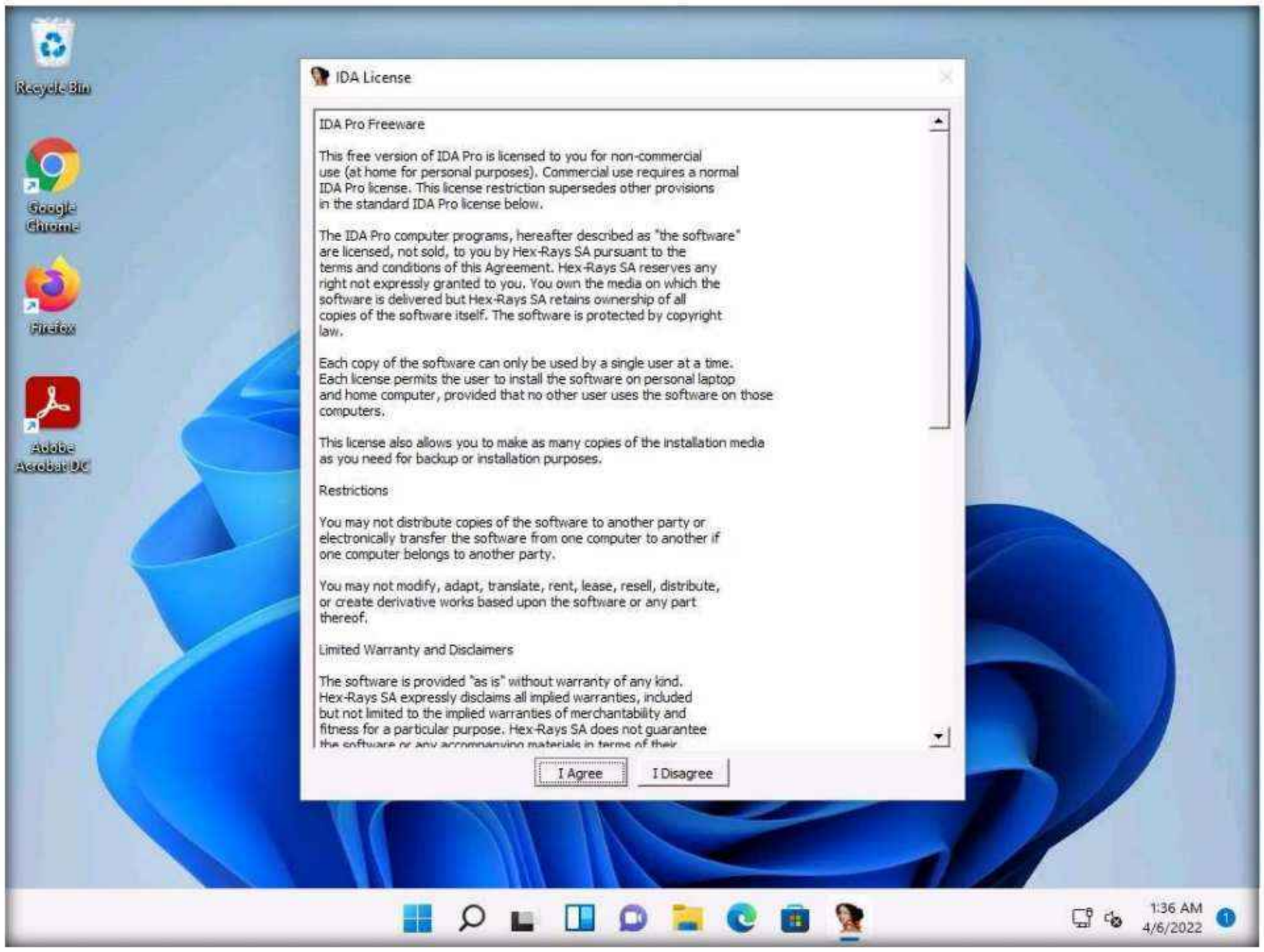
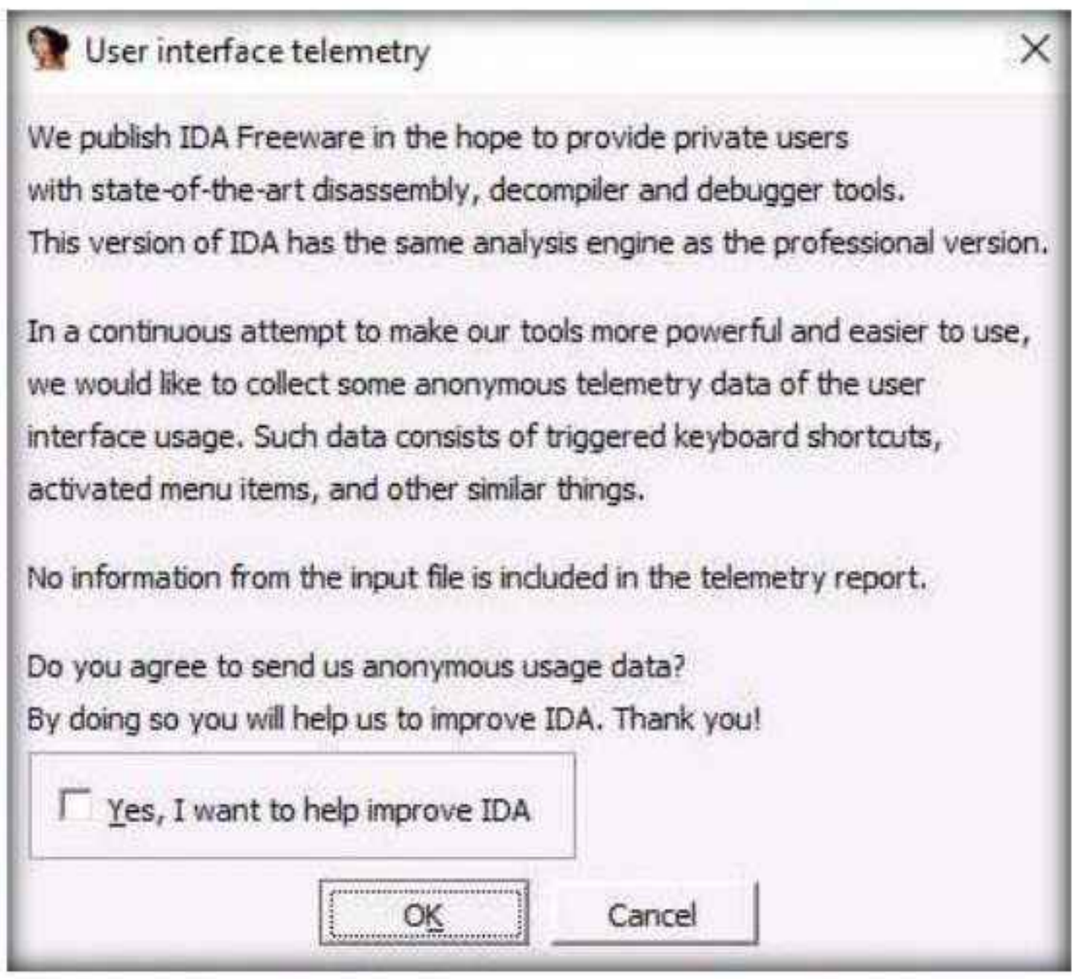
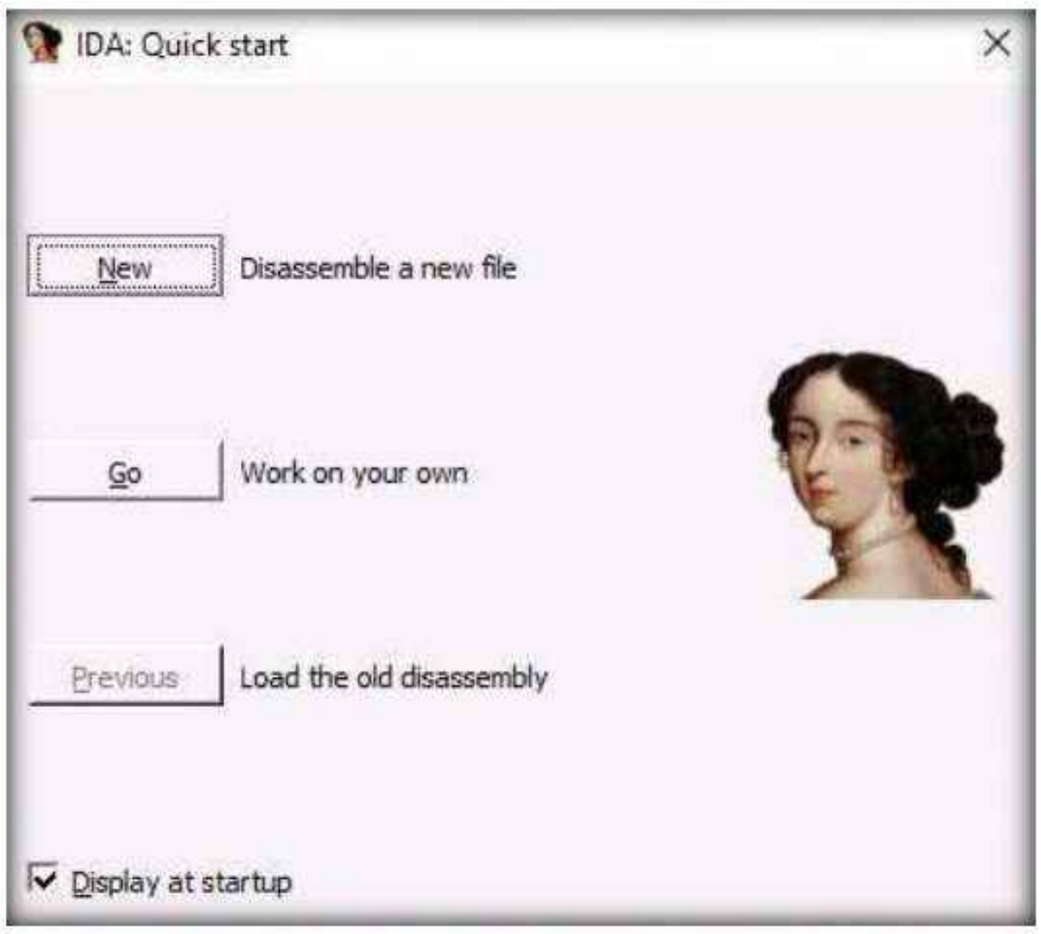
2. If the **IDA License** window appears, click on **I Agree**.



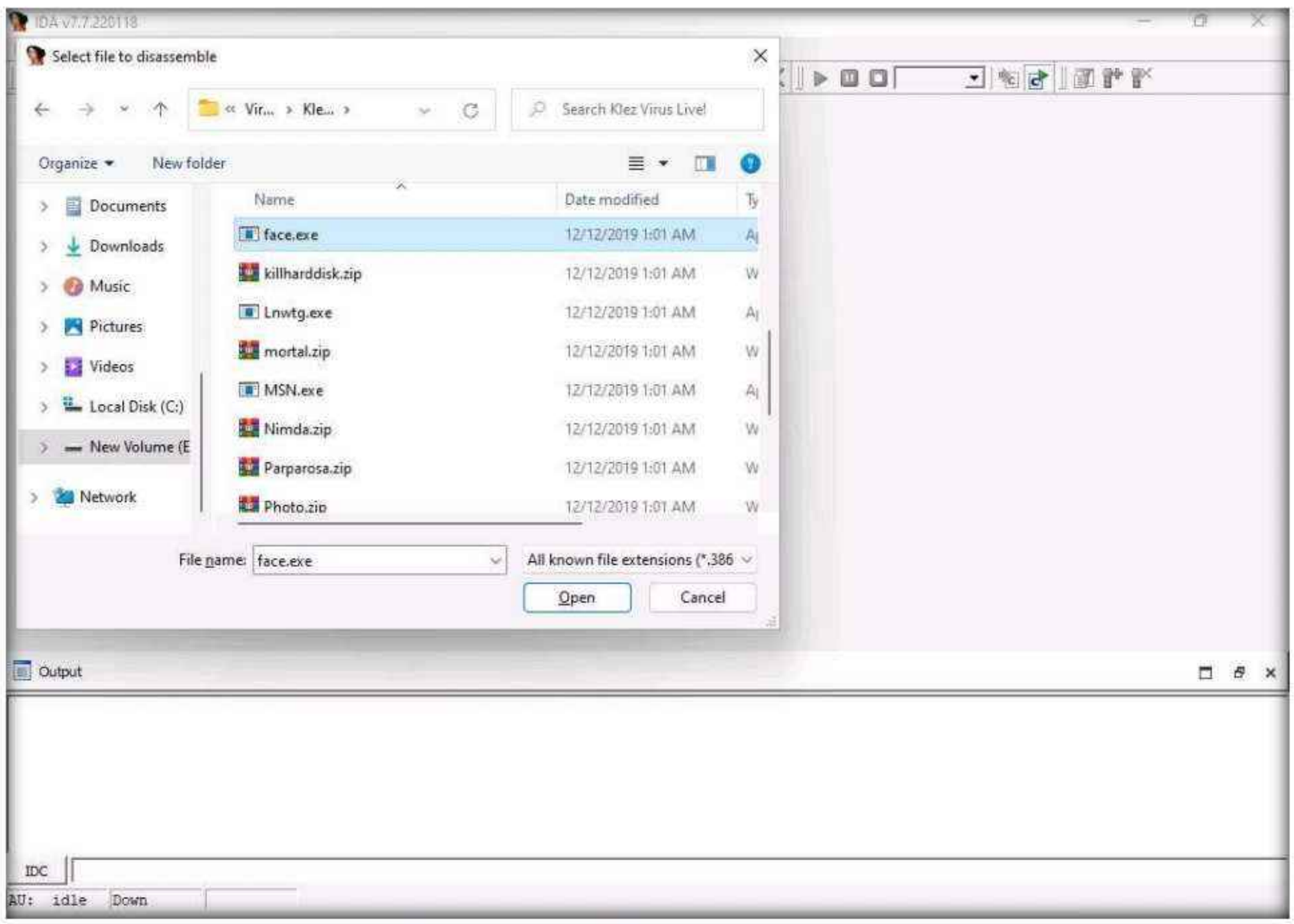
3. **User interface telemetry** window appears, uncheck **Yes, I want to help improve IDA** checkbox and click **OK**.



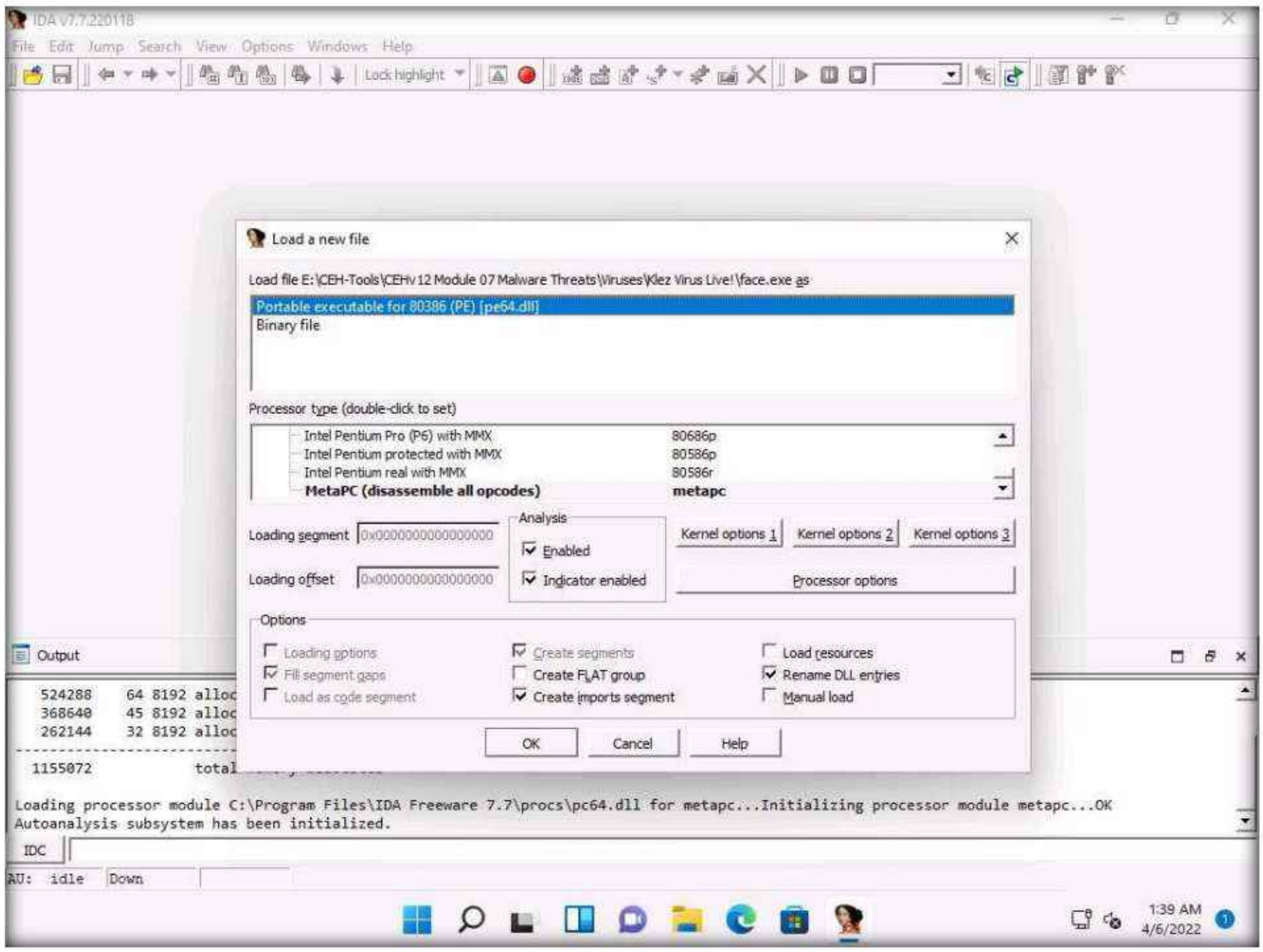
4. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.



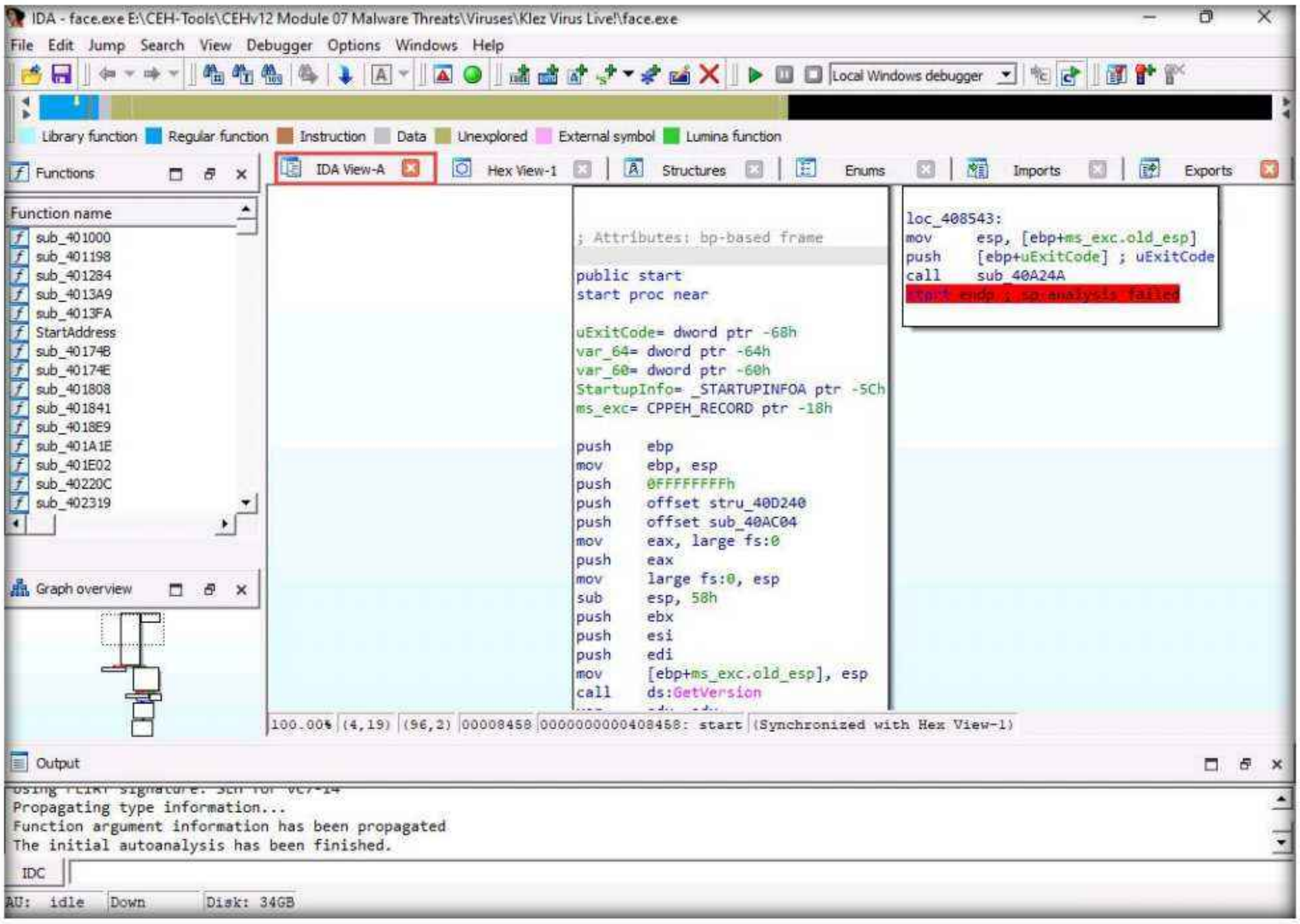
5. The **IDA** main window appears, along with the **Select file to disassemble** window.
6. In the **Select file to disassemble** window, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Open**.



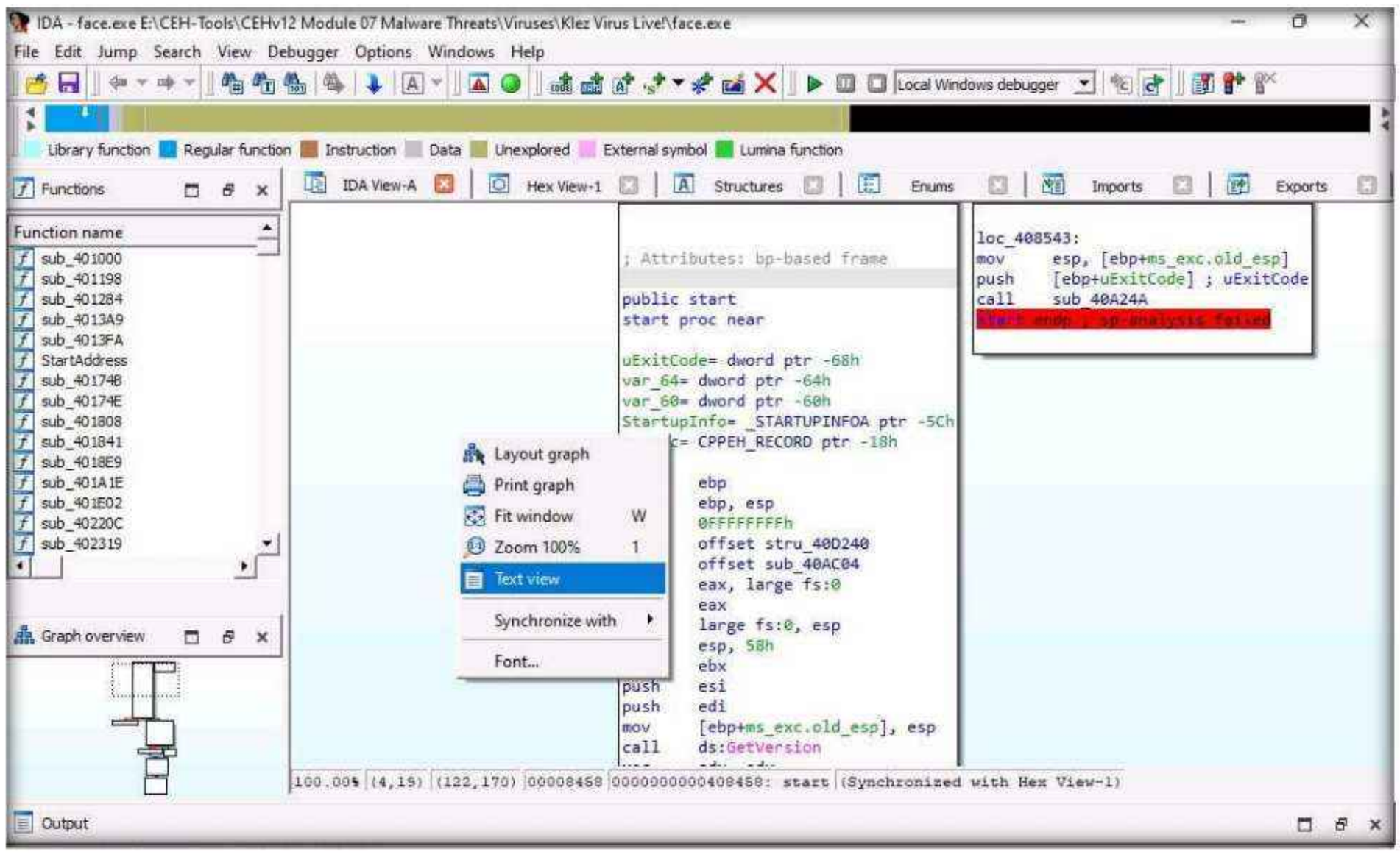
7. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.



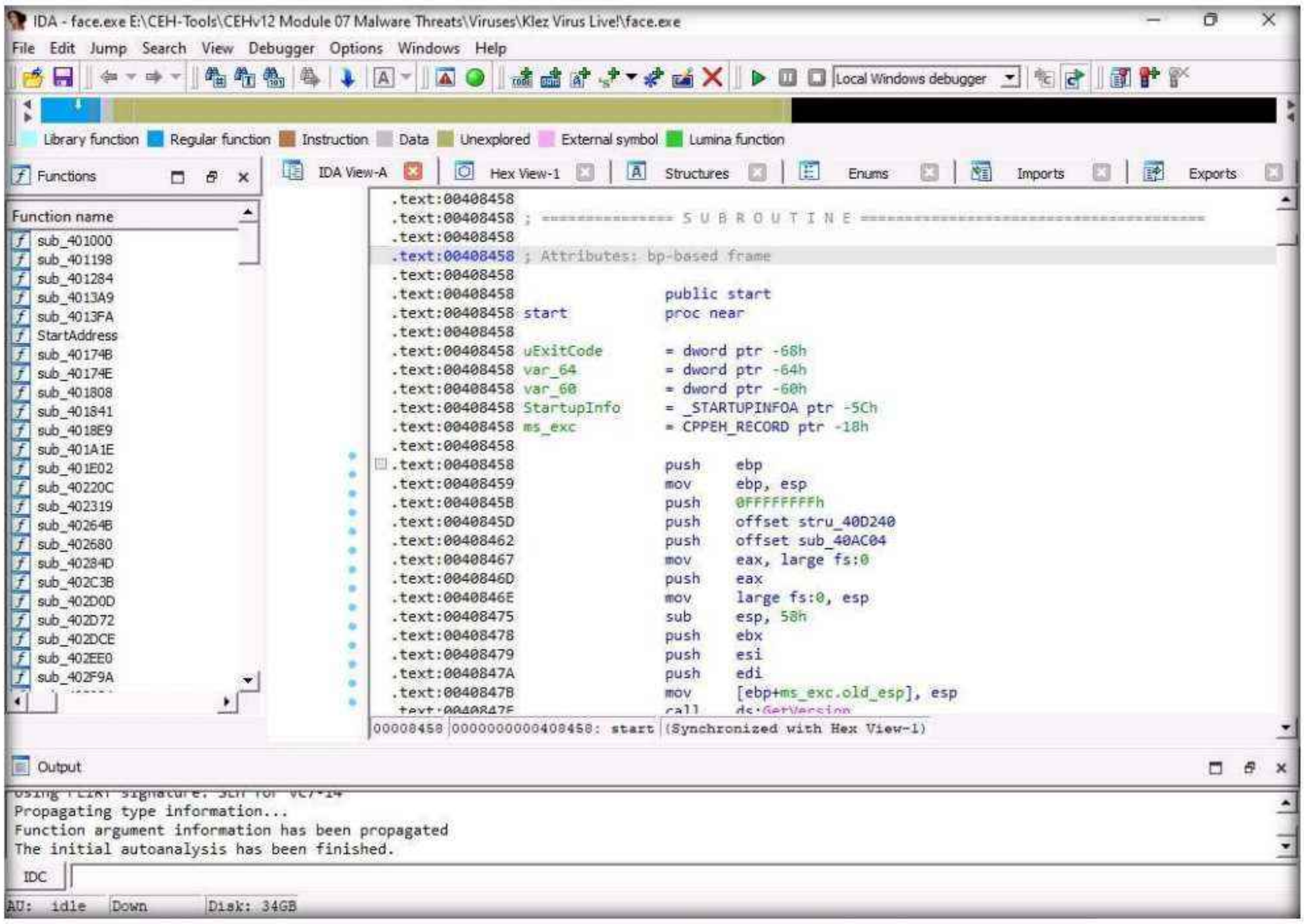
8. If a **Warning** pop-up appears, click **OK**.
9. If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.
10. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.



11. 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.

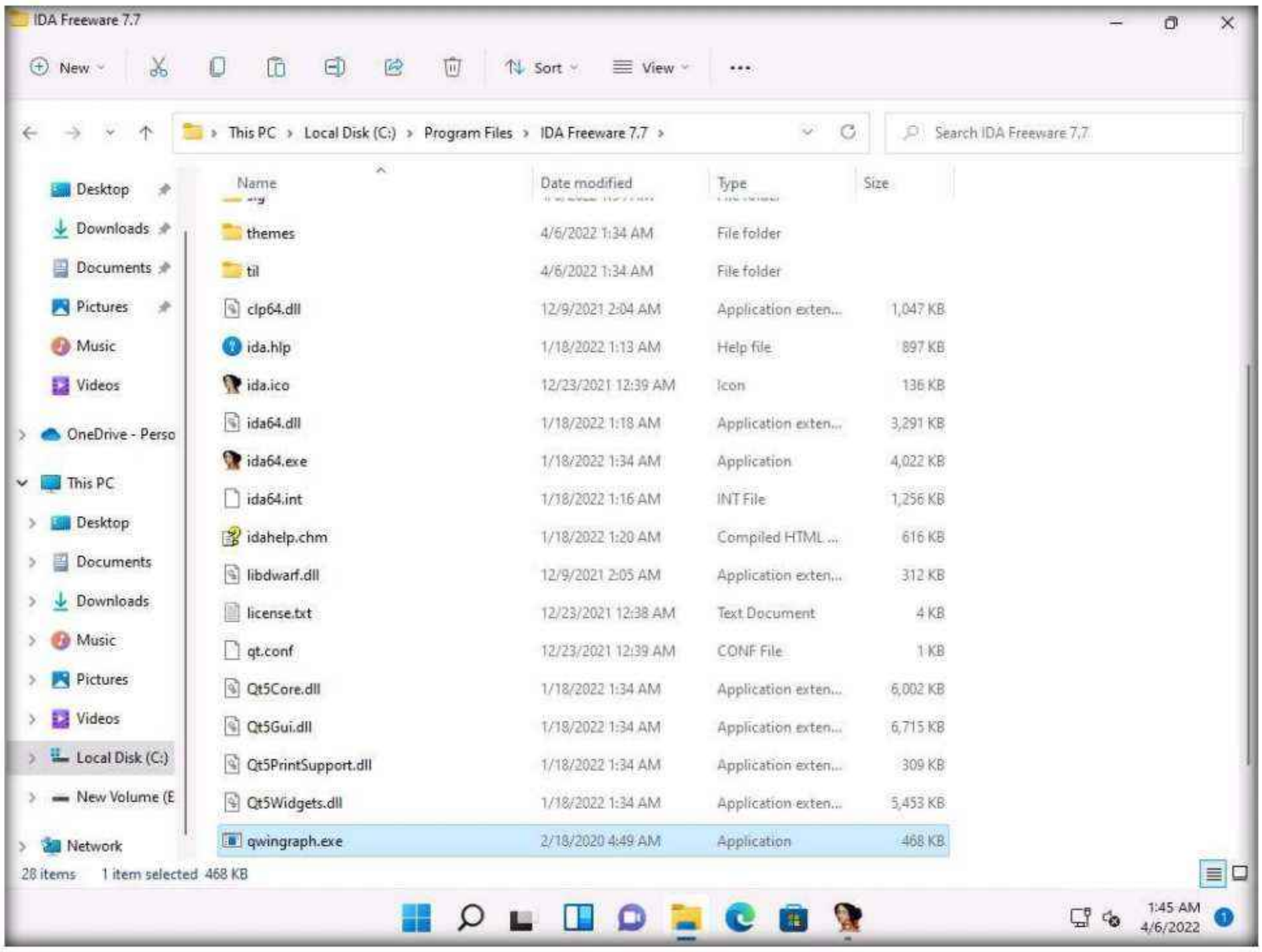


12. This reveals the text view of the malicious file, allowing analysis of its information.

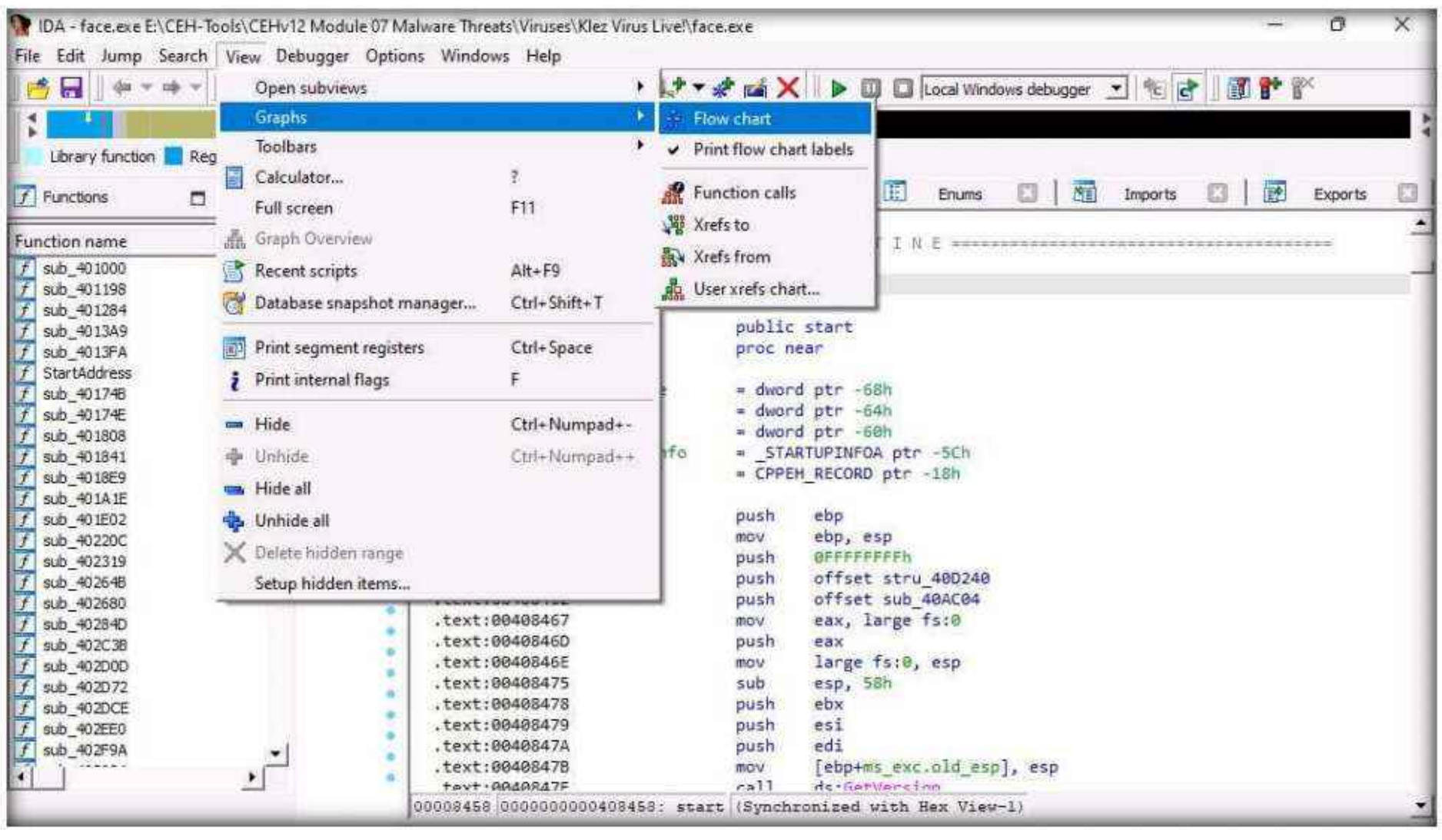


13. Now, minimize the IDA window, and navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**. Copy the **qwingraph.exe** file and paste it in IDA's installation location. In this task, the location is **C:\Program Files\IDA Freeware 7.7**.

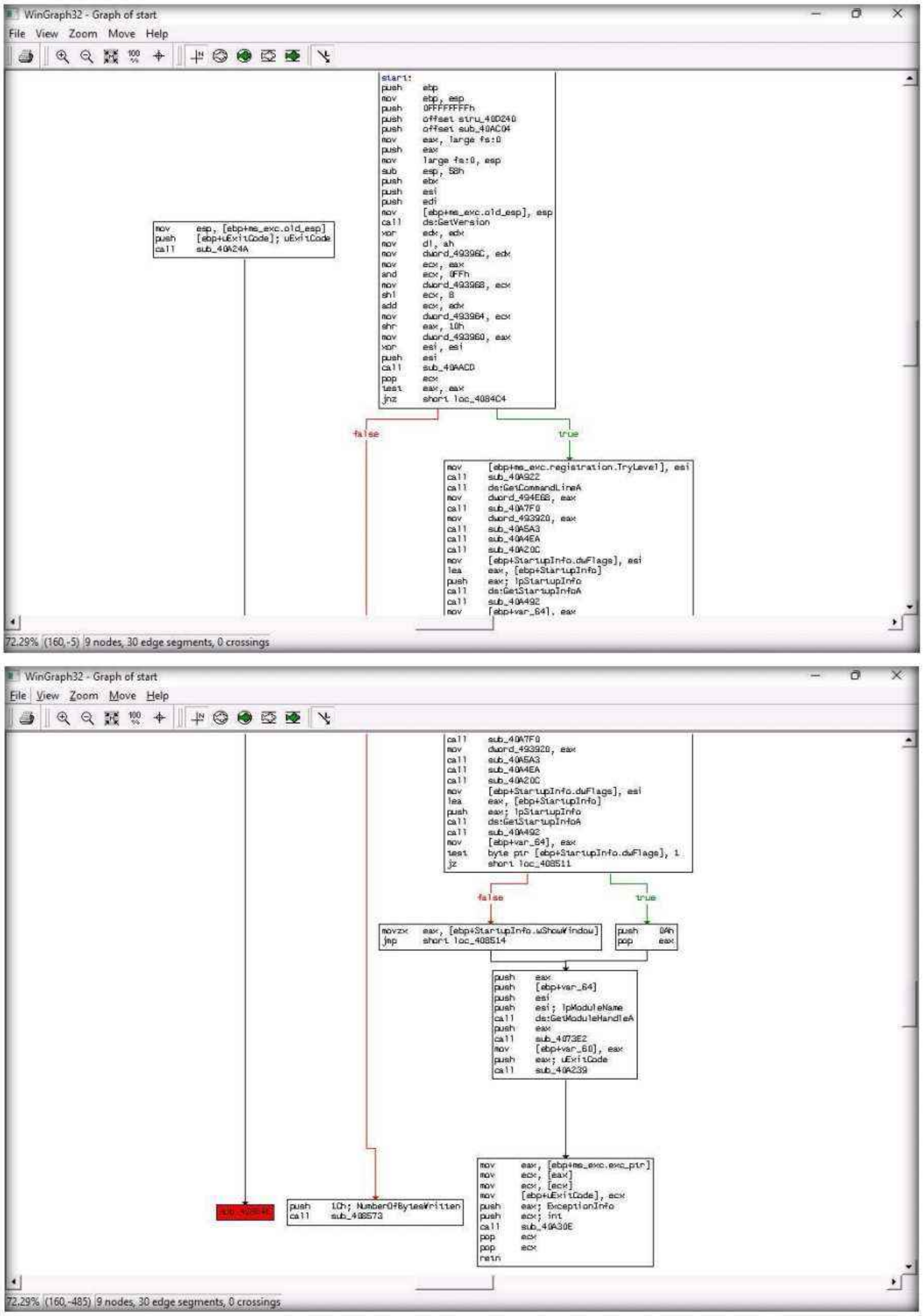
    Note: If a **Destination Folder Access** Denied notification appears, click **Continue**.



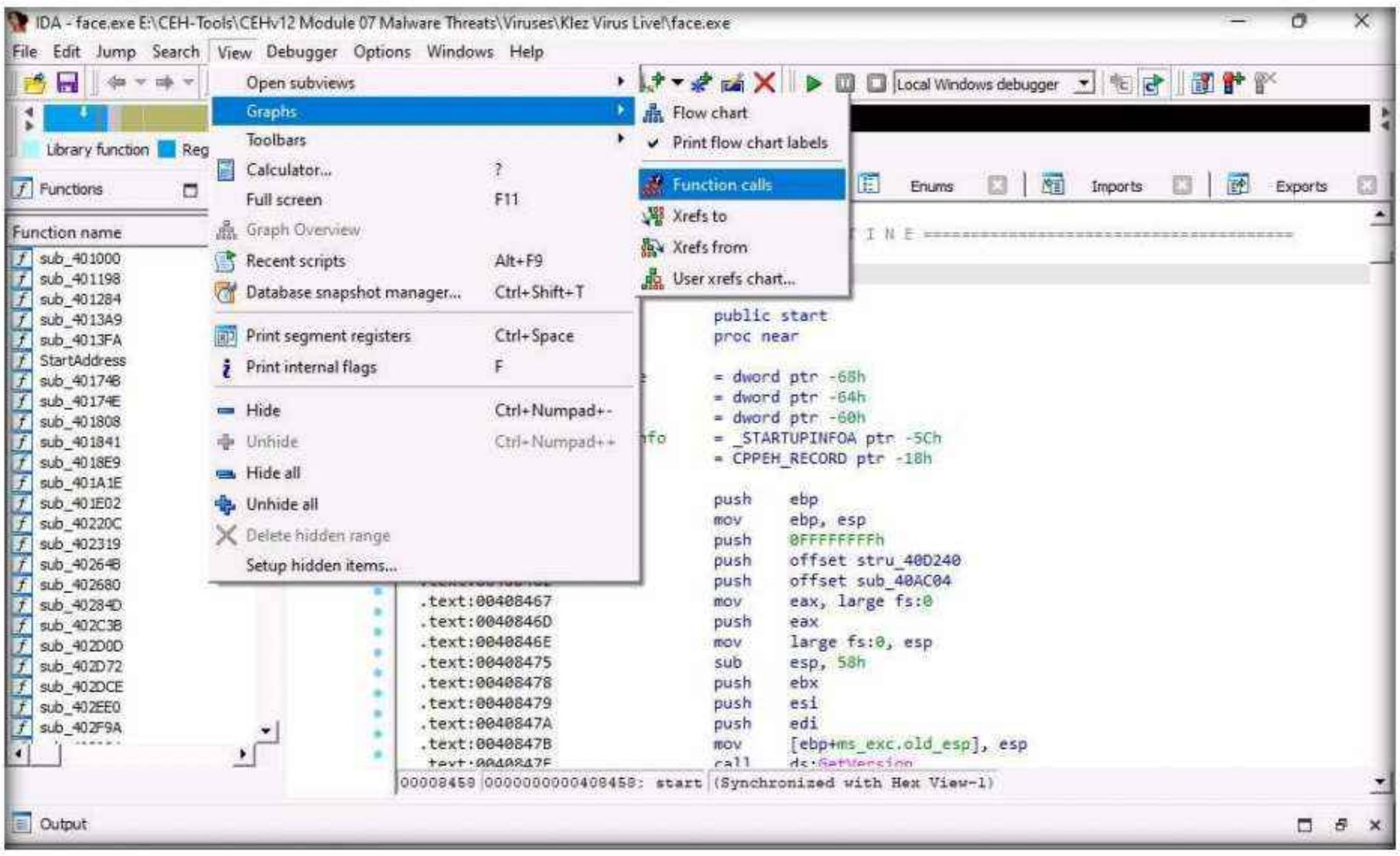
14. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View → Graphs** and click **Flow chart**.



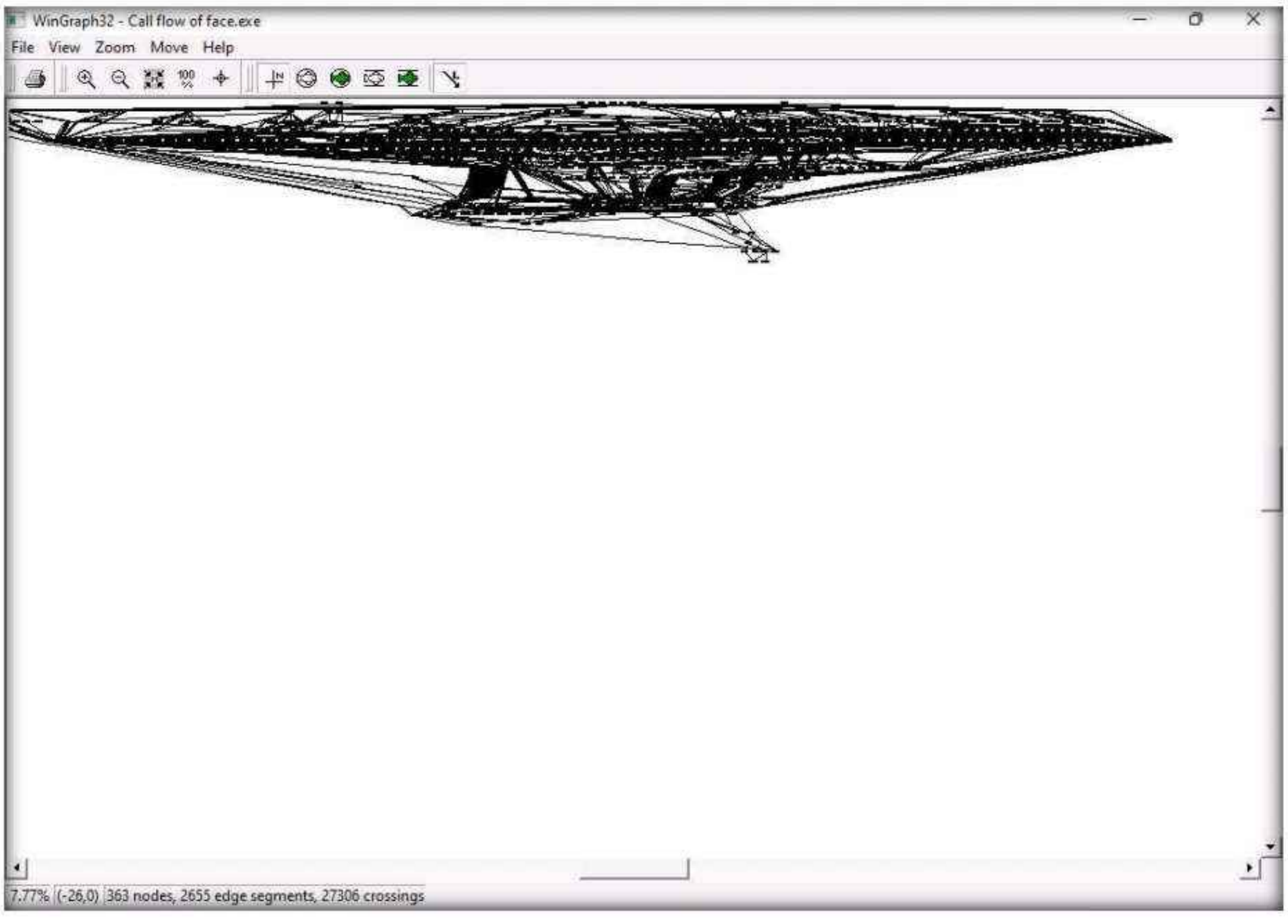
15. A **Graph** window appears with the flow. You may zoom in and adjust the screen to view this more clearly.

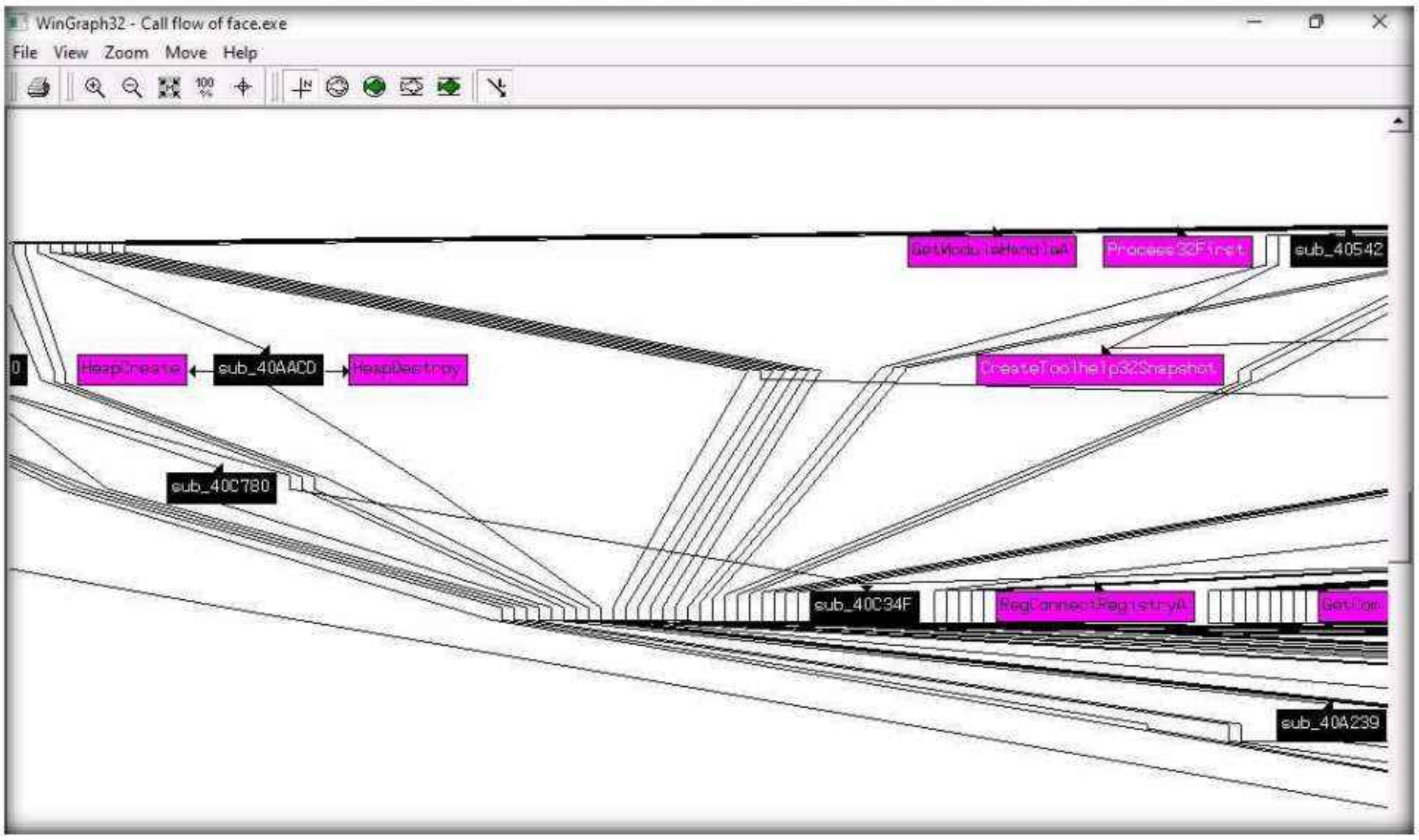


16. Close the **Graph** window, go to **View → Graphs**, and click **Function calls** from the menu bar.

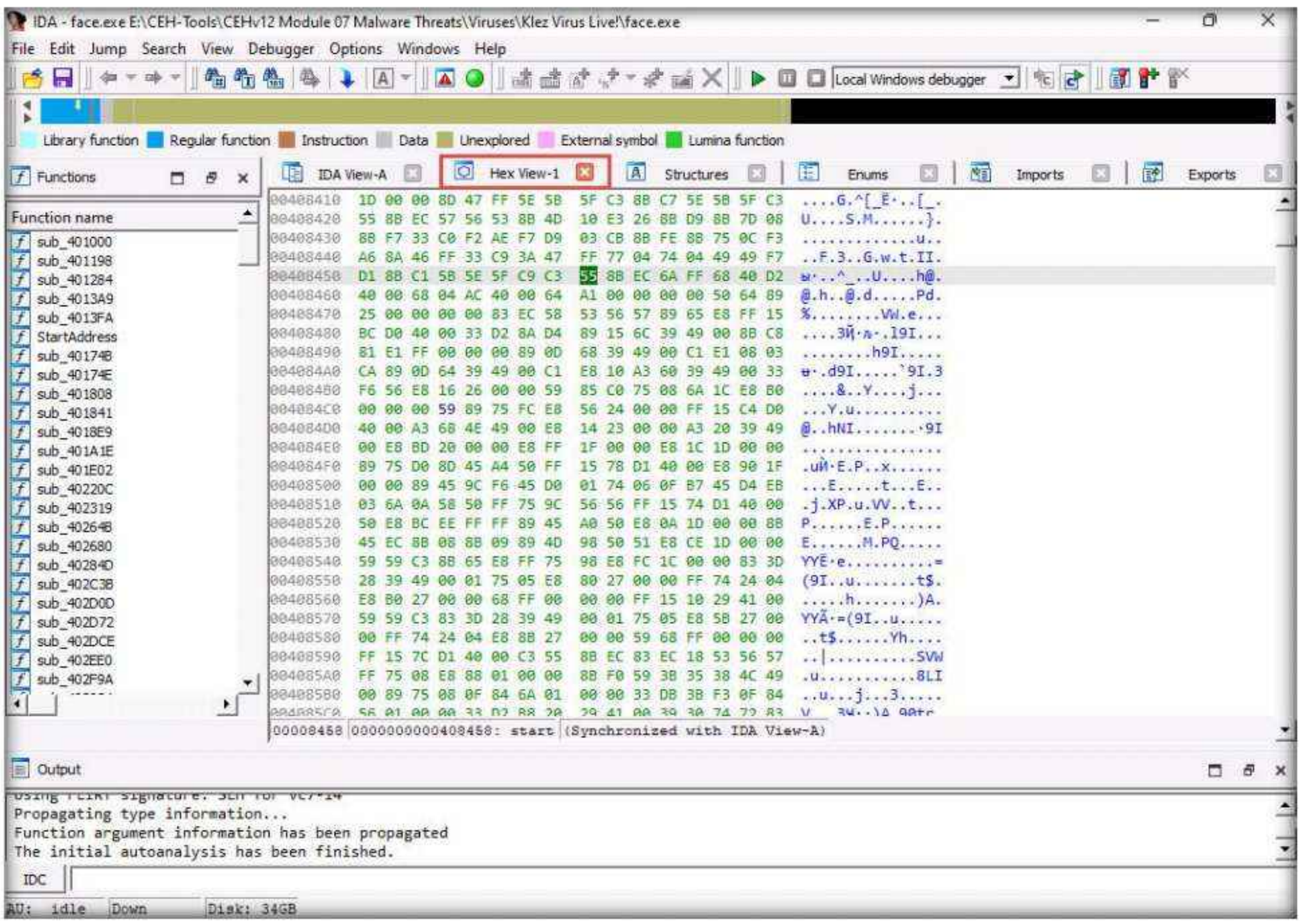


17. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.

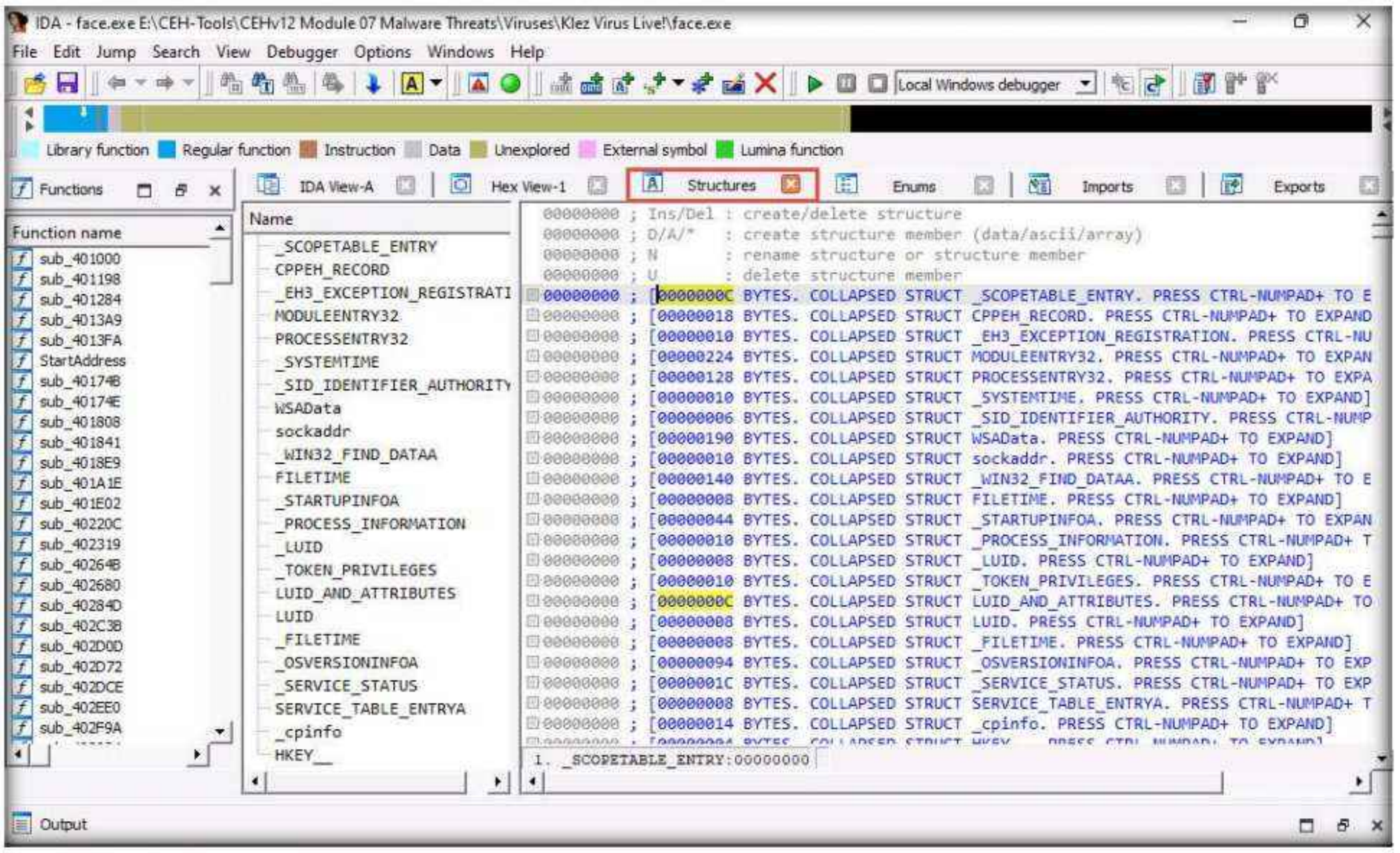




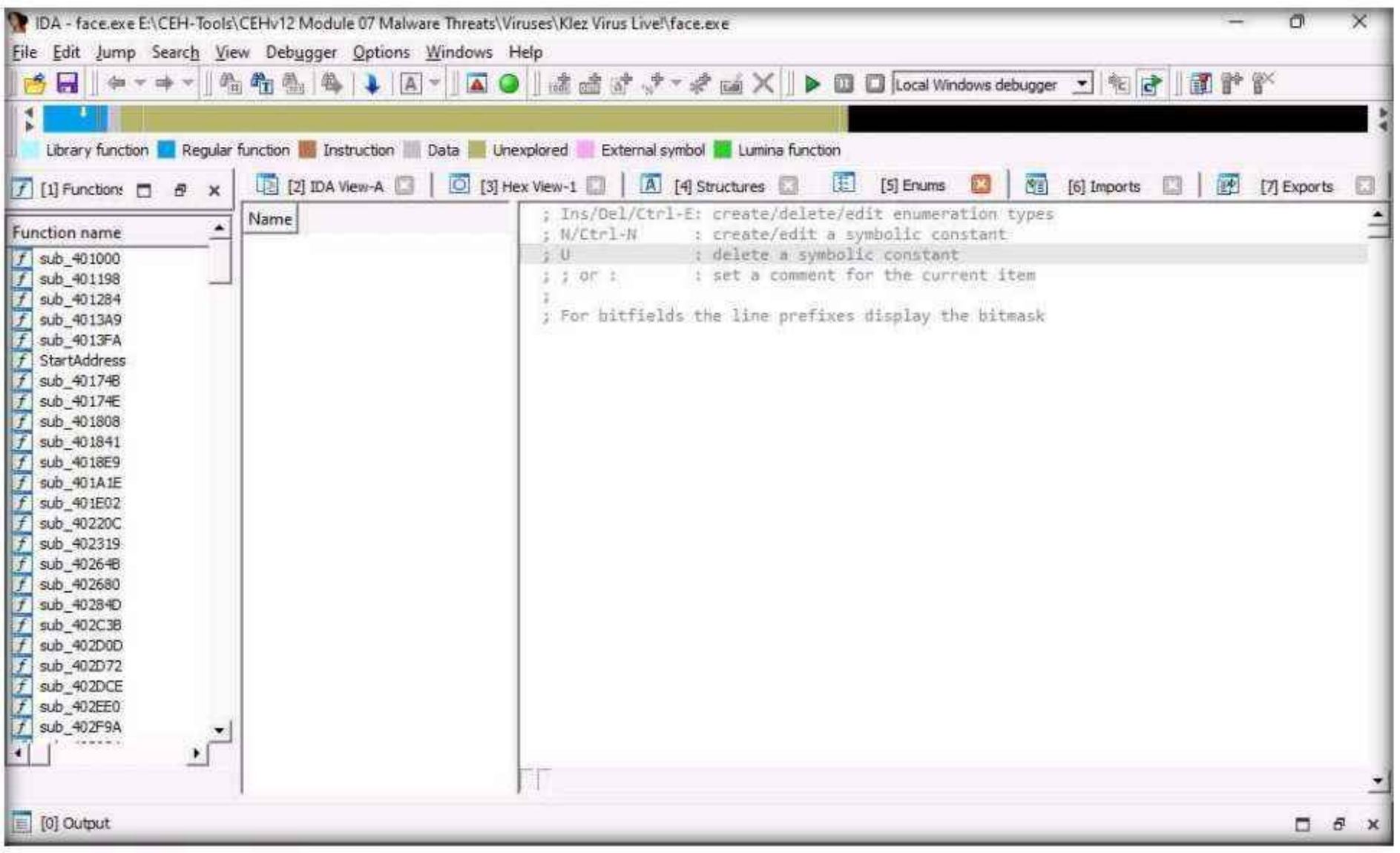
18. Click the **HexView-1** tab to view the hex value of the malicious file.



19. Click the **Structures** tab to view the structure of the file, as shown in the screenshot.



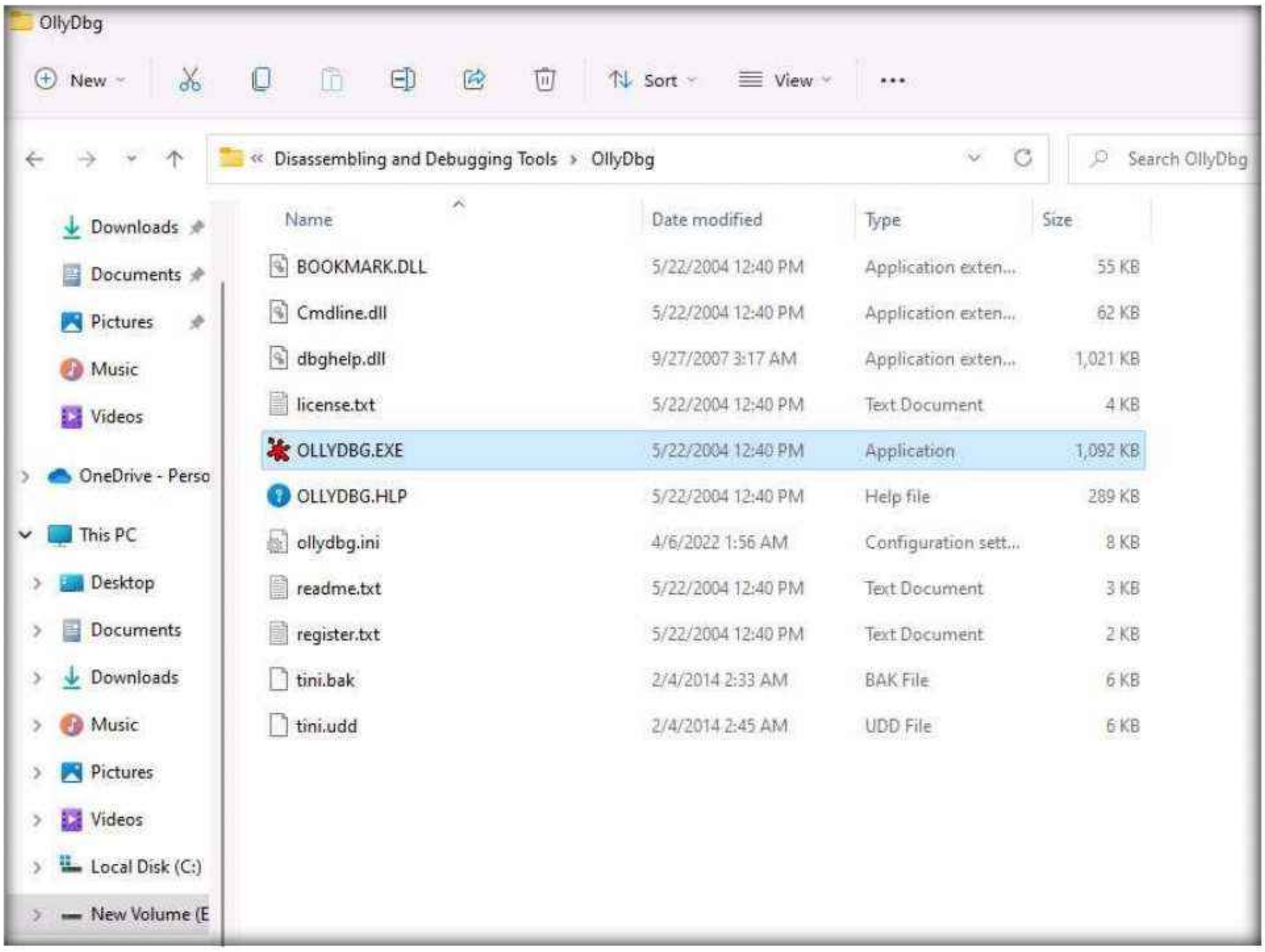
20. Click the **Enums** tab to view the Windows Enum results, as shown in the screenshot



21. Close all open windows. In the **Save database** pop-up, click **OK**.

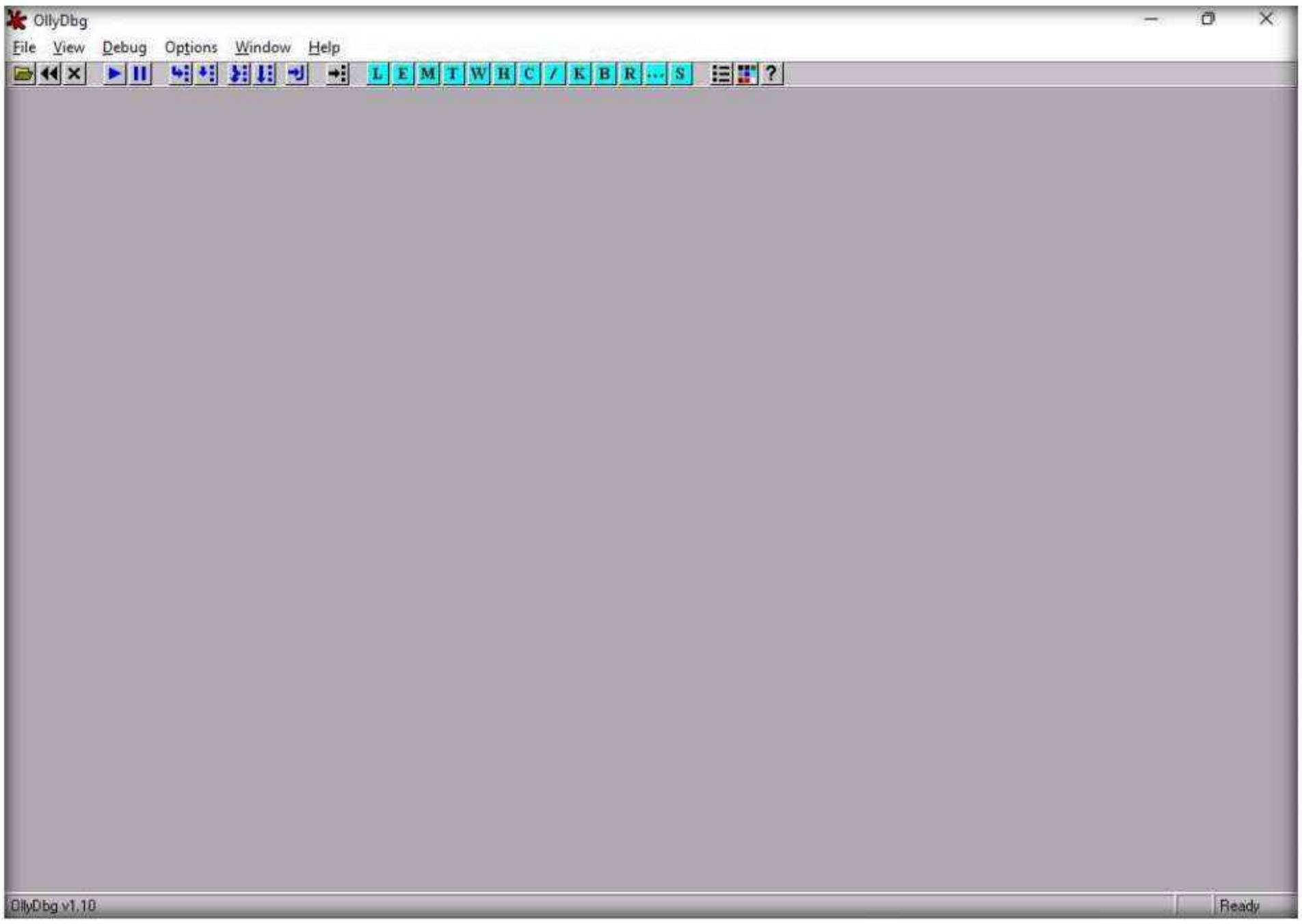
22. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **OLLYDBG.EXE**.

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

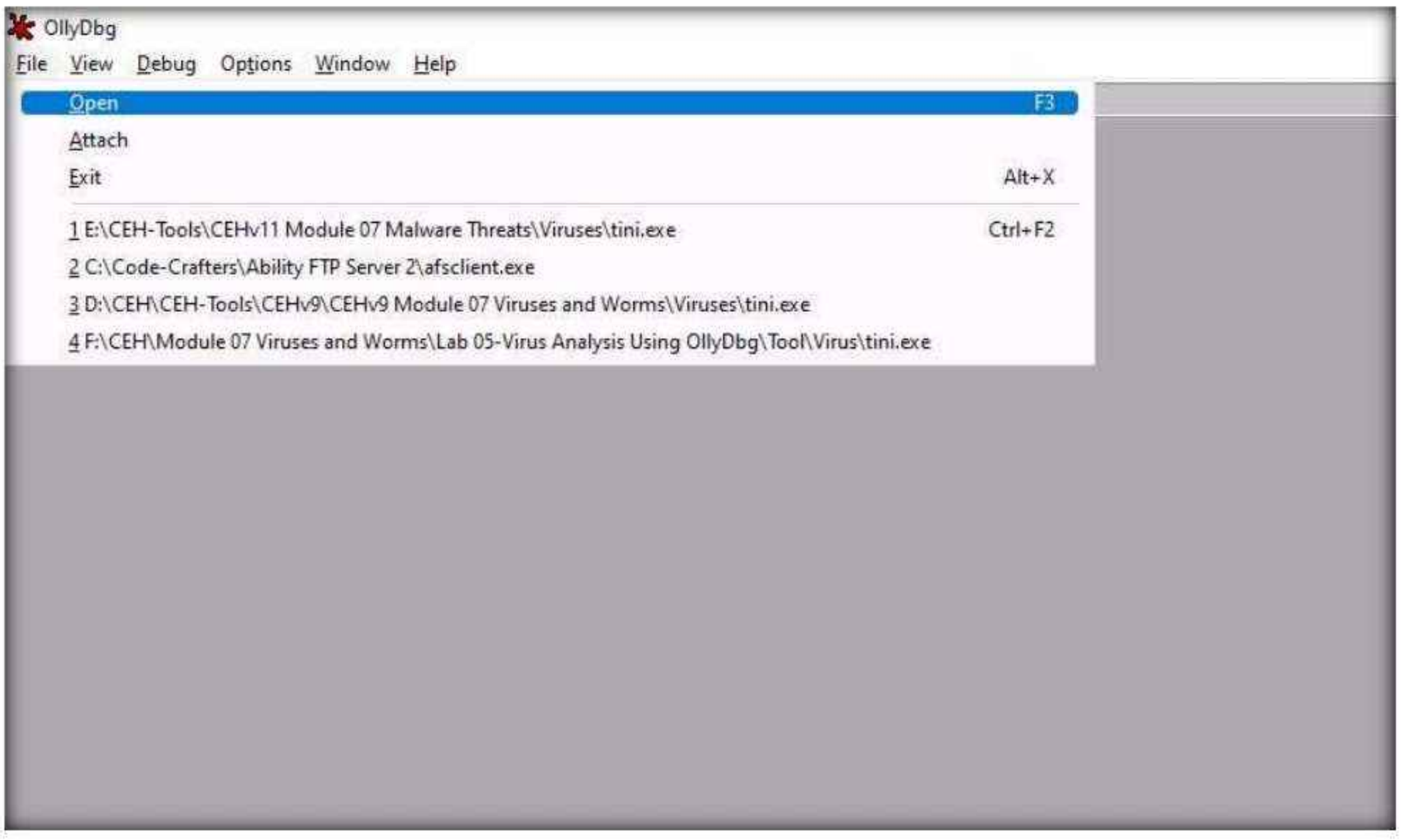


23. If a **UDD Directory Absent** dialog box appears, click **OK**.
24. If an OllyDbg warning message appears, for administrative rights, click **OK**.
25. The **OllyDbg** main window appears, as shown in the screenshot.

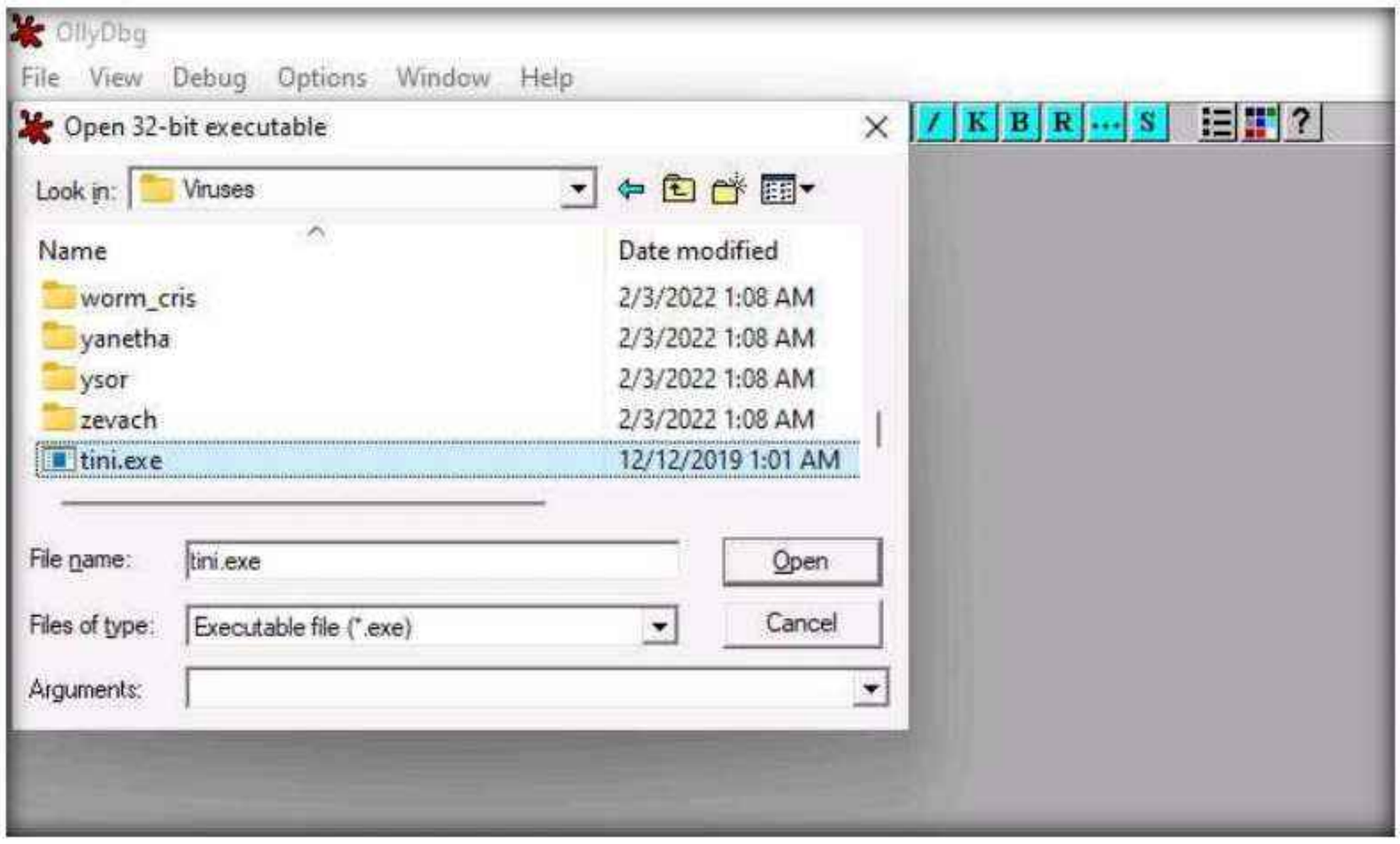
    Note: When you launch OllyDbg for the first time, several sub-windows might appear in the main window of OllyDbg; close all of them.



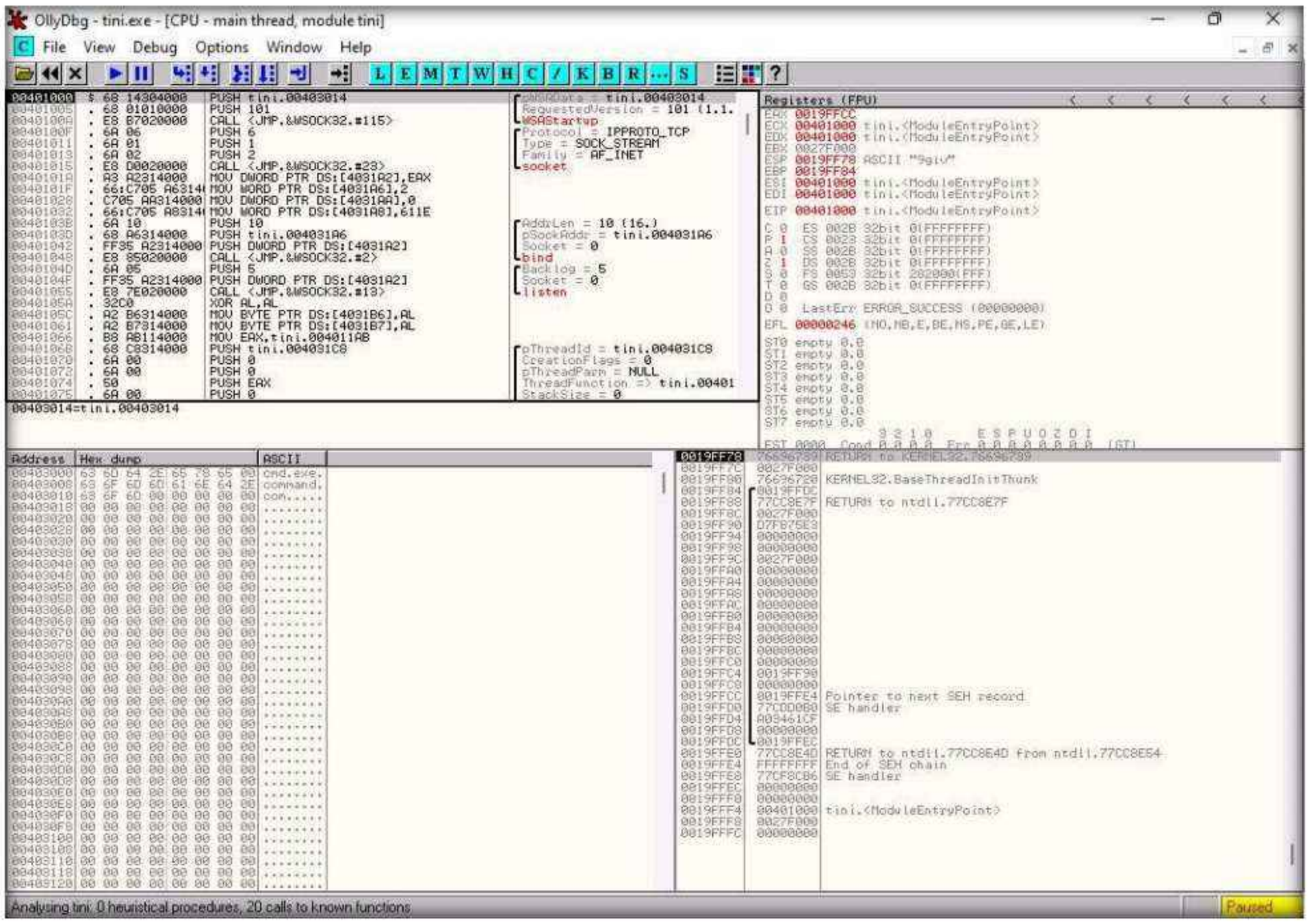
26. Choose **File** from the menu bar, and then choose **Open**.



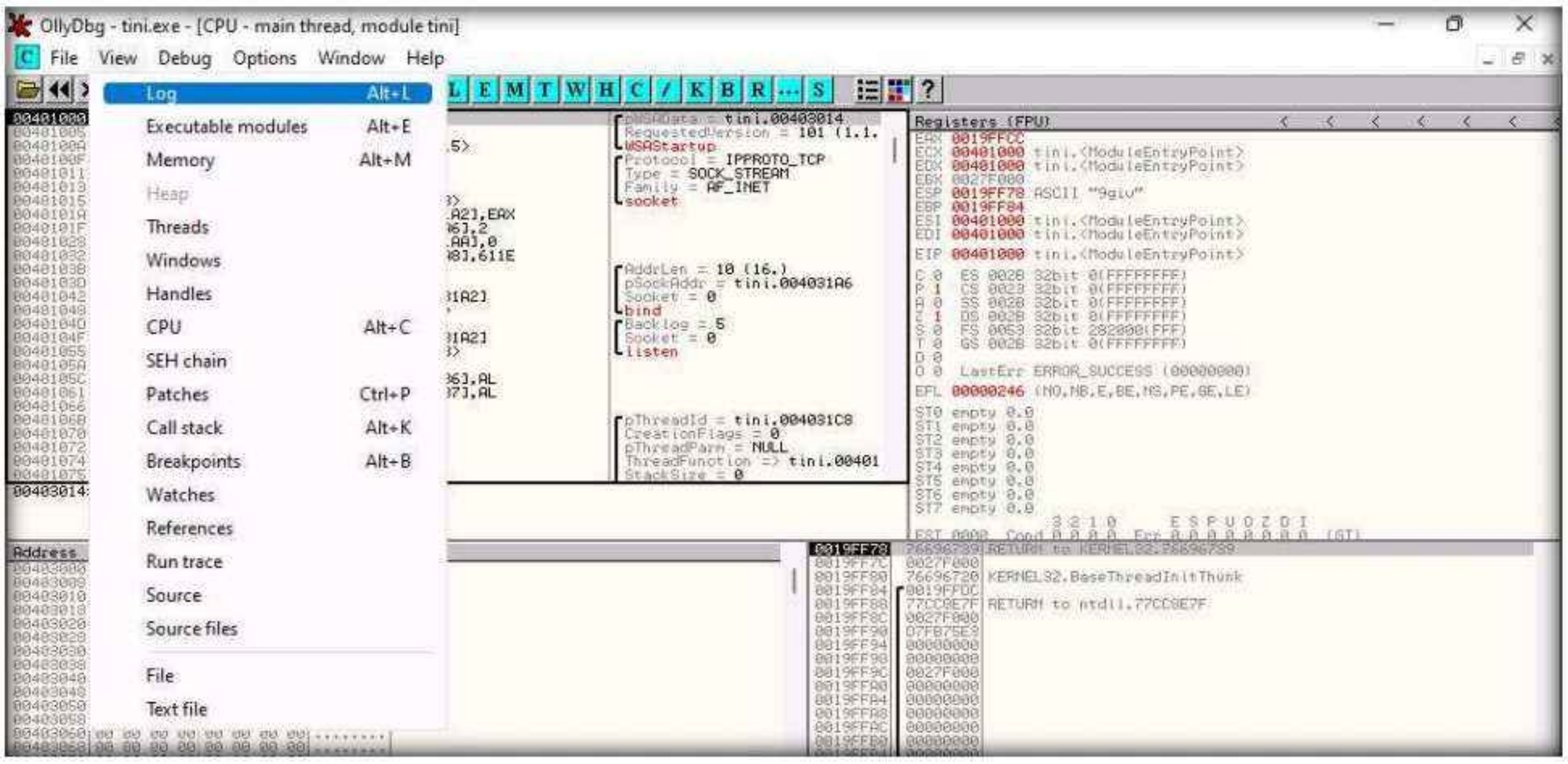
27. The **Open 32-bit executable** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.



28. The output appears in a window named **CPU - main thread, module tini**, maximize the window.

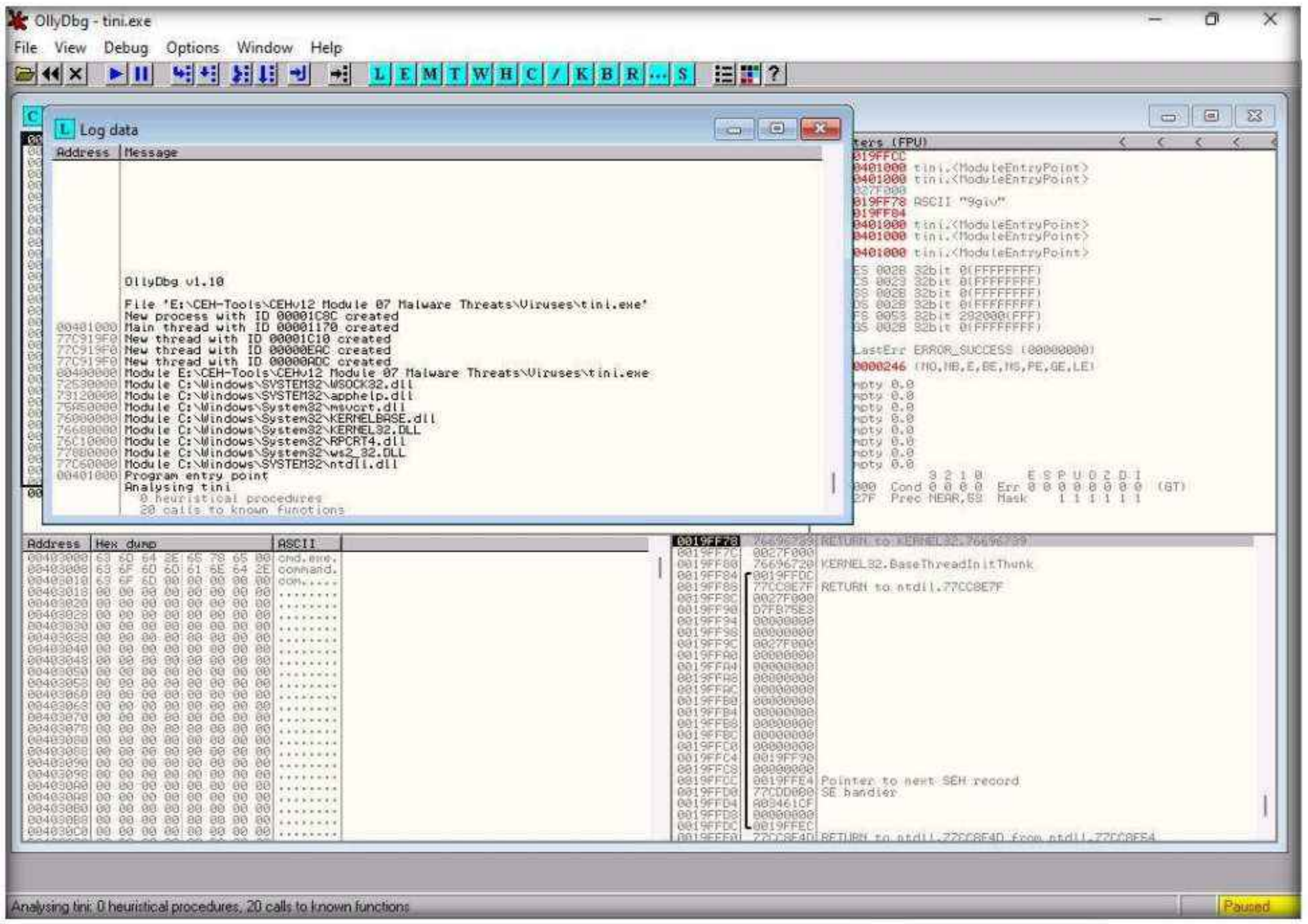


29. Choose **View** in the menu bar, and then choose **Log**.

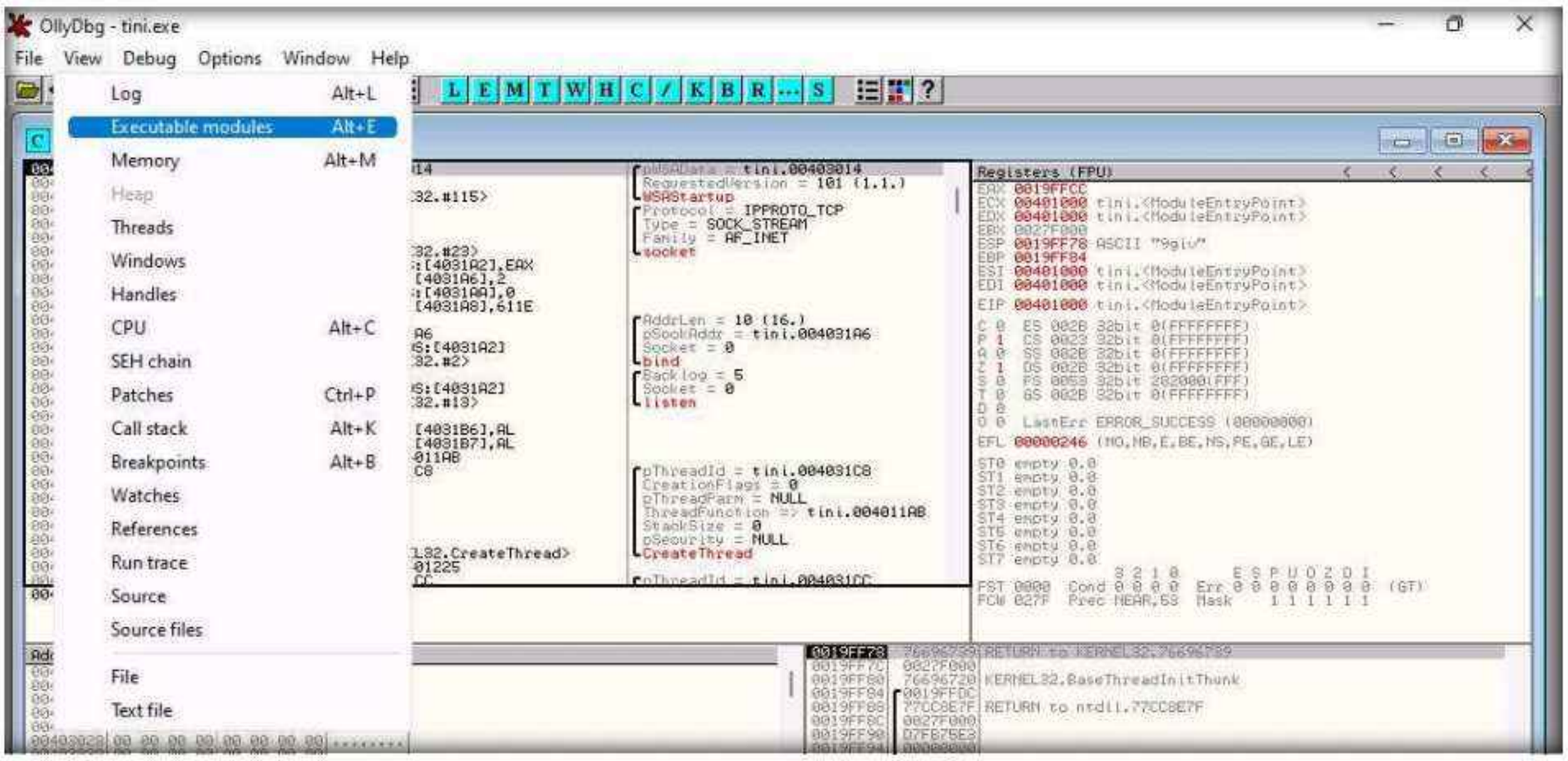


30. A window named **Log data** appears in OllyDbg, displaying the log details, as shown in the screenshot.

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



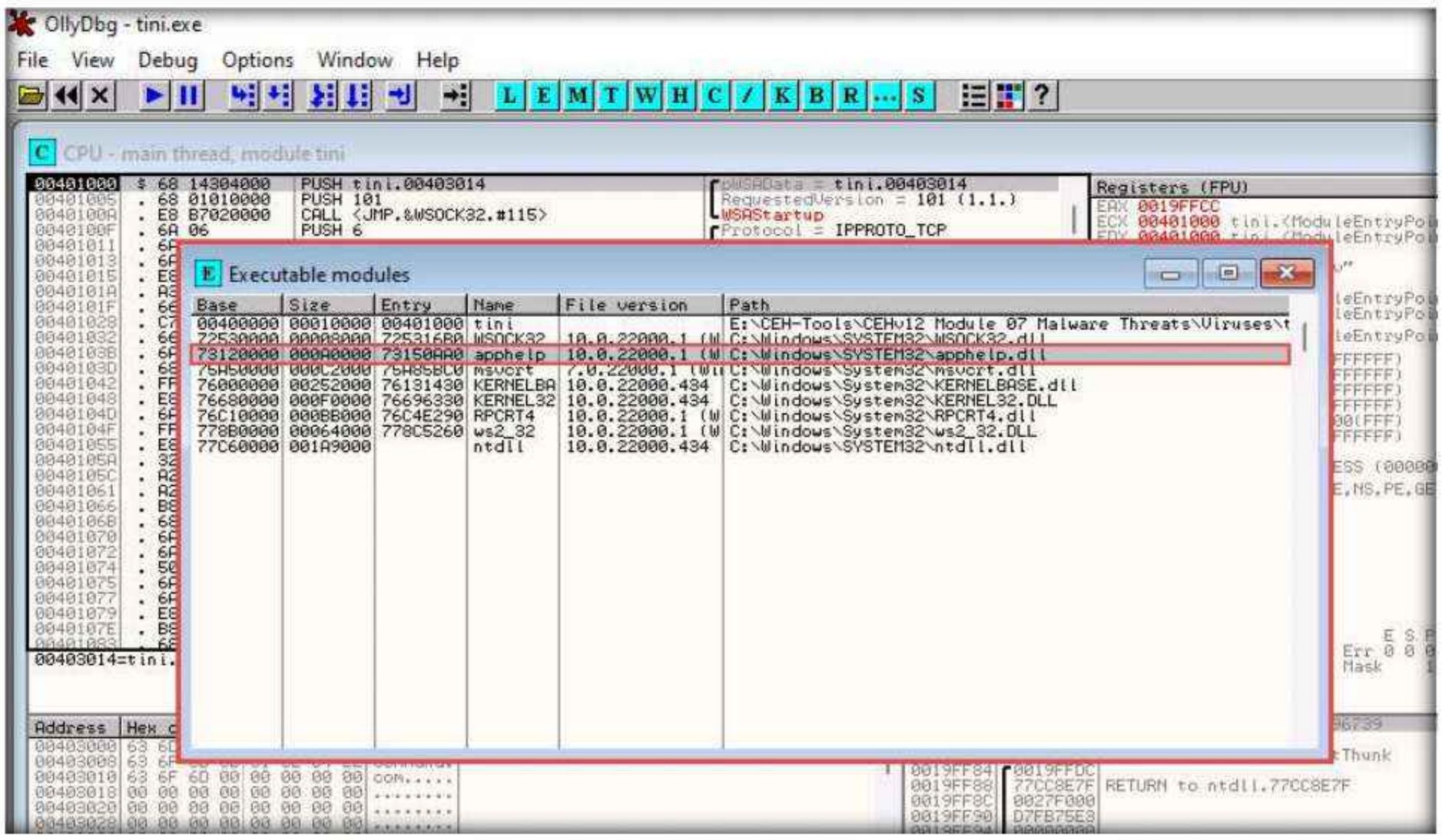
32. Choose **View** in the menu bar, and then choose **Executable modules**.



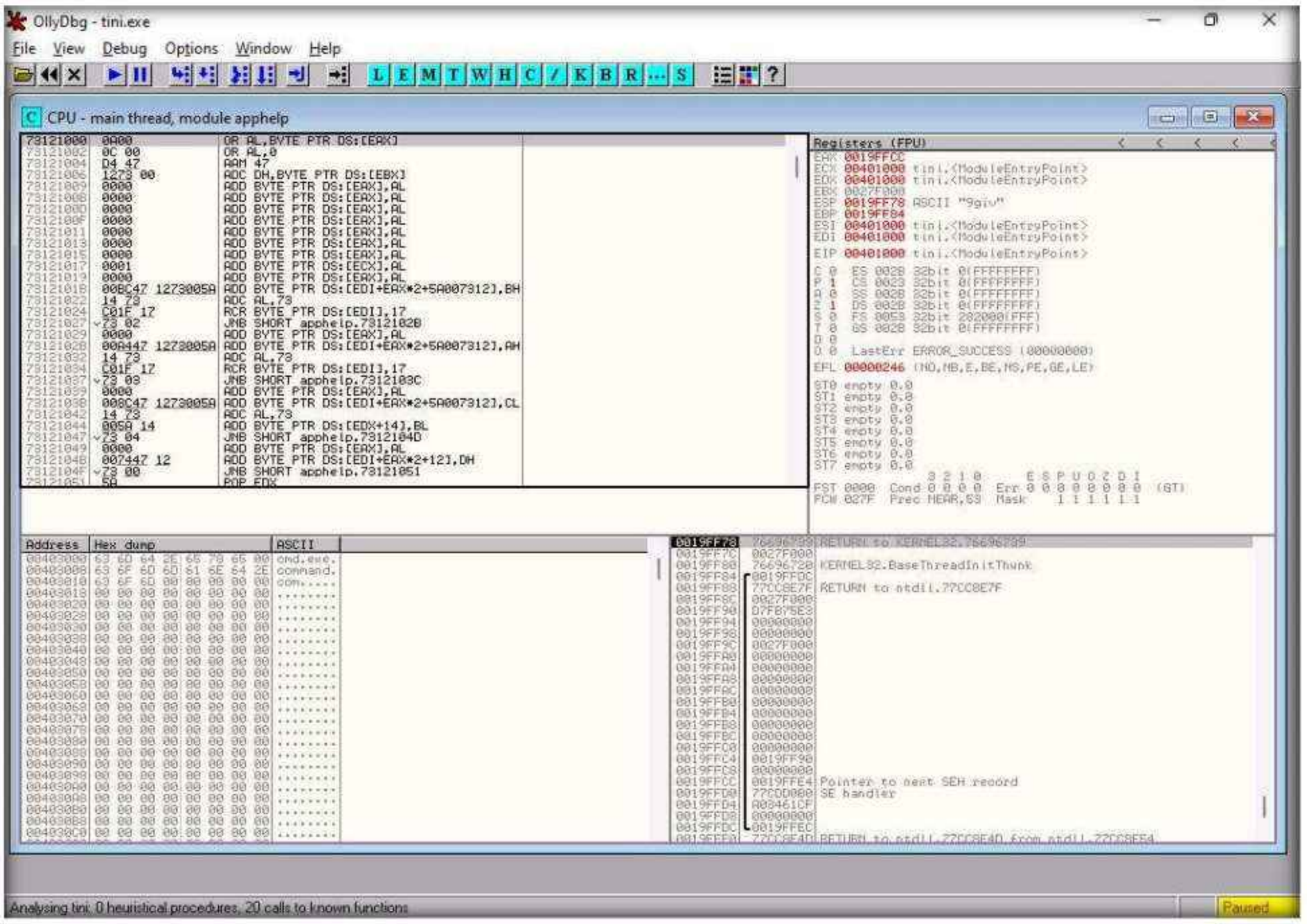
33. A window named **Executable modules** appears in OllyDbg, displaying all executable modules, as shown in the screenshot.

34. Double-click any module to view the complete information of the selected module.

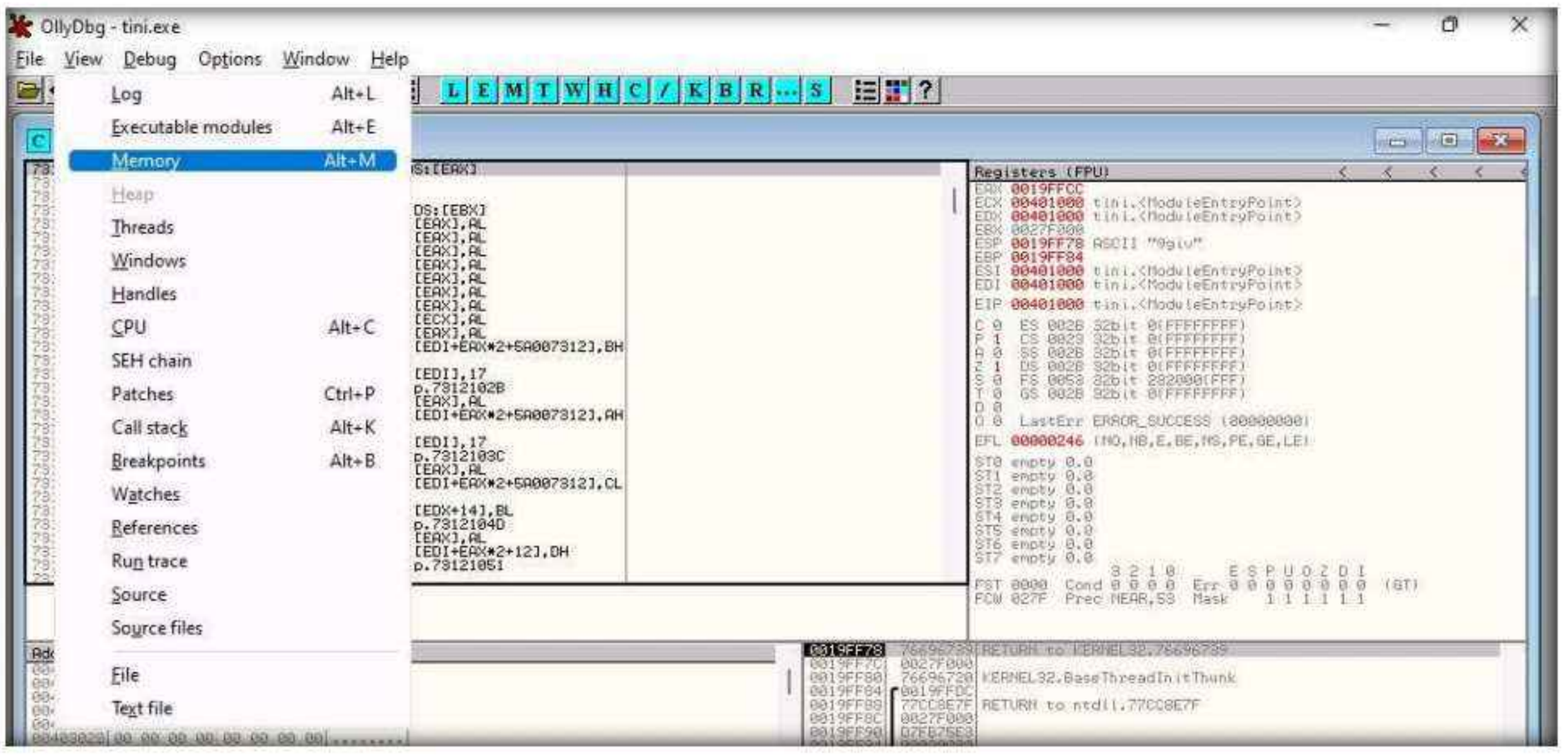
35. In this task, we are choosing the **73120000** module. The results might differ when you perform this task.



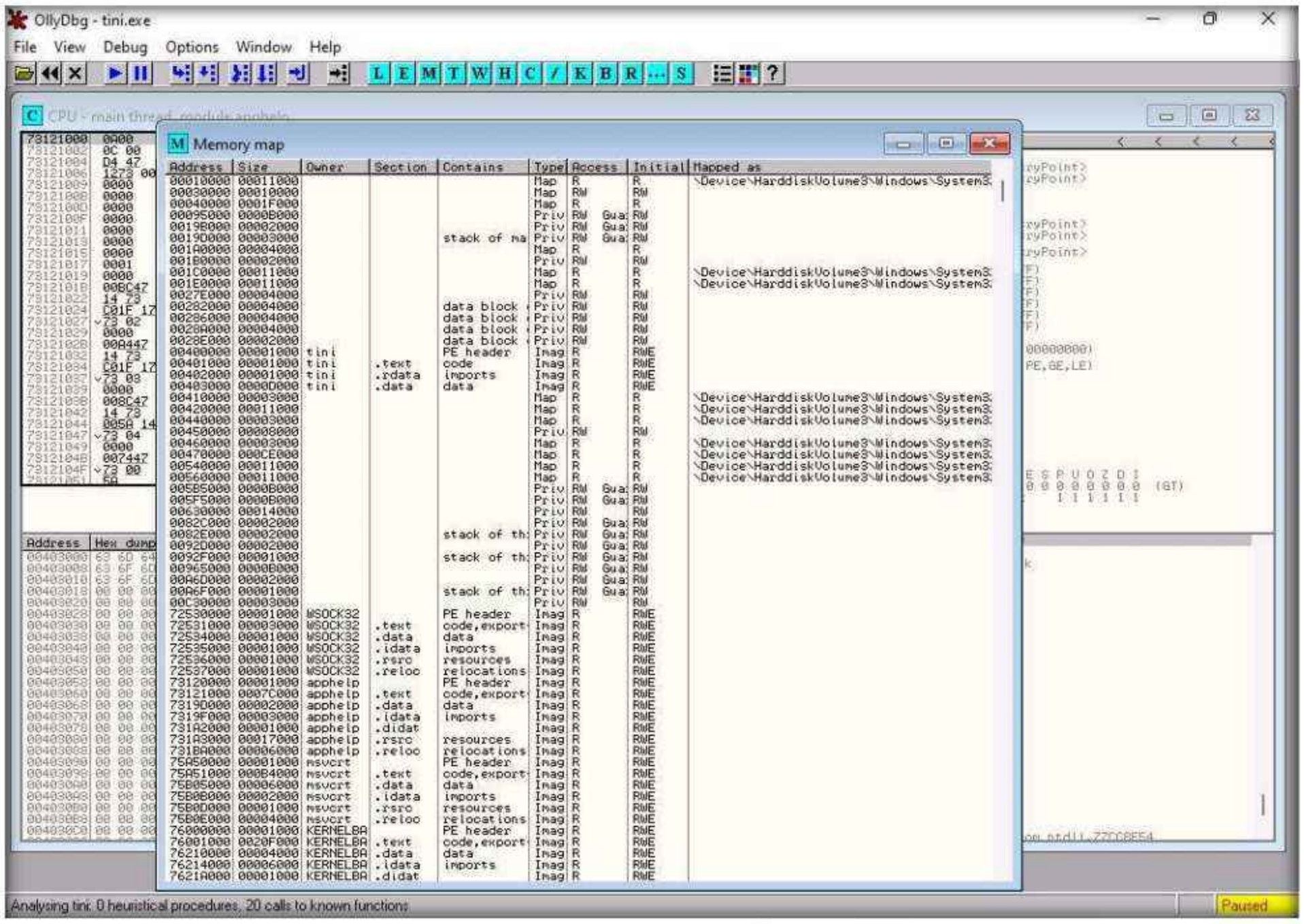
36. This will redirect you to the **CPU - main thread** window, as shown in the screenshot.



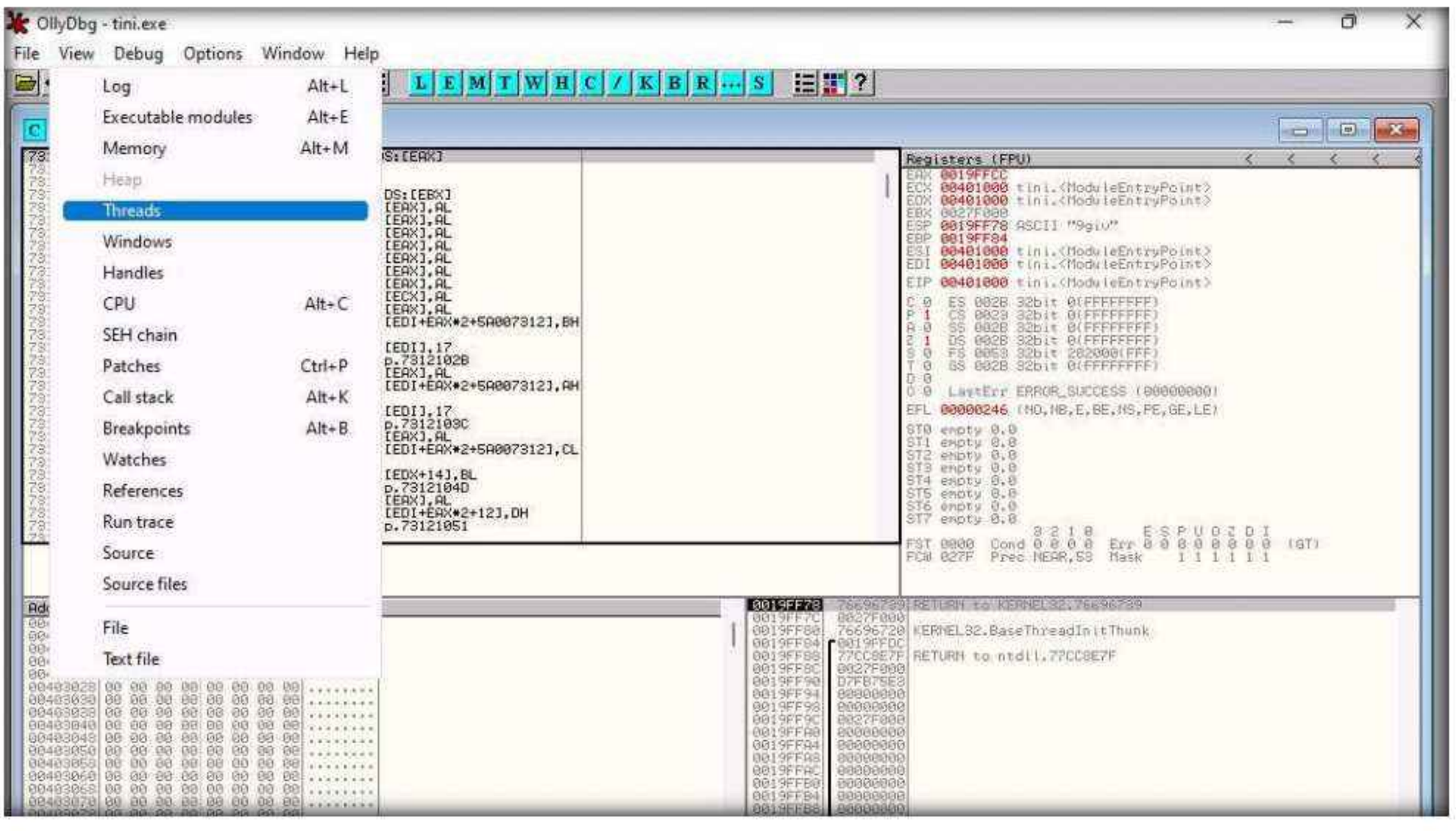
37. Choose **View** in the menu bar, and then choose **Memory**.



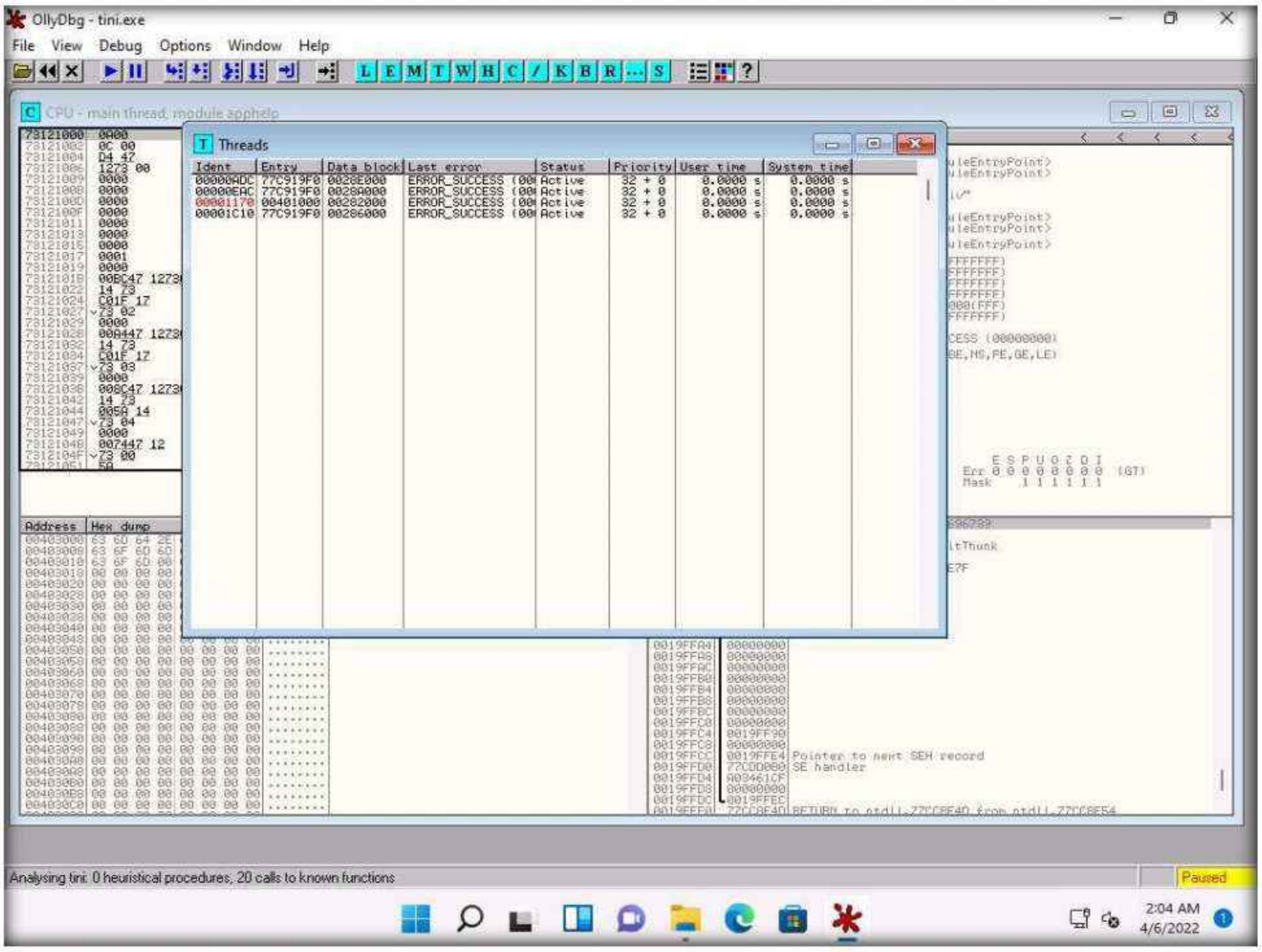
38. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.



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



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



41. This way, you can scan files and analyze the output using OllyDbg.

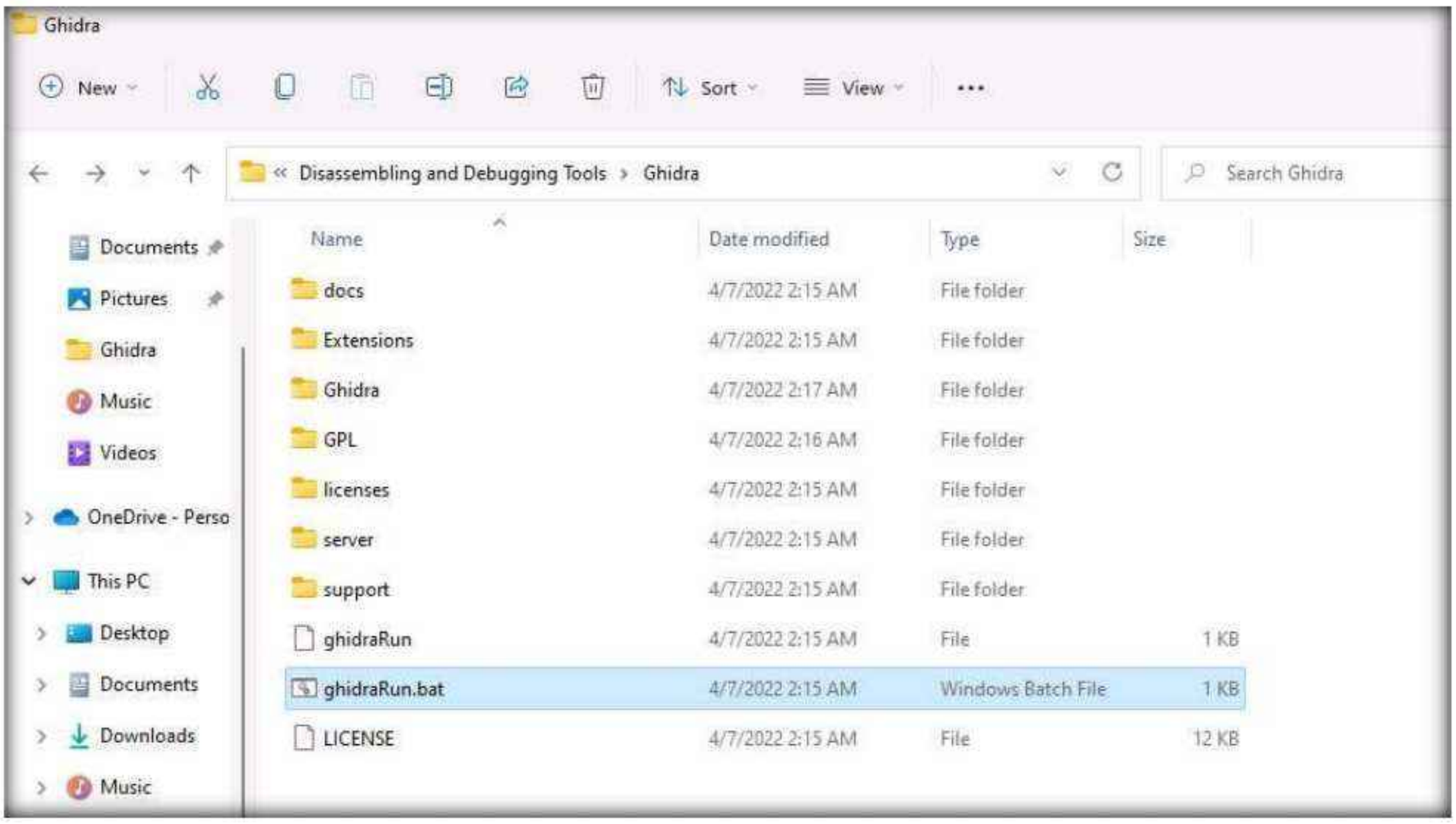
42. Close all open windows.

Task 8: Perform Malware Disassembly using Ghidra

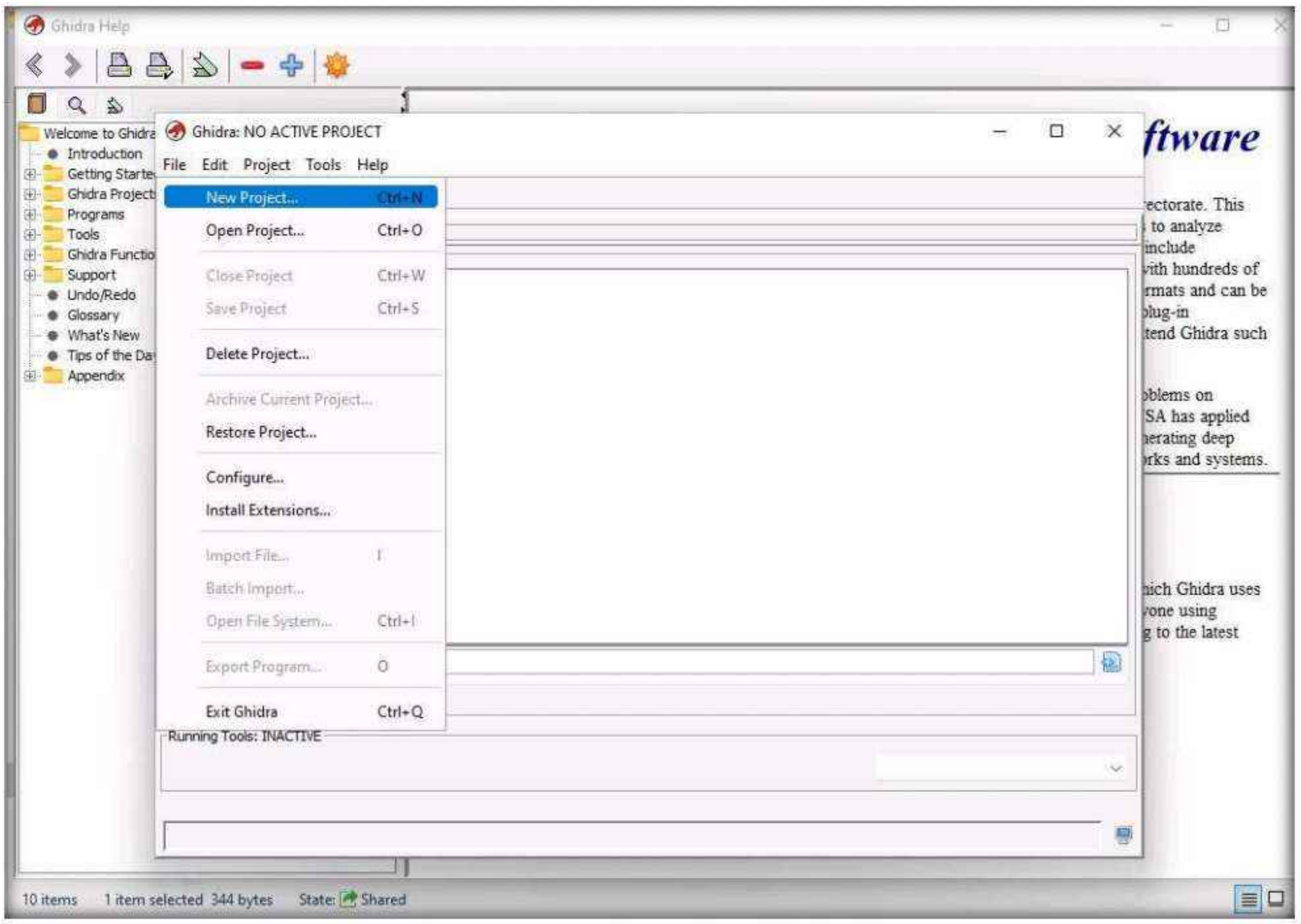
Ghidra is a software reverse engineering (SRE) framework that includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows, MacOS, and Linux. It's capabilities include disassembly, assembly, decompilation, debugging, emulation, graphing, and scripting. Ghidra supports a wide variety of processor instruction sets and executable formats and can be run in both user-interactive and automated modes. Analysts can also develop their own Ghidra plug-in components and/or scripts using the exposed API. In addition, there are numerous ways to extend Ghidra such as new processors, loaders/exporters, automated analyzers, and new visualizations.

Here, we will use Ghidra to perform malware disassembly.

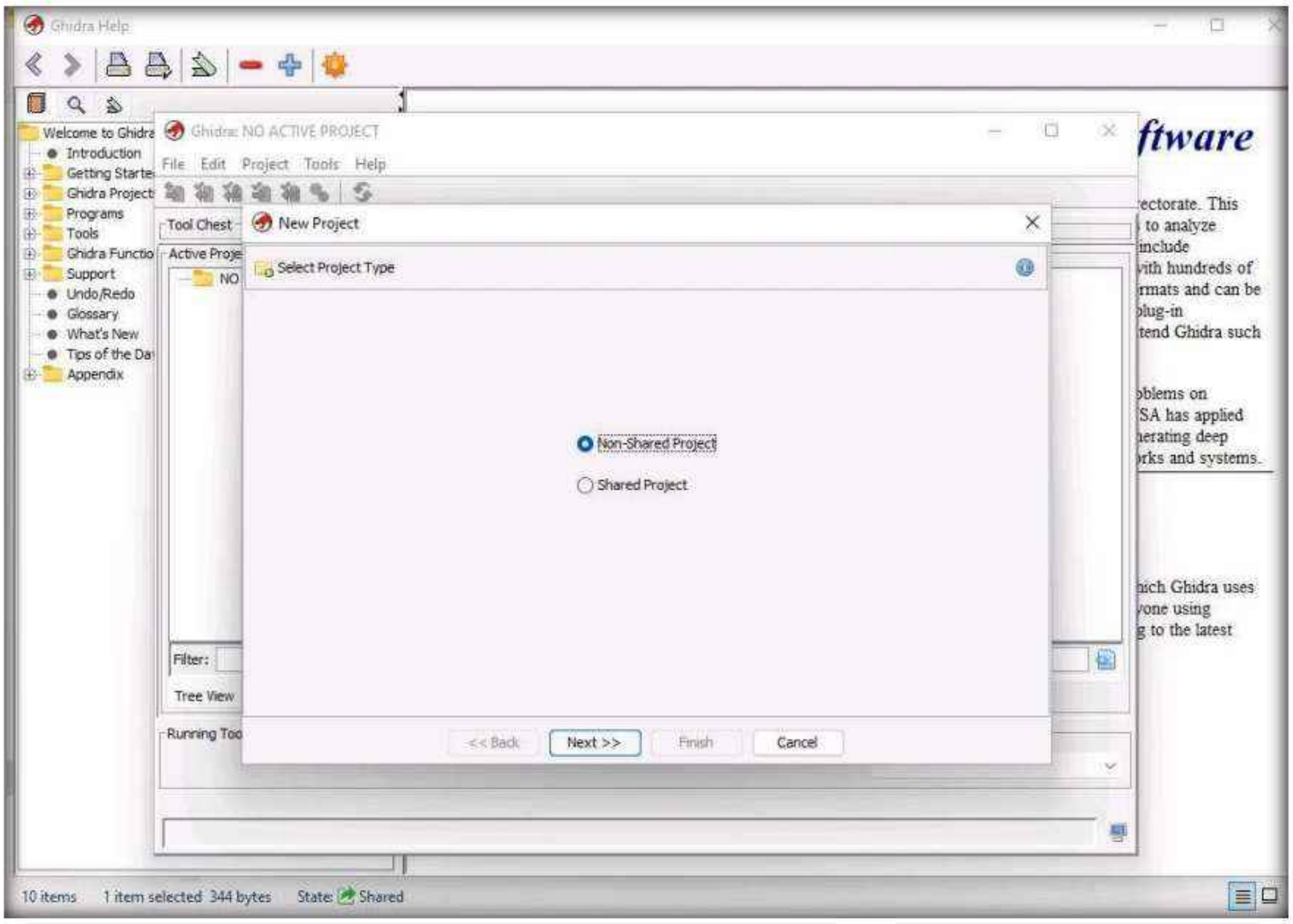
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\Ghidra** and double-click **ghidraRun.bat**.



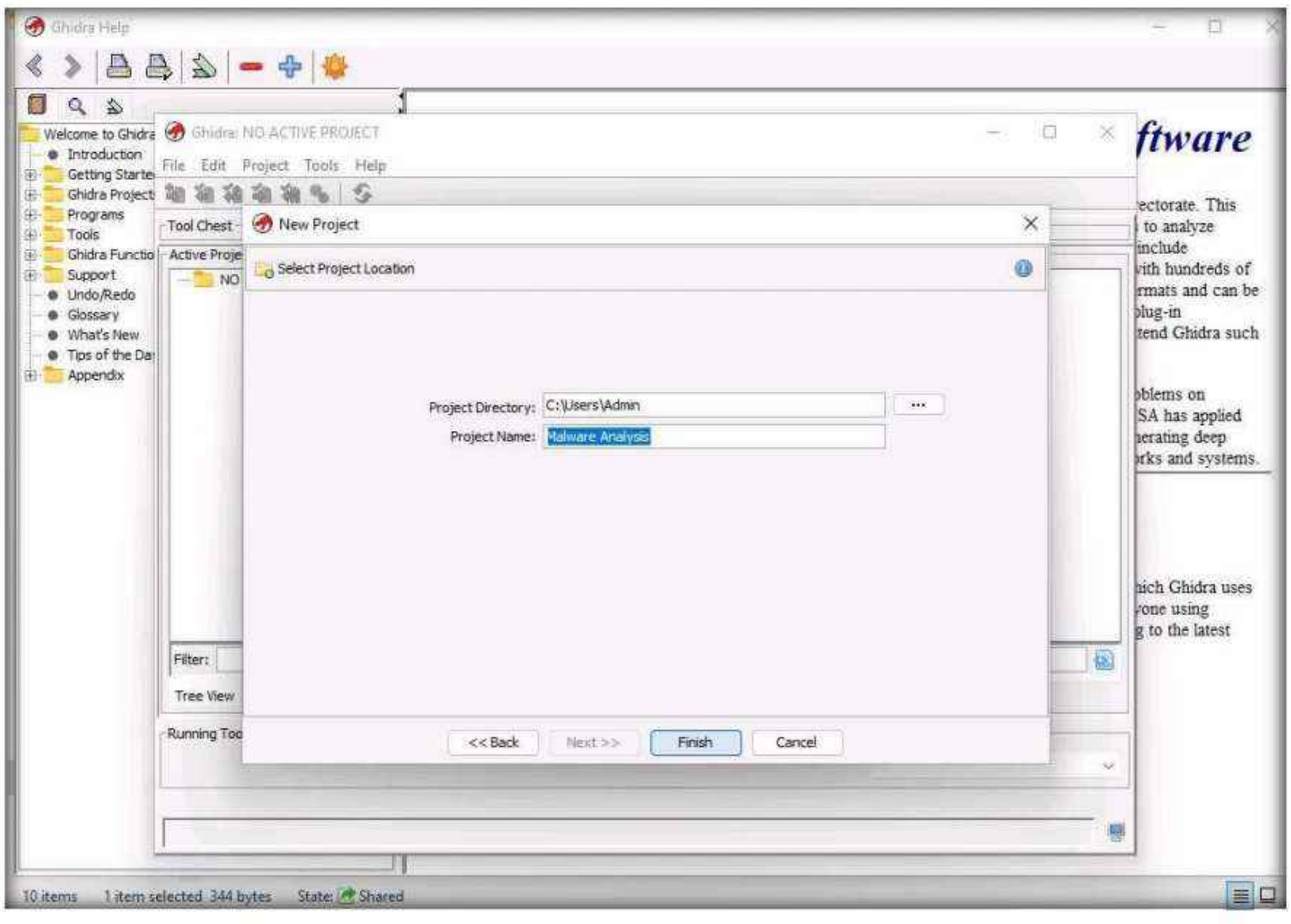
2. After Ghidra initializes, a **Tip of the Day** pop-up appears, click **Close** to close it.
3. **Ghidra: NO ACTIVE PROJECT** window appears, click **File** and select **New Project....**



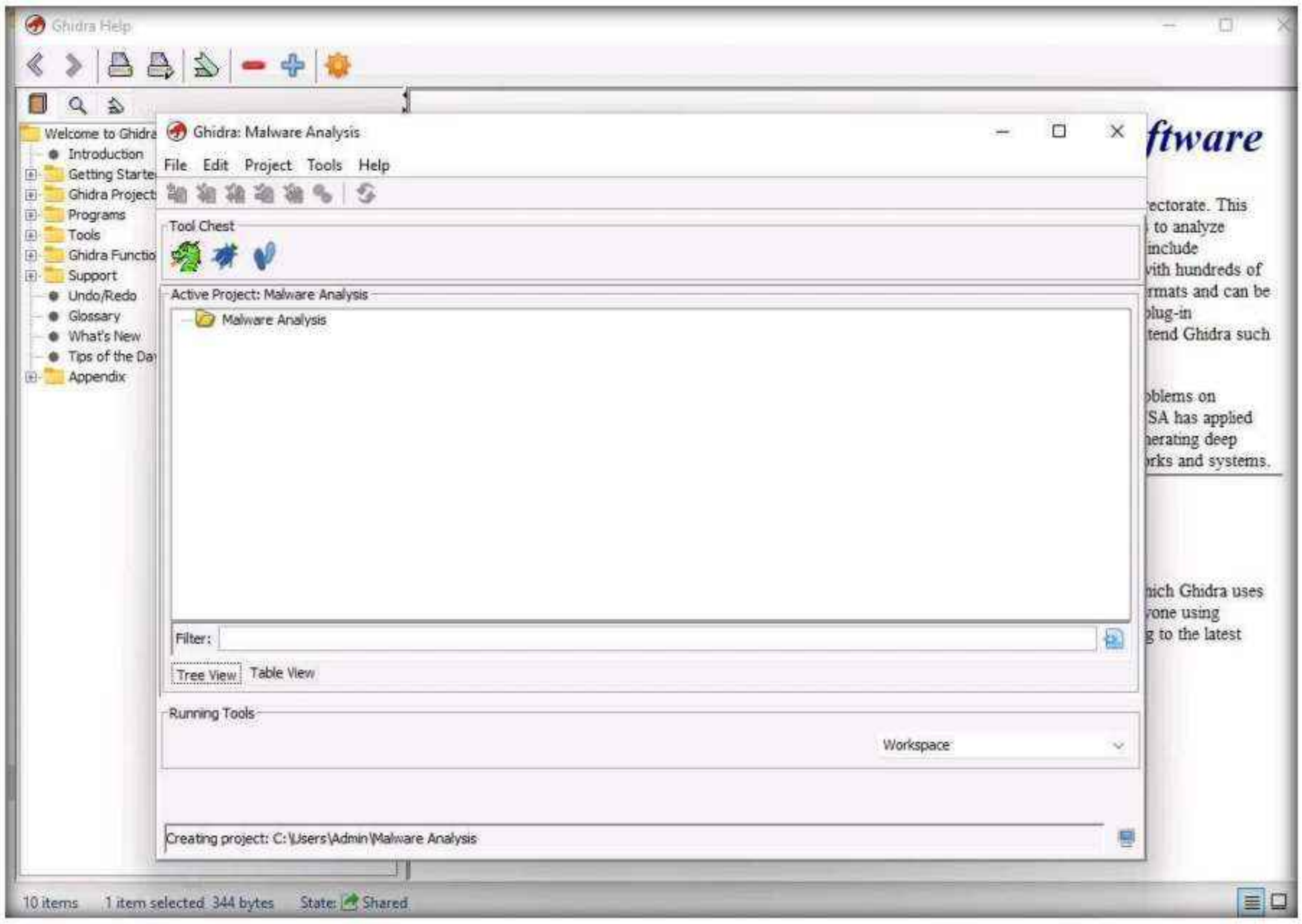
4. **New Project** window appears, leave the default selected option to **Non-Shared Project** and click **Next**.



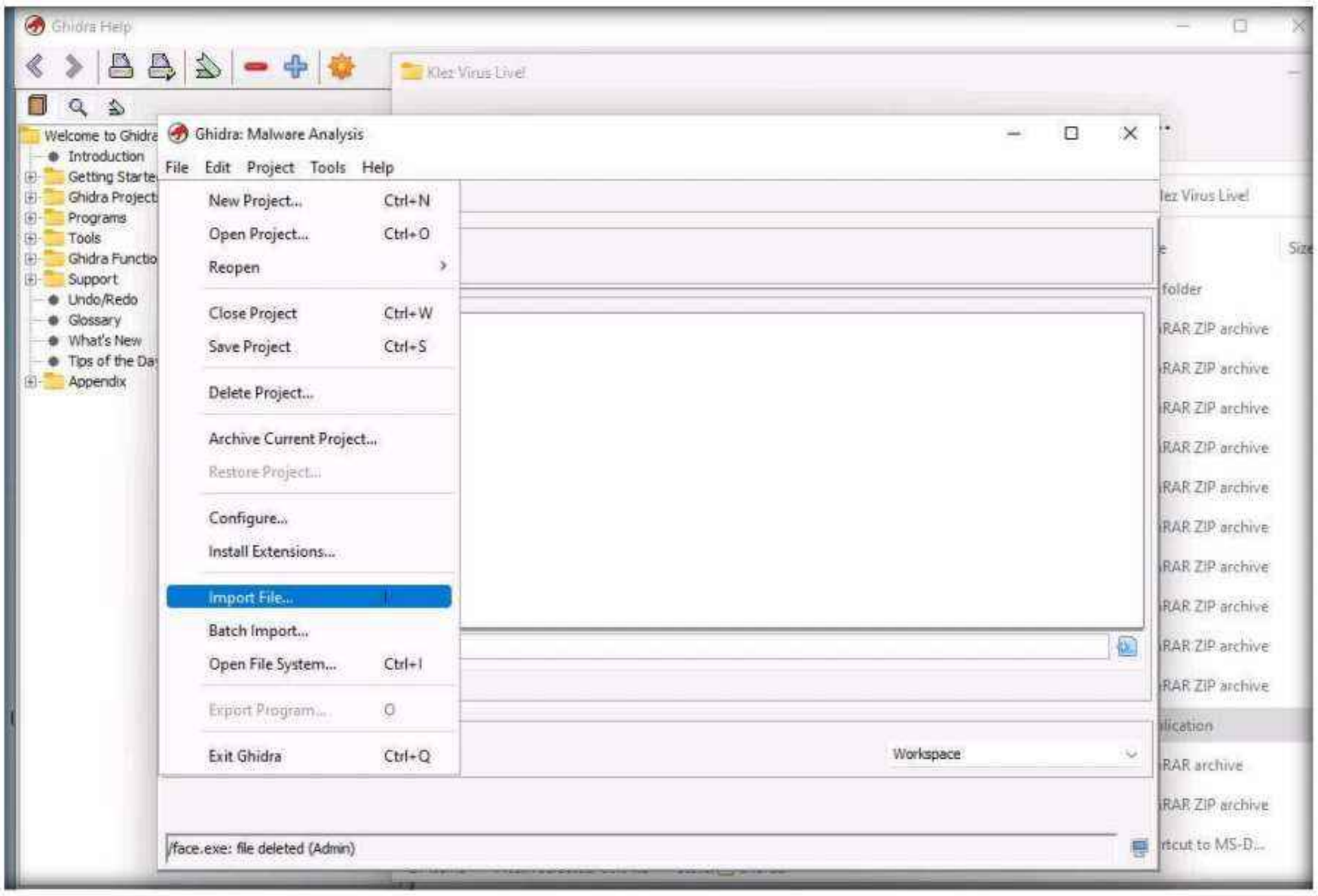
5. In the next window, enter the **Project Name** as **Malware Analysis** and click **Finish**.



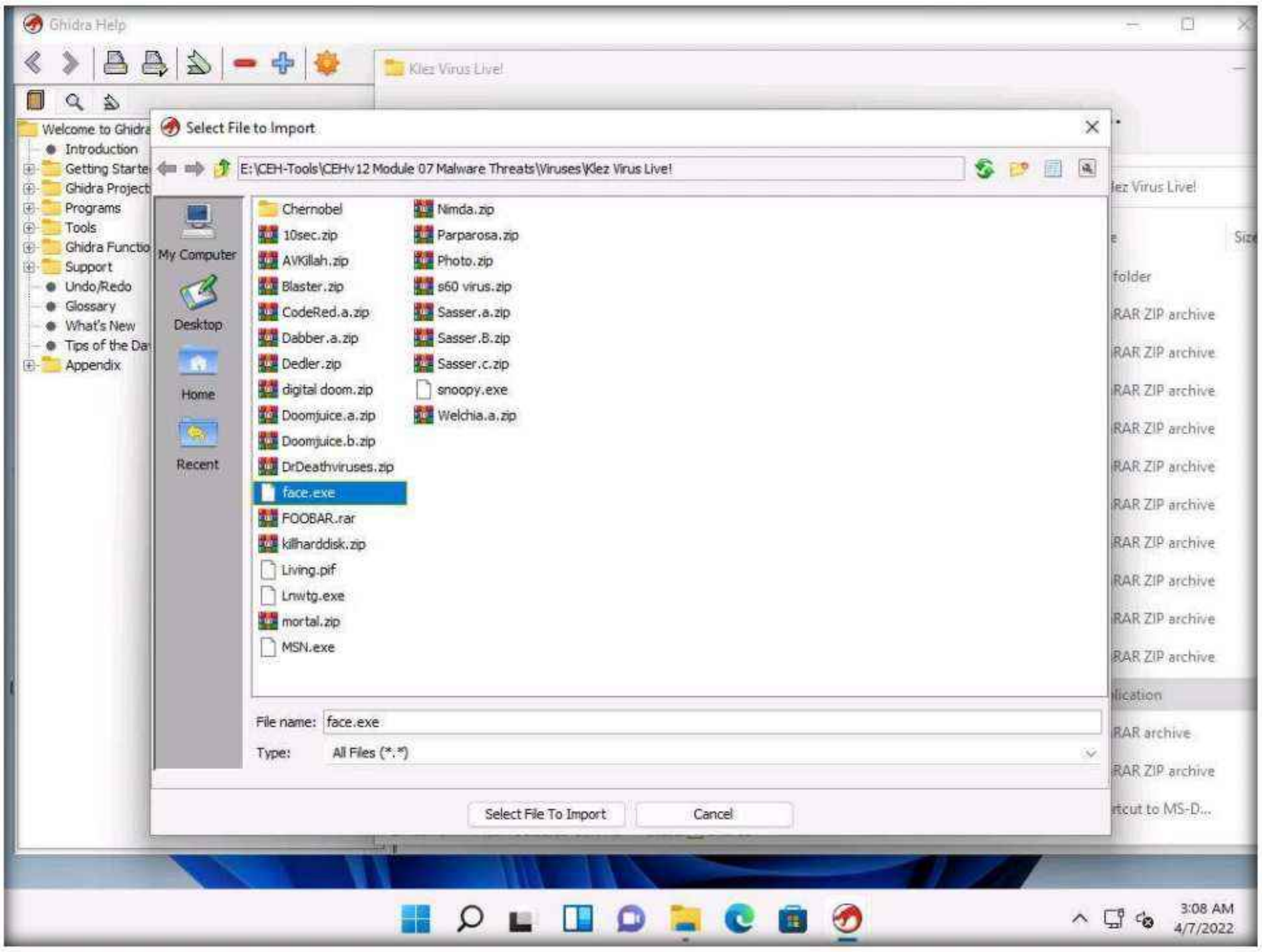
6. A new project with the name as **Malware Analysis** has been created, as shown in the screenshot.



