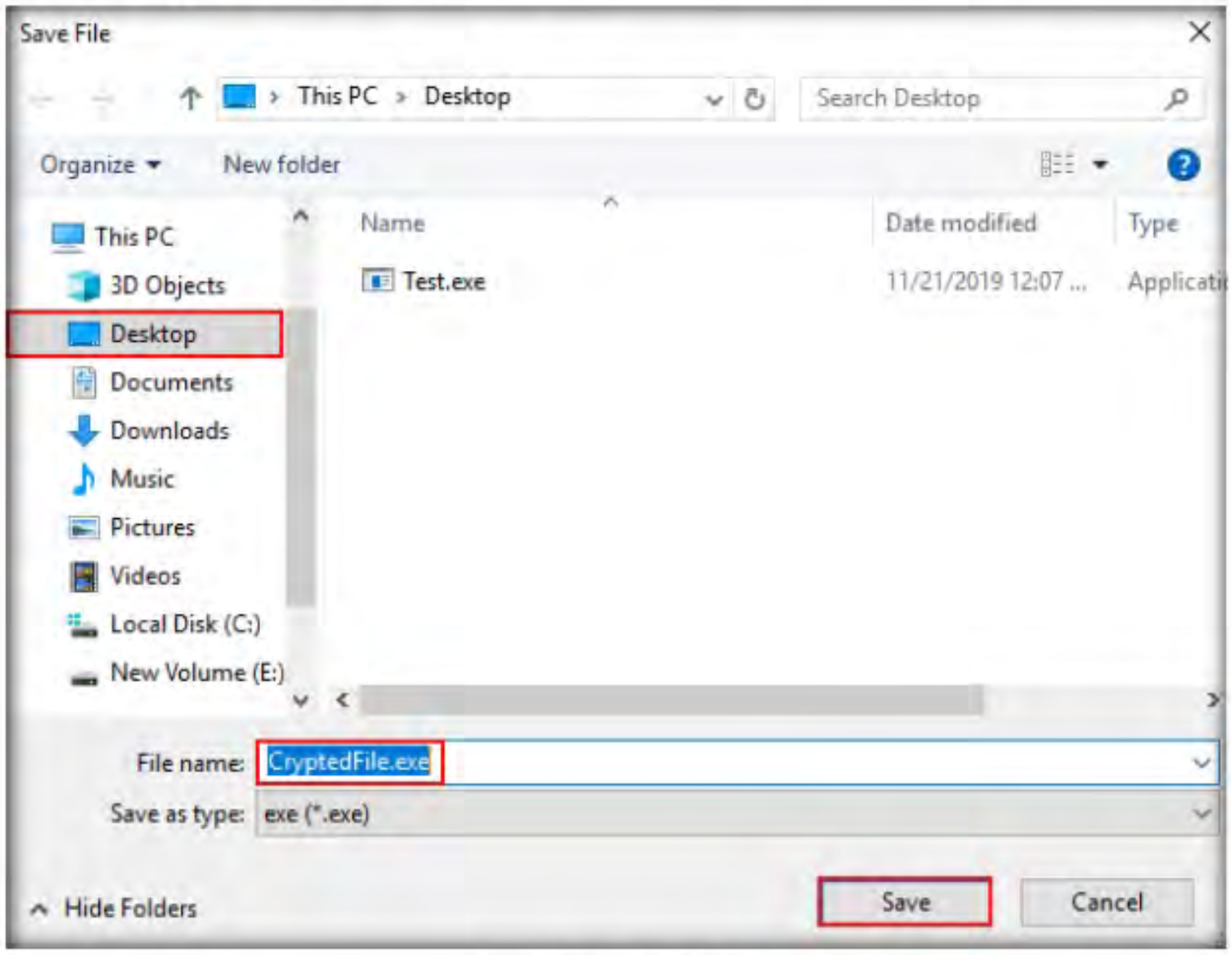


Figure 1.2.8: Save File dialog box

13. Once the encryption is finished, click **Close**.

Figure 1.2.9: Closing the GUI

TASK 2.3

Scan with VirusTotal

14. Maximize the web browser (here, **Google Chrome**). In the VirusTotal analysis page, click the **Upload file** icon in the top-right corner of the page.

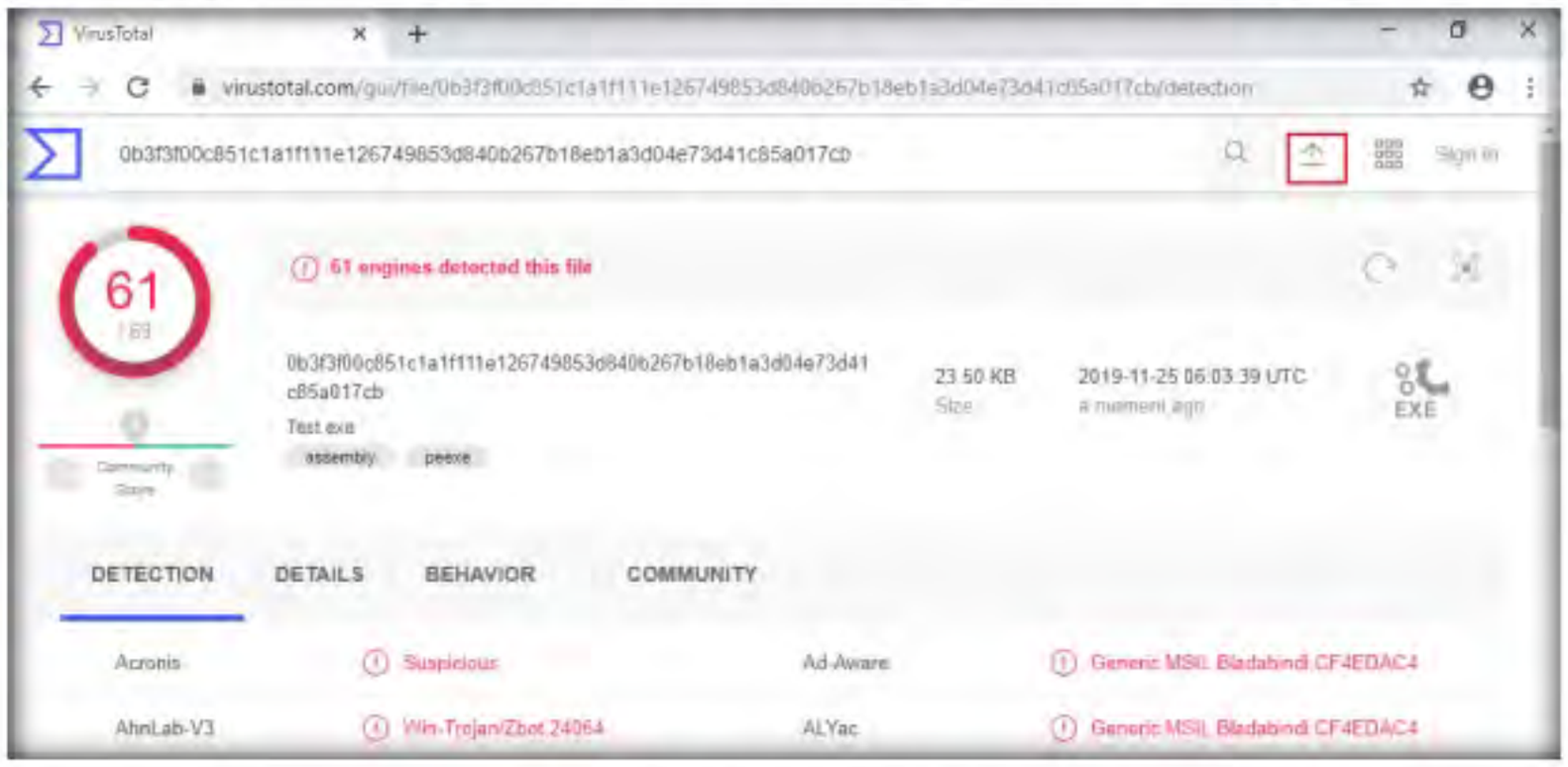


Figure 1.2.10: Uploading Encrypted Malware File

15. An **Open** dialog-box appears; navigate to the location where you saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.

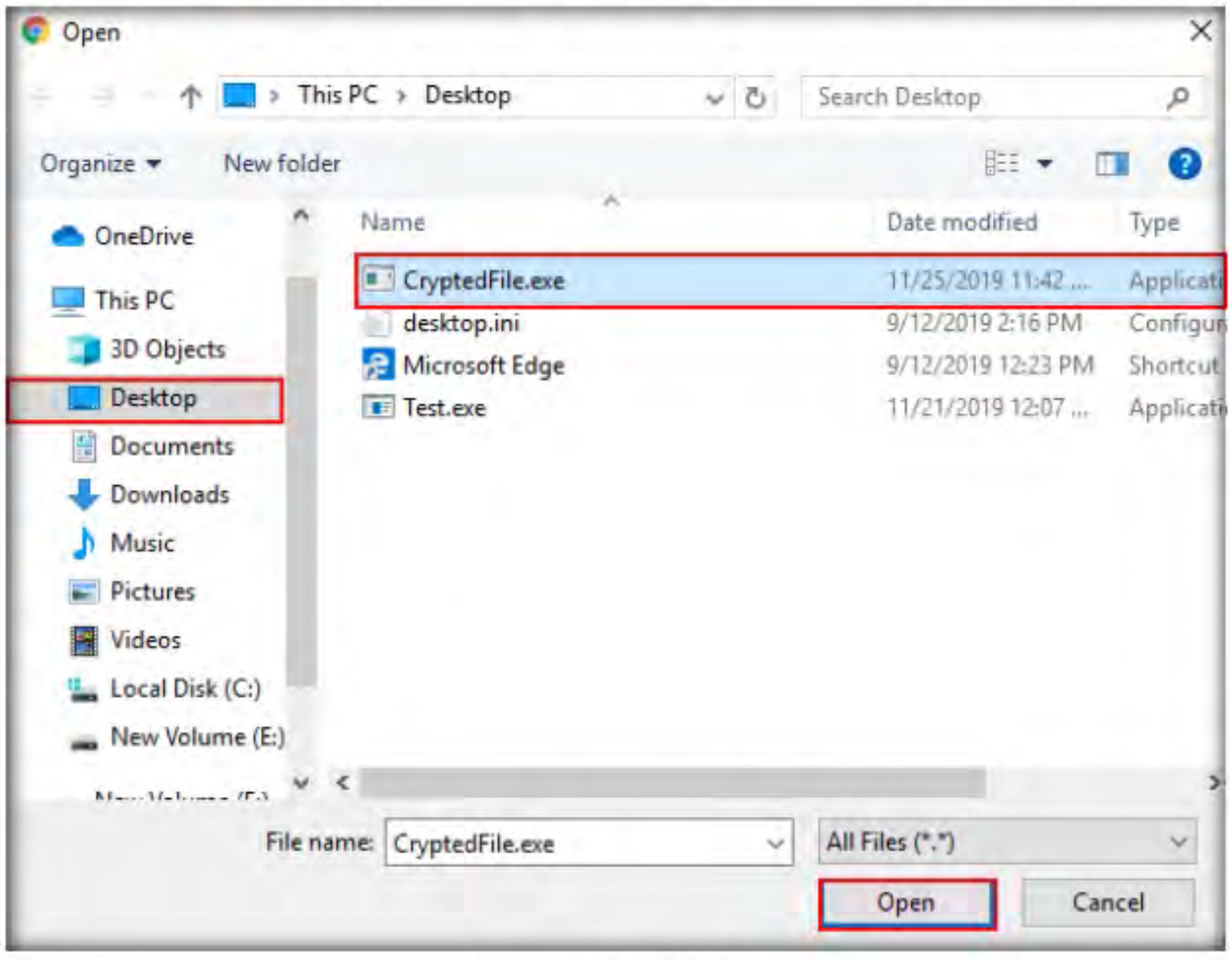


Figure 1.2.11: Open dialog box

16. Click **Confirm upload**.

Figure 1.2.12: Uploading Encrypted Malicious File to Analyze

17. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. It displays the scan result, as shown in the screenshot.

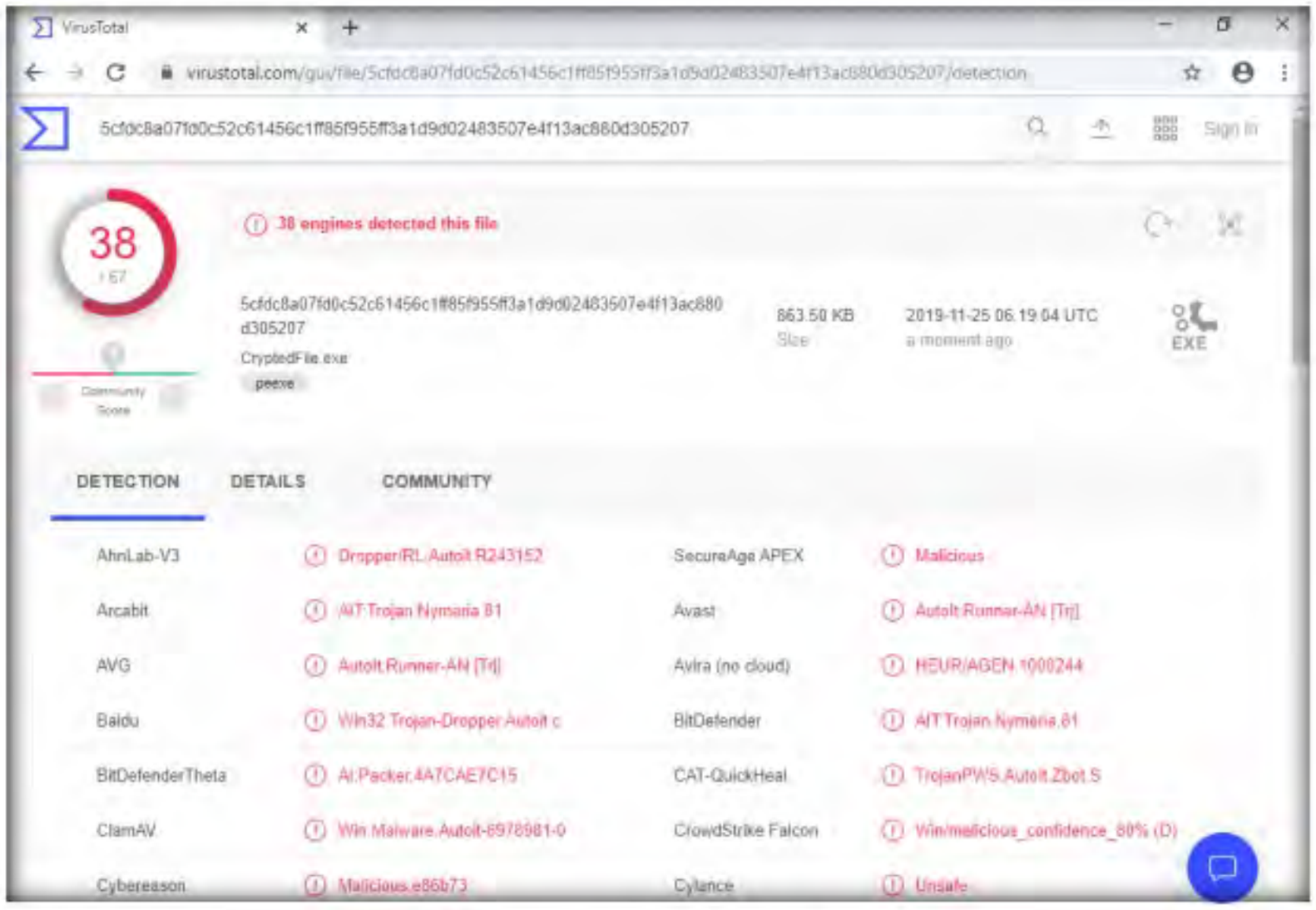


Figure 1.2.13: File detected by very few anti-virus programs

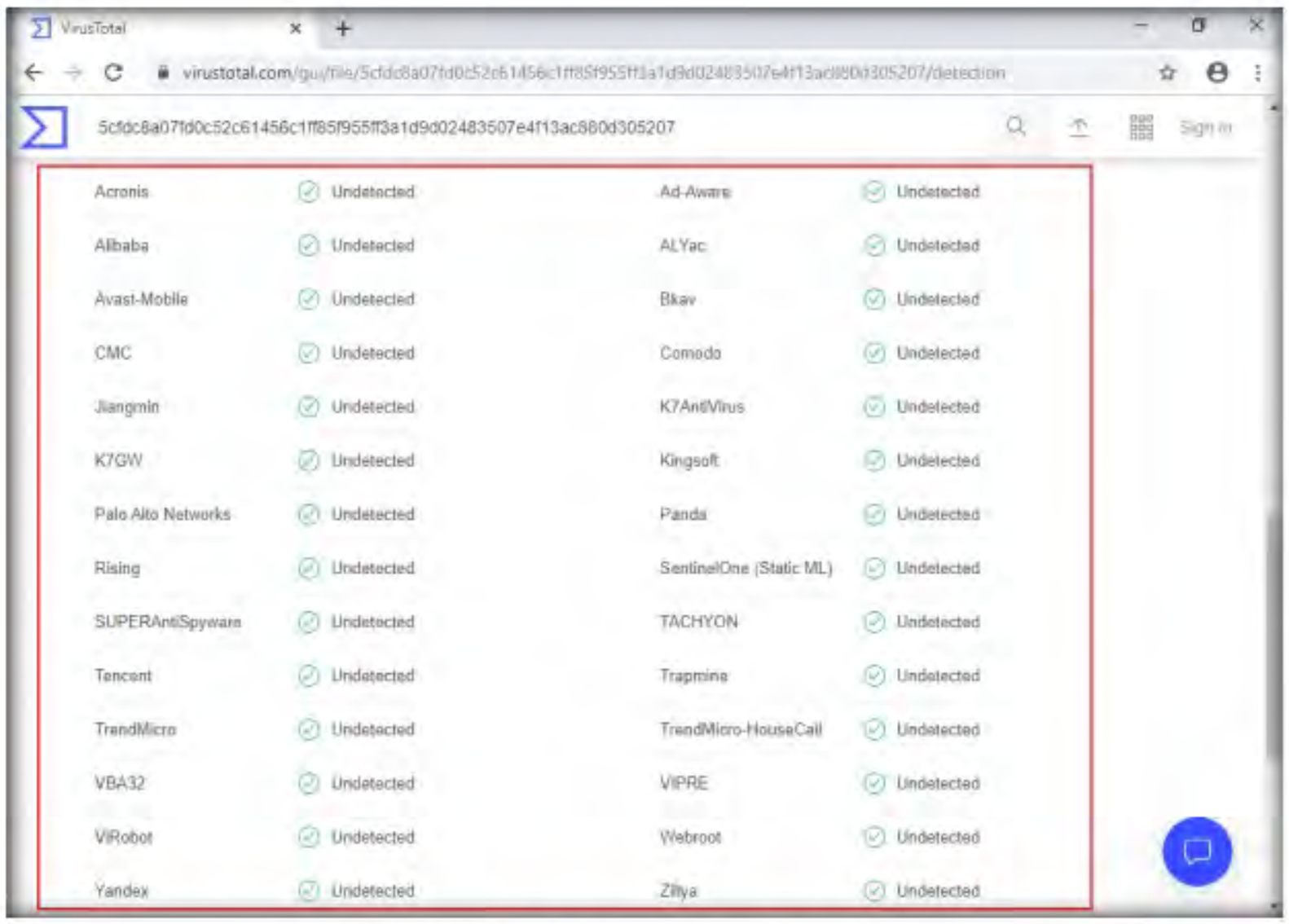


Figure 1.2.14: File detected by very few anti-virus programs

18. Only a few anti-virus programs have detected **CryptedFile.exe** as a malicious file. Minimize or close the browser window.

Note: The specific scan result might vary in your lab environment.

19. Now, we will test the functioning of a Crypted file (**CryptedFile.exe**).

TASK 2.4

Test the Crypted File

20. Go to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, double-click the **njRAT v0.7d.exe** file and launch njRAT by choosing the default port number **5552**, and then click **Start**.
21. In this exercise, we have already created a crypted file (**CryptedFile.exe**), built using njRAT.

Figure 1.2.15: Start njRAT

22. Use any technique to send **CryptedFile.exe** to the intended target—through email or any other source (In real-time, attackers send this server to the victim).

Note: In this lab, we copied the **CryptedFile.exe** file to the shared network location (**CEH-Tools**) to share the file.

23. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

24. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**CryptedFile.exe**), in which the attacker (here, **you**) sent the server executable, to the **Desktop** of **Windows Server 2016**.

25. Here, you are acting both as the **attacker** who logs into the **Windows 10** machine to create a malicious server and as the **victim** who logs into the **Windows Server 2016** virtual machine and downloads the server.

26. Double-click **CryptedFile.exe** to run this malicious executable.

Figure 1.2.16: Executing the Crypted file

27. As soon as the victim (here, **you**) double-clicks the server, the executable starts running, and the njRAT client (njRAT GUI) running on the **Windows 10** virtual machine establishes a persistent connection with the victim machine, as shown in the screenshot.

Figure 1.2.17: Connection established by njRAT

28. Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
29. Thus, you have created an undetectable Trojan that can bypass the anti-virus and firewall programs, as well as be used to maintain a persistent connection with the victim.
30. On completion of this lab, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
31. This concludes the demonstration of how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.
32. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.
33. Turn off the **Windows Server 2016** virtual machine.

TASK 3 Create a Server using the ProRat Tool

An ethical hacker or pen tester can use ProRat to audit their own network against remote access Trojans.

Note: The versions of the created client or host, and the appearance of the website may differ from this lab. However, the actual process of creating the server and client is as shown in this lab.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 3.1

Create Server with ProRat

1. Turn on the **Windows Server 2016** virtual machine.
2. Log in to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click the **ProRat.exe** file.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. The **ProRat** main window appears, as shown in the screenshot.

Attackers use malware to steal personal information, financial data, and business information from target systems. ProRat is a "remote administration tool" created by the PRO Group. ProRat was written in the C programming language and is capable of working with all Windows OSes. ProRat was designed to allow users to control their own computers remotely from other computers.

Figure 1.3.1: ProRat main window

However, attackers have co-opted it for their own nefarious purposes. Some hackers take control of remote computer systems to conduct a Denial-of-Service (DoS) attack, which renders the target system unavailable for normal personal or business use. These targeted systems include high-profile web servers such as banks and credit card gateways.

5. Click **Create**, and then click the **Create ProRat Server (342 Kbayt)** option to create a ProRat server.

Figure 1.3.2: Creating a ProRat Server

As with other Trojan horses, ProRat uses a client and server. It opens a port on the computer that allows the client to perform numerous operations on the server (the victim machine).

Some of ProRat's malicious actions on the victim's machine include:

- Logging keystrokes
- Stealing passwords
- Taking full control over files
- Drive formatting
- Opening and closing the DVD tray
- Hiding the taskbar, desktop, and start button
- Viewing system information

6. The **Create Server** window appears. In **Notifications**, leave the settings to default.

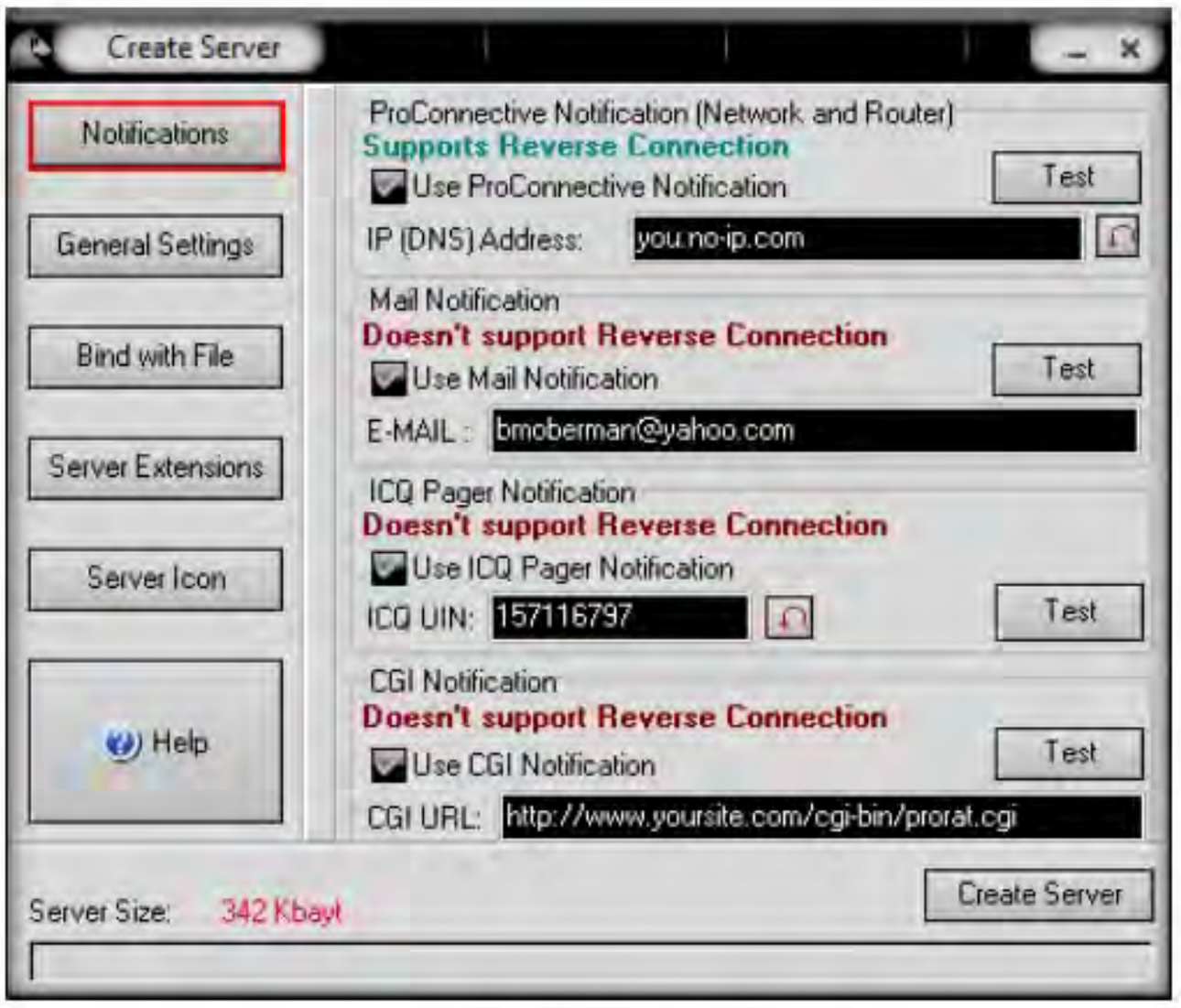


Figure 1.3.3: Create Server window

7. Click on the **General Settings** button to configure features such as **Server Port**, **Server Password**, **Victim Name**, and **port number**. In this lab, the default settings are chosen. Note down the **Server password**.
8. Uncheck the highlighted options under the **Victim Name** field, as shown in the screenshot.

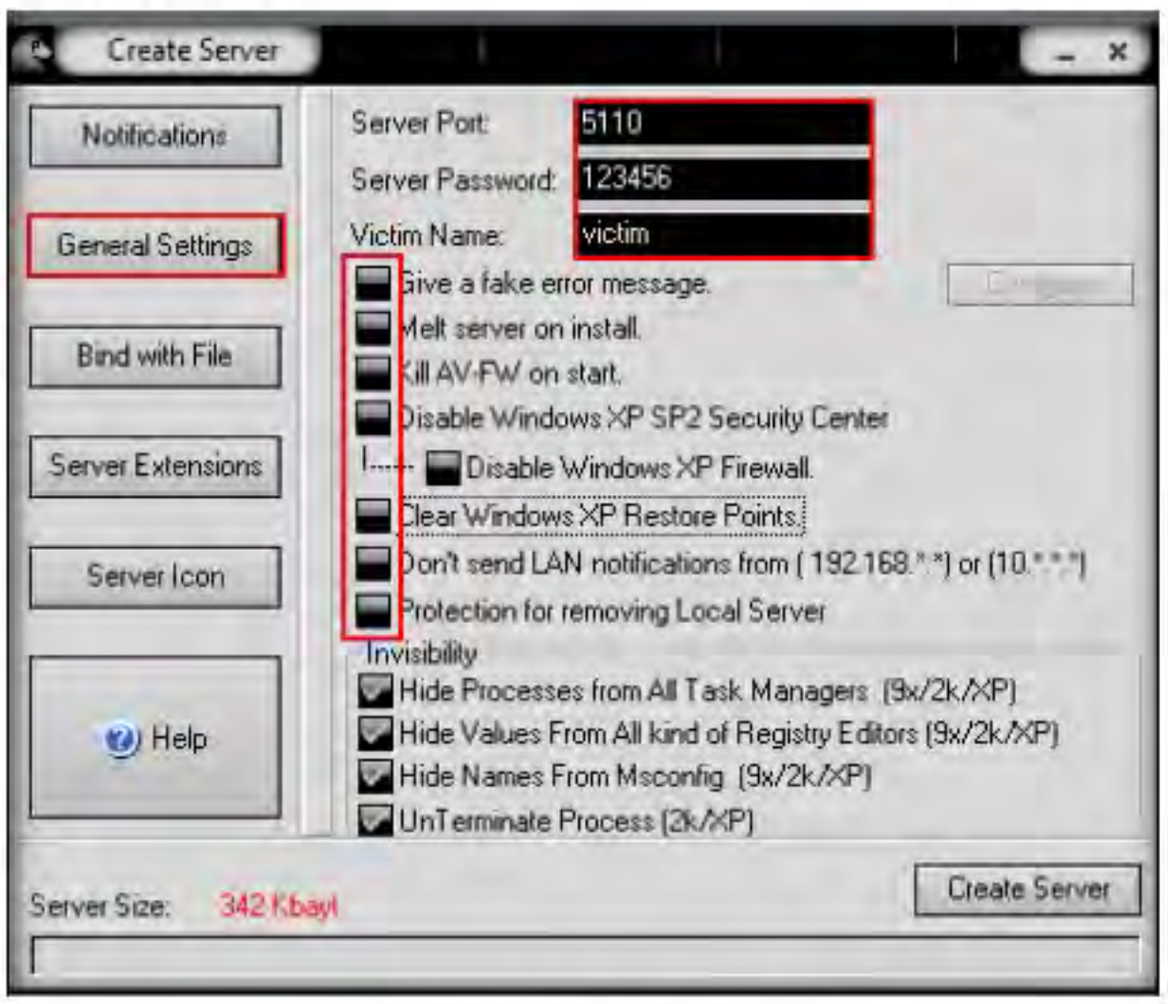


Figure 1.3.4: Configure the server

9. Click on the **Bind with File** button to bind the server with a file. In this lab, we are using a **.jpg** file to bind the server.
10. Check the **Bind server with a file** option and then click the **Select File** button.

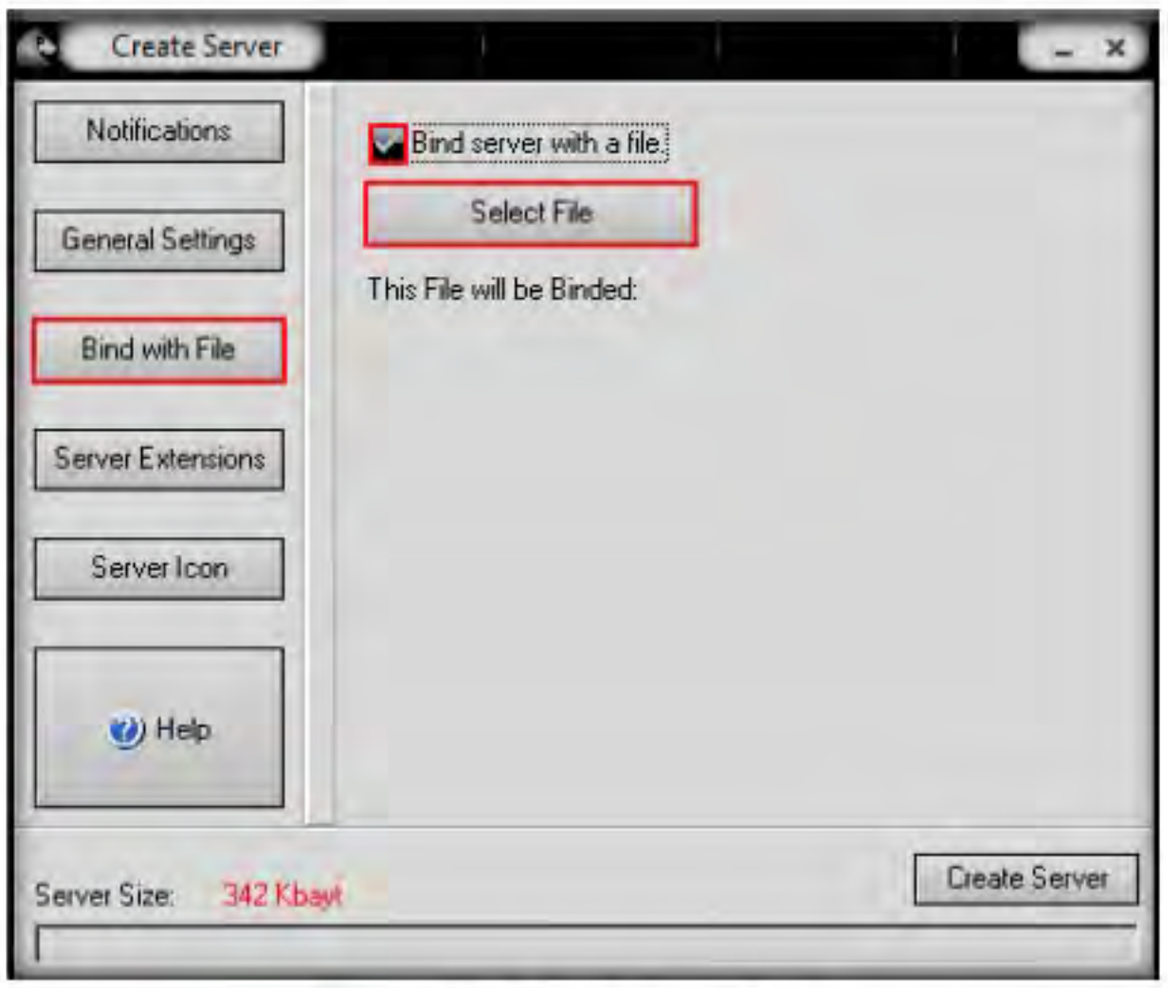


Figure 1.3.5: ProRat Binding with a file

11. An **open** pop-up window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images** and select **MyCar.jpg** in the browser window. Click **Open** to bind the file.

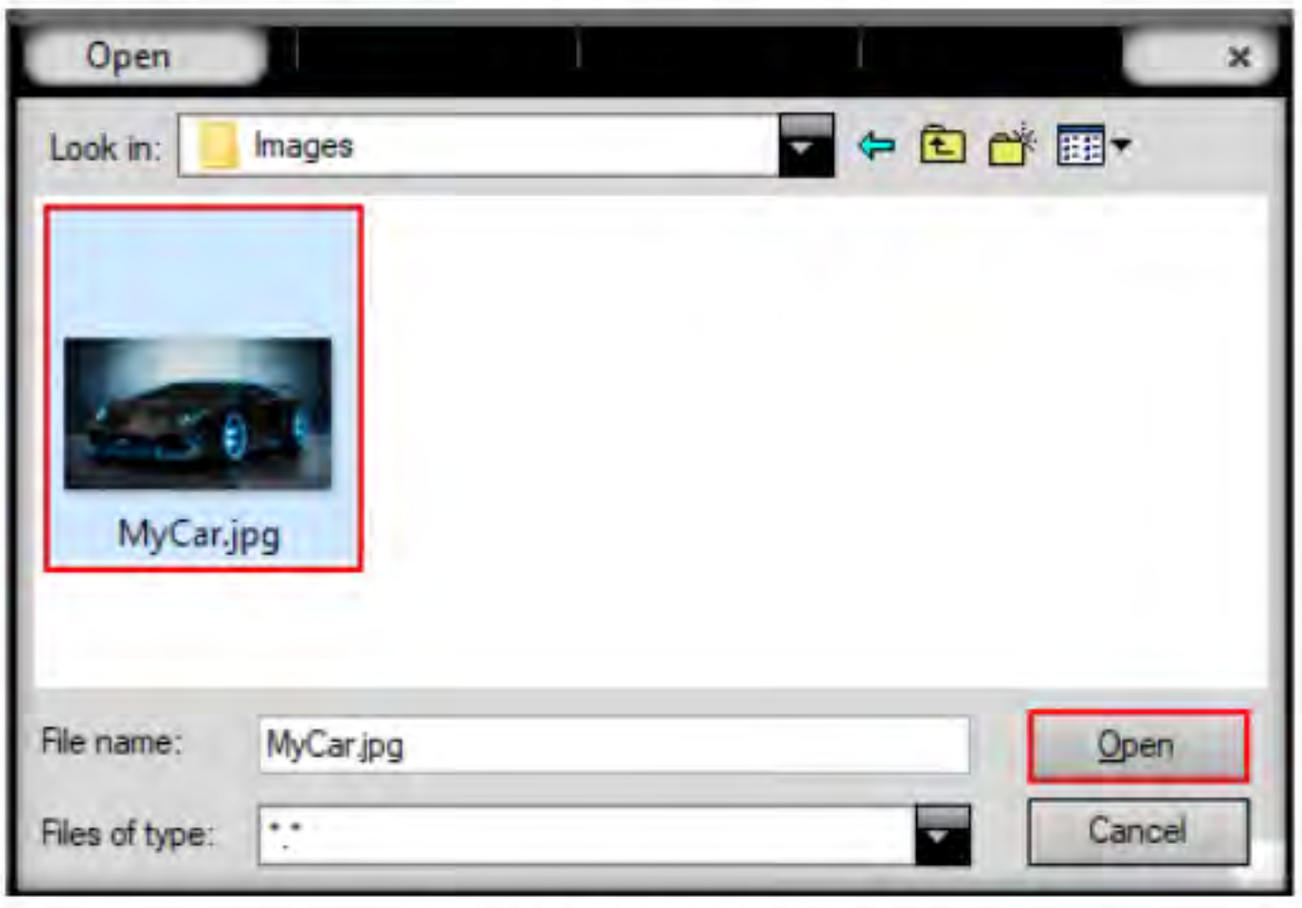


Figure 1.3.6: ProRat binding an image

12. A pop-up displays the prompt: **Server will bind with MyCar.jpg**; click **OK**.

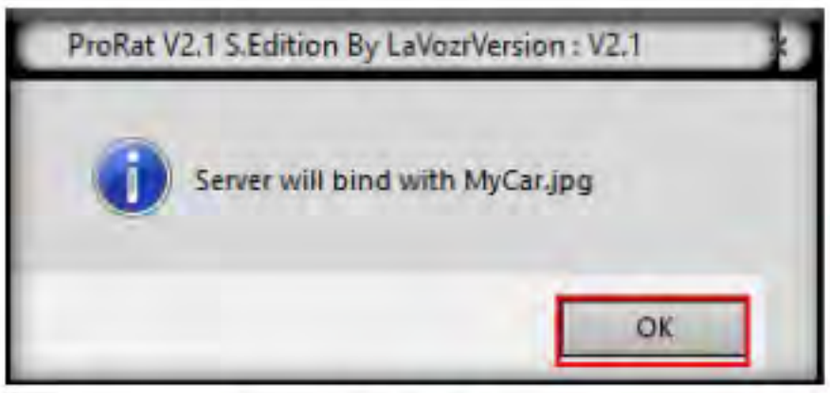


Figure 1.3.7: ProRat Pop-up

13. Click the **Server Extensions** button.
14. Under **Select Server Extension**, ensure that the **EXE (Has icon support)** checkbox is ticked.

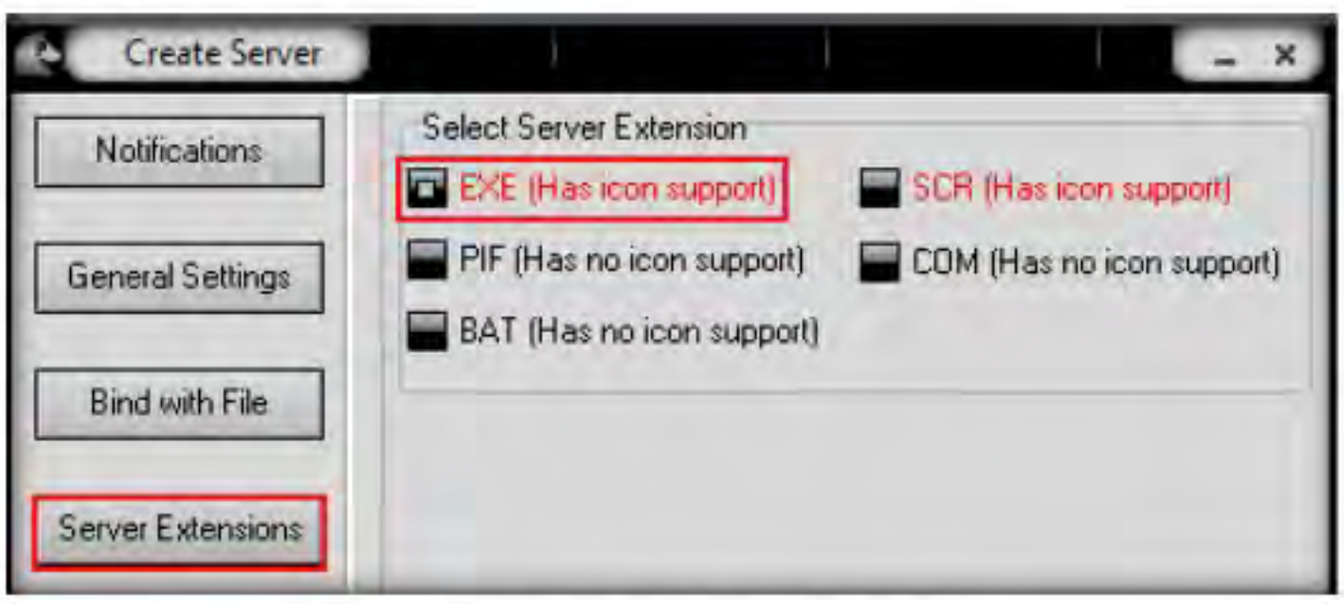


Figure 1.3.8: ProRat Server Extensions Settings

15. Click the **Server Icon** button. Under **Server Icon**, select any icon, and click **Create Server**.

Figure 1.3.9: ProRat creating a server

16. A pop-up states that the server has been created; click **OK**.

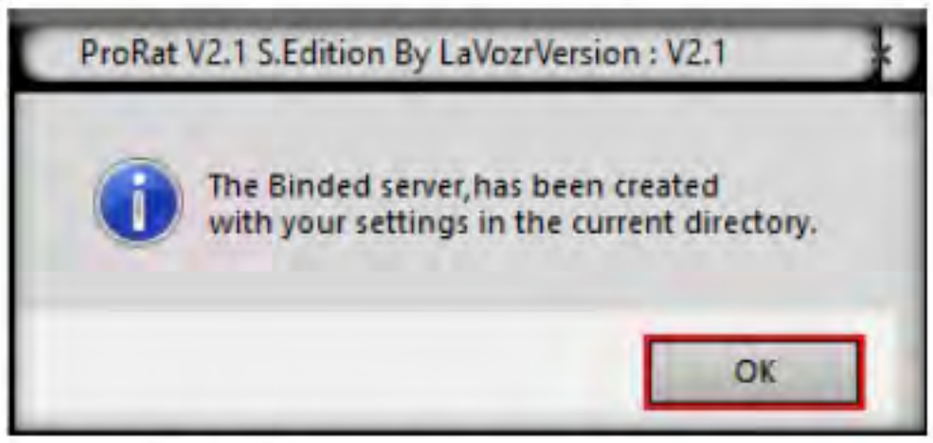


Figure 1.3.10: ProRat Server has created in the same current directory

17. The created server will be saved at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**. This server is named **binded_server.exe** by default. Close ProRat's Create Server window.

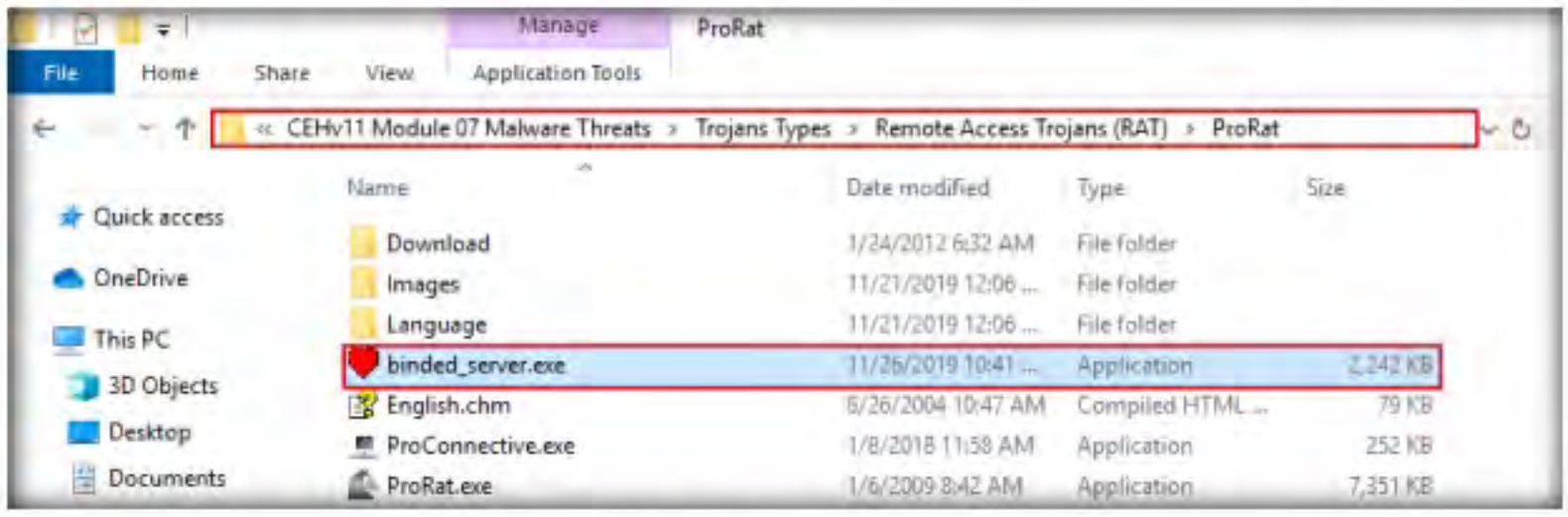


Figure 1.3.11: Server saved to the location

18. In real-time, hackers may craft such servers and send them by email or other communication media to the victim's machine.

Note: You need to **zip** the file before emailing it, as you cannot attach **.exe** files on some mail servers.

19. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

20. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click **binder_server.exe**.

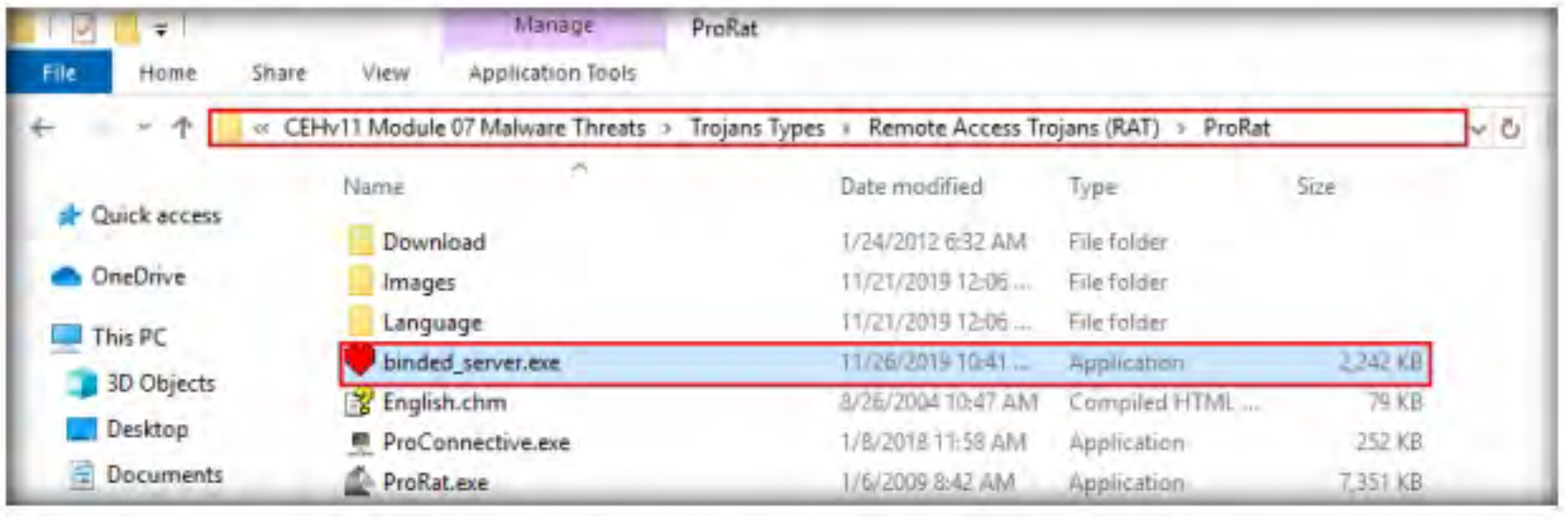


Figure 1.3.12: Executing the file sent from the Windows 10 machine

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

21. Switch back to the **Windows 10** virtual machine, and enter the IP address of **Windows Server 2016** in the **Ip** field; keep the default port number in the ProRat main window, and click **Connect**.
22. In this lab, the IP address of **Windows Server 2016** is **10.10.10.16**.

Note: The IP address of Windows Server 2016 may differ in your lab environment.

Figure 1.3.13: ProRat Connecting Infected Server

23. Enter the **password** you noted down when creating the server and click **OK**.

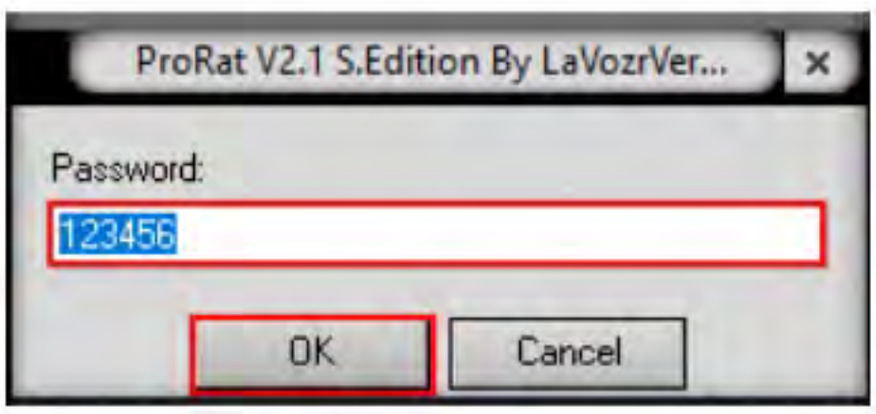


Figure 1.3.14: Entering the password

24. Now, you are **connected** to the victim machine.
25. ProRat begins to monitor user activities. It records all passwords, keystrokes, and other sensitive data.
26. To test the connection, click **PC Info**, and choose **System Information**.
27. ProRat displays the information of the victim machine, as shown in the screenshot.

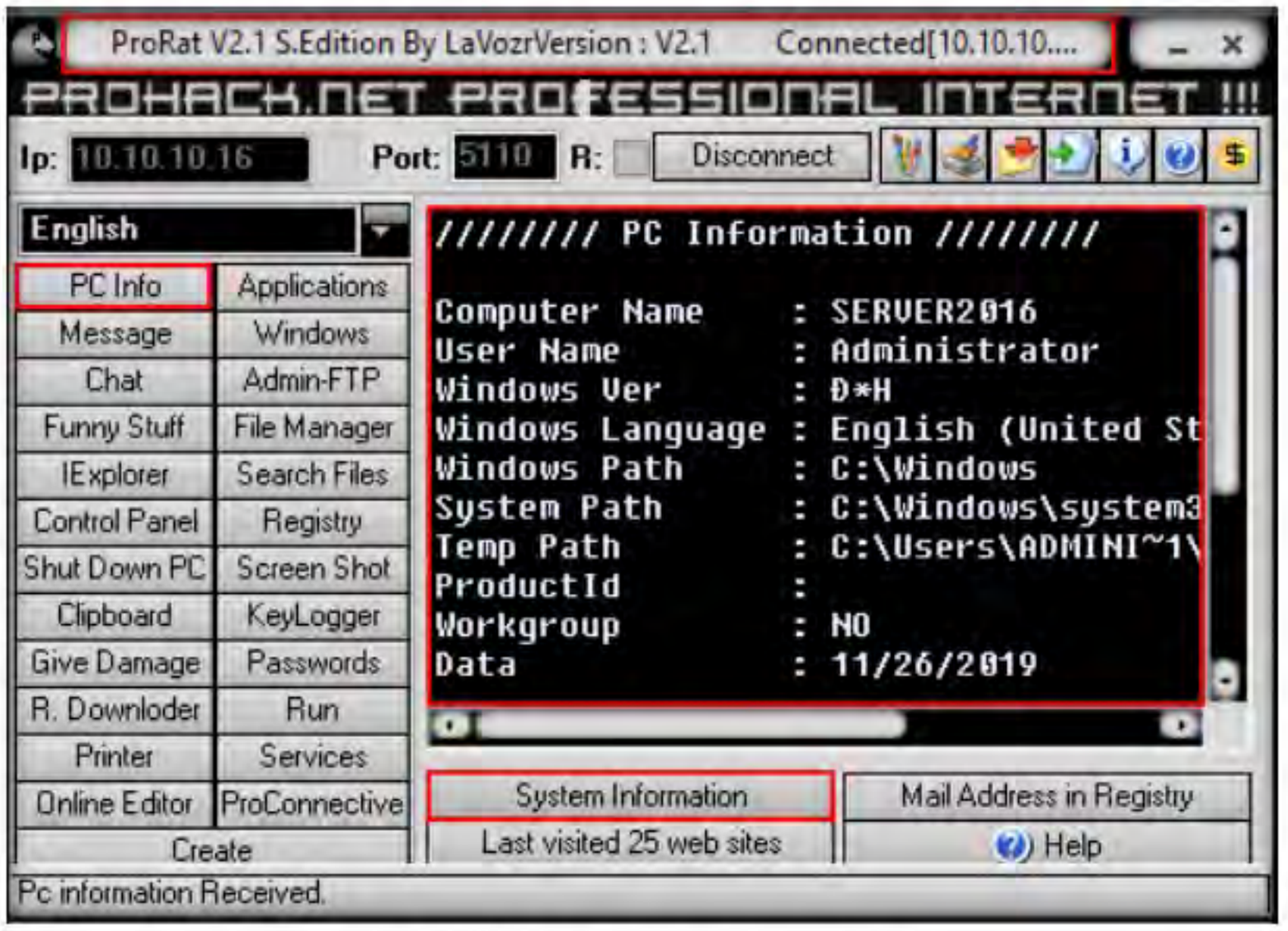


Figure 1.3.15: ProRat connected computer window

28. Click on **KeyLogger** to steal the user passwords for the online system. This will read the keystrokes performed on the victim machine.

TASK 3.2

Log All the Keystrokes

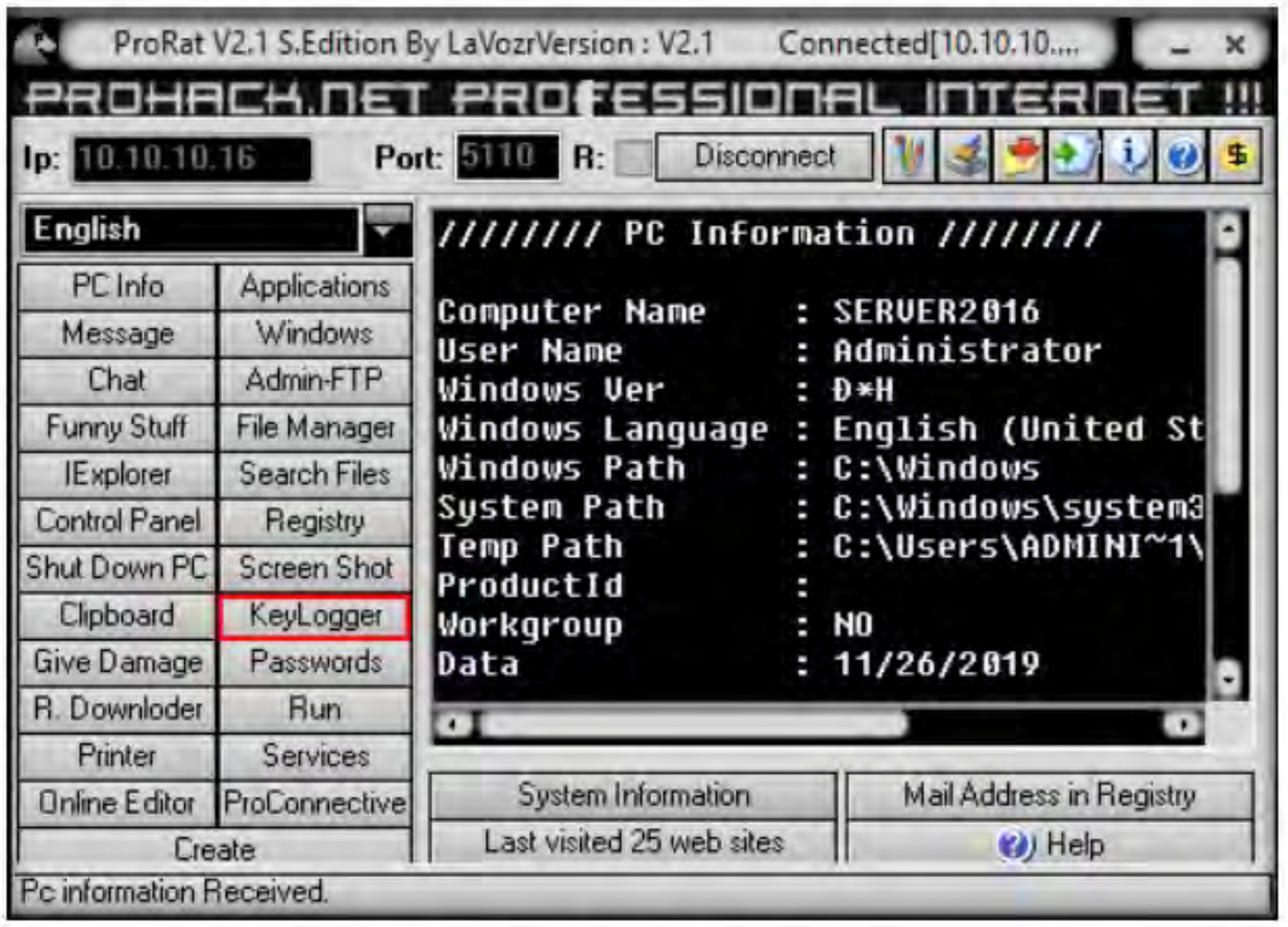


Figure 1.3.16: ProRat KeyLogger button

29. The **KeyLogger** window appears; click **Read Log** to view the key logs created by the target user on the victim machine.

Figure 1.3.17: ProRat KeyLogger window

30. Switch to the **Windows Server 2016** machine and open Notepad or a browser window, and type any text.

Figure 1.3.18: Text typed in Windows Server 2012 Notepad

31. While the victim is writing a **message** or entering a **username** and **password**, you can capture the log entity.

32. Now, switch to the **Windows 10** virtual machine, and periodically click **Read Log** to check for keystrokes logged from the victim machine. Close the KeyLogger window.

Note: ProRat Keylogger will not read special characters.

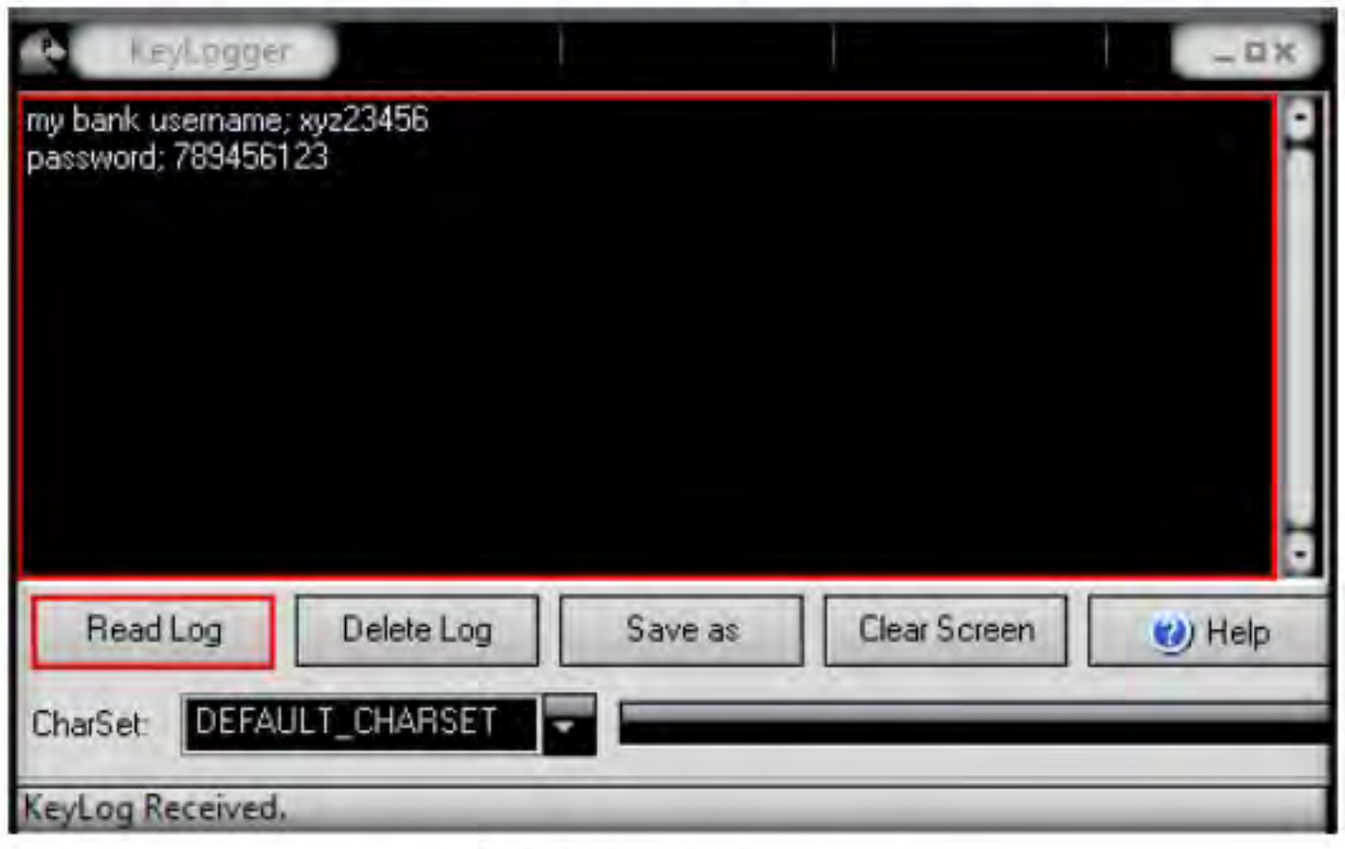


Figure 1.3.19: ProRat KeyLogger window

33. Now, click the **Registry** button to view the registry editor of the **Windows Server 2016** machine.

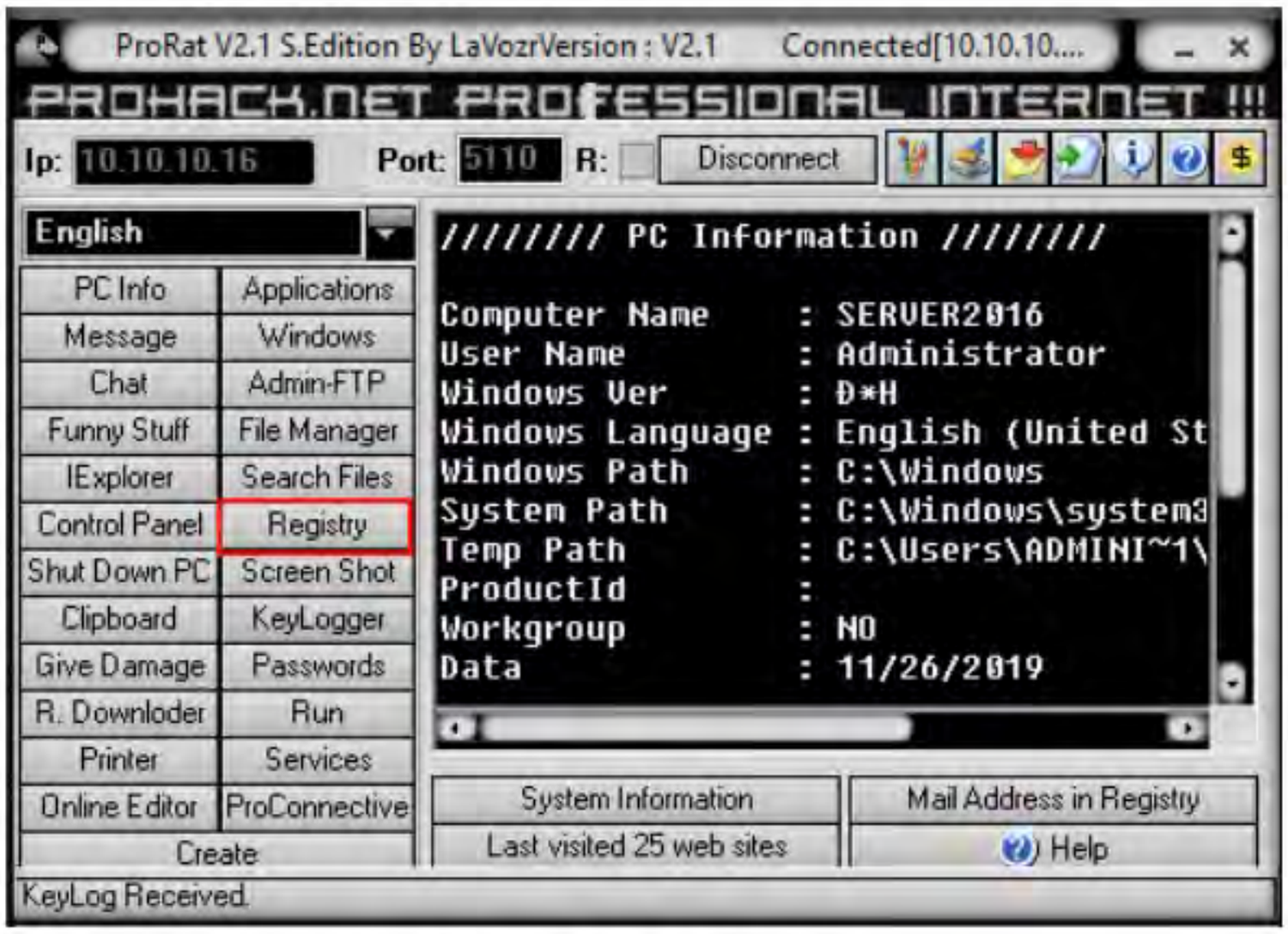


Figure 1.3.20: Pro Rat Registry option

34. The **Registry Editor** window appears, where you can choose the Registry Editor from the **Root Key** drop-down list. You can see and also modify the registry of the victim's machine, as shown in the screenshot.

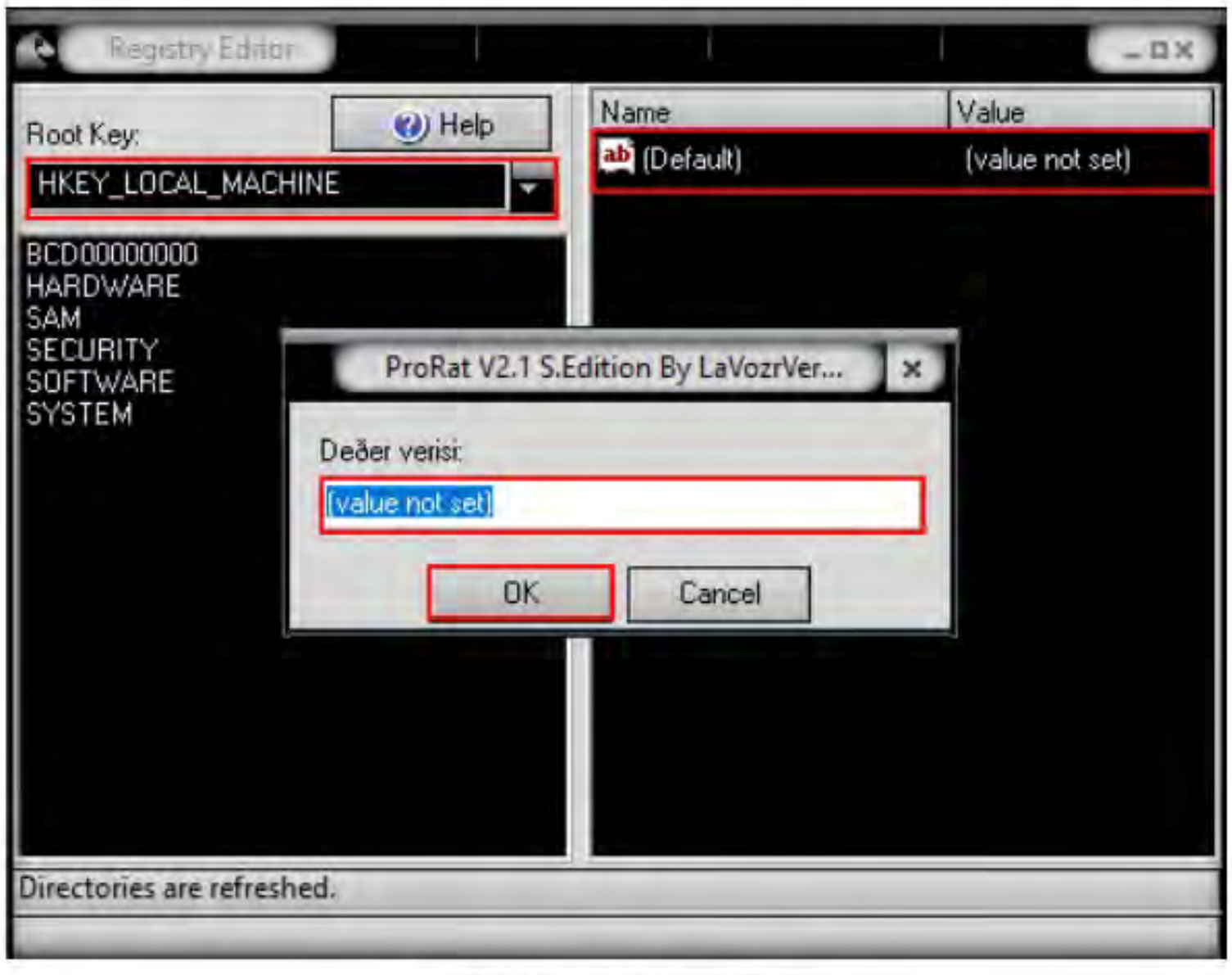


Figure 1.3.21: ProRat Editing registry

35. Close the **Registry** related windows and switch back to the ProRat main window.
36. In the same way, you can make use of the other options that allow you to explore and control the victim machine.
37. On the **Windows 10** machine, click **Disconnect** in the ProRat window.
38. On completion of this lab, launch **Task Manager**, look for the **services.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
39. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 4 Create a Trojan Server using Theef RAT Trojan

Note: The versions of the created client or host, and the appearance of its website, may differ from that of this lab. However, the actual process of creating the server and the client is the same.

Note: Ensure that the **Windows 10** and **Windows Server 2016** virtual machines are running.

TASK 4.1

Execute Server in the Victim Machine

1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**.
2. Log in to the **Windows Server 2016** virtual machine (as a **victim**) using the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

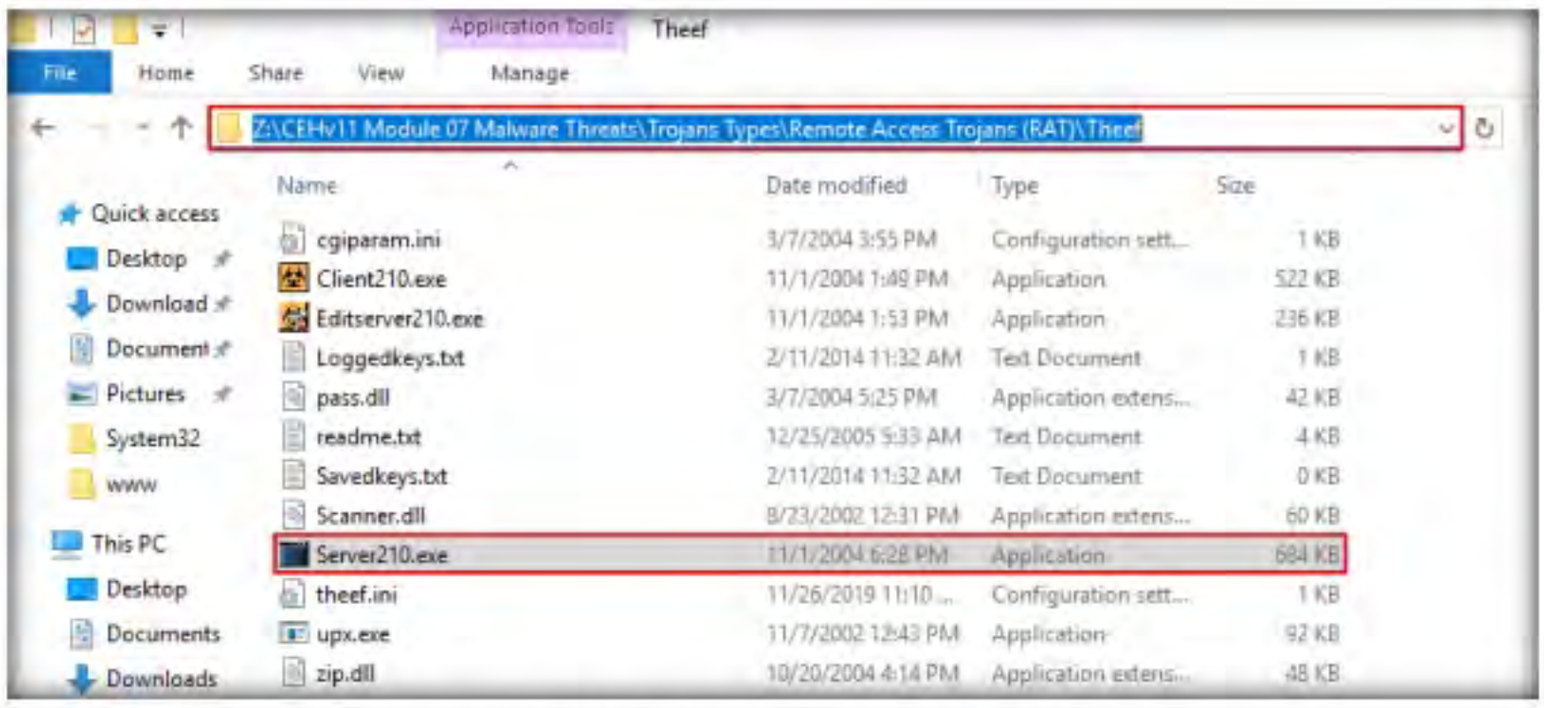


Figure 1.4.1: Windows Server 2012: Theef Folder

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. Now, log in to the **Windows 10** virtual machine (as an **attacker**) using the credentials **Admin** and **Pa$$w0rd**.

TASK 4.2

Establish Connection with the Target

5. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.

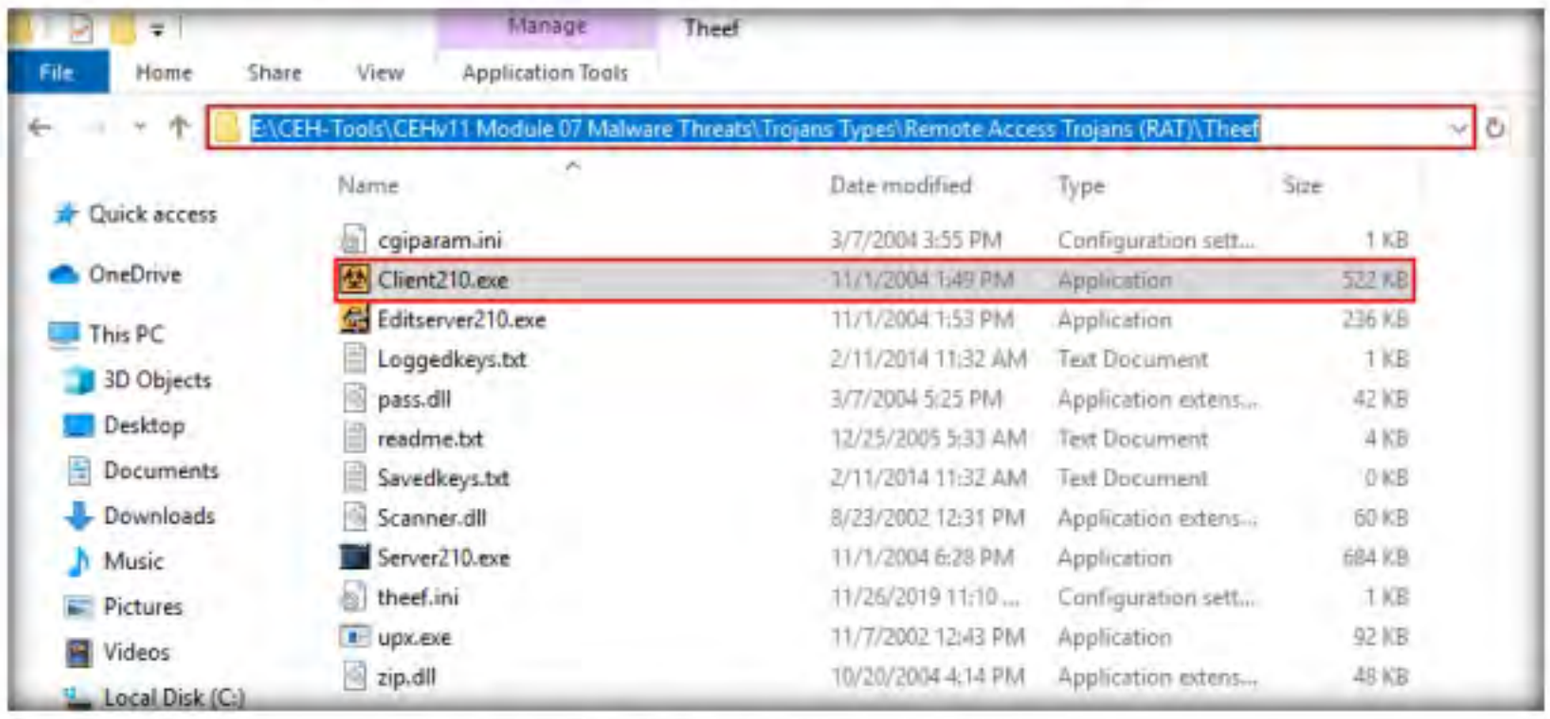


Figure 1.4.2: Windows 10-Running Client210.exe

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

6. The **Theef** main window appears, as shown in the screenshot.

7. Enter the IP address of the target machine (here, **Windows Server 2016**) in the **IP** field (**10.10.10.16**), and leave the **Port** and **FTP** fields set to default; click **Connect**.

Note: The target IP address may vary in your lab environment.

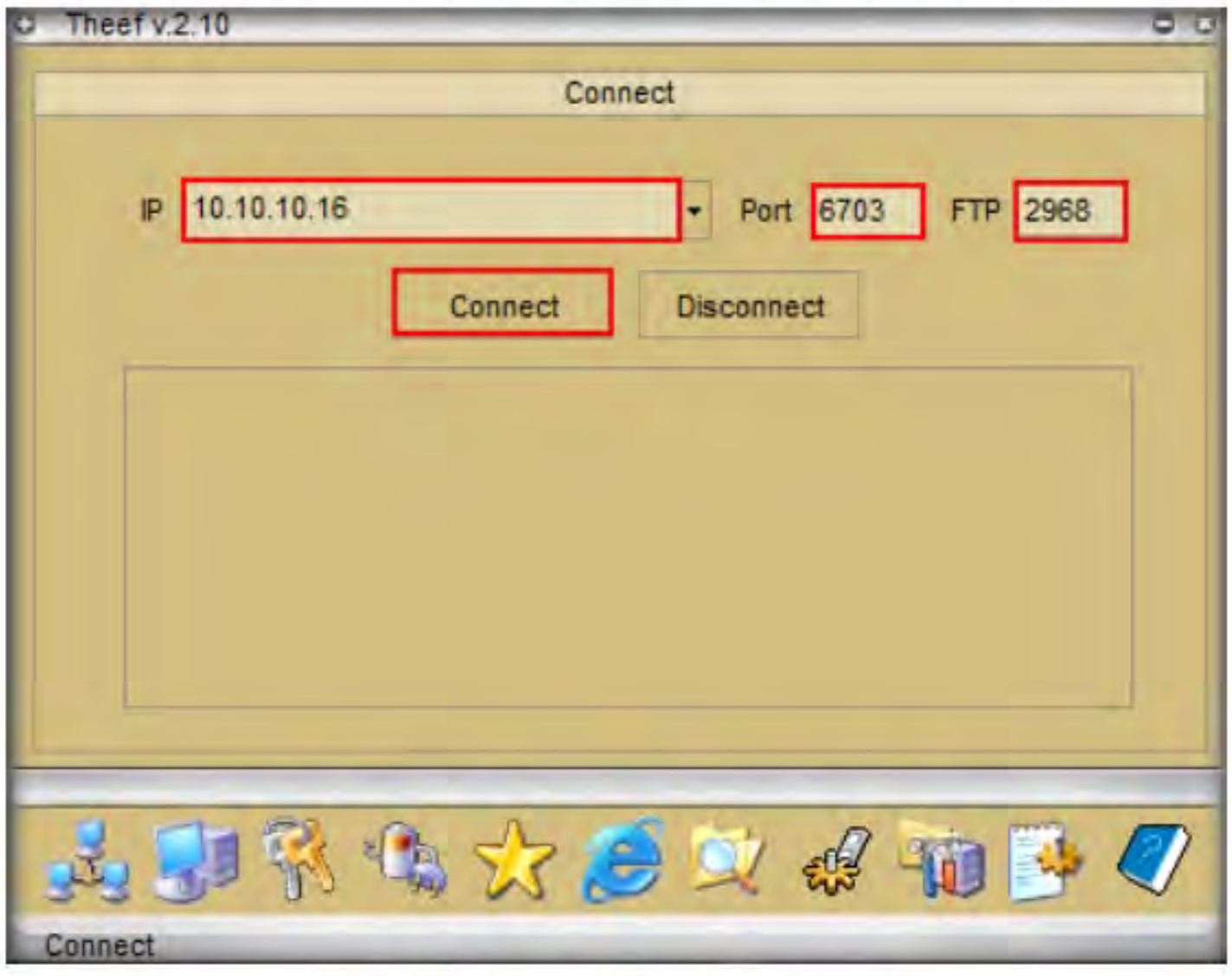


Figure 1.4.3: Theef Connecting to the Victim Machine

8. Now, from **Windows 10**, you have successfully established a remote connection with the **Windows Server 2016** machine.
9. To view the computer's information, click the **Computer Information** icon ( ) from the lower part of the window.

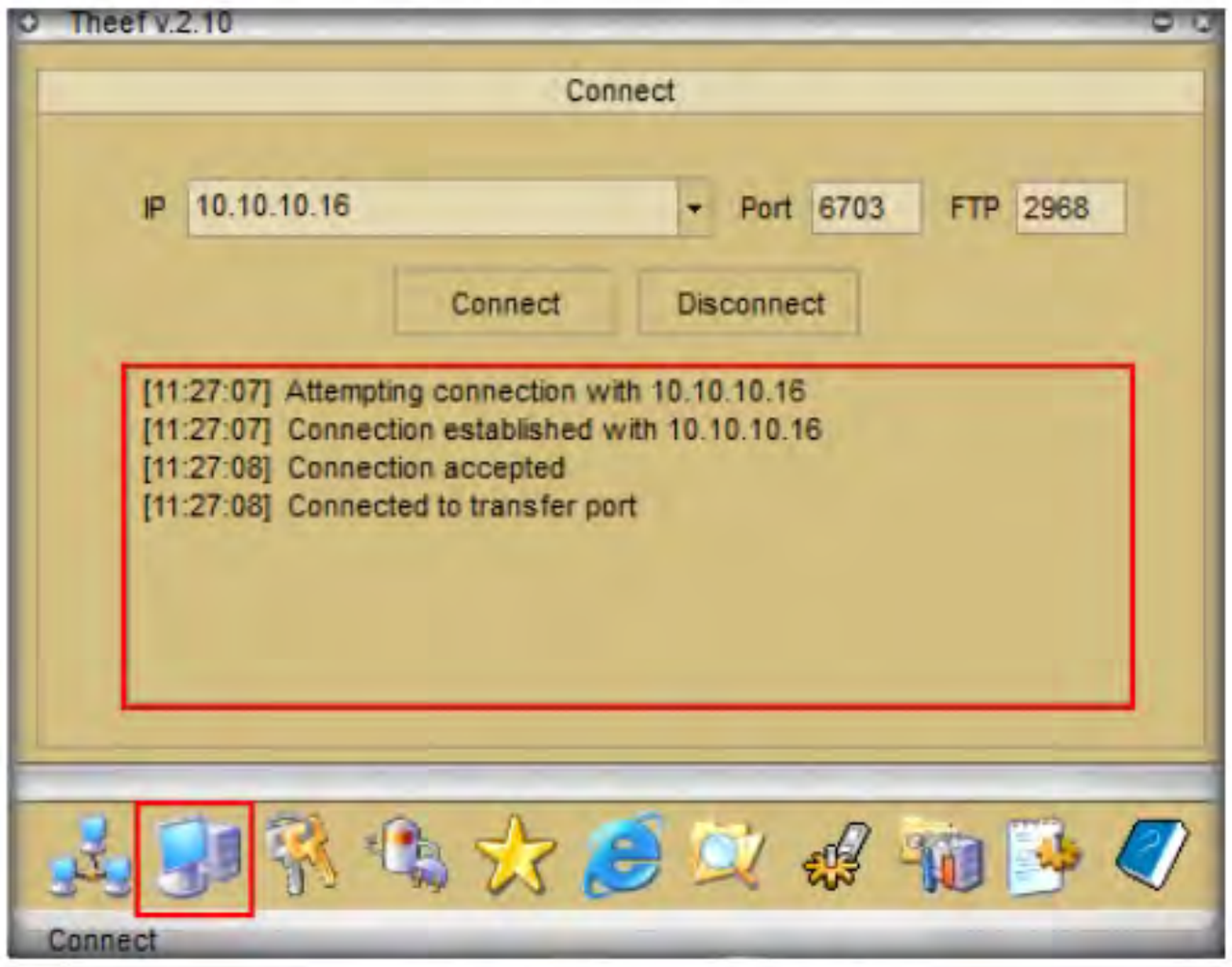


Figure 1.4.4: Theef Gained access to the Victim Machine

TASK 4.3

Extract System Information

10. In **Computer Information**, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.
11. Here, for example, selecting **PC Details** reveals computer-related information.

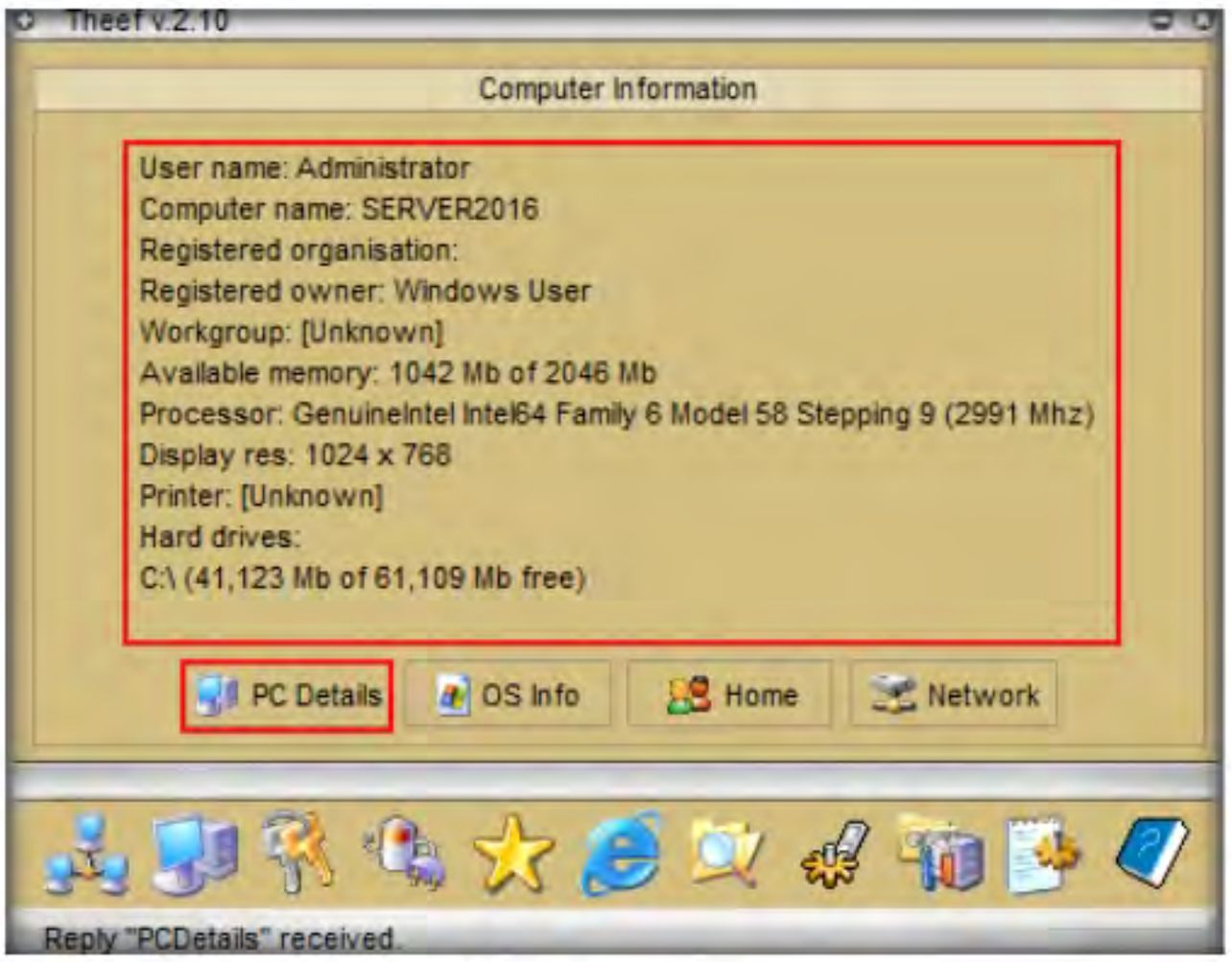


Figure 1.4.5: Theef Computer Information

12. Click the **Spy** icon ( ) to perform various operations on the target machine.

Figure 1.4.6: Theef Spy

13. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.

14. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.

TASK 4.4

Manipulate Tasks in the Task Manager

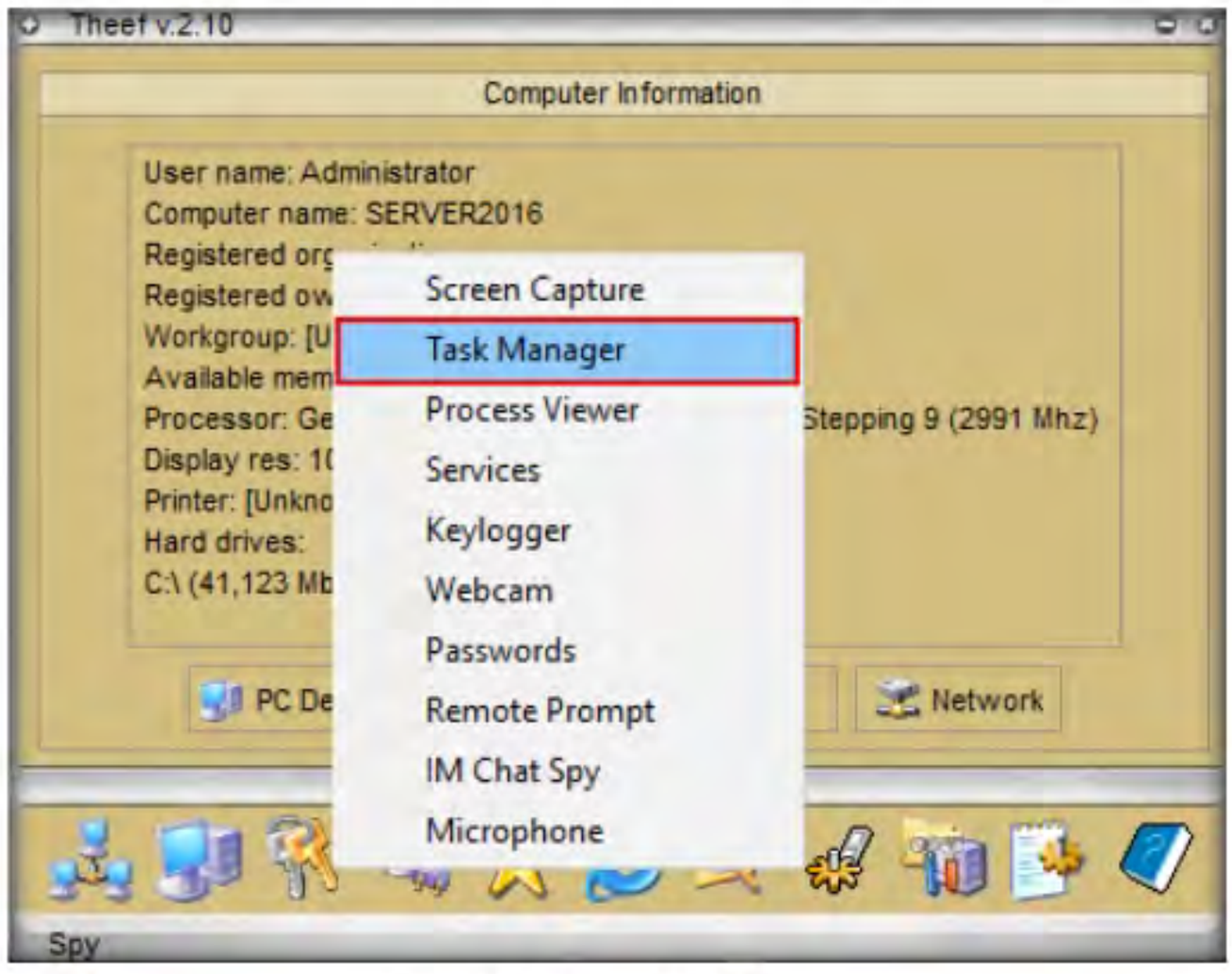


Figure 1.4.7: Selecting the Task Manager

15. In the **Task Manager** window, select a process (task);

    click the **Close window** icon ( ) to end the task on the target machine.

16. If you cannot see the running processes, click the **Reload** icon ( ) to view the processes.

17. Close the **Task Manager** window.

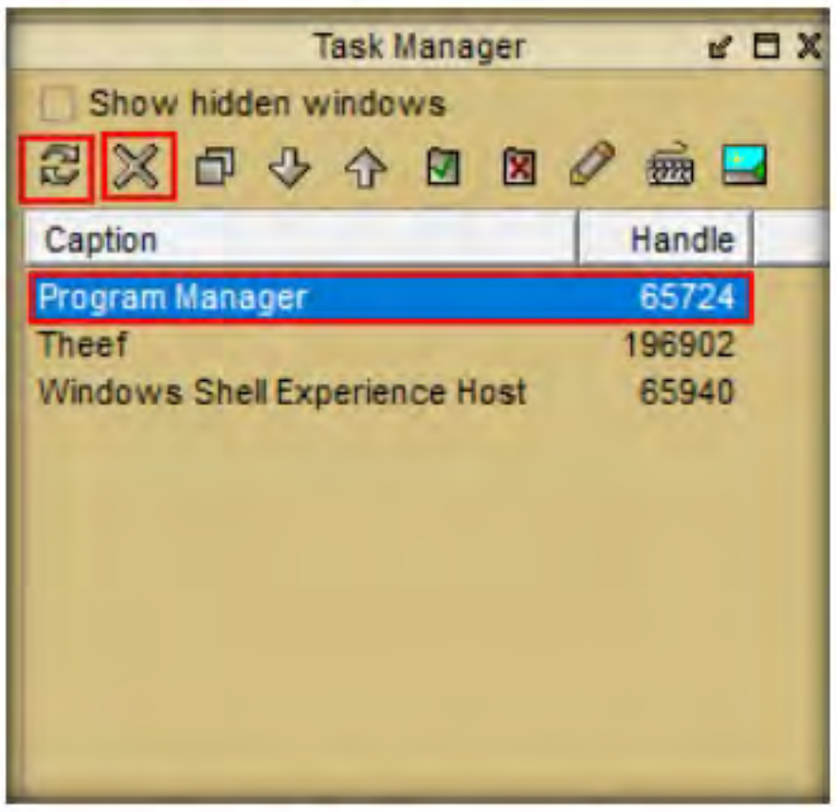


Figure 1.4.8: Theef Task Manager Window

Note: The tasks running in the task manager may vary in your lab environment.

