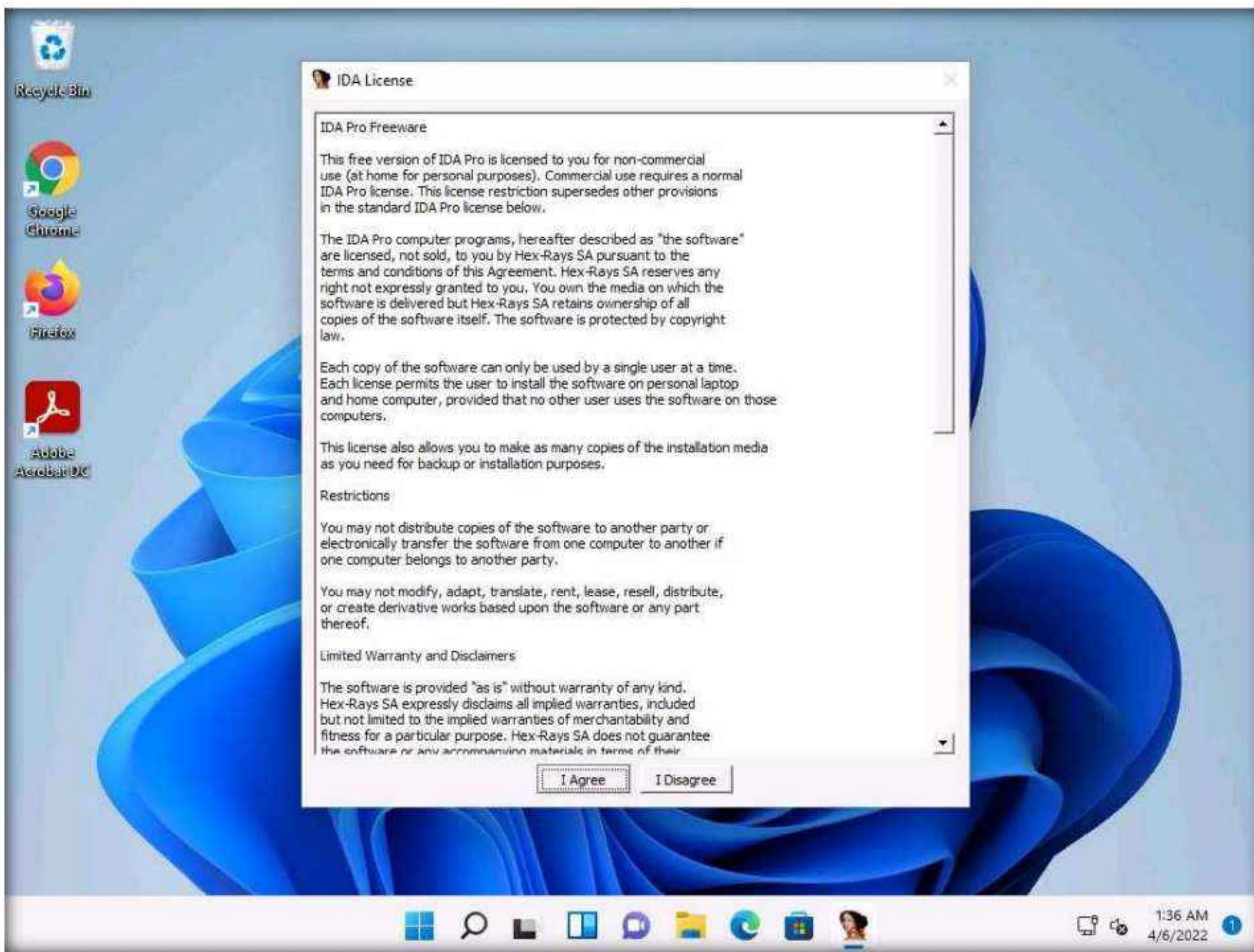
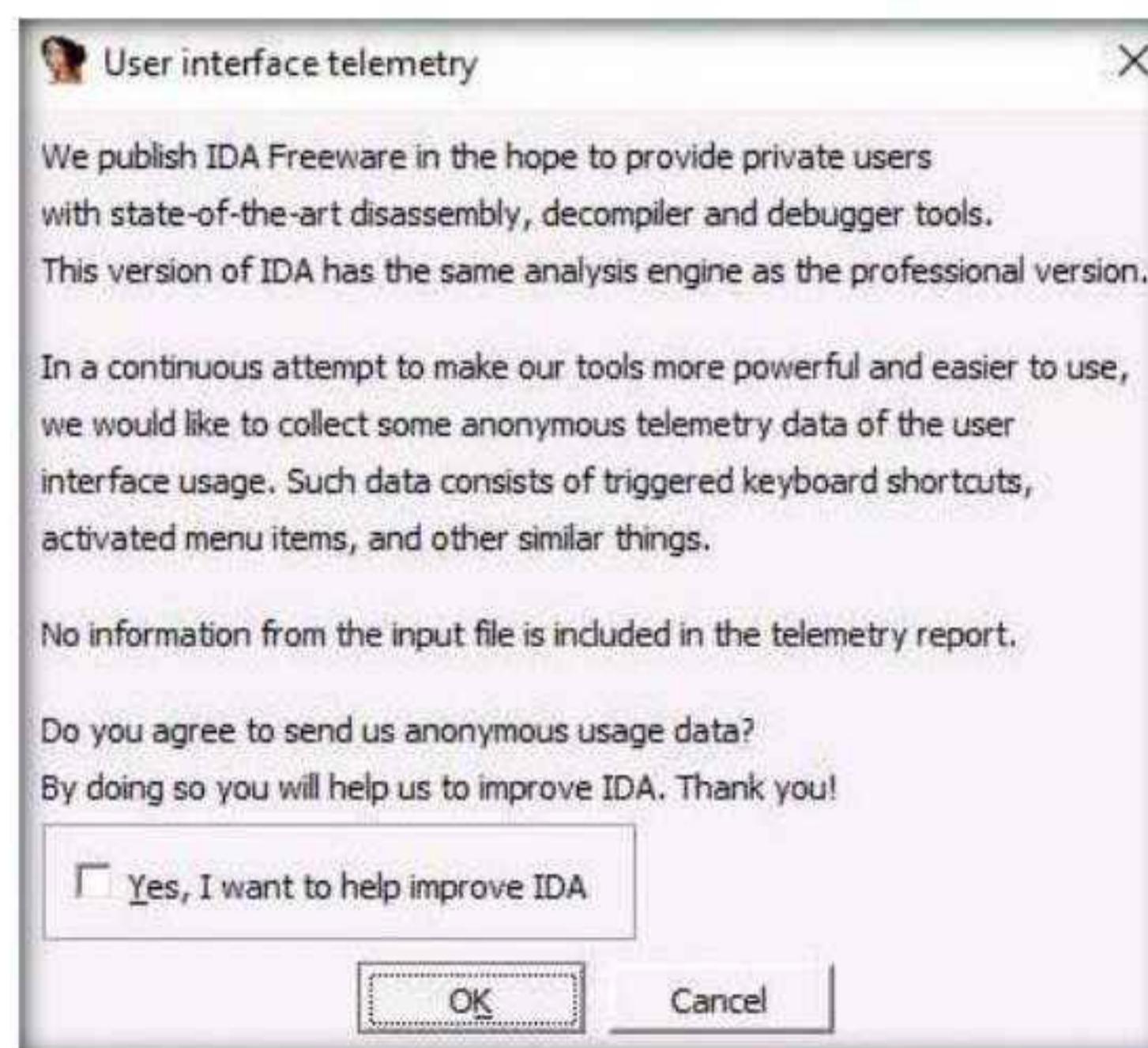


Module 07 – Malware Threats

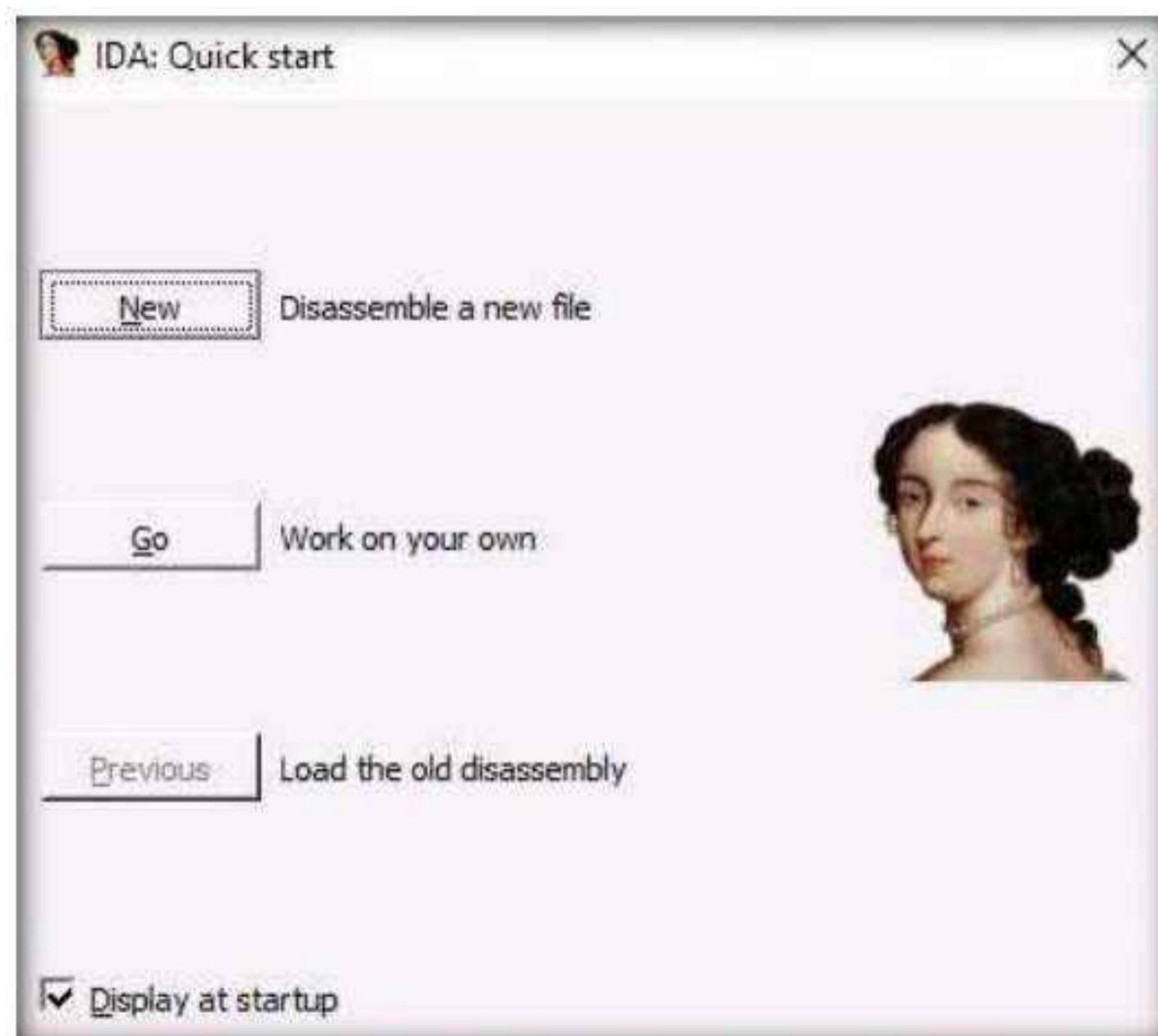
2. If the IDA License window appears, click on I Agree.



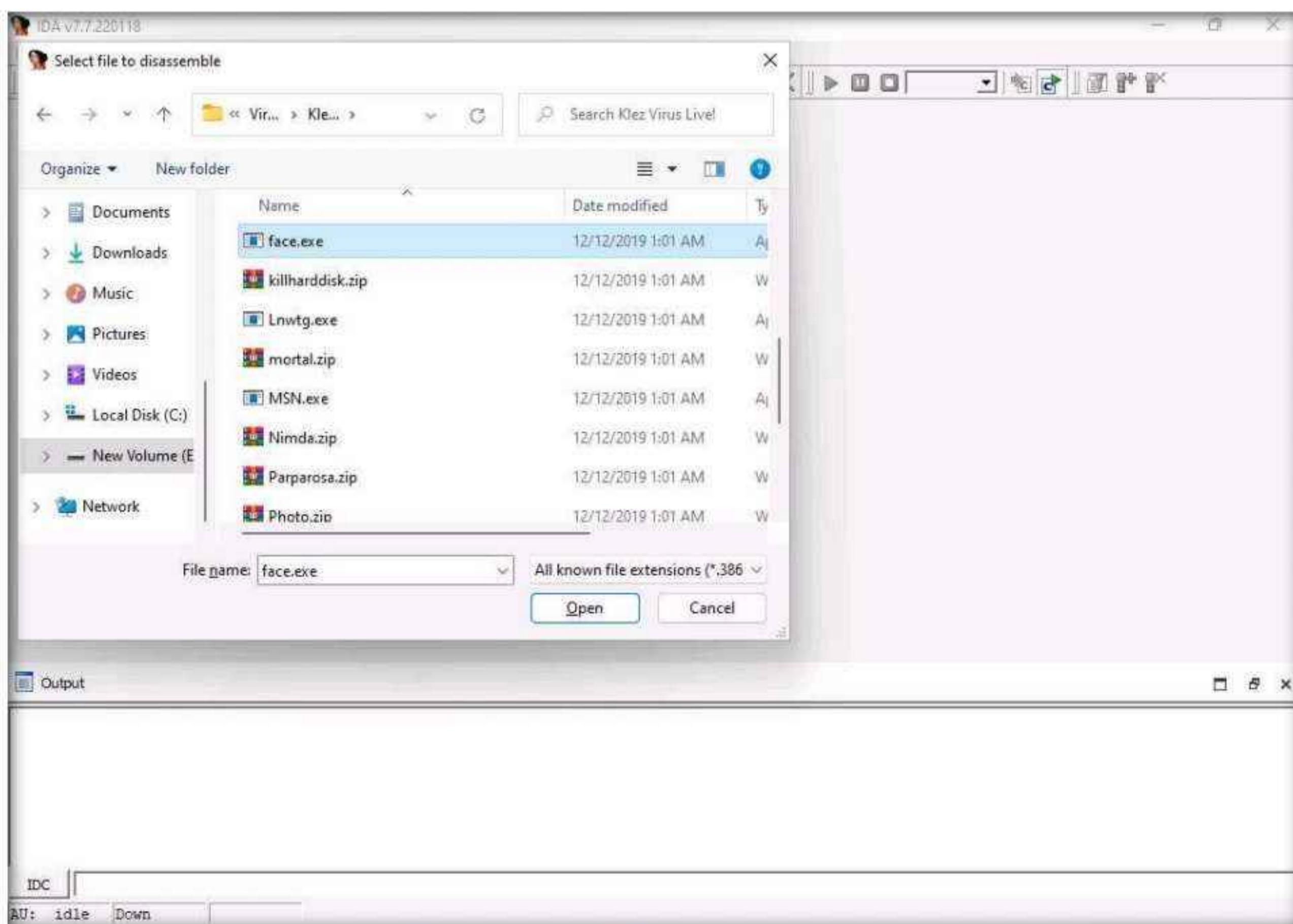
3. User interface telemetry window appears, uncheck Yes, I want to help improve IDA checkbox and click OK.



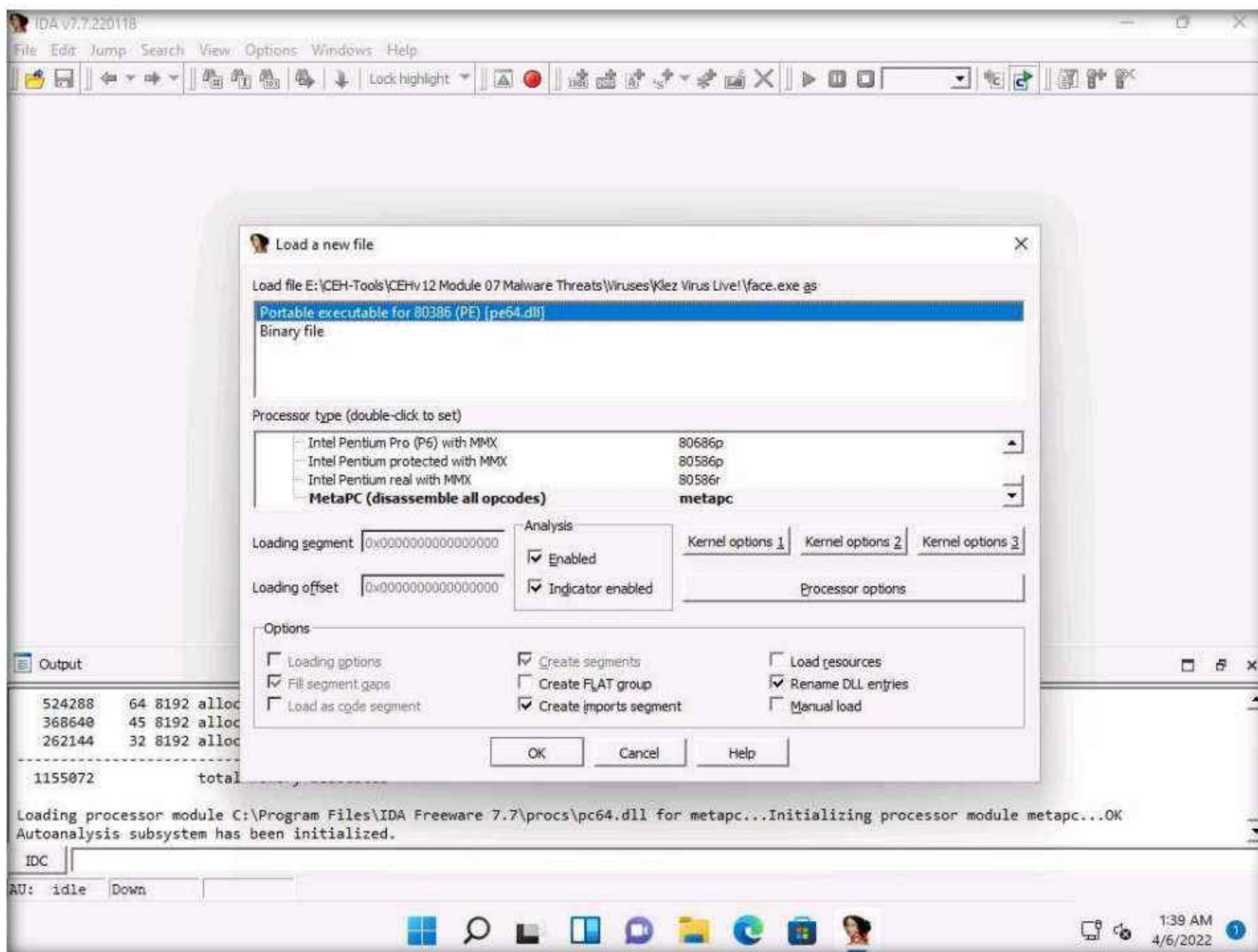
4. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.



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**.

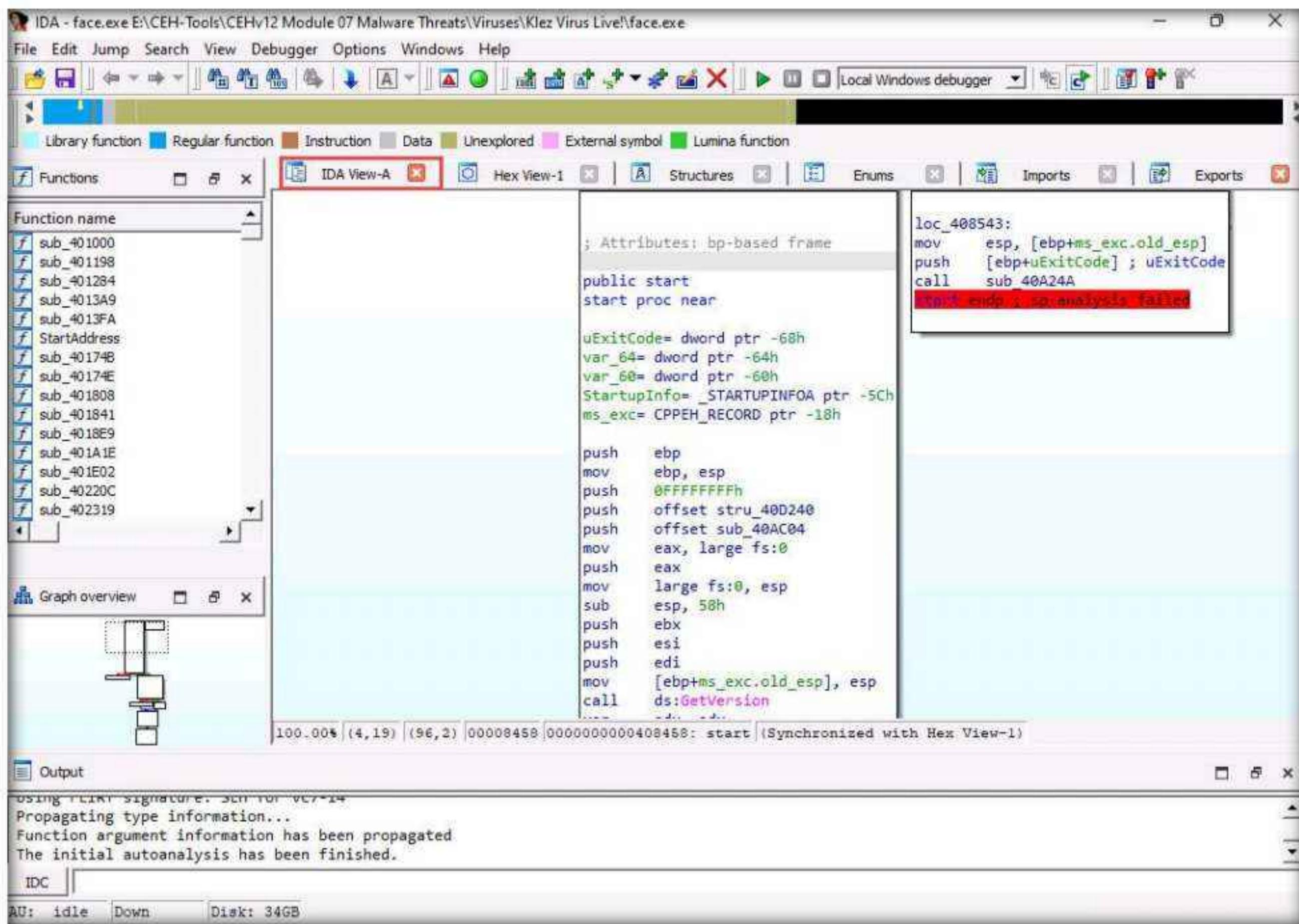


7. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.

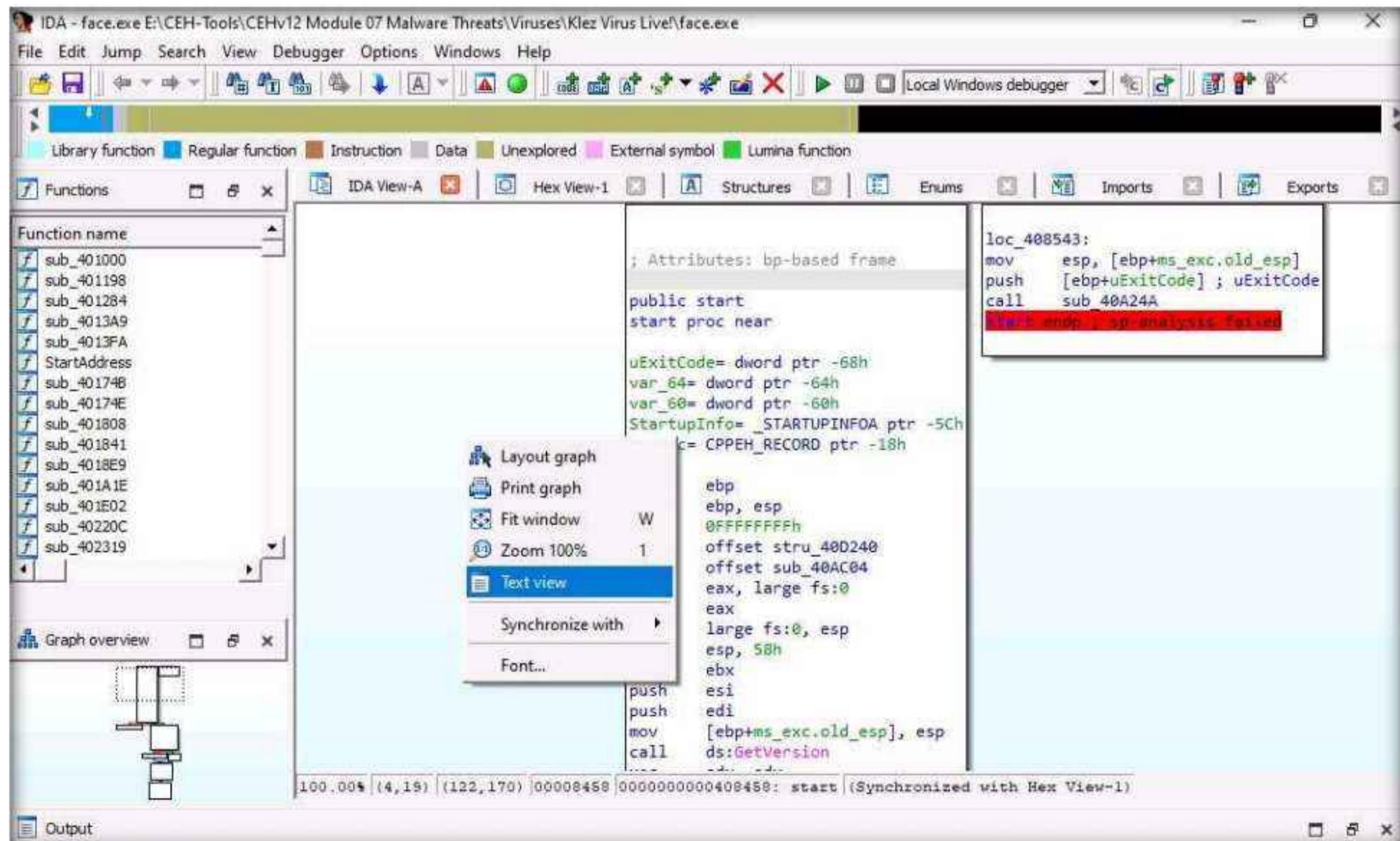


8. If a **Warning** pop-up appears, click **OK**.
9. If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.
10. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.

Module 07 – Malware Threats

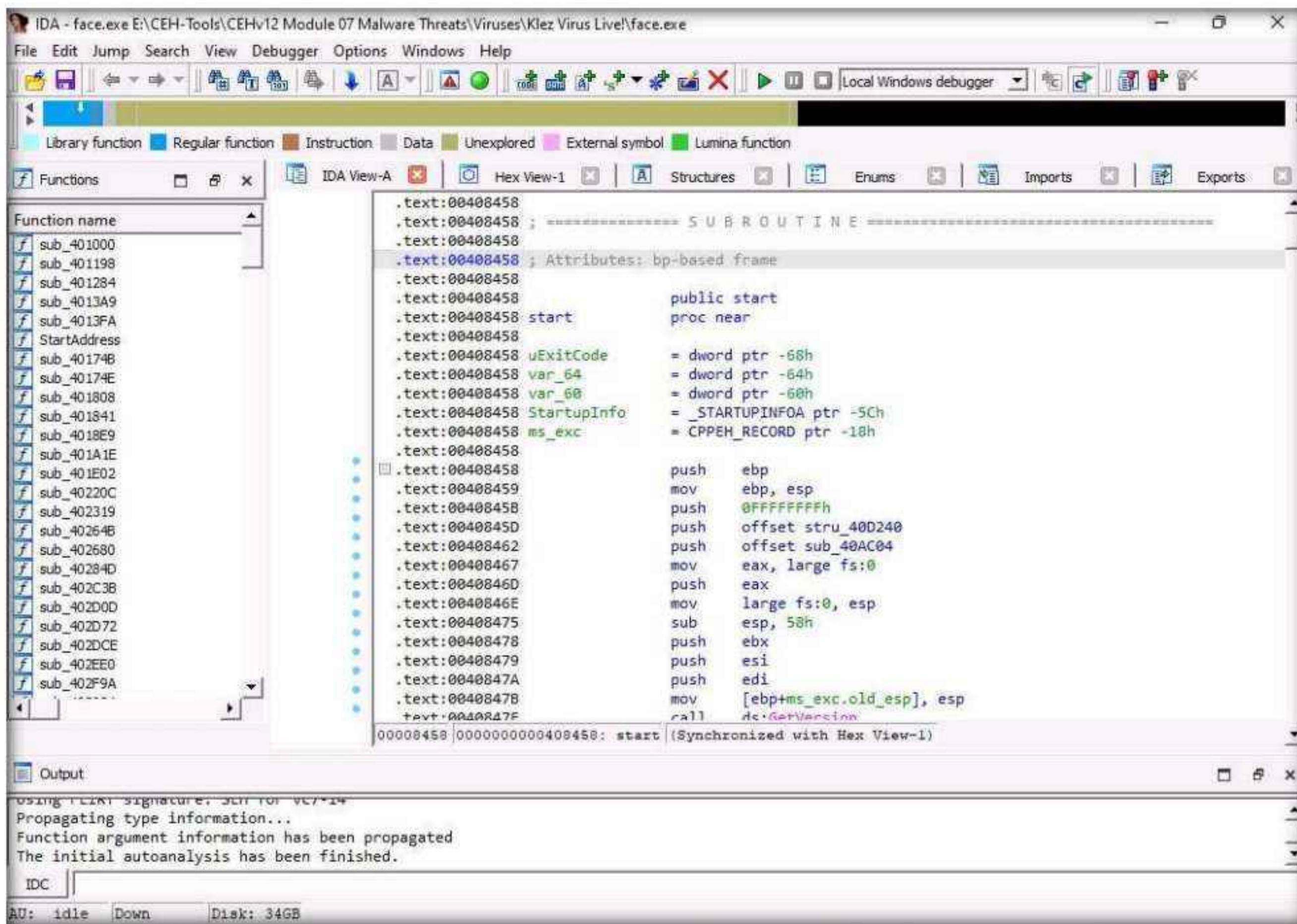


11. In the **IDA View-A** section, right-click anywhere and choose **Text view** from the context menu to view the text information of the malicious file uploaded to IDA for analysis.



Module 07 – Malware Threats

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



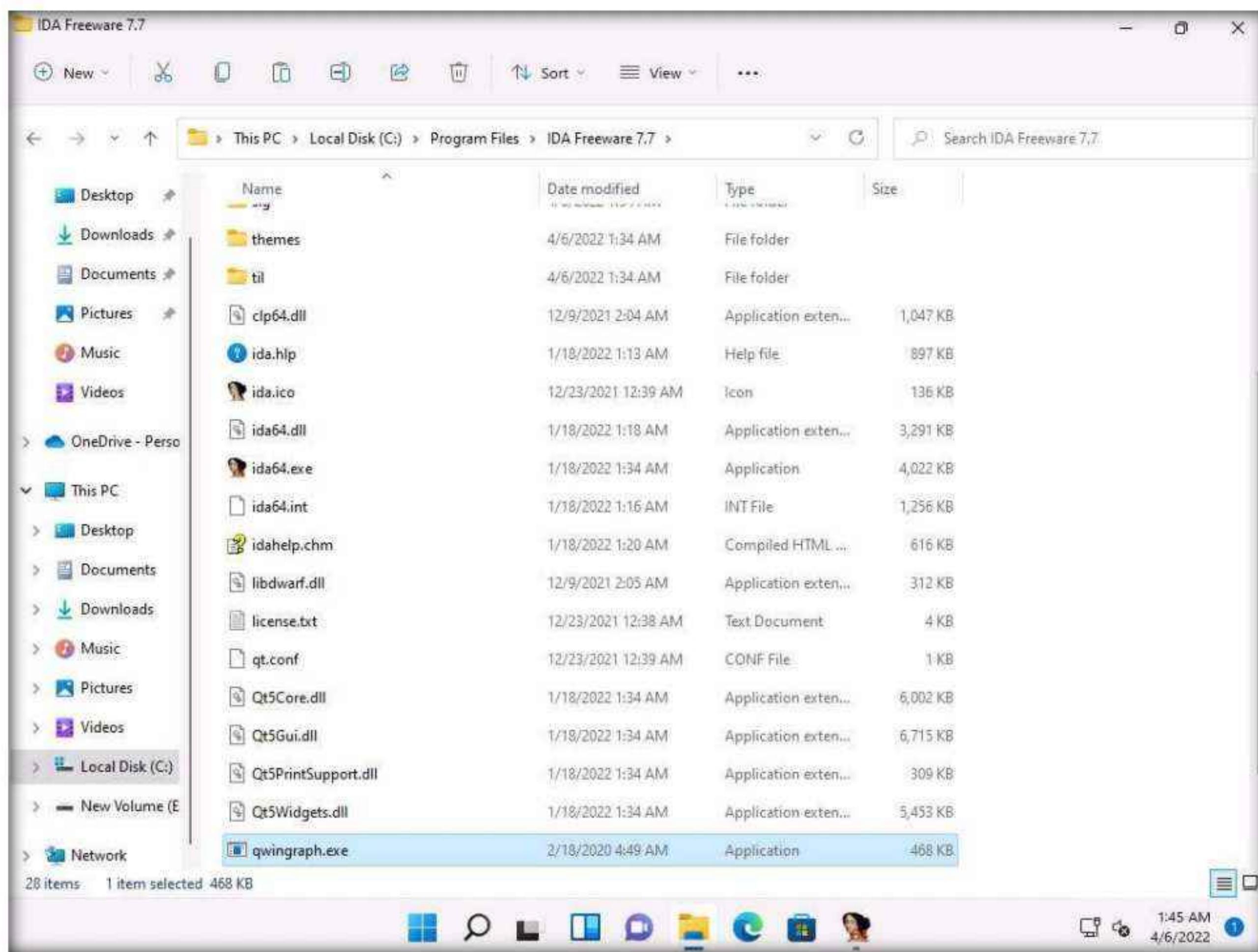
The screenshot shows the IDA Pro interface with the assembly view selected. The assembly code for the 'start' function is displayed, showing the initialization of variables and the call to the Windows API function GetVersion. The code includes comments and labels such as .text:00408458, .text:00408458 ; ----- SUB ROUTINE -----, and .text:00408458 ; Attributes: bp-based frame. The left pane shows a list of functions, and the bottom pane displays the output of the autoanalysis process.

```
.text:00408458
.text:00408458 ; ----- SUB ROUTINE -----
.text:00408458 ; Attributes: bp-based frame
.text:00408458
.text:00408458     public start
.text:00408458     proc near
.text:00408458
.text:00408458     uExitCode      = dword ptr -68h
.text:00408458     var_64        = dword ptr -64h
.text:00408458     var_60        = dword ptr -60h
.text:00408458     StartupInfo    = _STARTUPINFOA ptr -5Ch
.text:00408458     ms_exc        = CPPEH_RECORD ptr -18h
.text:00408458
.text:00408458     push    ebp
.text:00408459     mov     ebp, esp
.text:00408458     push    0FFFFFFFh
.text:0040845D     push    offset stru_40D240
.text:00408462     push    offset sub_40AC04
.text:00408467     mov     eax, large fs:0
.text:0040846D     push    eax
.text:0040846E     mov     large fs:0, esp
.text:00408475     sub    esp, 58h
.text:00408478     push    ebx
.text:00408479     push    esi
.text:0040847A     push    edi
.text:0040847B     mov     [ebp+ms_exc.old_esp], esp
.text:0040847C     call    AcGetVersion
.text:00408458 000000000408458: start (Synchronized with Hex View-1)
```

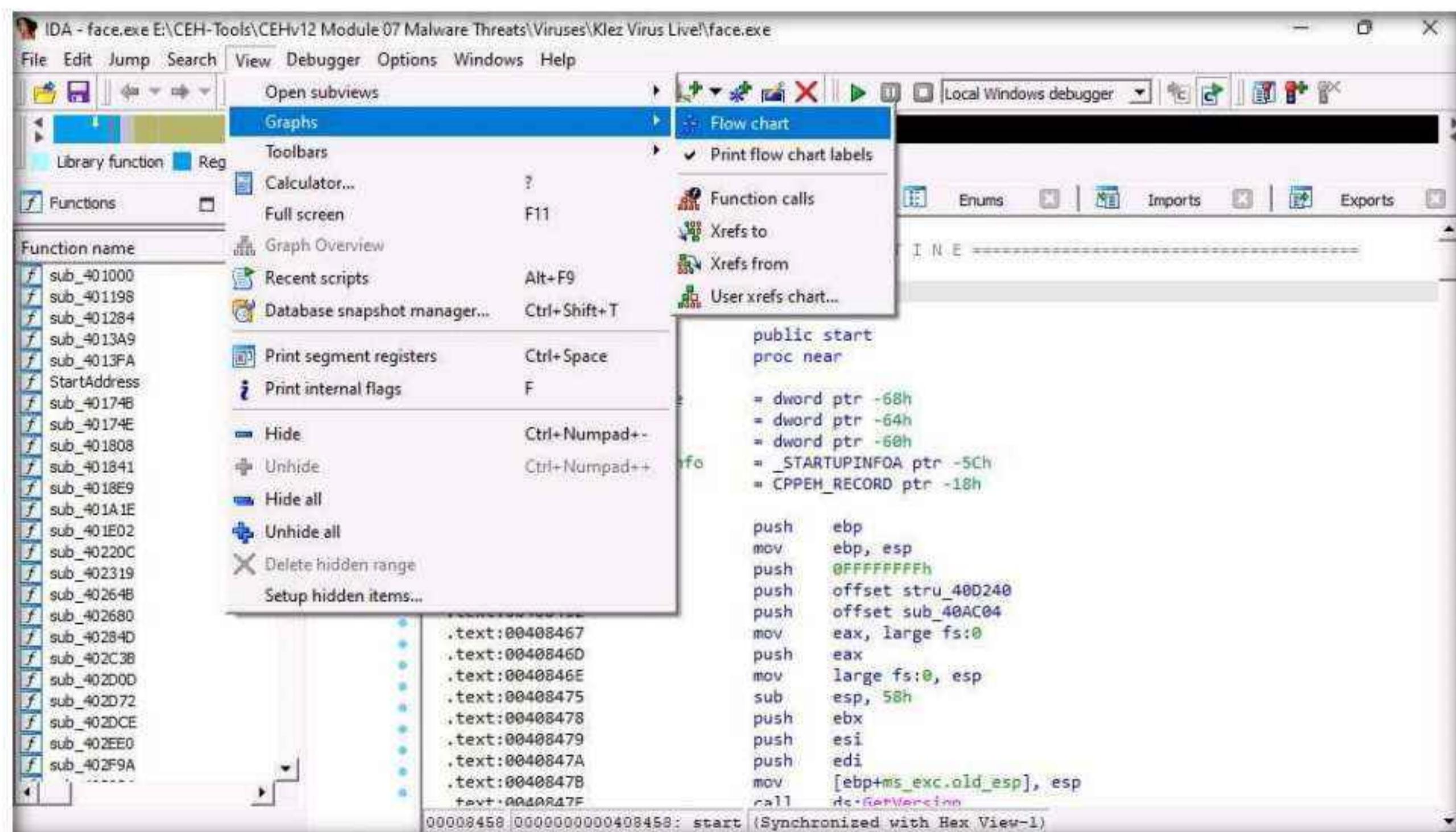
13. Now, minimize the IDA window, and navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**. Copy the **qwingraph.exe** file and paste it in IDA's installation location. In this task, the location is **C:\Program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

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

Module 07 – Malware Threats

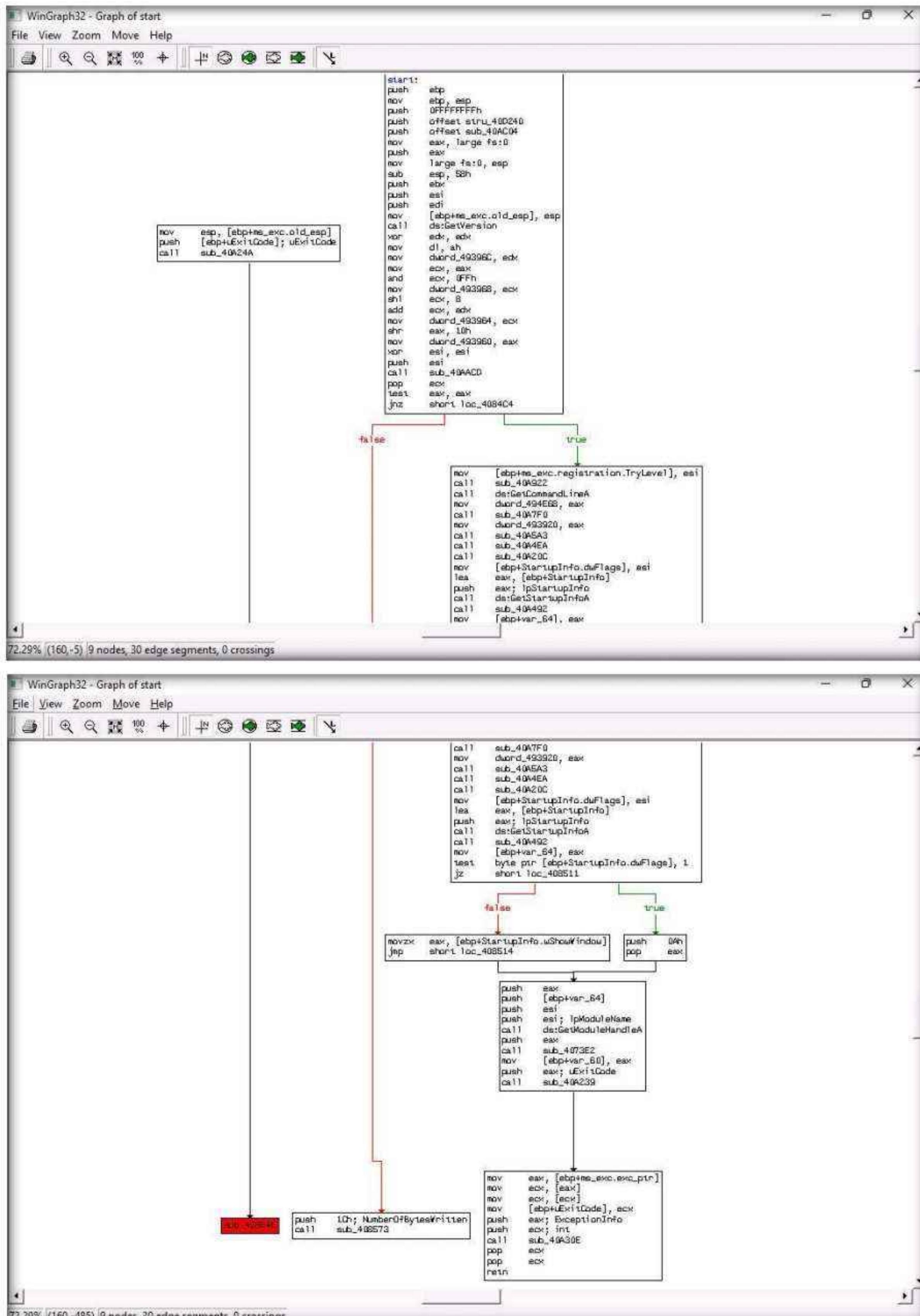


14. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View → Graphs** and click **Flow chart**.

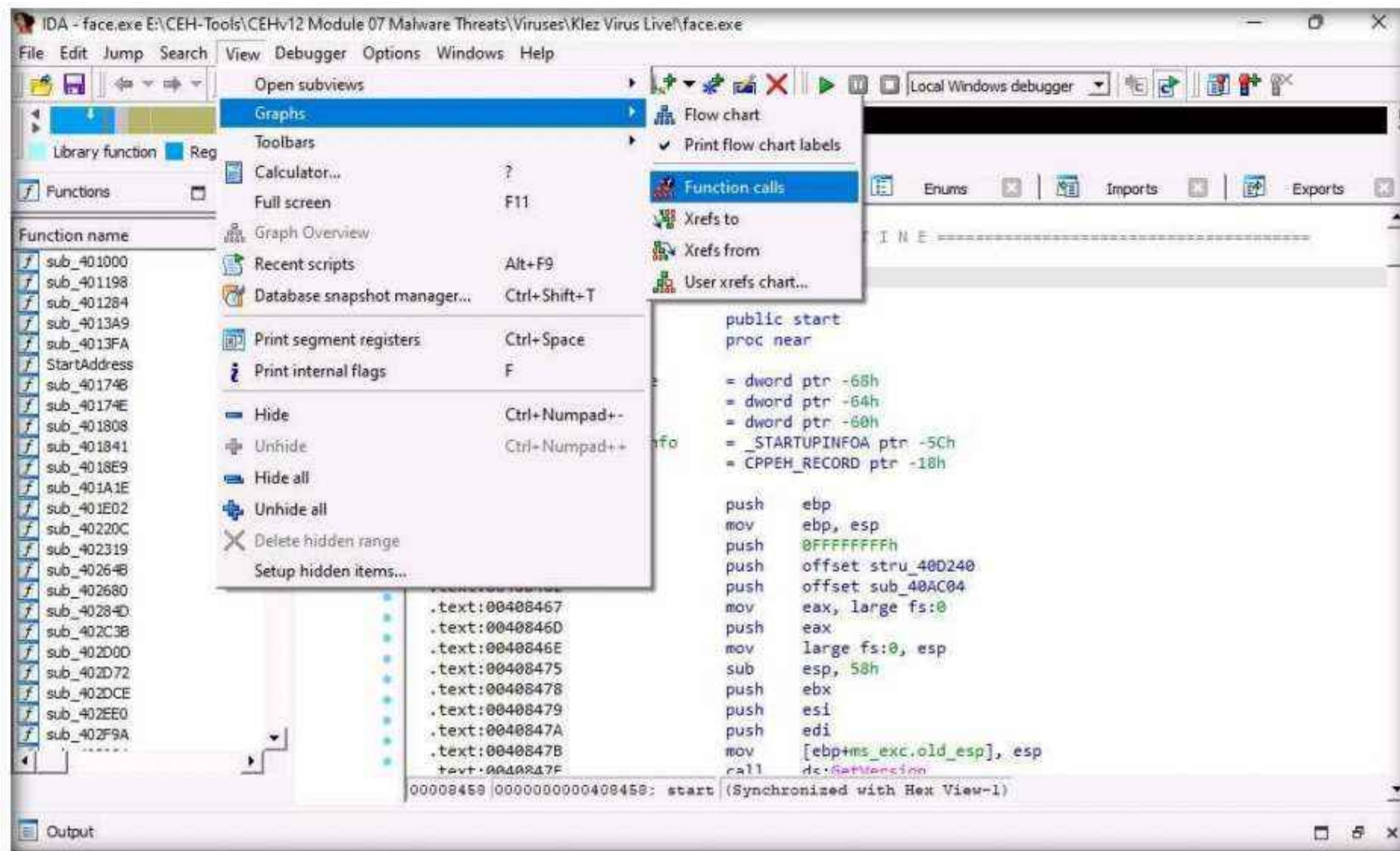


Module 07 – Malware Threats

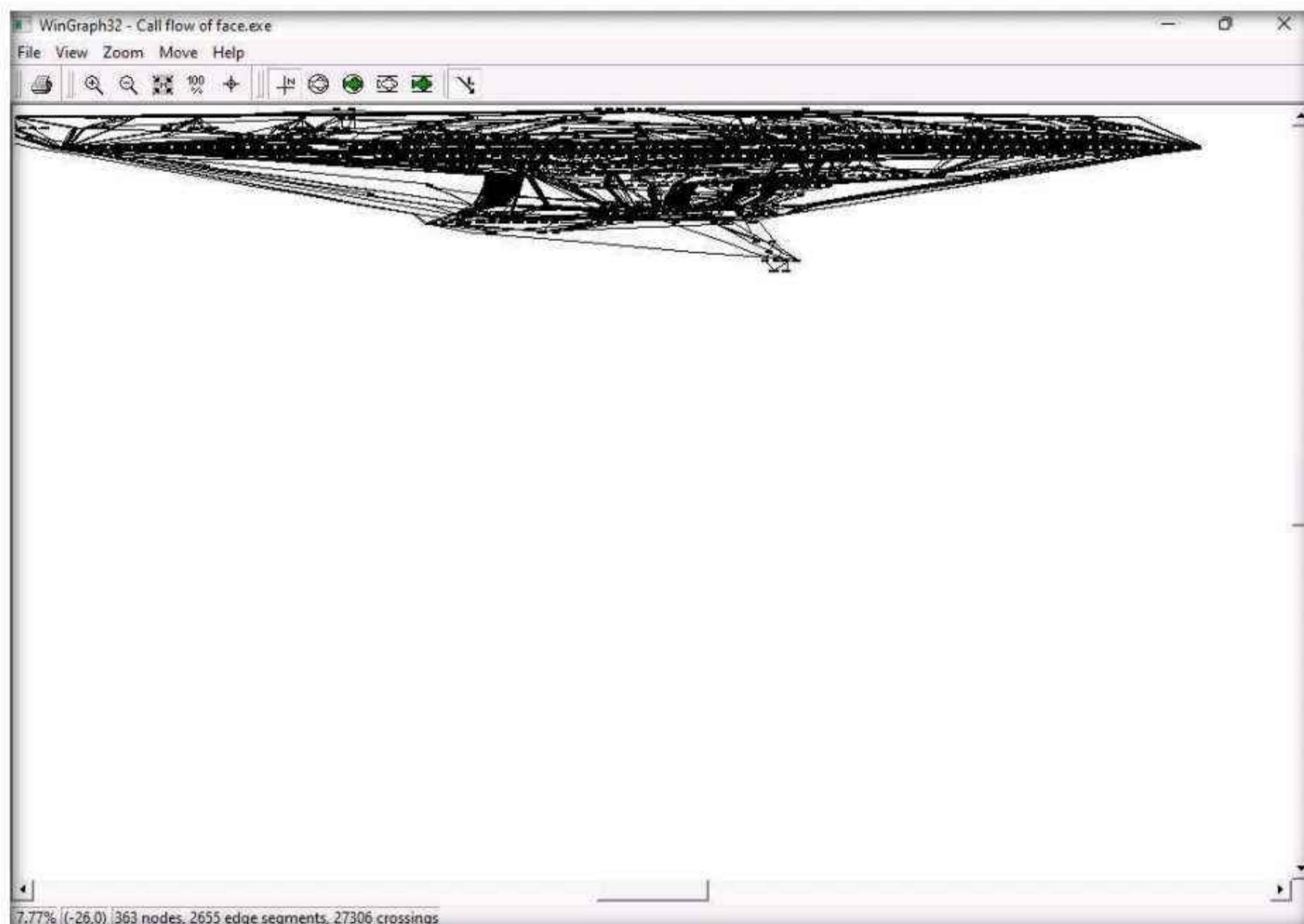
15. A Graph window appears with the flow. You may zoom in and adjust the screen to view this more clearly.

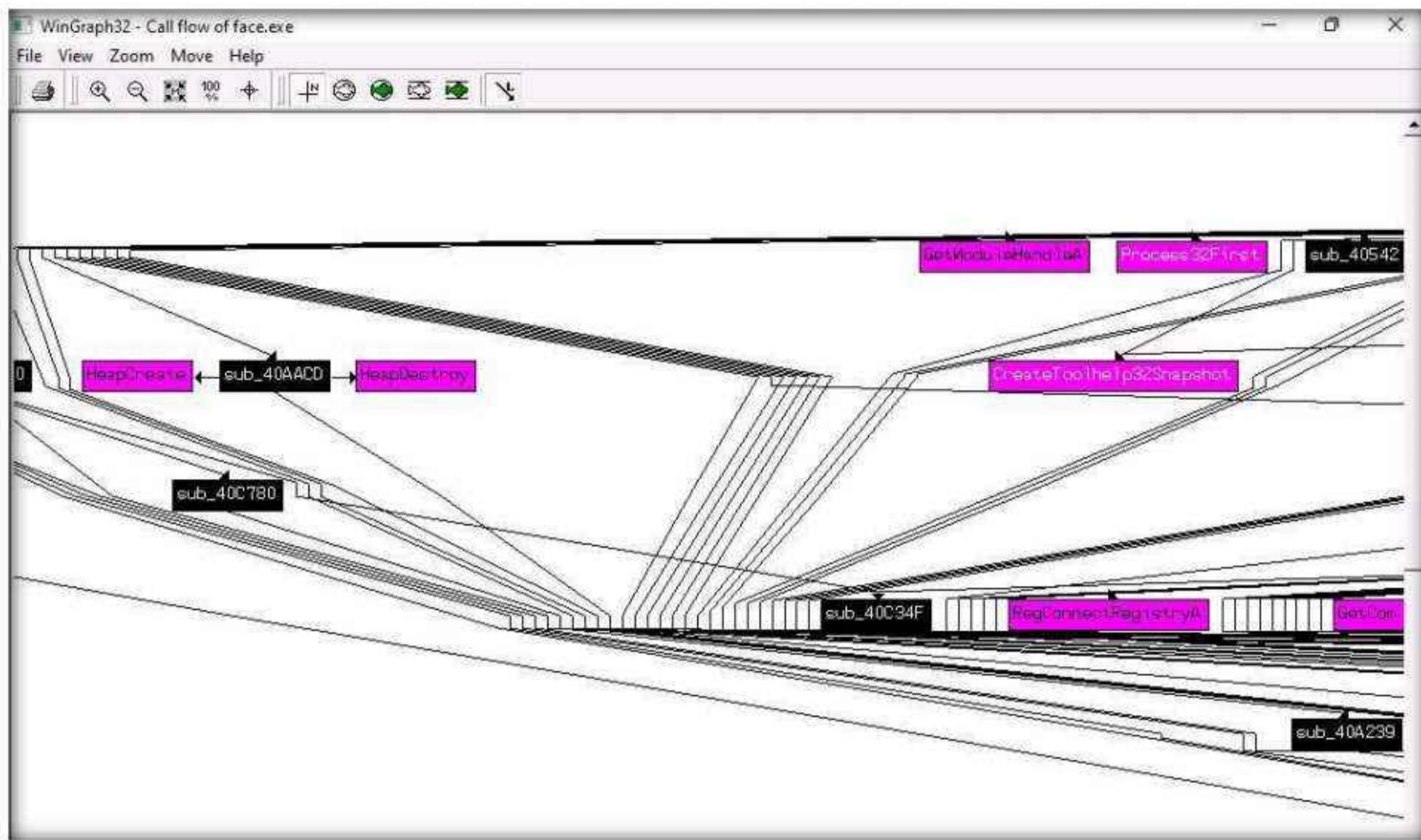


16. Close the Graph window, go to View → Graphs, and click Function calls from the menu bar.

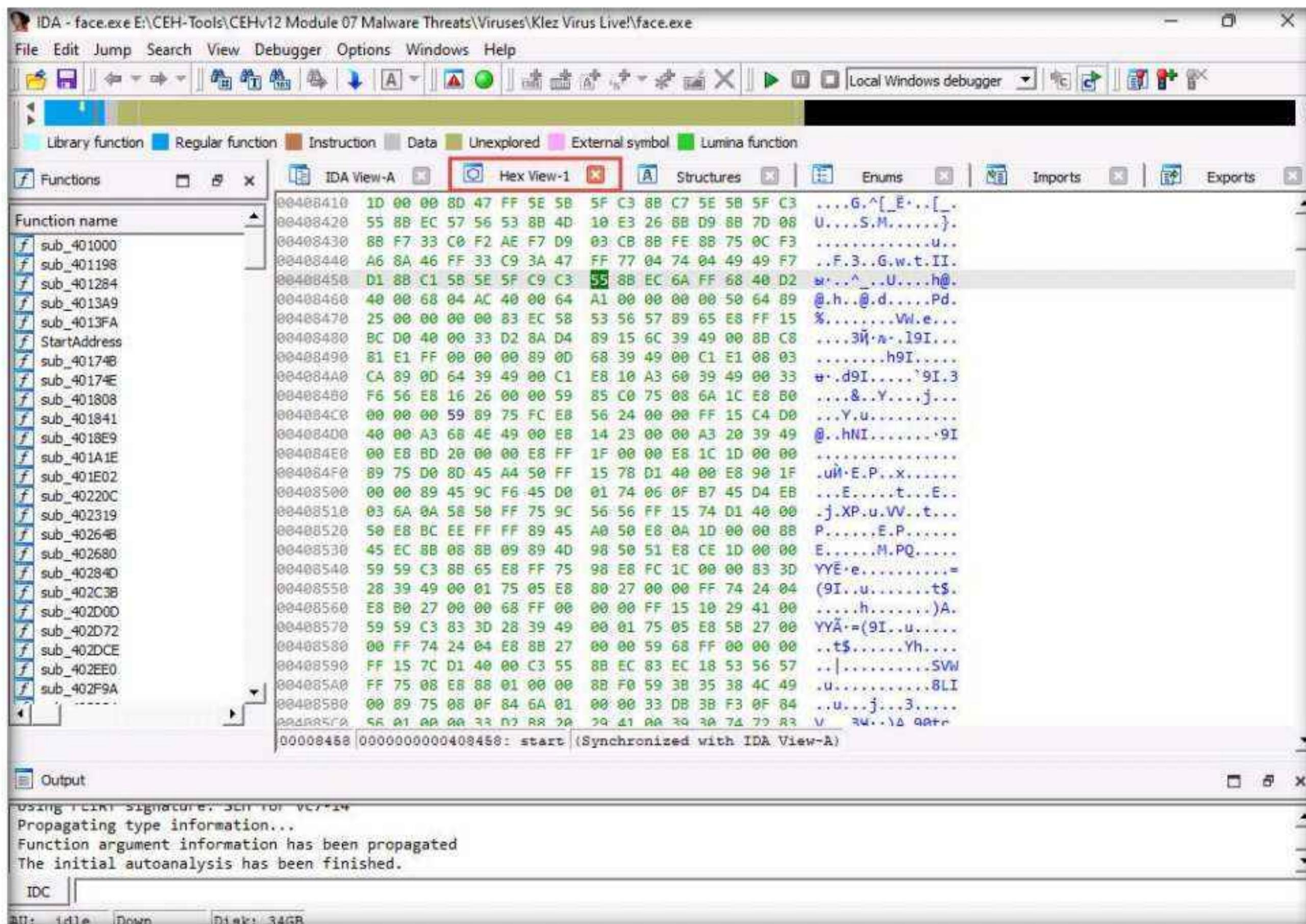


17. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.



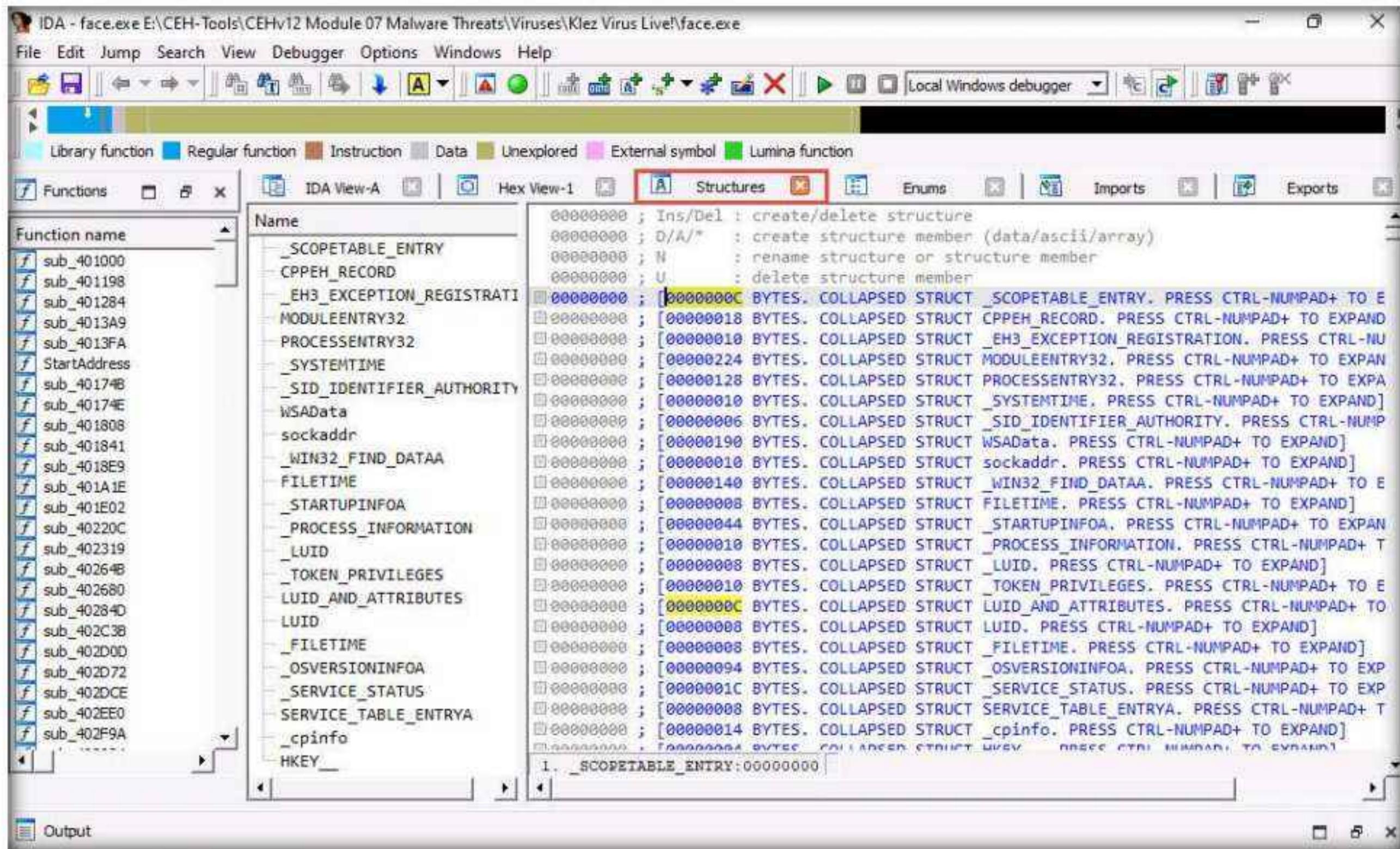


18. Click the HexView-1 tab to view the hex value of the malicious file.

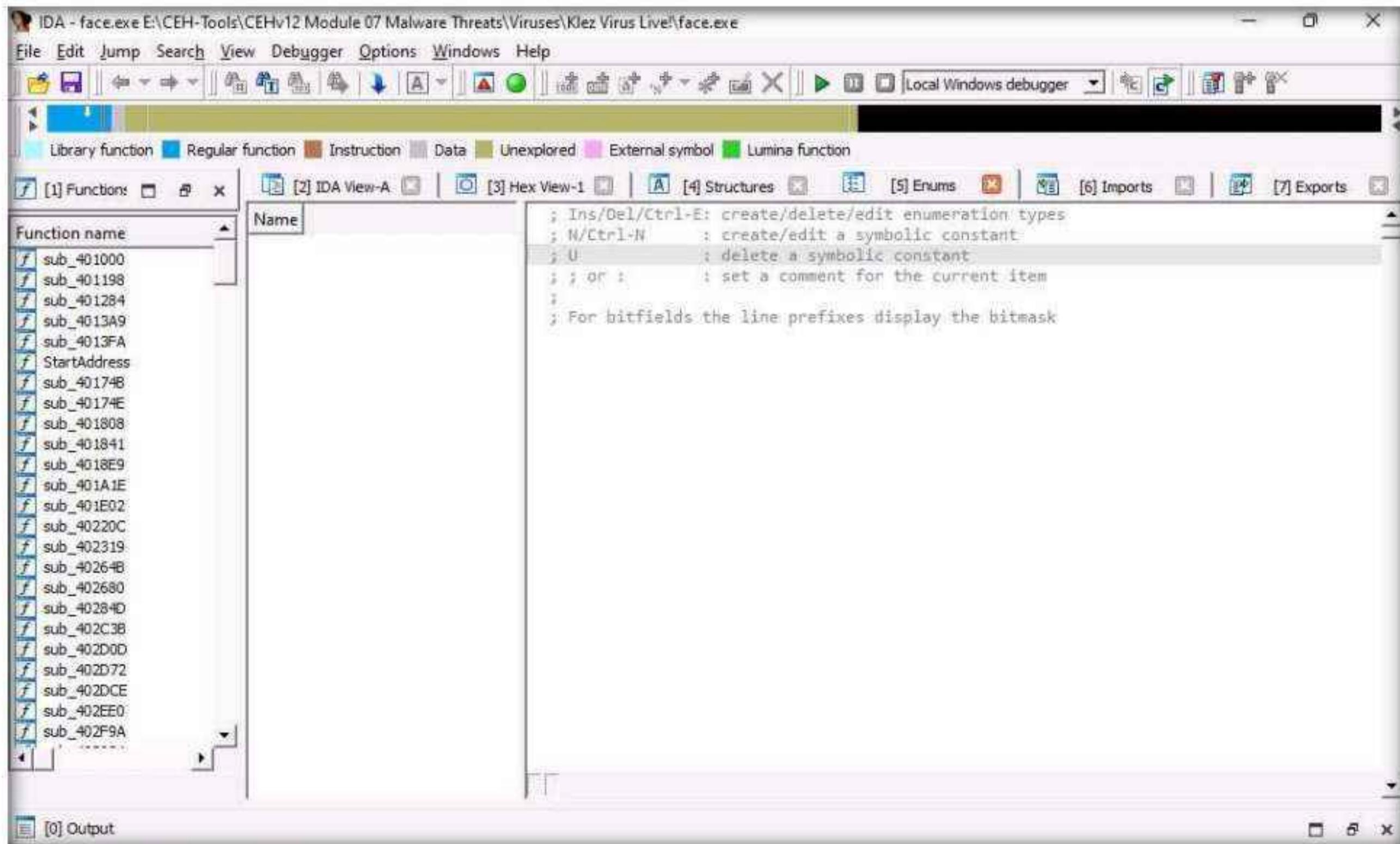


Module 07 – Malware Threats

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



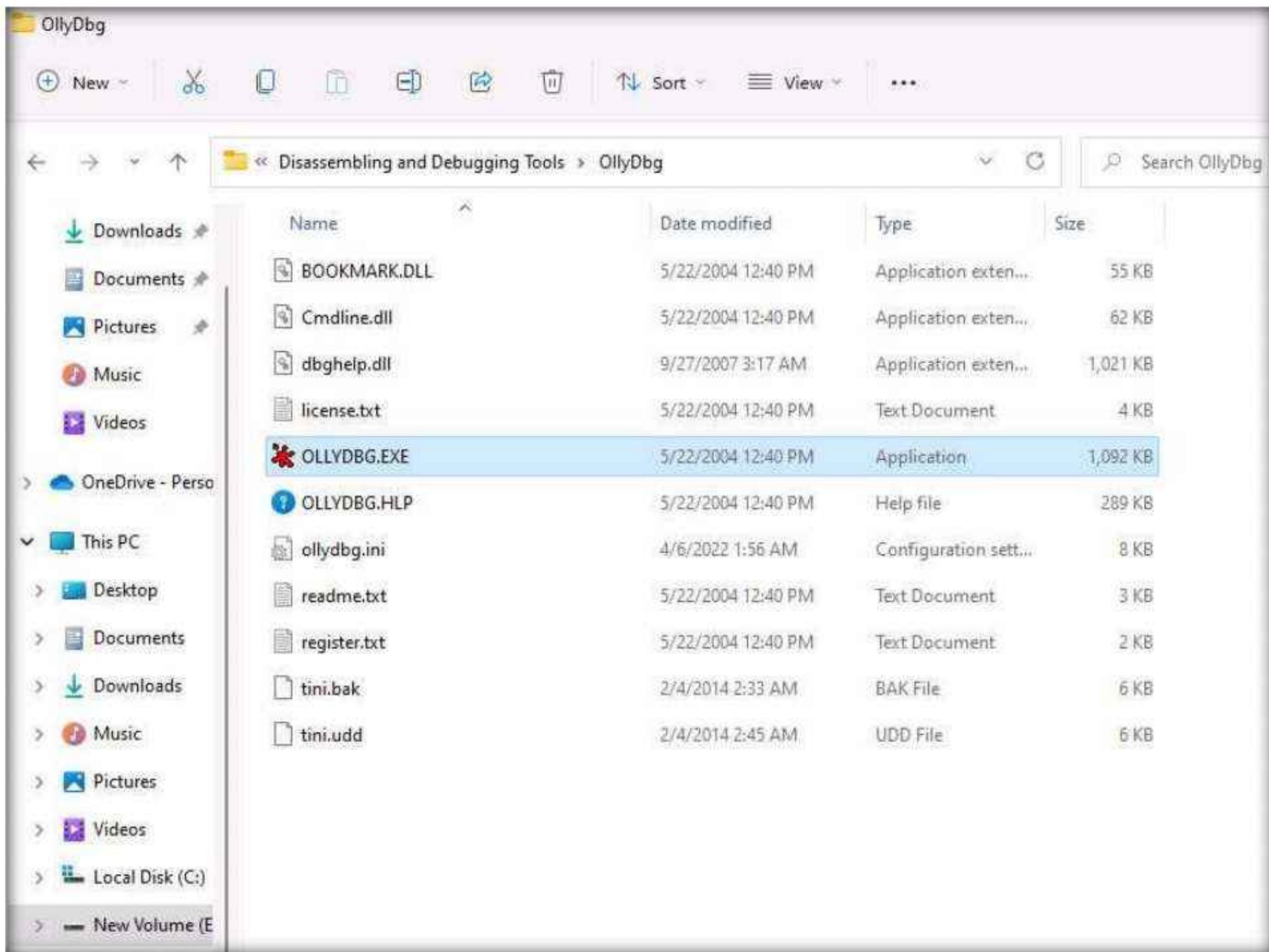
20. Click the **Enums** tab to view the Windows Enum results, as shown in the screenshot



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.

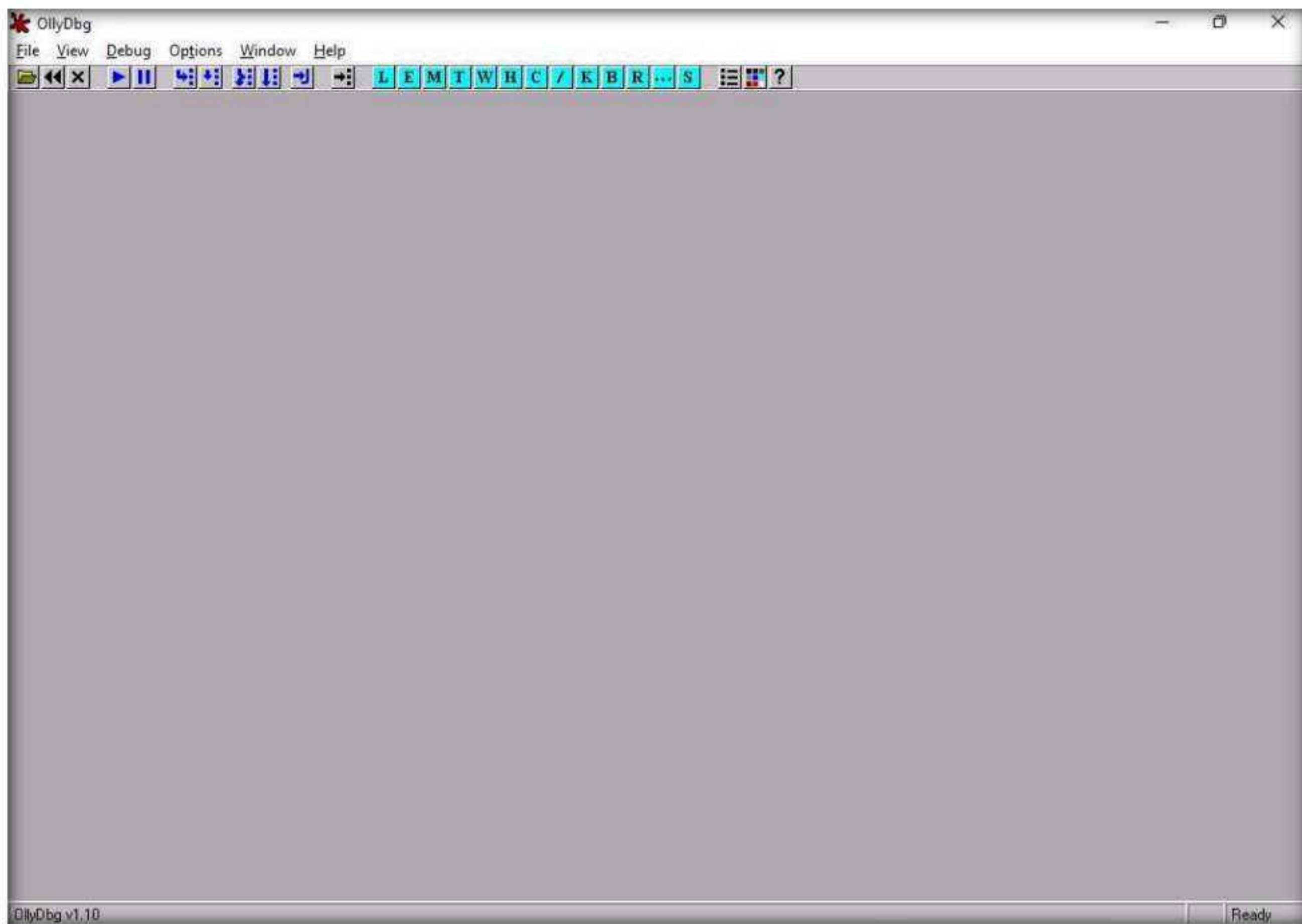
Note: If an Open File - Security Warning pop-up appears, click Run.



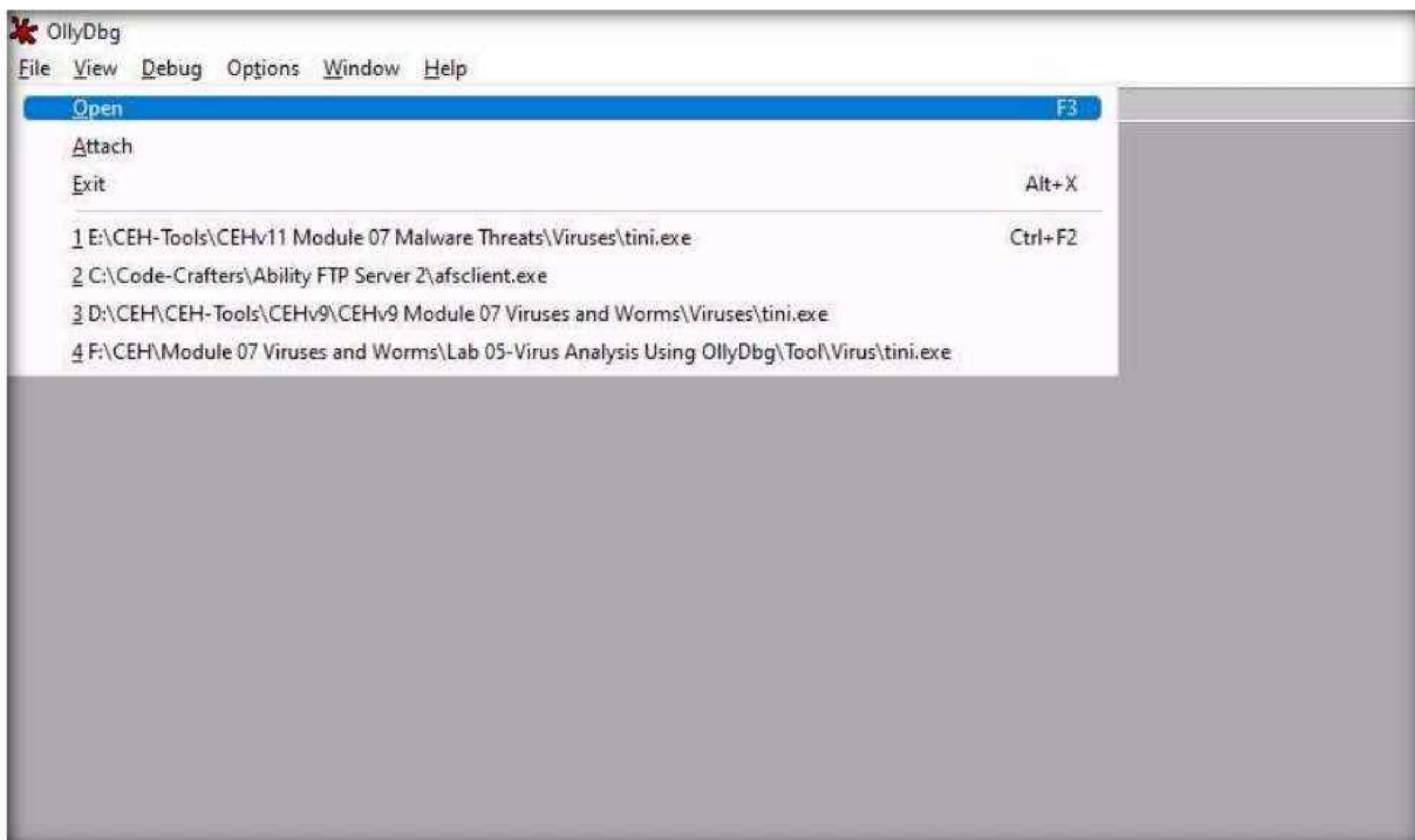
23. If a UDD Directory Absent dialog box appears, click OK.
24. If an OllyDbg warning message appears, for administrative rights, click OK.
25. The **OllyDbg** main window appears, as shown in the screenshot.

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

Module 07 – Malware Threats

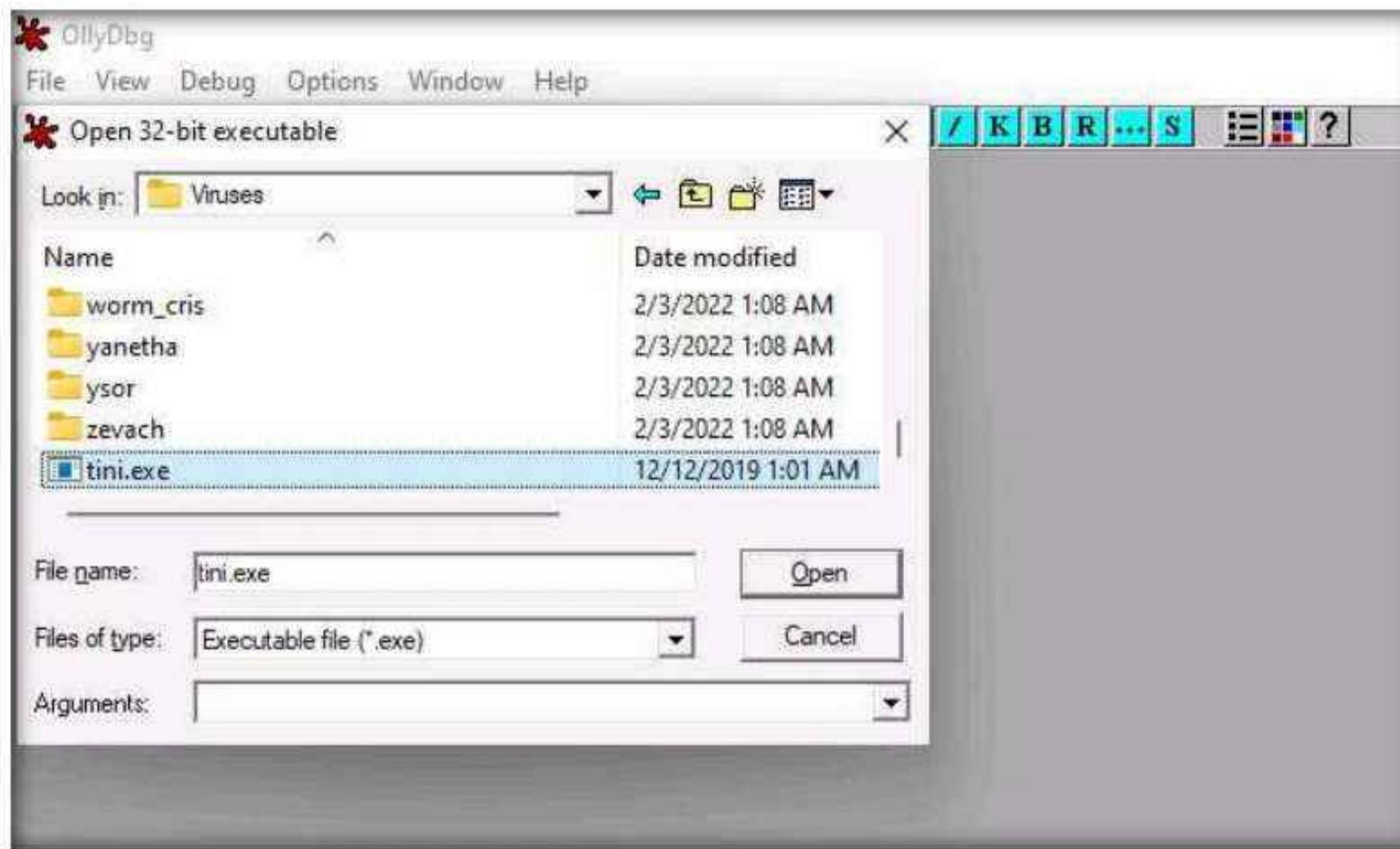


26. Choose **File** from the menu bar, and then choose **Open**.

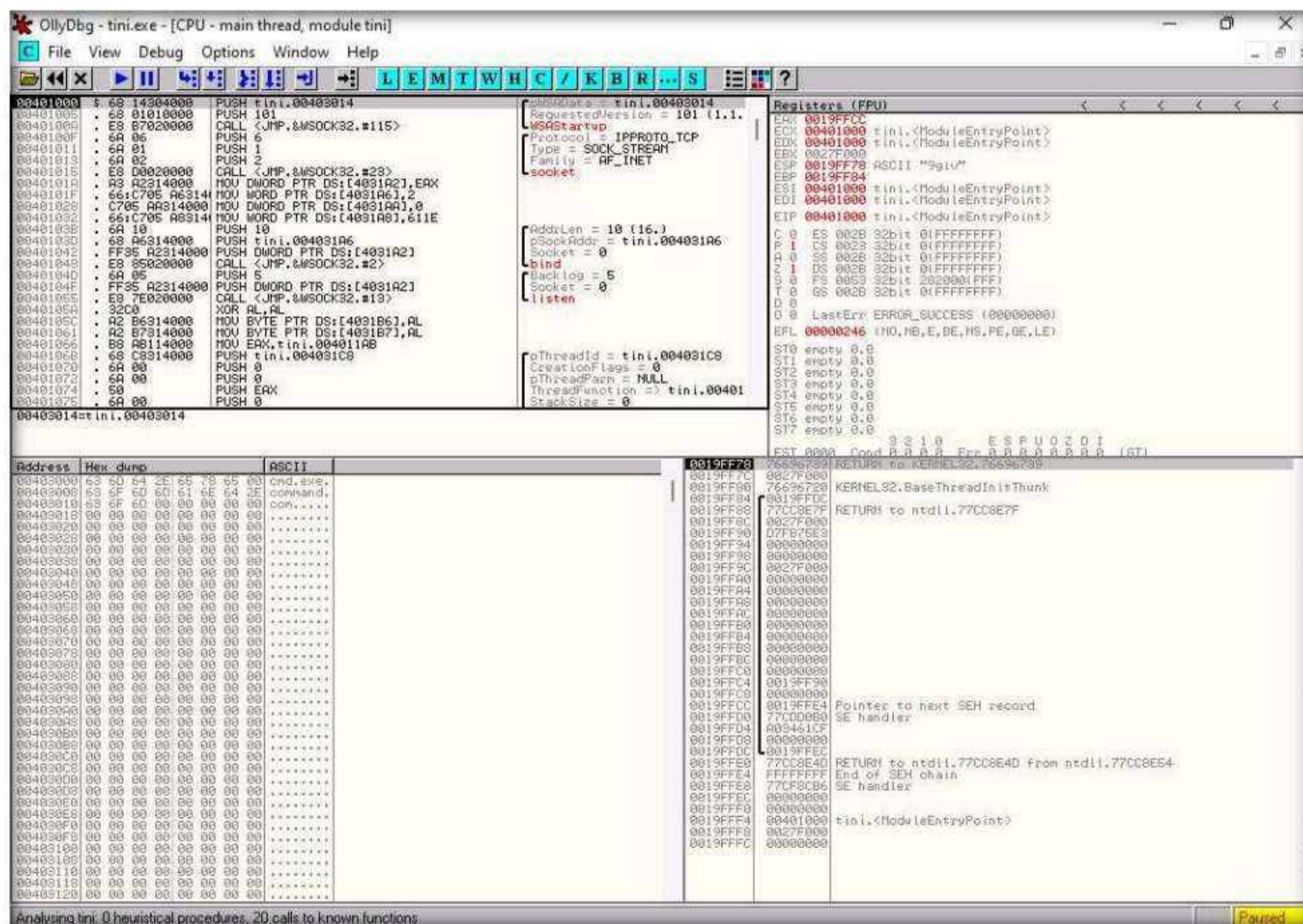


Module 07 – Malware Threats

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.

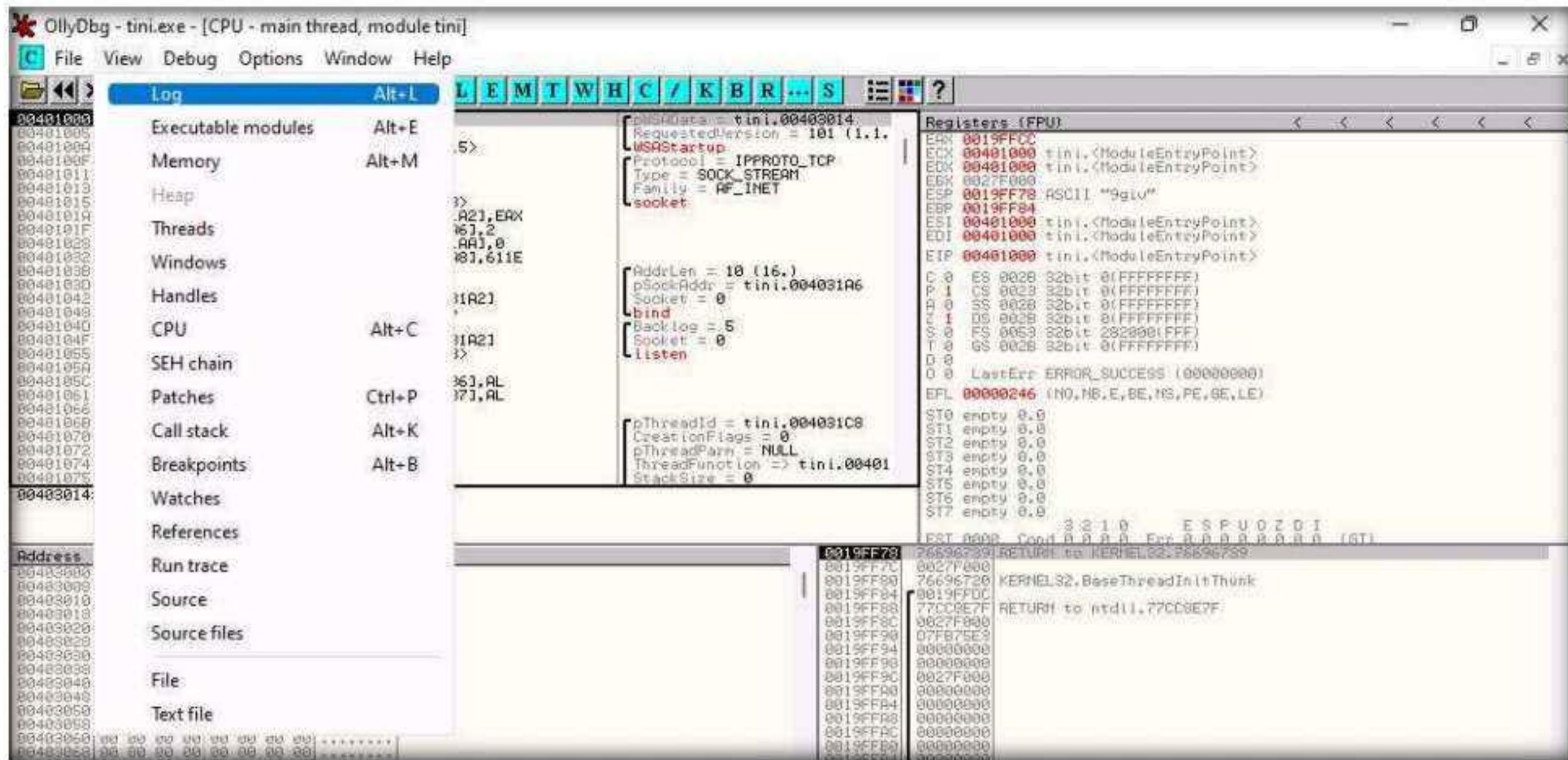


28. The output appears in a window named CPU - main thread, module tini, maximize the window.



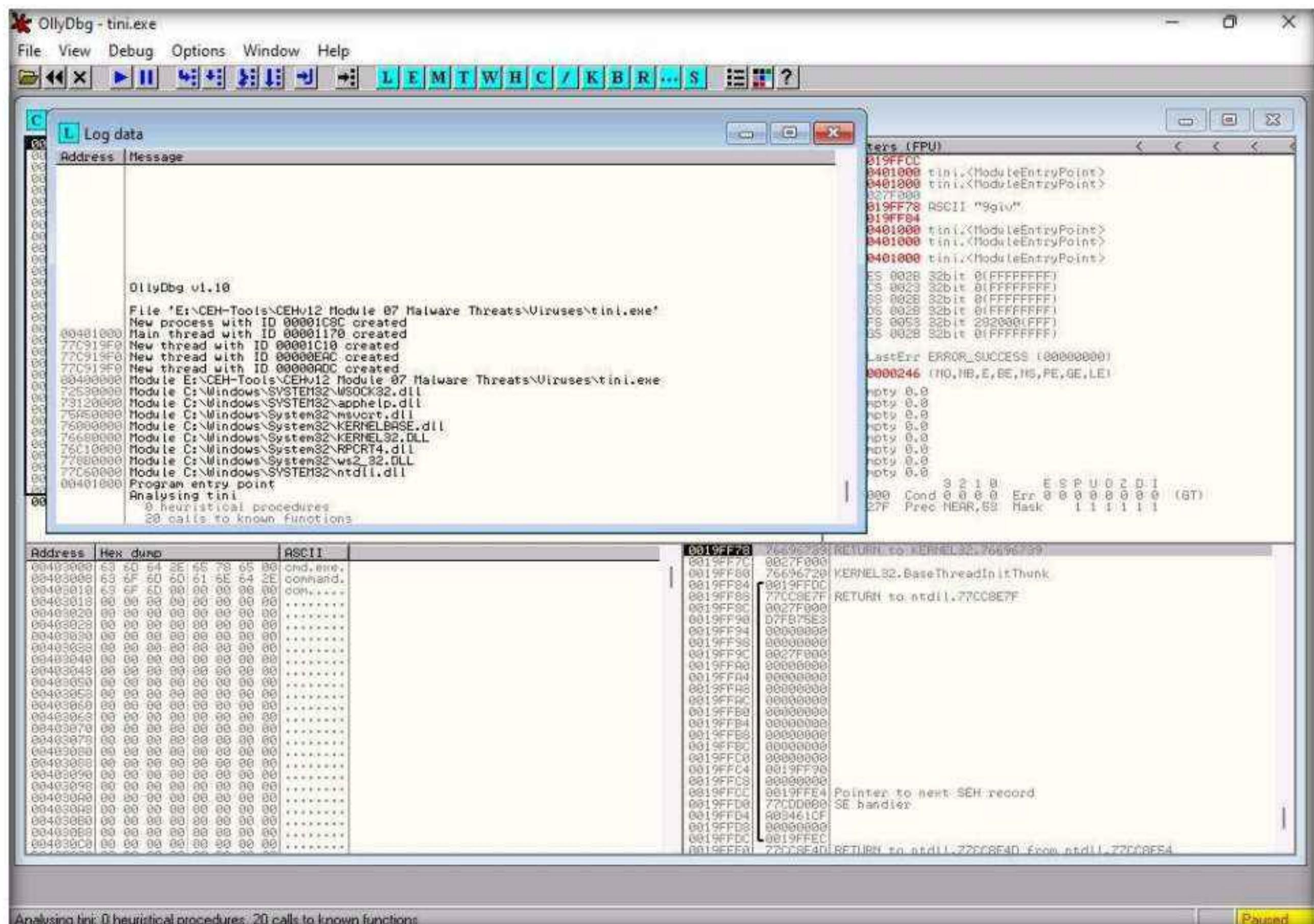
Module 07 – Malware Threats

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



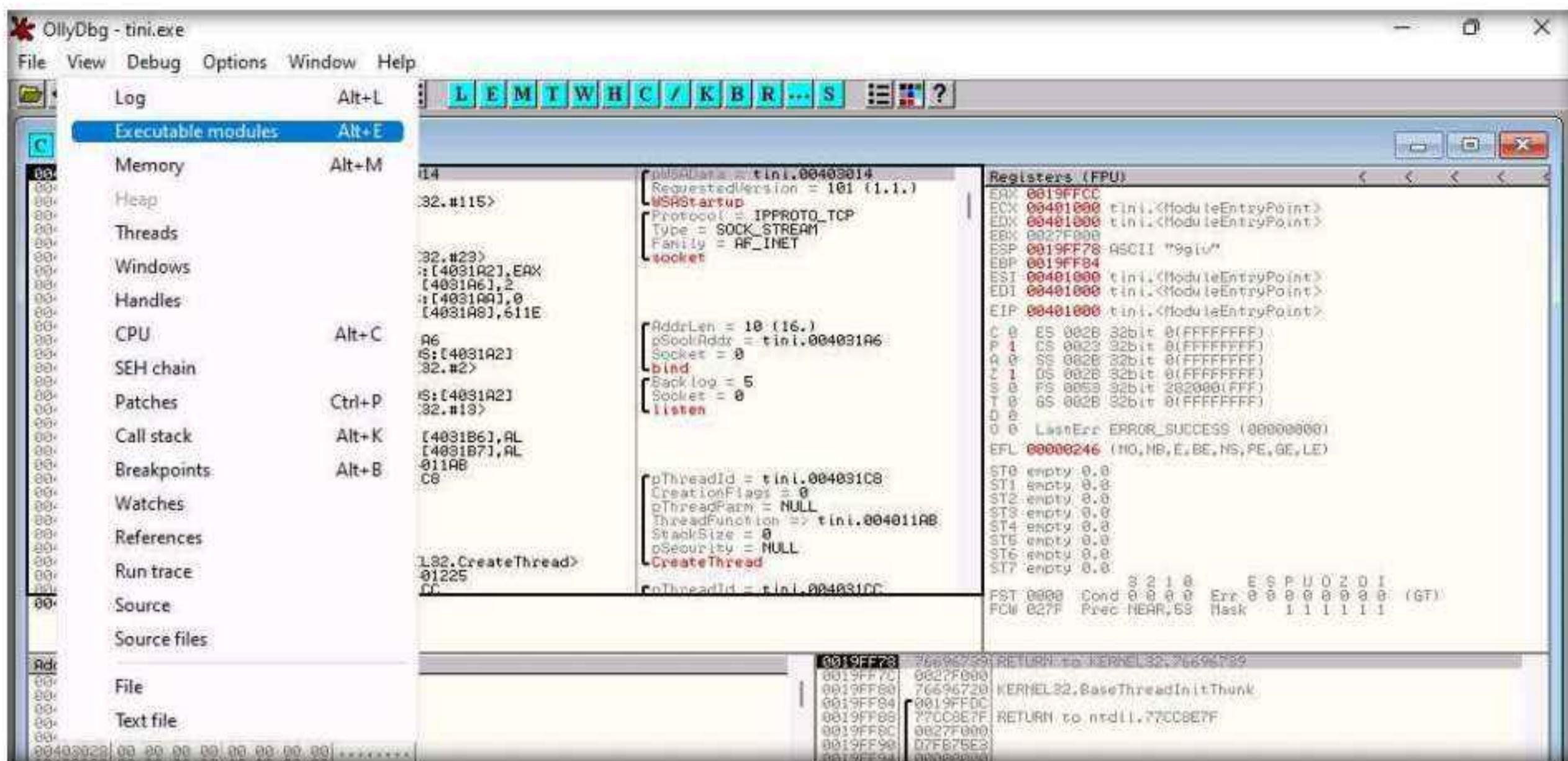
30. A window named **Log data** appears in OllyDbg, displaying the log details, as shown in the screenshot.

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.



Module 07 – Malware Threats

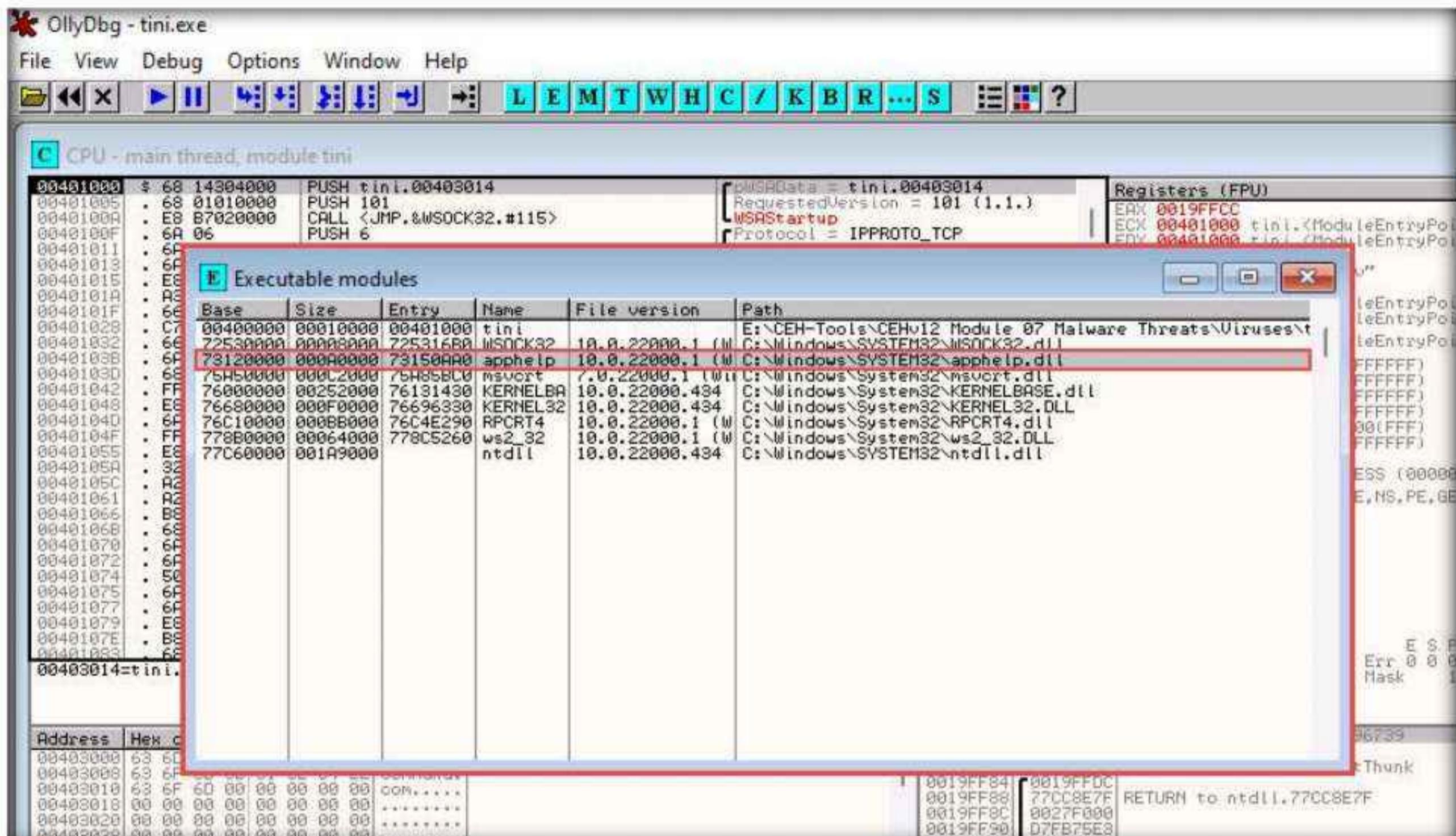
32. Choose **View** in the menu bar, and then choose **Executable modules**.



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

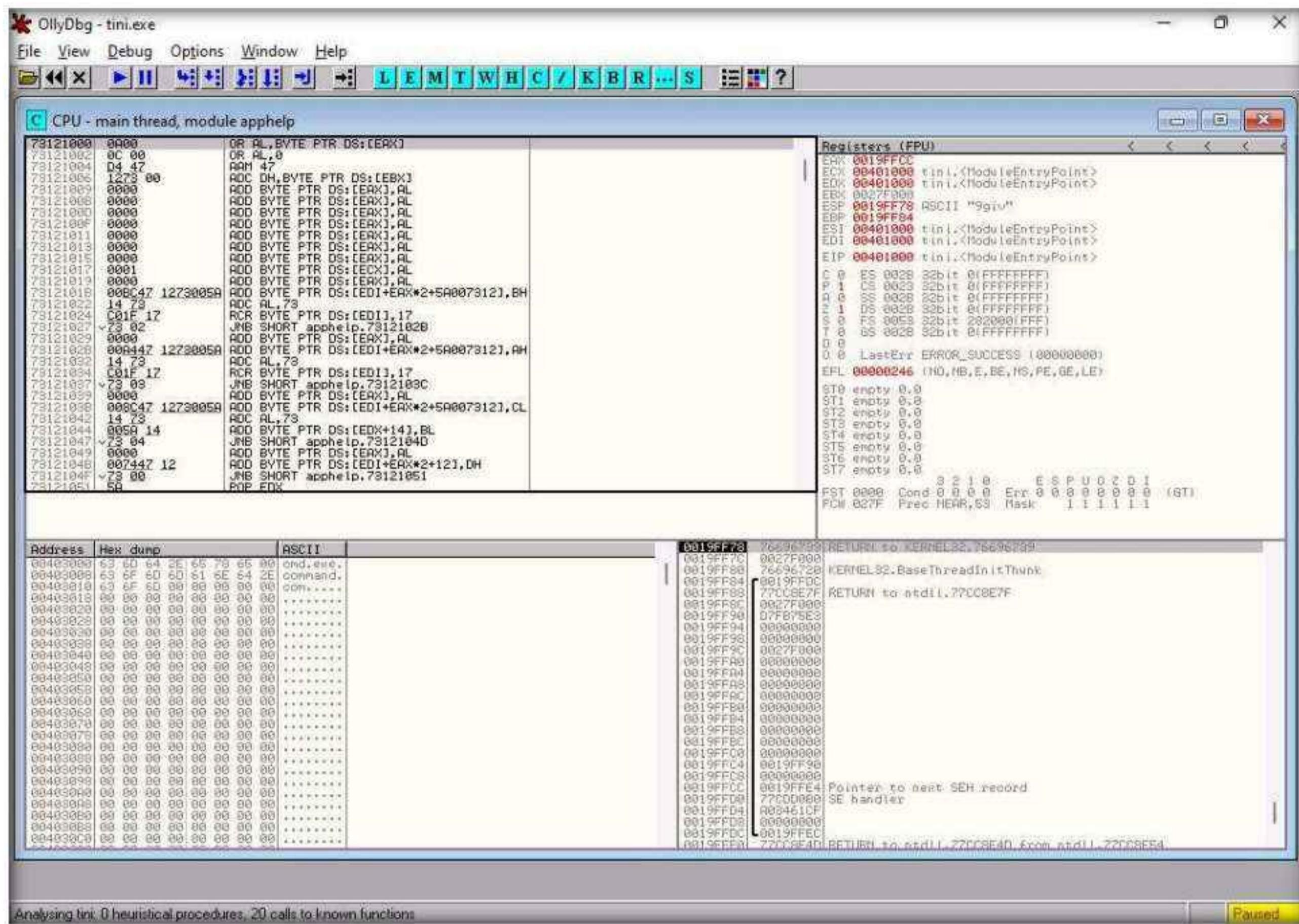
34. Double-click any module to view the complete information of the selected module.

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



Module 07 – Malware Threats

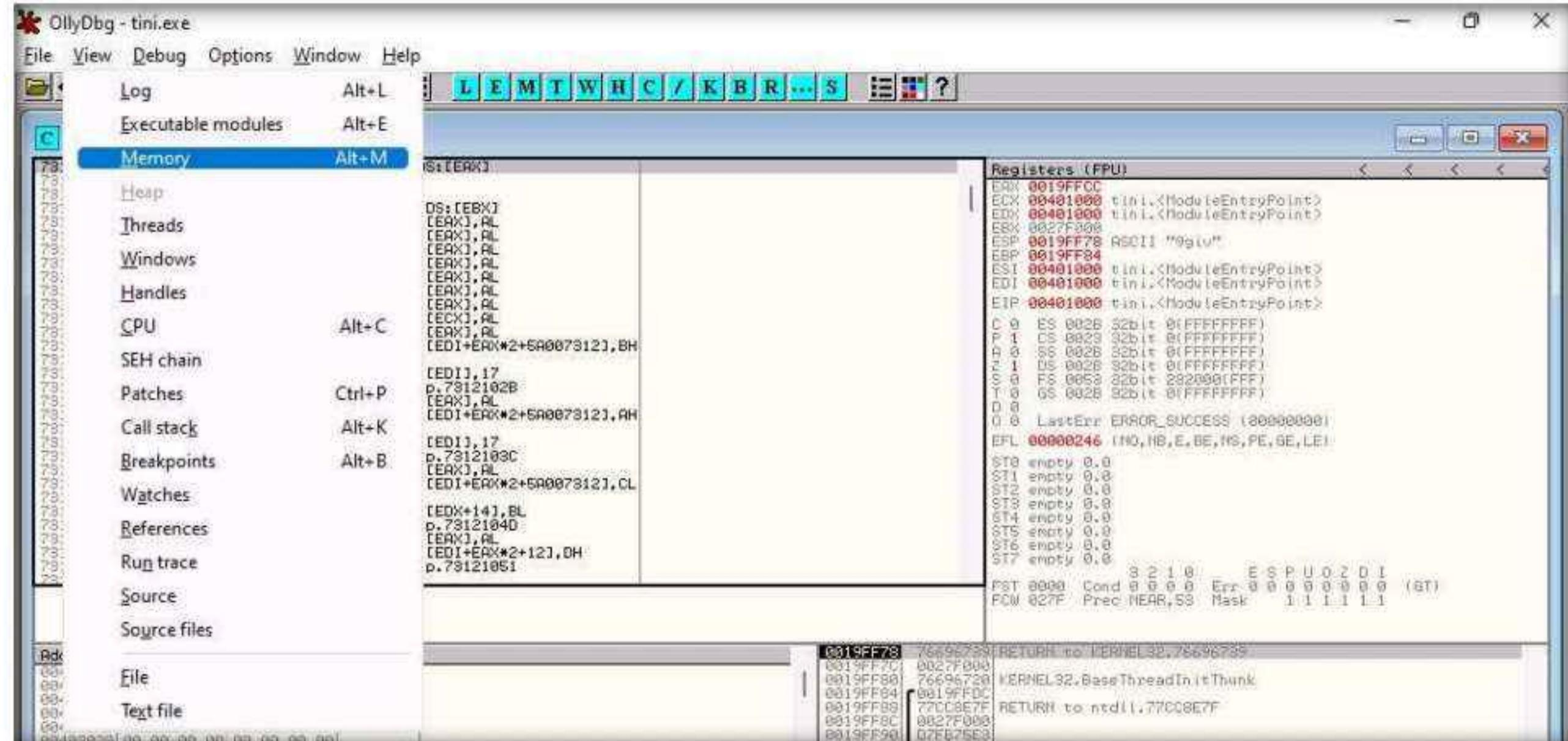
36. This will redirect you to the CPU - main thread window, as shown in the screenshot.



Analyzing tini: 0 heuristic procedures, 20 calls to known functions

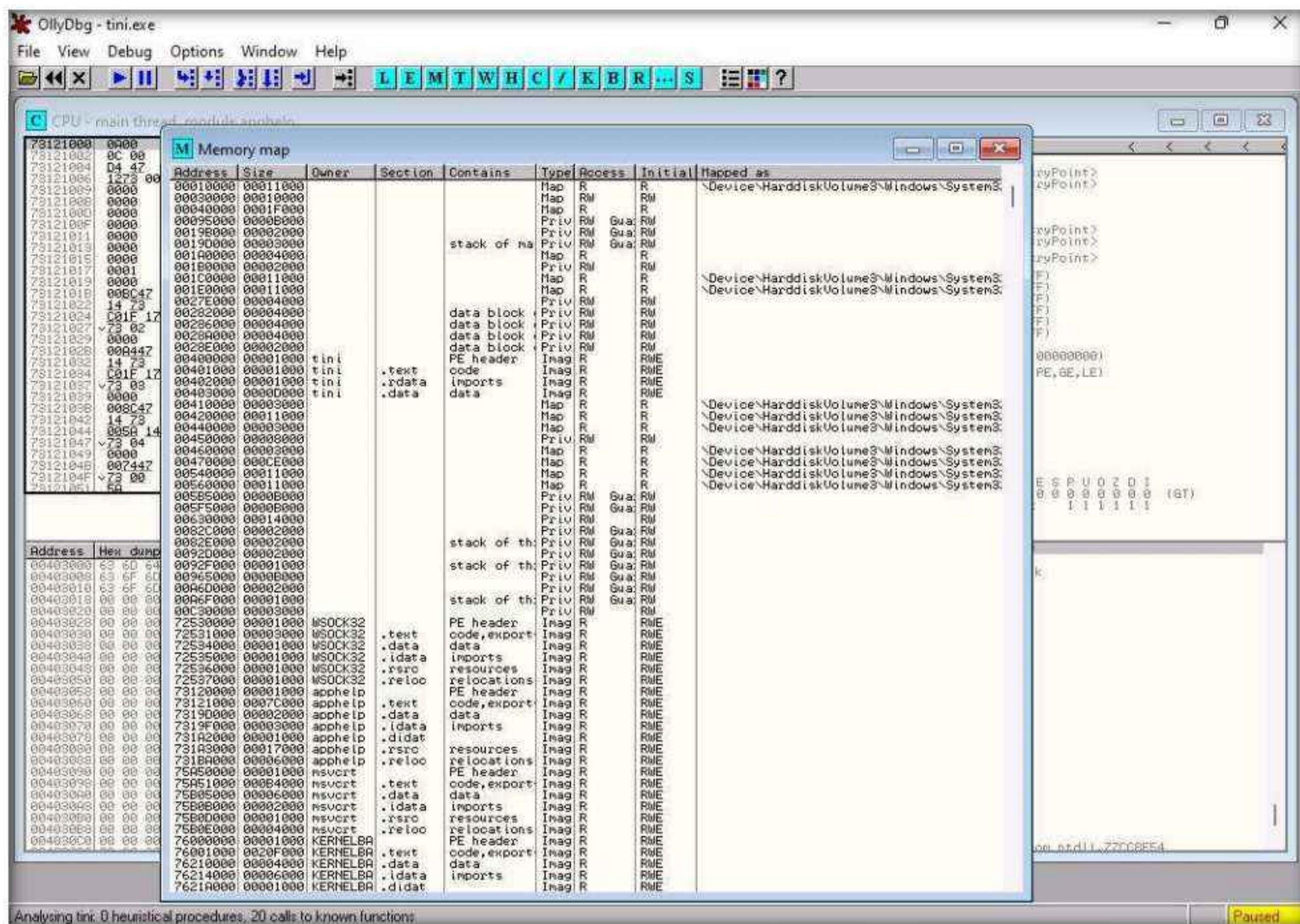
Paused

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

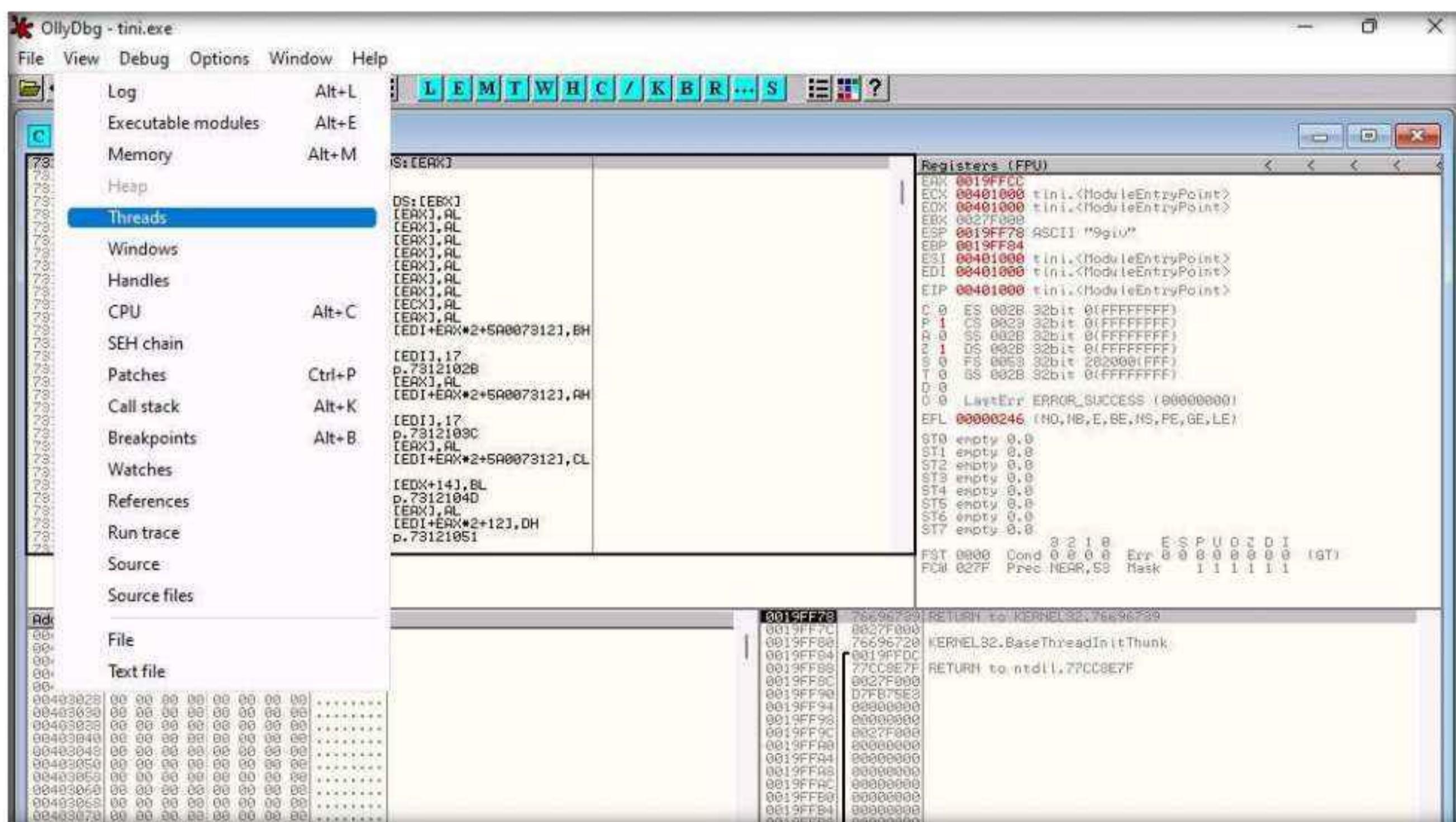


Module 07 – Malware Threats

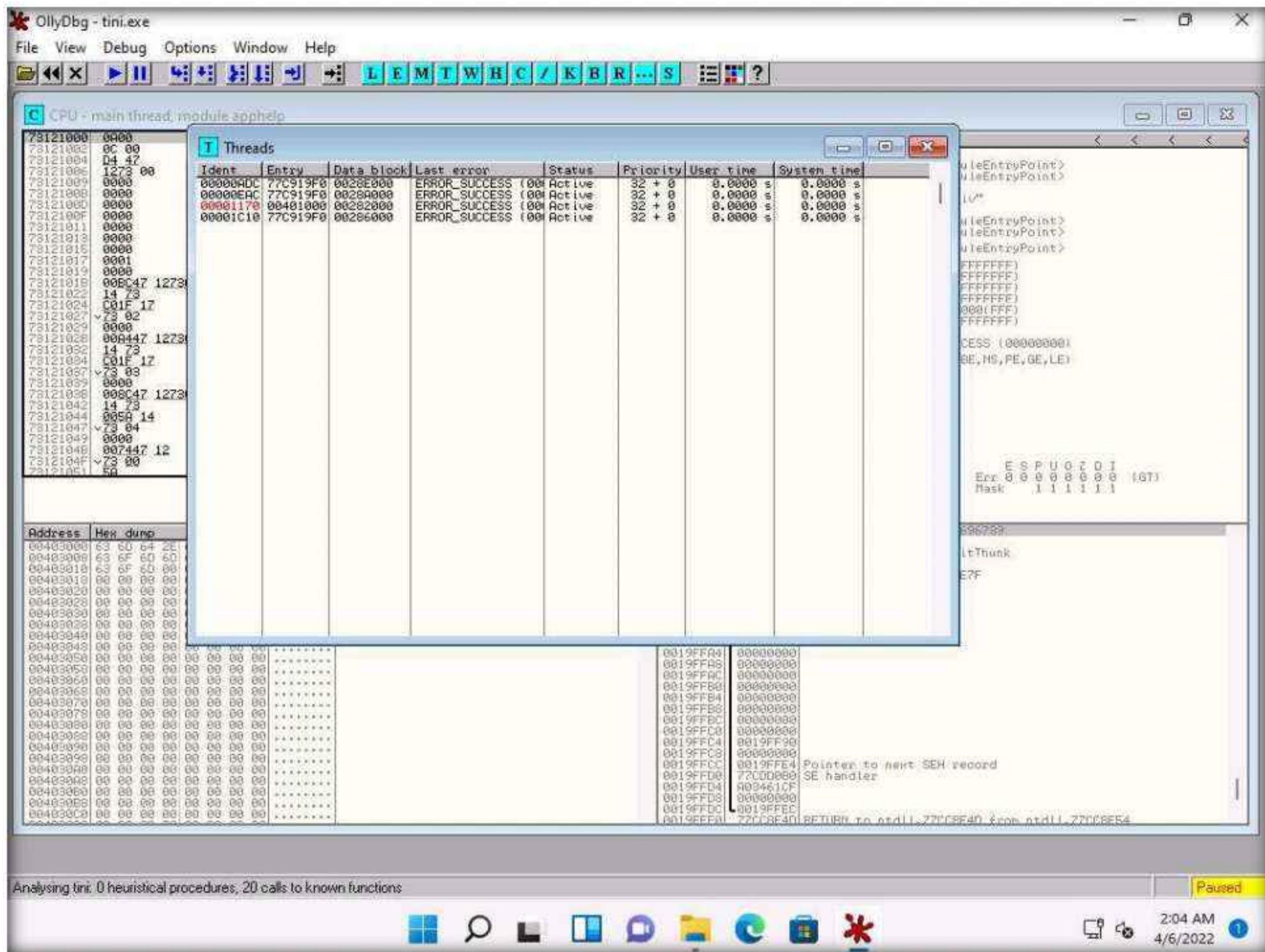
38. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.



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.

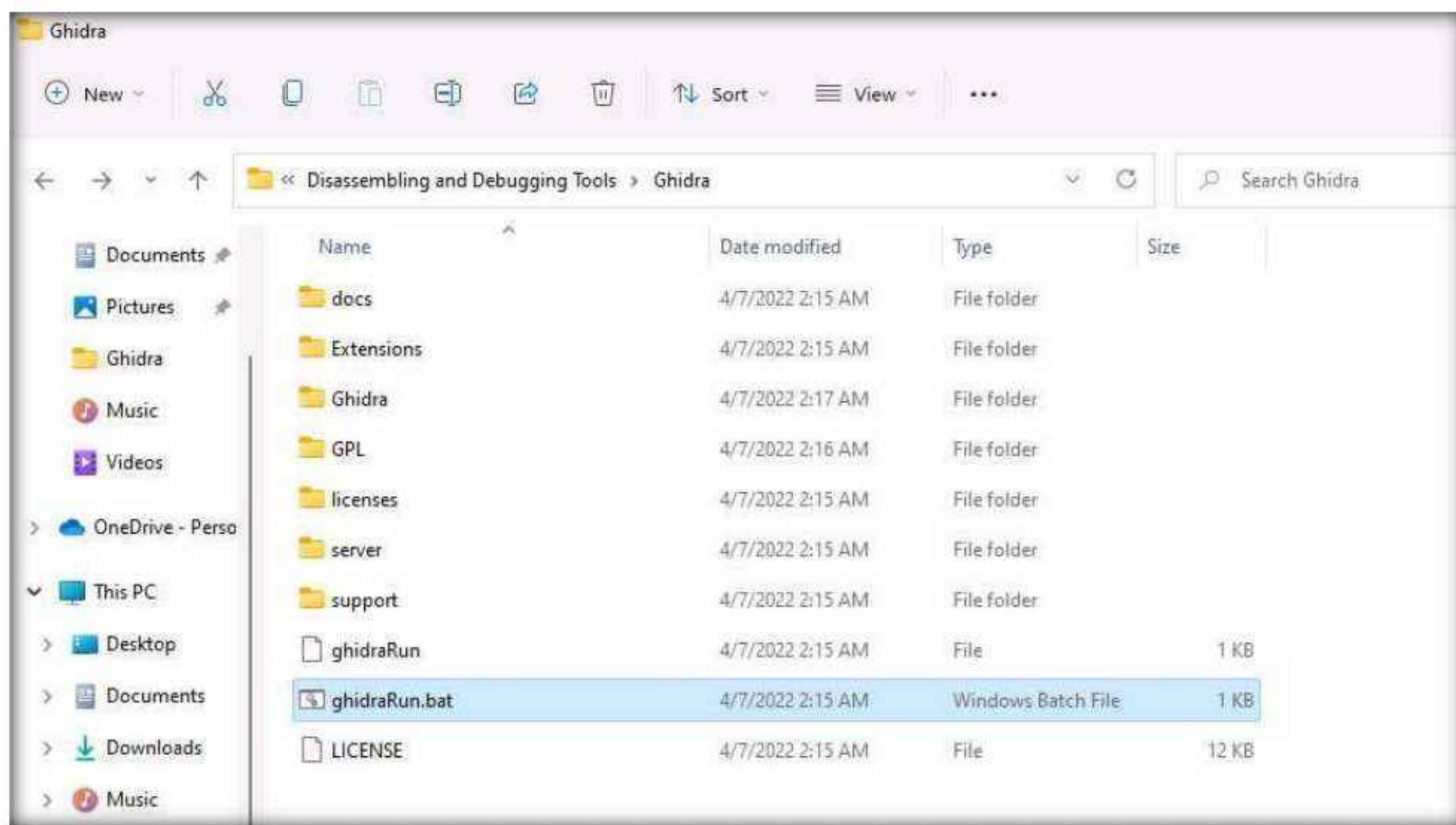
42. Close all open windows.

Task 8: Perform Malware Disassembly using Ghidra

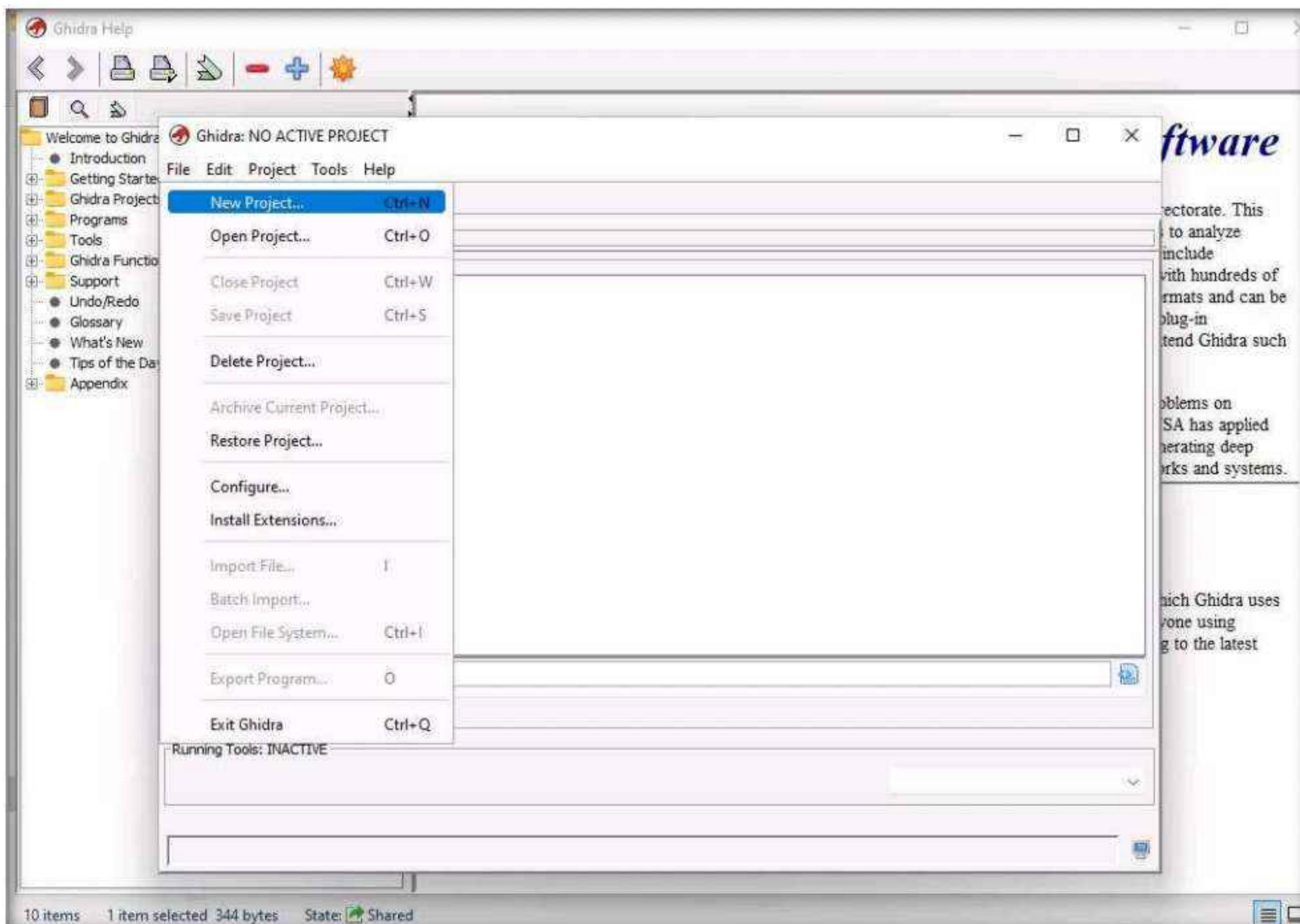
Ghidra is a software reverse engineering (SRE) framework that includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows, MacOS, and Linux. Its capabilities include disassembly, assembly, decompilation, debugging, 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.

- 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**.