7. Now, navigate to **File → Import File...**.

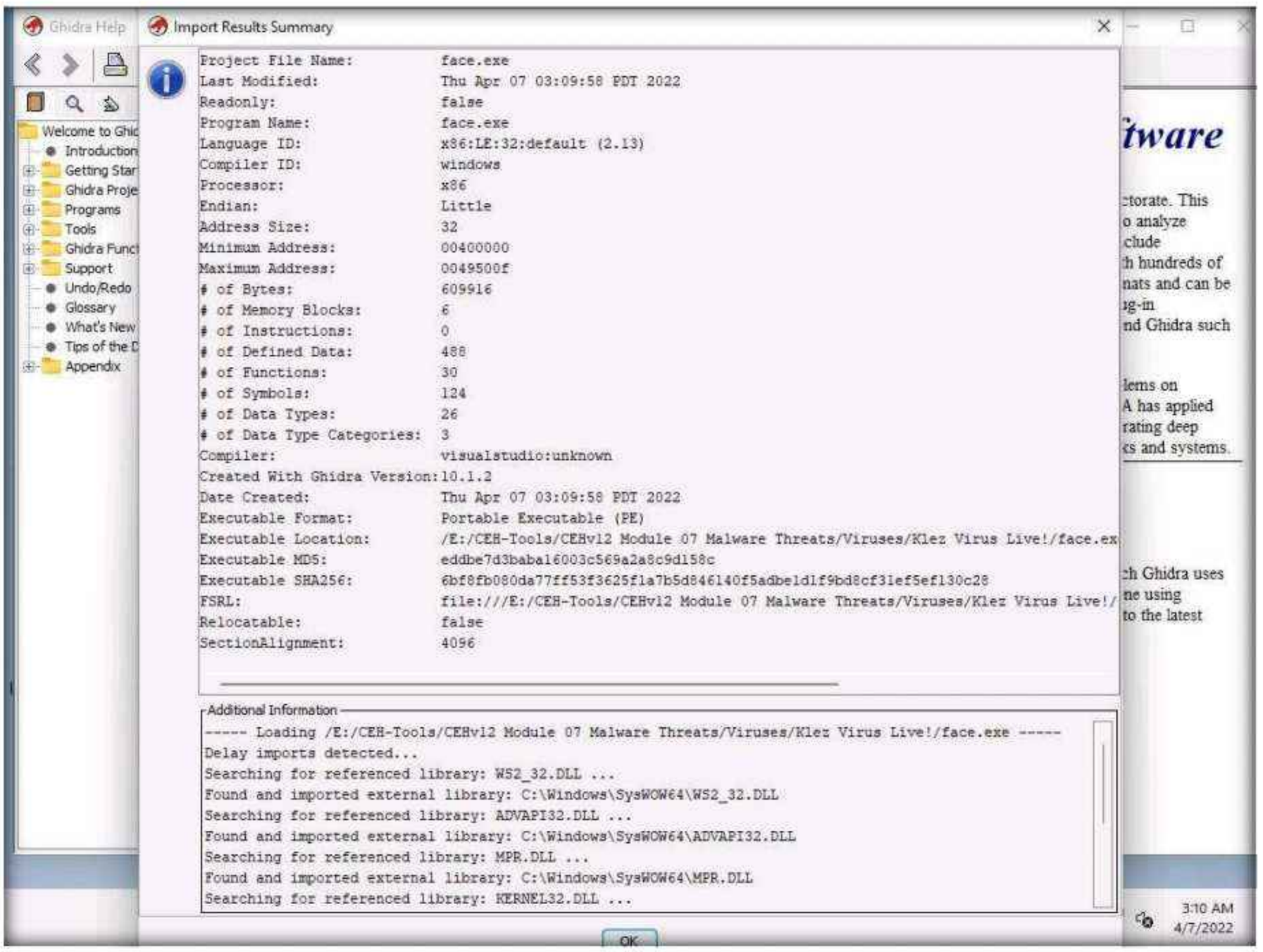


8. **Select File to Import** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Select File to Import**.

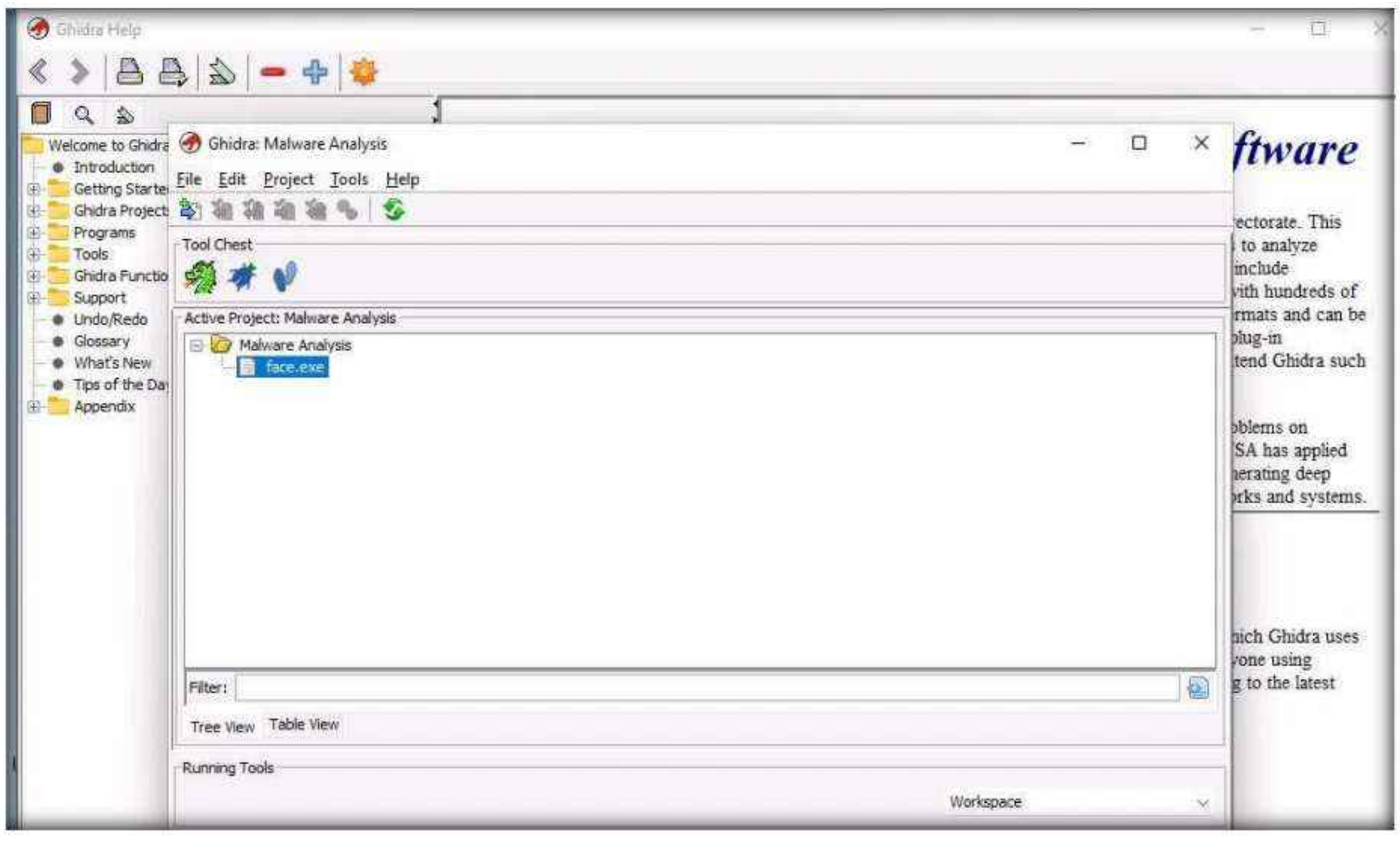


9. **Import** window appears, click **OK**.

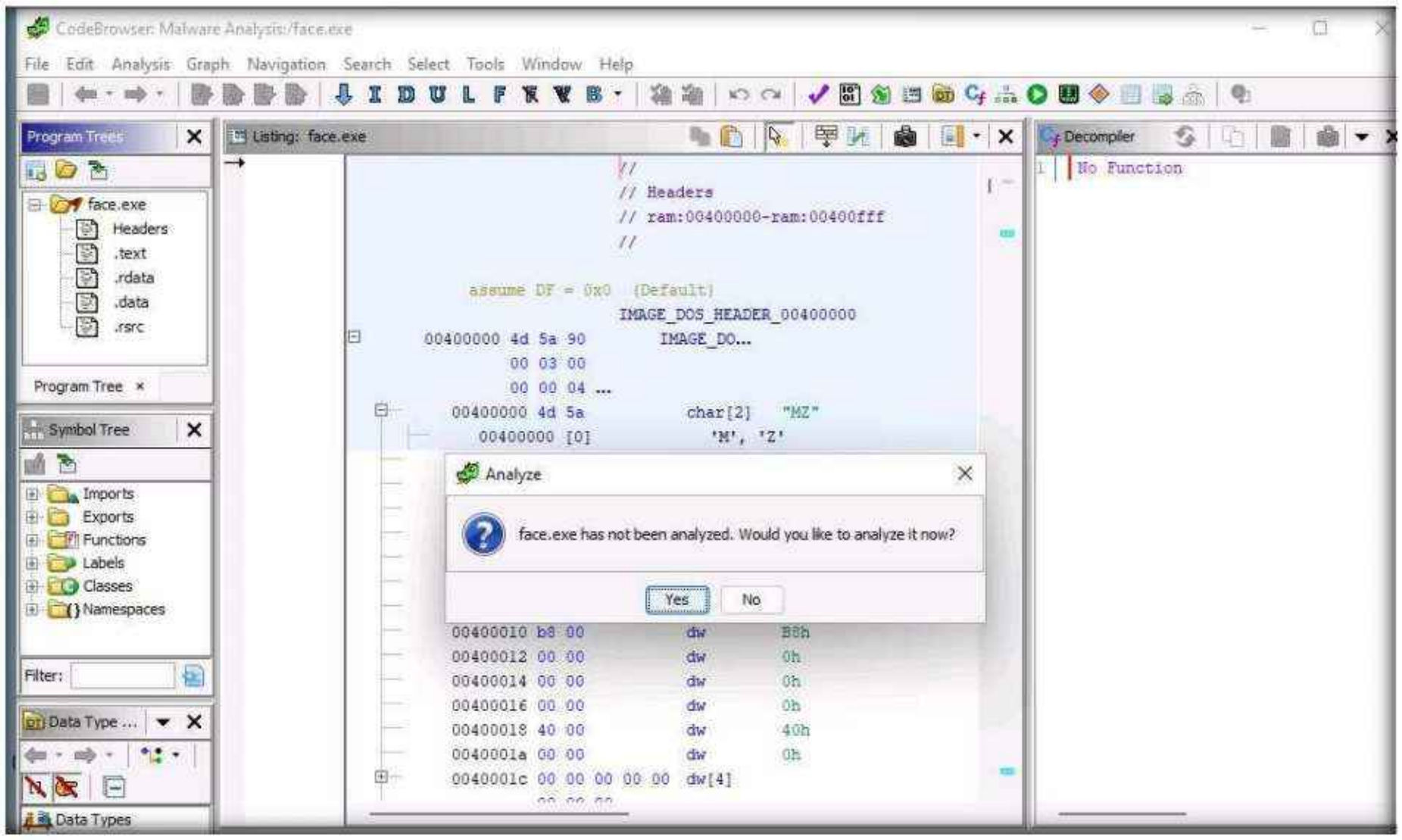
10. After the completion of file import, **Import Results Summary** window appears, click **OK**.



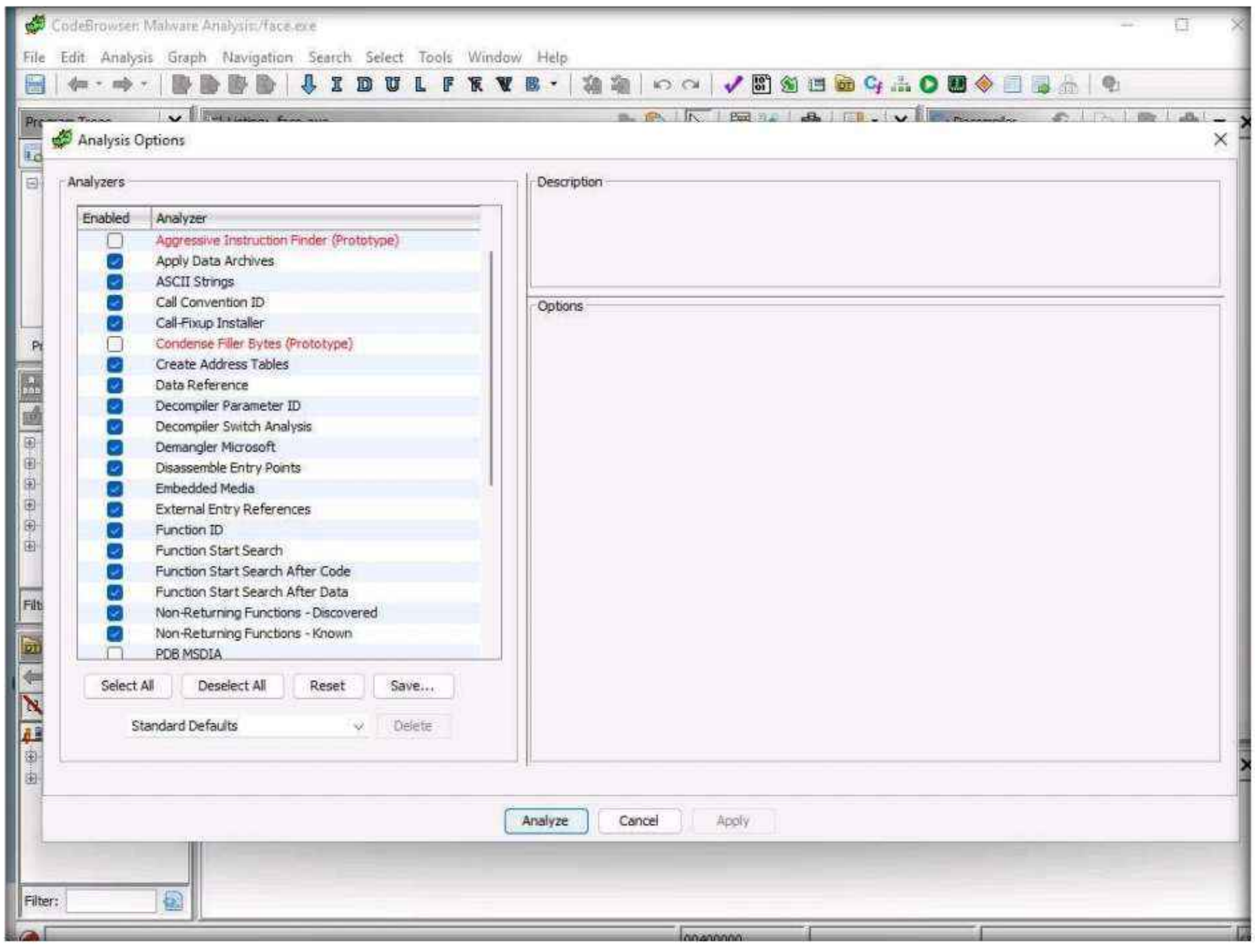
11. You can observe that **Face.exe** is added as a children node under the **Malware Analysis** project. Double-click **Face.exe** node.



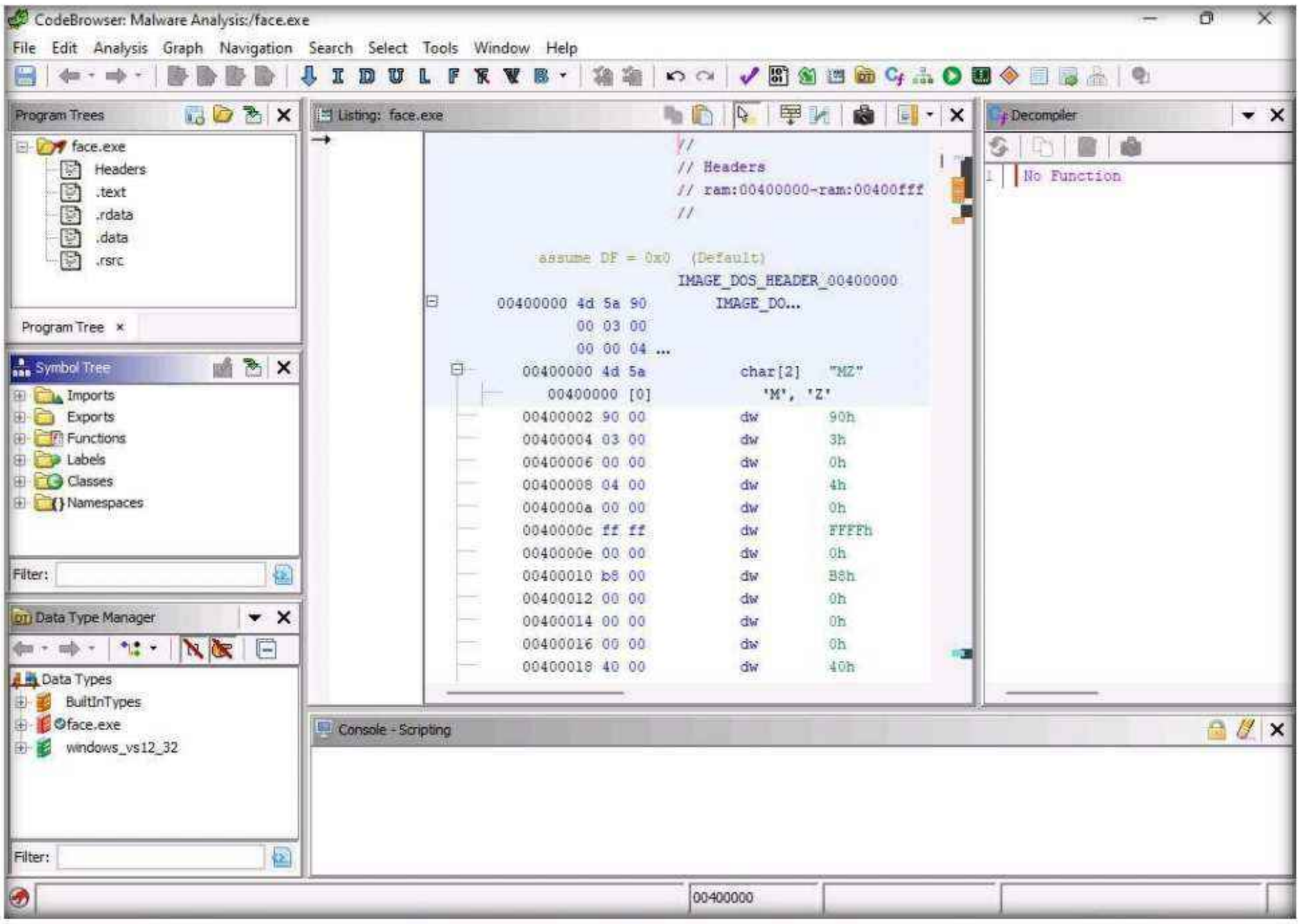
12. **Analyze** pop-up appears, click **Yes**.



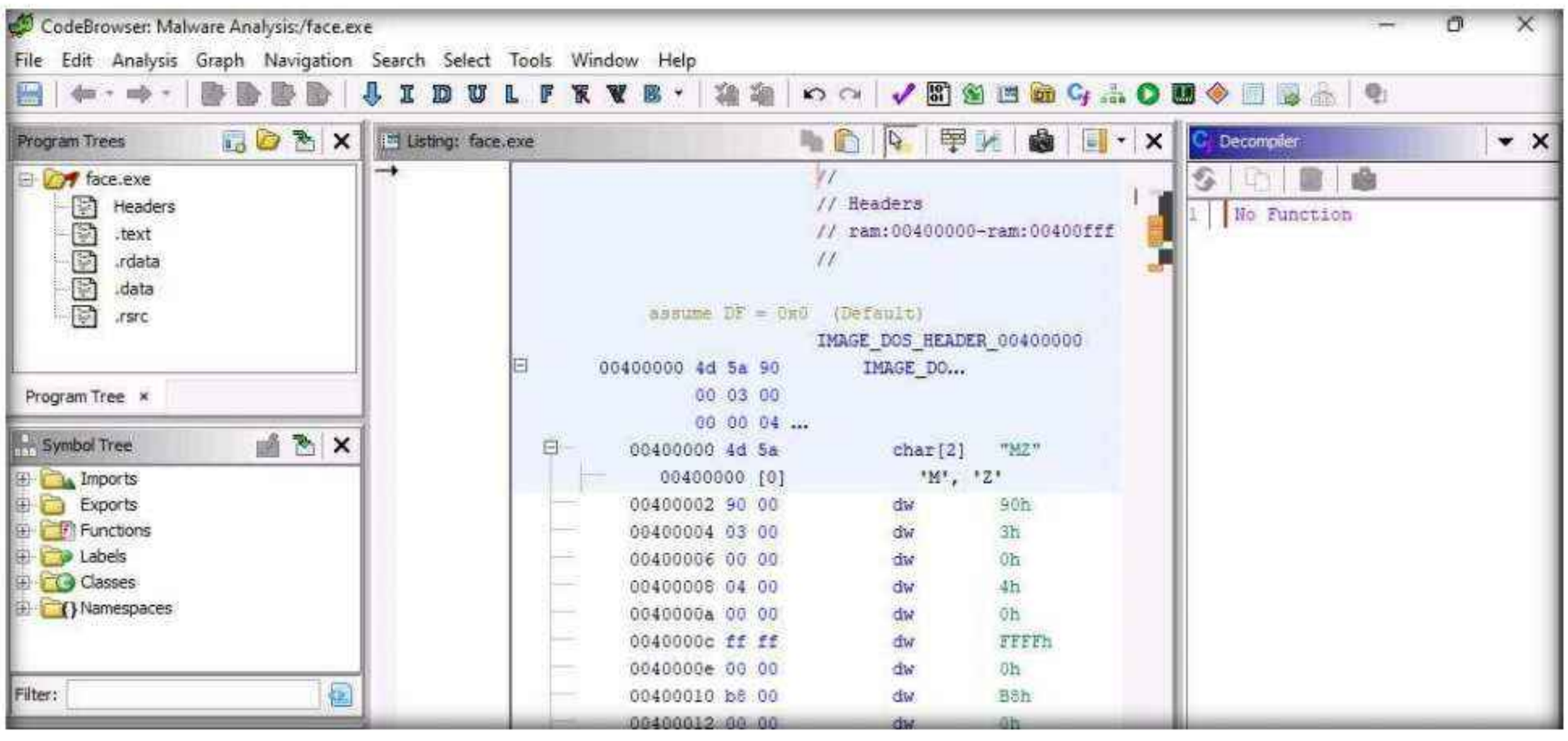
13. **Analyze Options** window appears, leave the default options and click **Analyze**.



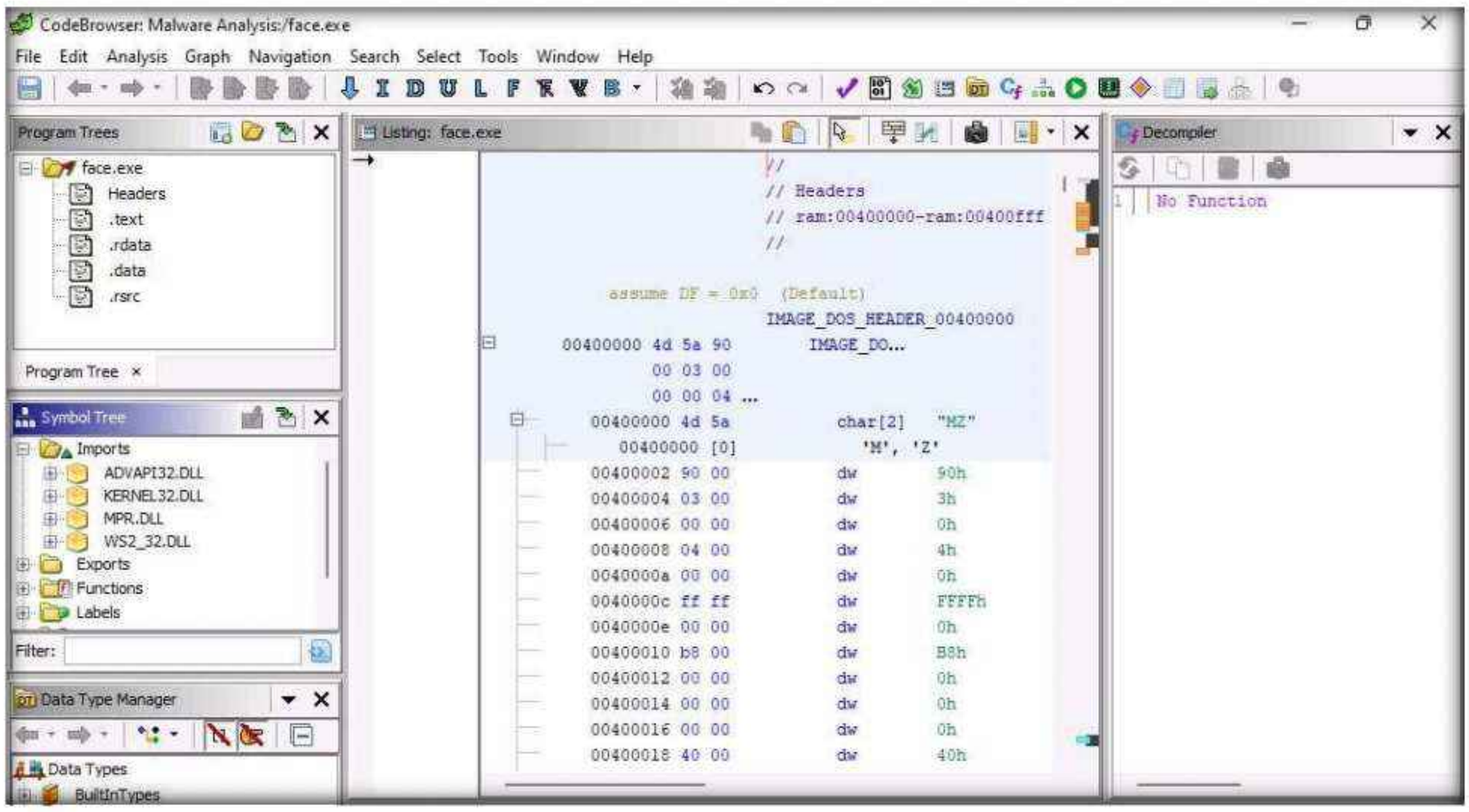
14. This initiates the analysis process, you can monitor the status bar present at the lower right section of the window. Wait for it to complete.
15. After the analysis, assembly code of face.exe file appears along with the decompiler, as shown in the screenshot.



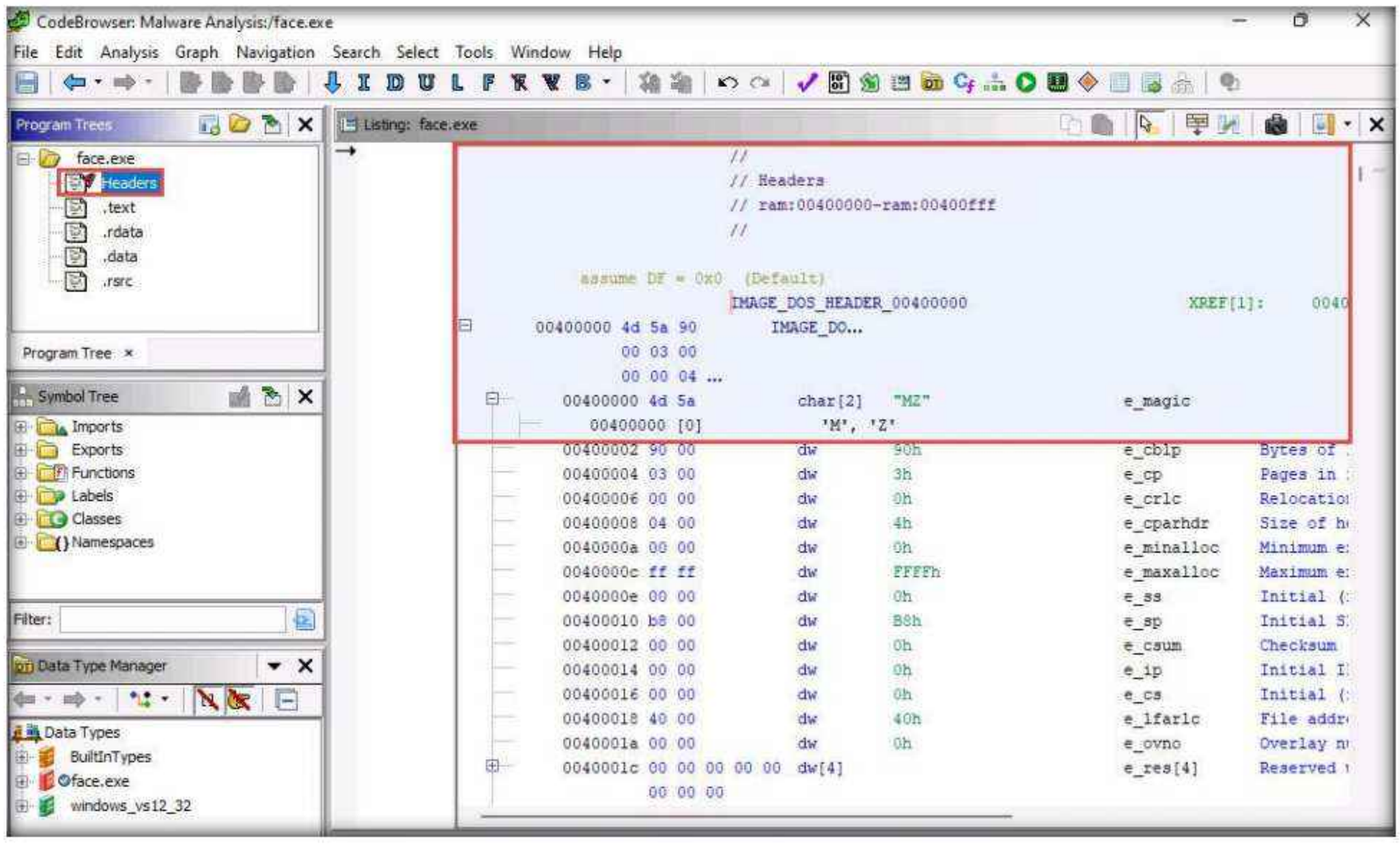
16. In the left pane, under **Symbol Tree**, you can observe various components of face.exe file such as Imports, Exports, Functions and Labels.



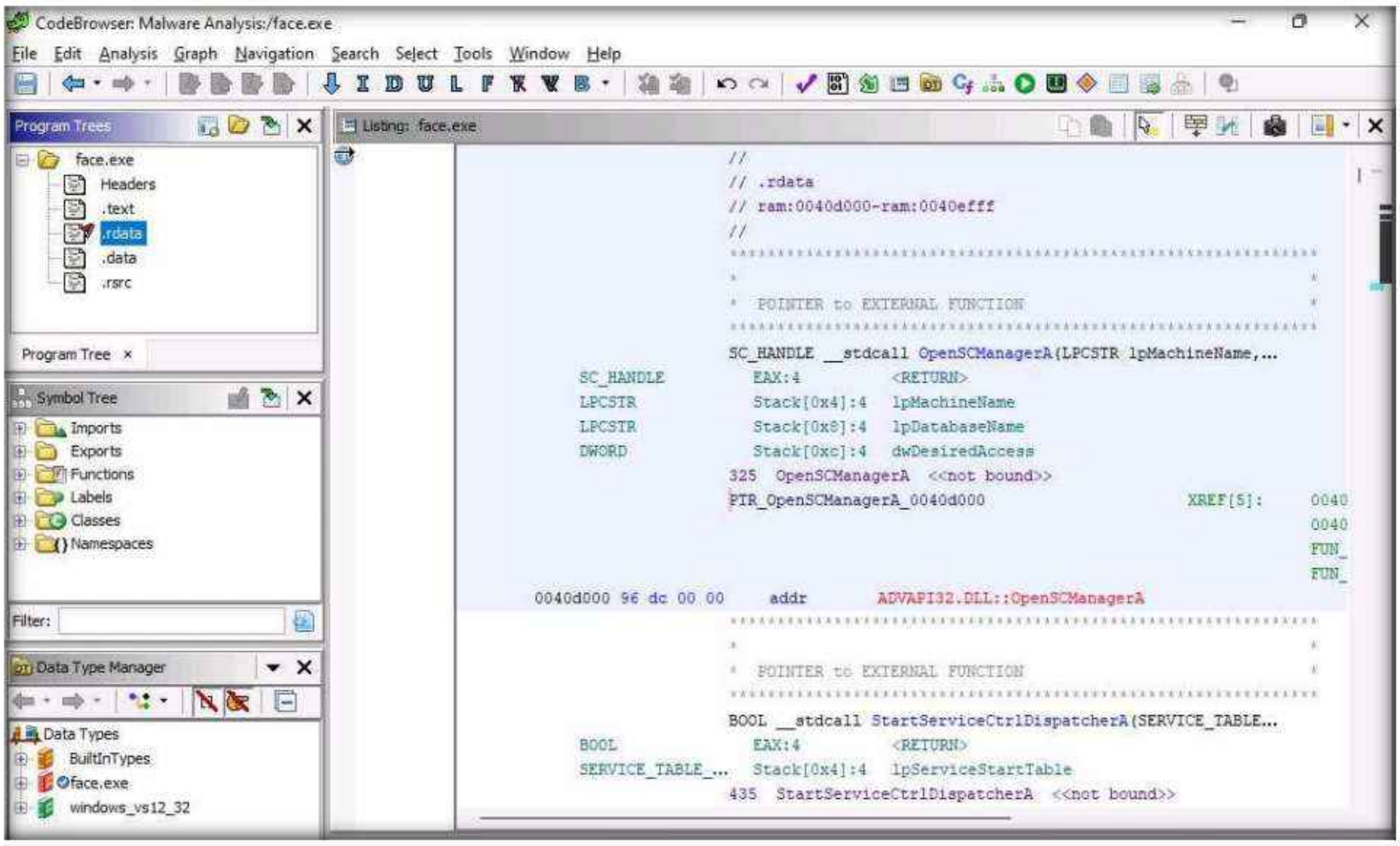
17. Click to expand **Imports** node and you can view the DLL files of face.exe.



18. Similarly, you can view other components under Symbol Tree to obtain additional information on face.exe.
19. Close the **Decompiler** tab.
20. Now, in the left-pane, under **Program Tree**, double-click **Headers** node to jump to the header function in the code snippet.



21. Similarly, double-click **.rdata** node to view the rdata function in the code snippet.



22. You can further explore various other functionalities in the Ghidra tool to analyze the face.exe file.
23. This concludes the demonstration of malware disassembly using Ghidra.
24. Close all the open windows.
25. You can also use other disassembling and debugging tools such as **Radare2** (https://rada.re), **WinDbg** (http://www.windbg.org), and **ProcDump** (https://docs.microsoft.com) to perform malware disassembly.
26. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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.

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 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, 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 Reg Organizer
- 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 Reviver
- Perform DNS monitoring using DNSQuerySniffer

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 80 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

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.

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.

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.

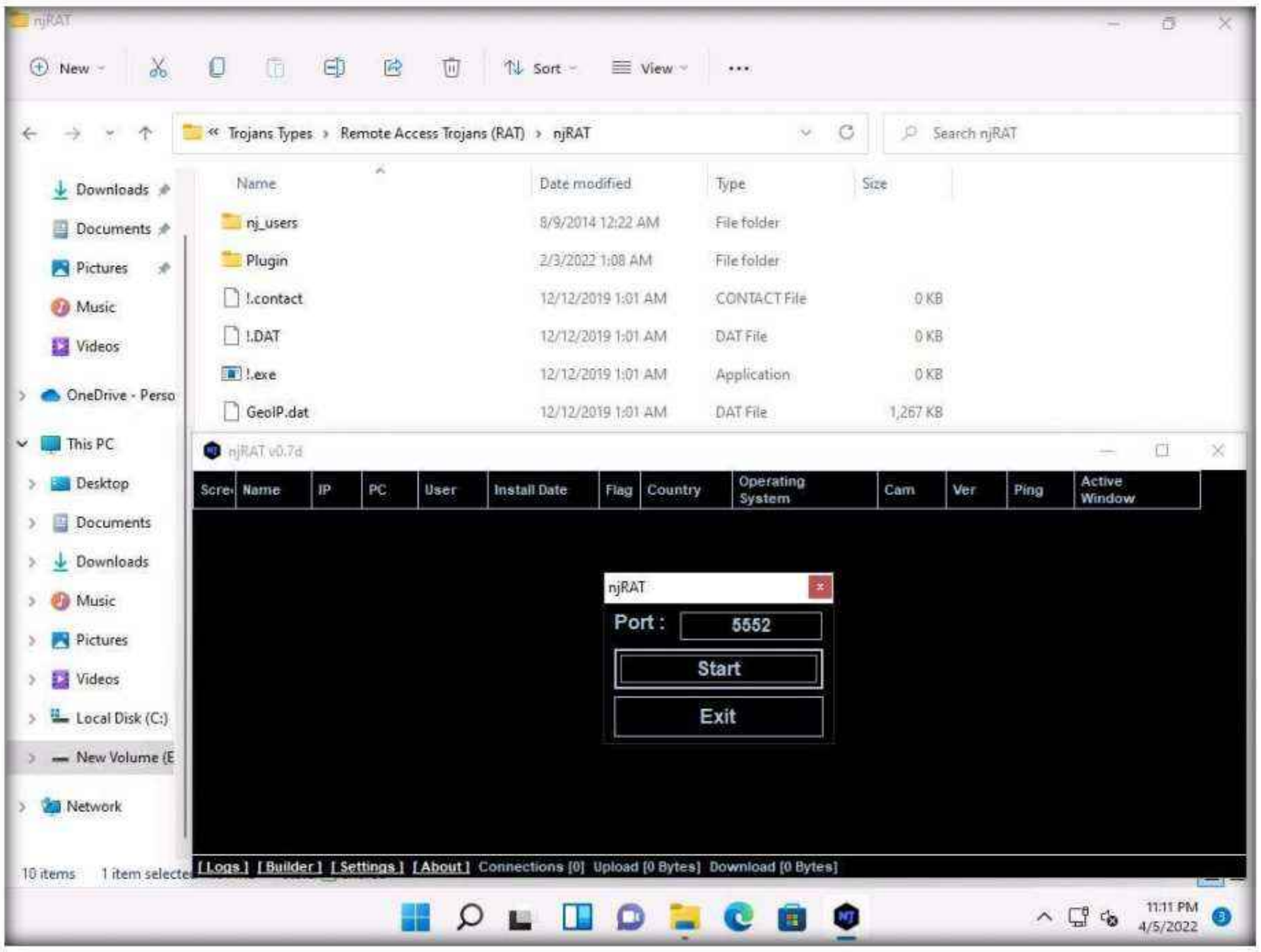
In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

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

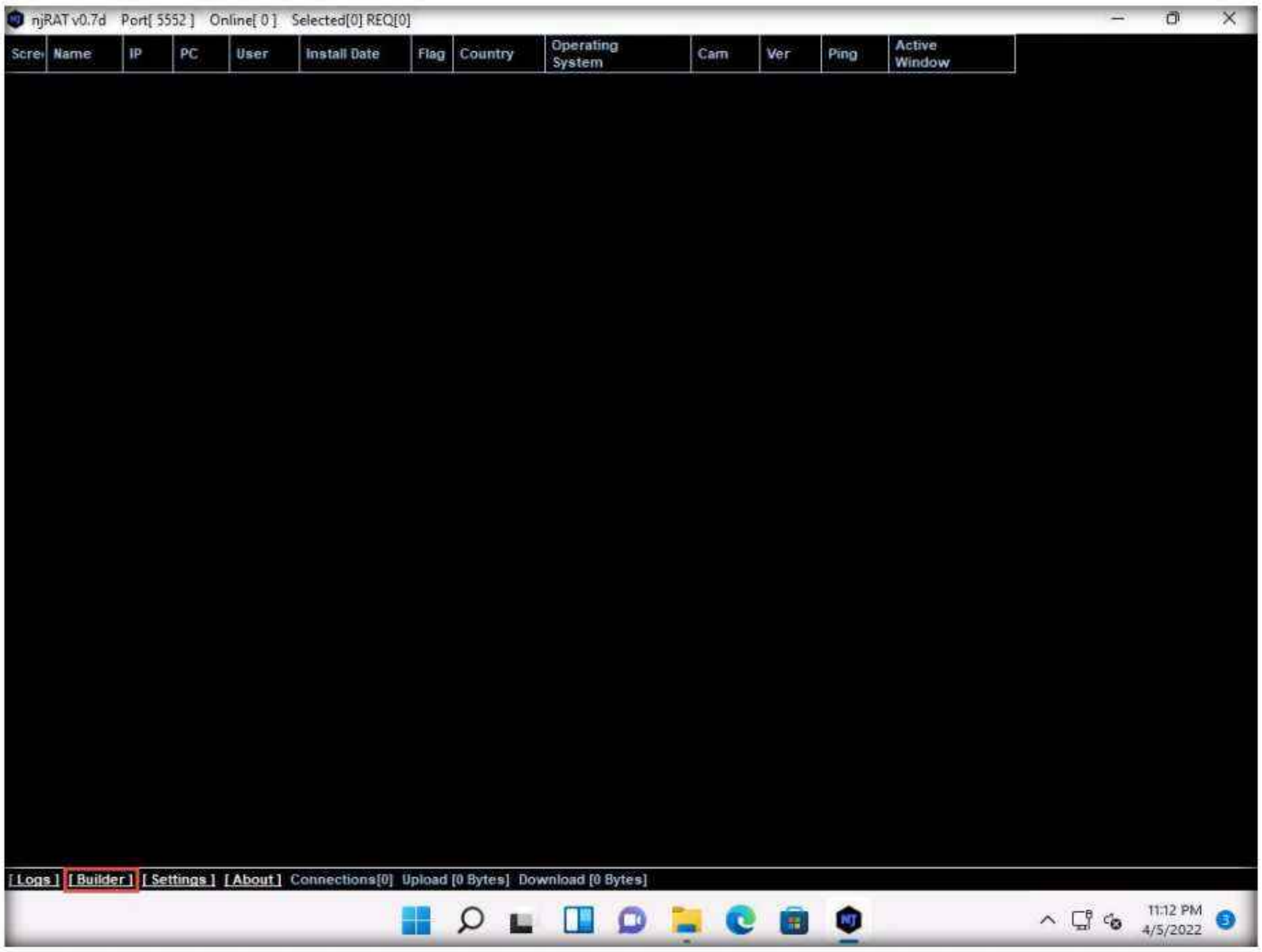
Note: This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine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

1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe** to launch **njRAT**. Click **Start**.



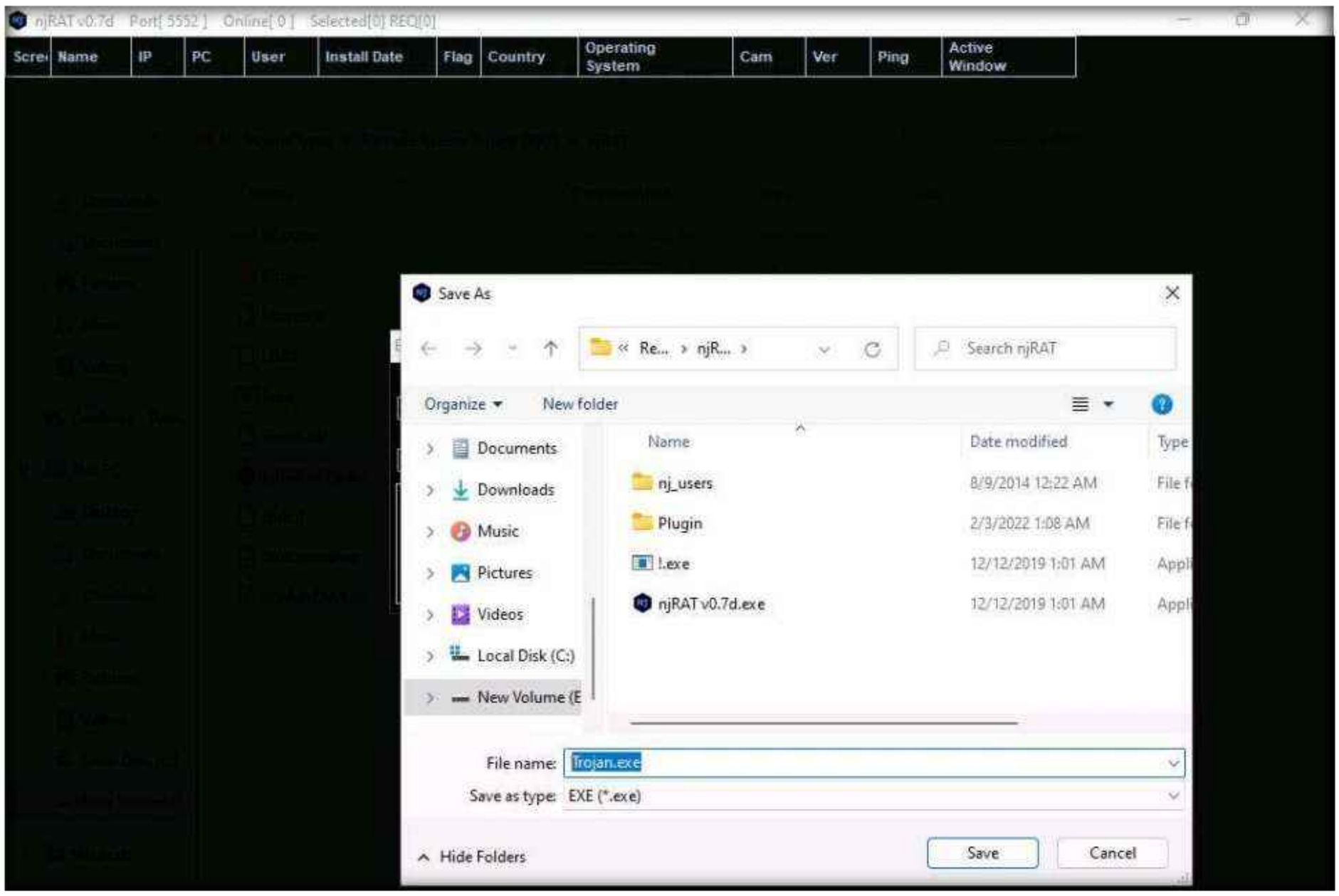
4. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.



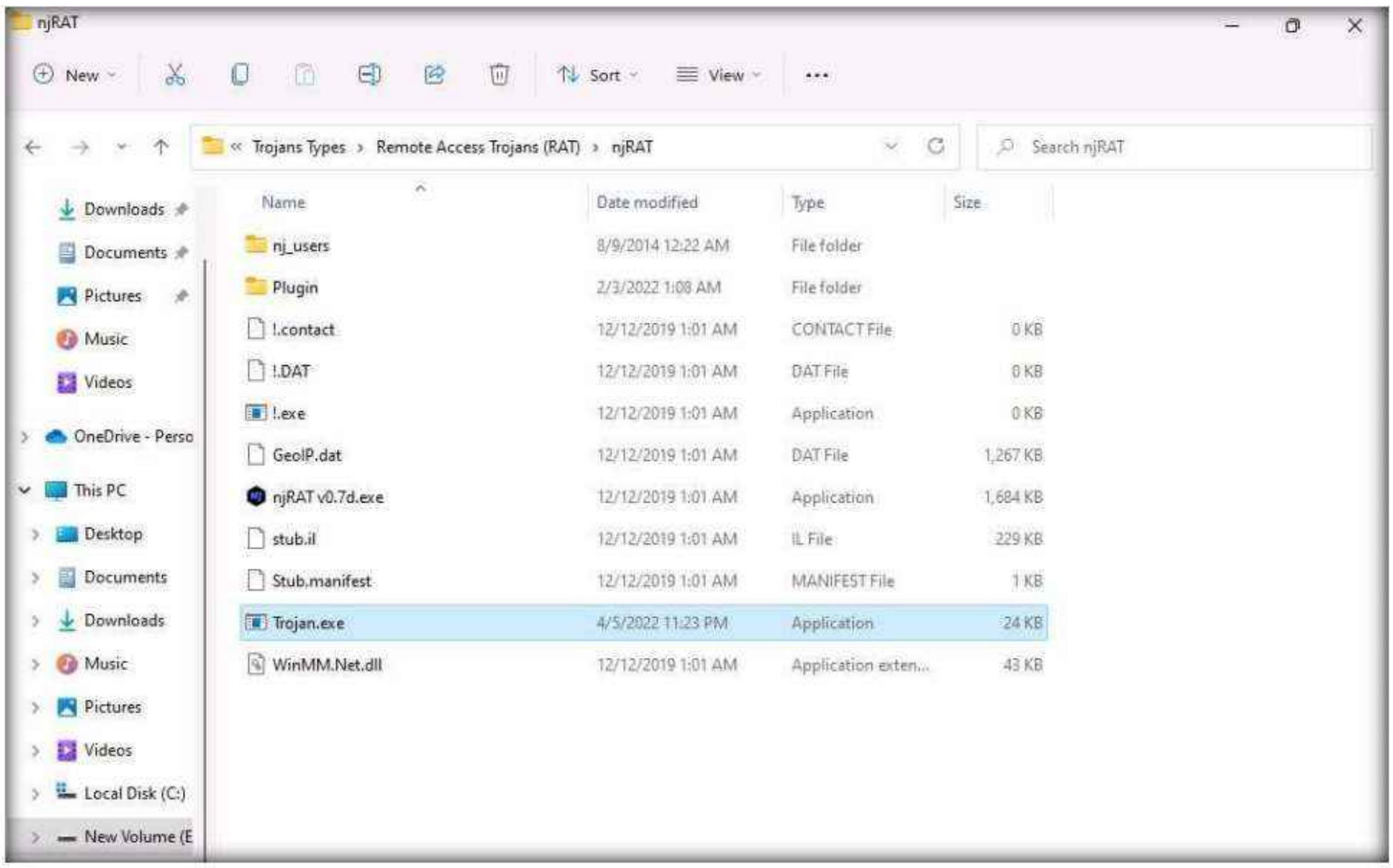
5. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registy StarUp**, rename **ExeName** as **Trojan.exe**. Leave the other settings to default, and click **Build**.

   Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.

6. **Save As** window appears, **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**. In the **File name**, enter **Trojan.exe** and click **Save**. **Done!** pop-up appears, click **OK**.

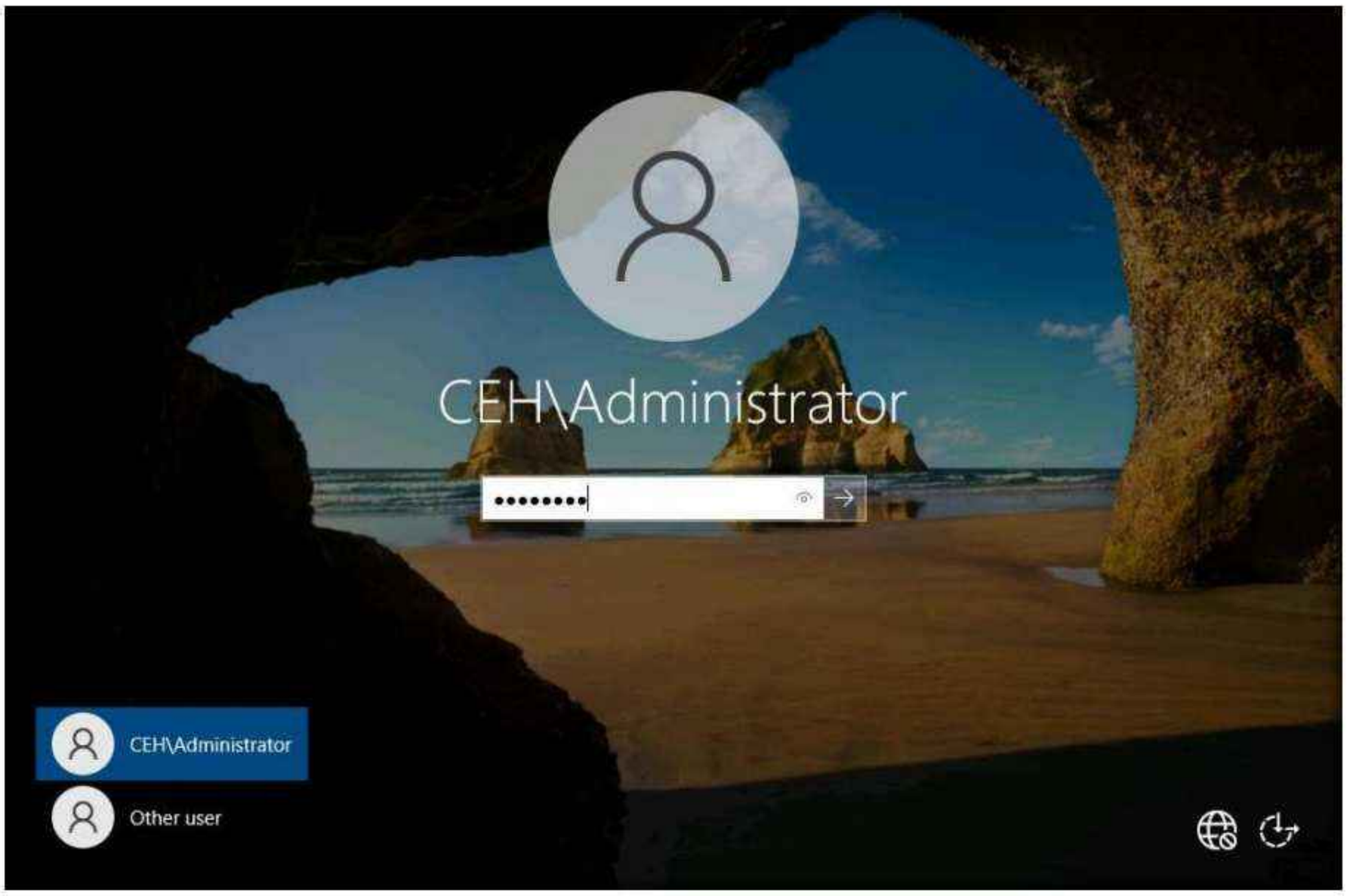


7. Minimize njRAT window. You can observe that a **Trojan.exe** file has been created at the location **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.

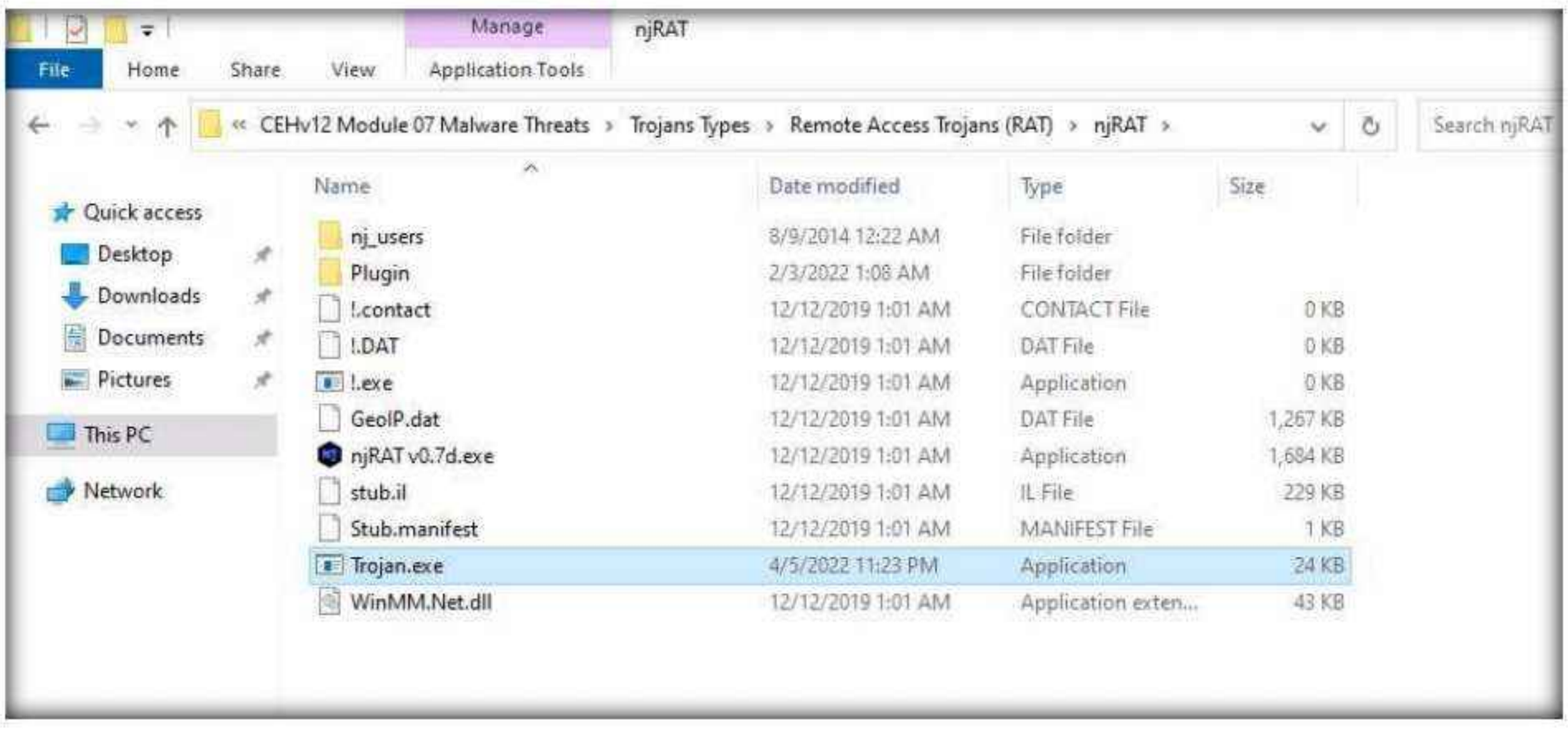


8. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

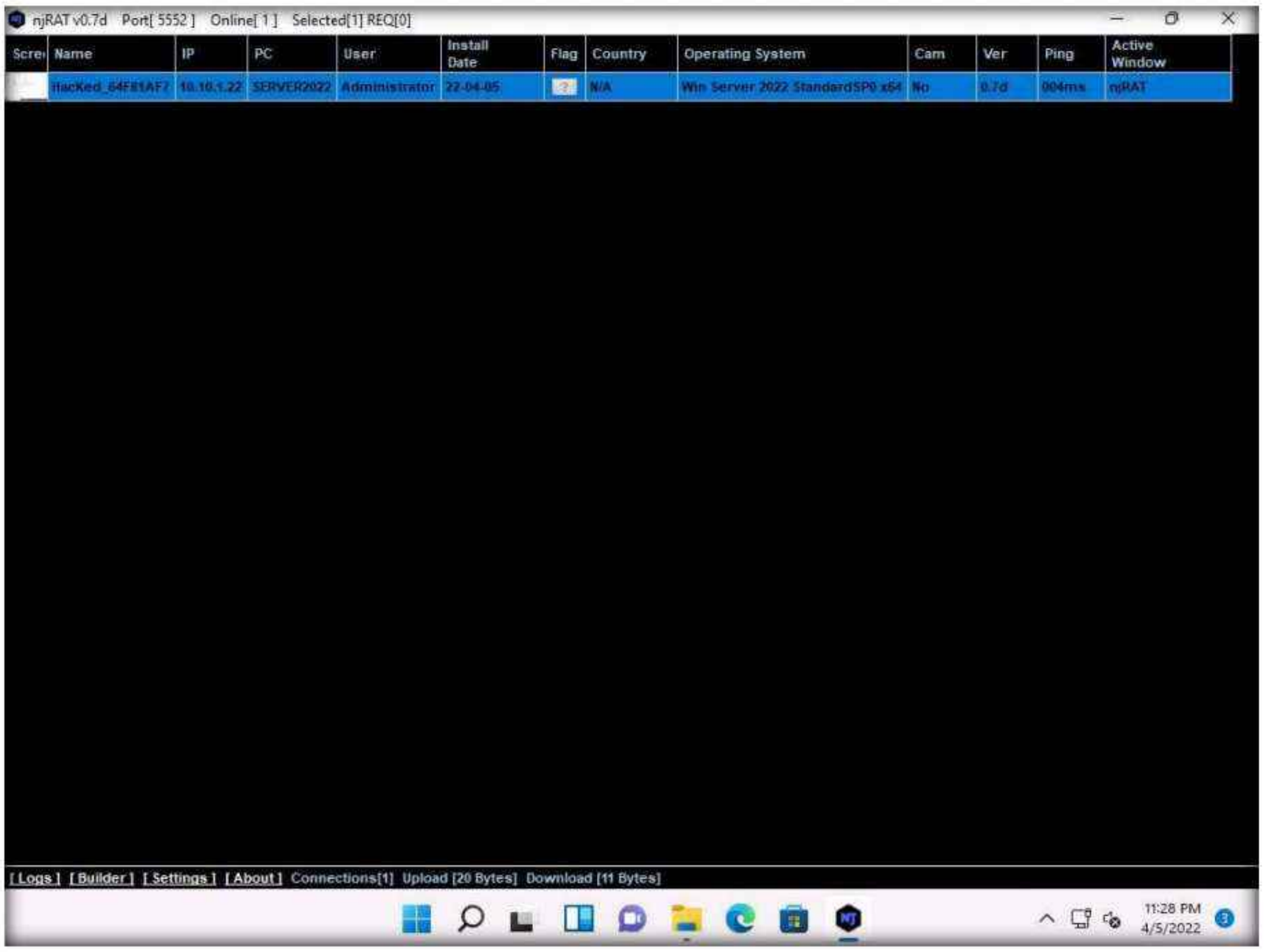
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



9. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.



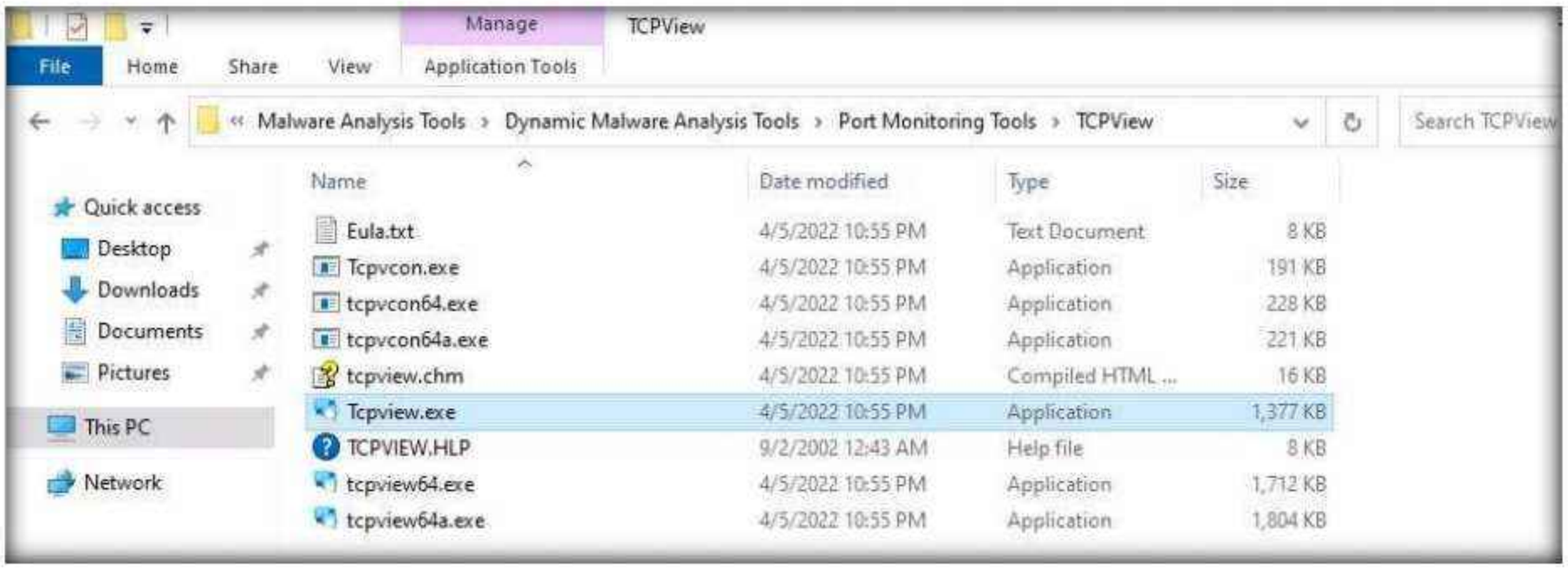
10. Observe that a connection has been established by the njRAT client. Click switch to the **Windows 11** virtual machine. Switch to **njRAT** window to observe the established connection.



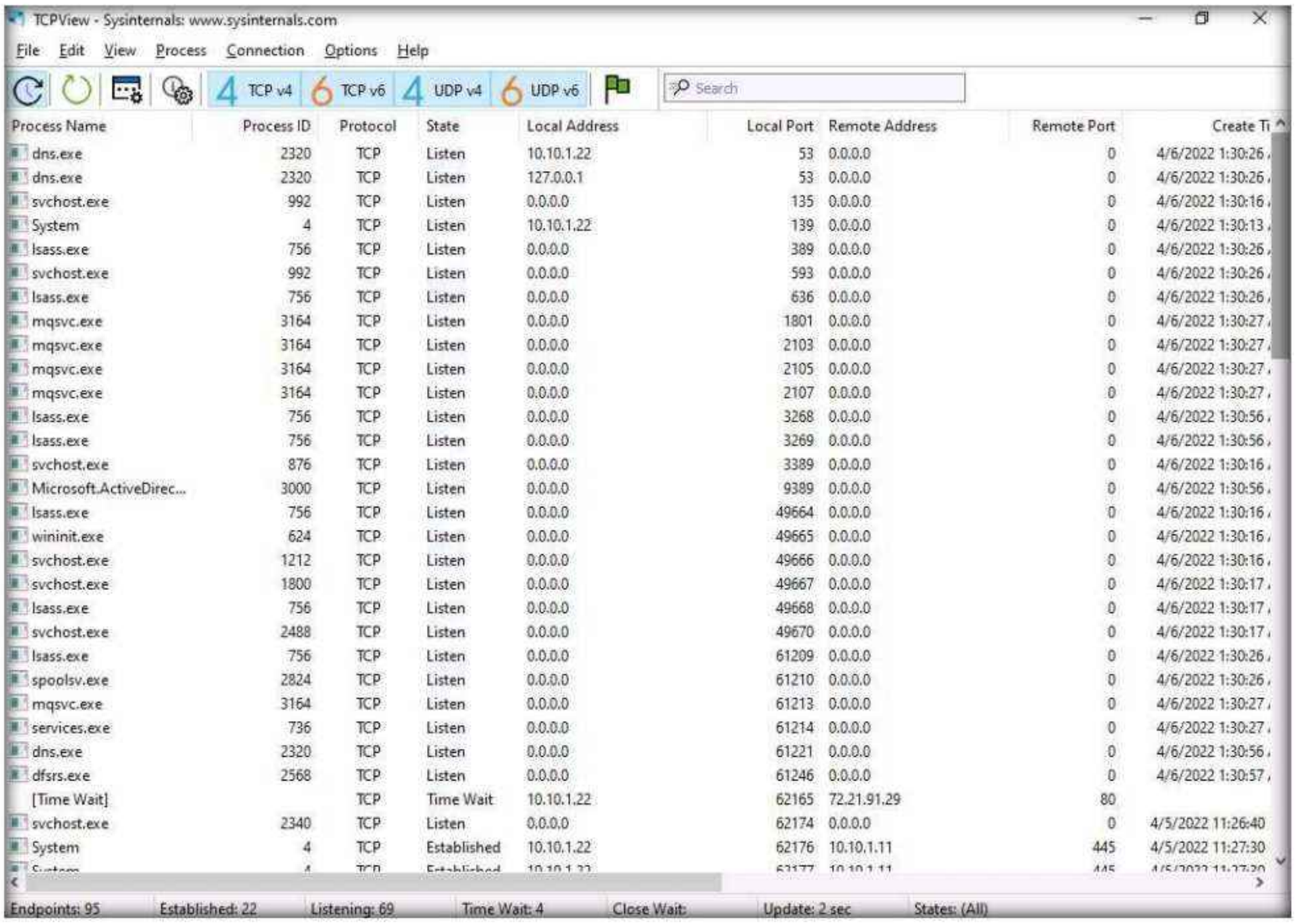
11. Now, let us analyze this process on **Windows Server 2022** using **TCPView** tool. Switch back to the **Windows Server 2022** virtual machine.

12. Navigate to **Z:\CEHv12 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**.

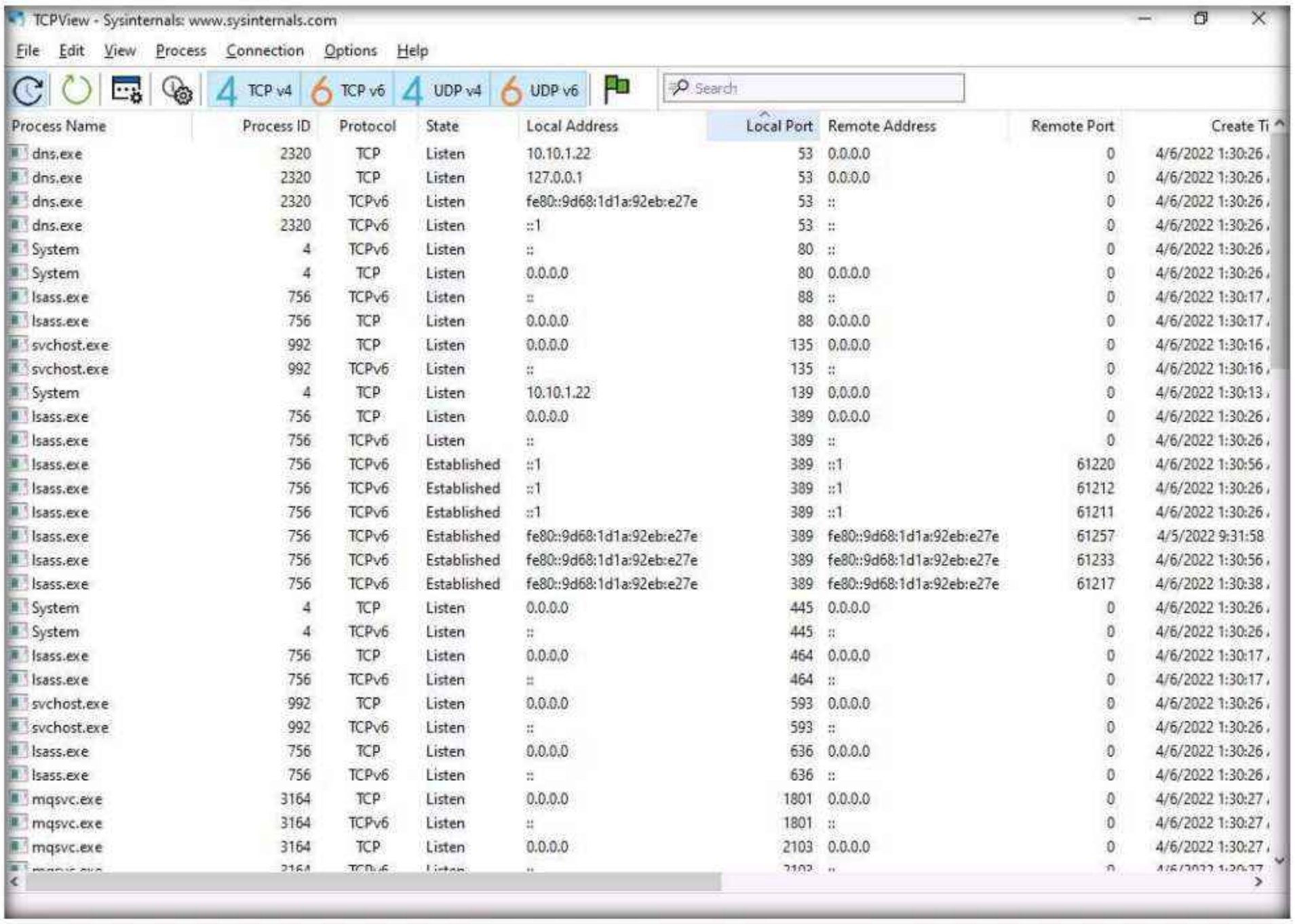


13. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.
14. The **TCPView** main window appears, displaying the details such as Process, ProcessId, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State, as shown in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



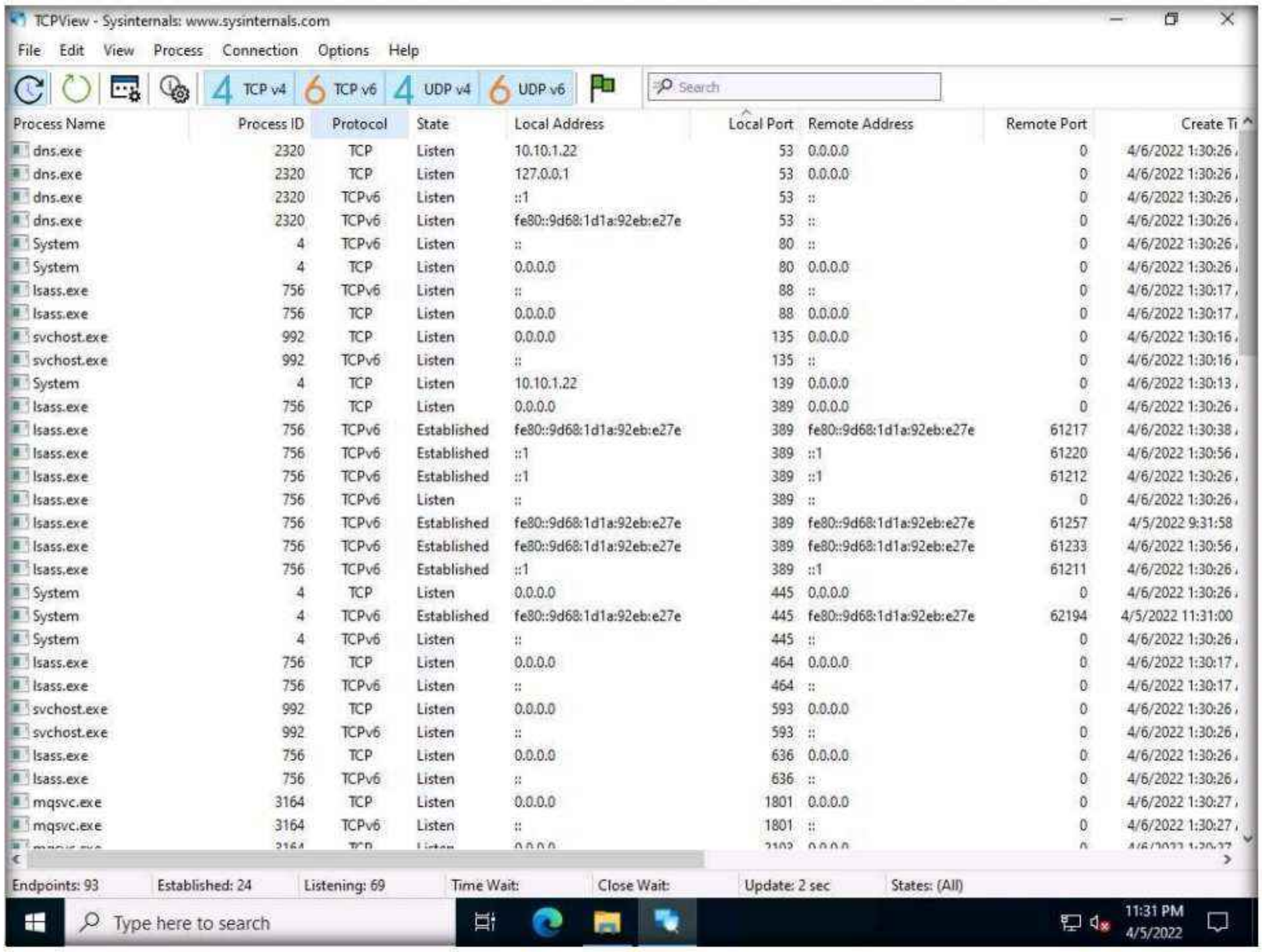
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Ti
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2103	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2105	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2107	0.0.0.0	0	4/6/2022 1:30:27
lsass.exe	756	TCP	Listen	0.0.0.0	3268	0.0.0.0	0	4/6/2022 1:30:56
lsass.exe	756	TCP	Listen	0.0.0.0	3269	0.0.0.0	0	4/6/2022 1:30:56
svchost.exe	876	TCP	Listen	0.0.0.0	3389	0.0.0.0	0	4/6/2022 1:30:16
Microsoft.ActiveDirec...	3000	TCP	Listen	0.0.0.0	9389	0.0.0.0	0	4/6/2022 1:30:56
lsass.exe	756	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	4/6/2022 1:30:16
wininit.exe	624	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	1212	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	1800	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	2488	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	61209	0.0.0.0	0	4/6/2022 1:30:26
spoolsv.exe	2824	TCP	Listen	0.0.0.0	61210	0.0.0.0	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	61213	0.0.0.0	0	4/6/2022 1:30:27
services.exe	736	TCP	Listen	0.0.0.0	61214	0.0.0.0	0	4/6/2022 1:30:27
dns.exe	2320	TCP	Listen	0.0.0.0	61221	0.0.0.0	0	4/6/2022 1:30:56
dfsrs.exe	2568	TCP	Listen	0.0.0.0	61246	0.0.0.0	0	4/6/2022 1:30:57
[Time Wait]		TCP	Time Wait	10.10.1.22	62165	72.21.91.29	80	
svchost.exe	2340	TCP	Listen	0.0.0.0	62174	0.0.0.0	0	4/5/2022 11:26:40
System	4	TCP	Established	10.10.1.22	62176	10.10.1.11	445	4/5/2022 11:27:30

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



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Ti
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	fe80::9d68:1d1a:92eb:e27e	53	::	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	::1	53	::	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	80	::	0	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	80	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	88	::	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	88	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	992	TCPv6	Listen	::	135	::	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	389	::	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	::1	389	::1	61220	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61212	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	::1	389	::1	61211	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61257	4/5/2022 9:31:58
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61233	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61217	4/6/2022 1:30:38
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	445	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	464	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCPv6	Listen	::	464	::	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCPv6	Listen	::	593	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	636	::	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCPv6	Listen	::	1801	::	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2103	0.0.0.0	0	4/6/2022 1:30:27

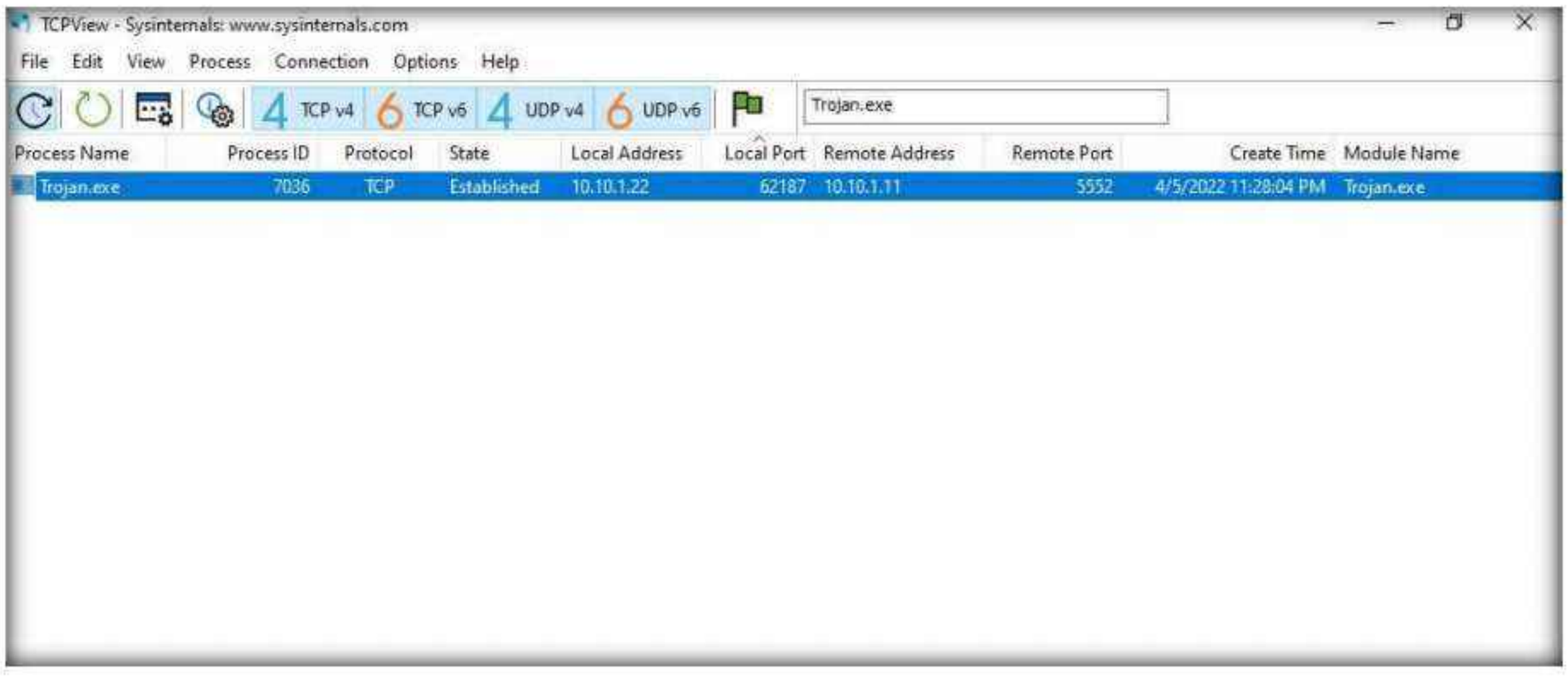
16. Observe the protocols running on different ports under the **Protocol** column.



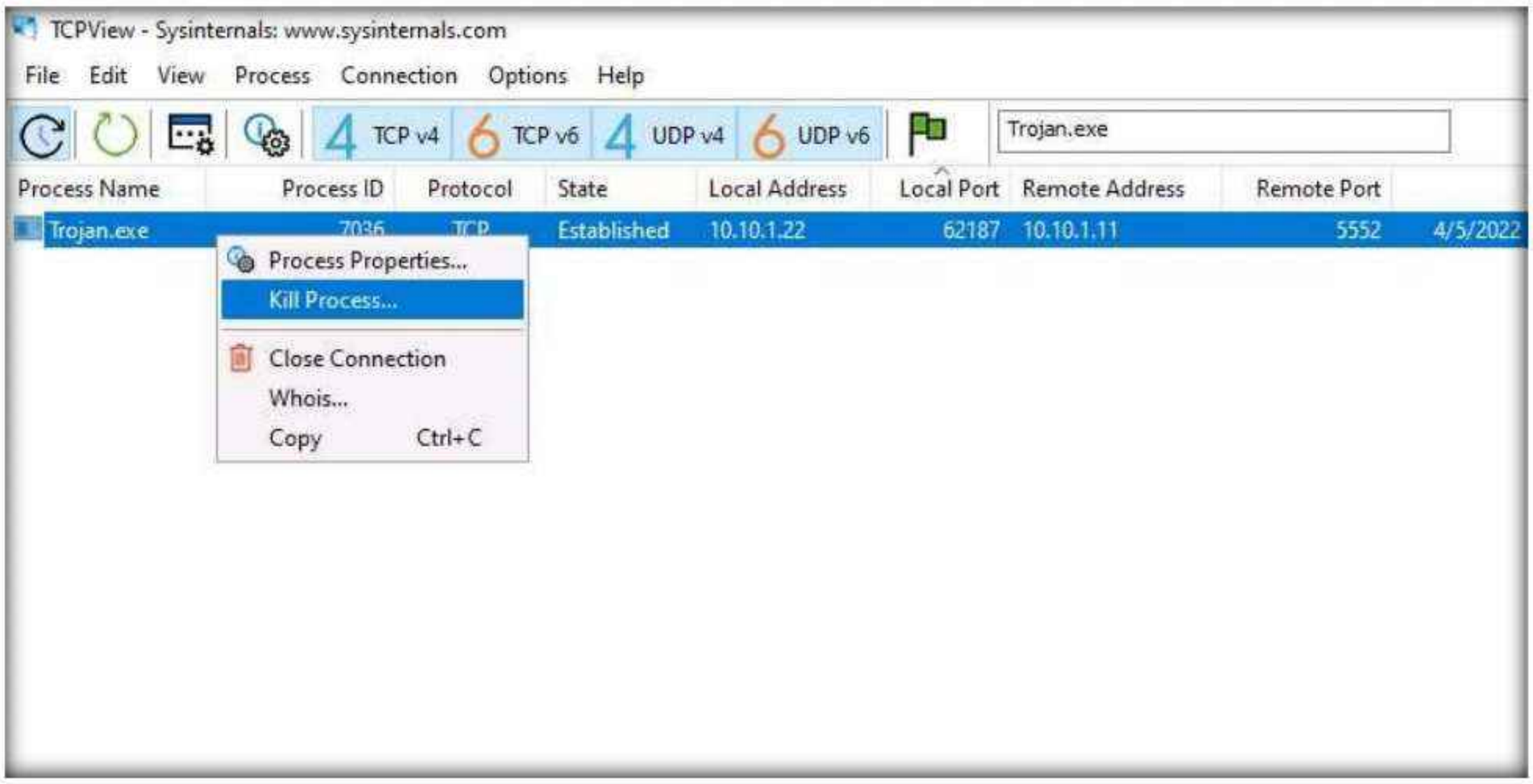
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Ti
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	::1	53	::	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	fe80::9d68:1d1a:92eb:e27e	53	::	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	80	::	0	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	80	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	88	::	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	88	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	992	TCPv6	Listen	::	135	::	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61217	4/6/2022 1:30:38
lsass.exe	756	TCPv6	Established	::1	389	::1	61220	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61212	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	389	::	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61257	4/5/2022 9:31:58
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61233	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61211	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	4/6/2022 1:30:26
System	4	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	445	fe80::9d68:1d1a:92eb:e27e	62194	4/5/2022 11:31:00
System	4	TCPv6	Listen	::	445	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	464	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCPv6	Listen	::	464	::	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCPv6	Listen	::	593	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	636	::	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCPv6	Listen	::	1801	::	0	4/6/2022 1:30:27

17. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.

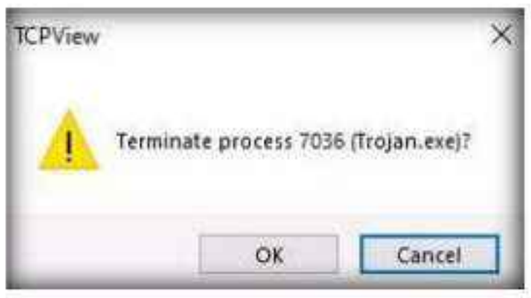
18. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2022** machine. You can see details such as **Remote Address** and **Remote Port**.



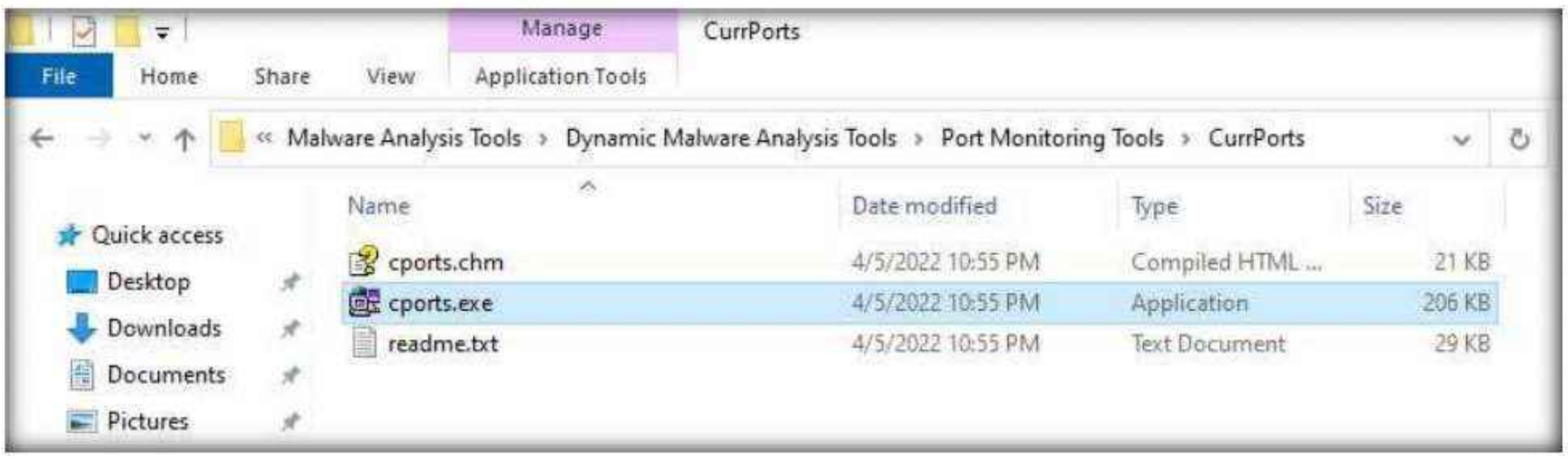
19. Right-click the process **Trojan.exe**; select **Kill Process...** to end the running process.



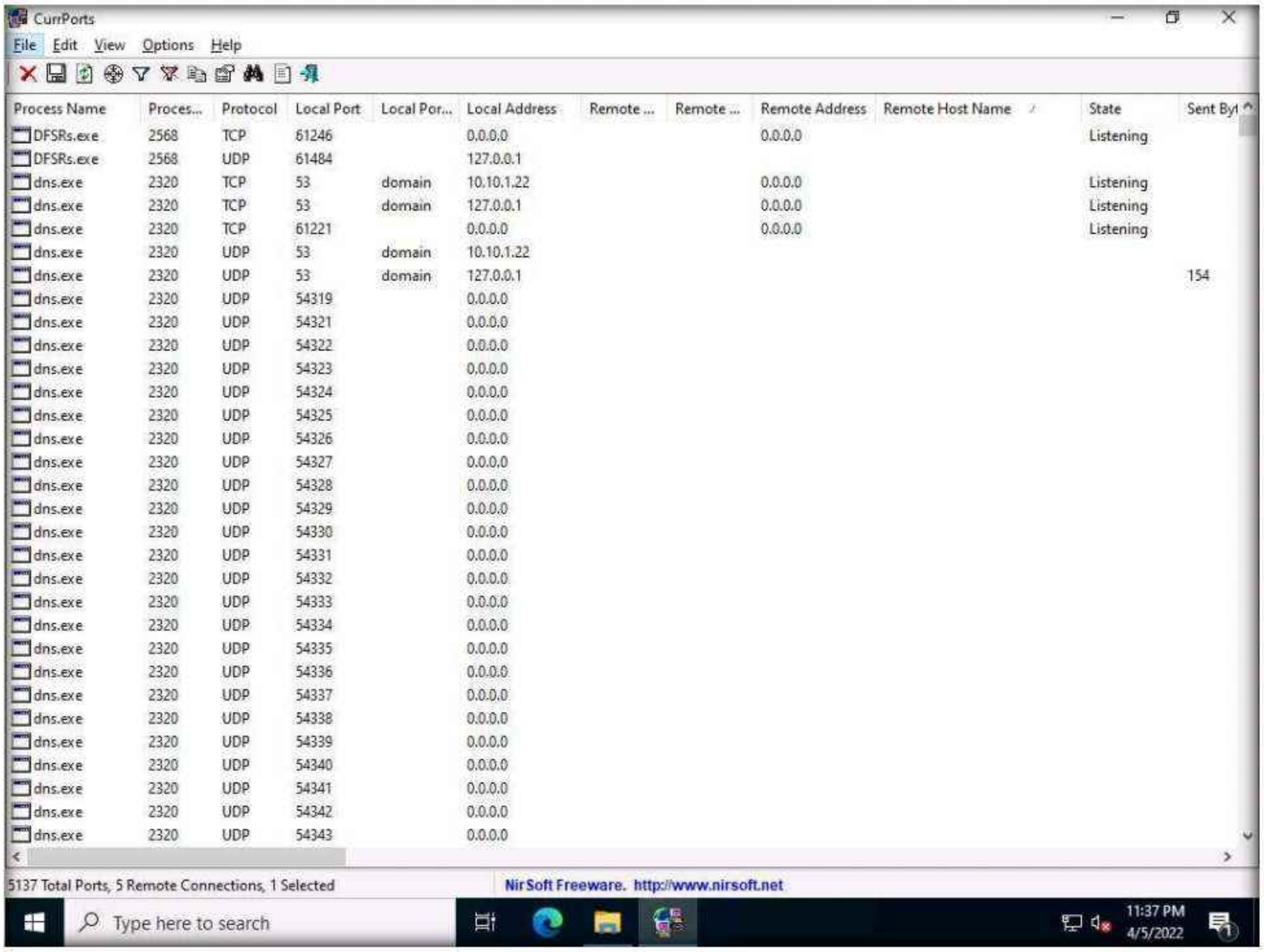
20. Normally, if a **TCPView** dialog box appears, click **OK** to terminate the process. However, for this task, do not Kill the process in this step as we are going to use this running process for the next task; click **Cancel**.



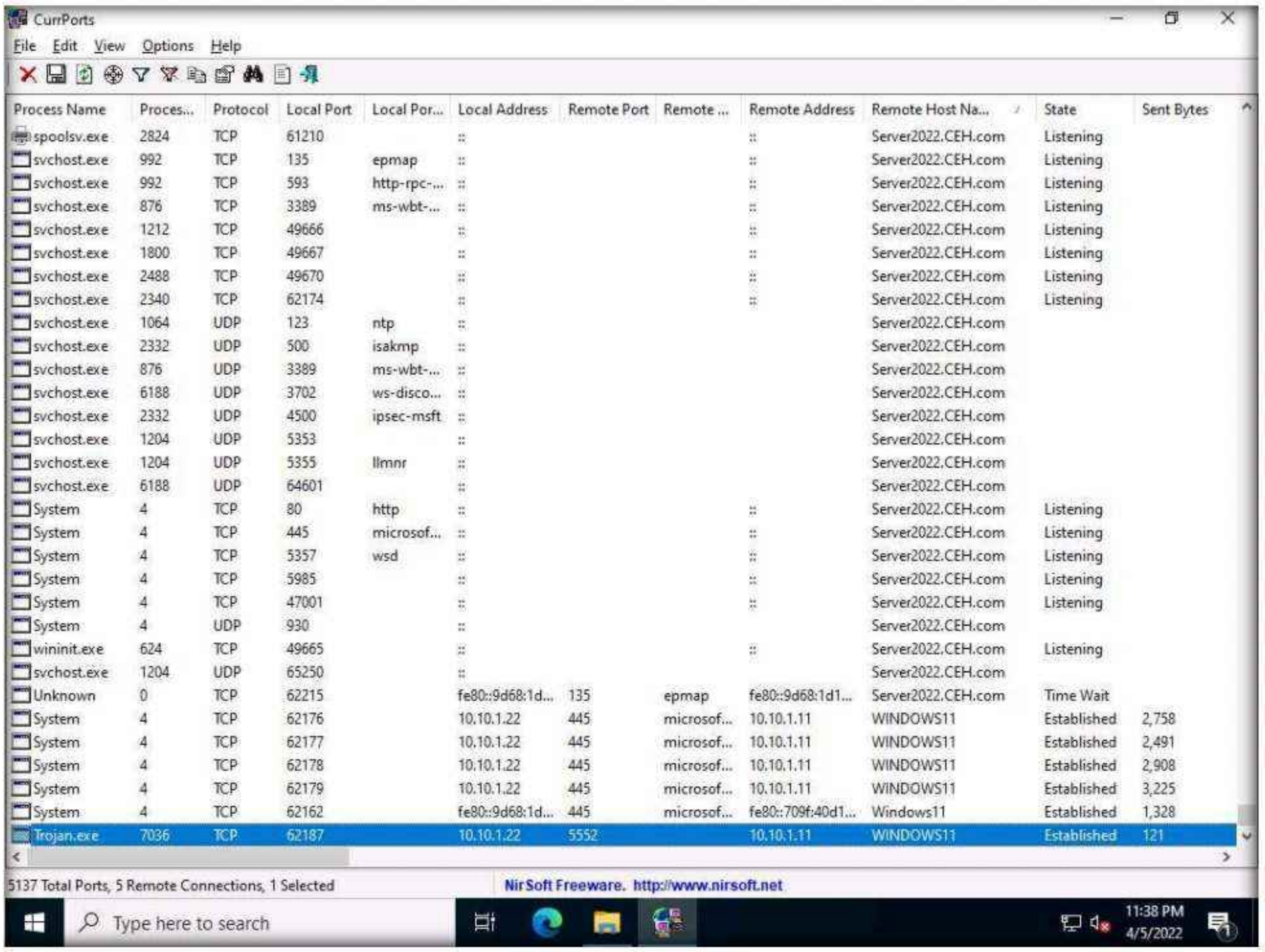
21. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.
22. Close the **TCPView** window.
23. Now, let us analyze this process on **Windows Server 2022** using **CurrPorts**.
24. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.



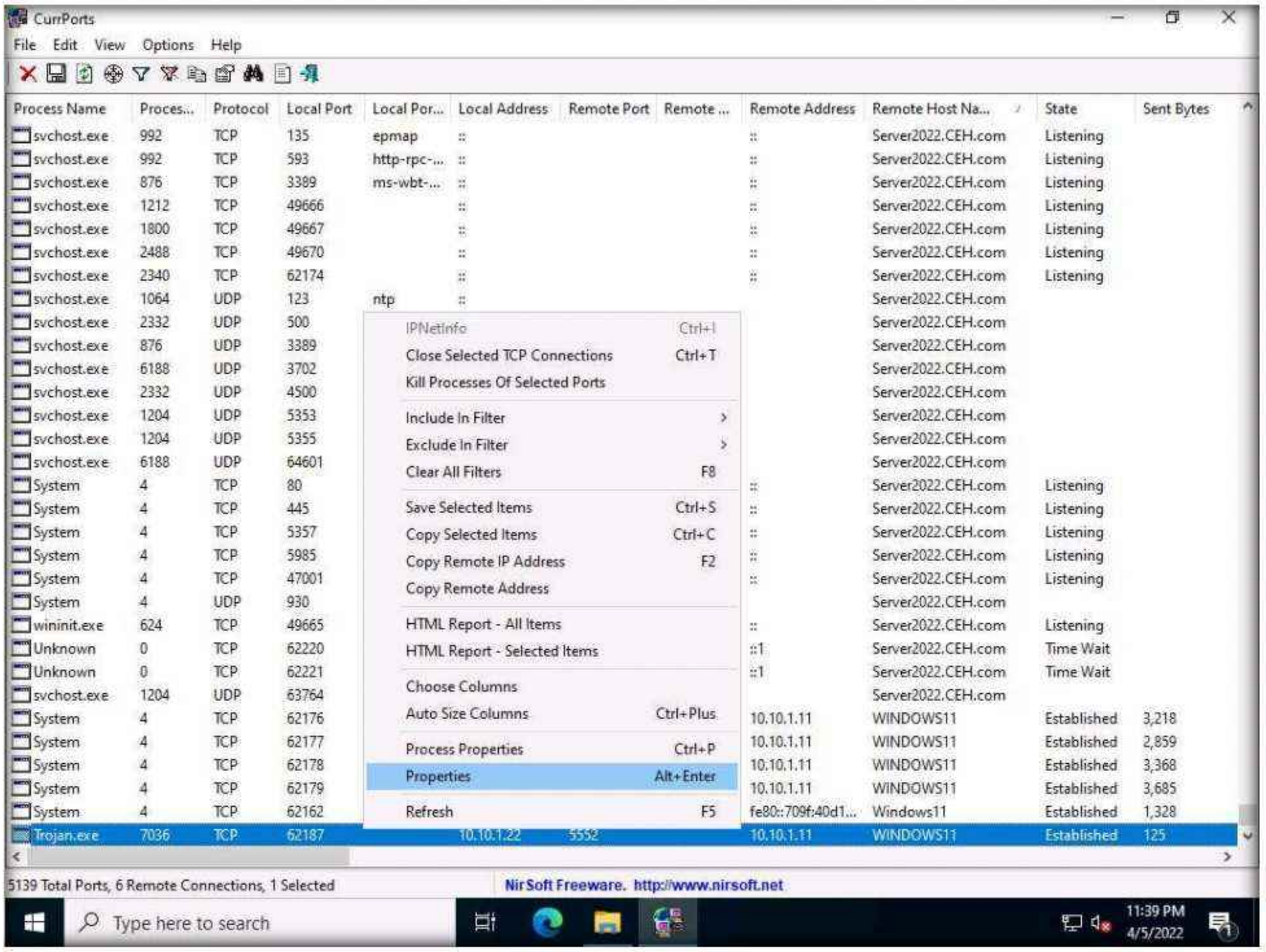
25. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine.



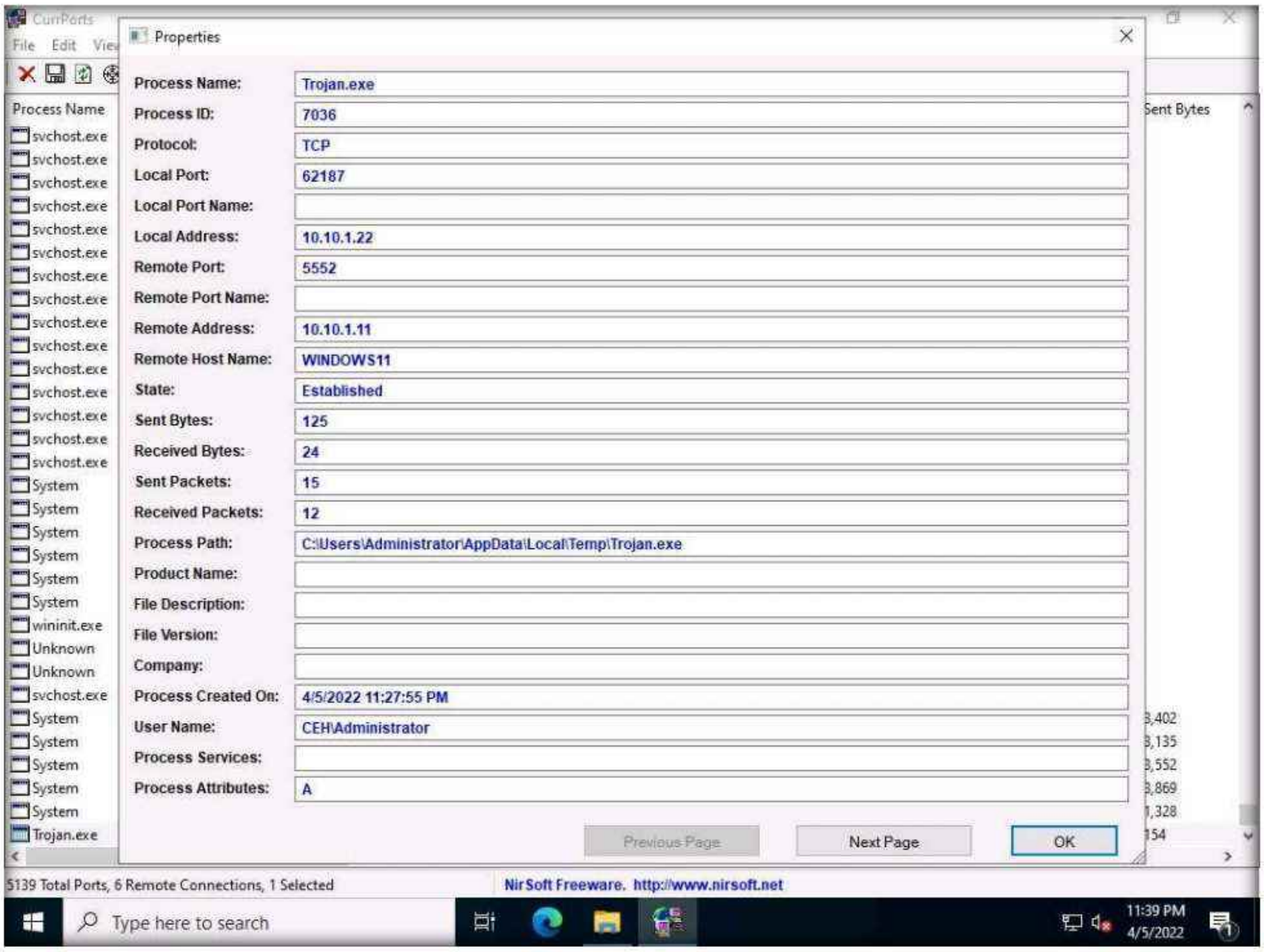
26. Scroll-down to search for **Trojan.exe** process running on the machine, as the shown in the screenshot. It is evident from the above screenshot that the process is connected to the machine on **port 5552**.



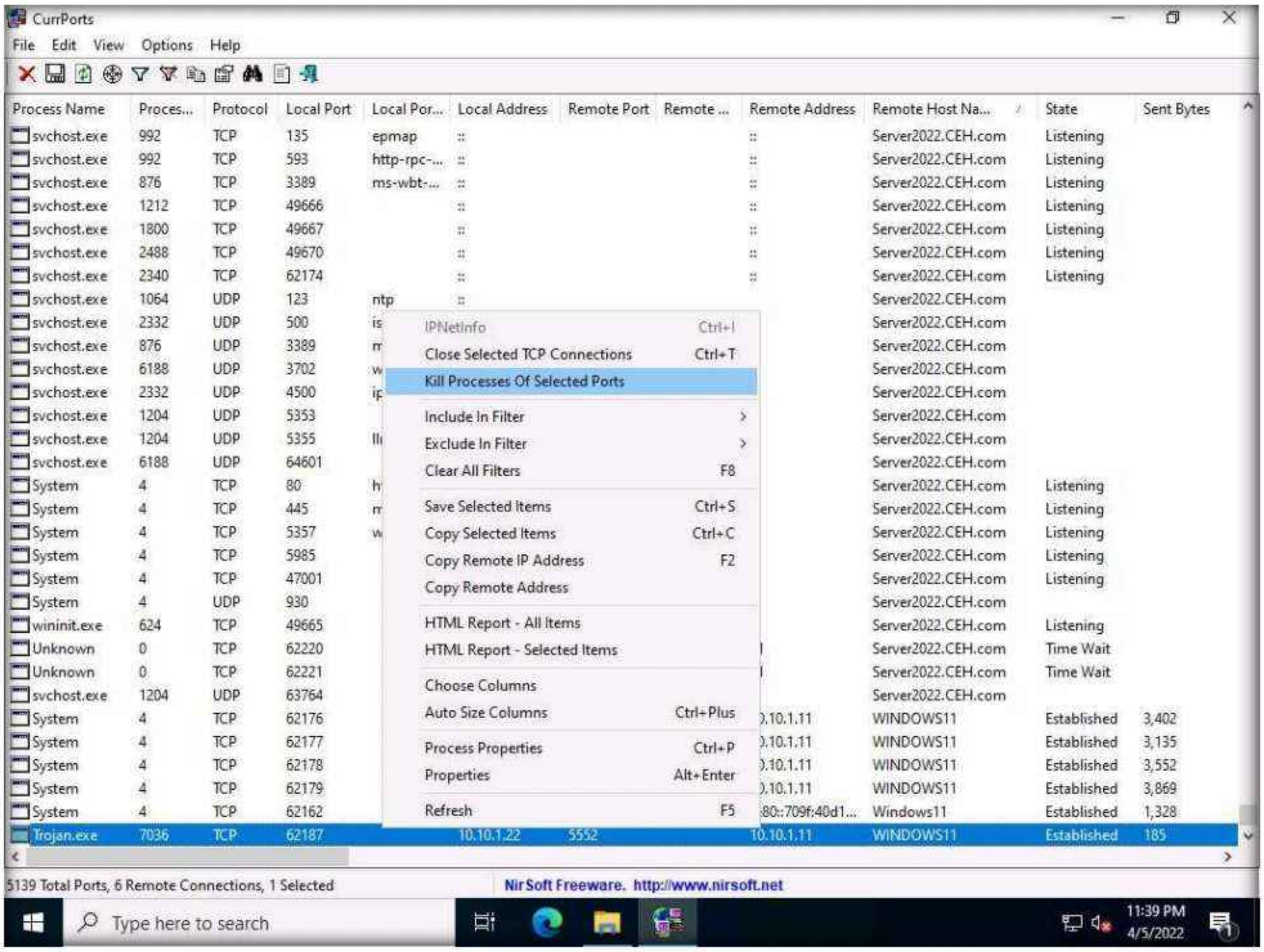
27. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.



28. 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.
29. Once you are done examining the properties associated with the process, click **OK**.



30. 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.
31. 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.



32. 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**.

33. This way, you can analyze the ports open on a machine and the processes running on it.
34. If a process is found to be suspicious, you may either kill the process or close the port.
35. Close all open windows.
36. You can also use other port monitoring tools such as **Port Monitor** (https://www.port-monitor.com), **TCP Port Monitoring** (https://www.dotcom-monitor.com), or **PortExpert** (https://www.kcsoftwares.com) to perform port monitoring.

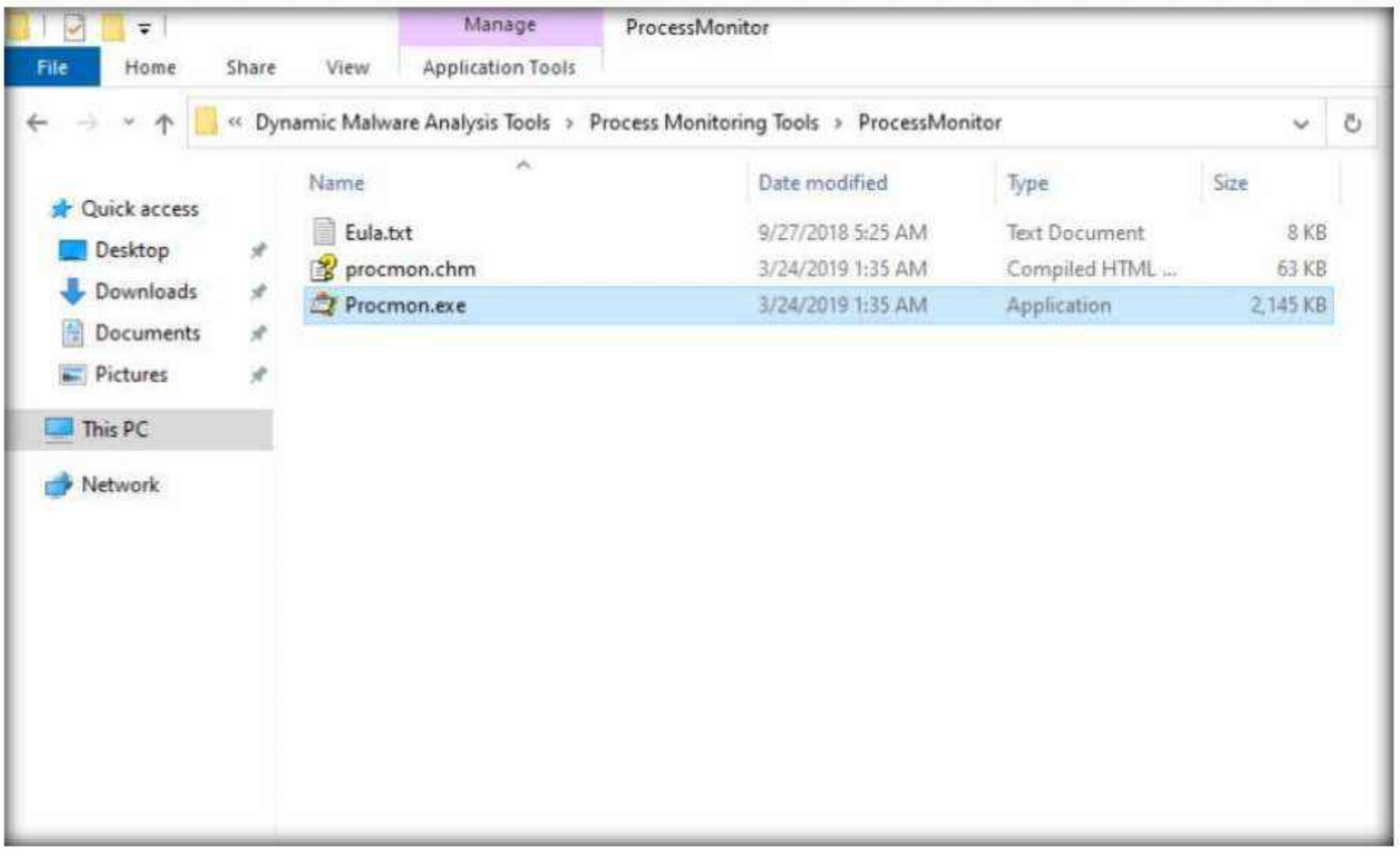
Task 2: Perform Process Monitoring using Process Monitor

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.

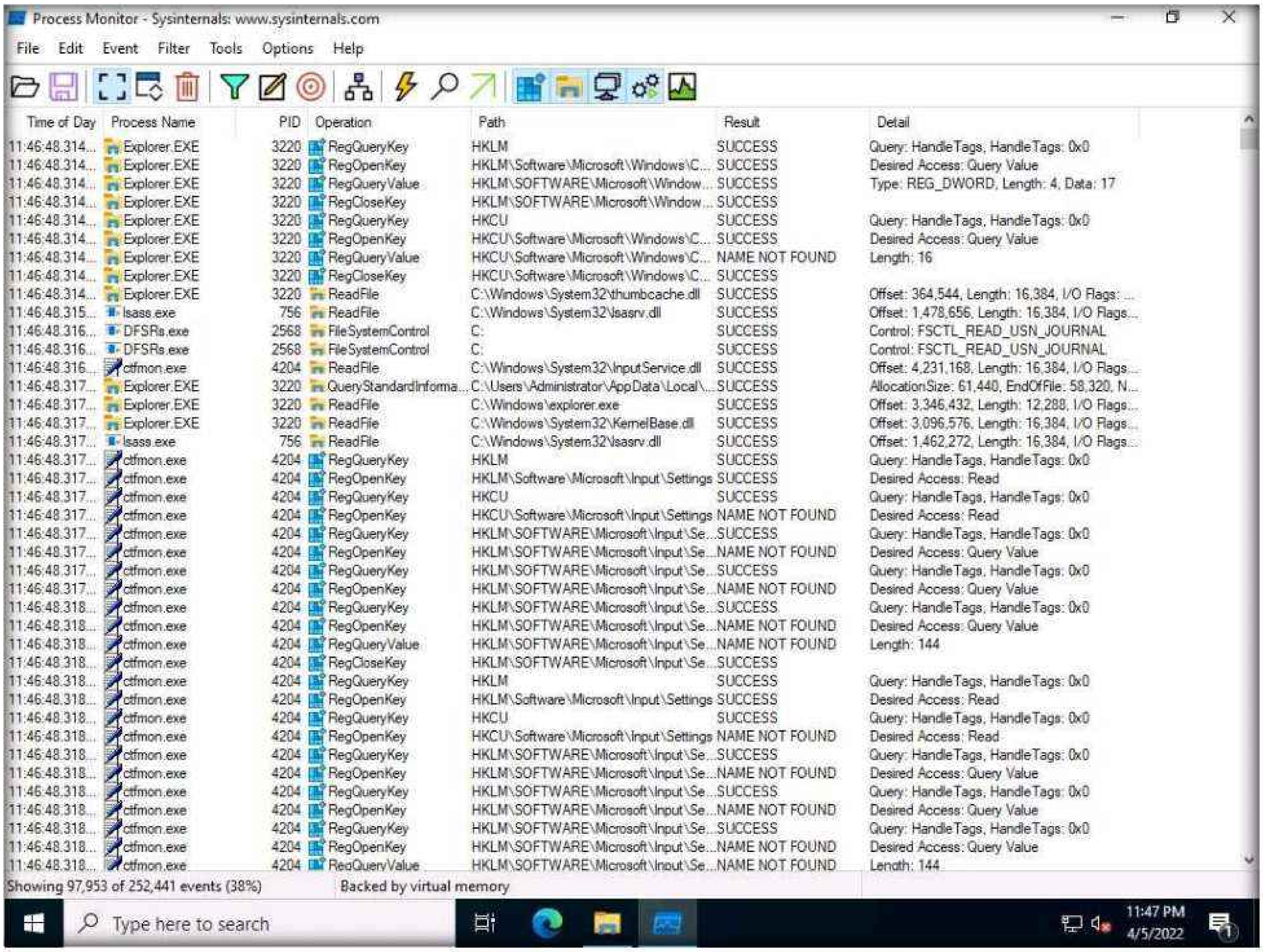
Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, 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.

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

1. On the **Windows Server 2022** machine, navigate to **Z:\CEHv12 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.

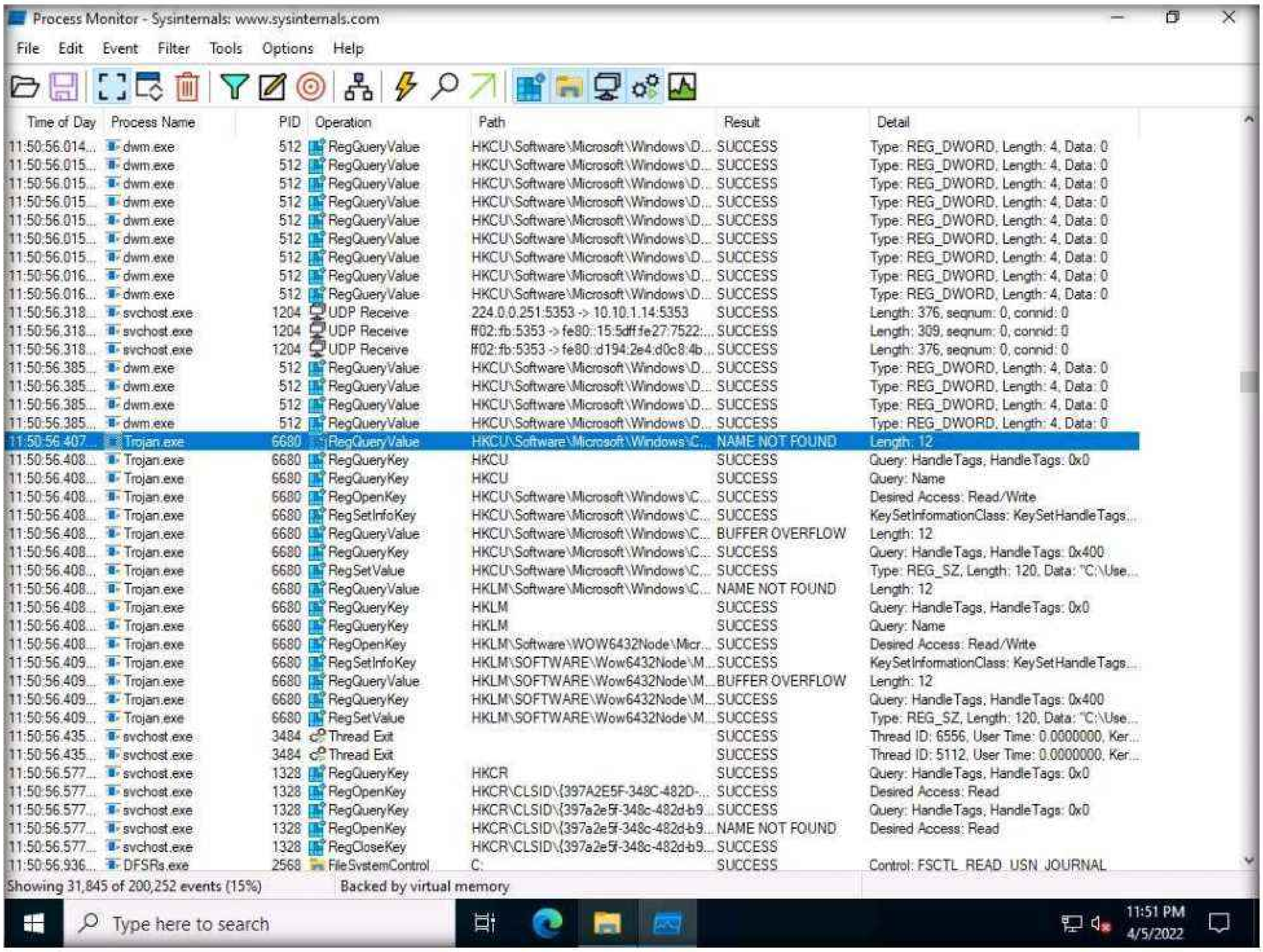


2. The **Process Monitor License Agreement** window appears; click **Agree**.
3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.

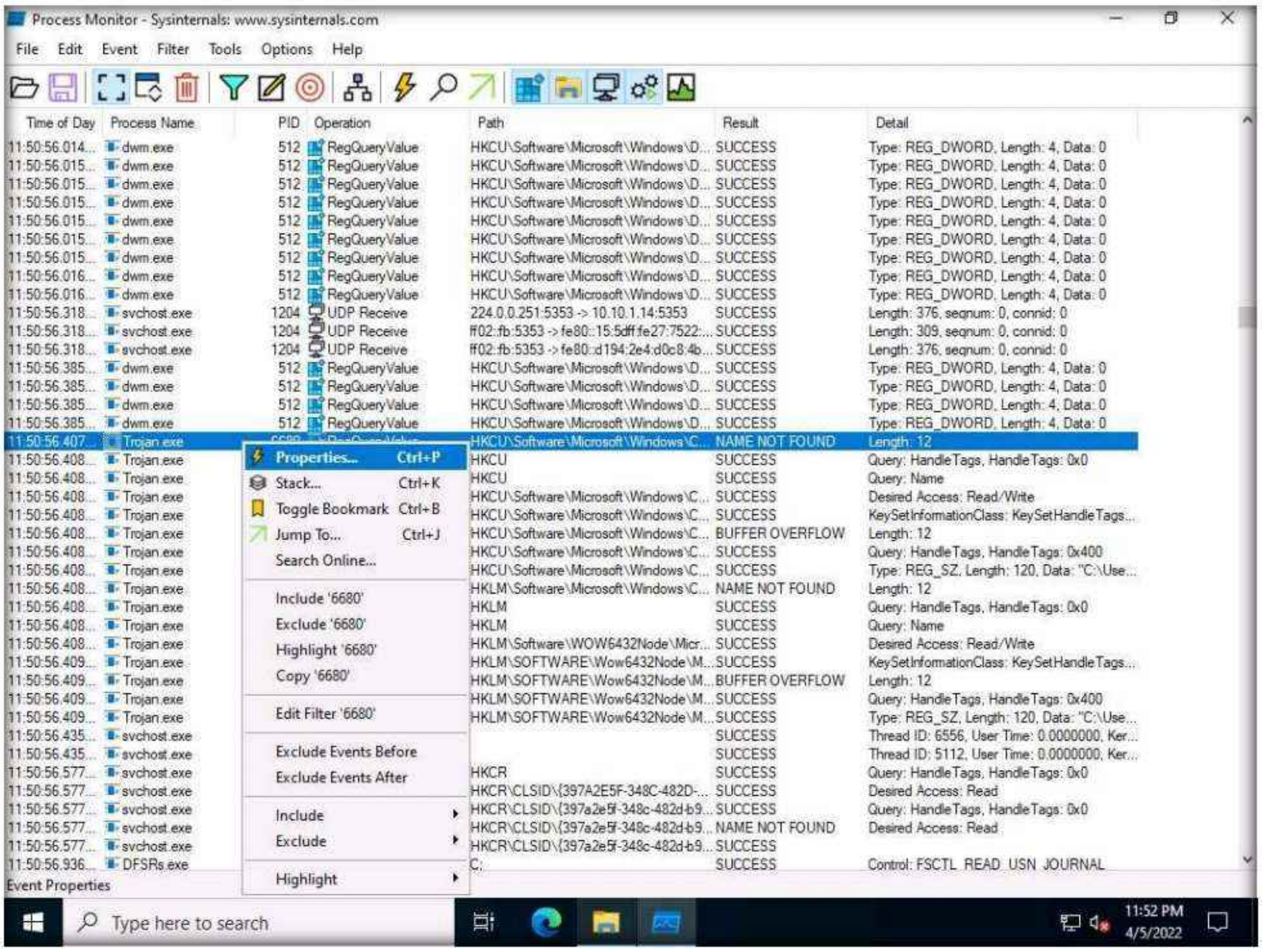


4. Scroll-down to look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.

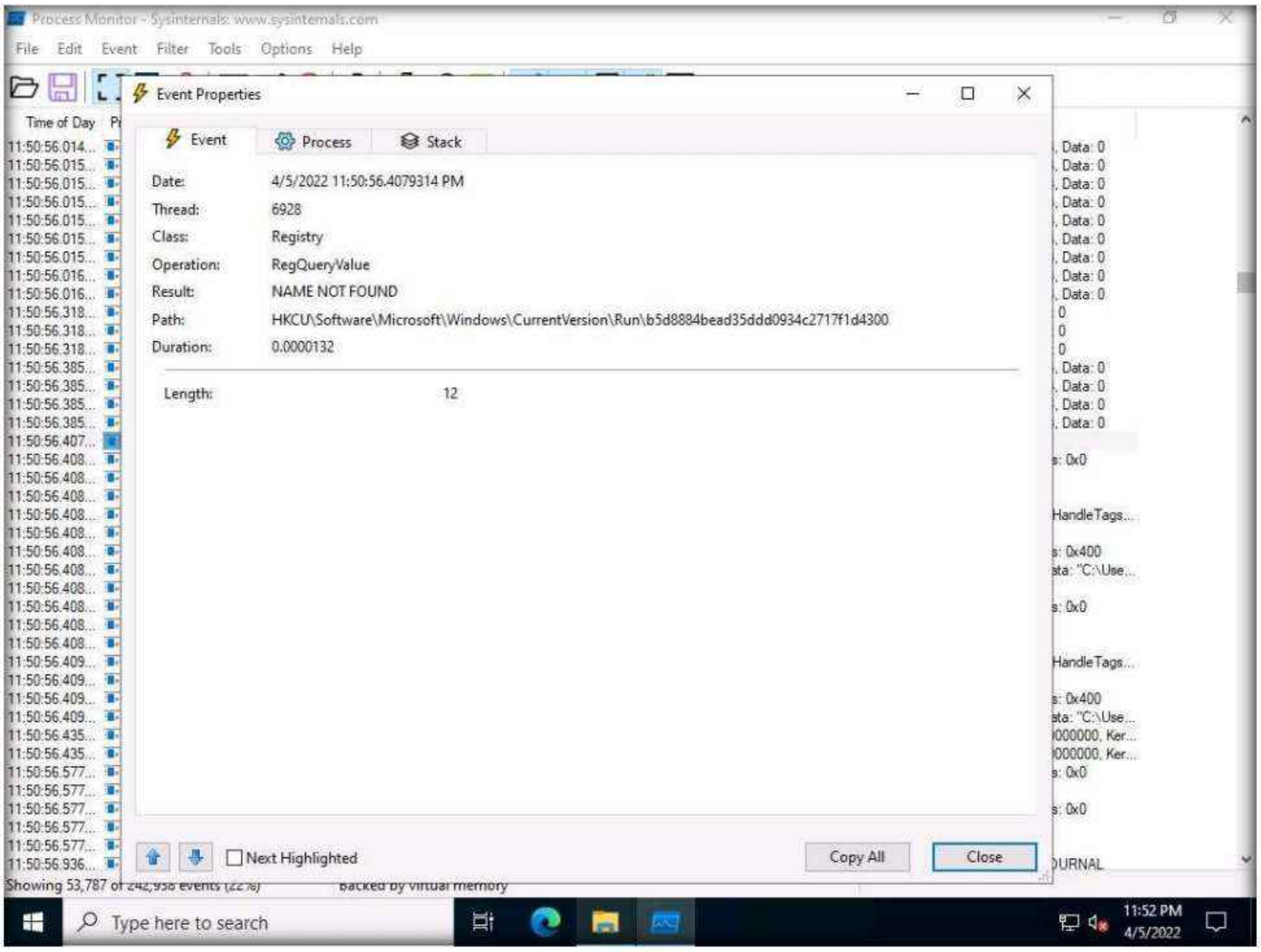
5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.



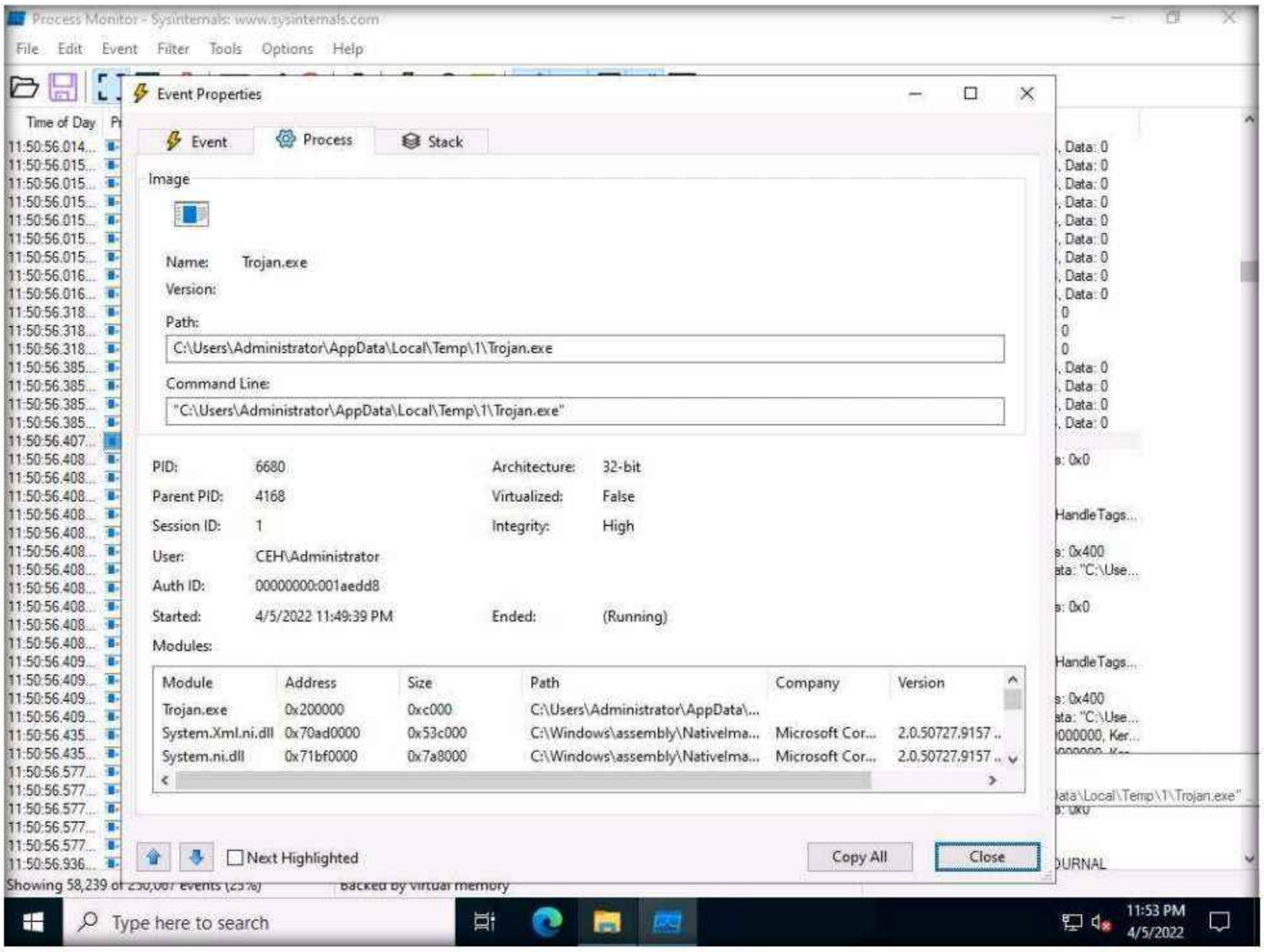
6. To view the properties of a running process, select the process (here, **Trojan.exe**), right-click on the process and select **Properties** from the context menu.



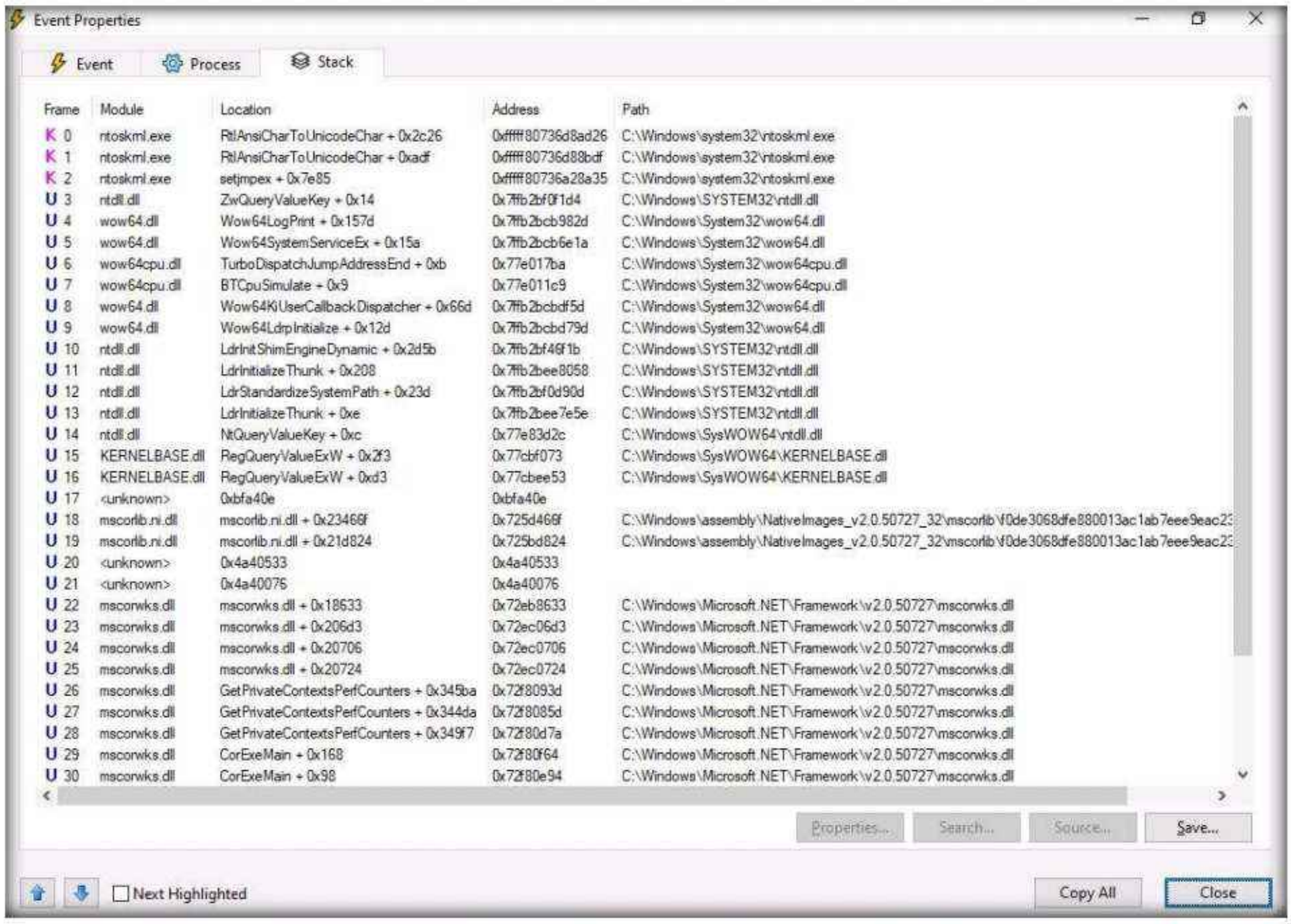
7. The **Event Properties** window appears with the details of the chosen process.
8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.



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.



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



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 11** and **Windows Server 2022** machines.
15. 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.
16. Turn off the **Windows Server 2022** virtual machine.

Task 3: Perform Registry Monitoring using Reg Organizer

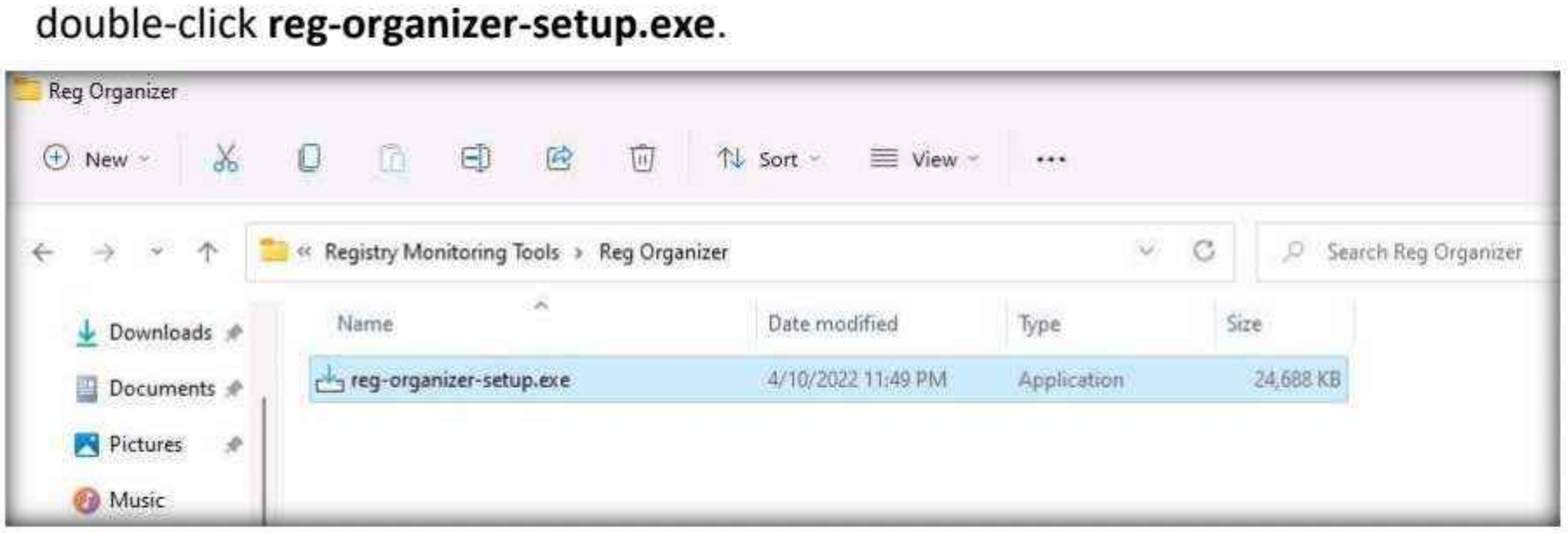
The Windows Registry stores OS and program configuration details such as settings and options. If the malware is a program, the registry stores its functionality. When an attacker installs a type of malware on the victim's machine, it generates a registry entry. One must have fair knowledge of the Windows 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.

Registry monitoring tools such as Reg Organizer provide a simple way to track registry modifications, which is useful in troubleshooting and monitoring background changes.

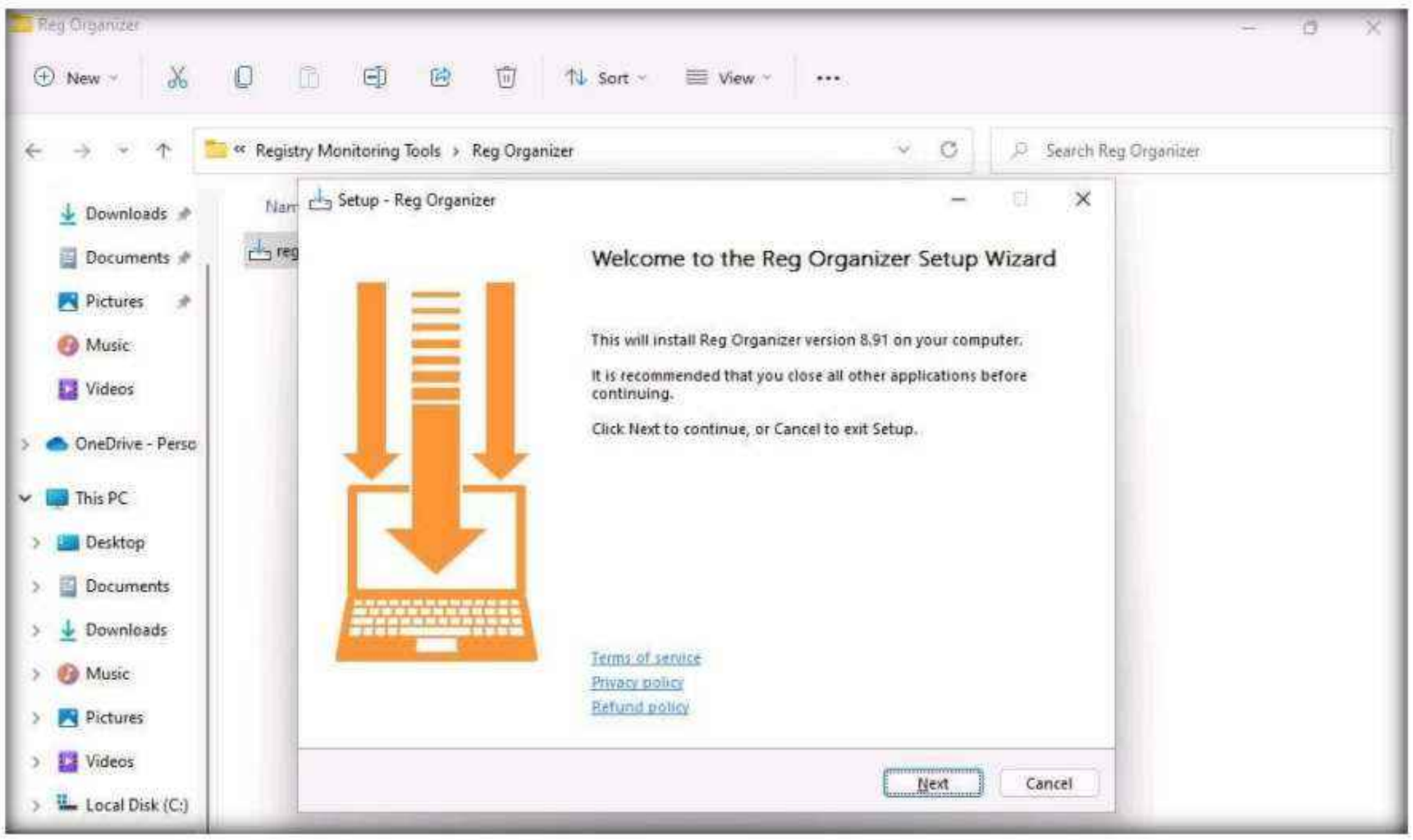
Reg Organizer: Reg Organizer is designed to edit keys and parameters, as well as to delete the content of.reg files. It allows users to perform various operations with the system registry such as export, import and copy key values. It can also perform a deep search to find even those keys associated with the application that cannot be found by other similar programs.