18. From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.

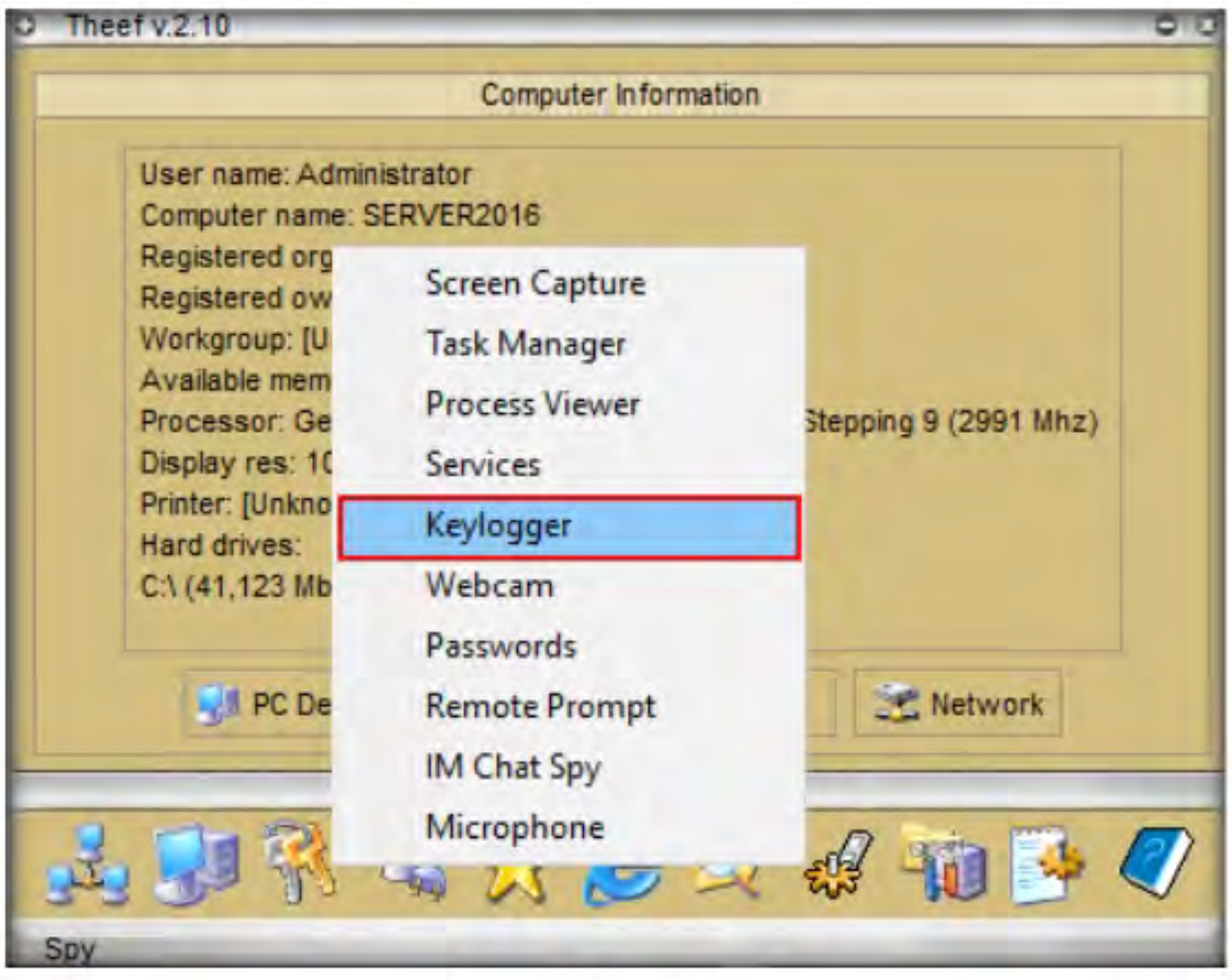


Figure 1.4.9: Theef Keylogger

19. The **Keylogger** pop-up appears; click the **Start** icon to read the keystrokes of the victim machine.

Figure 1.4.10: Theef Keylogger Screen

20. Switch back to the victim machine (**Windows Server 2016**). Open a browser window and browse some websites or open a text document and type some sensitive information.

Figure 1.4.11: Victim Machines Keystrokes

21. Switch back to the attacker machine (**Windows 10**) to view the recorded keystrokes of the victim machine in the Theef **Keylogger** window.

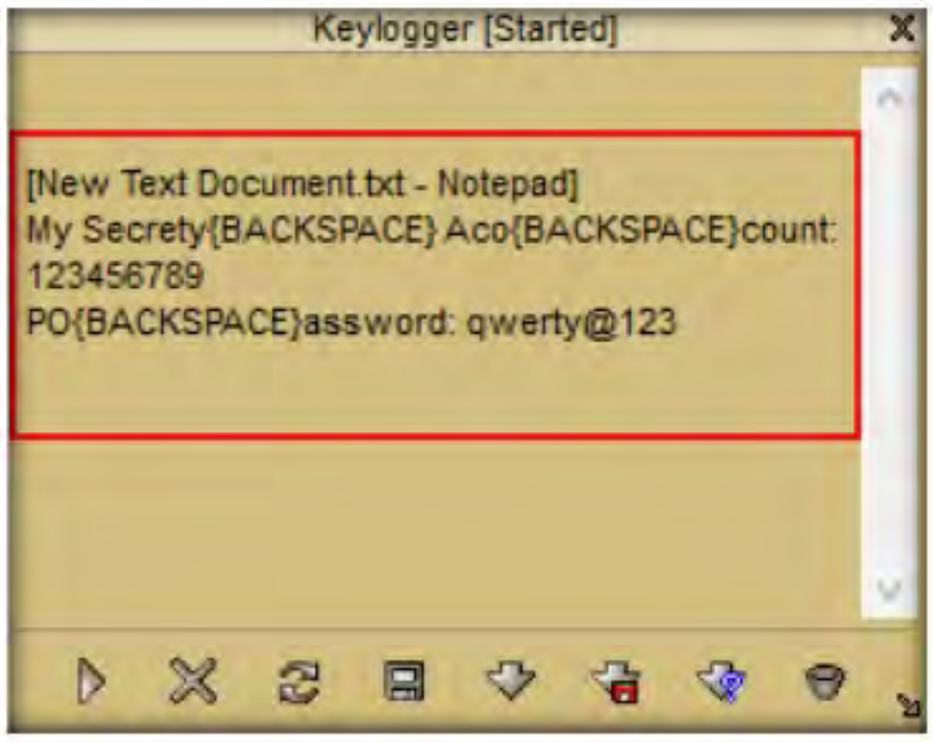


Figure 1.4.12: Theef Keylogger Recorded Keystrokes

22. Close the Theef **Keylogger** window.
23. Similarly, you can access the details of the victim machine by clicking on the various icons.

24. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines and turn off both of the virtual machines.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Infect the Target System using a Virus

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable codes and operates without the knowledge or desire of the user.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself *n* number of times, where *n* is a number specified by the attacker.

Worldwide, most businesses have been infected by a virus at some point. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can only infect outside machines with the assistance of computer users.

Like viruses, computer worms are standalone malicious programs that independently replicate, execute, and spread across network connections, without human intervention. Worms are a subtype of virus. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

An ethical hacker and pen tester during an audit of a target organization must determine whether viruses and worms can damage or steal the organization's information. They might need to construct viruses and worms and try to inject them into the target network to check their behavior, learn whether an anti-virus will detect them, and find out whether they can bypass the firewall.

Lab Objectives

- Create a virus using the JPS Virus Maker Tool and infect the target system

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- JPS Virus Maker Tool located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Duration

Time: 10 Minutes

Overview of Viruses and Worms

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs by making use of specific events. Viruses need such events to take place, since they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, Web sites, malicious advertisements, flashcards, pop-ups, or other methods. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings, or perform other malicious activities.

Like a virus, a worm does not require a host to replicate, but in some cases, the worm's host machine also infects. At first, Blackhat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they concentrated and targeted Windows OSes using the same worms by sharing them by email, IRC, and other network functions.

Lab Tasks

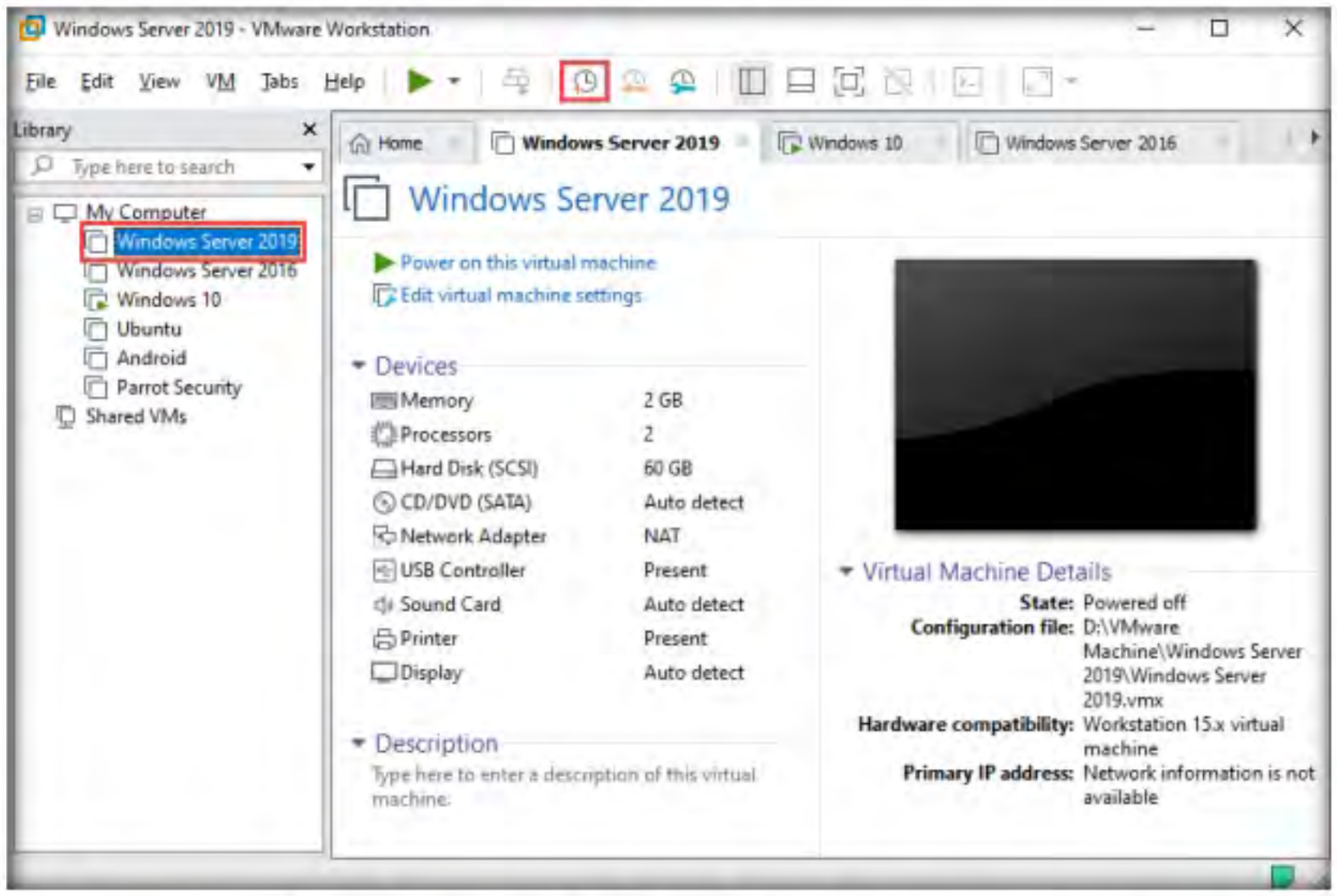
TASK 1

Create a Virus using the JPS Virus Maker Tool and Infect the Target System

An ethical hacker and pen-tester can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

Note: Before performing this task, take a snapshot of the **Windows Server 2019** virtual machine as the virus will infect the machine.

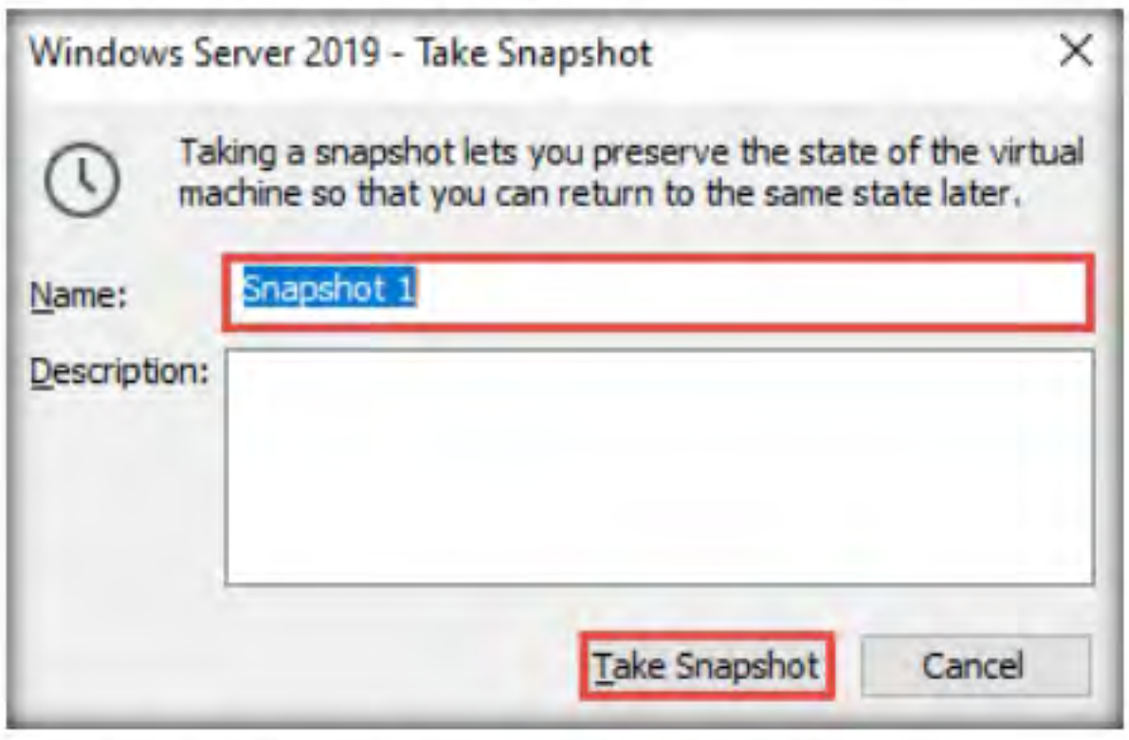
a. In the **VMware Workstation** window, click **Windows Server 2019** in the left pane and click the **Take a snapshot of this virtual machine** ( ) icon, as shown in the screenshot.



Note: Take a Snapshot of the virtual machine before launching the JPS Virus Maker tool.

The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.

b. The **Windows Server 2019 - Take Snapshot** pop-up appears; type a name for the snapshot in the **Name** field, leave the description field set to default, and click **Take Snapshot**.



1. Turn on the **Windows Server 2019** virtual machine.
2. Log in to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Launch JPS Virus Maker

3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.

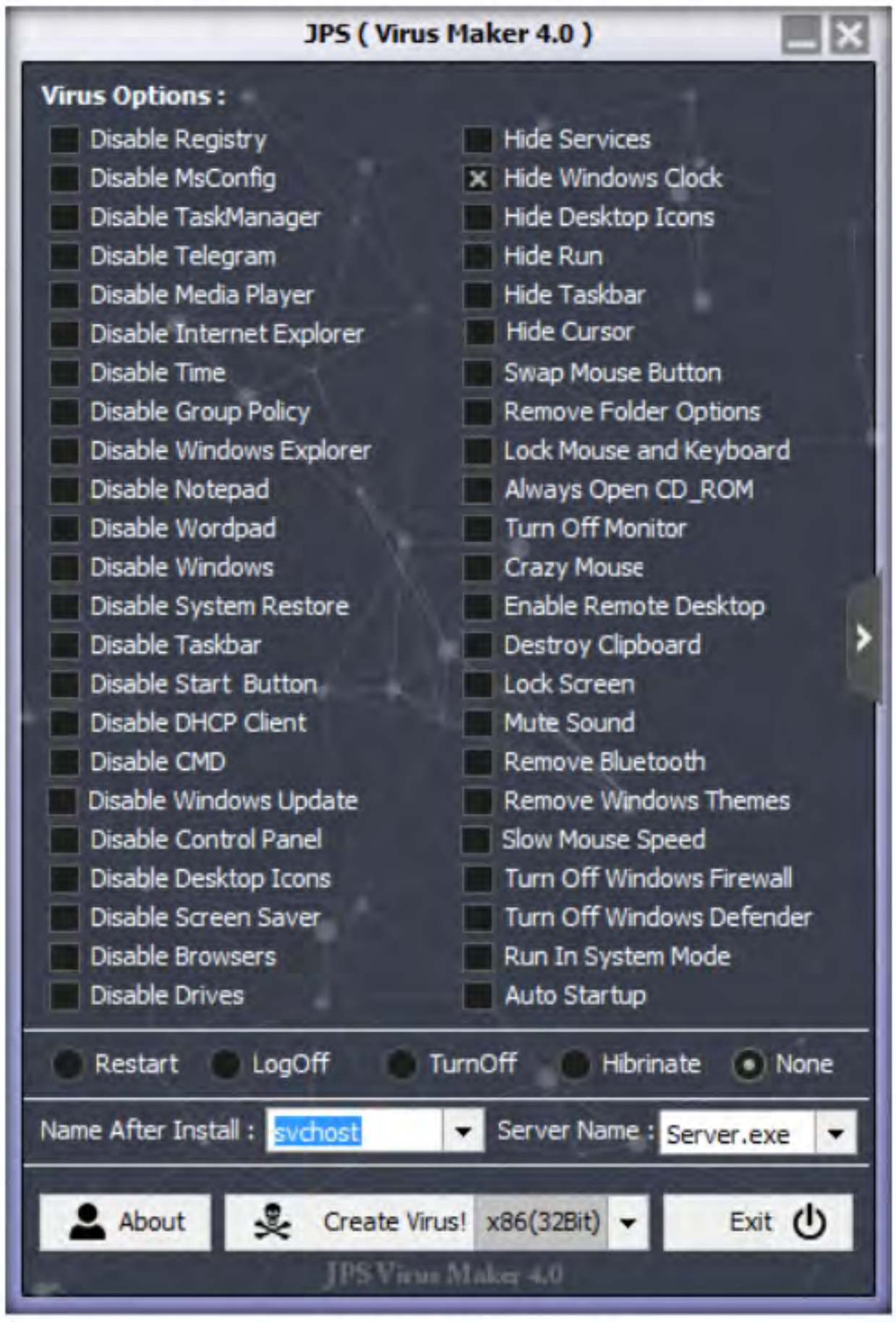


Figure 2.1.1: JPS Virus Maker main window

5. The window displays various features and options that can be chosen while creating a virus file.
6. From the **Virus Options**, check the **options** that you want to embed in a new virus file.
7. In this lab, the options embedded in the virus file are **Disable TaskManager**, **Disable Windows Update**, **Disable Control Panel**, **Disable Drives**, **Hide Windows Clock**, **Hide Desktop Icons**, **Enable Remote Desktop**, **Remove Bluetooth**, **Turn Off Windows Firewall**, **Turn Off Windows Defender**, and **Auto Startup**.

Figure 2.1.2: JPS Virus Maker main window with options selected

8. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.

9. Now, before clicking on **Create Virus!**, click the right arrow icon ( ) from the right-hand pane of the window to configure the virus options.

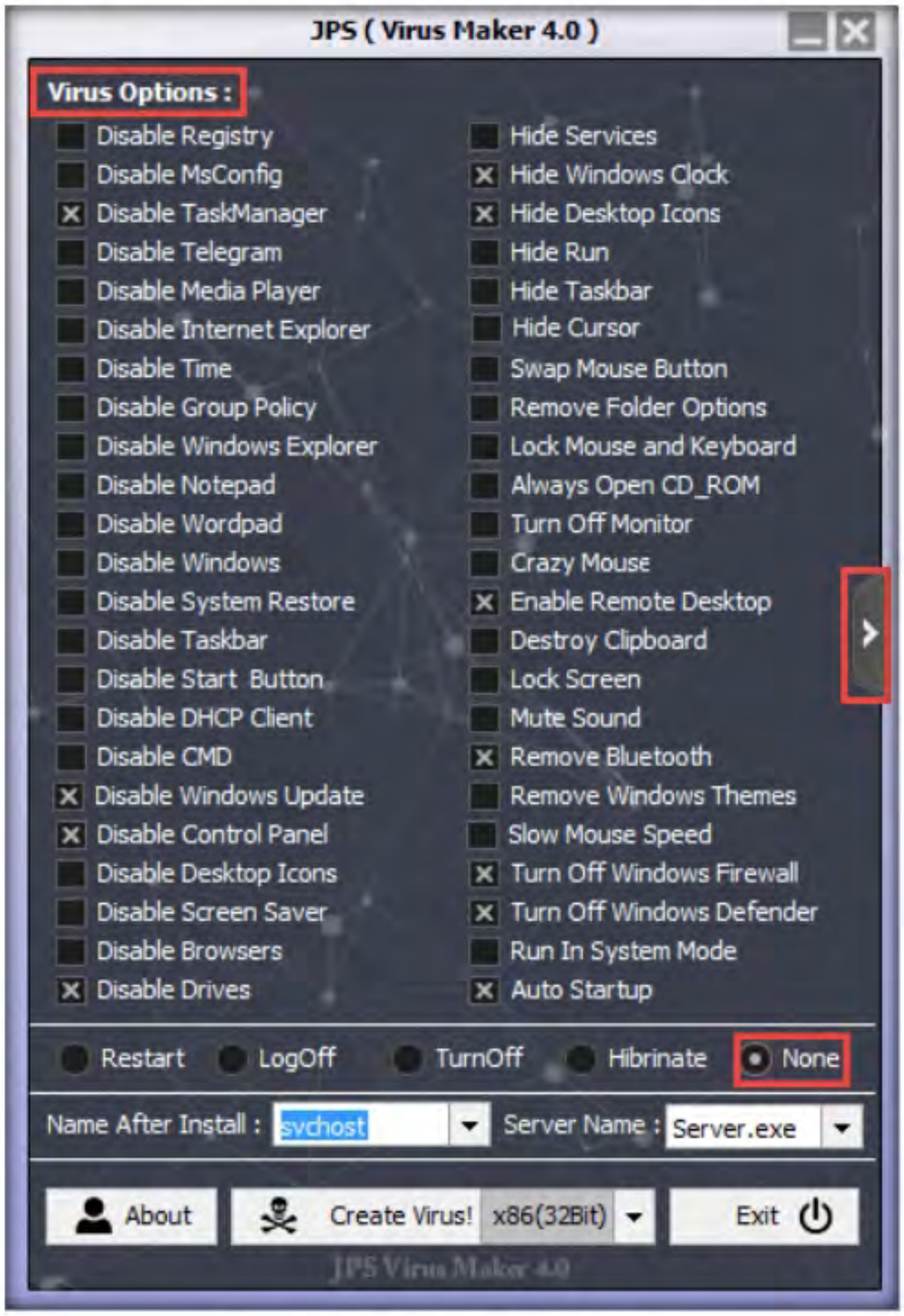


Figure 2.1.3: JPS Virus Maker Virus Configuration

TASK 1.2

Configure the Virus Options

10. A **Virus Options** window appears, as shown in the screenshot.
11. Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.
12. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self-replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.
13. Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.
14. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x64(32Bit)**; click **Create Virus!**

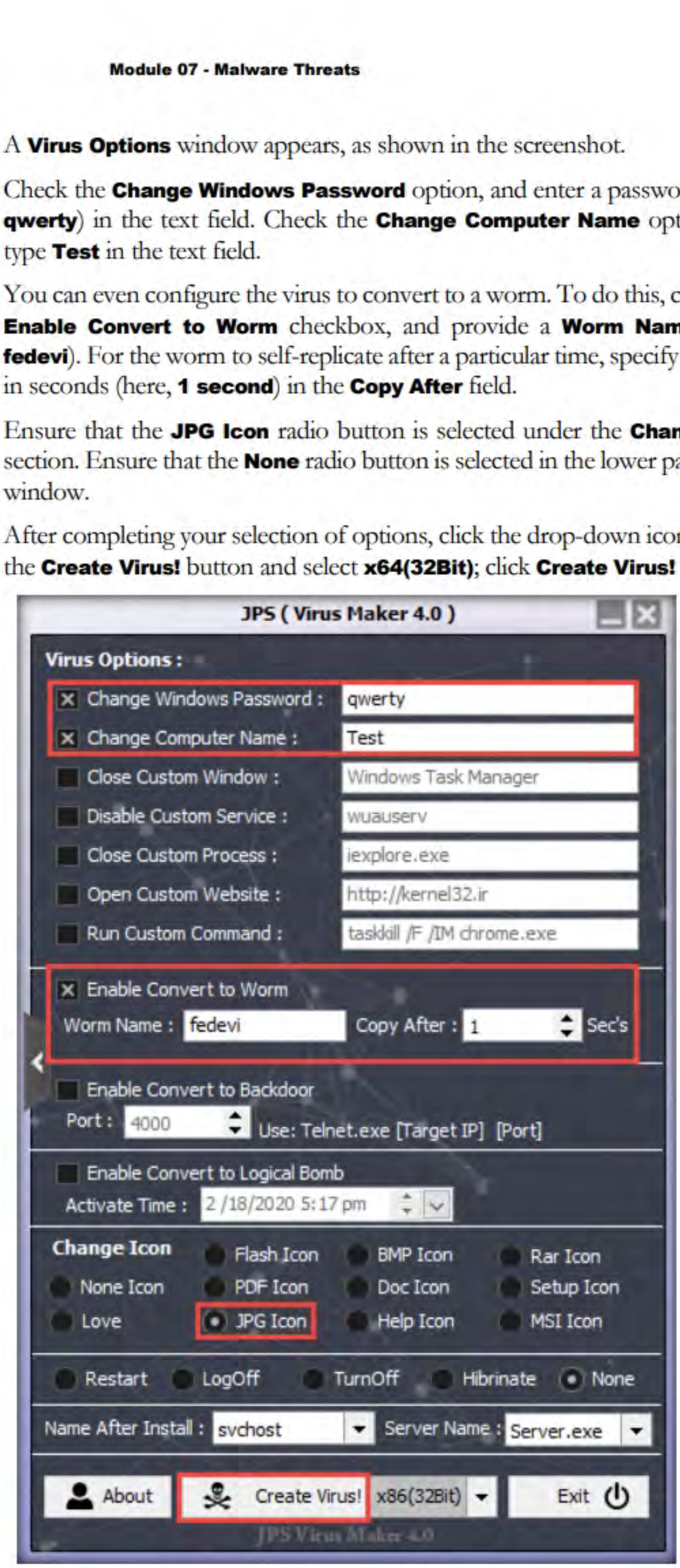


Figure 2.1.4: Creating a Virus

15. A **Virus Created Successful!** pop-up appears; click **OK**.

Figure 2.1.5: JPS Virus Maker Server Created successfully message

16. The newly created virus (server) is placed automatically in the **folder** where **jps.exe** is located, but with the name **Server.exe**. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and observe that the newly created virus with the name **Server.exe** is available at the specified location.

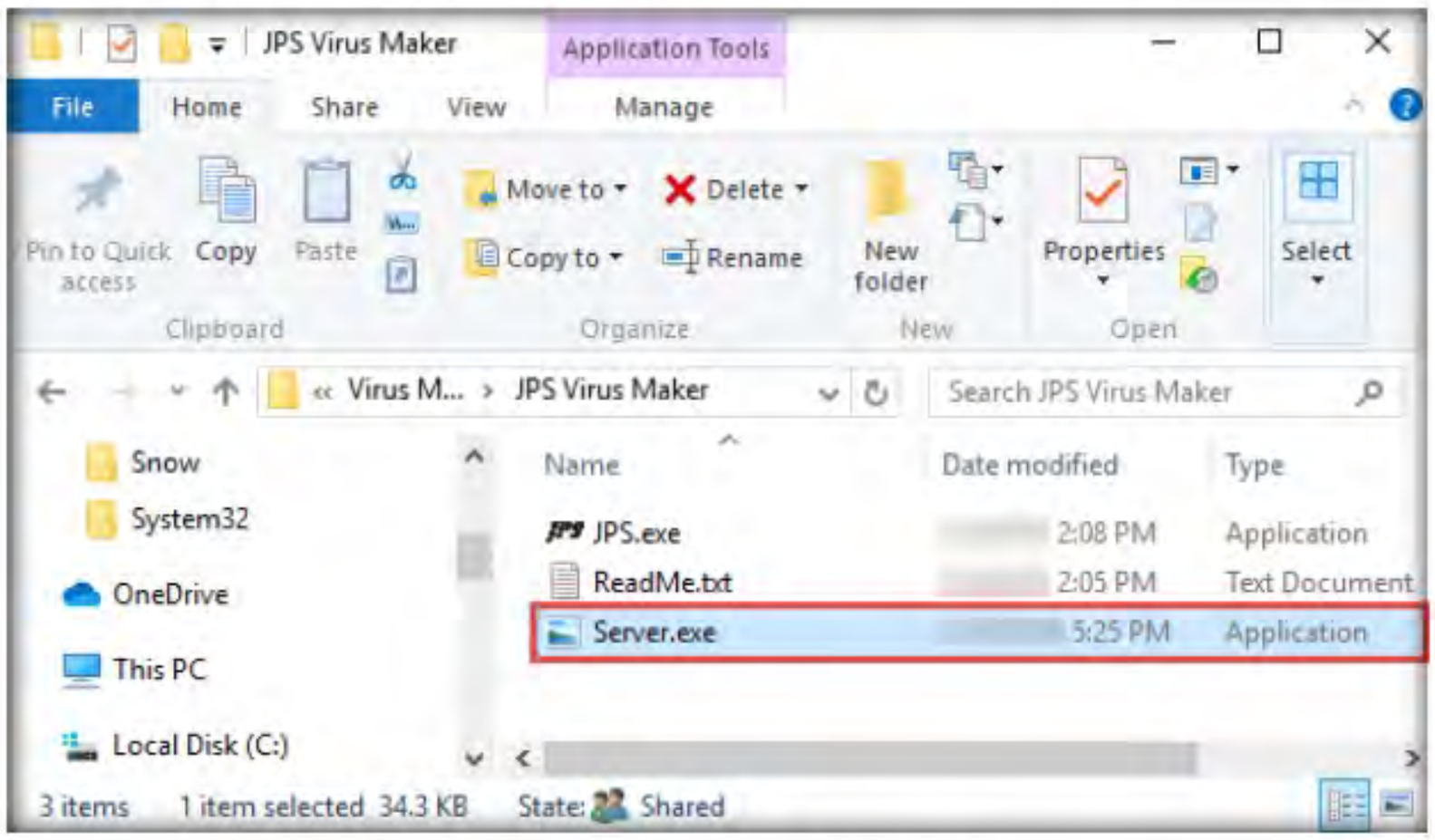


Figure 2.1.6: Virus Created in the Default Location

17. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
18. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
19. Log in to the **Windows Server 2019** virtual machine (as the **victim**) using the credentials **Administrator** and **Pa$$w0rd**.

20. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

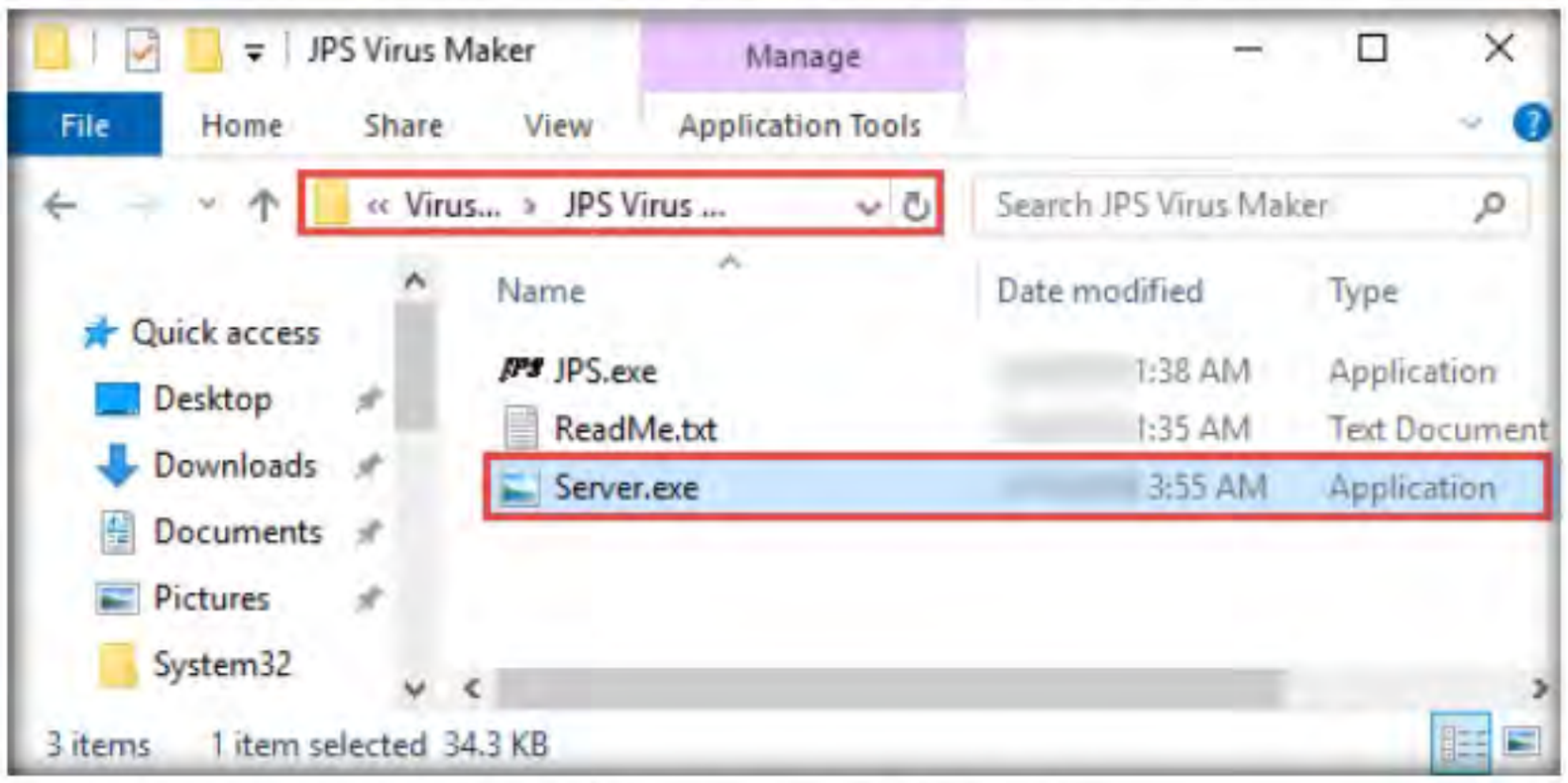


Figure 2.1.7: Executing a virus in the Victim Machine

21. Once you have executed the virus, the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

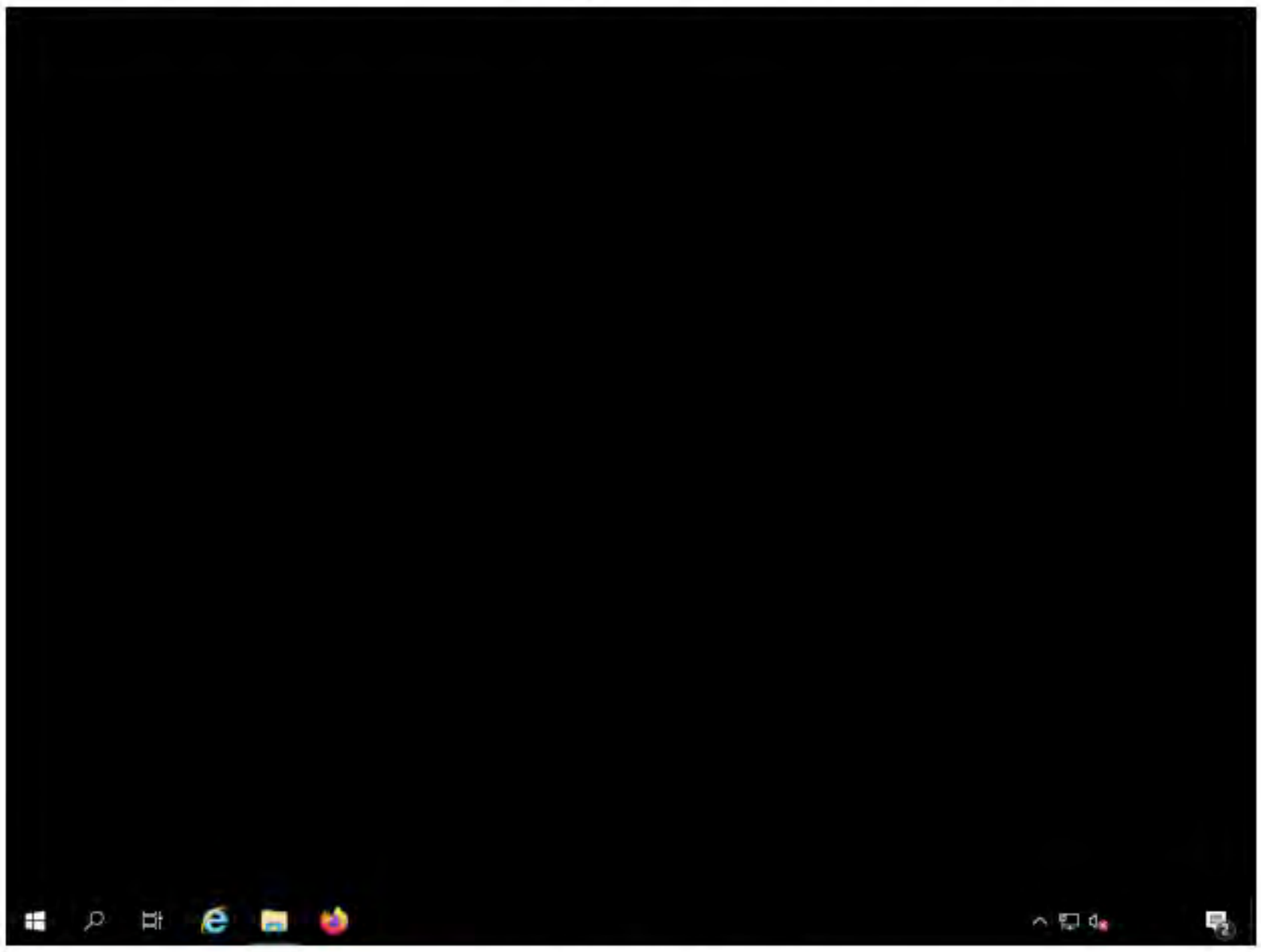


Figure 2.1.8: Virus executed successfully

22. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

Note: Here, the credentials are **Administrator** and **Pa$$w0rd**.

Figure 2.1.9: Victim machine unable to login with the Old Password

23. Now, login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.

Figure 2.1.10: Trying to log in with the new password created by the virus

24. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.

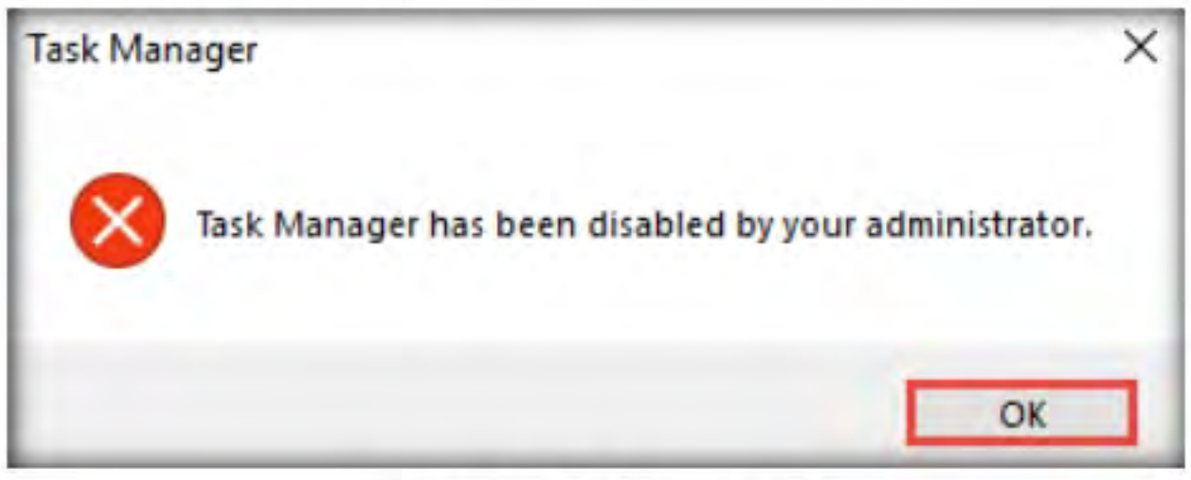


Figure 2.1.11: Task Manager disabled

25. You will get a similar error for all the applications that are disabled by the virus.
26. This is how attackers infect a system with viruses. Now, before going to the next task, click the **Revert this virtual machine to snapshot: (Saved snapshot)** icon to revert the machine to its initial state (before running virus).

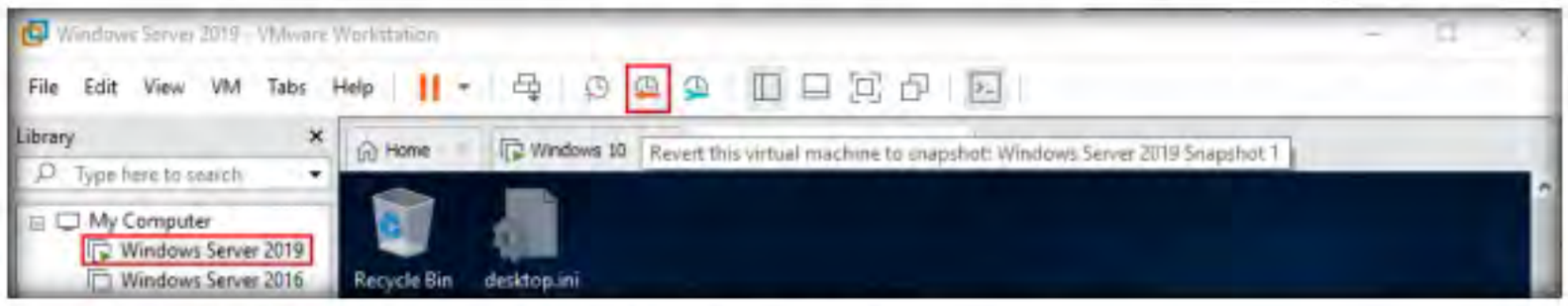


Figure 2.1.12: Reverting to Saved Snapshot

27. The **VMware Workstation** pop-up appears, stating that, **By restoring this snapshot, the current state will be lost**; click **Yes**.
28. Close all open windows on the **Windows 10** virtual machine.
29. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Perform Static Malware Analysis

Malware analysis is the process of reverse engineering a specific piece of malware to determine its origin, functionality, and potential impact.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers use sophisticated malware techniques as cyber weapons to steal sensitive data. Malware can inflict intellectual and financial losses on the target, be it an individual, a group of people, or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future problems, it is necessary to perform malware analysis. Many tools and techniques exist to perform such tasks.

Malware analysis provides an in-depth understanding of each individual sample and identifies emerging technology trends from large collections of malware samples without executing them. The samples of malware are mostly compatible with the Windows binary executable.

By performing malware analysis, detailed information regarding the malware can be extracted. This information includes items like the malicious intent of the malware, indicators of compromise, complexity level of the intruder, exploited vulnerability, extent of damage caused by the intrusion, perpetrator accountable for installing the malware, and system vulnerability the malware has exploited.

An ethical hacker and pen tester must perform malware analysis to understand the workings of the malware and assess the damage that it may cause to the information system. Malware analysis is an integral part of any penetration testing process.

Note: It is very dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

Lab Objectives

- Perform online malware scanning using VirusTotal
- Perform a strings search using BinText
- Identify packing and obfuscation methods using PEid
- Find the portable executable (PE) information of a malware executable file using PE Explorer
- Identify file dependencies using Dependency Walker
- Perform malware disassembly using IDA and OllyDbg

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- BinText located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText**
- PEid located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid**
- PE Explorer located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer**
- Dependency Walker located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**
- IDA located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**
- OllyDbg located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Lab Duration

Time: 40 Minutes

Overview of Static Malware Analysis

Static Malware Analysis, also known as code analysis, involves going through the executable binary code without executing it to gain a better understanding of the malware and its purpose.

The process includes the use of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects the technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size. Analyzing the binary code provides information about the malware's functionality, network signatures, exploit packaging technique, dependencies involved, as well as other information.

Some of the static malware analysis techniques are:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing and obfuscation methods
- Finding portable executable (PE) information
- Identifying file dependencies
- Malware disassembly

Lab Tasks

TASK 1

Perform Online Malware Scanning using VirusTotal

VirusTotal helps ethical hackers and penetration testers to analyze files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.

This lab activity will demonstrate how to analyze malware using online virus analysis services.

TASK 1.1

Launch and Upload Malicious Sample File on VirusTotal Scanning Service

1. Turn on the **Windows 10** victim machine and login with the credentials **Admin** and **Pa$$w0rd**.
2. Launch a web browser (here, **Google Chrome**), type **http://www.virustotal.com** in the address bar, and press **Enter**.

Note: If you are using a different browser, then the screenshots will differ from the images that you see on your screen.

3. The **VirusTotal** webpage appears in the browser; click **Choose file**.

VirusTotal aims to improve the anti-virus and security industry and make the Internet a safer place through the development of free tools and services. VirusTotal simply acts as an information aggregator. The aggregated data are the output of different antivirus engines, website scanners, file and URL analysis tools, and user contributions.

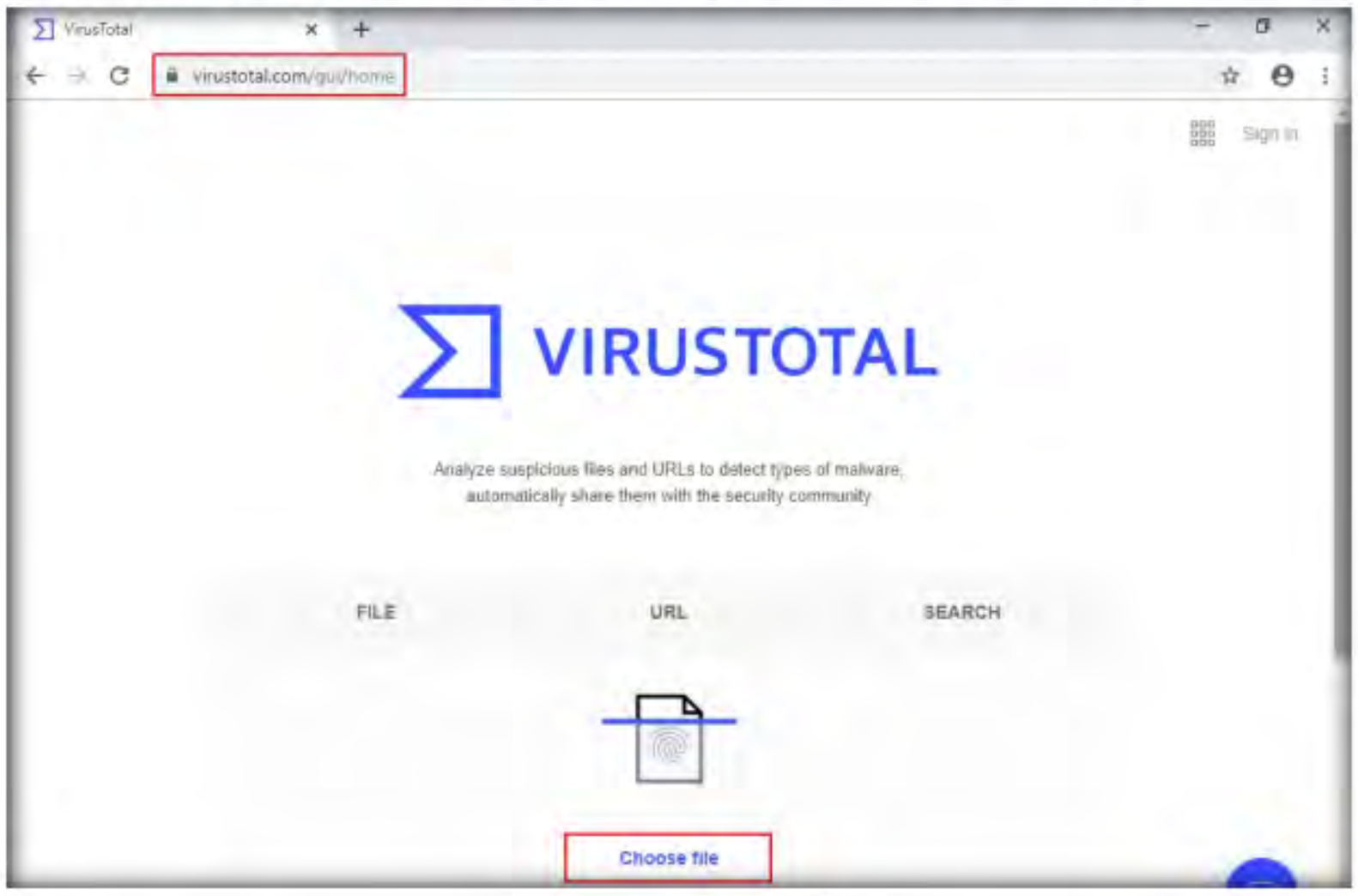


Figure 3.1.1: VirusTotal Home Page

The malware signatures of antivirus solutions present in VirusTotal are periodically updated as they are developed and distributed by anti-virus companies. The update polling frequency is 15 minutes—thus ensuring that these products are using the latest signature sets. Website scanning is done via API queries to the different companies providing the solution; hence, the most updated version of their dataset is always used.

4. The **Open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

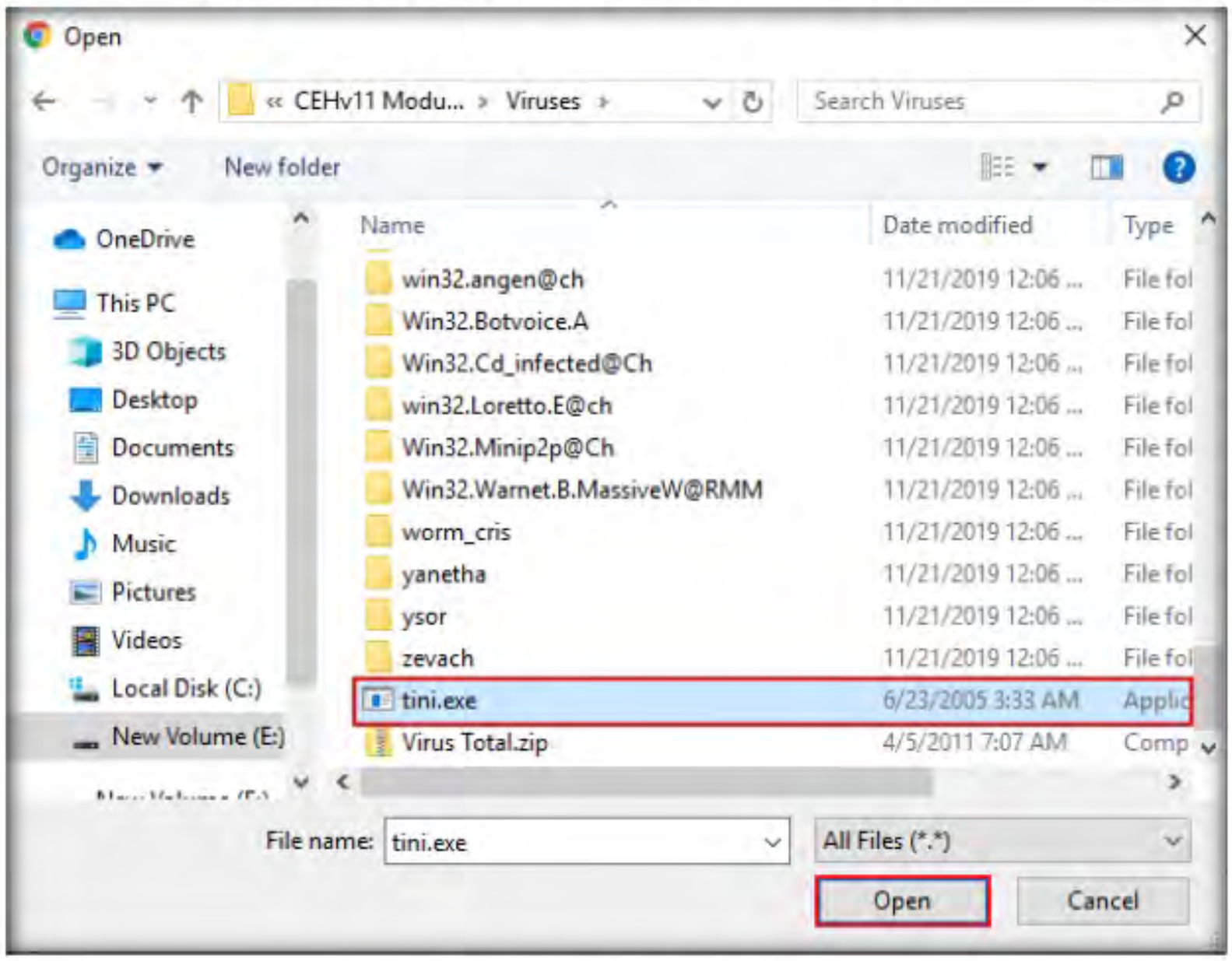


Figure 3.1.2: Select a file for Virus analysis

TASK 1.2

View the Result

5. The selected file will be sent to the VirusTotal server for analysis.
6. VirusTotal returns a detailed report displaying the result of each anti-virus for the selected **tini.exe** malicious file under the **DETECTION** tab, as shown in the screenshot.

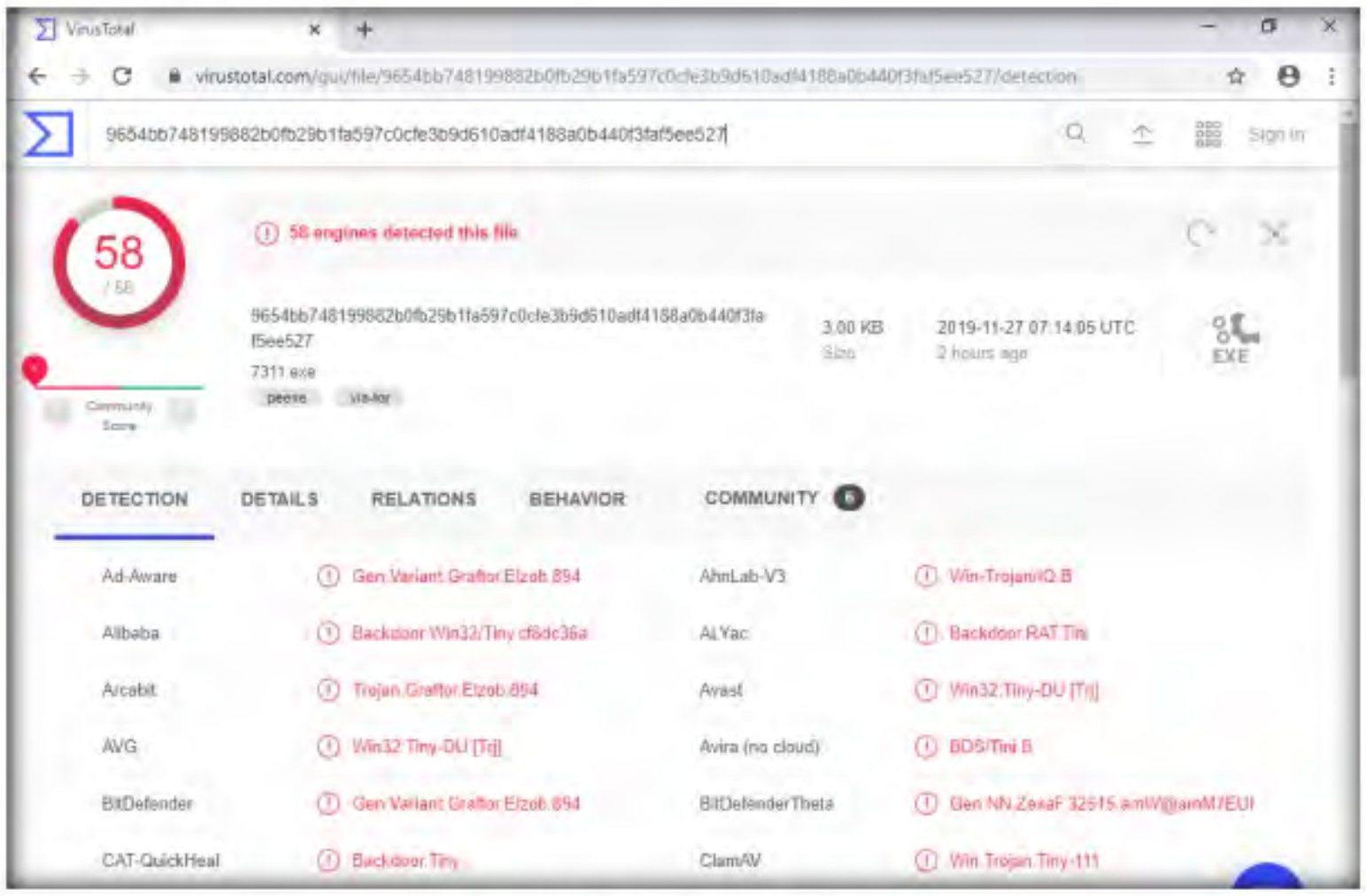


Figure 3.1.3: VirusTotal DETECTION Section

7. Now, click the **DETAILS** tab to view the malicious file details such as Basic Properties, History, Names, Portable Executable Info, Sections, Imports, and ExifTool File Metadata.

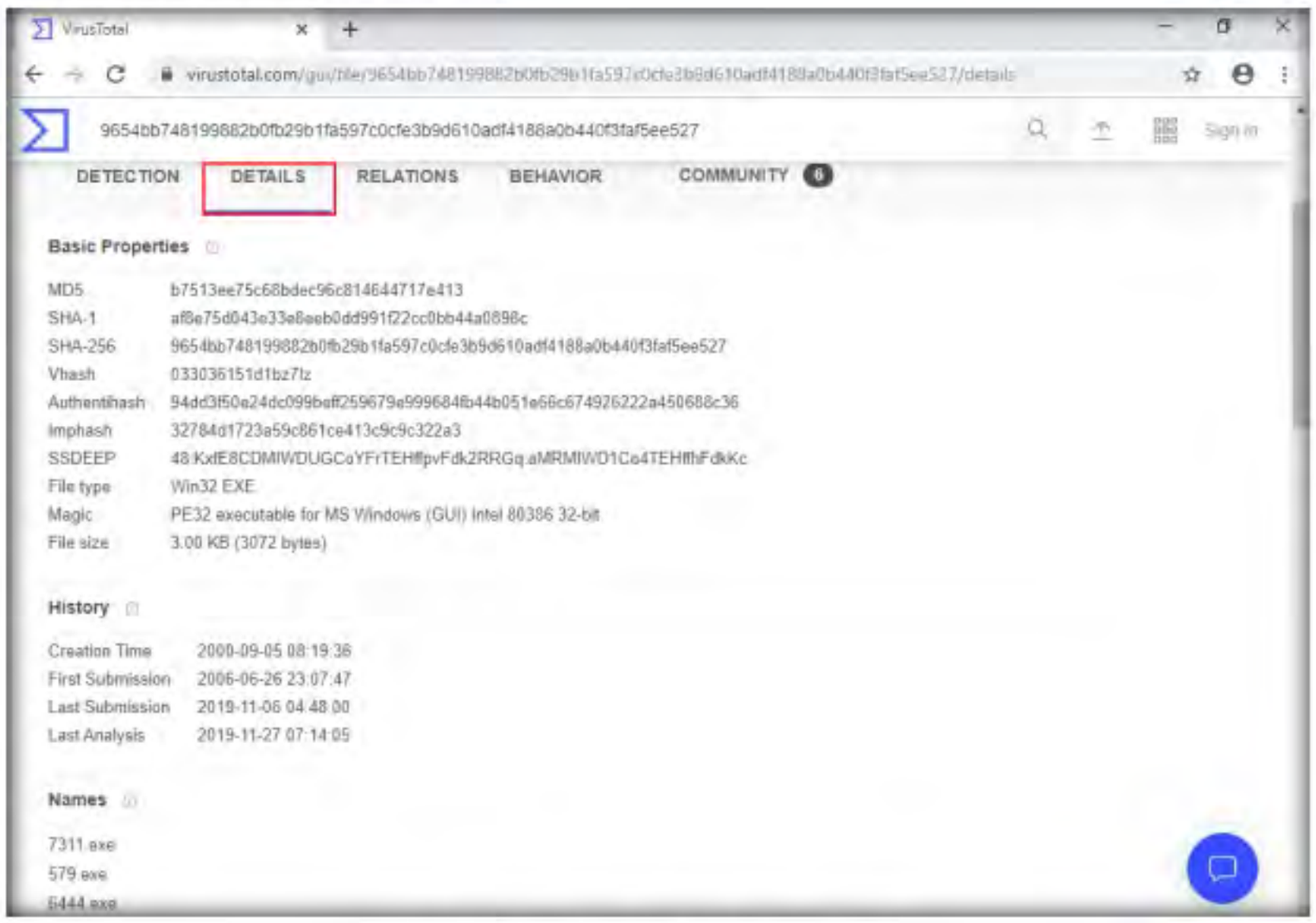


Figure 3.1.4: VirusTotal DETAILS Section

8. Click the **RELATIONS** tab to view Execution Parents, PE Resource Parents, Contained in Graphs, and Graph Summary. Scroll down to view other details.
9. To view **Graph Summary**, you will need a VirusTotal account.

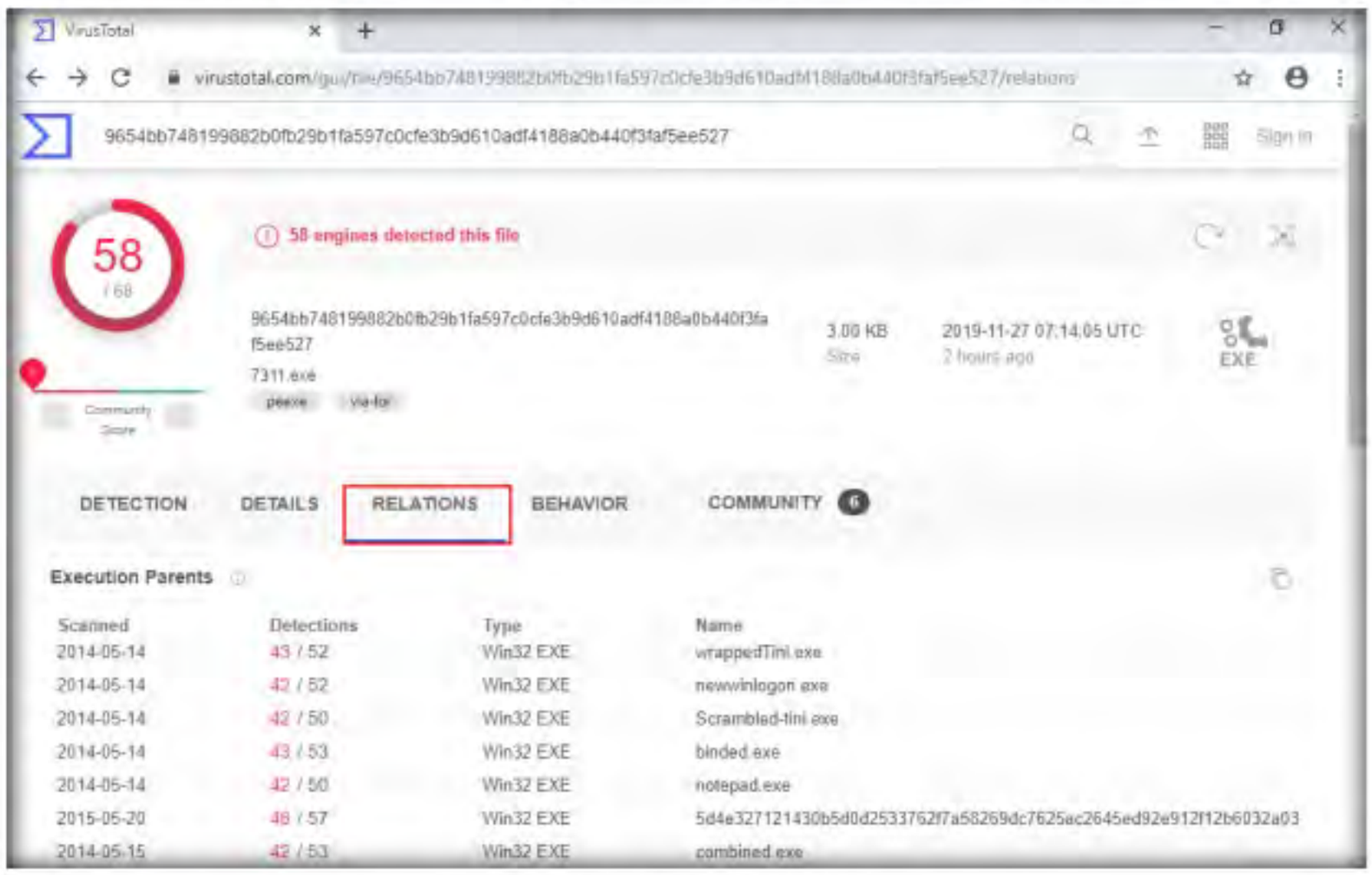


Figure 3.1.5: VirusTotal RELATIONS Section

You can also use other local and online malware scanning tools such as **Hybrid Analysis** (https://www.hybrid-analysis.com), **Cuckoo Sandbox** (https://cuckoosandbox.org), **Jotti** (https://virusscan.jotti.org), or **Valkyrie Sandbox** (https://valkyrie.comodo.com) to perform online malware scanning.

10. Click the **BEHAVIOR** tab to view the File System Actions, Process and Service Actions, Shell Commands, and Synchronization Mechanisms & Signals.

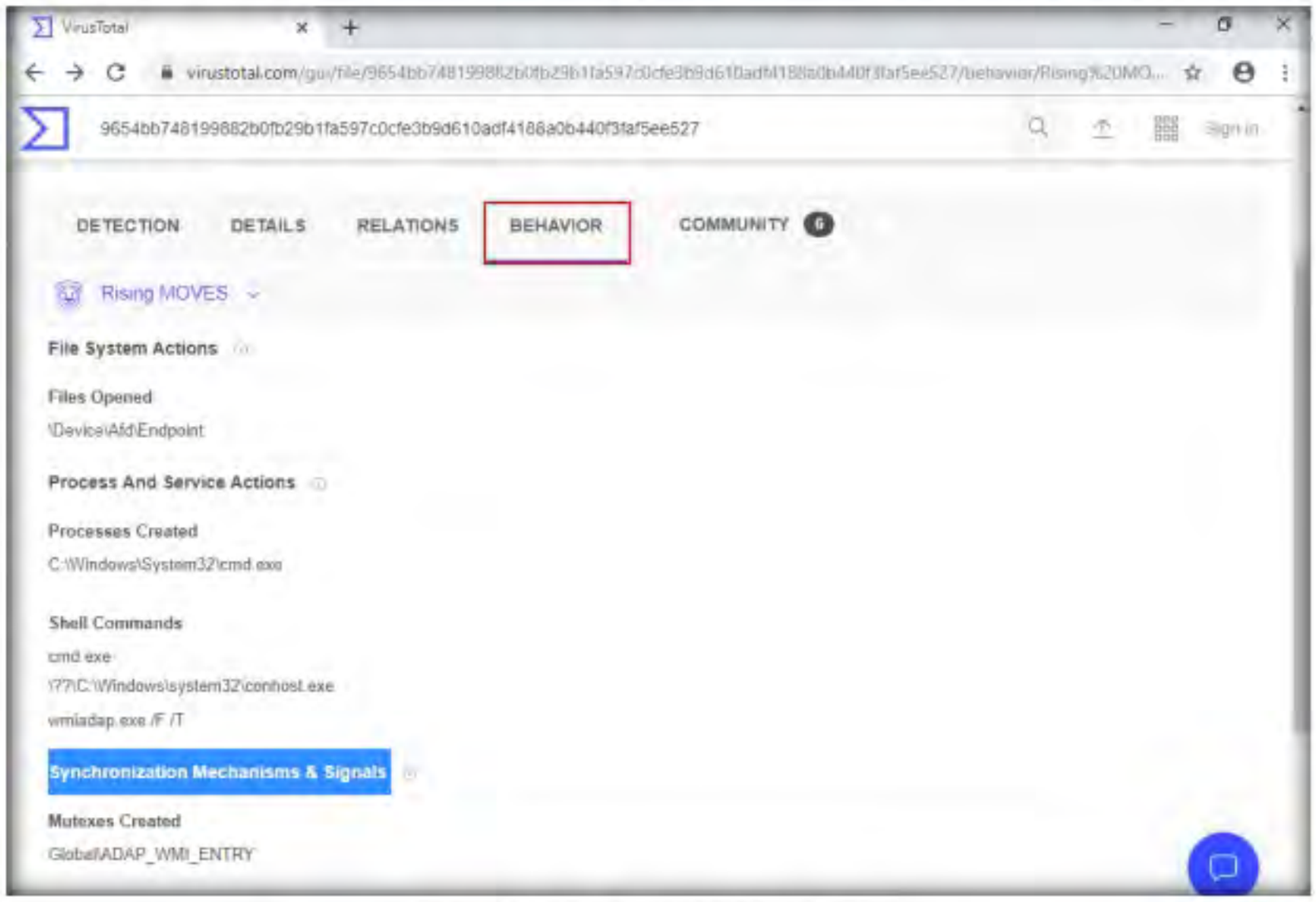


Figure 3.1.6: VirusTotal BEHAVIOR Section

11. Close the web browser once the analysis is complete.

TASK 2

Perform a Strings Search using BinText

Here, we will use the BinText tool to extract embedded strings from executable files.

TASK 2.1

Launch BinText

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText** and double-click **bintext.exe**.
2. The **BinText** main window appears; click **Browse** to provide a file to scan. Here, we need to provide a malicious file to analyze the text.
3. Make sure that the **Advanced view** option is checked.

Software programs include some strings that are commands to perform specific functions such as printing output. Strings communicate information from a program to its user. Various strings that could represent the malicious intent of a program such as reading the internal memory or cookie data, are embedded in the compiled binary code.

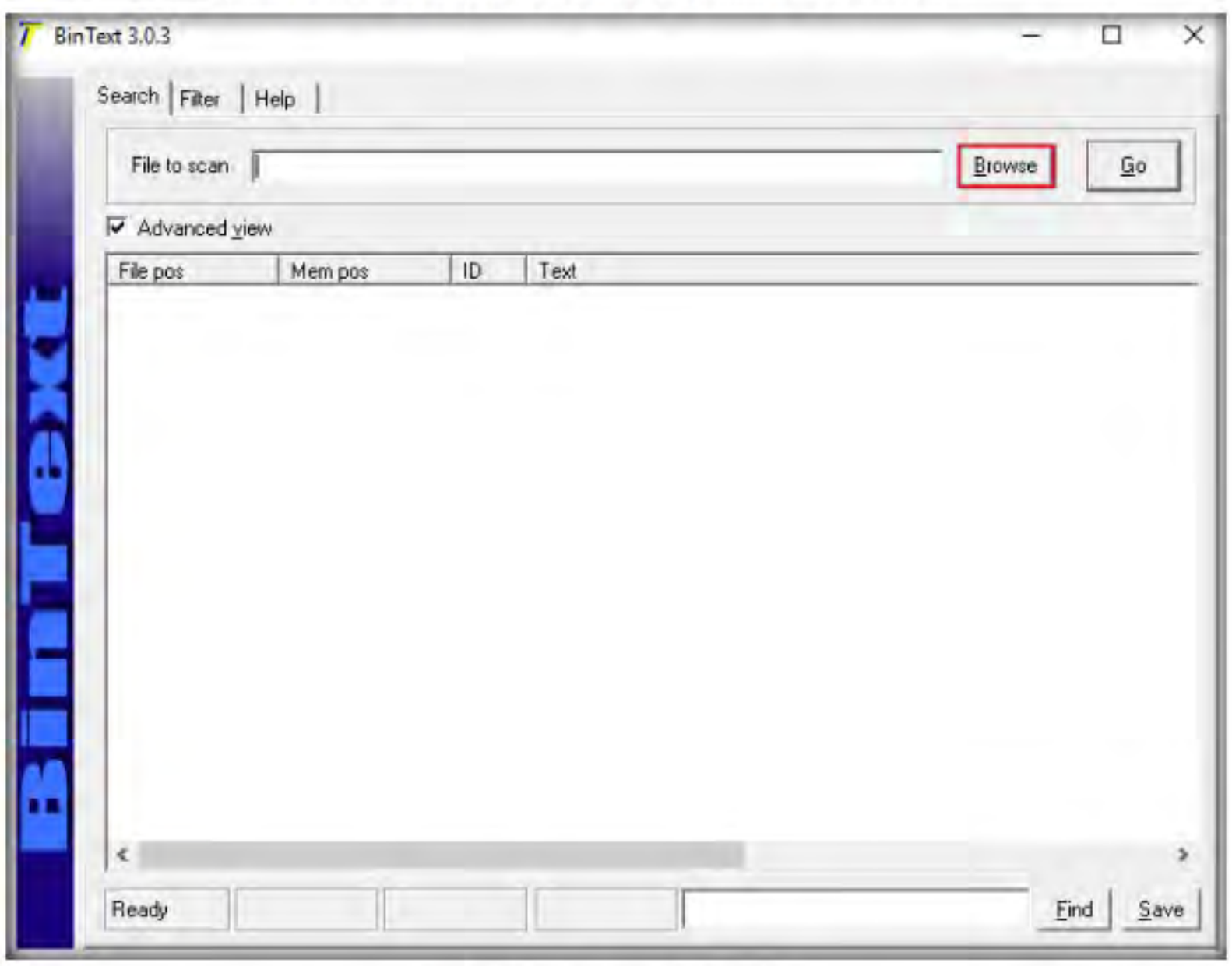


Figure 3.2.1: BinText Main Window

Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in it. You should be attentive while looking for strings and search for the embedded and encrypted strings for a complete analysis of the suspect file.

4. The **Open file for Scanning** window appears, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!** and select **face.exe**, the malicious file, and click **Open** to extract the text from the malicious file.

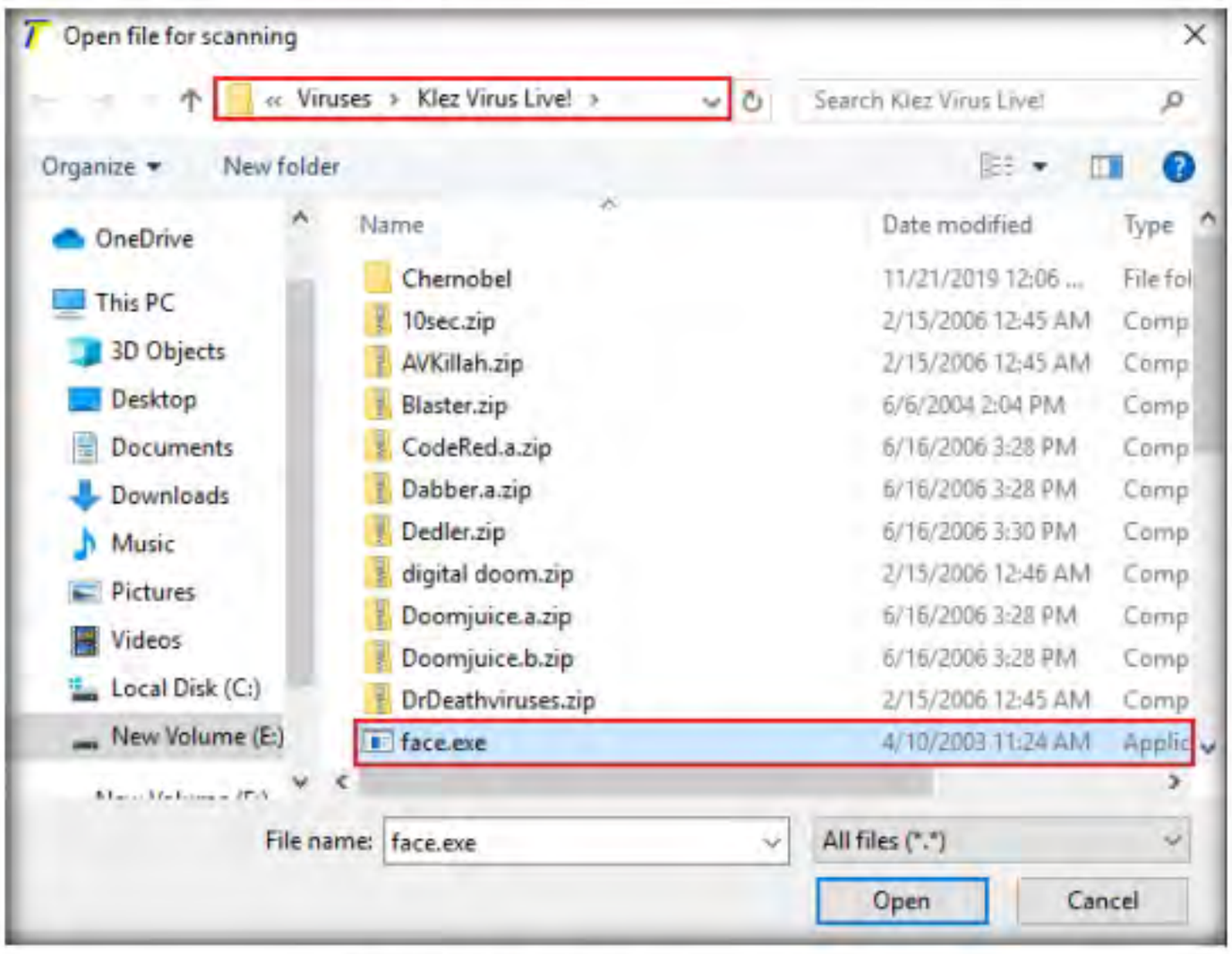


Figure 3.2.2: Open file for scanning Window

BinText is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful information for each item.

5. As soon as the file is provided for scan, click **Go**. BinText will start extracting the text from the designated malicious file.

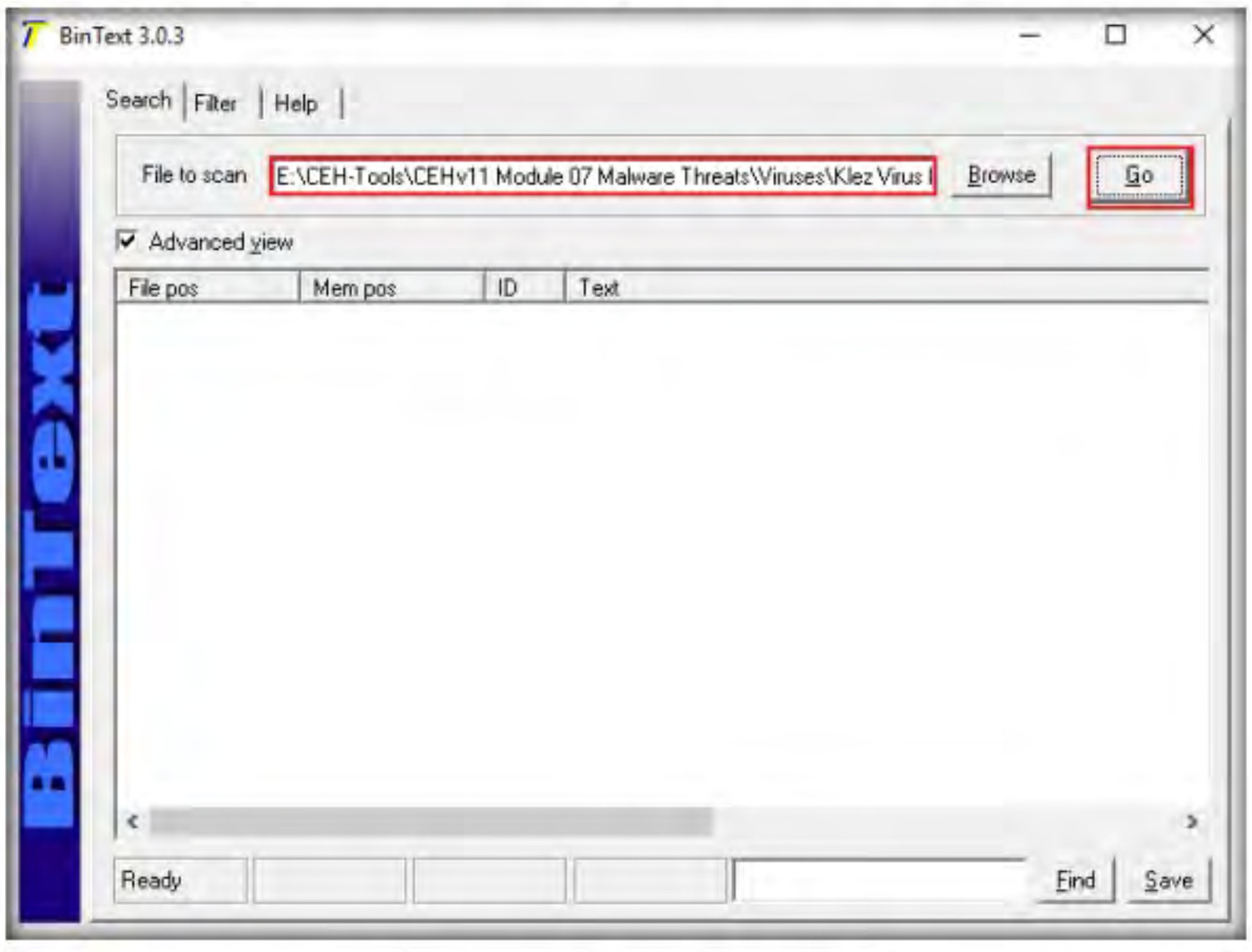


Figure 3.2.3: BinText Extracting Malicious File

TASK 2.2

View the Extract Embedded Strings

6. BinText extracts the provided malicious file's critical information, as shown in the screenshot.

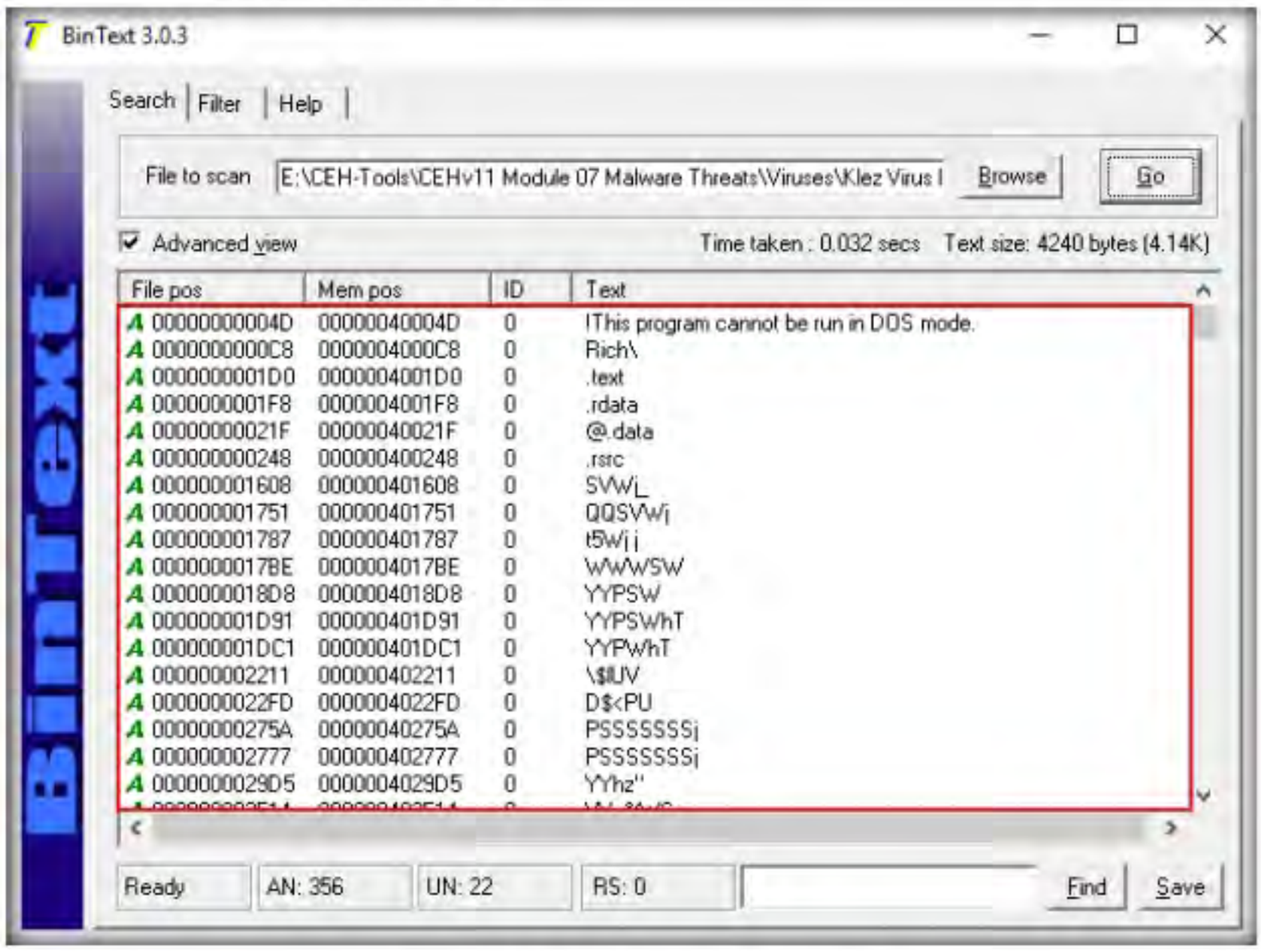


Figure 3.2.4: BinText Extracted Information

You can also use other string searching tools such as **FLOSS** (https://www.fireeye.com), **Strings** (https://docs.microsoft.com), **Free EXE DLL Resource Extract** (http://www.resourceextract.com), or **FileSeek** (https://www.fileseek.ca) to perform string search.

7. The type of string is designated by a colored letter to the left of the list. ANSI strings are marked with a green "A," Unicode strings (double byte ANSI) have a red "U," and resource strings have a blue "R."
8. "File pos" is the HEX position at which the text is located in the file.
9. "Mem pos" if the file is a Win32 PE file (such as Win95 EXEs and DLLs), then this is the HEX address at which the text is referred to in the memory at runtime, as determined by its sections table.
10. "ID" is the decimal string resource ID or 0 if it is not a resource string.
11. Close all windows once the analysis is complete.

TASK 3

Identify Packaging and Obfuscation Methods using PEid

Here, we will use the PEid tool to detect common packers, cryptors, and compilers for PE executable files.

TASK 3.1

Launch PEiD

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid** and double-click **PEiD.exe**.

2. The **PEiD** main window appears. Click the **Browse** button to upload a malicious file for analysis.

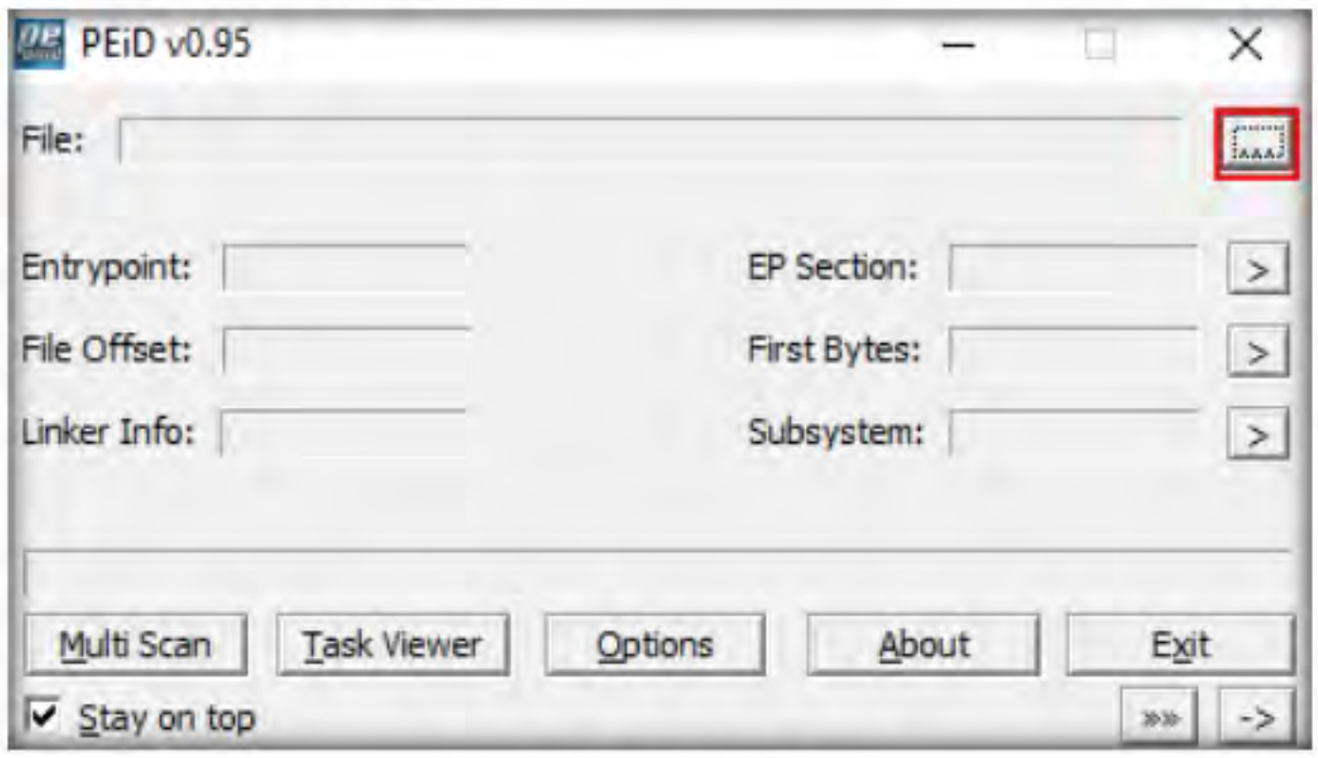


Figure 3.3.1: PEiD Main Window

Attackers often use packing and obfuscation or a packer to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file, and then runs the unpacked file. It complicates the task of reverse engineers to determine the actual program logic and other metadata via static analysis. The best approach is to try and identify if the file includes packed elements and locate the tool or method used to pack it.

3. The **Choose the file to open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select the **face.exe** file, and click **Open**.

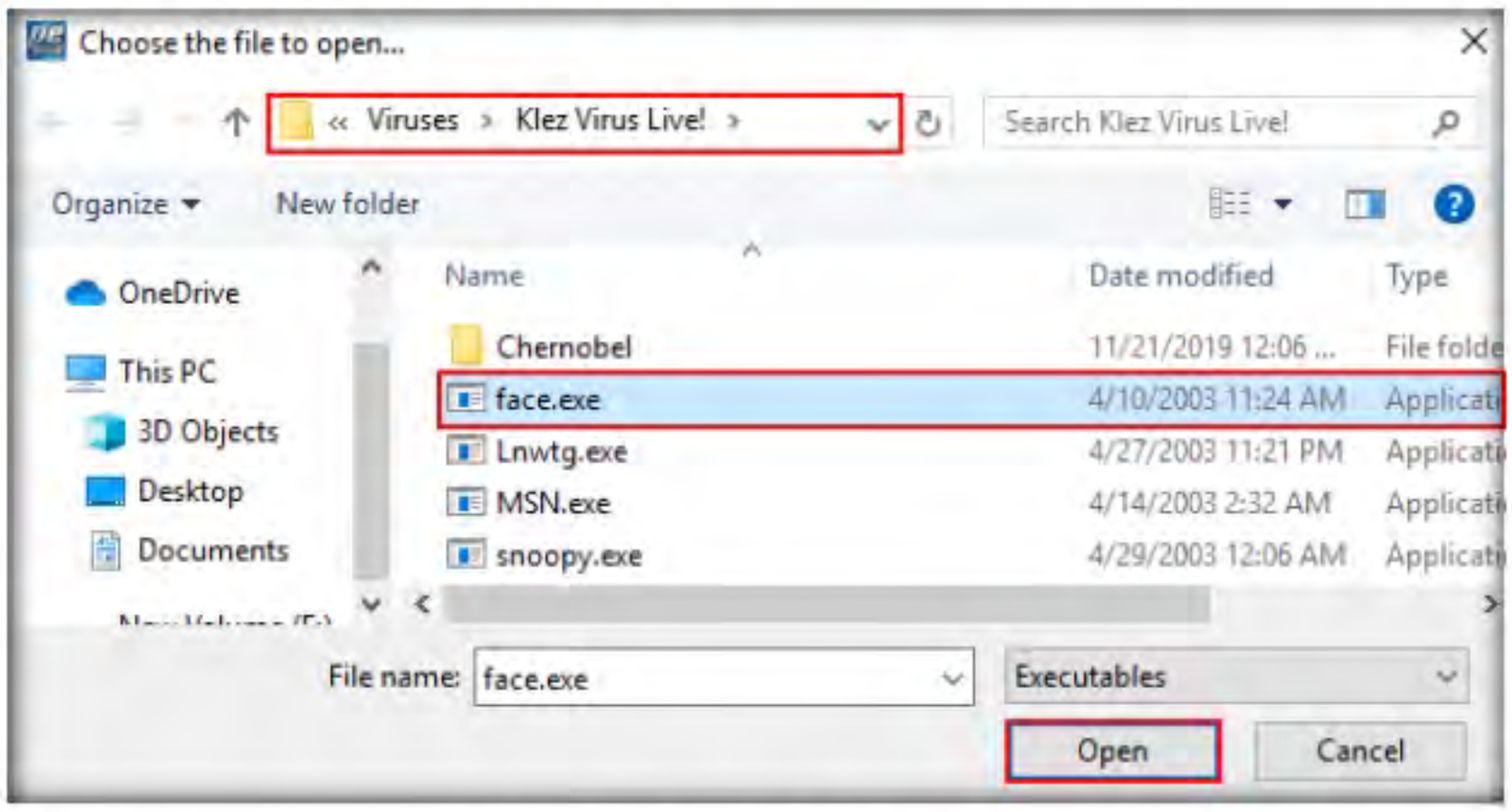


Figure 3.3.2: Choose the file to open window

PEid is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packer used in packing a program.

TASK 3.2

View the Result

4. As soon as you click **Open**, PEiD analyzes the file and provides information, as shown in the screenshot.

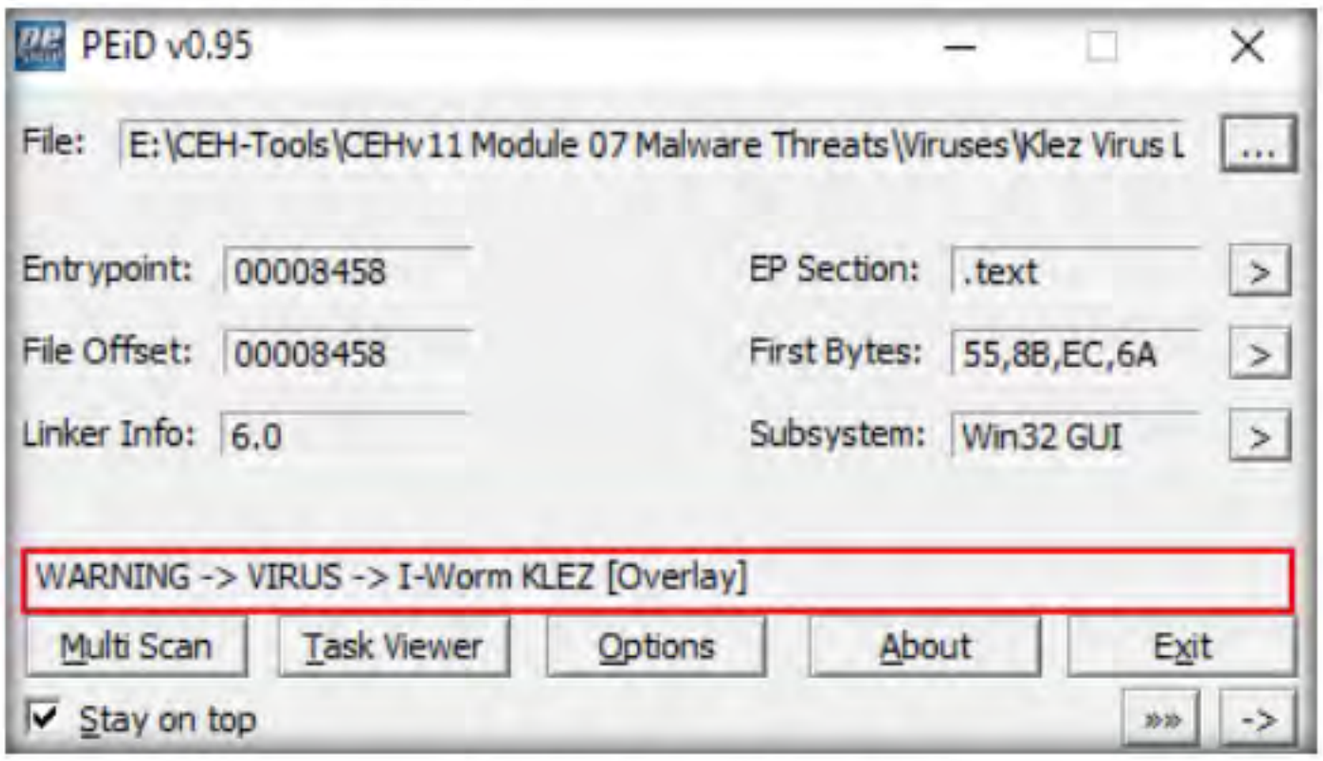


Figure 3.3.3: PEiD Extracted Information

5. Close all windows once the analysis is complete.

TASK 4

Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

Here, we will use the PE Explorer tool to view the PE information of a malware executable file.

TASK 4.1

Install PE Explorer

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer** and double-click **PE.Explorer_setup.exe**.
2. If a **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard-driven installation steps to install PE Explorer.
4. In the last step of the installation, make sure that the **Launch PE Explorer** option is checked to launch the application automatically; uncheck the **View PE Explorer User's Guide** option and click **Finish**.

You can also use other packaging/ obfuscation tools such as **Macro_Pack** (https://github.com), **UPX** (https://upx.github.io), or **ASPack** (http://www.aspack.com) to identify packing/ obfuscation methods.

The Portable Executable (PE) format is the executable file format used on Windows OSes that stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format that consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, and linked files, as well as strings, menus, and symbols.

Figure 3.4.1: PE Explorer Installation

TASK 4.2

Import File for Analysis

5. The **PE Explorer** main window appears. Navigate to **File** and click **Open File** from the menu to start exploring executable files. You can drag and drop the file into the PE Explorer window.