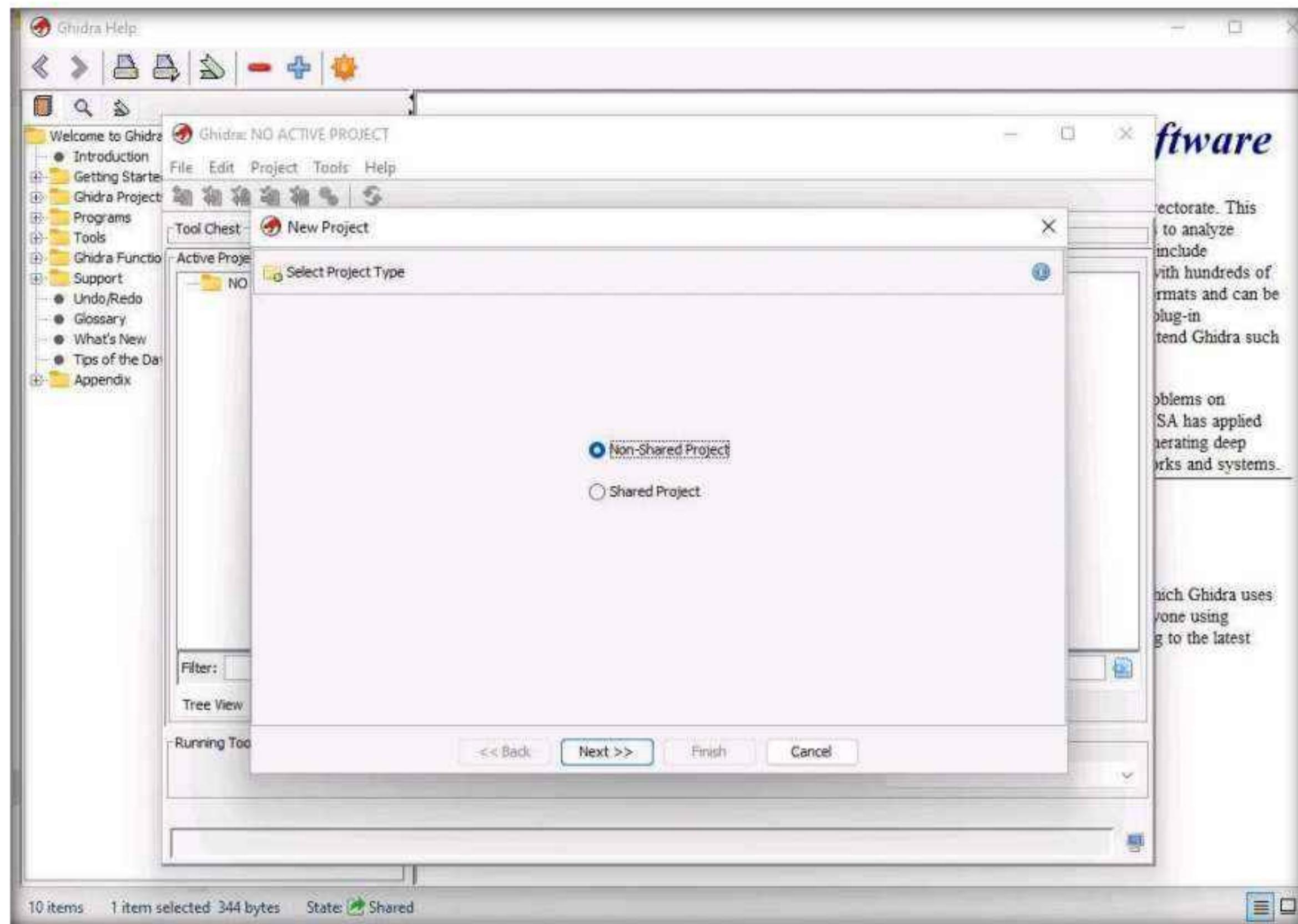


2. After Ghidra initializes, a **Tip of the Day** pop-up appears, click **Close** to close it.
3. **Ghidra: NO ACTIVE PROJECT** window appears, click **File** and select **New Project....**

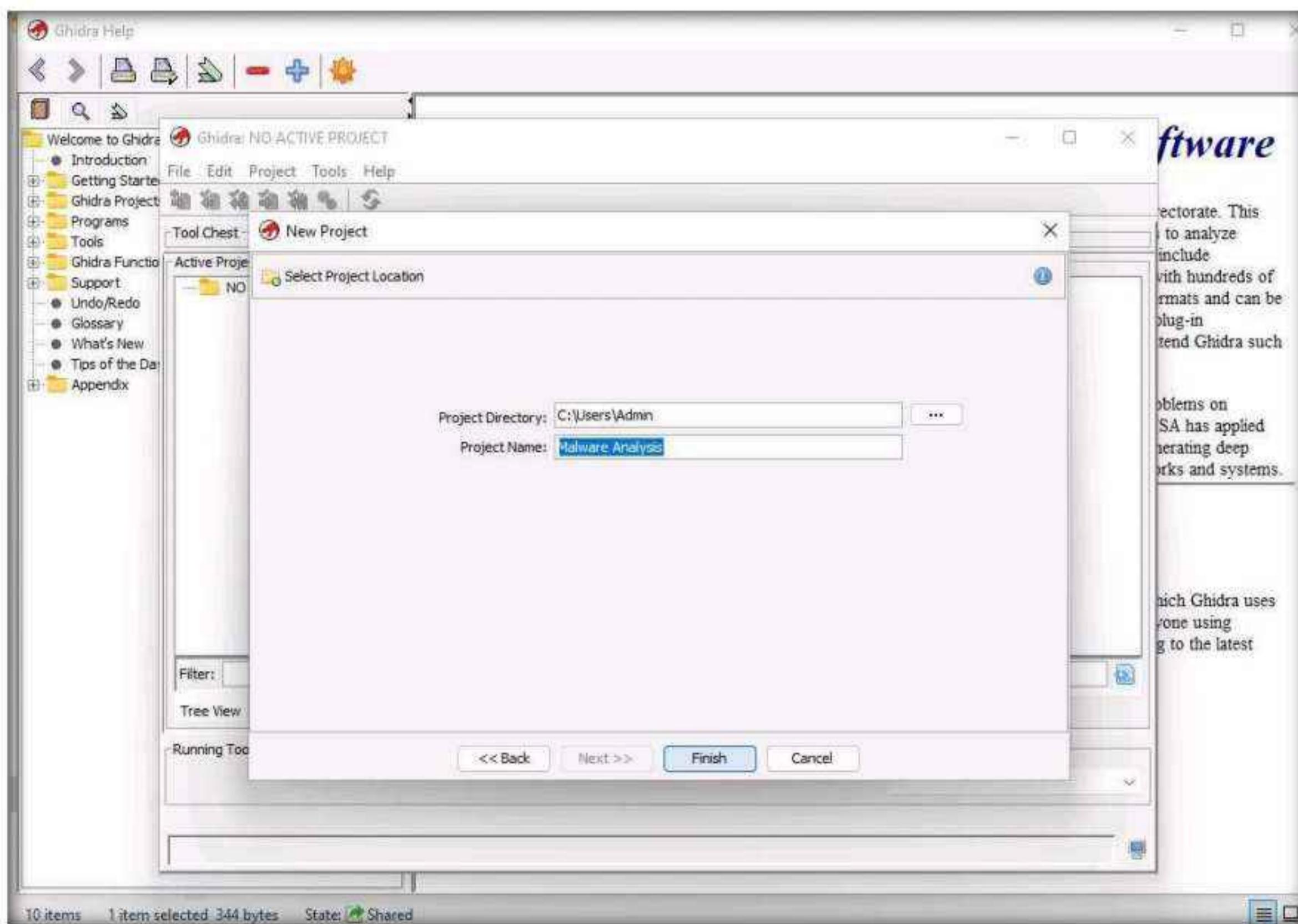


Module 07 – Malware Threats

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

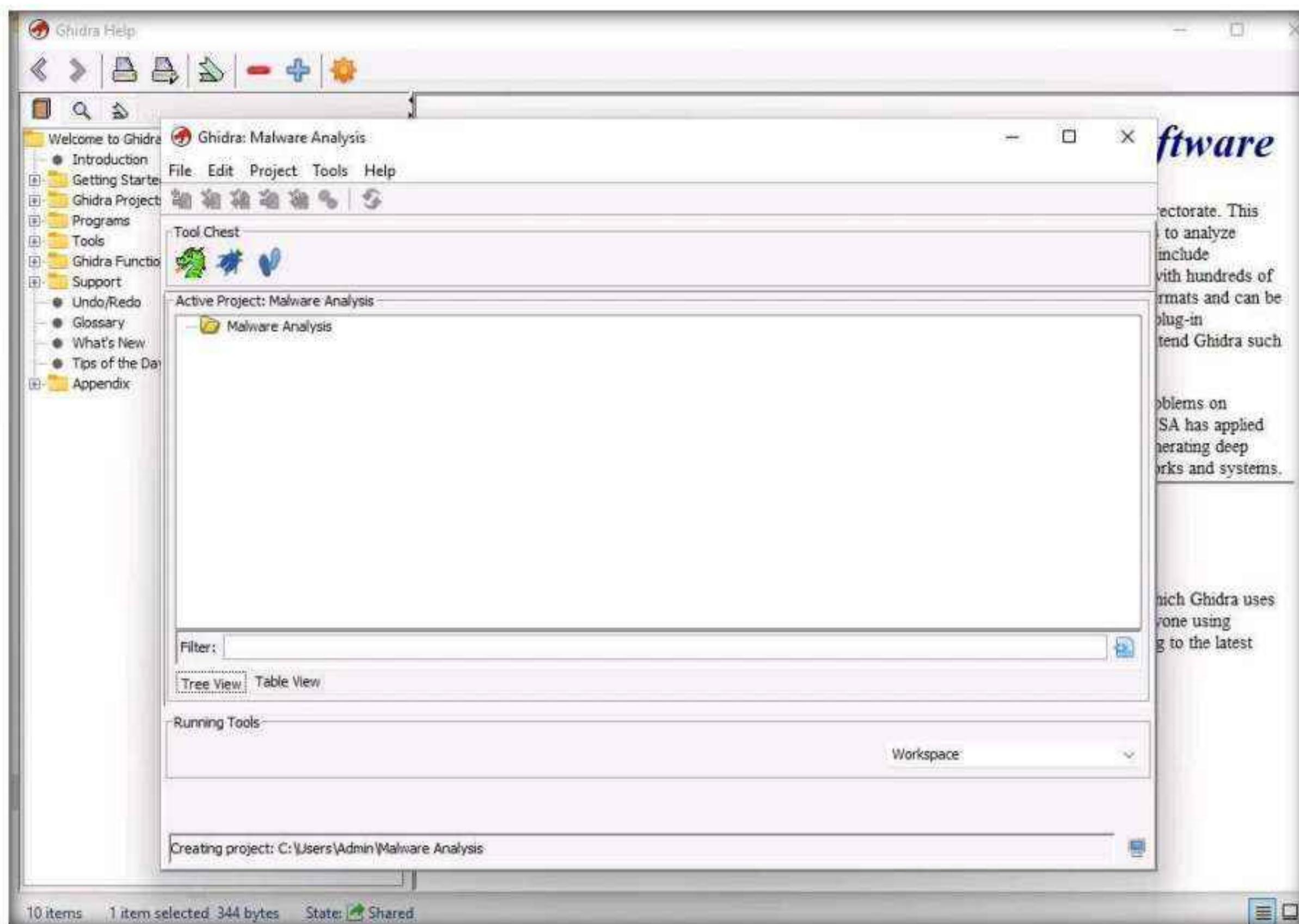


5. In the next window, enter the **Project Name** as **Malware Analysis** and click **Finish**.

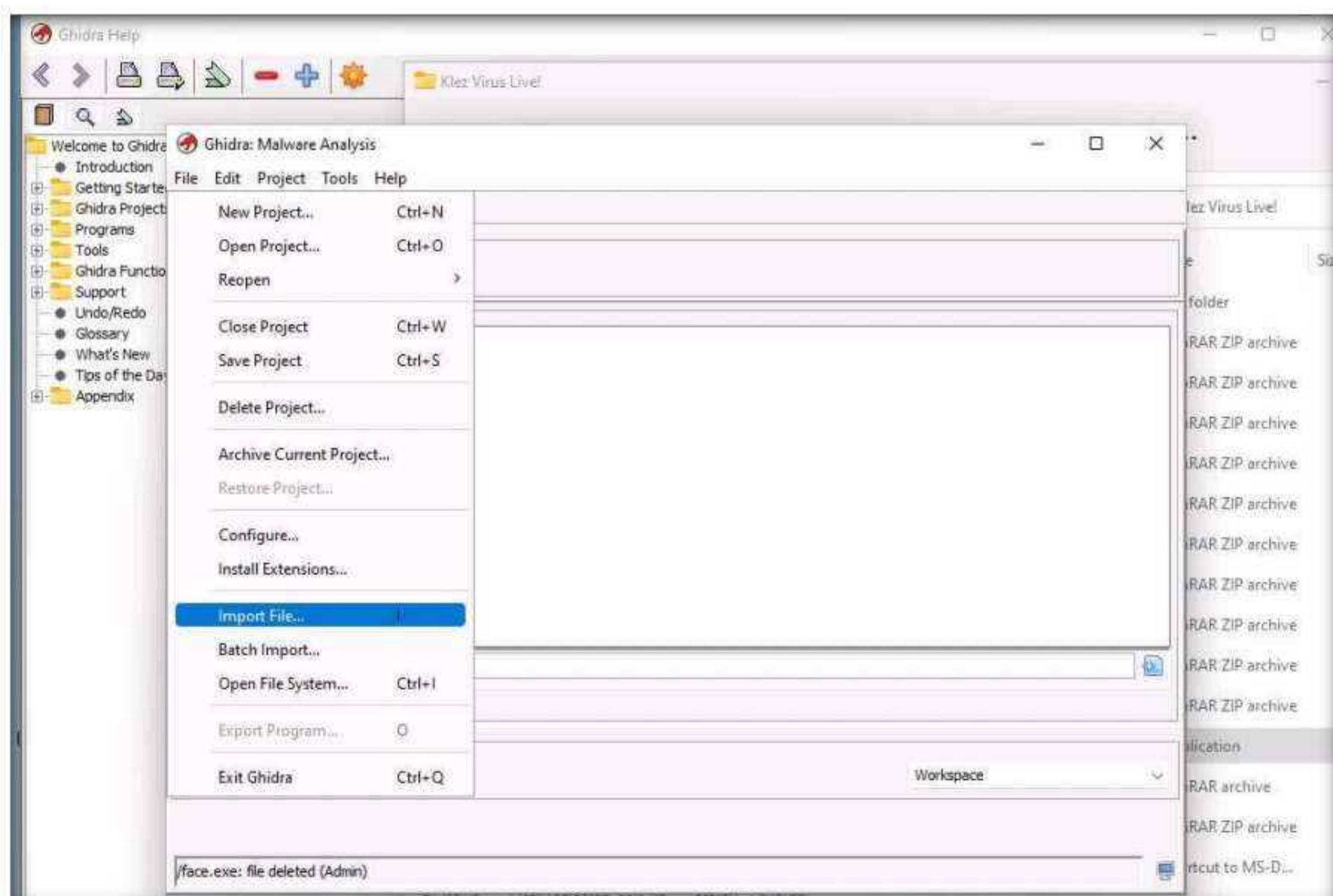


Module 07 – Malware Threats

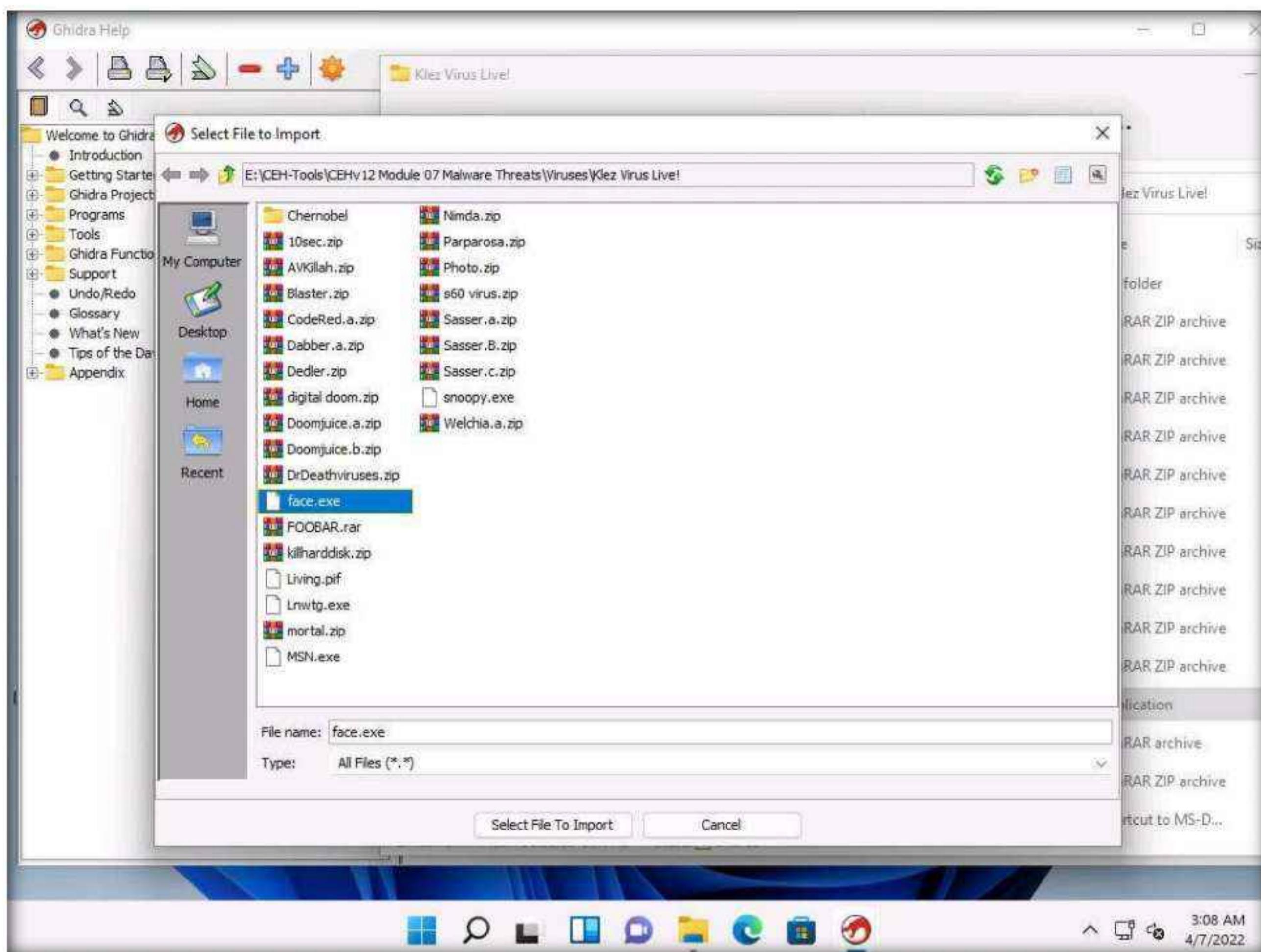
6. A new project with the name as **Malware Analysis** has been created, as shown in the screenshot.



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



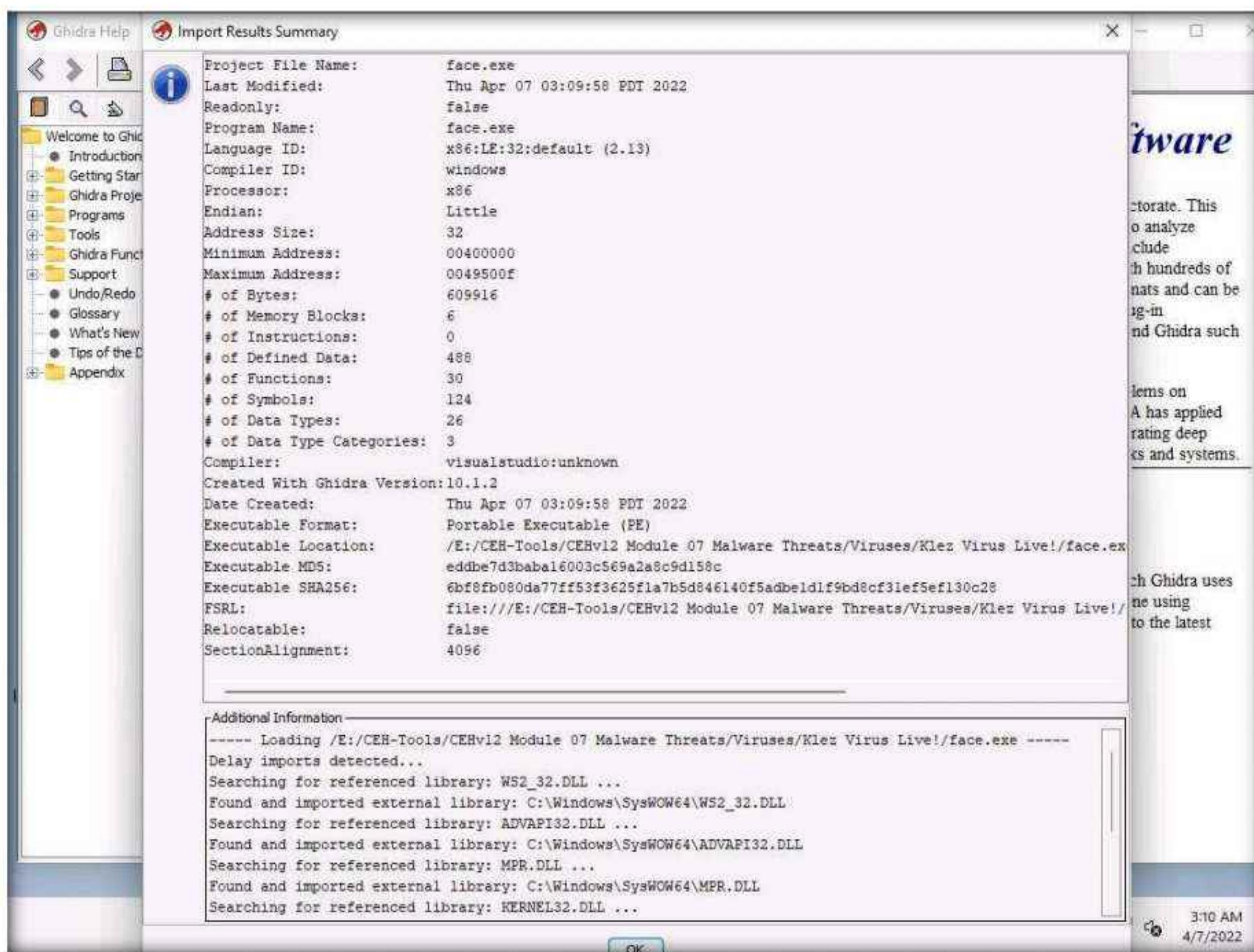
8. Select File to Import window appears, navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!, select face.exe, and click Select File to Import.



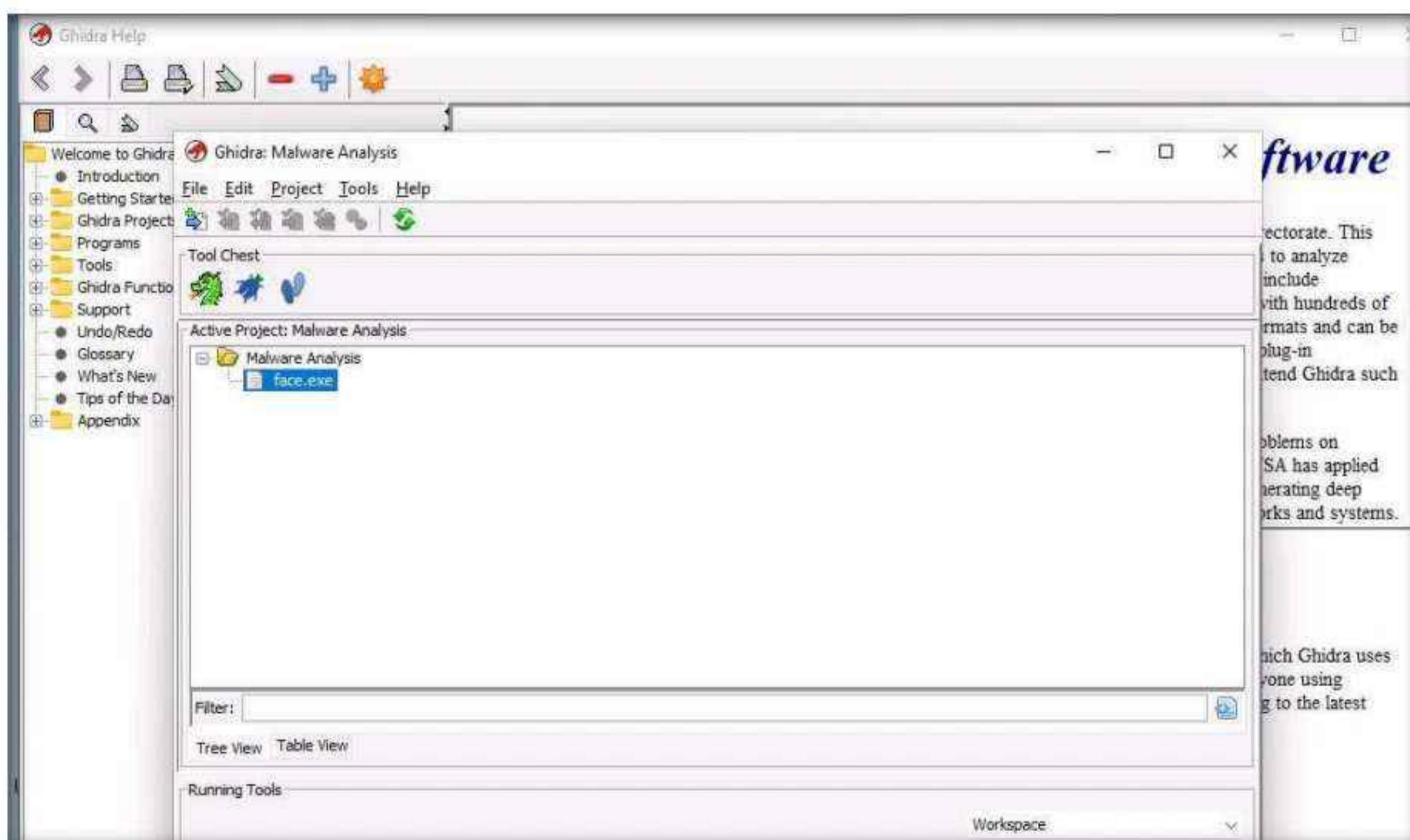
9. Import window appears, click OK.

Module 07 – Malware Threats

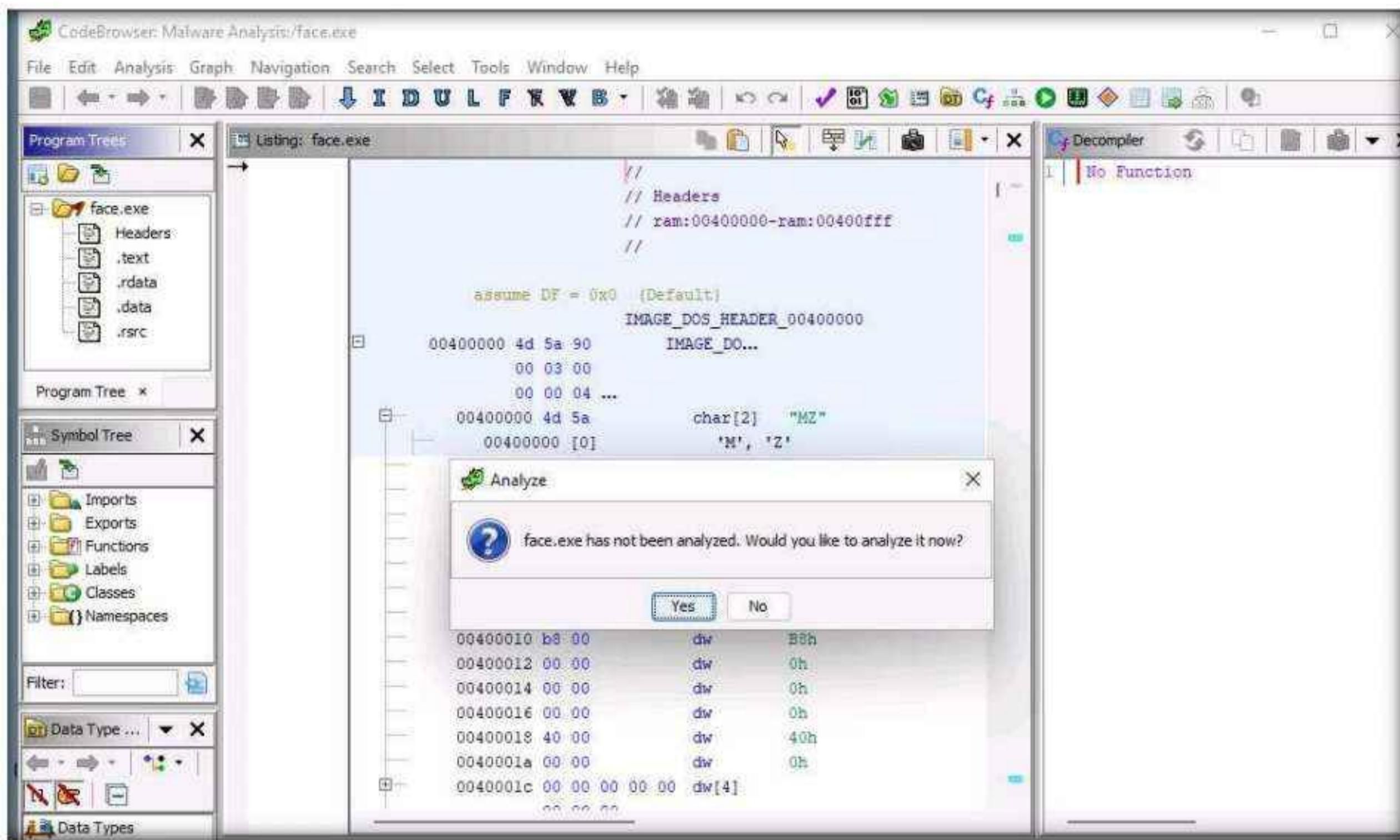
10. After the completion of file import, Import Results Summary window appears, click OK.



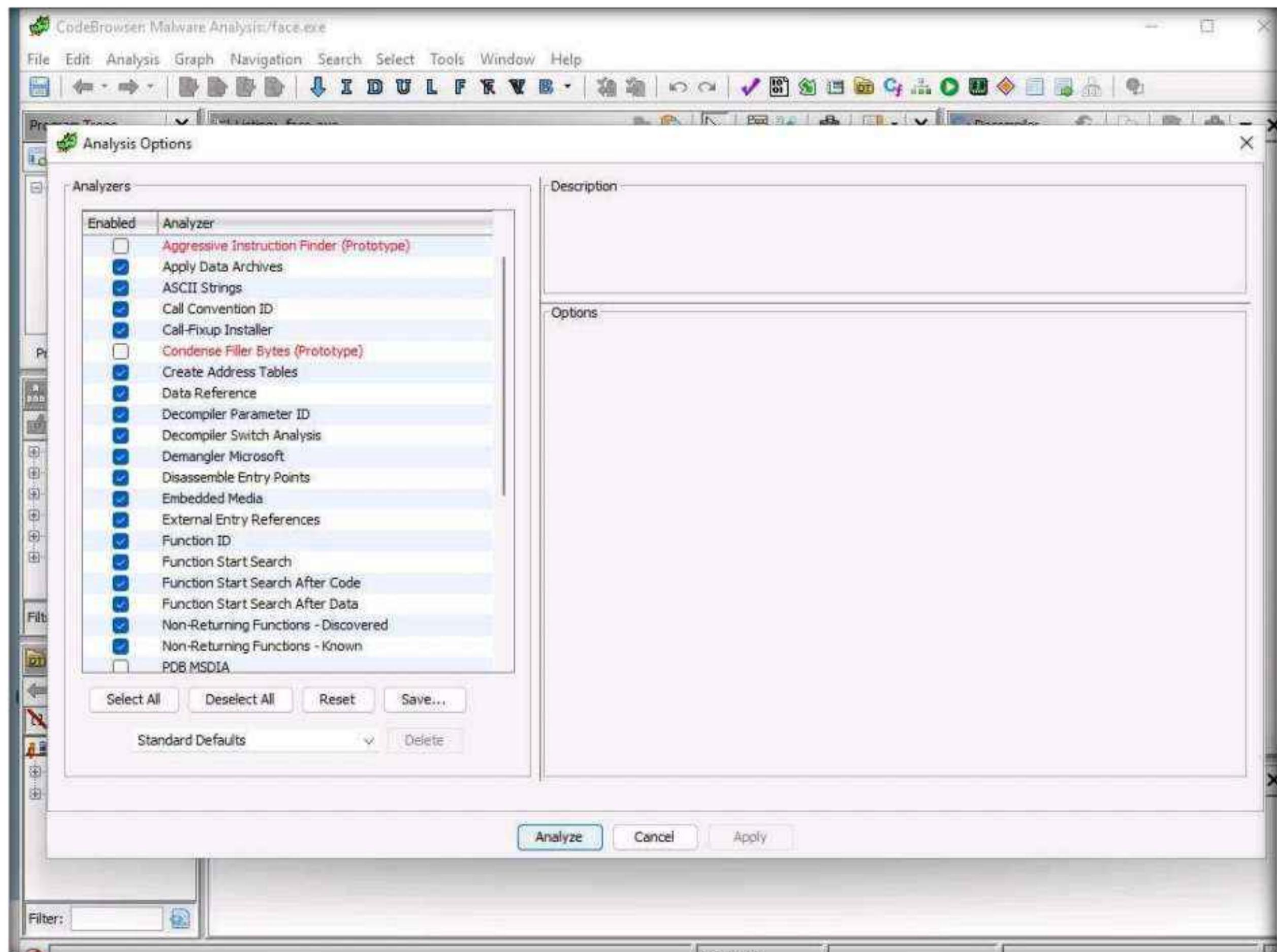
11. You can observe that **Face.exe** is added as a children node under the **Malware Analysis** project. Double-click **Face.exe** node.



12. Analyze pop-up appears, click Yes.



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



Module 07 – Malware Threats

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.

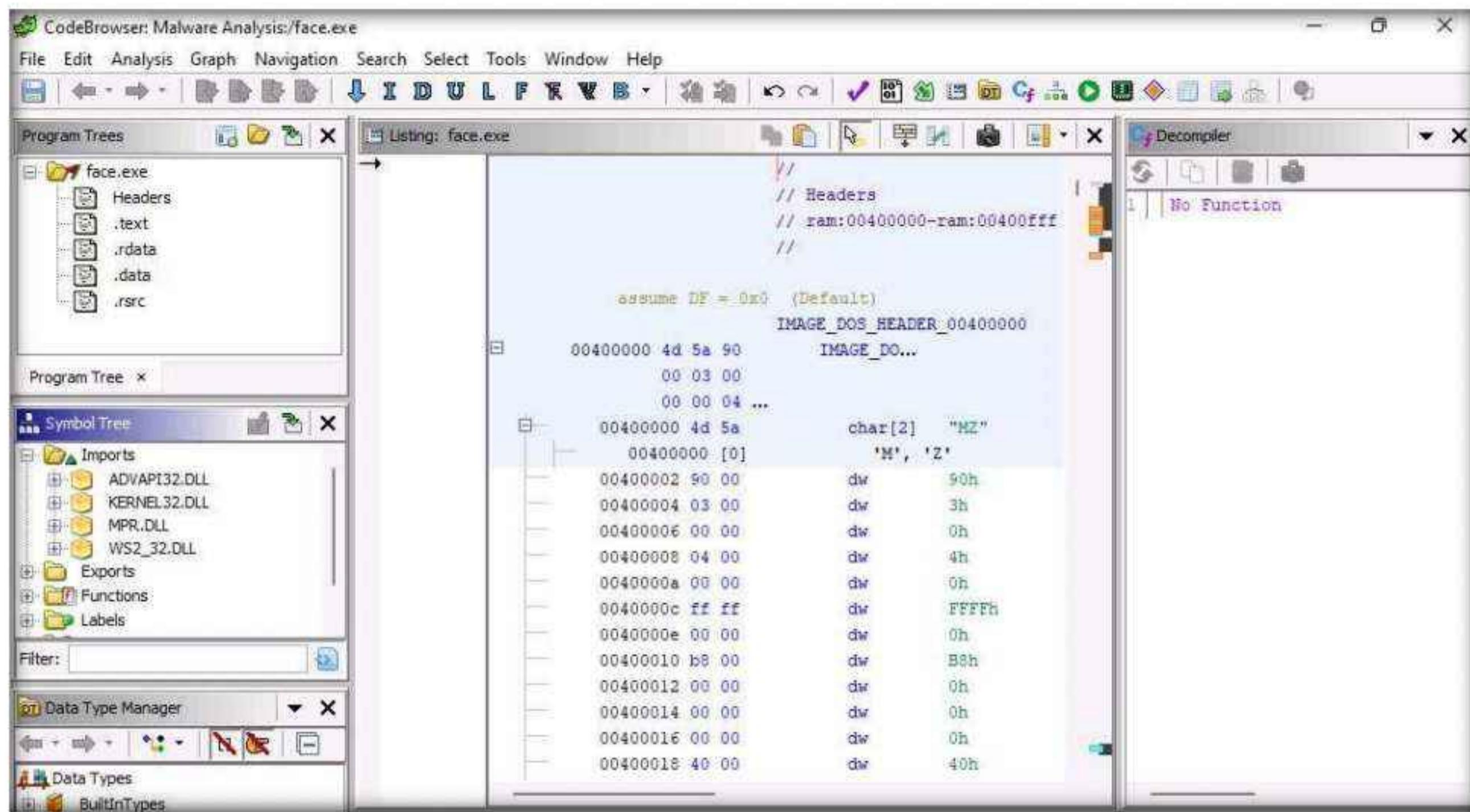
The screenshot shows the CodeBrowser interface for malware analysis. The main window displays the assembly listing for the file 'face.exe'. The assembly code starts with the MZ header and the IMAGE_DOS_HEADER structure. The left pane contains a 'Symbol Tree' showing components like Imports, Exports, Functions, Labels, Classes, and Namespaces. The bottom pane shows the memory dump starting at address 00400000. The status bar at the bottom right indicates the current memory address.

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

This screenshot is similar to the previous one, but the 'Symbol Tree' pane is more detailed, showing expanded sections for Imports, Exports, Functions, Labels, Classes, and Namespaces. The assembly listing and memory dump panes remain the same, displaying the initial bytes of the executable file.

Module 07 – Malware Threats

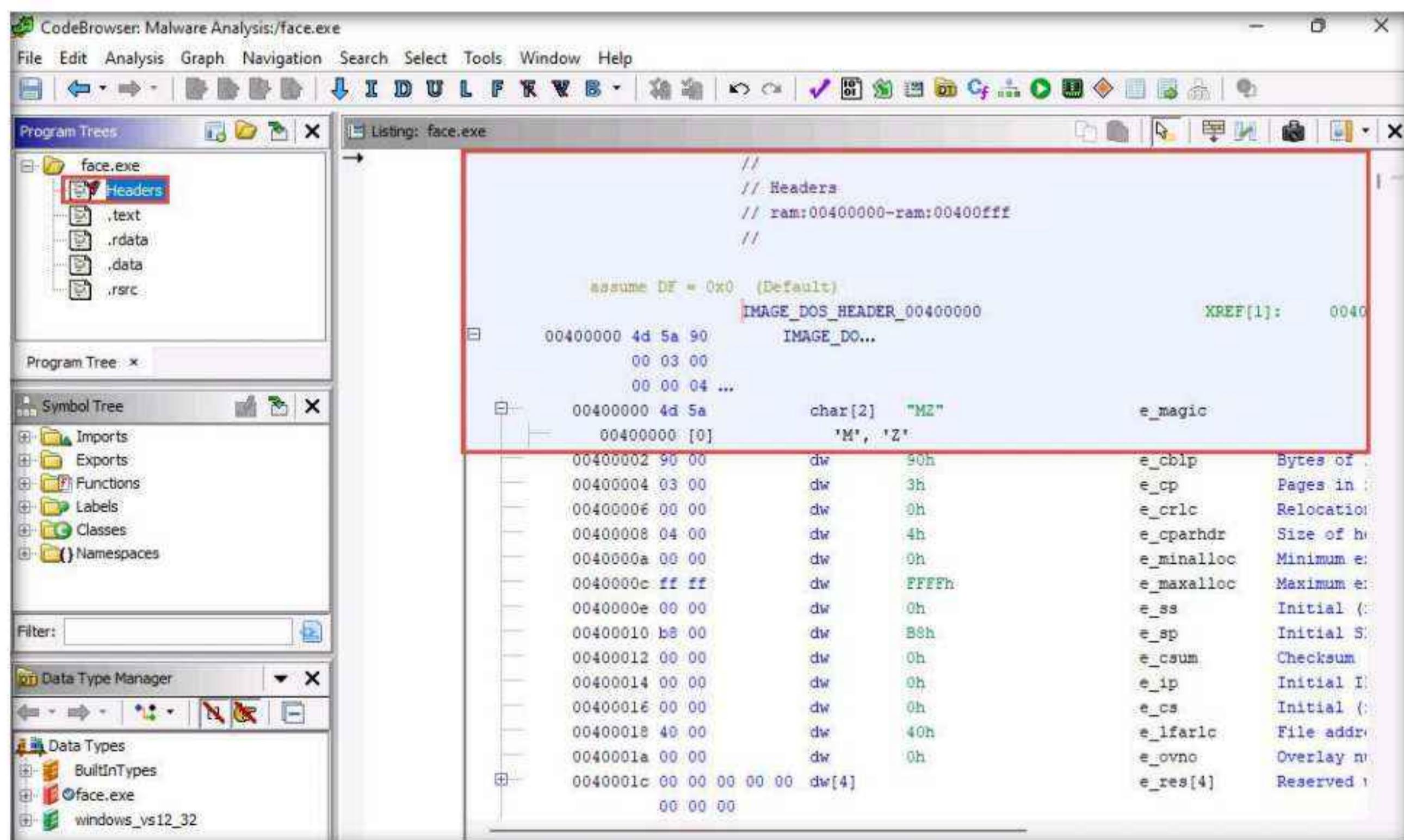
17. Click to expand **Imports** node and you can view the DLL files of face.exe.



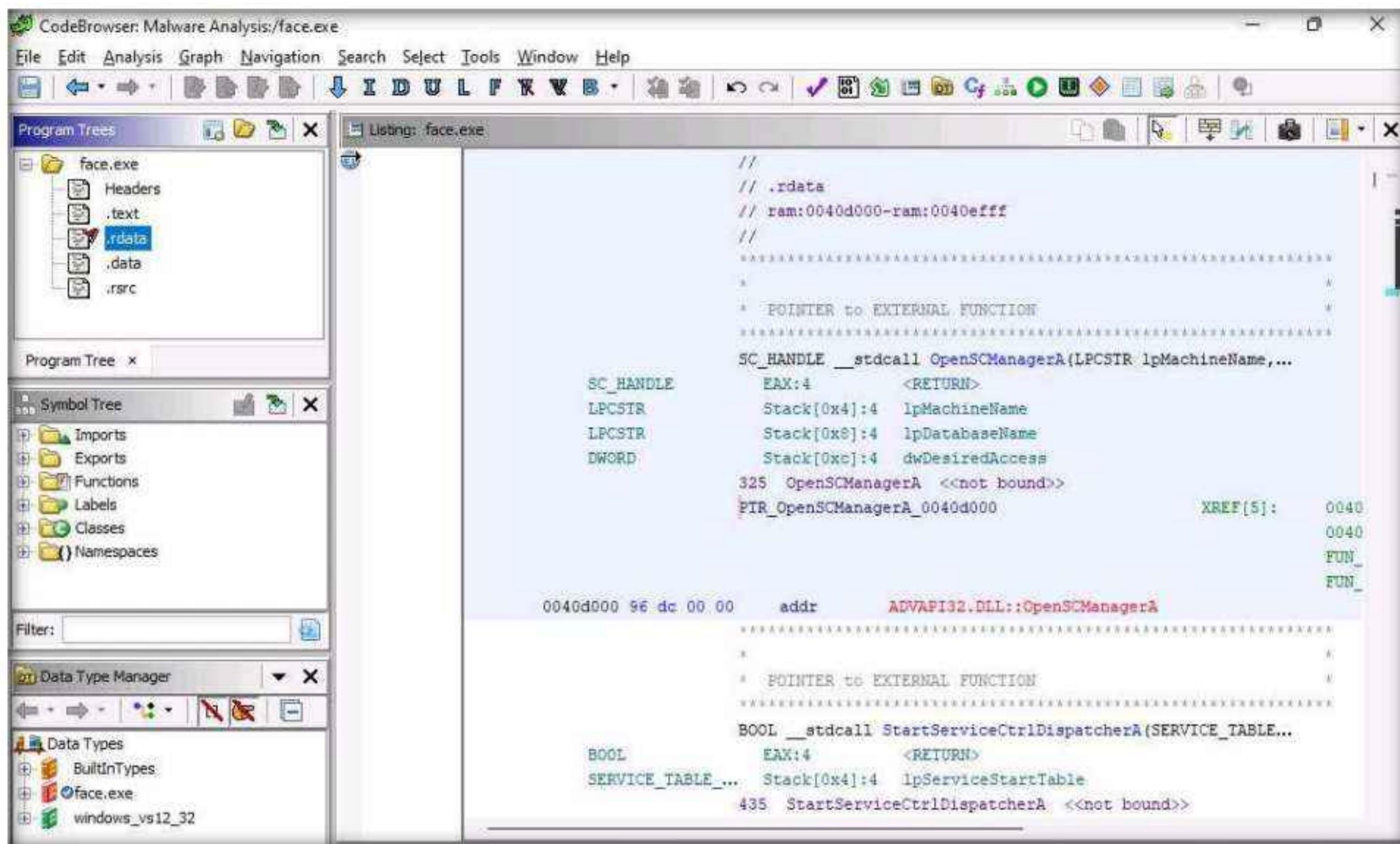
18. Similarly, you can view other components under Symbol Tree to obtain additional information on face.exe.

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	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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 Baselingining:** Baselingining 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.

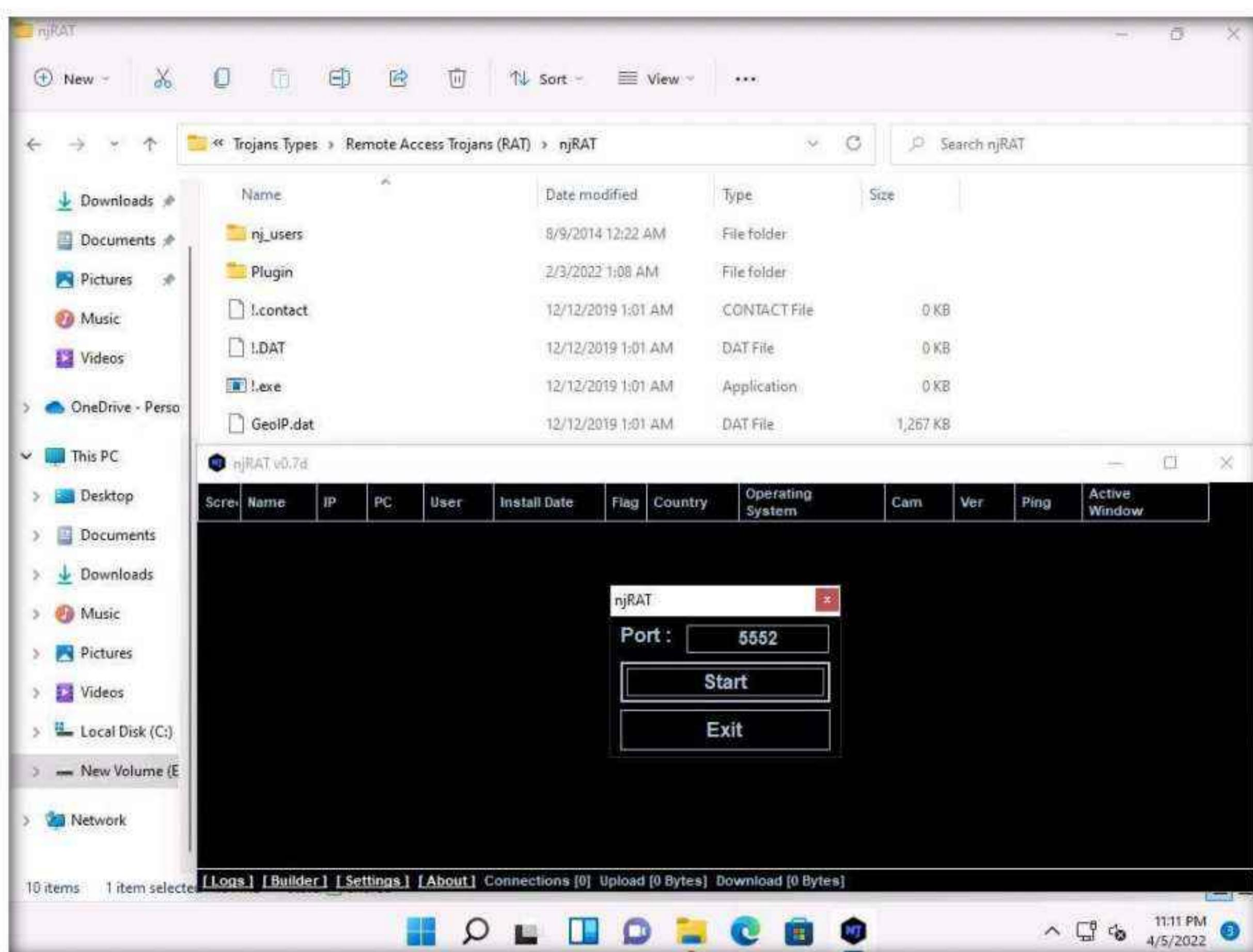
In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

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

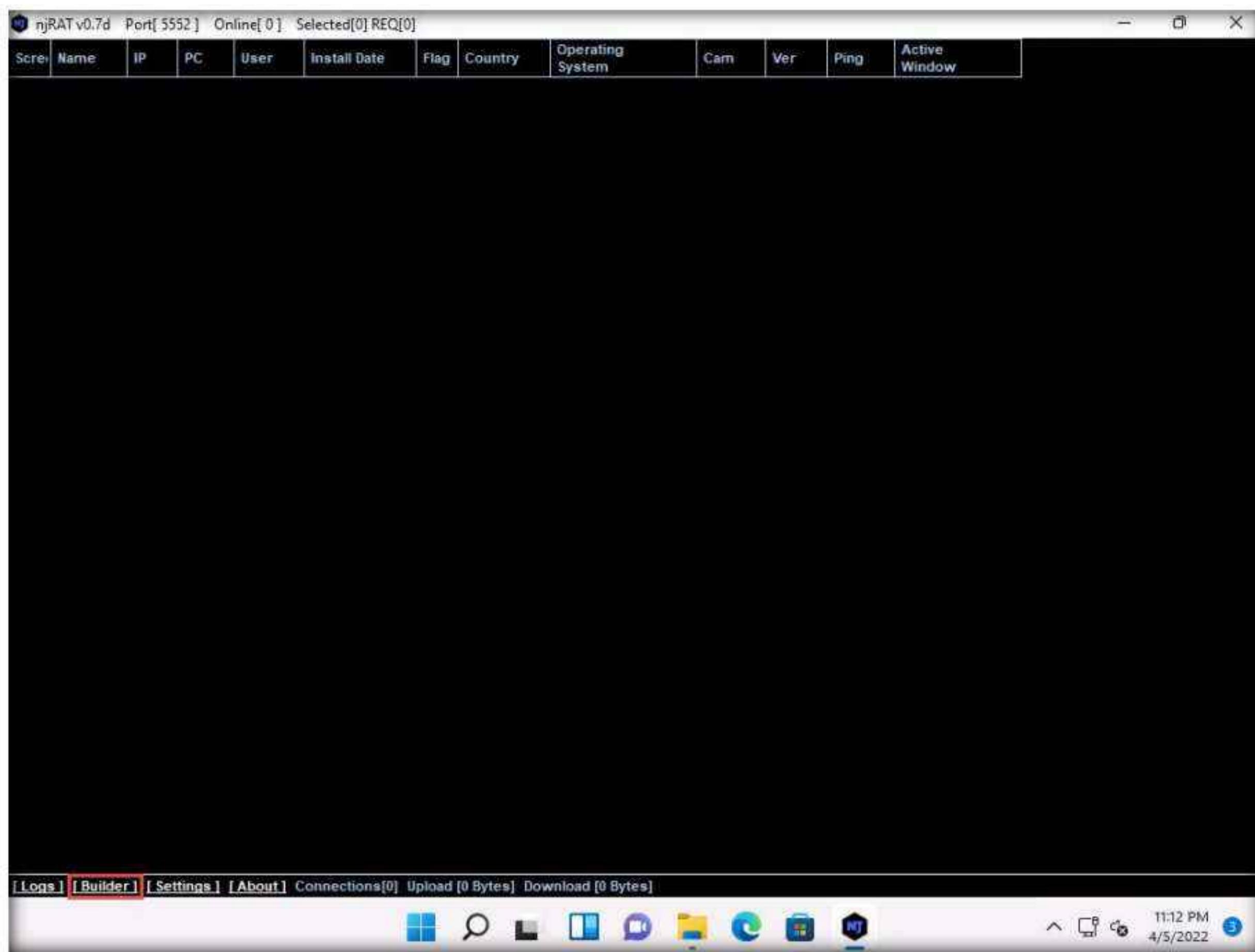
Module 07 – Malware Threats

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**.

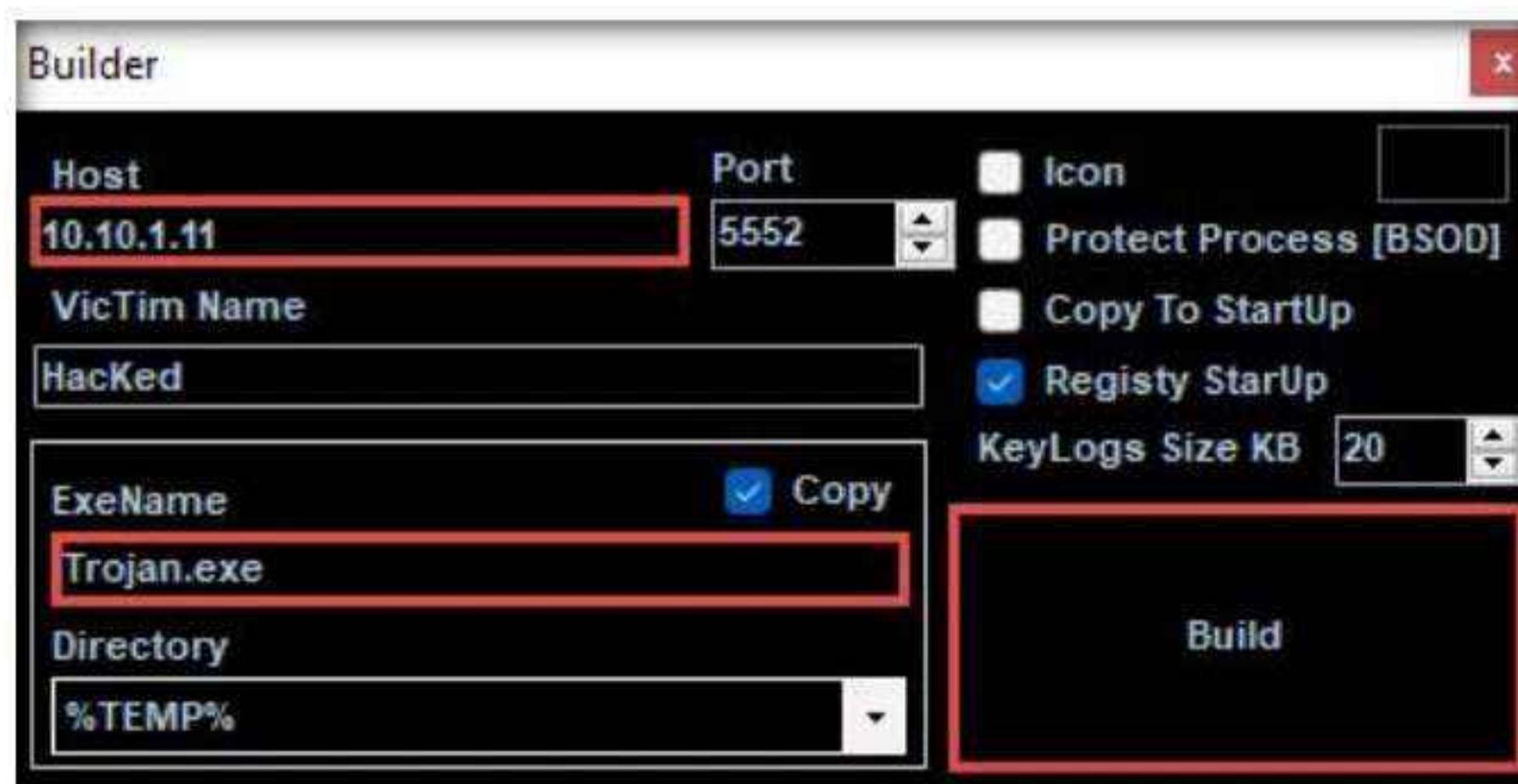


4. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.



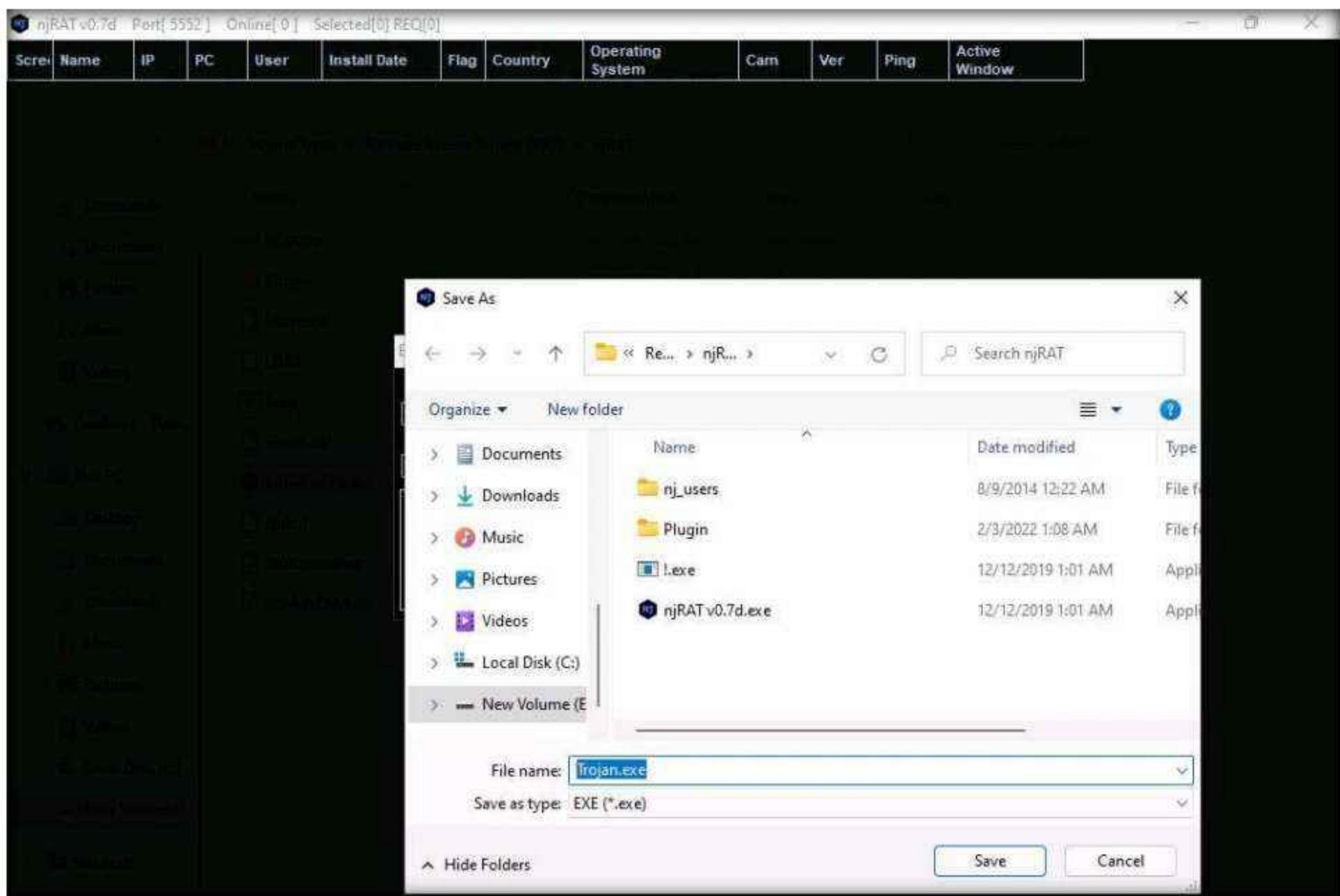
5. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registry StarUp**, rename **ExeName** as **Trojan.exe**. Leave the other settings to default, and click **Build**.

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

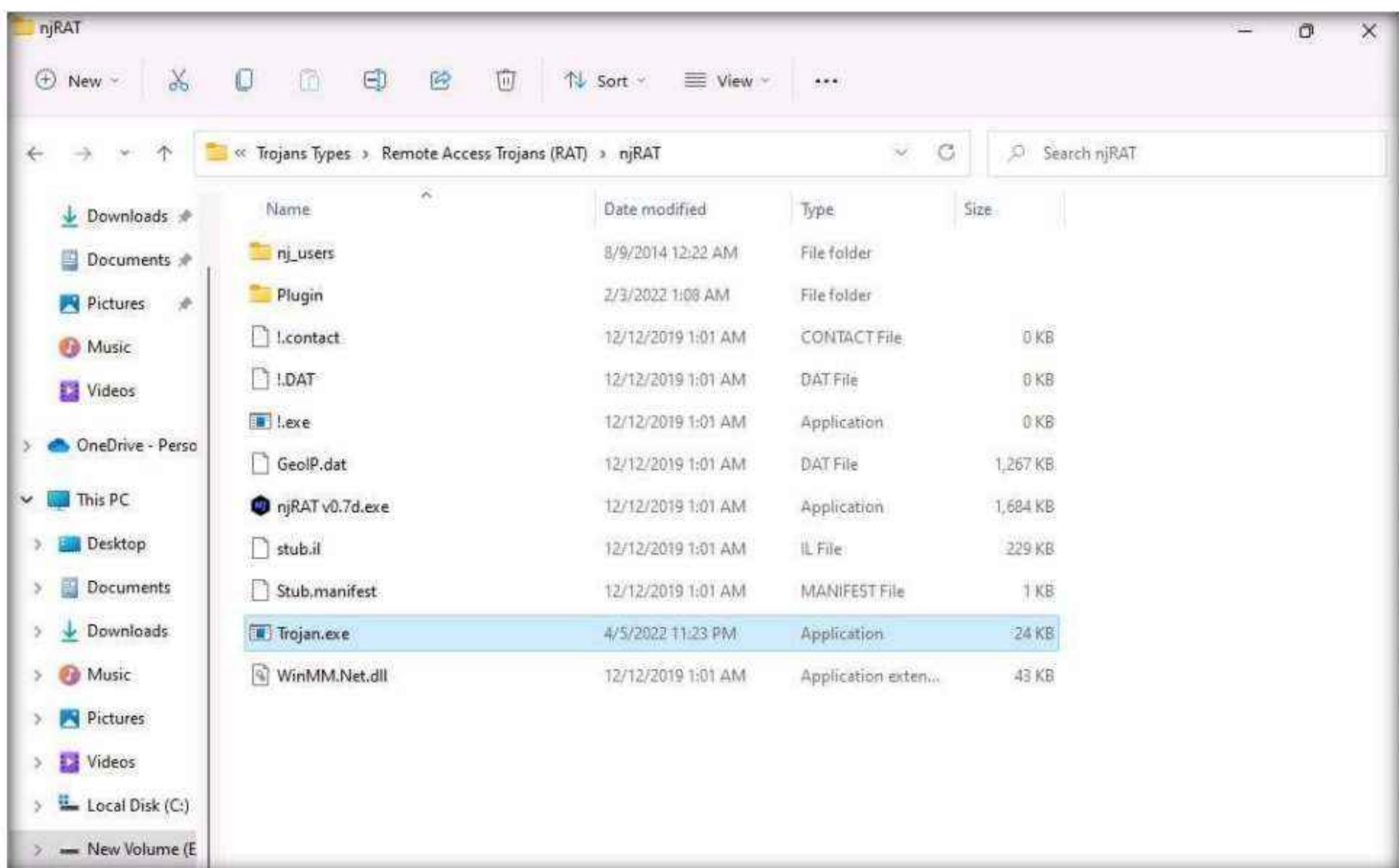


6. Save As window appears, E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT. In the File name, enter **Trojan.exe** and click **Save**. **Done!** pop-up appears, click **OK**.

Module 07 – Malware Threats

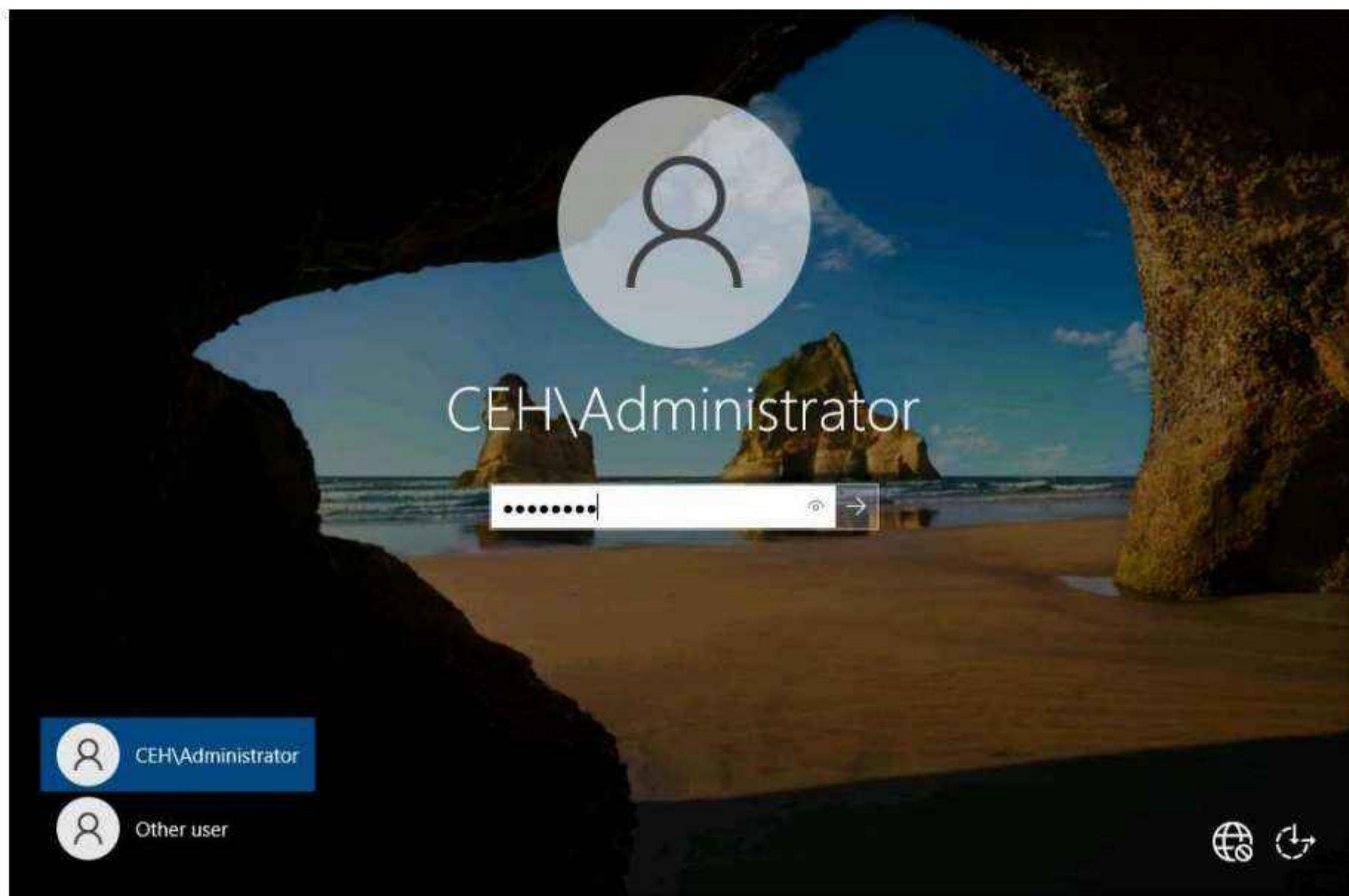


- Minimize njRAT window. You can observe that a **Trojan.exe** file has been created at the location **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.

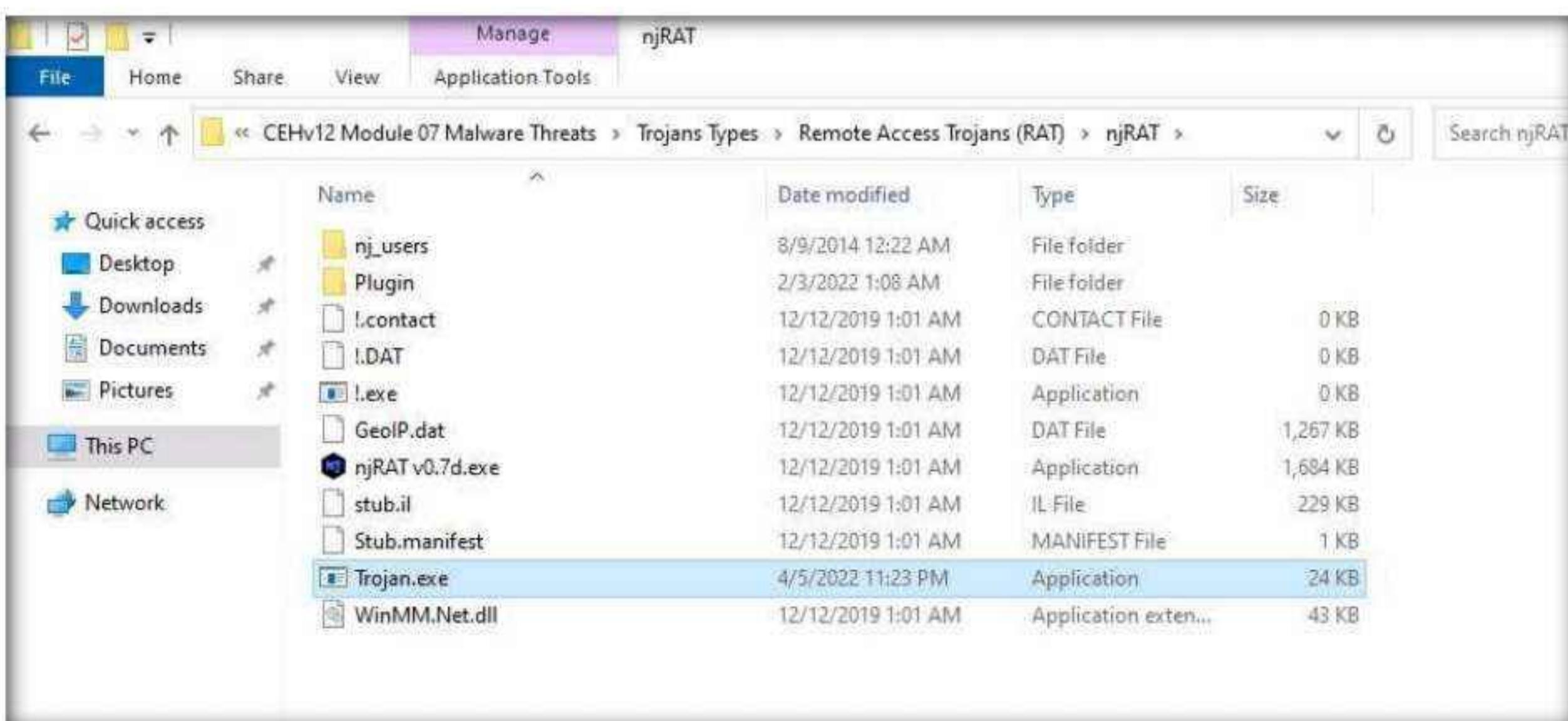


8. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

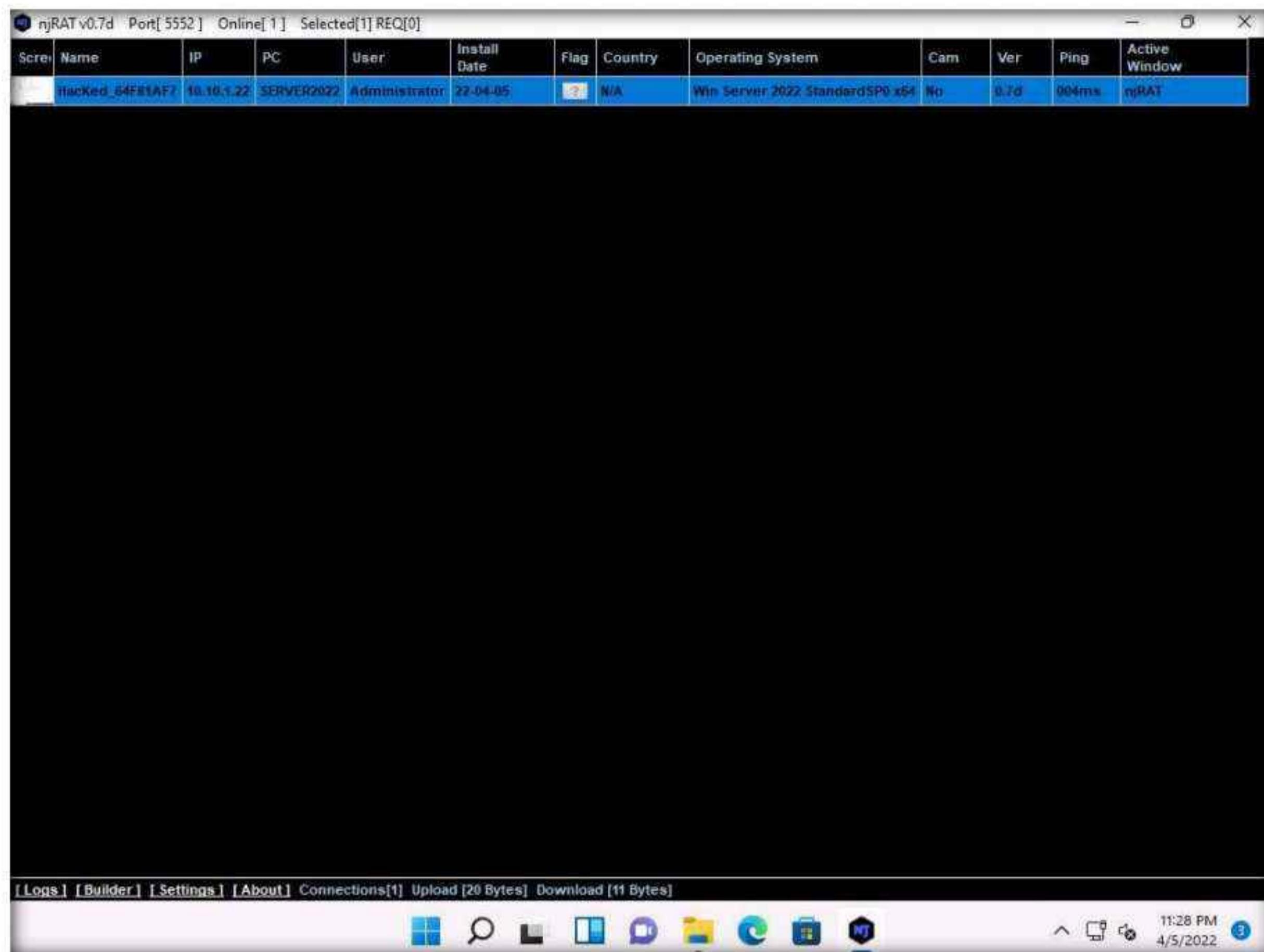
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



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

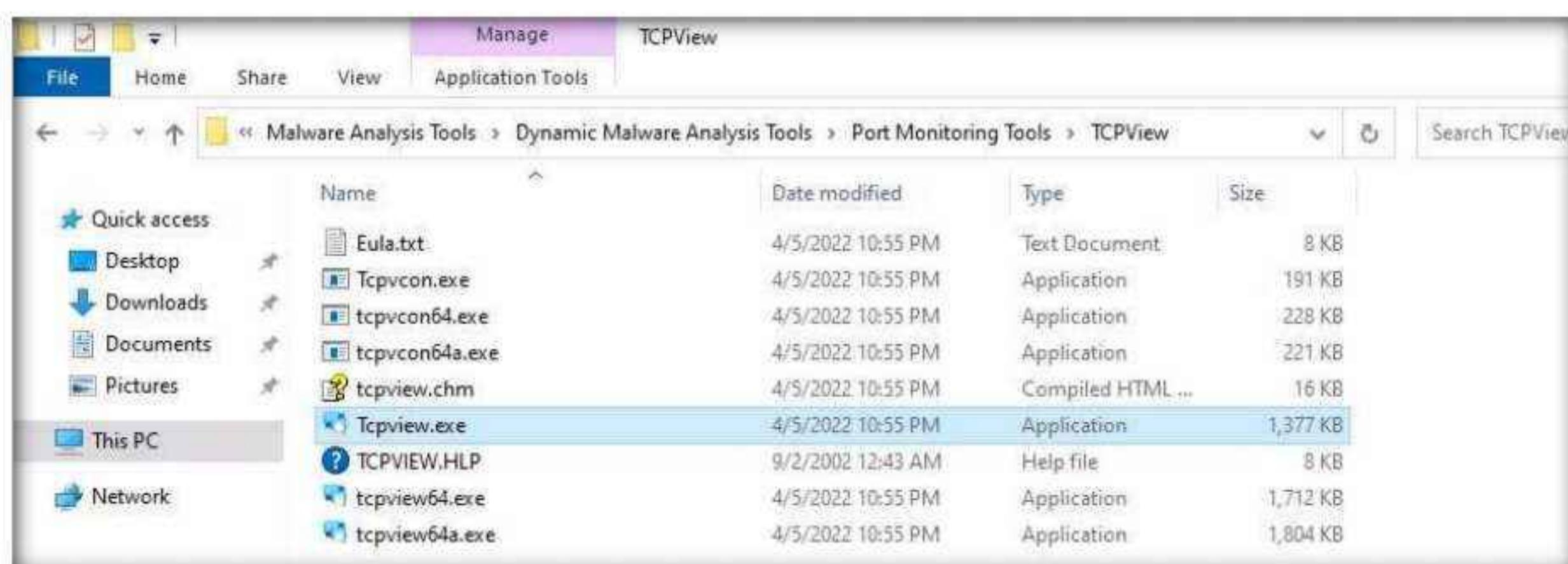


10. Observe that a connection has been established by the njRAT client. Click switch to the **Windows 11** virtual machine. Switch to **njRAT** window to observe the established connection.



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.

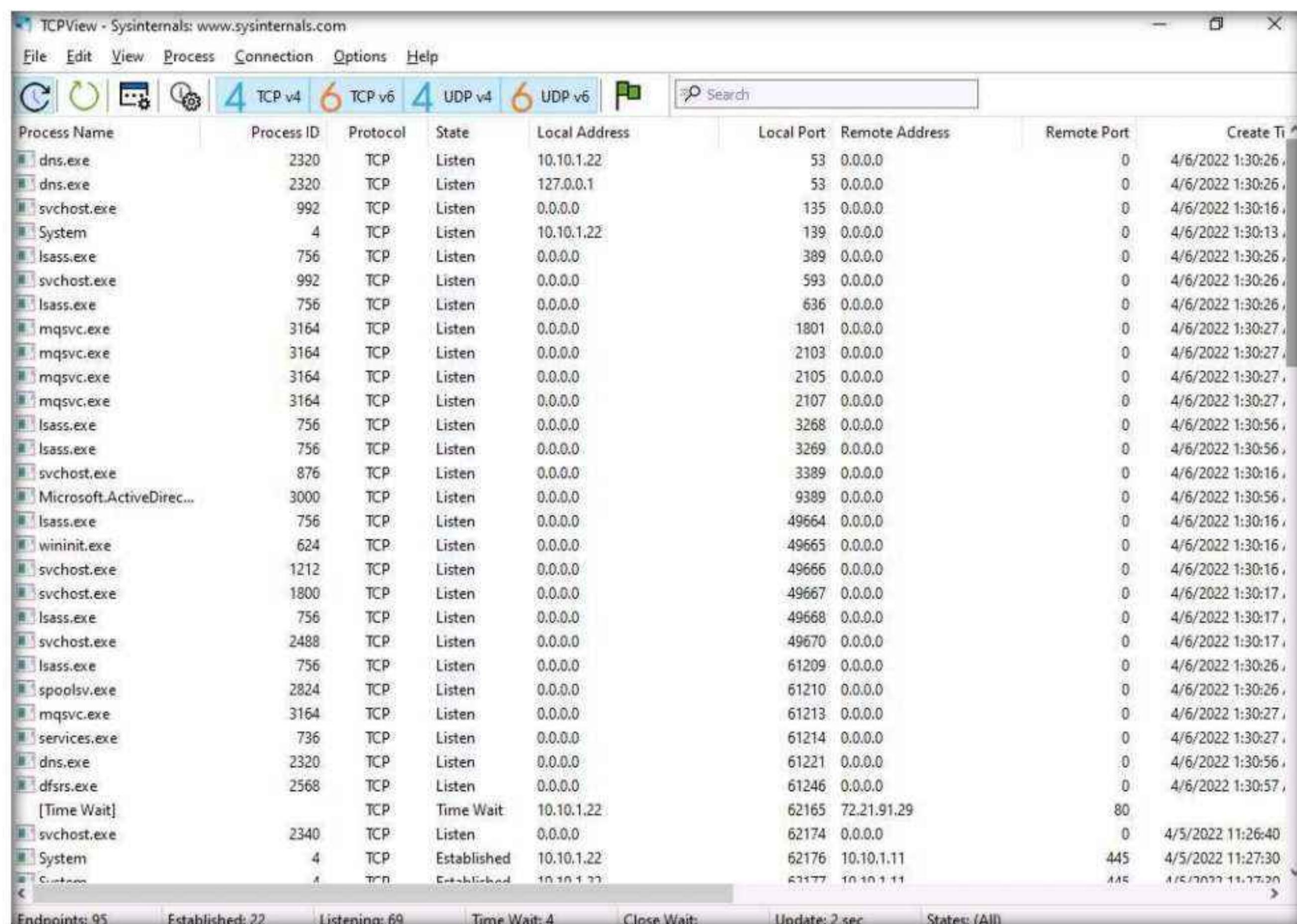
Note: If a User Account Control pop-up appears, click Yes.



Module 07 – Malware Threats

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.



The screenshot shows the TCPView application interface. The title bar reads "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, View, Process, Connection, Options, and Help. Below the menu is a toolbar with icons for Stop, Refresh, Filter, and a search bar labeled "Search". The main window is a grid table with the following columns: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, and Create Ti. The table lists numerous network connections, mostly from system processes like dns.exe, svchost.exe, and lsass.exe, showing various ports and states. At the bottom of the table, there are navigation arrows and a status bar with the following information: Endpoints: 95, Established: 22, Listening: 69, Time Wait: 4, Close Wait: 0, Update: 2 sec, and States: (All).

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,
dftrs.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
C:\temp	4	TCP	Established	10.10.1.11	63177	10.10.1.11	445	4/5/2022 11:27:30

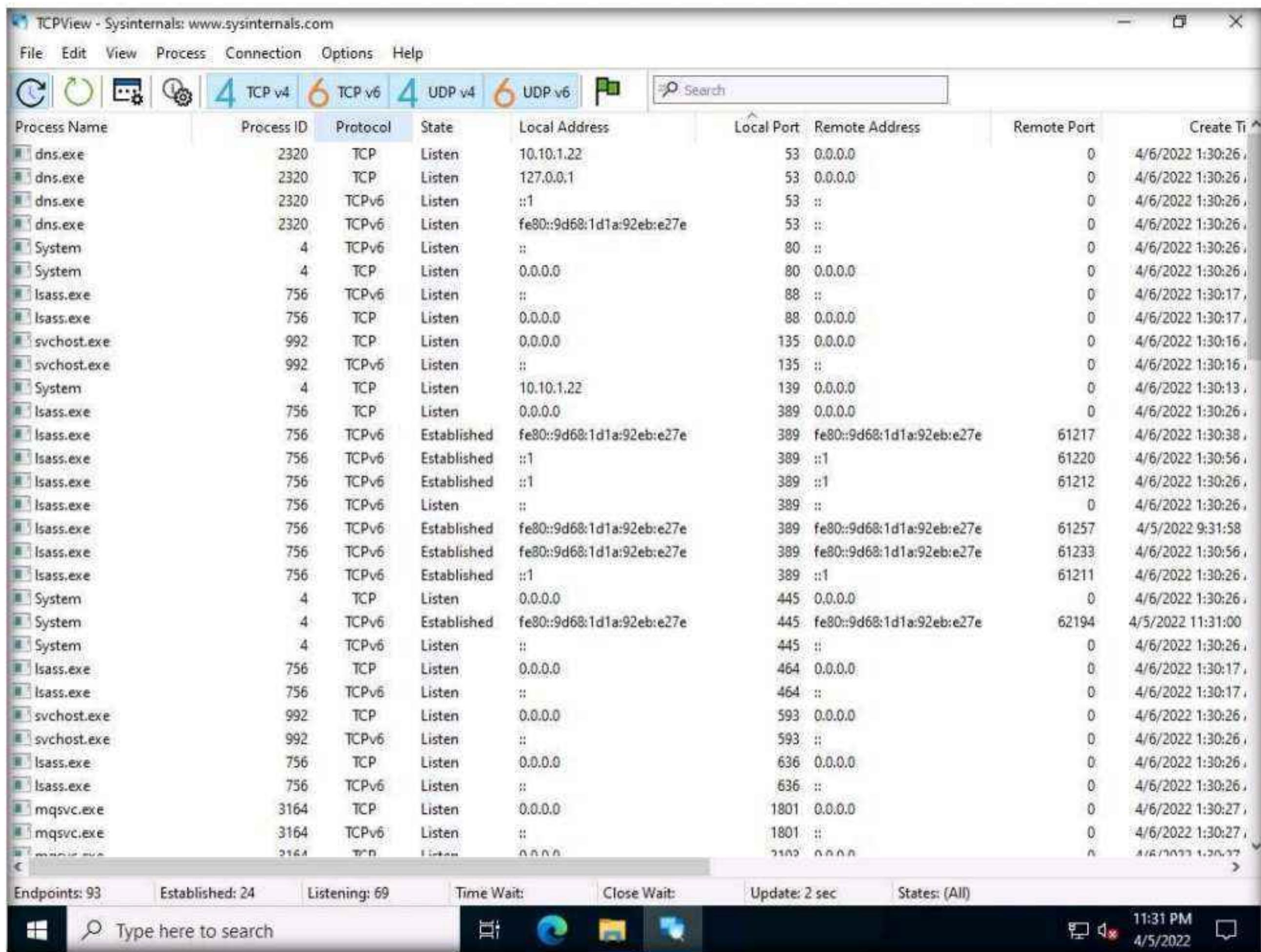
Module 07 – Malware Threats

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,
mqsvc.exe	3164	TCPv6	Listen	::	2103	::	0	4/6/2022 1:30:27,

Module 07 – Malware Threats

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

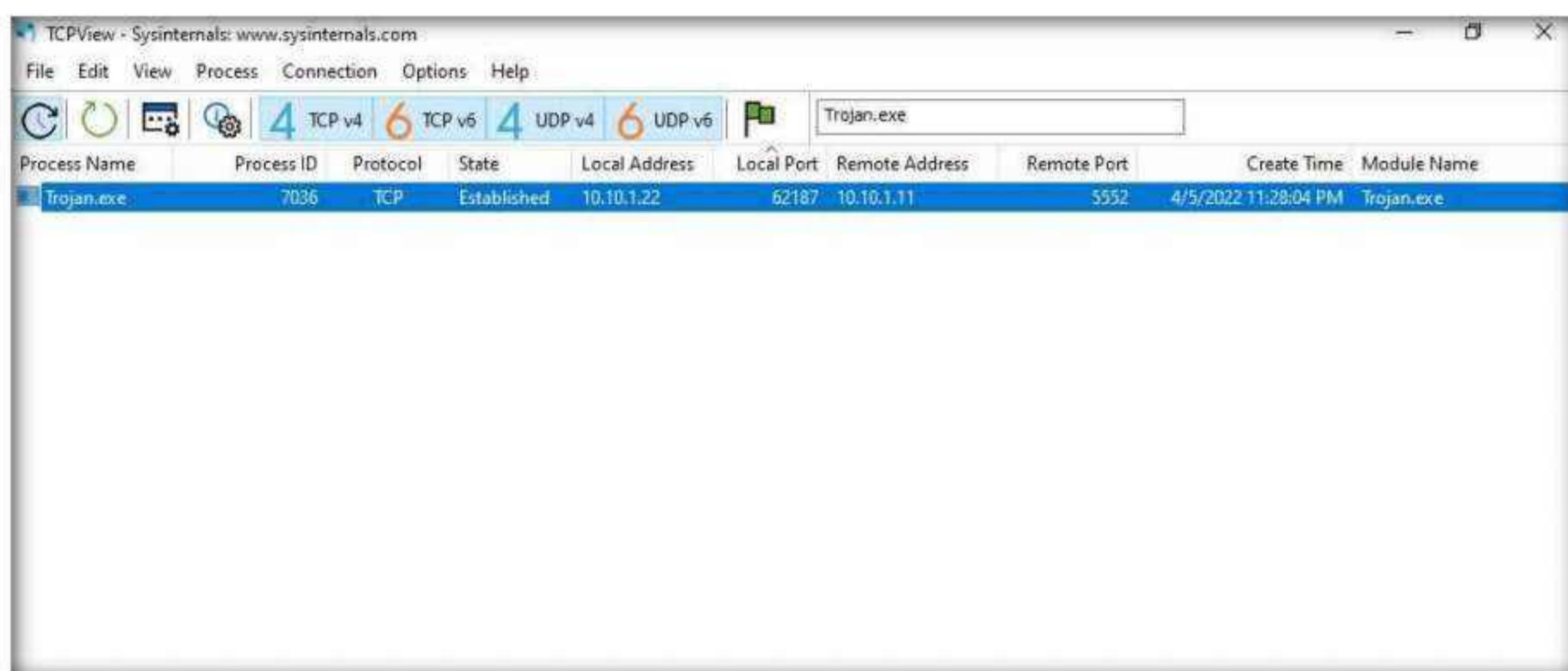


The screenshot shows the TCPView application interface. The main window displays a table of network connections. The columns are: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, and Create Time. The 'Protocol' column is highlighted. The table lists numerous entries, mostly from system processes like dns.exe, svchost.exe, and System, showing various port numbers and states (Listen, Established). A search bar at the top right contains the text 'Search'. At the bottom, there are status indicators: Endpoints: 93, Established: 24, Listening: 69, Time Wait: [empty], Close Wait: [empty], Update: 2 sec, States: (All). The taskbar at the bottom shows the Windows Start button, a search bar with 'Type here to search', and icons for File Explorer, Edge, and Task View. The date and time are shown as 4/5/2022 11:30:27 PM.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time
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
Isass.exe	756	TCPv6	Listen	::	88	::	0	4/6/2022 1:30:17
Isass.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
Isass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
Isass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61217	4/6/2022 1:30:38
Isass.exe	756	TCPv6	Established	::1	389	::1	61220	4/6/2022 1:30:56
Isass.exe	756	TCPv6	Established	::1	389	::1	61212	4/6/2022 1:30:26
Isass.exe	756	TCPv6	Listen	::	389	::	0	4/6/2022 1:30:26
Isass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61257	4/5/2022 9:31:58
Isass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61233	4/6/2022 1:30:56
Isass.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
Isass.exe	756	TCP	Listen	0.0.0.0	464	0.0.0.0	0	4/6/2022 1:30:17
Isass.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
Isass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
Isass.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	n	4/6/2022 1:30:27

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

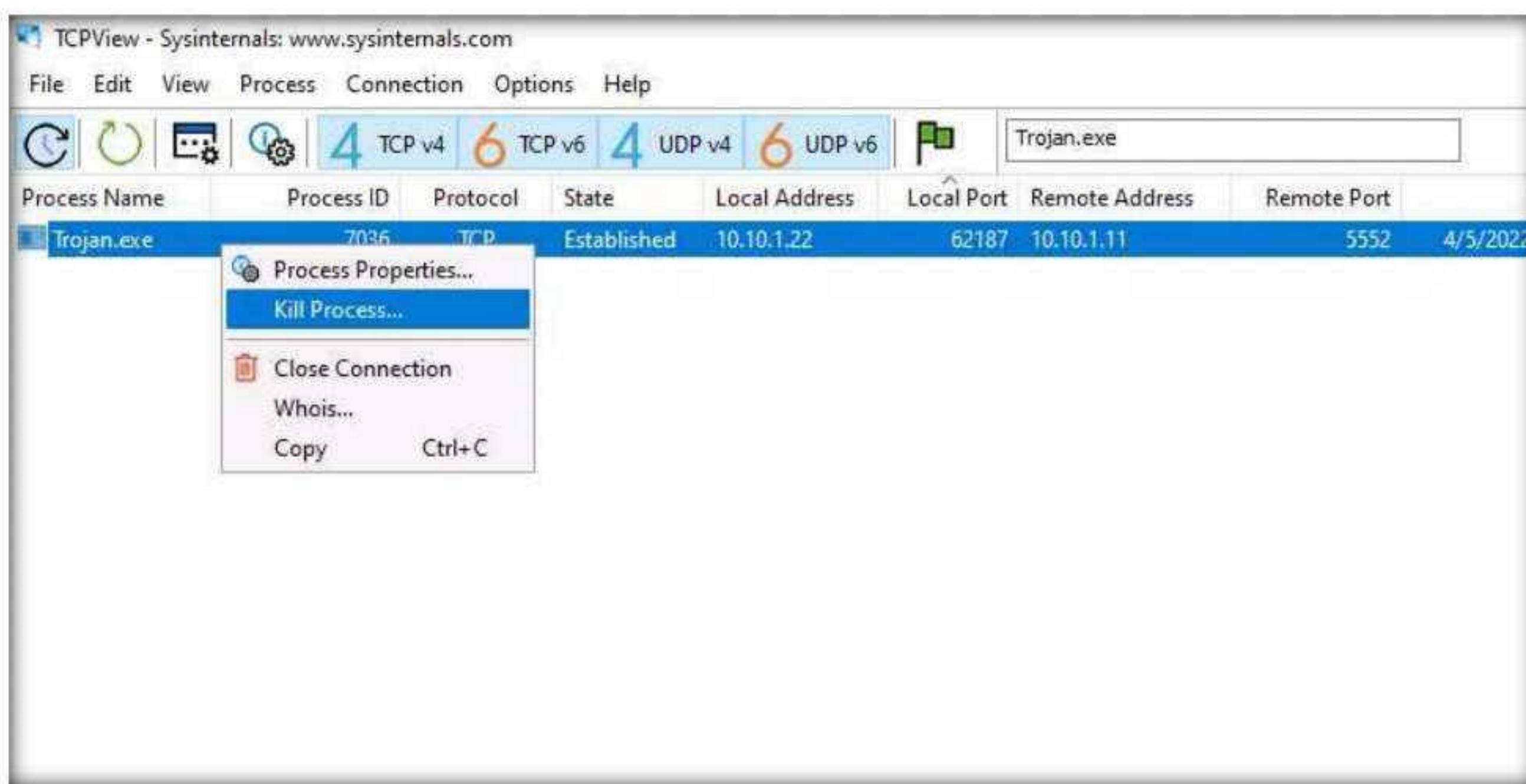
18. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2022** machine. You can see details such as **Remote Address** and **Remote Port**.



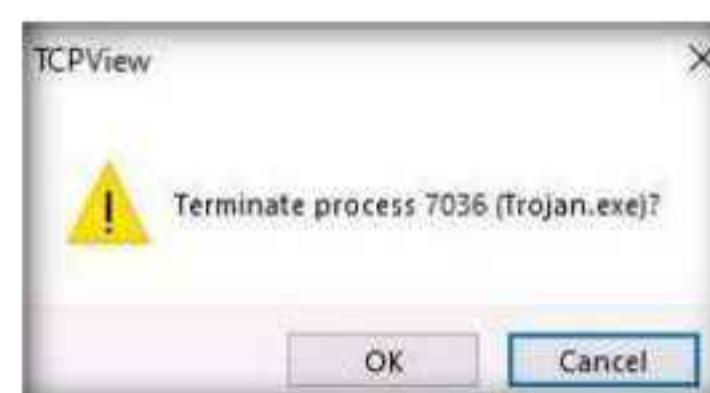
The screenshot shows the TCPView application interface with a search filter applied to 'Trojan.exe'. The main window displays a table of network connections. The columns are: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, and Module Name. One row is highlighted for the process 'Trojan.exe' with the following details: Process ID 7036, Protocol TCP, State Established, Local Address 10.10.1.22, Local Port 62187, Remote Address 10.10.1.11, Remote Port 5552, Create Time 4/5/2022 11:28:04 PM, and Module Name Trojan.exe. The taskbar at the bottom shows the Windows Start button, a search bar with 'Type here to search', and icons for File Explorer, Edge, and Task View. The date and time are shown as 4/5/2022 11:28:04 PM.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
Trojan.exe	7036	TCP	Established	10.10.1.22	62187	10.10.1.11	5552	4/5/2022 11:28:04 PM	Trojan.exe

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**.

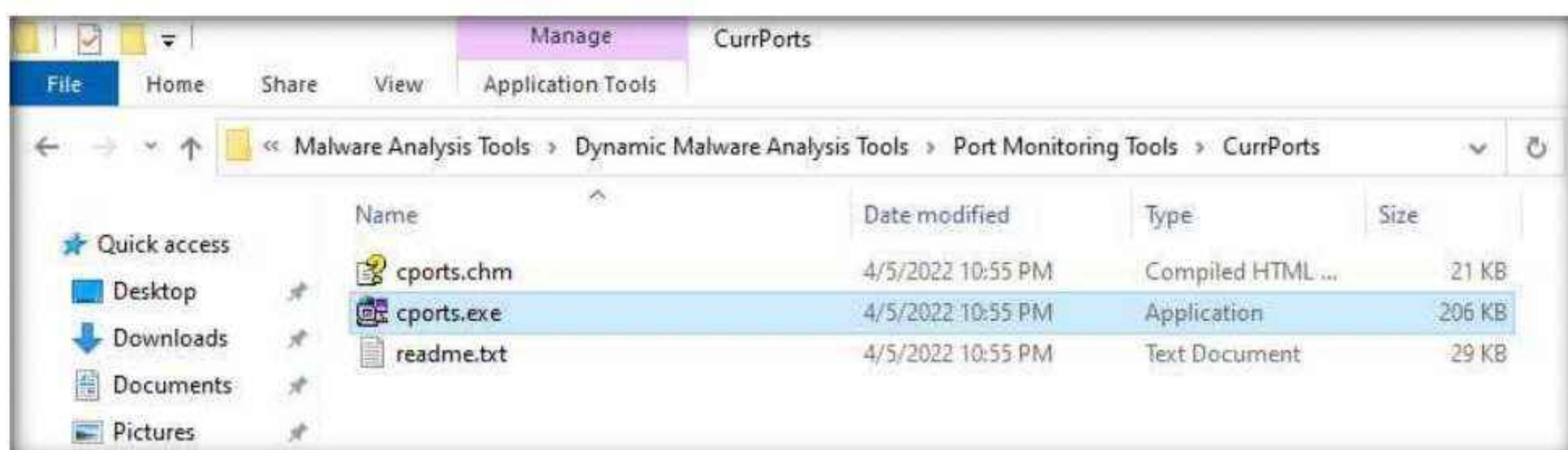


21. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.

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**.



Module 07 – Malware Threats

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

The screenshot shows the CurrPorts application window. The title bar reads "CurrPorts". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu is a toolbar with various icons. The main area is a table with the following columns: Process Name, Process ID, Protocol, Local Port, Local Port (domain), Local Address, Remote IP, Remote Port, Remote Address, Remote Host Name, State, and Sent By. The table lists numerous entries, mostly for "dns.exe" processes, with local ports ranging from 5120 to 54343. Most entries show "0.0.0.0" for both local and remote addresses, and "Listening" for the state. A single entry for "DFSRs.exe" has a local port of 2568 and a local address of "127.0.0.1". The status bar at the bottom left says "5137 Total Ports, 5 Remote Connections, 1 Selected". The status bar at the bottom right shows the time as "11:37 PM" and the date as "4/5/2022".

Process Name	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Sent By
DFSRs.exe	2568	TCP	61246		0.0.0.0			0.0.0.0		Listening	
DFSRs.exe	2568	UDP	61484		127.0.0.1						
dns.exe	2320	TCP	53	domain	10.10.1.22			0.0.0.0		Listening	
dns.exe	2320	TCP	53	domain	127.0.0.1			0.0.0.0		Listening	
dns.exe	2320	TCP	61221		0.0.0.0			0.0.0.0		Listening	
dns.exe	2320	UDP	53	domain	10.10.1.22						154
dns.exe	2320	UDP	53	domain	127.0.0.1						
dns.exe	2320	UDP	54319		0.0.0.0						
dns.exe	2320	UDP	54321		0.0.0.0						
dns.exe	2320	UDP	54322		0.0.0.0						
dns.exe	2320	UDP	54323		0.0.0.0						
dns.exe	2320	UDP	54324		0.0.0.0						
dns.exe	2320	UDP	54325		0.0.0.0						
dns.exe	2320	UDP	54326		0.0.0.0						
dns.exe	2320	UDP	54327		0.0.0.0						
dns.exe	2320	UDP	54328		0.0.0.0						
dns.exe	2320	UDP	54329		0.0.0.0						
dns.exe	2320	UDP	54330		0.0.0.0						
dns.exe	2320	UDP	54331		0.0.0.0						
dns.exe	2320	UDP	54332		0.0.0.0						
dns.exe	2320	UDP	54333		0.0.0.0						
dns.exe	2320	UDP	54334		0.0.0.0						
dns.exe	2320	UDP	54335		0.0.0.0						
dns.exe	2320	UDP	54336		0.0.0.0						
dns.exe	2320	UDP	54337		0.0.0.0						
dns.exe	2320	UDP	54338		0.0.0.0						
dns.exe	2320	UDP	54339		0.0.0.0						
dns.exe	2320	UDP	54340		0.0.0.0						
dns.exe	2320	UDP	54341		0.0.0.0						
dns.exe	2320	UDP	54342		0.0.0.0						
dns.exe	2320	UDP	54343		0.0.0.0						

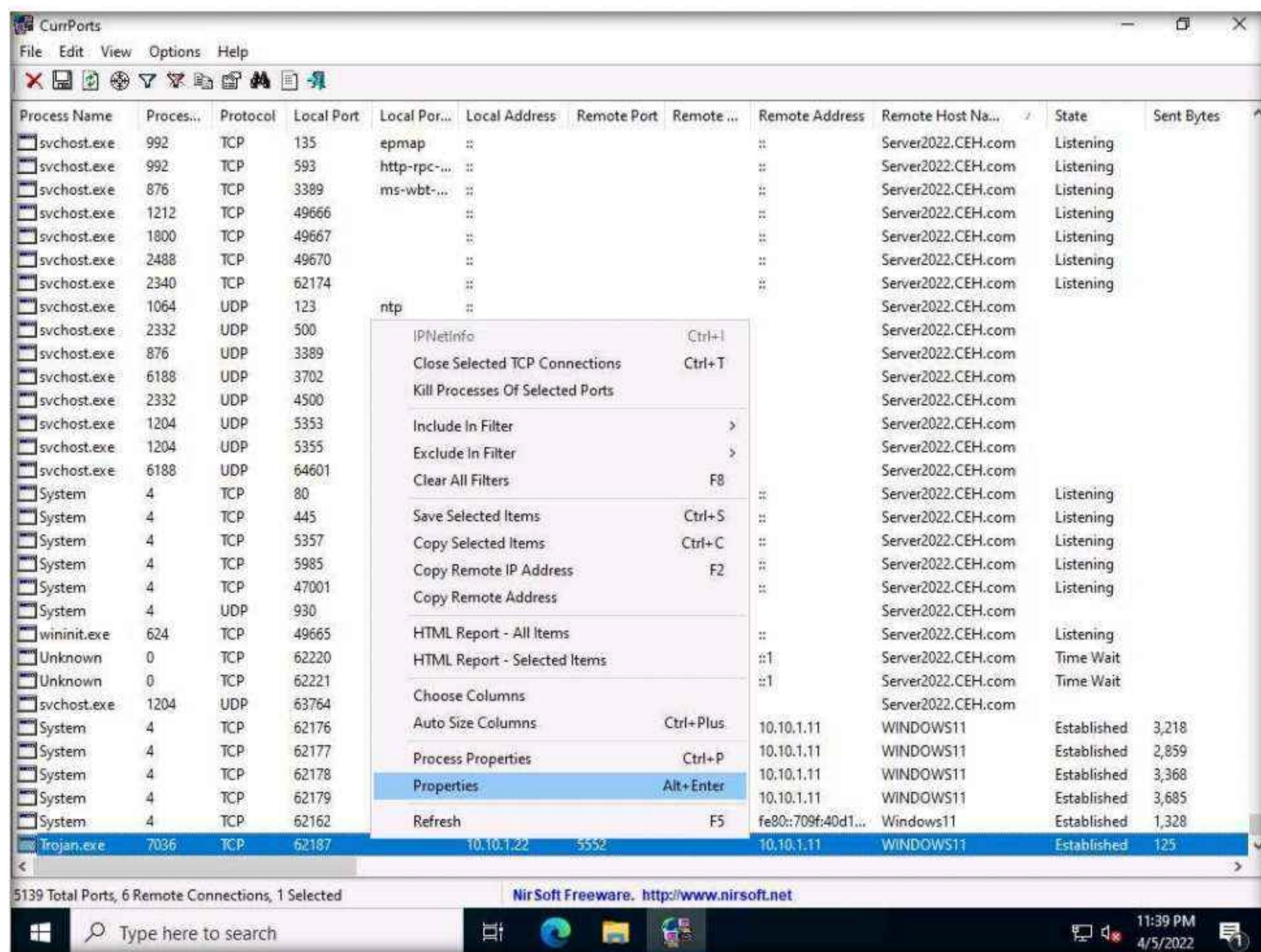
Module 07 – Malware Threats

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

Process Name	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote Port	Remote ...	Remote Address	Remote Host Na...	State	Sent Bytes
spoolsv.exe	2824	TCP	61210	:					Server2022.CEH.com	Listening	
svchost.exe	992	TCP	135	epmap	::				Server2022.CEH.com	Listening	
svchost.exe	992	TCP	593	http-rpc-...	::				Server2022.CEH.com	Listening	
svchost.exe	876	TCP	3389	ms-wbt-...	::				Server2022.CEH.com	Listening	
svchost.exe	1212	TCP	49666		::				Server2022.CEH.com	Listening	
svchost.exe	1800	TCP	49667		::				Server2022.CEH.com	Listening	
svchost.exe	2488	TCP	49670		::				Server2022.CEH.com	Listening	
svchost.exe	2340	TCP	62174		::				Server2022.CEH.com	Listening	
svchost.exe	1064	UDP	123	ntp	::				Server2022.CEH.com		
svchost.exe	2332	UDP	500	isakmp	::				Server2022.CEH.com		
svchost.exe	876	UDP	3389	ms-wbt-...	::				Server2022.CEH.com		
svchost.exe	6188	UDP	3702	ws-disco...	::				Server2022.CEH.com		
svchost.exe	2332	UDP	4500	ipsec-msft	::				Server2022.CEH.com		
svchost.exe	1204	UDP	5353		::				Server2022.CEH.com		
svchost.exe	1204	UDP	5355	llmnr	::				Server2022.CEH.com		
svchost.exe	6188	UDP	64601		::				Server2022.CEH.com		
System	4	TCP	80	http	::				Server2022.CEH.com	Listening	
System	4	TCP	445	microsof...	::				Server2022.CEH.com	Listening	
System	4	TCP	5357	wsd	::				Server2022.CEH.com	Listening	
System	4	TCP	5985		::				Server2022.CEH.com	Listening	
System	4	TCP	47001		::				Server2022.CEH.com	Listening	
System	4	UDP	930		::				Server2022.CEH.com		
wininit.exe	624	TCP	49665		::				Server2022.CEH.com	Listening	
svchost.exe	1204	UDP	65250		::				Server2022.CEH.com		
Unknown	0	TCP	62215	fe80::9d68:1d...	135	epmap	fe80::9d68:1d1...	Server2022.CEH.com	Time Wait		
System	4	TCP	62176	10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	2,758	
System	4	TCP	62177	10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	2,491	
System	4	TCP	62178	10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	2,908	
System	4	TCP	62179	10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	3,225	
System	4	TCP	62162	fe80::9d68:1d...	445	microsof...	fe80::709f:40d1...	Windows11	Established	1,328	
Trojan.exe	7036	TCP	62187	10.10.1.22	5552		10.10.1.11	WINDOWS11	Established	121	

Module 07 – Malware Threats

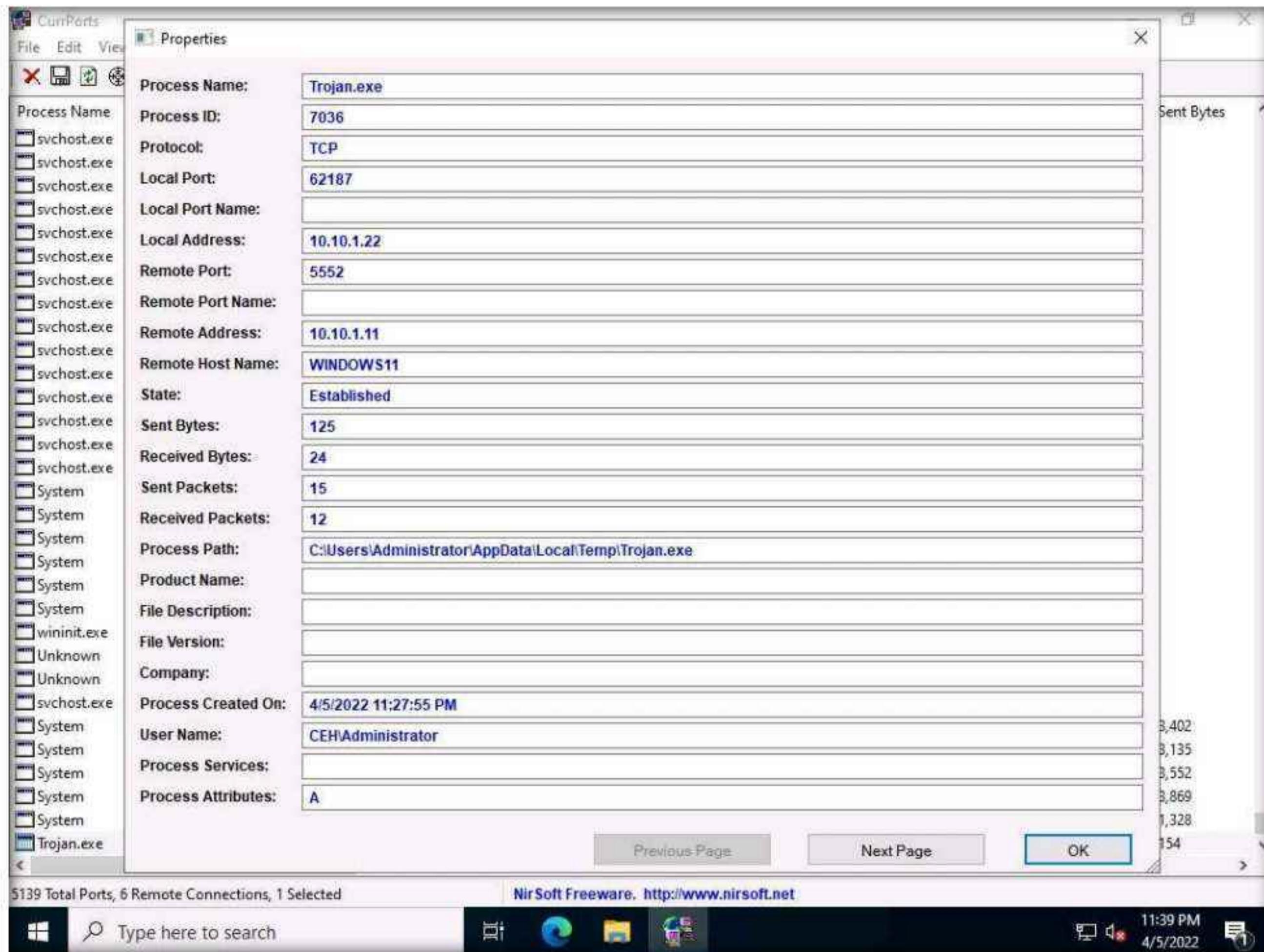
27. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context menu**.



Module 07 – Malware Threats

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.

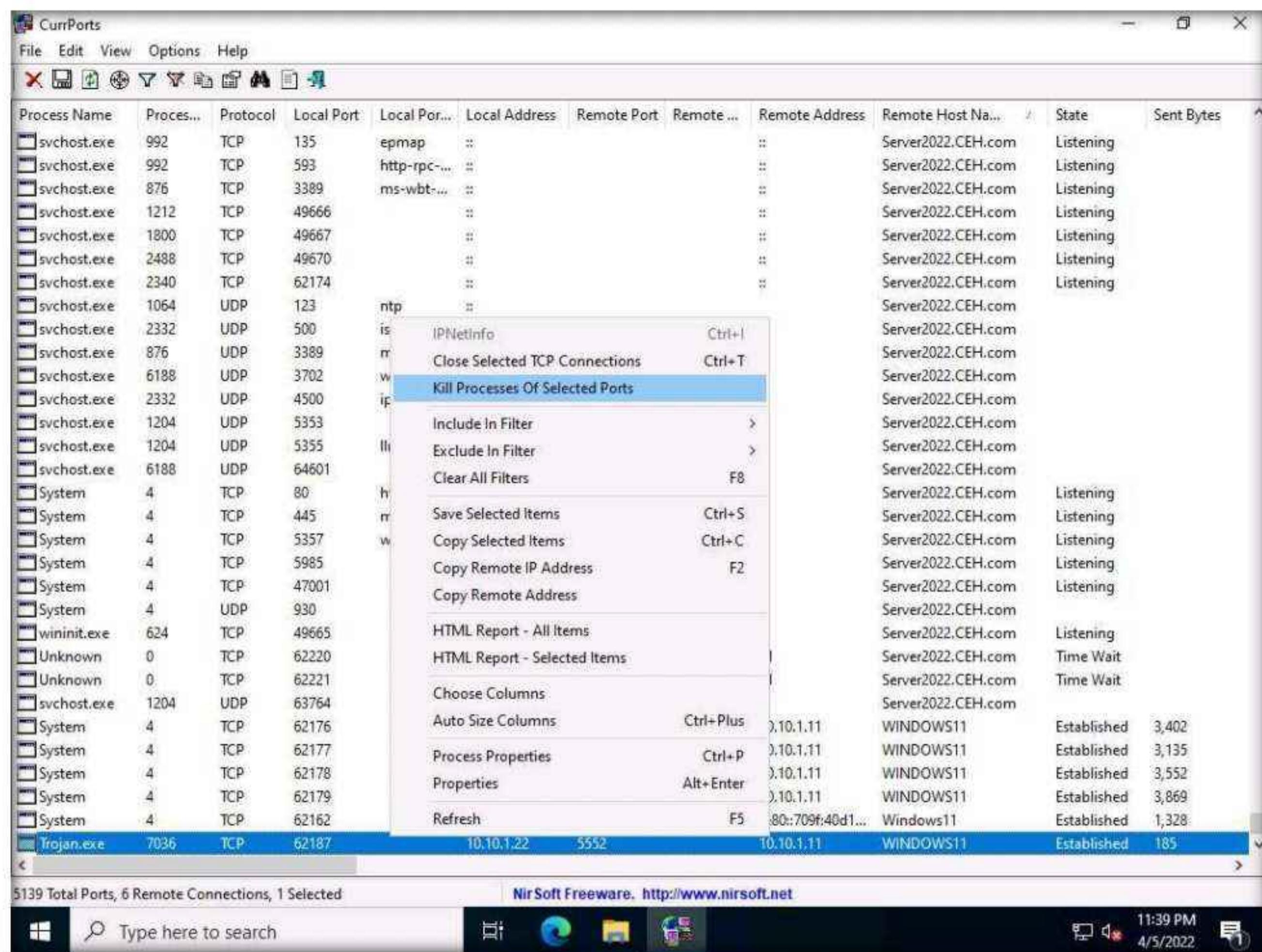
29. Once you are done examining the properties associated with the process, click **OK**.



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.

Module 07 – Malware Threats



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.

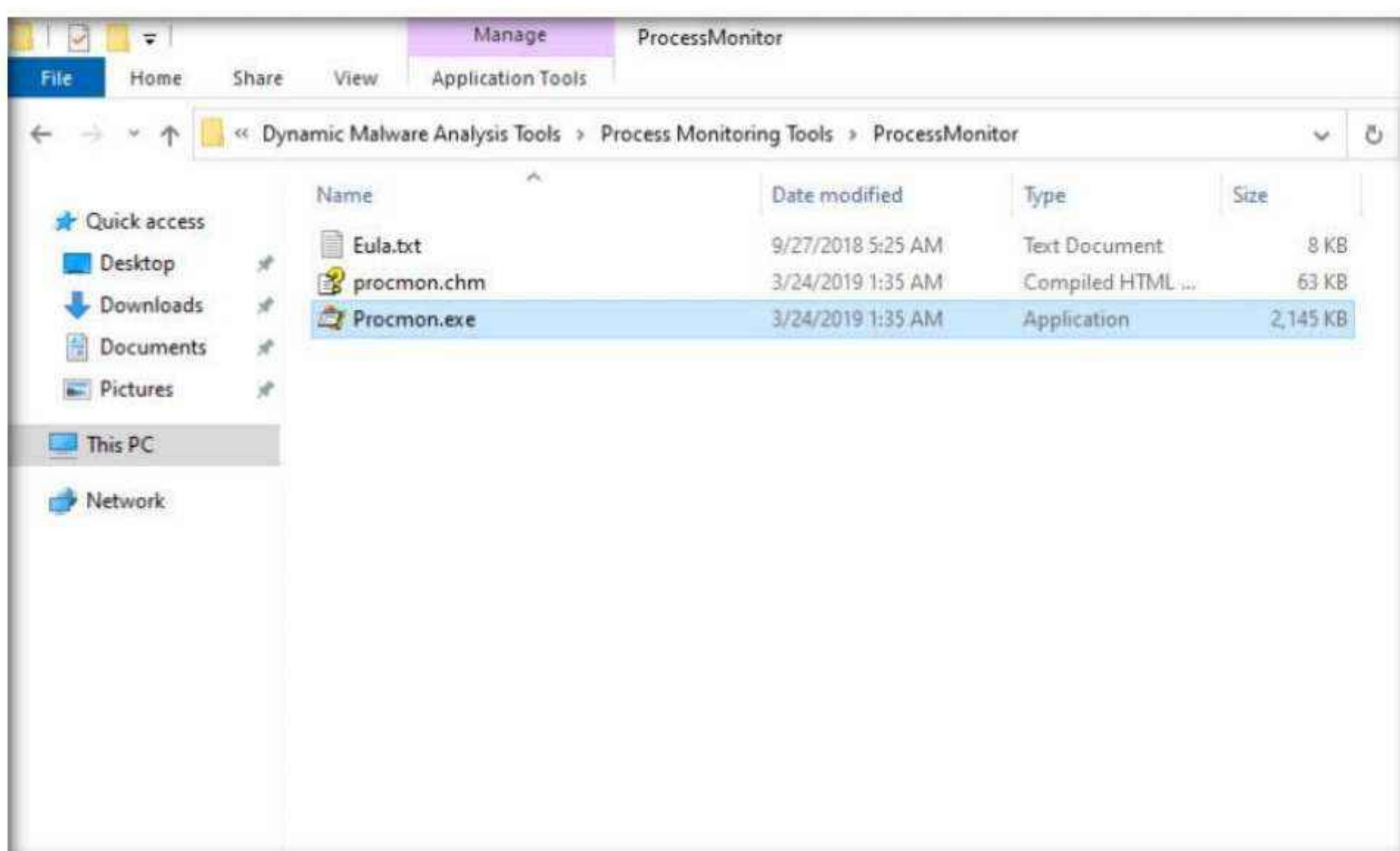
Task 2: Perform Process Monitoring using Process Monitor

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.

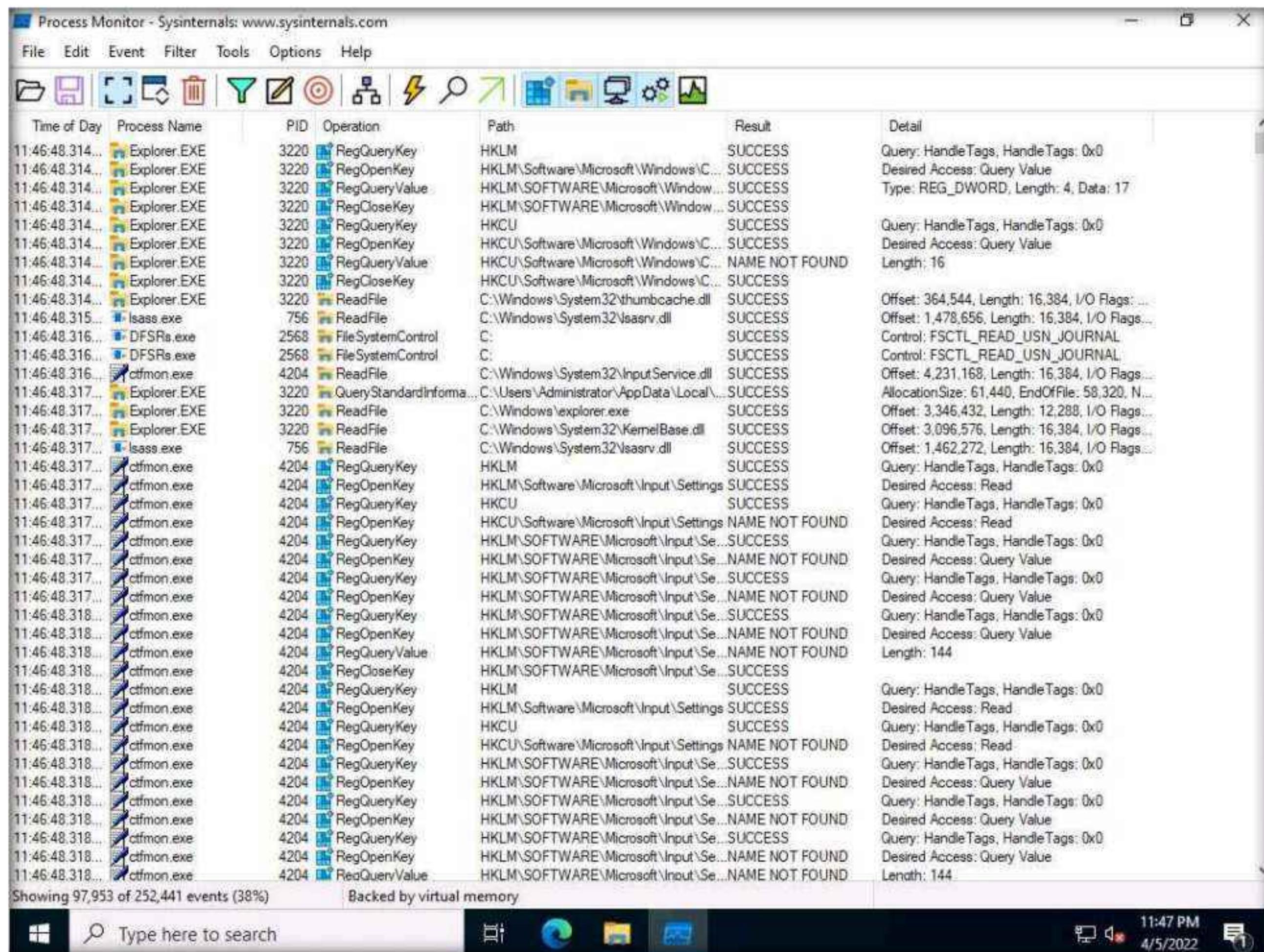
Here, we will use the Process Monitor tool to detect suspicious processes.

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.



Module 07 – Malware Threats

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.



The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. Below the menu is a toolbar with various icons. The main pane is a table with columns: Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The table lists numerous events from 11:46:48.314 to 11:46:48.318, mostly involving the "ctfmon.exe" process. The "Result" column shows many entries as "SUCCESS". The "Detail" column provides specific details for each event, such as file paths like "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" and "C:\Windows\System32\thumbcache.dll", and I/O flags like "Offset: 364,544, Length: 16,384, I/O Flags: ...". The status bar at the bottom indicates "Showing 97,953 of 252,441 events (38%) Backed by virtual memory". The taskbar at the bottom shows the Start button, a search bar with "Type here to search", and several pinned icons. The system tray shows the date and time as "11:47 PM 4/5/2022".

Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:46:48.314...	Explorer EXE	3220	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.314...	Explorer EXE	3220	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Query Value
11:46:48.314...	Explorer EXE	3220	RegQueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Type: REG_DWORD, Length: 4, Data: 17
11:46:48.314...	Explorer EXE	3220	RegCloseKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	
11:46:48.314...	Explorer EXE	3220	RegQueryKey	HKCU	SUCCESS	
11:46:48.314...	Explorer EXE	3220	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.314...	Explorer EXE	3220	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND	Desired Access: Query Value
11:46:48.314...	Explorer EXE	3220	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Length: 16
11:46:48.314...	Explorer EXE	3220	ReadFile	C:\Windows\System32\thumbcache.dll	SUCCESS	
11:46:48.315...	lsass.exe	756	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1,478,656, Length: 16,384, I/O Flags: ...
11:46:48.316...	DFSRs.exe	2568	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JOURNAL
11:46:48.316...	DFSRs.exe	2568	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JOURNAL
11:46:48.316...	ctfmon.exe	4204	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4,231,168, Length: 16,384, I/O Flags: ...
11:46:48.317...	Explorer EXE	3220	QueryStandardInformation	C:\Users\Administrator\AppData\Local\Temp\explorer.exe	SUCCESS	AllocationSize: 61,440, EndOfFile: 58,320, N...
11:46:48.317...	Explorer EXE	3220	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,346,432, Length: 12,288, I/O Flags: ...
11:46:48.317...	Explorer EXE	3220	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 3,096,576, Length: 16,384, I/O Flags: ...
11:46:48.317...	lsass.exe	756	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1,462,272, Length: 16,384, I/O Flags: ...
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Read
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Read
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:46:48.317...	ctfmon.exe	4204	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
11:46:48.317...	ctfmon.exe	4204	RegQueryKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:4						

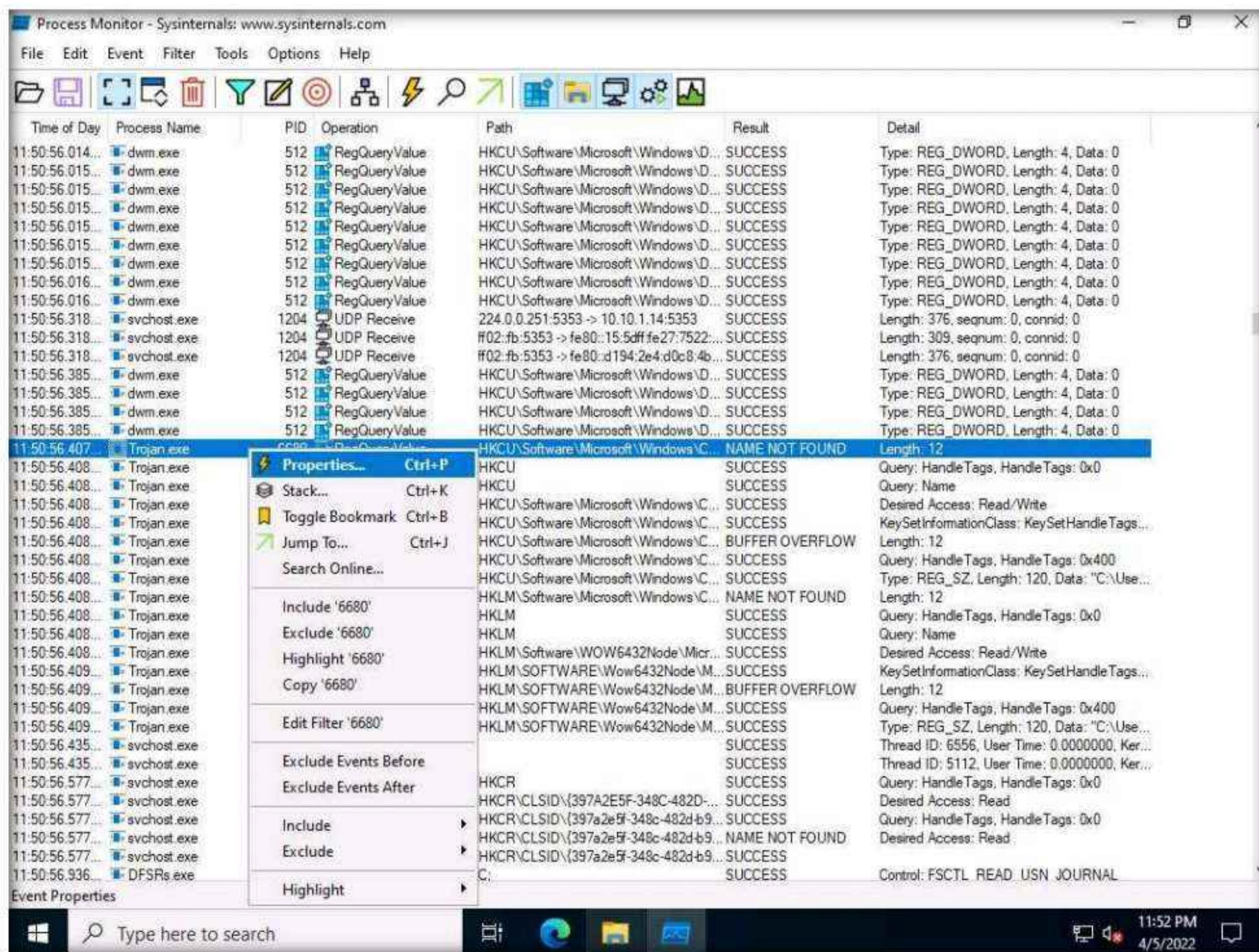
Module 07 – Malware Threats

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.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:50:56.014...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.015...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.015...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.015...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.015...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.015...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.015...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.015...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.016...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.016...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.318...	svchost.exe	1204	UDP Receive	224.0.0.251:5353 -> 10.10.1.14:5353	SUCCESS	Length: 376, seqnum: 0, connid: 0
11:50:56.318...	svchost.exe	1204	UDP Receive	F02:fb:5353 -> fe80:15:5dff:fe27:7522::	SUCCESS	Length: 309, seqnum: 0, connid: 0
11:50:56.318...	svchost.exe	1204	UDP Receive	F02:fb:5353 -> fe80:d194:2e4:d0c8:4b..	SUCCESS	Length: 376, seqnum: 0, connid: 0
11:50:56.385...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.385...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.385...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.385...	dwm.exe	512	RegQueryValue	HKCU\Software\Microsoft\Windows\D...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:50:56.407...	Trojan.exe	6680	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Length: 12
11:50:56.408...	Trojan.exe	6680	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:50:56.408...	Trojan.exe	6680	RegQueryKey	HKCU	SUCCESS	Query: Name
11:50:56.408...	Trojan.exe	6680	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Read/Write
11:50:56.408...	Trojan.exe	6680	RegSetInfoKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	KeySetInformationClass: KeySetHandleTags
11:50:56.408...	Trojan.exe	6680	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	BUFFER OVERFLOW	Length: 12
11:50:56.408...	Trojan.exe	6680	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTags, HandleTags: 0x400
11:50:56.408...	Trojan.exe	6680	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_SZ, Length: 120, Data: "C:\Use...
11:50:56.408...	Trojan.exe	6680	RegQueryValue	HKLM\Software\Microsoft\Windows\C...	NAME NOT FOUND	Length: 12
11:50:56.408...	Trojan.exe	6680	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:50:56.408...	Trojan.exe	6680	RegQueryKey	HKLM	SUCCESS	Query: Name
11:50:56.408...	Trojan.exe	6680	RegOpenKey	HKLM\Software\WOW6432Node\Micr...	SUCCESS	Desired Access: Read/Write
11:50:56.409...	Trojan.exe	6680	RegSetInfoKey	HKLM\Software\Wow6432Node\M...	SUCCESS	KeySetInformationClass: KeySetHandleTags
11:50:56.409...	Trojan.exe	6680	RegQueryValue	HKLM\Software\Wow6432Node\M...	BUFFER OVERFLOW	Length: 12
11:50:56.409...	Trojan.exe	6680	RegQueryKey	HKLM\Software\Wow6432Node\M...	SUCCESS	Query: HandleTags, HandleTags: 0x400
11:50:56.409...	Trojan.exe	6680	RegSetValue	HKLM\Software\Wow6432Node\M...	SUCCESS	Type: REG_SZ, Length: 120, Data: "C:\Use...
11:50:56.435...	svchost.exe	3484	Thread Exit		SUCCESS	Thread ID: 6556, User Time: 0.0000000, Ker...
11:50:56.435...	svchost.exe	3484	Thread Exit		SUCCESS	Thread ID: 5112, User Time: 0.0000000, Ker...
11:50:56.577...	svchost.exe	1328	RegQueryKey	HKCR	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:50:56.577...	svchost.exe	1328	RegOpenKey	HKCR\CLSID\{397A2E5F-348C-482D...	SUCCESS	Desired Access: Read
11:50:56.577...	svchost.exe	1328	RegQueryKey	HKCR\CLSID\{397a2e5f-348c-482d-b9...	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:50:56.577...	svchost.exe	1328	RegOpenKey	HKCR\CLSID\{397a2e5f-348c-482d-b9...	NAME NOT FOUND	Desired Access: Read
11:50:56.577...	svchost.exe	1328	RegCloseKey	HKCR\CLSID\{397a2e5f-348c-482d-b9...	SUCCESS	
11:50:56.936...	DFSRs.exe	2568	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN JOURNAL
Showing 31,845 of 200,252 events (15%)		Backed by virtual memory				

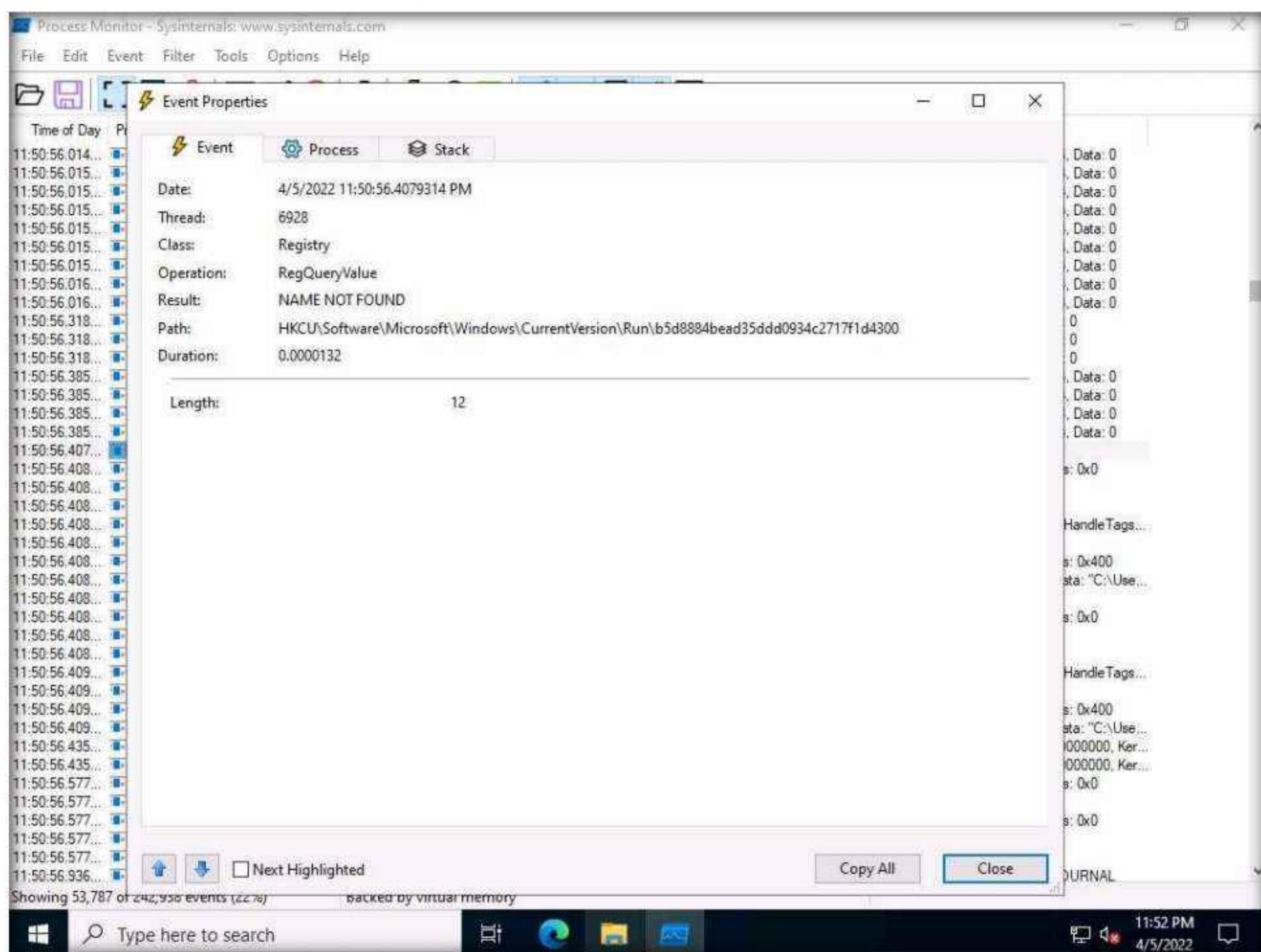
Module 07 – Malware Threats

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.