Here, we will use the registry monitoring tool Reg Organizer to scan the registry values for any changes.

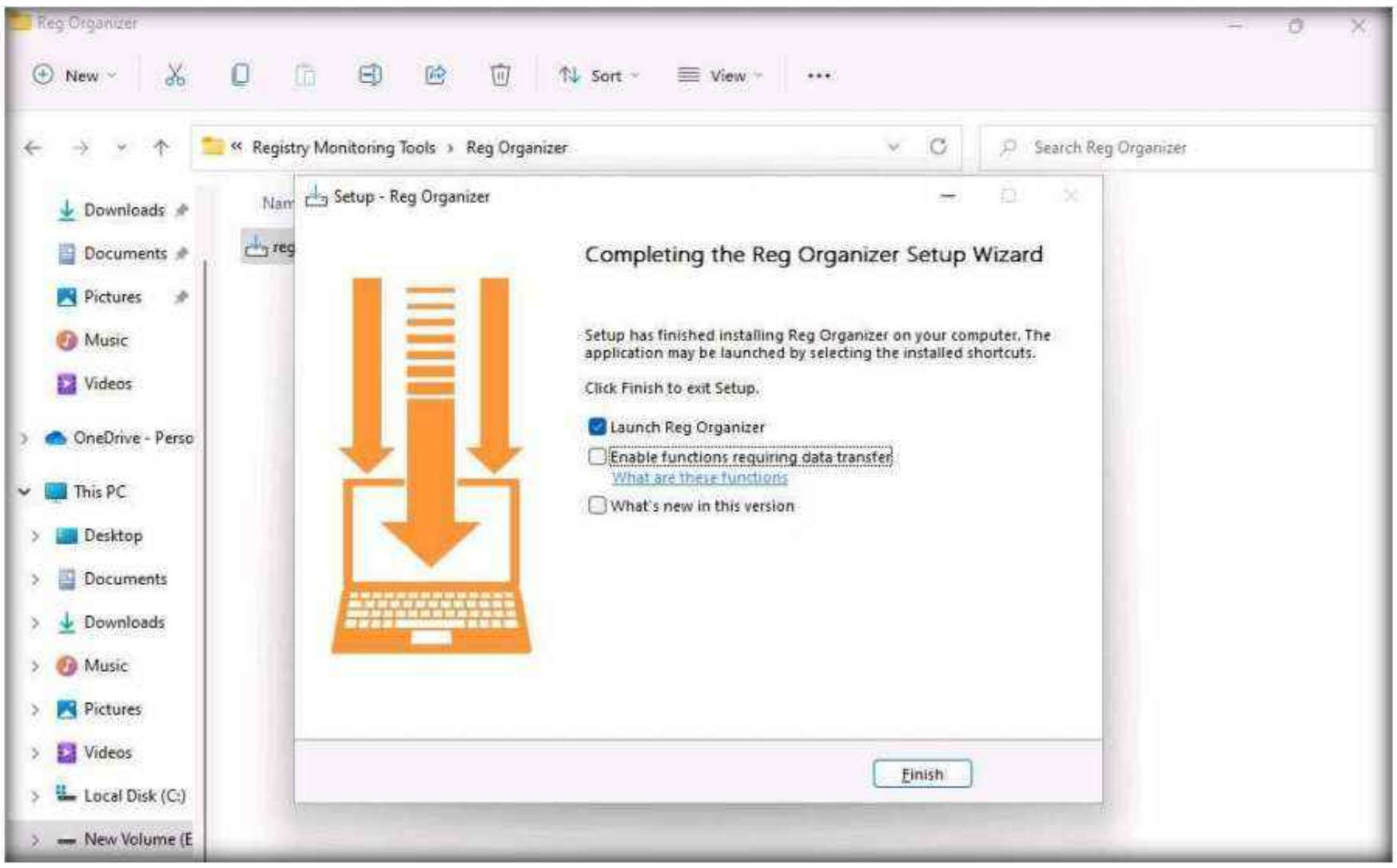
1. Switch to the **Windows 11** virtual machine.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\Reg Organizer**. double-click **reg-organizer-setup.exe**.



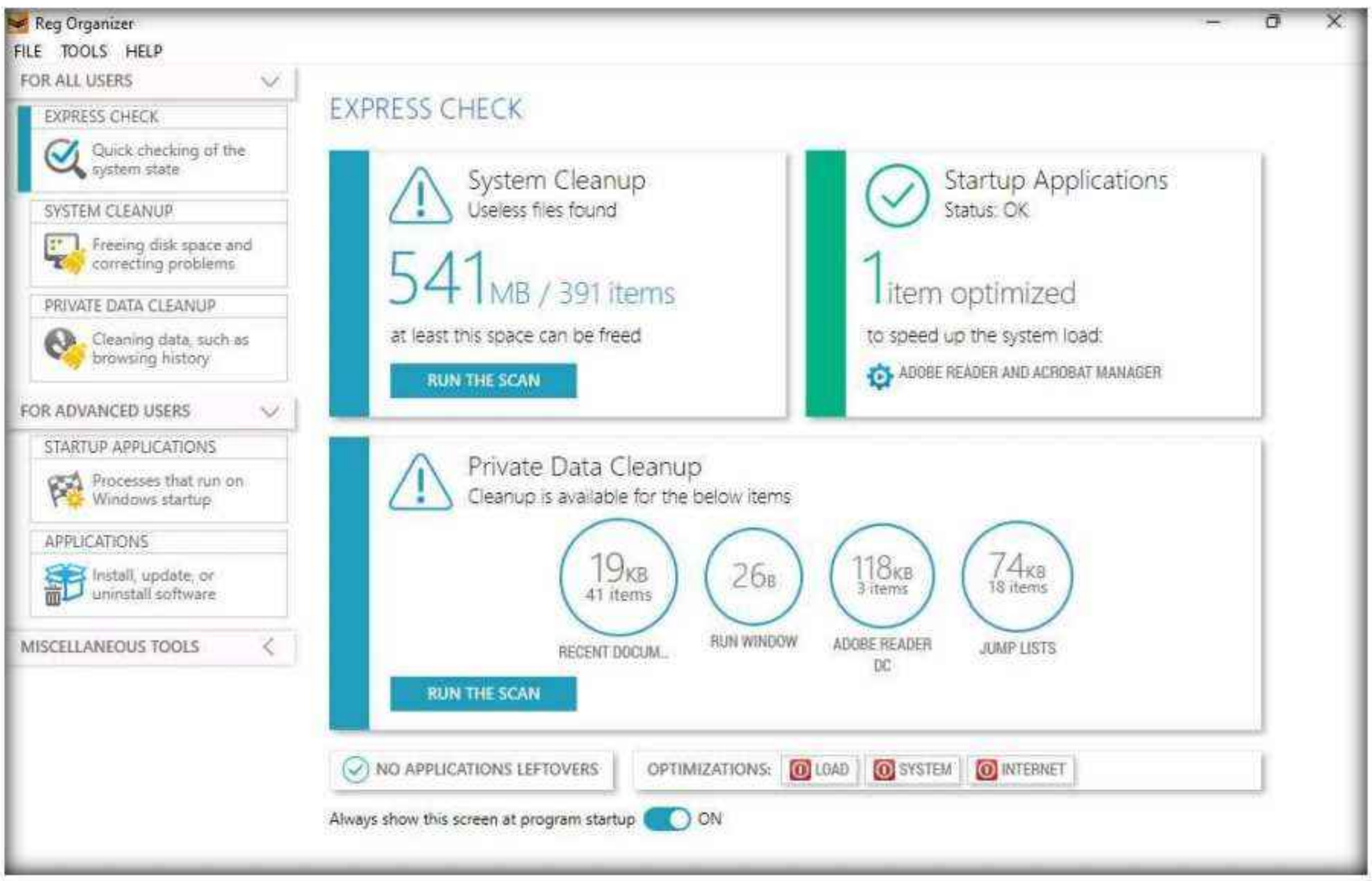
3. If **Open File - Security Warning** window appears, click **Run**.
4. If **User Account Control** window appears, click **Yes**.
5. **Setup - Reg Organizer** window appears, click **Next**.



6. Follow the wizard-driven installation steps to install the Reg Organizer.
7. After the completion of installation, **Completing the Reg Organizer Setup Wizard** appears, uncheck **Enable functions requiring data transfer** and **What's new in this version** checkboxes and click **Finish**.

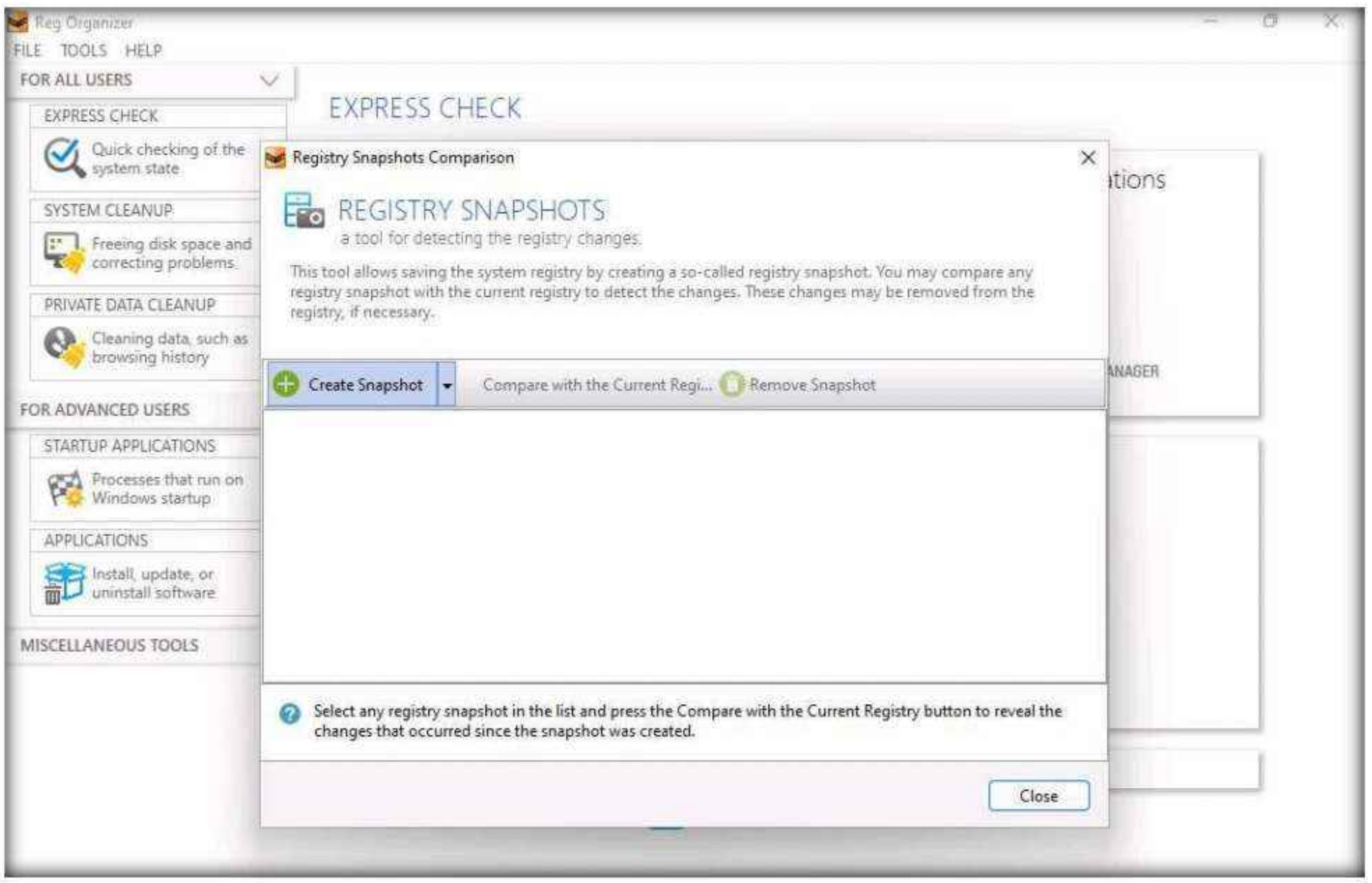


8. **Reg Organization** main window appears, displaying **System Cleanup**, **Startup Applications** and **Private Data Cleanup** sections, as shown in the screenshot.

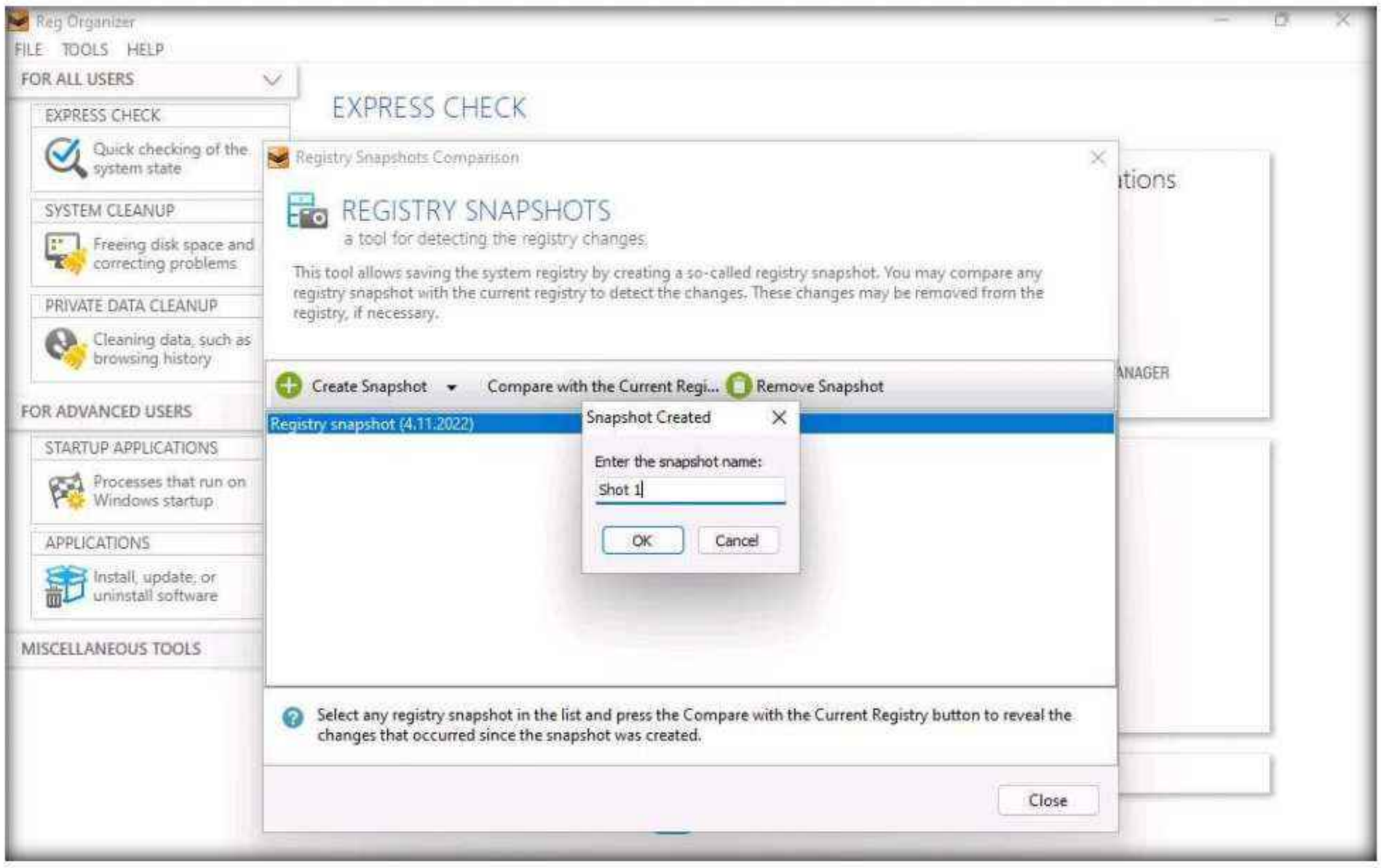


9. Now, click **TOOLS** from the menu bar and select **Registry Snapshots** option from the context menu.

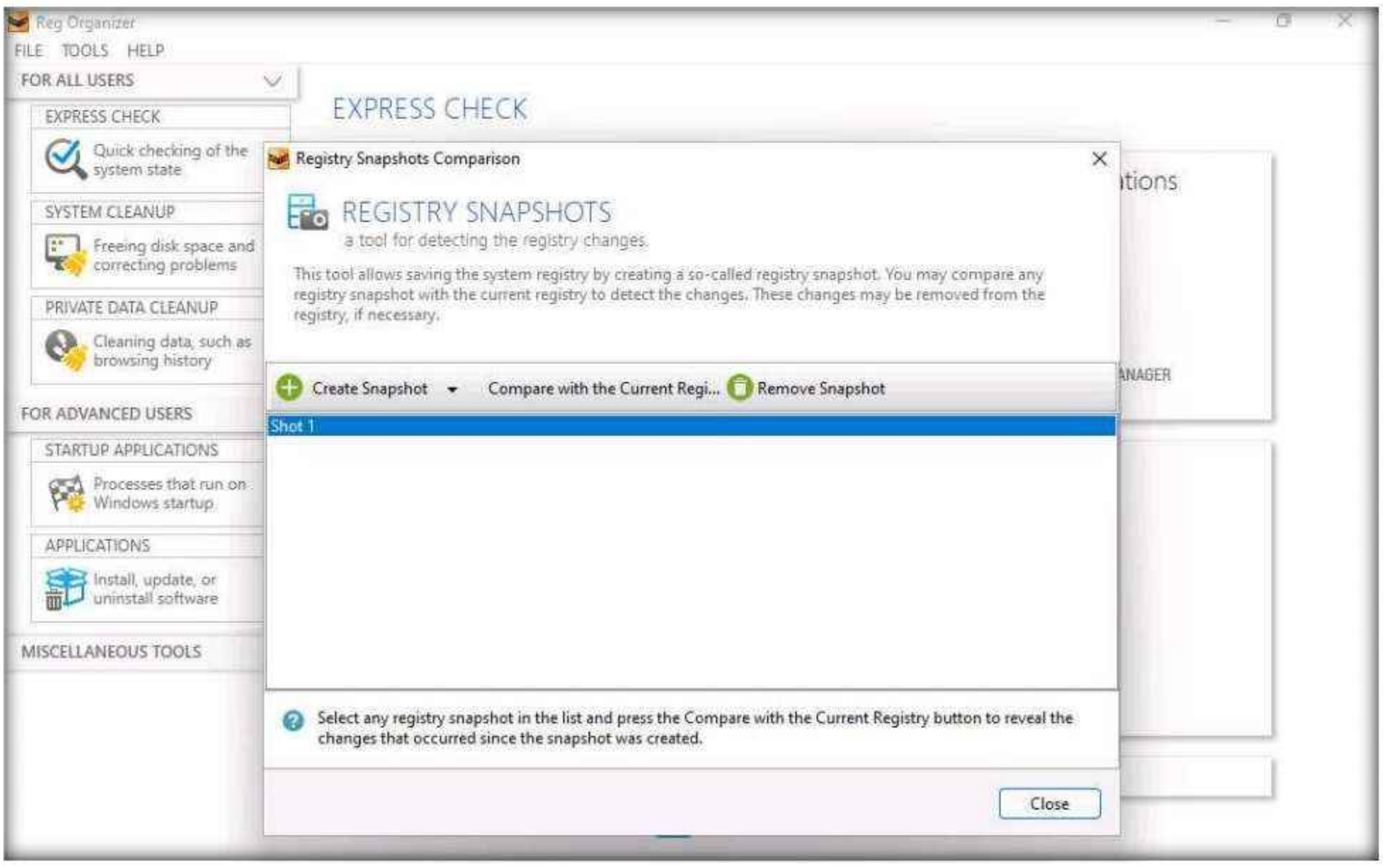
10. **Registry Snapshots Comparison** window appears, click **Create Snapshot** option.



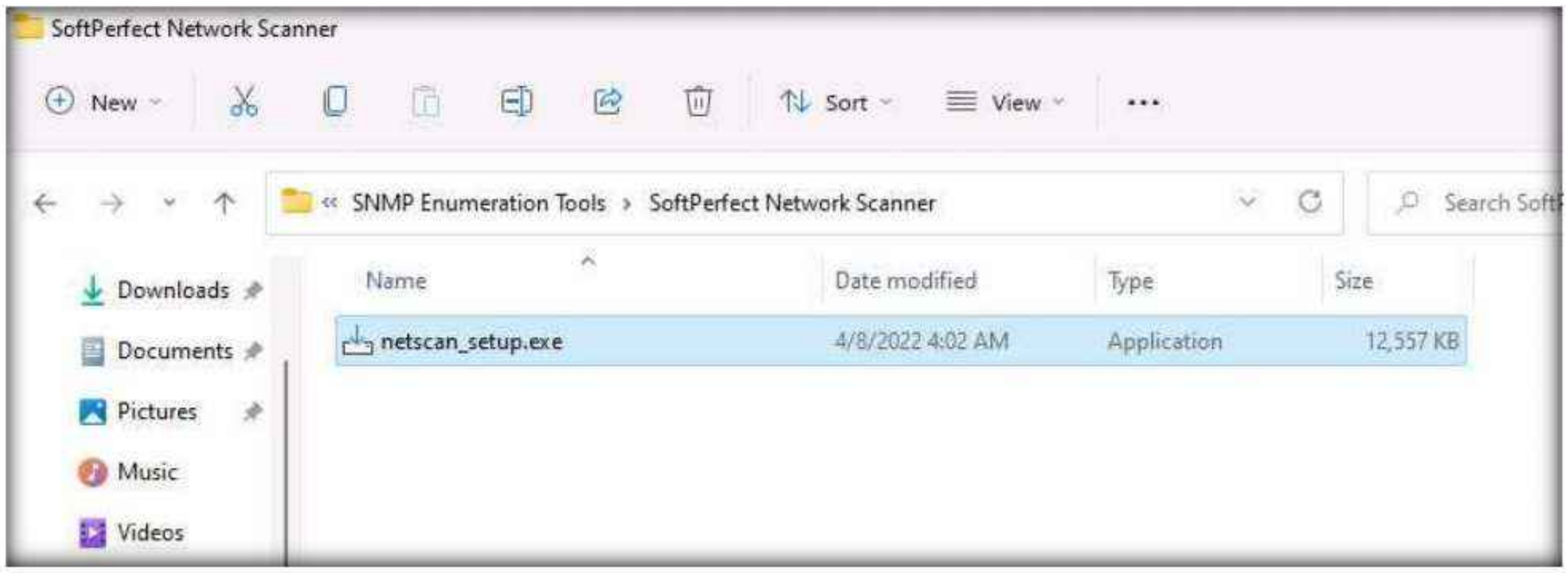
11. The process of taking a snapshot initializes and after it finishes, the **Snapshot Created** window appears; change the snapshot name to **Shot 1** in the **Enter the snapshot name** field and click **OK**.



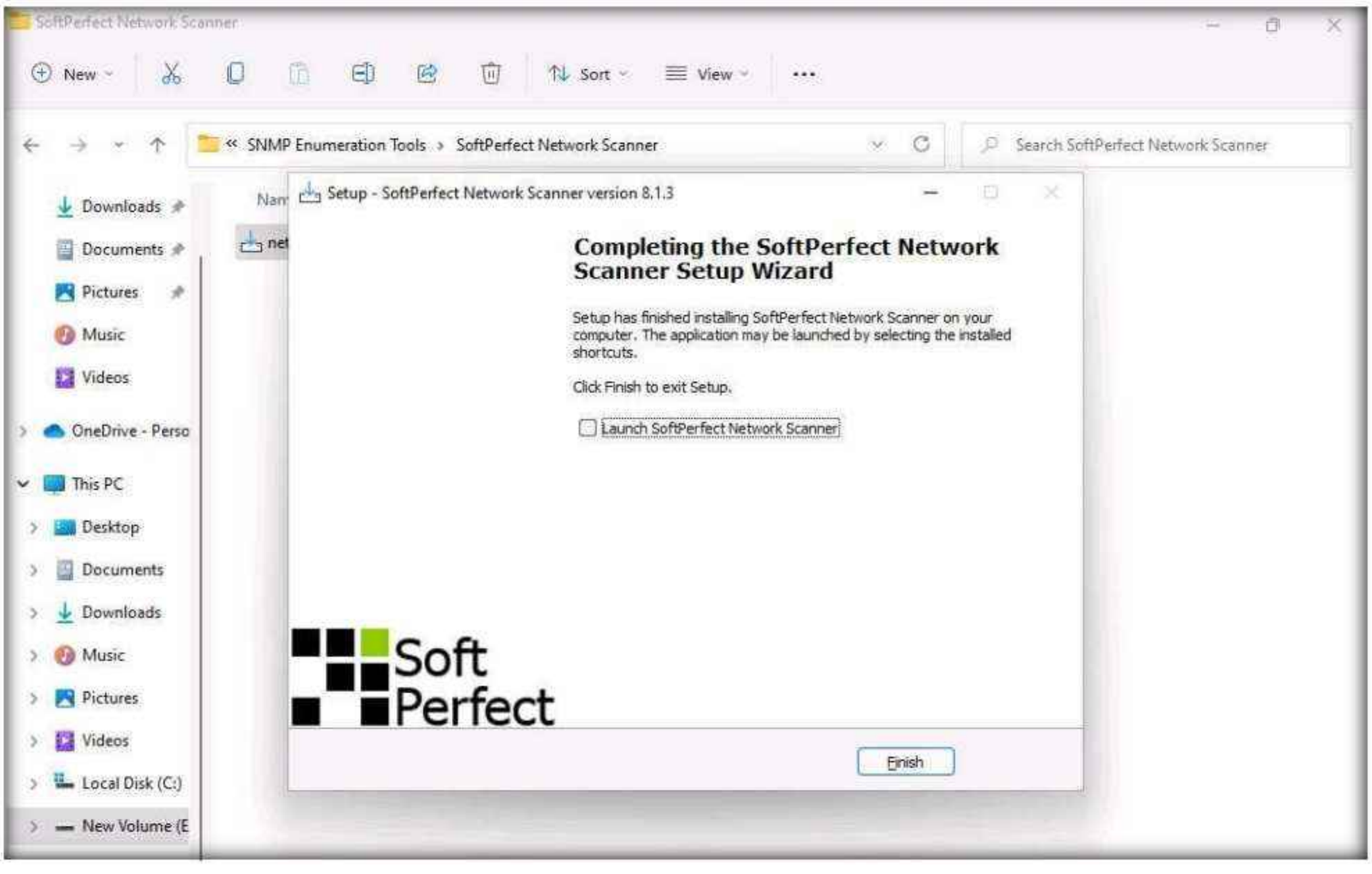
12. **Shot 1** is created and appears in the middle pane, as shown in the screenshot.



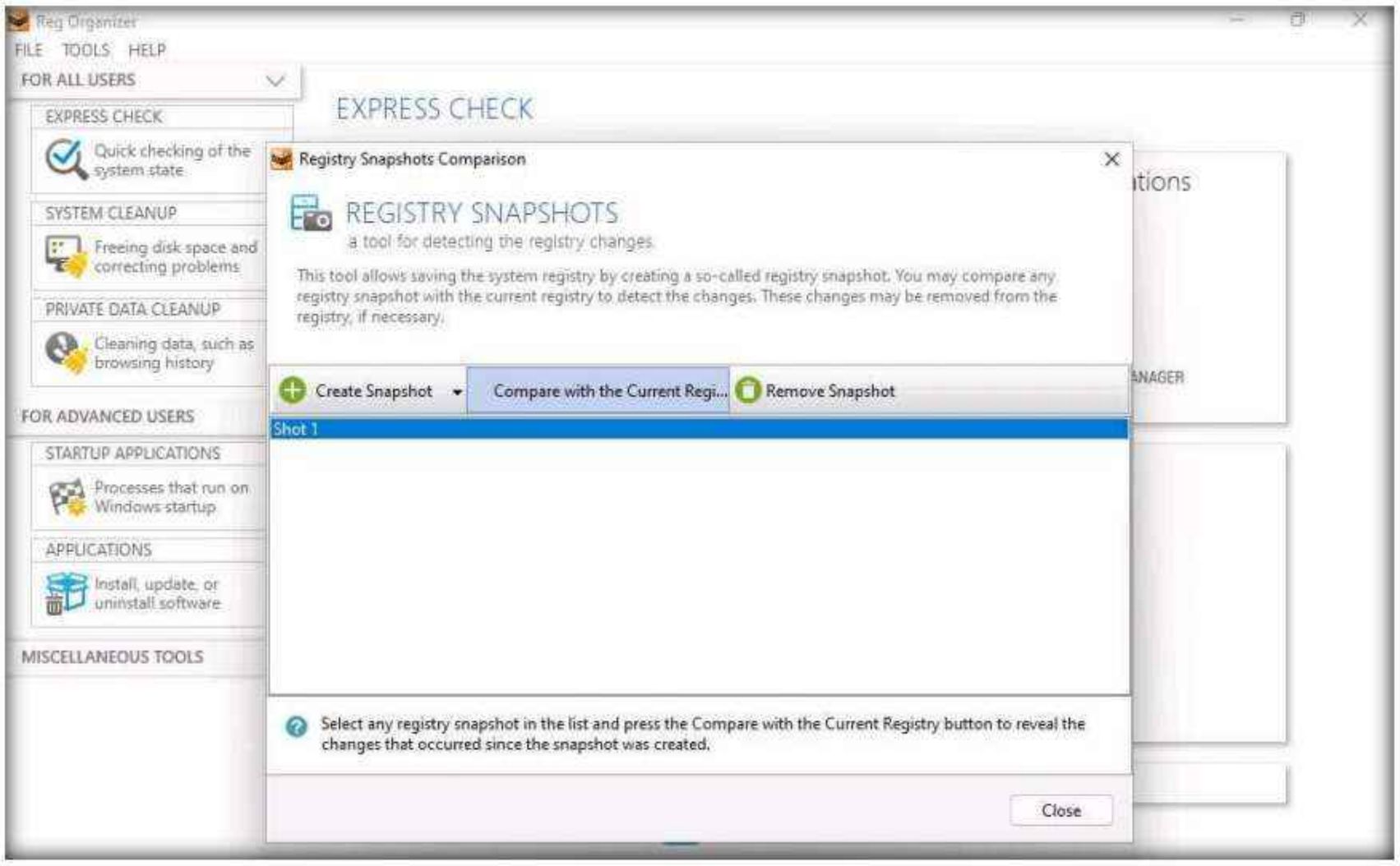
13. To demonstrate a change in the registry, install any application (here, **SoftPerfect Network Scanner**). However, you can install any application of your choice to identify changes in the registry entries.
14. Navigate to **E:\CEH-Tools\CEHv12 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.



15. Follow the wizard-driven installation steps to install the SoftPerfect Network Scanner.
16. Once the installation is complete, uncheck the **Launch SoftPerfect Network Scanner** option and click **Finish**.

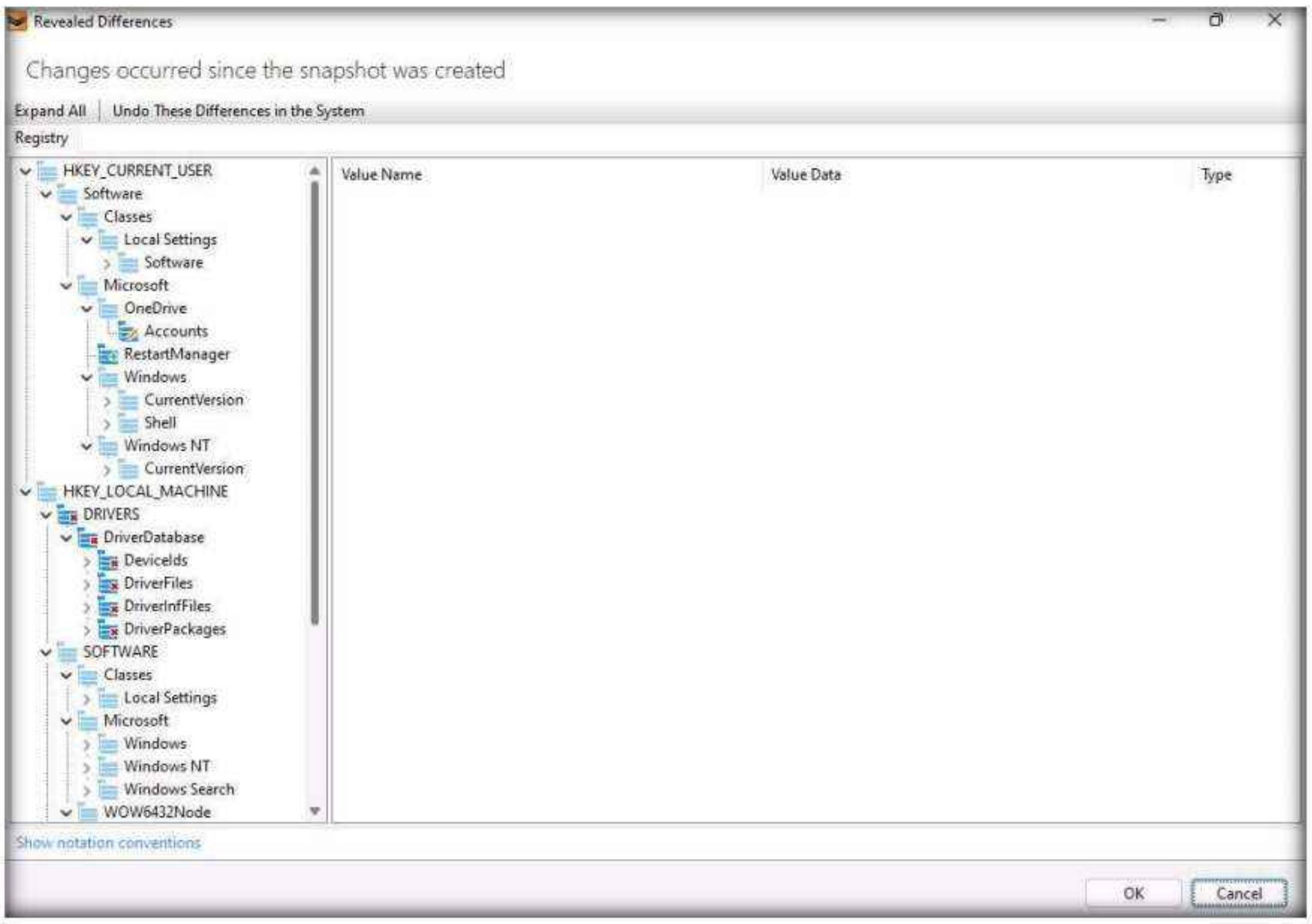


17. Now, click **Compare with Current Registry** option to compare the changes in the registry entries before and after installing SoftPerfect Network Scanner application.

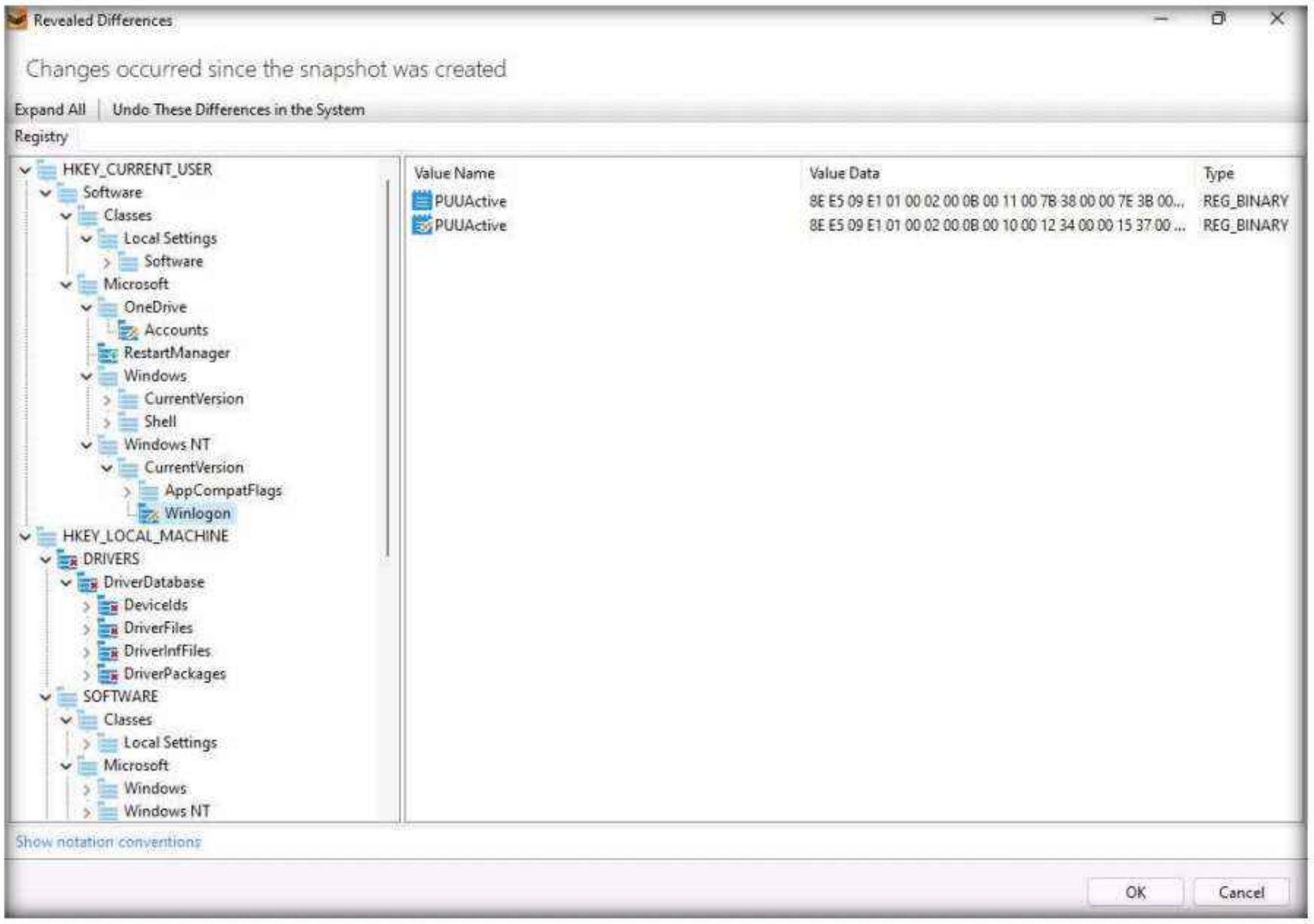


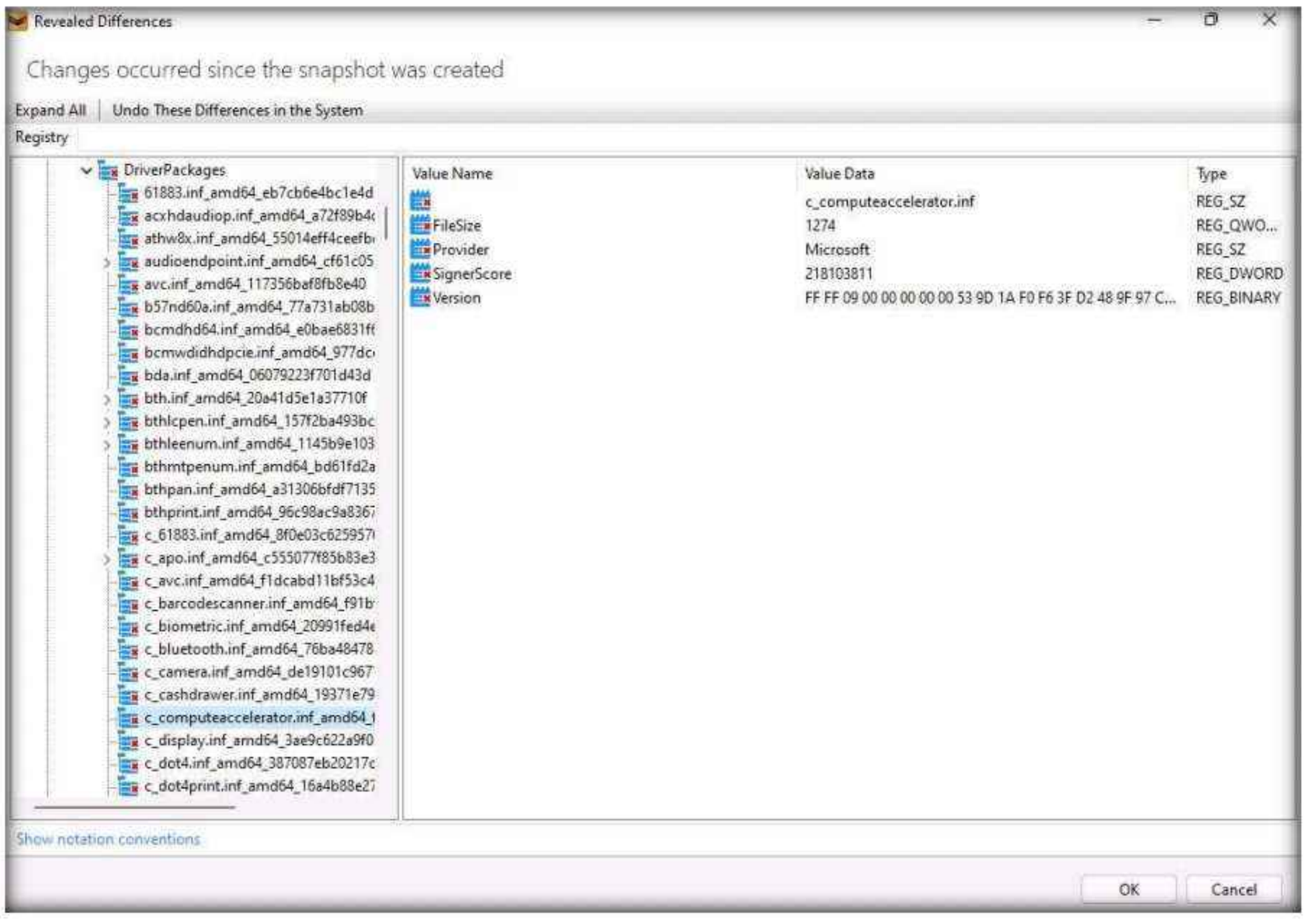
18. **Detecting changes...** process initializes and after it completes **Revealed Differences** window appears, as shown in the screenshot.

Note: The list of registry entries' may vary when you perform this task.



19. You can examine the Registry entries from the left-pane. To do so, expand the nodes, select the entry you want to check and key files appear in the right-pane, as shown in the screenshot.





20. By examining modified registry entries in the result, you can find any unwanted registry entries on the machine and stop or delete them manually.
21. Close all open windows on the **Windows 11** machine.
22. You can also use other registry monitoring tools such as **regshot** (https://sourceforge.net), **Registry Viewer** (https://accessdata.com), **RegScanner** (https://www.nirsoft.net), or **Registrar Registry Manager** (https://www.resplendence.com) to perform registry monitoring.

Task 4: Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

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

These malicious services run as the SYSTEM account or another privileged account, which provides more access compared to regular user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming the malicious services with the names similar to genuine Windows services to avoid detection.

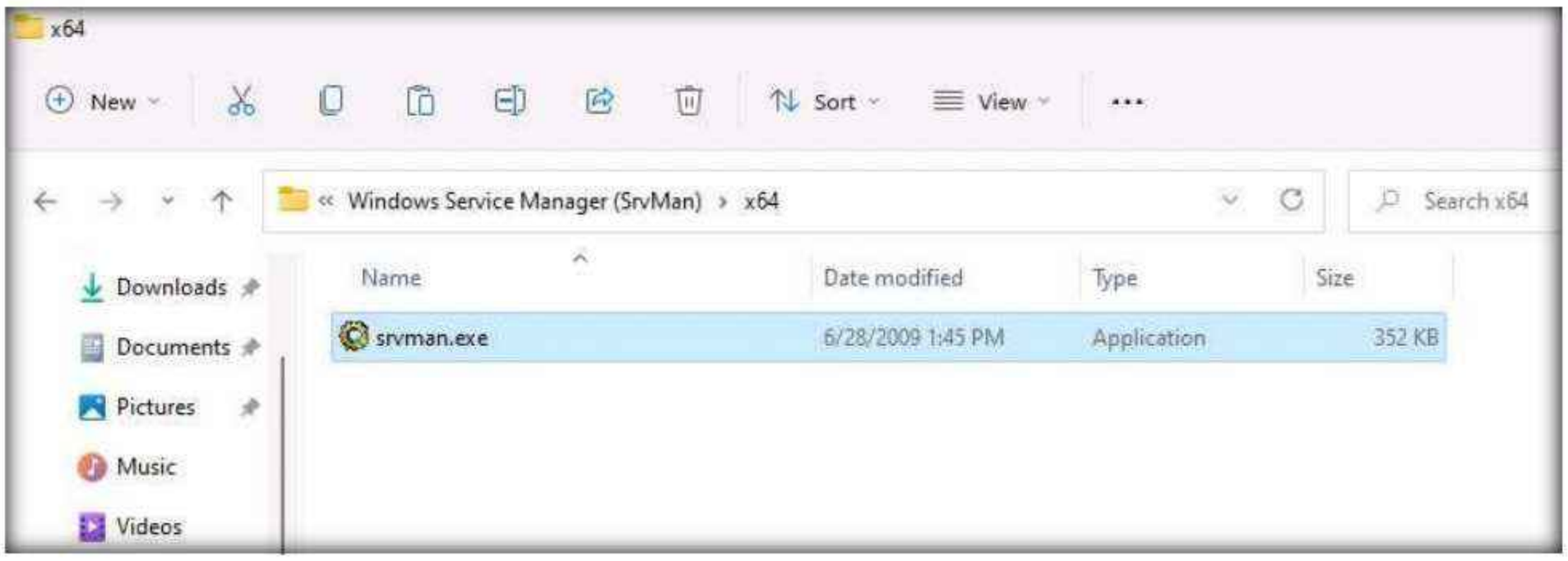
You can trace malicious services initiated by the suspect file during dynamic analysis by using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

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).

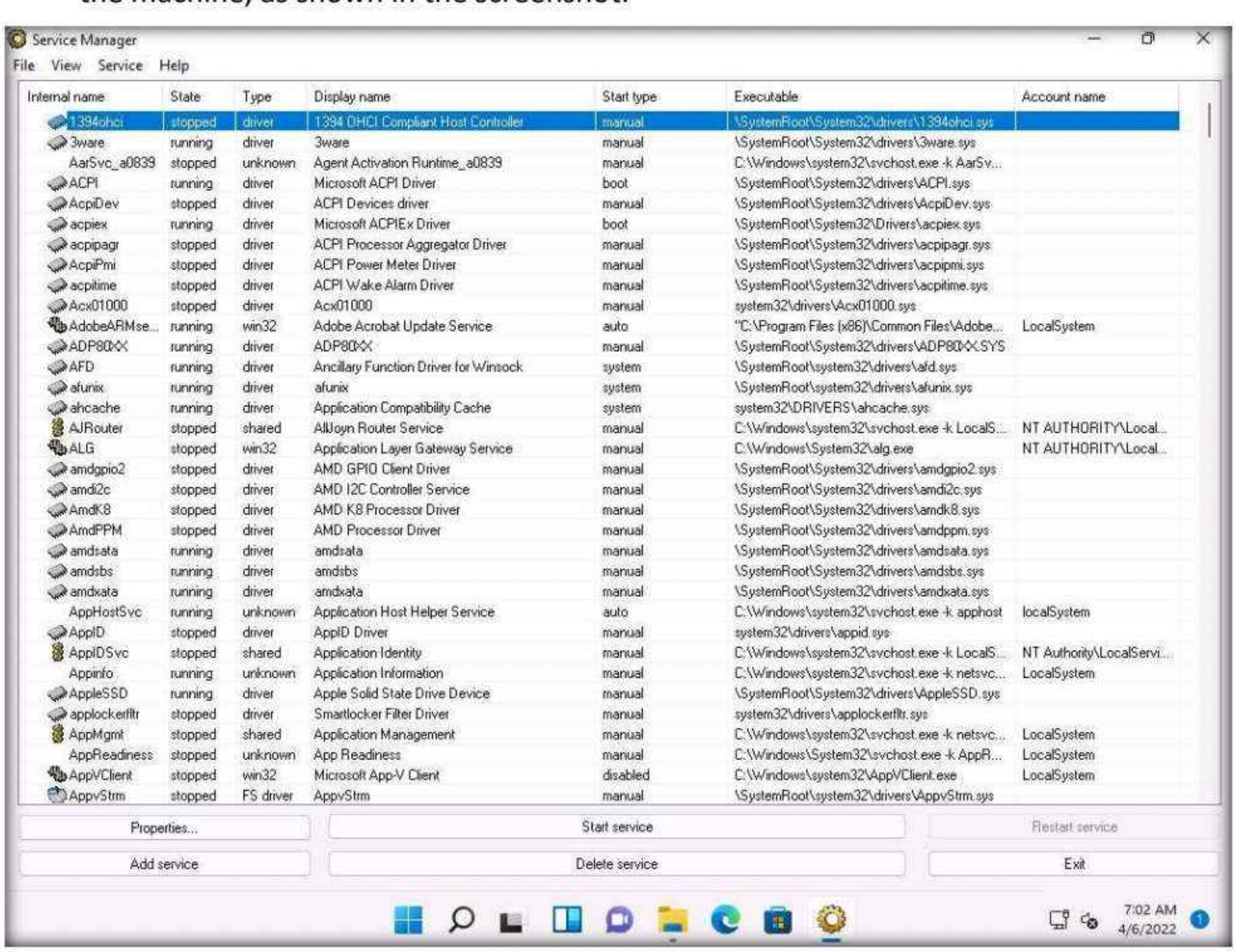
Here, we will use the SrvMan tool to check for suspicious windows services.

1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\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.

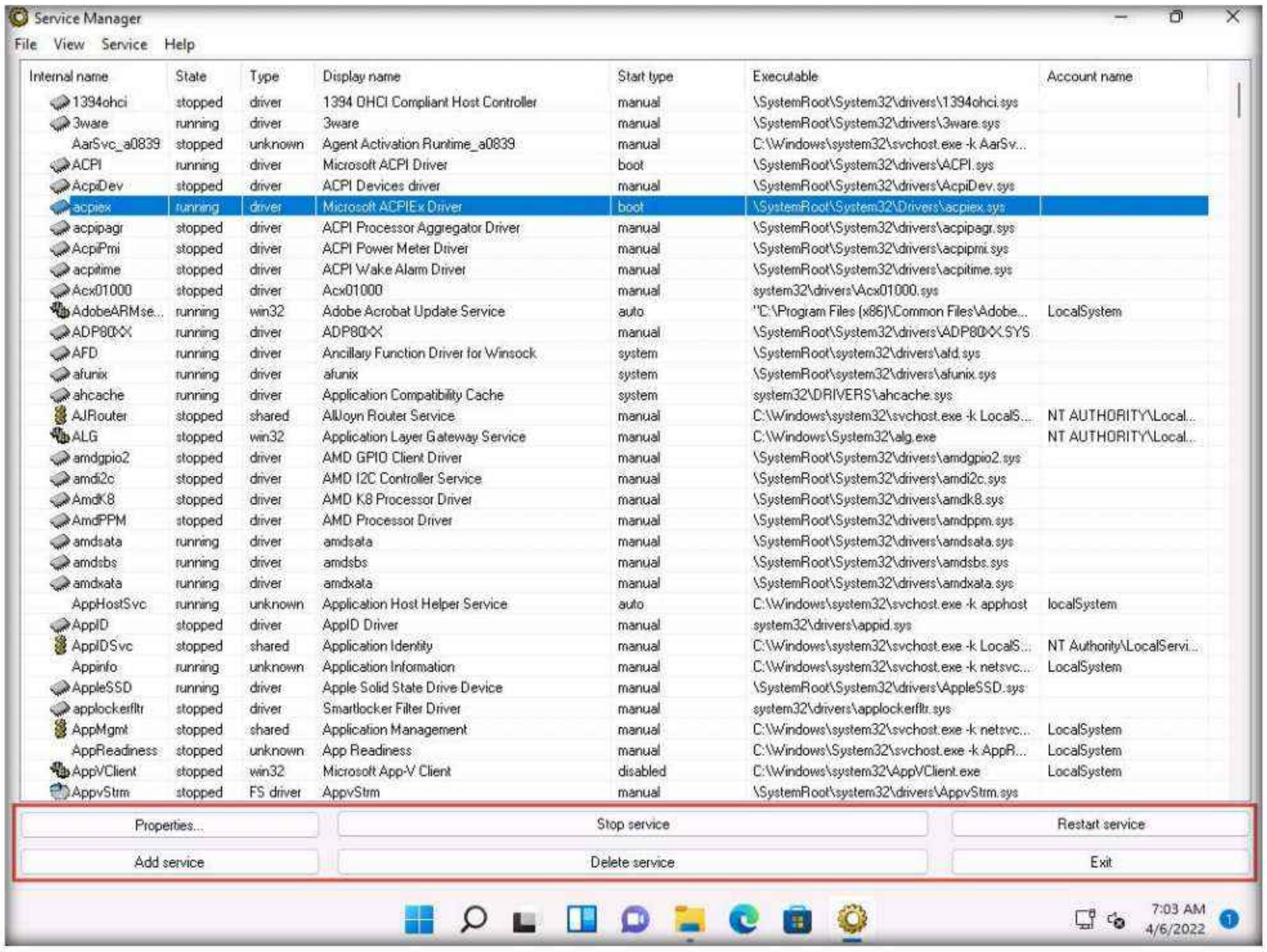


2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.



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.



11. Thus, you can monitor the unwanted services running on the machine using the Windows Service Manager.
12. Close the **Service Manager** window.
13. 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.

Task 5: Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

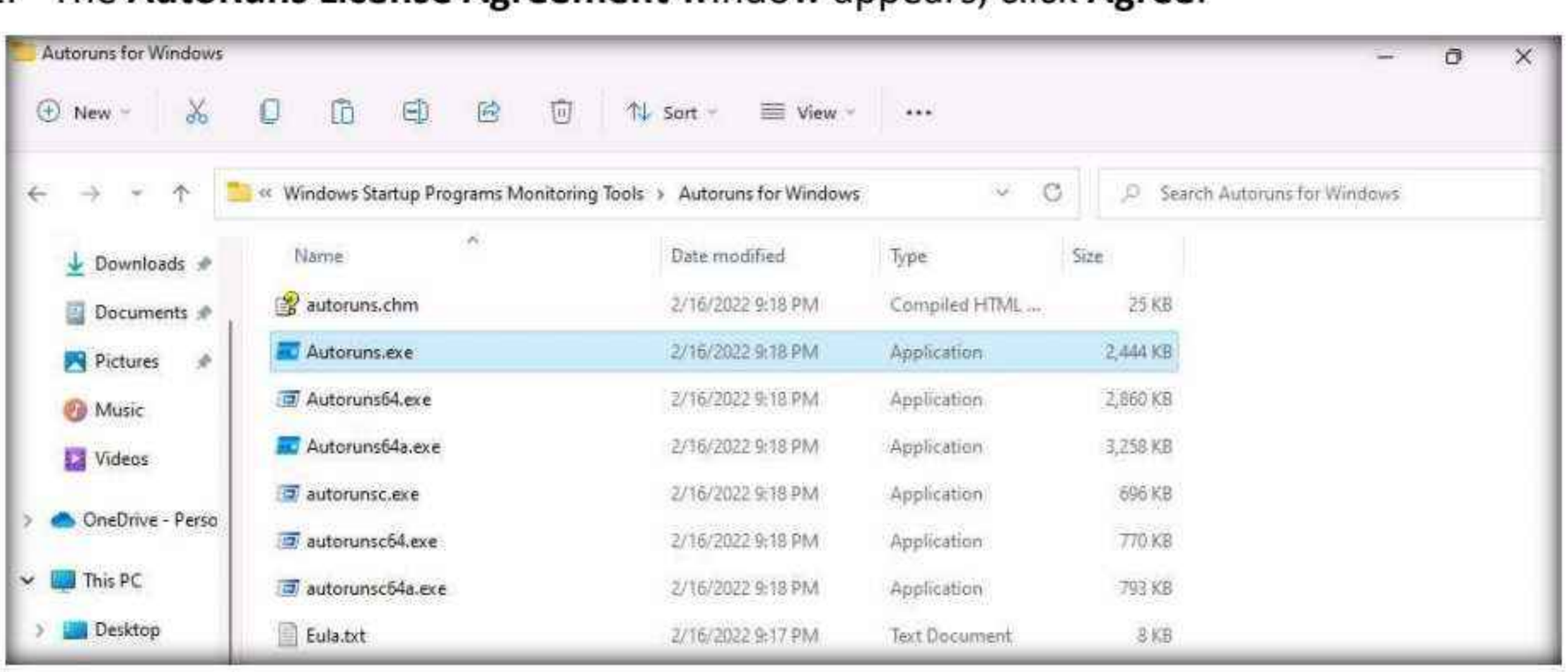
Startup programs are applications or processes that start when your system boots up. Attackers make many malicious programs such as Trojans and worms in such a way that they are executed during startup, and the user is unaware of the malicious program running in the background.

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.

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.

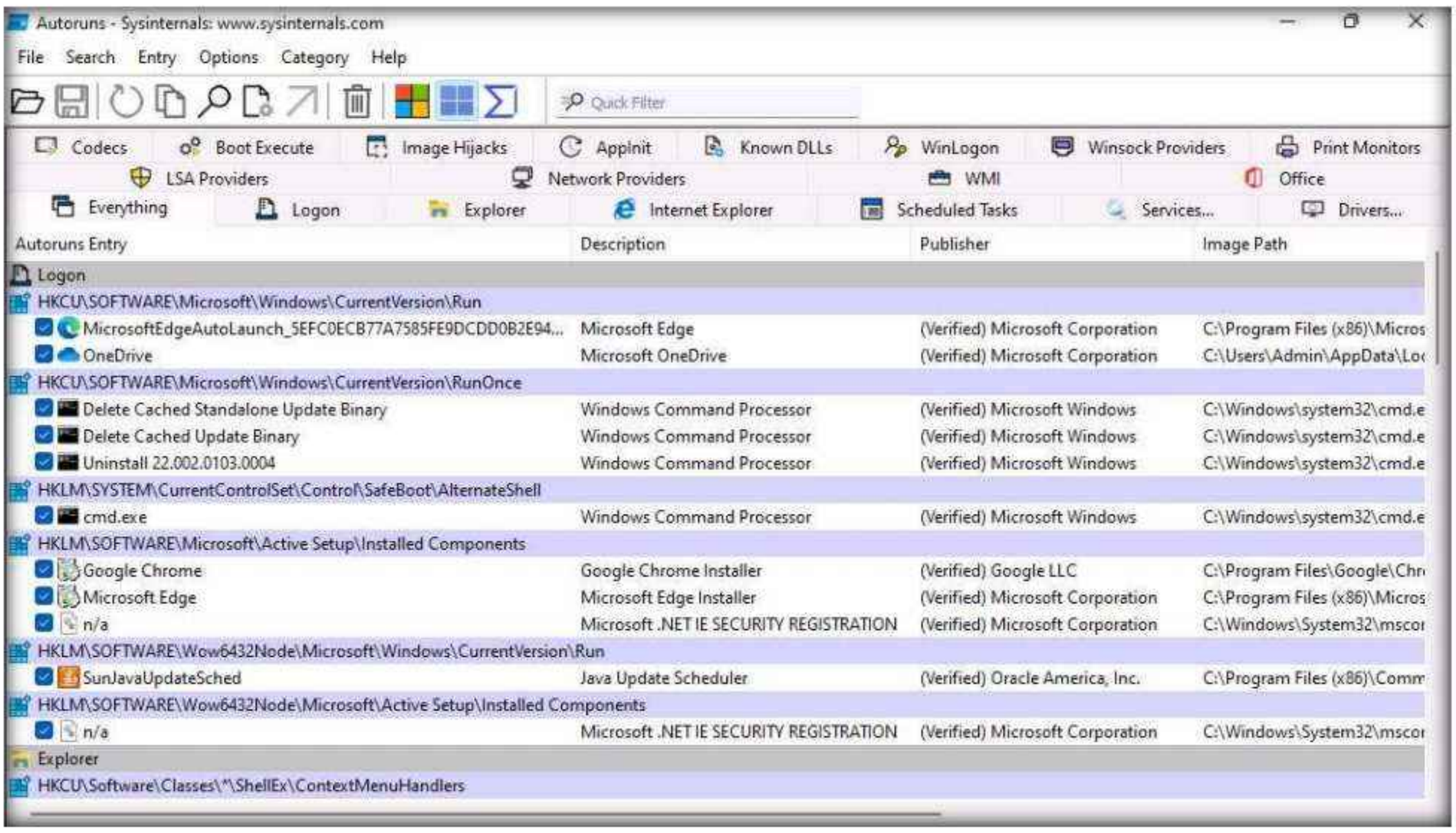
WinPatrol: WinPatrol provides the user with 14 different tabs to help in monitoring the system and its files. This security utility gives the user a chance to look for programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate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

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows** and double-click **Autoruns.exe**.
2. The **AutoRuns License Agreement** window appears; click **Agree**.

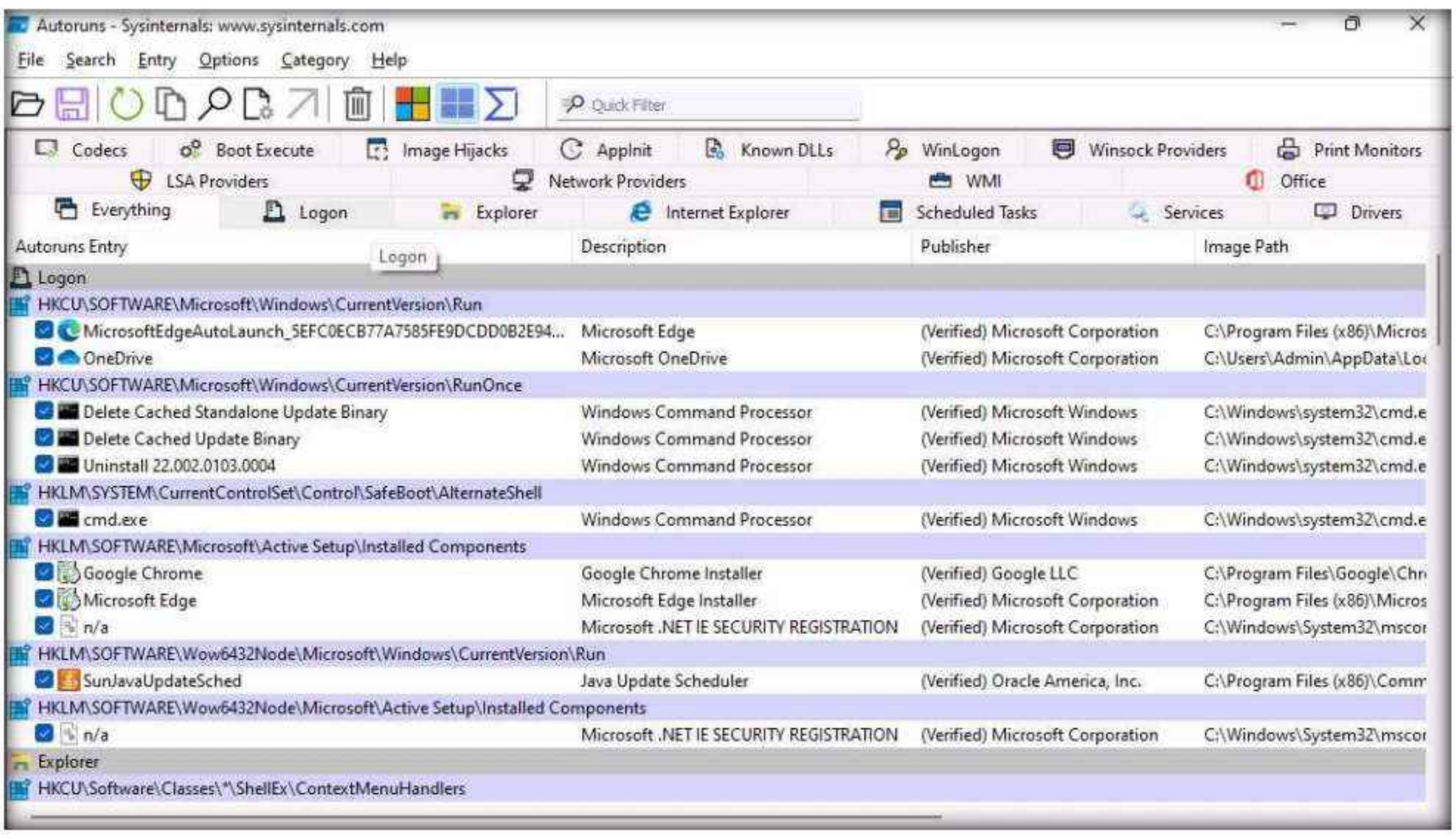


3. The **Autoruns** main window appears. It displays all **processes**, **dll's**, and **services**, as shown in the screenshot.

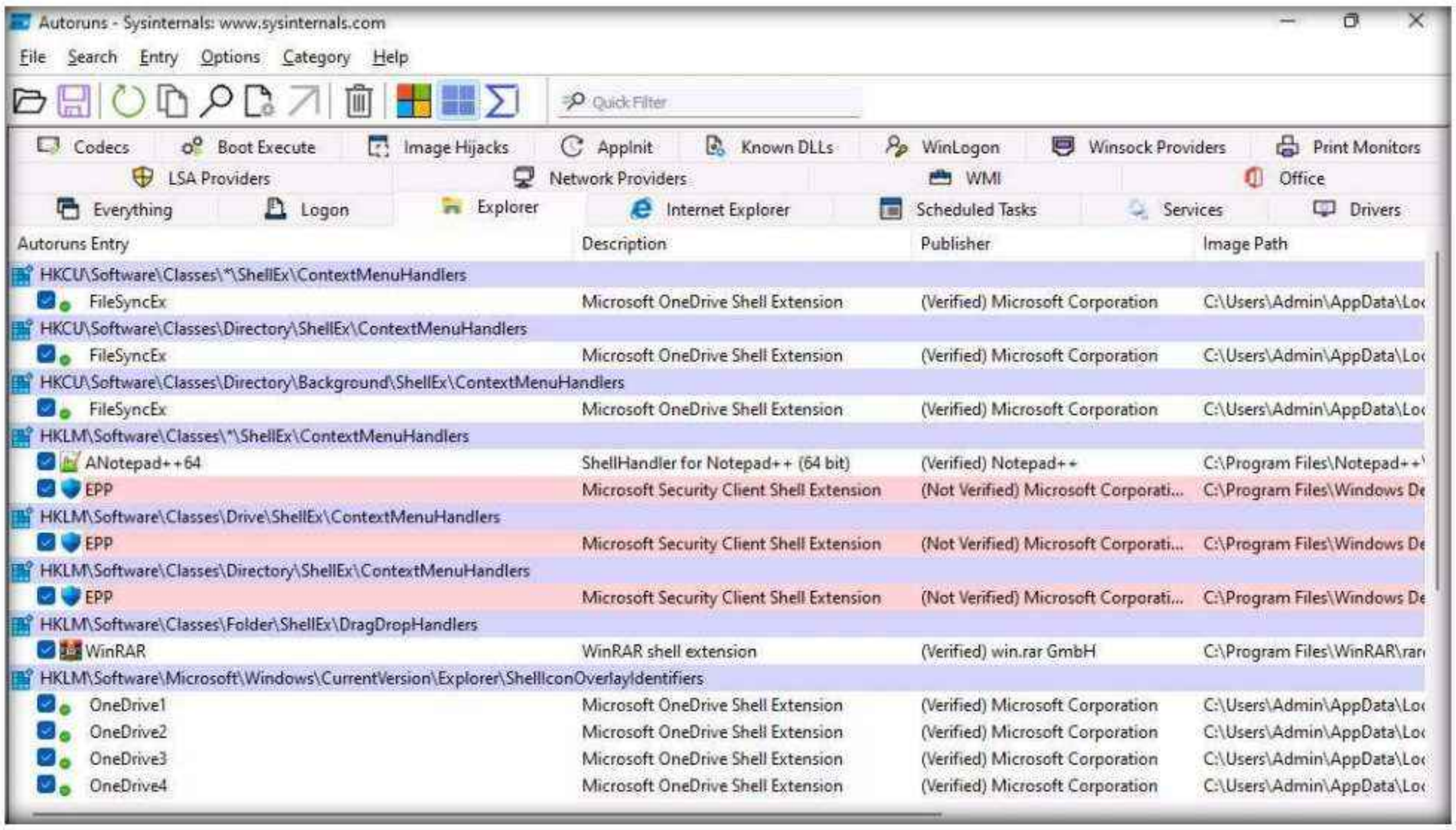
   Note: The application lists displayed under all the tabs may vary when you perform this task.



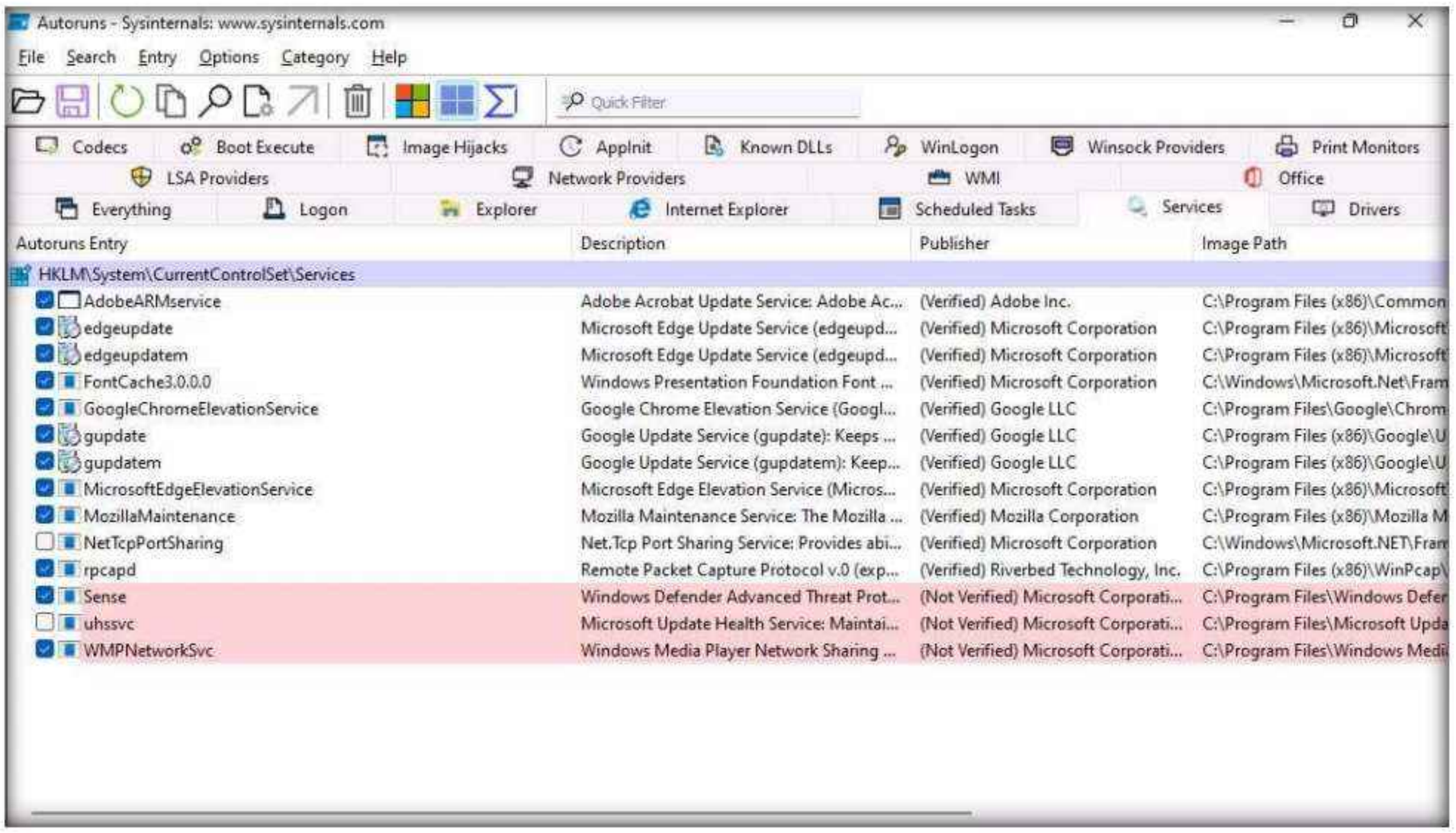
4. Click the **Logon** tab to view the applications that run automatically during login.



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

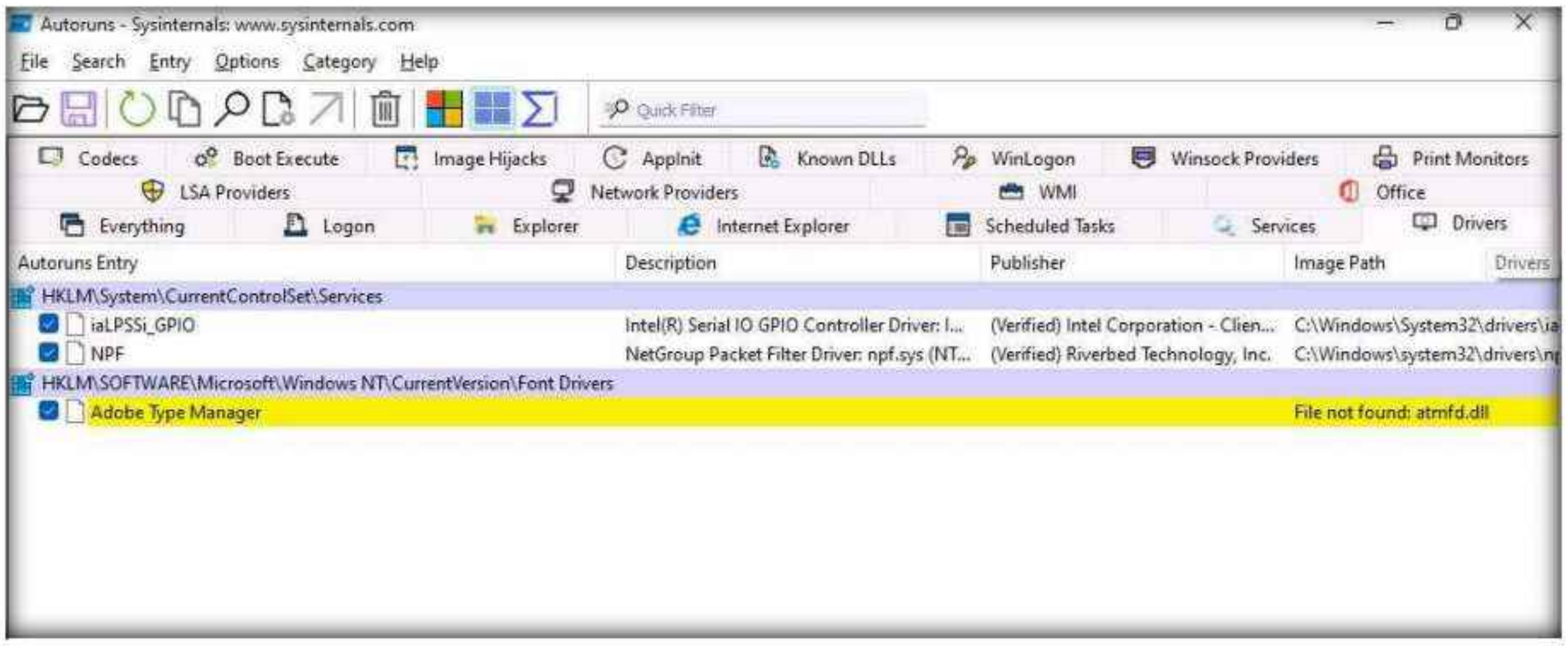


6. Clicking the **Services** tab displays all services that run automatically at system startup.



7. Click the **Drivers** tab to view all application drivers that run automatically at system startup.

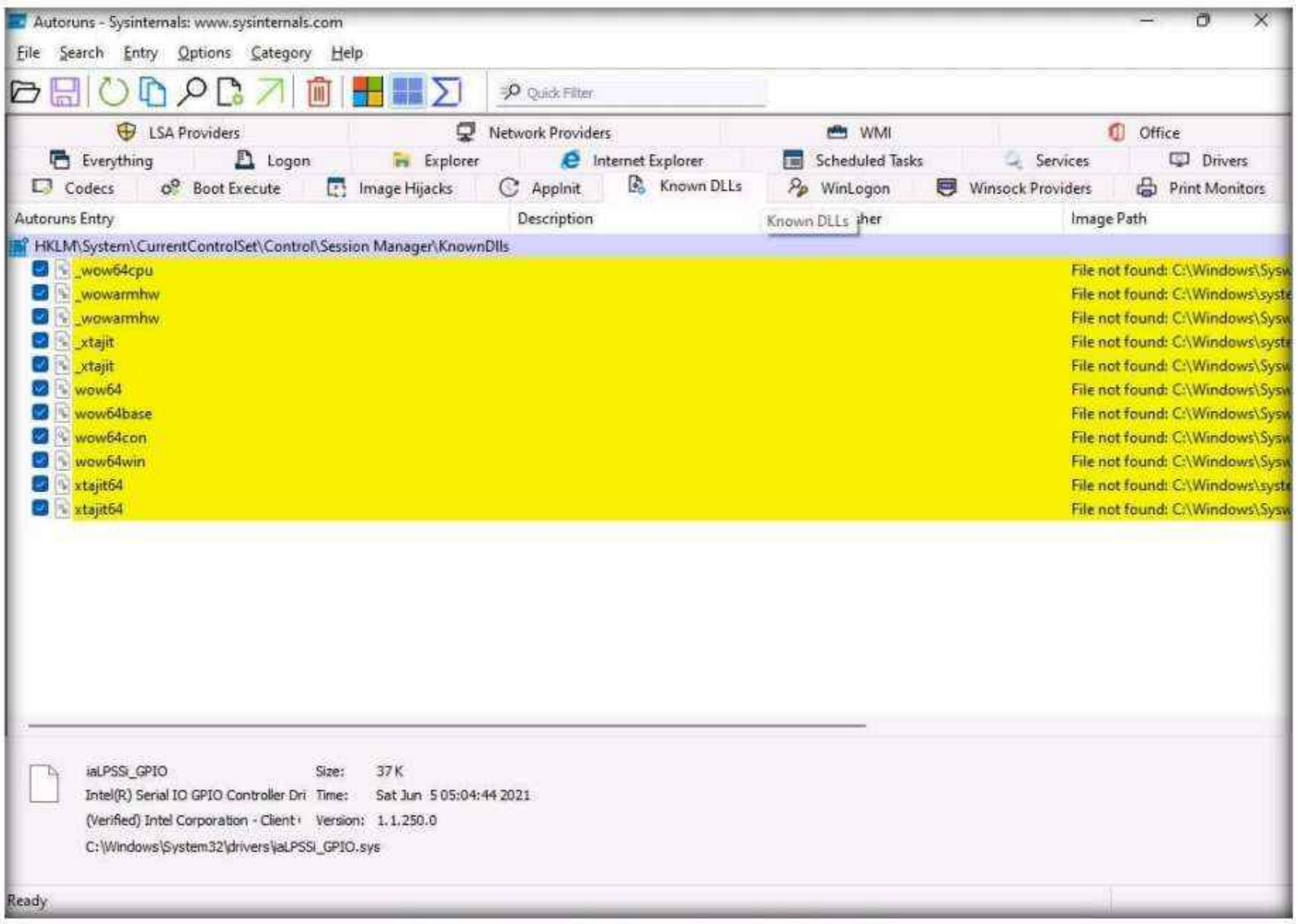
   Note: The list displayed under this tab may vary when you perform this task.



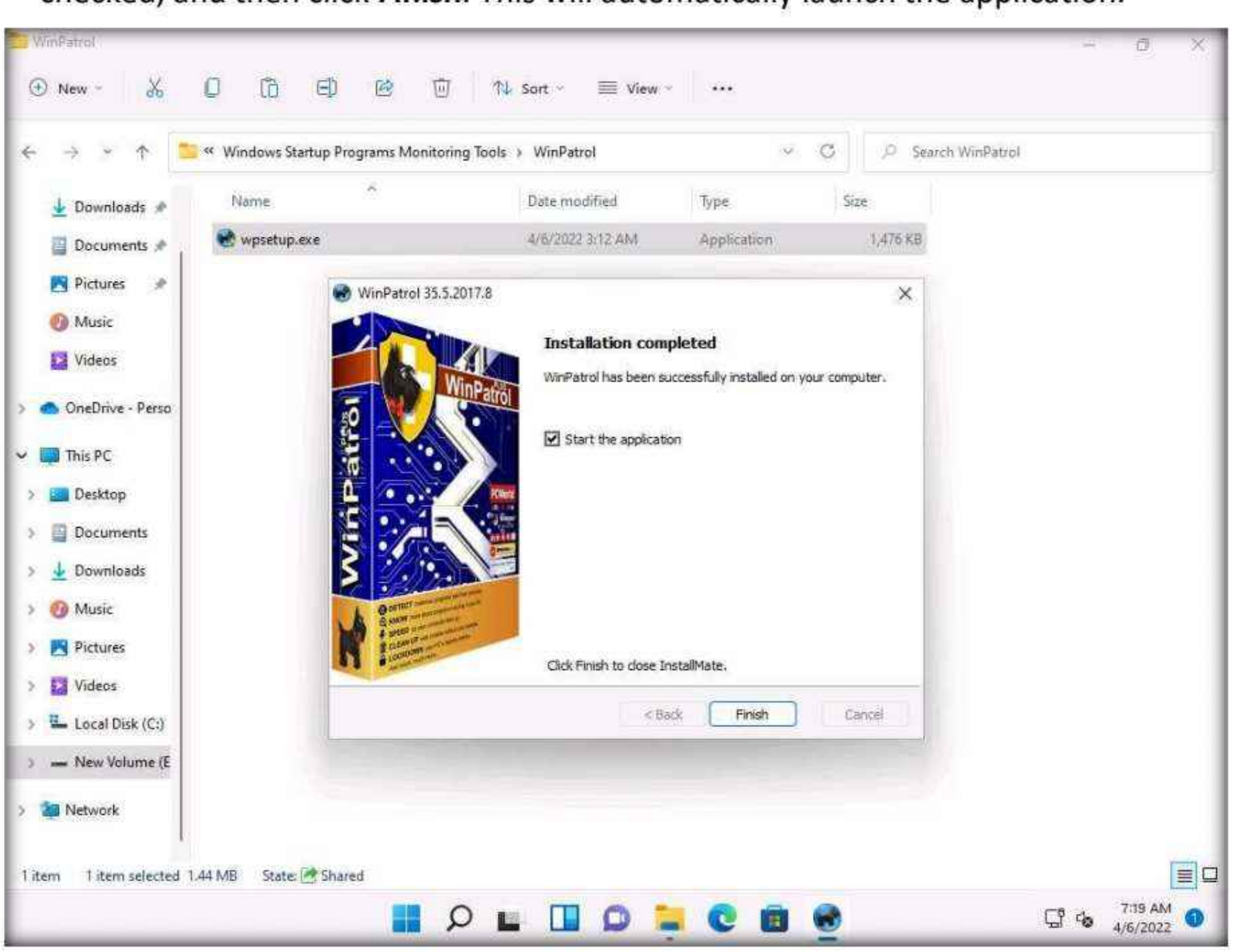
8. You can click on any driver to display its size, version, and the time at which it was automatically run at system startup (for the first time).

   Note: The list displayed under this tab may vary when you perform this task.

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

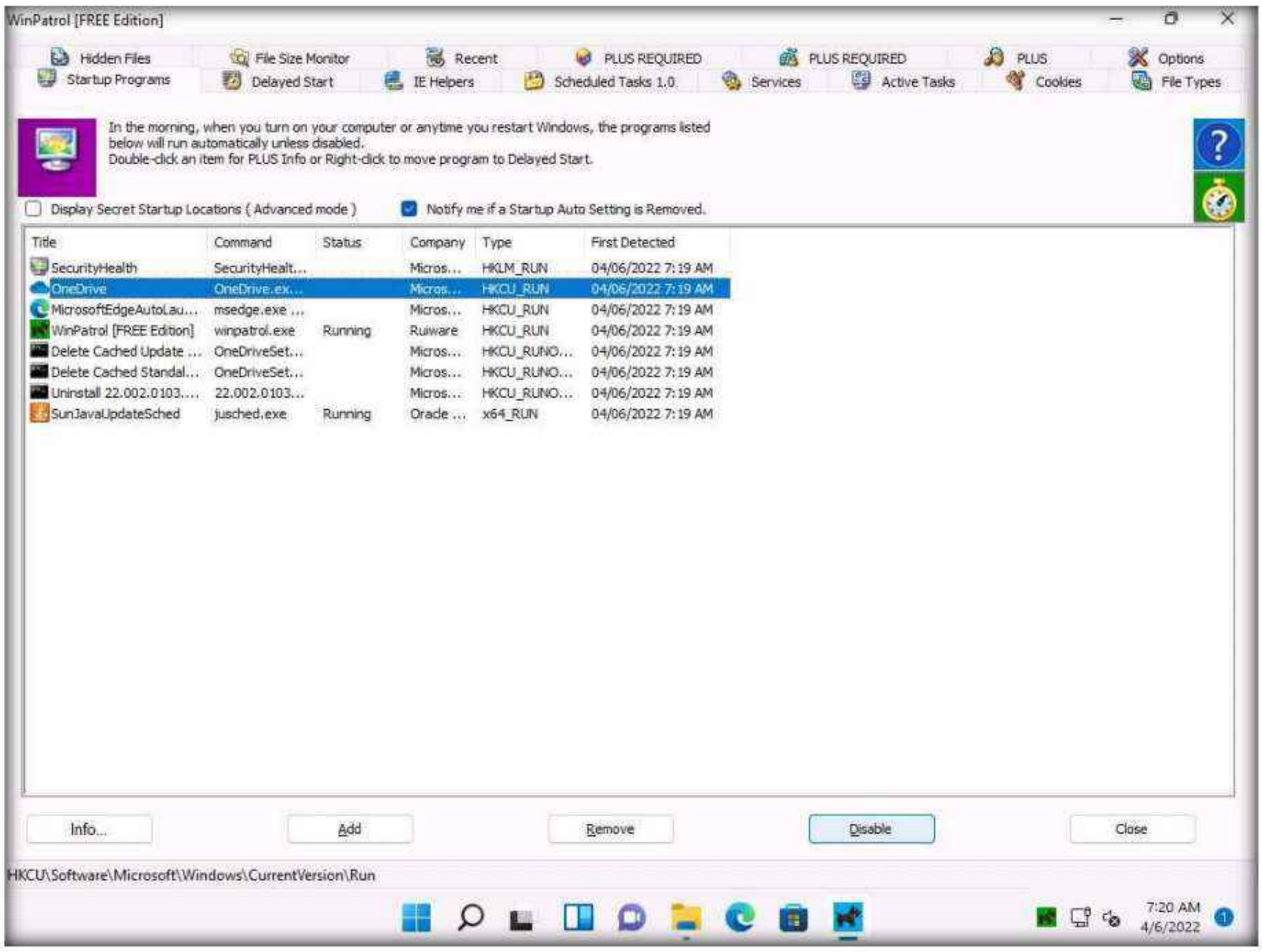


10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.
12. Now, we will find out which applications or processes start when the system boots up using the WinPatrol tool.
13. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 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.



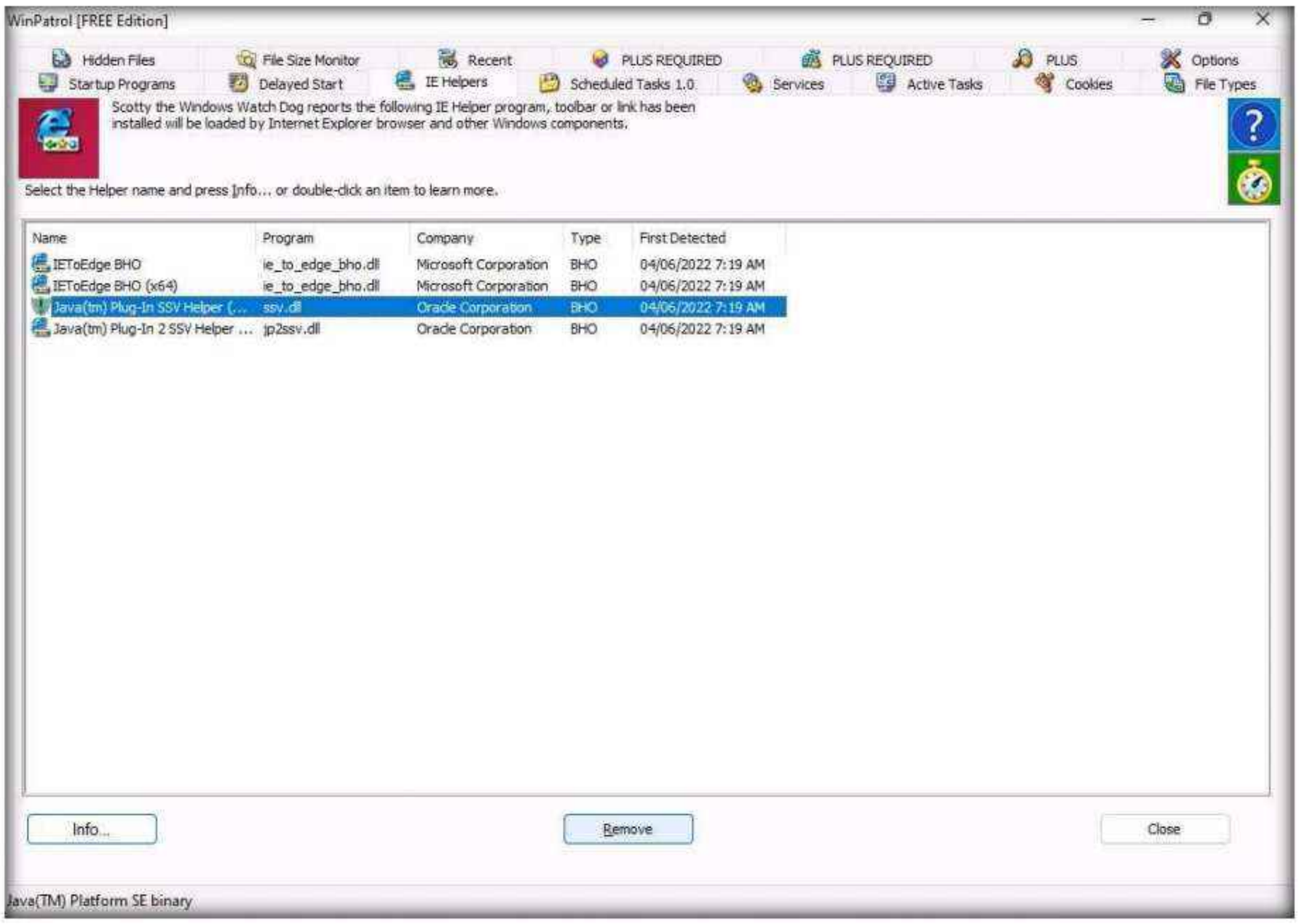
17. The WinPartol application window appears with the **PLUS** tab open by default. Click the **Startup Programs** tab.
18. Select any program that affects your system bootup (here, **OneDrive**) and click **Disable**, as shown in the screenshot.

    Note: The screenshot may differ when you perform this task.

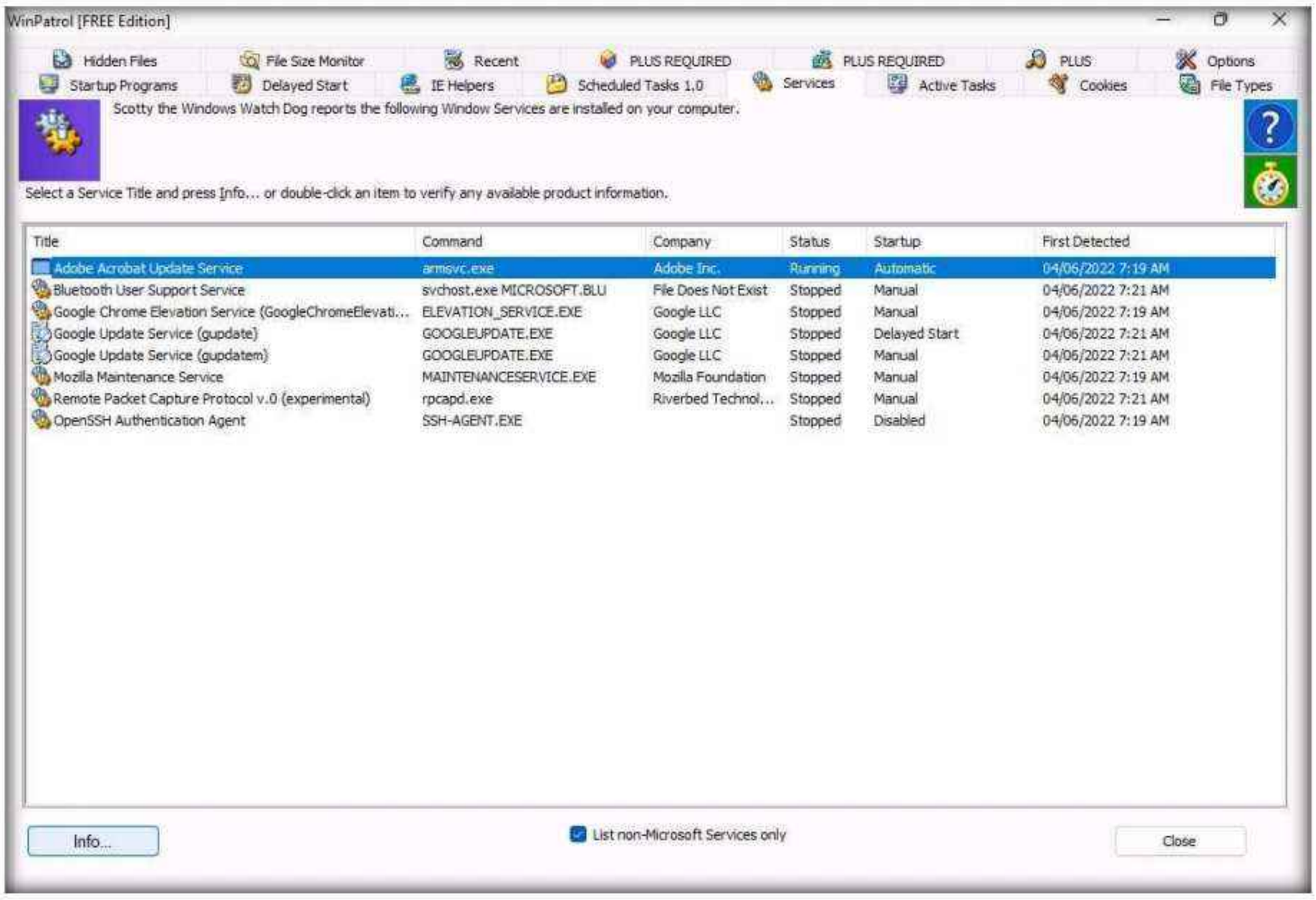


19. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.
20. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here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

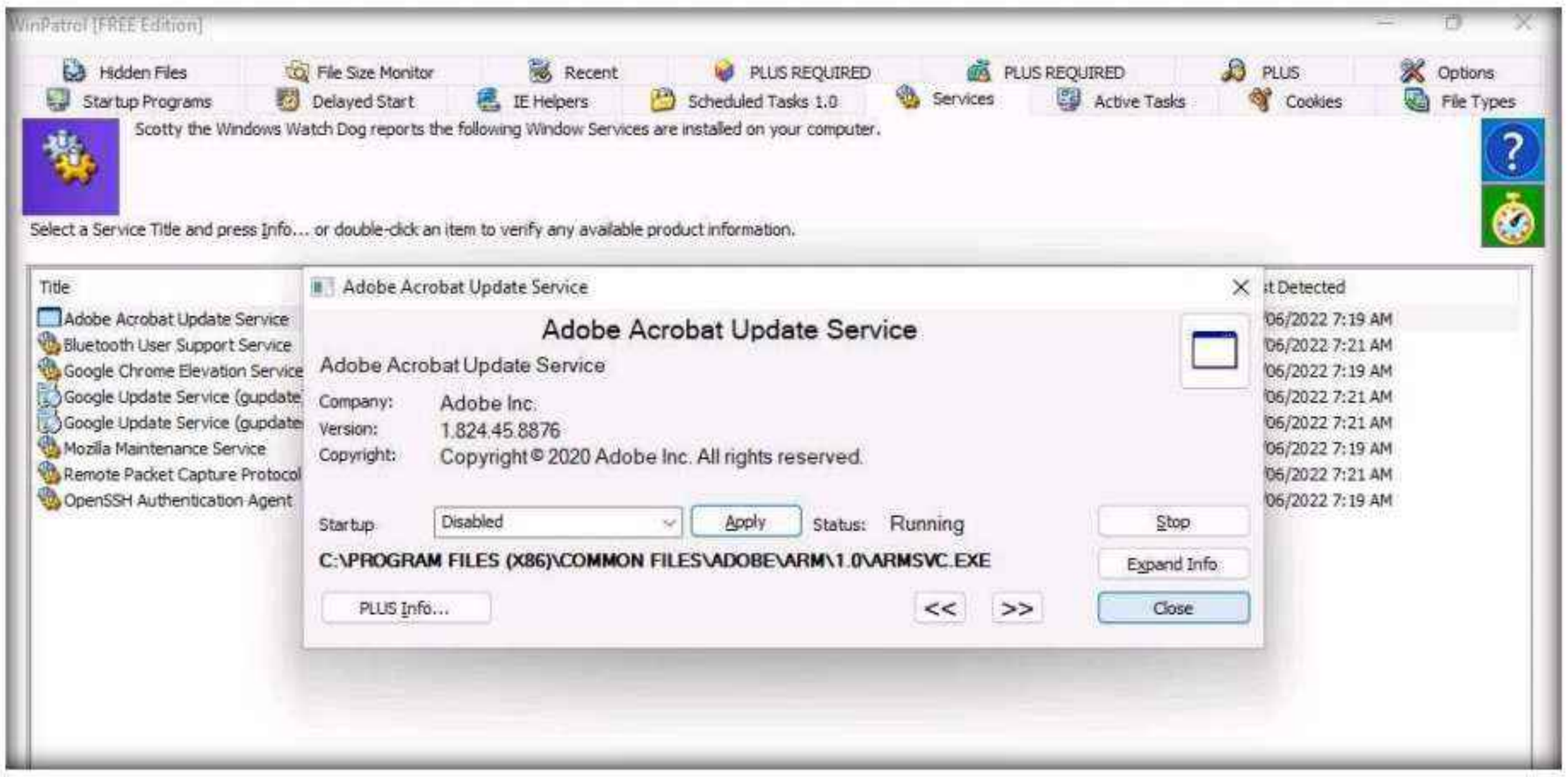
    Note: If a pop-up appears, as shown in the screenshot. Click **Yes** to proceed.



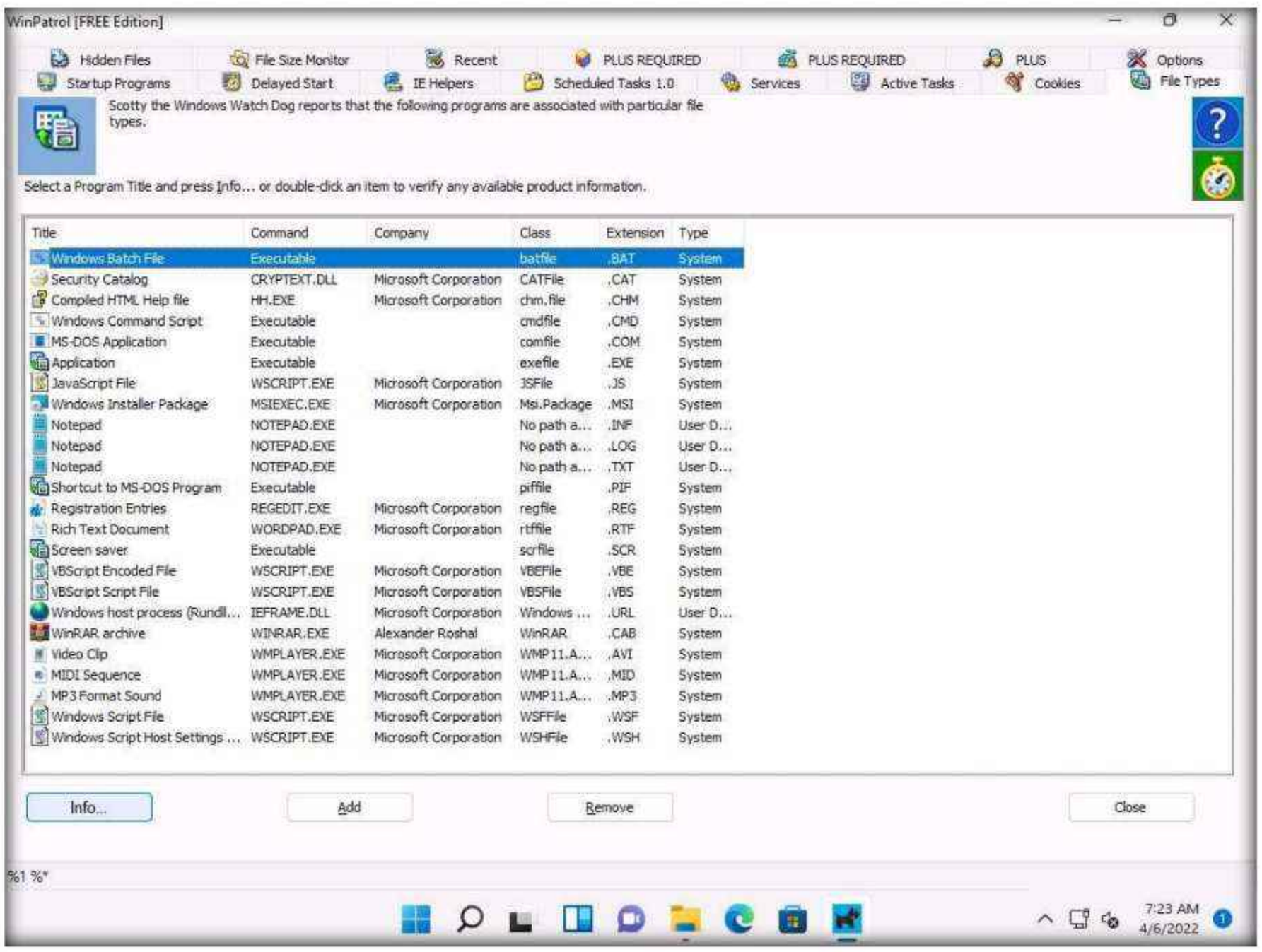
21. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info…**, as shown in the screenshot.



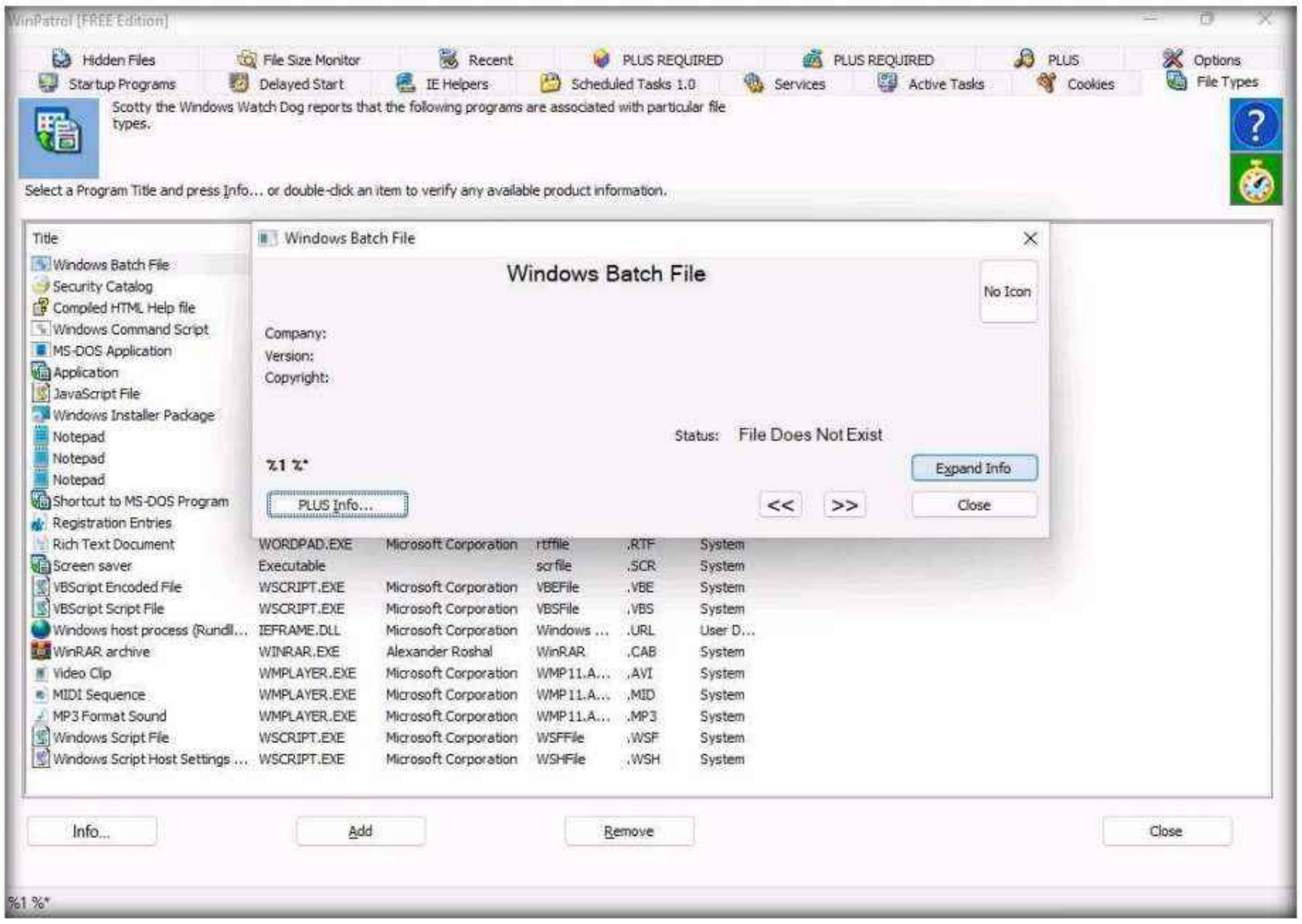
22. A window showing the service information appears. To disable a service, select **Disabled** from the drop-down list and click **Apply**, as shown in the screenshot. Click **Close** to exit the window.



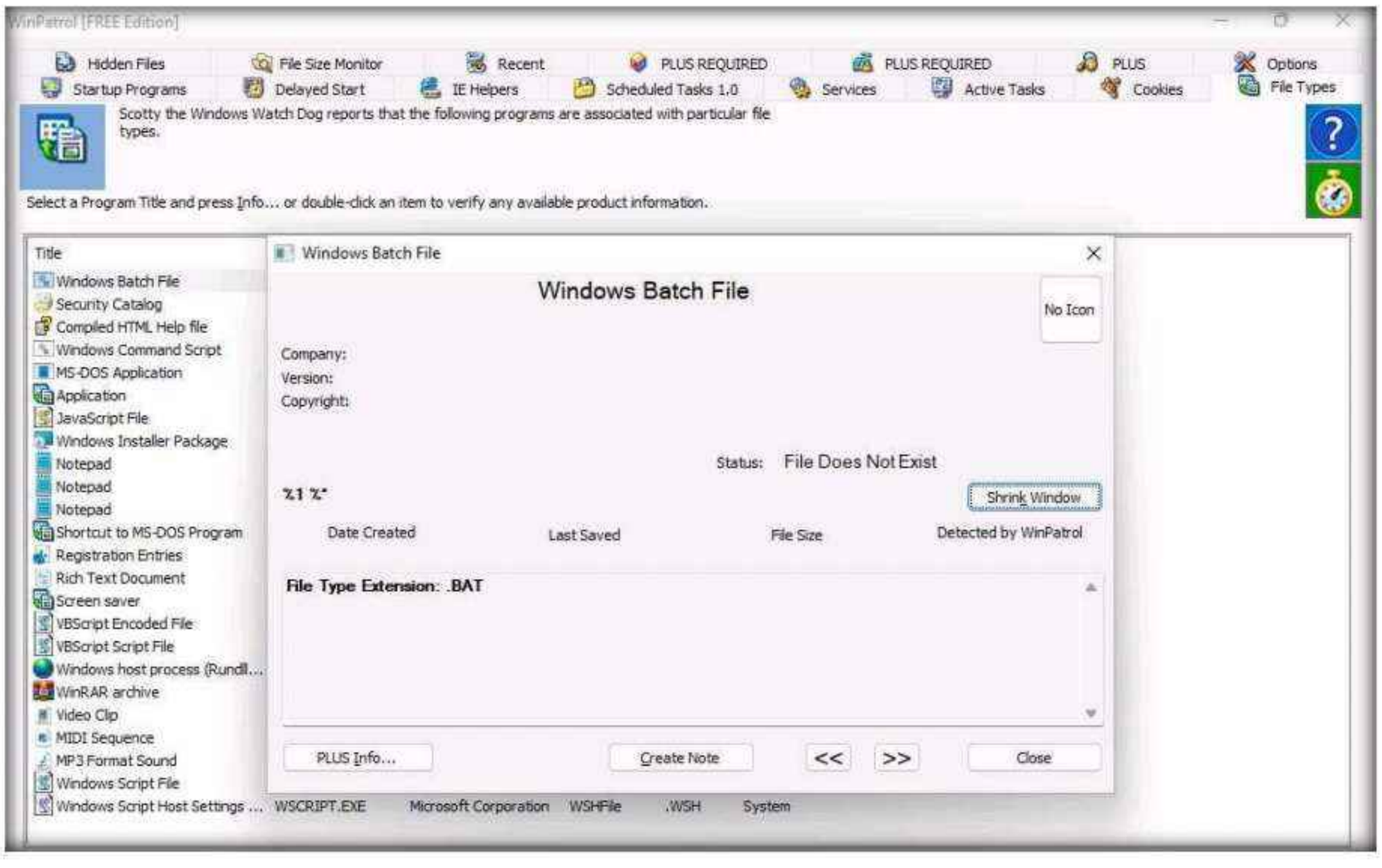
23. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info...** to view the available information.



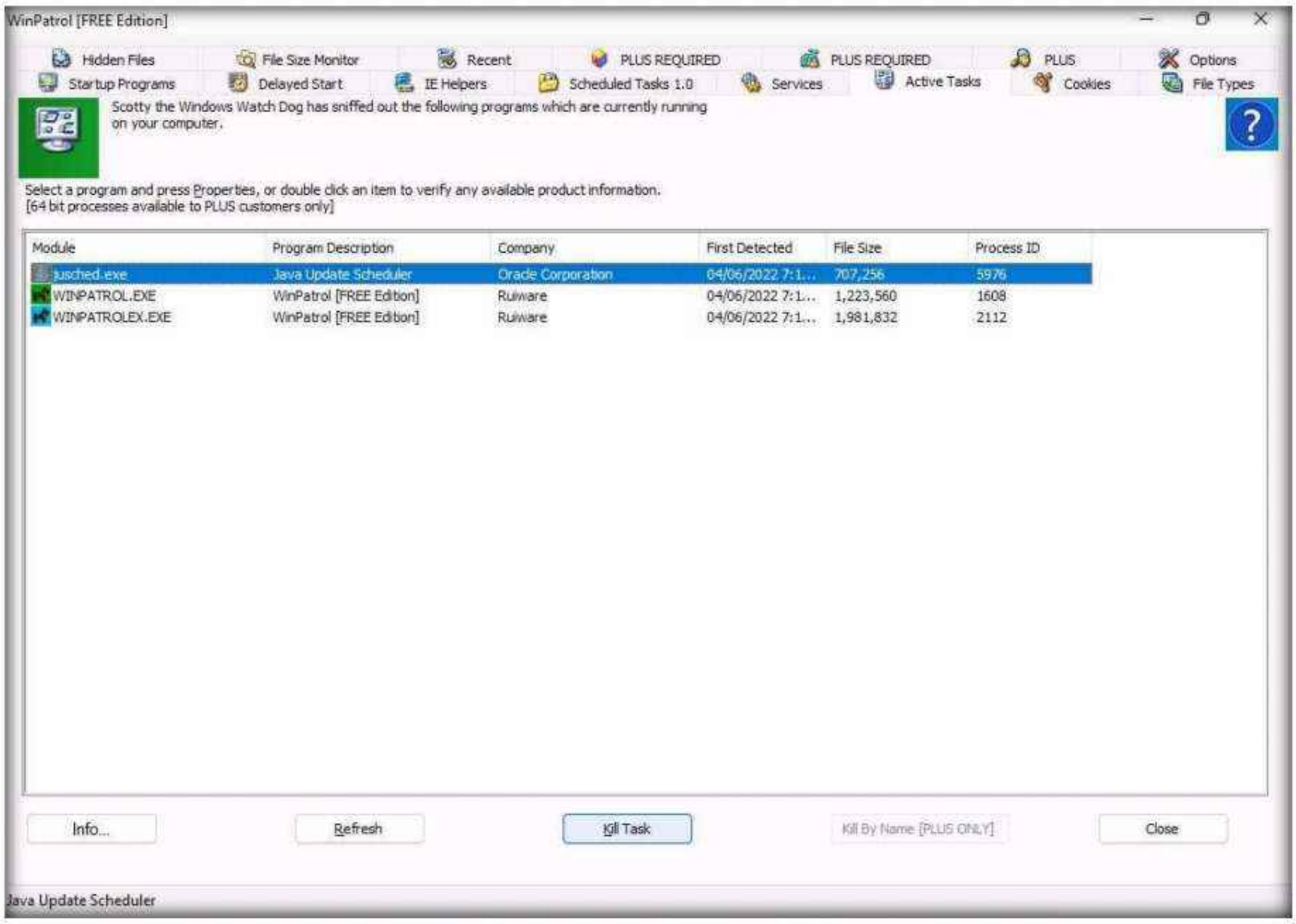
24. The **Windows Batch File** window appears, as shown in the screenshot. Click **Expand Info** to view the full info about the program.



25. 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.



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



27. 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.
28. Close all open windows on the **Windows 11** machine.
29. You can also use other Windows startup programs monitoring tools such as **Autorun Organizer** (https://www.chemtable.com), **Quick Startup** (https://www.glarysoft.com), or **Chameleon Startup Manager** (https://www.chameleon-managers.com) to perform startup programs monitoring.

Task 6: Perform Installation Monitoring using 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.

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.

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

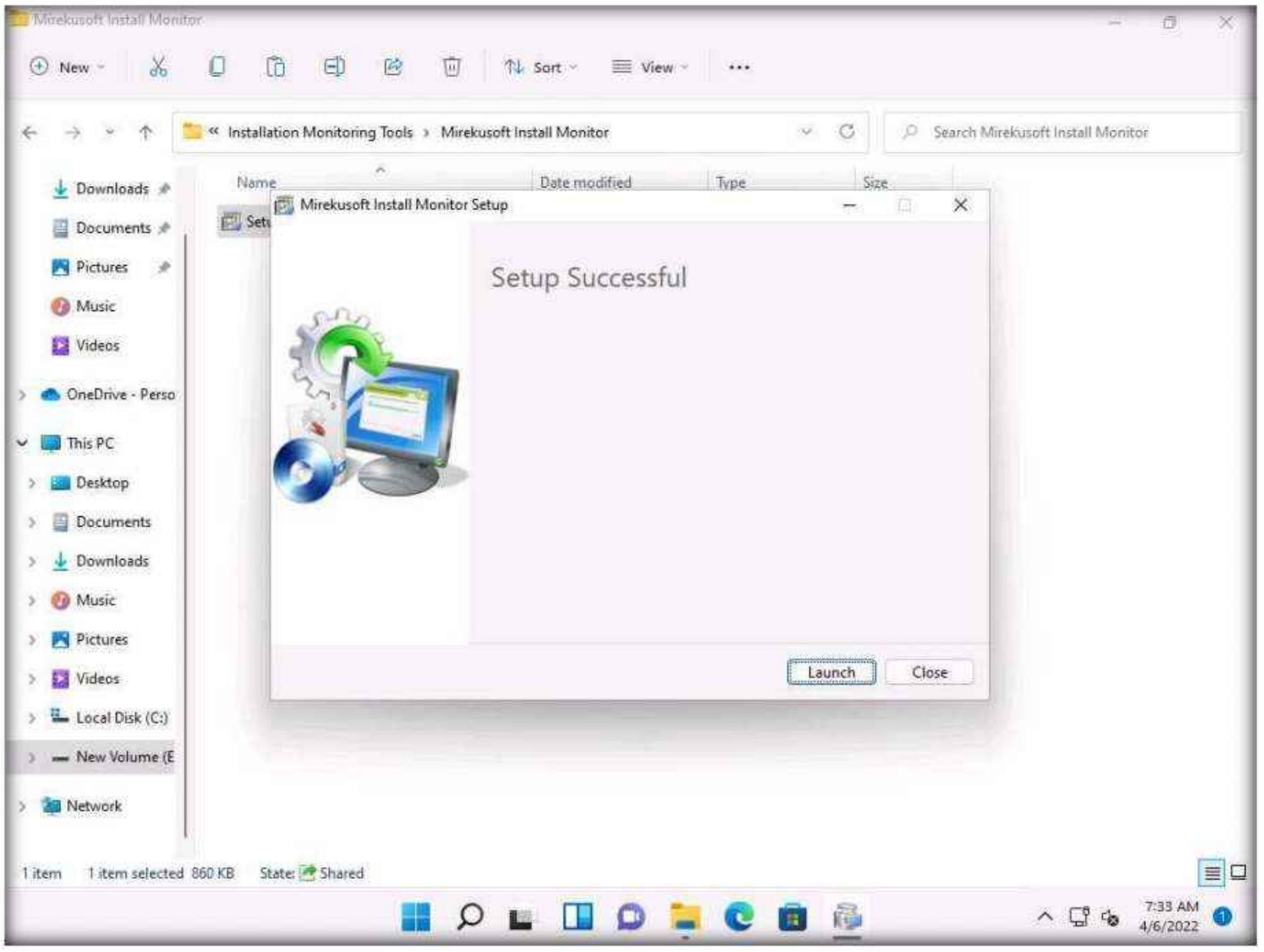
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor** and double-click **SetupInstallMonitor.exe**.

   Note: If **Update Available** wizard appears, click **Update** button.

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

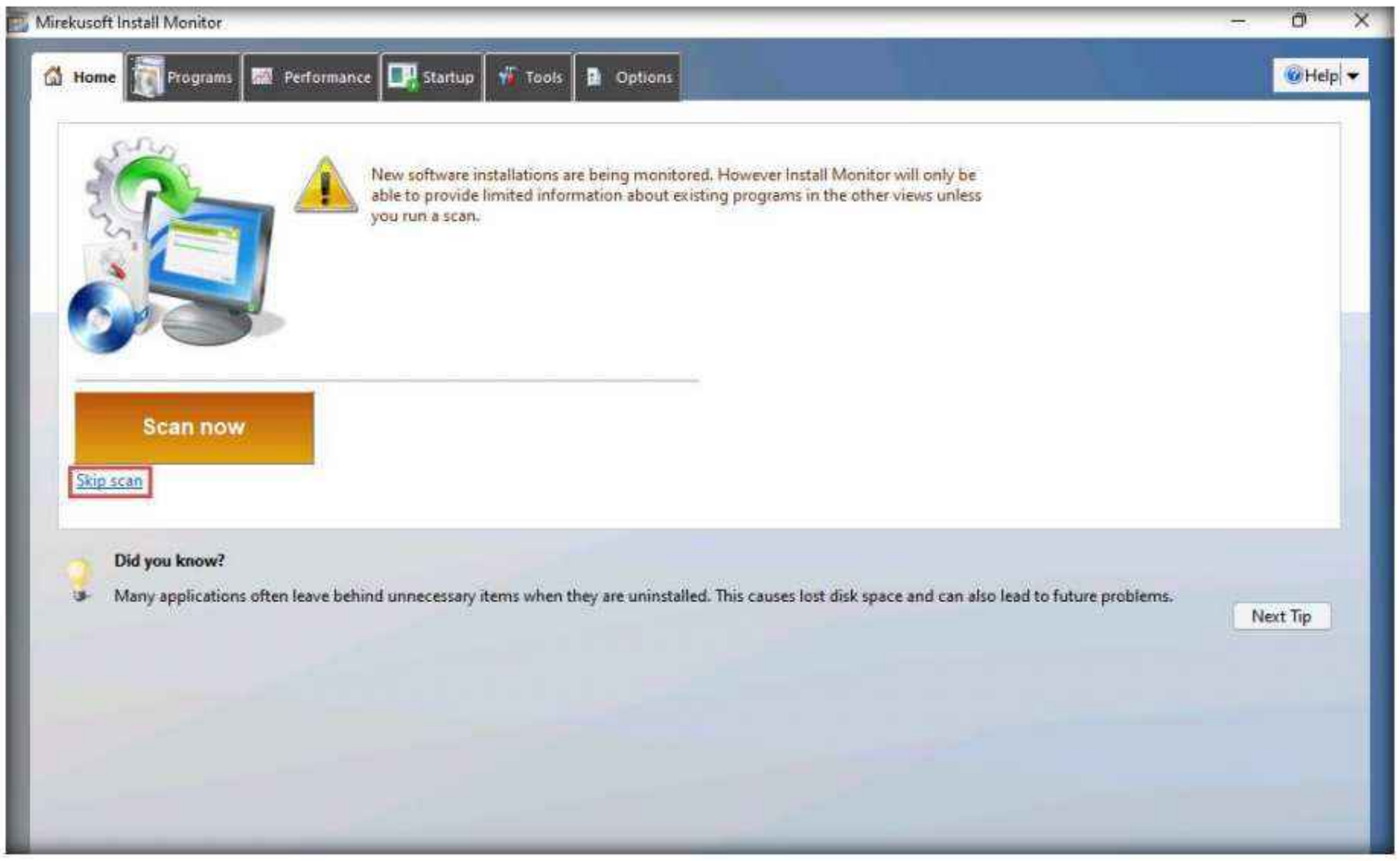
2. Follow the installation steps to install **Mirekusoft Install Monitor**.

3. The **Setup Successful** wizard appears; click **Launch**.



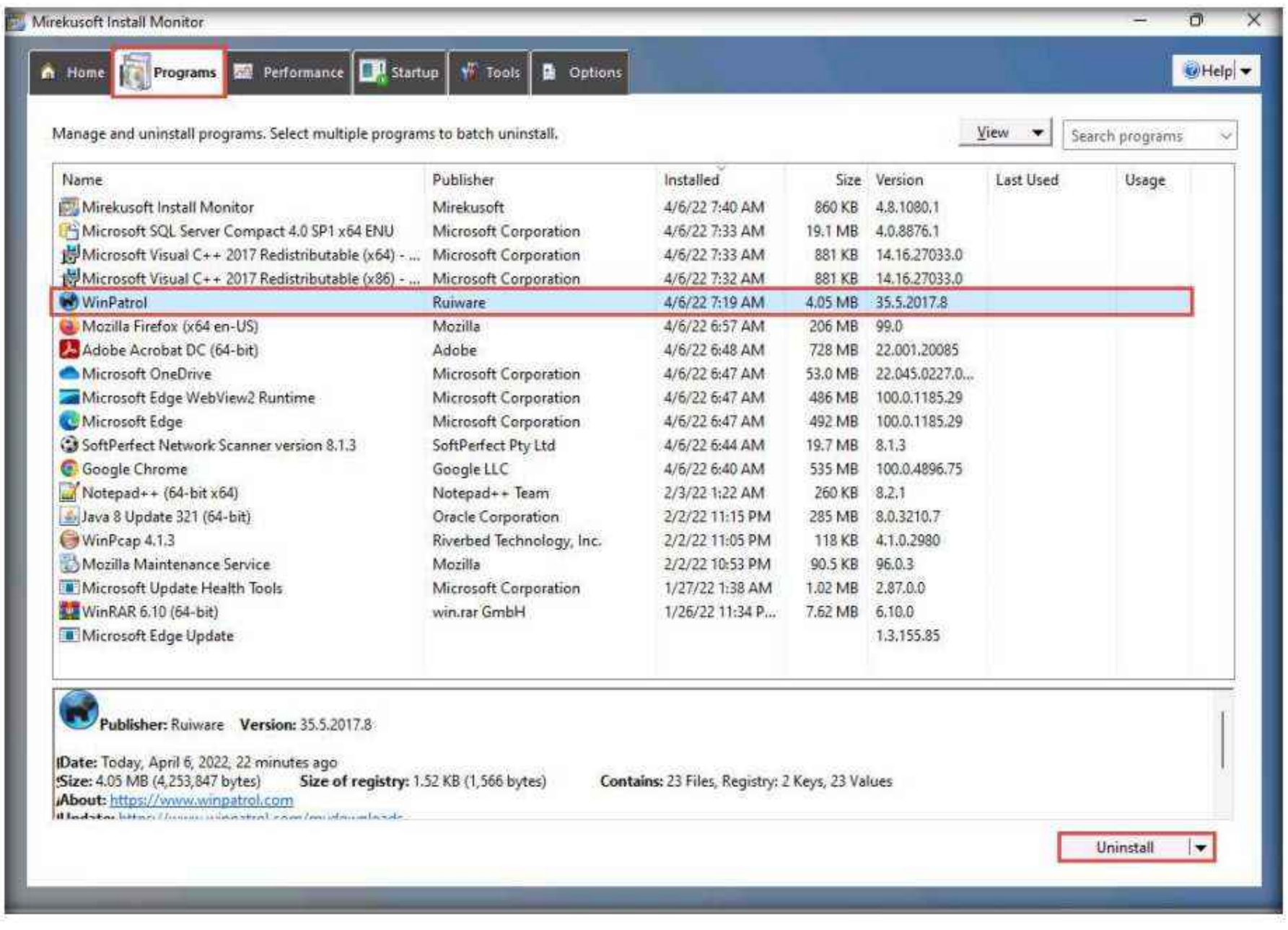
4. If a **User Account Control** window appears, click **Yes**.

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

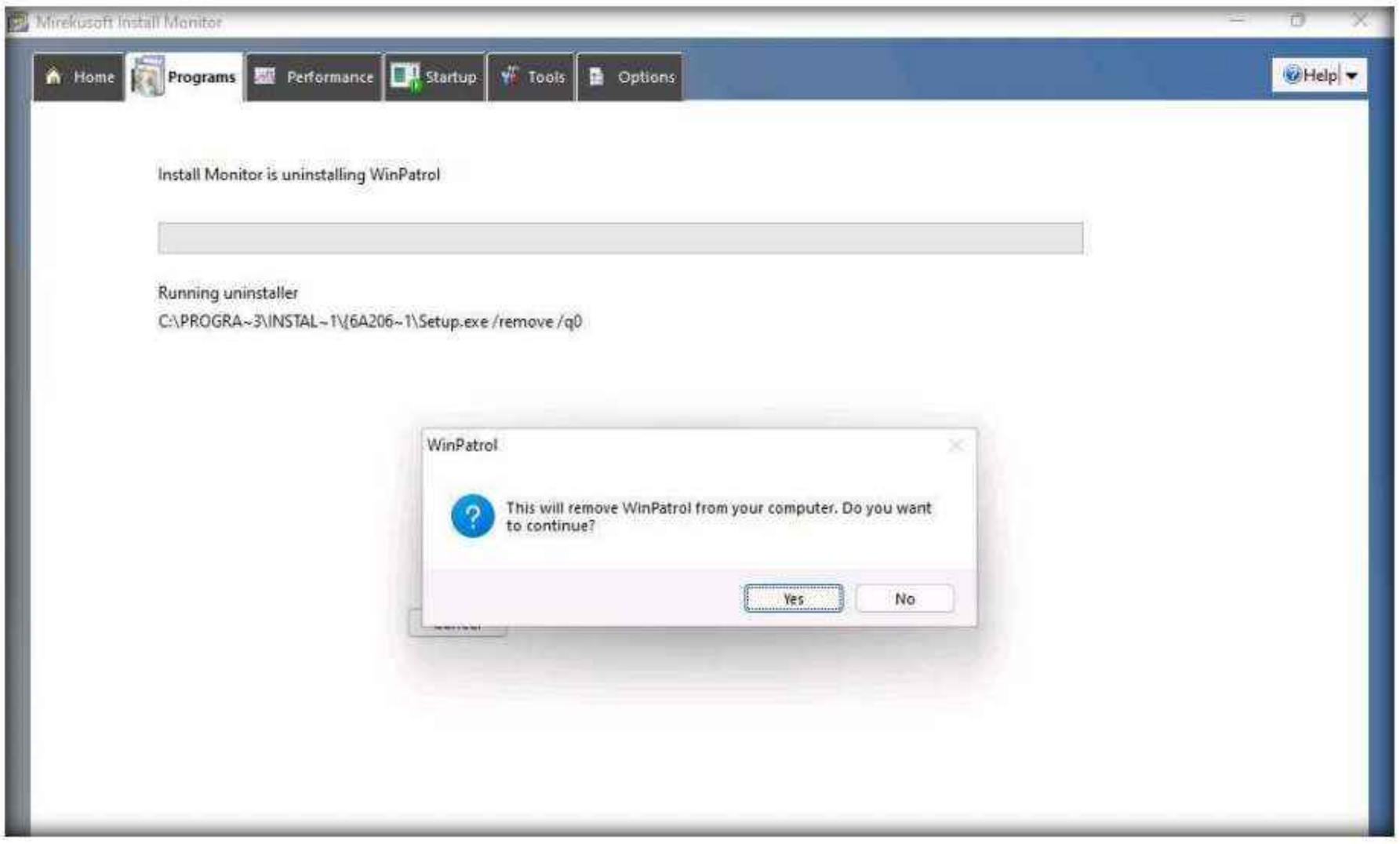


6. Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

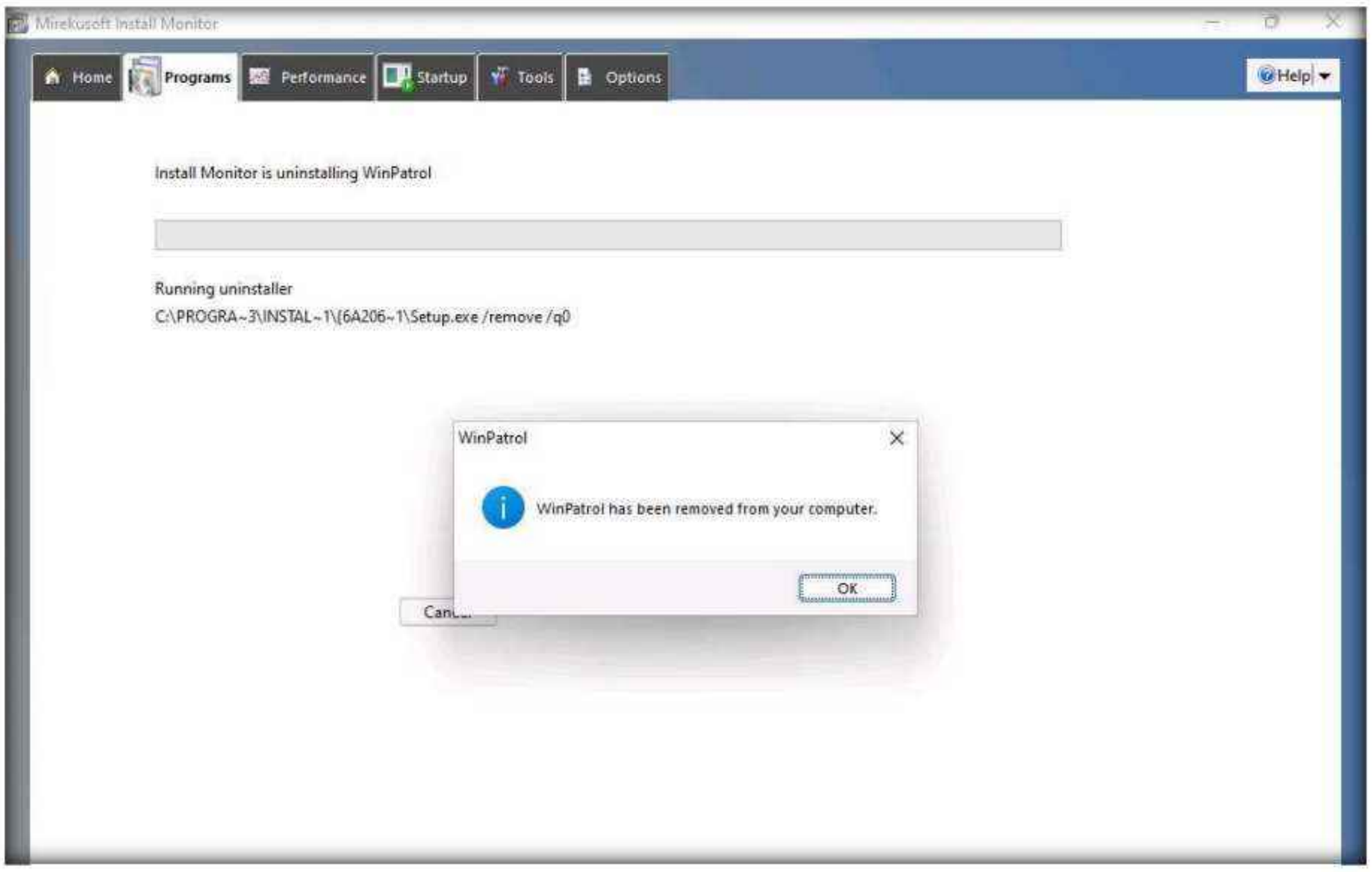
   Note: The **WinPatrol** pop-up appears; click **Reject Change**.



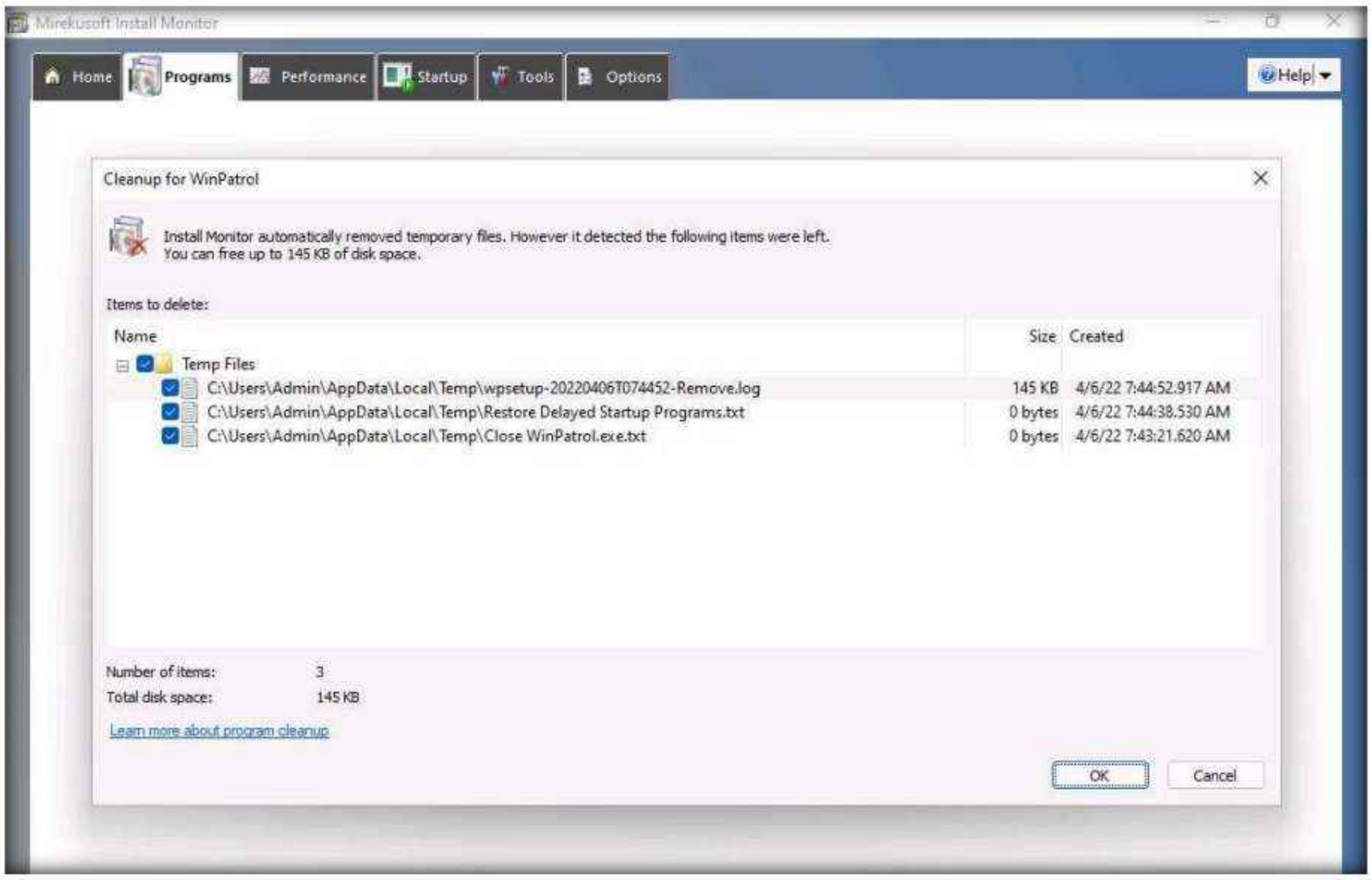
7. While uninstalling the application, a selected program pop-up appears, click **Yes** in all the **WinPatrol** pop-ups.



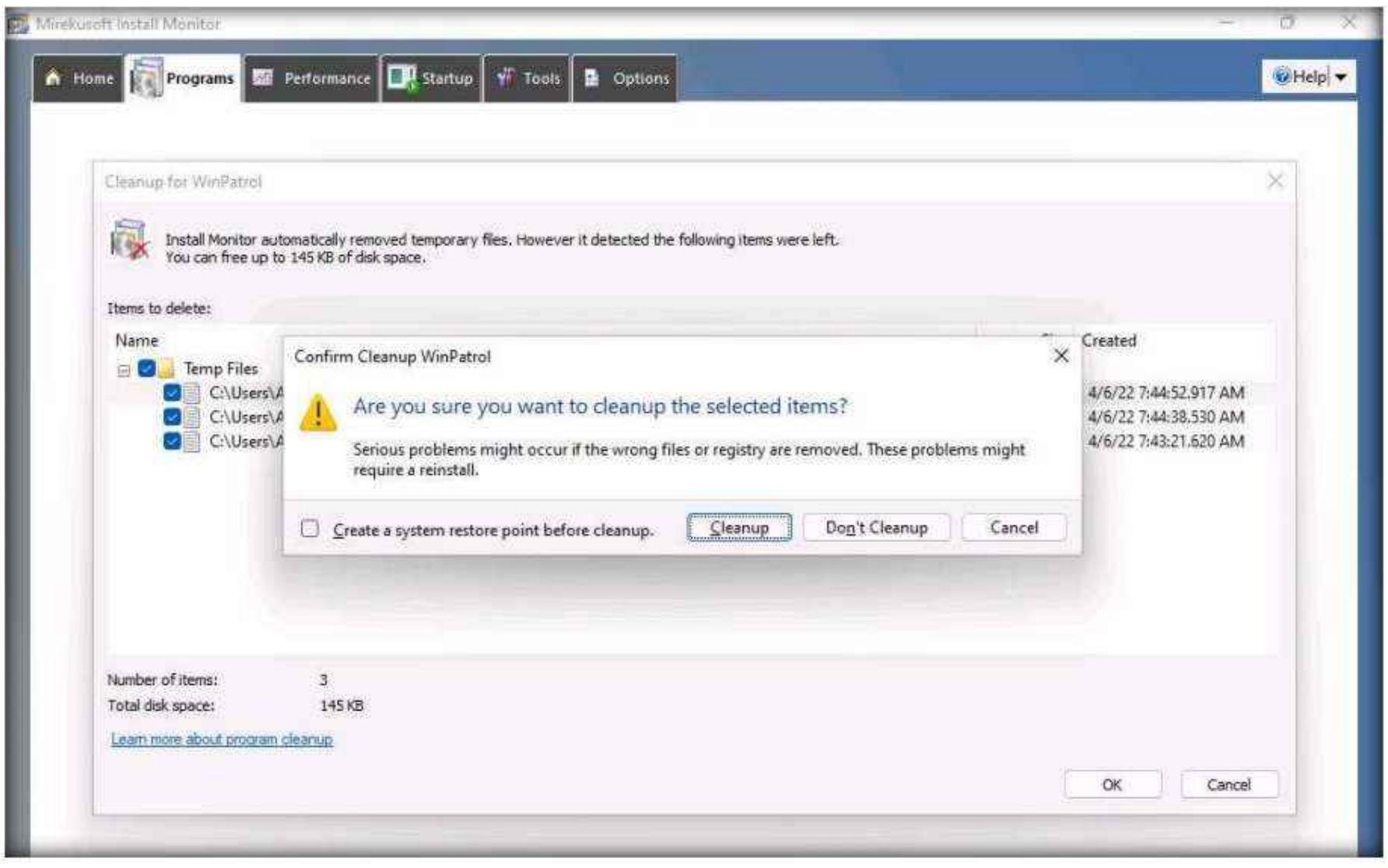
8. The **selected application is uninstalled from your computer** pop-up appears; click **OK**.
9. In the next **WinPatrol** pop-up, click **Yes**.
10. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.