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less familiar types such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

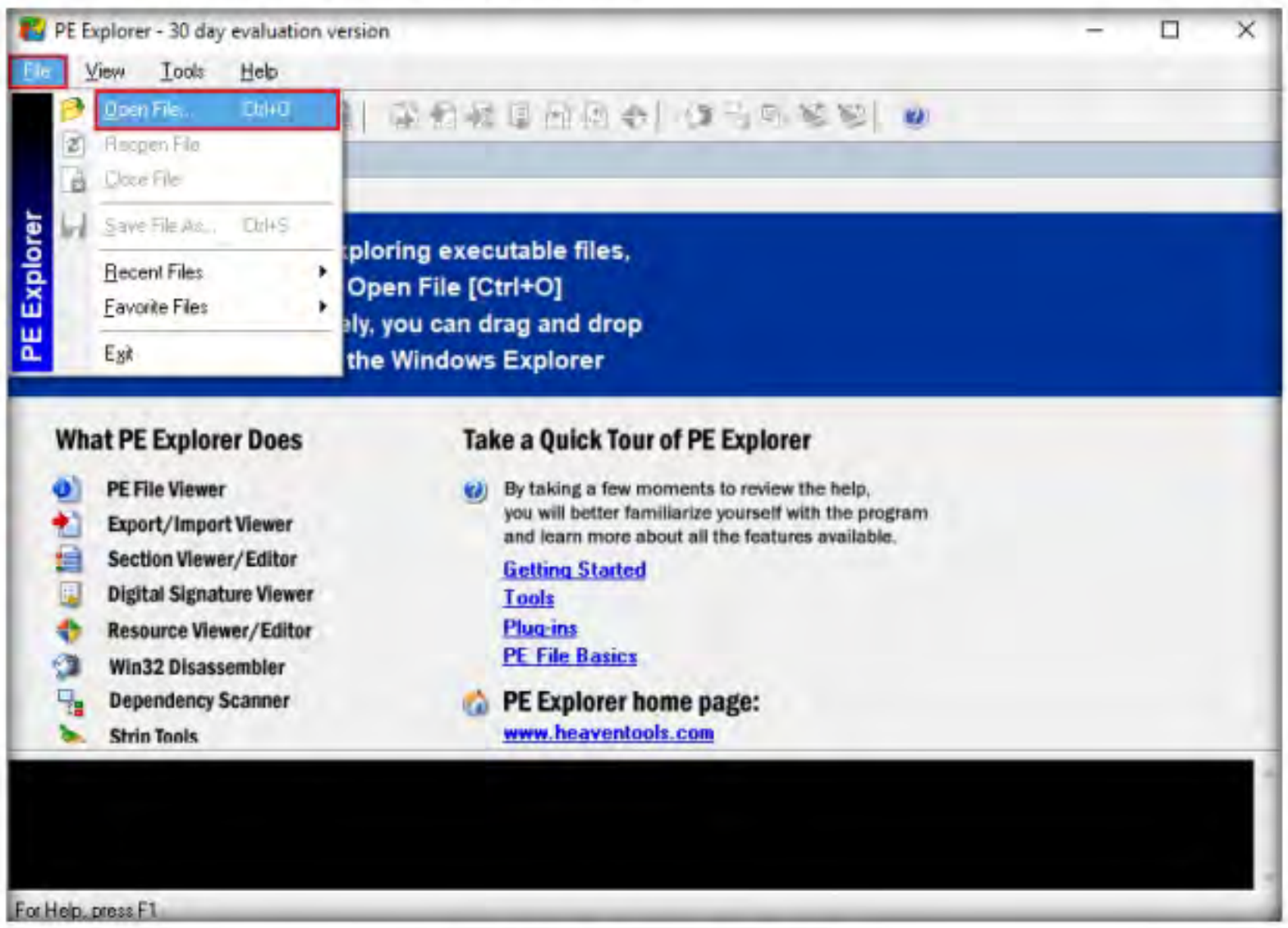


Figure 3.4.2: PE Explorer Main Window

6. An **open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **face.exe** file and click **Open**.

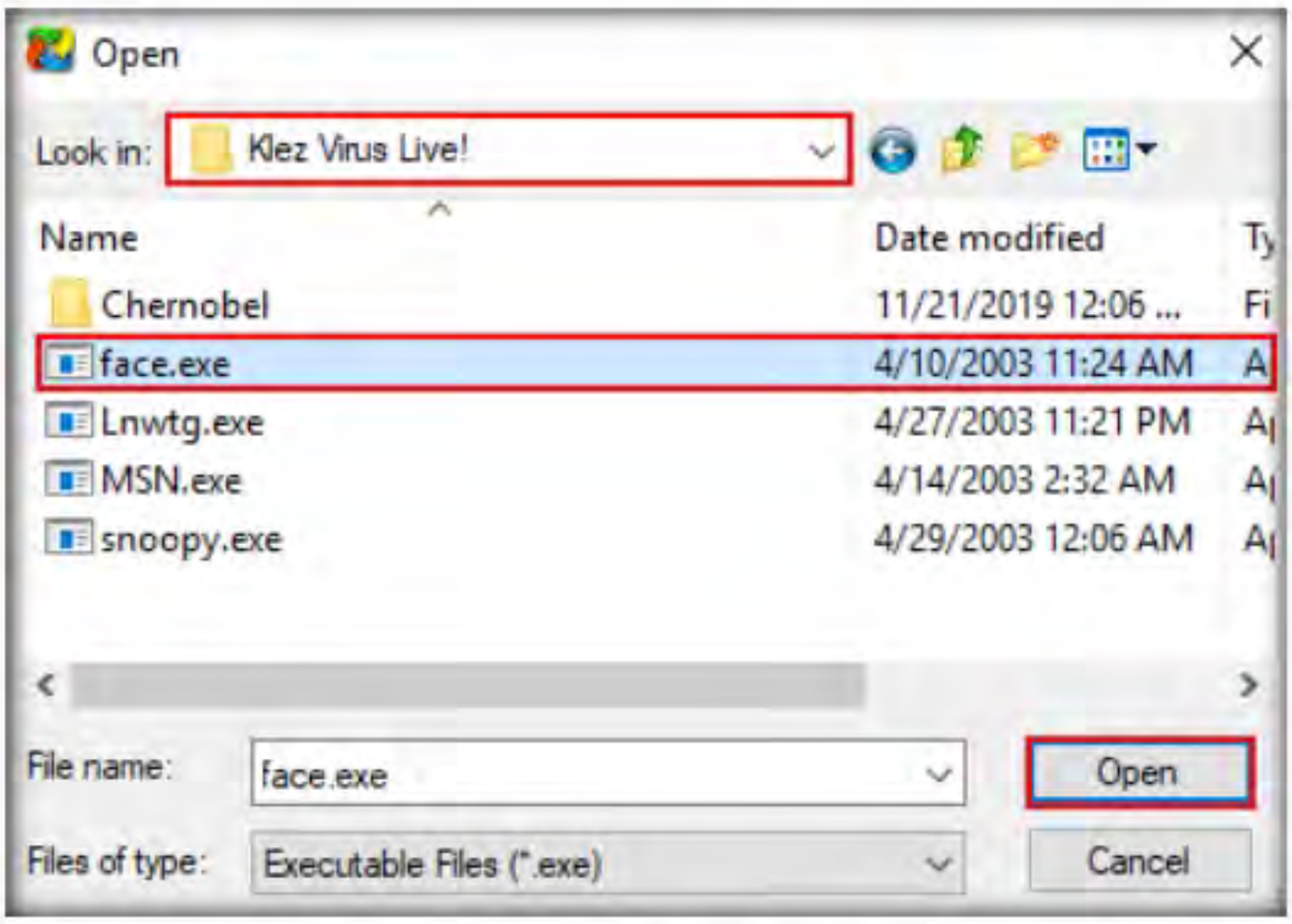


Figure 3.4.3: PE Explorer Importing Malicious File

7. The **PE Explorer** evaluation pop-up appears; click **Continue**.

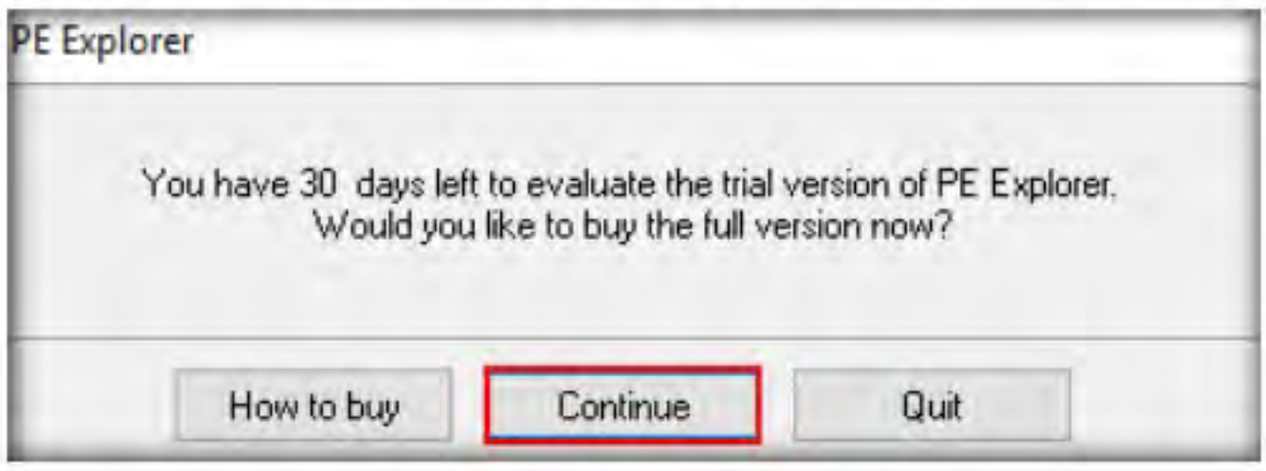


Figure 3.4.4: PE Explorer Evaluation pop-up

TASK 4.3

View the Result

8. PE Explorer provides you with an analysis of the file, as shown in the screenshot.
9. The **HEADERS INFO** section provides you with the ability to:
   a. View and save a text report on the file headers information
   b. Modify the entry point value
   c. Updates the value of the checksum in the header
   d. Set flag bits in the file header characteristics field

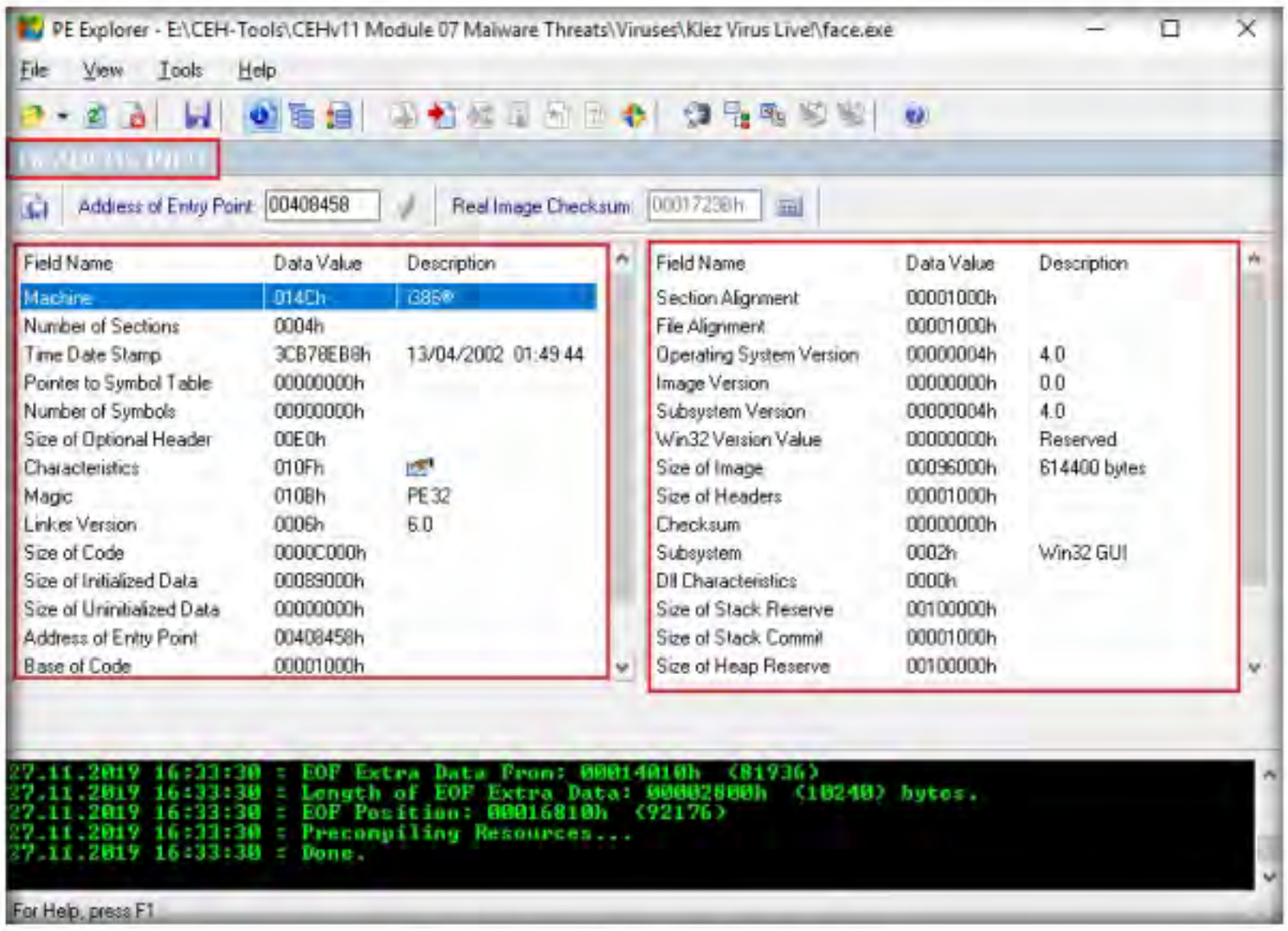


Figure 3.4.5: PE Explorer HEADERS INFO

10. Click the **Data Directories** icon ( ) from the menu bar. This will provide you with the **DATA DIRECTORIES** information such as the ability to view and edit the virtual address and size of the chosen directory describing provisions of parts of the code.
11. The trailing array of Data Directories cover pointers to the data in the sections.

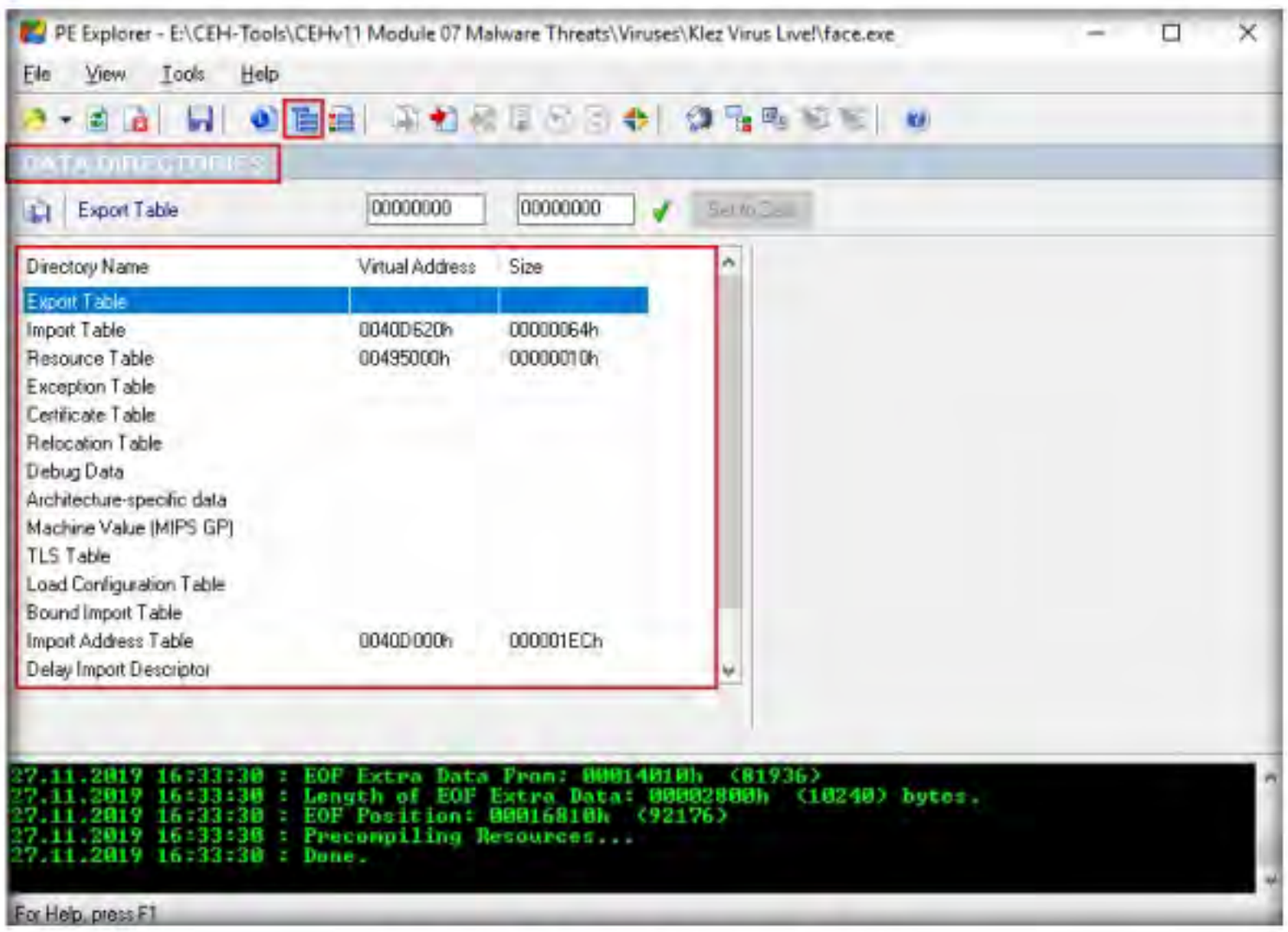


Figure 3.4.6: PE Explorer DATA DIRECTORIES

12. Click **Section Headers** icon () from the menu bar. This will provide you with the **SECTION HEADERS** information, allowing you to view all sections and information about their location and size.

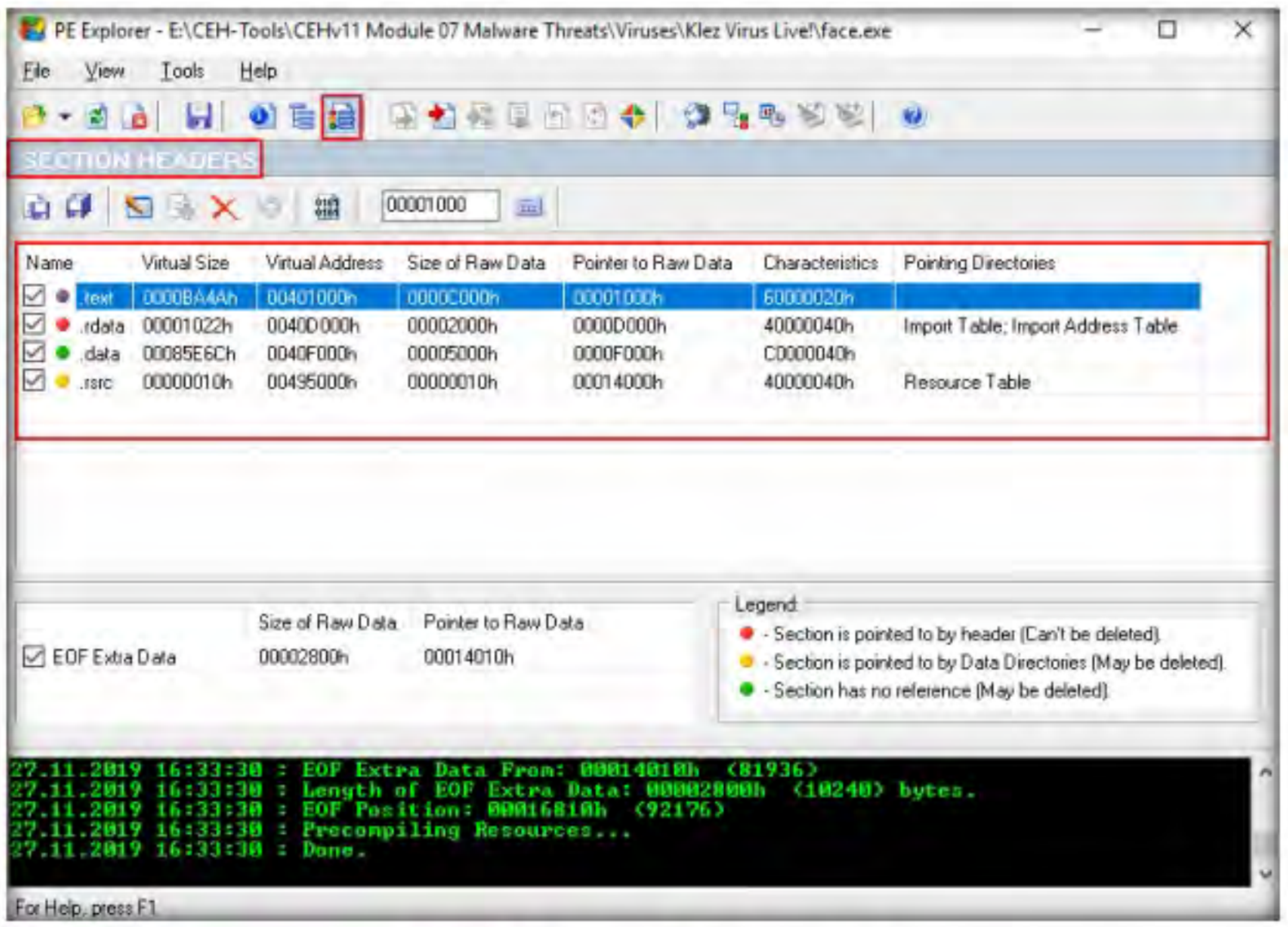


Figure 3.4.7: PE Explorer SECTION HEADERS

13. Double click on any section to view the raw content. This will open a mini hex viewer window.

14. Close the hex viewer window after analysis.

Figure 3.4.8: PE Explorer hex mini viewer

15. This is how to analyze a malicious file using PE Explorer. Close all open windows.

You can also use other PE extraction tools such as **Portable Executable Scanner (pescan)** (https://tzworks.net), **Resource Hacker** (http://www.angusj.com), or **PEView** (https://www.aldeid.com) to find the Portable Executable (PE) information of a malware executable file.

TASK 5

Identify File Dependencies using Dependency Walker

Here, we will use the Dependency Walker tool to identify the file dependencies of an executable file.

TASK 5.1

Launch Dependency Walker

Any software program depends on the various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. Programs store their import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly; this includes the process of registration and location on the machine.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**, and double-click **depends.exe**.
2. The **Dependency Walker** main window appears; navigate to **File** and click **Open** to import the malicious file.

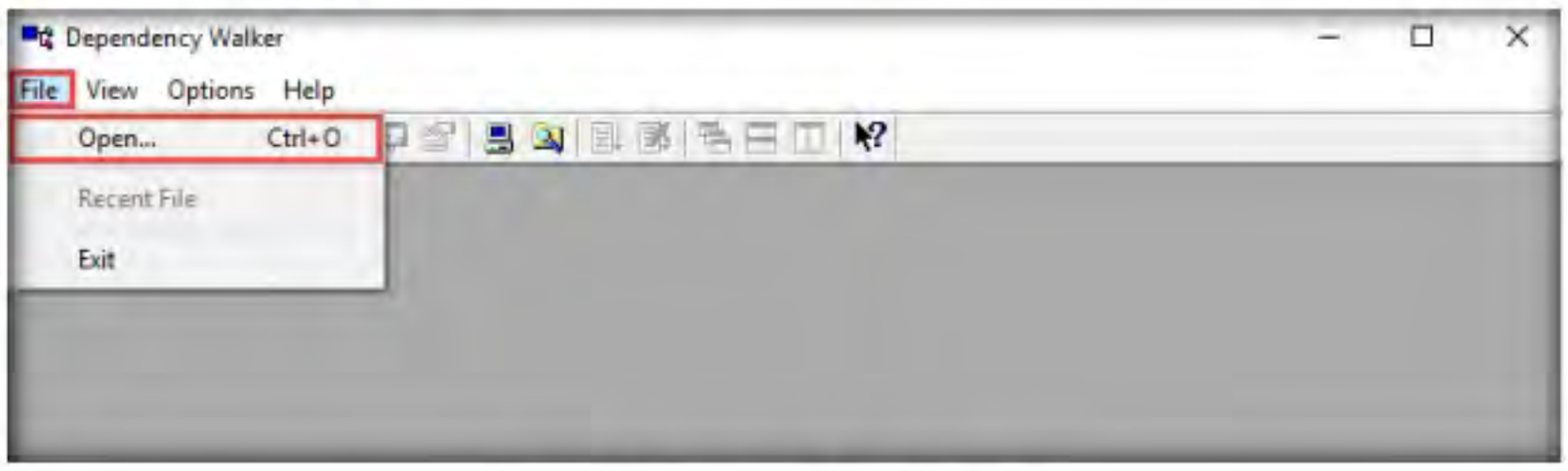


Figure 3.5.1: Dependency Walker Main Window

3. The **open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **snoopy.exe** file and click **Open**.

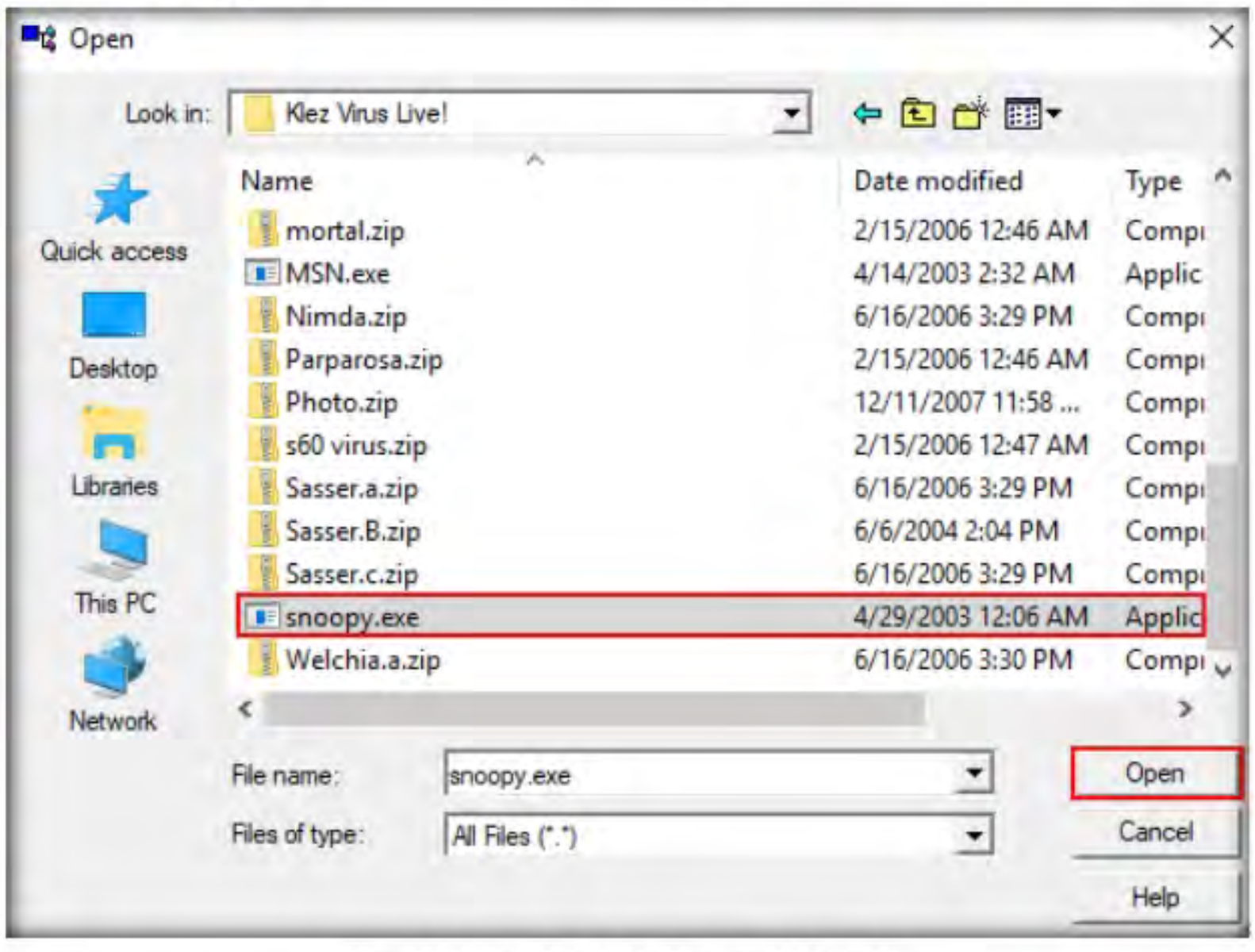


Figure 3.5.2: Dependency Walker Importing Malicious File

Find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Then, check to find and analyze these files to provide information about the malware in the file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all library functions may allow guessing about what the malware program can do. You should know the various DLLs used to load and run a program.

4. The **Dependency Walker** pop-up appears, along with the error detected while processing the file; click **OK**.

Figure 3.5.3: Dependency Walker Error

TASK 5.2

View the Result

5. The **SNOOPY.EXE** file is imported to the Dependency Walker, as shown in the screenshot.

6. Shrink the **.DLL** nodes to view all available DLLs for the malicious file.

The Dependency Walker tool lists all dependent modules of an executable file and builds hierarchical tree diagrams. It also records all functions that each module exports and calls. Further, it detects many common application problems such as missing and invalid modules, import and export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

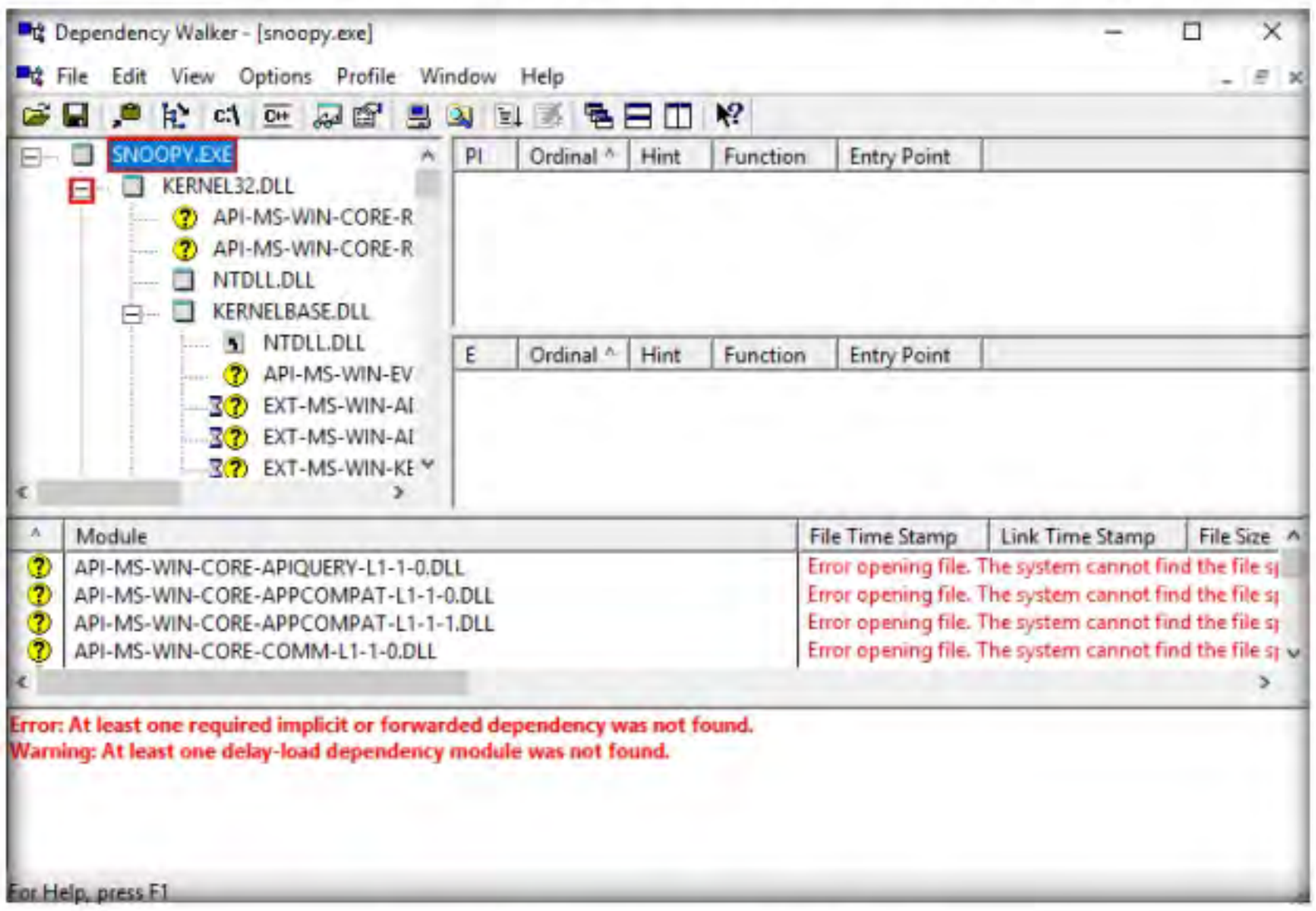


Figure 3.5.4: Dependency Walker Malicious File Imported

7. The available DLLs for snoopy.exe are listed, as shown in the screenshot.

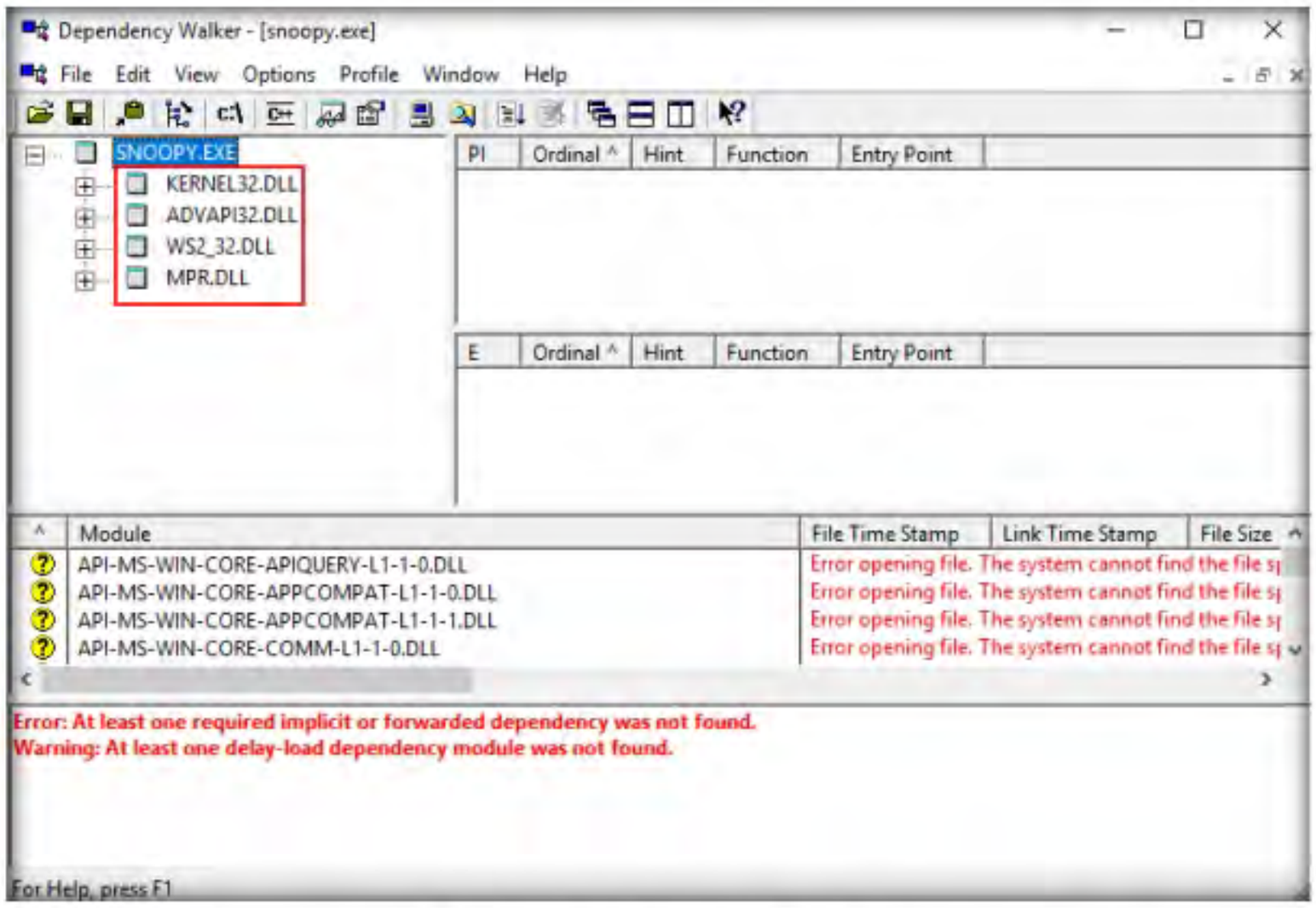


Figure 3.5.5: Dependency Walker DLL Files

8. Click on any DLL dependency to view the details of the DLL file. In this lab, we are choosing **KERNEL32.DLL**.

9. As soon as you select the DLL, the Dependency Walker displays the DLL details in the **Import Section** and **Export Section**, as shown in the screenshot.

You can also use other dependency checking tools such as **Dependency-check** (https://jeremylong.github.io), **Snyk** (https://snyk.io), **Hakiri** (https://hakiri.io), or **RetireJS** (https://retirejs.github.io) to identify file dependencies.

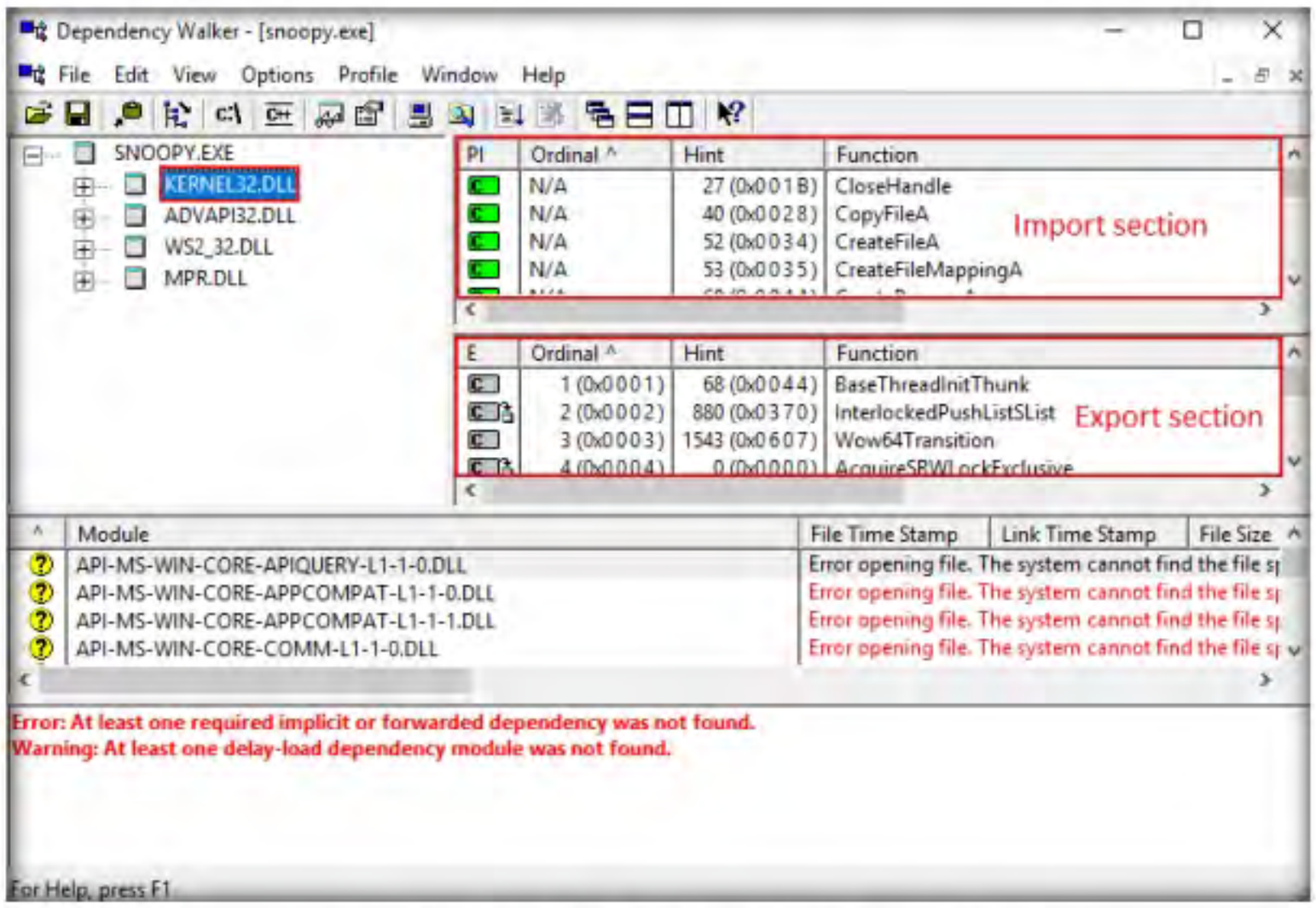


Figure 3.5.6: Dependency Walker Kernel32.DLL Dependencies

10. Analyze all DLL dependencies of the imported malicious file. Close all open windows once the analysis is complete.

TASK 6

TASK 6.1

Install and Launch IDA

Perform Malware Disassembly using IDA and OllyDbg

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA** and double-click **idafree70_windows.exe**.
2. If a **User Account Control** window appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

3. The IDA installation wizard appears; follow the wizard-driven installation steps to install IDA.
4. In the final step of the installation, ensure that the **Launch IDA** option is checked; this will launch the application automatically once you click **Finish**.

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools such as IDA Pro and OllyDbg.

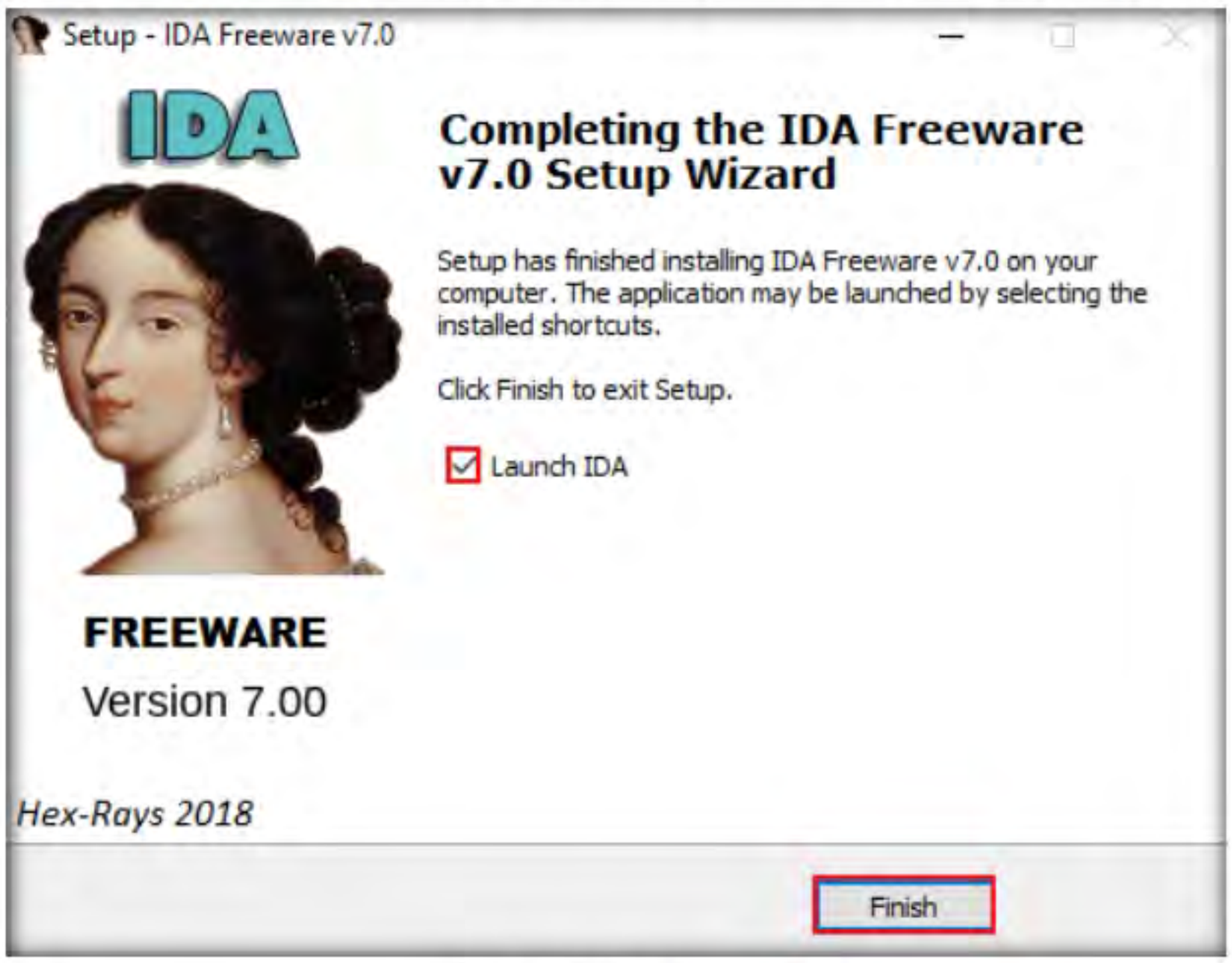


Figure 3.6.1: IDA Installation Completed

5. If the **IDA License** window appears, click on **I Agree**.

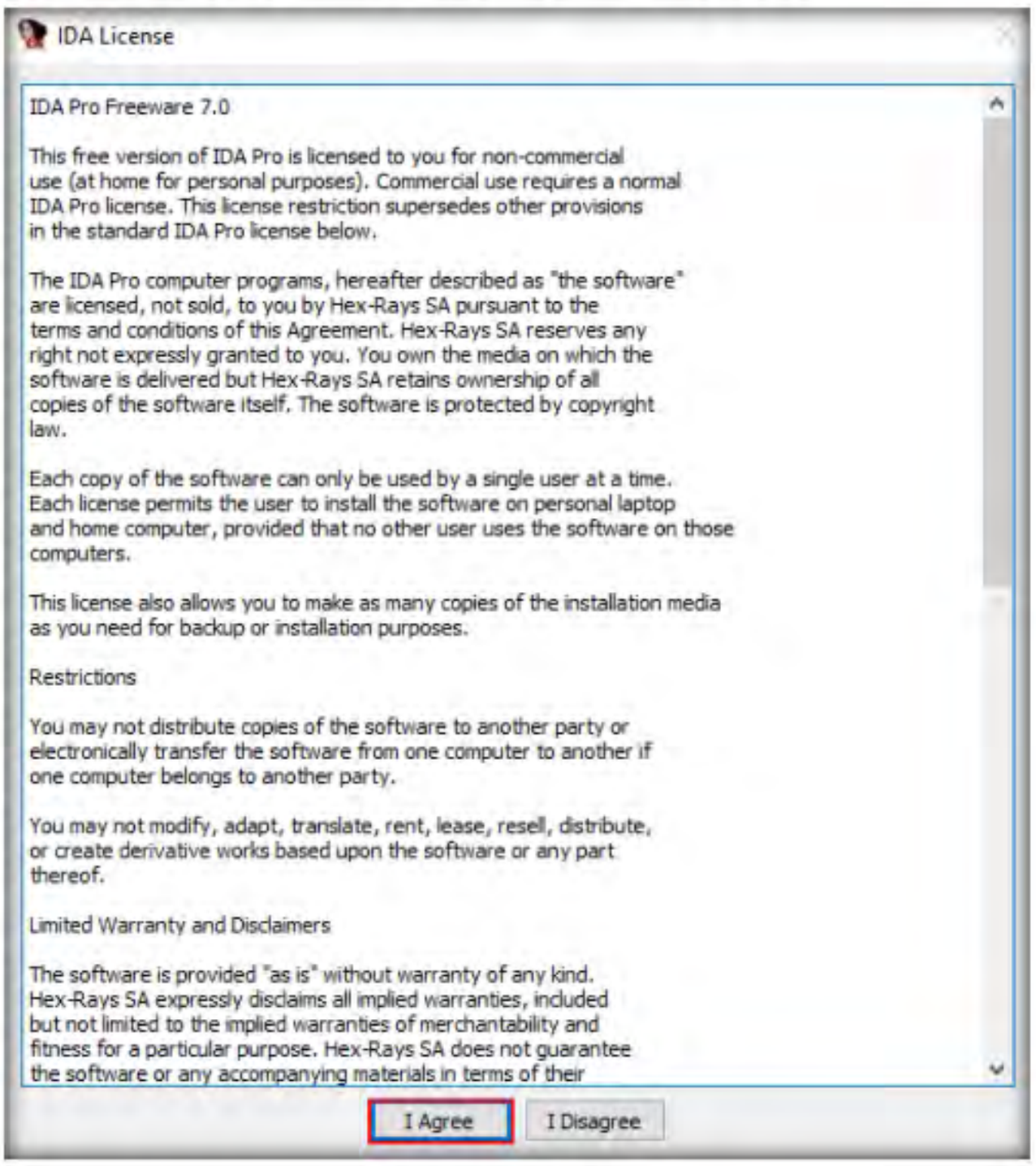


Figure 3.6.2: IDA License

TASK 6.2

Upload Malicious File for Disassembling

6. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.

Figure 3.6.3: IDA Quick Start

IDA

As a disassembler, IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called "assembly language." However, in real life, things are not always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms, and Trojans are often armored and obfuscated; as such, more powerful tools are required. The debugger in IDA complements the static analysis capabilities of the disassembler. By allowing an analyst to single-step through the code being investigated, the debugger often bypasses the obfuscation. It helps obtain data that the more powerful static disassembler will be able to process in depth.

7. The **IDA** main window appears, along with the **Select file to disassemble** window.
8. In the **Select file to disassemble** window, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Open**.

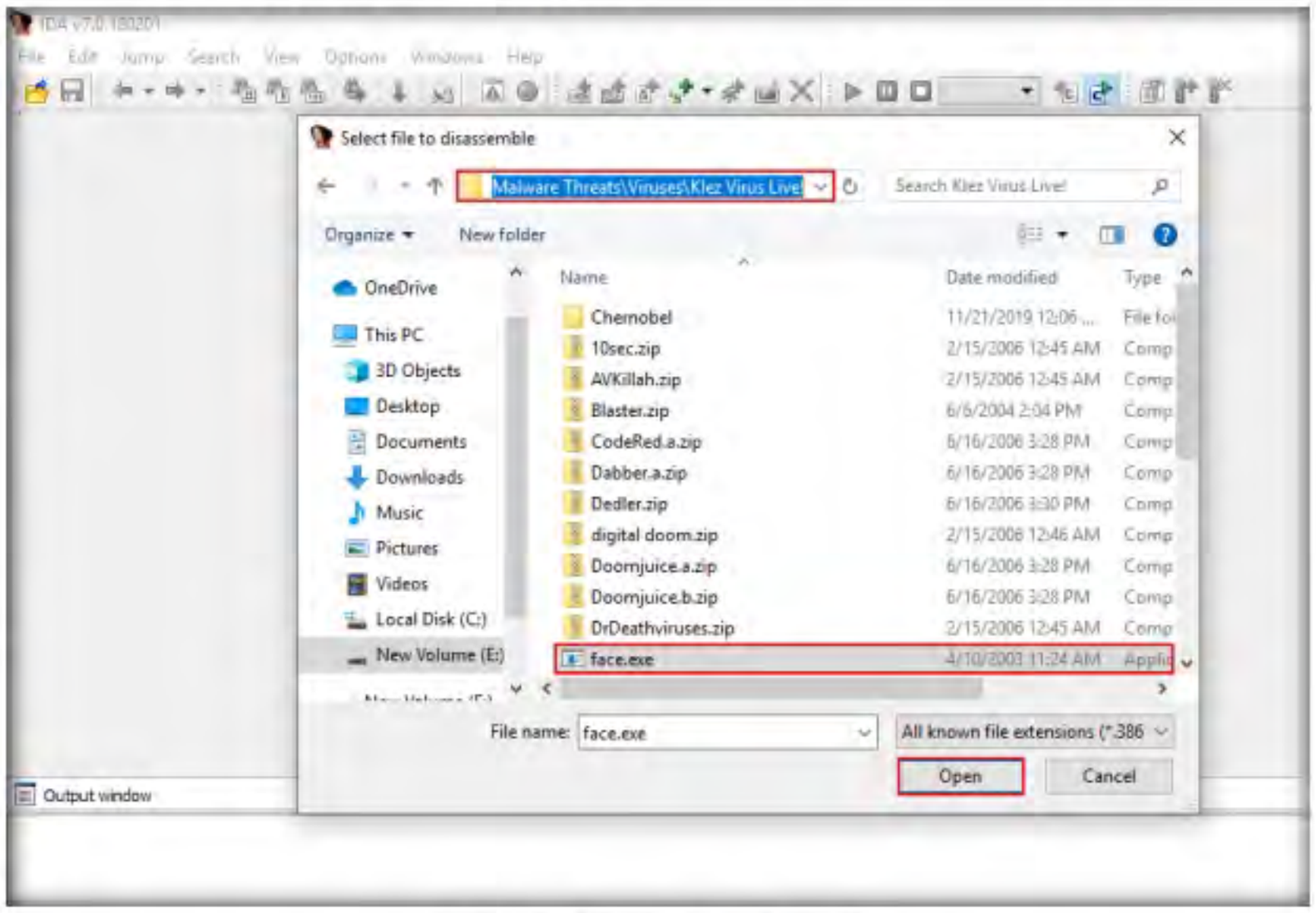


Figure 3.6.4: Choosing a file to Disassemble

9. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.

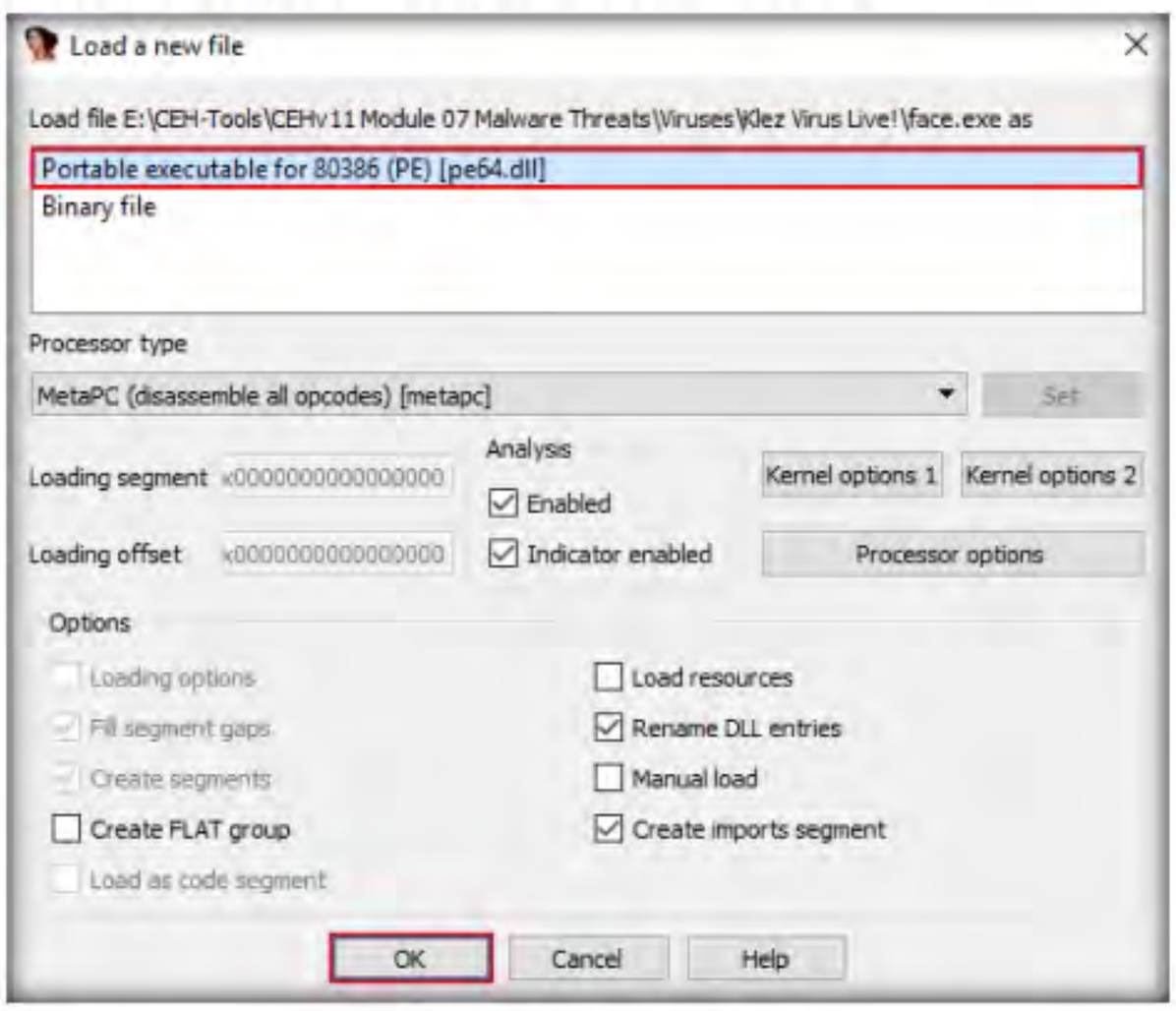


Figure 3.6.5: Load a New File

TASK 6.3

View the Result

10. If a **Warning** pop-up appears, click **OK**.
11. If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.
12. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.

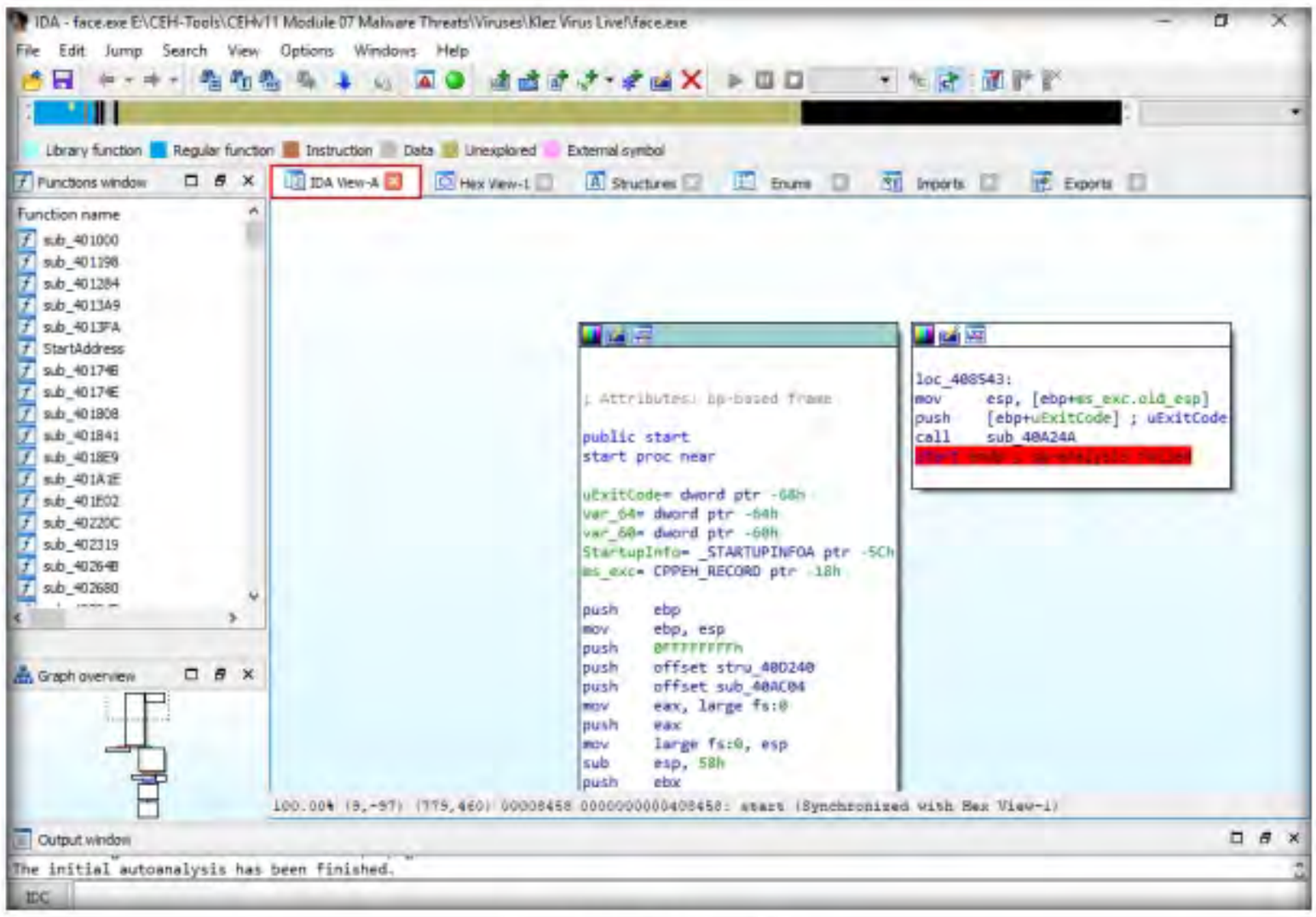


Figure 3.6.6: IDA View-A Tab

13. In the **IDA View-A** section, right-click anywhere and choose **Text view** from the context menu to view the text information of the malicious file uploaded to IDA for analysis.

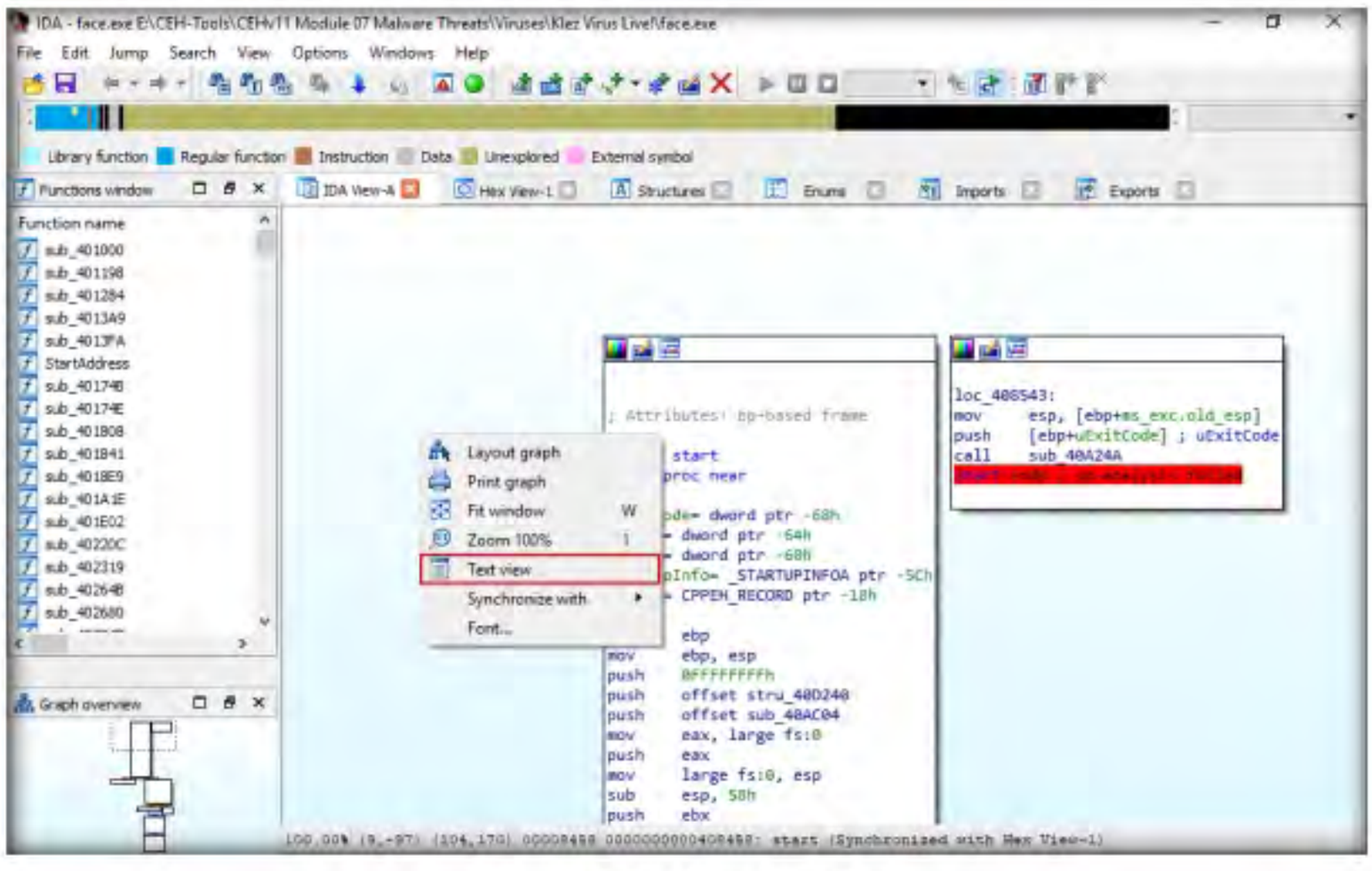


Figure 3.6.7: IDA View-A Text View

14. This reveals the text view of the malicious file, allowing analysis of its information.

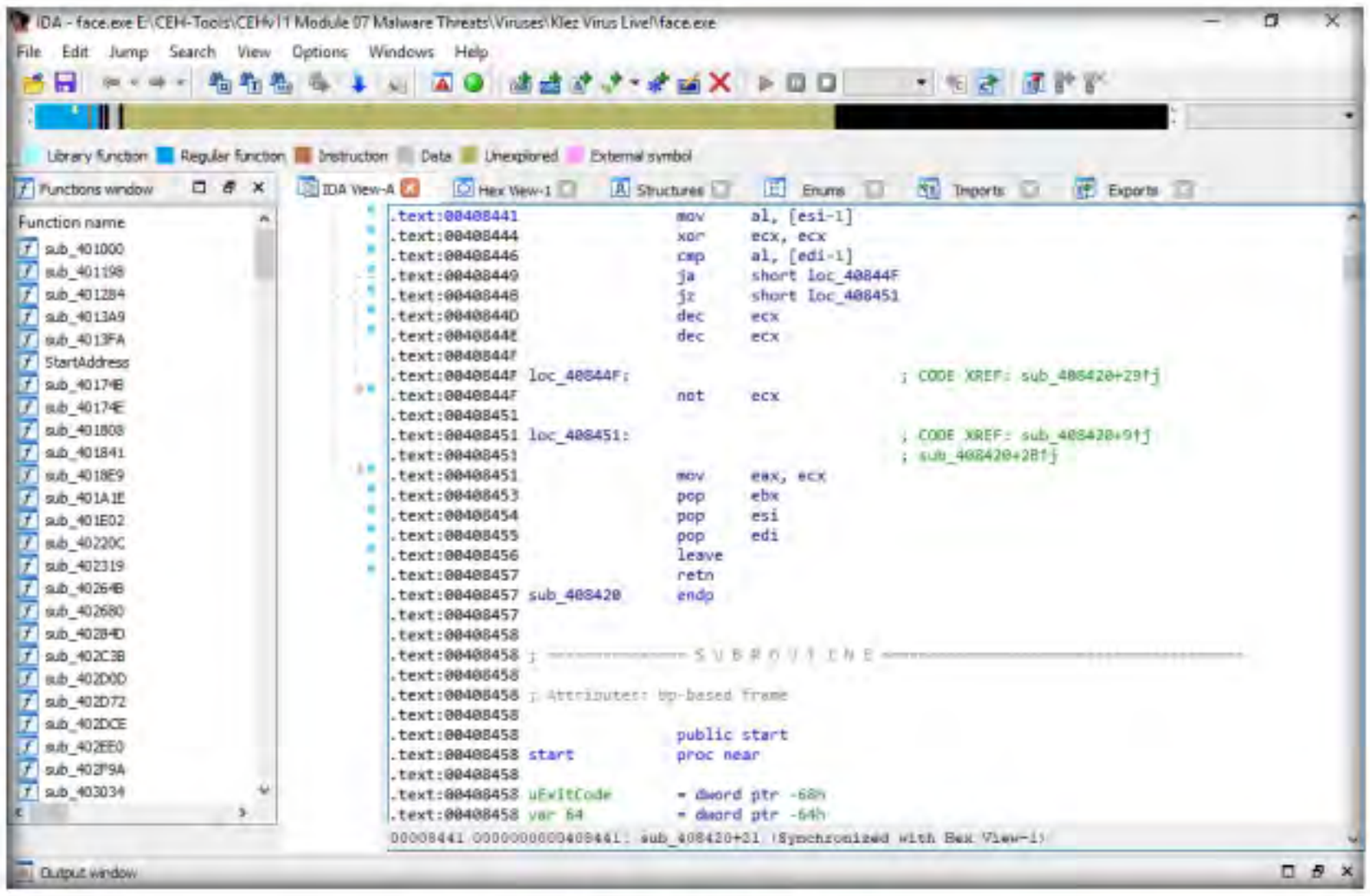


Figure 3.6.8: IDA View-A Text View

15. Now, minimize the IDA window, and navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**. Copy the **qwingraph.exe** file and paste it in IDA's installation location. In this lab, the location is **C:\Program Files\IDA Freeware 7.0**.

Note: If a **Destination Folder Access Denied** notification appears, click **Continue**.

16. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View → Graphs** and click **Flow chart**.

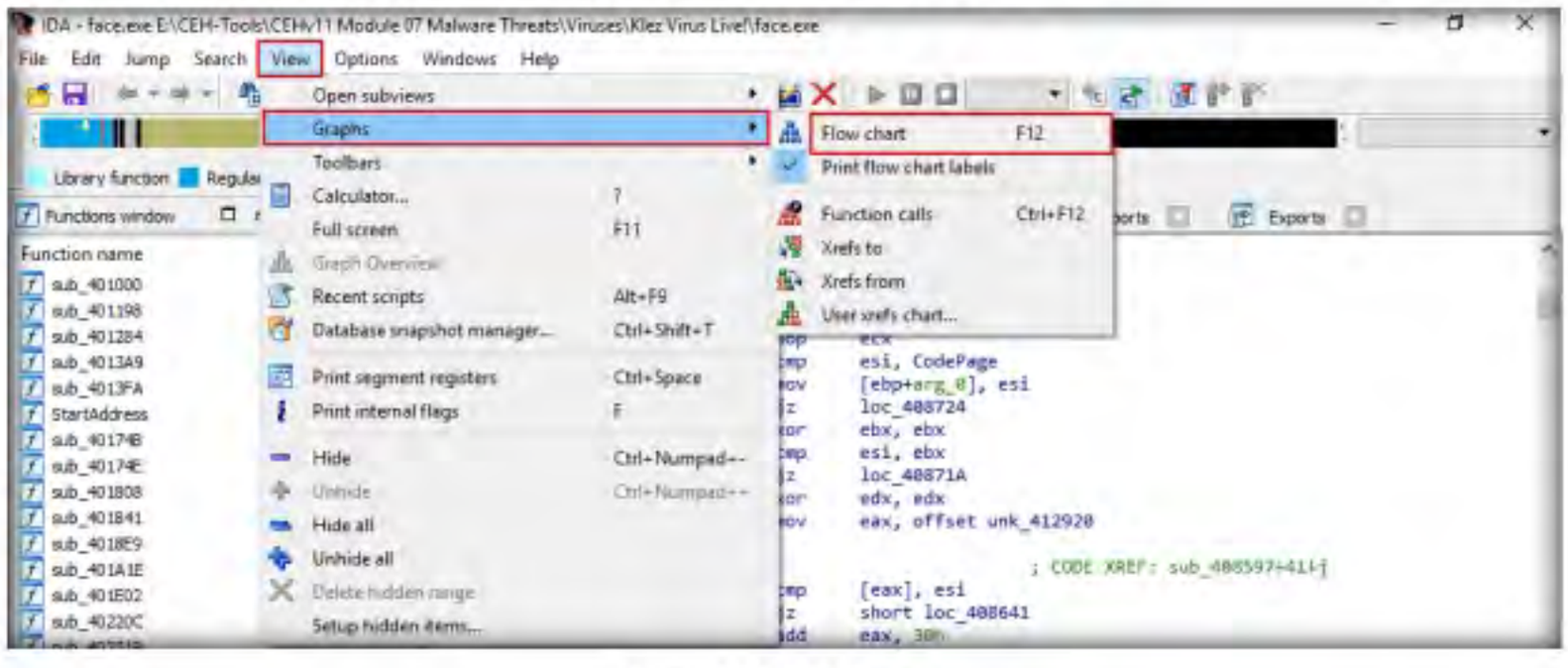


Figure 3.6.9: IDA Graphs

17. A **Graph** window appears with the flow. You may zoom in to view this more clearly.

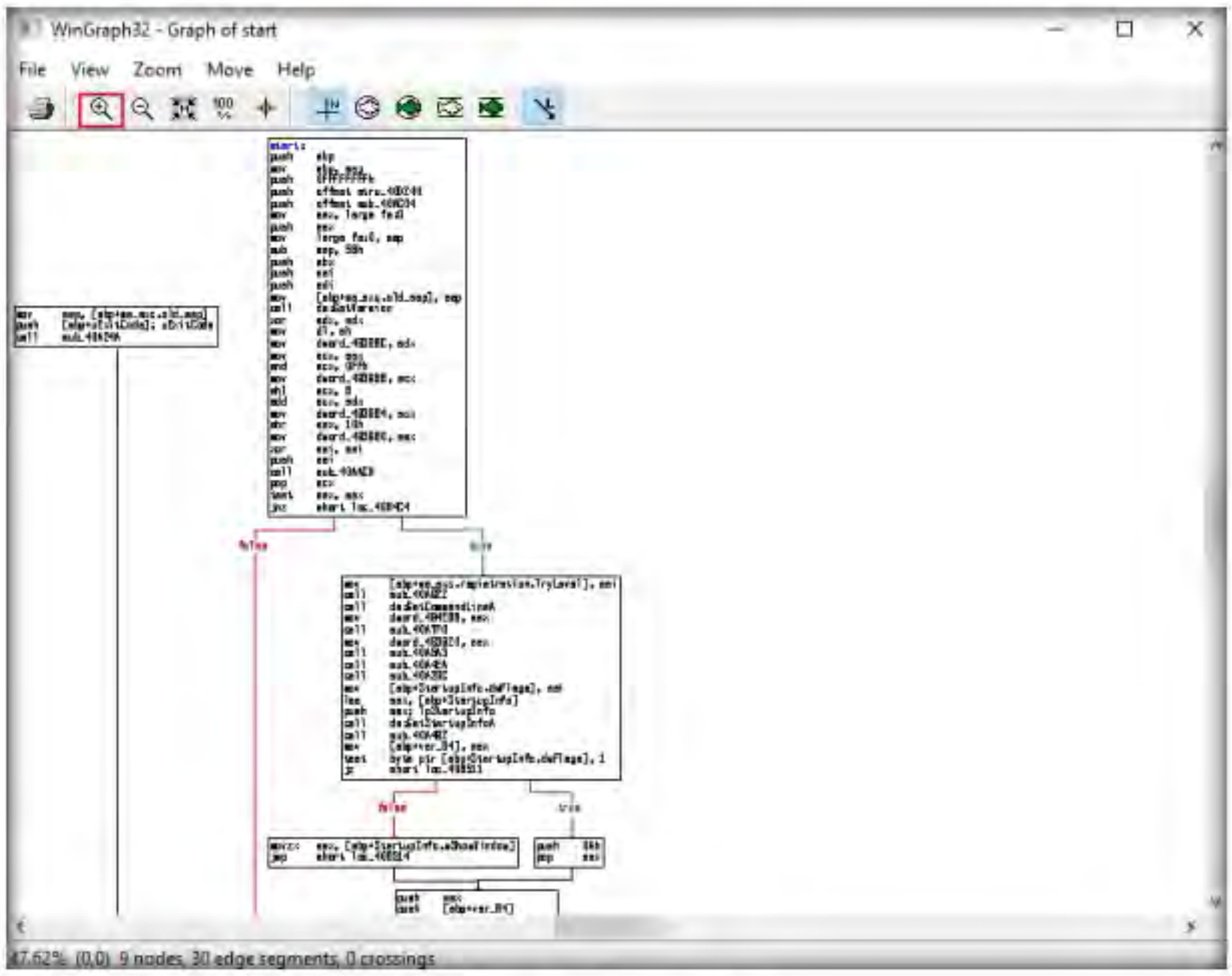


Figure 3.6.10: IDA Flow Chart

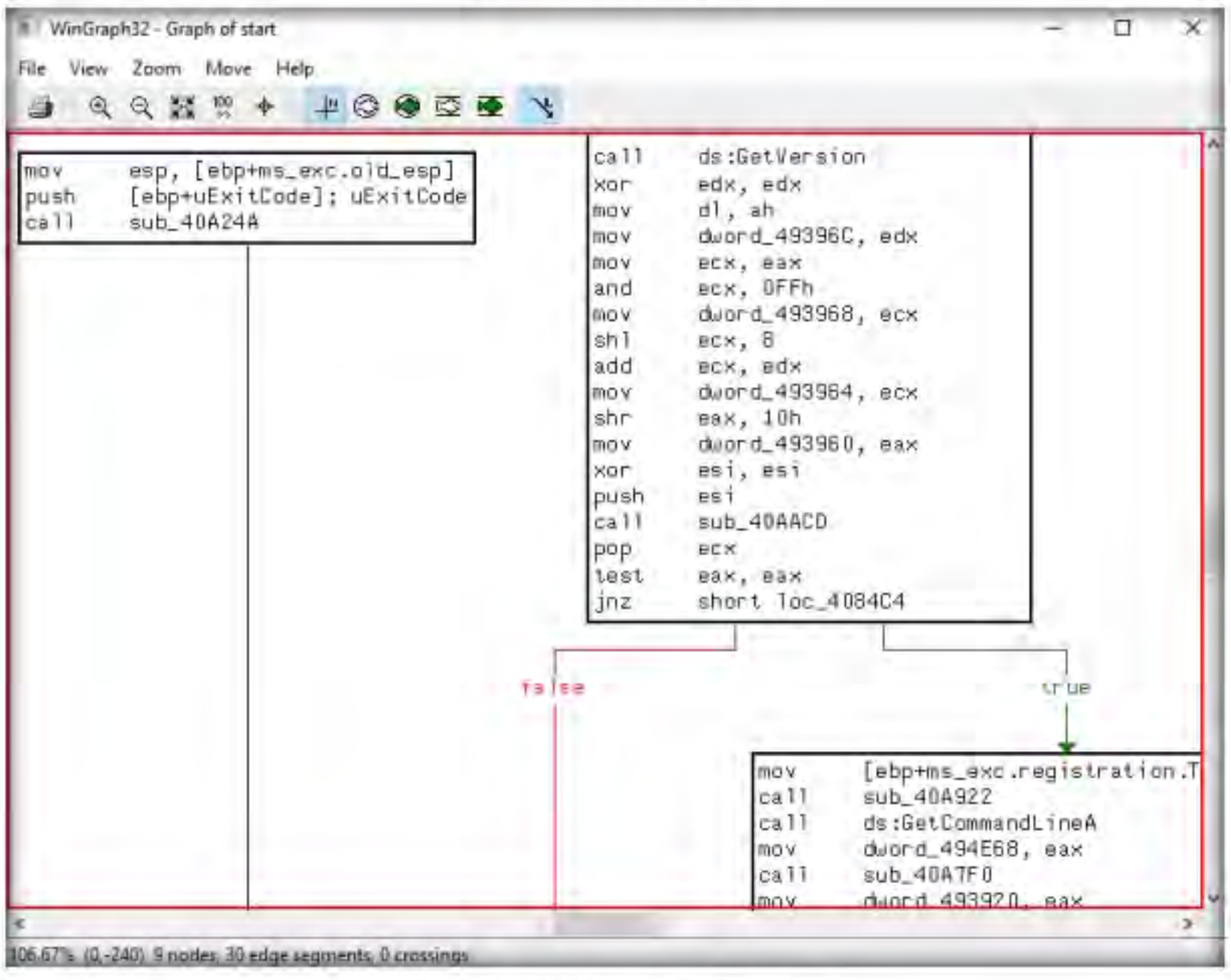


Figure 3.6.11: IDA Flow Chart Zoom View

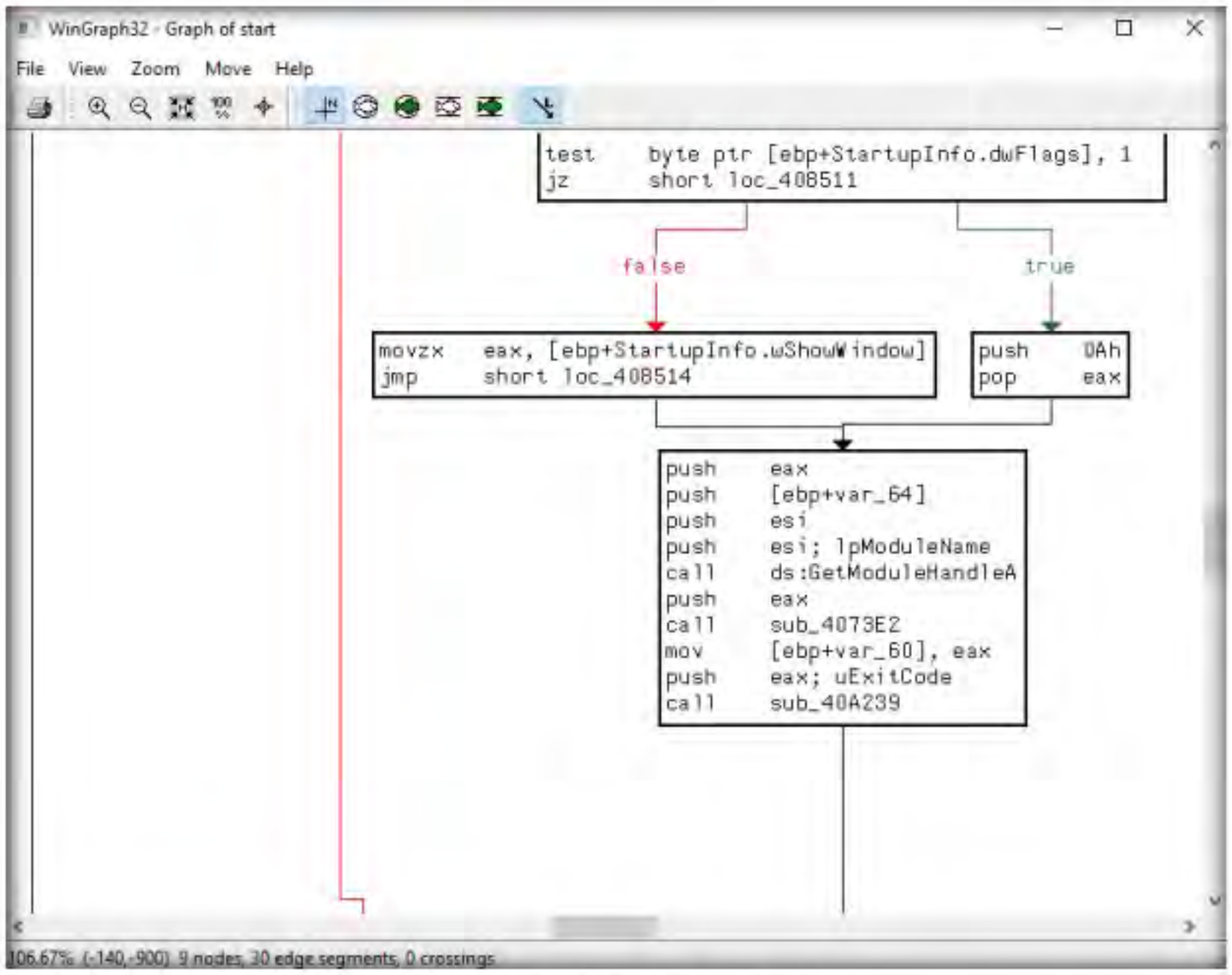


Figure 3.6.12: IDA Flow Chart More Details

18. Close the **Graph** window, go to **View → Graphs**, and click **Function calls** from the menu bar.

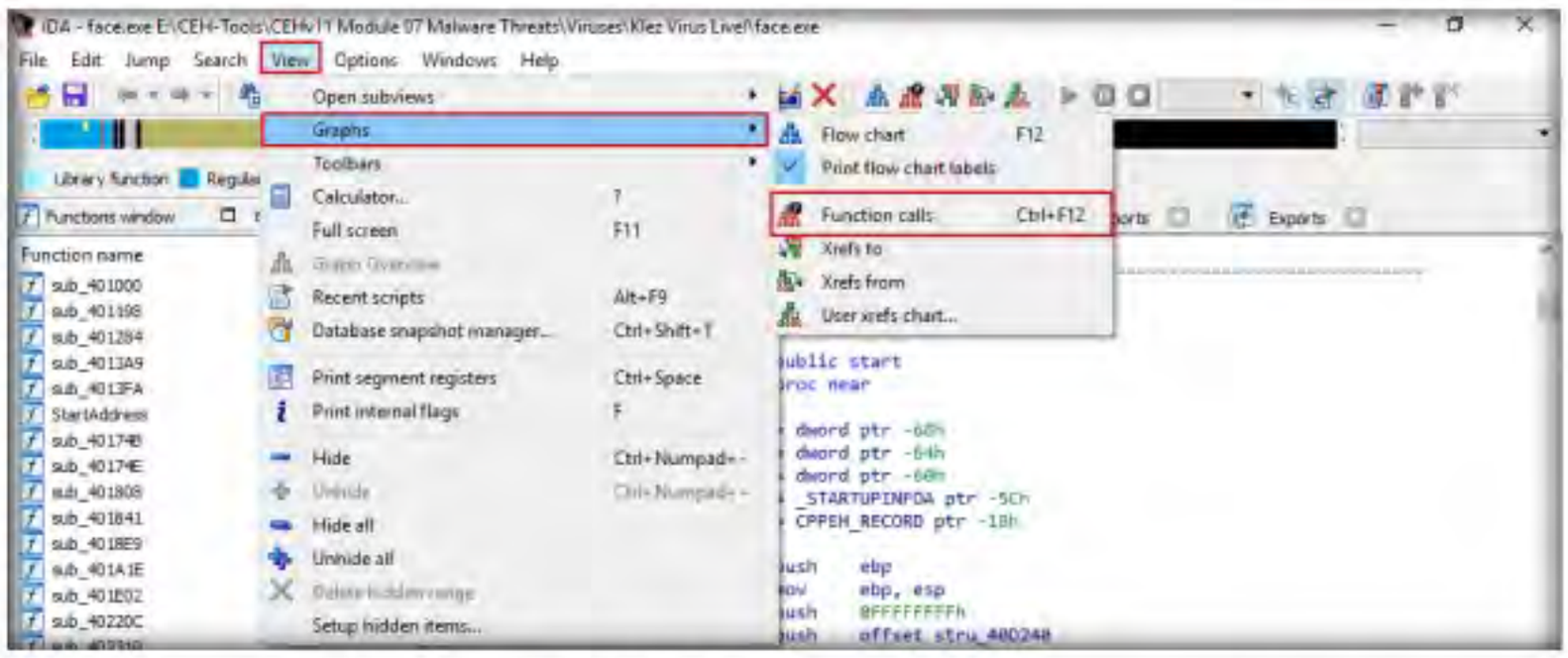


Figure 3.6.13: IDA Function Calls Menu

19. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.

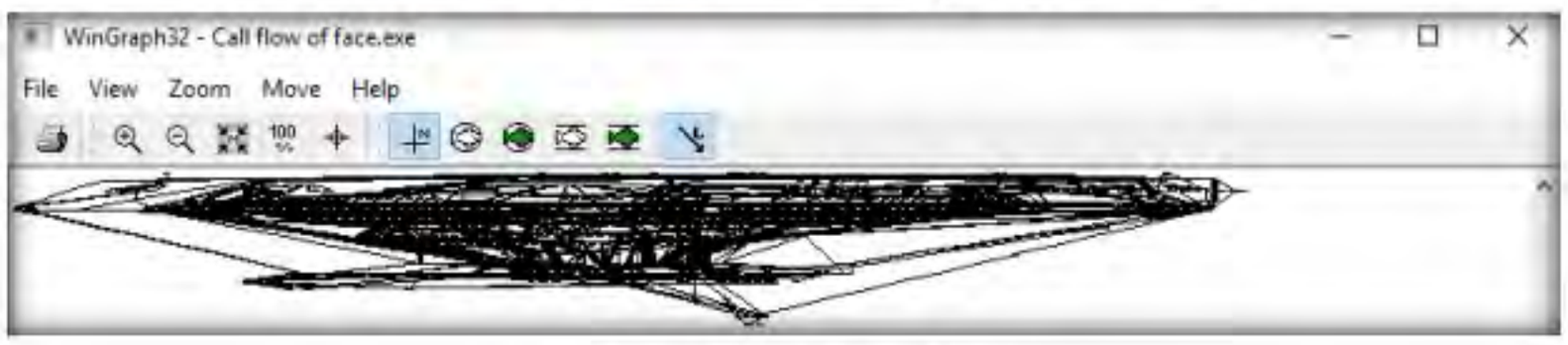


Figure 3.6.14: IDA Call Flow of face.exe

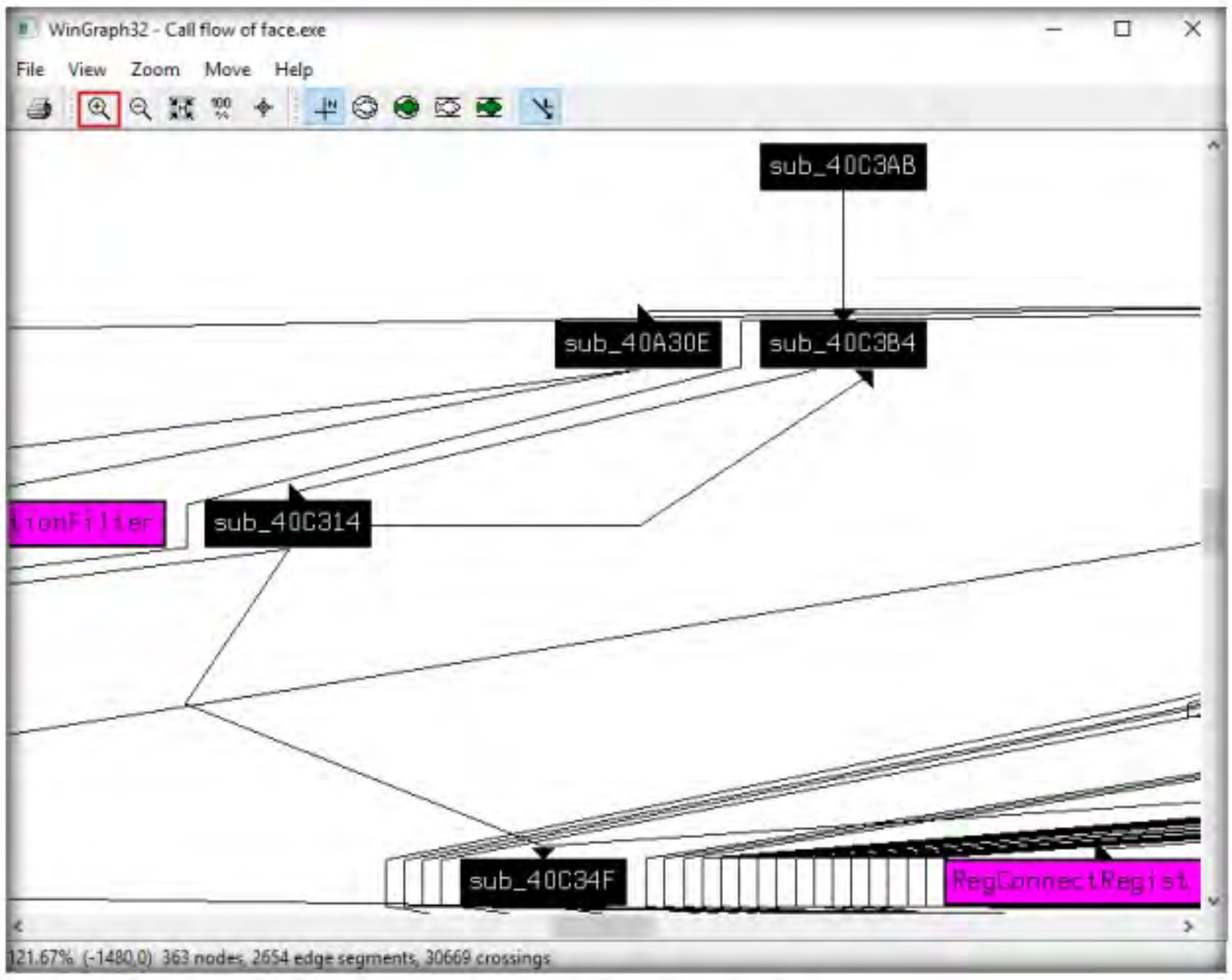


Figure 3.6.15: IDA Call Flow of face.exe with Zoom

20. Click the **HexView-1** tab to view the hex value of the malicious file.

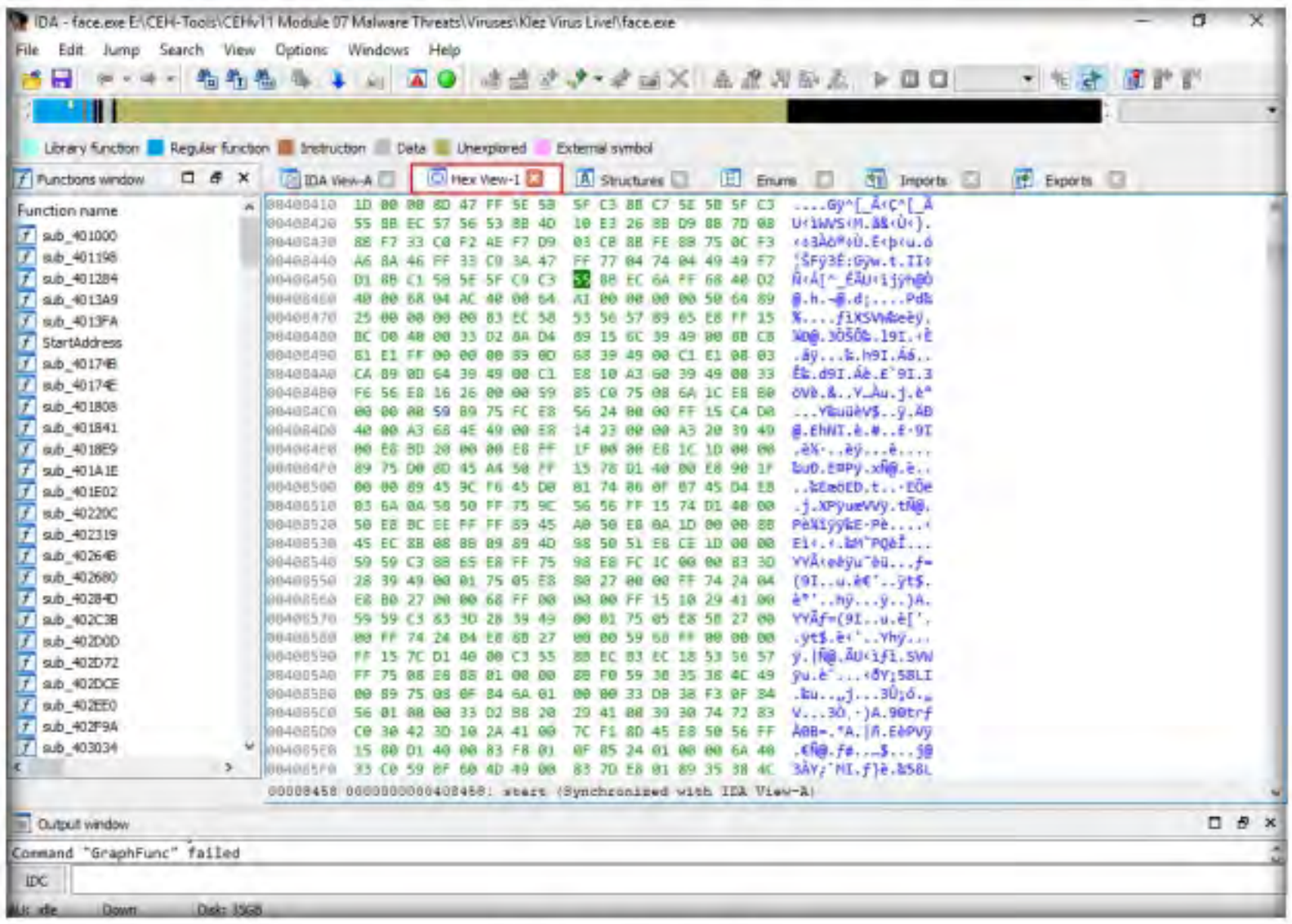


Figure 3.6.16: IDA Hex View-1

21. Click the **Structures** tab to view the structure of the file, as shown in the screenshot.
22. IDA displays all **Structures** (to expand the structures, click on **Ctrl** and **+**).