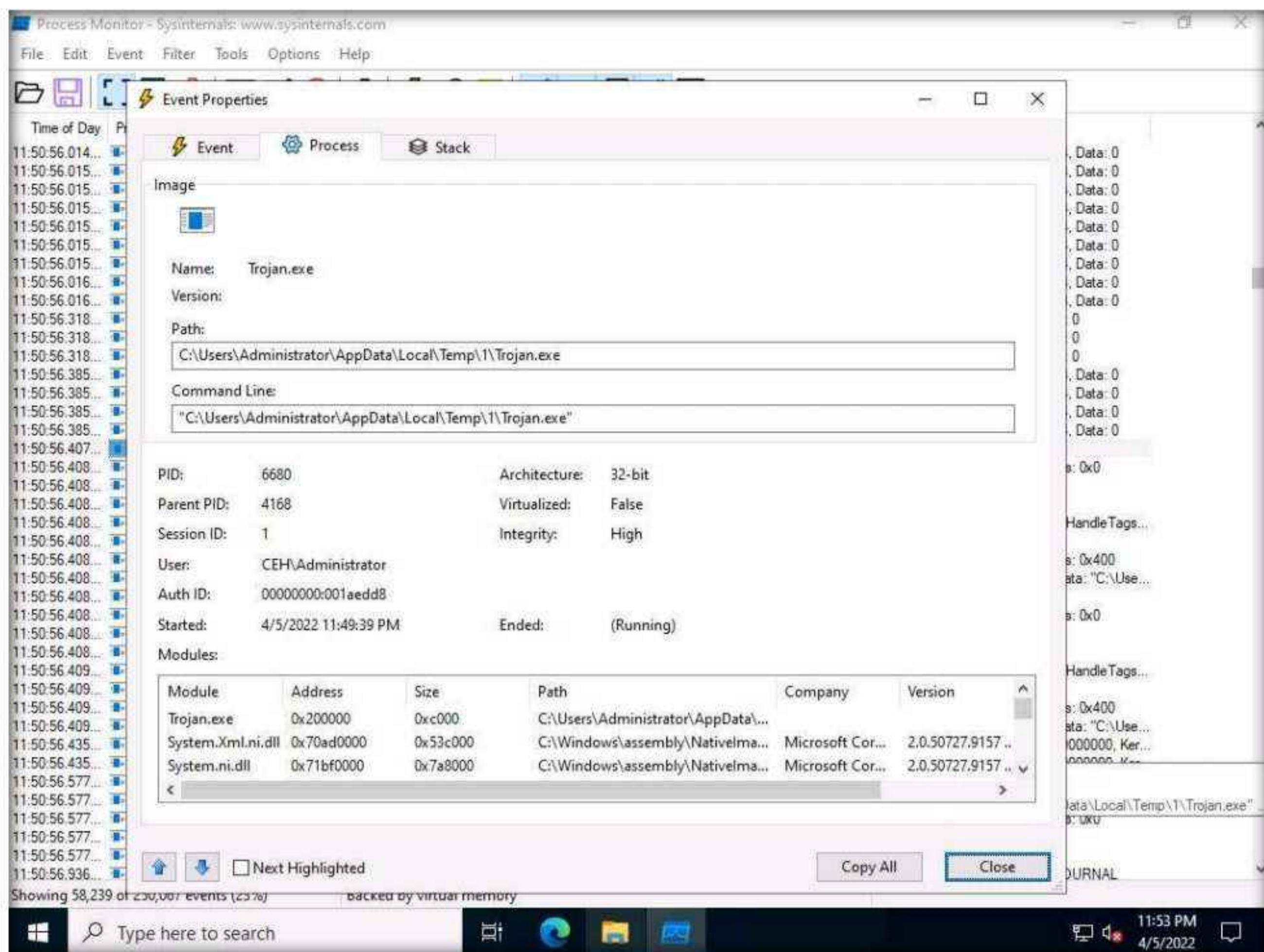
Module 07 – Malware Threats

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.



Module 07 – Malware Threats

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.



Module 07 – Malware Threats

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

The screenshot shows the 'Event Properties' window with the 'Stack' tab selected. The window displays a table of memory stack frames, each with a Frame number, Module name, Location, Address, and Path. The table has 30 rows, starting with Frame 0 (ntoskrnl.exe) and ending with Frame 30 (mscorwks.dll). The 'Path' column shows the full file path for each module, such as C:\Windows\system32\ntoskrnl.exe or C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\v0de306&fe880013ac1ab7eee9eac23. At the bottom of the window, there are buttons for 'Properties...', 'Search...', 'Source...', 'Save...', 'Copy All', and 'Close'.

Frame	Module	Location	Address	Path
K 0	ntoskrnl.exe	RtlAnsiCharToUnicodeChar + 0x2c26	0xffff80736d8ad26	C:\Windows\system32\ntoskrnl.exe
K 1	ntoskrnl.exe	RtlAnsiCharToUnicodeChar + 0xadf	0xffff80736d88bd	C:\Windows\system32\ntoskrnl.exe
K 2	ntoskrnl.exe	setjmpex + 0x7e85	0xffff80736a28a35	C:\Windows\system32\ntoskrnl.exe
U 3	ntdll.dll	ZwQueryValueKey + 0x14	0x7fb2bf01d4	C:\Windows\SYSTEM32\ntdll.dll
U 4	wow64.dll	Wow64LogPrint + 0x157d	0x7fb2bc982d	C:\Windows\System32\wow64.dll
U 5	wow64.dll	Wow64SystemServiceEx + 0x15a	0x7fb2bc961a	C:\Windows\System32\wow64.dll
U 6	wow64cpu.dll	TurboDispatchJumpAddressEnd + 0xb	0x77e017ba	C:\Windows\System32\wow64cpu.dll
U 7	wow64cpu.dll	BTcpuSimulate + 0x9	0x77e011c9	C:\Windows\System32\wow64cpu.dll
U 8	wow64.dll	Wow64KiUserCallbackDispatcher + 0x66d	0x7fb2bcd5d	C:\Windows\System32\wow64.dll
U 9	wow64.dll	Wow64LdrInitialize + 0x12d	0x7fb2bcd7d	C:\Windows\System32\wow64.dll
U 10	ntdll.dll	LdrInitShimEngineDynamic + 0x2d5b	0x7fb2bf461b	C:\Windows\SYSTEM32\ntdll.dll
U 11	ntdll.dll	LdrInitializeThunk + 0x208	0x7fb2bee8058	C:\Windows\SYSTEM32\ntdll.dll
U 12	ntdll.dll	LdrStandardizeSystemPath + 0x23d	0x7fb2bf0d90d	C:\Windows\SYSTEM32\ntdll.dll
U 13	ntdll.dll	LdrInitializeThunk + 0xe	0x7fb2bee7e5e	C:\Windows\SYSTEM32\ntdll.dll
U 14	ntdll.dll	NtQueryValueKey + 0xc	0x77e83d2c	C:\Windows\SysWOW64\ntdll.dll
U 15	KERNELBASE.dll	RegQueryValueExW + 0x2f3	0x77cbf073	C:\Windows\SysWOW64\KERNELBASE.dll
U 16	KERNELBASE.dll	RegQueryValueExW + 0xd3	0x77cbe53	C:\Windows\SysWOW64\KERNELBASE.dll
U 17	<unknown>	0xbfa40e	0xbfa40e	
U 18	mscorlib.ni.dll	mscorlib.ni.dll + 0x23468f	0x725d468f	C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\v0de306&fe880013ac1ab7eee9eac23
U 19	mscorlib.ni.dll	mscorlib.ni.dll + 0x21d824	0x725b0824	C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\v0de306&fe880013ac1ab7eee9eac23
U 20	<unknown>	0xa40533	0xa40533	
U 21	<unknown>	0xa40076	0xa40076	
U 22	mscorwks.dll	mscorwks.dll + 0x18633	0x72e8633	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 23	mscorwks.dll	mscorwks.dll + 0x206d3	0x72ec06d3	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 24	mscorwks.dll	mscorwks.dll + 0x20706	0x72ec0706	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 25	mscorwks.dll	mscorwks.dll + 0x20724	0x72ec0724	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 26	mscorwks.dll	GetPrivateContextsPerfCounters + 0x345ba	0x72f8093d	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 27	mscorwks.dll	GetPrivateContextsPerfCounters + 0x344da	0x72f8085d	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 28	mscorwks.dll	GetPrivateContextsPerfCounters + 0x349f7	0x72f80d7a	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 29	mscorwks.dll	CorExeMain + 0x168	0x72f80f64	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
U 30	mscorwks.dll	CorExeMain + 0x98	0x72f80e94	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll

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

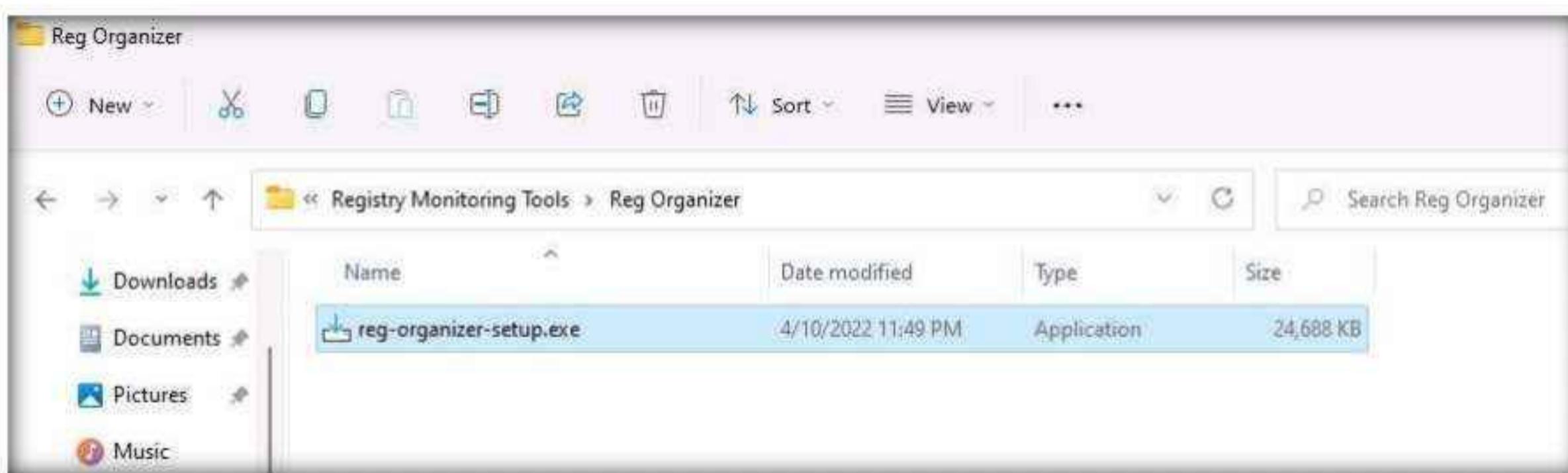
The Windows Registry stores OS and program configuration details such as settings and options. If the malware is a program, the registry stores its functionality. When an attacker installs a type of malware on the victim's machine, it generates a registry entry. One must have fair knowledge of the Windows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

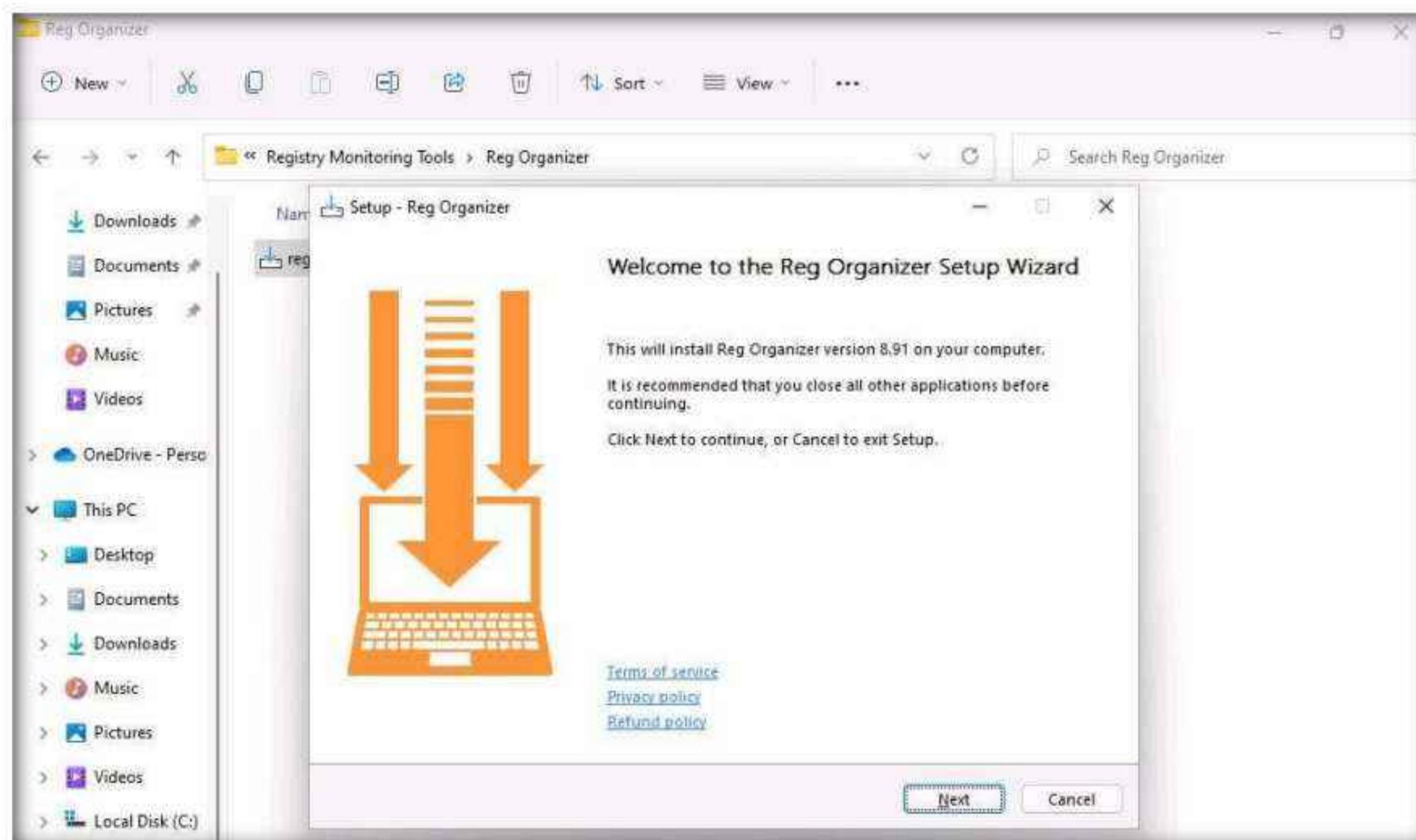
Reg Organizer: Reg Organizer is designed to edit keys and parameters, as well as to delete the content of.reg files. It allows users to perform various operations with the system registry such as export, import and copy key values. It can also perform a deep search to find even those keys associated 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**.

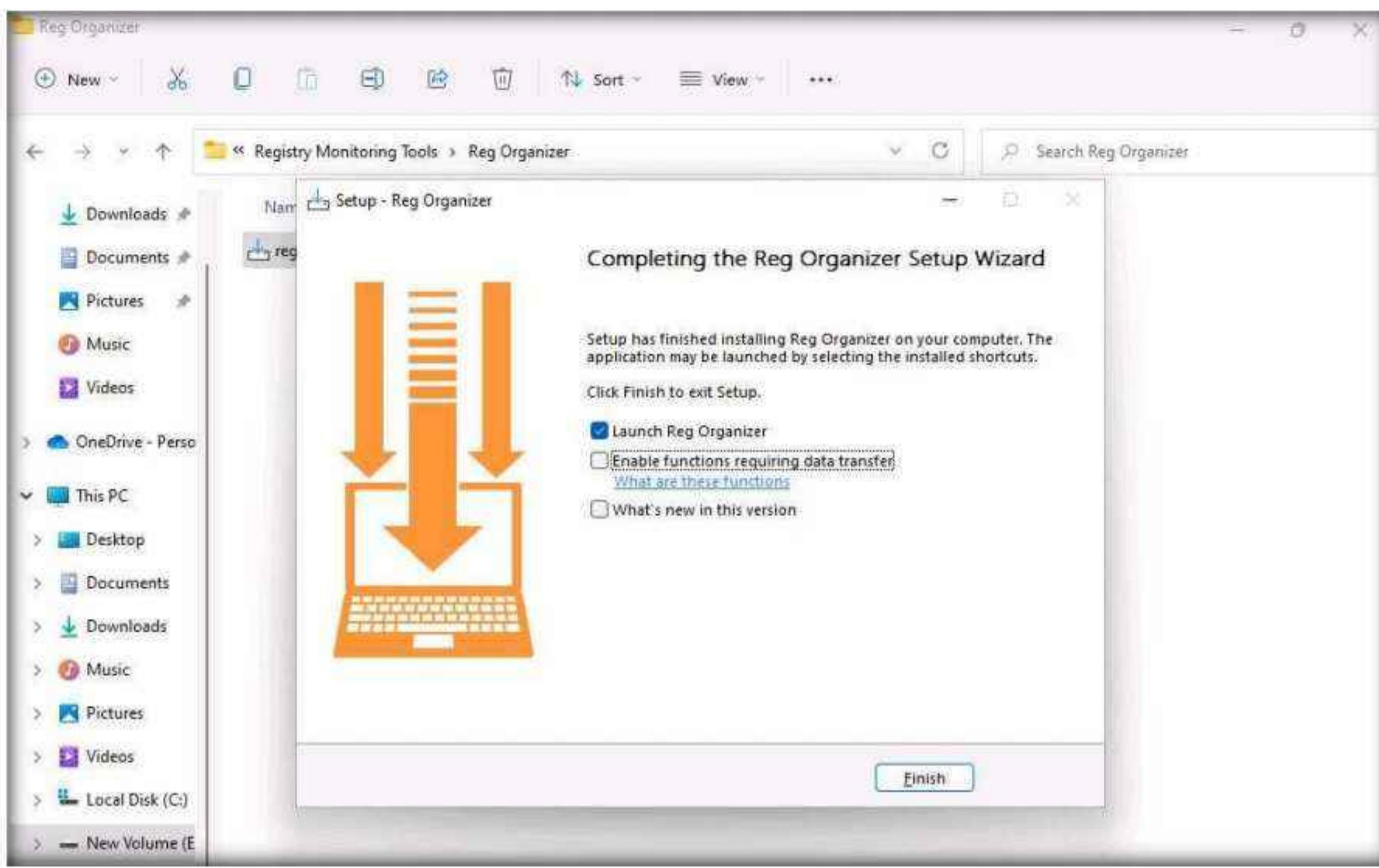


3. If **Open File - Security Warning** window appears, click **Run**.
4. If **User Account Control** window appears, click **Yes**.
5. **Setup - Reg Organizer** window appears, click **Next**.

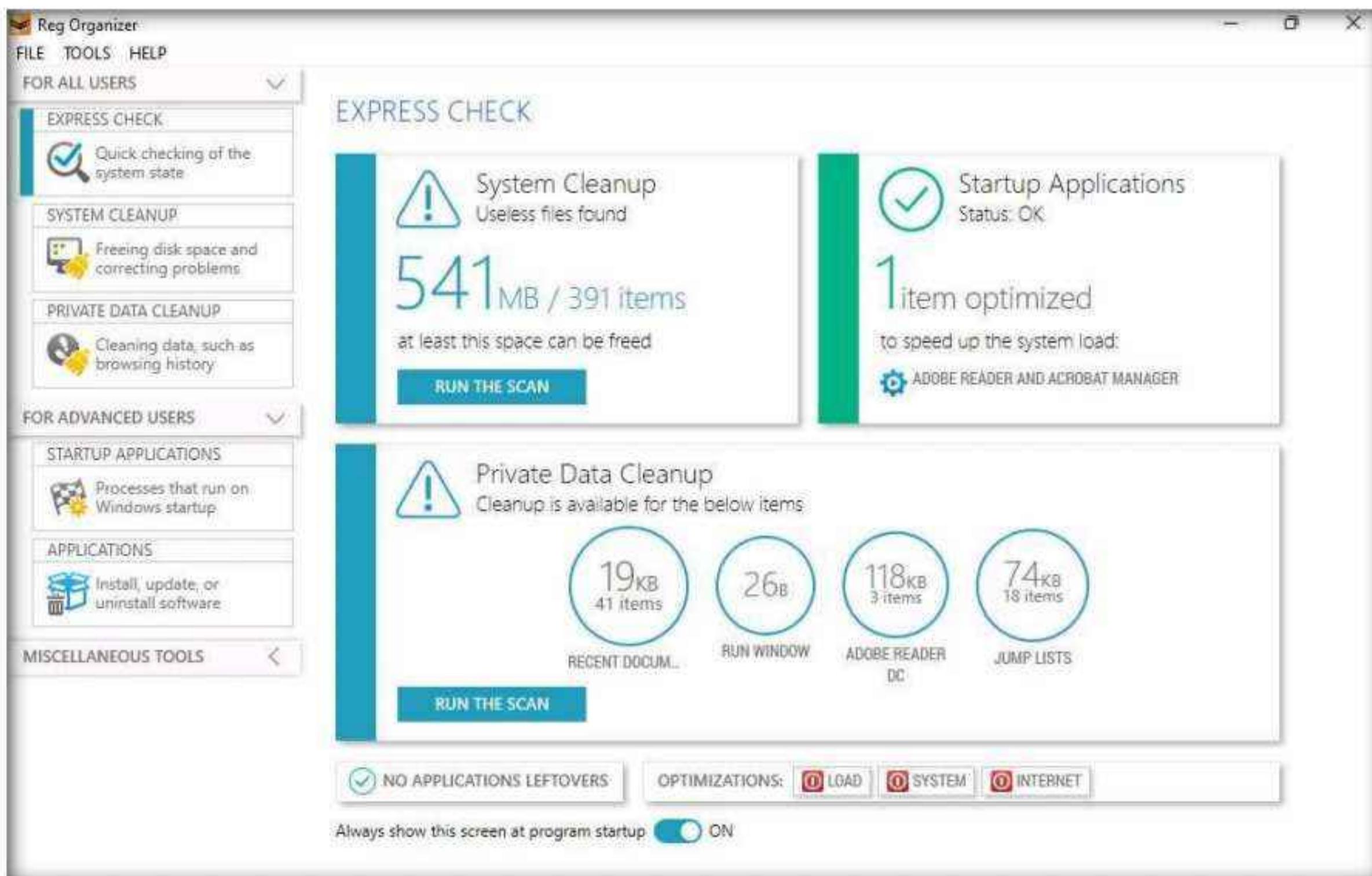


Module 07 – Malware Threats

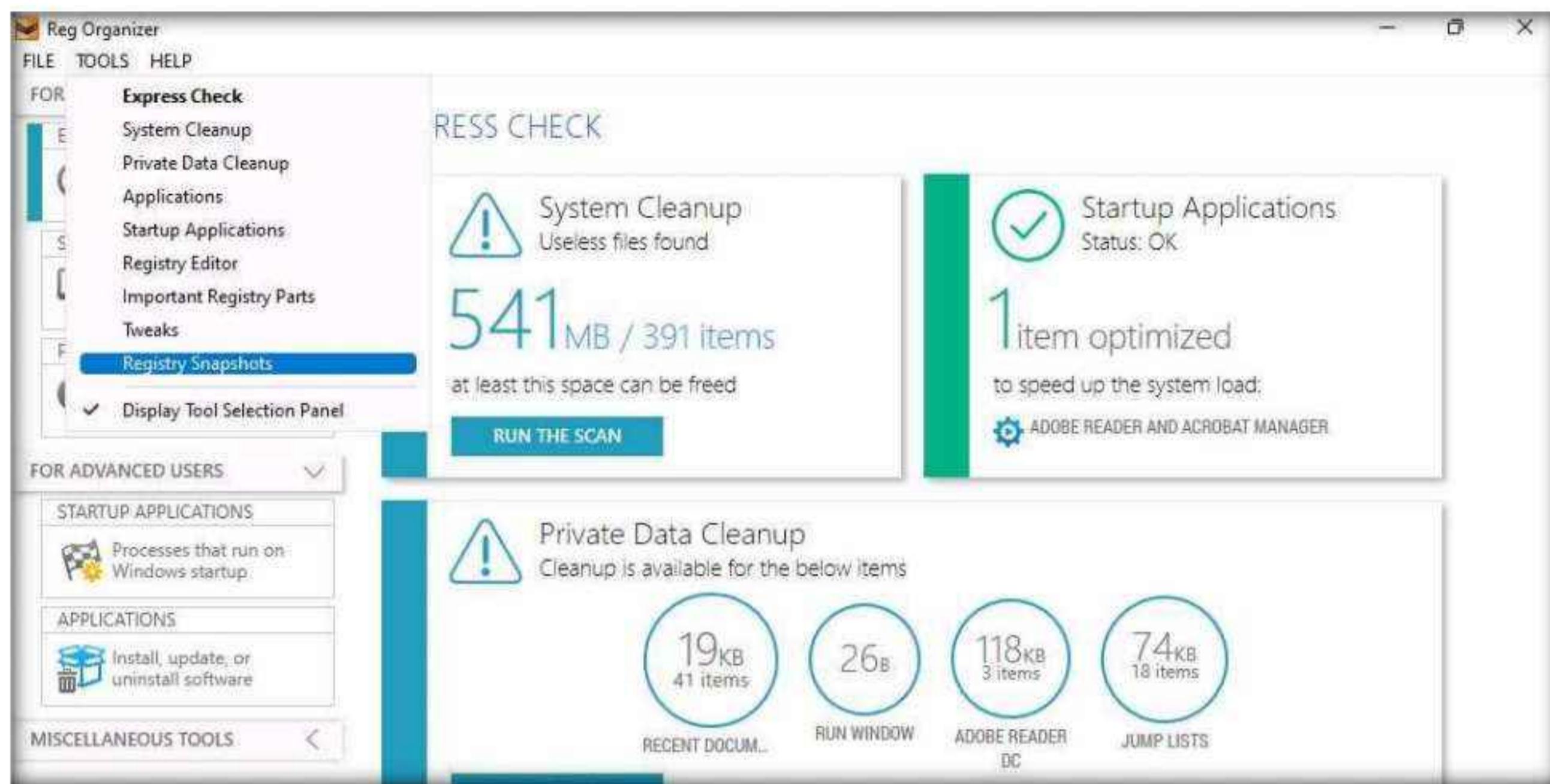
6. Follow the wizard-driven installation steps to install the Reg Organizer.
7. After the completion of installation, **Completing the Reg Organizer Setup Wizard** appears, uncheck **Enable functions requiring data transfer** and **What's new in this version** checkboxes and click **Finish**.



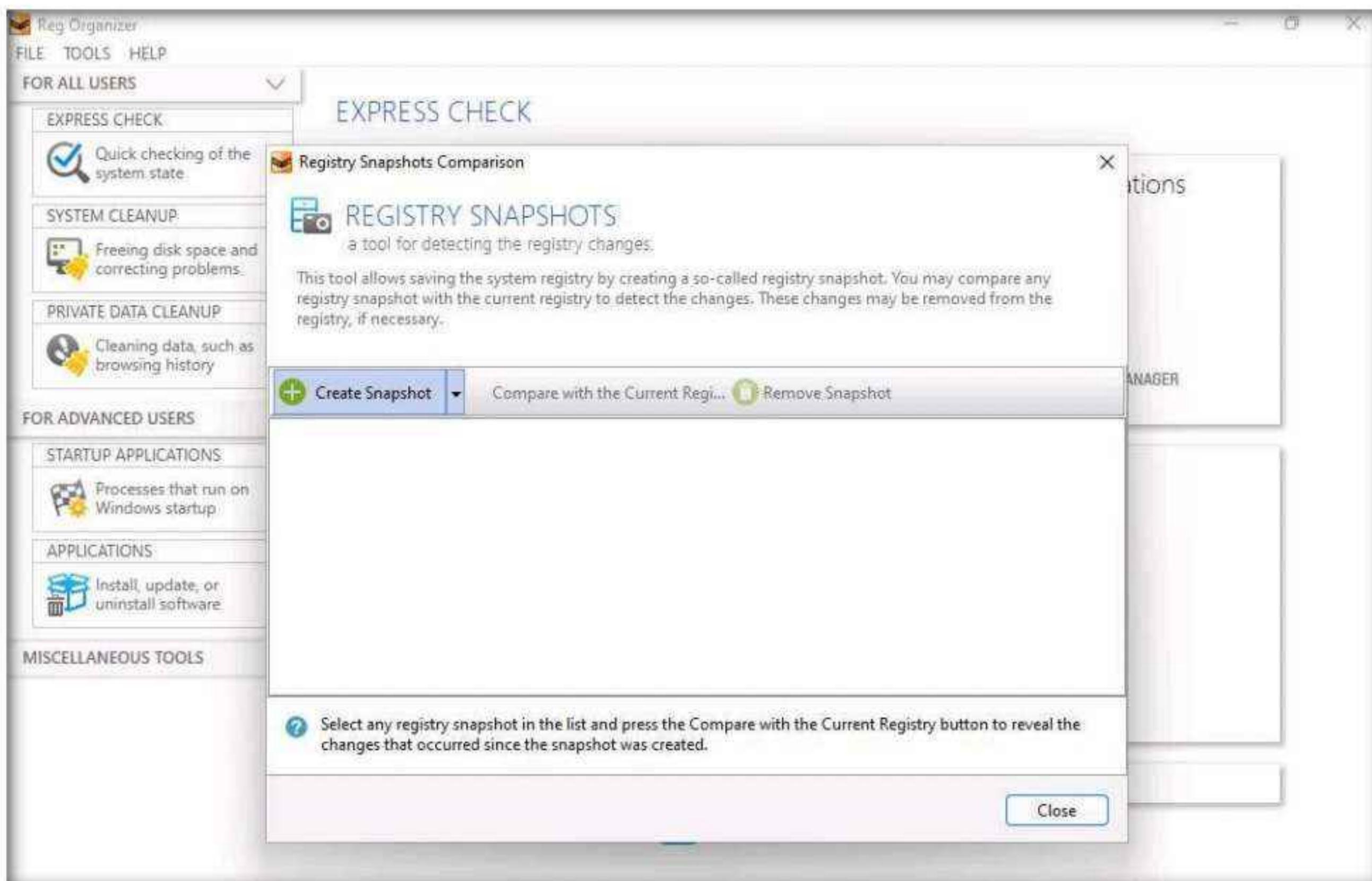
8. **Reg Organization** main window appears, displaying **System Cleanup**, **Startup Applications** and **Private Data Cleanup** sections, as shown in the screenshot.



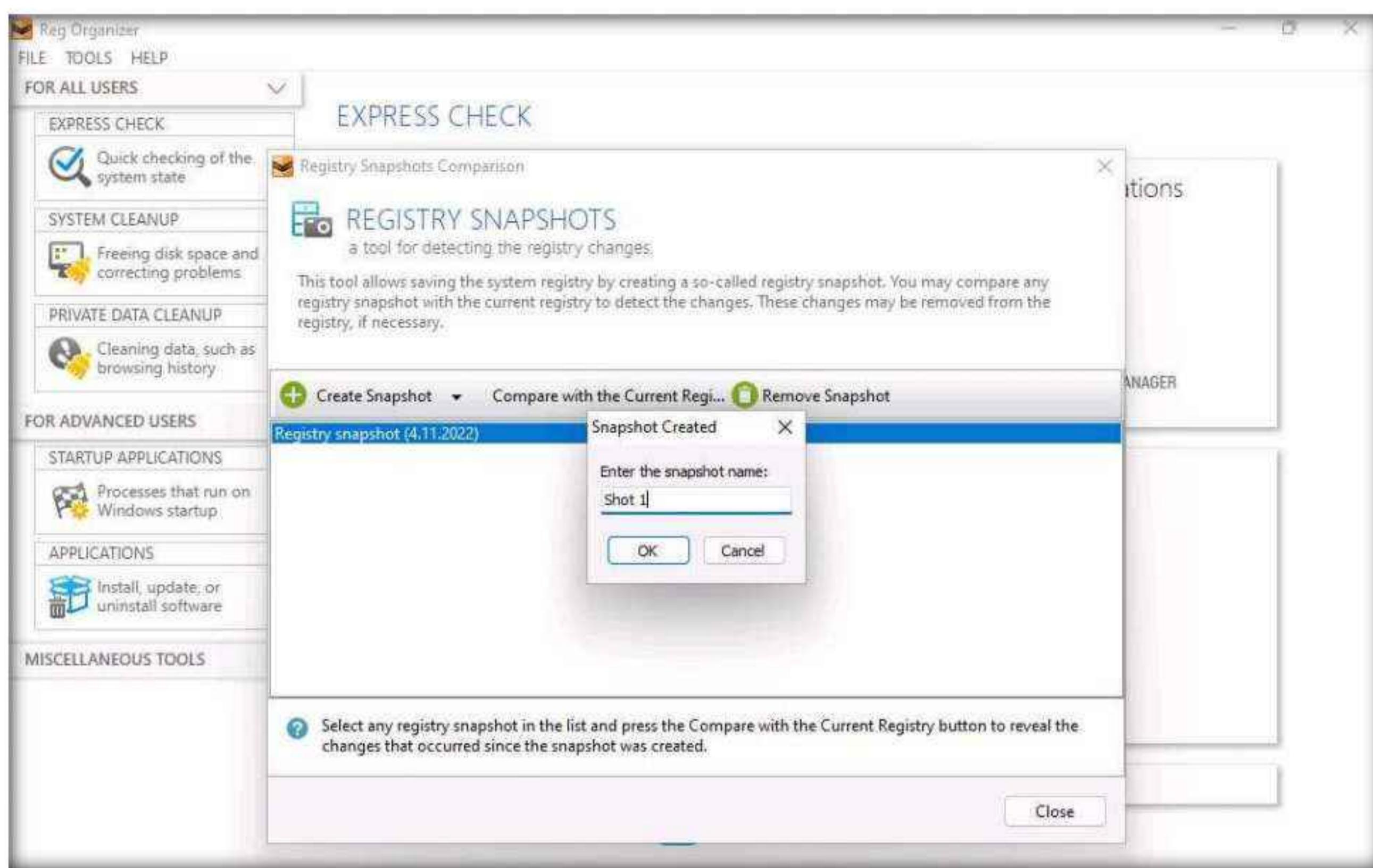
9. Now, click **TOOLS** from the menu bar and select **Registry Snapshots** option from the context menu.



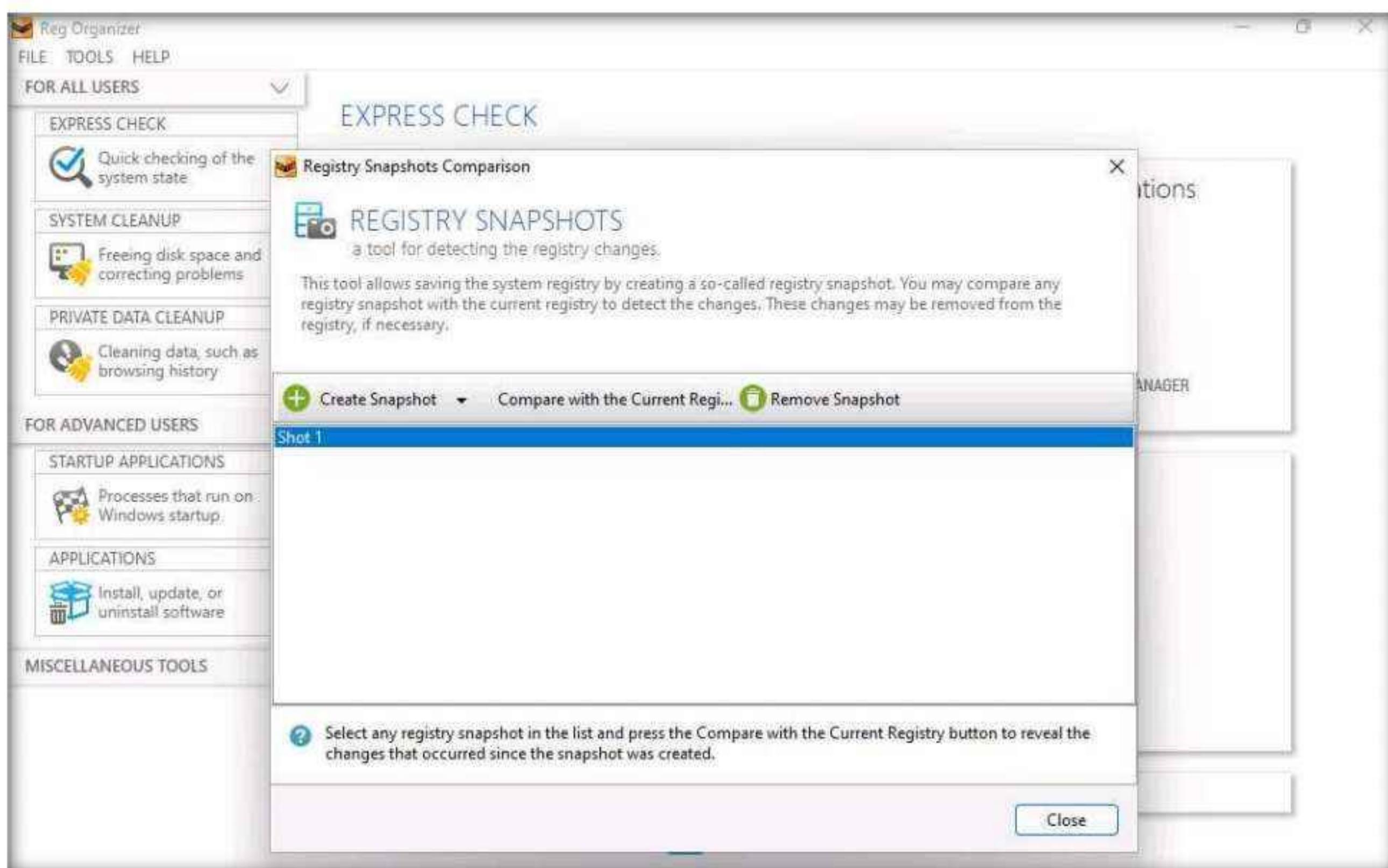
10. Registry Snapshots Comparison window appears, click **Create Snapshot** option.



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**.

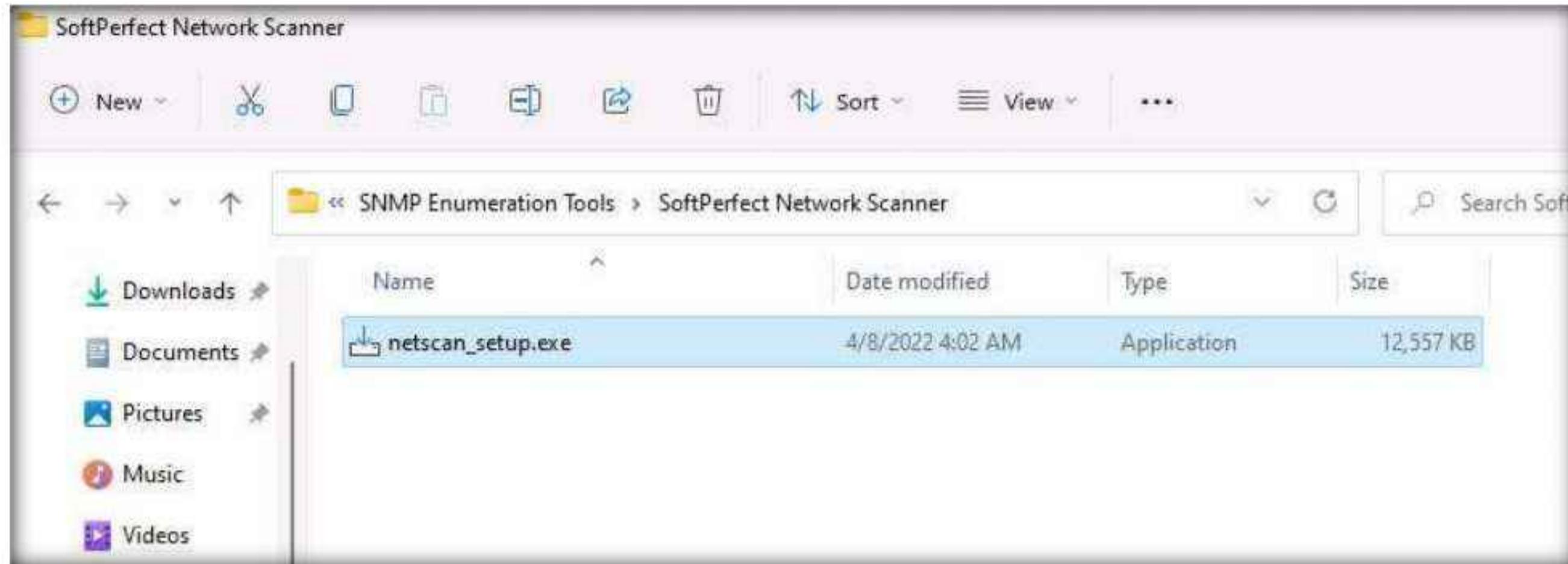


12. **Shot 1** is created and appears in the middle pane, as shown in the screenshot.

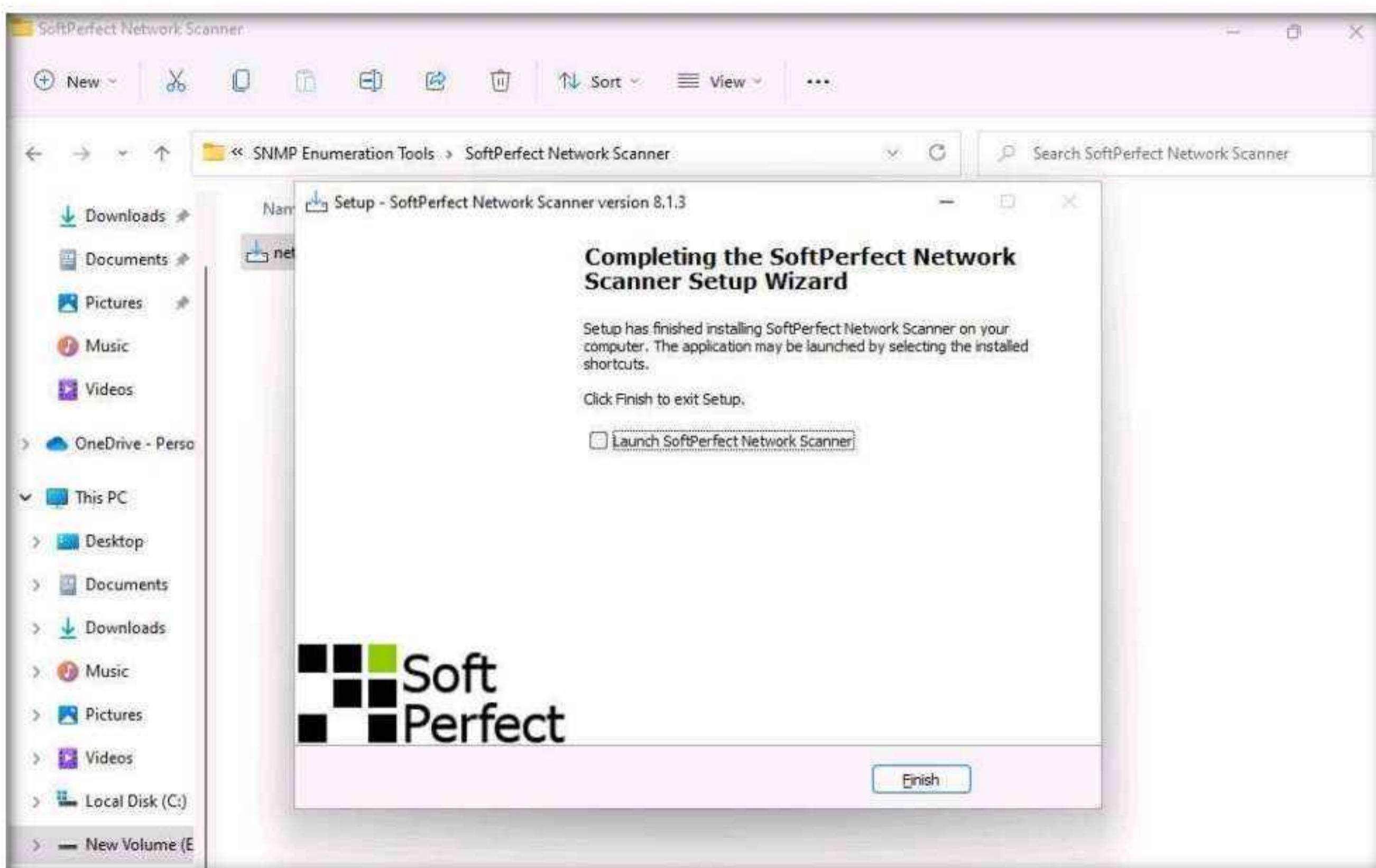


Module 07 – Malware Threats

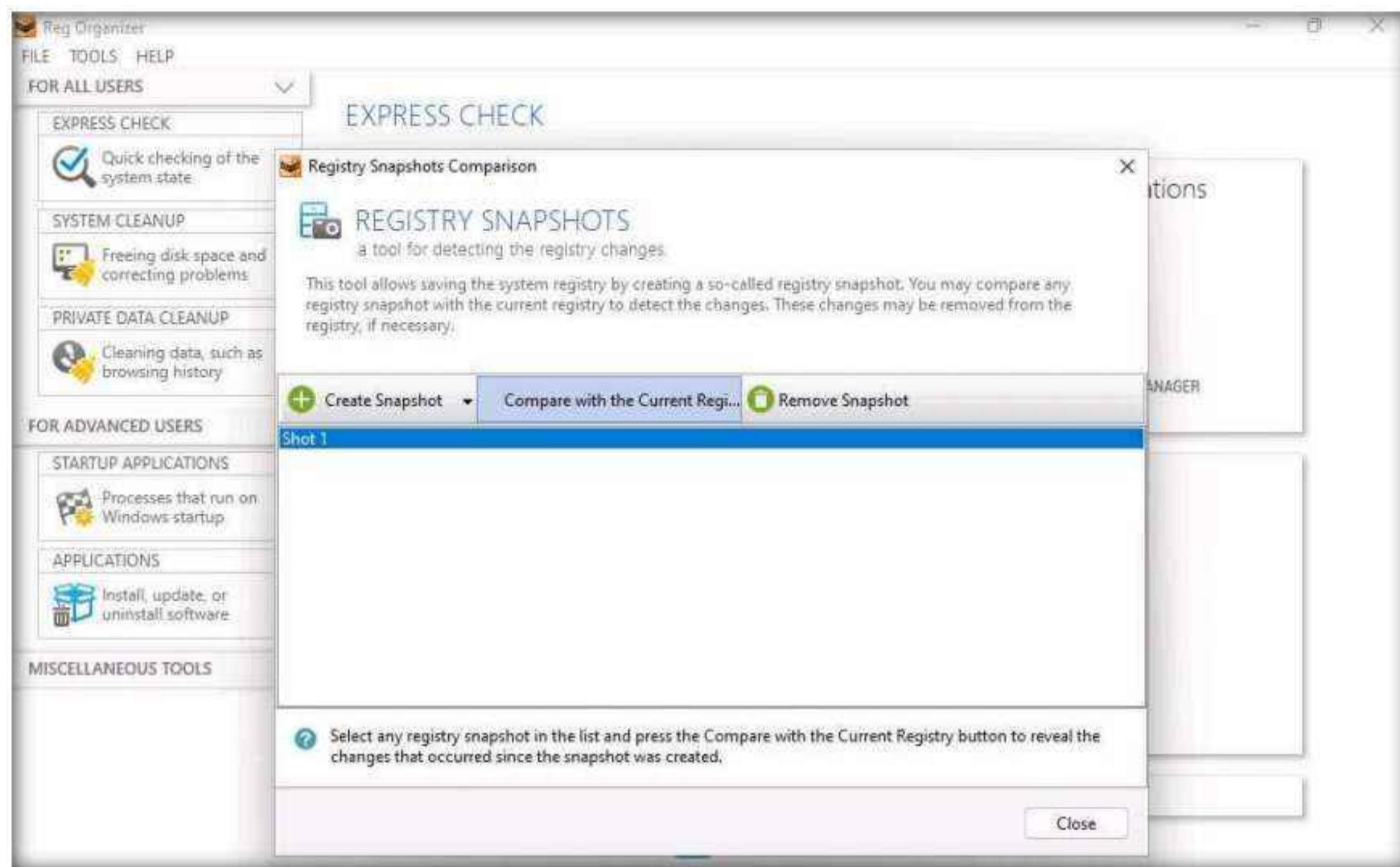
13. To demonstrate a change in the registry, install any application (here, **SoftPerfect Network Scanner**). However, you can install any application of your choice to identify changes in the registry entries.
14. Navigate to **E:\CEH-Tools\CEHv12 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect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

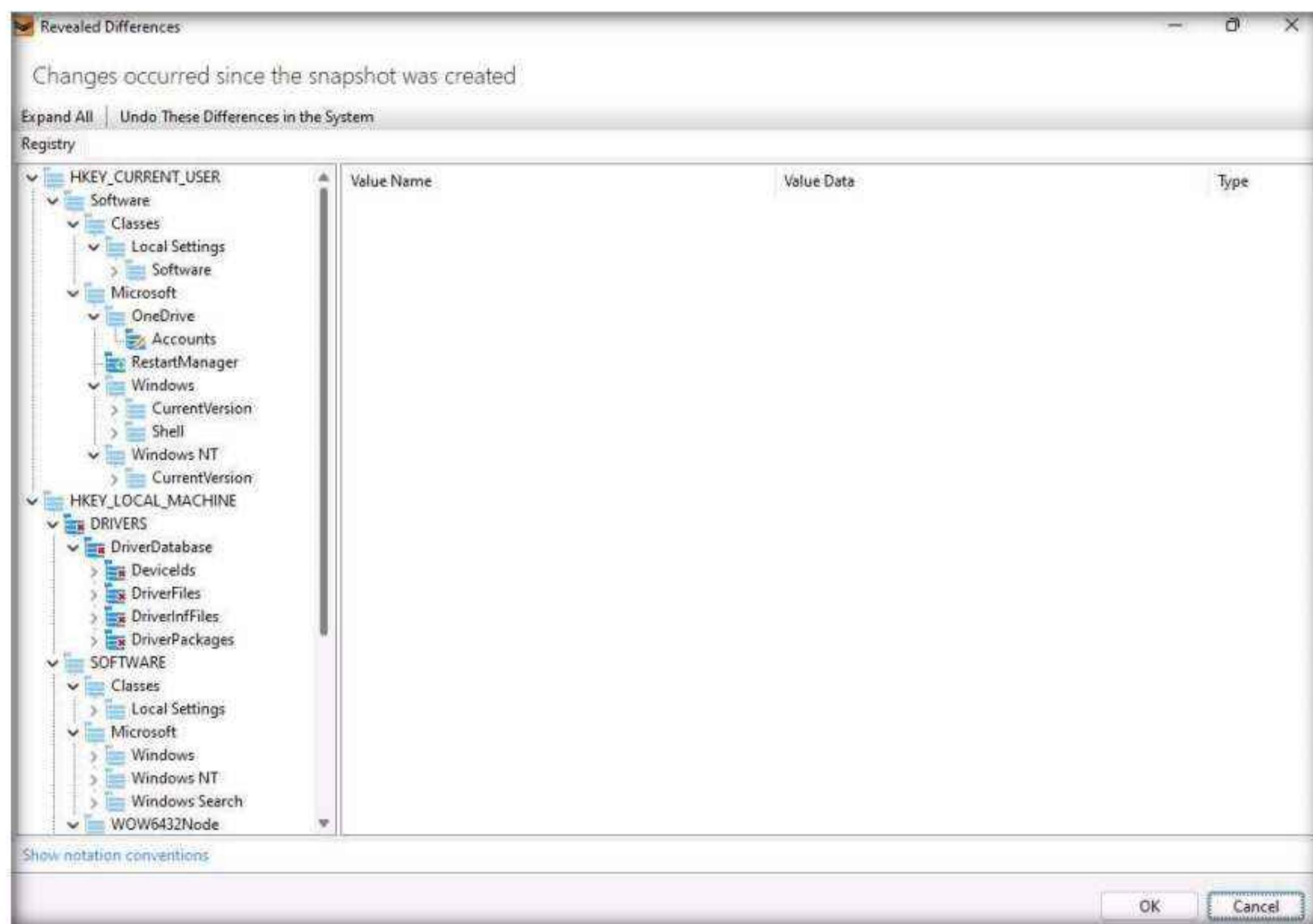


17. Now, click **Compare with Current Registry** option to compare the changes in the registry entries before and after installing SoftPerfect Network Scanner application.



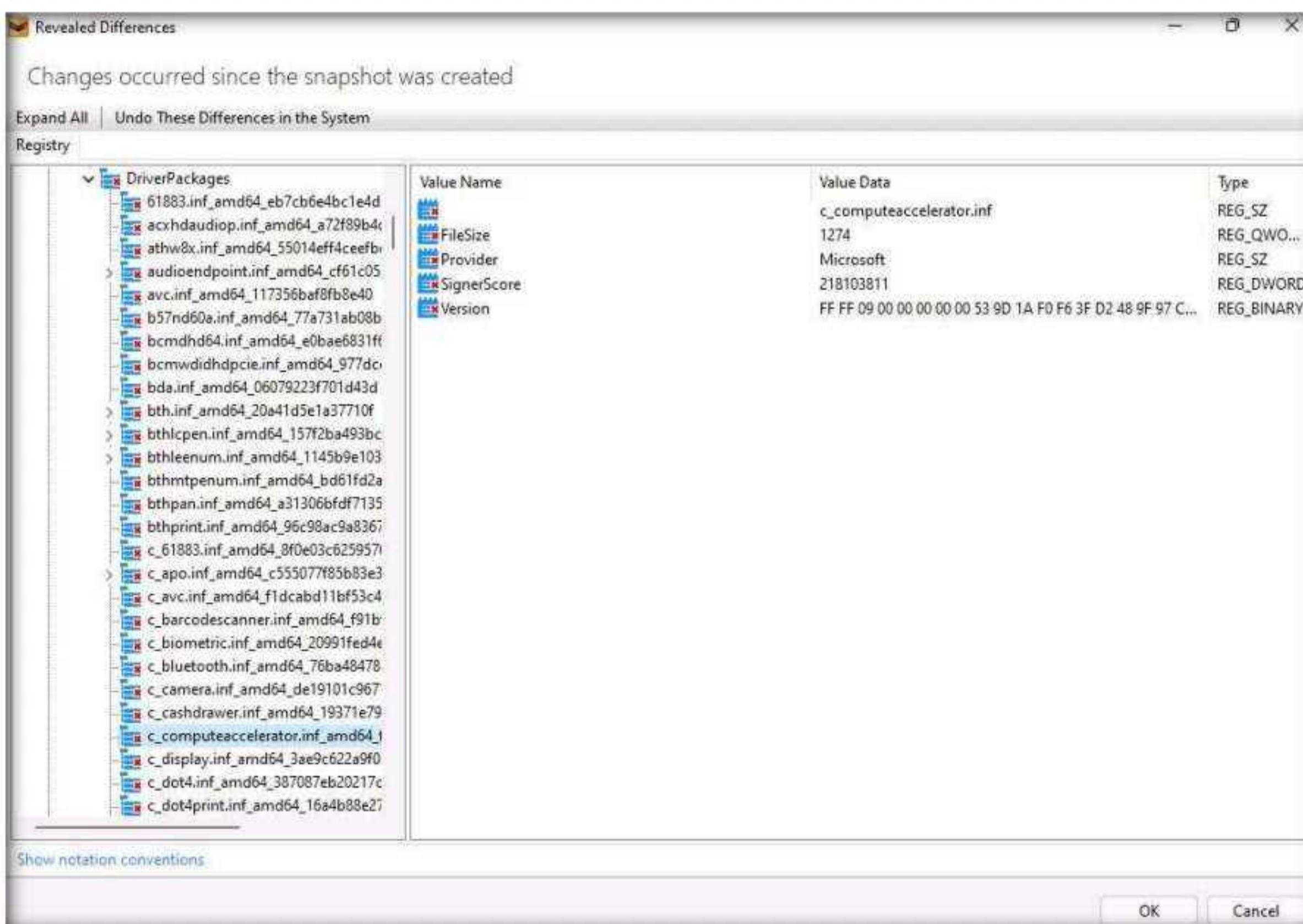
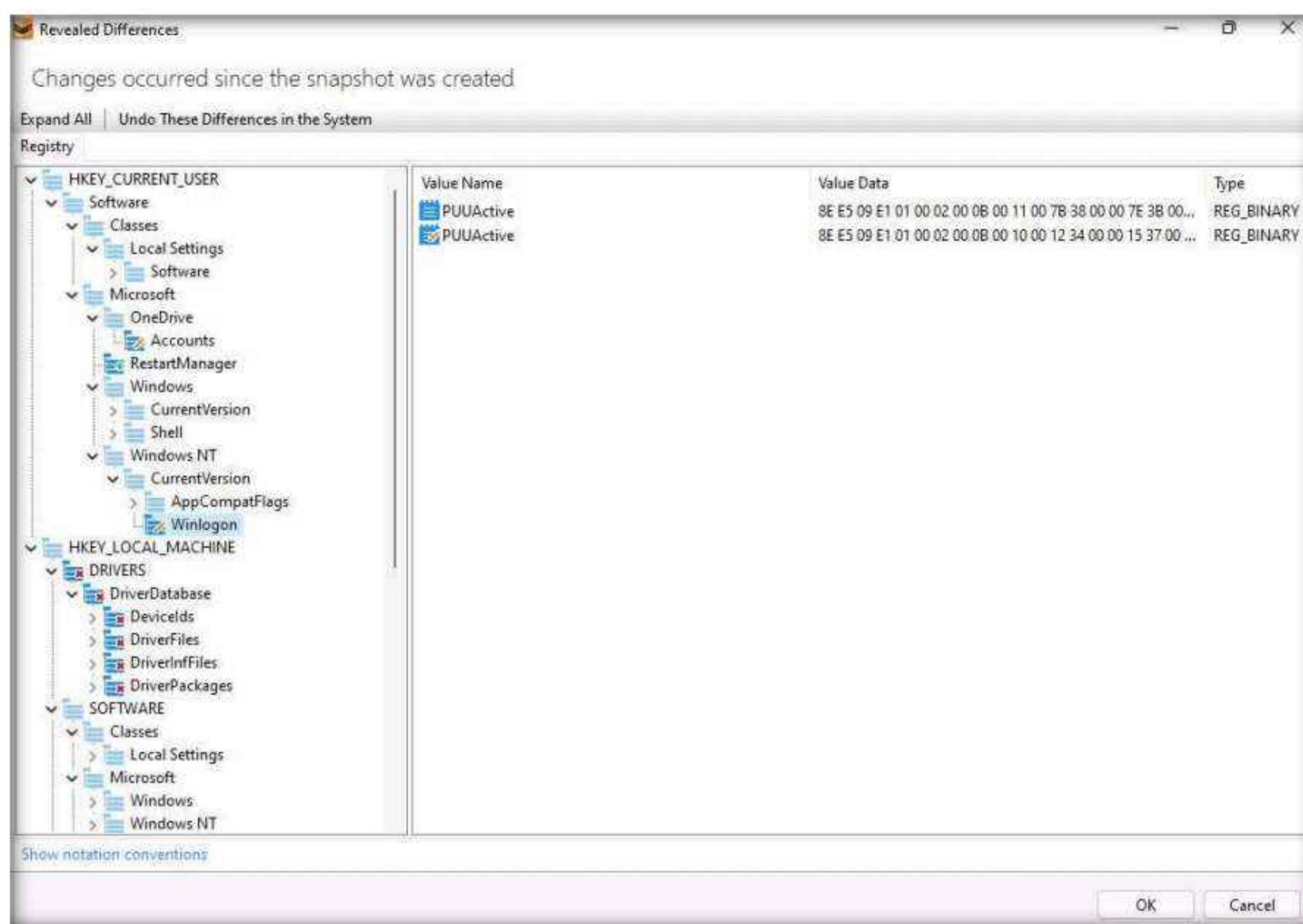
18. Detecting changes... process initializes and after it completes **Revealed Differences** window appears, as shown in the screenshot.

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



Module 07 – Malware Threats

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.

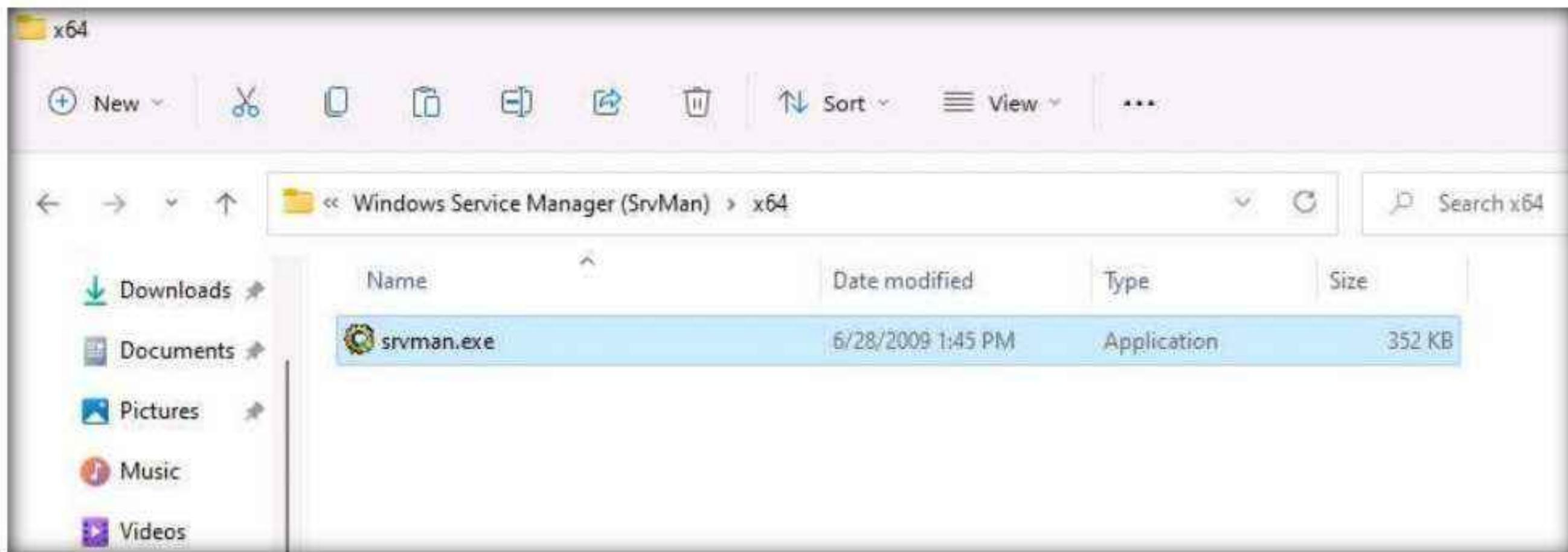
SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

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

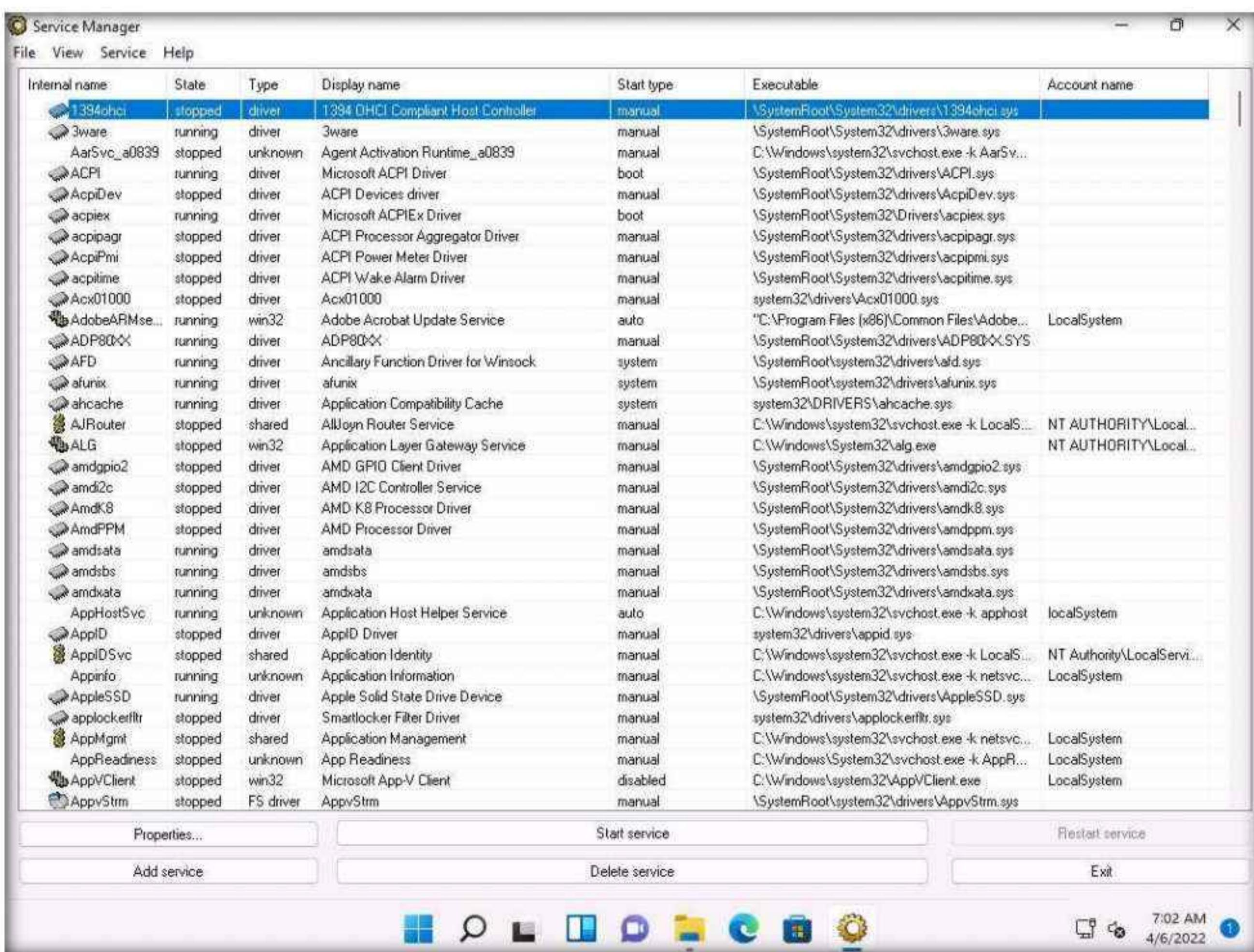
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\x64** and double-click **srvman.exe**.

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

Module 07 – Malware Threats



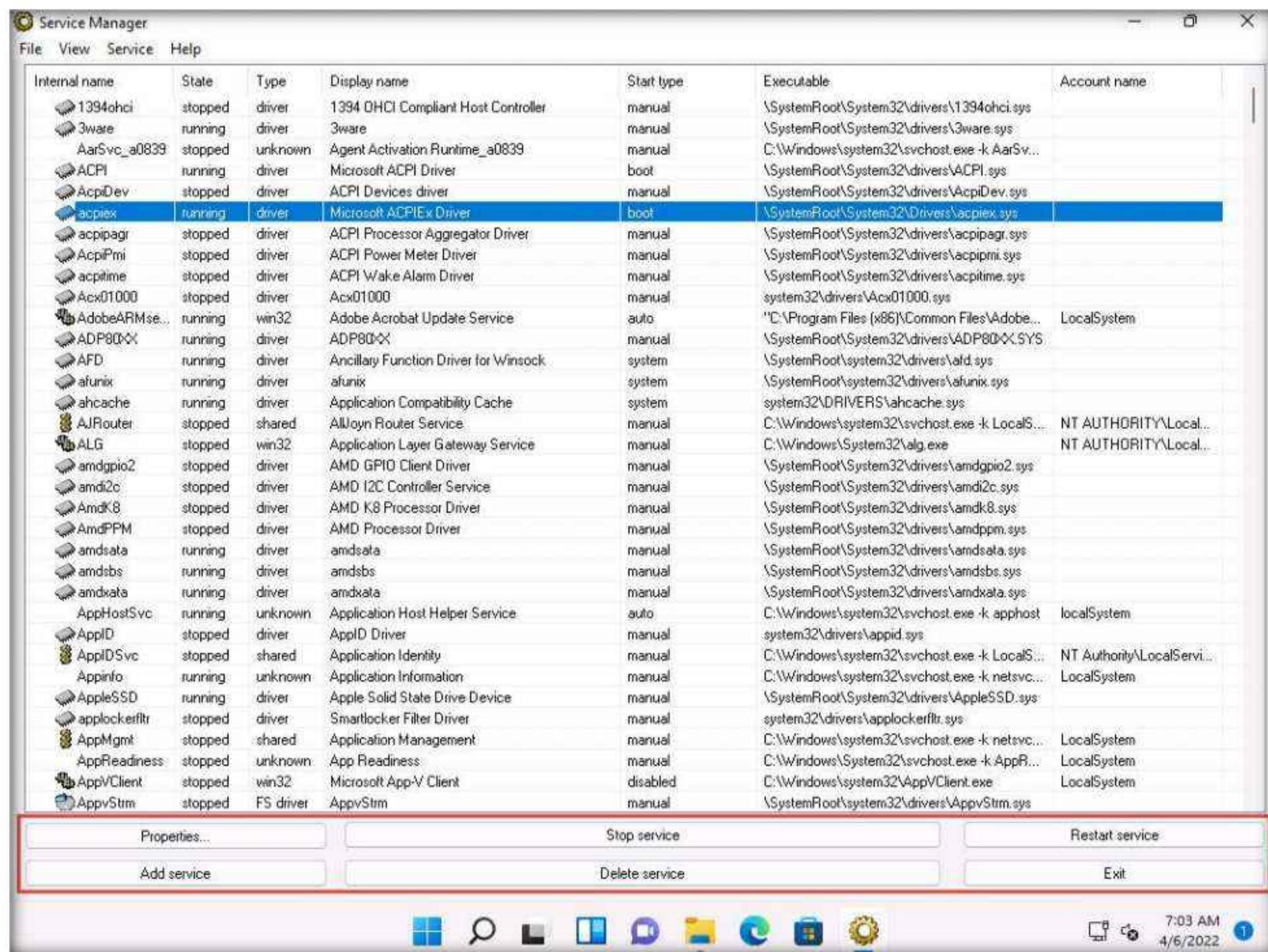
2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.



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.

Module 07 – Malware Threats

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.

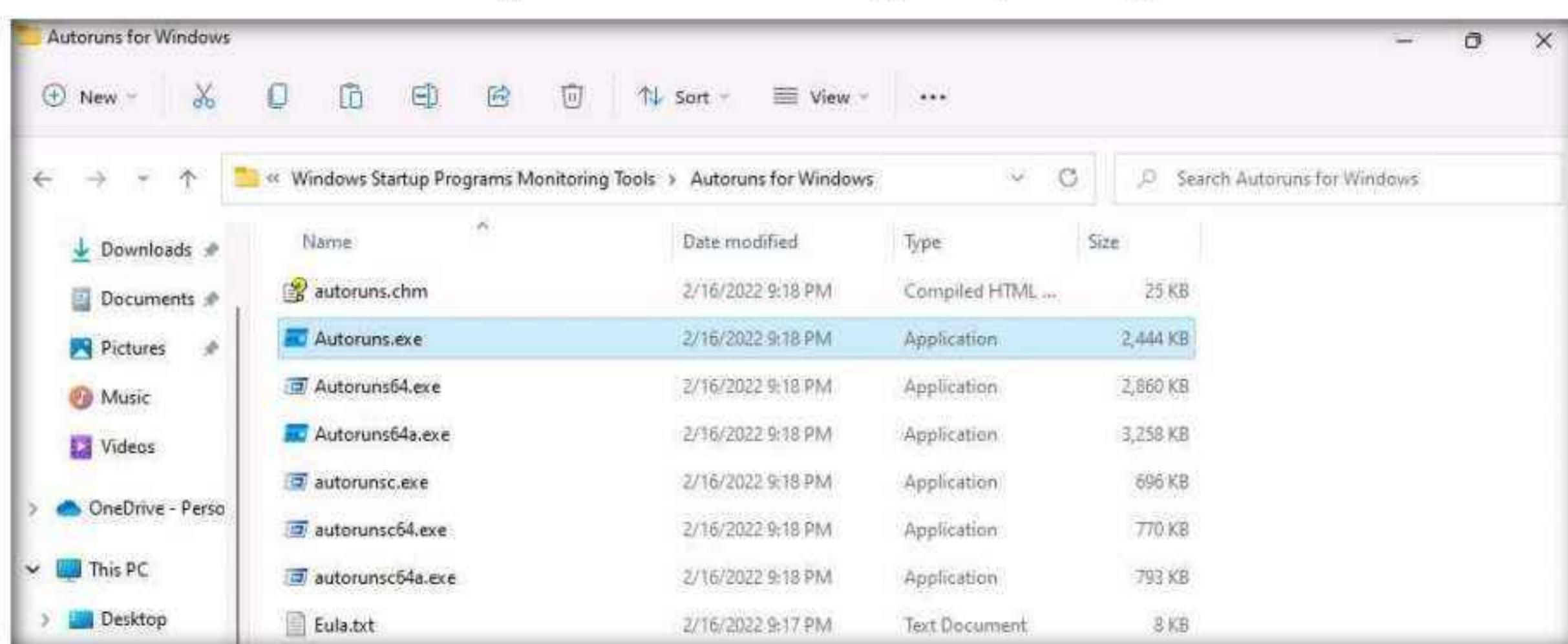
An ethical hacker or penetration tester must identify the applications or processes that start when a system boots up and remove any unwanted or malicious programs that can breach privacy or affect a system's health. Therefore, scanning for suspicious startup programs manually or using startup program 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**.



Module 07 – Malware Threats

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.

Autoruns Entry	Description	Publisher	Image Path
Logon			
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
MicrosoftEdgeAutoLaunch_5EFC0ECB77A7585FE9DCDD0B2E94...	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Micro
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Loc
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce			
Delete Cached Standalone Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
Delete Cached Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
Uninstall 22.002.0103.0004	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
HKLM\Software\Microsoft\Active Setup\Installed Components			
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chr
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Micro
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscor
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Comm
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components			
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscor
Explorer			
HKCU\Software\Classes*\ShellEx\ContextMenuHandlers			

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

Autoruns Entry	Description	Publisher	Image Path
Logon			
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
MicrosoftEdgeAutoLaunch_5EFC0ECB77A7585FE9DCDD0B2E94...	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Micro
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Loc
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce			
Delete Cached Standalone Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
Delete Cached Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
Uninstall 22.002.0103.0004	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e
HKLM\Software\Microsoft\Active Setup\Installed Components			
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chr
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Micro
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscor
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Comm
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components			
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscor
Explorer			
HKCU\Software\Classes*\ShellEx\ContextMenuHandlers			

Module 07 – Malware Threats

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

Autoruns Entry	Description	Publisher	Image Path
HKCU\Software\Classes*\ShellEx\ContextMenuHandlers			
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Local\OneDrive\ShellExt\FileSyncEx.dll
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Local\OneDrive\ShellExt\FileSyncEx.dll
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Local\OneDrive\ShellExt\FileSyncEx.dll
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers			
ANotepad++64	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	C:\Program Files\Notepad++\Notepad++.exe
EPP	Microsoft Security Client Shell Extension	(Not Verified) Microsoft Corporation	C:\Program Files\Windows Defender\EPP\ShellExt\EPP.dll
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers			
EPP	Microsoft Security Client Shell Extension	(Not Verified) Microsoft Corporation	C:\Program Files\Windows Defender\EPP\ShellExt\EPP.dll
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers			
EPP	Microsoft Security Client Shell Extension	(Not Verified) Microsoft Corporation	C:\Program Files\Windows Defender\EPP\ShellExt\EPP.dll
HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers			
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	C:\Program Files\WinRAR\winRAR.dll
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers			
OneDrive1	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Local\OneDrive\ShellExt\OneDrive1.dll
OneDrive2	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Local\OneDrive\ShellExt\OneDrive2.dll
OneDrive3	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Local\OneDrive\ShellExt\OneDrive3.dll
OneDrive4	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Admin\AppData\Local\OneDrive\ShellExt\OneDrive4.dll

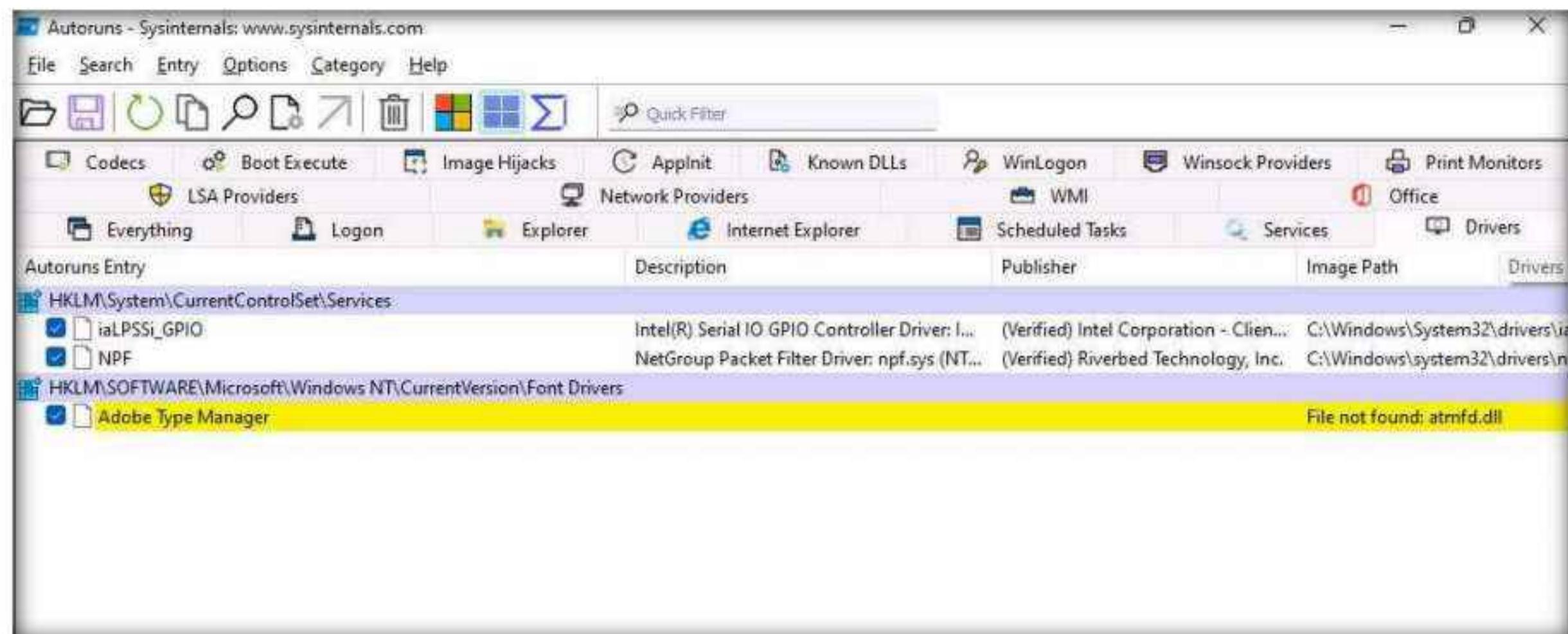
6. Clicking the **Services** tab displays all services that run automatically at system startup.

Autoruns Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Services			
AdobeARMservice	Adobe Acrobat Update Service: Adobe Ac...	(Verified) Adobe Inc.	C:\Program Files (x86)\Common Files\Adobe\Update\AdobeARMservice.exe
edgeupdate	Microsoft Edge Update Service (edgeupd...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\edgeupdate.exe
edgeupdatem	Microsoft Edge Update Service (edgeupd...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\edgeupdatem.exe
FontCache3.0.0.0	Windows Presentation Foundation Font ...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\FrameWork\v4.0.30319\FontCache.exe
GoogleChromeElevationService	Google Chrome Elevation Service (Googl...	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\GoogleChromeElevationService.exe
gupdate	Google Update Service (gupdate): Keeps ...	(Verified) Google LLC	C:\Program Files (x86)\Google\Update\gupdate.exe
gupdatem	Google Update Service (gupdatem): Keep...	(Verified) Google LLC	C:\Program Files (x86)\Google\Update\gupdatem.exe
MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Micros...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\MicrosoftEdgeElevationService.exe
MozillaMaintenance	Mozilla Maintenance Service: The Mozilla ...	(Verified) Mozilla Corporation	C:\Program Files (x86)\Mozilla\mozilla-maintenance.exe
NetTcpPortSharing	Net.Tcp Port Sharing Service: Provides abi...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319\NetTcpPortSharing.exe
rpcapd	Remote Packet Capture Protocol v.0 (exp...	(Verified) Riverbed Technology, Inc.	C:\Program Files (x86)\WinPcap\rpcapd.exe
Sense	Windows Defender Advanced Threat Prot...	(Not Verified) Microsoft Corporation	C:\Program Files\Windows Defender\Sense.exe
uhssvc	Microsoft Update Health Service: Maintai...	(Not Verified) Microsoft Corporation	C:\Program Files\Microsoft Update Health\uhssvc.exe
WMPNetworkSvc	Windows Media Player Network Sharing ...	(Not Verified) Microsoft Corporation	C:\Program Files\Windows Media\WMPNetworkSvc.exe

Module 07 – Malware Threats

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

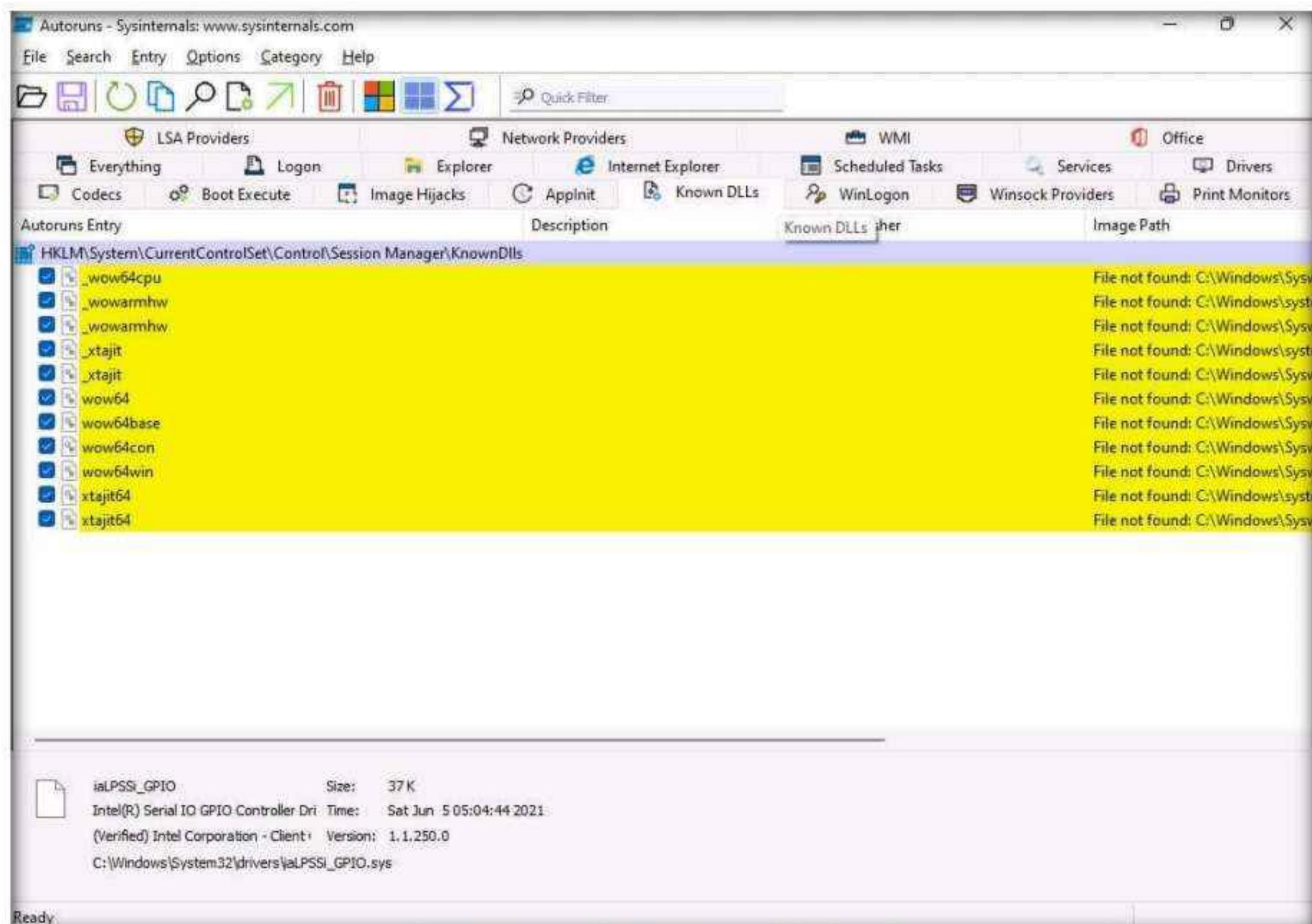
Note: The list displayed under this tab may vary when you perform this task.



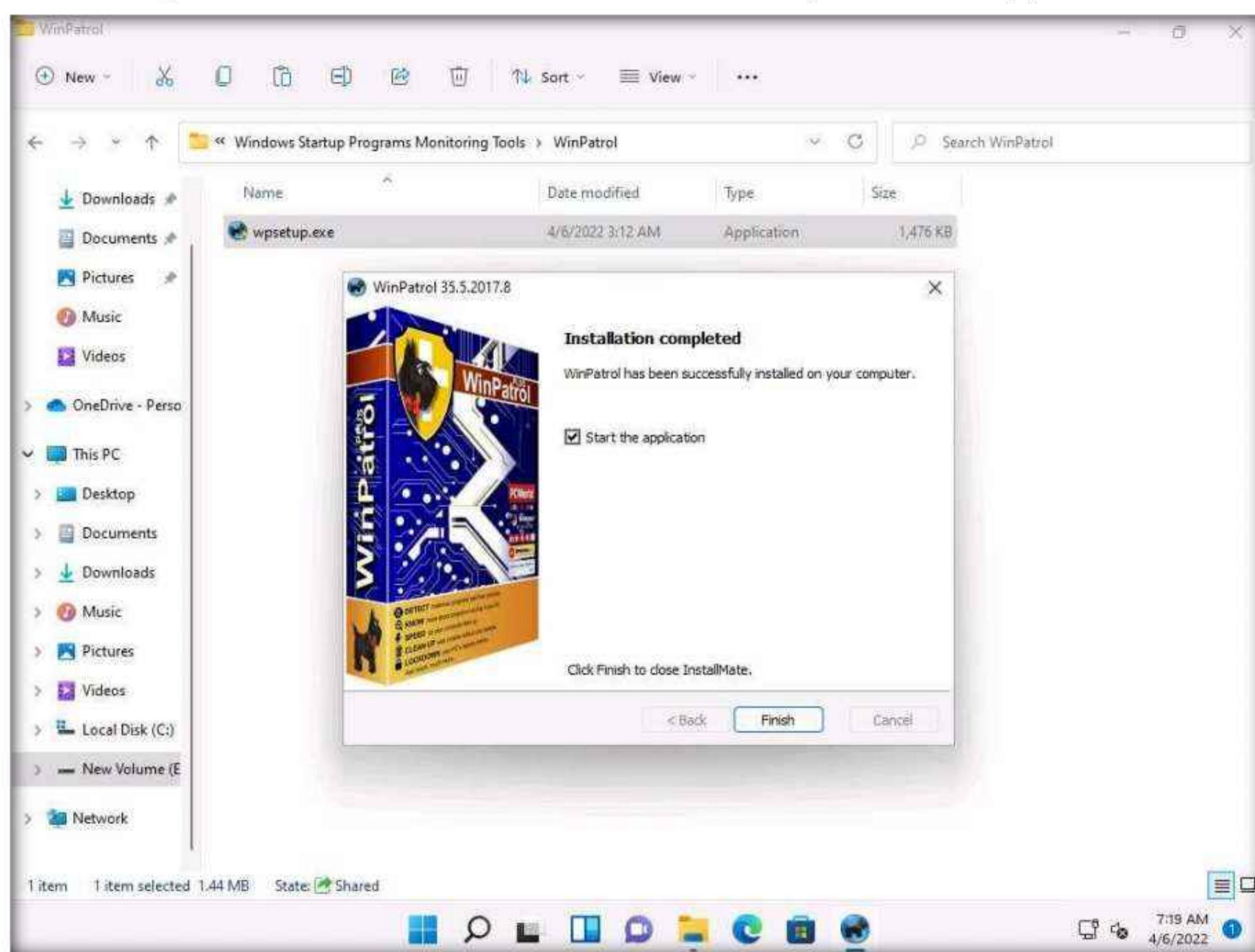
8. You can click on any driver to display its size, version, and the time at which it was automatically run at system startup (for the first time).

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.



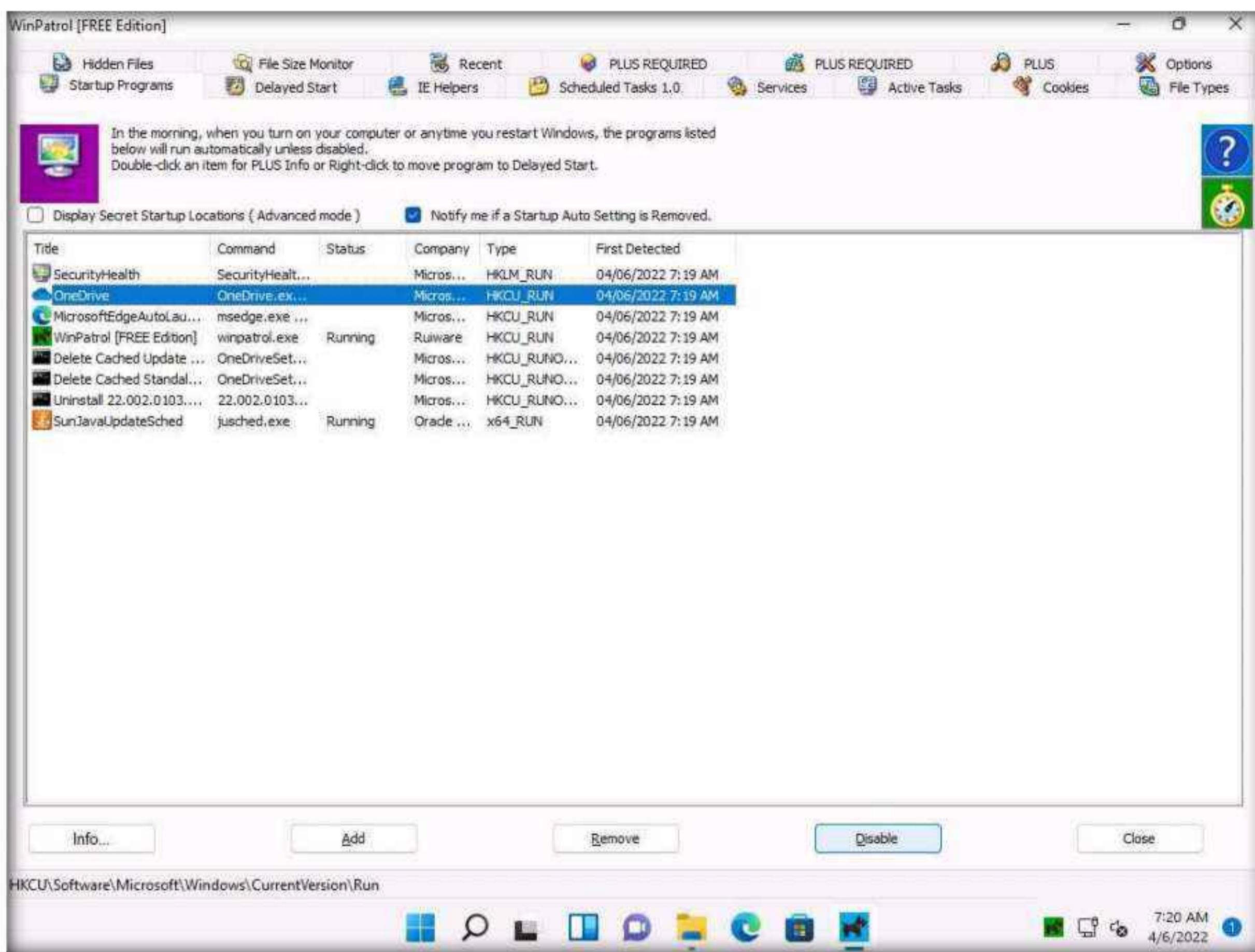
10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.
12. Now, we will find out which applications or processes start when the system boots up using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

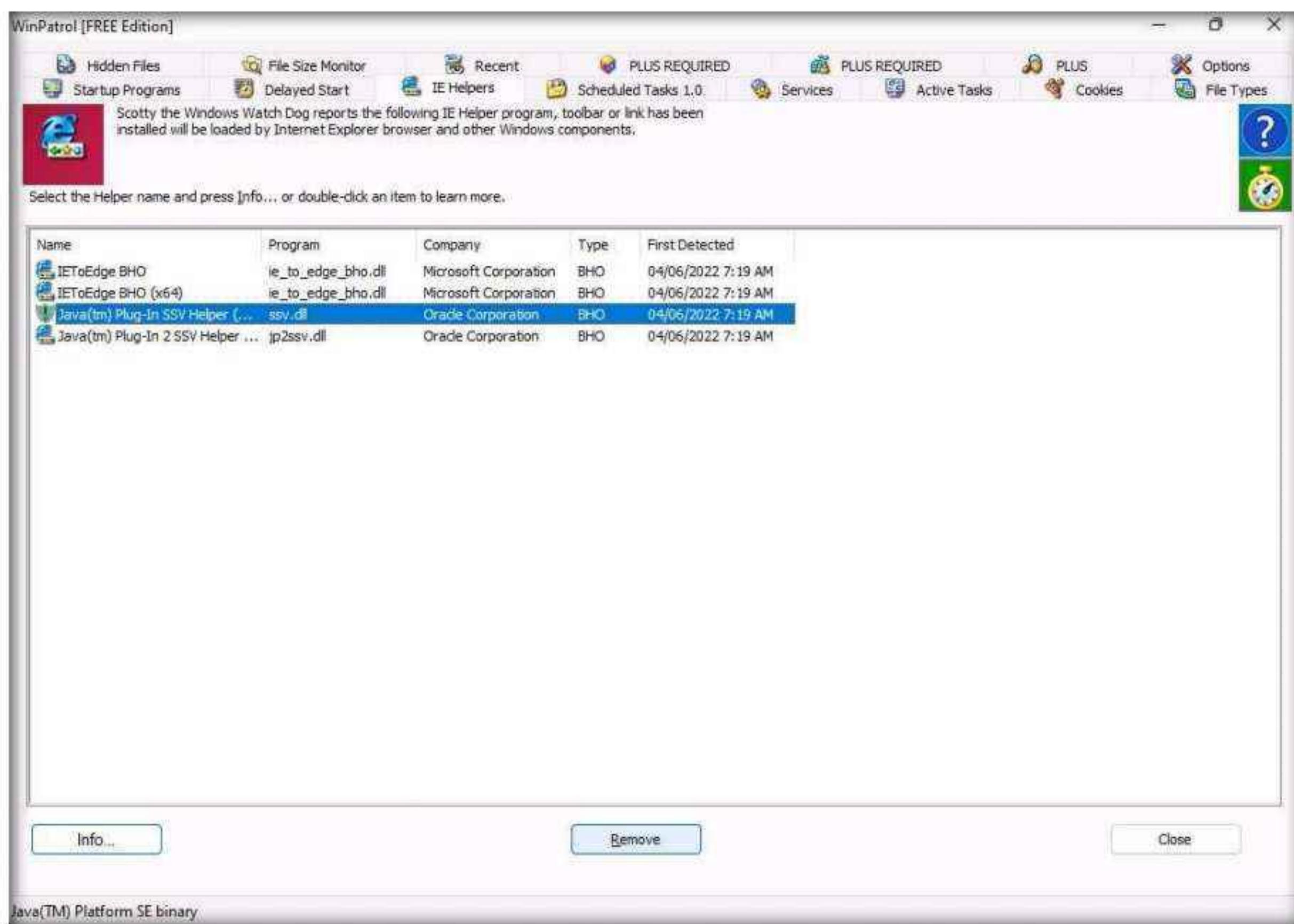
Module 07 – Malware Threats



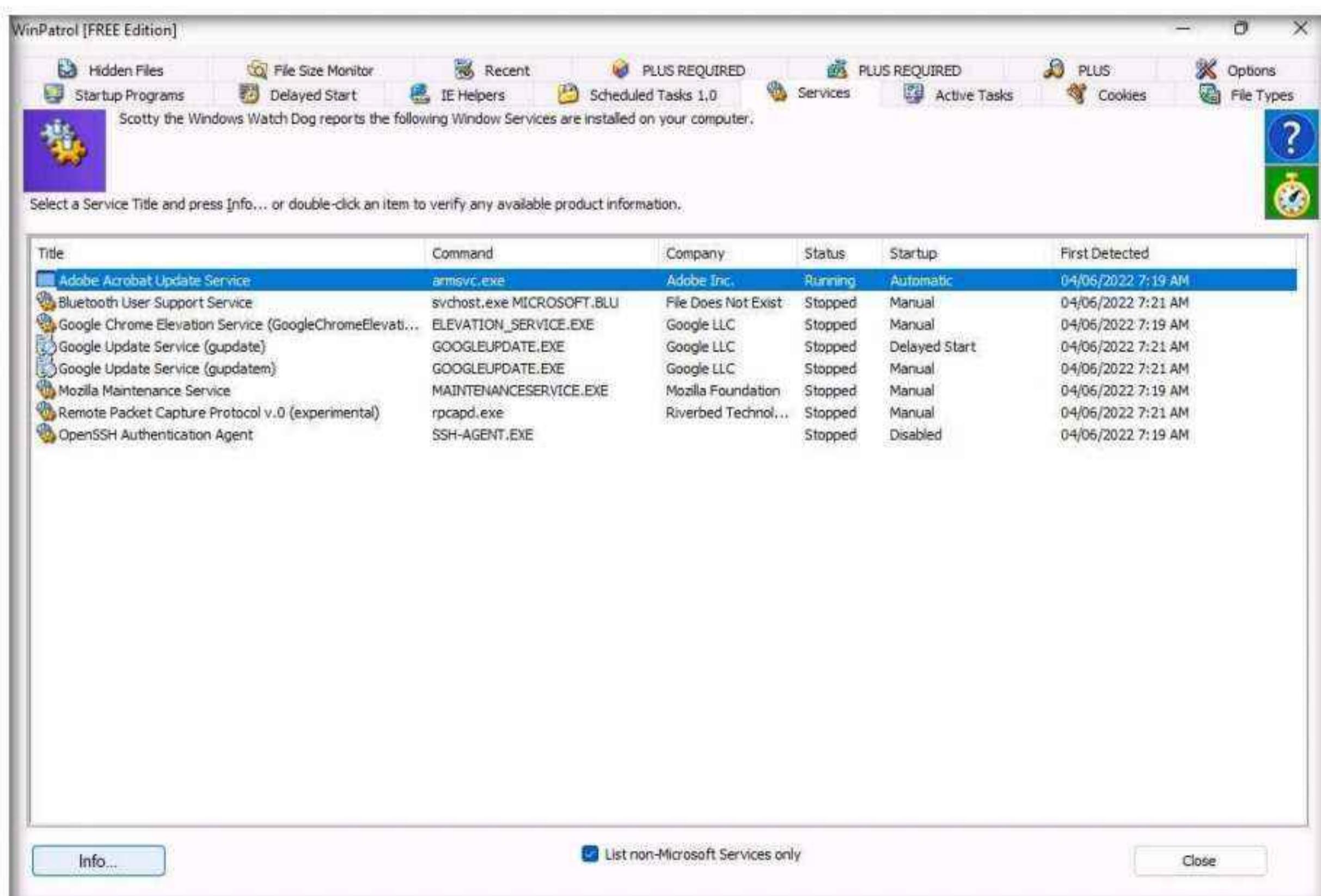
19. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.
 20. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here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

Module 07 – Malware Threats

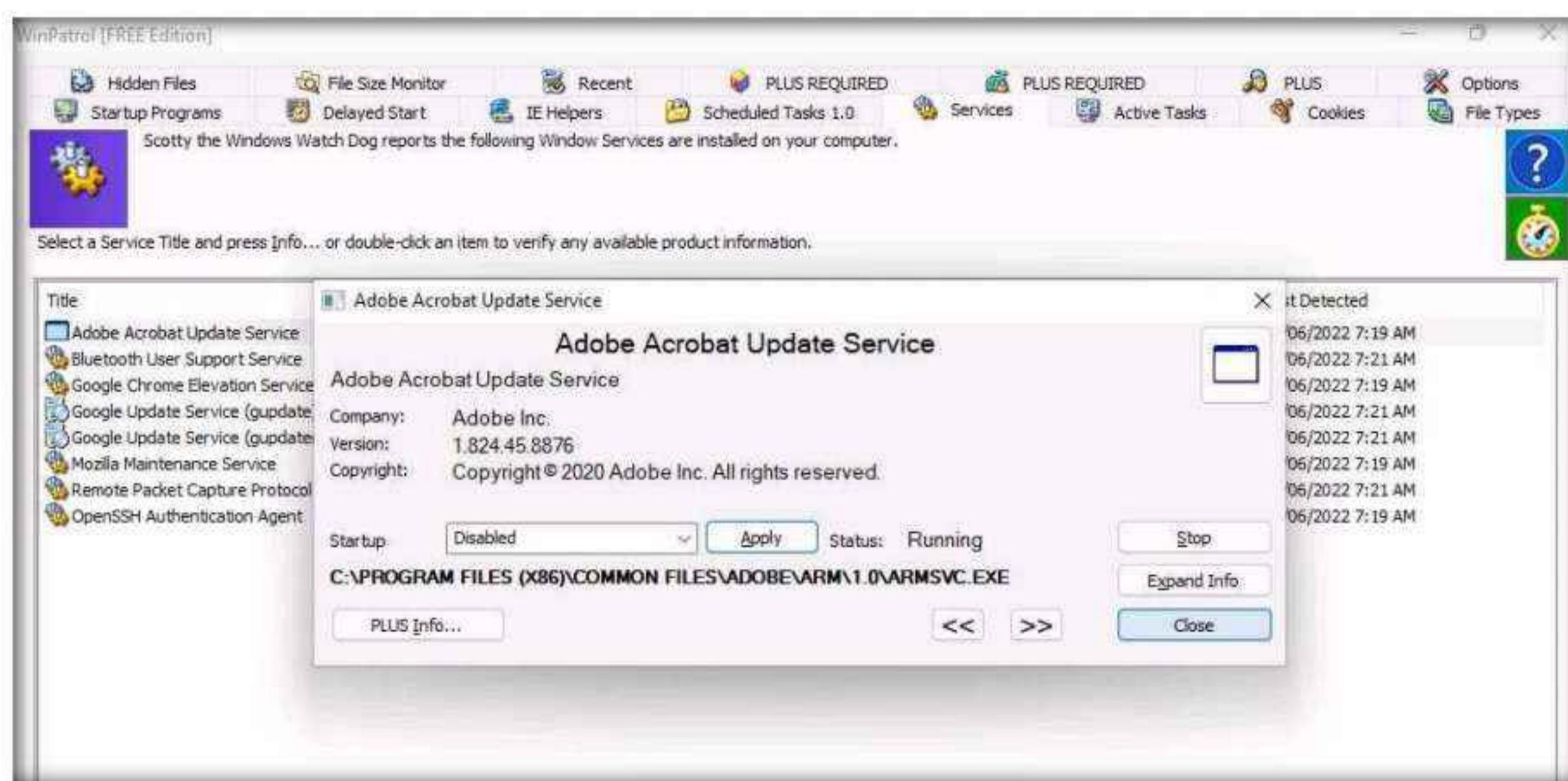


21. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info...**, as shown in the screenshot.

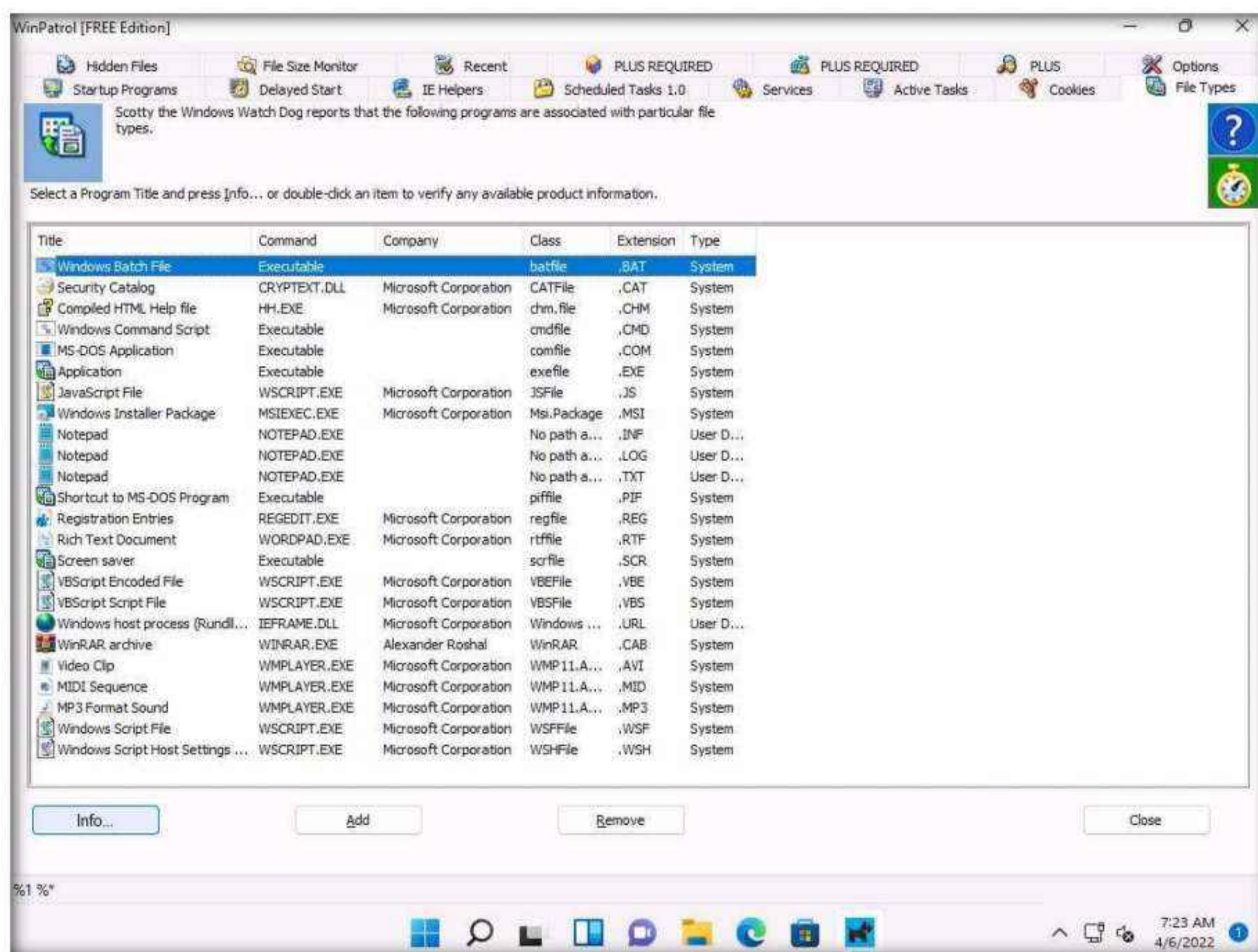


Module 07 – Malware Threats

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.

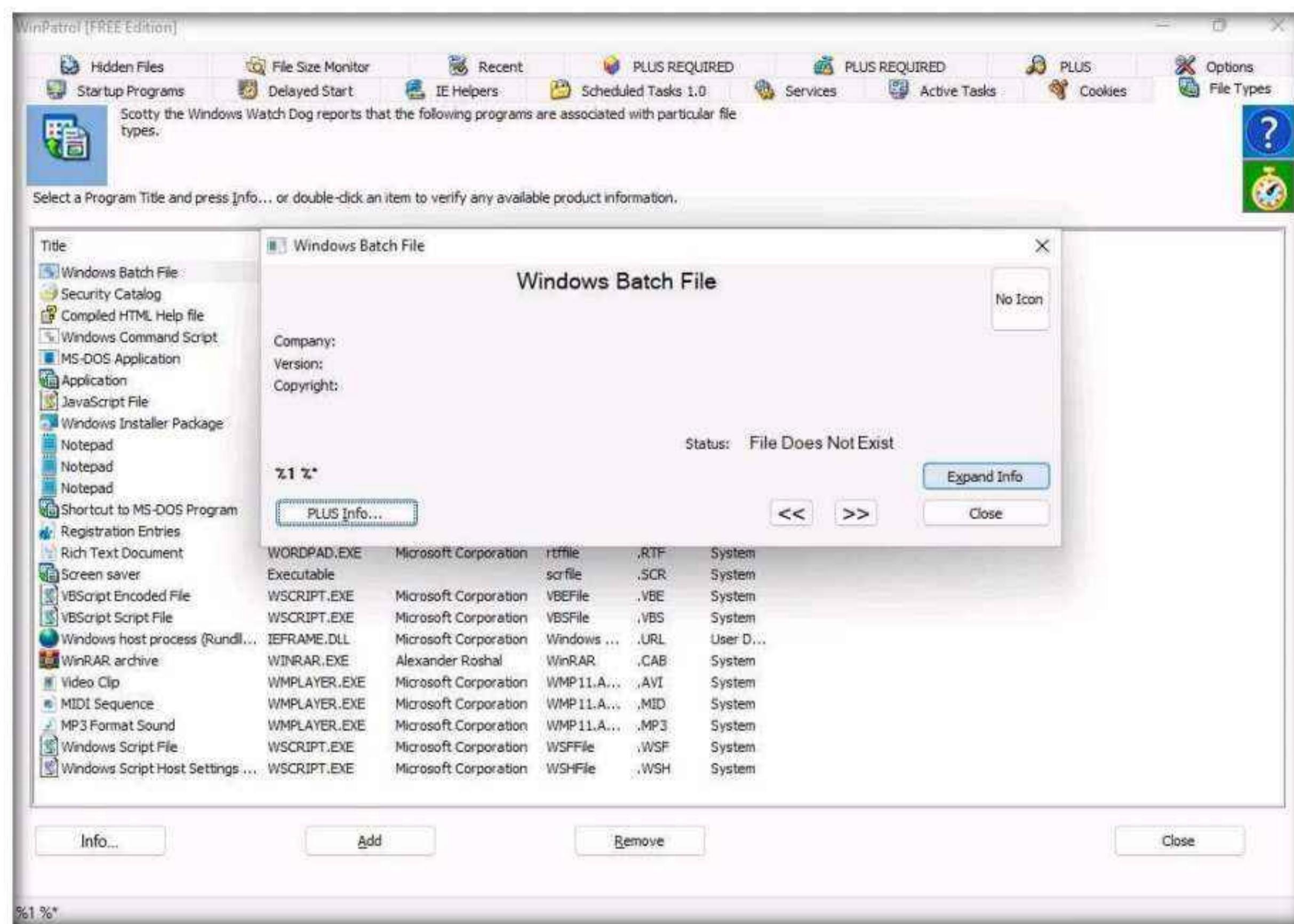


23. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info...** to view the available information.

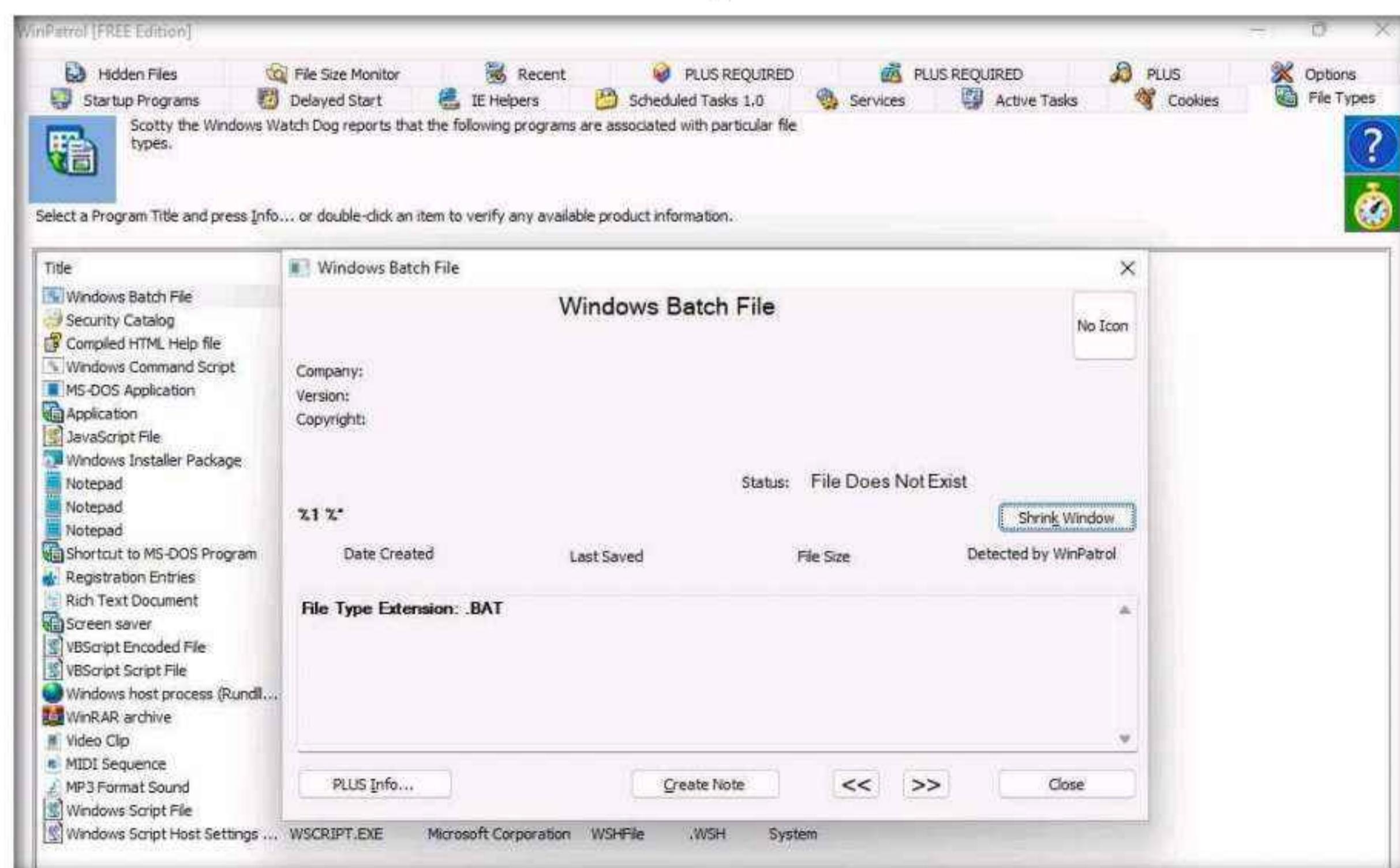


Module 07 – Malware Threats

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

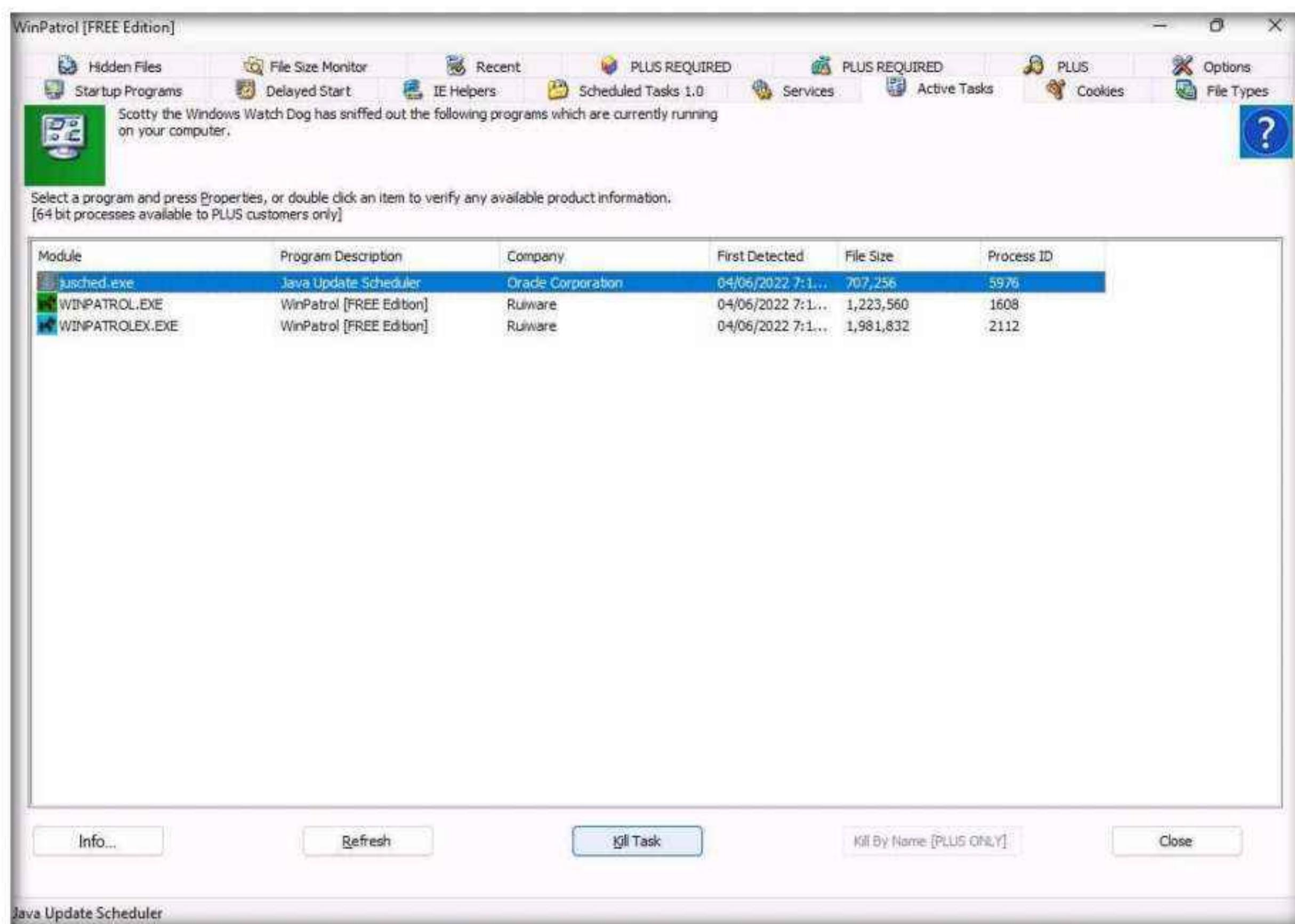


25. The expanded view shows all information related to the program and its associated file, as demonstrated in the screenshot. Analyze the info and close the window.



Module 07 – Malware Threats

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.

Module 07 – Malware Threats

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.

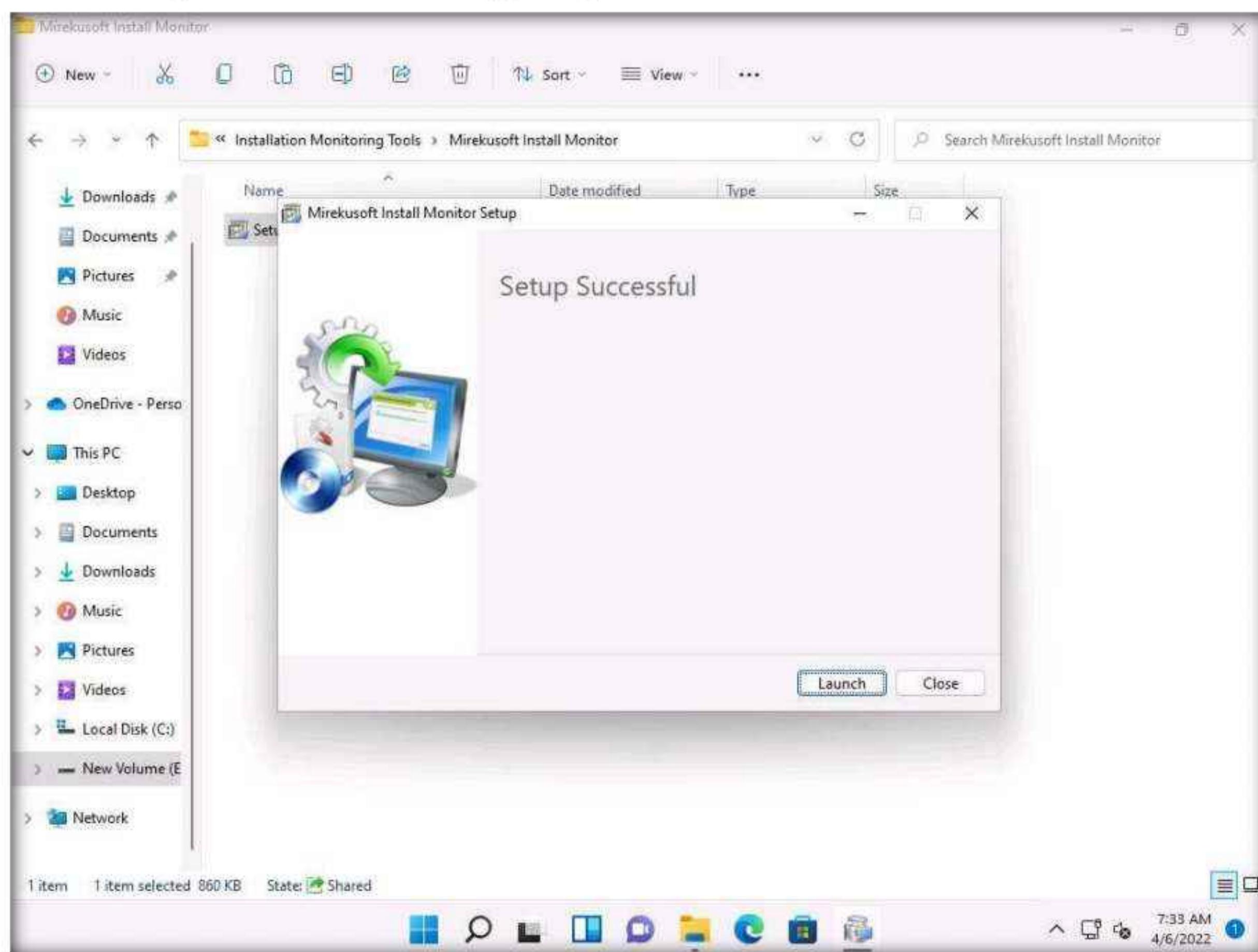
Here, we will use the Mirekusoft Install Monitor tool to detect hidden and background installations.

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.

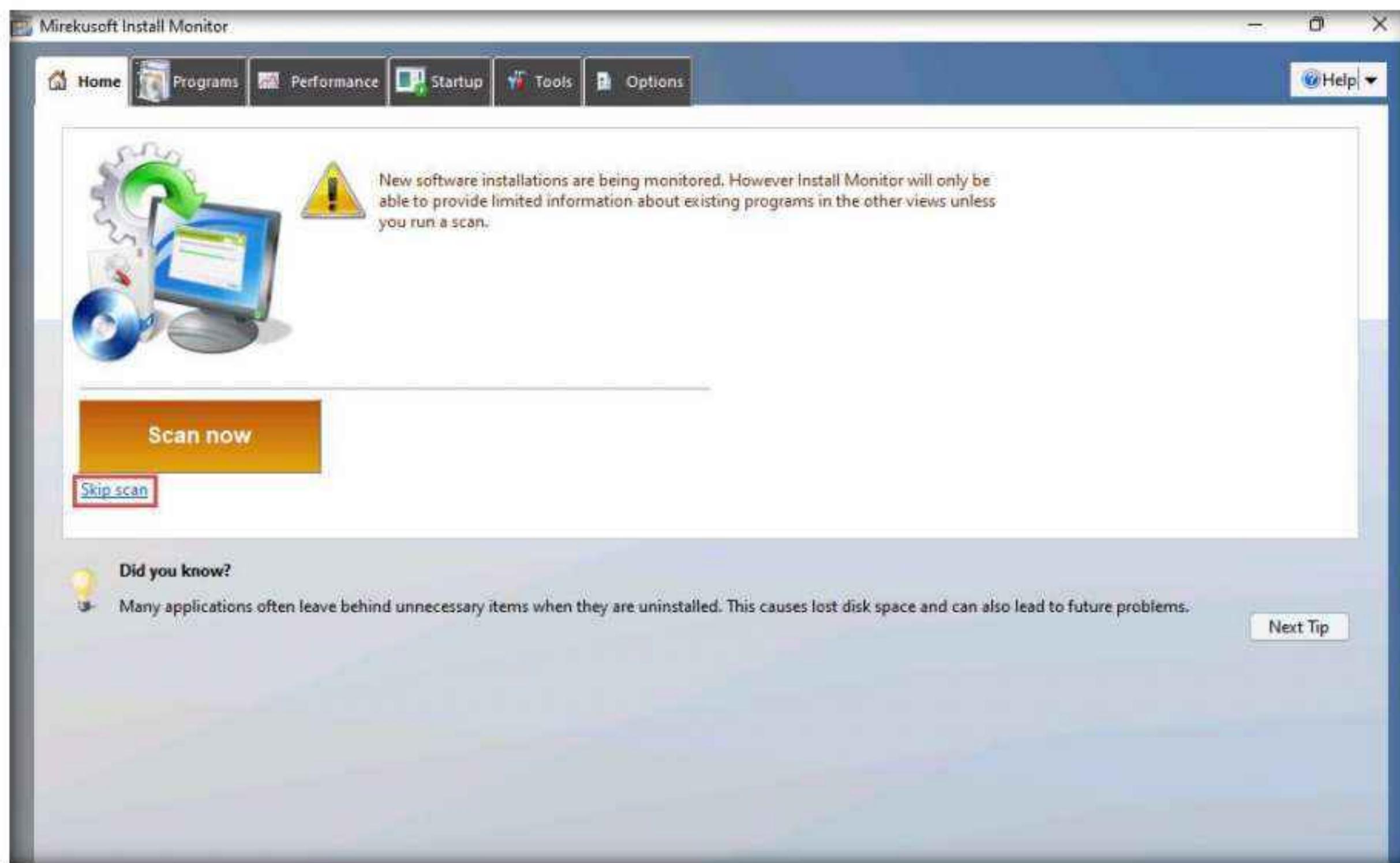
Note: If a **User Account Control** window appears, click **Yes**.

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



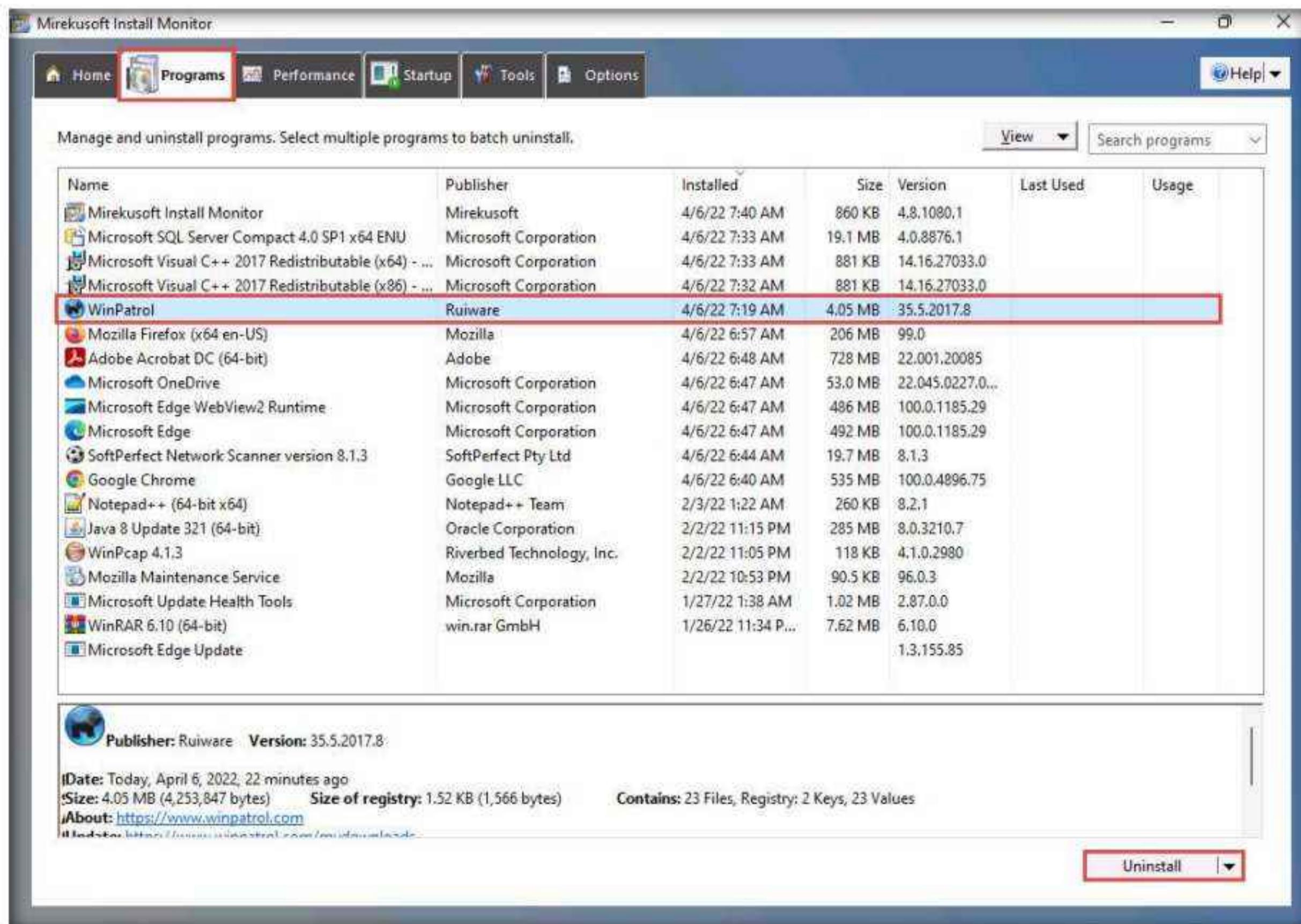
4. If a **User Account Control** window appears, click **Yes**.
5. The **Mirekusoft Install Monitor** main window appears, along with a **Welcome** pop-up, click **OK**. Click **Skip scan** in the **Home** tab.