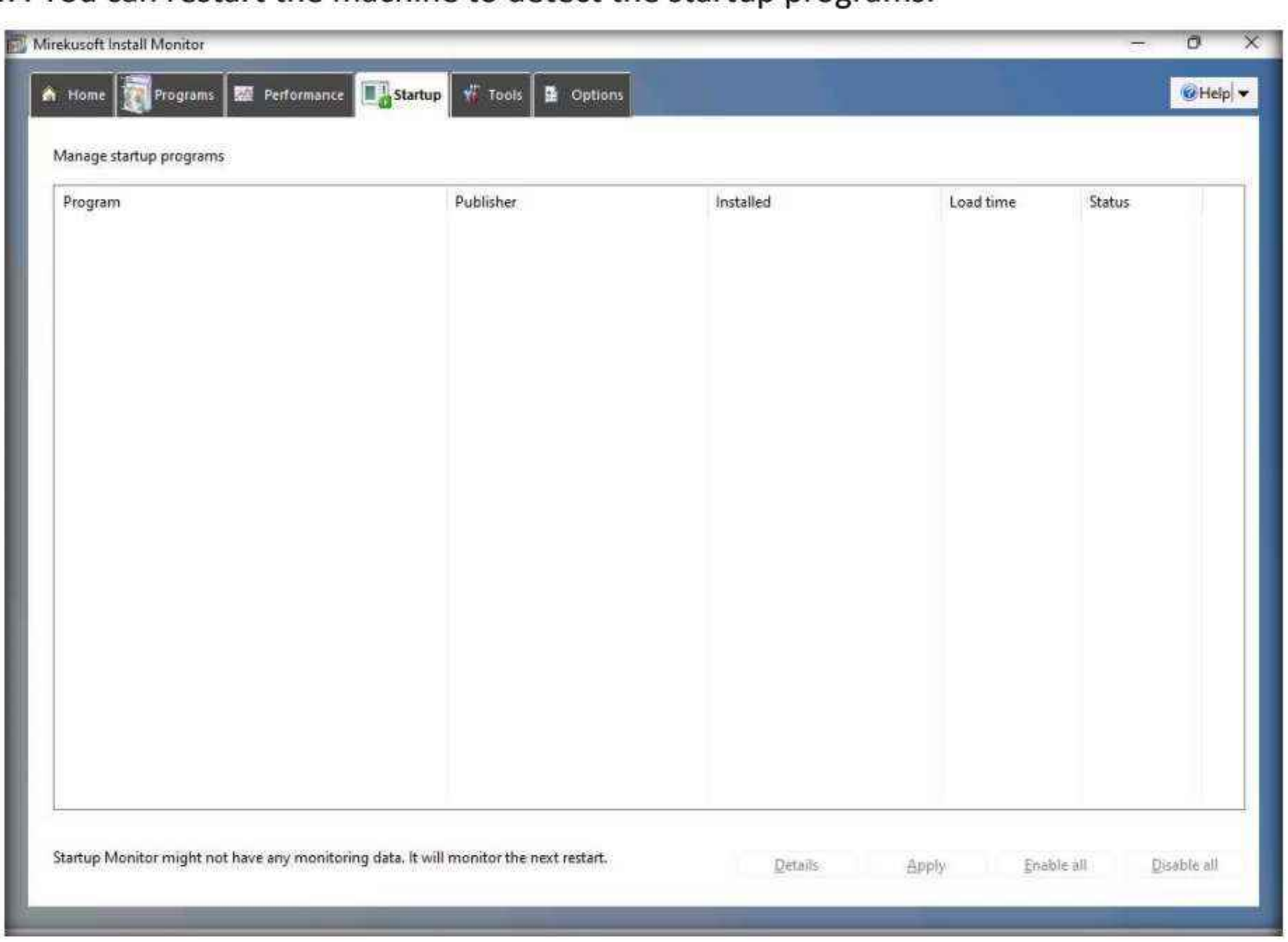
11. A **Cleanup for WinPatrol** window appears, click **OK**.



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



13. The selected application is uninstalled from your computer. Click the **Performance** tab to view and terminate currently running programs.
14. Here, you can select any program from the list and click **End Program** to terminate the program.
15. Click the **Startup** tab to view the programs that run automatically on Windows Startup.
16. In this task, 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.



18. This is how to monitor a Windows machine using Mirekusoft Install Monitor. Close all applications.
19. 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.

Task 7: Perform Files and Folder Monitoring using PA File Sight

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.

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.

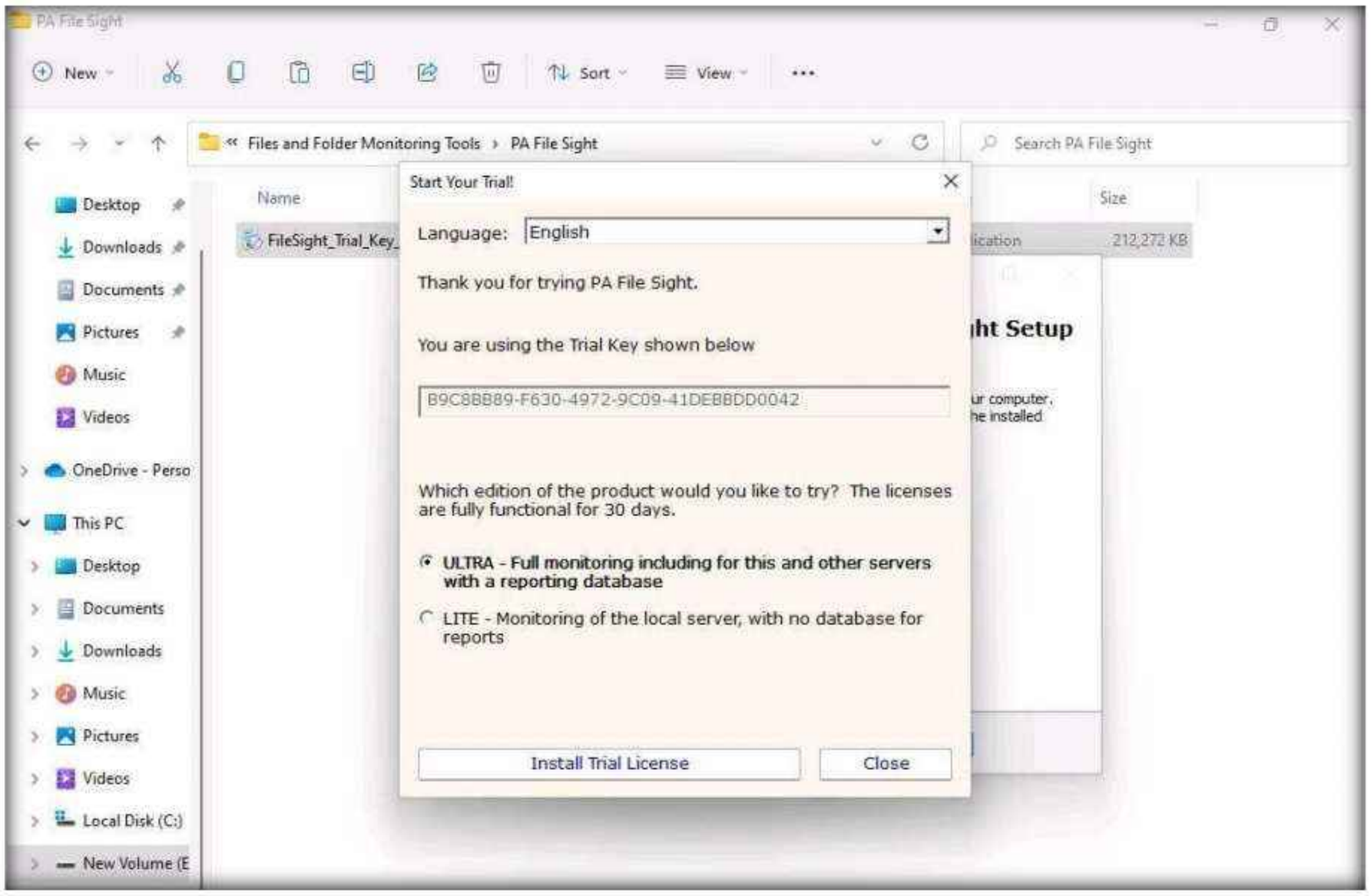
Features:

- 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

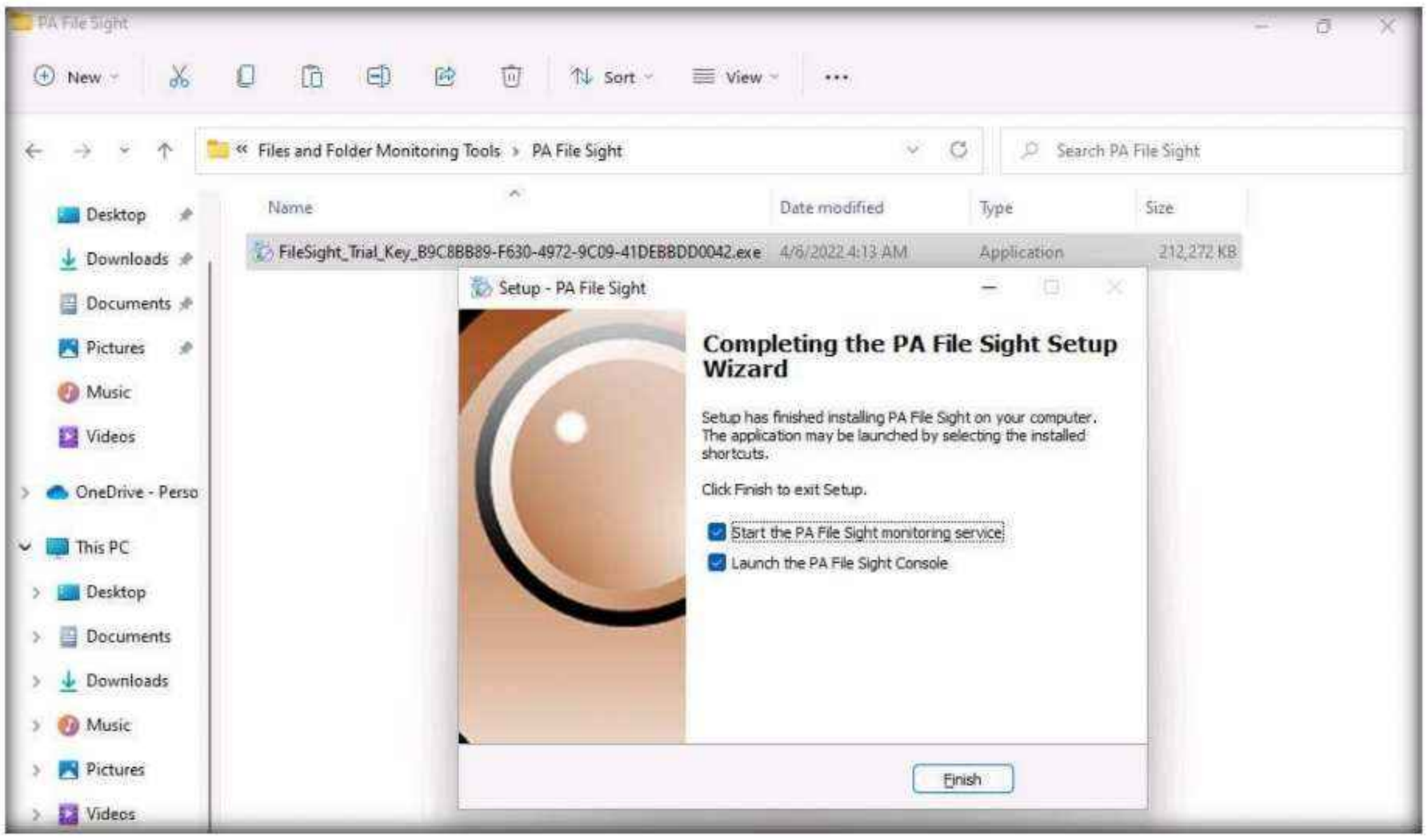
1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to the **Windows 11** virtual machine. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **FileSight_Trial_Key_E71BE154-2386-4CF3-BEA3-75830C985736.exe**.

   Note: If a **Open File - Security Warning** window appears, click **Run**. If a **User Account Control** window appears, click **Yes**.

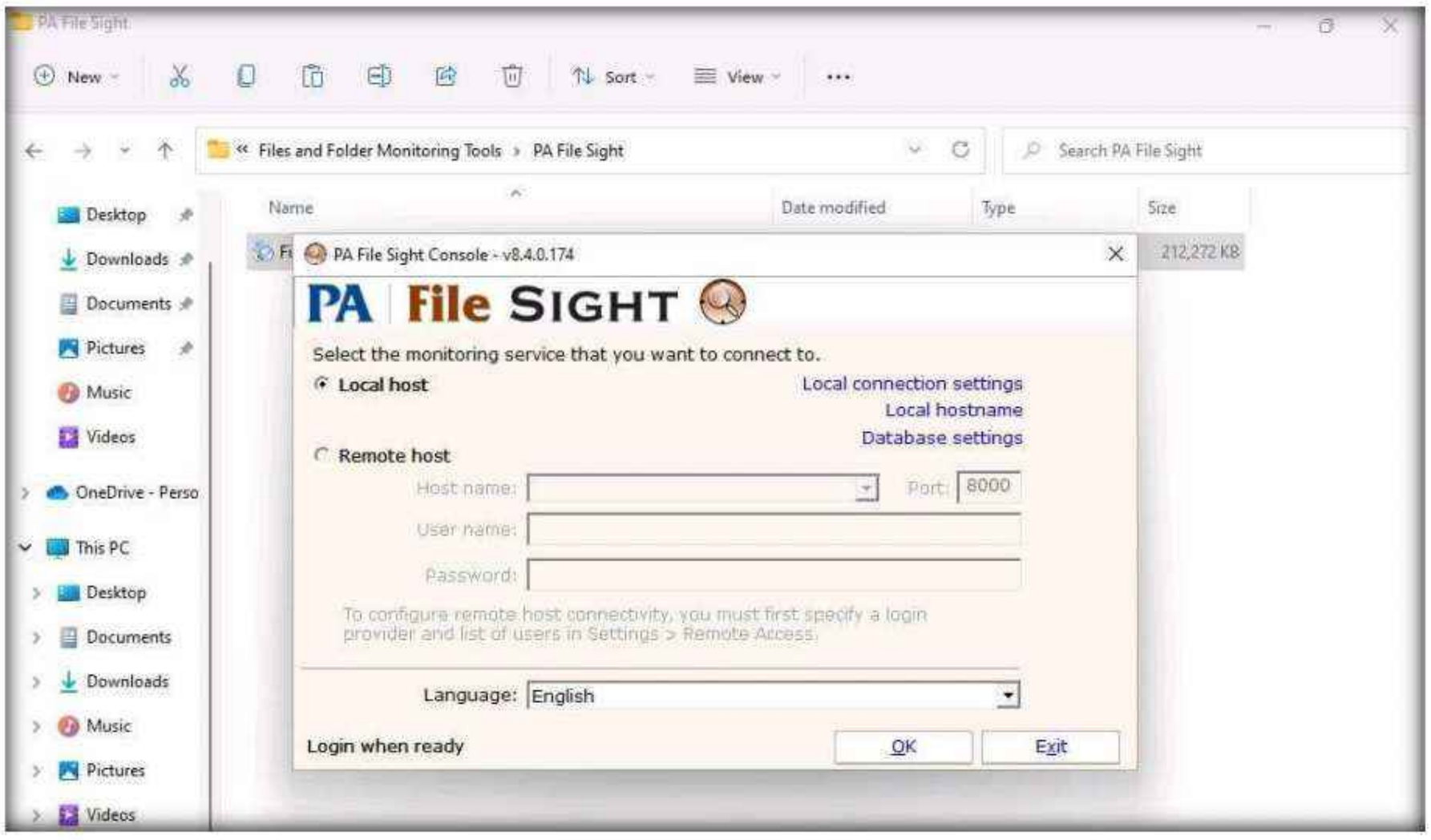
   Note: The name of the exe file might differ when you perform the lab.
3. The **Select Setup Language** pop-up appears; choose your preferred language, and then click **OK**.
4. Follow the default installation steps to install **PA File Sight**.
5. **Start Your Trial!** window appears, ensure that **Ultra** radio button is selected and click **Install Trial License**.



6. A **Success** window appears, click **OK**.
7. **Completing the PA File Sight Setup Wizard** appears; make sure that both the **Start the PA File Sight monitoring service** and the **Launch the PA File Sight Console** options are checked, and click **Finish**.
8. This will run the PA File Sight service and automatically launch the application.

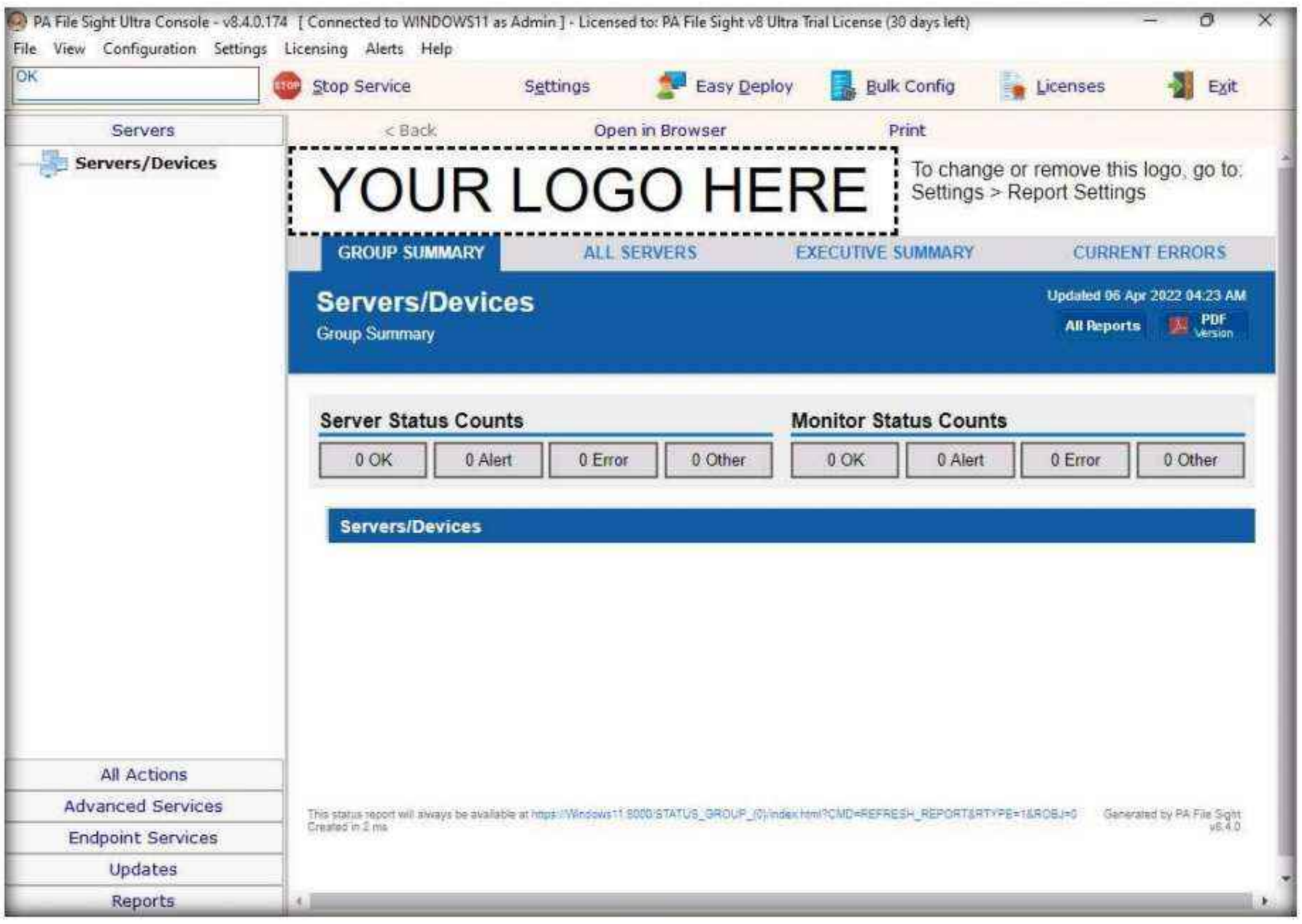


9. The **PA File Sight Console** window appears. By default, the **Local host** radio button is selected; click **OK**.



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

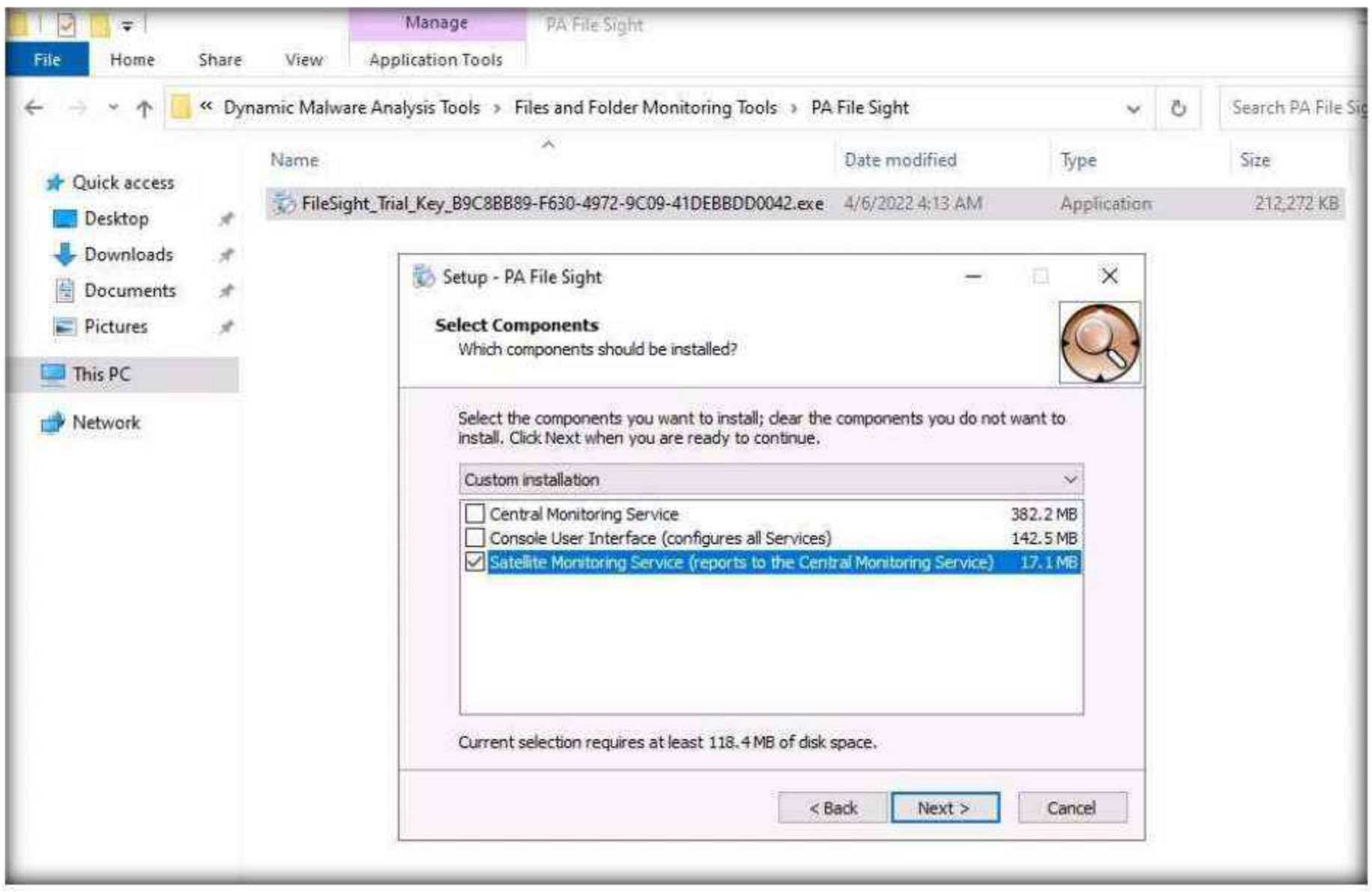
    Note: If a **Start Wizard** window appears, close it.



11. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
12. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **FileSight_Trial_Key_E71BE154-2386-4CF3-BEA3-75830C985736.exe**.

    Note: If a **Open File - Security Warning** window appears, click **Run**.

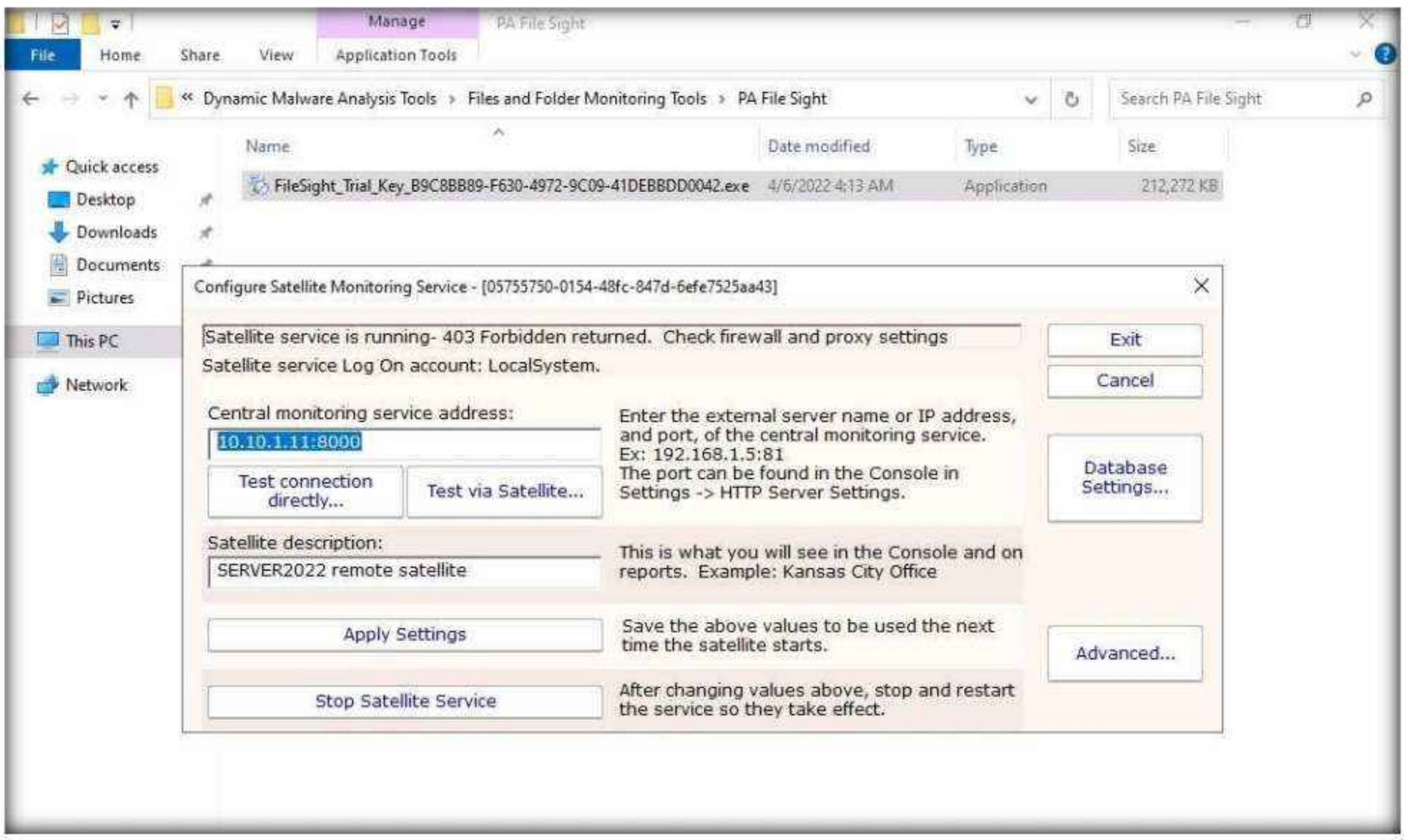
    Note: The name of the exe file might differ when you perform the lab.
13. The **Select Setup Language** pop-up appears; choose your preferred language and click **OK**.
14. Click the **Next** button until you see the **Select Components** wizard.
15. In the **Select Components** wizard, uncheck the **Central Monitoring Service** and **Console User Interface (configure all Services)** options, and check the **Satellite Monitoring Service (reports to the Central Monitoring Service)** option; then, click **Next**.



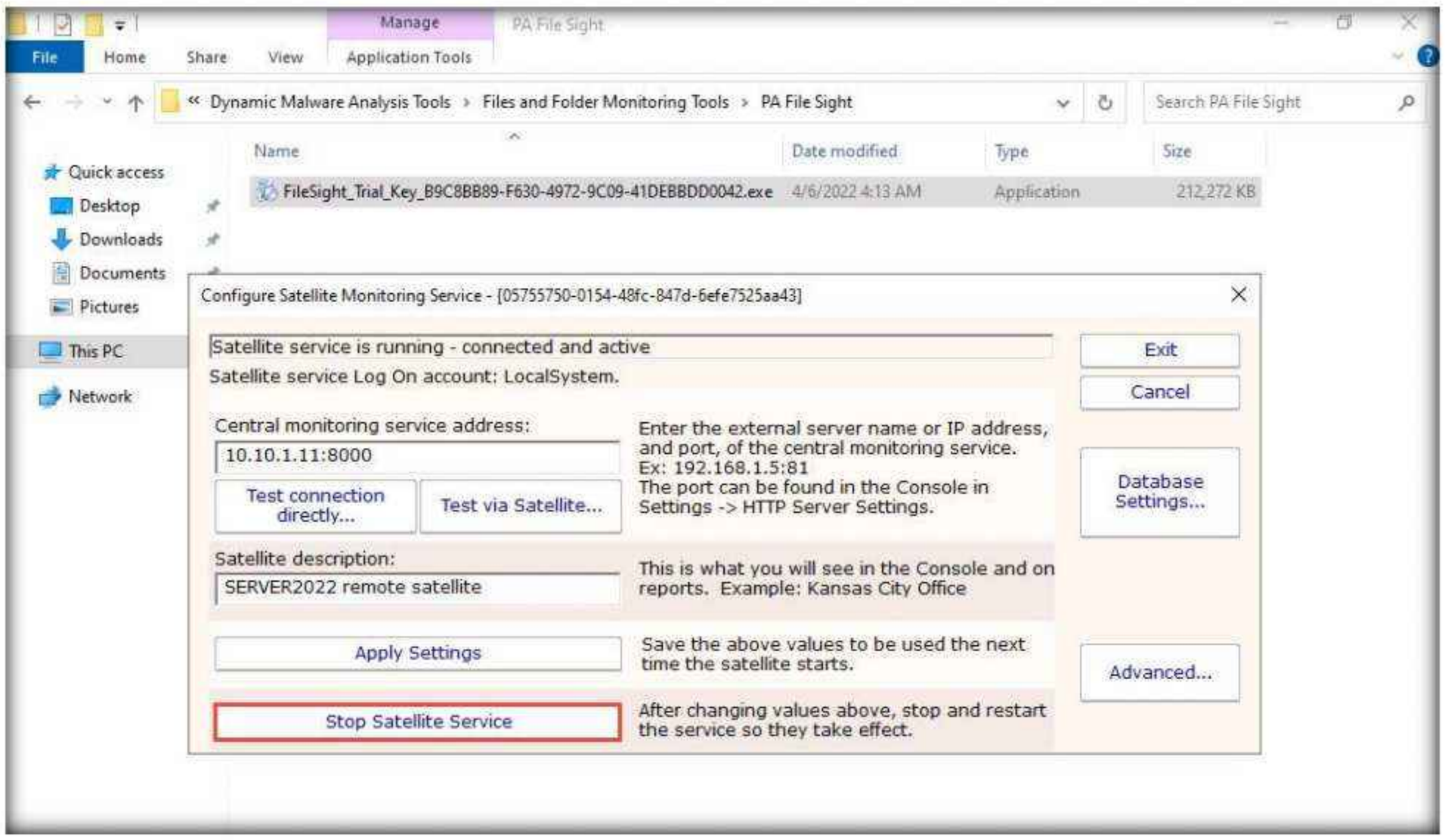
16. Follow the wizard-driven installation steps to install the application.
17. In the final step of the installation, make sure that the **Start the PA File Sight Satellite Monitoring Service** and **Configure the PA File Sight Satellite service** options are checked; then, click **Finish**.

18. The **Configure Satellite Monitoring Service** window appears; type the **Windows 11** IP address into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

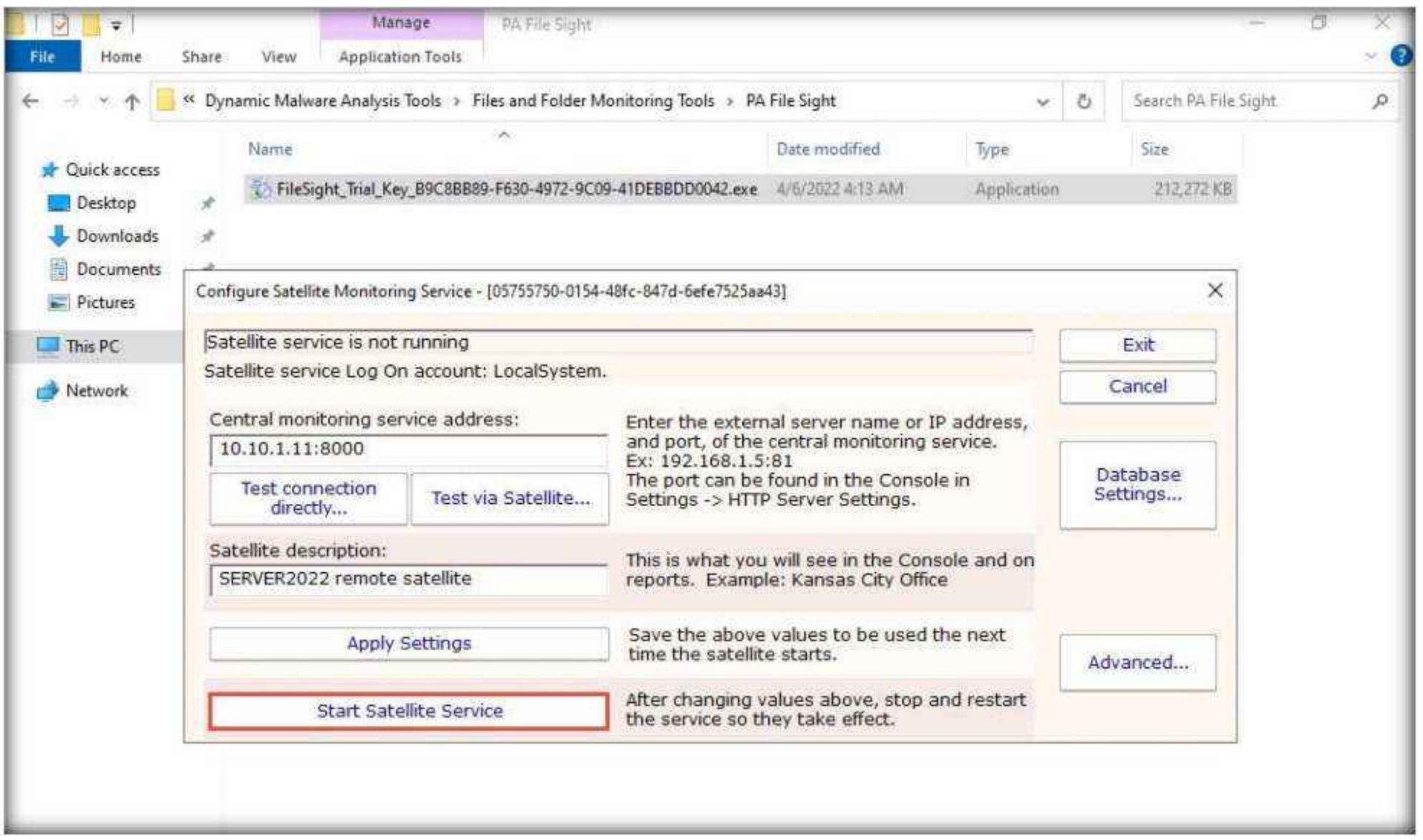
    Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.



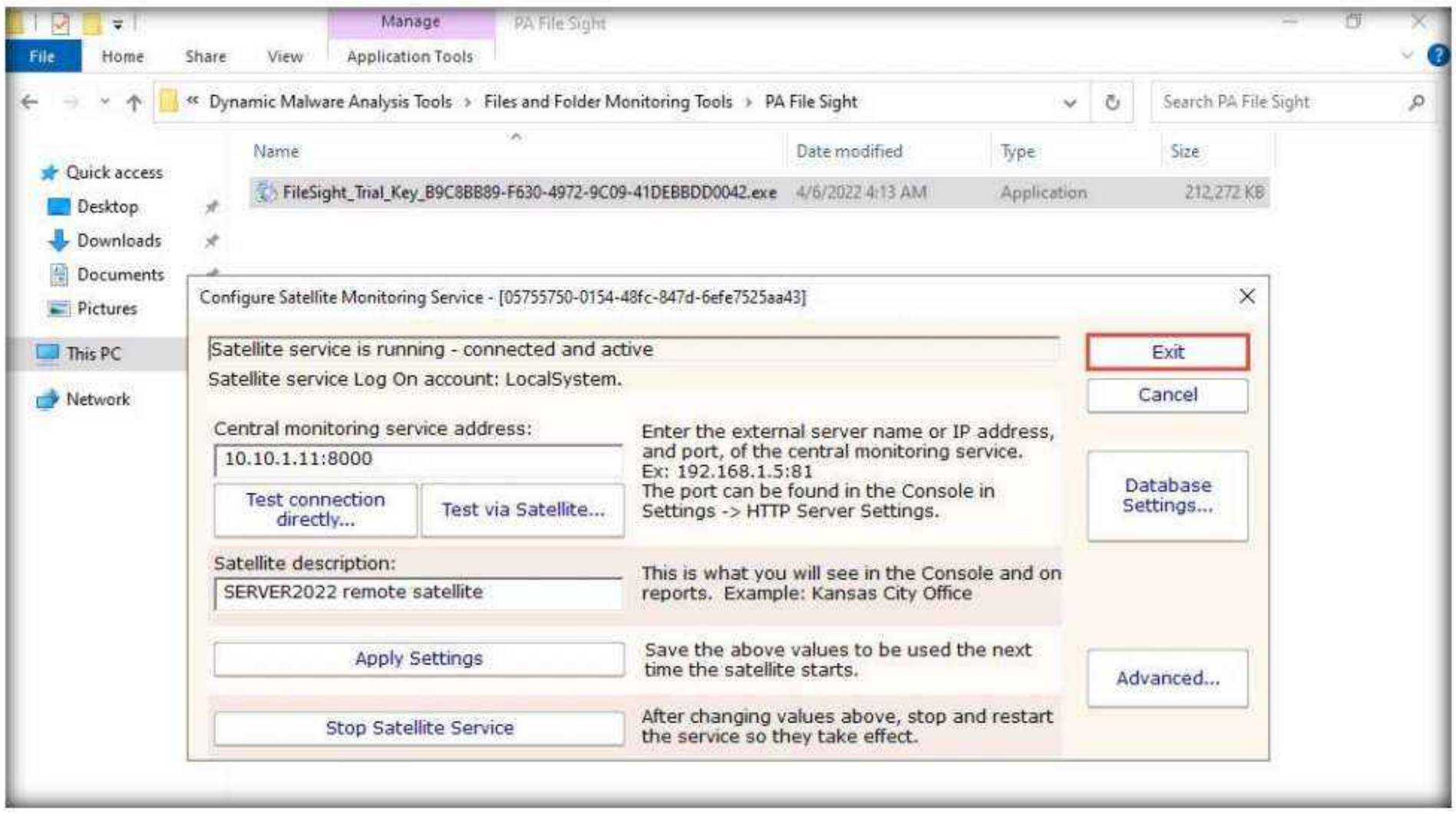
19. Click **Stop Satellite Service** to stop the satellite service.



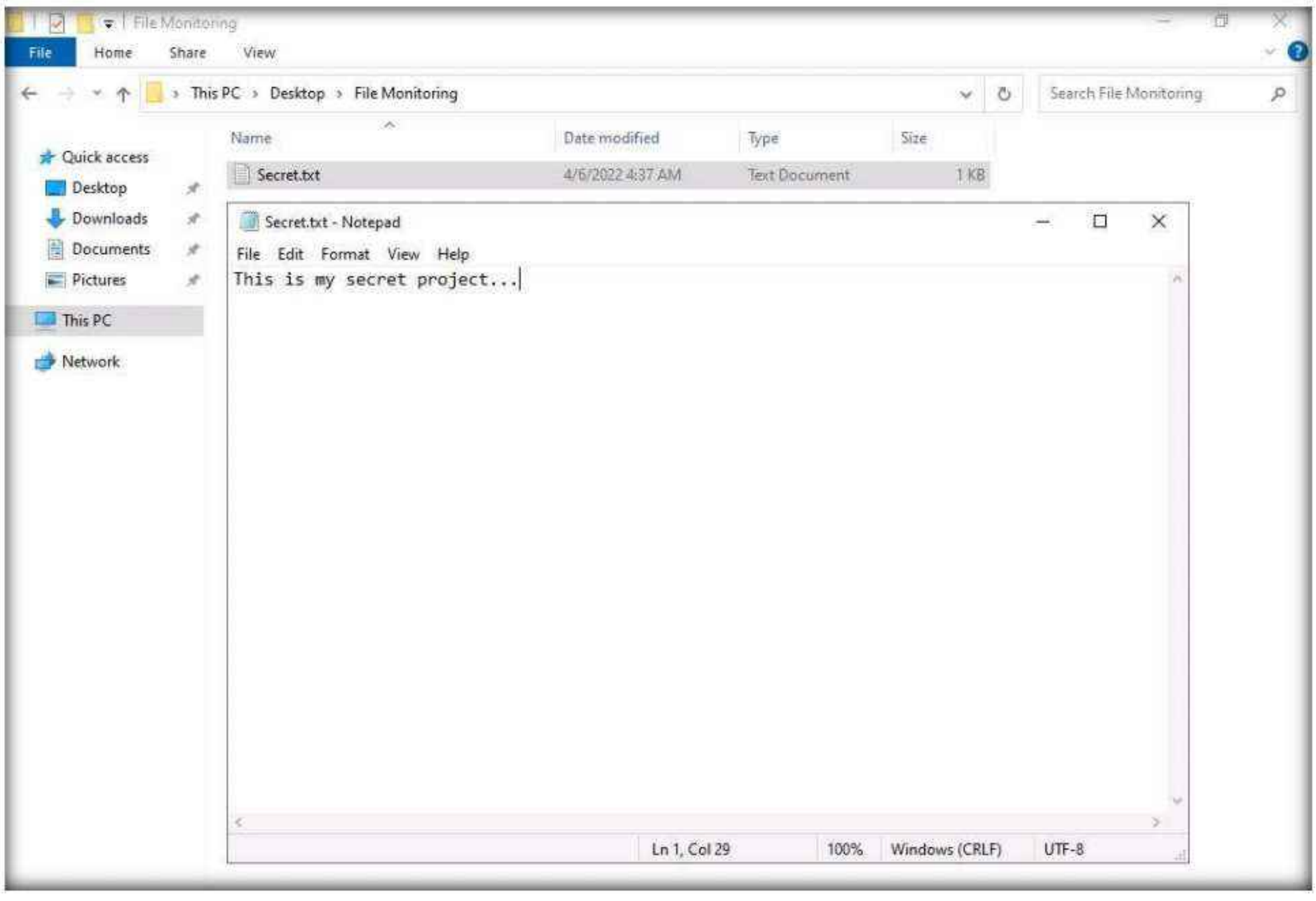
20. Once the service is stopped, click **Start Satellite Service**.



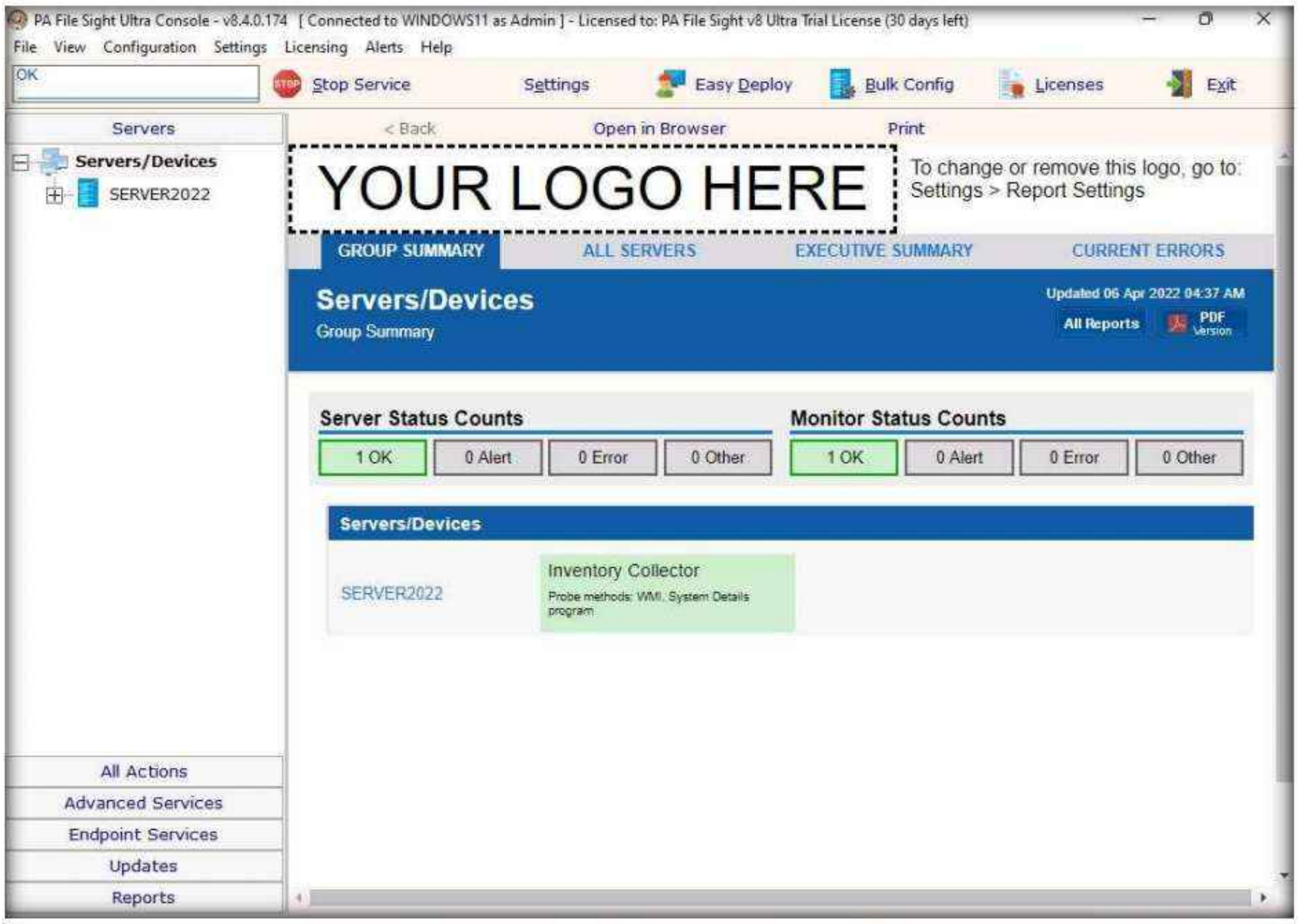
21. Once the service has started, click **Exit** to close the application.



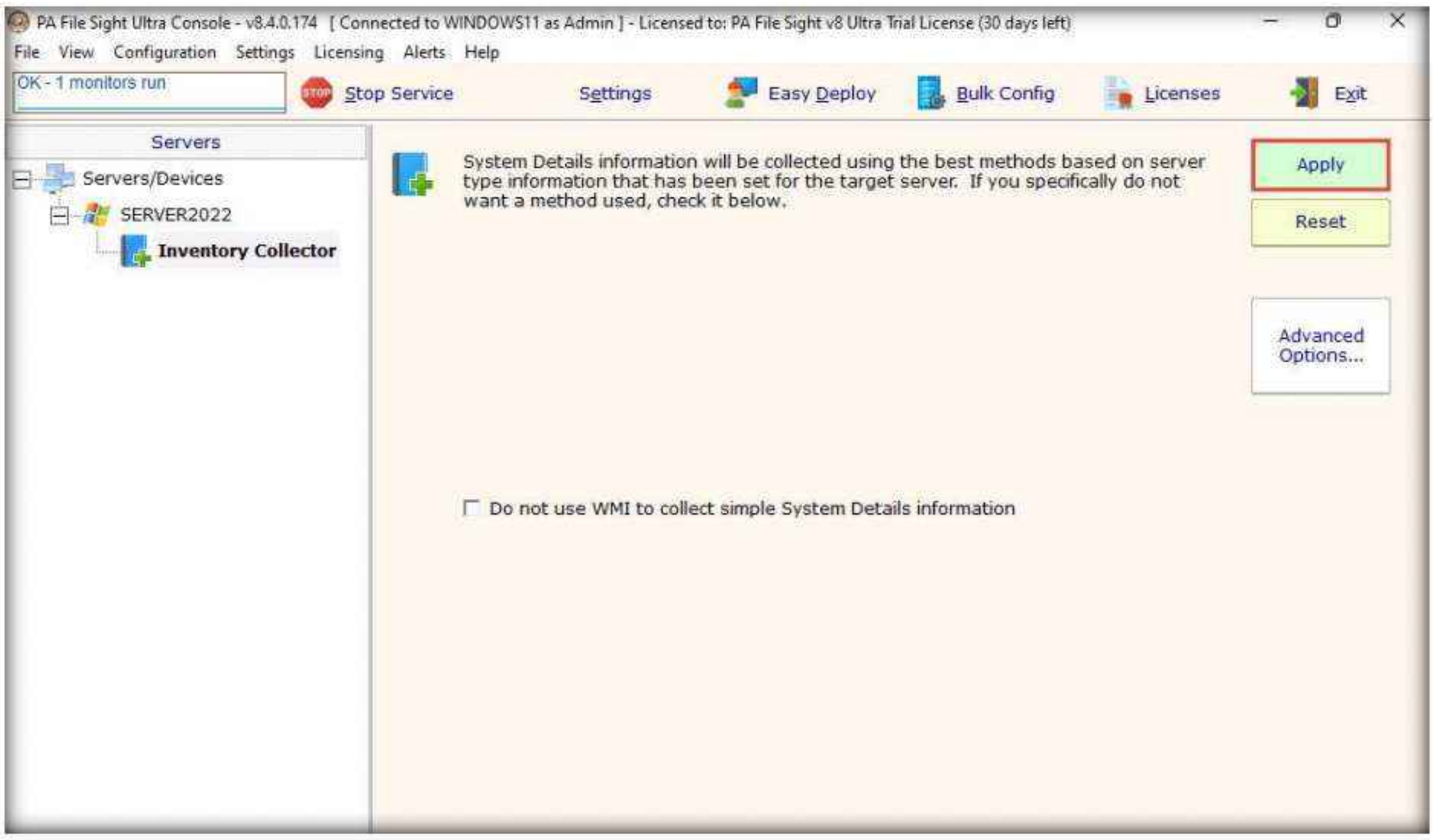
22. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.



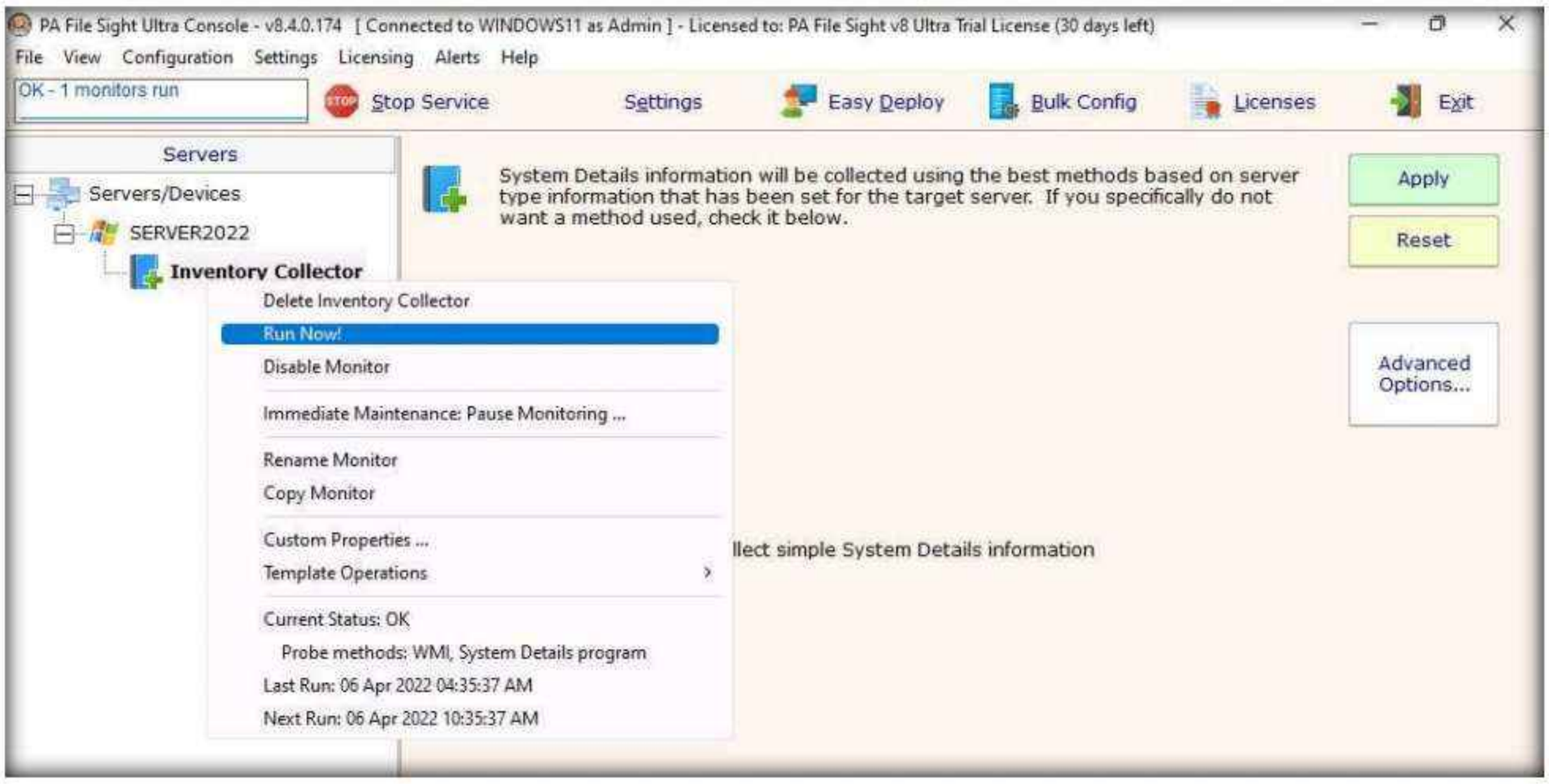
23. Switch back to the **Windows 11** virtual machine, and observe that PA File Sight starts monitoring the **Windows Server 2022** machine.



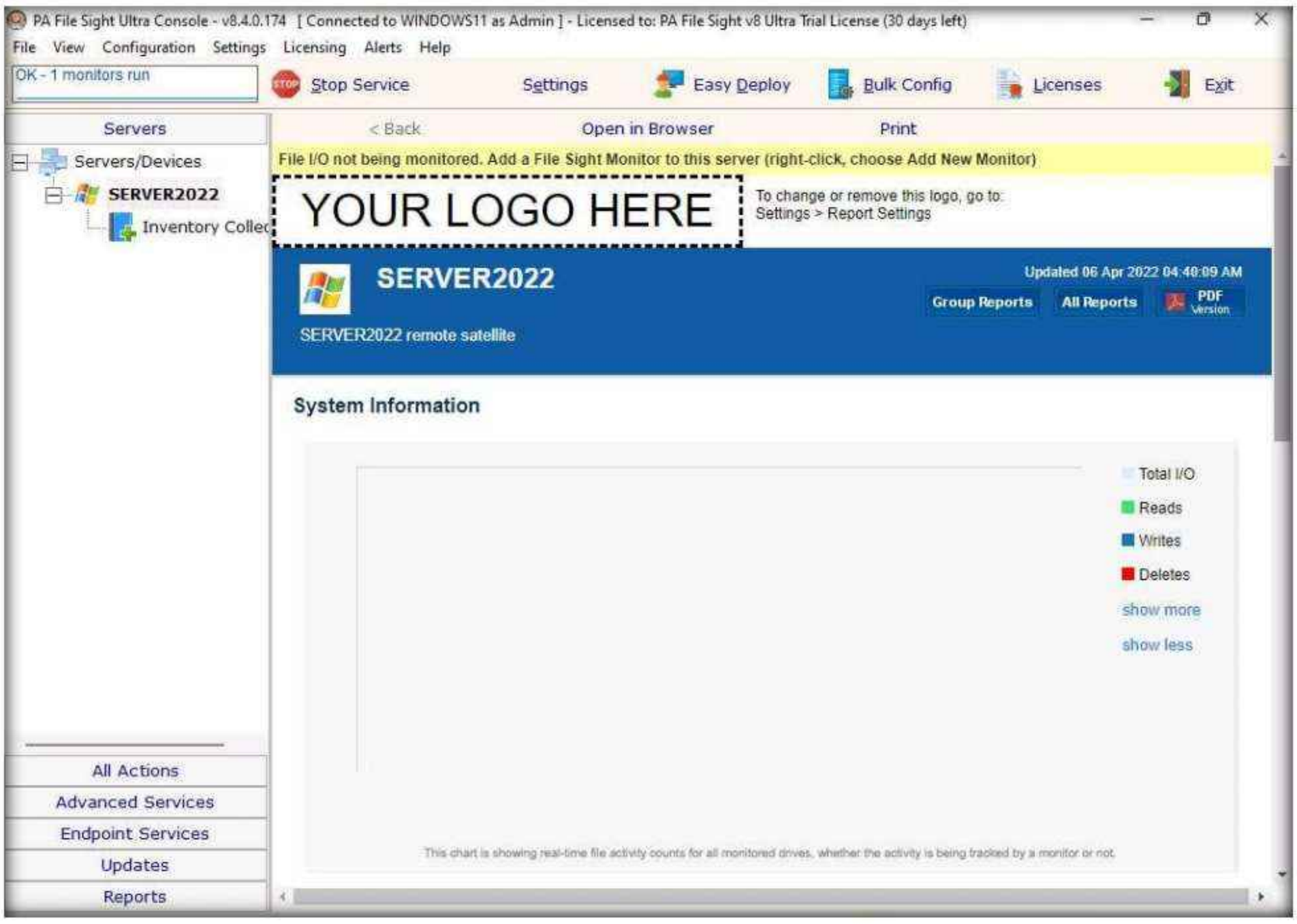
24. Expand the **Server2022** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.

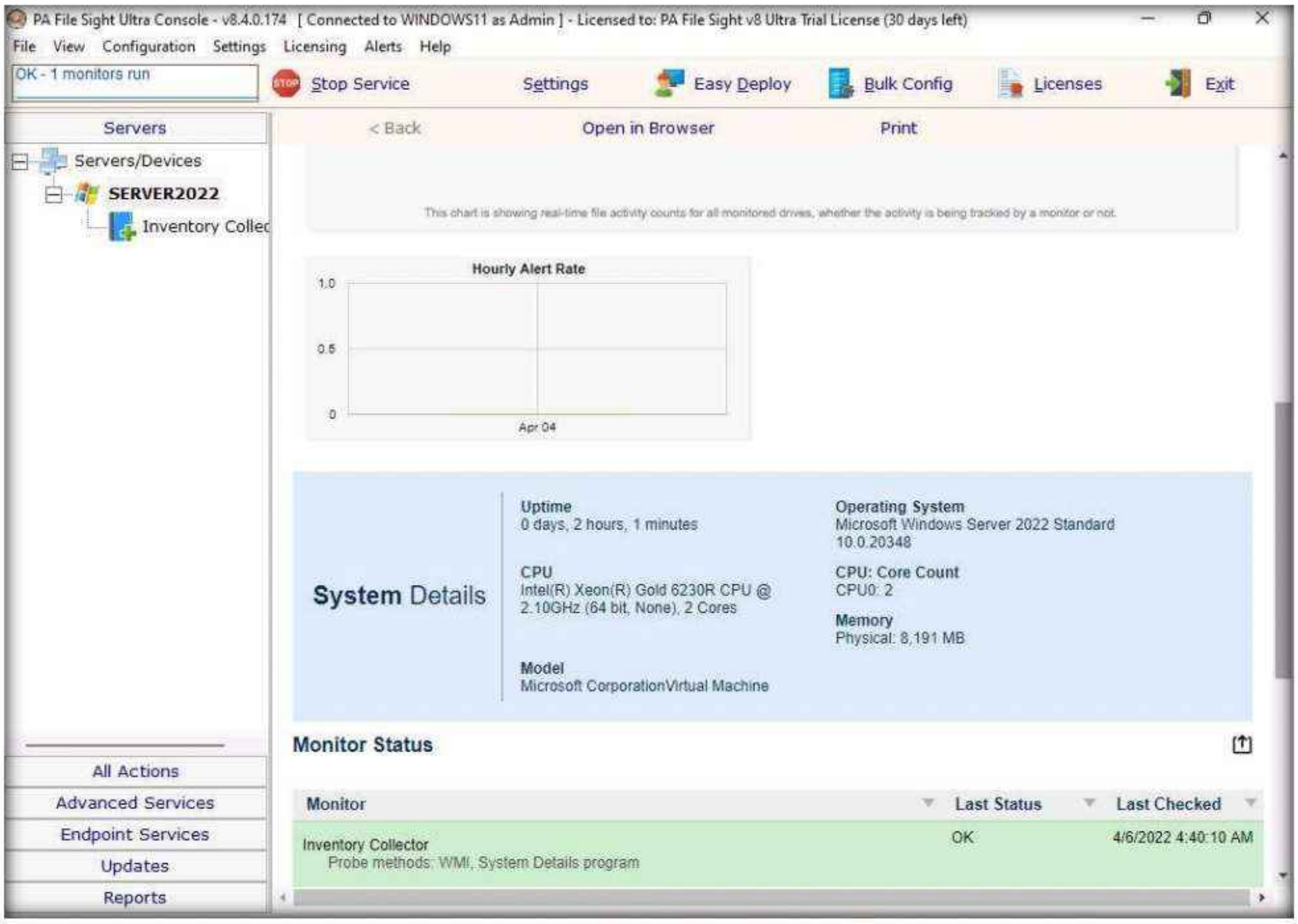


25. Now, right-click on **Inventory Collector** and click **Run Now!** from the context menu.

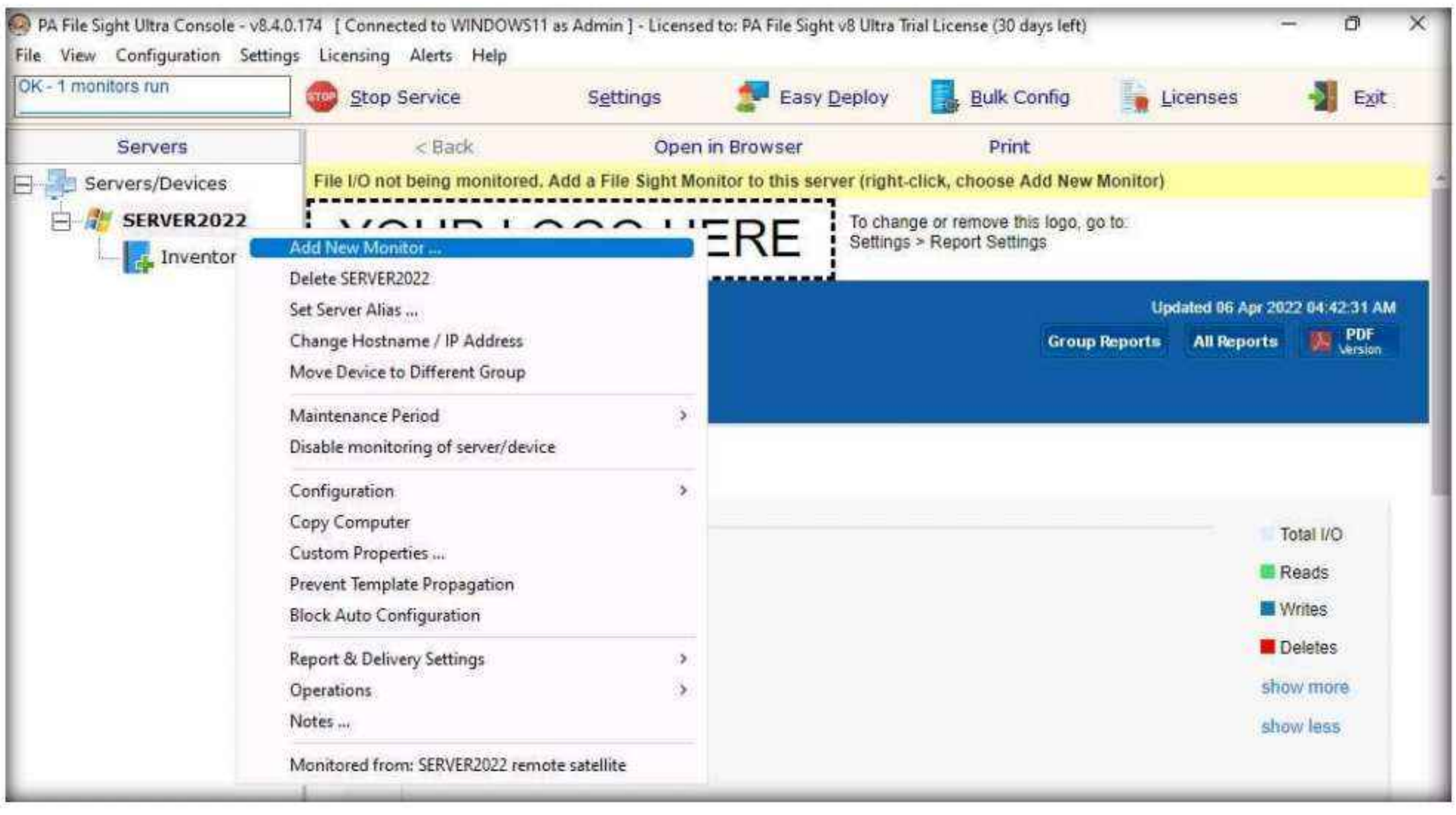


26. Select **Server2022** in the left pane and scroll down in the right pane, and you can see the complete system information for the **Windows Server 2022** machine on the dashboard.

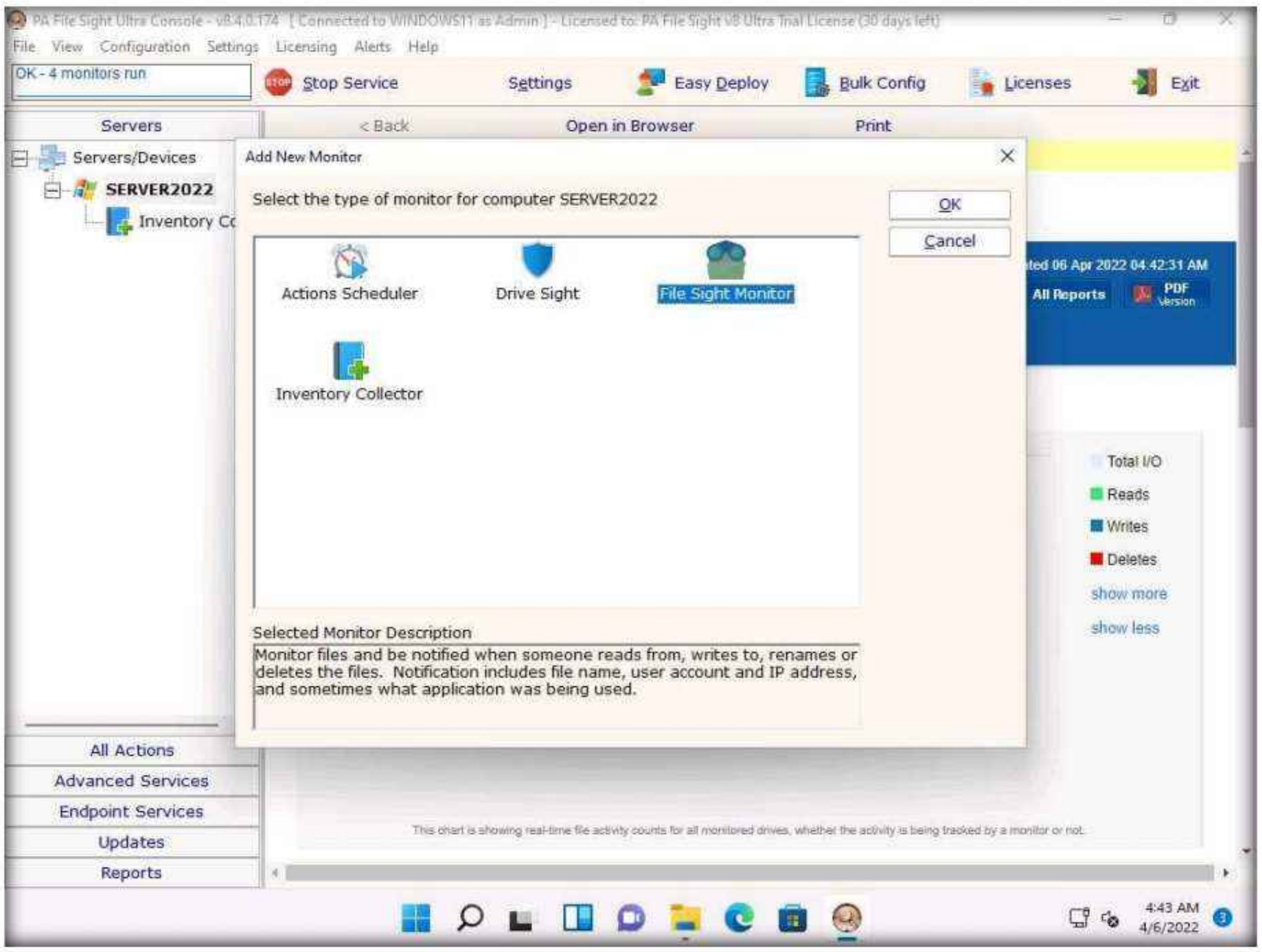




27. Right-click on **Server2022** and click the **Add New Monitor** option from the context menu.

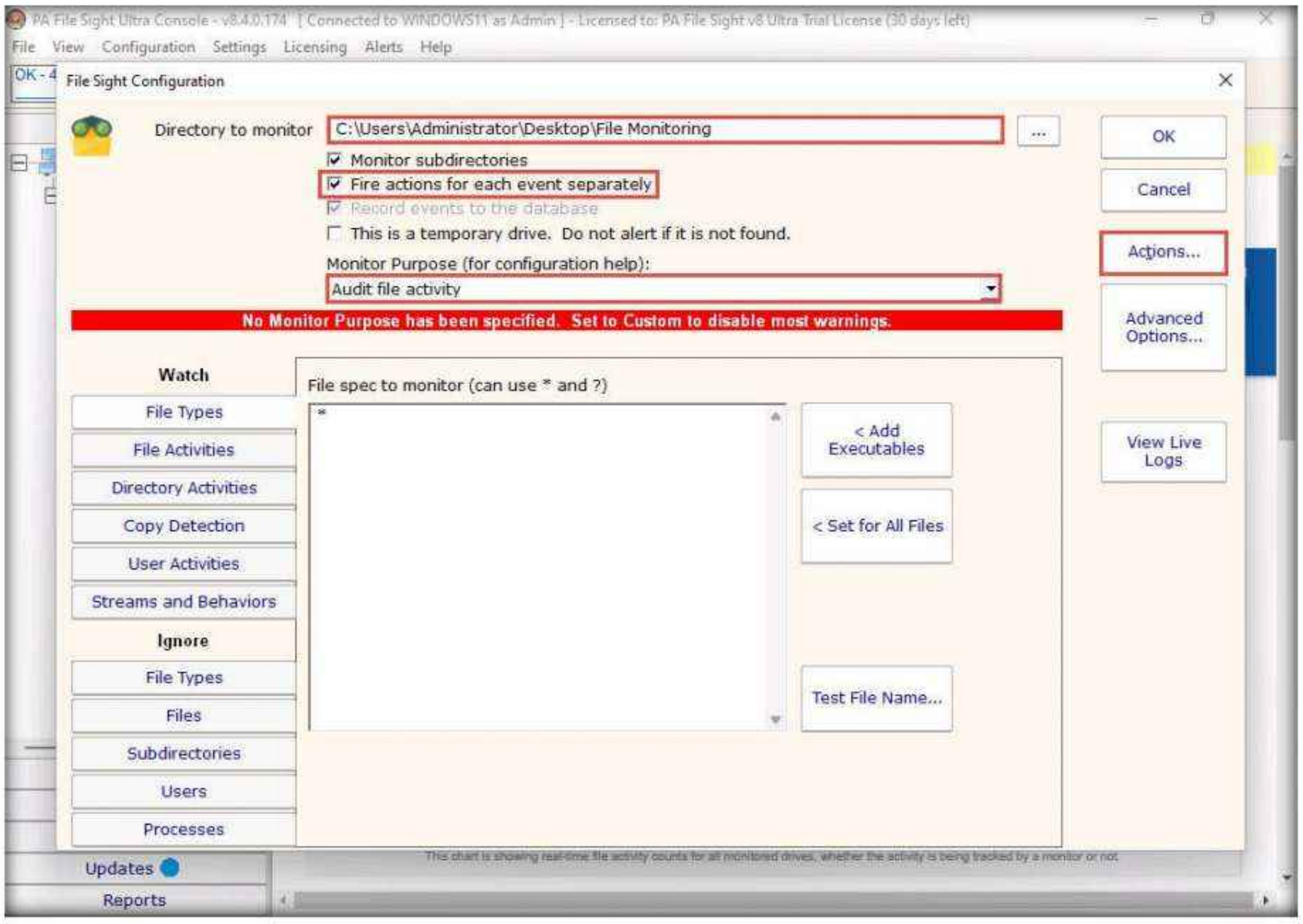


28. The **Add New Monitor** window appears, select the **File Sight Monitor** icon, and then click **OK**.

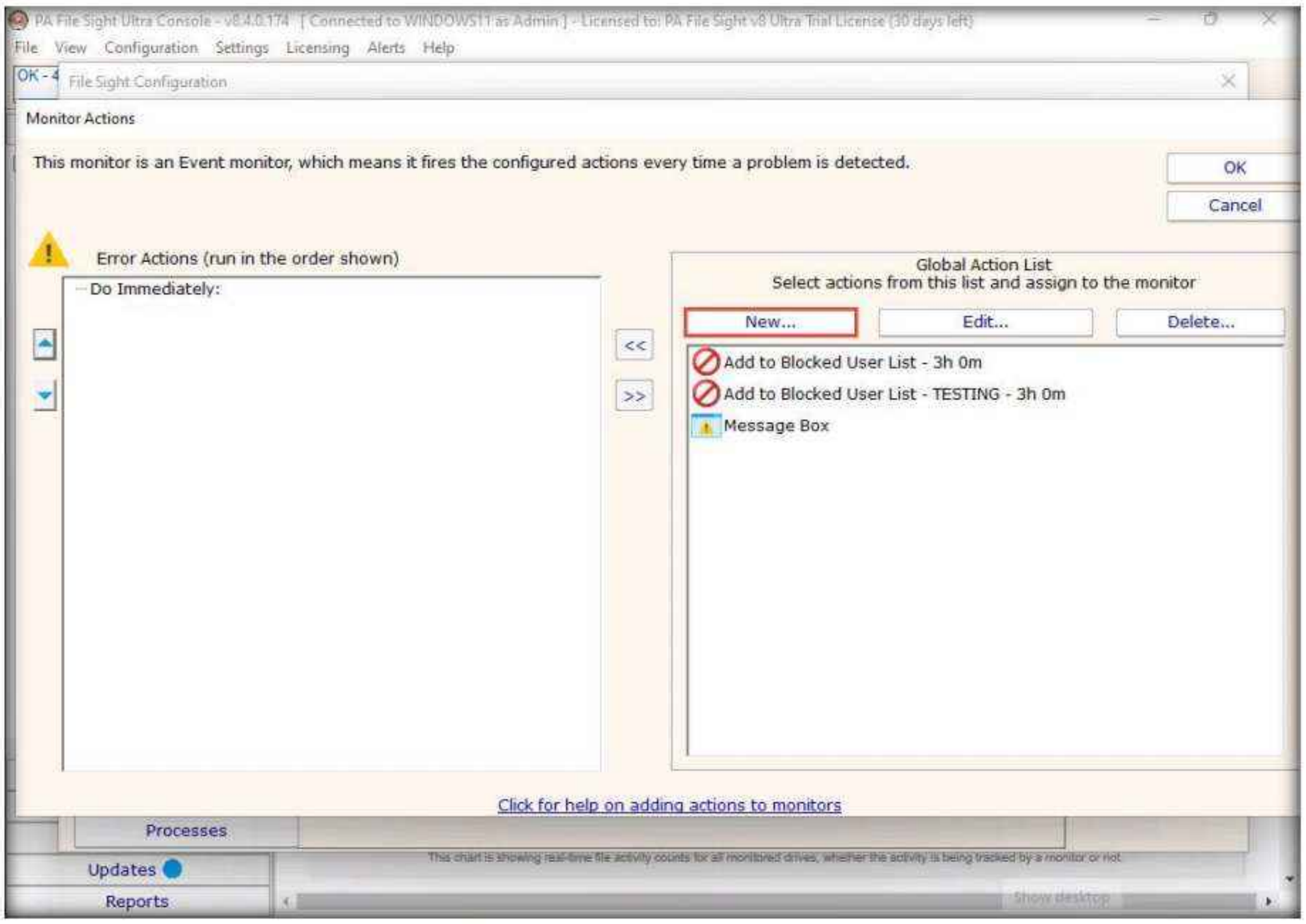


29. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **Server2022** machine (here, **C:\Users\Administrator\Desktop\File Monitoring**) and tick the **Fire actions for each event separately** checkbox.

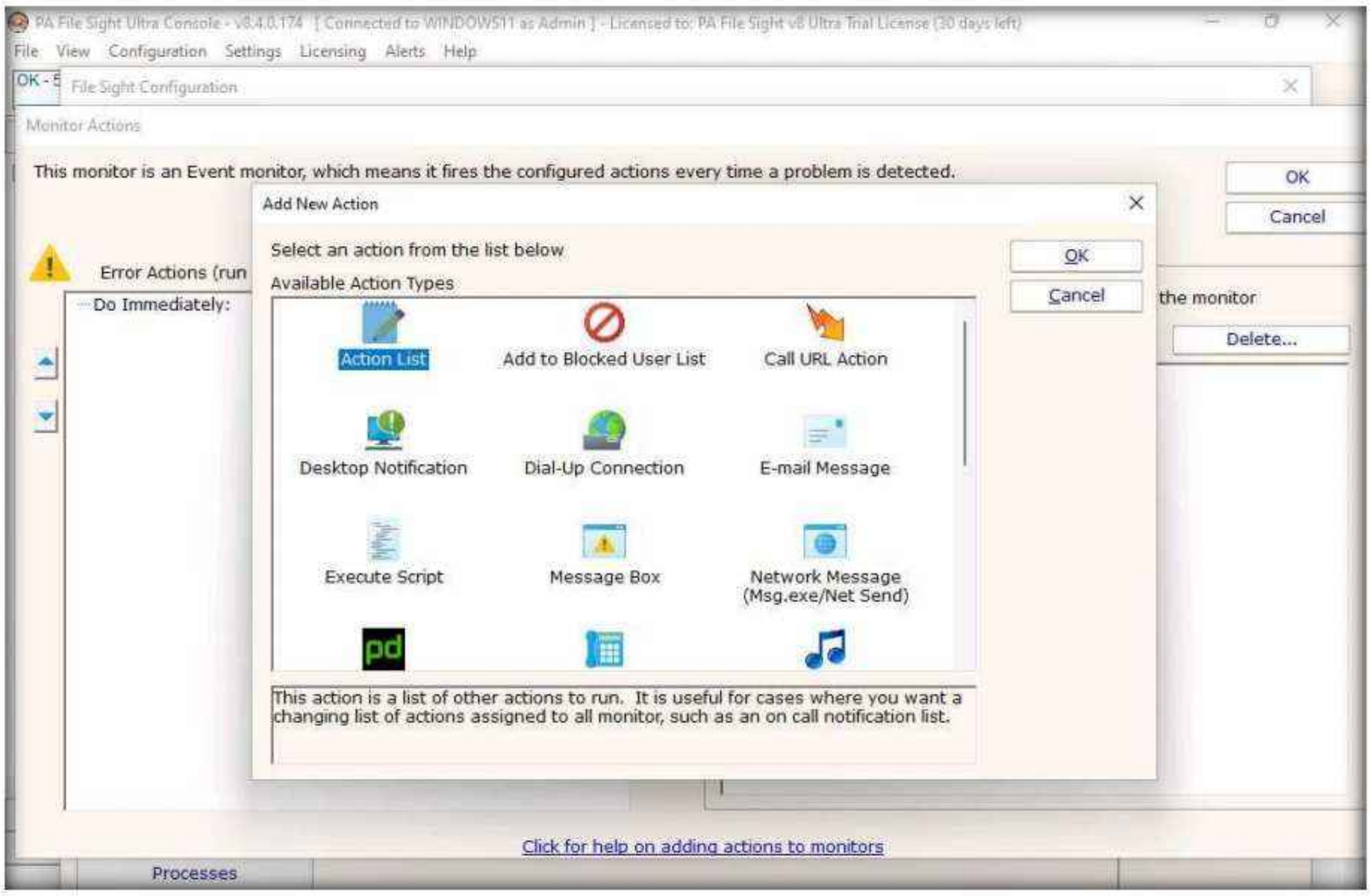
30. Choose **Audit file activity** from the **Monitor Purpose (for configuration help)** drop-down list, and then click **Actions**.



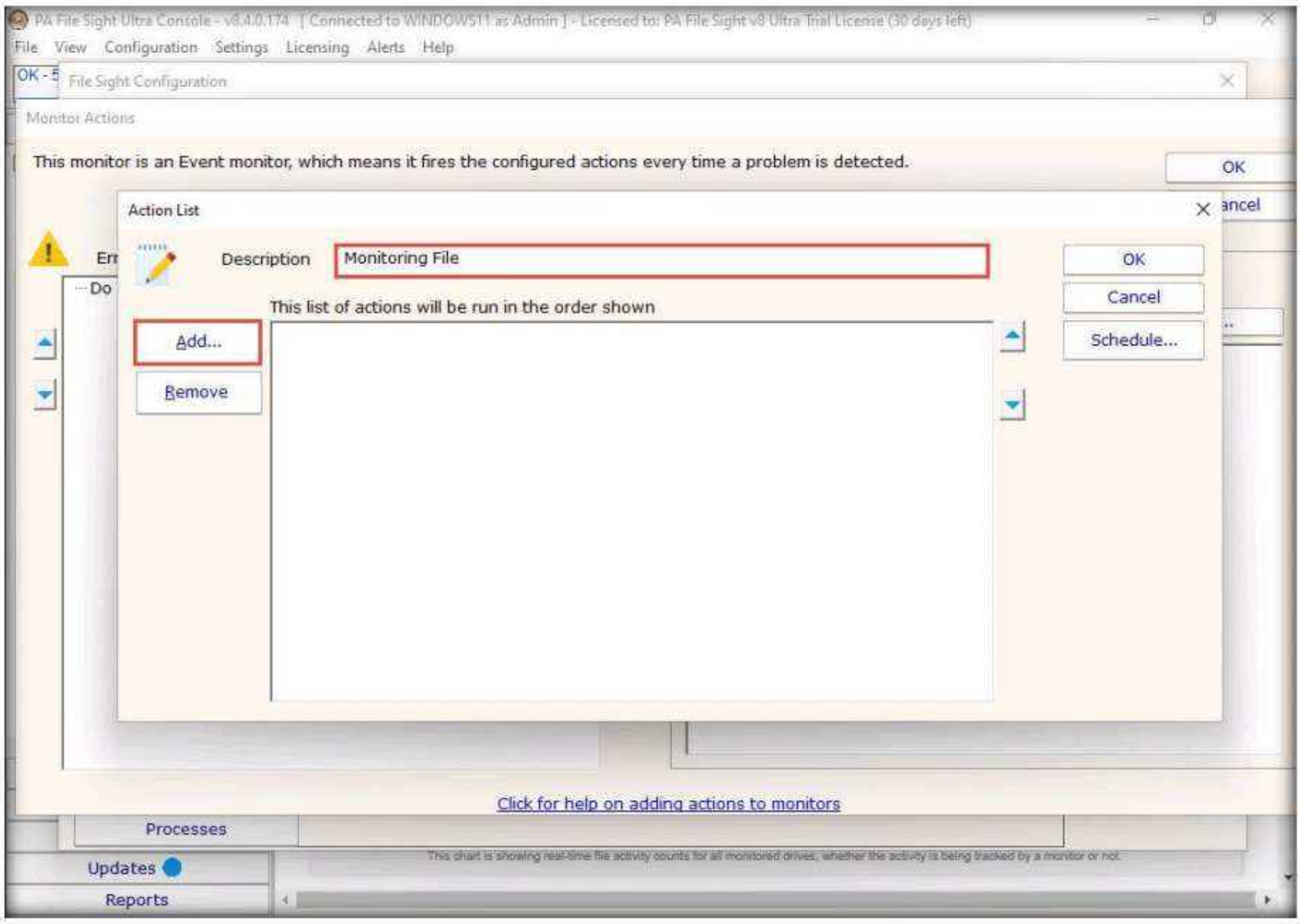
31. The **Monitor Actions** window appears; click **New** under **Global Action List**.



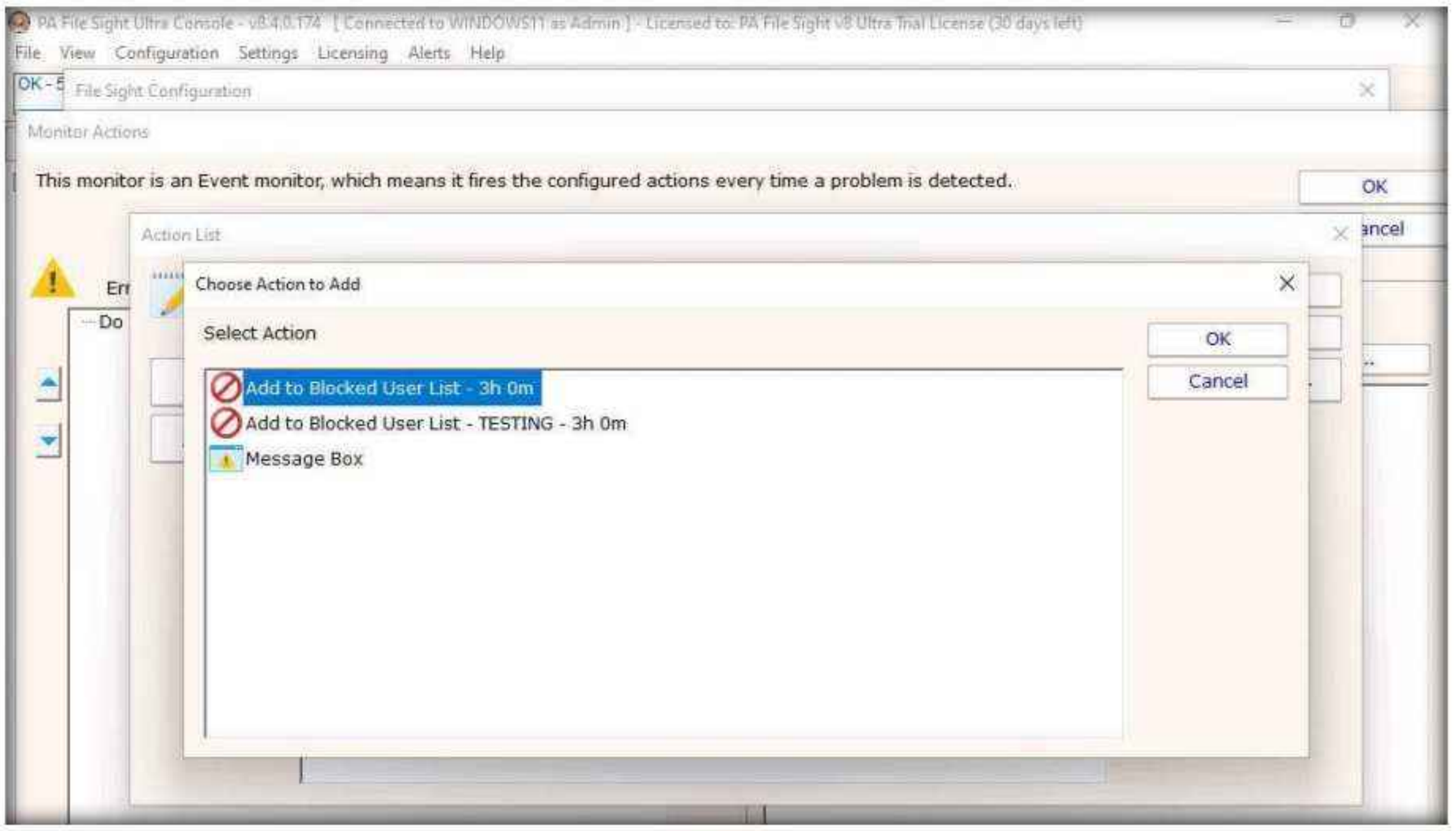
32. The **Add New Action** window appears. Select the **Action List** icon and click **OK**.



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

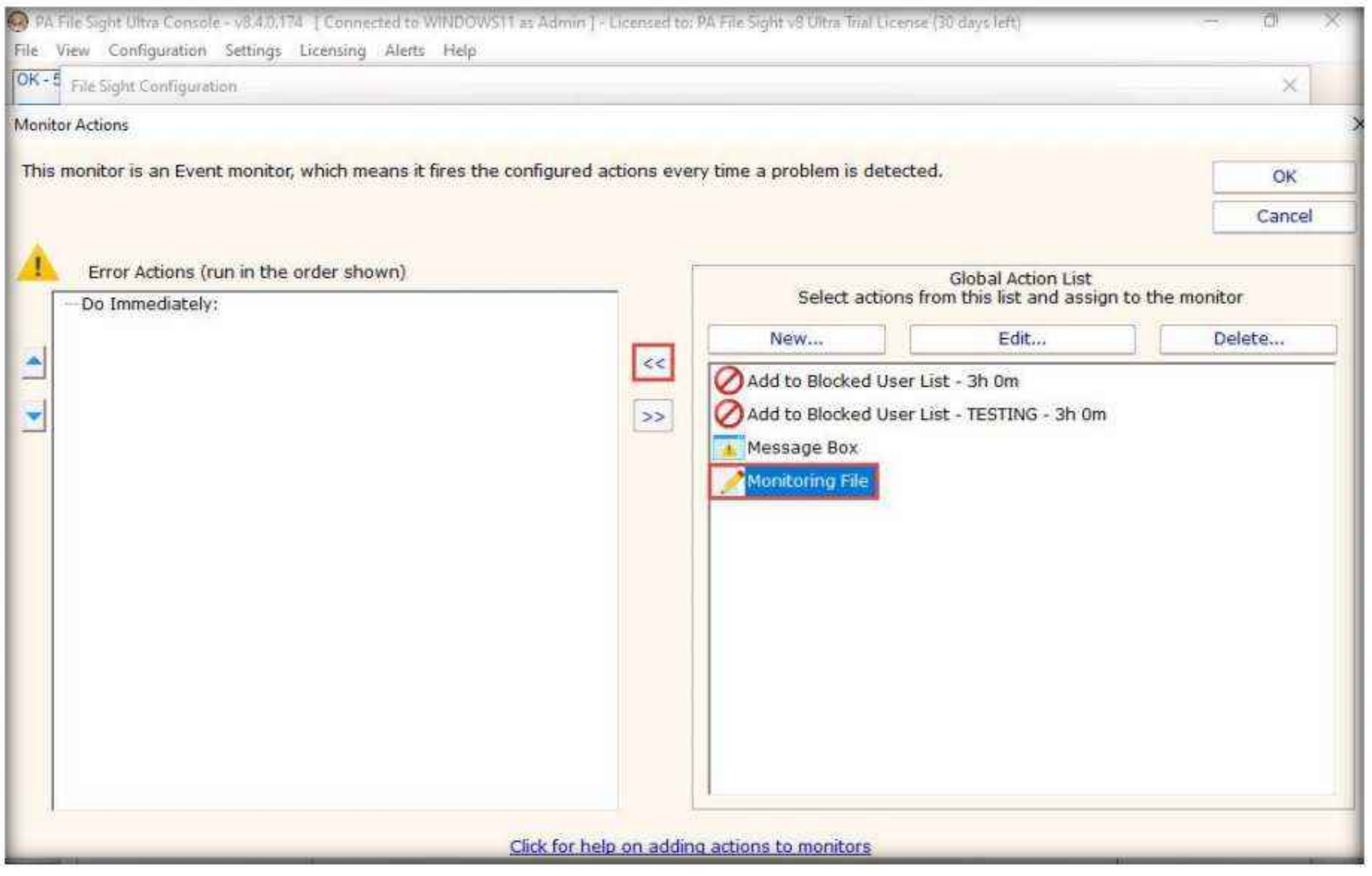


34. The **Choose Action to Add** window appears; choose any action from the list and click **OK**.

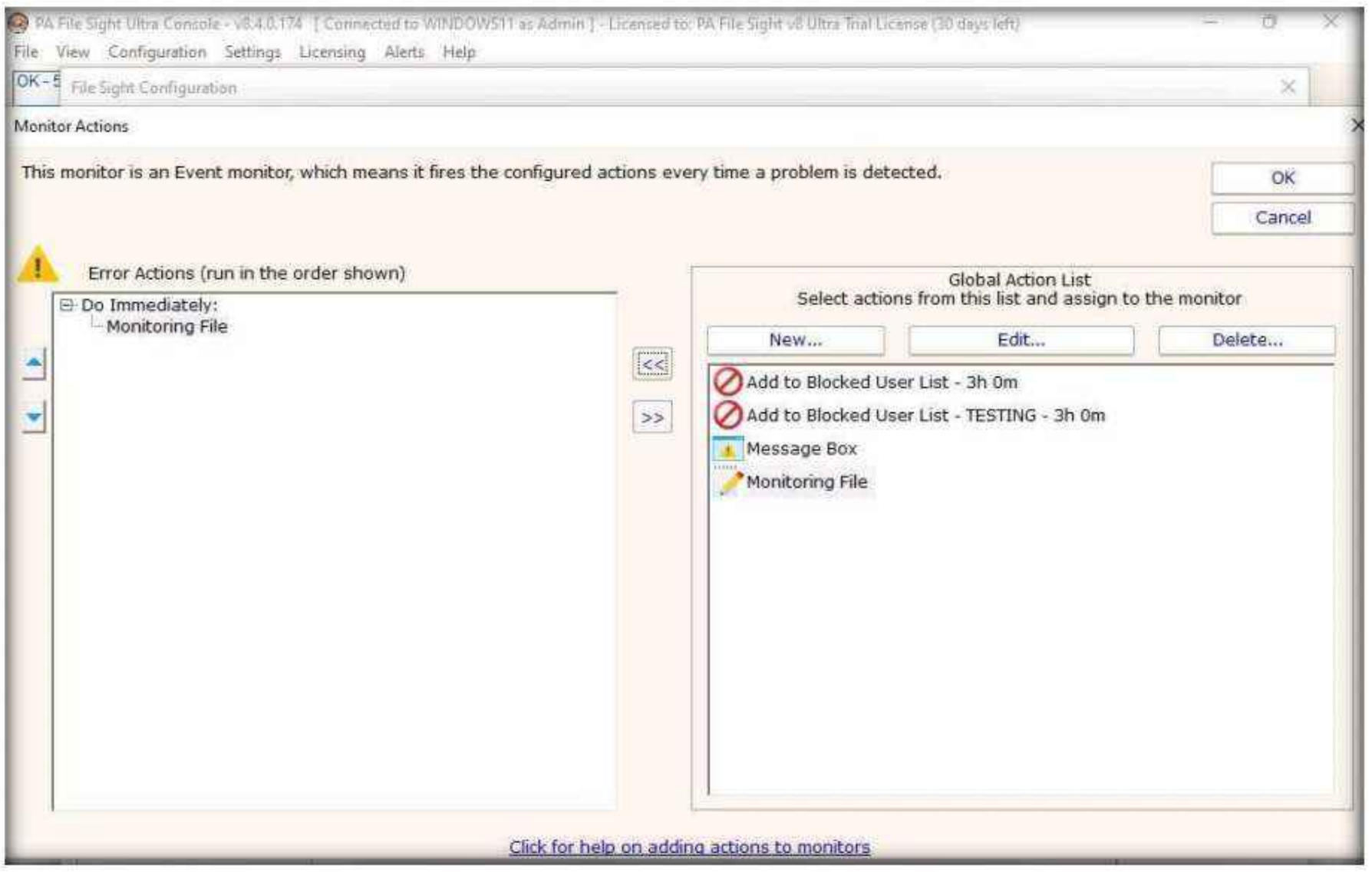


35. Click **OK** in the **Action List** window.

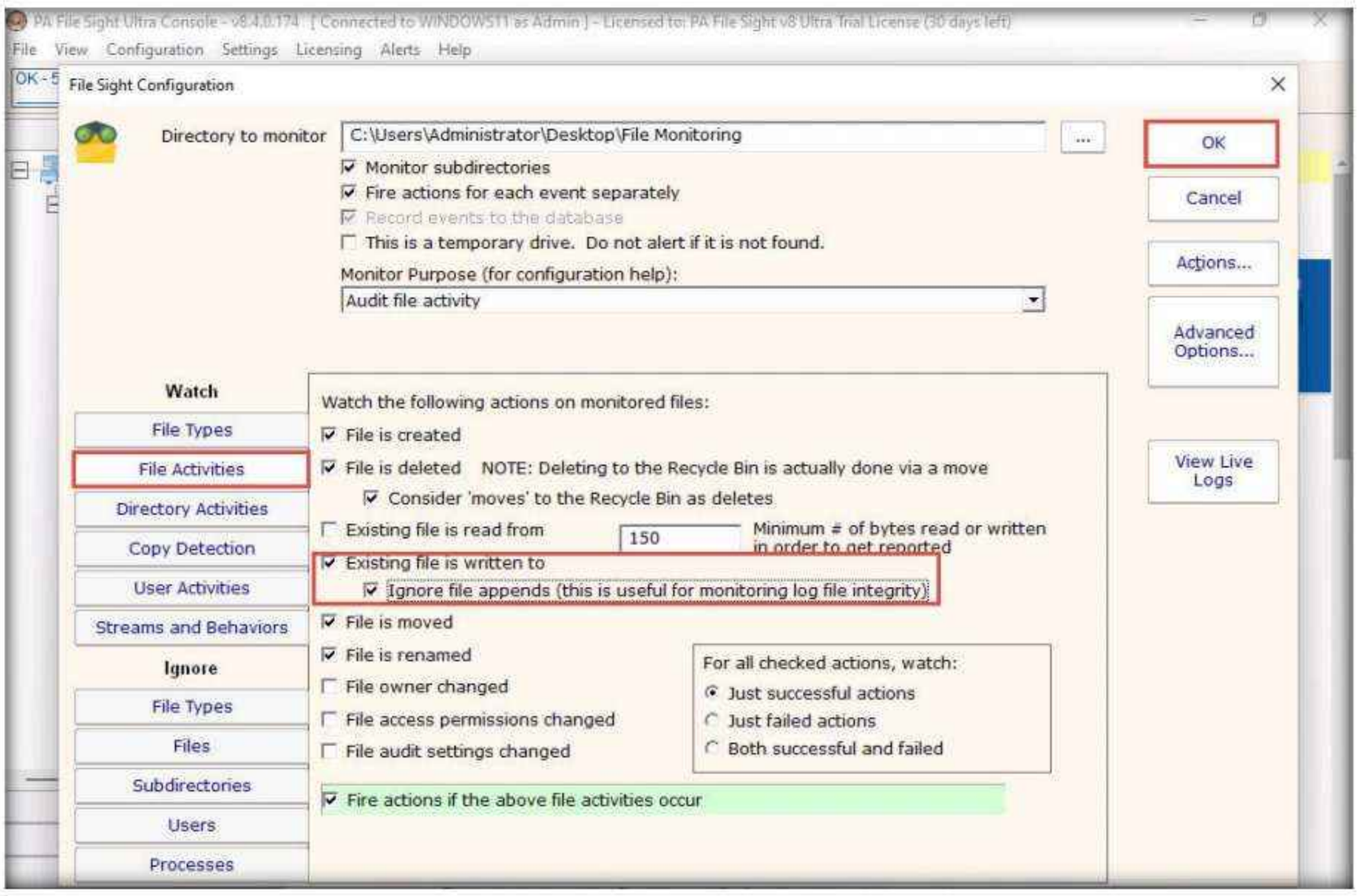
36. The **Monitor Actions** window appears; choose the newly created action (here, **Monitoring File**); and then click the **<<** icon to add the action.



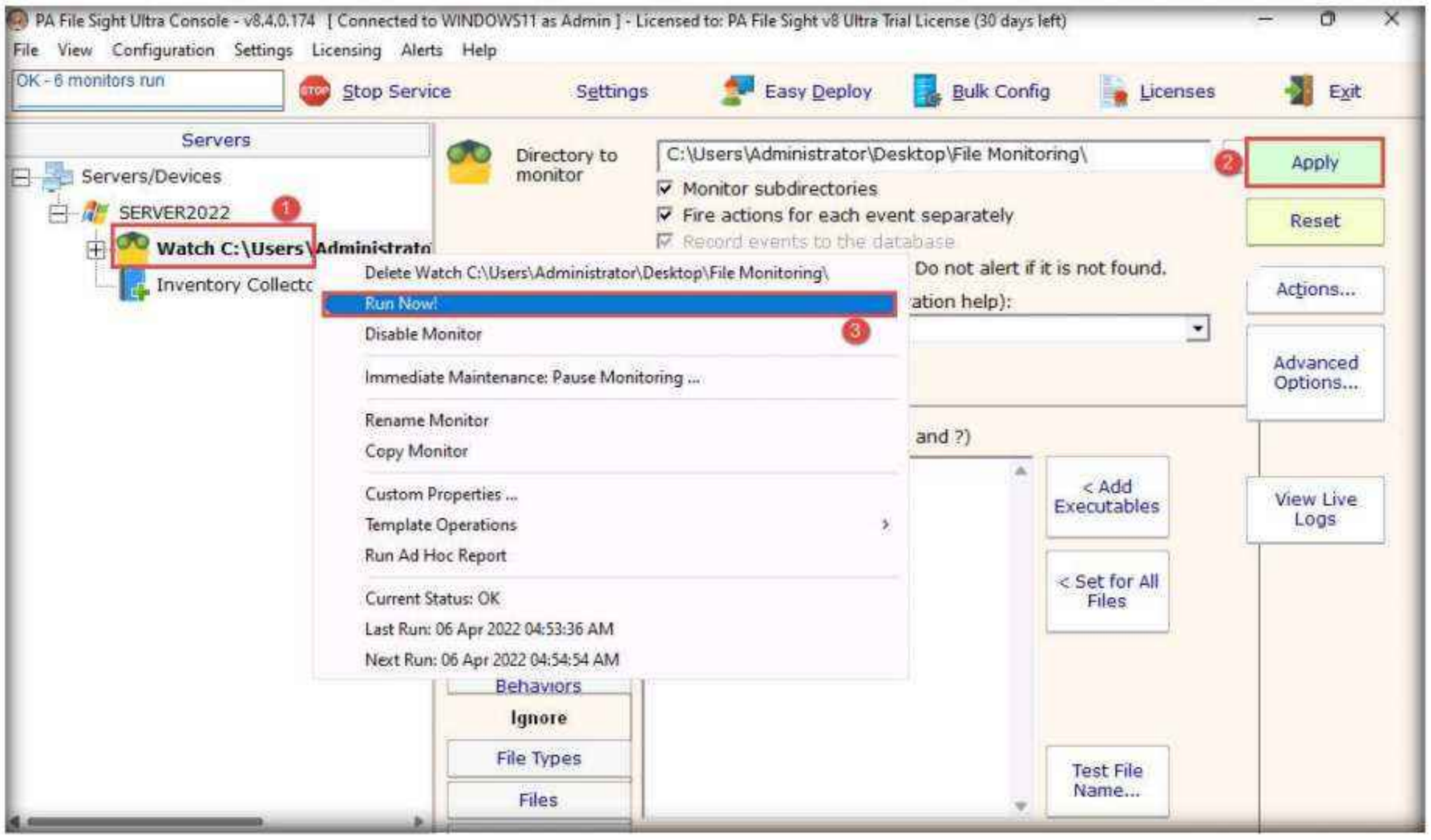
37. Once the action is added to the **Monitor Actions** window, click **OK**.



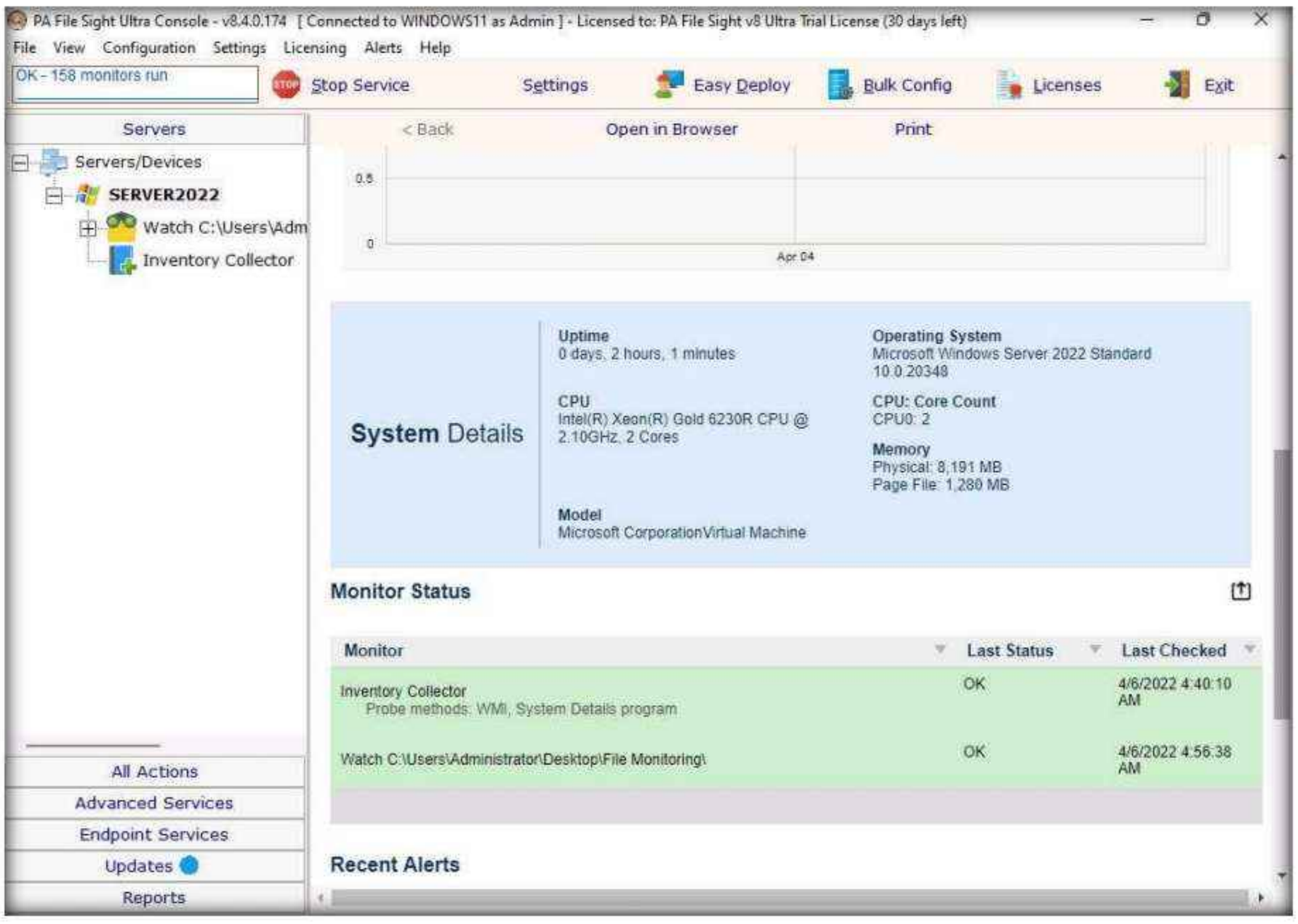
38. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.



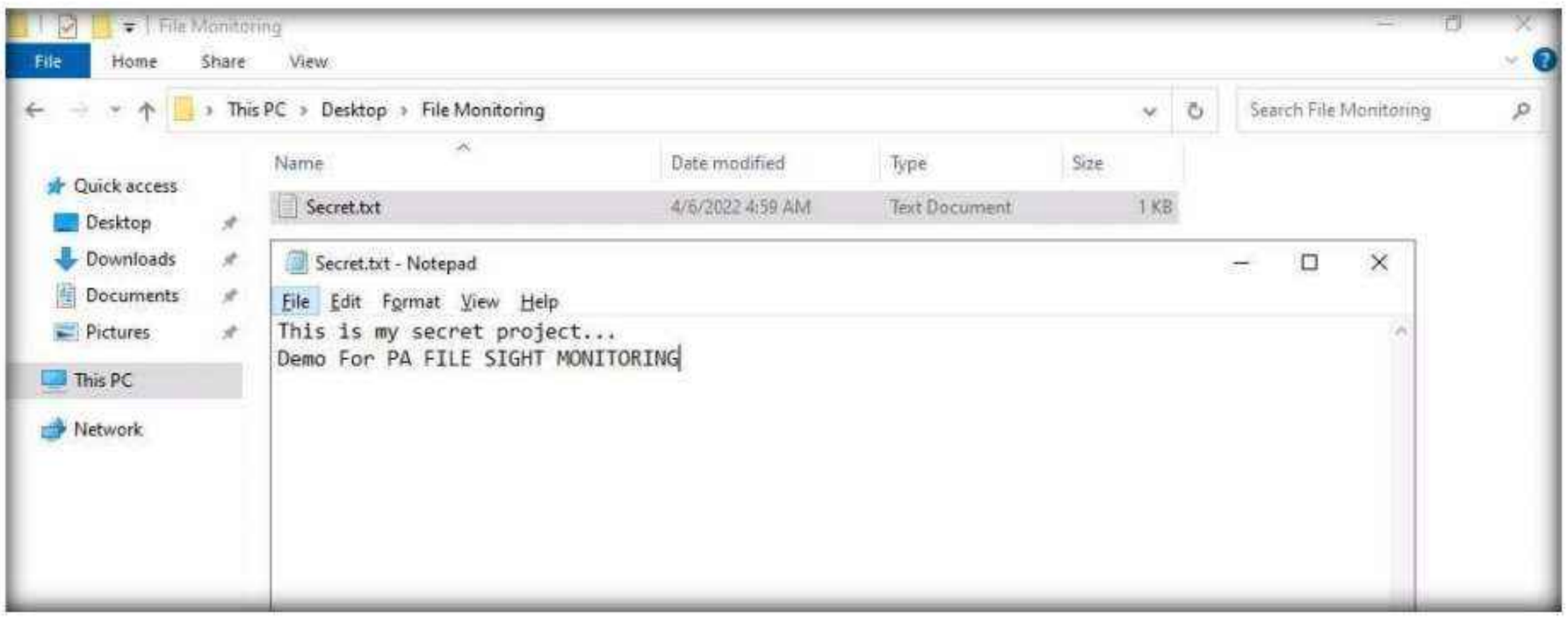
39. Under the **Server2022** node, **Watch** node will be added, select it and click **Apply** from the right-pane. Then right-click on the **File Monitoring** / **Watch** node and click **Run Now!** from the context menu.



40. Click the **Server2022** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.



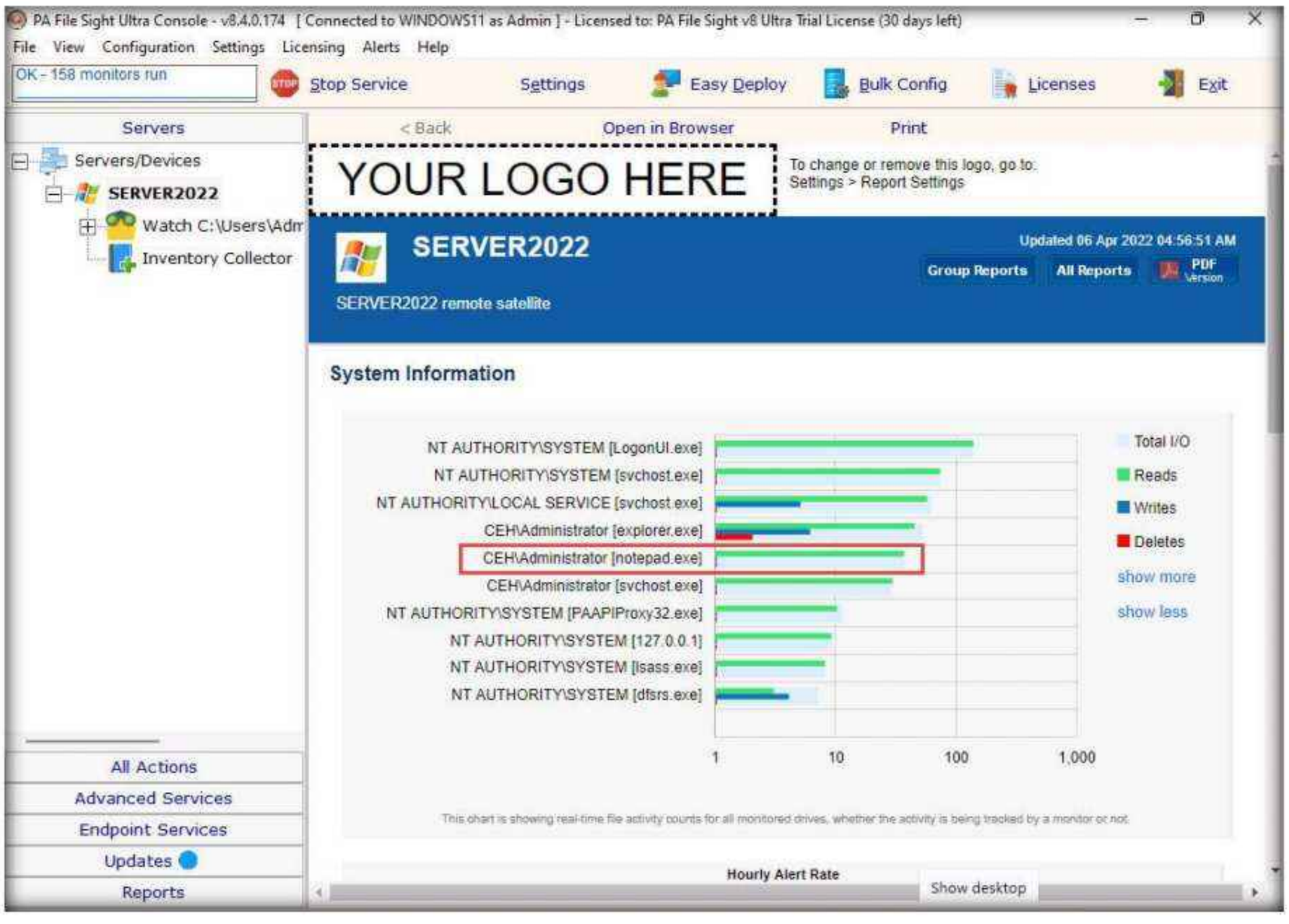
41. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**. Open **Secret.txt** in the **File Directory** on **Desktop**, modify some of the text in the file, and then **Save** and close the file.



42. Switch back to the **Windows 11** virtual machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.

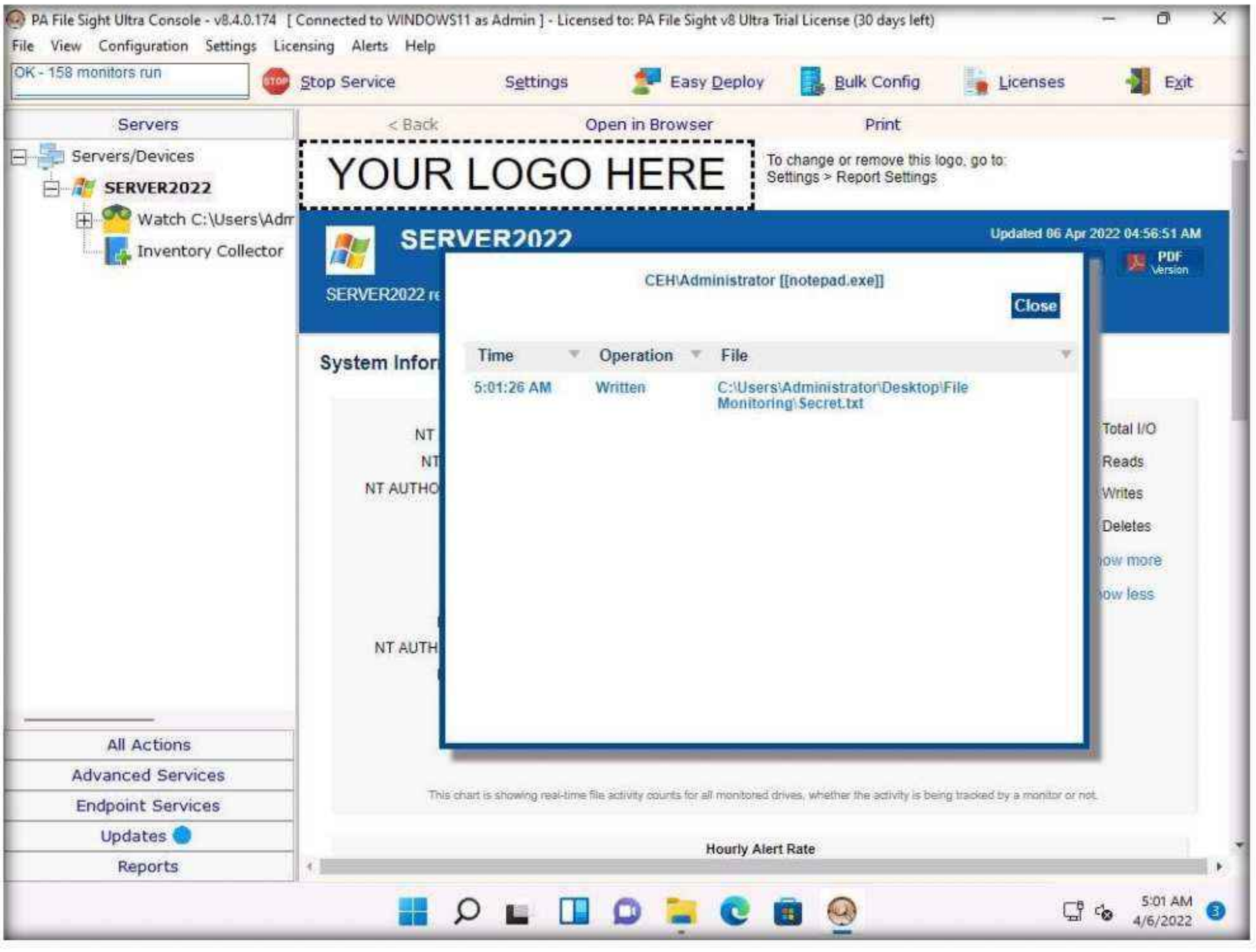
43. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.

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

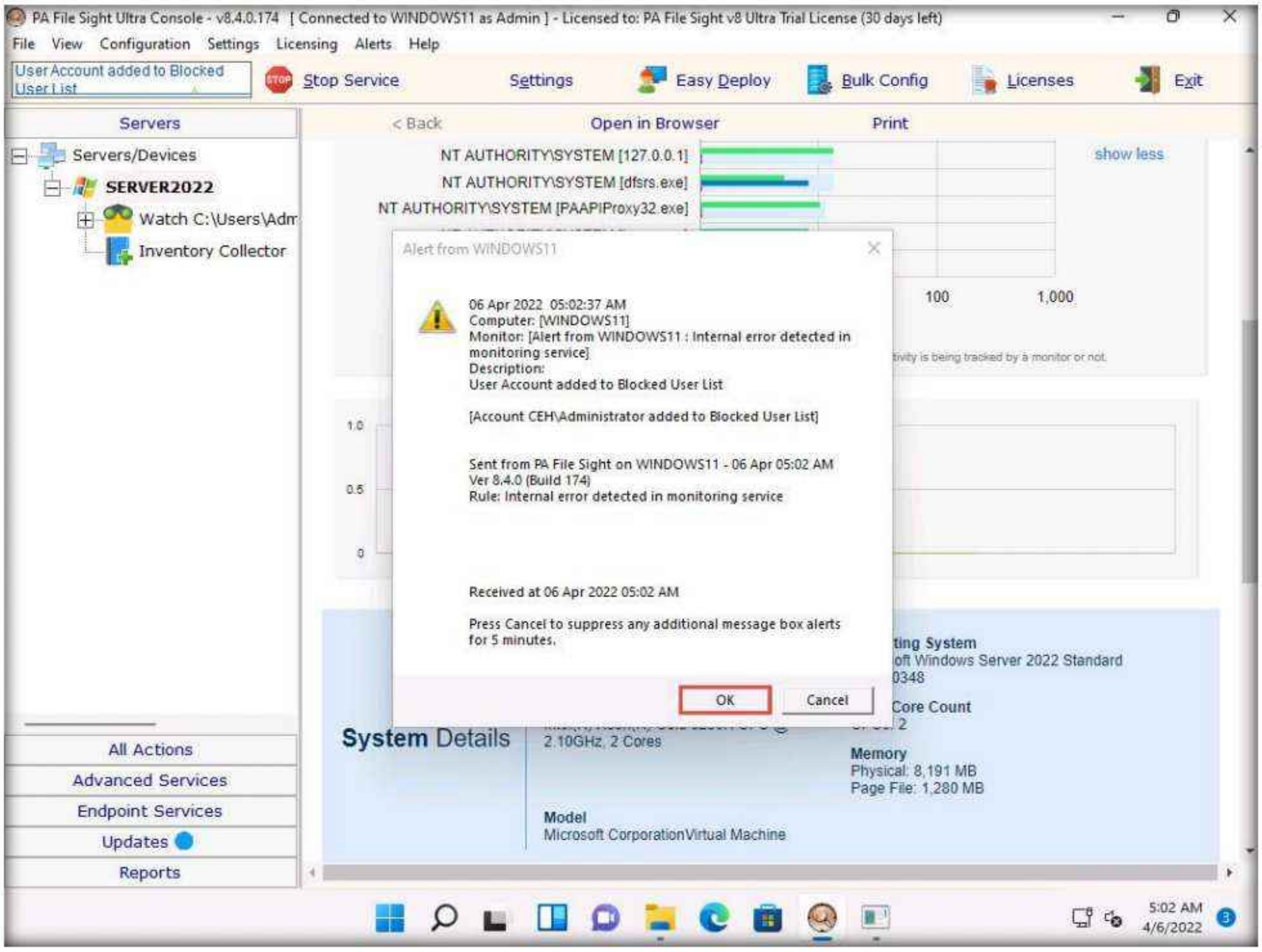


45. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then switch to the **Windows Server 2022** virtual machine, type some content into the **Secret.txt** file, save the file, and then immediately switch back to the **Windows 11** virtual machine to view the activity.

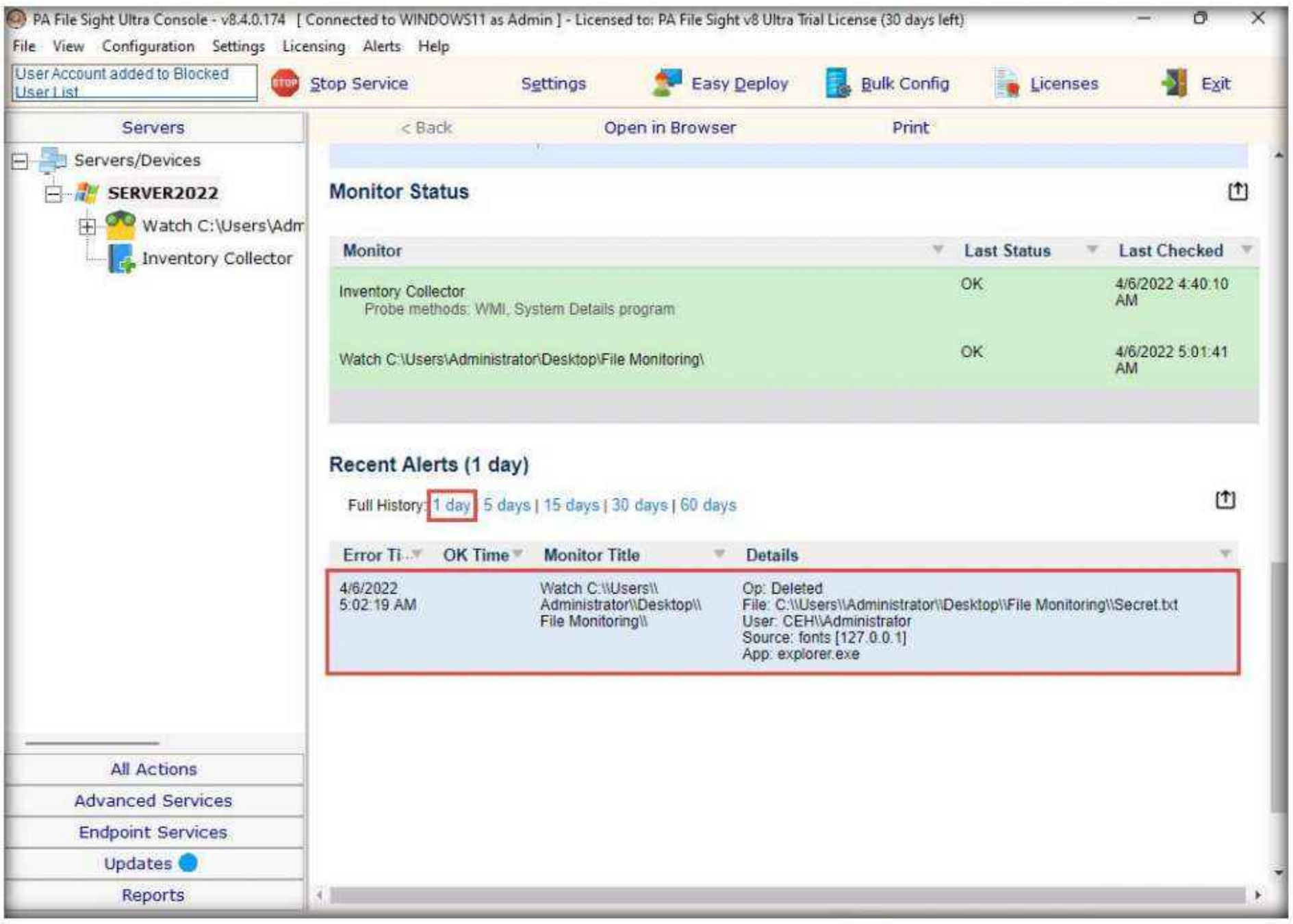
46. If you have added some text in the Secret.txt file, you can view that in the activity window.



47. Switch back to the **Windows Server 2022** virtual machine and delete the **Secret.txt** file, then switch back to the **Windows 11** virtual machine. Wait for a while and an **Alert from Windows11** pop-up appears, indicating an internal error, as shown in the screenshot.



48. Now, scroll down to view the **Recent Alerts** section; in the **Full History** option, select **1 day** link. You will find that the file has been deleted, as shown in the screenshot.



49. This is how to monitor the file integrity using PA File Sight.
50. Close all open windows.
51. 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.

Task 8: Perform Device Driver Monitoring using DriverView and Driver Reviver

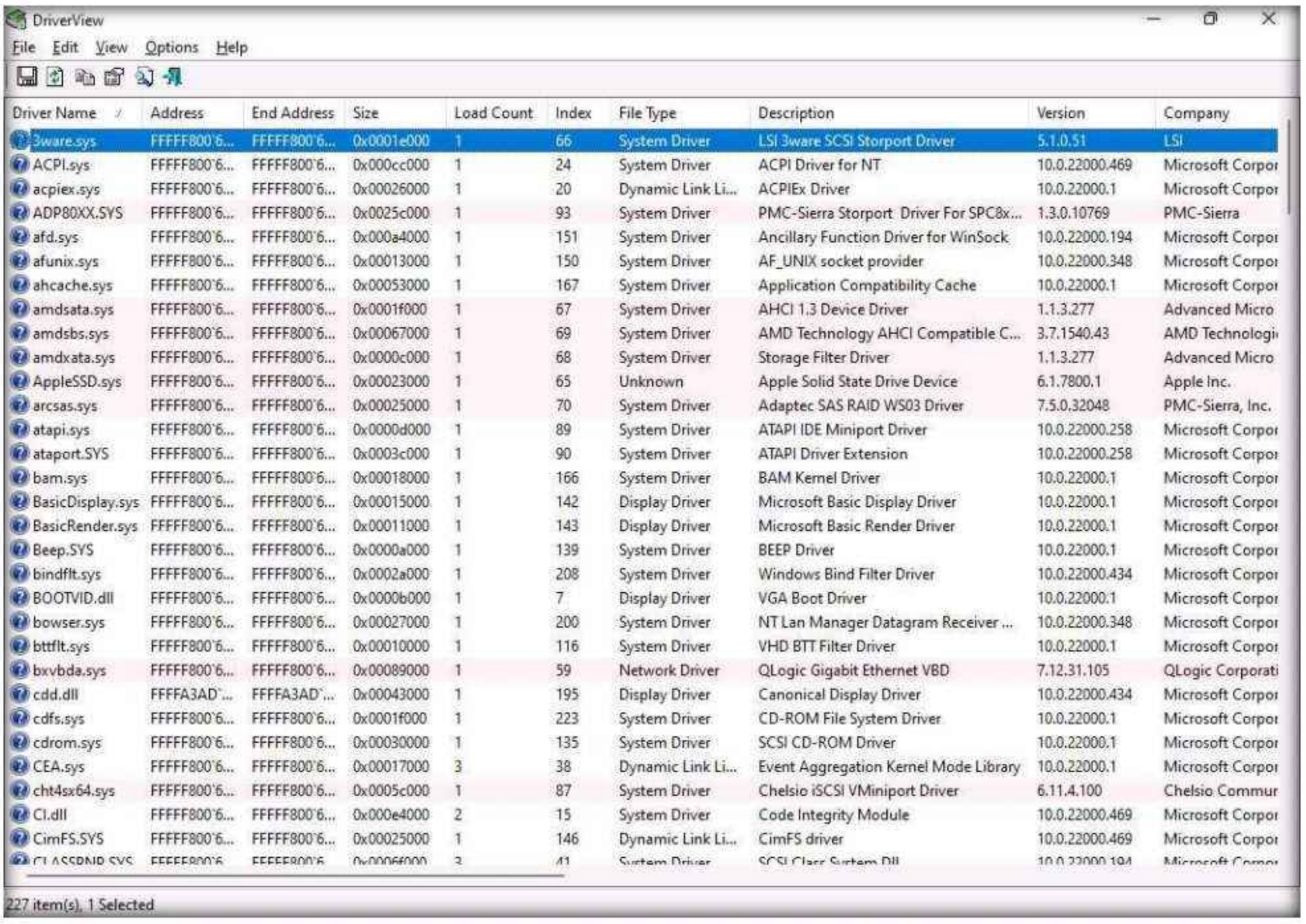
When the user downloads infected drivers from untrusted sources, the system installs malware along with the device drivers; malware uses these drivers as a shield to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Reviver that verify if they are genuine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

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.

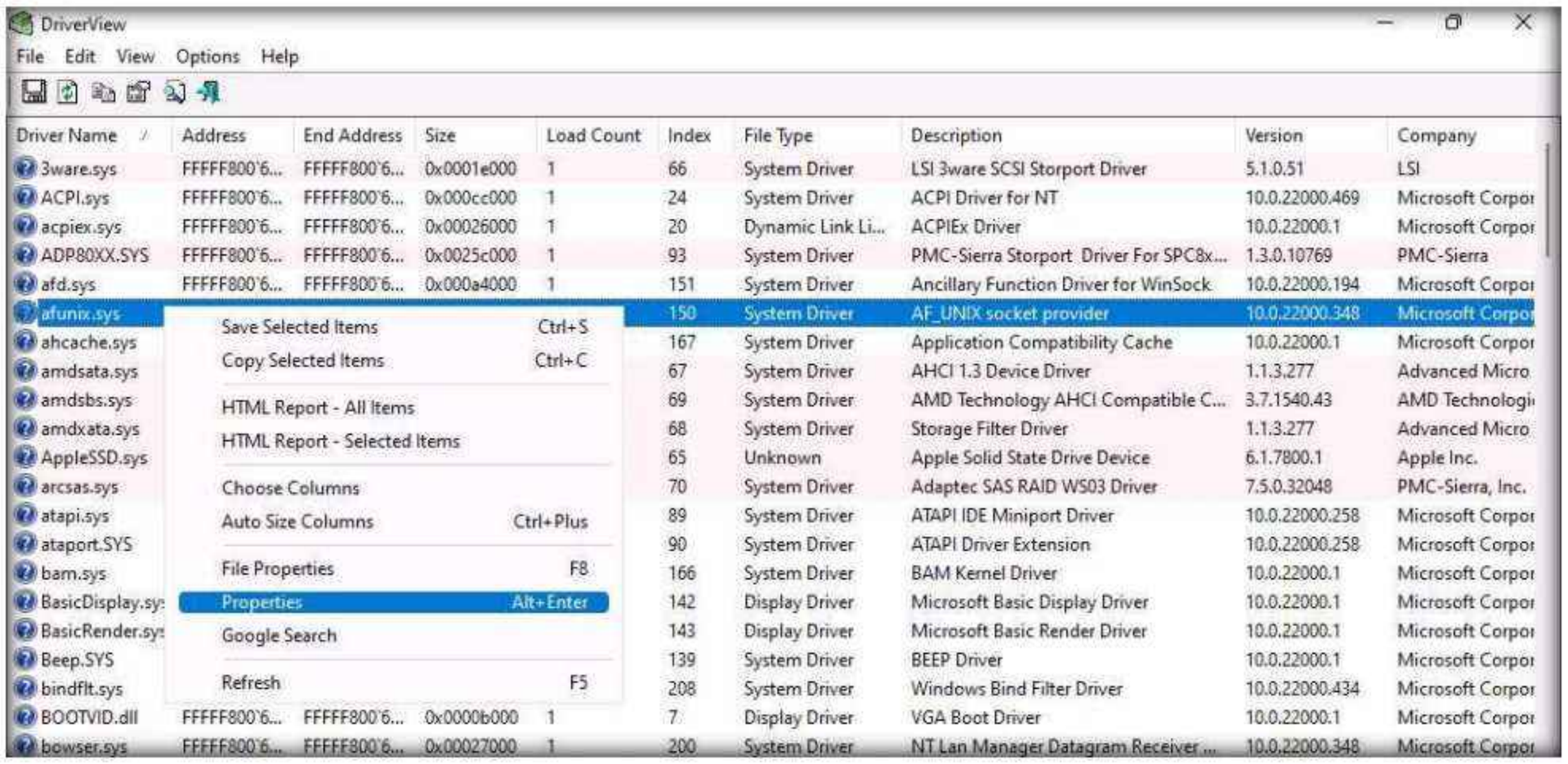
Driver Reviver: Without proper drivers, computers start to misbehave. Sometimes updating the drivers using conventional methods can be a daunting task. Outdated drivers are more vulnerable to hacking and can lead to a breach in the system. Driver Reviver provides an effective way of scanning your PC to identify out of date drivers. Driver Reviver can quickly and easily update these drivers to restore optimum performance to your PC and its hardware and extend its life.

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.

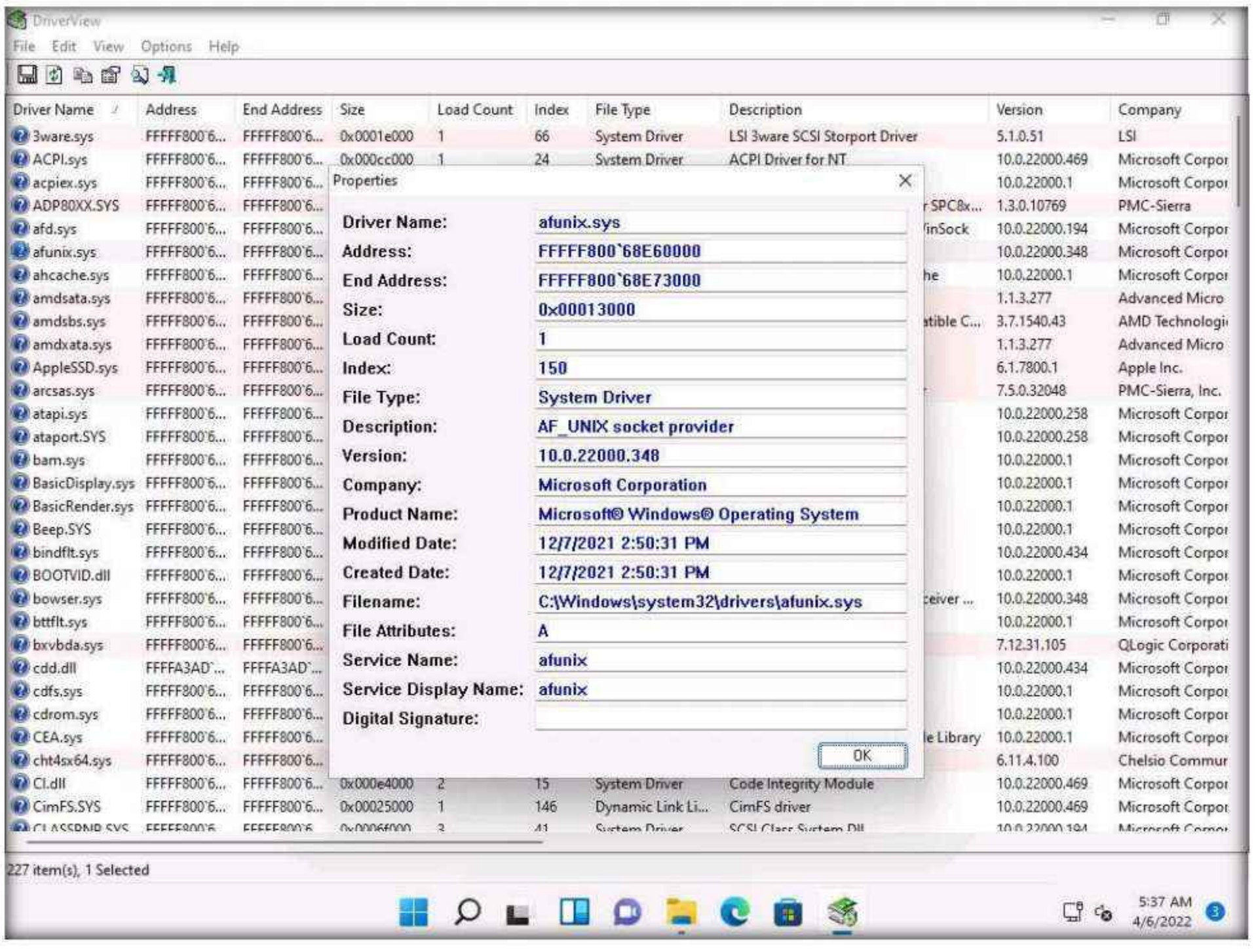
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView** and double-click **DriverView.exe** to launch the application.
2. The **DriverView** main window appears with a list of the installed drivers on your system, as shown in the screenshot.



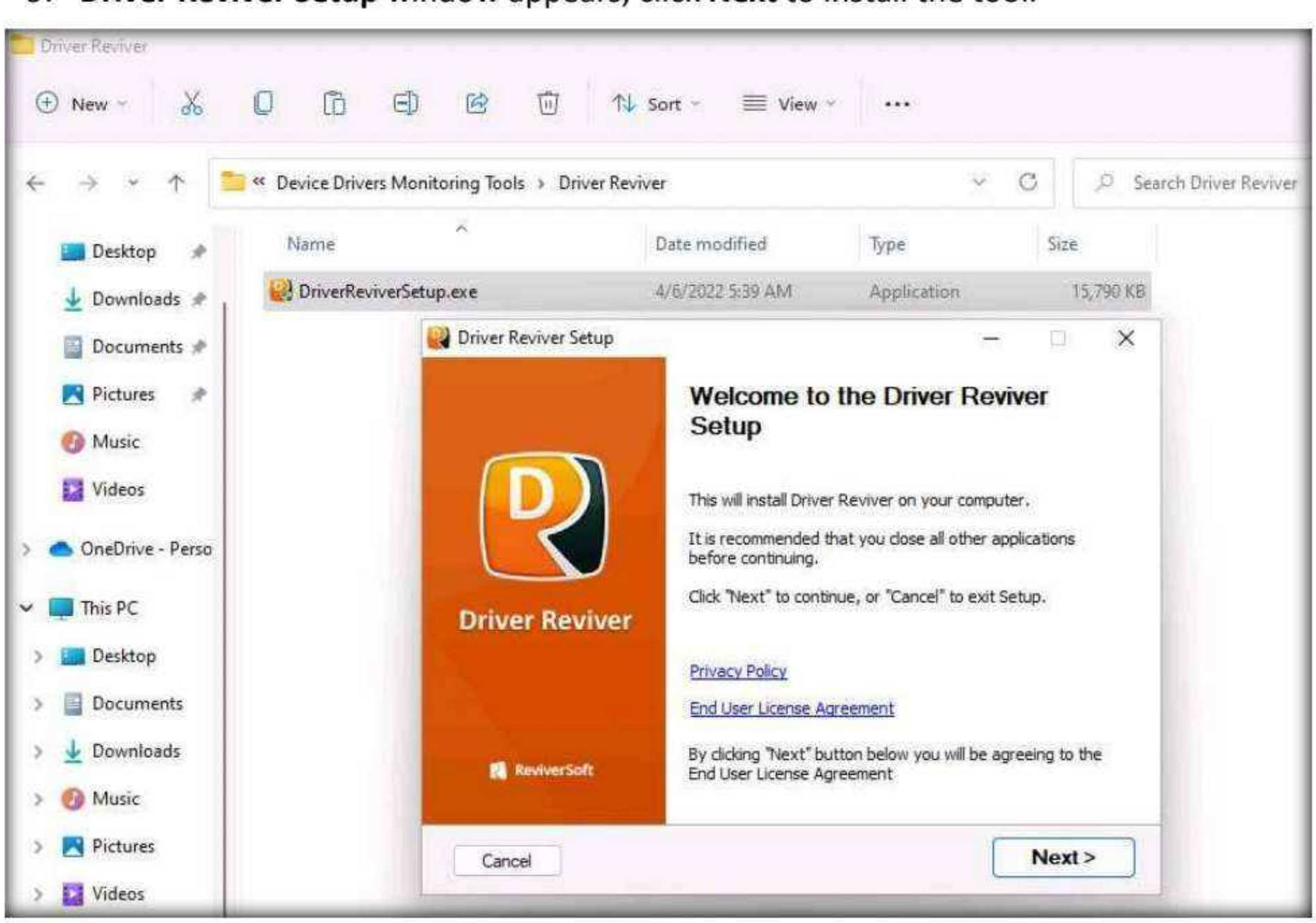
3. Right-click on any driver from the list and click **Properties** to view the complete details of the driver.



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**.



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 Reviver.
7. On **Windows 11**, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Reviver**. Double-click **DriverReviverSetup.exe** to launch the setup.
8. If a **User Account Control** window appears, click **Yes**.
9. **Driver Reviver Setup** window appears, click **Next** to install the tool.