Figure 3.6.17: IDA Structures Tab

23. Click the **Enums** tab to view the Windows Enum results, as shown in the screenshot.

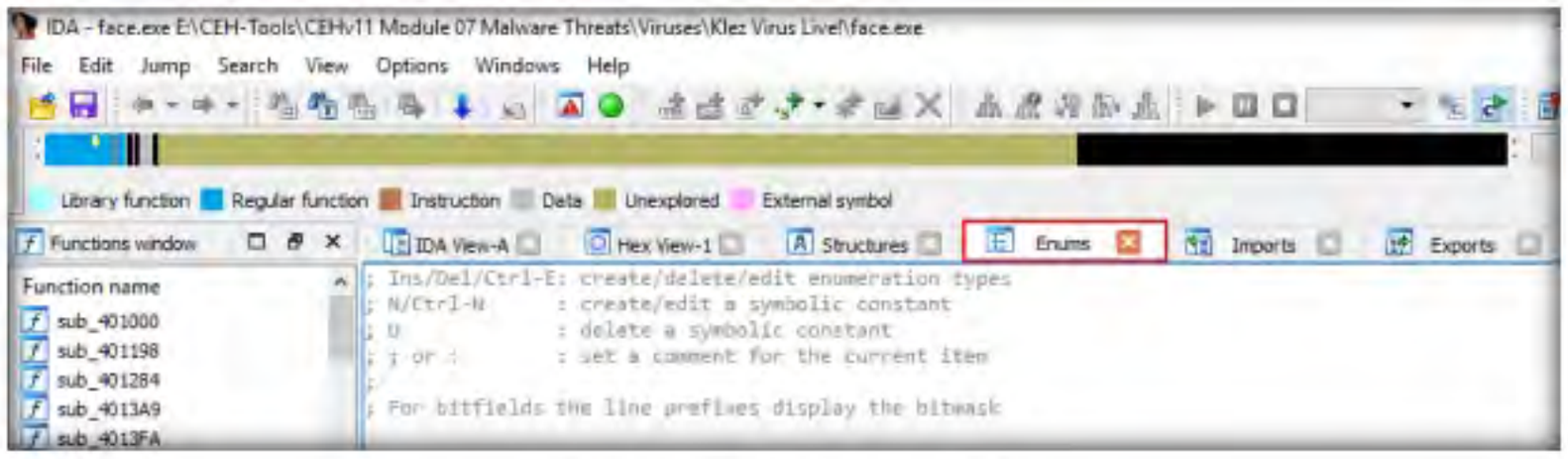


Figure 3.6.18: IDA Pro Enums Tab

24. Close all open windows.

TASK 6.4

Debug a Virus using OllyDbg

25. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **OLLYDBG.EXE**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

26. If a **UDD Directory Absent** dialog box appears, click **OK**.
27. If an OllyDbg warning message appears, for administrative rights, click **OK**.
28. The **OllyDbg** main window appears, as shown in the screenshot.

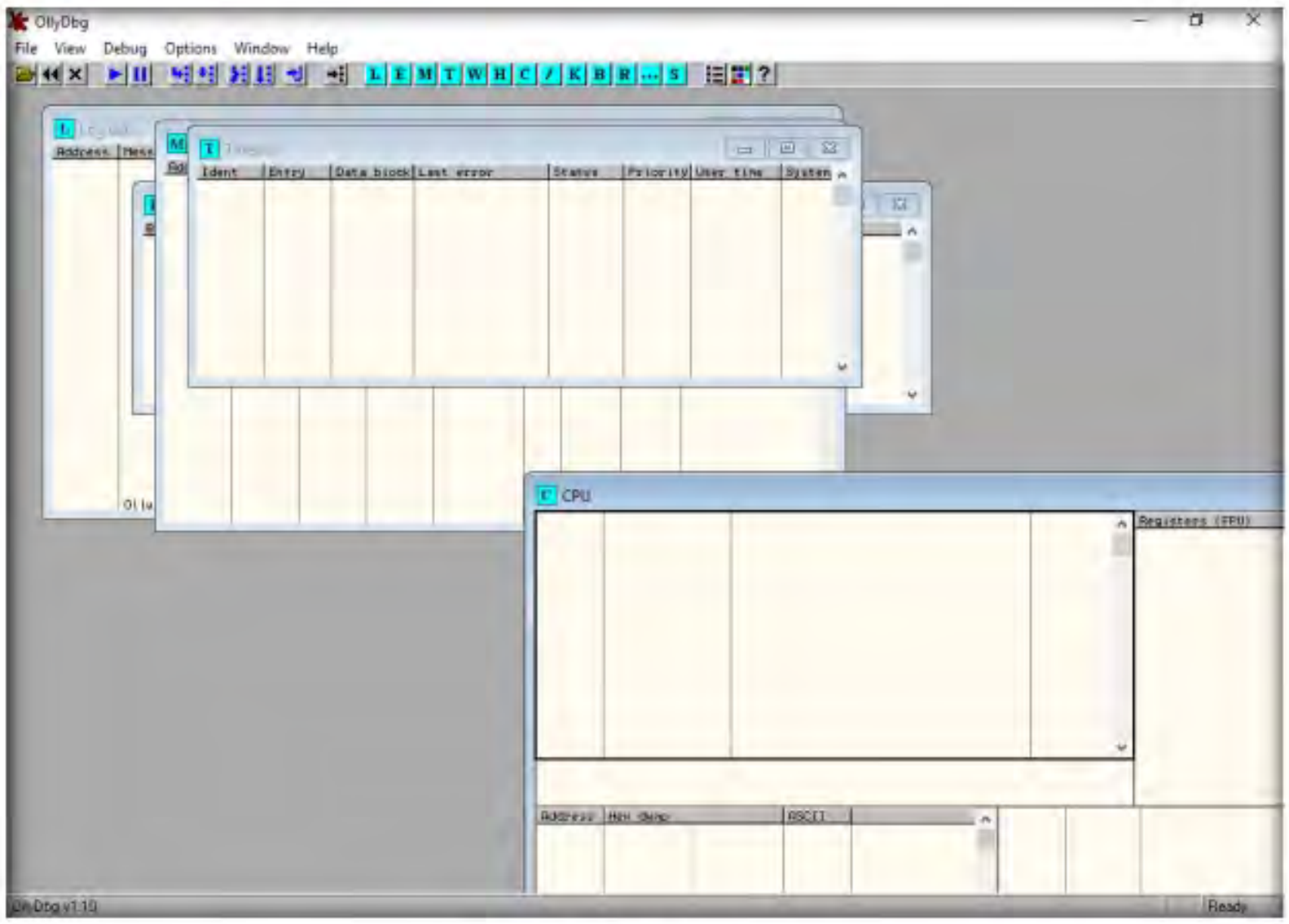


Figure 3.6.19: OllyDbg main window

OllyDbg

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter(), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue(), and NTDLL.NtQueryInformationProcess().

Note: When you launch OllyDbg for the first time, several sub-windows might appear in the main window of OllyDbg; close them all.

29. Choose **File** from the menu bar, and then choose **Open**.
30. The **Open 32-bit executable** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

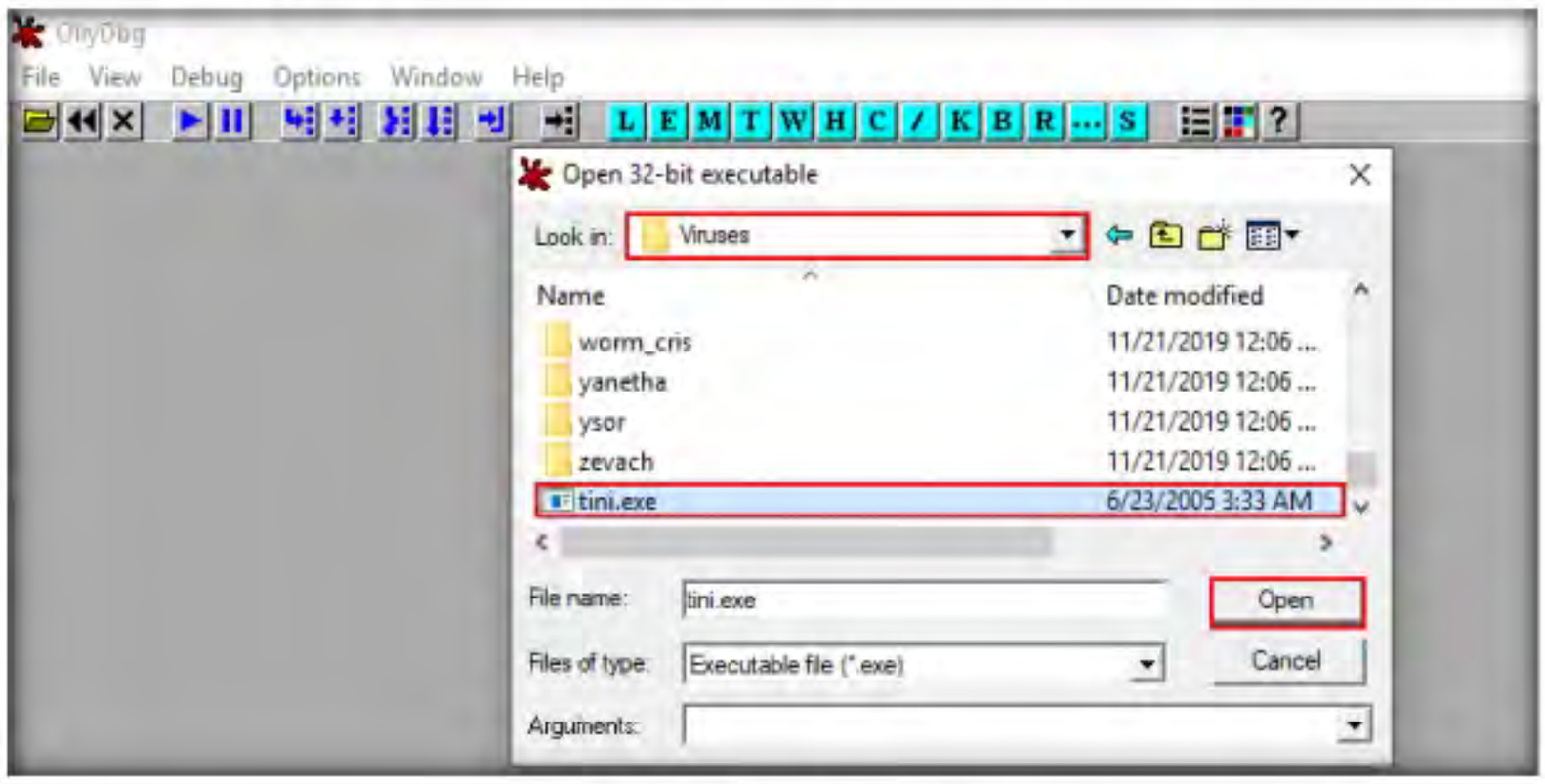


Figure 3.6.20: Select tini.exe Virus

31. The output appears in a window named **CPU - main thread, module ntdll**, as shown in the screenshot.

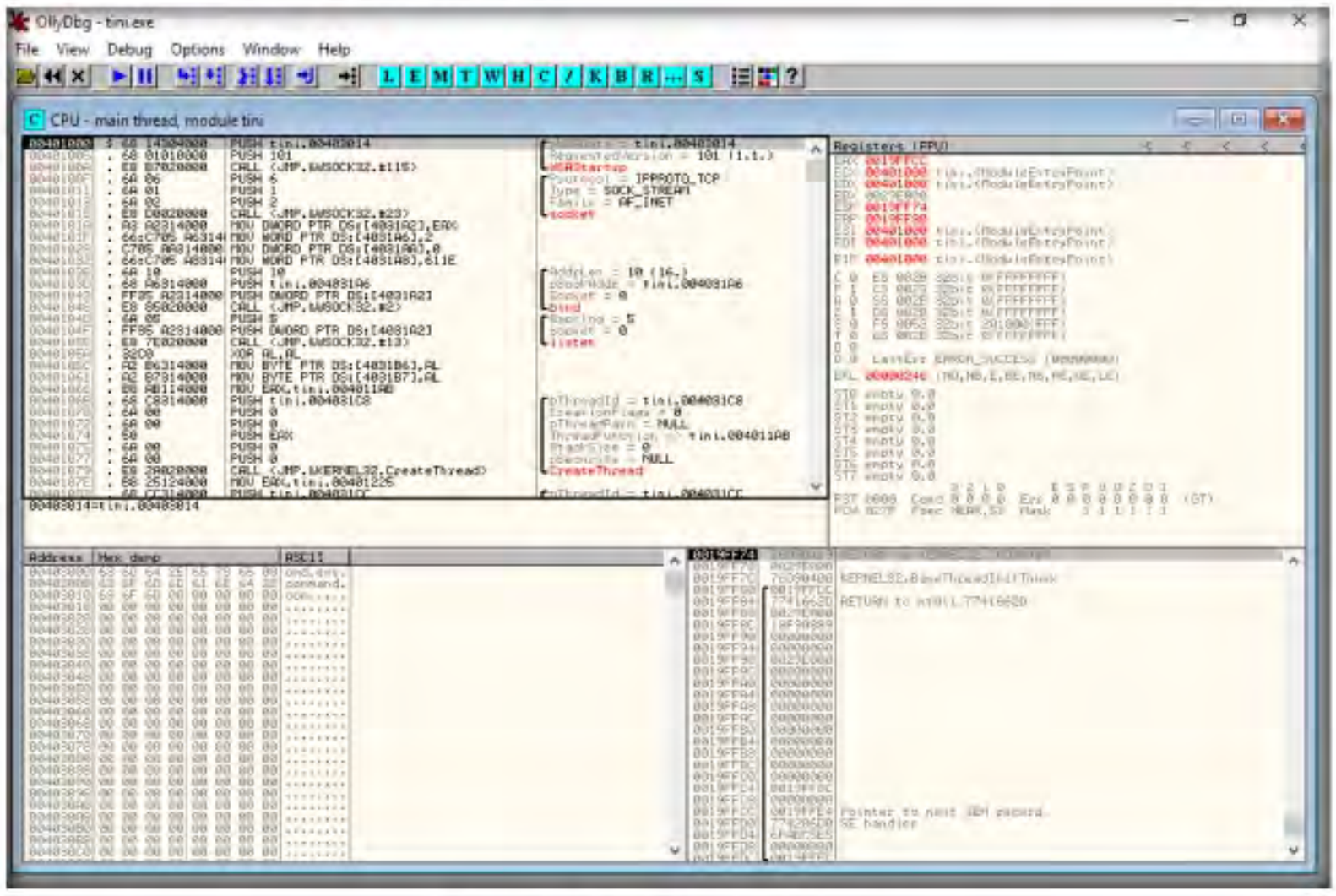


Figure 3.6.21: CPU utilization of tini.exe

32. Choose **View** in the menu bar, and then choose **Log**.

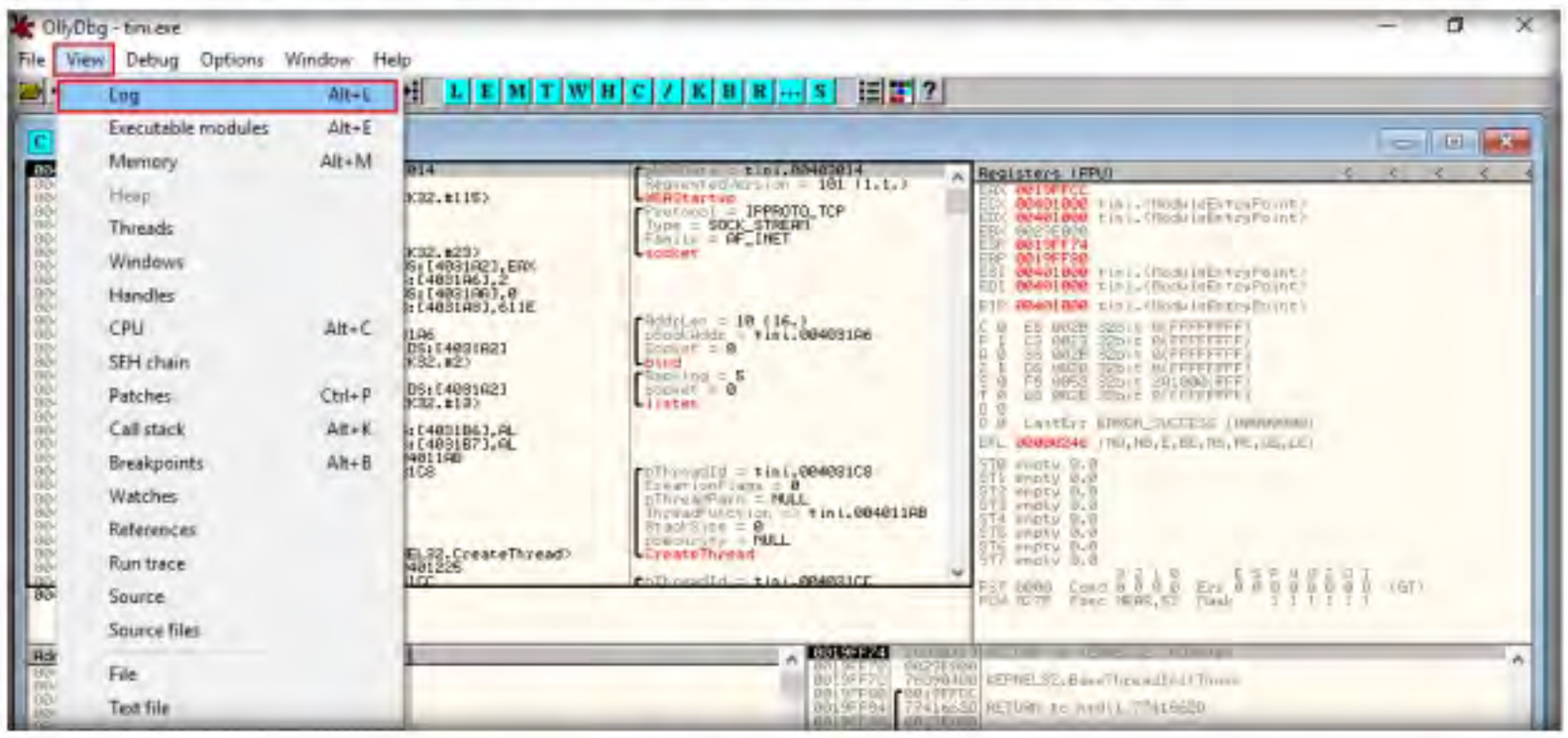


Figure 3.6.22: Select log information

33. A window named **Log data** appears in OllyDbg, displaying the log details, as shown in the screenshot.

34. The **Log data** also displays the program entry point and its calls to known functions. Close the **Log data** window after completing the analysis.

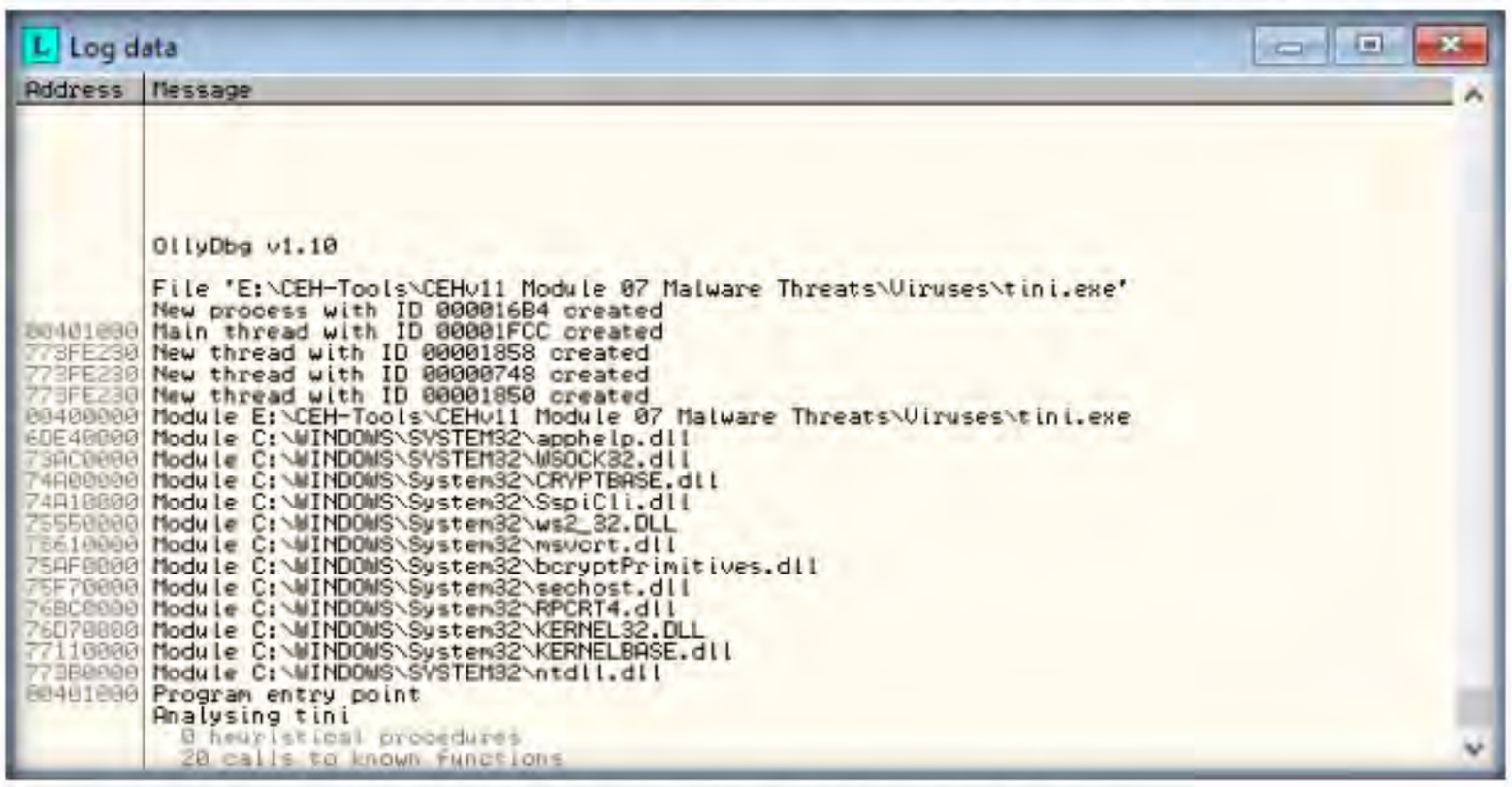


Figure 3.6.23: Output of Log data information of tini.exe

35. Choose **View** in the menu bar, and then choose **Executable modules**.

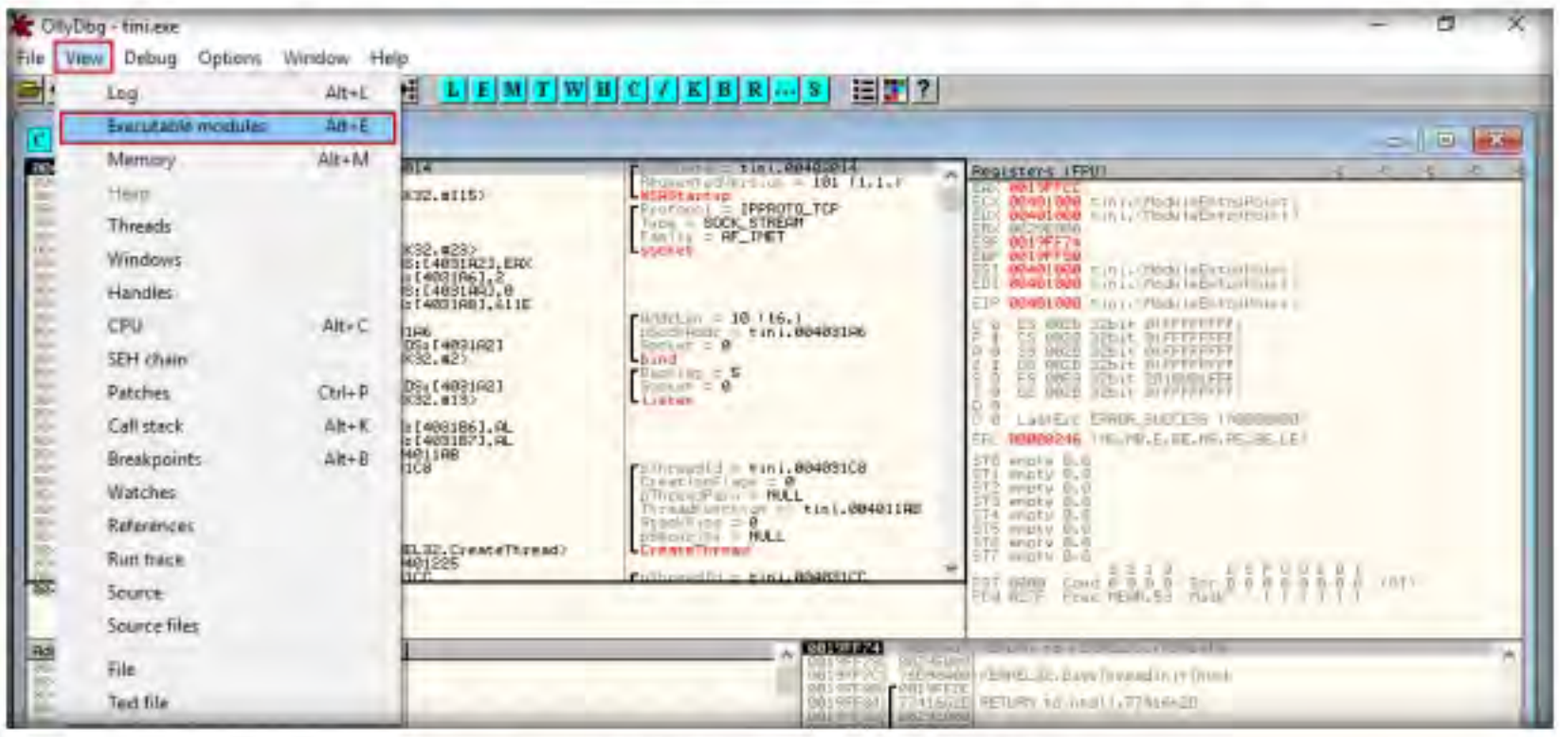


Figure 3.6.24: Viewing executable modules

36. A window named **Executable modules** appears in OllyDbg, displaying all executable modules, as shown in the screenshot.
37. Double-click any module to view the complete information of the selected module.
38. In this exercise, we are choosing the **6DE40000** module.

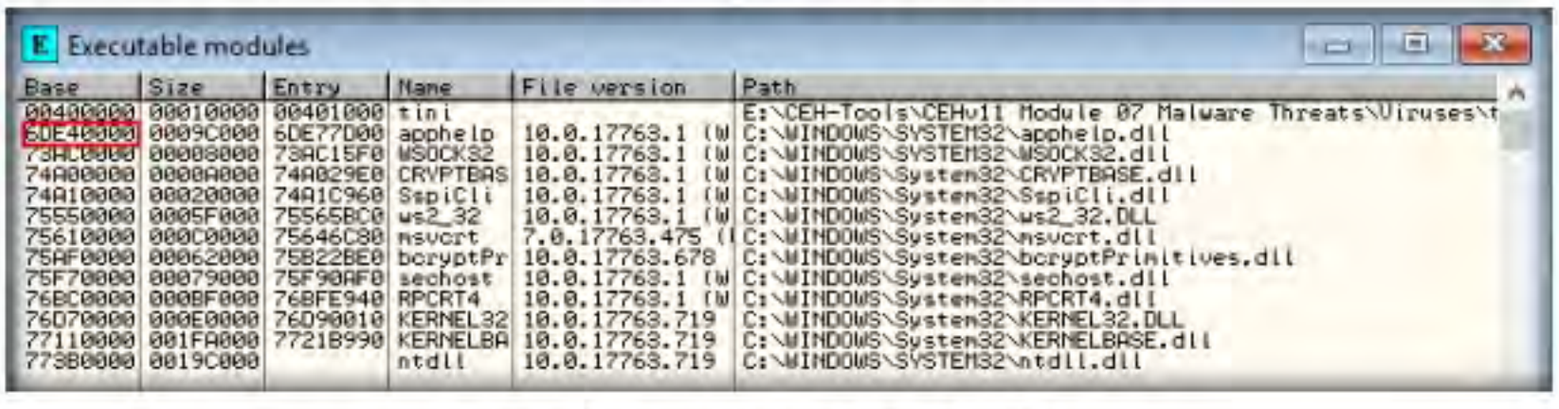


Figure 3.6.25: Output of executable modules of tini.exe

39. This will redirect you to the **CPU - main thread** window, as shown in the screenshot.

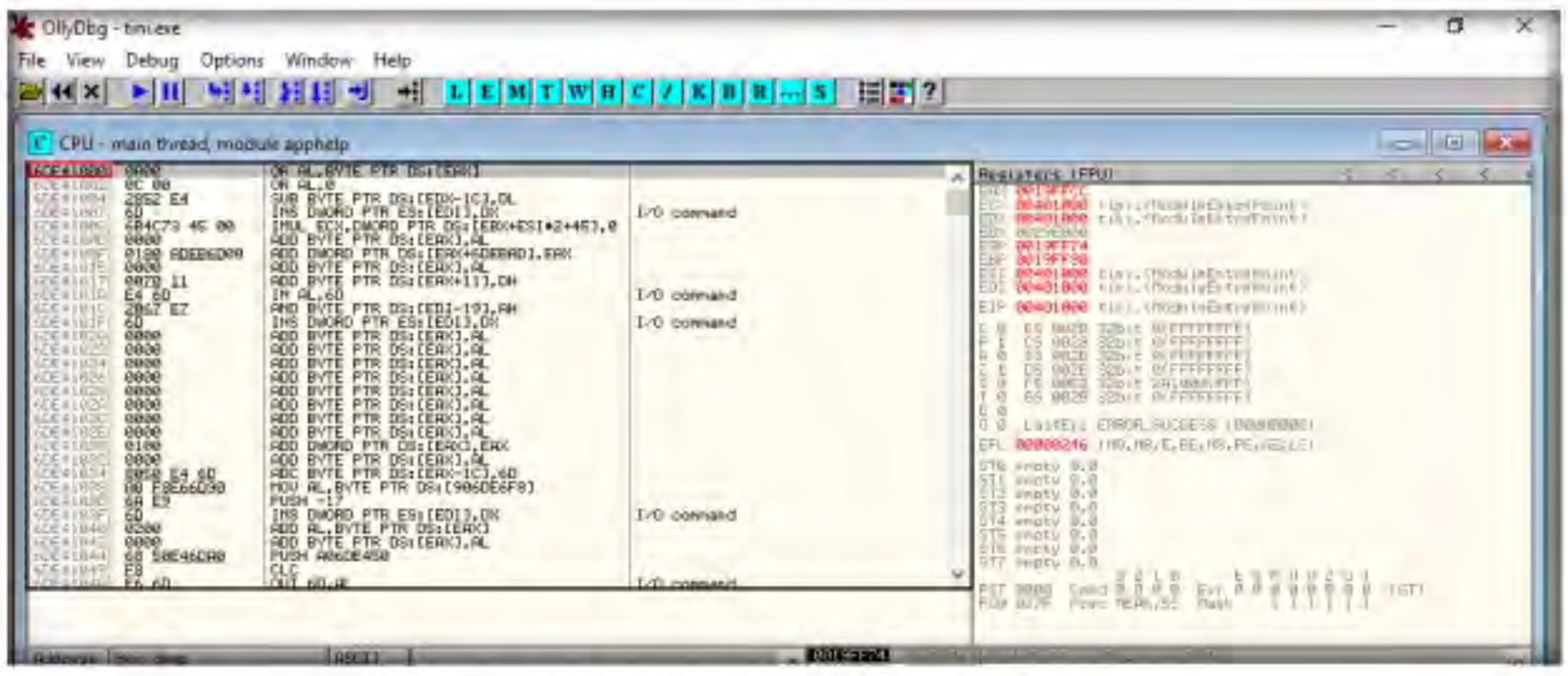


Figure 3.6.26: Output of executable modules of tini.exe

40. Choose **View** in the menu bar, and then choose **Memory**.

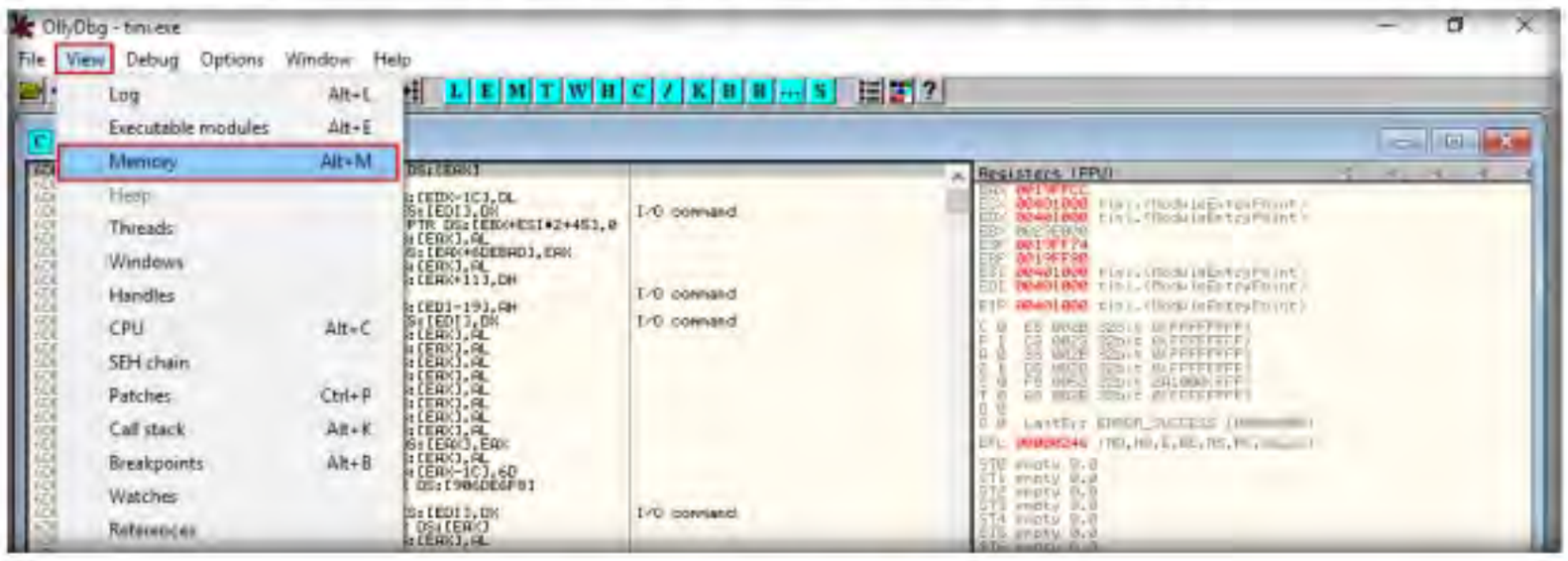
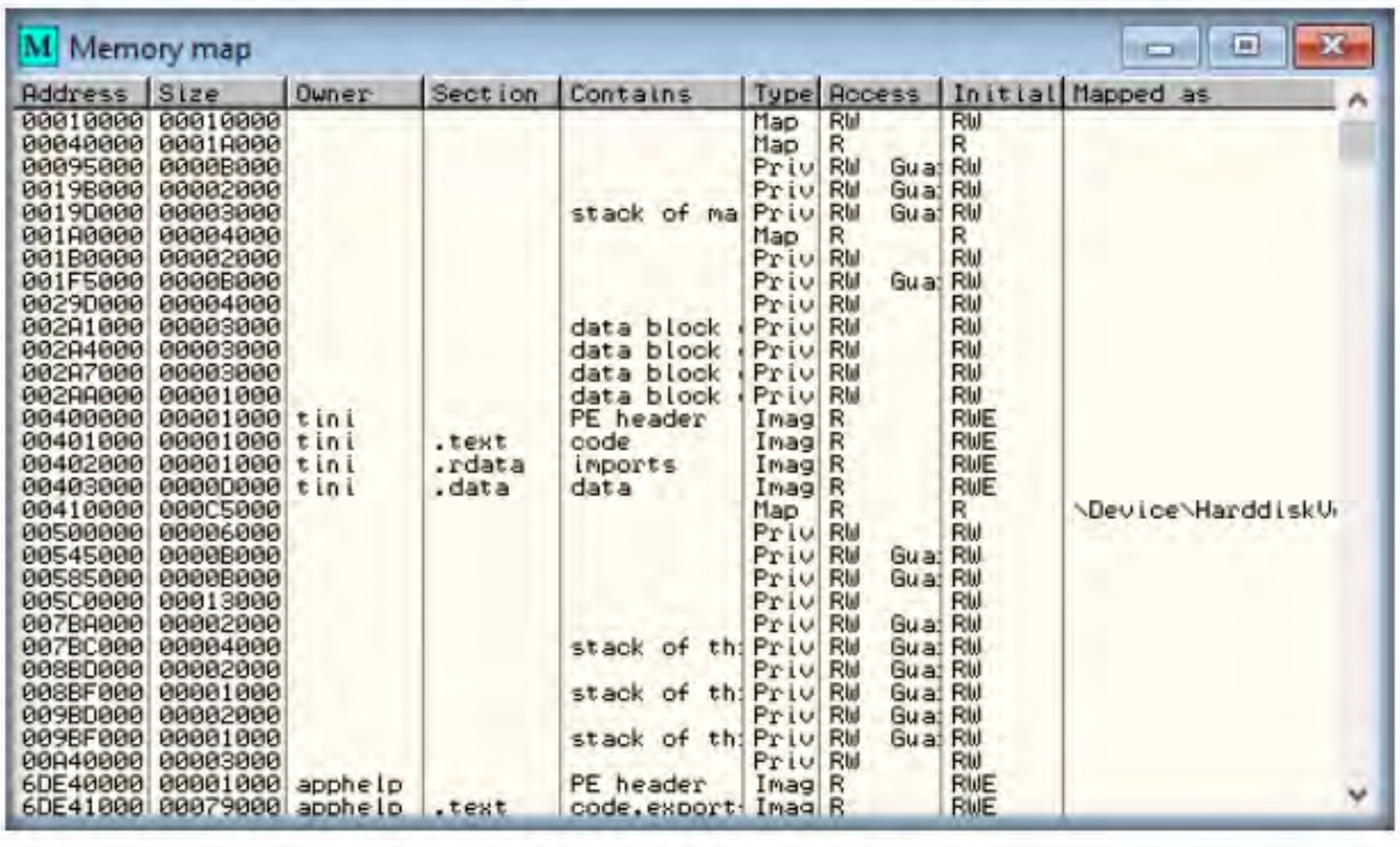


Figure 3.6.27: Viewing memory mappings

41. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.



Memory map

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00040000	0001A000				Map	R	R	
00095000	0000B000				Priv	RW Gua	RW	
0019B000	00002000				Priv	RW Gua	RW	
0019D000	00003000			stack of ma	Priv	RW Gua	RW	
001A0000	00004000				Map	R	R	
001B0000	00002000				Priv	RW	RW	
001F5000	0000B000				Priv	RW Gua	RW	
0029D000	00004000				Priv	RW	RW	
002A1000	00003000			data block	Priv	RW	RW	
002A4000	00003000			data block	Priv	RW	RW	
002A7000	00003000			data block	Priv	RW	RW	
002AA000	00001000			data block	Priv	RW	RW	
00400000	00001000	tini		PE header	Imag	R	RWE	
00401000	00001000	tini	.text	code	Imag	R	RWE	
00402000	00001000	tini	.rdata	imports	Imag	R	RWE	
00403000	0000D000	tini	.data	data	Imag	R	RWE	
00410000	000C5000				Map	R	R	\Device\HarddiskV
00500000	00006000				Priv	RW	RW	
00545000	0000B000				Priv	RW Gua	RW	
00585000	0000B000				Priv	RW Gua	RW	
005C0000	00013000				Priv	RW	RW	
007BA000	00002000				Priv	RW Gua	RW	
007BC000	00004000			stack of th	Priv	RW Gua	RW	
008BD000	00002000				Priv	RW Gua	RW	
008BF000	00001000			stack of th	Priv	RW Gua	RW	
009BD000	00002000				Priv	RW Gua	RW	
009BF000	00001000			stack of th	Priv	RW Gua	RW	
00A40000	00003000				Priv	RW	RW	
6DE40000	00001000	apphelp		PE header	Imag	R	RWE	
6DE41000	00079000	apphelp	.text	code,export	Imag	R	RWE	

Figure 3.6.28: Output of Memory map of tini.exe

42. Choose **View** in the menu bar, and then choose **Threads**.

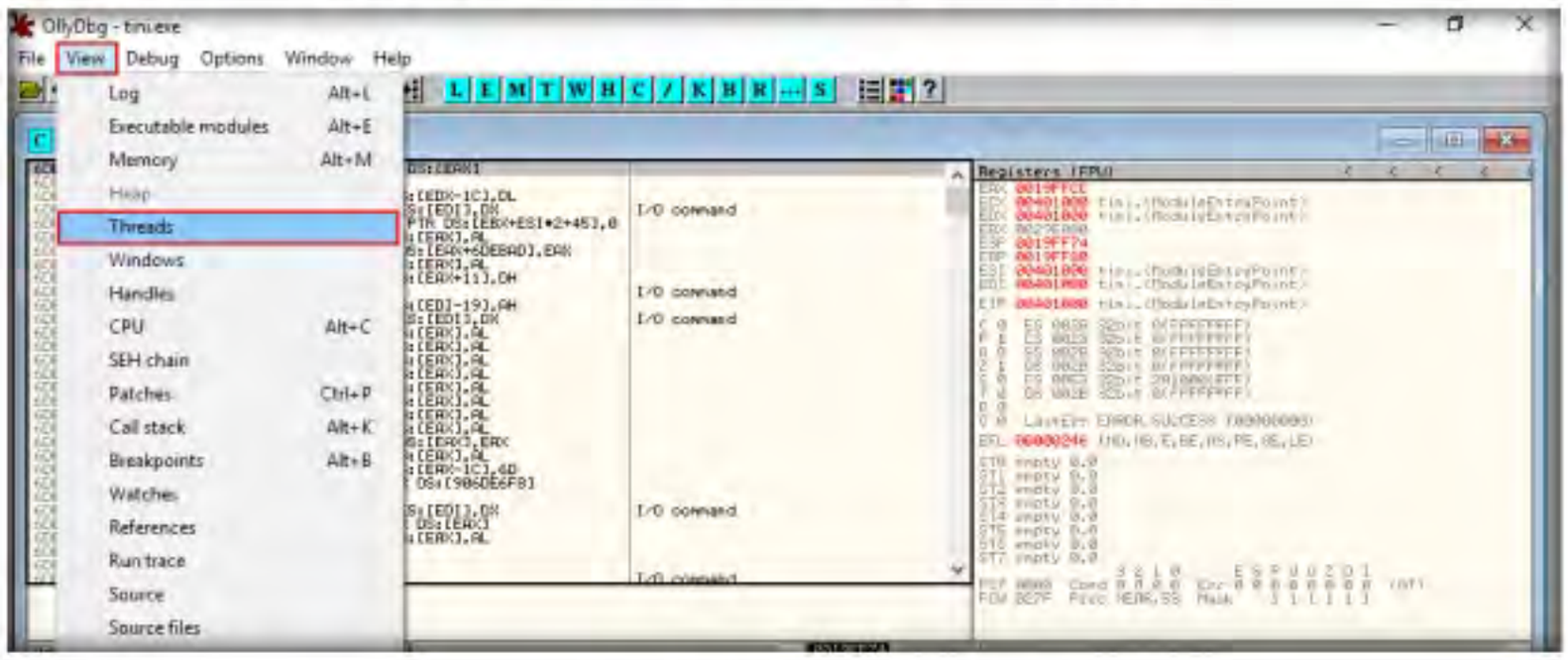


Figure 3.6.29: Viewing the threads

> You can also use other disassembling and debugging tools such as **Ghirda** (https://ghidra-sre.org), **Radare2** (https://rada.re), **WinDbg** (http://www.windbg.org), and **ProcDump** (https://docs.microsoft.com) to perform malware disassembly.

43. A window named **Threads** appears in OllyDbg, displaying all threads, as shown in the screenshot.

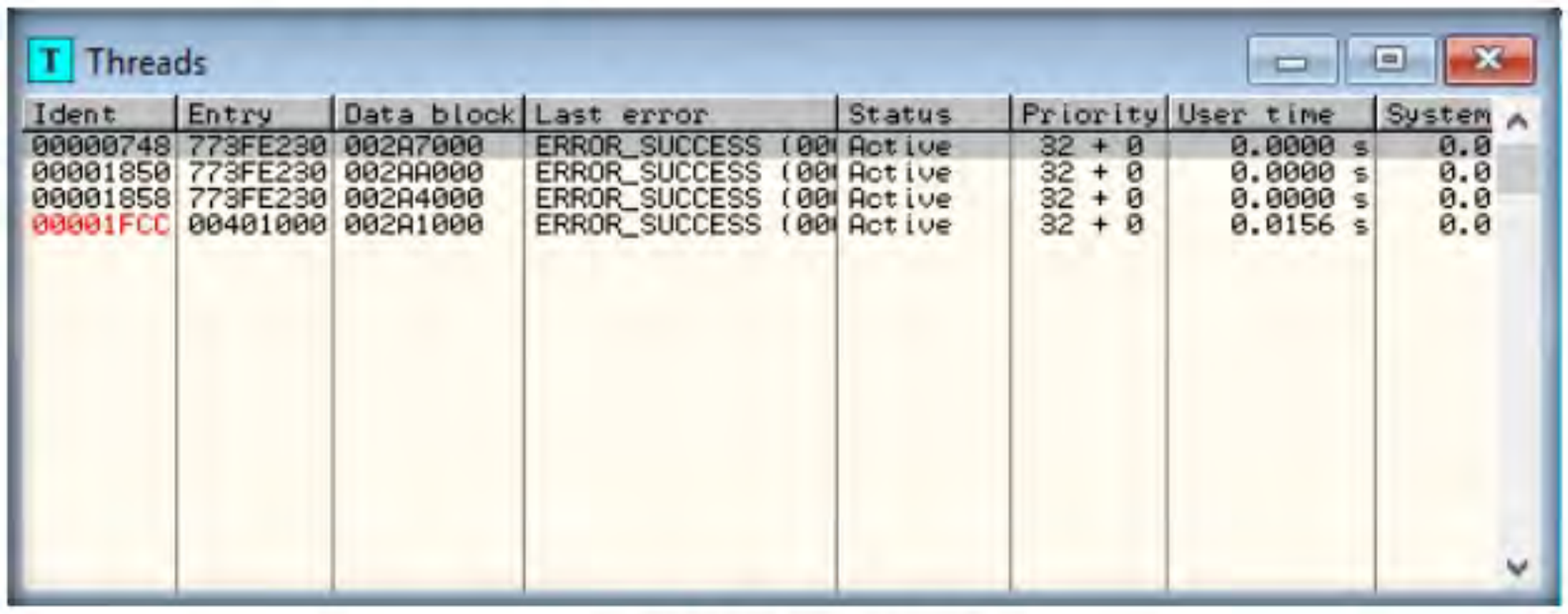


Figure 3.6.30: Output of threads

44. This way, you can scan files and analyze the output using OllyDbg.
45. Close all open windows and turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Perform Dynamic Malware Analysis

Dynamic malware analysis is the process of studying the behavior of malware by running it in a monitored environment.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Dynamic Malware Analysis, also known as behavioral analysis, involves executing malware code to learn how it interacts with the host system and its impact after infecting the system.

Dynamic analysis involves the execution of malware to examine its conduct and operations and identify technical signatures that confirm the malicious intent. It reveals information such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, and DLL and linked files located on the system or network.

This type of analysis requires a safe environment such as virtual machines and sandboxes to deter the spreading of malware. The environment design should include tools that can capture every movement of the malware in detail and give feedback. Typically, virtual systems act as a base for conducting such experiments.

An ethical hacker and pen tester must perform dynamic malware analysis to find out about the applications and processes running on a computer and remove unwanted or malicious programs that can breach privacy or affect the system's health.

Lab Objectives

- Perform port monitoring using TCPView and CurrPorts
- Perform process monitoring using Process Monitor
- Perform registry monitoring using Regshot and jv16 PowerTools
- Perform Windows services monitoring using Windows Service Manager (SrvMan)
- Perform startup program monitoring using Autoruns for Windows and WinPatrol

- Perform installation monitoring using Mirekusoft Install Monitor
- Perform files and folder monitoring using PA File Sight
- Perform device driver monitoring using DriverView and Driver Booster
- Perform DNS monitoring using DNSQuerySniffer

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- TCPView located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView**
- CurrPorts located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts**
- ProcessMonitor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor**
- Regshot located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\regshot**
- jv16 PowerTools located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\jv16 PowerTools**
- Windows Service Manager (SrvMan) located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\srvman-1.0**
- Autoruns for Windows located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows**
- WinPatrol located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**
- Mirekusoft Install Monitor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor**

- PA File Sight located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight**
- DriverView located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView**
- Driver Booster located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Booster**
- DNSQuerySniffer located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Duration

Time: 85 Minutes

Overview of Dynamic Malware Analysis

Dynamic analysis is performed to gather valuable information about malware activity, including the files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified processes, and services the malware started, and other items.

You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network, and ensure that the testing system can recover to an earlier set timeframe (prior to launching the malware) in case anything goes wrong during the test.

To achieve this, you need to perform the following:

- **System Baselining**

  Baselining refers to the process of capturing a system's state (taking snapshot of the system) at the time the malware analysis begins. This can be used to compare the system's state after executing the malware file, which will help understand the changes that the malware has made across the system. A system baseline involves recording details of the file system, registry, open ports, network activity, and other items.

- **Host Integrity Monitoring**

  Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves using the same tools to take a snapshot of the

system before and after the incident or actions and analyzing the changes to evaluate the malware's impact on the system and its properties.

In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, and other characteristics.

Host integrity monitoring includes:

- Port monitoring
- Process monitoring
- Registry monitoring
- Windows services monitoring
- Startup program monitoring
- Event logs monitoring and analysis
- Installation monitoring
- Files and folder monitoring
- Device driver monitoring
- Network traffic monitoring and analysis
- DNS monitoring and resolution
- API calls monitoring

Lab Tasks

TASK 1 — Perform Port Monitoring using TCPView and CurrPorts

Note: This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine and find that the process associated with the server is running on it.

TASK 1.1

Create a Server and Execute it on Remote Machine

1. Turn on the **Windows 10** and **Windows Server 2016** victim machines.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe** to launch njRAT.
4. Create a server and save it to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.

5. While building the server, assign the server name **Trojan.exe** for demonstration purposes.

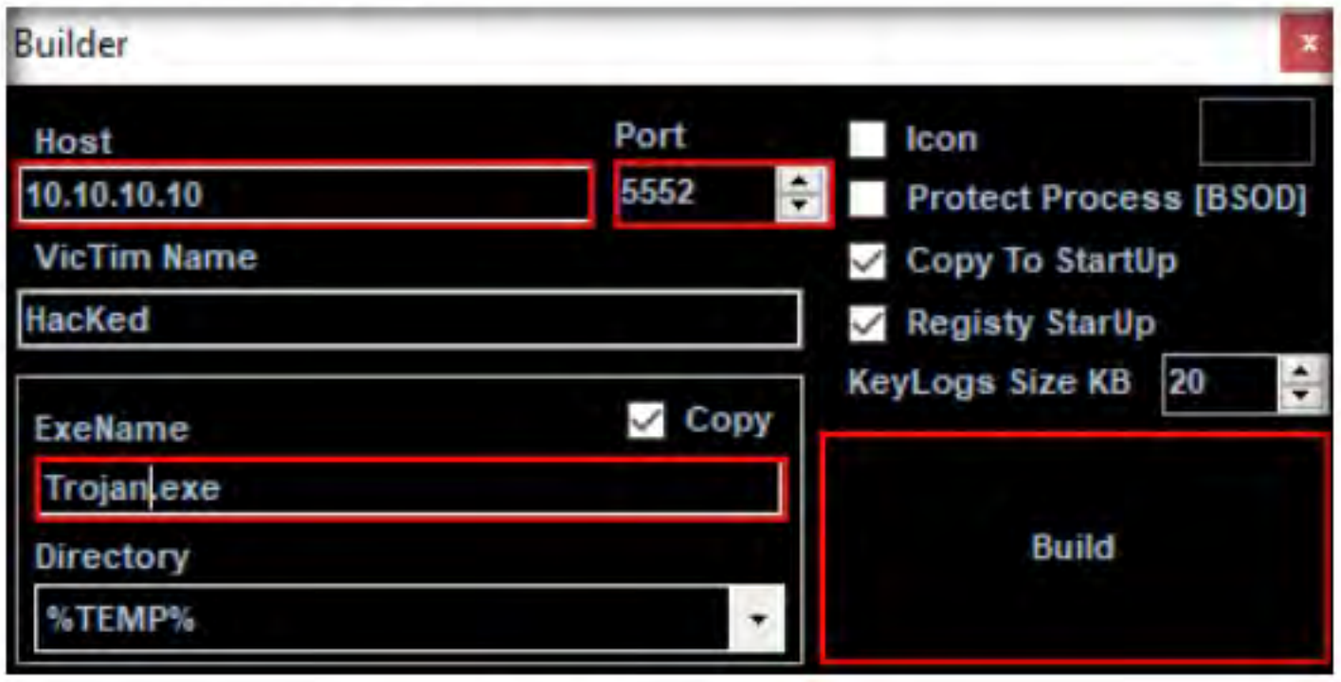


Figure 4.1.1: Building a Server

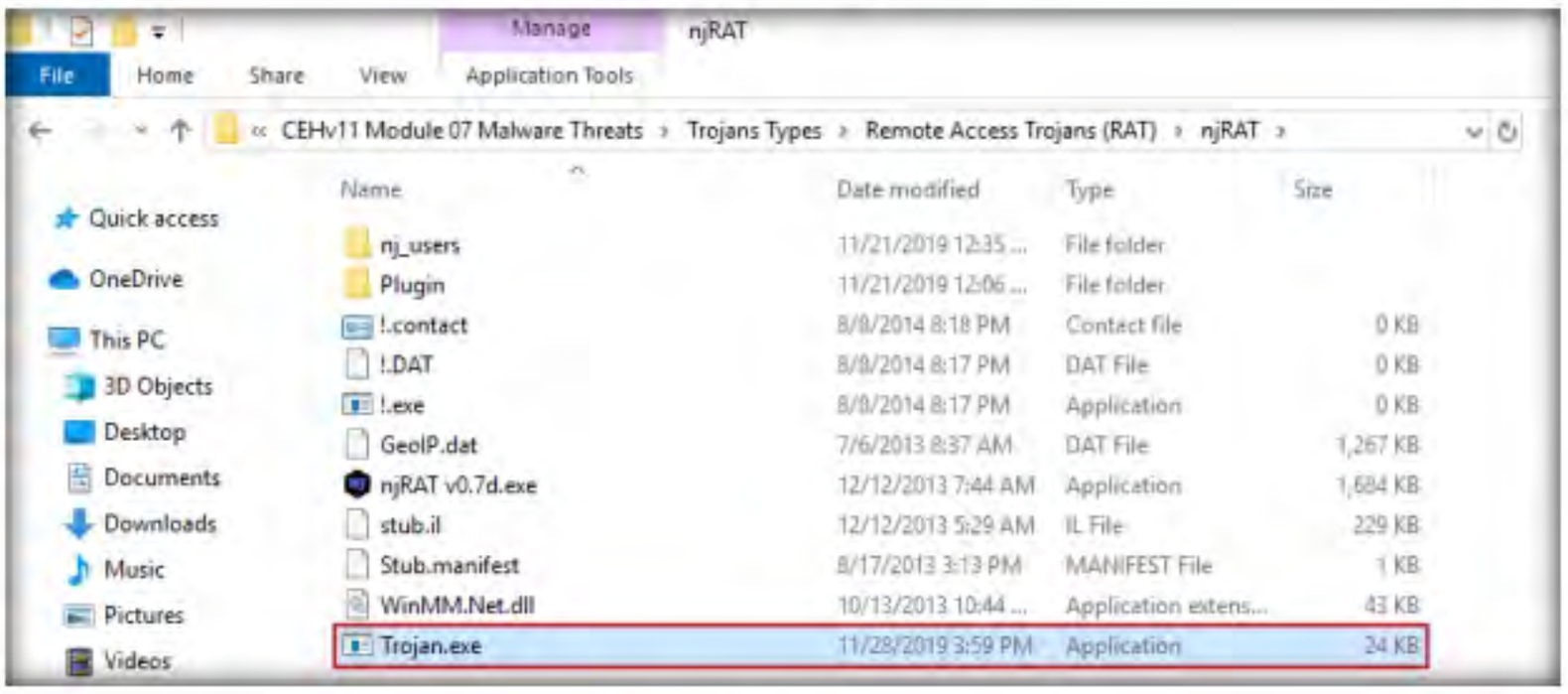


Figure 4.1.2: Server Built

6. Switch to the **Windows Server 2016** virtual machine and log in using the credentials **Administrator** and **Pa$$w0rd**.

7. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.

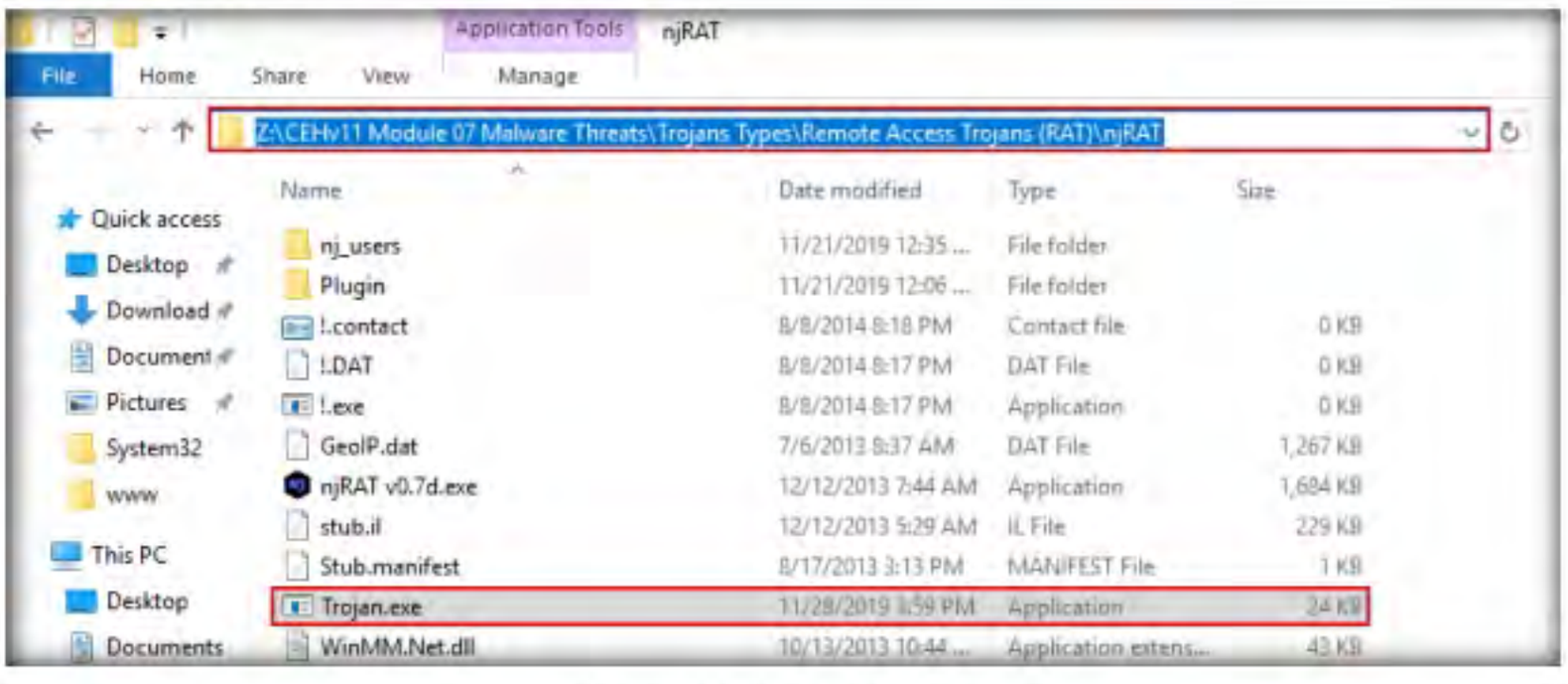


Figure 4.1.3: Sharing the Server

We know that the Internet uses a software protocol named TCP/IP to format and transfer data. Malware programs corrupt the system and open system input and output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also act as backdoors or communication channels for other types of harmful malware and programs. They open unused ports on the victim's machine to connect back to the malware handlers. You can identify the malware trying to access a particular port by installing port monitoring tools such as TCPView and CurrPorts.

8. Observe that a connection has been established by the njRAT client running on the **Windows 10** virtual machine.

Figure 4.1.4: Connection Established

TASK 1.2

Analyze the Processes Running on each Port using TCPView

9. Now, let us analyze this process on **Windows Server 2016** using **TCPView** tool. Switch back to the **Windows Server 2016** virtual machine.
10. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **Tcpview.exe** to launch the application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

11. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.
12. The **TCPView** main window appears, displaying the details such as Process, ProcessId, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State, as shown in the screenshot.

TCPView

TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

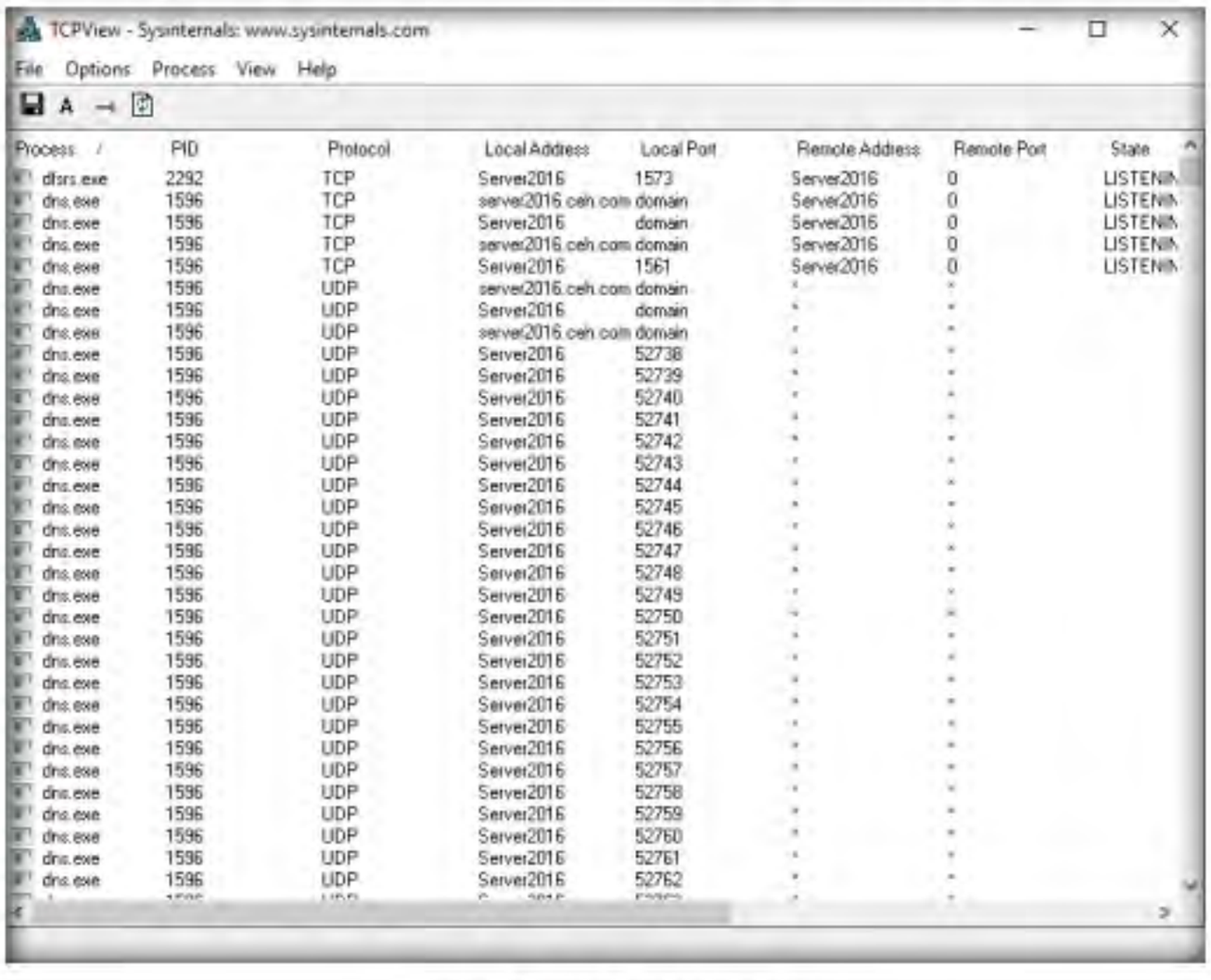


Figure 4.1.5: TCPView Main window

13. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.

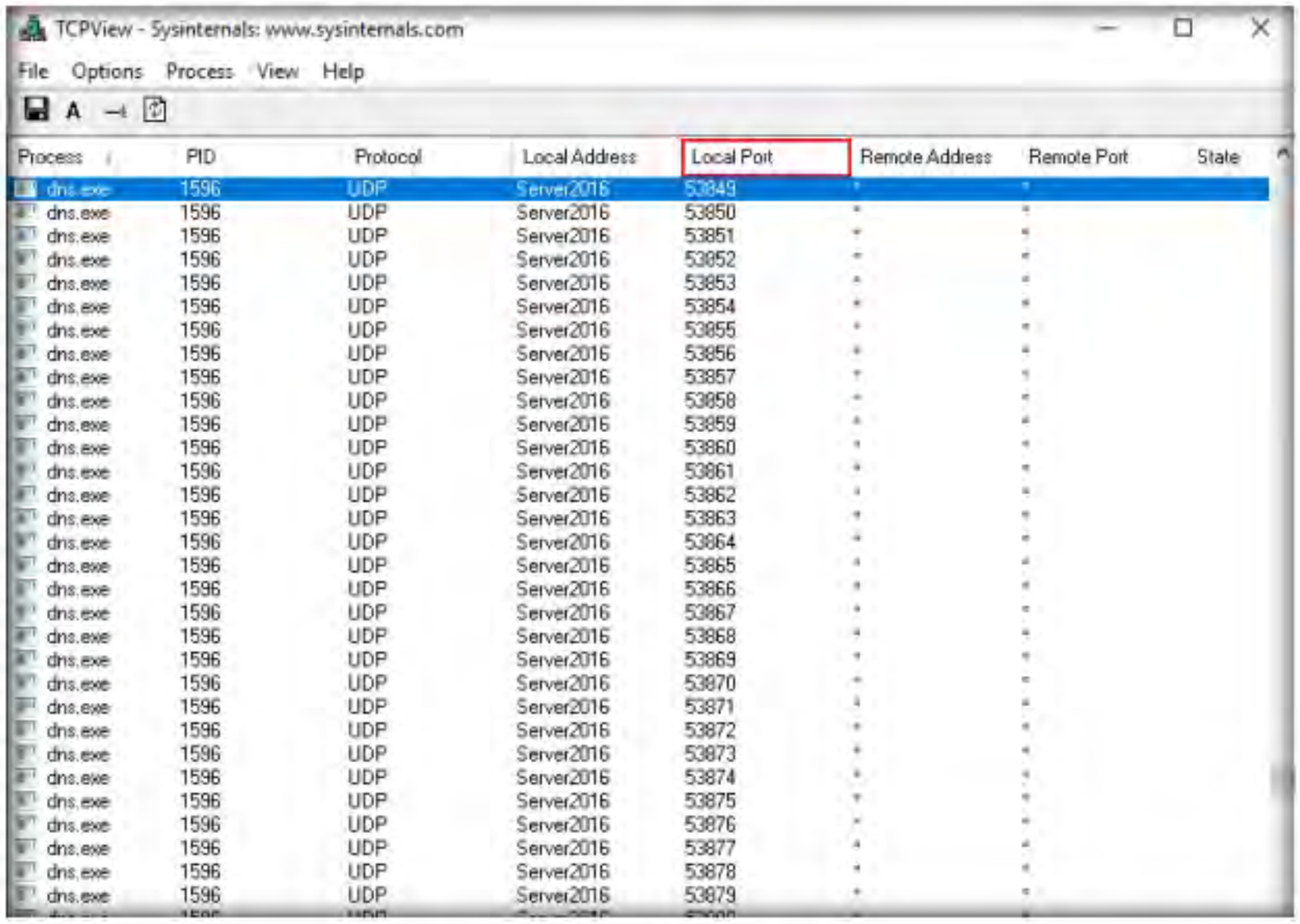


Figure 4.1.6: TCPView Analyzing Ports

14. Observe the protocols running on different ports under the **Protocol** column.

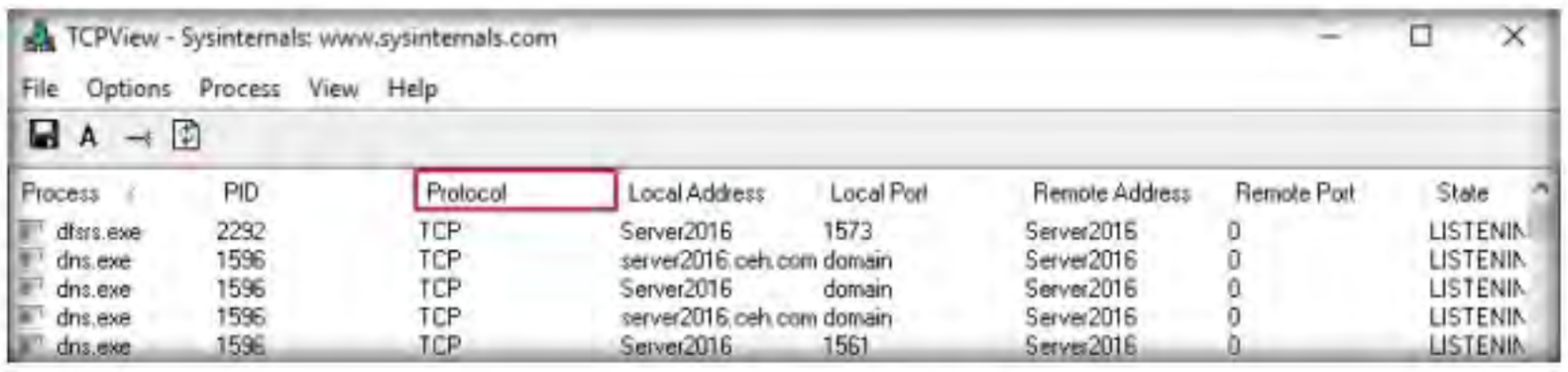


Figure 4.1.7: TCPView Analyzing Protocols

15. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.
16. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2016** machine. You can see details such as **Remote Address** and **Remote Port**.

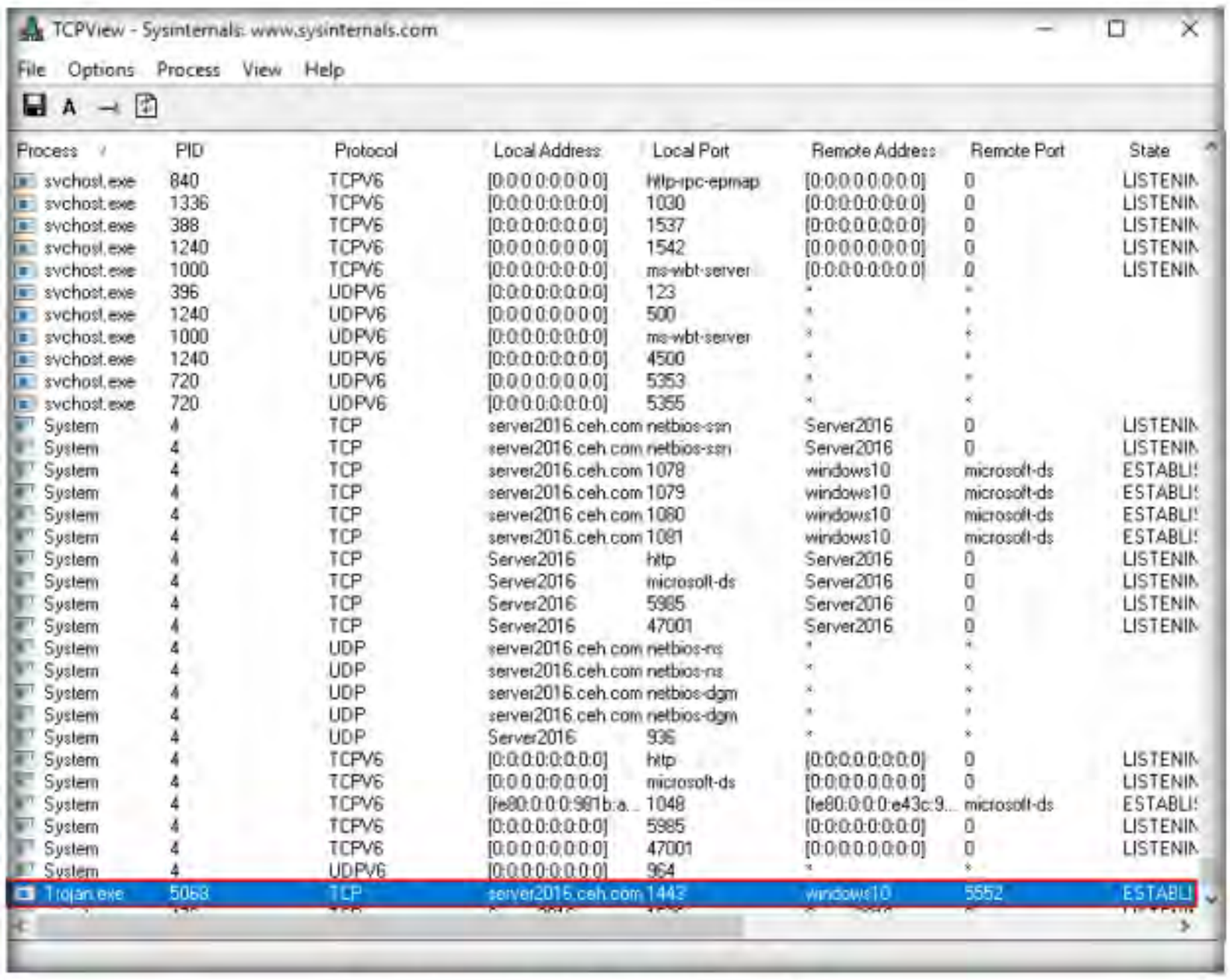


Figure 4.1.8: TCPView Looking for Malicious Application

17. To see the process properties, navigate to **Process**, and then click **Process Properties**.

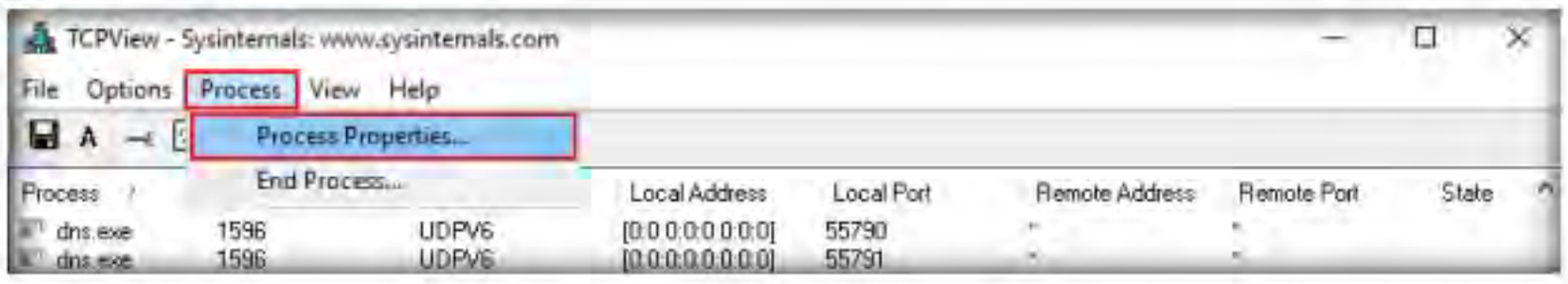


Figure 4.1.9: TCPView Process Properties

18. The properties for the selected process window appears (here, **Trojan.exe**); click **End Process** to kill the process. This will end the running process.

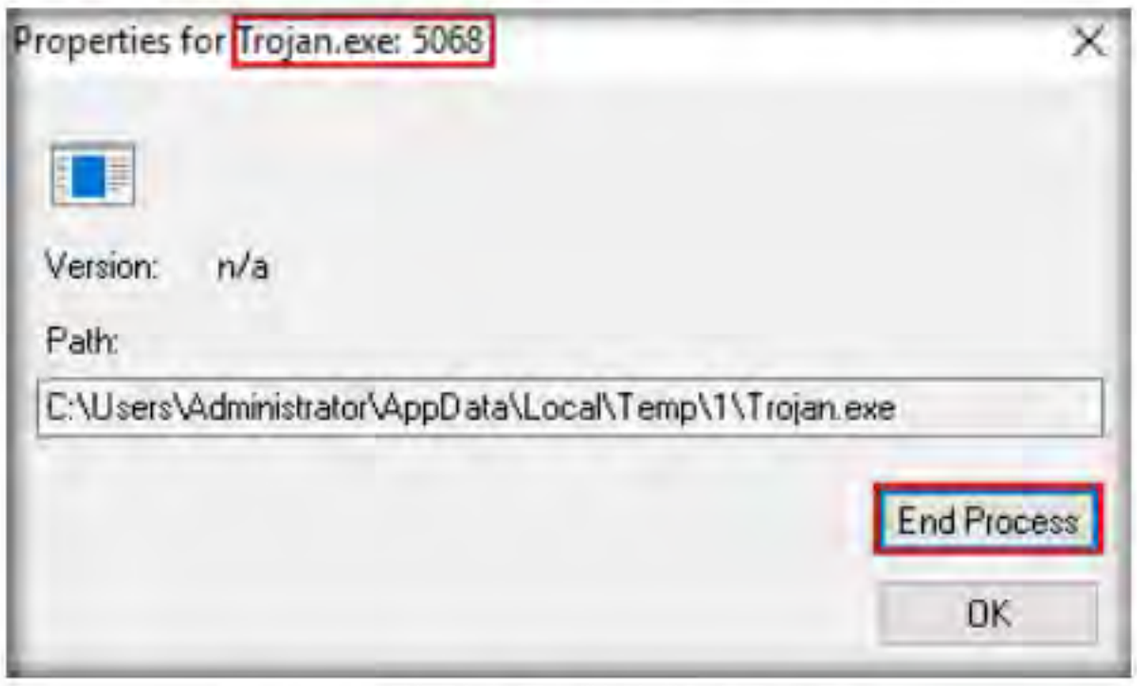


Figure 4.1.10: TCPView Properties of the Selected Process

19. Normally, if a **TCPView** dialog box appears, click **Yes** to terminate the process. However, for this lab, do not Kill the process in this step as we are going to use this running process for the next task; click **No**.

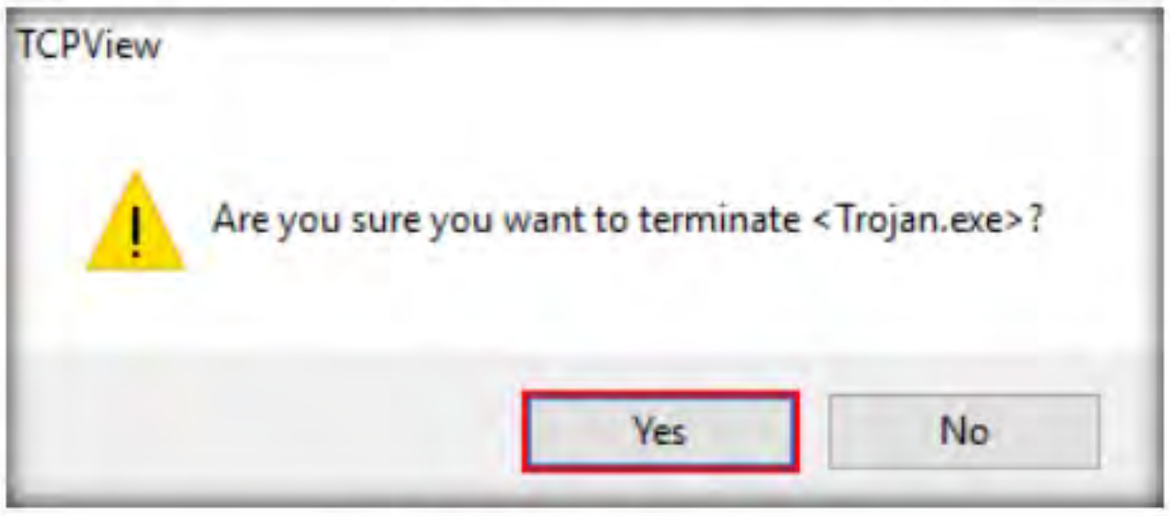


Figure 4.1.11: TCPView Killing Processes

20. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.
21. Close the **TCPView** window.

TASK 1.3

Examine the Malicious Processes Using CurrPorts

22. Now, let us analyze this process on **Windows Server 2016** using **CurrPorts**.
23. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.
24. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine. Here, you can observe the **Trojan.exe** process running on the machine, as the shown in the screenshot.

CurrPorts

CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.

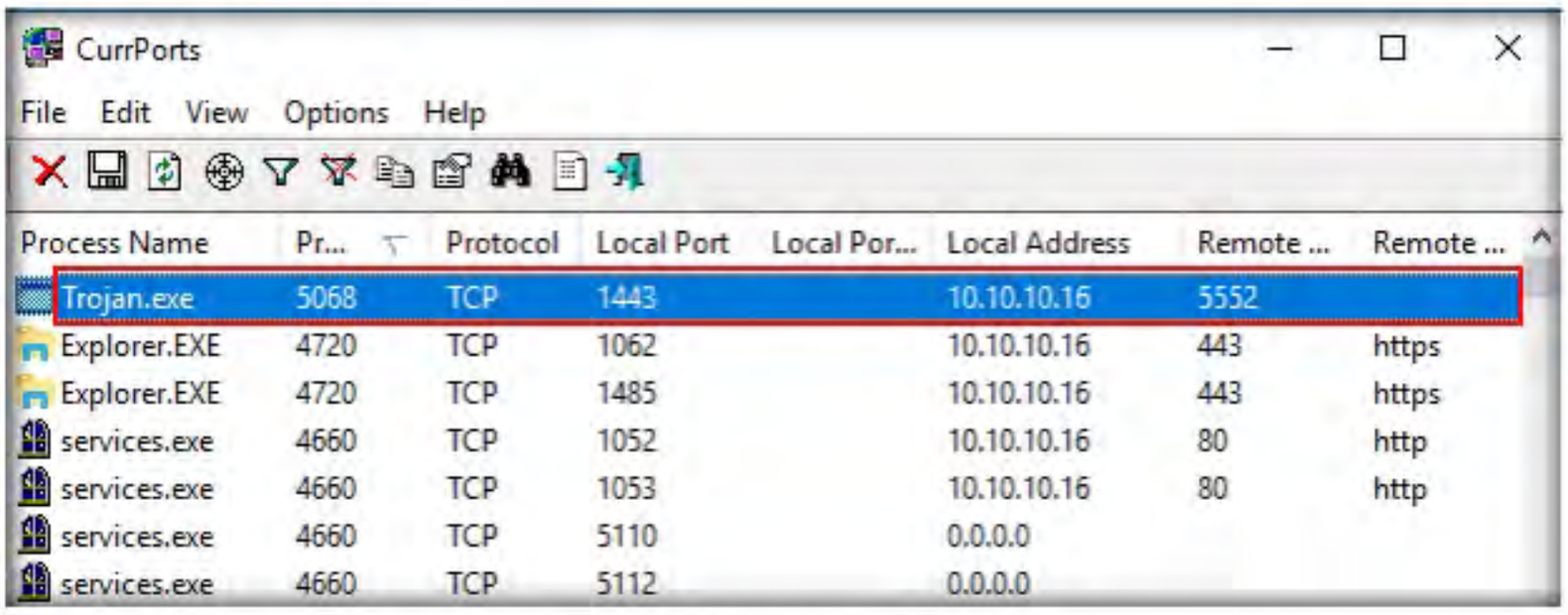


Figure 4.1.12: Viewing the Process

25. It is evident from the above screenshot that the process is connected to the machine on **port 5552**.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

26. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.

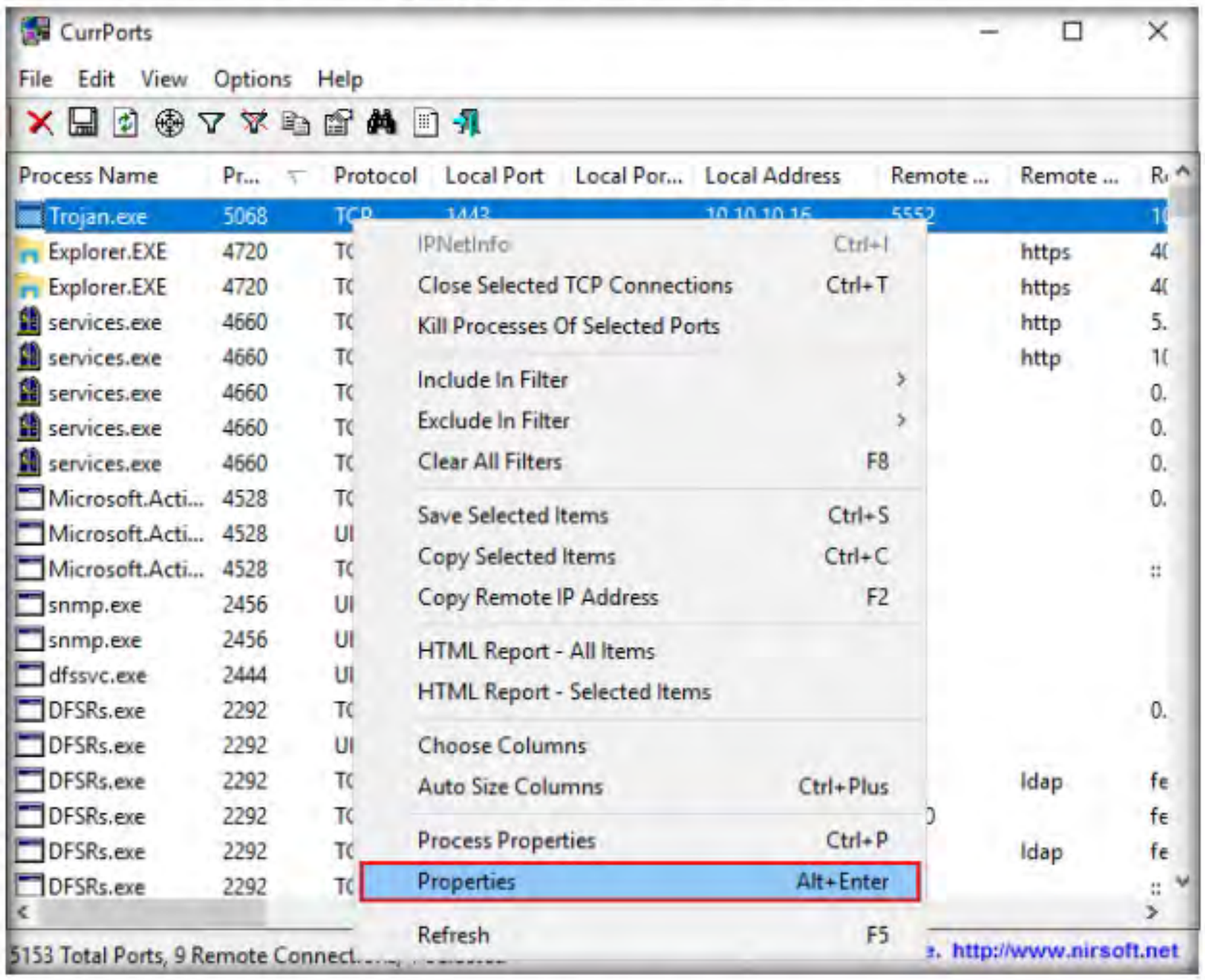


Figure 4.1.13: Viewing the Properties

27. The **Properties** window appears, displaying information related to the process such as the name of the process, its process ID, Remote Address, Process Path, Remote Host Name, and other details.
28. Once you are done examining the properties associated with the process, click **OK**.

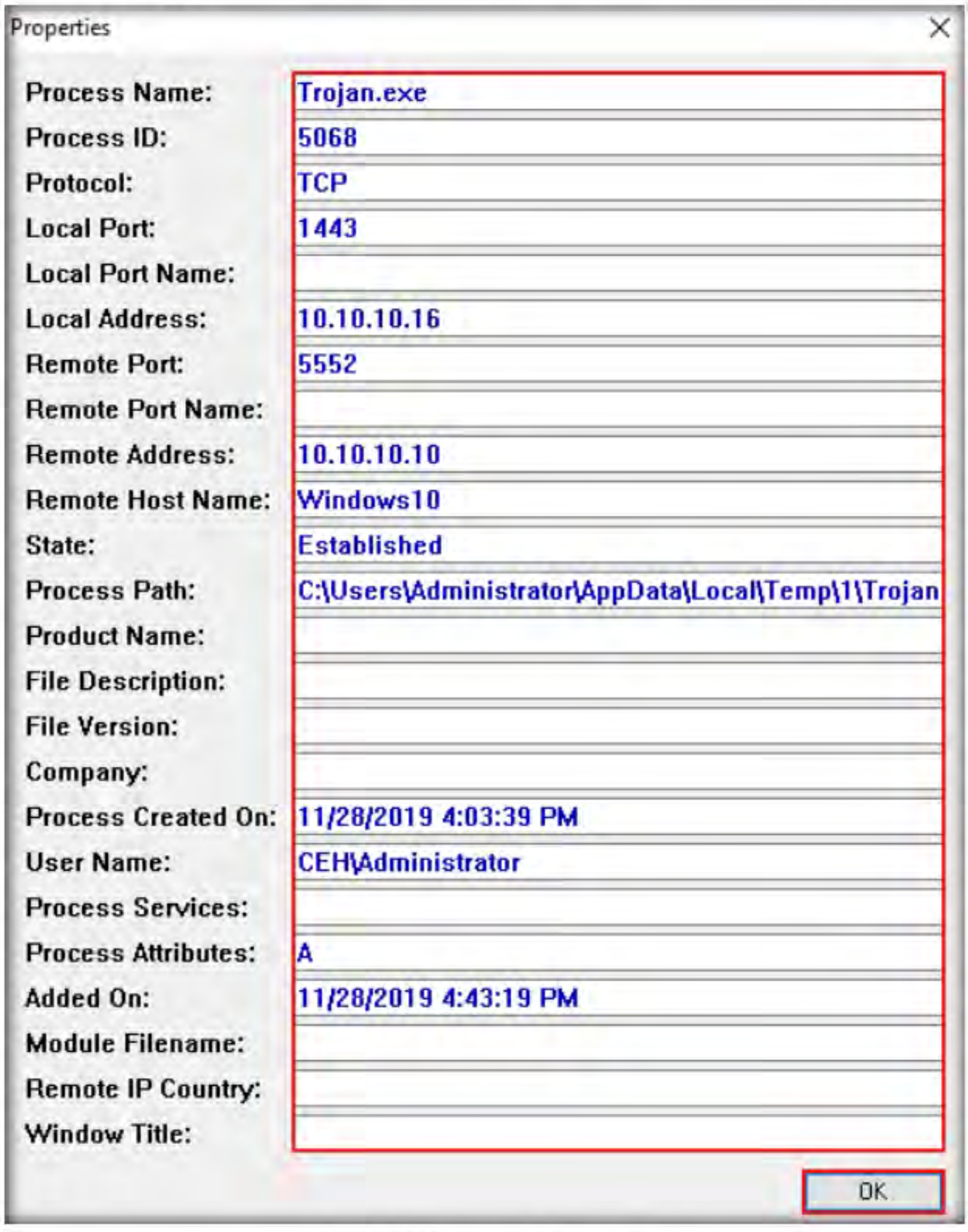


Figure 4.1.14: Examining the Properties

TASK 1.4

Kill the Malicious Process

29. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it and selecting **Kill Processes Of Selected Ports** from the context menu.

30. Alternatively, you may select **Close Selected TCP Connections**, so that the port closes, and the attacker can never regain connection through the port unless you open it.

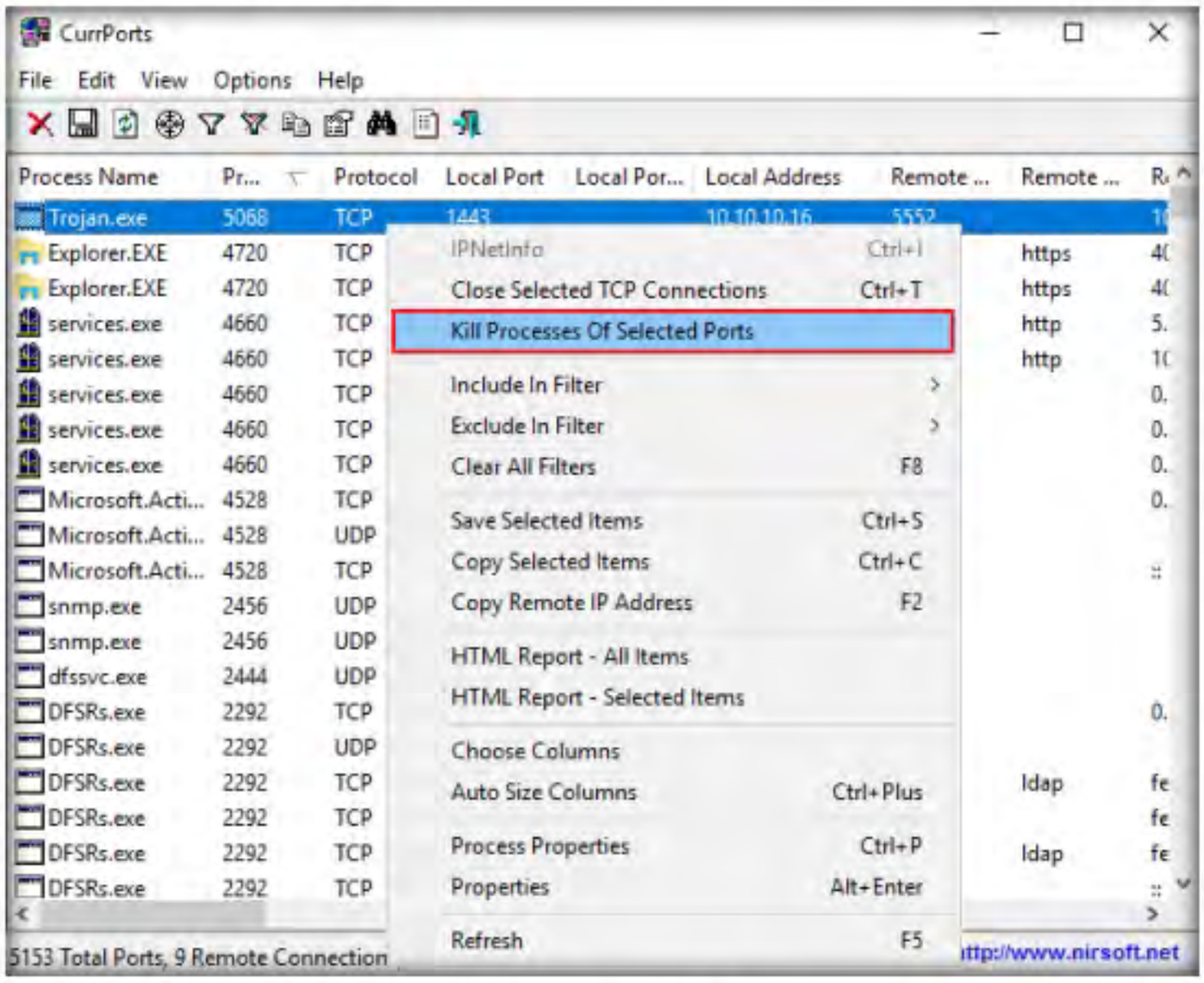


Figure 4.1.15: Killing the Process

You can also use other port monitoring tools such as **Port Monitor** (https://www.port-monitor.com), **CurrPorts** (https://www.nirsoft.net), **TCP Port Monitoring** (https://www.dotcom-monitor.com), or **PortExpert** (http://www.kcsoftwares.com) to perform port monitoring.

31. Normally, when the **CurrPorts** dialog-box appears, you would click **Yes** to close the connection. However, do not Kill the process at this step, as this running process will be used for the next task; click **No**.

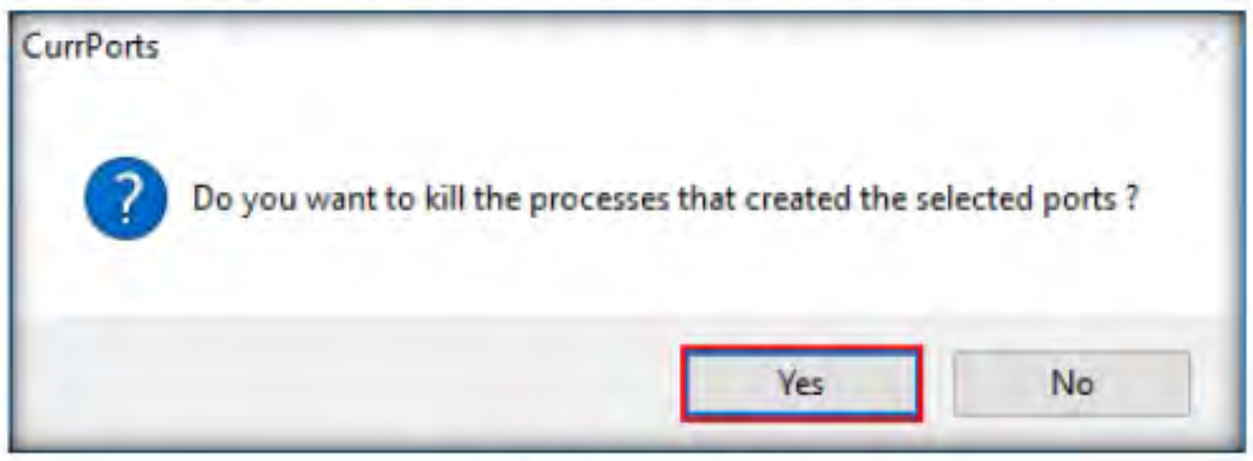


Figure 4.1.16: Killing the Process

32. This way, you can analyze the ports open on a machine and the processes running on it.
33. If a process is found to be suspicious, you may either kill the process or close the port.
34. Close all open windows.

TASK 2

Perform Process Monitoring using Process Monitor

Here, we will use the Process Monitor tool to detect suspicious processes.

TASK 2.1

Launch Process Monitor and View the Result

1. On the **Windows Server 2016** virtual machine, navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor** and double-click **Procmon.exe** to launch the Process Monitor tool.
2. The **Process Monitor License Agreement** window appears; click **Agree**.
3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.

Process monitoring will help in understanding the processes that malware initiates and takes over after execution. You should also observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes that malware starts.