Module 07 – Malware Threats



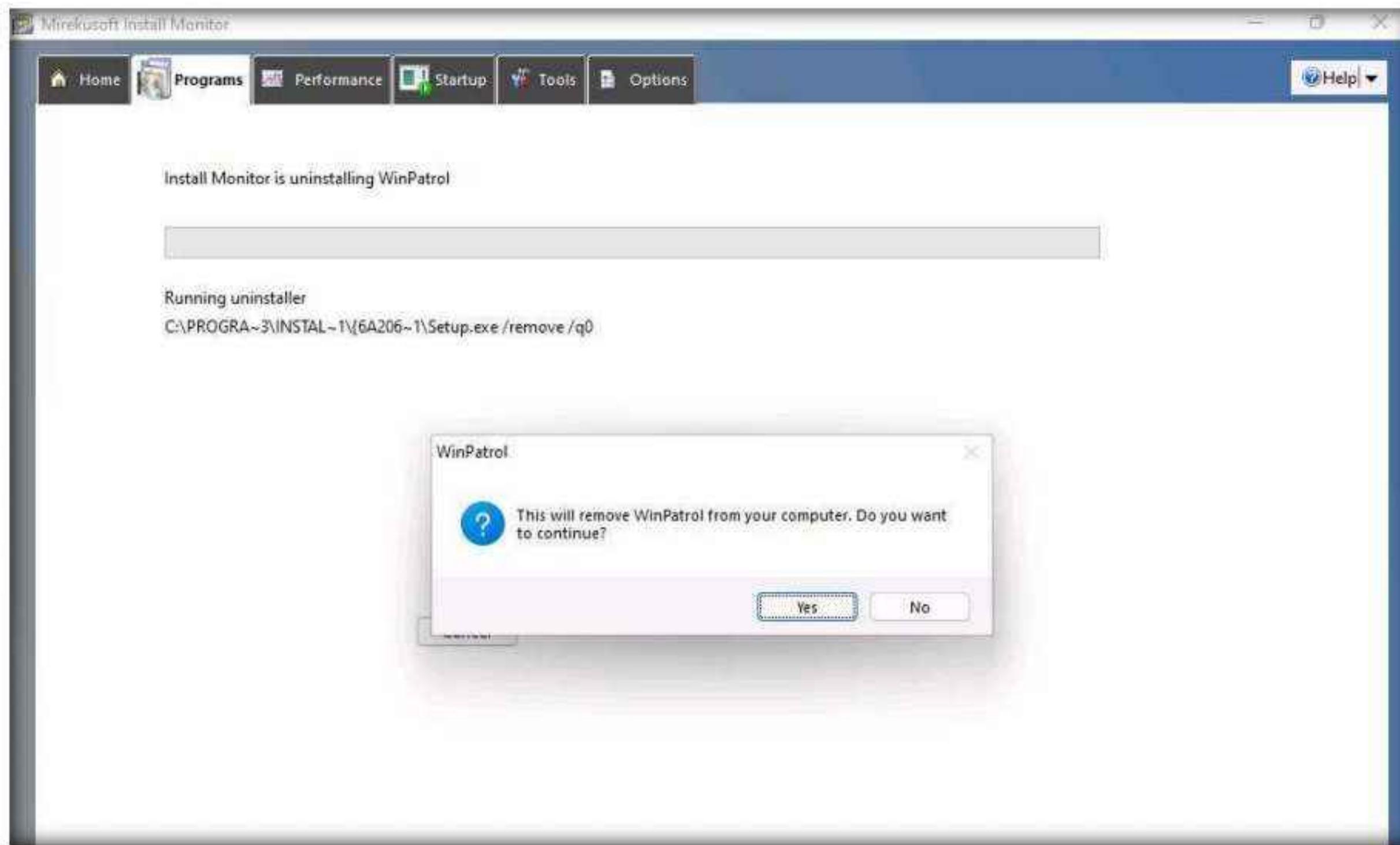
6. Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

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

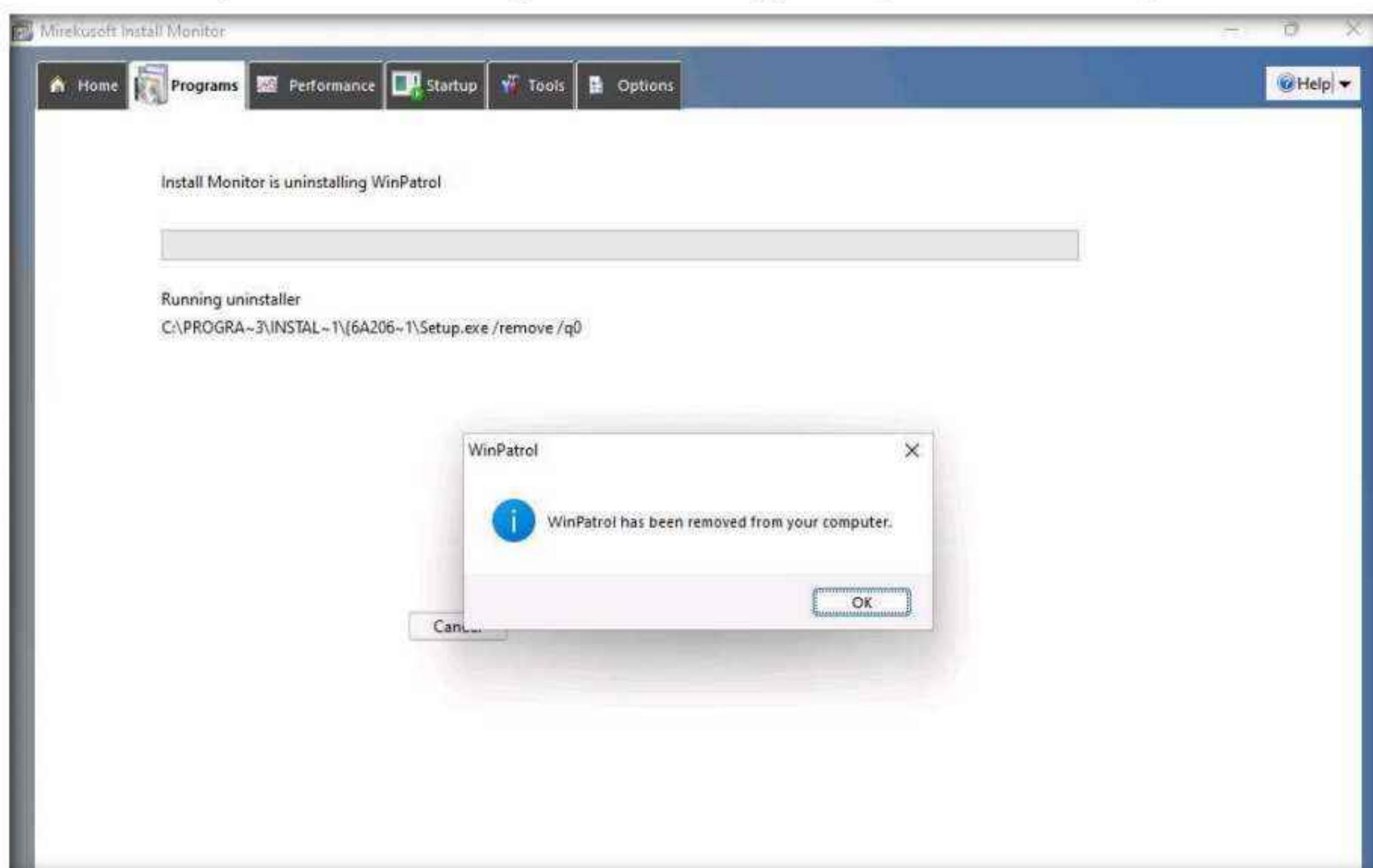


Module 07 – Malware Threats

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

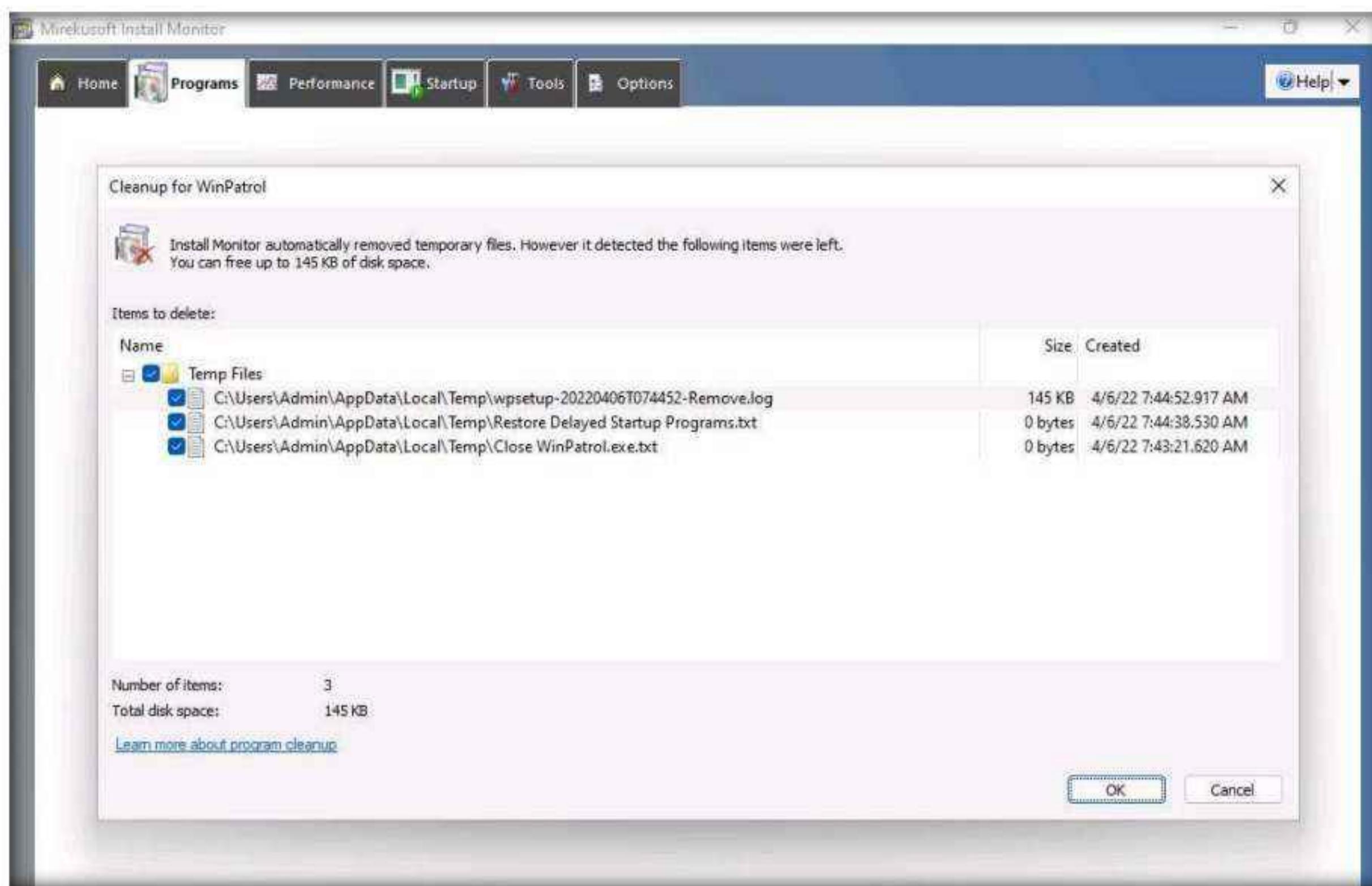


8. The **selected application is uninstalled from your computer** pop-up appears; click **OK**.
9. In the next **WinPatrol** pop-up, click **Yes**.
10. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.

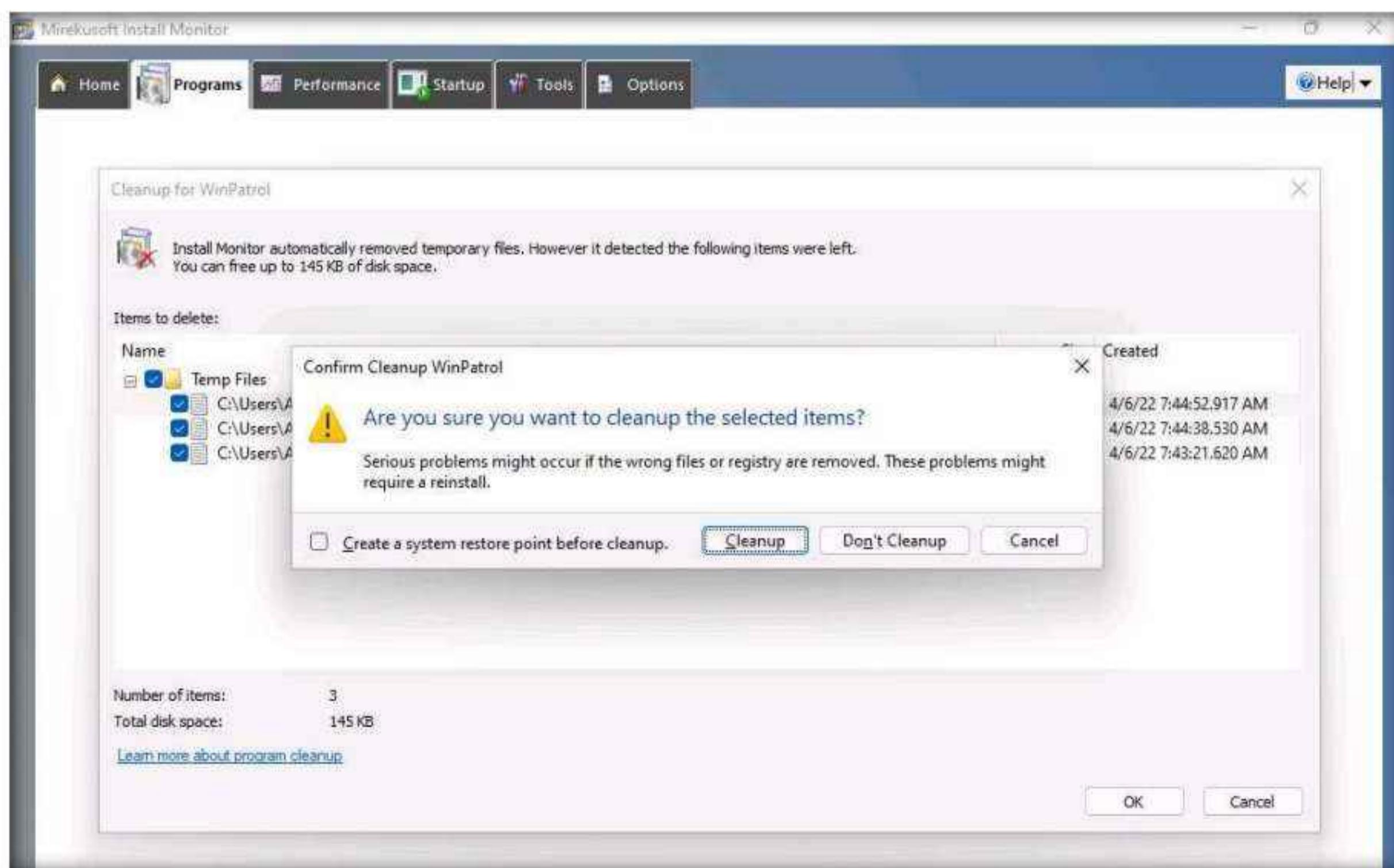


Module 07 – Malware Threats

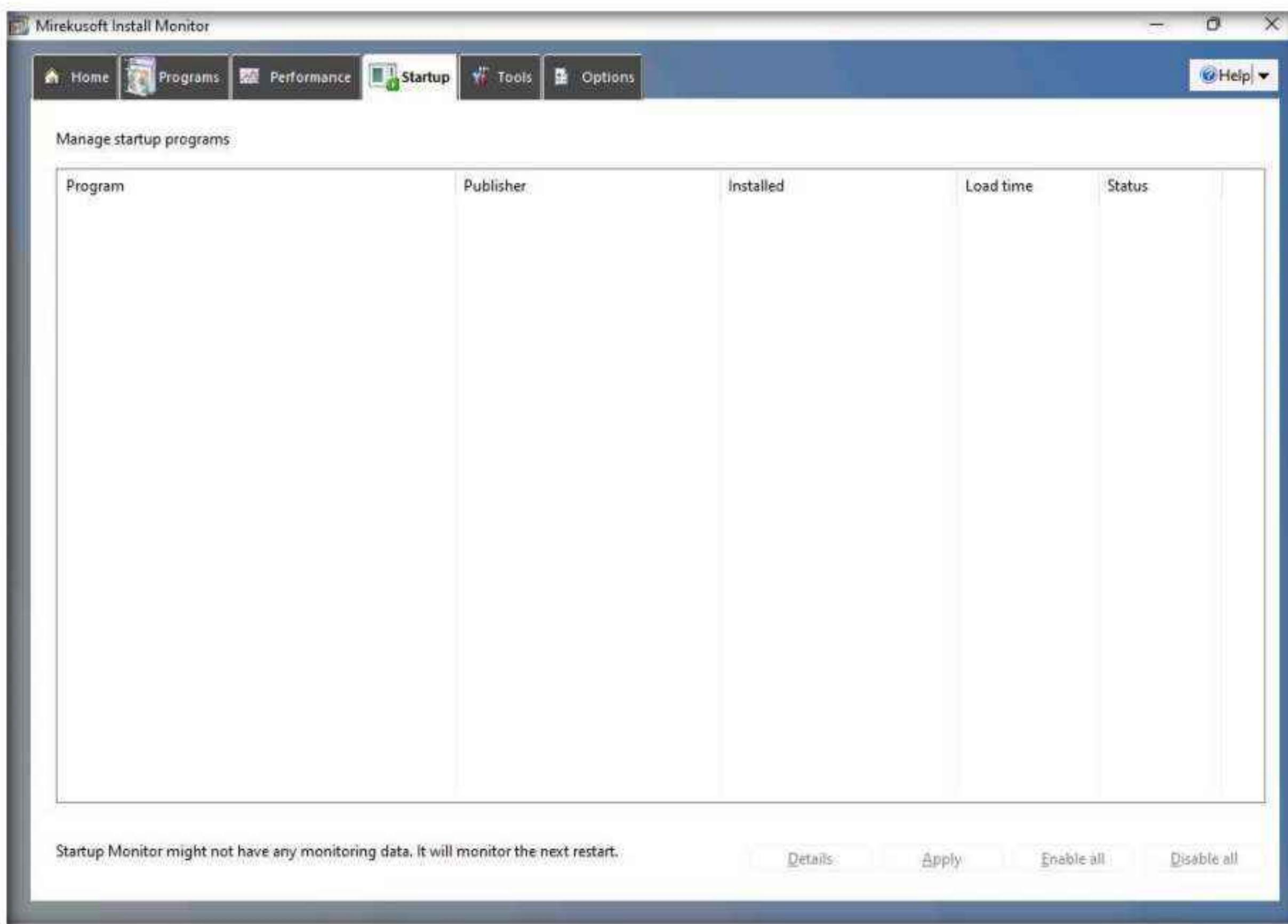
11. A Cleanup for WinPatrol window appears, click OK.



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:

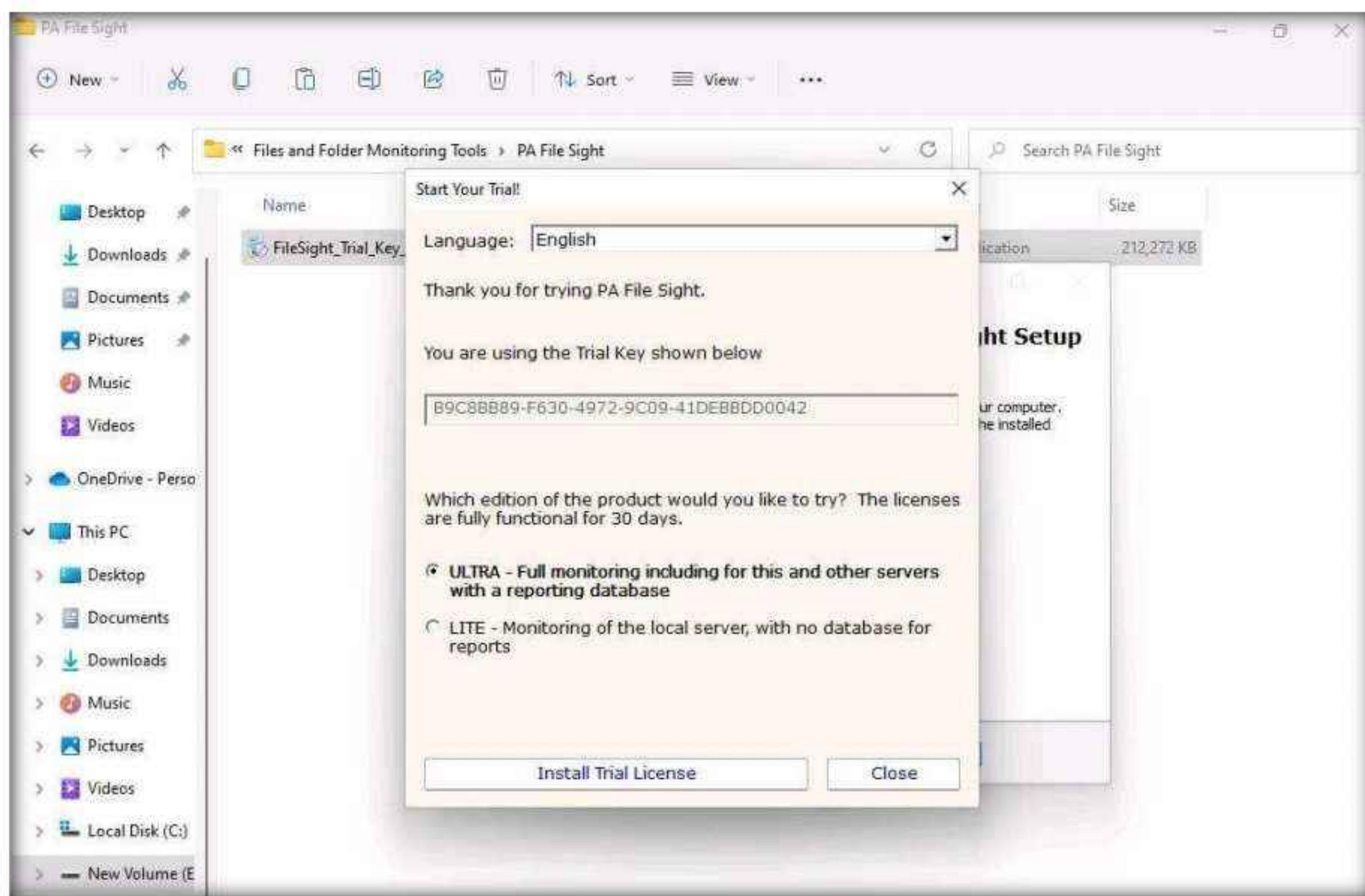
- Compromised computers are blocked from reaching files on other protected servers on the network
- Detects users copying files and optionally blocks access
- Real-time alerts allow the appropriate staff to investigate immediately
- Audits who is deleting, moving, and reading files

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**.

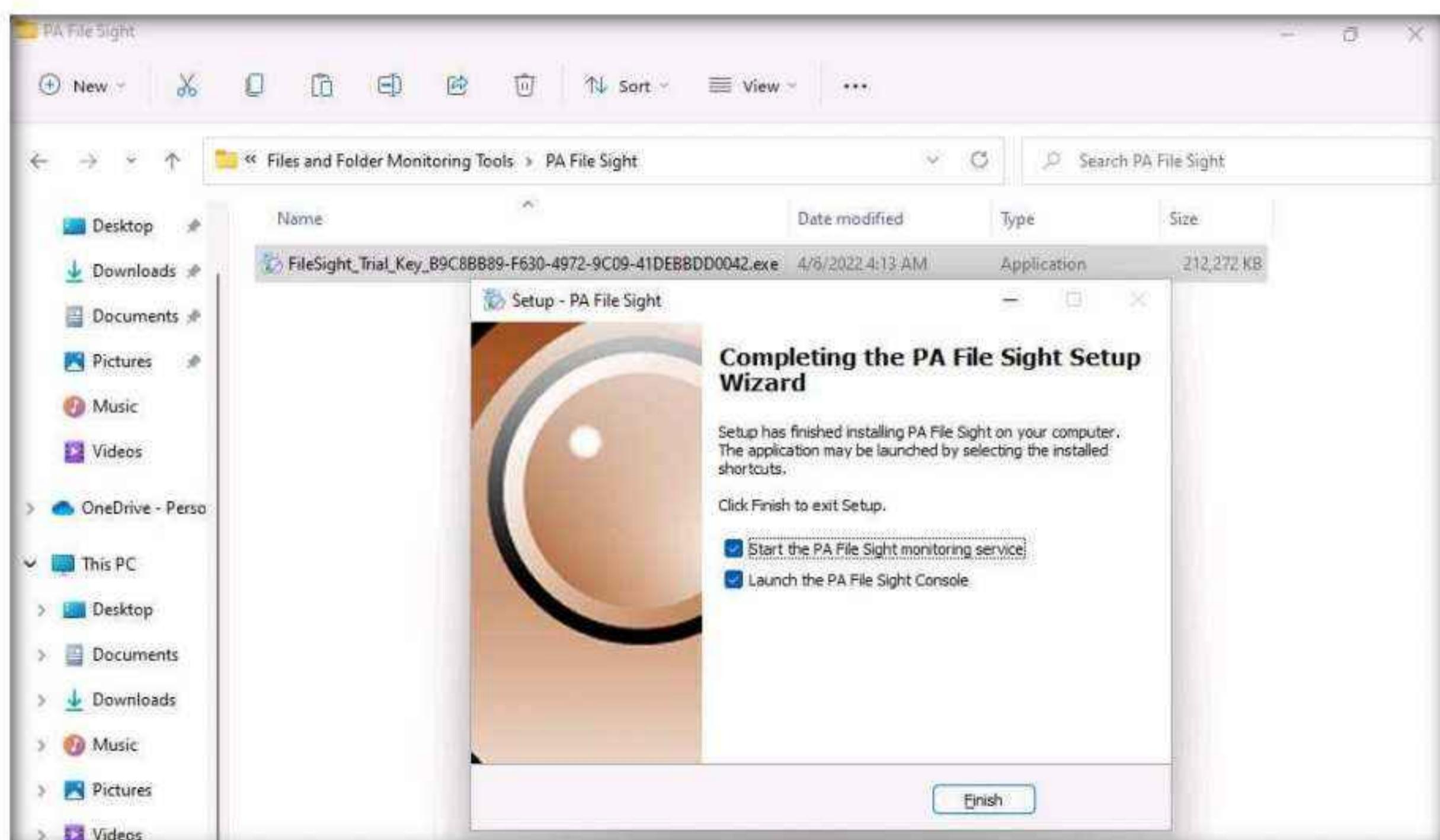
Note: If a **Open File - Security Warning** window appears, click **Run**. If a **User Account Control** window appears, click **Yes**.

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**.

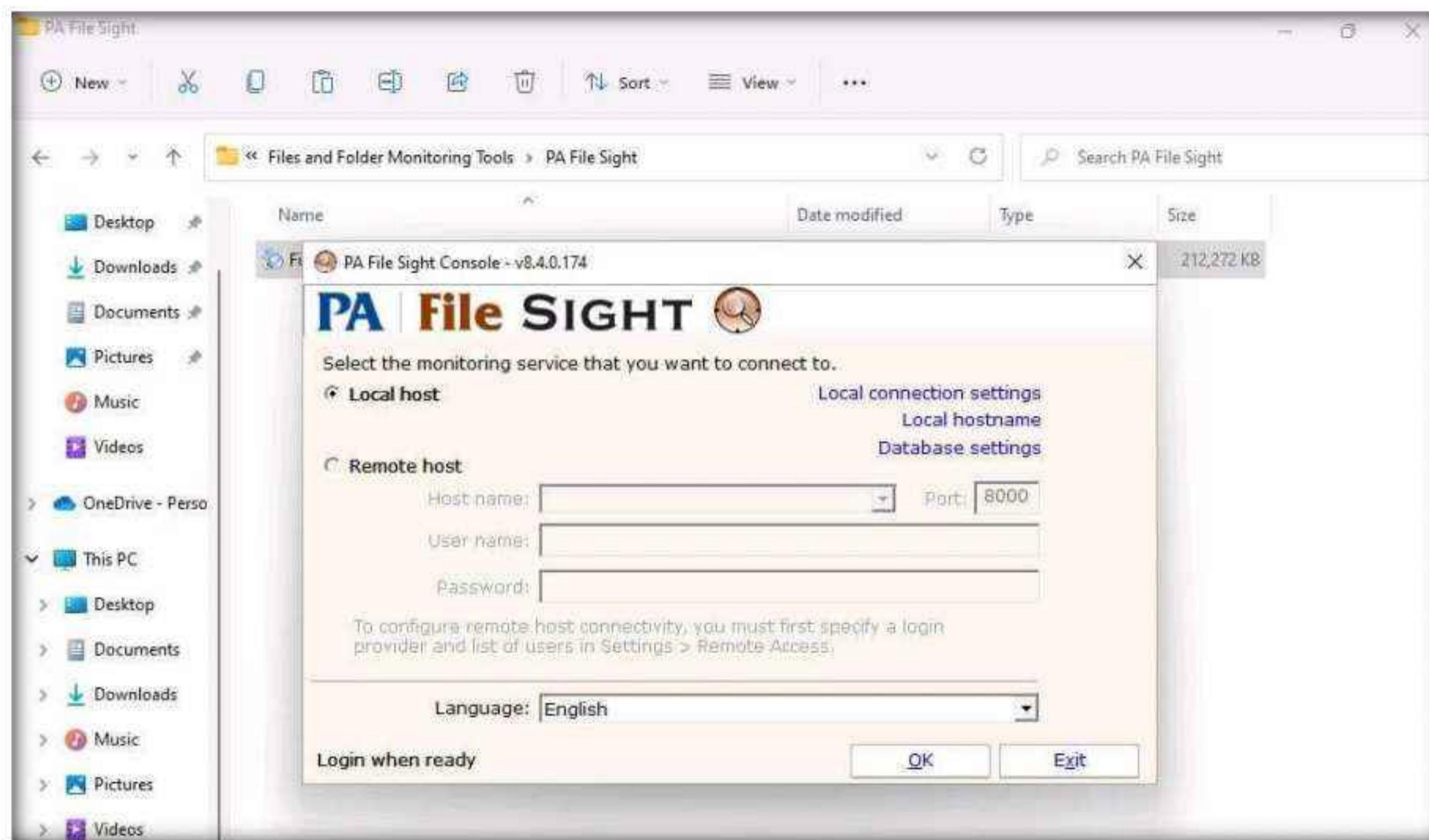


6. A Success window appears, click **OK**.
7. **Completing the PA File Sight Setup Wizard** appears; make sure that both the **Start the PA File Sight monitoring service** and the **Launch the PA File Sight Console** options are checked, and click **Finish**.
8. This will run the PA File Sight service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



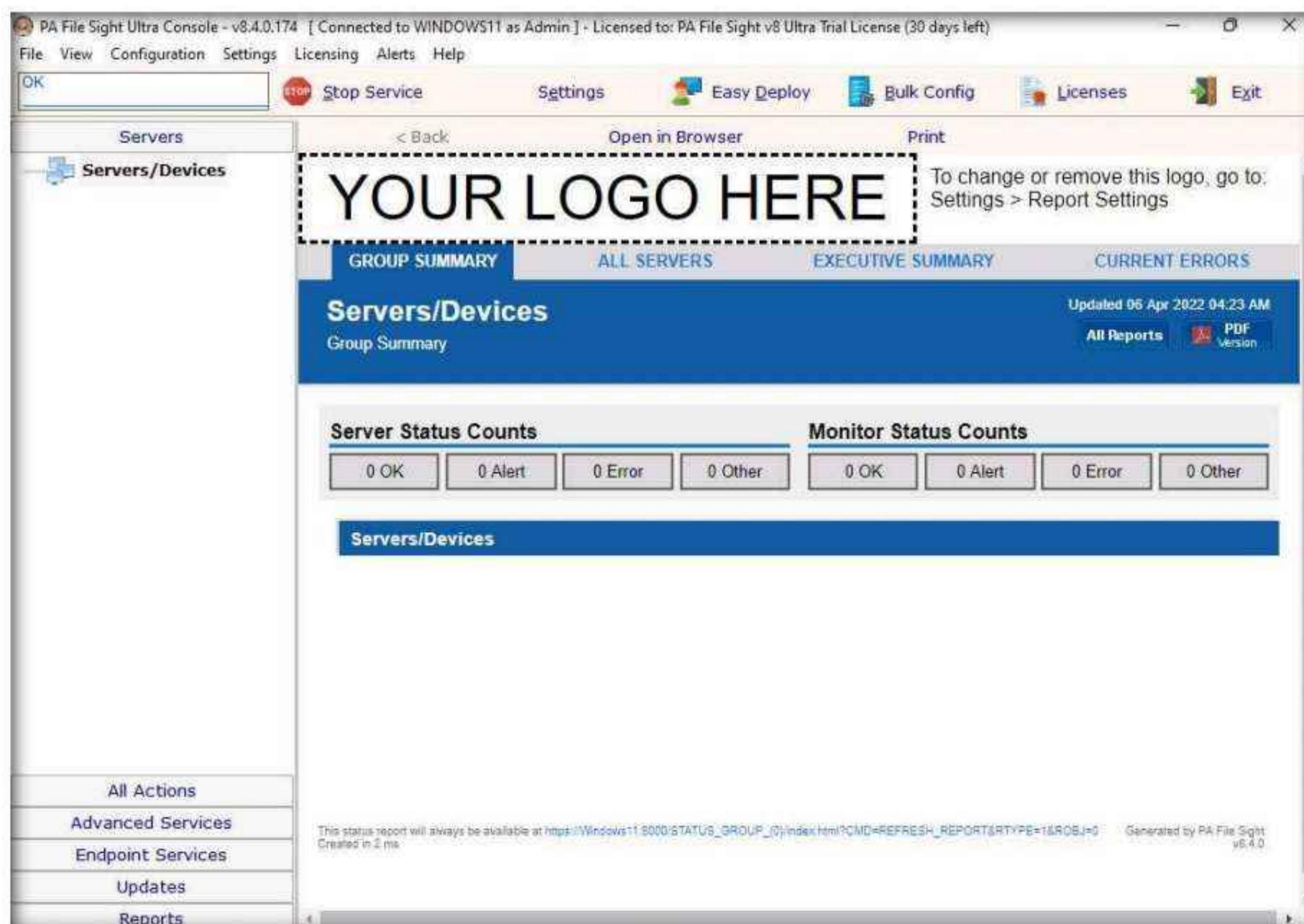
Module 07 – Malware Threats

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

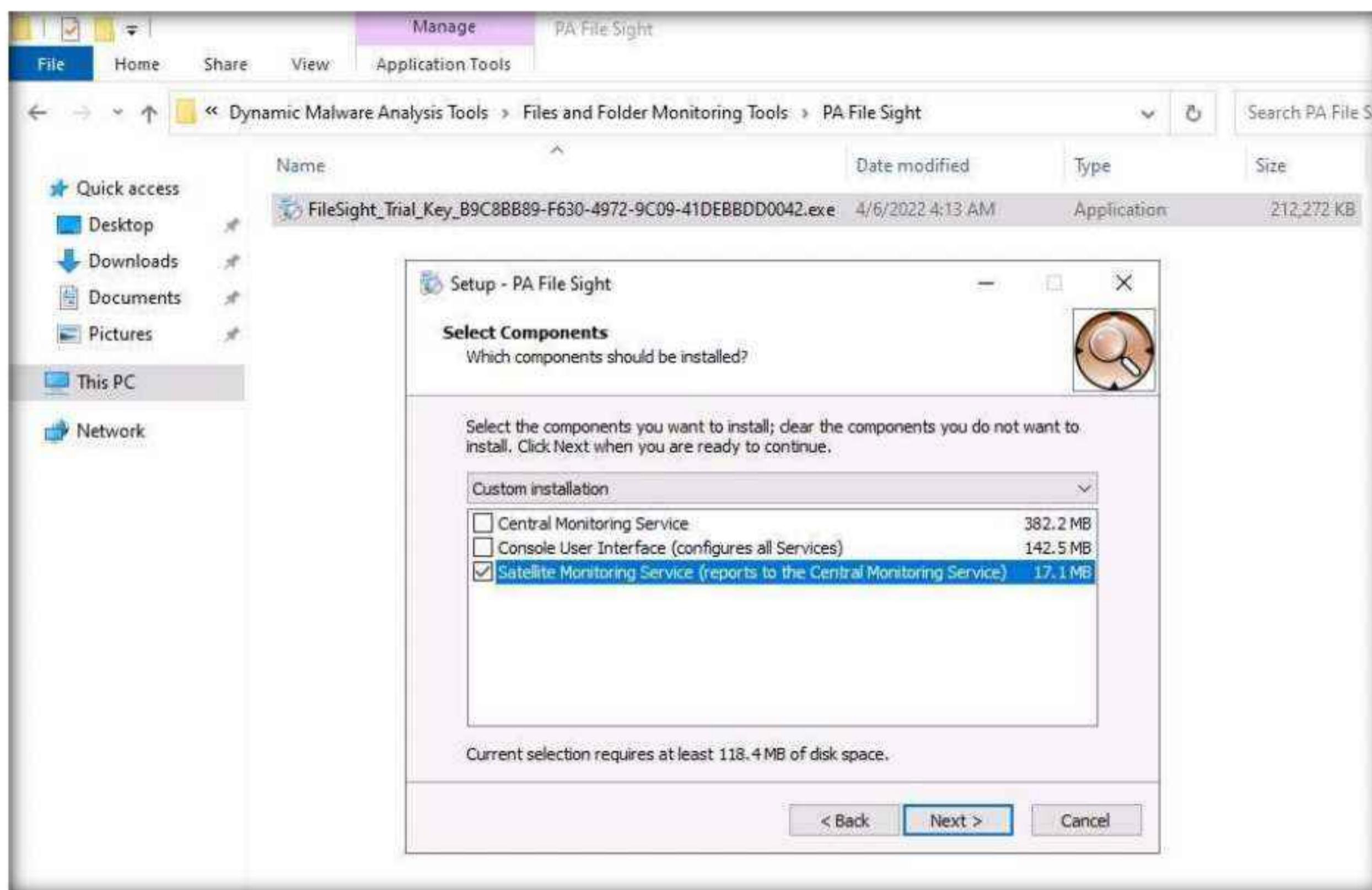


10. The **PA File Sight Ultra Console** main window appears.

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

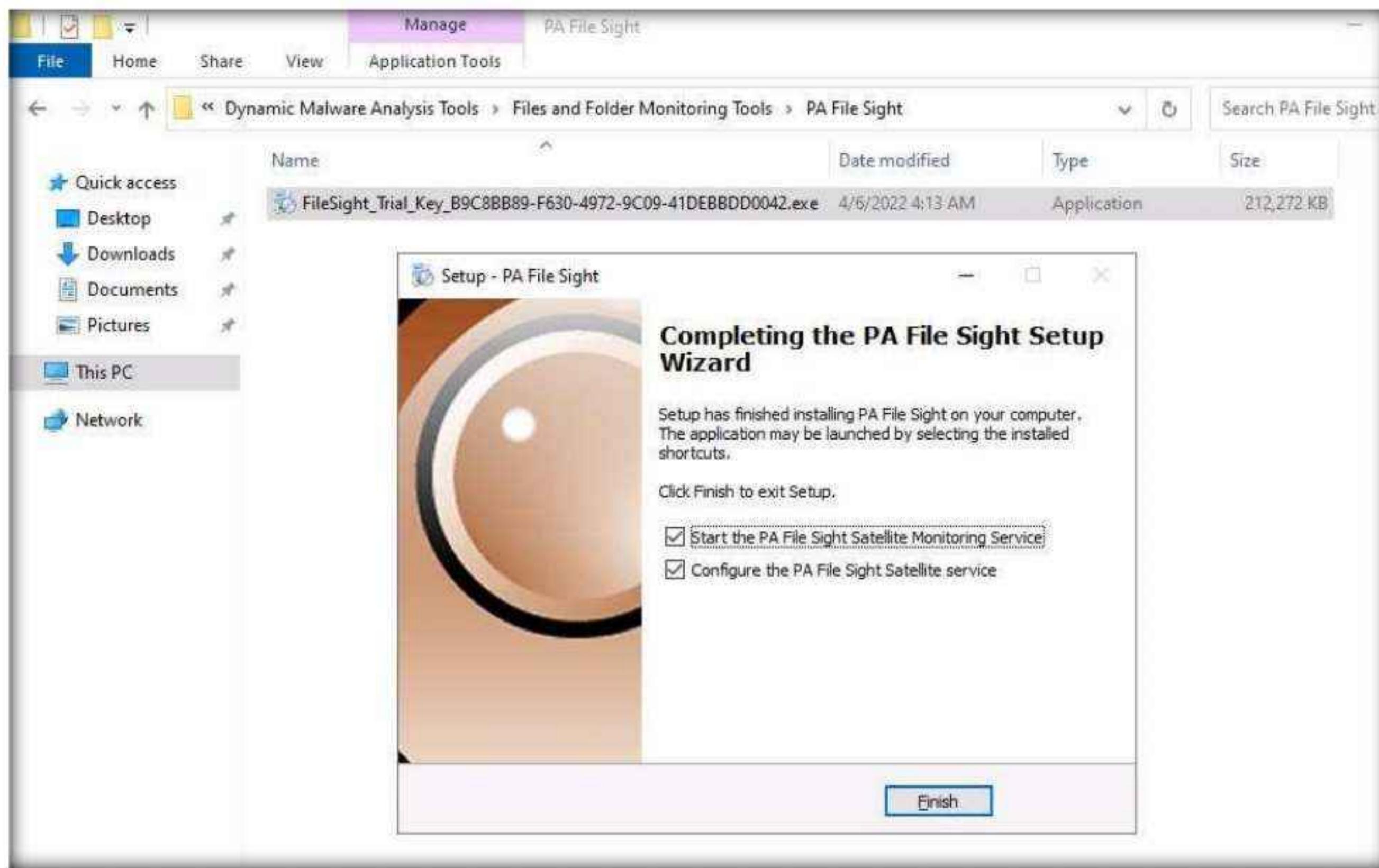


11. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
12. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic 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 (configures all Services)** options, and check the **Satellite Monitoring Service (reports to the Central Monitoring Service)** option; then, click **Next**.



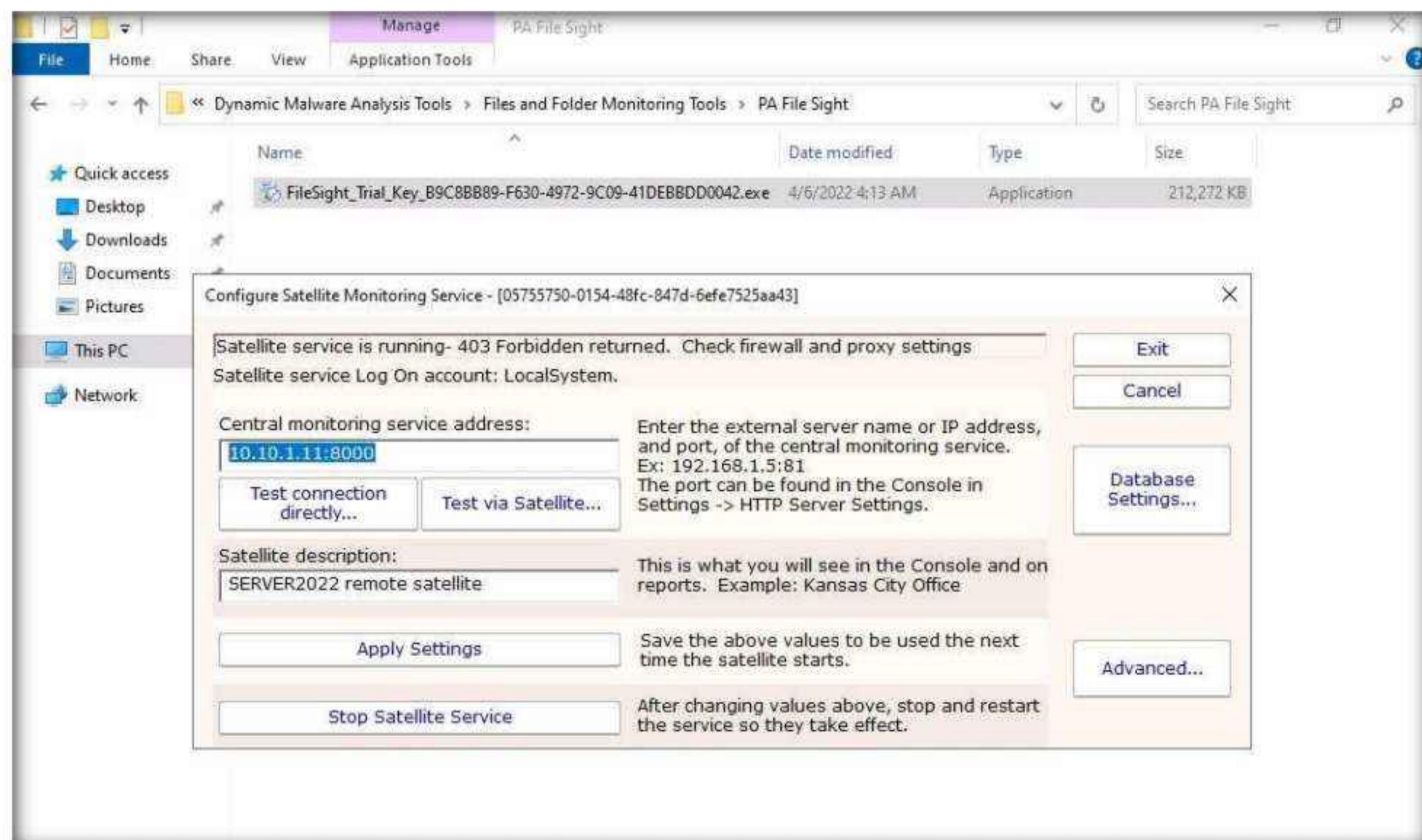
16. Follow the wizard-driven installation steps to install the application.
17. In the final step of the installation, make sure that the **Start the PA File Sight Satellite Monitoring Service** and **Configure the PA File Sight Satellite service** options are checked; then, click **Finish**.

Module 07 – Malware Threats



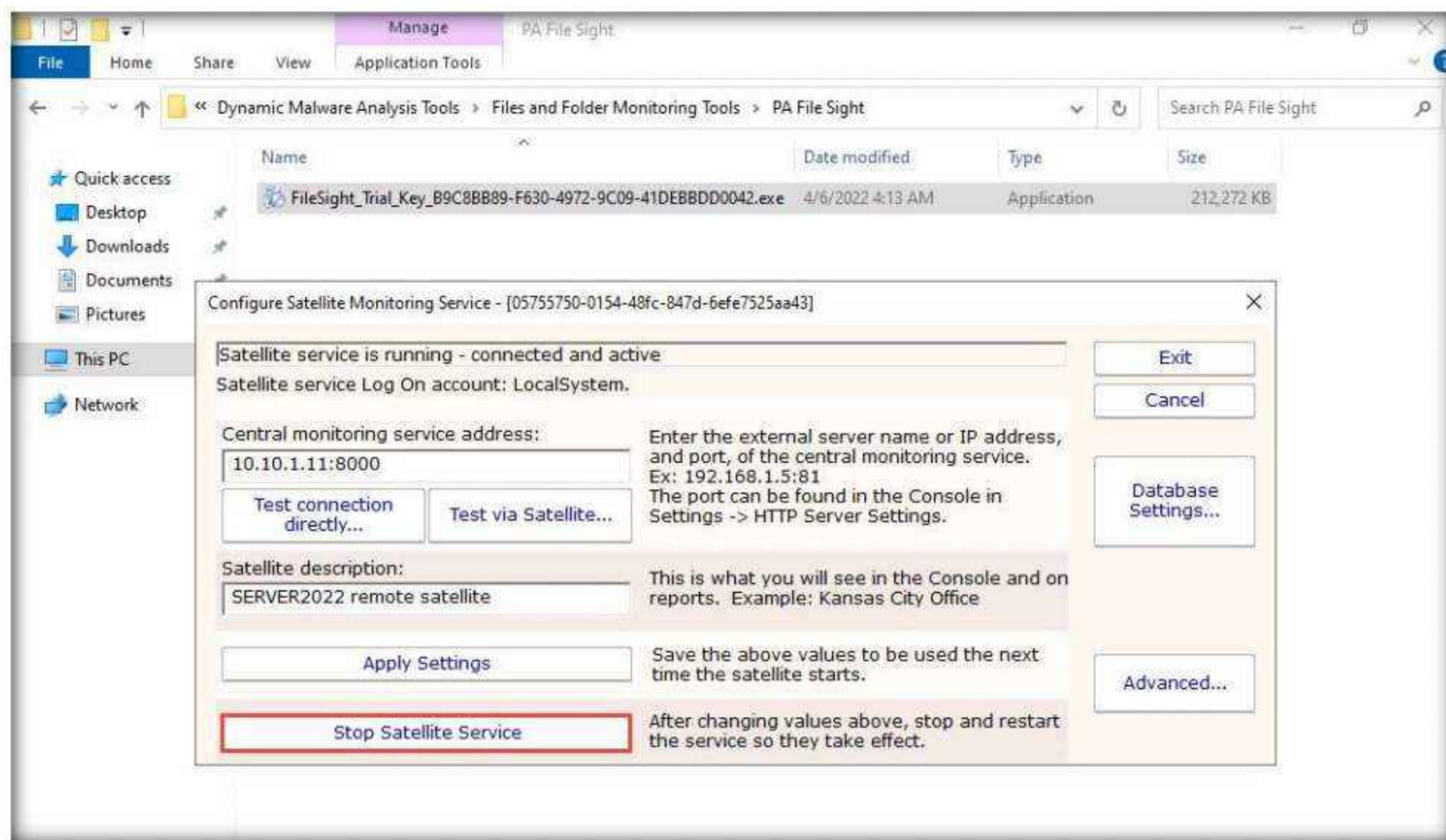
18. The **Configure Satellite Monitoring Service** window appears; type the **Windows 11 IP address** into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

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

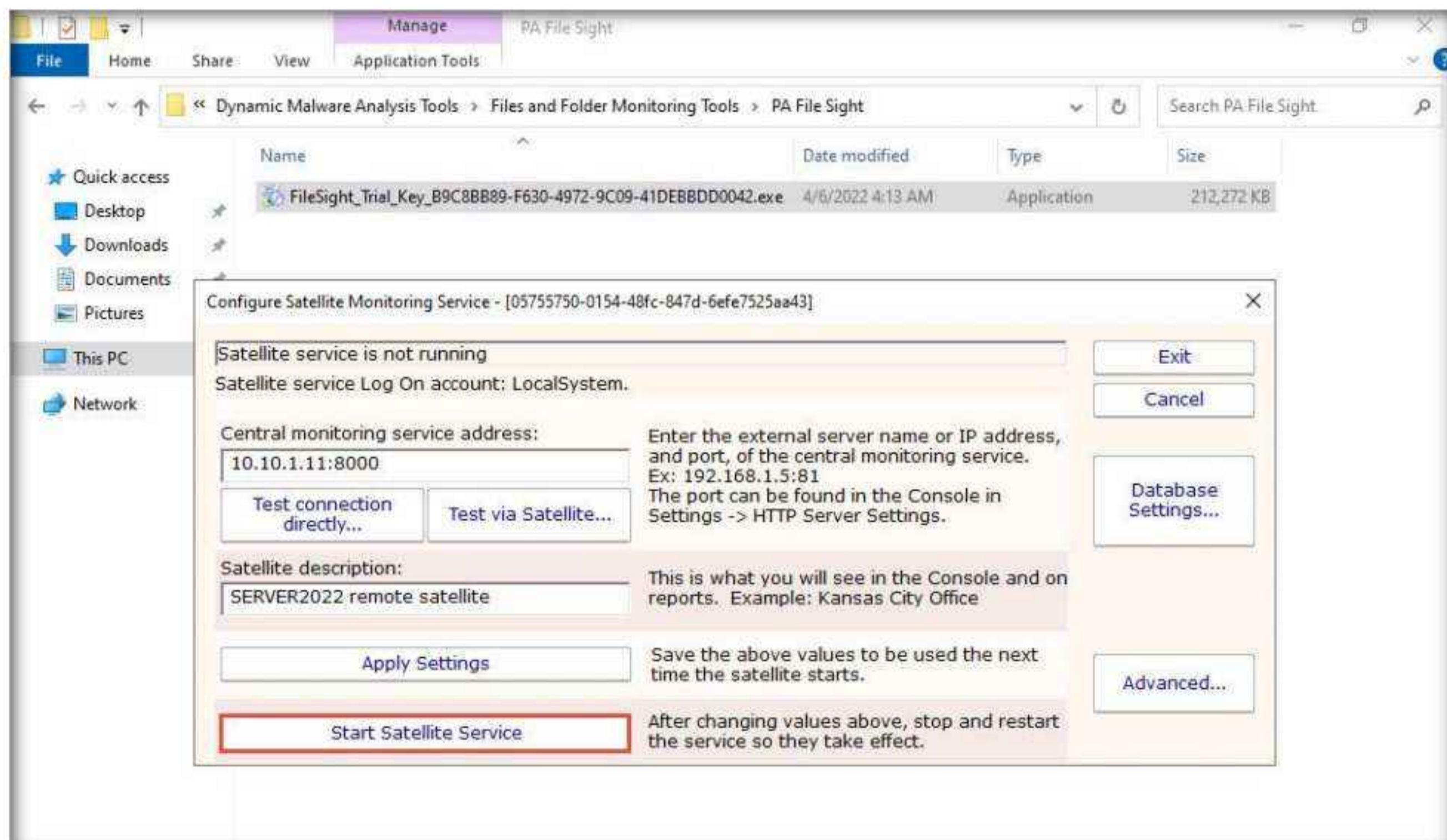


Module 07 – Malware Threats

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

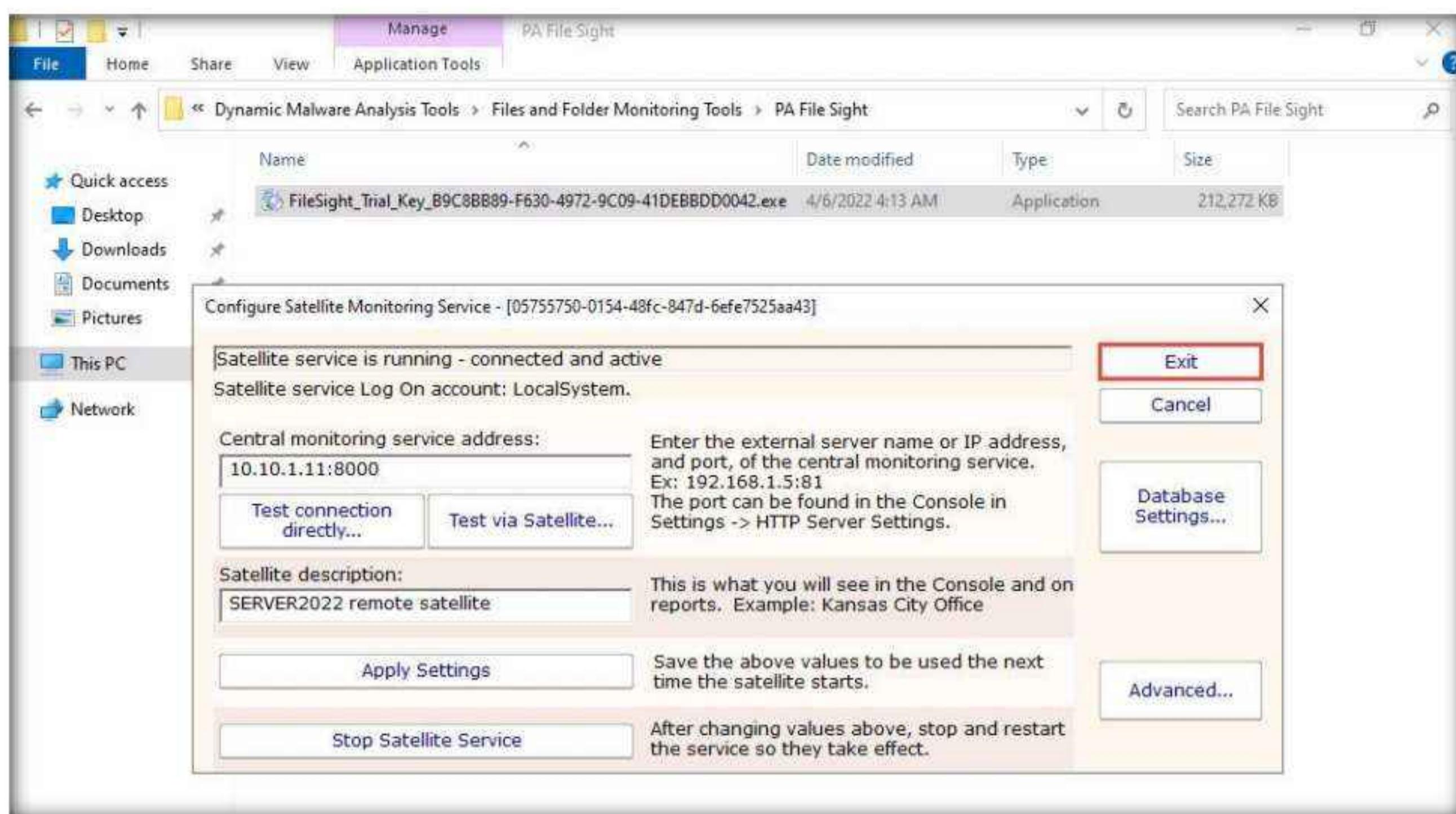


20. Once the service is stopped, click **Start Satellite Service**.

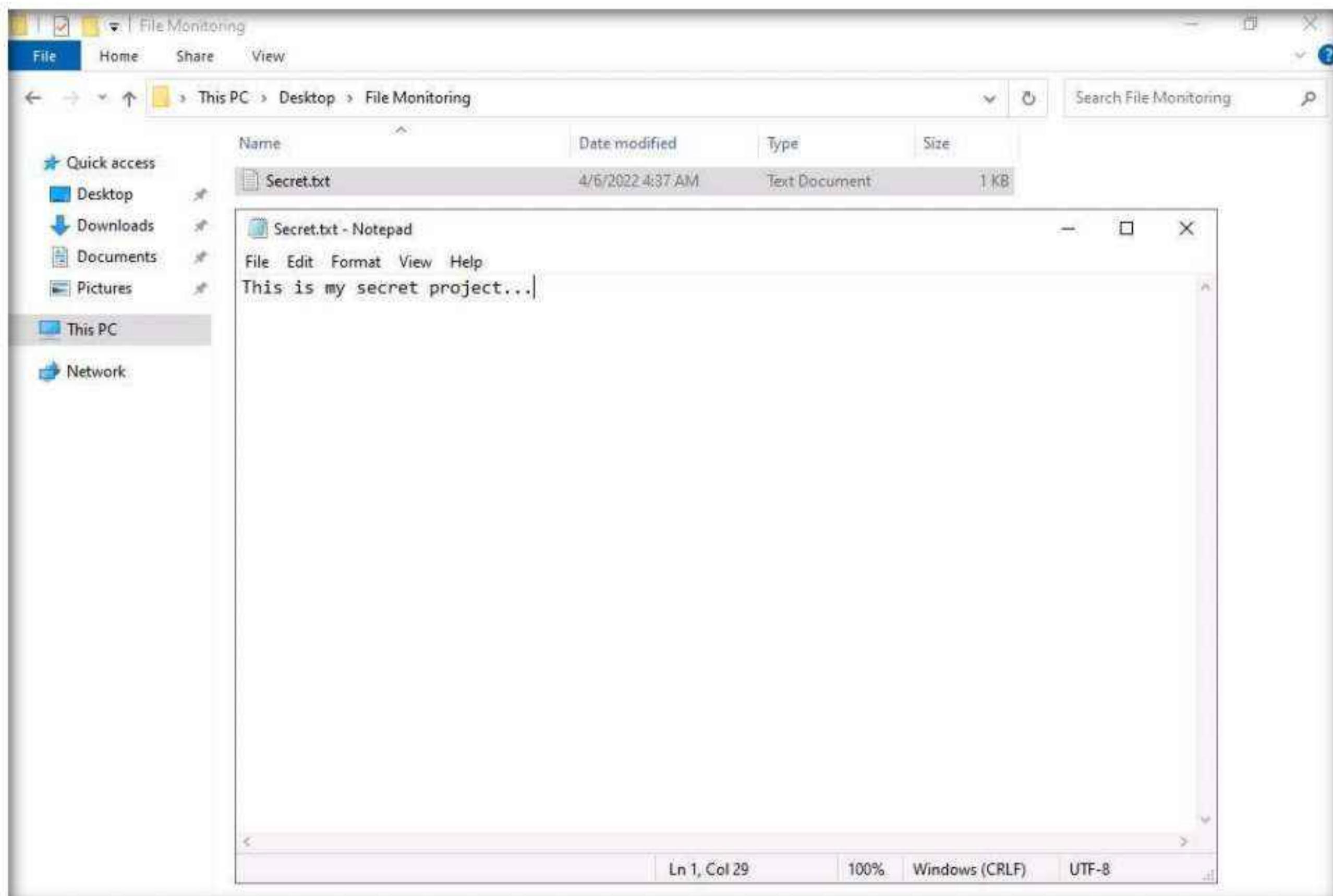


Module 07 – Malware Threats

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

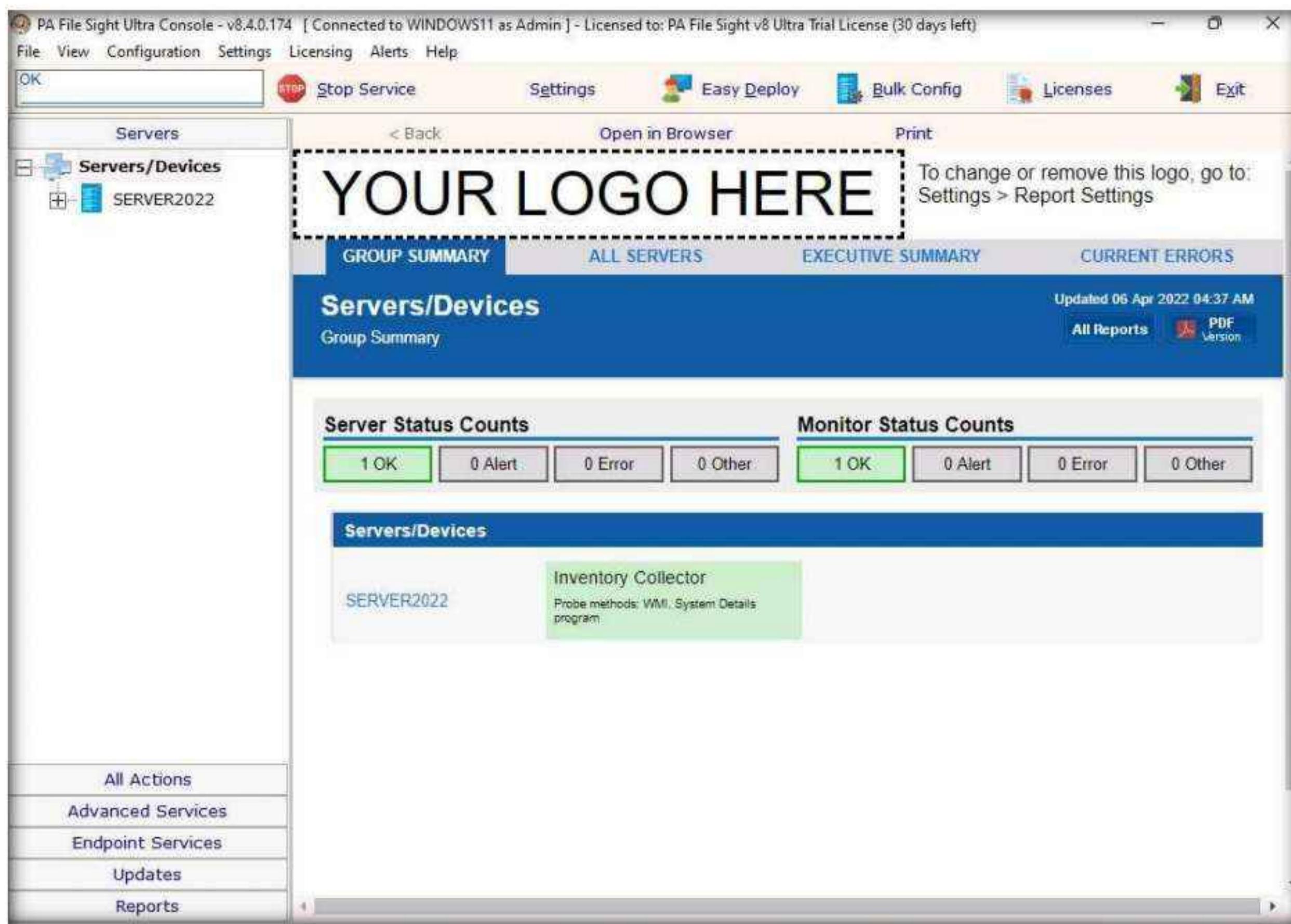


22. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.

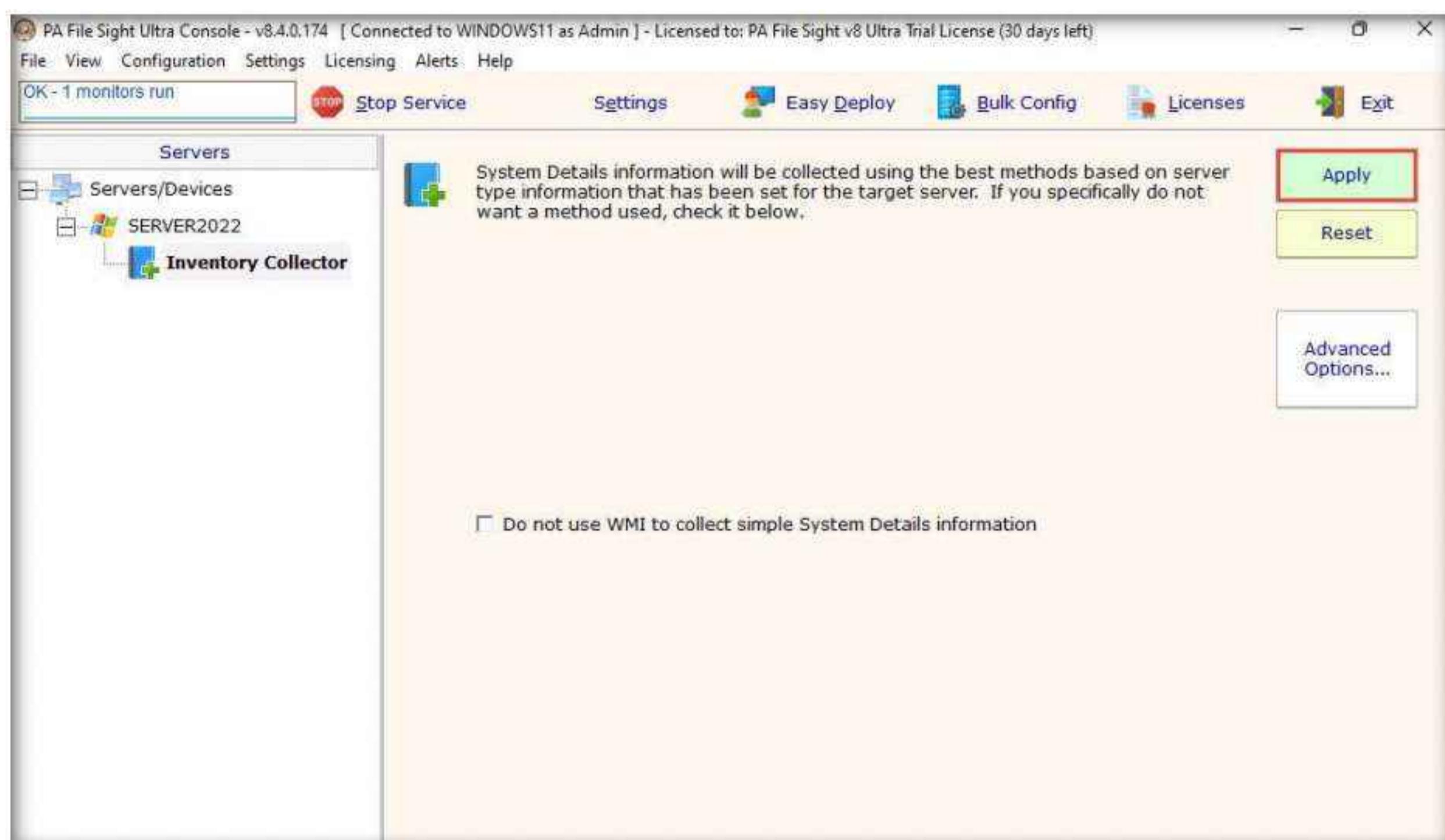


Module 07 – Malware Threats

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

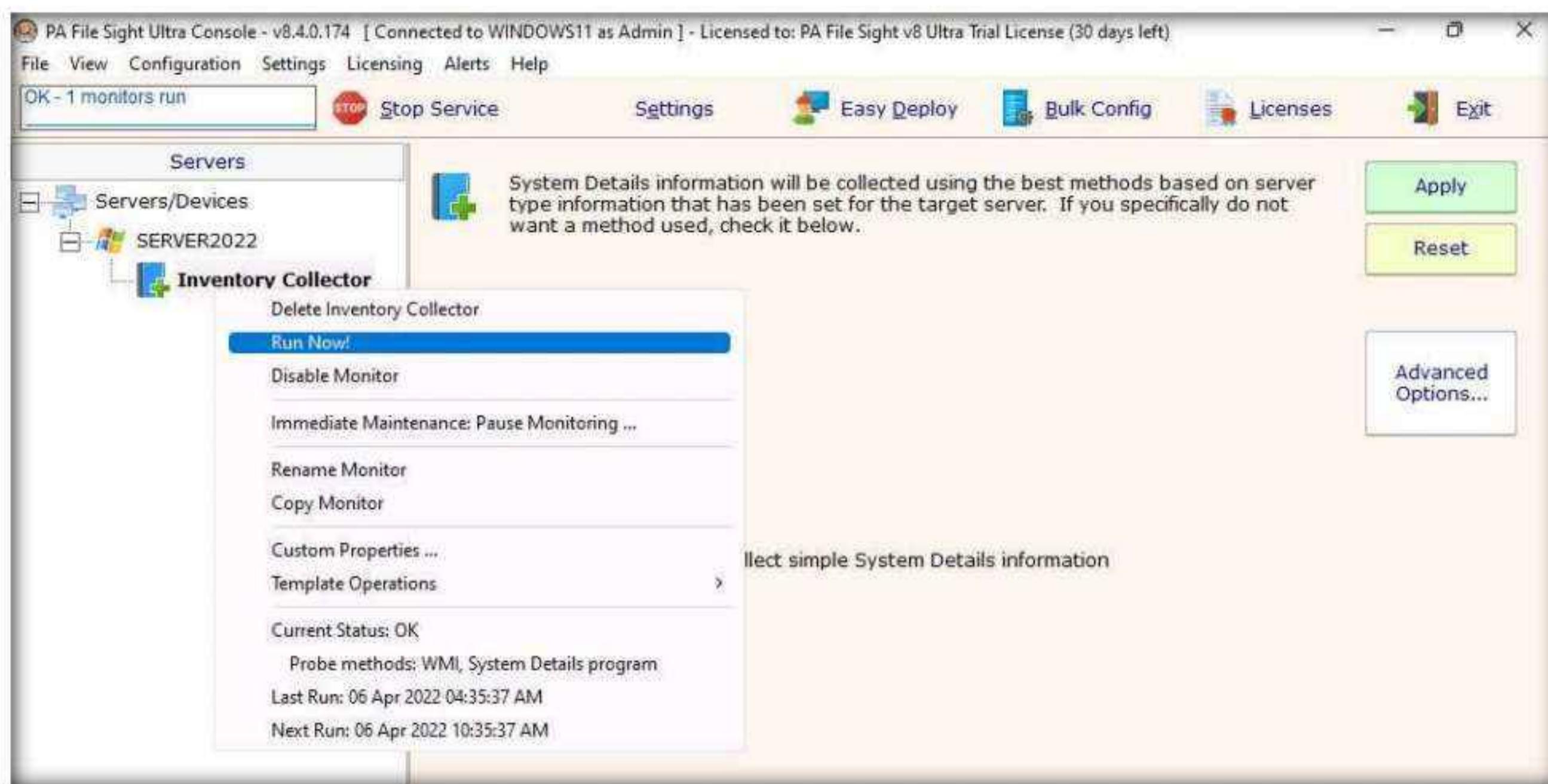


24. Expand the **Server2022** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.

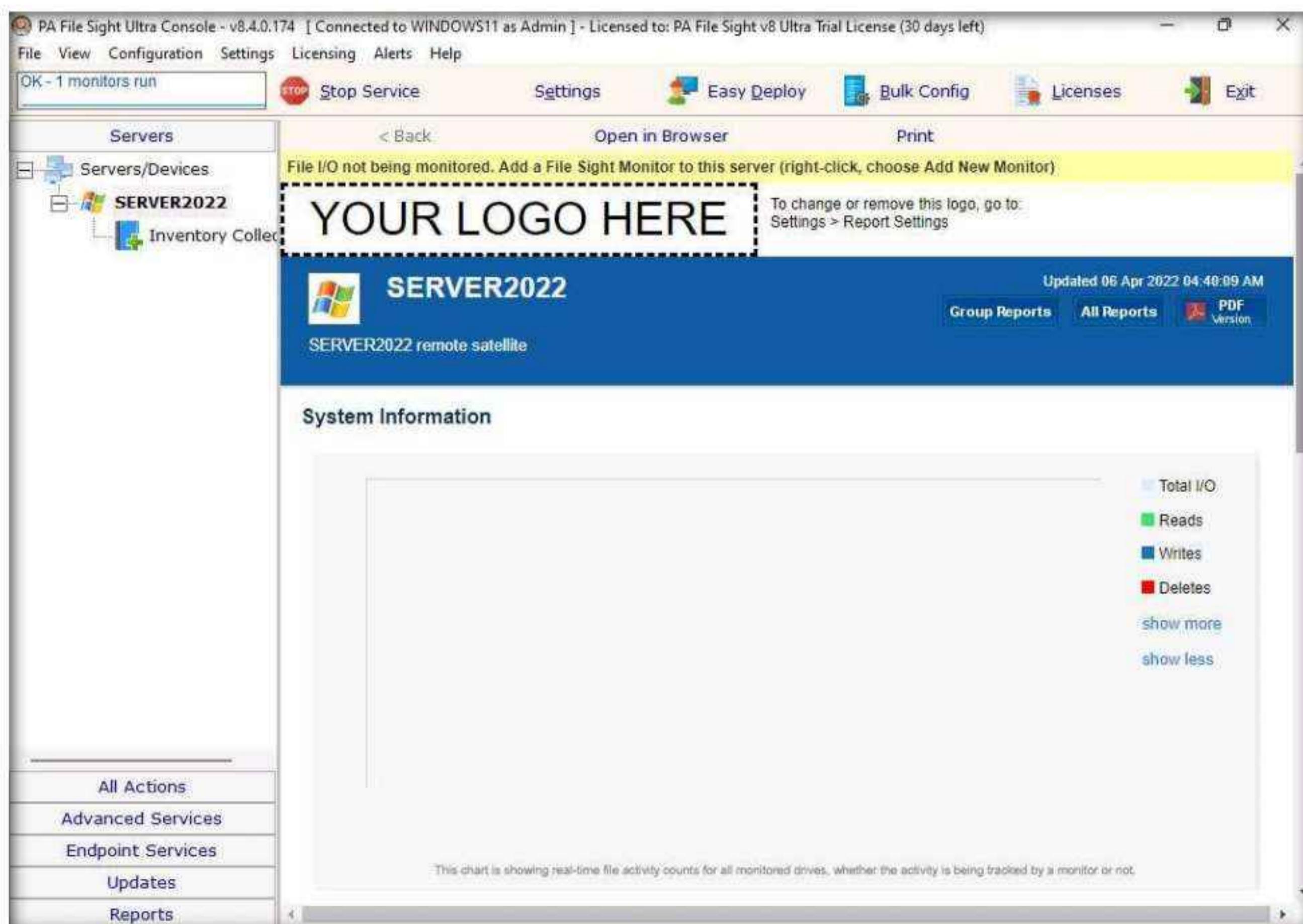


Module 07 – Malware Threats

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.



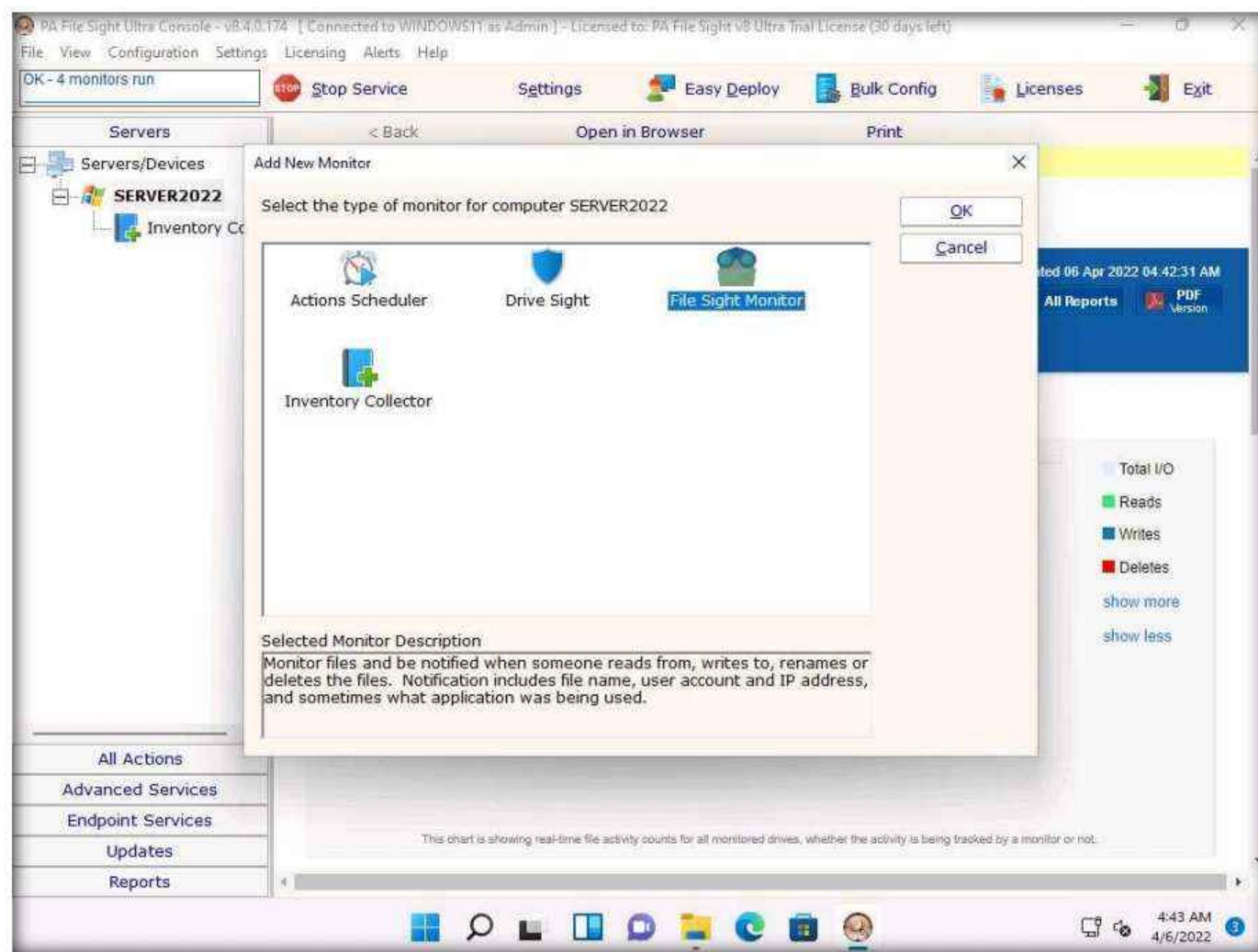
Module 07 – Malware Threats

The screenshot shows the PA File Sight Ultra Console interface. The top menu bar includes File, View, Configuration, Settings, Licensing, Alerts, and Help. A message at the top states "OK - 1 monitors run". Below the menu is a toolbar with Stop Service, Settings, Easy Deploy, Bulk Config, Licenses, and Exit. On the left, a tree view shows "Servers/Devices" expanded to "SERVER2022" and "Inventory Collector". A chart titled "Hourly Alert Rate" is displayed with a value of 0.0 for April 04. The main area contains "System Details" and "Monitor Status" sections. Under "System Details", it shows Uptime (0 days, 2 hours, 1 minutes), Operating System (Microsoft Windows Server 2022 Standard 10.0.20348), CPU (Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz (64 bit, None), 2 Cores), and Memory (Physical: 8,191 MB). Under "Monitor Status", there is one entry for "Inventory Collector" with a status of "OK" and last checked at "4/6/2022 4:40:10 AM". A sidebar on the left lists All Actions, Advanced Services, Endpoint Services, Updates, and Reports.

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

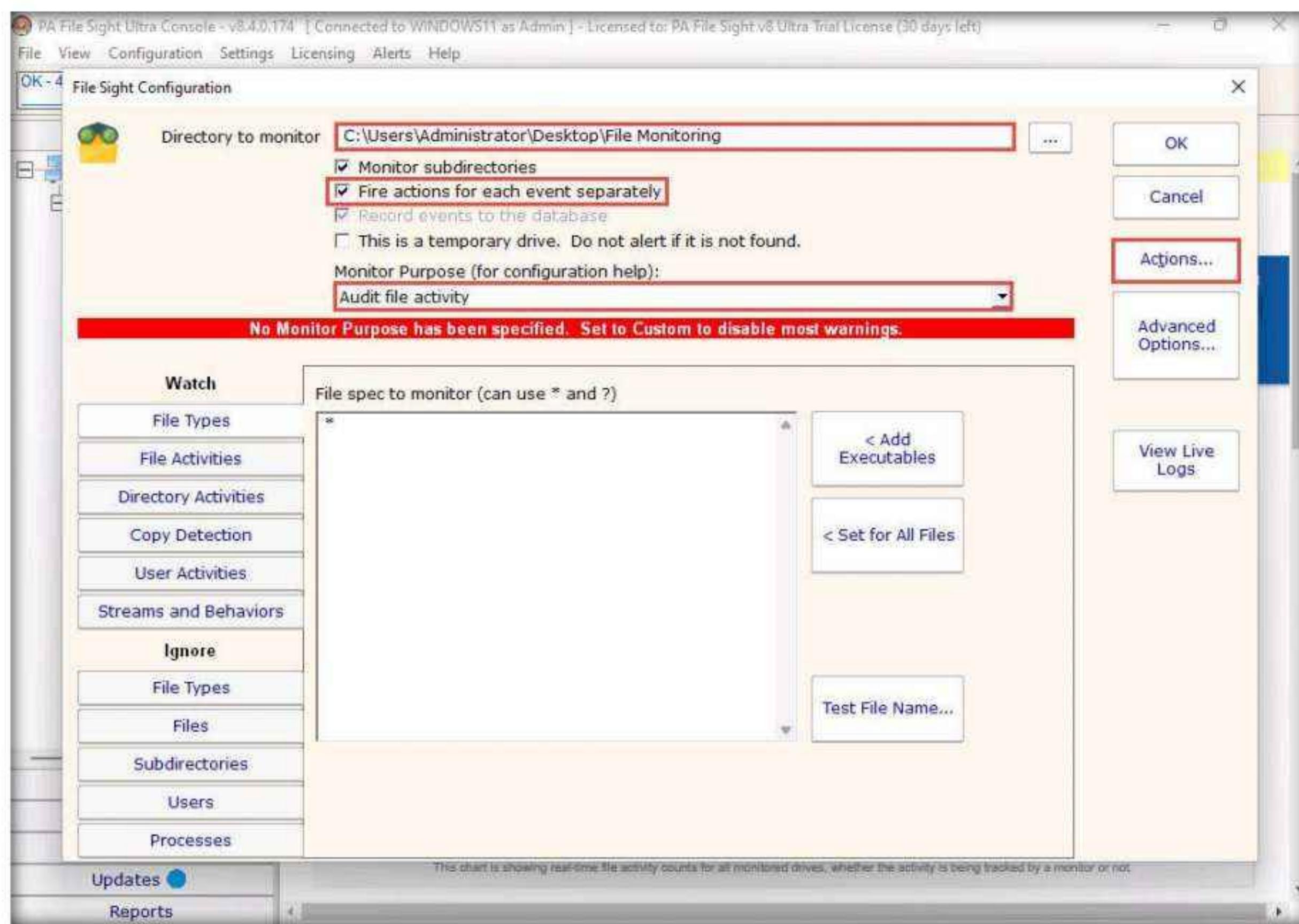
The screenshot shows the PA File Sight Ultra Console interface with the context menu open over "SERVER2022". The menu items include "Add New Monitor ...", "Delete SERVER2022", "Set Server Alias ...", "Change Hostname / IP Address", "Move Device to Different Group", "Maintenance Period", "Disable monitoring of server/device", "Configuration", "Copy Computer", "Custom Properties ...", "Prevent Template Propagation", "Block Auto Configuration", "Report & Delivery Settings", "Operations", and "Notes ...". A note above the menu says "File I/O not being monitored. Add a File Sight Monitor to this server (right-click, choose Add New Monitor)". To the right of the menu, there is a logo placeholder "YOUR LOGO HERE" with instructions to change it via "Settings > Report Settings". A status bar at the bottom right shows "Updated 06 Apr 2022 04:42:31 AM" and links for "Group Reports", "All Reports", and "PDF Version". A legend on the right identifies four data series: "Total I/O" (light blue), "Reads" (green), "Writes" (dark blue), and "Deletes" (red).

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

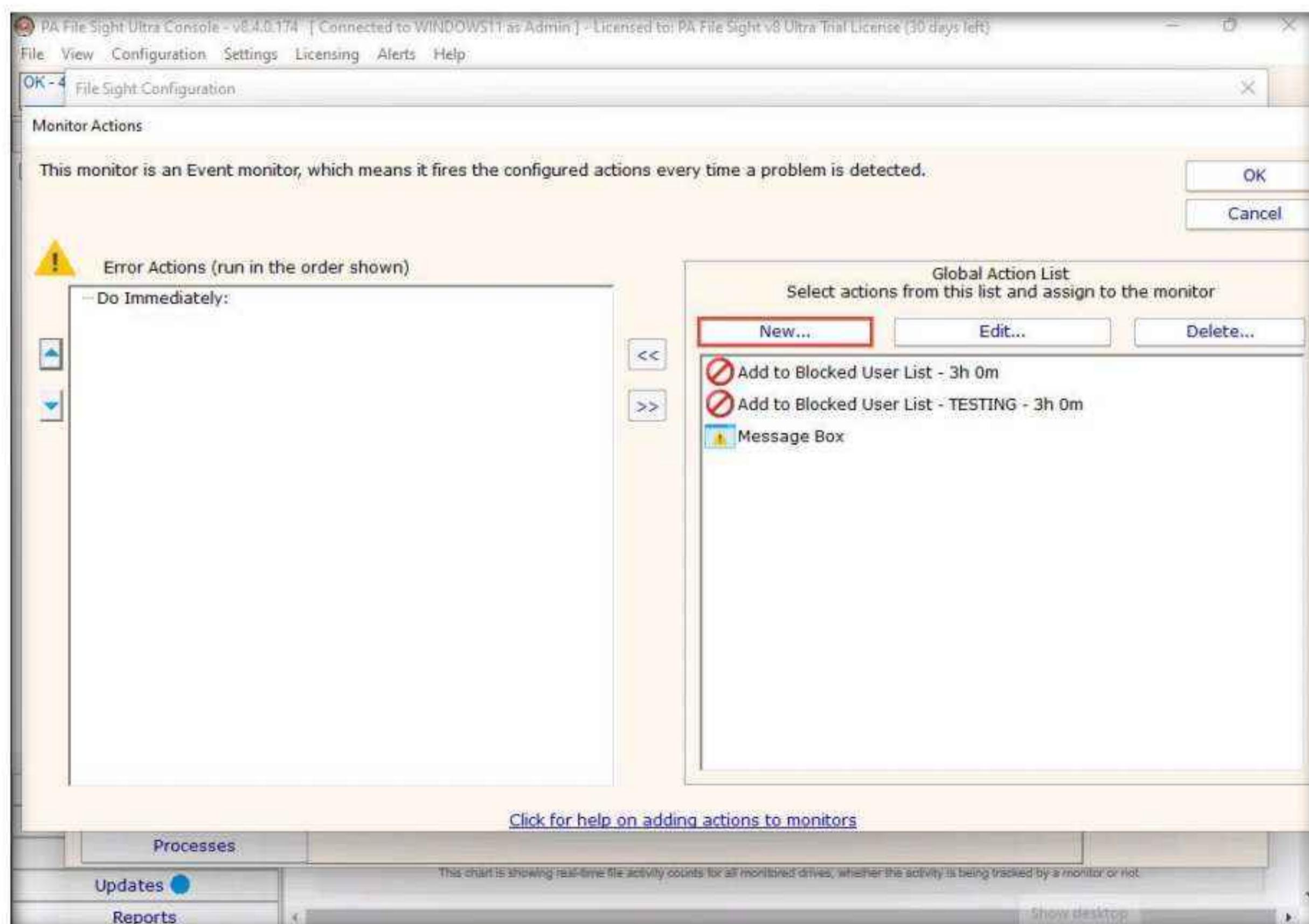


29. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **Server2022** machine (here, **C:\Users\Administrator\Desktop\File Monitoring**) and tick the **Fire actions for each event separately** checkbox.
30. Choose **Audit file activity** from the **Monitor Purpose (for configuration help)** dropdown list, and then click **Actions**.

Module 07 – Malware Threats

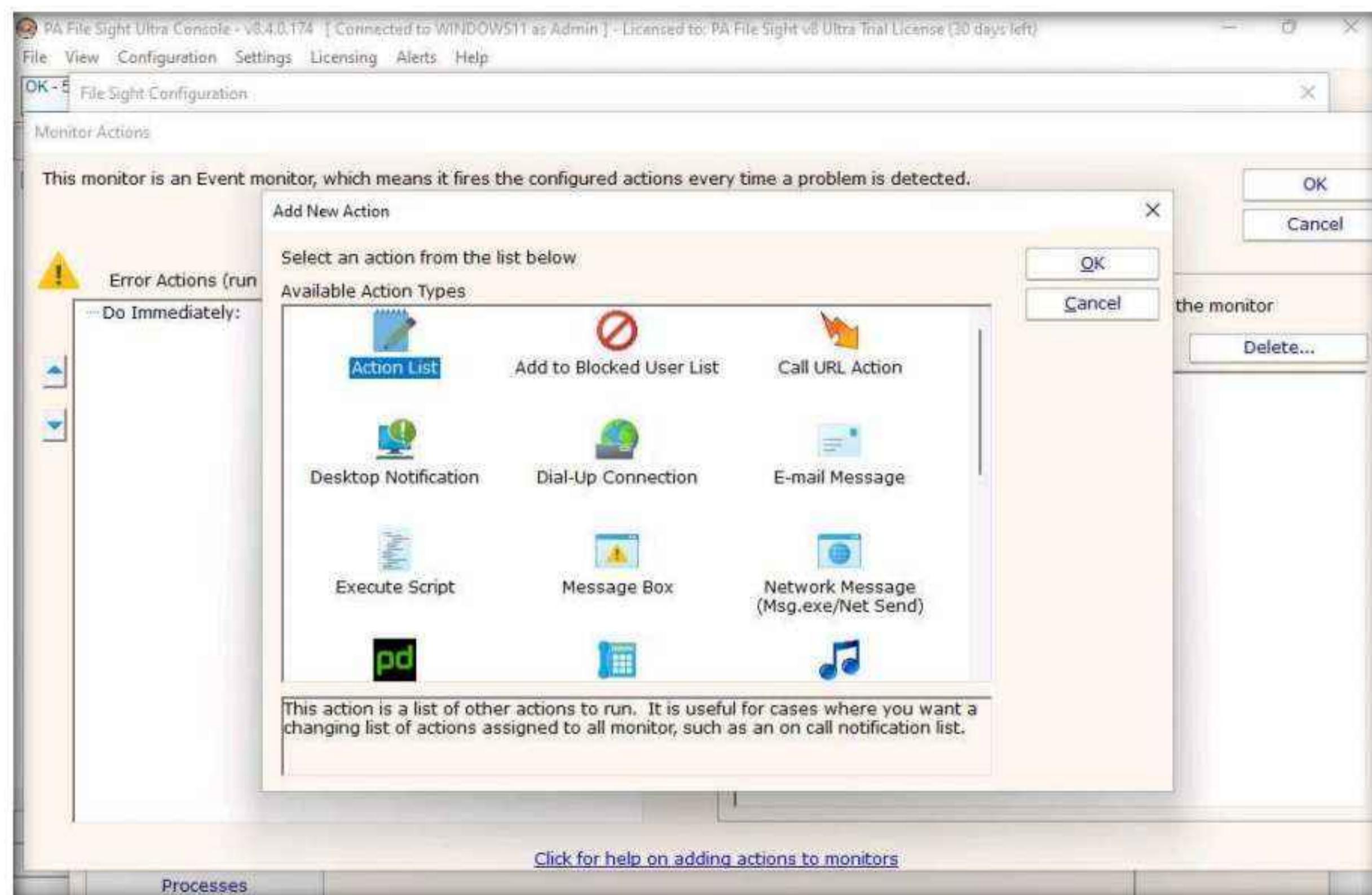


31. The Monitor Actions window appears; click New under Global Action List.

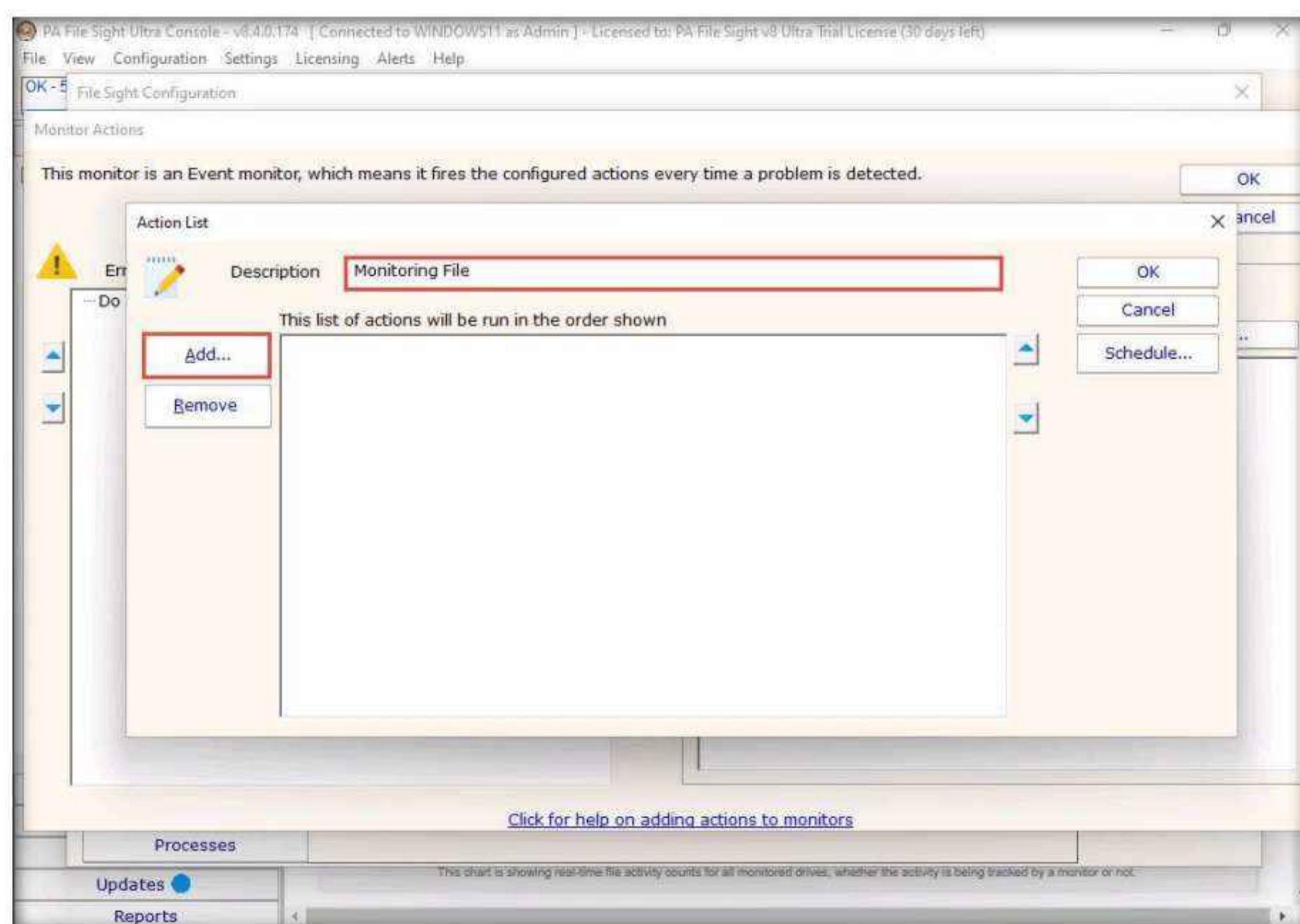


Module 07 – Malware Threats

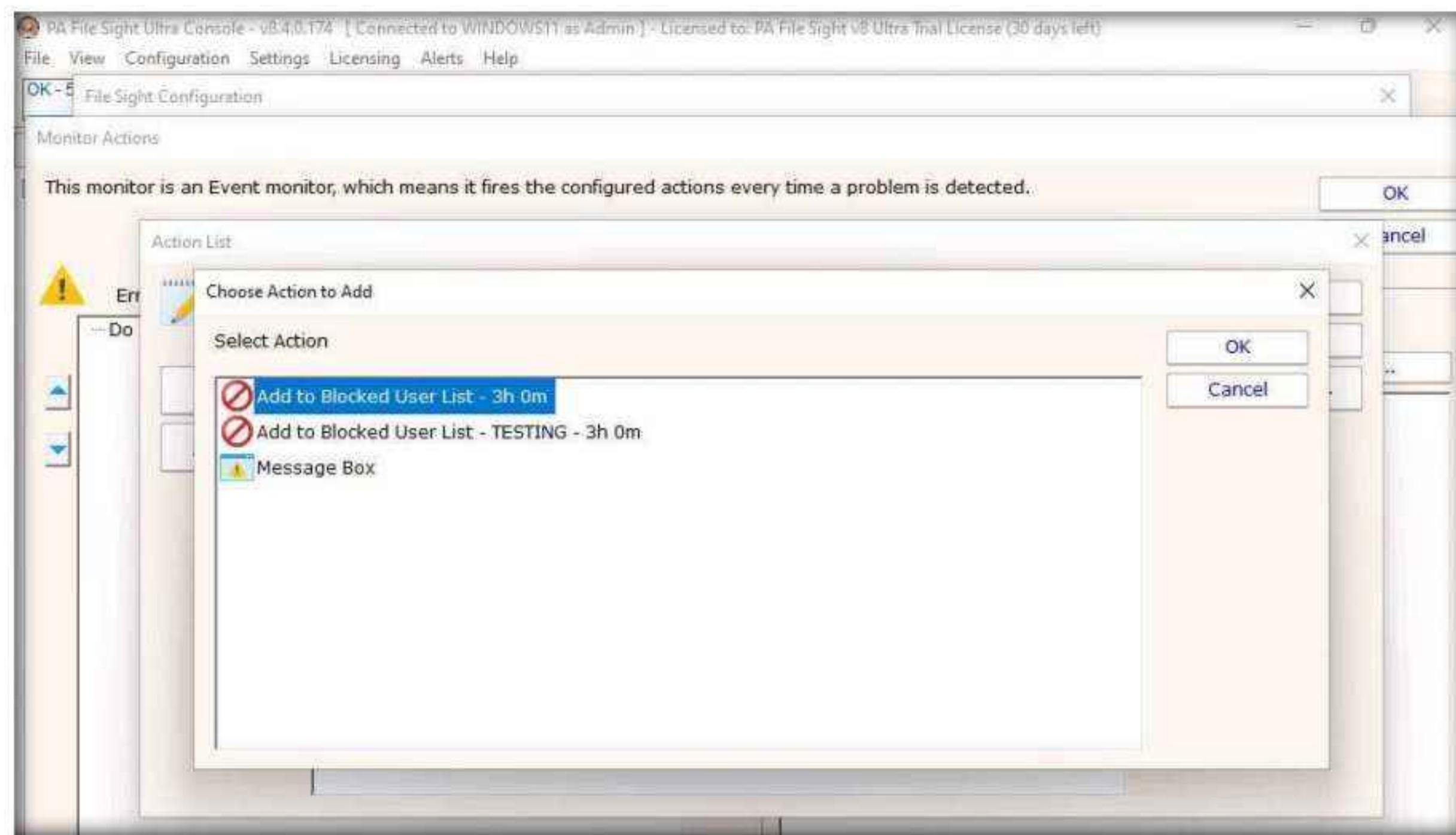
32. The Add New Action window appears. Select the Action List icon and click OK.



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

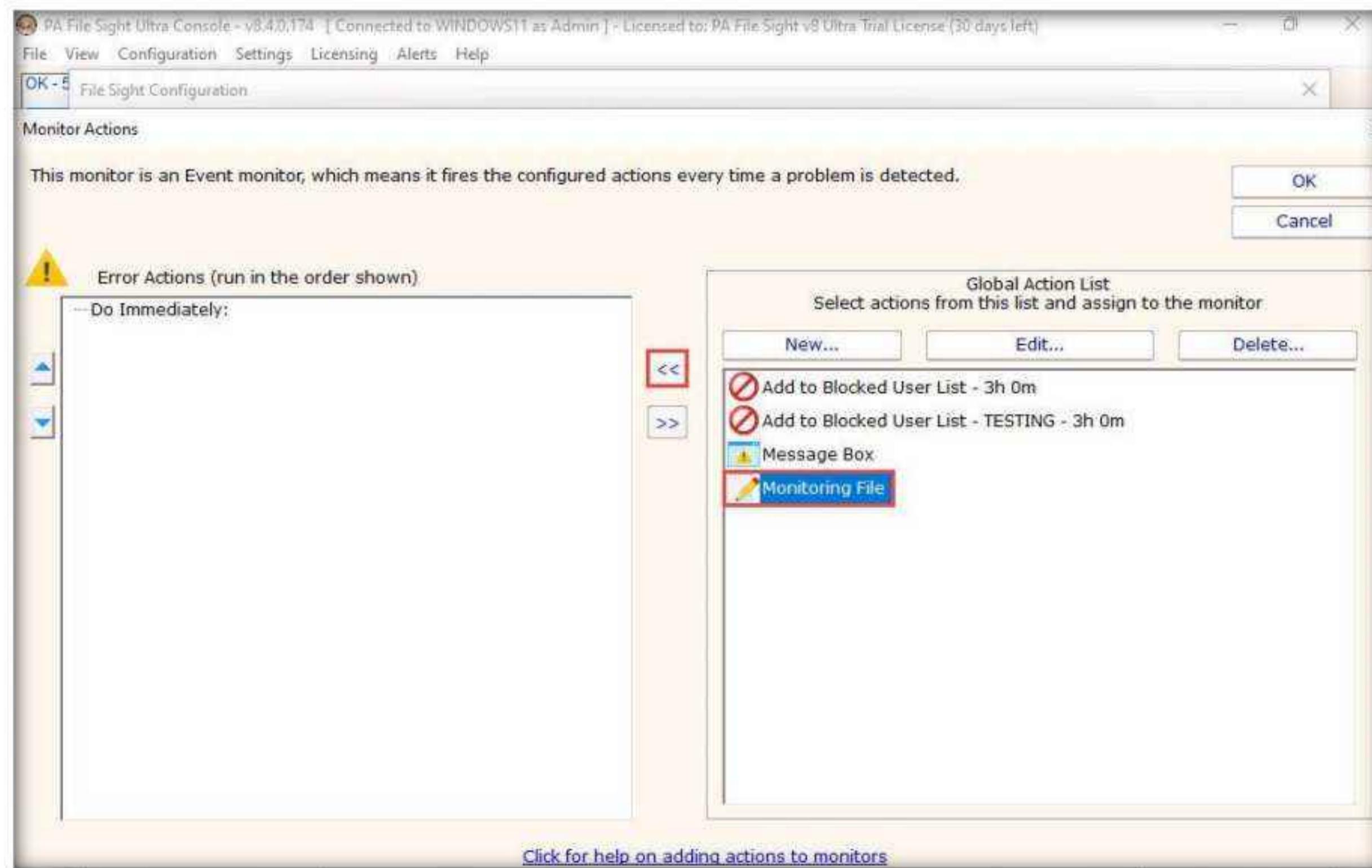


34. The **Choose Action to Add** window appears; choose any action from the list and click **OK**.



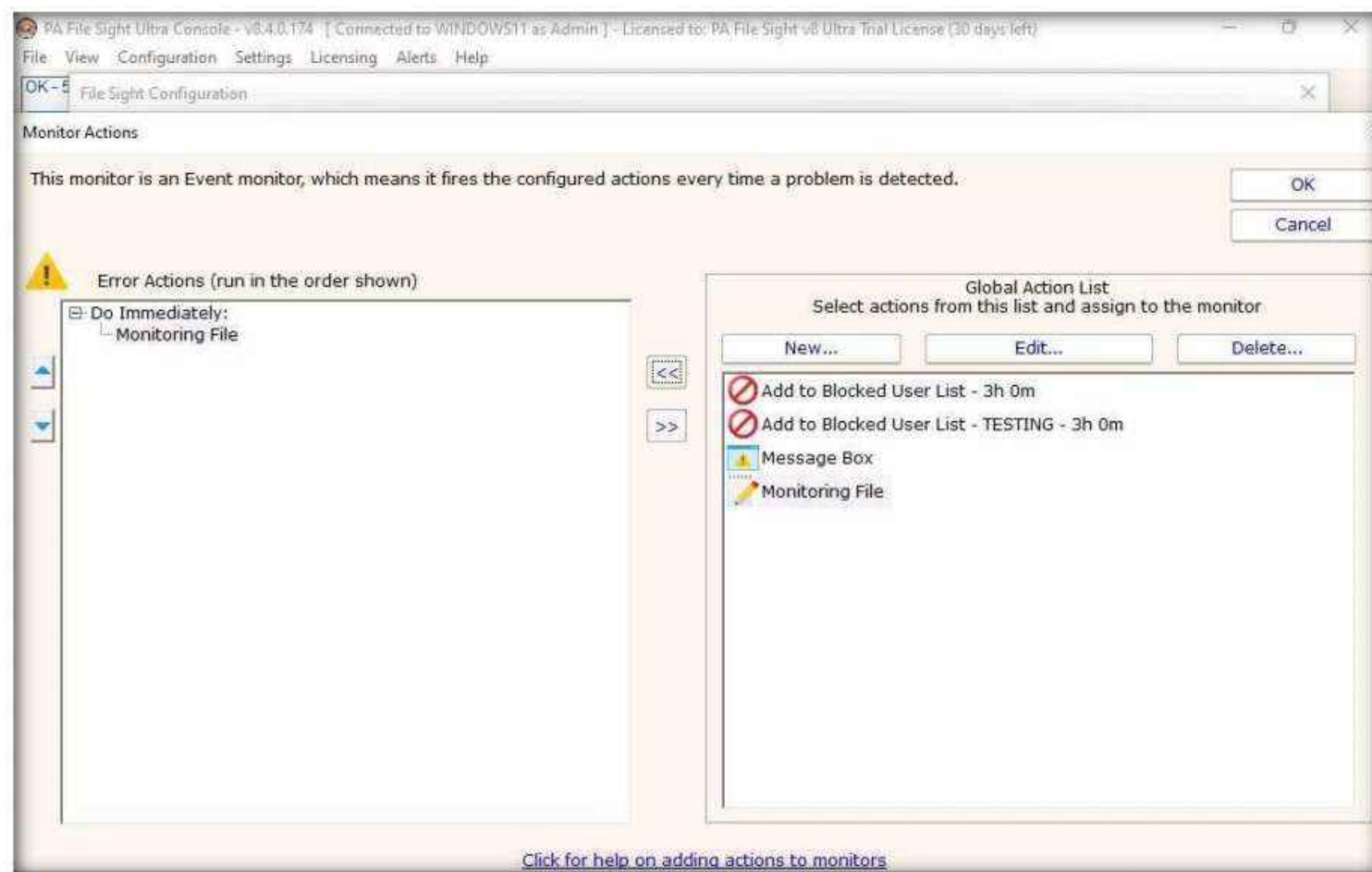
35. Click **OK** in the **Action List** window.

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

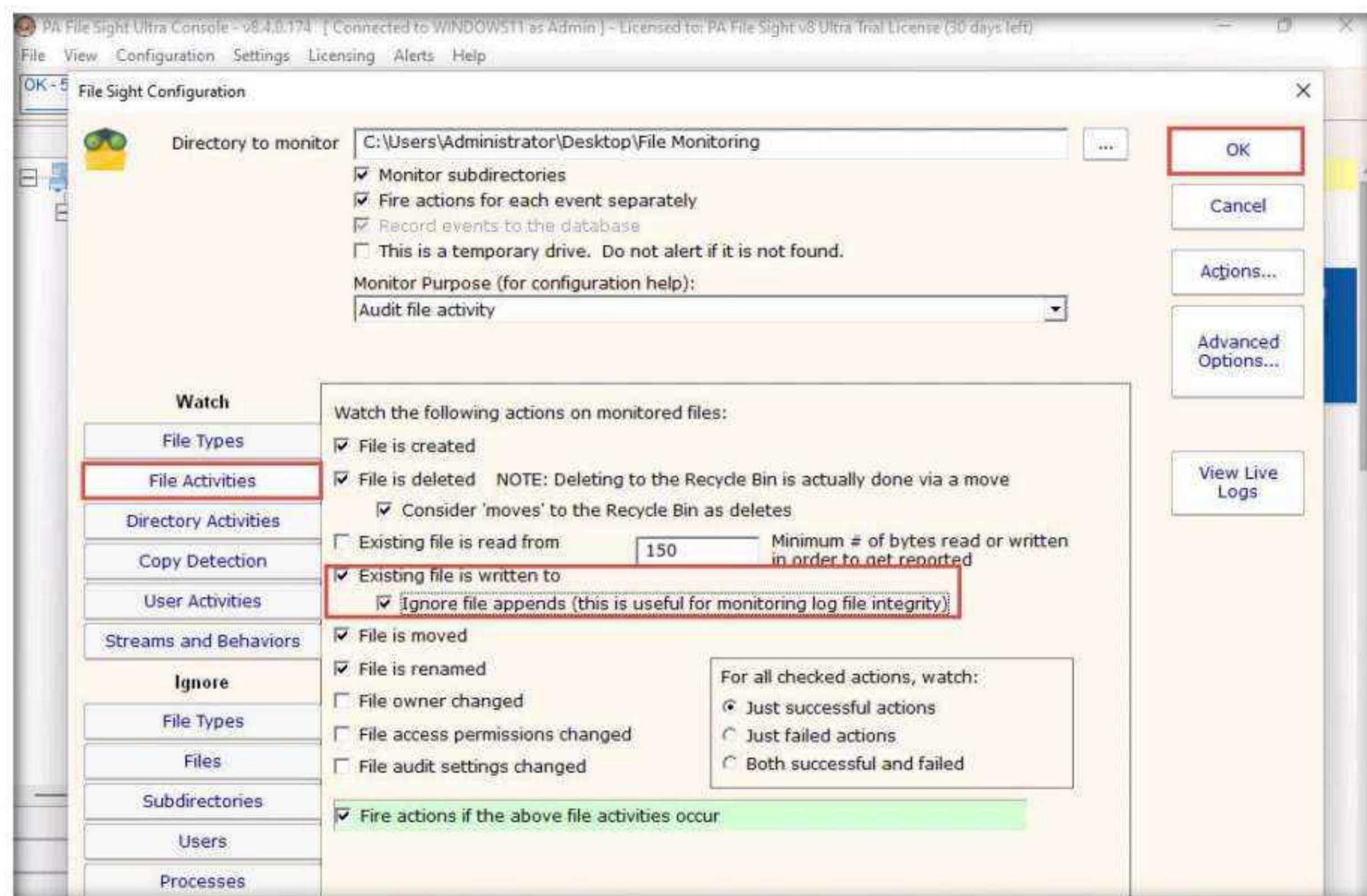


Module 07 – Malware Threats

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

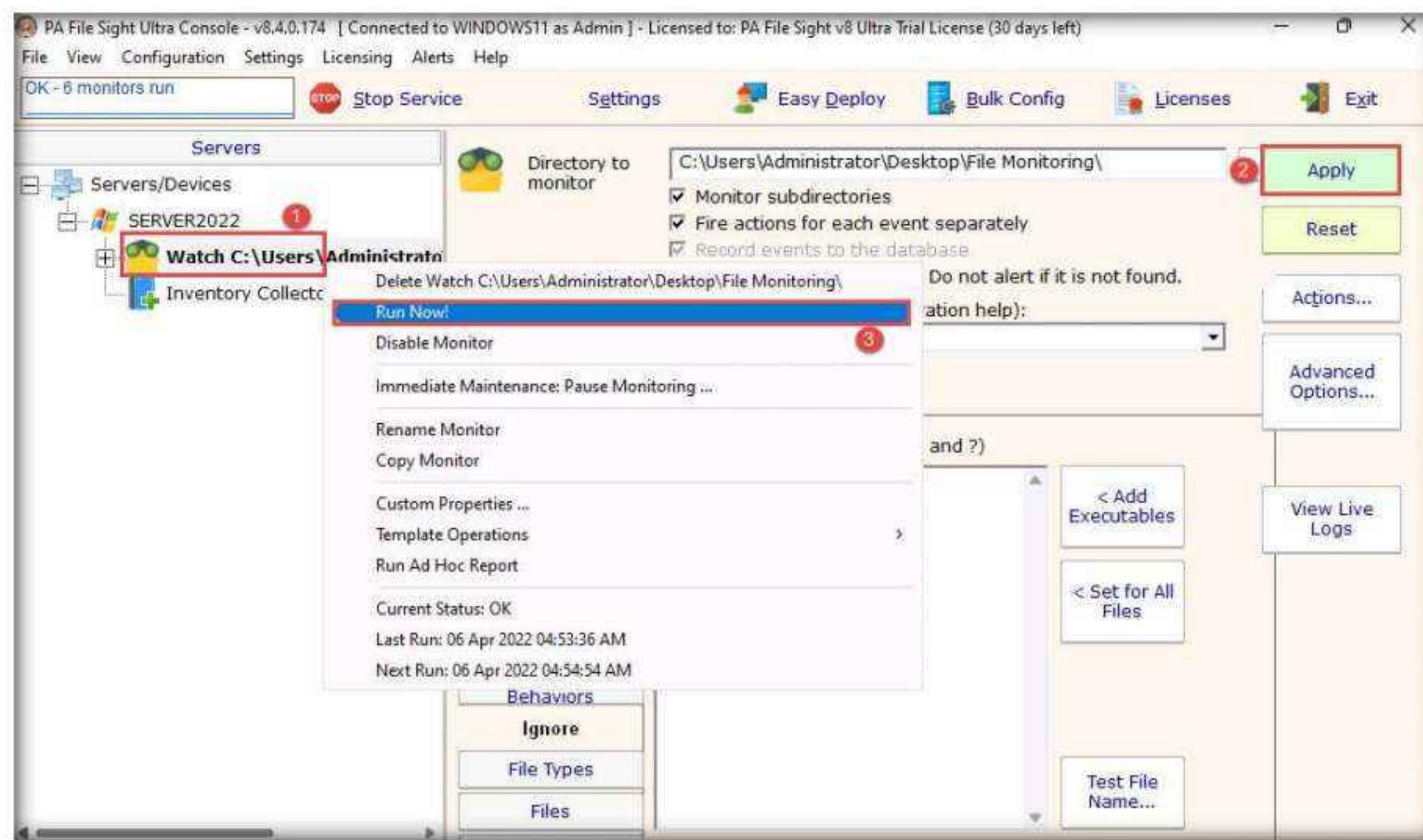


38. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.

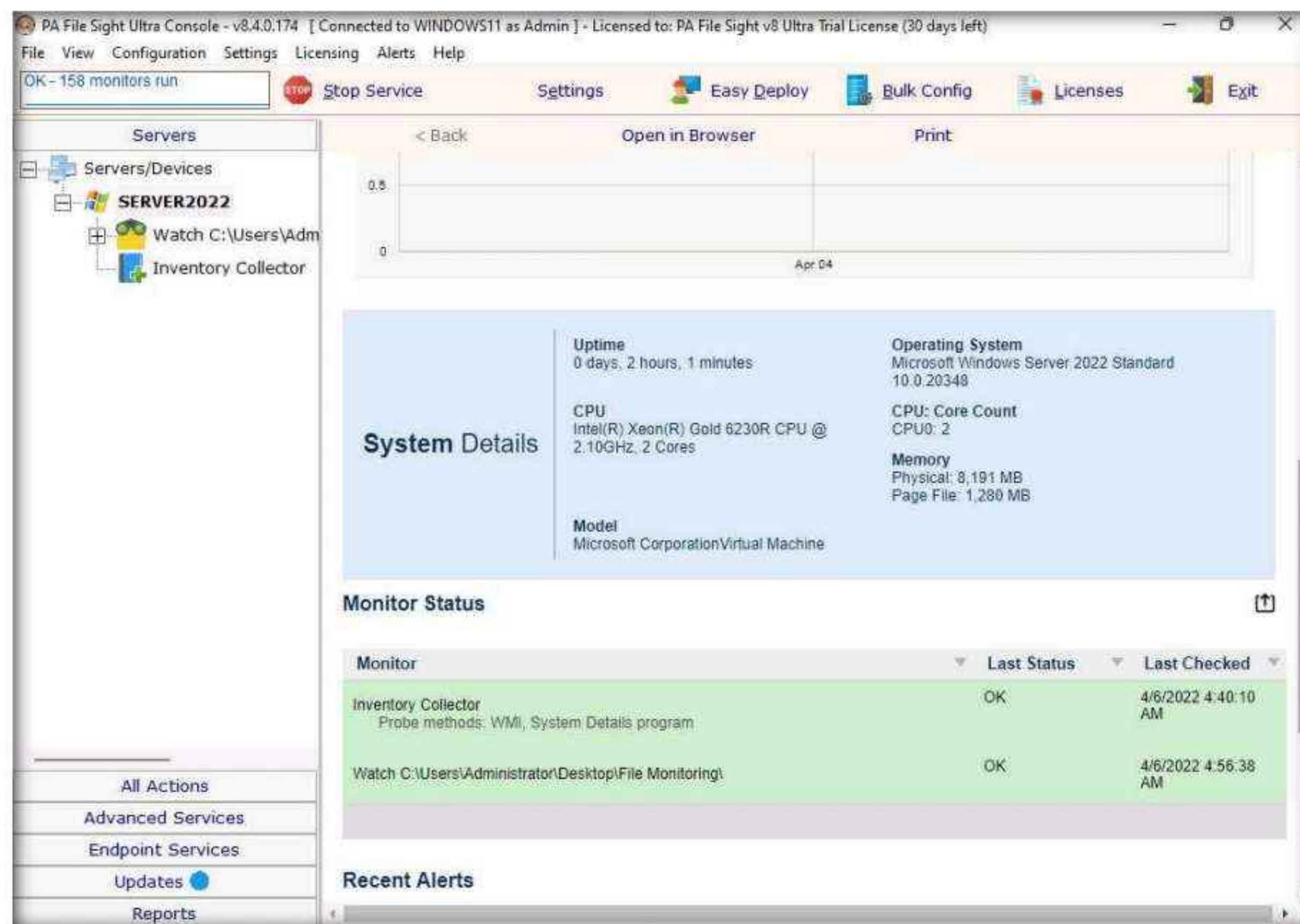


Module 07 – Malware Threats

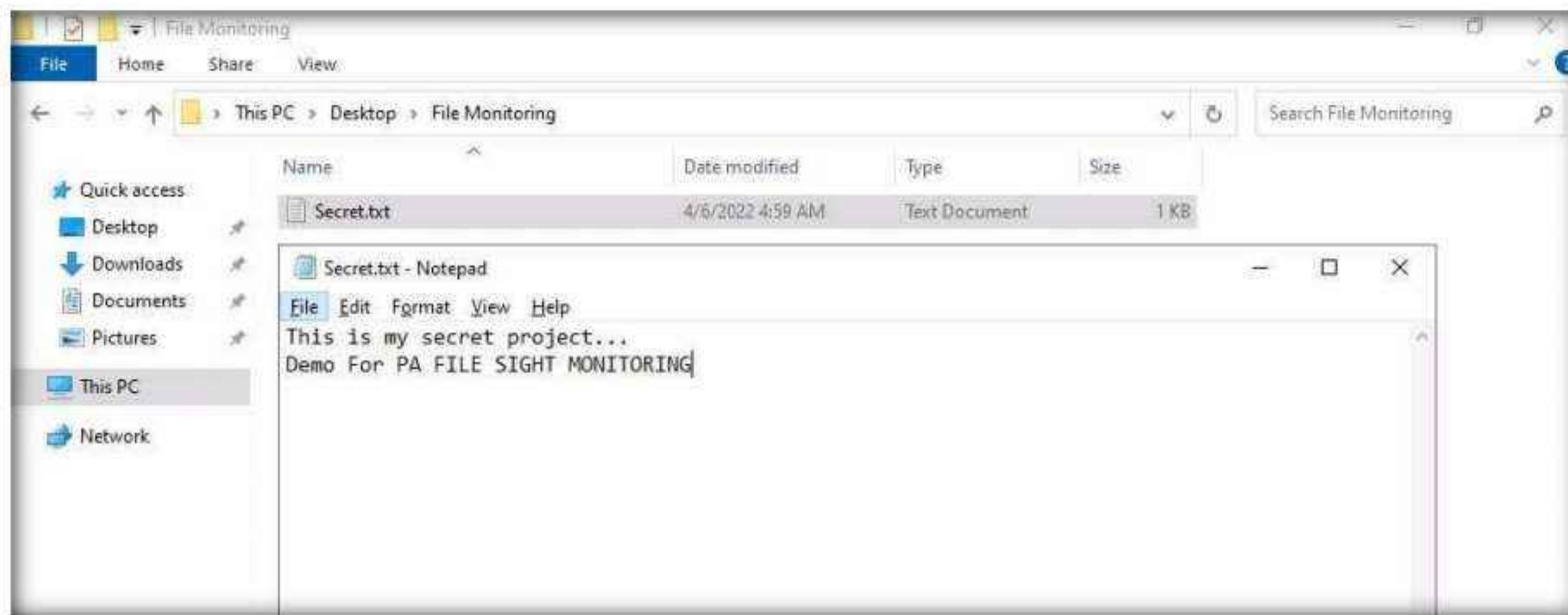
39. Under the **Server2022** node, **Watch** node will be added, select it and click **Apply** from the right-pane. Then right-click on the **File Monitoring / Watch** node and click **Run Now!** from the context menu.



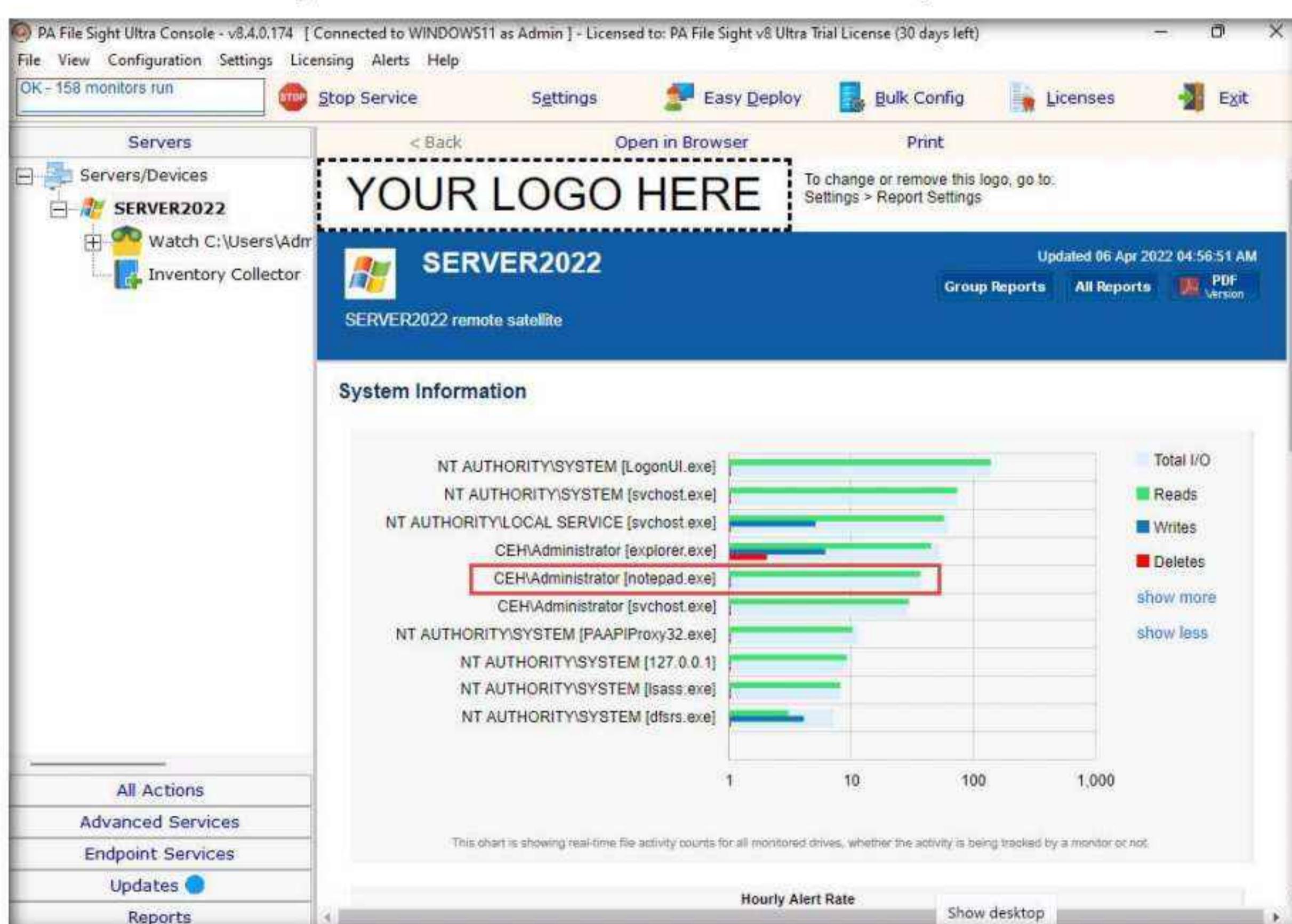
40. Click the **Server2022** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.



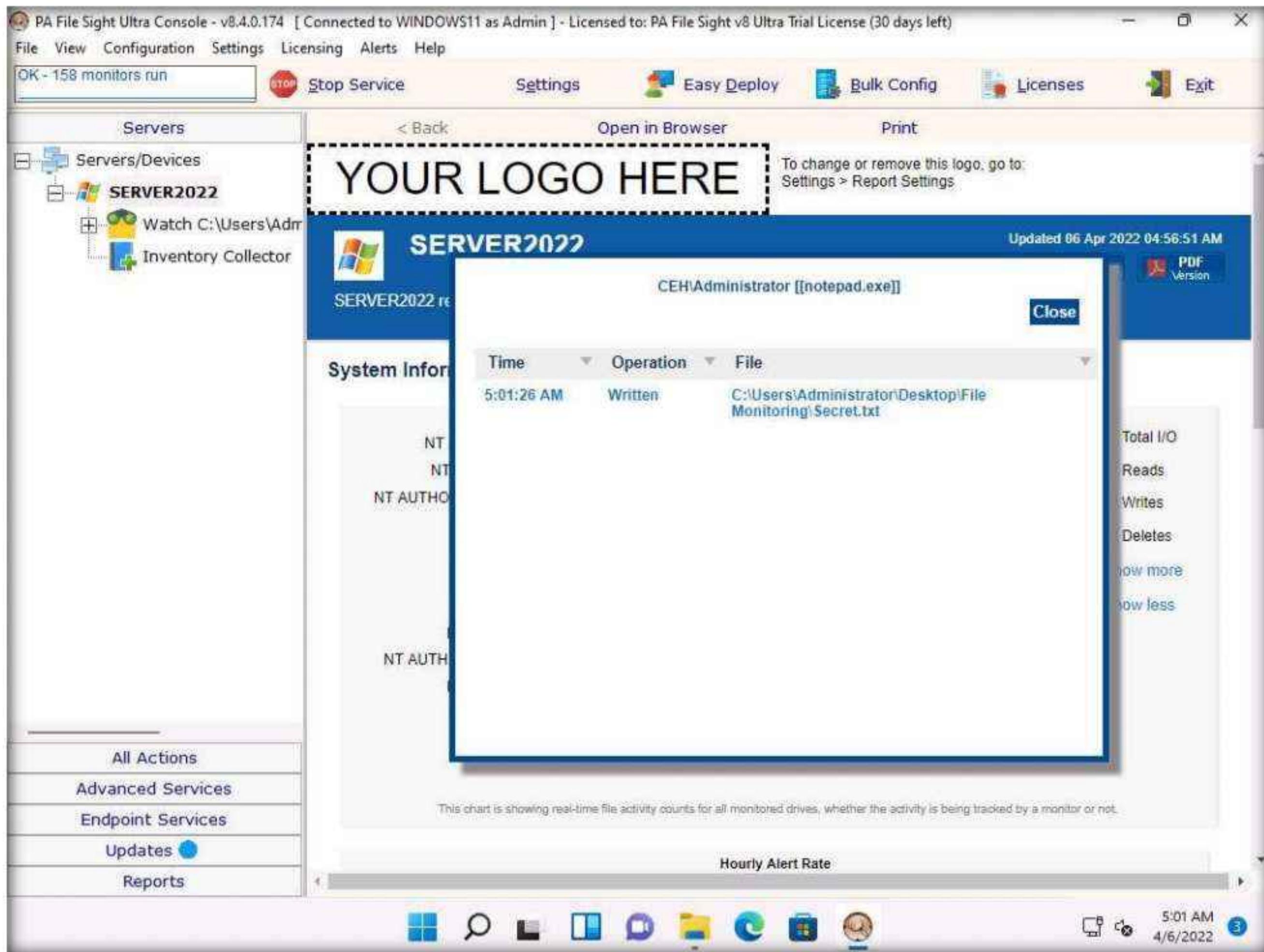
41. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**. Open **Secret.txt** in the **File Directory on Desktop**, modify some of the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



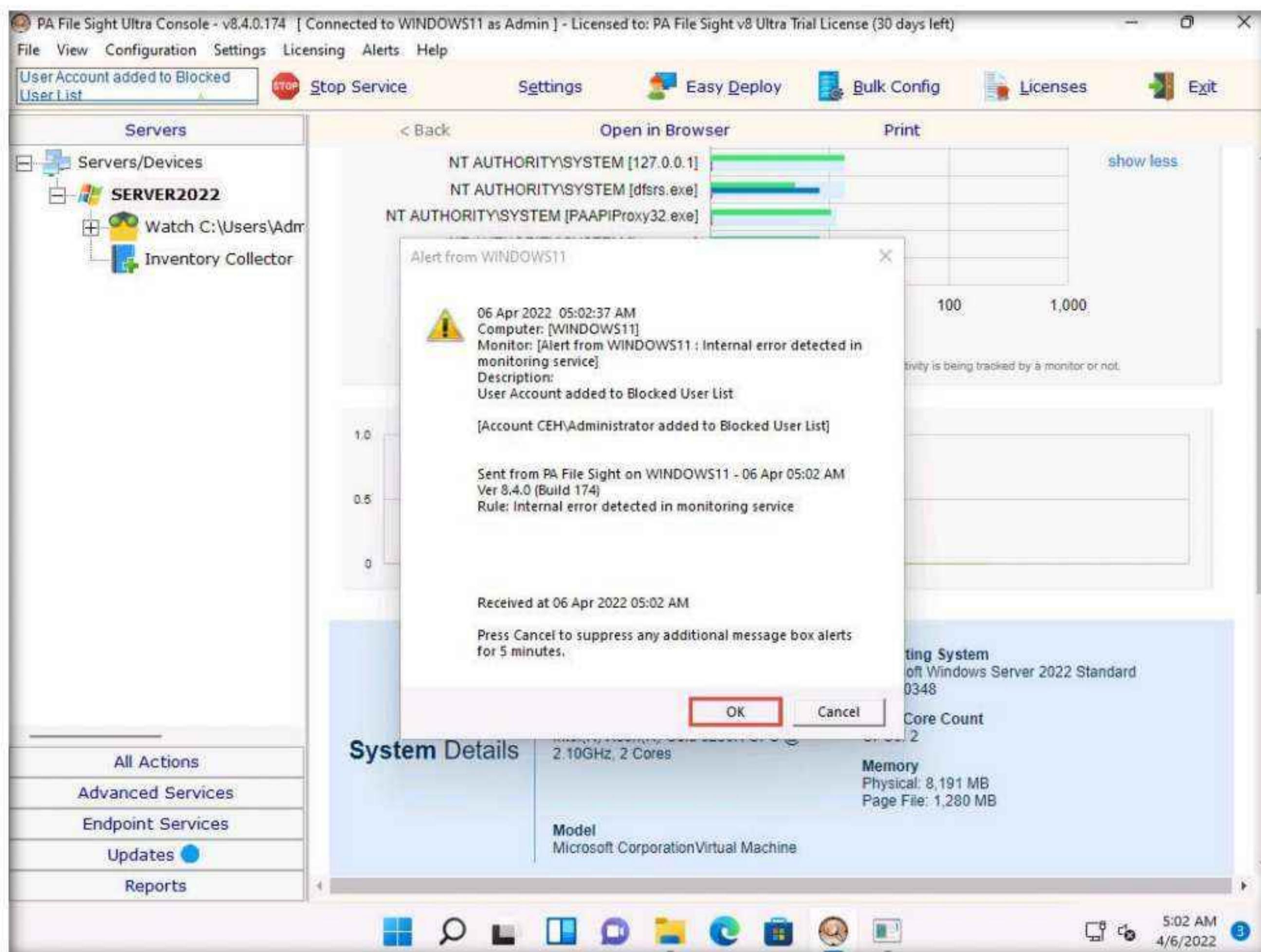
42. Switch back to the **Windows 11** virtual machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.
 43. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.
 44. Click on the **notepad.exe** link to view the activities done by the user.