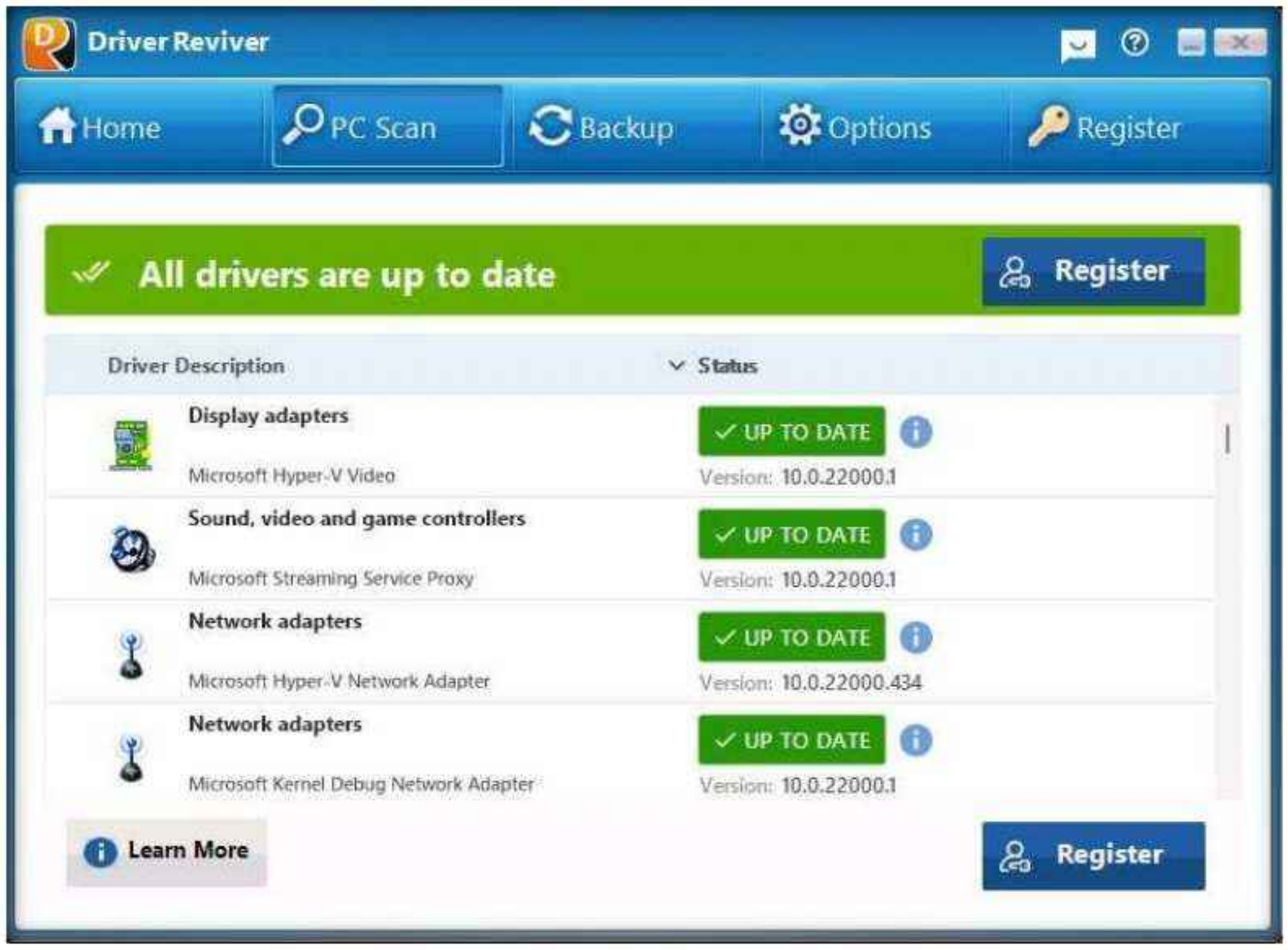
10. Installation window appears and after the completion of installation, Driver Reviver initializes the scan for drivers, as shown in the screenshot.

    Note: If a browser window opens automatically close the browser.

11. After the scan finishes, a list of system drivers are displayed.
12. Along with the list of drivers you can see their **Status** as **OUTDATED** or **UP TO DATE**.

    Note: Here, all the drivers are already up to date.

    Note: The result might vary when you perform this task.



13. If the drivers are outdated, then you can click **Update All** button to update all the drivers.

14. Now, navigate to the **Home** tab, here you can view information such as **System details**, **System**, **Processor**, **Graphics**, **Memory(RAM)** and **Hard Drives**, as shown in the screenshot,

15. Navigate to the **Backup** tab, here you can create Backup or Restore the system drivers.

16. Uninstall the **Driver Reviver** software by navigating to **Control Panel → Programs → Uninstall a program**.

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

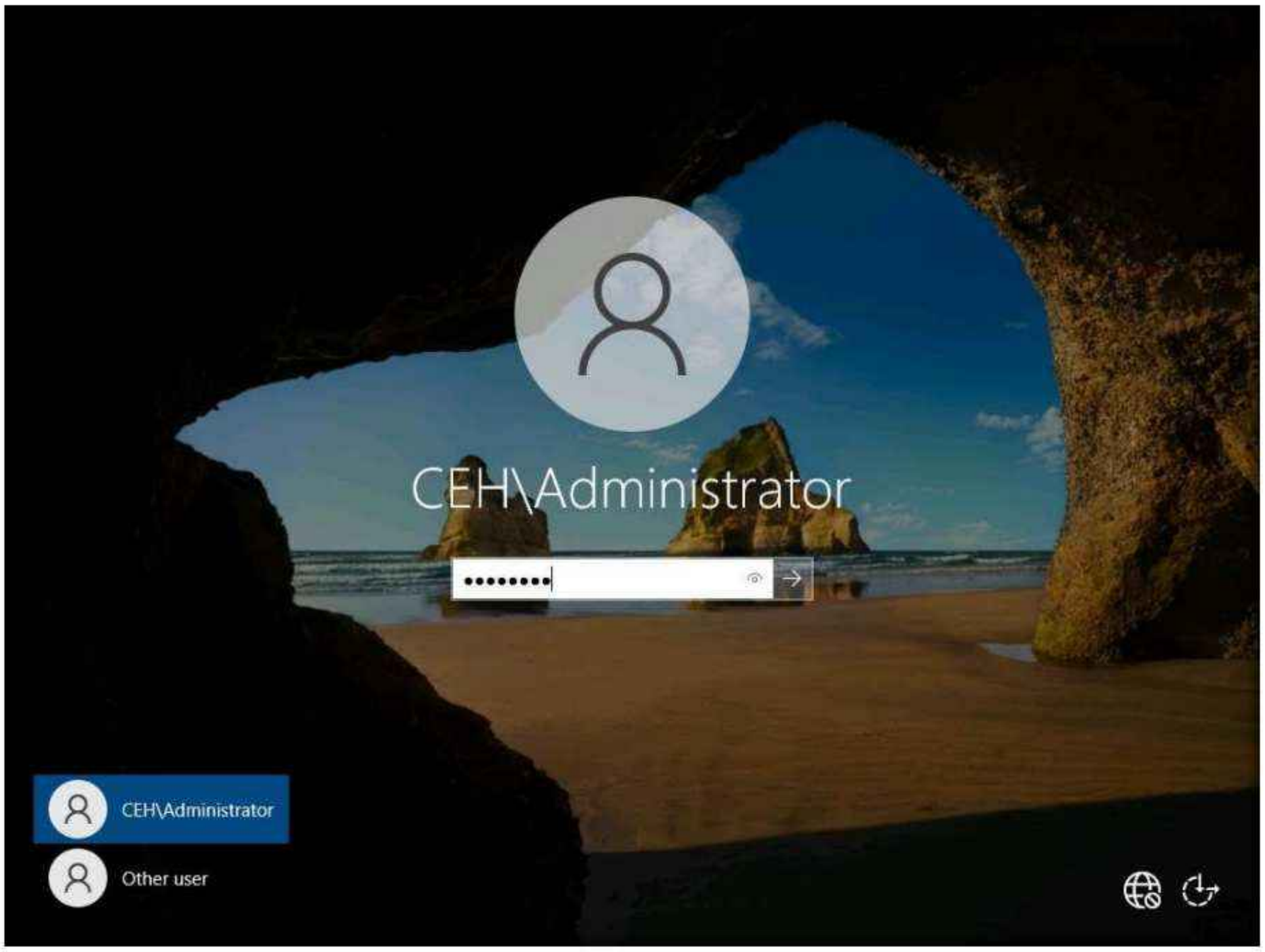
17. Close all open windows.

18. You can also use other device driver monitoring tools such as **Driver Booster** (https://www.iobit.com), **Driver Easy** (https://www.drivereasy.com), **Driver Fusion** (https://treexy.com), or **Driver Genius 22** (https://www.driver-soft.com) to perform device driver monitoring.

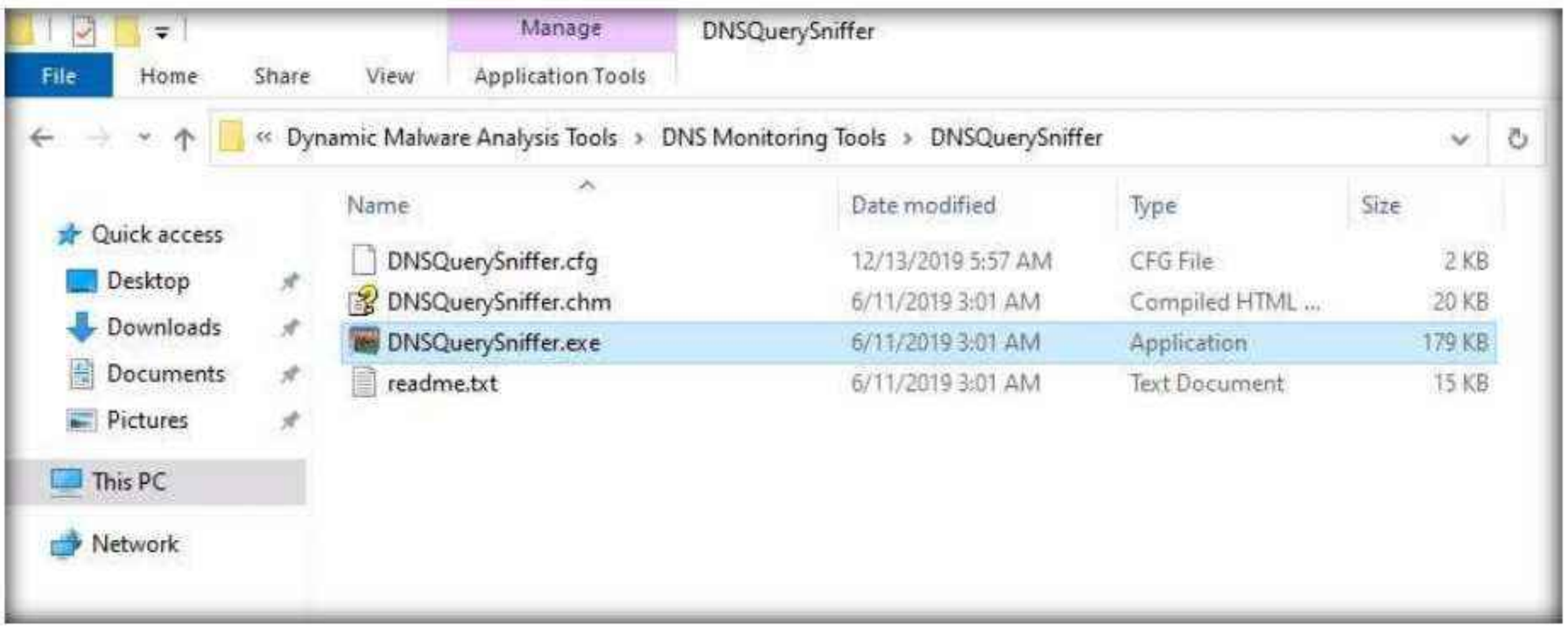
Task 9: Perform DNS Monitoring using DNSQuerySniffer

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.

1. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.



2. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**, and then double-click **DNSQuerySniffer.exe**.

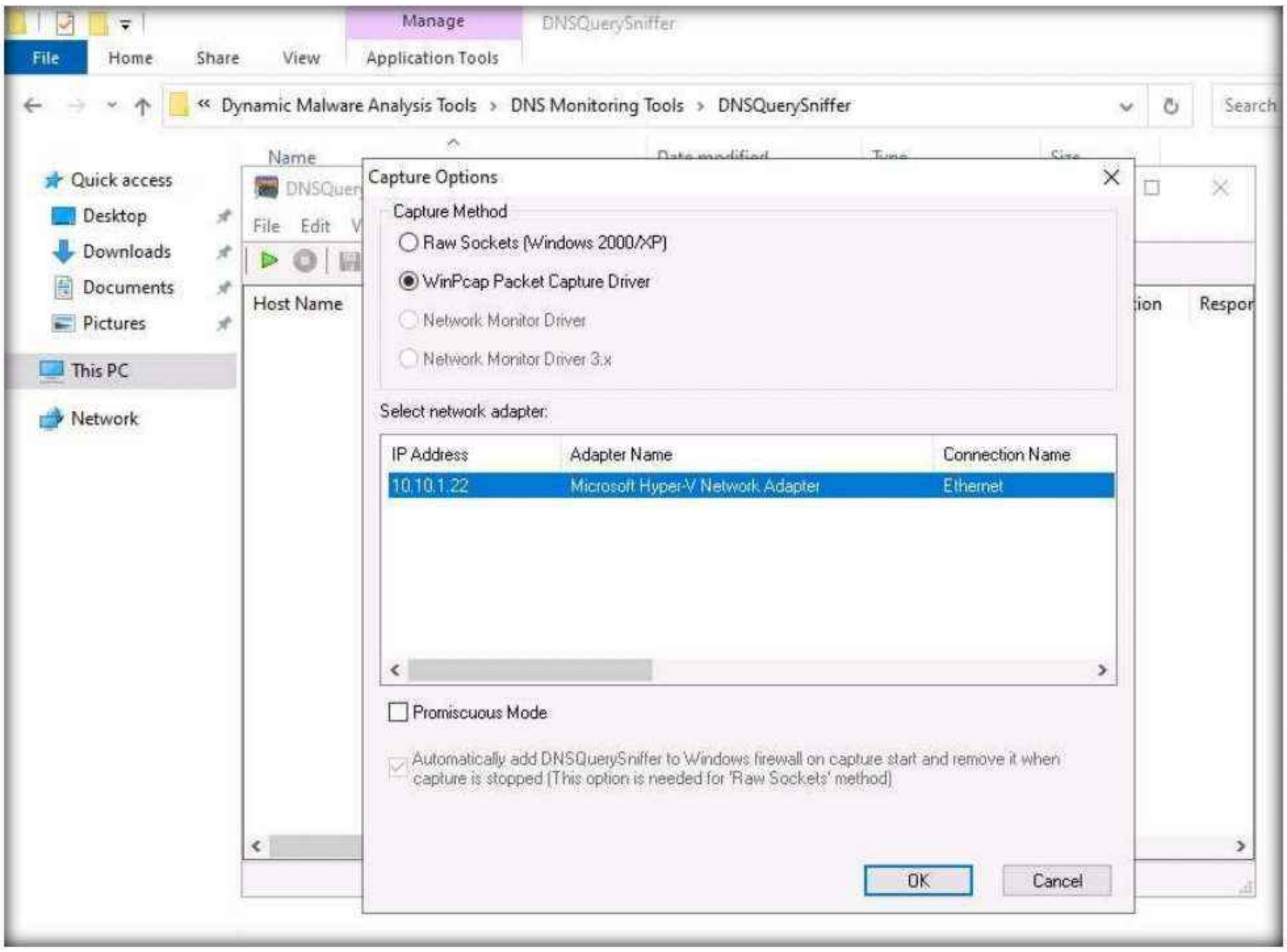


3. The main window of **DNSQuerySniffer** appears, along with the **Capture Options** window.

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

4. In the **Capture Options** window, ensure that the **WinPcap Packet Capture Driver** option is selected under the **Capture Method** field.

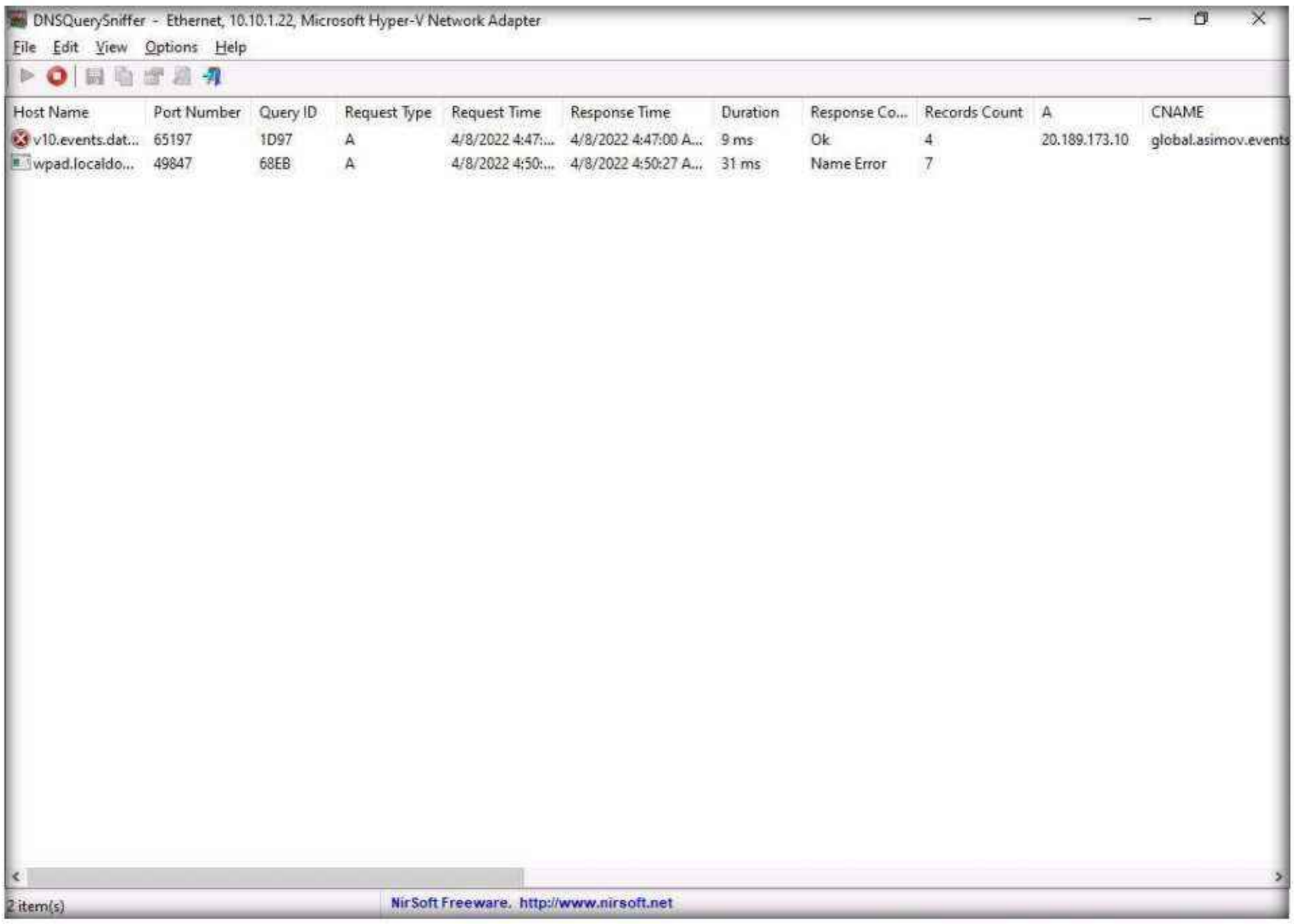
5. In the Select network adapter section, select the **Windows Server 2022** network adapter (here, **Ethernet**).
6. Click **OK** to start sniffing.

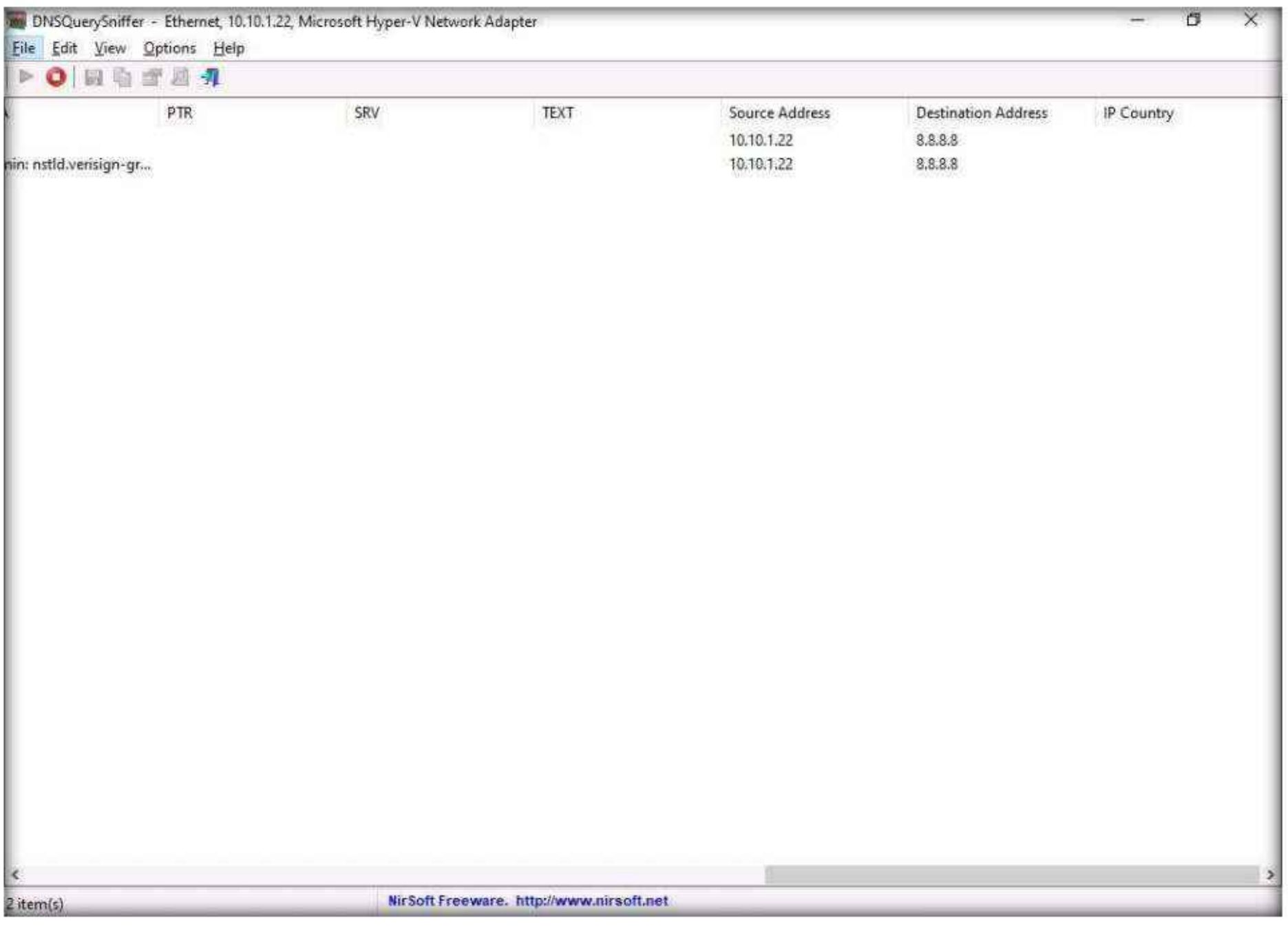


7. The DNSQuerySniffer starts monitoring the network traffic and takes some time to capture the traffic. Leave the window intact. It shows the DNS queries sent on your system along with its complete information such as host name, port number, request time, response time, duration, source address, and destination address, as shown in the screenshot.

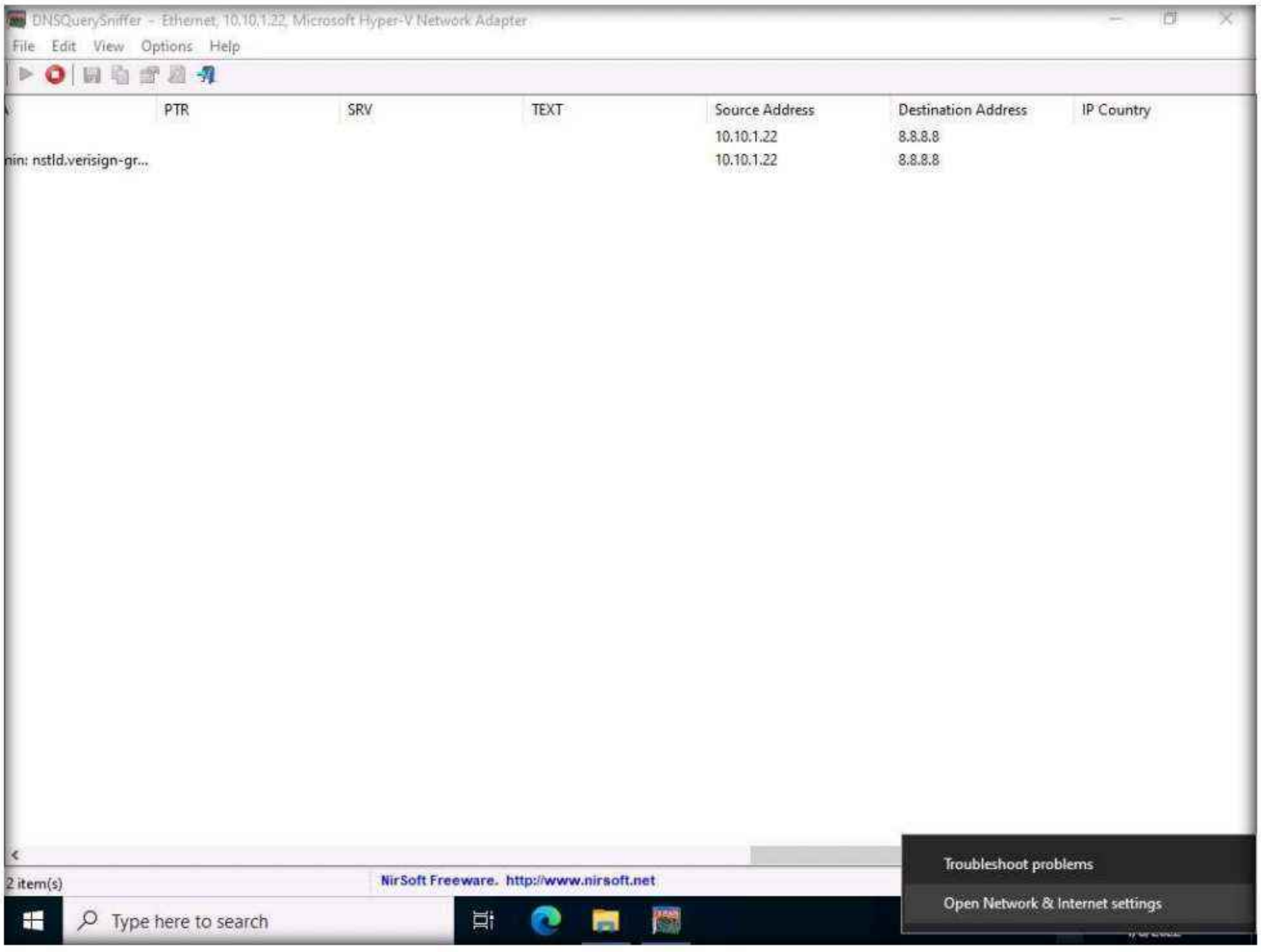
Note: It takes approximately 5 minutes to capture the traffic.

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

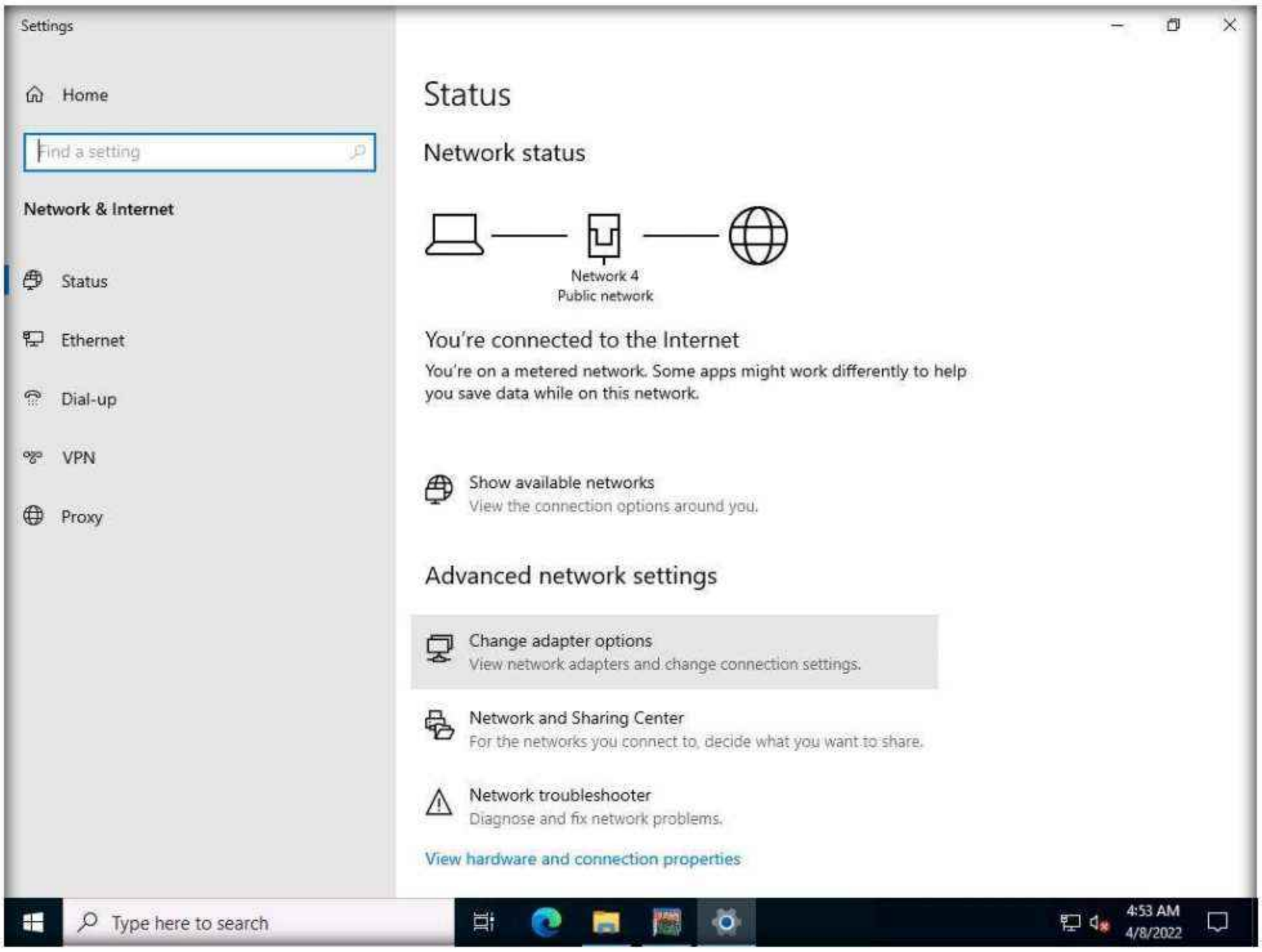




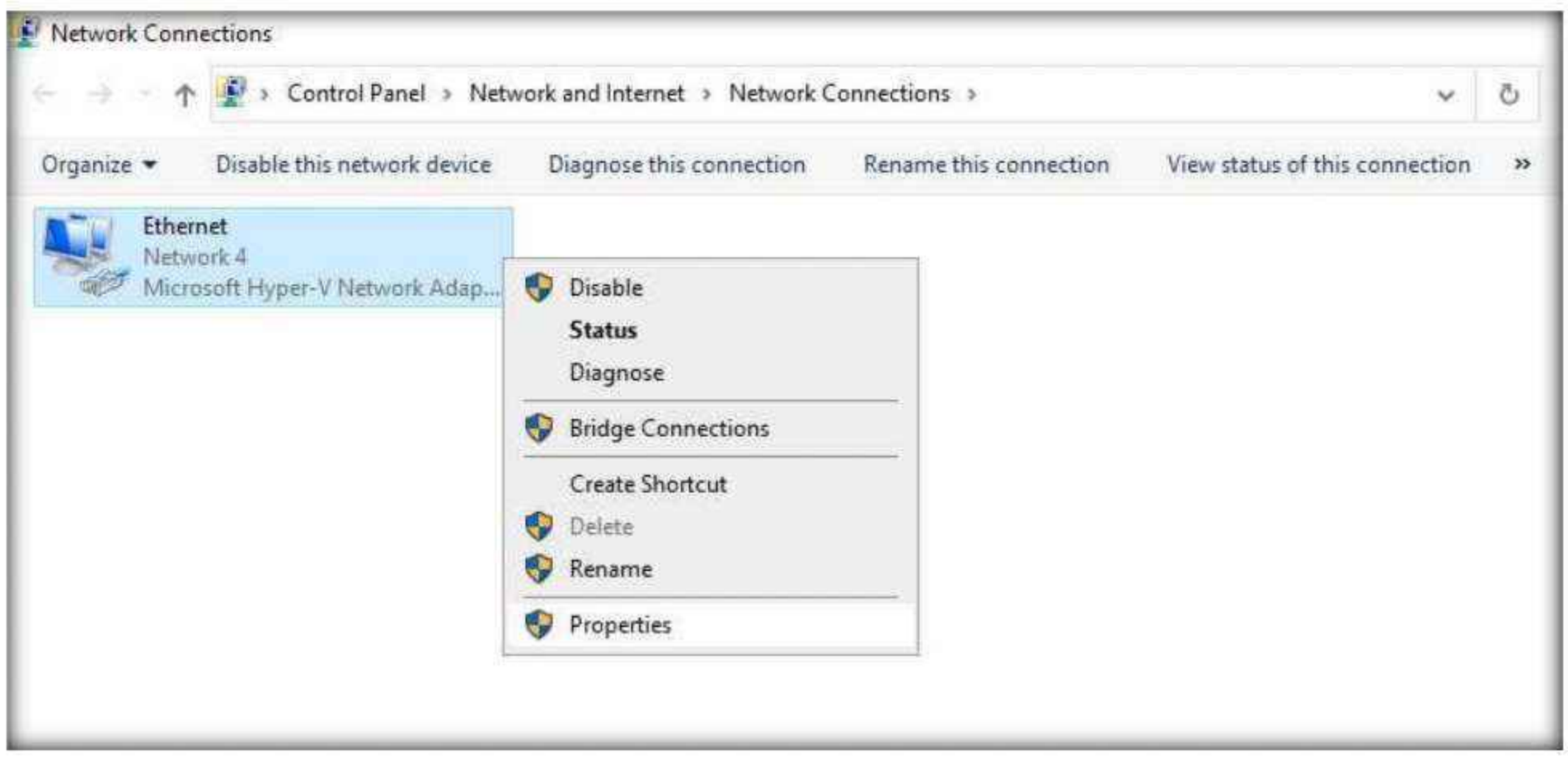
8. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
9. In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine. For demonstration purposes, we are changing the DNS of the **Windows Server 2022** machine in the **Network & Internet settings**.
10. Right-click on the **Network** icon in the lower-right corner of Desktop and click **Open Network & Internet settings**.



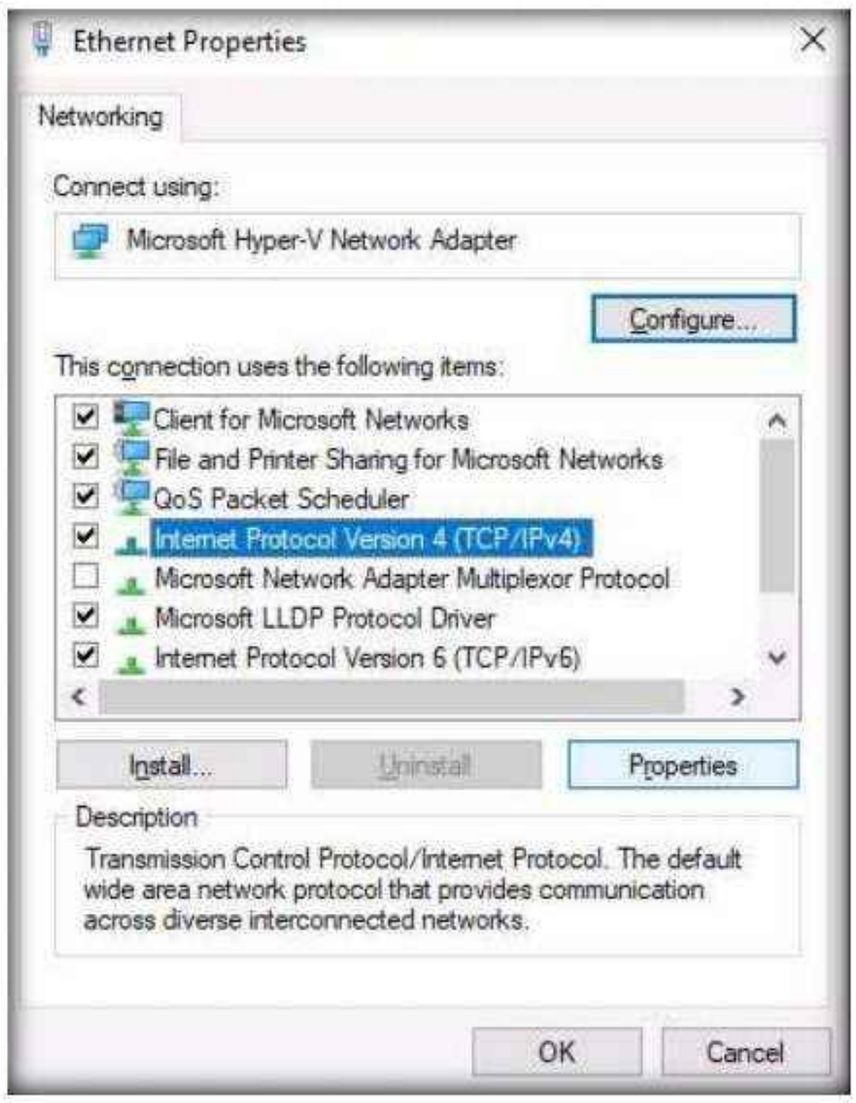
11. The **Network Status** window appears. Click **Change adapter options** under **Change your network settings**.



12. Right-click on the network adapter (here, **Ethernet**) and click **Properties**.

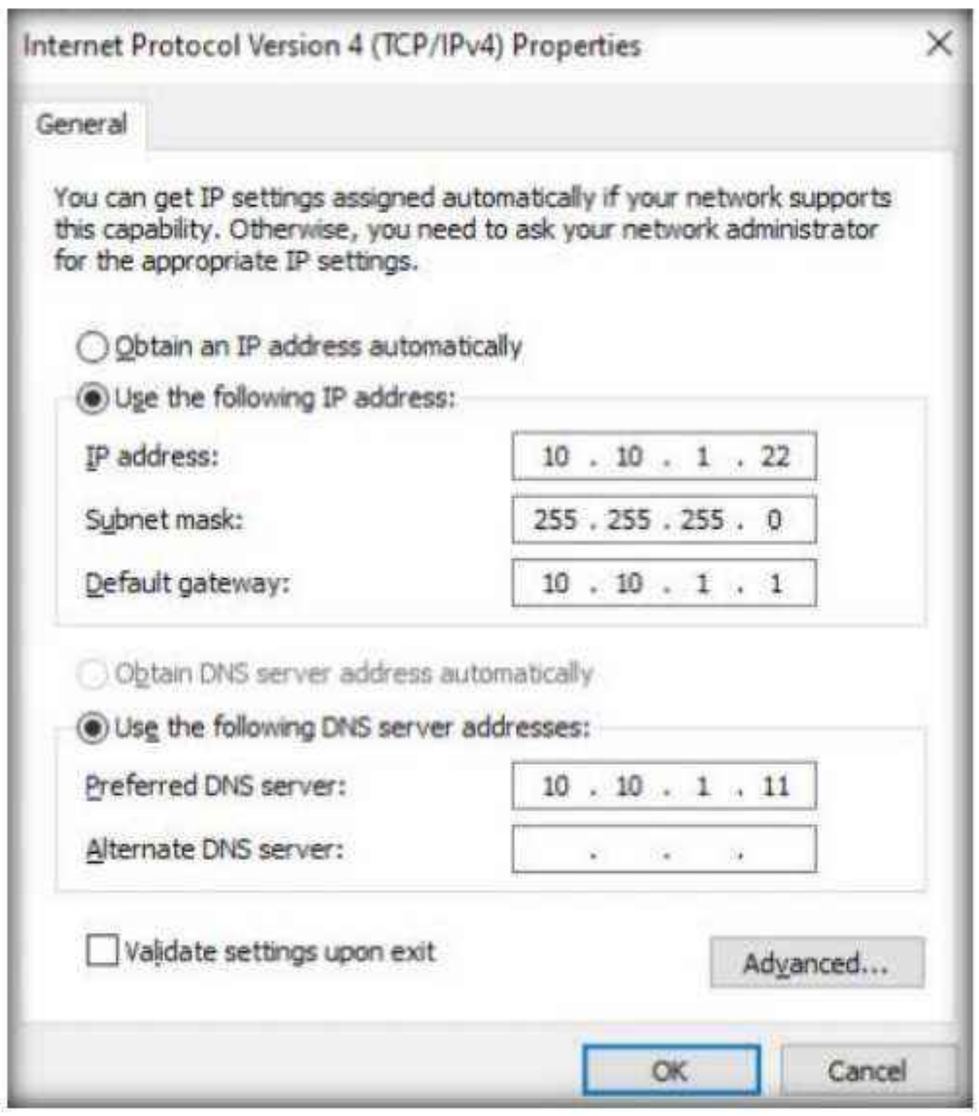


13. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



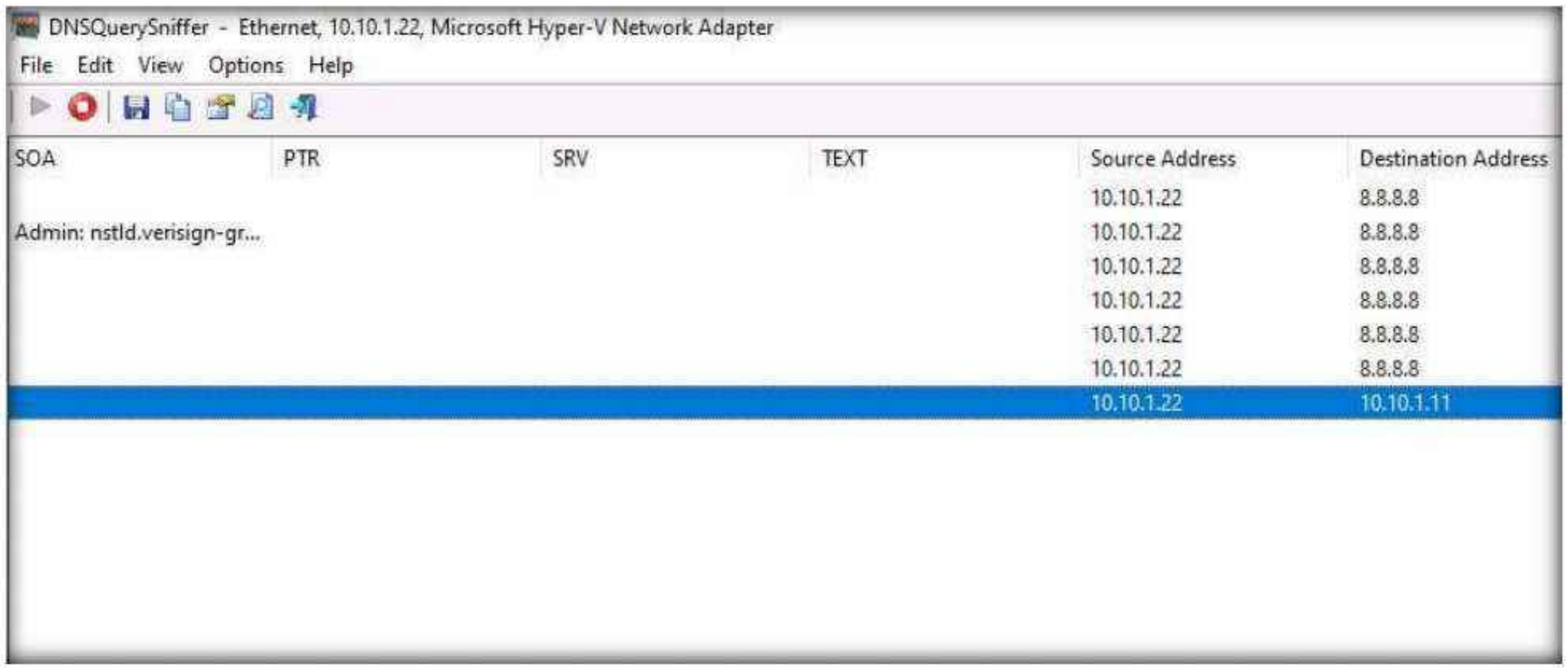
14. The **Internet Protocol Version 4(TCP/IPv4) Properties** window appears. Change the **Preferred DNS server** with the **Windows 11** IP address and click **OK**. In this task, the **Windows 11** IP address is **10.10.1.11**.

15. Click **OK**, and then **Close** the Adapter Properties window.

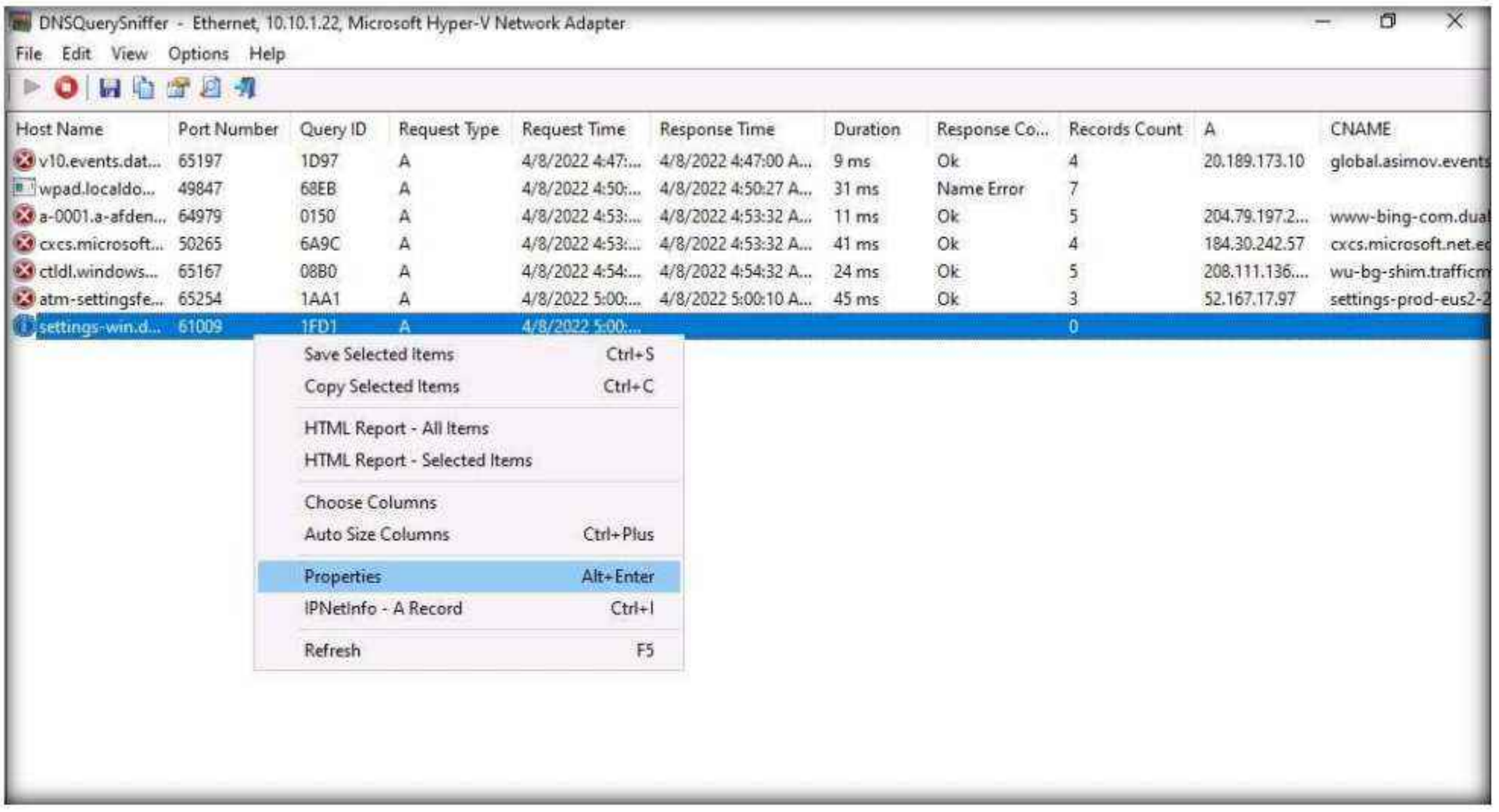


16. Switch to the **DNSQuerySniffer** window; observe the few recorded logs for which DNS has changed.

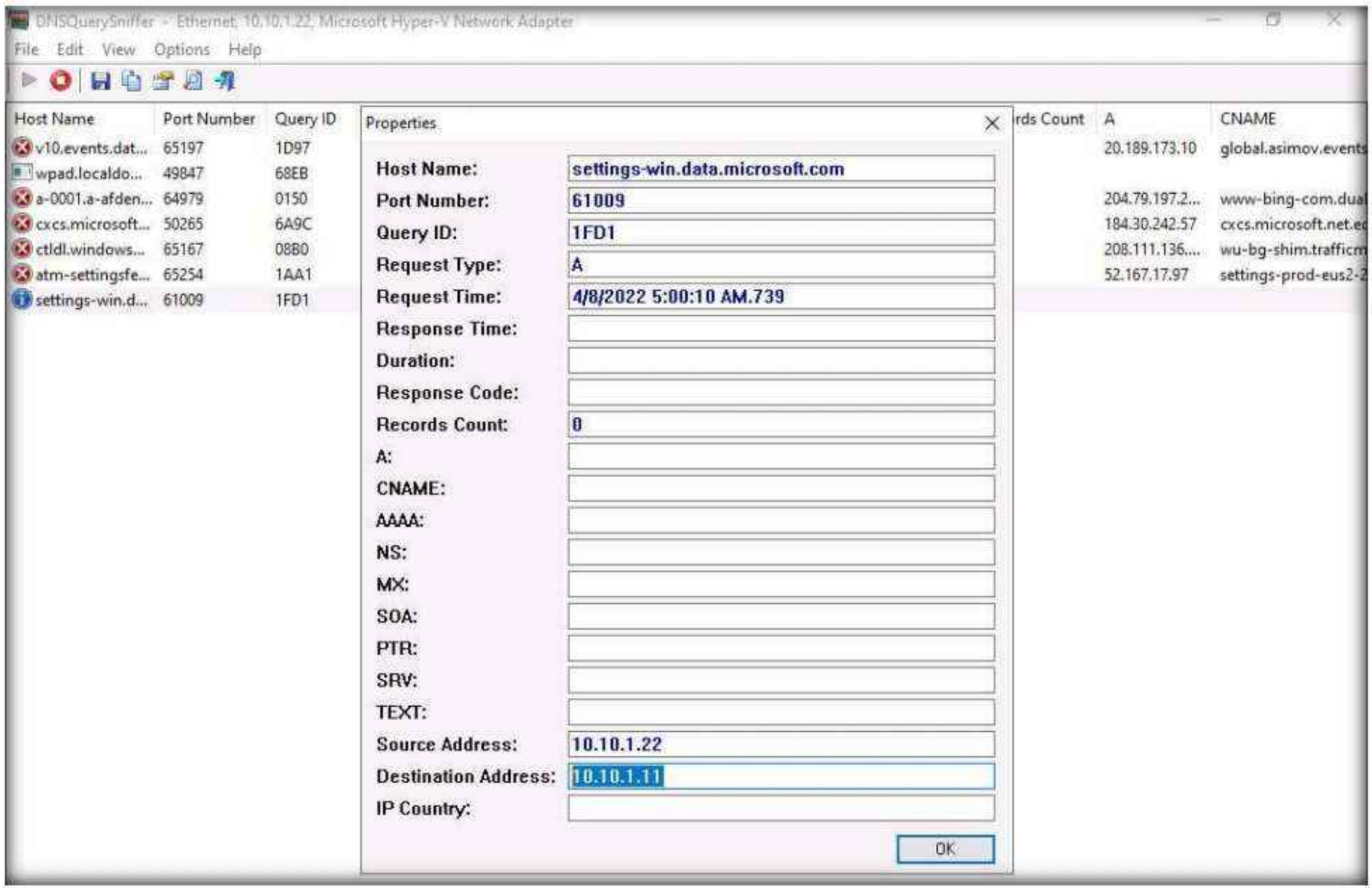
    Note: Wait for approximately 10 minutes to capture the logs.



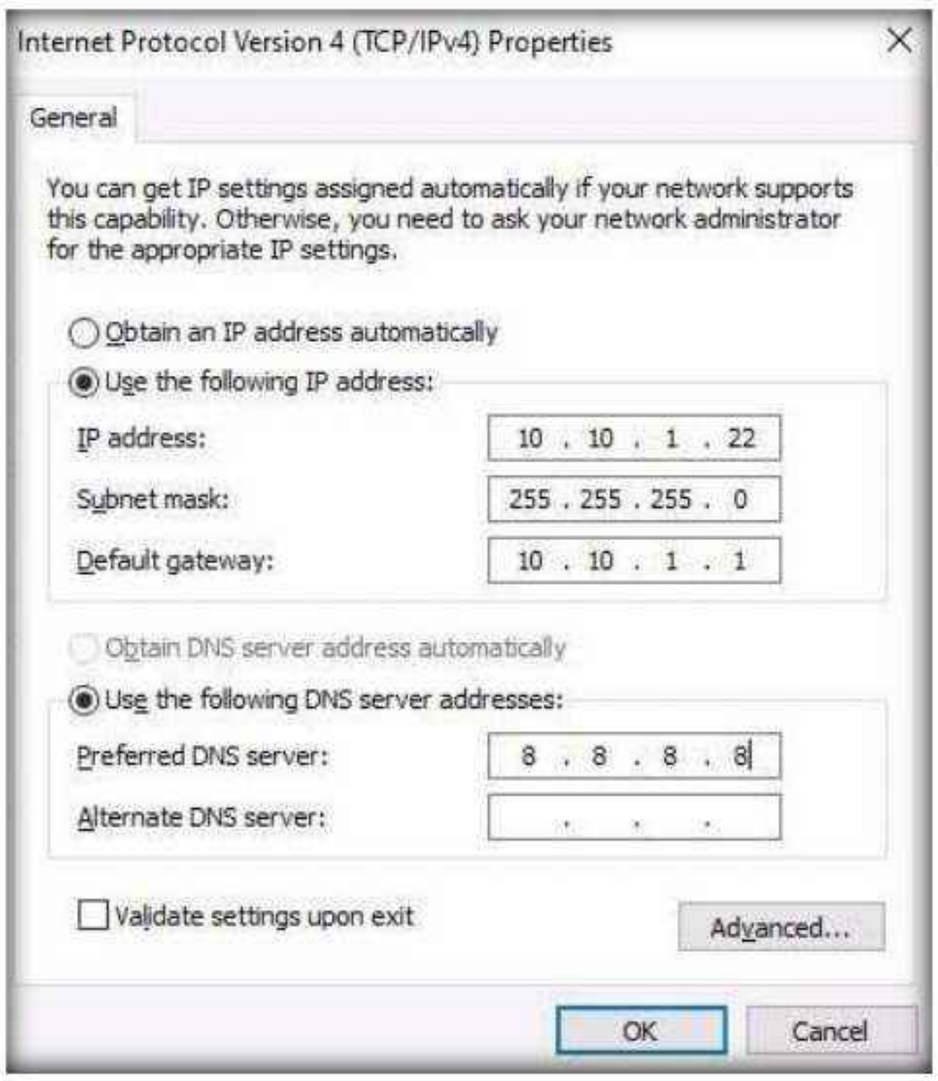
17. Right-click on the log for which DNS has changed and select **Properties** from the context menu.



18. In the **Properties** window, observe that there is a change in DNS. Click **OK** to close the window.



19. After completion of the task, go to the network settings, change DNS **8.8.8.8** in the **Windows Server 2022** machine, and close all applications.



20. Close all open windows.
21. You can also use other DNS monitoring/resolution tools such as **DNSstuff** (https://www.dnsstuff.com), or **Sonar Lite** (https://constellix.com) to perform DNS monitoring.
22. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Sniffing

Module 08

Sniffing

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.

Lab Scenario

Earlier modules taught how to damage target systems by infecting them using malware, which gives limited or full control of the target systems to further perform data exfiltration.

Now, as an ethical hacker or pen tester, it is important to understand network sniffing. Packet sniffing allows a person to observe and access the entire network's traffic from a given point. It monitors any bit of information entering or leaving the network. There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network. Although passive sniffing was once predominant, proper network-securing architecture has been implemented (switch-based network) to mitigate this kind of attack. However, there are a few loopholes in switch-based network implementation that can open doors for an attacker to sniff the network traffic.

Attackers hack the network using sniffers, where they mainly target the protocols vulnerable to sniffing. Some of these vulnerable protocols include HTTP, FTP, SMTP, POP, Telnet, IMAP, and NNTP. The sniffed traffic comprises data such as FTP and Telnet passwords, chat sessions, email and web traffic, and DNS traffic. Once attackers obtain such sensitive information, they might attempt to impersonate target user sessions.

Thus, an ethical hacker or pen tester needs to assess the security of the network's infrastructure, find the loopholes in the network using various network auditing tools, and patch them up to ensure a secure network environment.

The labs in this module provide real-time experience in performing packet sniffing on the target network using various packet sniffing techniques and tools.

Lab Objective

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

- Sniff the network
- Analyze incoming and outgoing packets for any attacks
- Troubleshoot the network for performance
- Secure the network from attacks

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 125 Minutes

Overview of Network Sniffing

Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

Packet sniffers are used to convert the host system's NIC to promiscuous mode. The NIC in promiscuous mode can then capture the packets addressed to the specific network. There are two types of sniffing. Each is used for different types of networks. The two types are:

- **Passive Sniffing**: Passive sniffing involves sending no packets. It only captures and monitors the packets flowing in the network
- **Active Sniffing**: Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN; it also refers to sniffing through a switch

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform network sniffing. Recommended labs that assist in learning various network sniffing techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform Active Sniffing	√	√	√
	1.1 Perform MAC Flooding using macof	√		√
	1.2 Perform a DHCP Starvation Attack using Yersinia	√		√
	1.3 Perform ARP Poisoning using arpspoof		√	√
	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel		√	√

	1.5 Spoof a MAC Address using TMAC and SMAC		√	√
	1.6 Spoof a MAC Address of Linux Machine using macchanger		√	√
2	Perform Network Sniffing using Various Sniffing Tools	√	√	√
	2.1 Perform Password Sniffing using Wireshark	√		√
	2.2 Analyze a Network using the Omnipeek Network Protocol Analyzer		√	√
	2.3 Analyze a Network using the SteelCentral Packet Analyzer		√	√
3	Detect Network Sniffing	√		√
	3.1 Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network	√		√
	3.2 Detect ARP Poisoning using the Capsa Network Analyzer	√		√

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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

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

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

Lab 1

Perform Active Sniffing

Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch.

Lab Scenario

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden.

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

Lab Objectives

- Perform MAC flooding using macof
- Perform a DHCP starvation attack using Yersinia
- Perform ARP poisoning using arpspoof
- Perform an Man-in-the-Middle (MITM) attack using Cain & Abel
- Spoof a MAC address using TMAC and SMAC
- Spoof a MAC address of Linux machine using macchanger

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine

- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Active Sniffing

Active sniffing involves sending out multiple network probes to identify access points. The following is the list of different active sniffing techniques:

- **MAC Flooding**: Involves flooding the CAM table with fake MAC address and IP pairs until it is full
- **DNS Poisoning**: Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not
- **ARP Poisoning**: Involves constructing a large number of forged ARP request and reply packets to overload a switch
- **DHCP Attacks**: Involves performing a DHCP starvation attack and a rogue DHCP server attack
- **Switch port stealing**: Involves flooding the switch with forged gratuitous ARP packets with the target MAC address as the source
- **Spoofing Attack**: Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Lab Tasks

Task 1: Perform MAC Flooding using macof

MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

Here, we will use the macof tool to perform MAC flooding.

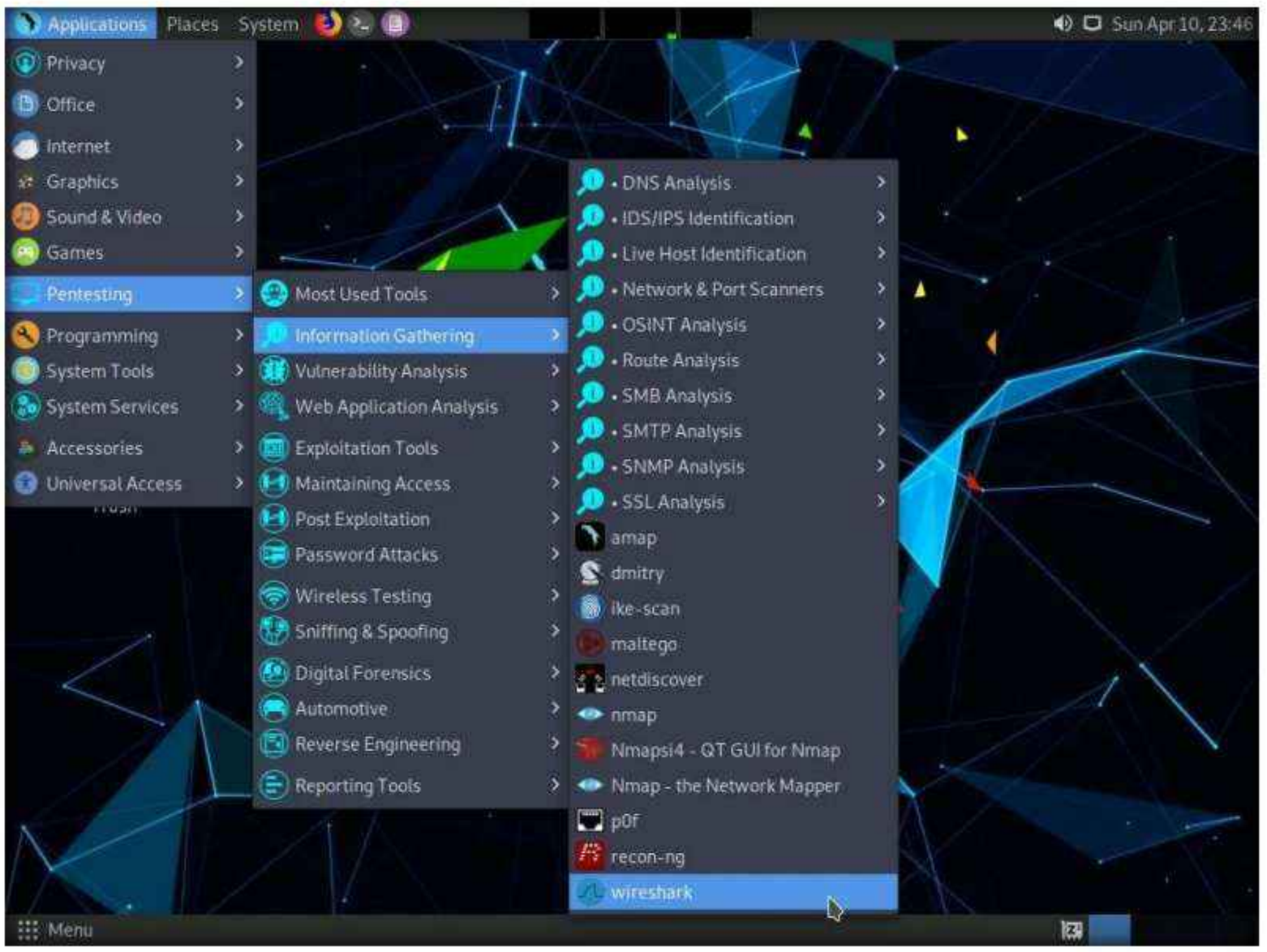
Note: For demonstration purposes, we are using only one target machine (namely, **Windows 11**). However, you can use multiple machines connected to the same network. Macof will send

the packets with random MAC addresses and IP addresses to all active machines in the local network.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

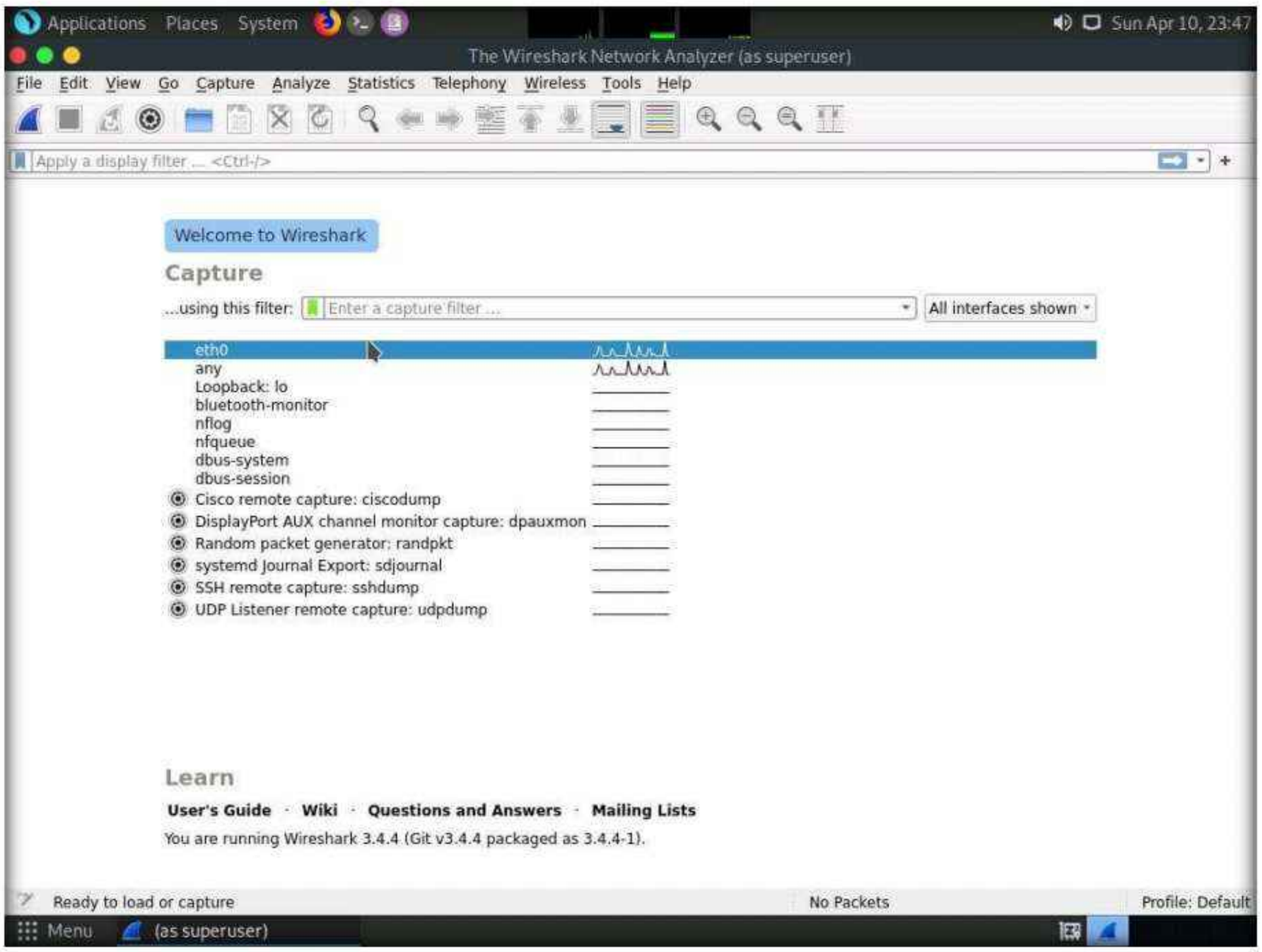
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



4. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

5. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



6. Leave the **Wireshark** application running.
7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

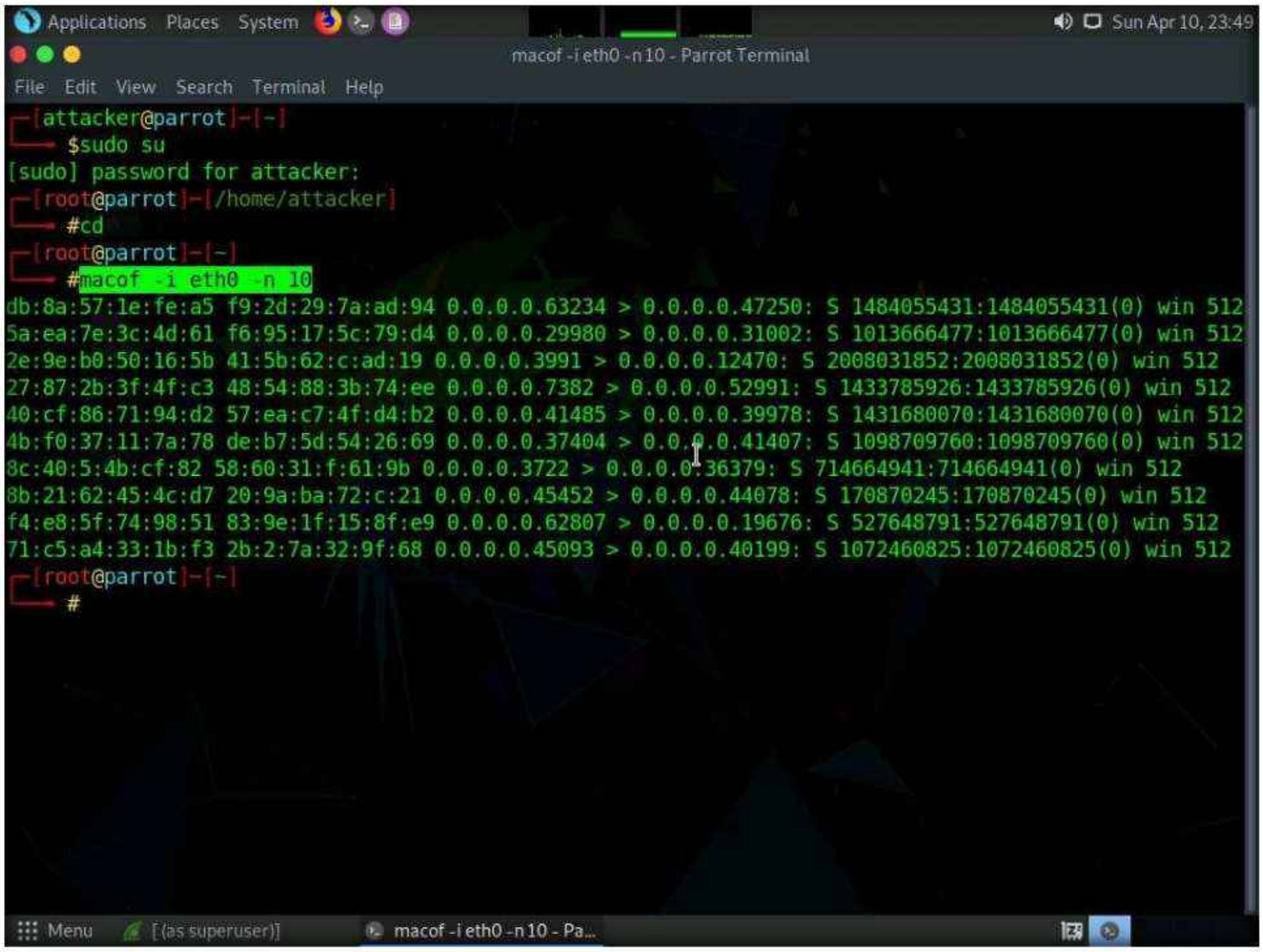
   Note: The password that you type will not be visible.
10. Now, type **cd** and press **Enter** to jump to the root directory.

11. The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.

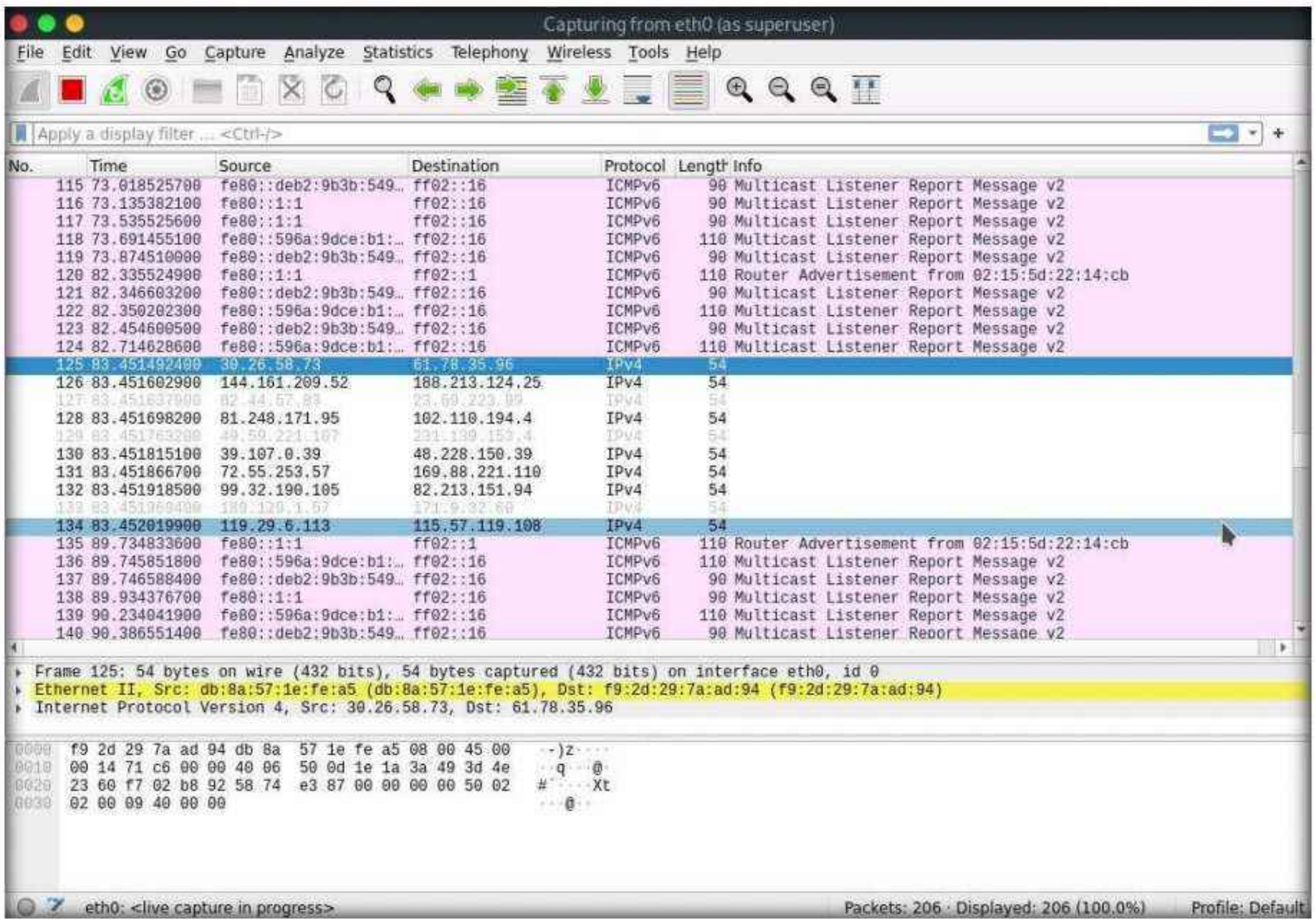
    Note: **-i**: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).

    Note: You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d**: Specifies the destination IP address).

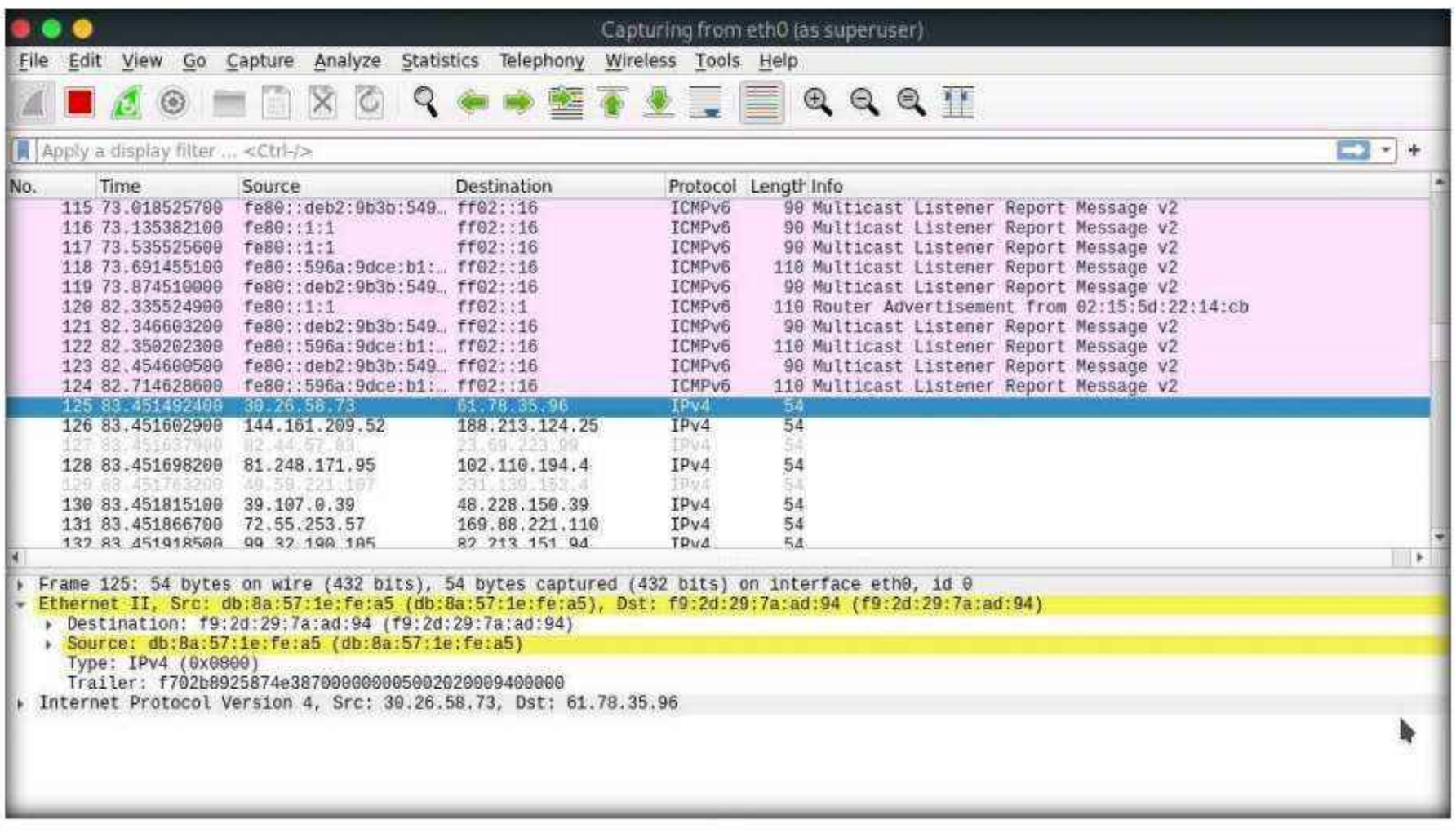
12. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.



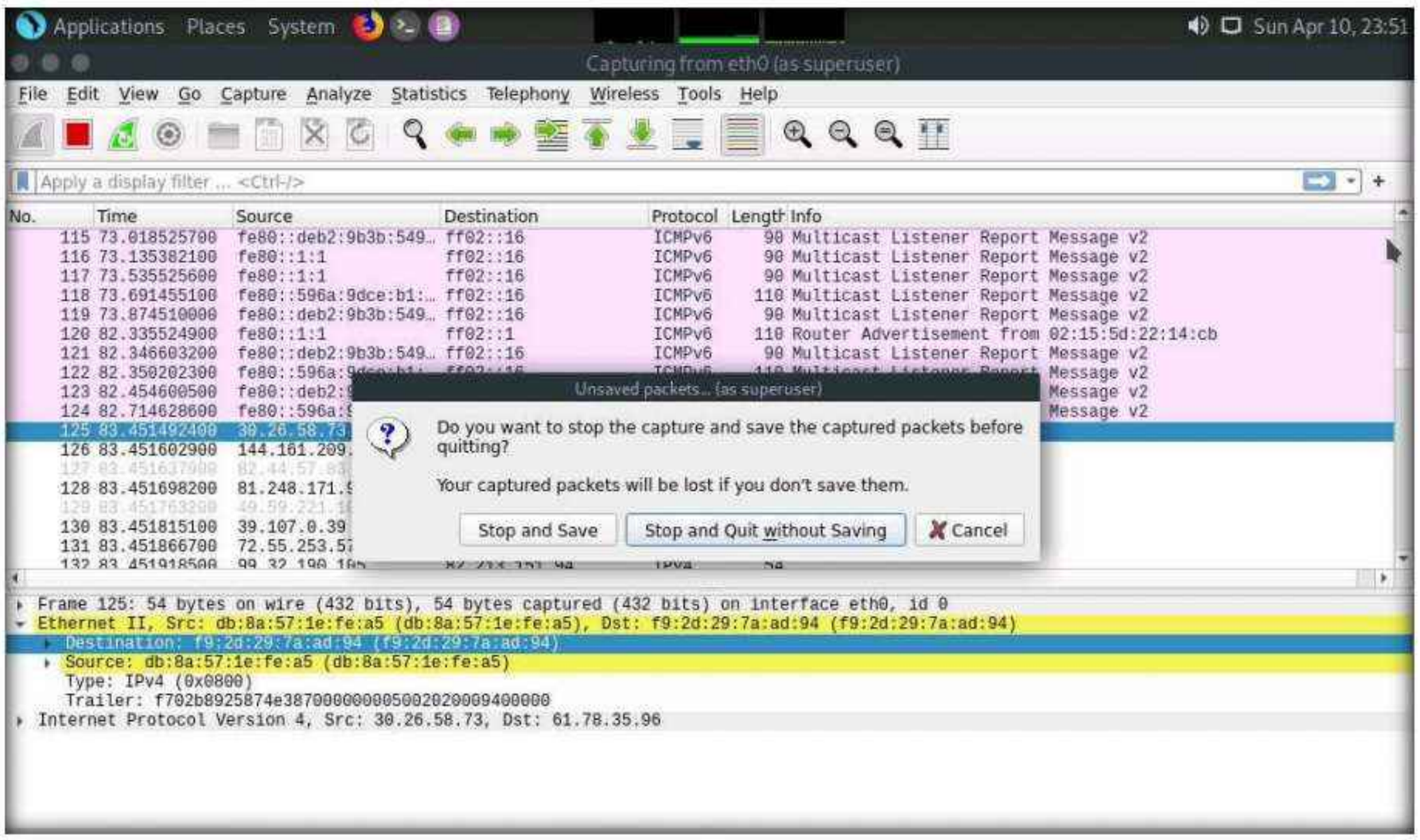
13. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.



14. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



15. Similarly, you can switch to a different machine to see the same packets that were captured by Wireshark in the **Parrot Security** machine.
16. Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.
17. Close the **Wireshark** window. If an **Unsaved packets**... pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application.



18. This concludes the demonstration of how to perform MAC flooding using macof.
19. Close all open windows and document all the acquired information.

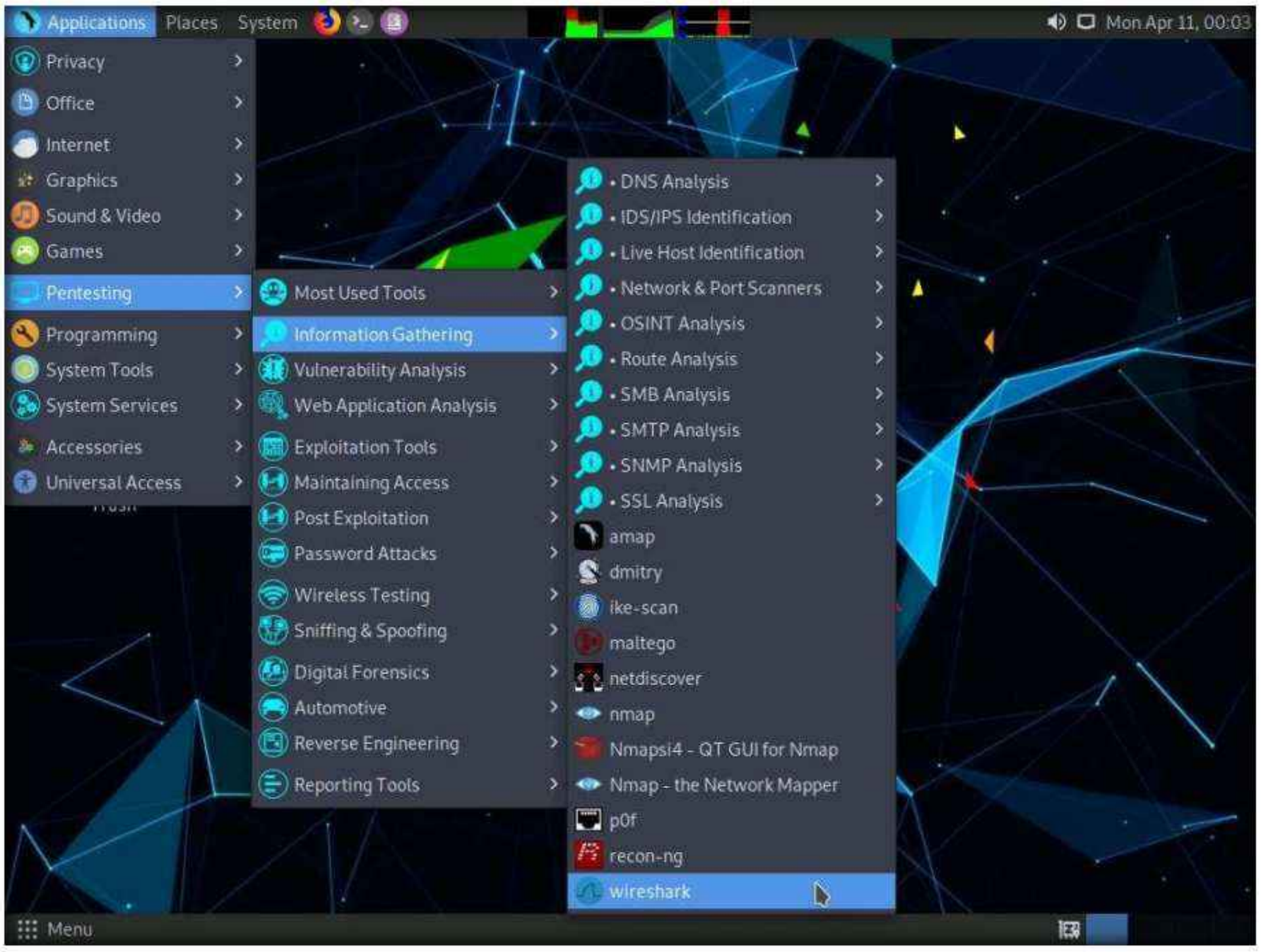
Task 2: Perform a DHCP Starvation Attack using Yersinia

In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. This attack can be performed by using various tools such as Yersinia and Hyenae.

Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

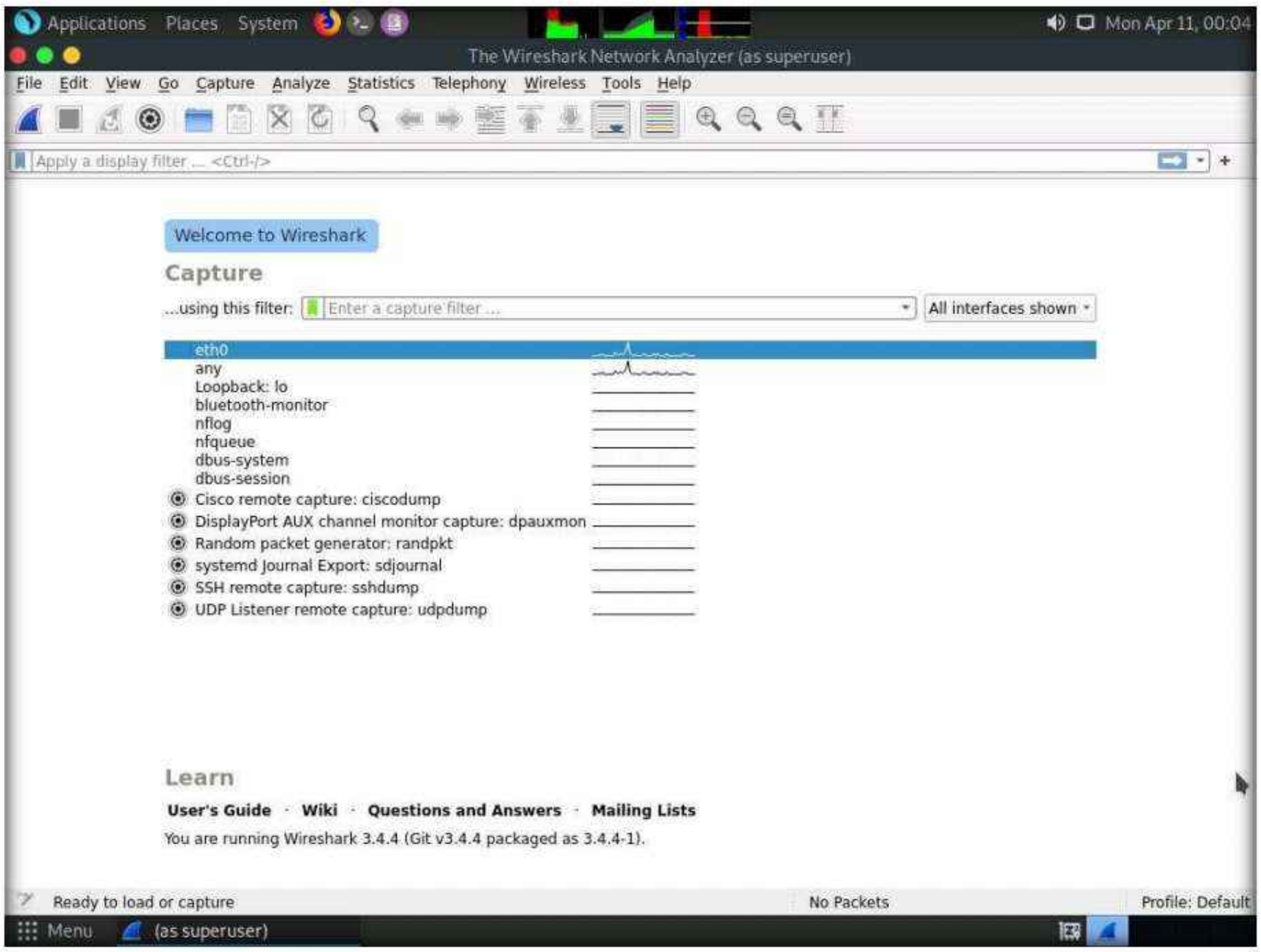
Here, we will use the Yersinia tool to perform a DHCP starvation attack on the target system.

1. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.



2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



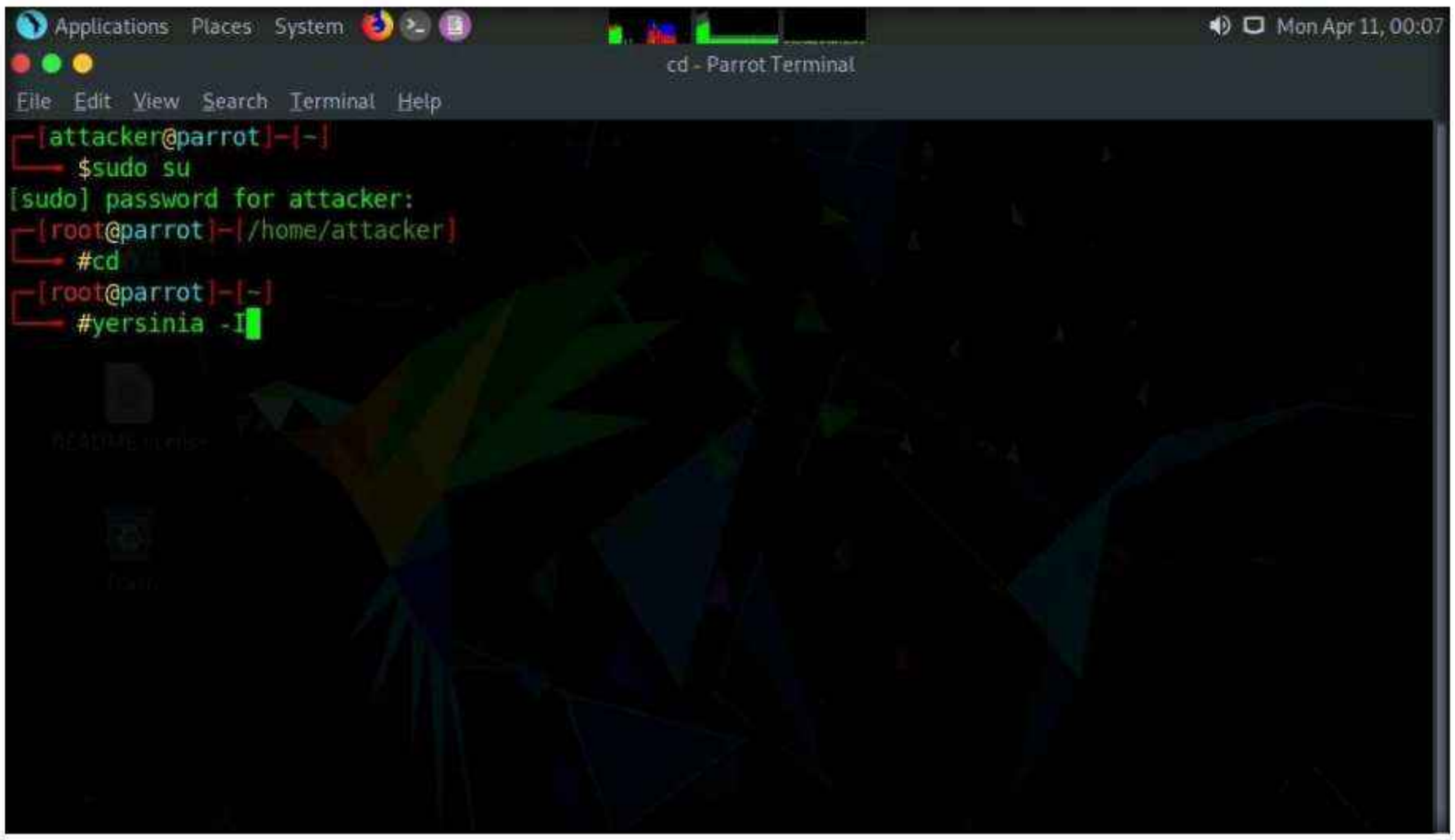
4. Leave the **Wireshark** application running.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
8. Now, type **cd** and press **Enter** to jump to the root directory.

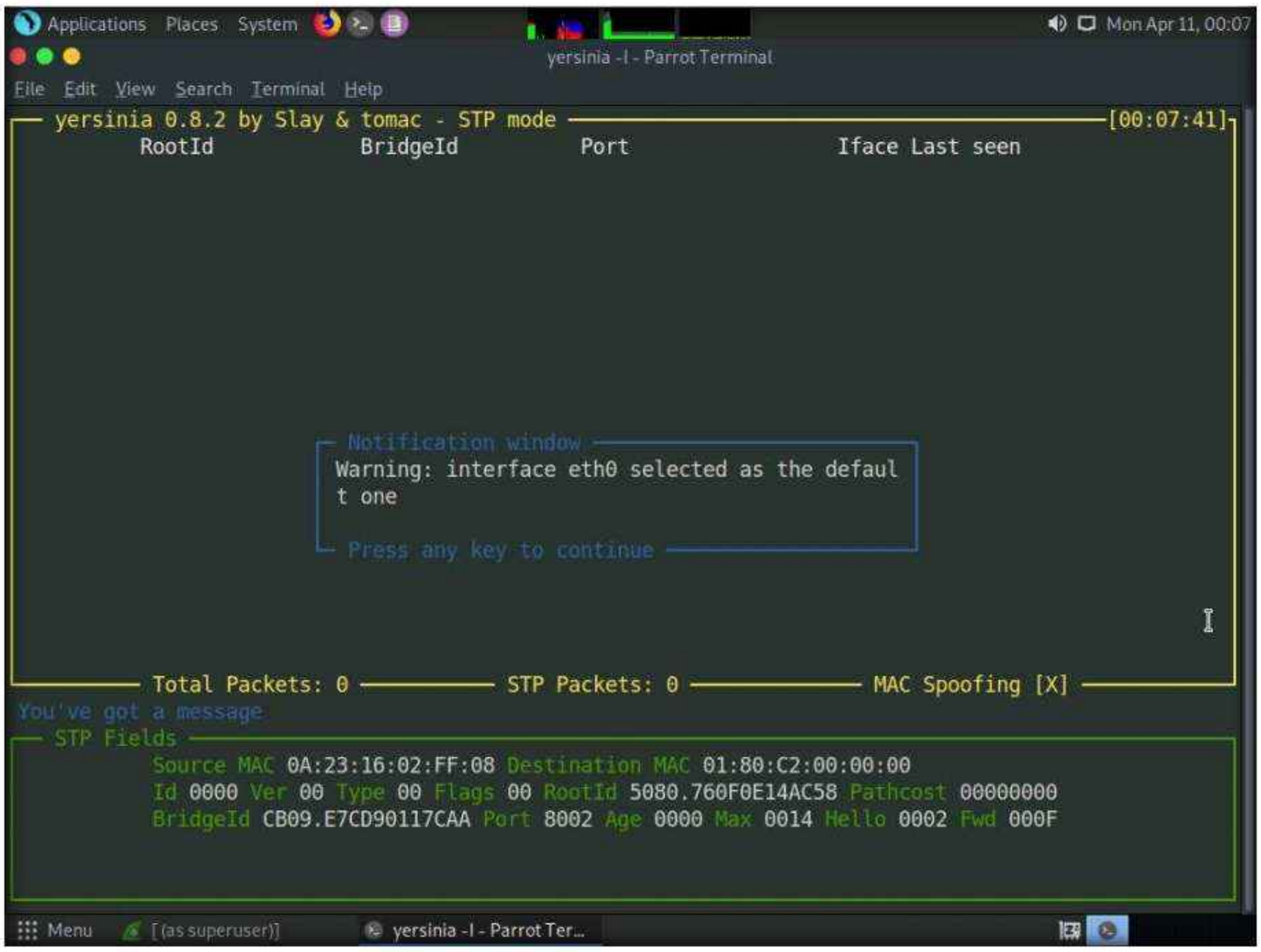
   Note: Click the **Maximize Window** icon to maximize the terminal window.

   Note: The interactive mode of the Yersinia application only works in a maximized terminal window.
9. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.

   Note: **-I**: Starts an interactive ncurses session.

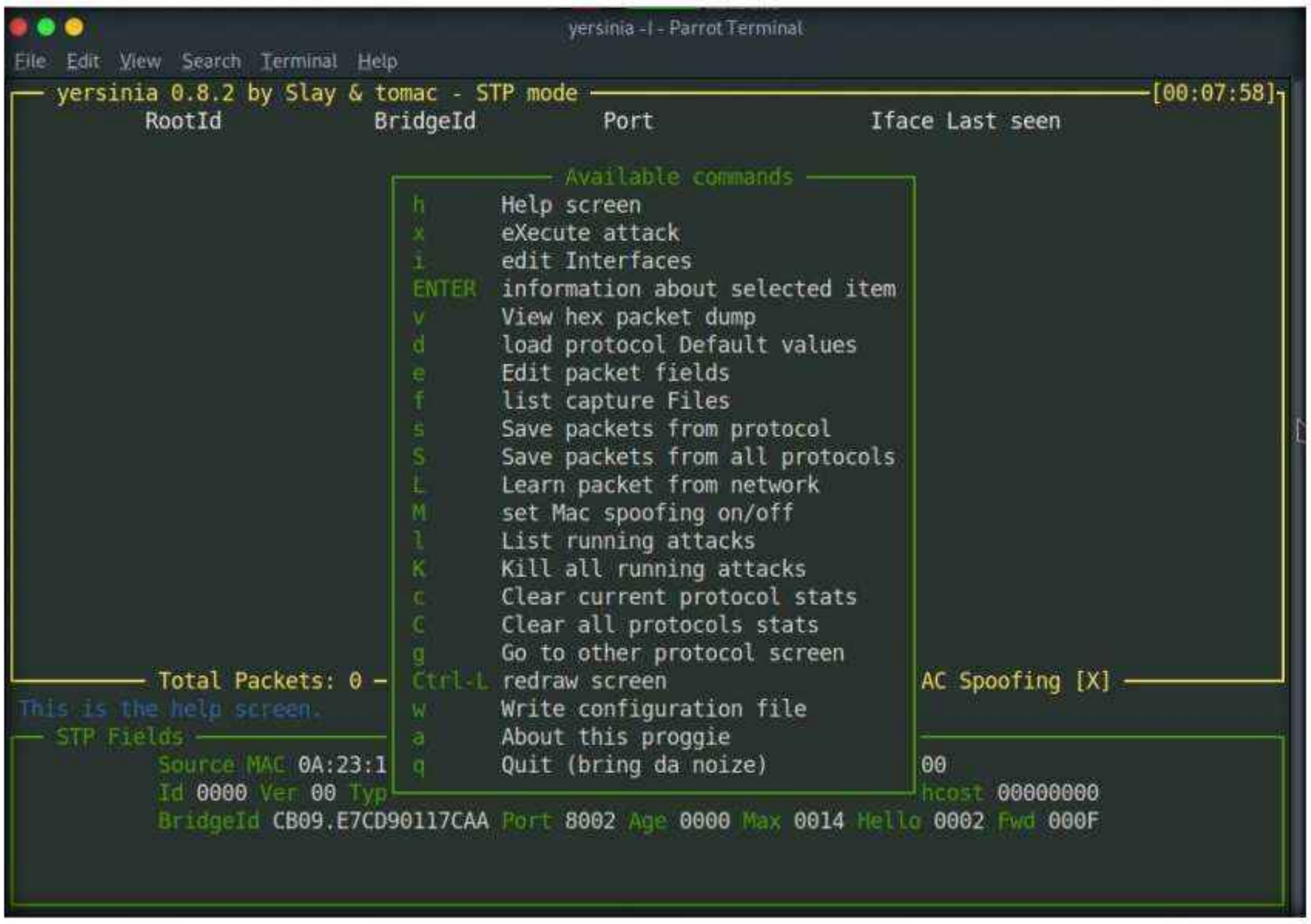


10. Yersinia interactive mode appears in the terminal window.



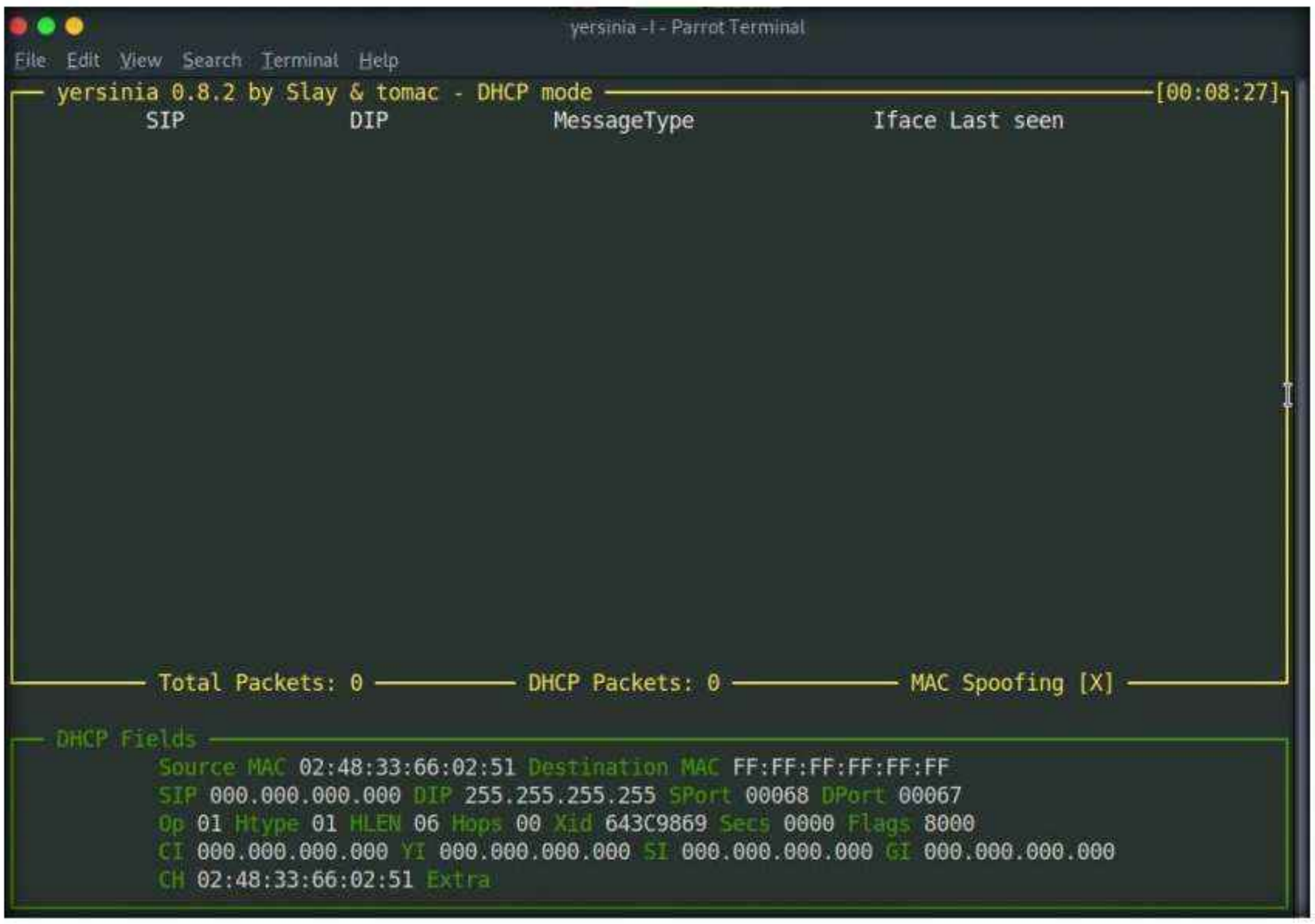
11. To remove the **Notification window**, press any key, and then press **h** for help.

12. The **Available commands** option appears, as shown in the screenshot.



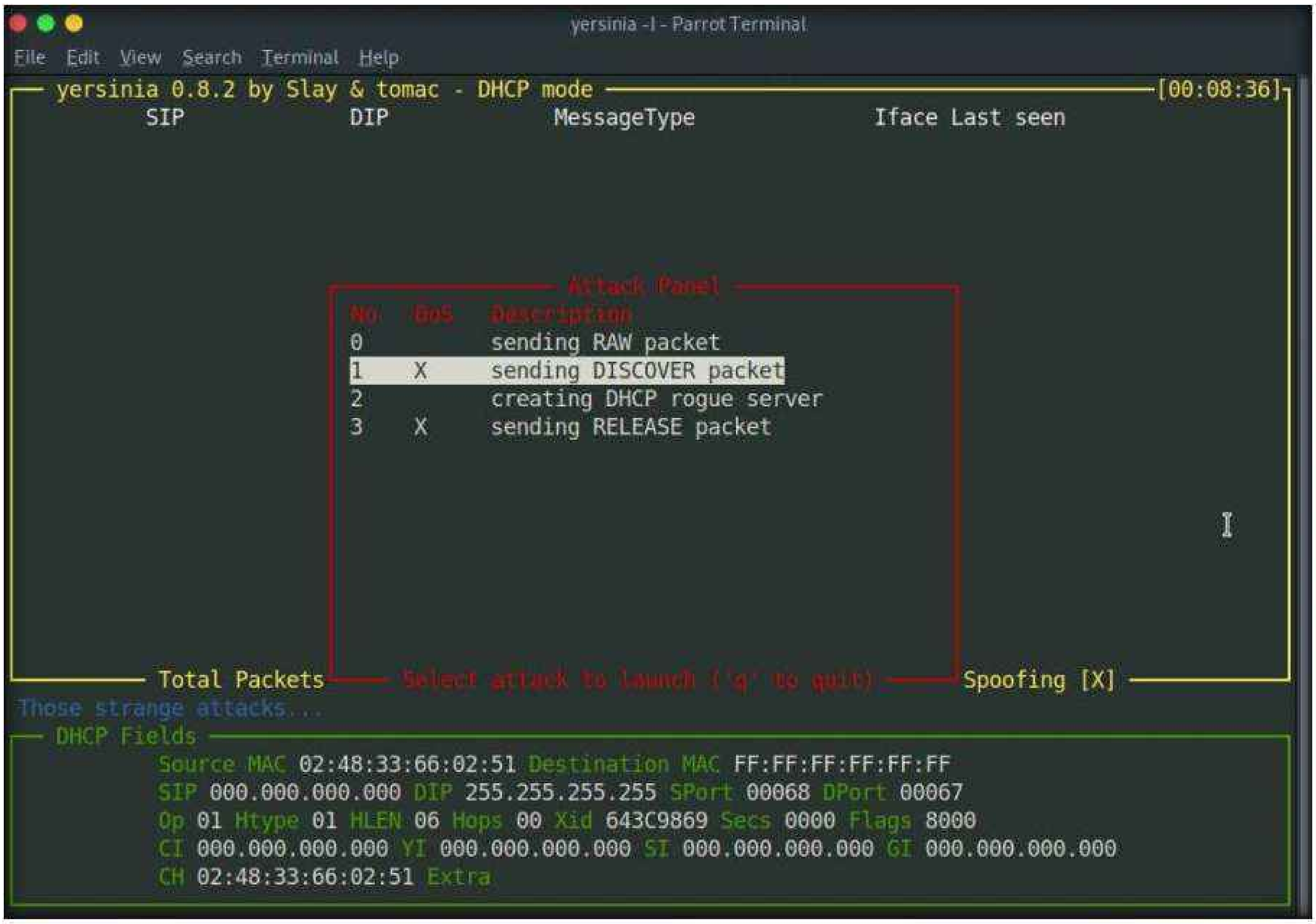
13. Press **q** to exit the help options.

14. Press **F2** to select DHCP mode. In DHCP mode, **STP Fields** in the lower section of the window change to **DHCP Fields**, as shown in the screenshot.



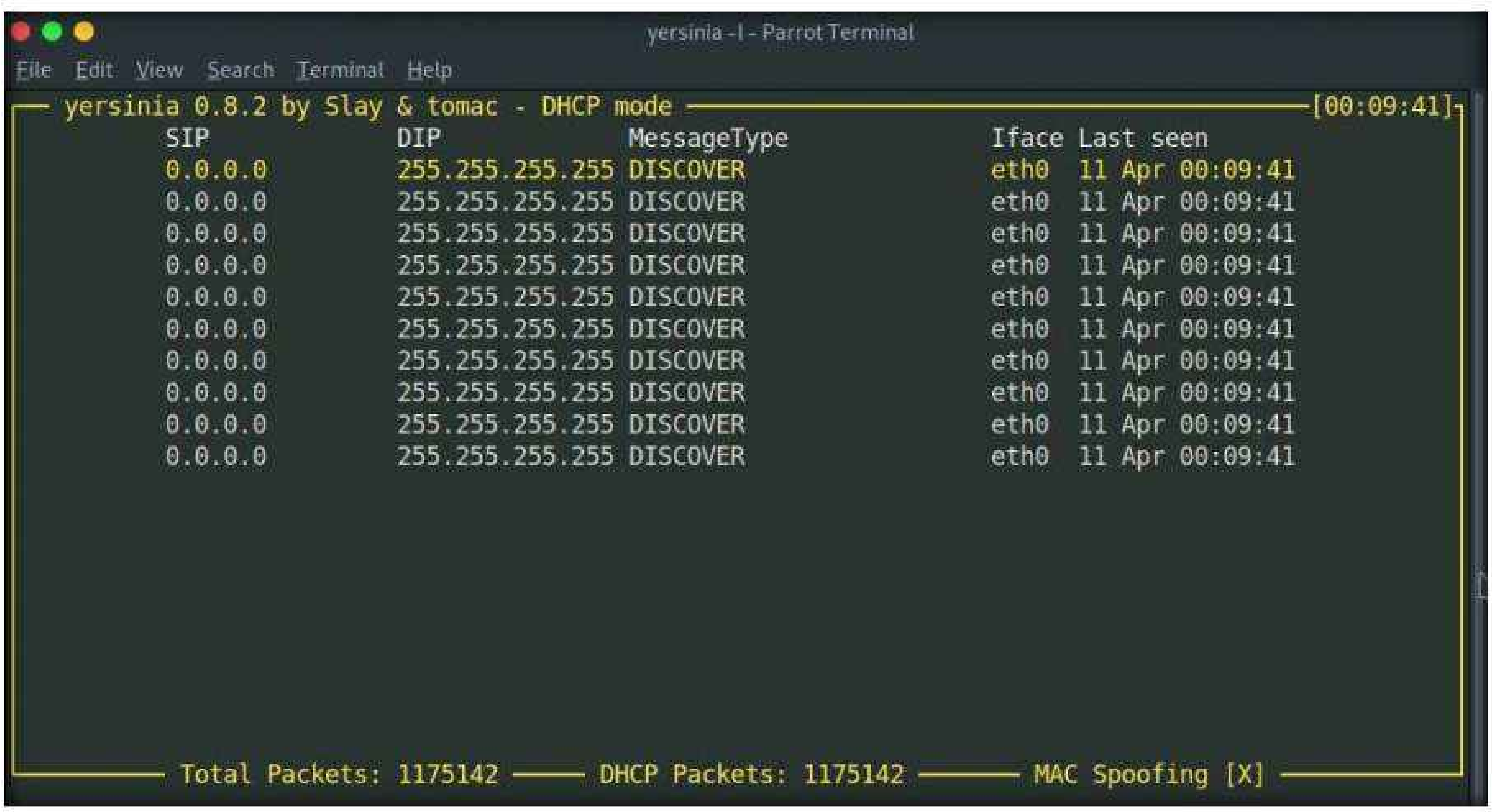
15. Press **x** to list available attack options.

16. The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.

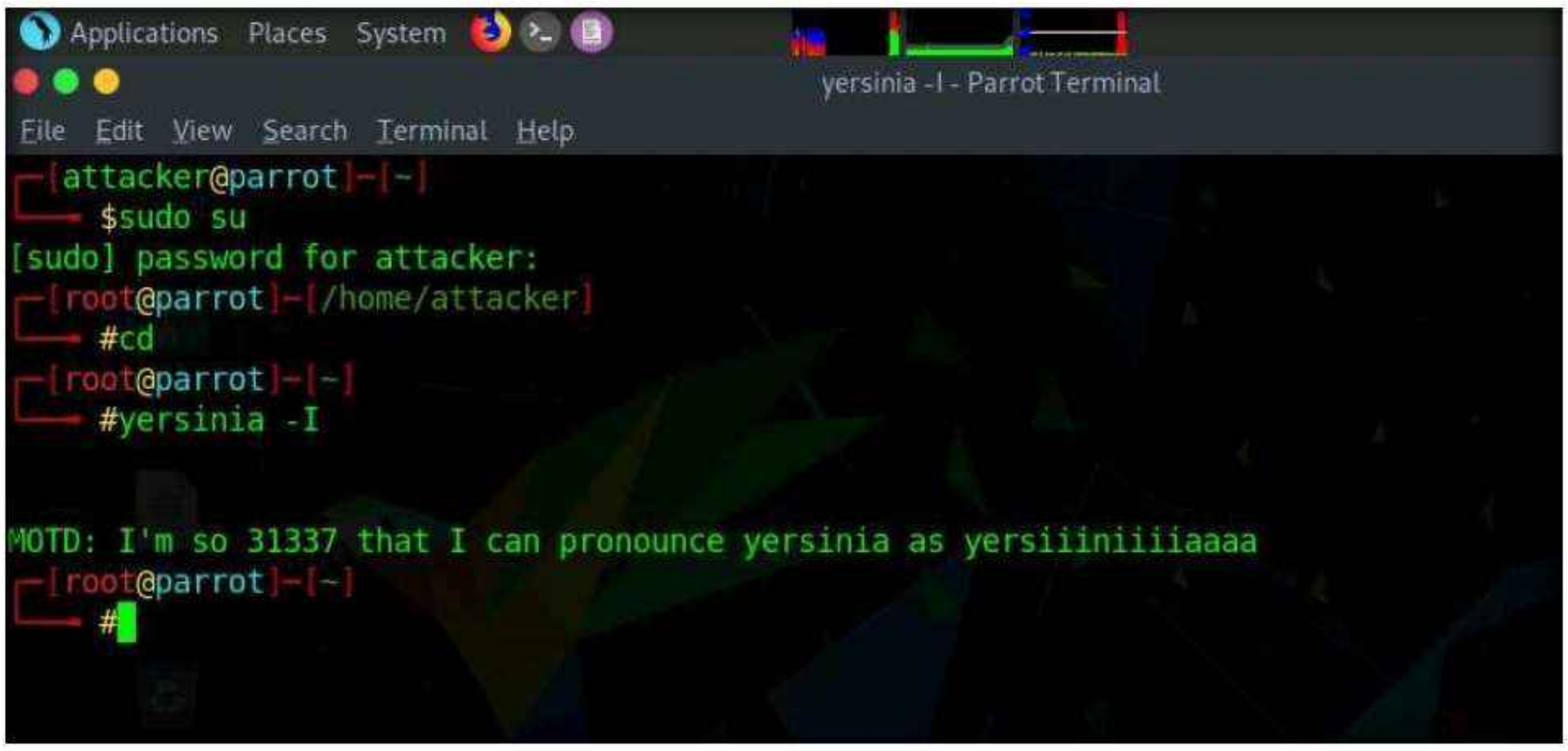


17. **Yersinia** starts sending DHCP packets to the network adapter and all active machines in the local network, as shown in the screenshot.

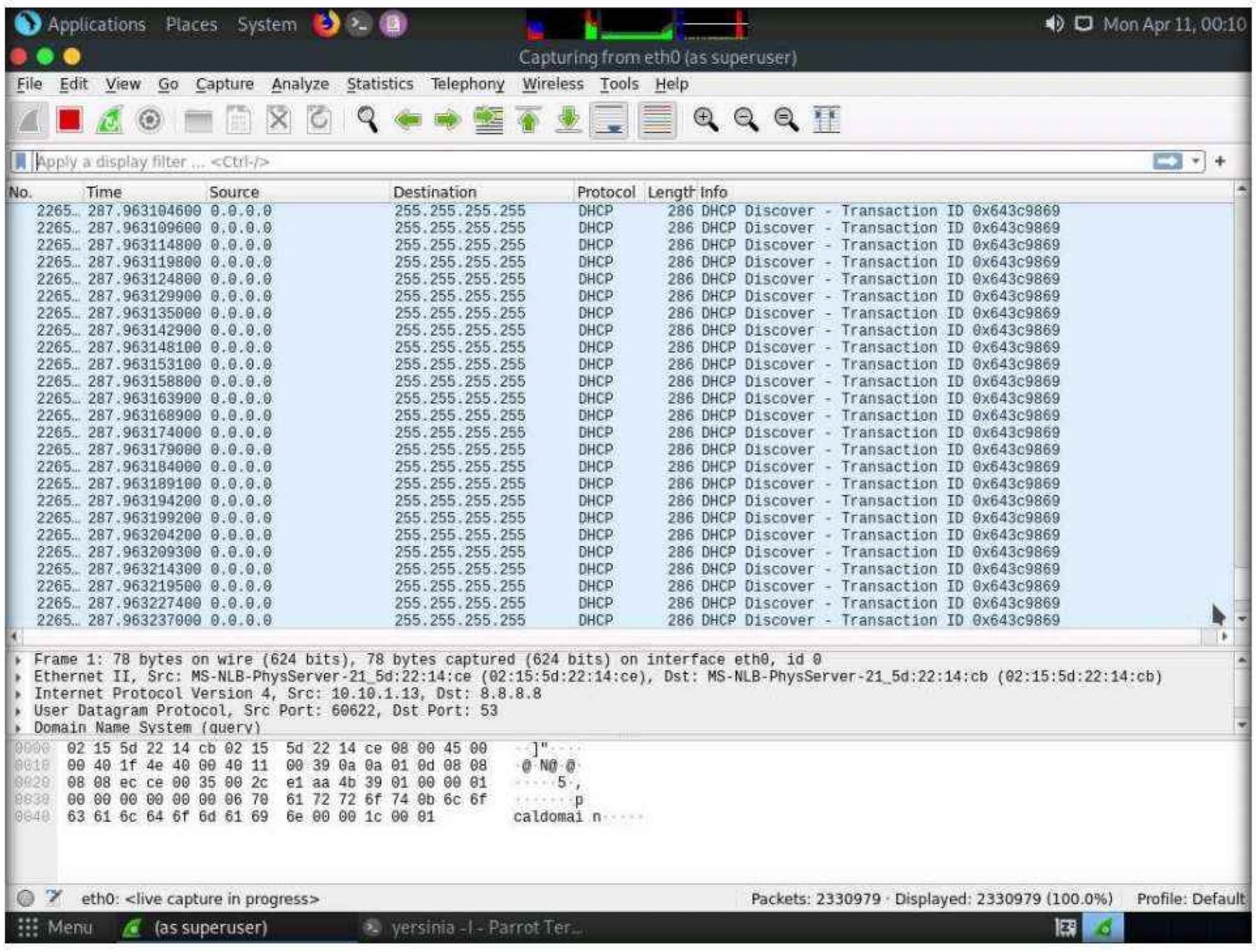
    Note: If you are using multiple targets, you will observe the same packets on all target machines.



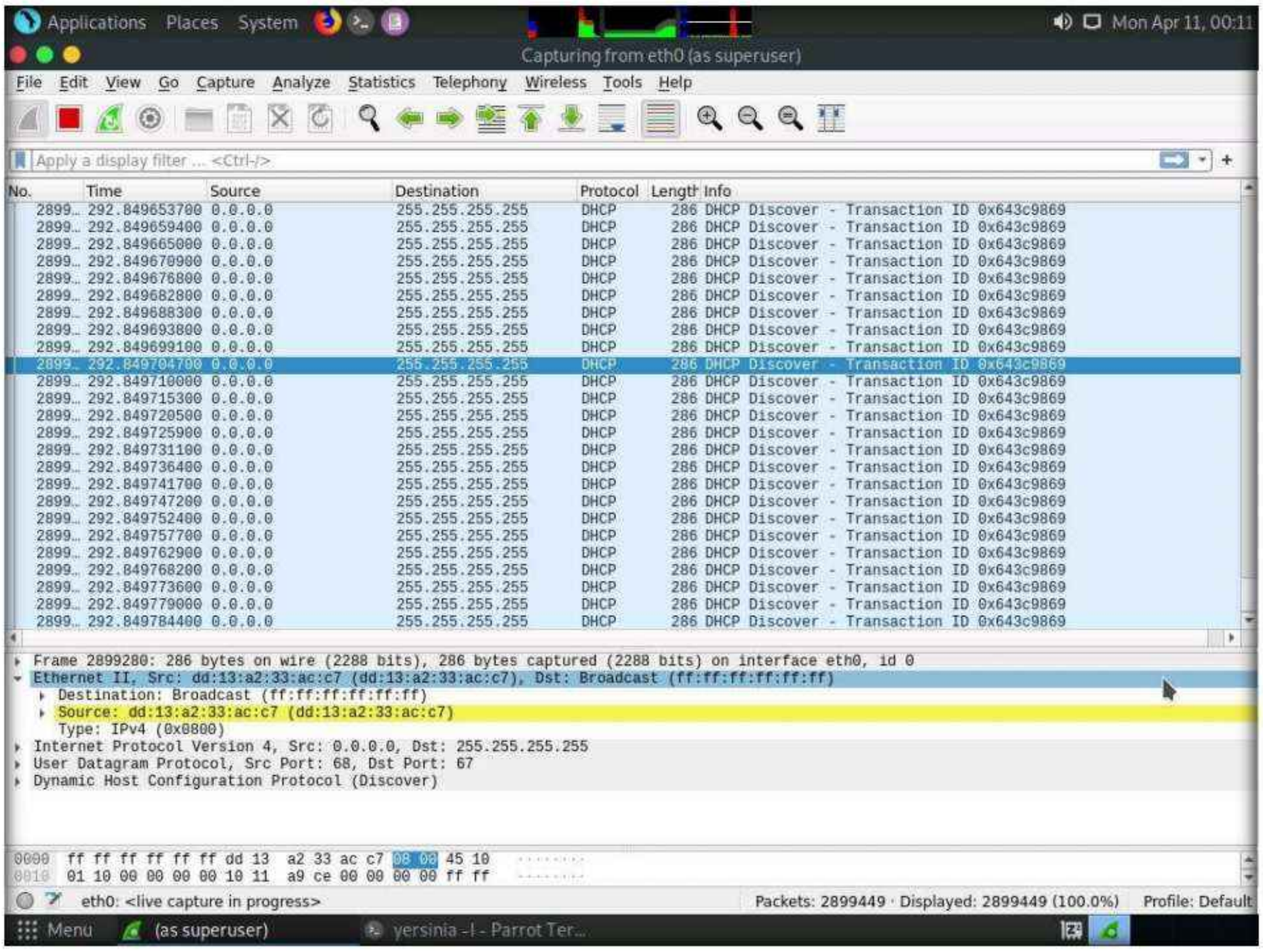
18. After a few seconds, press **q** to stop the attack and terminate Yersinia, as shown in the screenshot.



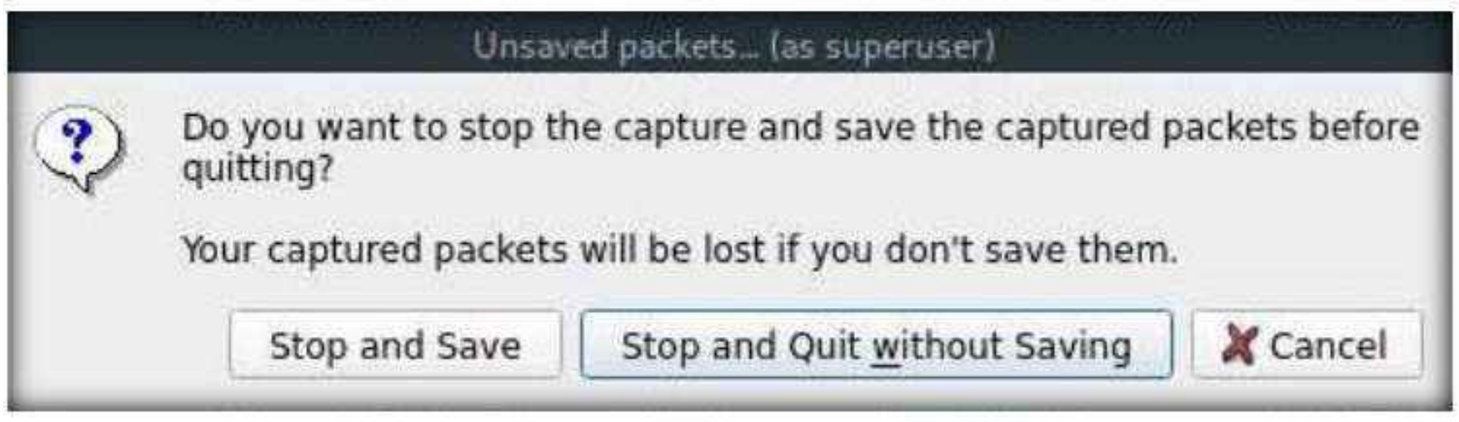
19. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.



20. Click on any DHCP packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



21. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.



22. This concludes the demonstration of how to perform a DHCP starvation attack using Yersinia.
23. Close all open windows and document all the acquired information.

Task 3: Perform ARP Poisoning using arpspoof

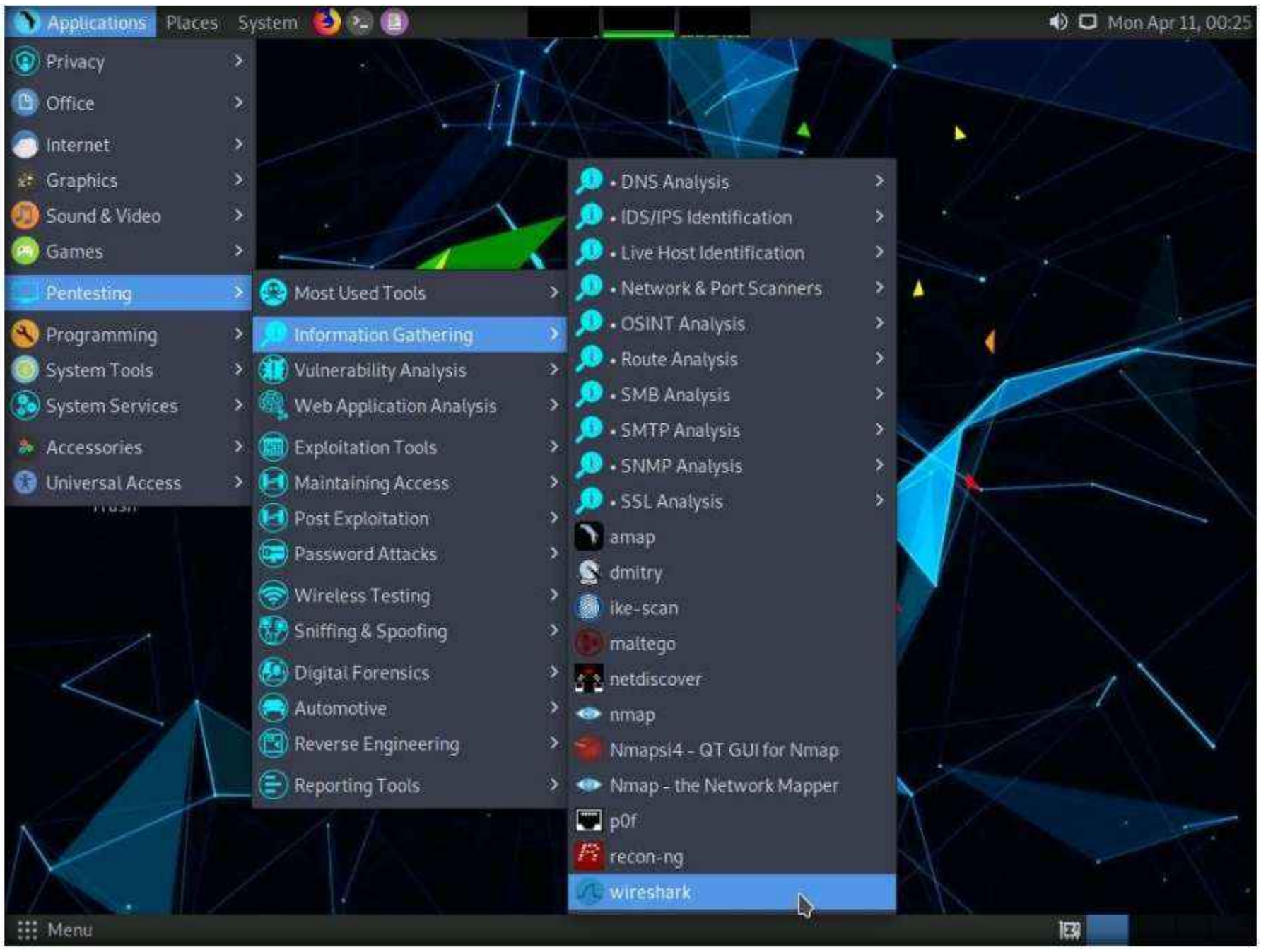
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends the frames to the attacker's computer, where the attacker can modify them before sending them to the source machine (User A) in an MITM attack.

arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

Here, we will use the arpspoof tool to perform ARP poisoning.

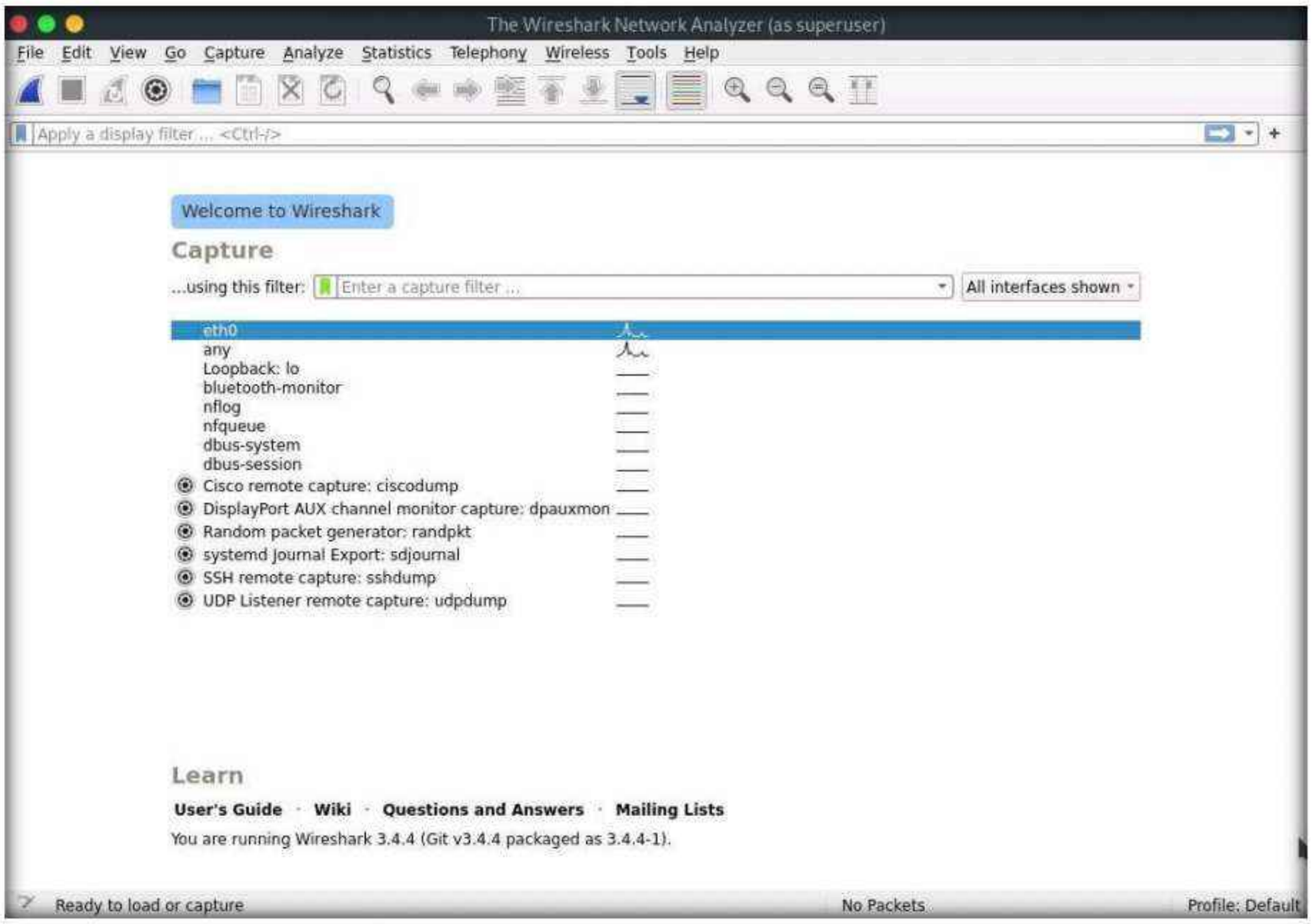
Note: In this lab, we will use the **Parrot Security (10.10.1.13)** machine as the host system and the **Windows 11 (10.10.1.11)** machine as the target system.

1. Turn on the **Windows 11** virtual machine.
2. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.



3. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

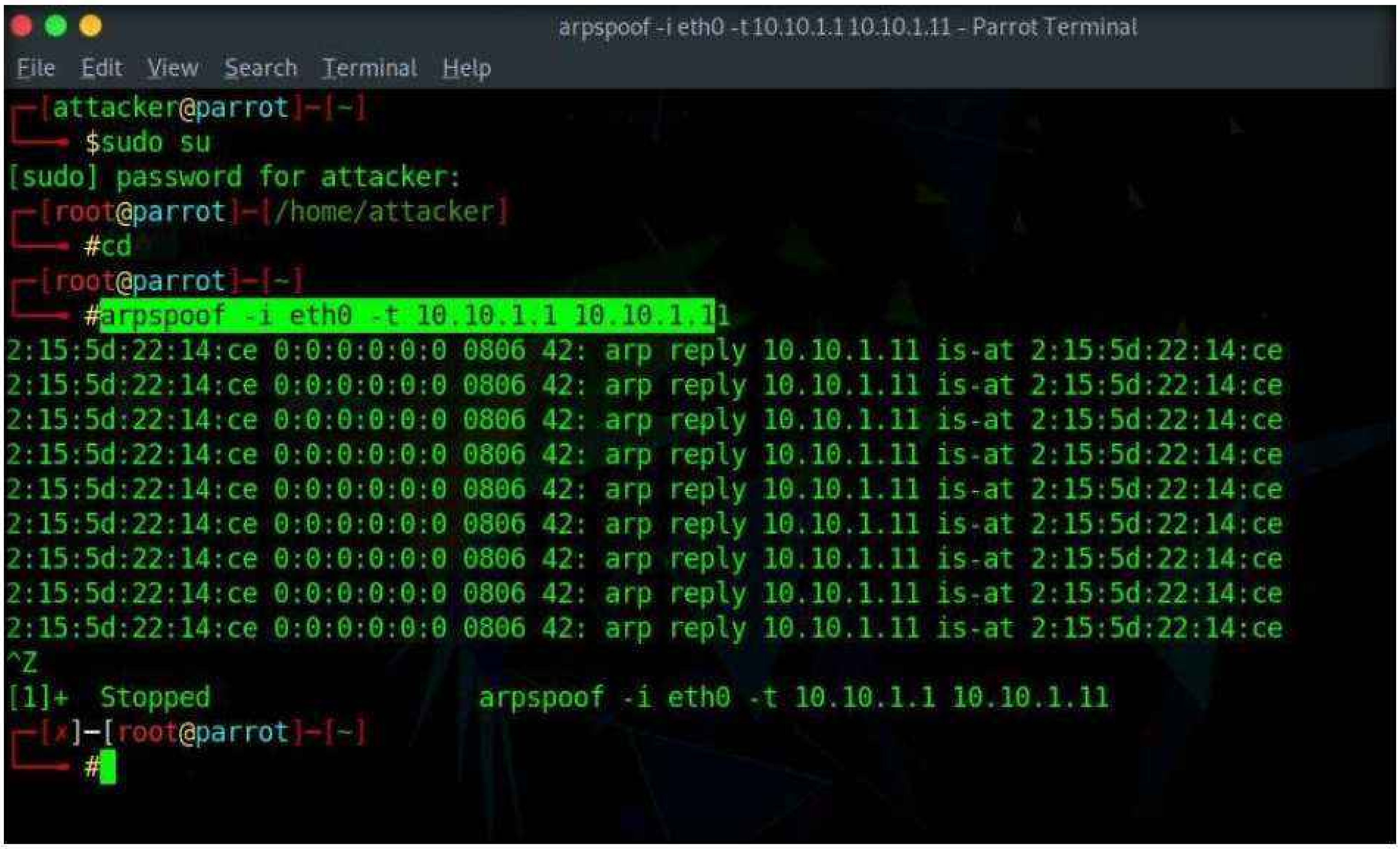


5. Leave the **Wireshark** application running.
6. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
9. Now, type **cd** and press **Enter** to jump to the root directory.
10. In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.1.1 10.10.1.11** and press **Enter**.