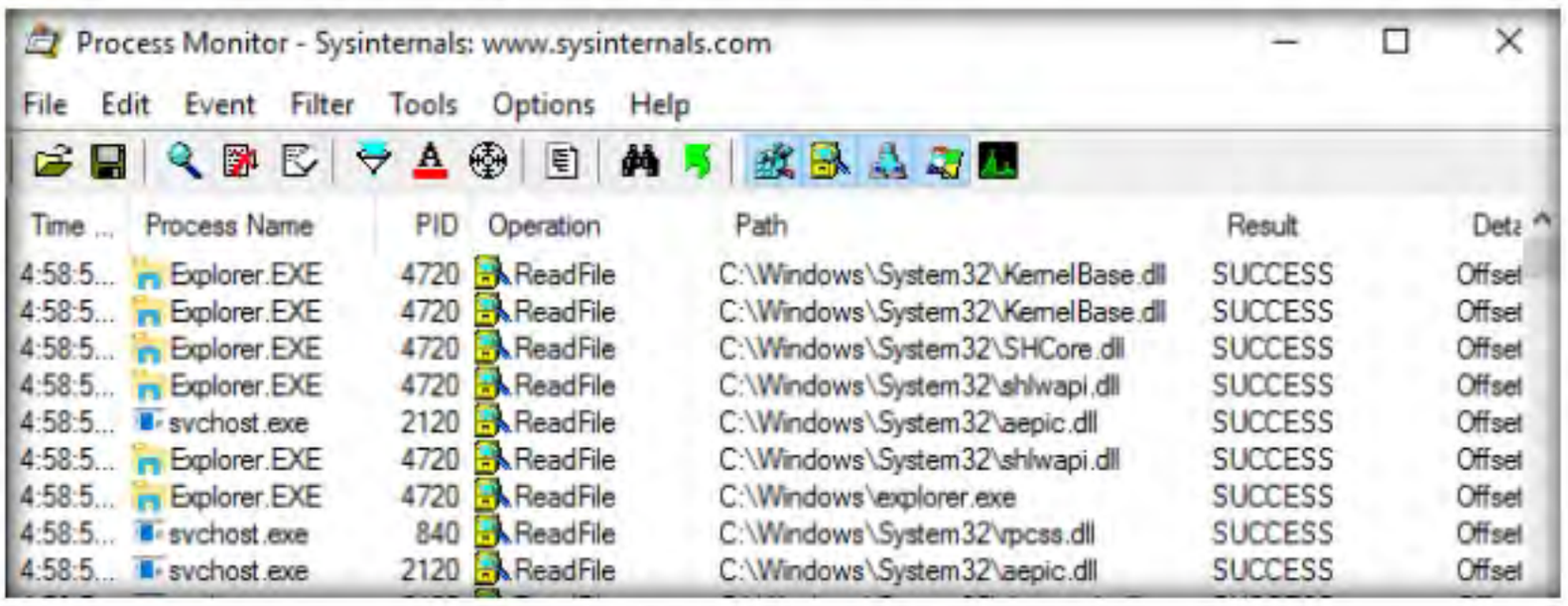


Figure 4.2.1: Process Monitor Main Window

4. Look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.
5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.

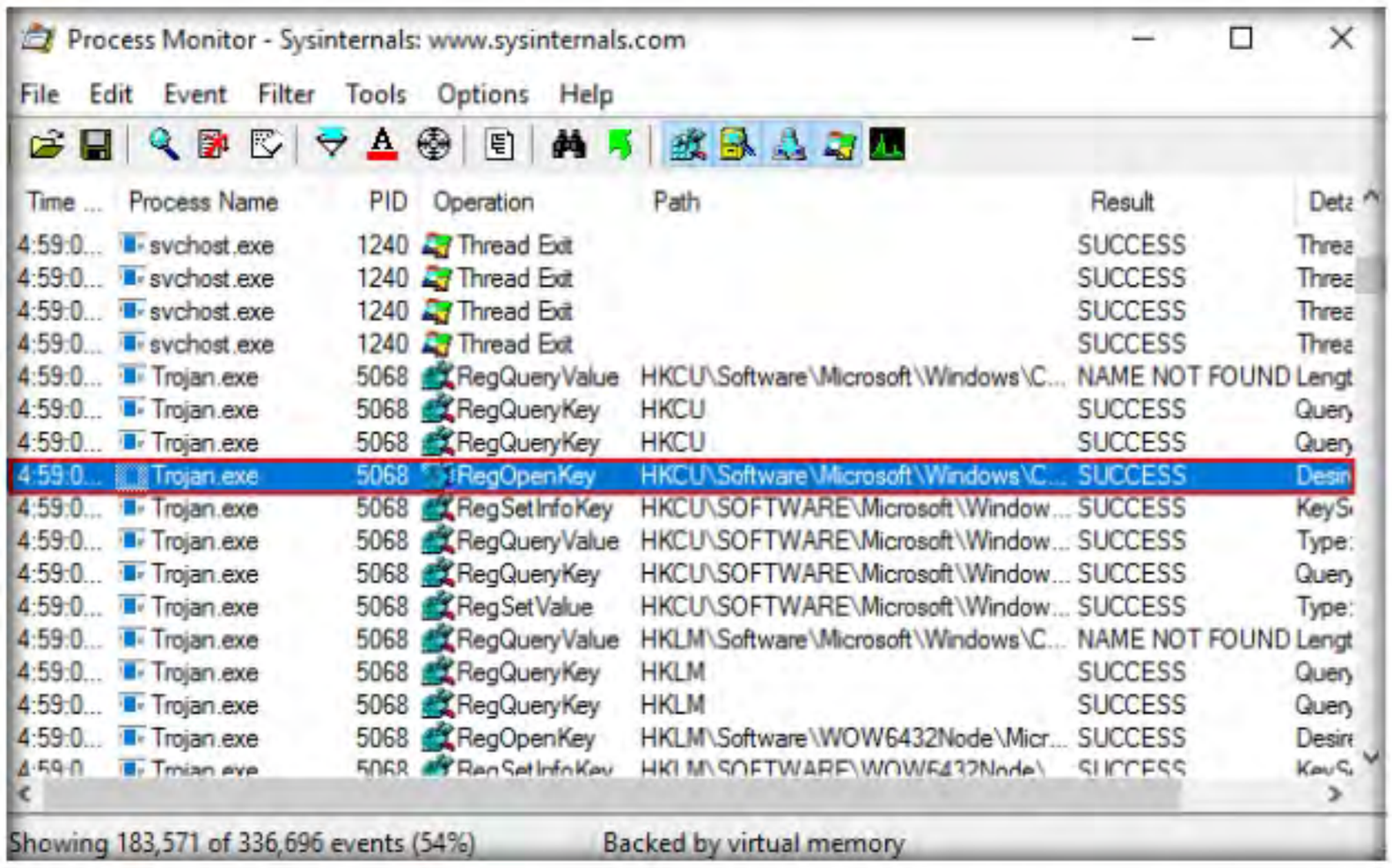


Figure 4.2.2: Process Monitor Running Malicious Process

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

6. To view the properties of a running process, select the process (here, **Trojan.exe**), navigate to **Event**, and click **Properties** from the menu.

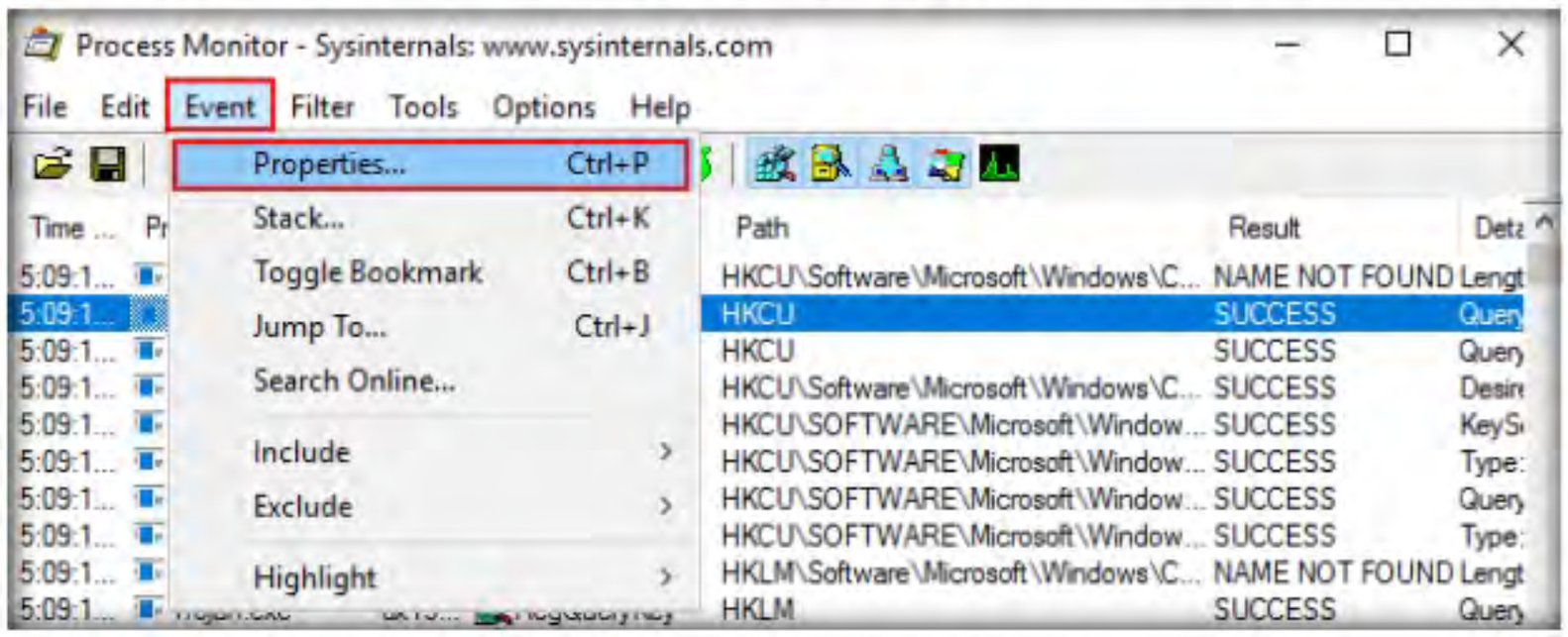


Figure 4.2.3: Process Monitor Viewing Properties

7. The **Event Properties** window appears with the details of the chosen process.
8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.

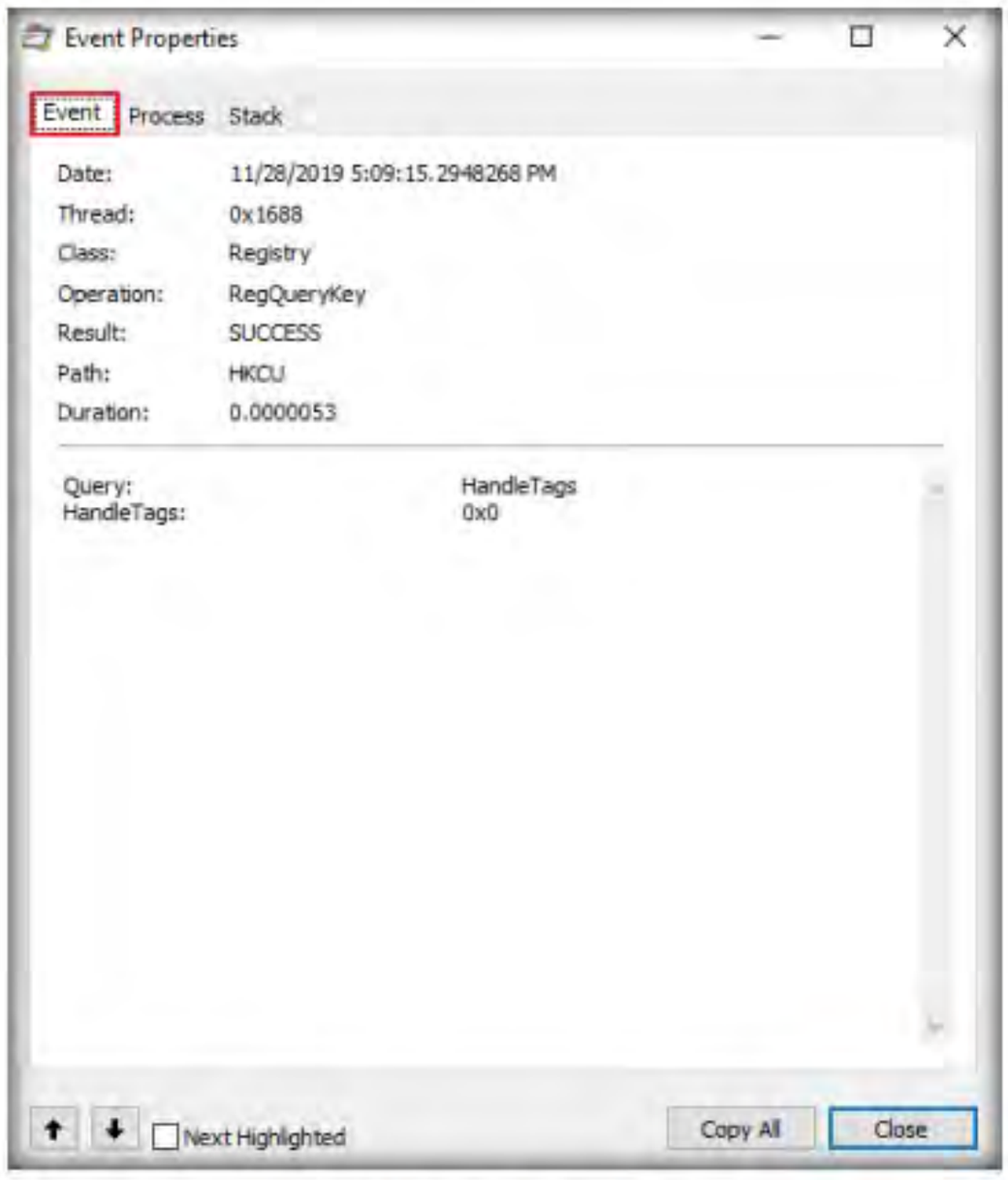


Figure 4.2.4: Process Monitor Event Tab

9. Once the analysis is complete, click the **Process** tab.
10. The **Process** tab shows the complete details of the process running, as shown in the screenshot.

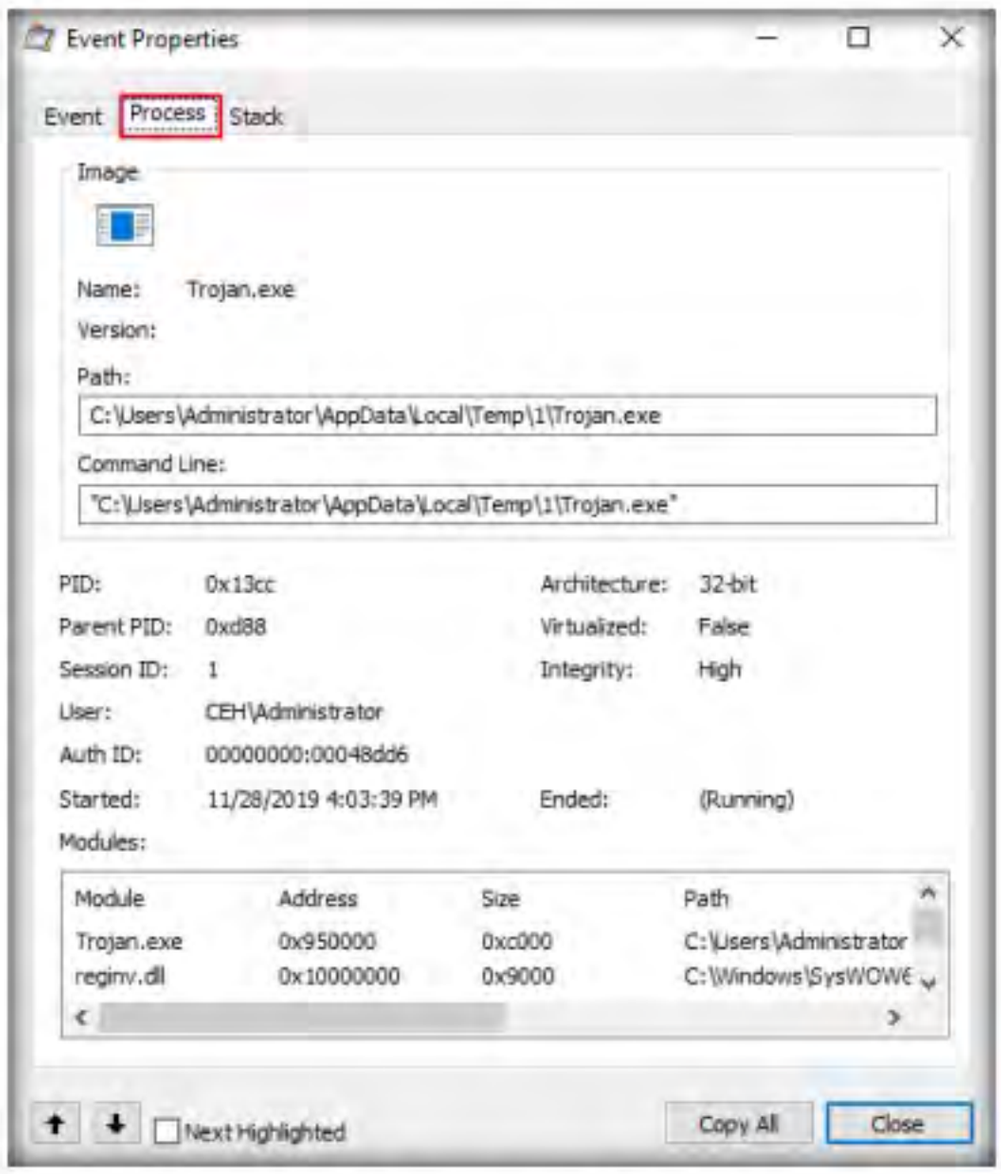


Figure 4.2.5: Process Monitor Process Tab

You can also use other process monitoring tools such as **Process Explorer** (https://docs.microsoft.com), **OpManager** (https://www.manageengine.com), **Monit** (https://mmonit.com), or **ESET SysInspector** (https://www.eset.com) to perform process monitoring.

11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.

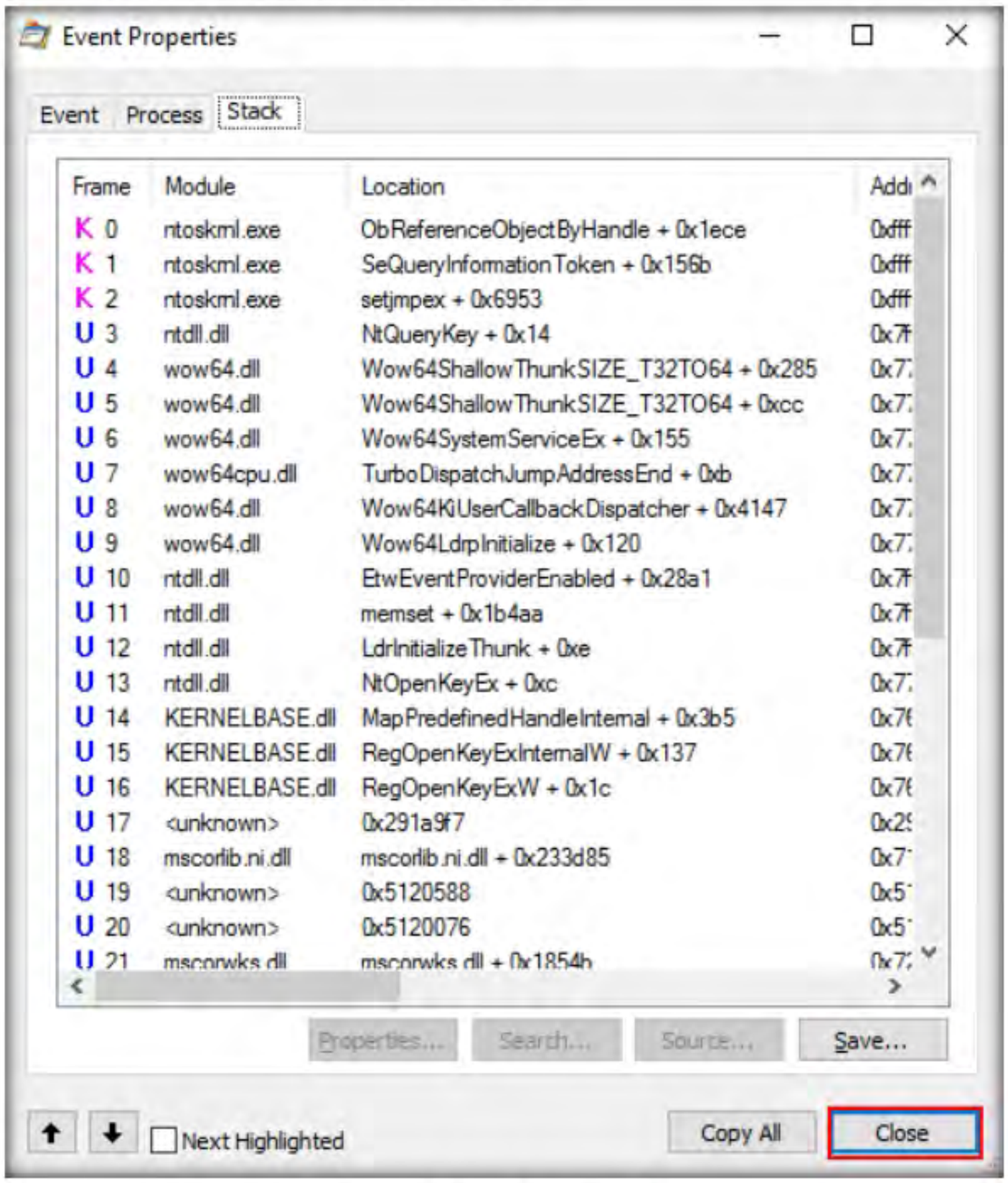


Figure 4.2.6: Process Monitor Stack Tab

12. This way, you can analyze the processes running on a machine.
13. If a process is found to be suspicious, you may either kill the process or close the port.
14. Close all windows on the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 3 Perform Registry Monitoring using Regshot and jv16 PowerTools

Here, we will use the registry monitoring tools Regshot and jv16 PowerTools to scan the registry values for any suspicious entries that may indicate a malware infection.

TASK 3.1

Run Regshot as Admin

The Windows registry stores OS and program configuration details such as settings and options. If the malware is a program, the registry stores its functionality. When an attacker installs a type of malware on the victim's machine, it generates a registry entry. One must have a fair knowledge of the Windows registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. While most computer users generally do not do this, monitoring the registry entries is a great way to track any modifications made to your system.

1. Log in to the **Windows 10** machine and navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\regshot**. Right-click **Regshot-x86-Unicode.exe** and choose **Run as administrator** from the context menu, as shown in the screenshot.
2. If a **User Account Control** window appears, click **Yes**.

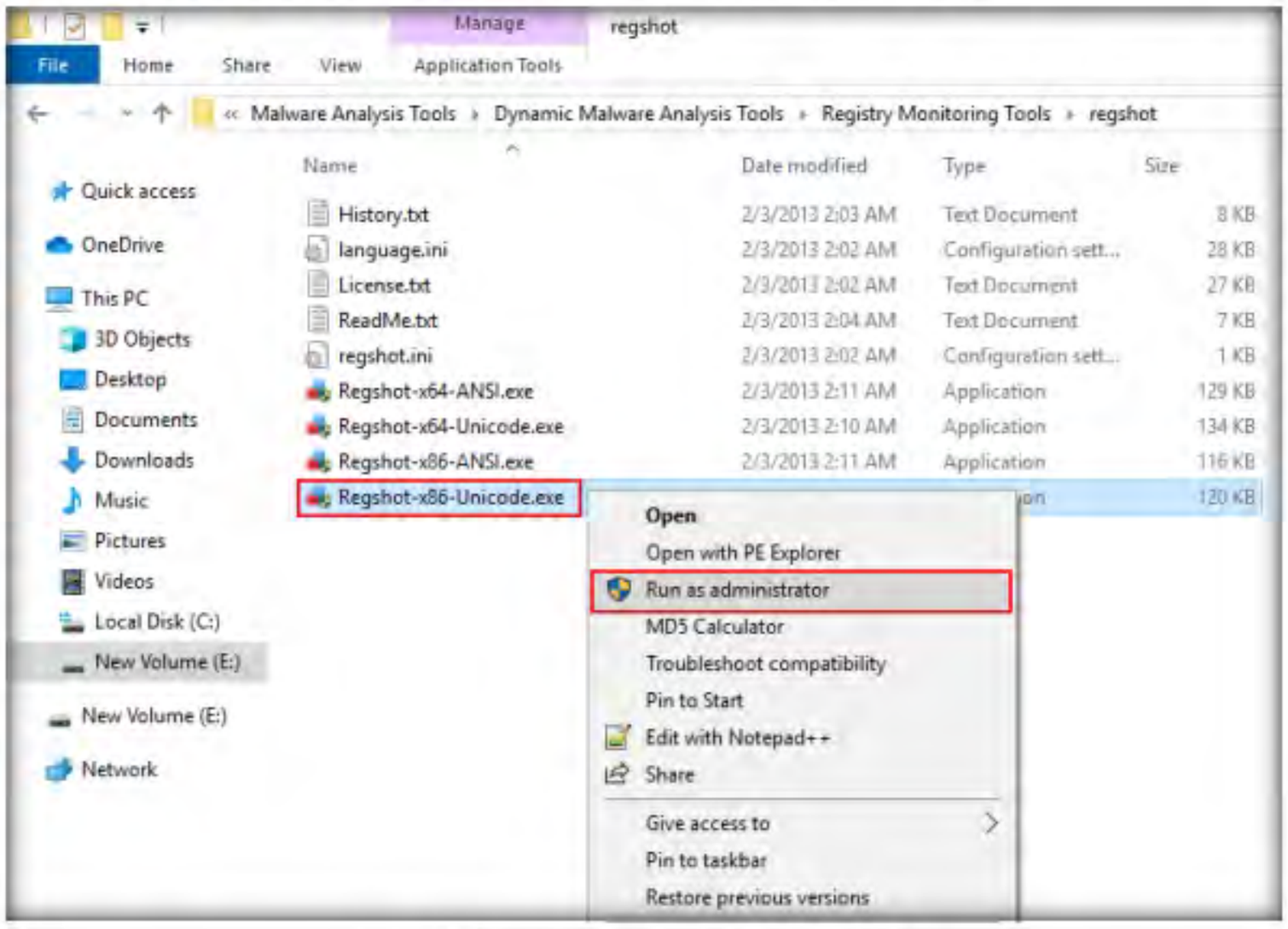


Figure 4.3.1: Launching Regshot in Administrator Mode

TASK 3.2

Take the 1st Registry Snapshot

Registry monitoring tools such as Regshot and jv16 PowerTools provide a simple way to perform the interesting task of tracking registry modifications, which proves to be useful in troubleshooting and monitoring background changes.

3. The **Regshot** application window opens, select the **HTML document** radio button, and in the **Output path** menu, click the **...** (...) button.

Figure 4.3.2: Taking Shot 1

Regshot

Regshot is a registry compare utility that helps to compare changes in registry entries after installing or uninstalling a program or manually modifying the registry. The purpose of this utility is to compare your registry at two separate points by taking a snapshot of the registry before and after any program or settings are added, removed, or otherwise modified.

4. The **Browse For Folder** window appears; choose **Desktop**, and then click **OK**, as shown in the screenshot.

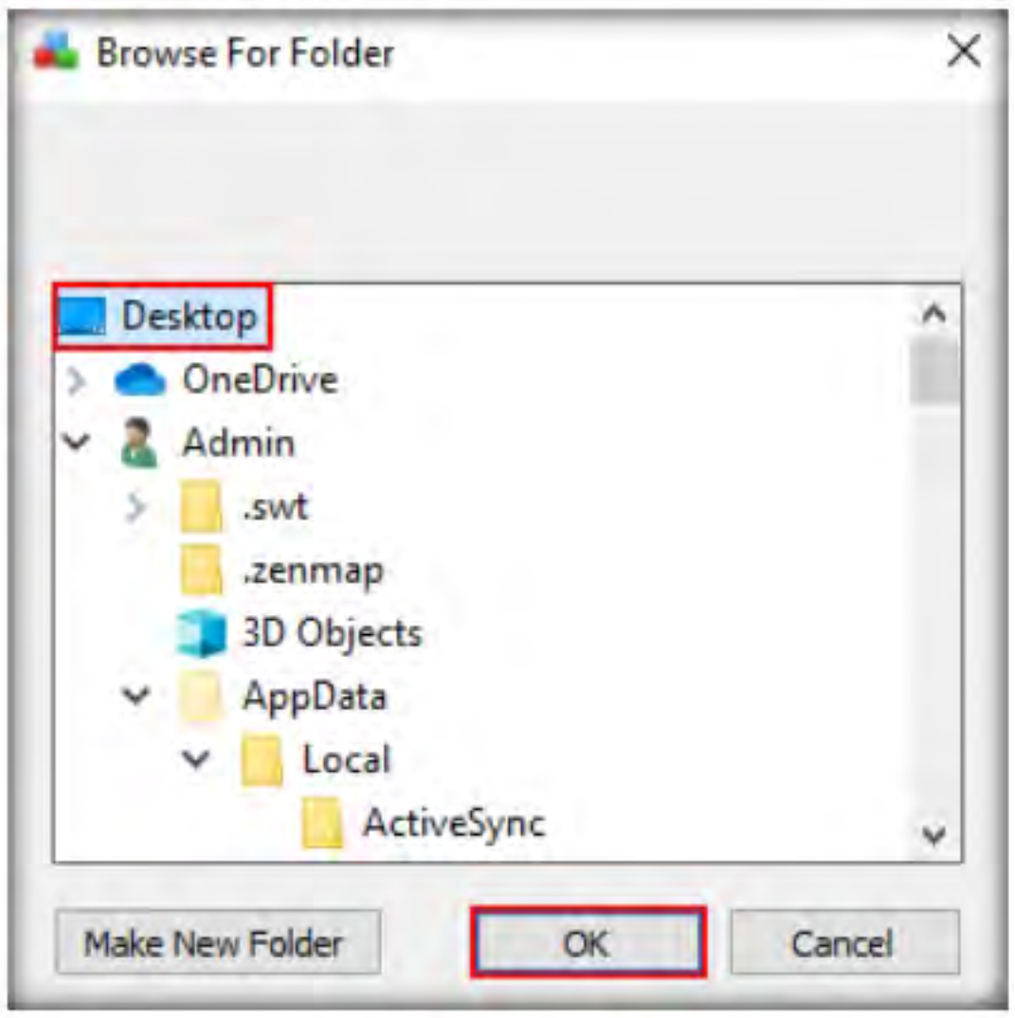


Figure 4.3.3: Browse For Folder

5. In Regshot's main window, click the **1st shot** button, as shown in the screenshot.

Figure 4.3.4: Save 1st Shot

6. A context menu appears; click **Shot and Save...**

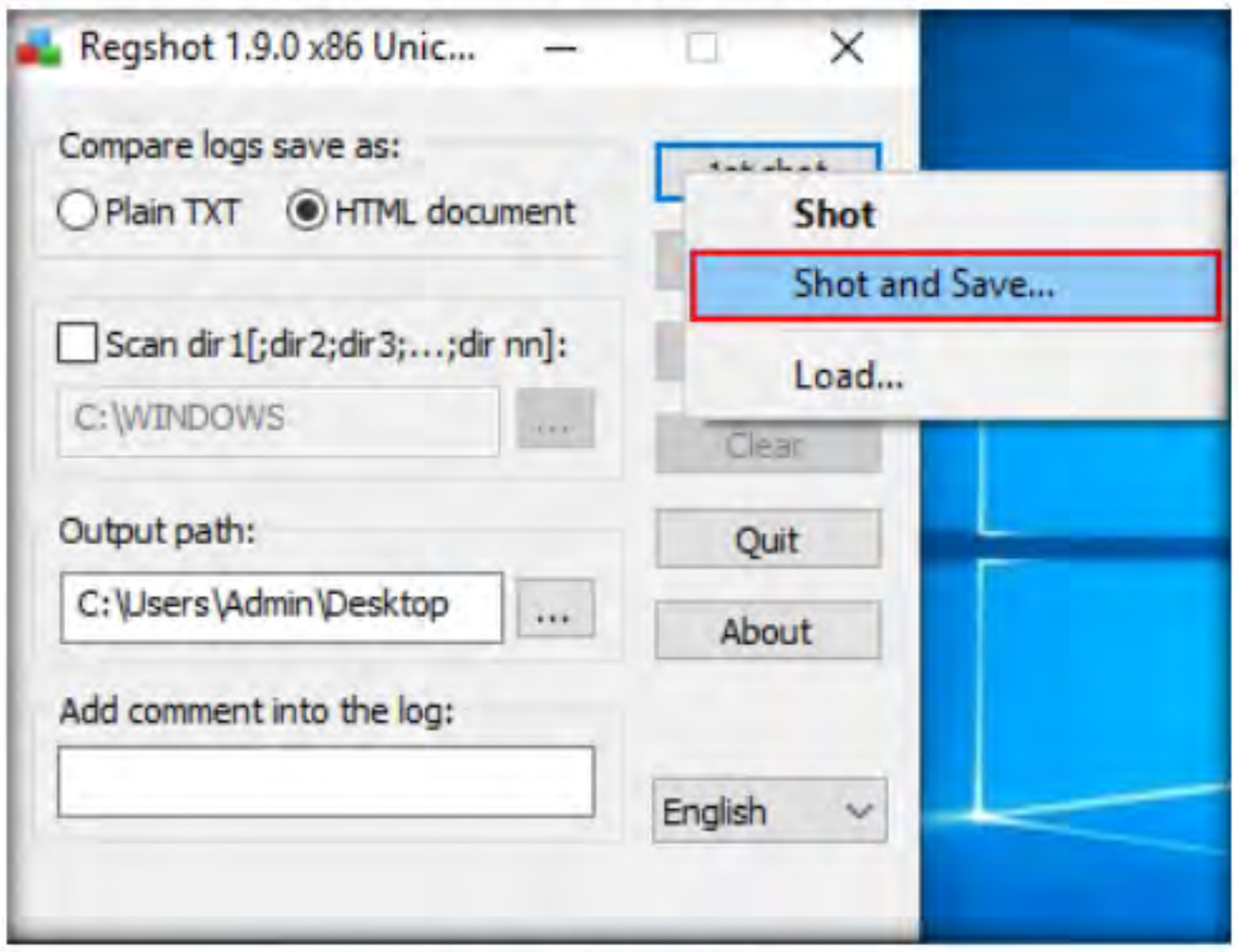


Figure 4.3.5: Saving 1st Shot

7. The **Save As** window appears; enter the file name (here **Shot 1**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

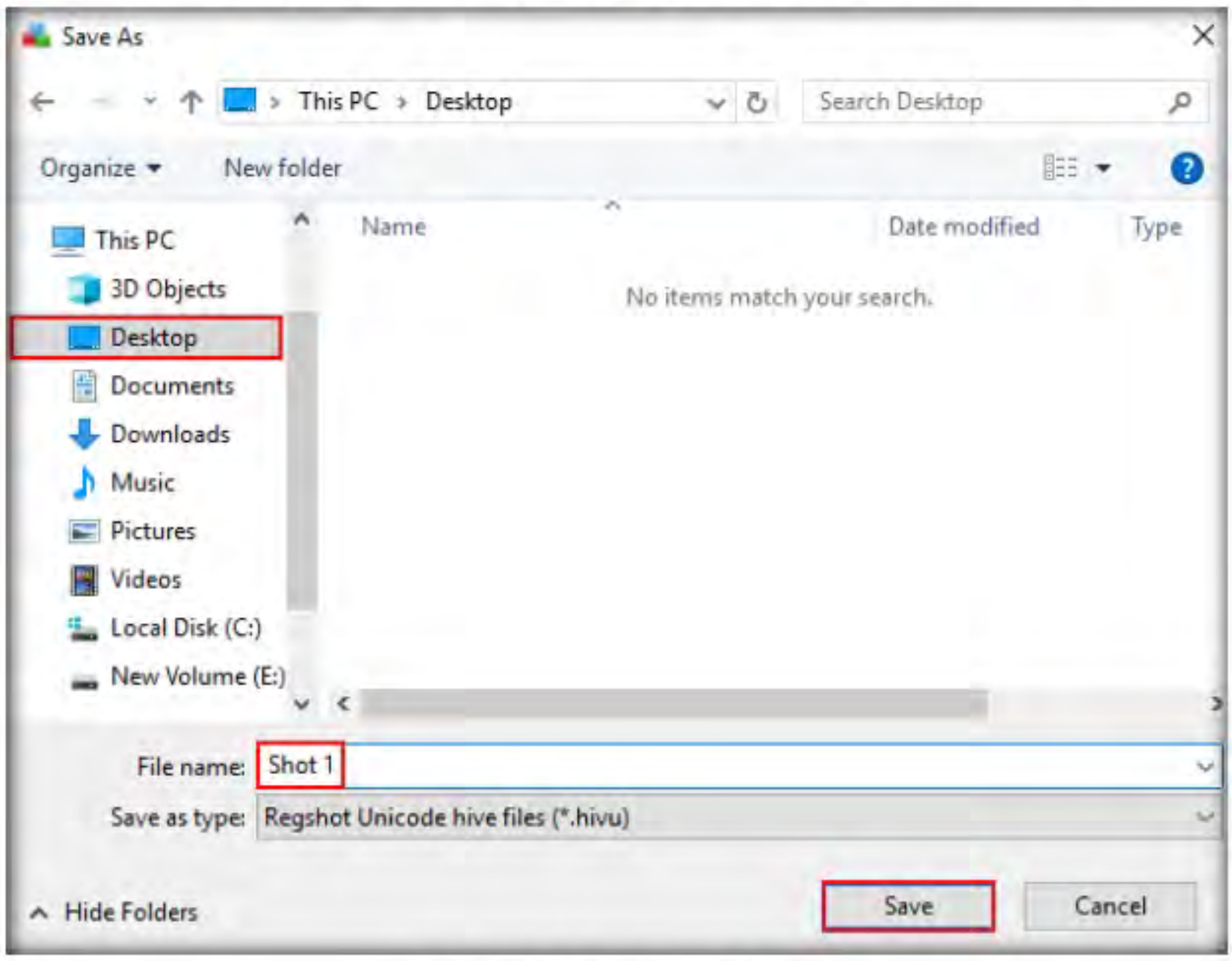


Figure 4.3.6: 1st Shot Saved on Desktop

TASK 3.3

Install/Uninstall an application

8. Now to demonstrate a change in the registry, install an application (here, **SoftPerfect Network Scanner**).
9. Navigate to **E:\CEH-Tools\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.
10. If a **User Account Control** window appears, click **Yes**.
11. Follow the wizard-driven installation steps to install the SoftPerfect Network Scanner.
12. Once the installation is complete, uncheck the **Launch SoftPerfect Network Scanner** option and click **Finish**.

Note: You can install any application to view the changes in the registry. For demonstration purposes, we have installed the SoftPerfect Network Scanner.

Figure 4.3.7: Installing an Application

TASK 3.4

Take the 2nd Registry Snapshot

13. Switch to the **Regshot** application window; leave all settings to default, and click **2nd shot**.
14. A context menu appears; click **Shot and Save...**, as shown in the screenshot.

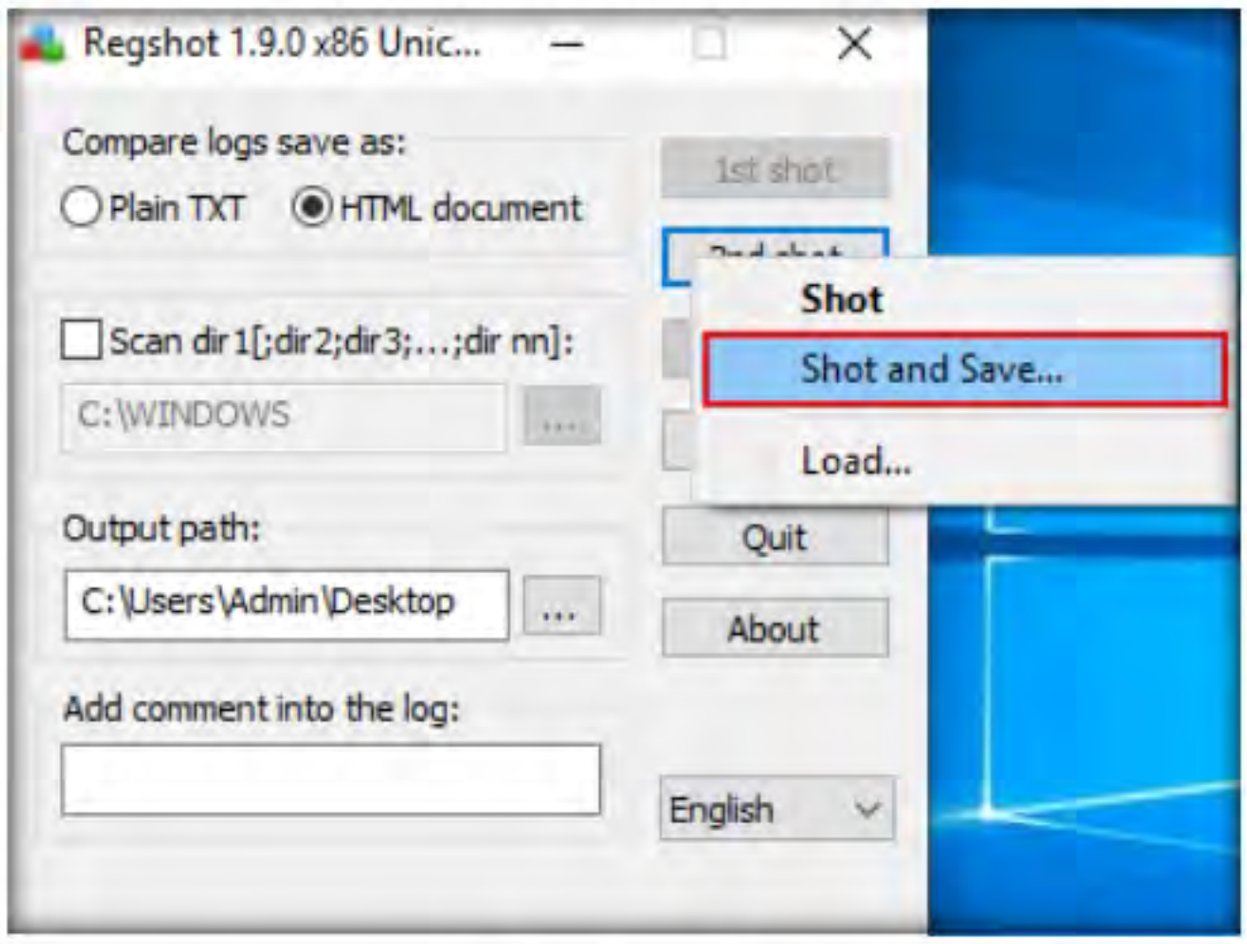


Figure 4.3.8: Taking 2nd Shot

15. The **Save As** window appears; enter the file name (here **Shot 2**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

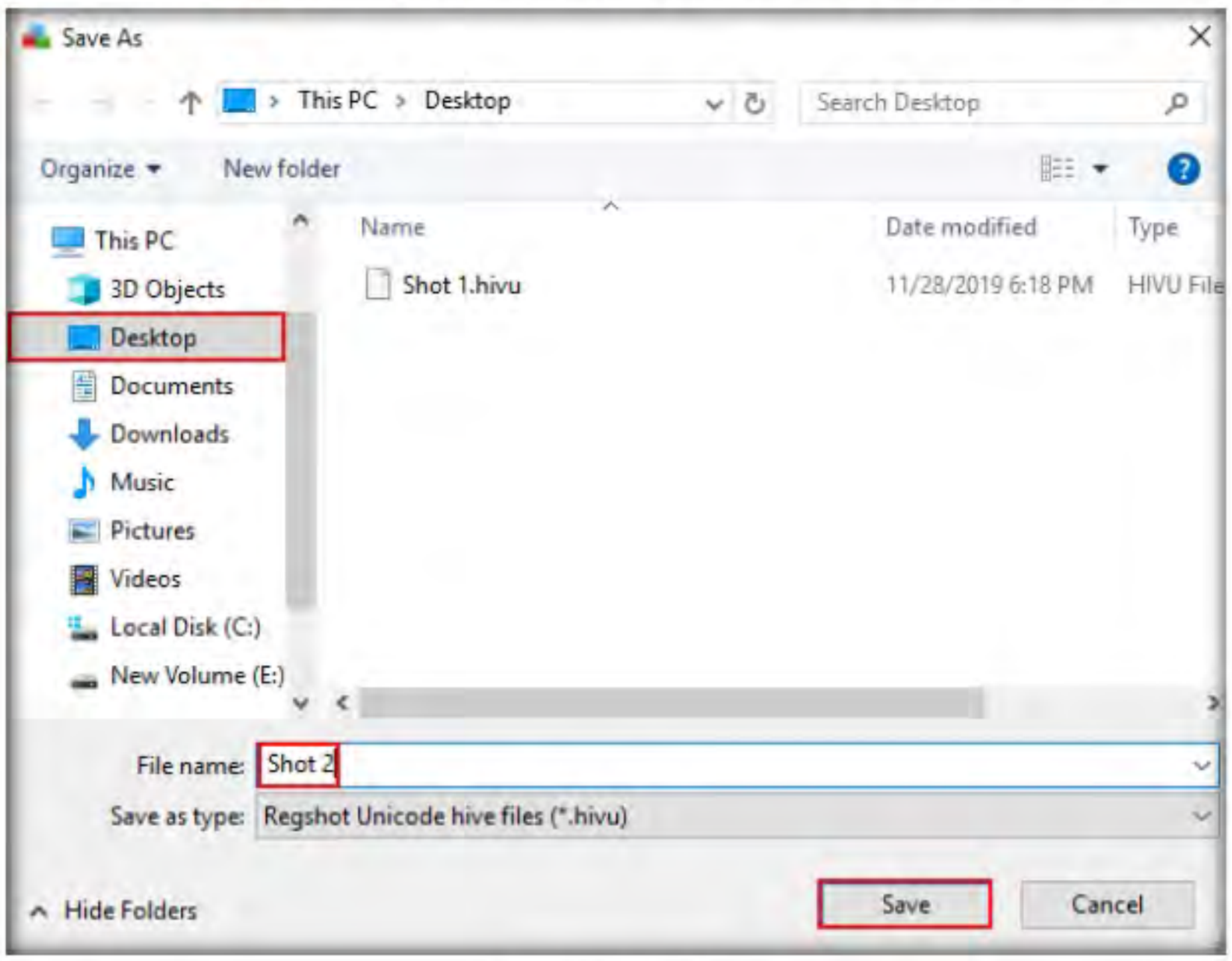


Figure 4.3.9: Saving 2nd Shot

TASK 3.5

Compare and Analyze the Results

16. Now, return to the **Regshot** application window and click **Compare**, as shown in the screenshot.

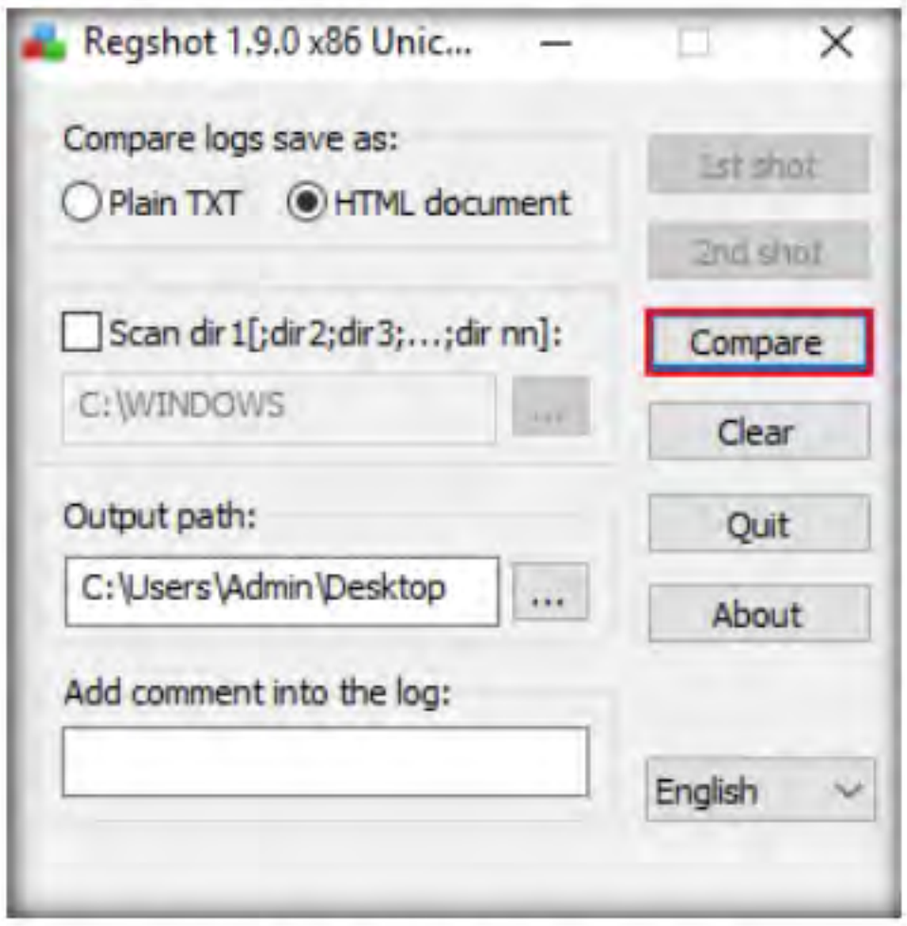


Figure 4.3.10: Comparing both 1st and 2nd Shot

17. The comparison of both shots opens in a default browser window (here, **Microsoft Edge**), as shown in the screenshot.

18. Observe the registry entries that have been modified by comparing the 1st and the 2nd shots, as shown in the screenshot.

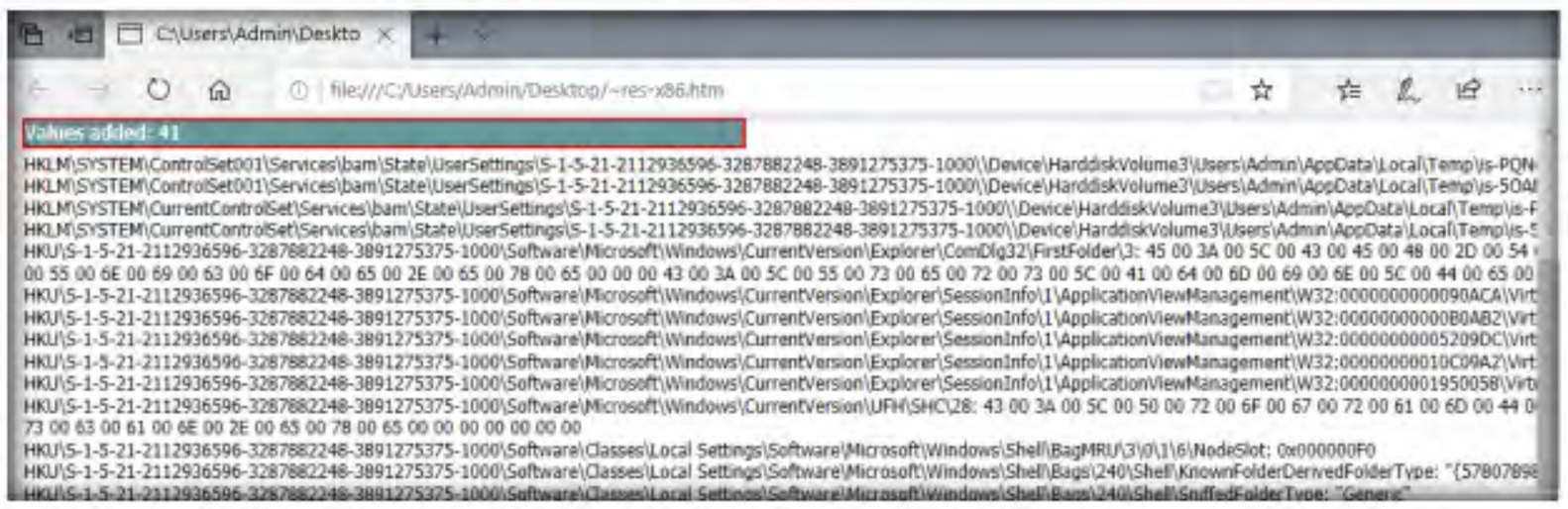


Figure 4.3.11: HTML report showing the changes made in the registry

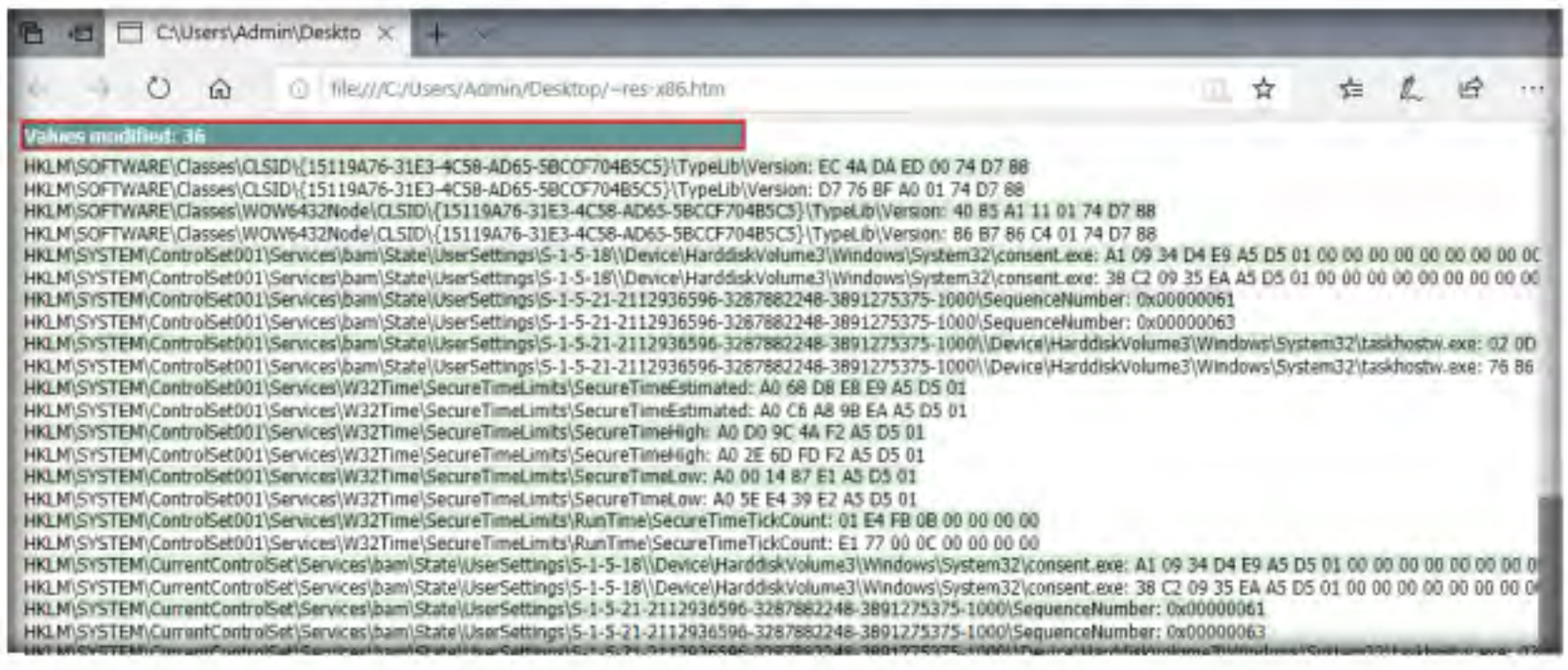


Figure 4.3.12: HTML report showing the changes made in the registry

19. By examining modified registry entries in the result, you can find any unwanted registry entries on the machine and stop or delete them manually.
20. Close all open windows on the **Windows 10** virtual machine.
21. Now, we will perform an intensive scan for unwanted resources using jv16 PowerTools.

TASK 3.6

Perform Intensive Scan for Unwanted Resources using jv16 PowerTools

22. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\jv16 PowerTools** and double-click **jv16pt_setup.exe**.
23. If the **User Account Control** window appears, click **Yes**.
24. Follow the wizard-driven installation steps to install jv16 Power Tools.
25. The **jv16 PowerTools Quick Tutorial** window appears; click **Next**.

Note: If the **jv16 PowerTools Quick Tutorial** window does not appear, then double-click the **jv16 PowerTools** short-cut icon on **Desktop** to launch the application.

jv16 PowerTools

jv16 PowerTools is a PC system utility software that works by cleaning out unneeded files and data, cleaning the Windows registry, automatically fixing system errors, and applying optimization to your system. It allows the user to scan and monitor the Registry.

Figure 4.3.13: jv16 PowerTools Quick Tutorial

Further, jv16 helps in detecting registry entries created by malware. The "Clean and Speedup My Computer" feature of the Registry Cleaner in jv16 PowerTools is a solution for fixing registry errors and system errors, cleaning registry leftovers, as well as managing unneeded files such as old log files and temporary files.

26. In the **Please select your language** wizard, choose a language (here, **English**) and click **Next**.
27. The **How long would you like your trial to be?** wizard appears; leave the fields blank and click **Next**.
28. In the next **How long would you like your trial to be?** wizard screen, leave the fields blank and click **Next**.
29. The **jv16 PowerTools** pop-up appears; click **No**.
30. The **A few tips to get you started** wizard appears; click **Next**.
31. The **Simple or full user interface** wizard appears; choose the **Show me all the features and options available** radio button, and then click **Next**.

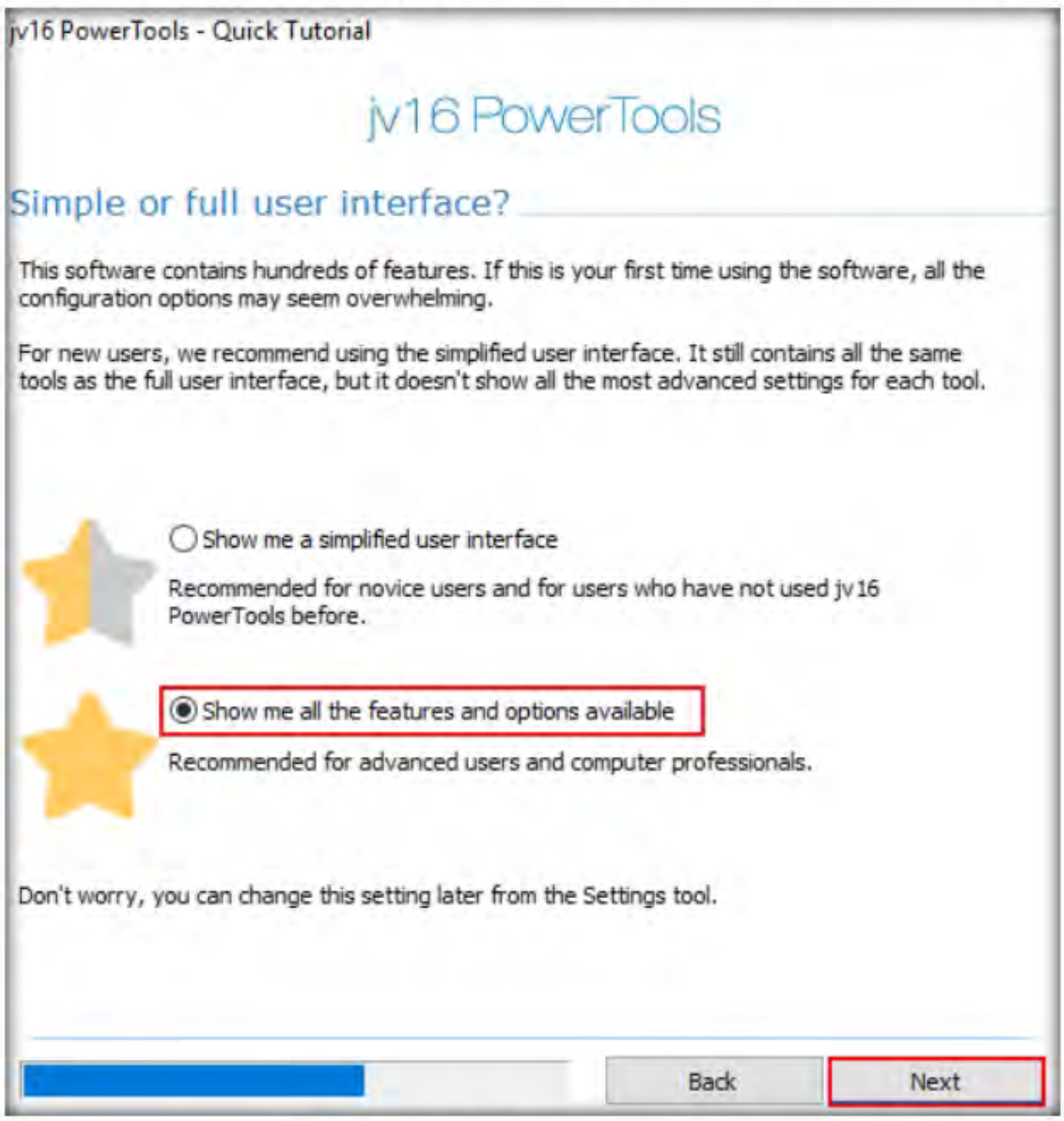


Figure 4.3.14: jv16 PowerTools Simple or full user interface

32. Click **Next** in the **Global Ignore List** wizard.
33. In the **Default Settings** wizard, leave all settings set to default, and then click **Next**.

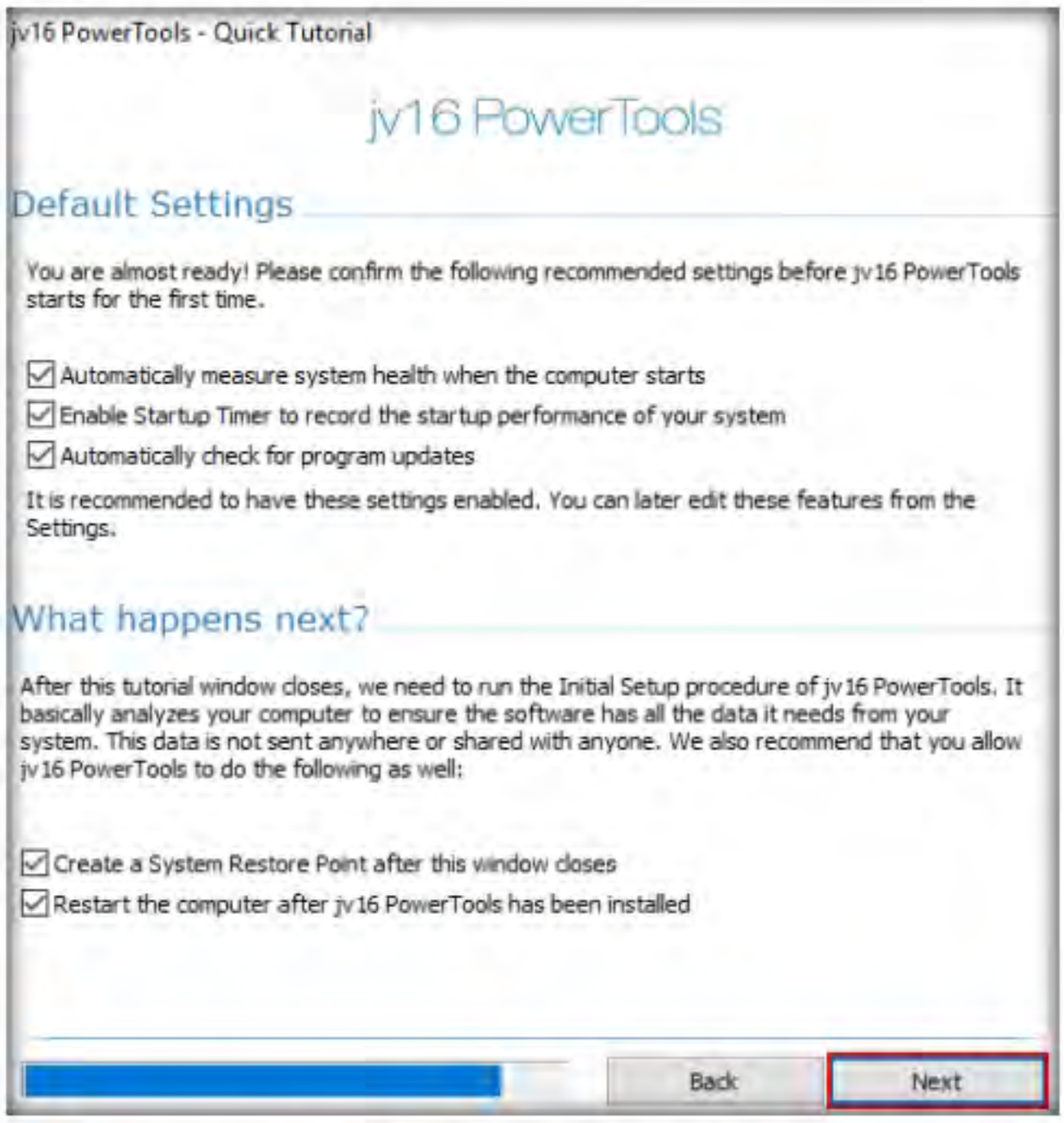


Figure 4.3.15: jv16 PowerTools Default Settings Wizard

34. The **Performing Initial Setup** window appears. Make sure that the **Restart computer after done** option is checked. Once the setup is done, the machine will automatically restart.

Figure 4.3.16: jv16 PowerTools Performing Initial Setup

35. Once the machine has restarted, log in to the machine and observe that the jv16 PowerTools application launches automatically, along with a **jv16 PowerTools** pop-up; click **No**.

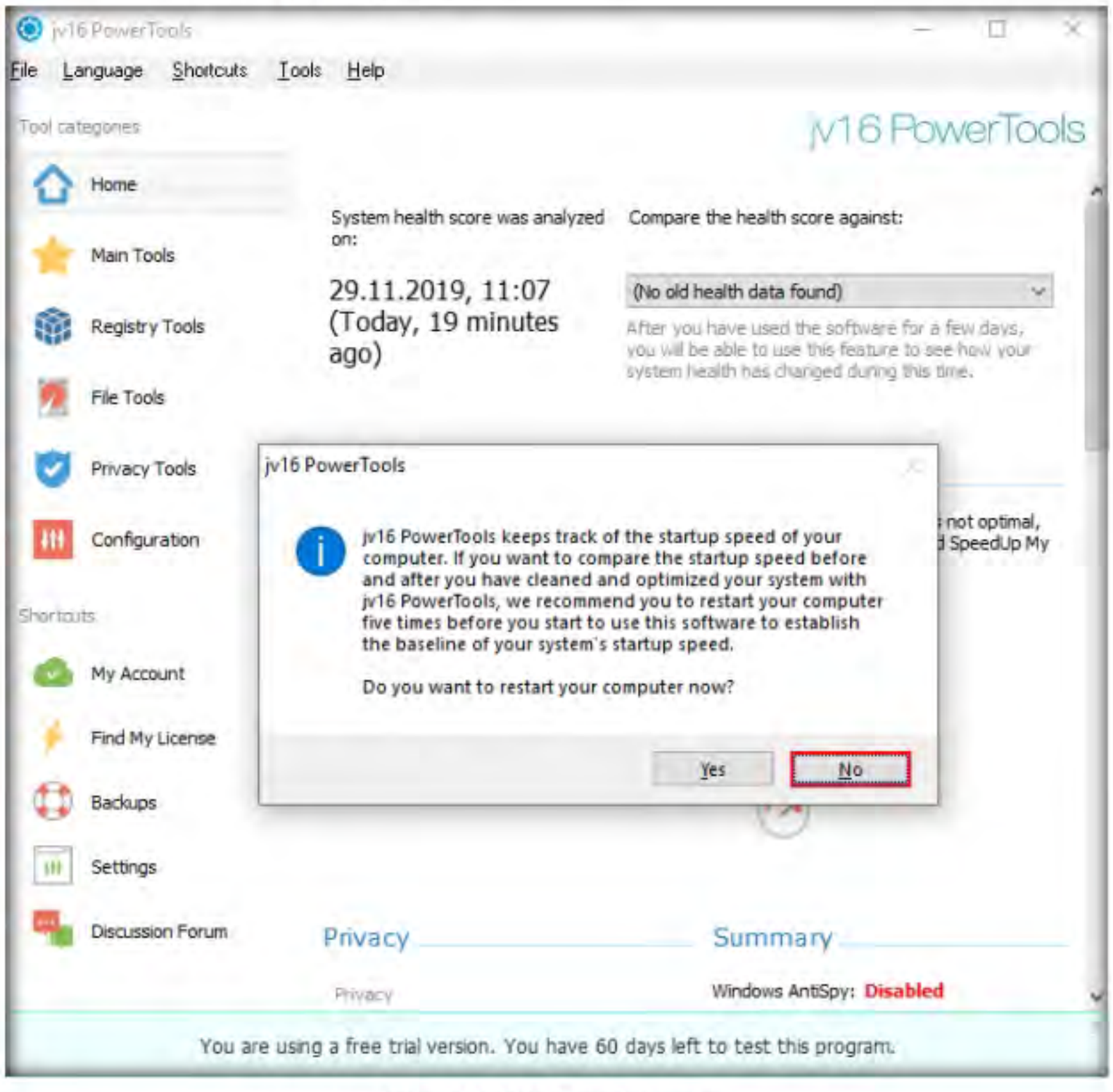


Figure 4.3.17: jv16 PowerTools pop-up

36. The **jv16 PowerTools** main window appears, as shown in the screenshot. By default, the **Home** option is selected, which displays the System Health, Privacy, Registry Integrity, and System Startup Times Summaries.

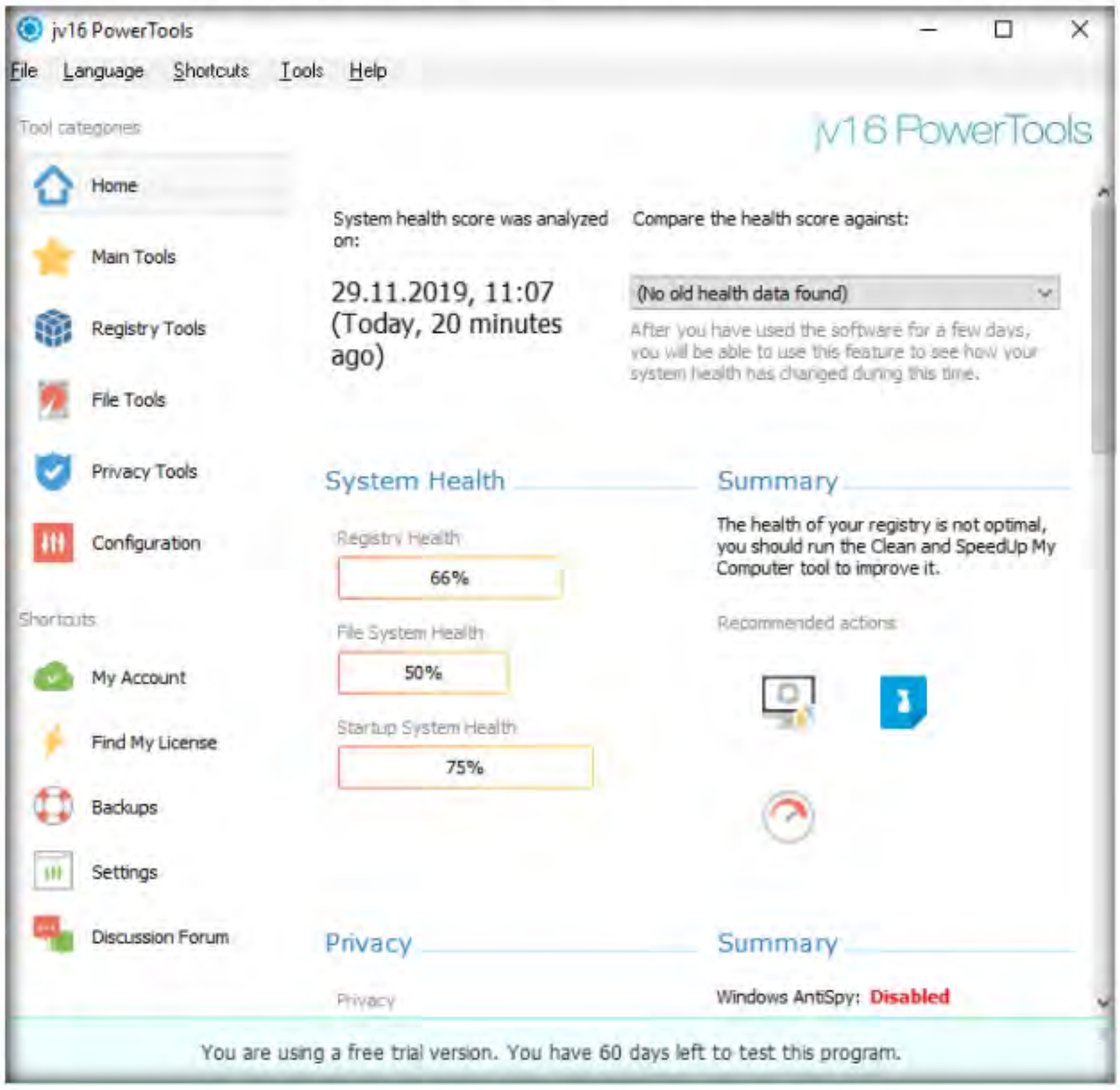


Figure 4.3.18: jv16 PowerTools Home Screen

37. Click the **Main Tools** section from the left pane to view the available tools in jv16 PowerTools. The **Main Tools** section lists out all available tool features, as shown in the screenshot.
38. Click the **Clean and SpeedUp My Computer** icon.

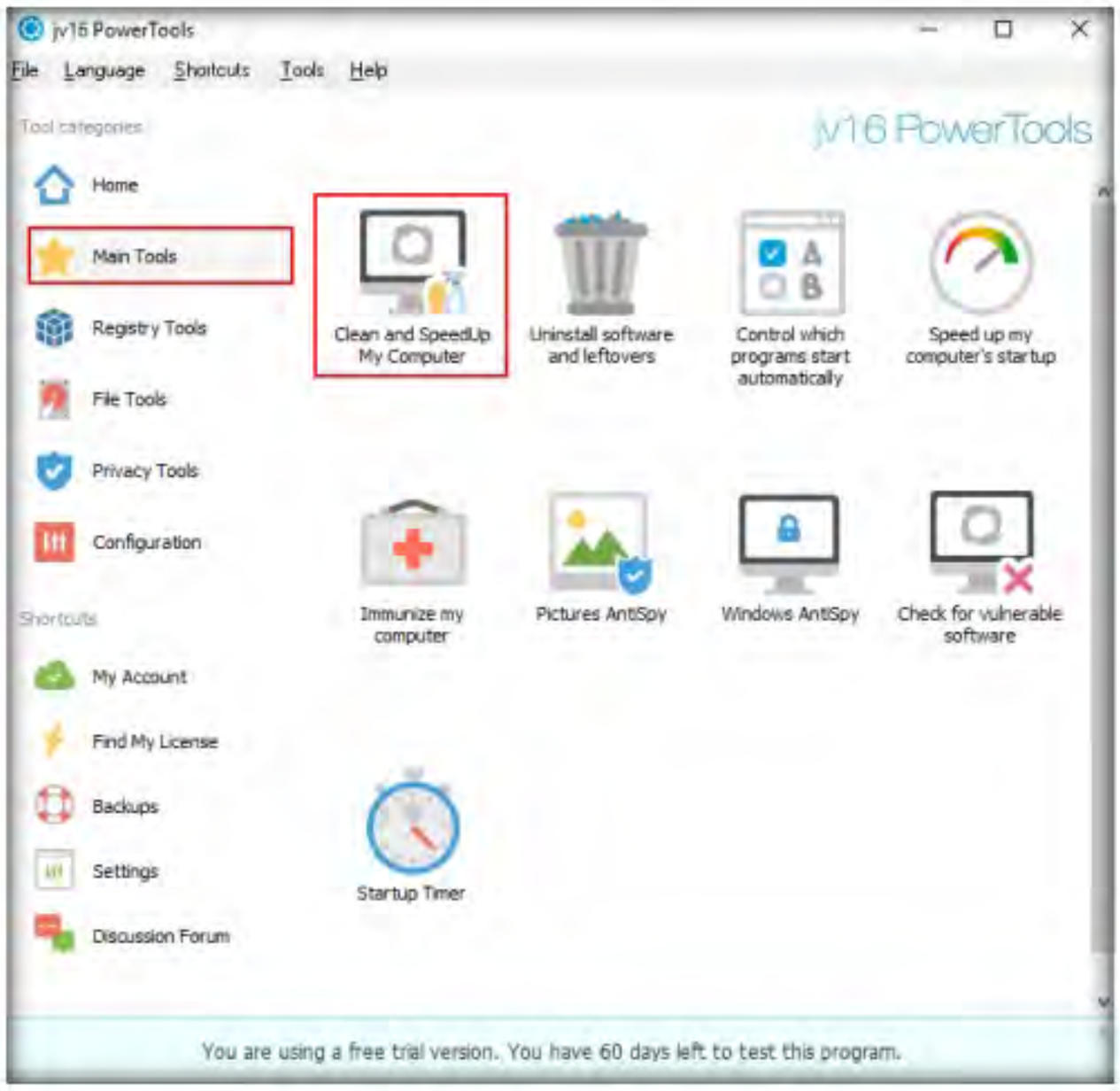


Figure 4.3.19: jv16 PowerTools Clean and SpeedUp My Computer

39. The **Clean and SpeedUp My Computer** wizard appears. Click the **Settings** and click **Start**.

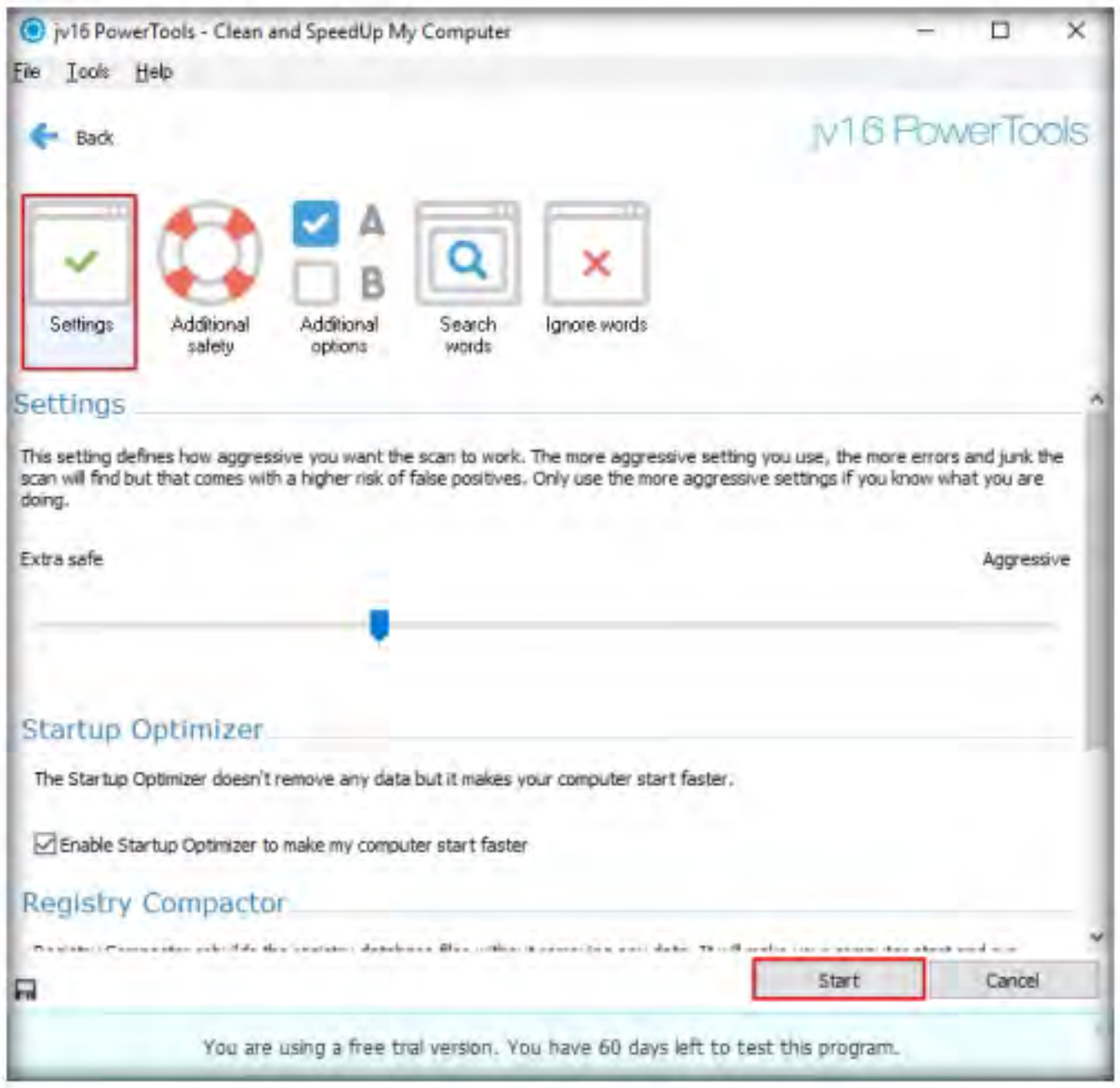


Figure 4.3.20: jv16 PowerTools Clean and SpeedUp My Computer Settings

40. The tool starts analyzing the machine. The process takes a few minutes.

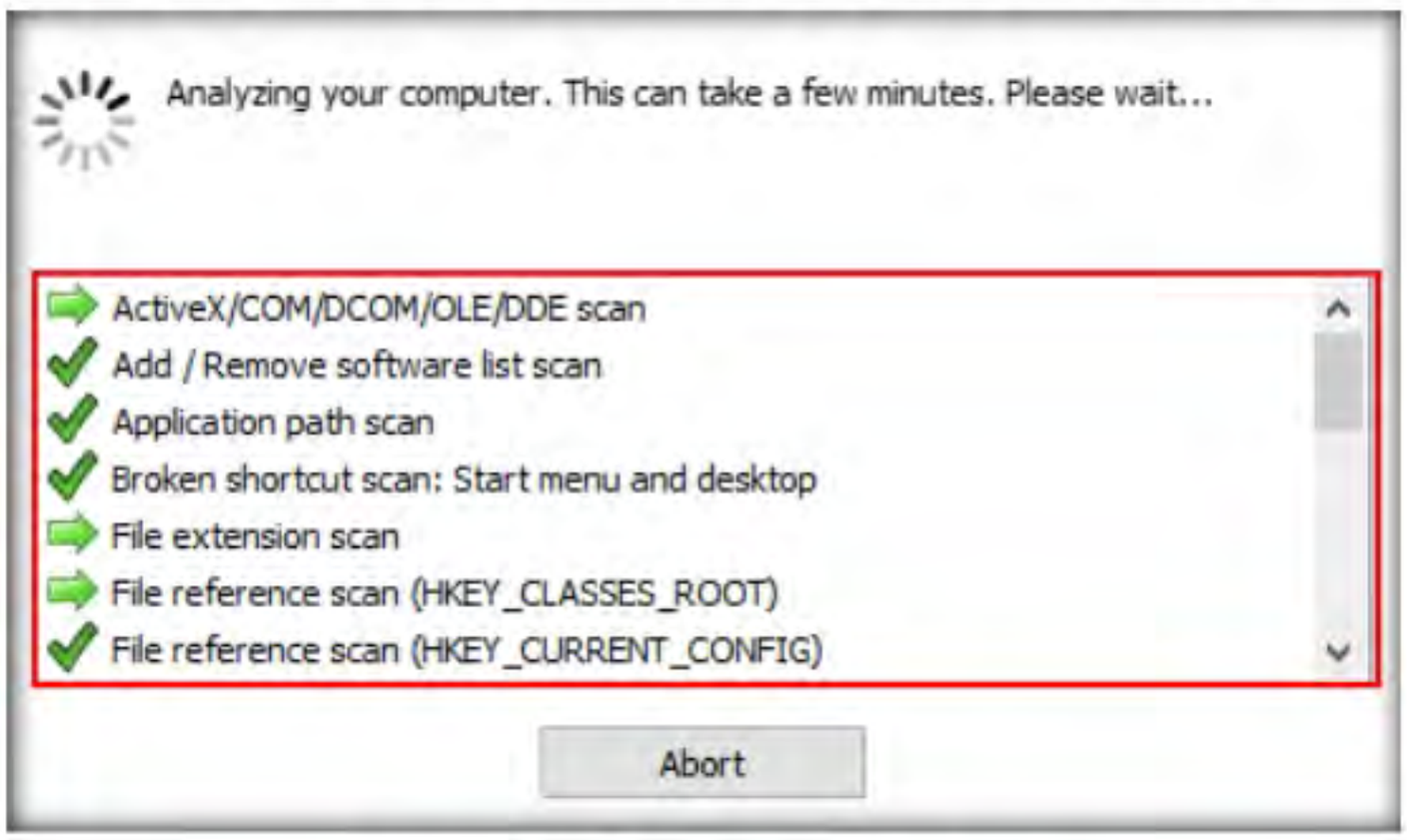


Figure 4.3.21: jv16 PowerTools Analyzing Computer

41. Once the scanning is complete, jv16 PowerTools displays the **Registry Errors**, **Temp Files**, and other results.

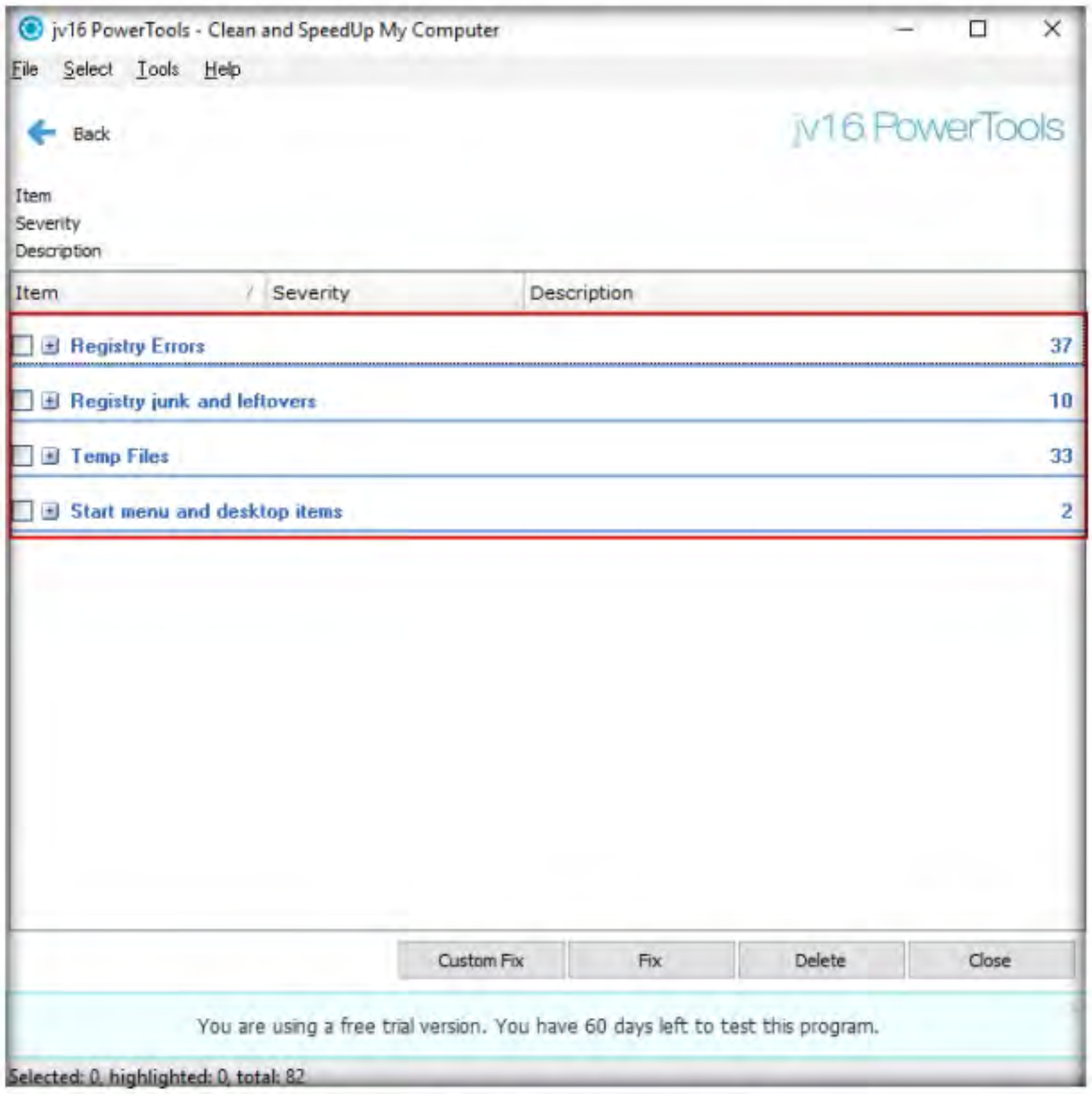


Figure 4.3.22: jv16 PowerTools Unwanted Entries

42. To view the registry errors, expand the **Registry Errors** node, and then expand the **Invalid file or directory reference** node.

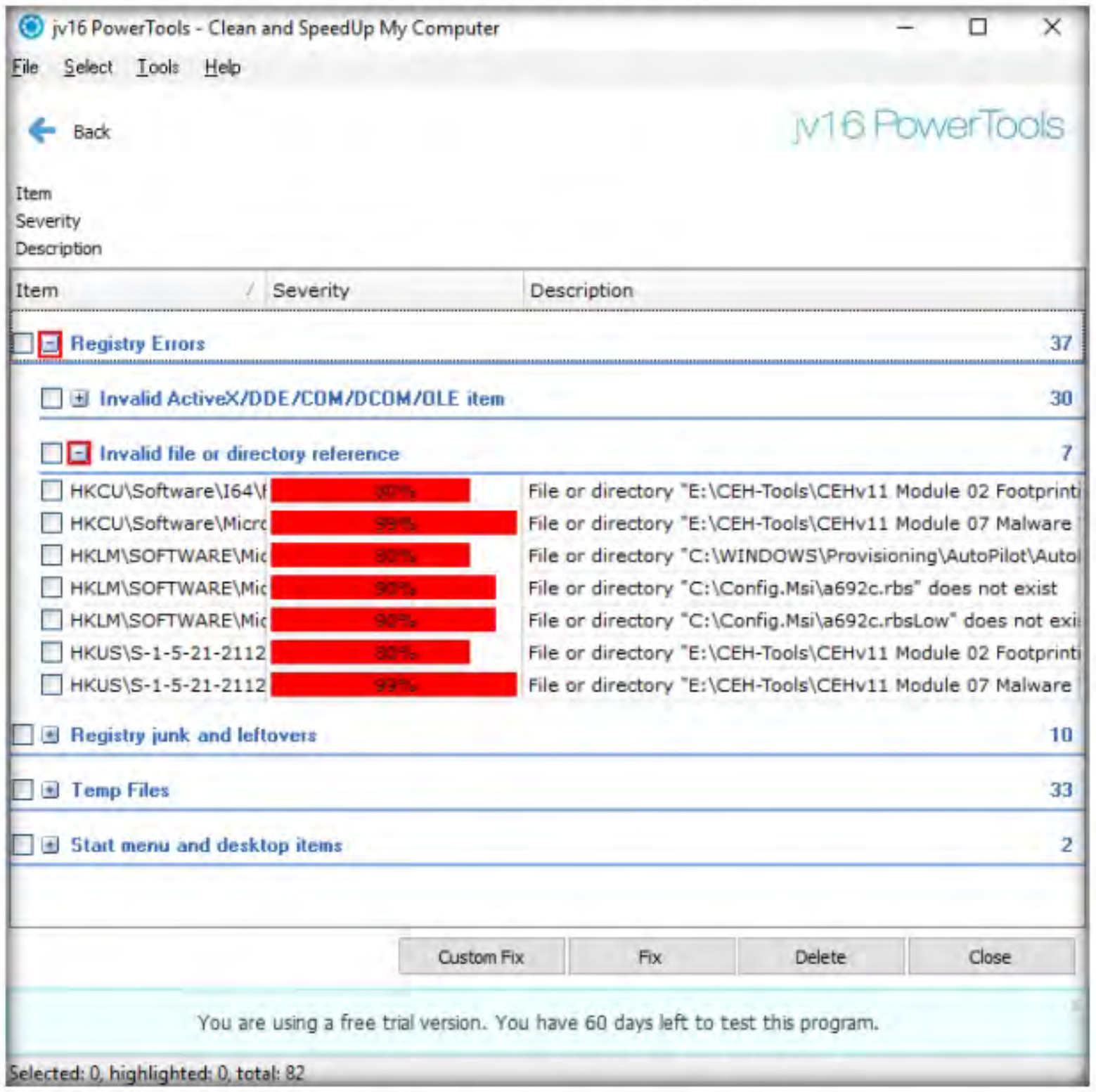


Figure 4.3.23: jv16 PowerTools Invalid File or Directory Reference

43. In the same way, expand the other items in the list to view all temporary files, log files, and other data.

44. Select all items in the application window, and then click **Delete**.

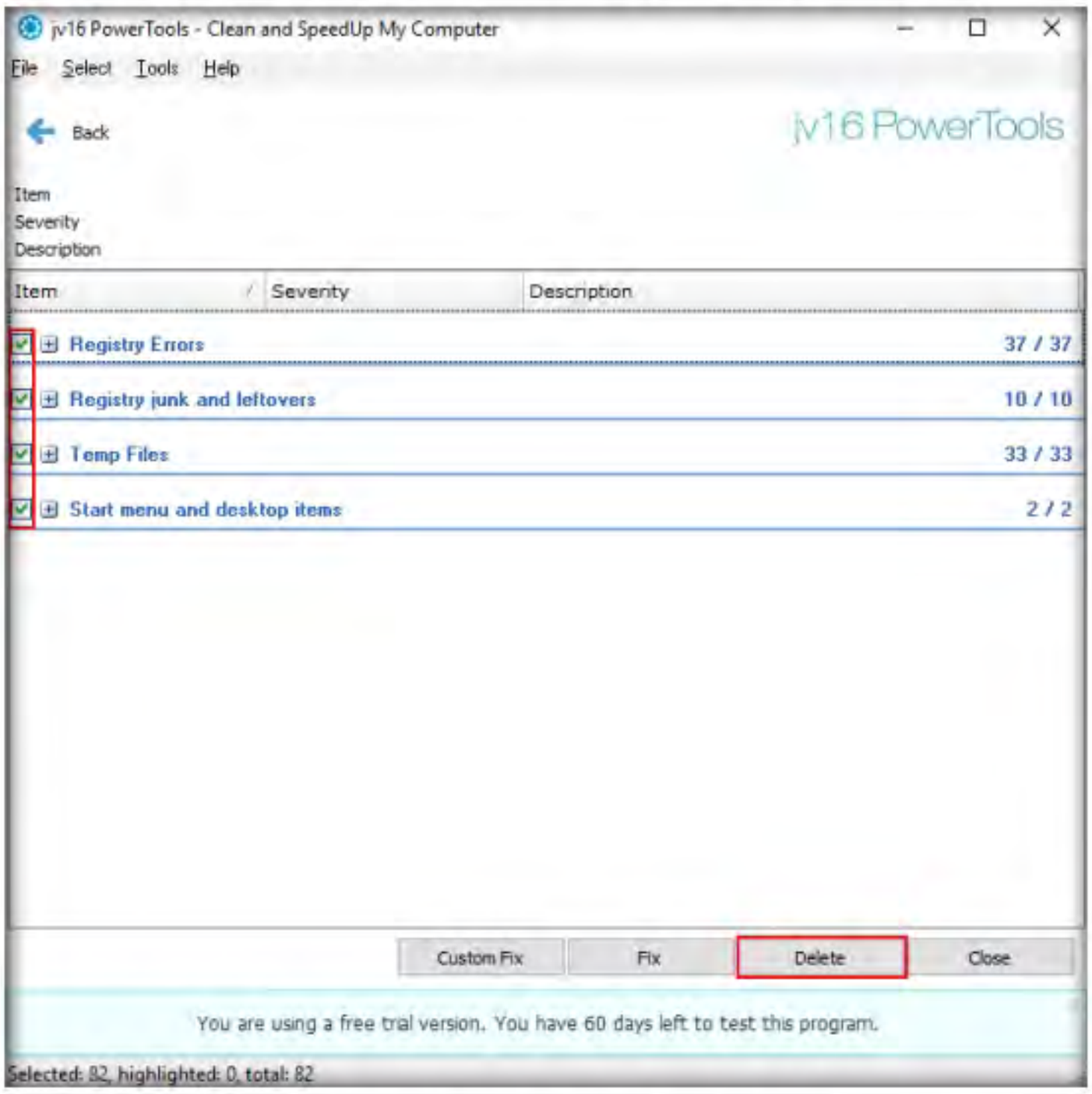


Figure 4.3.24: jv16 PowerTools Deleting Unwanted Entries

45. The **jv16 PowerTools** pop-up appears. If you want to create a backup, click **Yes**. In this lab, we have selected the **No** option, which deletes all files.

Figure 4.3.25: jv16 PowerTools Backup Confirmation

46. This deletes all unwanted or harmful registries, logs, temporary files, and other identified files, ensuring the safety of your computer.
47. If a **jv16 Power Tools** pop-up appears, asking you to restart the computer, click **No**.
48. If a **Clean and Fix My Computer** dialogue-box appears, close it.
49. jv16 PowerTools redirects you to the **Main Tools** section; click **Control which programs start automatically**.