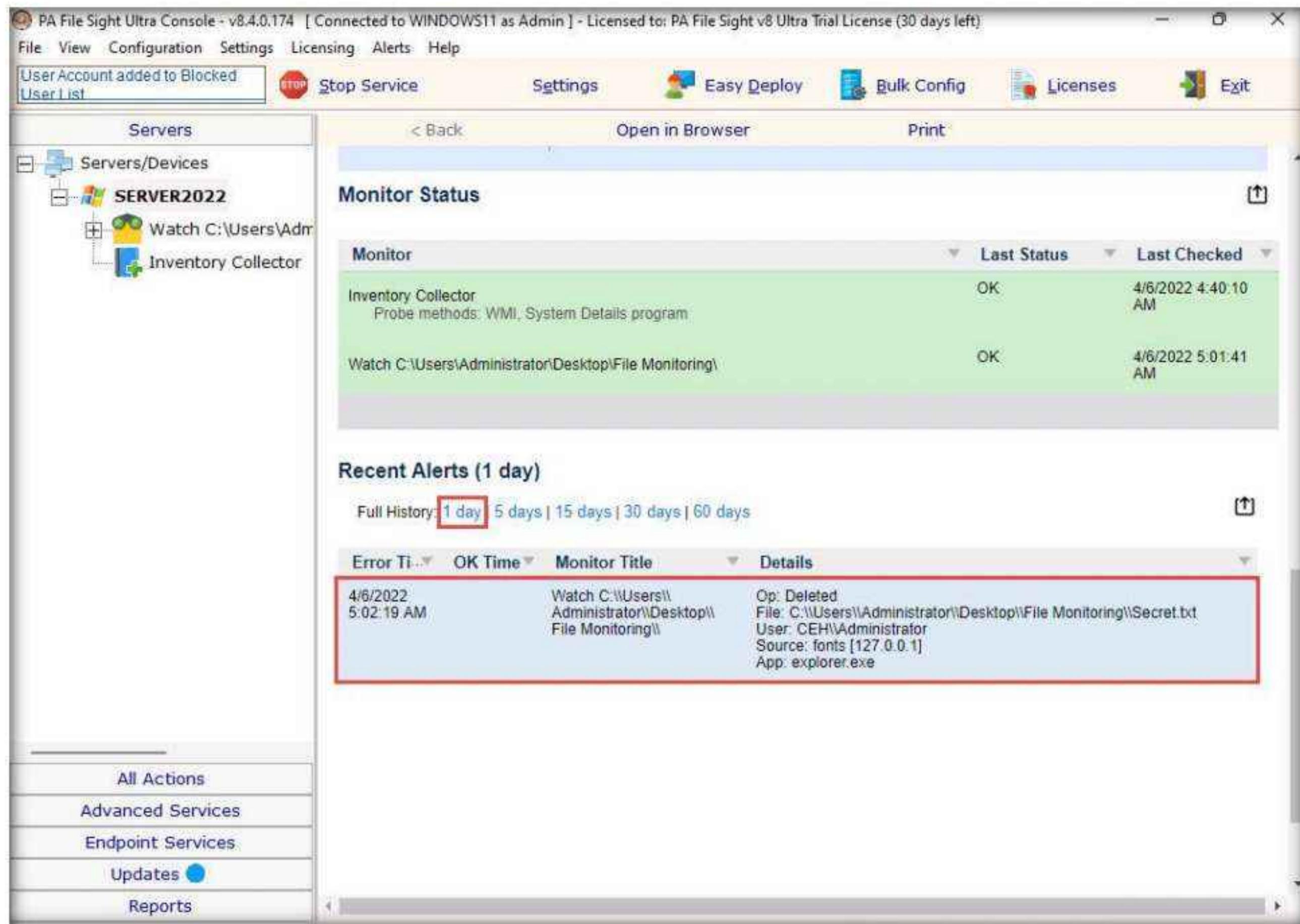
45. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then switch to the **Windows Server 2022** virtual machine, type some content into the **Secret.txt** file, save the file, and then immediately switch back to the **Windows 11** virtual machine to view the activity.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

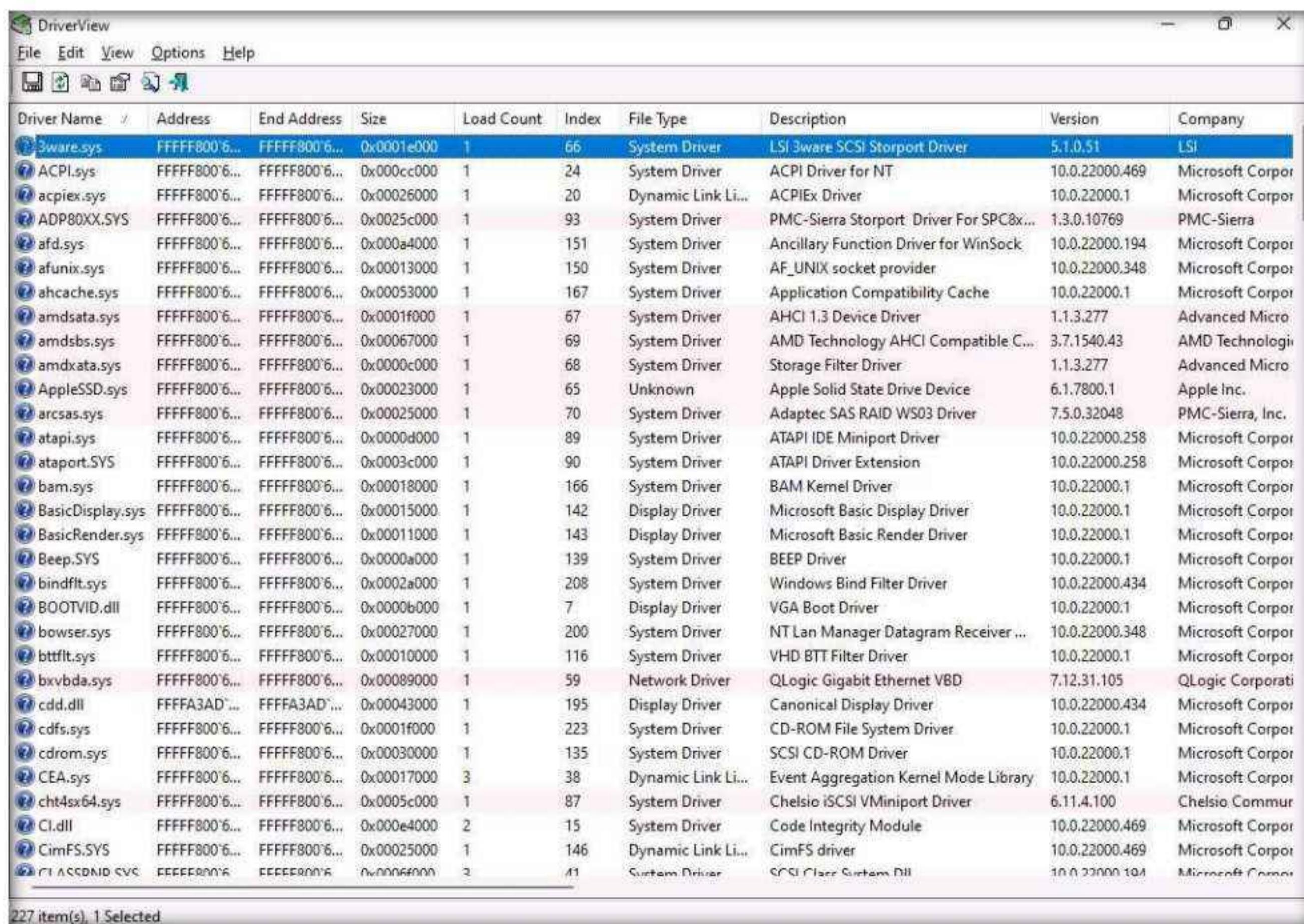
DriverView: The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

Module 07 – Malware Threats

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.

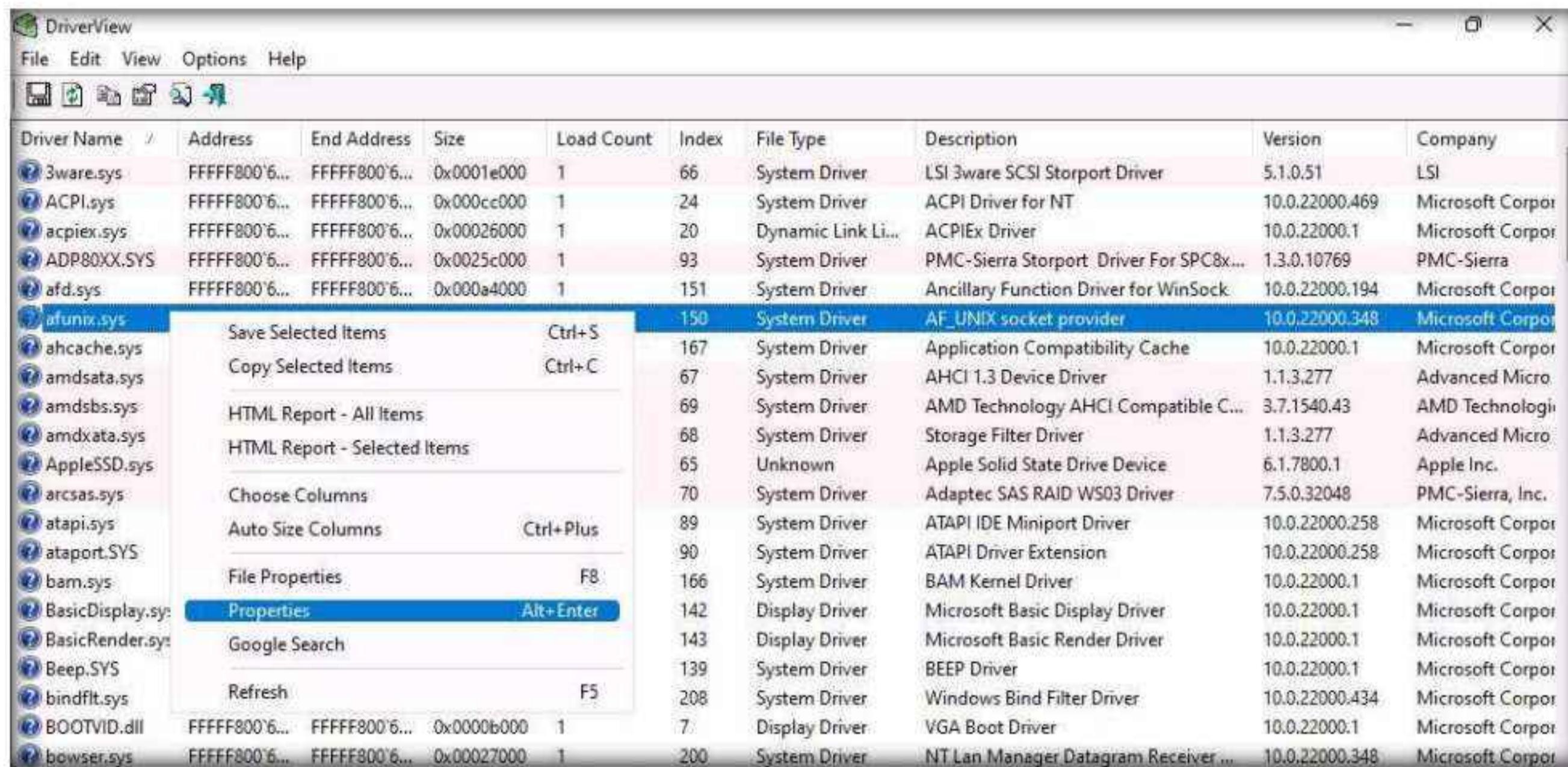


The screenshot shows the DriverView application window. The menu bar includes File, Edit, View, Options, Help, and a toolbar with icons for search, refresh, and file operations. The main area is a grid table with the following columns: Driver Name, Address, End Address, Size, Load Count, Index, File Type, Description, Version, and Company. The table lists numerous drivers, such as LSI 3ware SCSI Storport Driver, ACPI Driver for NT, and various Microsoft and third-party drivers like AHCI 1.3 Device Driver, AMD Technology AHCI Compatible C..., and Apple Solid State Drive Device. The bottom status bar indicates "227 item(s), 1 Selected".

Driver Name	Address	End Address	Size	Load Count	Index	File Type	Description	Version	Company
3ware.sys	FFFFF800'6...	FFFFF800'6...	0x0001e000	1	66	System Driver	LSI 3ware SCSI Storport Driver	5.1.0.51	LSI
ACPI.sys	FFFFF800'6...	FFFFF800'6...	0x000cc000	1	24	System Driver	ACPI Driver for NT	10.0.22000.469	Microsoft Corpor
acpiex.sys	FFFFF800'6...	FFFFF800'6...	0x00026000	1	20	Dynamic Link Li...	ACPIEx Driver	10.0.22000.1	Microsoft Corpor
ADP80XX.SYS	FFFFF800'6...	FFFFF800'6...	0x0025c000	1	93	System Driver	PMC-Sierra Storport: Driver For SPC8x...	1.3.0.10769	PMC-Sierra
afd.sys	FFFFF800'6...	FFFFF800'6...	0x000a4000	1	151	System Driver	Ancillary Function Driver for WinSock	10.0.22000.194	Microsoft Corpor
afunix.sys	FFFFF800'6...	FFFFF800'6...	0x00013000	1	150	System Driver	AF_UNIX socket provider	10.0.22000.348	Microsoft Corpor
ahcache.sys	FFFFF800'6...	FFFFF800'6...	0x00053000	1	167	System Driver	Application Compatibility Cache	10.0.22000.1	Microsoft Corpor
amdsata.sys	FFFFF800'6...	FFFFF800'6...	0x0001f000	1	67	System Driver	AHCI 1.3 Device Driver	1.1.3.277	Advanced Micro
amdsbs.sys	FFFFF800'6...	FFFFF800'6...	0x00067000	1	69	System Driver	AMD Technology AHCI Compatible C...	3.7.1540.43	AMD Technologi
amdxata.sys	FFFFF800'6...	FFFFF800'6...	0x0000c000	1	68	System Driver	Storage Filter Driver	1.1.3.277	Advanced Micro
AppleSSD.sys	FFFFF800'6...	FFFFF800'6...	0x00023000	1	65	Unknown	Apple Solid State Drive Device	6.1.7800.1	Apple Inc.
arcsas.sys	FFFFF800'6...	FFFFF800'6...	0x00025000	1	70	System Driver	Adaptec SAS RAID WS03 Driver	7.5.0.32048	PMC-Sierra, Inc.
atapi.sys	FFFFF800'6...	FFFFF800'6...	0x0000d000	1	89	System Driver	ATAPI IDE Miniport Driver	10.0.22000.258	Microsoft Corpor
ataport.SYS	FFFFF800'6...	FFFFF800'6...	0x0003c000	1	90	System Driver	ATAPI Driver Extension	10.0.22000.258	Microsoft Corpor
bam.sys	FFFFF800'6...	FFFFF800'6...	0x00018000	1	166	System Driver	BAM Kernel Driver	10.0.22000.1	Microsoft Corpor
BasicDisplay.sys	FFFFF800'6...	FFFFF800'6...	0x00015000	1	142	Display Driver	Microsoft Basic Display Driver	10.0.22000.1	Microsoft Corpor
BasicRender.sys	FFFFF800'6...	FFFFF800'6...	0x00011000	1	143	Display Driver	Microsoft Basic Render Driver	10.0.22000.1	Microsoft Corpor
Beep.SYS	FFFFF800'6...	FFFFF800'6...	0x0000a000	1	139	System Driver	BEEP Driver	10.0.22000.1	Microsoft Corpor
bindflt.sys	FFFFF800'6...	FFFFF800'6...	0x0002a000	1	208	System Driver	Windows Bind Filter Driver	10.0.22000.434	Microsoft Corpor
BOOTVID.dll	FFFFF800'6...	FFFFF800'6...	0x0000b000	1	7	Display Driver	VGA Boot Driver	10.0.22000.1	Microsoft Corpor
bowser.sys	FFFFF800'6...	FFFFF800'6...	0x00027000	1	200	System Driver	NT Lan Manager Datagram Receiver ...	10.0.22000.348	Microsoft Corpor
bttflt.sys	FFFFF800'6...	FFFFF800'6...	0x00010000	1	116	System Driver	VHD BTT Filter Driver	10.0.22000.1	Microsoft Corpor
bxbnda.sys	FFFFF800'6...	FFFFF800'6...	0x00089000	1	59	Network Driver	QLogic Gigabit Ethernet VBD	7.12.31.105	QLogic Corporati
cdd.dll	FFFFFA3AD'...	FFFFFA3AD'...	0x00043000	1	195	Display Driver	Canonical Display Driver	10.0.22000.434	Microsoft Corpor
cdfs.sys	FFFFF800'6...	FFFFF800'6...	0x0001f000	1	223	System Driver	CD-ROM File System Driver	10.0.22000.1	Microsoft Corpor
cdrom.sys	FFFFF800'6...	FFFFF800'6...	0x00030000	1	135	System Driver	SCSI CD-ROM Driver	10.0.22000.1	Microsoft Corpor
CEA.sys	FFFFF800'6...	FFFFF800'6...	0x00017000	3	38	Dynamic Link Li...	Event Aggregation Kernel Mode Library	10.0.22000.1	Microsoft Corpor
cht4x64.sys	FFFFF800'6...	FFFFF800'6...	0x0005c000	1	87	System Driver	Chelsio iSCSI VMiniport Driver	6.11.4.100	Chelsio Commun
Cl.dll	FFFFF800'6...	FFFFF800'6...	0x000e4000	2	15	System Driver	Code Integrity Module	10.0.22000.469	Microsoft Corpor
CimFS.SYS	FFFFF800'6...	FFFFF800'6...	0x00025000	1	146	Dynamic Link Li...	CimFS driver	10.0.22000.469	Microsoft Corpor
CL ASCIIID CVS	FFFFF800'6...	FFFFF800'6...	0x00006000	2	41	System Driver	SCSI Client System Dll	10.0.22000.101	Microsoft Corpor

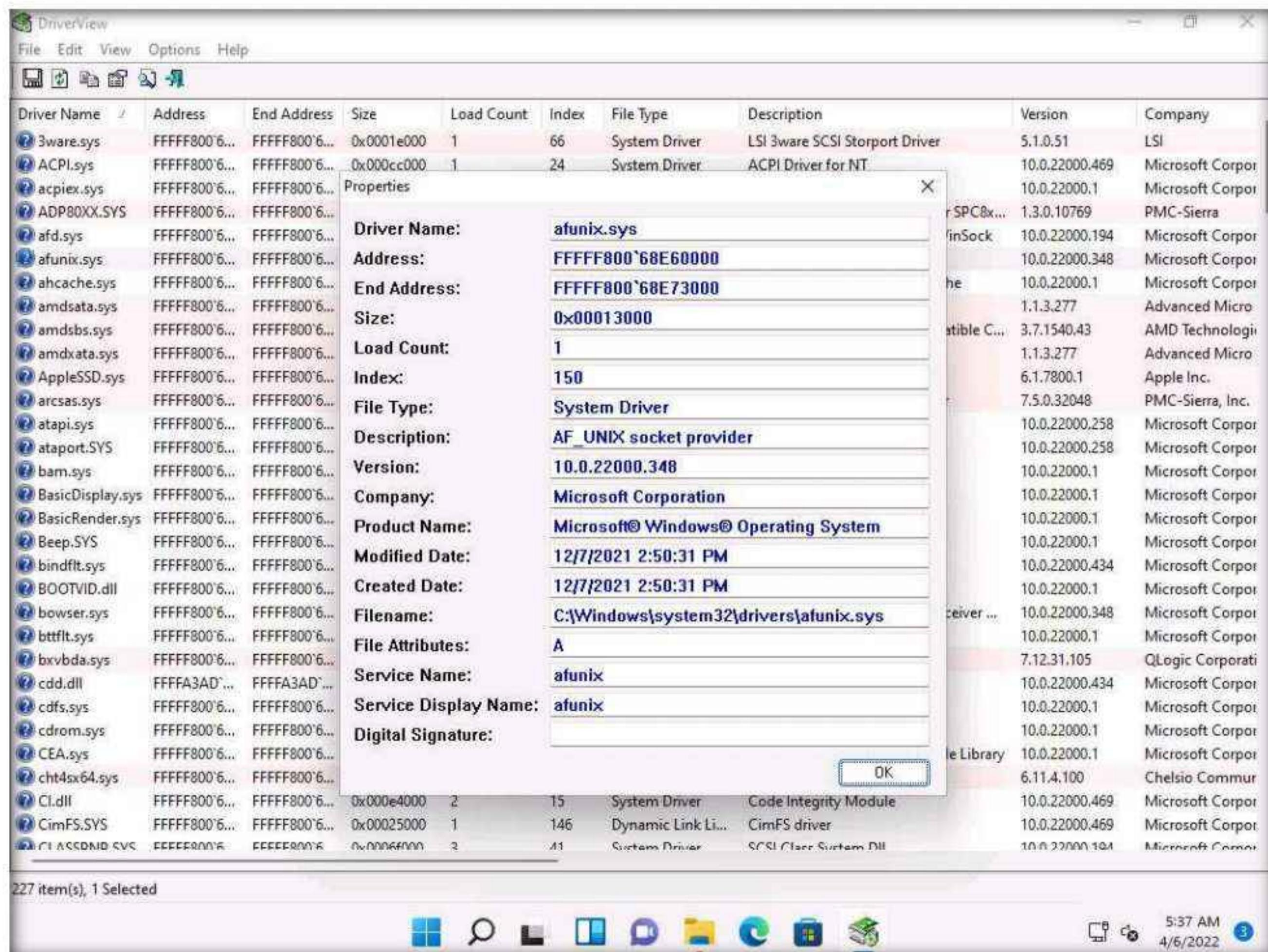
Module 07 – Malware Threats

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

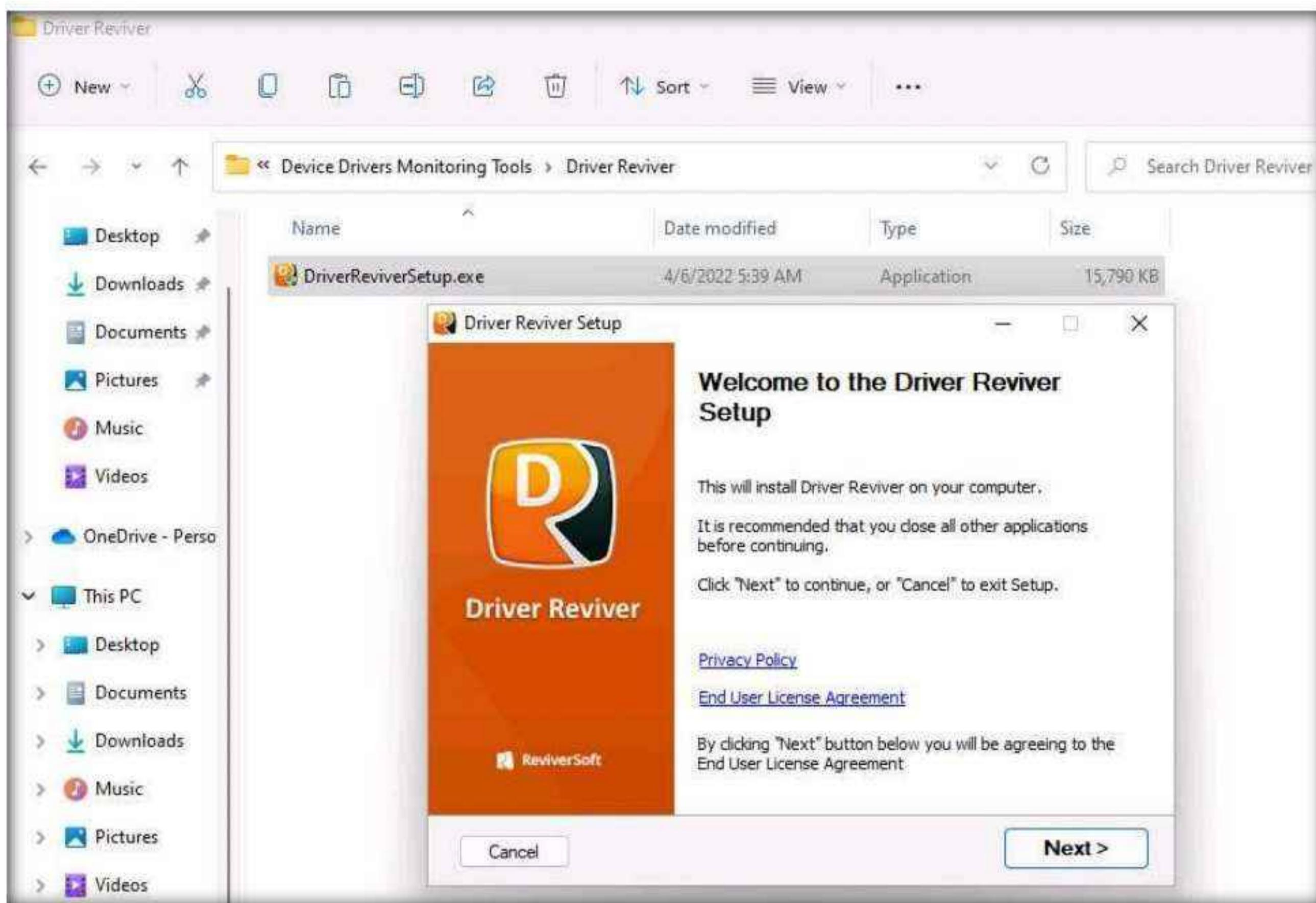


Driver Name	Address	End Address	Size	Load Count	Index	File Type	Description	Version	Company
3ware.sys	FFFFF800'6...	FFFFF800'6...	0x0001e000	1	66	System Driver	LSI 3ware SCSI Storport Driver	5.1.0.51	LSI
ACPI.sys	FFFFF800'6...	FFFFF800'6...	0x000cc000	1	24	System Driver	ACPI Driver for NT	10.0.22000.469	Microsoft Corpor
acpiex.sys	FFFFF800'6...	FFFFF800'6...	0x00026000	1	20	Dynamic Link Li...	ACPIEx Driver	10.0.22000.1	Microsoft Corpor
ADP80XX.SYS	FFFFF800'6...	FFFFF800'6...	0x0025c000	1	93	System Driver	PMC-Sierra Storport Driver For SPC8x...	1.3.0.10769	PMC-Sierra
afd.sys	FFFFF800'6...	FFFFF800'6...	0x000a4000	1	151	System Driver	Ancillary Function Driver for WinSock	10.0.22000.194	Microsoft Corpor
afunix.sys	Save Selected Items Ctrl+S			150	System Driver	AF_UNIX socket provider	10.0.22000.348	Microsoft Corpor	
ahcache.sys	Copy Selected Items Ctrl+C			167	System Driver	Application Compatibility Cache	10.0.22000.1	Microsoft Corpor	
amdsata.sys	HTML Report - All Items			67	System Driver	AHCI 1.3 Device Driver	1.1.3.277	Advanced Micro	
amdsbs.sys	HTML Report - Selected Items			69	System Driver	AMD Technology AHCI Compatible C...	3.7.1540.43	AMD Technologi	
amdxata.sys				68	System Driver	Storage Filter Driver	1.1.3.277	Advanced Micro	
AppleSSD.sys				65	Unknown	Apple Solid State Drive Device	6.1.7800.1	Apple Inc.	
arcsas.sys				70	System Driver	Adaptec SAS RAID WS03 Driver	7.5.0.32048	PMC-Sierra, Inc.	
atapi.sys				89	System Driver	ATAPI IDE Miniport Driver	10.0.22000.258	Microsoft Corpor	
ataport.SYS				90	System Driver	ATAPI Driver Extension	10.0.22000.258	Microsoft Corpor	
bam.sys				166	System Driver	BAM Kernel Driver	10.0.22000.1	Microsoft Corpor	
BasicDisplay.sys	File Properties F8			142	Display Driver	Microsoft Basic Display Driver	10.0.22000.1	Microsoft Corpor	
BasicRender.sys	Properties Alt+Enter			143	Display Driver	Microsoft Basic Render Driver	10.0.22000.1	Microsoft Corpor	
Beep.SYS	Google Search			139	System Driver	BEEP Driver	10.0.22000.1	Microsoft Corpor	
bindflt.sys	Refresh F5			208	System Driver	Windows Bind Filter Driver	10.0.22000.434	Microsoft Corpor	
BOOTVID.dll	FFFFF800'6...	FFFFF800'6...	0x0000b000	1	7	Display Driver	VGA Boot Driver	10.0.22000.1	Microsoft Corpor
bowser.sys	FFFFF800'6...	FFFFF800'6...	0x00027000	1	200	System Driver	NT Lan Manager Datagram Receiver ...	10.0.22000.348	Microsoft Corpor

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.

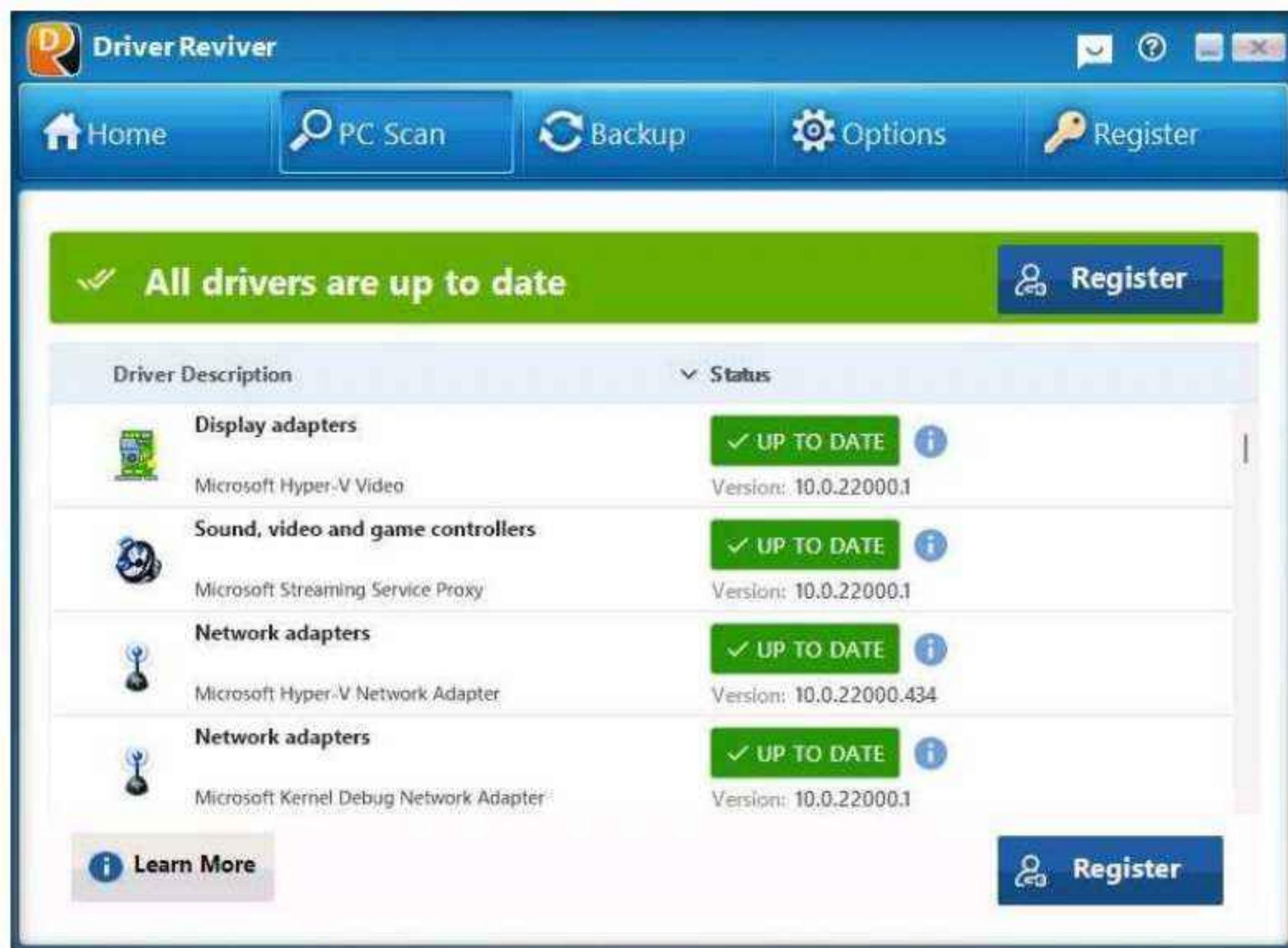
Note: If a browser window opens automatically close the browser.

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**, **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.

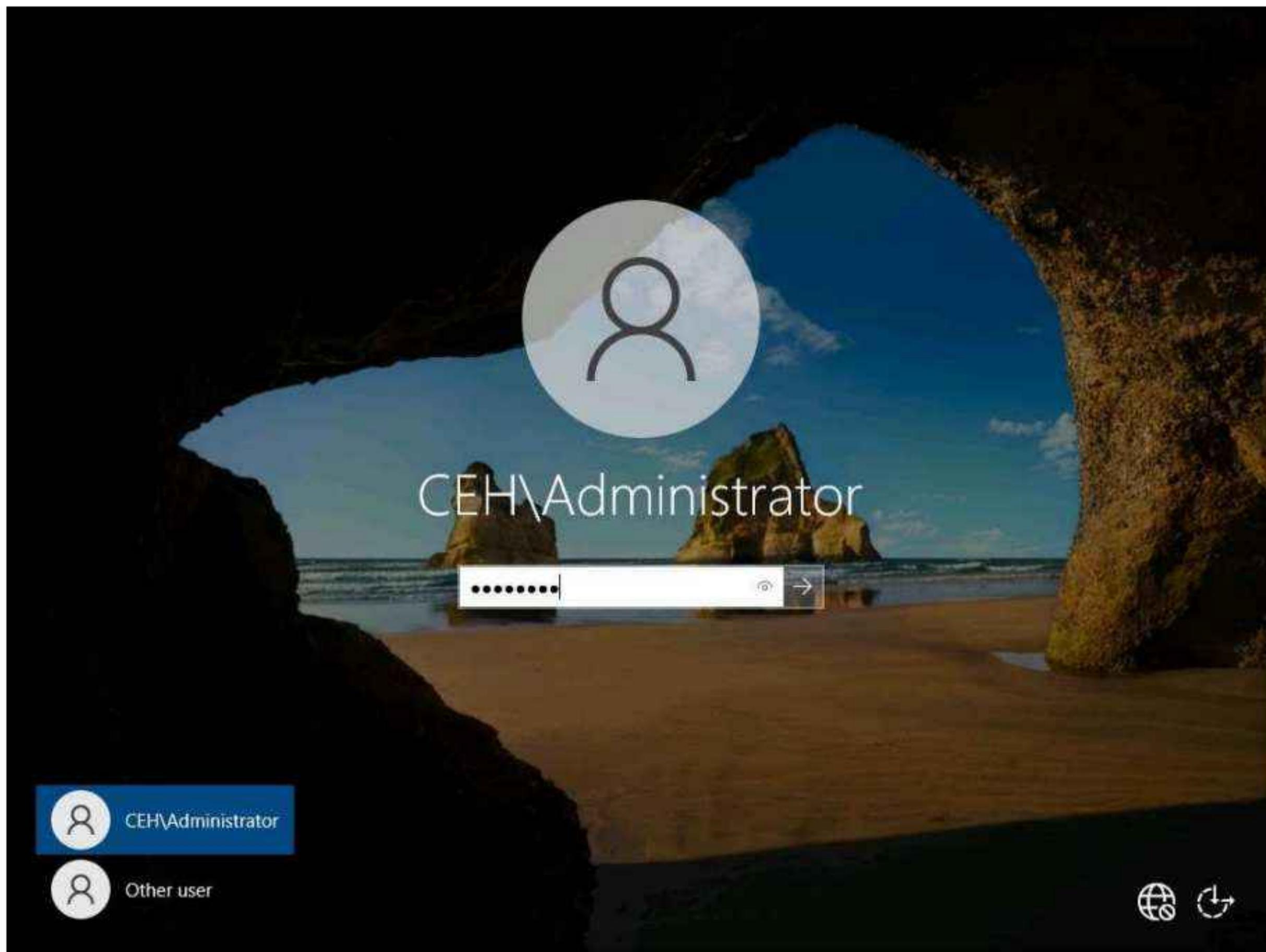
17. Close all open windows.

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

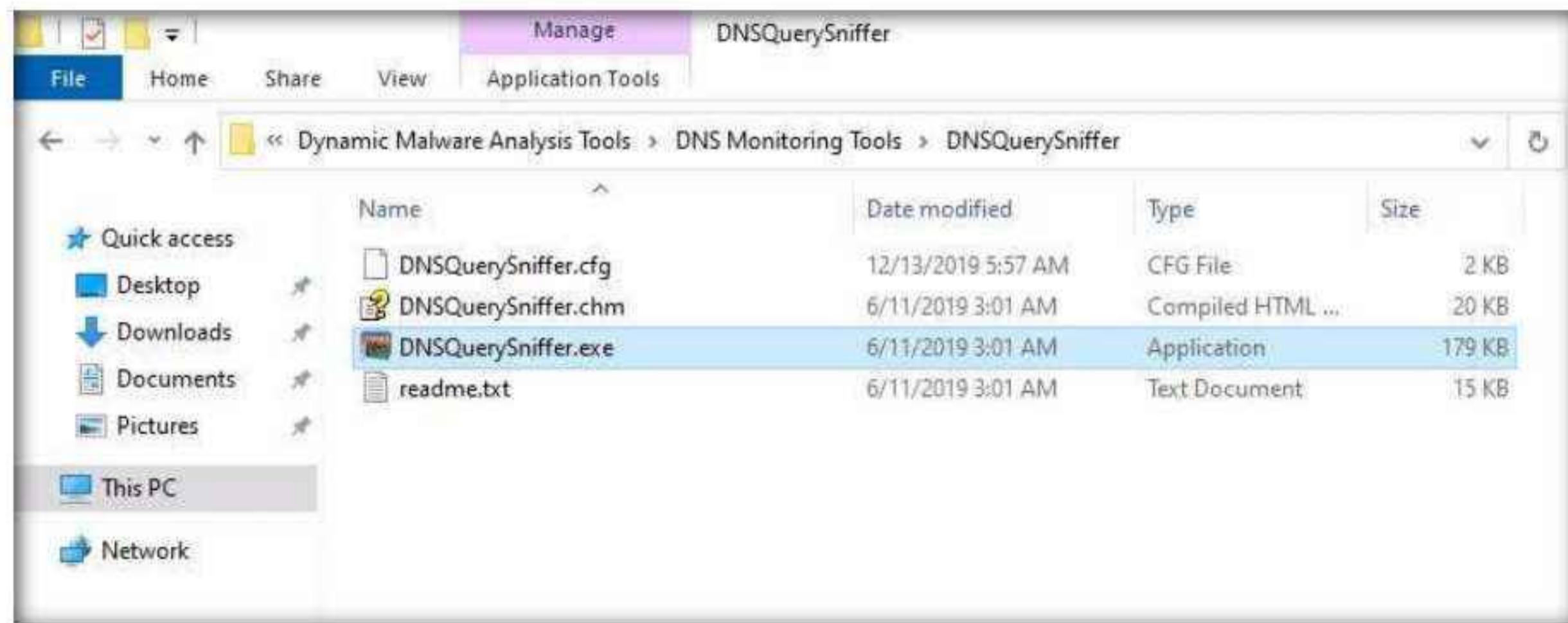
Task 9: Perform DNS Monitoring using DNSQuerySniffer

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.



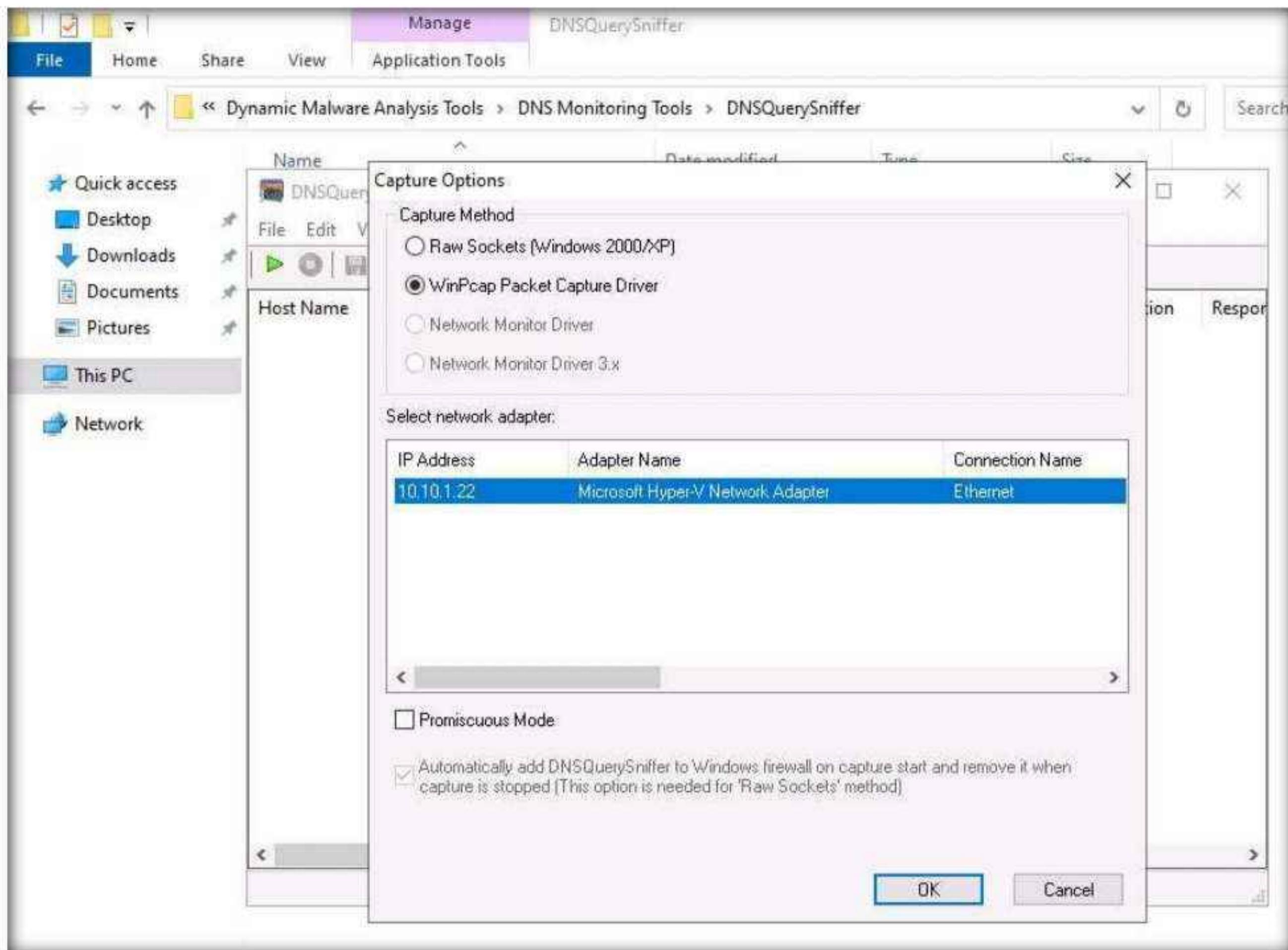
3. The main window of DNSQuerySniffer appears, along with the Capture Options window.

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.

Module 07 – Malware Threats

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.

Module 07 – Malware Threats

The screenshot shows two windows of the DNSQuerySniffer application running on a Microsoft Hyper-V Network Adapter. Both windows display a table of DNS queries with the following columns: Host Name, Port Number, Query ID, Request Type, Request Time, Response Time, Duration, Response Co..., Records Count, A, and CNAME.

Top Window Data:

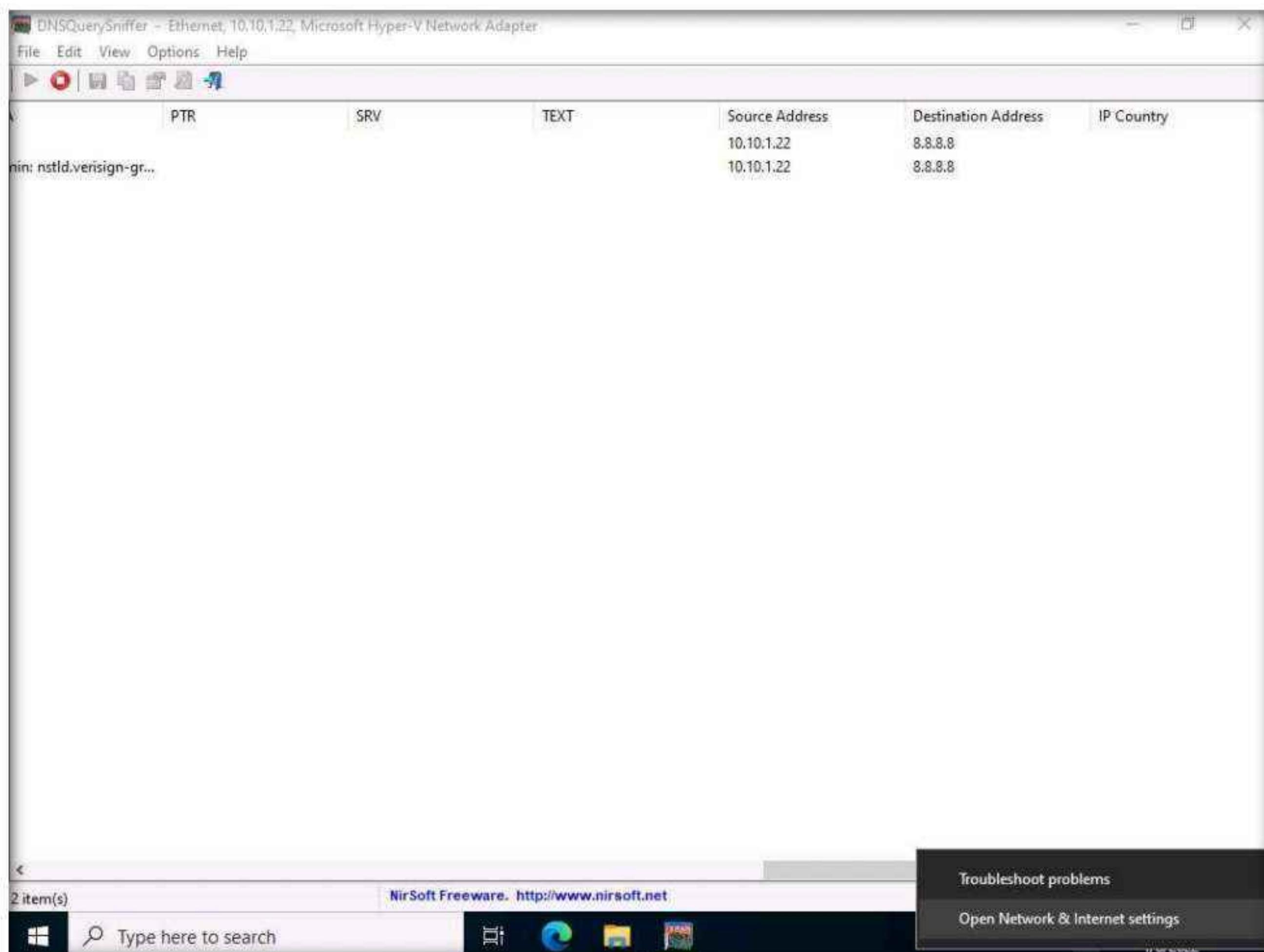
Host Name	Port Number	Query ID	Request Type	Request Time	Response Time	Duration	Response Co...	Records Count	A	CNAME
v10.events.dat...	65197	1D97	A	4/8/2022 4:47:...	4/8/2022 4:47:00 A...	9 ms	Ok	4	20.189.173.10	global.asimov.events
wpad.localdo...	49847	68EB	A	4/8/2022 4:50:...	4/8/2022 4:50:27 A...	31 ms	Name Error	7		

Bottom Window Data:

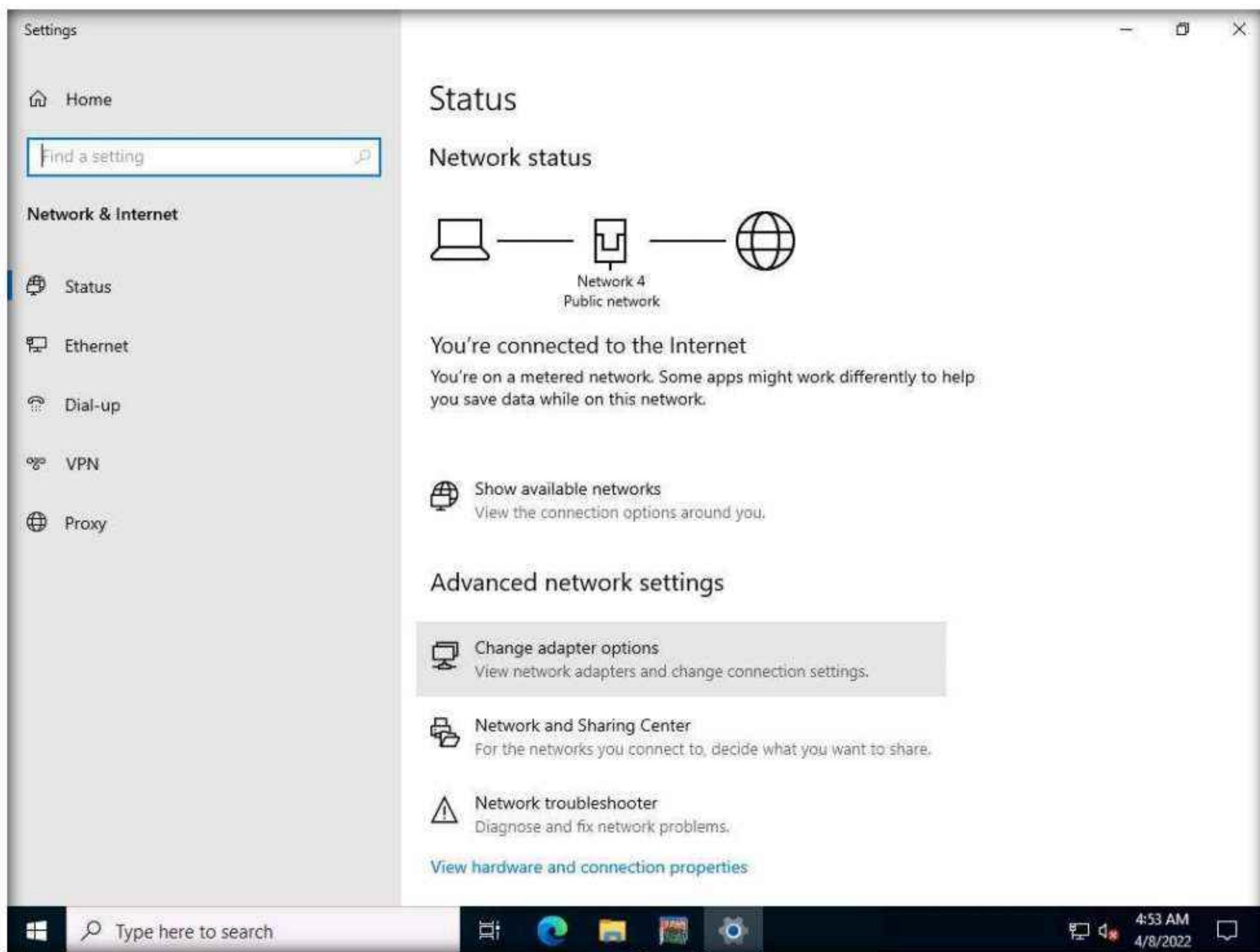
PTR	SRV	TEXT	Source Address	Destination Address	IP Country
nin: ns1d.verisign-gr...			10.10.1.22	8.8.8.8	
			10.10.1.22	8.8.8.8	

Module 07 – Malware Threats

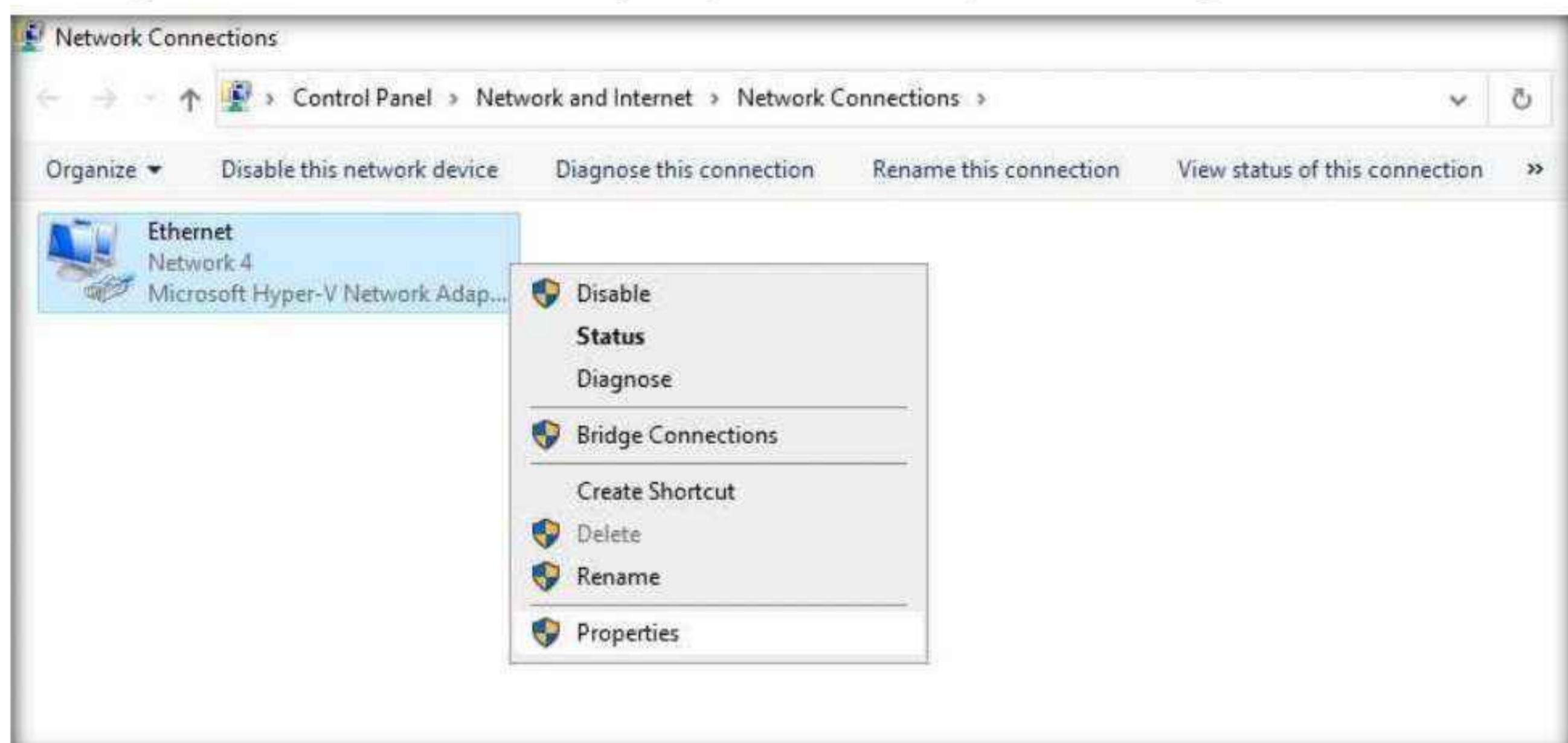
8. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
9. In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine. For demonstration purposes, we are changing the DNS of the **Windows Server 2022** machine in the **Network &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



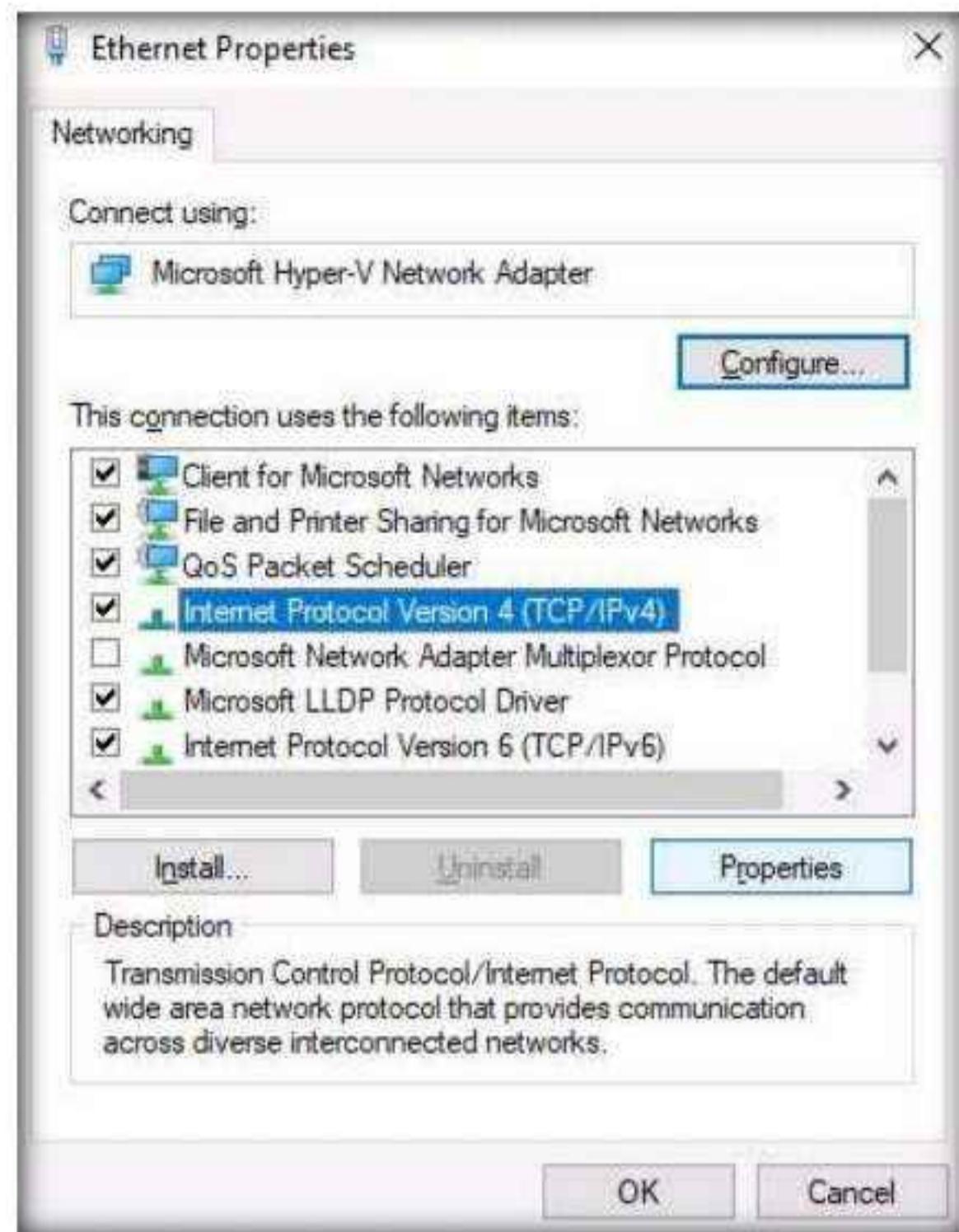
11. The Network Status window appears. Click **Change adapter options** under **Change your network settings**.



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

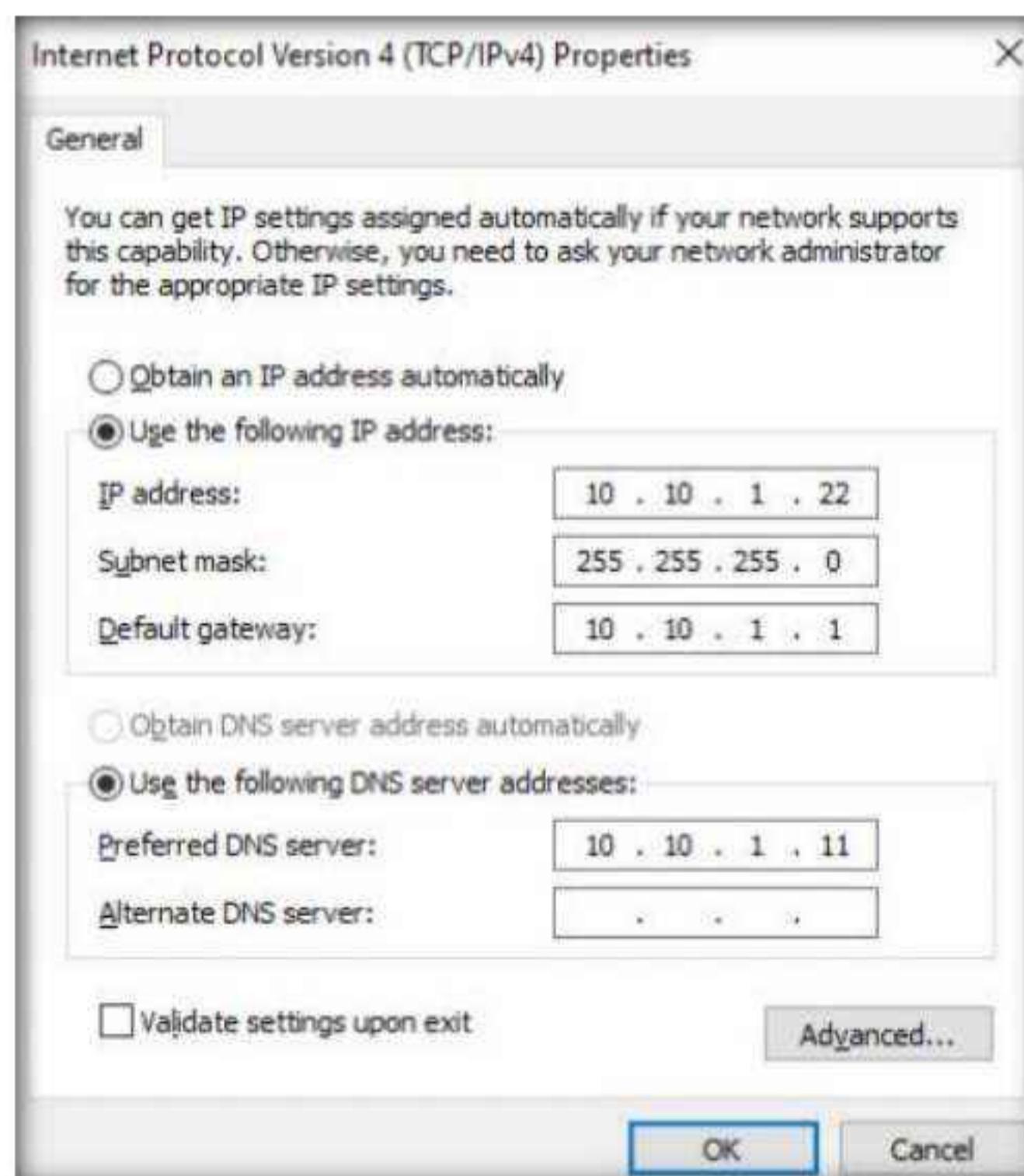


13. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



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**.

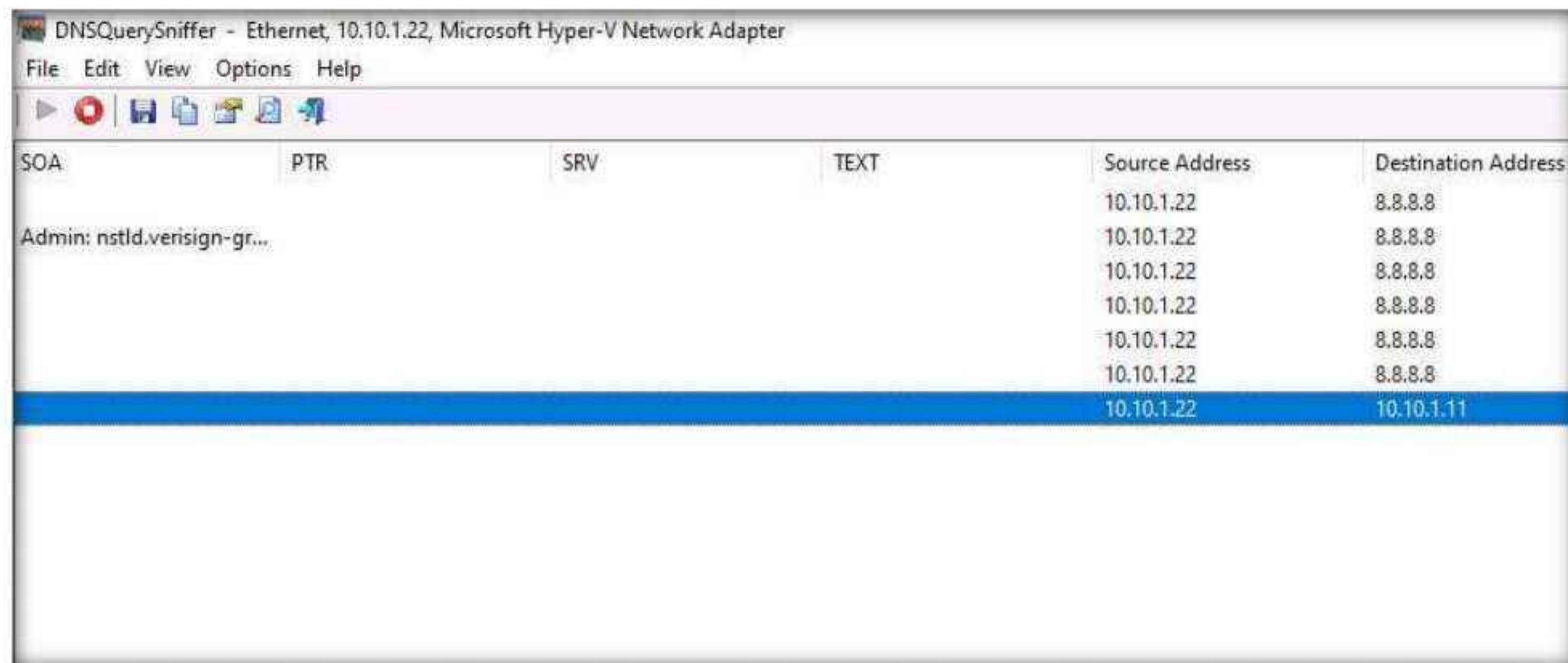
15. Click **OK**, and then **Close** the Adapter Properties window.



Module 07 – Malware Threats

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

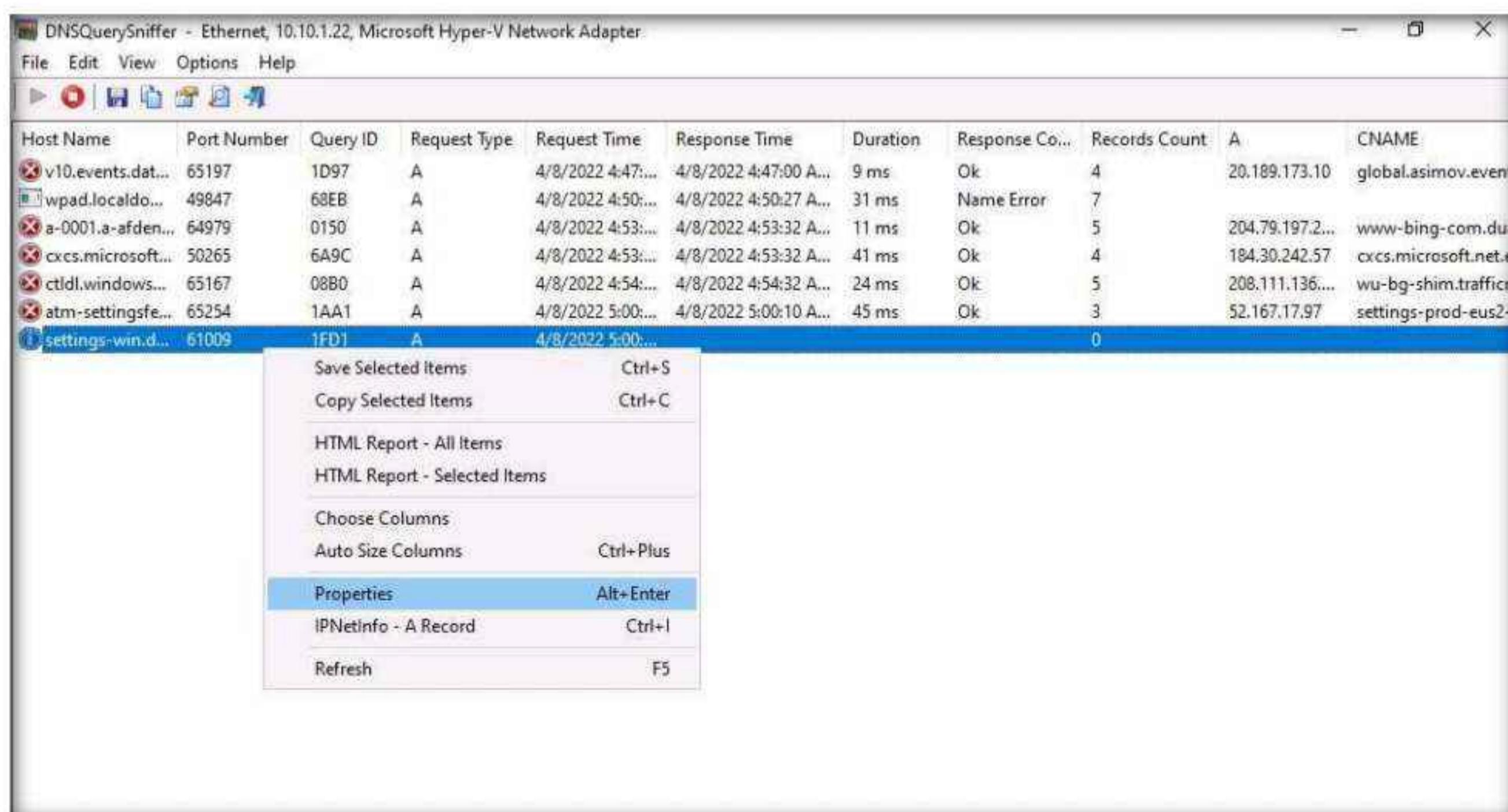
Note: Wait for approximately 10 minutes to capture the logs.



The screenshot shows the DNSQuerySniffer interface with a list of captured DNS logs. The columns are labeled SOA, PTR, SRV, TEXT, Source Address, and Destination Address. The logs show various DNS queries and responses, with the last entry being highlighted in blue.

SOA	PTR	SRV	TEXT	Source Address	Destination Address
				10.10.1.22	8.8.8.8
Admin: ns1ld.verisign-gr...				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	10.10.1.11

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

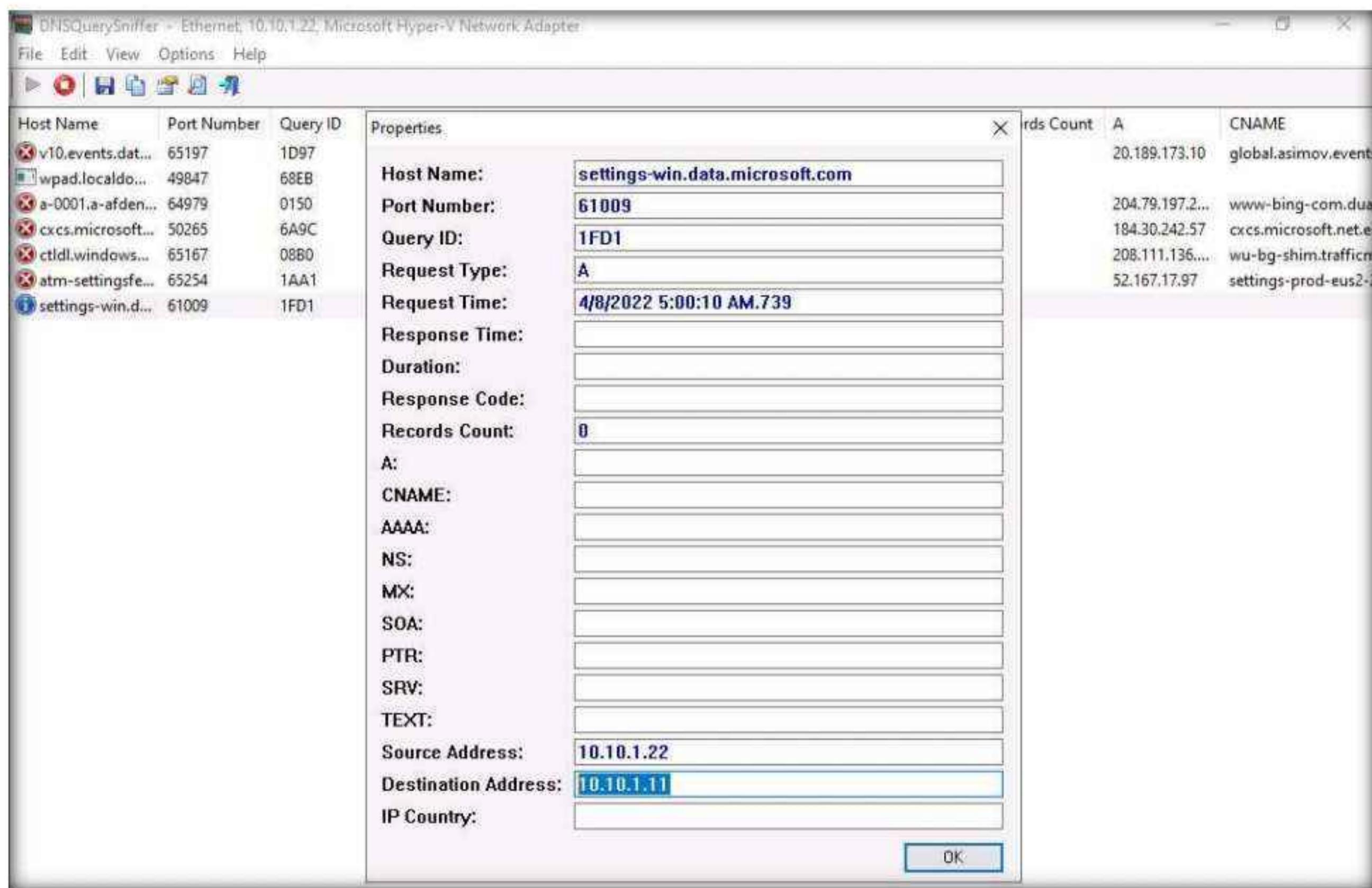


The screenshot shows the DNSQuerySniffer interface with a context menu open over a specific log entry. The menu options include Save Selected Items (Ctrl+S), Copy Selected Items (Ctrl+C), HTML Report - All Items, HTML Report - Selected Items, Choose Columns, Auto Size Columns (Ctrl+Plus), Properties (Alt+Enter), IPNetInfo - A Record (Ctrl+I), and Refresh (F5). The 'Properties' option is highlighted in blue.

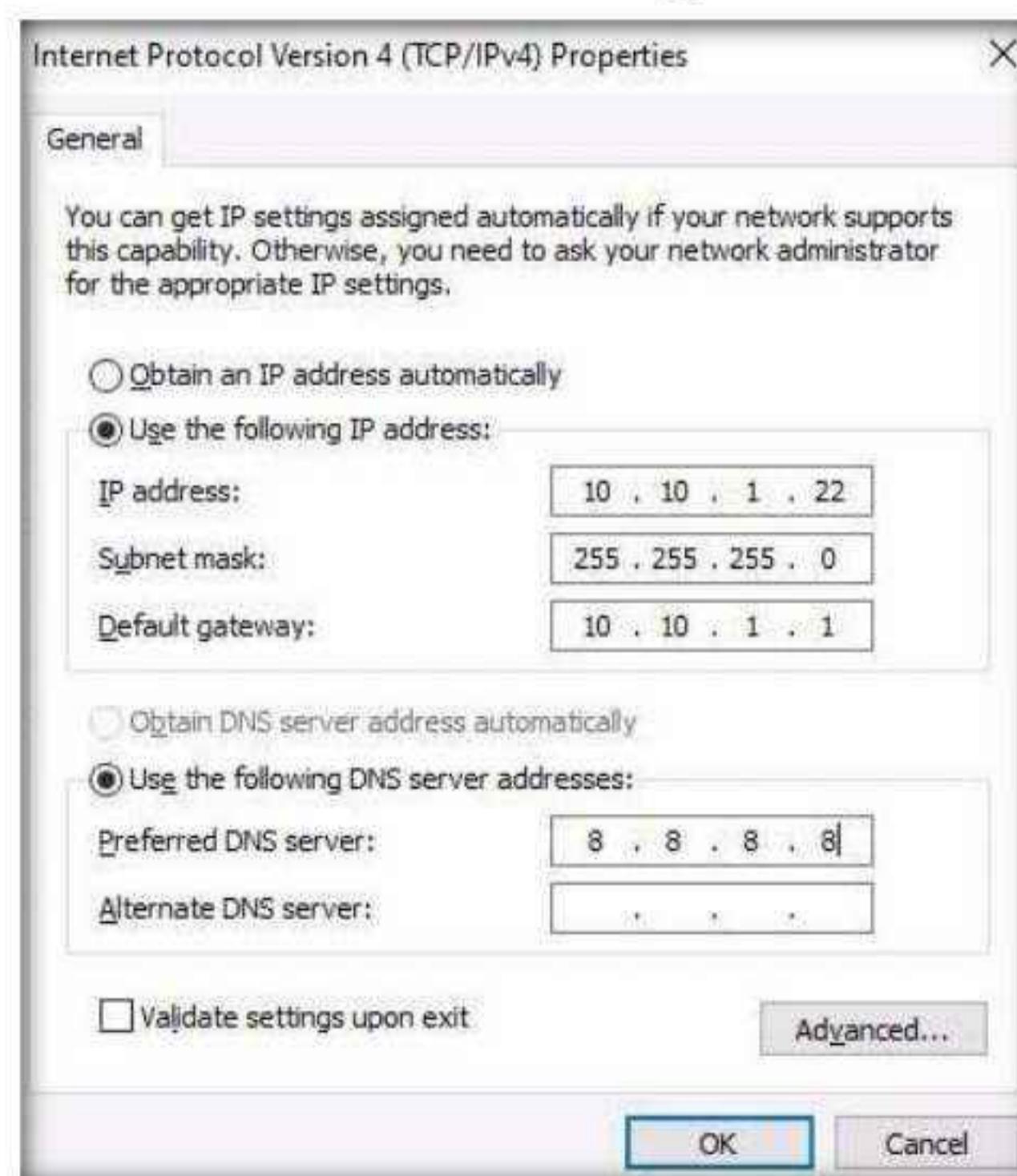
Save Selected Items	Ctrl+S
Copy Selected Items	Ctrl+C
HTML Report - All Items	
HTML Report - Selected Items	
Choose Columns	
Auto Size Columns	Ctrl+Plus
Properties	Alt+Enter
IPNetInfo - A Record	Ctrl+I
Refresh	F5

Module 07 – Malware Threats

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	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> CyberQ

CEH Lab Manual

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		✓	✓

Module 08 – Sniffing

	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 Omnipacket 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

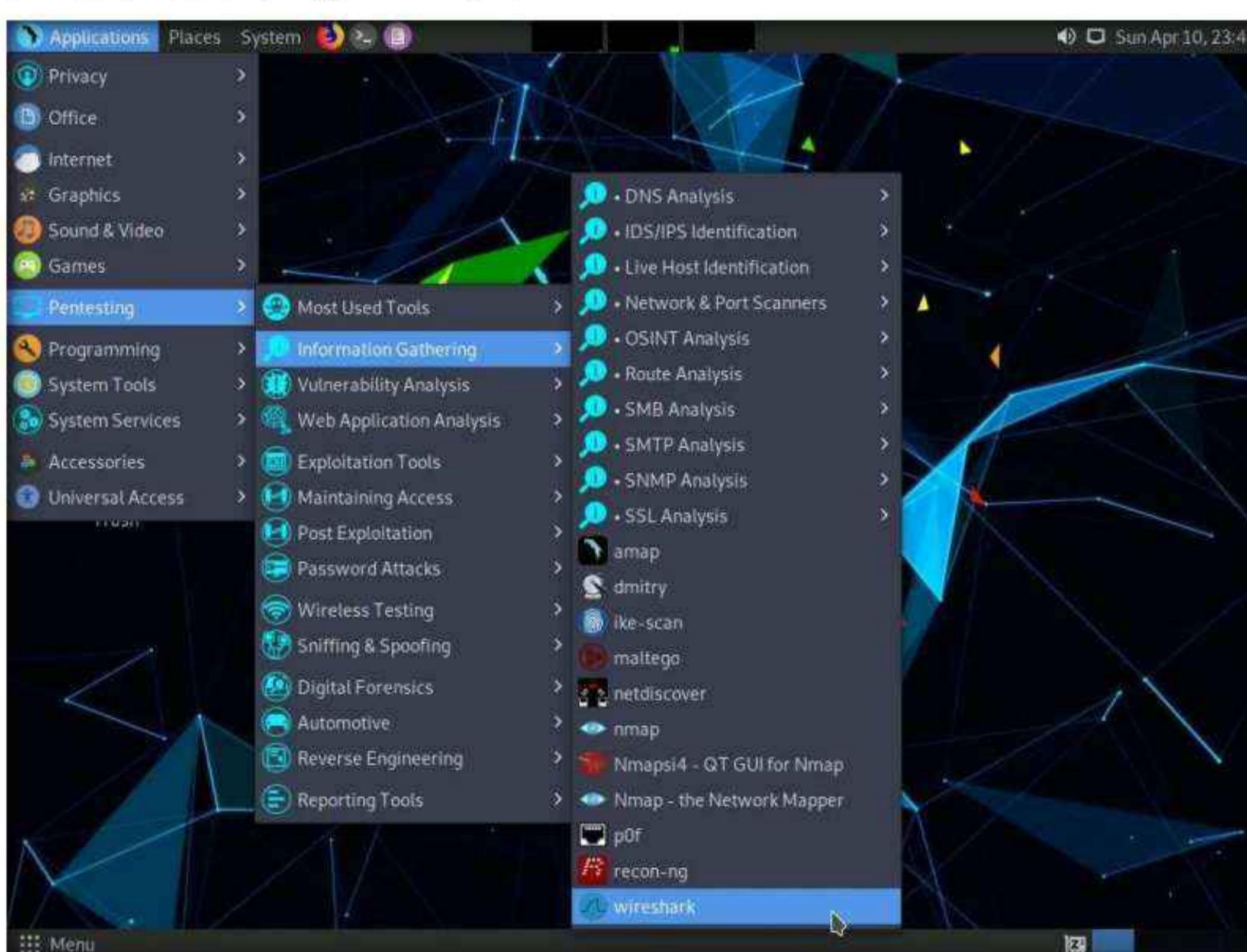
the packets with random MAC addresses and IP addresses to all active machines in the local network.

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**.

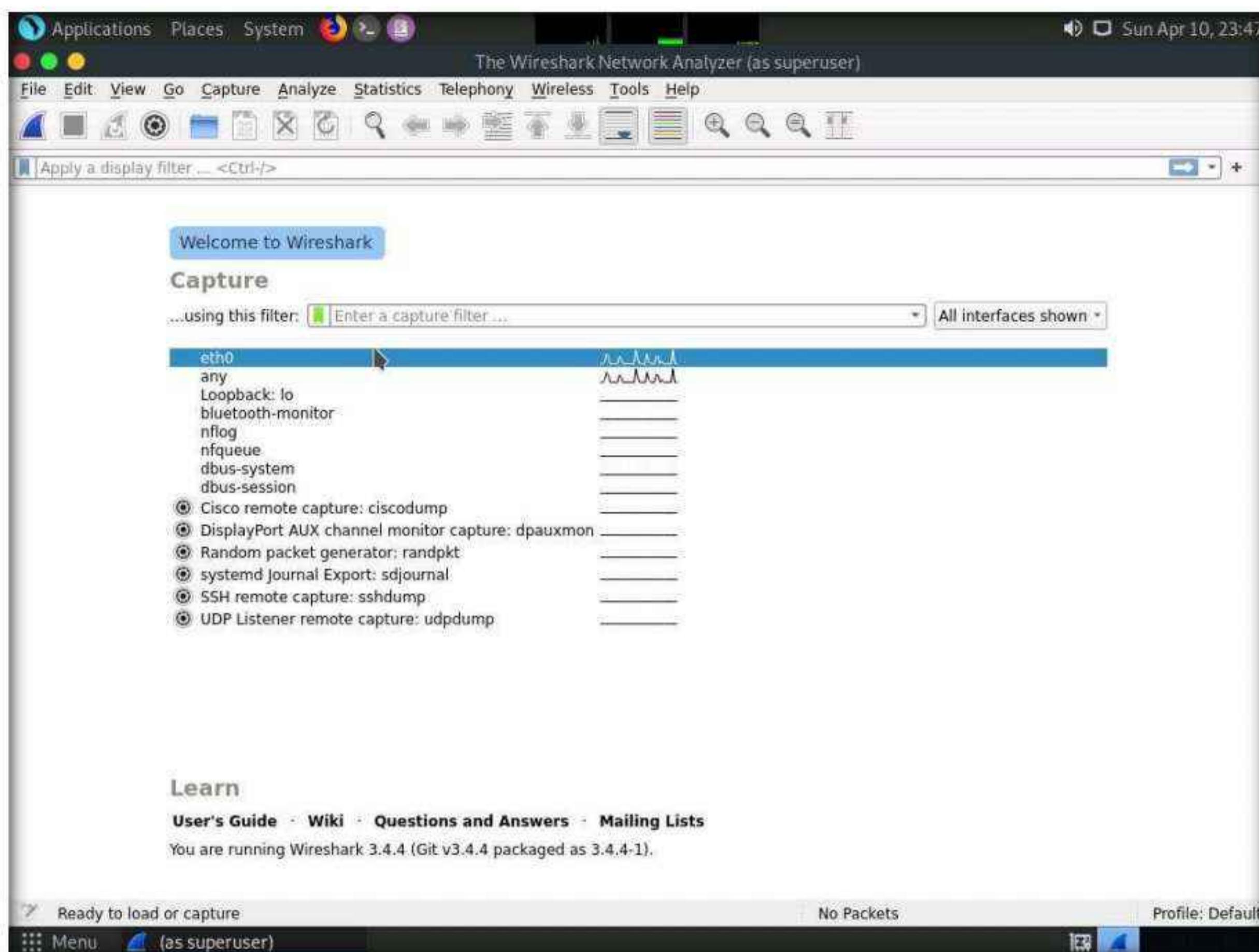


4. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



Module 08 – Sniffing

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.

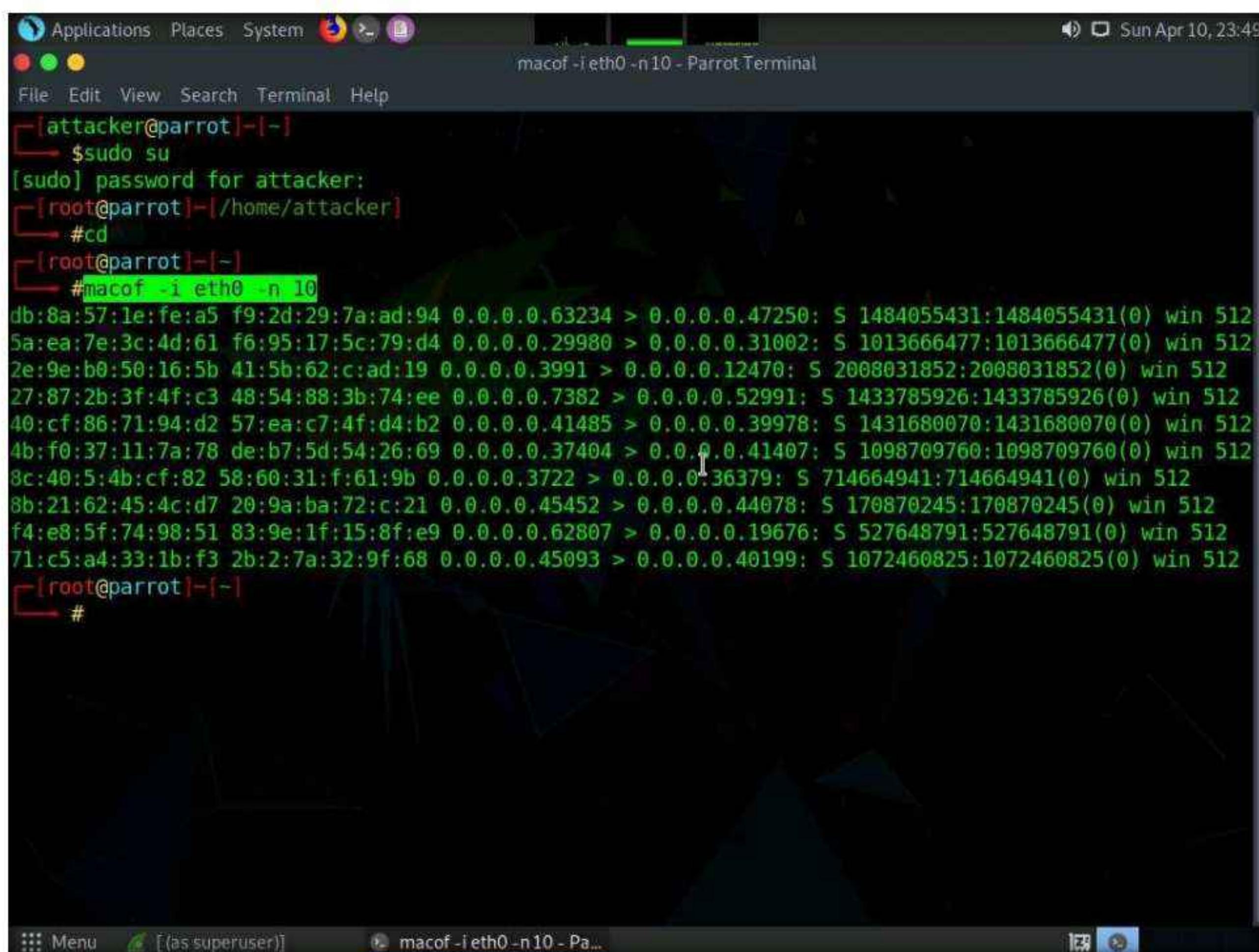
```
cd - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ 
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd
[root@parrot]~#
```

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.

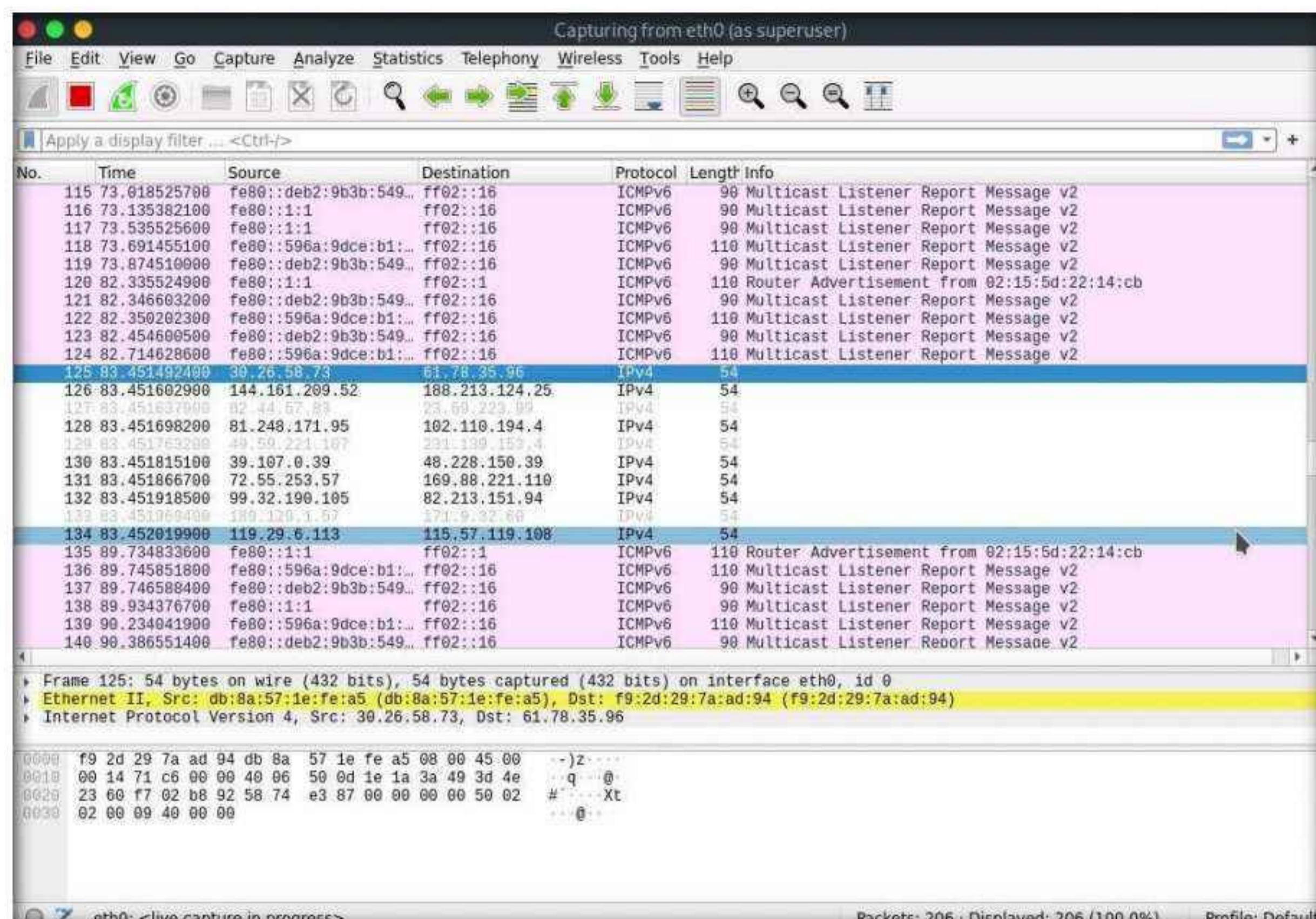


The screenshot shows a terminal window titled "macof -i eth0 -n 10 - Parrot Terminal". The terminal is running as root on a Parrot OS system. The user has entered the command "#macof -i eth0 -n 10" and is observing the output, which lists numerous MAC addresses being flooded into the CAM table. The terminal window is part of a desktop environment with a dark theme.

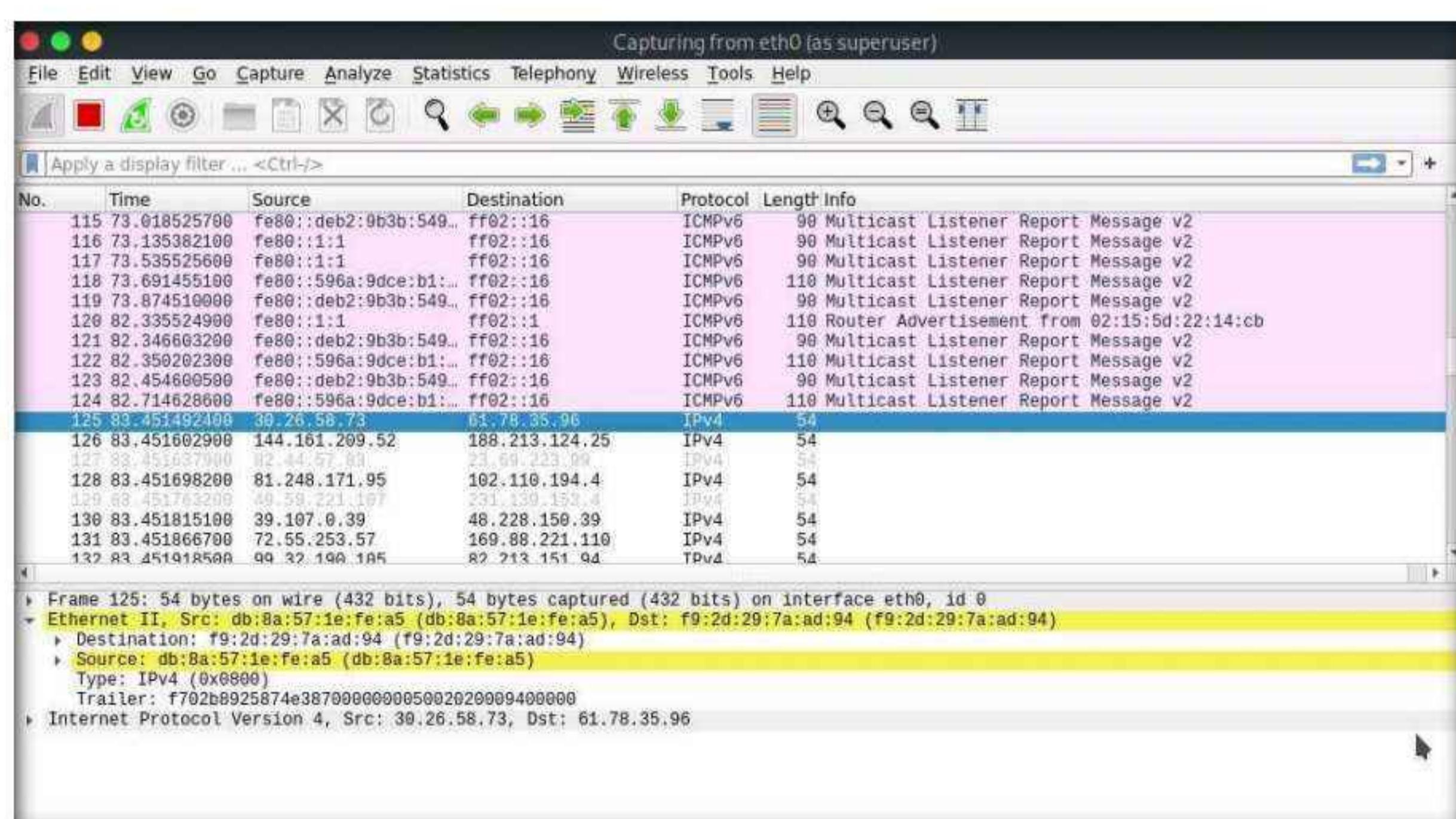
```
[attacker@parrot]~[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#macof -i eth0 -n 10
db:8a:57:1e:fe:a5 f9:2d:29:7a:ad:94 0.0.0.0.63234 > 0.0.0.0.47250: S 1484055431:1484055431(0) win 512
5a:ea:7e:3c:4d:61 f6:95:17:5c:79:d4 0.0.0.0.29980 > 0.0.0.0.31002: S 1013666477:1013666477(0) win 512
2e:9e:b0:50:16:5b 41:5b:62:c:ad:19 0.0.0.0.3991 > 0.0.0.0.12470: S 2008031852:2008031852(0) win 512
27:87:2b:3f:4f:c3 48:54:88:3b:74:ee 0.0.0.0.7382 > 0.0.0.0.52991: S 1433785926:1433785926(0) win 512
40:cf:86:71:94:d2 57:ea:c7:4f:d4:b2 0.0.0.0.41485 > 0.0.0.0.39978: S 1431680070:1431680070(0) win 512
4b:f0:37:11:7a:78 de:b7:5d:54:26:69 0.0.0.0.37404 > 0.0.0.0.41407: S 1098709760:1098709760(0) win 512
8c:40:5:4b:cf:82 58:60:31:f:61:9b 0.0.0.0.3722 > 0.0.0.0.36379: S 714664941:714664941(0) win 512
6b:21:62:45:4c:d7 20:9a:ba:72:c:21 0.0.0.0.45452 > 0.0.0.0.44078: S 170870245:170870245(0) win 512
f4:e8:5f:74:98:51 83:9e:1f:15:8f:e9 0.0.0.0.62807 > 0.0.0.0.19676: S 527648791:527648791(0) win 512
71:c5:a4:33:1b:f3 2b:2:7a:32:9f:68 0.0.0.0.45093 > 0.0.0.0.40199: S 1072460825:1072460825(0) win 512
[root@parrot]~[~]
#
```

Module 08 – Sniffing

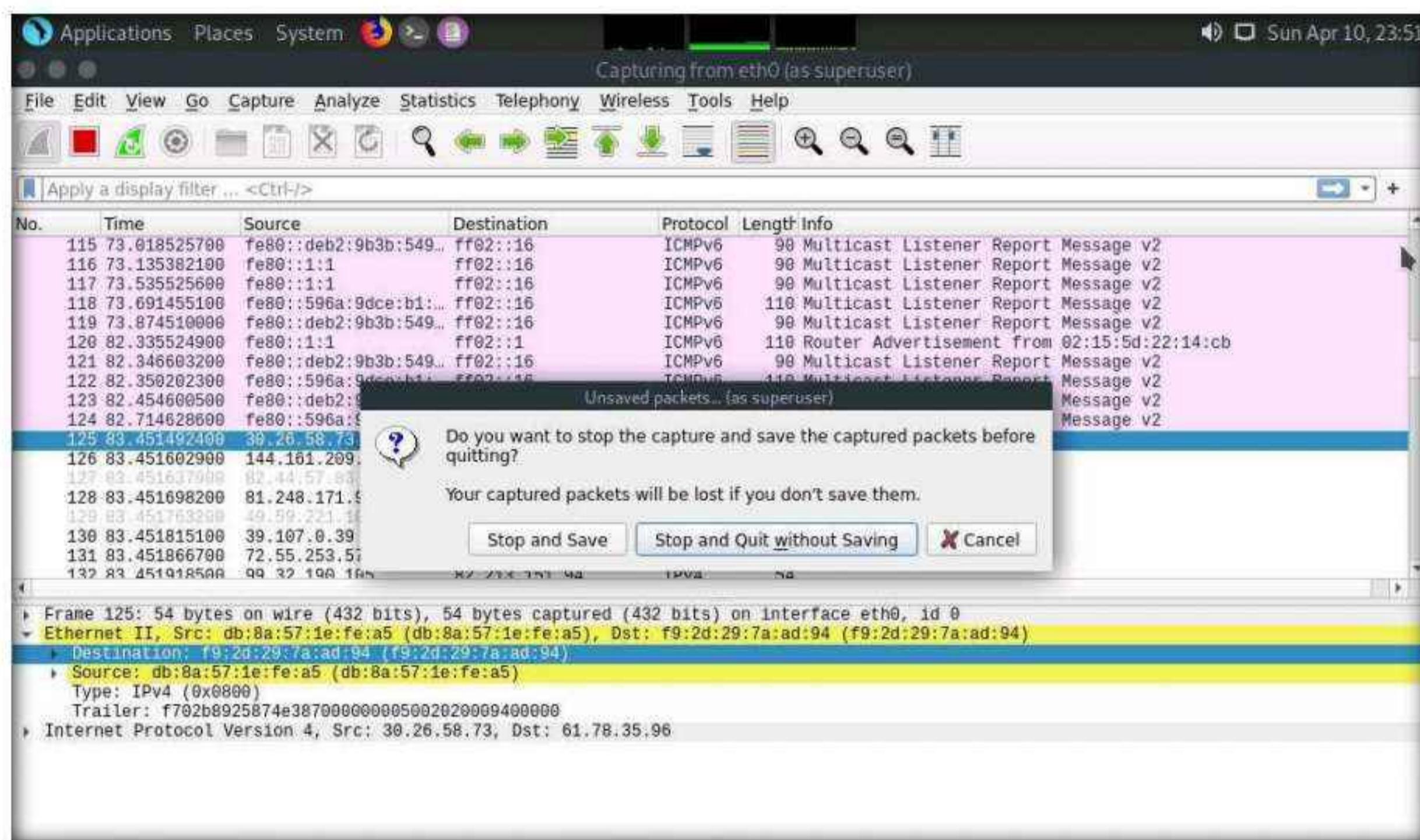
13. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.



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

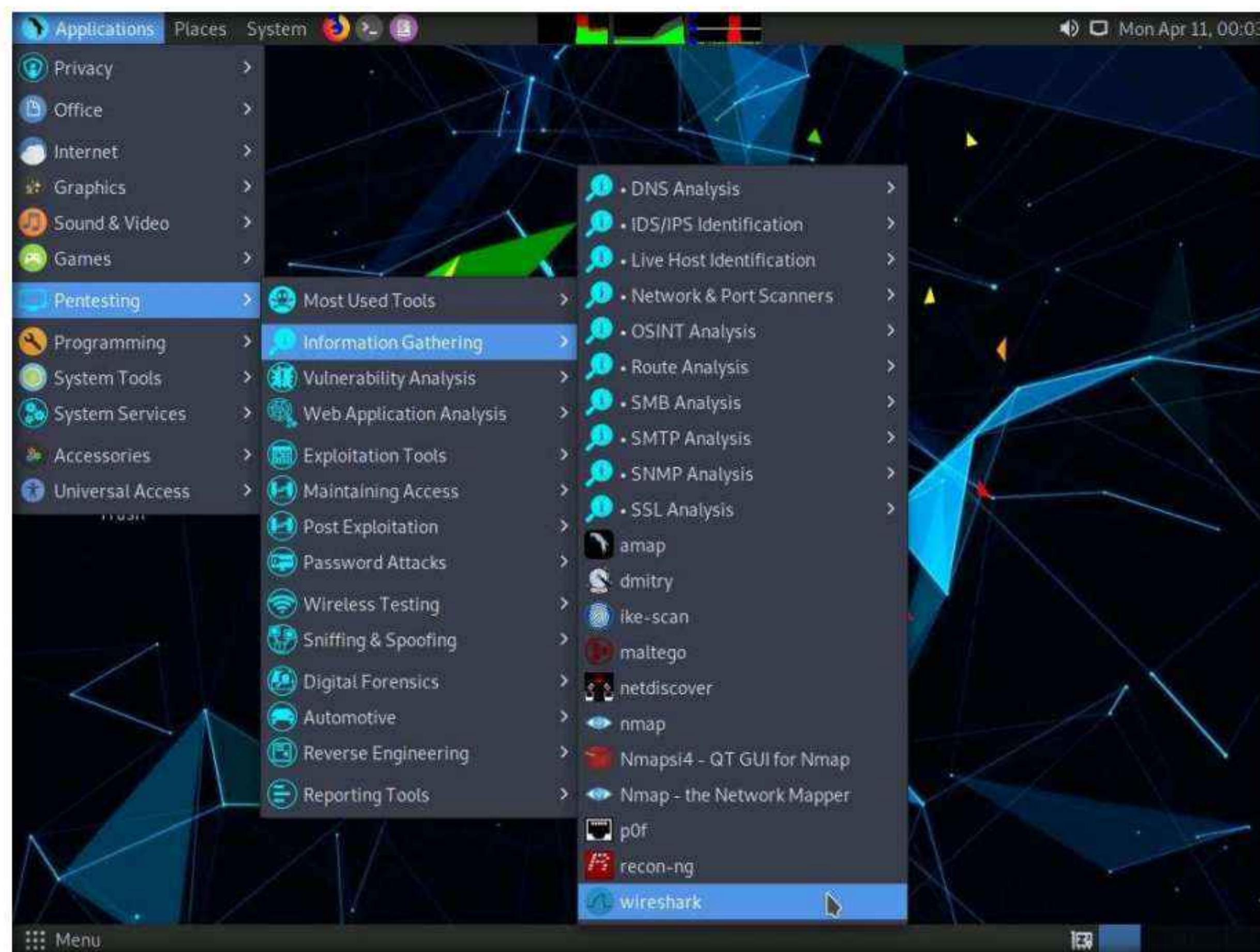
In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, 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.

Module 08 – Sniffing

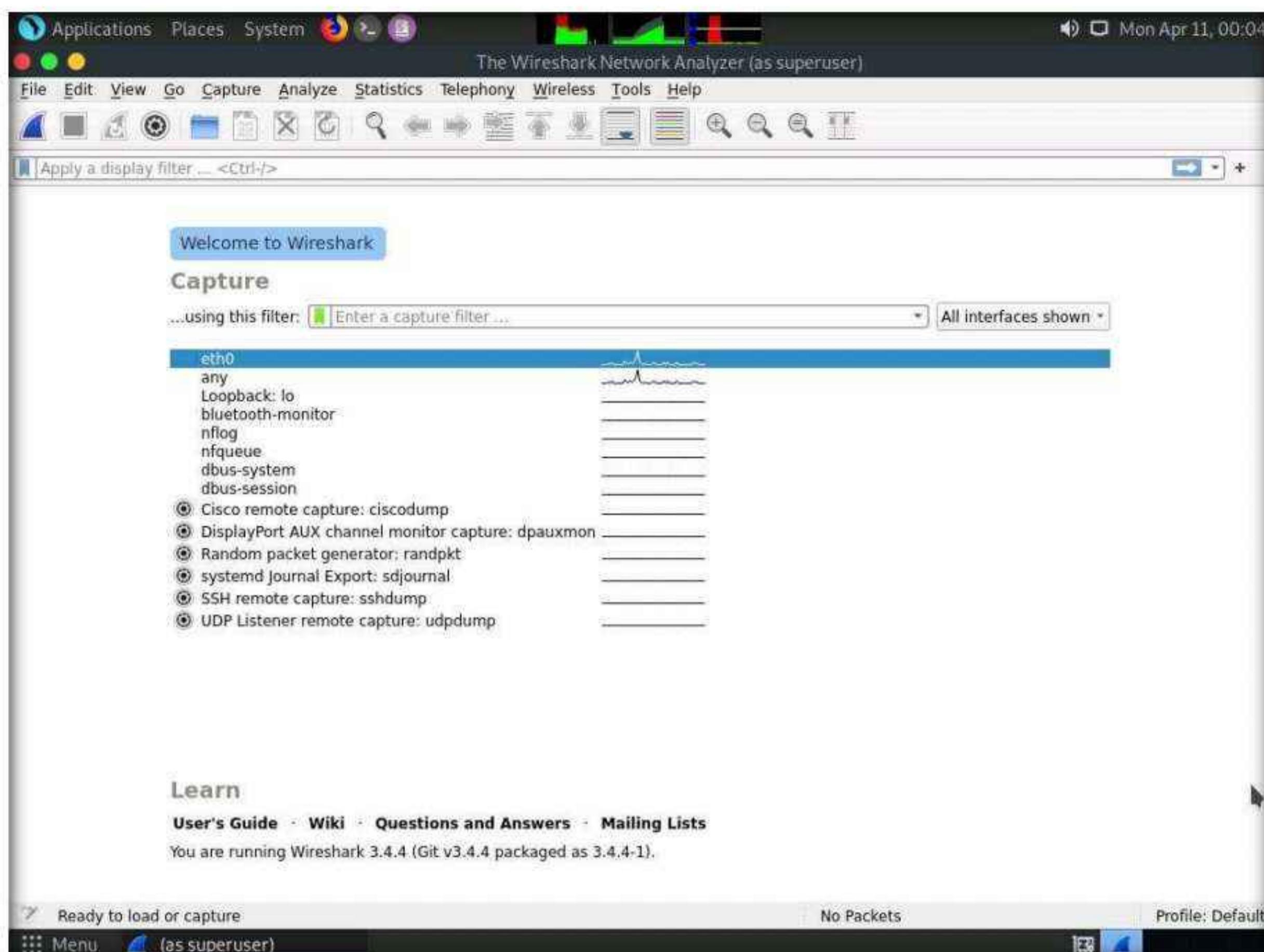
1. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



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

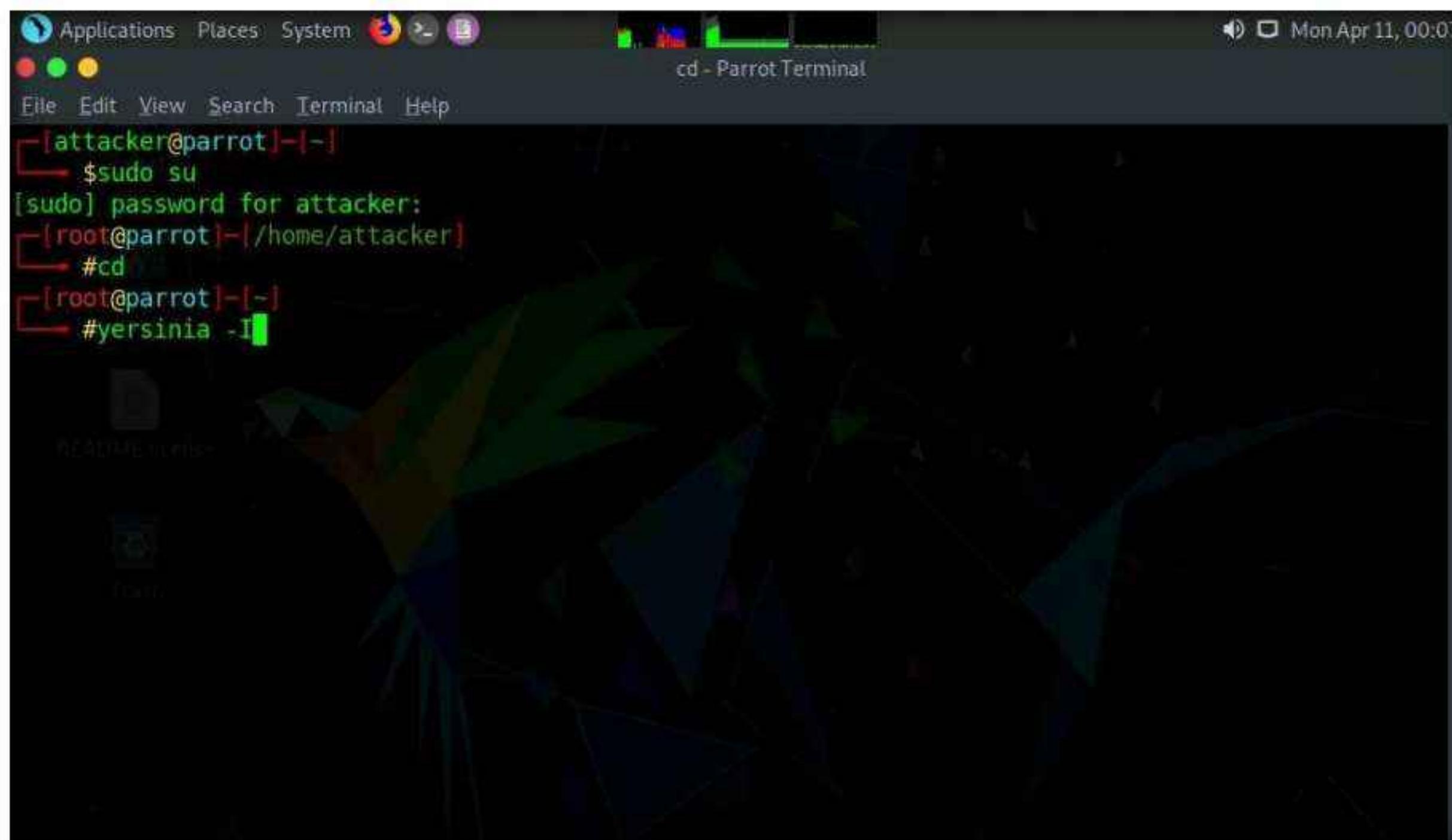


3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



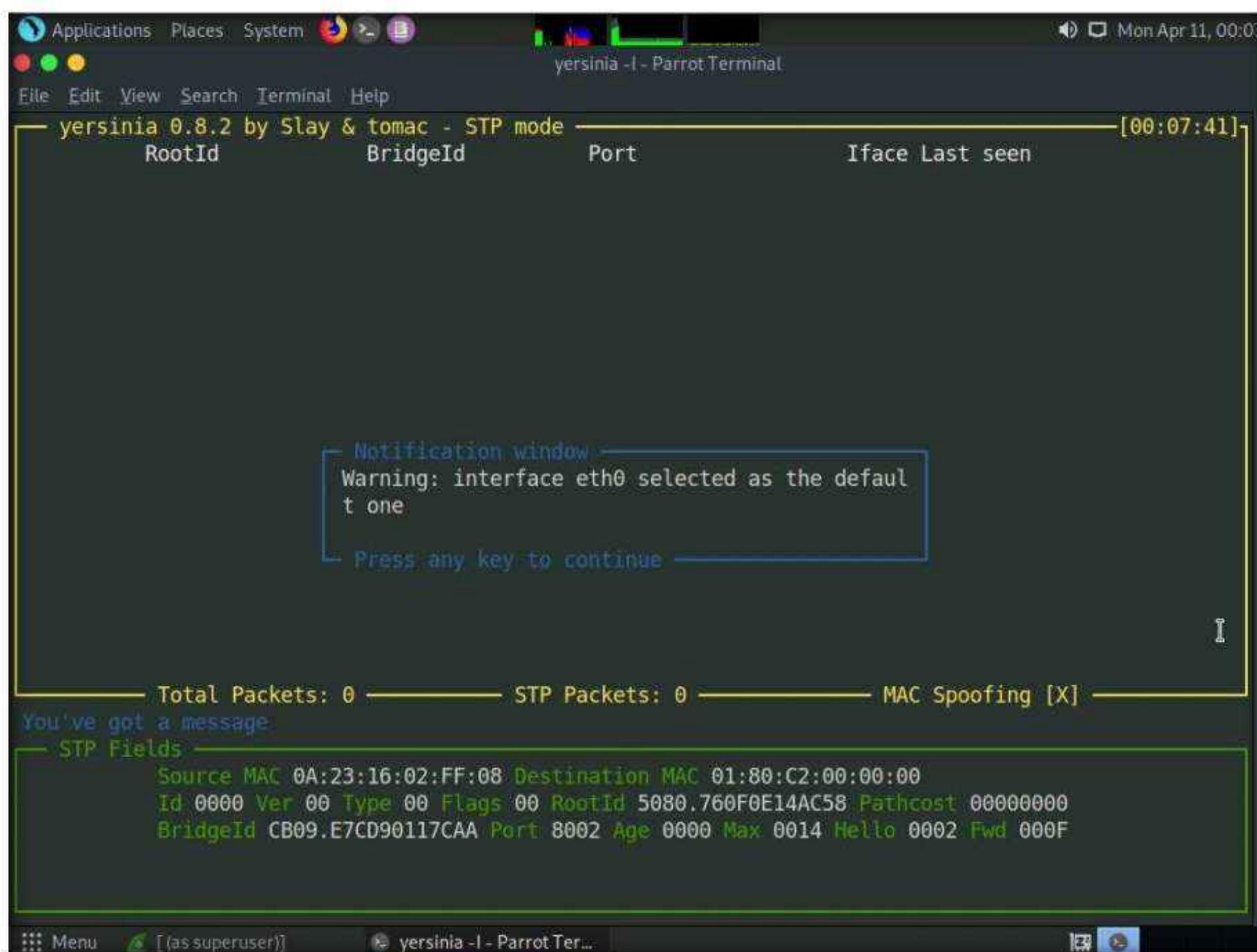
4. Leave the **Wireshark** application running.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo]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

Module 08 – Sniffing



```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# yersinia -I
```

10. Yersinia interactive mode appears in the terminal window.



```
yersinia 0.8.2 by Slay & tomac - STP mode [00:07:41]
RootId      BridgeId      Port      Iface Last seen
Total Packets: 0      STP Packets: 0      MAC Spoofing [X]
You've got a message:
Press any key to continue
```

The notification window contains the following text:

```
Notification window
Warning: interface eth0 selected as the default one
Press any key to continue
```

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.

The screenshot shows a terminal window titled "yersinia -1 - Parrot Terminal". The title bar also displays "yersinia 0.8.2 by Slay & tomac - STP mode" and the time "[00:07:58]". The main interface has columns for "RootId", "BridgeId", "Port", and "Iface Last seen". A context menu titled "Available commands" is open, listing various options like "Help screen", "eXecute attack", and "Quit (bring da noize)". In the bottom left, it says "Total Packets: 0" and "This is the help screen.". In the bottom right, there's a section for "AC Spoofing [X]" with fields for "00" and "hcost 00000000". The bottom status bar shows "BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F".

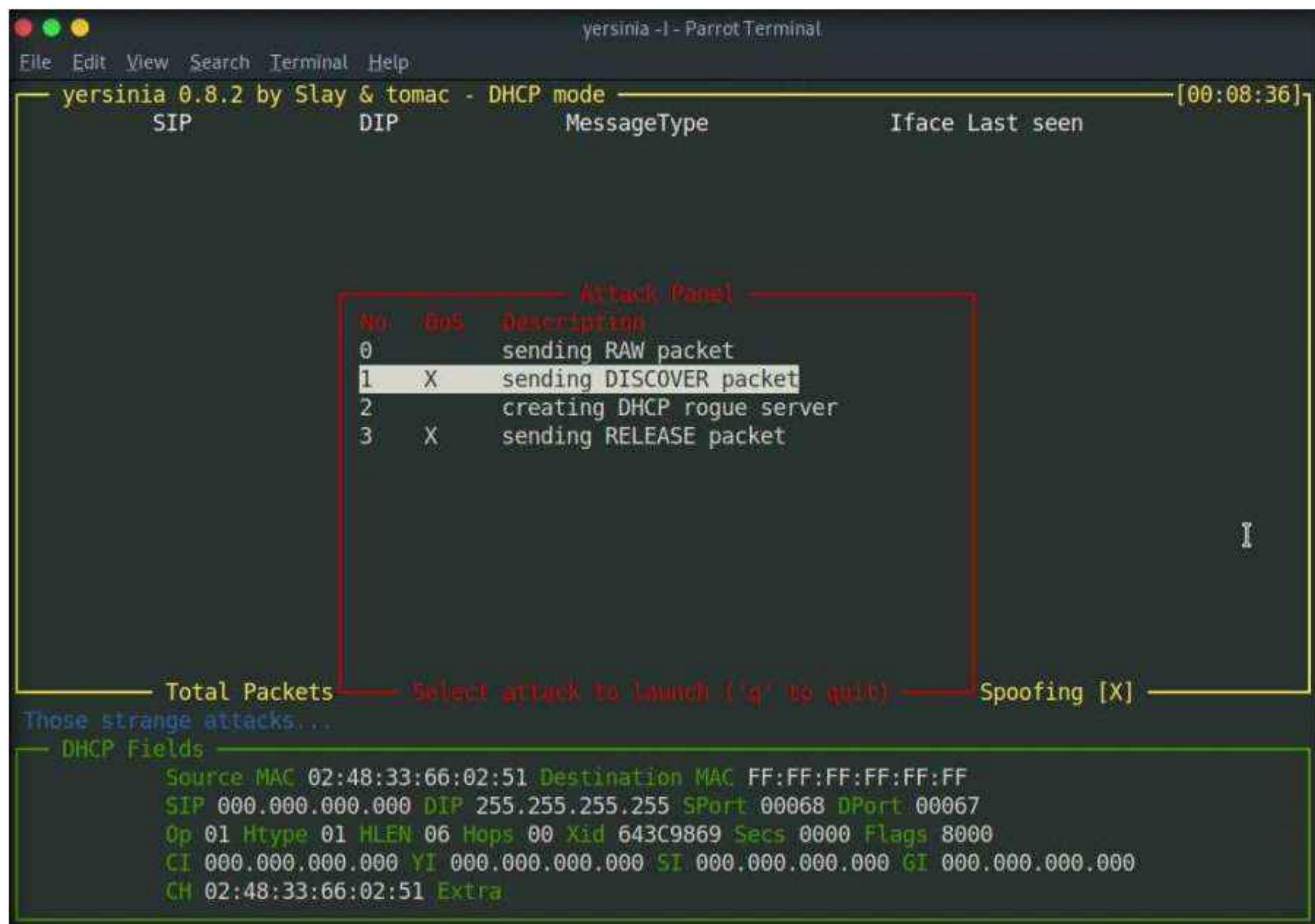
13. Press **q** to exit the help options.

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.

The screenshot shows a terminal window titled "yersinia -1 - Parrot Terminal". The title bar displays "yersinia 0.8.2 by Slay & tomac - DHCP mode" and the time "[00:08:27]". The main interface has columns for "SIP", "DIP", "MessageType", and "Iface Last seen". At the bottom, it shows "Total Packets: 0", "DHCP Packets: 0", and "MAC Spoofing [X]". A section titled "DHCP Fields" displays detailed network configuration parameters. The bottom status bar shows "BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F".

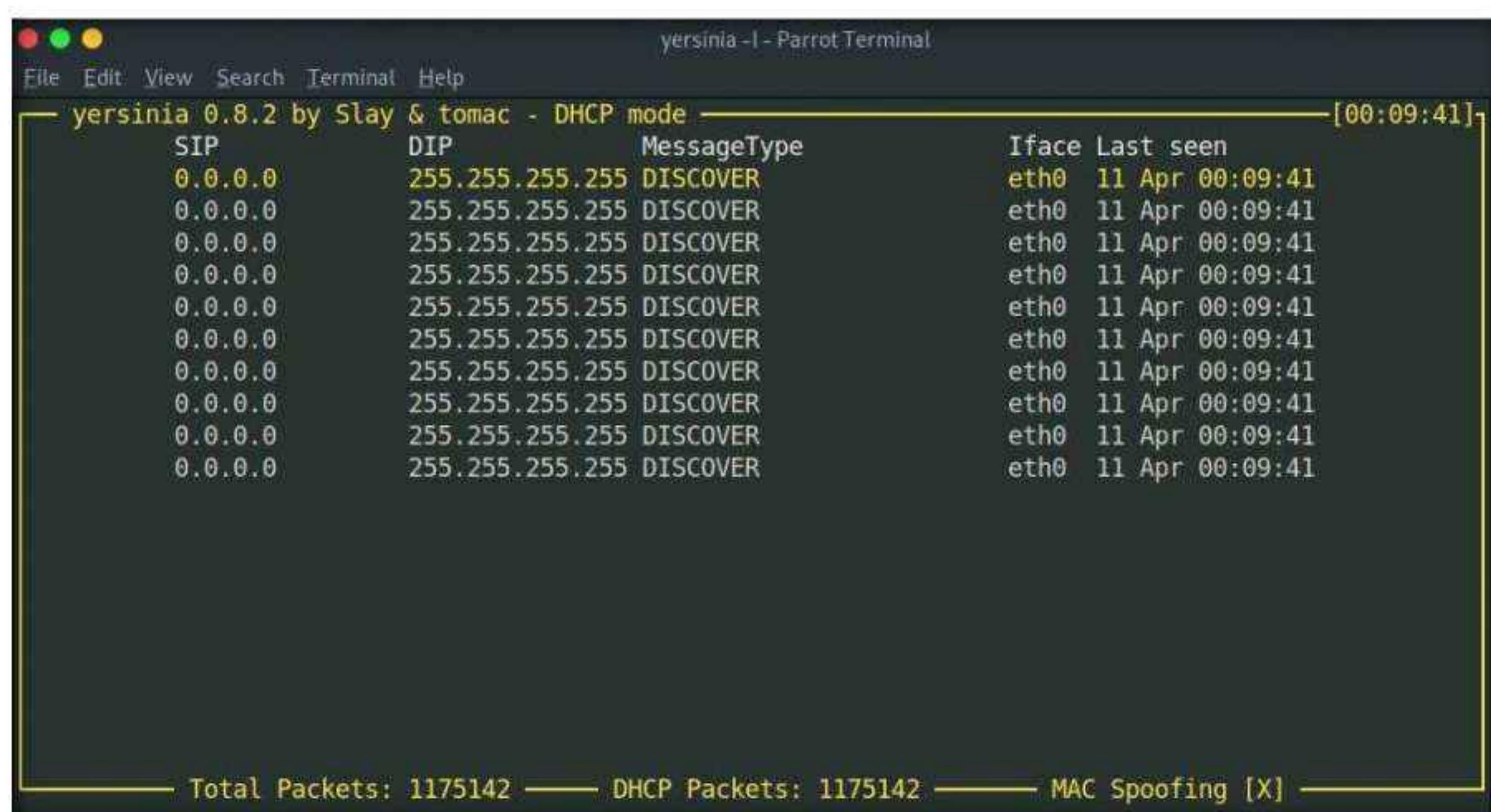
15. Press x to list available attack options.

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.



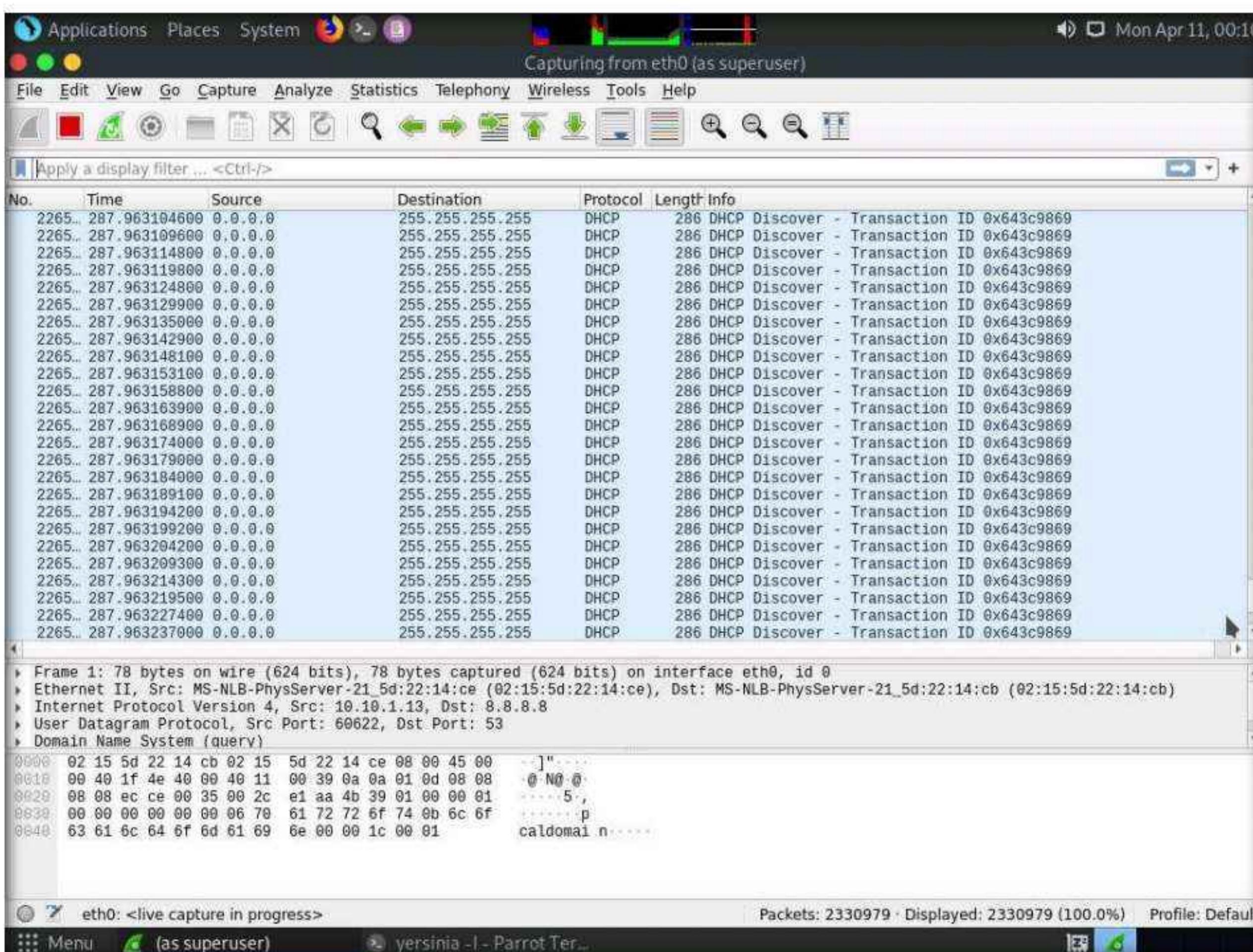
Module 08 – Sniffing

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

```
[attacker@parrot] ~
└─$ sudo su
[sudo] password for attacker:
[root@parrot] ~
└─# cd
[root@parrot] ~
└─# yersinia -I

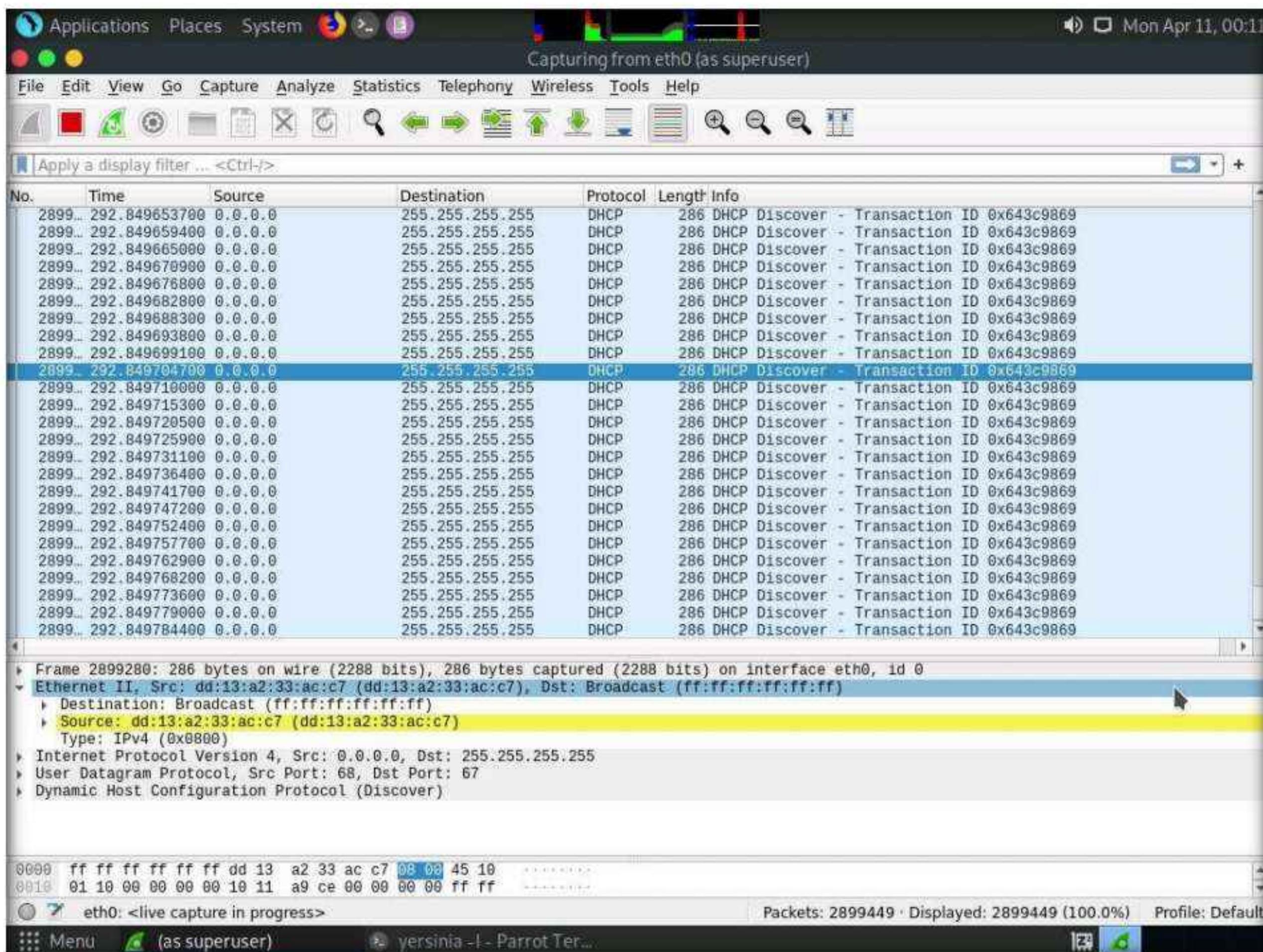
MOTD: I'm so 31337 that I can pronounce yersinia as yersiiiniiiaaaa
[root@parrot] ~
└─#
```

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

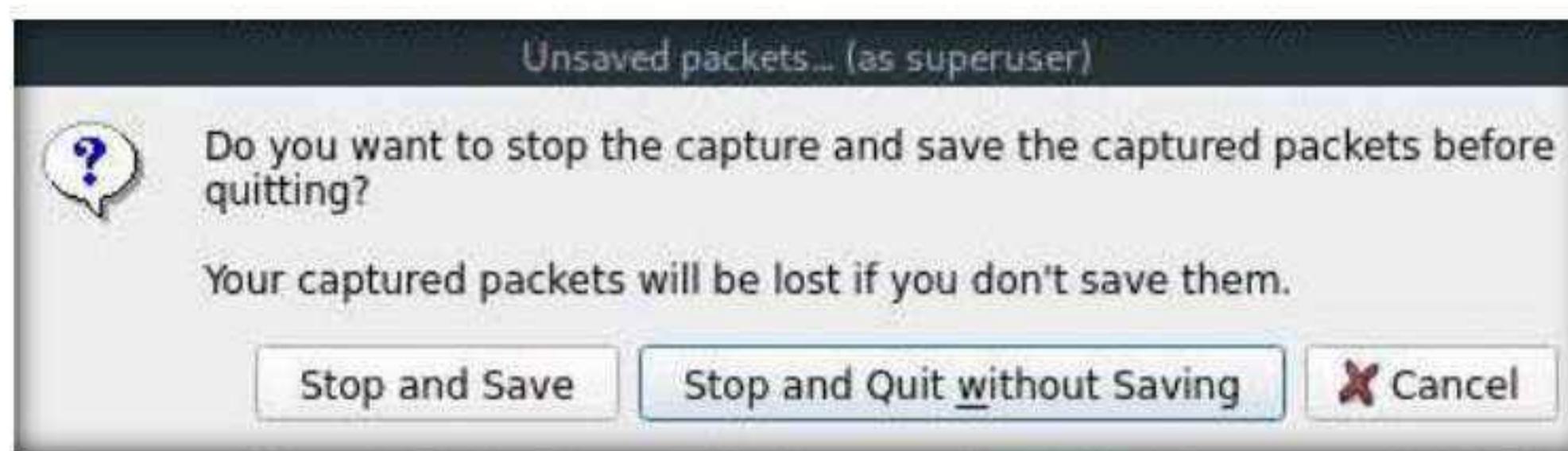


Module 08 – Sniffing

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

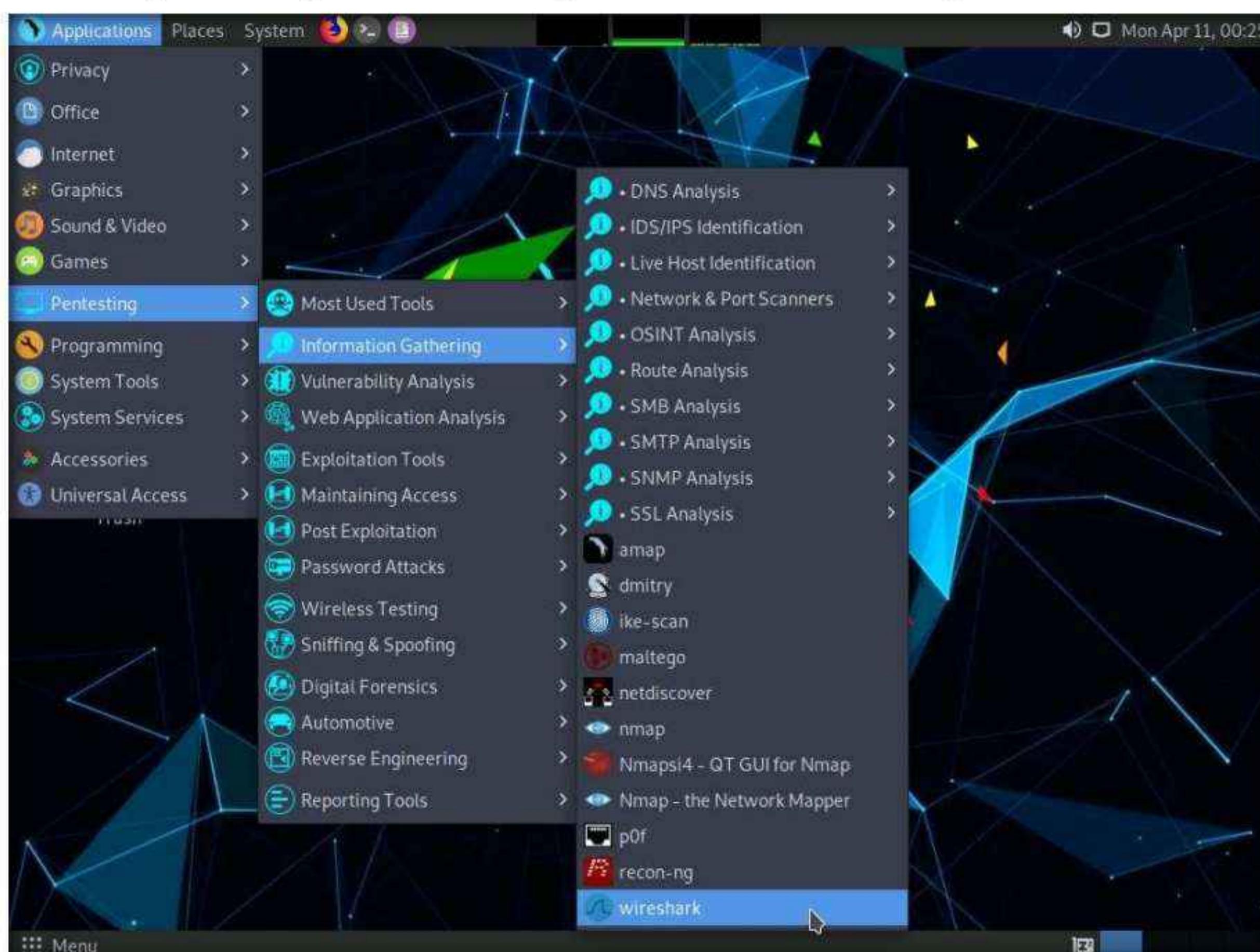
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the 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.