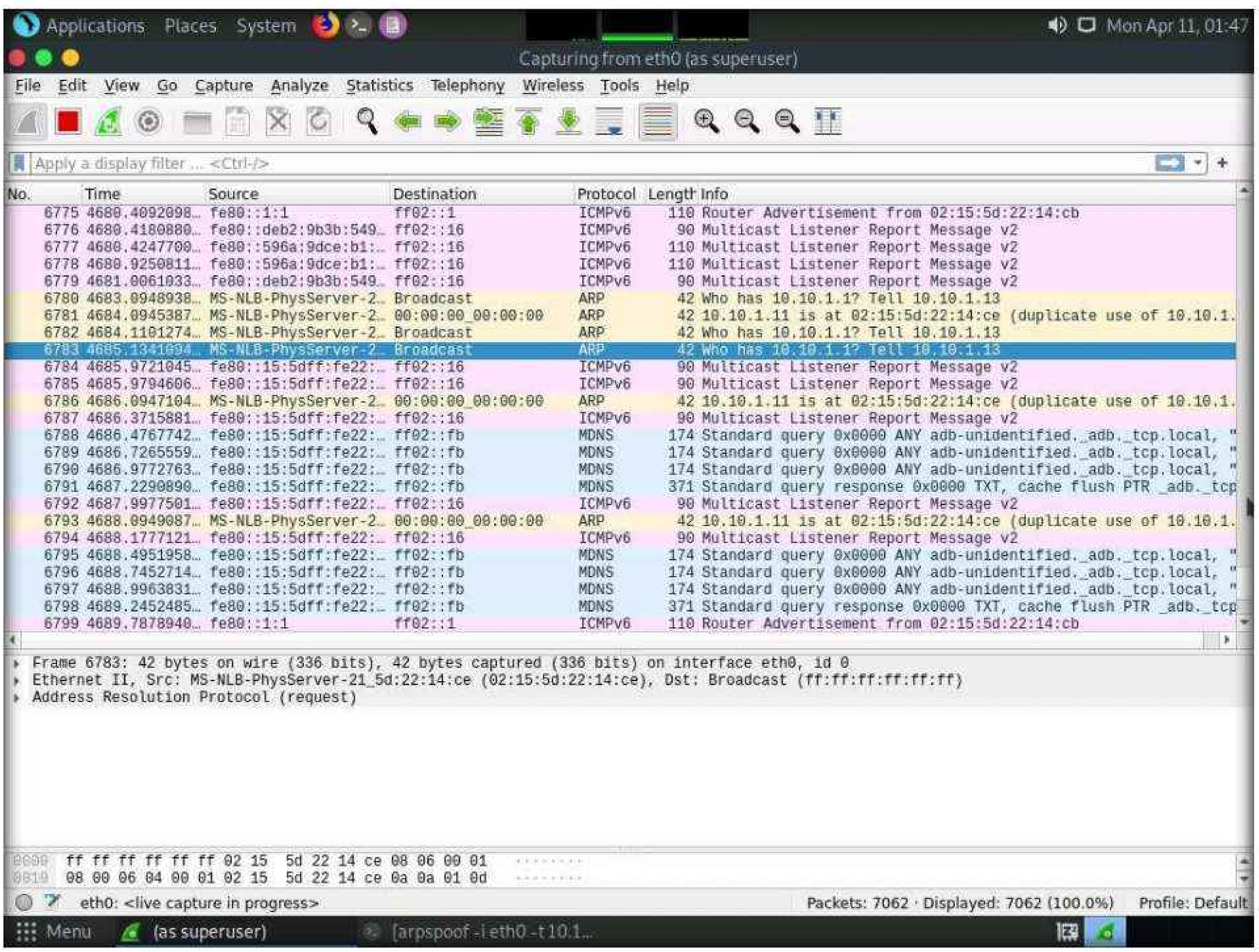
    (Here, **10.10.1.11** is IP address of the target system [**Windows 11**], and **10.10.1.1** is IP address of the access point or gateway)

    Note: **-i**: specifies network interface and **-t**: specifies target IP address.
11. Issuing the above command informs the access point that the target system (**10.10.1.11**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.
12. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

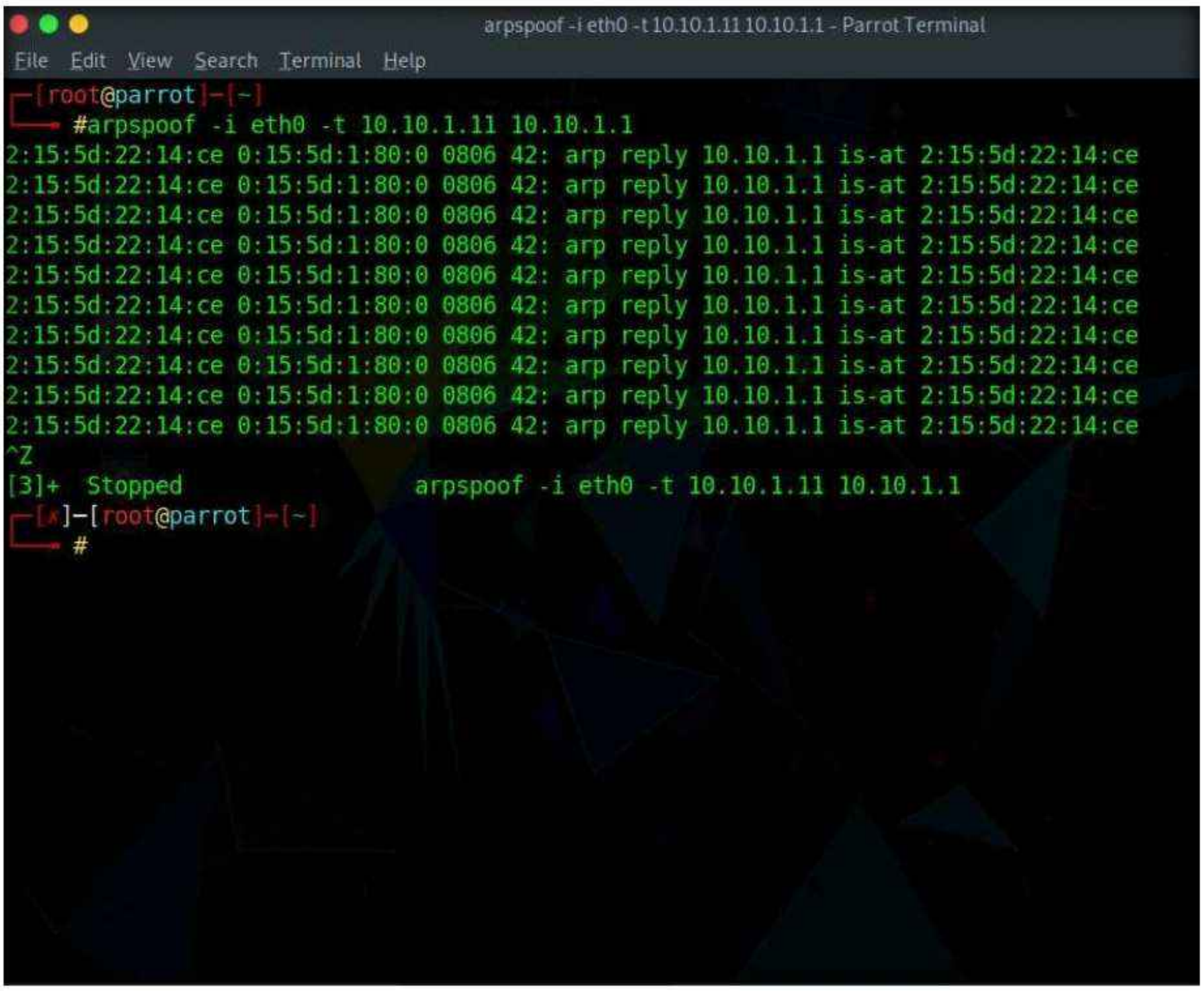
    Note: The MAC addresses might differ when you perform this task.



13. Switch to the **Wireshark** window and you can observe the captured **ARP** packets, as shown in the screenshot.

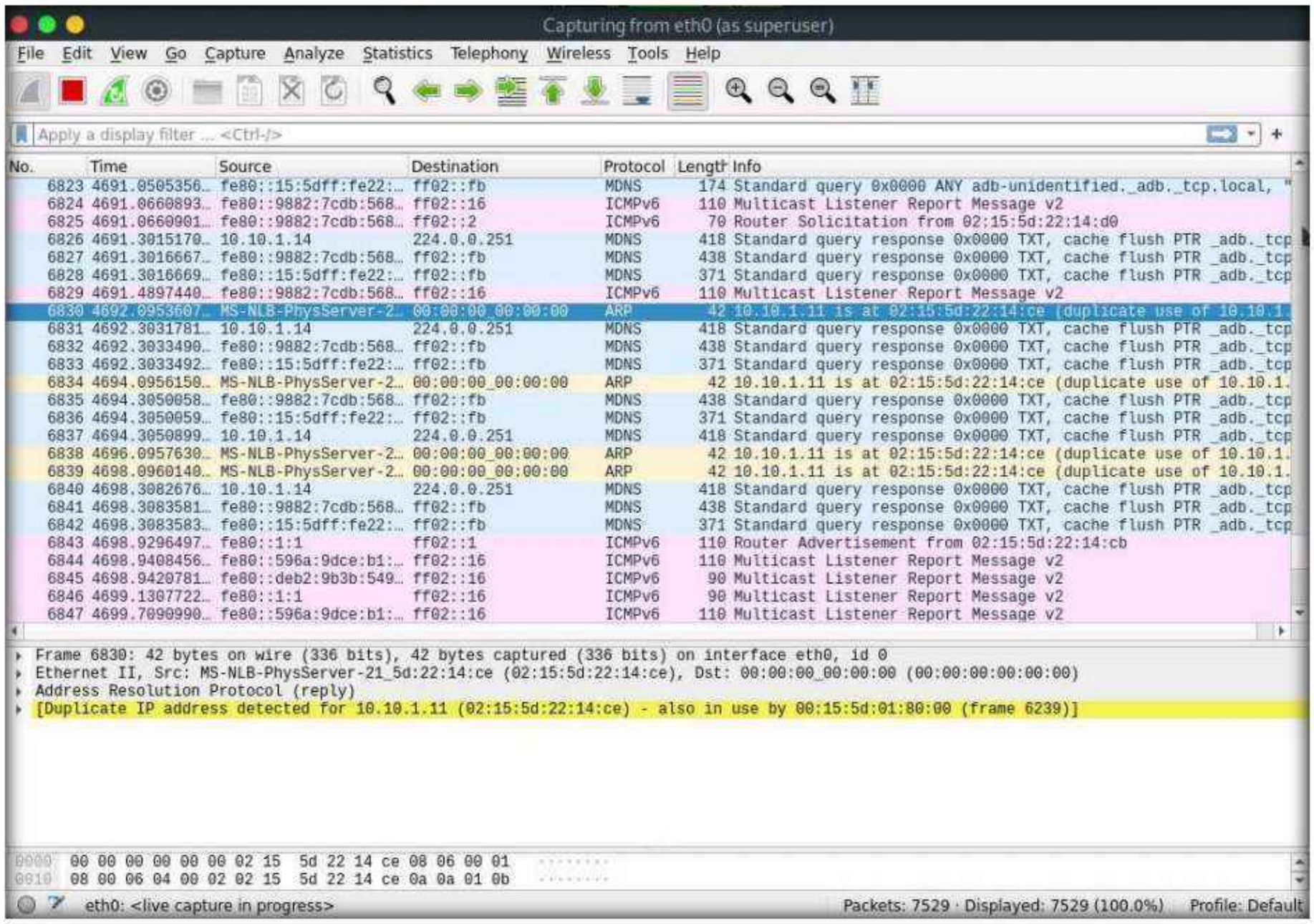


14. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.1.11 10.10.1.1** and press **Enter**.
15. Through the above command, the host system informs the target system (**10.10.1.11**) that it is the access point (**10.10.1.1**).
16. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.



17. In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.1.11 detected!**"
18. Click on any ARP packet and expand the **Ethernet II** node in the packet details section. As shown in the screenshot, you can observe the MAC addresses of IP addresses **10.10.1.1** and **10.10.1.11**.

    Note: Here, the MAC address of the host system (**Parrot Security**) is **02:15:5d:22:14:ce**.
19. Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 11**) and access point. Therefore, the alert warning of a duplicate use of **10.10.1.11** is displayed.



Note: You can navigate to the **Windows 11** machine and see the IP addresses and their corresponding MAC addresses. You will observe that the MAC addresses of IP addresses **10.10.1.1** and **10.10.1.13** are the same, indicating the occurrence of an ARP poisoning attack, where 10.10.11.13 is the **Parrot Security** machine and 10.10.1.1 is the access point.

20. Attackers use the arpspoof tool to obtain the ARP cache; then, the MAC address is replaced with that of an attacker's system. Therefore, any traffic flowing from the victim to the gateway will be redirected to the attacker's system.
21. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
22. Close all open windows and document all the acquired information.

Task 4: Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel

An attacker can obtain usernames and passwords using various techniques or by capturing data packets. By merely capturing enough packets, attackers can extract a target's username and password if the victim authenticates themselves in public networks, especially on unsecured websites. Once a password is hacked, an attacker can use the password to interfere with the victim's accounts such as by logging into the victim's email account, logging onto PayPal and draining the victim's bank account, or even change the password.

As a preventive measure, an organization's administrator should advice employees not to provide sensitive information while in public networks without HTTPS connections. VPN and SSH tunneling must be used to secure the network connection. An expert ethical hacker and penetration tester (hereafter, pen tester) must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), authentication mechanisms, and encryption techniques.

Another effective method for obtaining usernames and passwords is by using Cain & Abel to perform MITM attacks.

An MITM attack is used to intrude into an existing connection between systems and to intercept the messages being exchanged. Using various techniques, attackers split the TCP connection into two connections—a client-to-attacker connection and an attacker-to-server connection. After the successful interception of the TCP connection, the attacker can read, modify, and insert fraudulent data into the intercepted communication.

MITM attacks are varied and can be carried out on a switched LAN. MITM attacks can be performed using various tools such as Cain & Abel.

Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

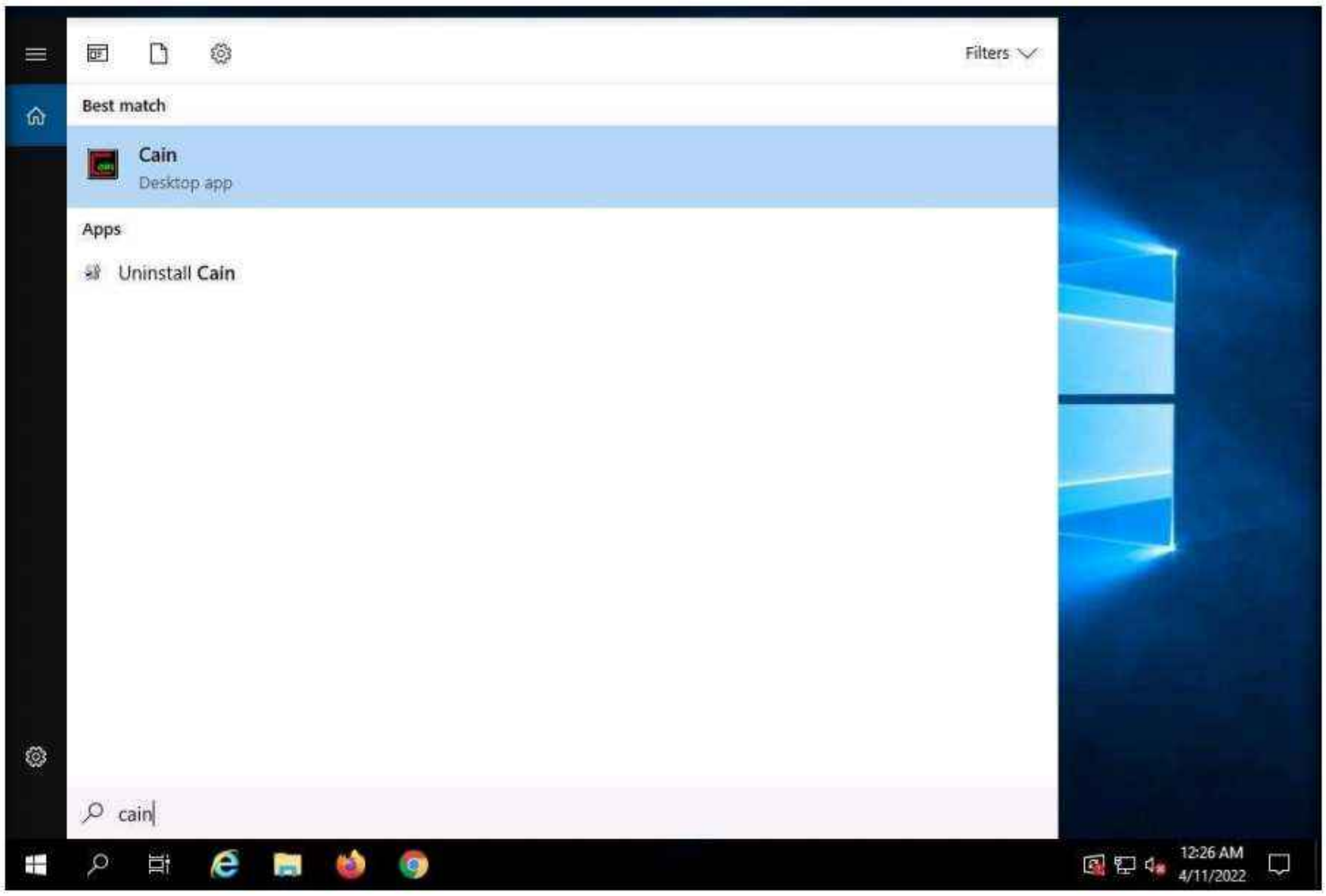
Here, we will use the Cain & Abel tool to perform an MITM attack.

Note: Ensure that **Windows 11** and **Parrot Security** virtual machines are running.

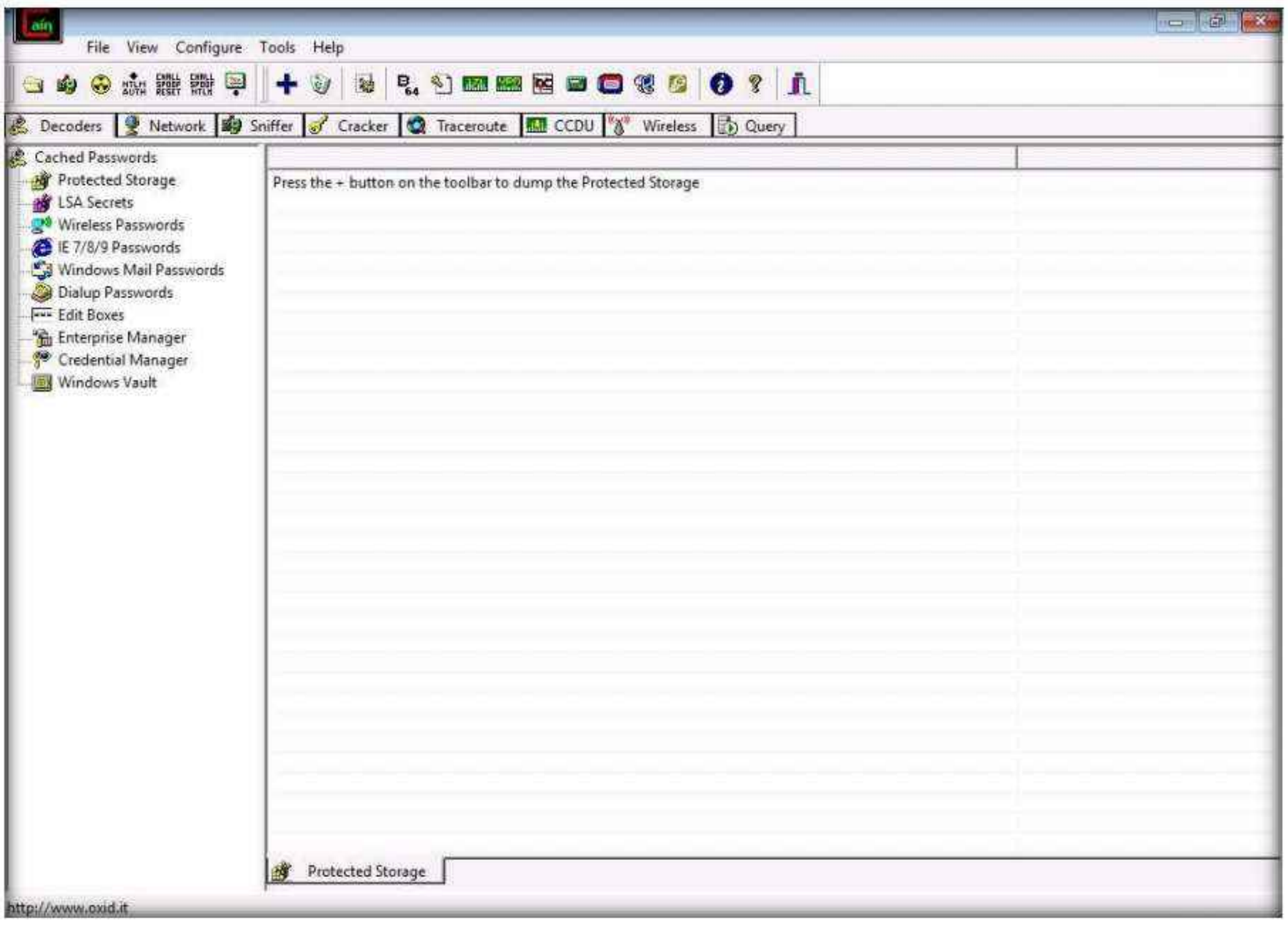
1. Turn on the **Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

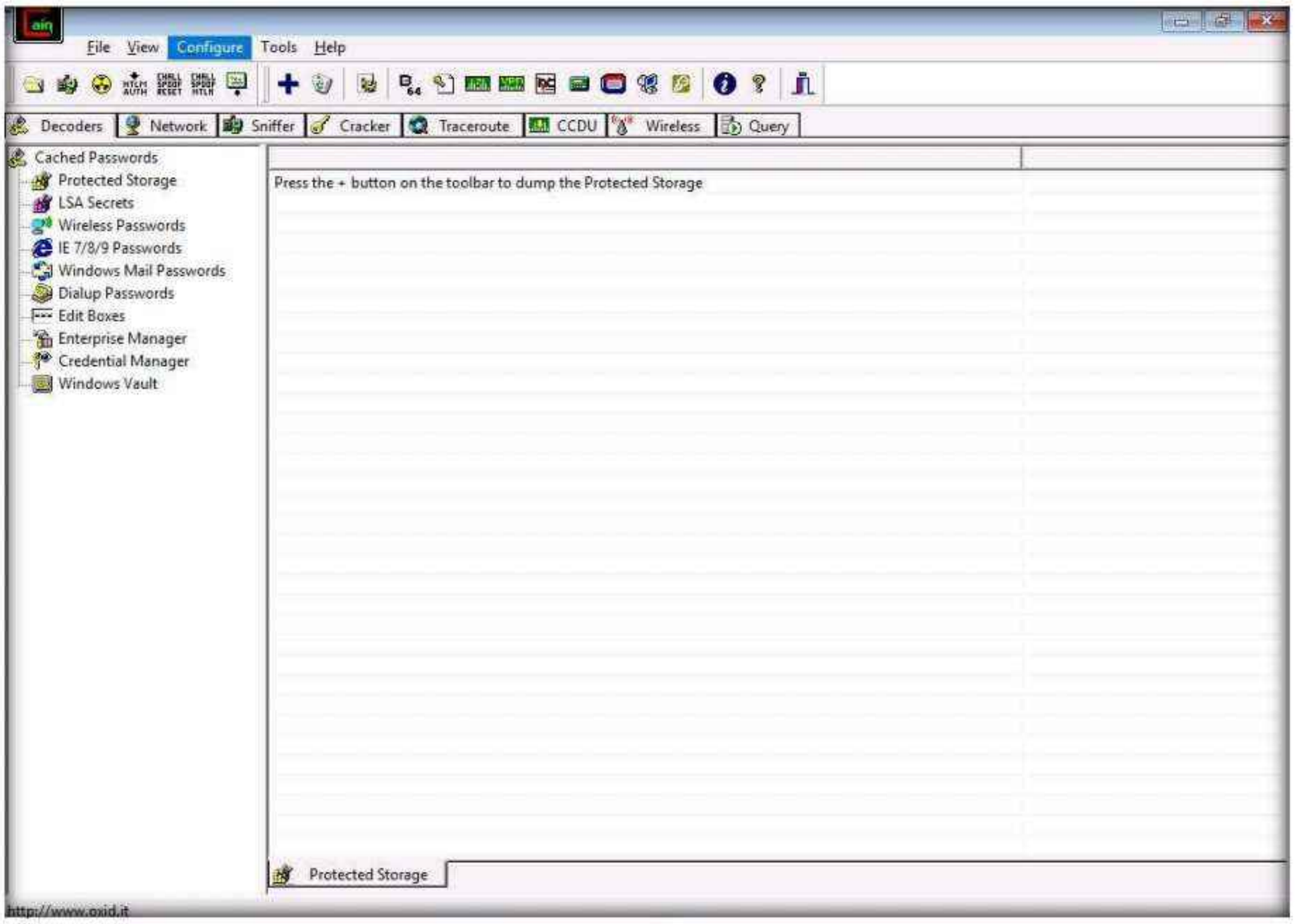
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



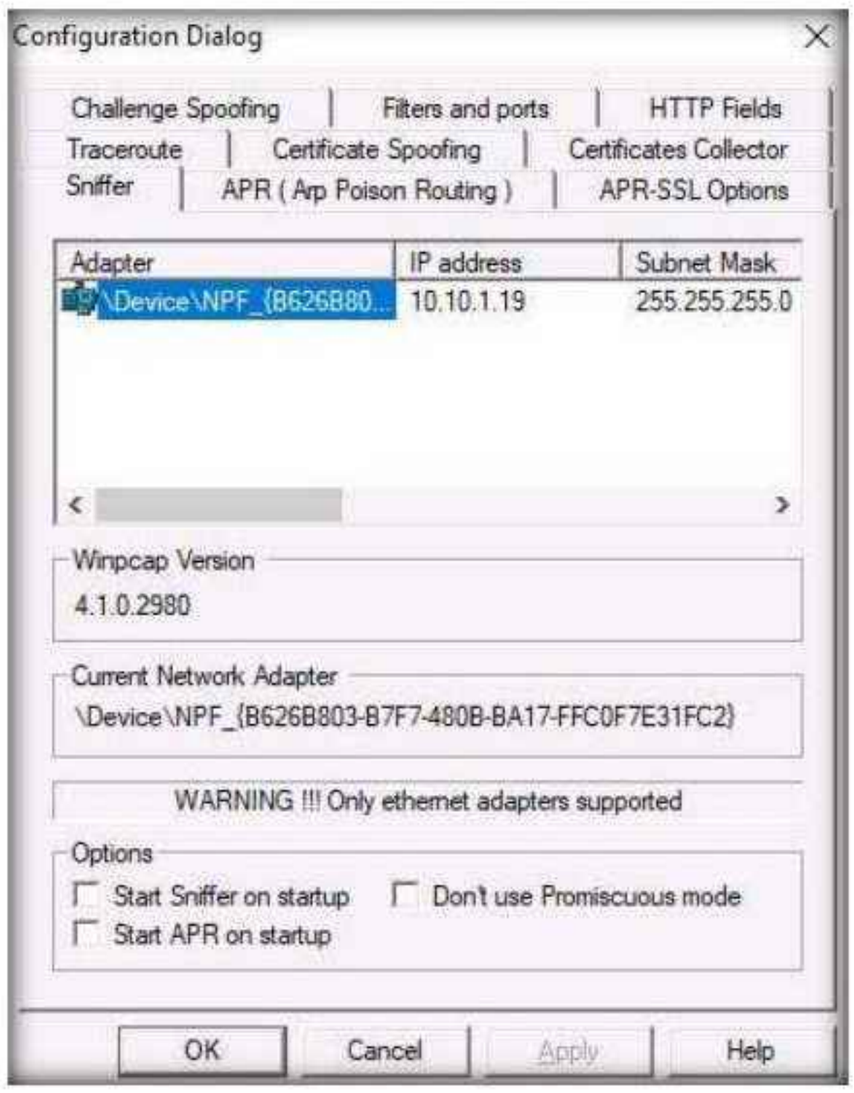
4. The **Cain & Abel** main window appears, as shown in the screenshot.



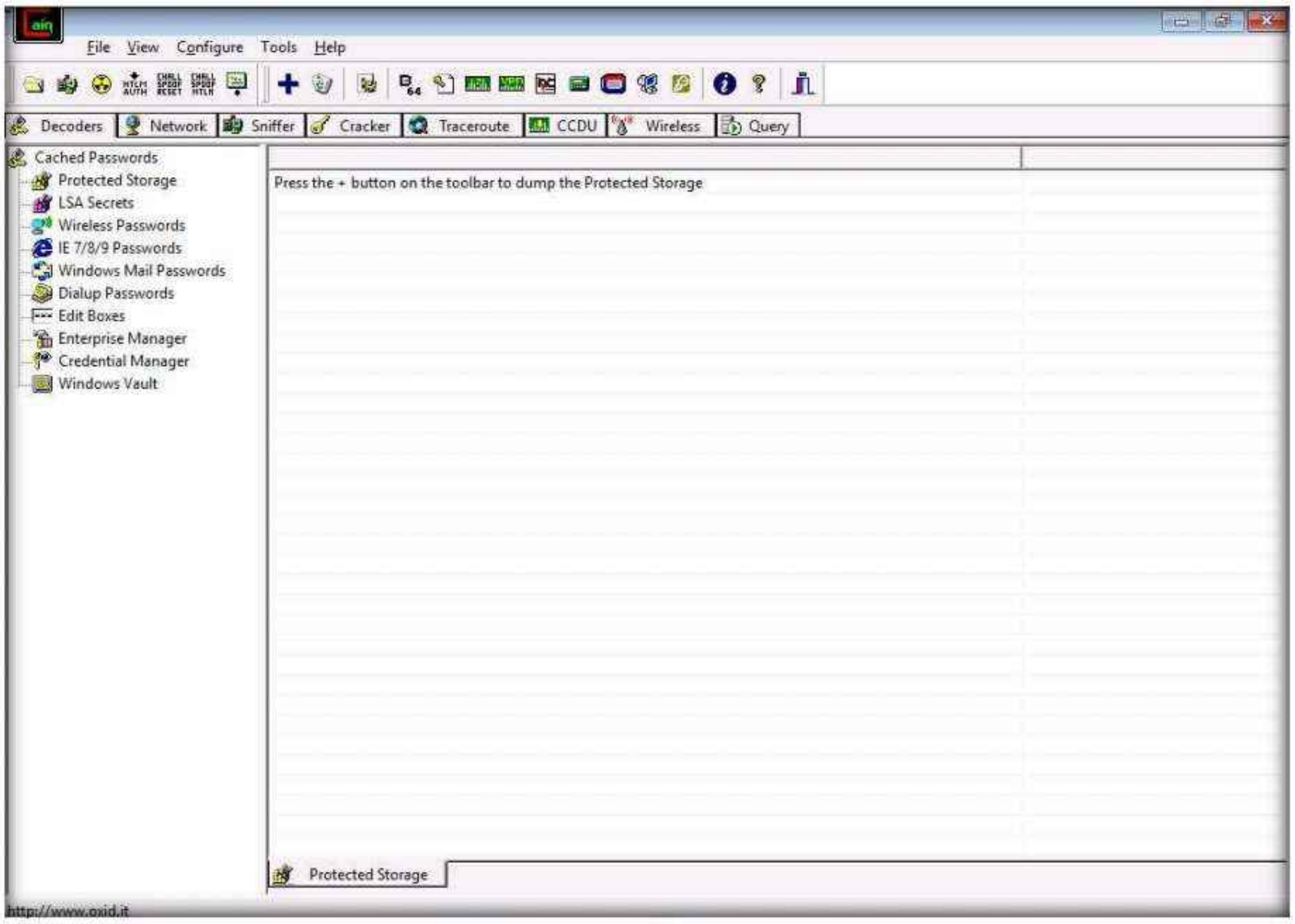
5. Click **Configure** from the menu bar to configure an ethernet card.



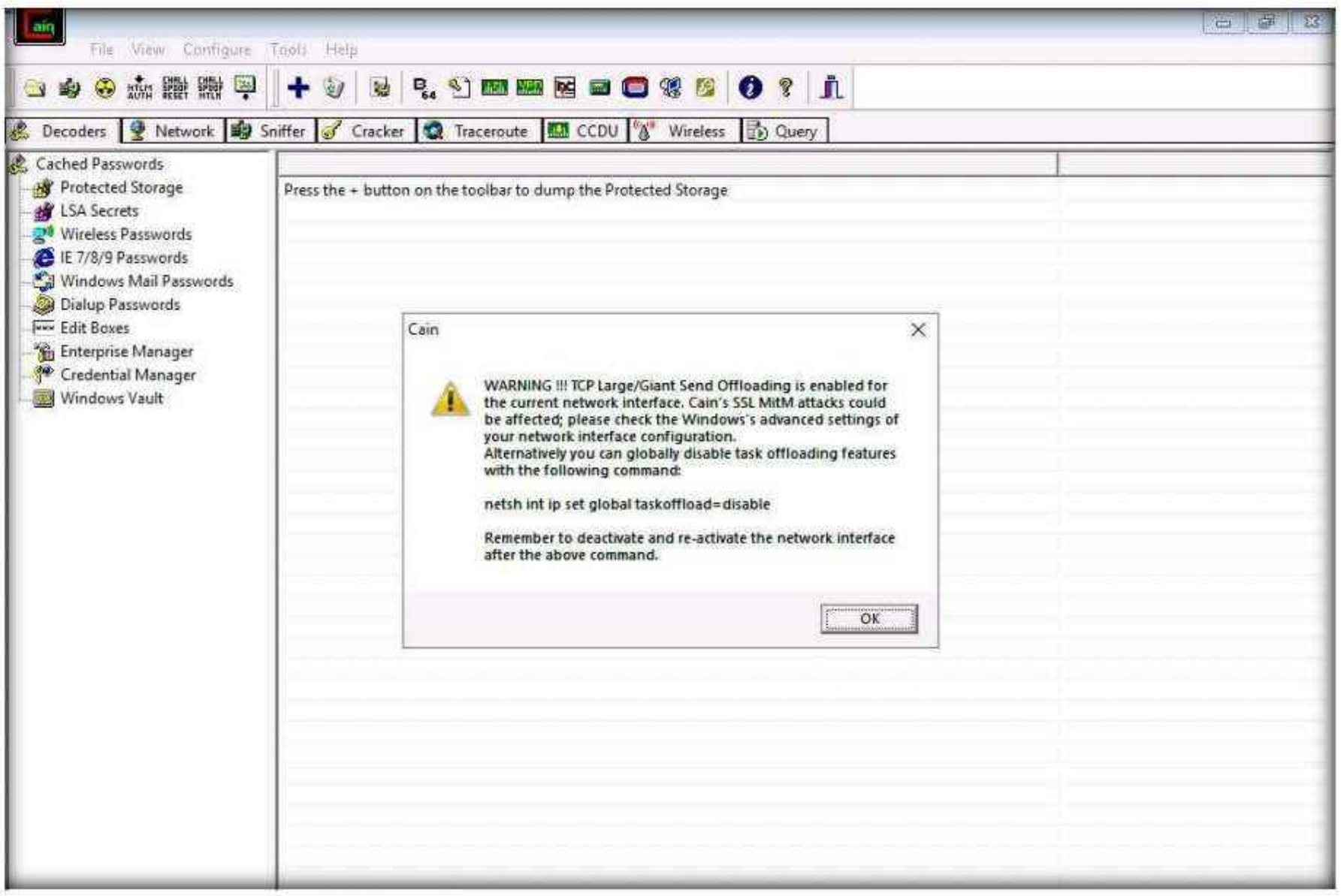
6. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.



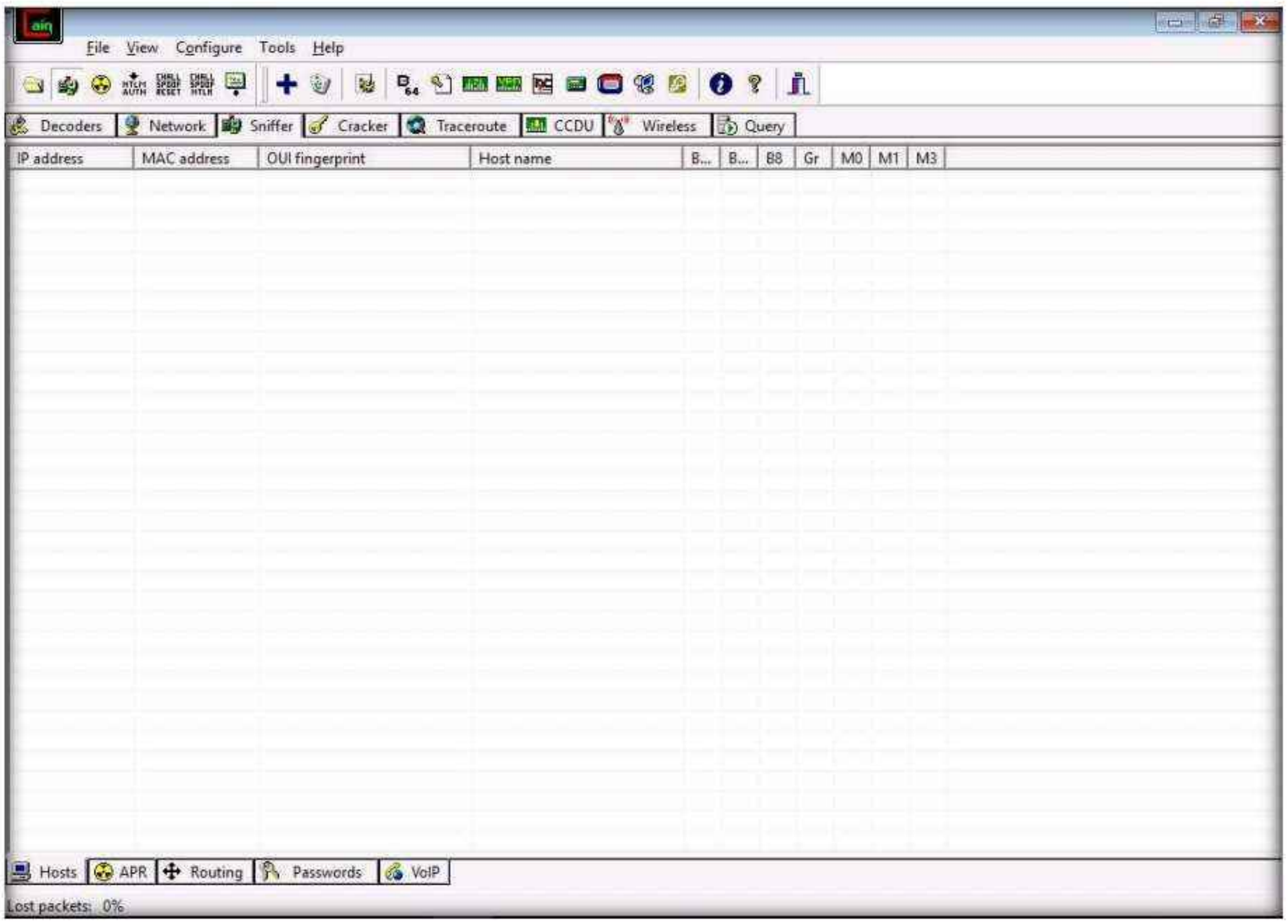
7. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



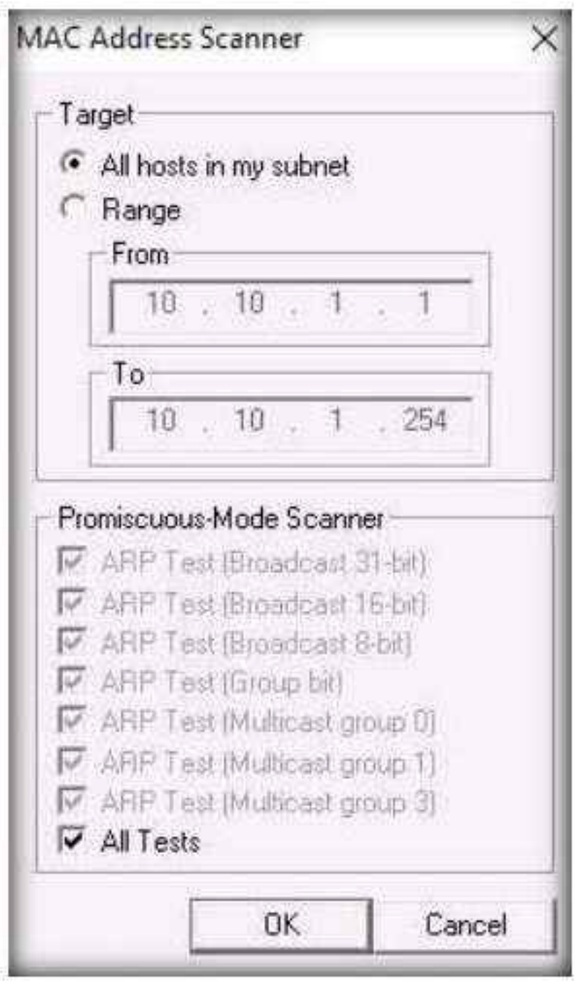
8. A **Cain** pop-up appears and displays a **Warning** message; click **OK**.



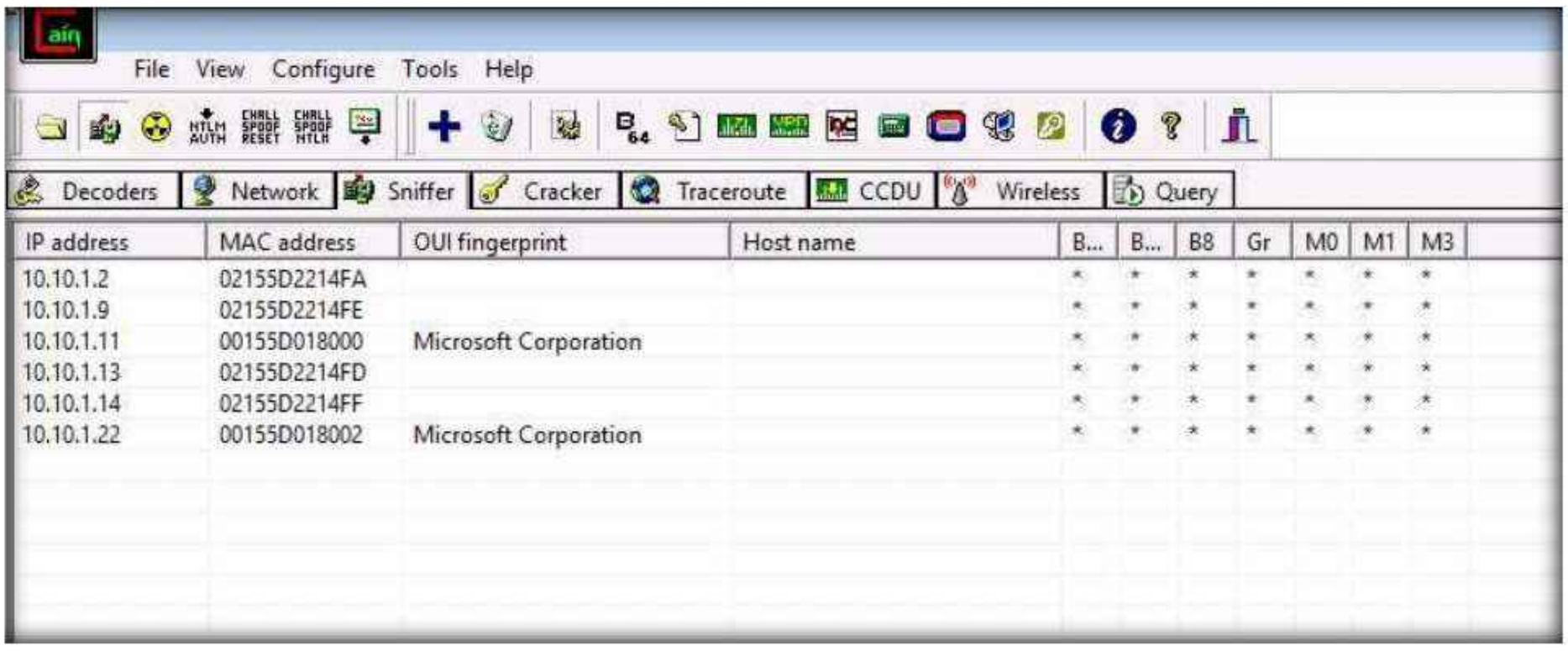
9. Now, click the **Sniffer** tab.



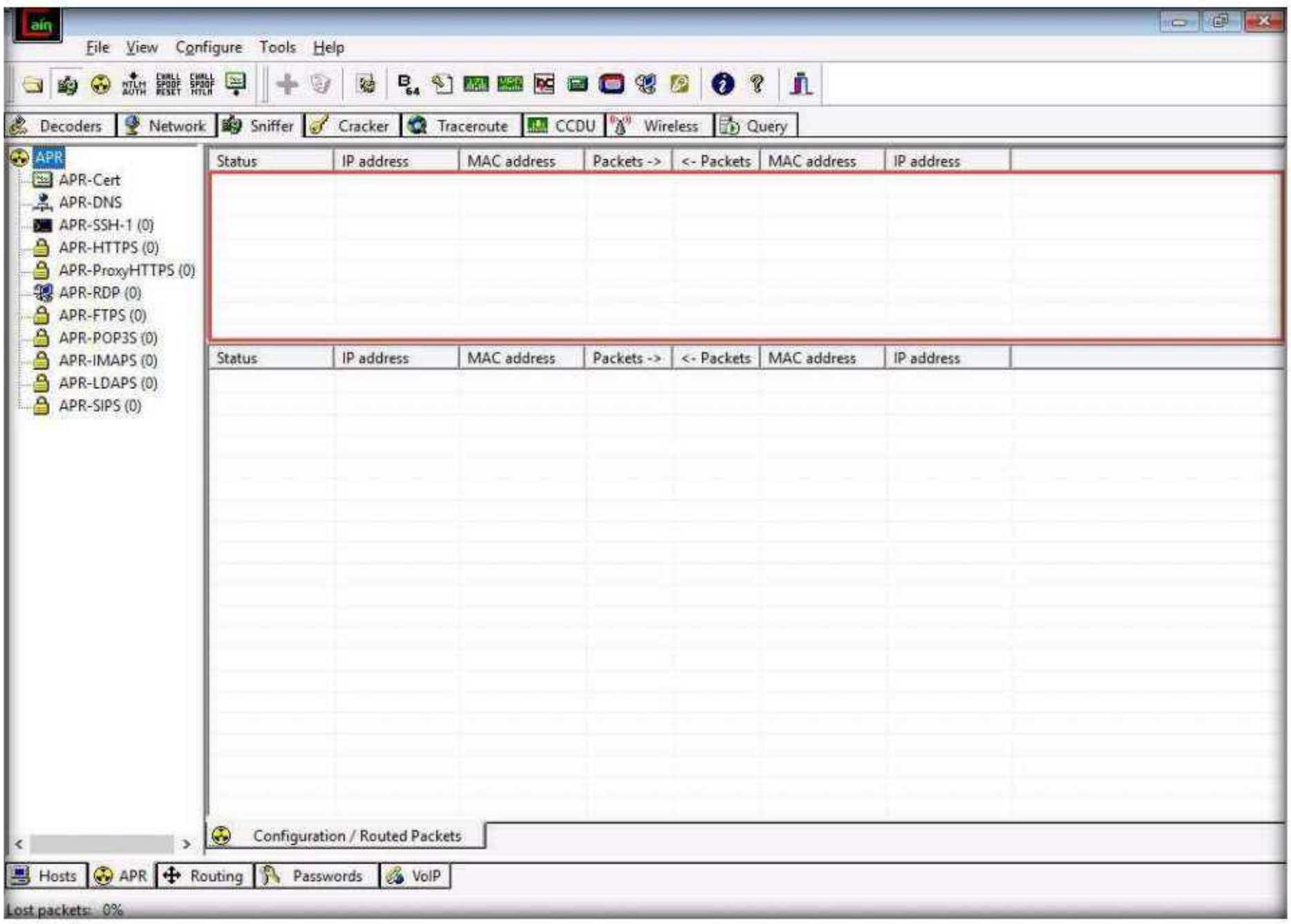
10. Click the plus (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
11. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.



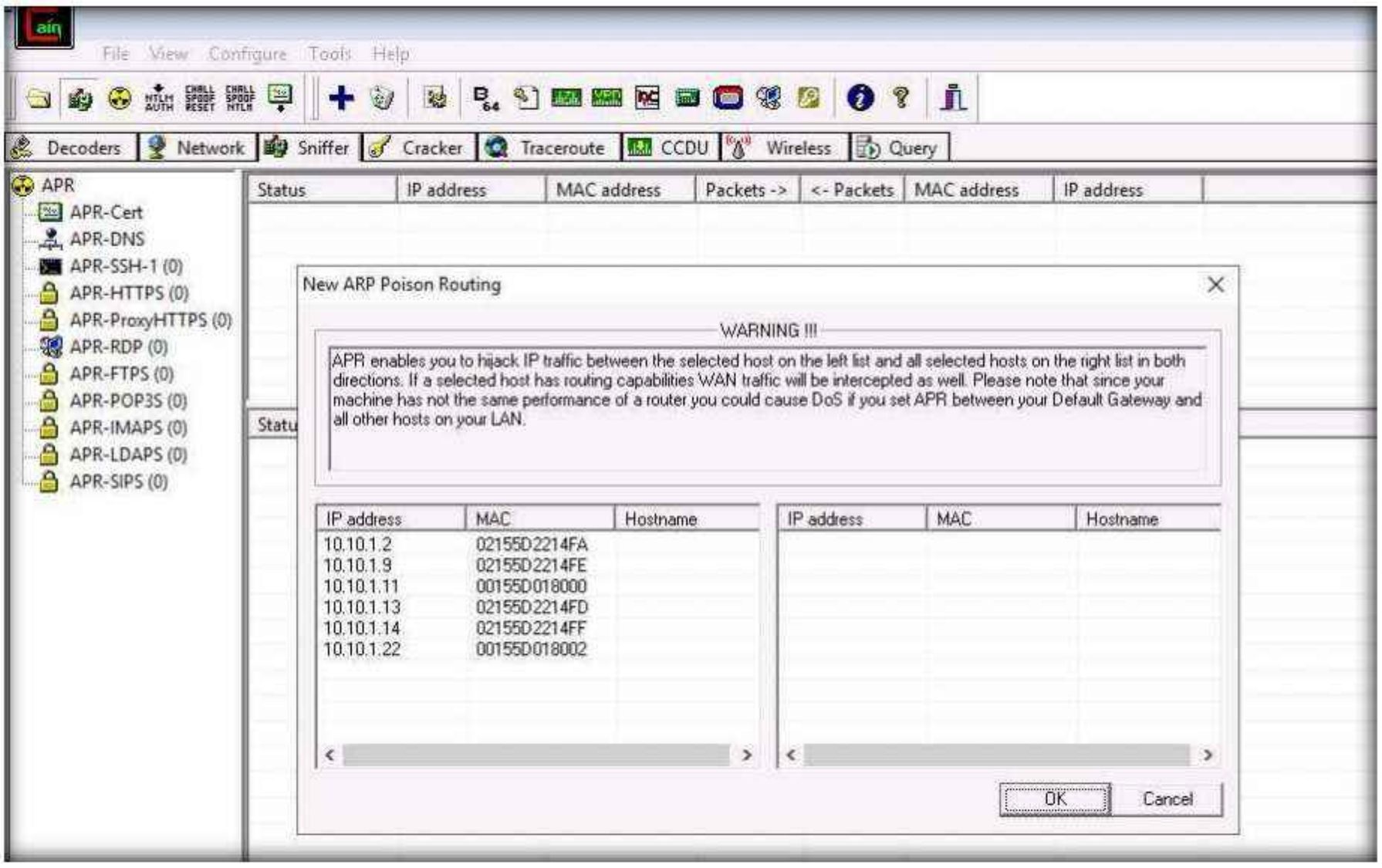
12. Cain & Abel starts scanning for MAC addresses and lists all those found.
13. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.



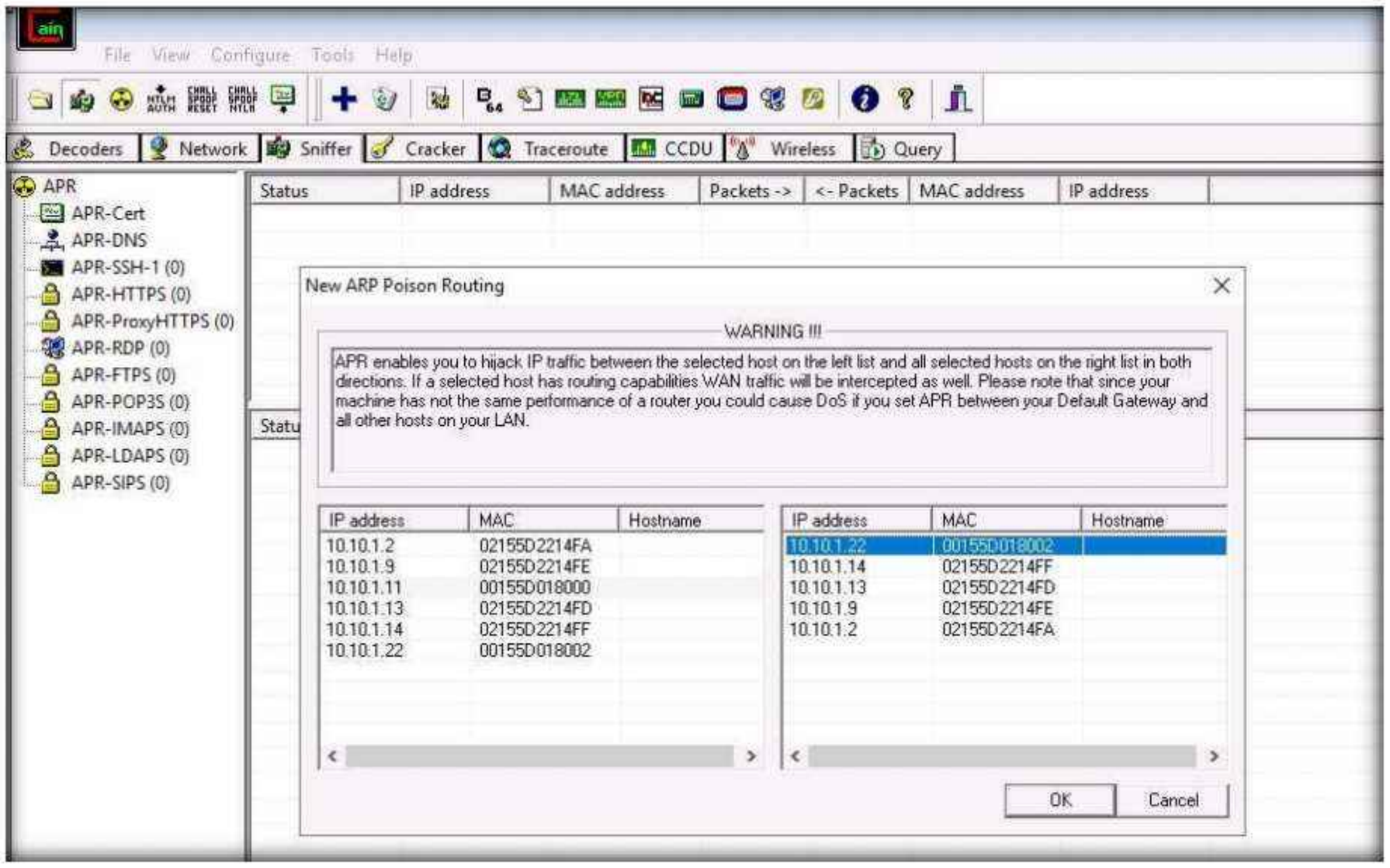
14. Now, click the **APR** tab at the bottom of the window.
15. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.



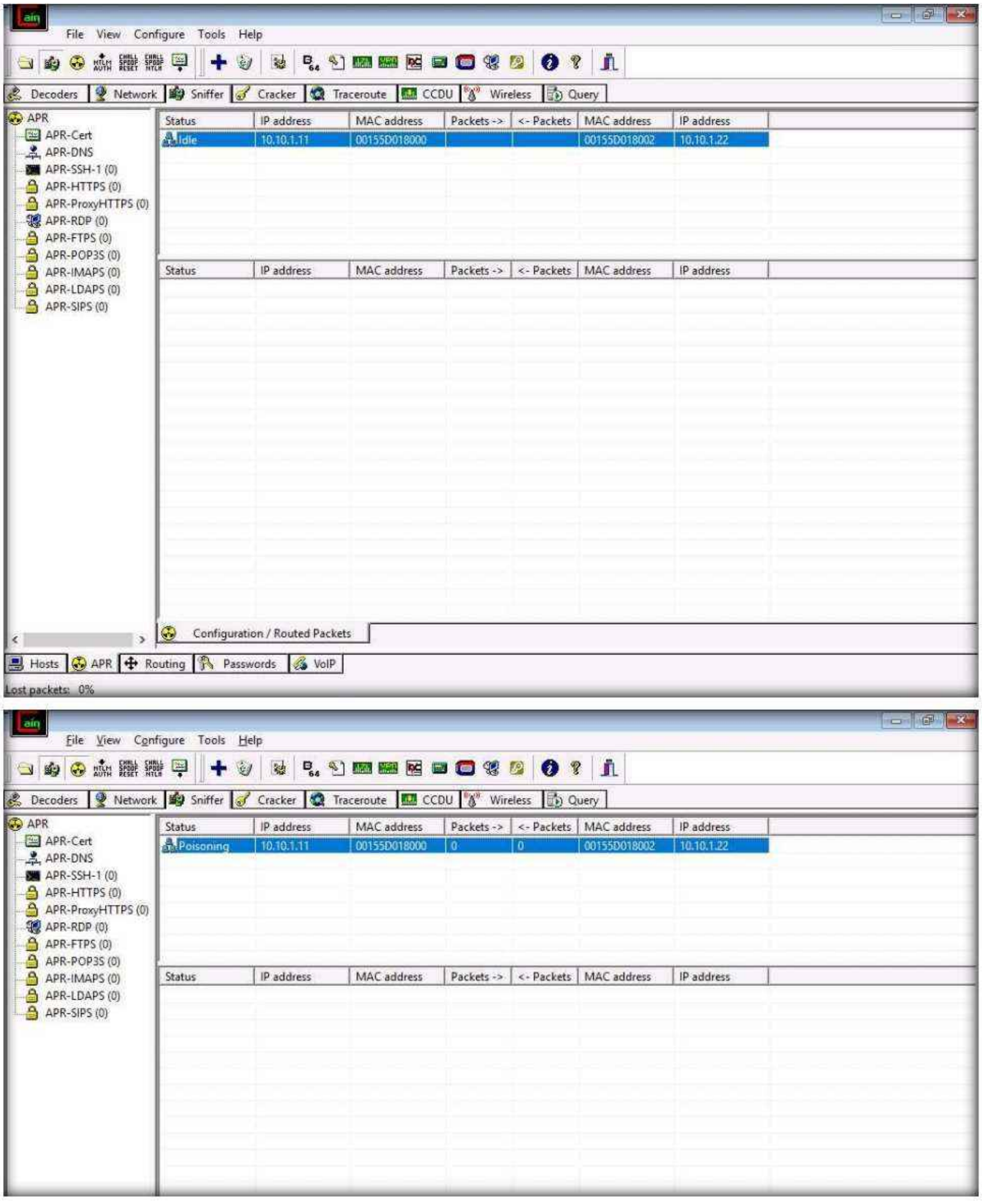
16. Click the plus (**+**) icon, a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.



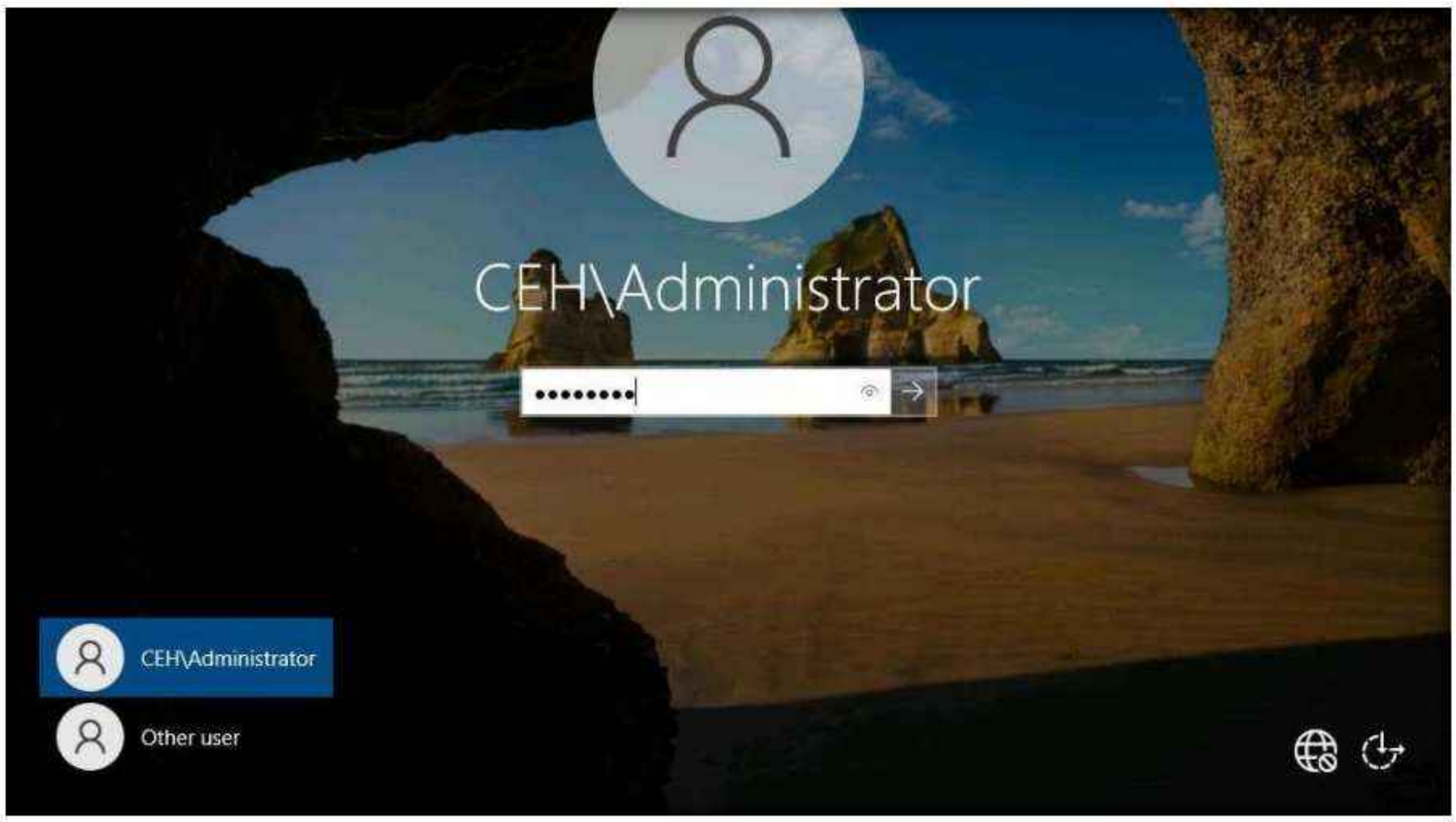
17. To monitor the traffic between two systems (here, **Windows 11** and **Windows Server 2022**), click to select **10.10.1.11** (Windows 11) from the left-hand pane and **10.10.1.22** (**Windows Server 2022**) from the right-hand pane; click **OK**.



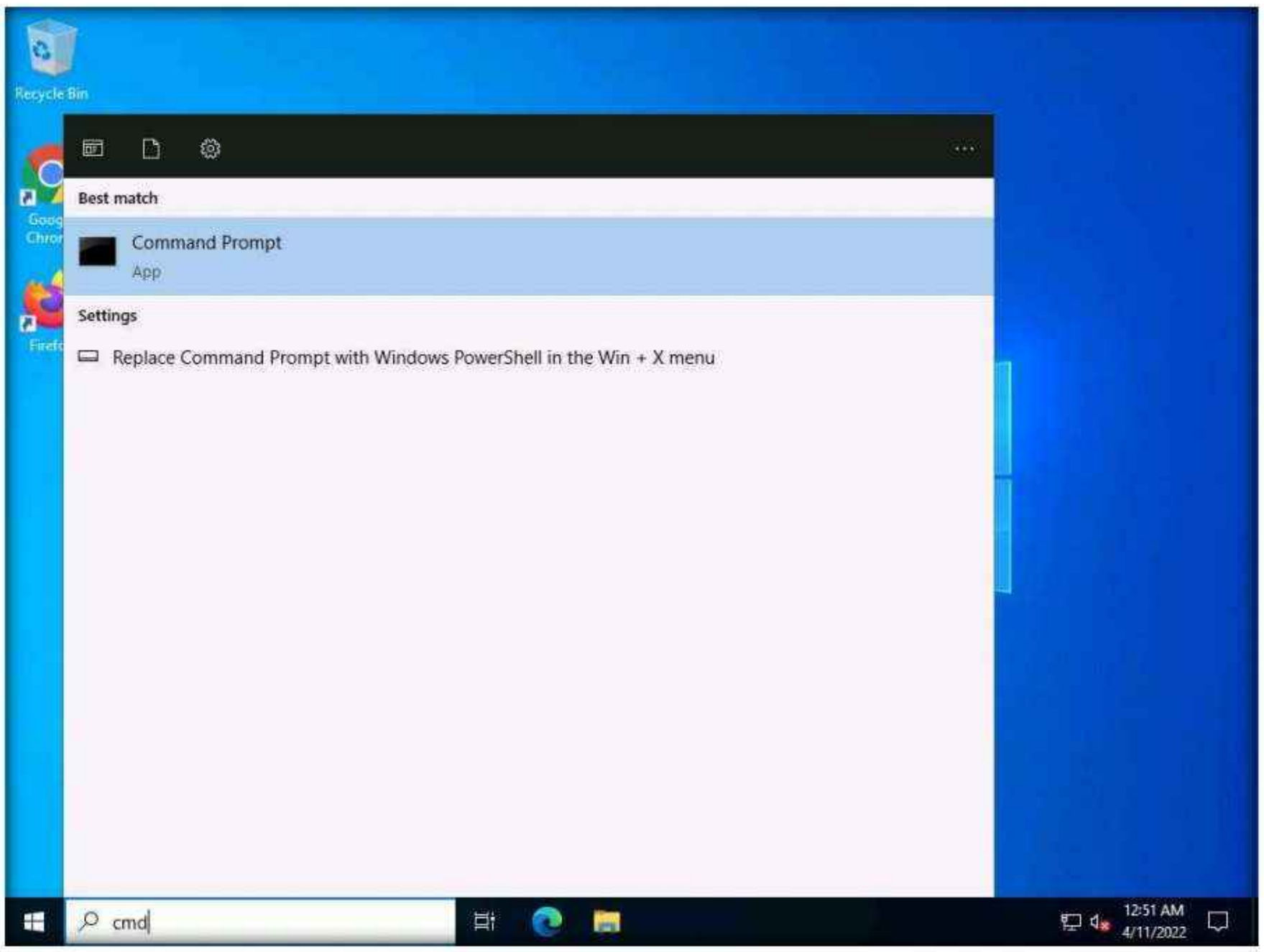
18. Click to select the created target IP address scan displayed in the **Configuration / Routes Packets** tab.
19. Click on the **Start/Stop APR** icon to start capturing ARP packets. The **Status** will change from **Idle** to **Poisoning**.



20. Switch to the **Windows Server 2022** virtual machine, click **Ctrl+Alt+Del**. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

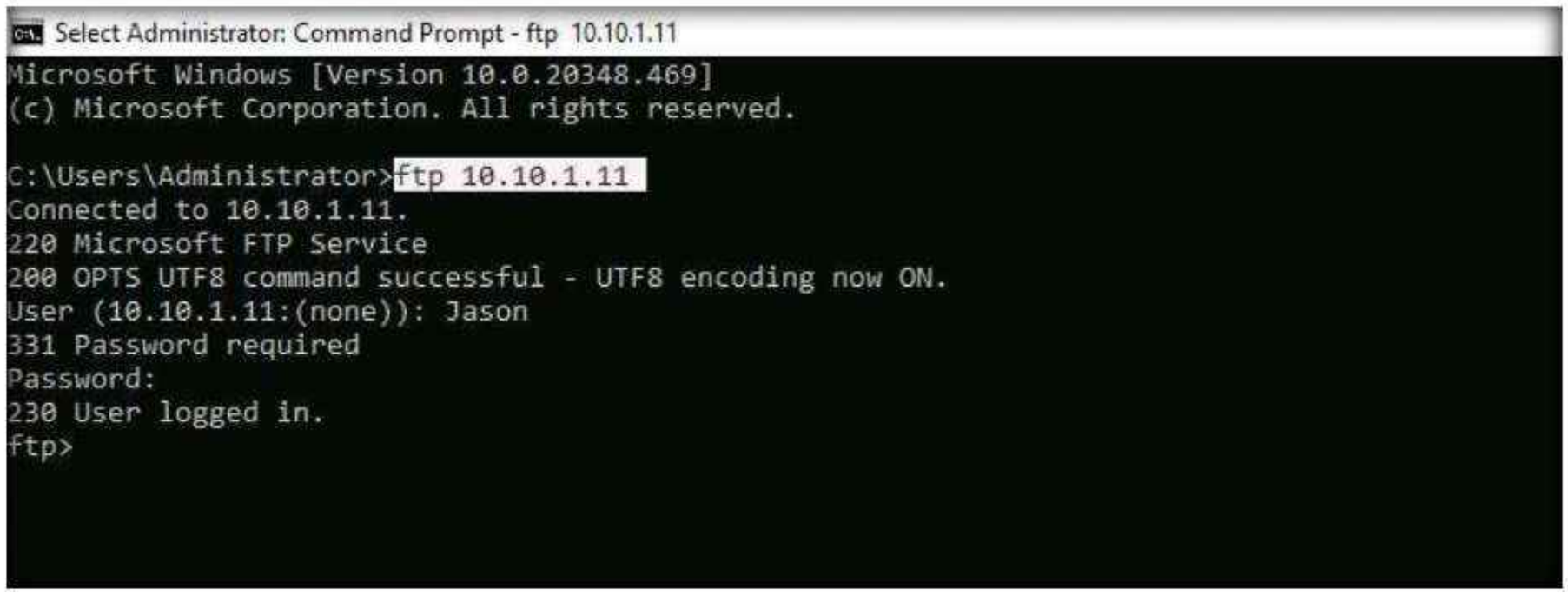


21. Click the **Type here to search** icon at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.

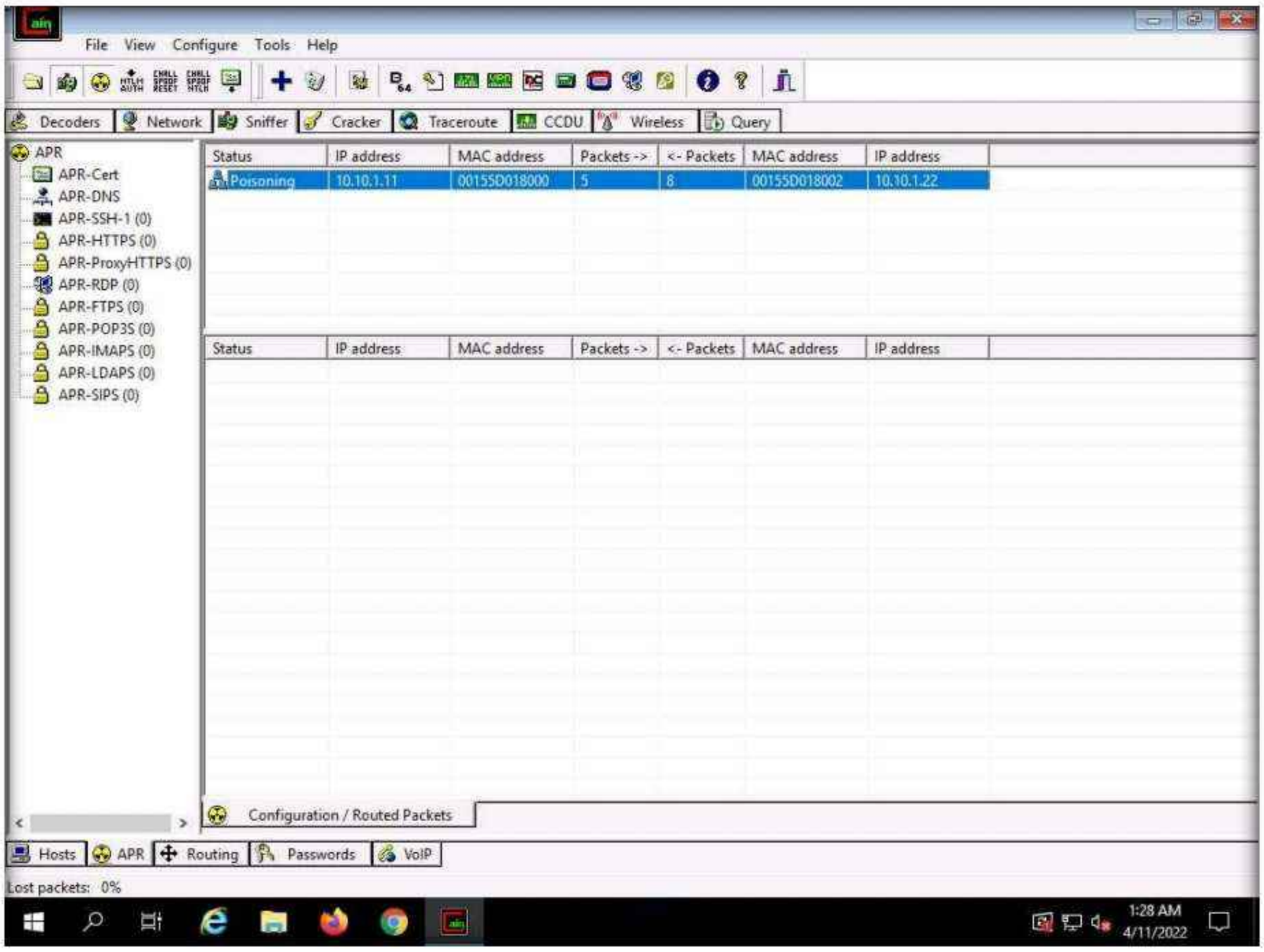


22. The **Command Prompt** window appears; type **ftp 10.10.1.11** (the IP address of **Windows 11**) and press **Enter**.
23. When prompted for a **User**, type "**Jason**" and press **Enter**; for a **Password**, type "**qwerty**" and press **Enter**.

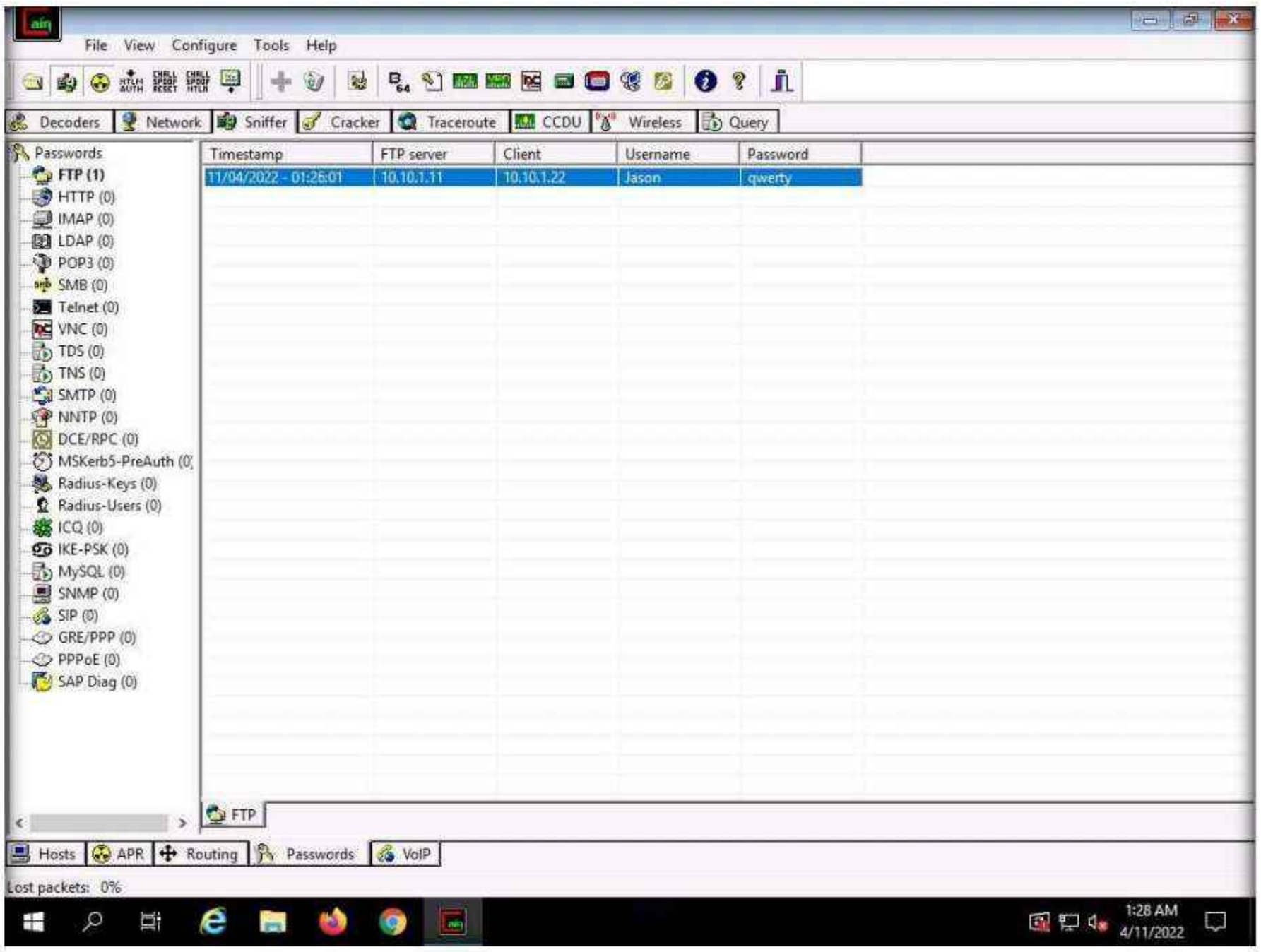
    Note: Irrespective of a successful login, Cain & Abel captures the password entered during login.



24. Switch back to the **Windows Server 2019** virtual machine; observe that the tool lists packet exchange.



25. Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the sniffed password for **ftp 10.10.1.11**, as shown in the screenshot.



Note: In real-time, attackers use the ARP poisoning technique to perform sniffing on the target network. Using this method, attackers can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

26. This concludes the demonstration of how to perform an MITM attack using Cain & Abel.
27. Close all open windows and document all the acquired information.
28. Turn off the **Windows Server 2022**, **Windows Server 2019**, **Parrot Security**, **Ubuntu**, and **Android** virtual machines.

Task 5: Spoof a MAC Address using TMAC and SMAC

A MAC duplicating or spoofing attack involves sniffing a network for the MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then, the attacker spoofs their own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker receives all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user.

If an administrator does not have adequate packet-sniffing skills, it is hard to defend against such intrusions. So, an expert ethical hacker and pen tester must know how to spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. This lab demonstrates how to spoof a MAC address to remain unknown to an attacker.

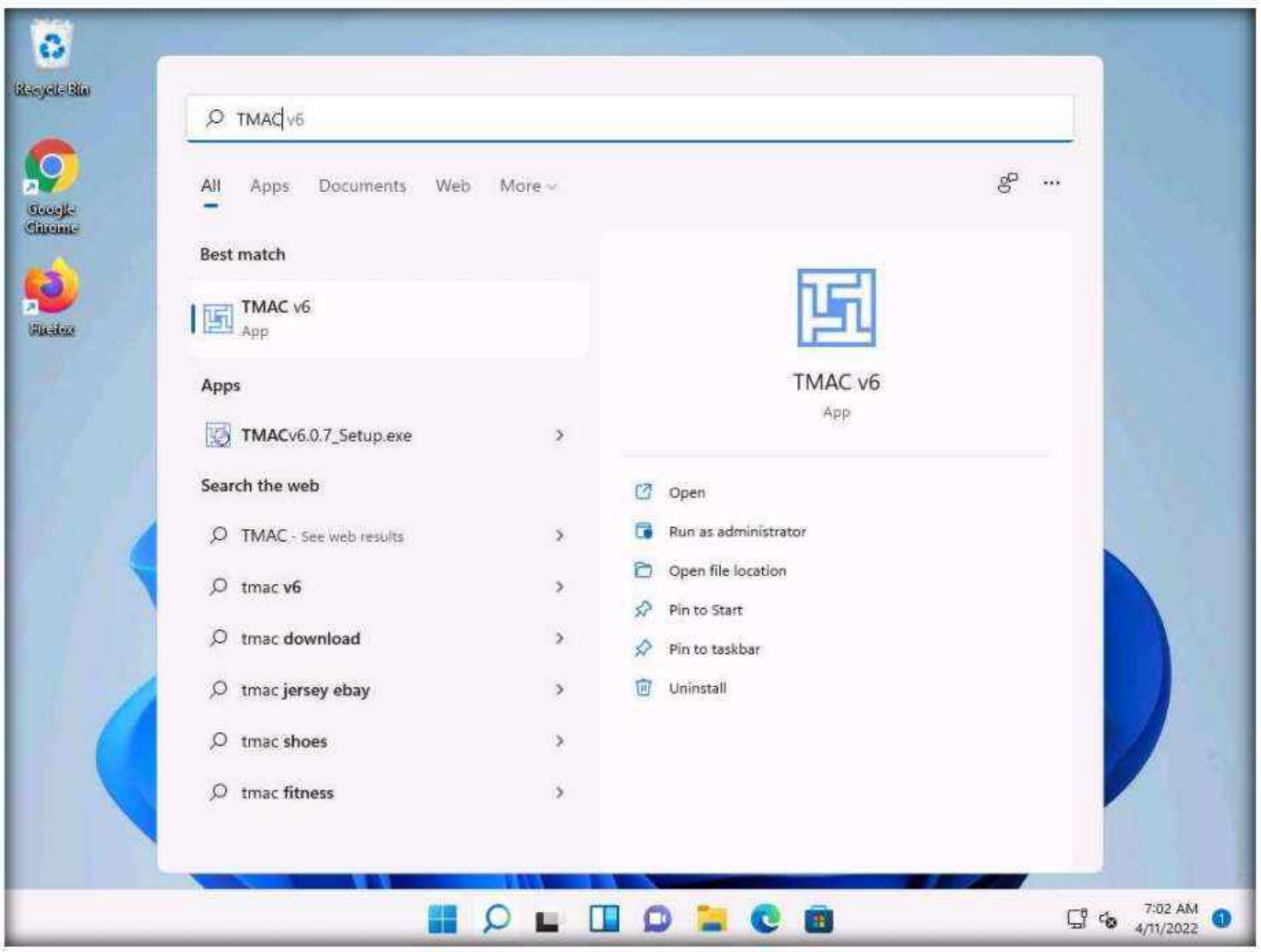
Here, we will use TMAC and SMAC tools to perform MAC spoofing.

1. Switch to the **Windows 11** machine.

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

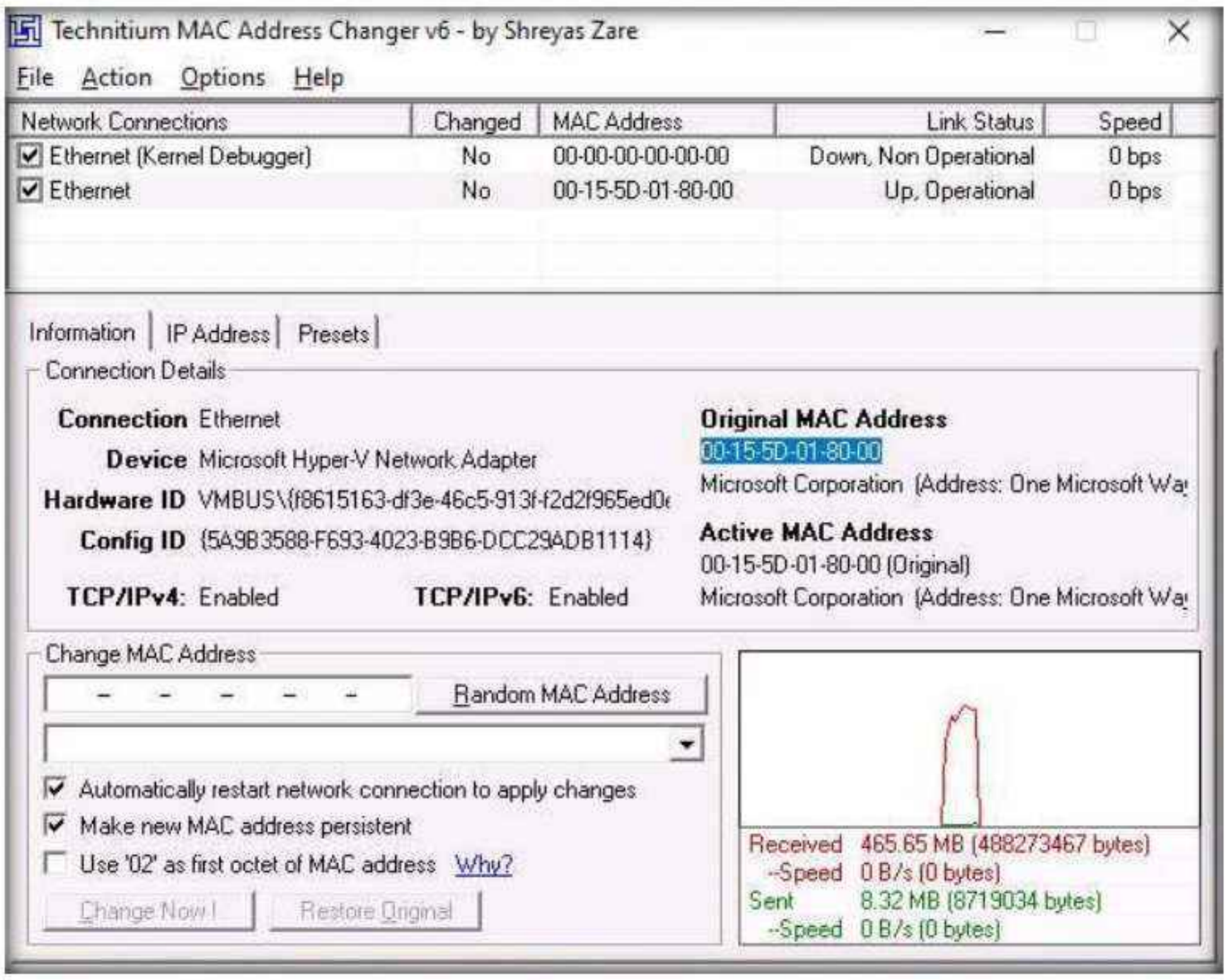
2. Click **Search** icon () on the **Desktop**. Type **TMAC** in the search field, the **TMAC v6** appears in the results, click **Open** to launch it.

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

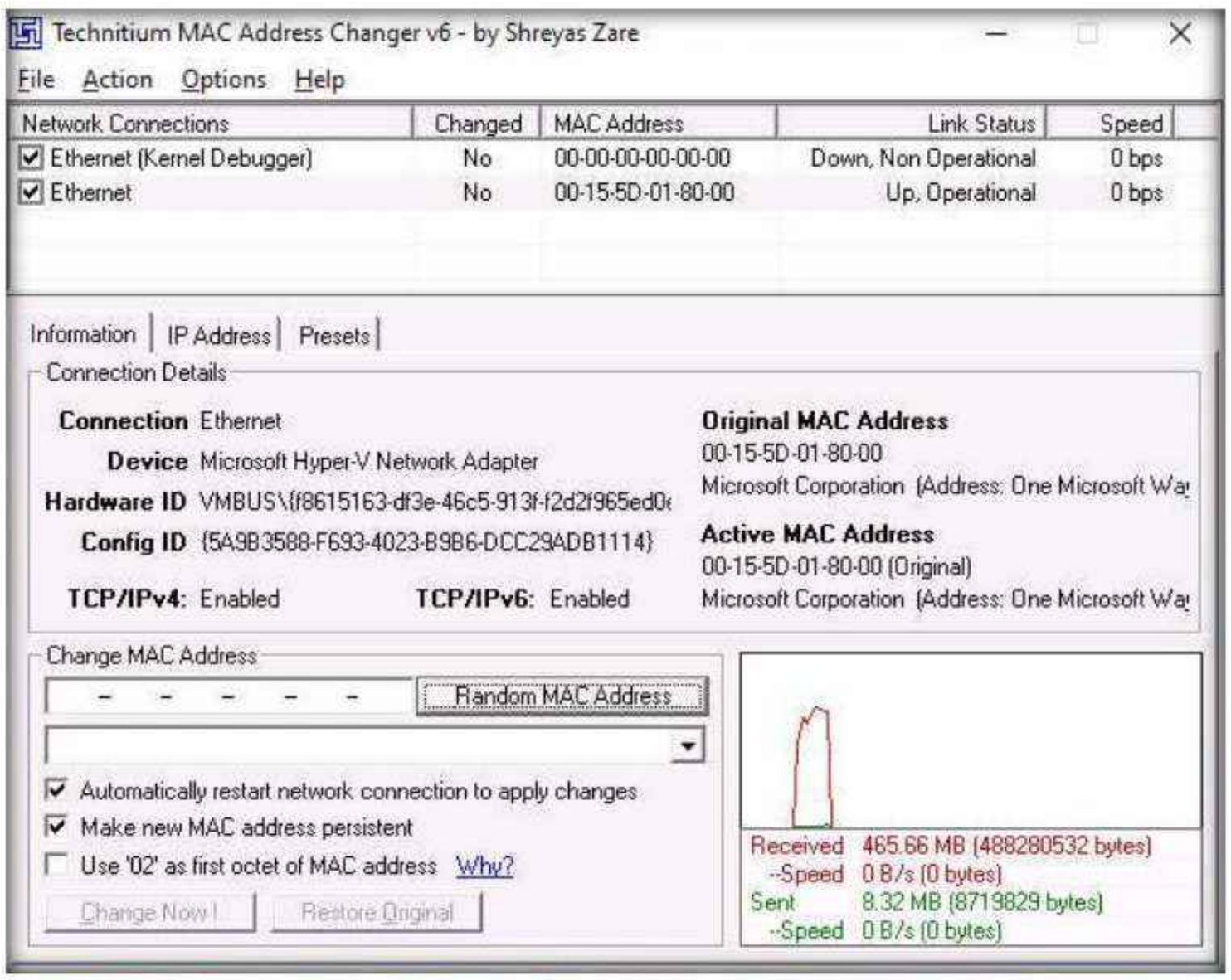


3. The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.
4. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet**).

5. Under the **Information** tab, note the **Original MAC Address** of the network adapter, as shown in the screenshot.

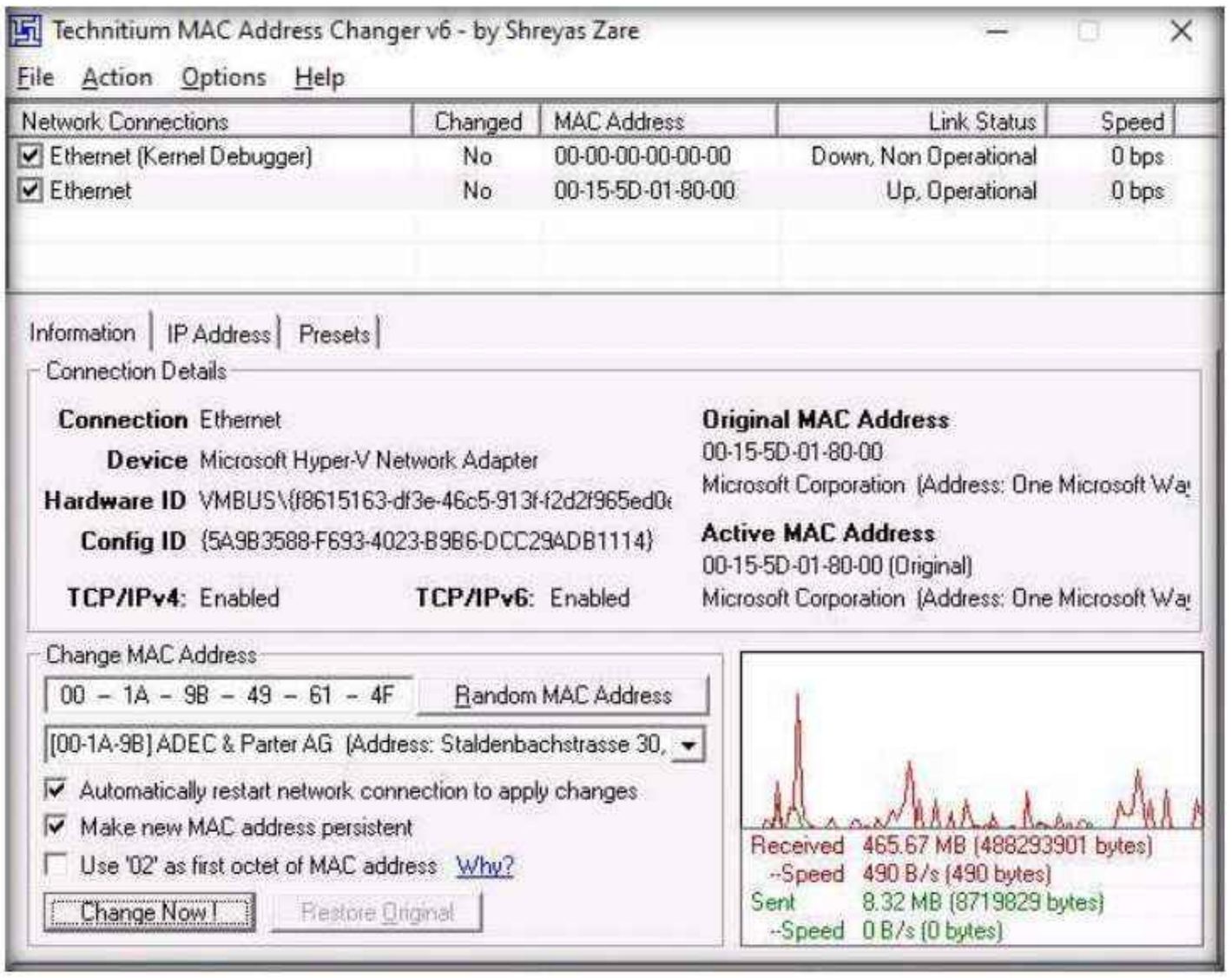


6. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

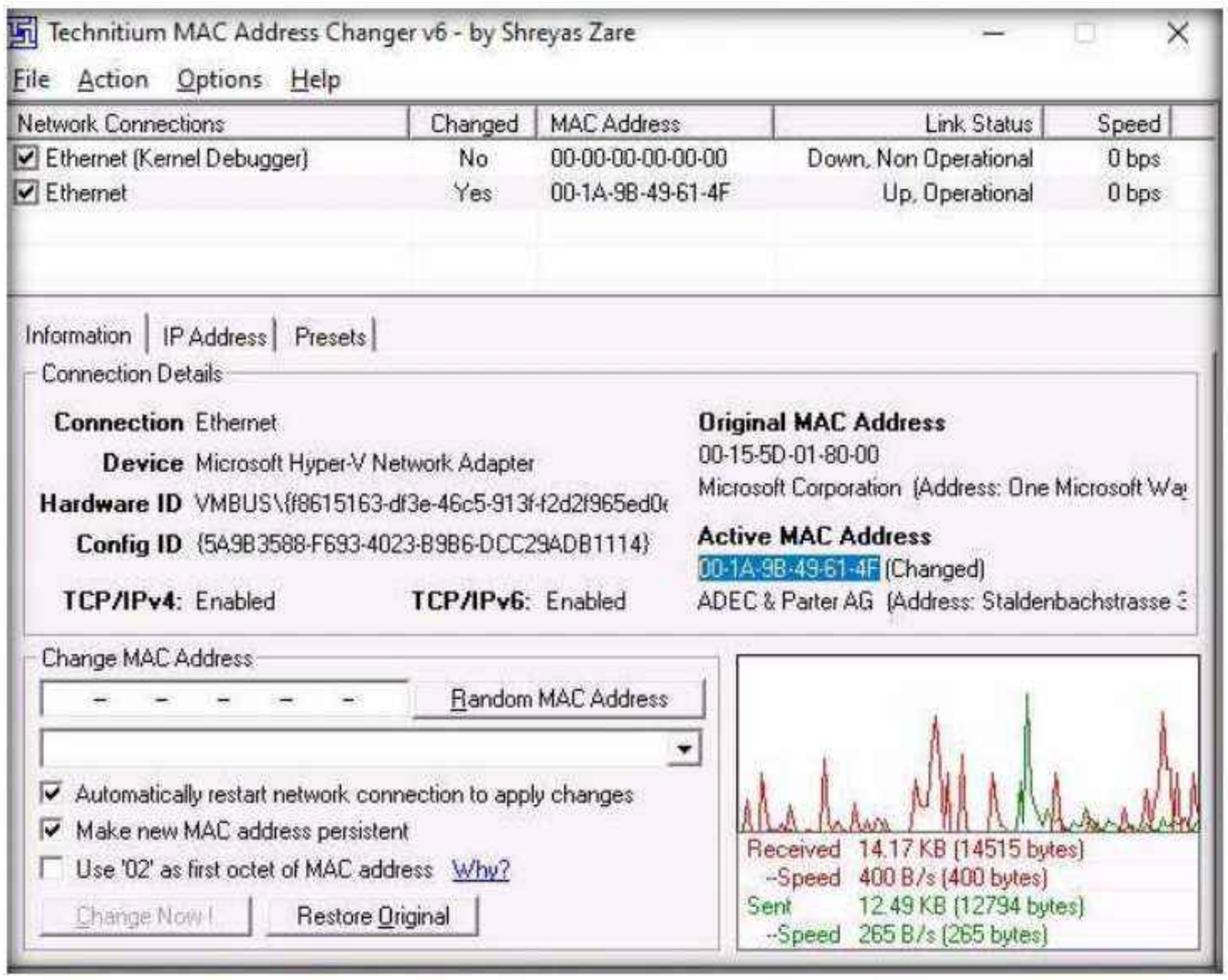


7. A **Random MAC Address** is generated and appears under the **Change MAC Address** field. Click the **Change Now !** button to change the MAC address.

   Note: The **MAC Address Changed Successfully** pop-up appears; click **Ok**.

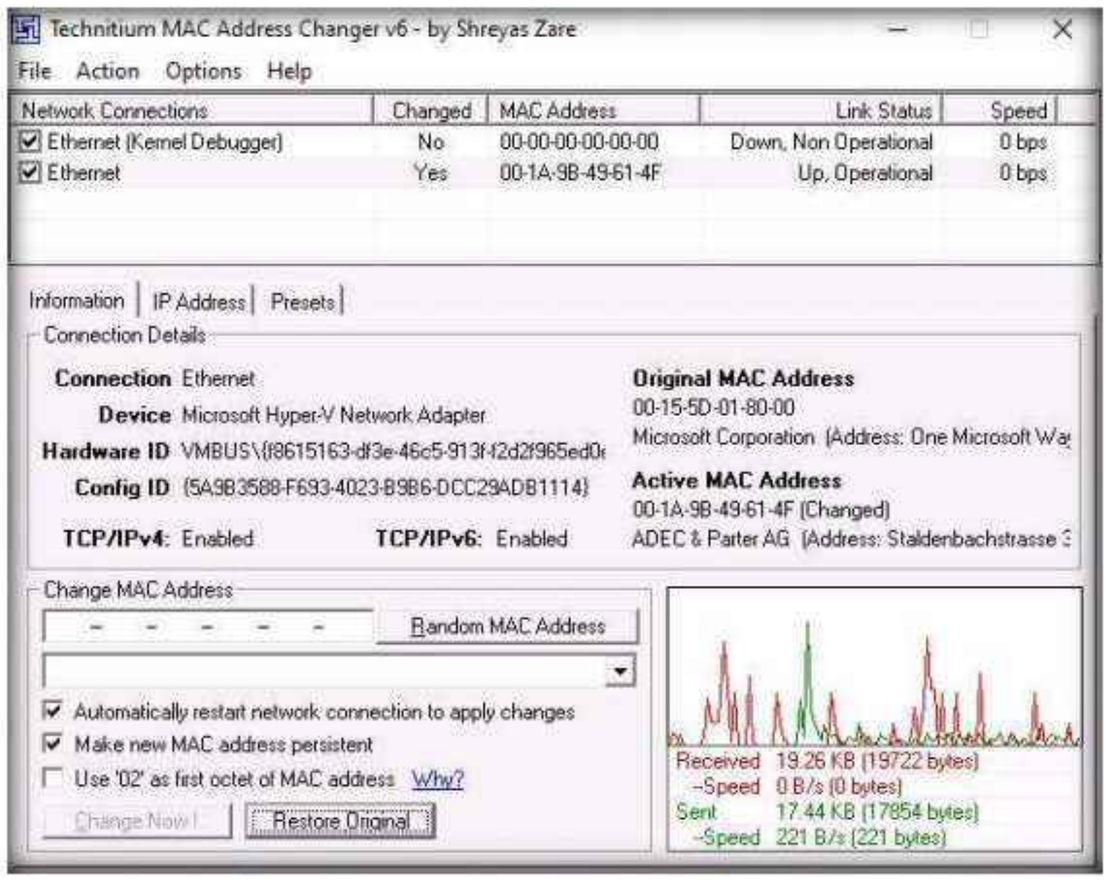


8. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.



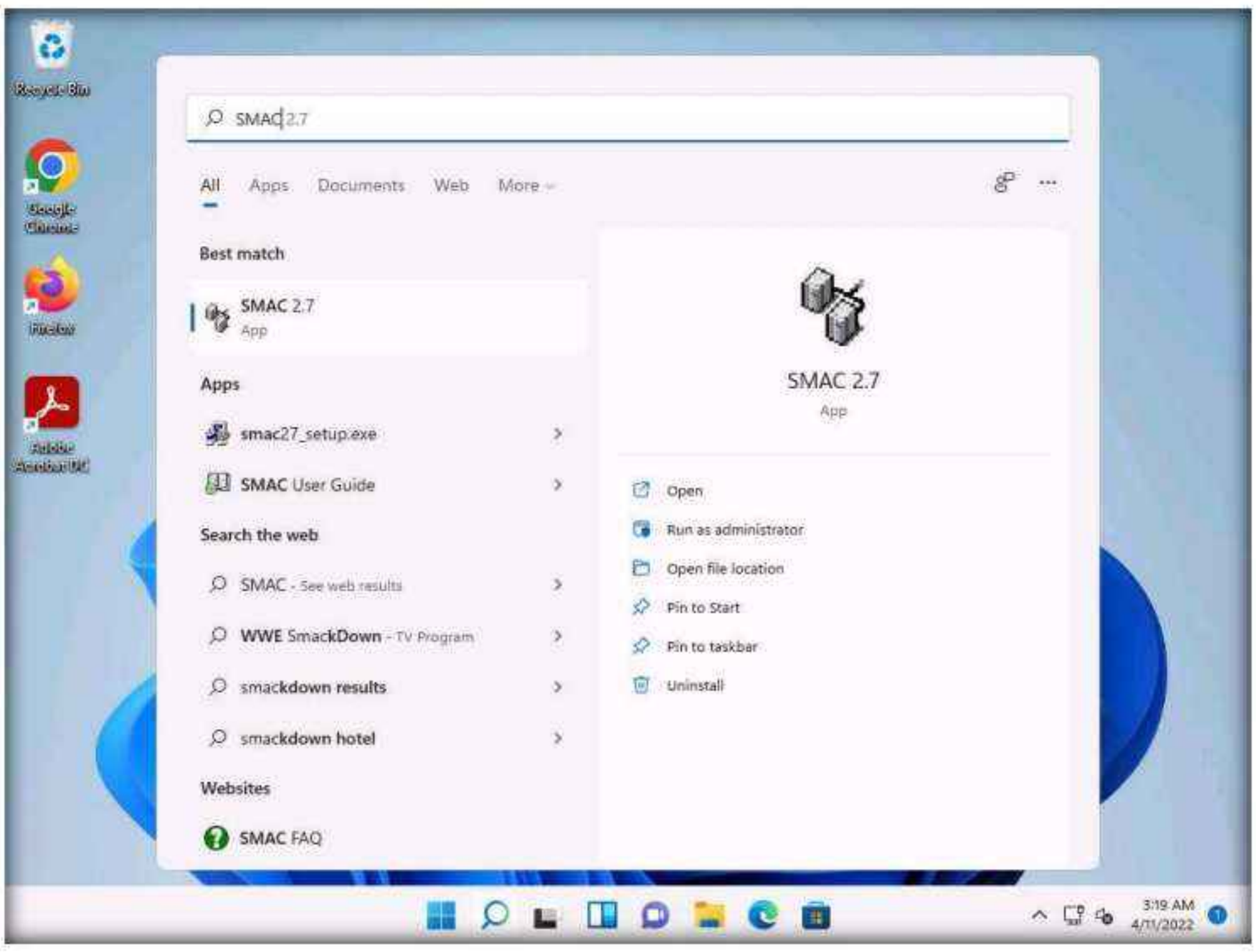
9. To restore the original MAC address, you can click on the **Restore Original** button present at the bottom of the TMAC window.

   Note: The **MAC Address Restored Successfully** pop-up appears; click **OK**.

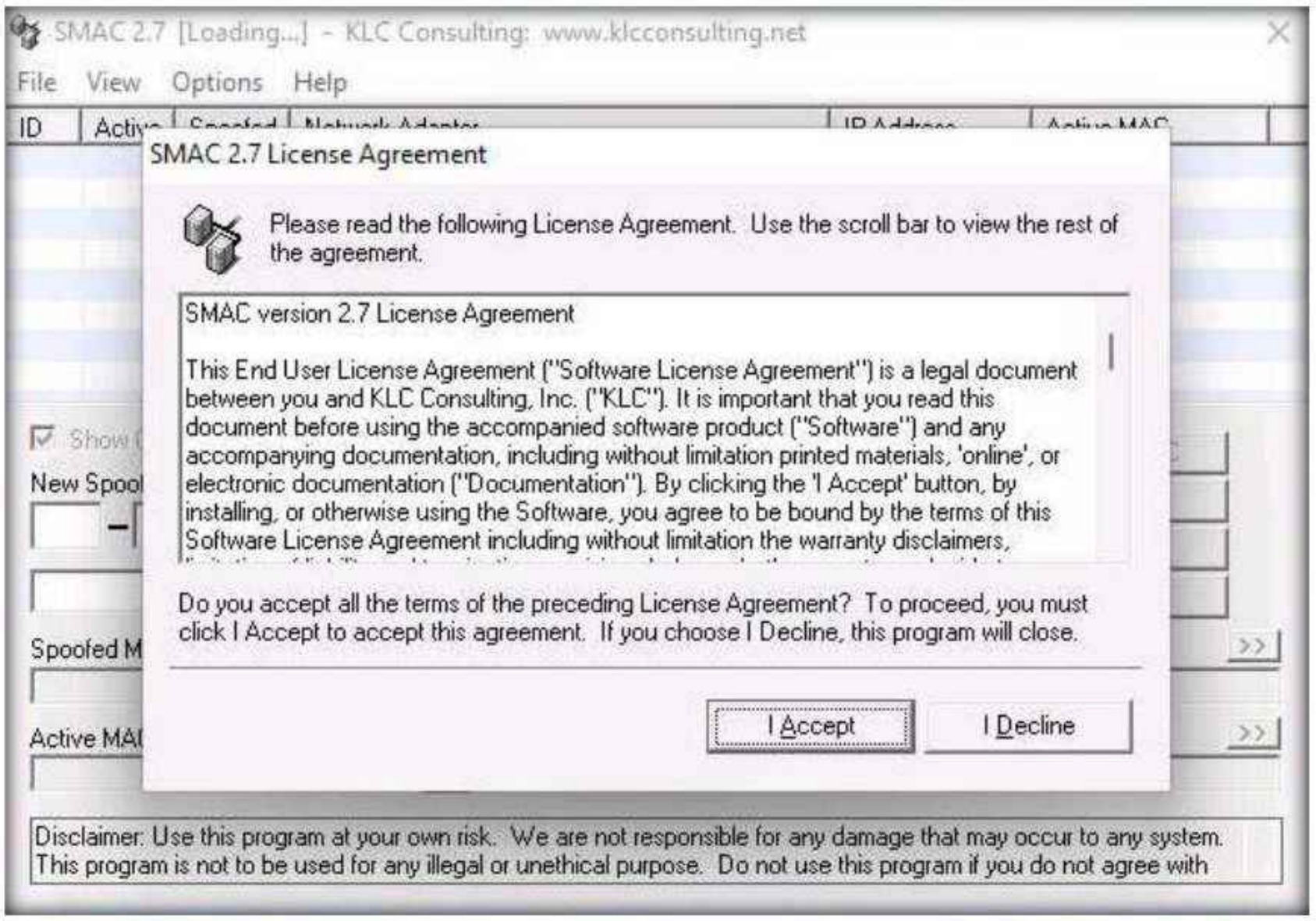


10. Close the **TMAC** main window.
11. Now, we shall perform MAC spoofing using the SMAC tool.
12. Click **Search** icon () on the **Desktop**. Type **SMAC** in the search field, the **SMAC 2.7** appears in the results, click **Open** to launch it.

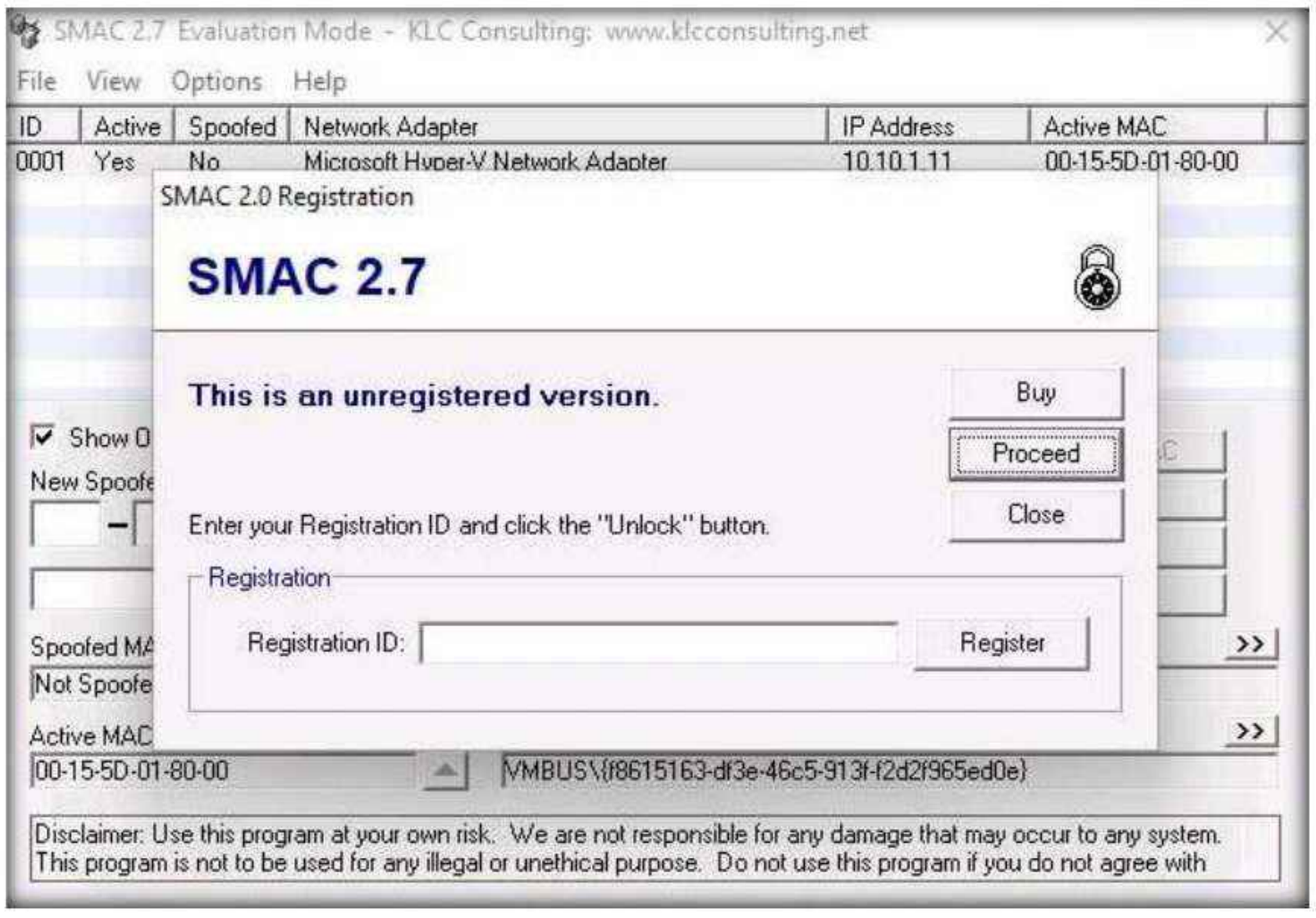
    Note: If a **User Account Control** pop-up appears, click **Yes**.



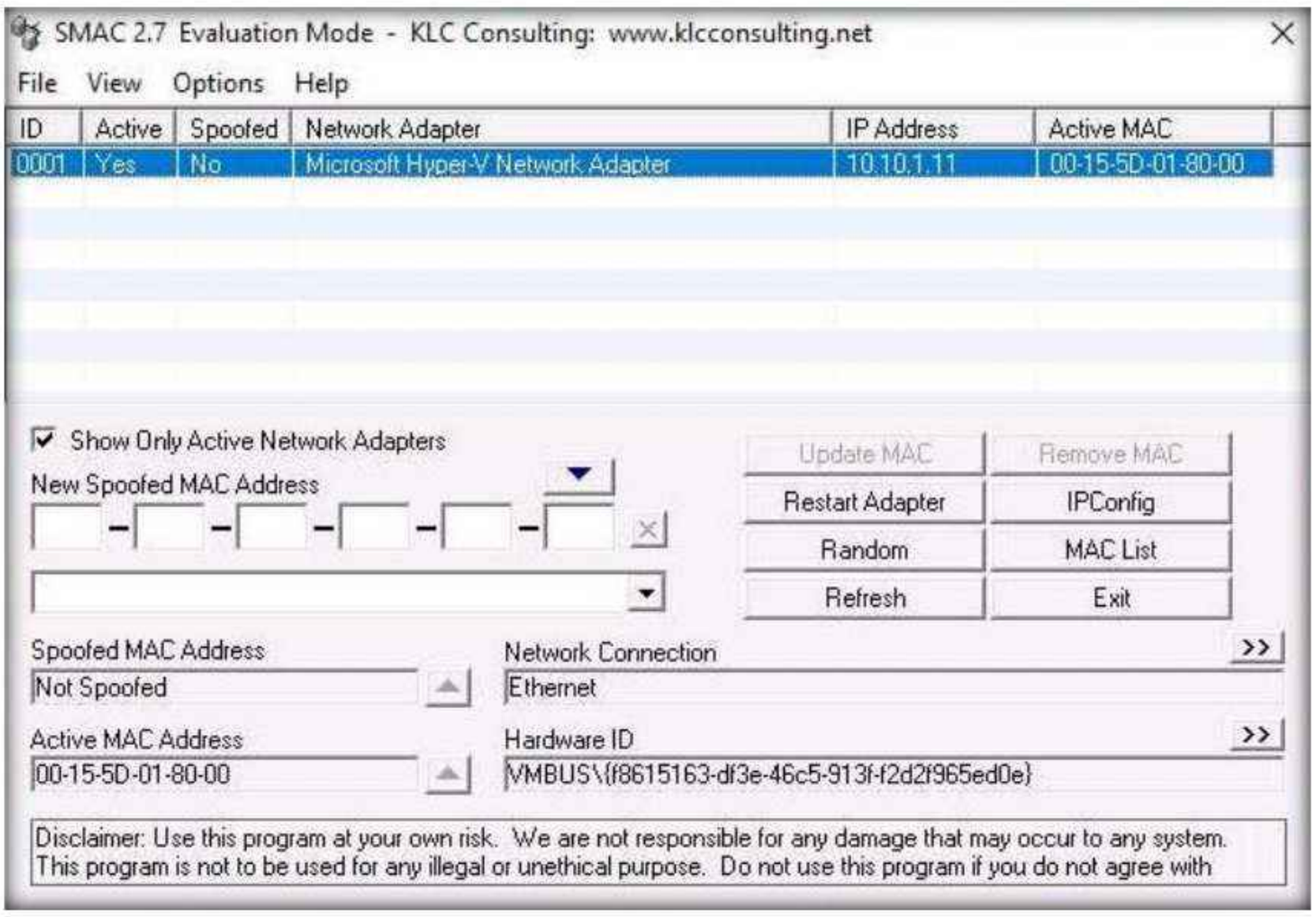
13. The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.



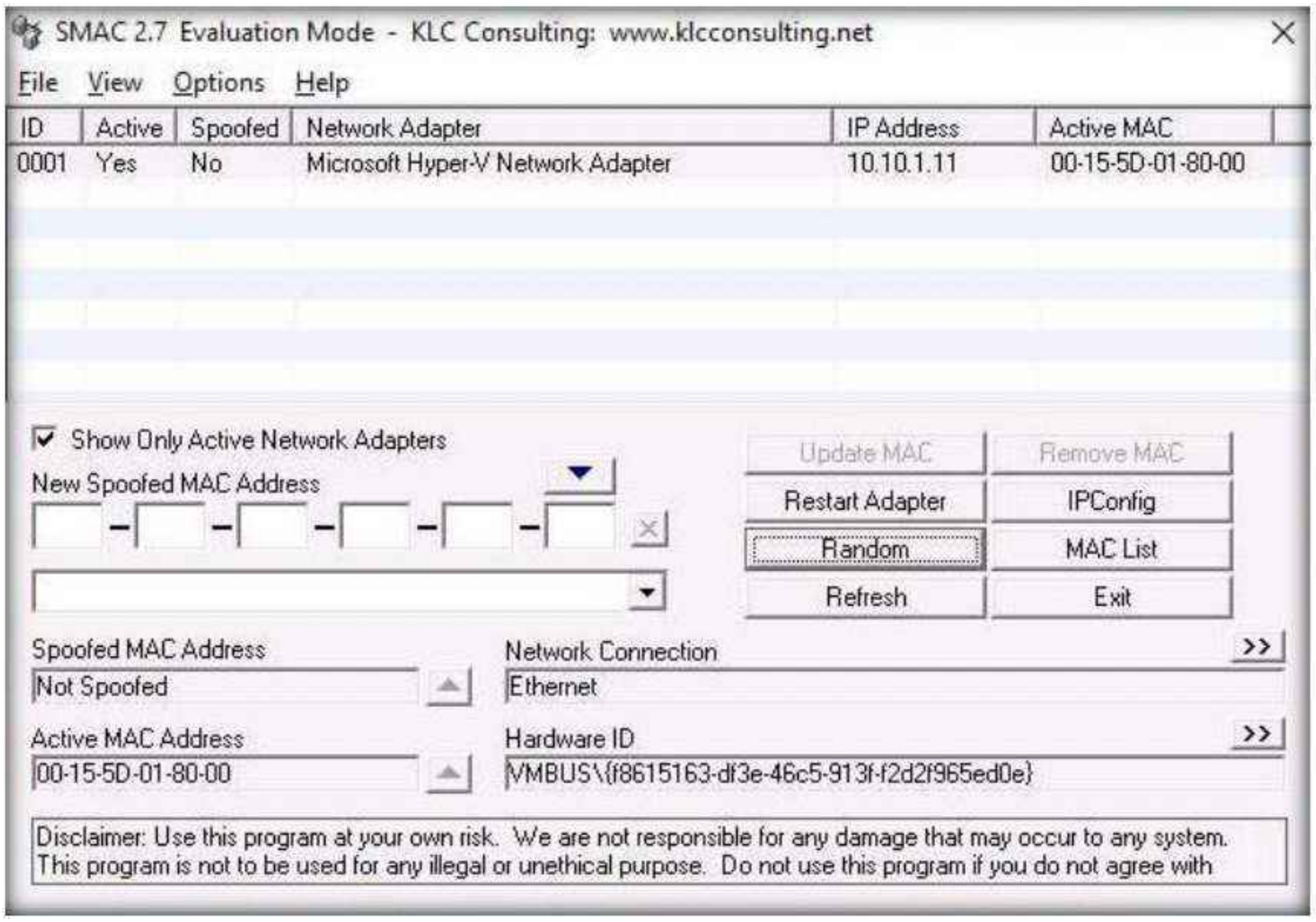
14. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.



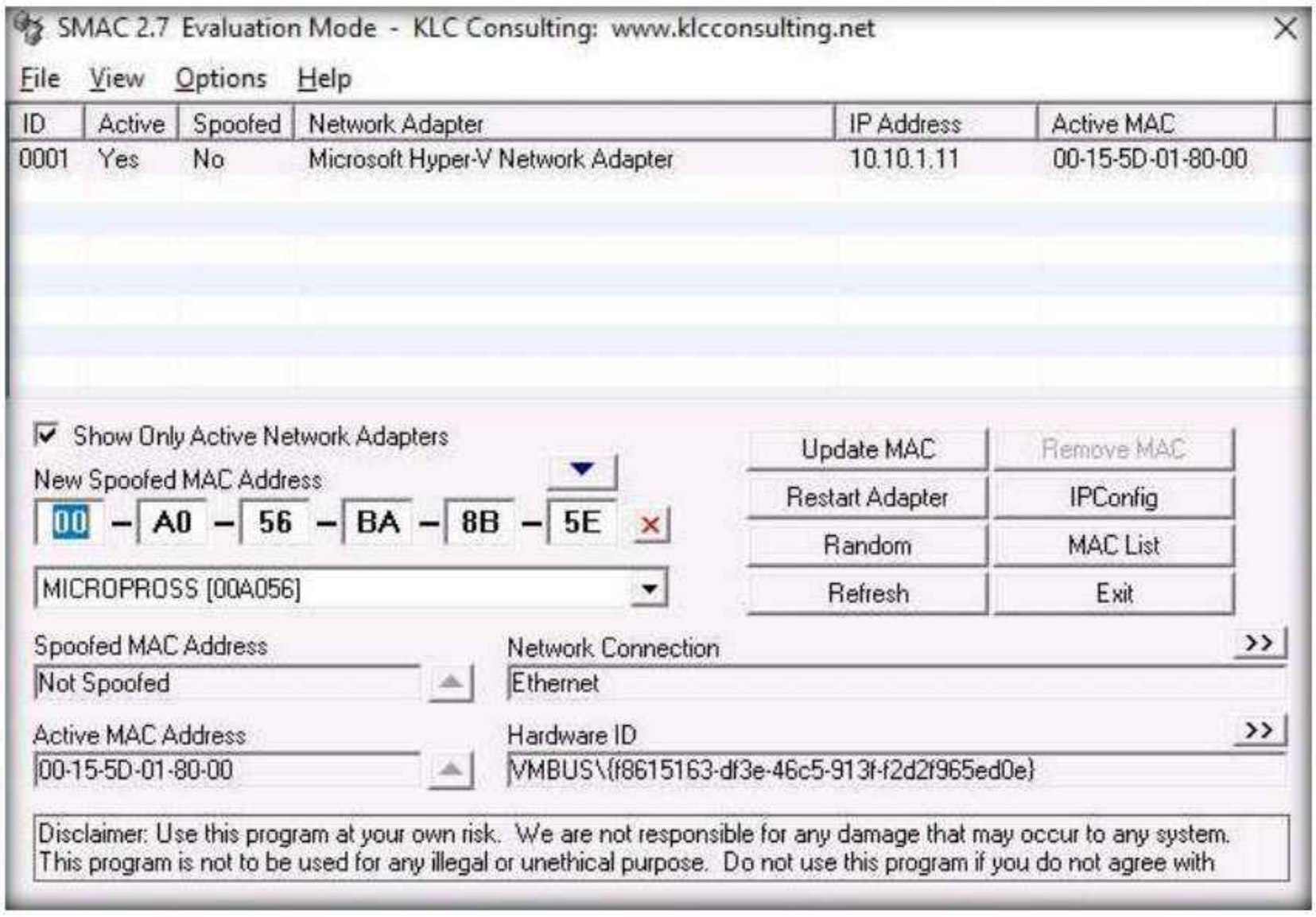
15. The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.



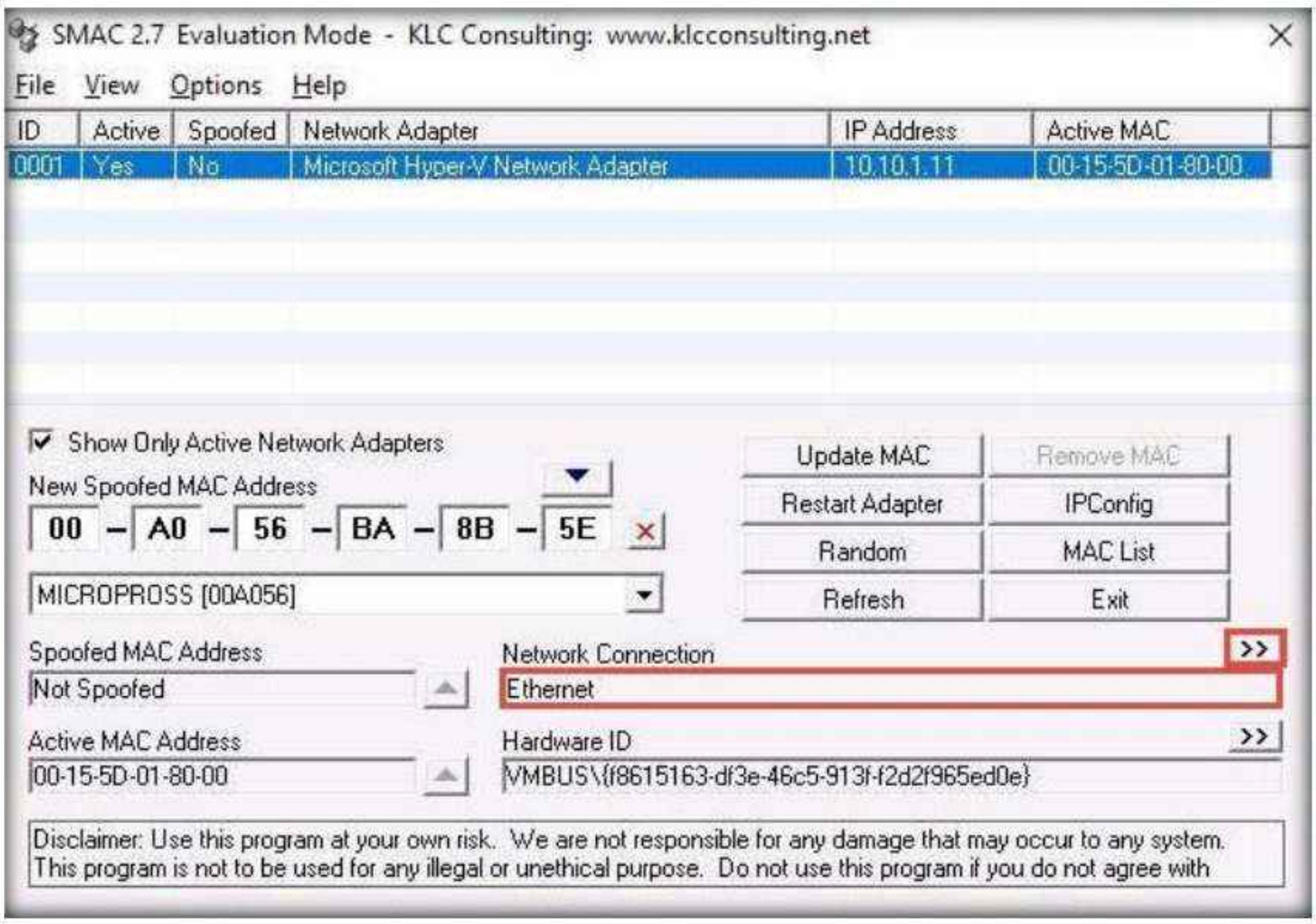
16. Click the **Random** button to generate a random MAC address.



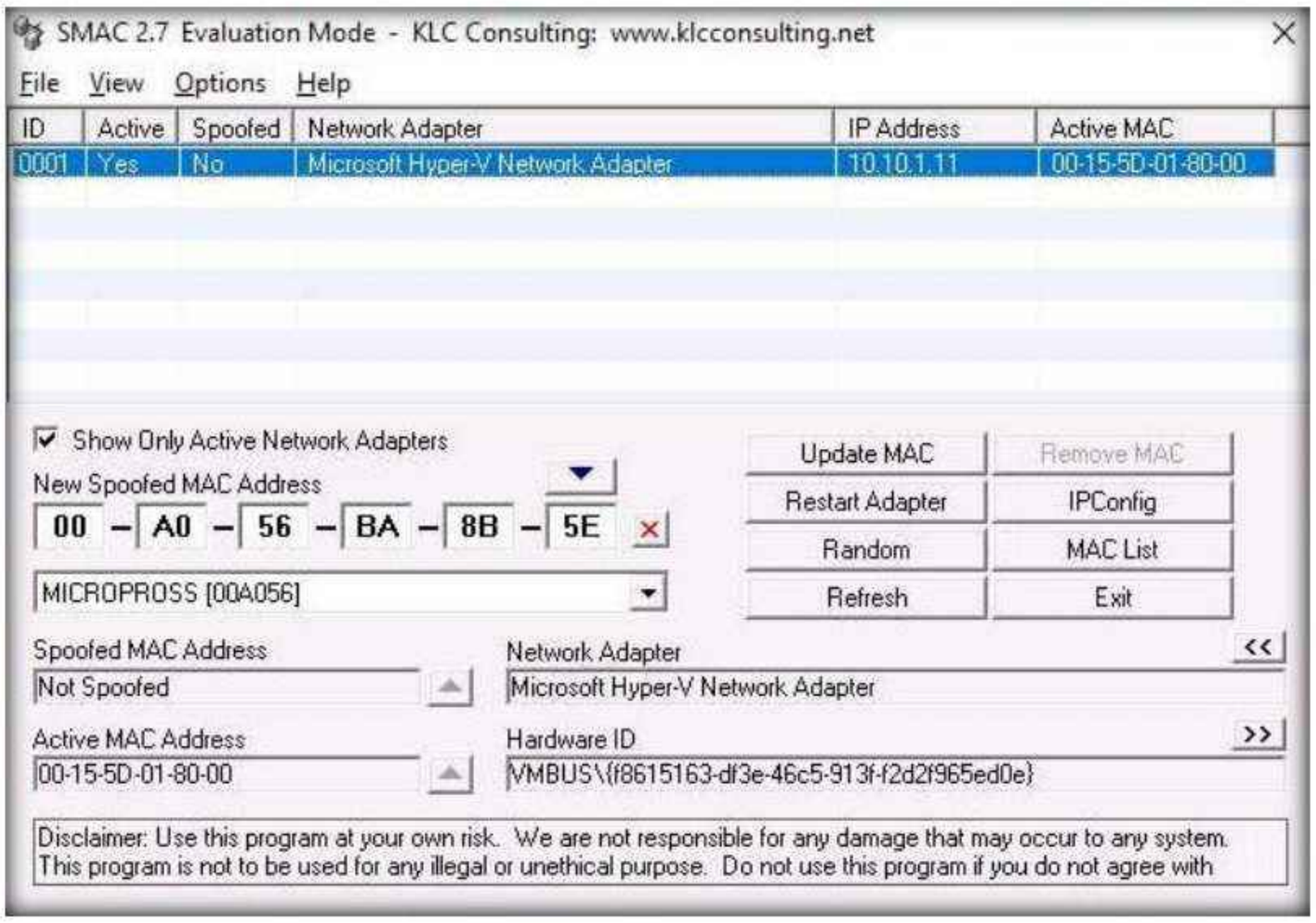
17. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.



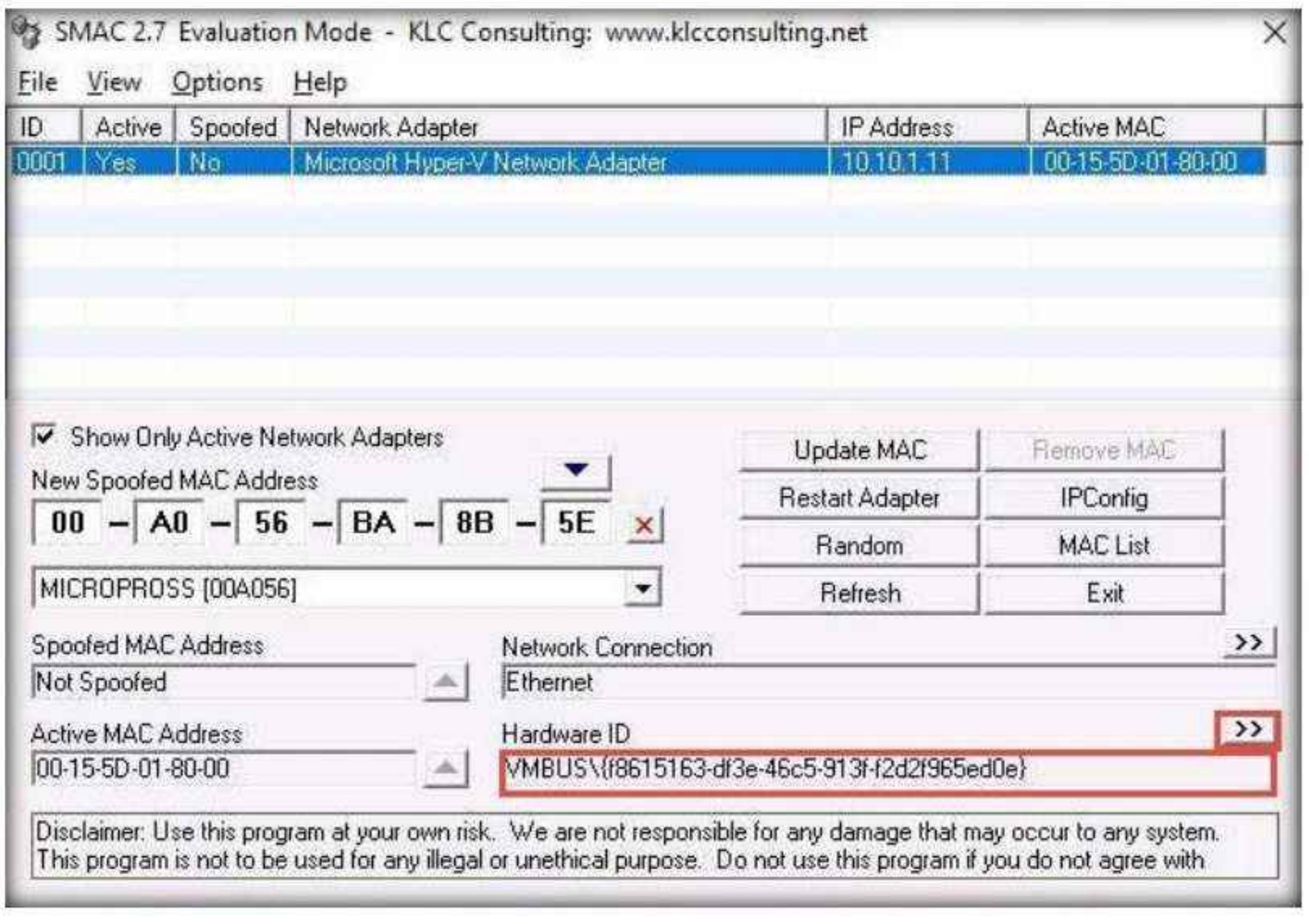
18. Click the forward arrow button (**>>**) under **Network Connection** to view the **Network Adapter** information.



19. Clicking the back arrow (**<<**) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.



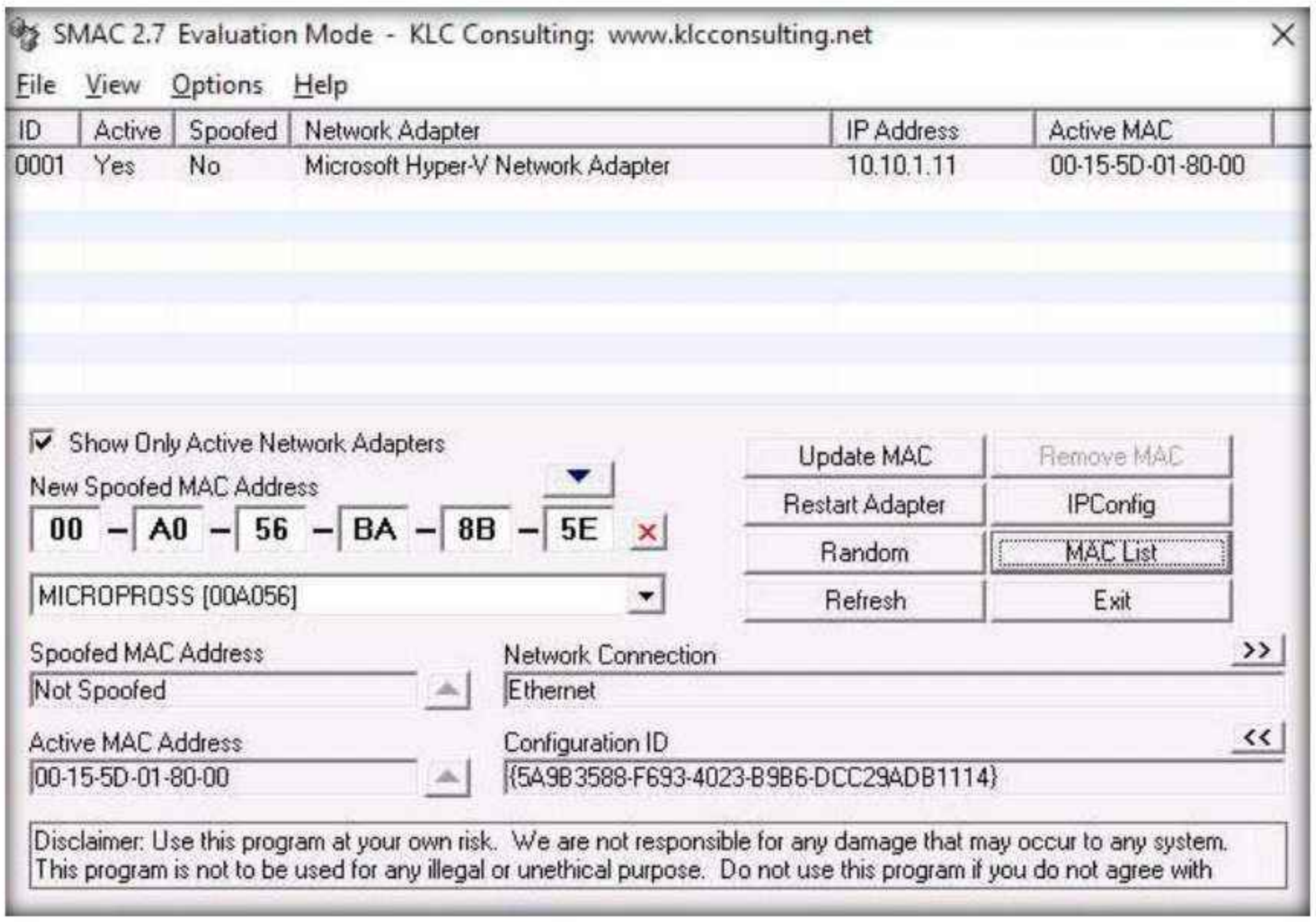
20. Similarly, you can click the forward arrow button (**>>**) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (**<<**) to toggle back to **Hardware ID** information.



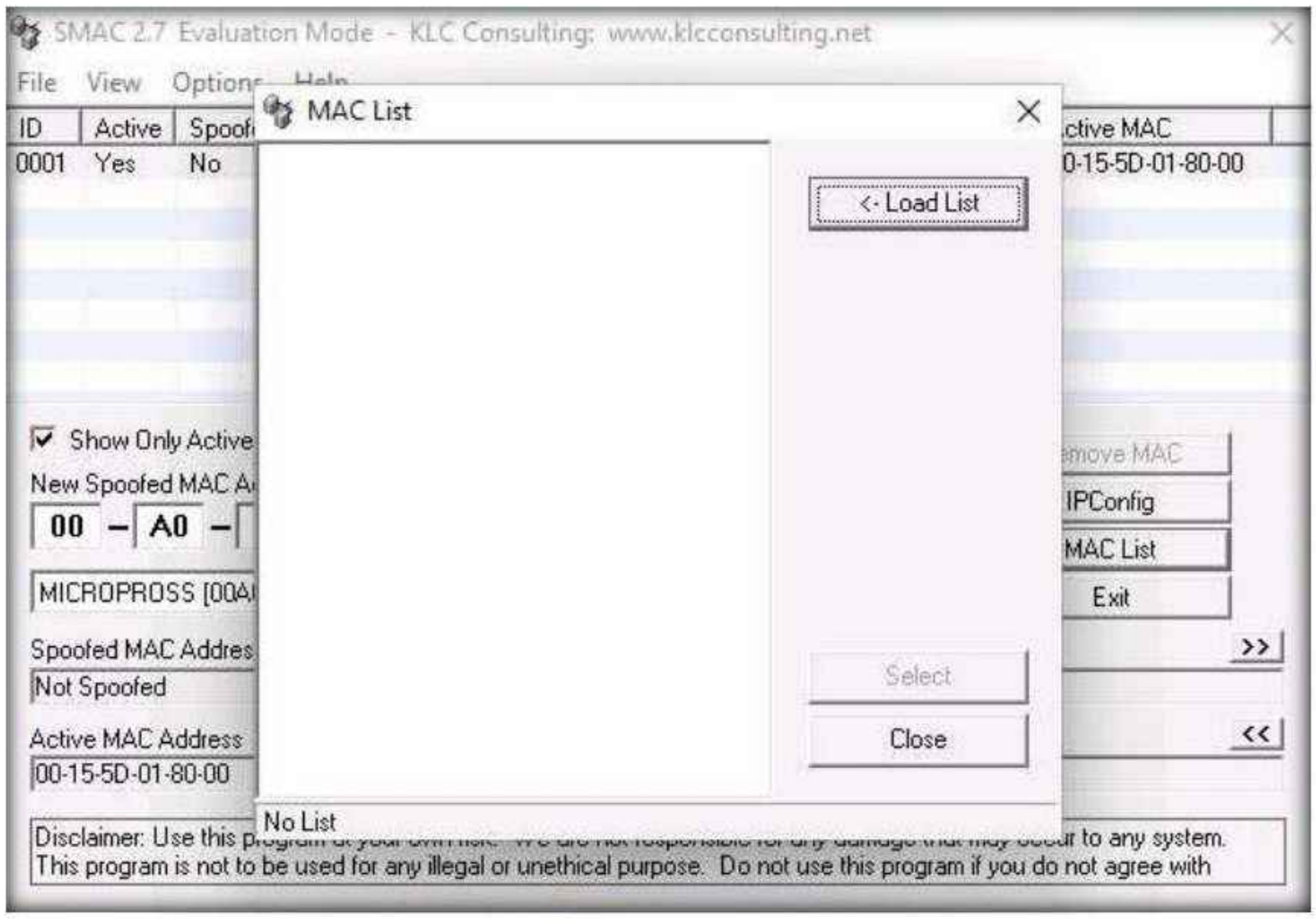
21. Click the **IPConfig** button to view the ipconfig information.

22. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.

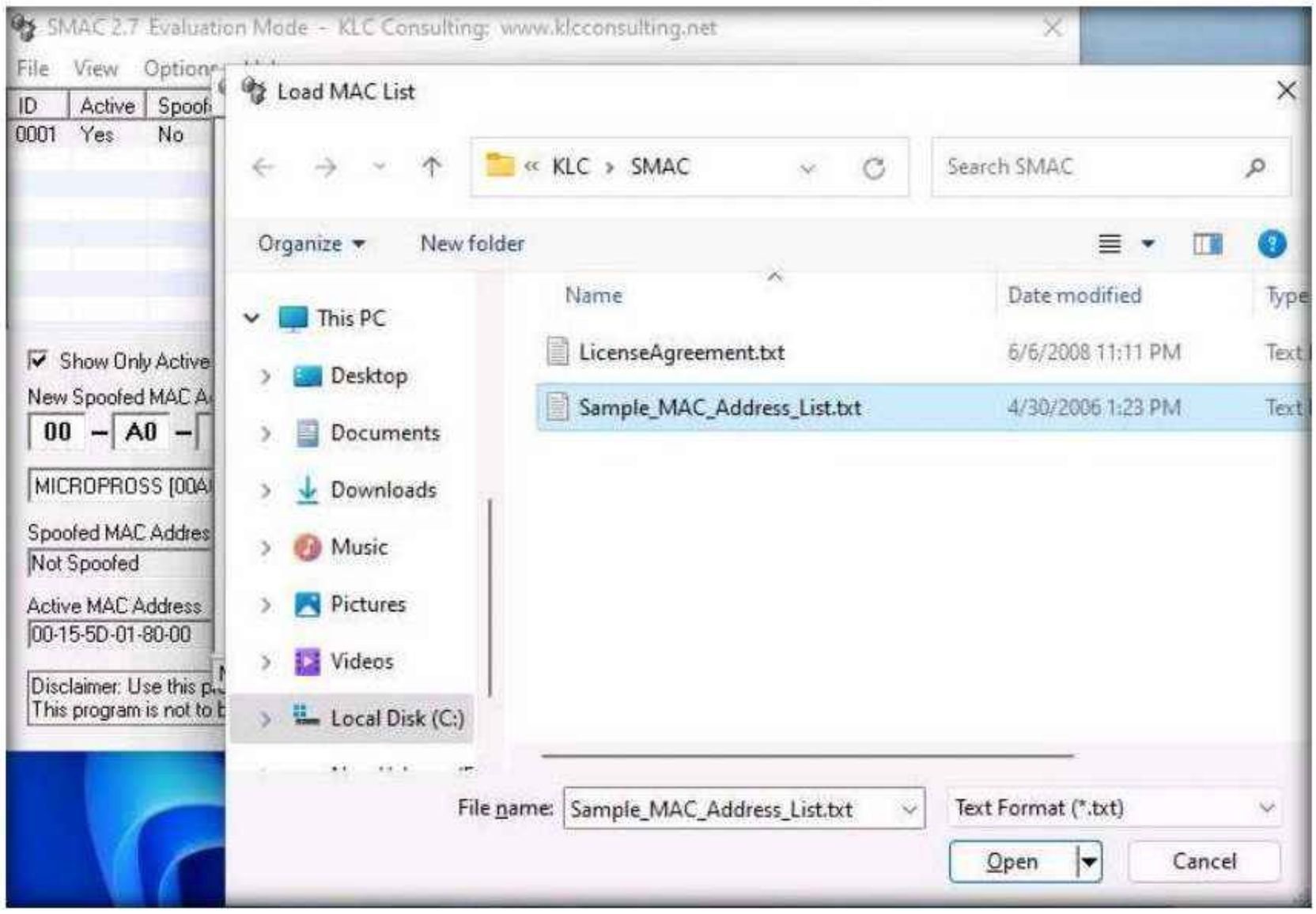
23. Click the **MAC List** button to import the MAC address list into SMAC.