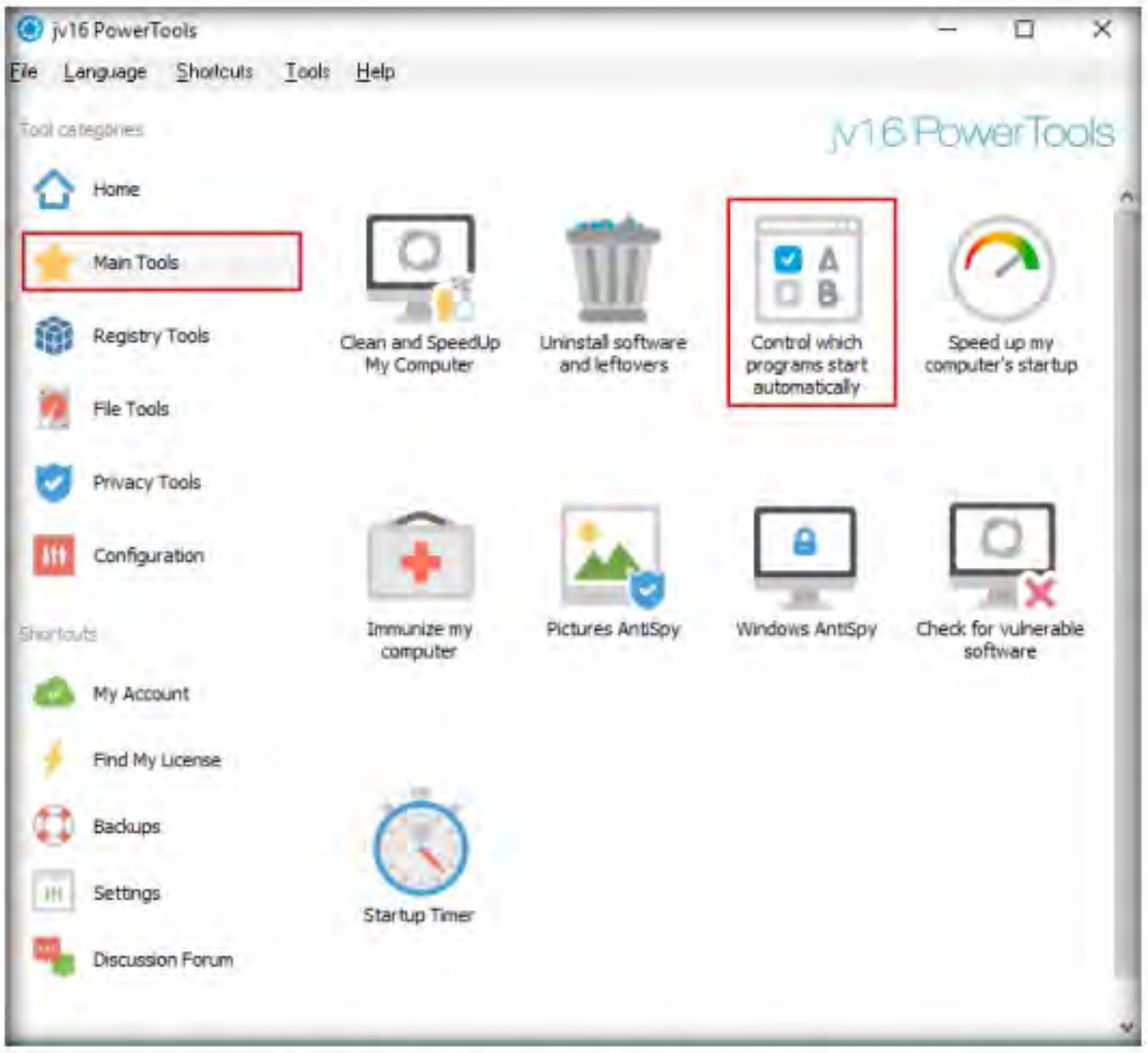


Figure 4.3.26: jv16 PowerTools Control which Programs Start Automatically

50. Select the software of your choice in the **Startup Manager** and assign the appropriate action for the software you check.

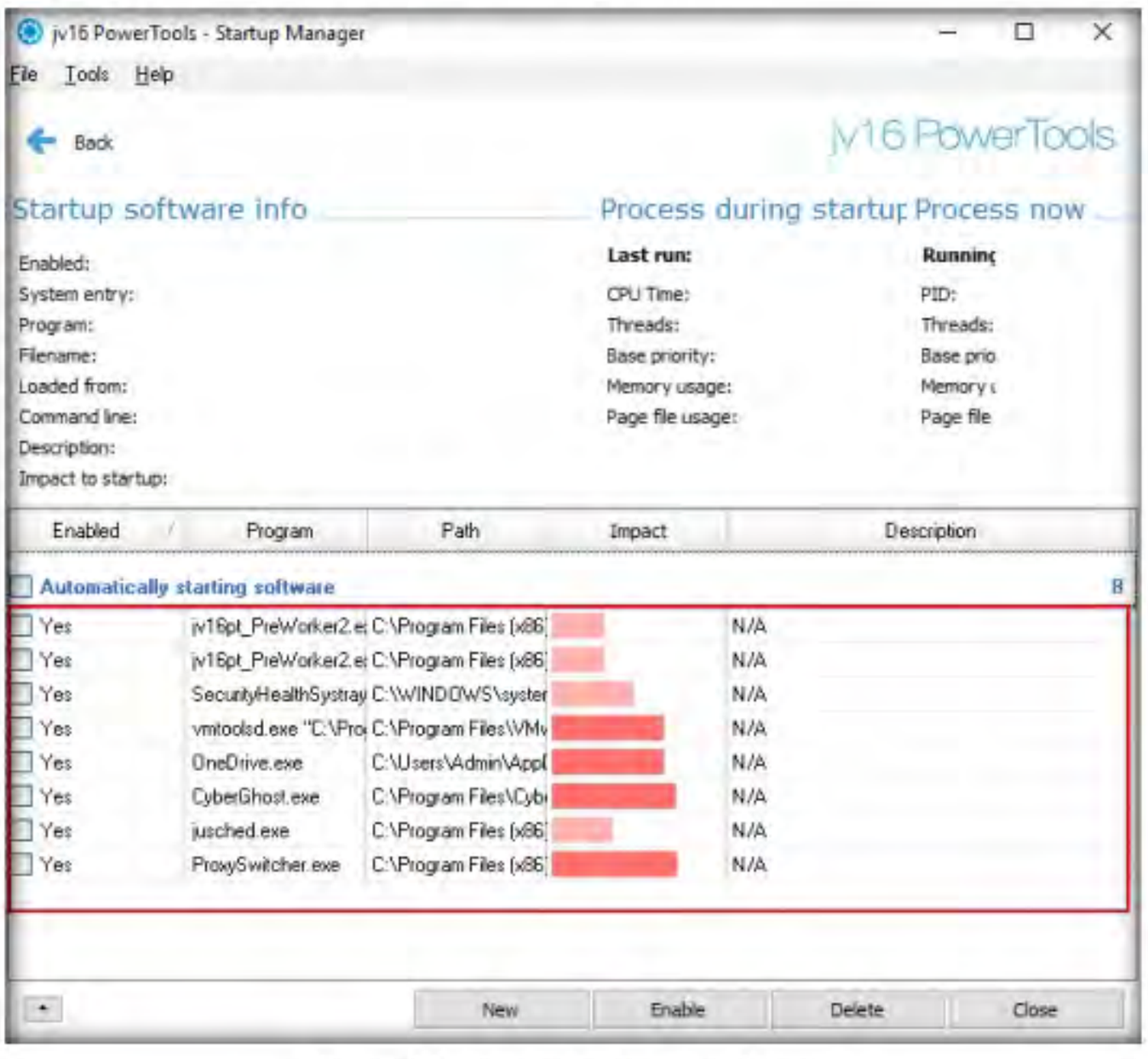


Figure 4.3.27: jv16 PowerTools - Startup Manager

51. Thus, you could find any Trojans or malicious files running at system startup and choose the appropriate actions against them. Click **Close** in the **Startup Manager** wizard, which will redirect you to the **Main Tools** section of jv16 PowerTools.
52. Select **Registry Tools** to view Registry-related functions.
53. This section helps you to find, manage, monitor, compress, clean, or replace **registry files**.

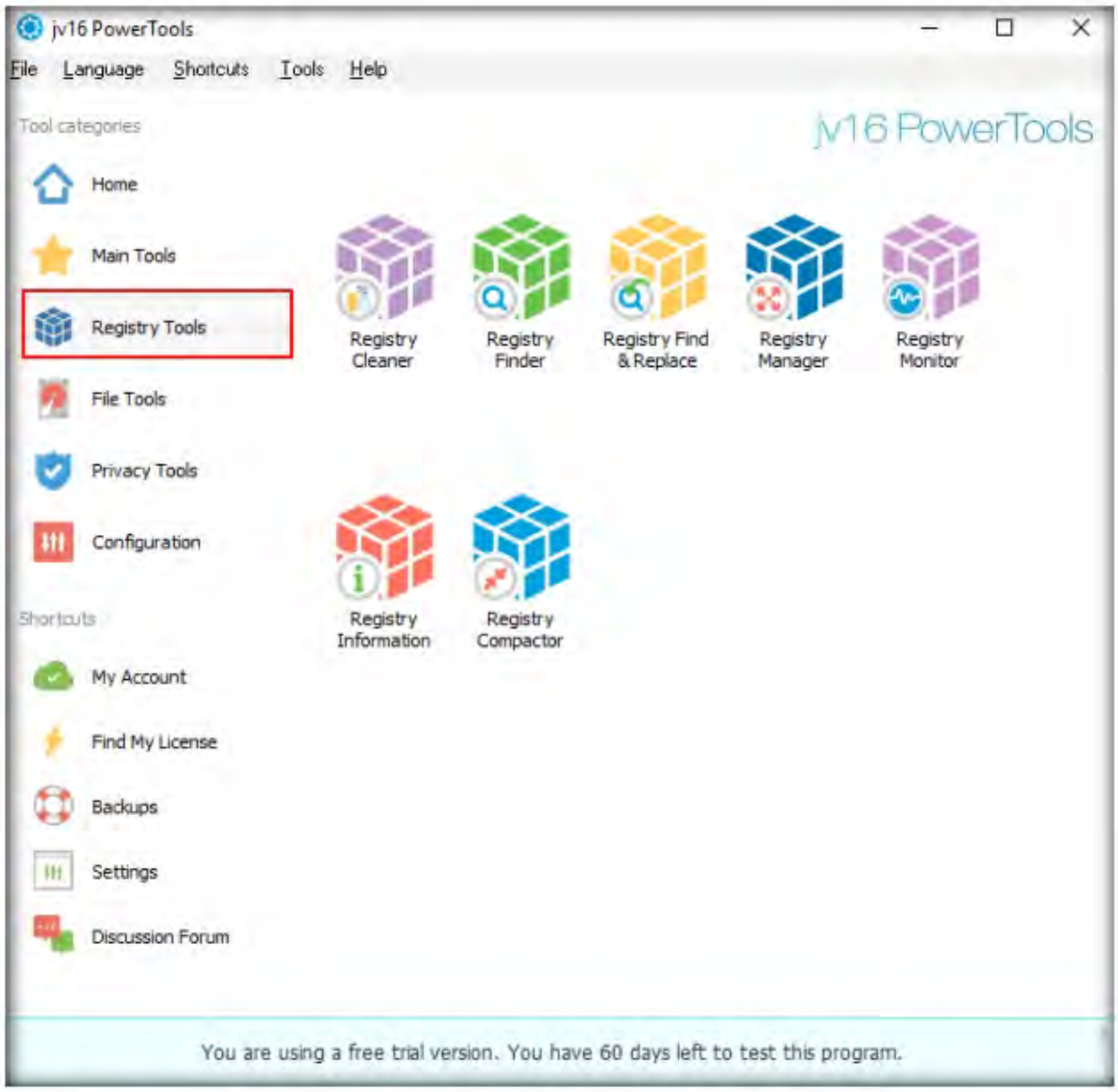


Figure 4.3.28: jv16 PowerTools Registry Tools

54. Click **File Tools** to view file-related functions.
55. This section helps you to find, recover, clean, organize, or merge files or directories.

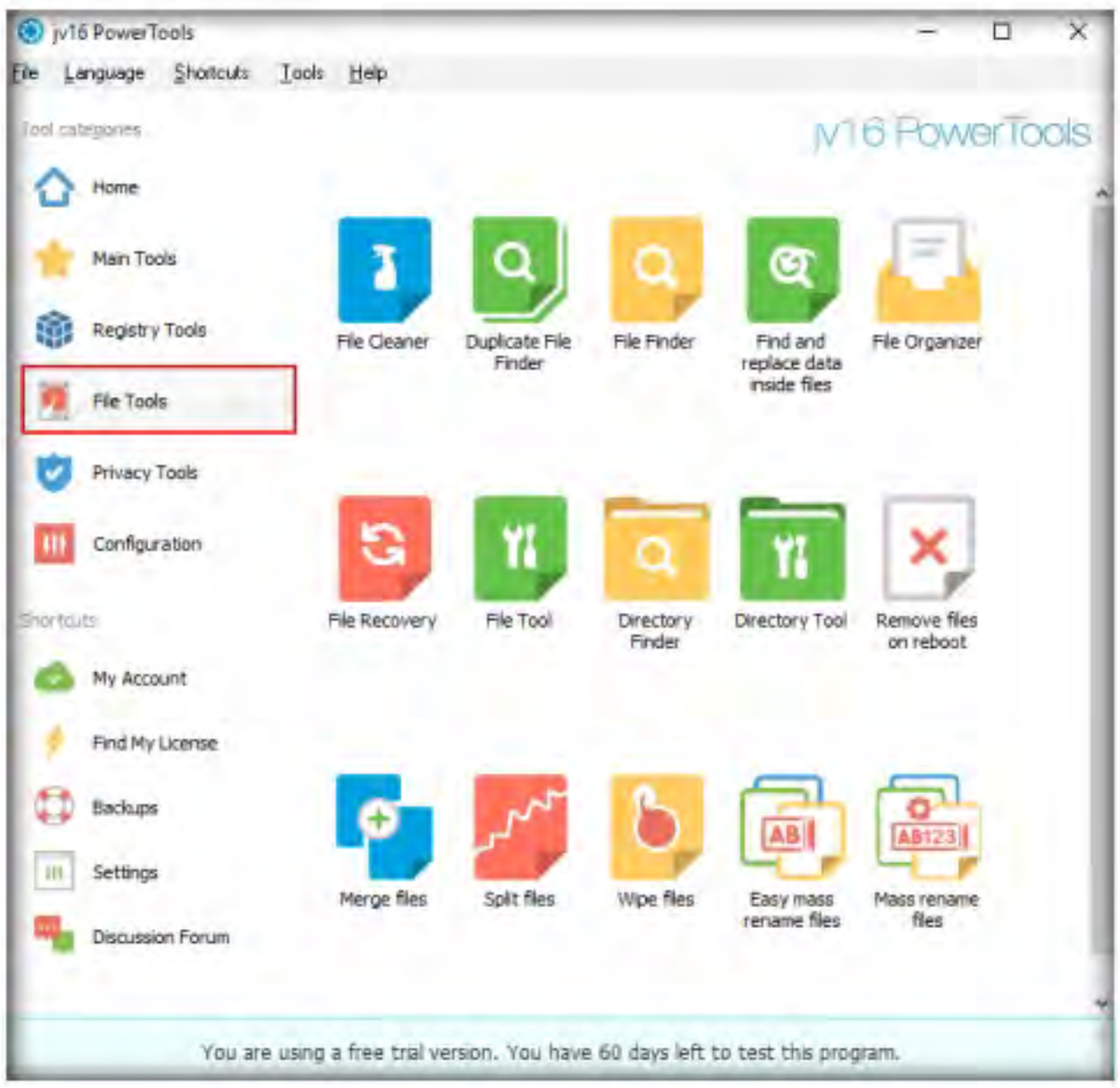


Figure 4.3.29: jv16 PowerTools File Tools

56. Select **Privacy Tools** to view privacy-related functions
57. This section helps you to check for vulnerable software, spyware, clear your history, and perform other tasks.

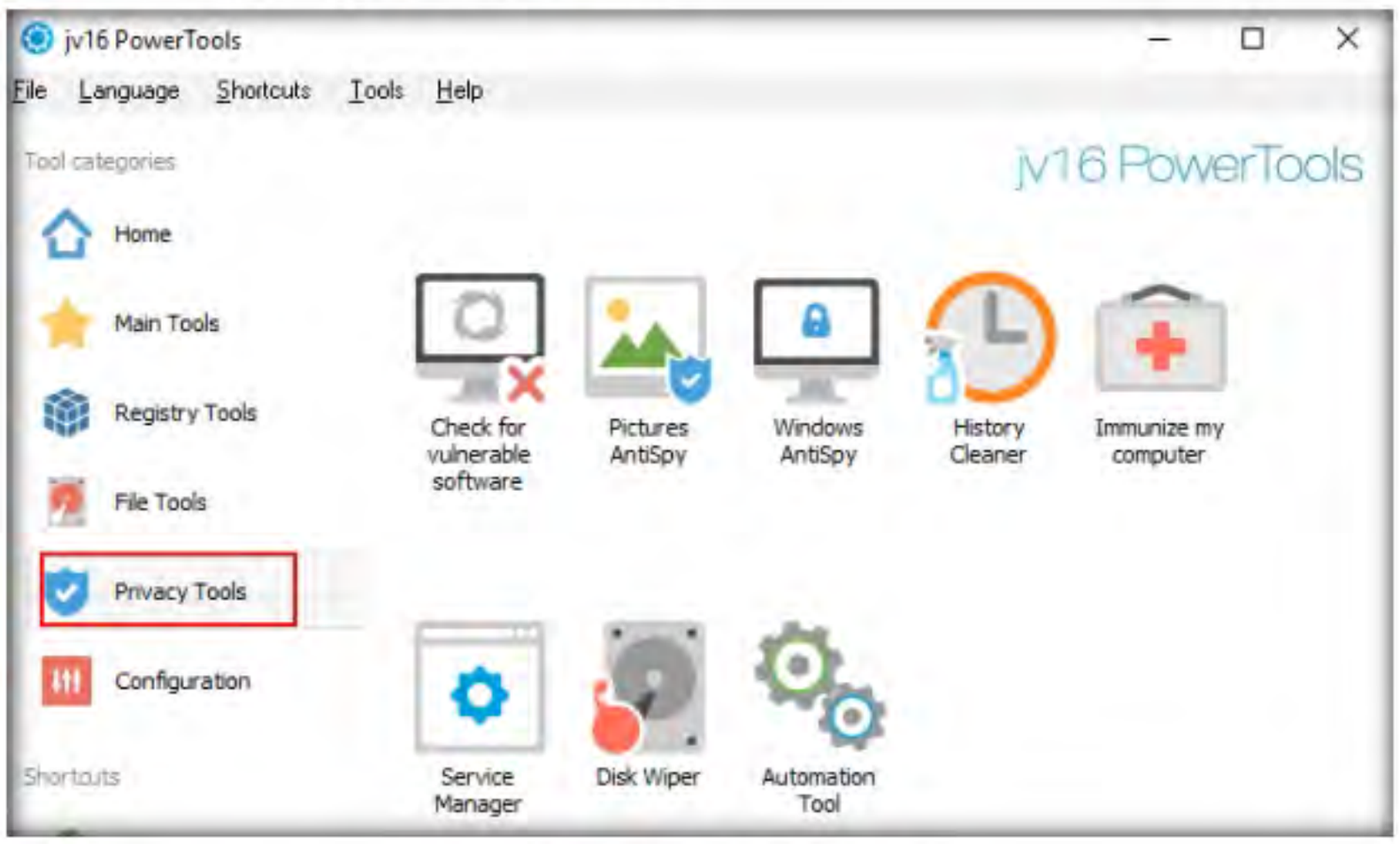


Figure 4.3.30: jv16 PowerTools Privacy Tools

58. The **Disk Wiper** option wipes the disk—this is *not* recommended.
59. Select **Backups** to view the system-related backups.

Figure 4.3.31: jv16 PowerTools Select Backups

You can also use other registry monitoring tools such as **Reg Organizer** (https://www.chemtable.com), **Registry Viewer** (https://accessdata.com), **RegScanner** (https://www.nirsoft.net), or **Registrar Registry Manager** (https://www.resplendence.com) to perform registry monitoring.

60. The **Jv16 PowerTools - Backup Tool** window appears, displaying the **registry**, **file**, and **other backups**.

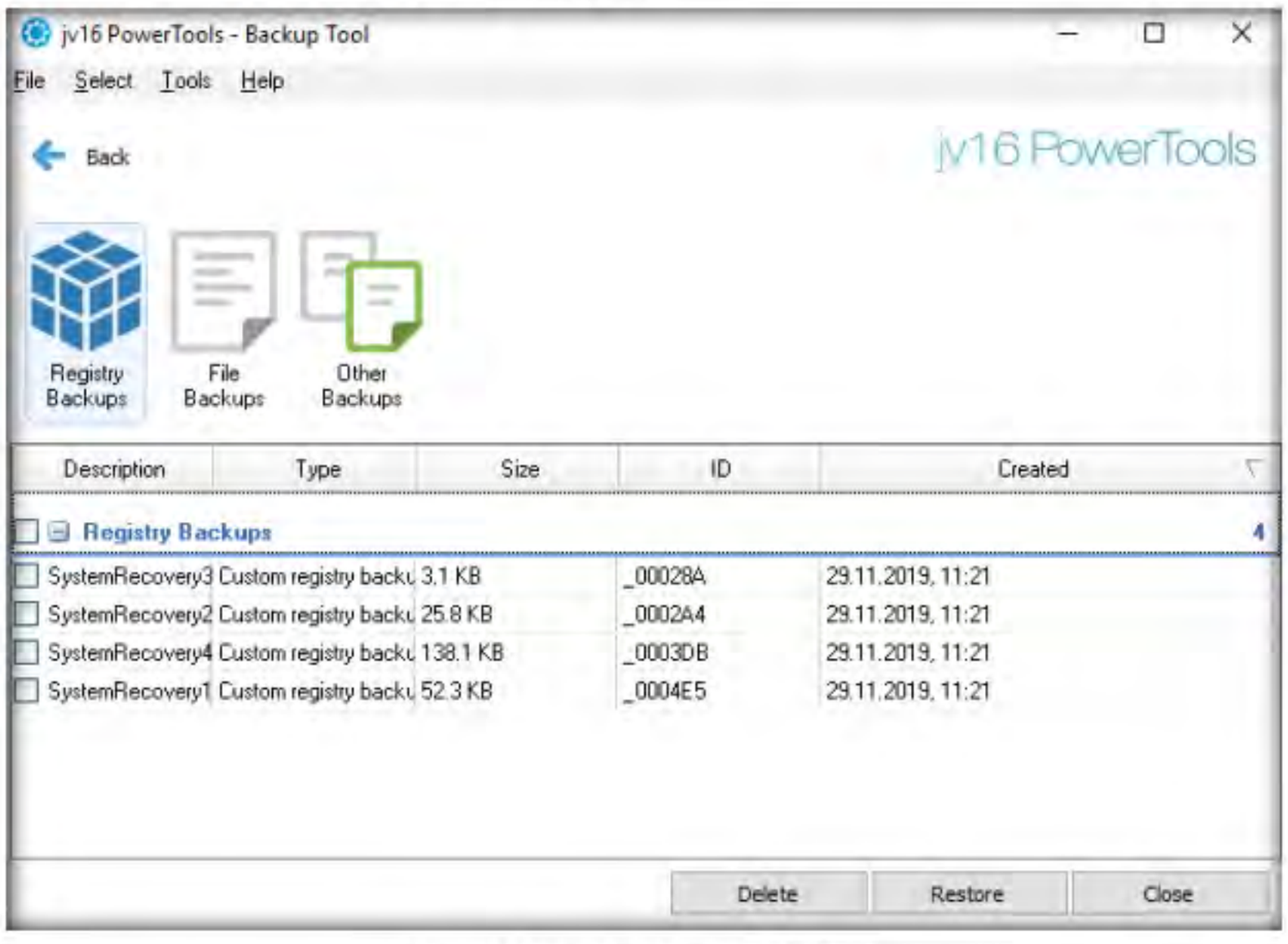


Figure 4.3.32: jv16 PowerTools - Backup Tool

61. You can choose whether to delete or restore backups in this window.
62. Click **Close** on the **Jv16 PowerTools - Backup Tool** window; this will redirect you to the **Main Tools** section of jv16 PowerTools.

Note: If a restart prompt appears, then restart the machine.

63. Examining the result of the jv16 PowerTools scan reveals unwanted registry entries and other suspicious activities on the machine and allows the user to stop or delete them.
64. Close the **jv16 PowerTools** main window.

TASK 4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

Here, we will use the SrvMan tool to check for suspicious windows services.

TASK 4.1

Launch Service Manager and View the Result

1. On the **Windows 10** machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\srvman-1.0\x64** and double-click **srvman.exe**.

   Note: You can choose any of the executable files for the Windows Service Manager according to your computer and OS design.

2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. As most services run in the background to support processes and applications, malicious services are invisible, even when they are performing harmful activities on the system, and can even function without intervention or input. Malware spawns Windows services that allow attackers to control the victim machine and pass malicious instructions remotely. Malware may also employ rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

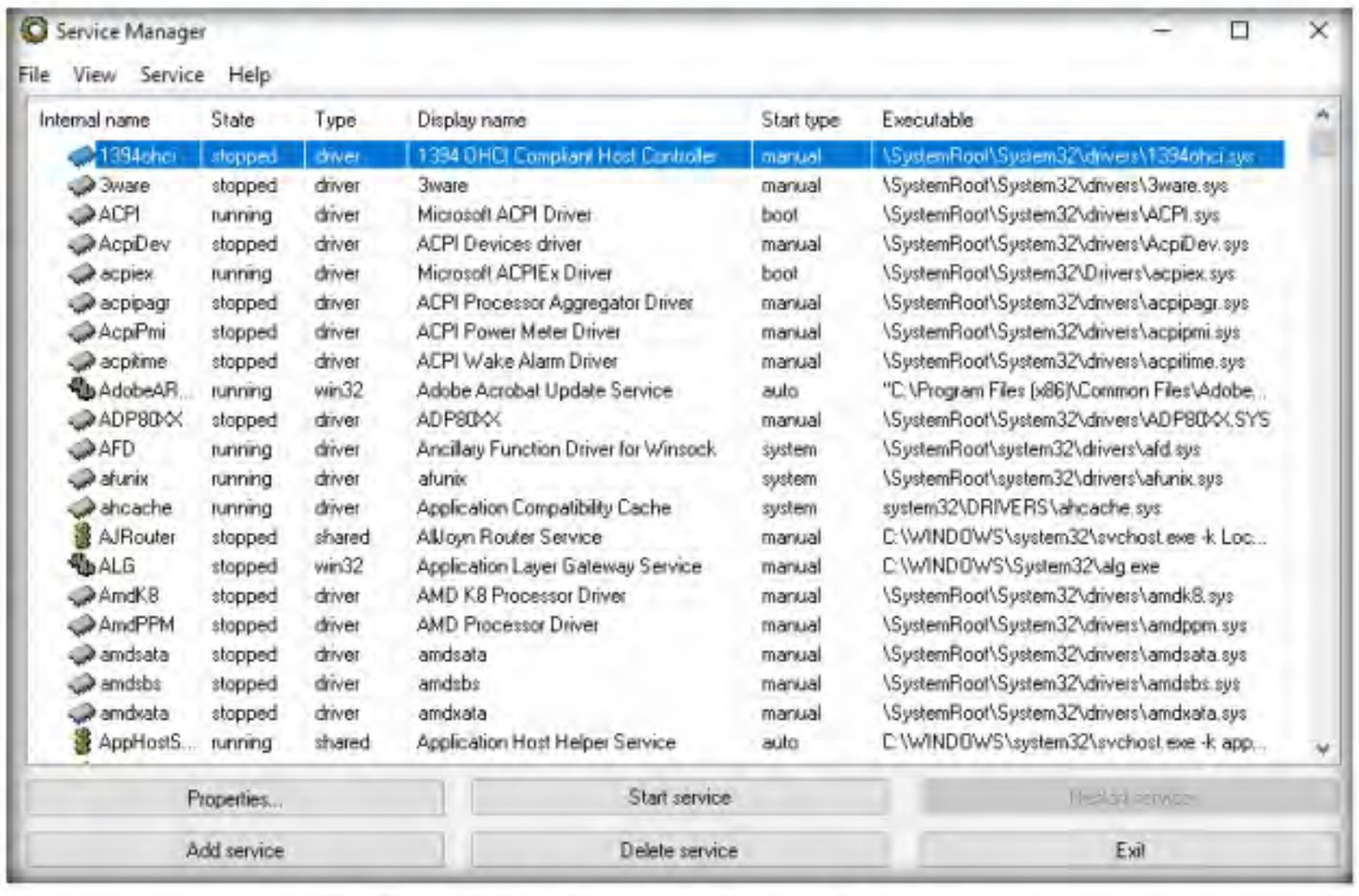


Figure 4.4.1: Windows Service Manager Main Window

4. The Service Manager shows the **Internal name**, **State**, **Type**, **Display name**, **Start type**, and **Executable** data of the services.

5. Here, you can choose any unwanted service that is running on your computer, and **Stop** or **Delete** that service by choosing the appropriate action.
6. You can view the properties of the selected service by clicking on **Properties**.
7. To Start a stopped service, click the **Start service** button. To stop a running service, click **Stop service**.
8. To restart any running service, click the **Restart service** button.
9. To add a new service to your machine, click the **Add service** button.
10. To delete any running or stopped service, click the **Delete service** button.

You can trace malicious services initiated by the suspect file during dynamic analysis by using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

You can also use other Windows service monitoring tools such as **Advanced Windows Service Manager** (https://securityxploded.com), **Process Hacker** (https://processhacker.sourceforge.io), **Netwrix Service Monitor** (https://www.netwrix.com), or **AnVir Task Manager** (https://www.anvir.com) to perform Windows services monitoring.

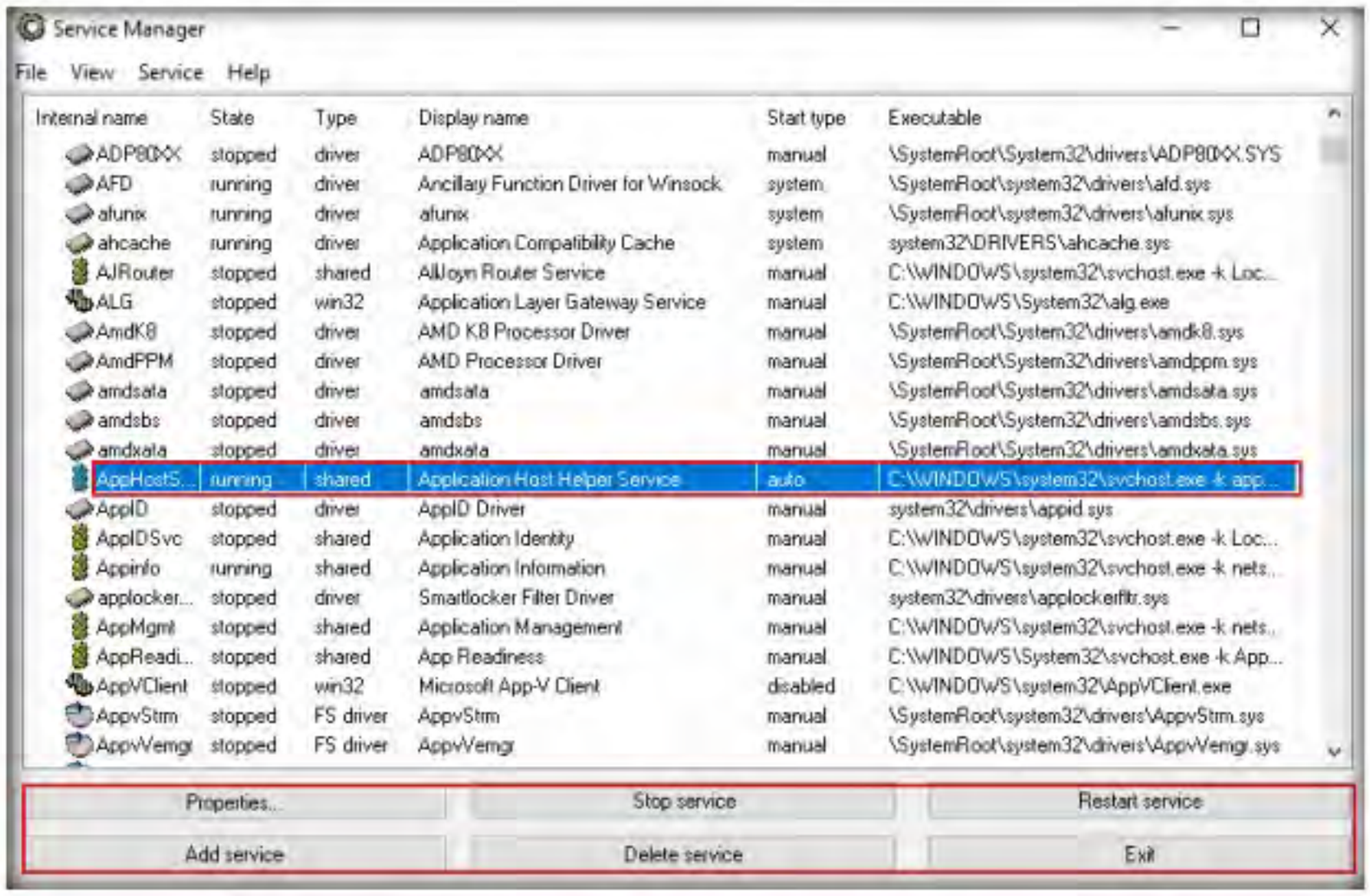


Figure 4.4.2: Windows Service Manager Features

11. Thus, you can monitor the unwanted services running on the machine using the Windows Service Manager.
12. Close the **Service Manager** window.

TASK 5

Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

TASK 5.1

Launch AutoRuns

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows** and double-click **Autoruns.exe**.

Startup programs are applications or processes that start when your system boots up. Attackers make many malicious programs such as Trojans and worms in such a way that they are executed during startup, and the user is unaware of the malicious program running in the background.

An ethical hacker or penetration tester must identify the applications or processes that start when a system boots up and remove any unwanted or malicious programs that can breach privacy or affect a system's health. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools like Autoruns for Windows and WinPatrol is essential for detecting malware.

2. The **AutoRuns License Agreement** window appears; click **Agree**.

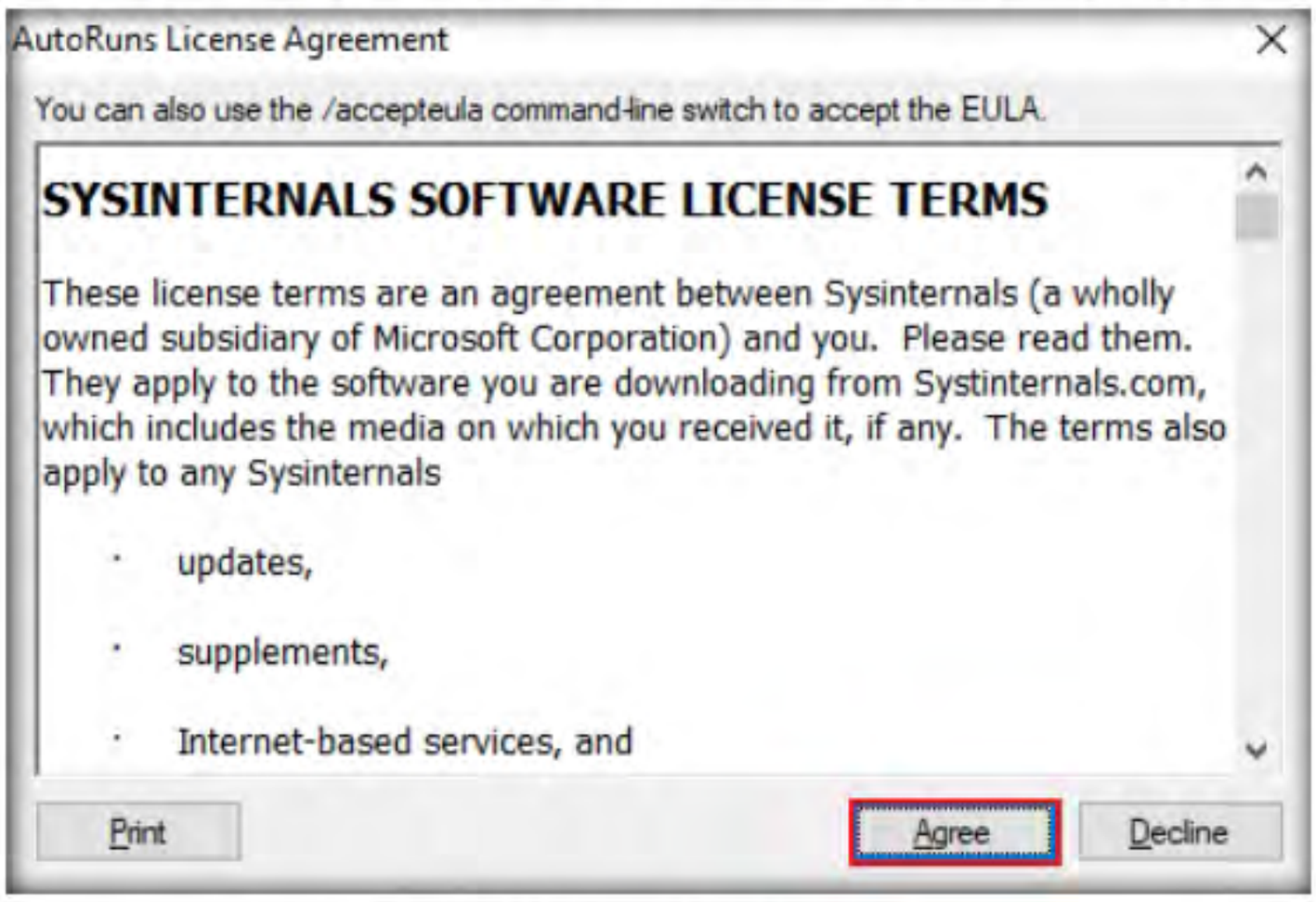


Figure 4.5.1: Autoruns License Agreement

3. The **Autoruns** main window appears. It displays all **processes**, **dll's**, and **services**, as shown in the screenshot.

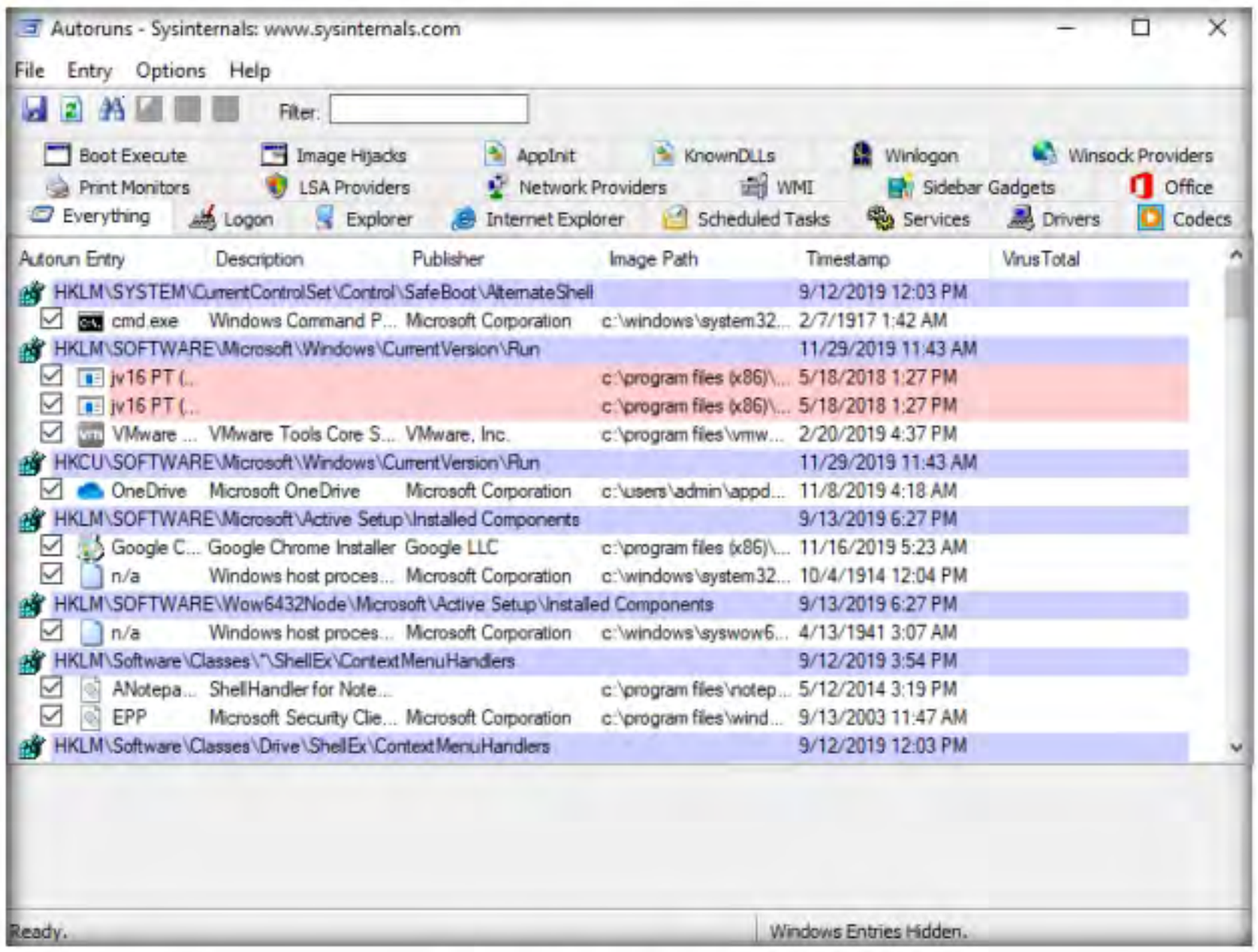


Figure 4.5.2: Autoruns Main Window

Note: The application lists displayed under all the tabs may vary in your lab environment.

Autoruns for Windows

This utility can auto-start the location of any startup monitor, display which programs are configured to run during system bootup or login, and show the entries in the order Windows processes them. As soon as this program is included in the startup folder, Run, RunOnce, and other Registry keys, users can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user zoom in on third-party auto-starting images that add to the users' system, and it has support for looking at the auto-starting images configured for other accounts configured on the system.

4. Click the **Logon** tab to view the applications that run automatically during login.

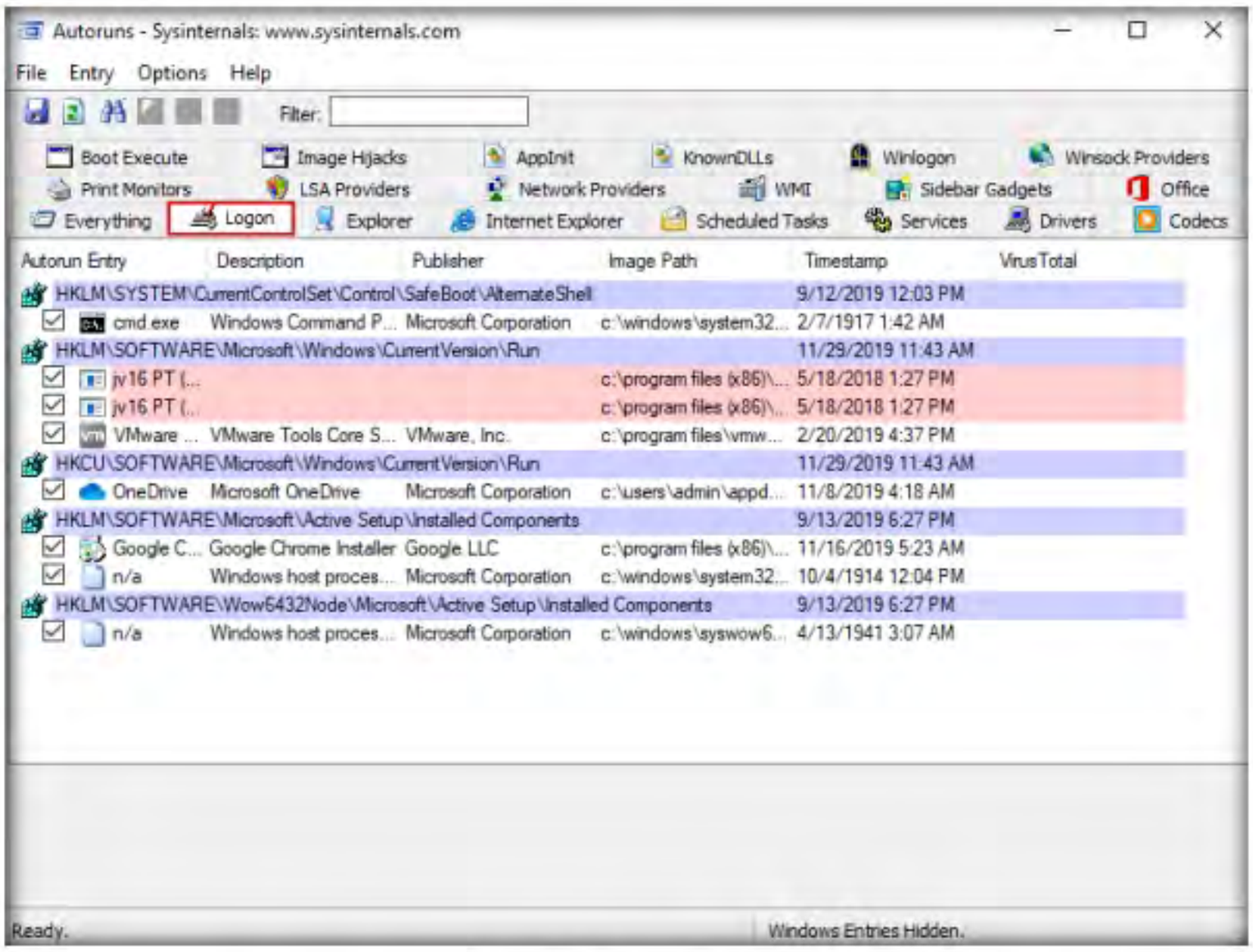


Figure 4.5.3: Autoruns Logon list

5. Click the **Explorer** tab to view the explorer applications that run automatically at system startup.

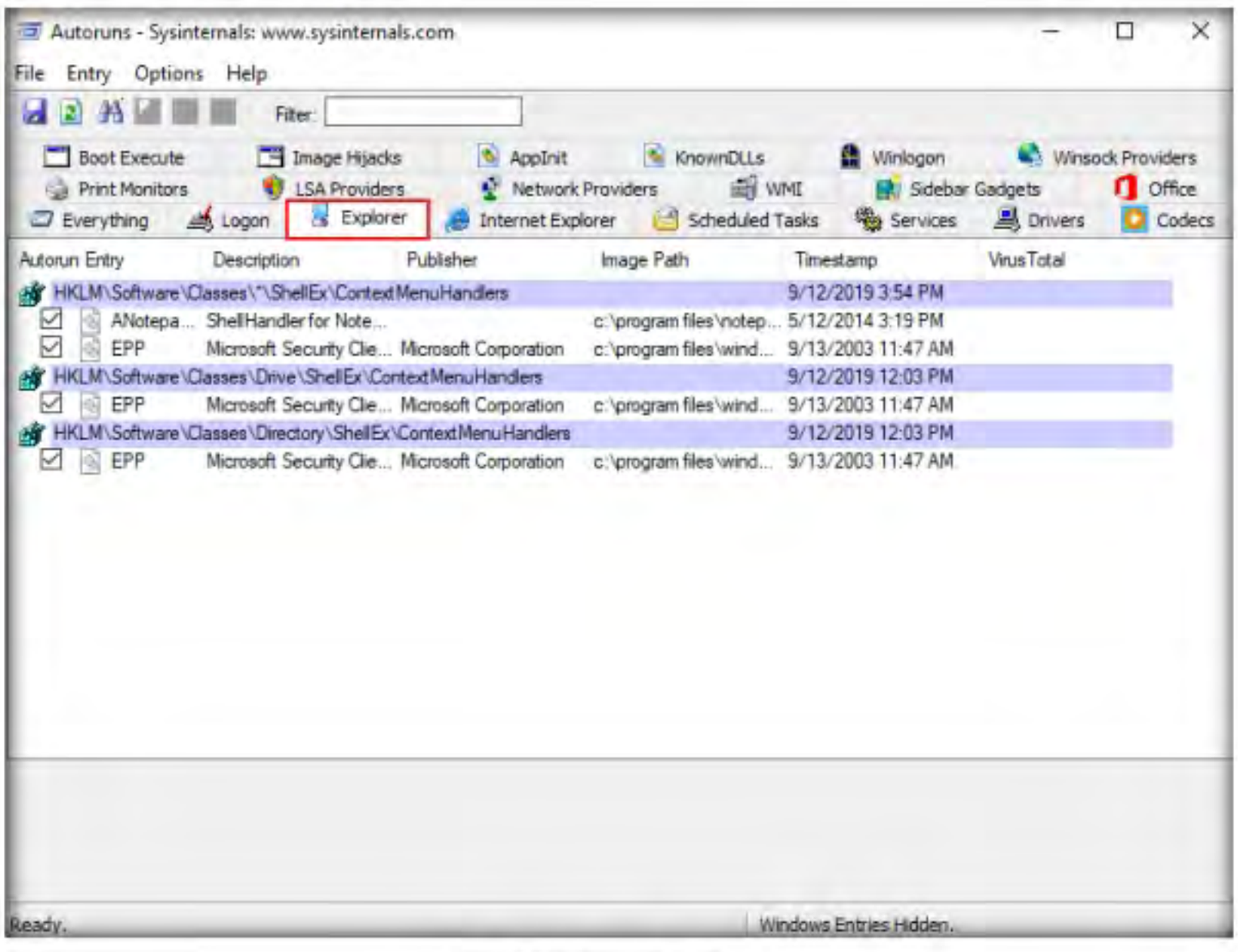


Figure 4.5.4: Autoruns Explorer list

6. Clicking the **Services** tab displays all services that run automatically at system startup.

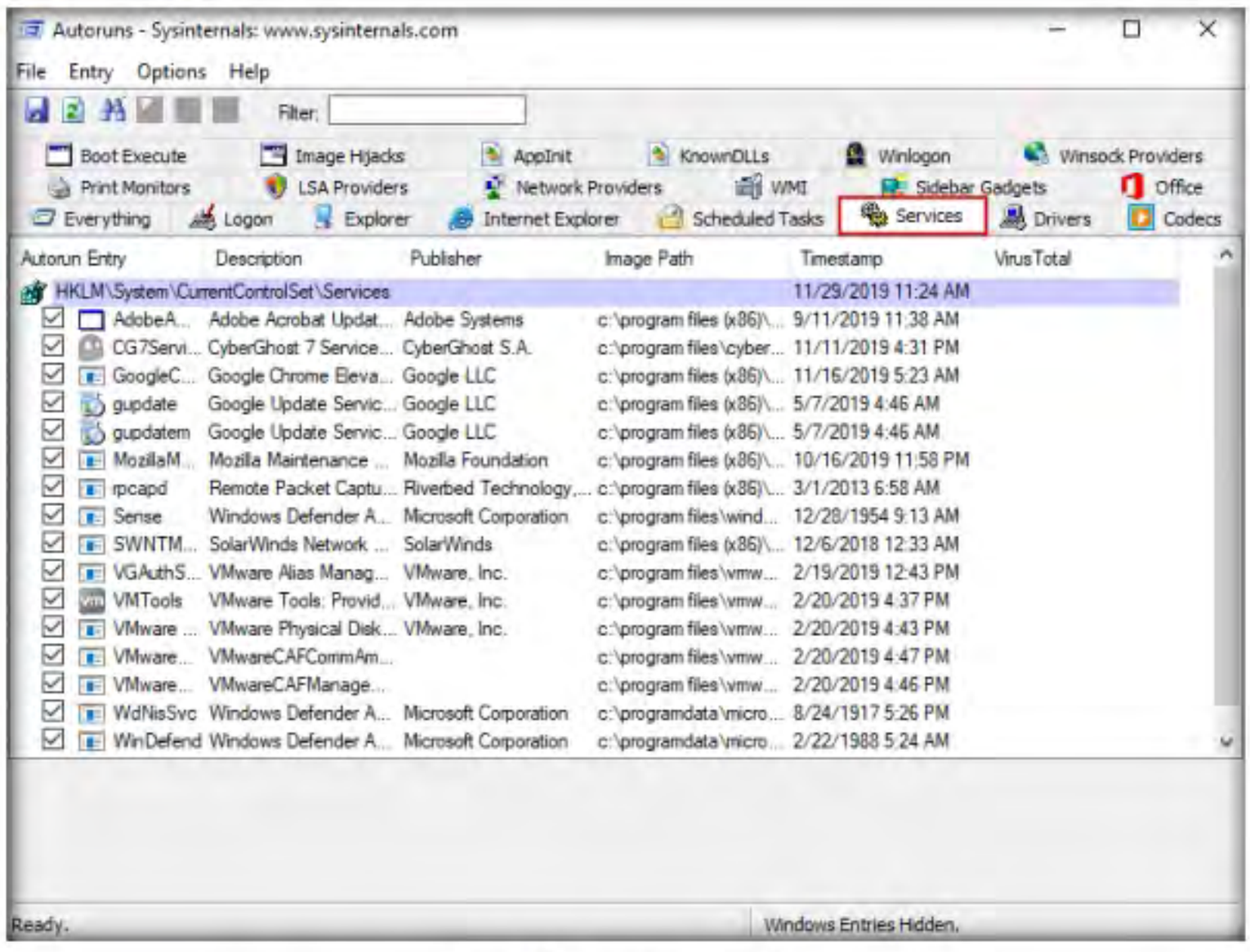


Figure 4.5.5: Autoruns Services list

7. Click the **Drivers** tab to view all application drivers that run automatically at system startup.
8. For example, here, **ebdrv** is selected. Clicking this driver displays the size, version, and the time at which it was automatically run at system startup (for the first time).

Note: The list displayed under this tab may vary in your lab environment.

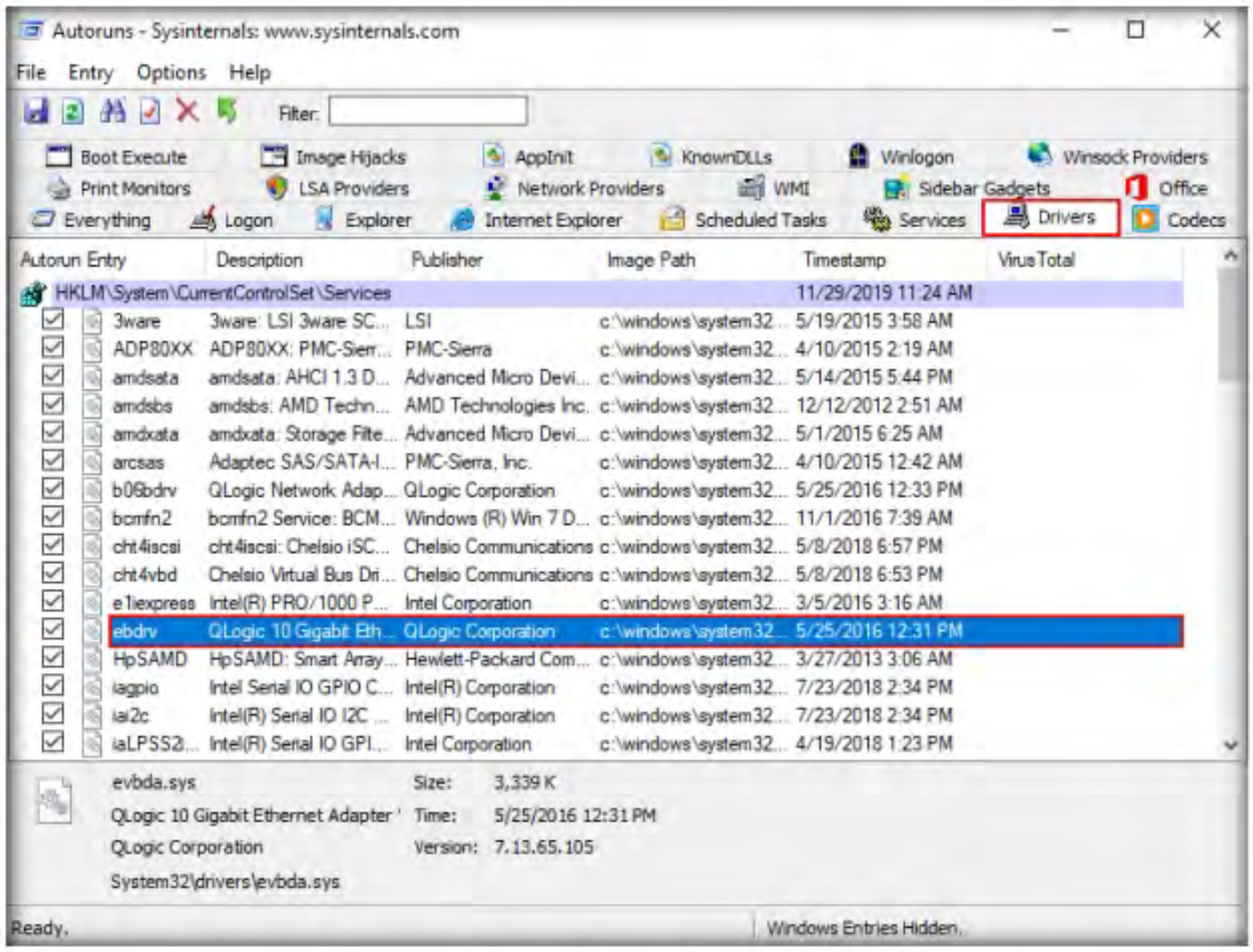


Figure 4.5.6: Autoruns Drivers list

9. Click the **KnownDLLs** tab to view all known DLLs that start automatically at system startup.

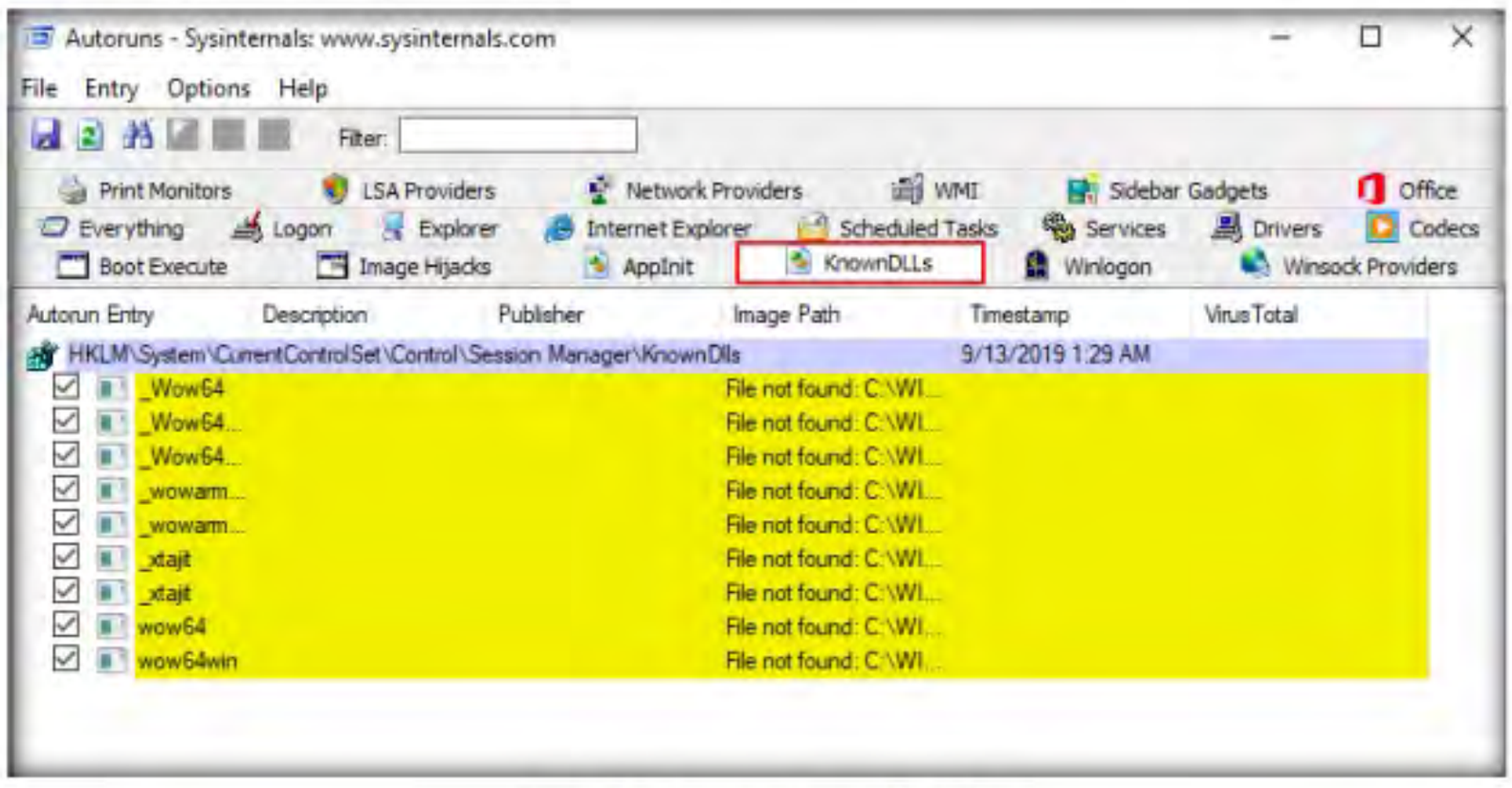


Figure 4.5.7: Autoruns Known DLL's list

10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.
12. Now, we will find out which applications or processes start when the system boots up using the WinPatrol tool.

TASK 5.2

Install WinPatrol

13. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**. Double-click **wpsetup.exe** to launch the setup.
14. If a **User Account Control** window appears, click **Yes**.
15. Follow the wizard-driven installation steps to install WinPatrol.
16. In the **Installation completed** wizard, make sure that the **Start the application** options is checked, and then click **Finish**. This will automatically launch the application.

WinPatrol

WinPatrol provides the user with 14 different tabs to help in monitoring the system and its files. This security utility gives the user a chance to look for programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate and malicious programs.

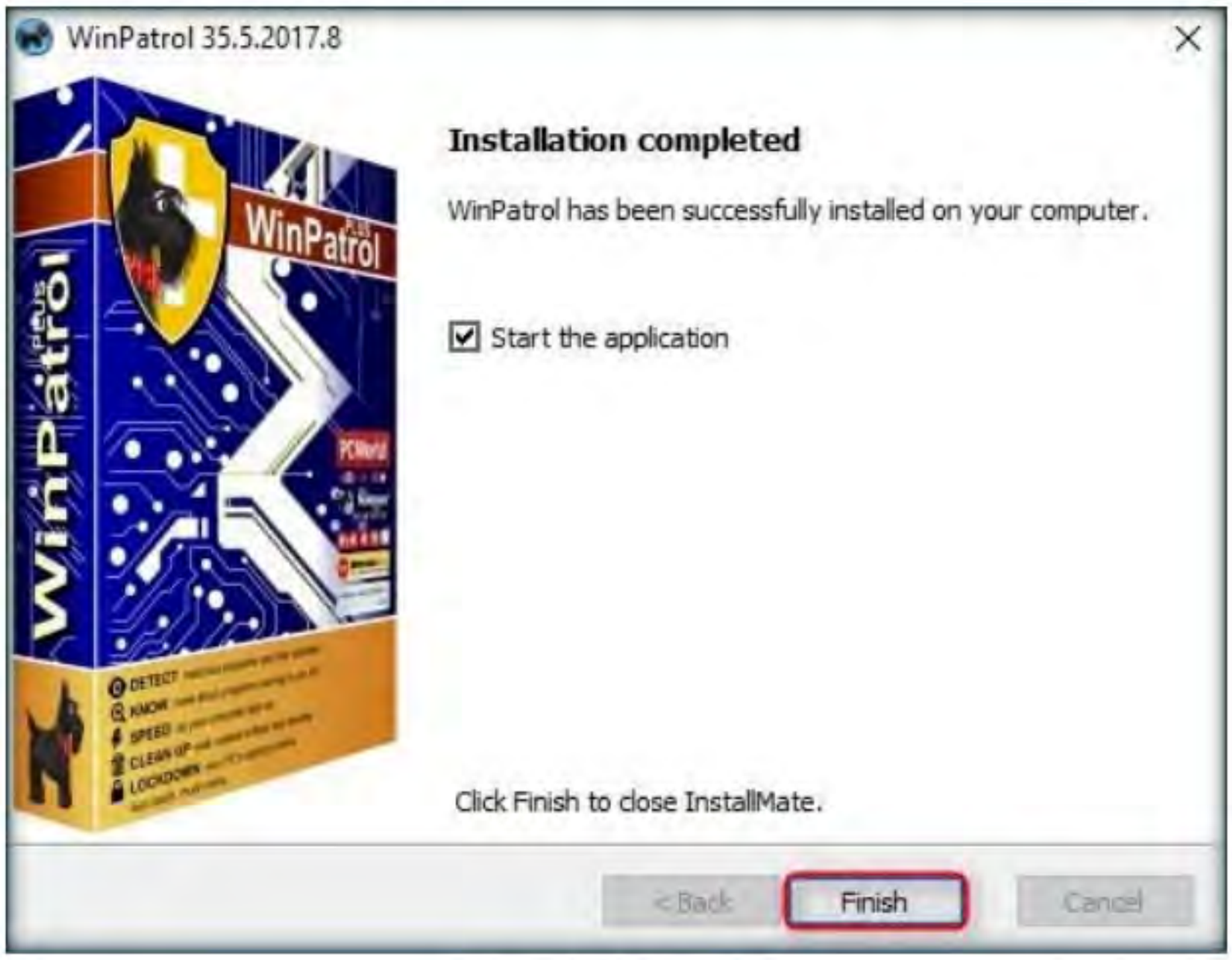


Figure 4.5.8: Installation completed

TASK 5.3

Monitor the System

17. The WinPartol application window appears with the **PLUS** tab open by default. Click the **Startup Programs** tab.
18. Select any program that affects your system bootup (here, **OneDrive**) and click **Disable**, as shown in the screenshot.

Note: The screenshot may differ from the image on the screen in your lab environment.

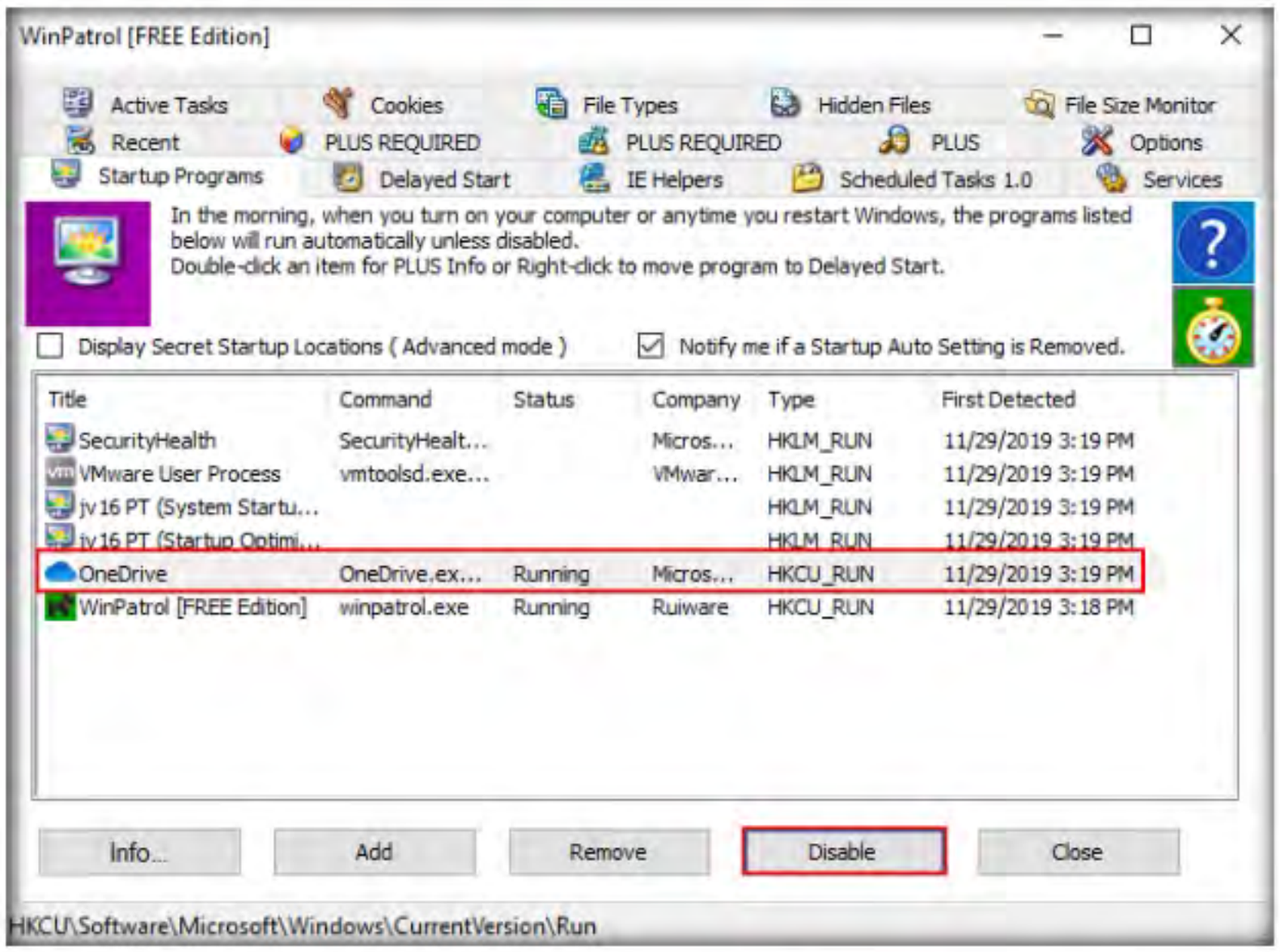


Figure 4.5.9: Startup programs tab

19. A popup appears, as shown in the screenshot. Click **Yes** to proceed.

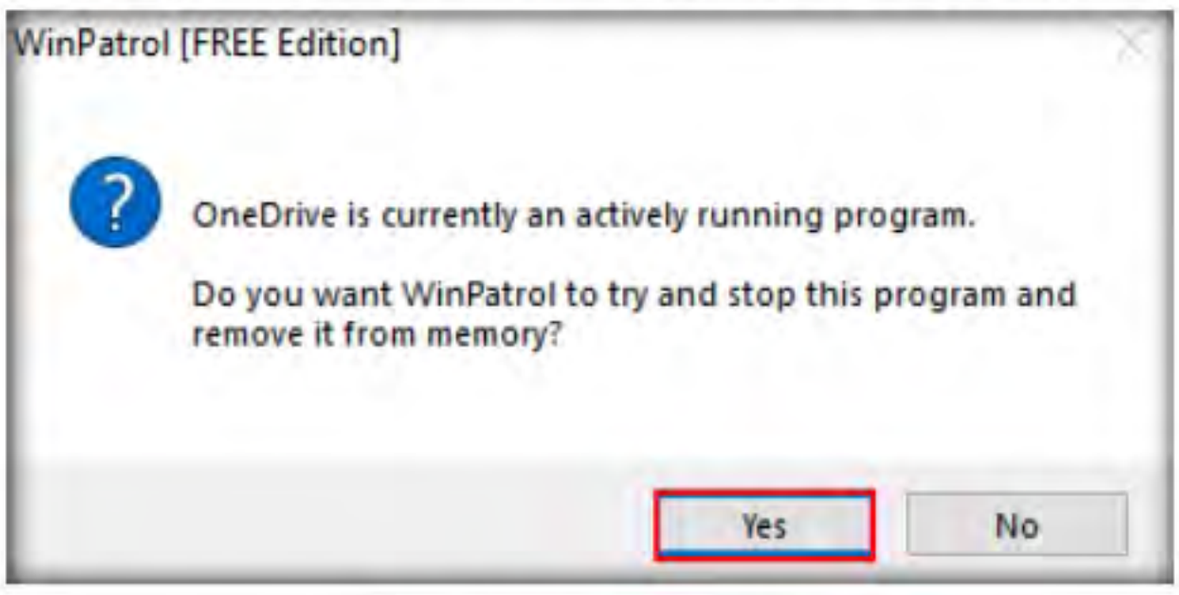


Figure 4.5.10: Confirmation prompt

20. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.
21. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here **Java(tm) Plug-In SSV Helper**), and then click **Remove**.

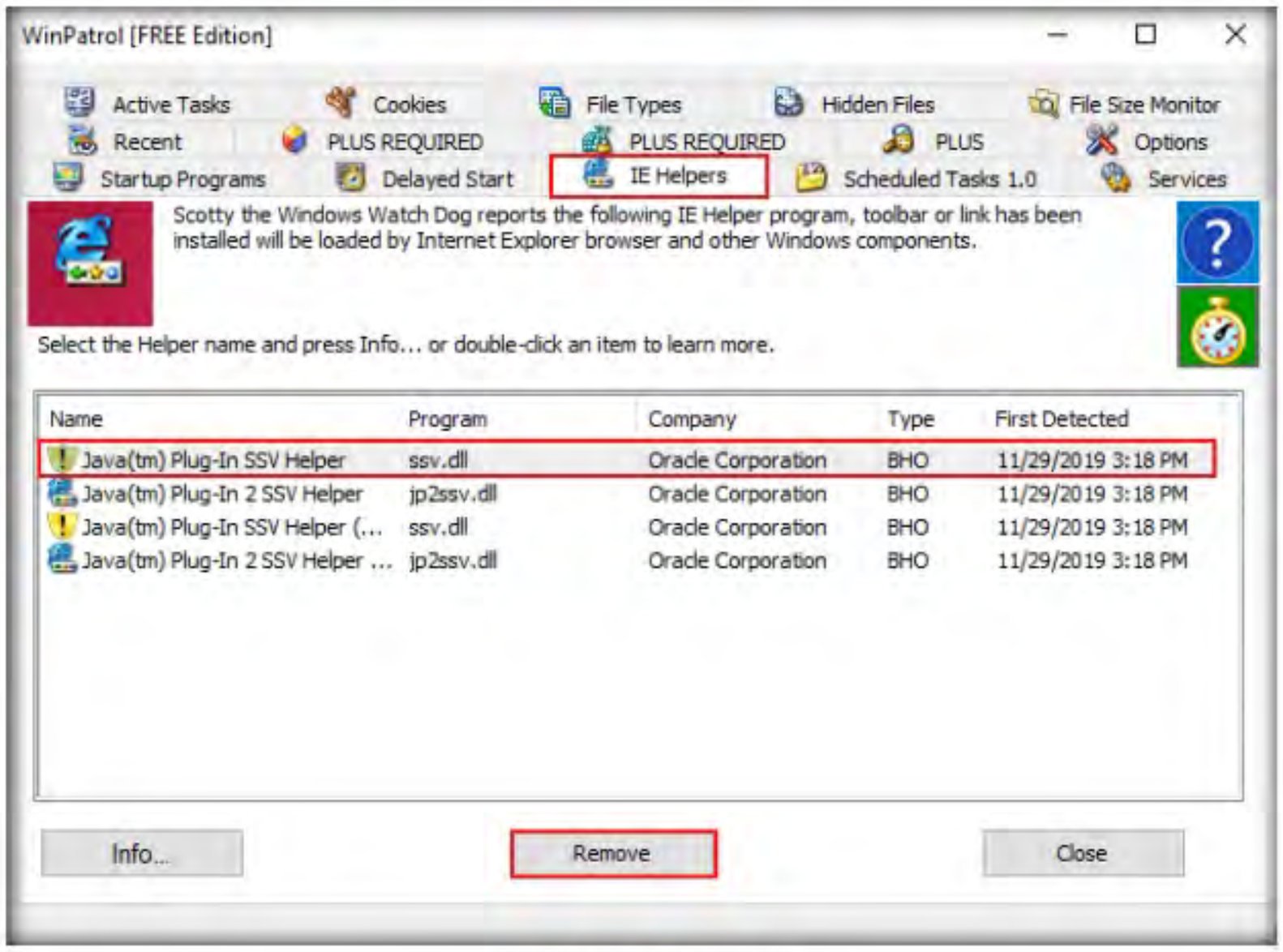


Figure 4.5.11: IE Helpers tab

22. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info...**, as shown in the screenshot.

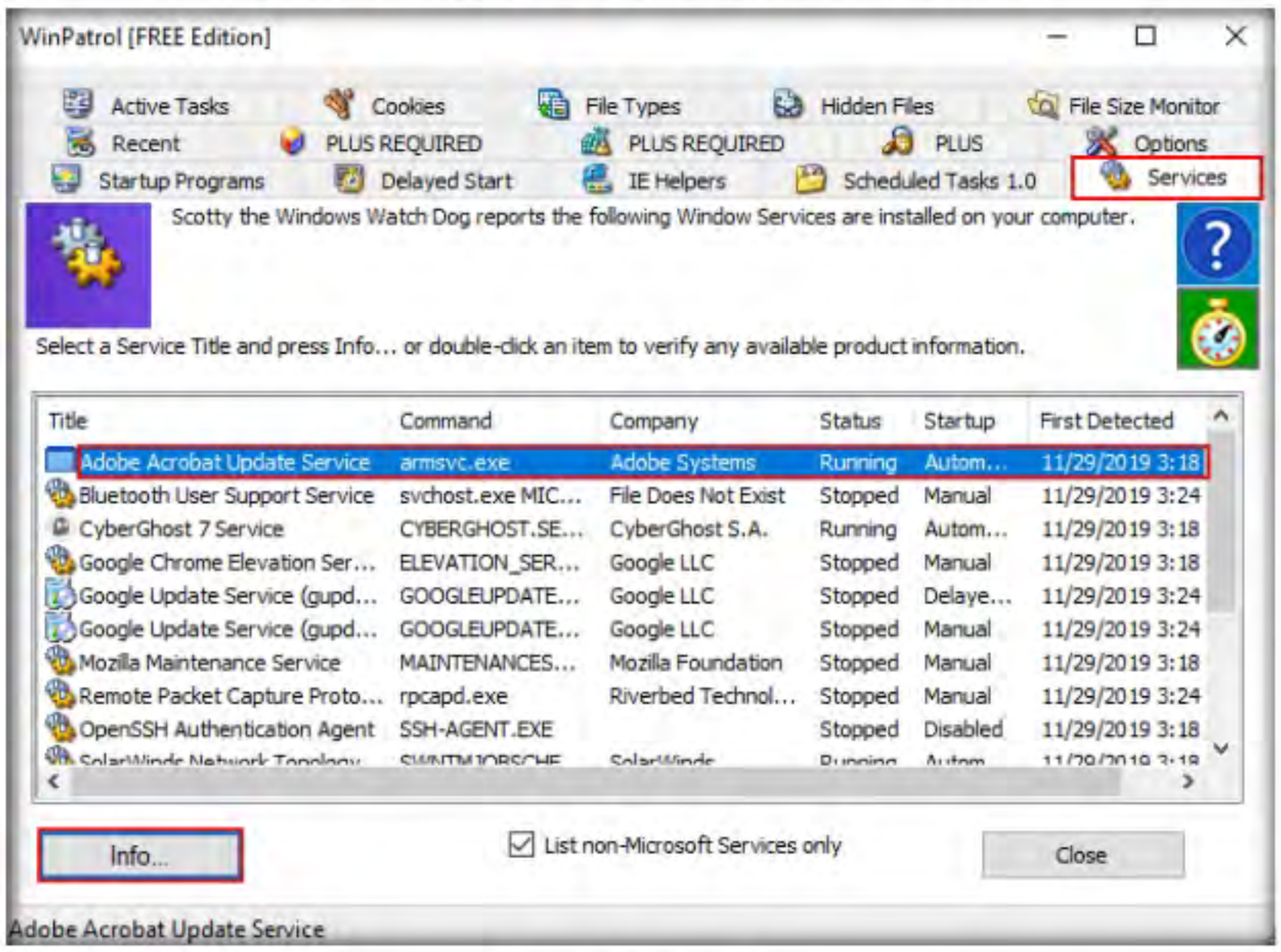


Figure 4.5.12: Services tab

23. A window showing the service information appears. To disable a service, select **Disabled** from the drop-down list and click **Apply**, as shown in the screenshot. Click **Close** to exit the window.

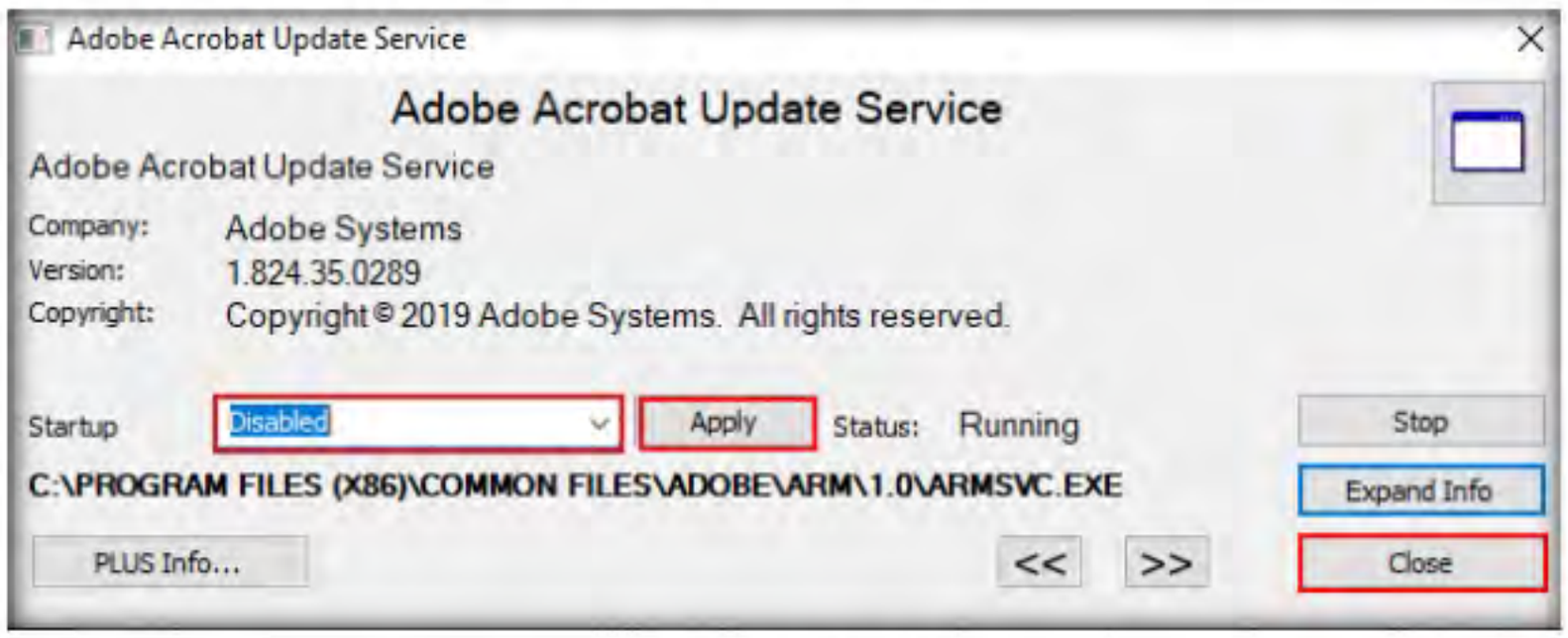


Figure 4.5.13: Service details

24. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info...** to view the available information.

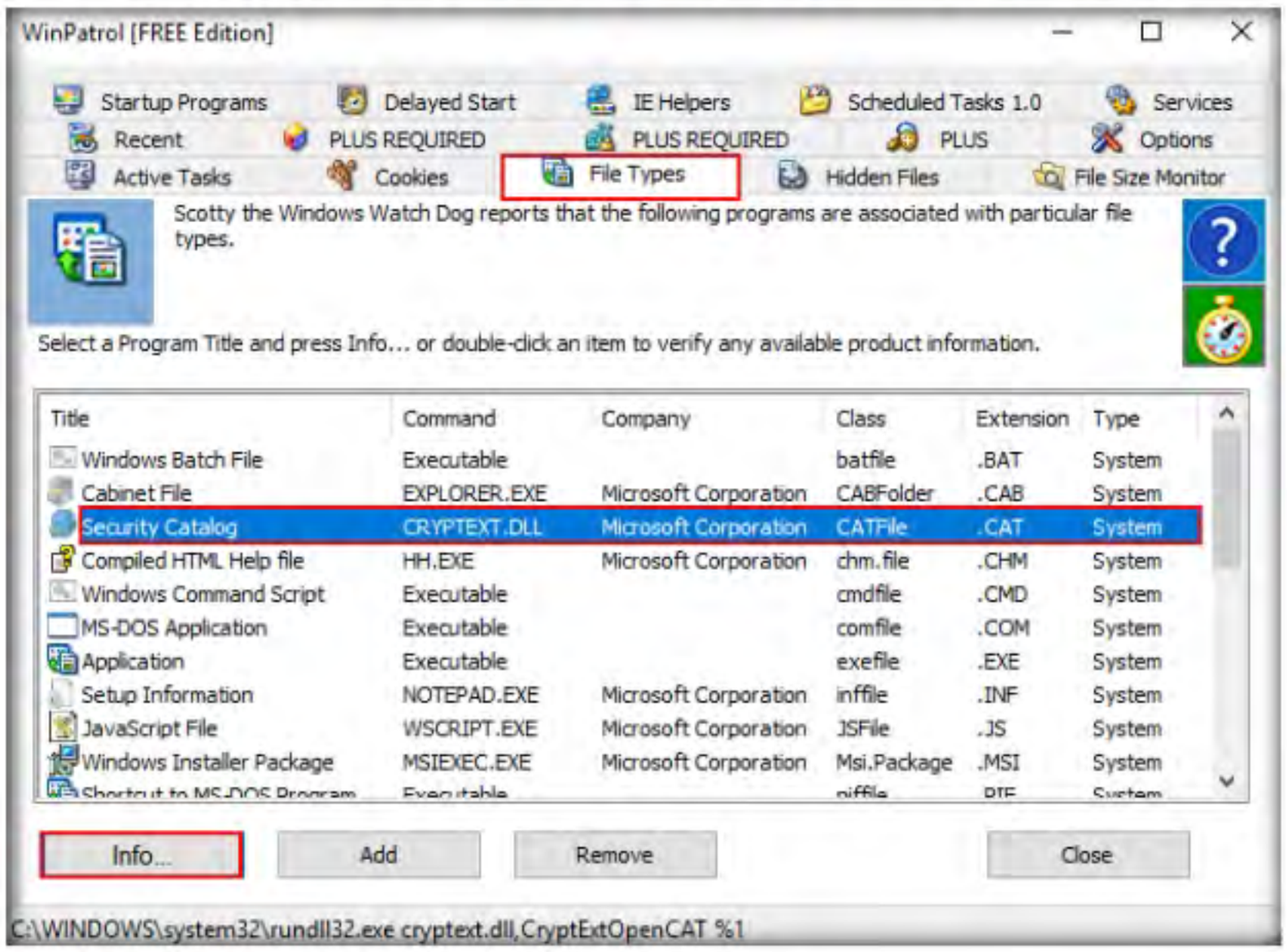


Figure 4.5.14: File Types tab

25. The **Security Catalog** window appears, as shown in the screenshot. Click **Expand Info** to view the full info about the program.

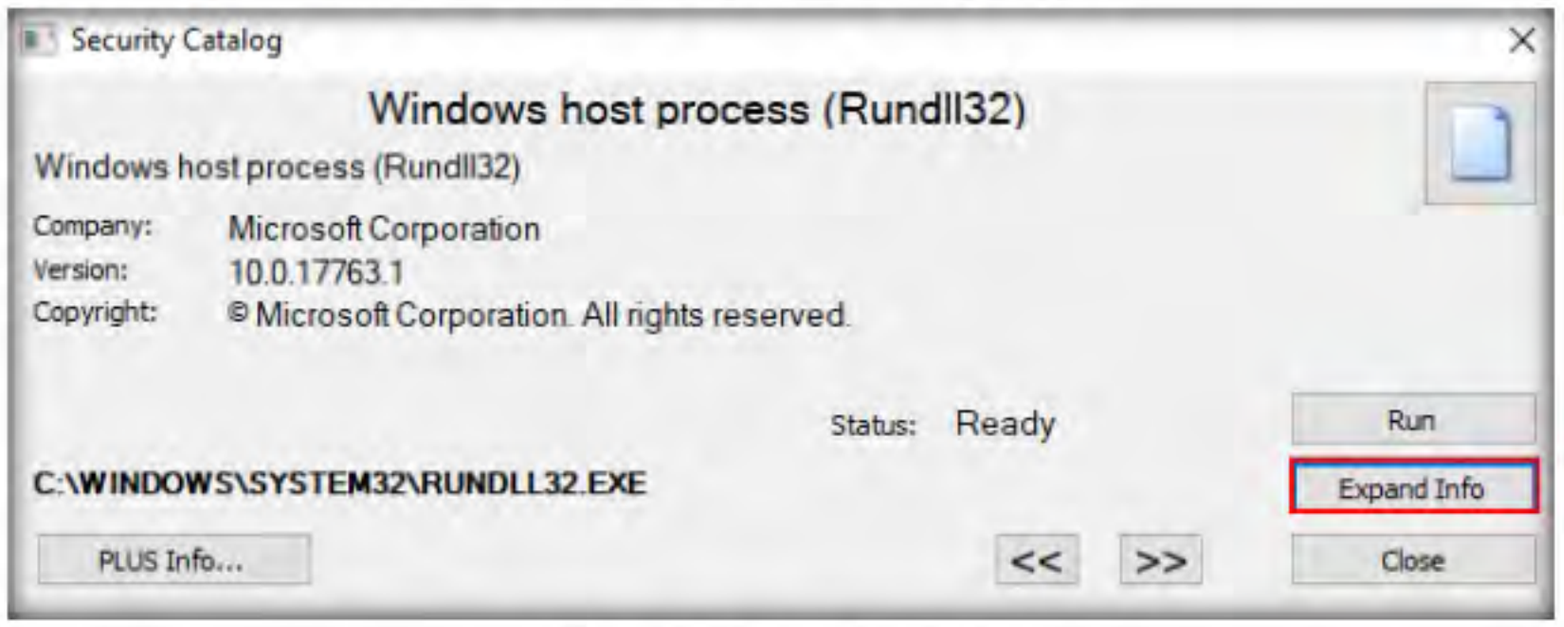


Figure 4.5.15: Security catalog window

26. The expanded view shows all information related to the program and its associated file, as demonstrated in the screenshot. Analyze the info and close the window.

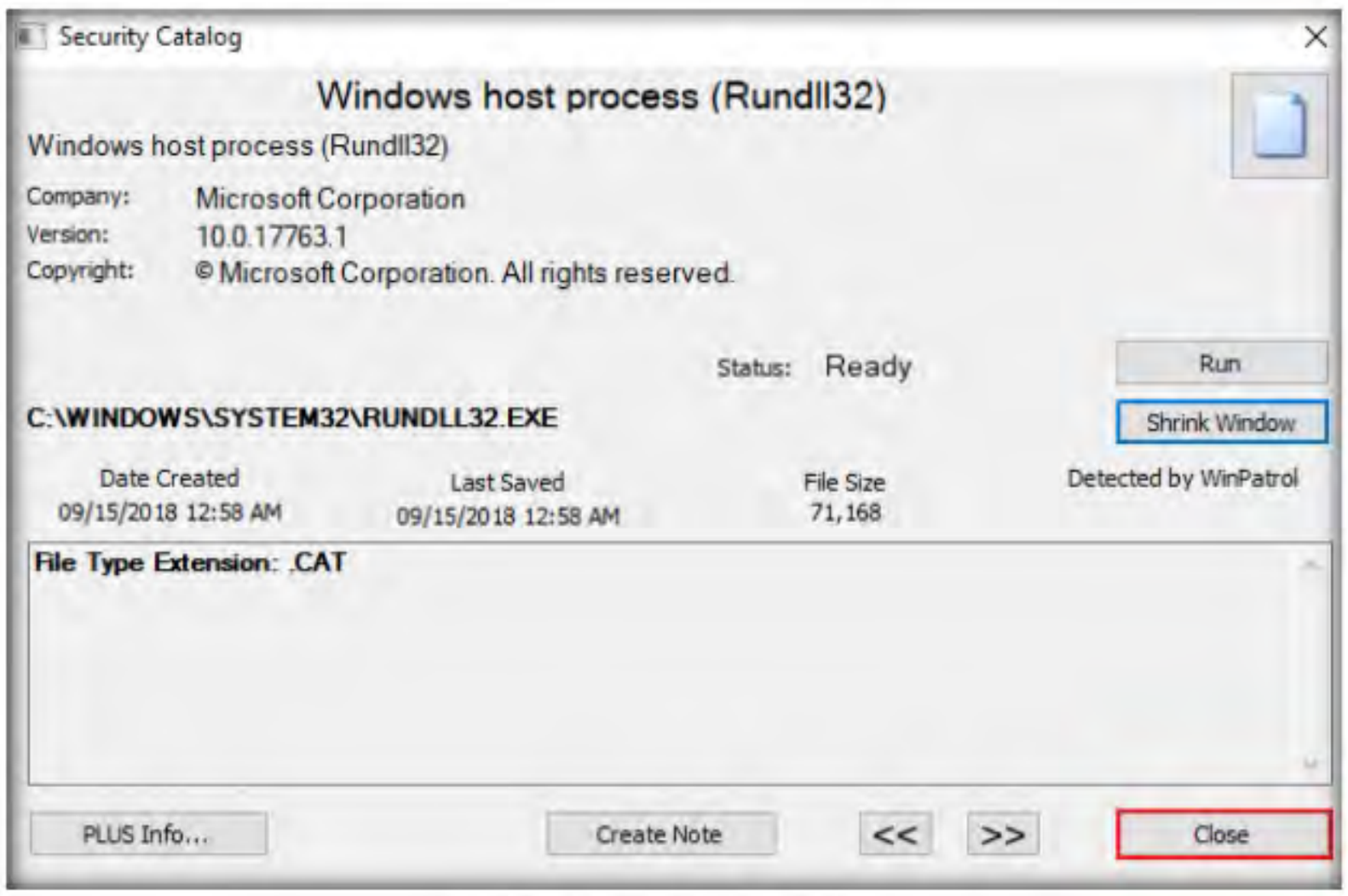


Figure 4.5.16: Security catalog window

27. Now, switch to the **Active Tasks** tab to view the current tasks running on your computer. Select any task (here, **PROXYSWITCHER**) and click **Kill Task** to end the task, as shown in the screenshot.

You can also use other Windows startup programs monitoring tools such as **Autorun Organizer** (https://www.chemtable.com), **Quick Startup** (https://www.glarysoft.com), **StartEd Pro** (http://www.outertech.com), or **Chameleon Startup Manager** (http://www.chameleon-managers.com) to perform startup programs monitoring.

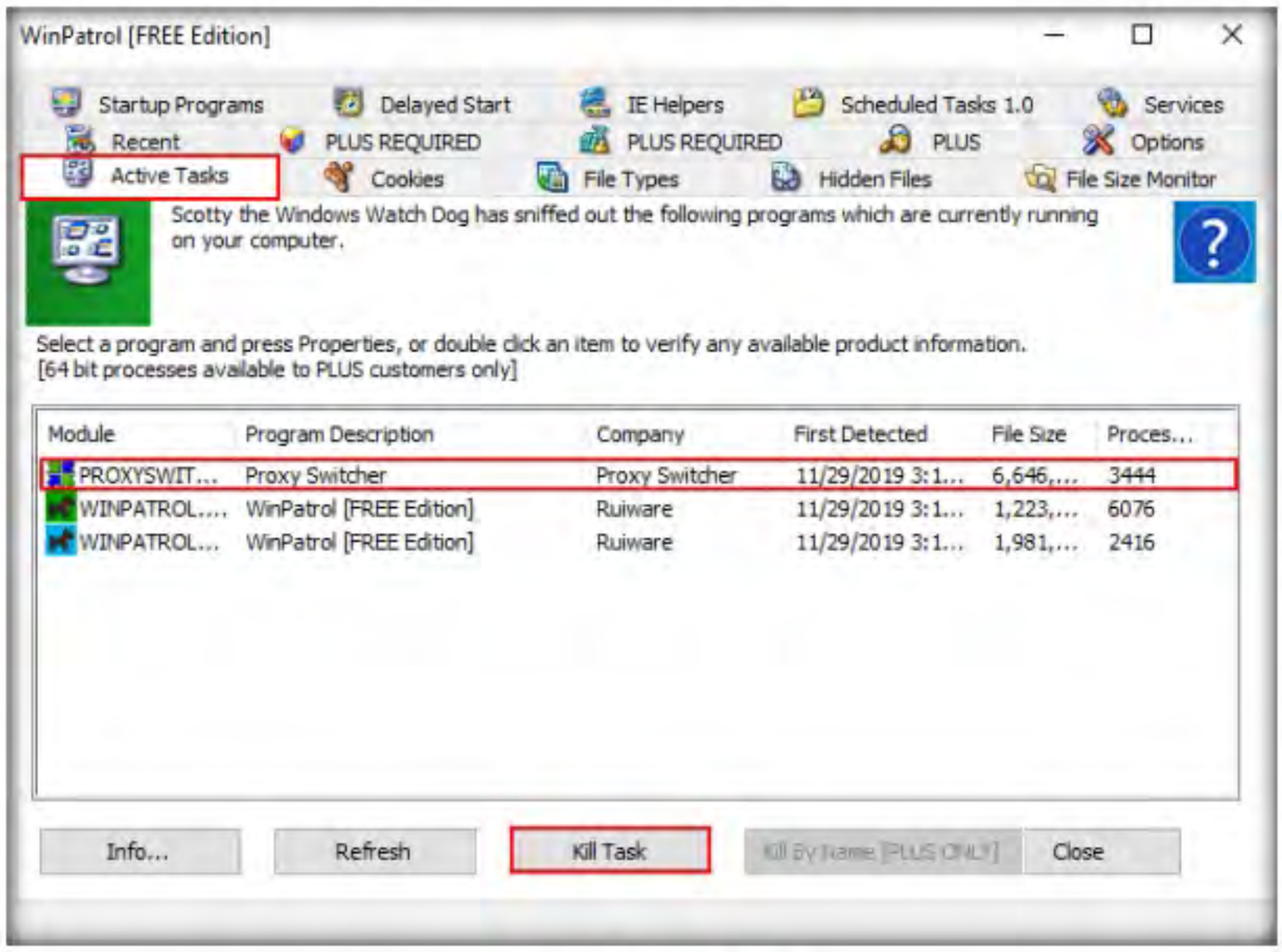


Figure 4.5.17: Active tasks tab

28. By examining all these tabs, you can find any unwanted process or application running on the machine when the system boots up and manually stop or delete them.
29. Close all open windows on the **Windows 10** virtual machine.

TASK 6 Perform Installation Monitoring using Mirekusoft Install Monitor

Here, we will use the Mirekusoft Install Monitor tool to detect hidden and background installations.

TASK 6.1

Install Mirekusoft Install Monitor

When the system or users install or uninstall any software application, there is a chance that it will leave traces of the application data on the system. Installation monitoring help to detect hidden and background installations that malware performs.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor** and double-click **SetupInstallMonitor.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

2. Follow the installation steps to install **Mirekusoft Install Monitor**.
3. The **Setup Successful** wizard appears; click **Launch**.

Figure 4.6.1: Mirekusoft Install Monitor Setup Successful Wizard

Mirekusoft Install Monitor automatically monitors what gets placed on your system and allows you to uninstall it completely. Install Monitor works by monitoring what resources such as file and registry, are created when a program is installed. It provides detailed information about the software installed, including how much disk space, CPU, and memory your programs are using. It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

4. If a **User Account Control** window appears, click **Yes**.
5. The **Mirekusoft Install Monitor** main window appears, along with a **Welcome** pop-up, click **OK**. Click **Skip scan** in the **Home** tab.