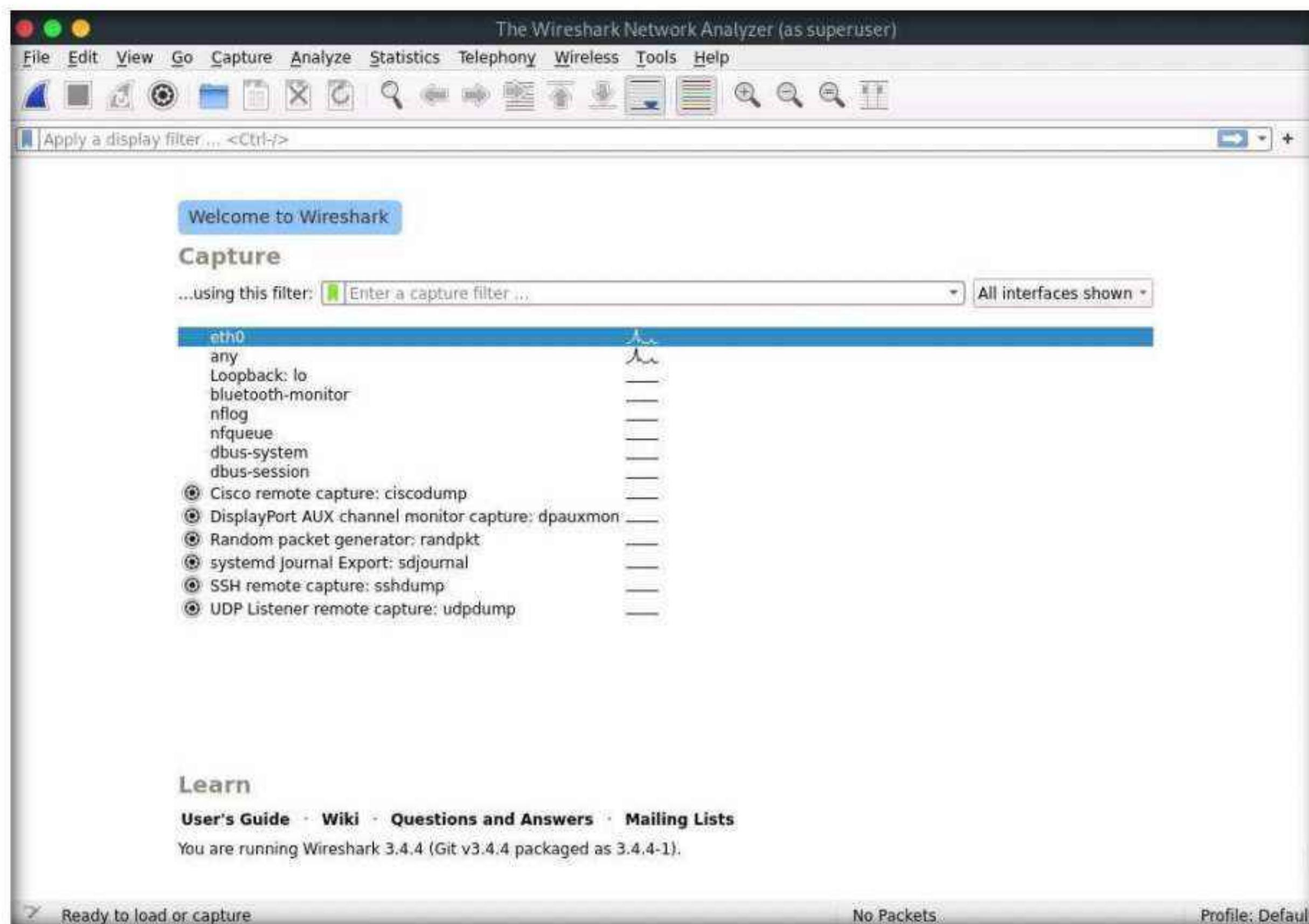
Note: In this lab, we will use the **Parrot Security (10.10.1.13)** machine as the host system and the **Windows 11 (10.10.1.11)** machine as the target system.

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.



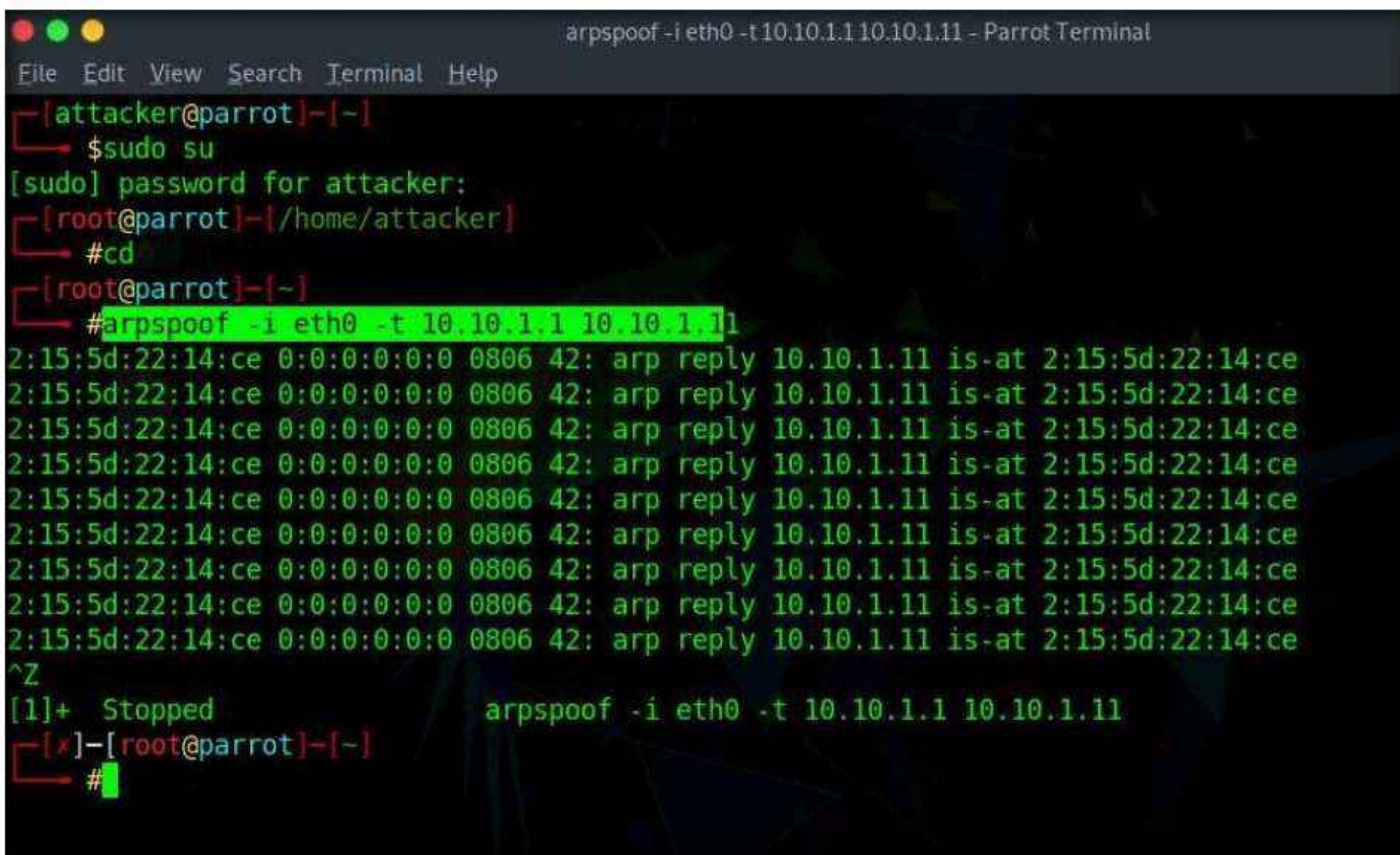
5. Leave the **Wireshark** application running.
6. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In 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 **arp spoof -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.

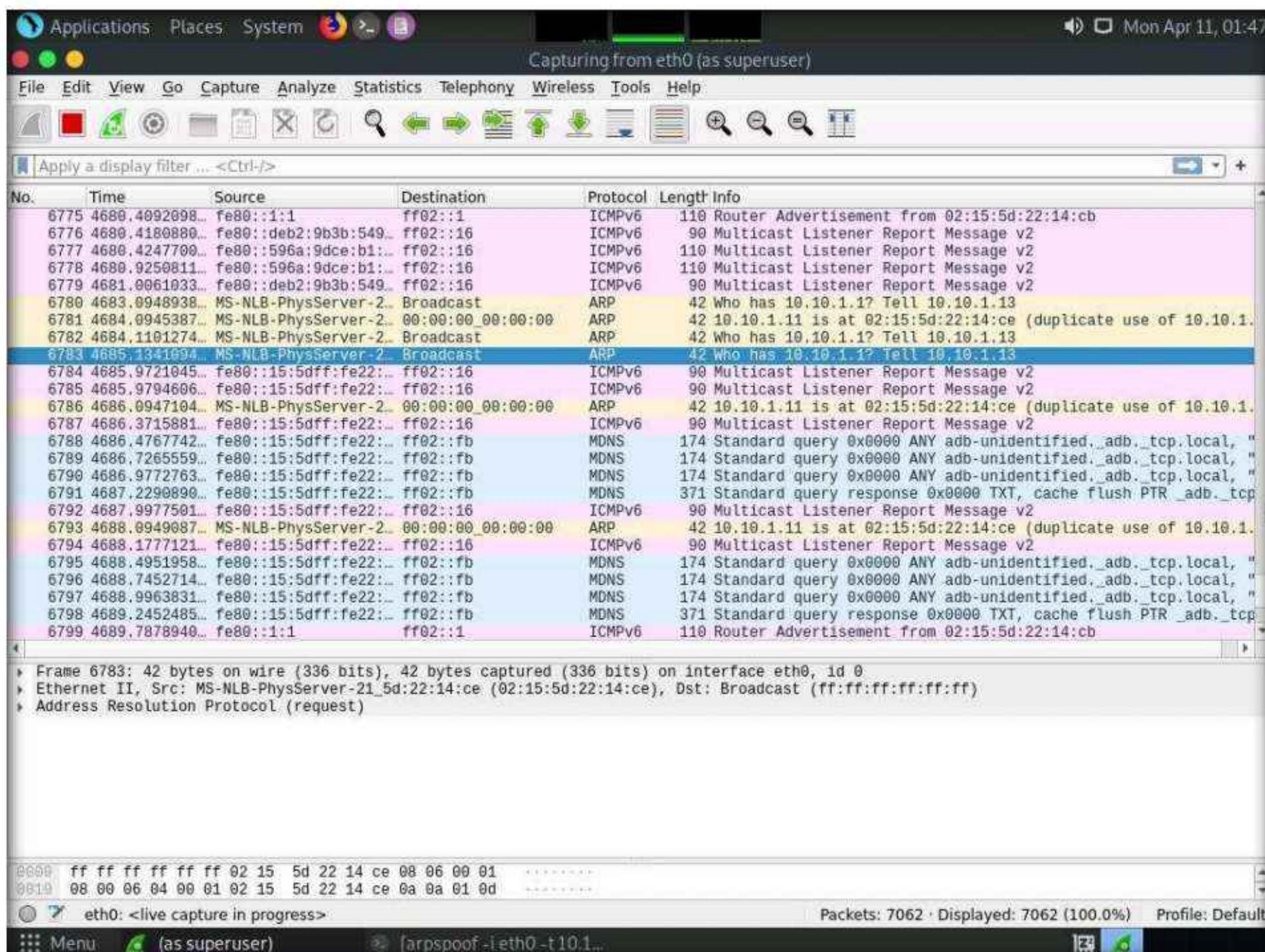
Note: The MAC addresses might differ when you perform this task.

Module 08 – Sniffing



```
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# arpspoof -i eth0 -t 10.10.1.1 10.10.1.11
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
^Z
[1]+  Stopped                  arpspoof -i eth0 -t 10.10.1.1 10.10.1.11
[root@parrot] ~
#
```

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

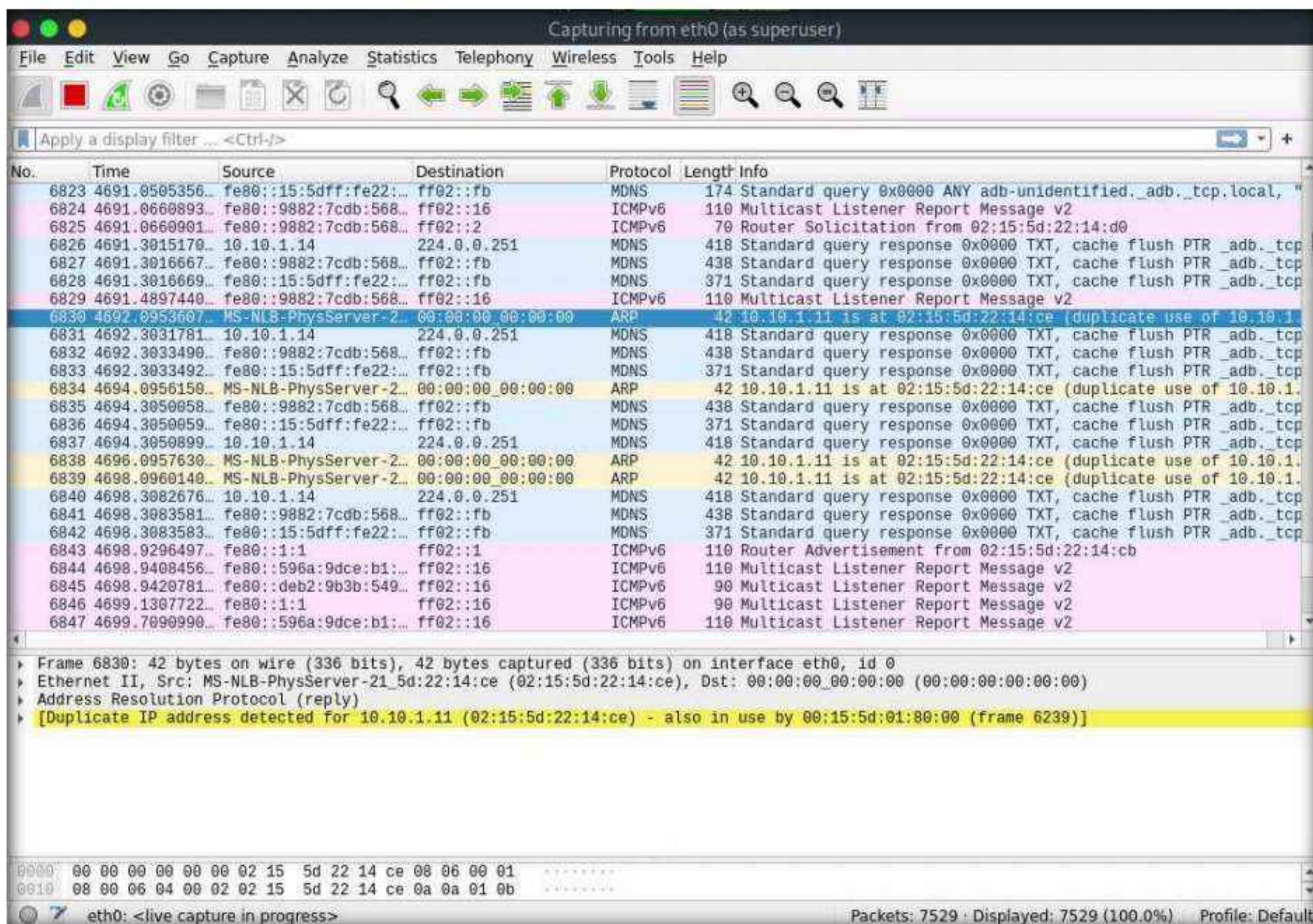


14. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.1.11 10.10.1.1** and press **Enter**.
15. Through the above command, the host system informs the target system (**10.10.1.11**) that it is the access point (**10.10.1.1**).
16. After sending a few packets,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

The screenshot shows a terminal window titled "arp spoof -i eth0 -t 10.10.1.11 10.10.1.1 - Parrot Terminal". The terminal is running on a Parrot Security OS. The user has entered the command "#arp spoof -i eth0 -t 10.10.1.11 10.10.1.1" and is seeing a series of arp reply messages. The user then presses ^Z to stop the process, which is indicated by "[3]+ Stopped". The terminal prompt "#>" is visible at the bottom.

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.

Module 08 – Sniffing



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 advise 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.

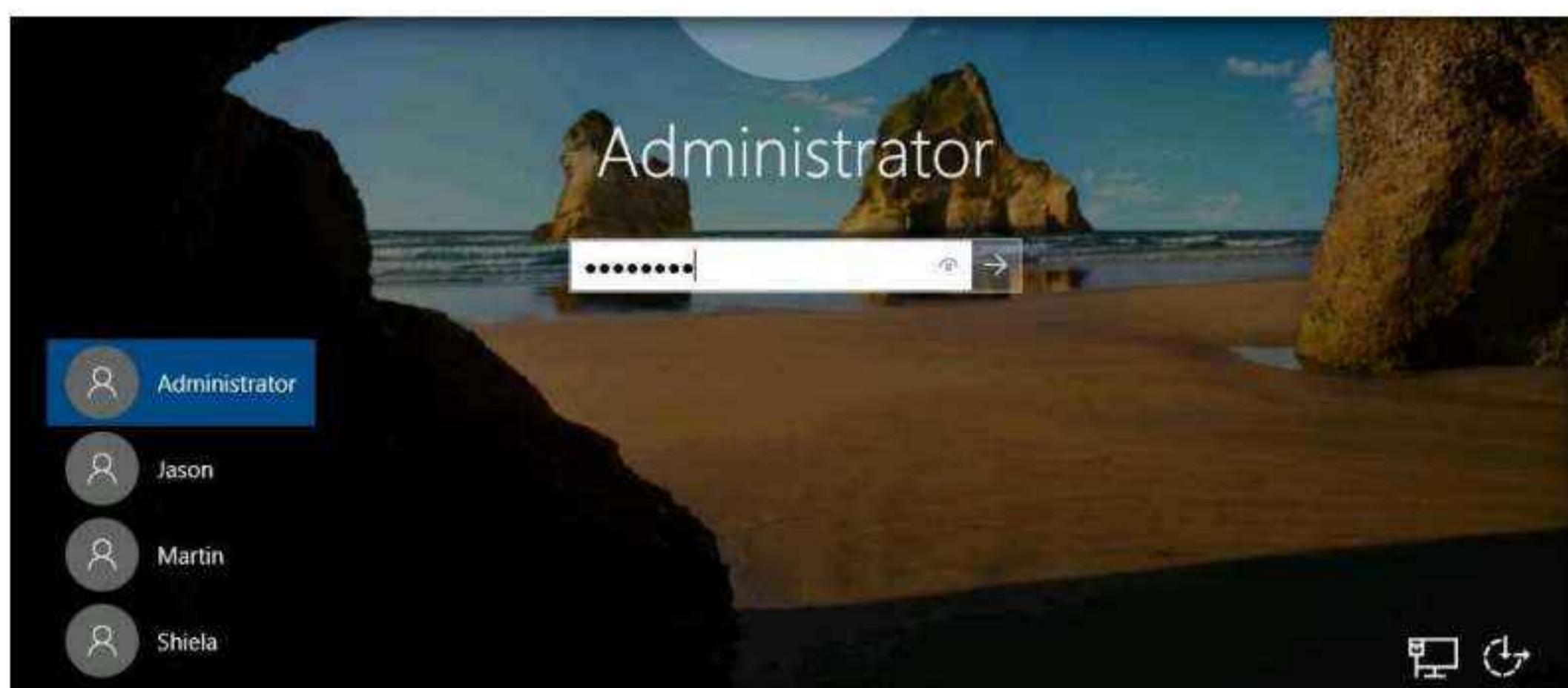
Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

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

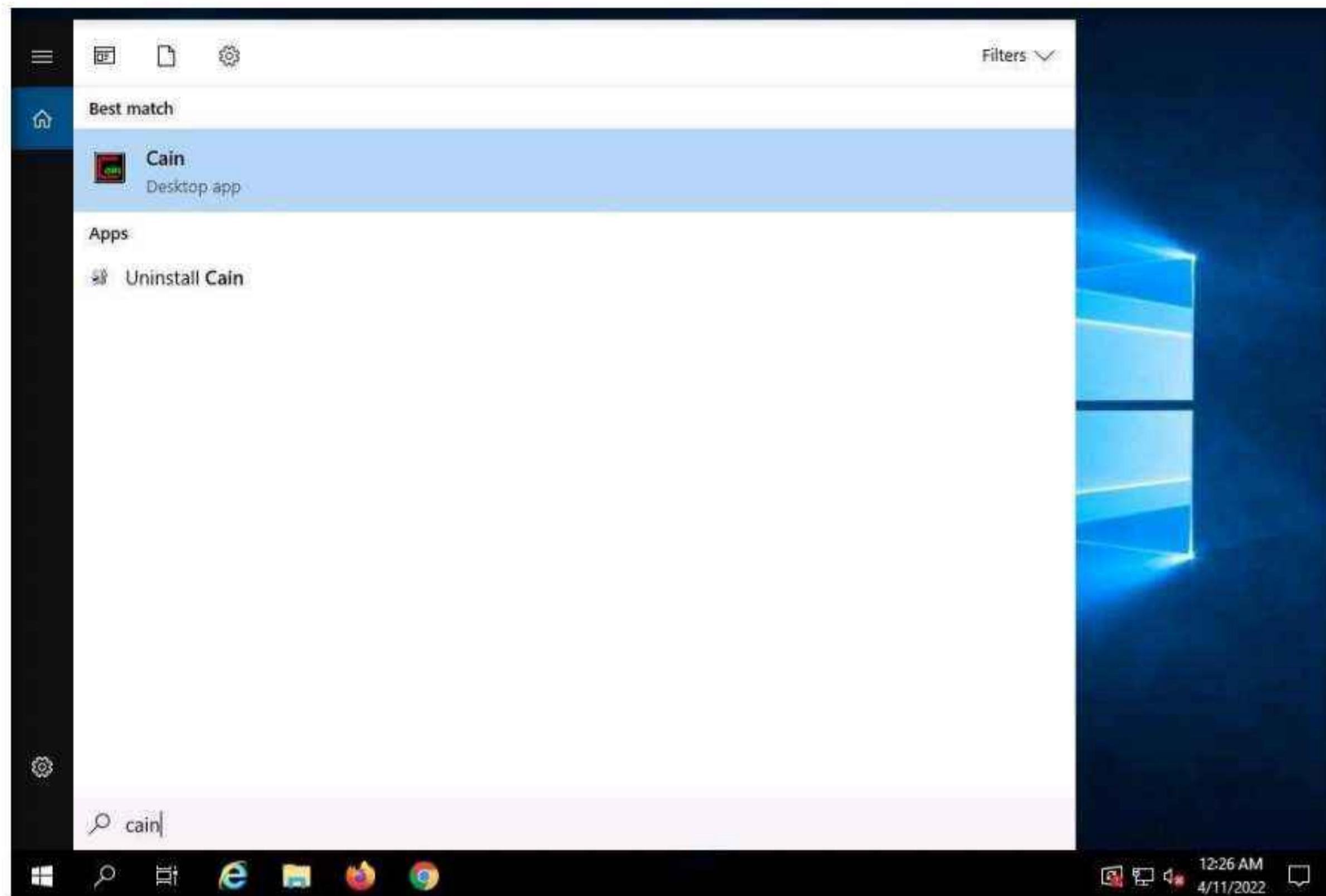
Note: Ensure that **Windows 11** and **Parrot Security** virtual machines are running.

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.

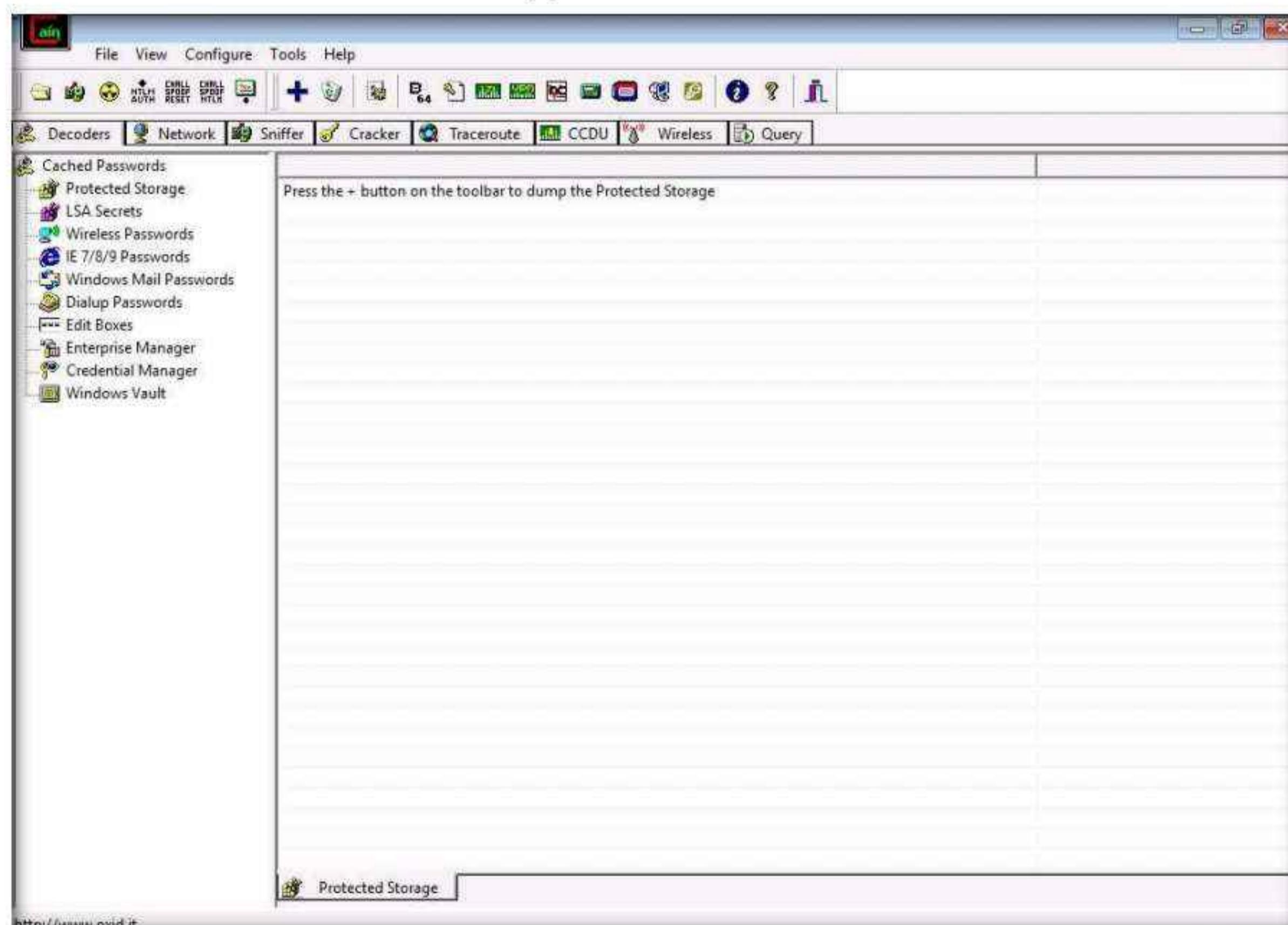
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



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

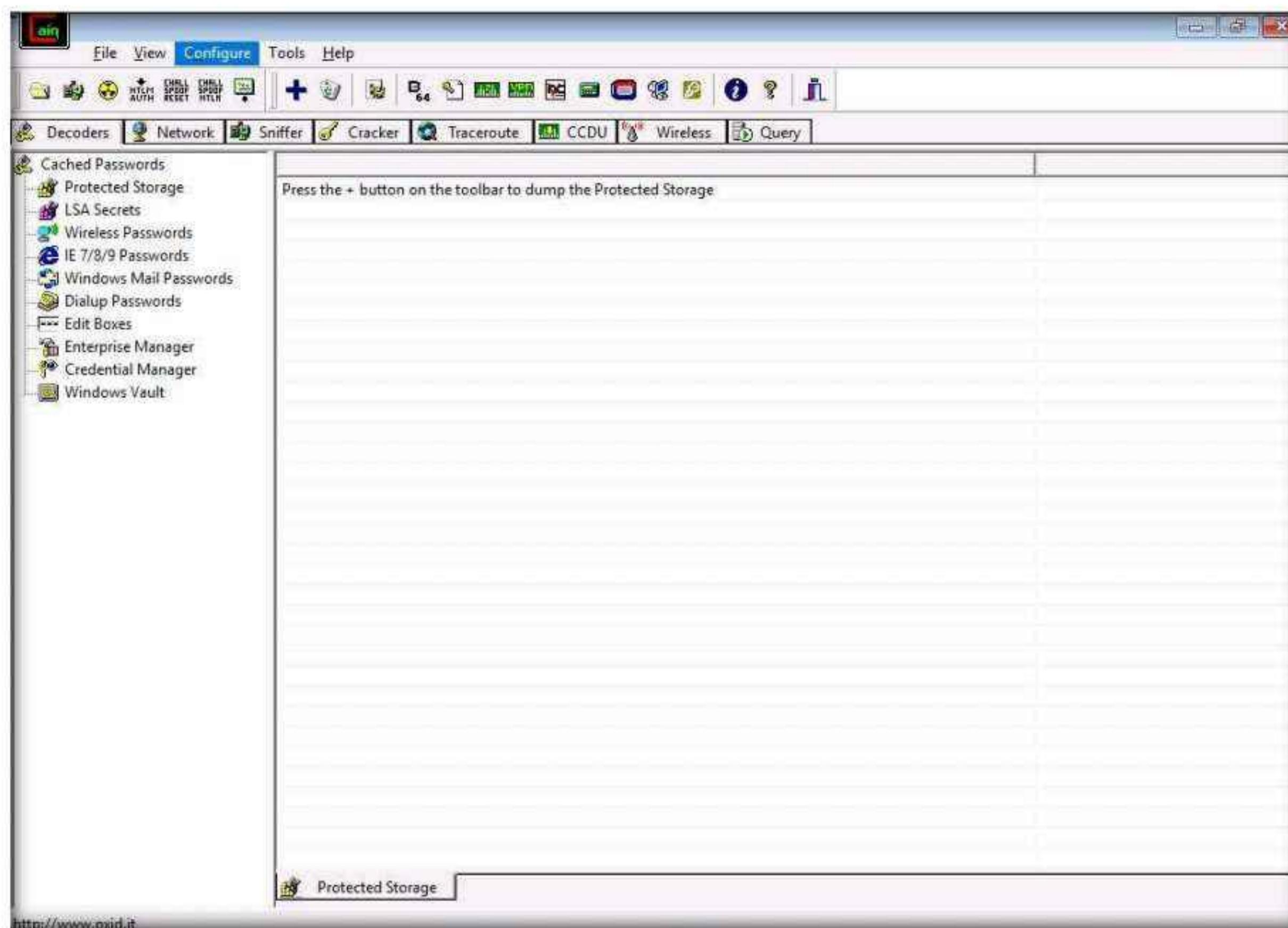


4. The **Cain & Abel** main window appears, as shown in the screenshot.



Module 08 – Sniffing

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

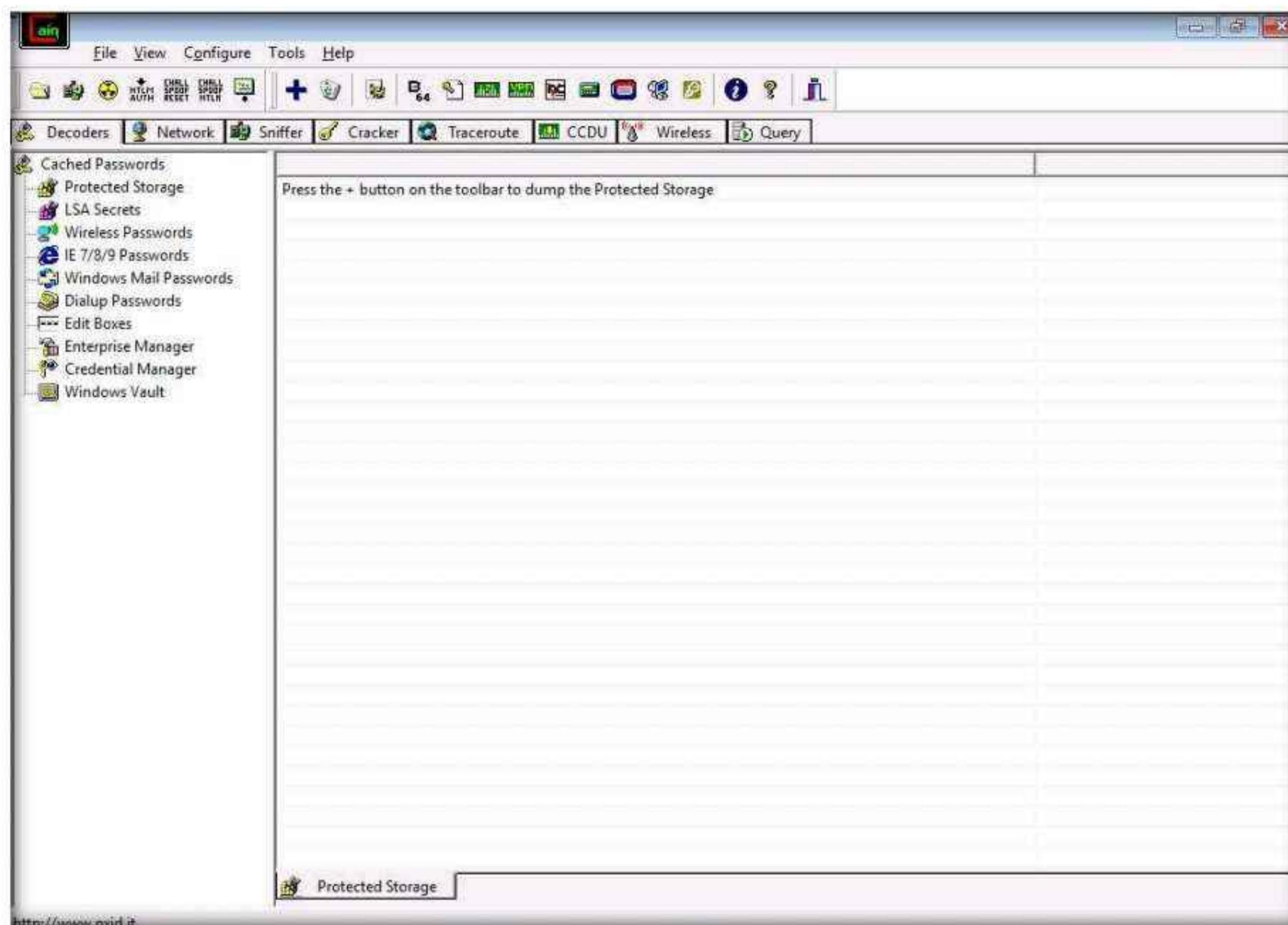


6. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.

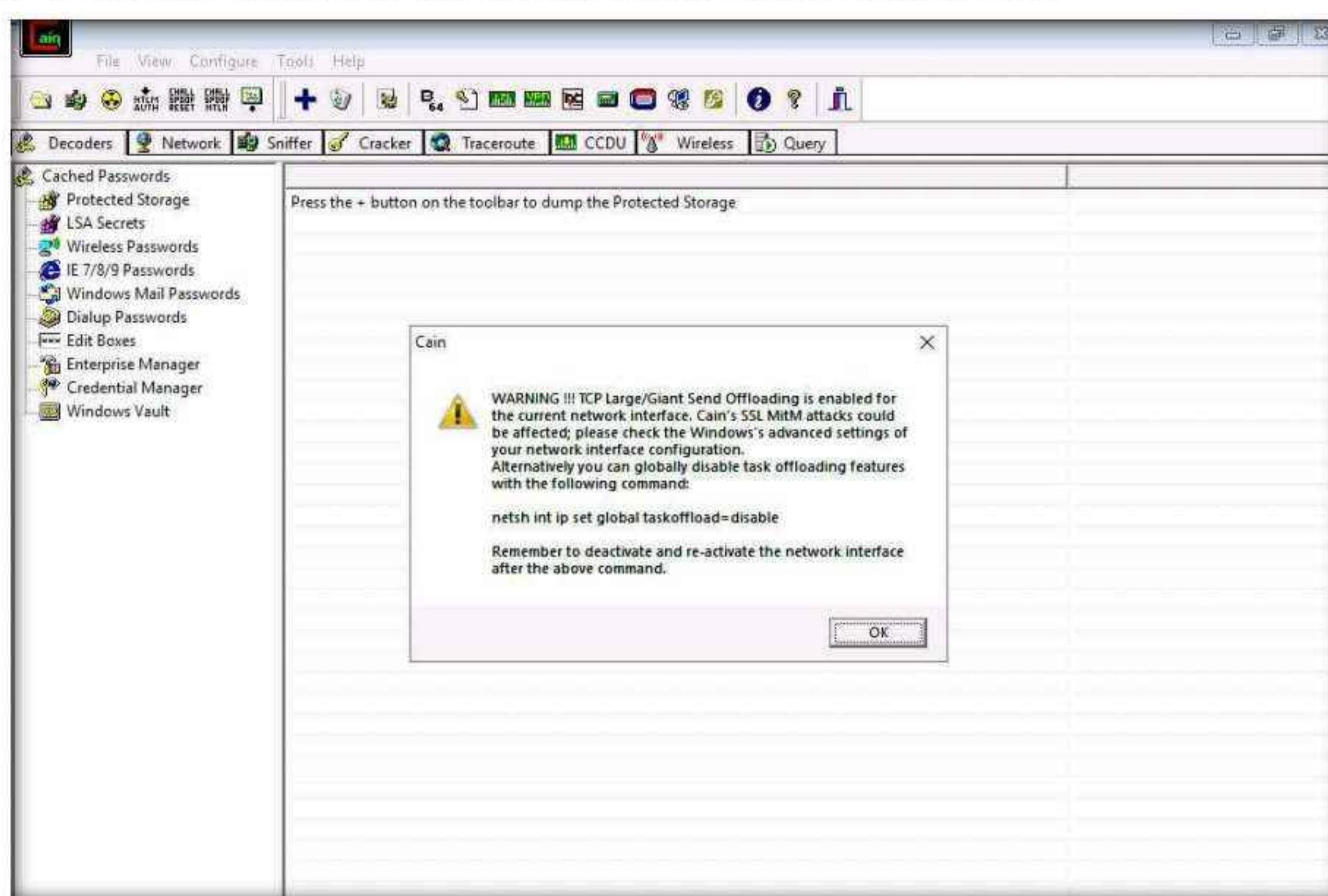


Module 08 – Sniffing

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

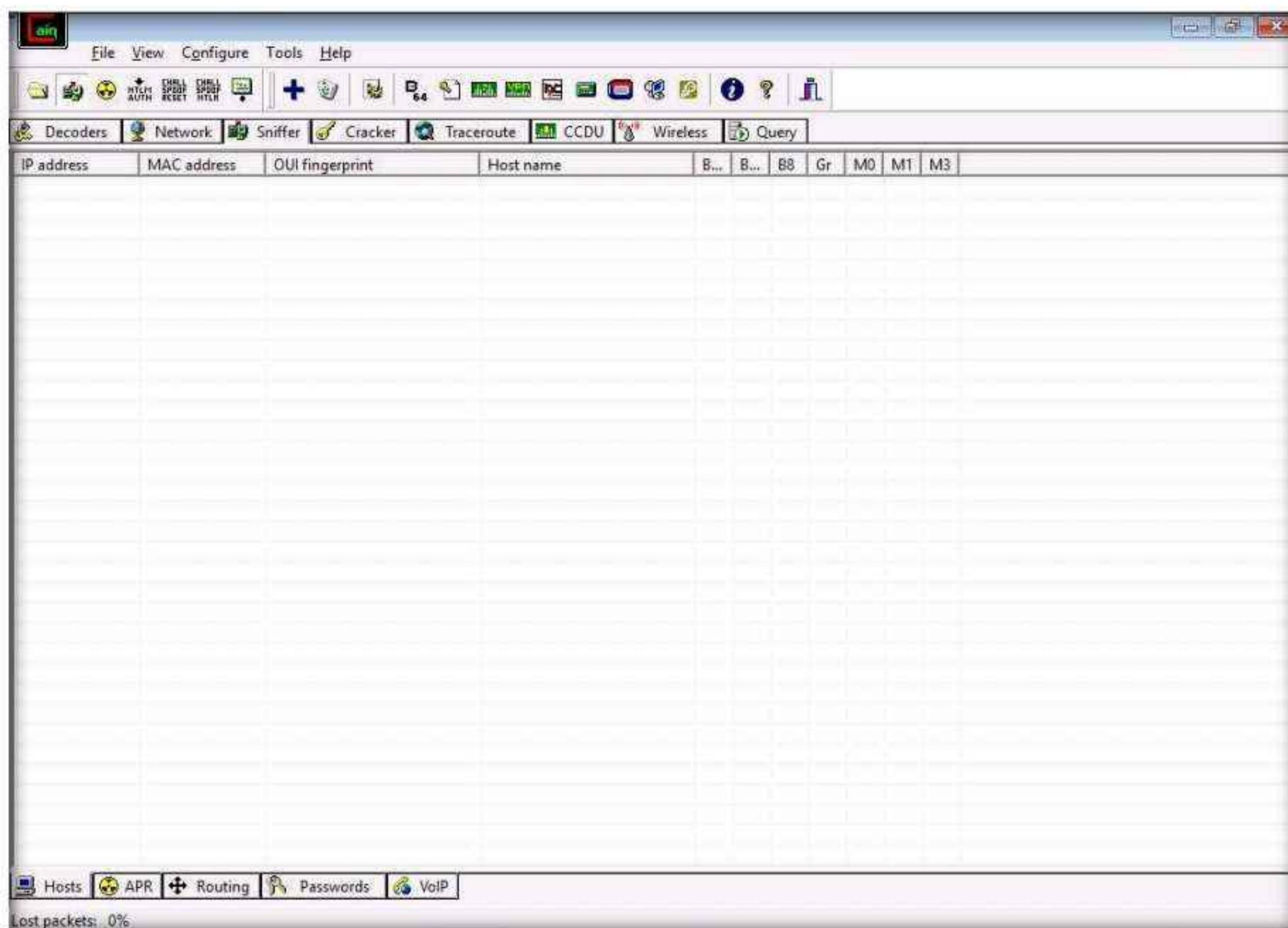


8. A Cain pop-up appears and displays a Warning message; click OK.

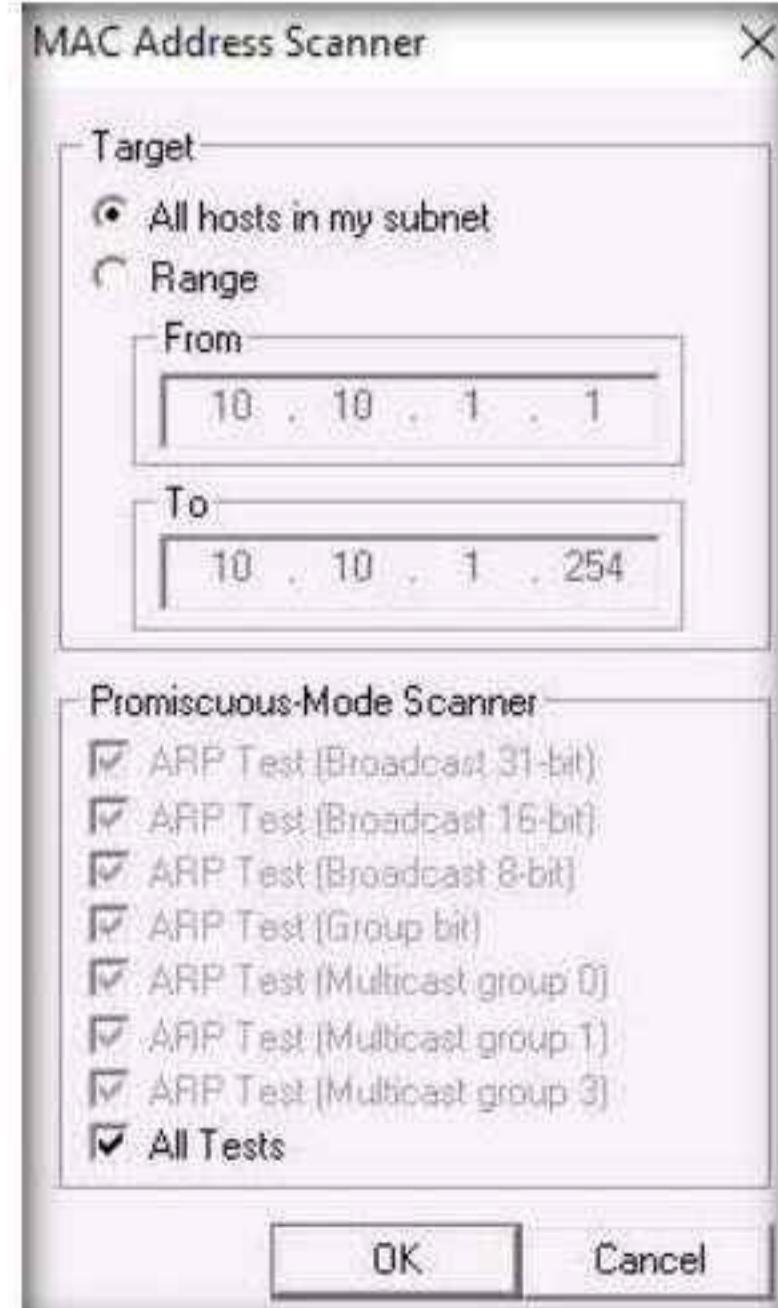


Module 08 – Sniffing

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**.



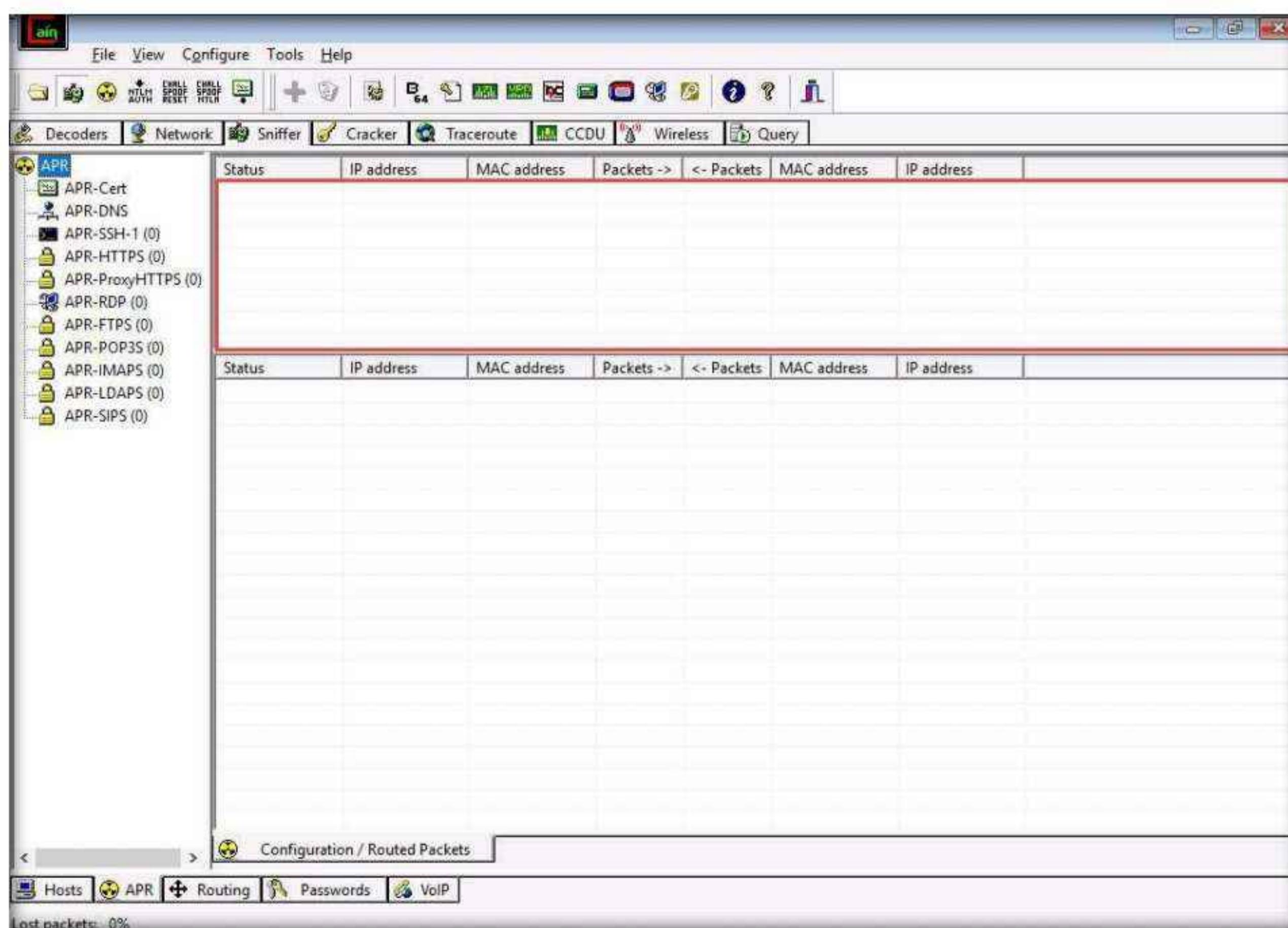
Module 08 – Sniffing

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.

The screenshot shows the Cain & Abel interface. The main window displays a table of network information:

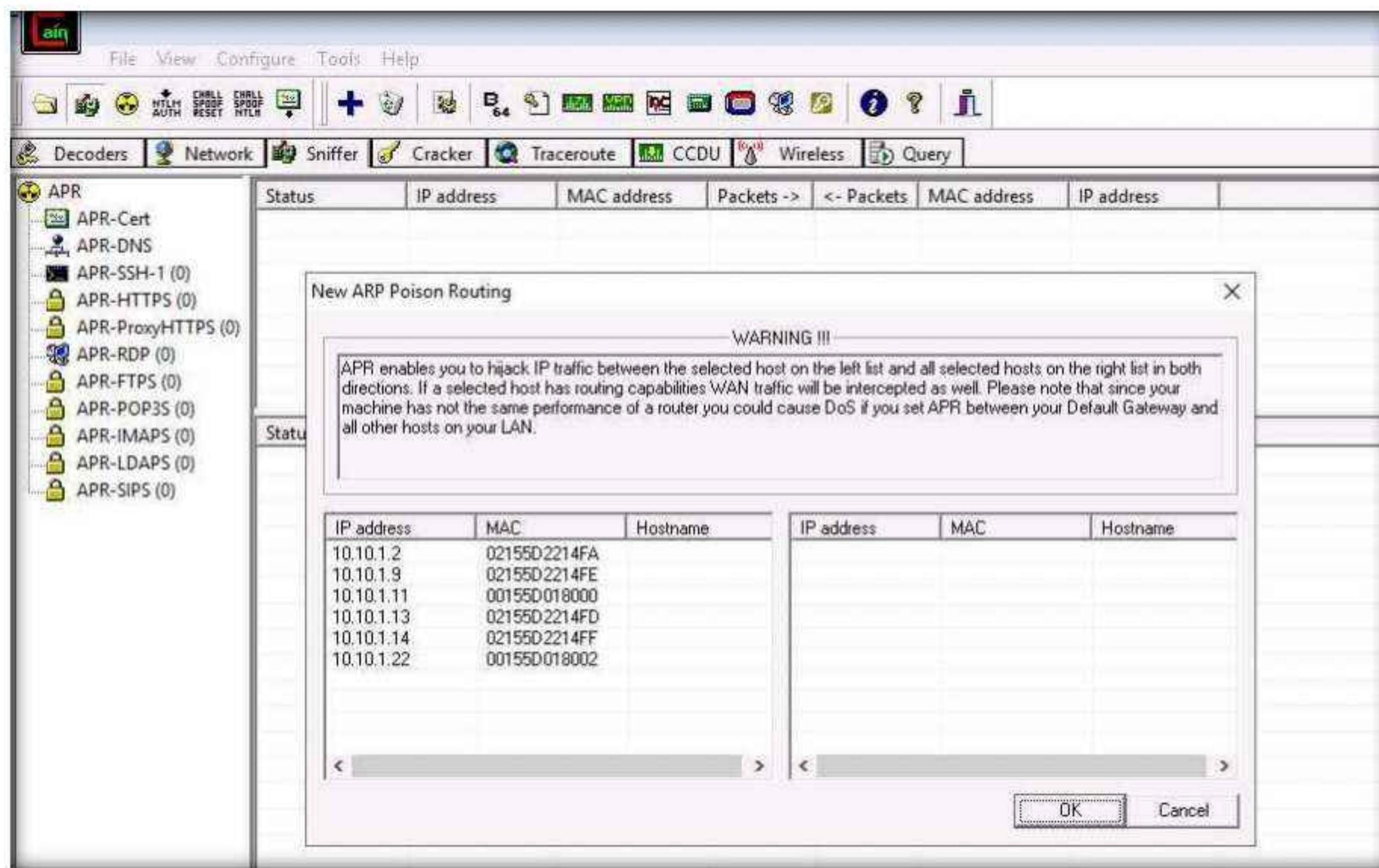
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.2	02155D2214FA			*	*	*	*	*	*	*
10.10.1.9	02155D2214FE			*	*	*	*	*	*	*
10.10.1.11	00155D018000	Microsoft Corporation		*	*	*	*	*	*	*
10.10.1.13	02155D2214FD			*	*	*	*	*	*	*
10.10.1.14	02155D2214FF			*	*	*	*	*	*	*
10.10.1.22	00155D018002	Microsoft Corporation		*	*	*	*	*	*	*

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.

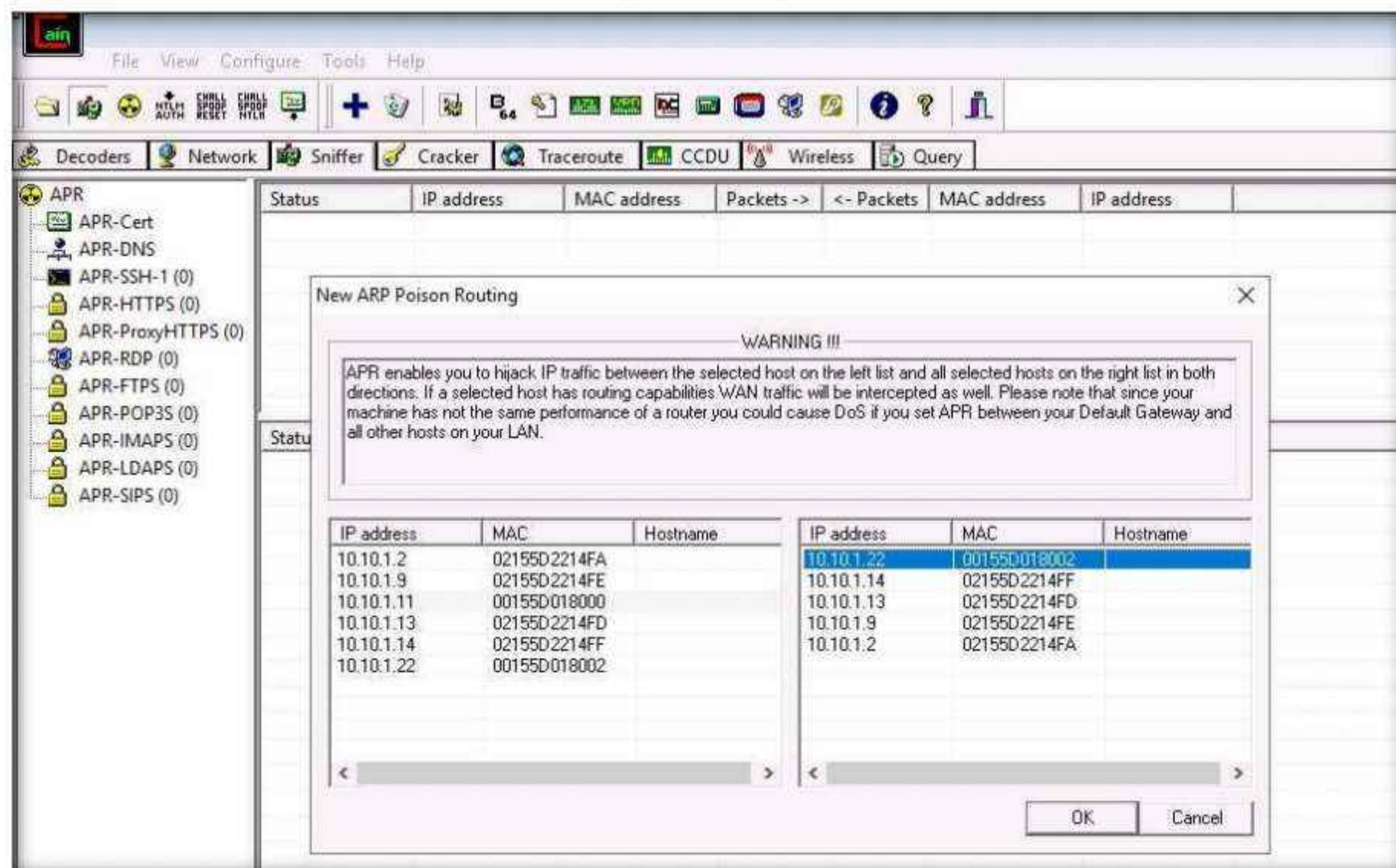


Module 08 – Sniffing

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**.



Module 08 – Sniffing

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**.

The screenshot displays two instances of the Cain & Abel software interface. Both windows are titled "Configuration / Routed Packets".

The left pane of both windows shows a tree view of APR (Advanced Port Reconnaissance) targets:

- APR-Cert
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (0)
- APR-ProxyHTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIPS (0)

The right pane contains a table with the following columns: Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address.

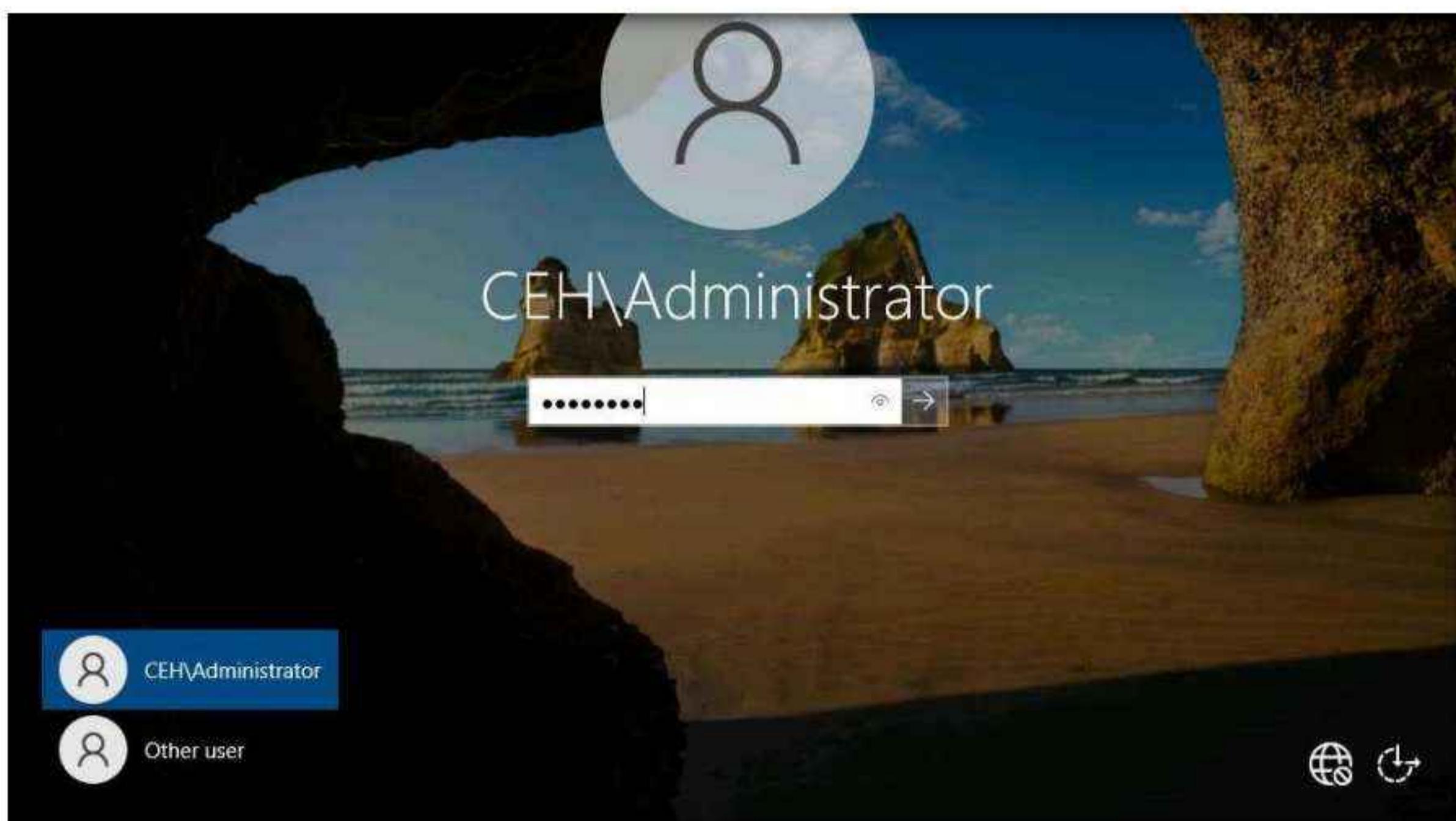
In the top window (Status: Idle), the first row shows:

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.10.1.11	00155D018000	0	0	00155D018002	10.10.1.22

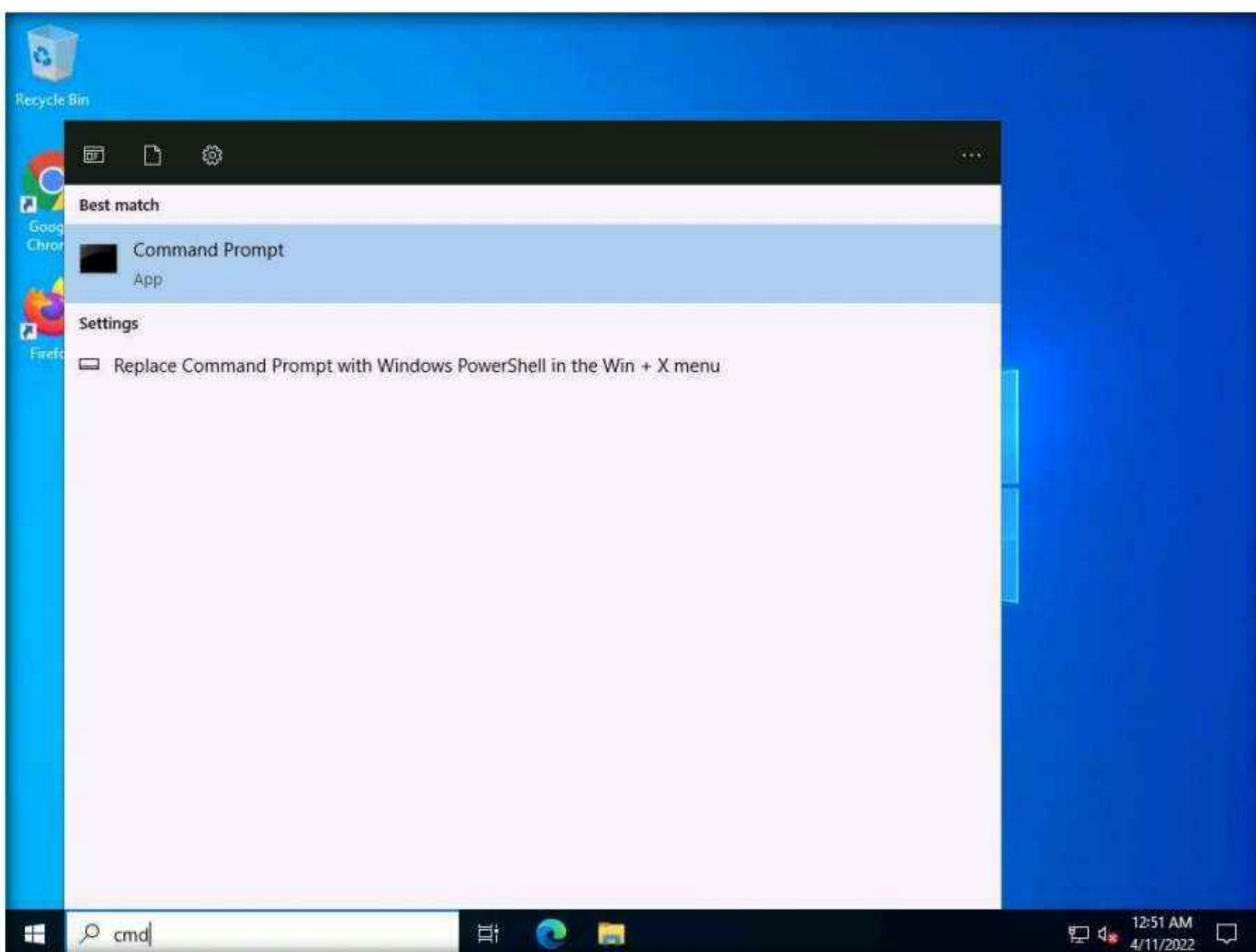
In the bottom window (Status: Poisoning), the first row shows:

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.10.1.11	00155D018000	0	0	00155D018002	10.10.1.22

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.



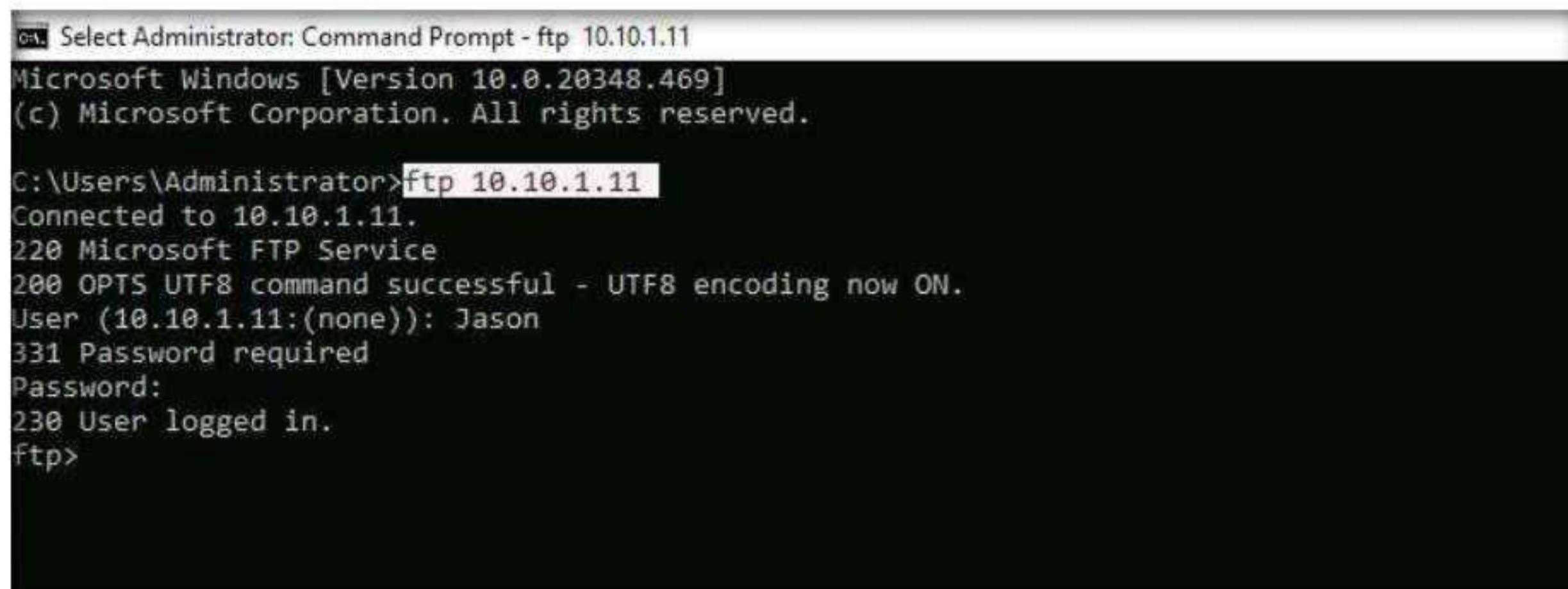
21. Click the **Type here to search** icon at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.



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**.

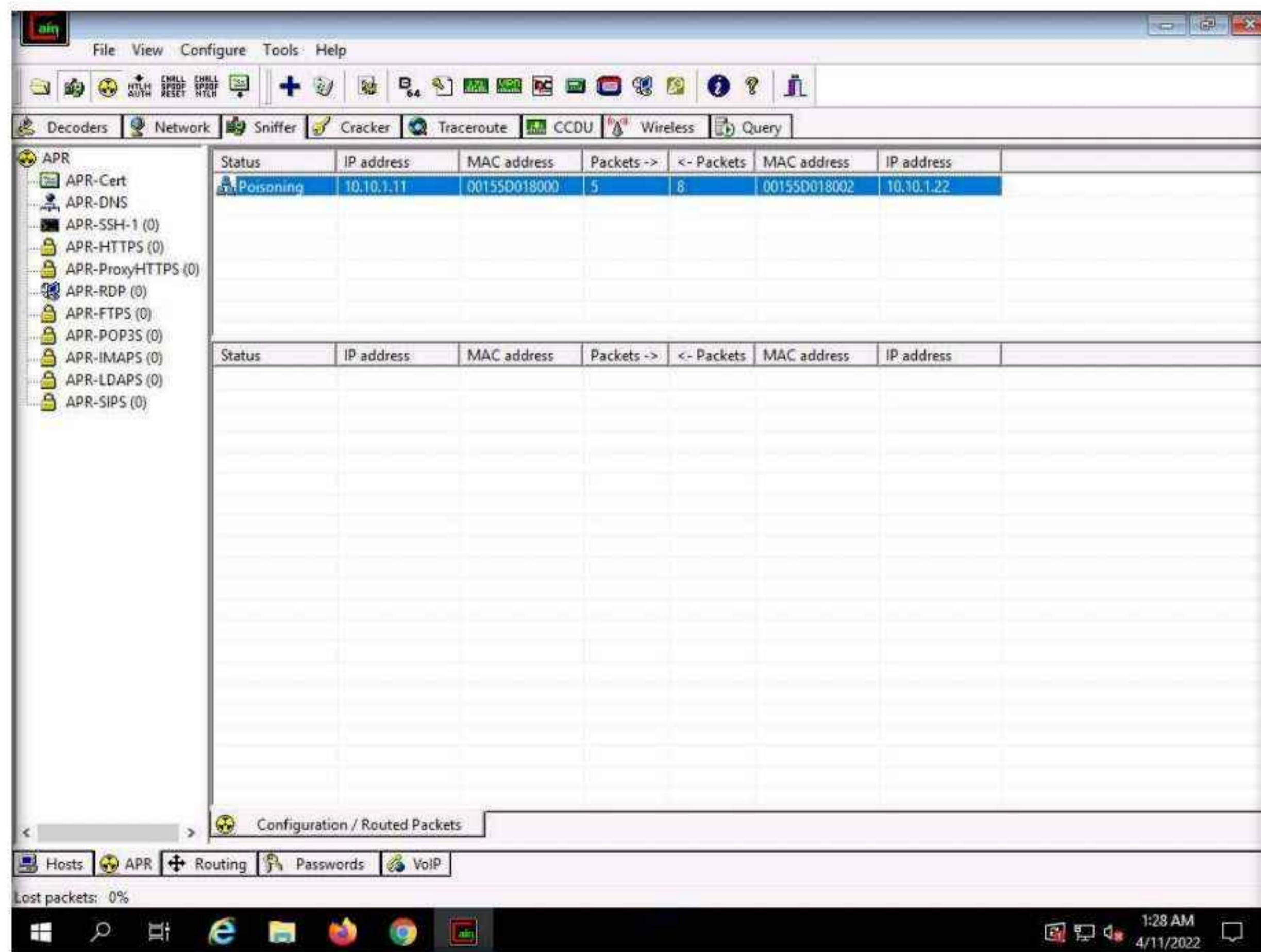
Note: Irrespective of a successful login, Cain & Abel captures the password entered during login.



```
on Select Administrator: Command Prompt - ftp 10.10.1.11
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.1.11:(none)): Jason
331 Password required
Password:
230 User logged in.
ftp>
```

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.

Timestamp	FTP server	Client	Username	Password
11/04/2022 - 01:26:01	10.10.1.11	10.10.1.22	Jason	qwerty

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.

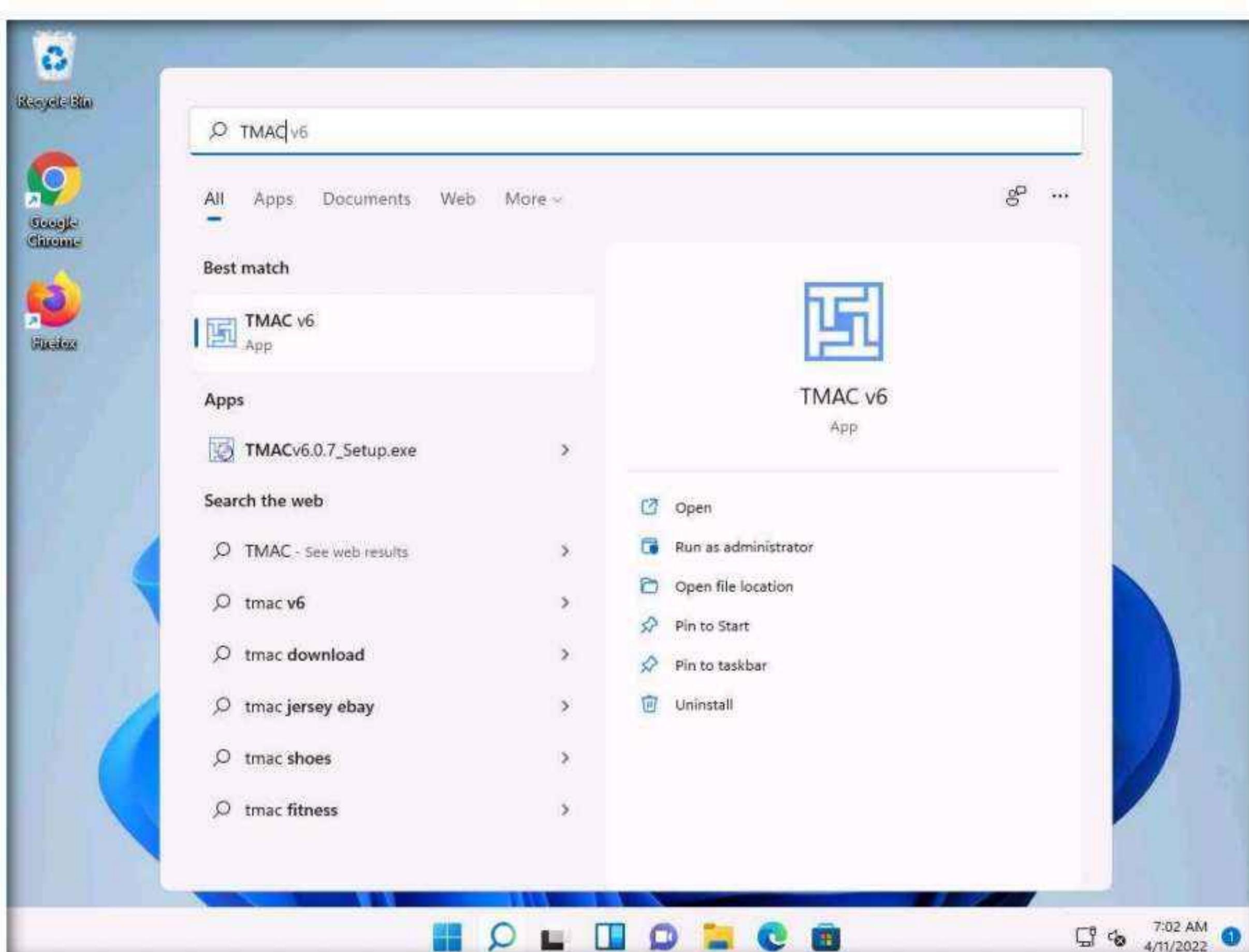
Here, we will use TMAC and SMAC tools to perform MAC spoofing.

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

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

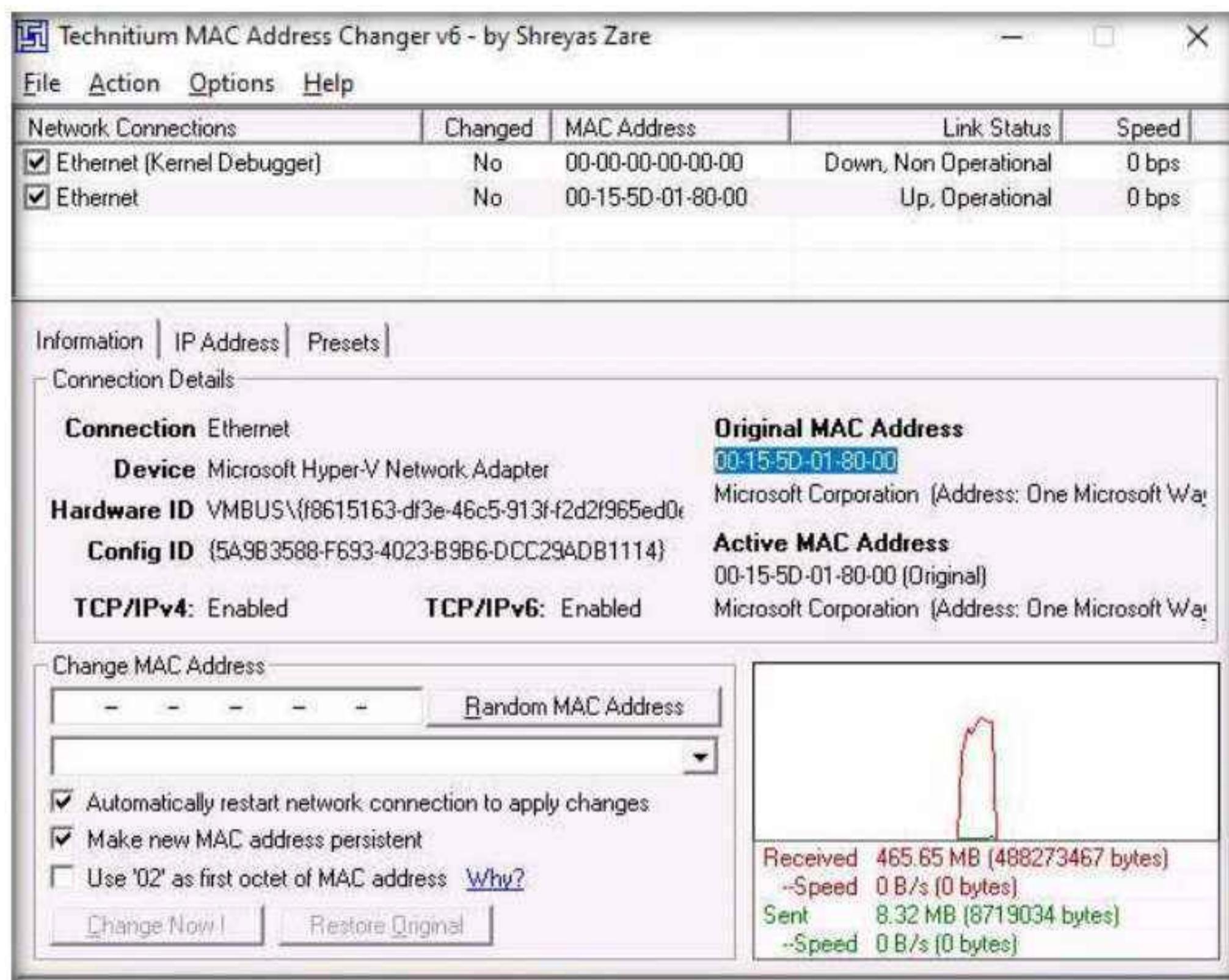
2. Click **Search** icon () on the **Desktop**. Type **TMAC** in the search field, the **TMAC v6** appears in the results, click **Open** to launch it.

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

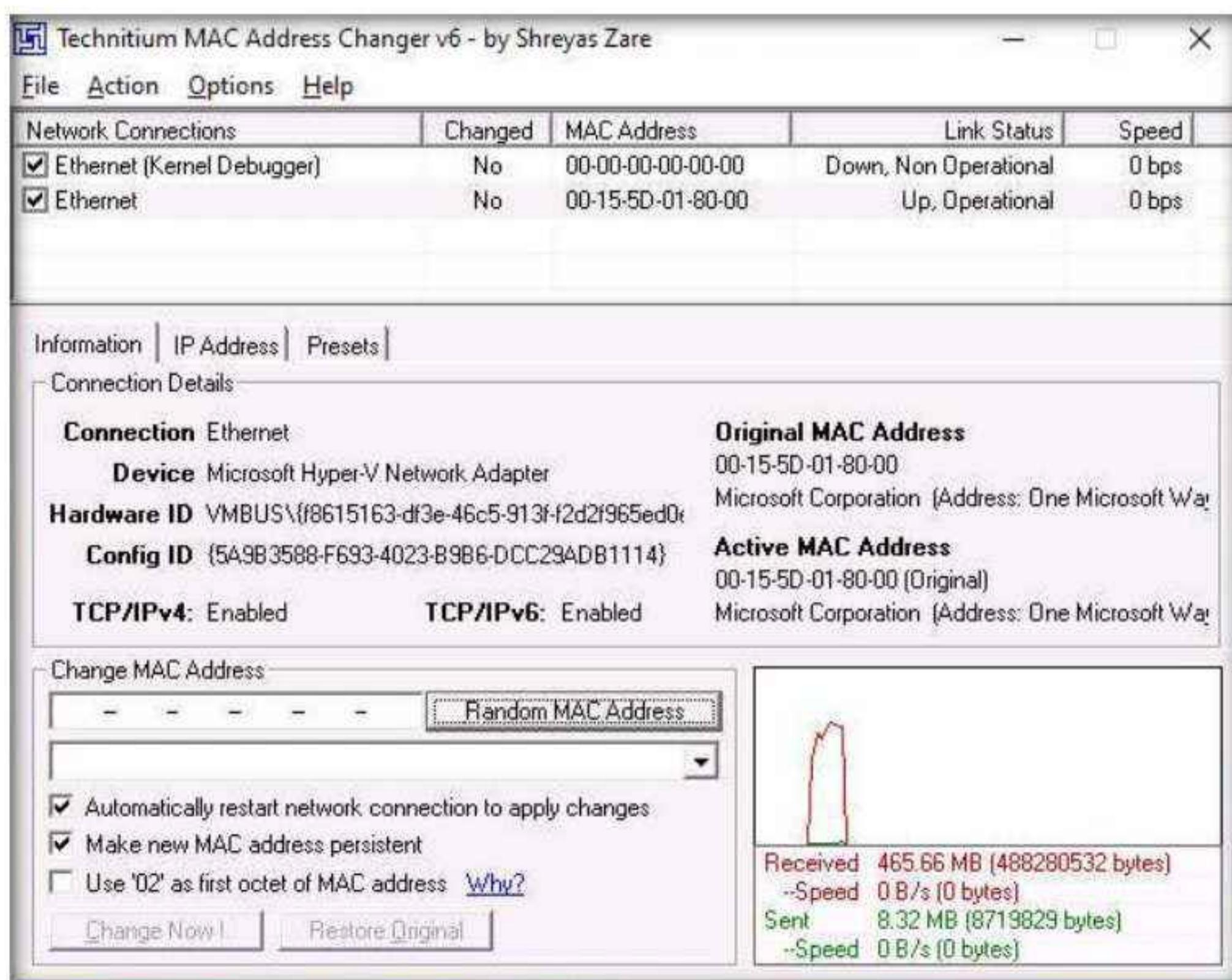


3. The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.
 4. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet**).

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

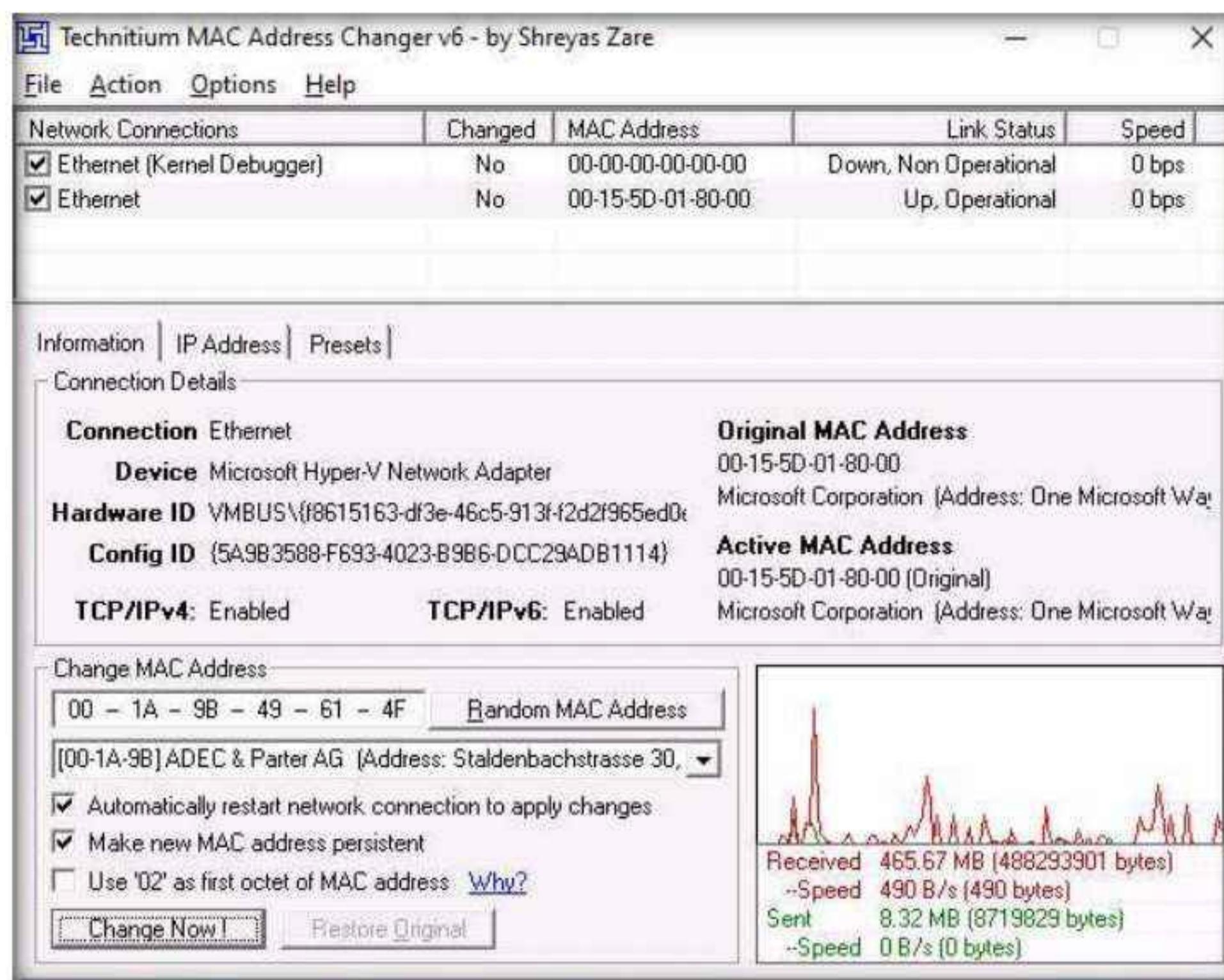


6. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

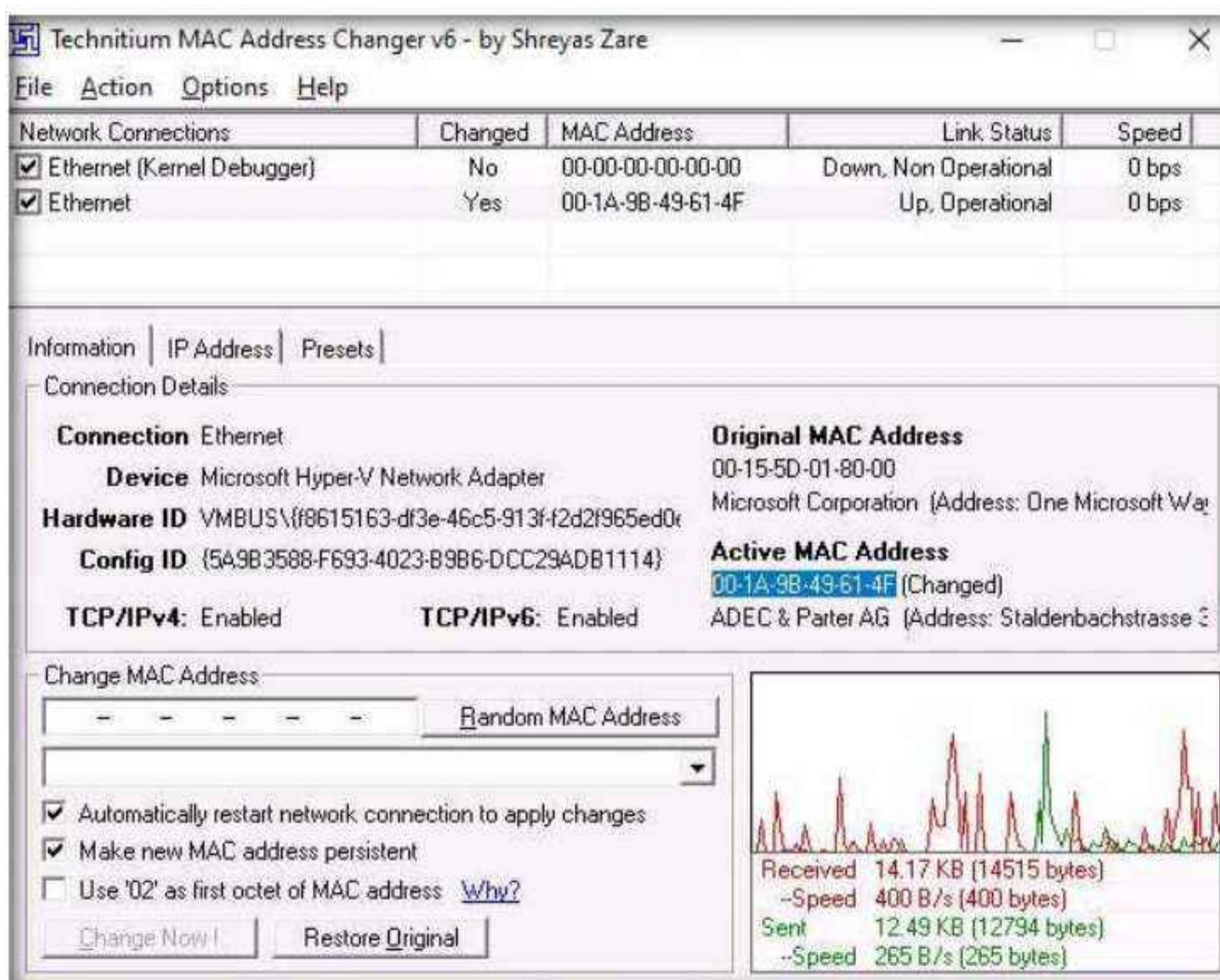


7. A Random MAC Address is generated and appears under the **Change MAC Address** field. Click the **Change Now!** button to change the MAC address.

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



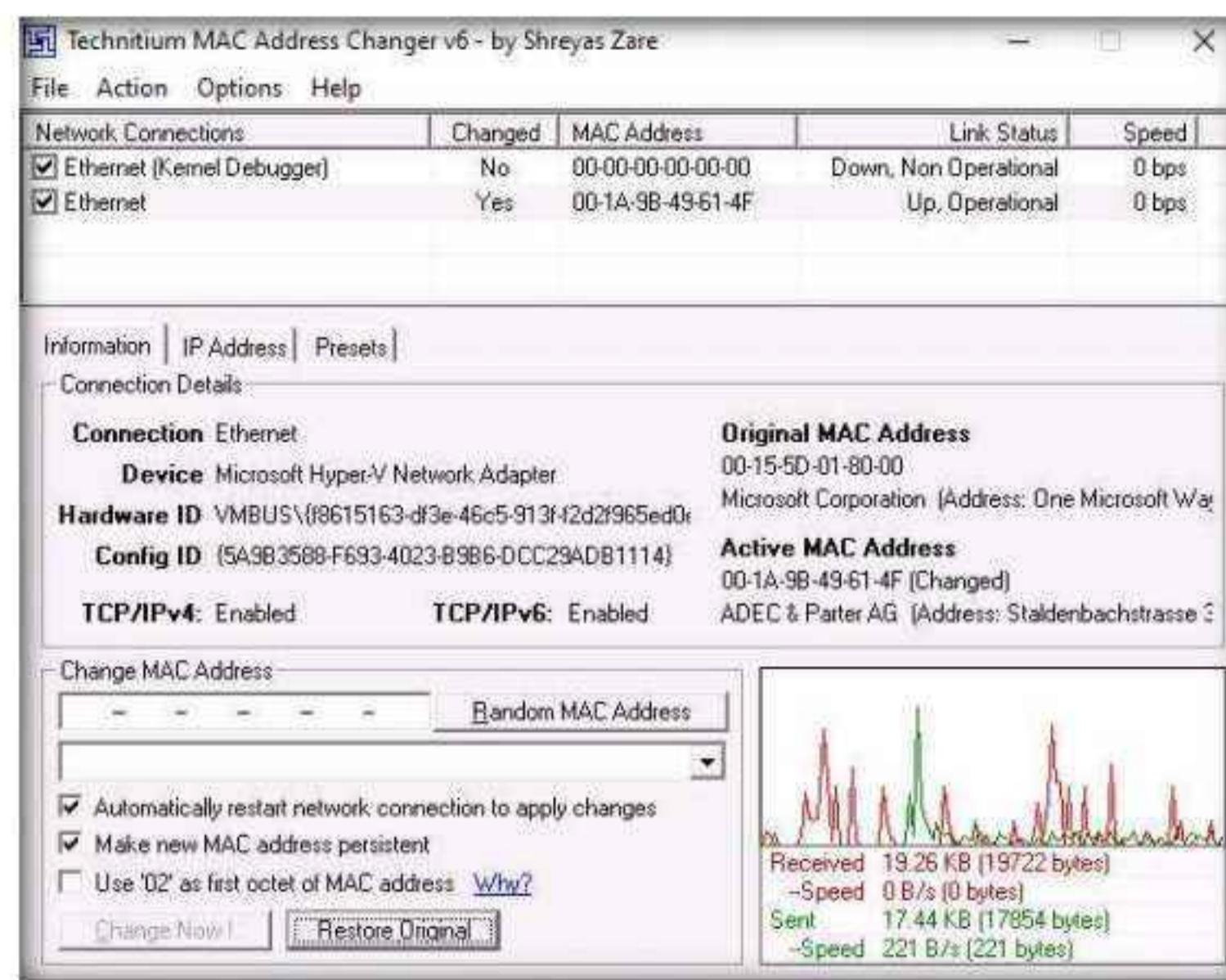
8. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.



Module 08 – Sniffing

- 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**.

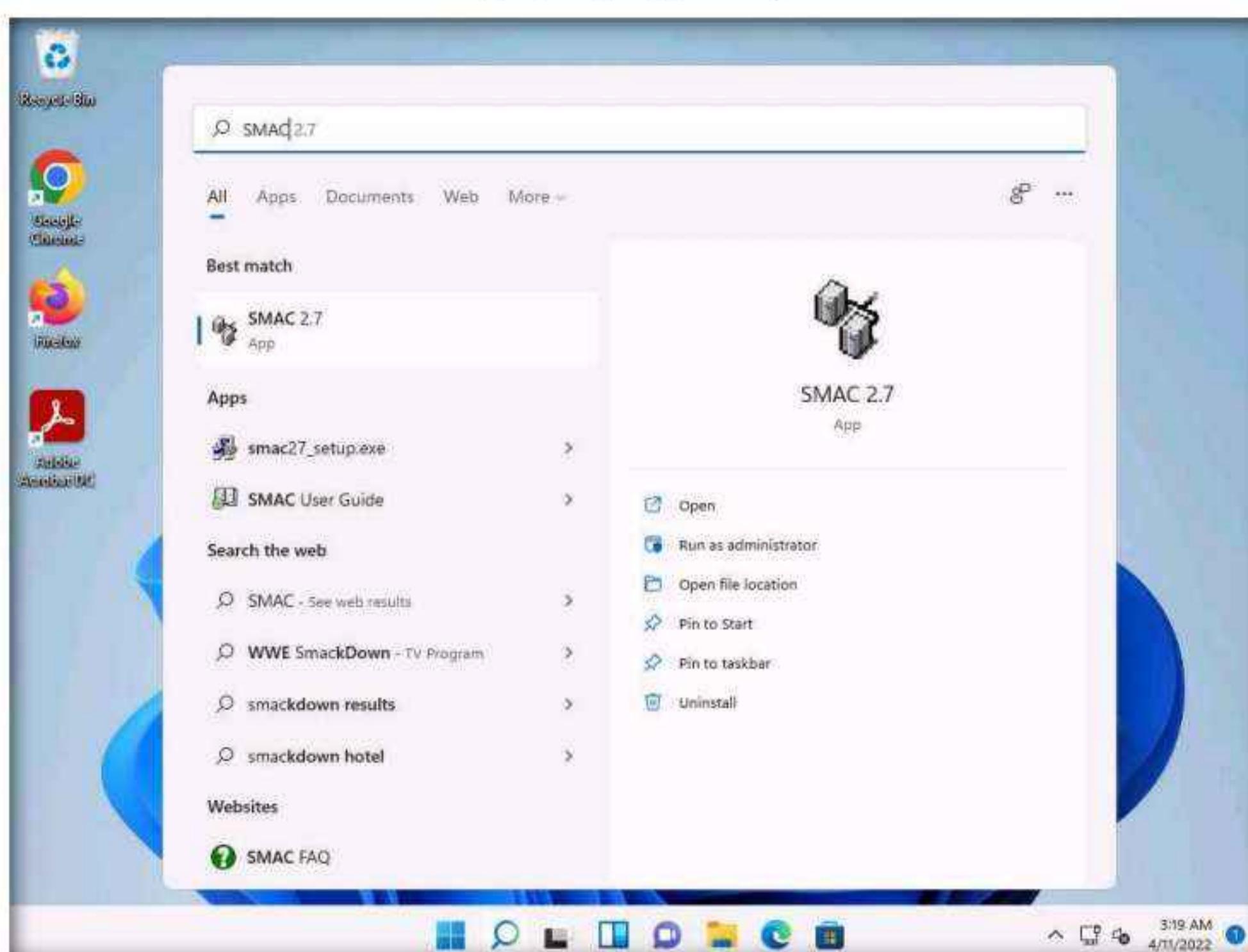


- Close the TMAC main window.

- Now, we shall perform MAC spoofing using the SMAC tool.

- 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.

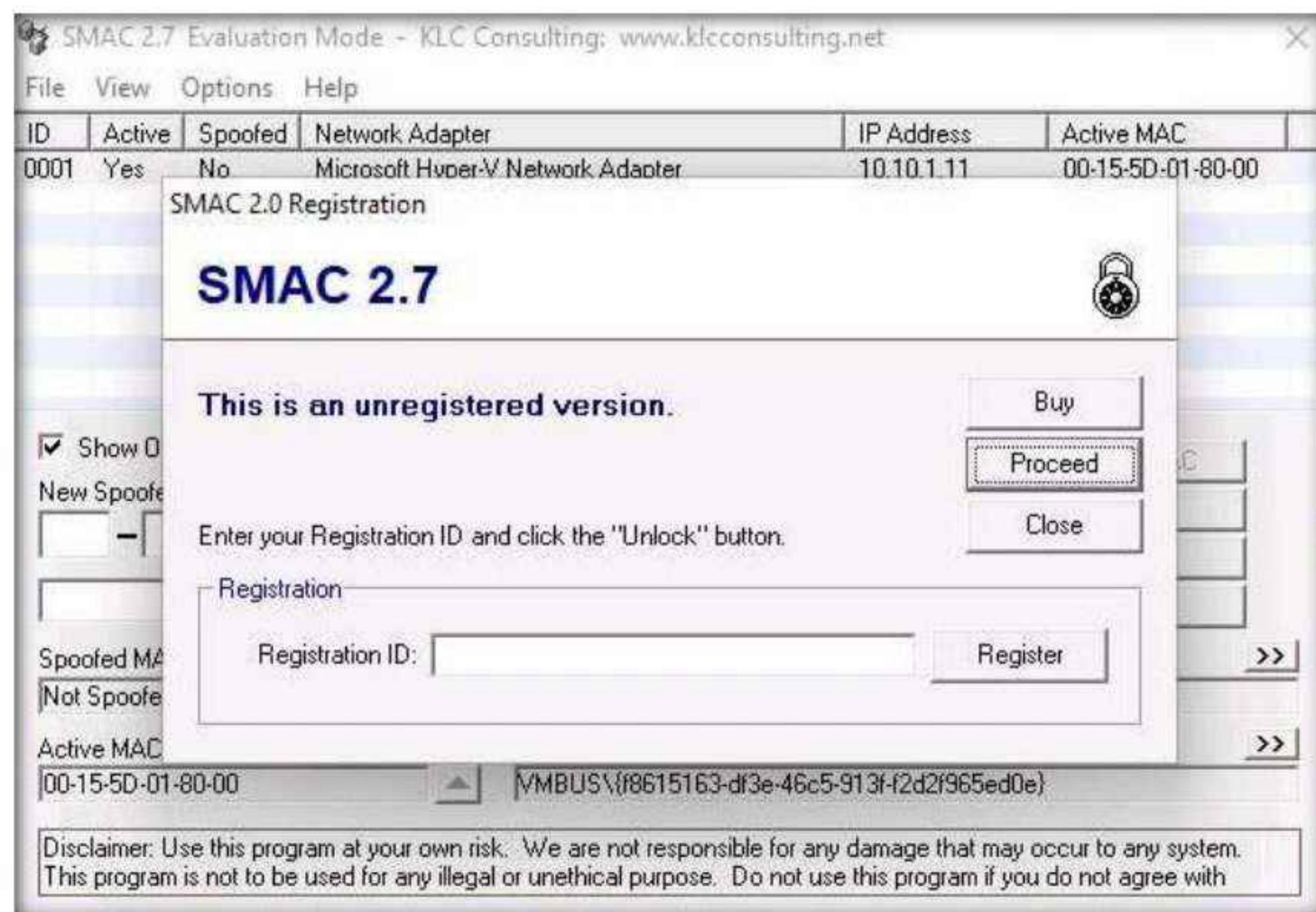
Note: If a **User Account Control** pop-up appears, click **Yes**.



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

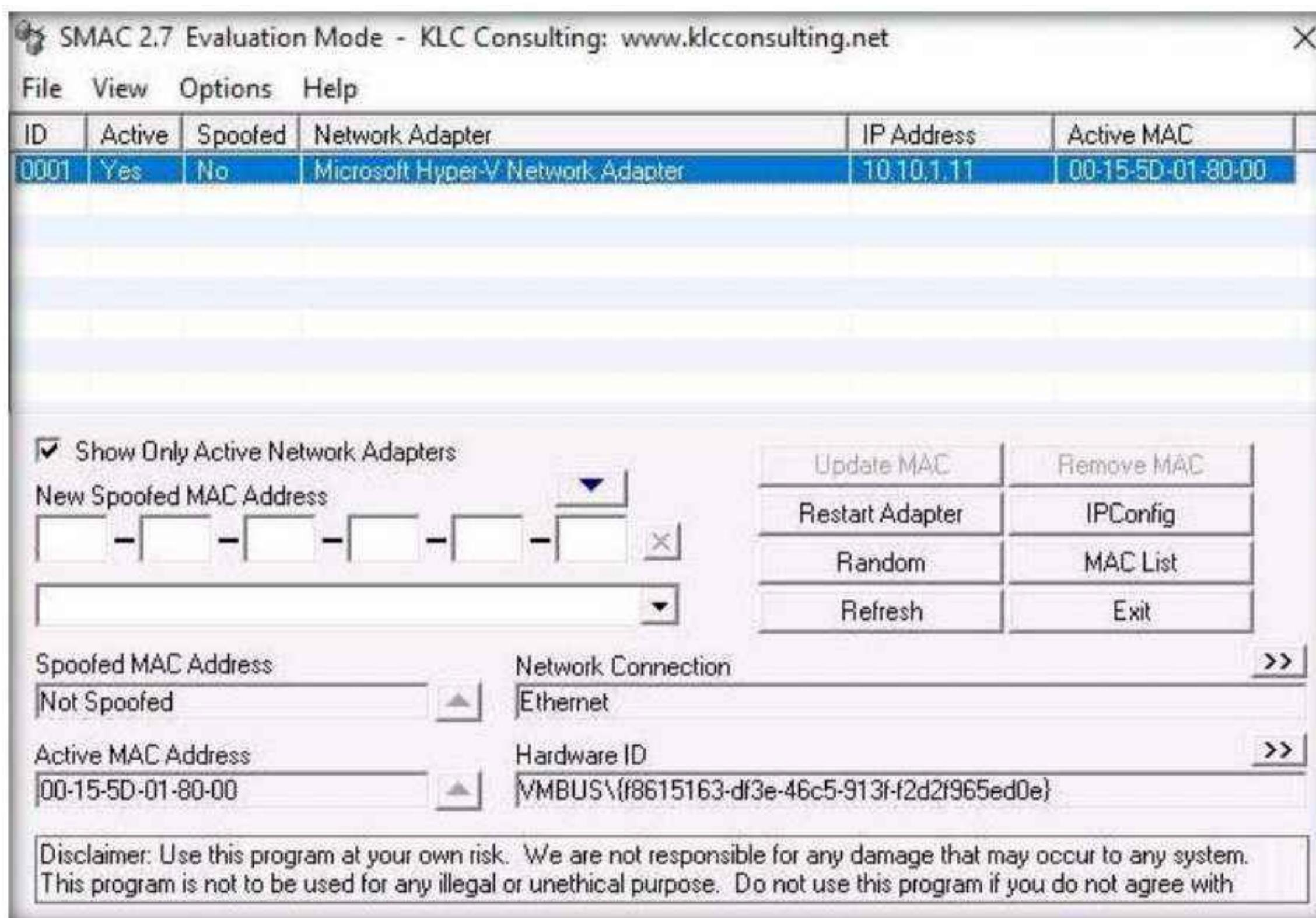


14. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.

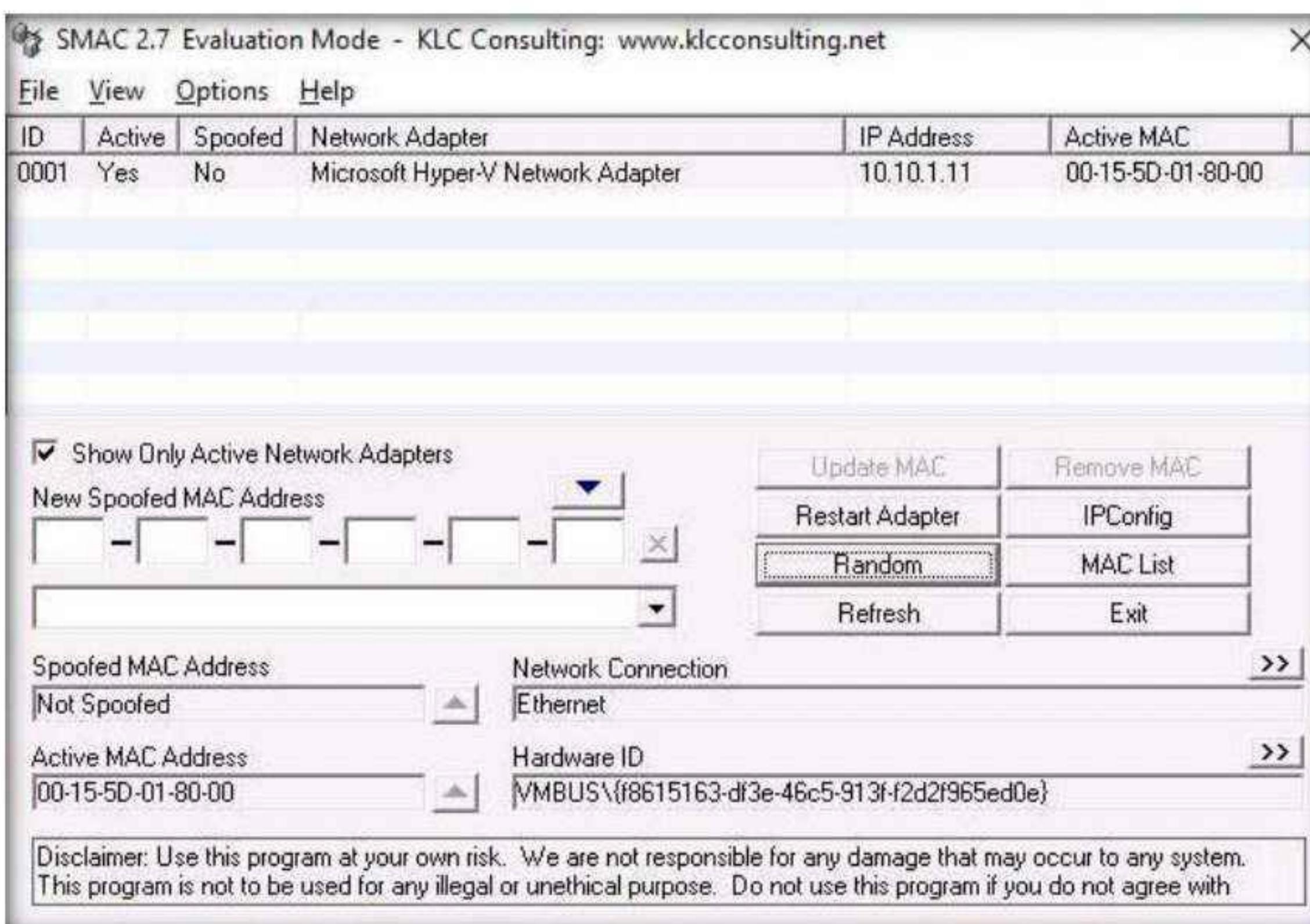


Module 08 – Sniffing

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

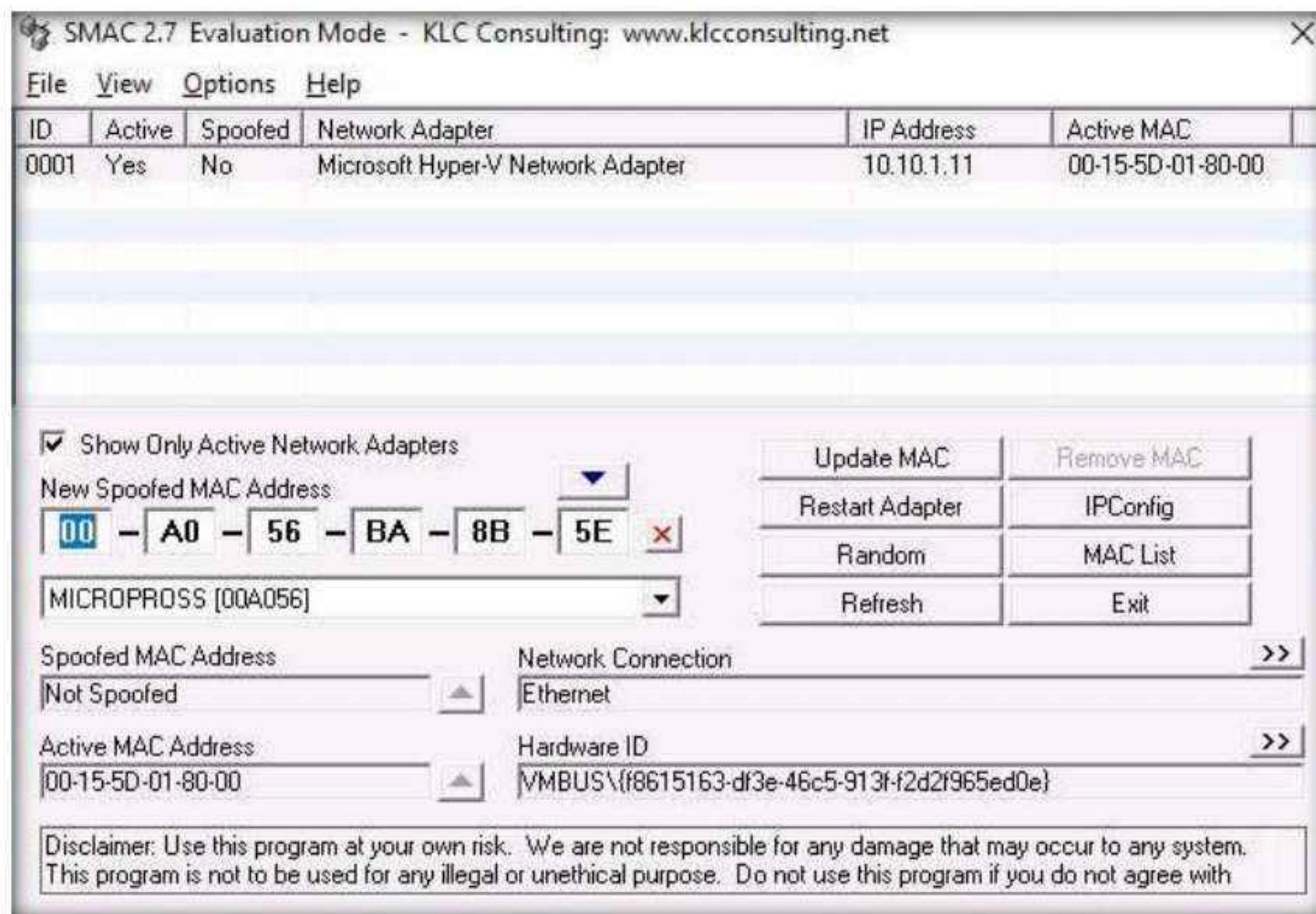


16. Click the **Random** button to generate a random MAC address.

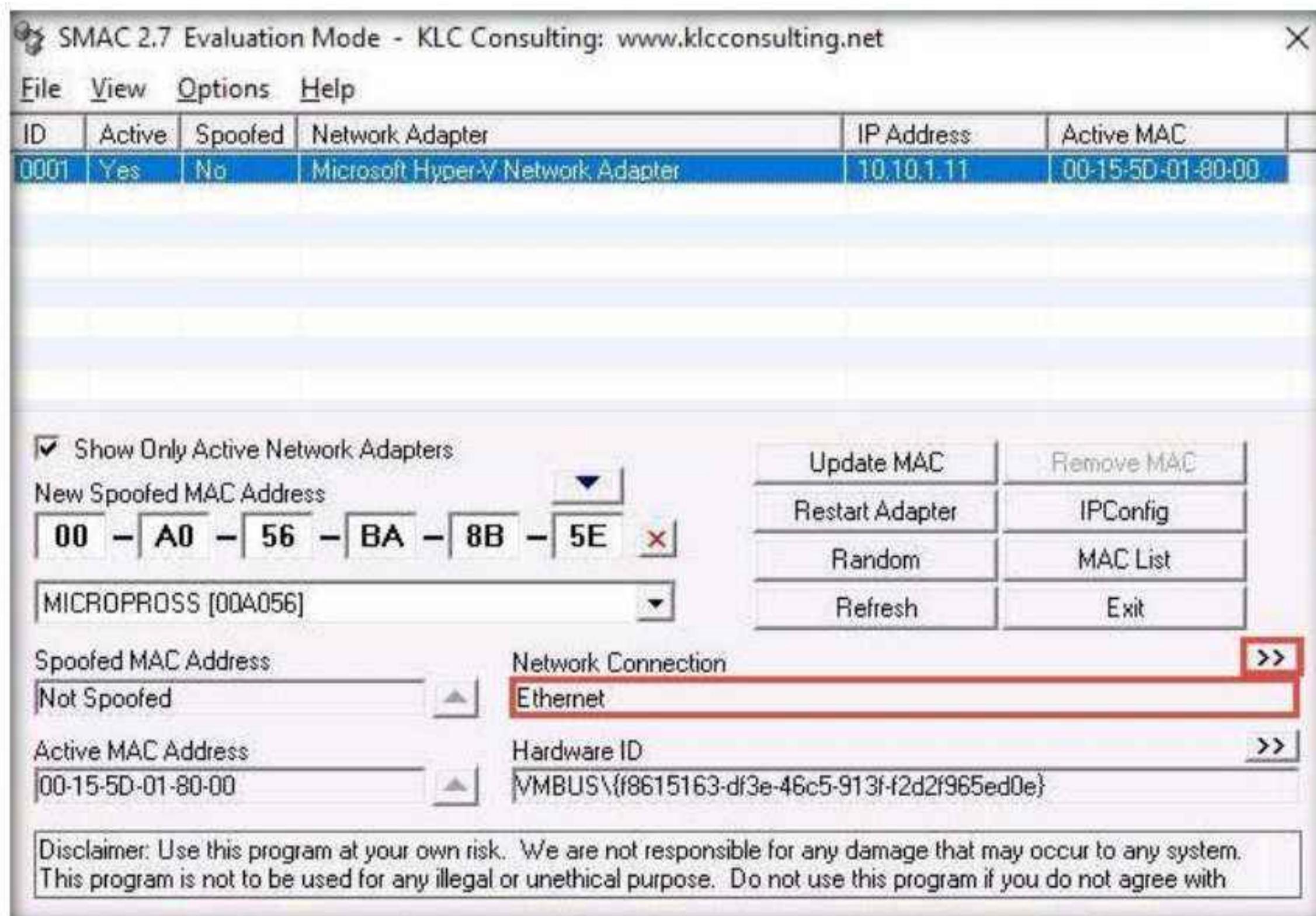


Module 08 – Sniffing

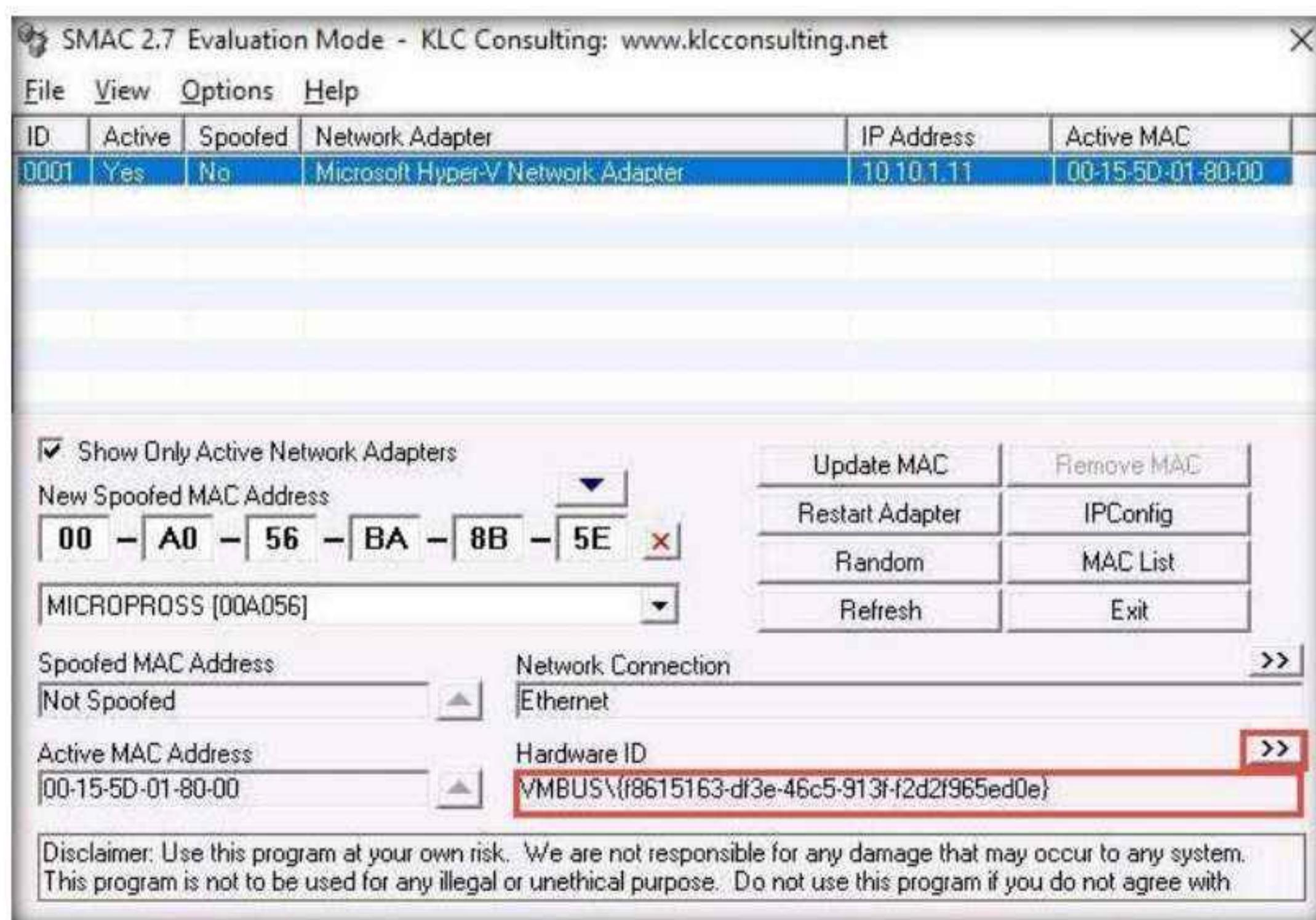
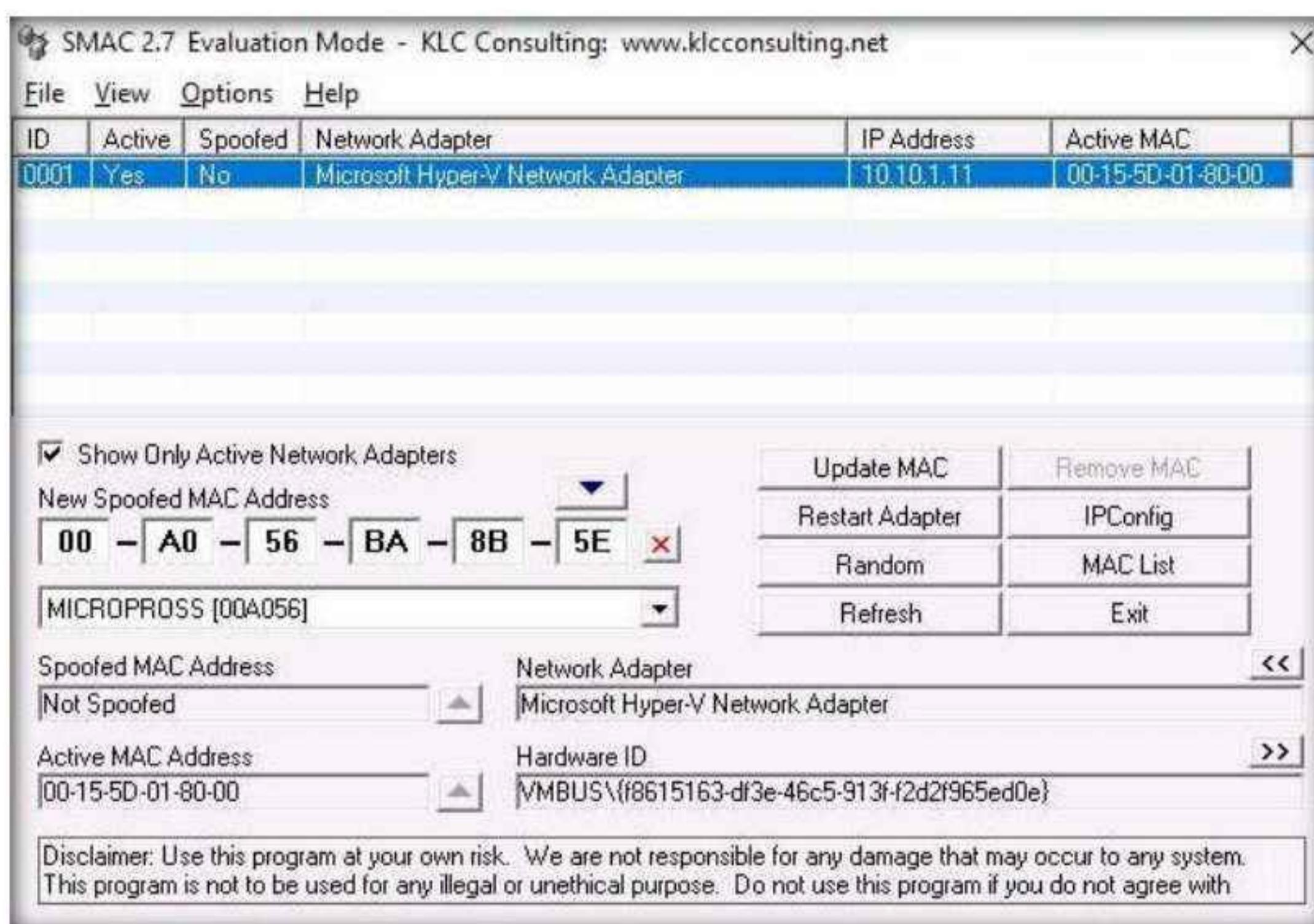
17. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.