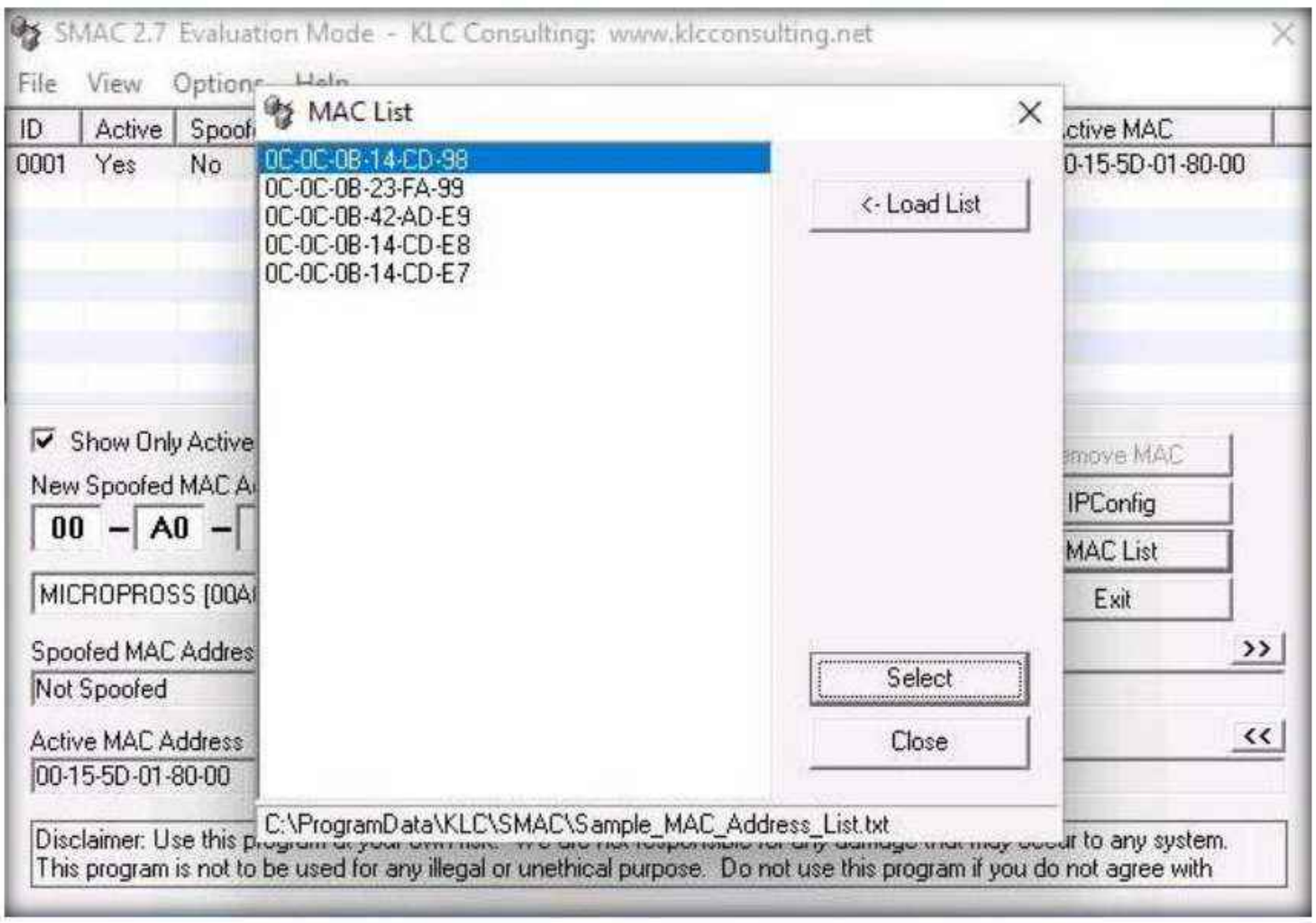
24. The **MAC List** window appears; click the **Load List** button.



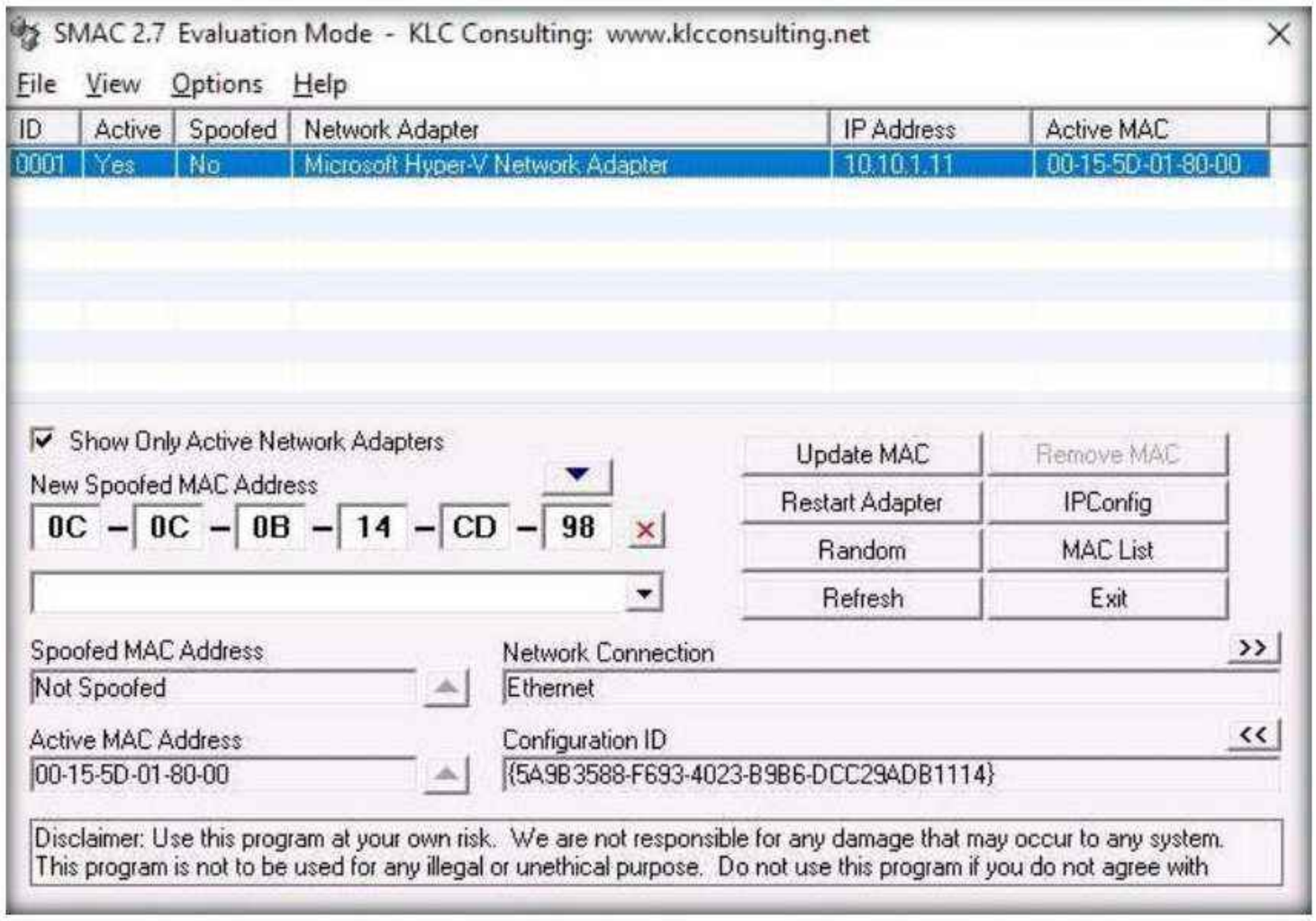
25. The **Load MAC List** window appears; select the **Sample_MAC_Address_List.txt** file and click **Open**.



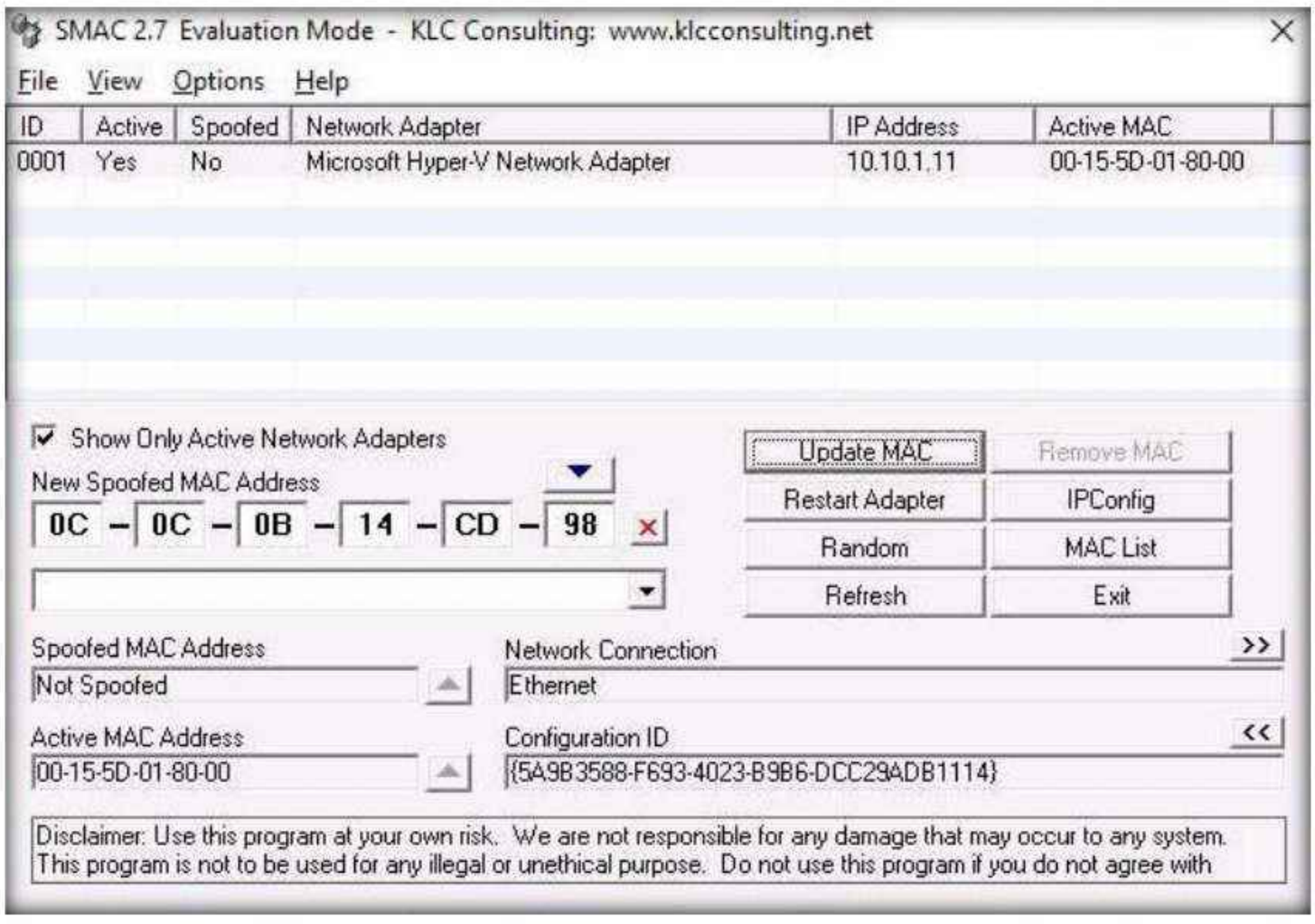
26. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.



27. The selected MAC address appears under the **New Spoofed MAC Address** field.



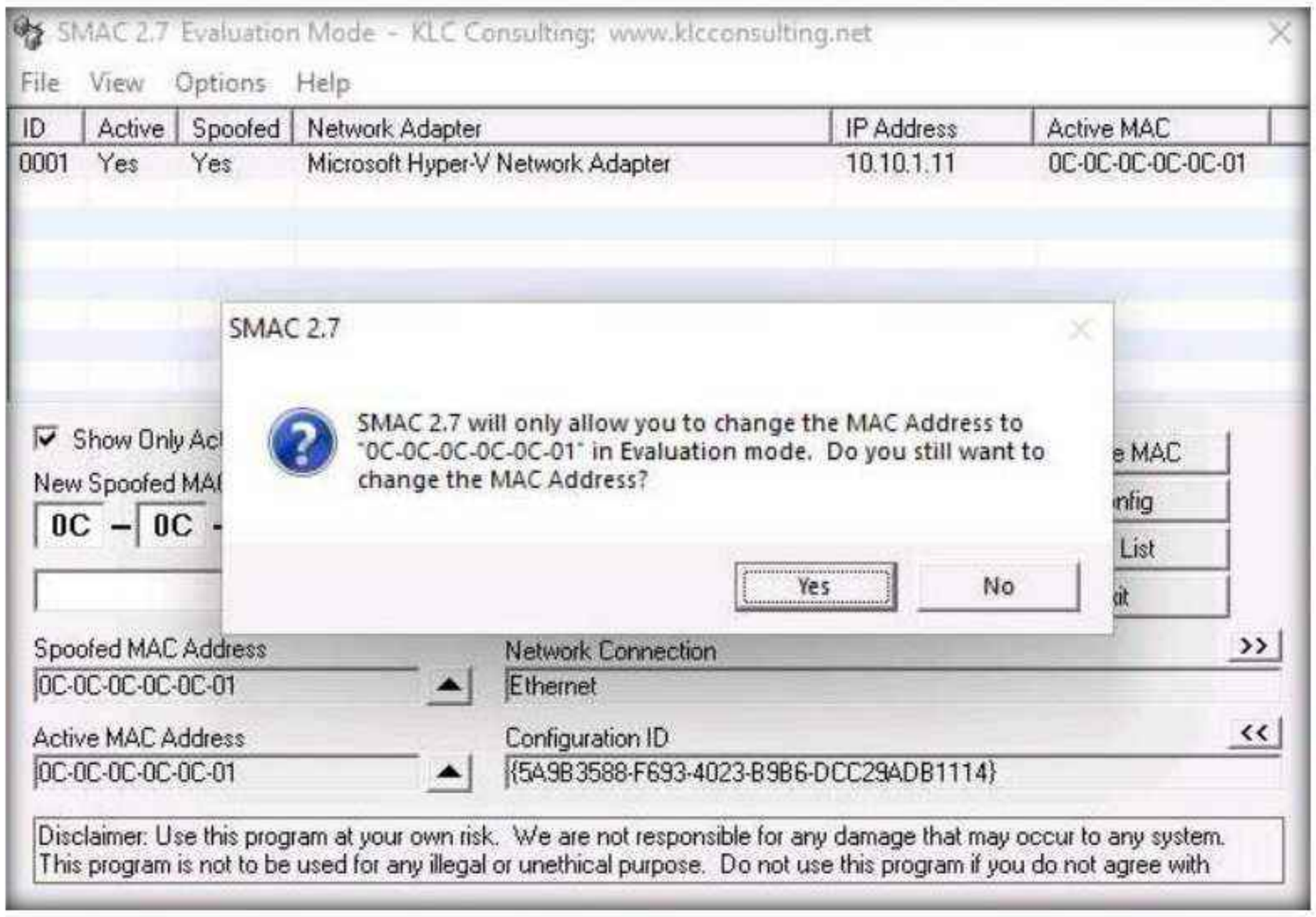
28. Click the **Update MAC** button to update the machine's MAC address information.



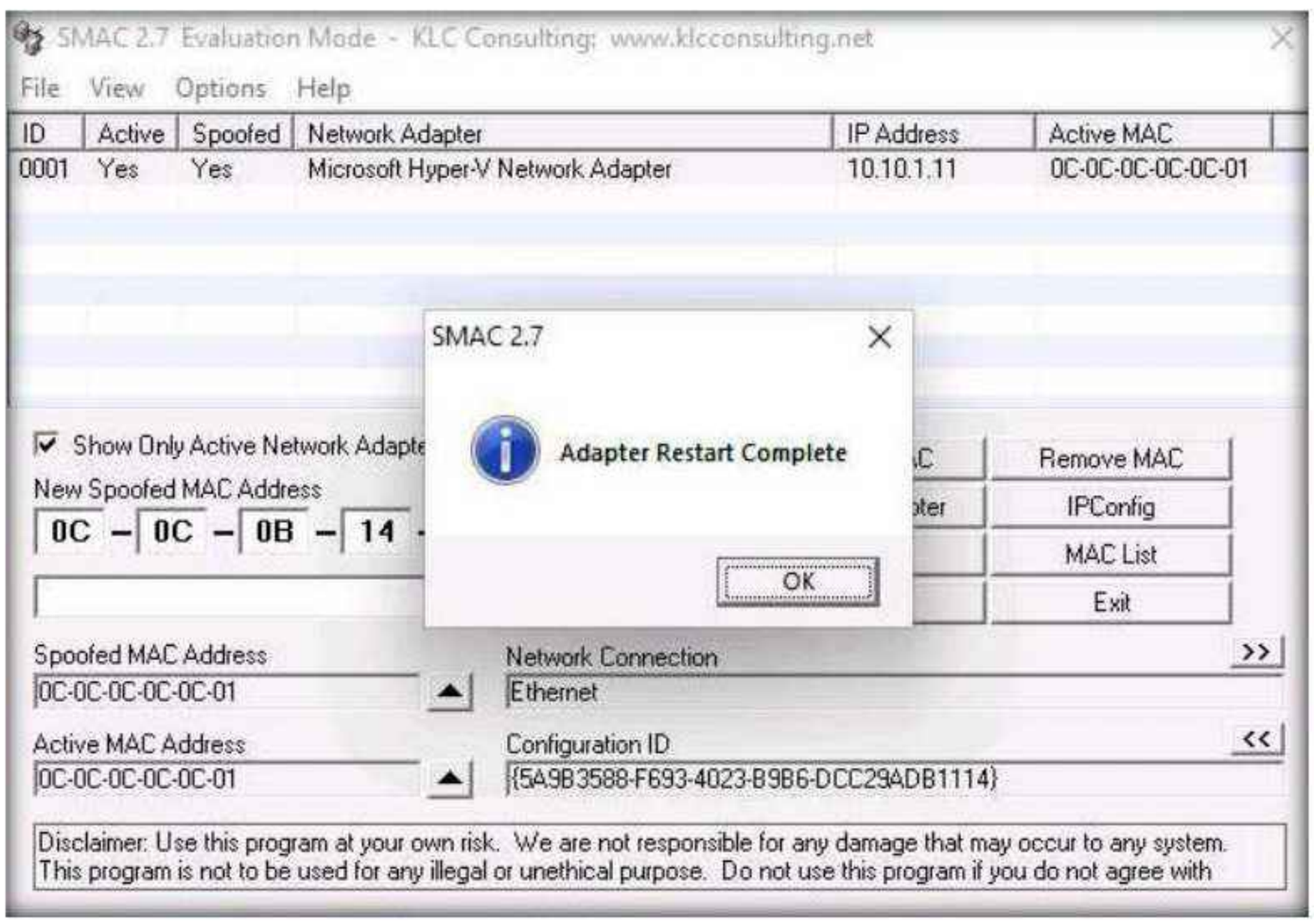
29. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

    Note: This dialog box only appears in the evaluation or trial version.

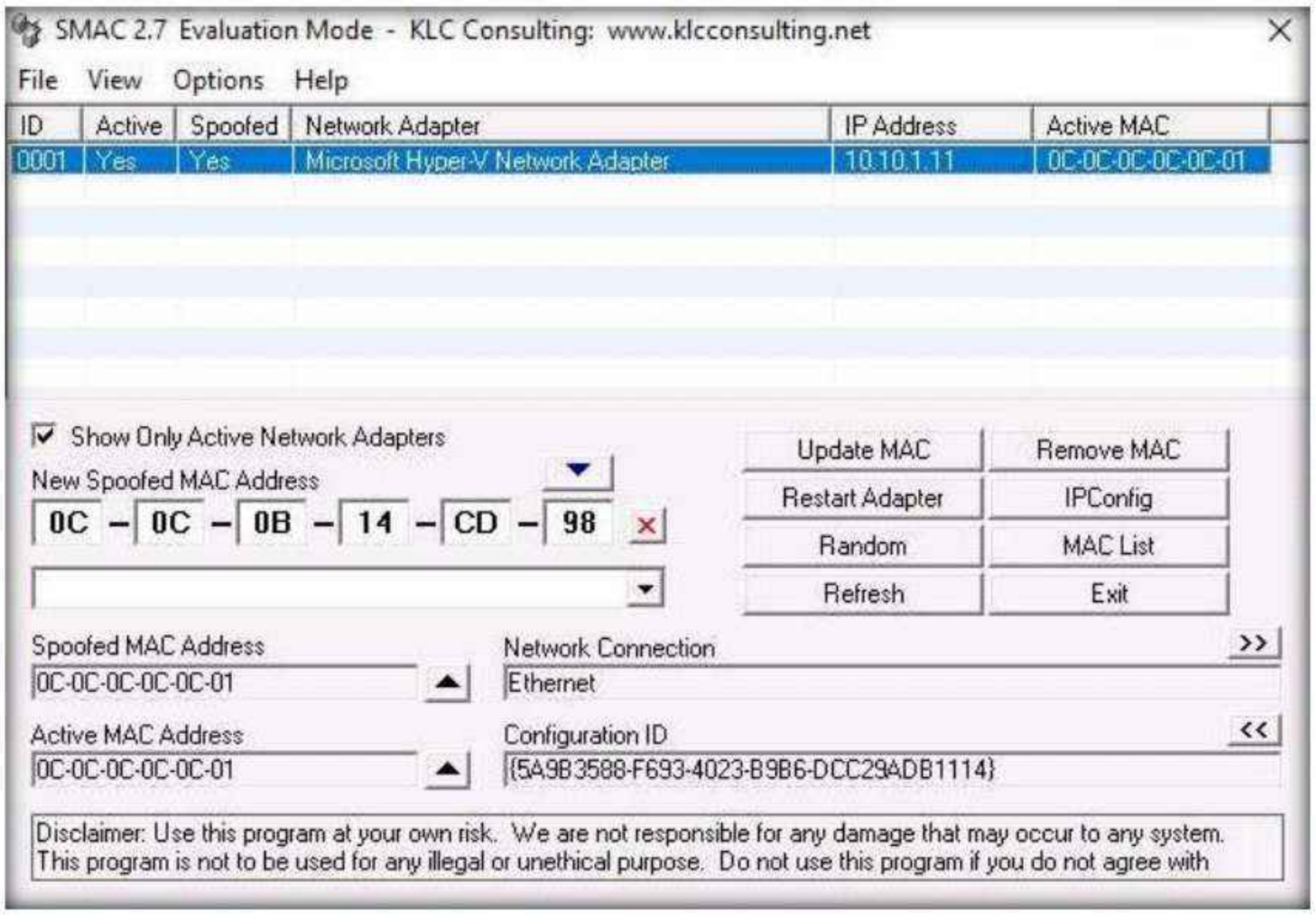
    Note: In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.



30. After successfully spoofing the MAC address, a **SMAC** pop-up appears, stating **"Adapter Restart Complete"**; click **OK**.



31. Once the adapter is restarted, a random MAC address is assigned to your machine. You can see the newly generated MAC address under **Spoofed MAC Address** and **Active MAC Address**.



Note: By spoofing the MAC address, an attacker can simulate attacks such as ARP poisoning and MAC flooding without revealing their own actual MAC address.

32. To restore the MAC address back to its original setting, click the **Remove MAC** button.
33. This concludes the demonstration of spoofing MAC addresses using TMAC and SMAC.
34. Close all open windows and document all the acquired information.
35. Turn off the **Windows 11** virtual machine.

Task 6: Spoof a MAC Address of Linux Machine using macchanger

A MAC address is a unique number that can be assigned to every network interface, and it is used by various systems programs and protocols to identify a network interface. It is not possible to change MAC address that is hard coded on the NIC (Network interface controller). However, many drivers allow the MAC address to be changed. Some tools can make the operating system believe that the NIC has the MAC address of user's choice. Masking of the MAC address is known as MAC spoofing and involves changing the computer's identity. MAC spoofing can be performed using numerous tools.

Here, we will be using macchanger utility to change the MAC address of a Linux system

1. Turn on the **Parrot Security** virtual machine.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

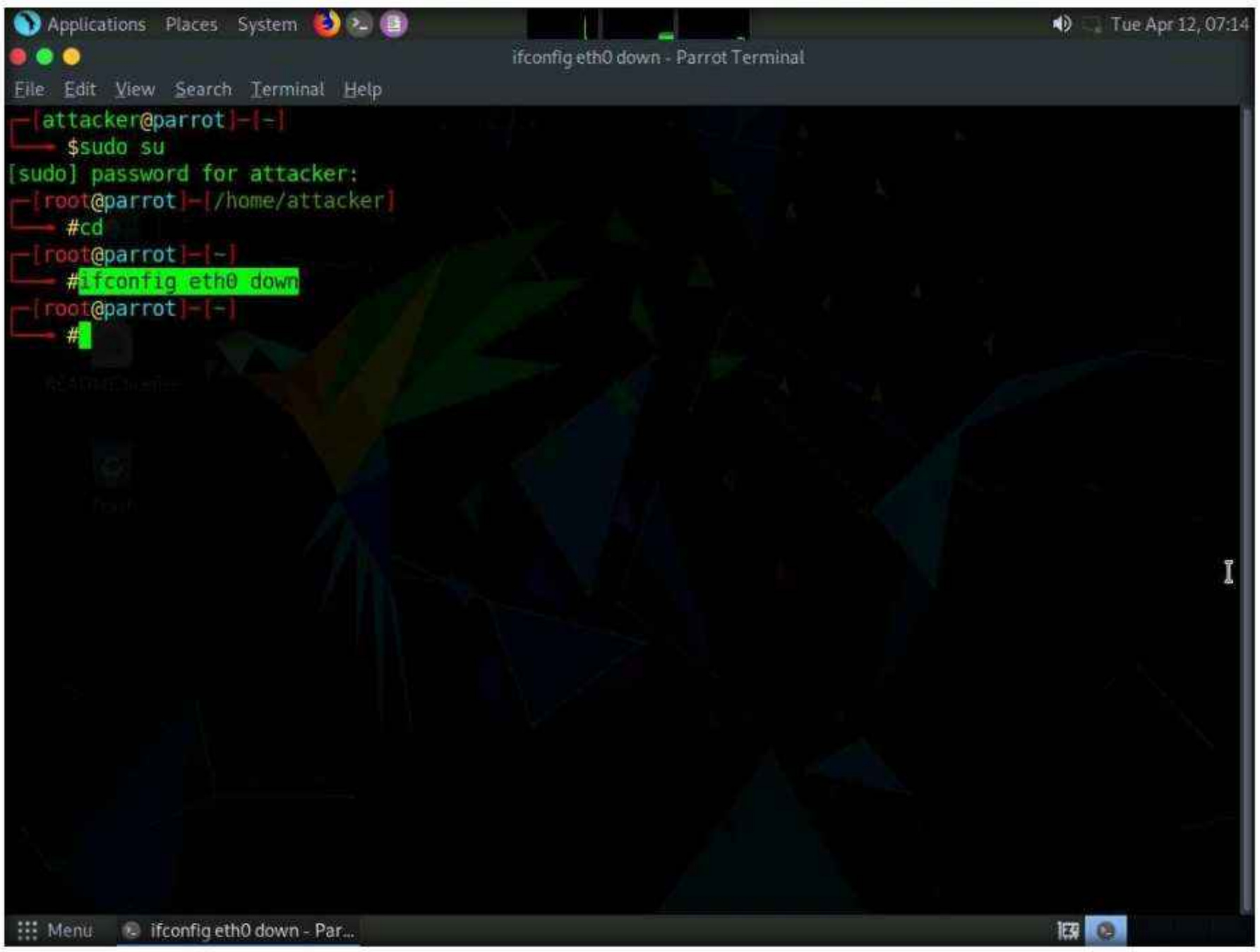
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

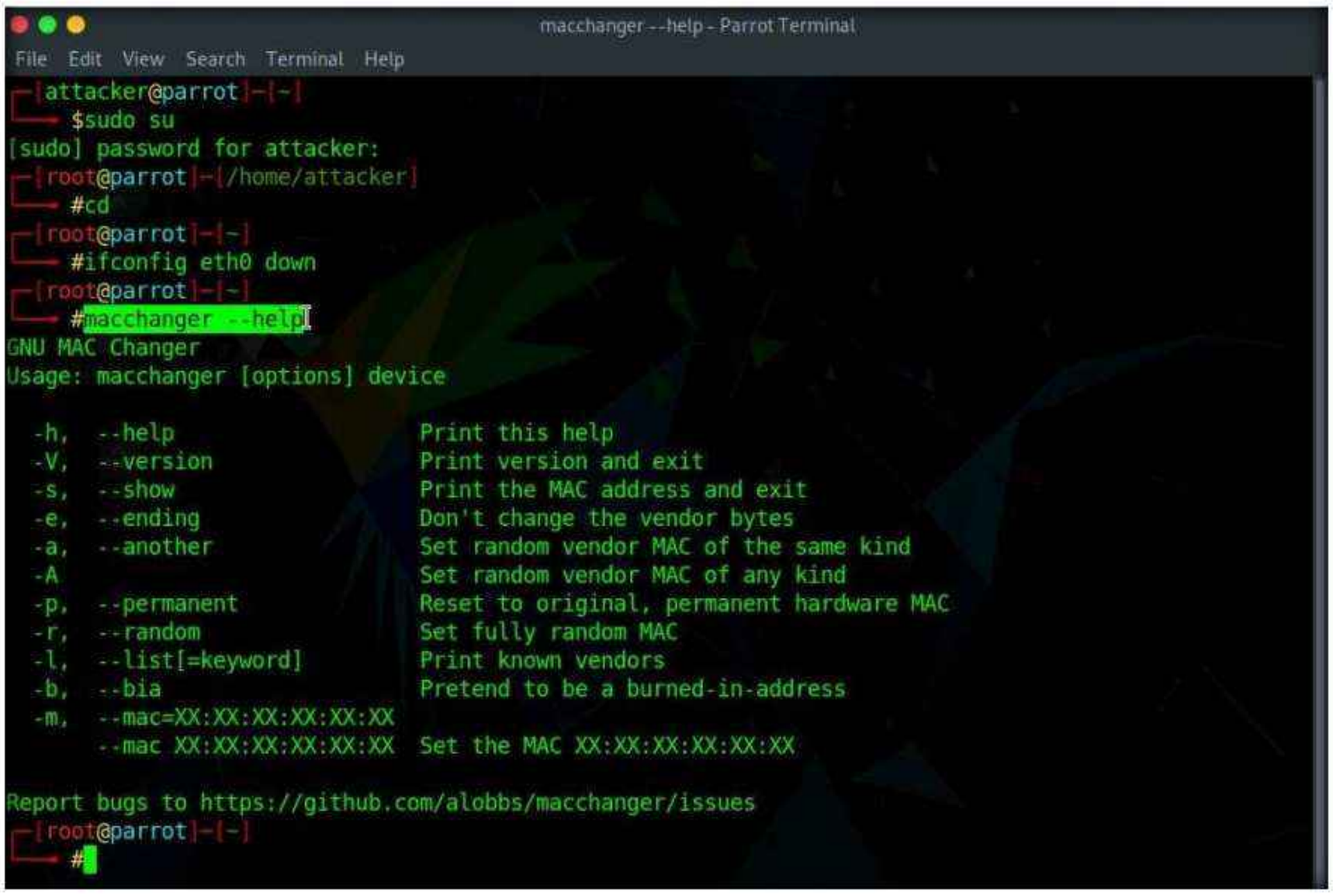
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the [sudo] password for attacker field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Before changing the MAC address, we need to turn off the network interface.
8. Type **ifconfig eth0 down** and press **Enter**, to turn off the network interface.

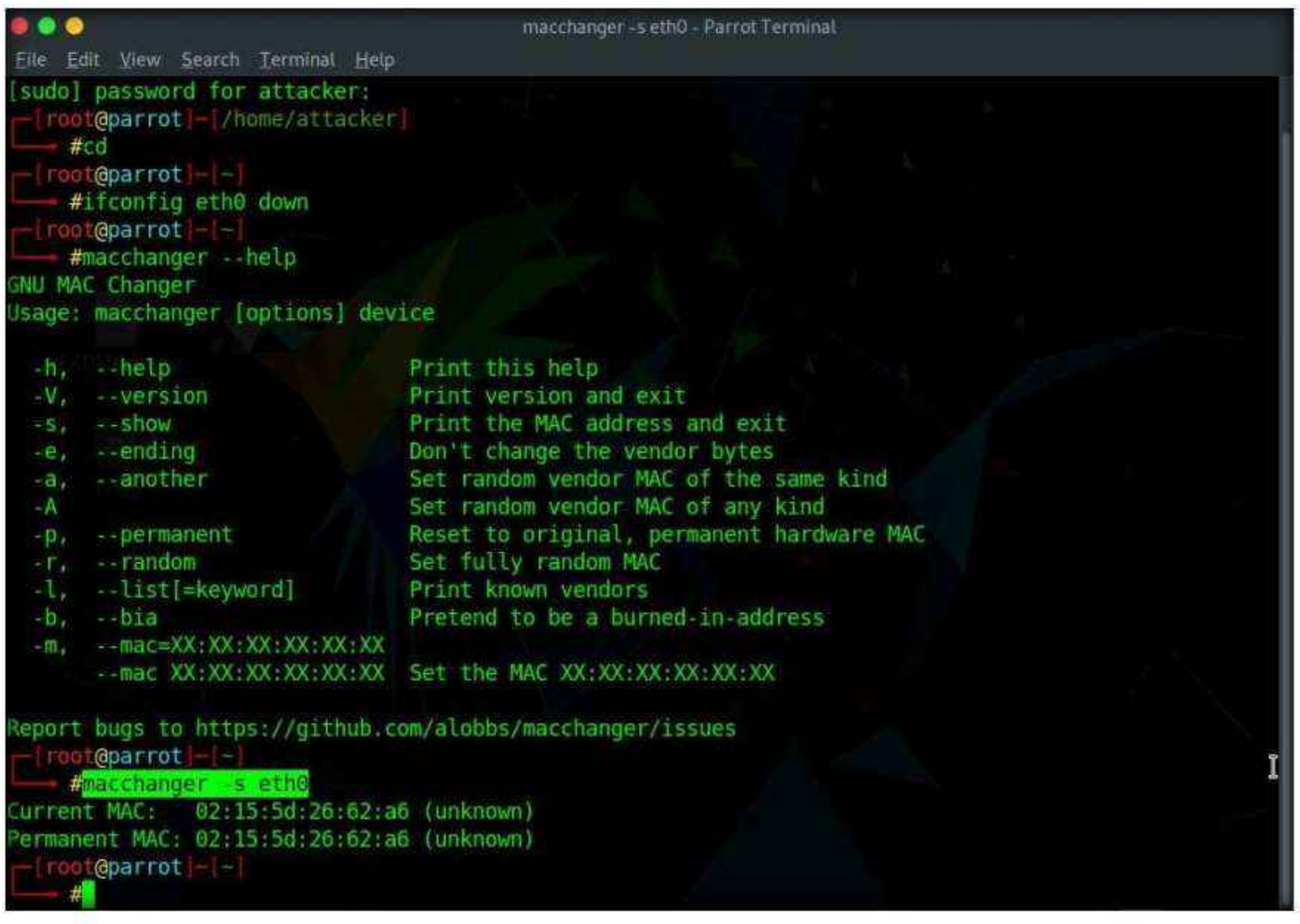


9. Type **macchanger --help** command to see the available options of macchanger tool.



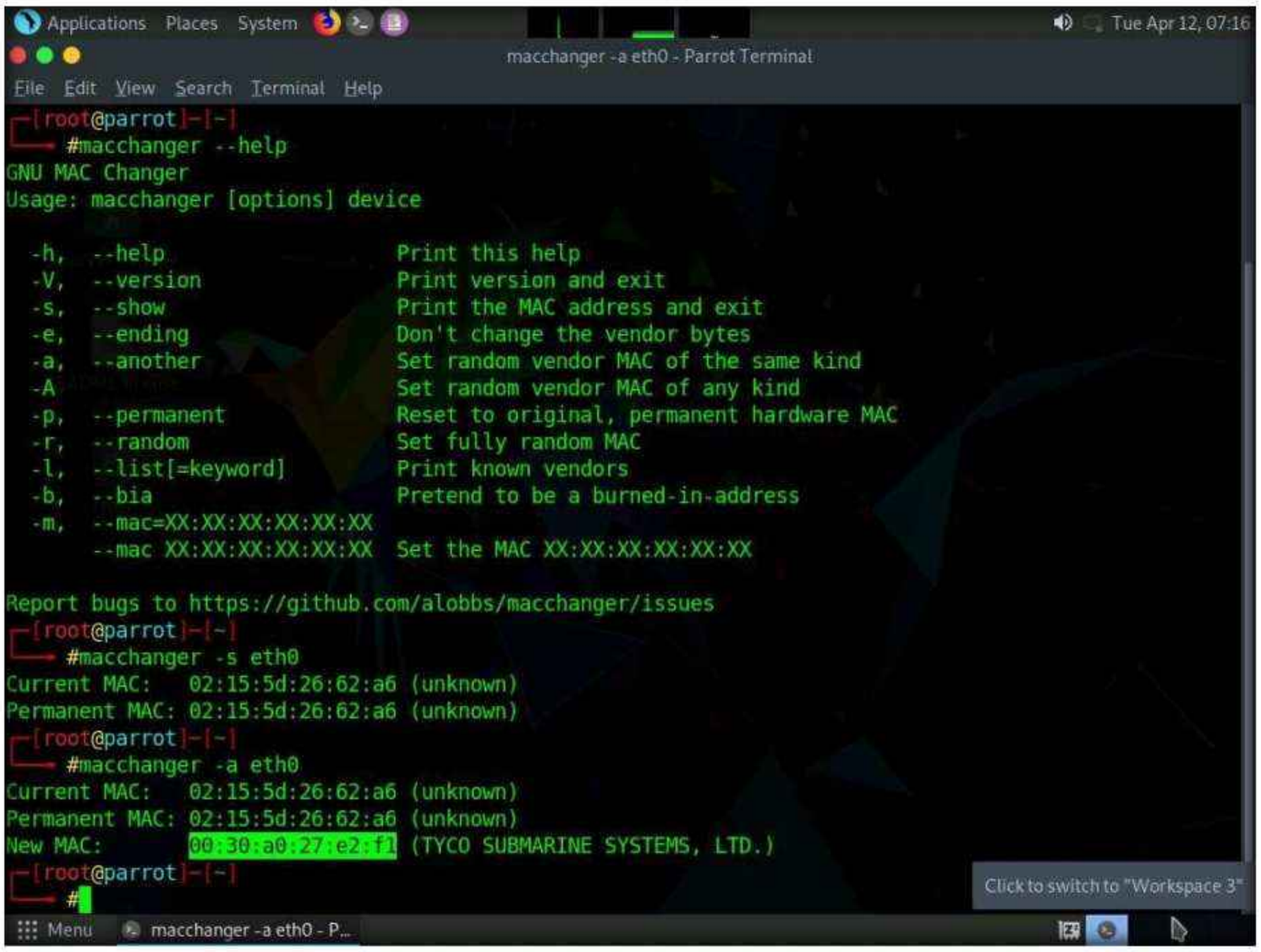
10. To see the current MAC address of the **Parrot Security** machine, type **macchanger -s eth0** and press **Enter**.

    Note: **-s**: prints the MAC address of the machine.

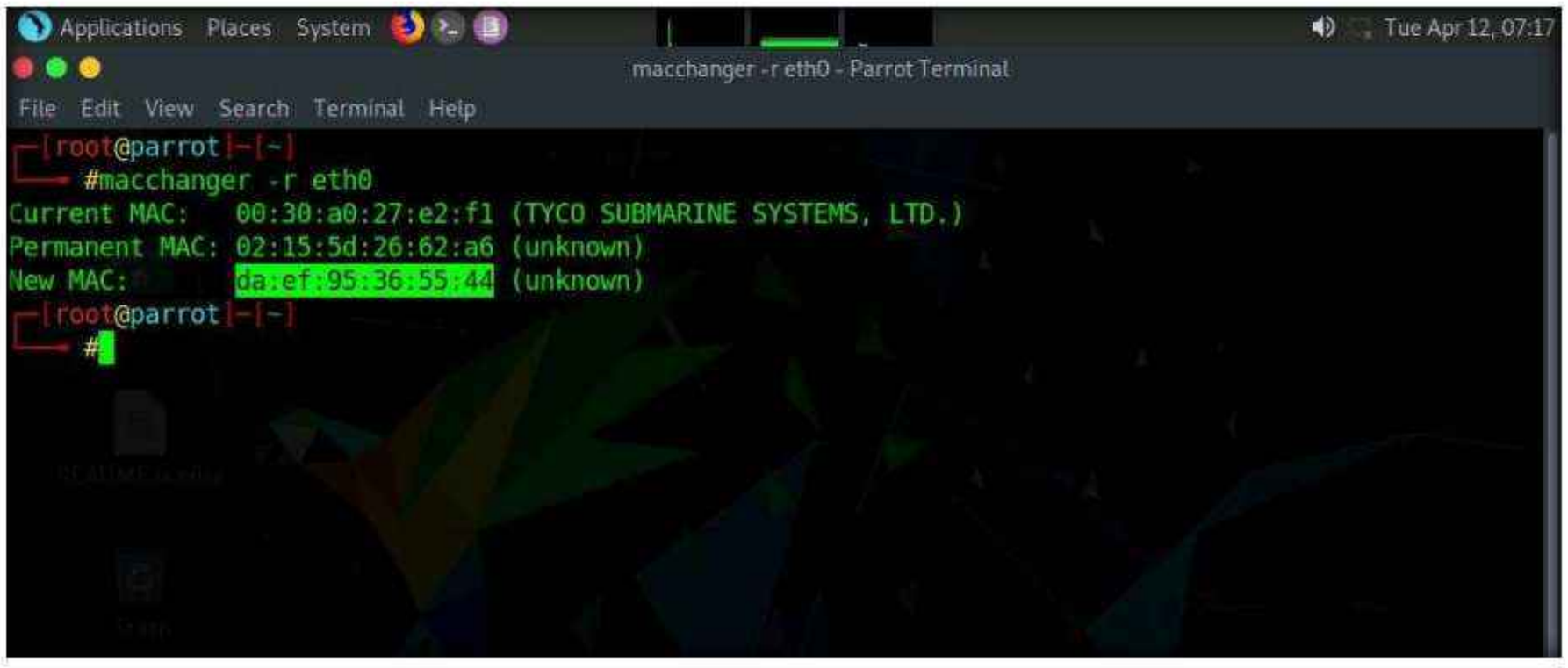


11. Now we will change the MAC address of the network interface.
12. In the terminal type, **macchanger -a eth0** and press **Enter**, to set a random vendor MAC address to the network interface.

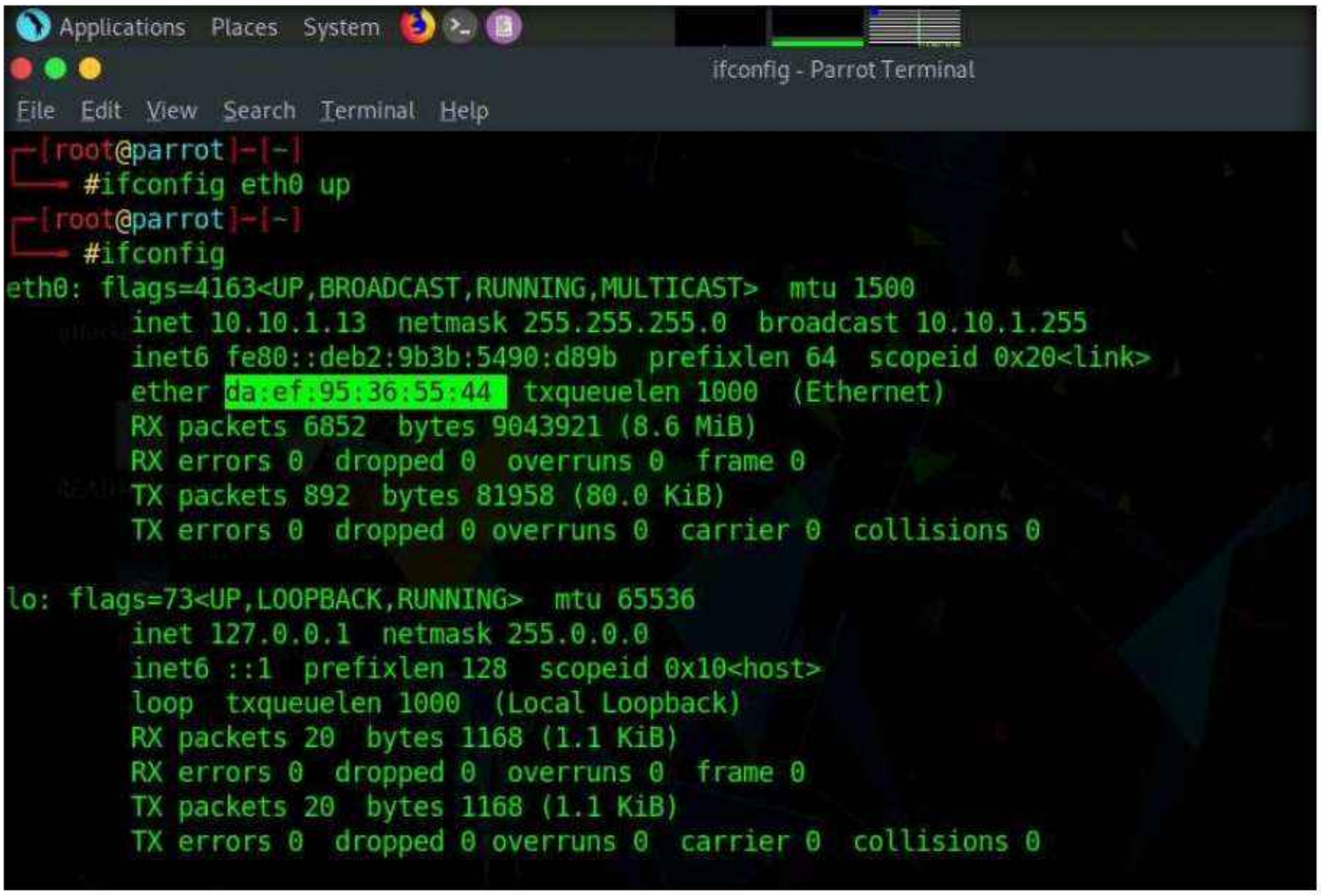
    Note: **-a**: sets random vendor MAC address to the network interface.



13. Now, type **macchanger -r eth0** and press **Enter**, to set a random MAC address to the network interface.



14. To enable the network interface type **ifconfig eth0 up** and press **Enter**.
15. To check the changed MAC address, type **ifconfig** and press **Enter**.



16. You can observe that a random MAC address is set to the network interface.
17. This concludes the demonstration of how to spoof a MAC address of Linux machine using macchanger
18. Close all open windows and document all the acquired information.
19. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Lab 2

Perform Network Sniffing using Various Sniffing Tools

Ethical hackers and pen testers are aided in network sniffing by various tools that make it an easy task.

Lab Scenario

Data traversing an HTTP channel flow in plain-text format and is therefore prone to MITM attacks. Network administrators can use sniffers for helpful purposes such as to troubleshoot network problems, examine security problems, and debug protocol implementations. However, an attacker can use sniffing tools such as Wireshark to sniff the traffic flowing between the client and the server. The traffic obtained by the attacker might contain sensitive information such as login credentials, which can then be used to perform malicious activities such as user-session impersonation.

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can only capture data packets from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises leave their switch ports open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

The information gathered in the previous step may be insufficient to reveal the potential vulnerabilities of the target. There may be more information to help find loopholes in the target. An ethical hacker needs to perform network security assessments and suggest proper troubleshooting techniques to mitigate attacks. This lab provides hands-on experience of how to use sniffing tools to sniff network traffic and capture it on a remote interface.

Lab Objectives

- Perform password sniffing using Wireshark
- Analyze a network using the Omnipeek Network Protocol Analyzer
- Analyze a network using the SteelCentral Packet Analyzer

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Network Sniffing Tools

System administrators use automated tools to monitor their networks, but attackers misuse these tools to sniff network data. Network sniffing tools can be used to perform a detailed network analysis. When protecting a network, it is important to have as many details about the packet traffic as possible. By actively scanning the network, a threat hunter can stay vigilant and respond quickly to attacks.

Lab Tasks

Task 1: Perform Password Sniffing using Wireshark

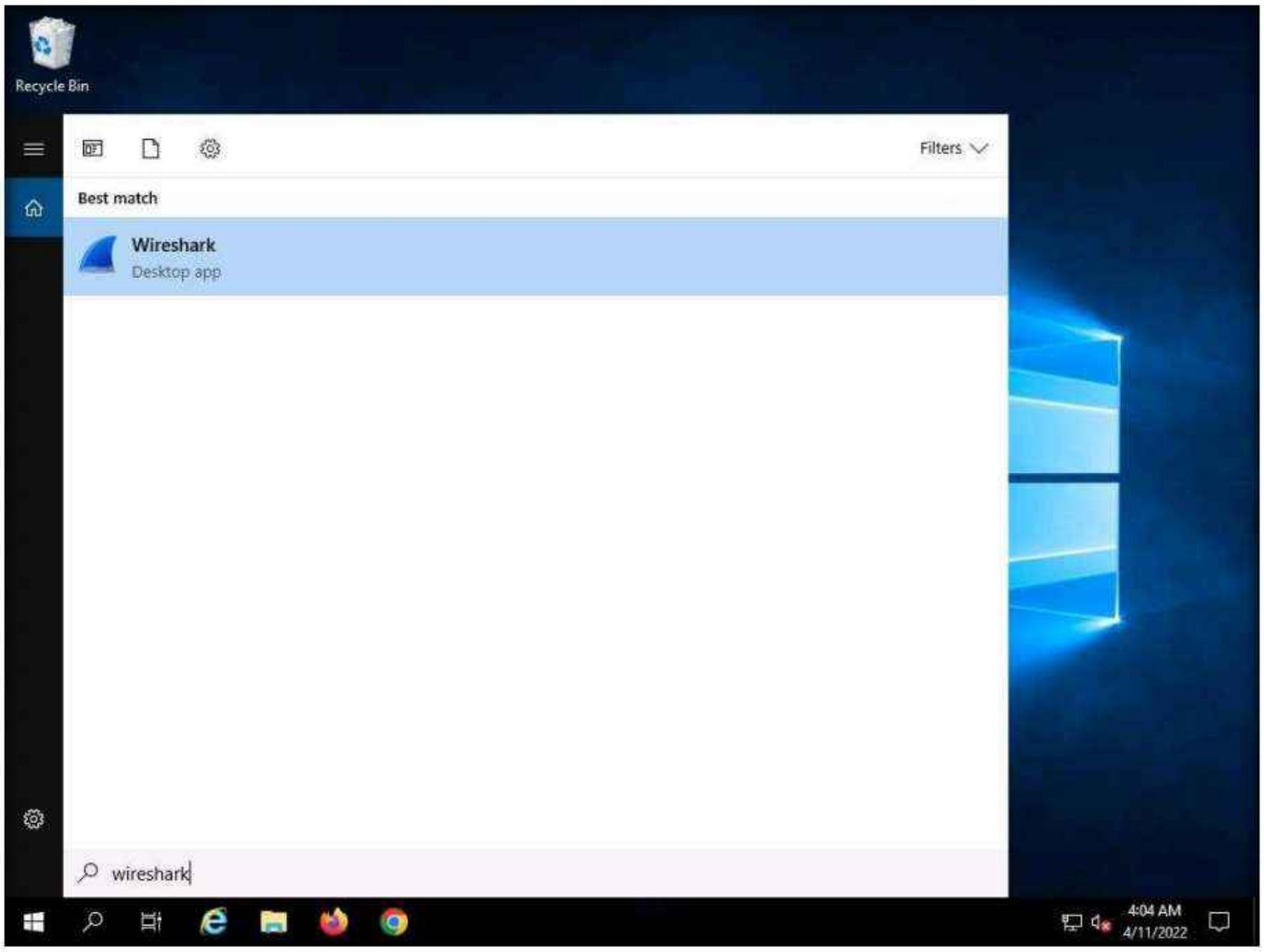
Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. The captured files can be programmatically edited via the command-line. A set of filters for customized data displays can be refined using a display filter.

Here, we will use the Wireshark tool to perform password sniffing.

Note: In this task, we will use the **Windows Server 2019** (**10.10.1.19**) machine as the host machine and the **Windows 11** (**10.10.1.11**) machine as the target machine.

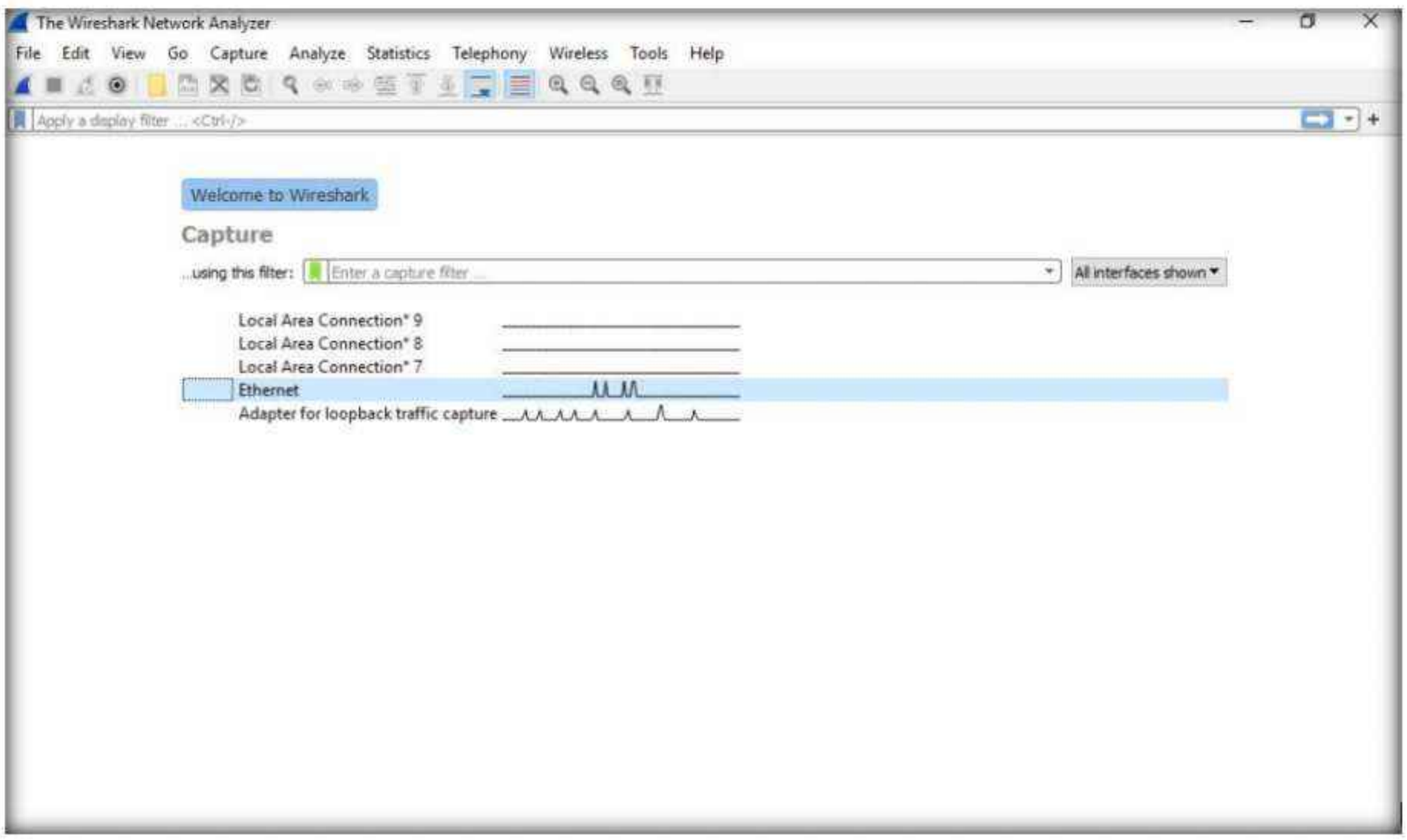
1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.

   Note: If the **Software update** window appears, click **Remind me later**.

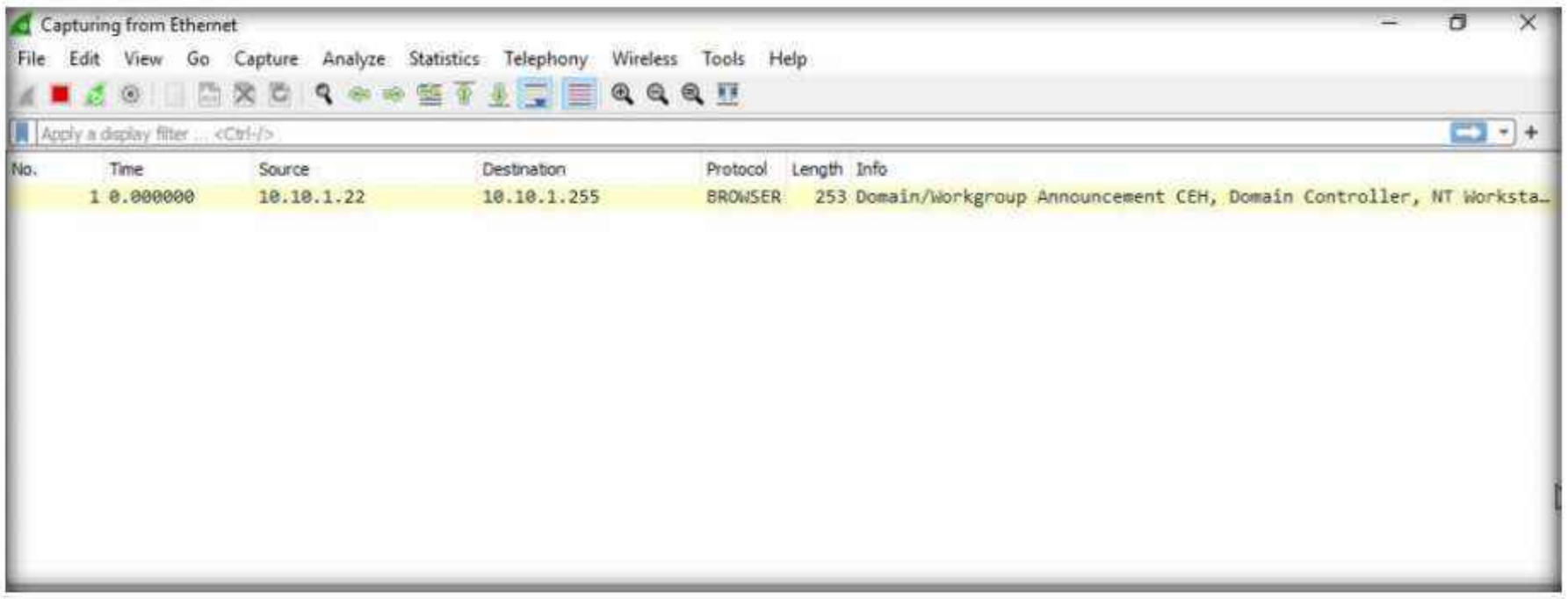


4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

   Note: If a **Software Update** pop-up appears click on **Remind me later**.



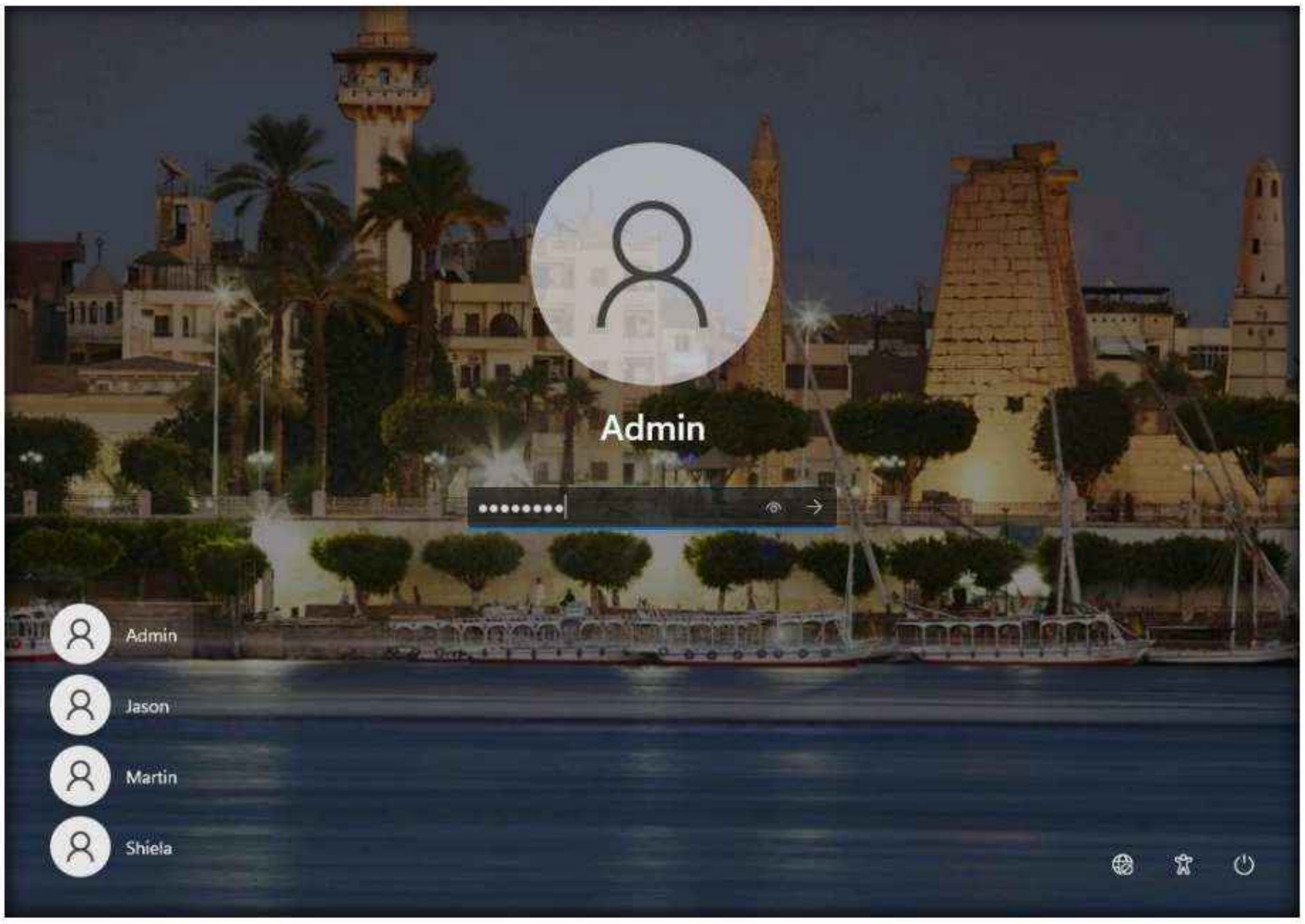
5. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.



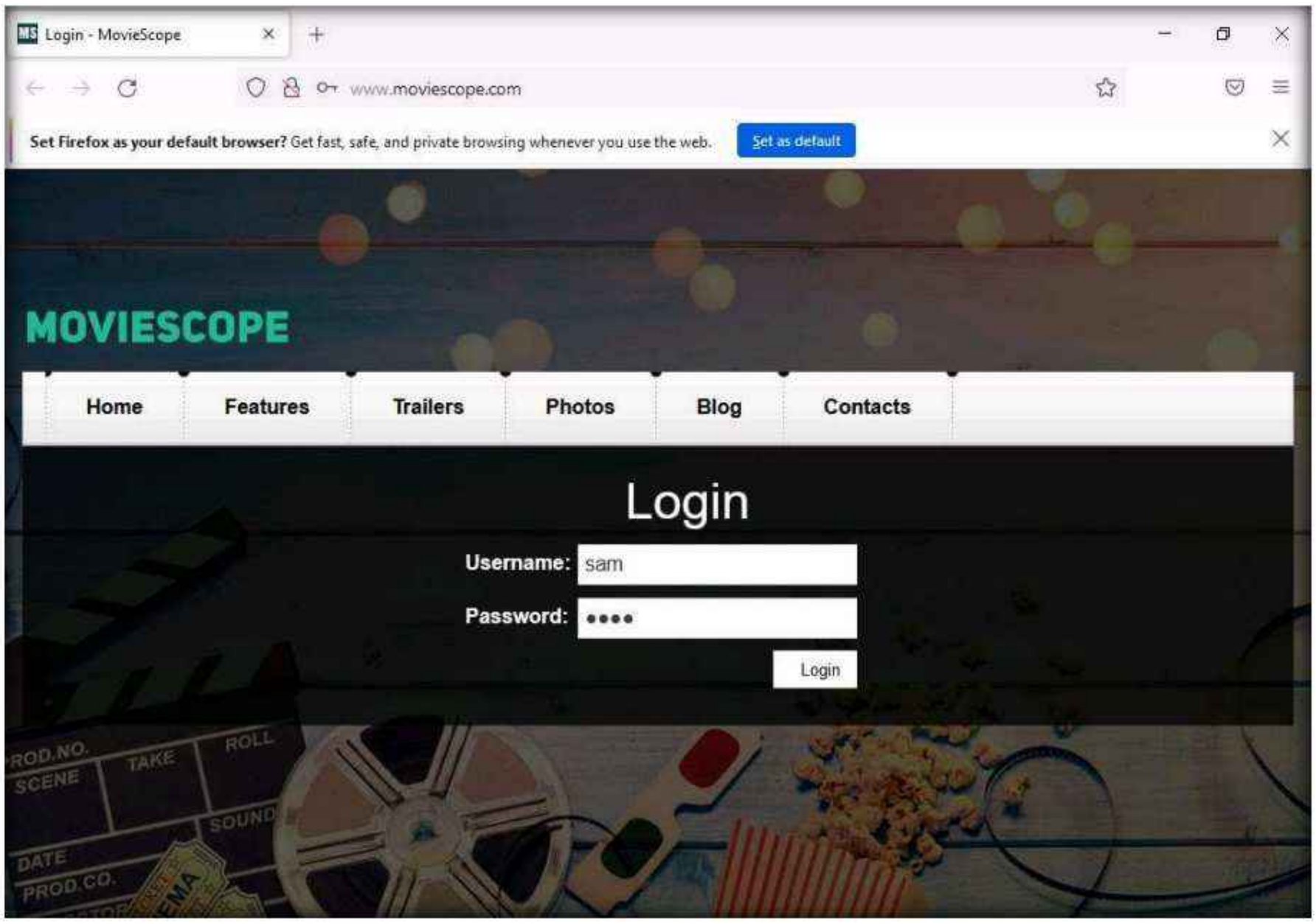
6. Now, switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**.
7. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

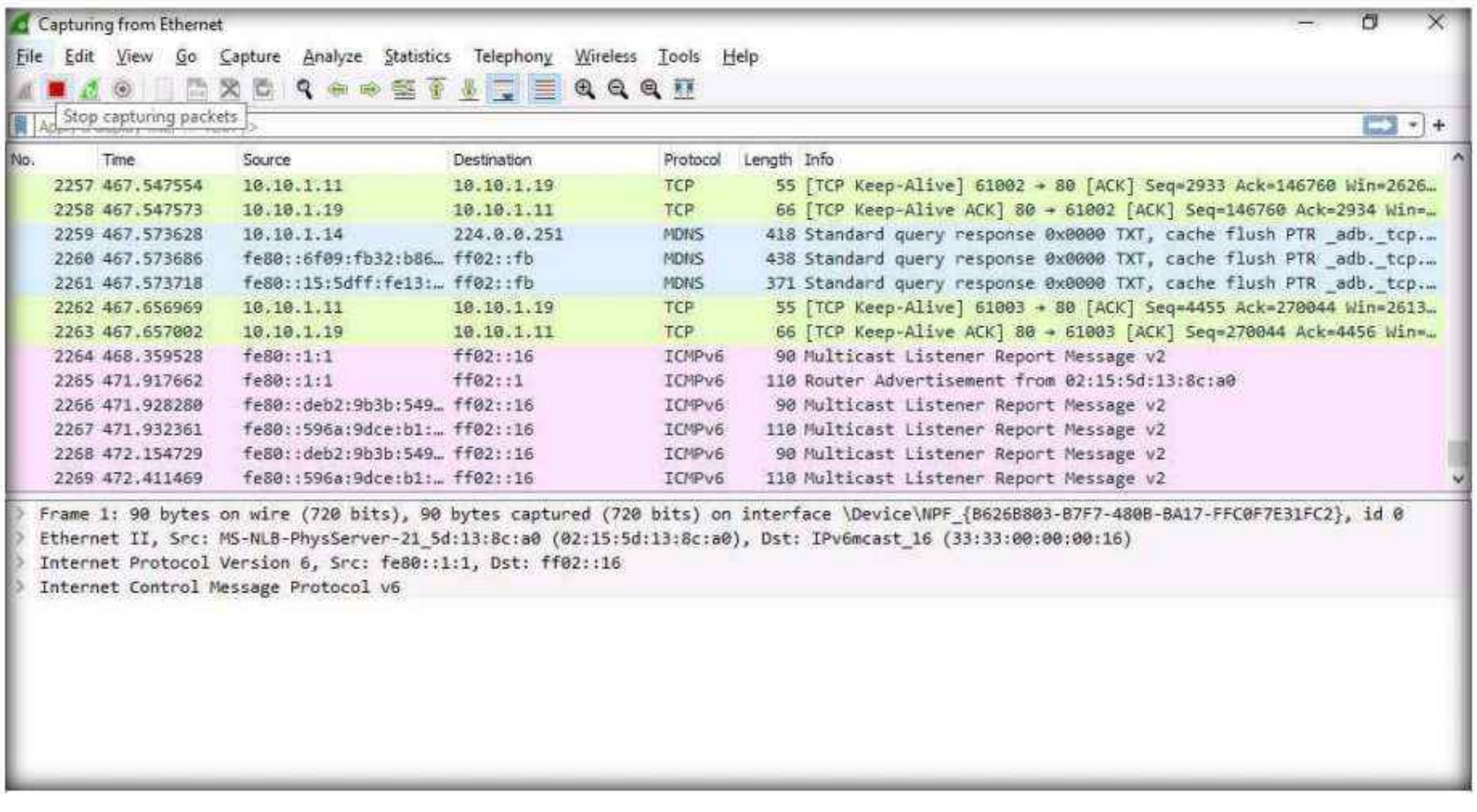
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



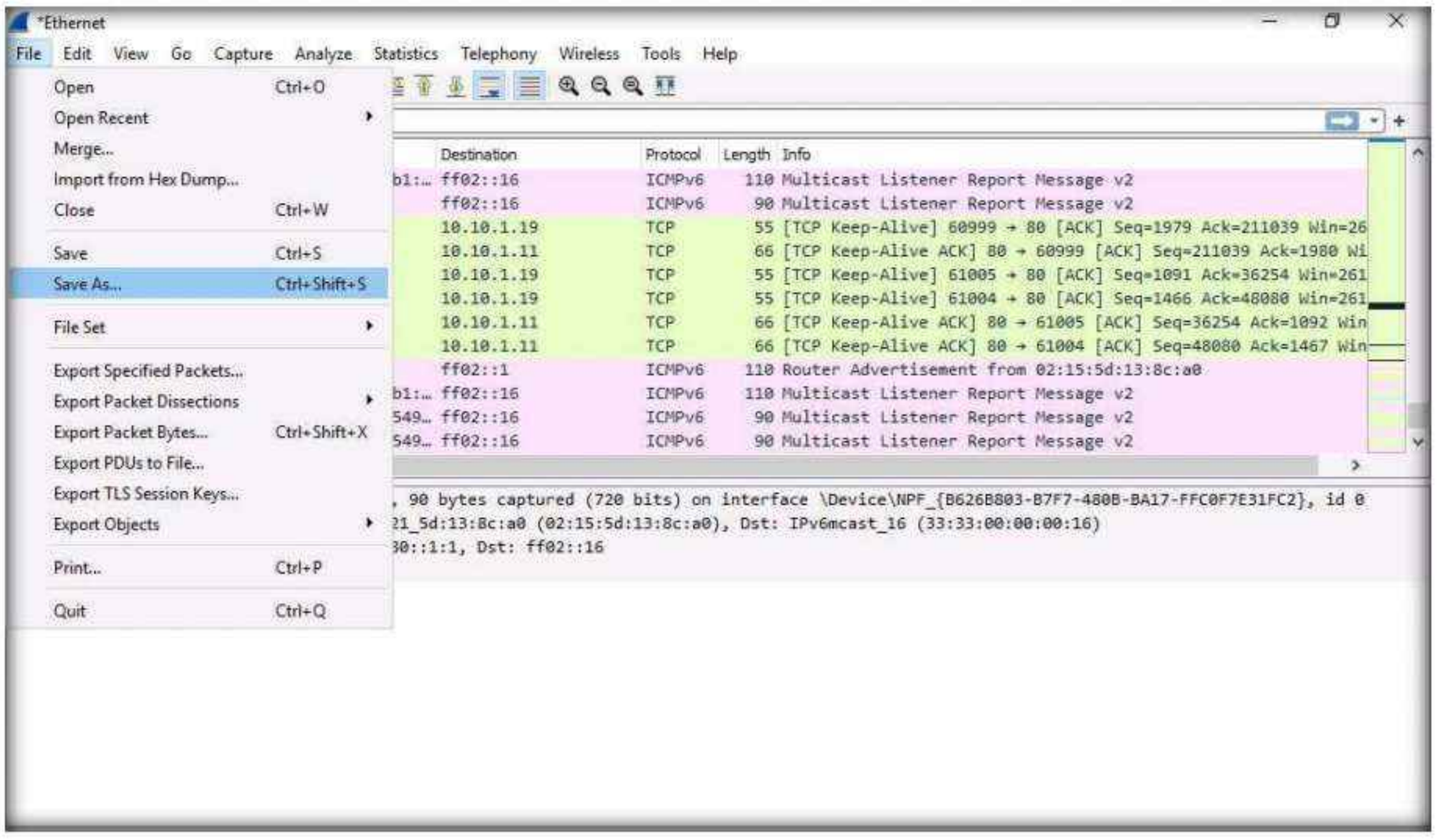
8. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **http://www.moviescope.com/** in the address bar, and press **Enter**.
9. The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in the screenshot.



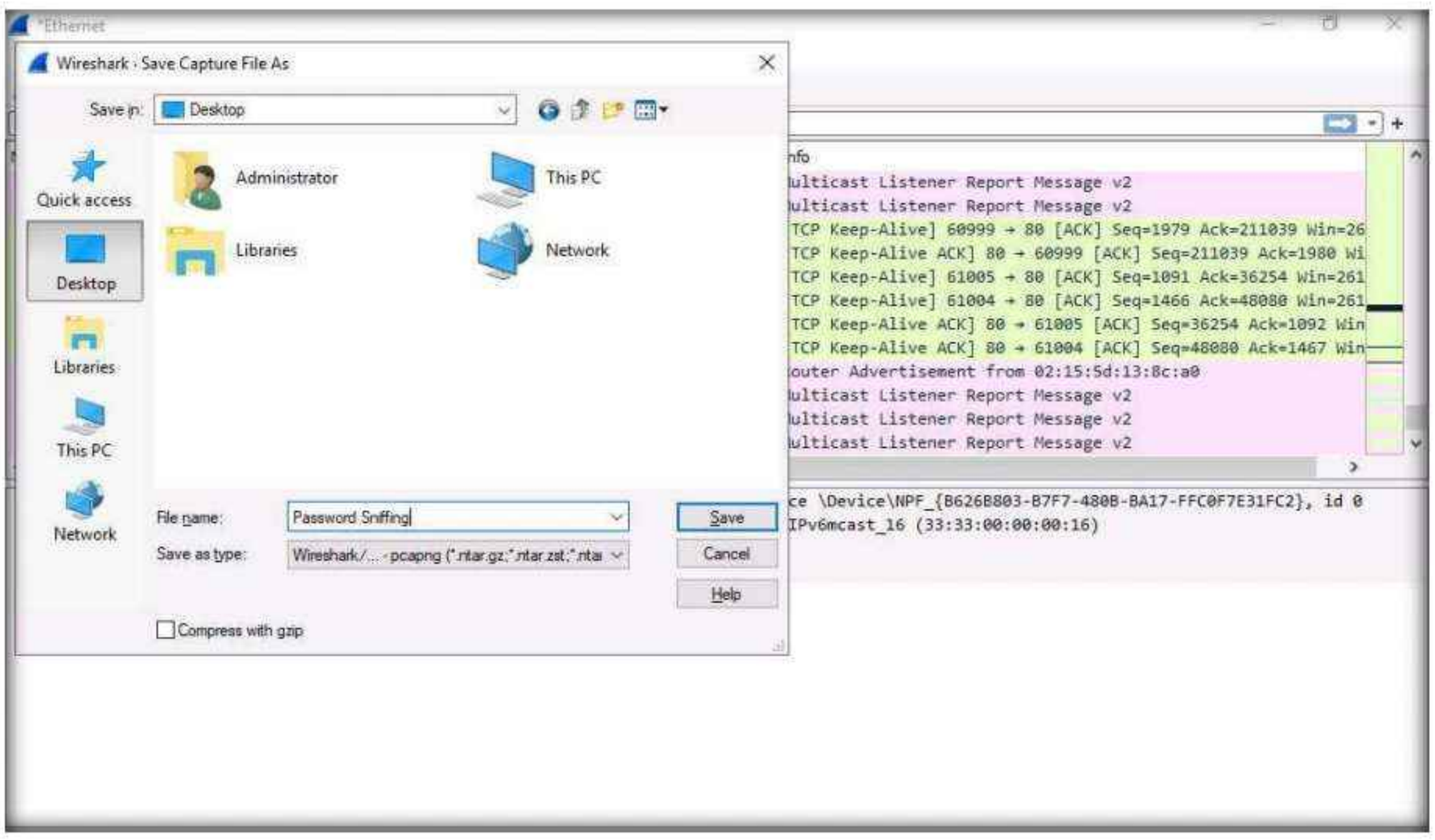
10. Switch back to **Windows Server 2019** virtual machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.



11. Click **File → Save As...** from the top-left corner of the window to save the captured packets.

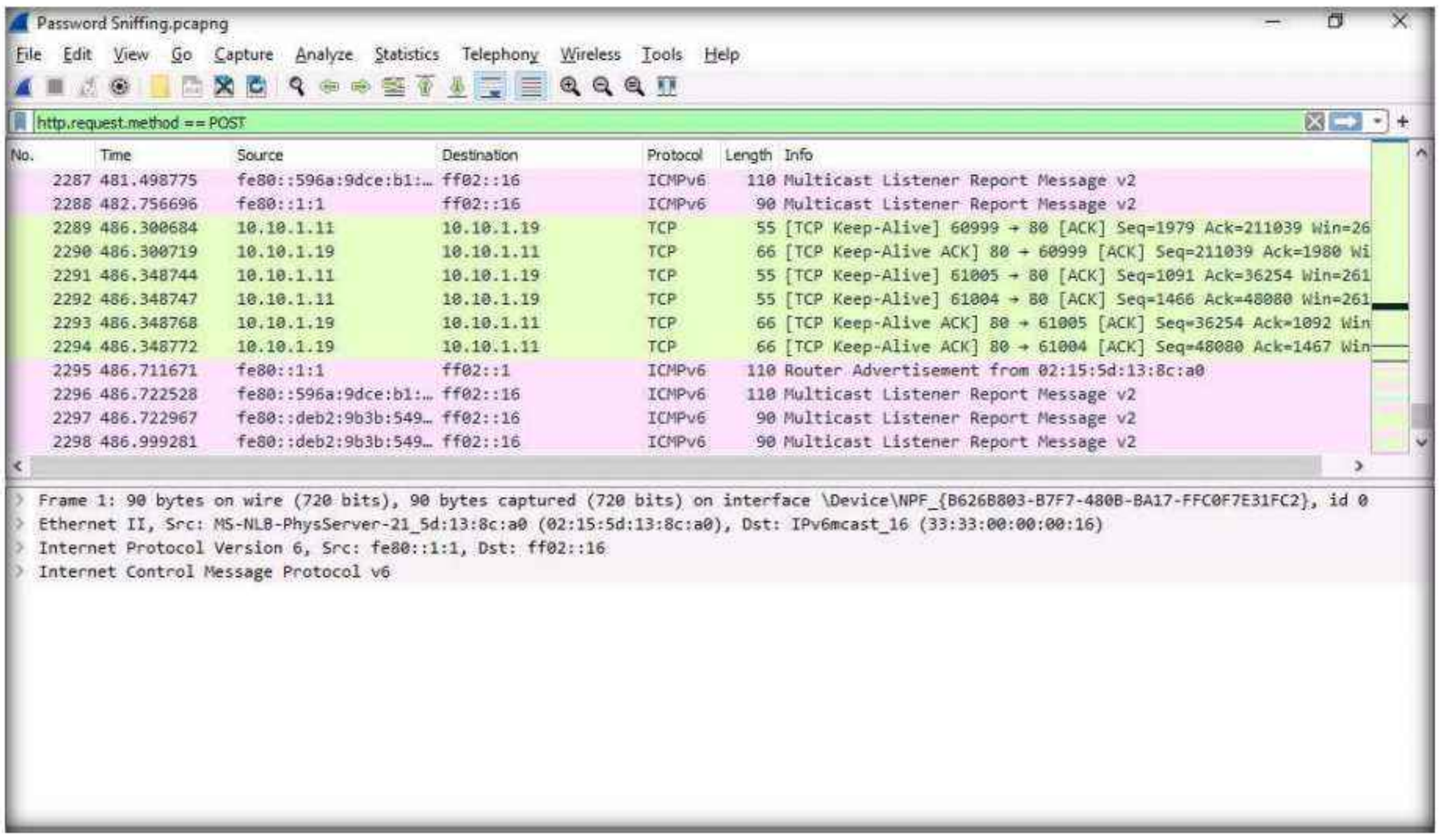


12. The **Wireshark: Save file as** window appears. Select any location to save the file, specify **File name** as **Password Sniffing**, and click **Save**.

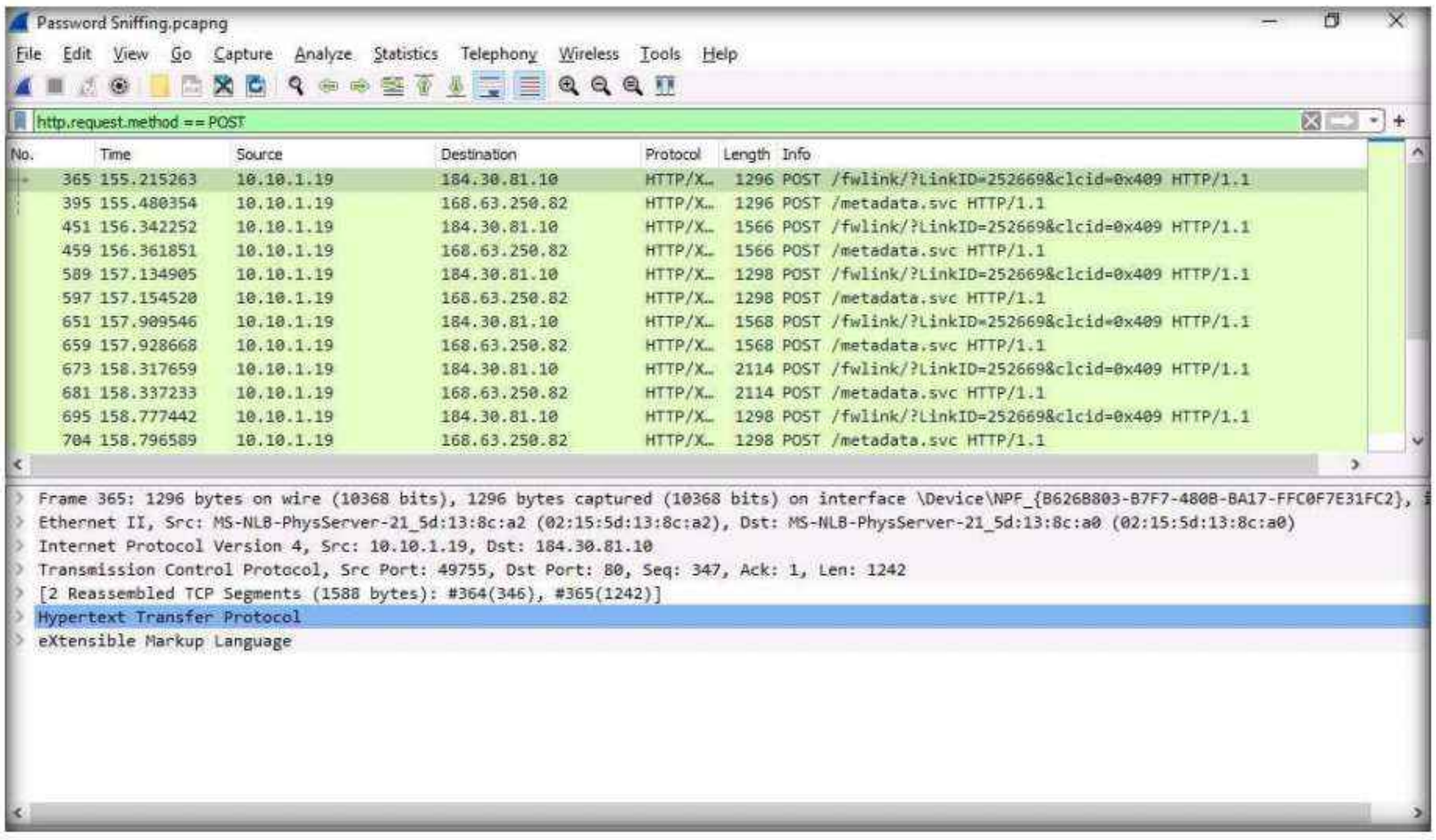


13. In the **Apply a display filter field**, type **http.request.method == POST** and click the arrow icon (→) to apply the filter.

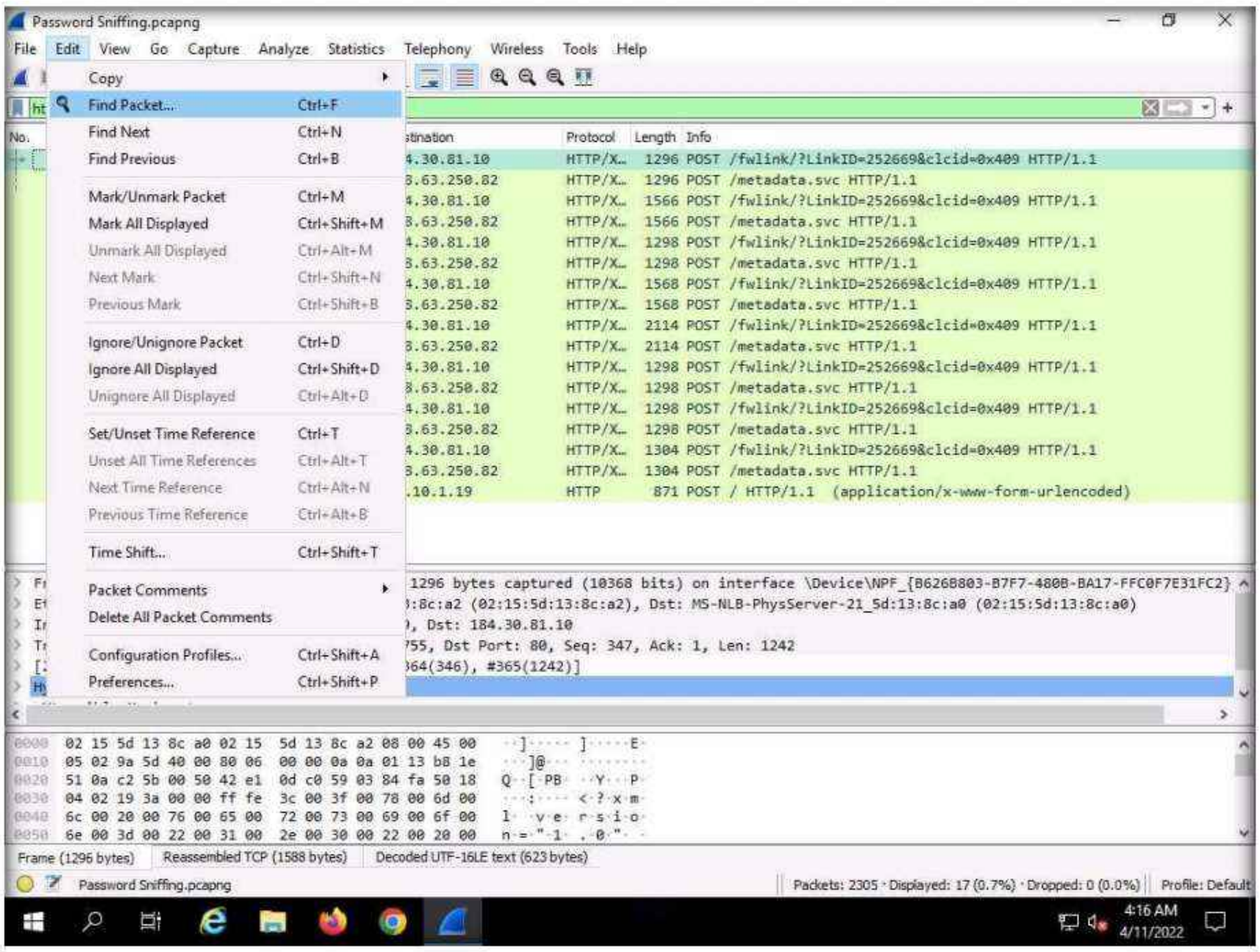
    Note: Applying this syntax helps you narrow down the search for http POST traffic.



14. Wireshark only filters **http POST** traffic packets, as shown in the screenshot.



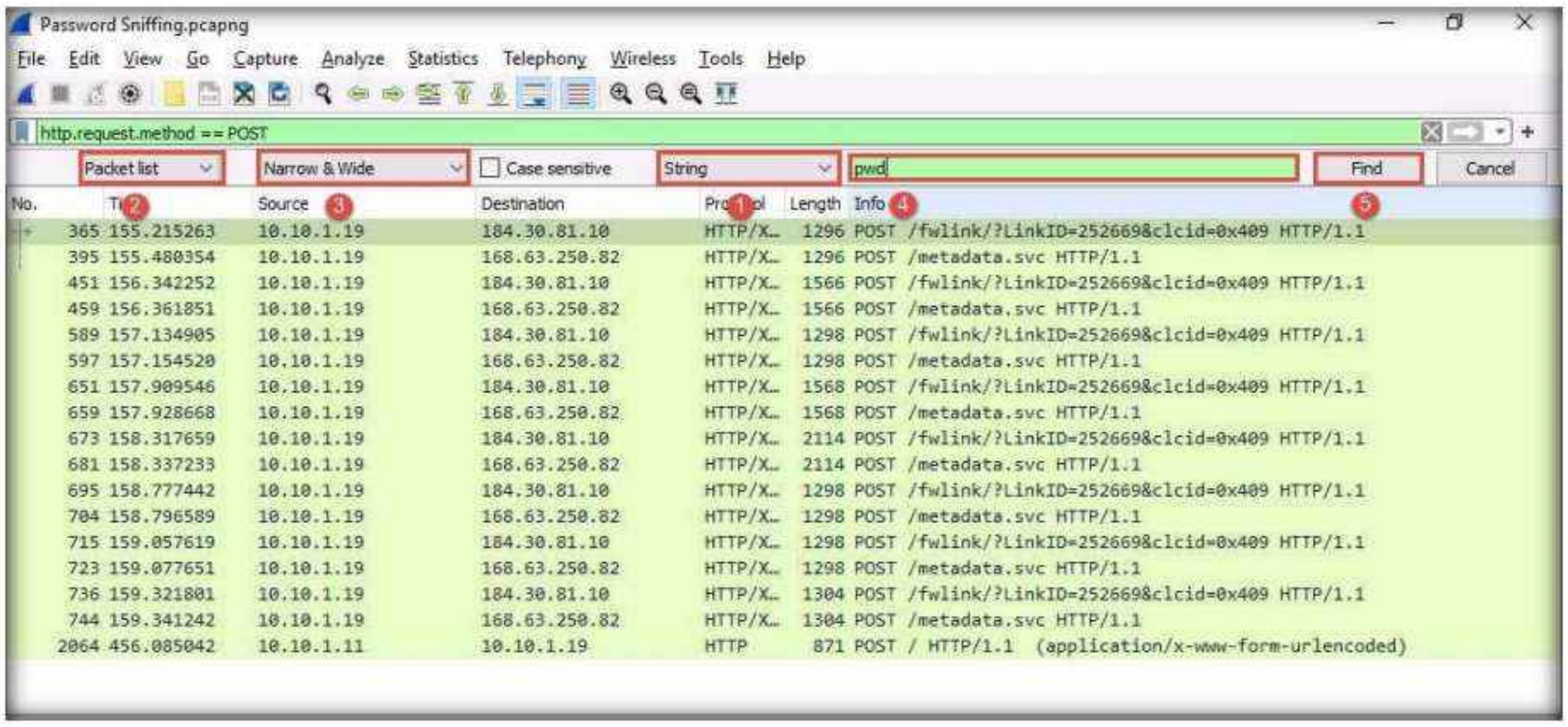
15. Now, click **Edit** from the menu bar and click **Find Packet…**.



16. The **Find Packet** section appears below the display filter field.

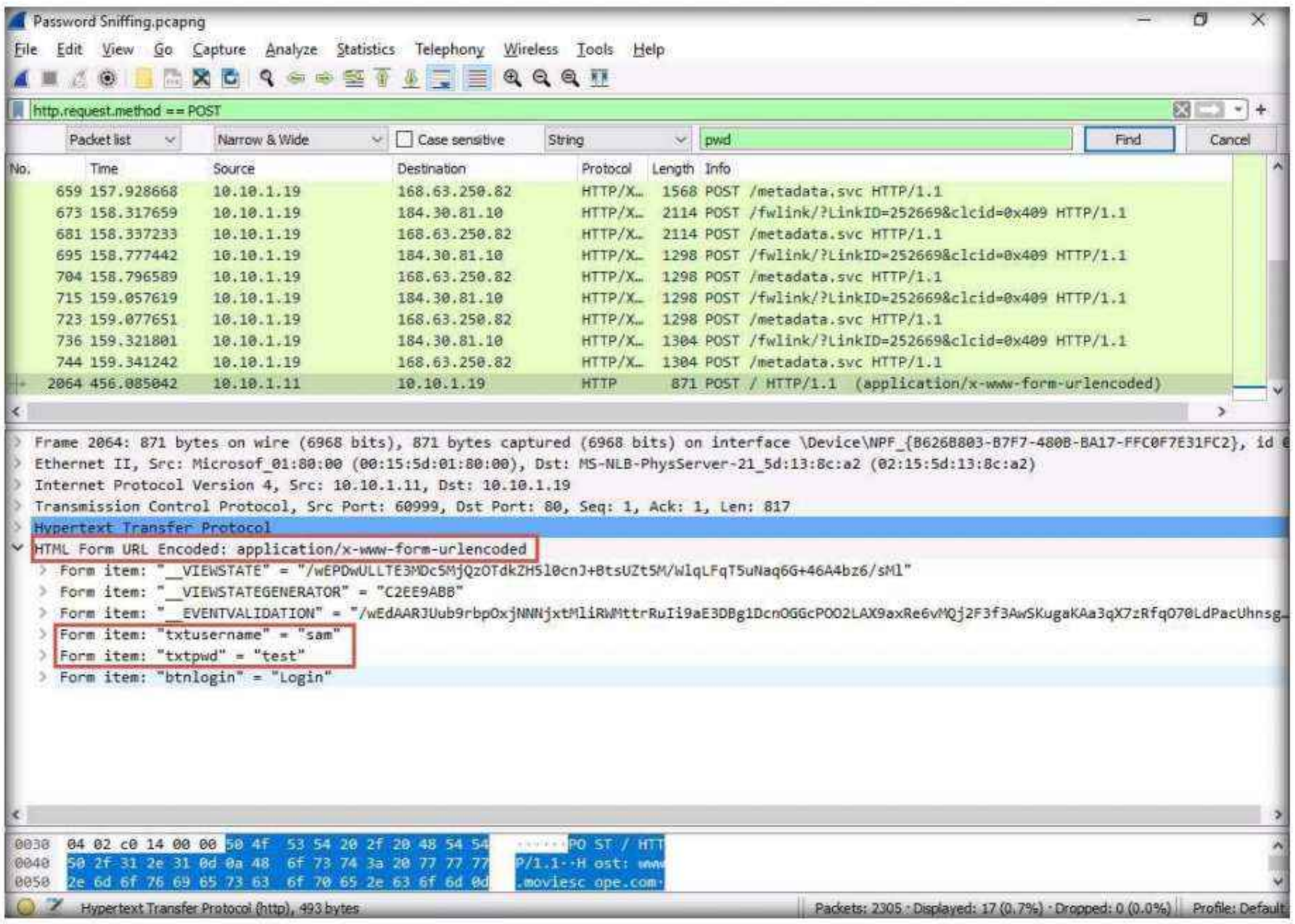
17. Click **Display filter**, select **String** from the drop-down options. Click **Packet list**, select **Packet details** from the drop-down options, and click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options.

18. In the field next to **String**, type **pwd** and click the **Find** button.



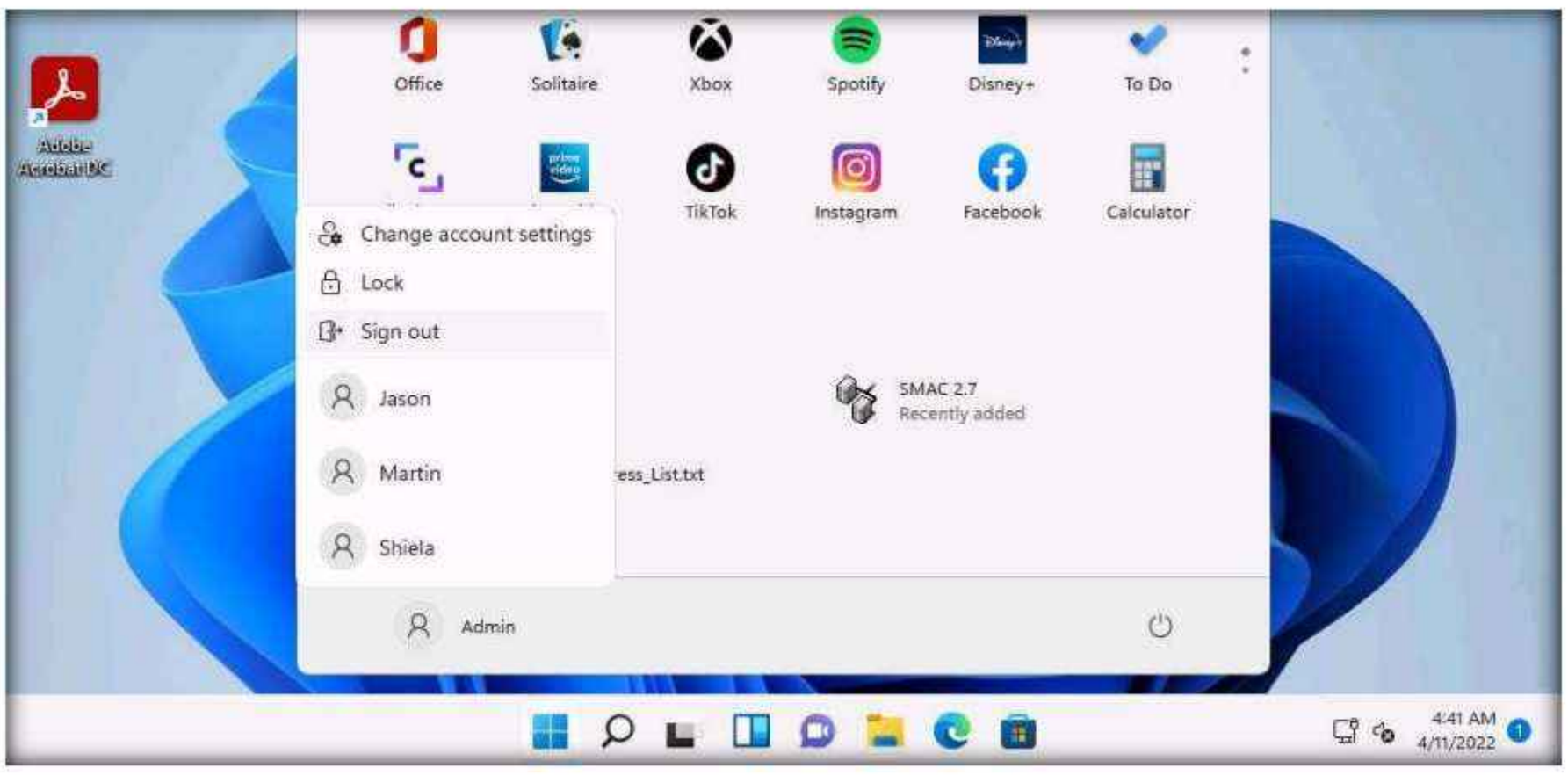
19. **Wireshark** will now display the sniffed password from the captured packets.

20. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** node from the packet details section, and view the captured username and password, as shown in the screenshot.

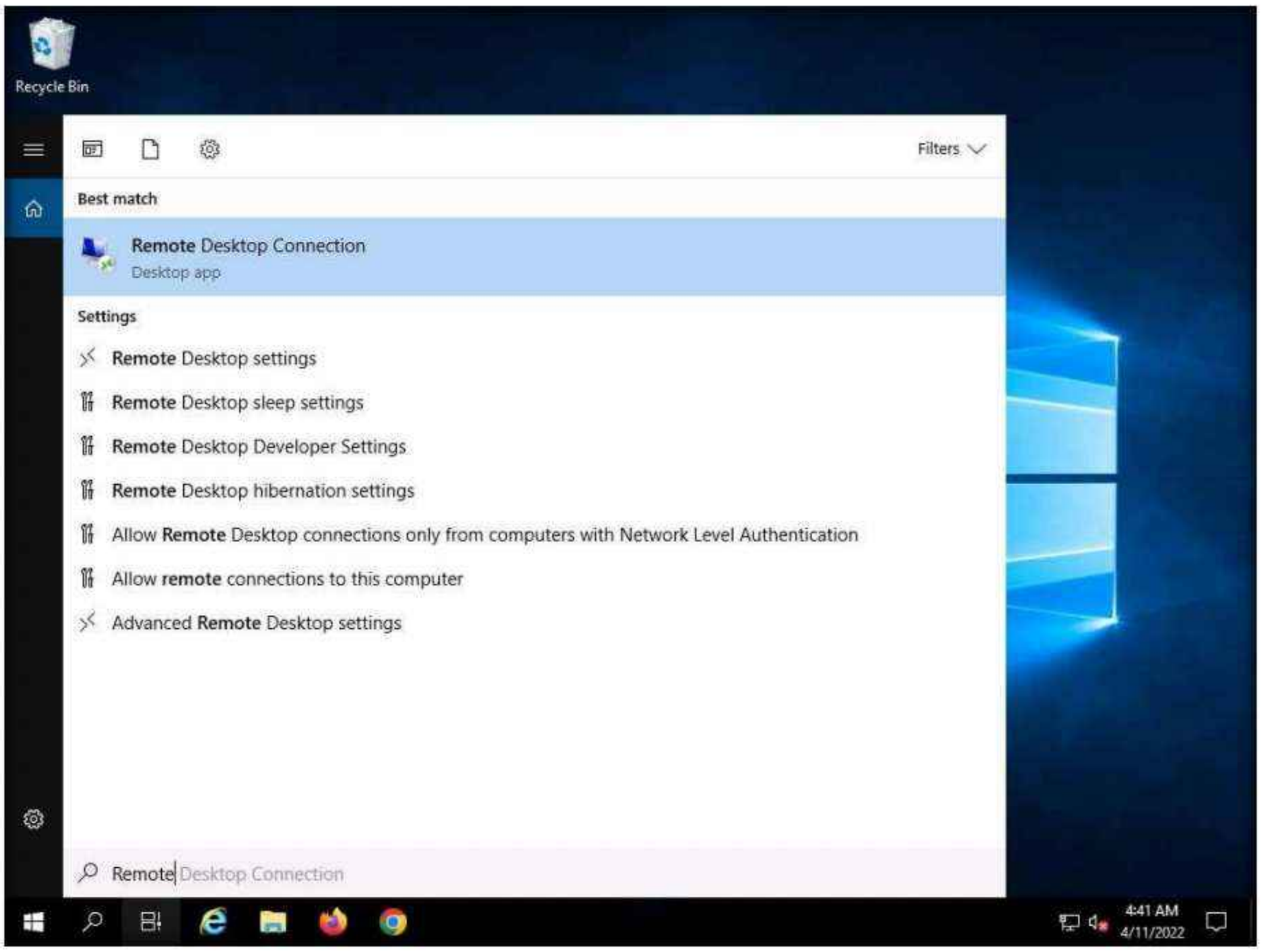


21. Close the **Wireshark** window.

22. Switch to the **Windows 11** virtual machine, close the web browser, and sign out from the **Admin** account.



23. Switch back to the **Windows Server 2019** virtual machine.
24. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

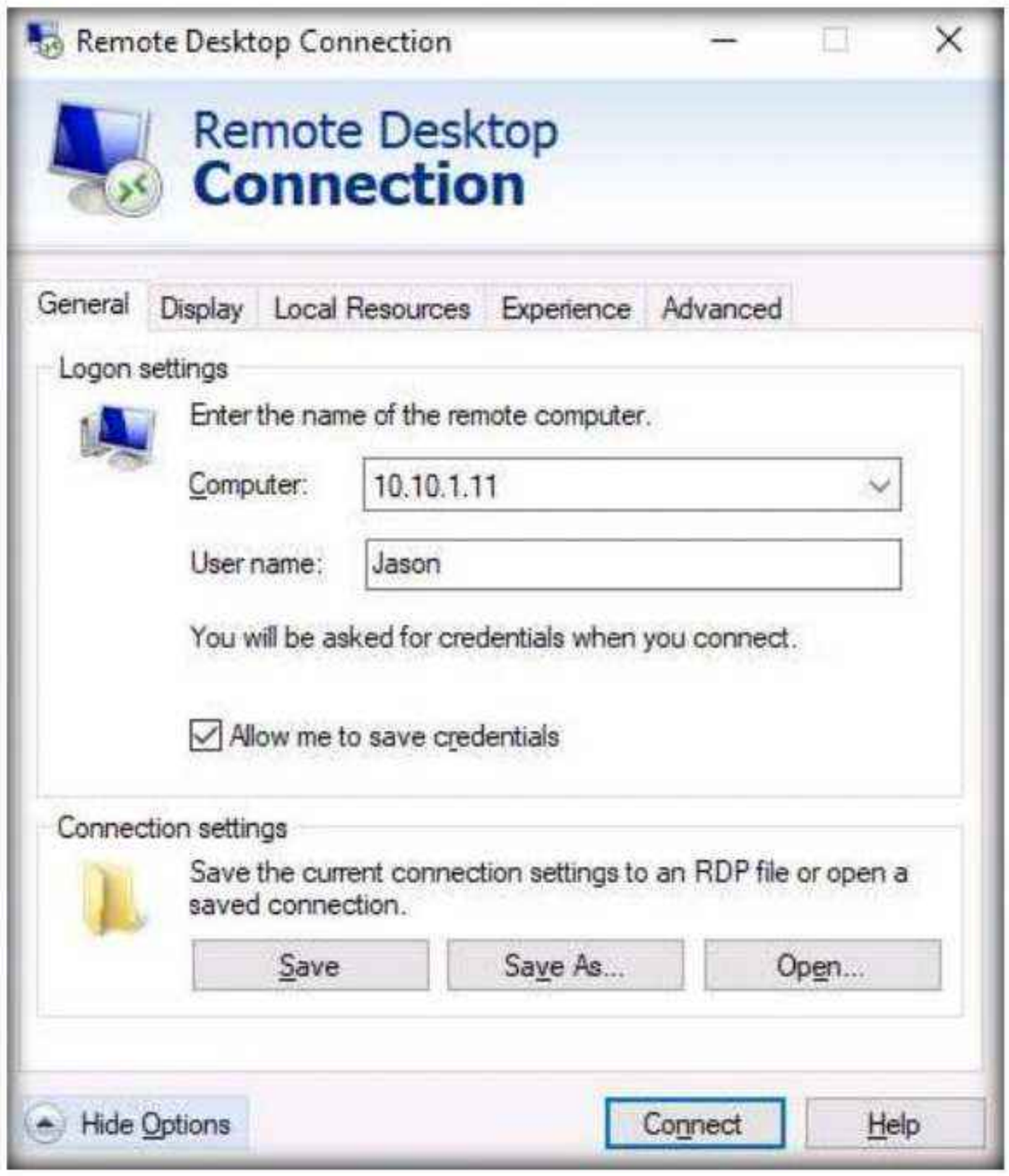


25. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

Note: If some previously accessed IP address appears in the **Computer** field, delete it.

26. The dialog-box expands; under the **General** tab, type **10.10.1.11** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

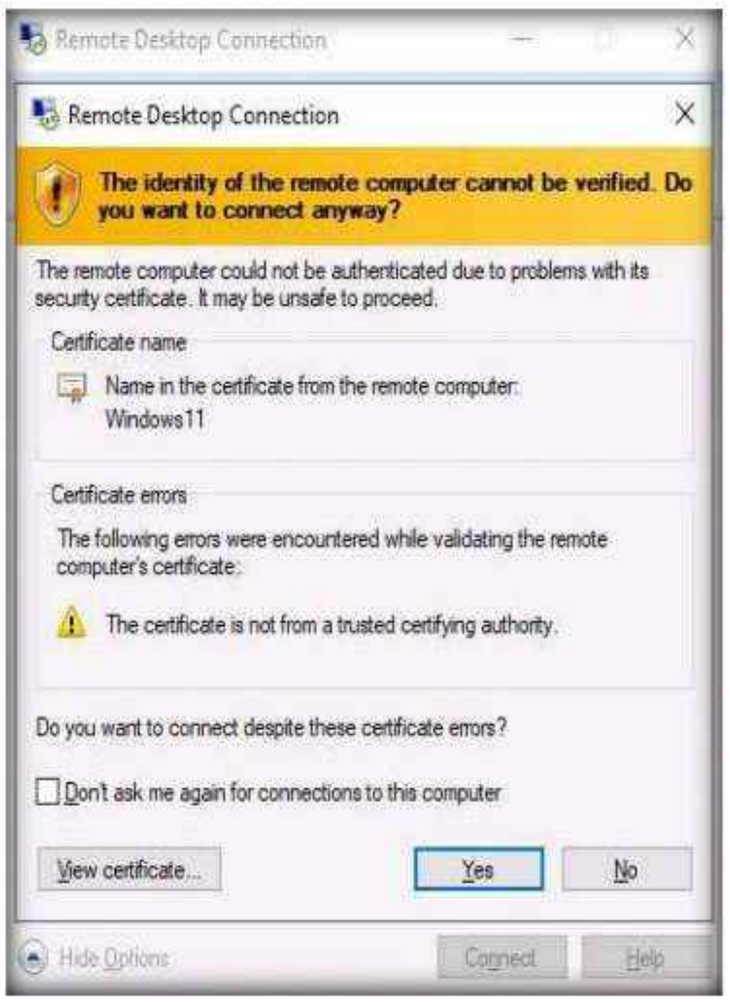
Note: The IP address and username might differ in your lab environment. The target system credentials (**Jason** and **qwerty**) we are using here are obtained in the previous labs.



27. The **Windows Security** pop-up appears. Enter **Password** (**qwerty**) and click **OK**.

Note: If **Remember me** option is checked uncheck it.

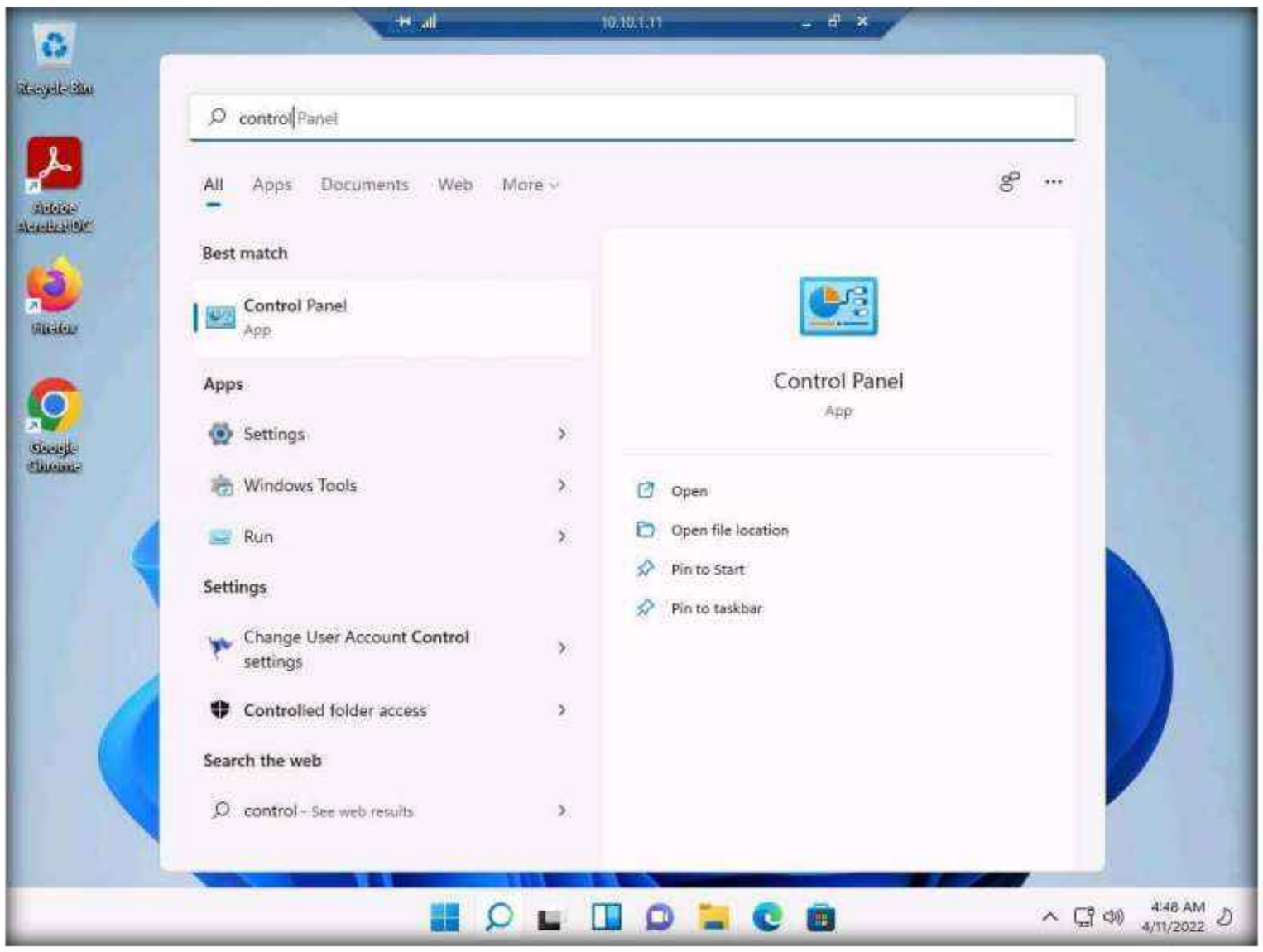
28. The **Remote Desktop Connection** pop-up appears; click **Yes**.



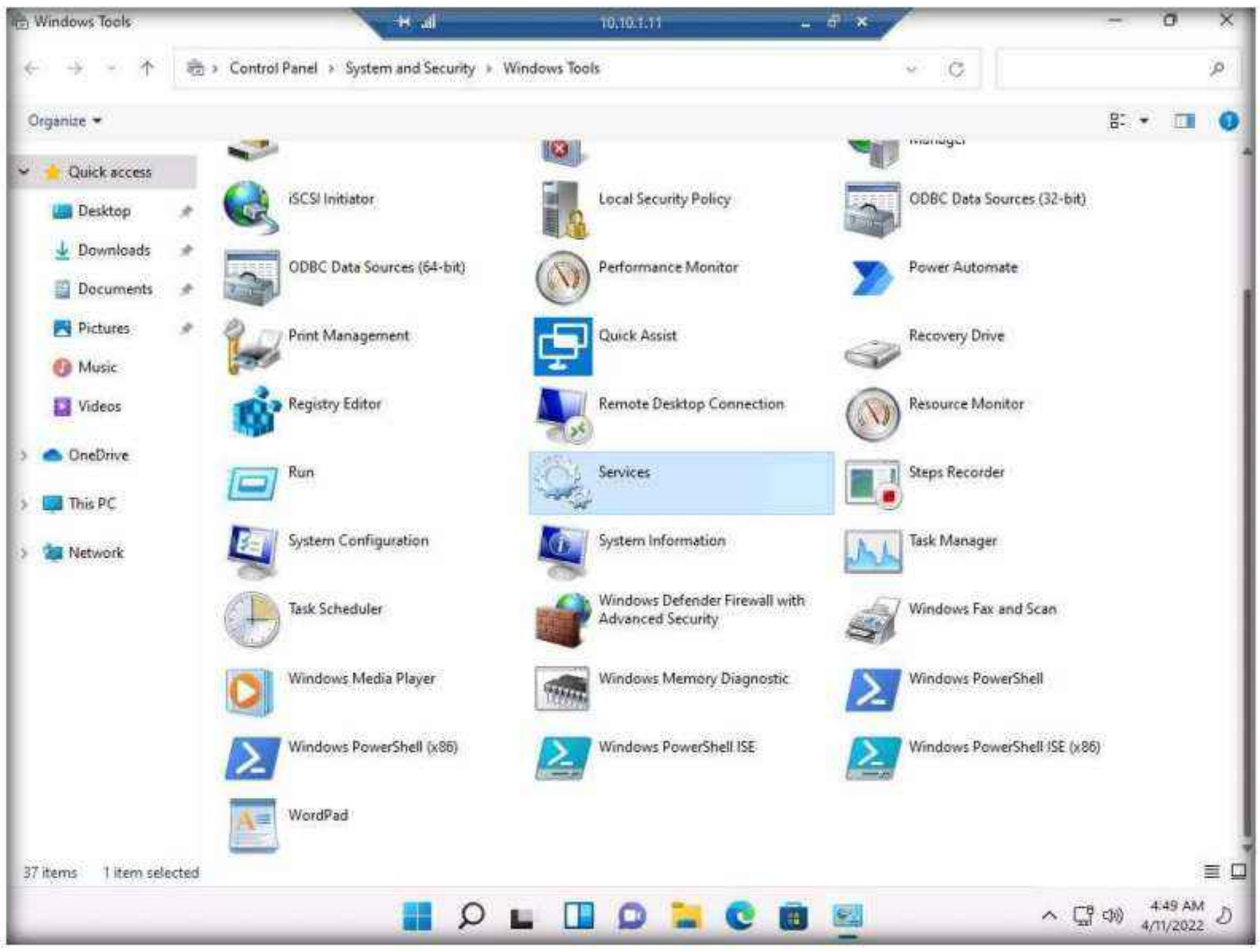
29. A remote connection to the target system (**Windows 11**) appears, as shown in the screenshot.

Note: If a **Choose privacy settings for your device** window appears, click on **Next** in the next window click on **Next** and in the next window click on **Accept**.

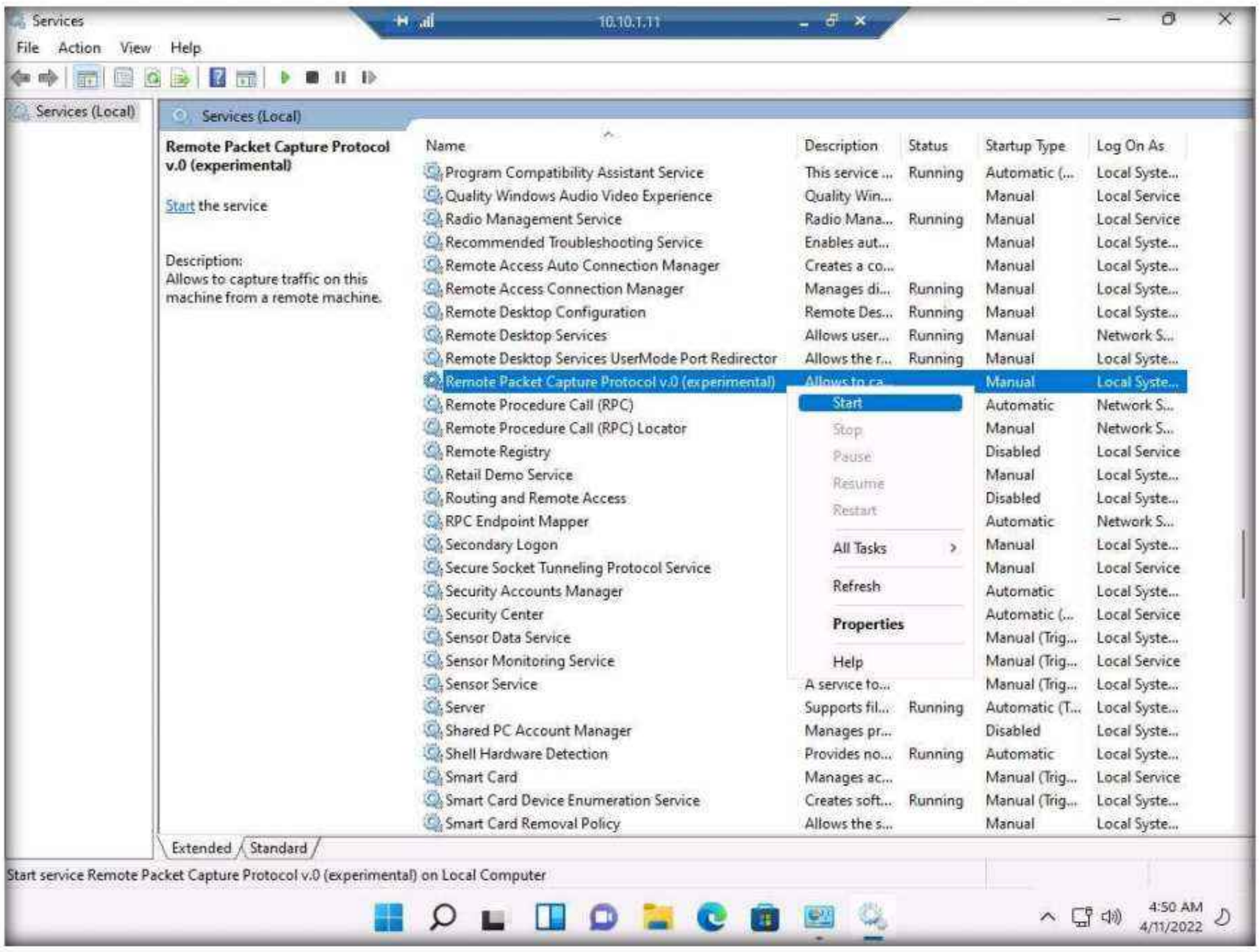
30. Click **Search** icon () on the **Desktop**. Type **Control** in the search field, the **Control Panel** appears in the results, click **Open** to launch it.



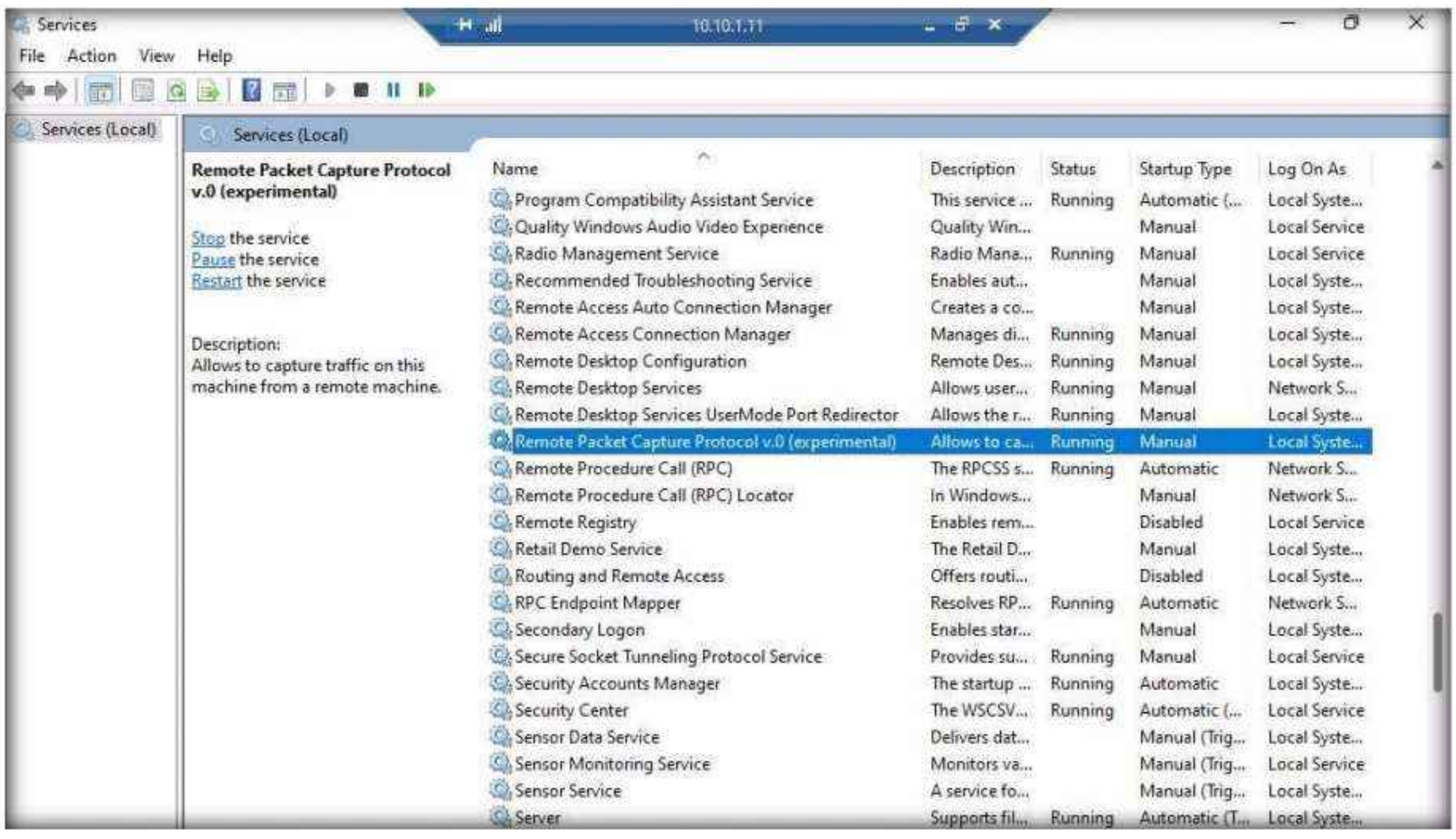
31. The **Control Panel** window appears; navigate to **System and Security → Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.



32. The **Services** window appears. Choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service, and click **Start**.



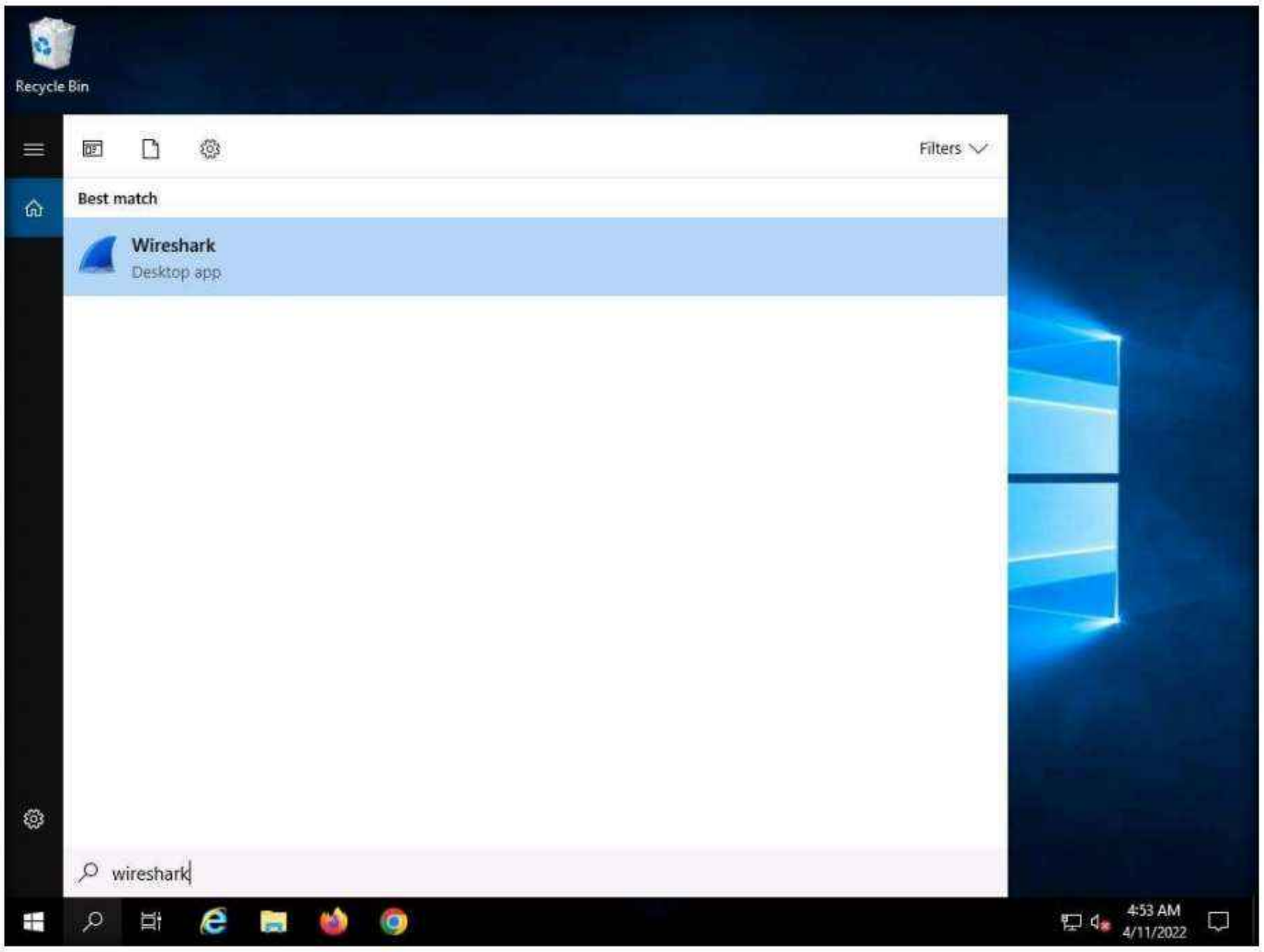
33. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.



34. Close all open windows on the **Windows 11** machine and close **Remote Desktop Connection**.

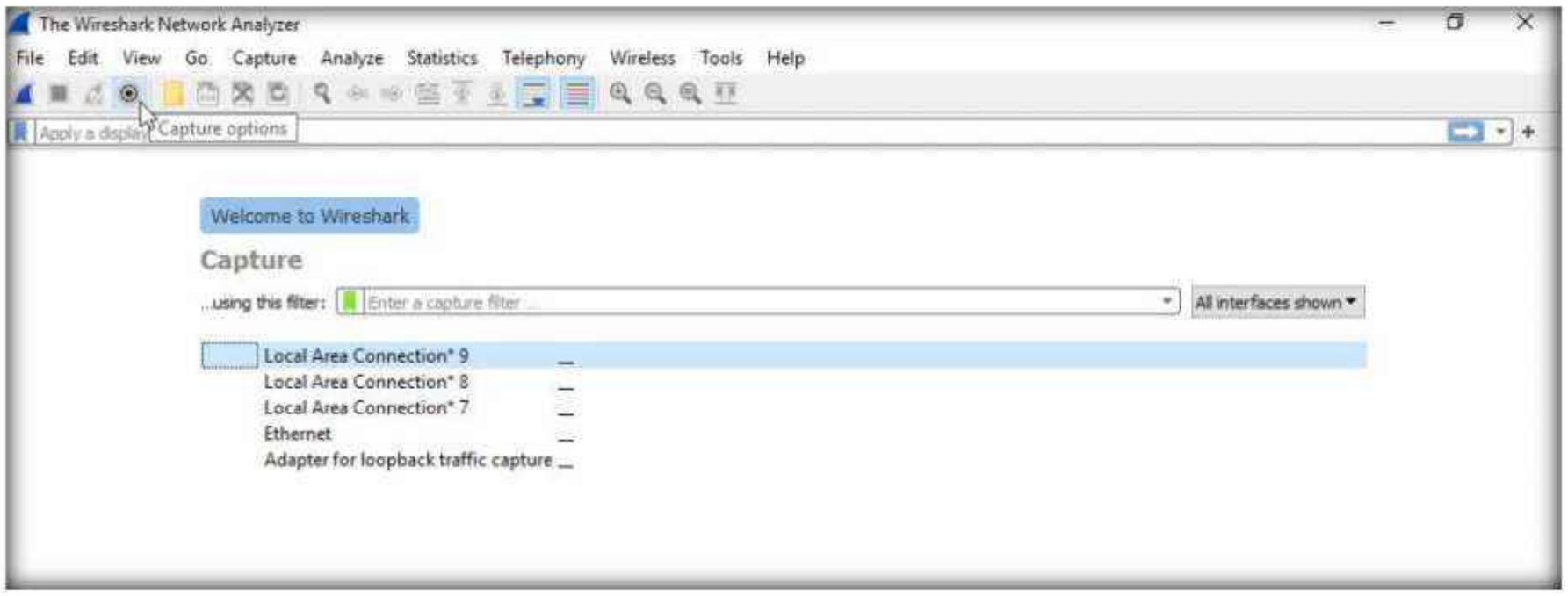
    Note: If a **Remote Desktop Connection** pop-up appears, click **OK**.

35. Now, in **Windows Server 2019**, click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results, to launch **Wireshark**.

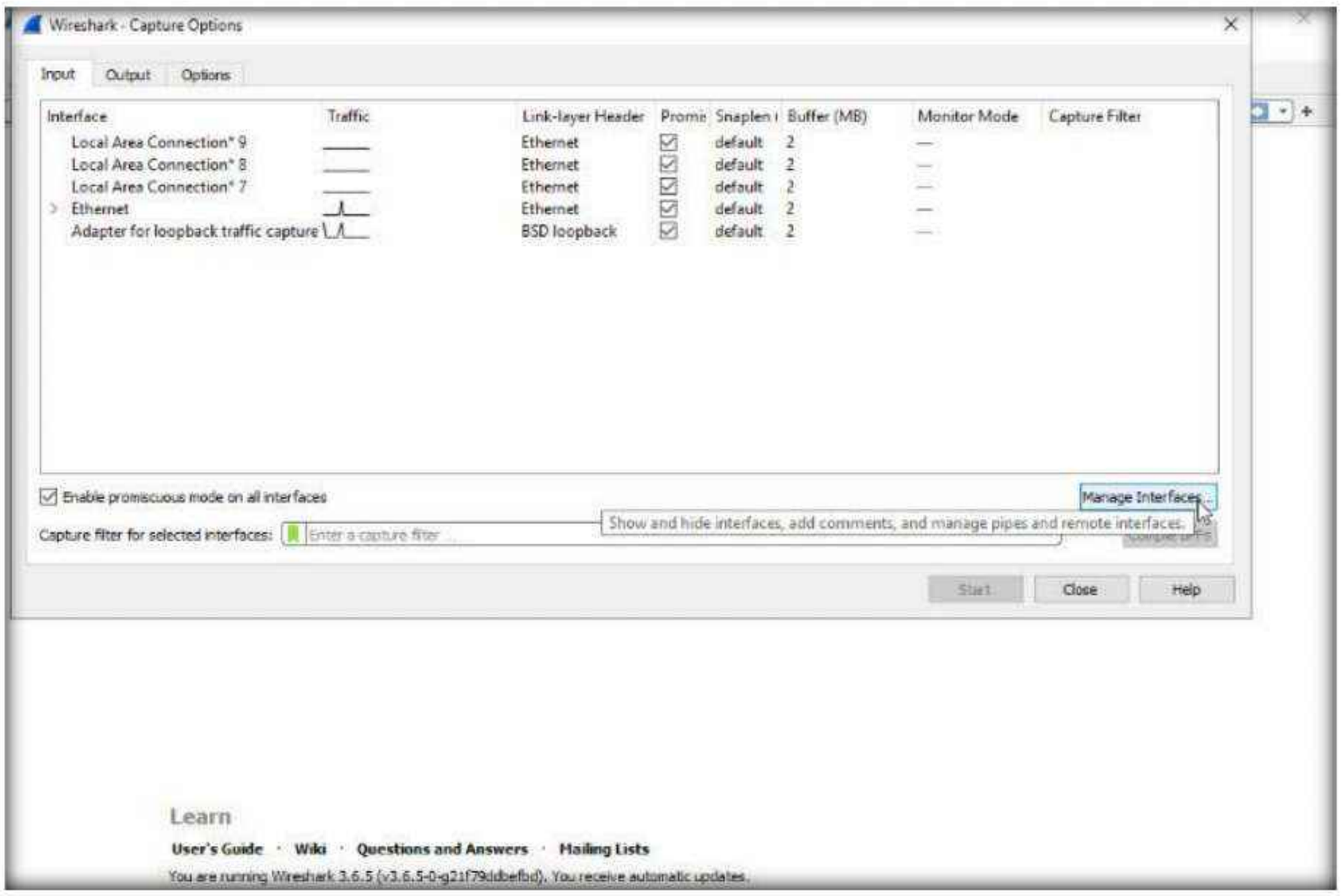


36. The **Wireshark Network Analyzer** window appears; click the **Capture options** icon from the toolbar.

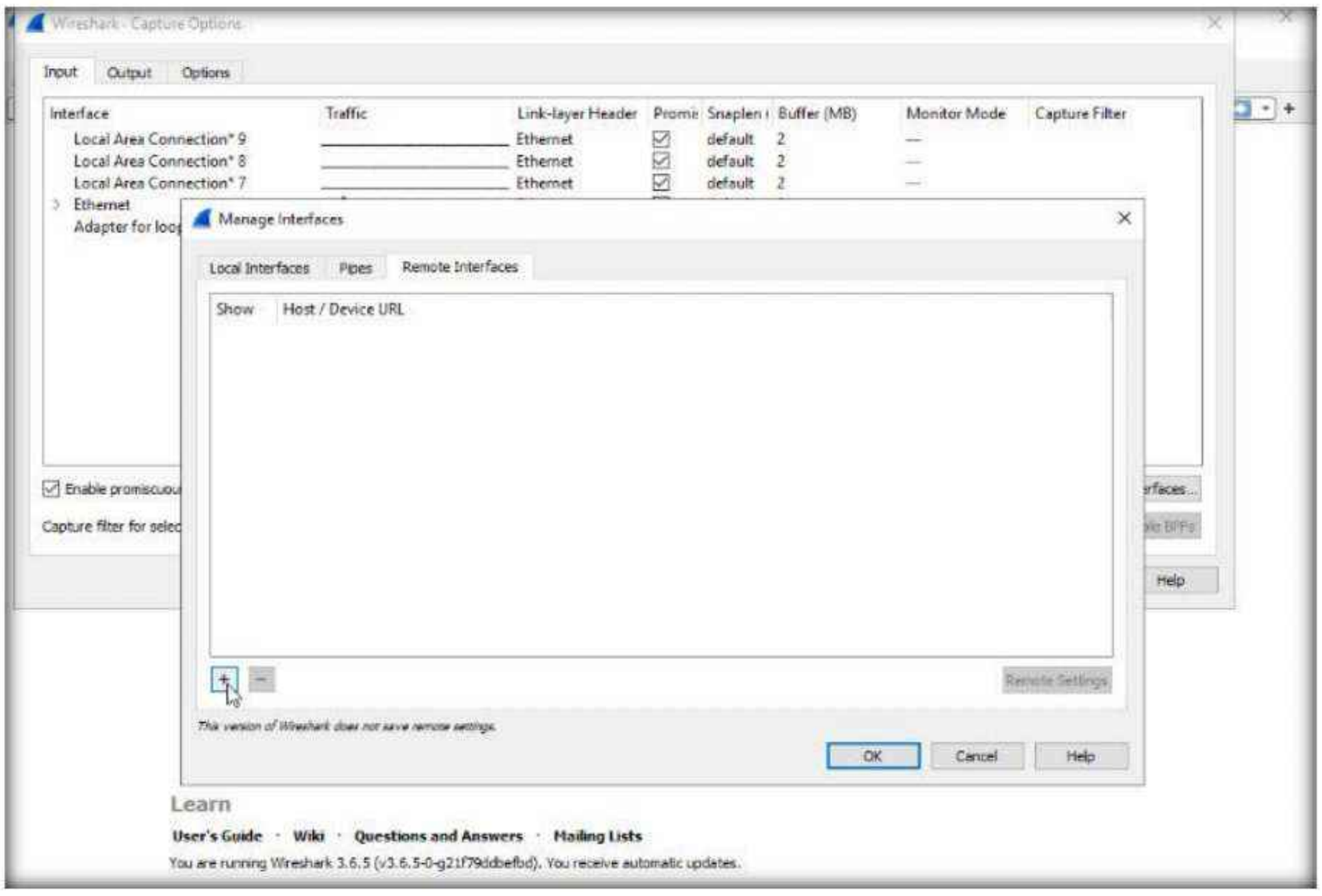
    Note: If a **Software Update** pop-up appears click on **Remind me later**.



37. The **Wireshark**. **Capture Options** window appears; click the **Manage Interfaces…** button.

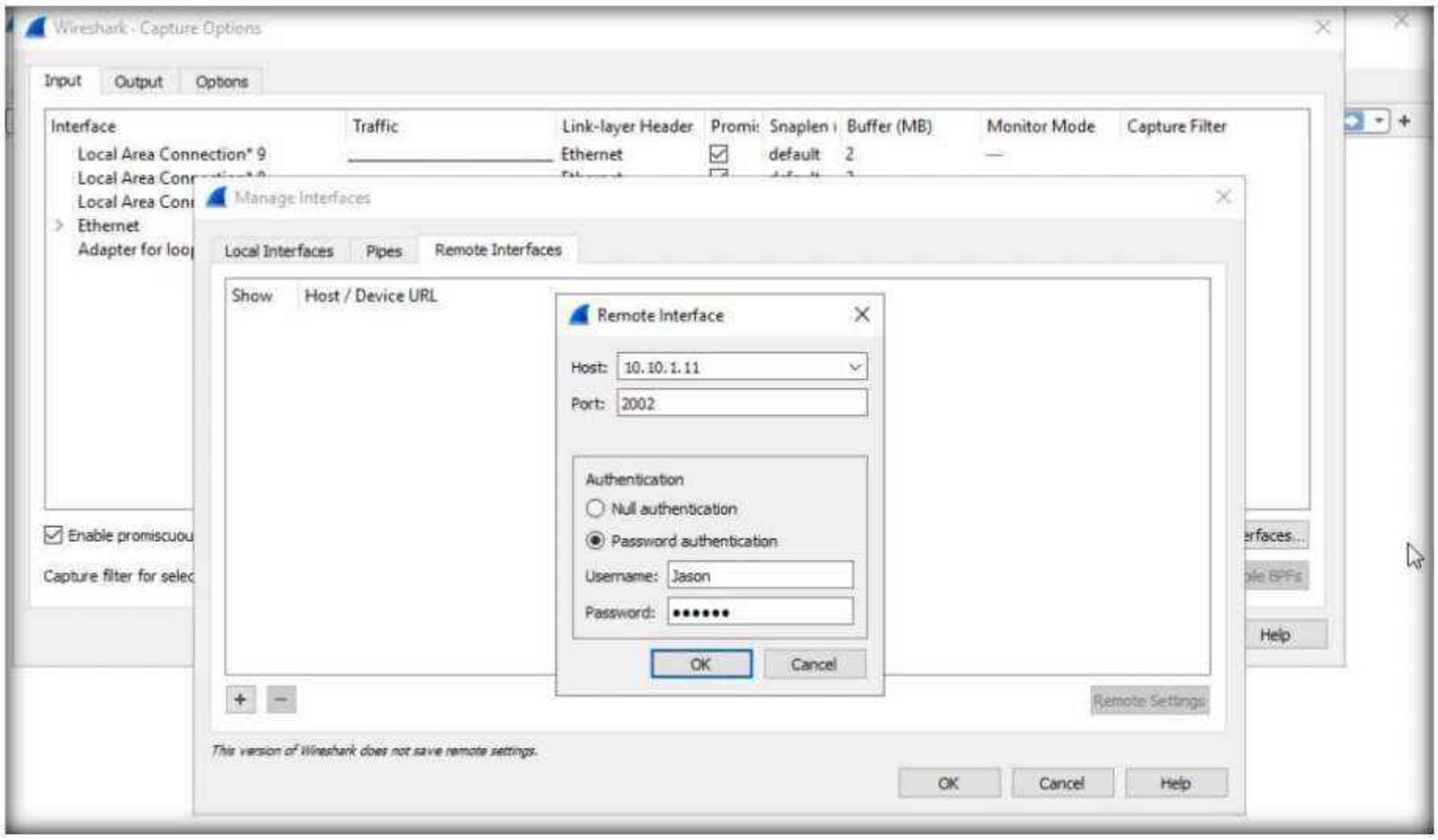


38. The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface** icon (**+**).

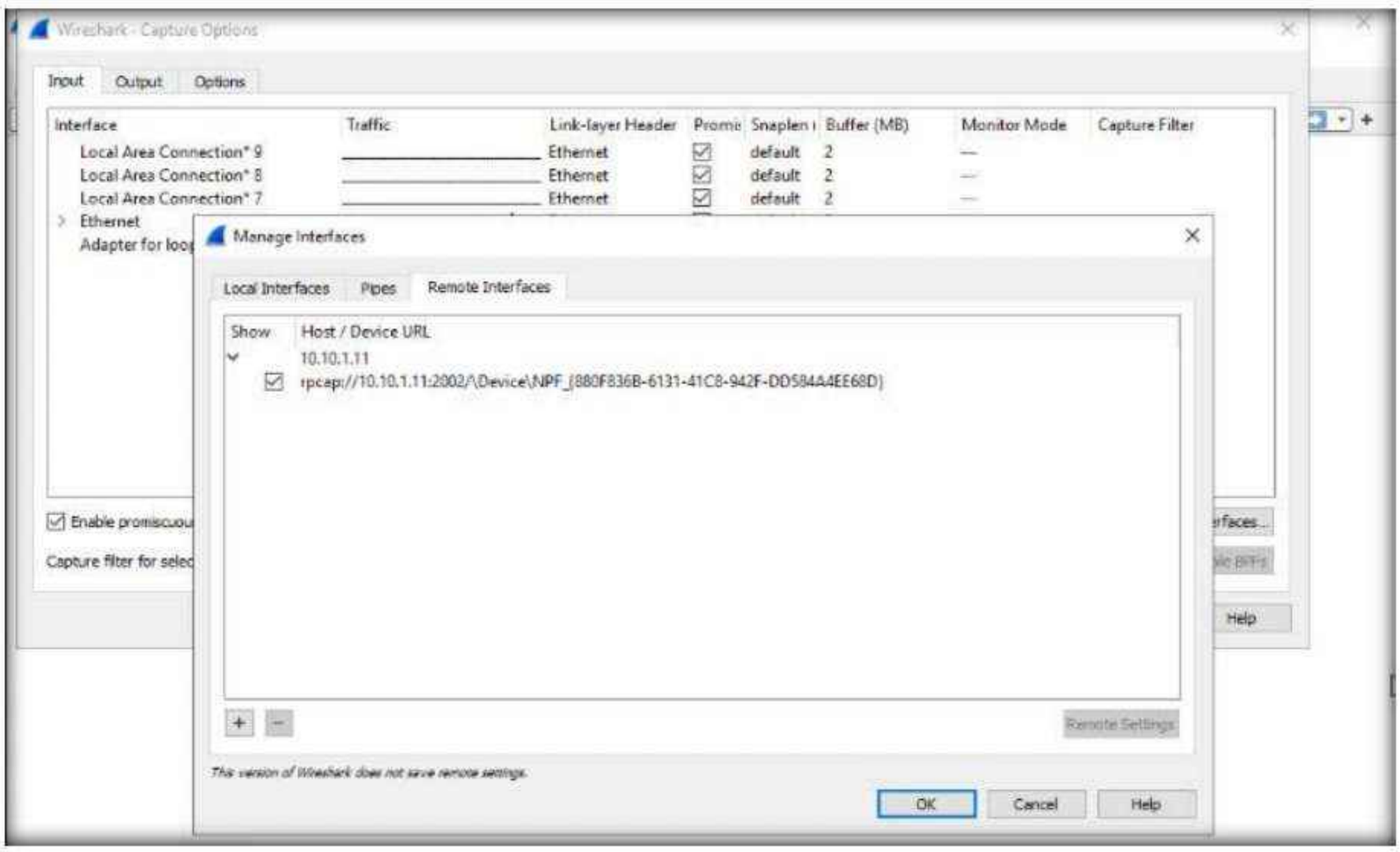


39. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.1.11**); and in the **Port** field, enter the port number as **2002**.
40. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.

    Note: The IP address and user credentials may differ when you perform this task.

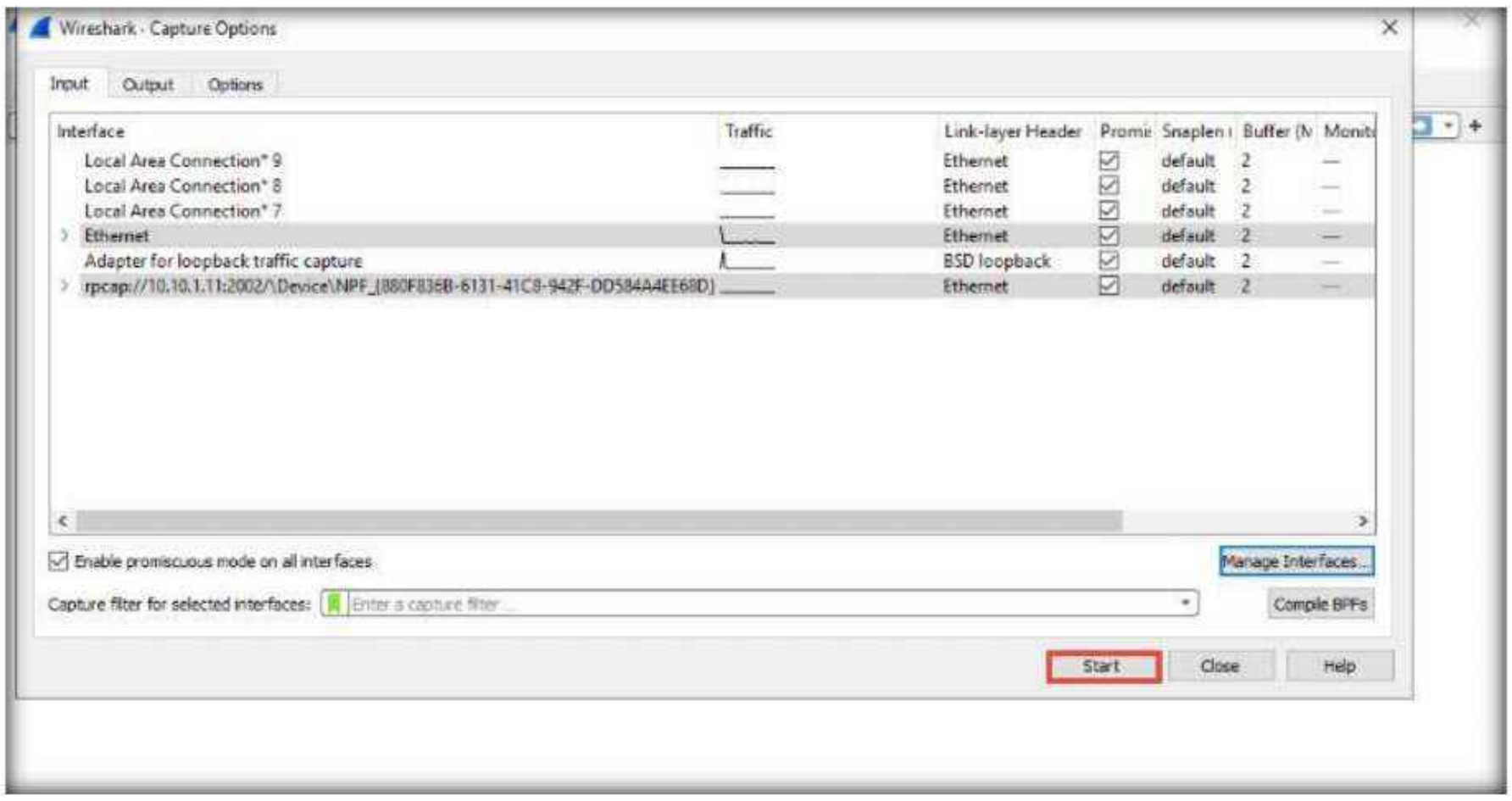


41. A new remote interface is added to the **Manage Interfaces** window; click **OK**.

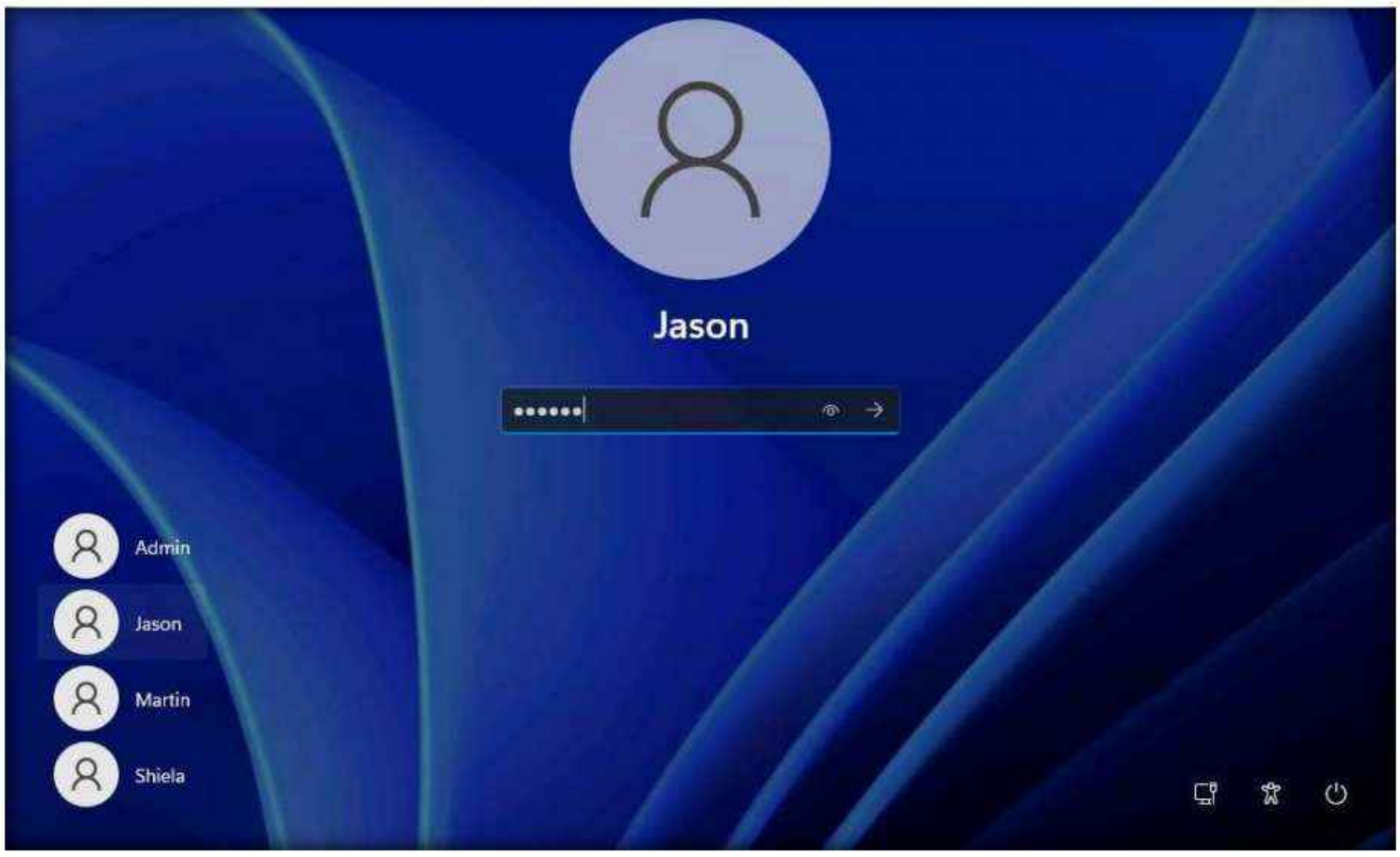


42. The newly added remote interface appears in the **Wireshark**. **Capture Options** window; click **Start**.

    Note: Ensure that both **Ethernet** and **rpcap** interfaces are selected.

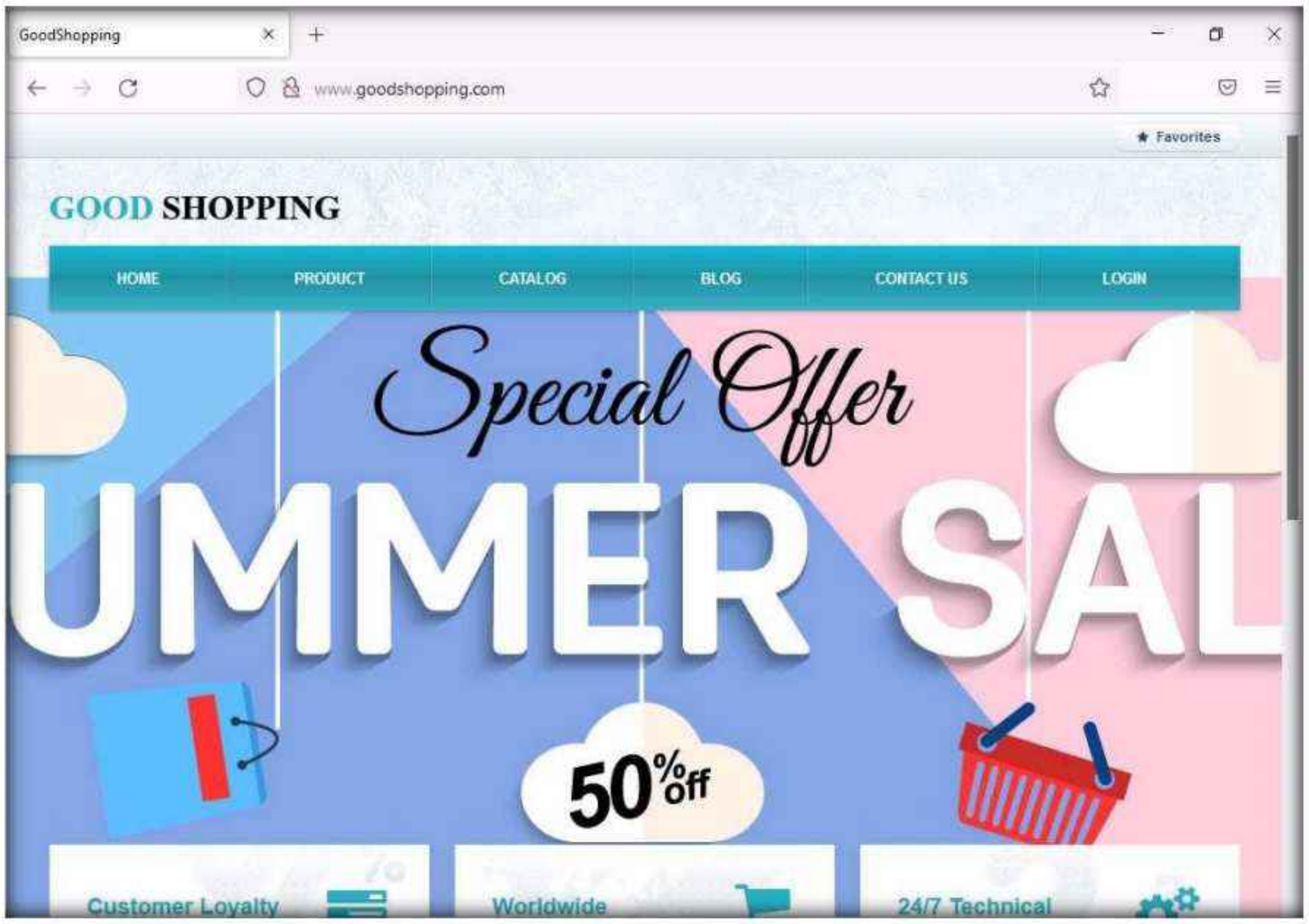


43. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. Select **Jason** from the list of user accounts in the left-pane, click **qwerty** to enter the password and press **Enter** to log in. Here, you are signing in as the victim.

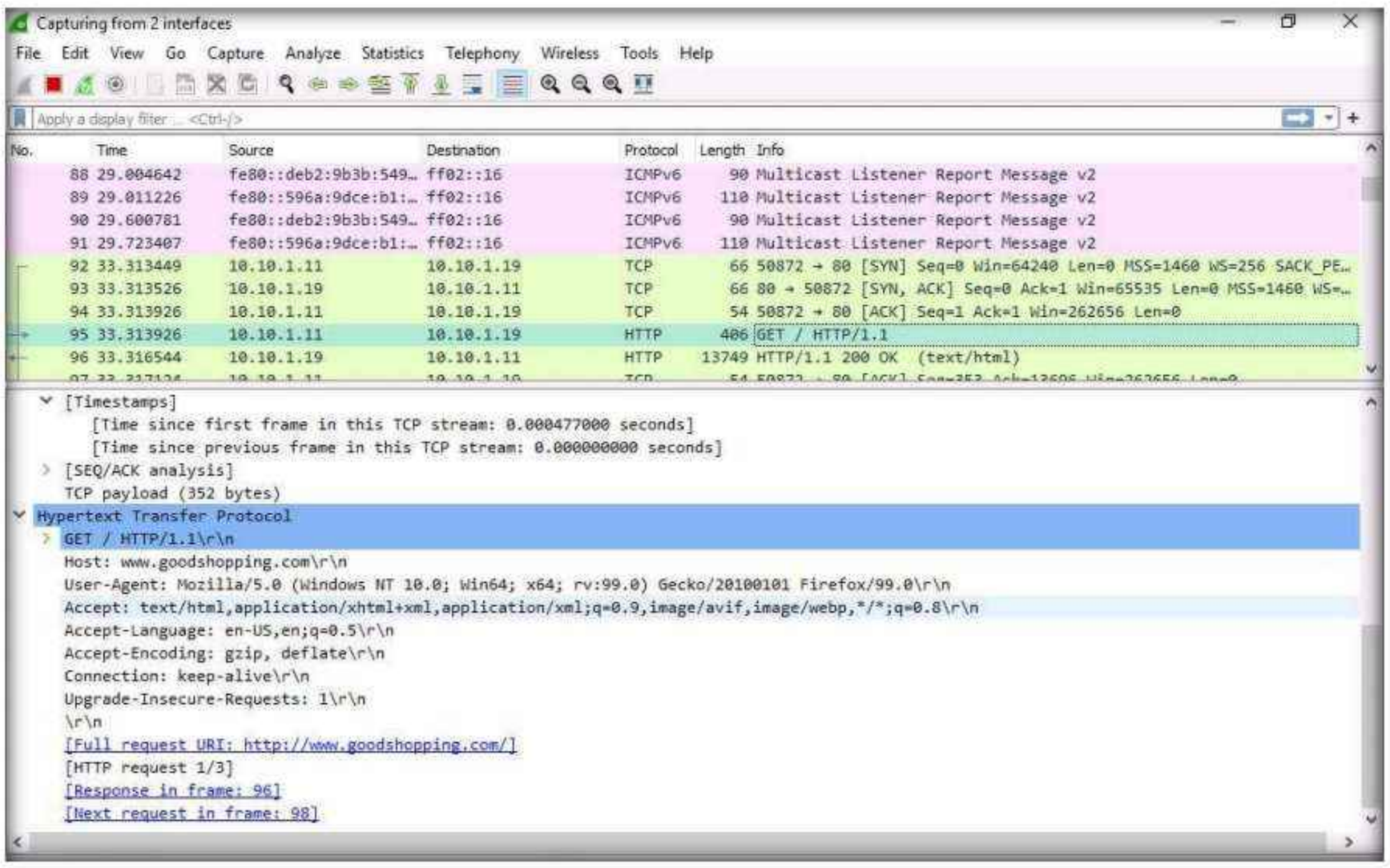


44. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **http://www.goodshopping.com**).

Note: Although we are only browsing the Internet here, you could also log in to your account and sniff the credentials.



45. Switch back to the **Windows Server 2019** virtual machine. **Wireshark** starts capturing packets as soon as the user (here, you) begins browsing the Internet, the shown in the screenshot.



46. After a while, click the **Stop capturing packet** icon on the toolbar to stop live packet capture.
47. This way, you can use Wireshark to capture traffic on a remote interface.

    Note: In real-time, when attackers gain the credentials of a victim's machine, they attempt to capture its remote interface and monitor the traffic its user browses to reveal confidential user information.
48. This concludes the demonstration of how to perform password sniffing using Wireshark.
49. Close all open windows and document all the acquired information.

Task 2: Analyze a Network using the Omnipeek Network Protocol Analyzer

OmniPeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. It performs analysis, drills down, and fixes performance bottlenecks across multiple network segments. It includes analytic plug-ins that provide targeted visualization and search abilities.

An ethical hacker or pen tester can use this tool to monitor and analyze network traffic of the target network in real-time, identify the source location of that traffic, and attempt to obtain sensitive information as well as find any network loopholes.

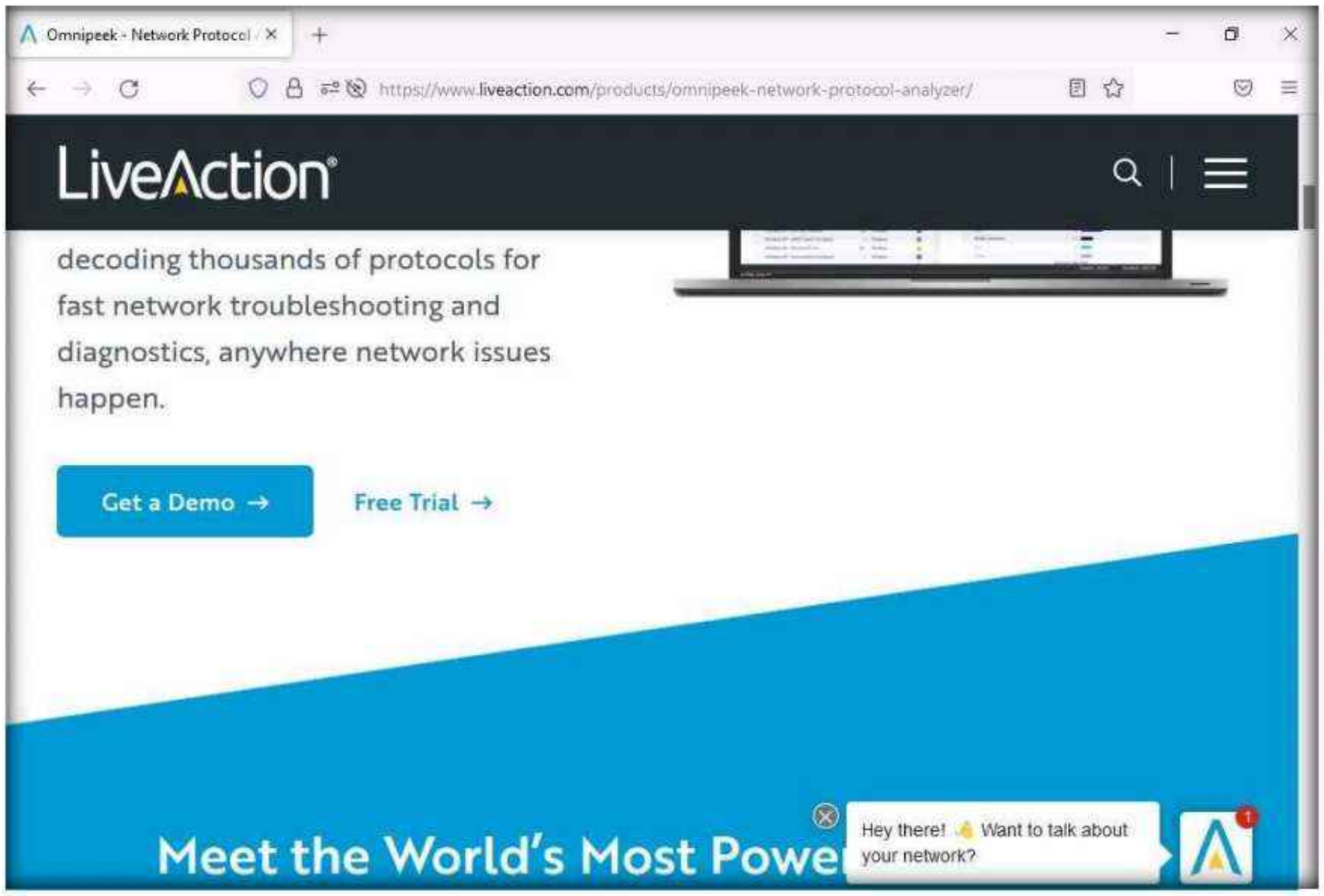
Note: Before starting this lab, we need to find the User IDs associated with the usernames for the **Windows 11** machine.

1. Switch to the **Windows 11** virtual machine.
2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/** in the address bar, and press **Enter**.

   Note: If a website cookie notification appears, click **Accept**.
3. The **LiveAction** website appears; click the **Free Trial** button.

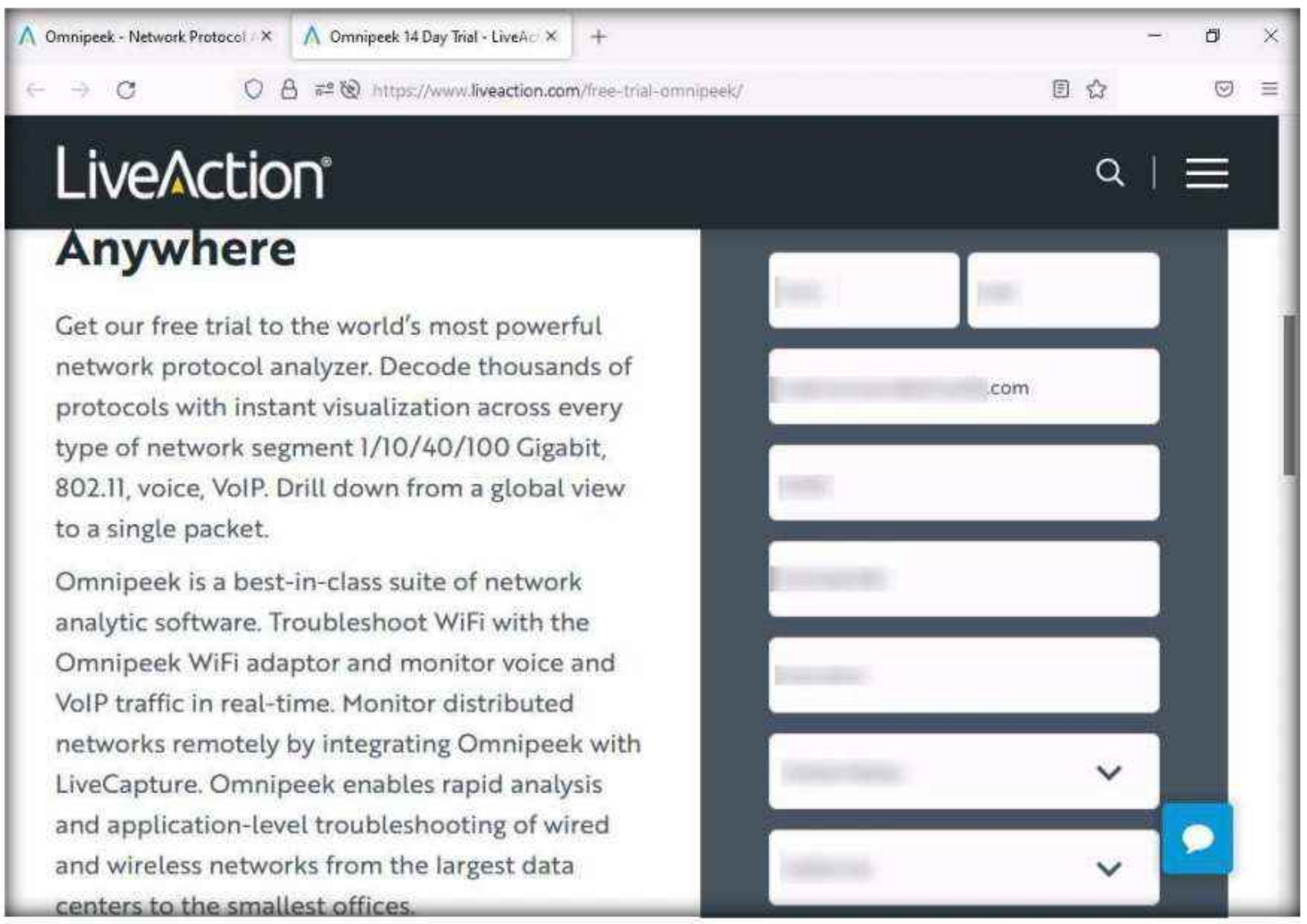
   Note: If **Warning: Potential Security Risk Ahead** page appears, click **Advanced**, and click **Accept the Risk and Continue**.

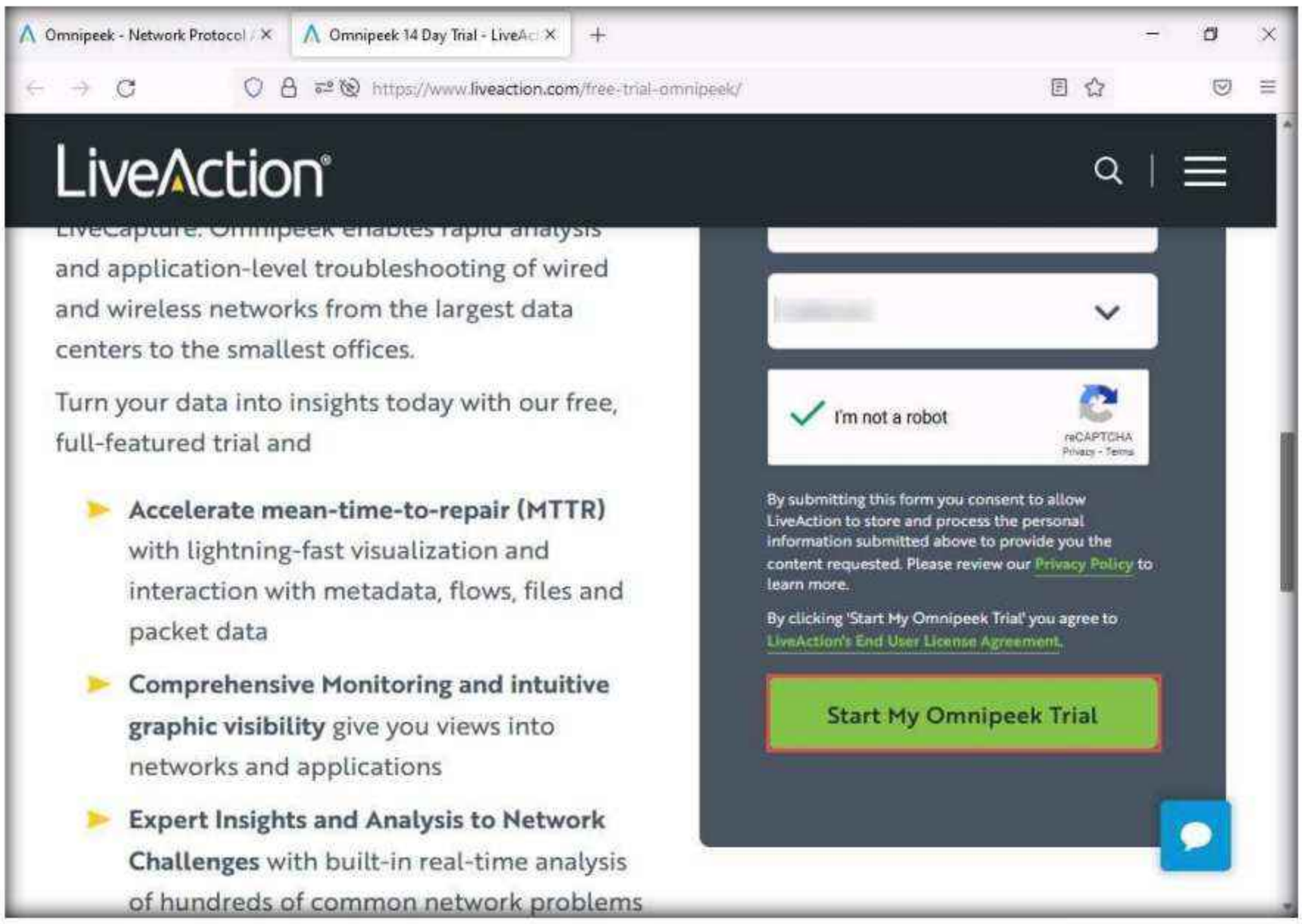
   Note: You will be redirected to a cart in live action, click checkout.



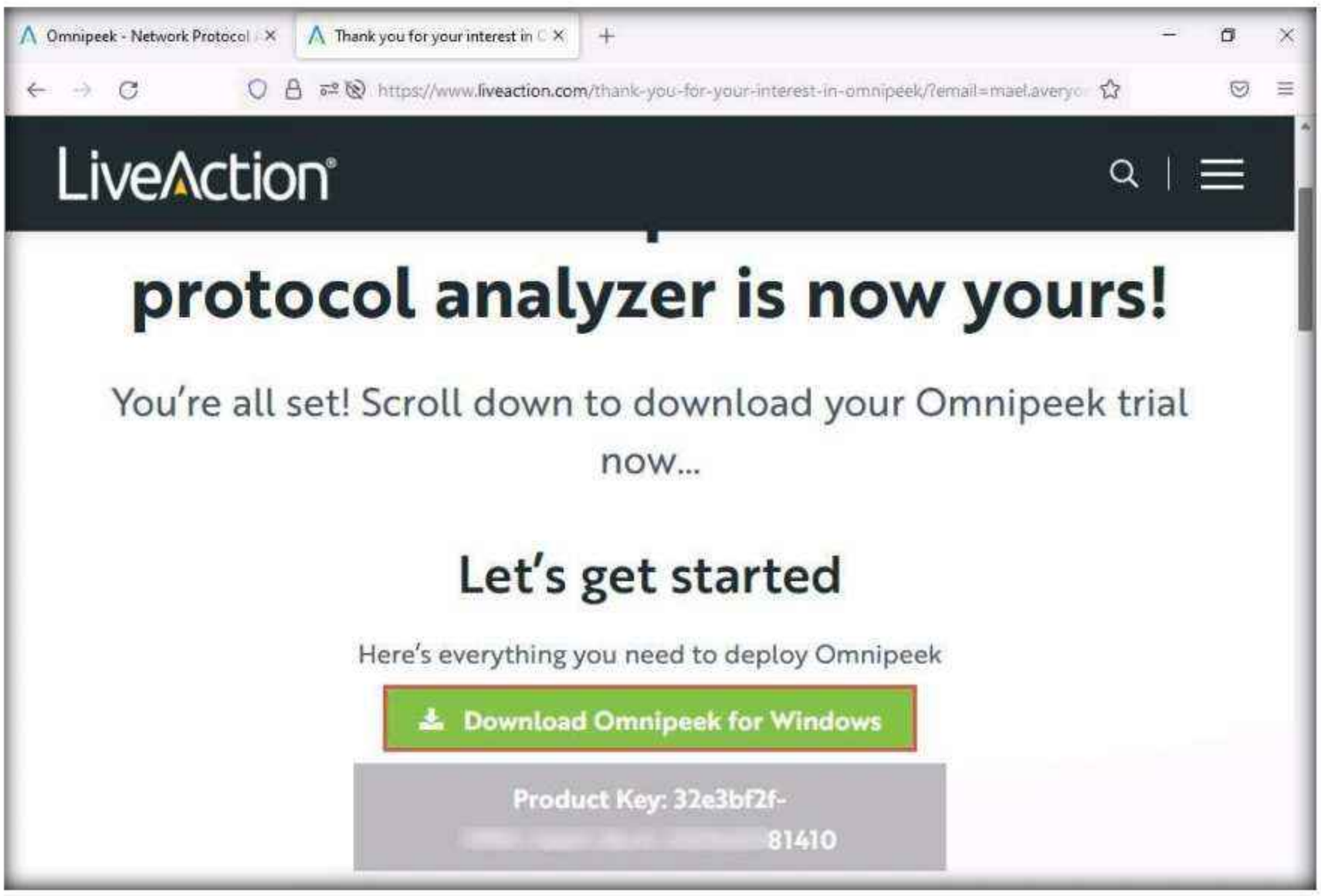
4. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **Start My Omnipeek Trial** button.

   Note: Here, you must provide your professional **EMAIL ADDRESS** (work or school accounts).





5. The **Let's get started** webpage appears, displaying the License Key and download link for Omnipeek. Click on the **Download Omnipeek for Windows** button to begin the download.

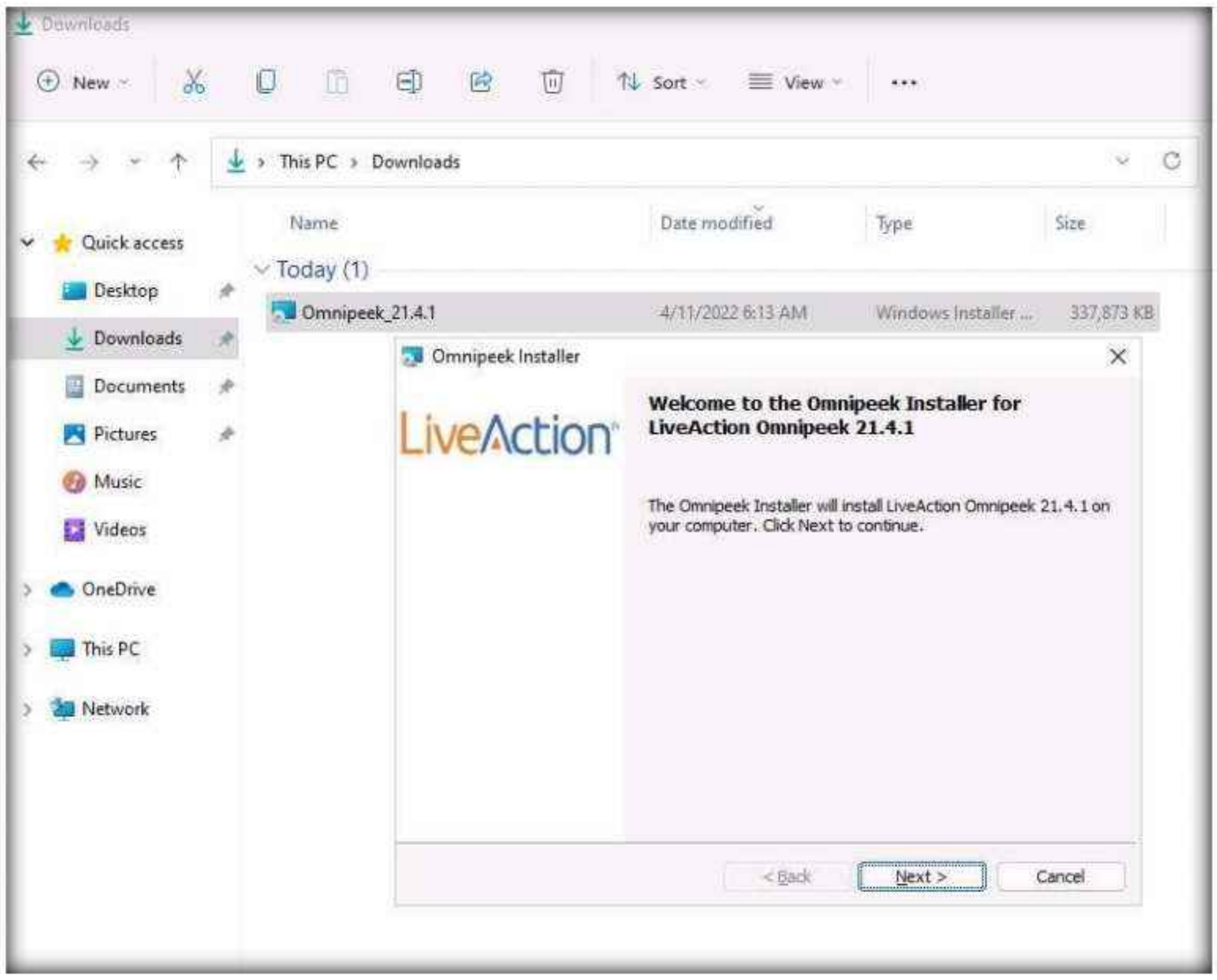


Note: If **Opening Omnipeek_21.4.1msi** pop-up appears; click **Save File** to download the application.

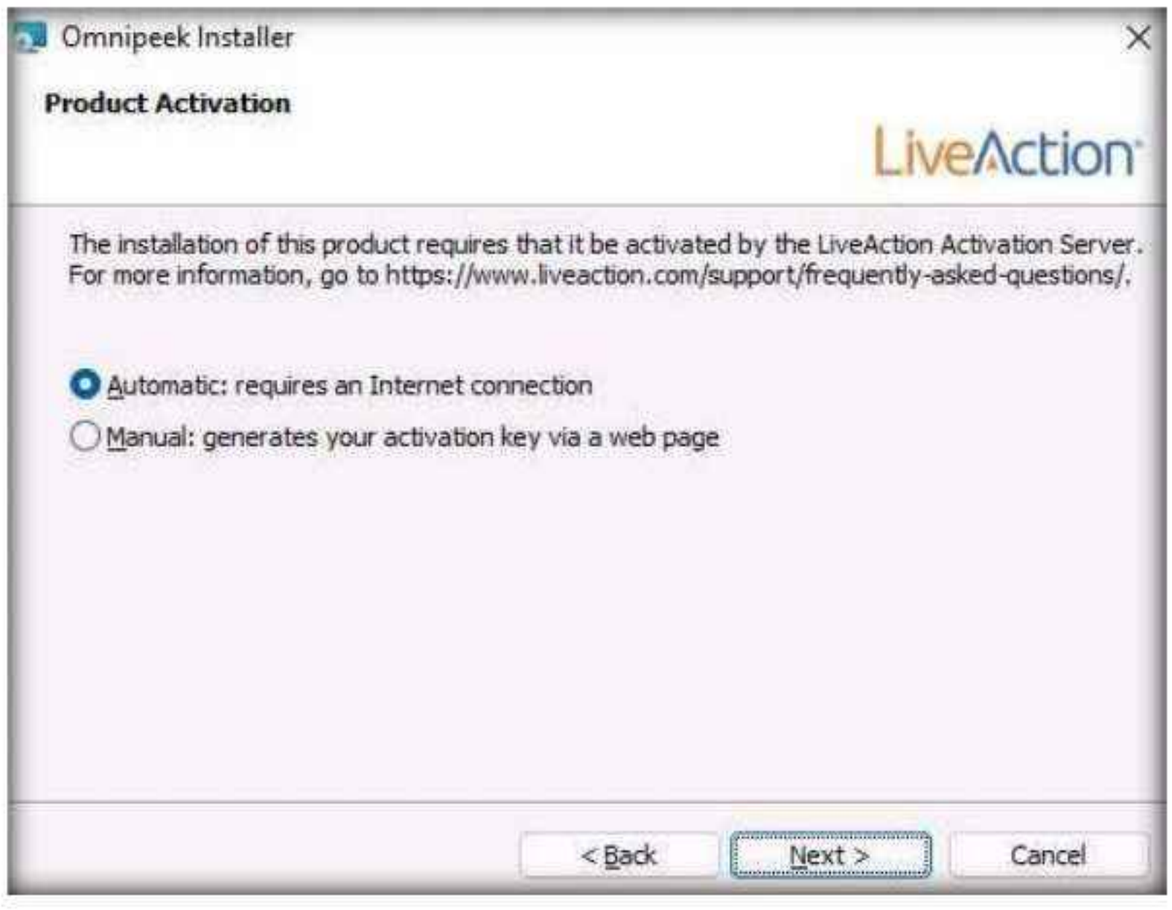
6. On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek_21.4.1msi**.

   Note: The version of **Omnipeek** might differ when you perform the task.

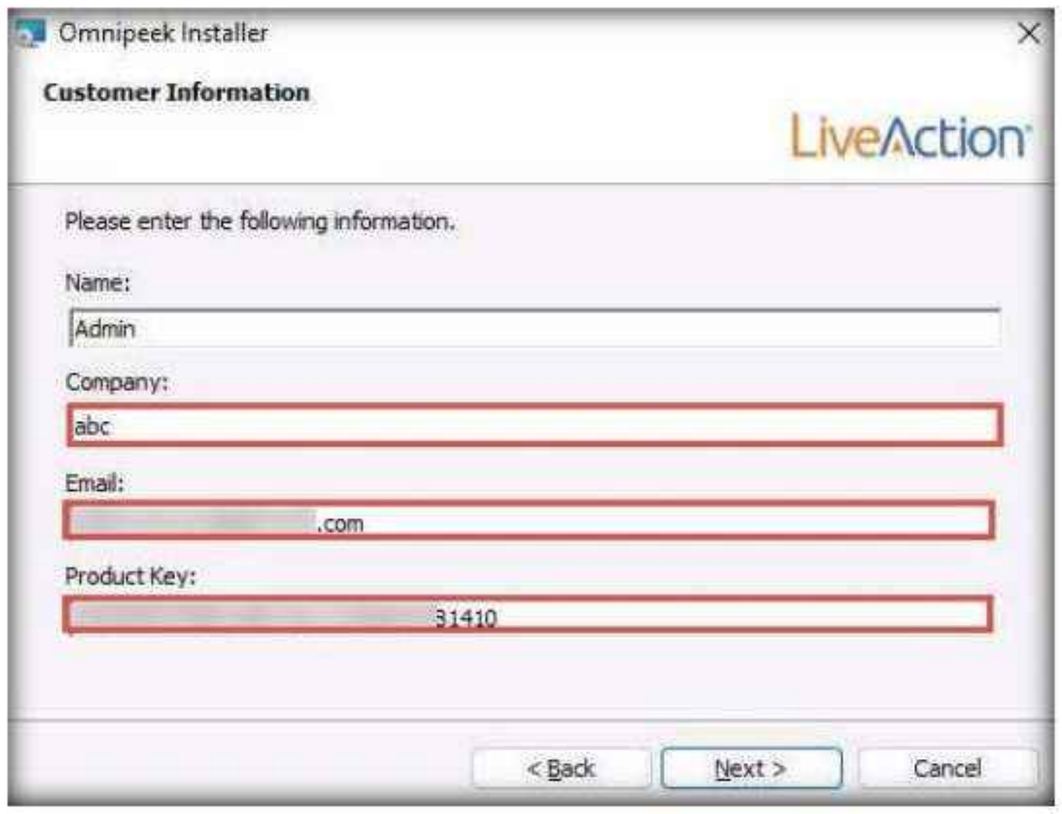
7. If an **Open File - Security Warning** pop-up appears, click **Run**.
8. The **OmniPeek Installer** wizard appears; click **Next**.



9. In the **Product Activation** wizard, ensure that the **Automatic**: **requires an Internet connection** radio-button is selected and click **Next**.



10. The **Customer Information** wizard appears; type a **Company Name** (here, **abc**) and **Email** (provided at the time of registration). For the serial number field, switch to the **Mozilla Firefox** browser and copy the **License Key**. Close the browser.
11. Switch back to the **Ompnipeek Installer** window, paste the **License Key** in the **Serial Number or Product Key** field, and then click **Next**.

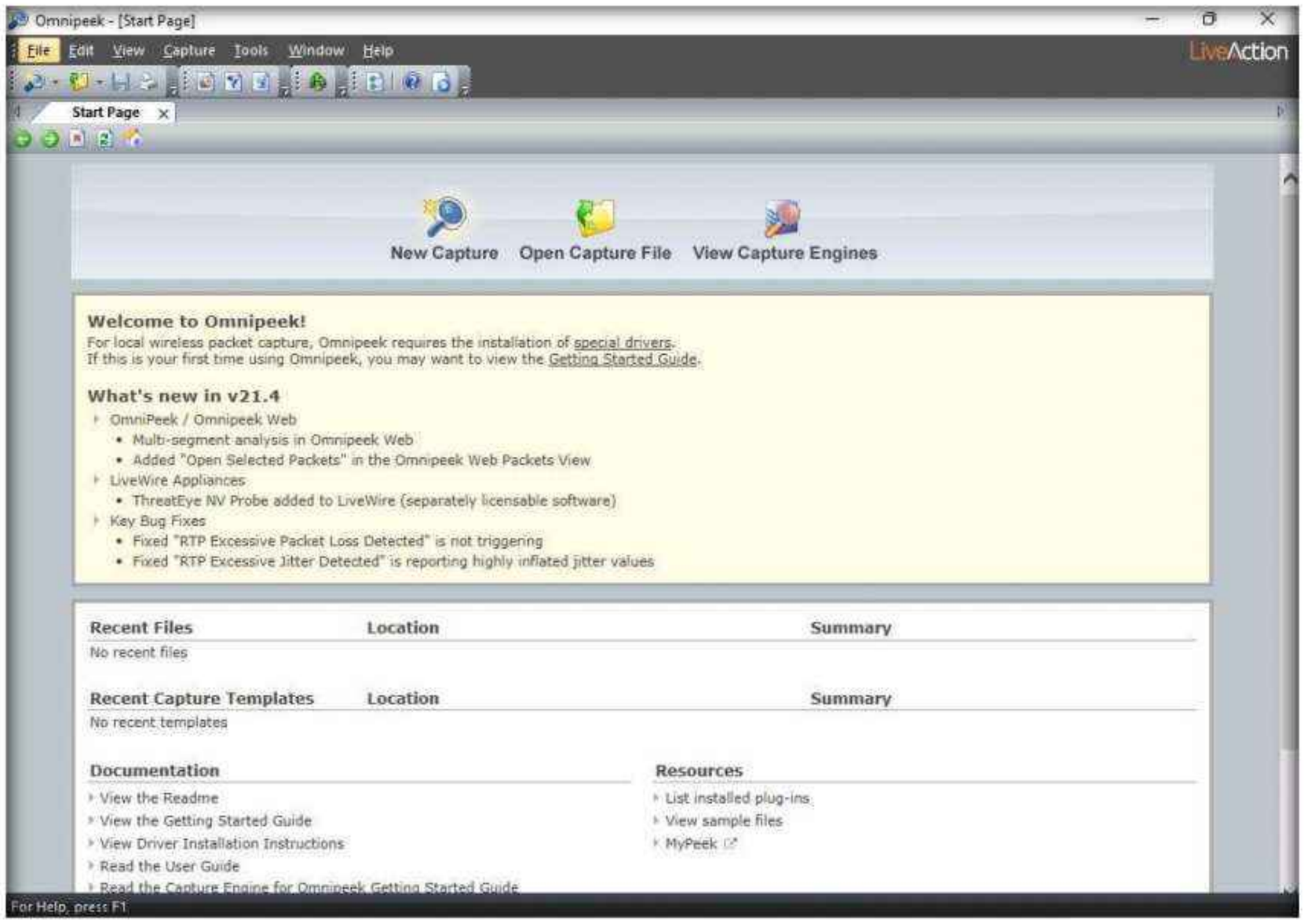


12. Follow the wizard-driven installation steps to install Omnipeek using the default settings.
13. While **Installing LiveAction Omnipeek**, if a **User Account Control** pop-up appears, click **Yes**.
14. On completion of the installation, the **Omnipeek Installer Completed** wizard appears; uncheck **View Readme**, ensure that the **Launch Omnipeek** option is checked, and click **Finish**.

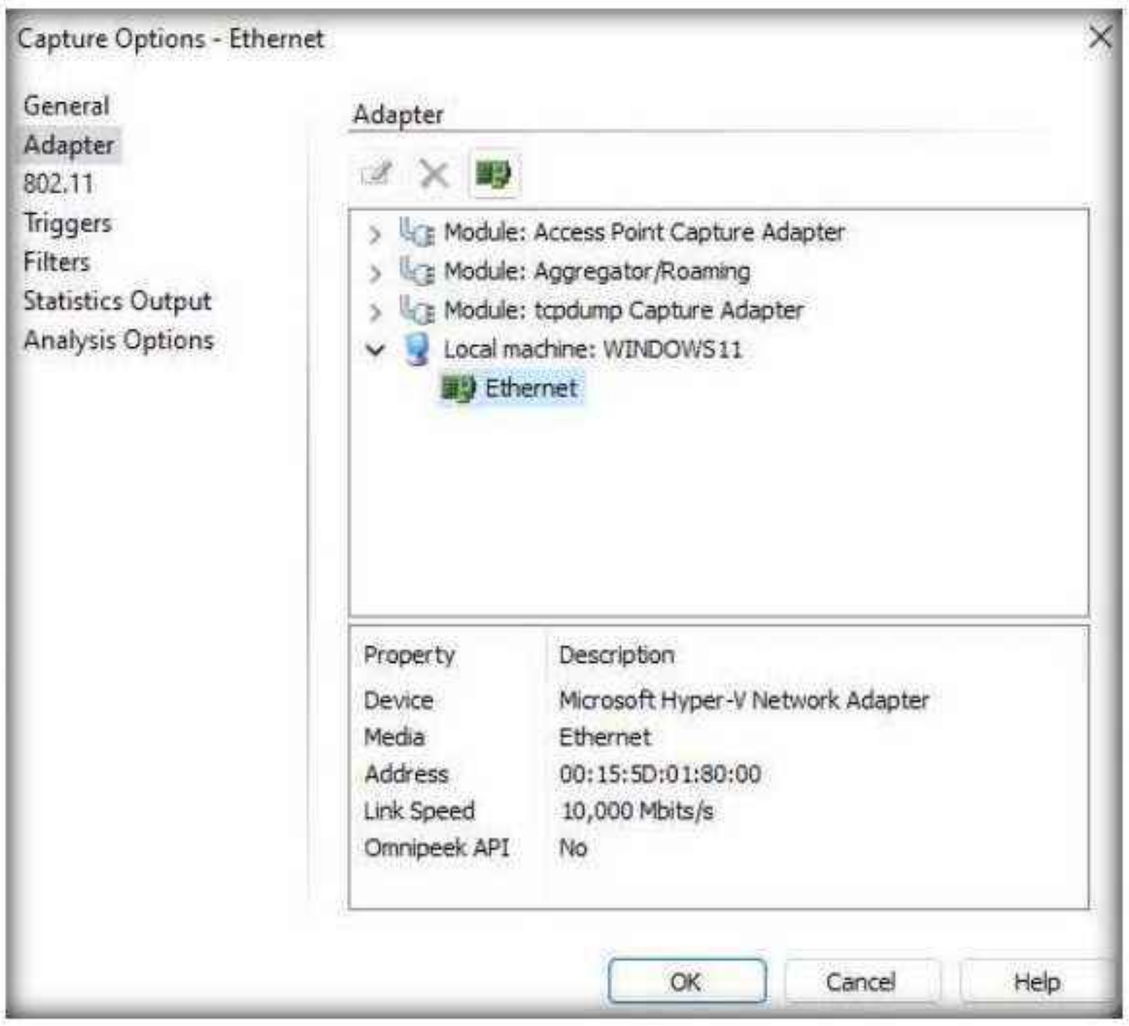
    Note: If a **User Account Control** pop-up appears, click **Yes**.

15. The **Omnipeek** evaluation dialog-box appears; click **OK**.

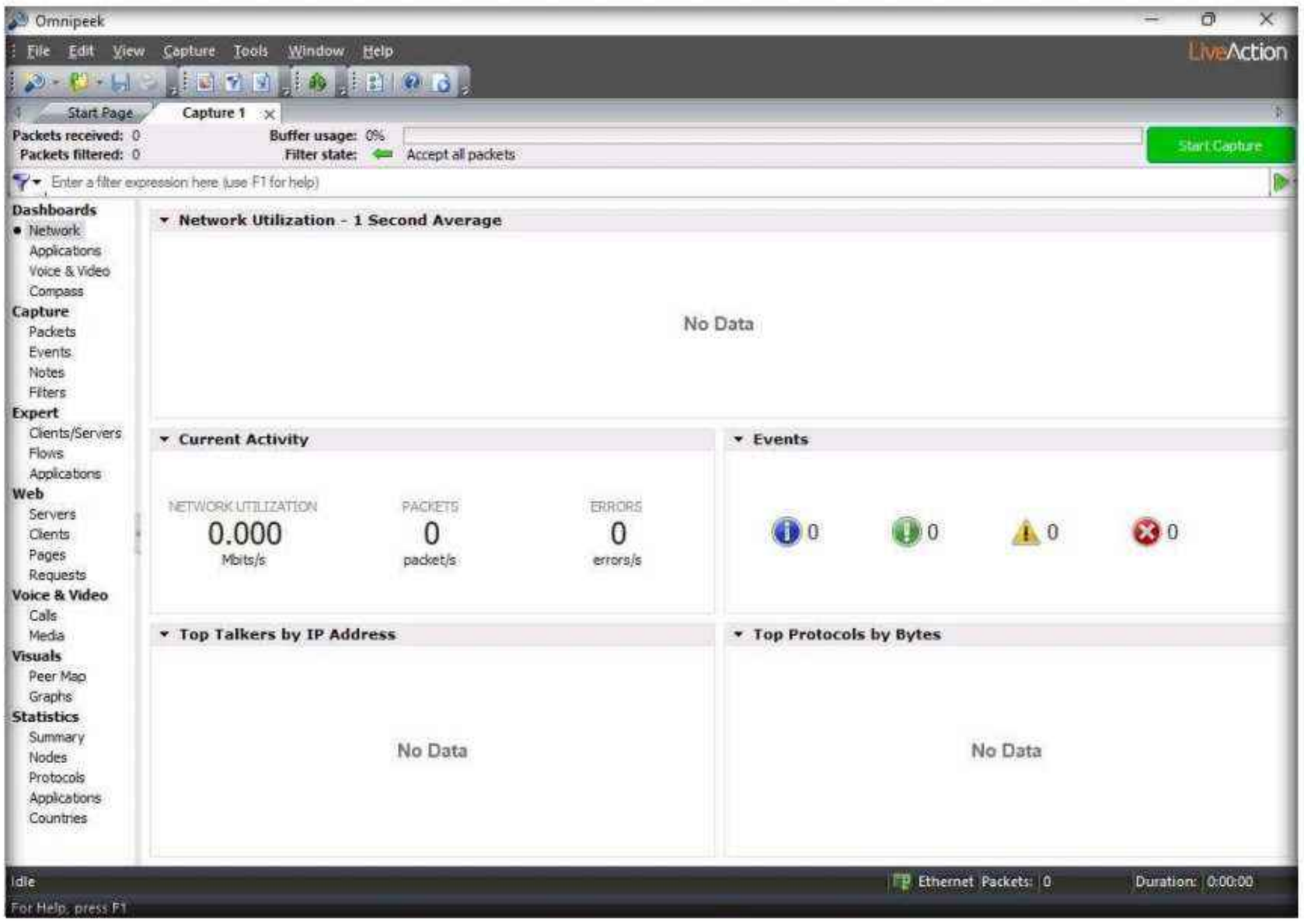
16. The **Omnipeek** main window appears, as shown in the screenshot.
17. Click on the **New Capture** option from the Omnipeek's main screen to create an Omnipeek capture window.



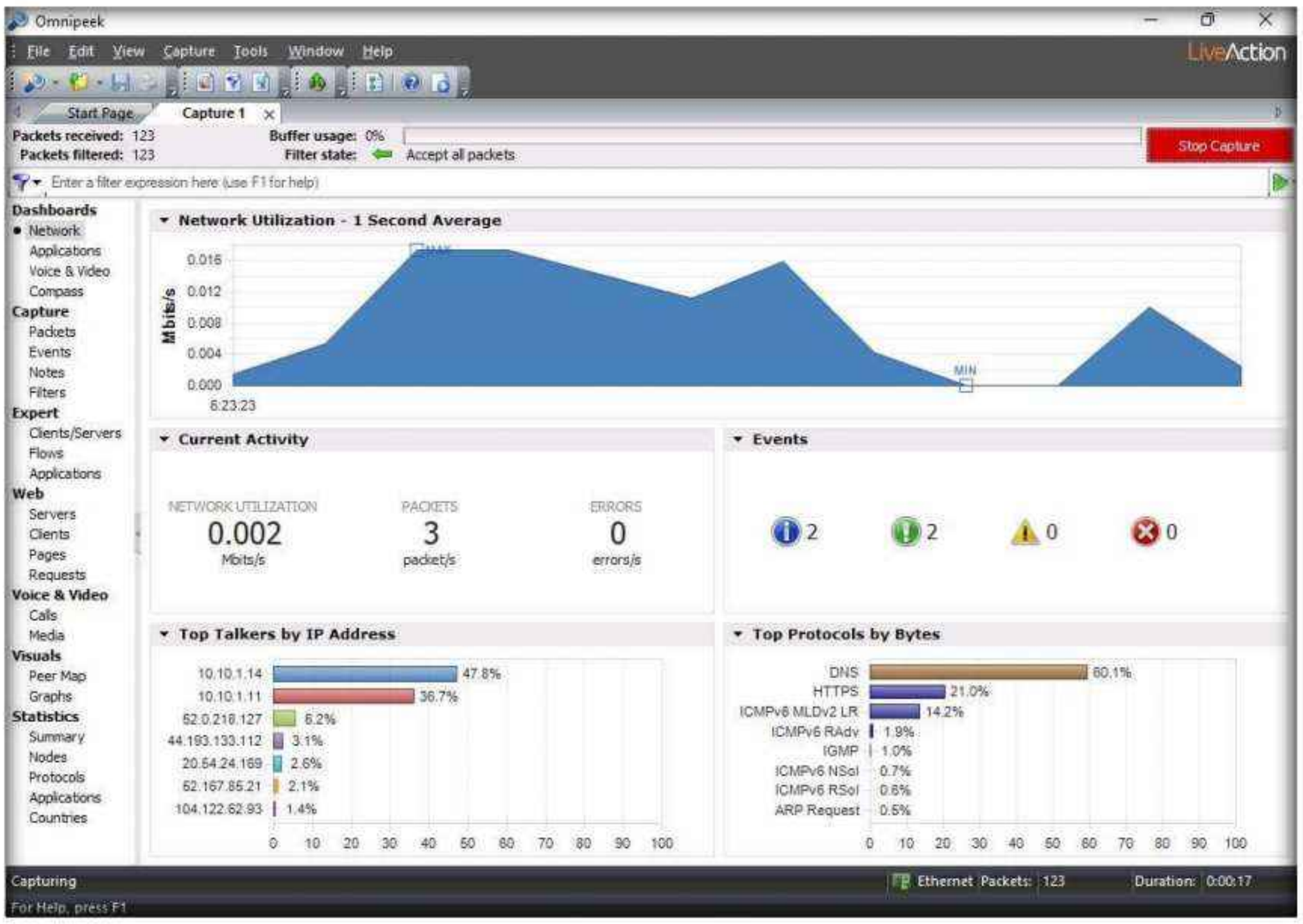
18. The **Capture Options** window appears; by default, the **Adapter** option opens-up.
19. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS11** node, select **Ethernet**, and click **OK**.



20. The **Capture 1** tab appears; click the **Start Capture** button in the right-hand corner of the window to begin capturing packets.

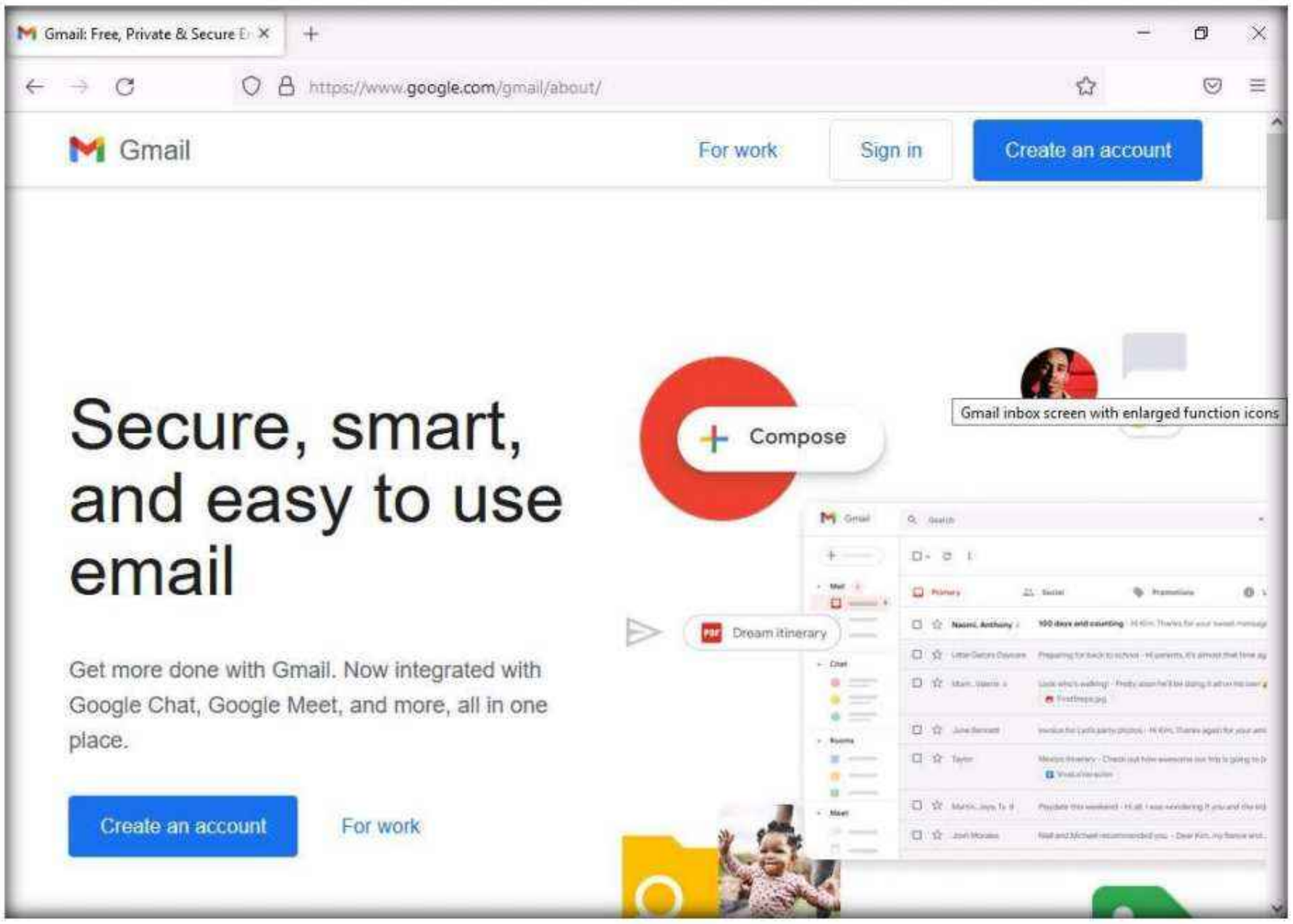


21. The **Start Capture** button changes to read "**Stop Capture**" and traffic statistics begin to populate **Network** under the **Dashboards** section, as shown in the screenshot.



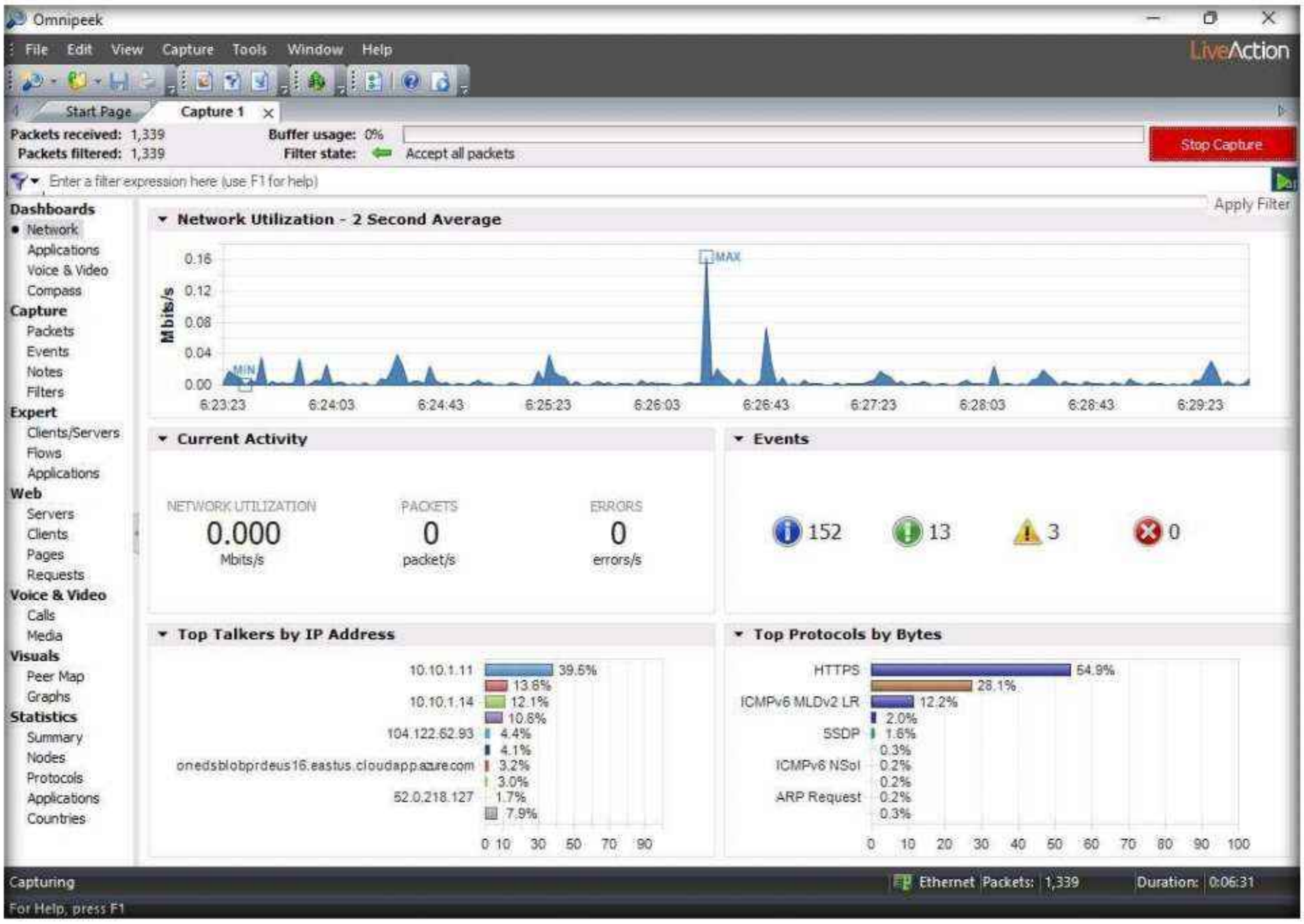
22. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **https://www.gmail.com**).

    Note: Social networking websites are blocked from this environment due to some security reasons. However, if you want to run this lab task you can use some other website of your choice or else you can run this task in your local environment.

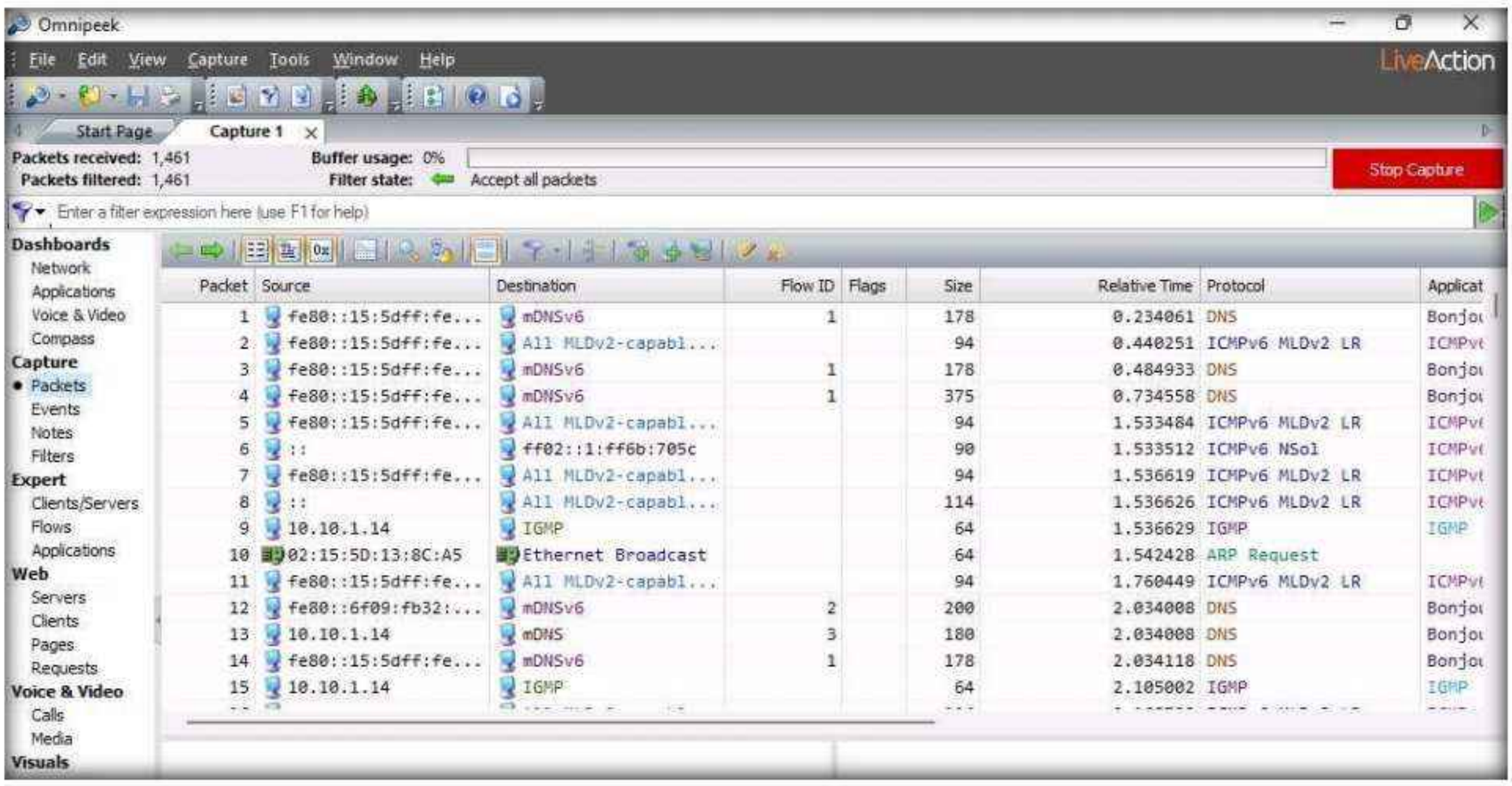


24. Now, switch back to the **Windows 11** virtual machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.

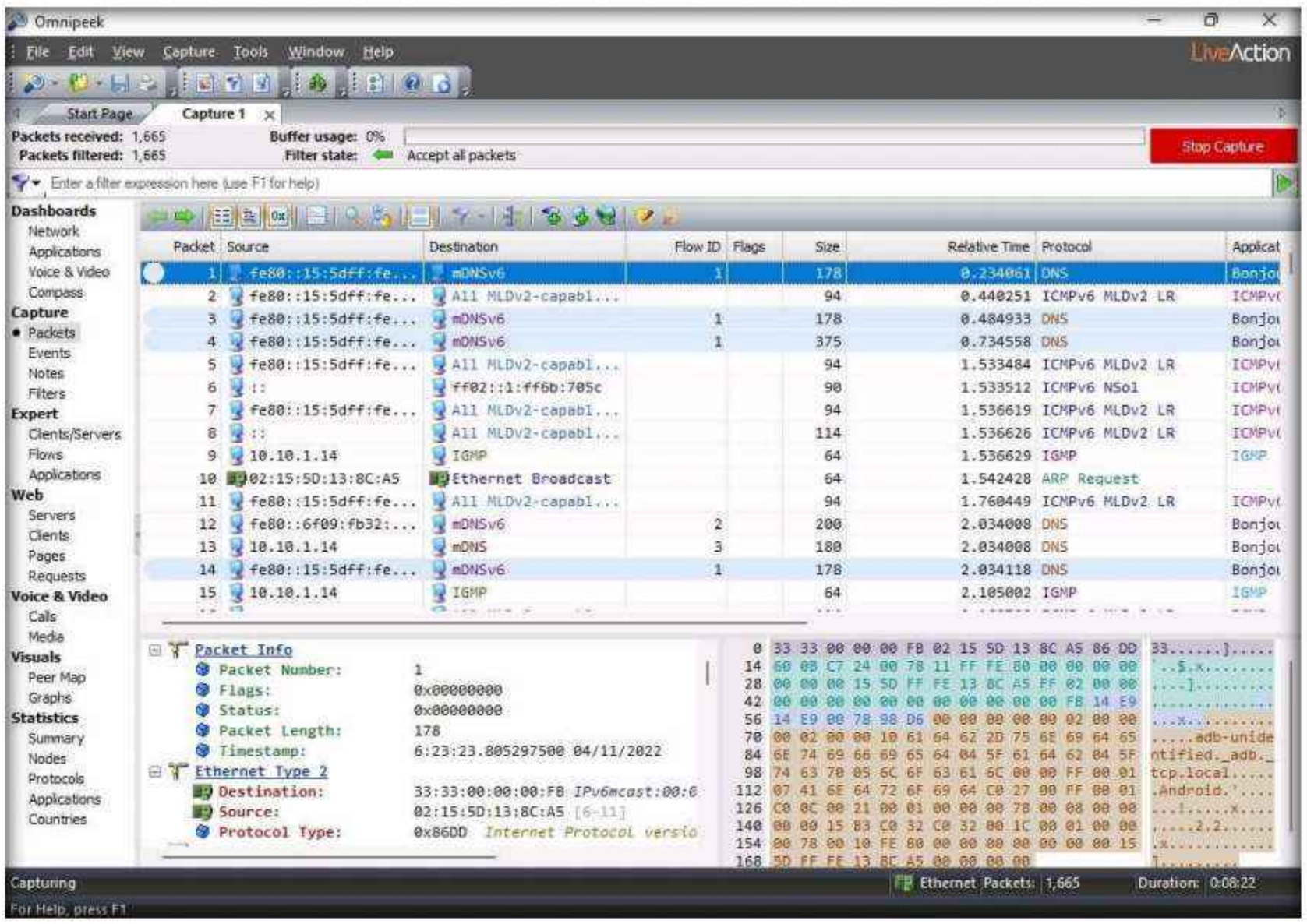
25. You can observe the network traffic along with the websites visited by the target machine.



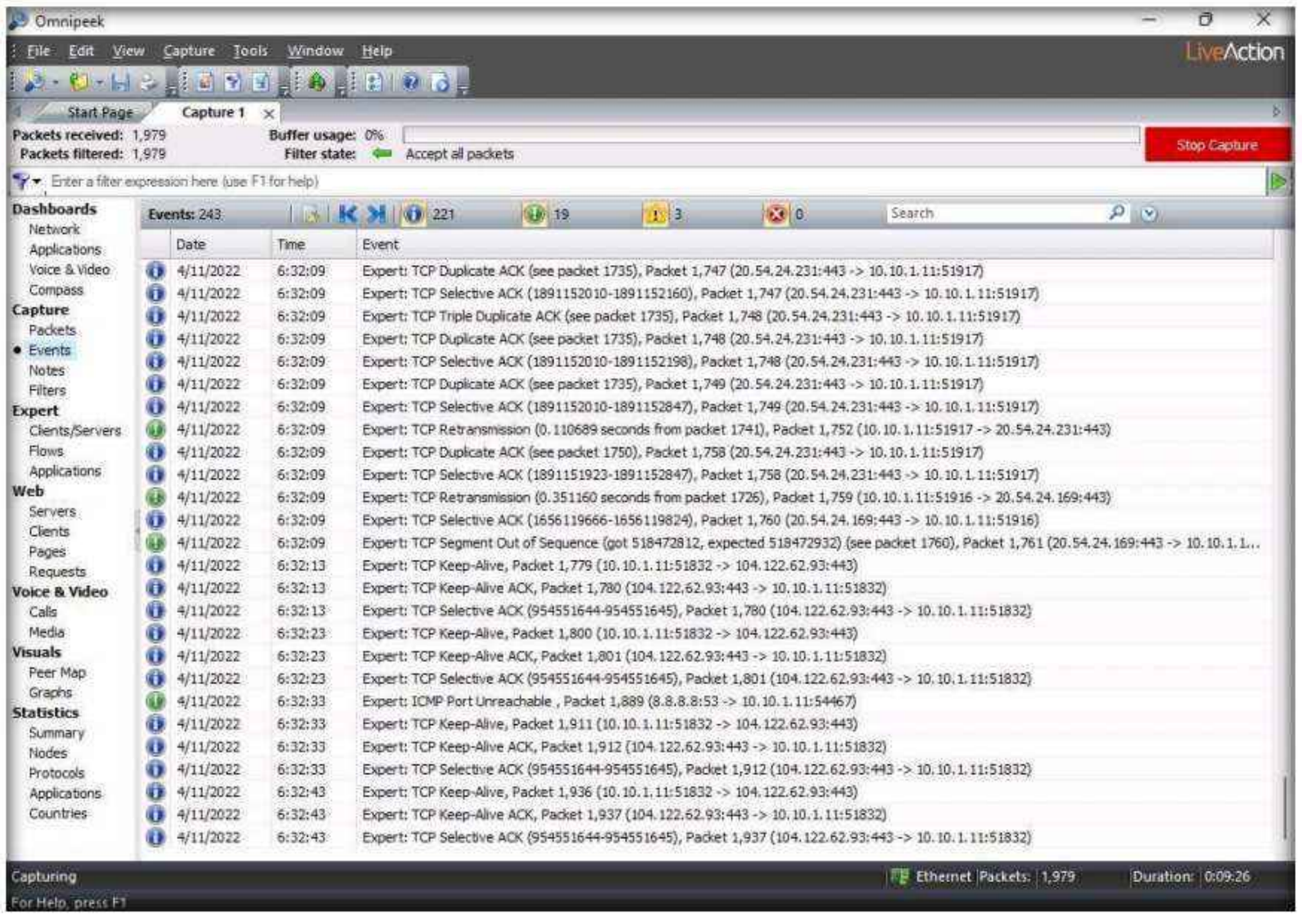
26. To view the captured packets, select **Packets** under the **Capture** section in the left-hand pane. You can observe the outgoing and incoming network packets of the target system.



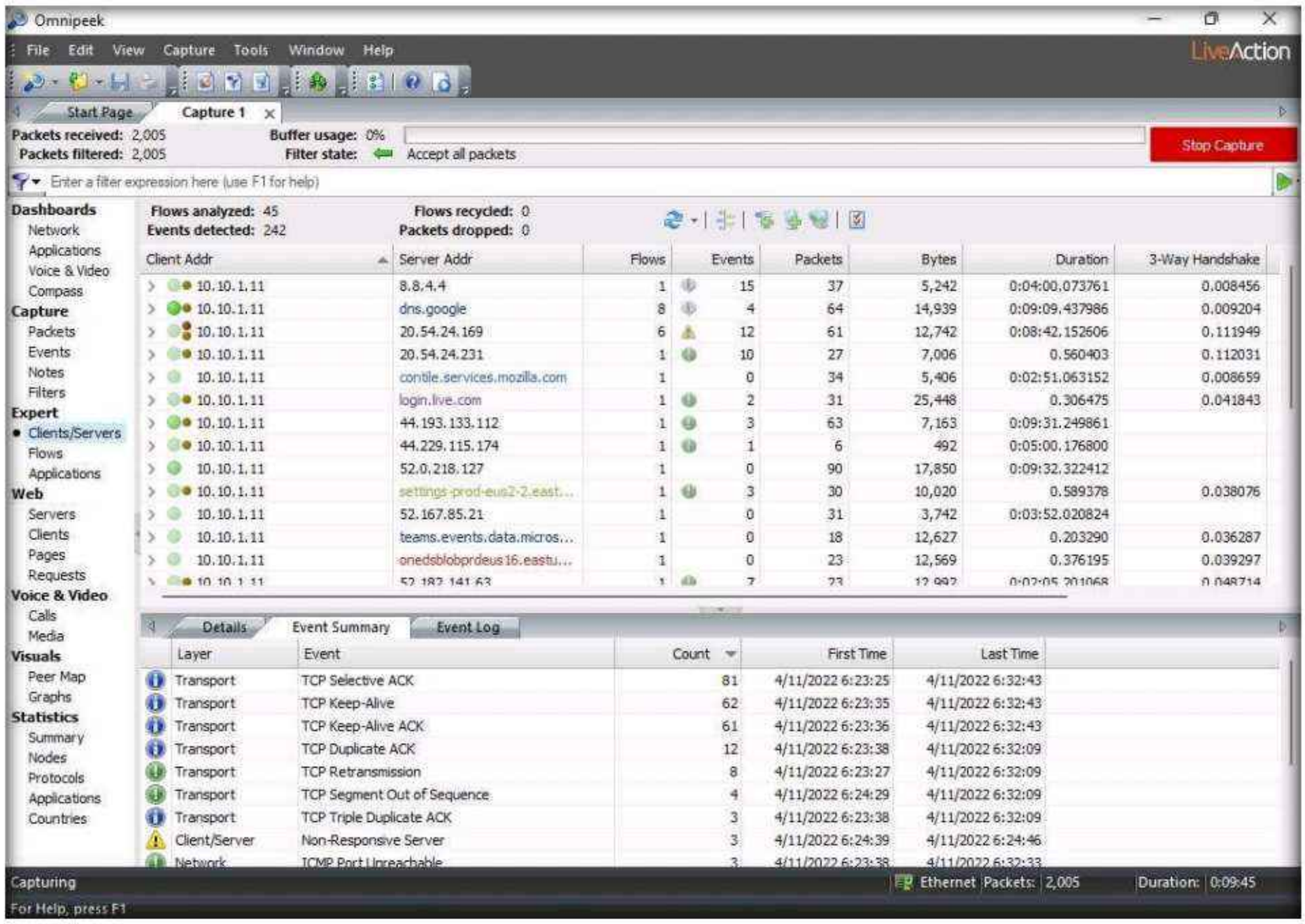
27. You can further click the **Show Decode View** and **Show Hex View** icons to view detailed information regarding any selected packet.



28. Click **Events** under the **Capture** section in the left-hand pane to view the events occurring in the network.



29. Click **Clients/Servers** under the **Expert** section in the left-hand pane to view a list of active systems in the local network.

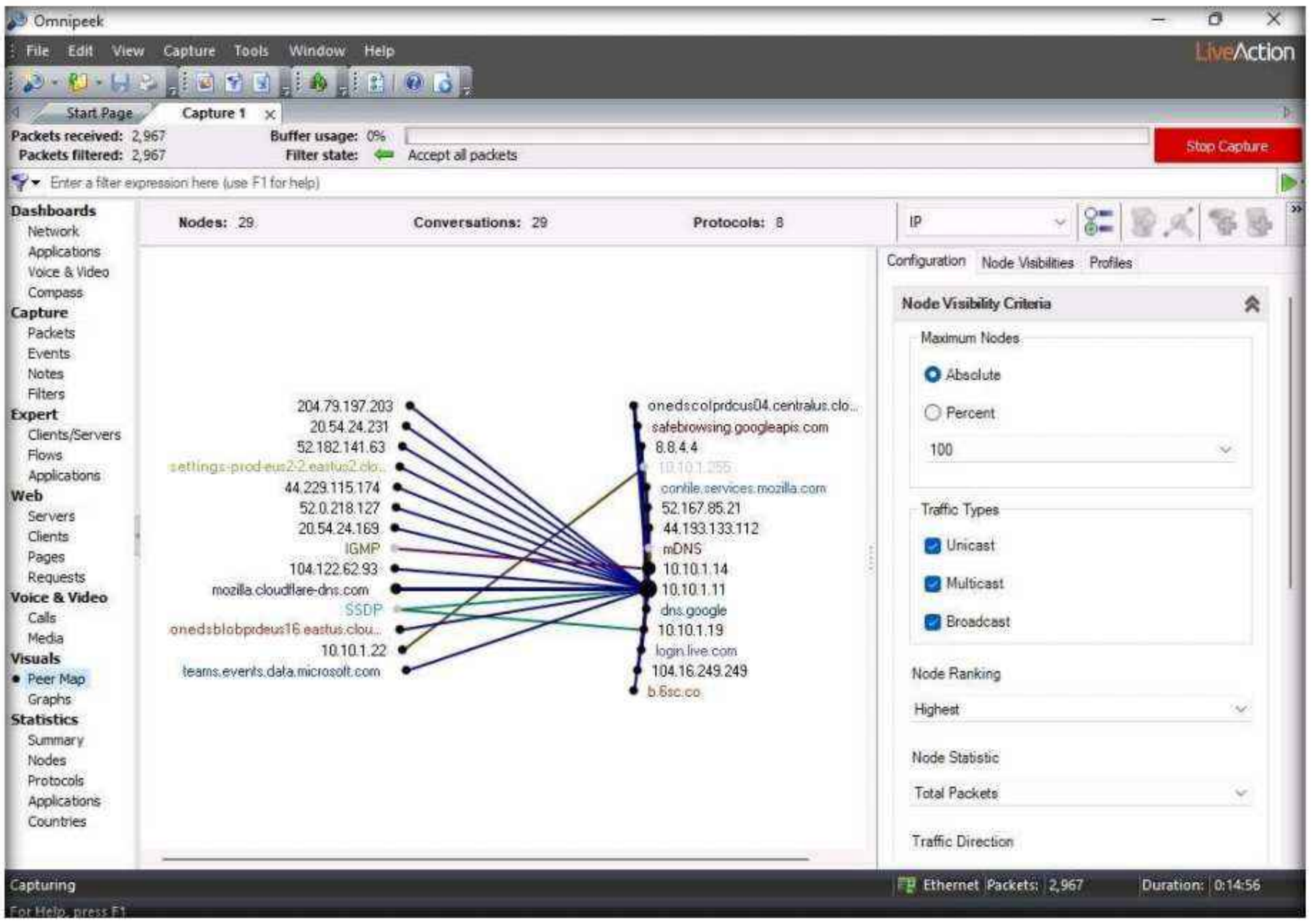


30. Similarly, under the **Flows** and **Applications** options, you can view the packet flow and applications running on the systems in the local network.

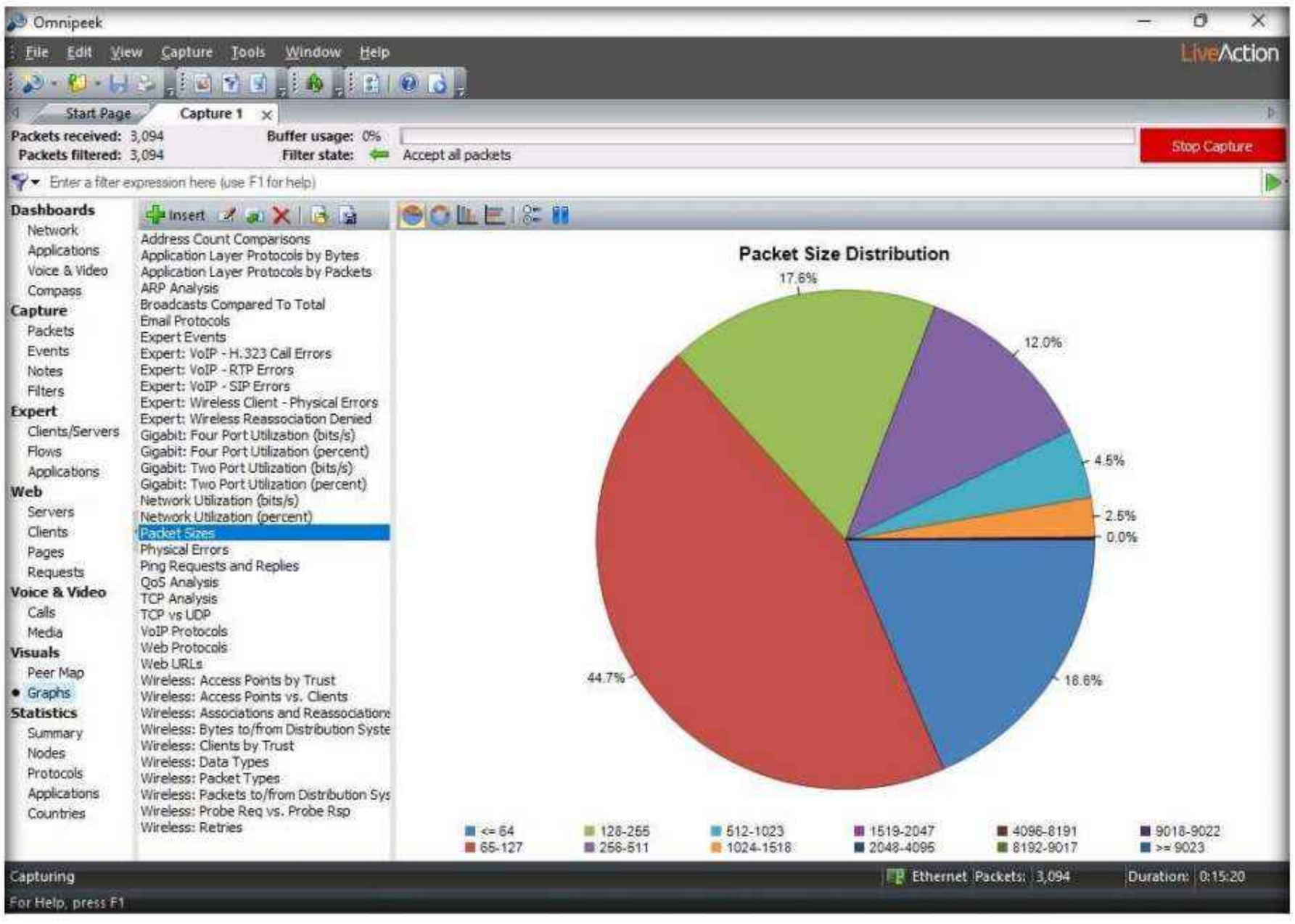
31. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.

32. Click **Peer Map** under the **Visuals** section in the left-hand pane to show a mapped view of the network traffic. By default, all **Traffic Types** (**Unicast**, **Multicast**, and **Broadcast**) are selected.

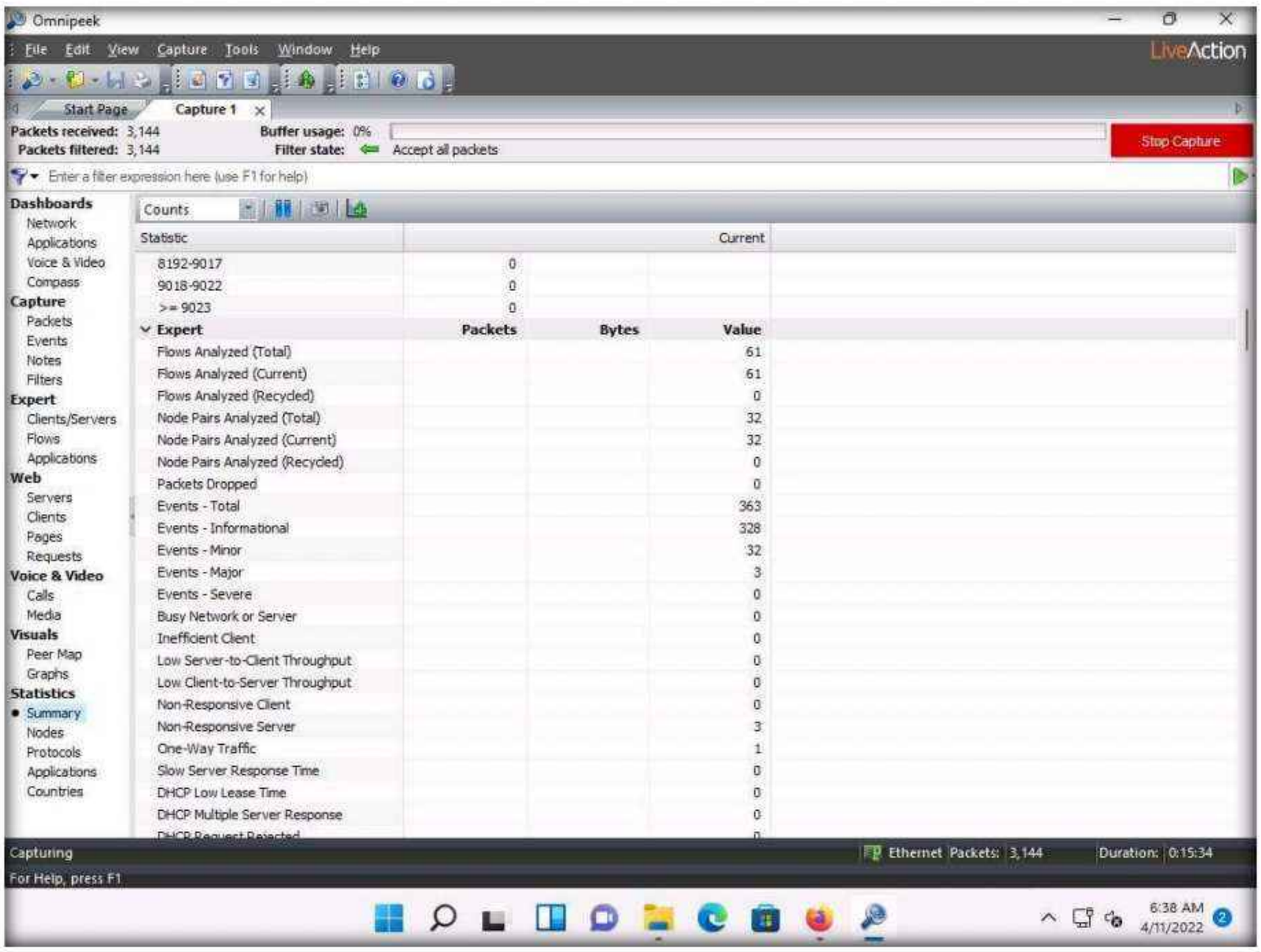
Note: You can select any traffic according to your purpose.



33. Similarly, under the **Visuals** section, you can click the **Graphs** option to show graphs on packet size, QoS analysis, TCP analysis, TCP vs. UDP, and web protocols.

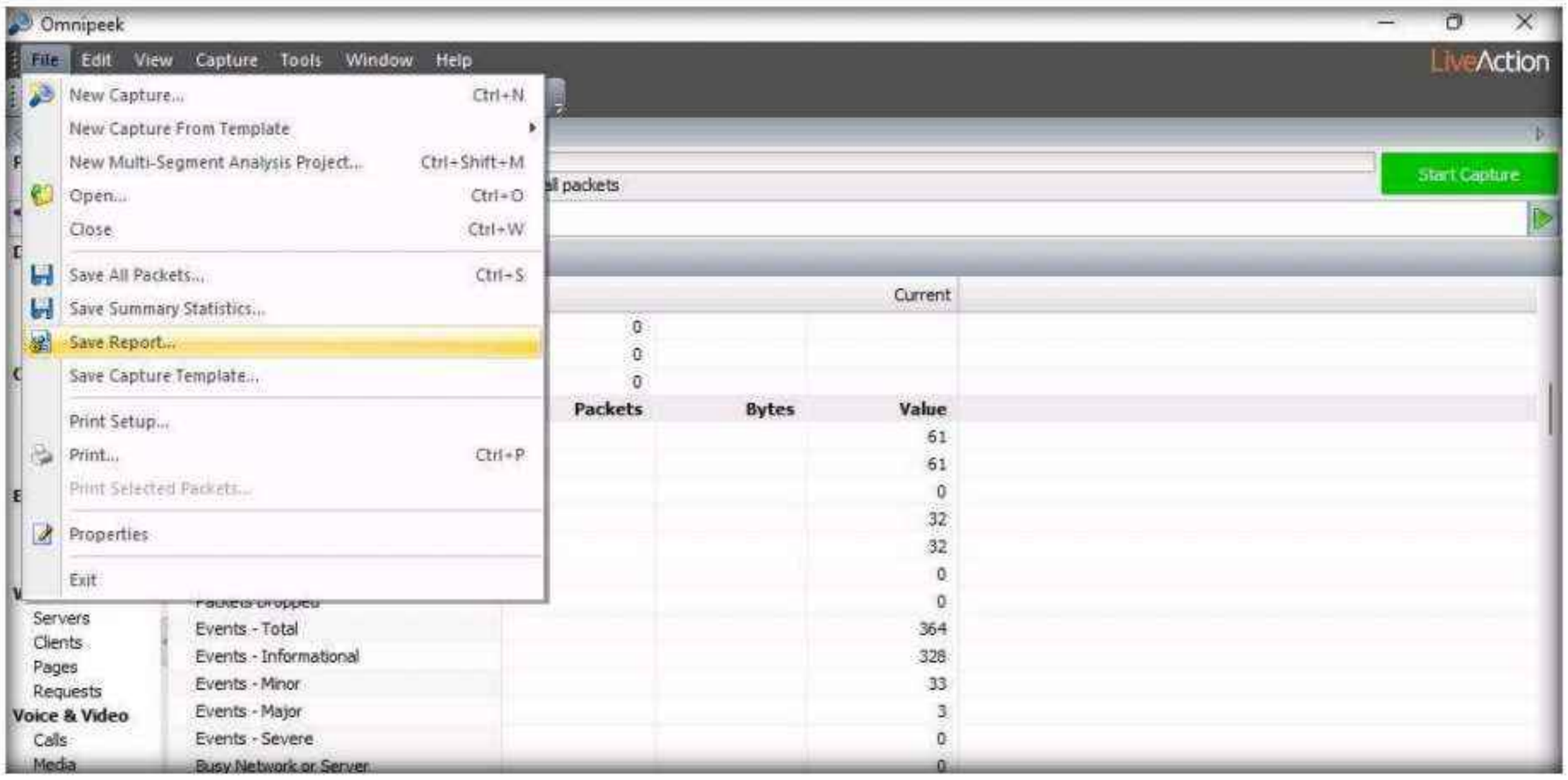


34. Click on the **Summary** option under the **Statistics** section in the left-hand pane to view a summary report of the network analysis.

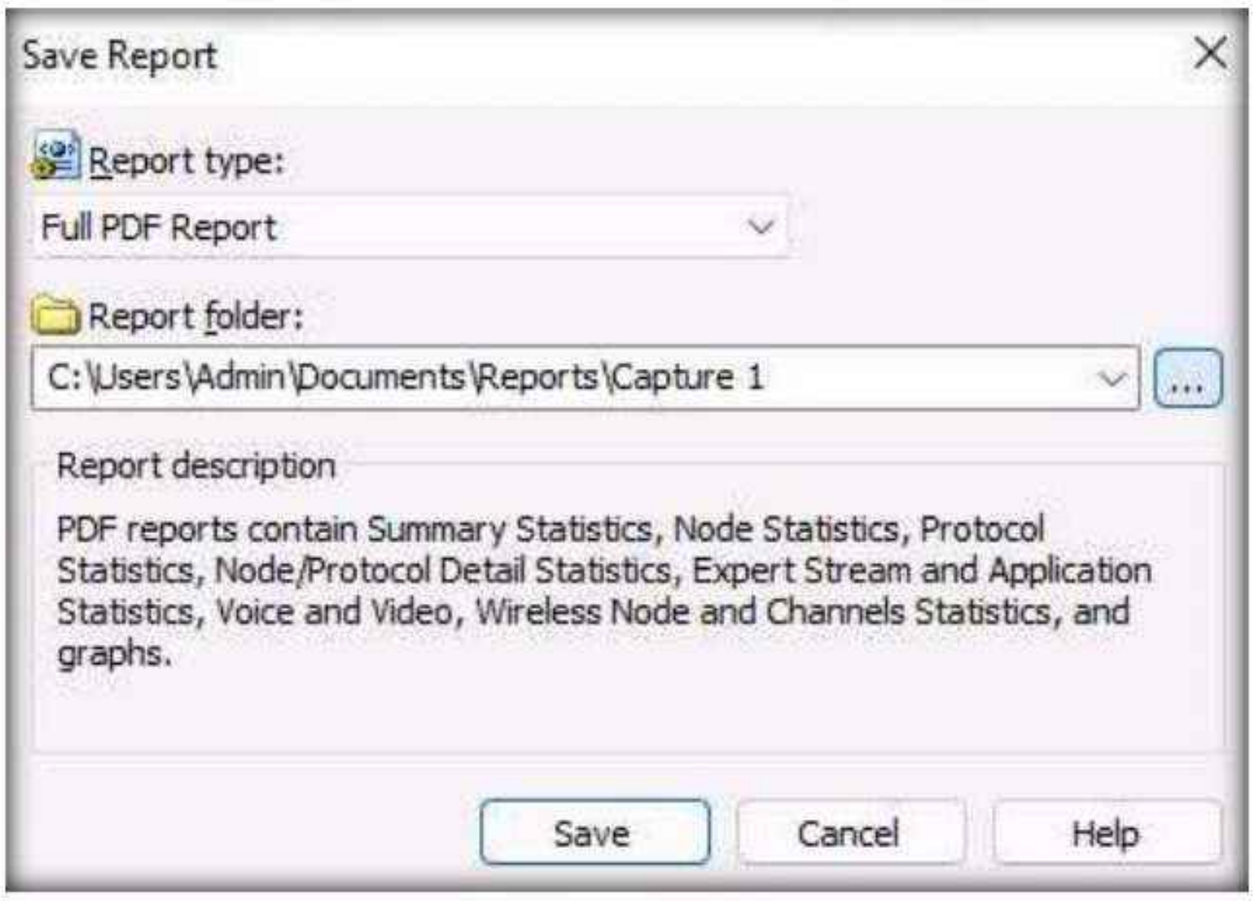


35. Stop the packet capturing by clicking on the **Stop Capture** button in the right-hand corner of the window. The **Stop Capture** button will toggle back to the **Start Capture** button.

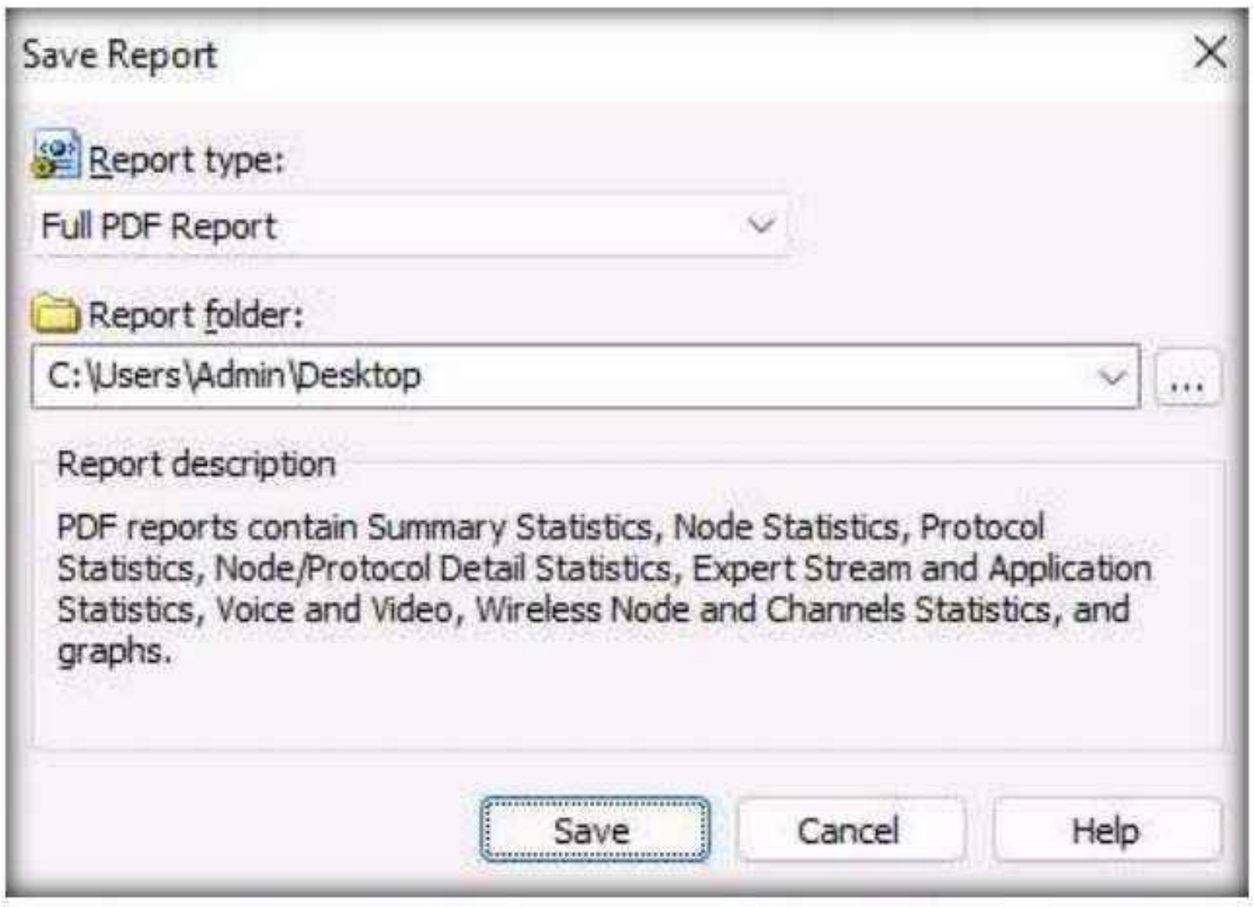
36. Click **File** from the menu bar and click **Save Report…** to save the report.



37. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon to change the download location.

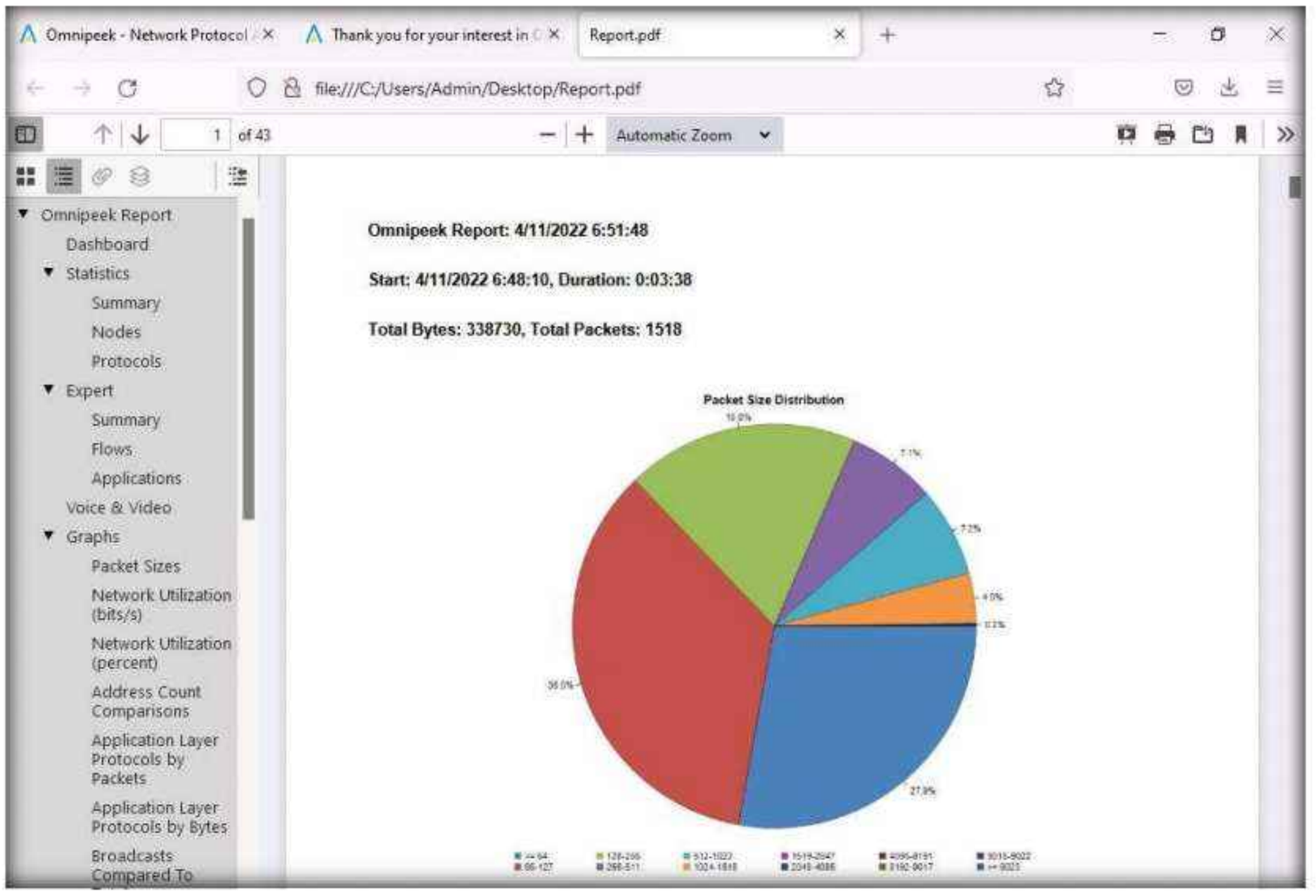


38. The **Browse For Folder** window appears; select the **Desktop** as your save location and click **OK**.
39. The changed save location appears in the **Report folder** field; click the **Save** button to save the report.

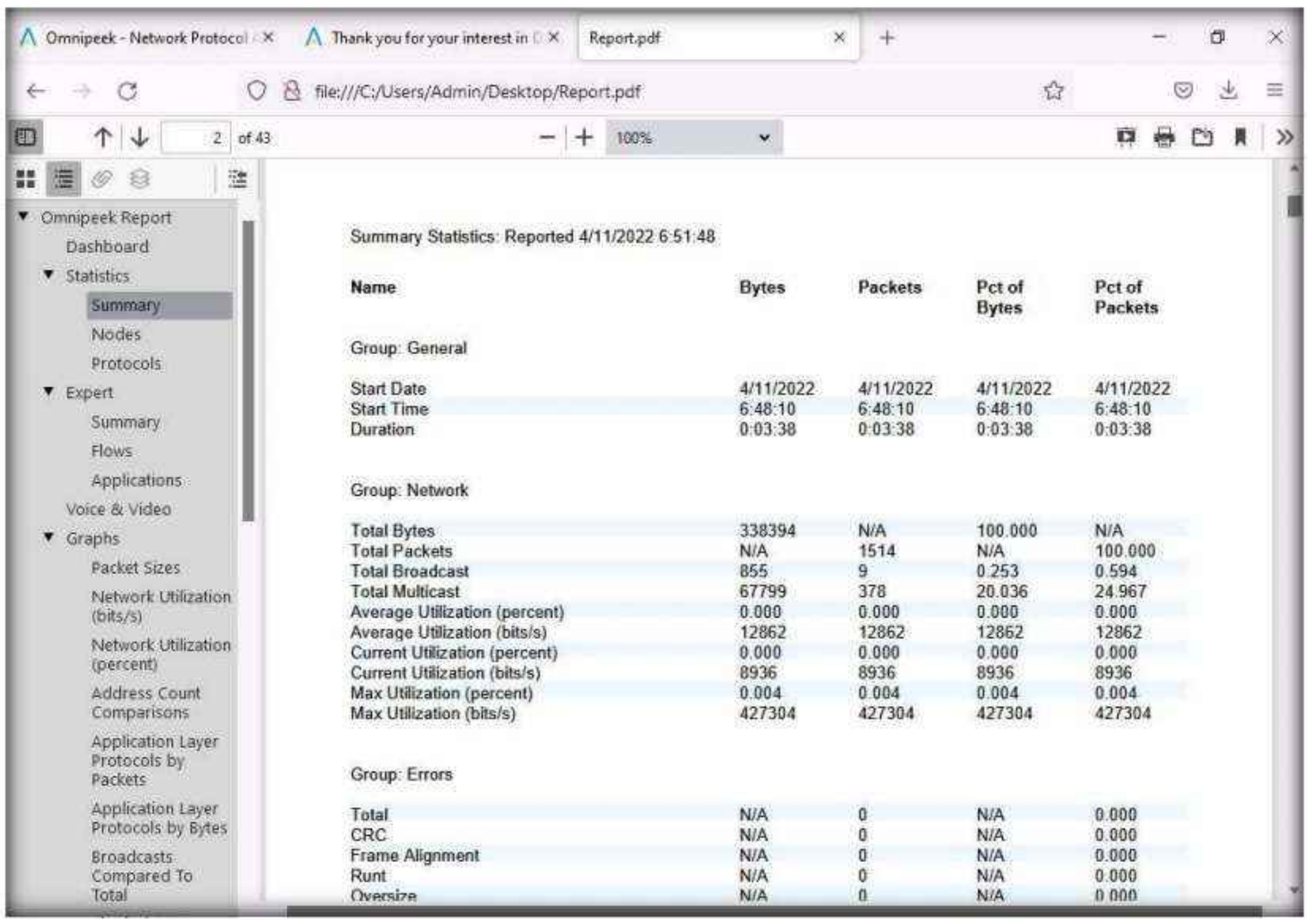


40. The saved report automatically appears, as shown in the screenshot.

    Note: If **How do you want to open this file?** pop-up appears, select **Firefox** and click on **OK**.



41. Scroll down the page in the pdf to view the complete report.



Note: In real-time, an attacker may perform this analysis to obtain sensitive information as well as to find any loopholes in the network.

42. This concludes the demonstration of analyzing a network using the Omnipeek Network Protocol Analyzer.

43. Close all open windows and document all the acquired information.

Task 3: Analyze a Network using the SteelCentral Packet Analyzer

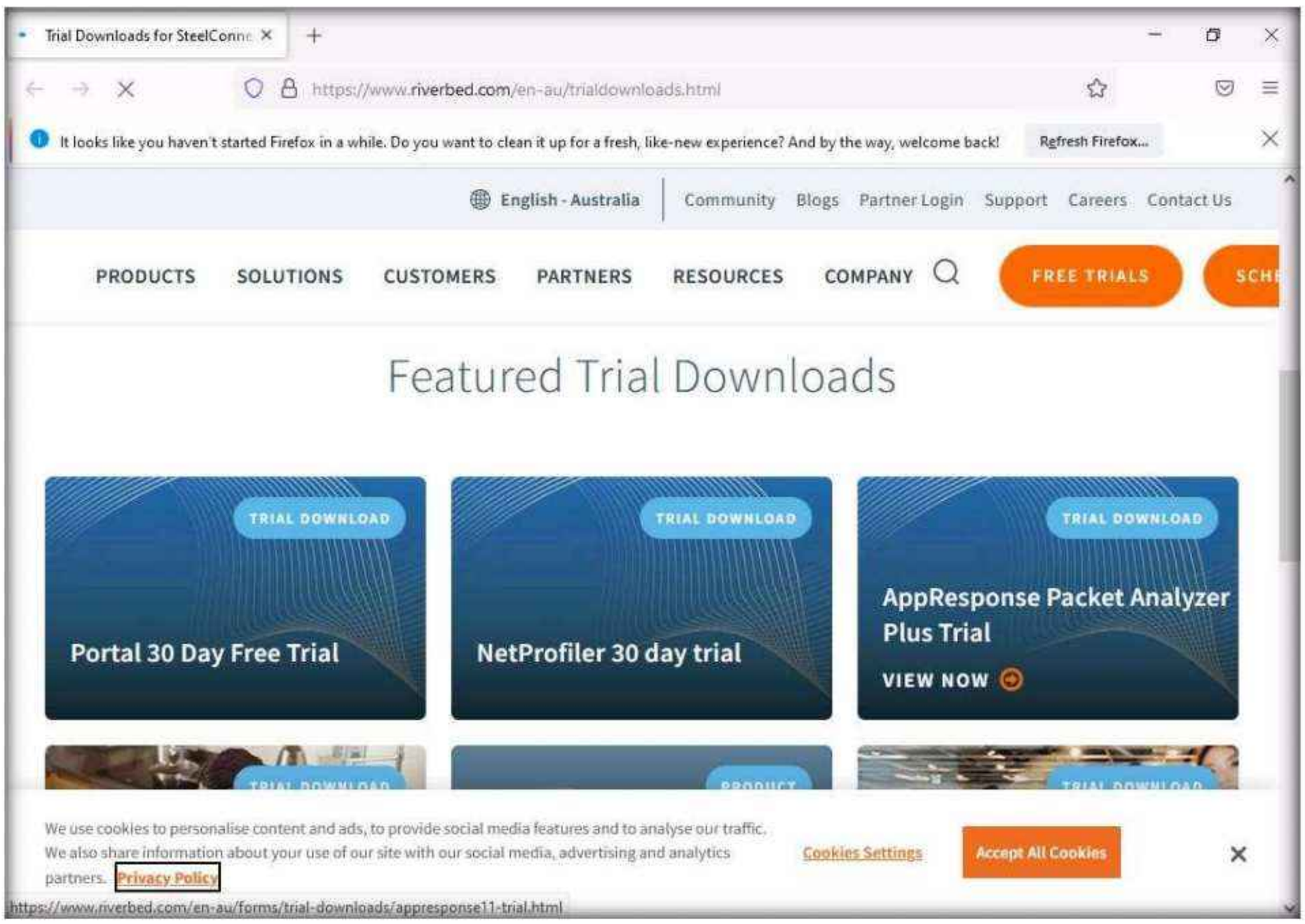
SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

Here, we will use the SteelCentral Packet Analyzer tool to analyze a network.

1. Switch to the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**) now type **https://www.riverbed.com/in/trialdownloads.html** in the address bar; press **Enter**.
2. The **riverbed** website appears, displaying **TRIAL DOWNLOADS**. Scroll down and click on **AppResponse Packet Analyzer Plus Trial**.

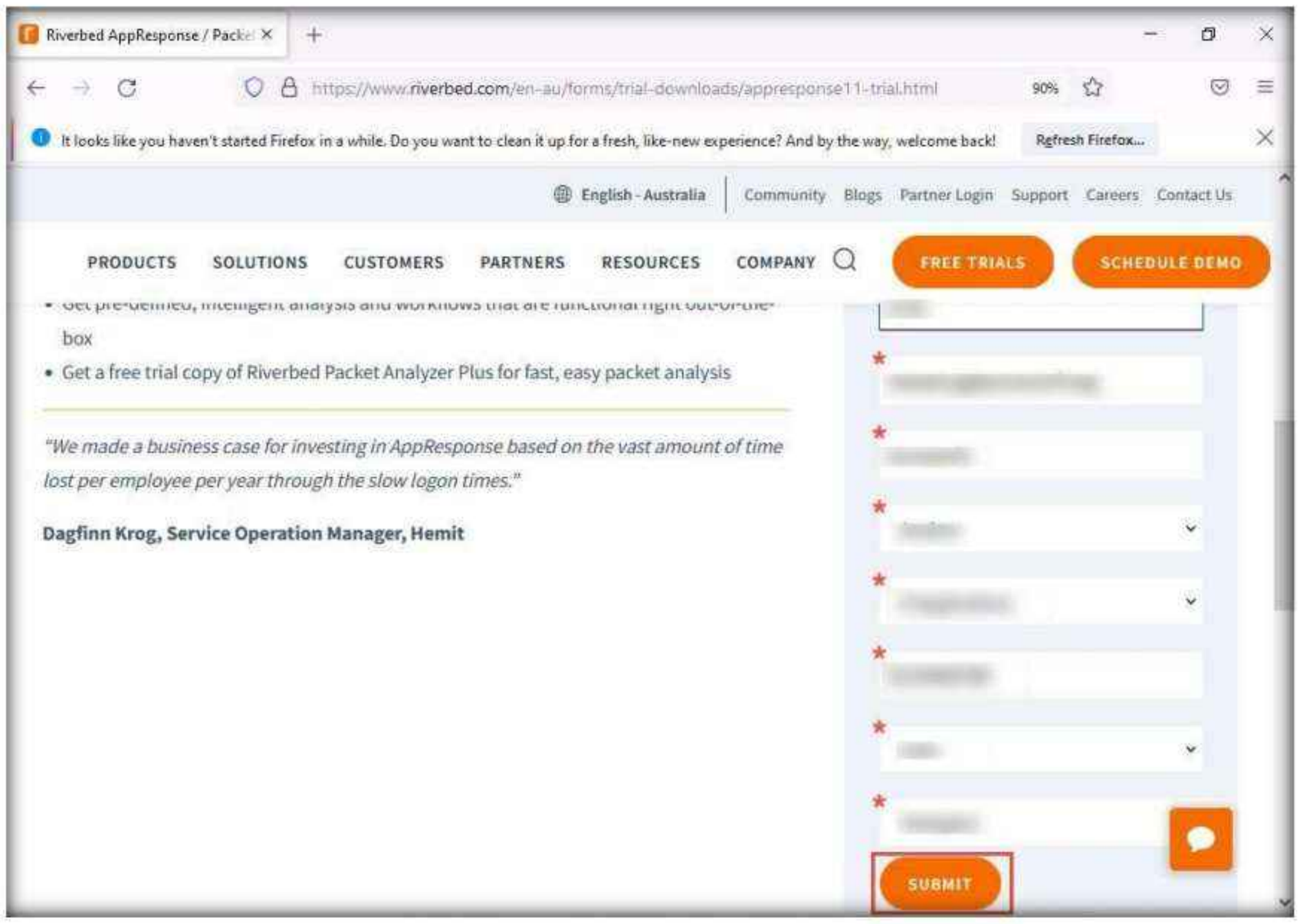
   Note: The tool version might differ in your lab environment.

   Note: At the bottom of the page click on **Accept All Cookies**.



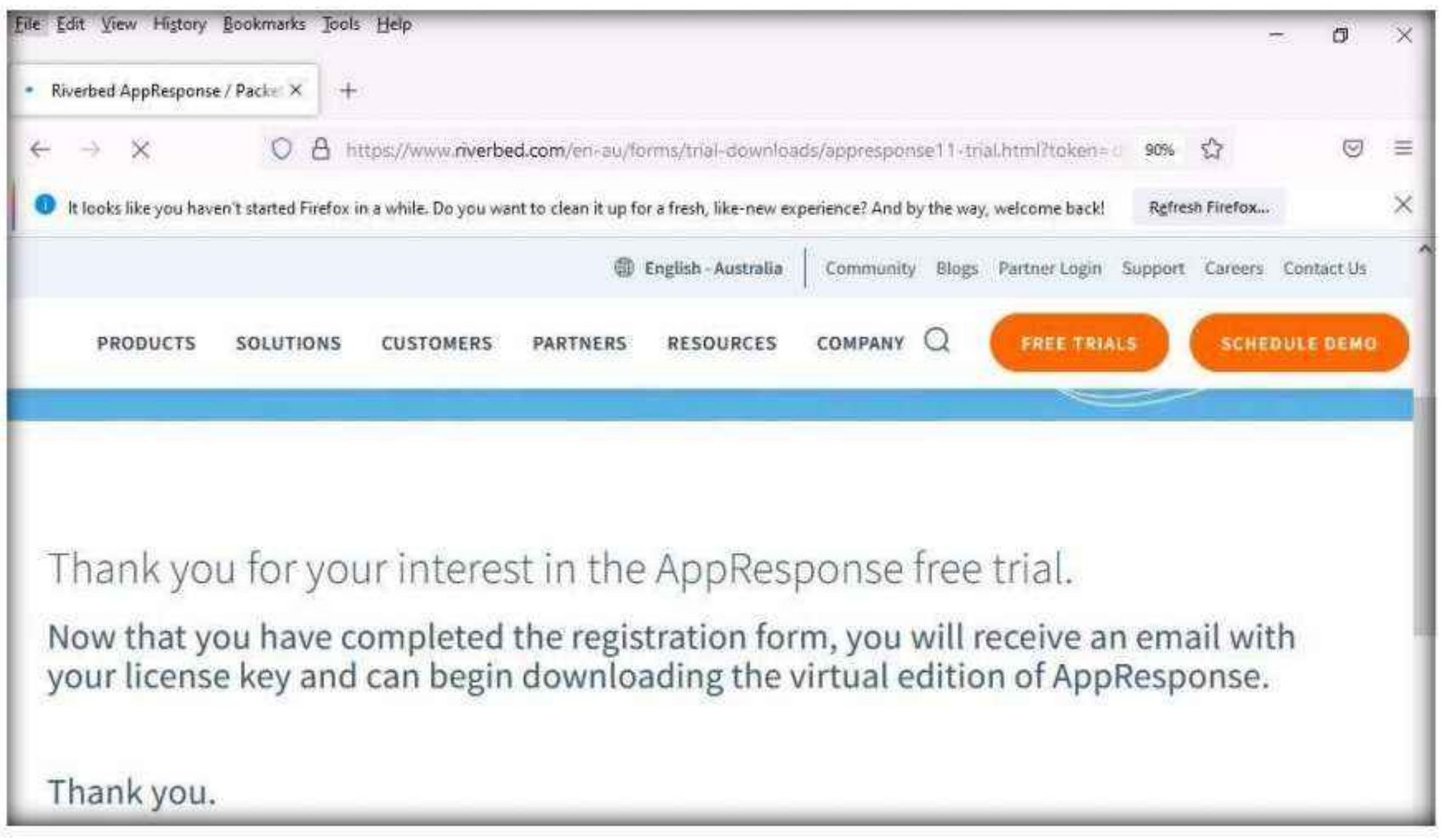
3. A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.

   Note: Here, you must give your work email to create an account.

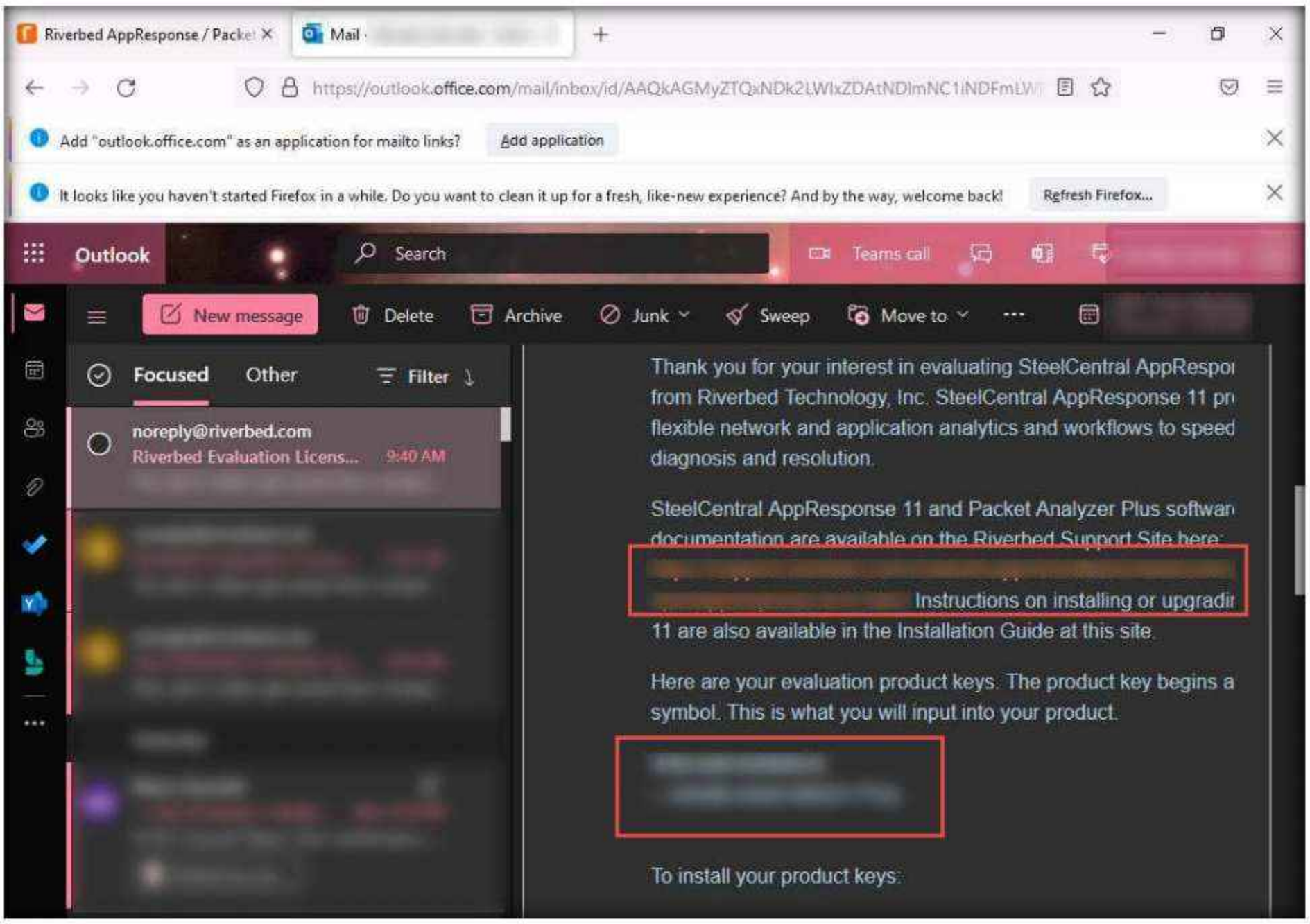


   Note: If a **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

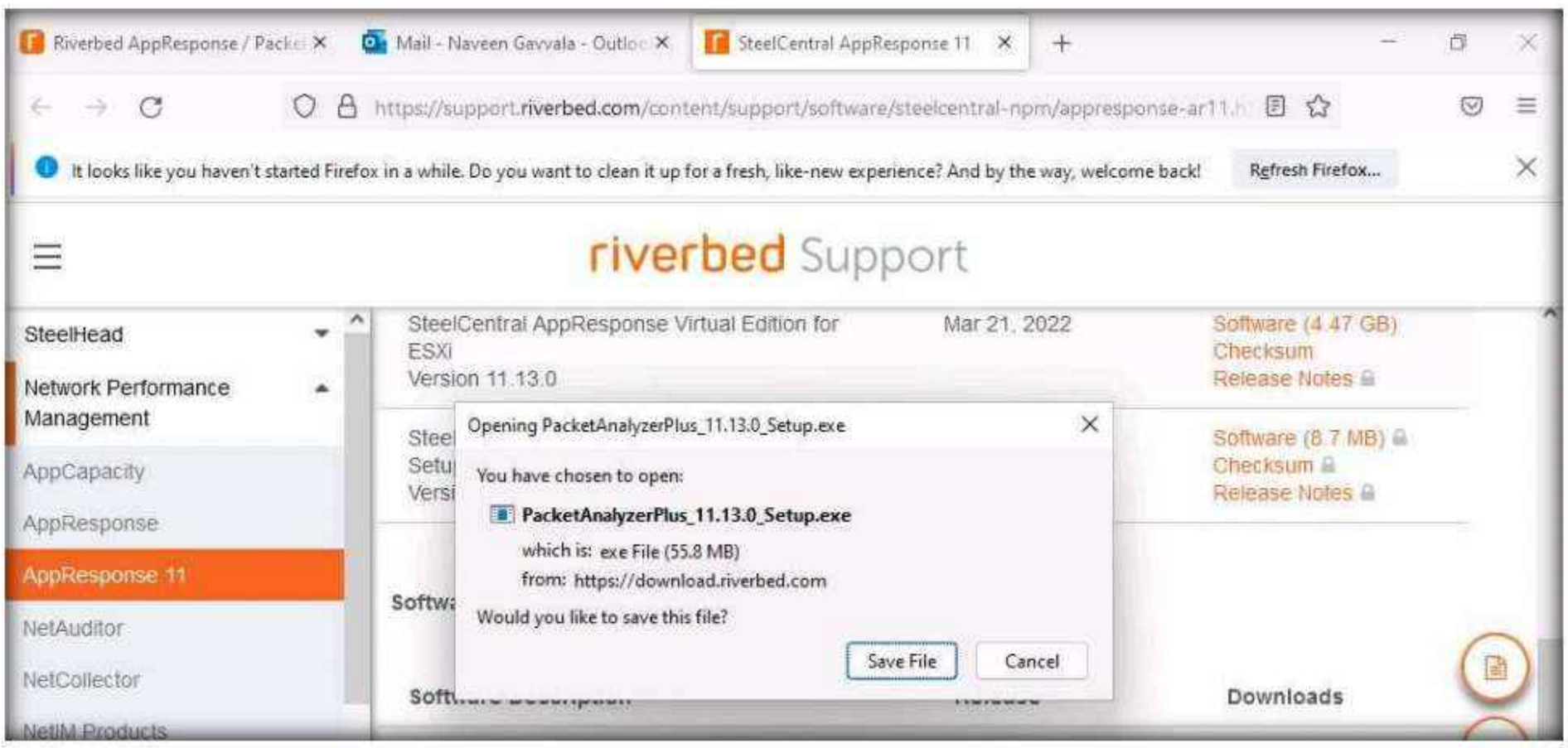
4. A **Thank You** webpage appears with information regarding the trial version.



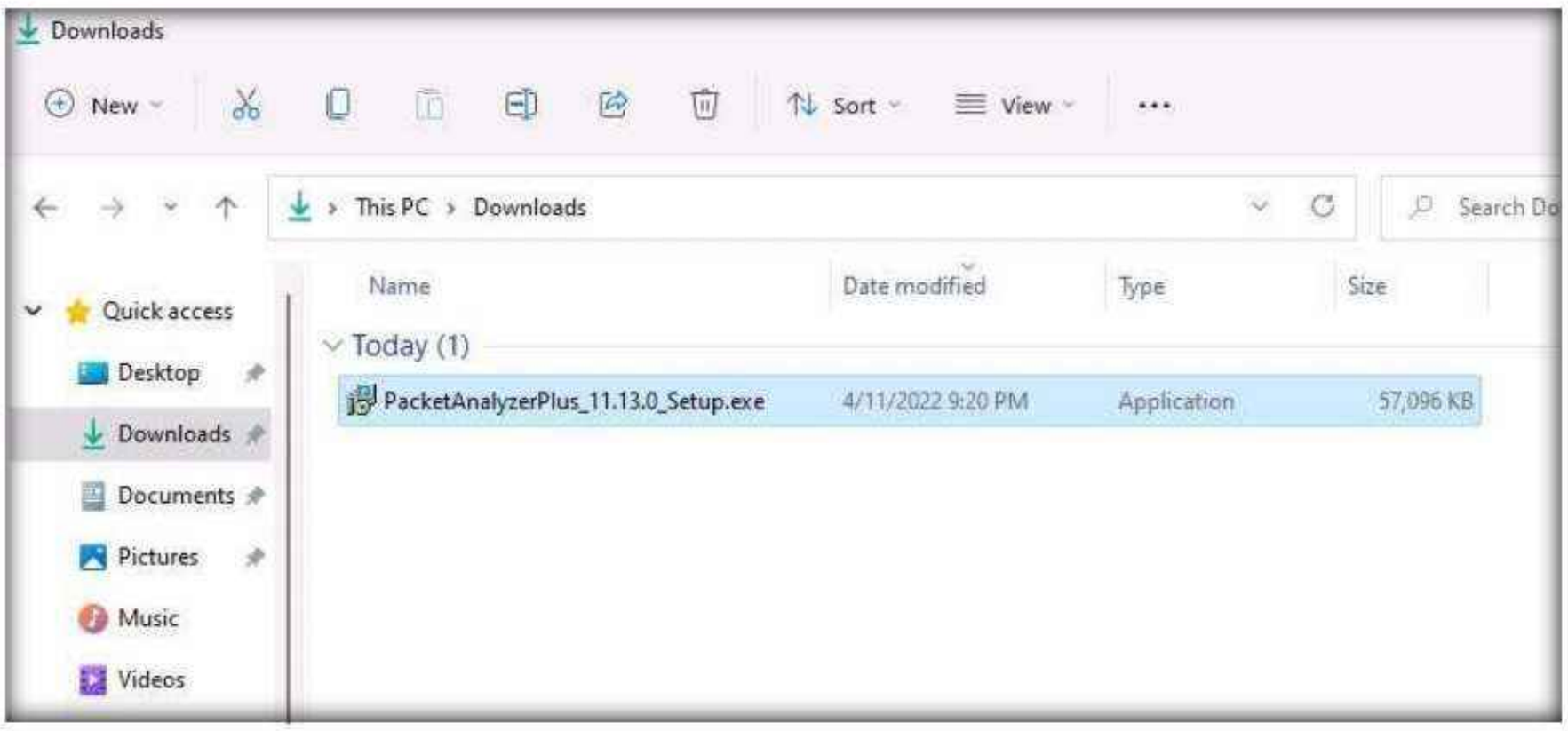
5. Open a new tab and log in to the email account you provided during registration. Open the email from **Riverbed Evaluation License Request for SteelCentral AppResponse Virtual**, and click the **Software** link to download SteelCentral Packet Analyzer.



6. The Opening **PacketAnalyzer_11.13.0_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.



7. On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer_11.13.0_Setup.exe**.



8. The **Open File - Security Warning** window appears; click **Run**.
9. The **SteelCentral Packet Analyzer Plus Setup** window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.