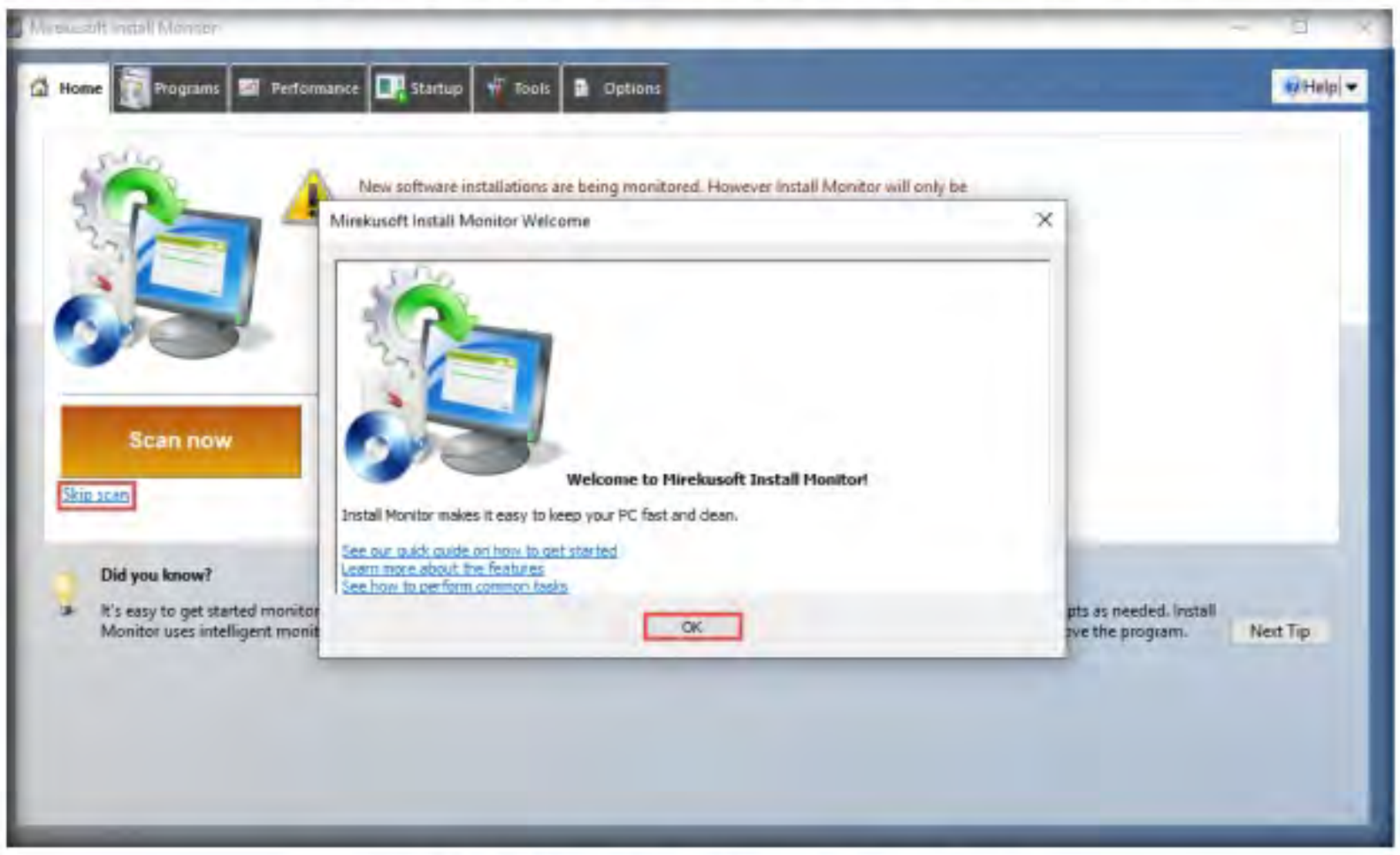


Figure 4.6.2: Mirekusoft Install Monitor Welcome Window

TASK 6.2

View the Result

6. Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

Note: The **WinPatrol** pop-up appears; click **Reject Change**.

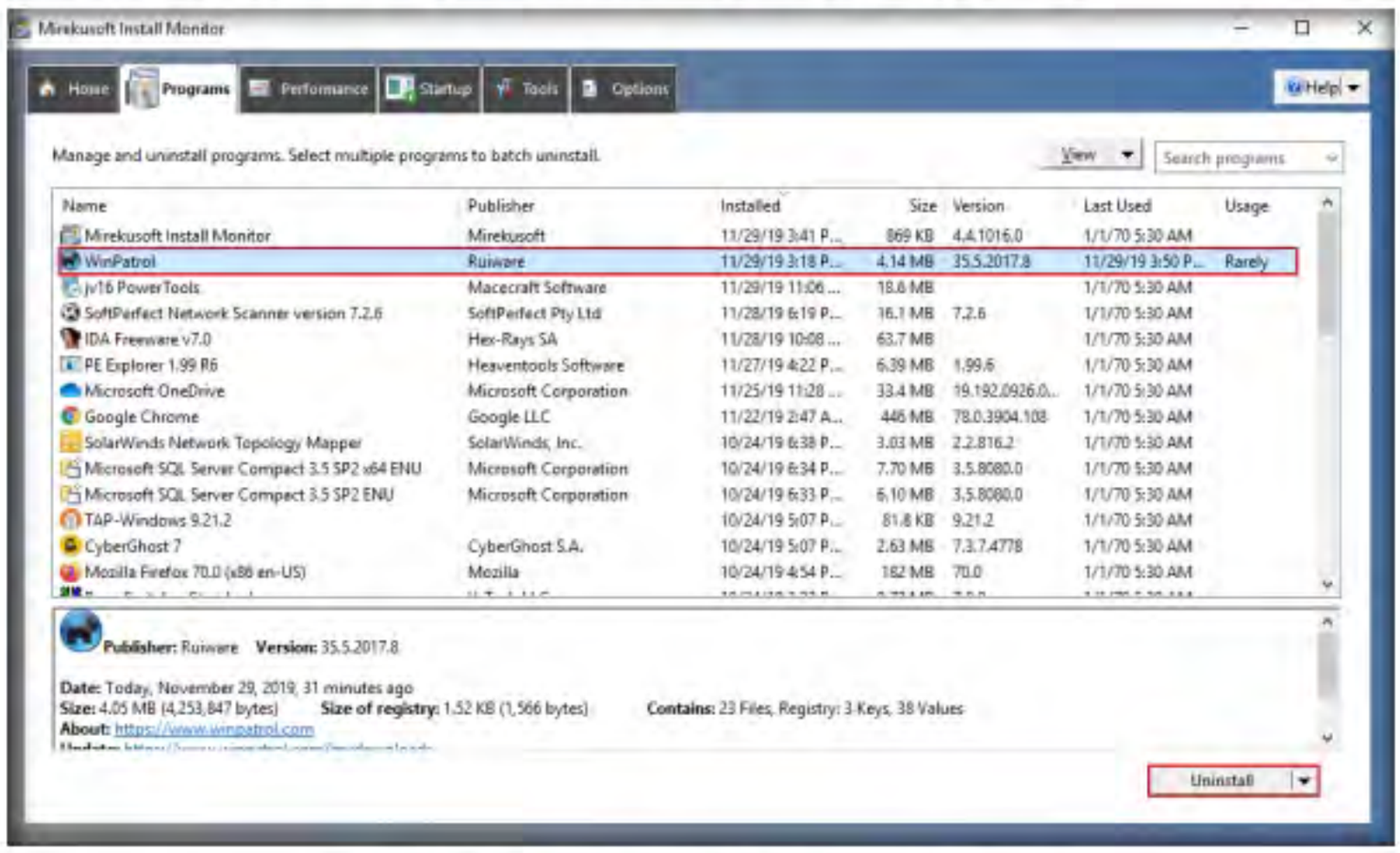


Figure 4.6.3: Mirekusoft Install Monitor Uninstalling Program

7. While uninstalling the application, a selected program pop-up appears, click **Yes** in all the **WinPatrol** pop-ups.

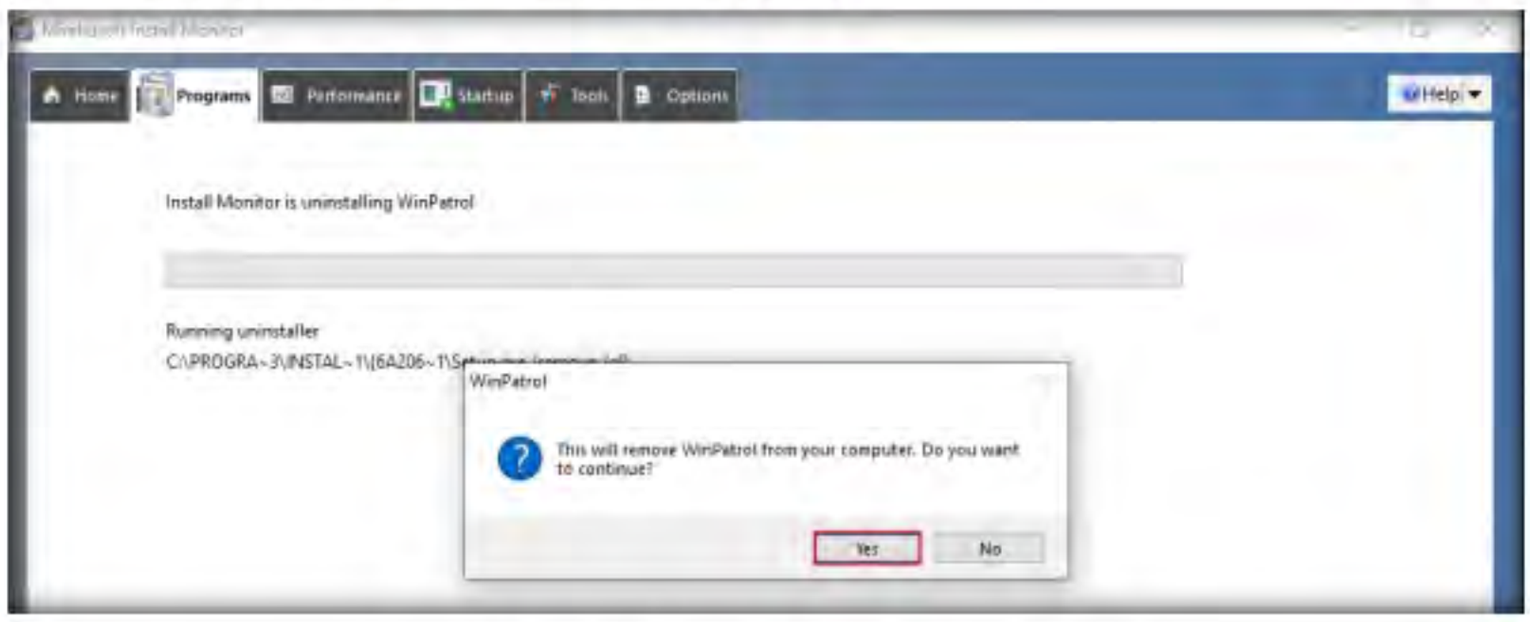


Figure 4.6.4: Mirekusoft Install Monitor Program Confirmation

8. The **selected application is uninstalled from your computer** pop-up appears; click **OK**.

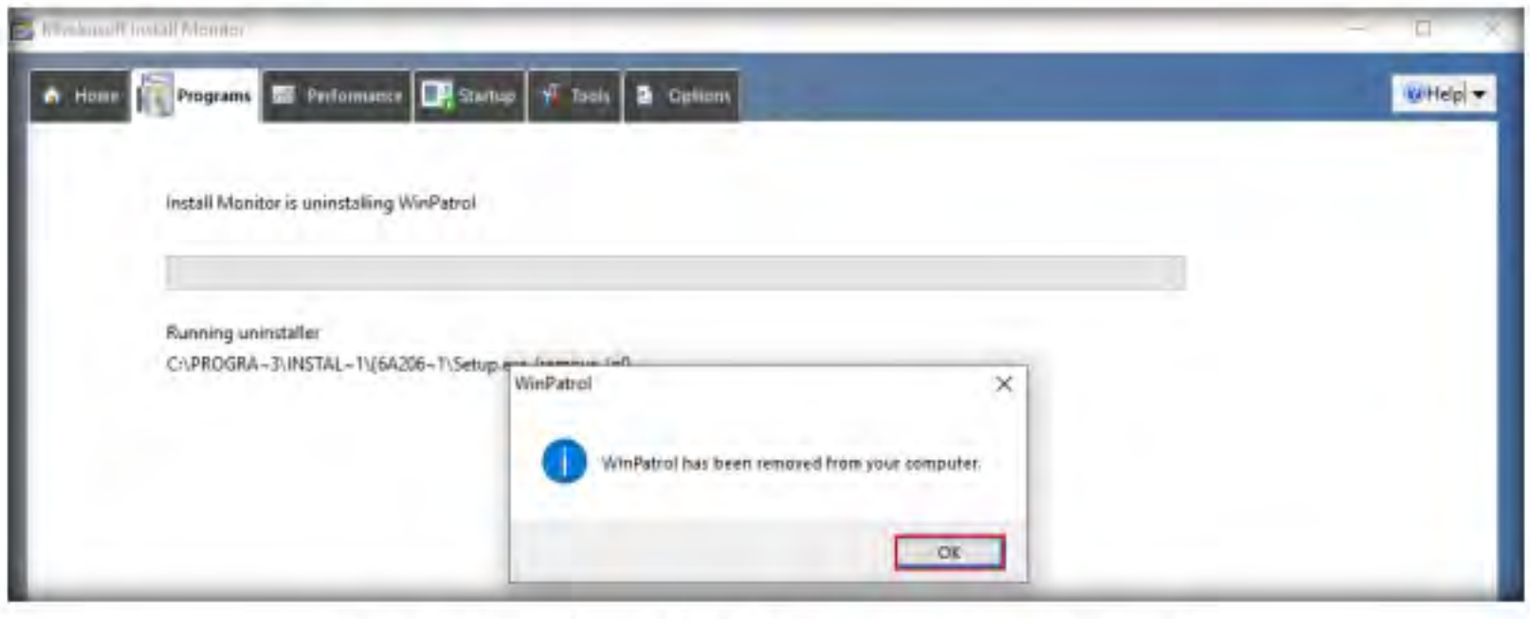


Figure 4.6.5: Mirekusoft Install Monitor Successfully Uninstalled

9. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.

Figure 4.6.6: Mirekusoft Install Monitor Cleanup Confirmation

10. The **Confirm Cleanup** pop-up appears; click **Cleanup**. This will delete all the supported files for the related application that you have uninstalled from your computer.

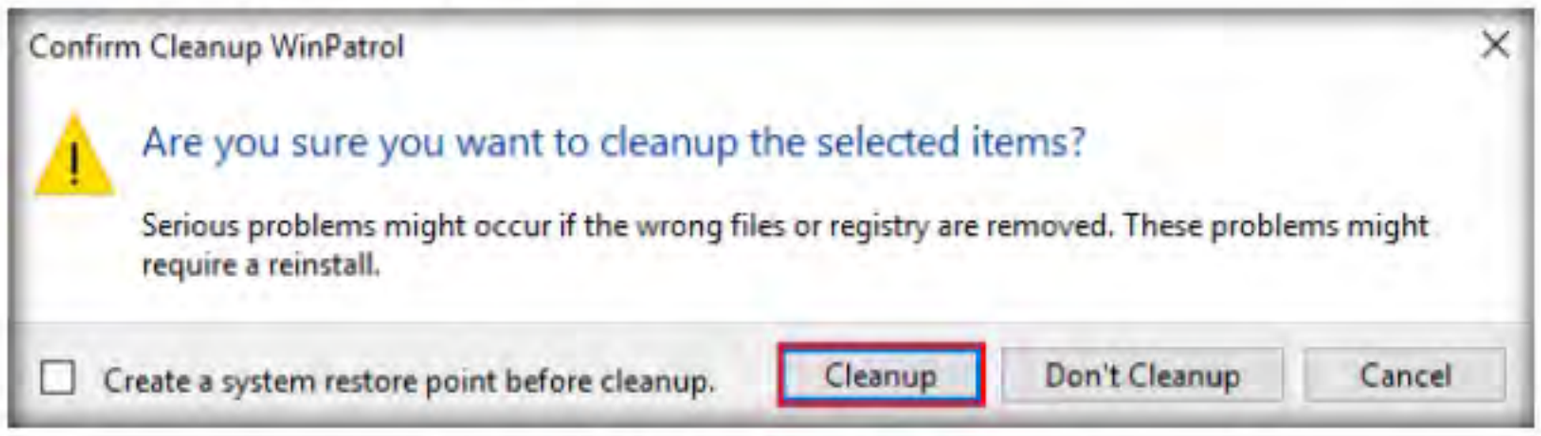


Figure 4.6.7: Mirekusoft Install Monitor Cleanup

11. The selected application is uninstalled from your computer. Click the **Performance** tab to view and terminate currently running programs.
12. Select any program from the list and click **End Program**. In this lab, we are choosing **Adobe Acrobat Update Service**.

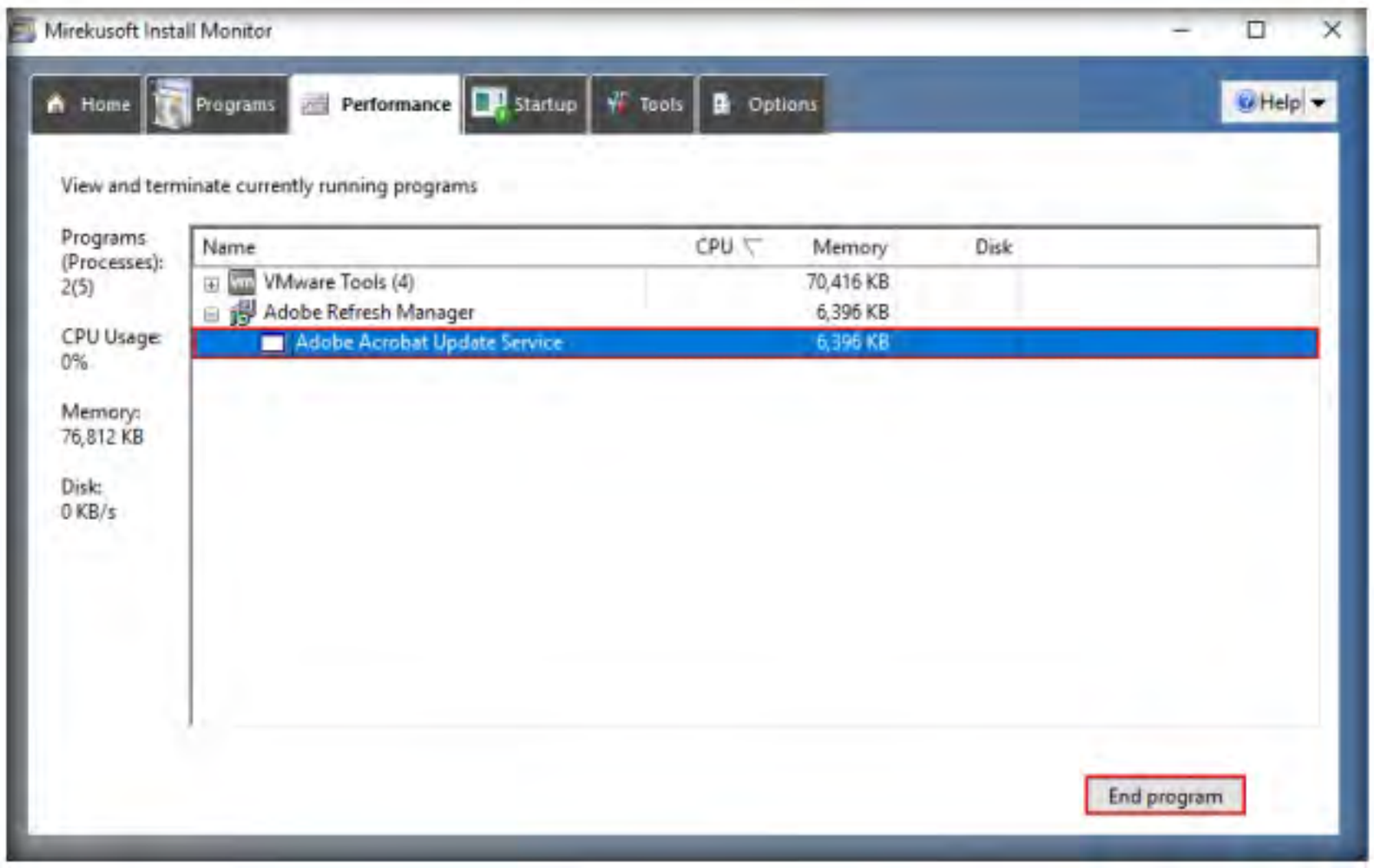


Figure 4.6.8: Mirekusoft Install Monitor Performance Tab

13. The **End Program** pop-up appears for the selected program; click **Yes**.

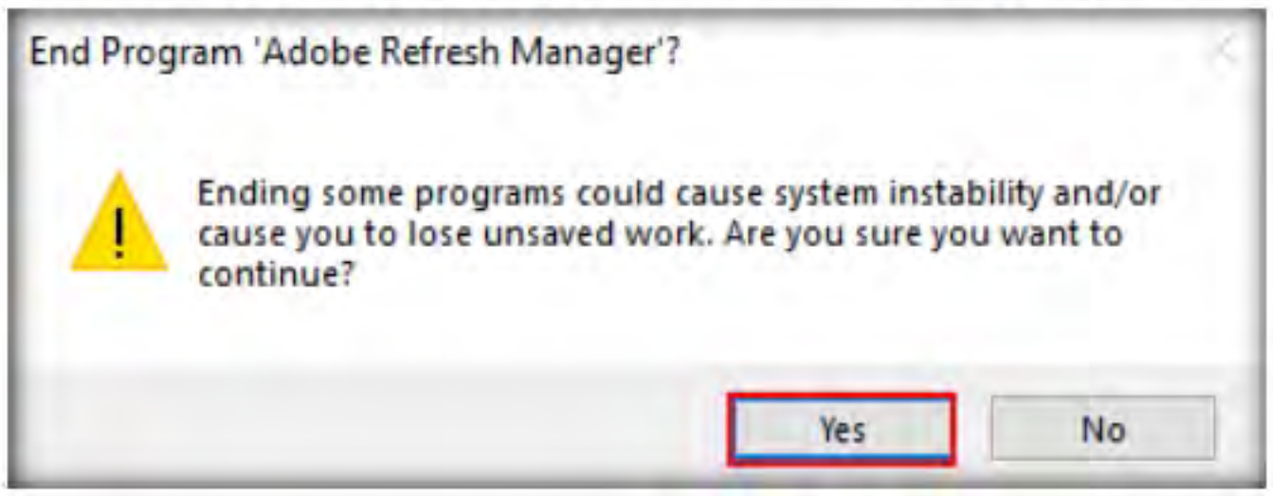


Figure 4.6.9: Mirekusoft Install Monitor End Program Confirmation

14. This will end the running program.
15. Click the **Startup** tab to view the programs that run automatically on Windows Startup.
16. In this lab, Mirekusoft Install Monitor has not detected startup programs. If the program does detect them, choose the application that you want to disable on startup, and click **Disable**.
17. You can restart the machine to detect the startup programs.

You can also use other installation monitoring tools such as **SysAnalyzer** (https://www.aldeid.com), **Advanced Uninstaller PRO** (https://www.advanceduninstaller.com), **REVO UNINSTALLER PRO** (https://www.revouninstaller.com), or **Comodo Programs Manager** (https://www.comodo.com) to perform installation monitoring.

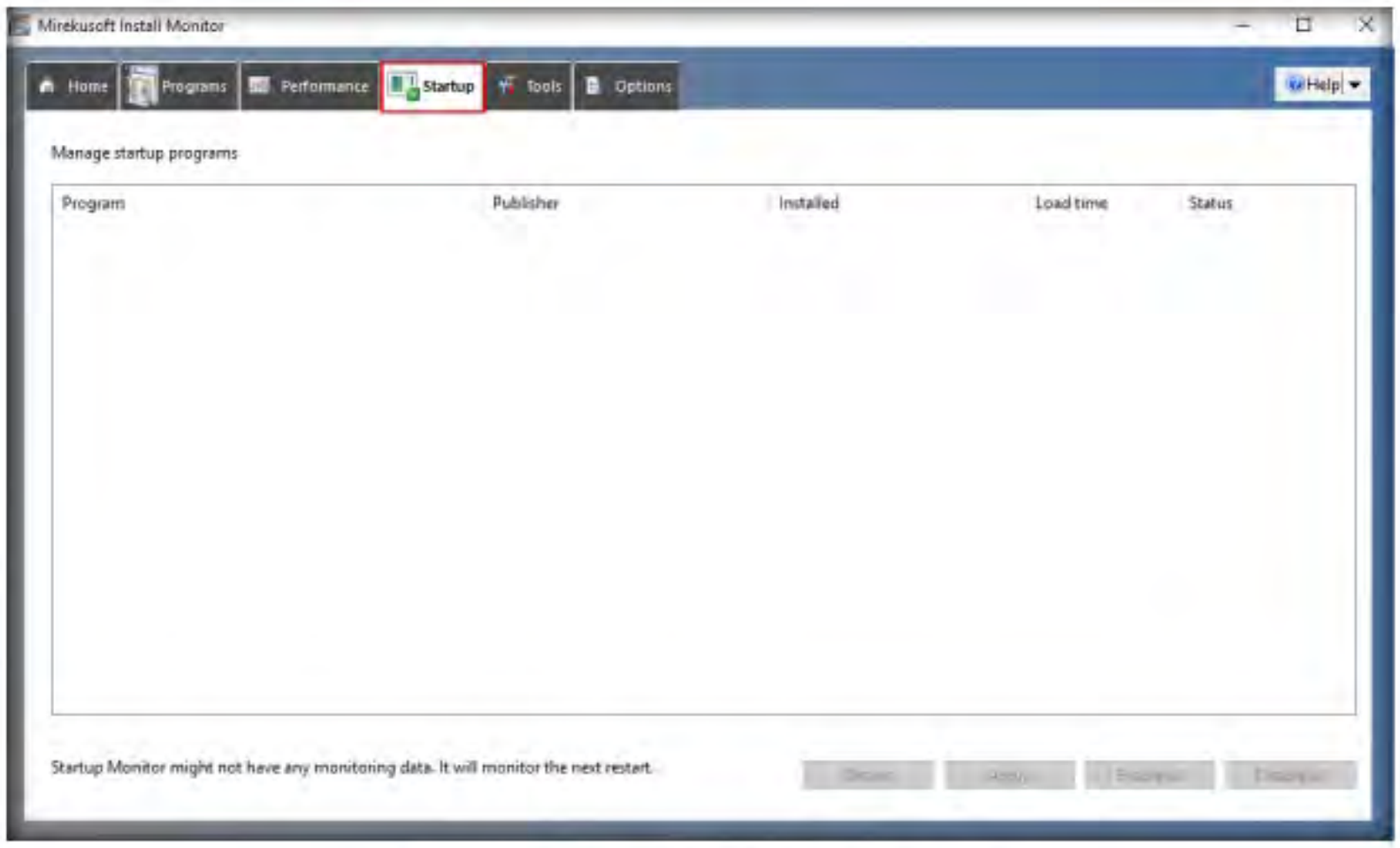


Figure 4.6.10: Mirekusoft Install Monitor Startup Tab

18. This is how to monitor a Windows machine using Mirekusoft Install Monitor. Close all applications.

TASK 7

Perform Files and Folder Monitoring using PA File Sight

1. Before starting this task, Launch and log in to the **Windows Server 2016** virtual machine using the credentials **Administrator** and **Pa$$w0rd**.

TASK 7.1

Install and Launch PA File Sight

2. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **filesightultra.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

3. The **Select Setup Language** pop-up appears; choose your preferred language, and then click **OK**.
4. Follow the default installation steps to install **PA File Sight**.
5. **Completing the PA File Sight Ultra Setup Wizard** appears; make sure that both the **Start the PA File Sight Ultra monitoring service** and the **Launch the PA File Sight Ultra Console** options are checked, and click **Finish**.
6. This will run the PA File Sight service and automatically launch the application.

Malware can modify system files and folders to save information in them. You should be able to find the files and folders that malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware plans to execute on a specific schedule.

Figure 4.7.1: PA File Sight Installation Completed

An ethical hacker or penetration tester must scan the system for suspicious files and folders using file and folder monitoring tools such as PA File Sight to detect any malware installed and any system file modifications.

PA File Sight is a protection and auditing tool. It detects ransomware attacks coming from a network and stops them.

7. The **PA File Sight Console** window appears. By default, the **Local host** radio button is selected; click **OK**.

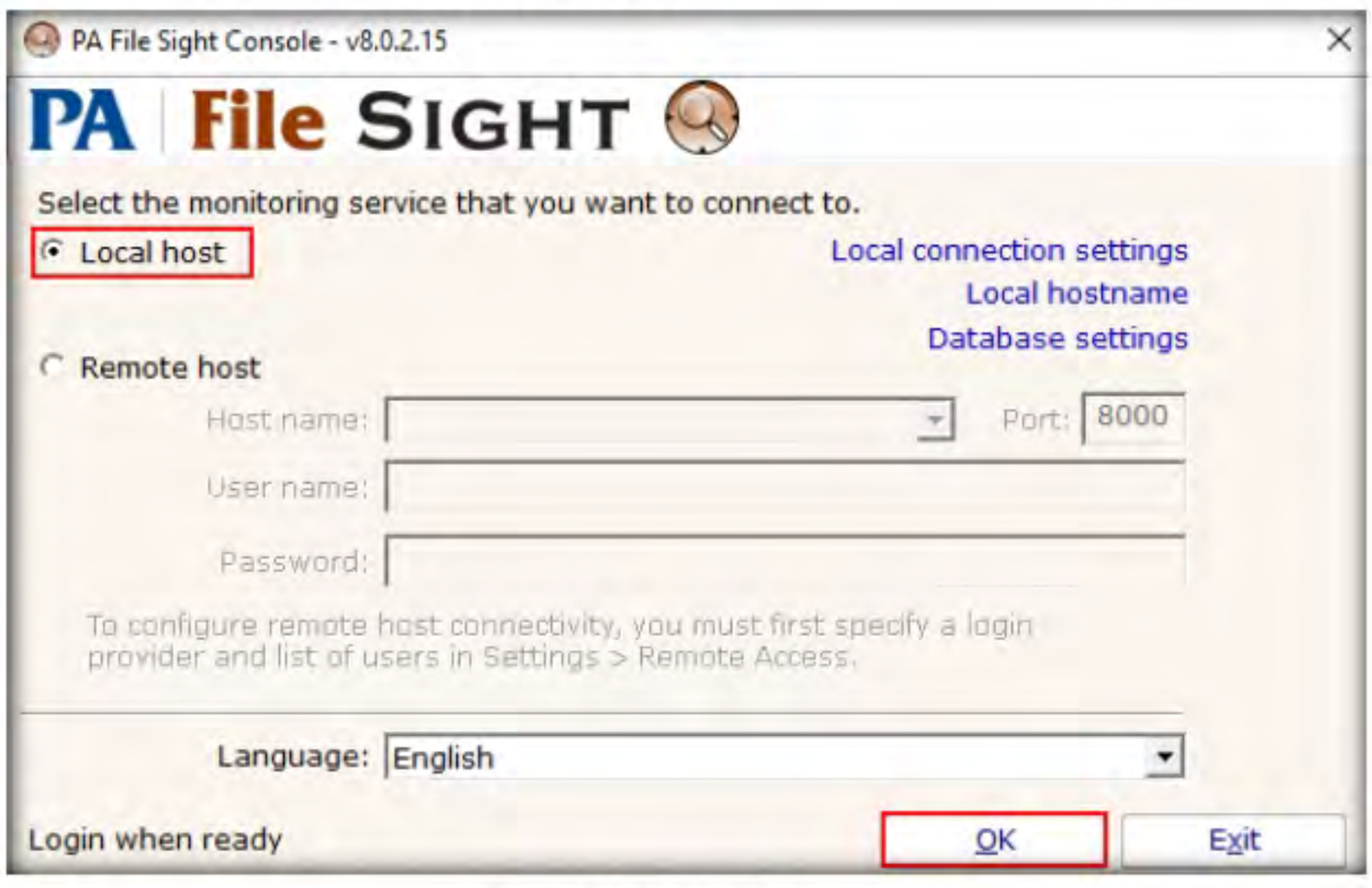


Figure 4.7.2: PA File Sight Console

Features:

- Compromised computers are blocked from reaching files on other protected servers on the network
- Detects users copying files and optionally blocks access
- Real-time alerts allow the appropriate staff to investigate immediately
- Audits who is deleting, moving, and reading files

8. The **PA File Sight Ultra Console** main window appears.

Note: If a **Start Wizard** window appears, close it.

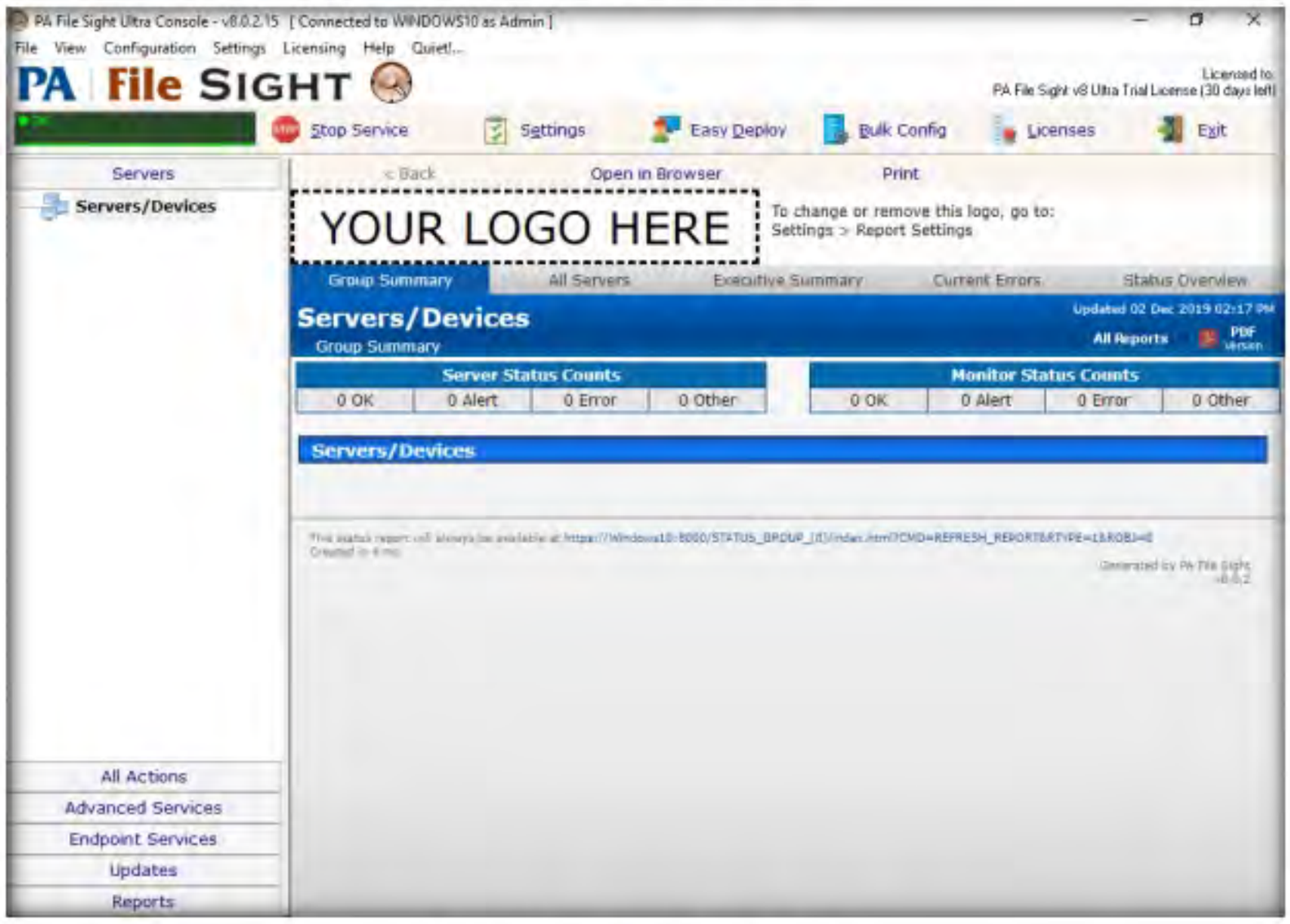


Figure 4.7.3: PA File Sight Main Window

TASK 7.2

Install Satellite Monitoring Service

9. Switch to the **Windows Server 2016** virtual machine. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **filesightultra.exe**.
10. The **Select Setup Language** pop-up appears; choose your preferred language and click **OK**.
11. Click the **Next** button until you see the **Select Components** wizard.
12. In the **Select Components** wizard, uncheck the **Central Monitoring Service** and **Console User Interface (configure all Services)** options, and check the **Satellite Monitoring Service (reports to Central Monitoring Service)** option; then, click **Next**.

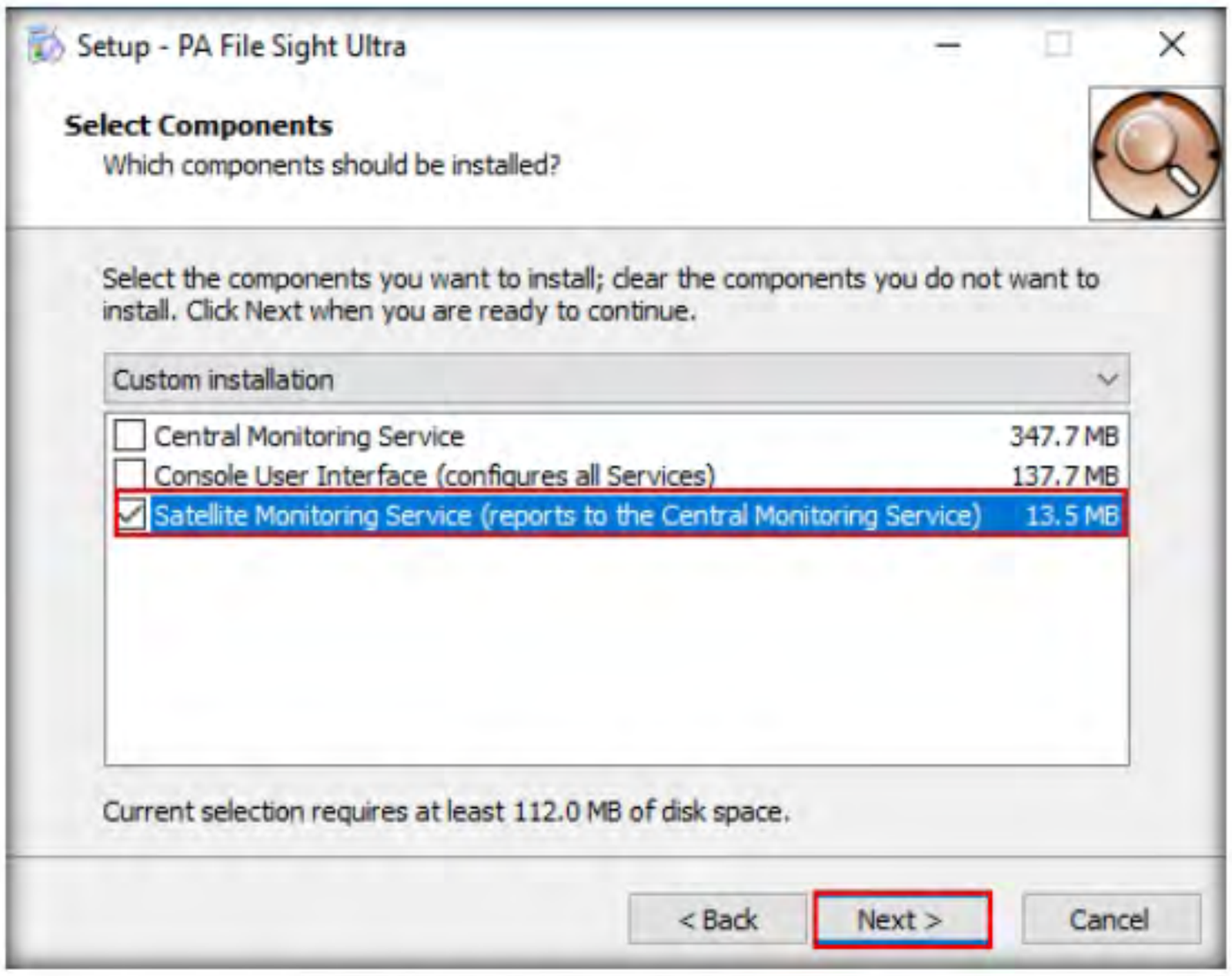


Figure 4.7.4: PA File Sight Satellite Monitoring Service

13. Follow the wizard-driven installation steps to install the application.
14. In the final step of the installation, make sure that the **Start the PA File Sight Ultra Satellite Monitoring Service** and **Configure the PA File Sight Ultra Satellite service** options are checked; then, click **Finish**.

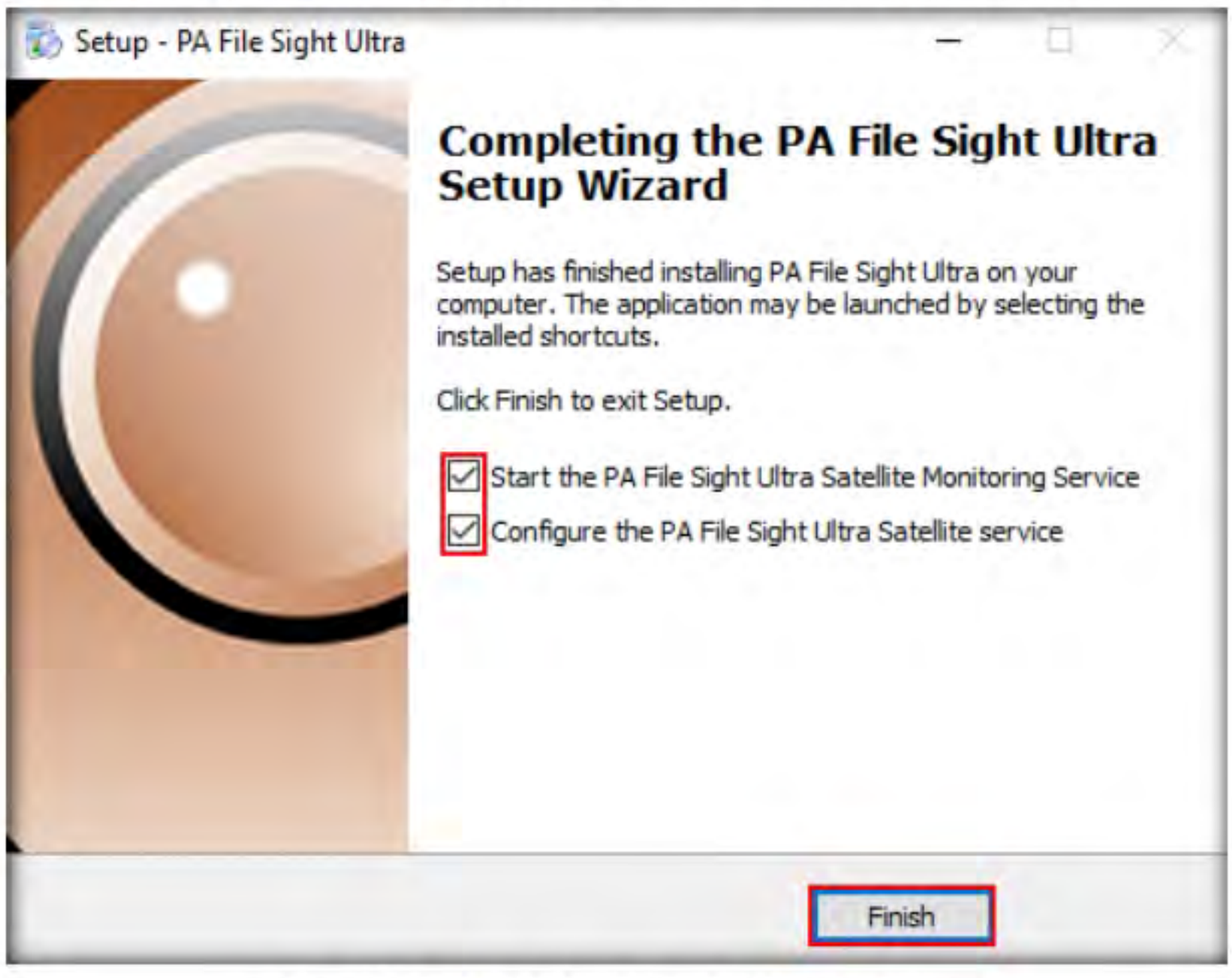


Figure 4.7.5: PA File Sight Installing Satellite Monitoring Service

TASK 7.3

Configure Satellite Monitoring Service

15. The **Configure Satellite Monitoring Service** window appears; type the **Windows 10** IP address into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

Note: In this task, the IP address of the **Windows 10** machine is **10.10.10.10**. the IP address may vary in your lab environment.

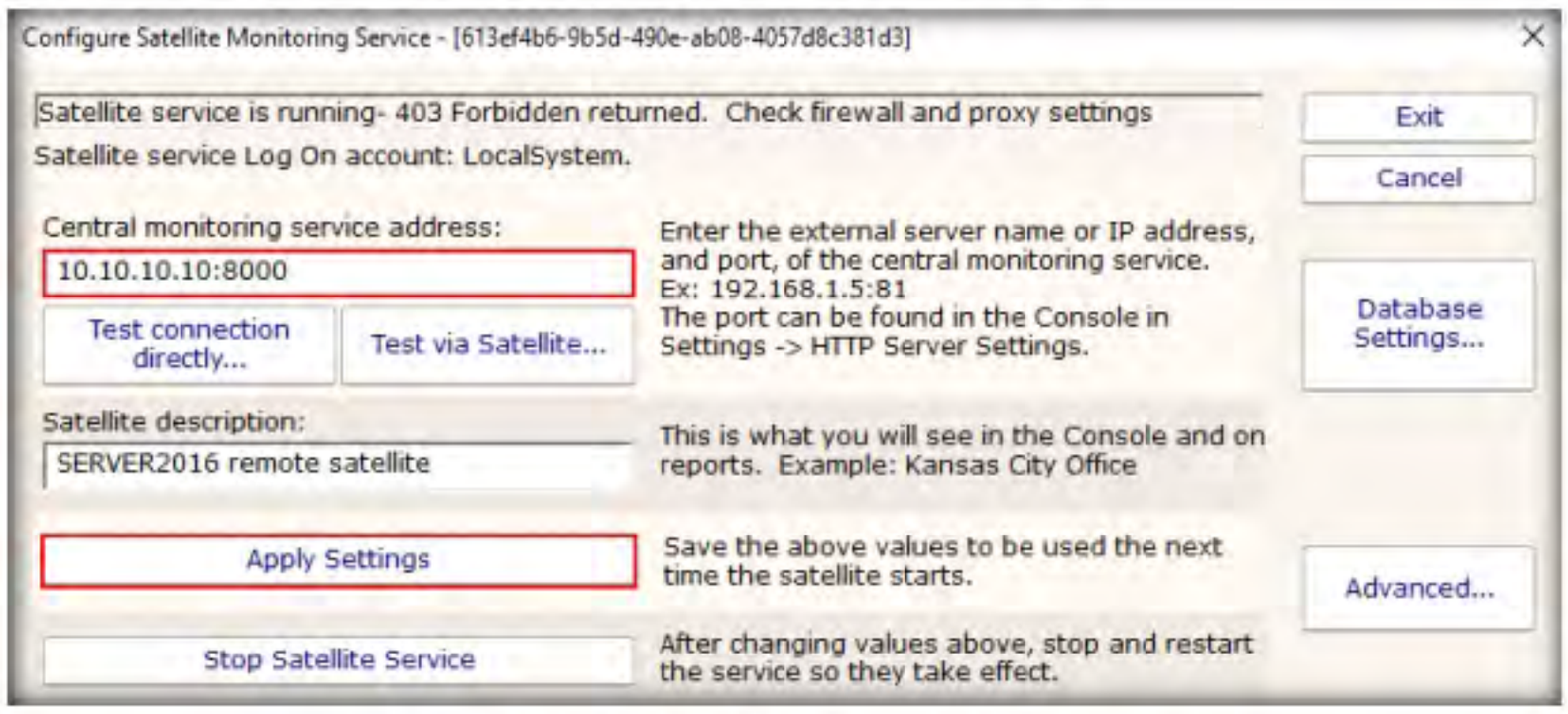


Figure 4.7.6: PA File Sight Satellite Service Configuration

16. Click **Stop Satellite Service** to stop the satellite service.

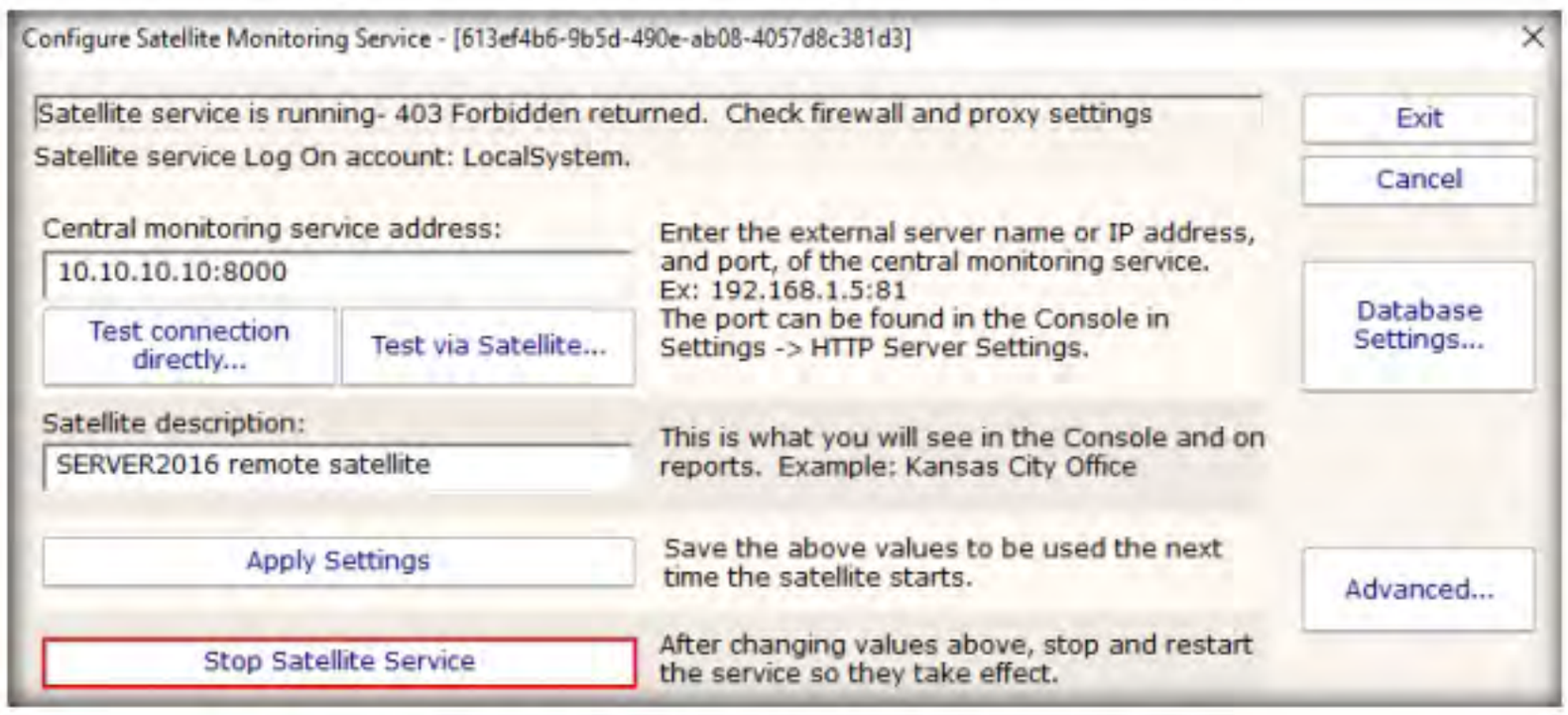


Figure 4.7.7: PA File Sight Stopping Satellite Service

17. Once the service is stopped, click **Start Satellite Service**.

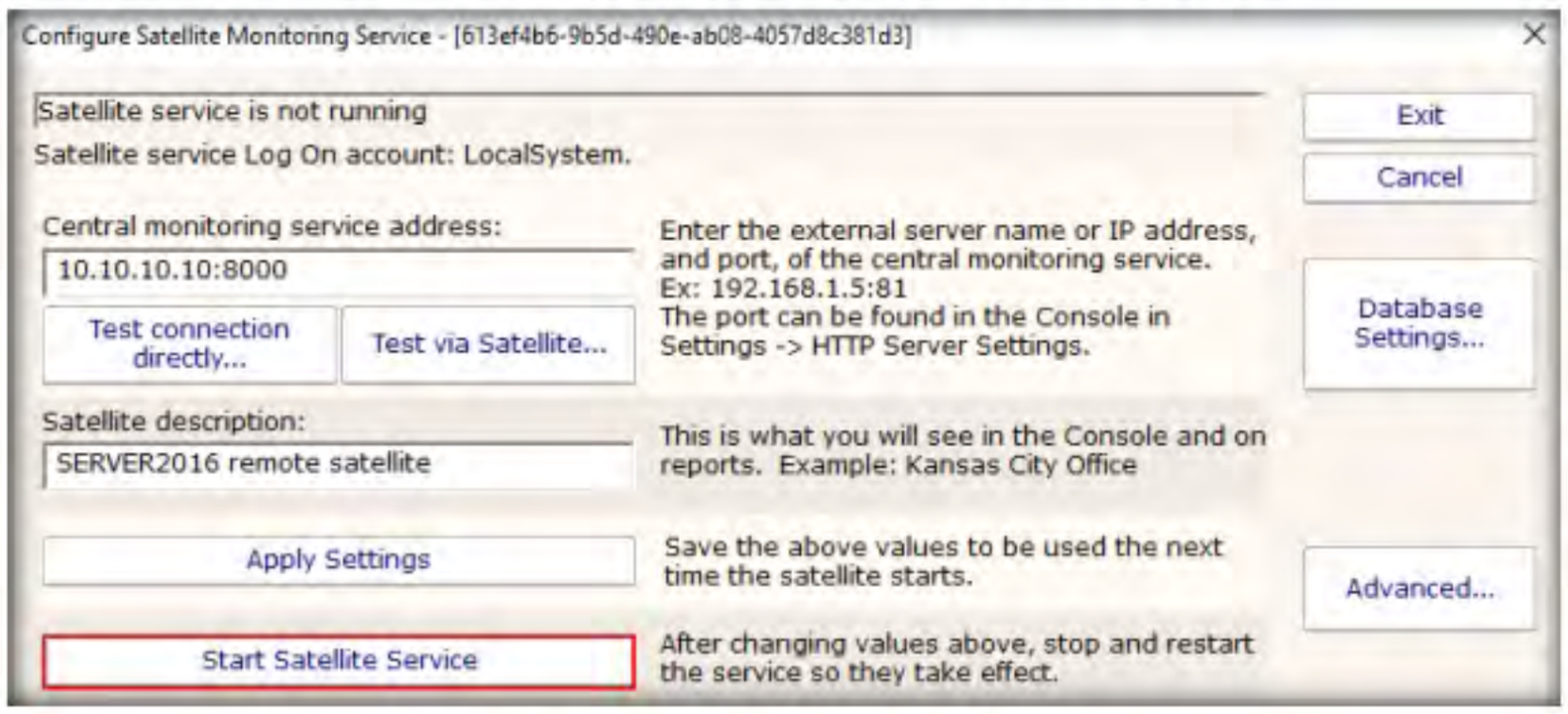


Figure 4.7.8: PA File Sight Starting Satellite Service

18. Once the service has started, click **Exit** to close the application.

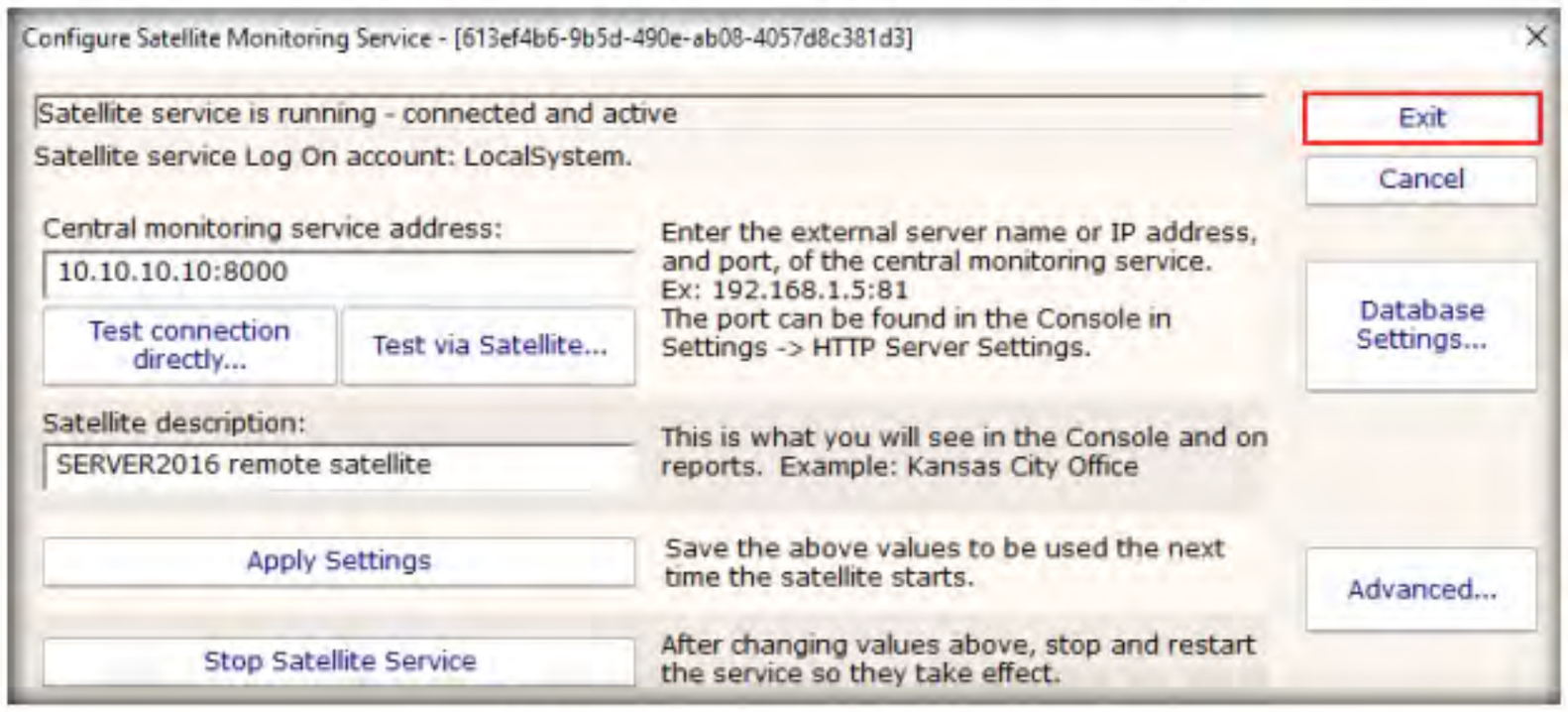


Figure 4.7.9: PA File Sight Configuring Satellite Monitoring

TASK 7.4

Create a File for Monitoring

19. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.

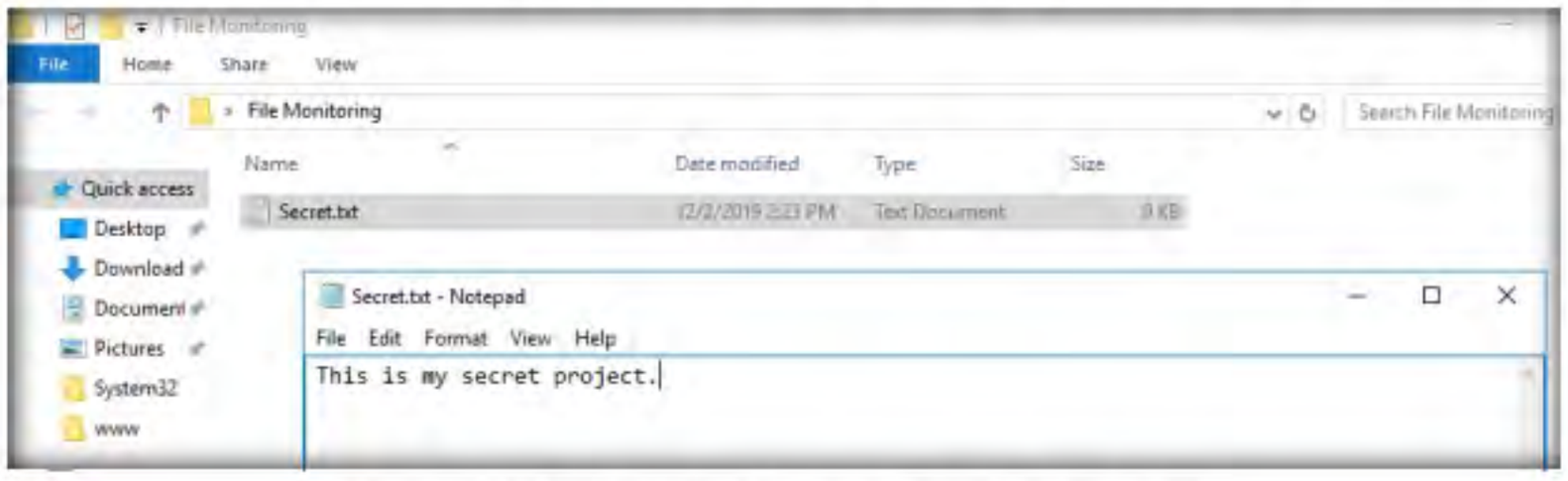


Figure 4.7.10: Creating a Text Document in Windows Server 2016

20. Switch back to the **Windows 10** machine, and observe that PA File Sight starts monitoring the **Windows Server 2016** machine.

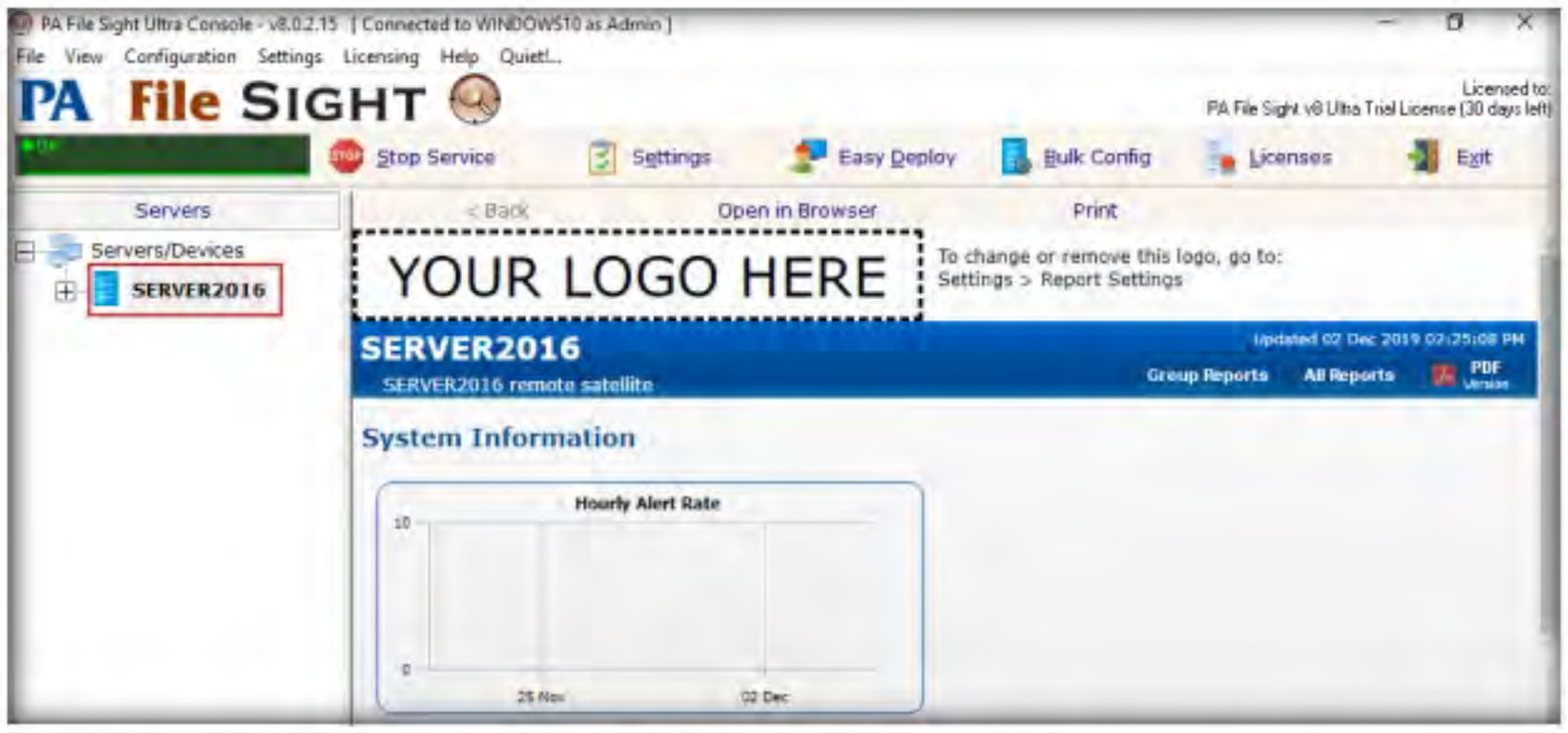


Figure 4.7.11: PA File Sight Server Added

21. Expand the **SERVER2016** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.

Figure 4.7.12: PA File Sight Inventory Collector

22. Now, right-click on **Inventory Collector** and click **Run Now!** from the context menu.

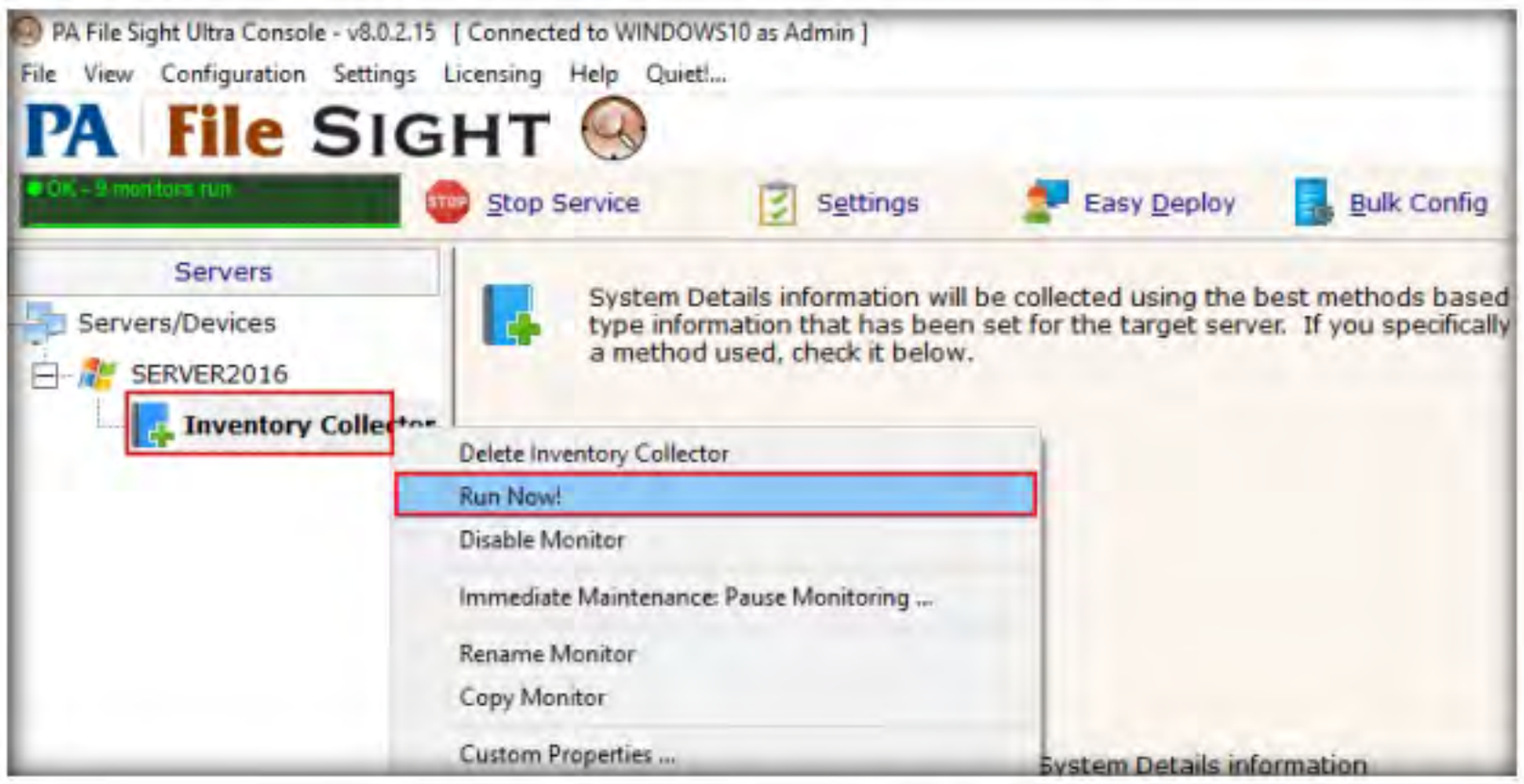


Figure 4.7.13: PA File Sight Inventory Collector Run Now!

23. Select **SERVER2016** in the left pane and scroll down, and you can see the complete system information for the **Windows Server 2016** machine on the dashboard.

Figure 4.7.14: PA File Sight Dashboard

TASK 7.5

Add New Monitor

24. Right-click on **SERVER2016** and click the **Add New Monitor** option from the context menu.

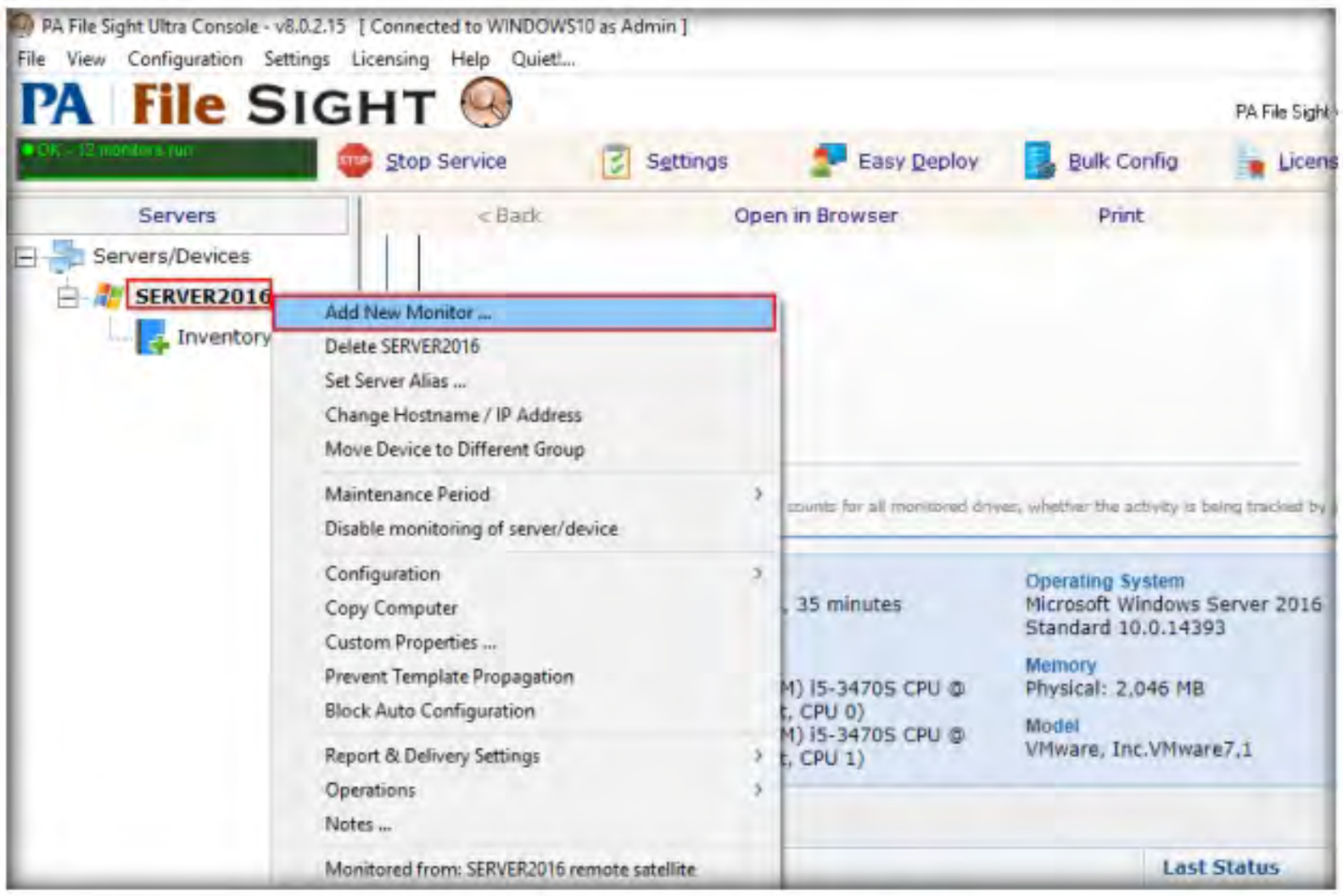


Figure 4.7.15: PA File Sight Add New Monitor Option

25. The **Add New Monitor** window appears, select the **File Sight Monitor** icon, and then click **OK**.

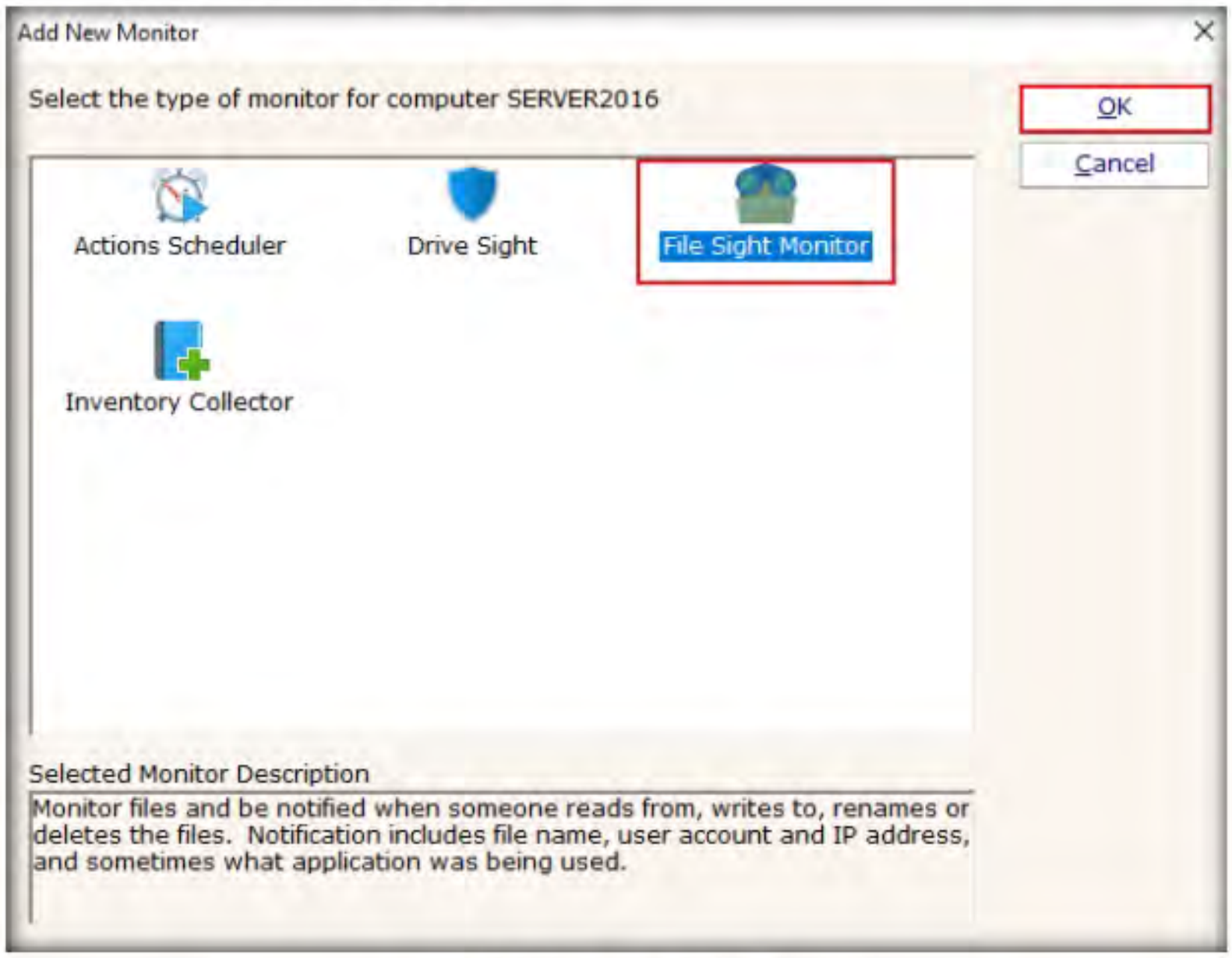


Figure 4.7.16: PA File Sight Add New Monitor

26. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **SERVER2016** machine (here, **C:\users\Administrator\Desktop\File monitoring**) and tick the **Fire actions for each event separately** checkbox.

27. Choose **Audit file activity** from the **Monitor Purpose (for configuration help)** drop-down list, and then click **Actions**.

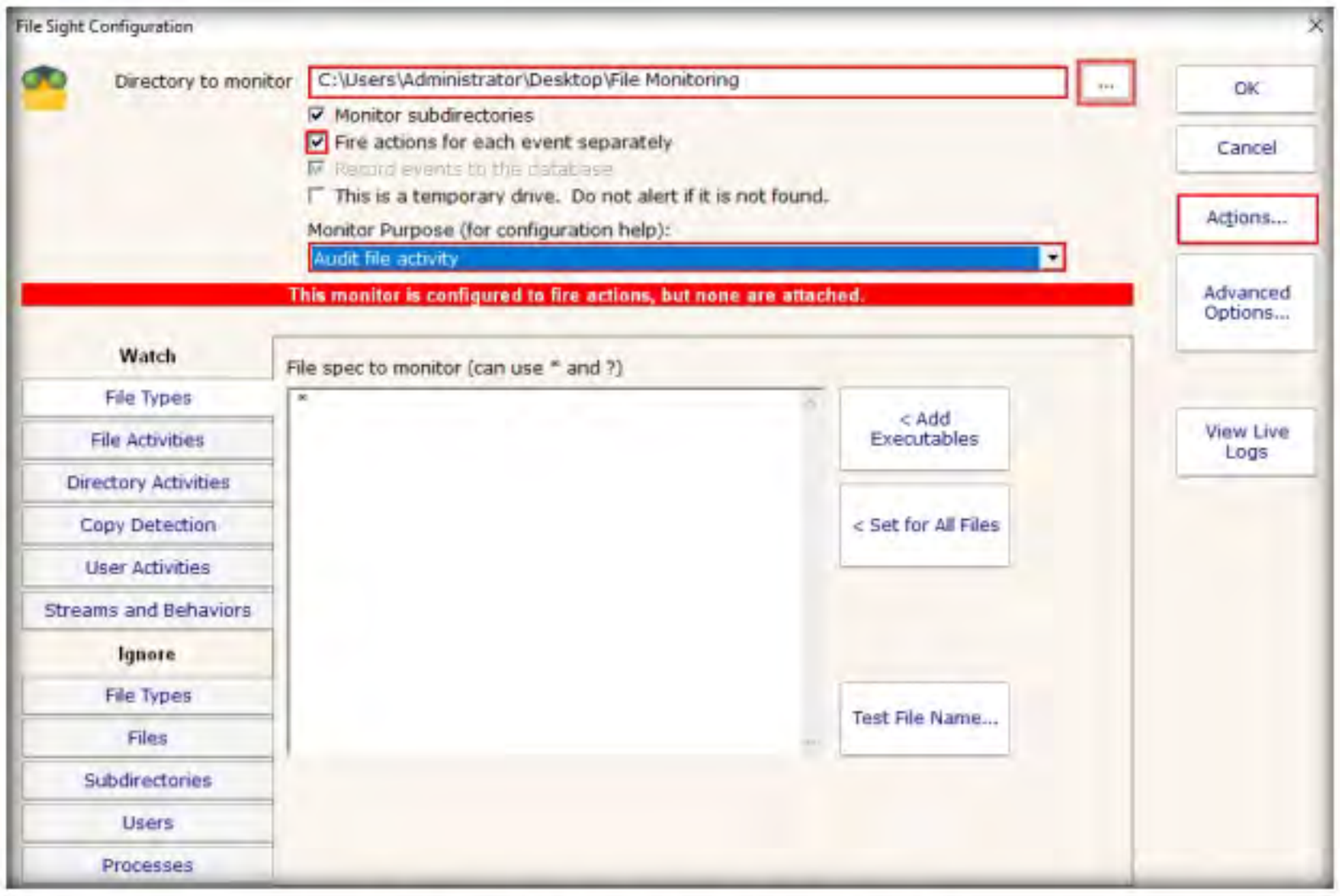


Figure 4.7.17: PA File Sight File Sight Configuration

28. The **Monitor Actions** window appears; click **New** under **Global Action List**.

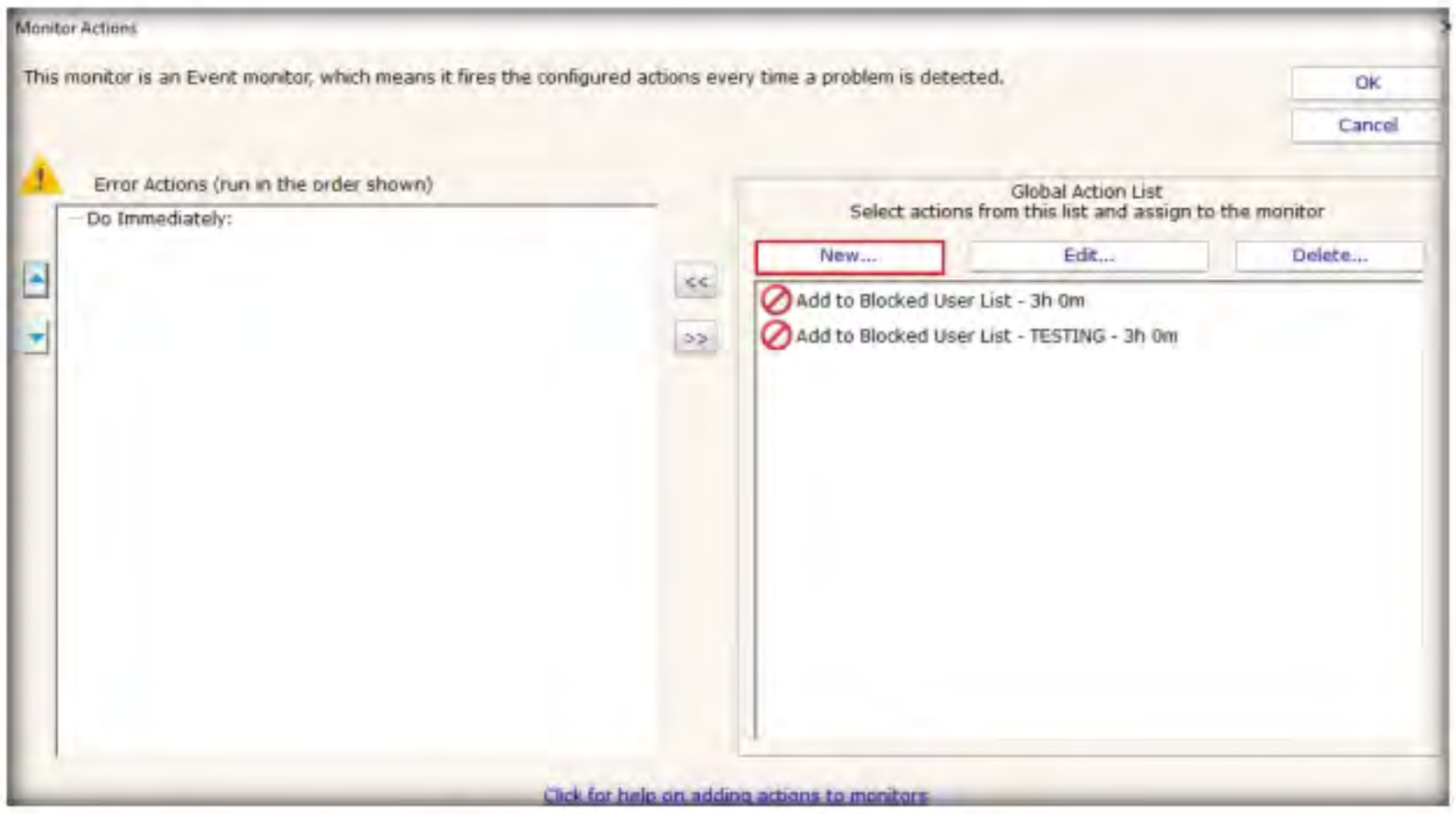


Figure 4.7.18: PA File Sight Global Action List

29. The **Add New Action** window appears. Select the **Action List** icon and click **OK**.

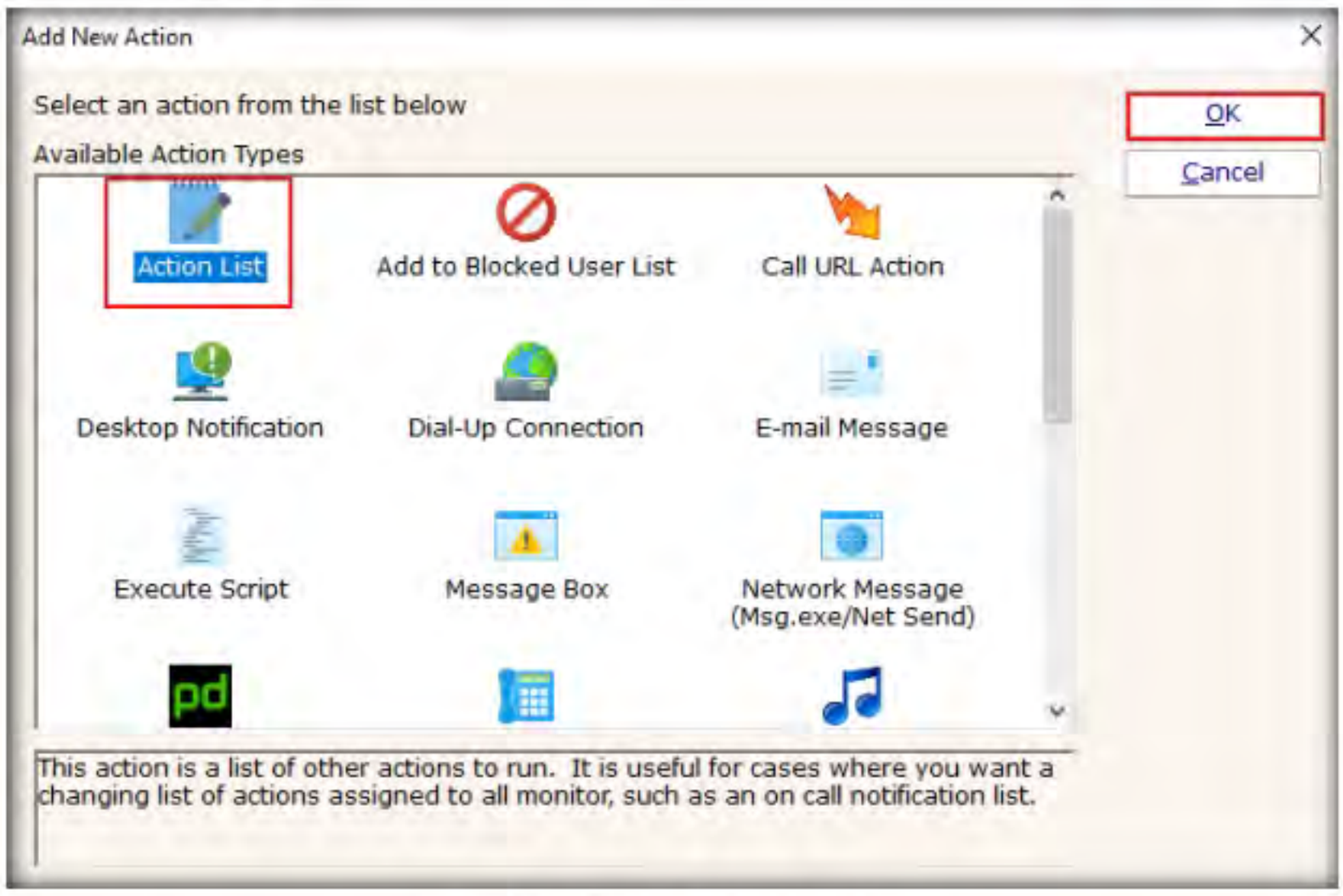


Figure 4.7.19: PA File Sight Add New Action

30. The **Action List** window appears. Type a description in the **Description** field and click **Add** to choose actions.

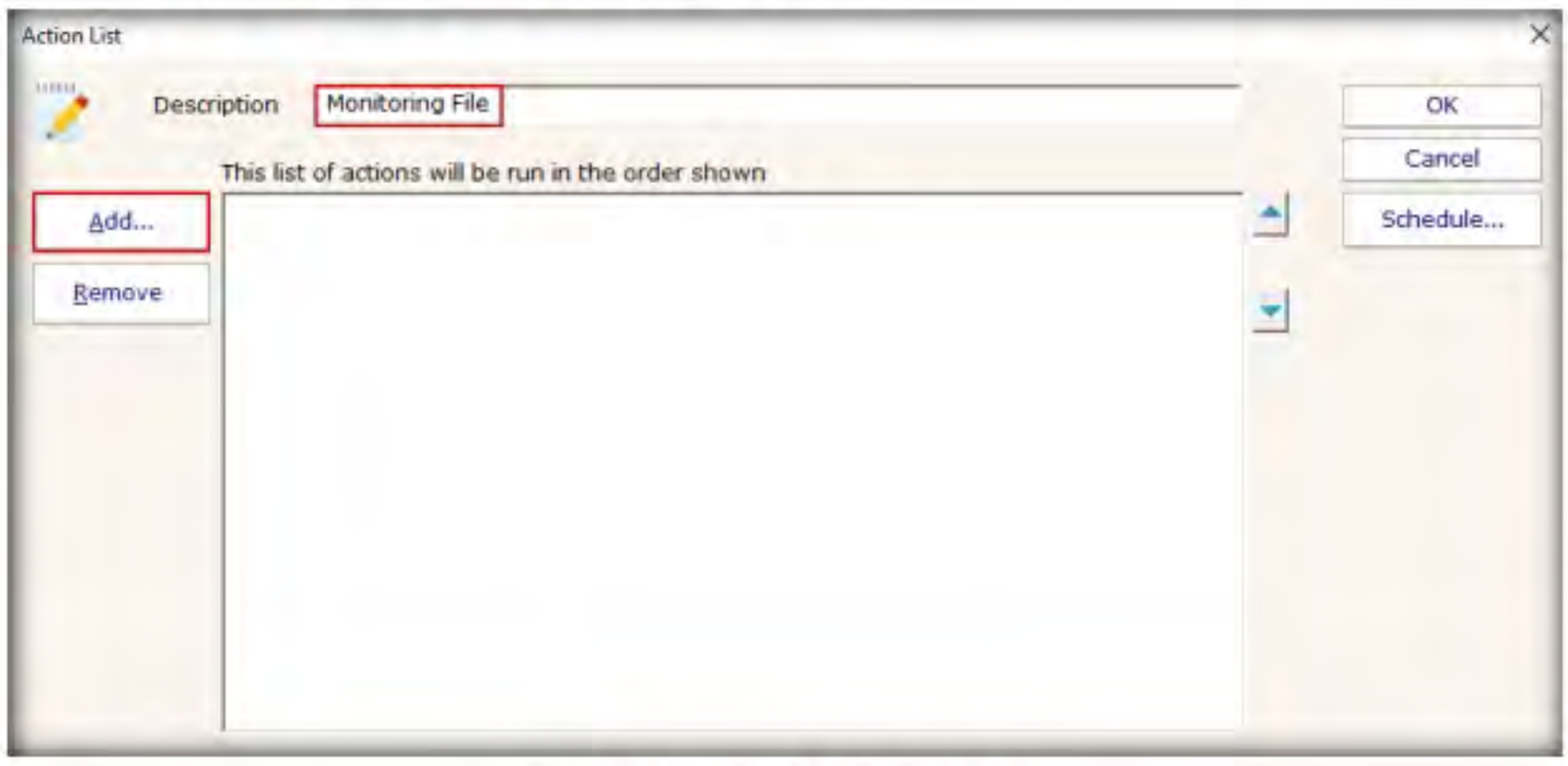


Figure 4.7.20: PA File Sight Action List

31. The **Choose Action to Add** window appears; choose any action from the list and click **OK**.

Figure 4.7.21: PA File Sight Choose Action to Add

32. Click **OK** in the **Action List** window.
33. The **Monitor Actions** window appears; choose the newly created action (here, **Monitoring File**); and then click the **<<** icon to add the action.

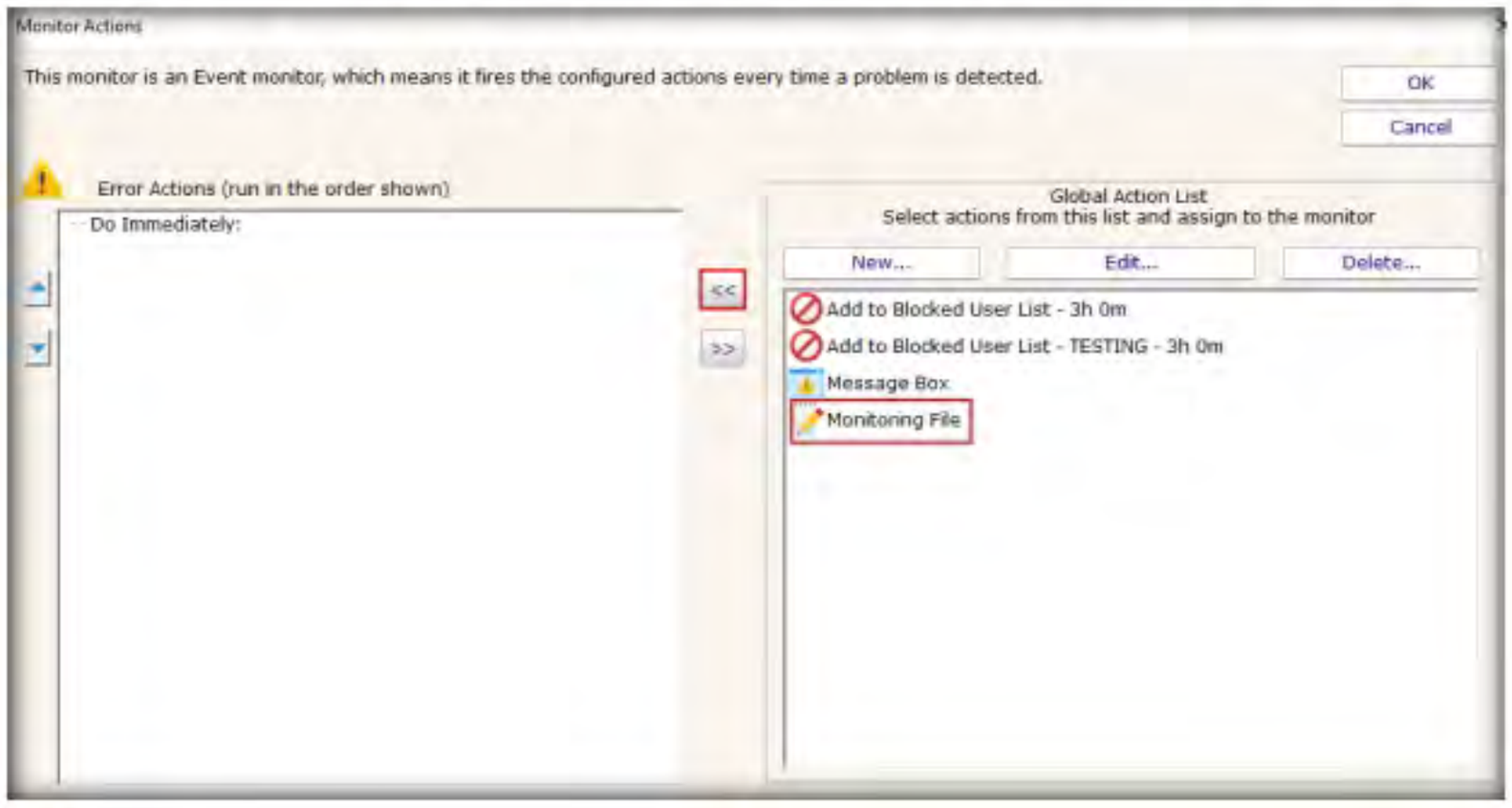


Figure 4.7.22: PA File Sight Global Action List

34. Once the action is added to the **Monitor Actions** window, click **OK**.

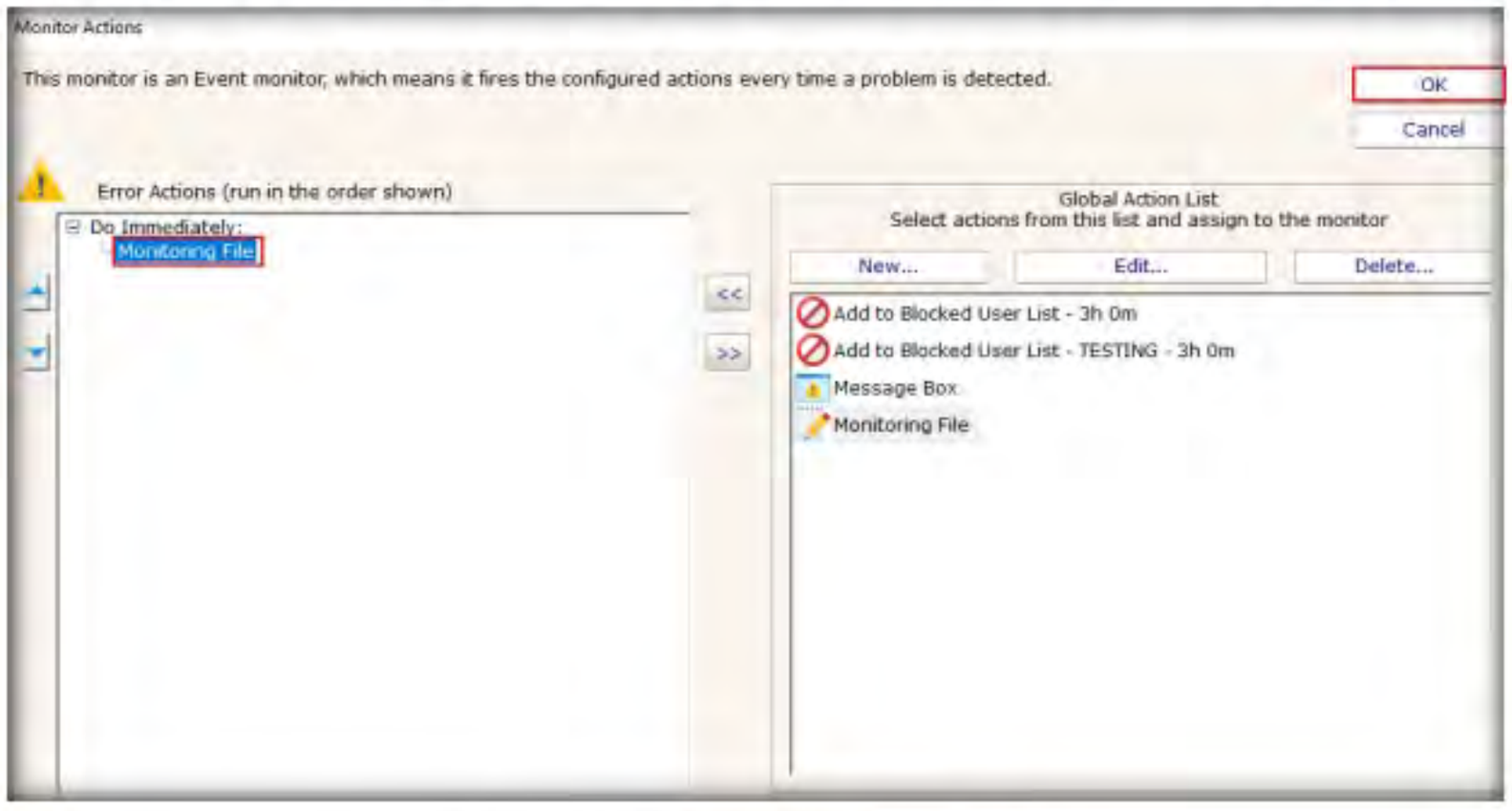


Figure 4.7.23: PA File Sight Action Added

35. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.