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

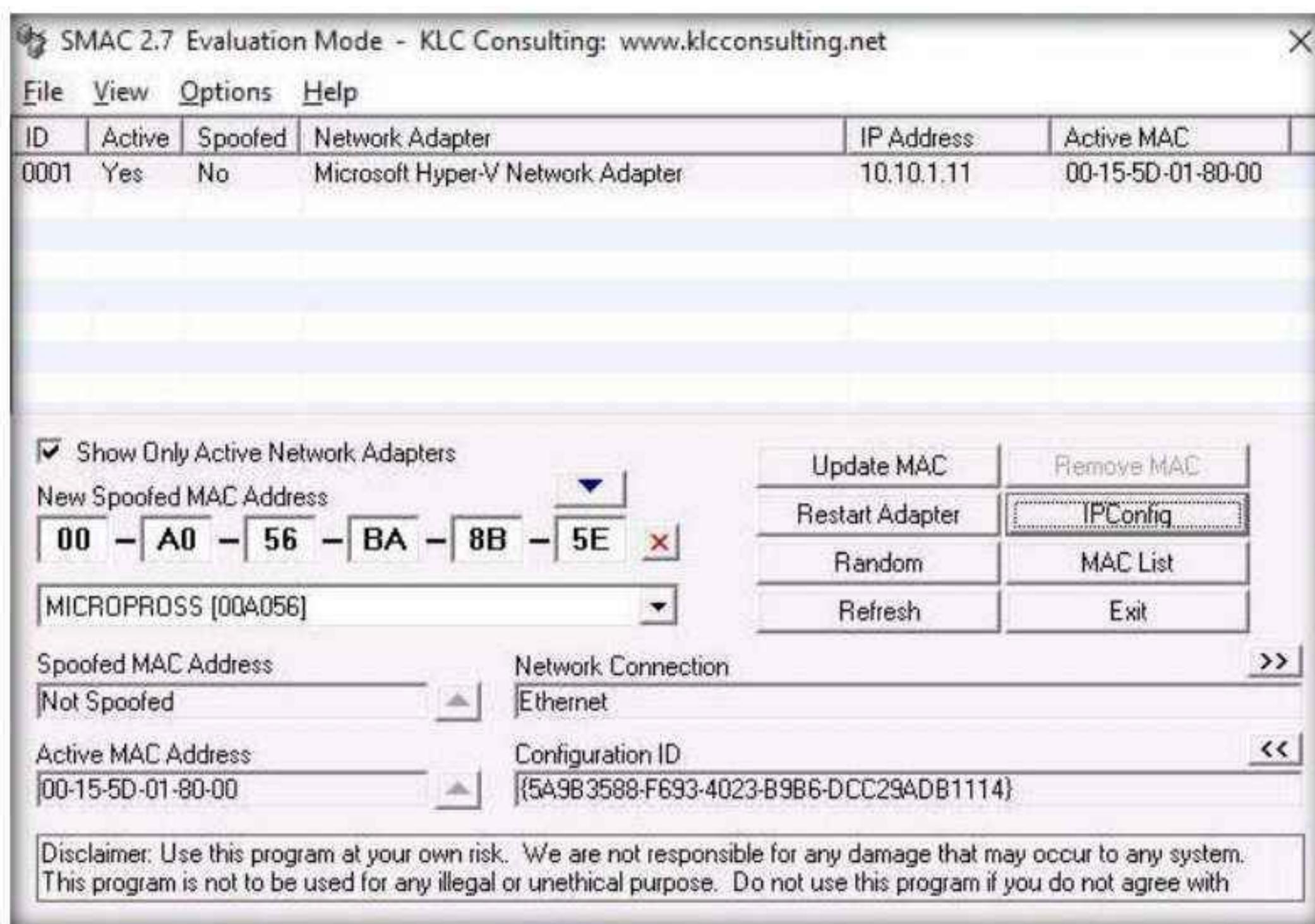


19. Clicking the back arrow (<<) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.

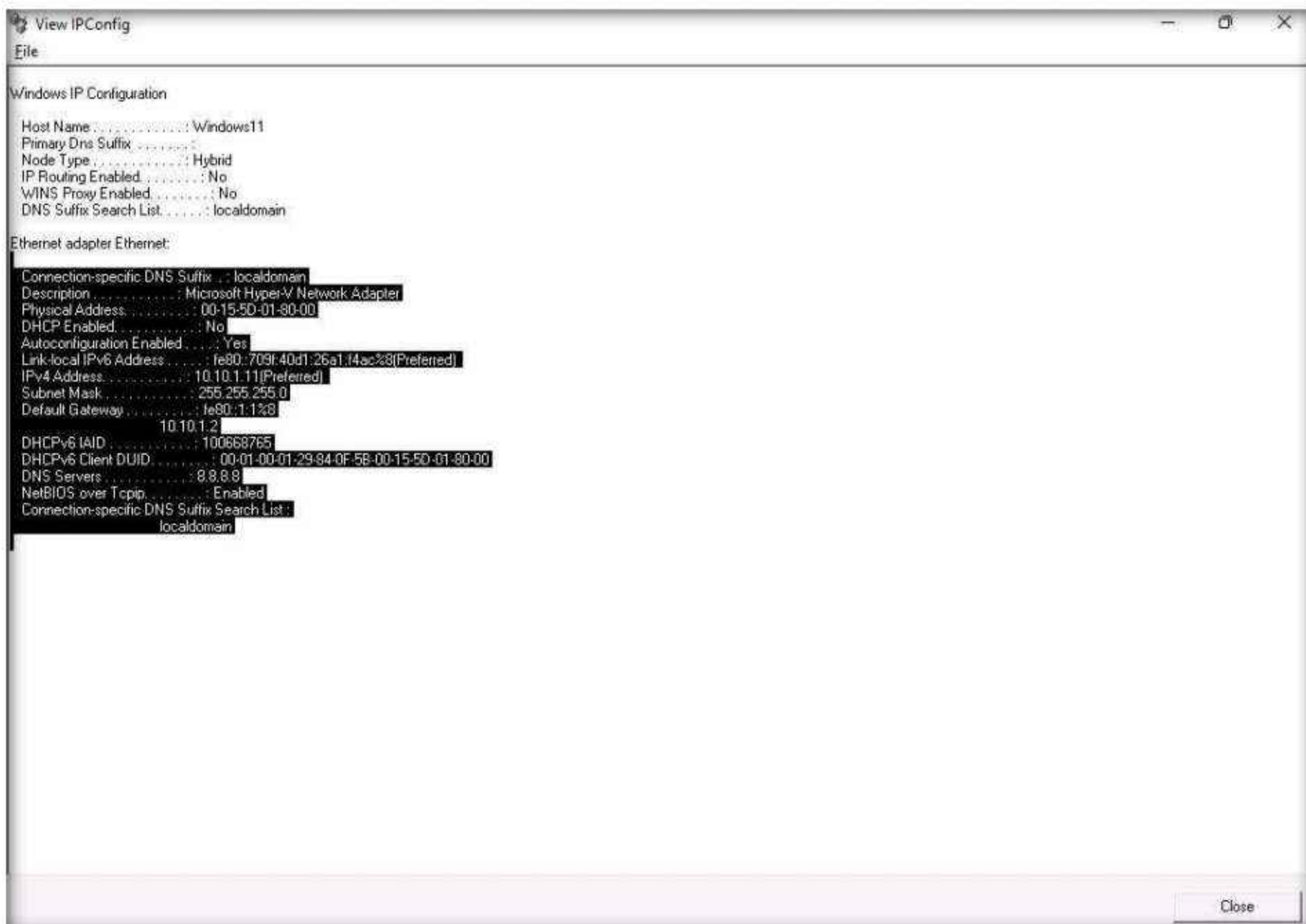


Module 08 – Sniffing

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

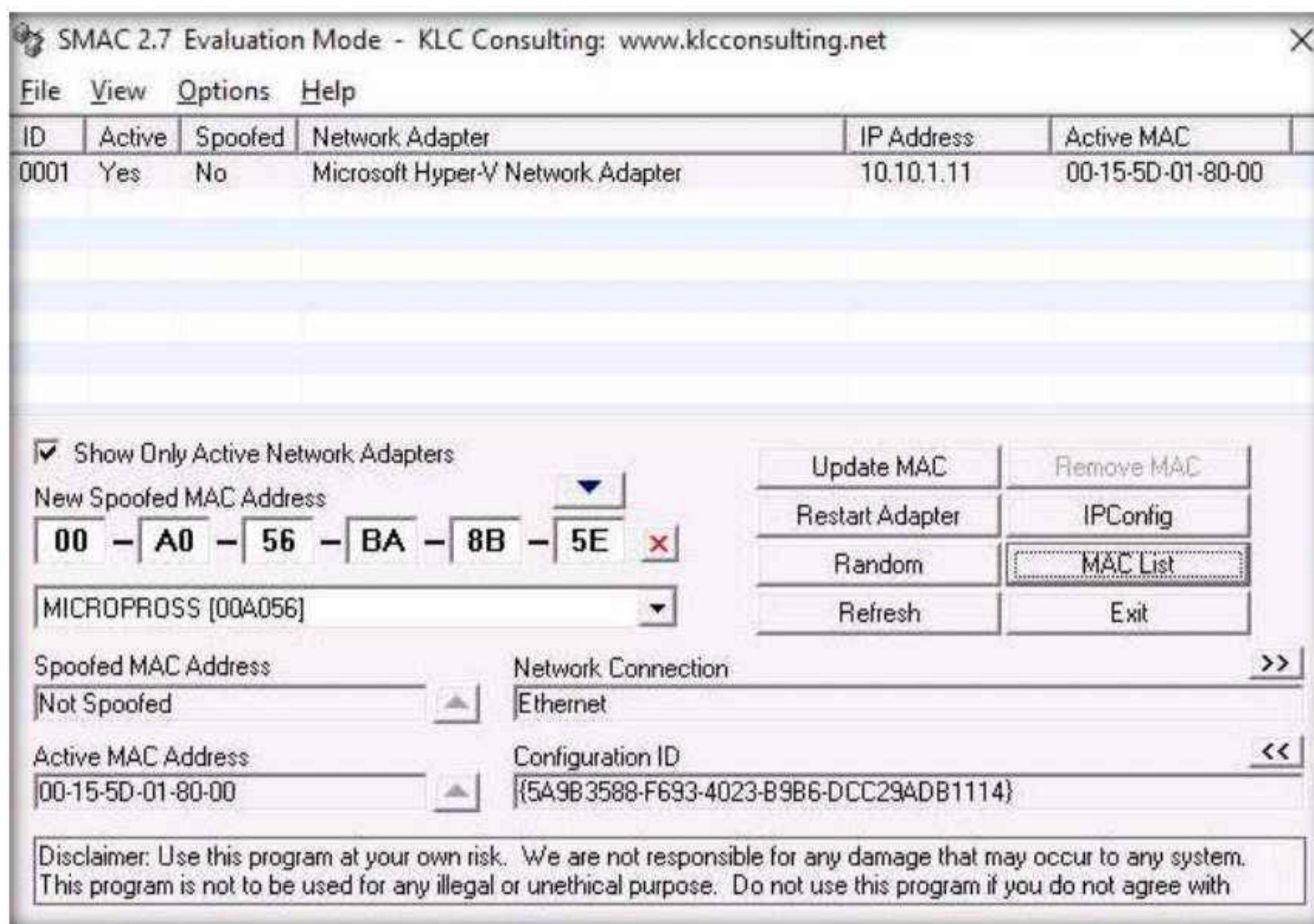


22. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.

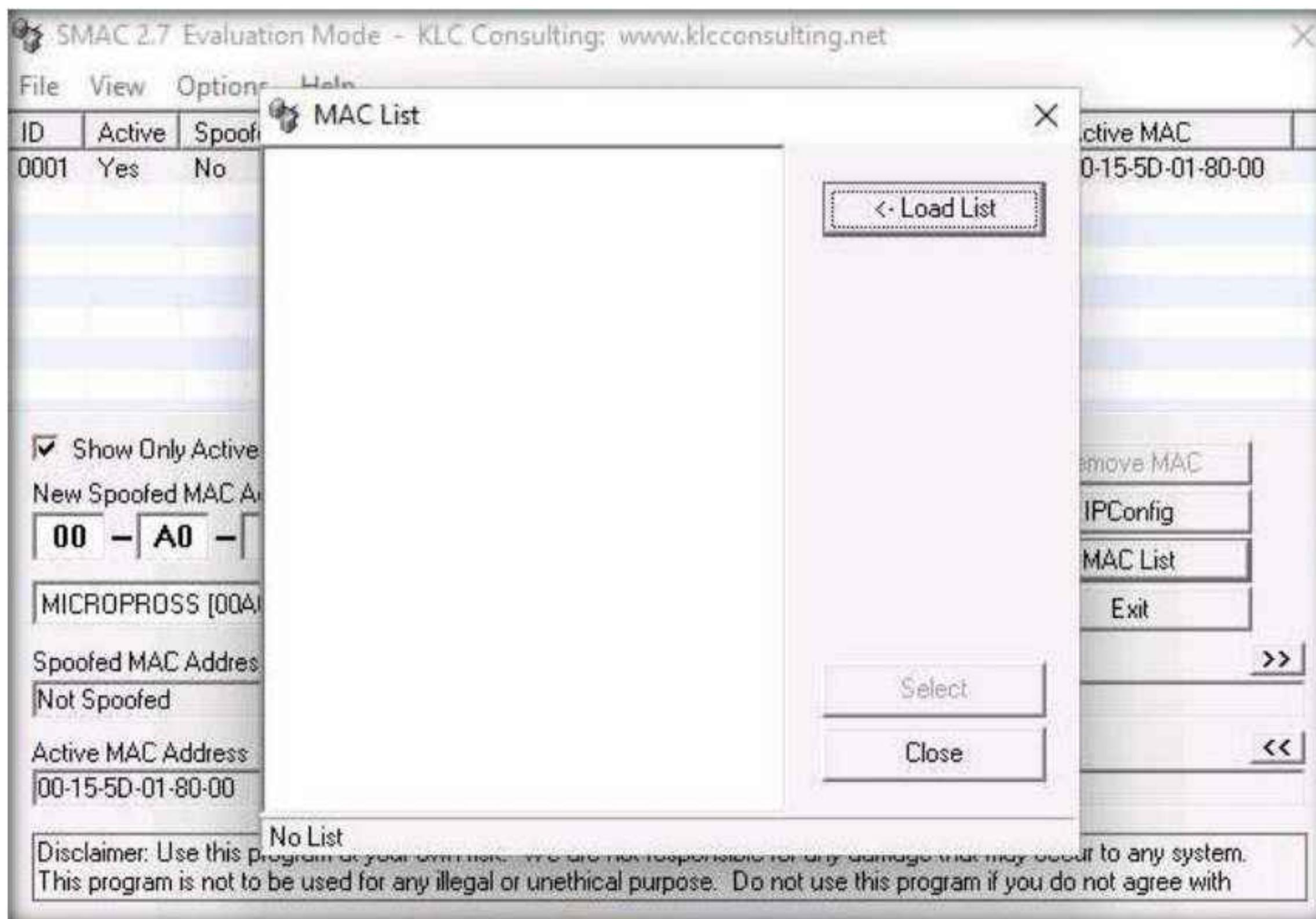


Module 08 – Sniffing

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

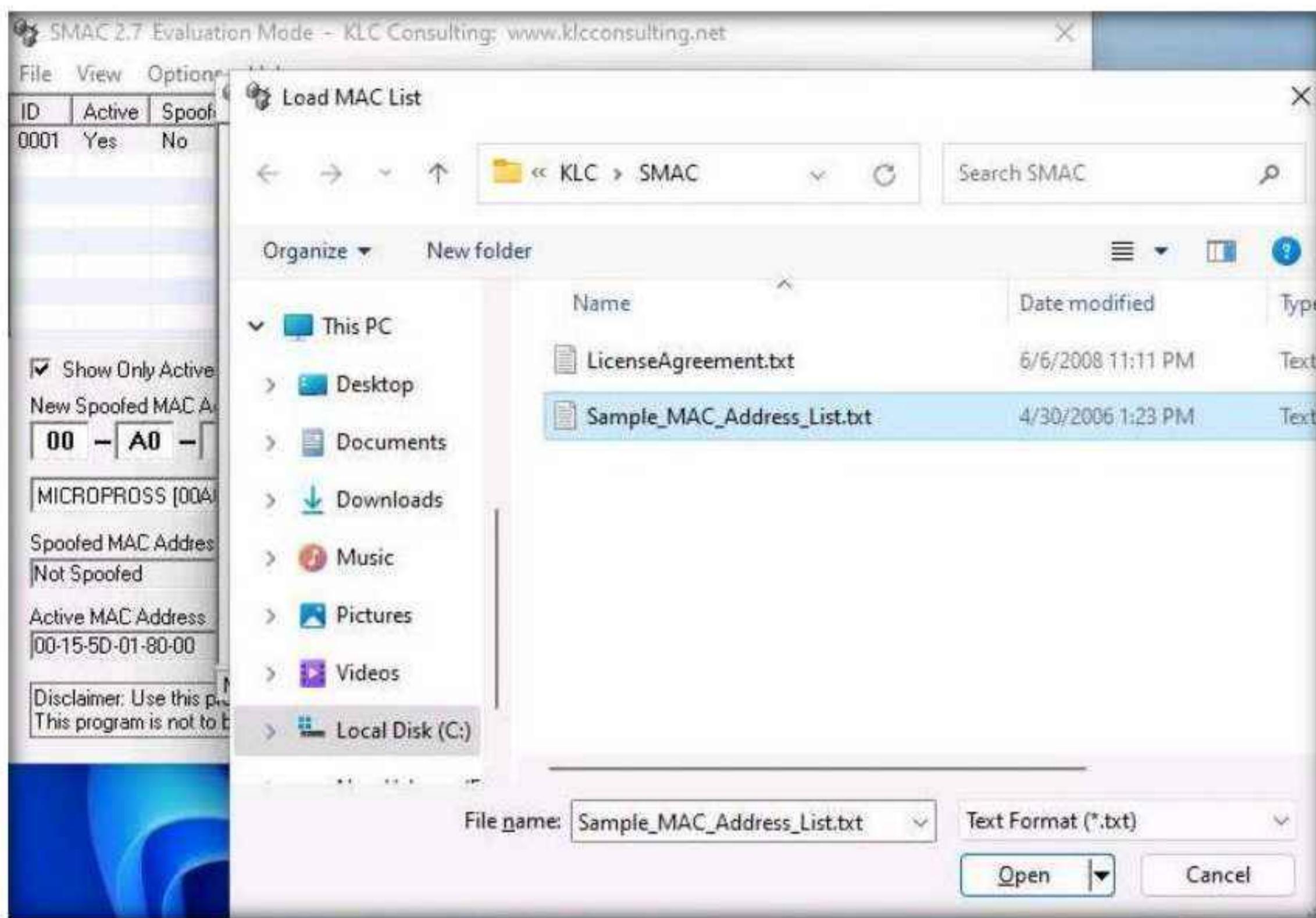


24. The **MAC List** window appears; click the **Load List** button.

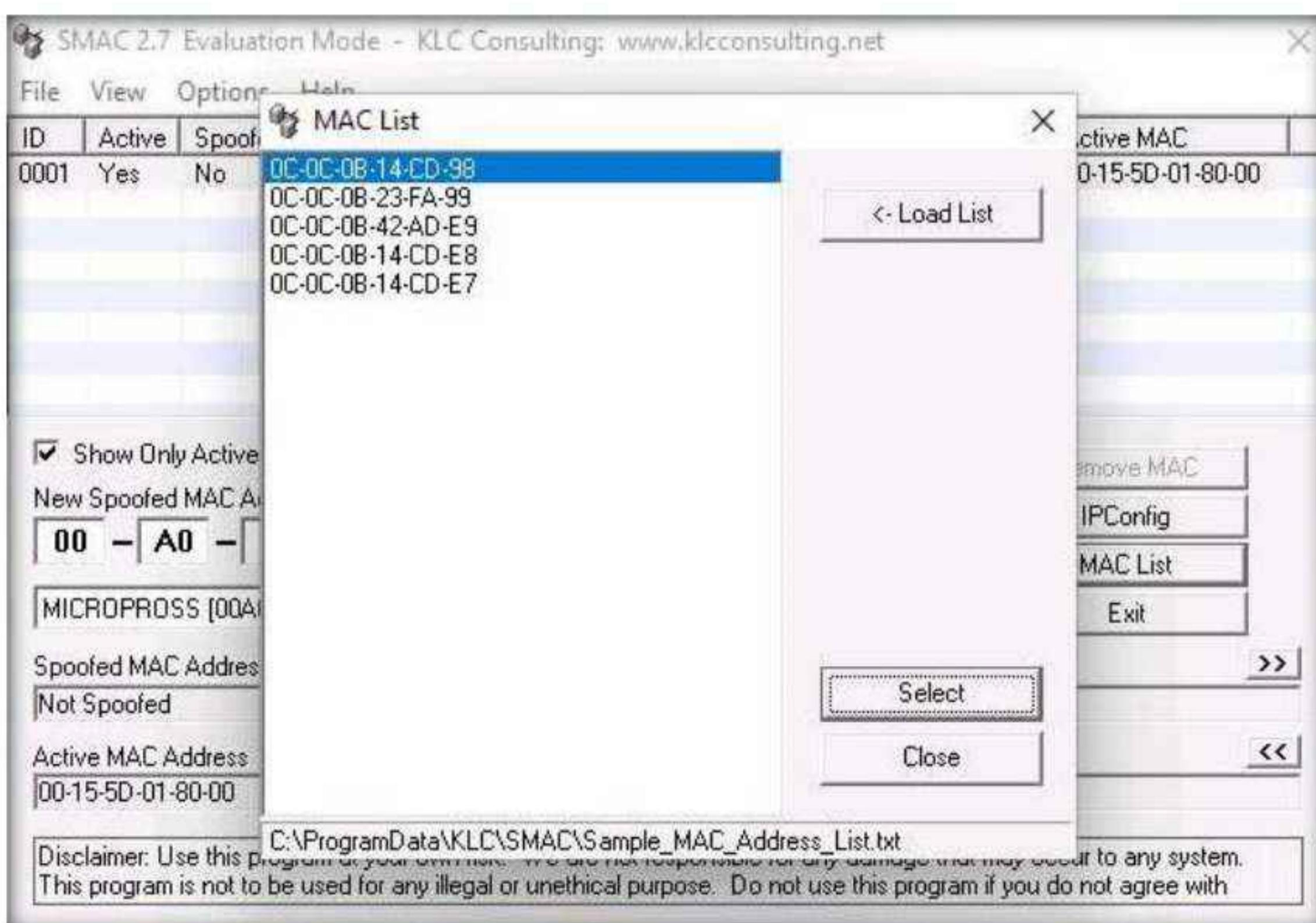


Module 08 – Sniffing

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

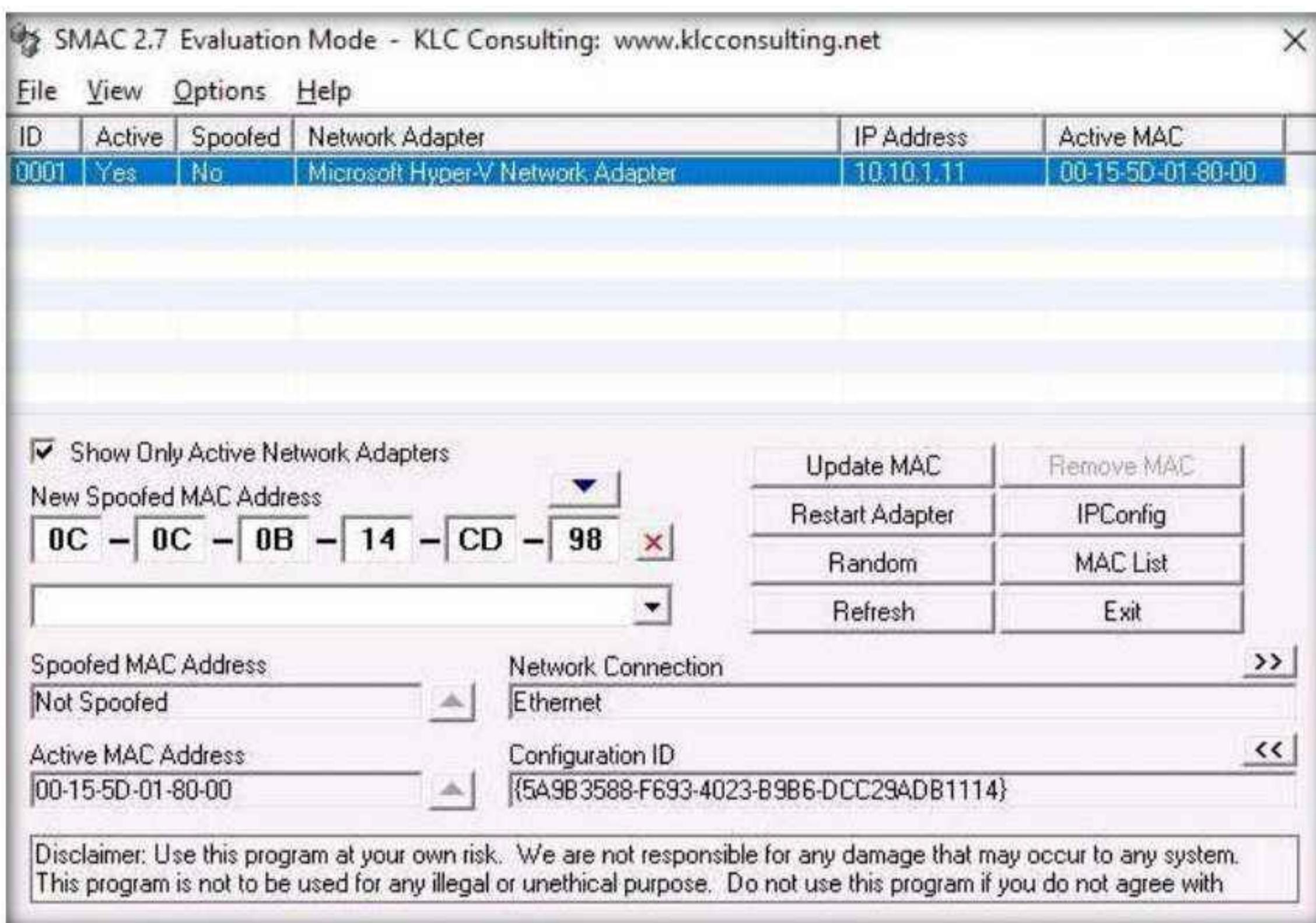


26. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.

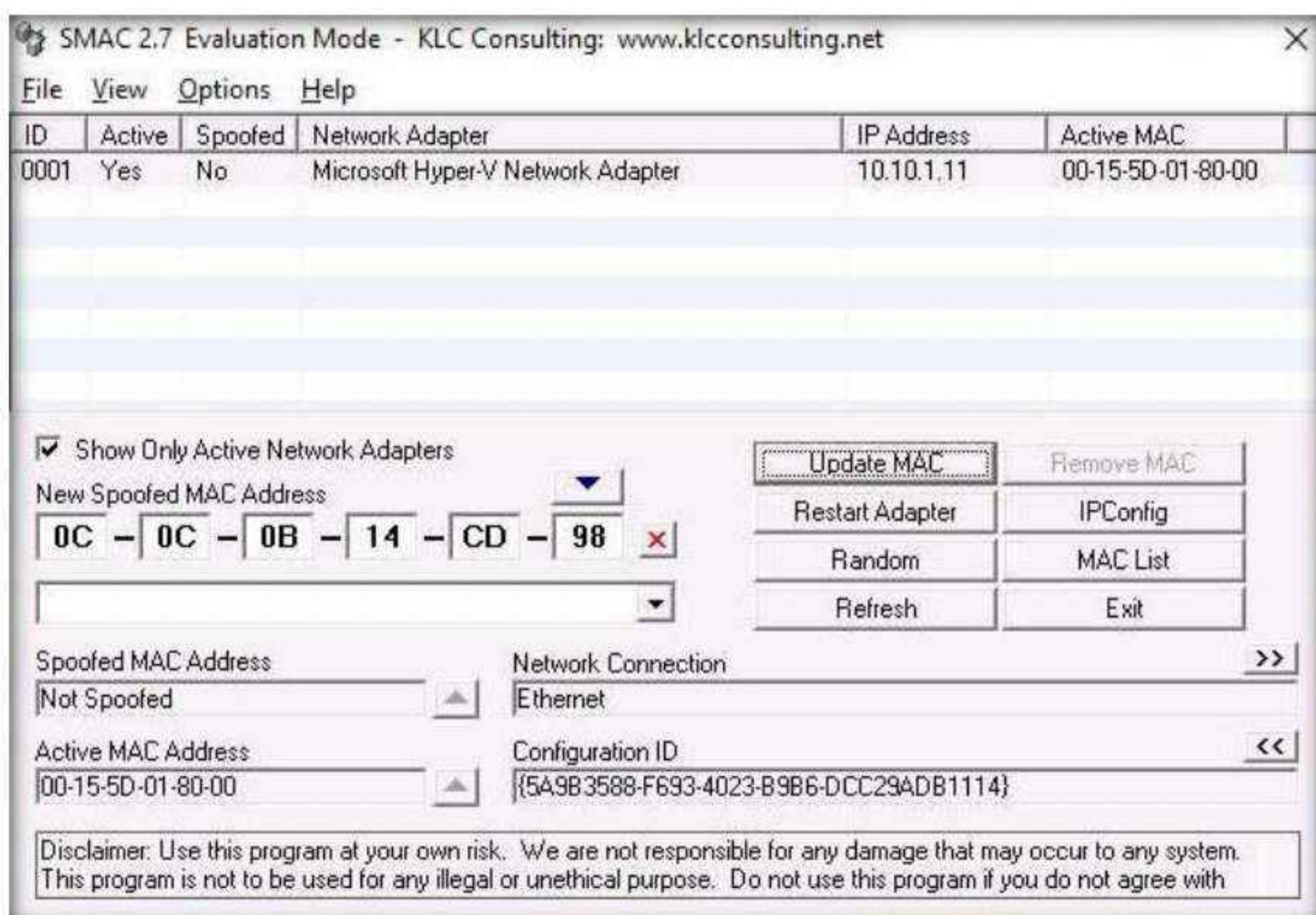


Module 08 – Sniffing

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



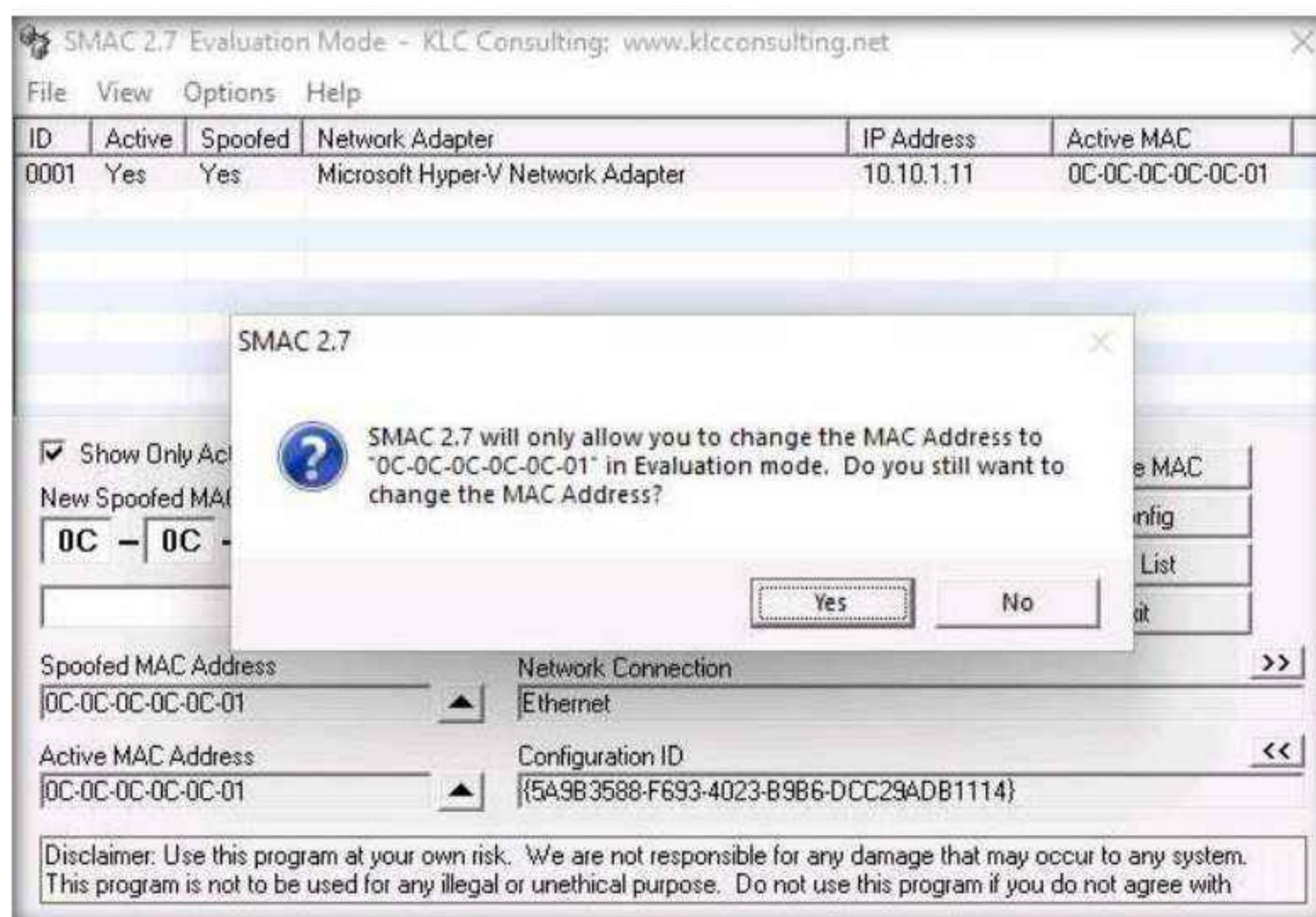
28. Click the **Update MAC** button to update the machine's MAC address information.



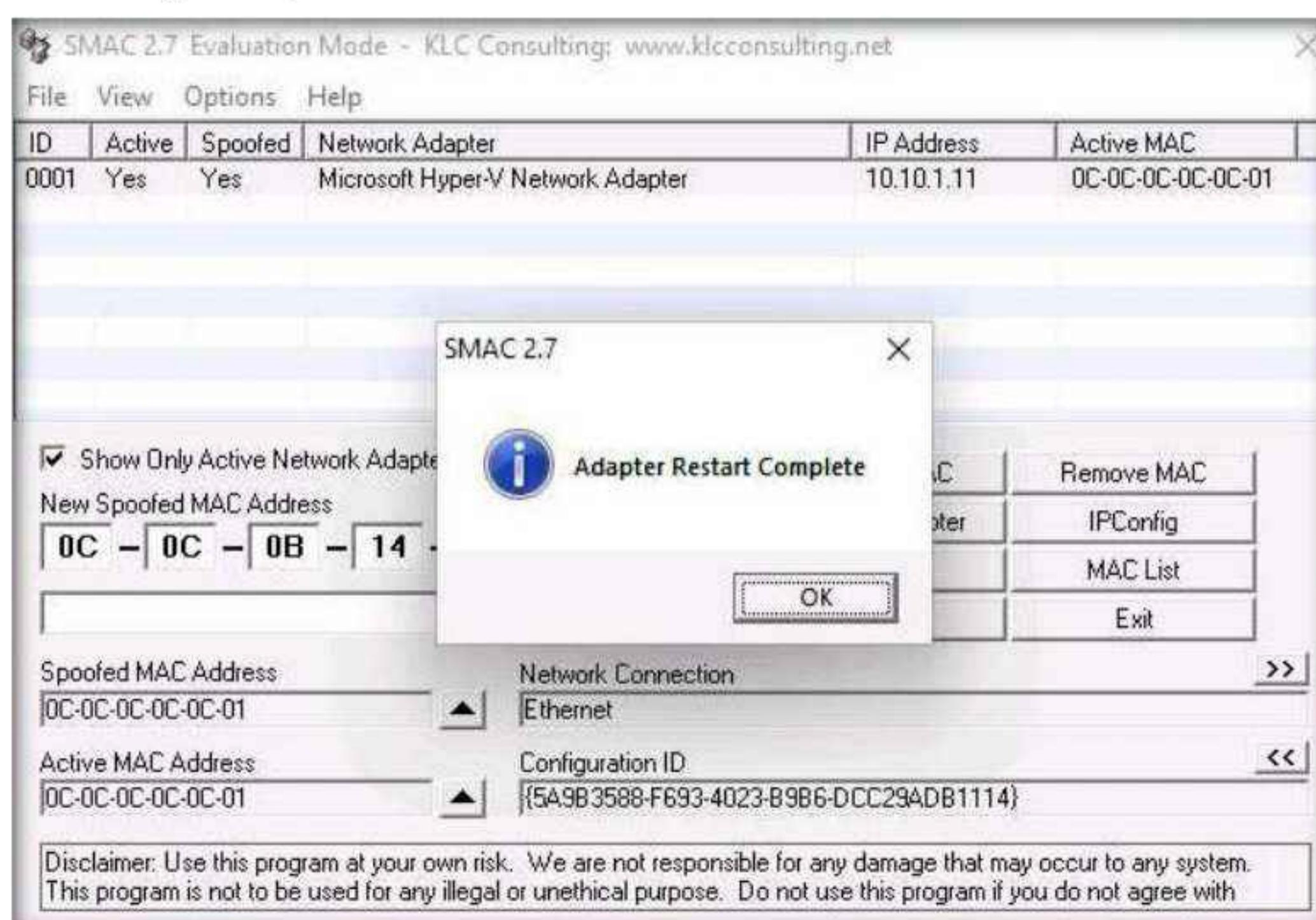
29. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

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

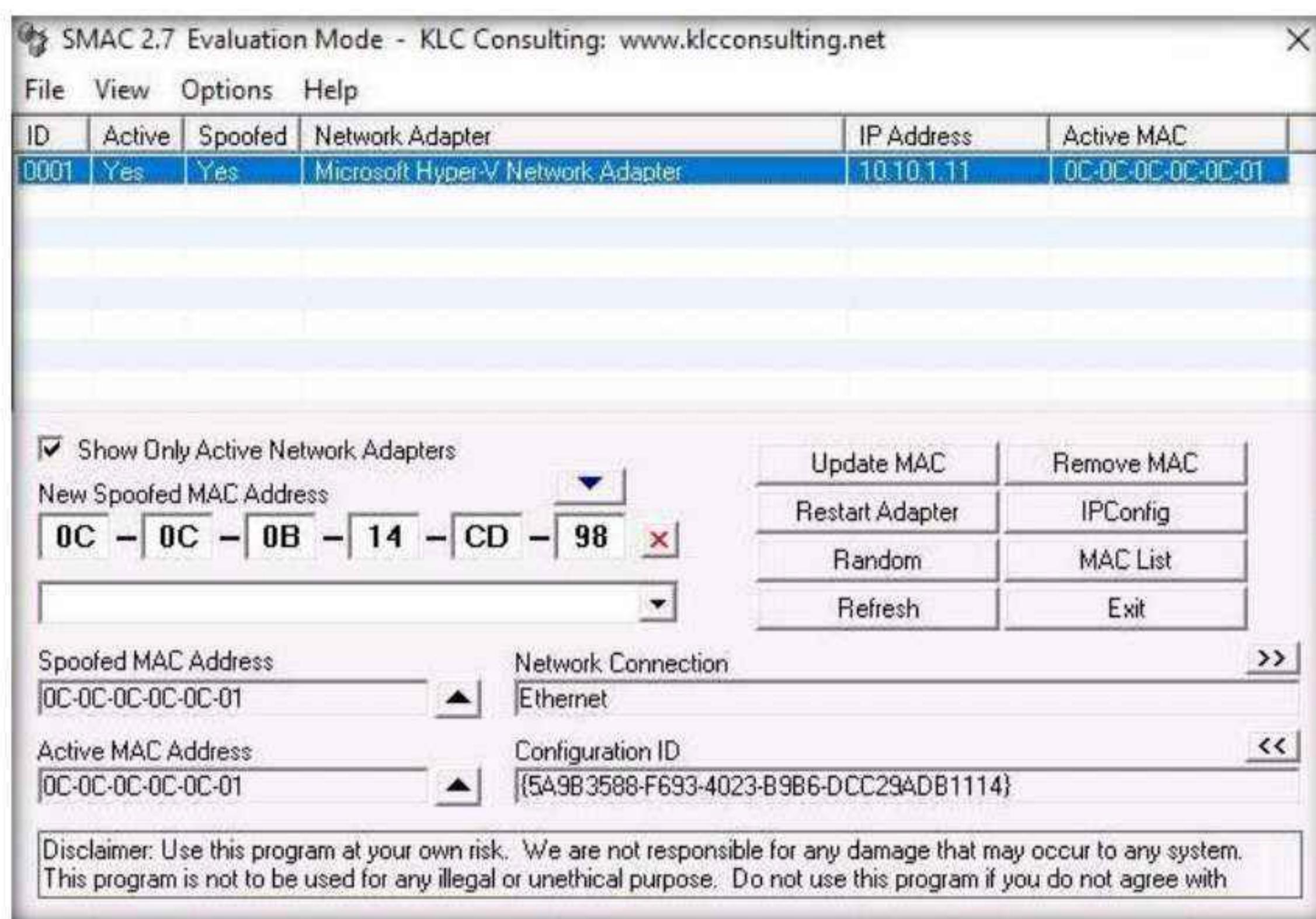
Note: In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.



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

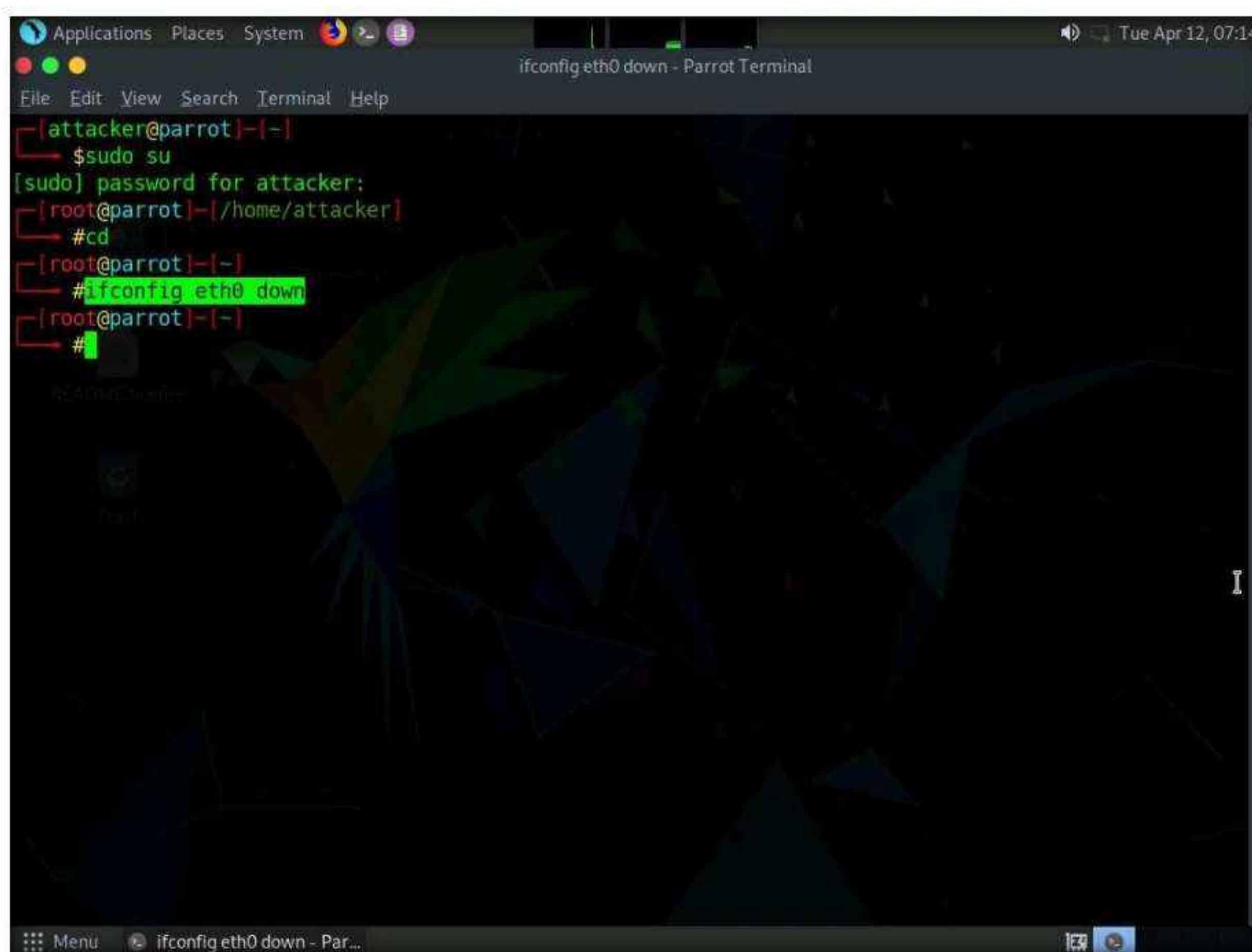
1. Turn on the **Parrot Security** virtual machine.

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.



```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# ifconfig eth0 down
[root@parrot] ~
#
```

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

```
macchanger --help - Parrot Terminal

[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# ifconfig eth0 down
[root@parrot] ~
# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --ending         Don't change the vendor bytes
-a, --another        Set random vendor MAC of the same kind
-A, --permanent      Set random vendor MAC of any kind
-p, --permanent      Reset to original, permanent hardware MAC
-r, --random         Set fully random MAC
-l, --list[=keyword] Print known vendors
-b, --bia            Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
[root@parrot] ~
#
```

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.

```
macchanger -s eth0 - Parrot Terminal

[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# ifconfig eth0 down
[root@parrot] ~
# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --ending         Don't change the vendor bytes
-a, --another        Set random vendor MAC of the same kind
-A, --permanent      Set random vendor MAC of any kind
-p, --permanent      Reset to original, permanent hardware MAC
-r, --random         Set fully random MAC
-l, --list[=keyword] Print known vendors
-b, --bia            Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
[root@parrot] ~
# macchanger -s eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
[root@parrot] ~
#
```

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.

```
Applications Places System macchanger -a eth0 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~
#macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --ending         Don't change the vendor bytes
-a, --another        Set random vendor MAC of the same kind
-A                 Set random vendor MAC of any kind
-p, --permanent     Reset to original, permanent hardware MAC
-r, --random         Set fully random MAC
-l, --list[=keyword] Print known vendors
-b, --bia            Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
[root@parrot] ~
#macchanger -s eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
[root@parrot] ~
#macchanger -a eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
New MAC: 00:30:a0:27:e2:f1 (TYCO SUBMARINE SYSTEMS, LTD.)
[root@parrot] ~
#
```

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

```
Applications Places System macchanger -r eth0 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~
#macchanger -r eth0
Current MAC: 00:30:a0:27:e2:f1 (TYCO SUBMARINE SYSTEMS, LTD.)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
New MAC: da:ef:95:36:55:44 (unknown)
[root@parrot] ~
#
```

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**.

```
[root@parrot]~[~]
[root@parrot]~[~]# ifconfig eth0 up
[root@parrot]~[~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.255.0 broadcast 10.10.1.255
        inet6 fe80::deb2:9b3b:5490:d89b prefixlen 64 scopeid 0x20<link>
            ether da:ef:95:36:55:44 txqueuelen 1000 (Ethernet)
            RX packets 6852 bytes 9043921 (8.6 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 892 bytes 81958 (80.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 20 bytes 1168 (1.1 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 20 bytes 1168 (1.1 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

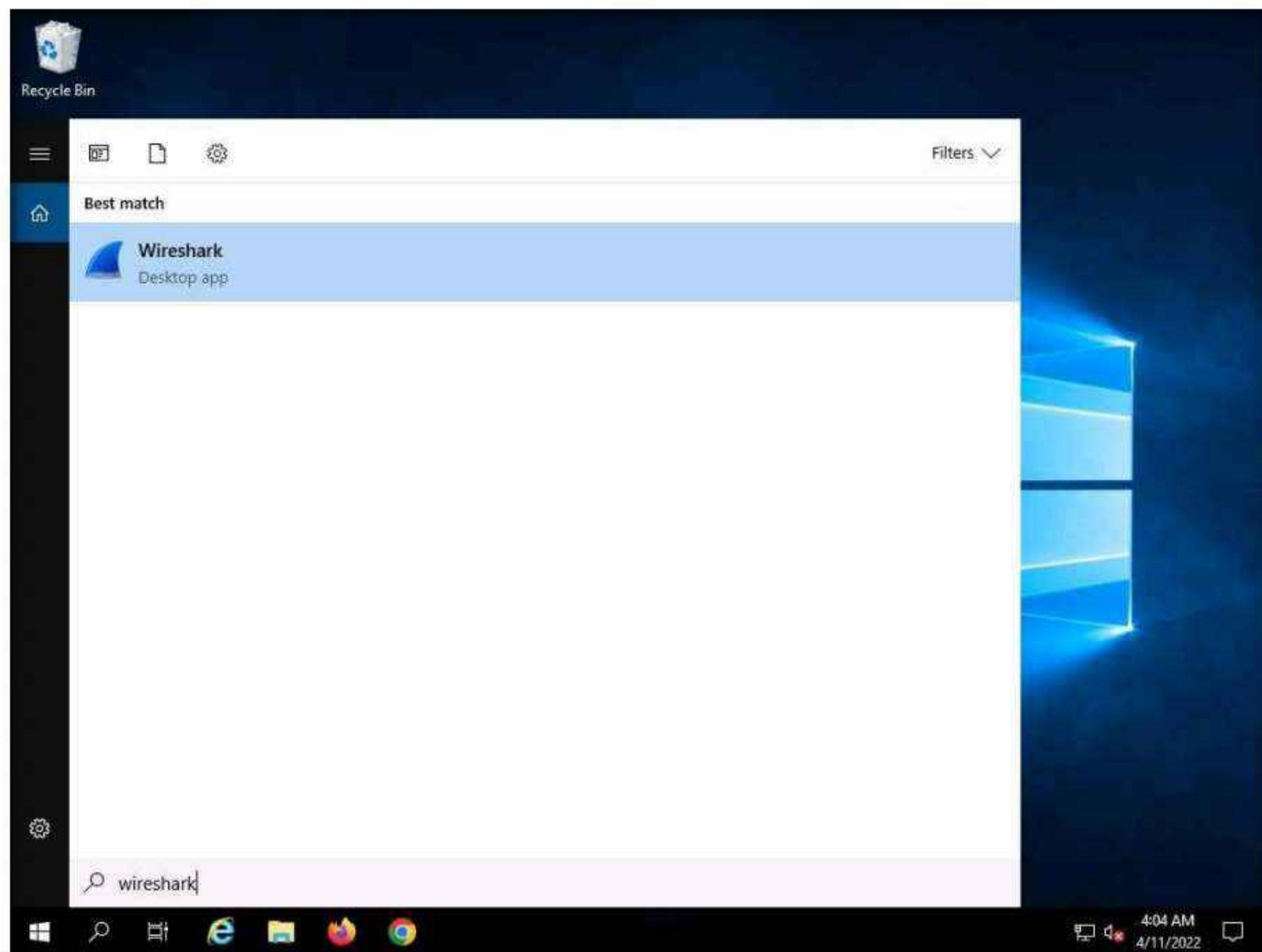
Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI 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.

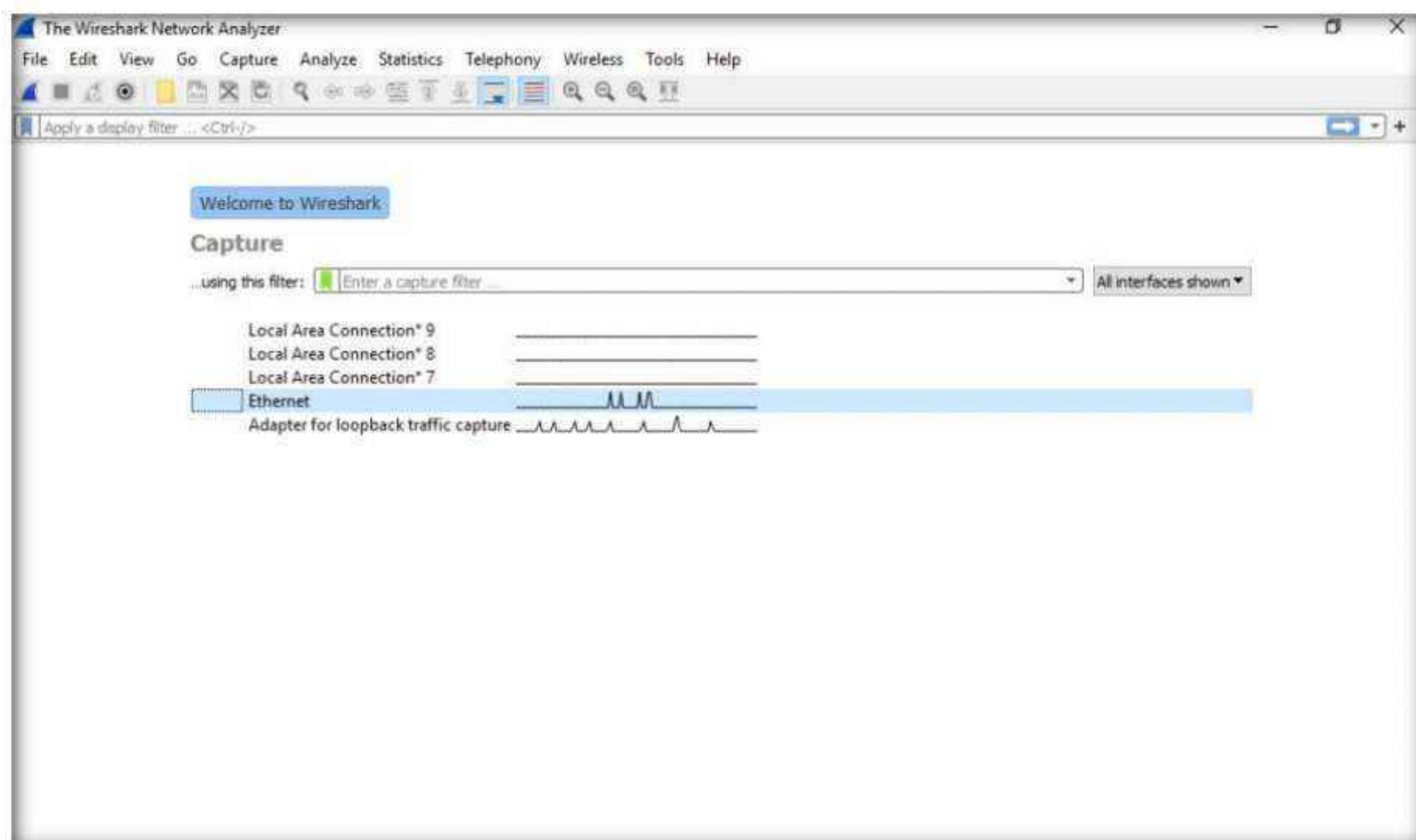
1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** 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**.

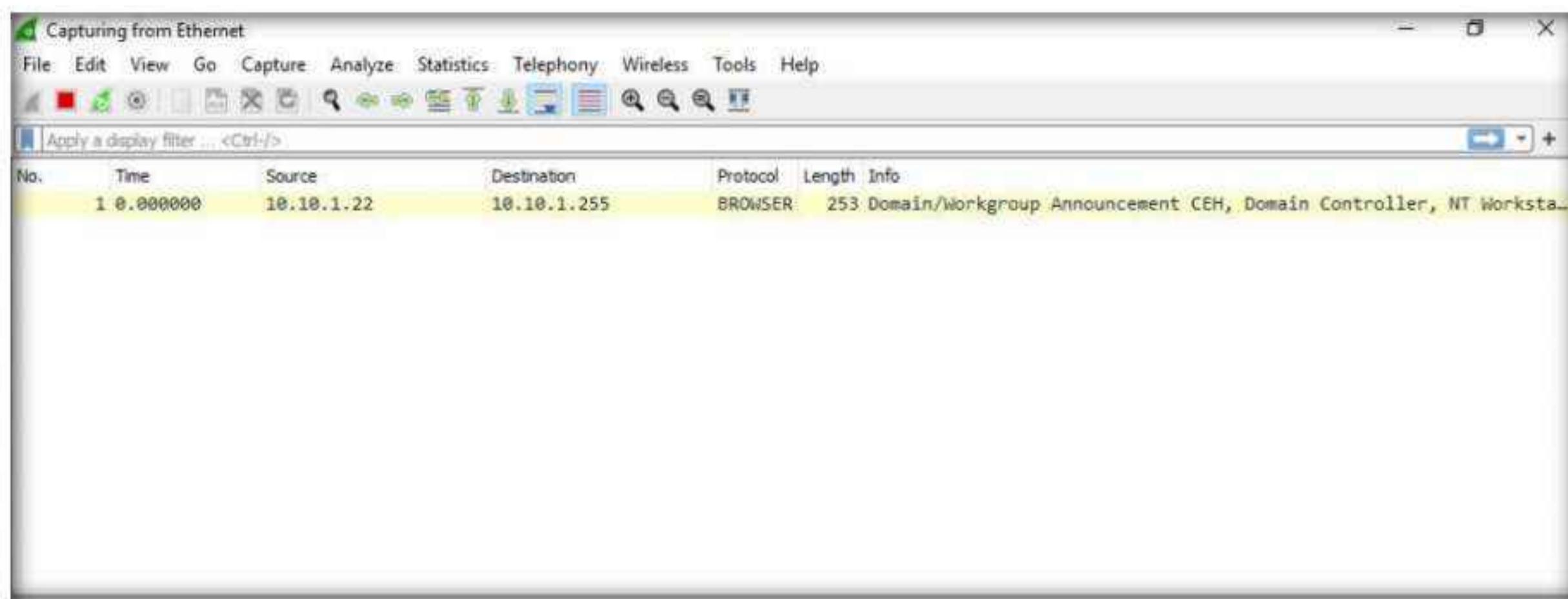


4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

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



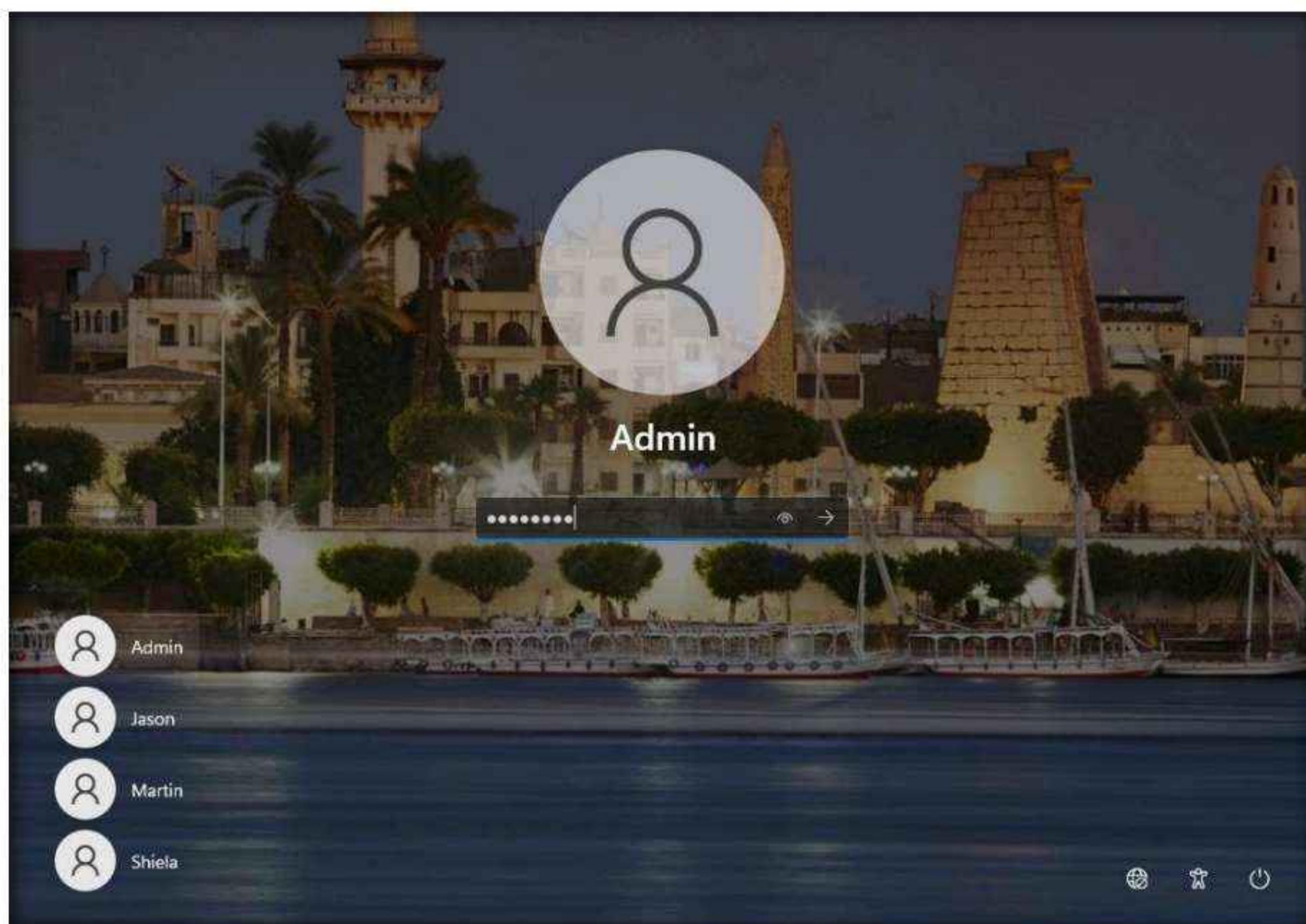
5. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.



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.

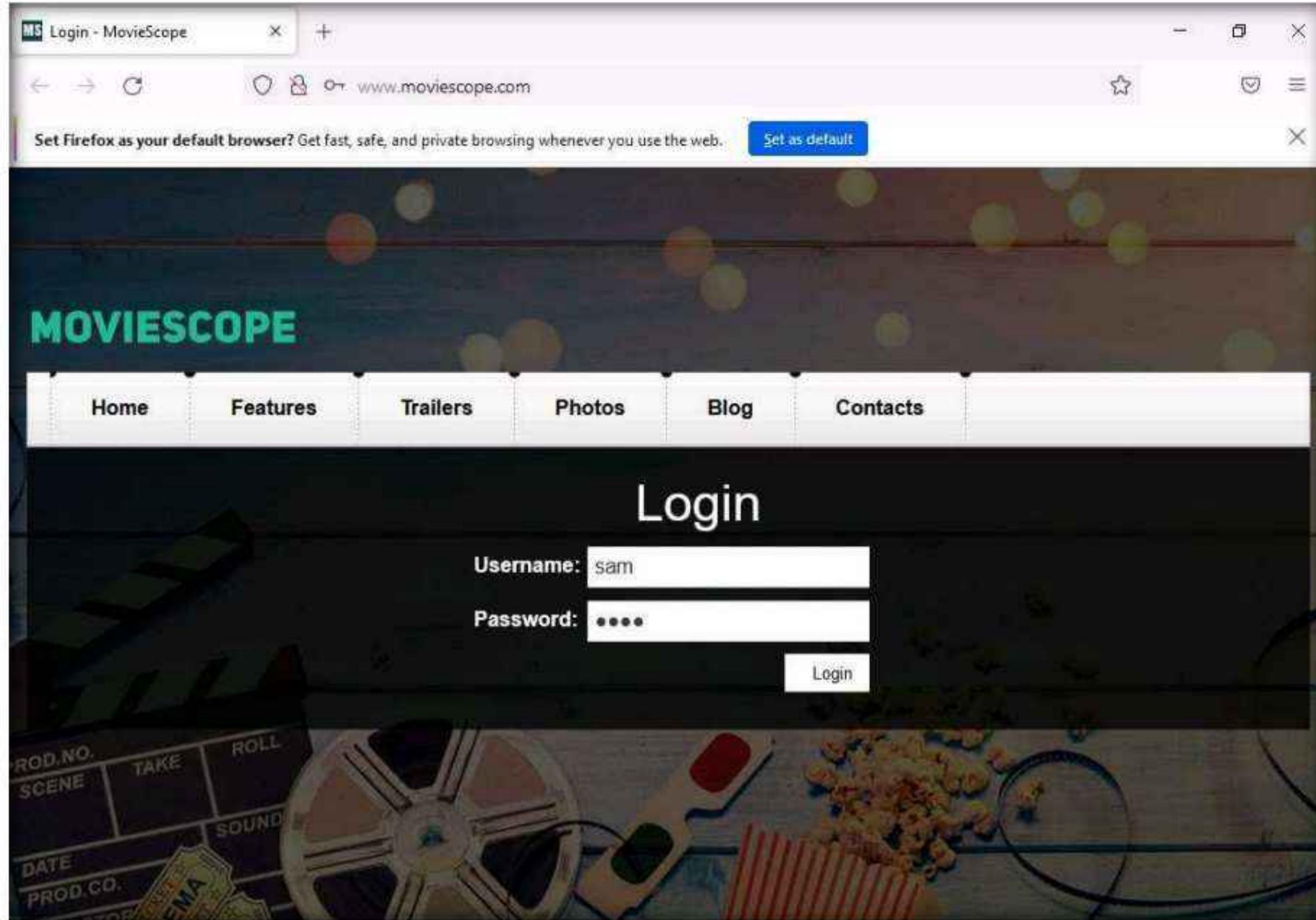
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

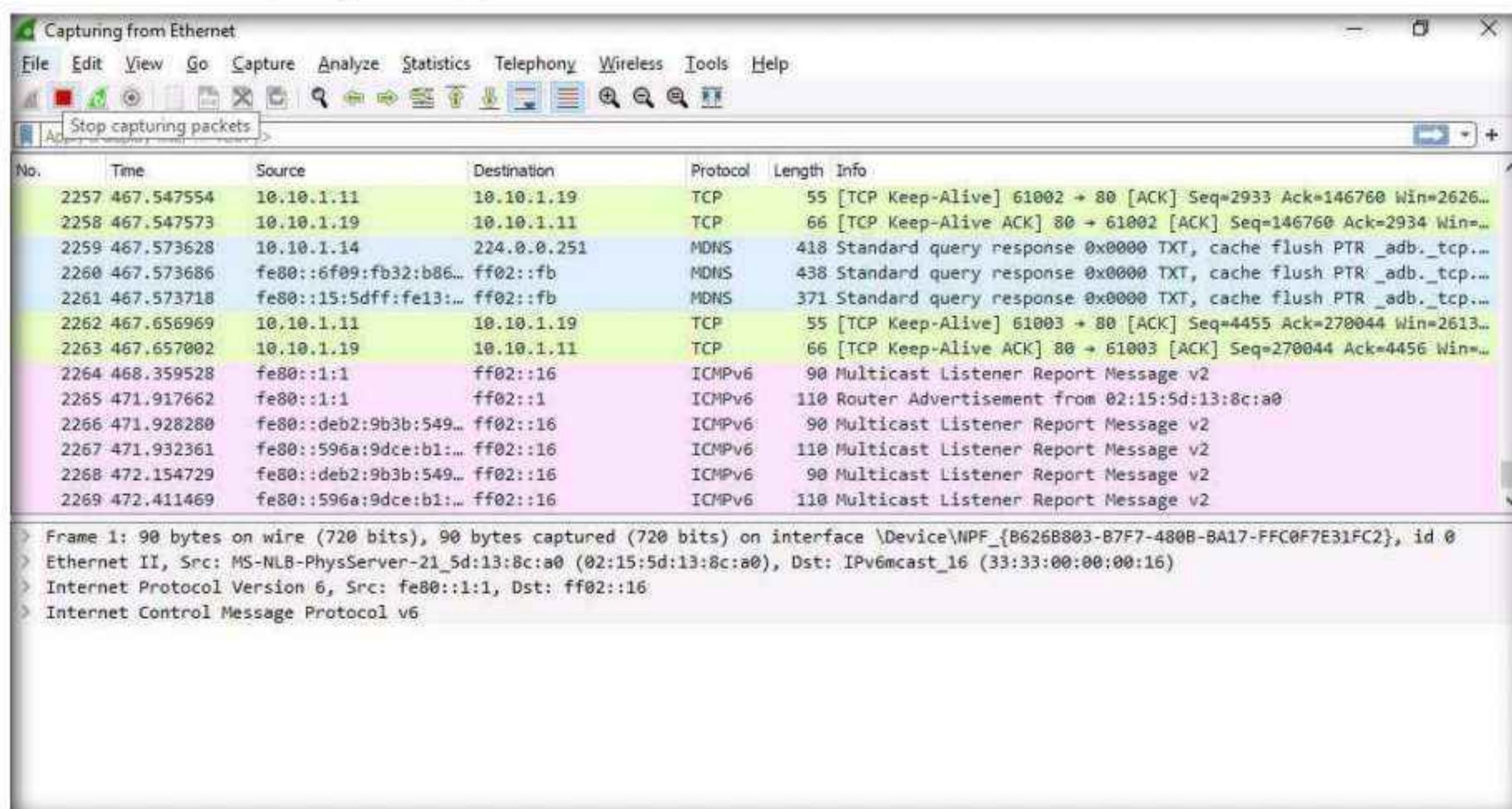


Module 08 – Sniffing

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.

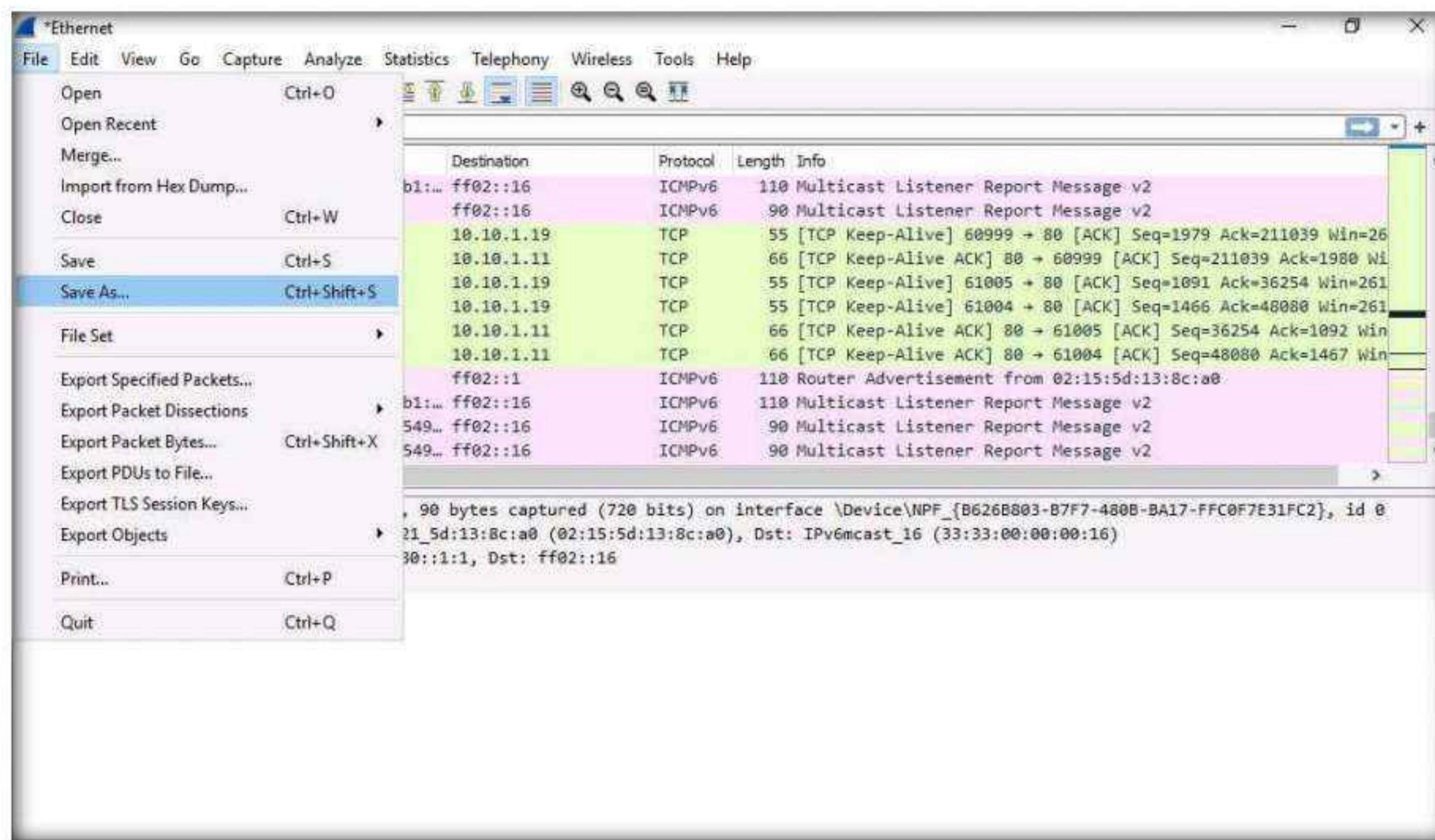


10. Switch back to **Windows Server 2019** virtual machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.

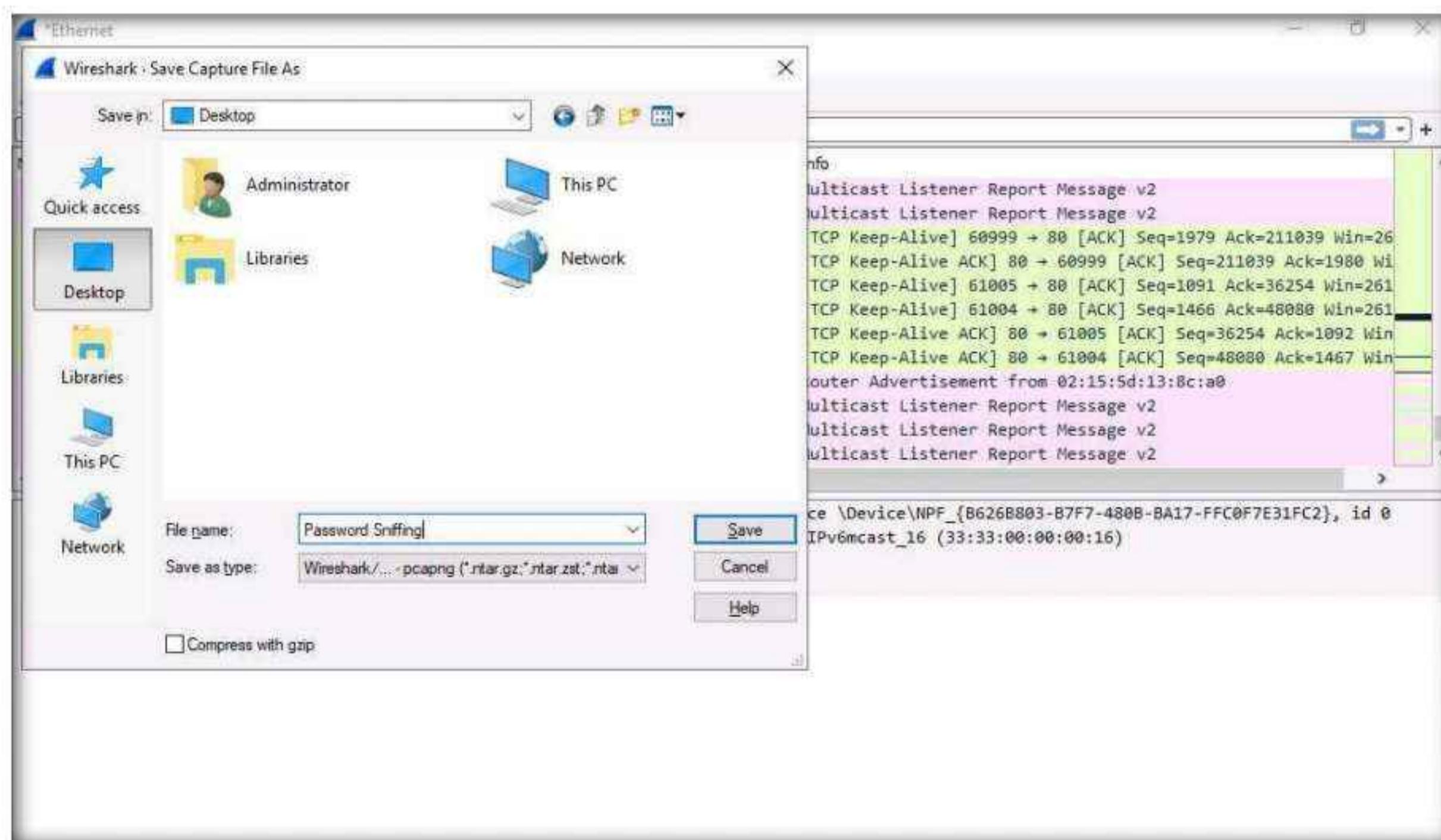


Module 08 – Sniffing

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



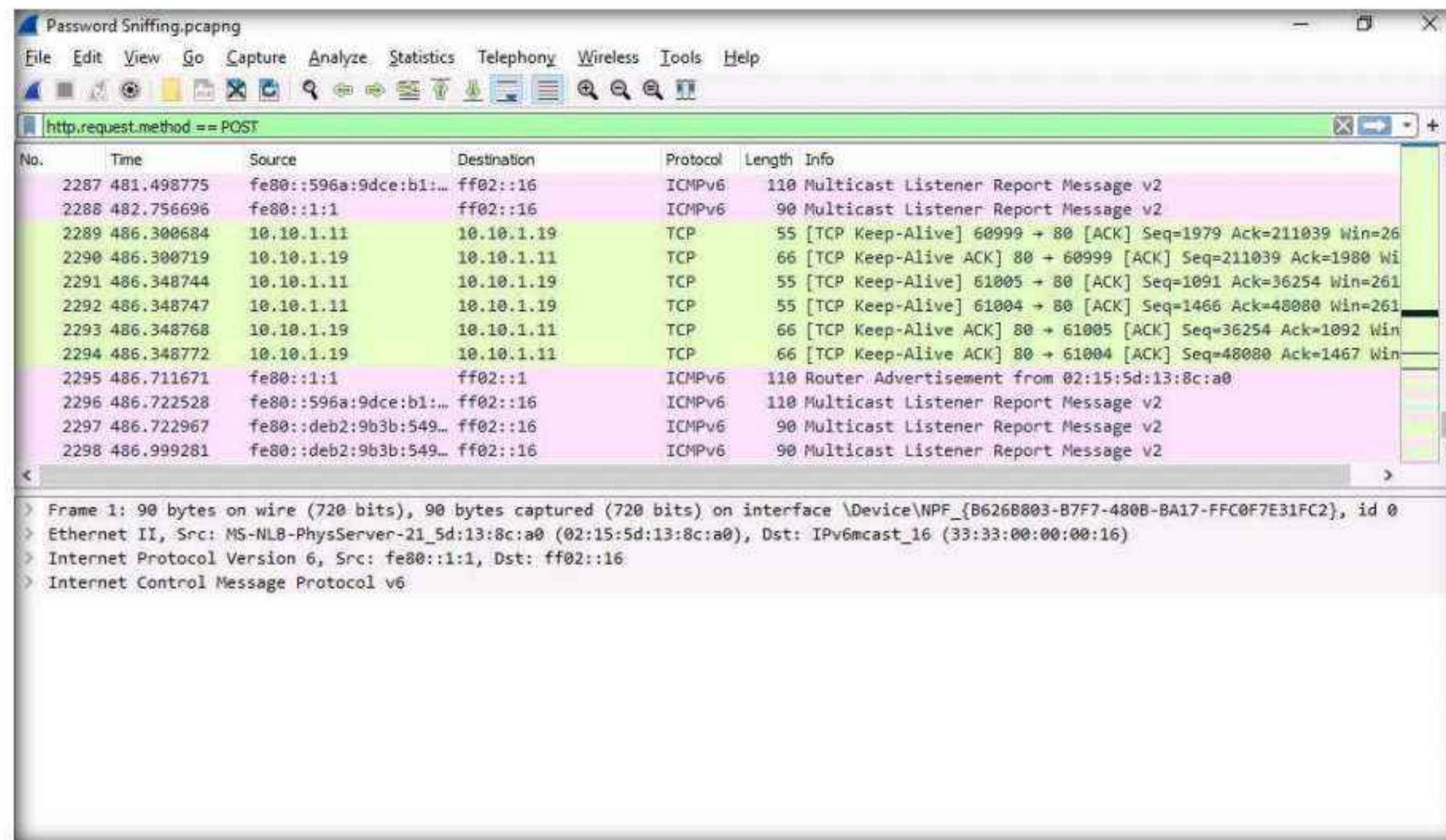
12. The **Wireshark: Save file as** window appears. Select any location to save the file, specify **File name as Password Sniffing**, and click **Save**.



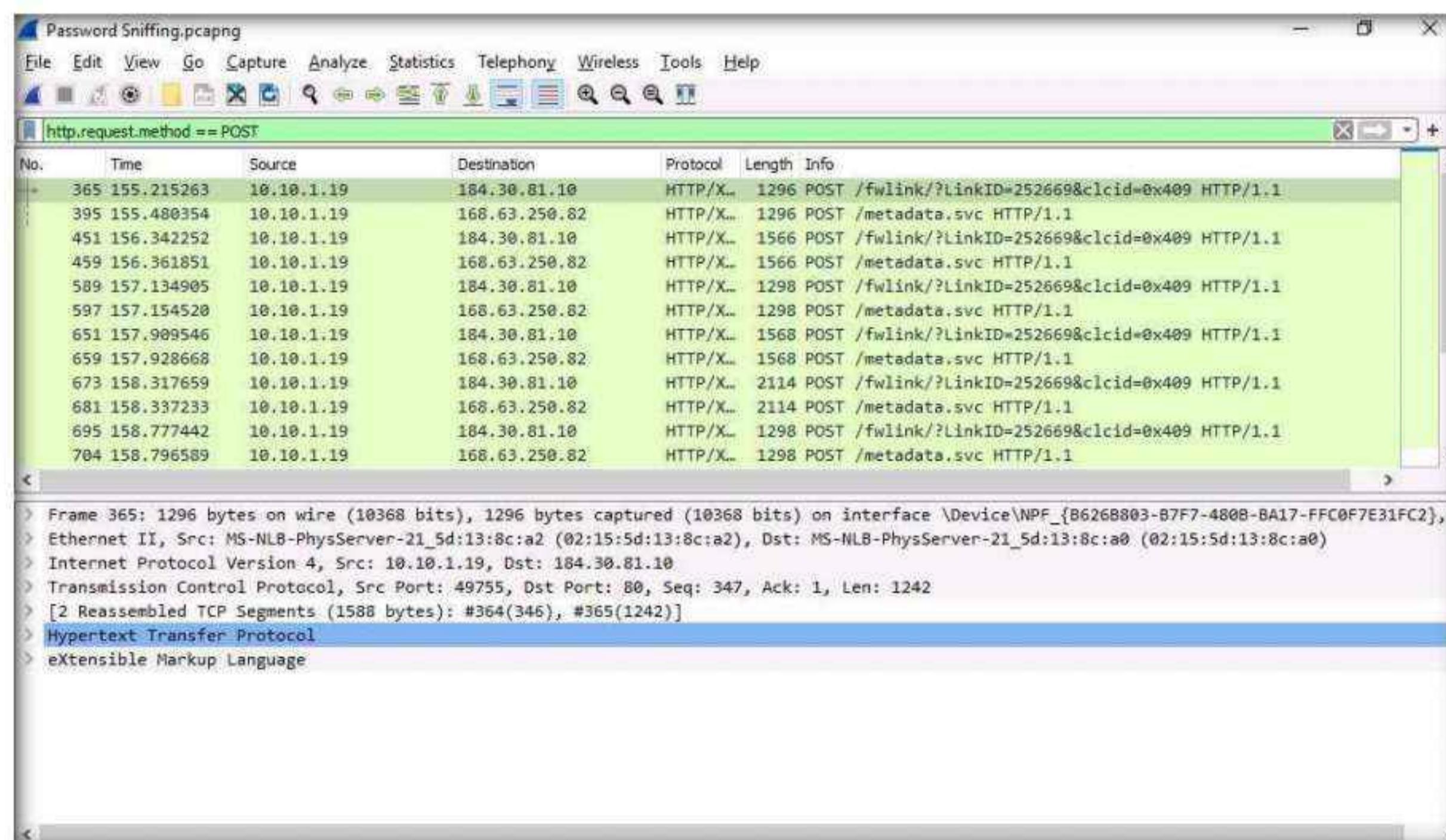
Module 08 – Sniffing

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.

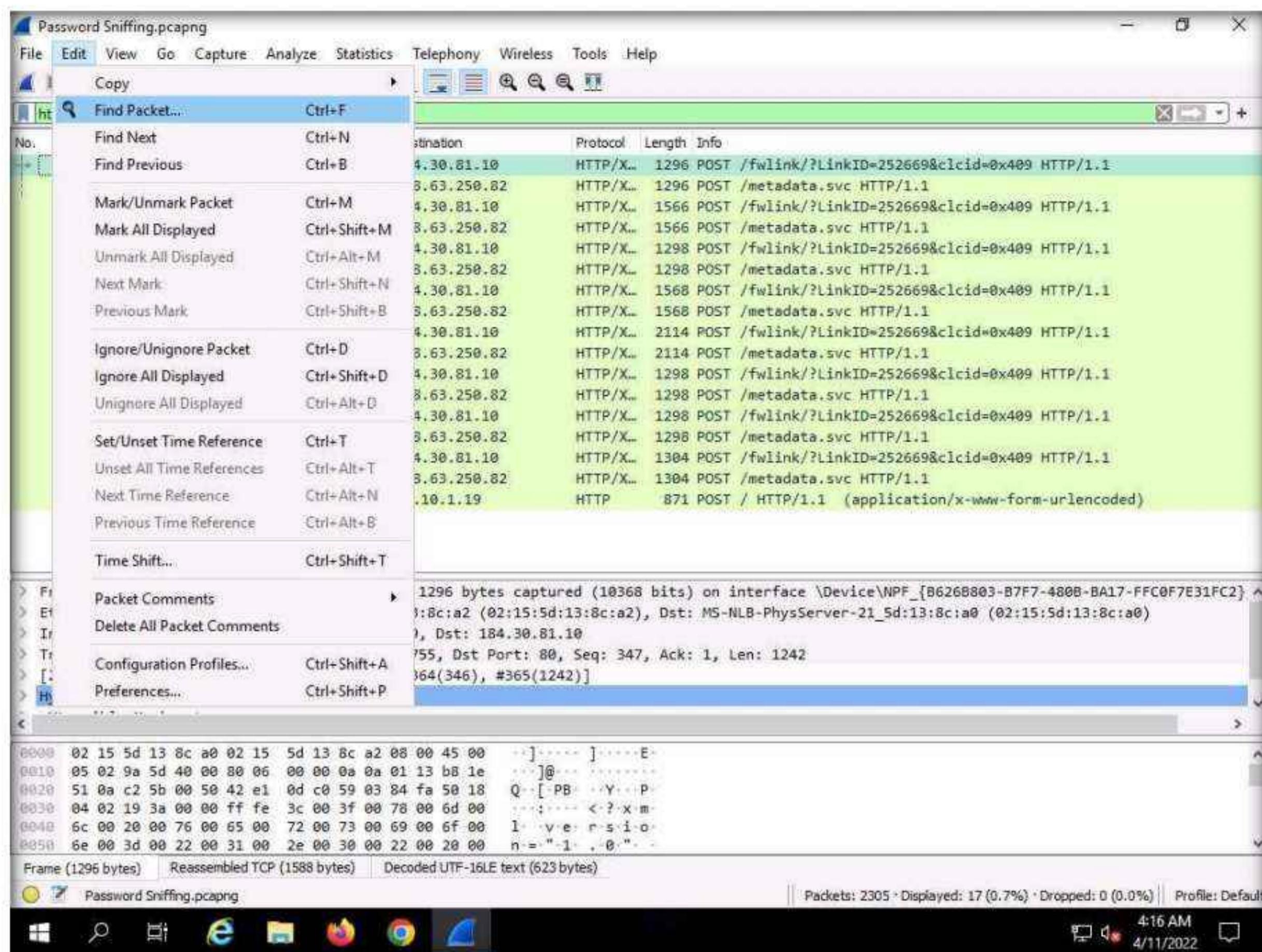


14. Wireshark only filters **http POST** traffic packets, as shown in the screenshot.



Module 08 – Sniffing

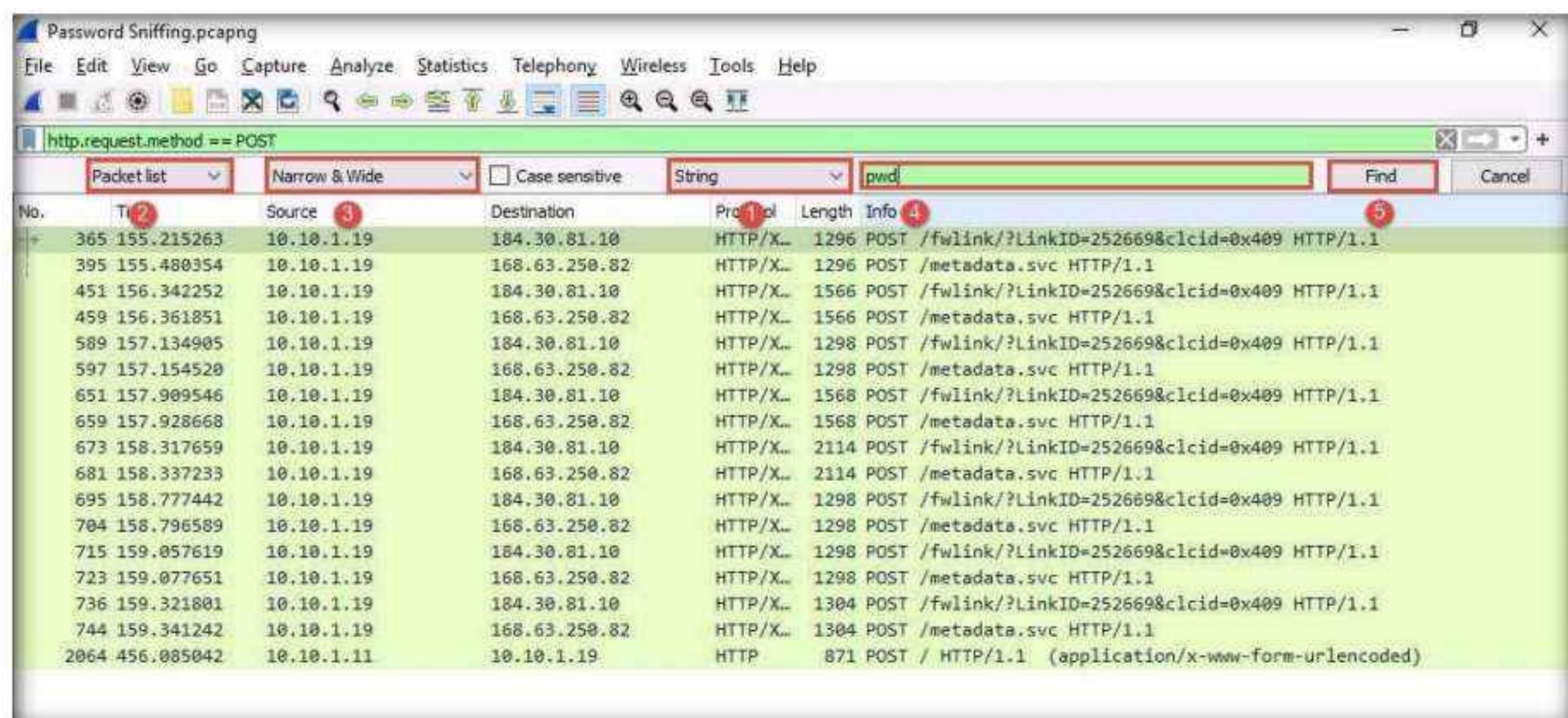
15. Now, click **Edit** from the menu bar and click **Find Packet....**



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.

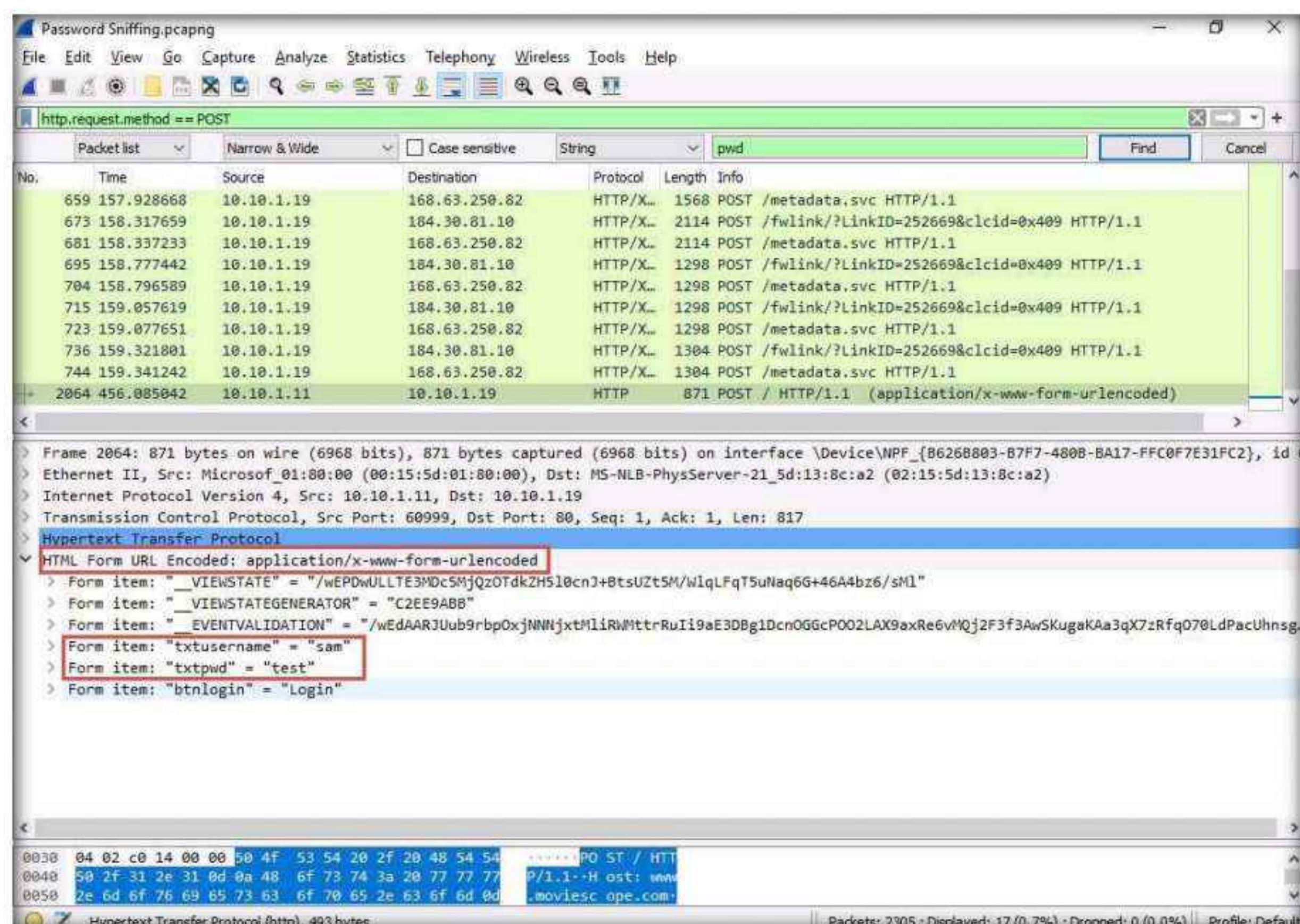
18. In the field next to **String**, type **pwd** and click the **Find** button.



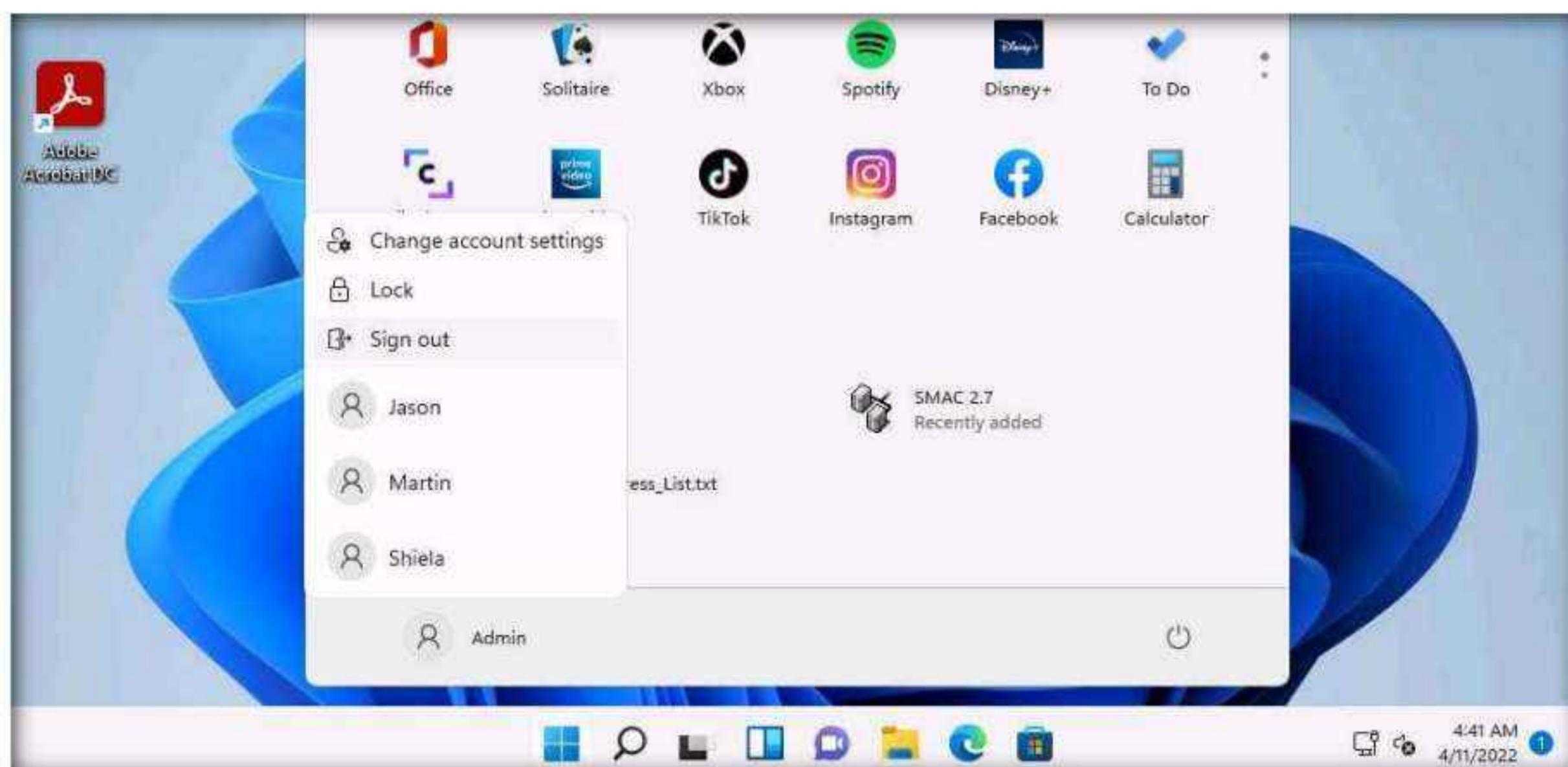
19. Wireshark will now display the snuffed password from the captured packets.

Module 08 – Sniffing

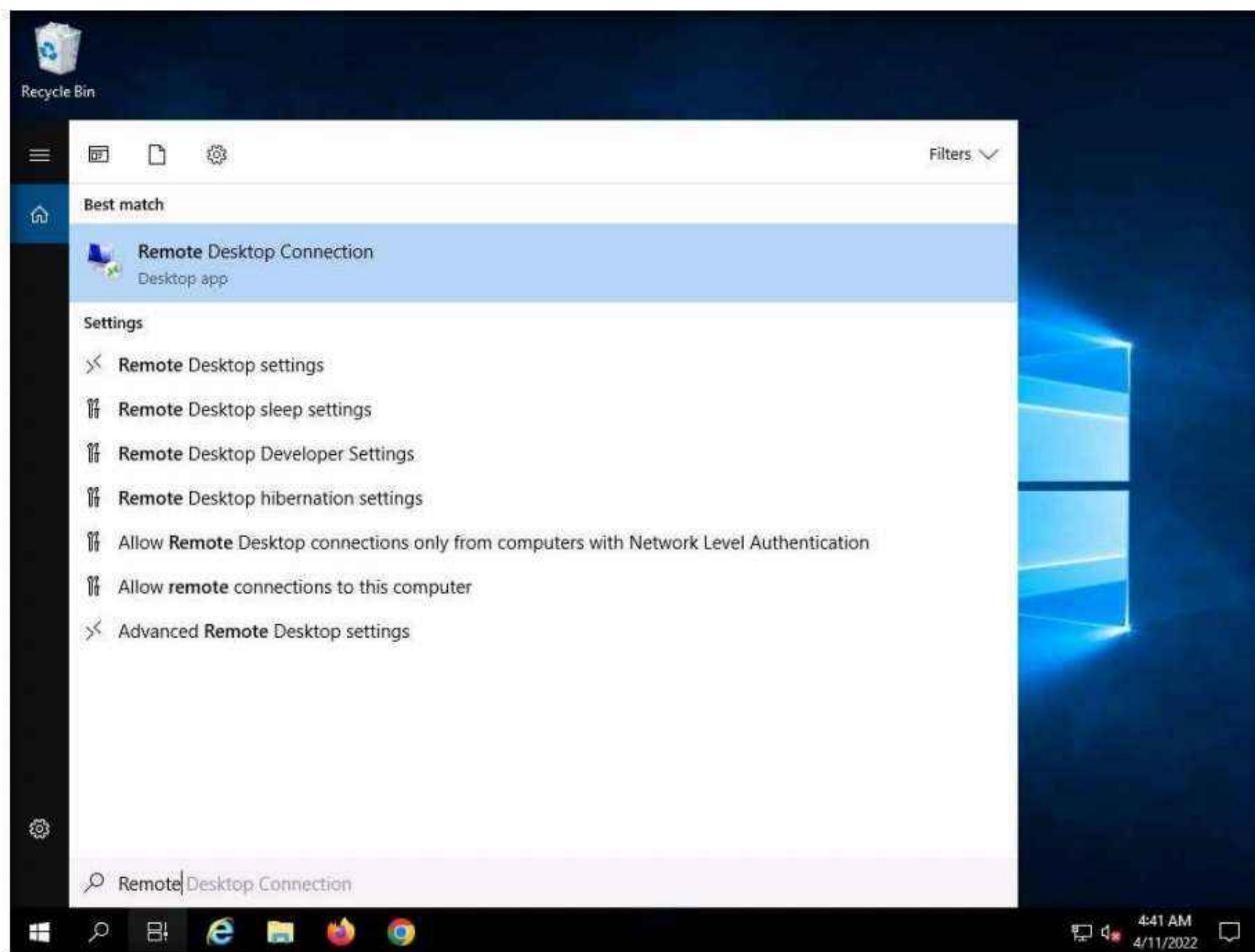
20. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** node from the packet details section, and view the captured username and password, as shown in the screenshot.



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.



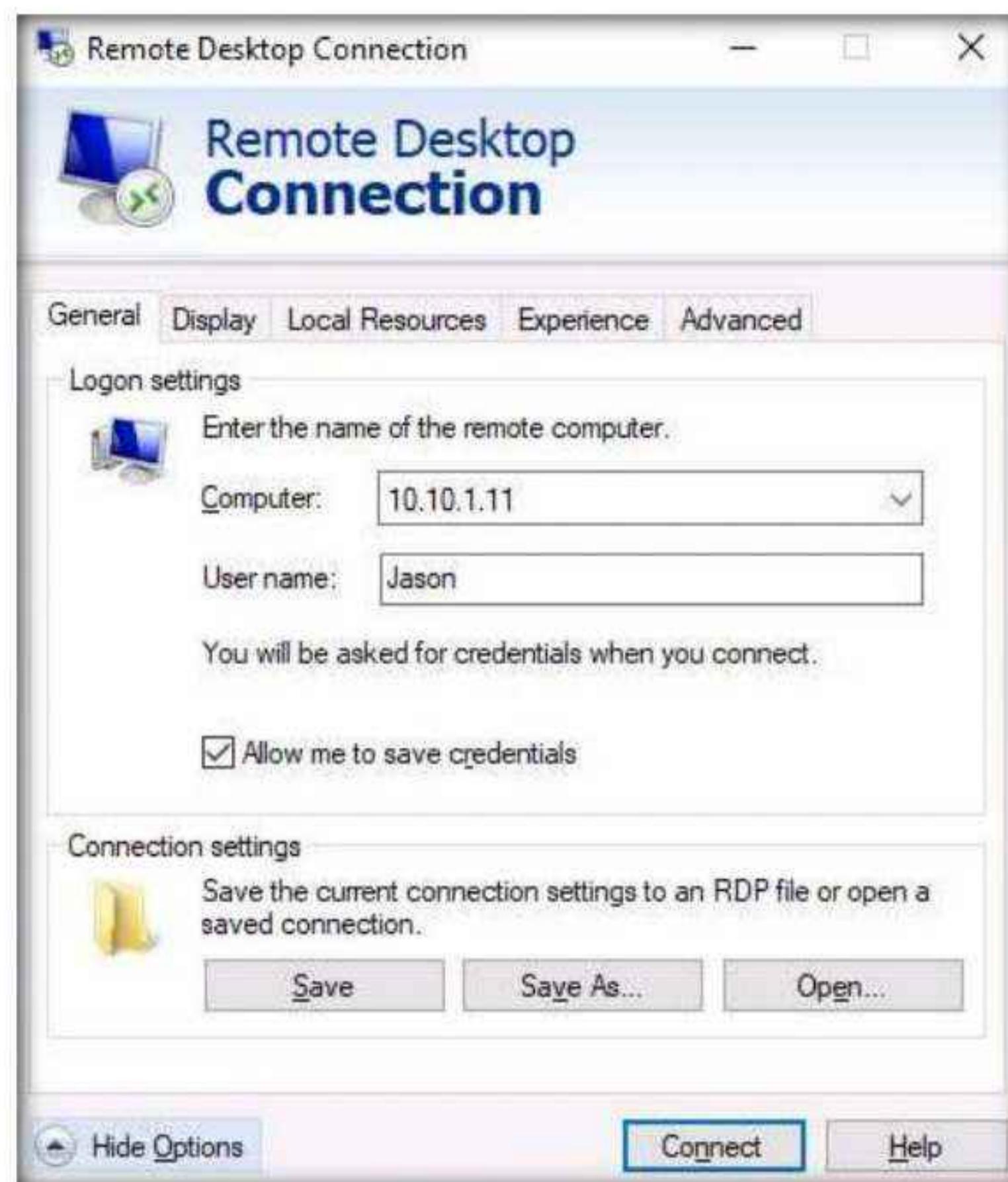
25. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

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.

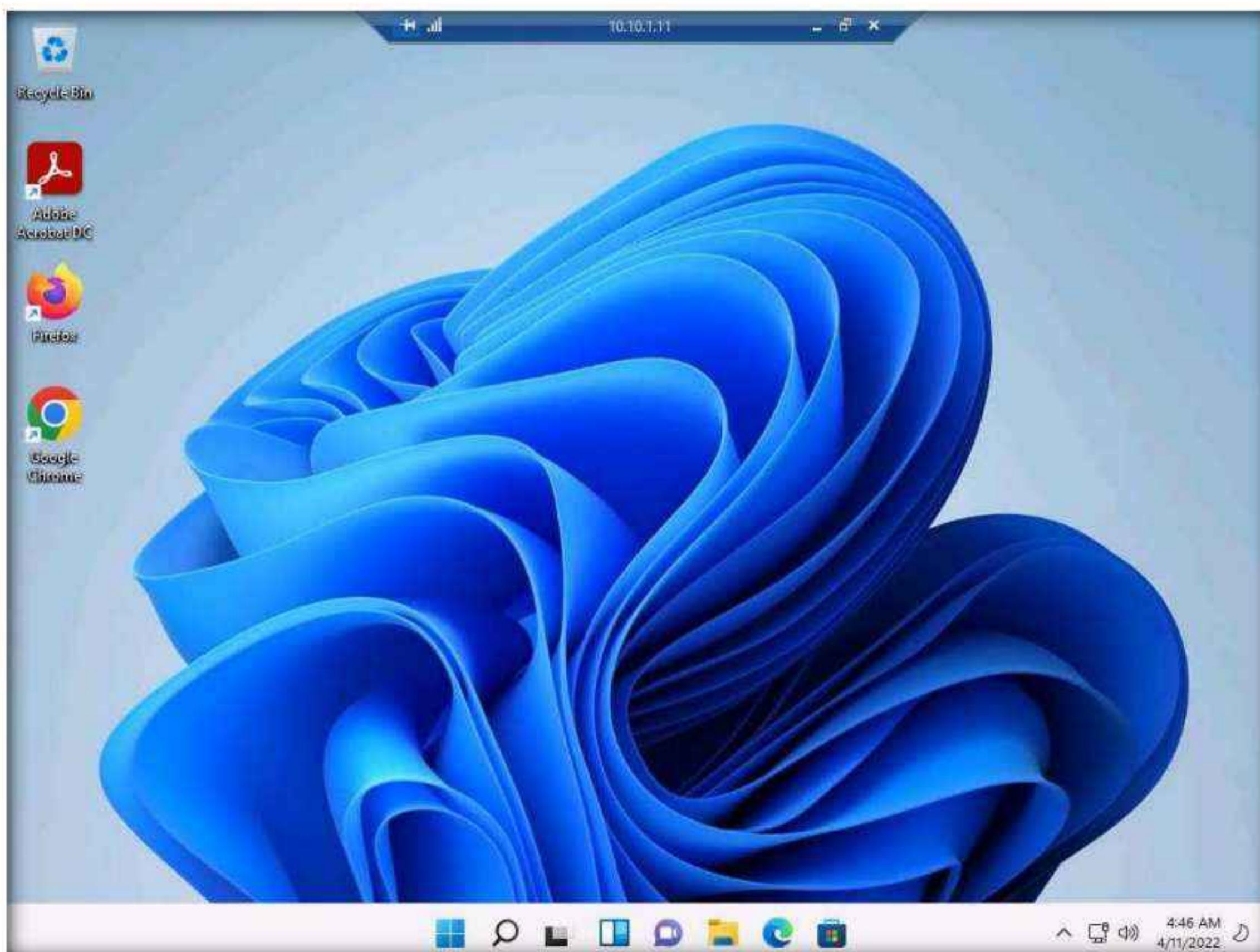


28. The **Remote Desktop Connection** pop-up appears; click **Yes**.

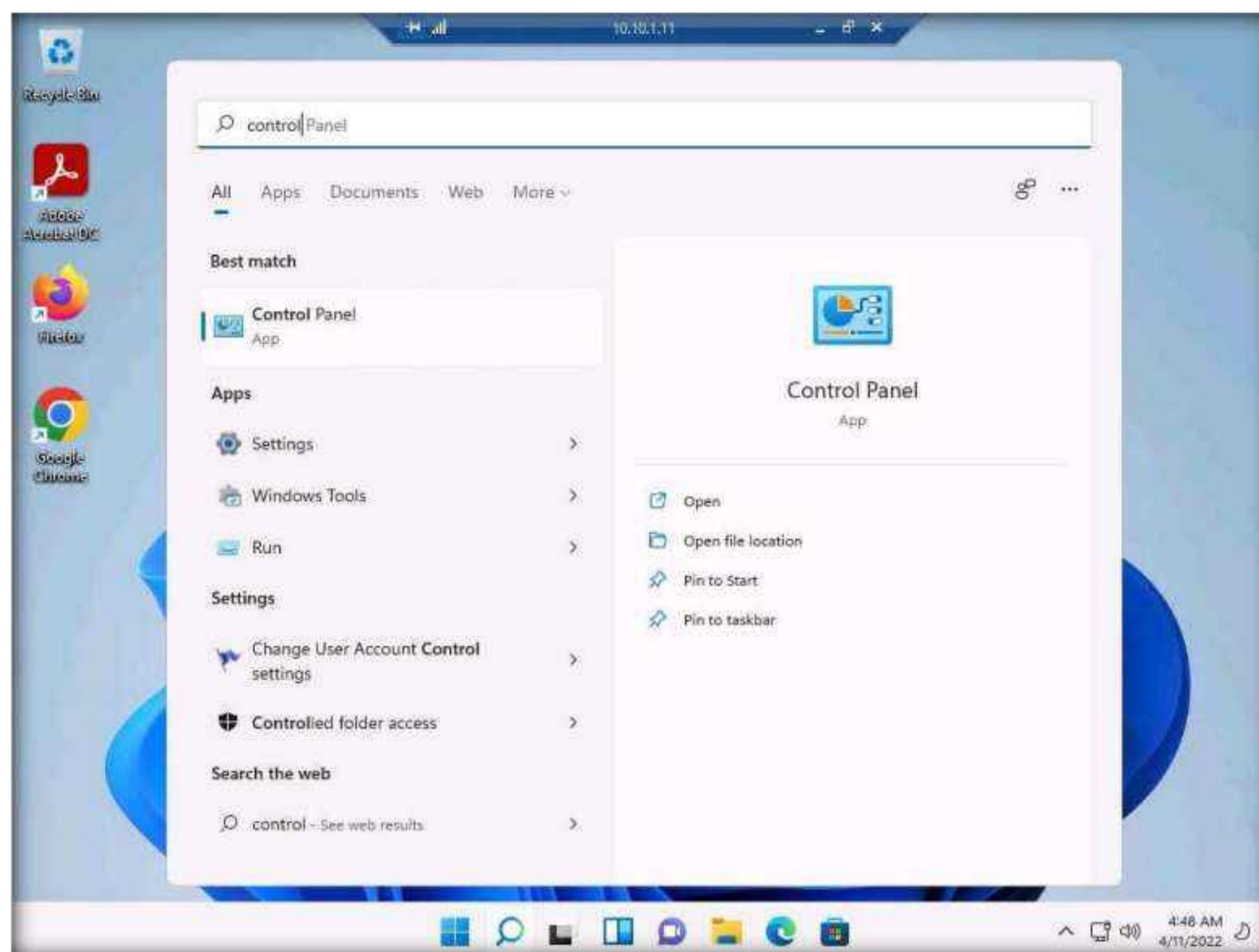


29. A remote connection to the target system (**Windows 11**) appears, as shown in the screenshot.

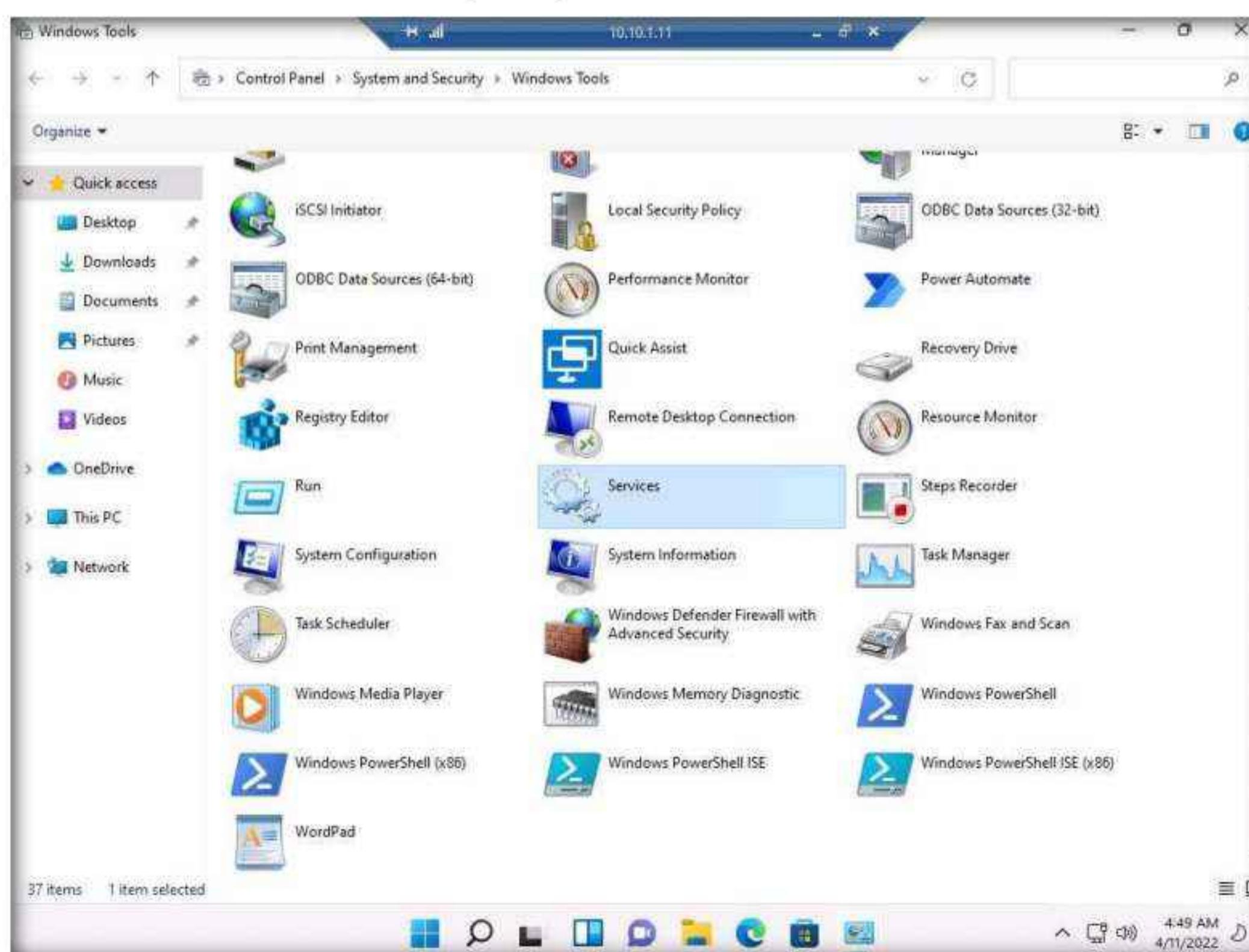
Note: If a **Choose privacy settings for your device** window appears, click on **Next** in the next window click on **Next** and in the next window click on **Accept**.



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.

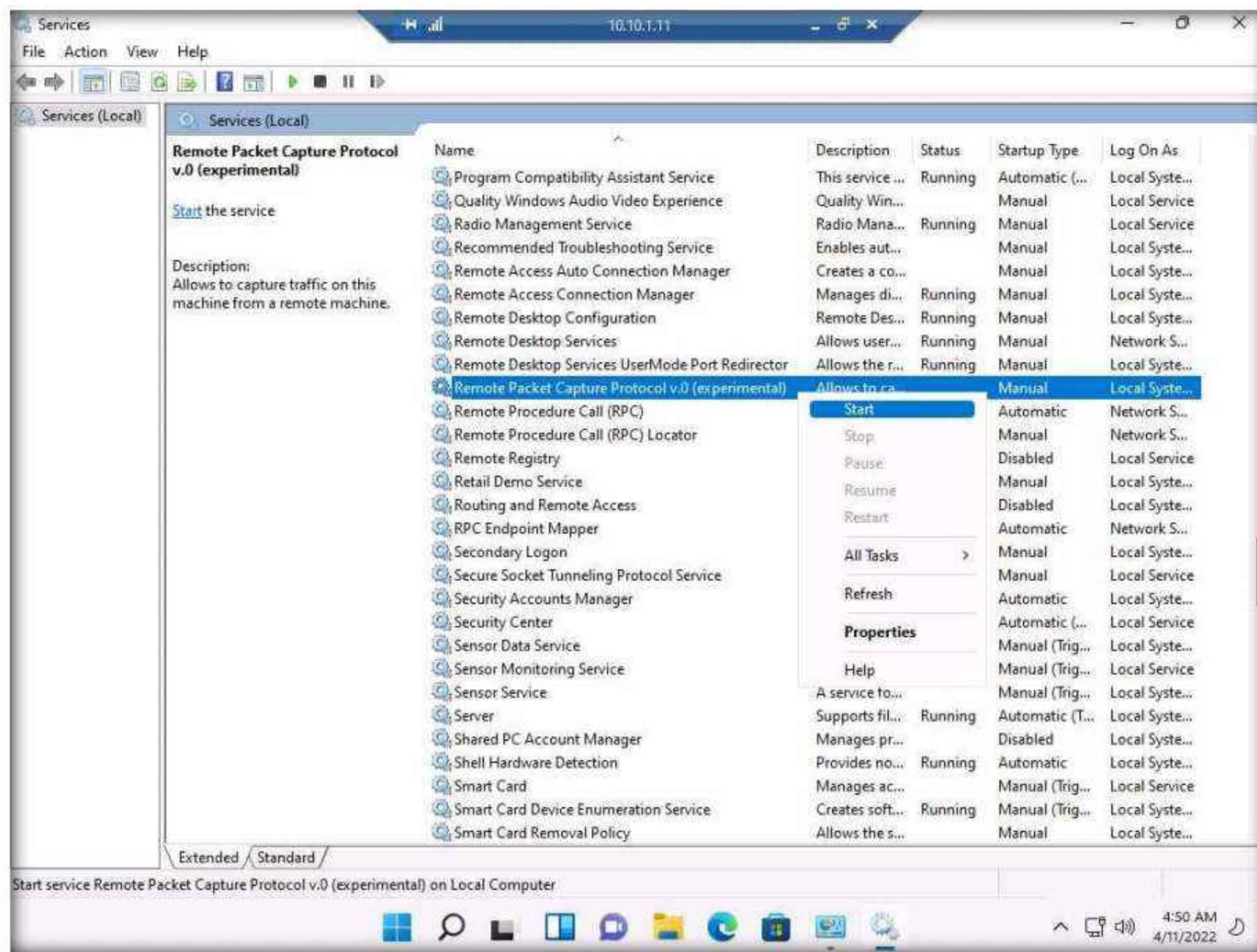


31. The **Control Panel** window appears; navigate to **System and Security → Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.

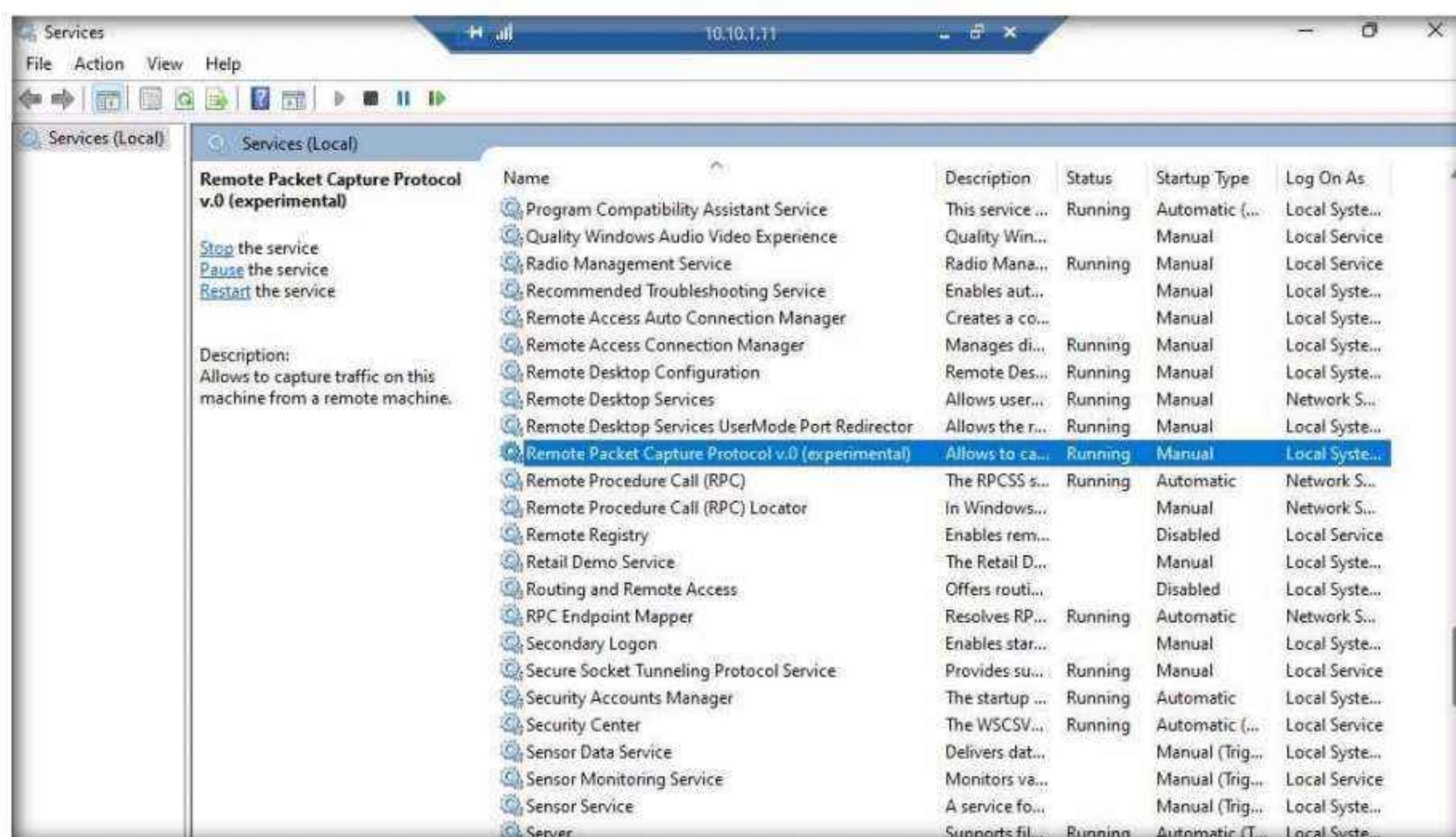


Module 08 – Sniffing

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



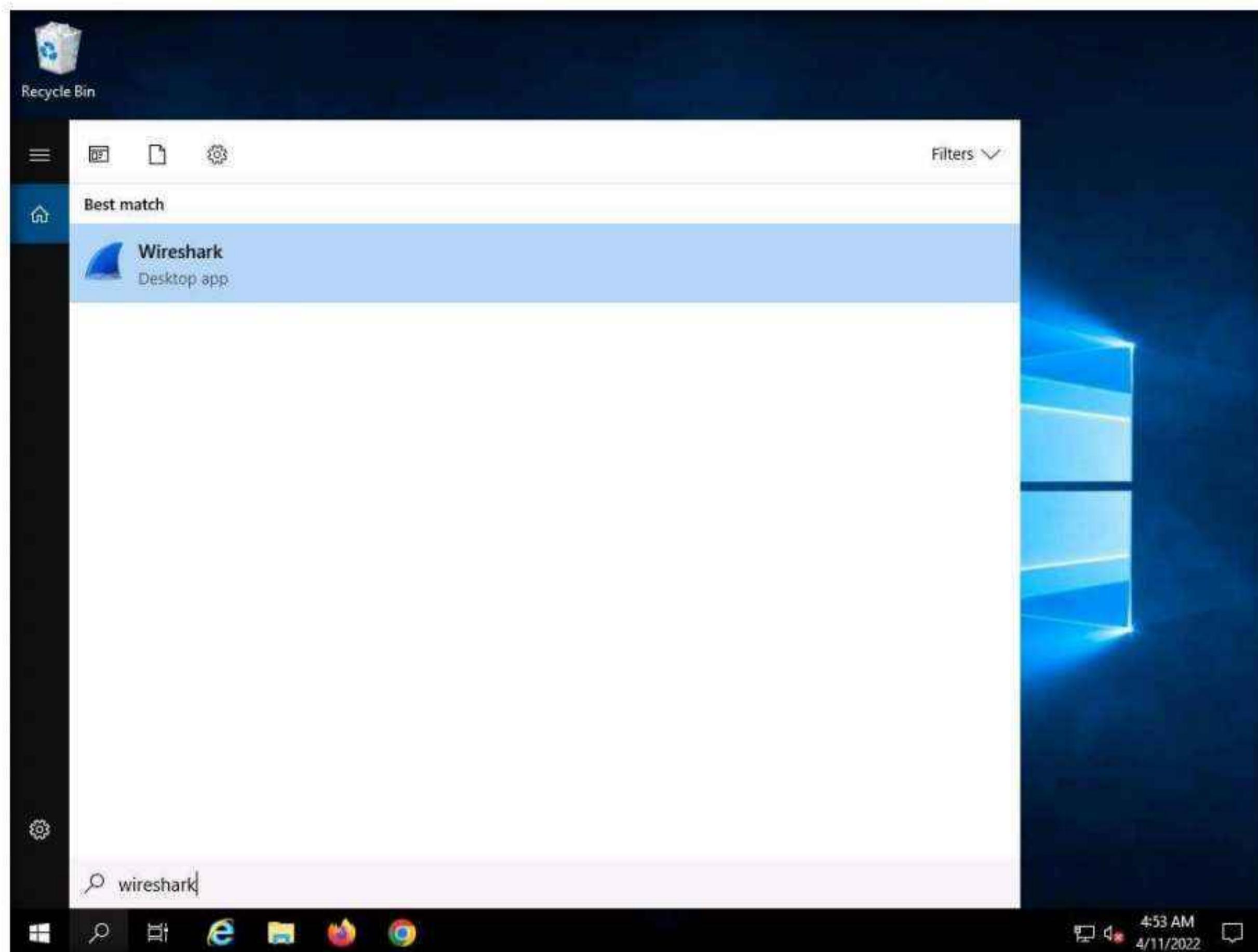
33. The Status of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.



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

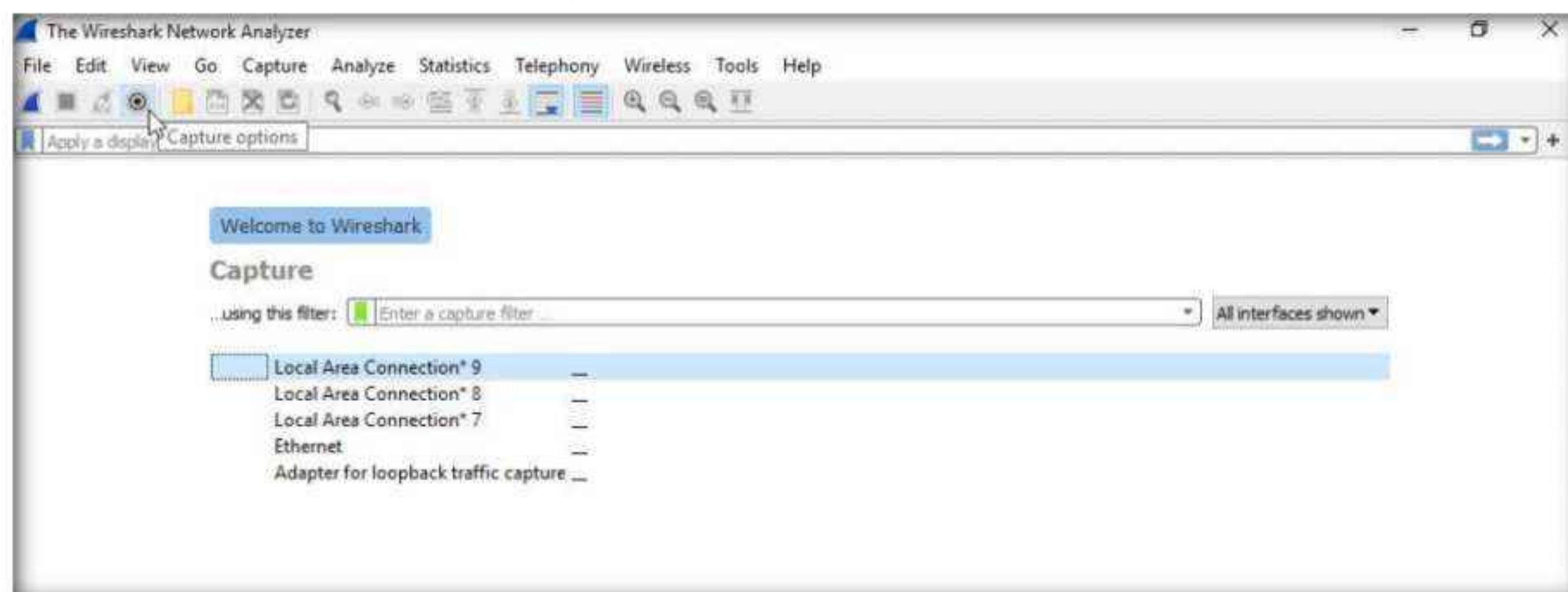
Note: If a **Remote Desktop Connection** pop-up appears, click **OK**.

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**.



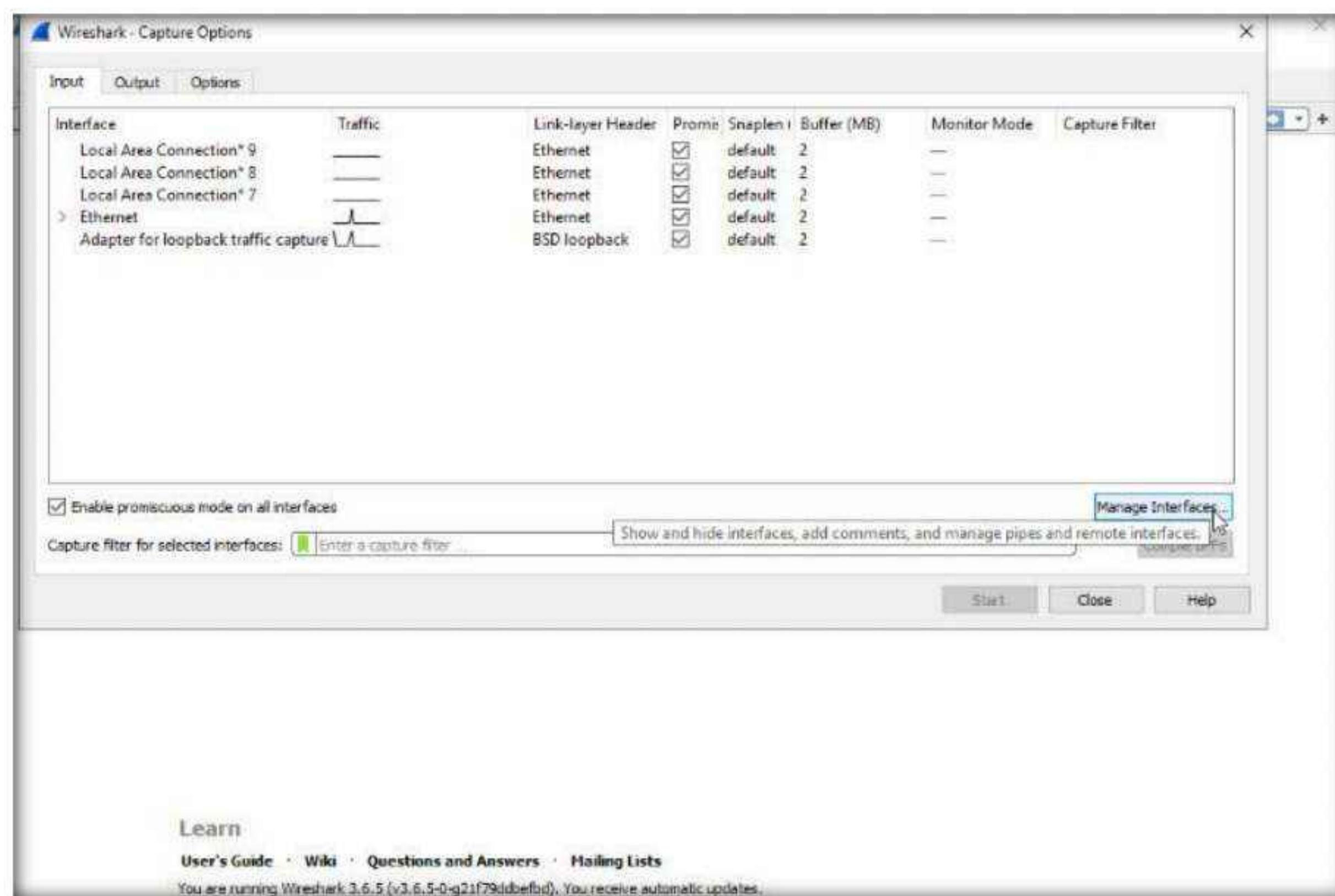
36. The **Wireshark Network Analyzer** window appears; click the **Capture options** icon from the toolbar.

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

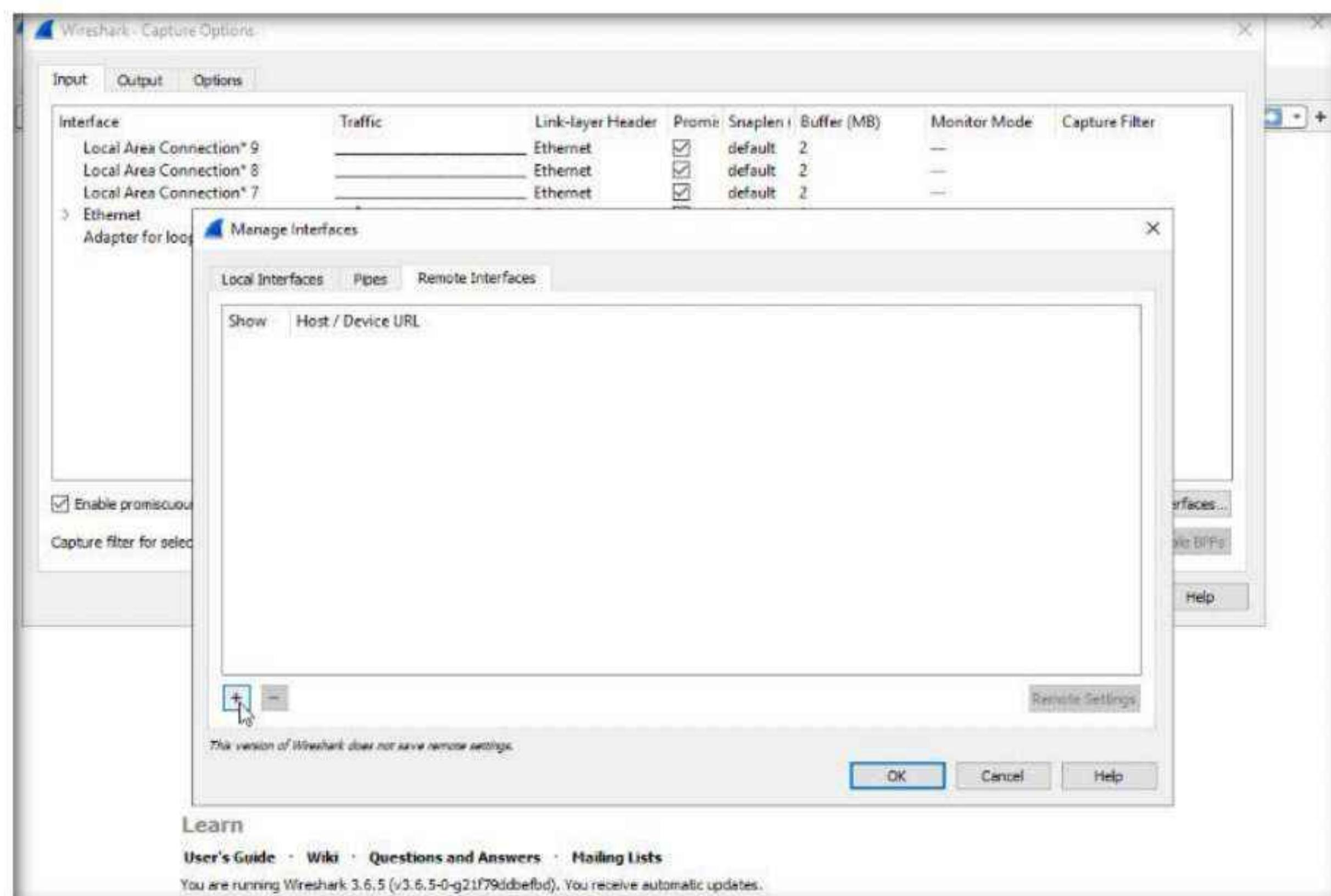


Module 08 – Sniffing

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



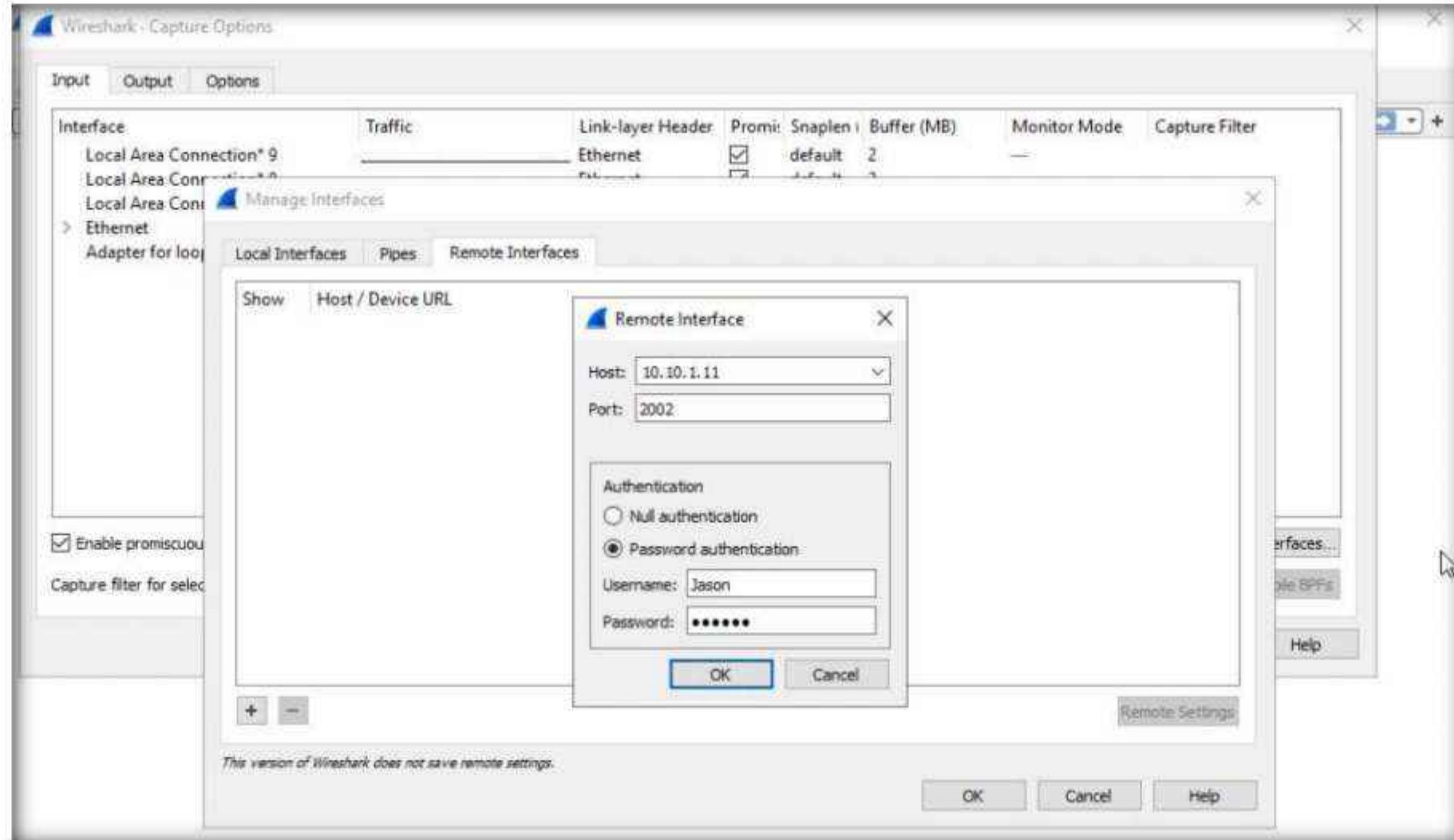
38. The Manage Interfaces window appears; click the Remote Interfaces tab, and then the Add a remote host and its interface icon (+).



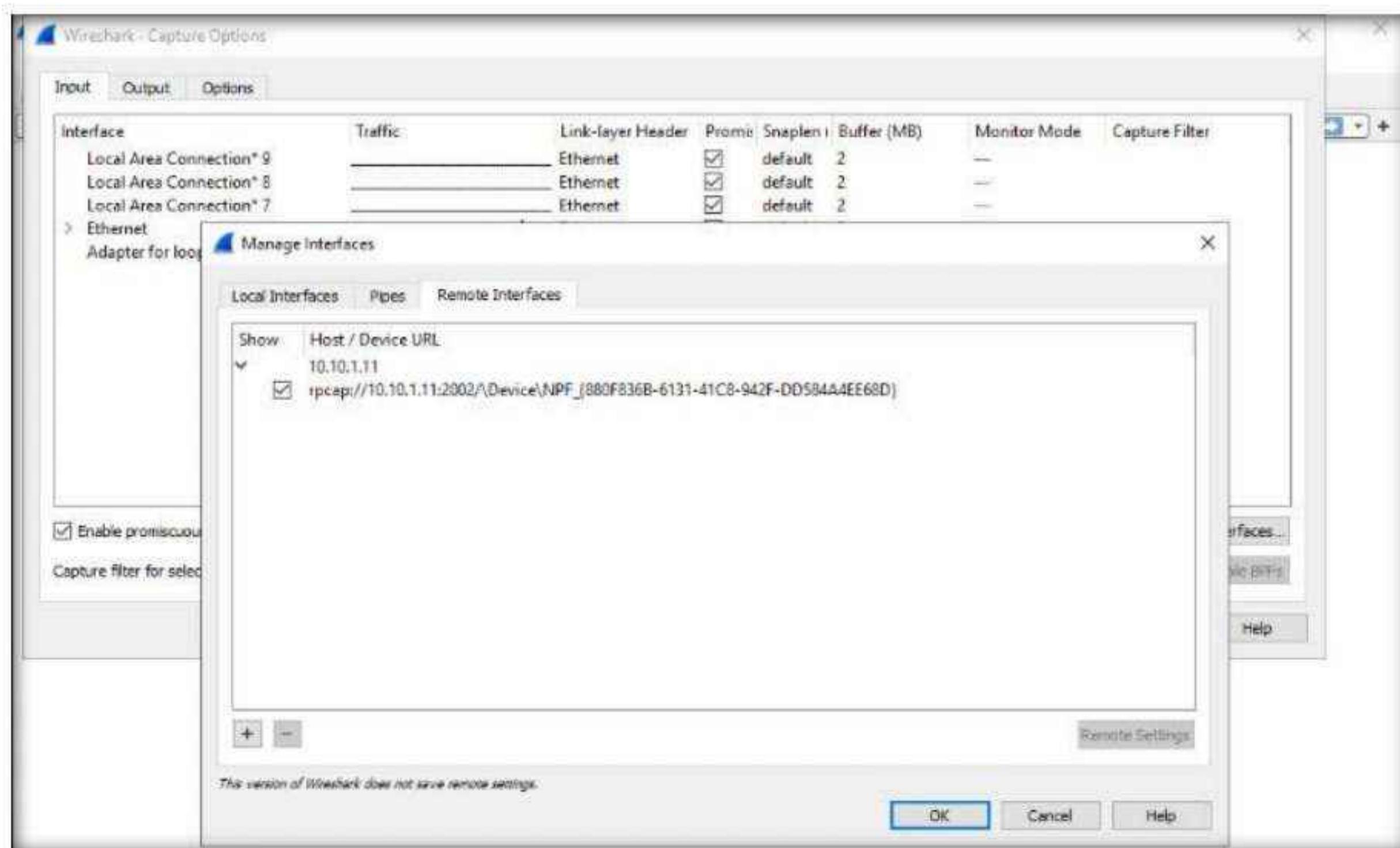
Module 08 – Sniffing

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 **qwertys**); click **OK**.

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

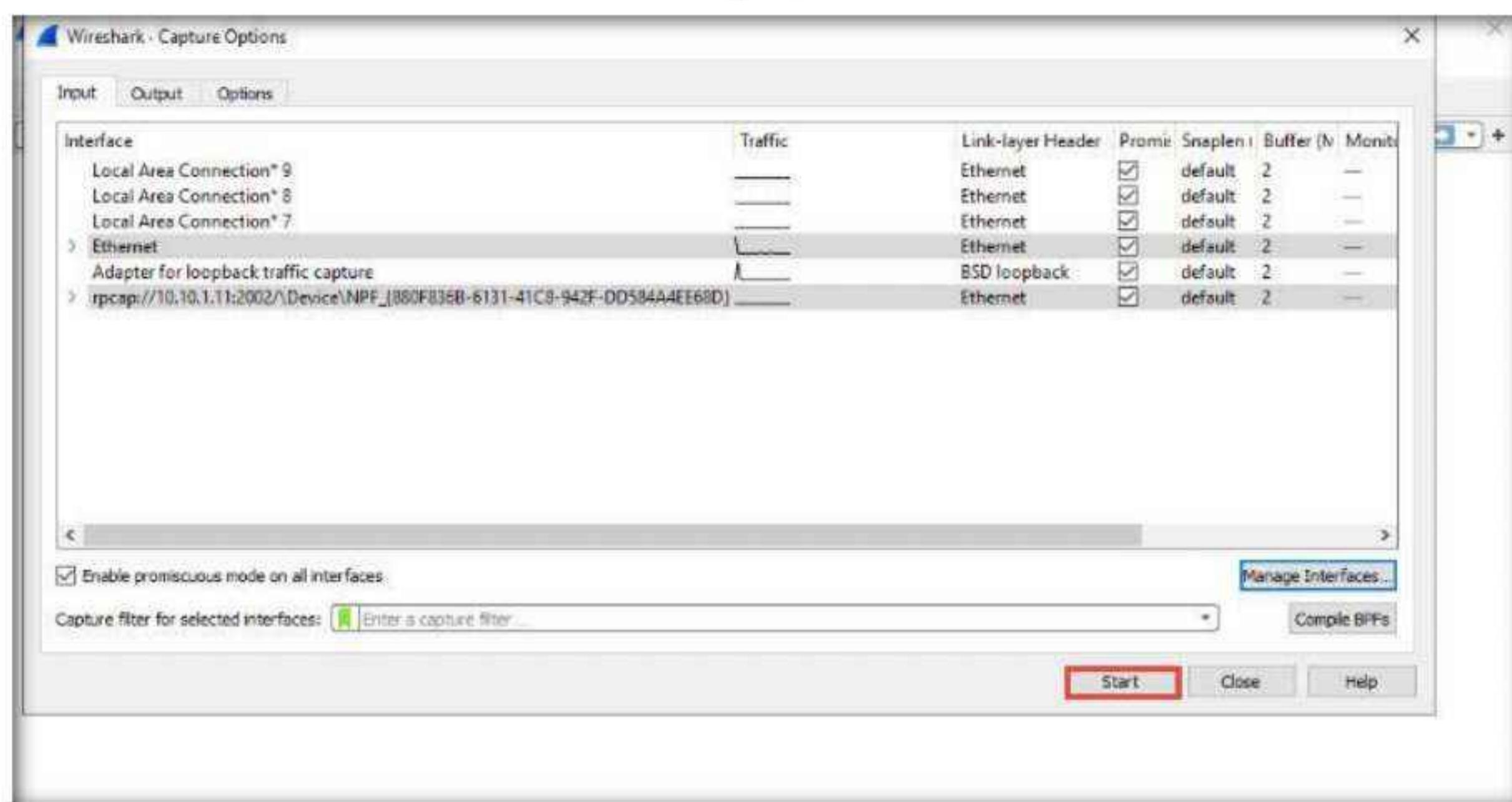


41. A new remote interface is added to the **Manage Interfaces** window; click **OK**.

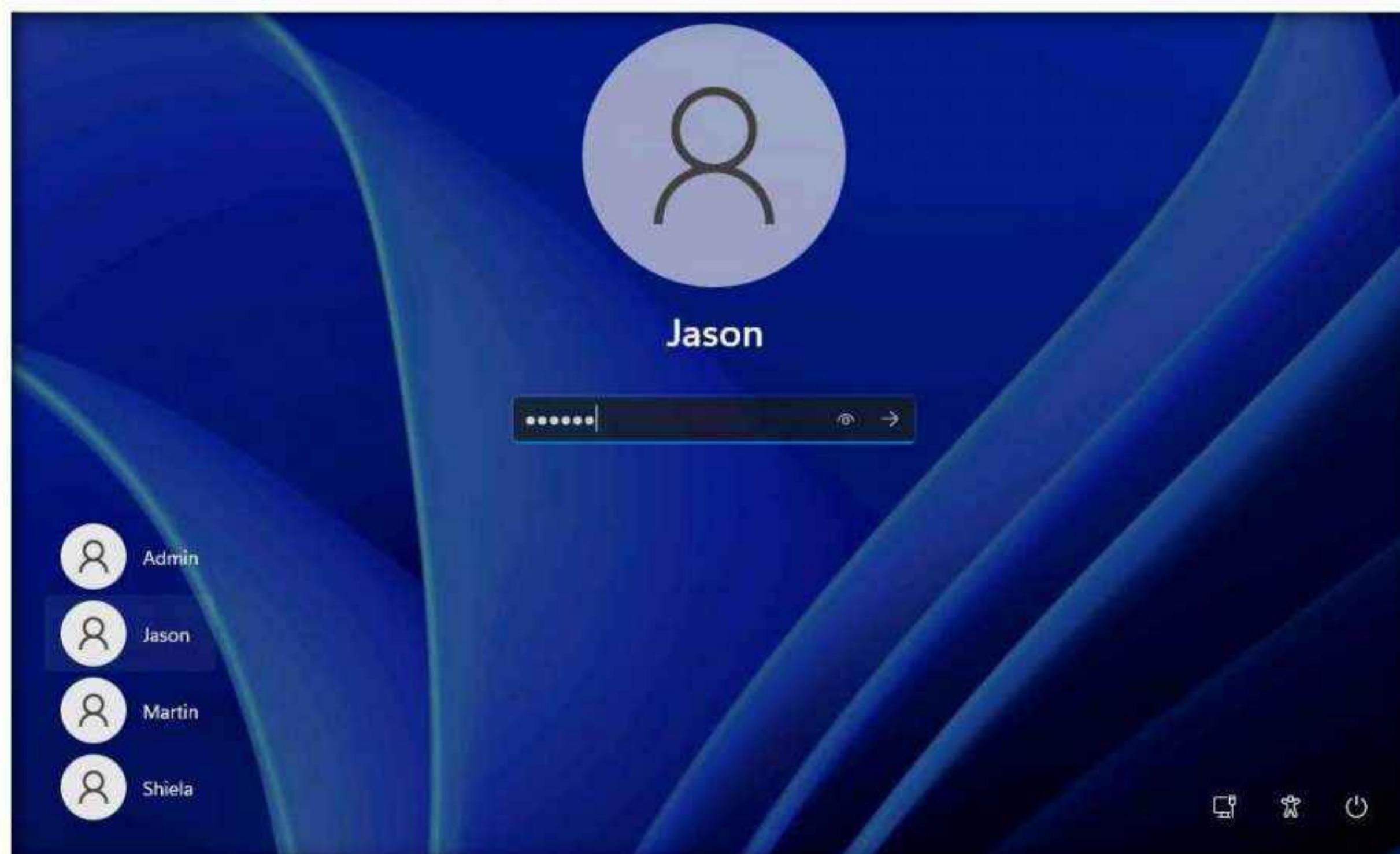


42. The newly added remote interface appears in the **Wireshark. Capture Options** window; click **Start**.

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

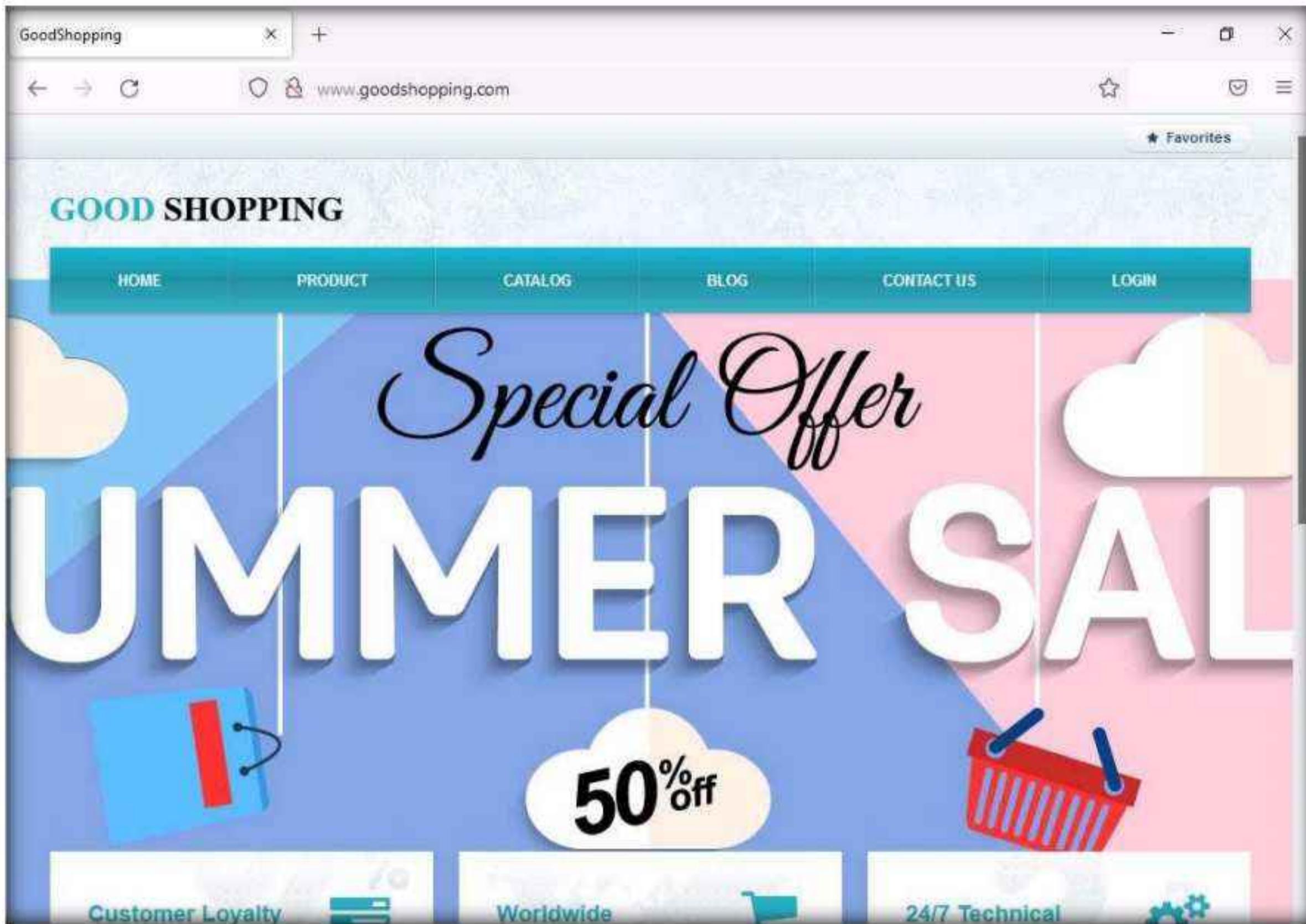


43. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. Select **Jason** from the list of user accounts in the left-pane, click **qwerty** to enter the password and press **Enter** to log in. Here, you are signing in as the victim.

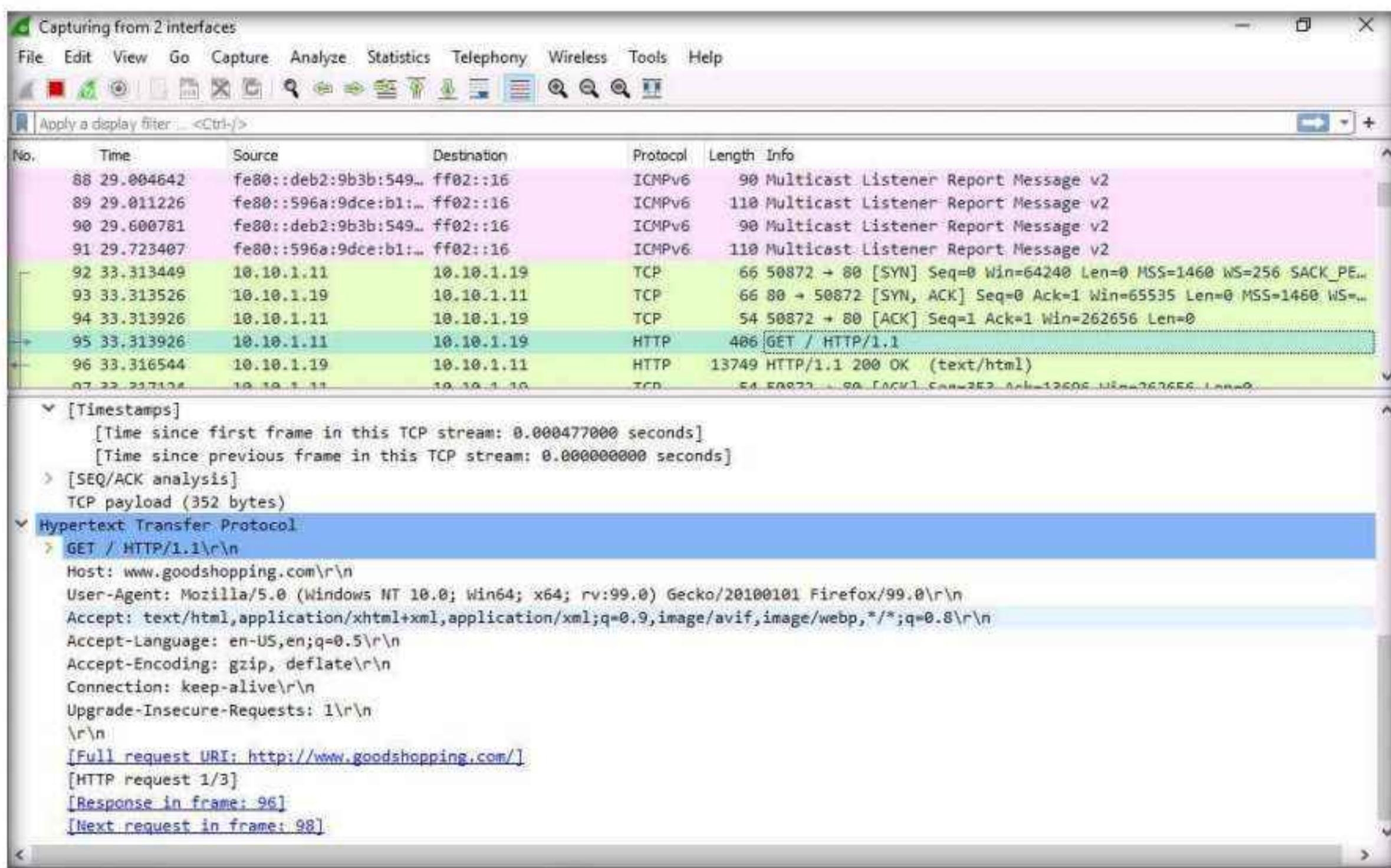


44. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, <http://www.goodshopping.com>).

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, 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.

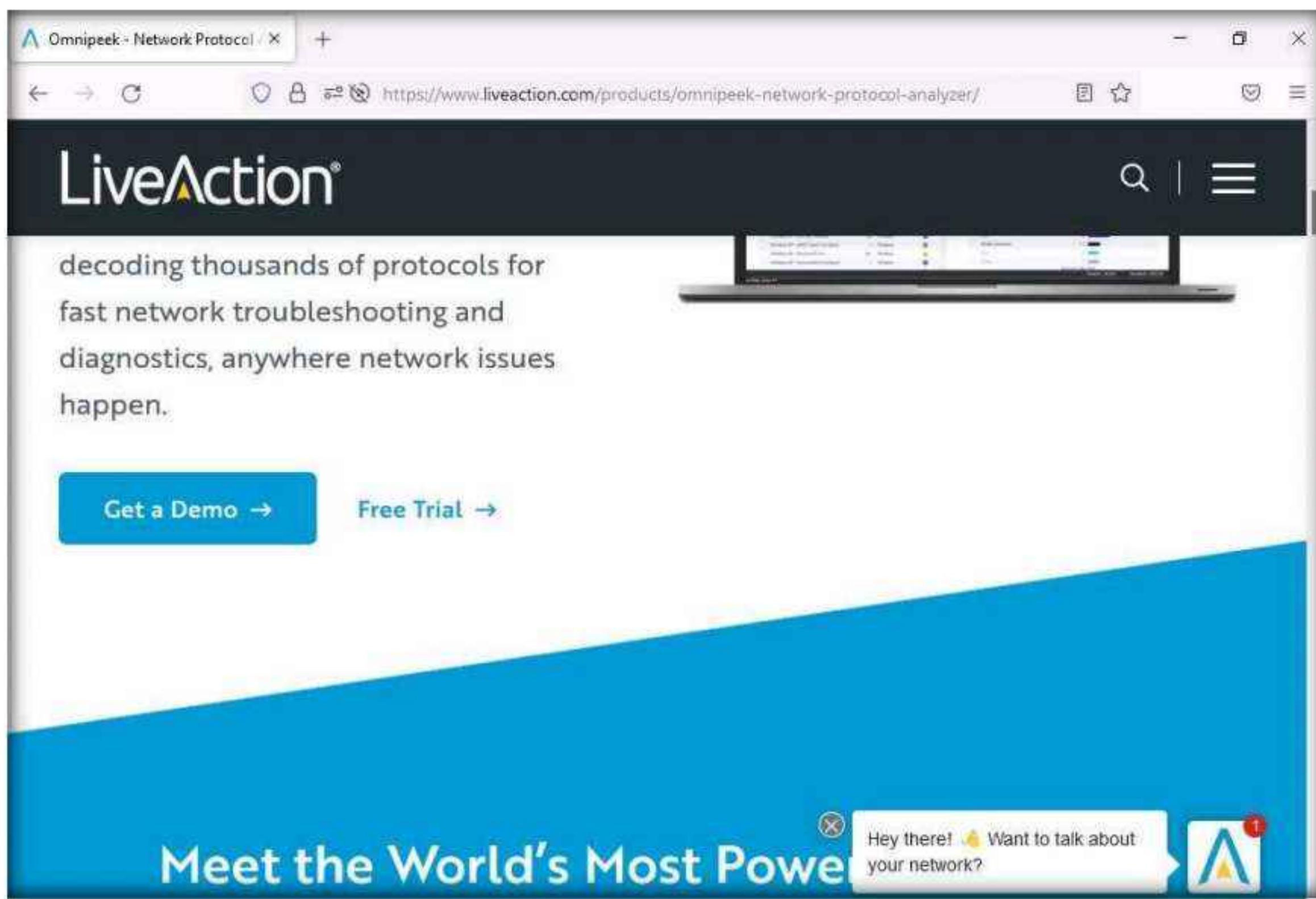
1. Switch to the **Windows 11** virtual machine.
2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on <https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/> in the address bar, and press **Enter**.

Note: If a website cookie notification appears, click **Accept**.

3. The **LiveAction** website appears; click the **Free Trial** button.

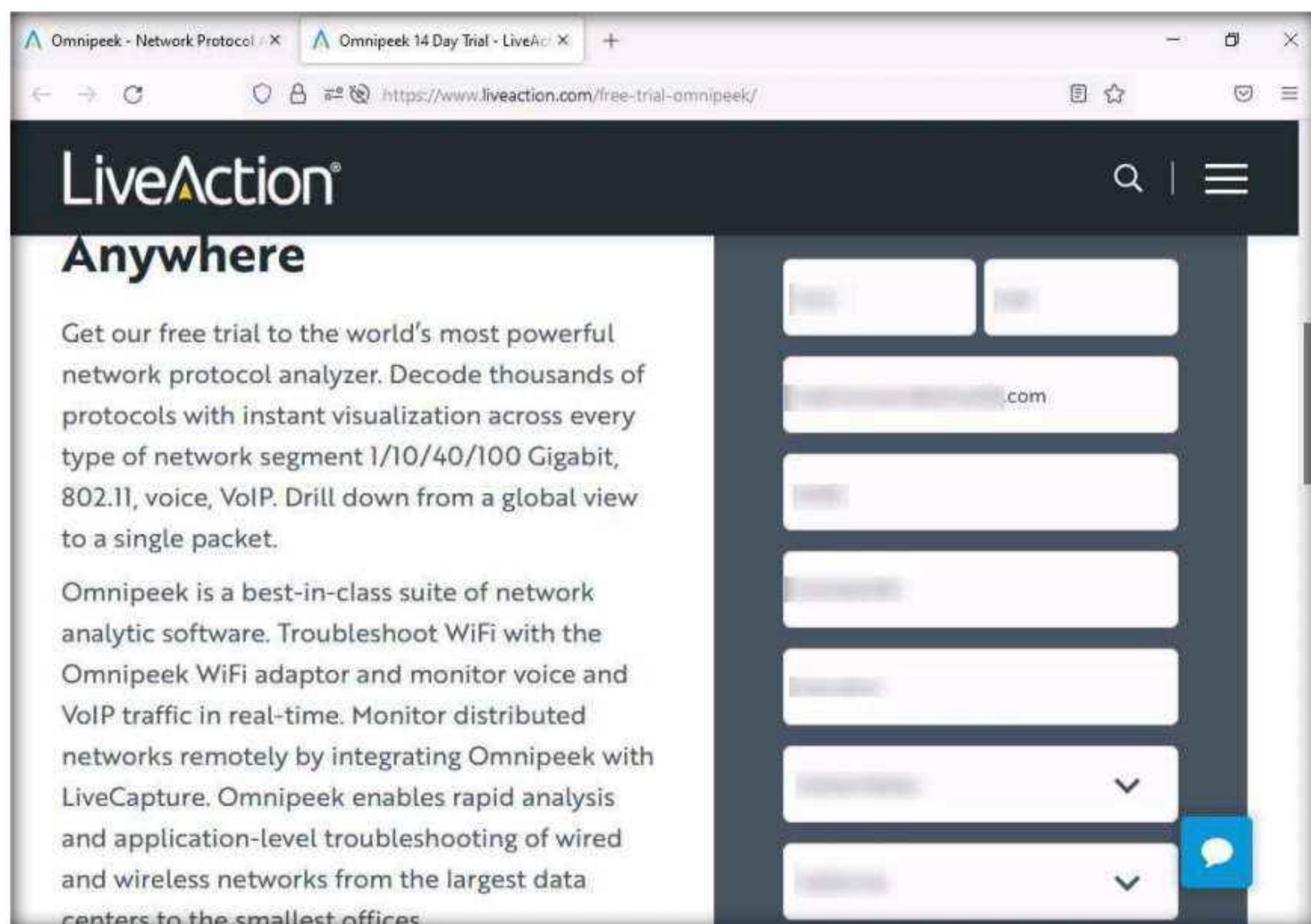
Note: If **Warning: Potential Security Risk Ahead** page appears, click **Advanced**, and click **Accept the Risk and Continue**.

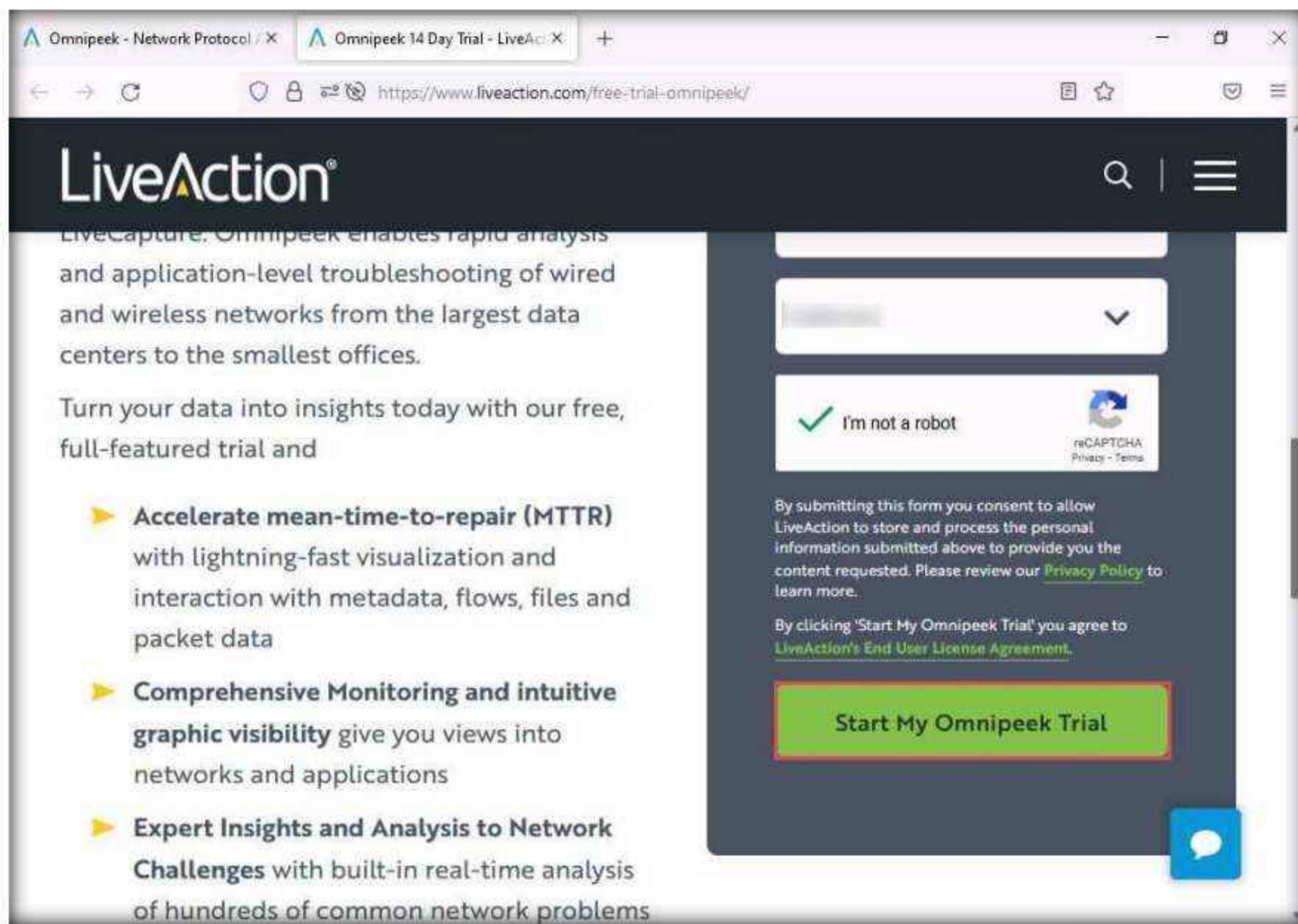
Note: You will be redirected to a cart in live action, click checkout.



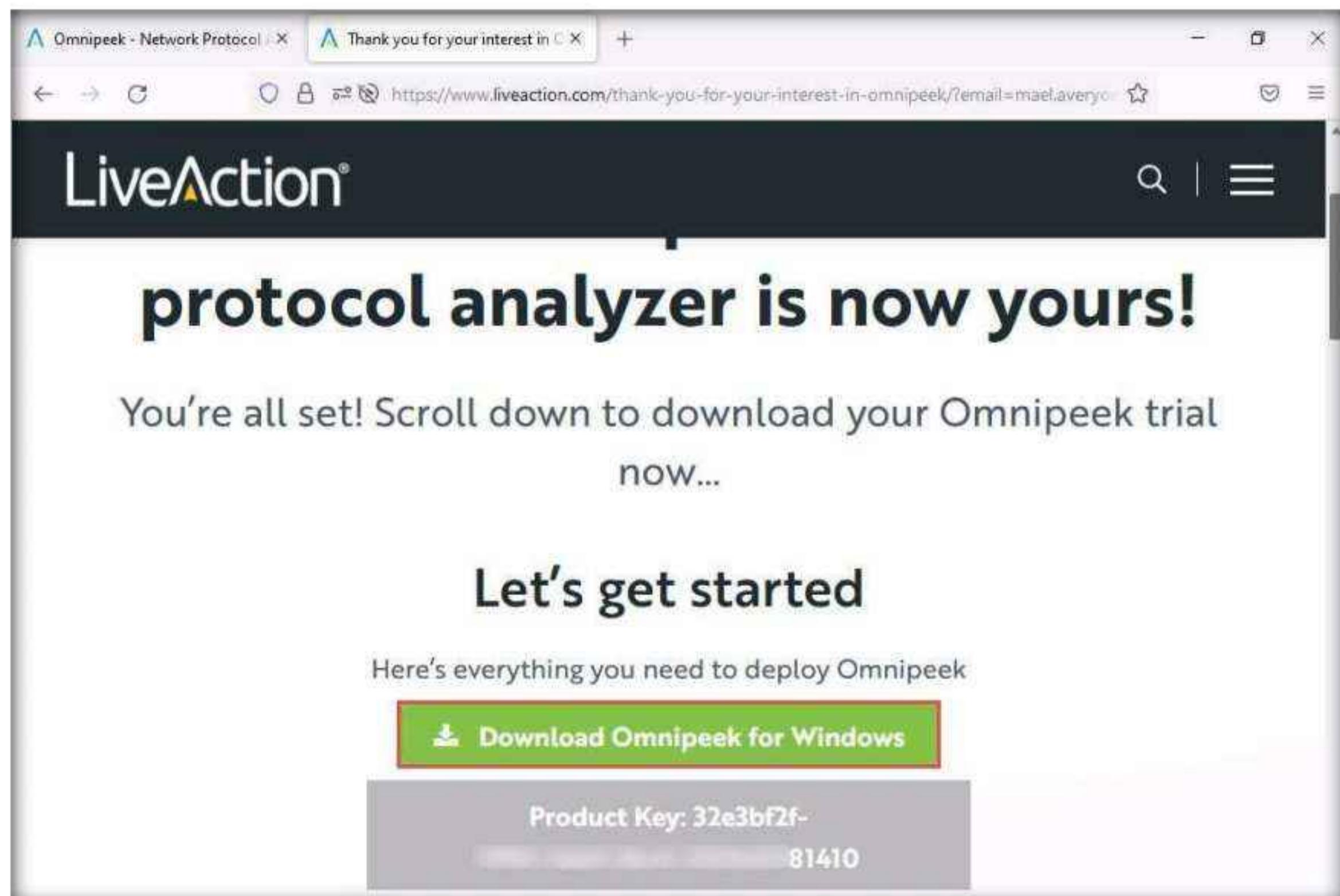
4. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **Start My Omnipack Trial** button.

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 Omnipoke. Click on the **Download Omnipoke for Windows** button to begin the download.



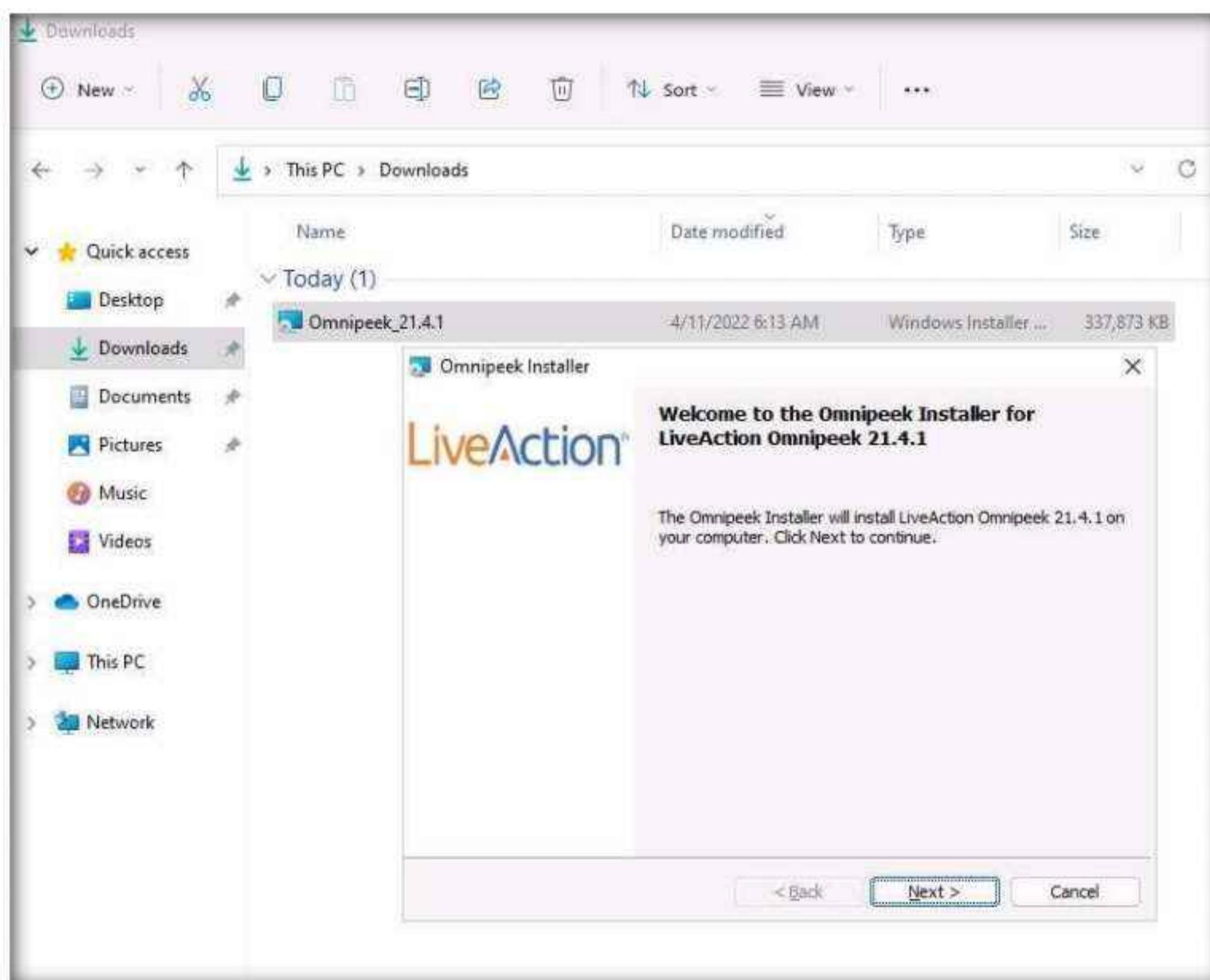
Note: If **Opening Omnipoke_21.4.1msi** pop-up appears; click **Save File** to download the application.

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 **Omnipeek 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 Omnipoke using the default settings.
13. While **Installing LiveAction Omnipoke**, 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 Omnipoke** option is checked, and click **Finish**.

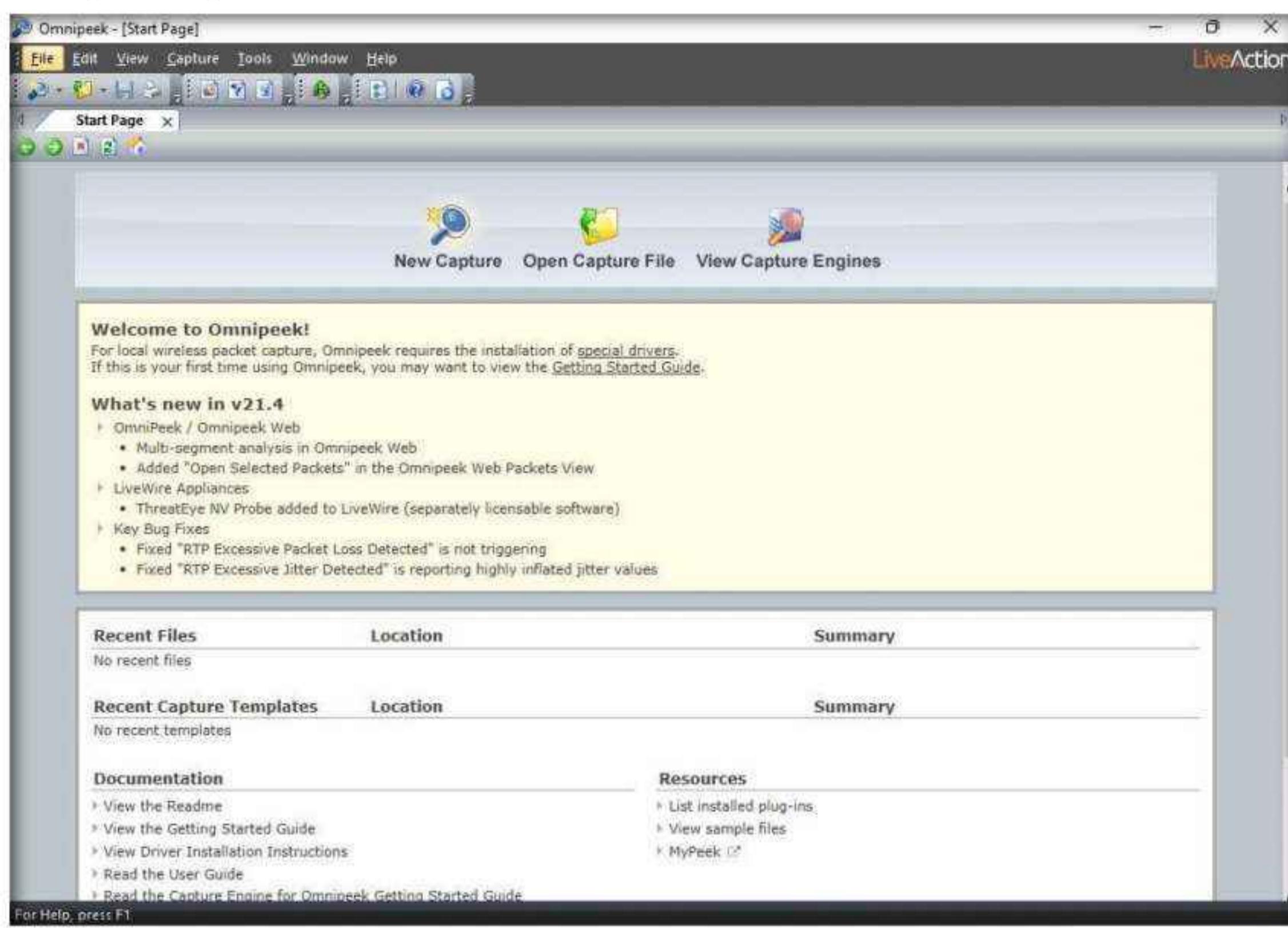
Note: If a **User Account Control** pop-up appears, click **Yes**.



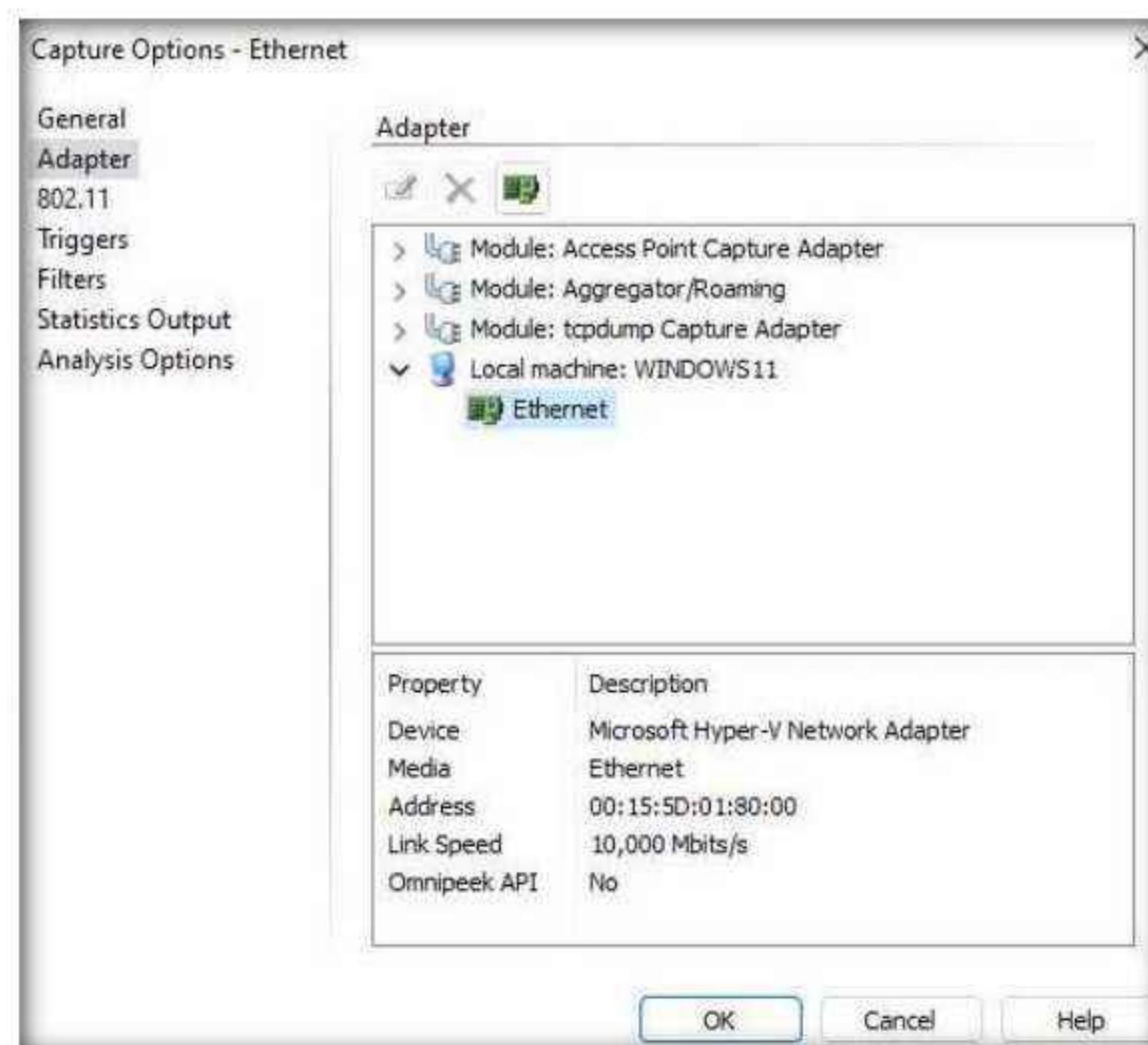
15. The **Omnipeek** evaluation dialog-box appears; click **OK**.

Module 08 – Sniffing

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

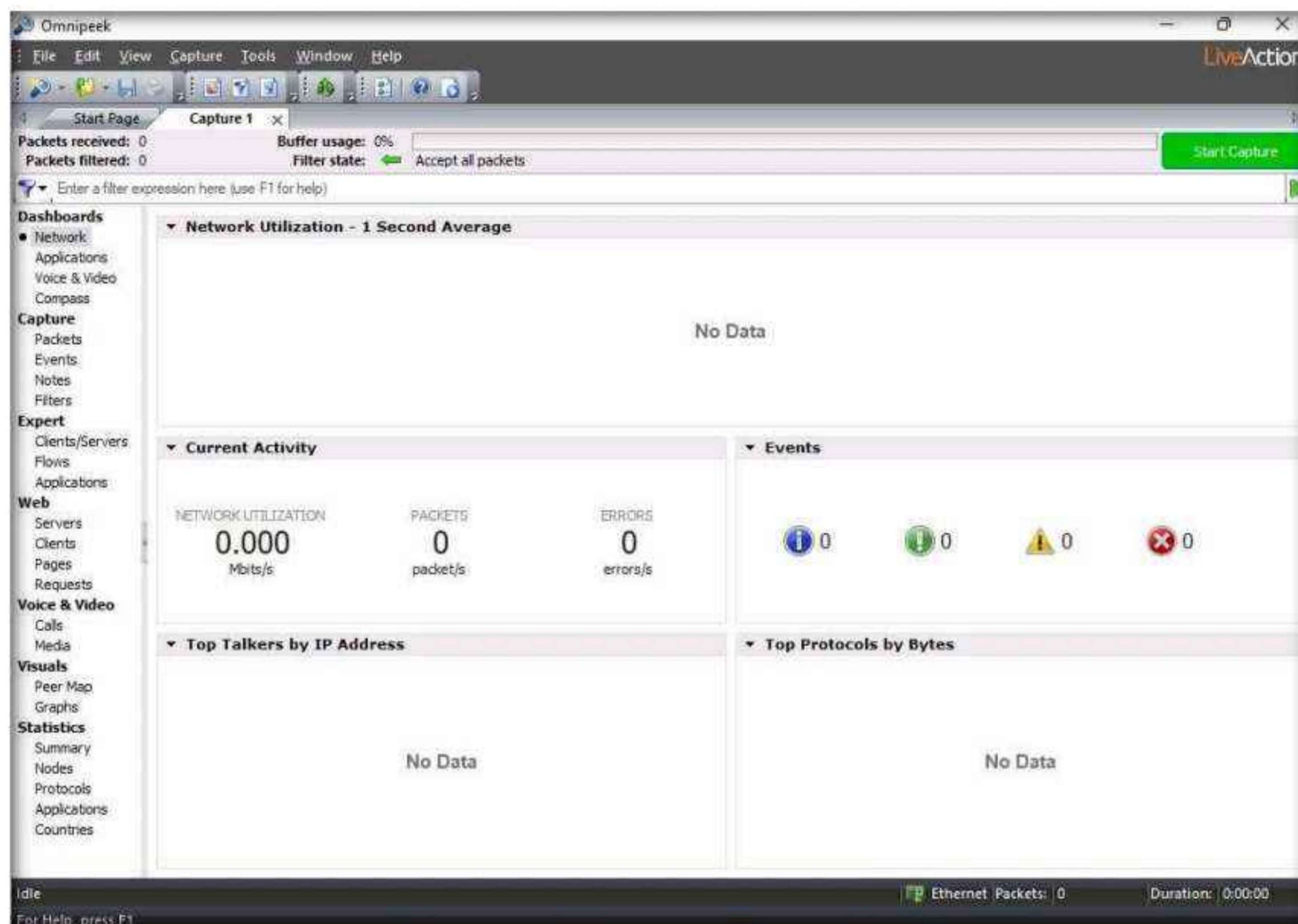


18. The **Capture Options** window appears; by default, the **Adapter** option opens-up.
19. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS11** node, select **Ethernet**, and click **OK**.



Module 08 – Sniffing

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

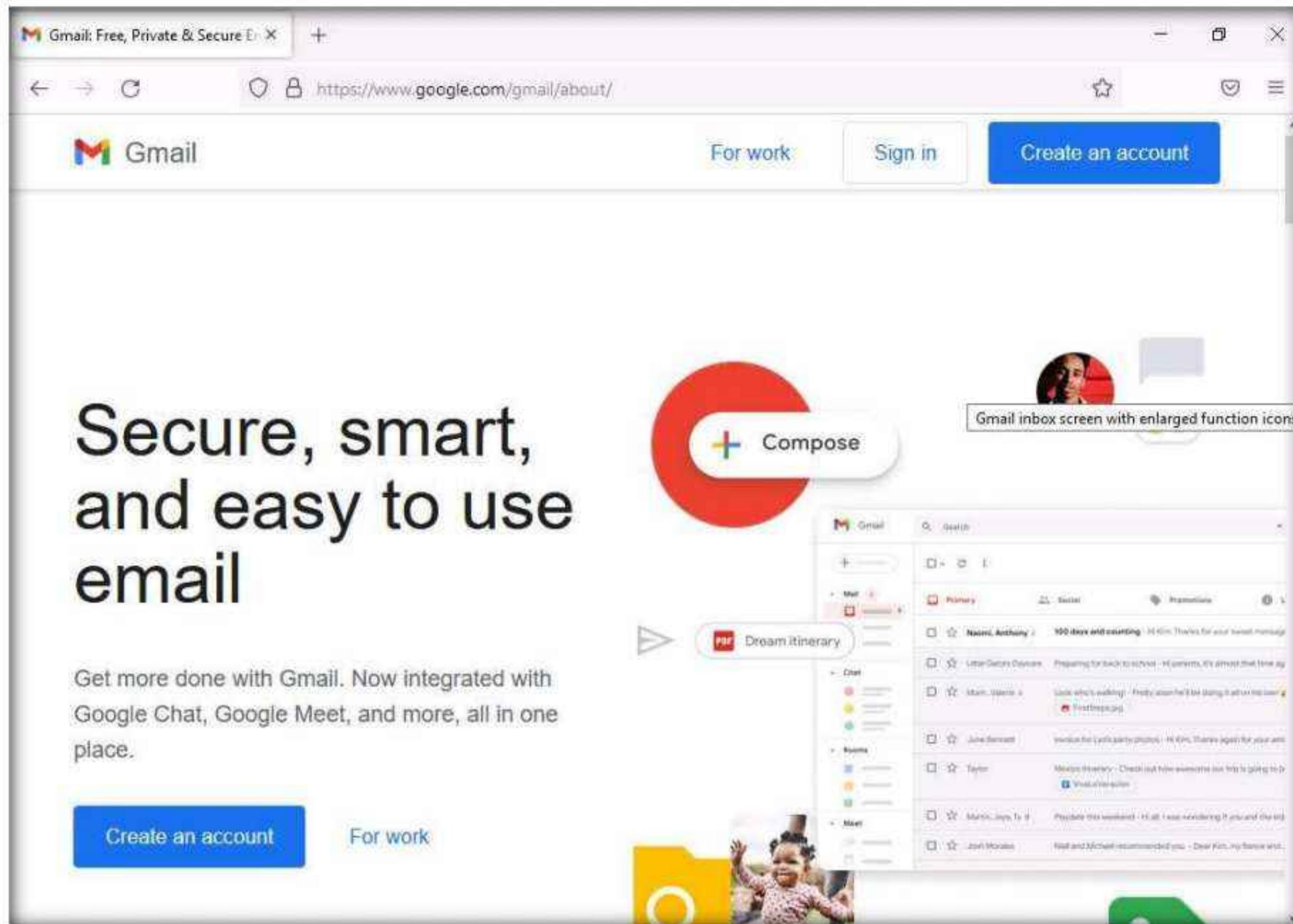


21. The **Start Capture** button changes to read “**Stop Capture**” and traffic statistics begin to populate **Network** under the **Dashboards** section, as shown in the screenshot.



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>).

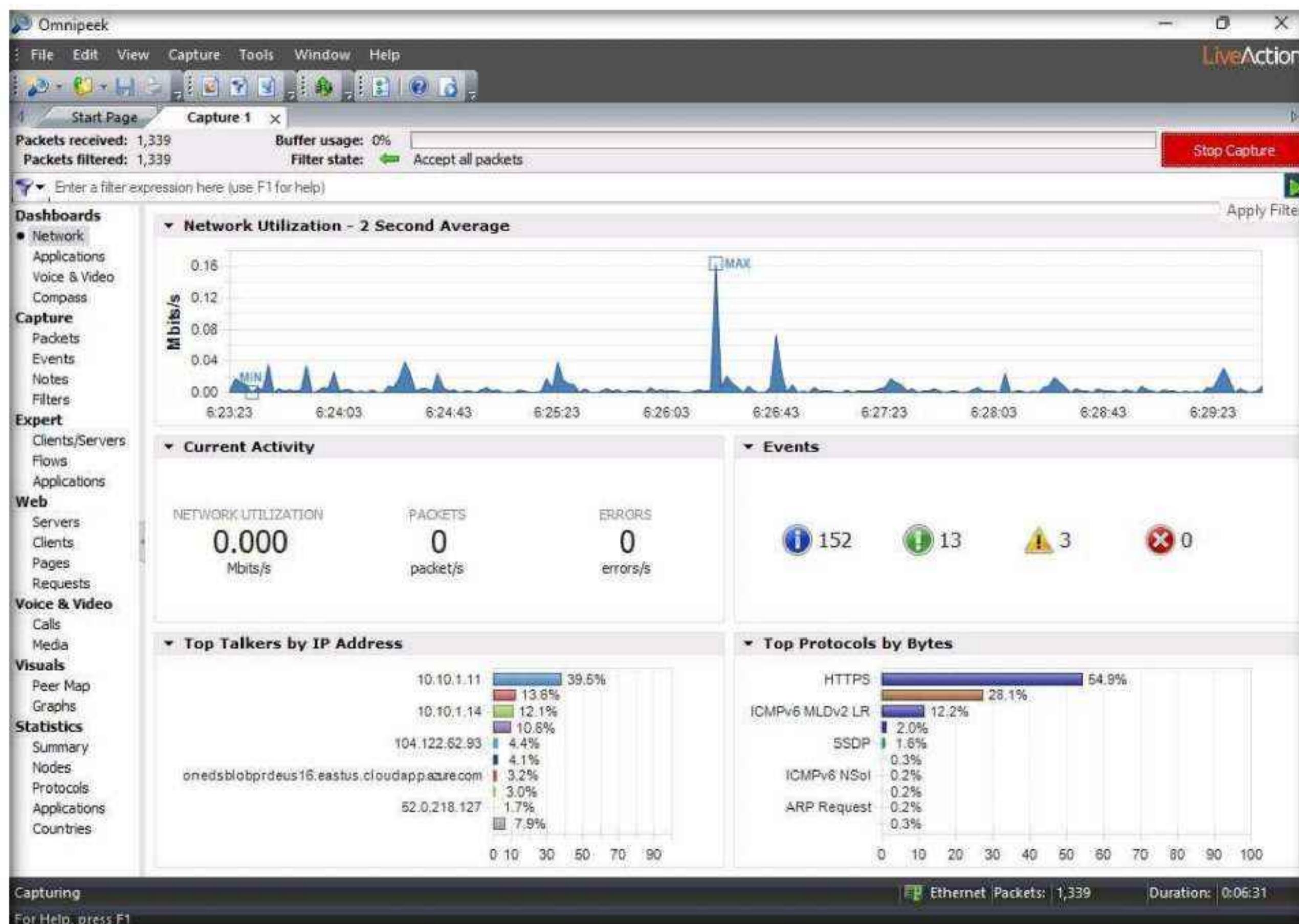
Note: Social networking websites are blocked from this environment due to some security reasons. However, if you want to run this lab task you can use some other website of your choice or else you can run this task in your local environment.



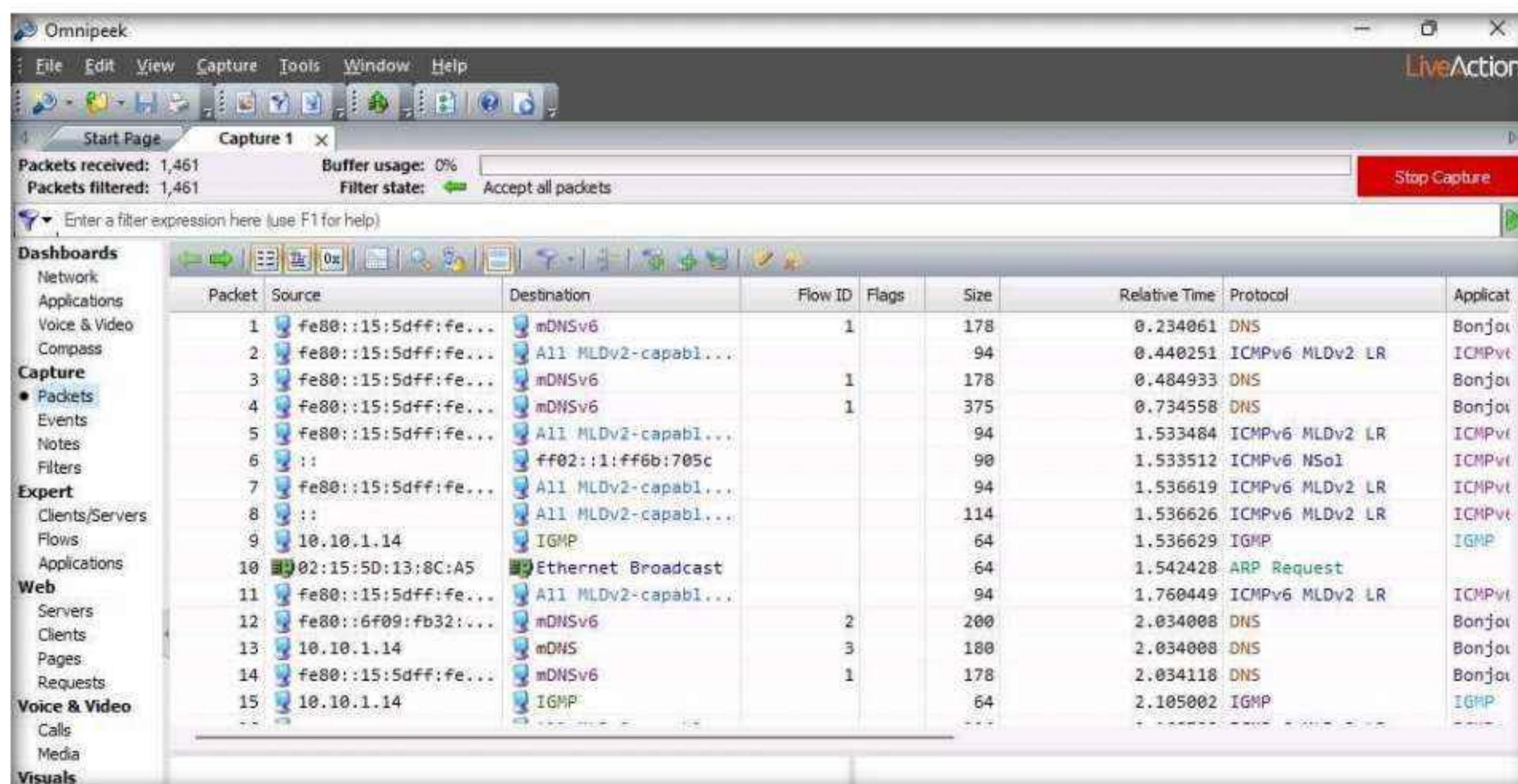
24. Now, switch back to the **Windows 11** virtual machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.

Module 08 – Sniffing

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

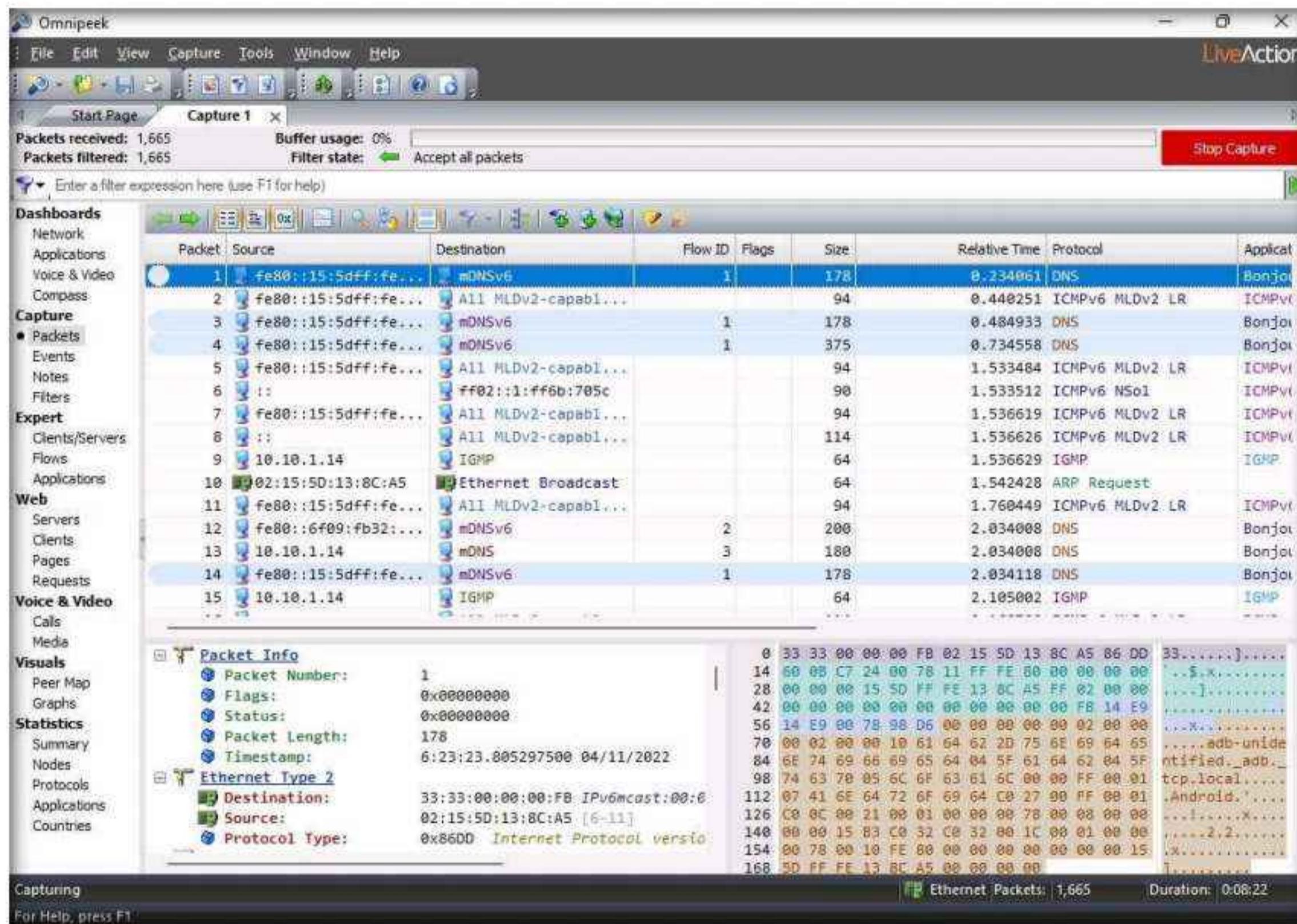


26. To view the captured packets, select **Packets** under the **Capture** section in the left-hand pane. You can observe the outgoing and incoming network packets of the target system.

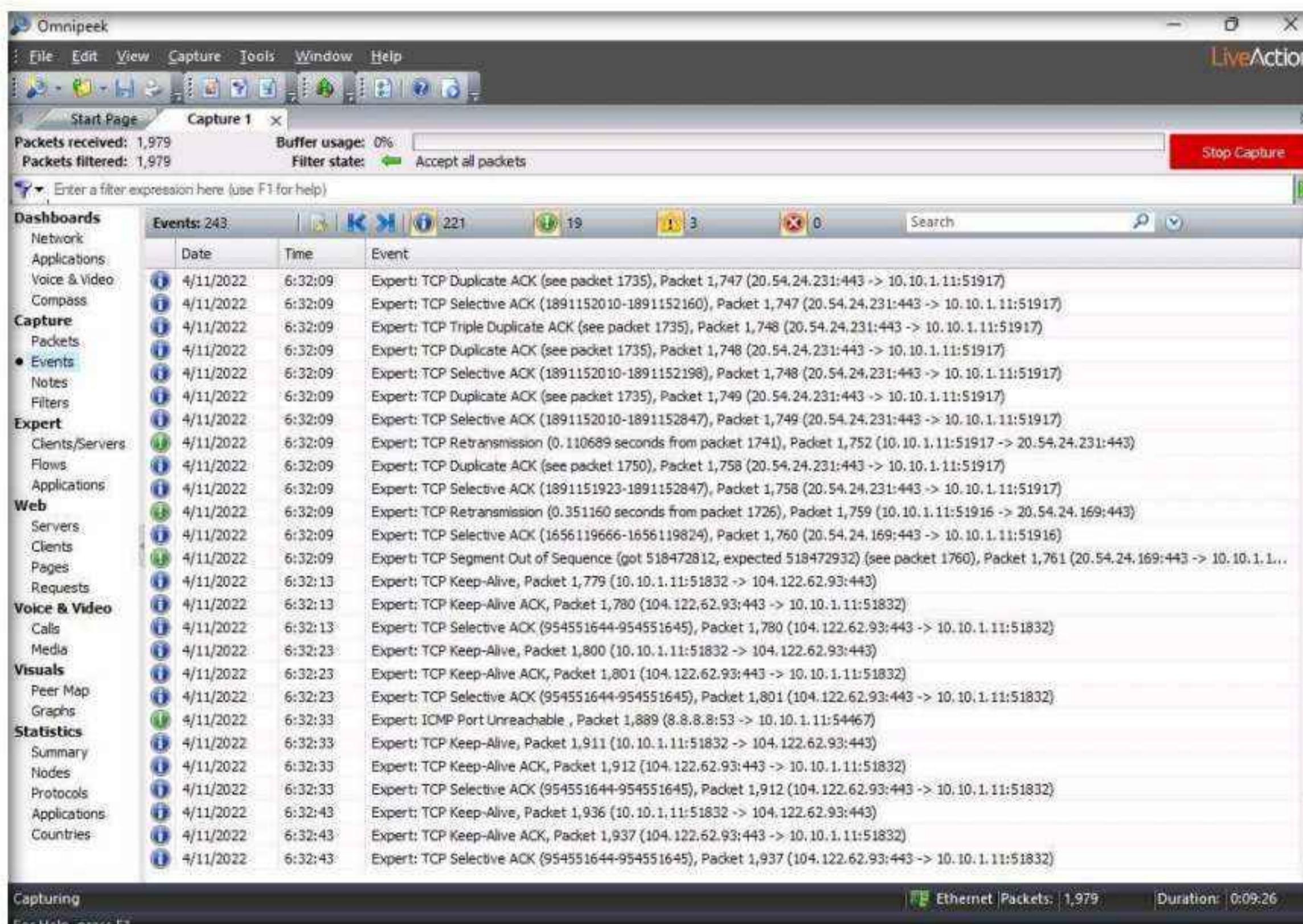


Module 08 – Sniffing

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

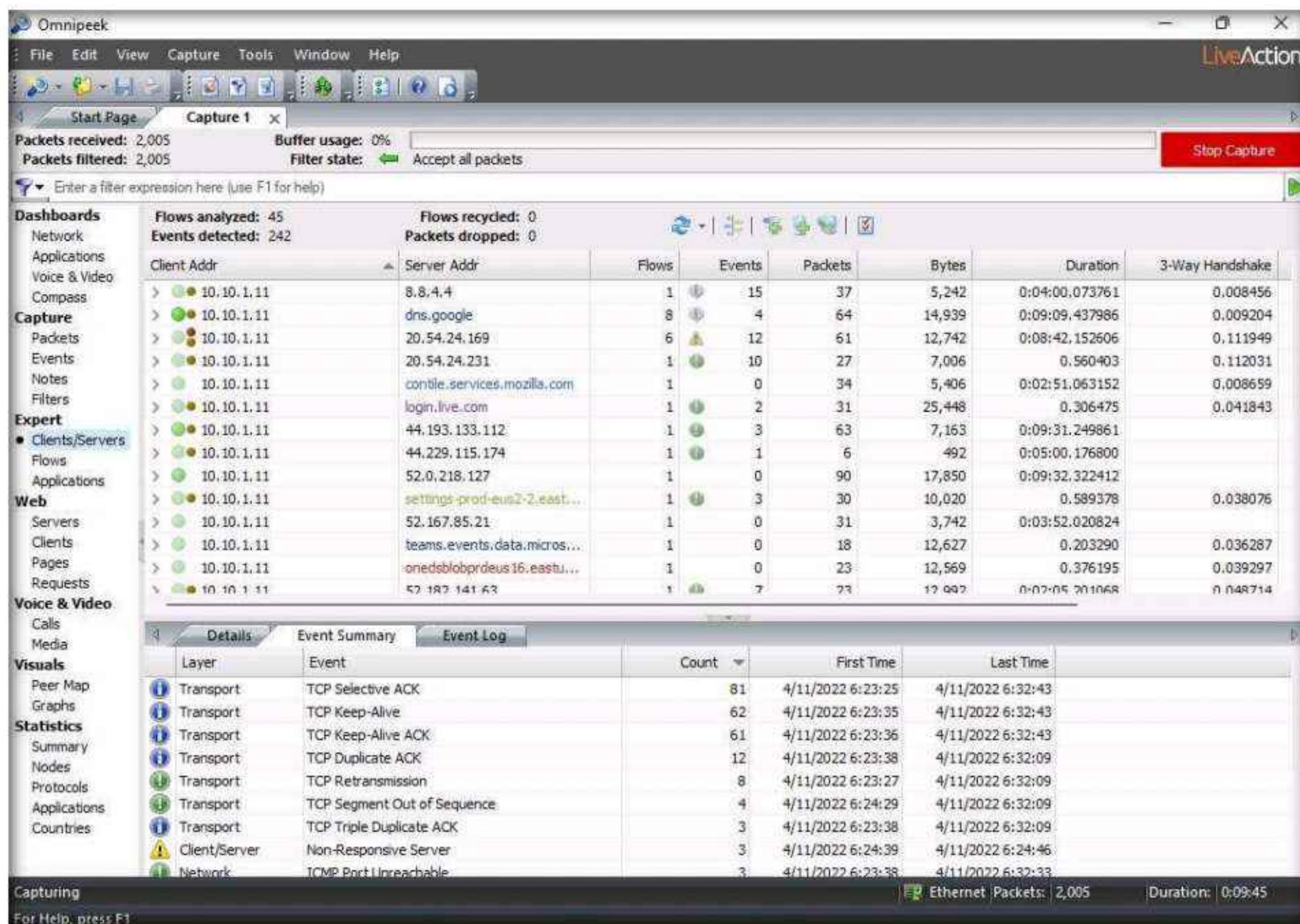


28. Click **Events** under the **Capture** section in the left-hand pane to view the events occurring in the network.



Module 08 – Sniffing

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

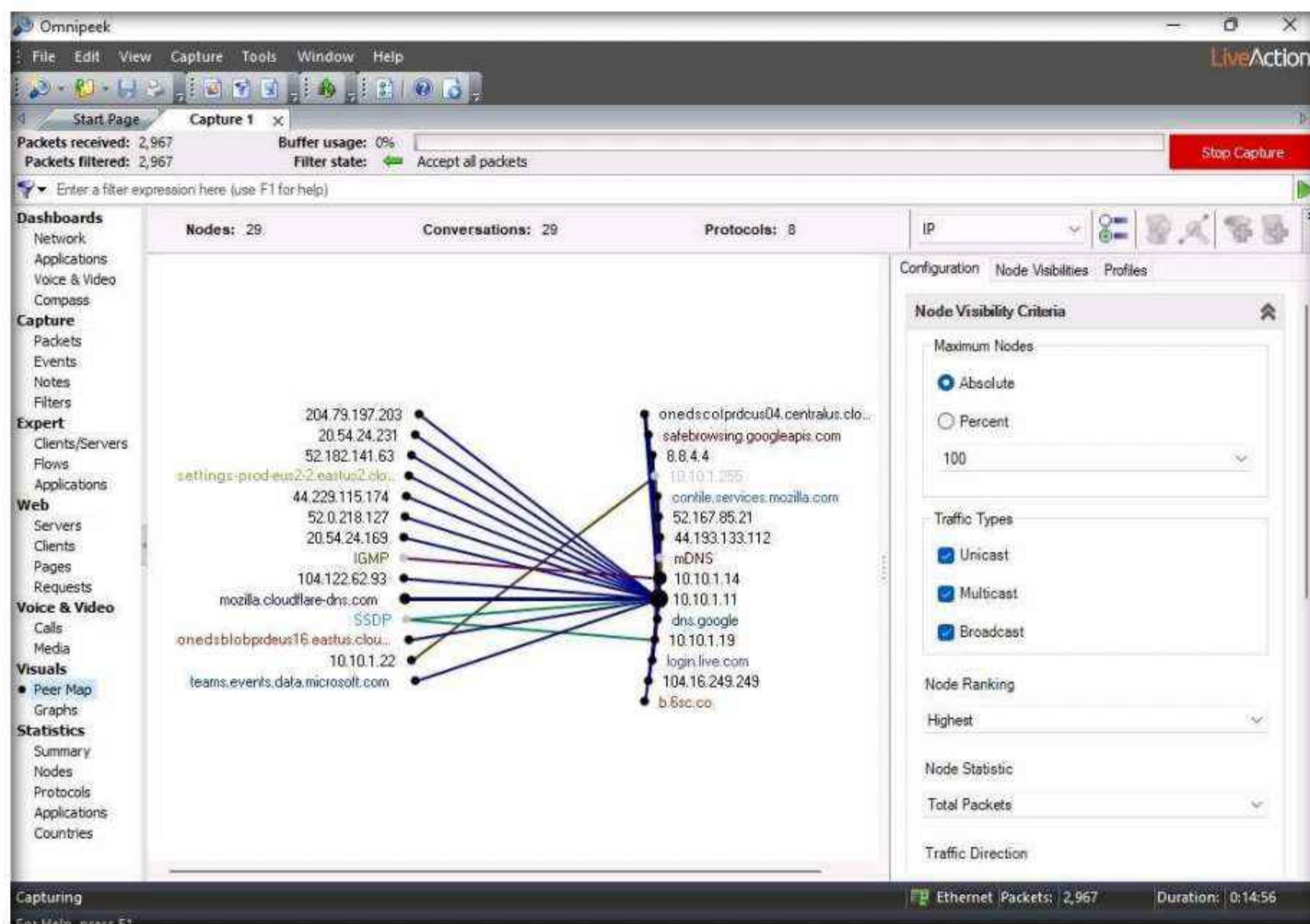


30. Similarly, under the **Flows** and **Applications** options, you can view the packet flow and applications running on the systems in the local network.

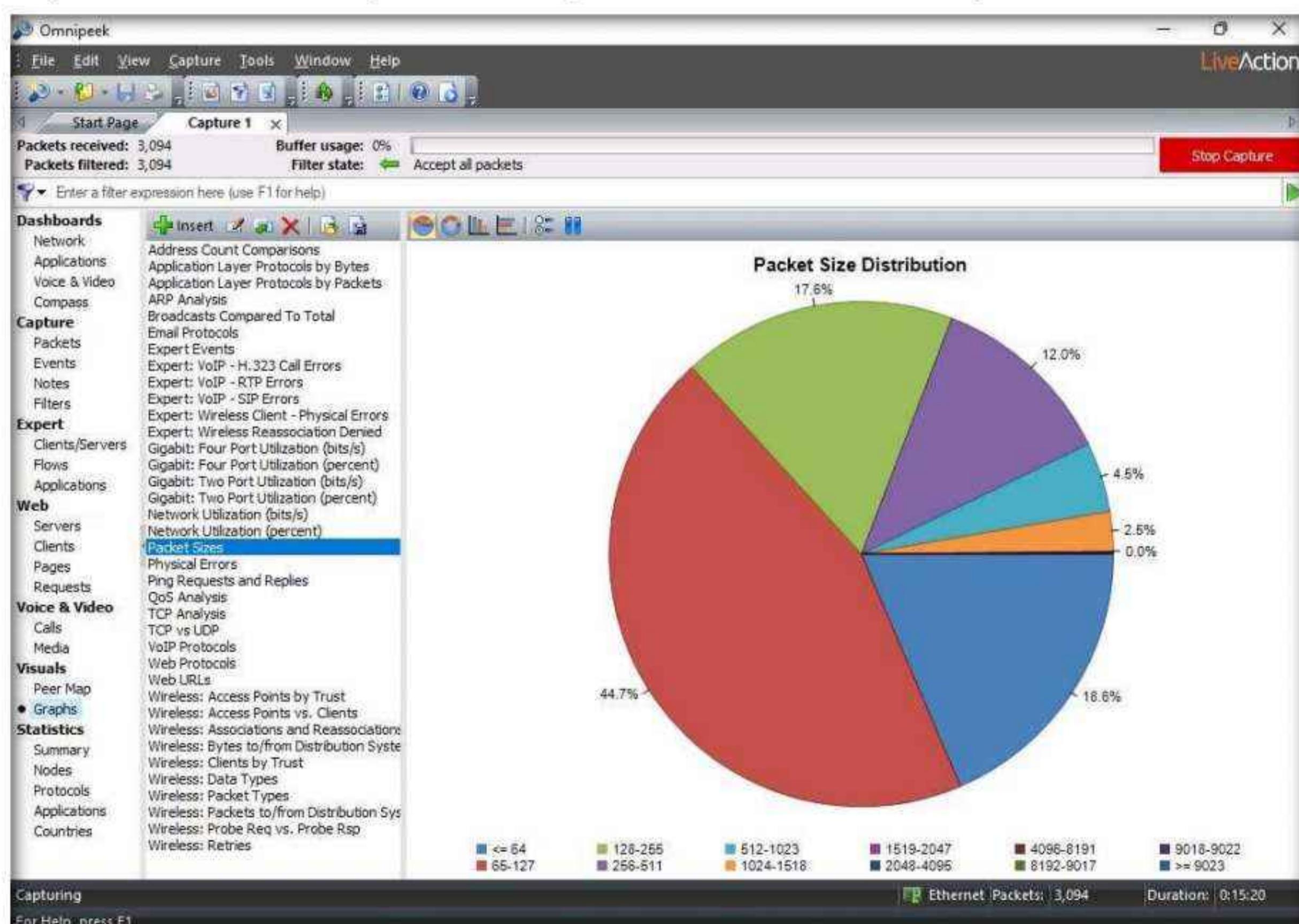
31. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.
32. Click **Peer Map** under the **Visuals** section in the left-hand pane to show a mapped view of the network traffic. By default, all **Traffic Types (Unicast, Multicast, and Broadcast)**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

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

Module 08 – Sniffing

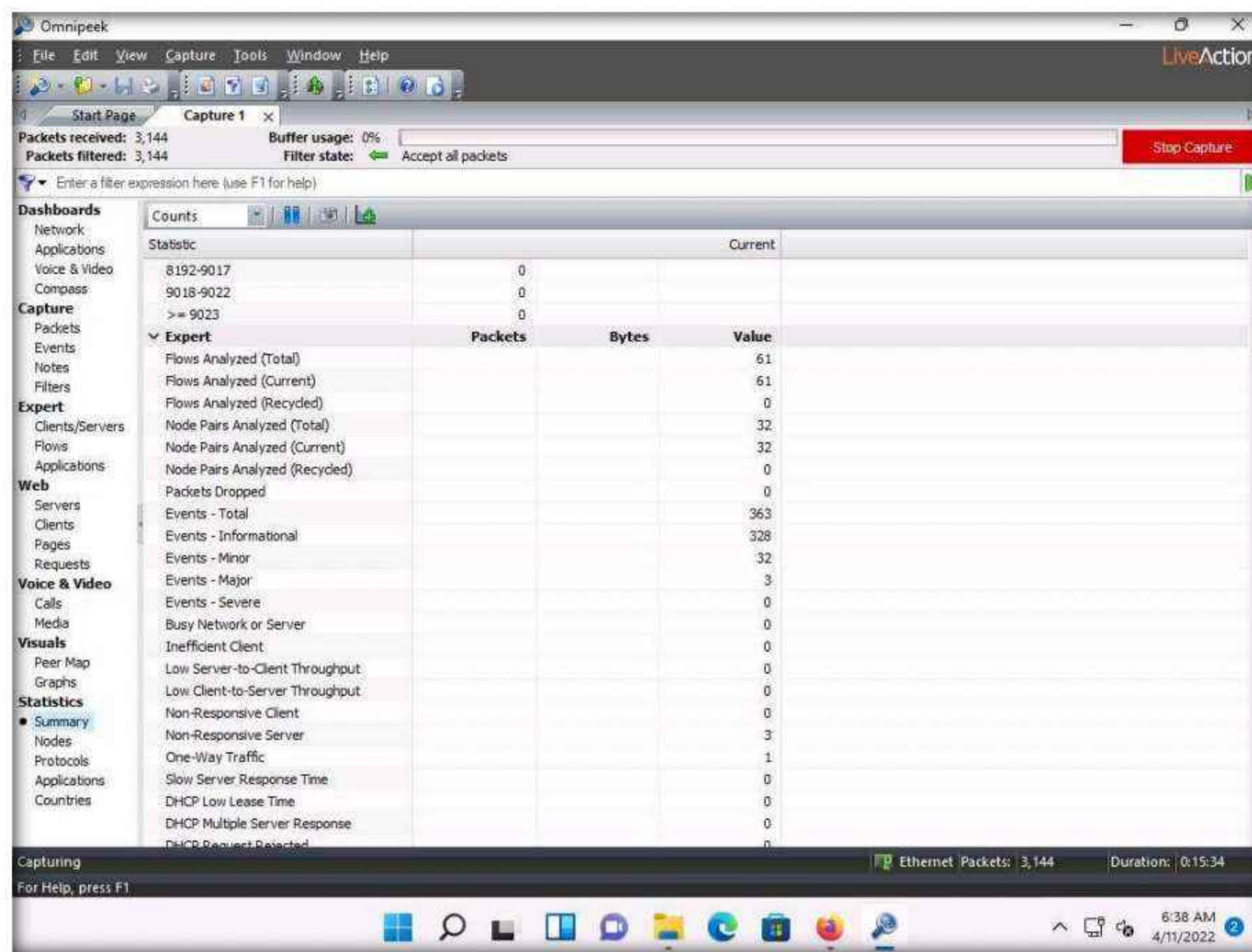


33. Similarly, under the **Visuals** section, you can click the **Graphs** option to show graphs on packet size, QoS analysis, TCP analysis, TCP vs. UDP, and web protocols.



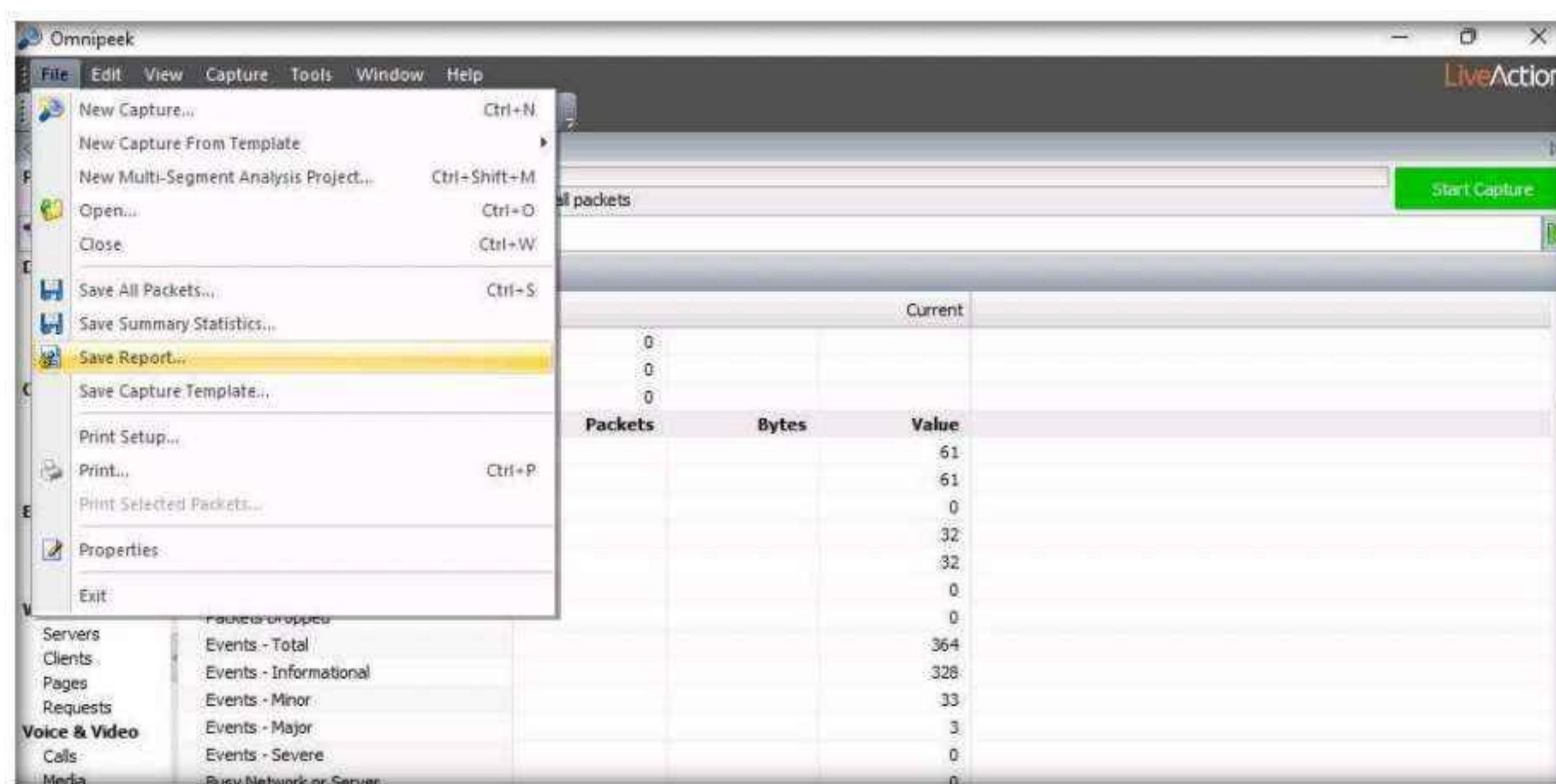
Module 08 – Sniffing

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

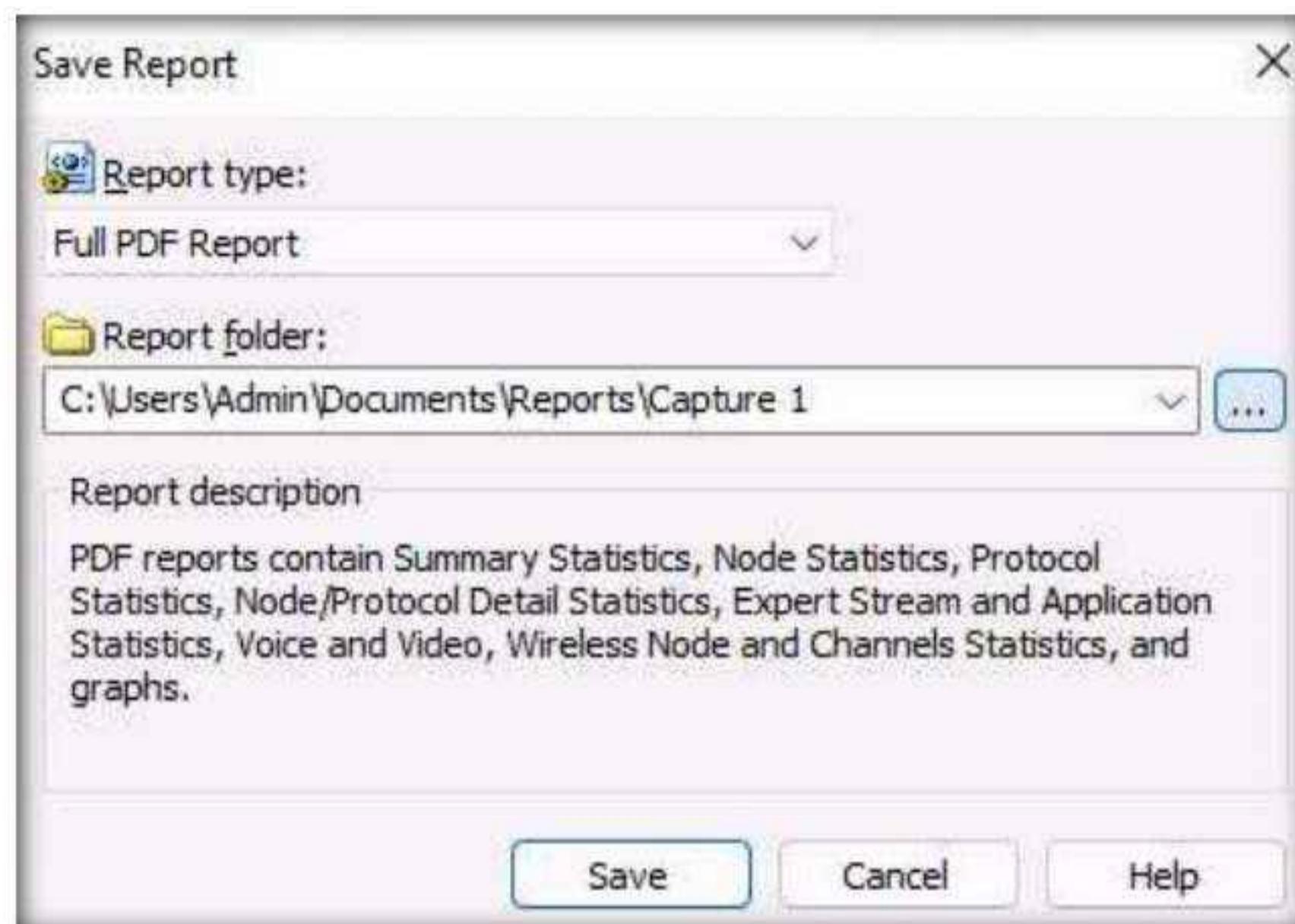


35. Stop the packet capturing by clicking on the **Stop Capture** button in the right-hand corner of the window. The **Stop Capture** button will toggle back to the **Start Capture** button.

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

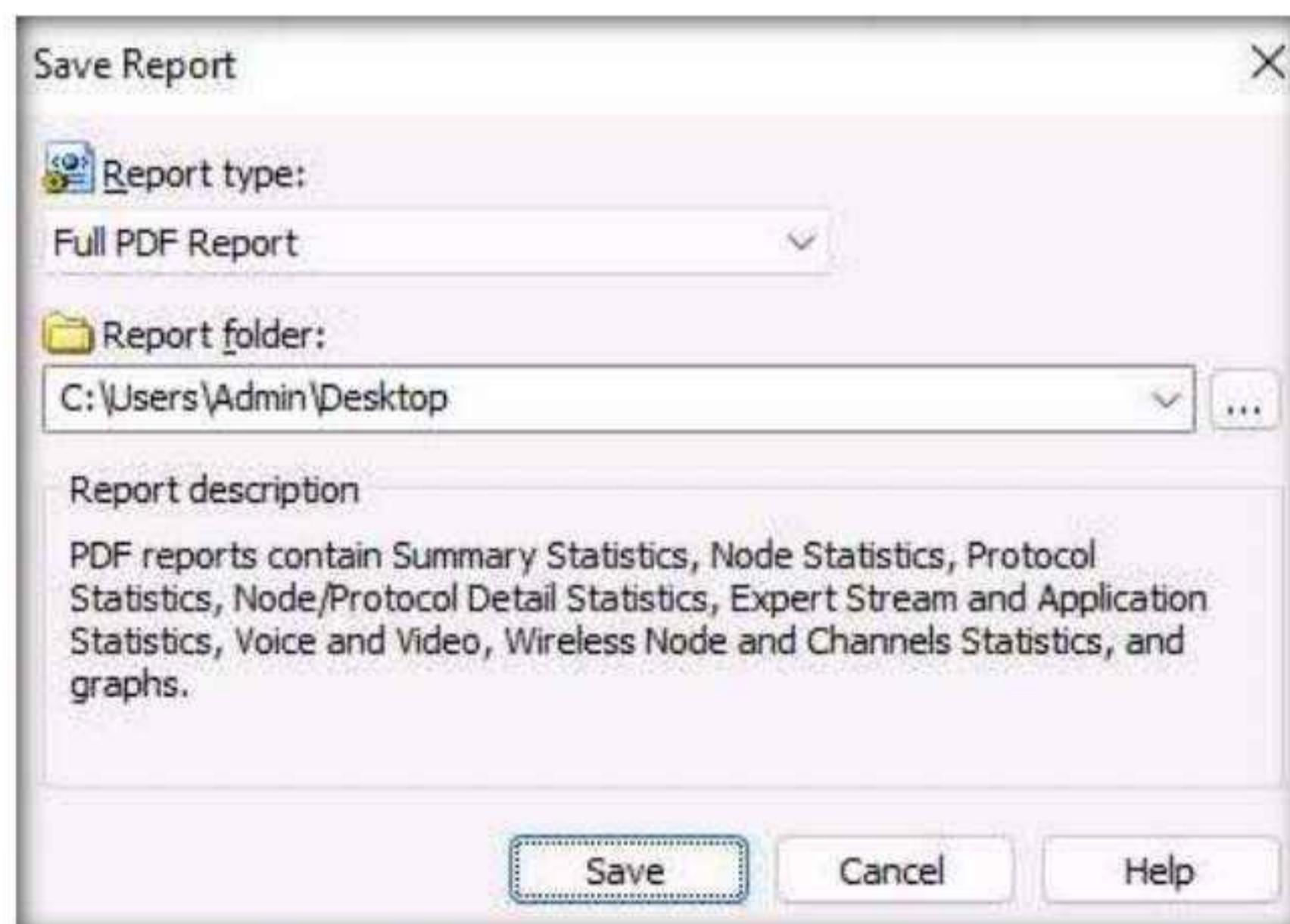


37. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon to change the download location.



38. The **Browse For Folder** window appears; select the **Desktop** as your save location and click **OK**.

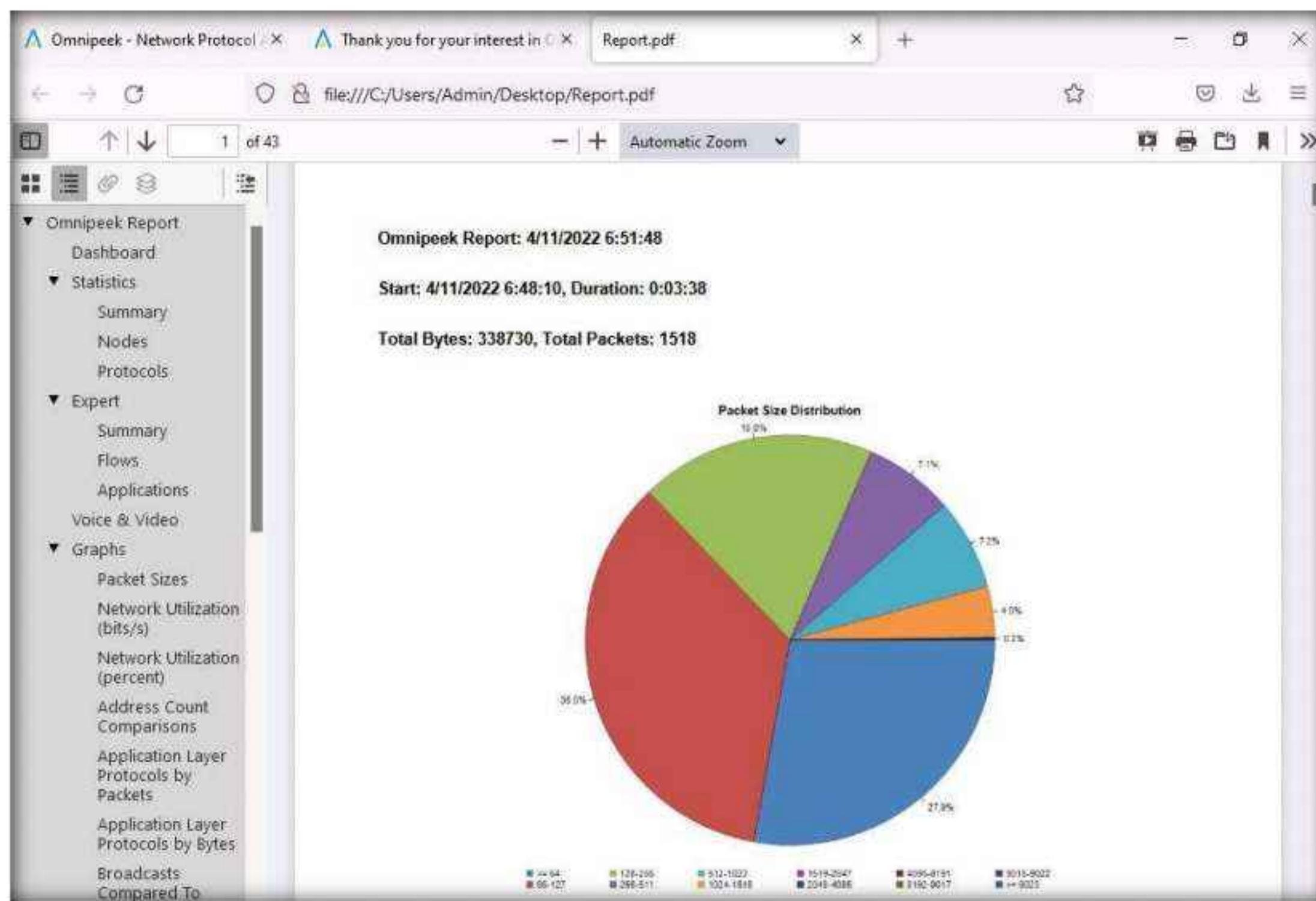
39. The changed save location appears in the **Report folder** field; click the **Save** button to save the report.



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**.

Module 08 – Sniffing



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

The figure shows a screenshot of the Omnipacket Network Protocol Analyzer interface, specifically the 'Summary' section of the 'Statistics' report. The table provides a detailed breakdown of network traffic statistics. The columns include Name, Bytes, Packets, Pct of Bytes, and Pct of Packets.

Name	Bytes	Packets	Pct of Bytes	Pct of Packets
Group: General				
Start Date	4/11/2022	4/11/2022	4/11/2022	4/11/2022
Start Time	6:48:10	6:48:10	6:48:10	6:48:10
Duration	0:03:38	0:03:38	0:03:38	0:03:38
Group: Network				
Total Bytes	338394	N/A	100.000	N/A
Total Packets	N/A	1514	N/A	100.000
Total Broadcast	855	9	0.253	0.594
Total Multicast	67799	378	20.036	24.967
Average Utilization (percent)	0.000	0.000	0.000	0.000
Average Utilization (bits/s)	12862	12862	12862	12862
Current Utilization (percent)	0.000	0.000	0.000	0.000
Current Utilization (bits/s)	8936	8936	8936	8936
Max Utilization (percent)	0.004	0.004	0.004	0.004
Max Utilization (bits/s)	427304	427304	427304	427304
Group: Errors				
Total	N/A	0	N/A	0.000
CRC	N/A	0	N/A	0.000
Frame Alignment	N/A	0	N/A	0.000
Runt	N/A	0	N/A	0.000
Oversize	N/A	0	N/A	0.000

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 Omnipacket Network Protocol Analyzer.

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

Task 3: Analyze a Network using the SteelCentral Packet Analyzer

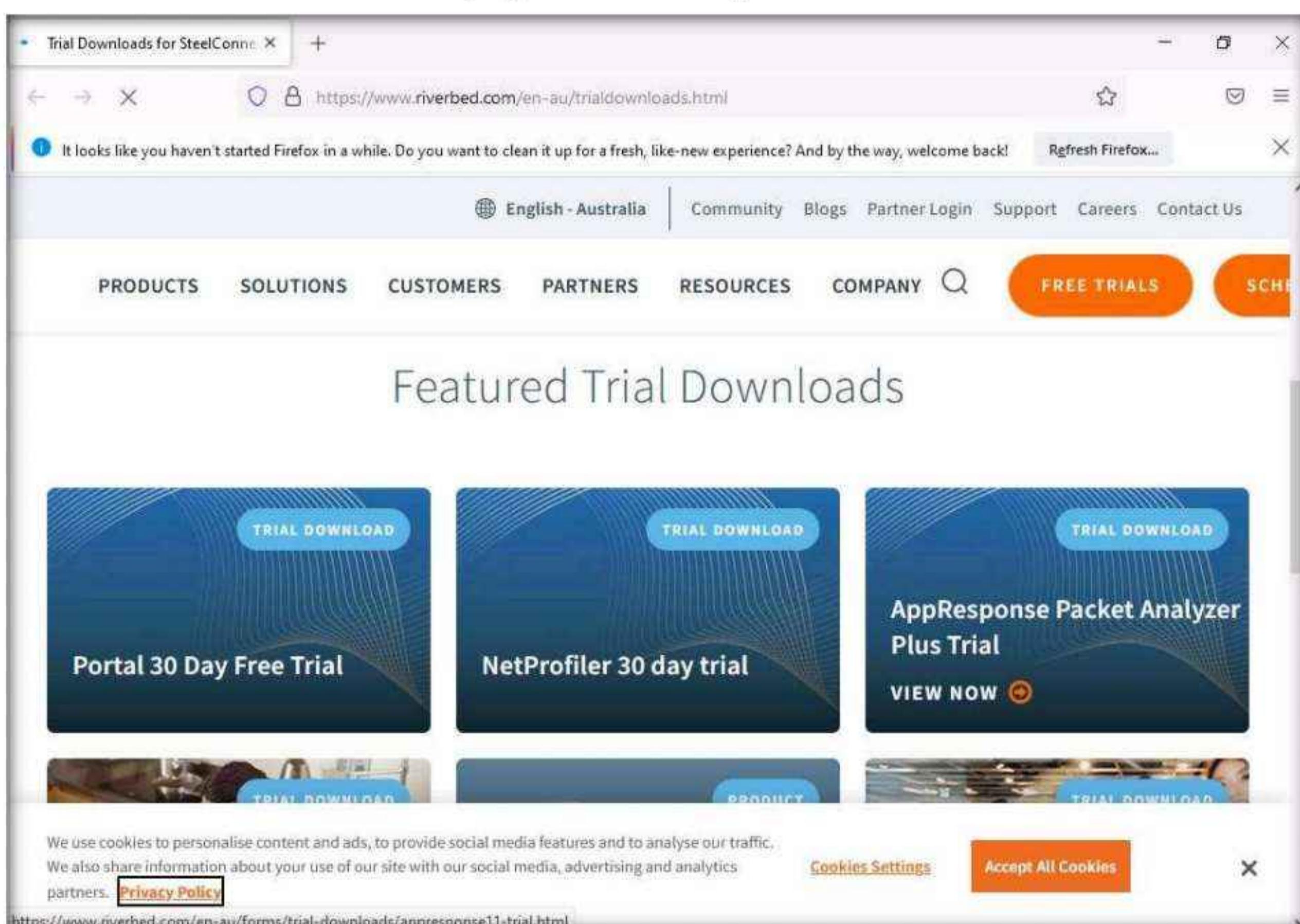
SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (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.

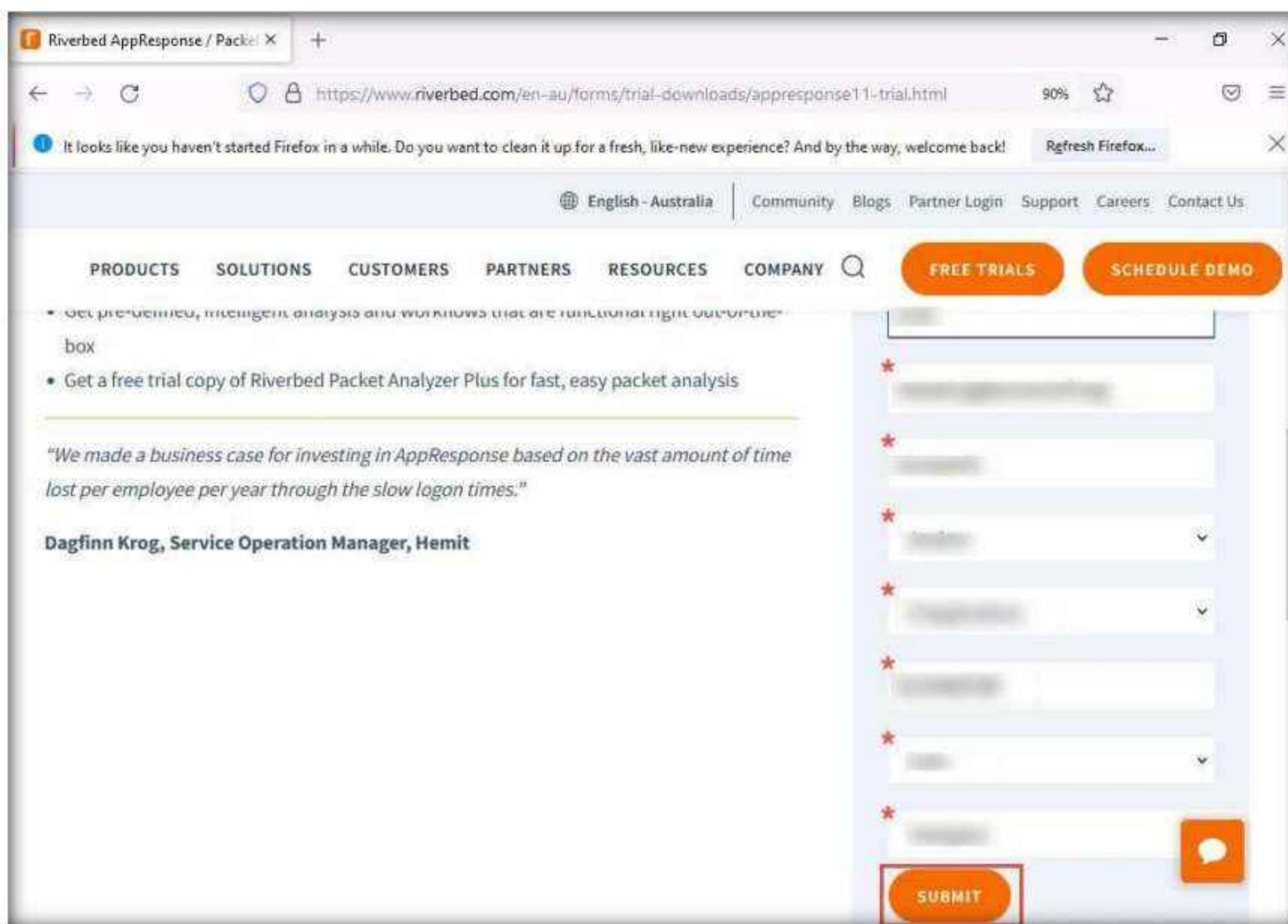
Note: At the bottom of the page click on **Accept All Cookies**.



Module 08 – Sniffing

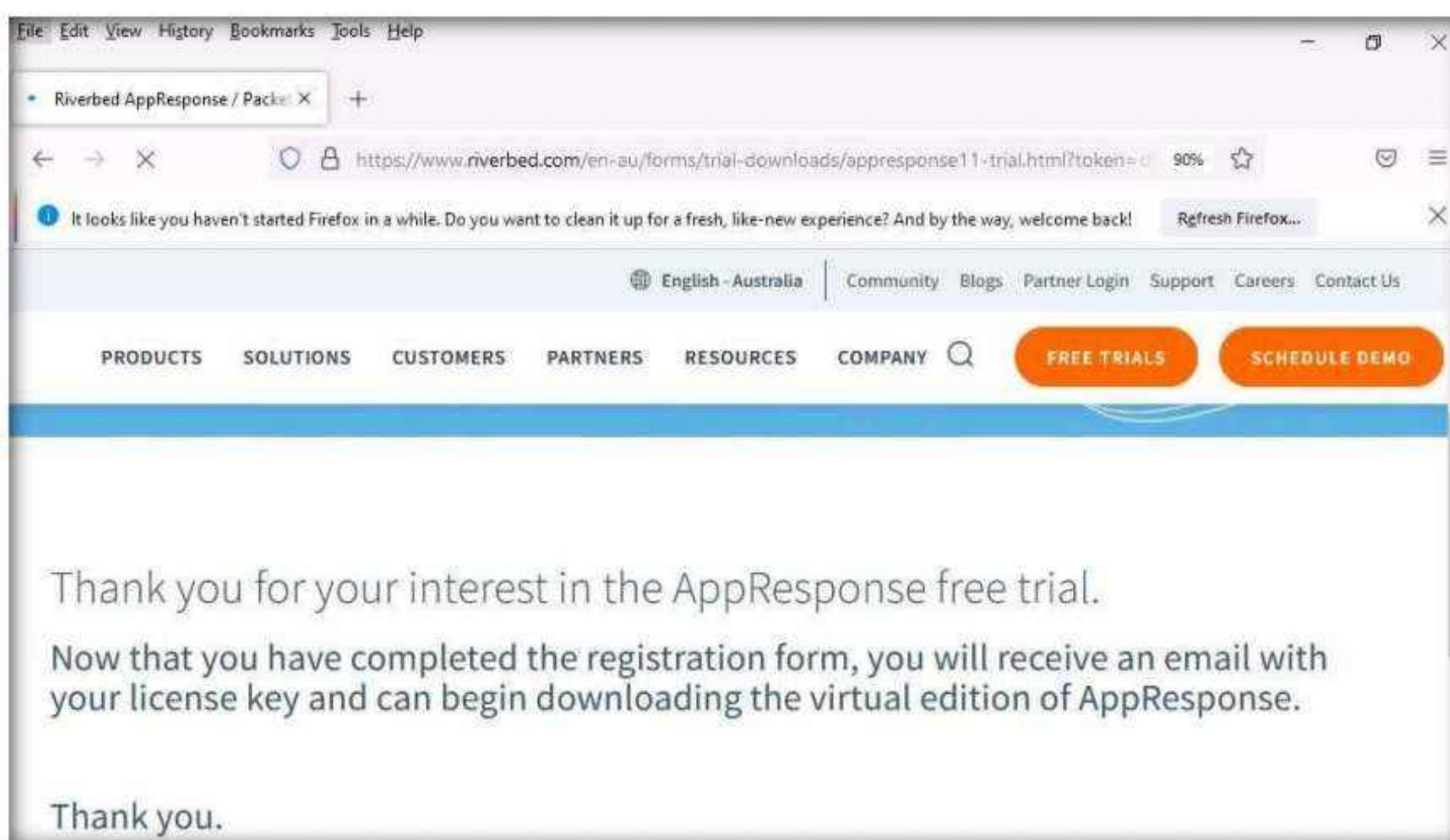
3. A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.

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

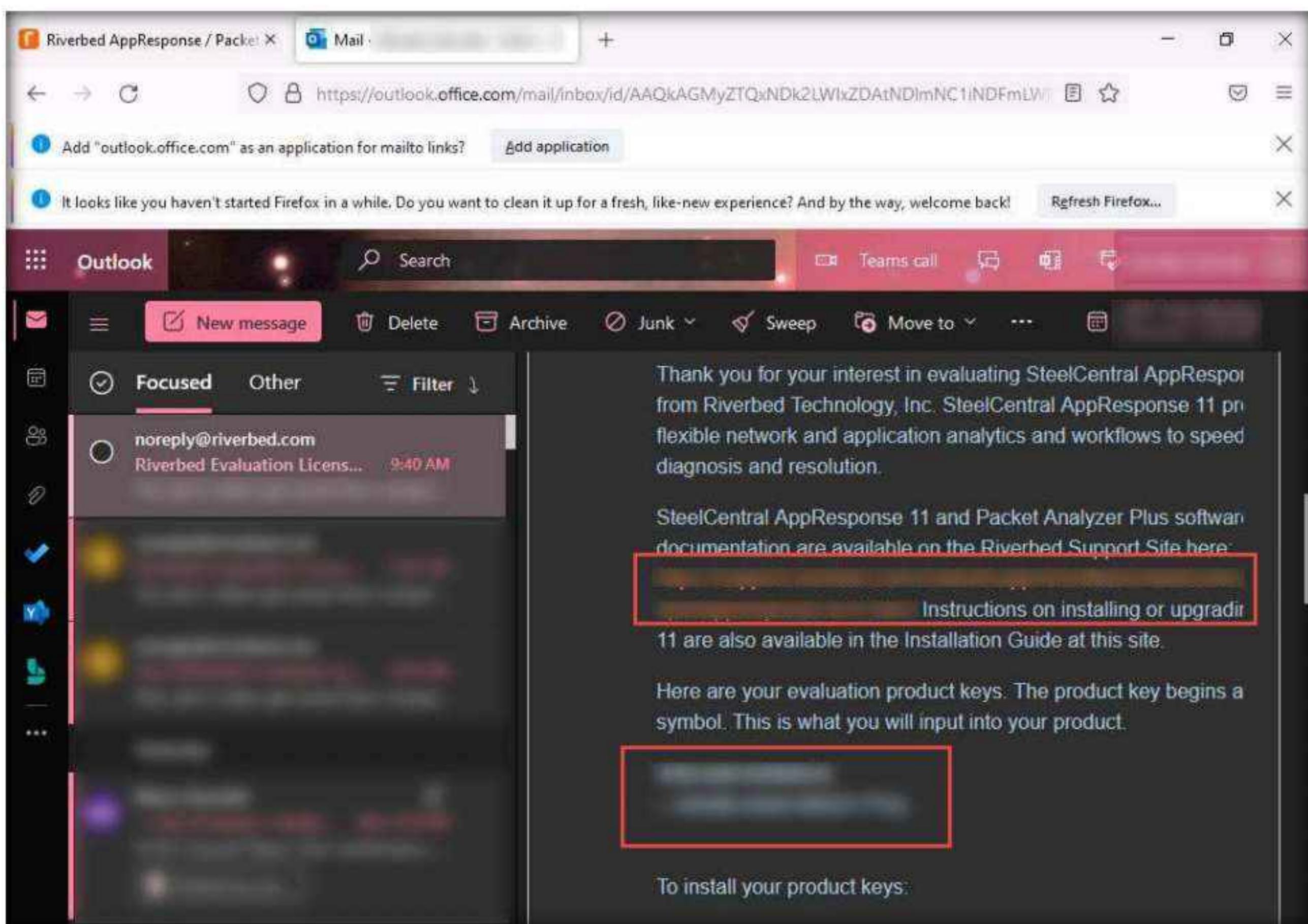


Note: If a **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

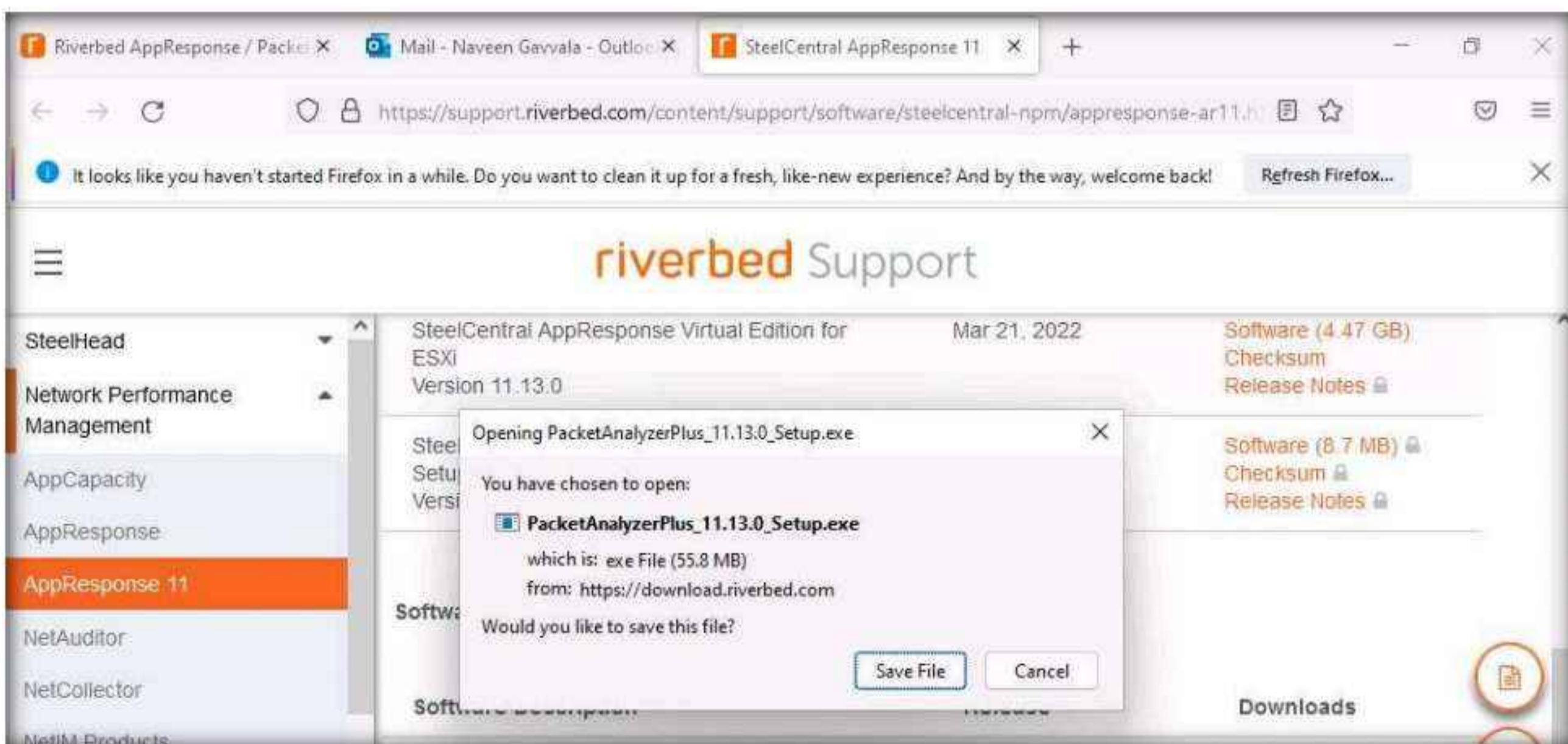
4. A **Thank You** webpage appears with information regarding the trial version.



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.

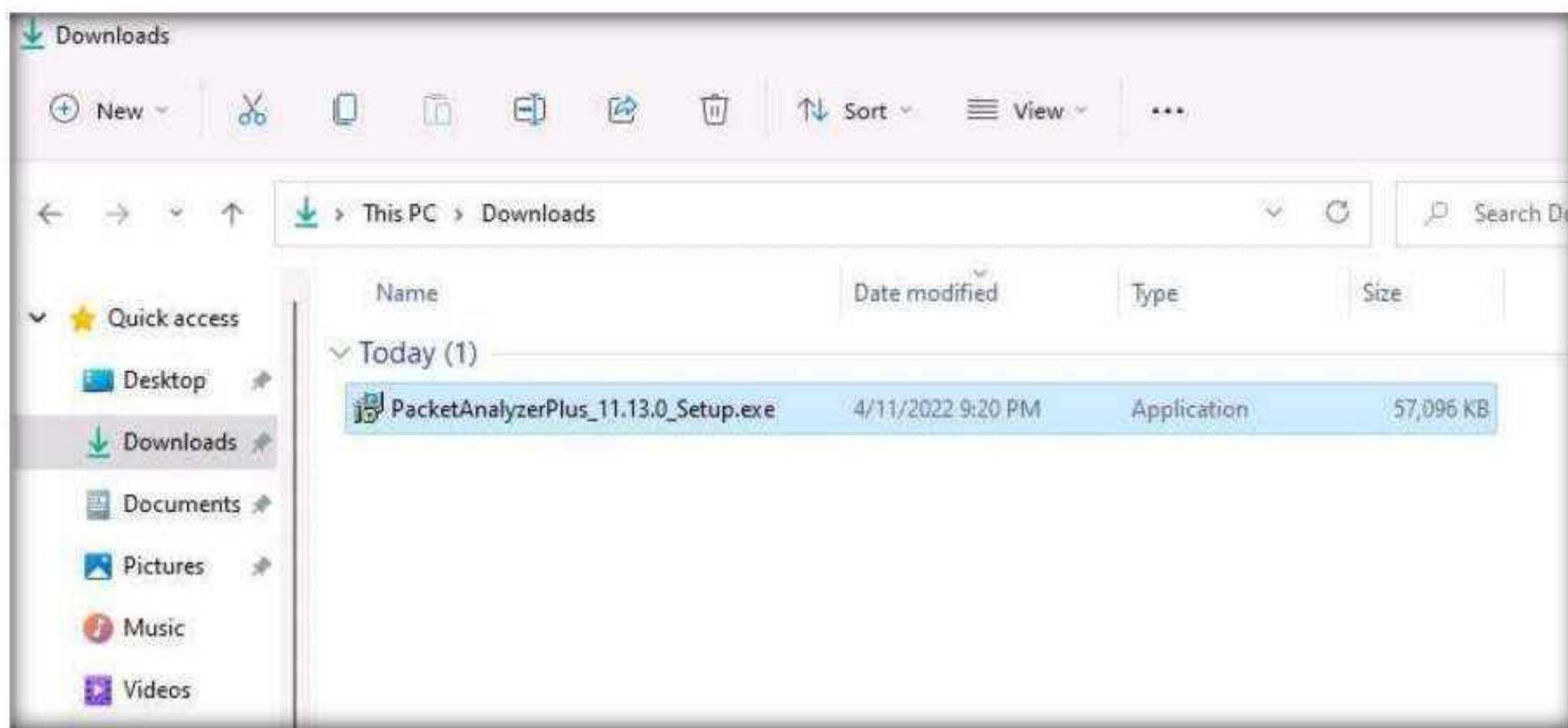


6. The Opening **PacketAnalyzer_11.13.0_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.



Module 08 – Sniffing

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.