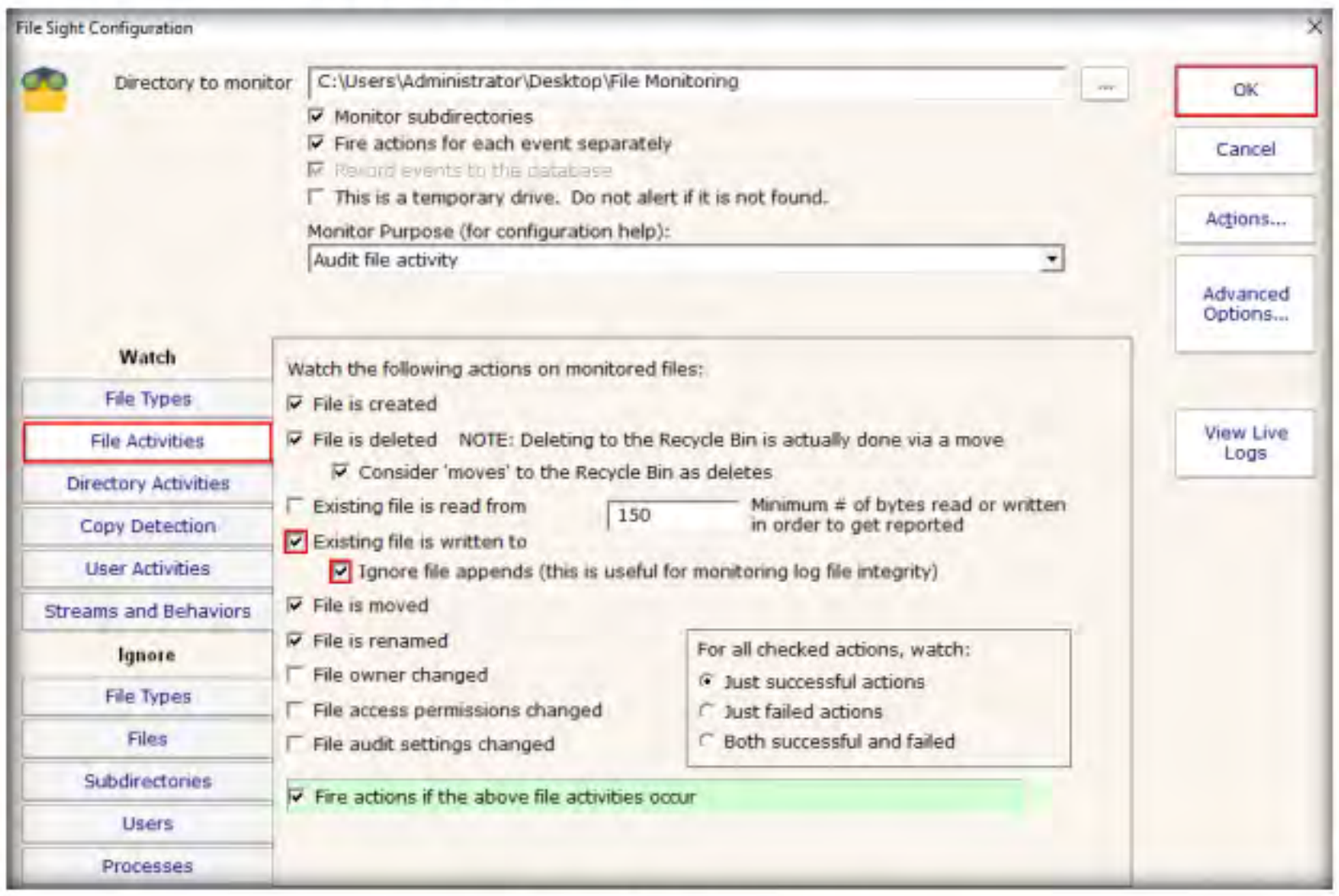


Figure 4.7.24: PA File Sight File Activities

36. Under the **SERVER2016** node, File Sight Directory Monitoring will be added, as shown in the screenshot. Click **Apply**, and then right-click on the **File Monitoring** node and click **Run Now!** from the context menu.

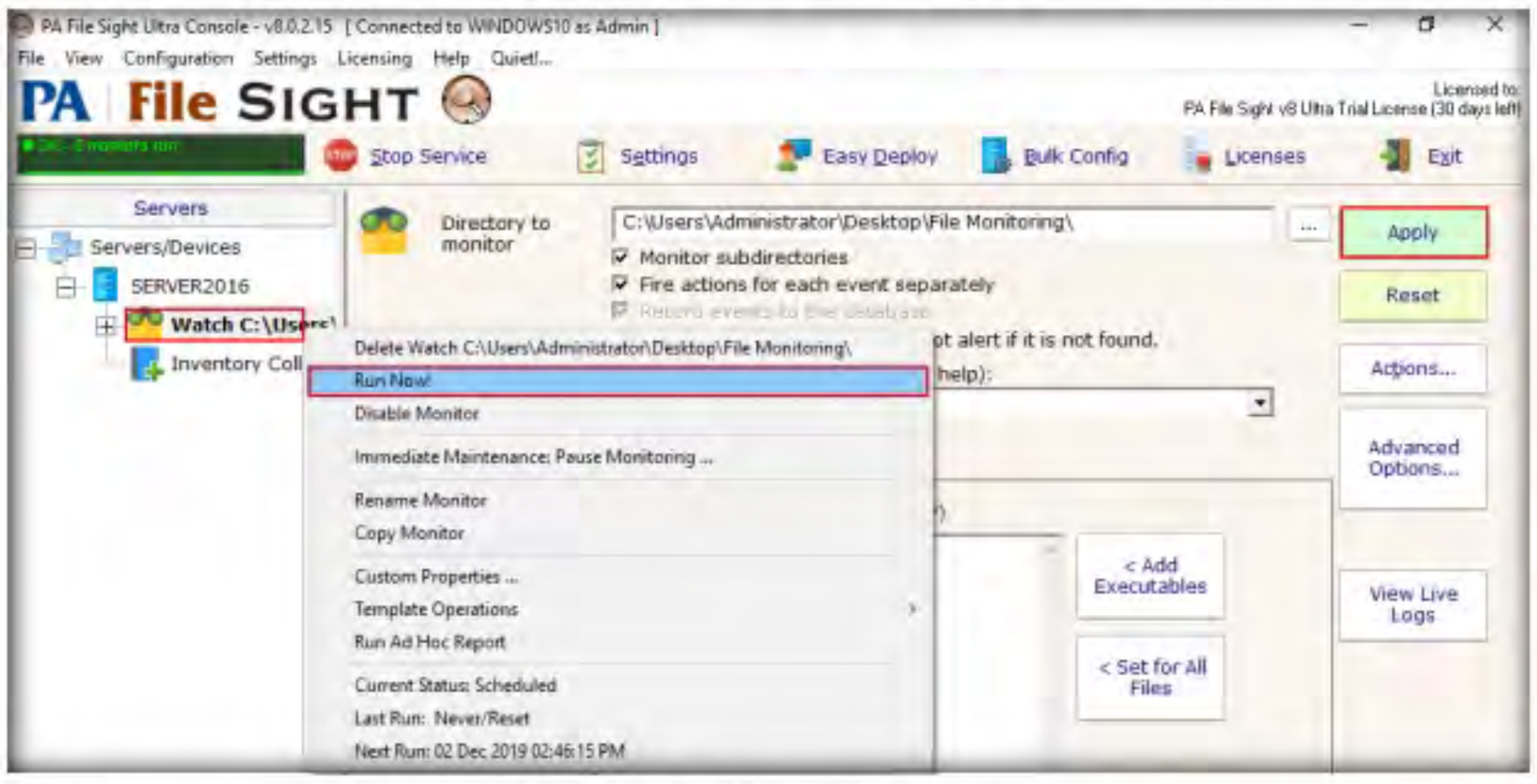


Figure 4.7.25: PA File Sight Run Now!

37. Click the **SERVER2016** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.

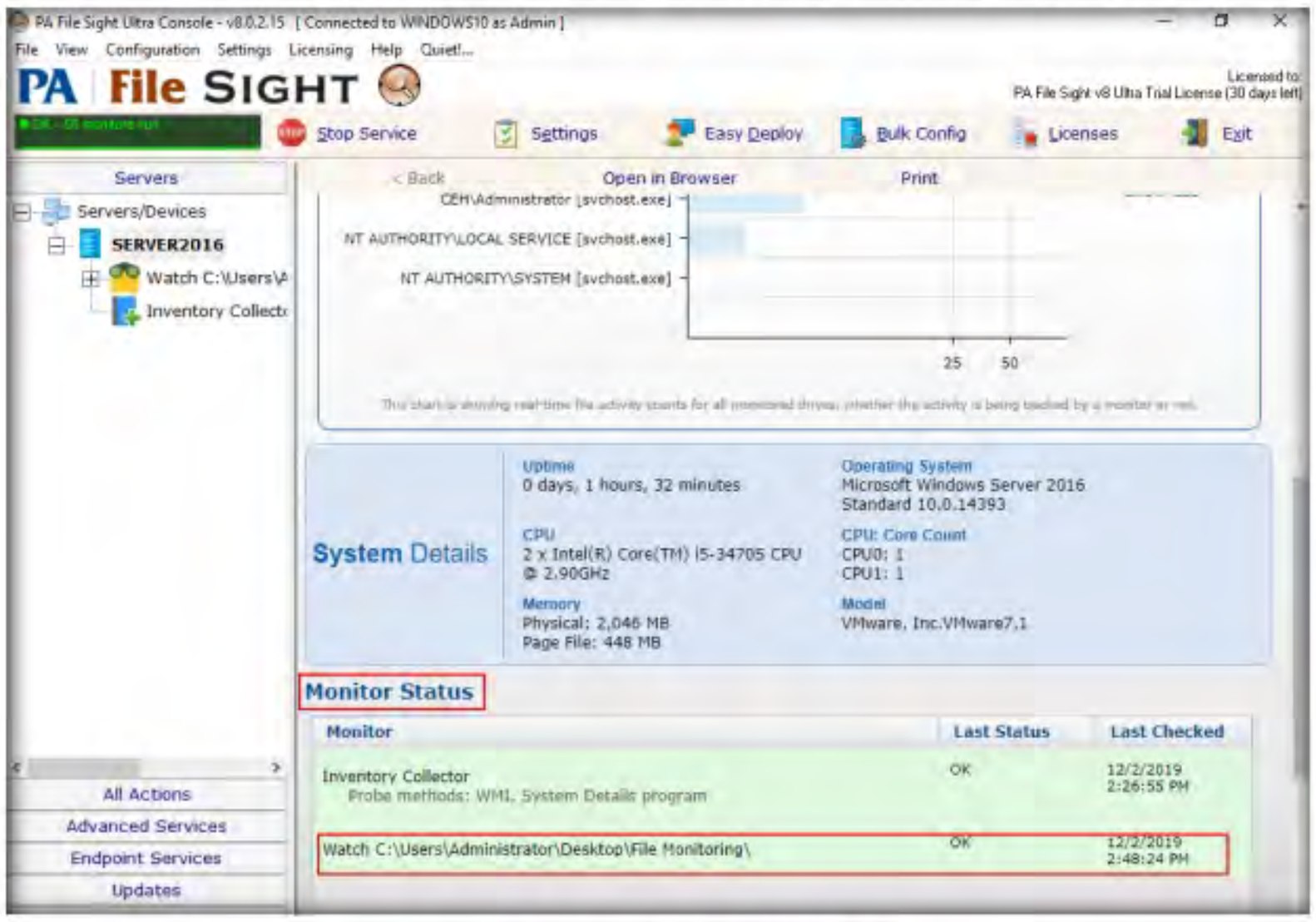


Figure 4.7.26: PA File Sight Monitor Status

38. Switch back to the **Windows Server 2016** machine, open **Secret.txt** in the **File Directory** on **Desktop**, modify some of the text in the file, and then **Save** and close the file.

Figure 4.7.27: Modifying Secret.txt file in Windows Server 2016

39. Switch back to the **Windows 10** machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.
40. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.

41. Click on the **notepad.exe** link to view the activities done by the user.

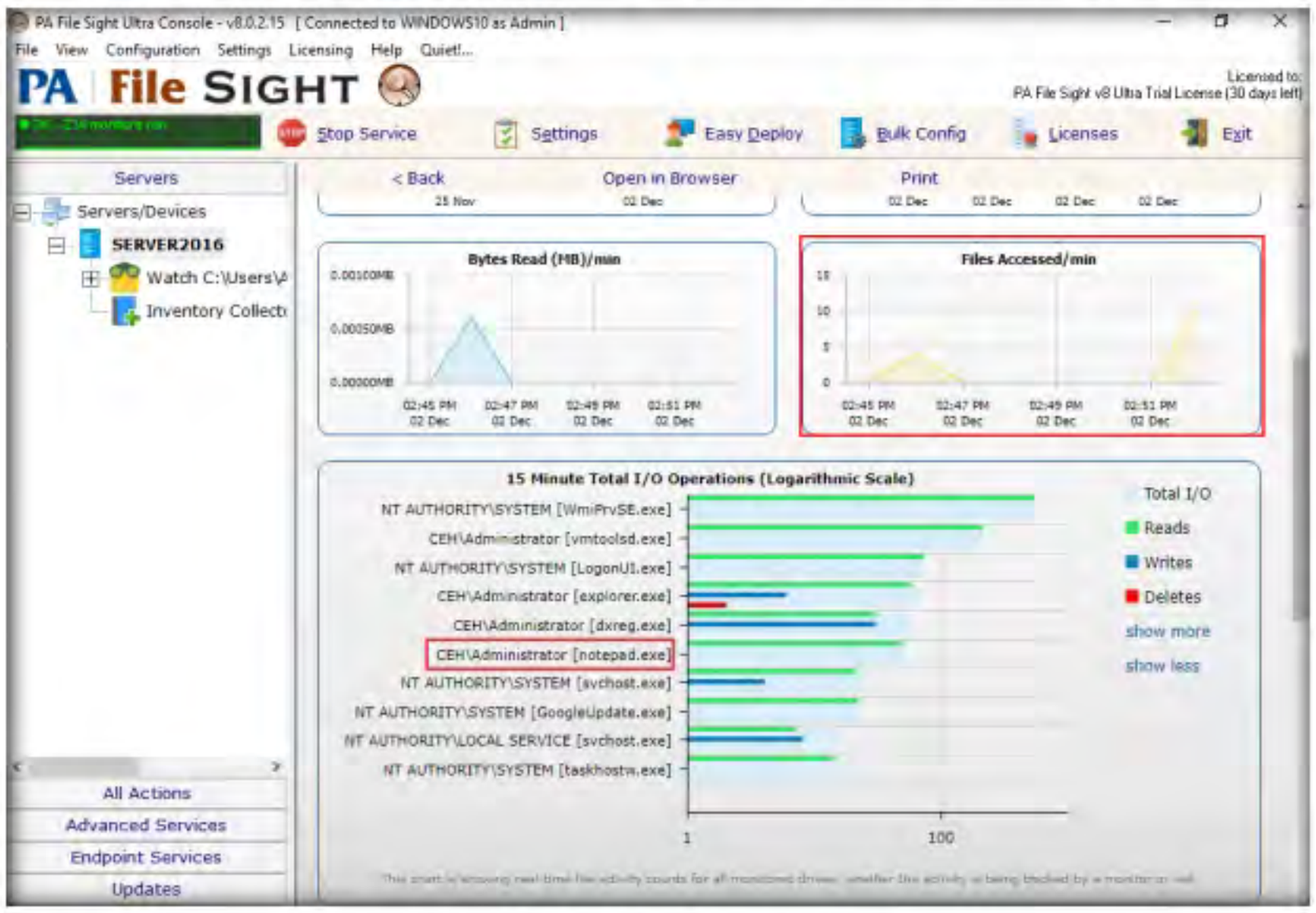


Figure 4.7.28: PA File Sight Graphical Logs

42. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then switch to the Windows Server 2016 machine, type some content into the Secret.txt file, save the file, and then immediately switch to the Windows 10 machine to view the activity.

43. If you have added some text in the Secret.txt file, you can view that in the activity window.

Figure 4.7.29: PA File Sight Activity Recorded

44. Switch back to the **Windows Server 2016** machine and delete the **Secret.txt** file, then switch back to the **Windows 10** machine and scroll down to view the **Recent Alerts** section; you will find that the file has been deleted.

45. You can see all the actions performed on that file.

You can also use other file and folder integrity checking tools such as **Tripwire File Integrity and Change Manager** (https://www.tripwire.com), **Netwrix Auditor** (https://www.netwrix.com), **Verisys** (https://www.ionx.co.uk), or **CSP File Integrity Checker** (https://www.cspsecurity.com) to perform file and folder monitoring.

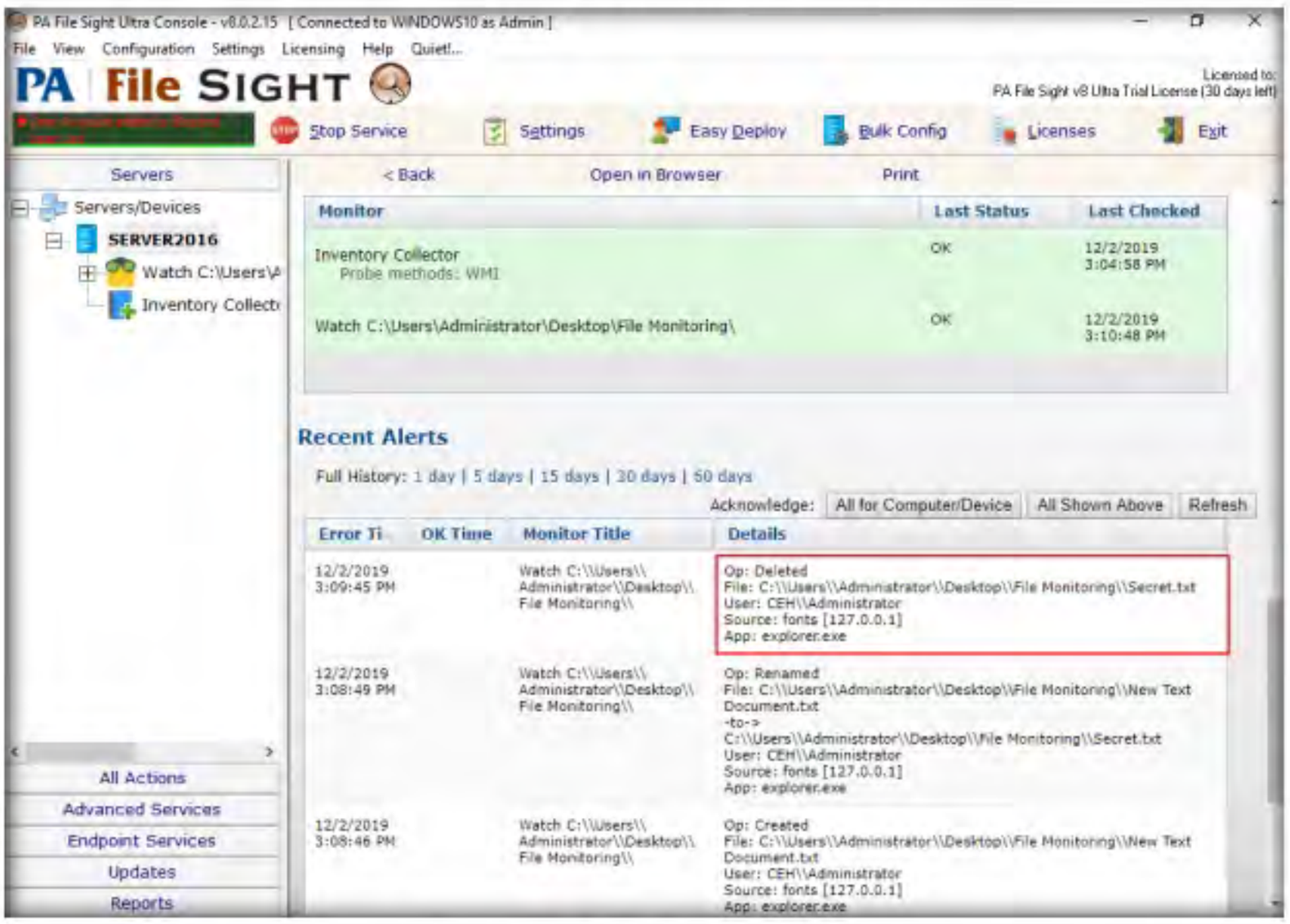


Figure 4.7.30: PA File Sight Recent Alerts

46. This is how to monitor the file integrity using PA File Sight.

47. Close all open windows.

TASK 8 Perform Device Driver Monitoring using DriverView and Driver Booster

An ethical hacker and penetration tester must scan the system for suspicious device drivers and make sure that the systems runs smoothly by ensuring that all outdated drivers are updated and that the system processes optimized to keep the performance of the system at its peak.

TASK 8.1 Launch DriverView

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView** and double-click **DriverView.exe** to launch the application.
2. The **DriverView** main window appears with a list of the installed drivers on your system, as shown in the screenshot.

When the user downloads infected drivers from untrusted sources, the system installs malware along with the device drivers; malware uses these drivers as a shield to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Booster that verify if they are genuine and downloaded from the publisher's original site.

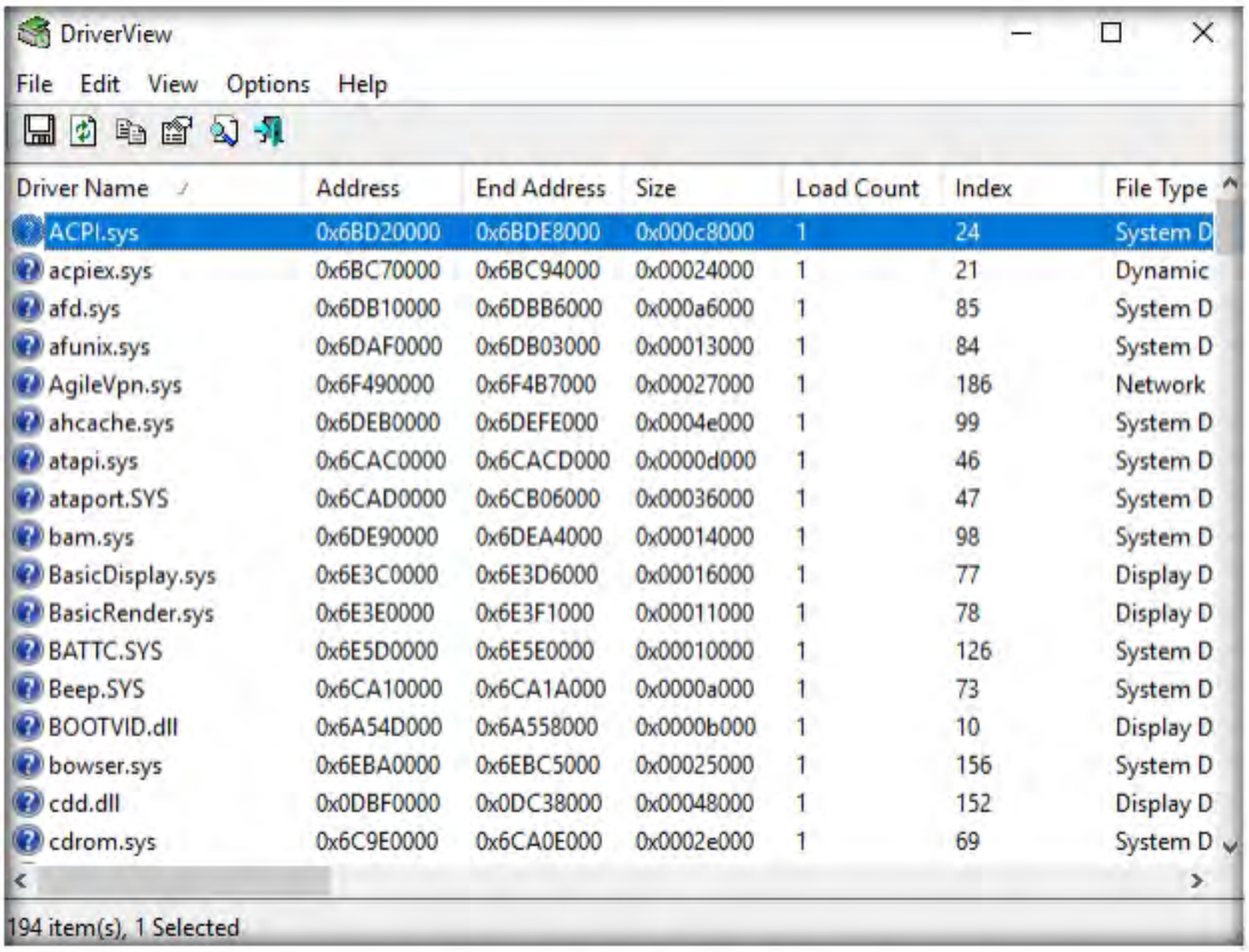


Figure 4.8.1: DriverView Main Window

DriverView

The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

3. Right-click on any driver from the list and click **Properties** to view the complete details of the driver.

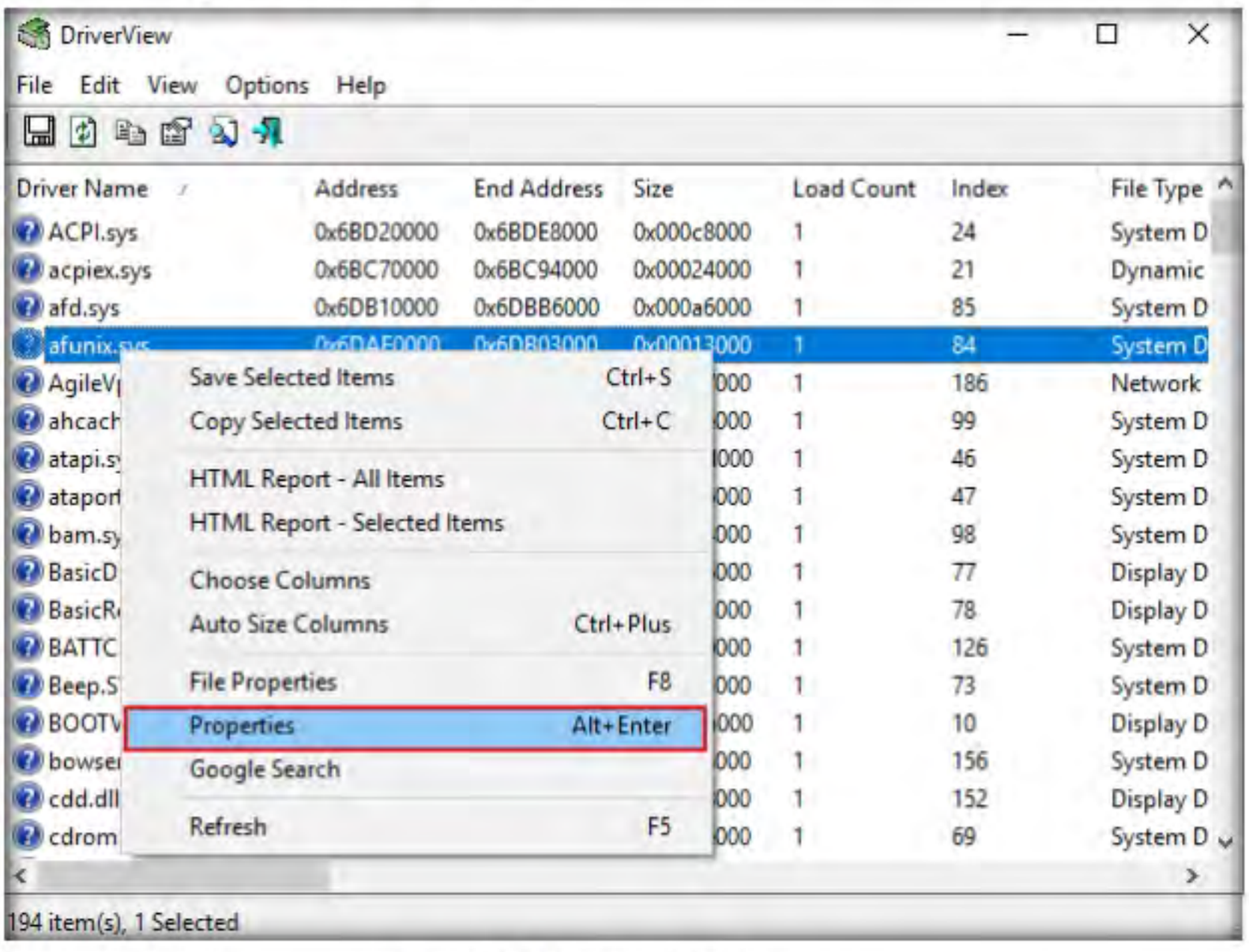


Figure 4.8.2: DriverView Select Properties

4. The **Properties** window appears with the complete details of the installed driver, as shown in the screenshot. Once the analysis is done, click **OK**.

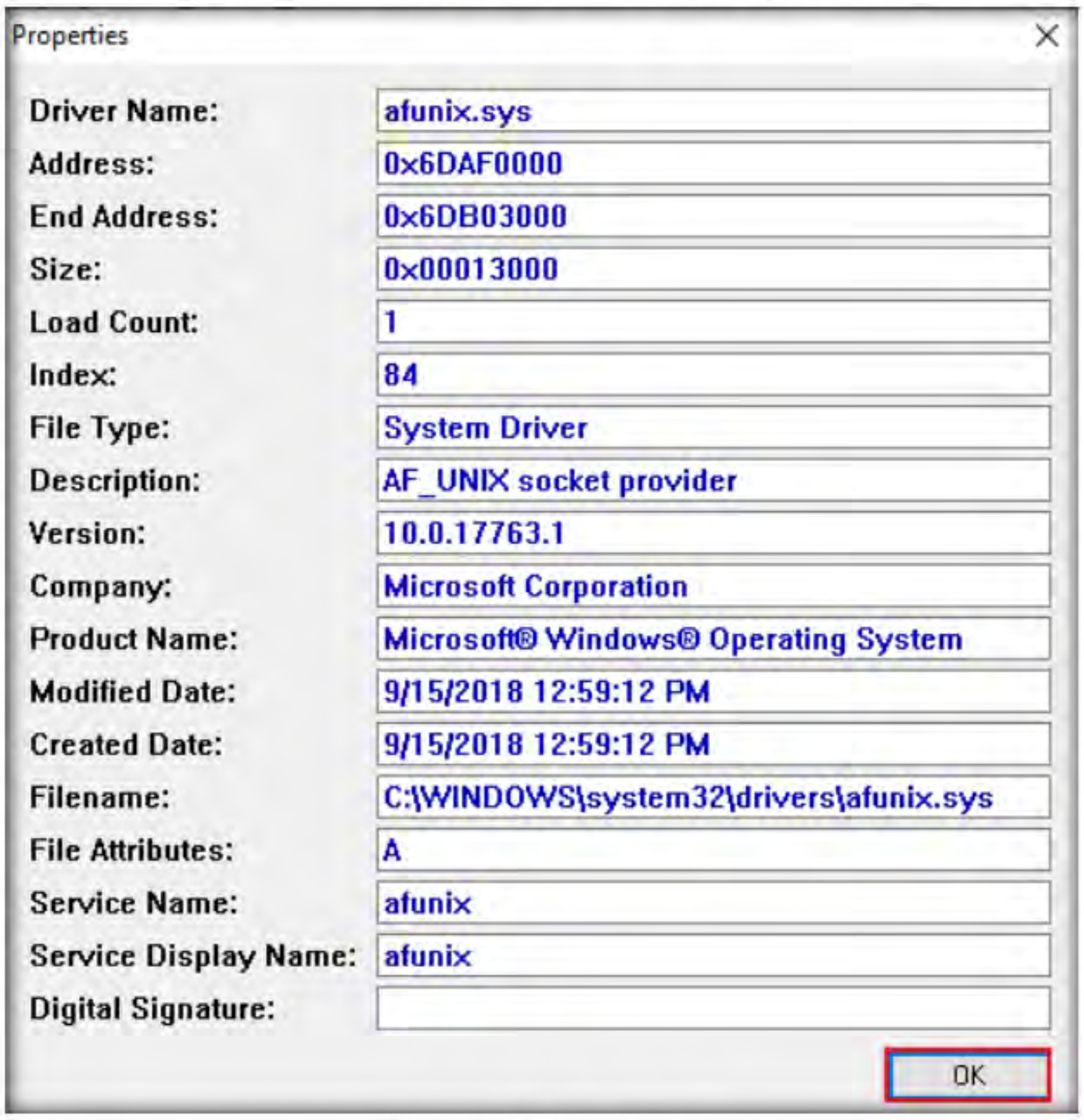


Figure 4.8.3: DriverView Properties

5. This is how to monitor the drivers installed on a machine. **Close** the **DriverView** window.
6. Now, we will see how to update system drivers and optimize the PC performance using Driver Booster.

TASK 8.2

Install Driver Booster and dashlane

7. On **Windows 10**, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Booster**. Double-click **driver_booster_setup.exe** to launch the setup.
8. If a **User Account Control** window appears, click **Yes**.

Driver Booster

Without proper drivers, computers start to misbehave. Sometimes updating the drivers using conventional methods can be a daunting task. Outdated drivers are more vulnerable to hacking and can lead to a breach in the system. Driver Booster provides a better way of updating the drivers with its all-in-one command center with automatic backup and updates, which helps the smooth functioning of the system.

9. The **Install Driver Booster** window appears; click **Install** to start the installation process.

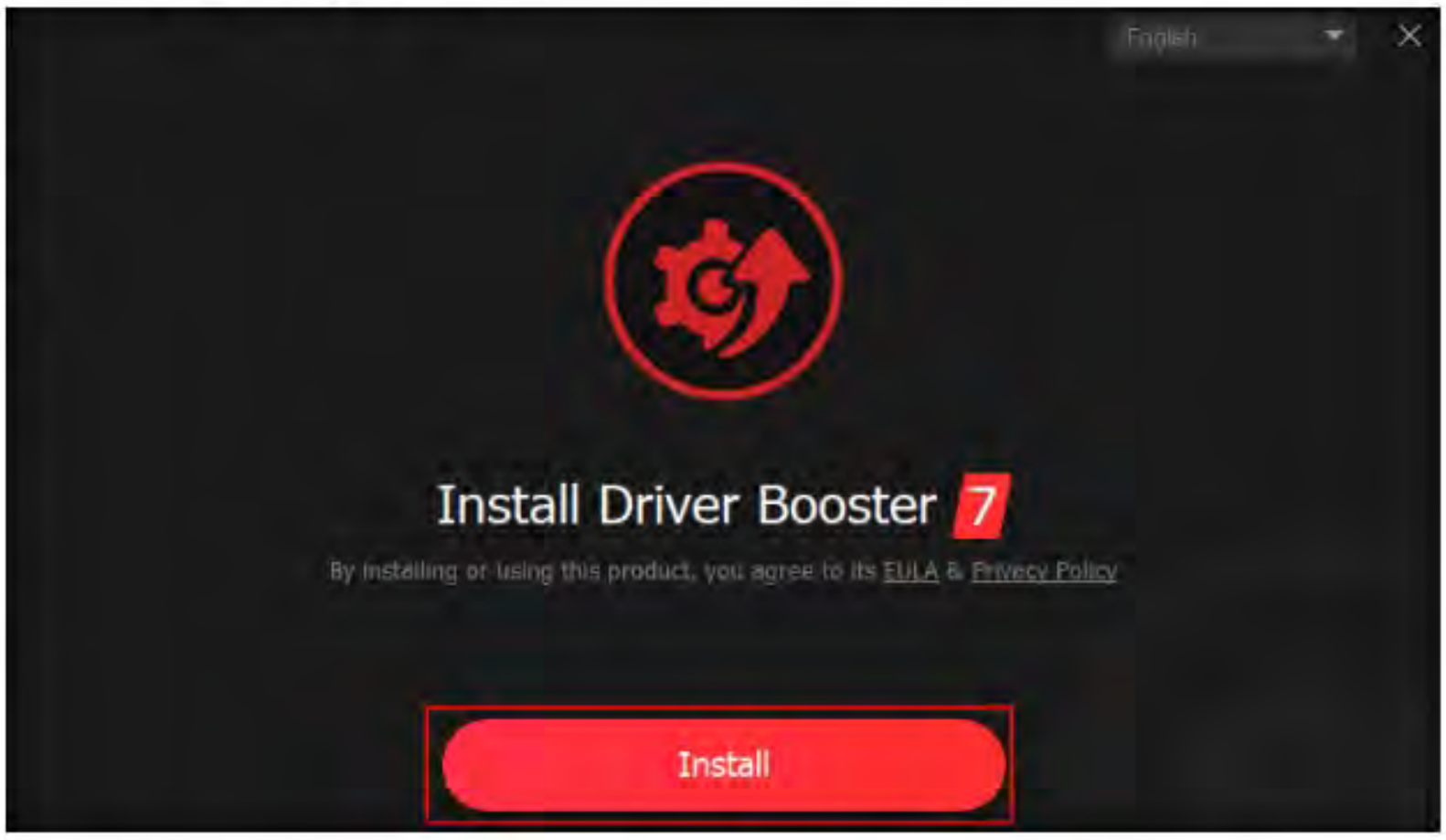


Figure 4.8.4: Driver Booster Install Screen

10. The **dashlane** window appears; select the **Yes** radio button and click **Install**.
11. The program starts to install on your system.
12. If an **Opera** wizard appears, select the **No, thanks** radio button and click **Next**.
13. The **Subscribe to IObit Newsletter** window appears; click **No, thanks**.
14. The **Installation completed** window appears after a successful installation; click **Scan Now**.

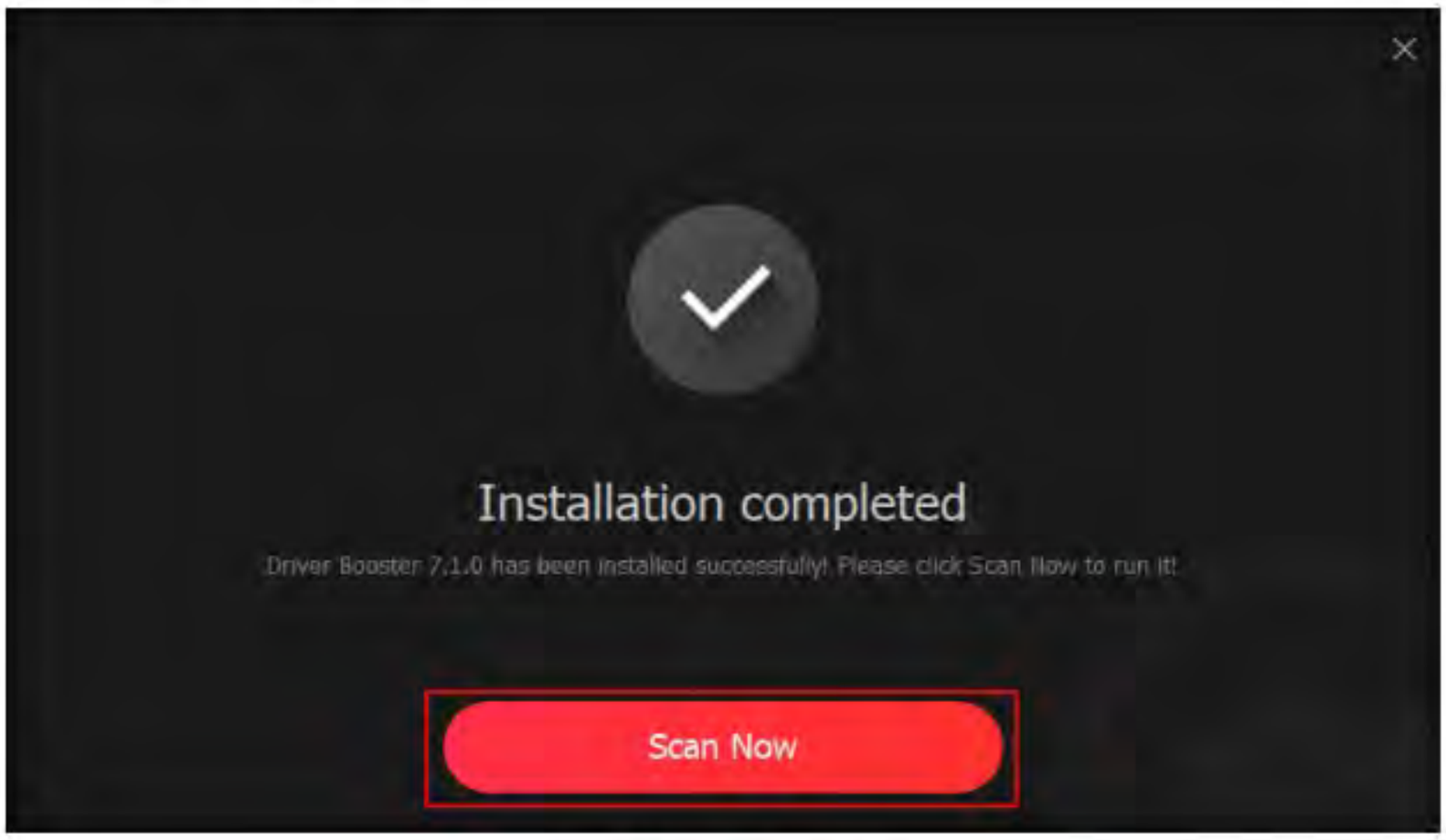


Figure 4.8.5: Installation finished

TASK 8.3

Conduct a Driver Scan

15. Driver Booster starts scanning the system for outdated or missing drivers, as shown in the screenshot.

Figure 4.8.6: Driver Booster scanning the system

16. Close the pop-up window. Driver Booster scans all available drivers on the machine, and if any outdated driver is installed, the software alerts you. Install the updated driver version.
17. To get information about an installed driver, click the link, as shown in the screenshot.

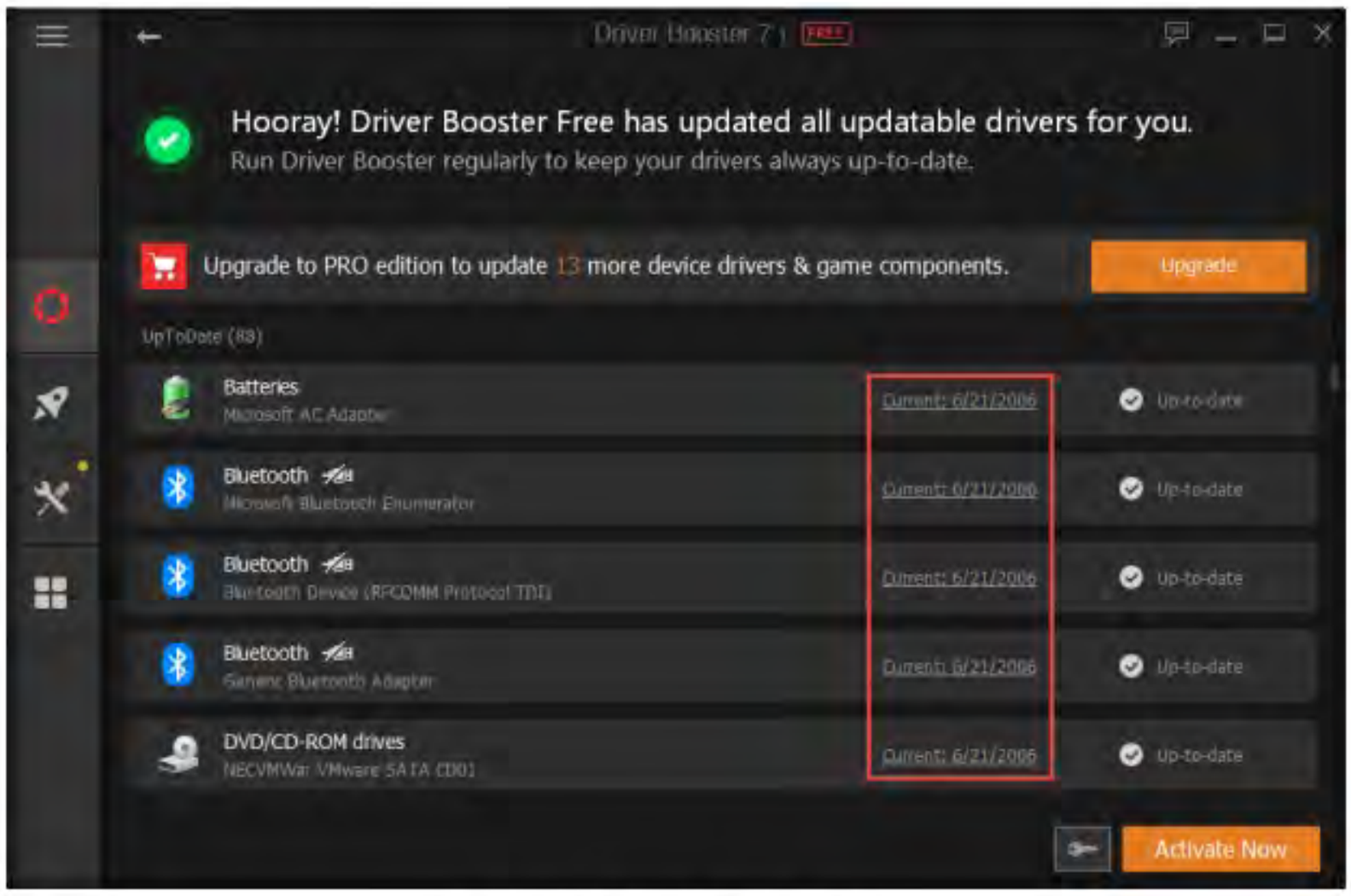


Figure 4.8.7: Scan results being displayed

TASK 8.4

Analyze the Scan Results

18. The **Driver Details** window appears, showing the driver information. Here you can **Roll Back** a faulty driver or **Uninstall** it completely. Read all the details and close the window.

Figure 4.8.8: Driver Details window

19. Click the **Action Center** icon from the left pane, and then click the **Install now** button for **Advanced SystemCare**.

Figure 4.8.9: Installing Advanced SystemCare

20. The **Optional Offer** window appears; click **Install**.

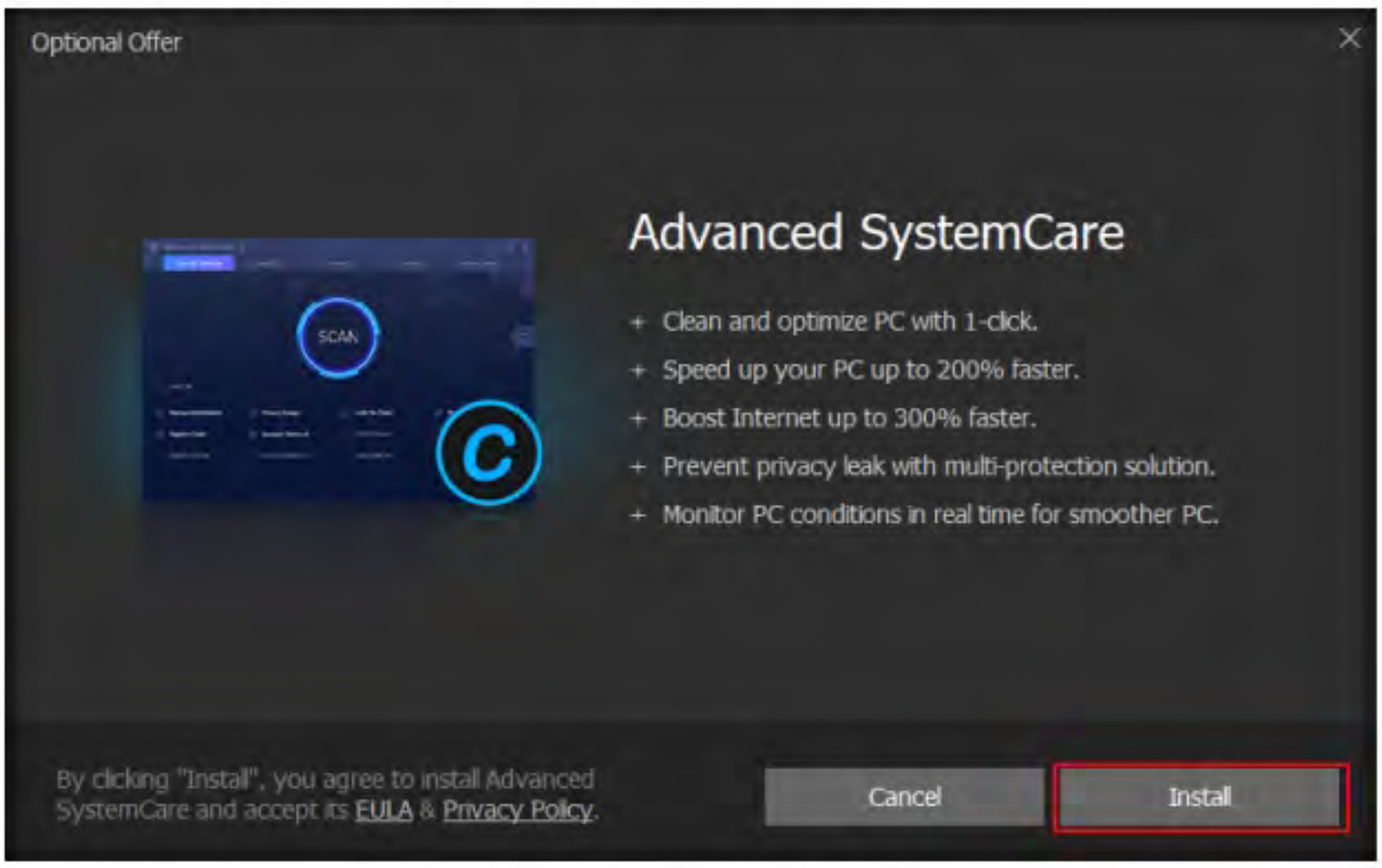


Figure 4.8.10: Advanced SystemCare Installation

TASK 8.5

Clean and Optimize System

21. Advanced SystemCare is installed. Check the **Select All** checkbox, and then click **Scan**, as shown in the screenshot.

Figure 4.8.11: Advanced system care main window

22. The application starts scanning the computer, as shown in the screenshot.
23. As it takes 10 to 15 minutes to complete, we have Stopped the scan.

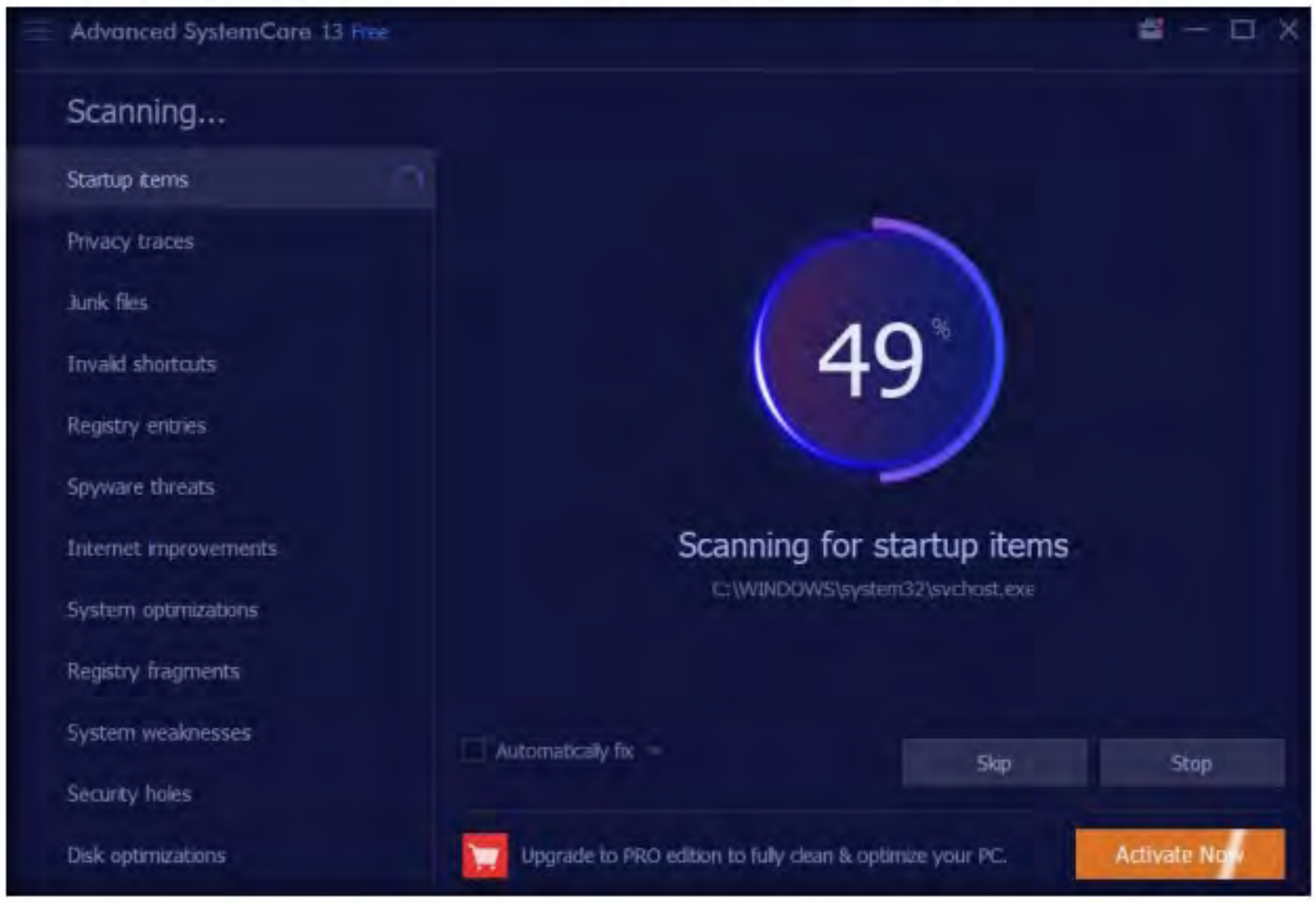


Figure 4.8.12: Advanced system care scan in progress

24. Once the scan finishes, a **Summary** is shown, as shown in the screenshot. Click the **Fix** button in the bottom-right corner to resolve the discovered PC issues.

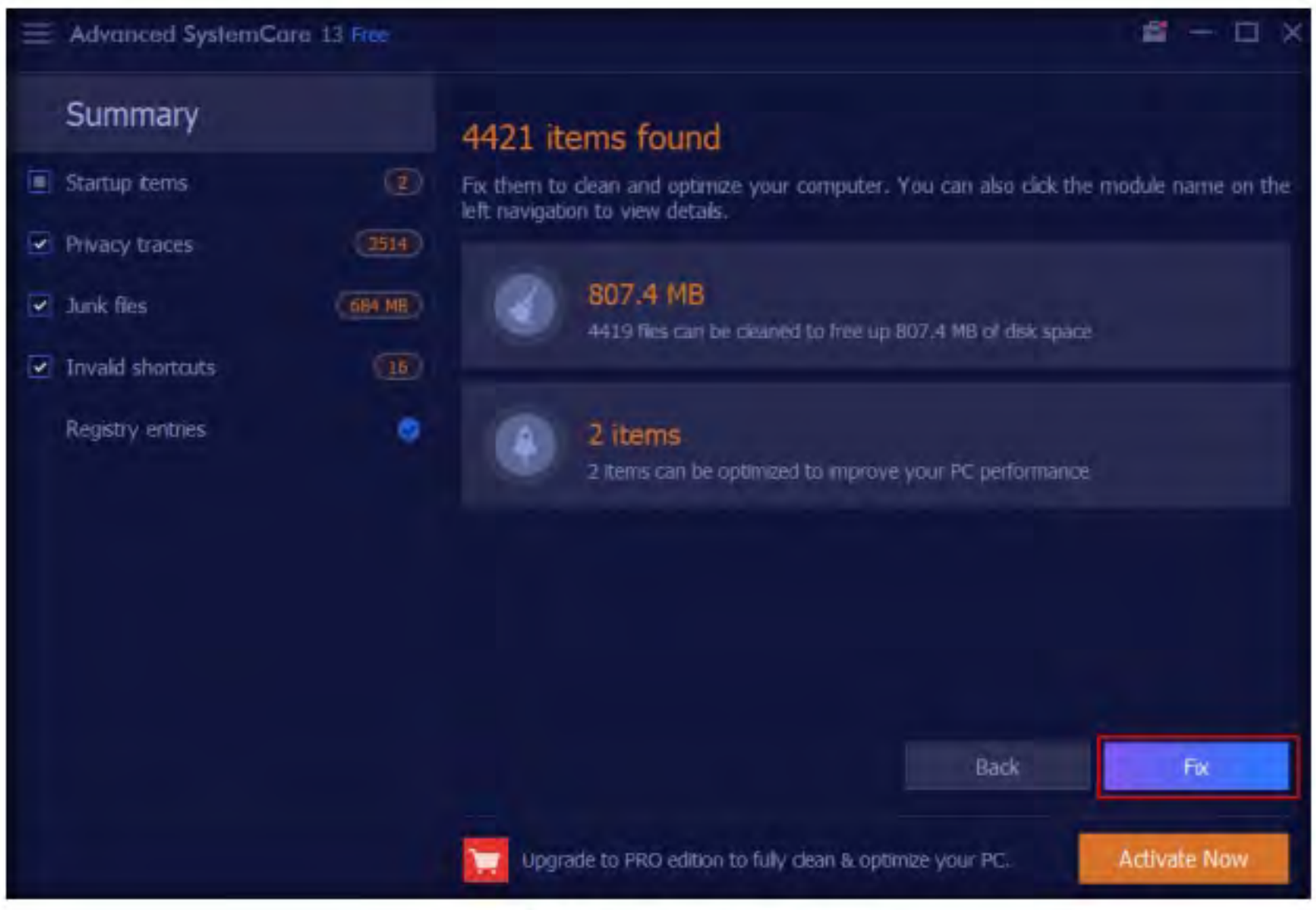


Figure 4.8.13: Summary of the system scan

25. The application starts to fix the PC issues found, as shown in the screenshot.

Figure 4.8.14: Advanced system scan fixing PC issues

You can also use other device driver monitoring tools such as **Driver Reviver** (https://www.reviversoft.com), **Driver Easy** (https://www.drivereasy.com), **Driver Fusion** (https://treexy.com), or **Driver Genius** (http://www.driver-soft.com) to perform device driver monitoring.

26. After the process is complete, the **Fix completed!** window appears, showing **Your current PC health status**, as shown in the screenshot. Analyze the results and close the application.

Figure 4.8.15: Problems fixed by Advanced SystemCare

27. Close all open windows.

Perform DNS Monitoring using DNSQuerySniffer

TASK 9

TASK 9.1

Launch DNSQuerySniffer

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**, and then double-click **DNSQuerySniffer.exe**.
2. The main window of **DNSQuerySniffer** appears, along with the **Capture Options** window.

Note: If the **Capture Options** window does not appear, then navigate to the **Options** menu and select **Capture Options**.

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and other types), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records. You can easily export the DNS query information to a CSV, tab-delimited, XML, or HTML file, or copy the DNS queries to the clipboard and then paste them into Excel or another spreadsheet application.

3. In the **Capture Options** window, ensure that the **WinPcap Packet Capture Driver** option is selected under the **Capture Method** field.
4. In the Select network adapter section, select the **Windows 10** network adapter (here, **Ethernet0**).

Note: In your lab environment, the Ethernet driver and the IP address of the Windows 10 may differ.

5. Click **OK** to start sniffing.

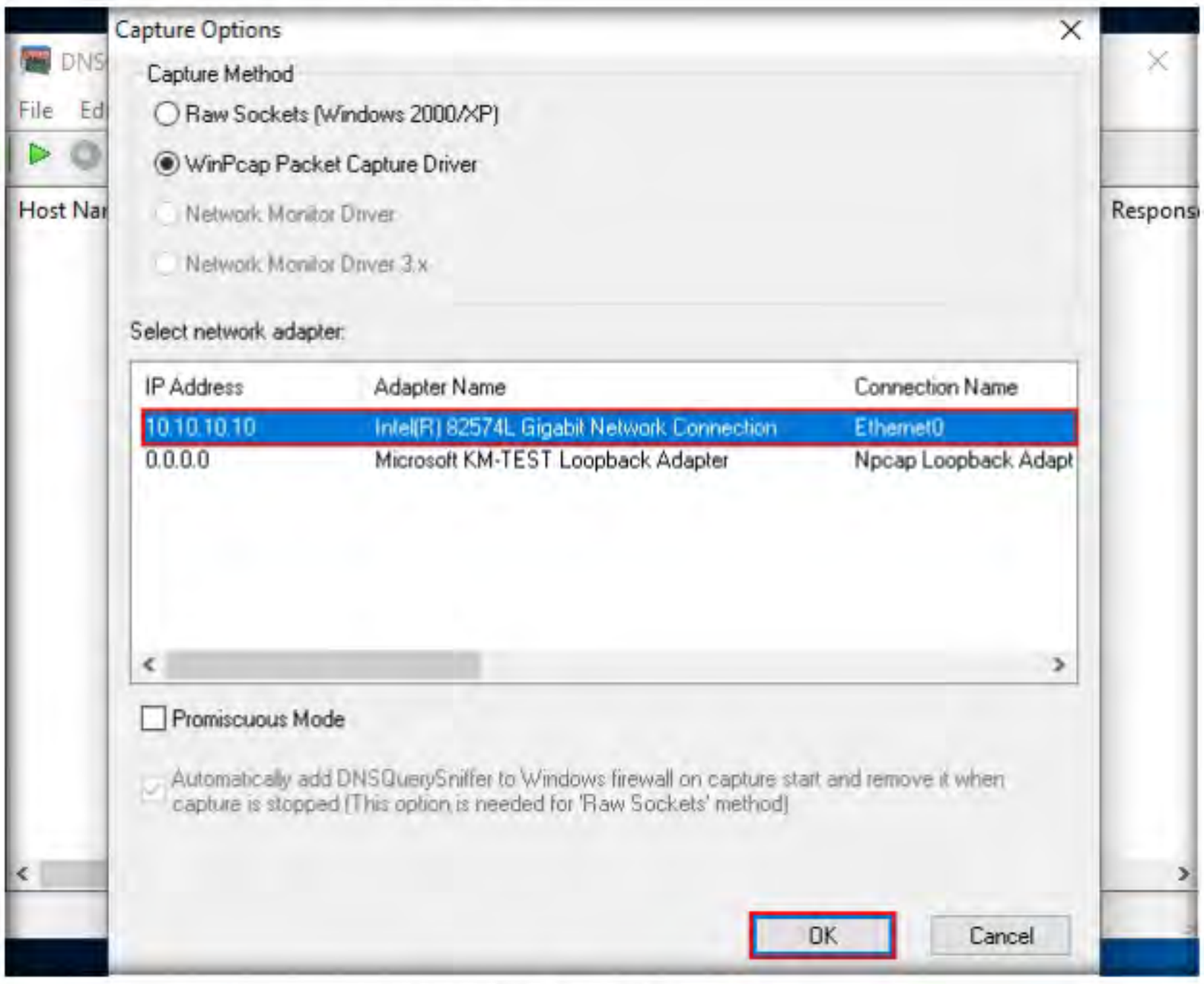


Figure 4.9.1: Capture Options window

6. The DNSQuerySniffer starts monitoring the network traffic and takes some time to capture the traffic. Leave the window intact. It shows the DNS queries sent on your system along with its complete information

such as host name, port number, request time, response time, duration, source address, and destination address, as shown in the screenshot.

Note: To view the **Source Address** and **Destination Address** columns, scroll to the right side of the window.

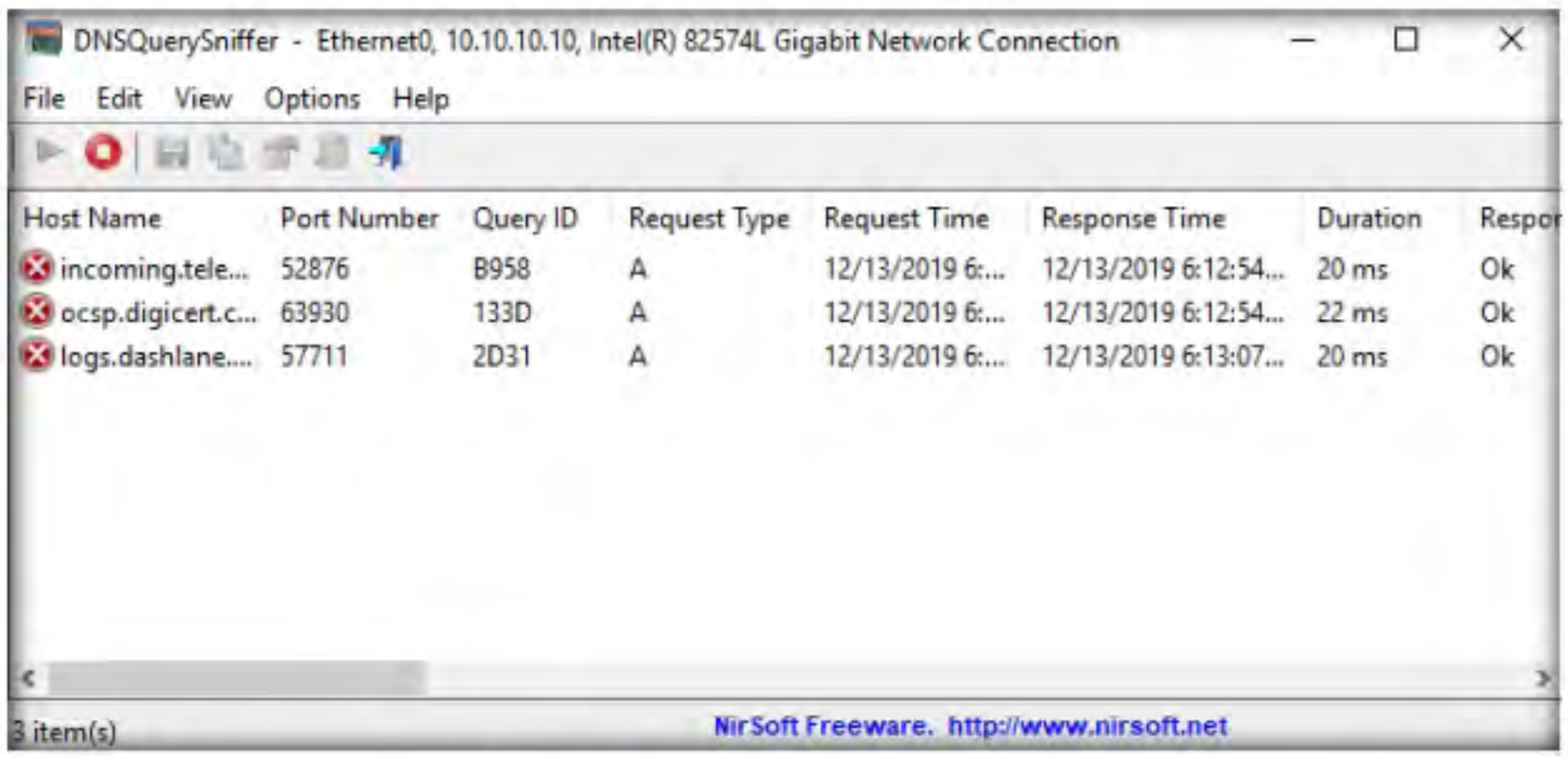


Figure 4.9.2: DNSQuerySniffer Main Window

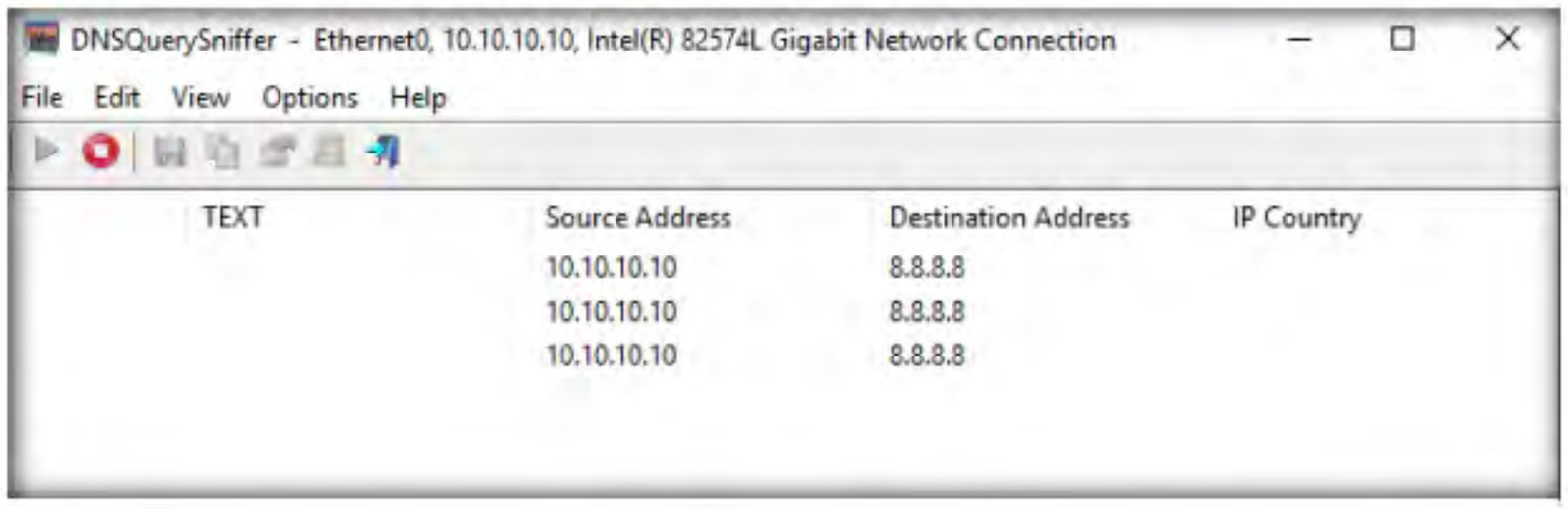


Figure 4.9.3: DNSQuerySniffer Main Window showing DNS address

7. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
8. In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine. For demonstration purposes, we are changing the DNS of the **Windows 10** machine in the **Network & Internet** settings.
9. Right-click on the **Network** icon in the lower-right corner of **Desktop** and click **Open Network & Internet settings**.

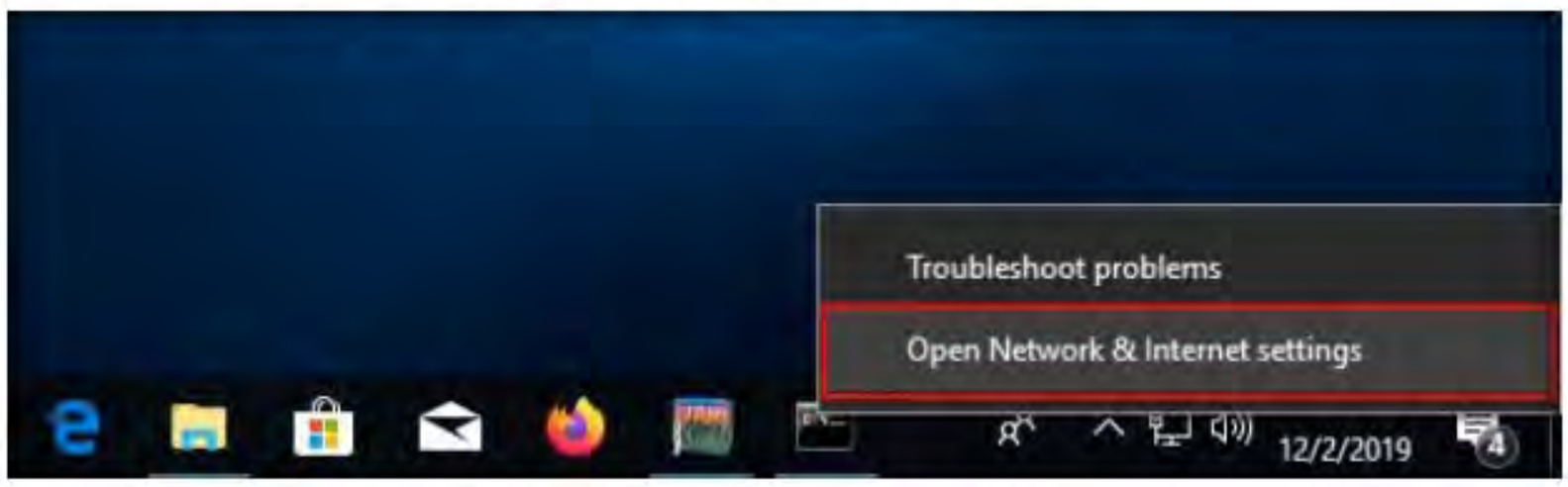


Figure 4.9.4: Open Network & Internet Settings

10. The **Network Status** window appears. Click **Change adapter options** under **Change your network settings**.

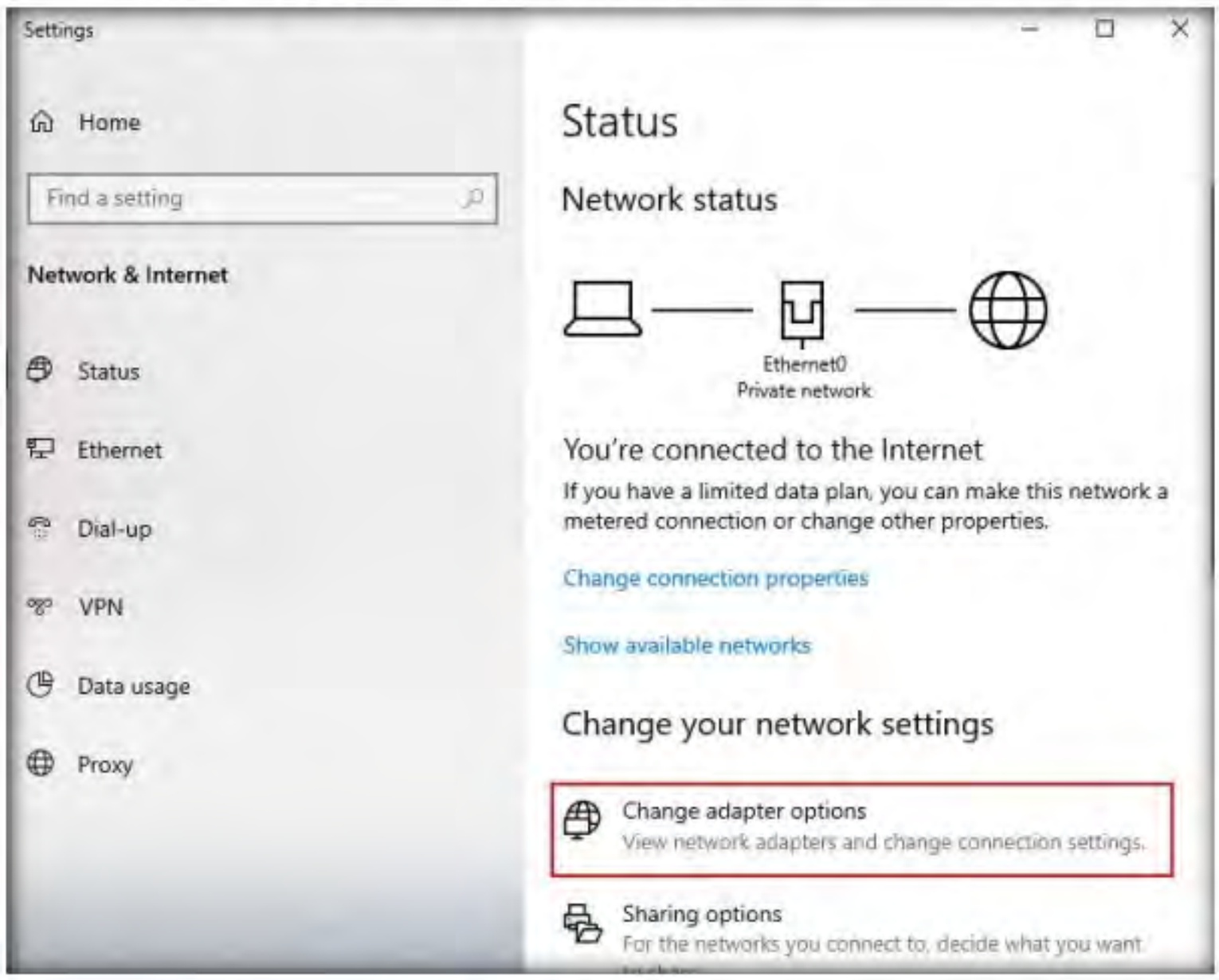


Figure 4.9.5: Change your network settings

11. Right-click on the network adapter (here, **Ethernet0**) and click **Properties**.

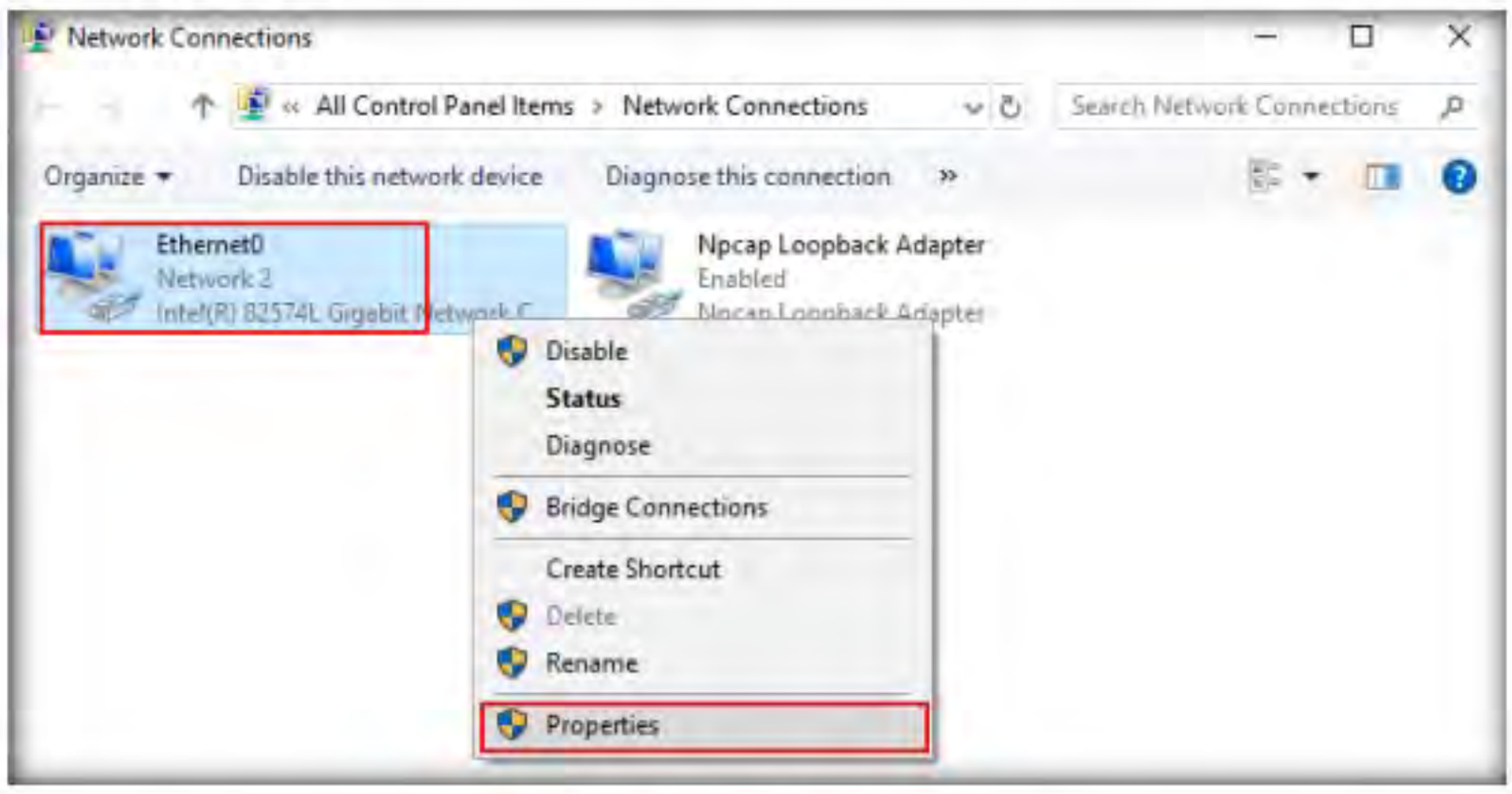


Figure 4.9.6: Available Network Adapter

12. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

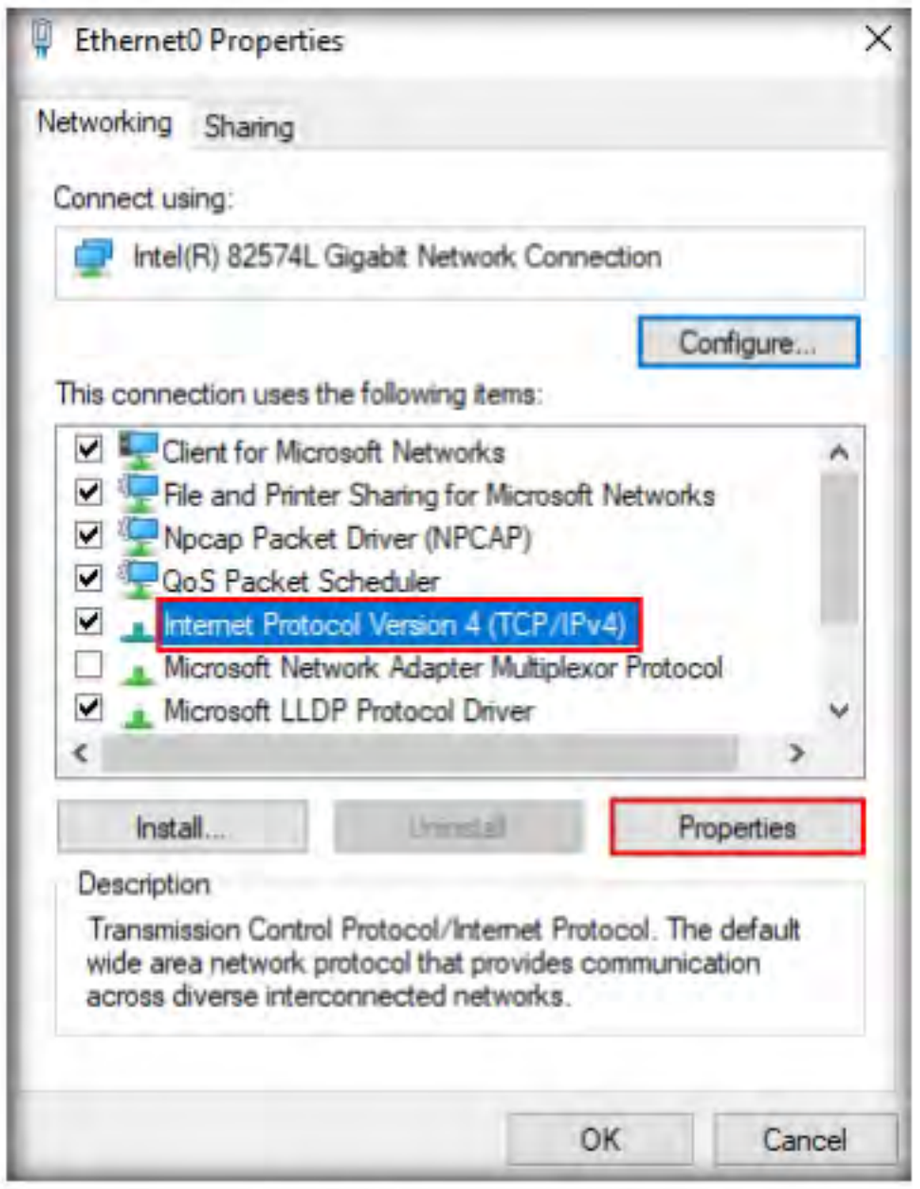


Figure 4.9.7: Adapter Properties

13. The **Internet Protocol Version 4(TCP/IPv4) Properties** window appears. Change the **Preferred DNS server** with the **Windows Server 2016** IP address and click **OK**. In this task, the **Windows Server 2016** IP address is **10.10.10.16**. This may vary in your lab environment.
14. Click **OK**, and then **Close** the Adapter Properties window.

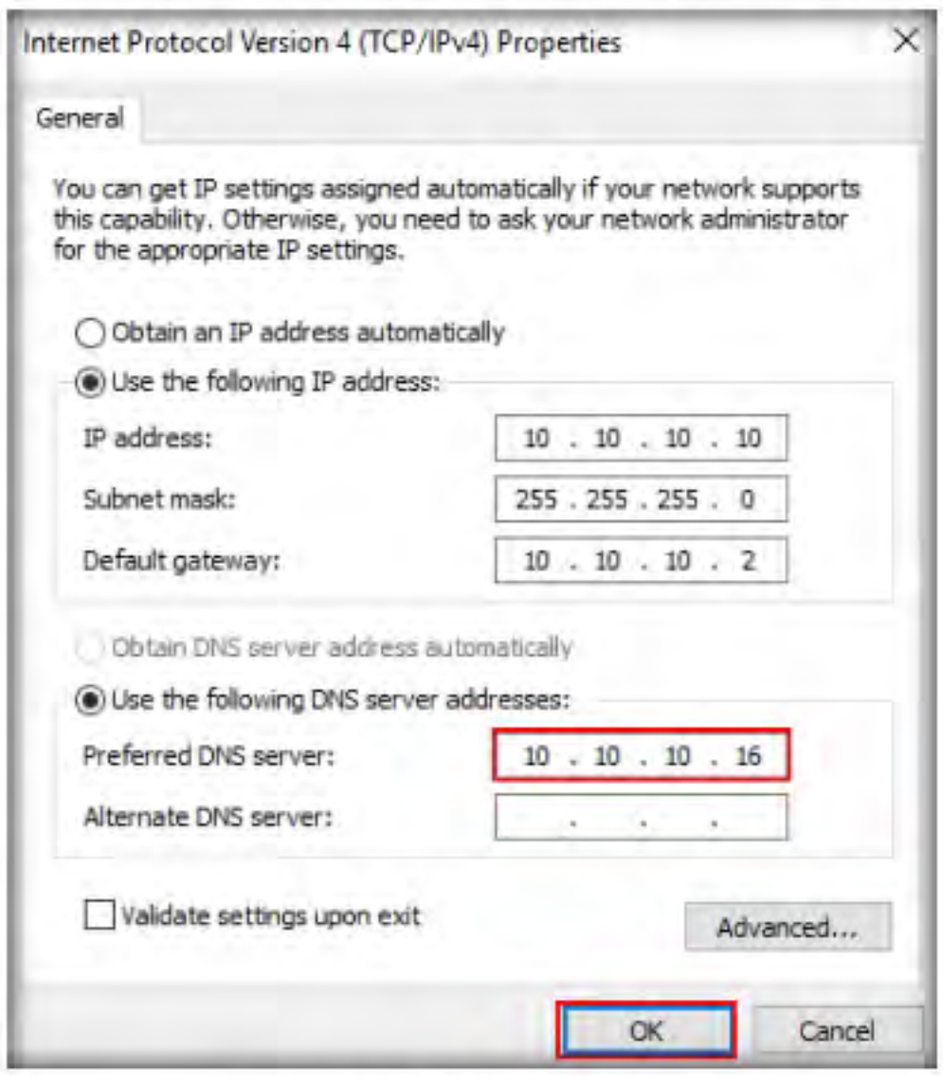


Figure 4.9.8: TCP/IPv4 Properties

15. Switch to the **DNSQuerySniffer** window; observe the few recorded logs. Right-click on the log for which DNS has changed and select **Properties** from the context menu.

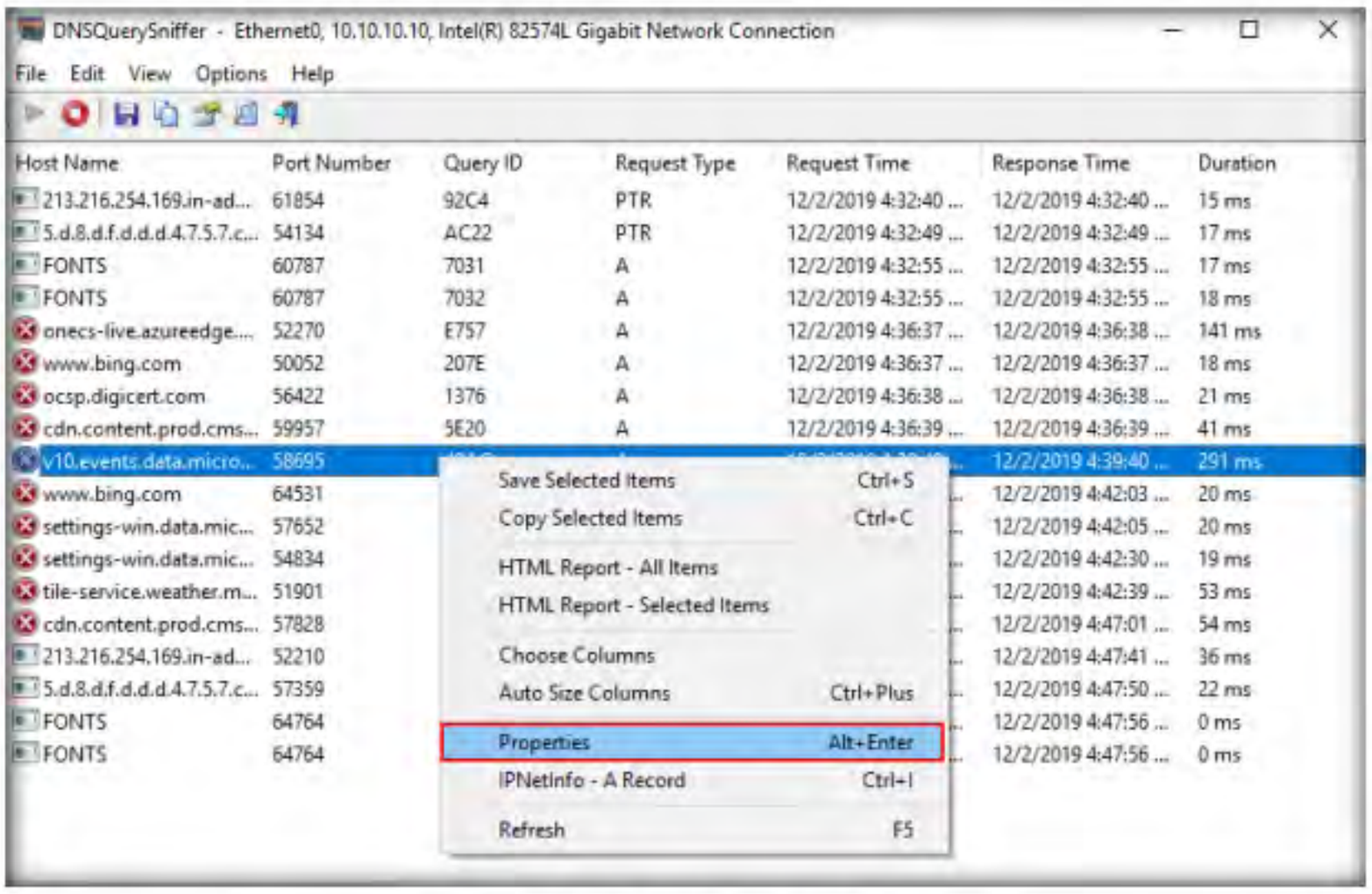


Figure 4.9.9: DNSQuerySniffer Logs

16. In the **Properties** window, observe that there is a change in DNS.

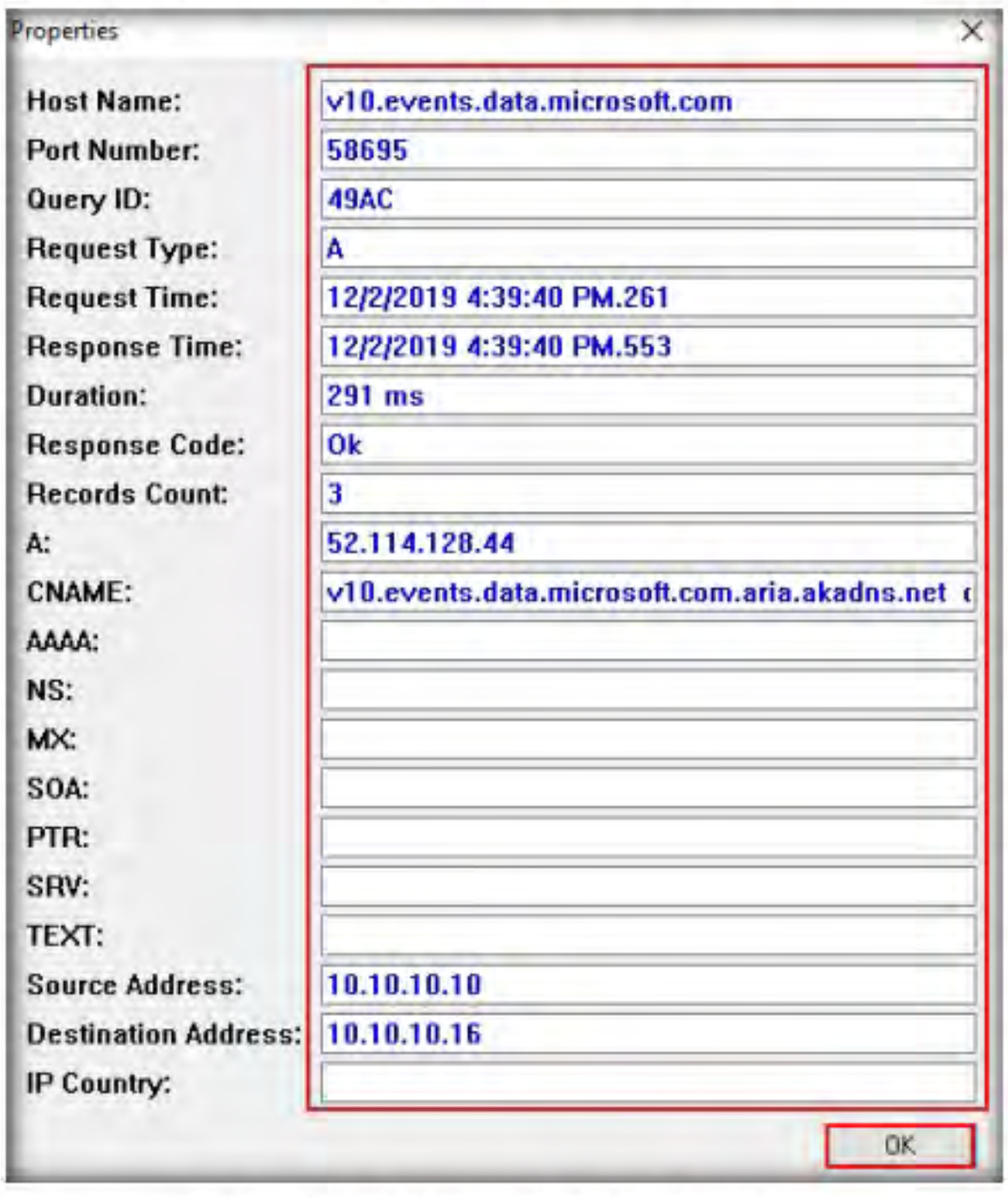


Figure 4.9.10: DNSQuerySniffer Log Properties

17. After completion of the task, go to the network settings, change DNS 8.8.8.8 in the **Windows 10** machine, and close all applications.
18. Uninstall the **DriverBooster** and **Advanced SystemCare** software by navigating to **Control Panel** → **Programs** → **Uninstall a program**.

Note: While uninstalling, remove all the files of tools from the system.

19. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.

You can also use other DNS monitoring/ resolution tools such as **DNSstuff** (https://www.dnsstuff.com), **DNS Lookup Tool** (https://www.ultratools.com), or **Sonar Lite** (https://constellix.com) to perform DNS monitoring.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs