Module 08: Sniffing

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.

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

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:

1. Perform active sniffing
    - 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

2. Perform network sniffing using various sniffing tools
    - Perform password sniffing using Wireshark
    - Analyze a network using the Omnipeek Network Protocol Analyzer
    - Analyze a network using the SteelCentral Packet Analyzer
3. Detect network sniffing
    - Detect ARP poisoning and promiscuous mode in a switch-based network
    - Detect ARP poisoning using the Capsa Network Analyzer

Lab 1: Perform Active Sniffing

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

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

Task 1: Perform MAC Flooding using macof

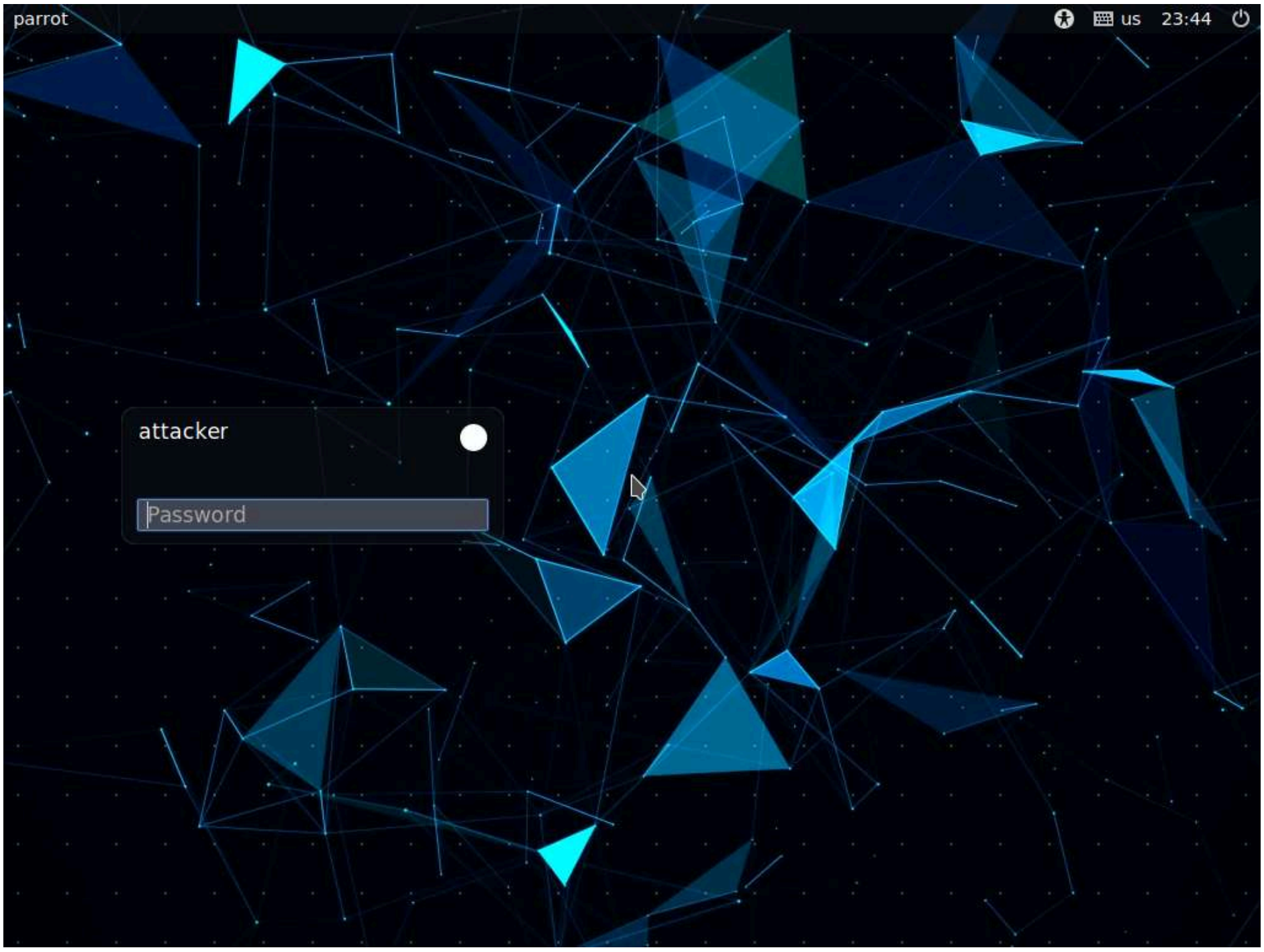
MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

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.

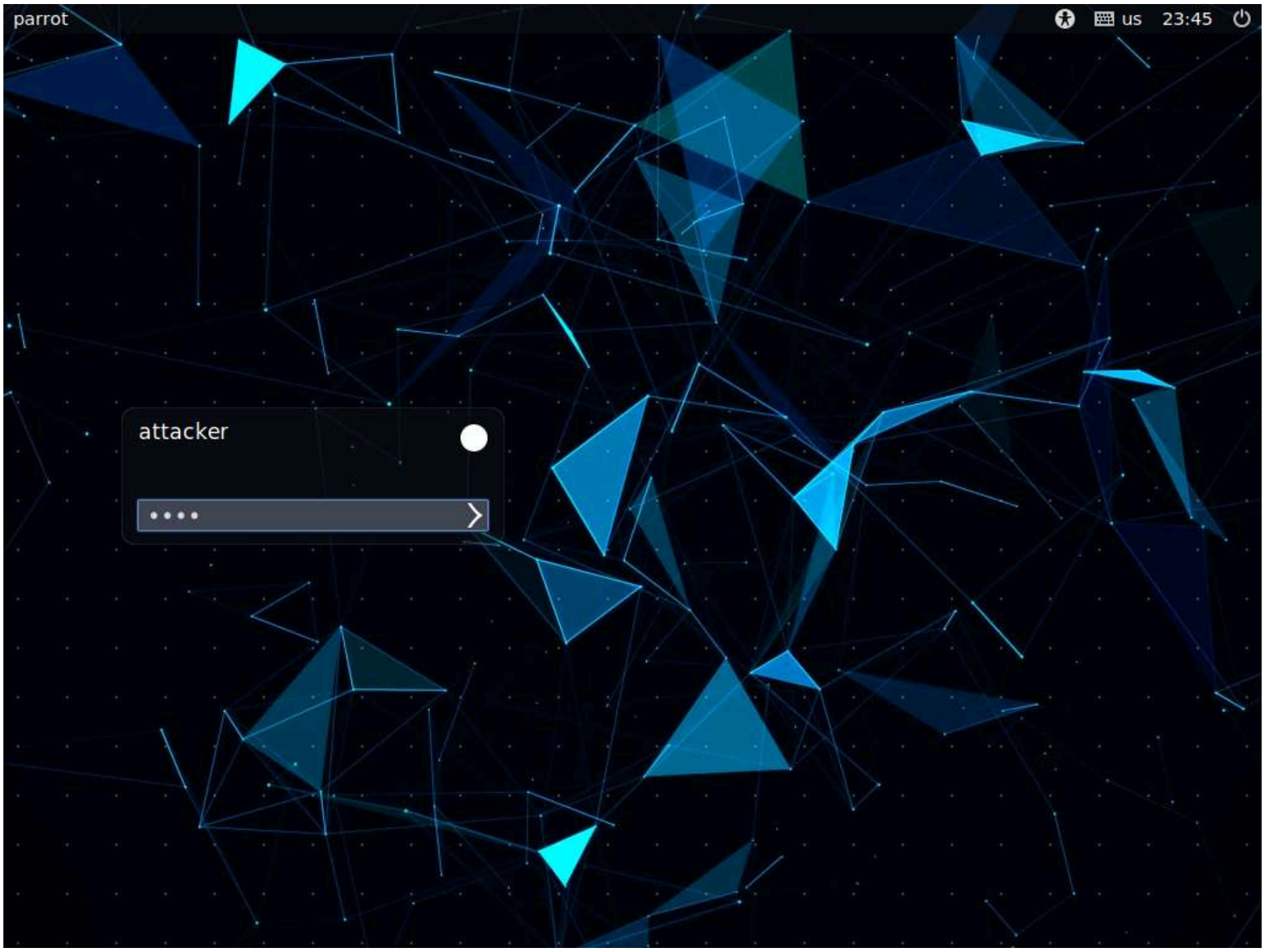
> Note: For demonstration purposes, we are using only one target machine (namely, **Windows 11**). However, you can use multiple machines connected to the same network. Macof will send the packets with random MAC addresses and IP addresses to all active machines in the local network.

1. By default **CEHv11 Parrot Security** machine is selected.

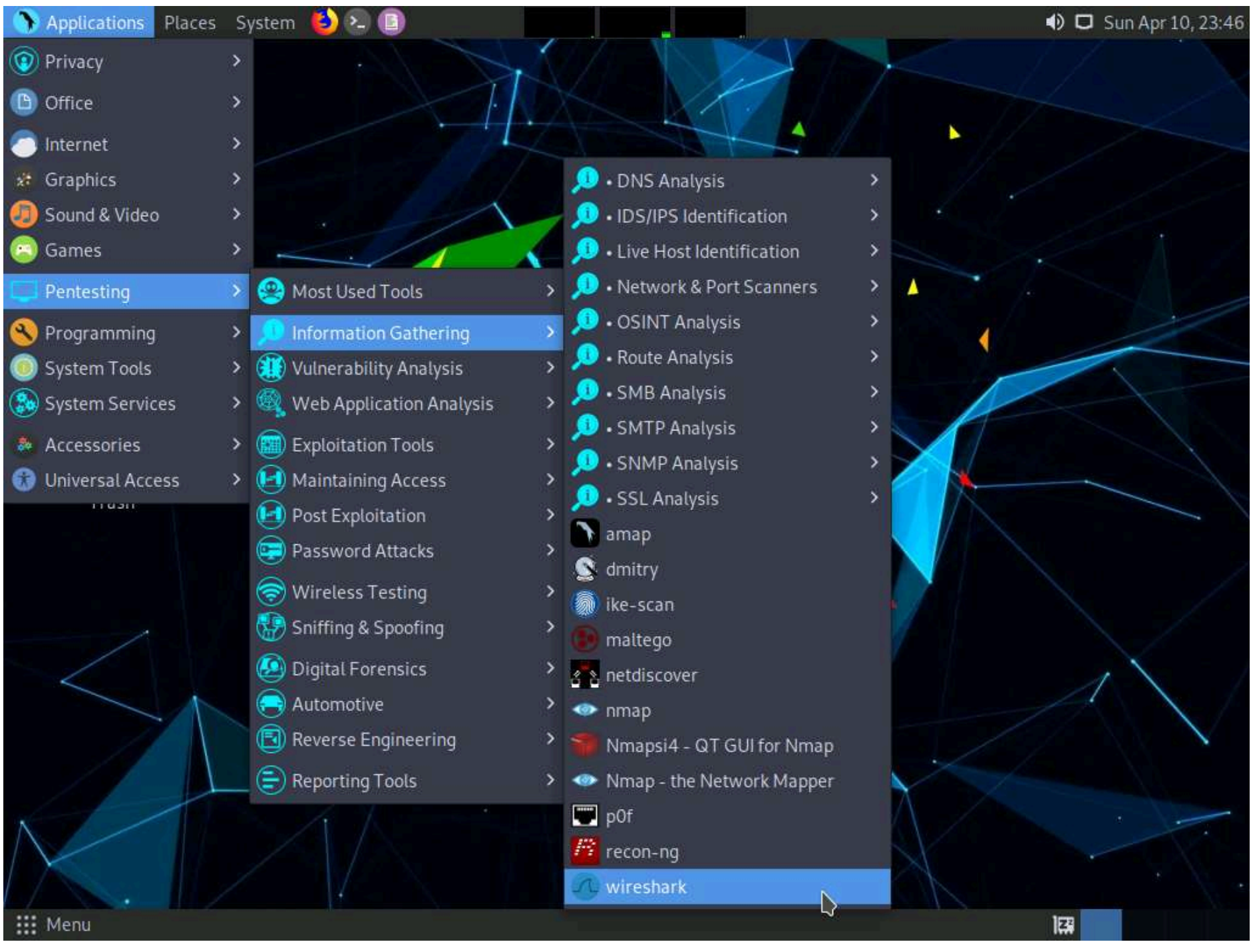


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

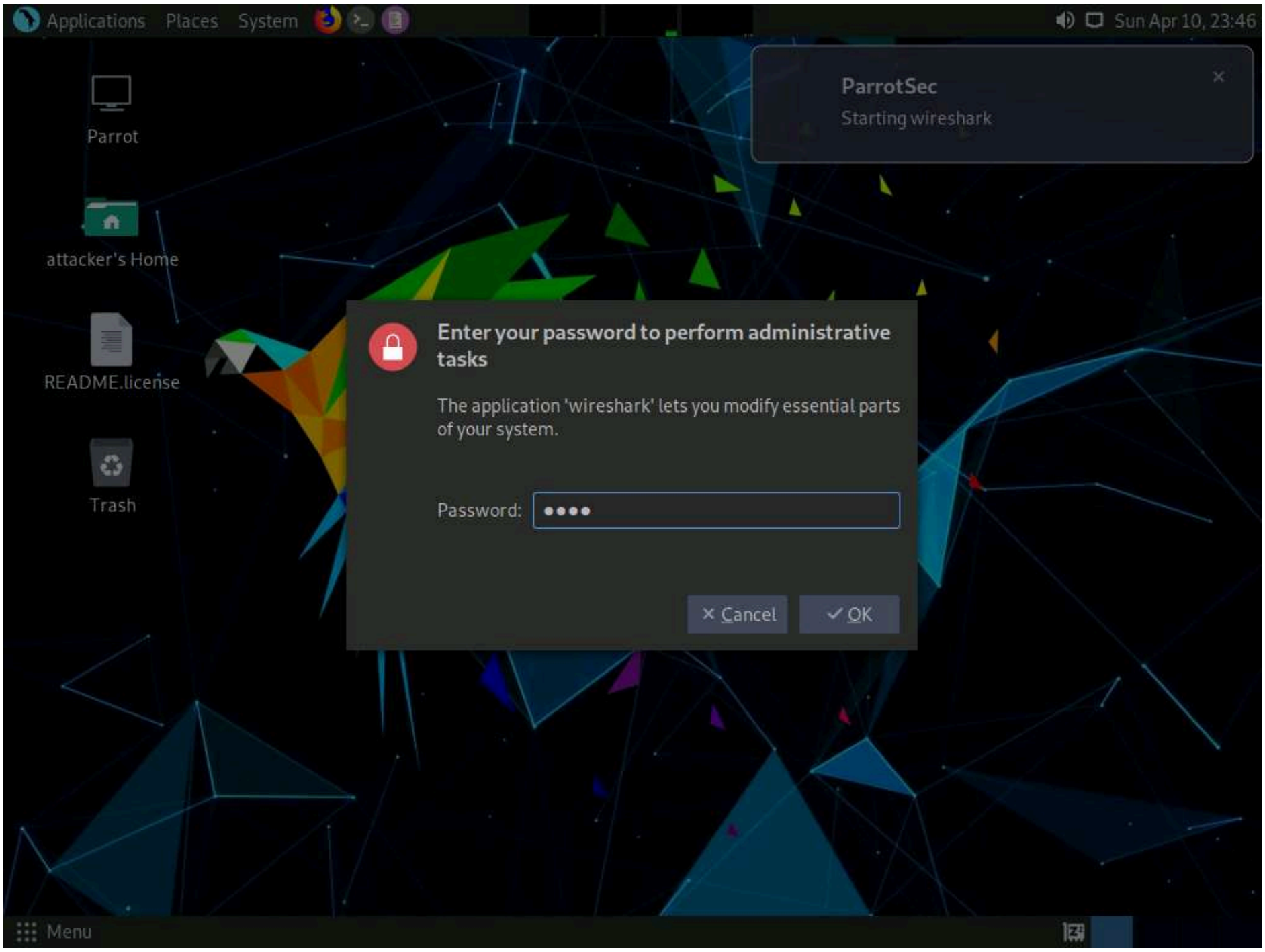
> Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
>
> Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



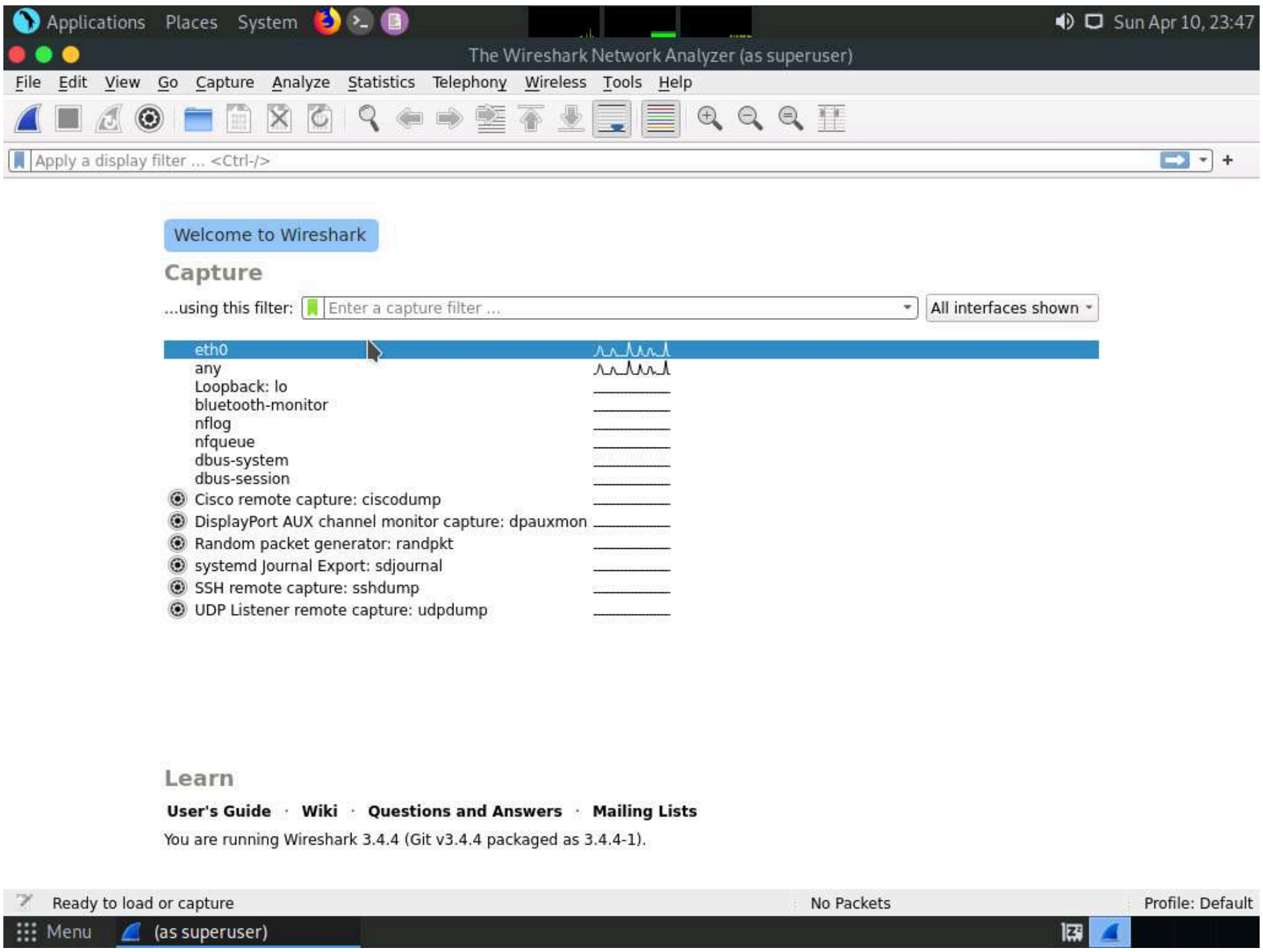
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



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

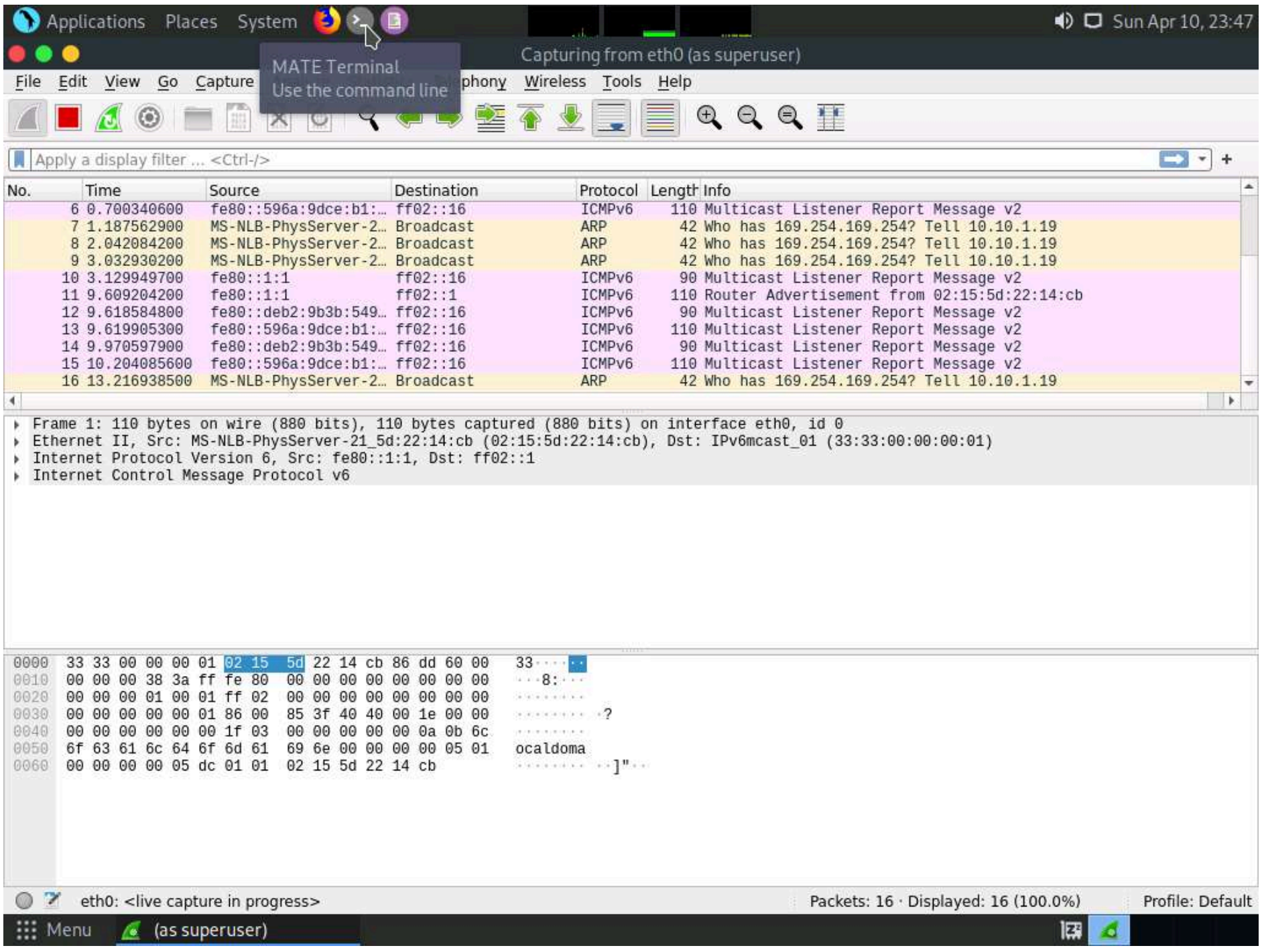


5. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



6. Leave the **Wireshark** application running.

7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

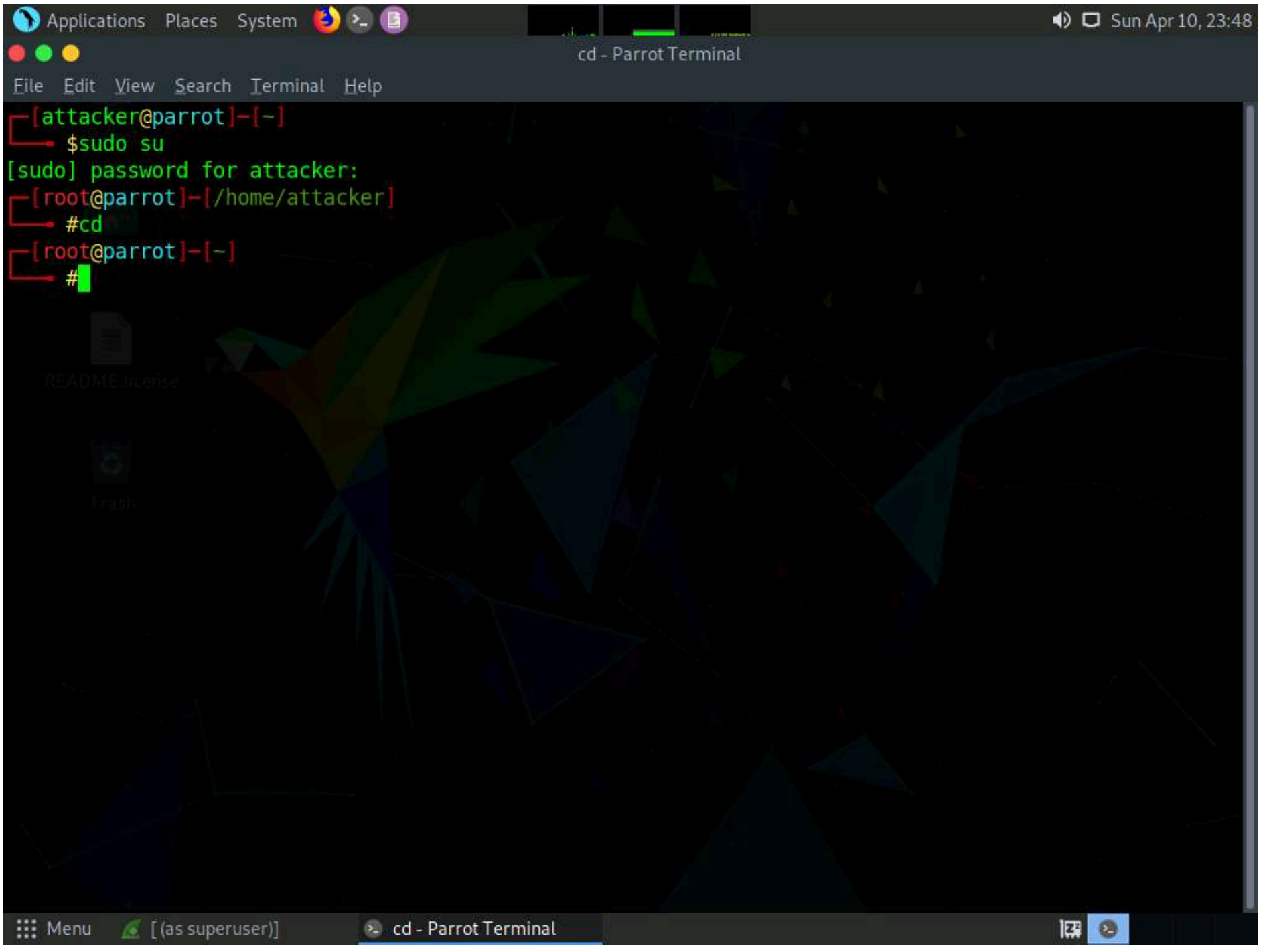


8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

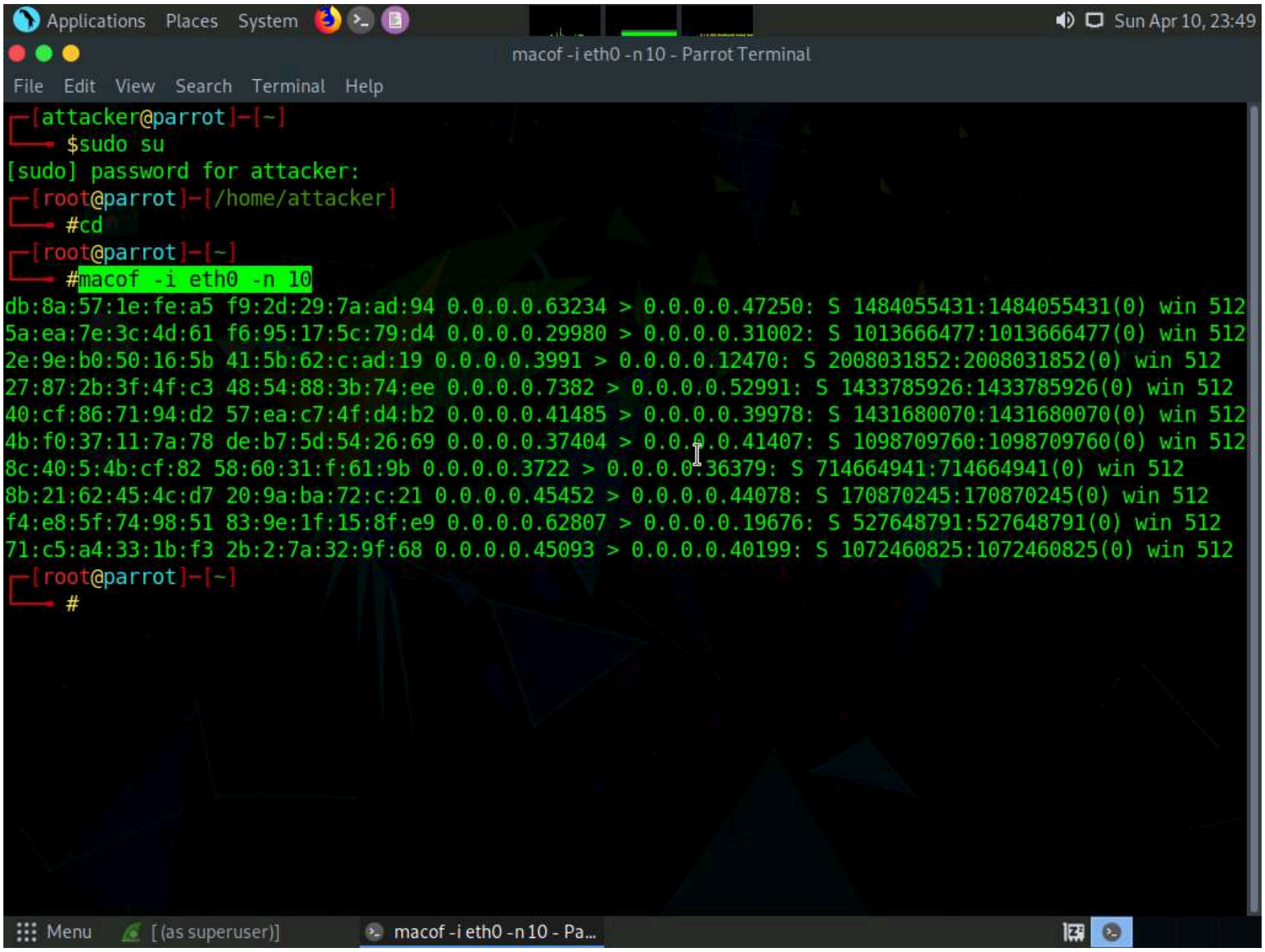
10. Now, type **cd** and press **Enter** to jump to the root directory.



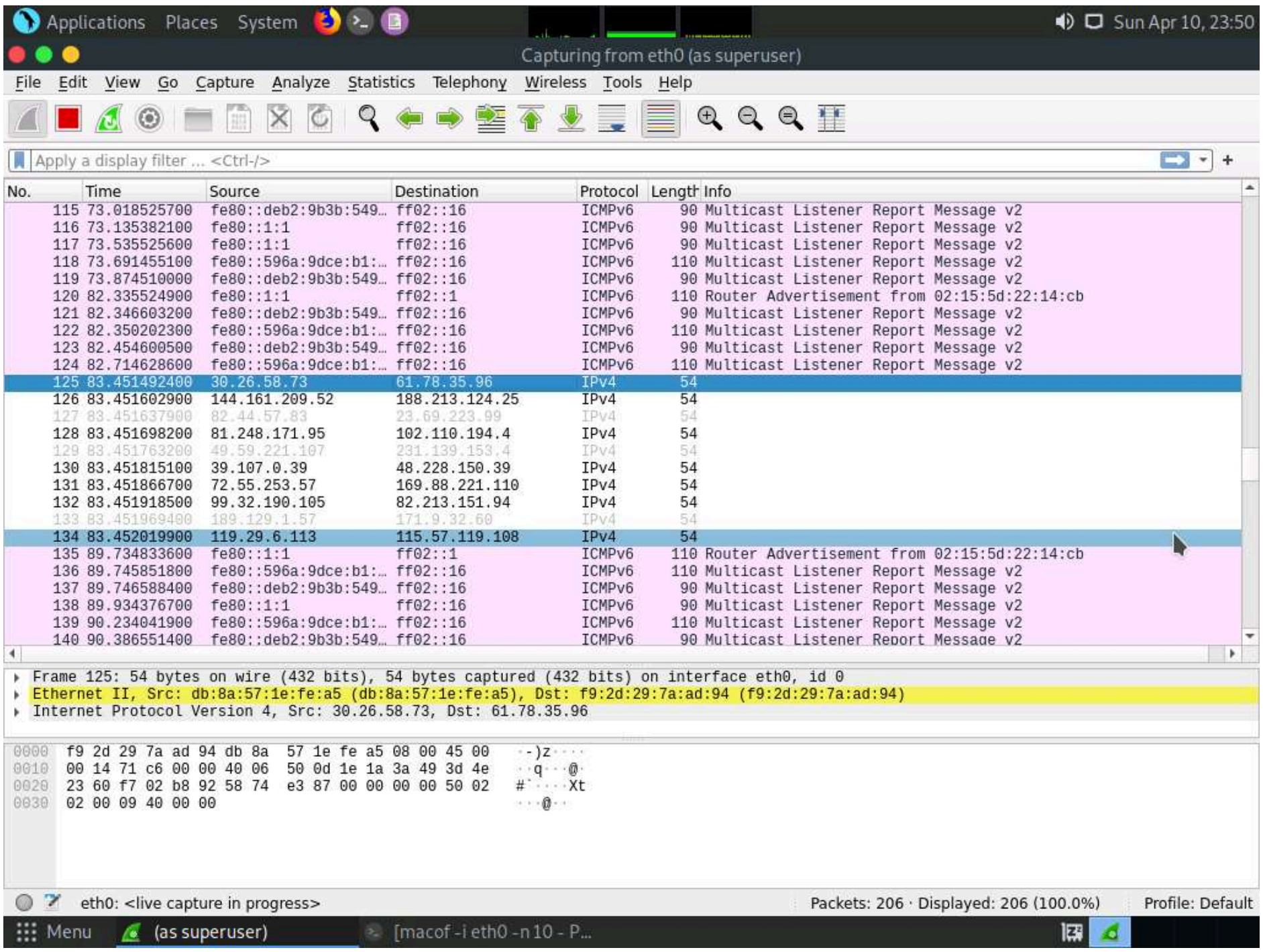
11. The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.

> Note: **-i**: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).
>
> Note: You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d**: Specifies the destination IP address).

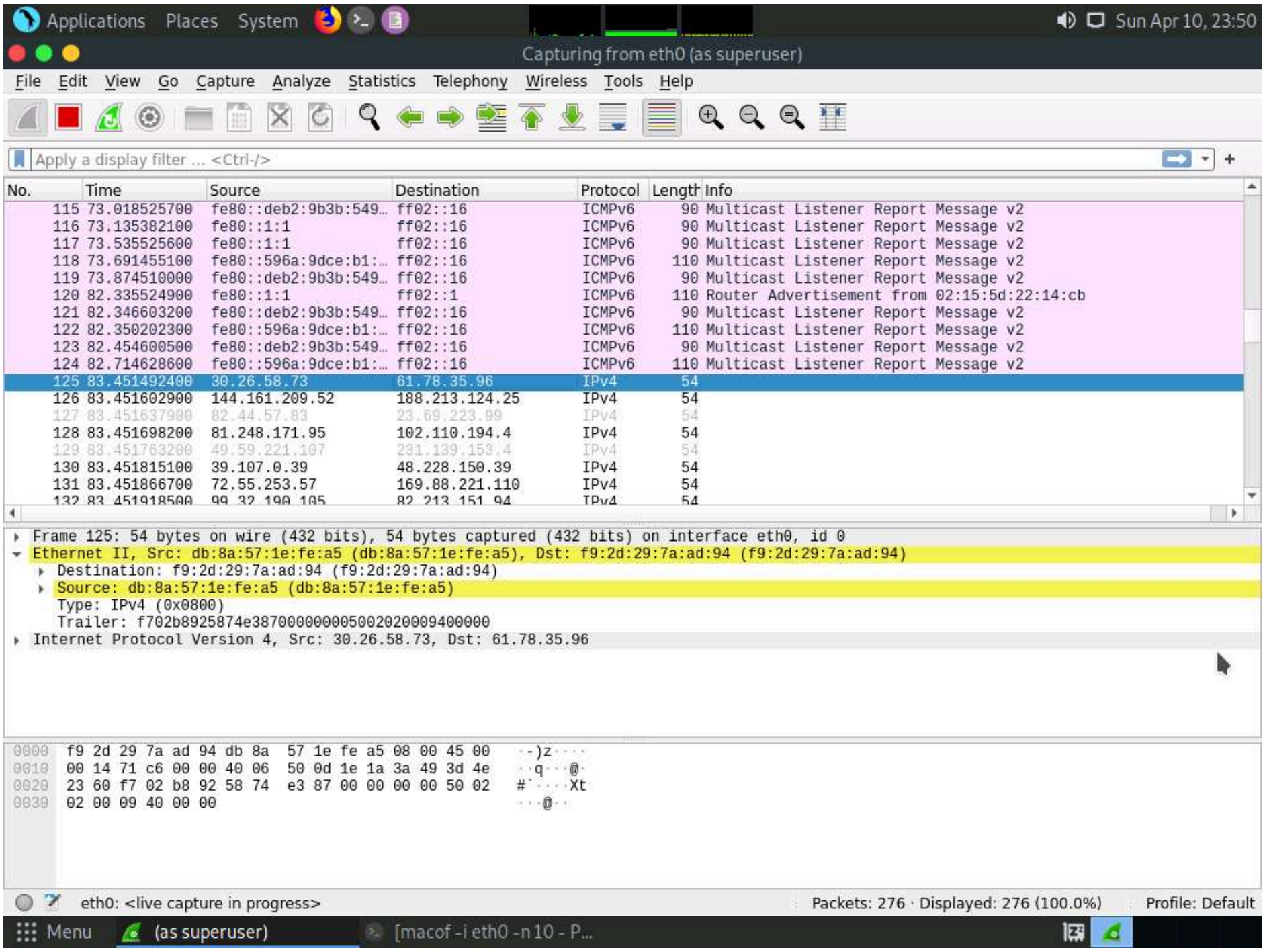
12. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.



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



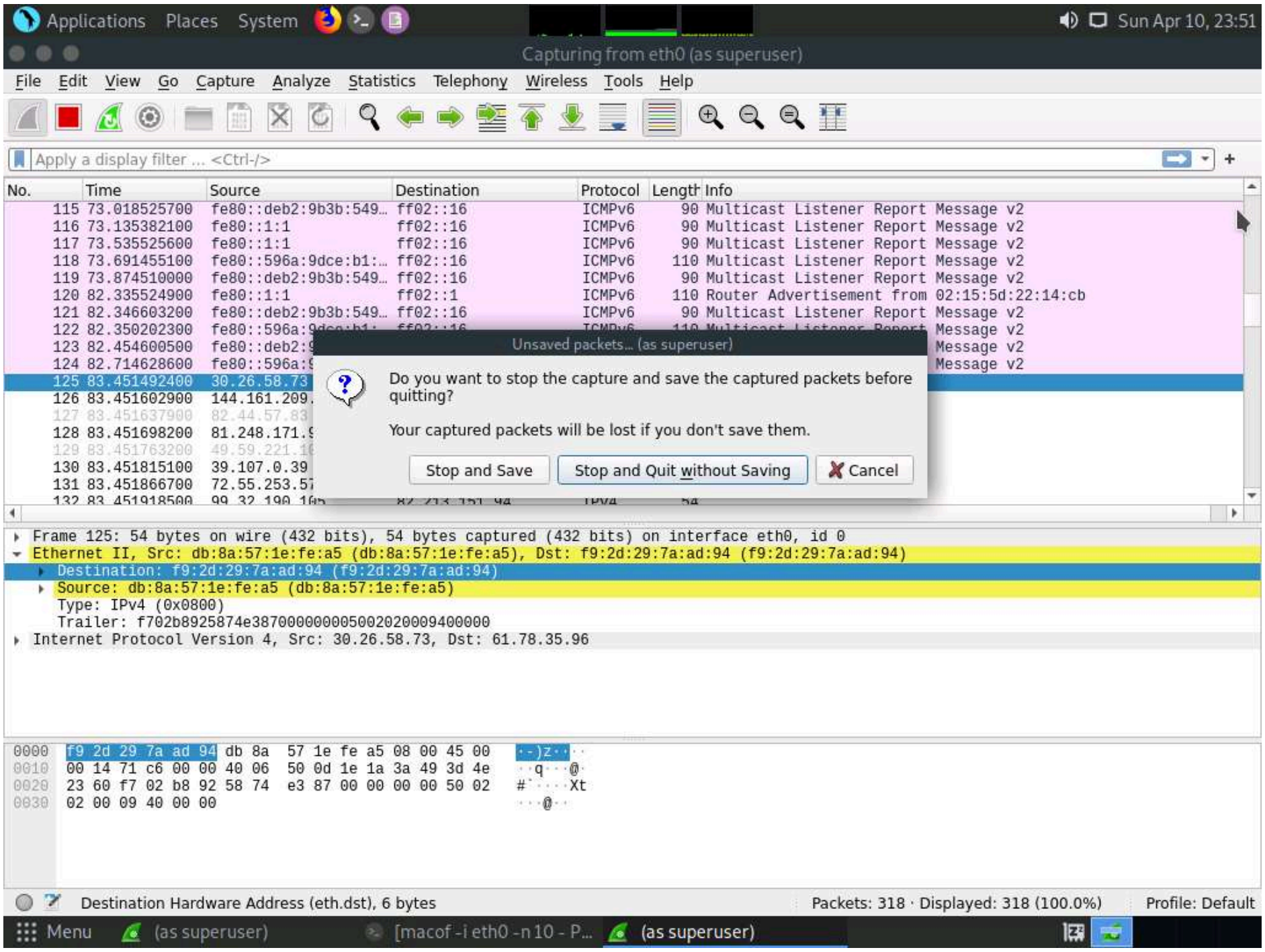
14. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



15. Similarly, you can switch to a different machine to see the same packets that were captured by Wireshark in the **Parrot Security** machine.

16. Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.

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



18. This concludes the demonstration of how to perform MAC flooding using macof.

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

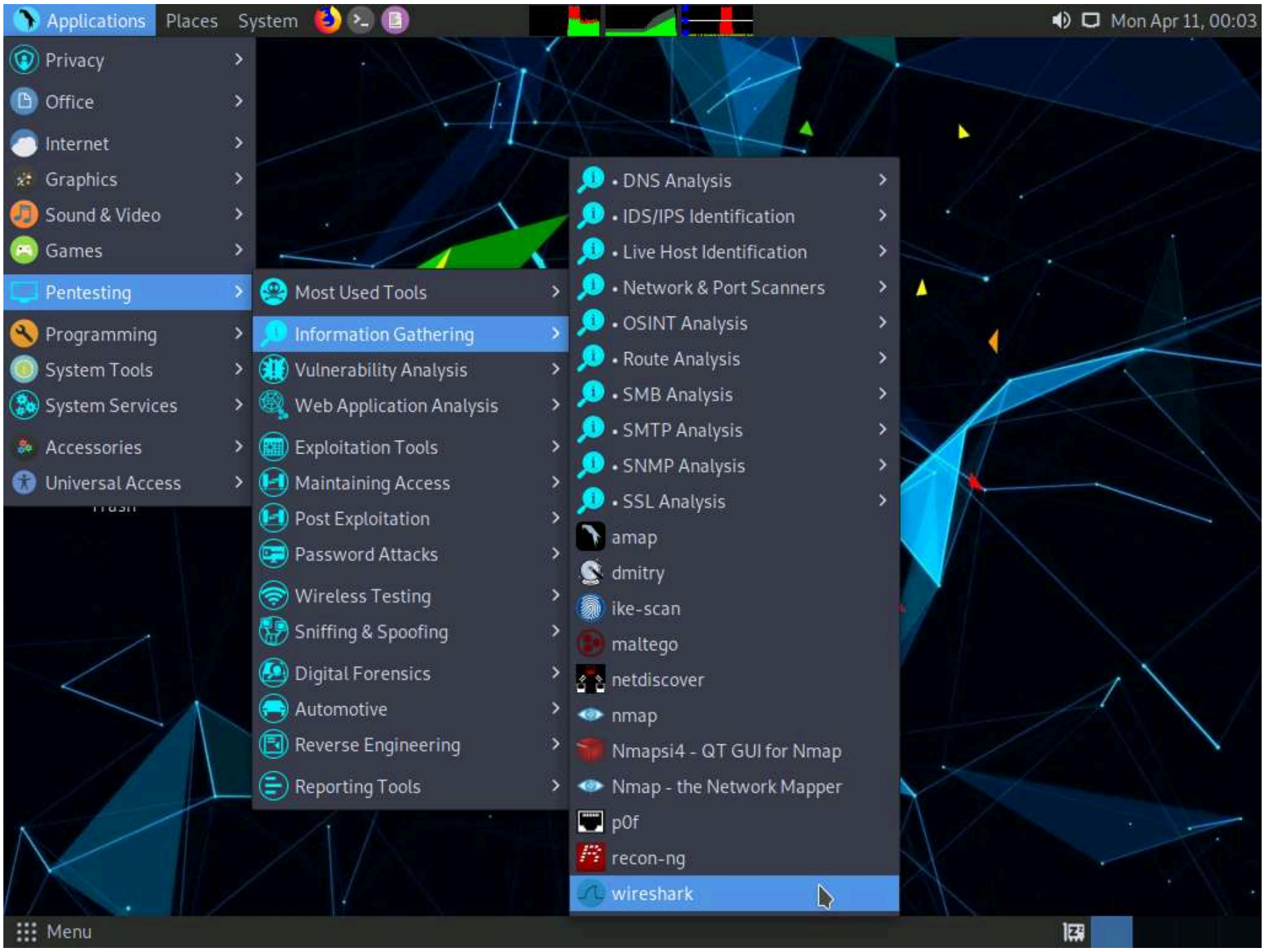
Task 2: Perform a DHCP Starvation Attack using Yersinia

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

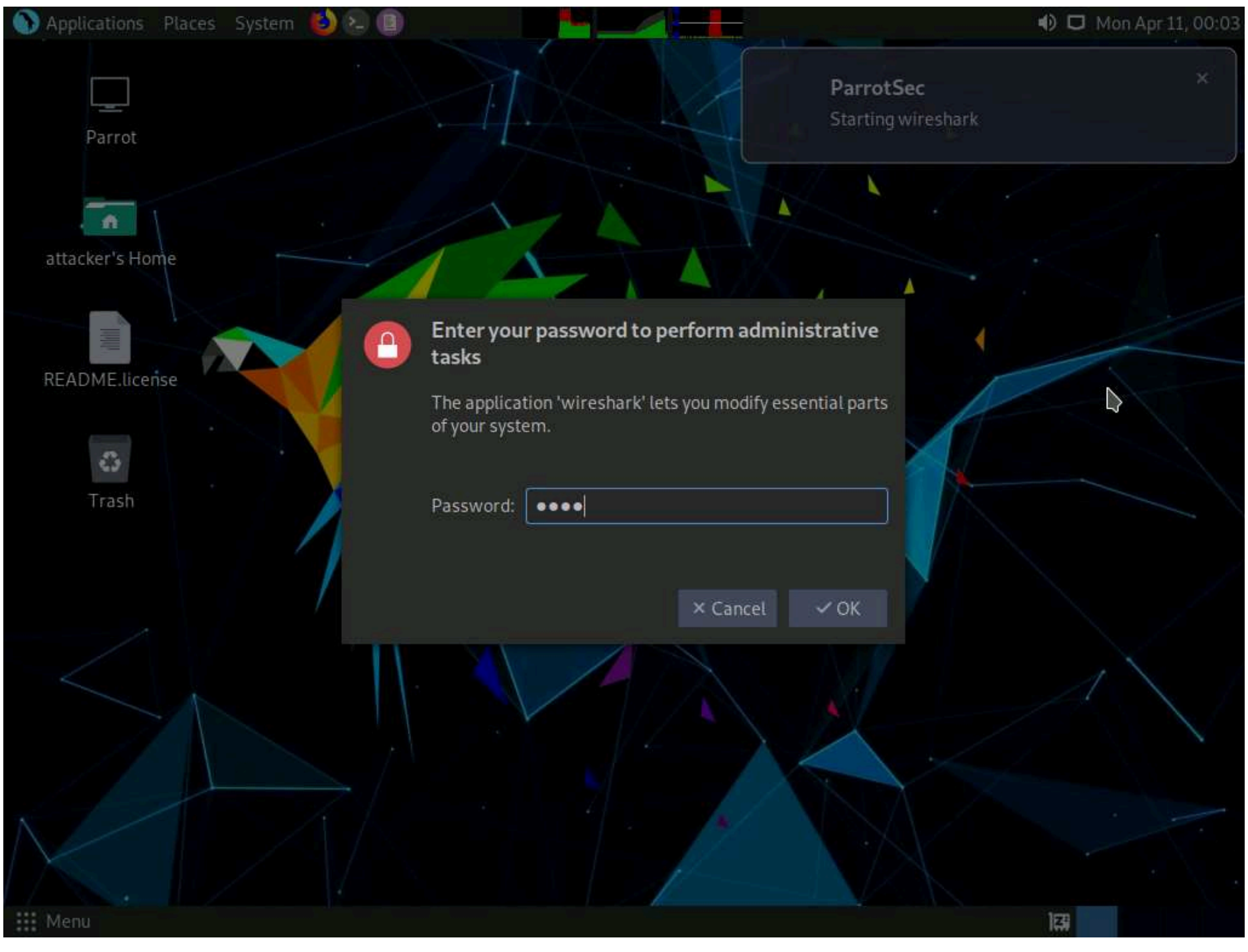
Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

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

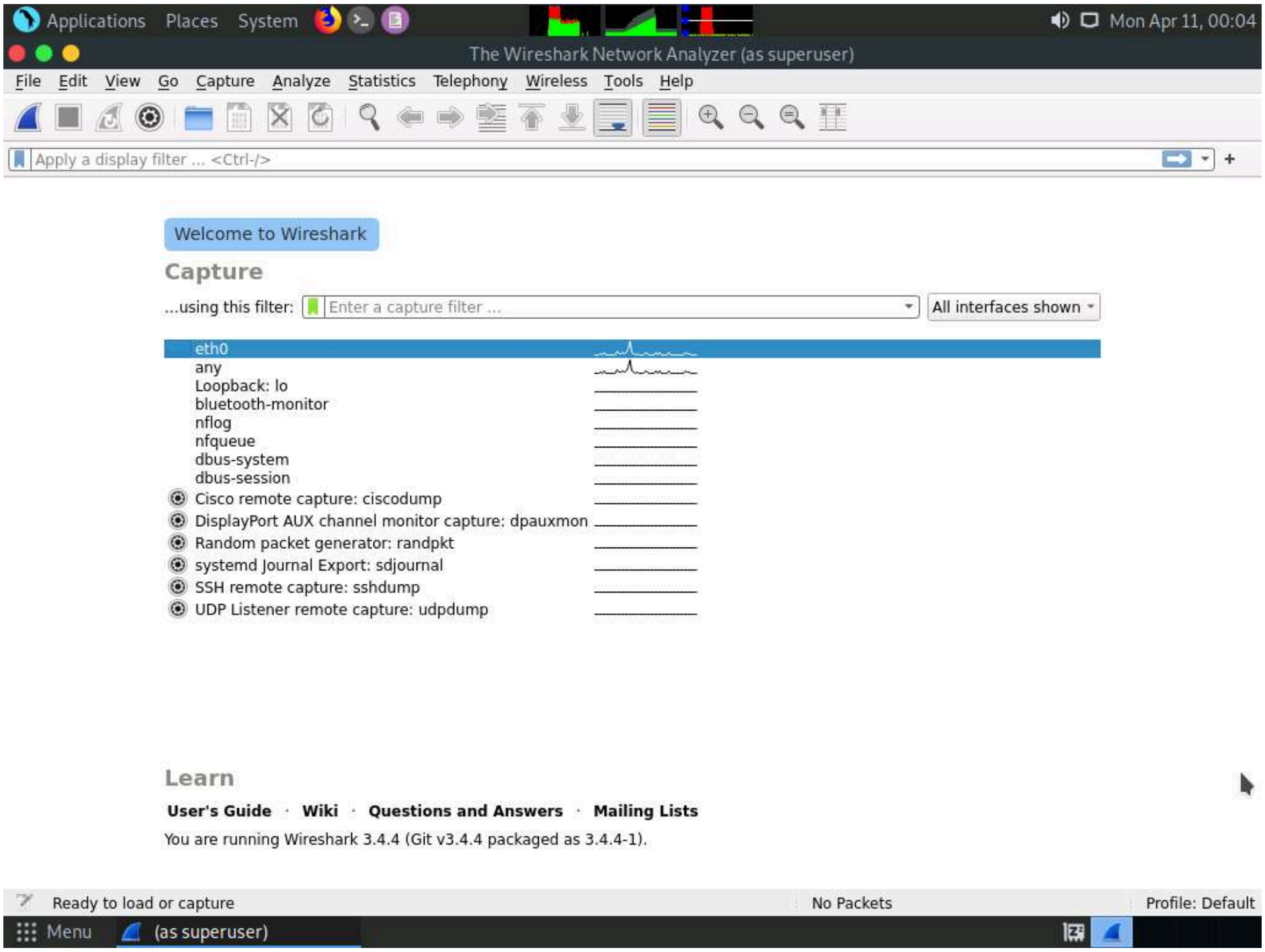
1. On the **Parrot Security** machine; click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



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

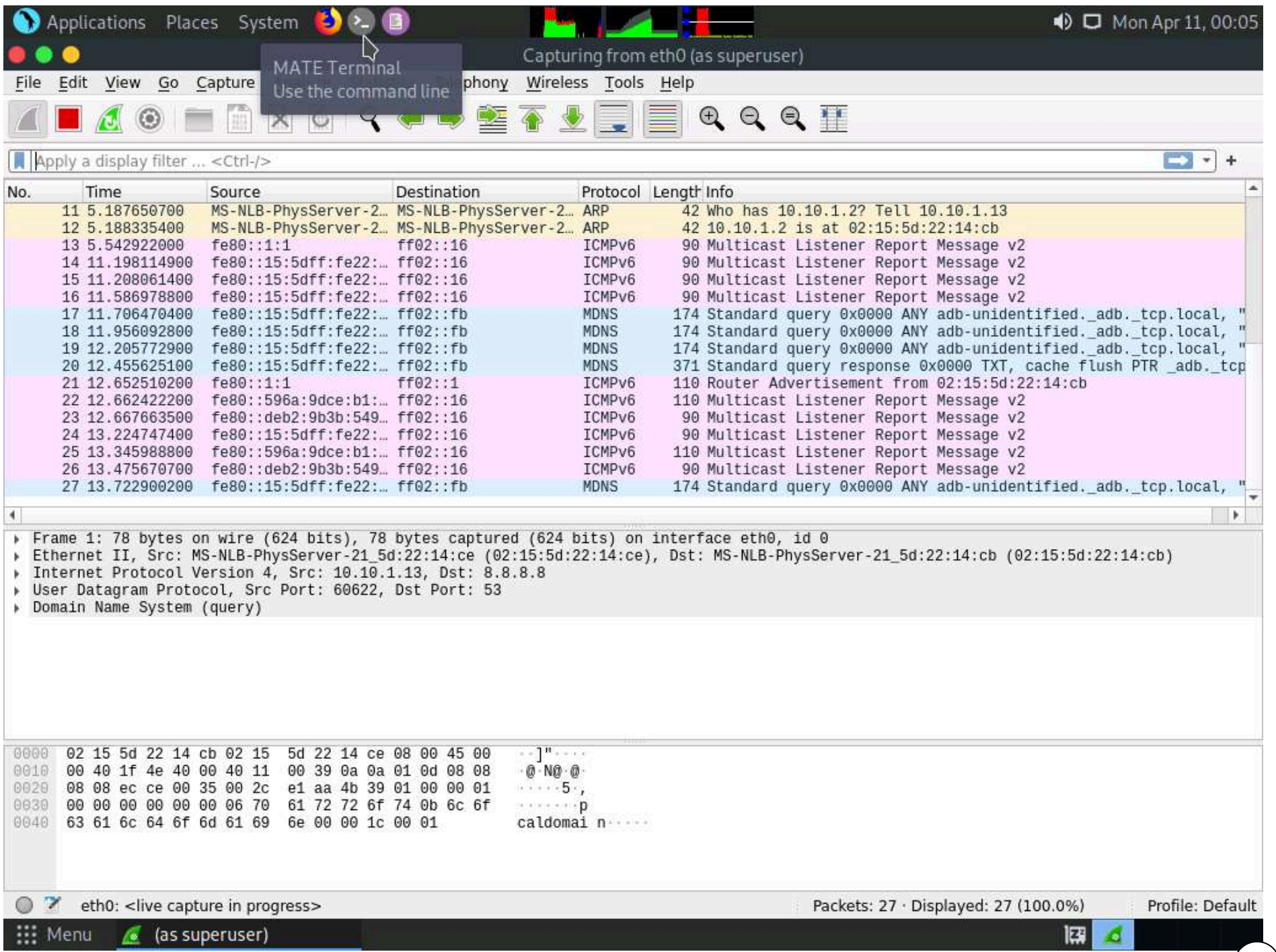


3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



4. Leave the **Wireshark** application running.

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



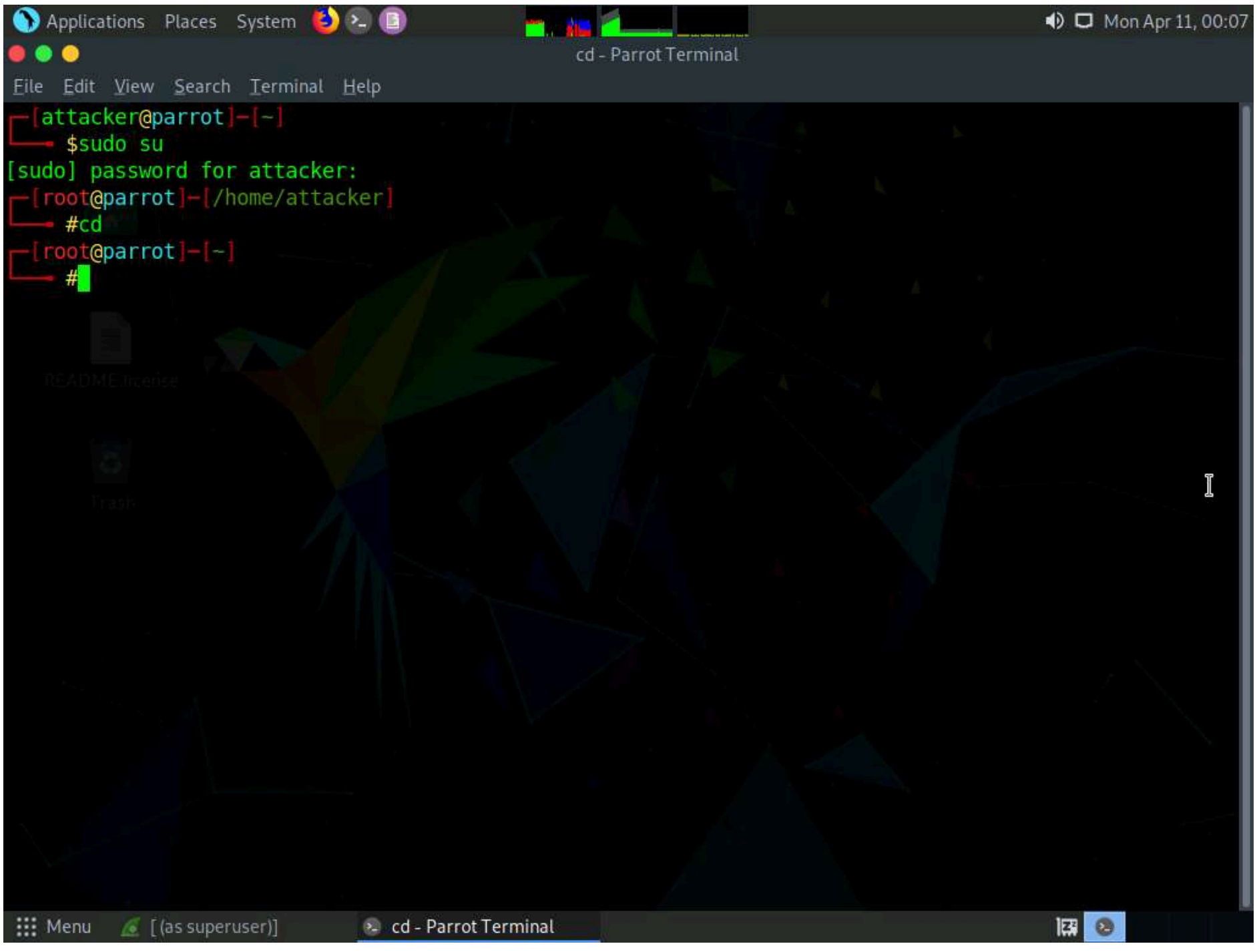
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

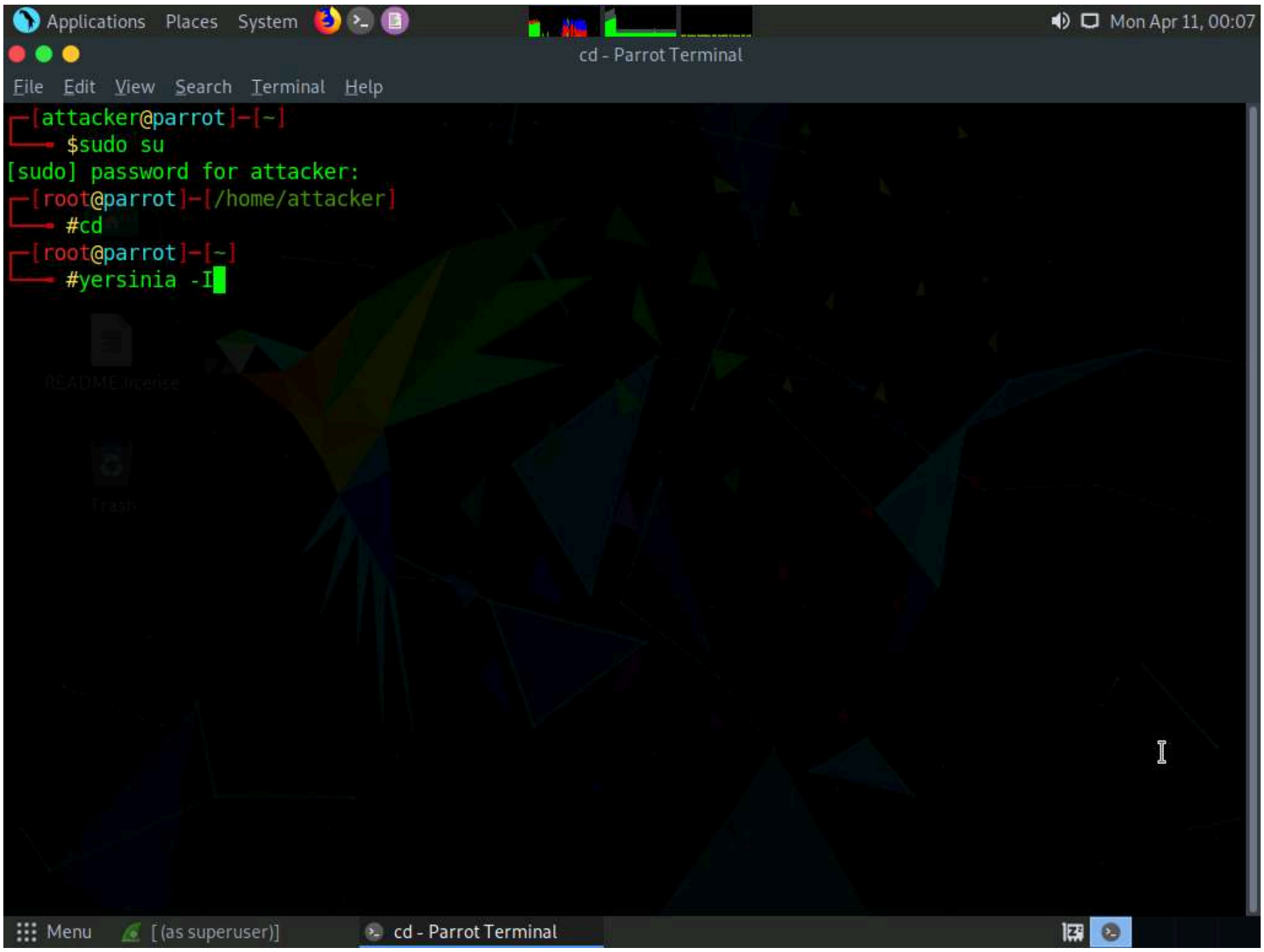
8. Now, type **cd** and press **Enter** to jump to the root directory.

> Note: Click the **Maximize Window** icon to maximize the terminal window.
>
> Note: The interactive mode of the Yersinia application only works in a maximized terminal window.

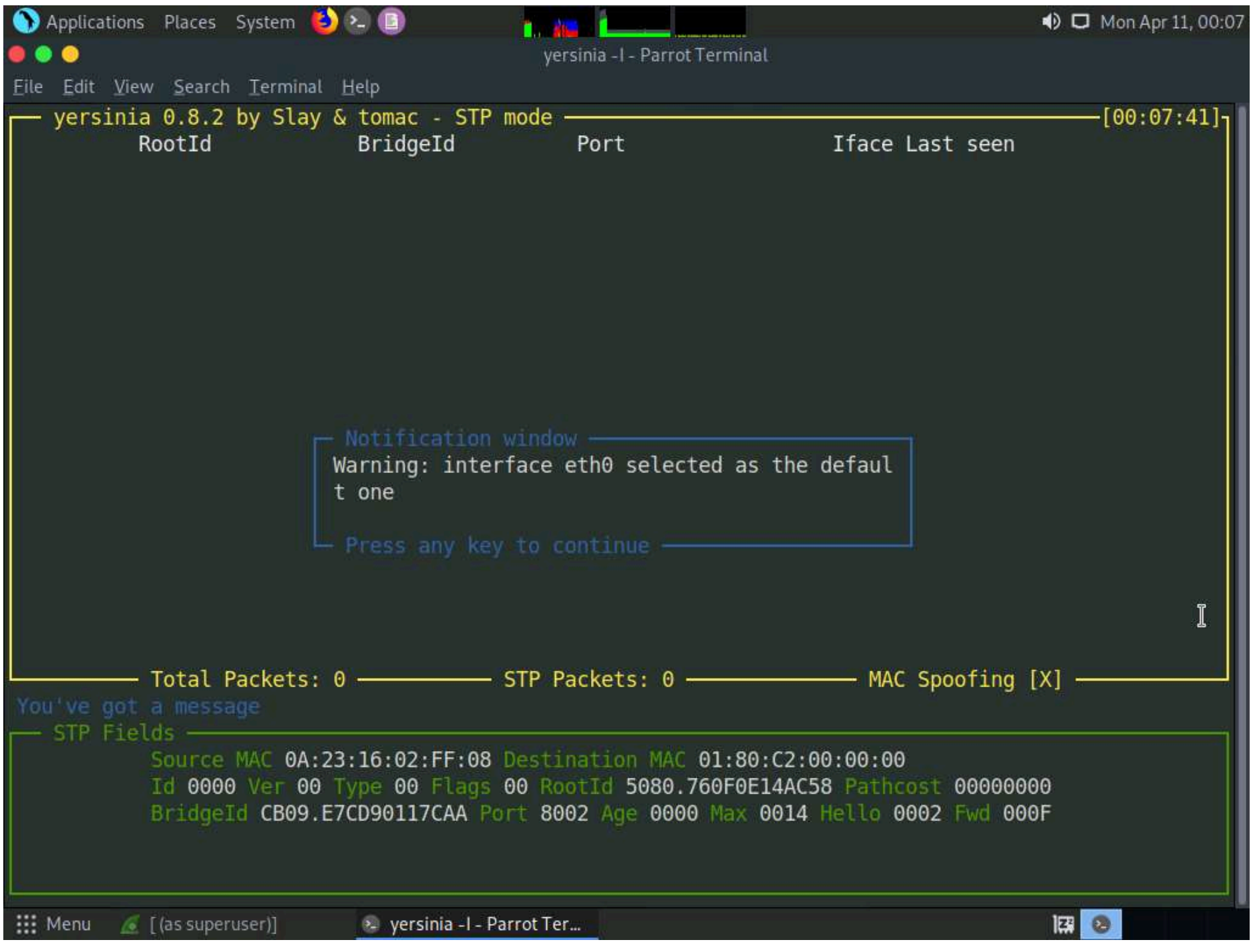


9. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.

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

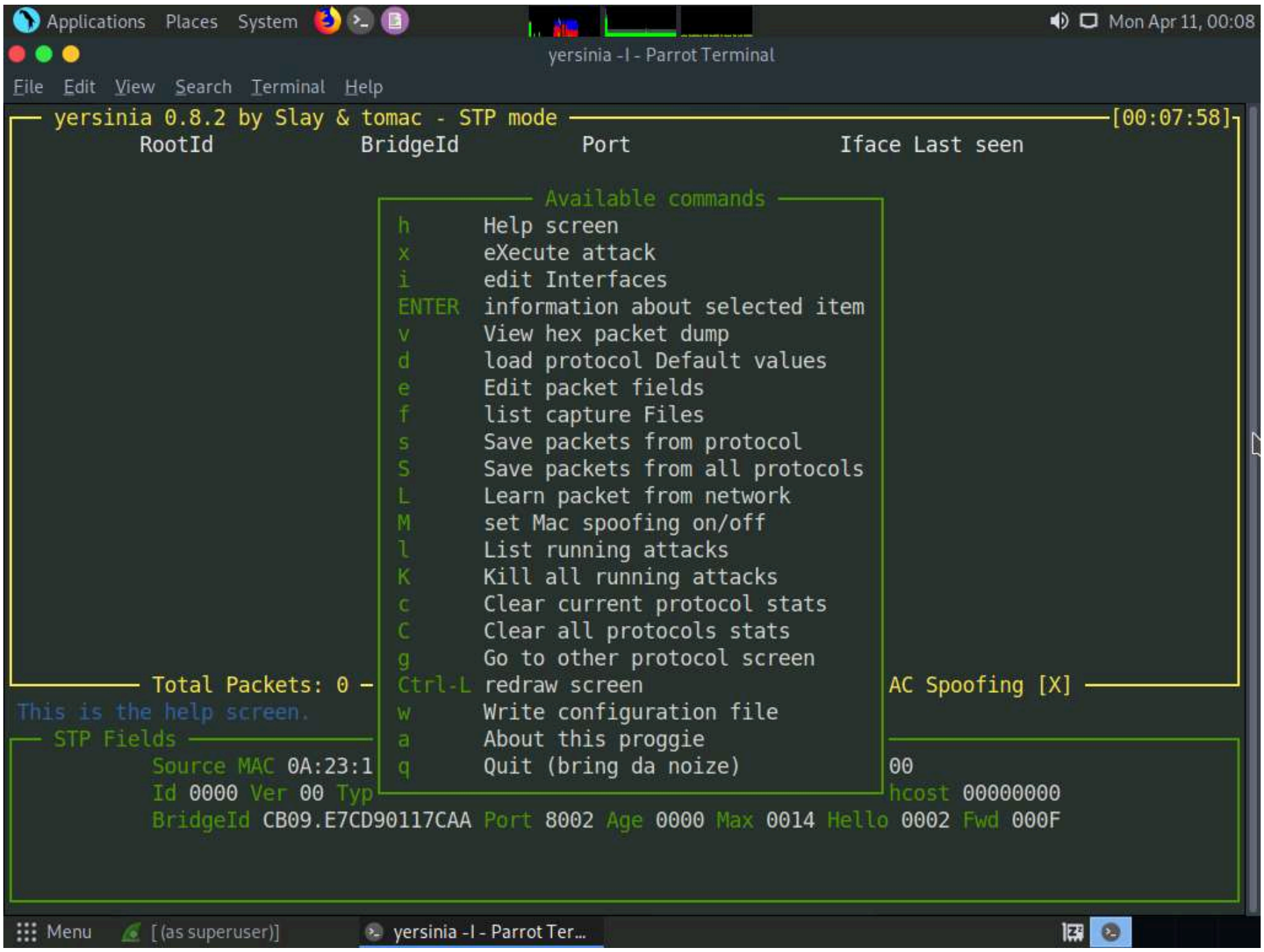


10. Yersinia interactive mode appears in the terminal window.



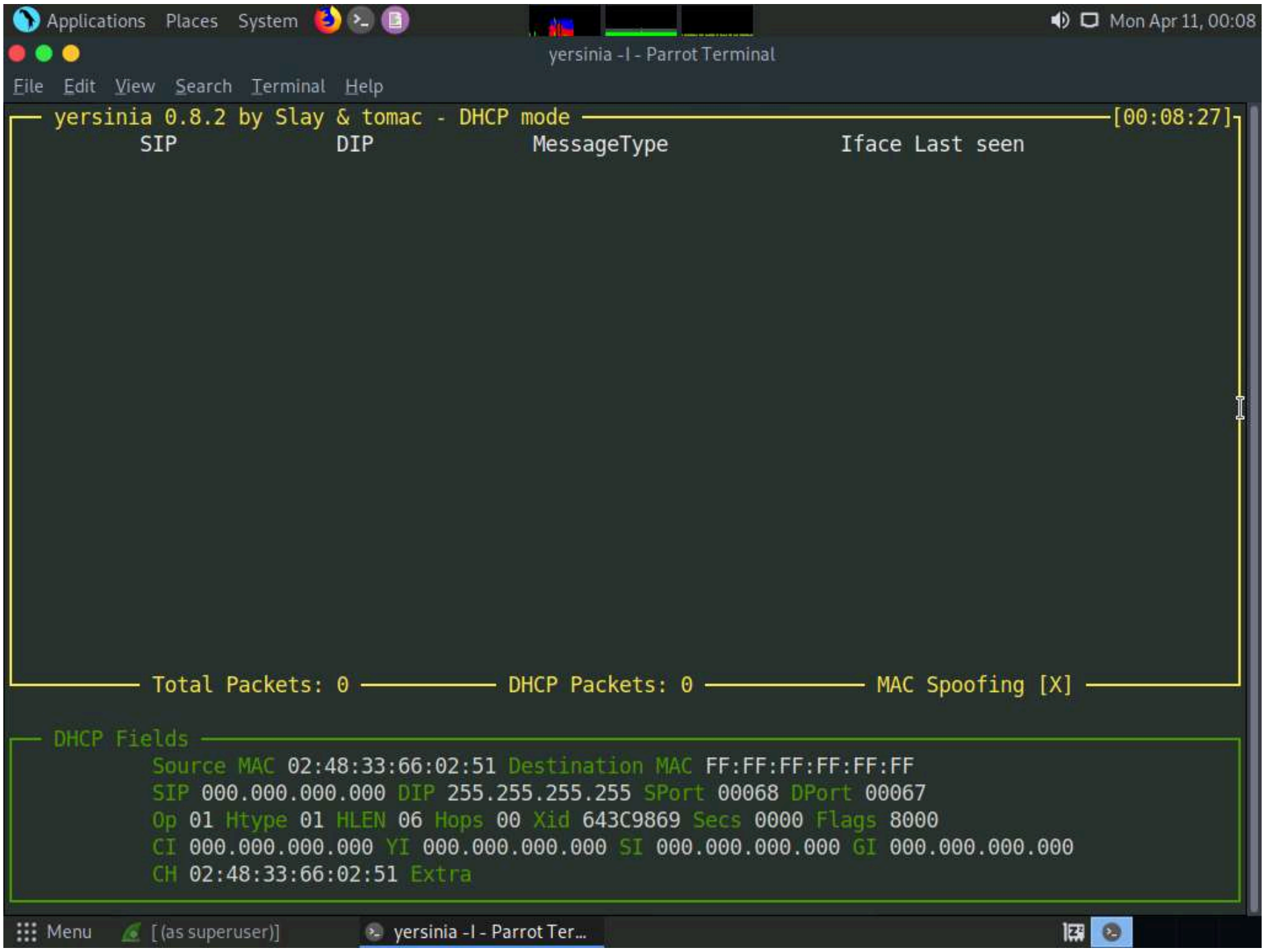
11. To remove the **Notification window**, press any key, and then press **h** for help.

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



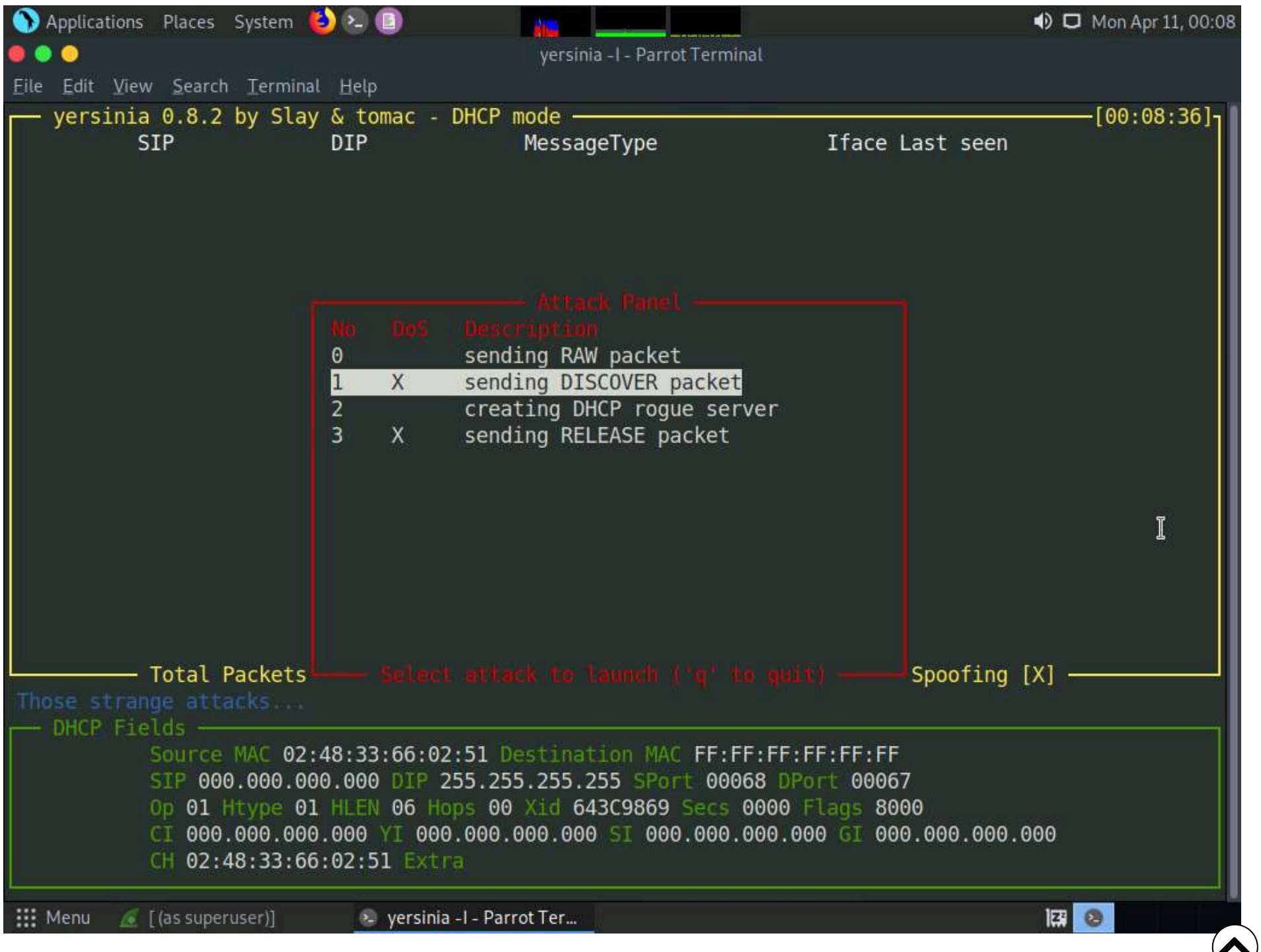
13. Press **q** to exit the help options.

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



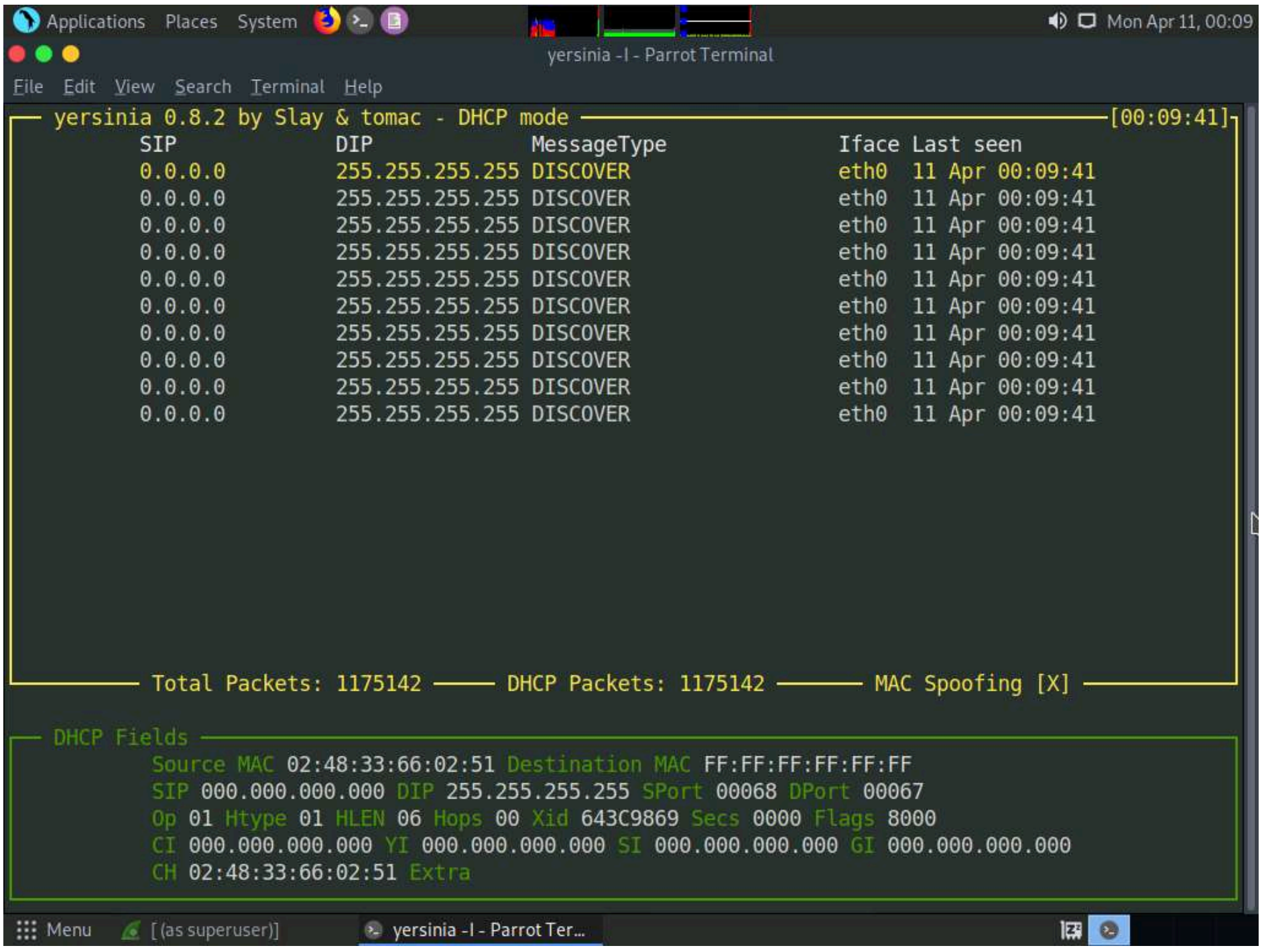
15. Press **x** to list available attack options.

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

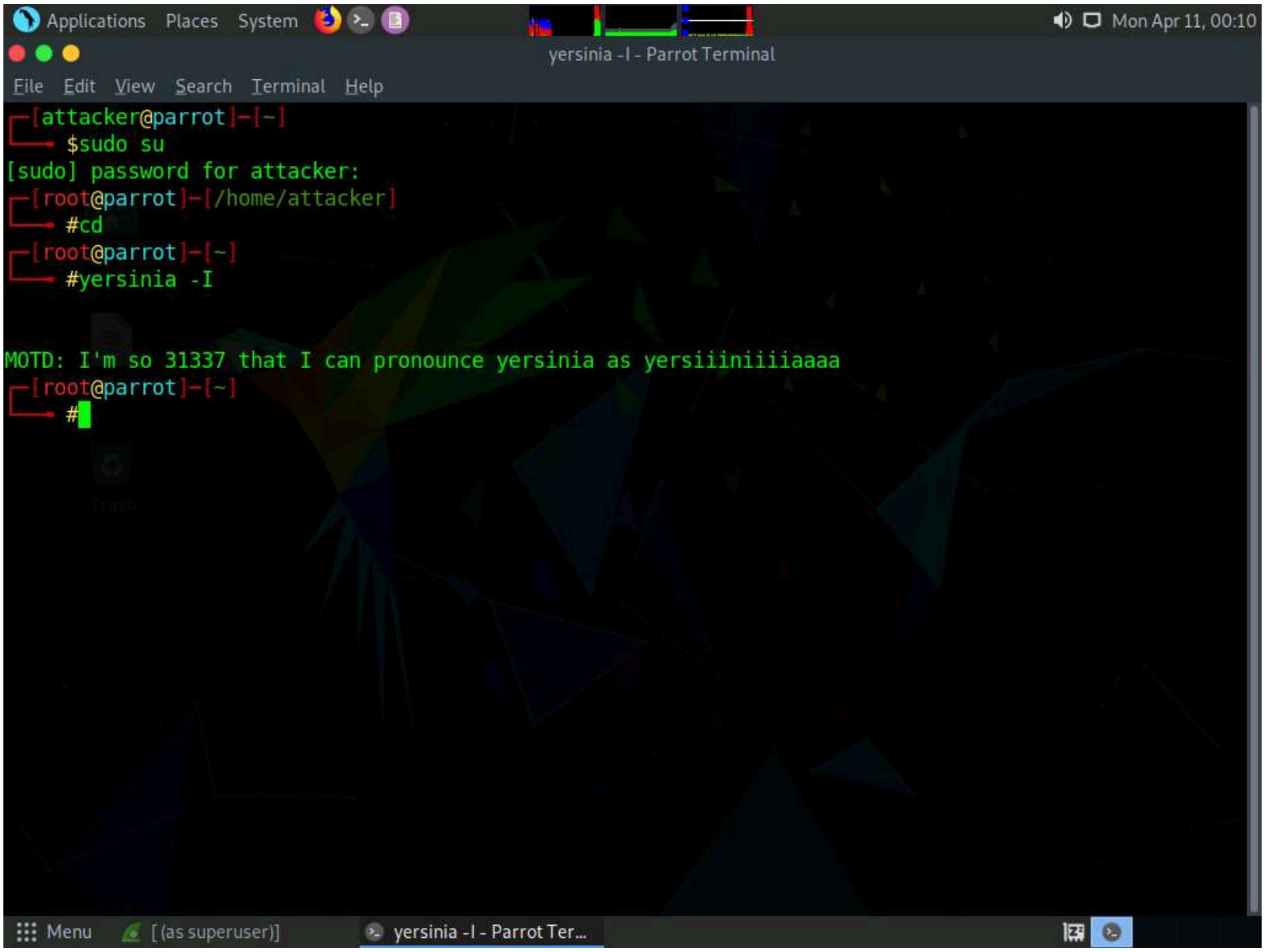


17. **Yersinia** starts sending DHCP packets to the network adapter and all active machines in the local network, as shown in the screenshot.

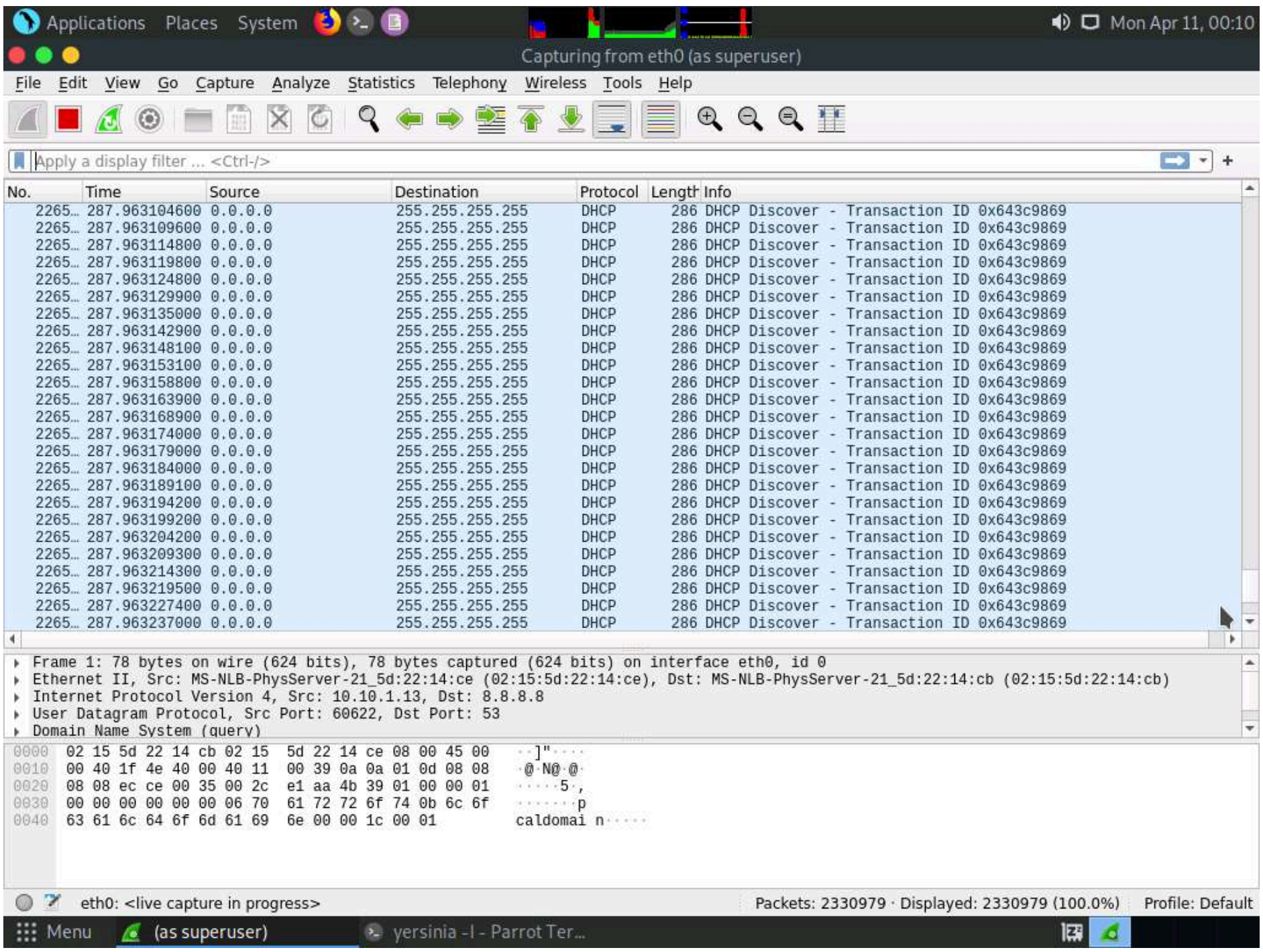
Note: If you are using multiple targets, you will observe the same packets on all target machines.



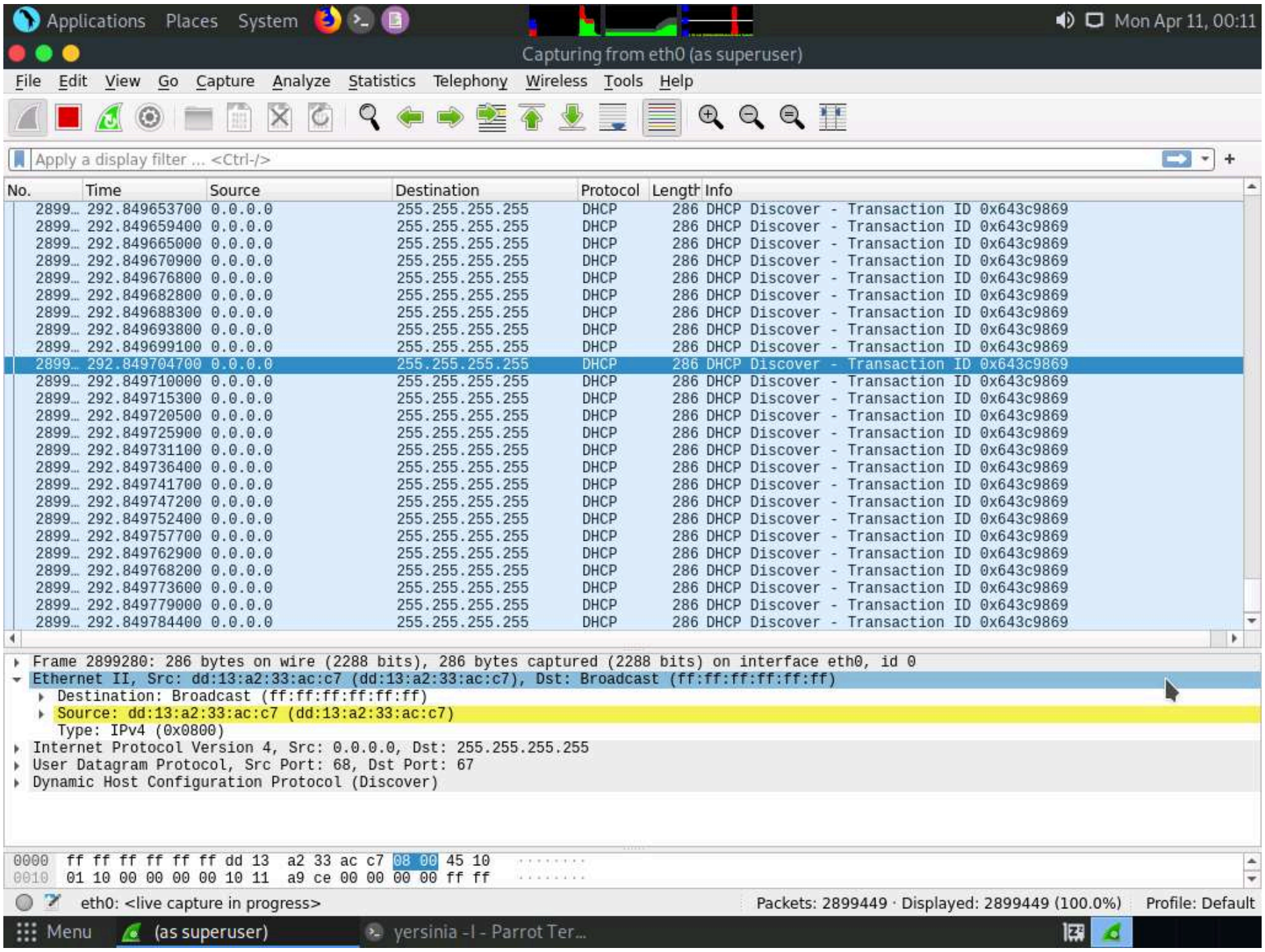
18. After a few seconds, press **q** to stop the attack and terminate Yersinia, as shown in the screenshot.



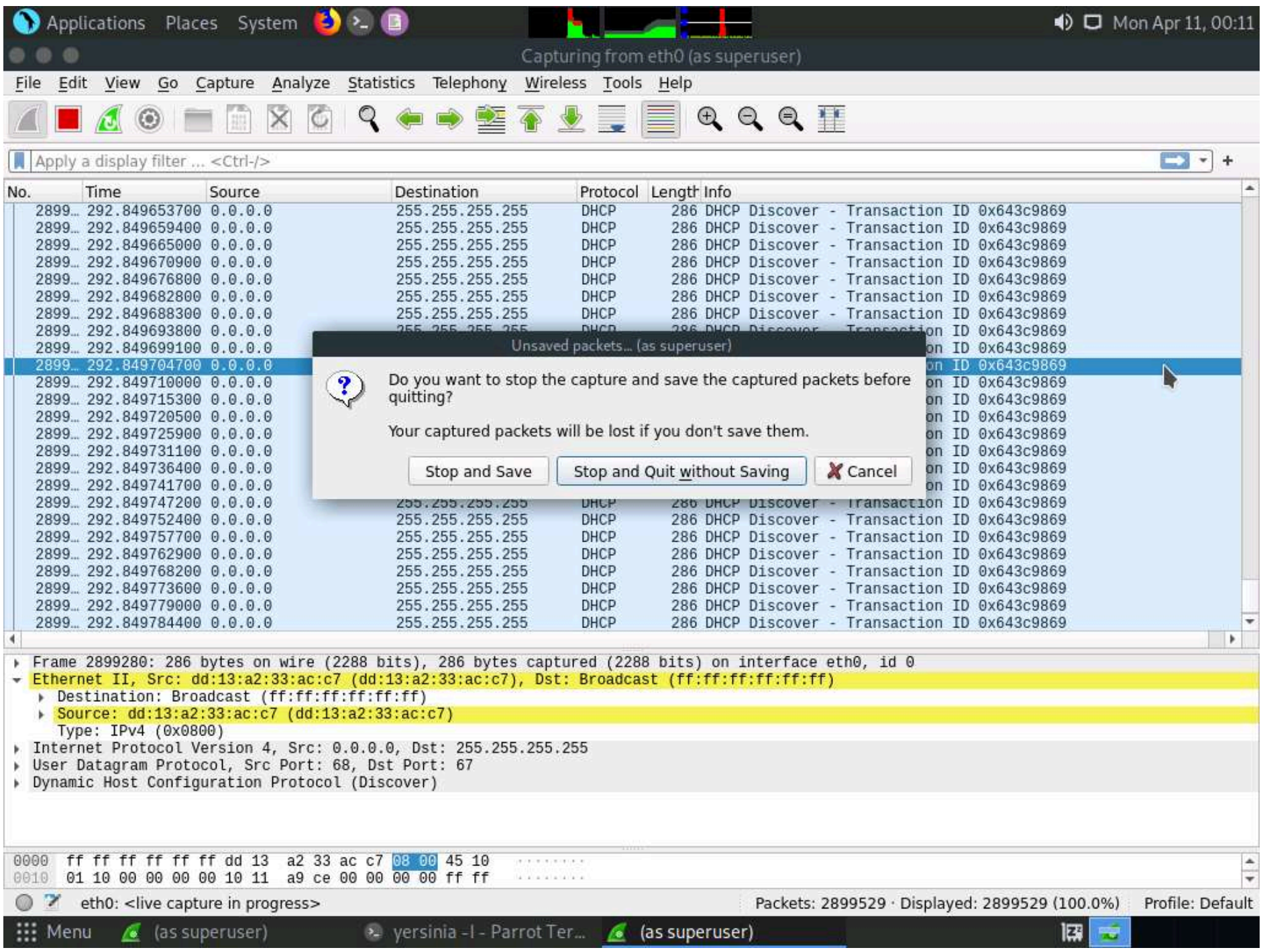
19. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.



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



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



22. This concludes the demonstration of how to perform a DHCP starvation attack using Yersinia.

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

Task 3: Perform ARP Poisoning using arpspoof

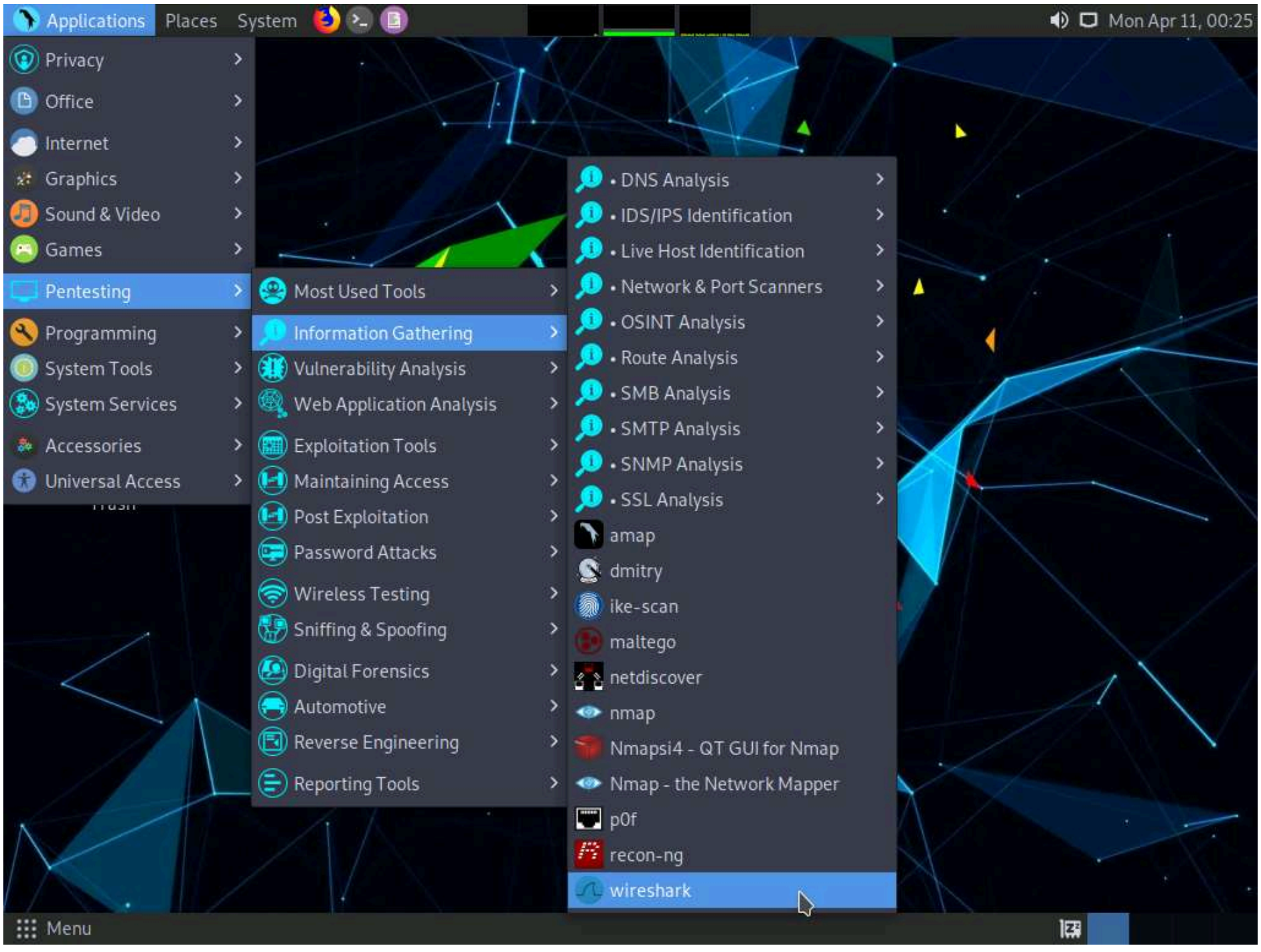
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the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

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

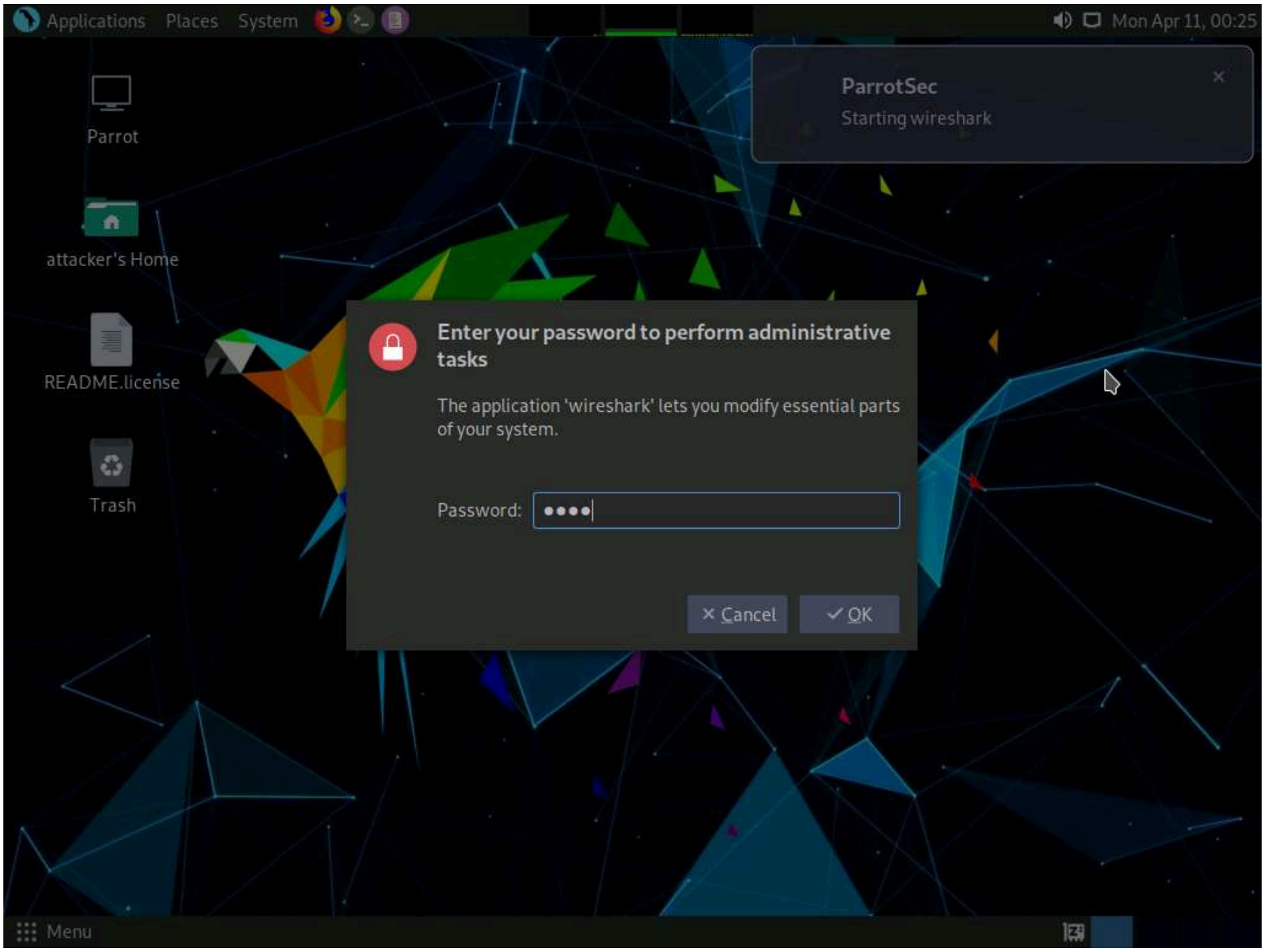
Here, we will use the arpspoof tool to perform ARP poisoning.

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

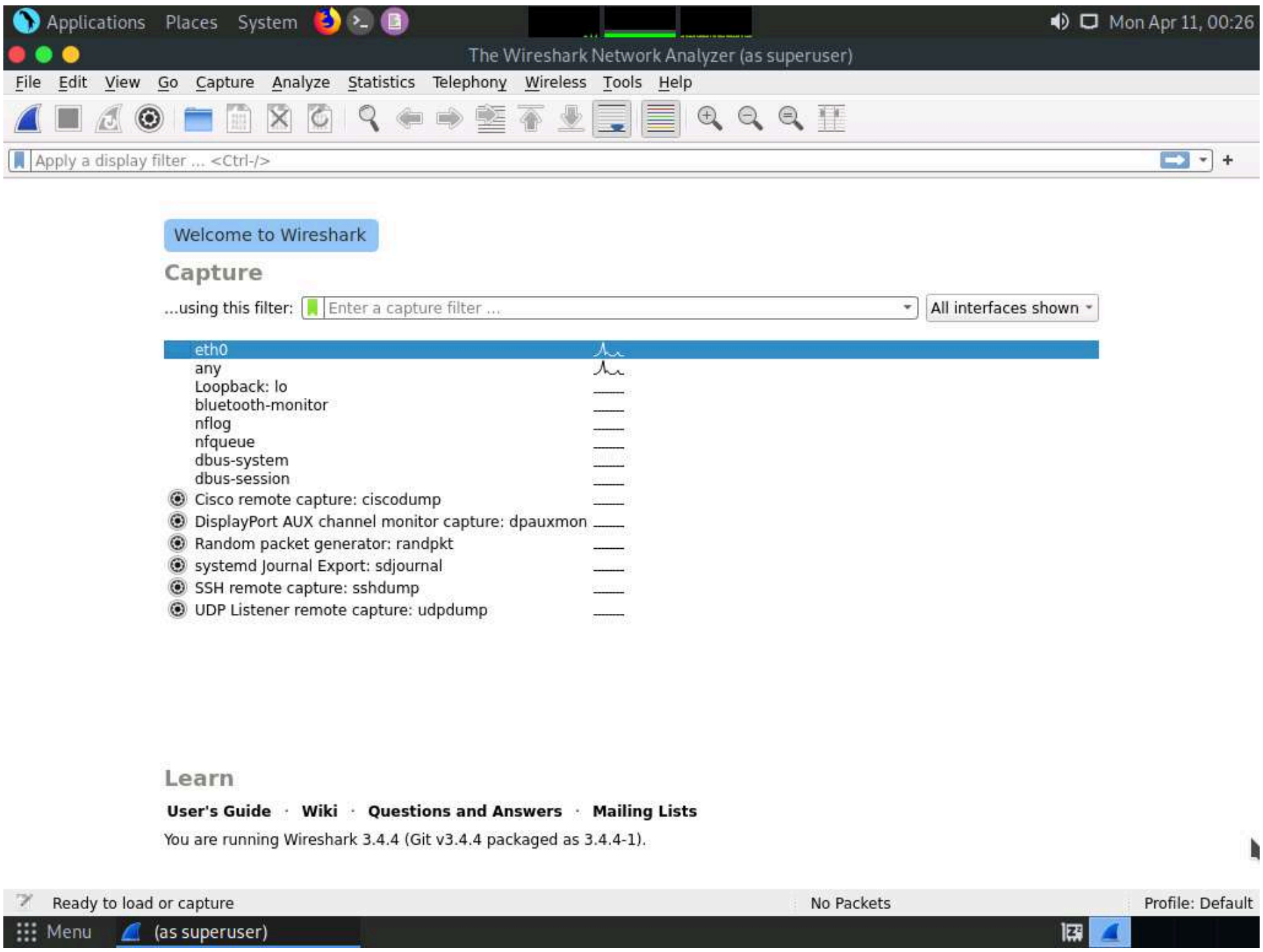
1. On the **Parrot Security** machine; click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



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

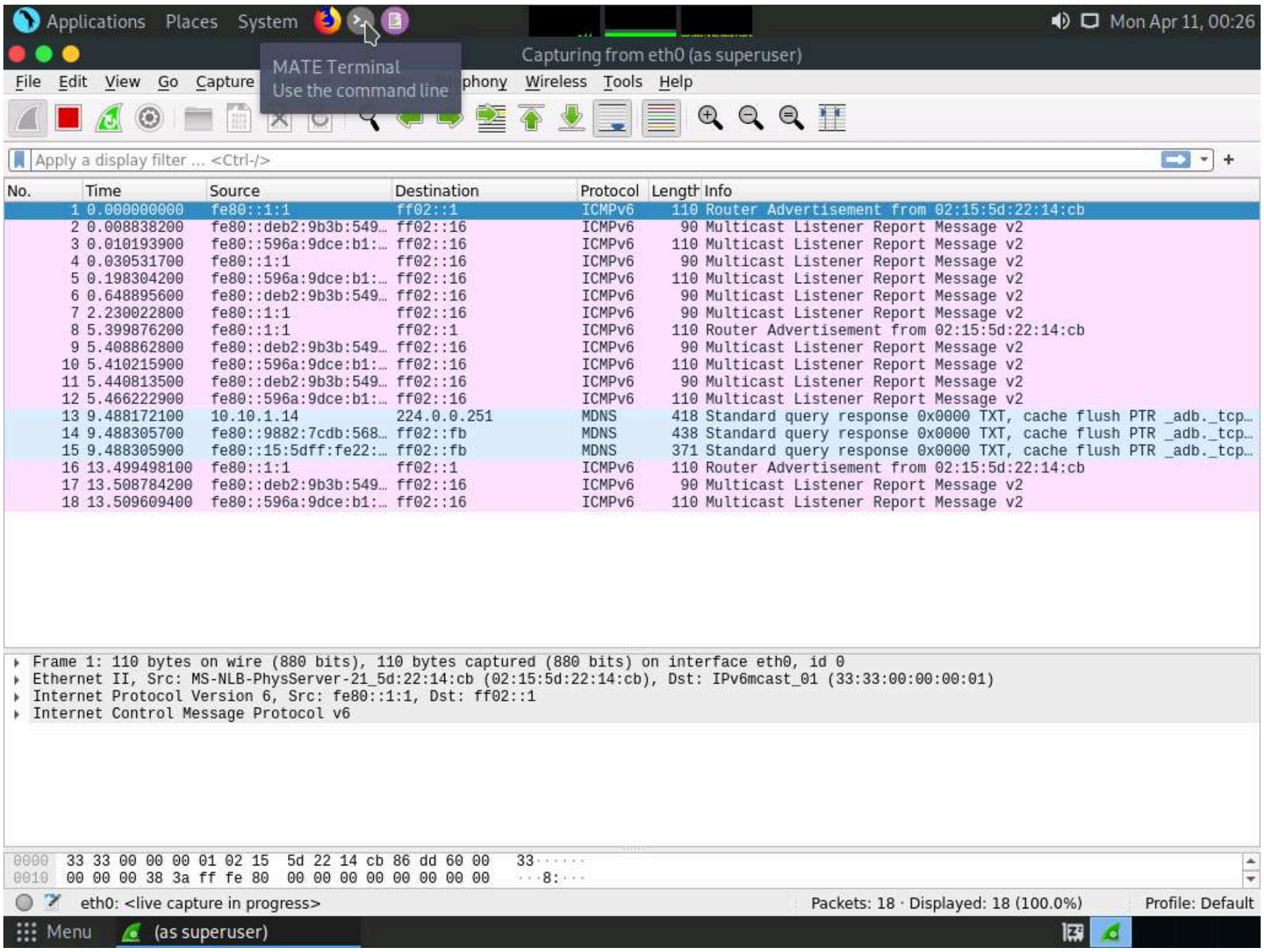


3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



4. Leave the **Wireshark** application running.

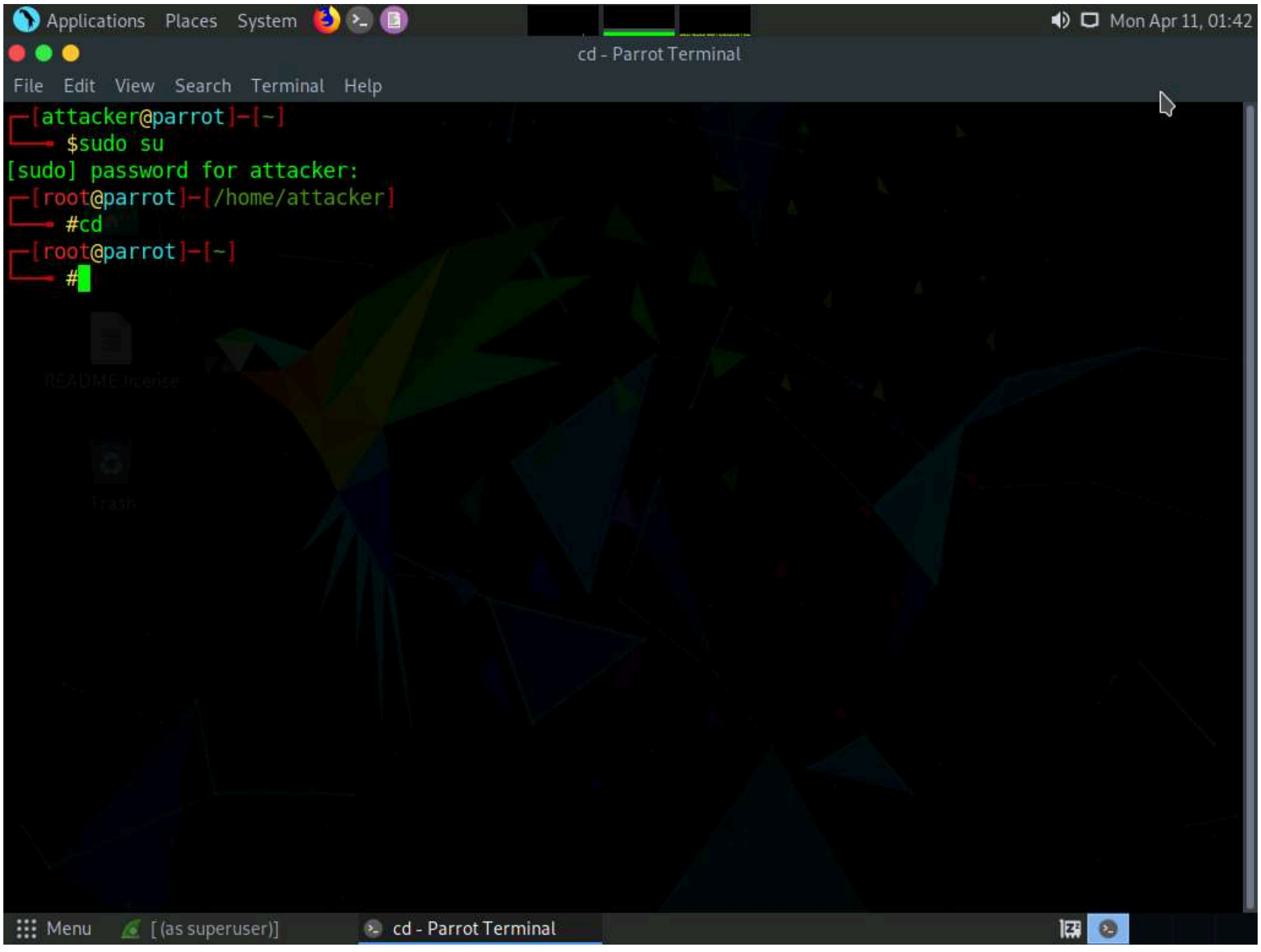
5. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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**.

8. Now, type **cd** and press **Enter** to jump to the root directory.



9. In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.1.1 10.10.1.11** and press **Enter**.

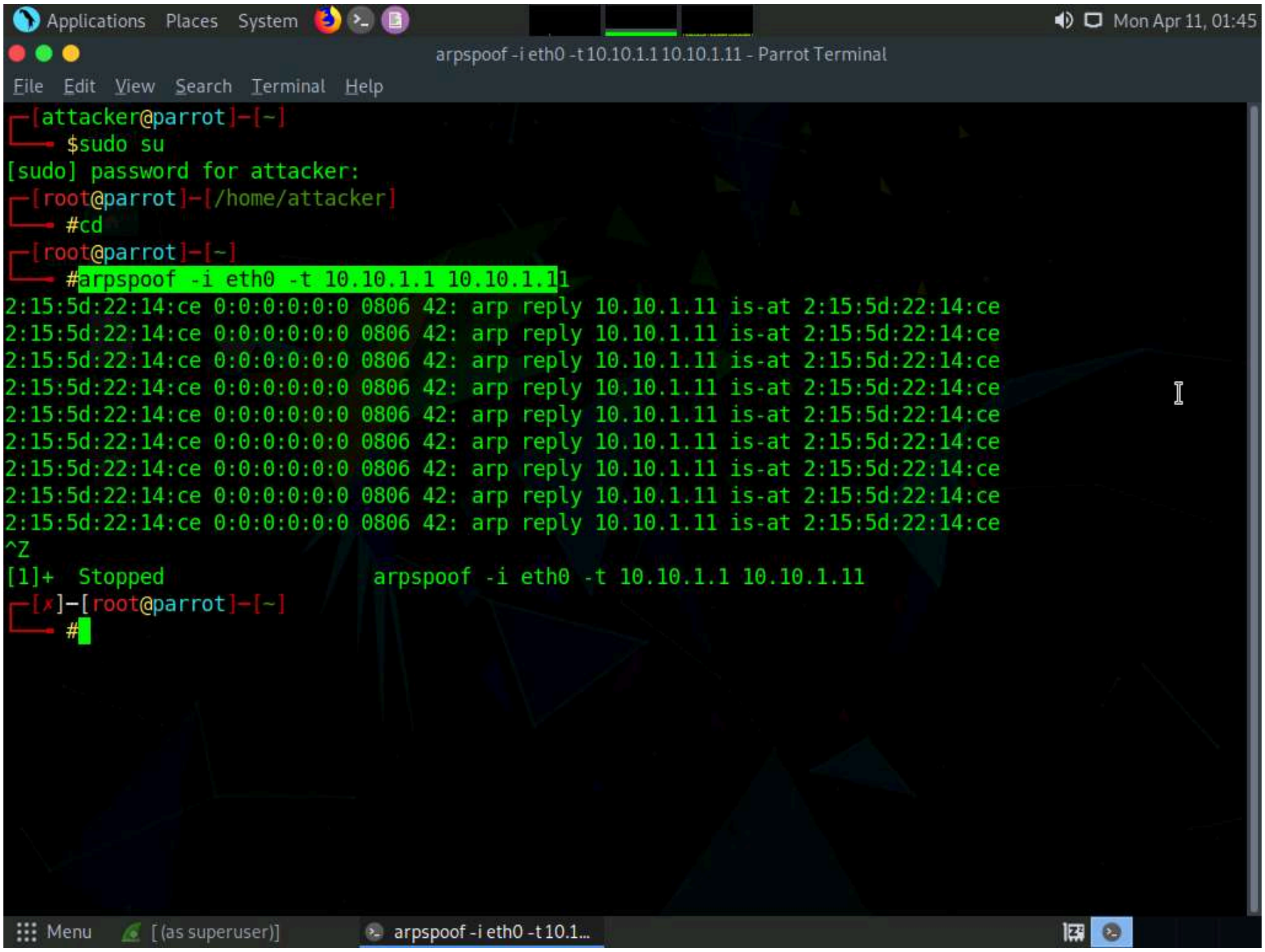
   (Here, **10.10.1.11** is IP address of the target system [**Windows 11**], and **10.10.1.1** is IP address of the access point or gateway)

Note: **-i**: specifies network interface and **-t**: specifies target IP address.

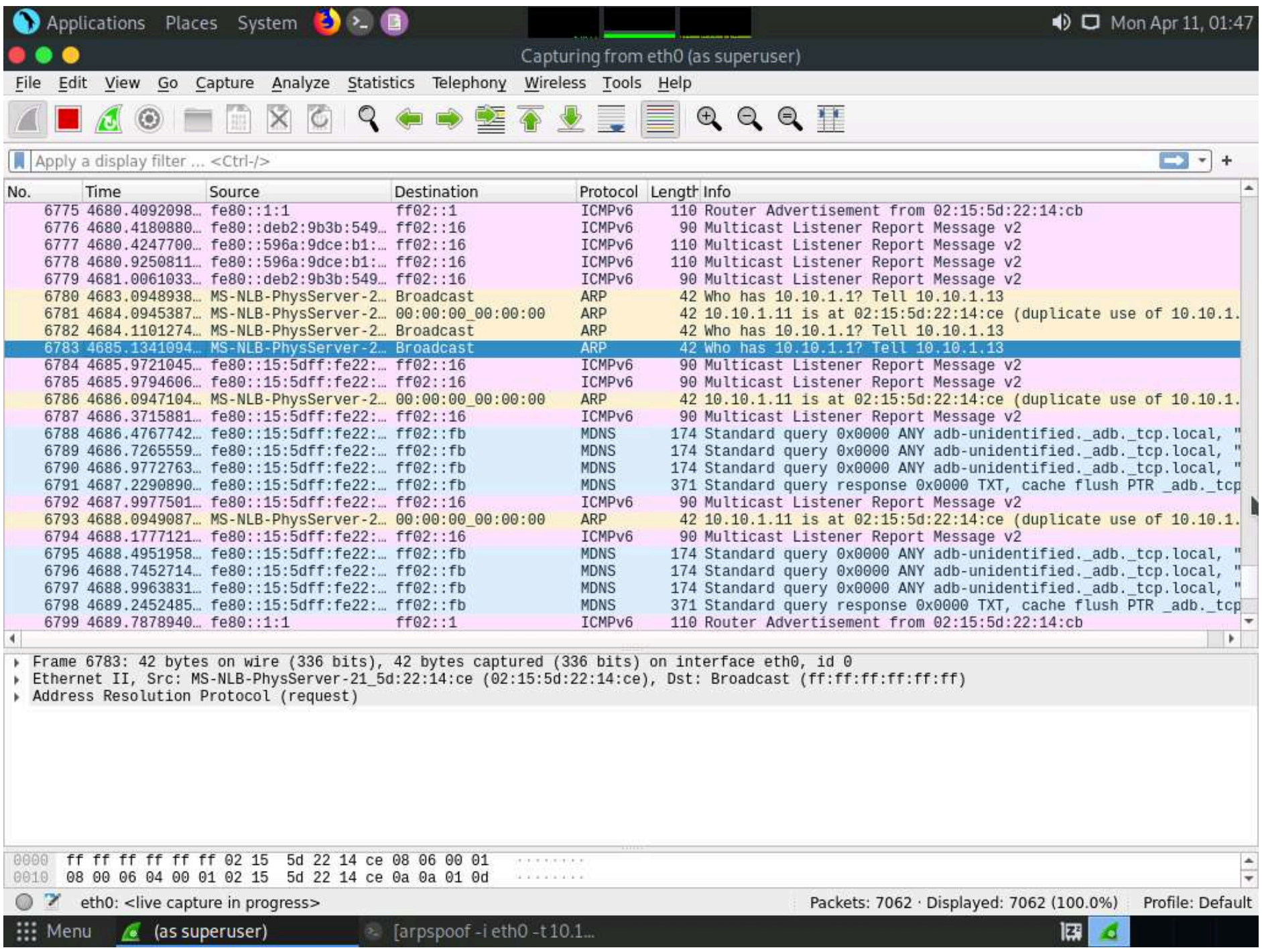
10. Issuing the above command informs the access point that the target system (**10.10.1.11**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.

11. 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.



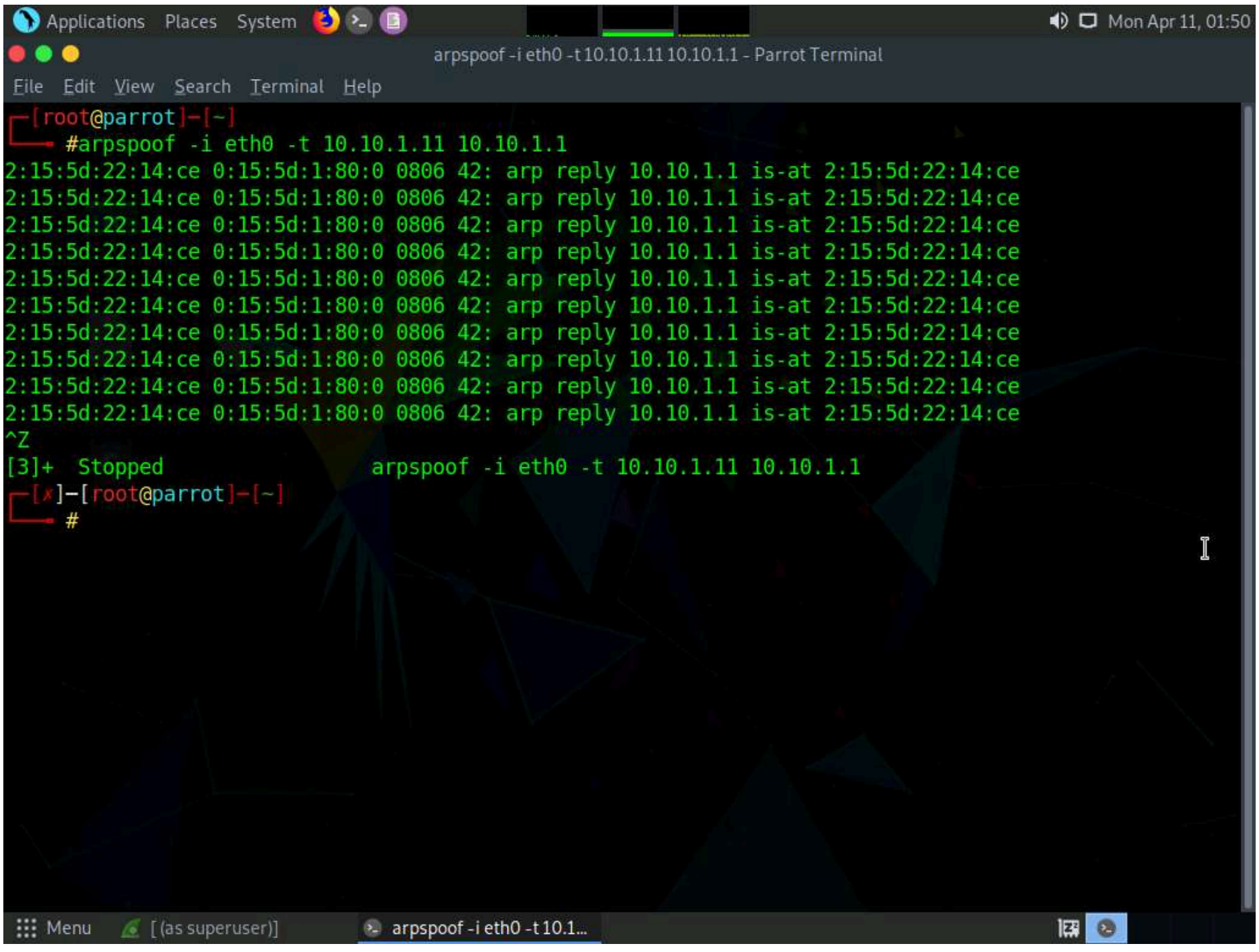
12. Switch to the **Wireshark** window and you can observe the captured **ARP** packets, as shown in the screenshot.



13. 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**.

14. 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**).

15. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

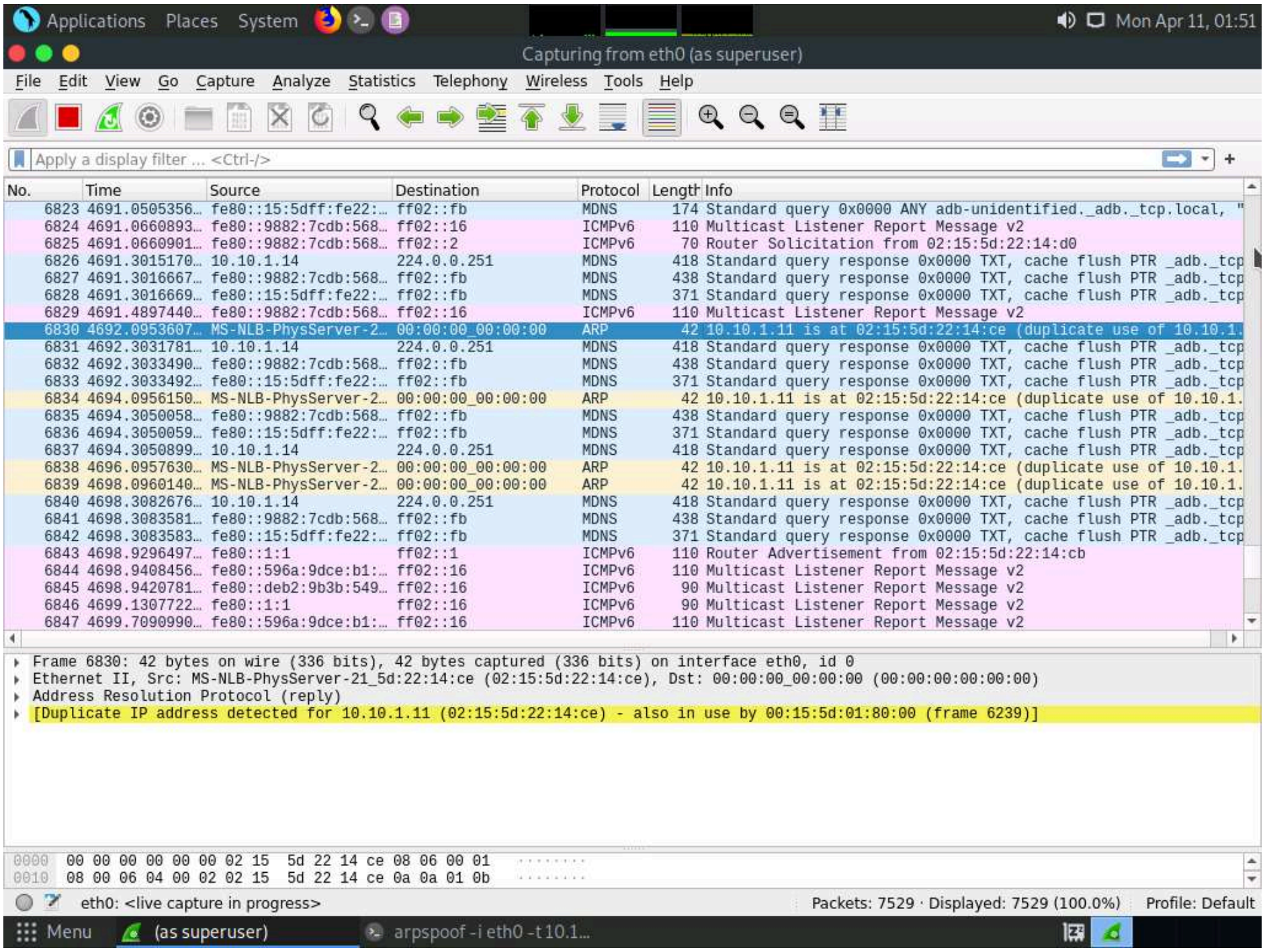


16. In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.1.11 detected!**"

17. 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**.

18. Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 11**) and access point. Therefore, the alert warning of a duplicate use of **10.10.1.11** is displayed.



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

19. 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.
20. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
21. Close all open windows and document all the acquired information.

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

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

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

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

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

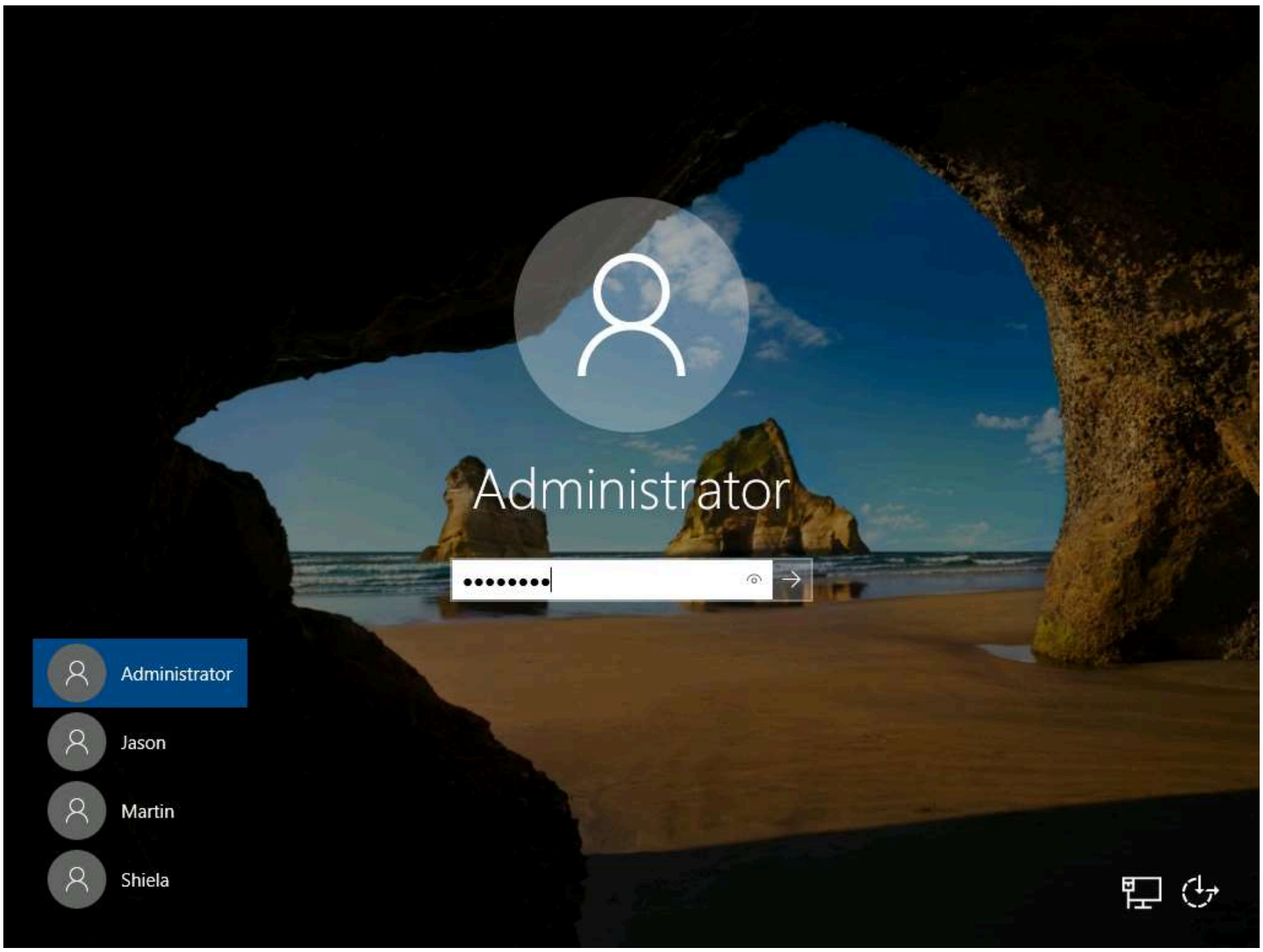
MITM attacks are varied and can be carried out on a switched LAN. MITM attacks can be performed using various tools such as Cain & Abel.

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

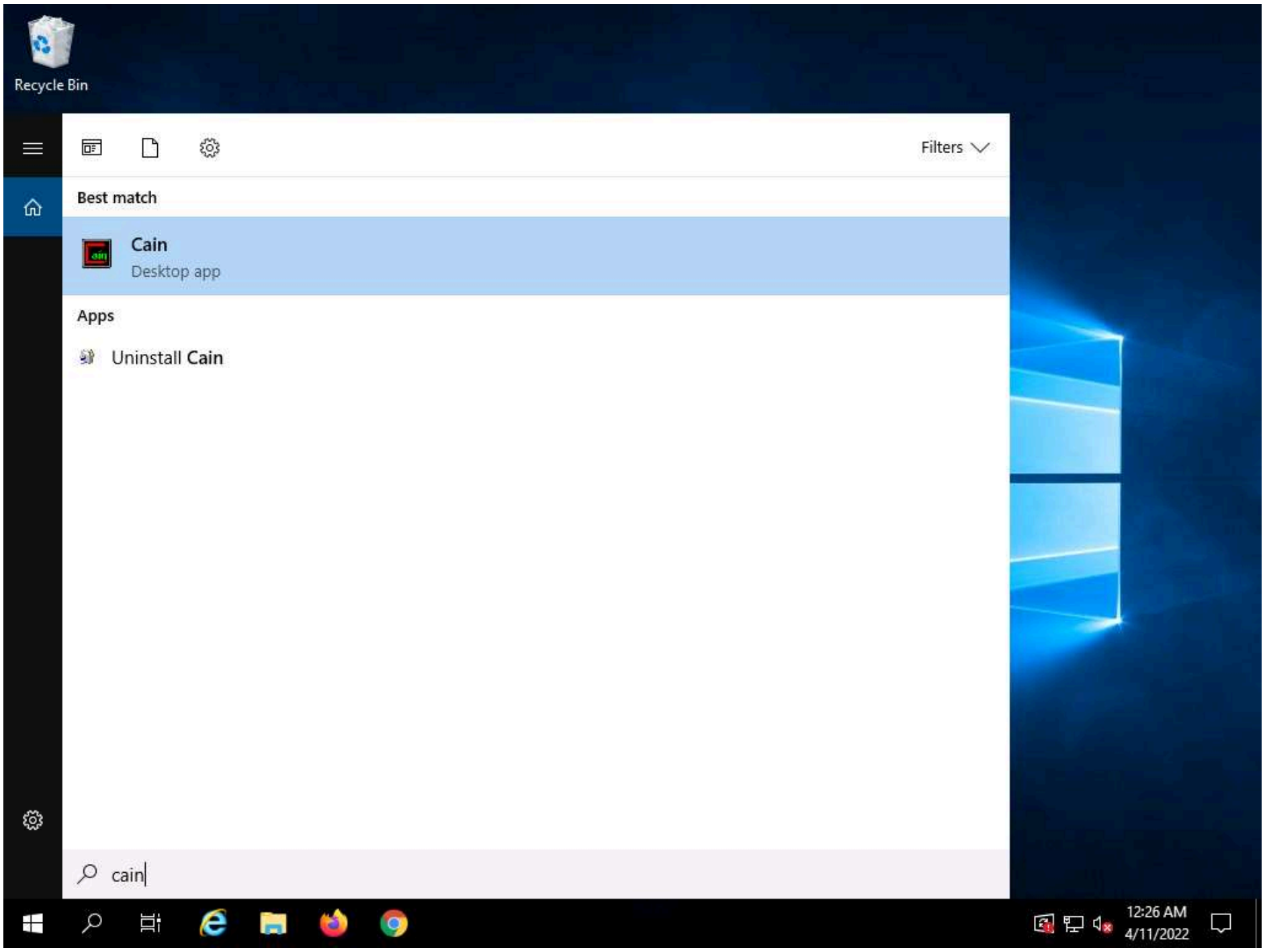
Here, we will use the Cain & Abel tool to perform an MITM attack.

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

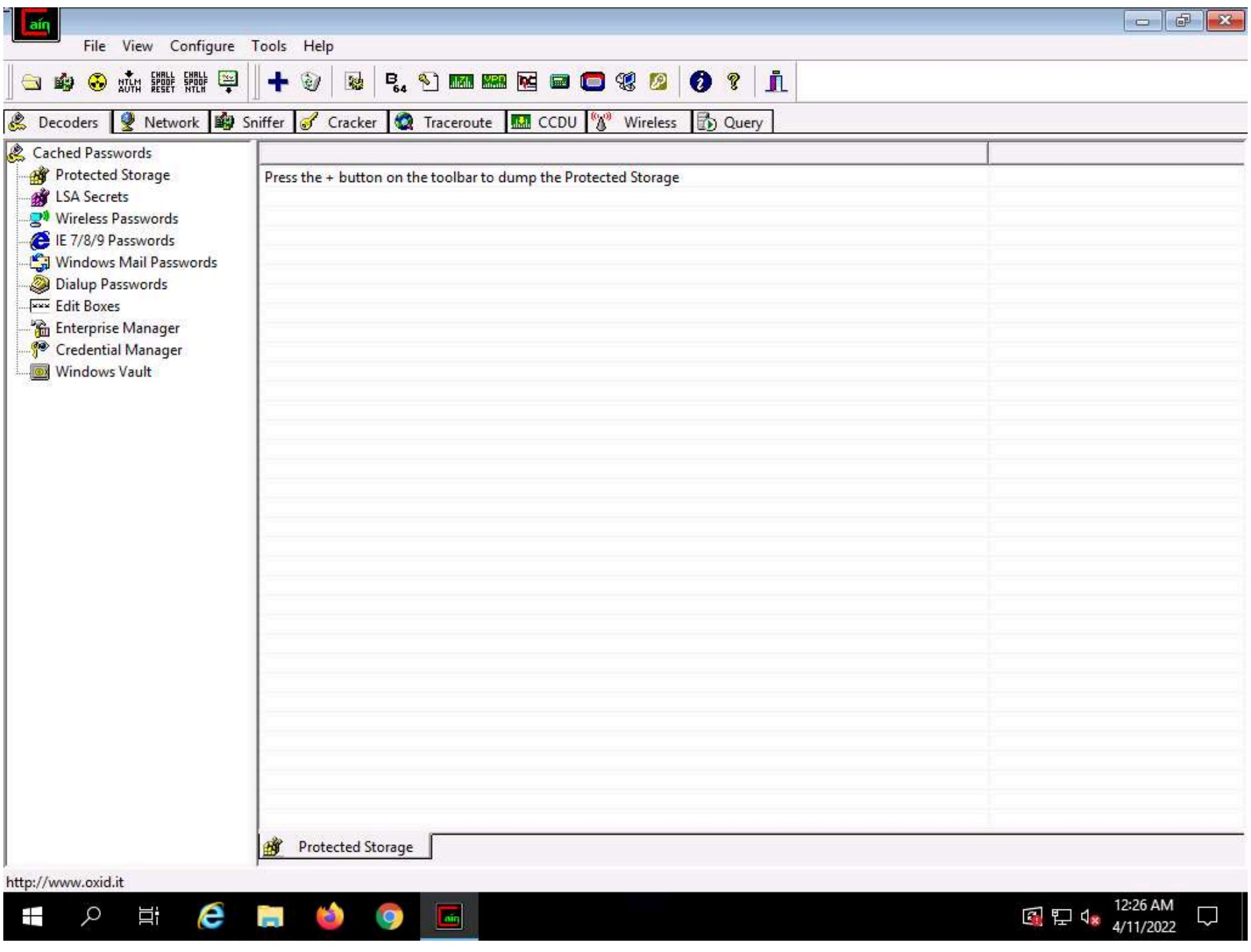
> Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



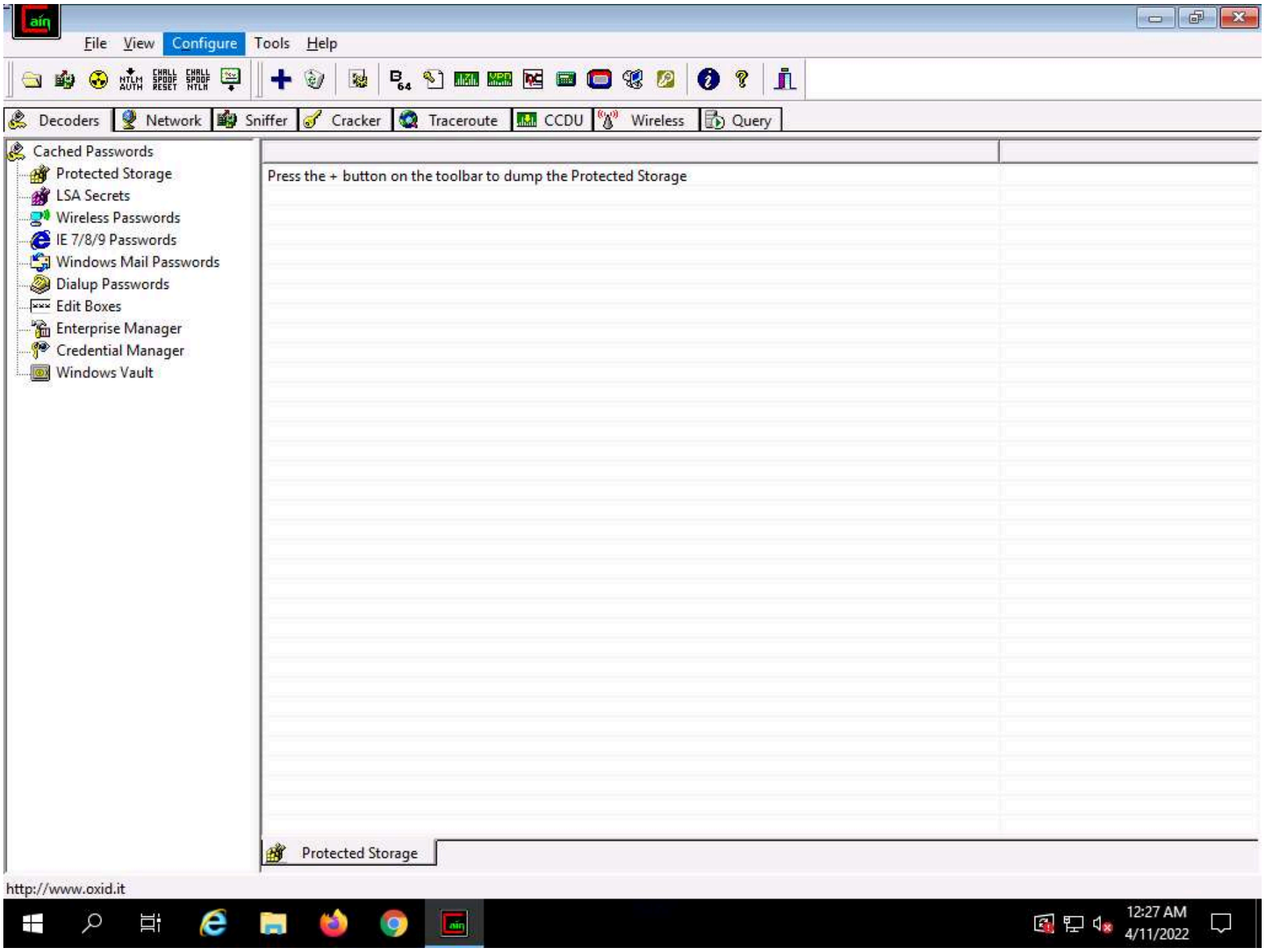
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



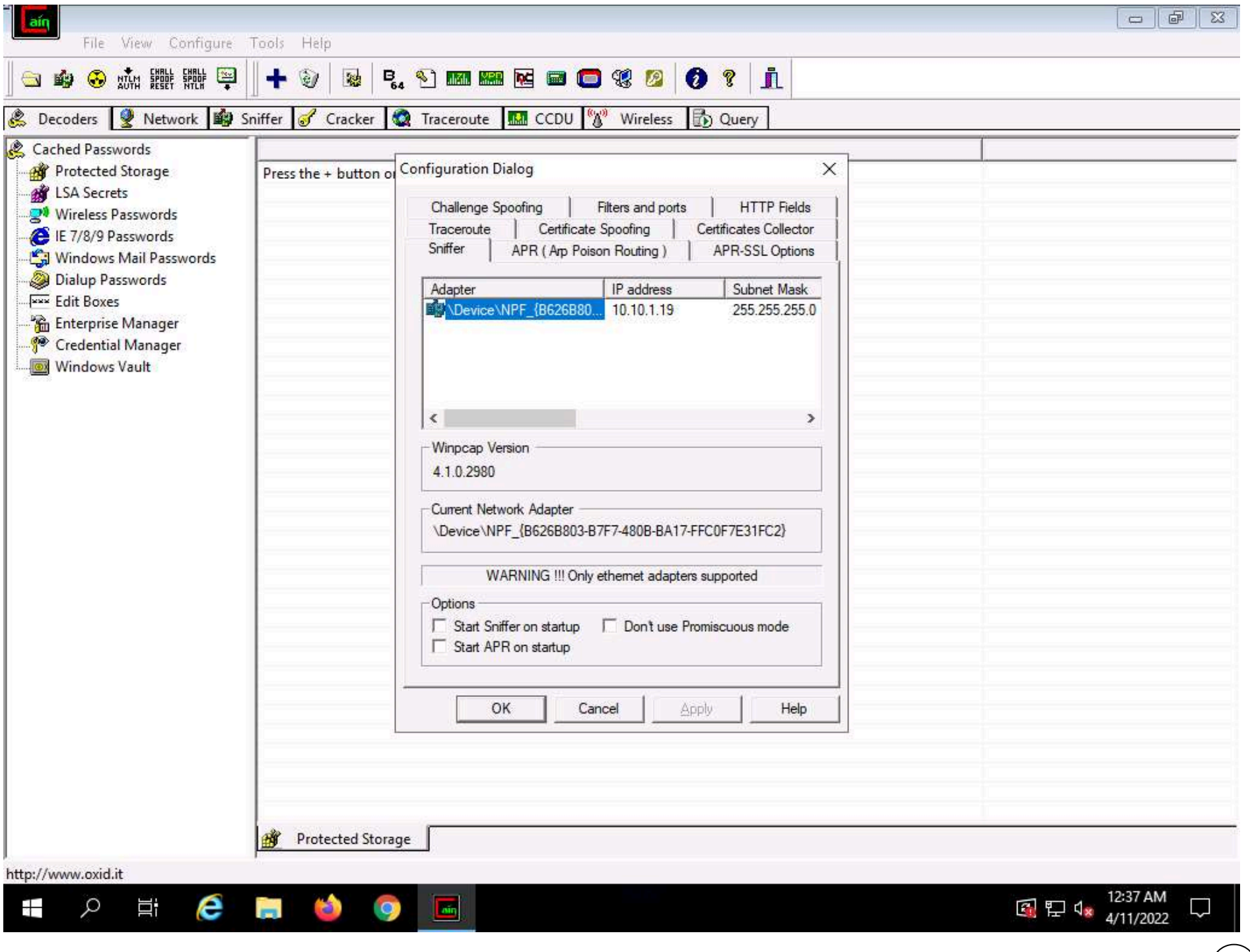
4. The **Cain & Abel** main window appears, as shown in the screenshot.



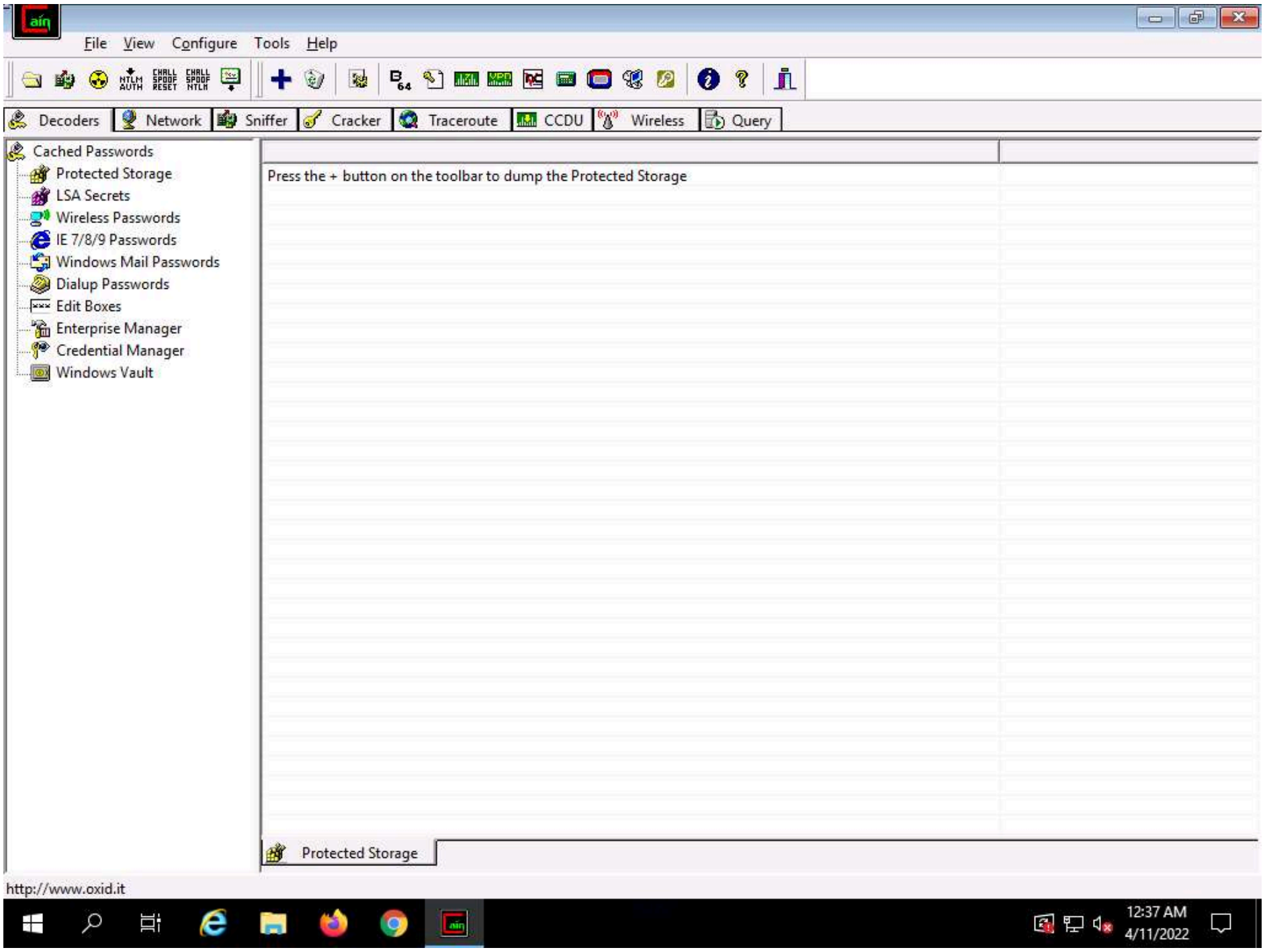
5. Click **Configure** from the menu bar to configure an ethernet card.



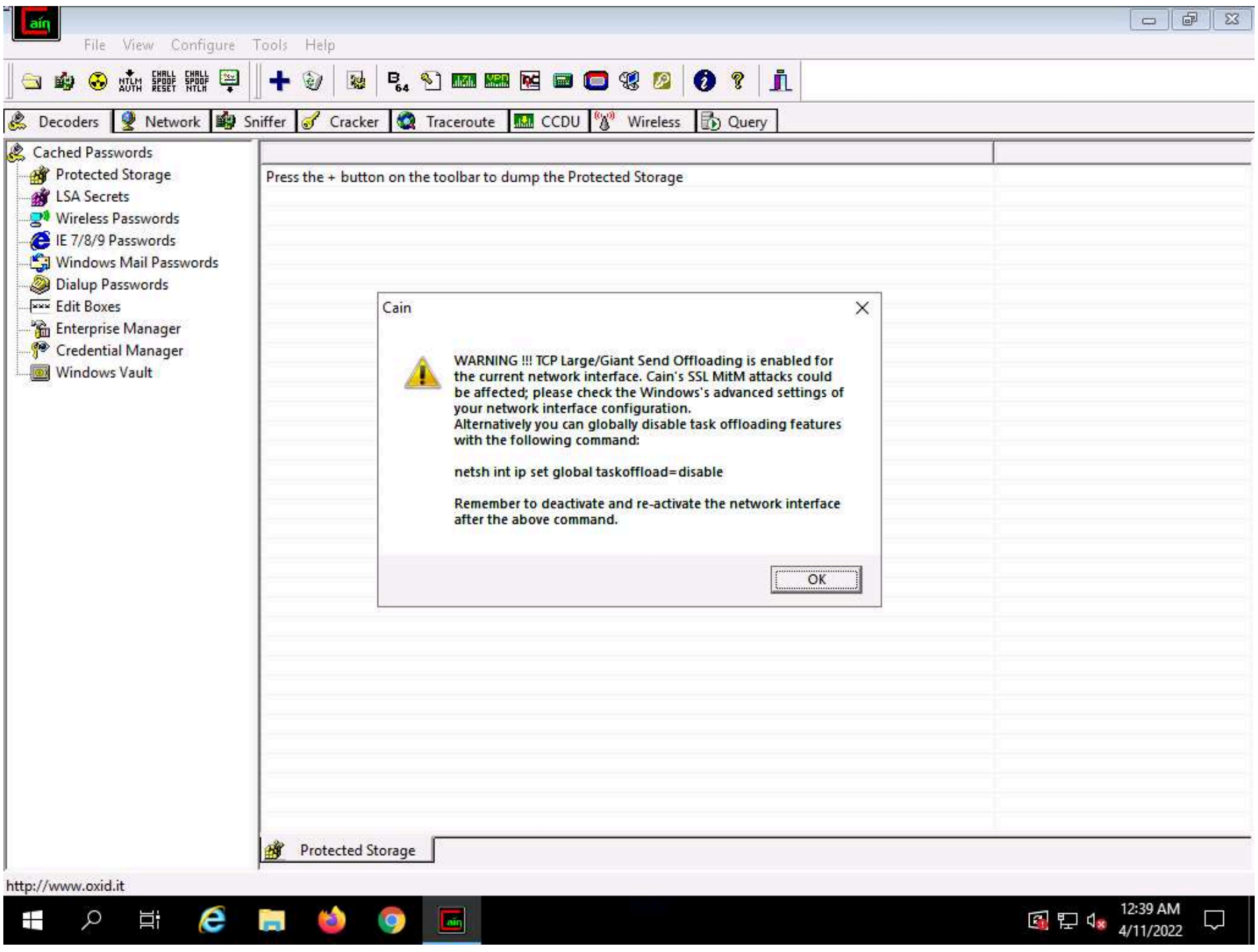
6. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.



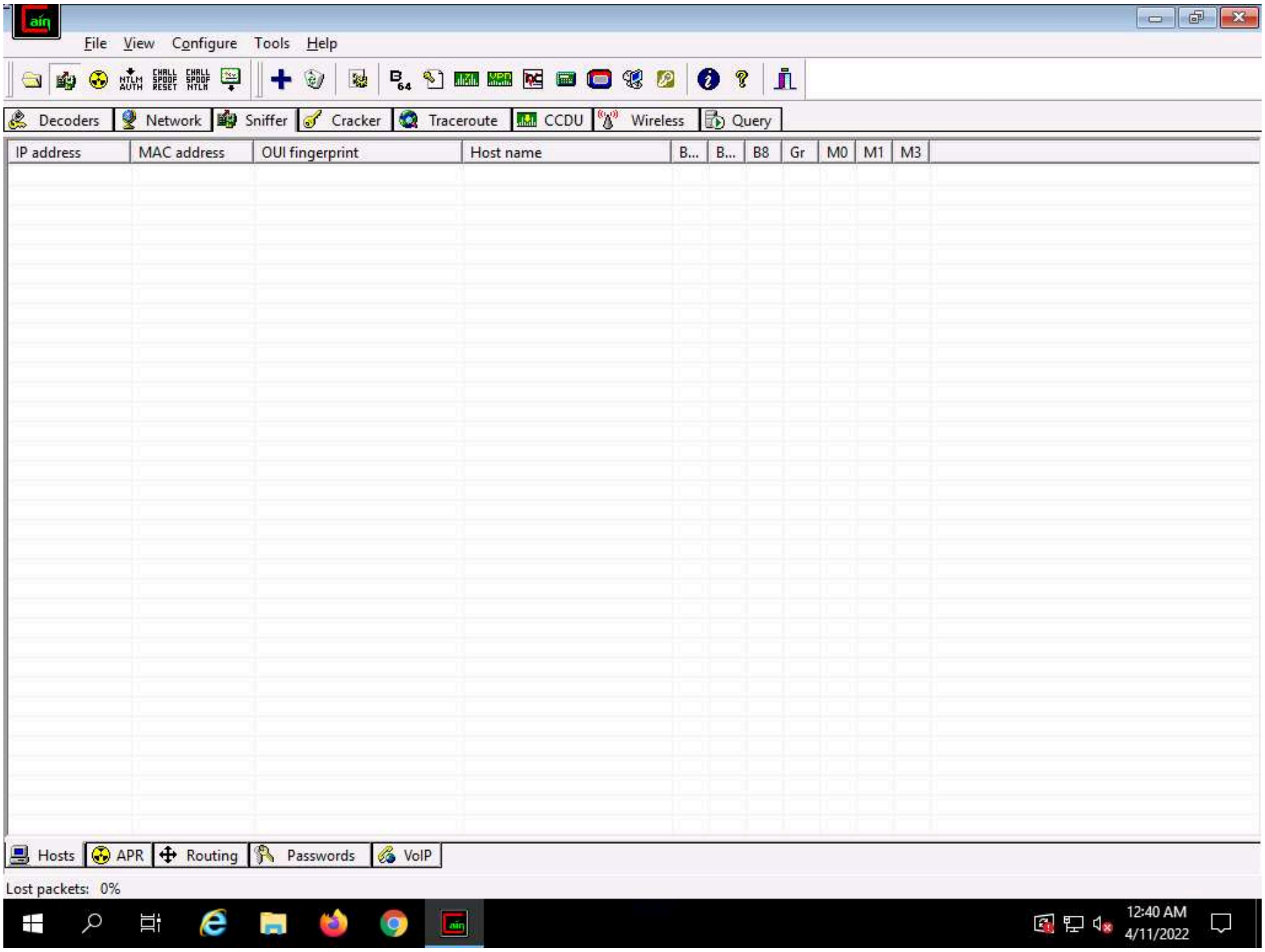
7. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



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

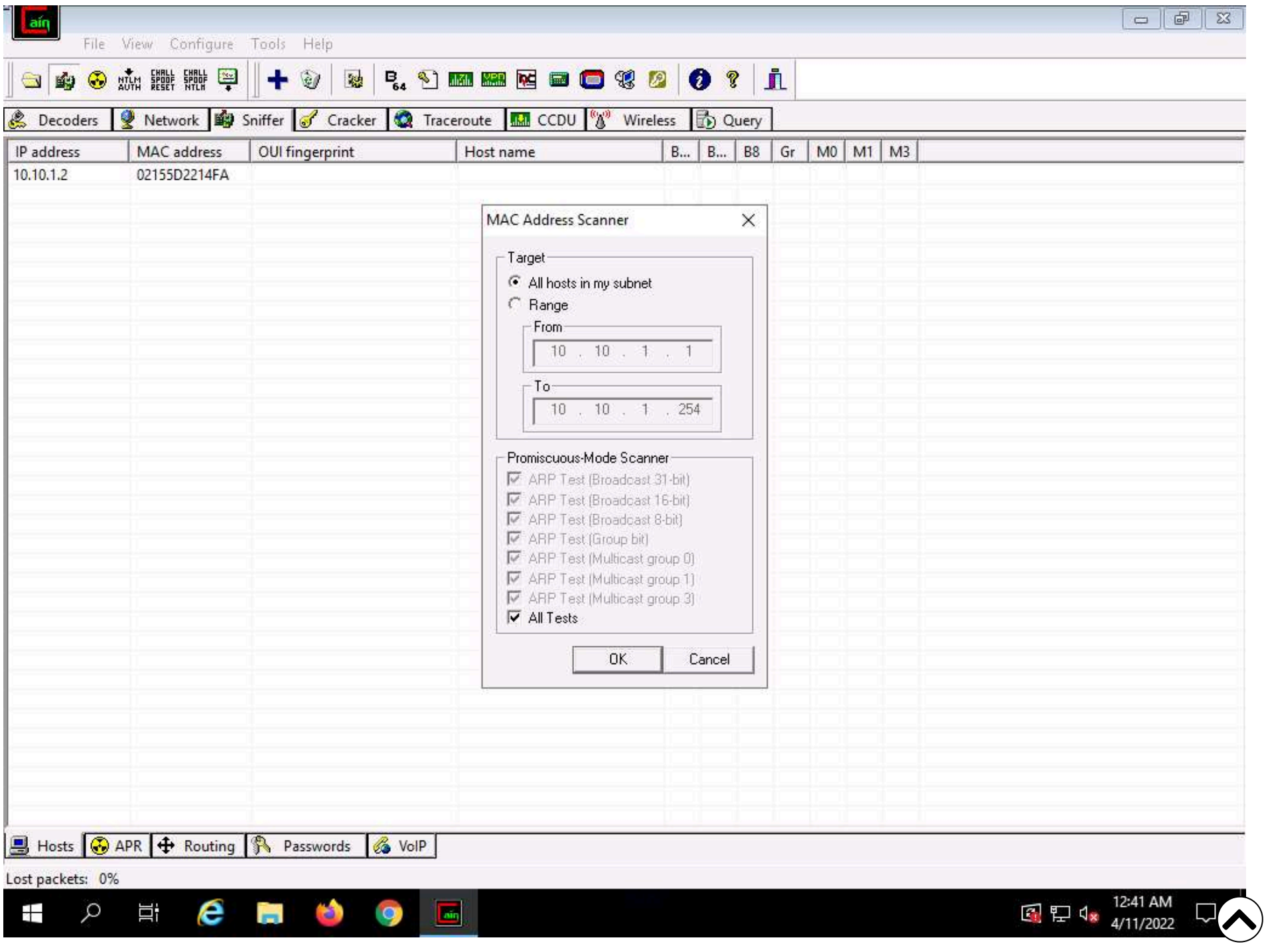


9. Now, click the **Sniffer** tab.



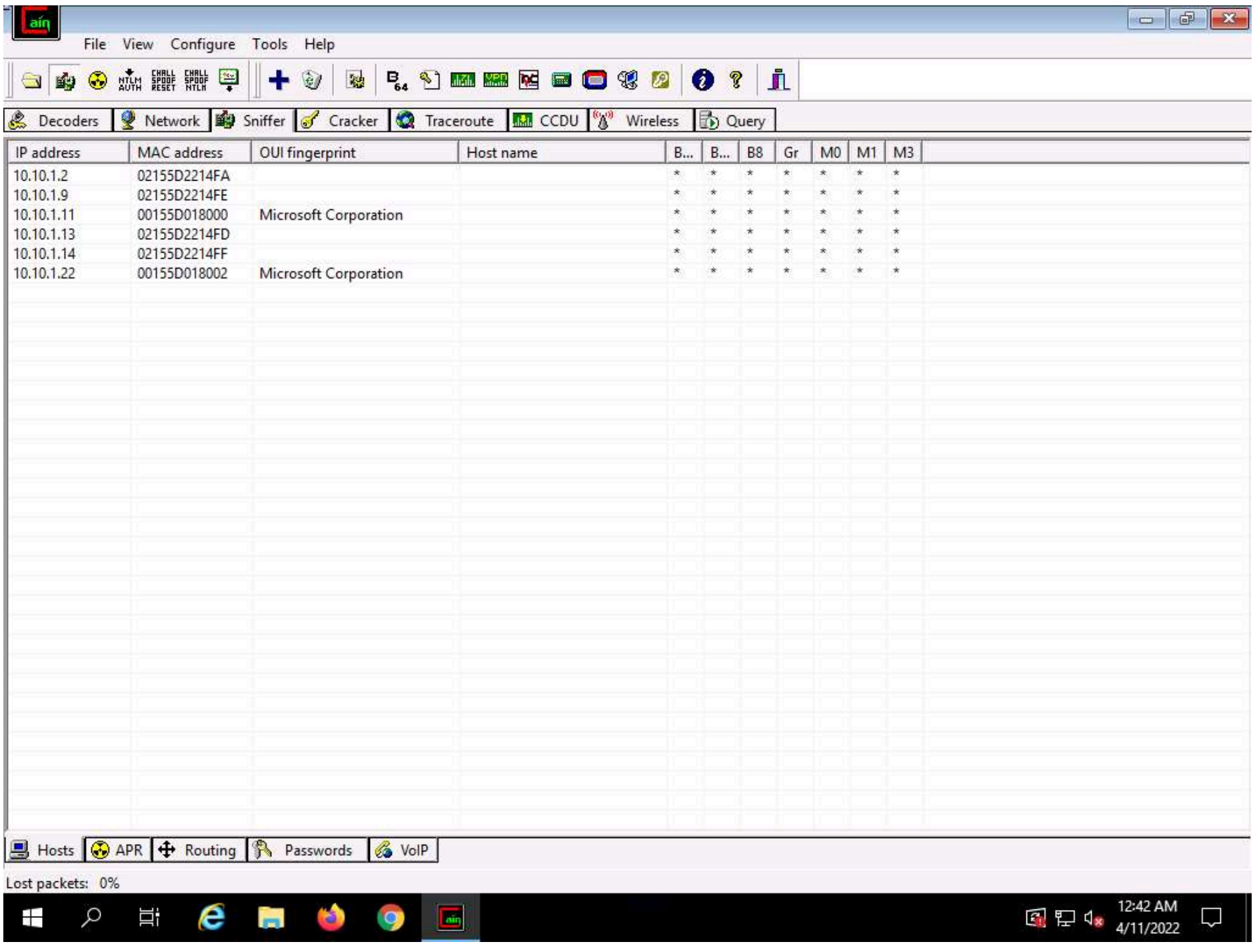
10. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

11. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.



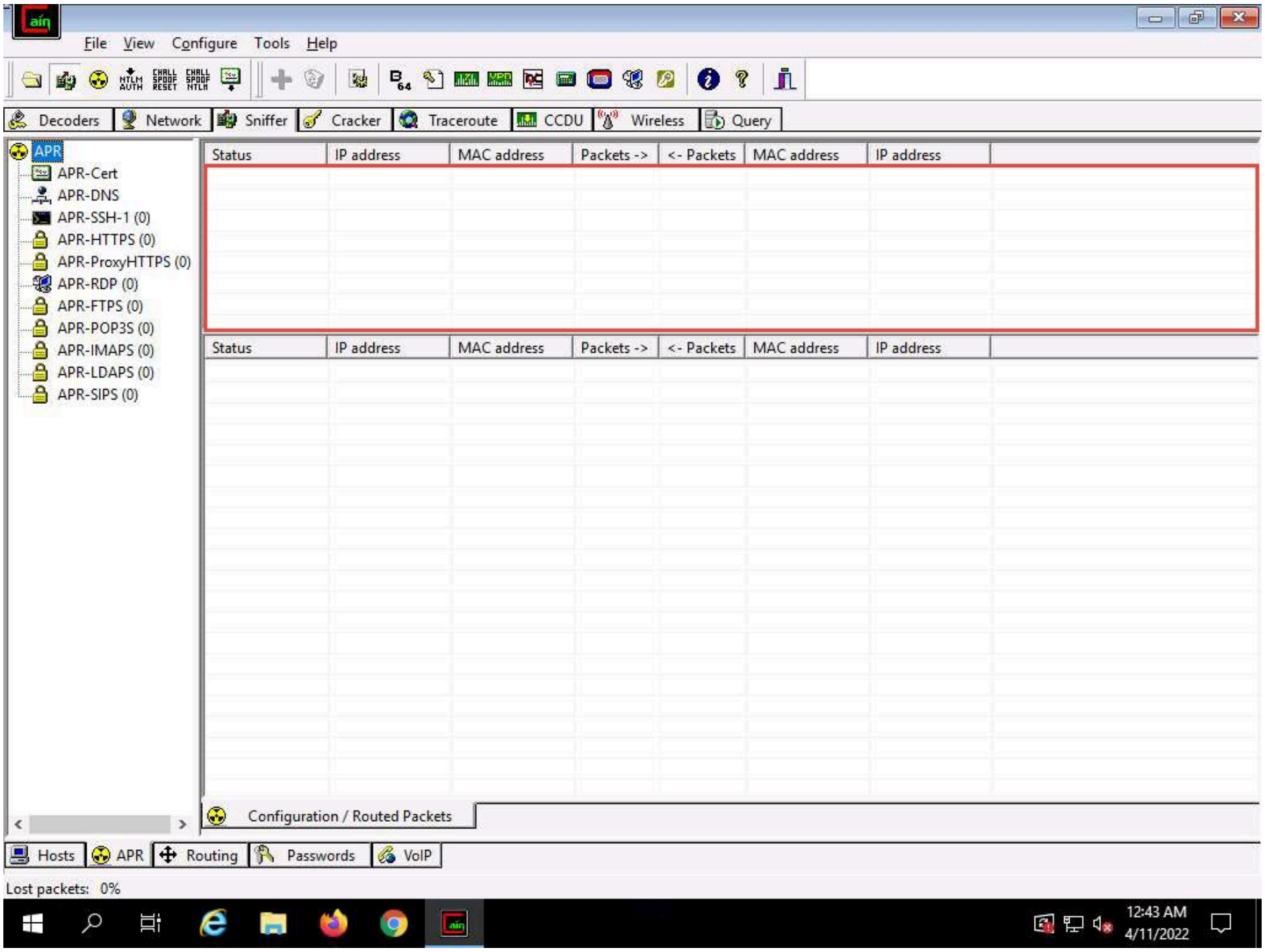
12. Cain & Abel starts scanning for MAC addresses and lists all those found.

13. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

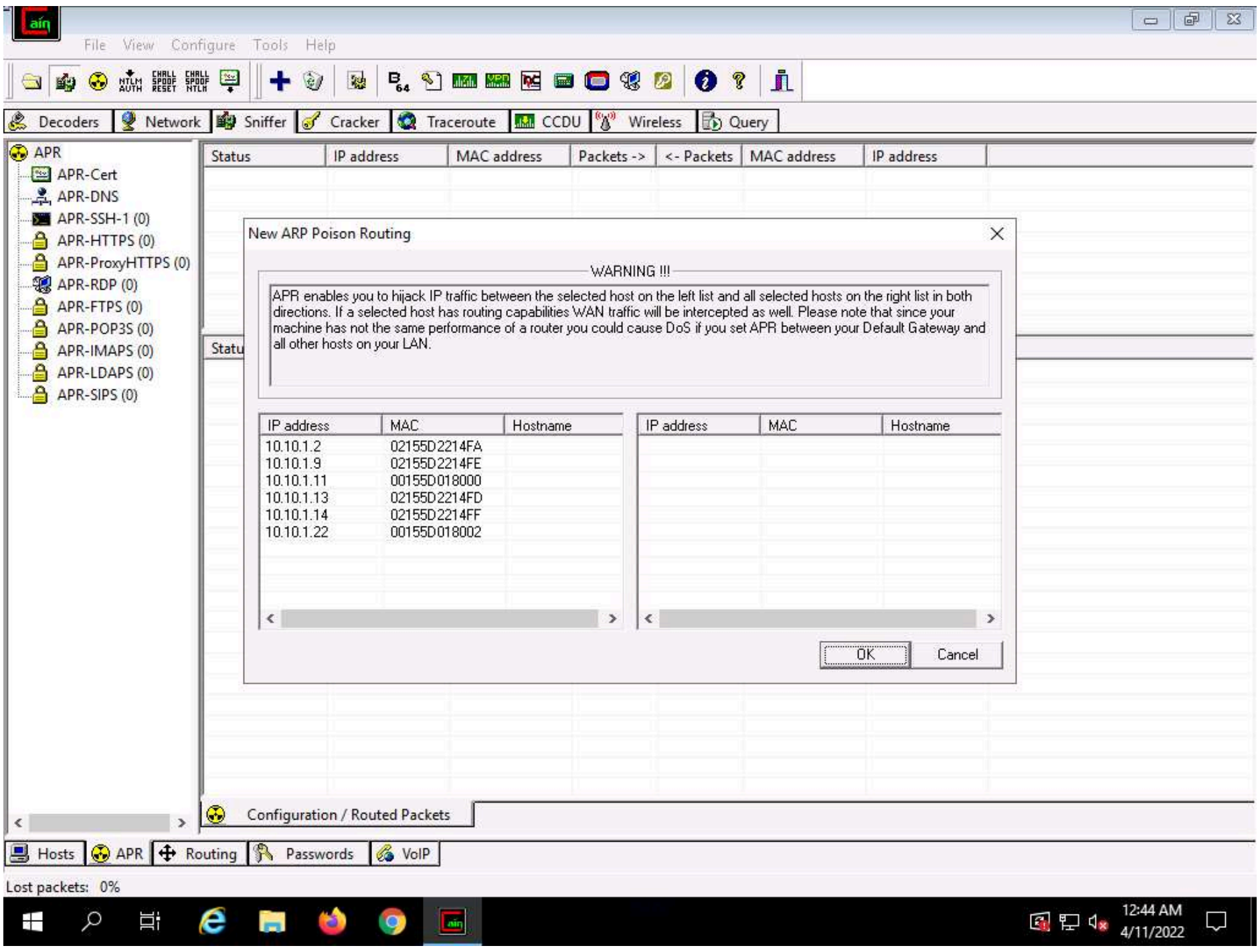


14. Now, click the **APR** tab at the bottom of the window.

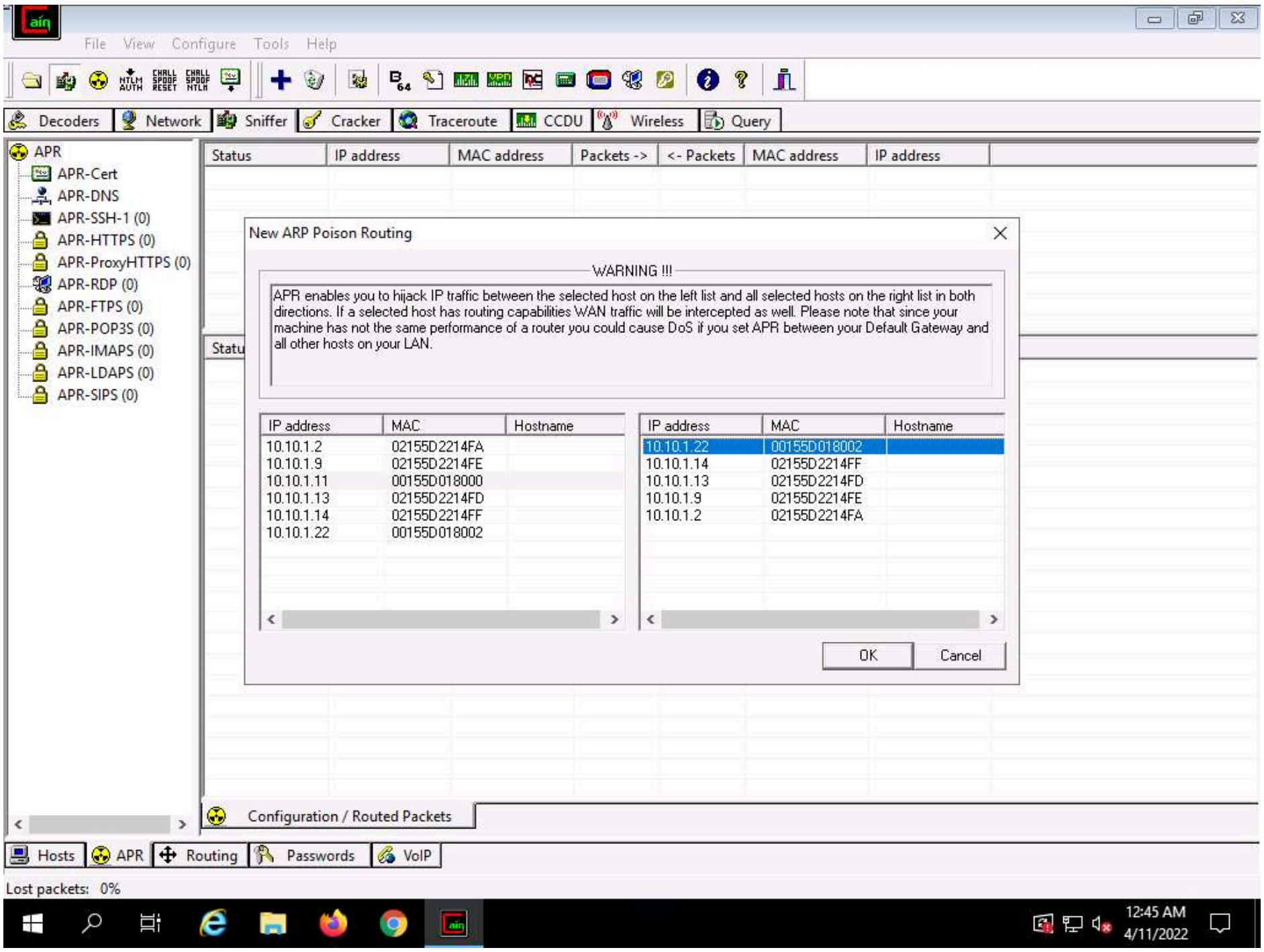
15. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (**+**) icon.



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

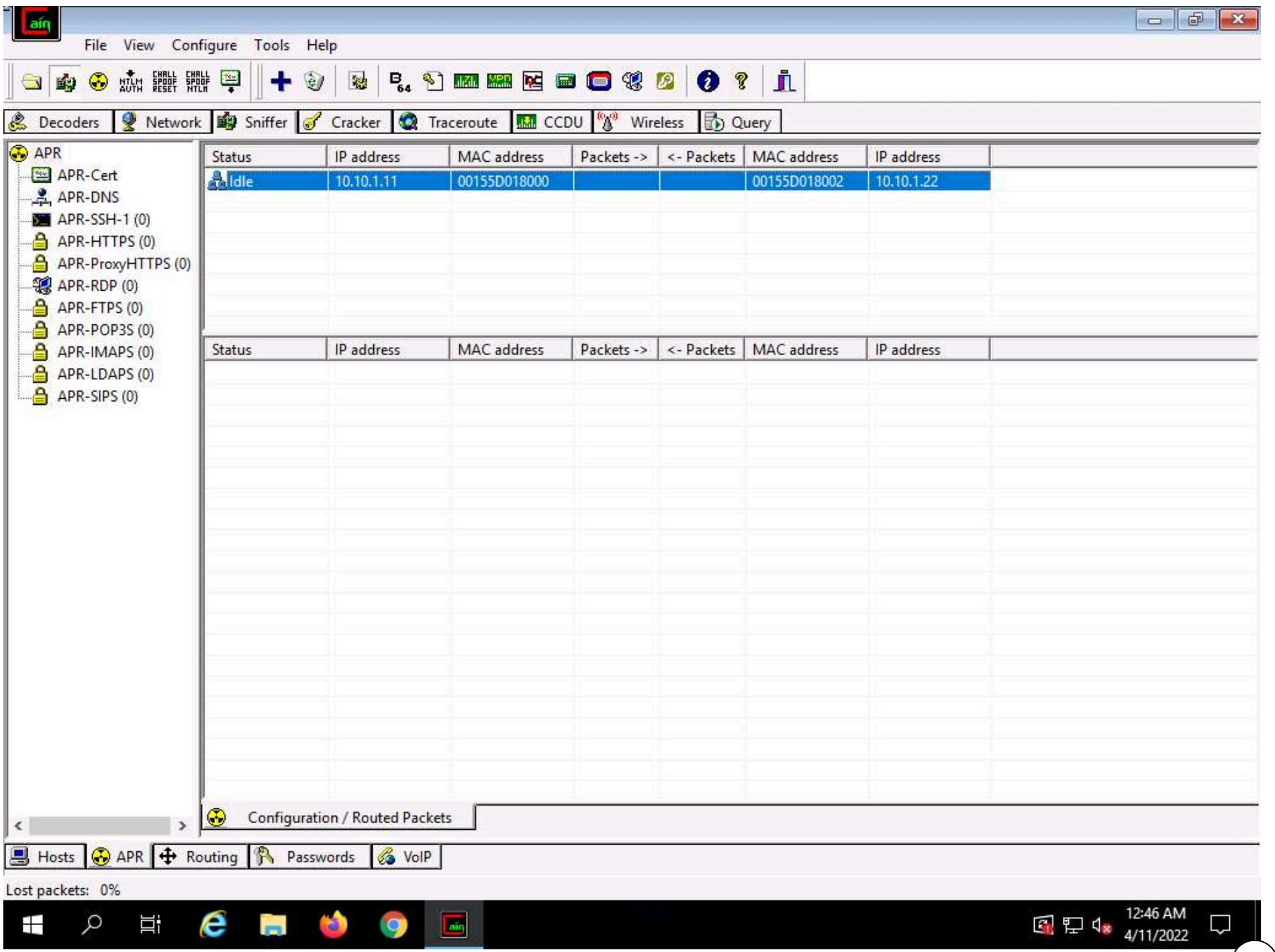


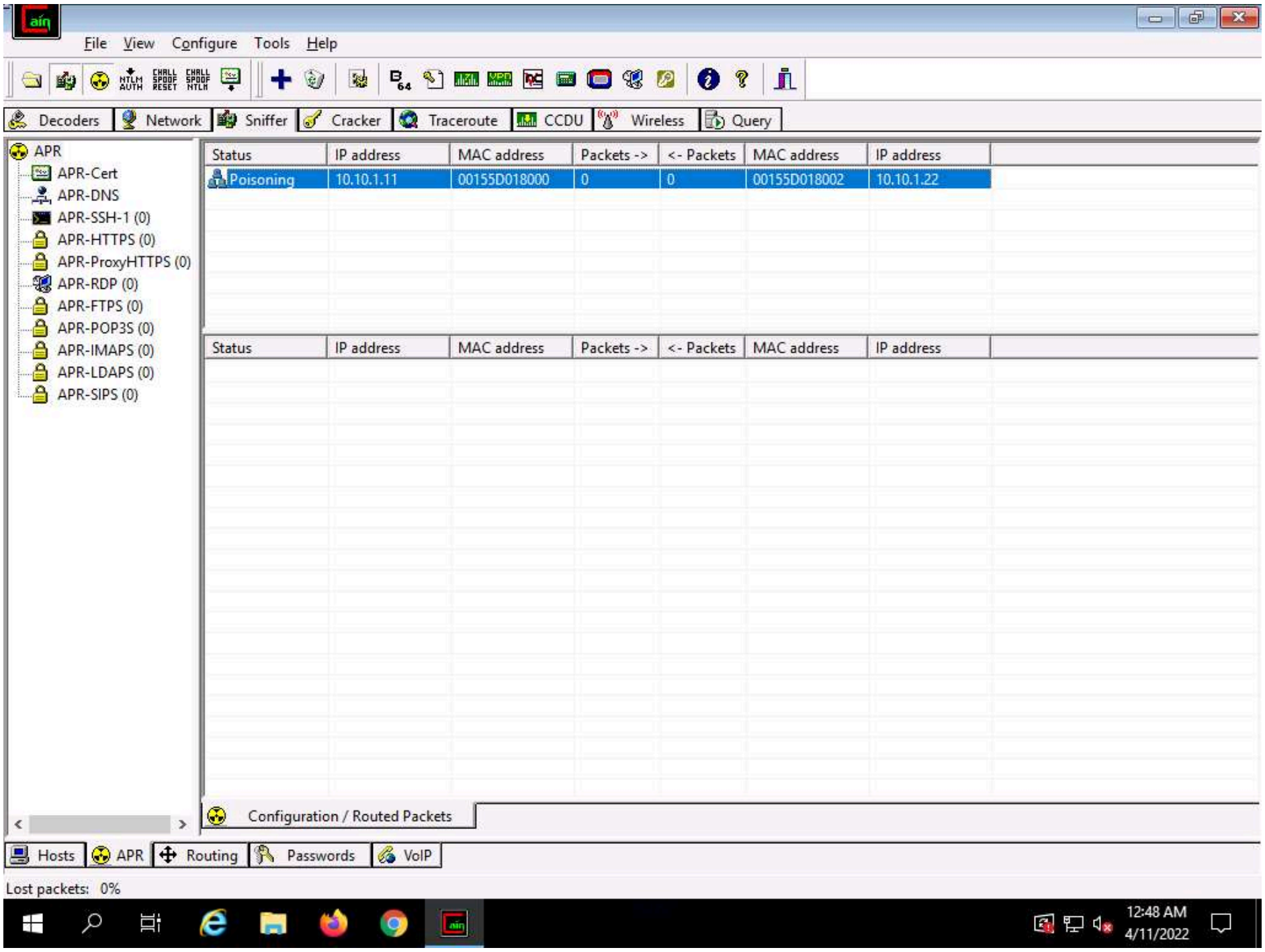
17. To monitor the traffic between two systems (here, **Windows 11** and **Windows Server 2022**), click to select **10.10.1.11** (Windows 11) from the left-hand pane and **10.10.1.22** (**Windows Server 2022**) from the right-hand pane; click **OK**.



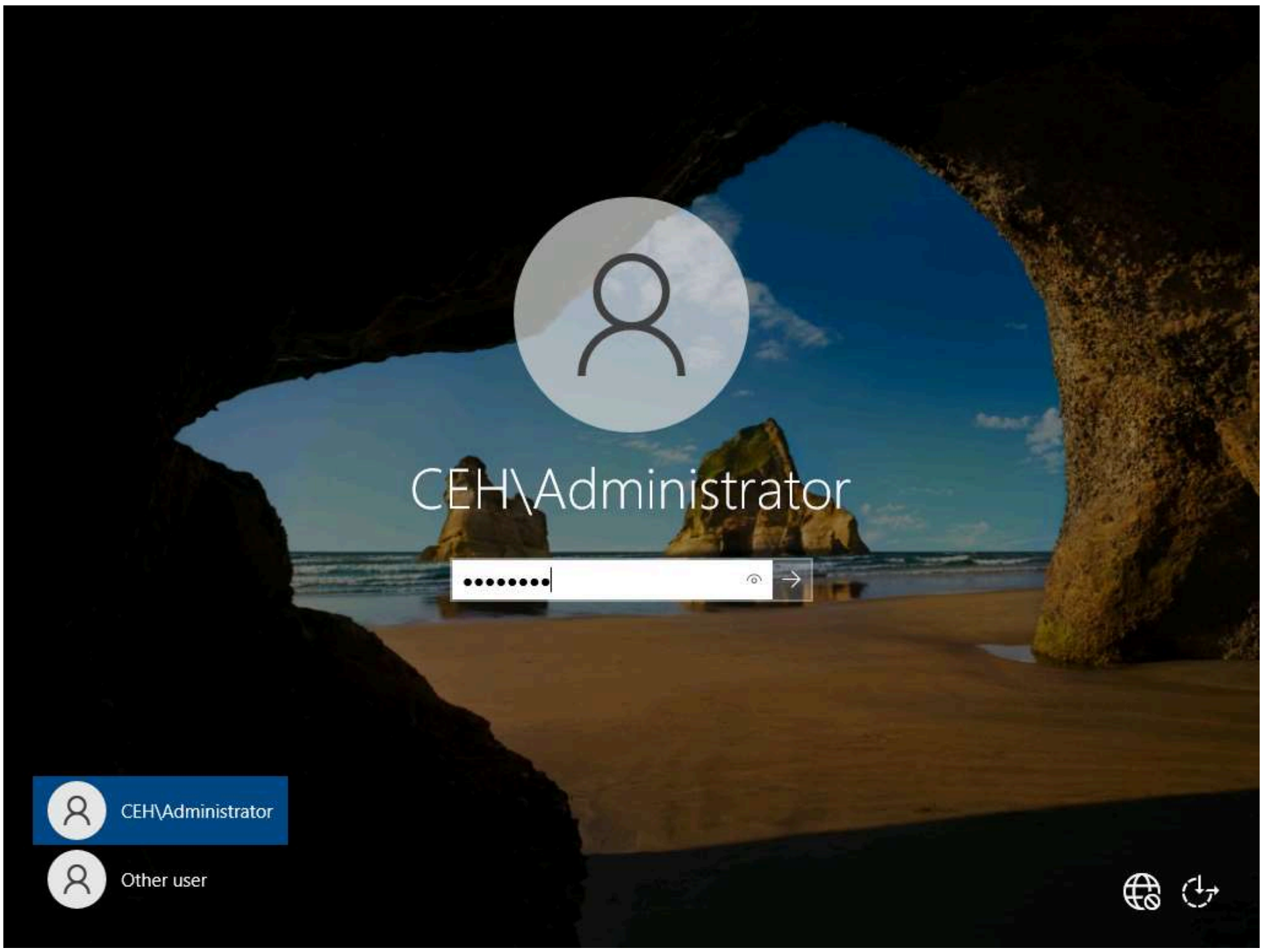
18. Click to select the created target IP address scan displayed in the **Configuration / Routes Packets** tab.

19. Click on the **Start/Stop APR** icon to start capturing ARP packets. The **Status** will change from **Idle** to **Poisoning**.

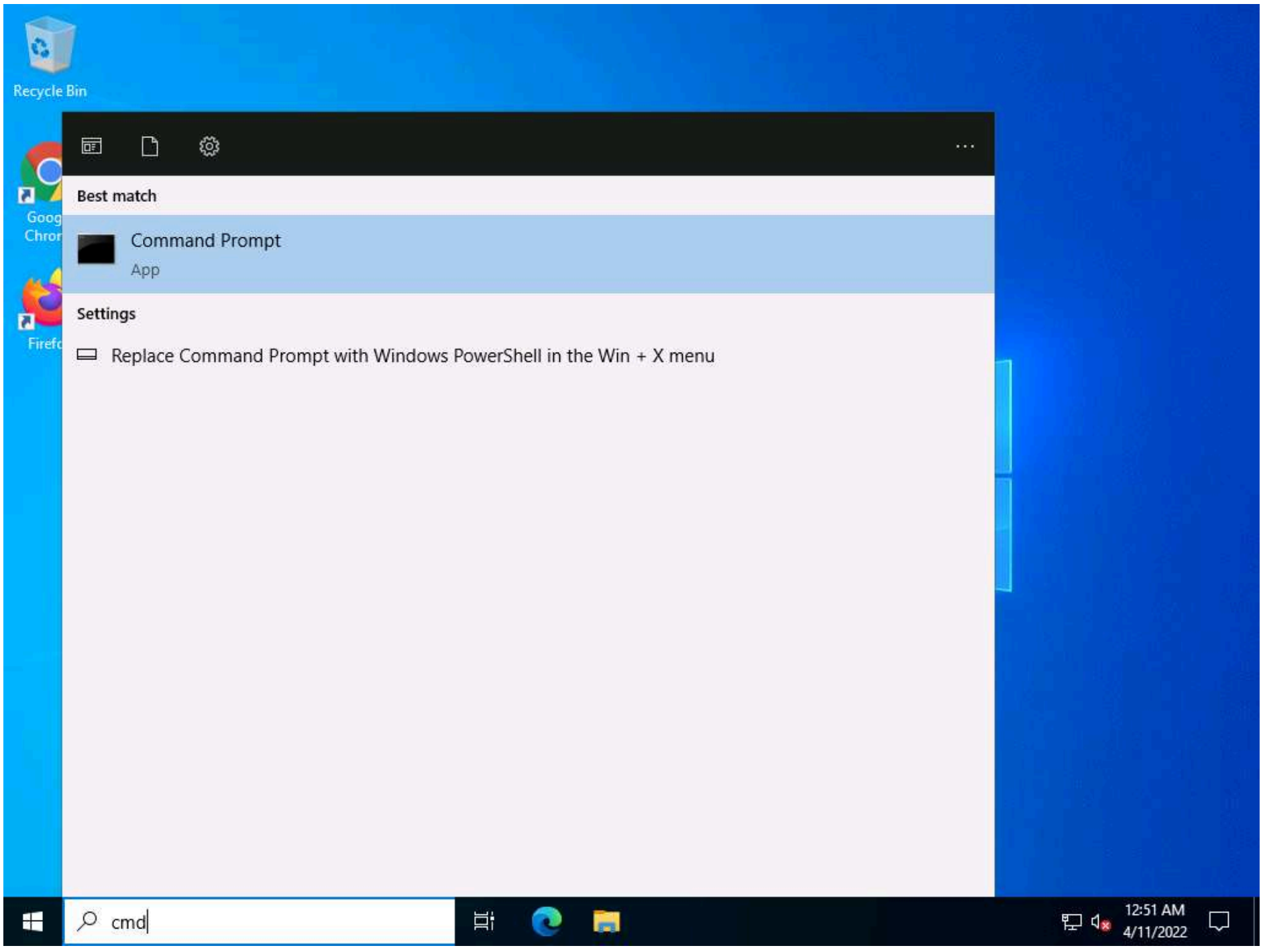




20. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine, click **Ctrl+Alt+Del**. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



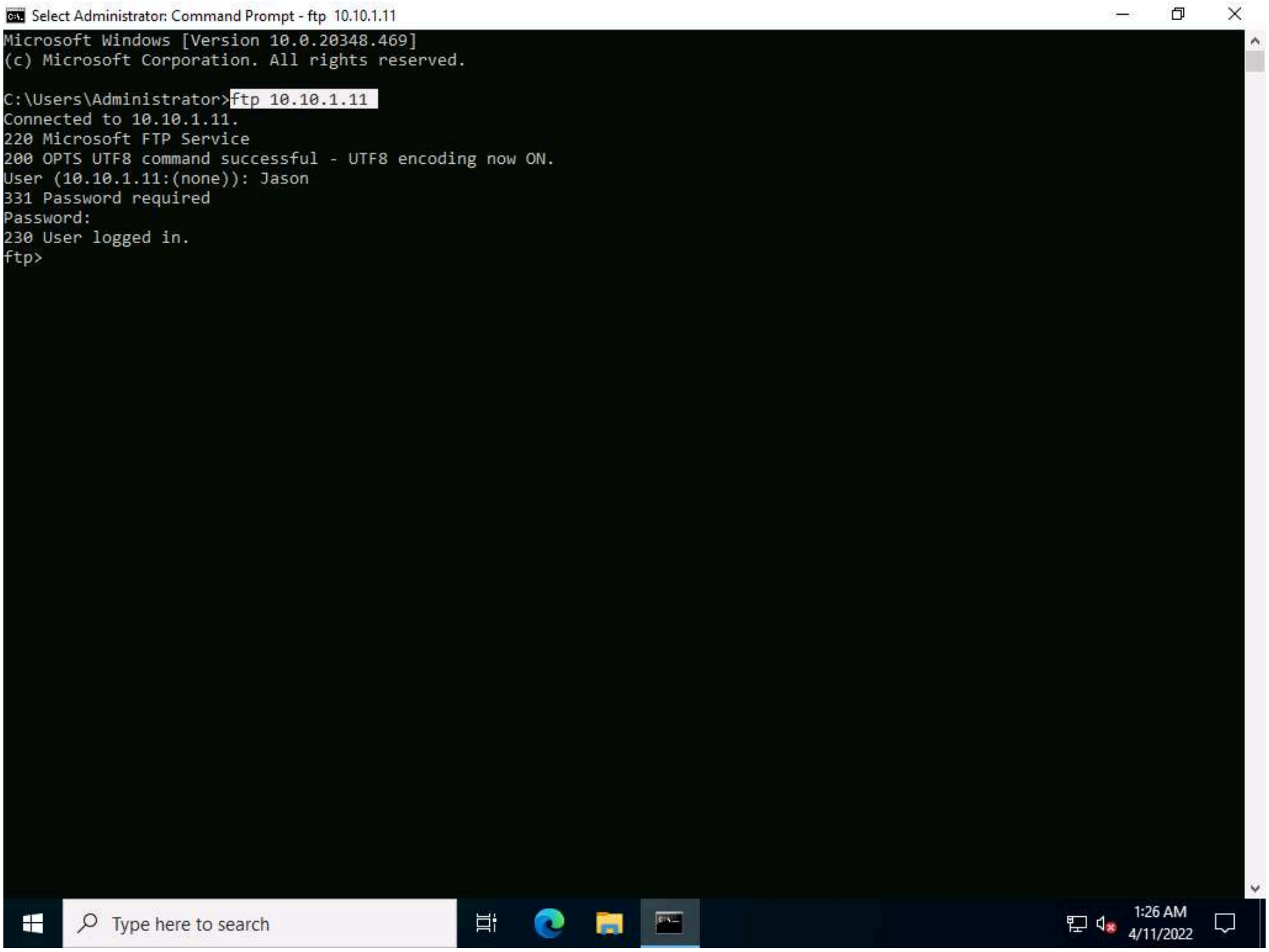
21. Click the **Type here to search** icon at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.



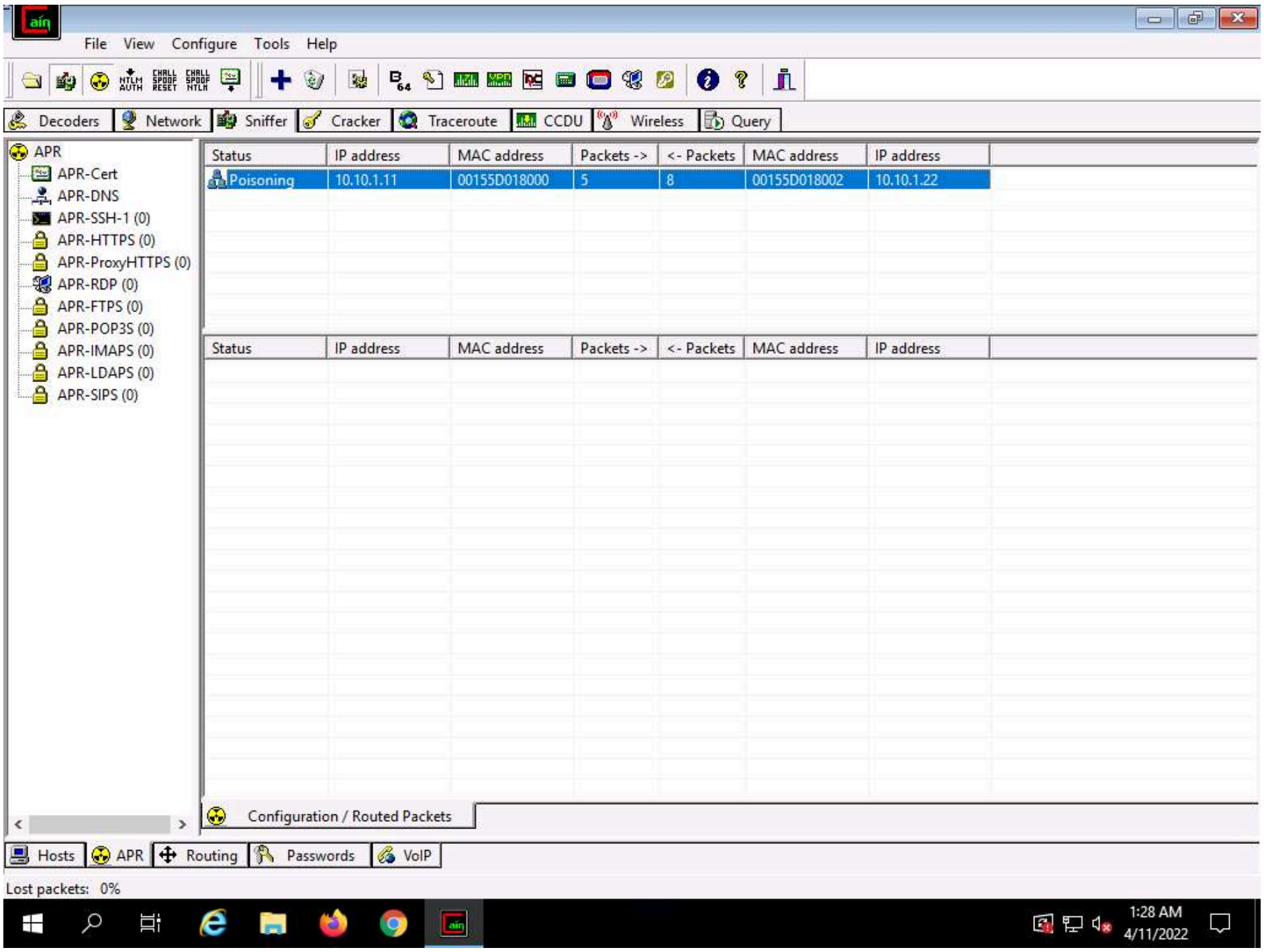
22. The **Command Prompt** window appears; type **ftp 10.10.1.11** (the IP address of **Windows 11**) and press **Enter**.

23. When prompted for a **User**, type "**Jason**" and press **Enter**; for a **Password**, type "**qwerty**" and press **Enter**.

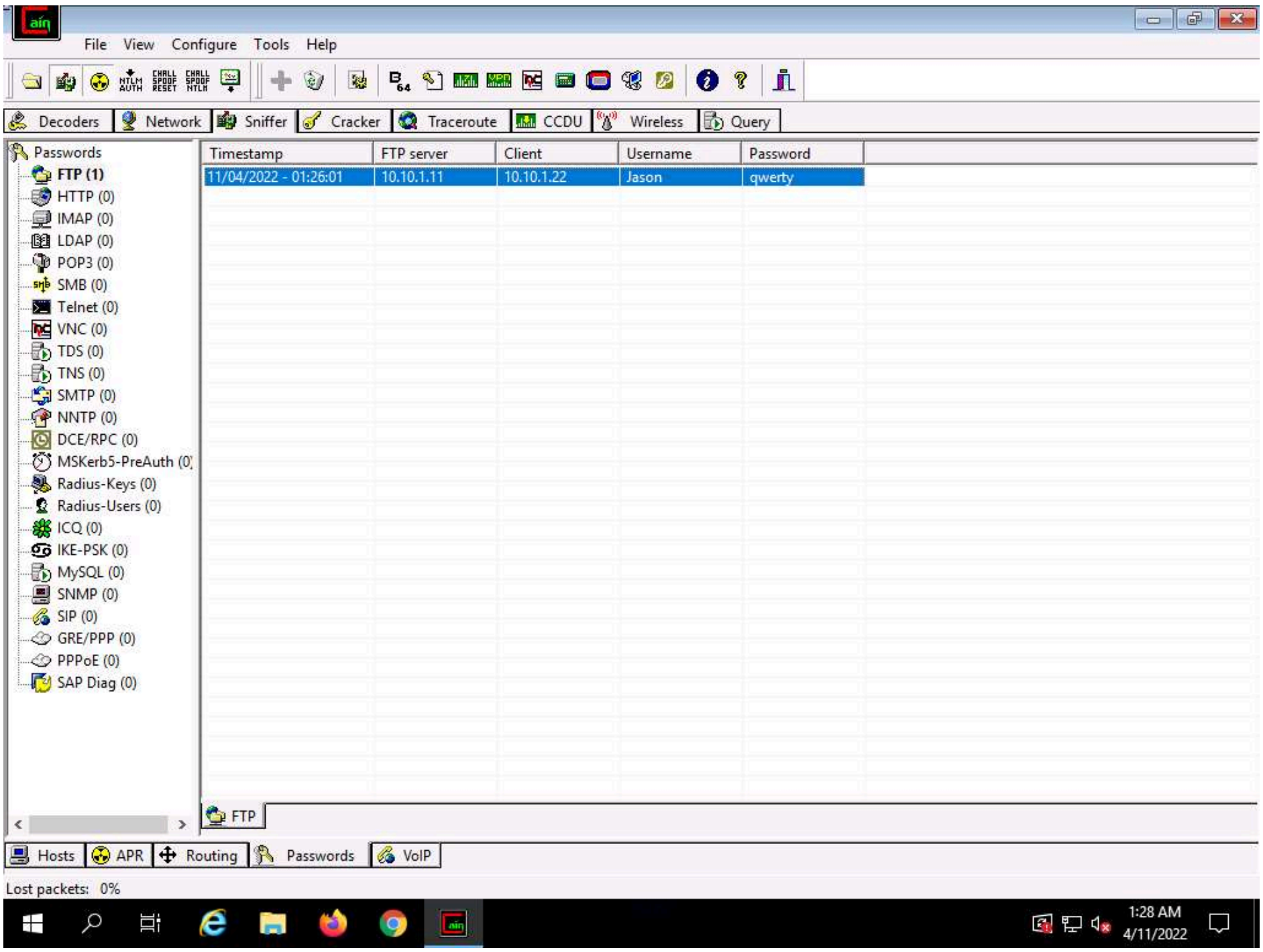
Note: Irrespective of a successful login, Cain & Abel captures the password entered during login.



24. Click **CEHv12 Windows Server 2019** to switch back to the **Windows Server 2019** machine; observe that the tool lists packet exchange.



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



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

26. This concludes the demonstration of how to perform an MITM attack using Cain & Abel.

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

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.

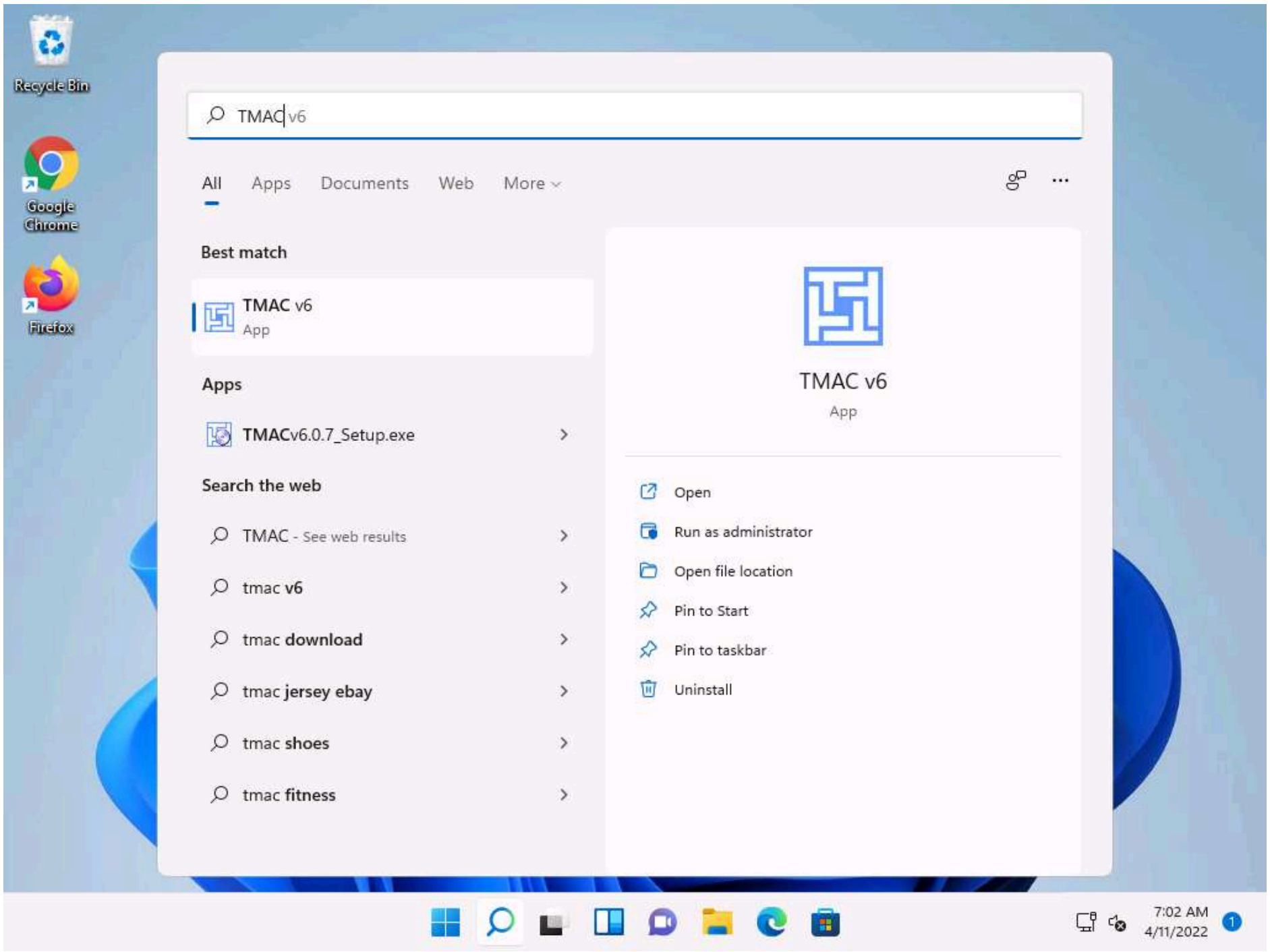
Here, we will use TMAC and SMAC tools to perform MAC spoofing.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

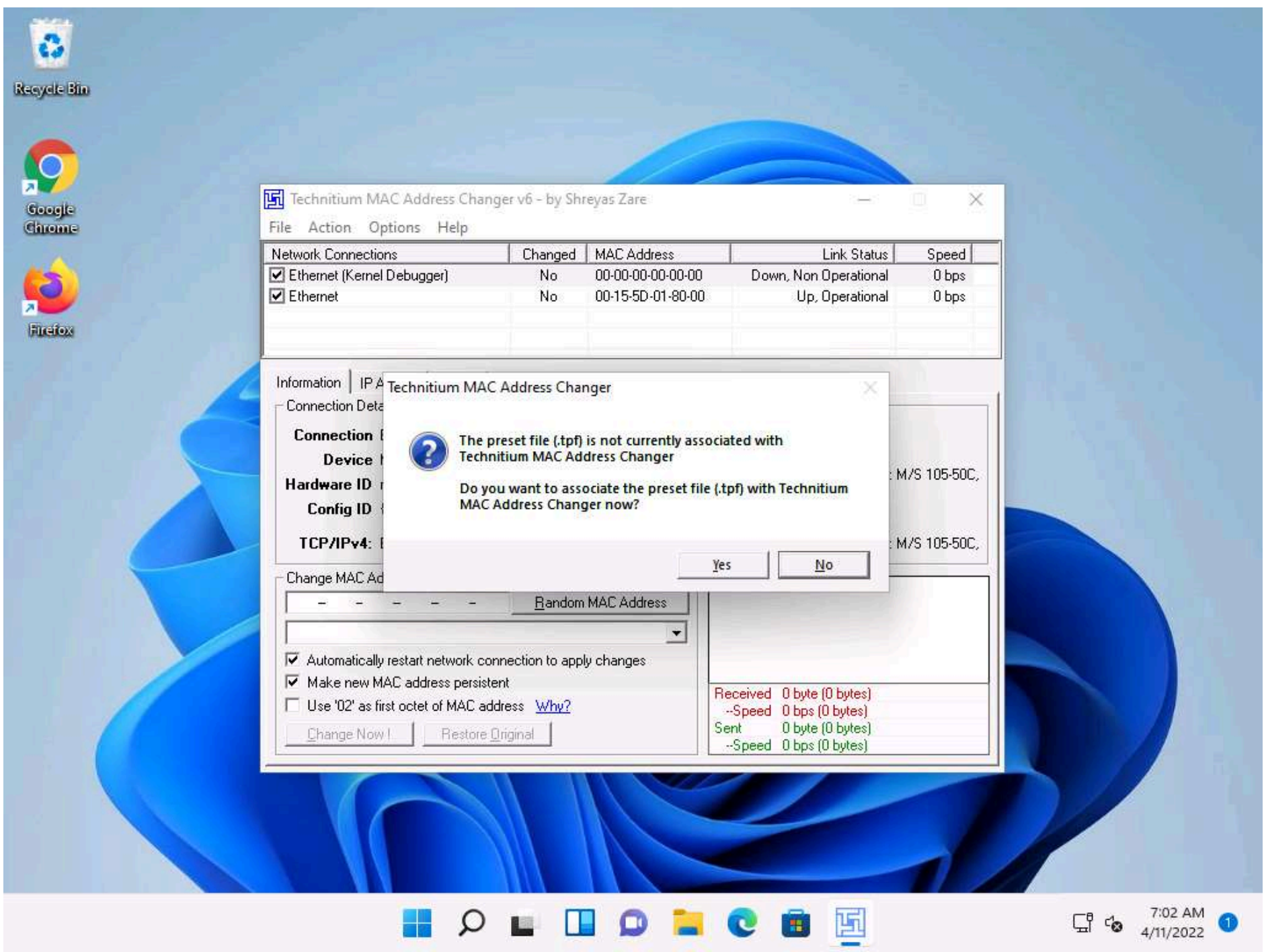
> Note: If a **User Account Control** pop-up appears, click **Yes**.

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

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

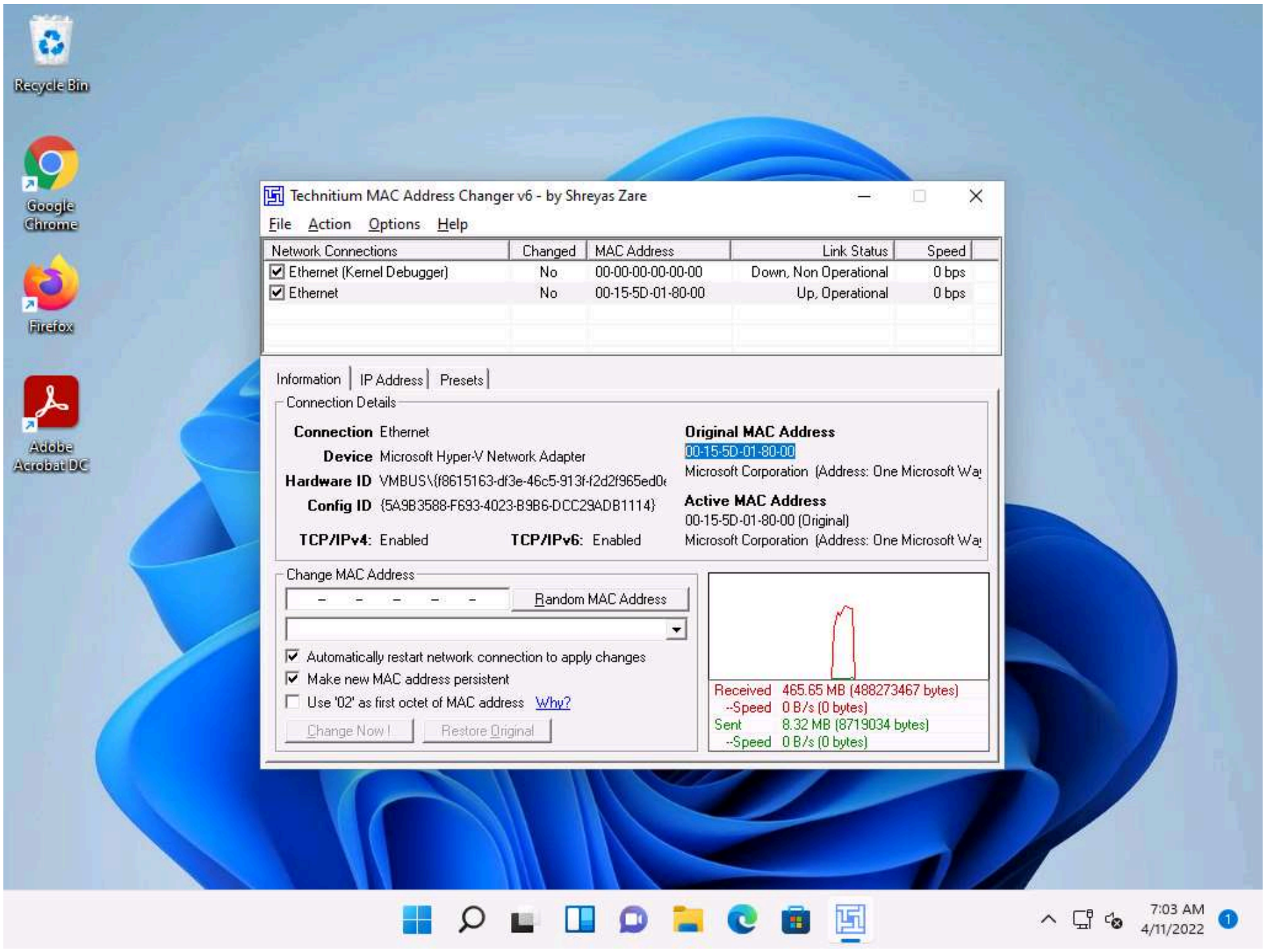


3. The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.

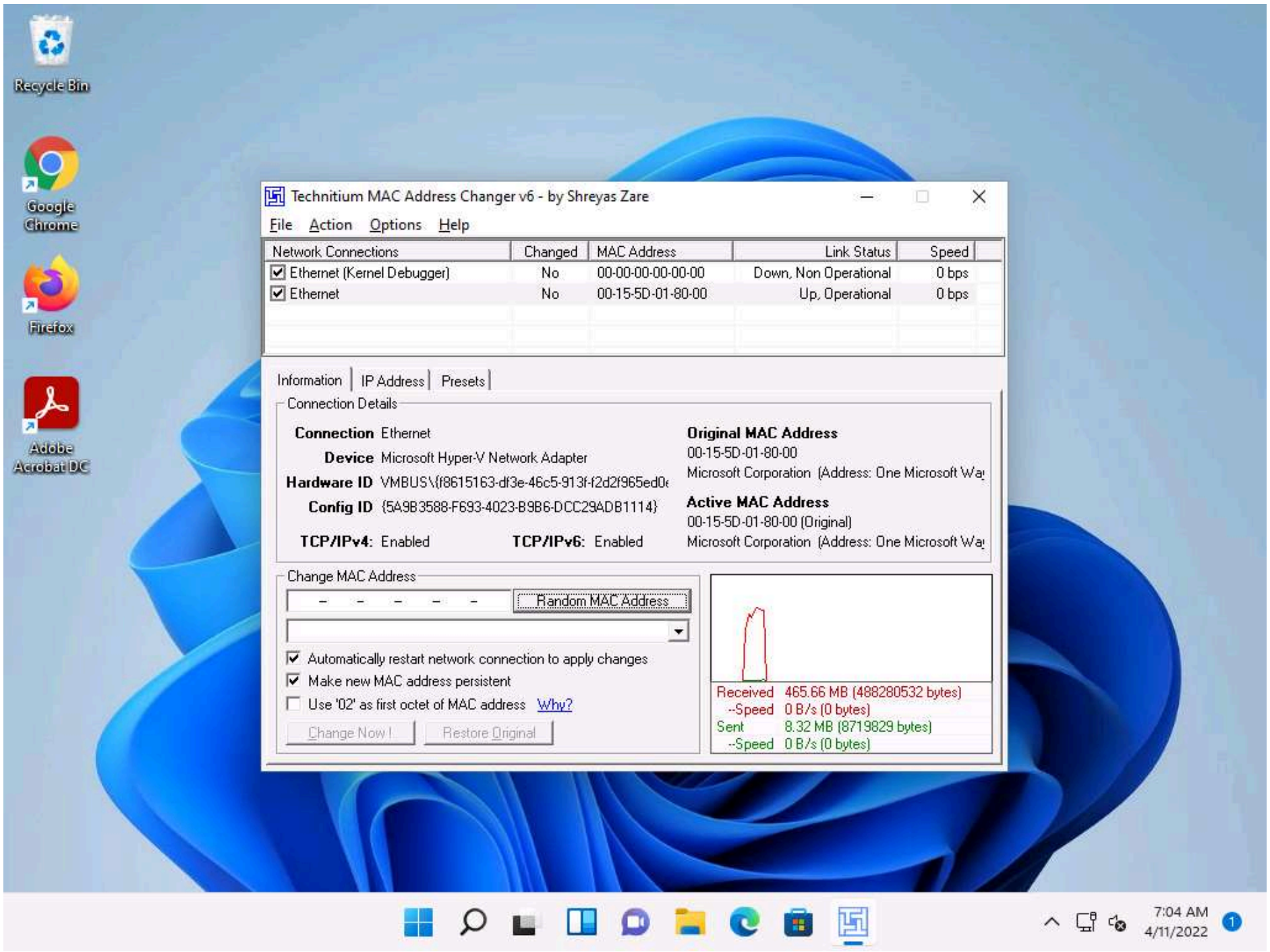


4. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet**).

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

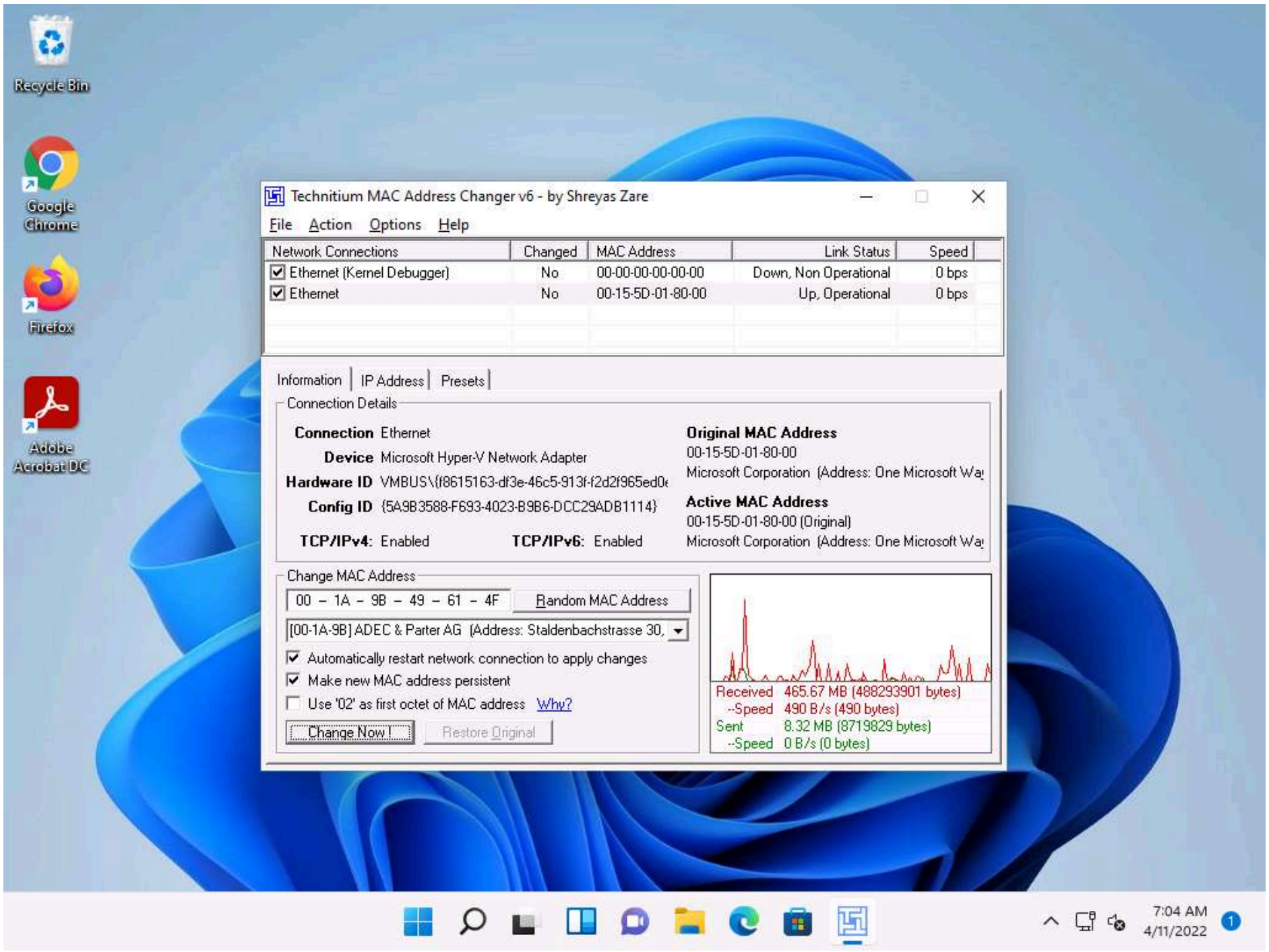


6. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

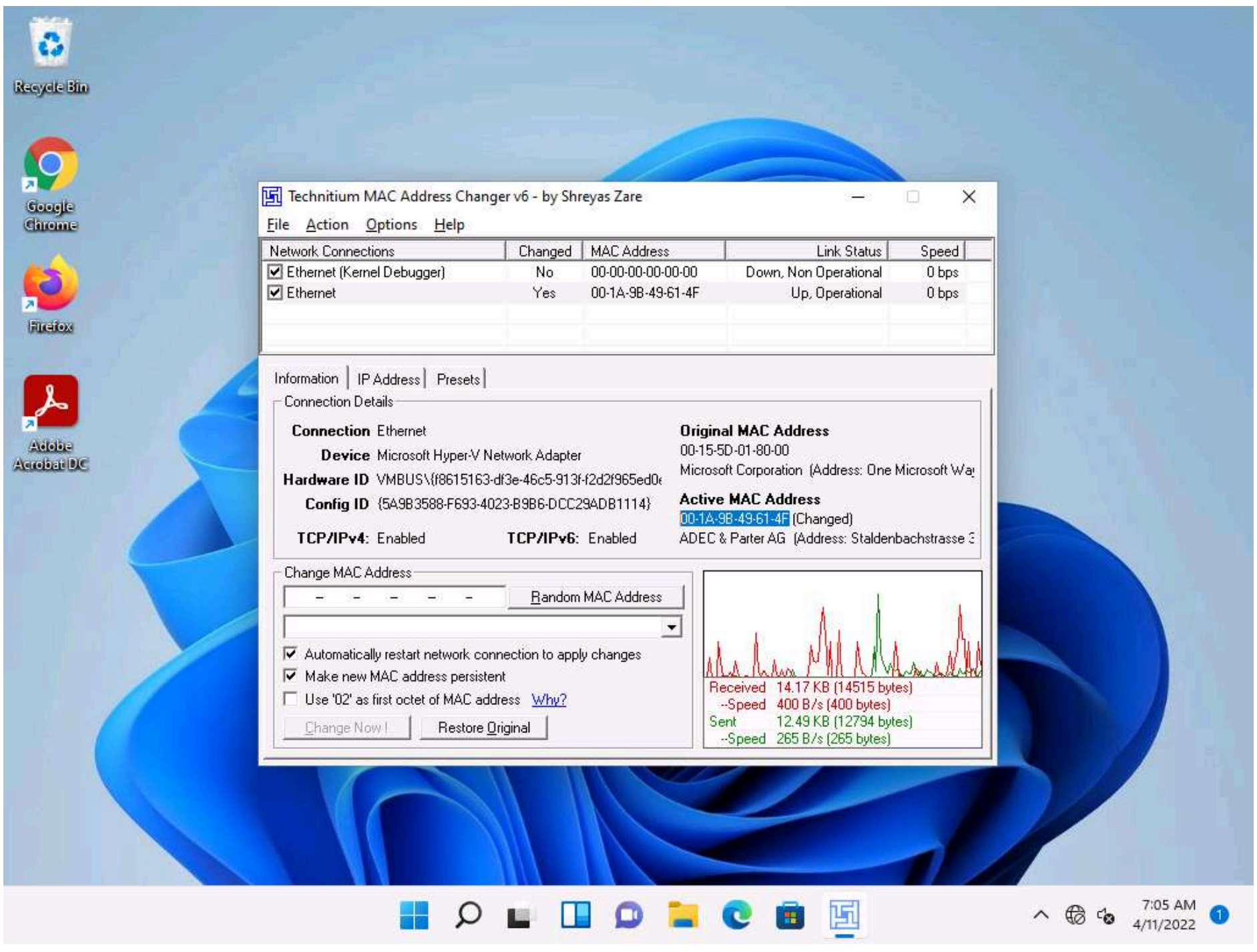


7. A **Random MAC Address** is generated and appears under the **Change MAC Address** field. Click the **Change Now !** button to change the MAC address.

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

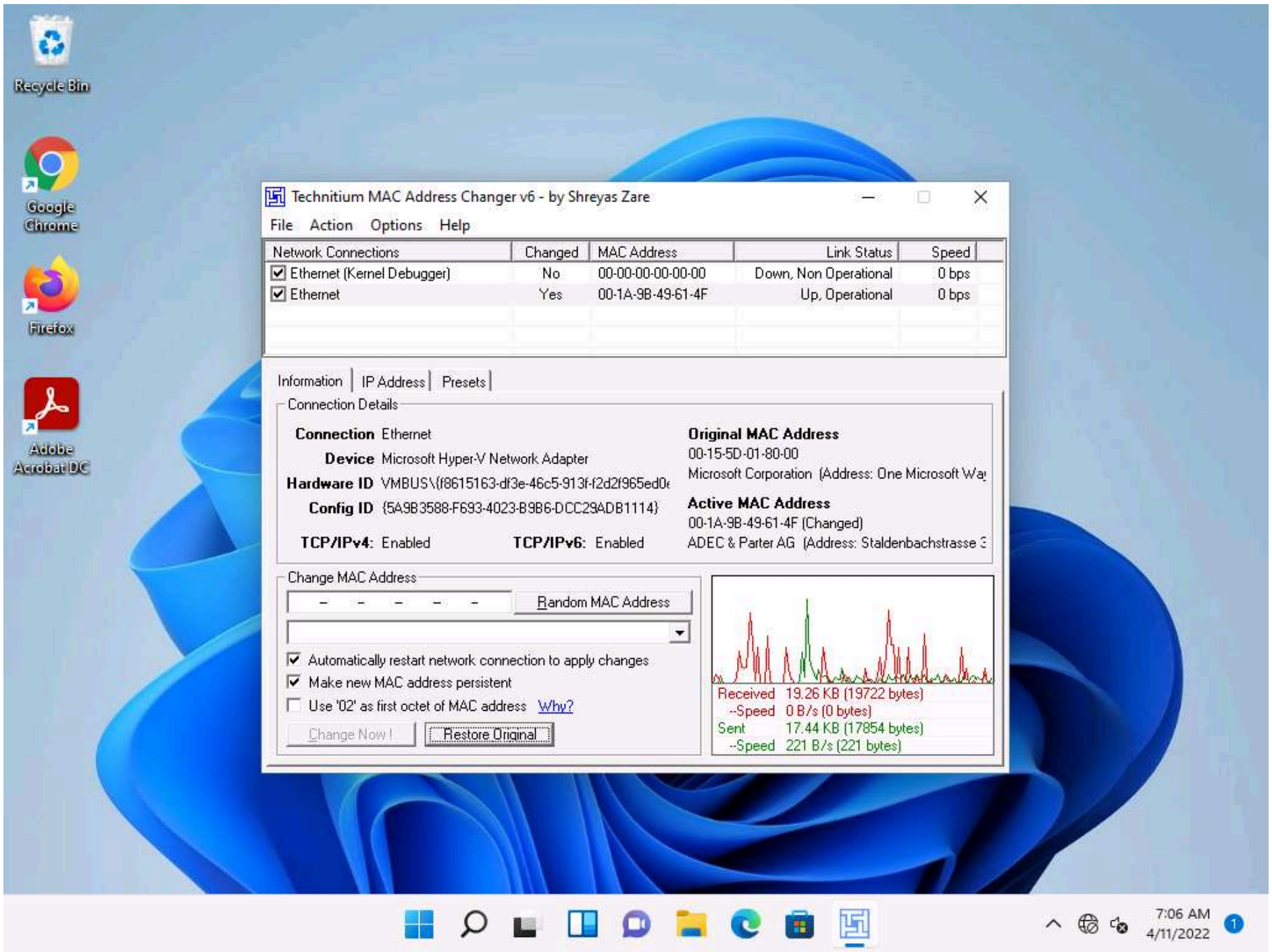


8. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.



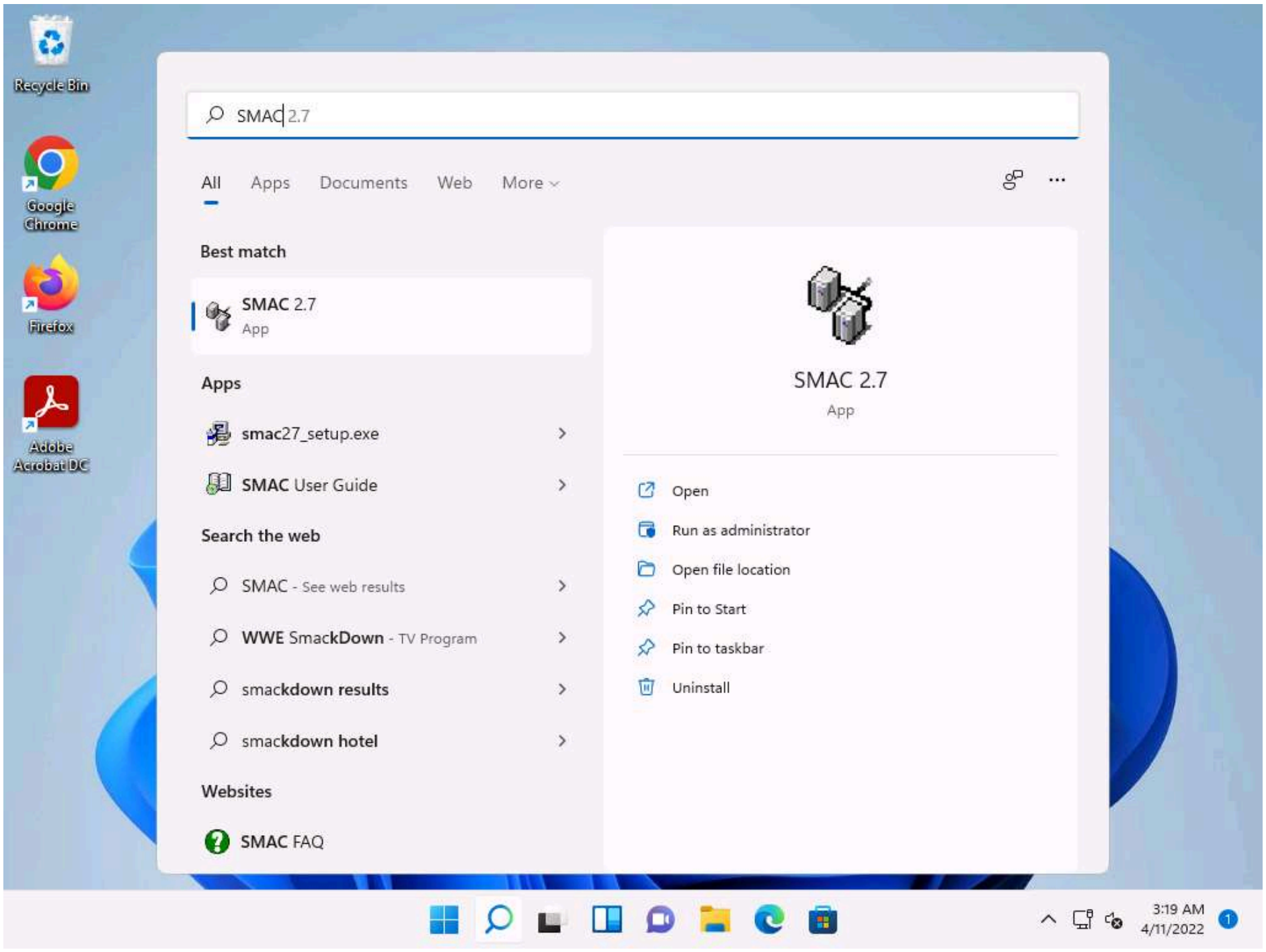
9. To restore the original MAC address, you can click on the **Restore Original** button present at the bottom of the TMAC window.

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

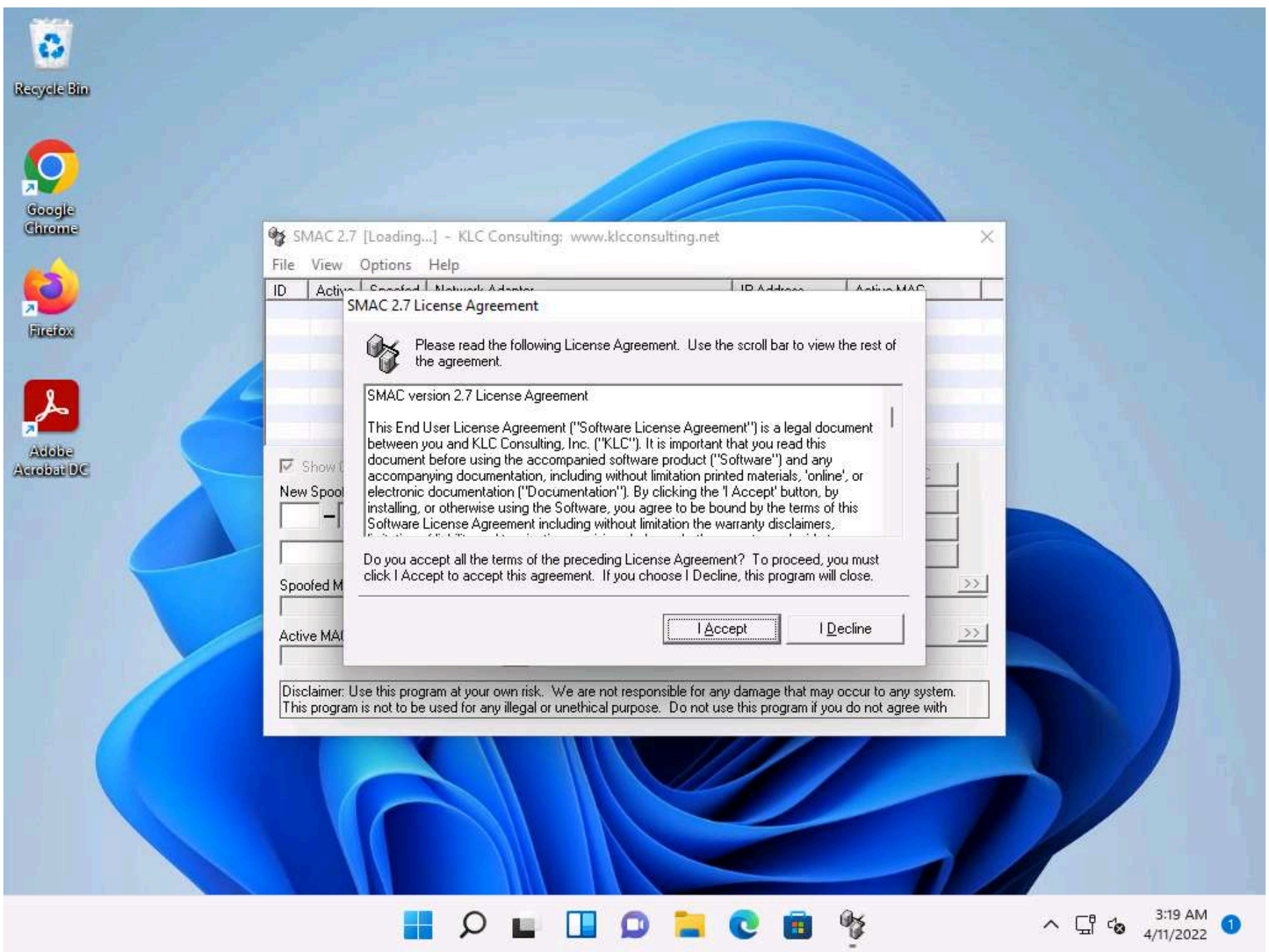


10. Close the **TMAC** main window.
11. Now, we shall perform MAC spoofing using the SMAC tool.
12. Click **Search** icon ( ) on the **Desktop**. Type **SMAC** in the search field, the **SMAC 2.7** appears in the results, click **Open** to launch it.

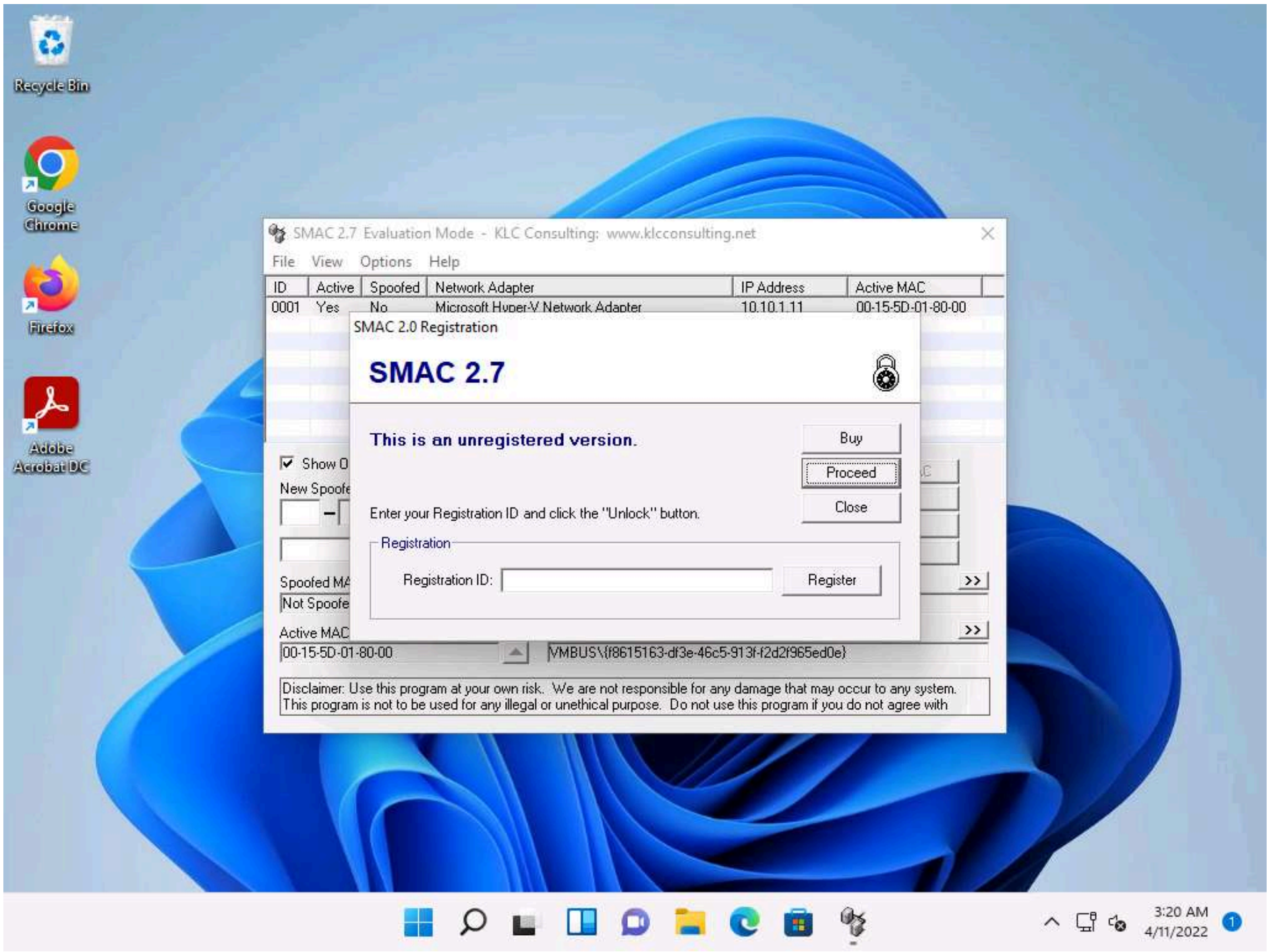
Note: If a **User Account Control** pop-up appears, click **Yes**.



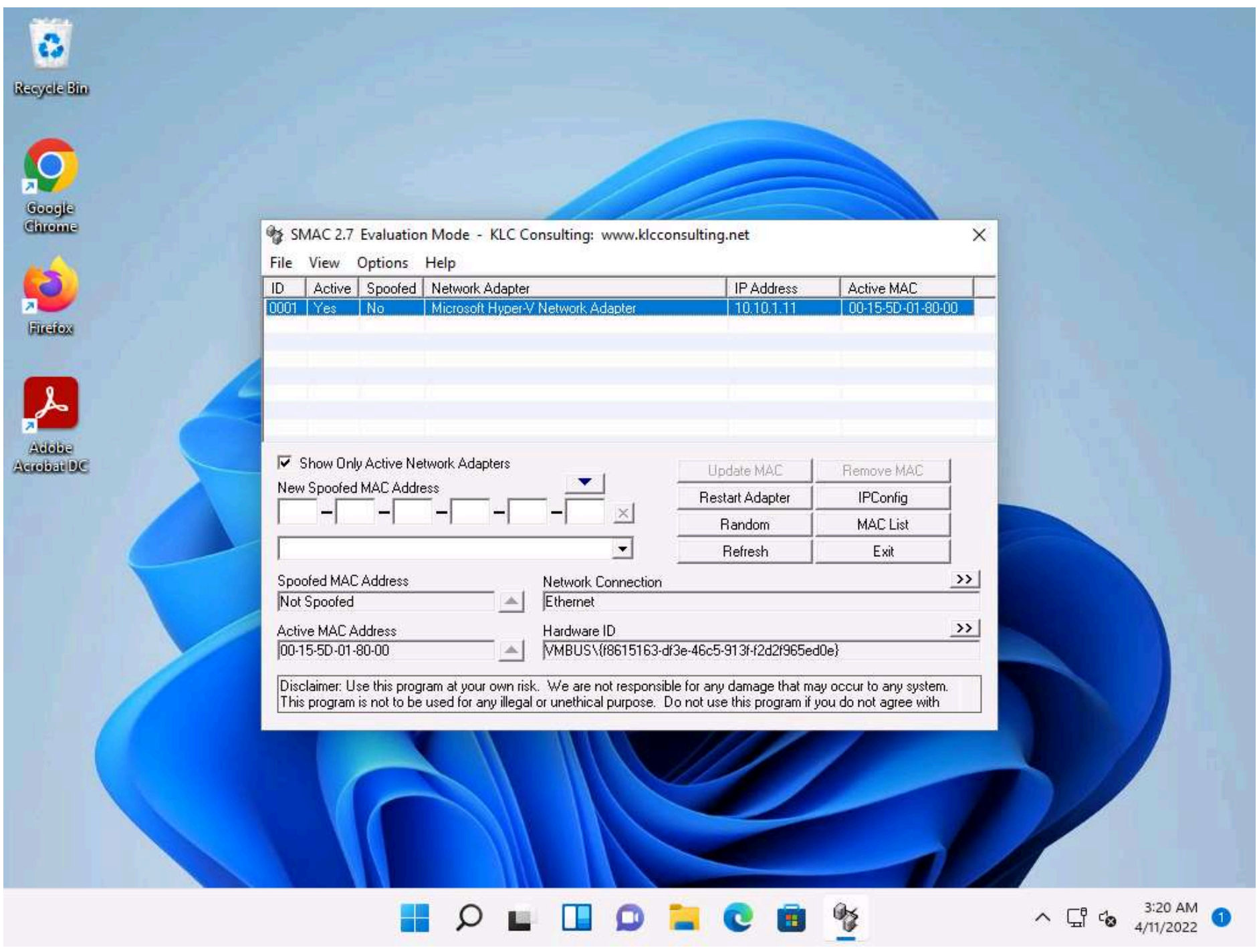
13. The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.



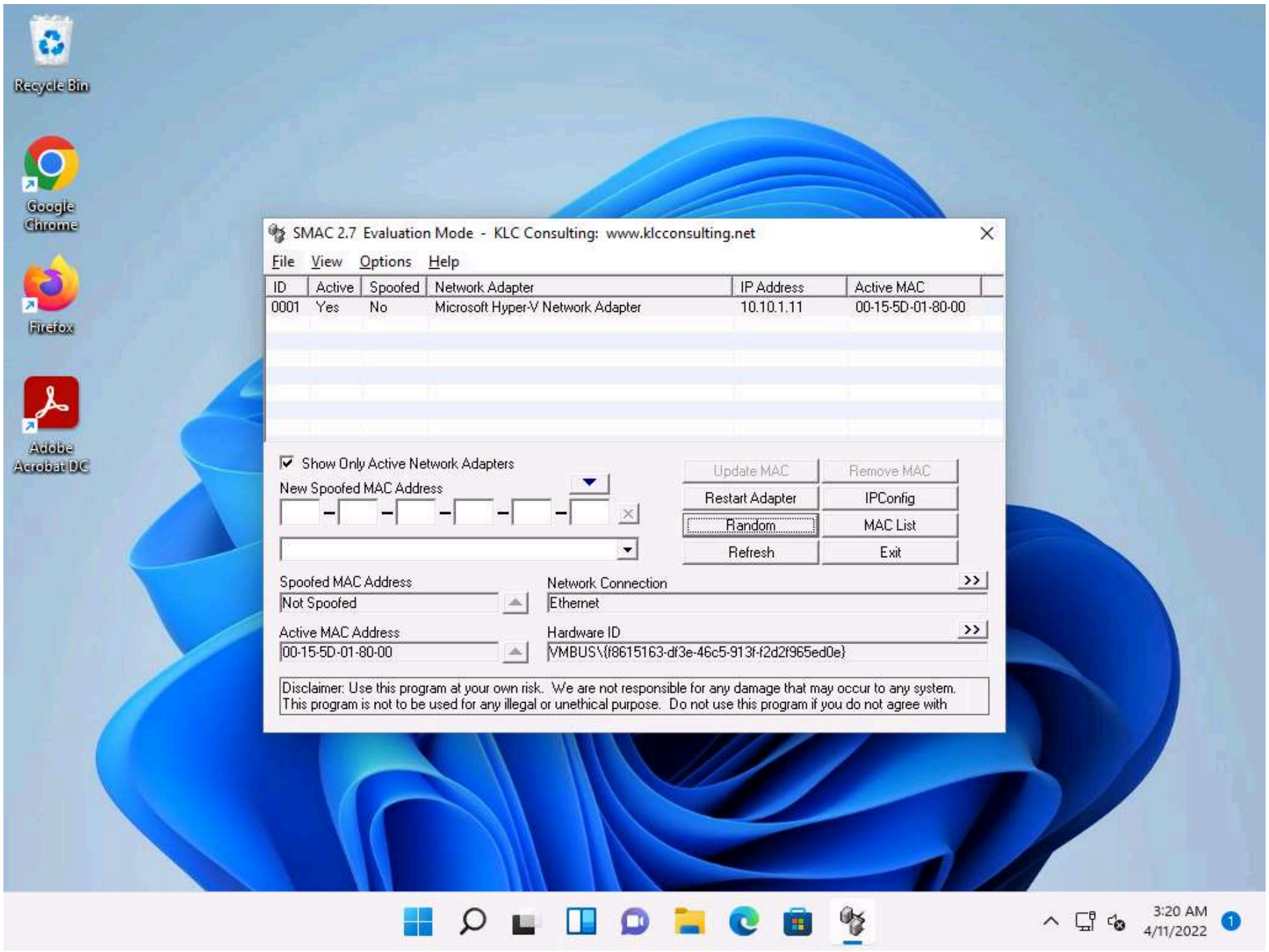
14. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.



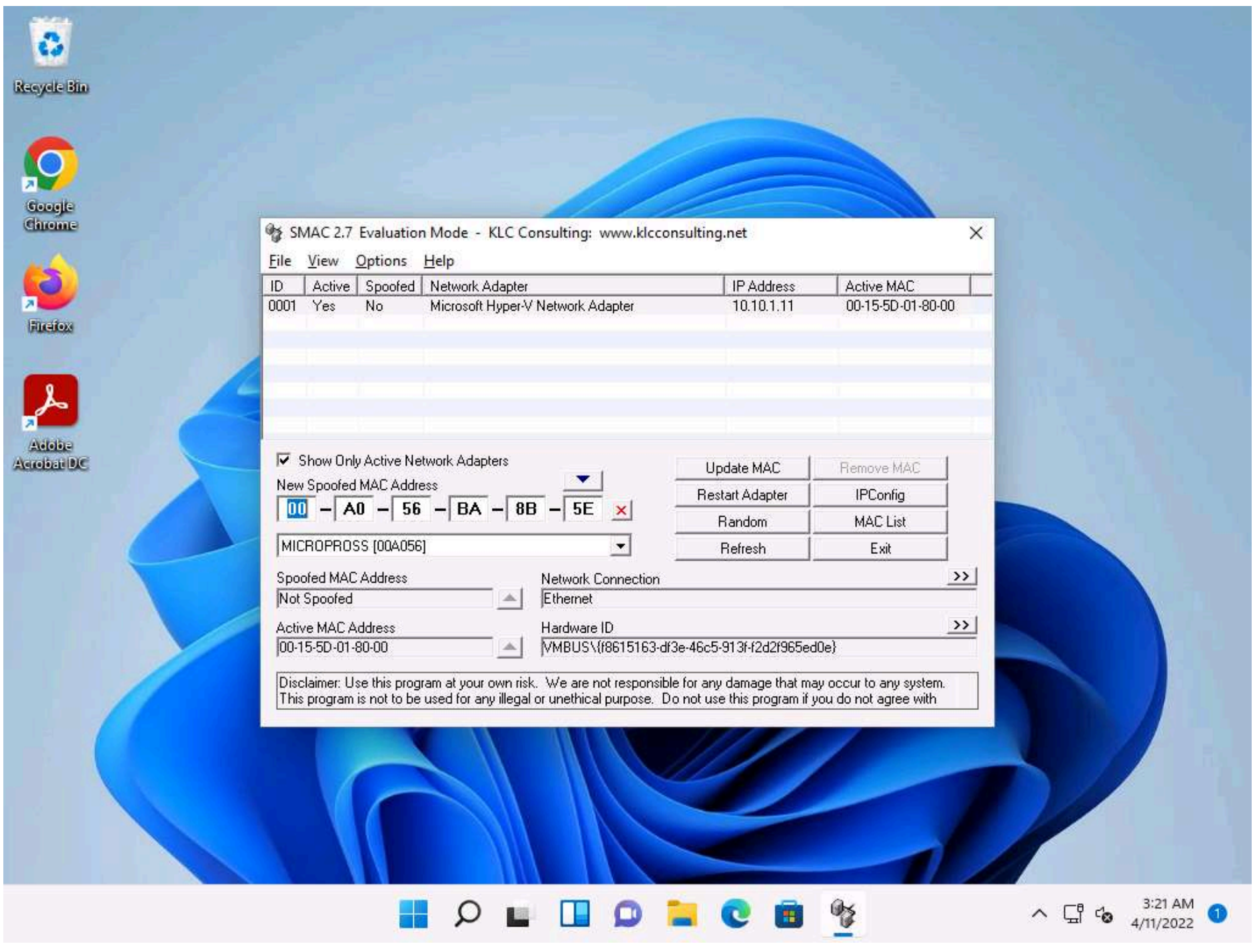
15. The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.



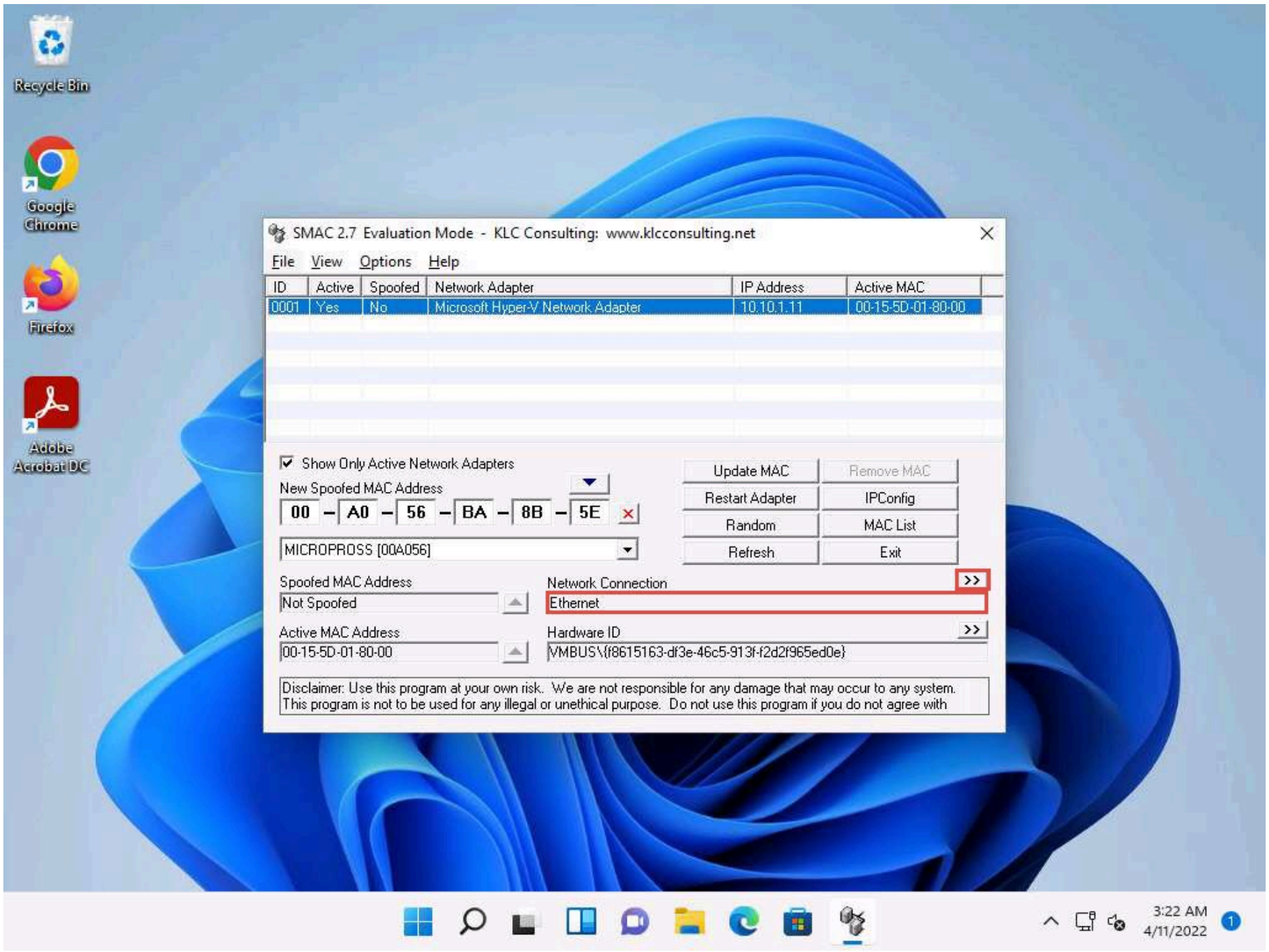
16. Click the **Random** button to generate a random MAC address.



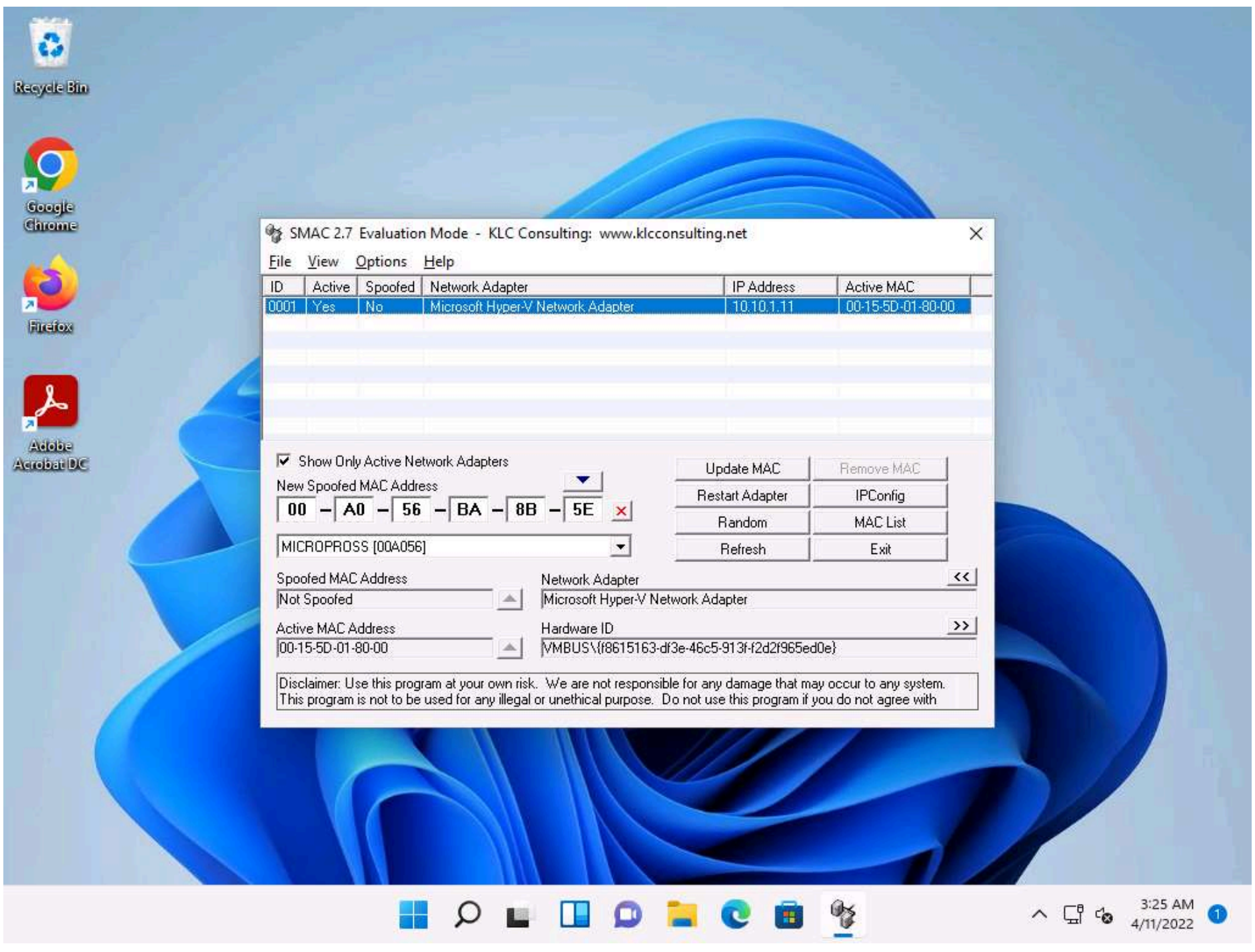
17. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.



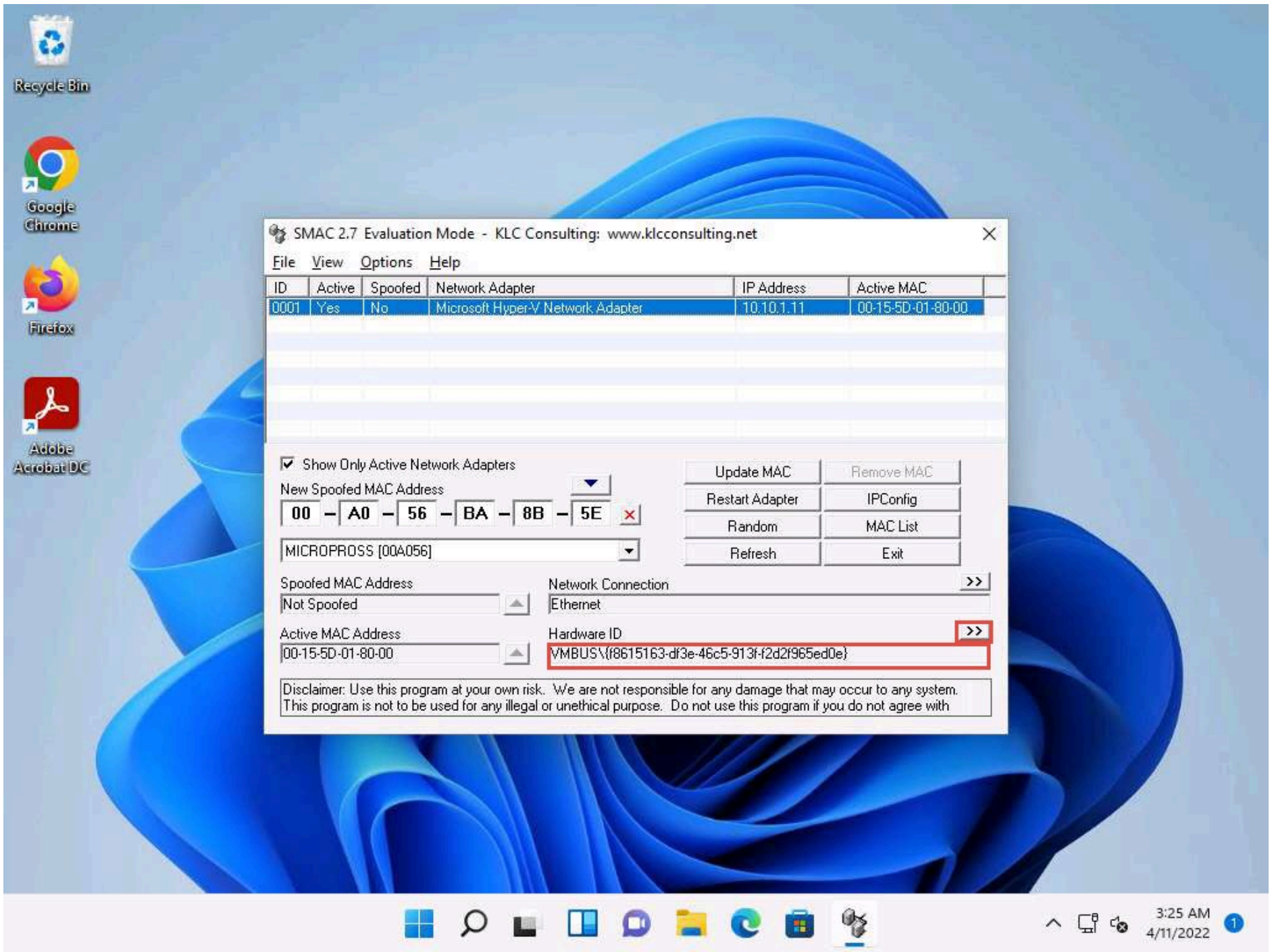
18. Click the forward arrow button (**>>**) under **Network Connection** to view the **Network Adapter** information.



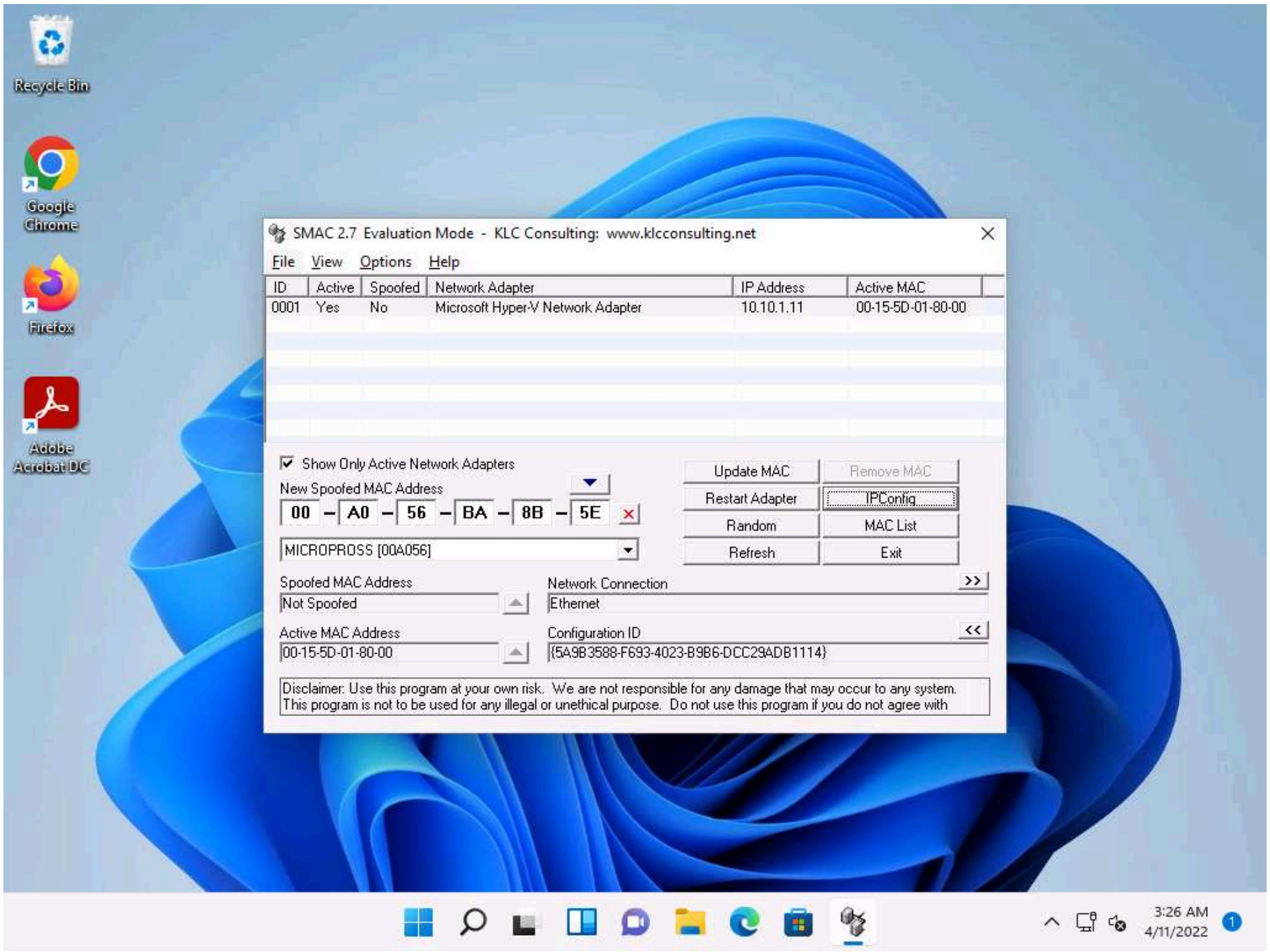
19. Clicking the back arrow (<<) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.



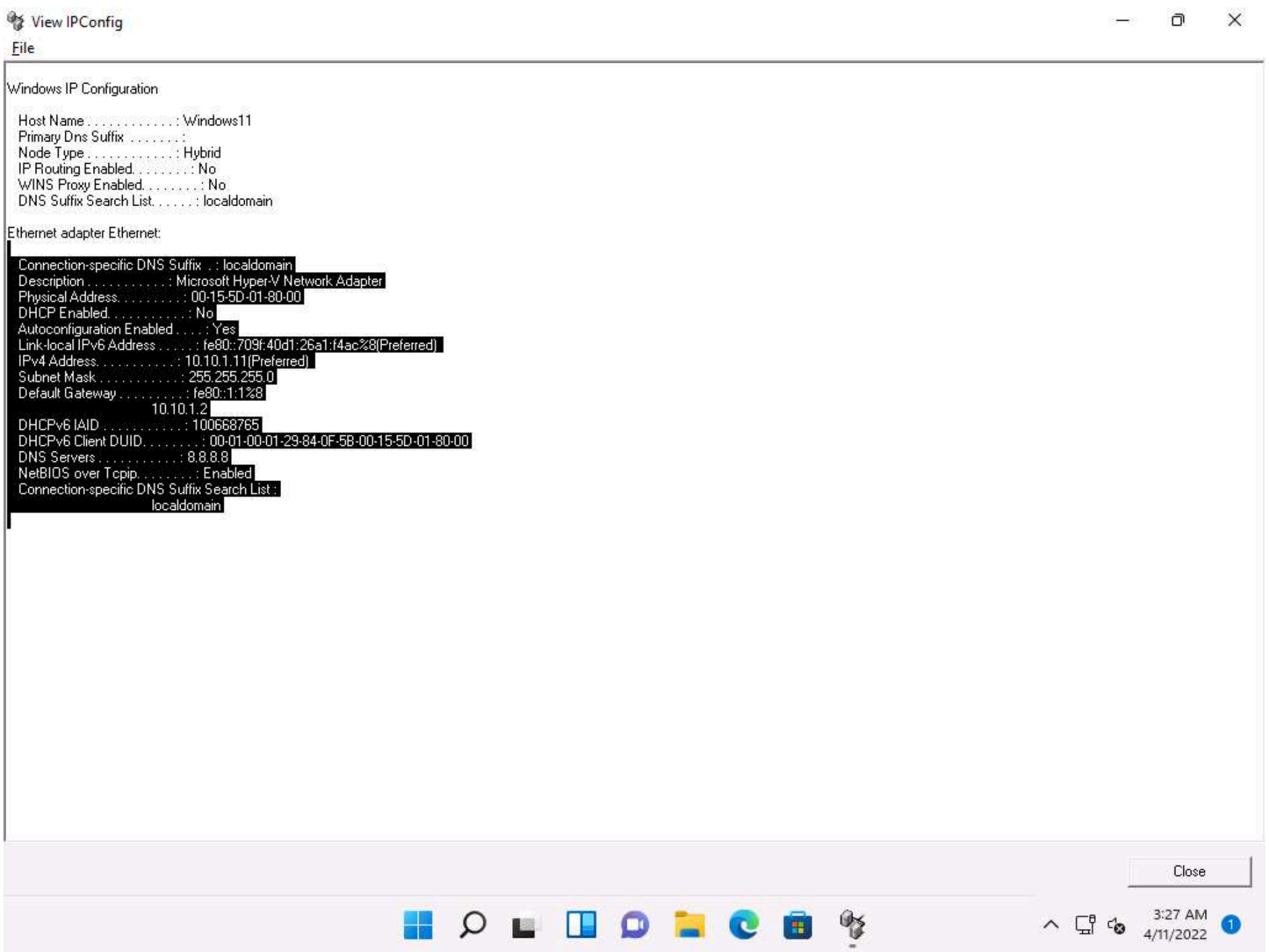
20. Similarly, you can click the forward arrow button (**>>**) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (**<<**) to toggle back to **Hardware ID** information.



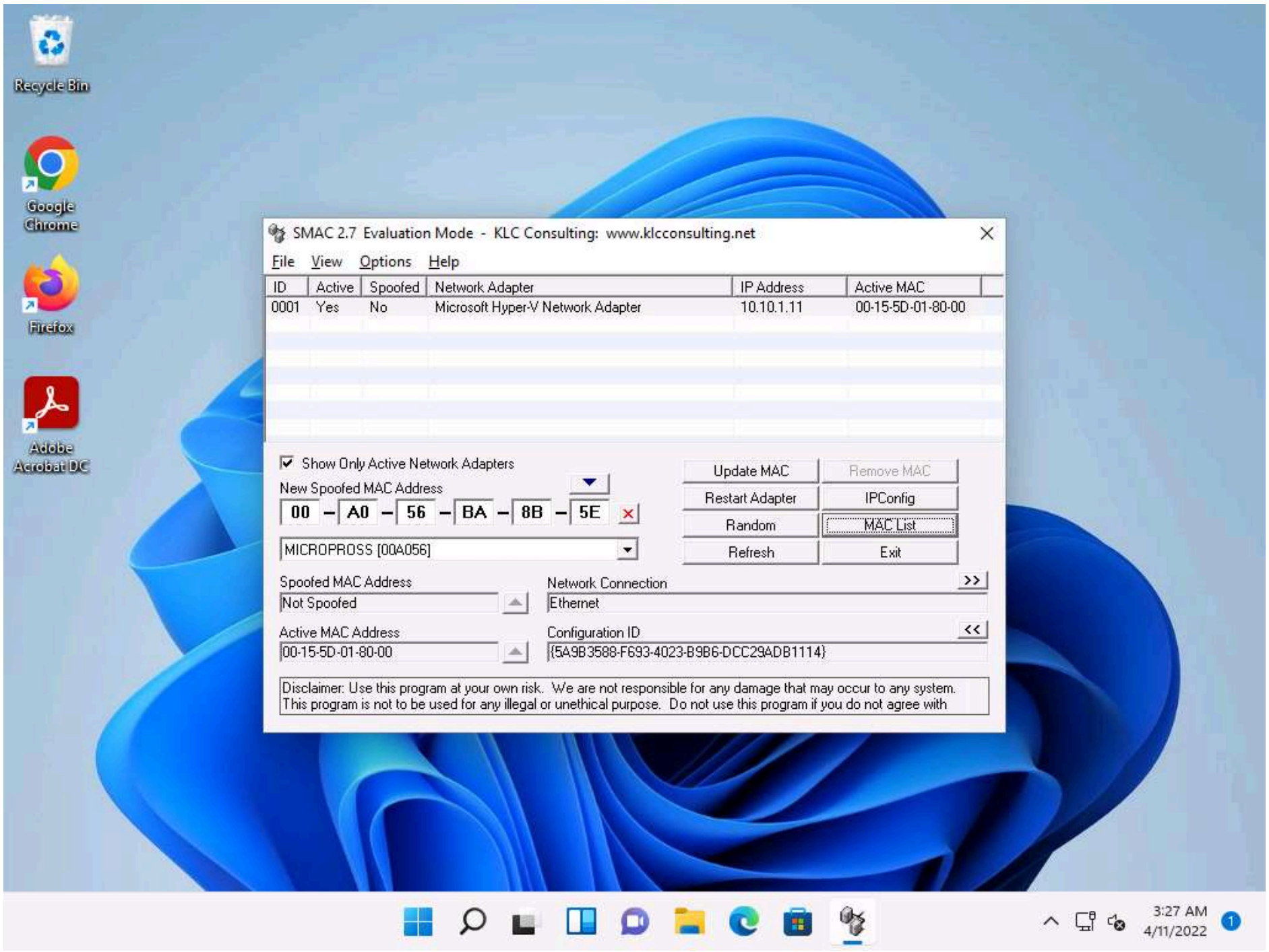
21. Click the **IPConfig** button to view the ipconfig information.



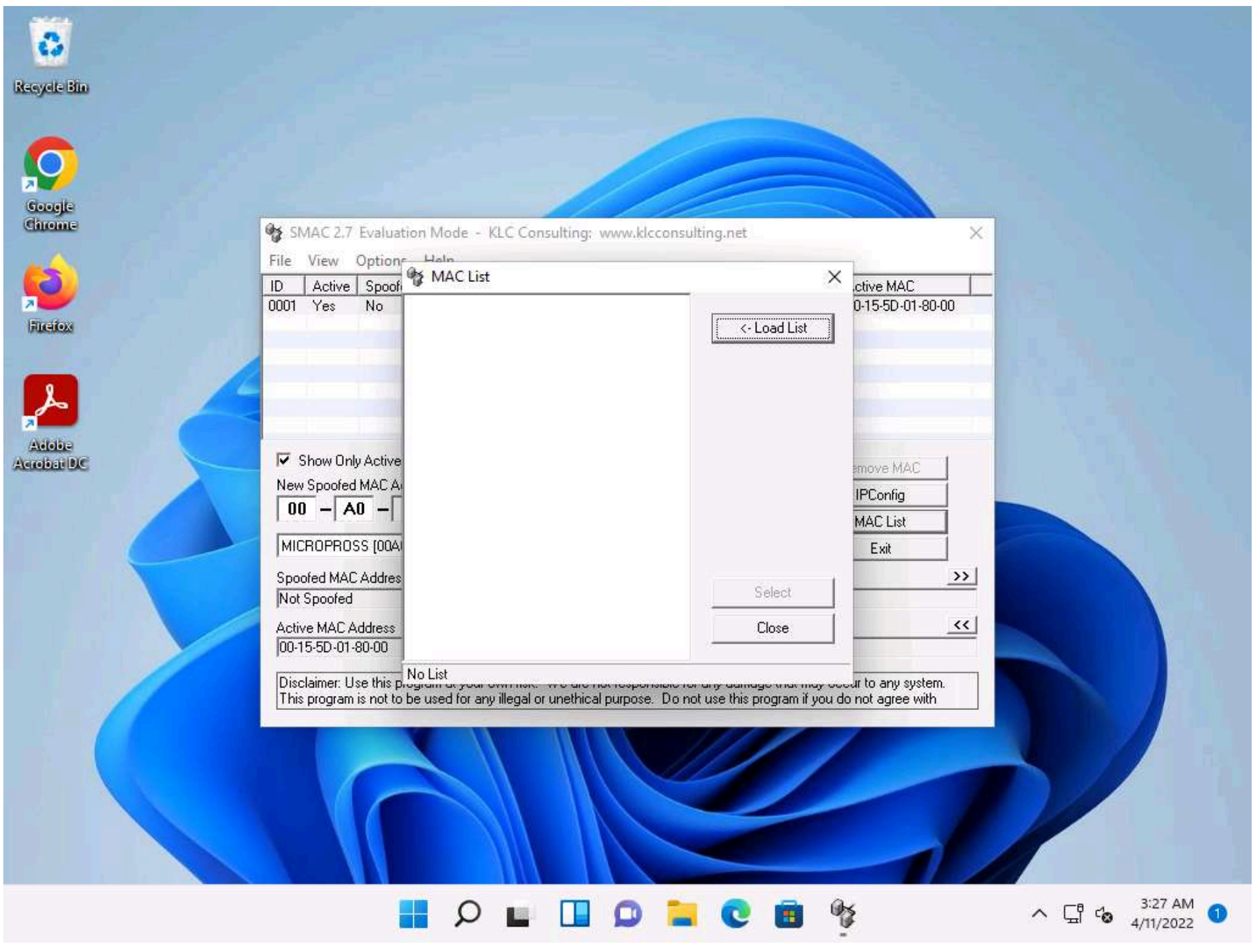
22. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.



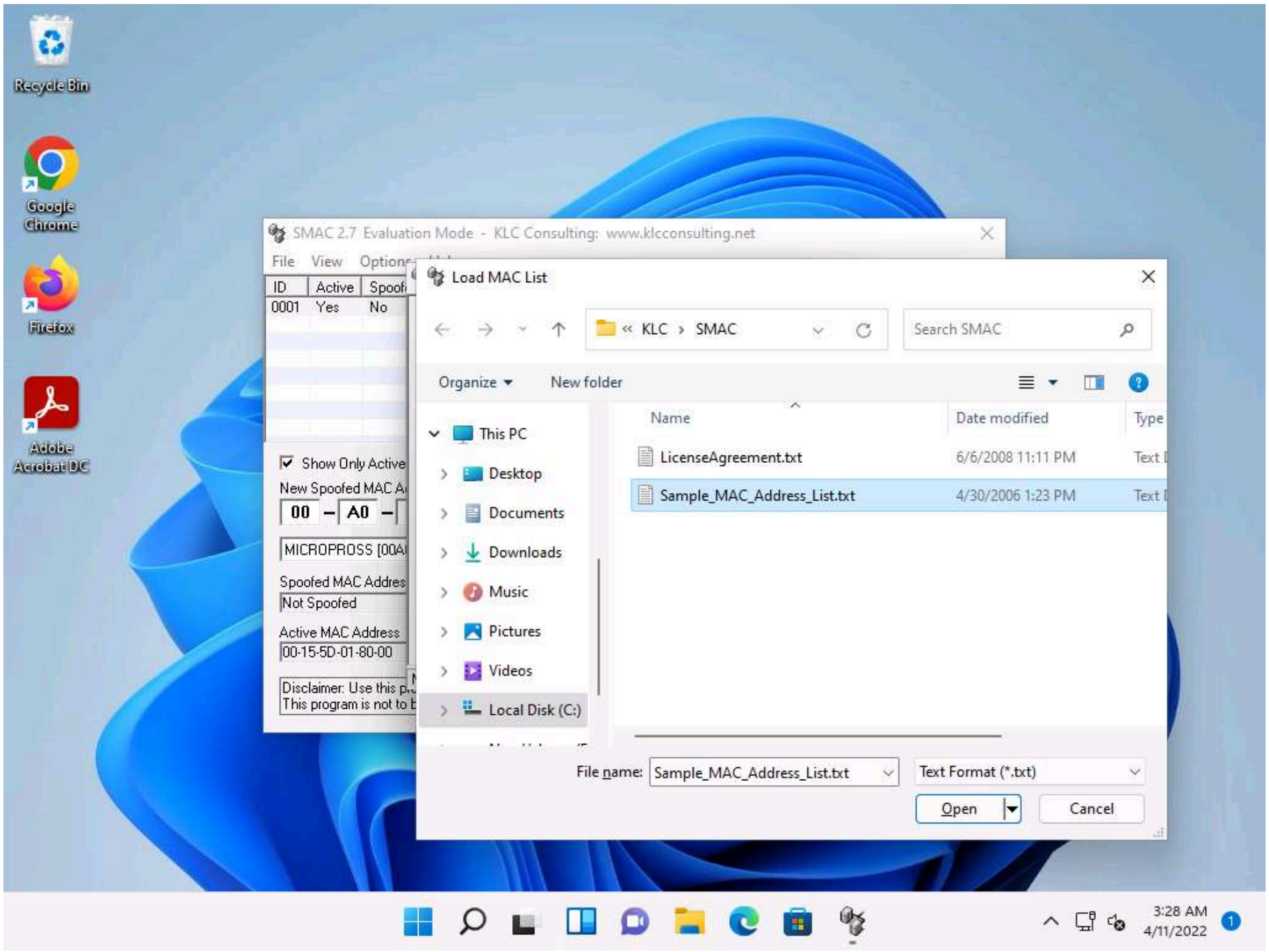
23. Click the **MAC List** button to import the MAC address list into SMAC.



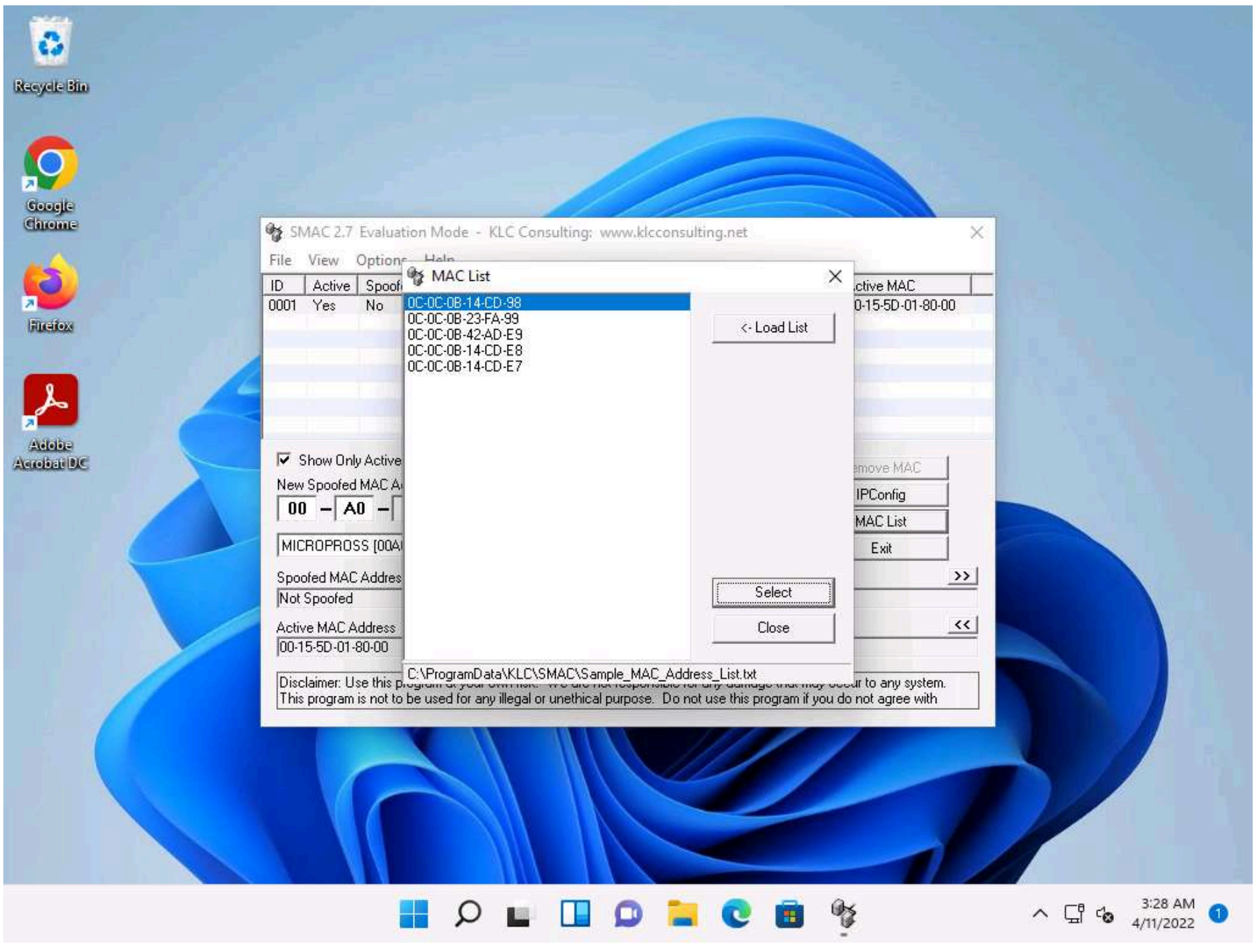
24. The **MAC List** window appears; click the **Load List** button.



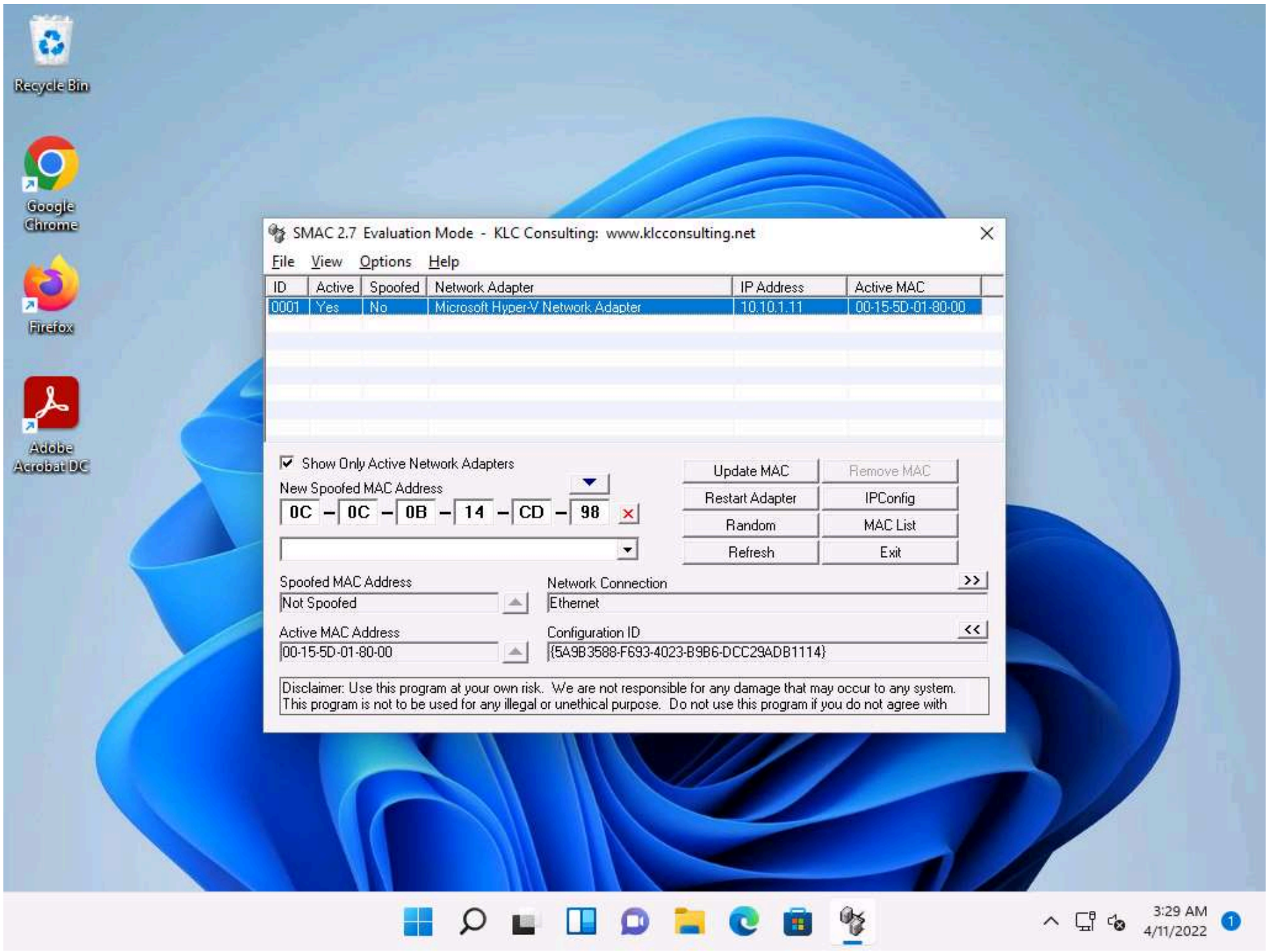
25. The **Load MAC List** window appears; select the **Sample_MAC_Address_List.txt** file and click **Open**.



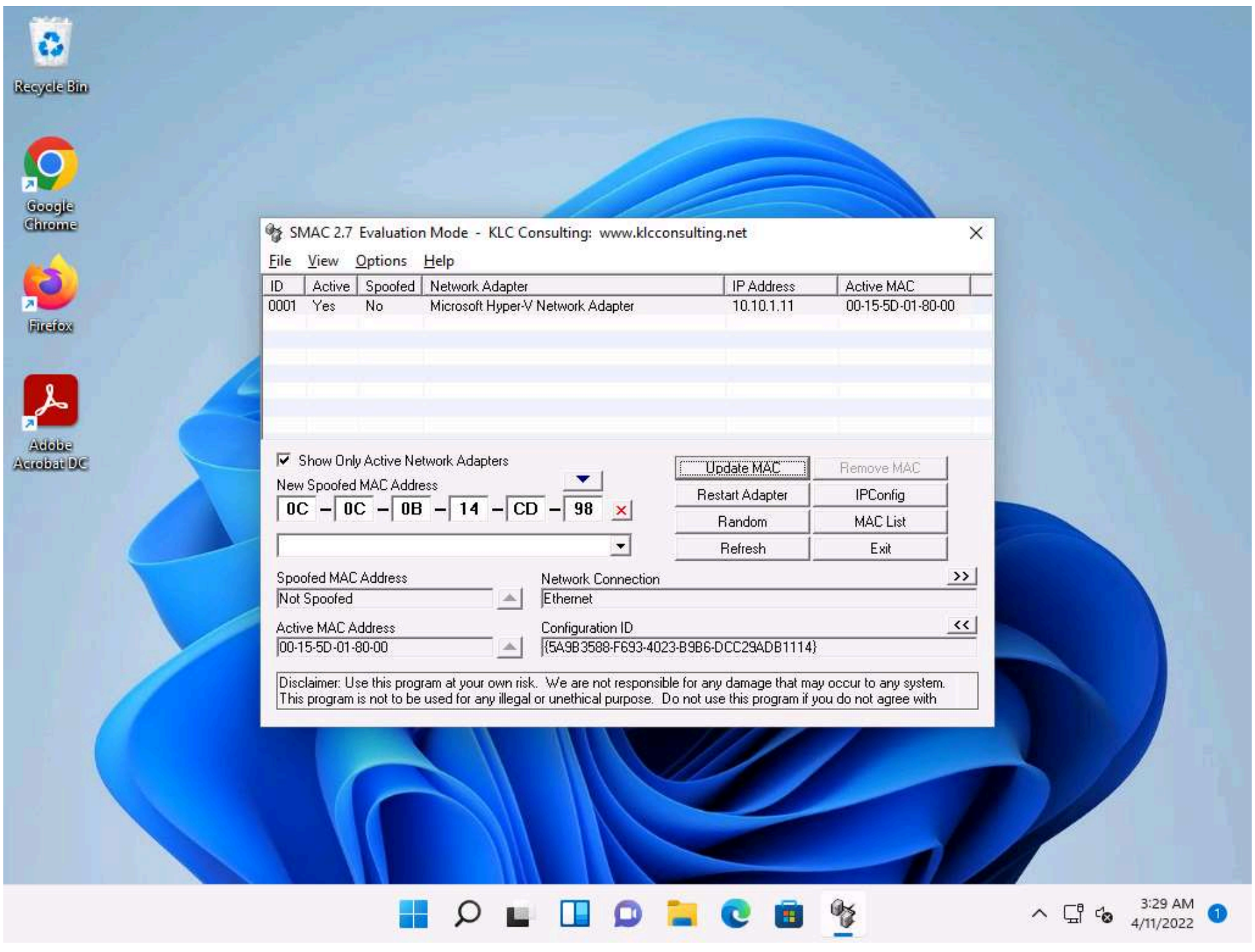
26. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.



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



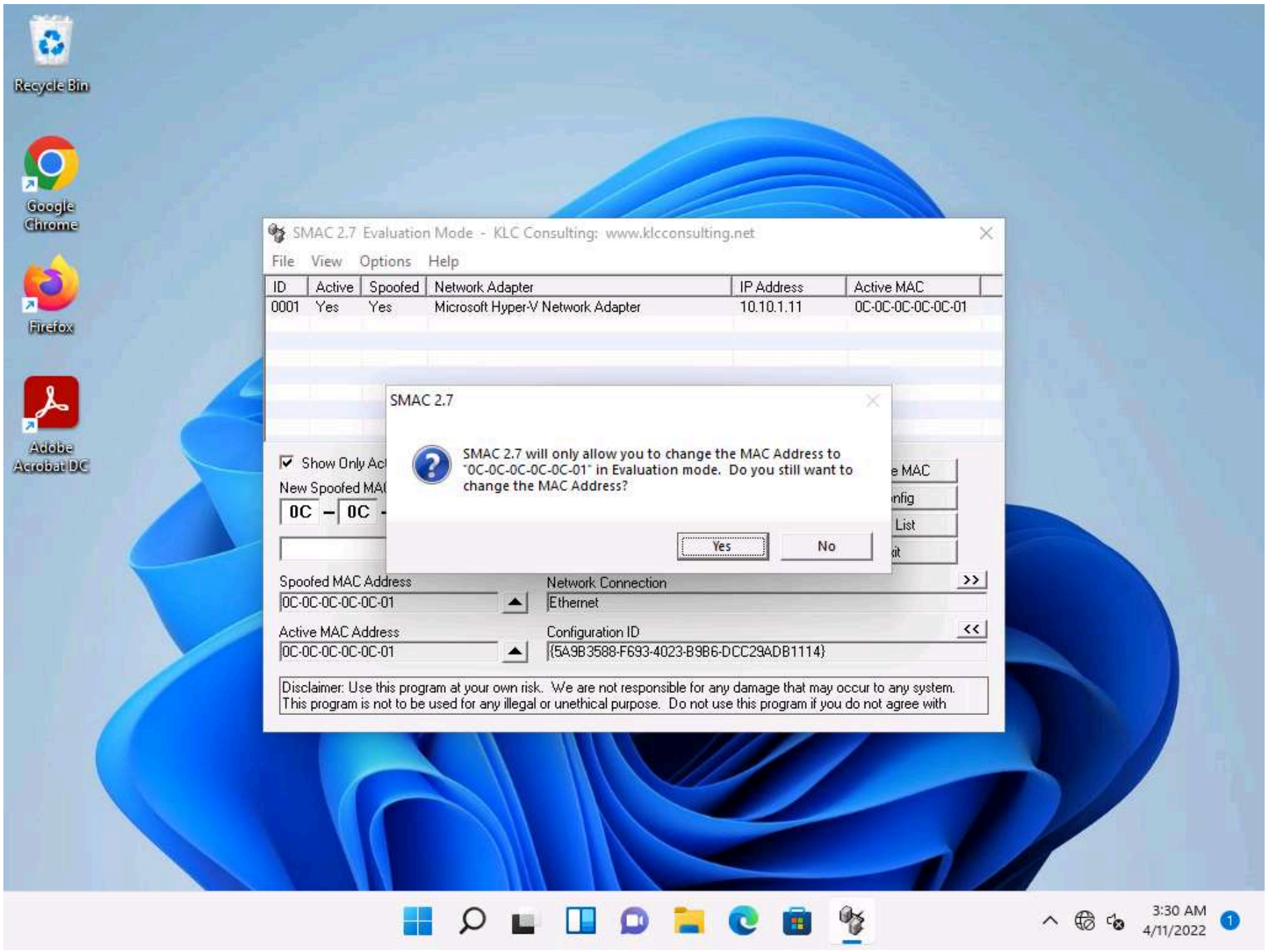
28. Click the **Update MAC** button to update the machine's MAC address information.



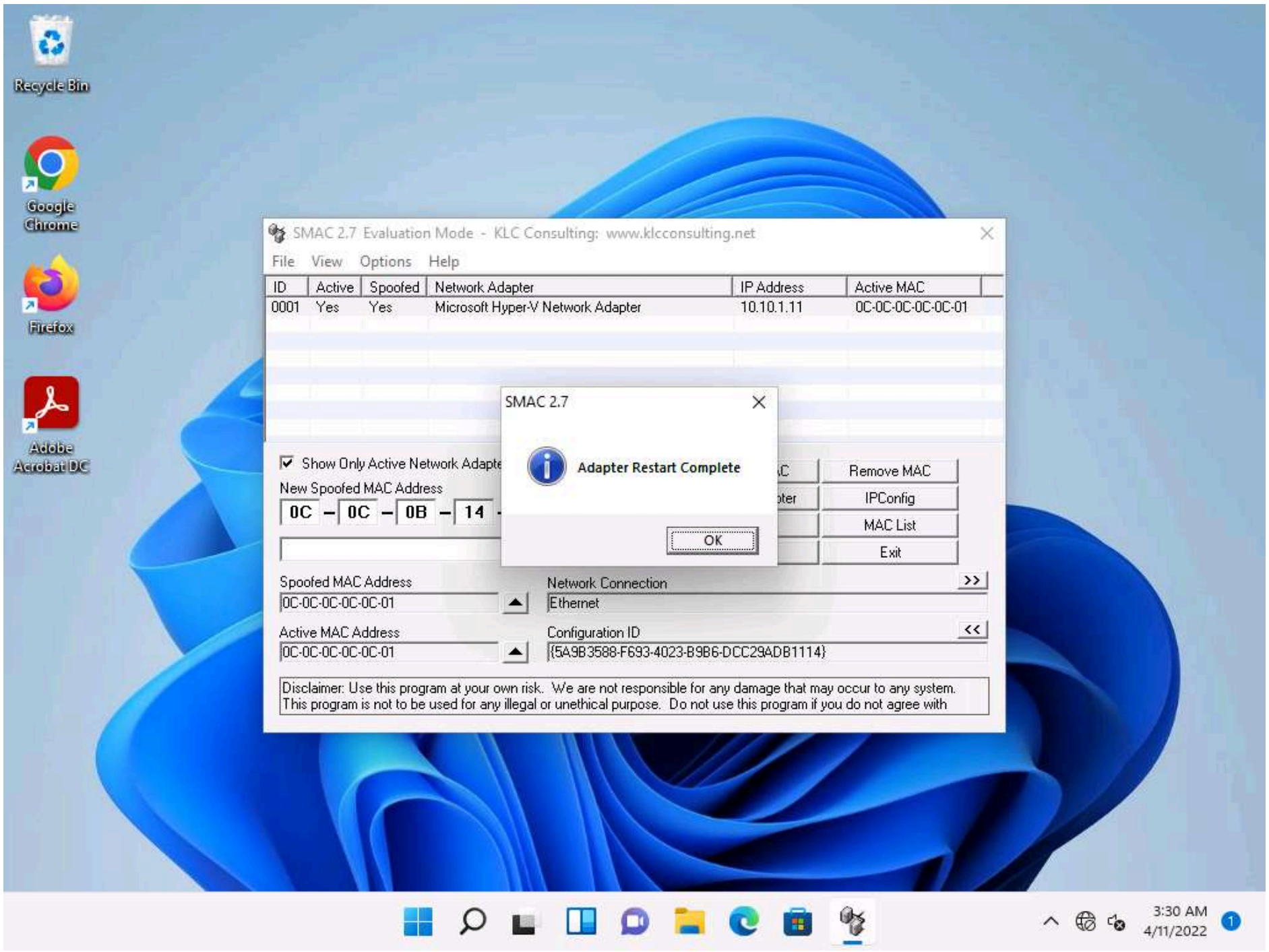
29. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

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

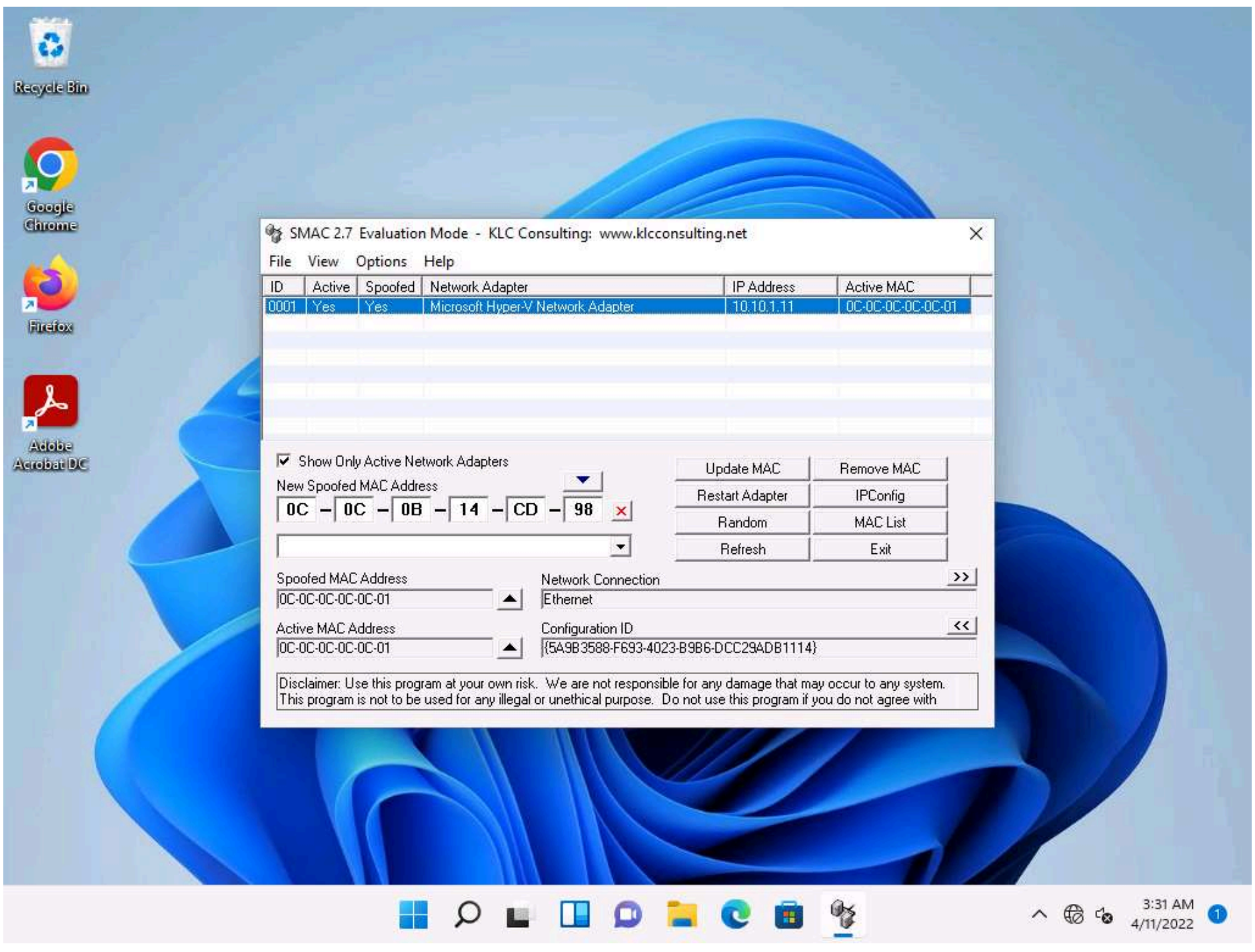
Note: In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.



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



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



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

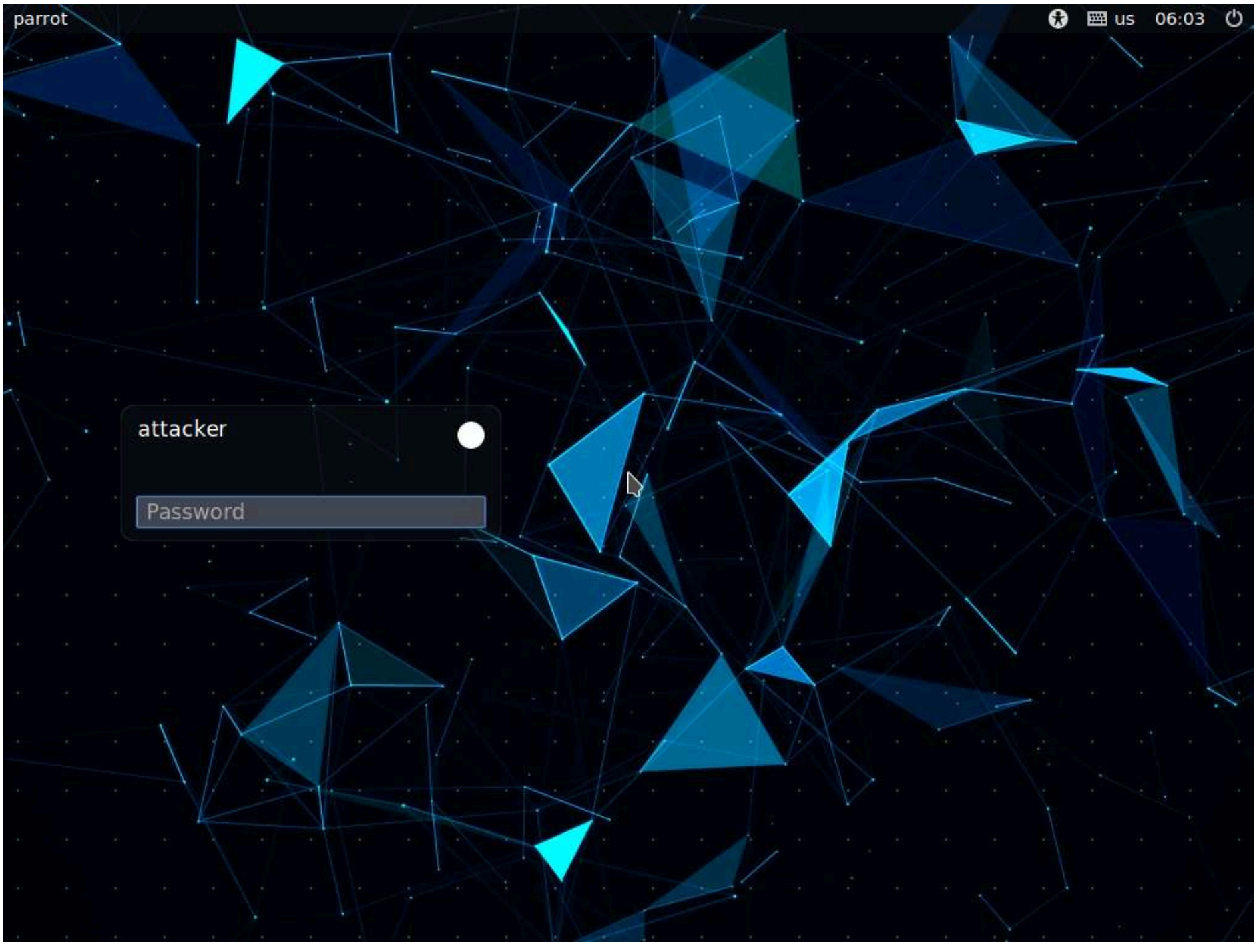
32. To restore the MAC address back to its original setting, click the **Remove MAC** button.
33. This concludes the demonstration of spoofing MAC addresses using TMAC and SMAC.
34. Close all open windows and document all the acquired information.

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 controoller). 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

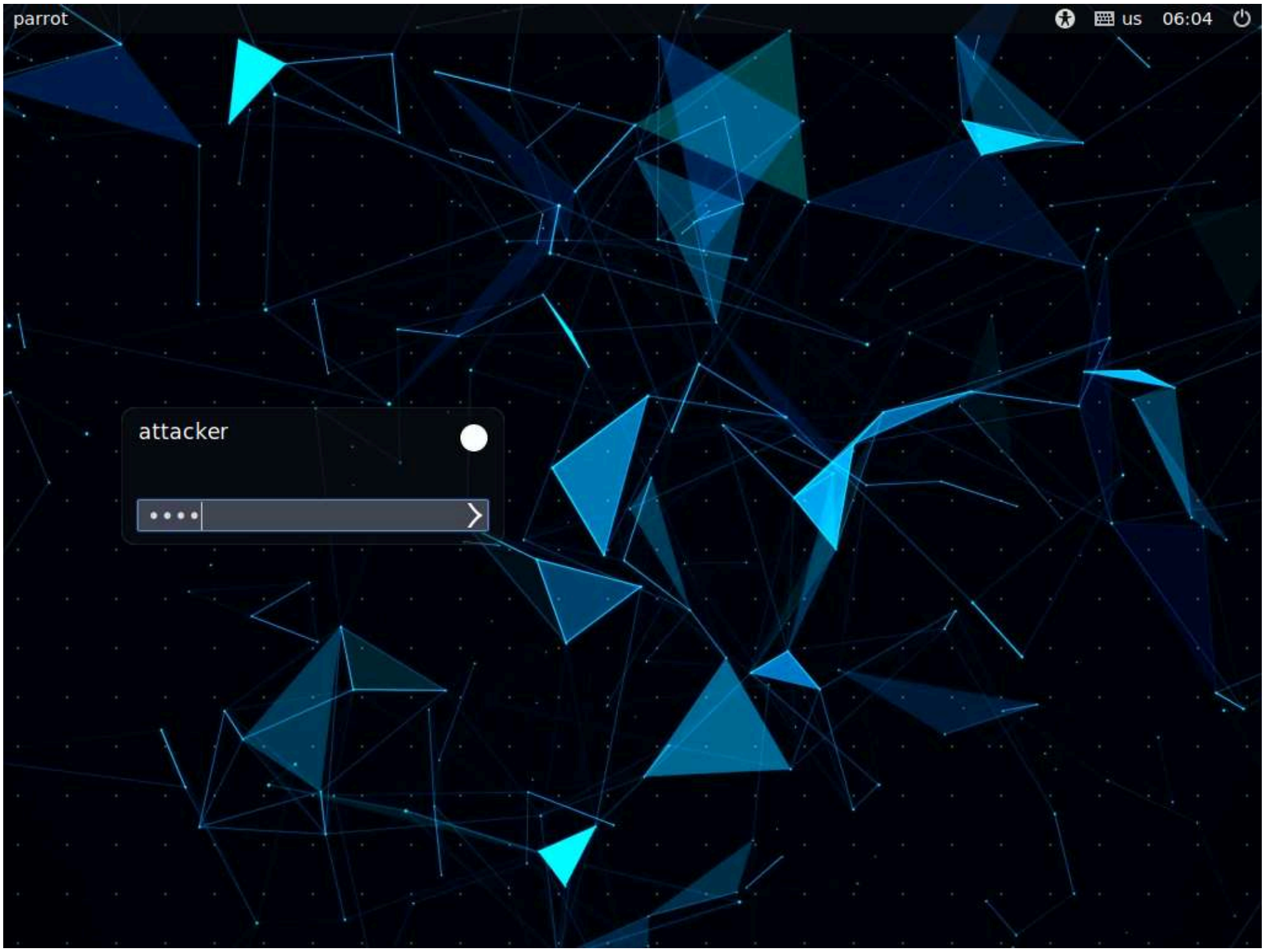
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.



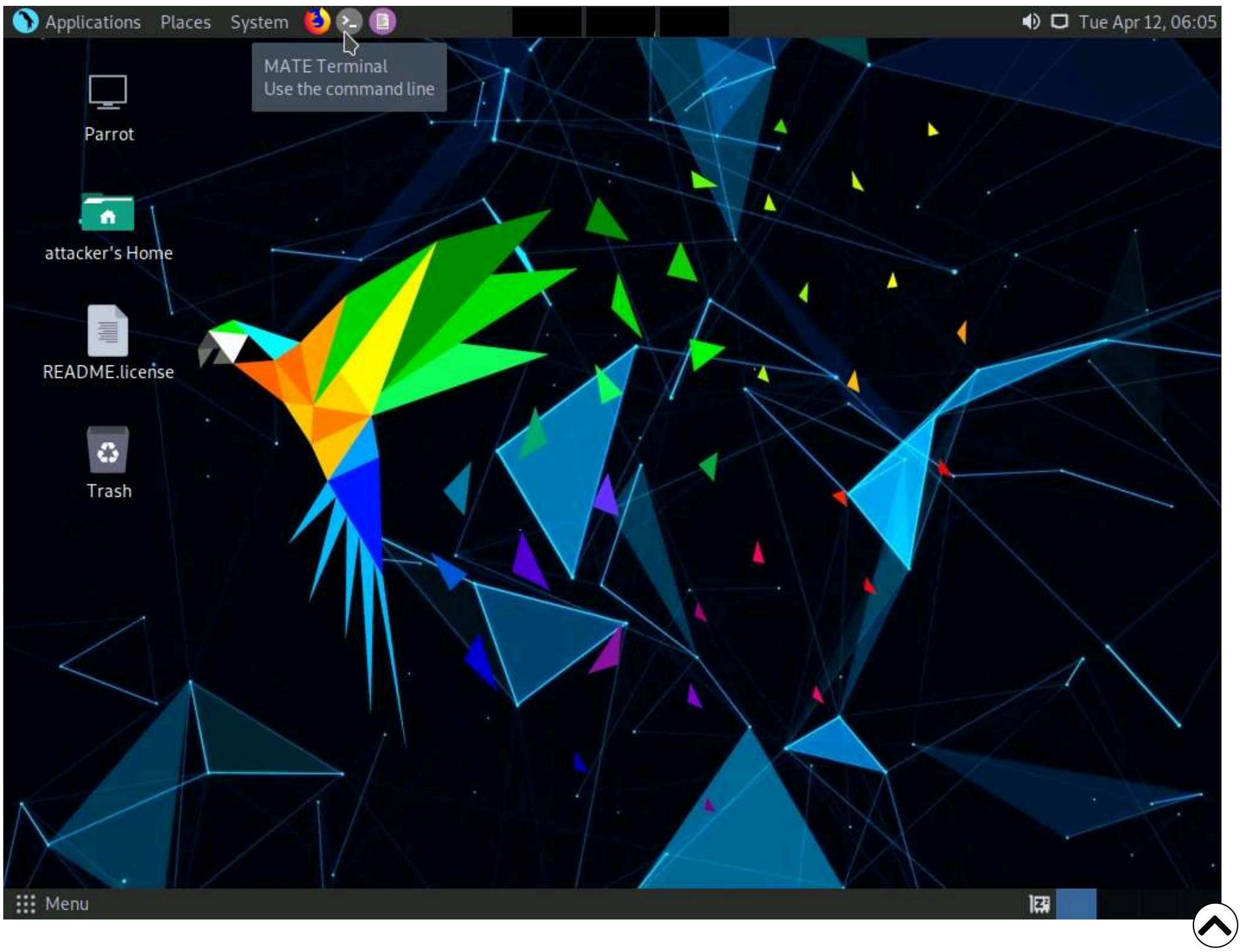
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

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



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

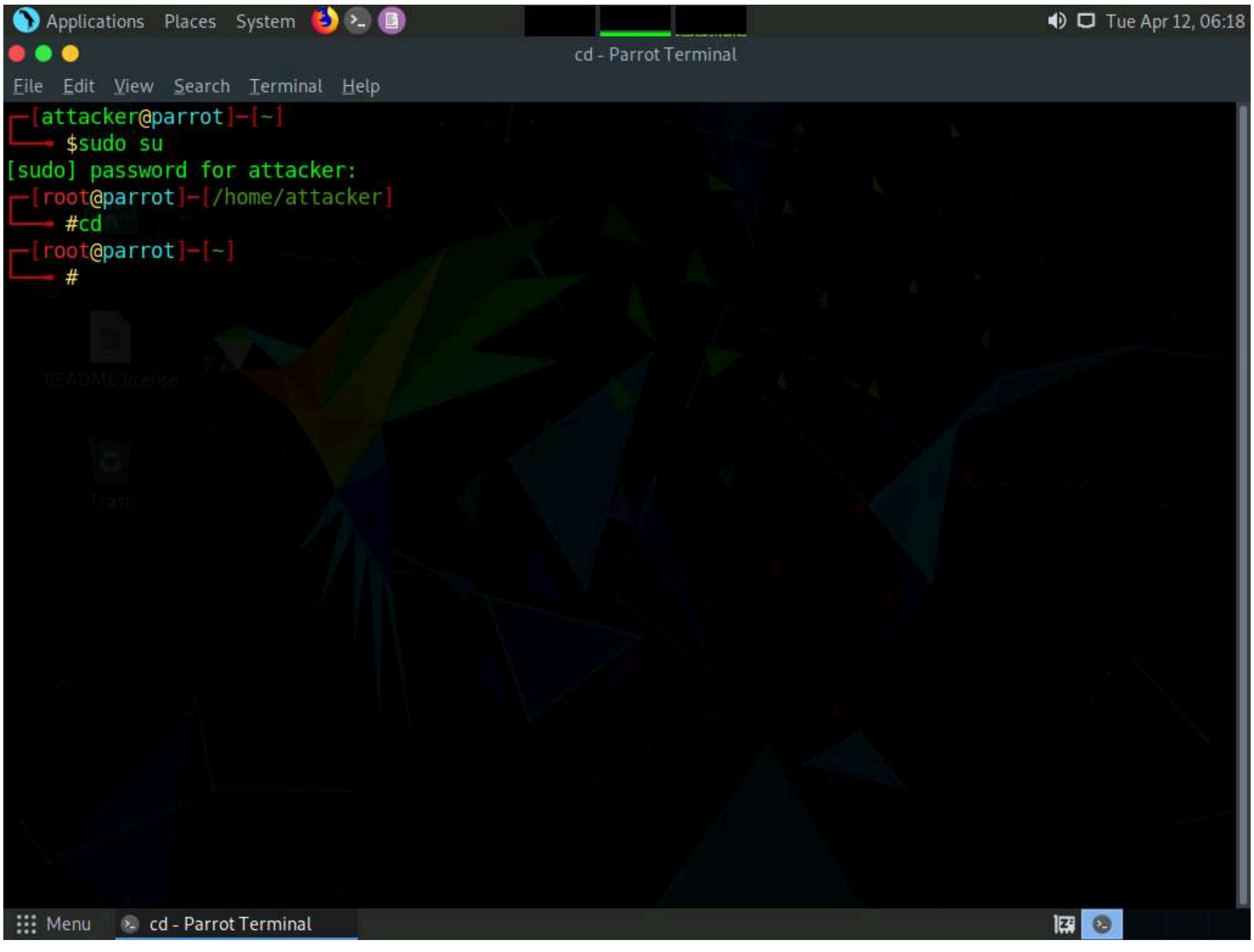


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

5. In the [sudo] password for attacker field, type **toor** as a password and press **Enter**.

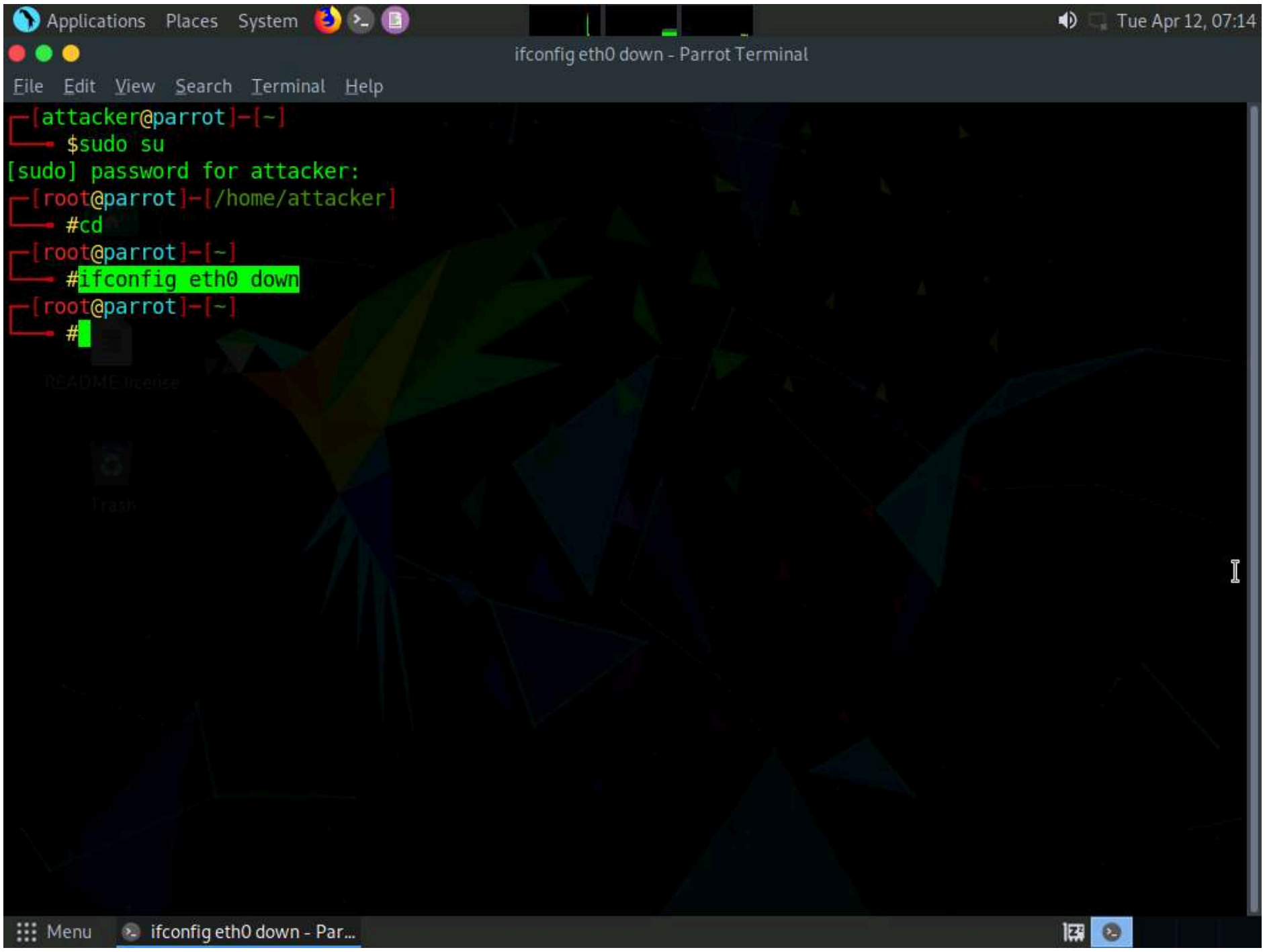
Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

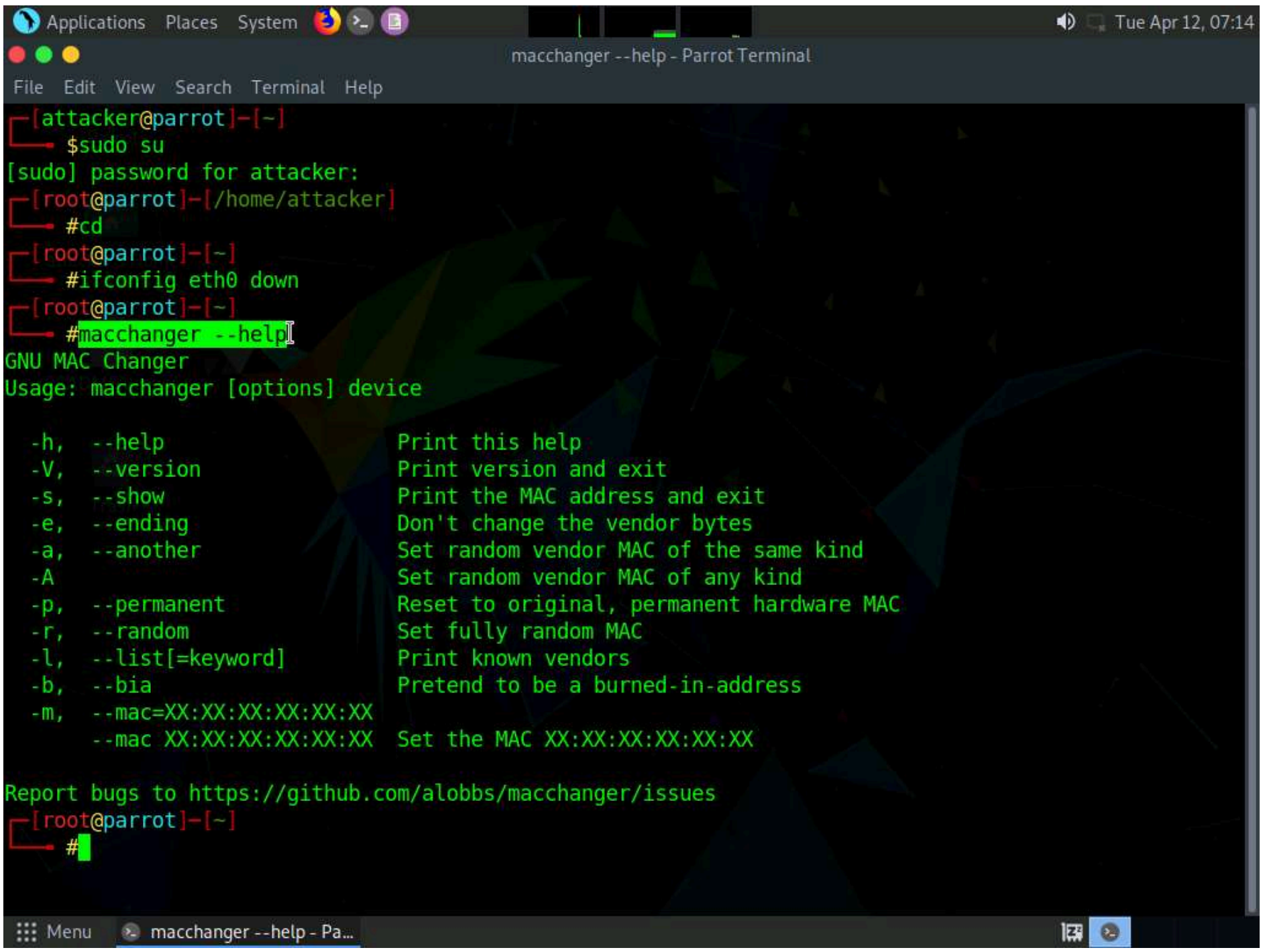


7. Before changing the MAC address we need to turn off the network interface.

8. Type **ifconfig eth0 down** and press **Enter**, to turn off the network interface.

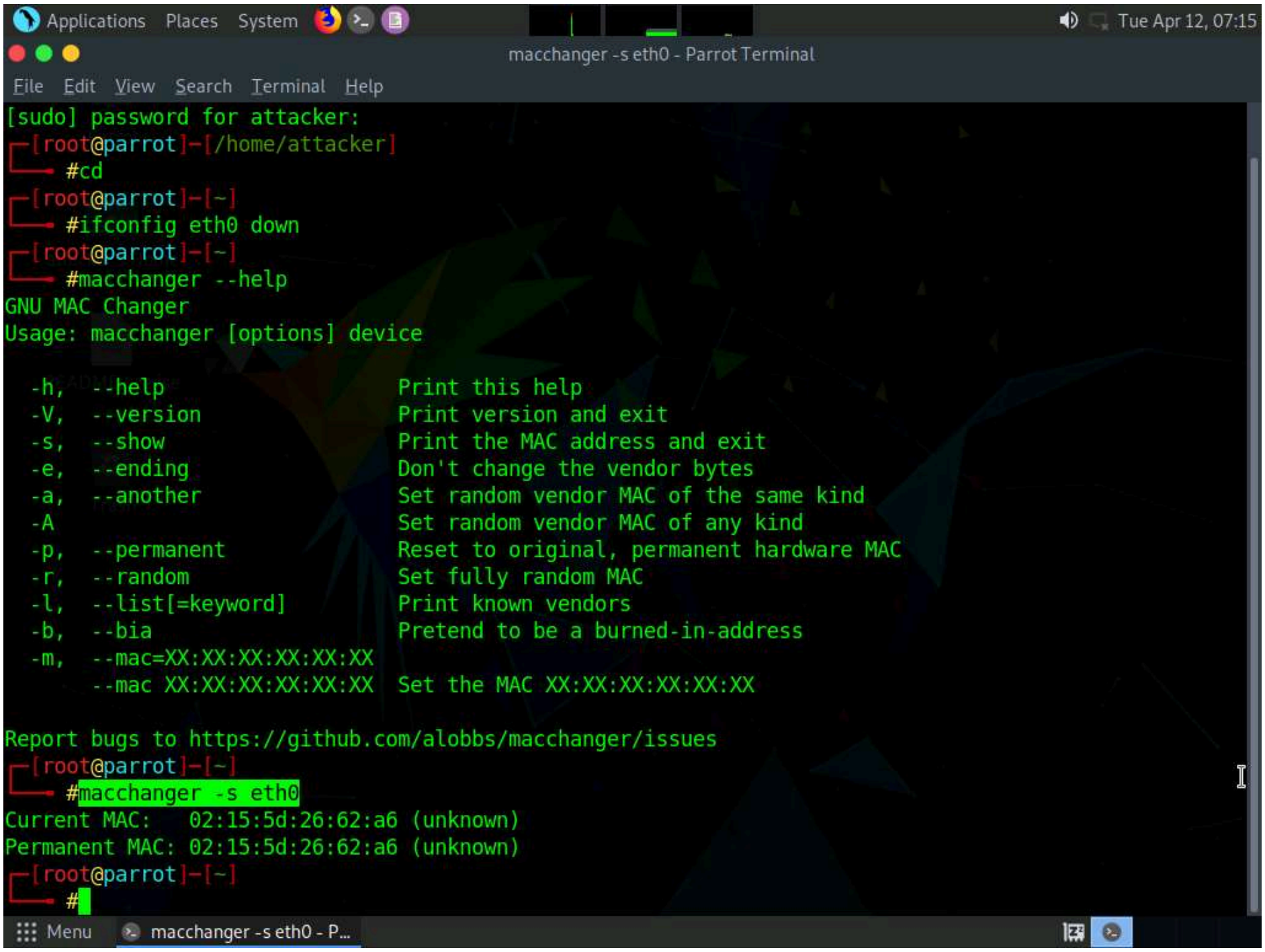


9. Type **macchanger --help** command to see the available options of macchanger tool.



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

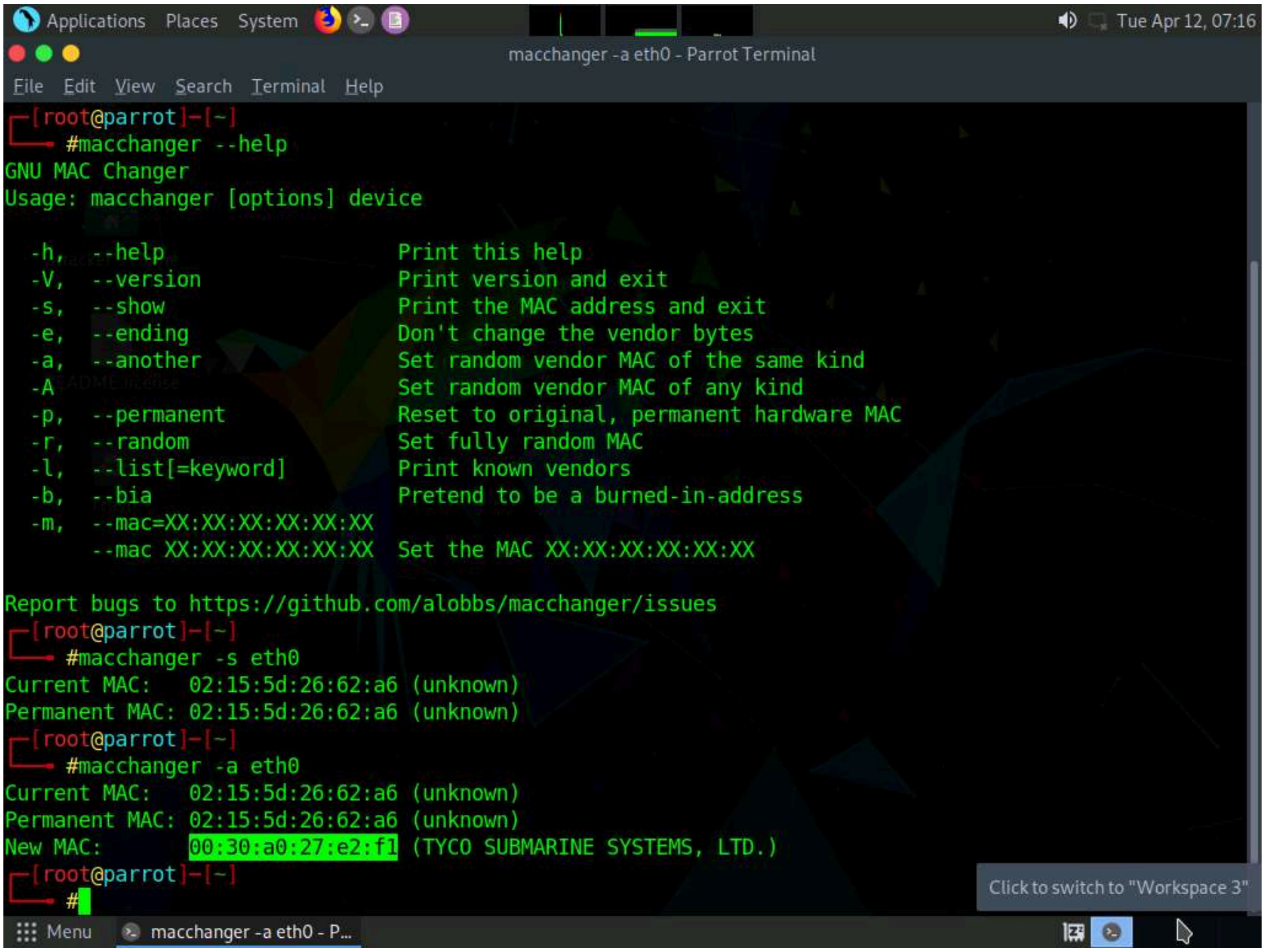
Note: **-s**: prints the MAC address of the machine.



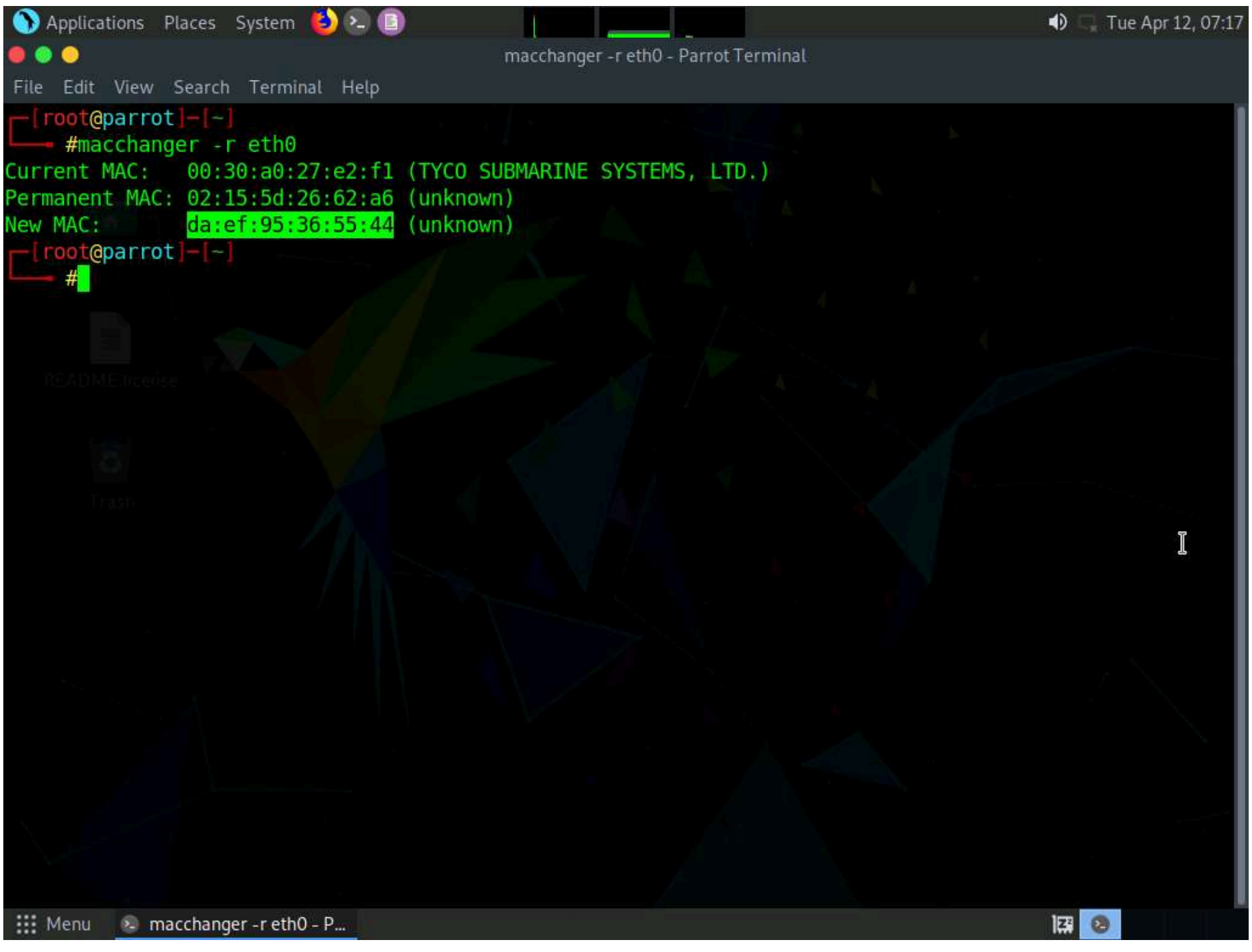
11. Now we will change the MAC address of the network interface.

12. In the terminal type, **macchanger -a eth0** and press **Enter**, to set a random vendor MAC address to the network interface.

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

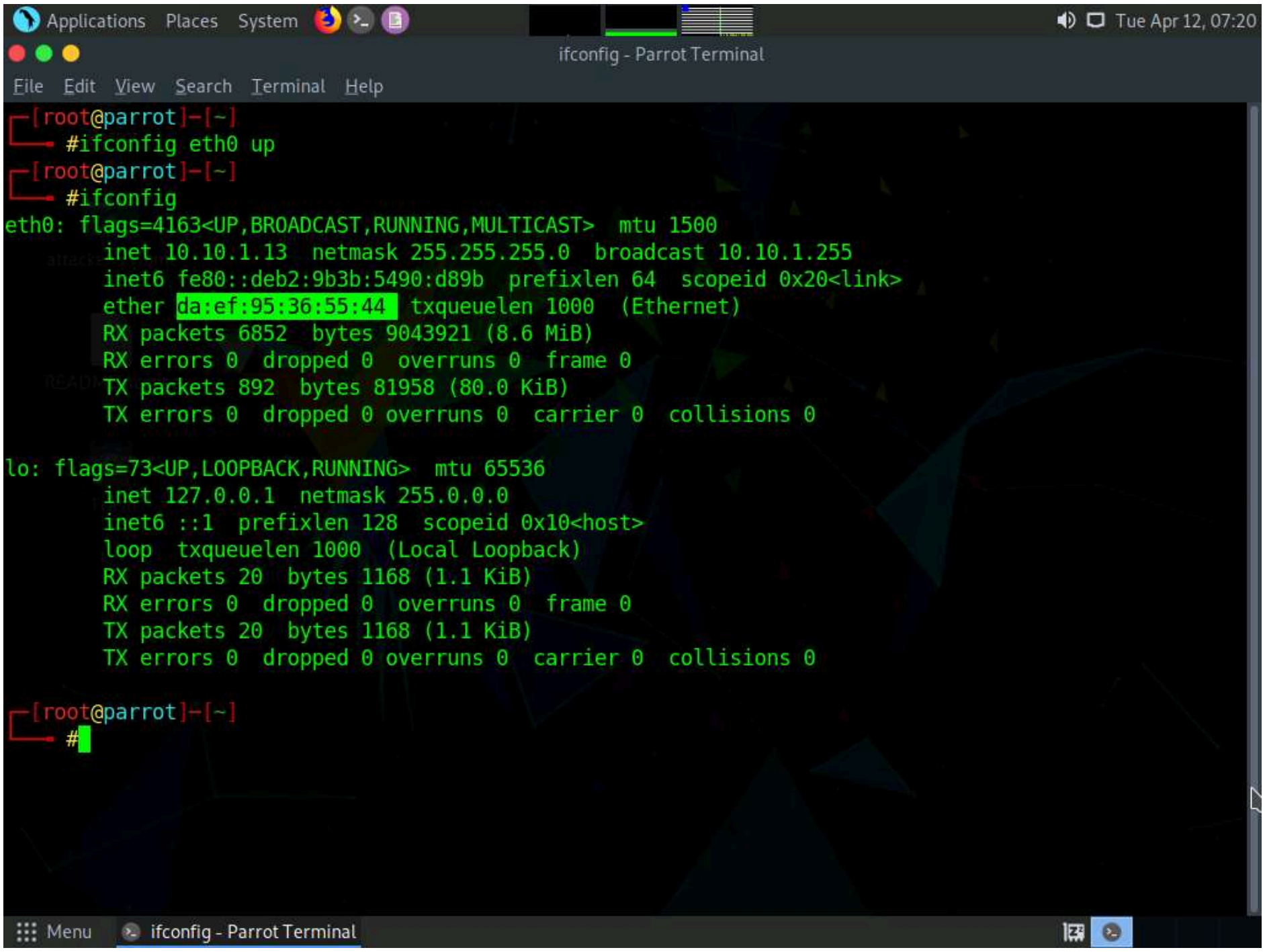


13. Now, type **macchanger -r eth0** and press **Enter**, to set a random MAC address to the network interface.



14. To enable the network interface type **ifconfig eth0 up** and press **Enter**.

15. To check the changed MAC address, type **ifconfig** and press **Enter**.



16. You can observe that a random MAC address is set to the network interface.
17. This concludes the demonstration of how to spoof a MAC address of Linux machine using macchanger
18. Close all open windows and document all the acquired information.
19. Now, before proceeding to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section. If a **Finish Event** pop-up appears, click on **Finish**.

Lab 2: Perform Network Sniffing using Various Sniffing Tools

Lab Scenario

Data traversing an HTTP channel flows 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

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.

Task 1: Perform Password Sniffing using Wireshark

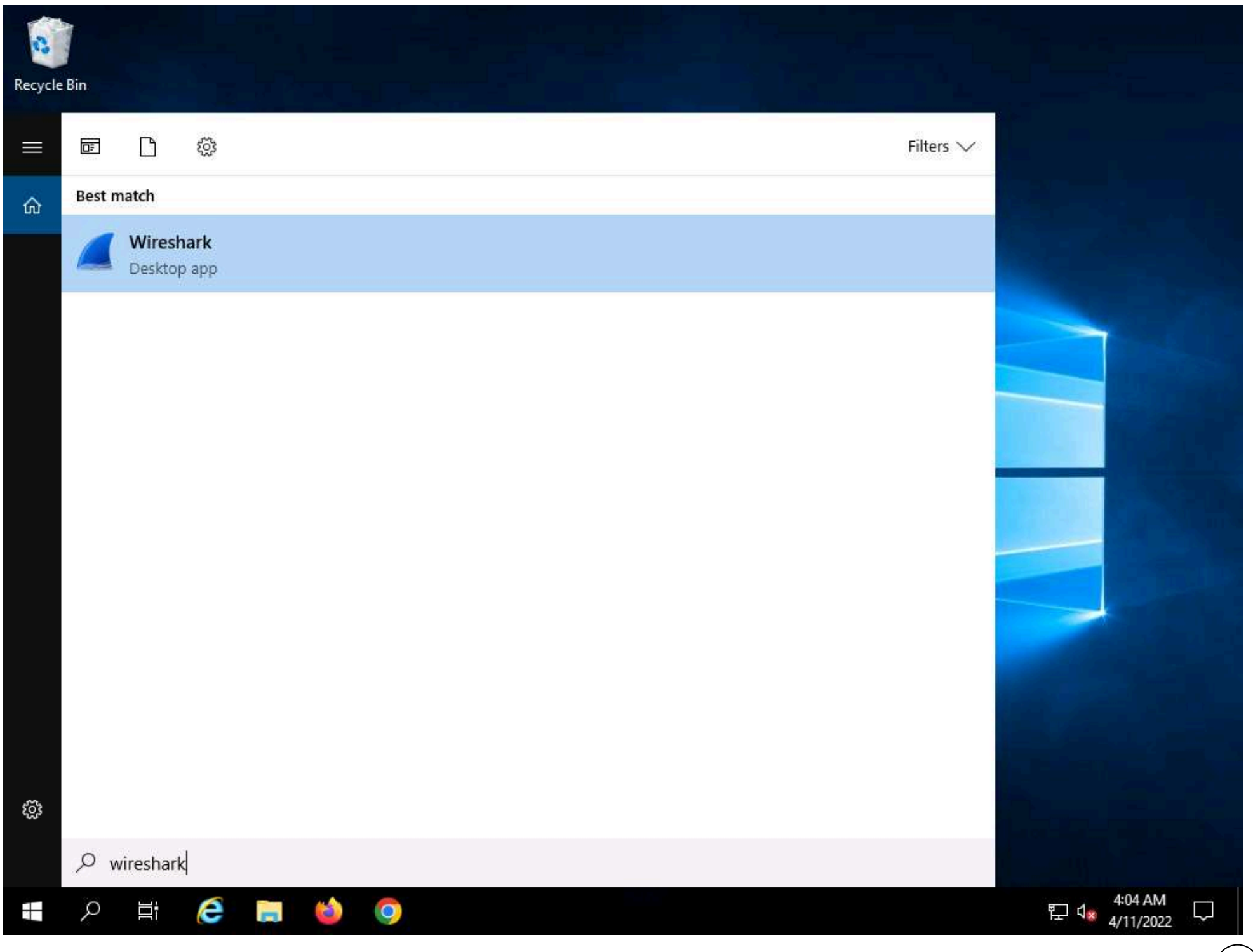
Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI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

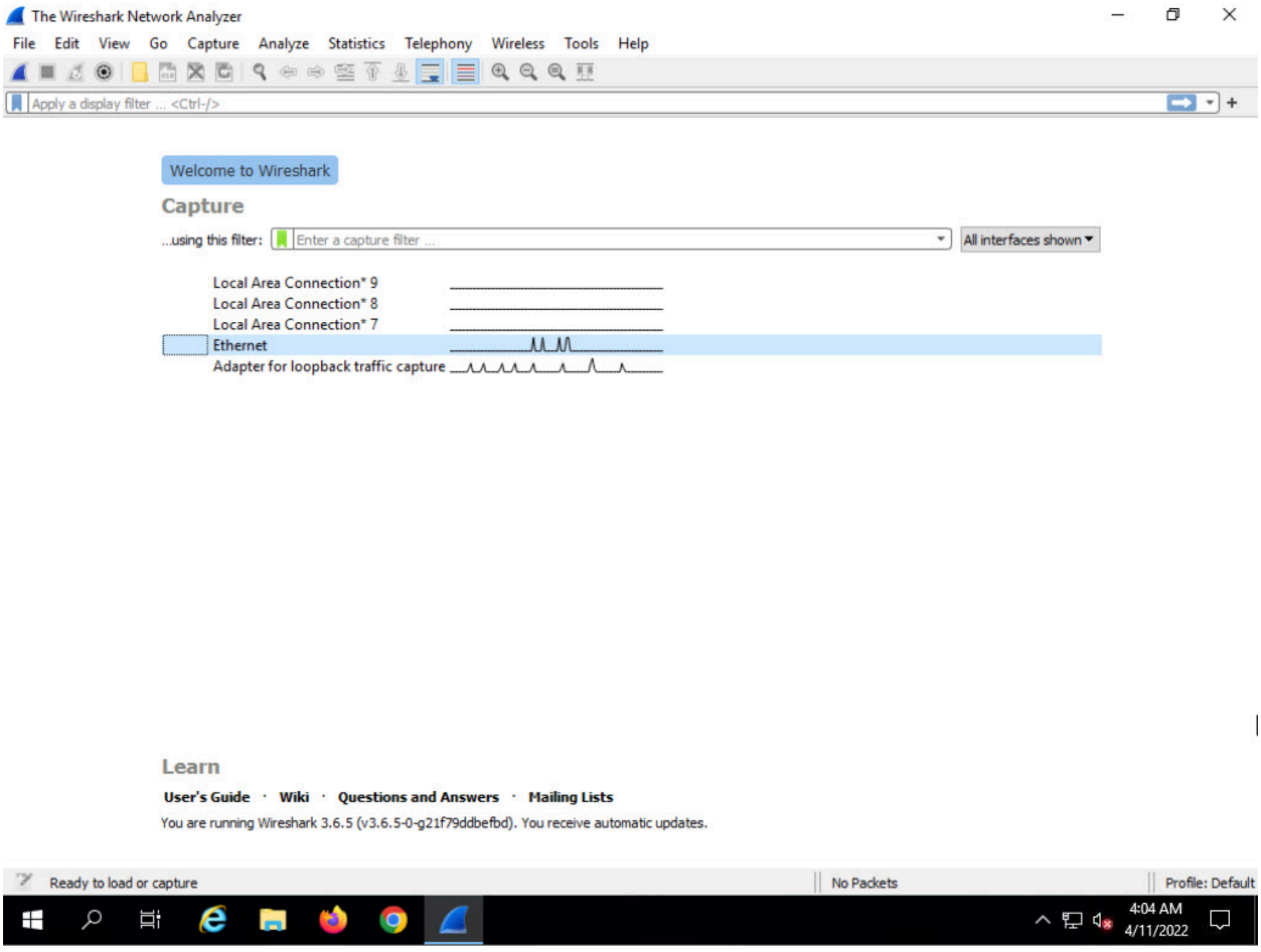
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Click the **Type here to search** 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**.

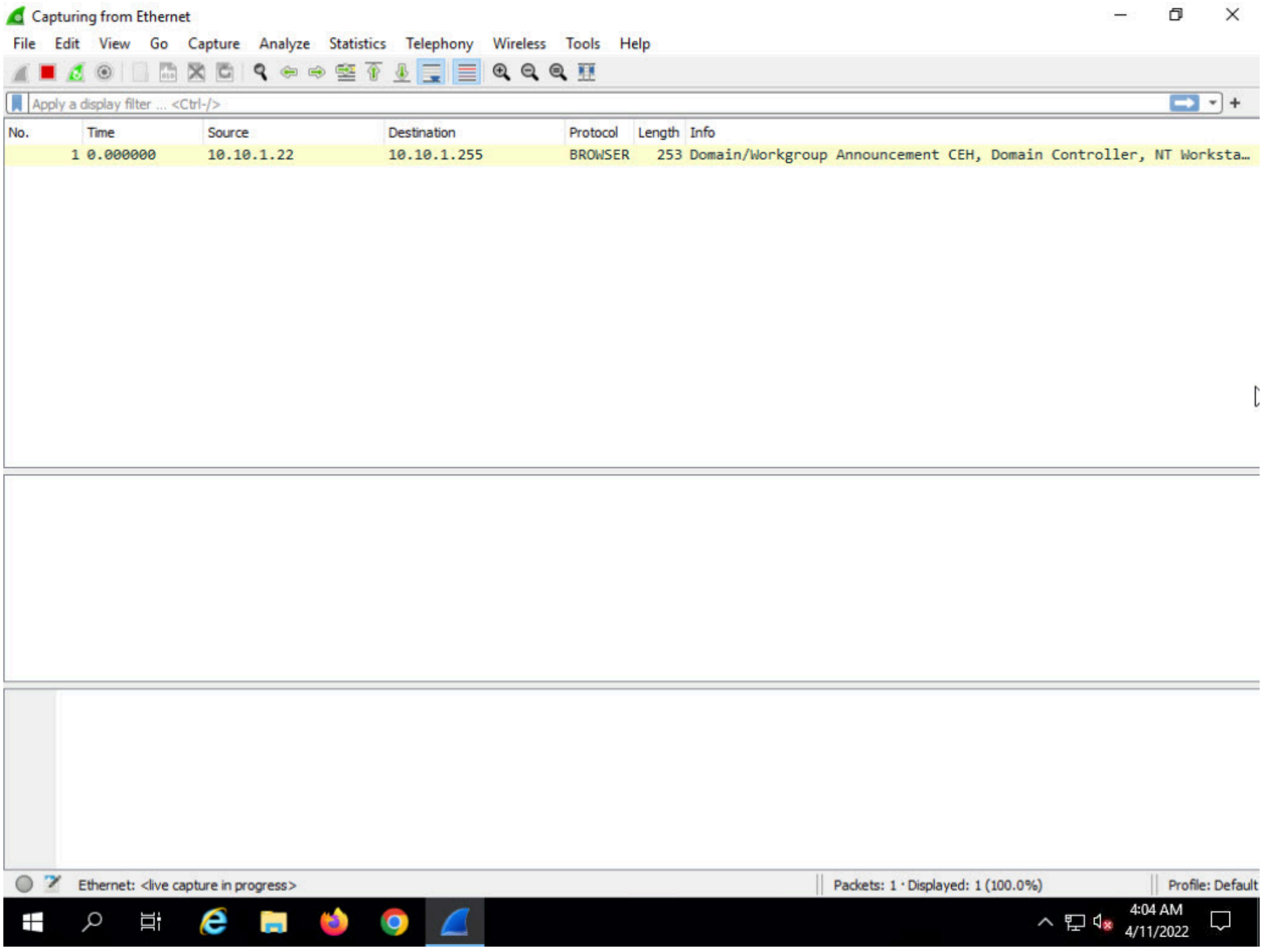


4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

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.

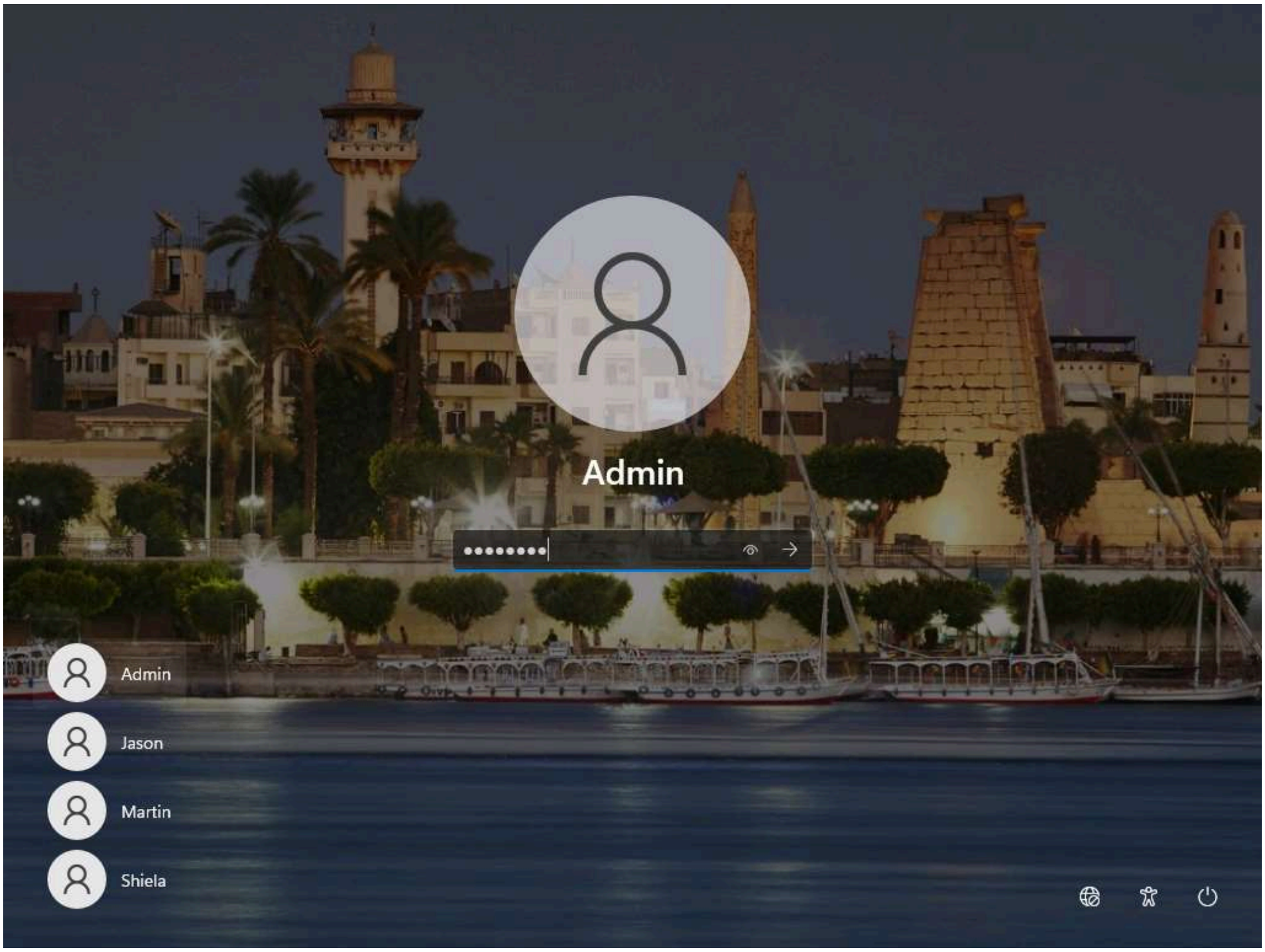


6. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**.

7. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

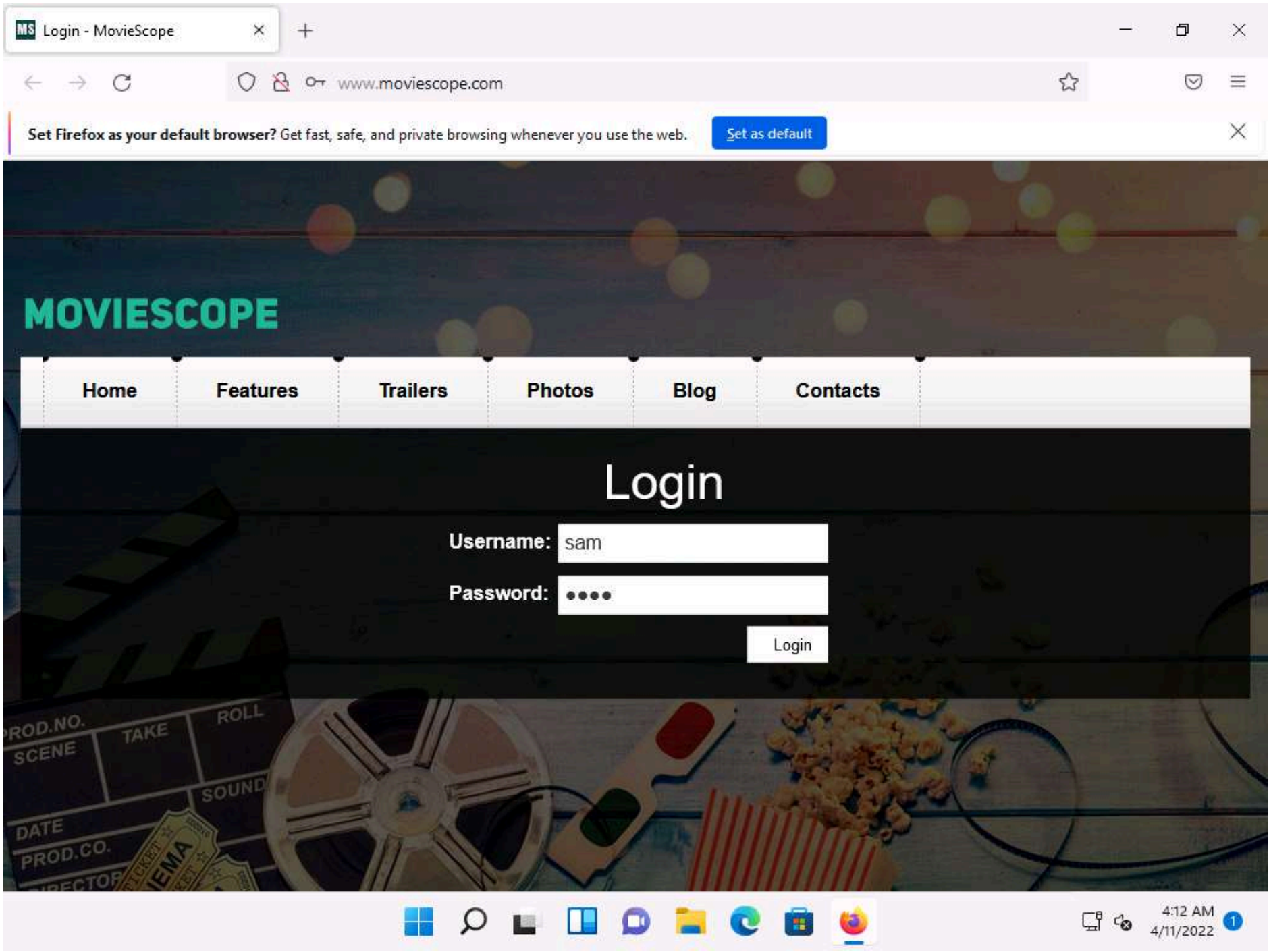
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

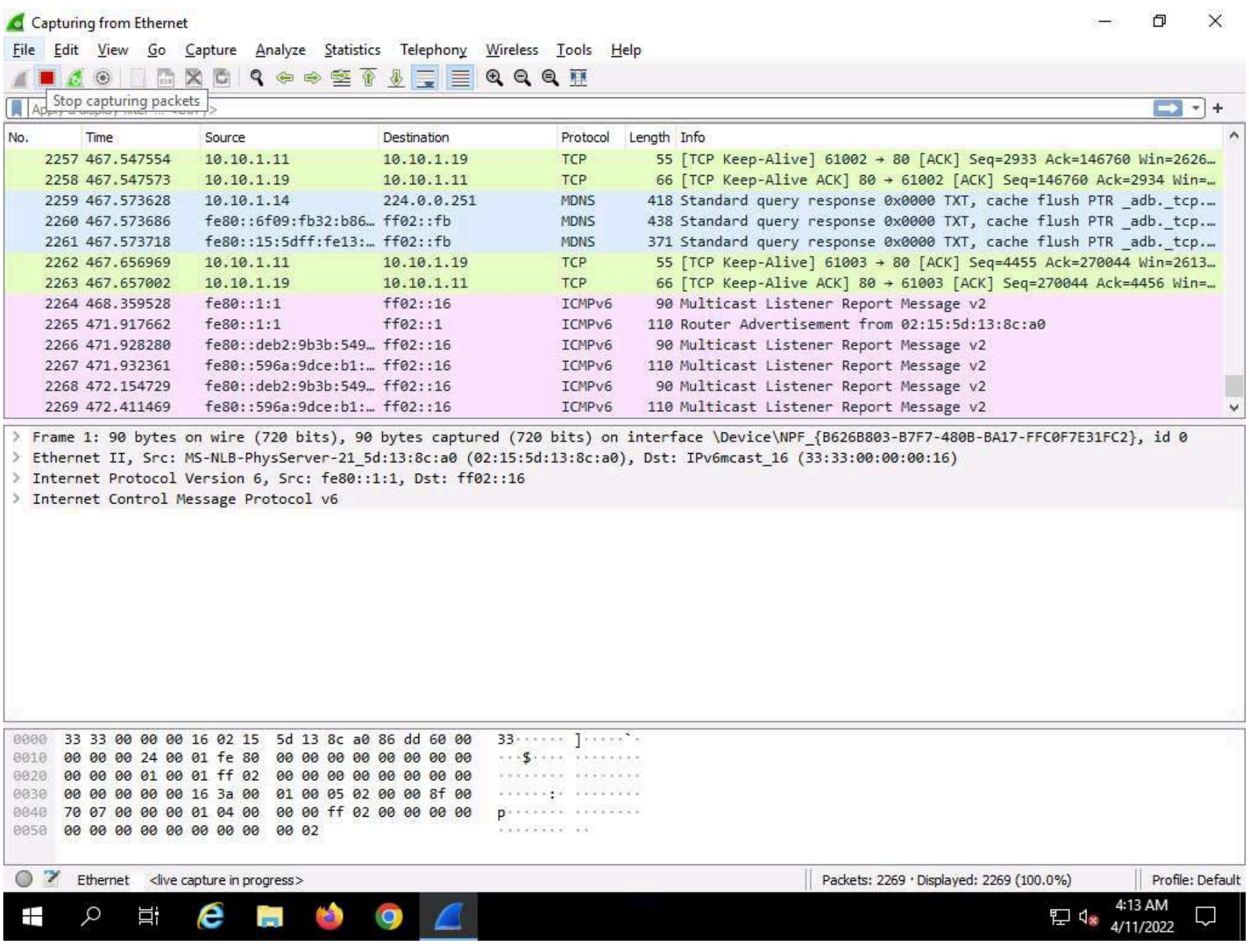


8. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **http://www.moviescope.com/** in the address bar, and press **Enter**.

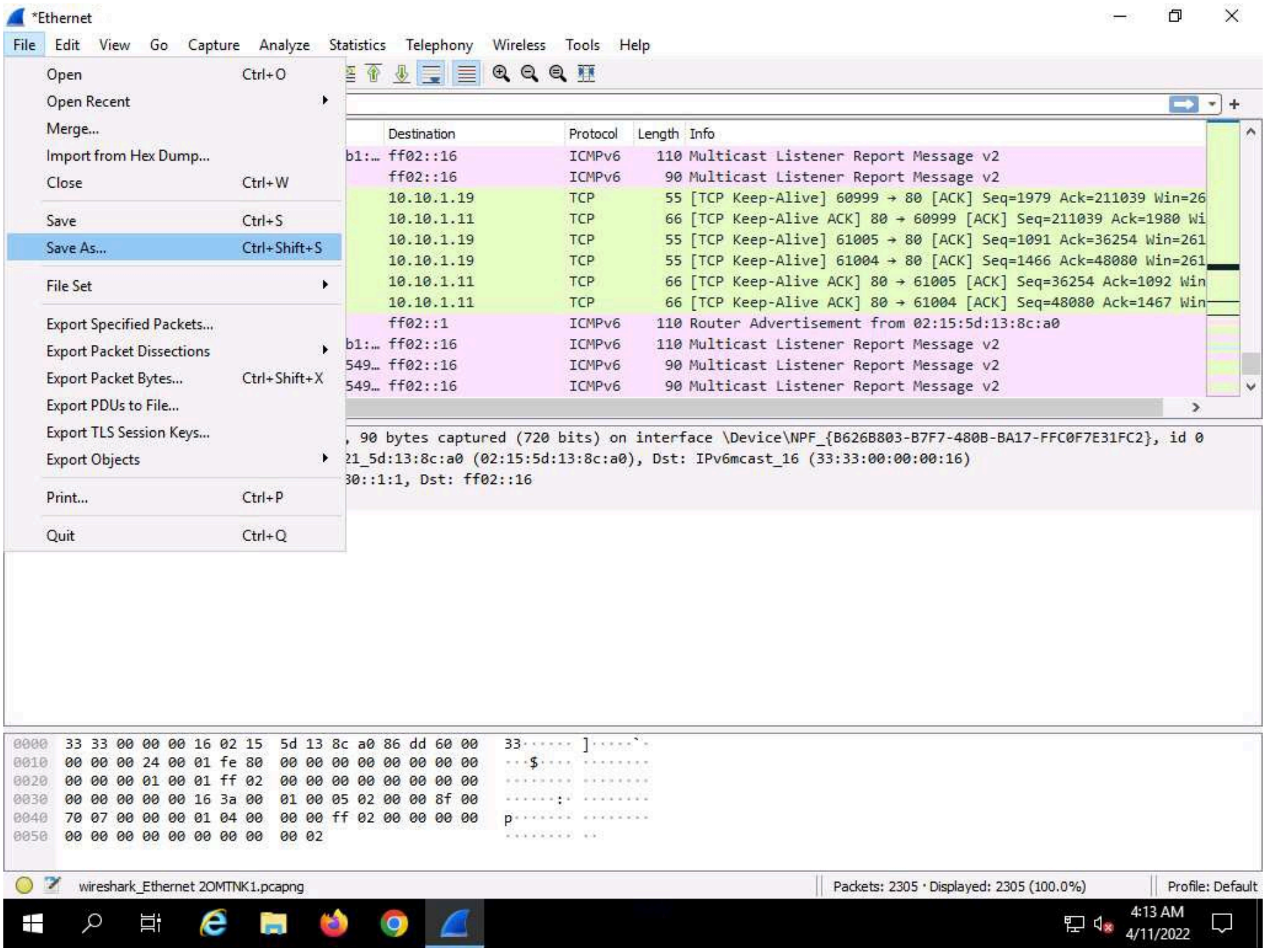
9. The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in the screenshot.



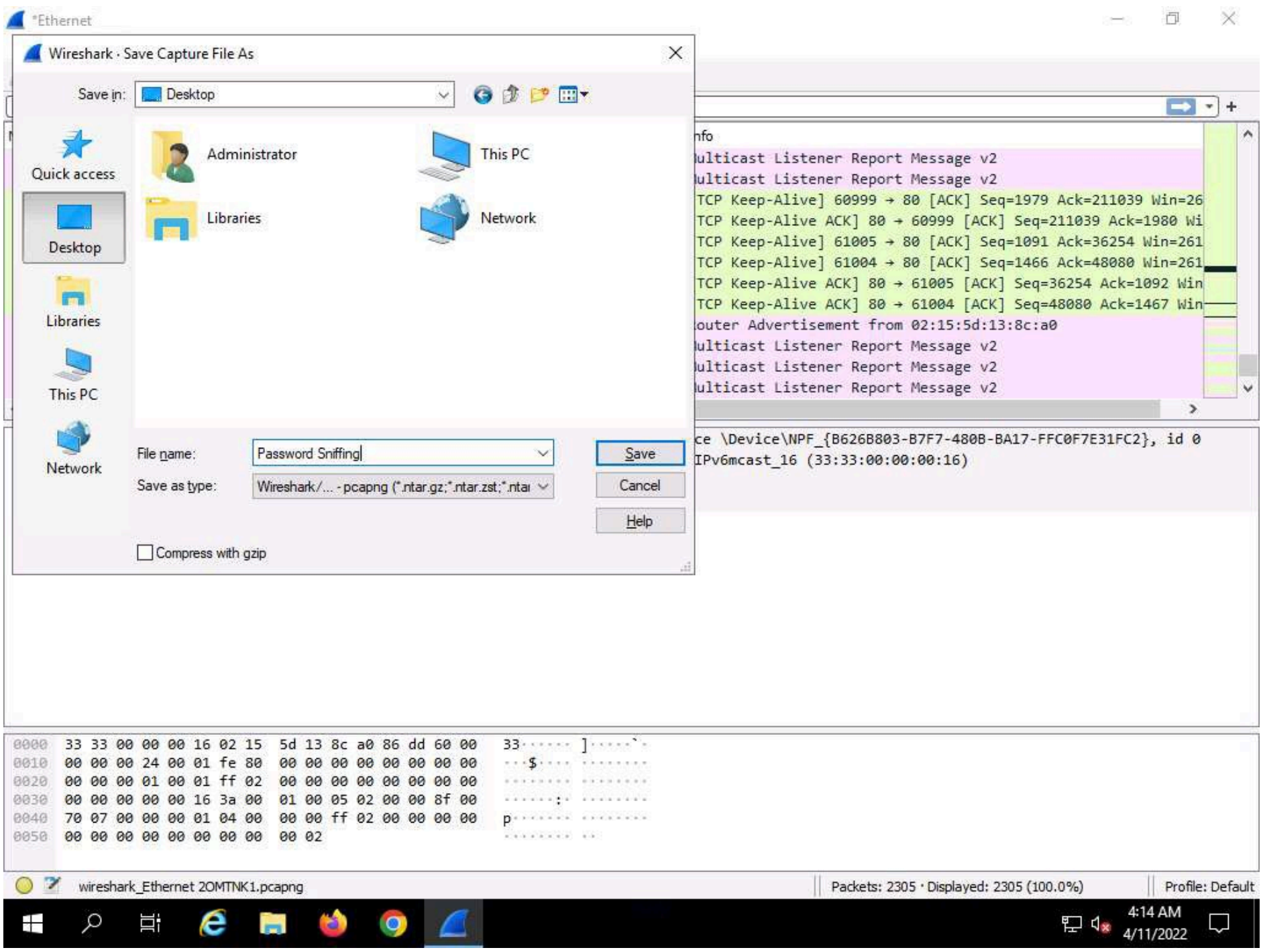
10. Click **CEHv12 Windows Server 2019** to switch back to **Windows Server 2019** machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.



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

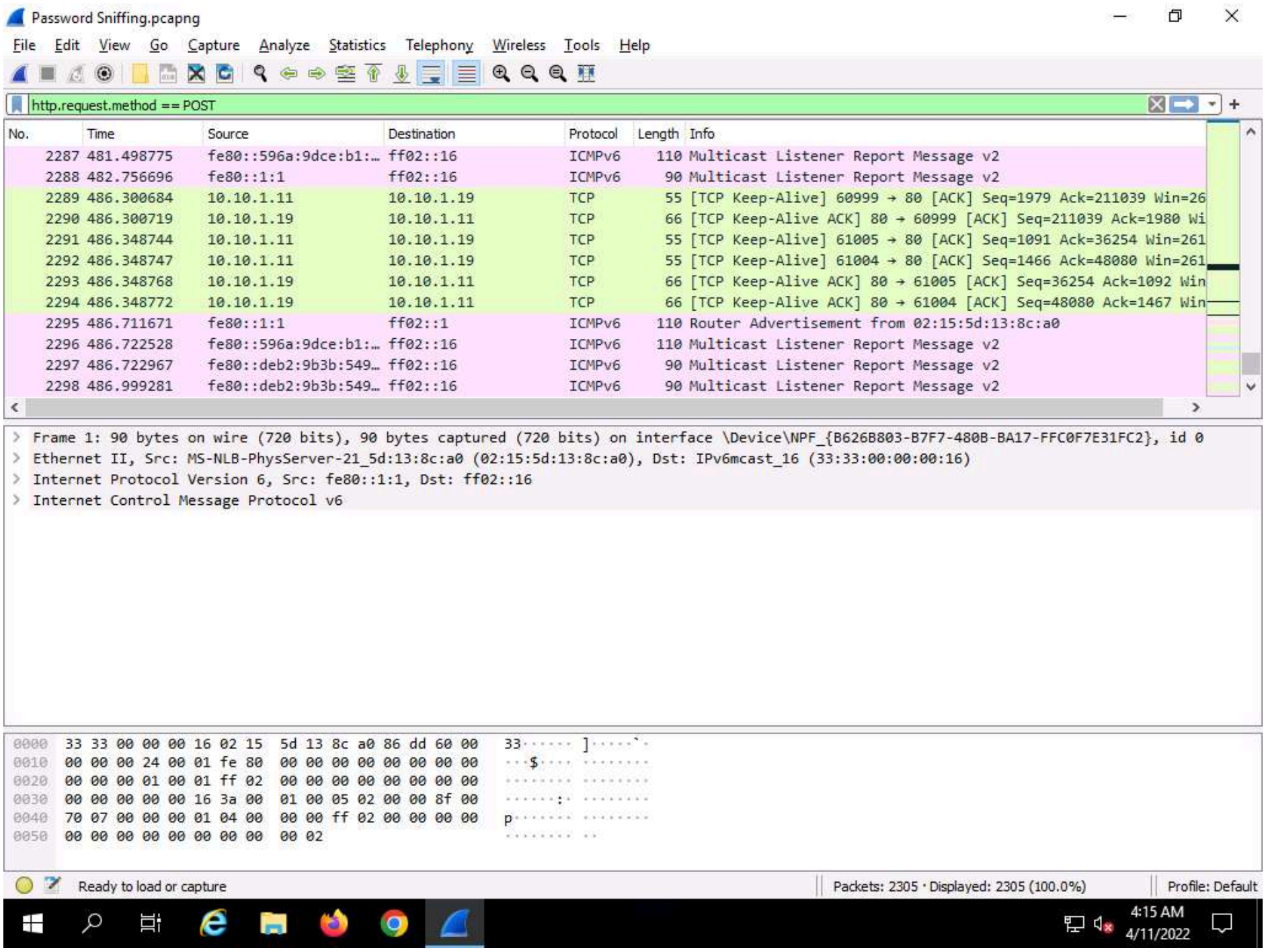


12. The **Wireshark: Save file as** window appears. Select any location to save the file, specify **File name** as **Password Sniffing**, and click **Save**.

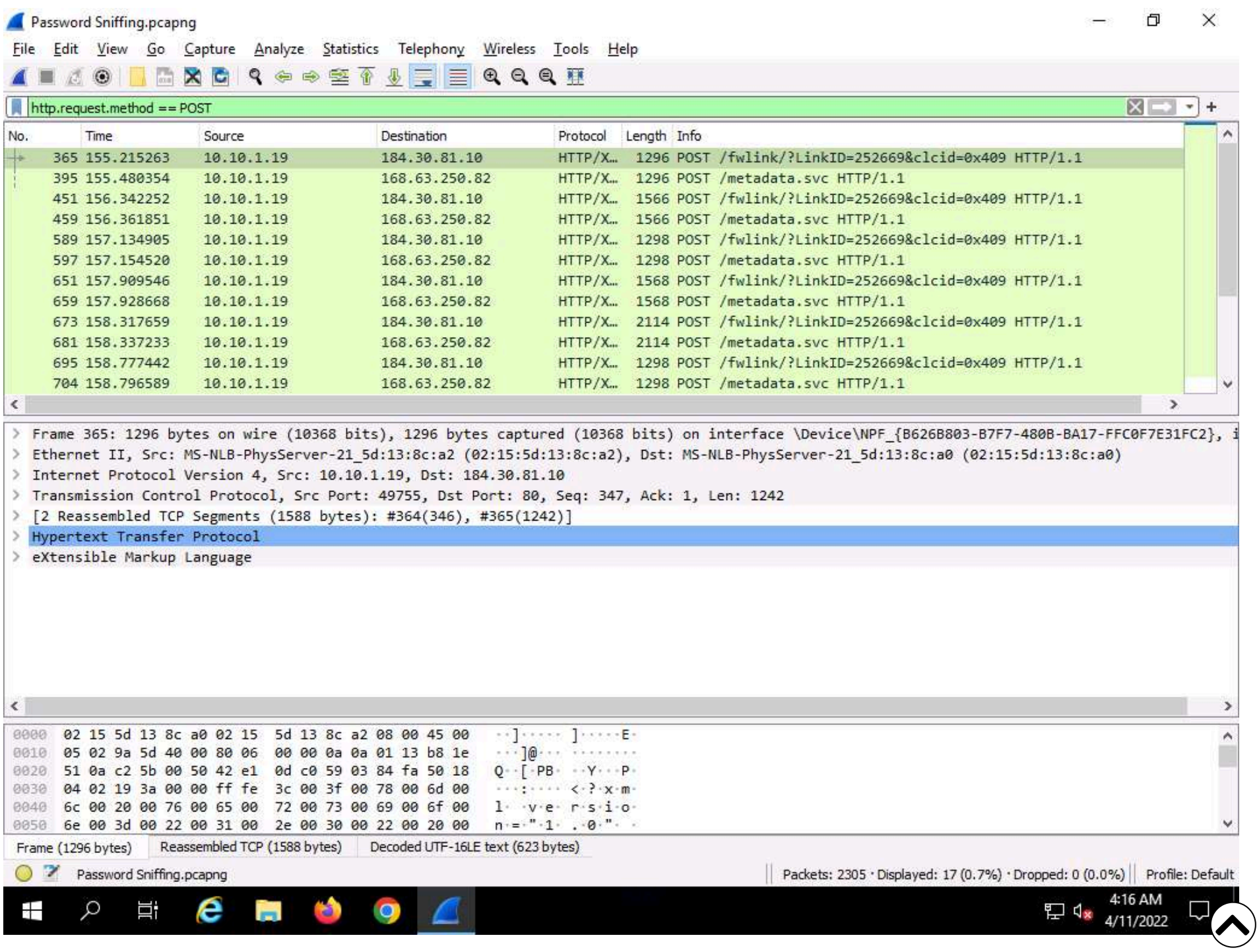


13. In the **Apply a display filter field**, type **http.request.method == POST** and click the arrow icon (**-->**) to apply the filter.

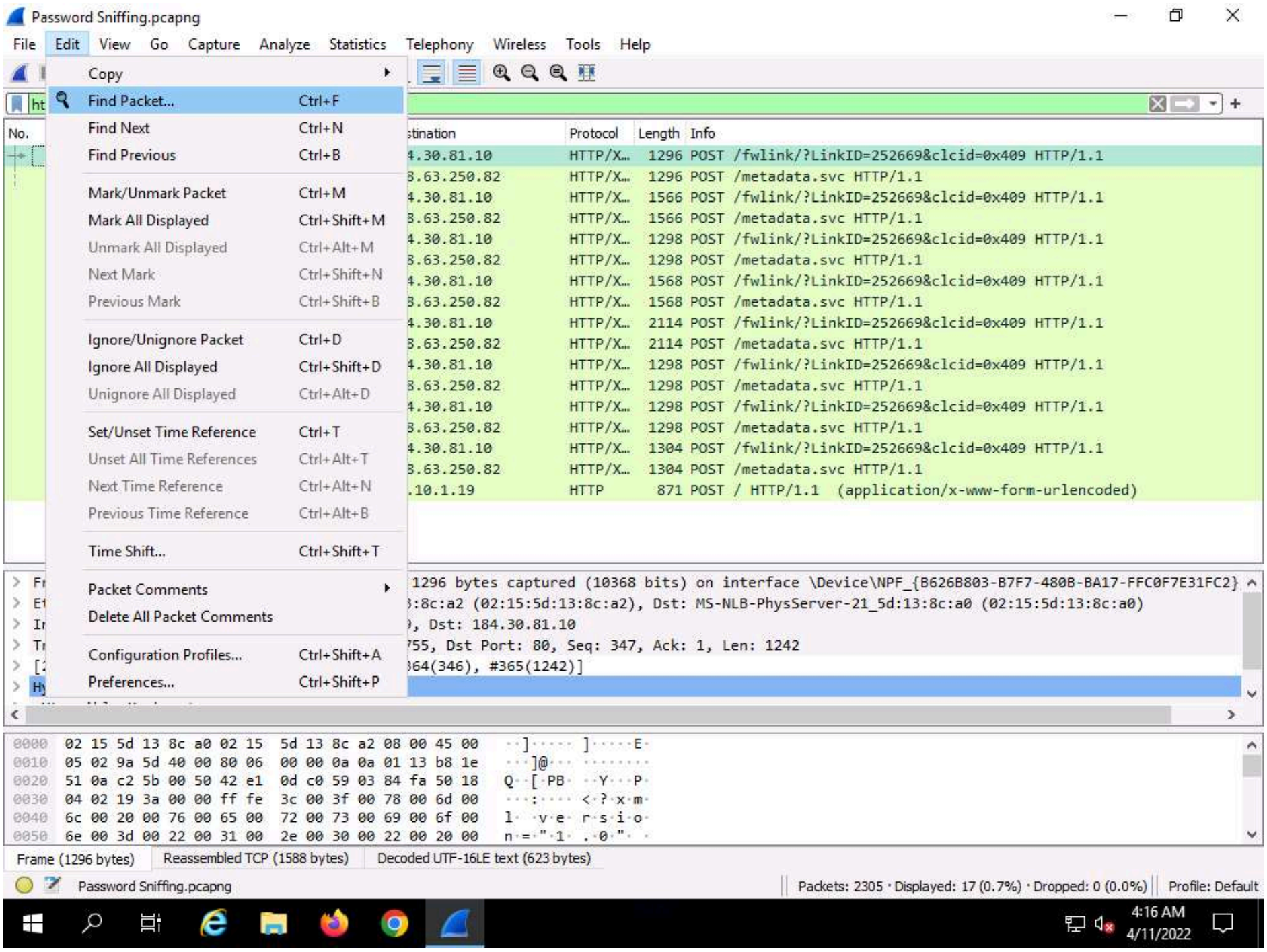
Note: Applying this syntax helps you narrow down the search for http POST traffic.



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



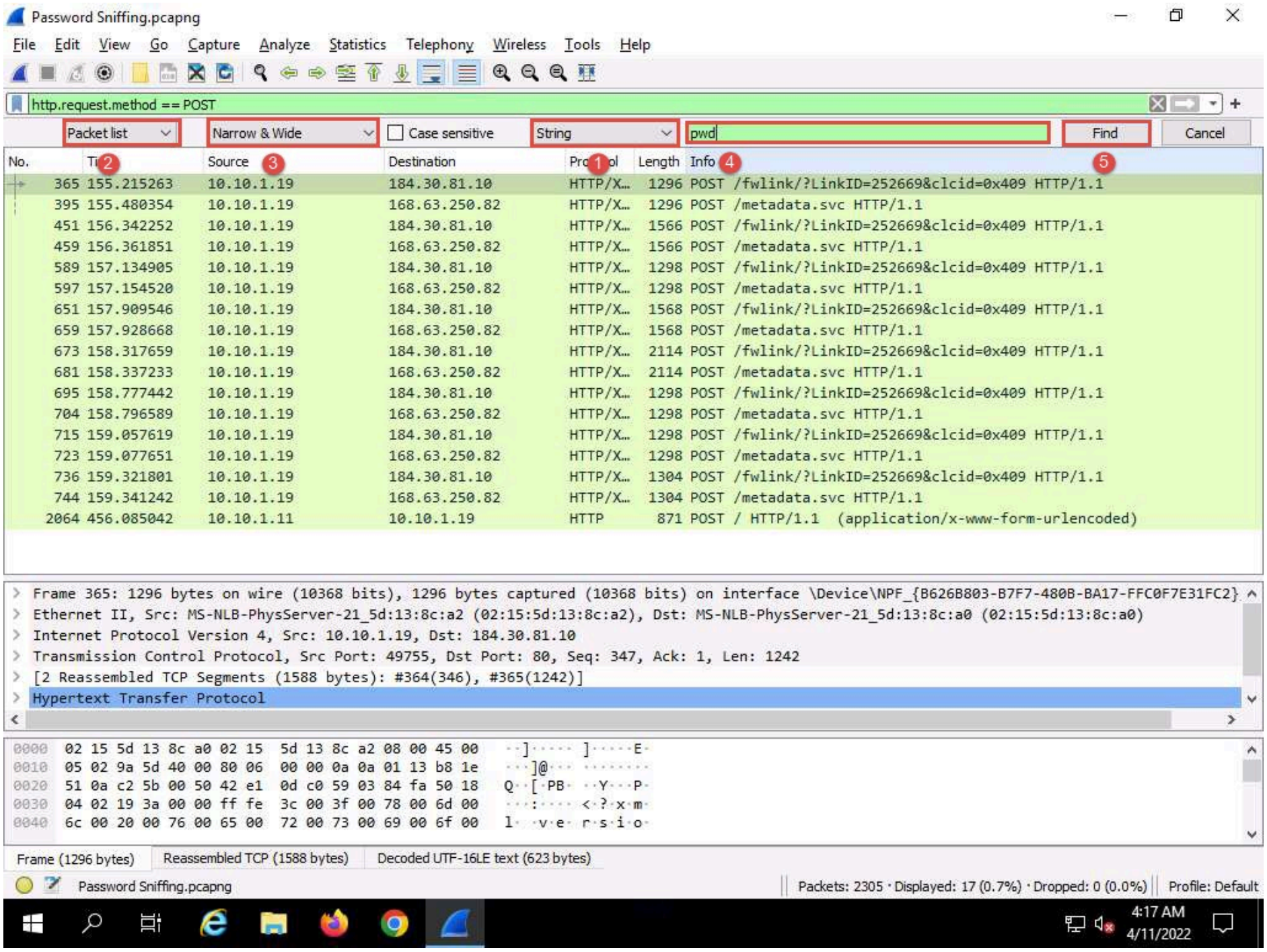
15. Now, click **Edit** from the menu bar and click **Find Packet...**.



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

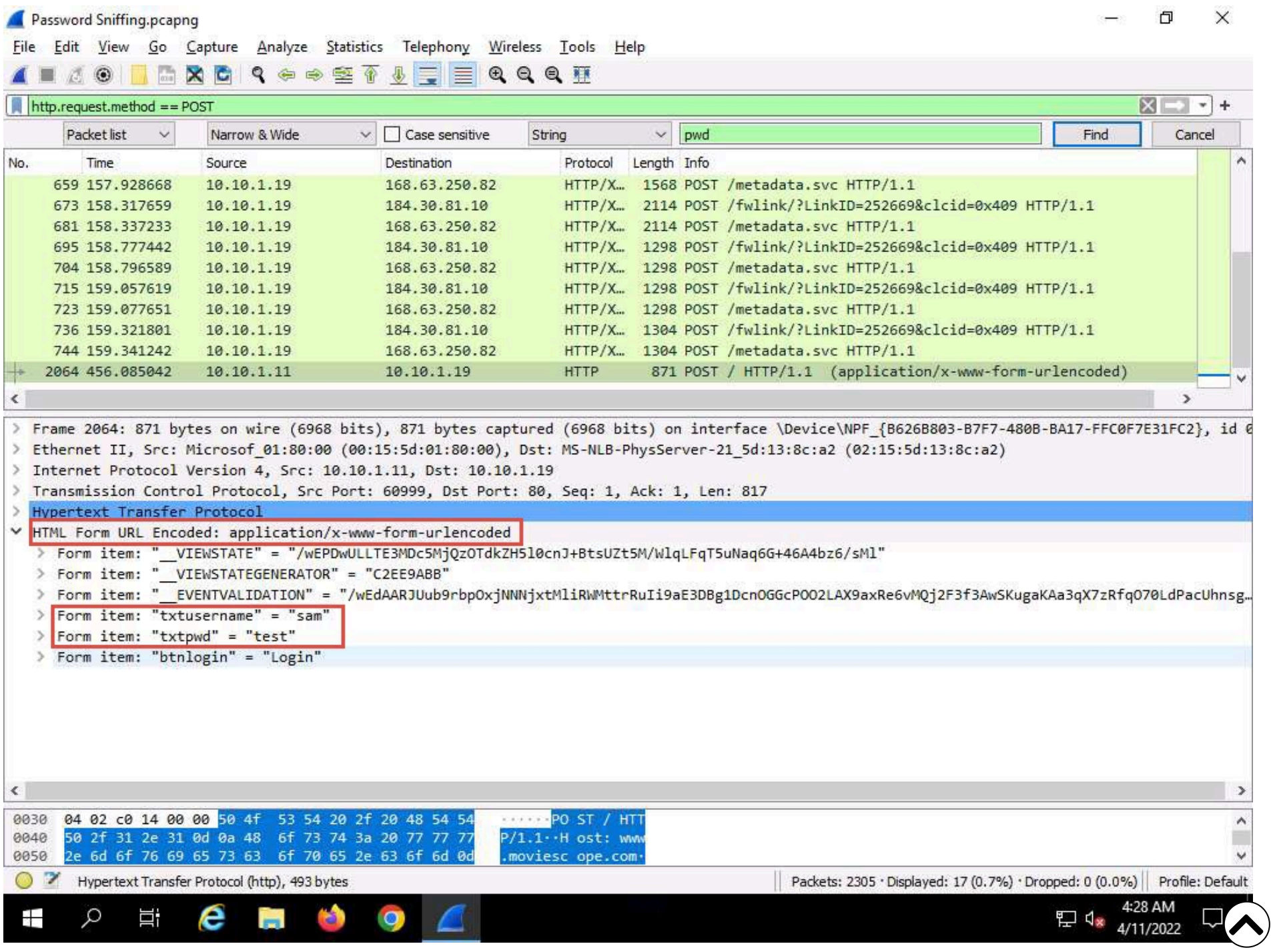
17. Click **Display filter**, select **String** from the drop-down options. Click **Packet list**, select **Packet details** from the drop-down options, and click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options.

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



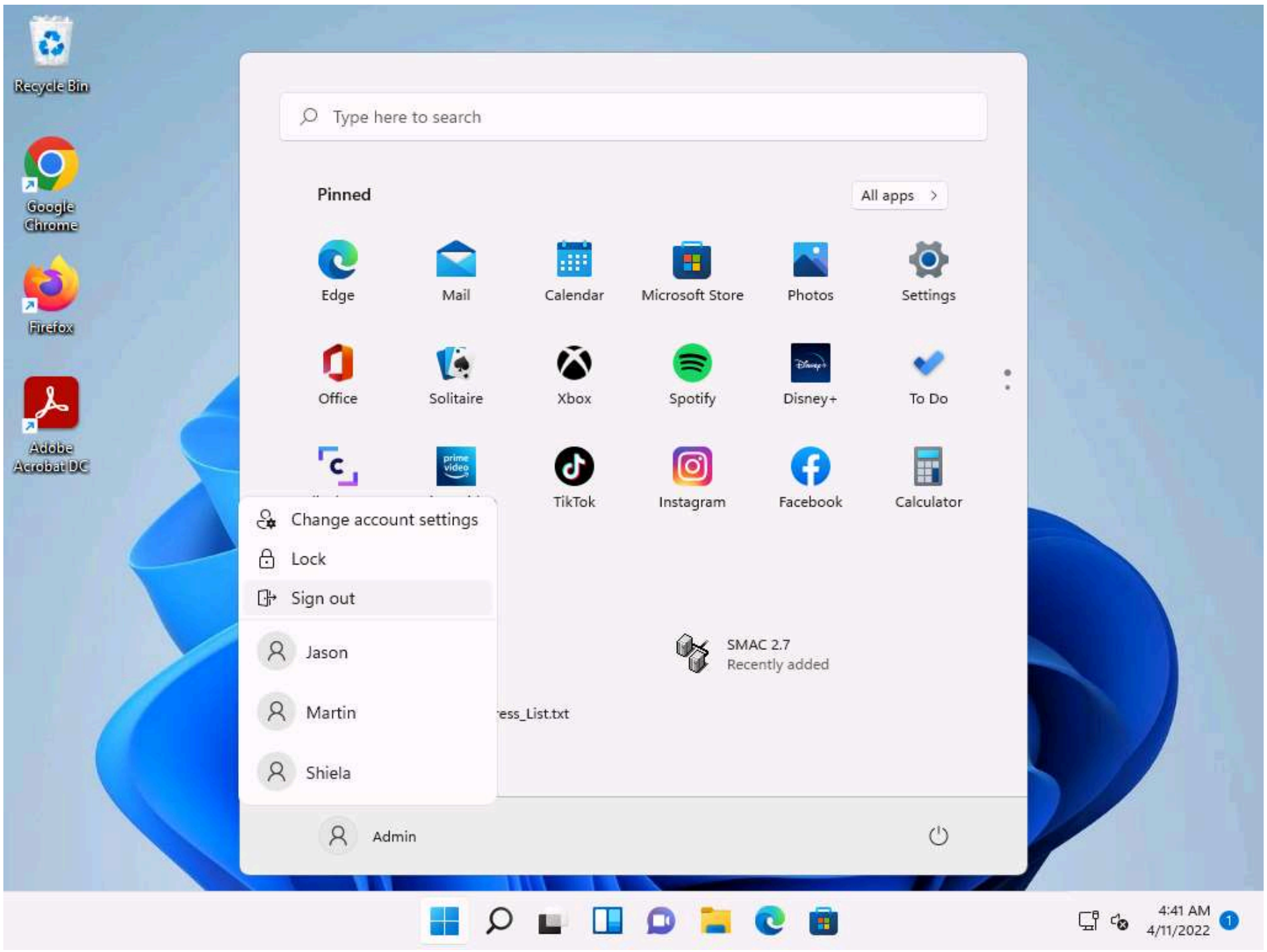
19. **Wireshark** will now display the sniffed password from the captured packets.

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



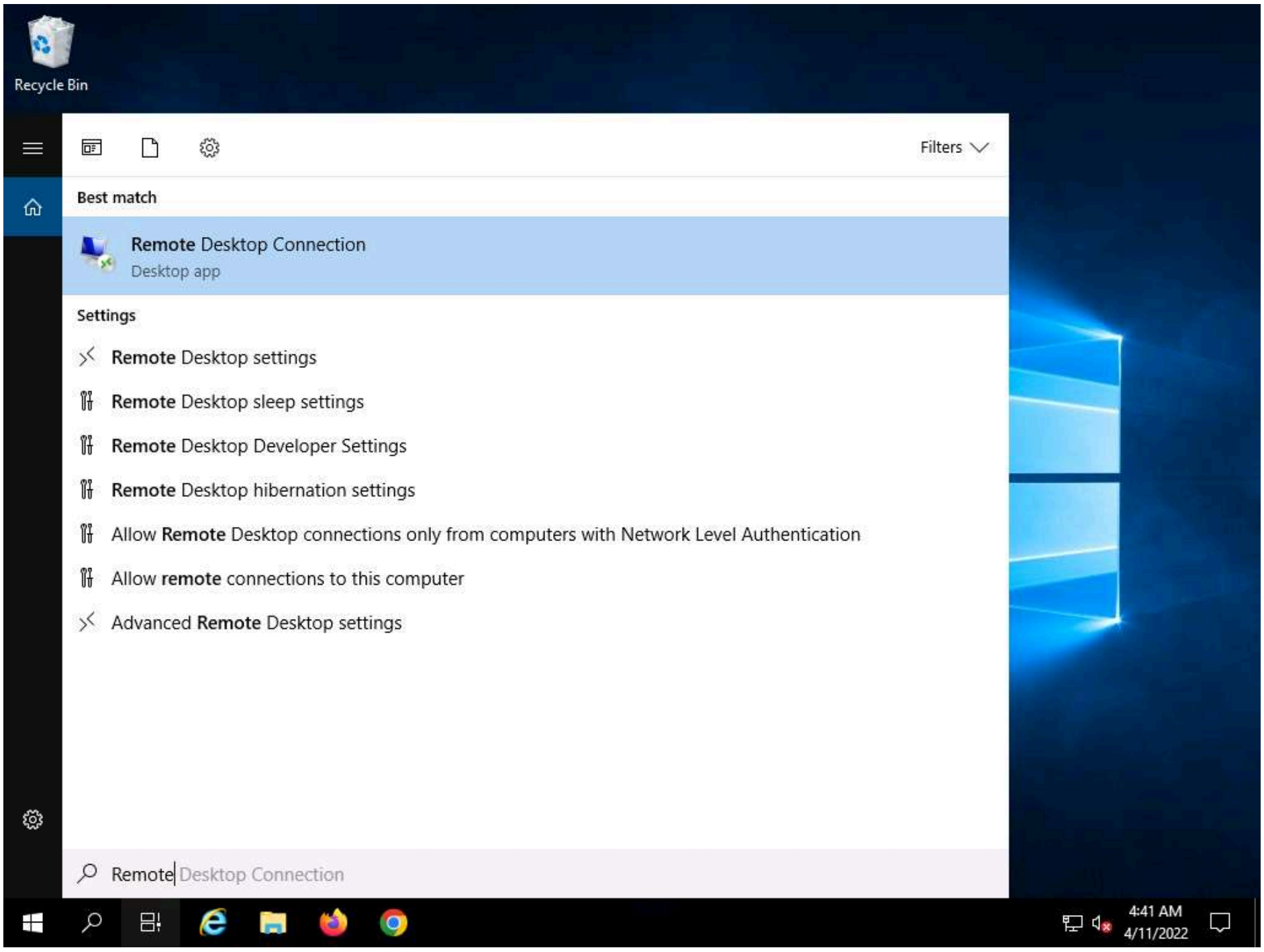
21. Close the **Wireshark** window.

22. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, close the web browser, and sign out from the **Admin** account.



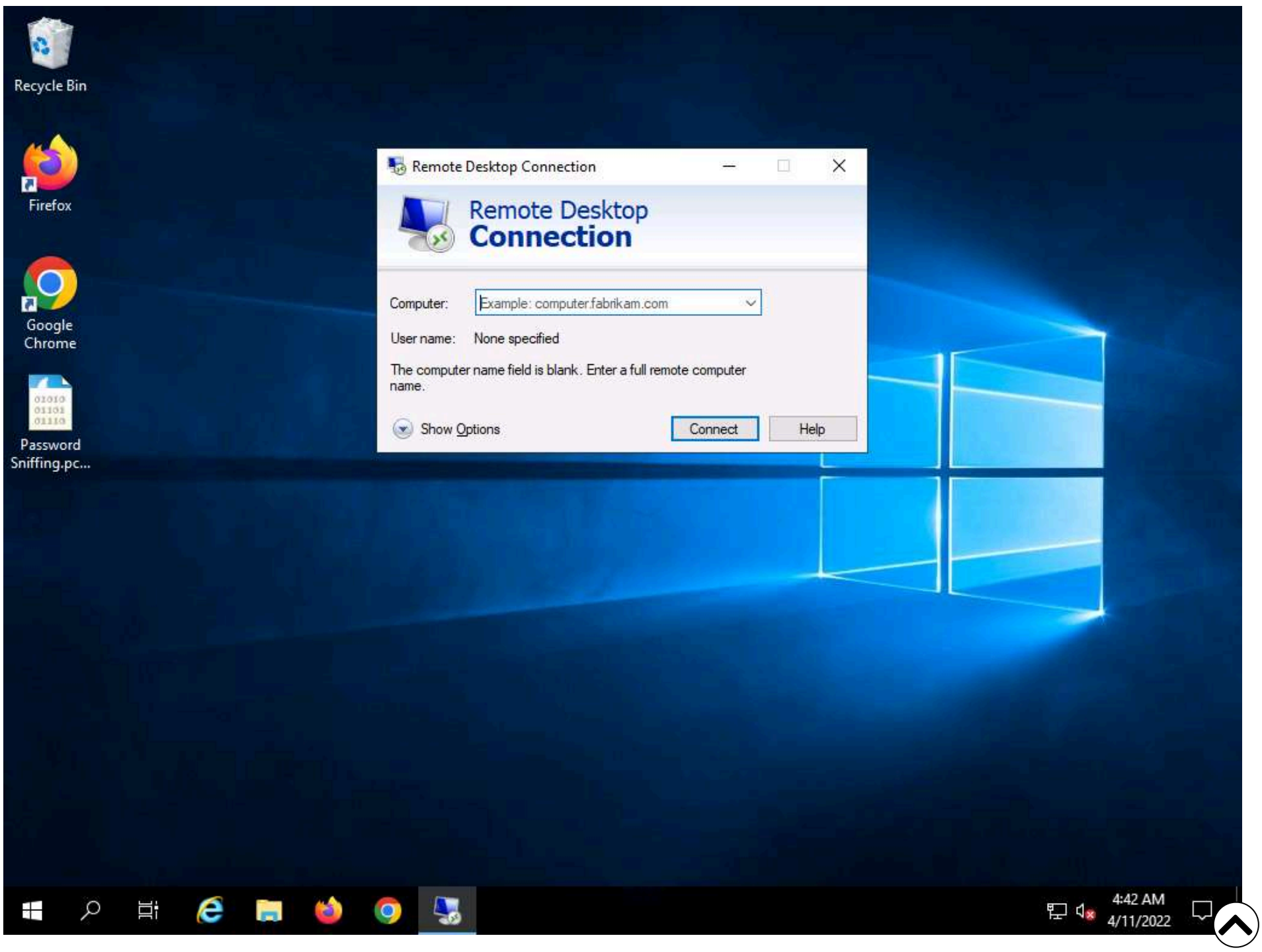
23. Click **CEHv12 Windows Server 2019** to switch back to the **Windows Server 2019** machine.

24. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



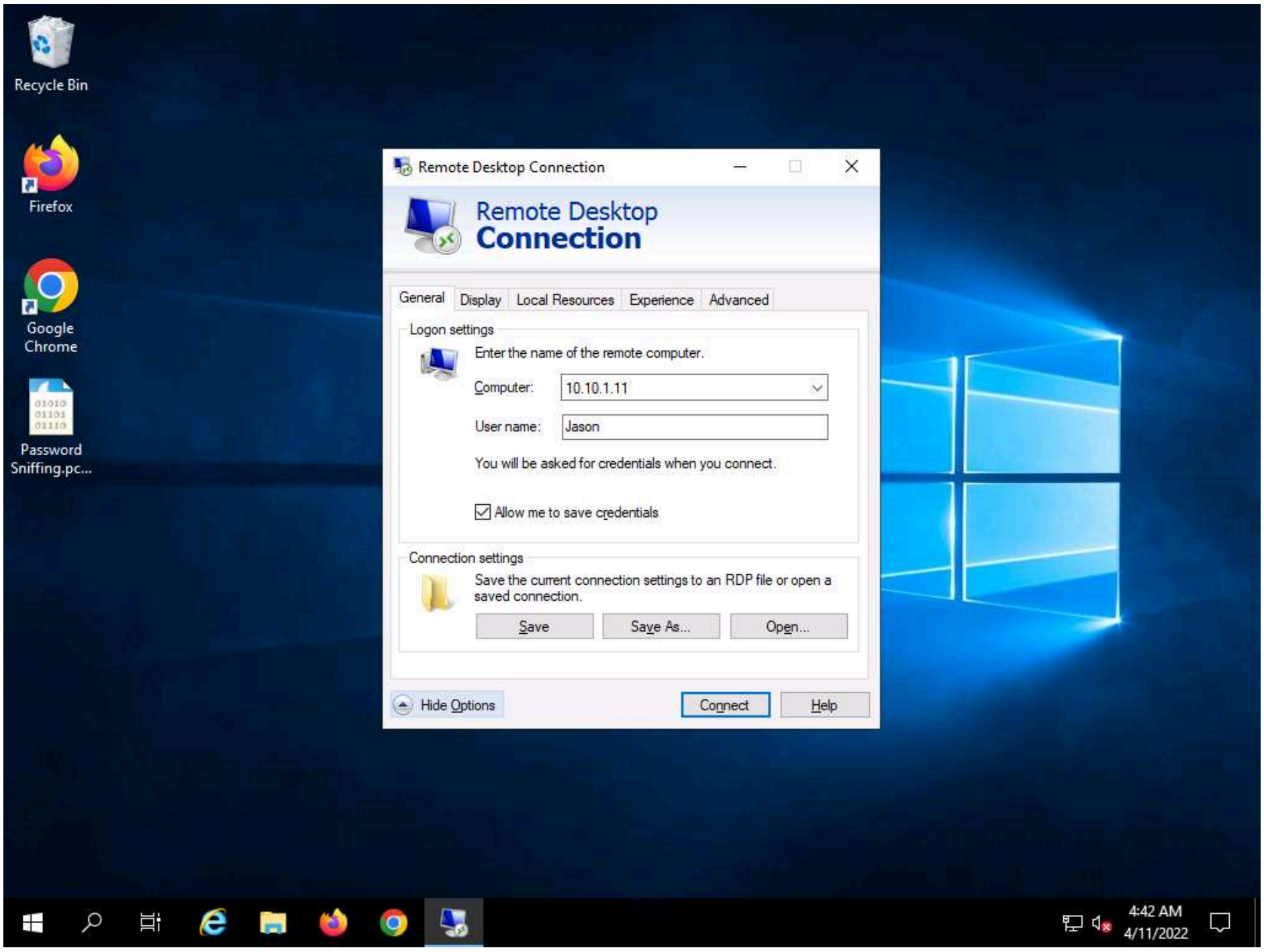
25. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

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



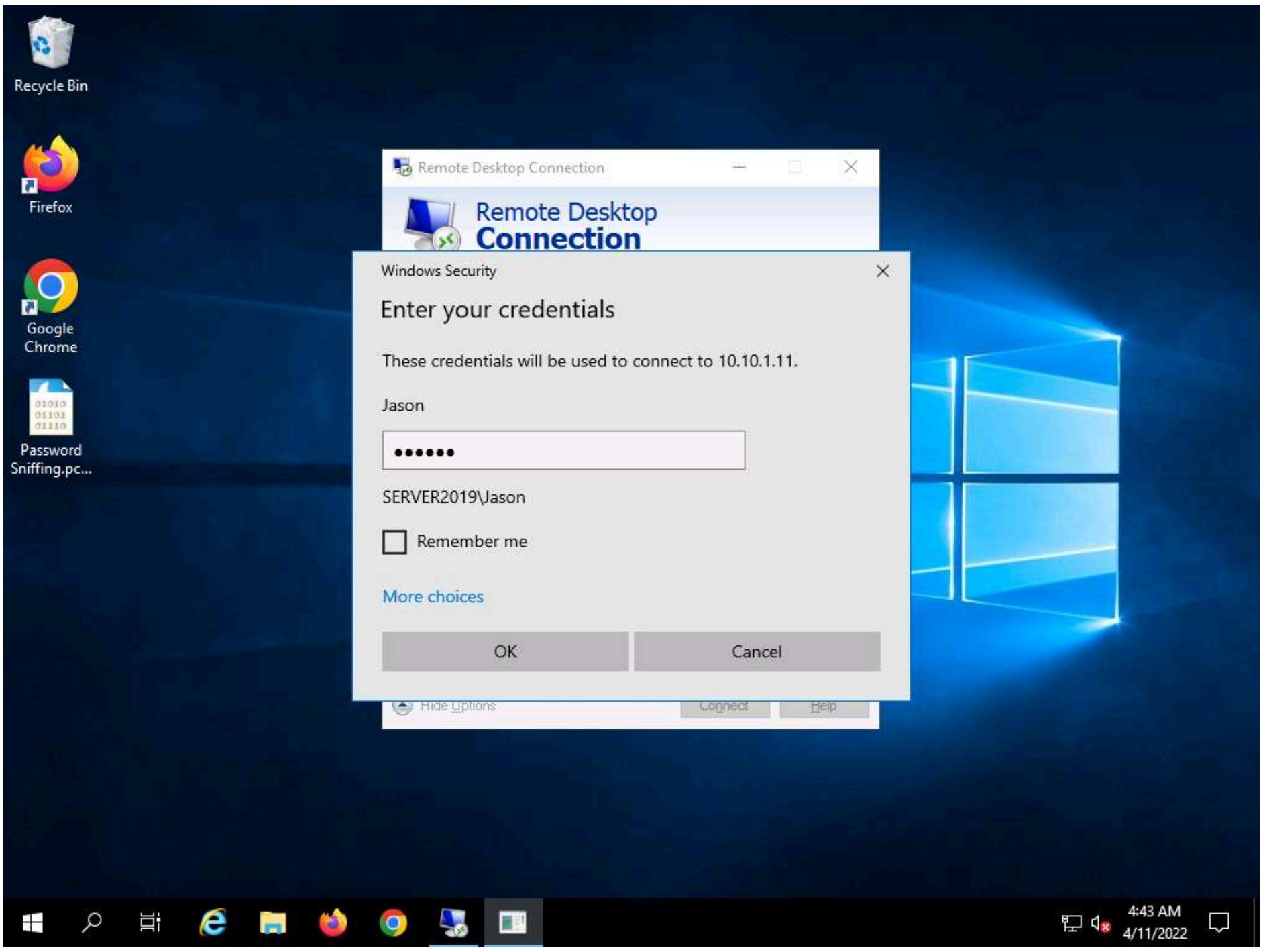
26. The dialog-box expands; under the **General** tab, type **10.10.1.11** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

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

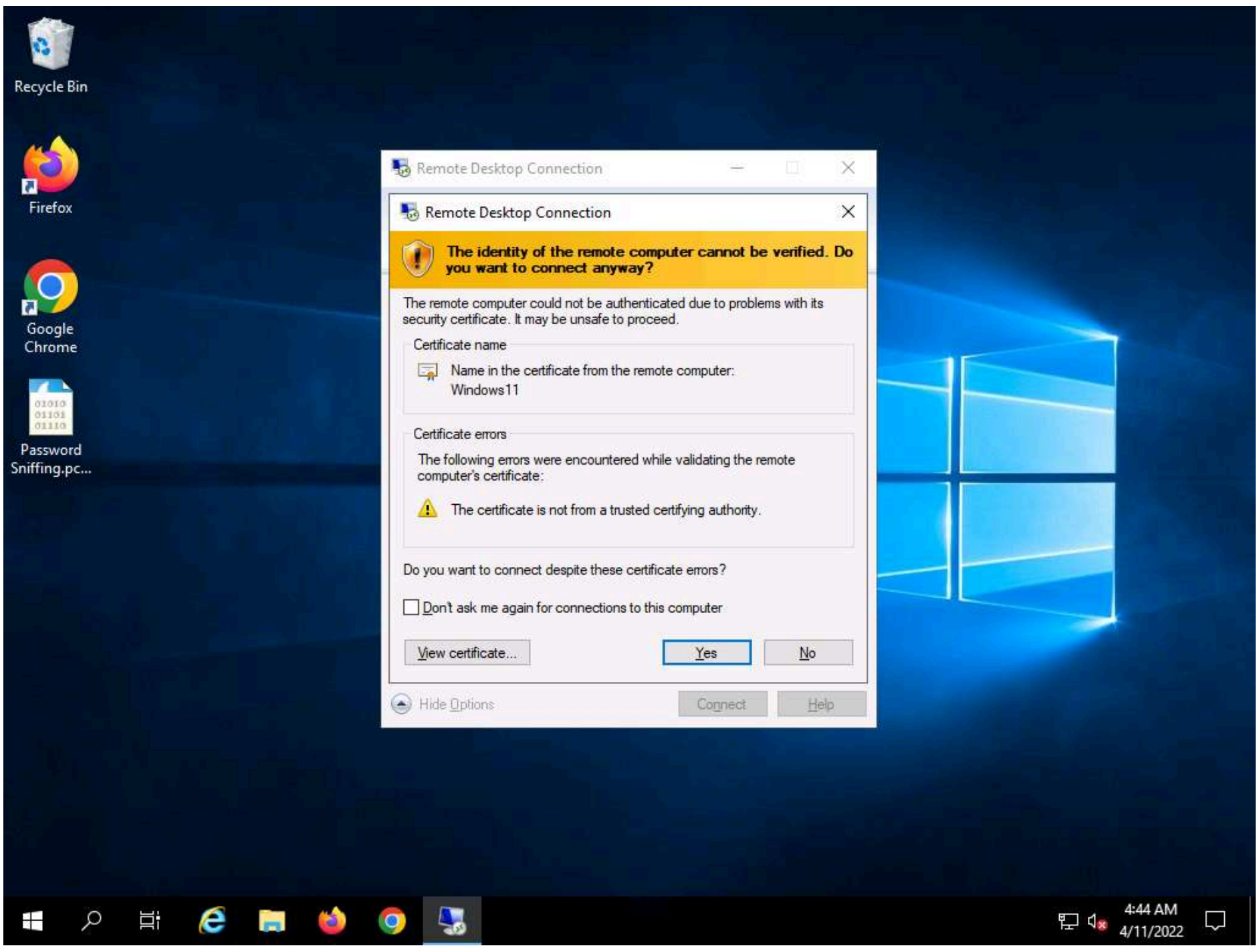


27. The **Windows Security** pop-up appears. Enter **Password** (**qwerty**) and click **OK**.

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

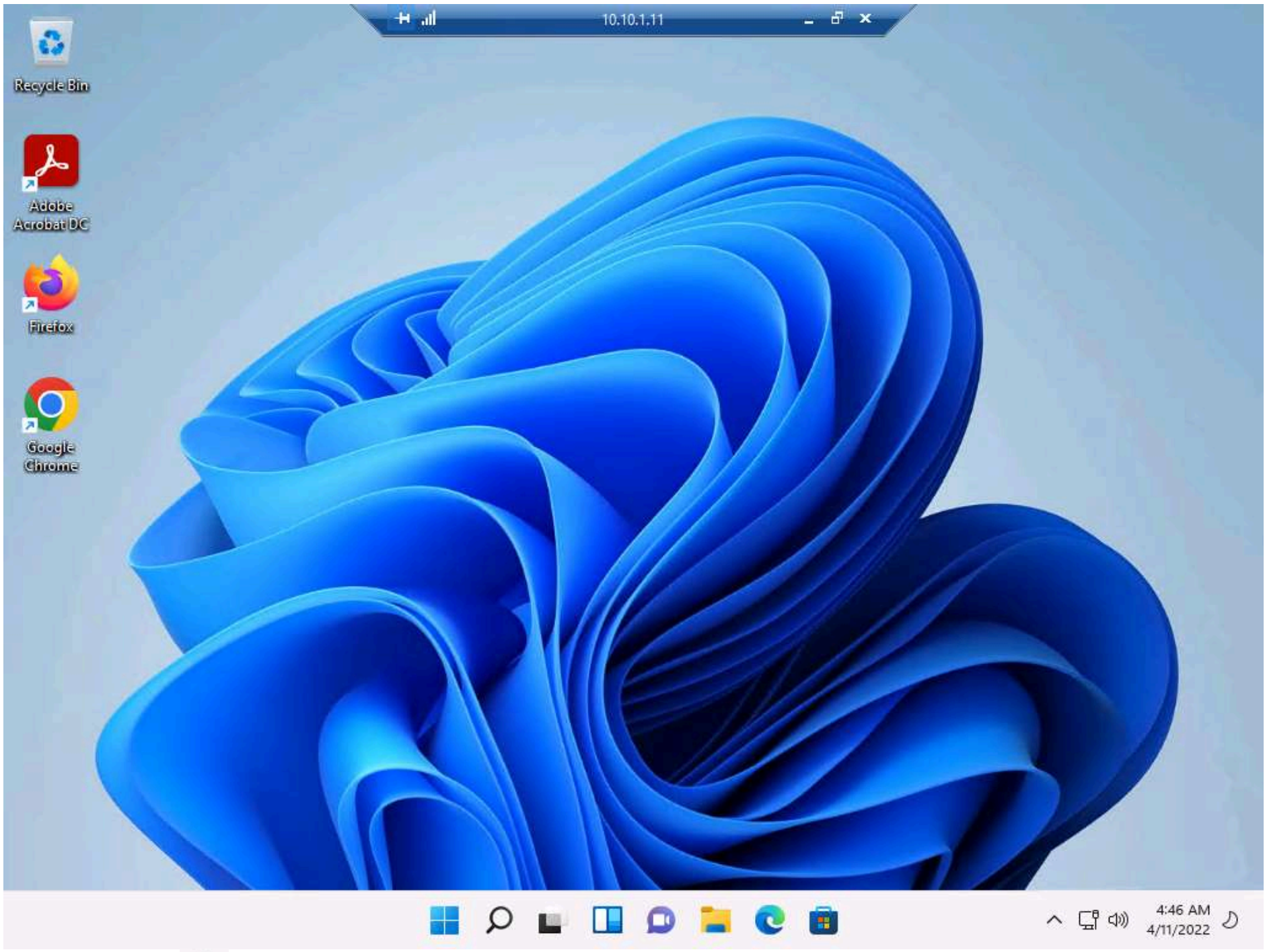


28. The **Remote Desktop Connection** pop-up appears; click **Yes**.

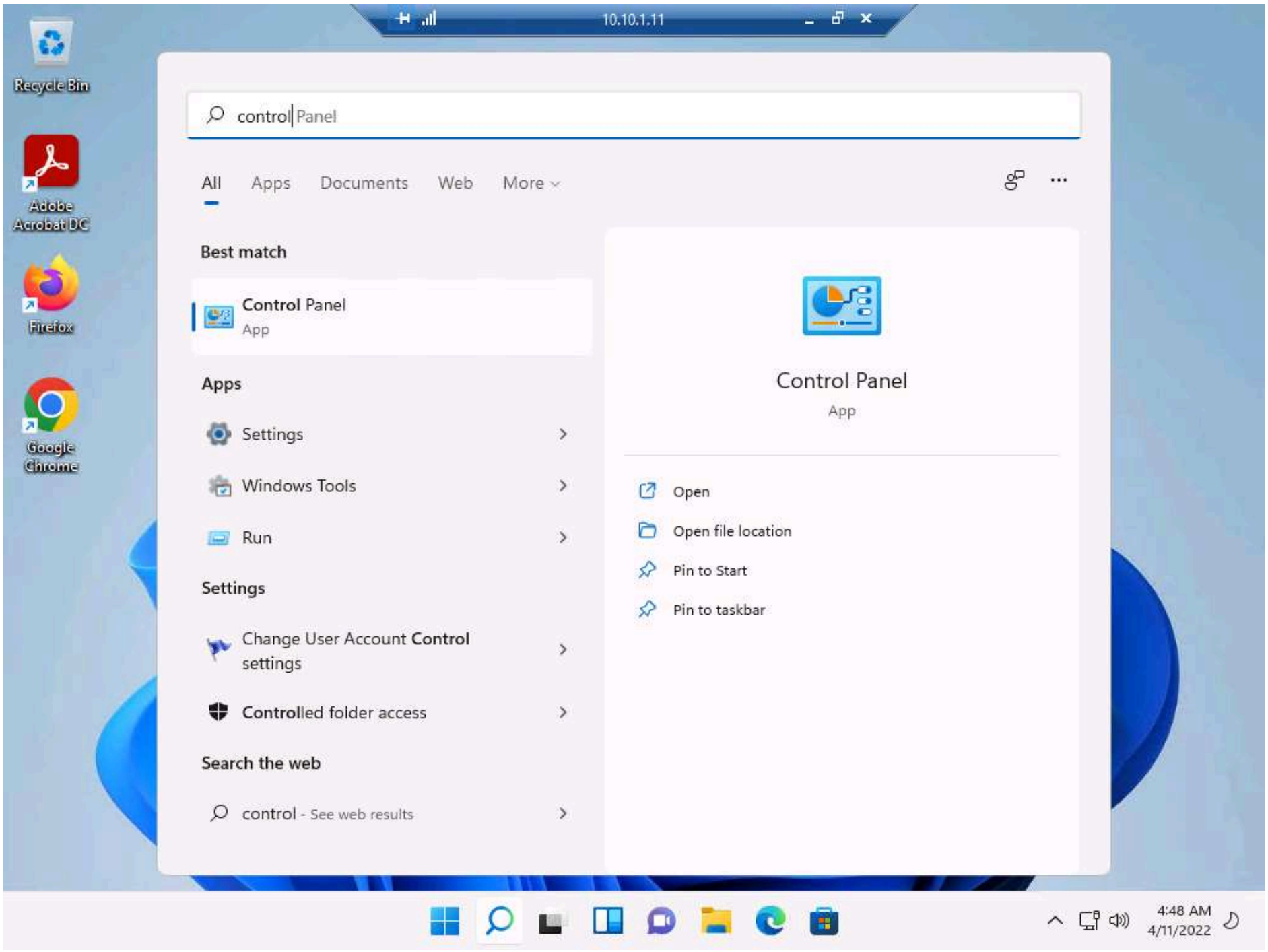


29. A remote connection to the target system (**Windows 11**) appears, as shown in the screenshot.

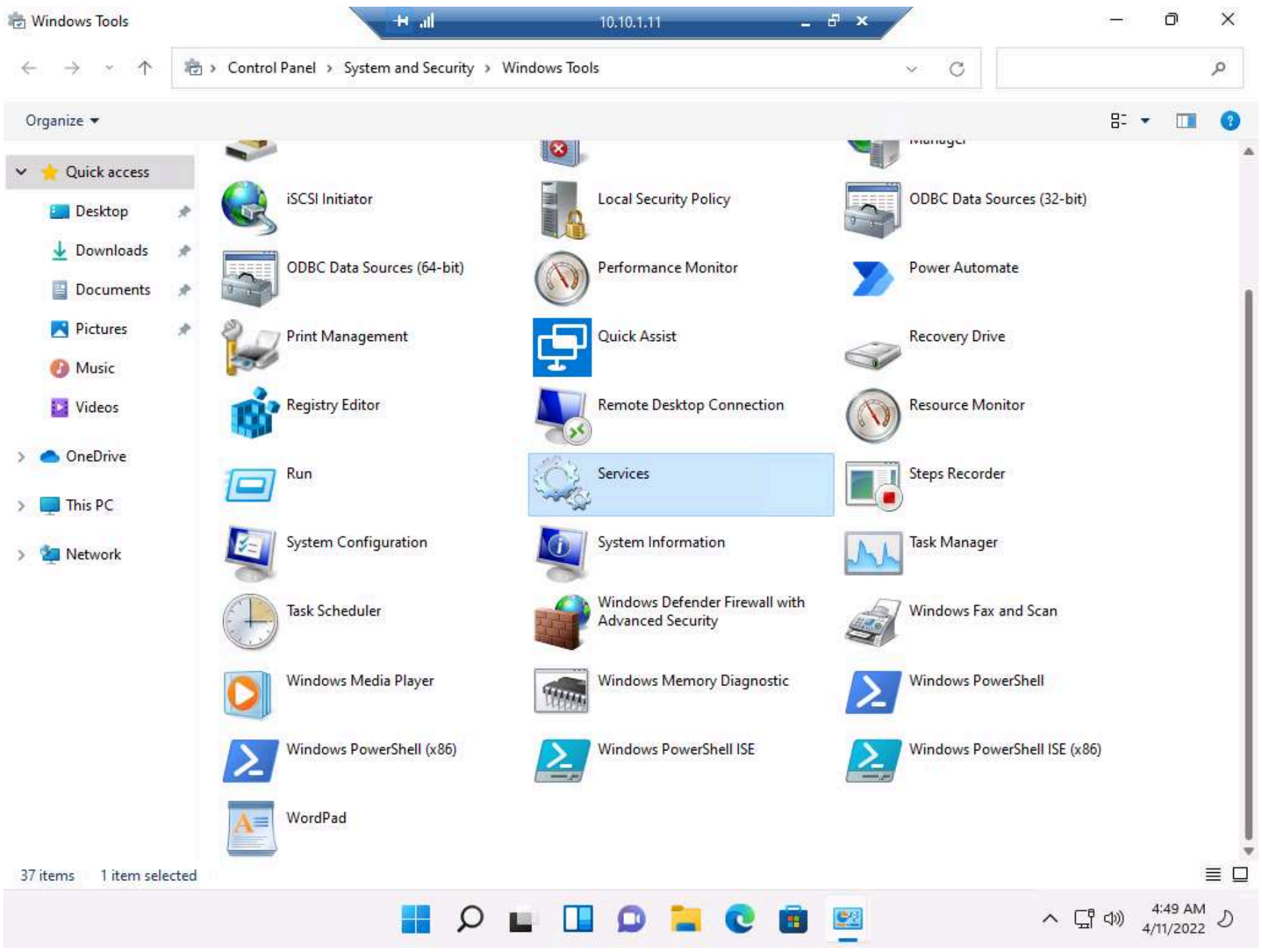
Note: If a **Choose privacy settings for your device** window appears, click on **Next** in the next window click on **Next** and in the next window click on **Accept**.



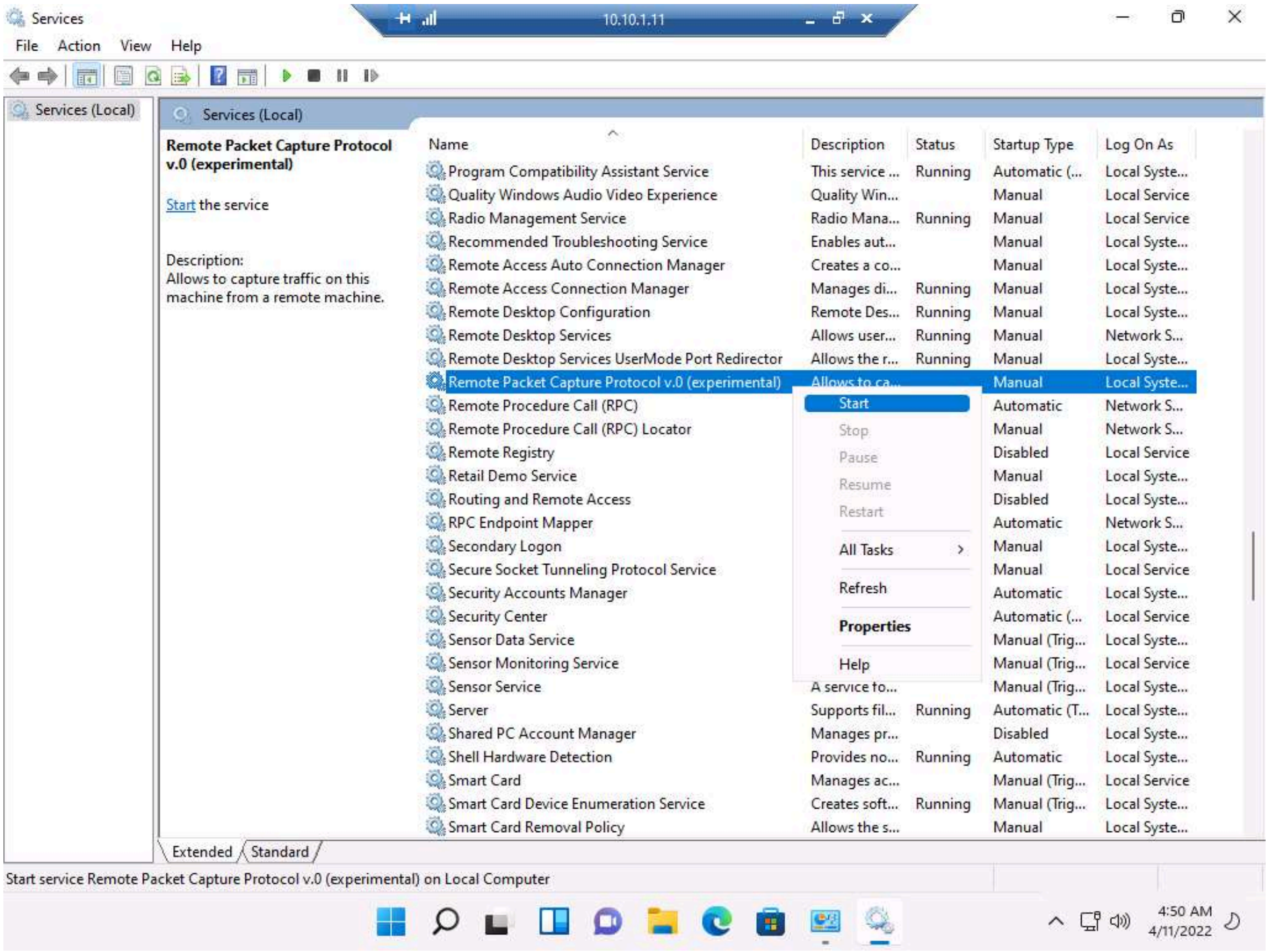
30. Click **Search** icon ( ) on the **Desktop**. Type **Control** in the search field, the **Control Panel** appears in the results, click **Open** to launch it.



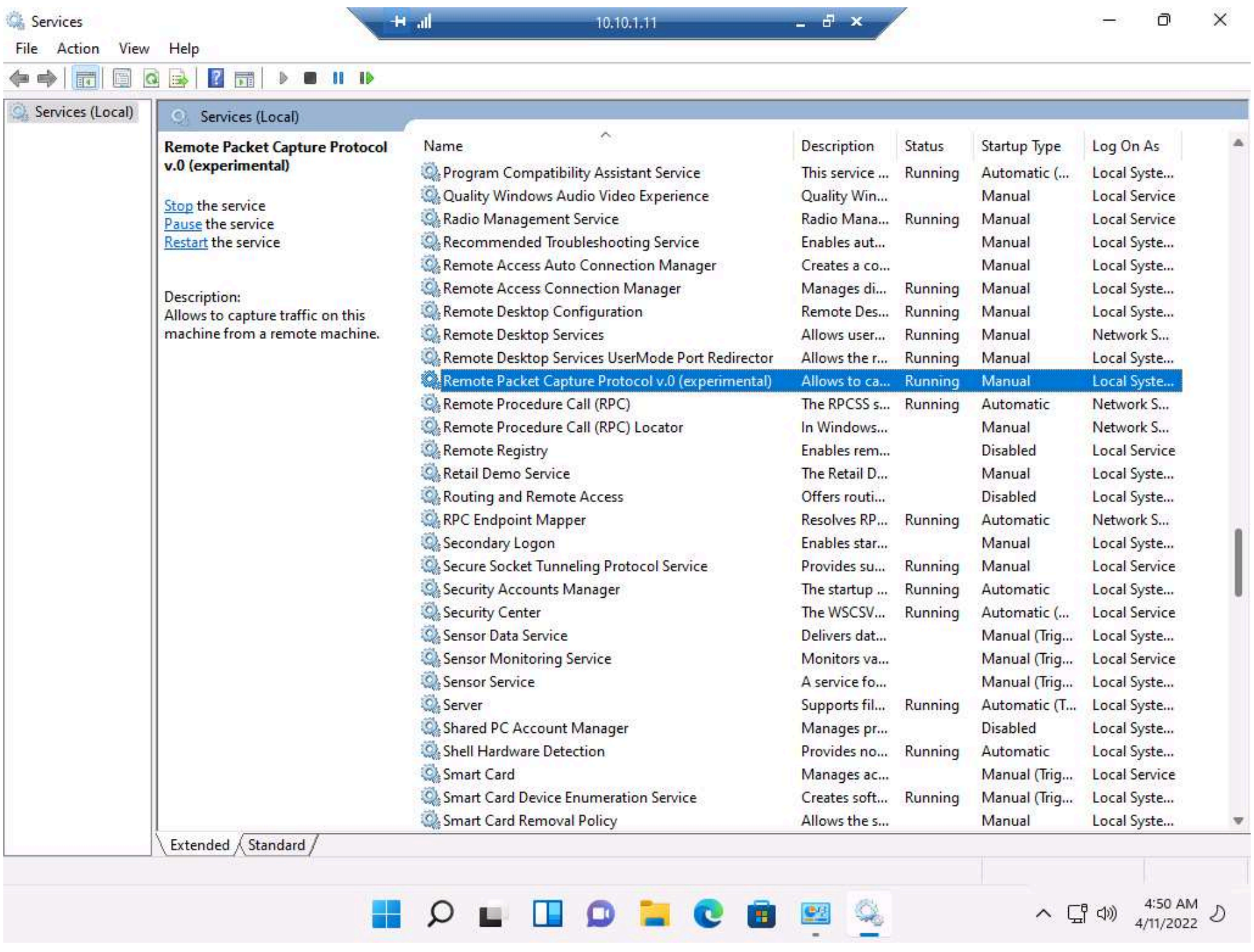
31. The **Control Panel** window appears; navigate to **System and Security --> Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.



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



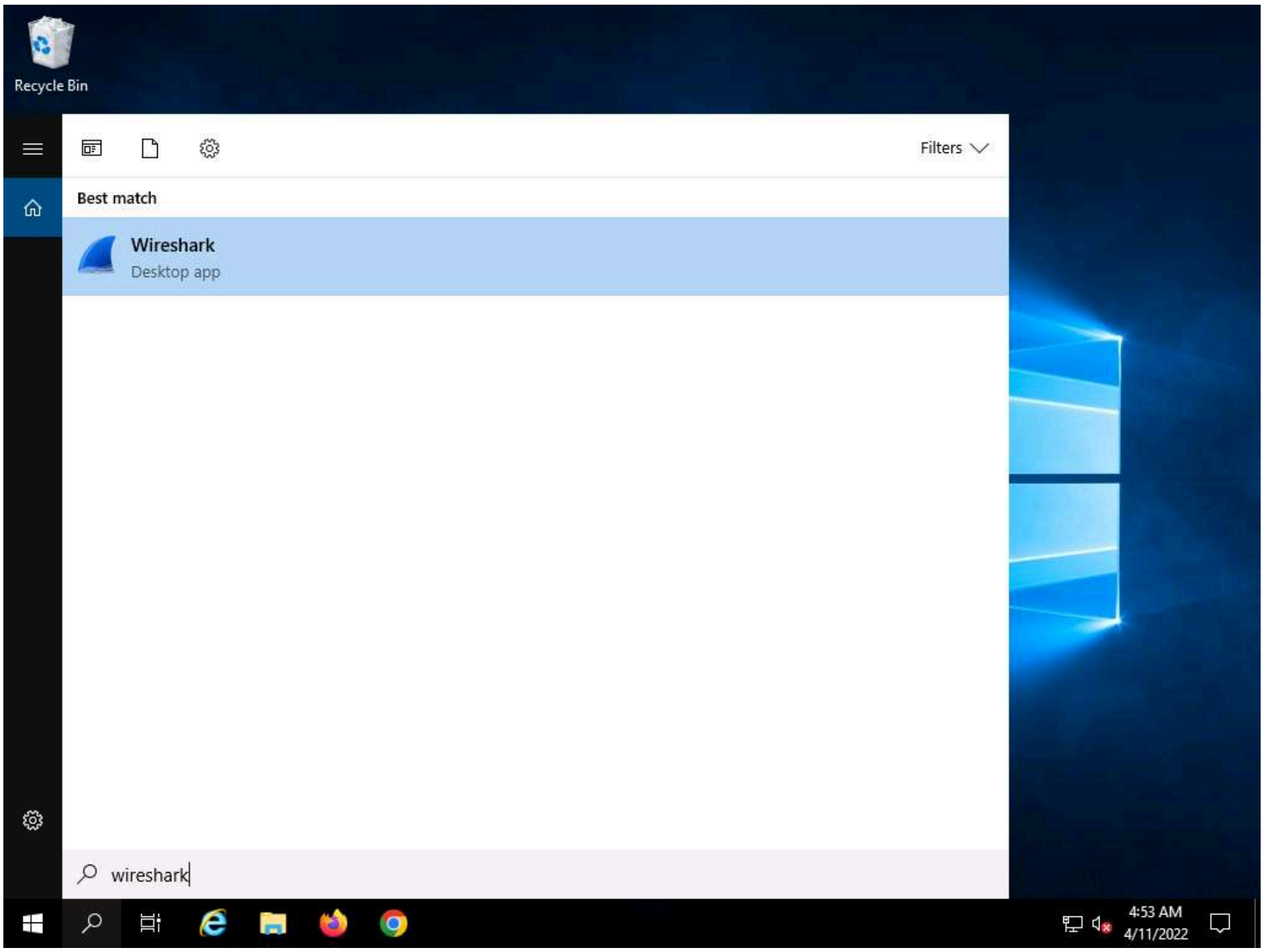
33. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.



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

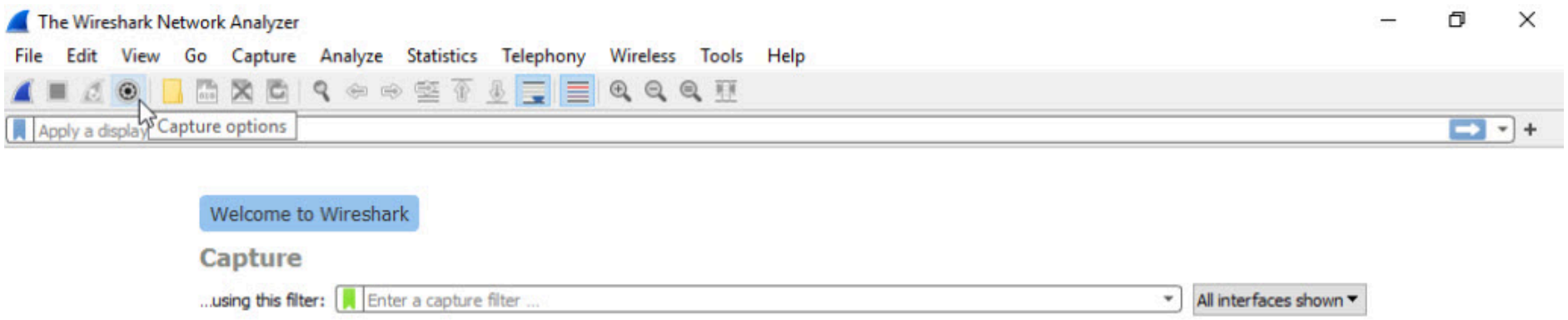
Note: If a **Remote Desktop Connection** pop-up appears, click **OK**.

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

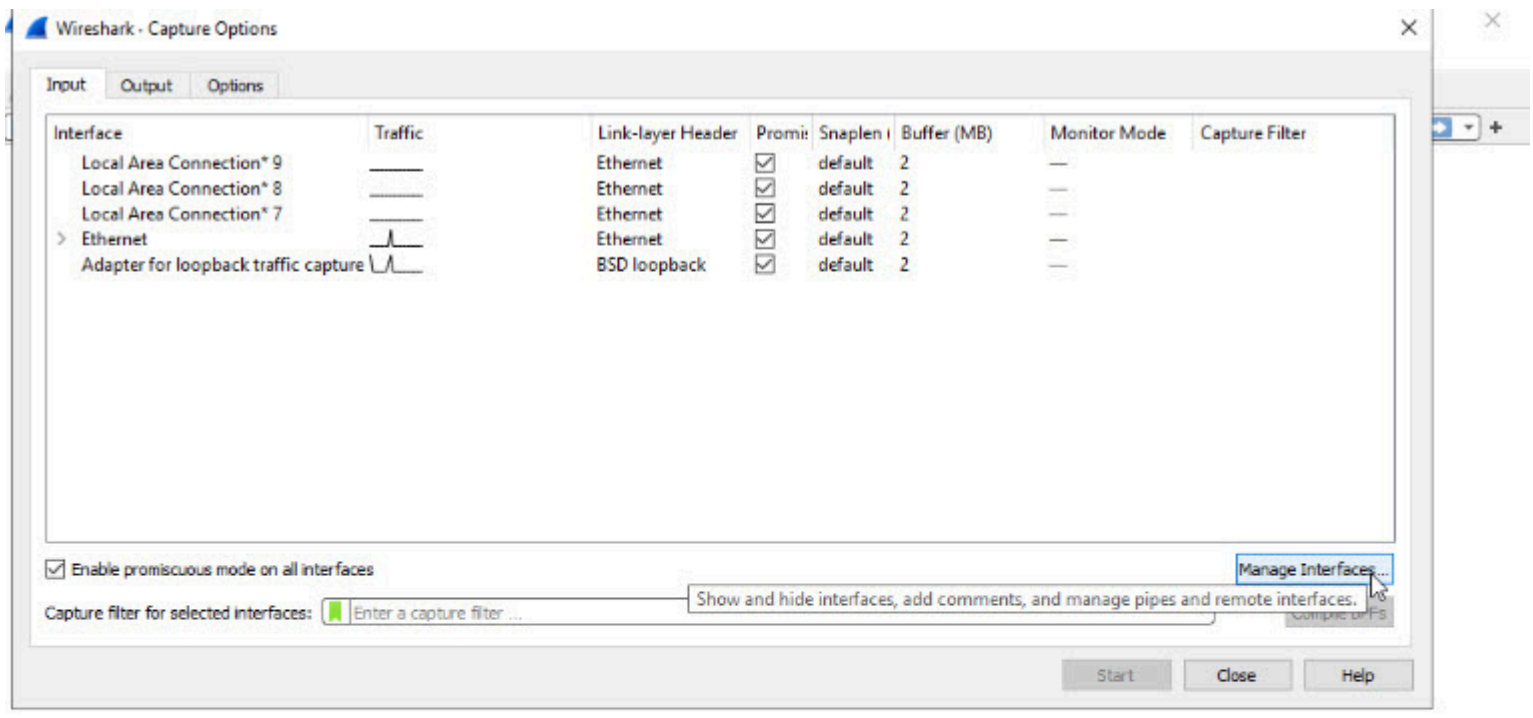


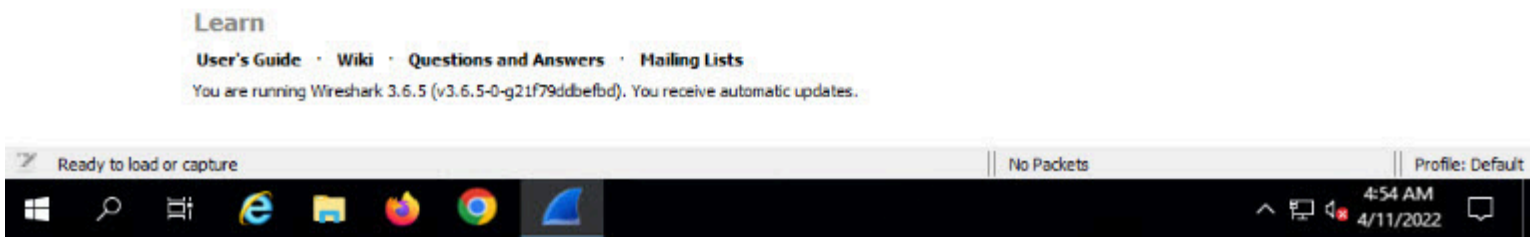
36. The **Wireshark Network Analyzer** window appears; click the **Capture options** icon from the toolbar.

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

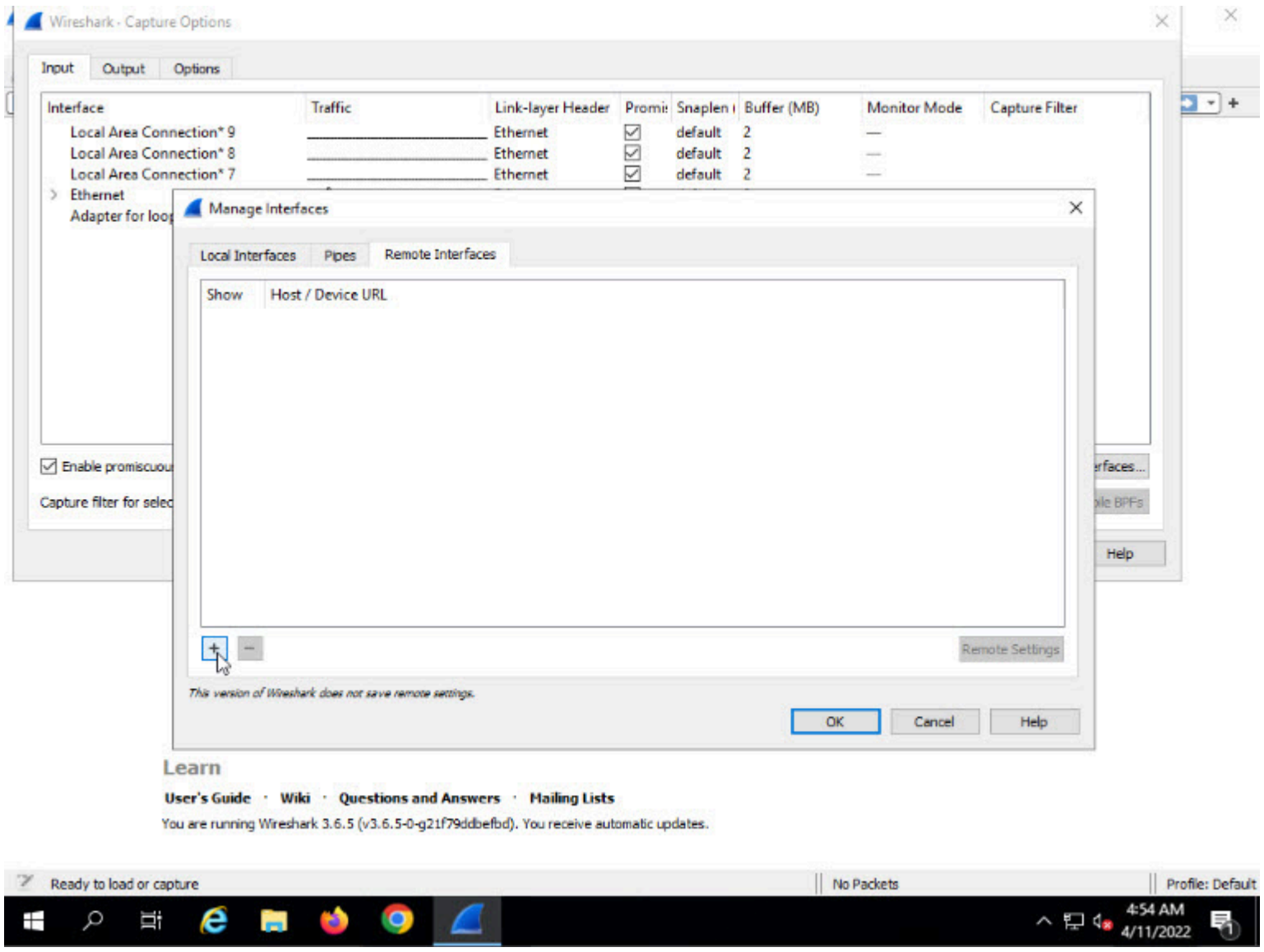


37. The **Wireshark**. **Capture Options** window appears; click the **Manage Interfaces...** button.





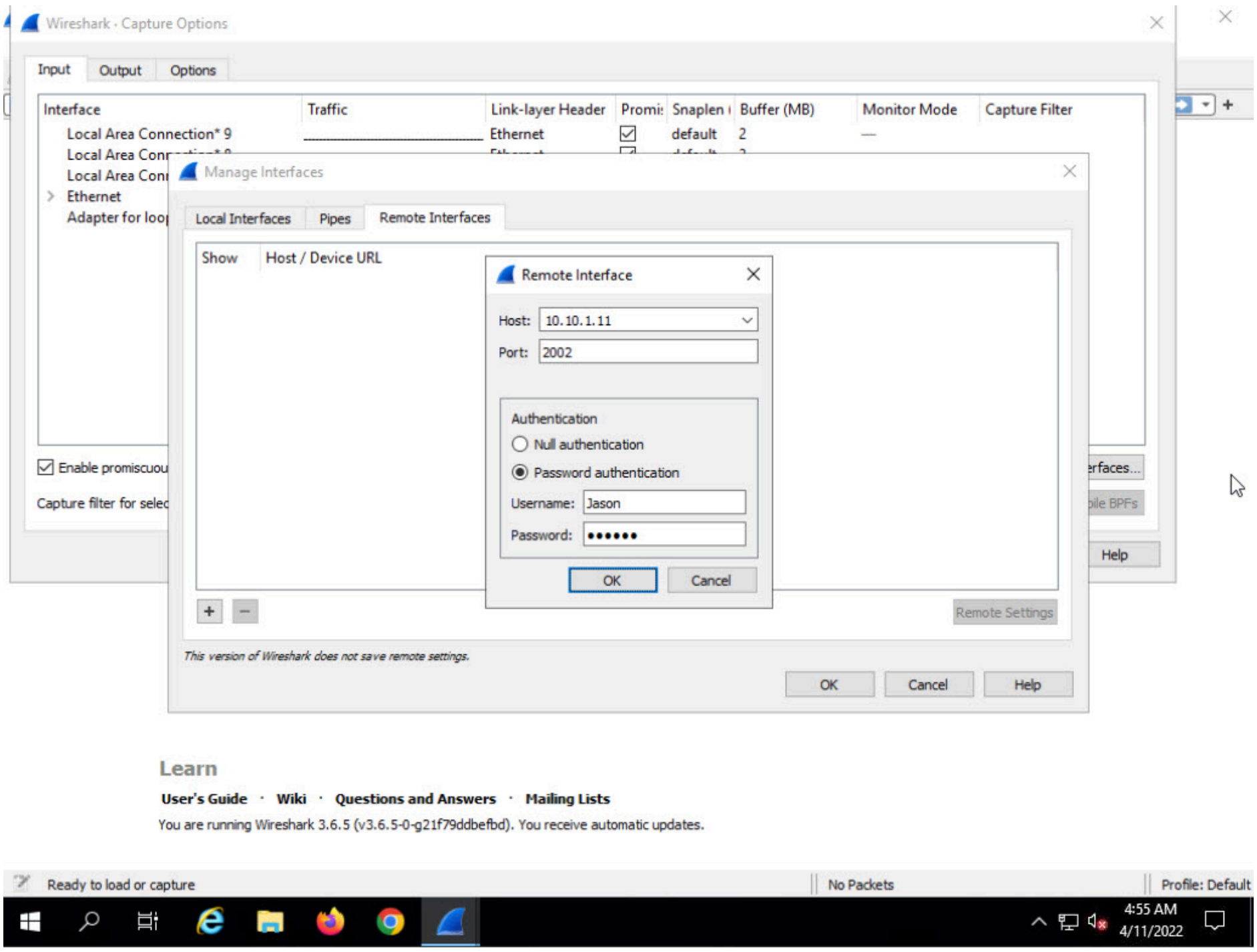
38. The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface** icon (+).



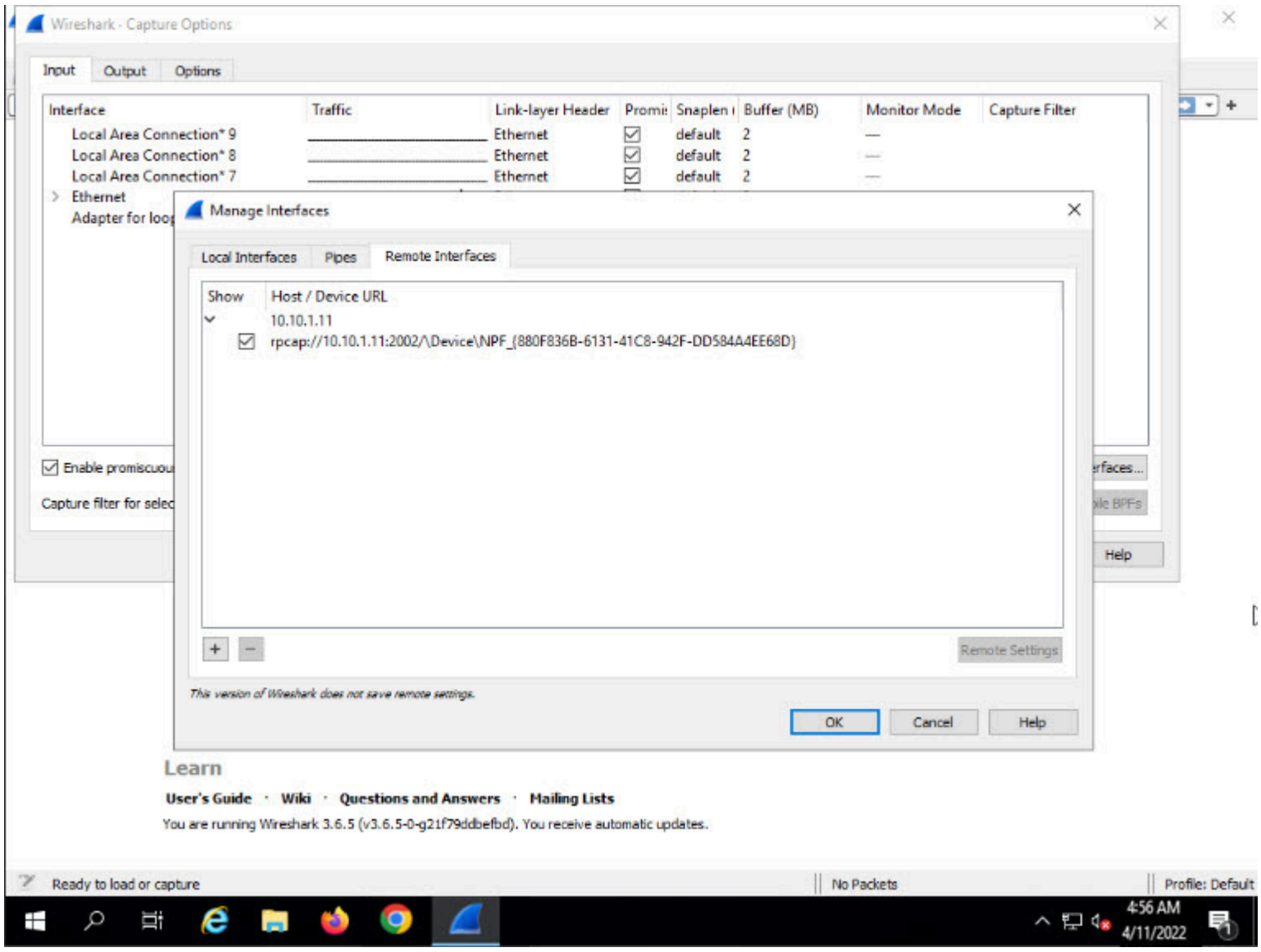
39. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.1.11**); and in the **Port** field, enter the port number as **2002**.

40. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.

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

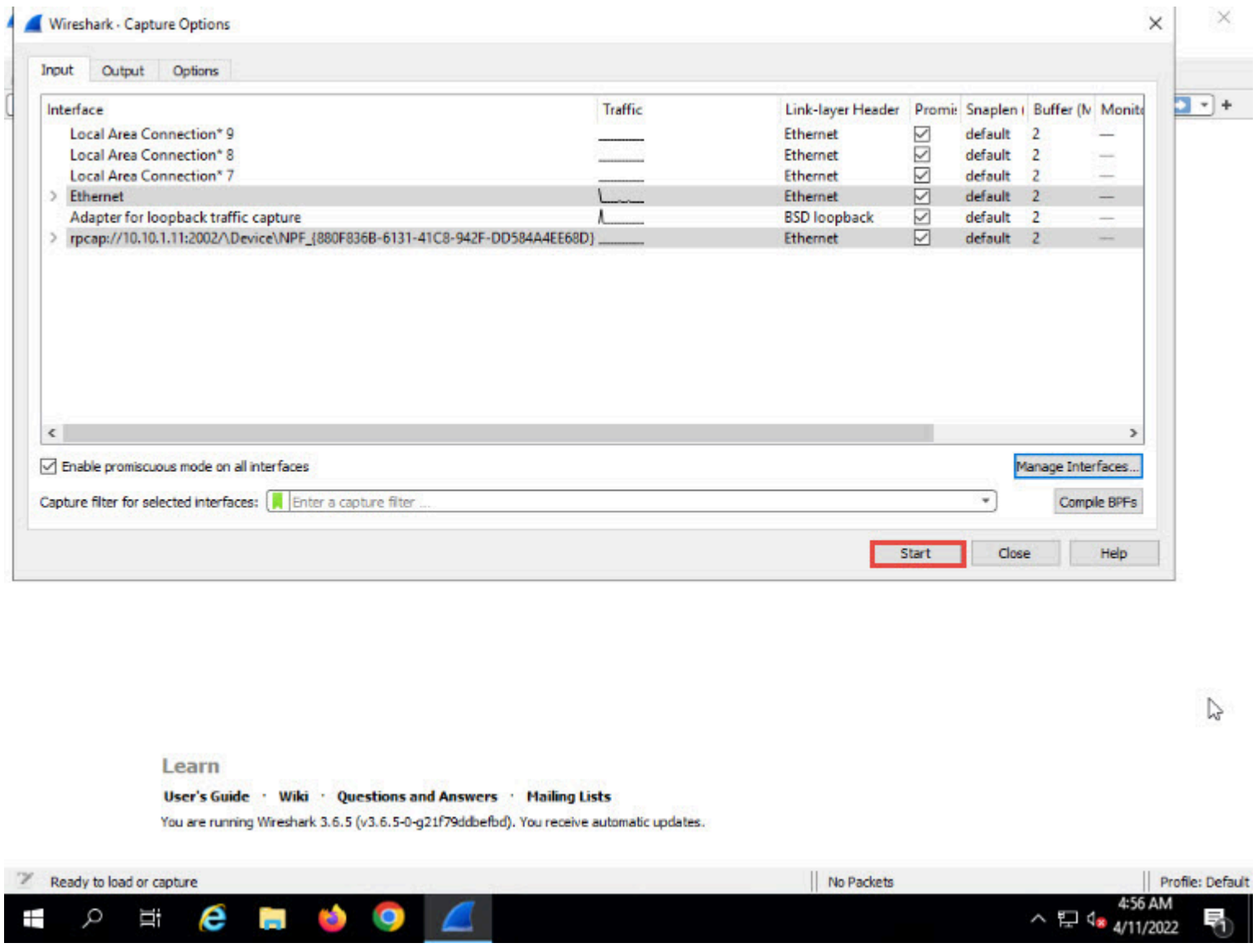


41. A new remote interface is added to the **Manage Interfaces** window; click **OK**.

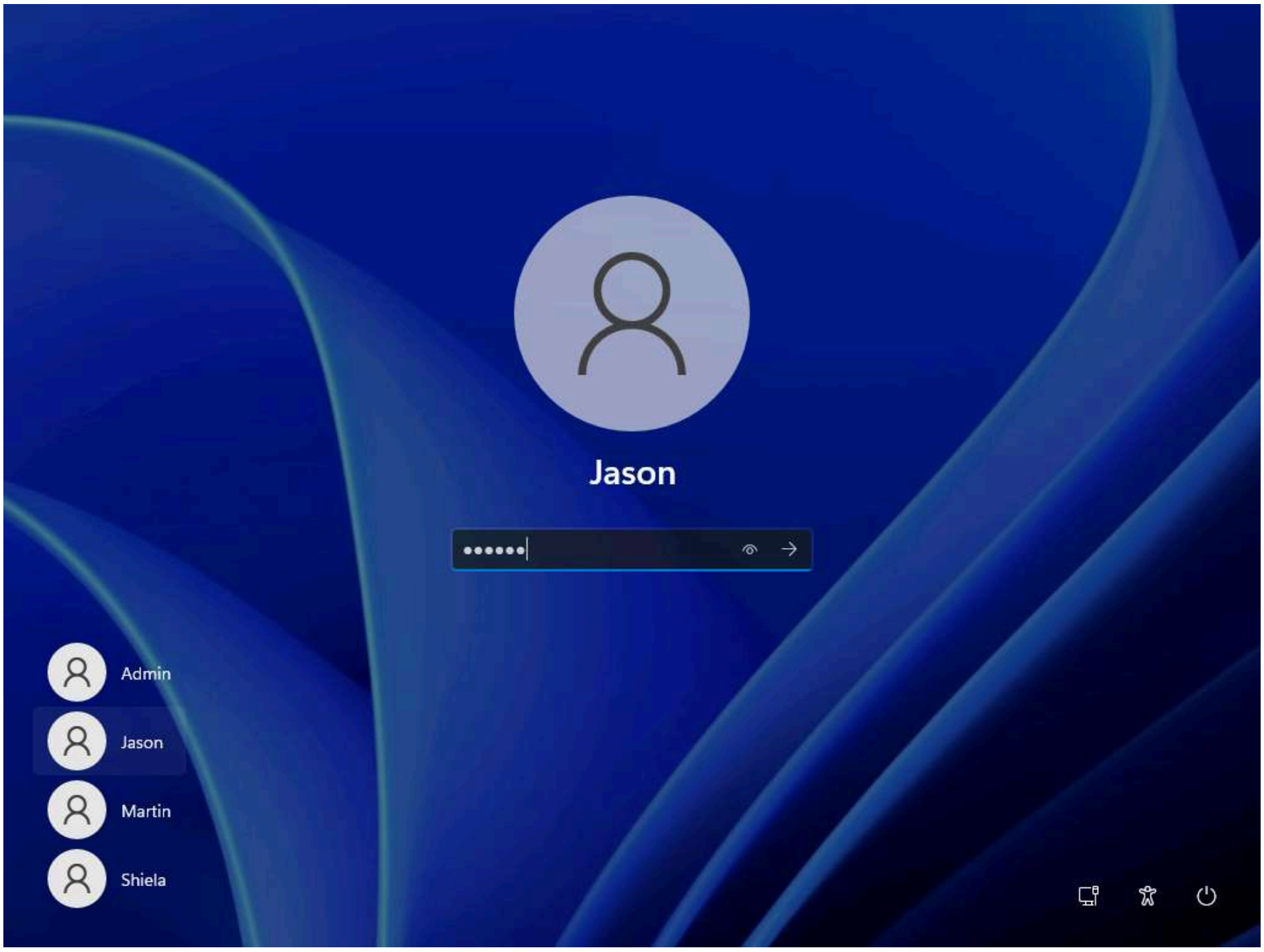


42. The newly added remote interface appears in the **Wireshark**. **Capture Options** window; click **Start**.

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

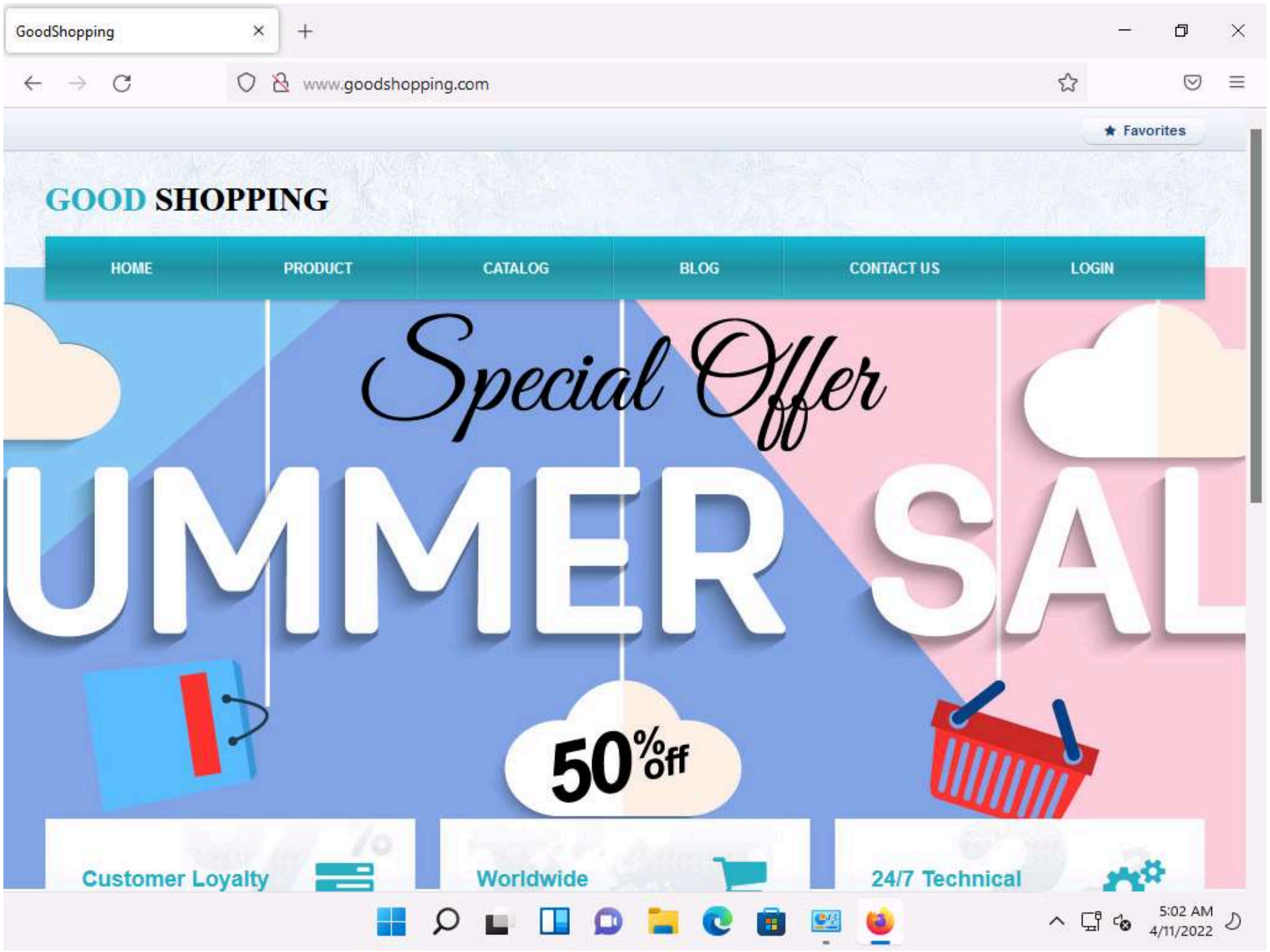


43. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**. Select **Jason** from the list of user accounts in the left-pane, click **qwerty** to enter the password and press **Enter** to log in. Here, you are signing in as the victim.

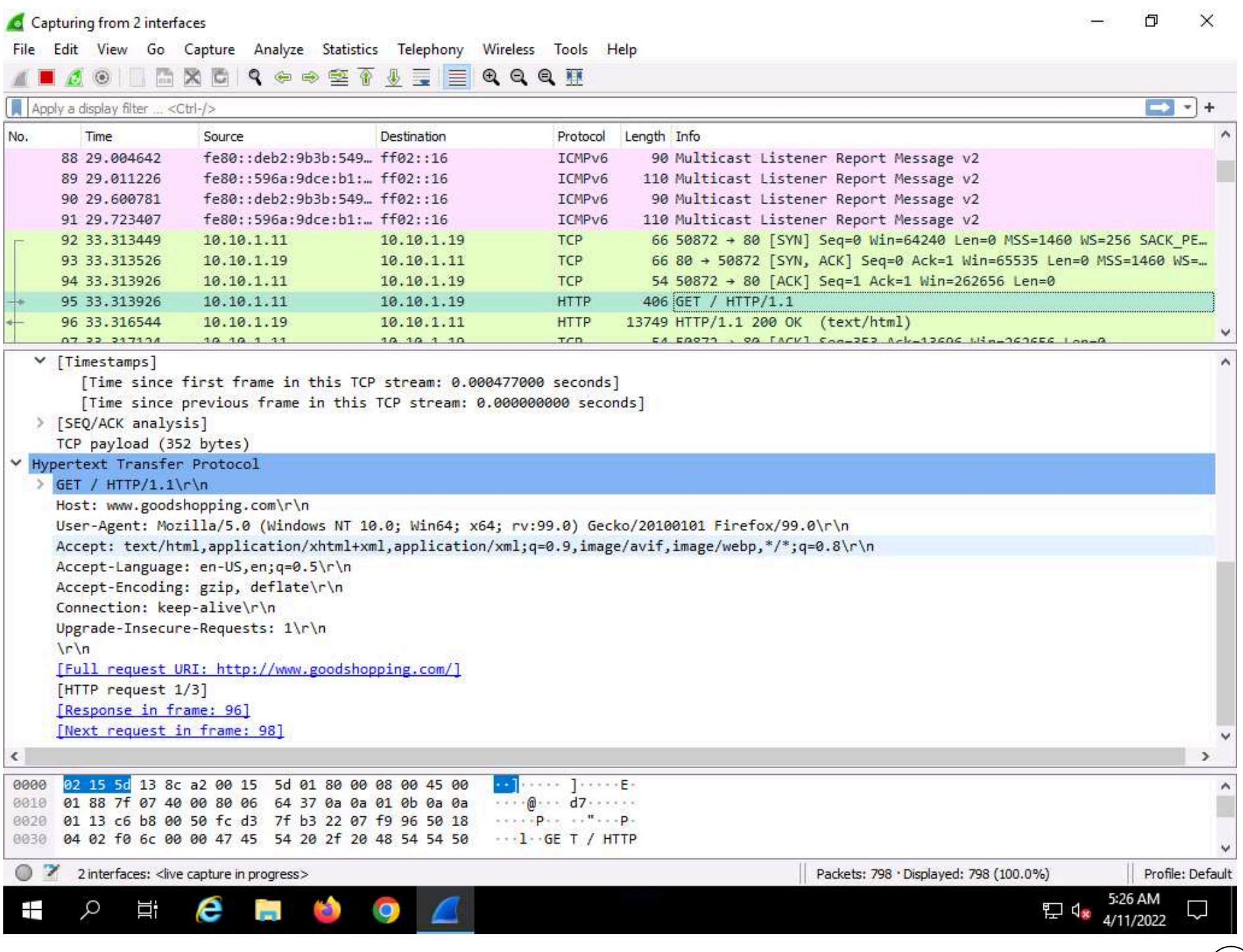


44. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **http://www.goodshopping.com**).

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



45. Click **CEHv12 Windows Server 2019** to switch back to the **Windows Server 2019** machine. **Wireshark** starts capturing packets as soon as the user (here, you) begins browsing the Internet, the shown in the screenshot.



46. After a while, click the **Stop capturing packet** icon on the toolbar to stop live packet capture.

47. This way, you can use Wireshark to capture traffic on a remote interface.

> Note: In real-time, when attackers gain the credentials of a victim's machine, they attempt to capture its remote interface and monitor the traffic its user browses to reveal confidential user information.

48. This concludes the demonstration of how to perform password sniffing using Wireshark.

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

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

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

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

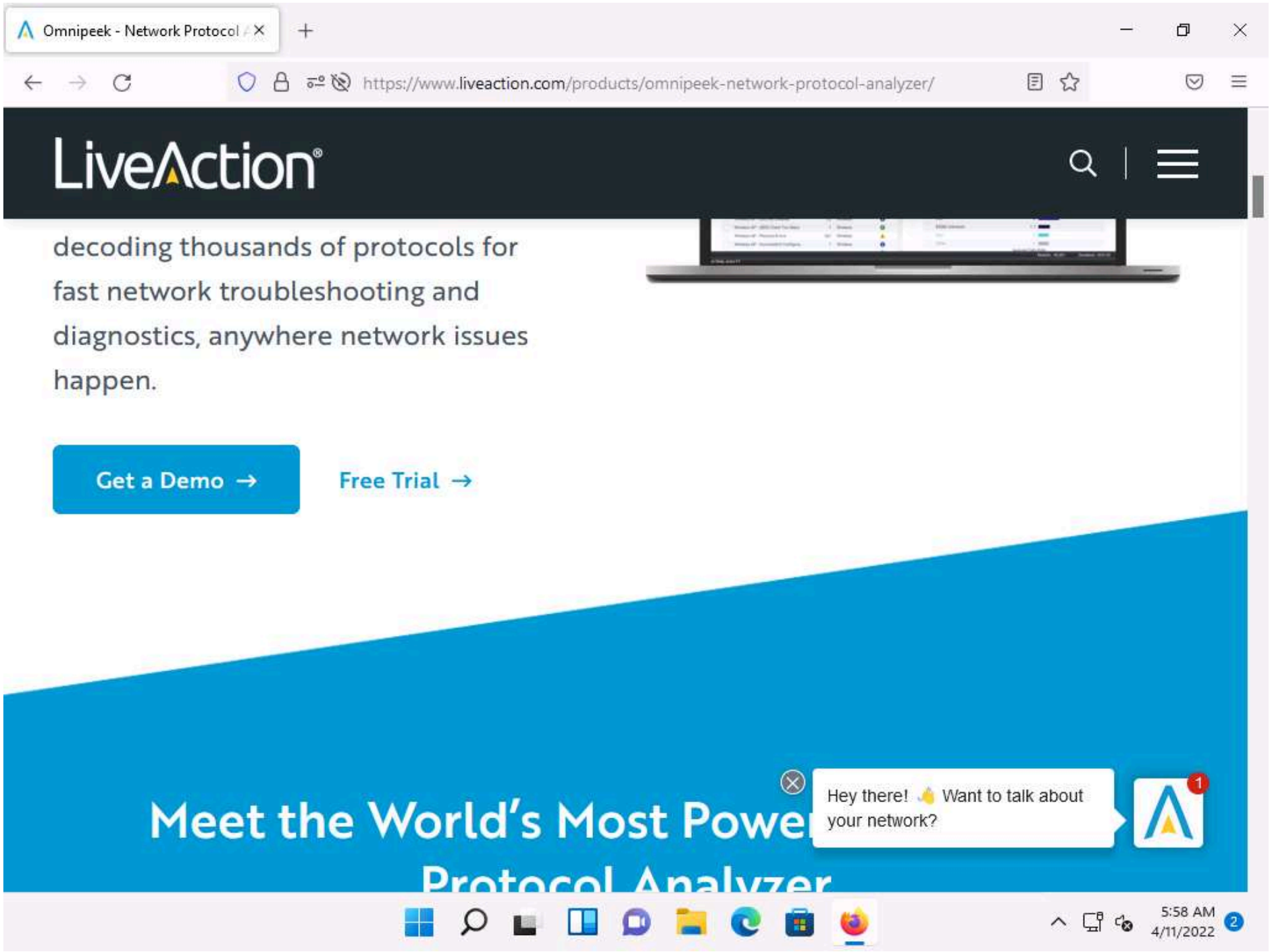
> Note: Before starting this lab, we need to find the User IDs associated with the usernames for the **Windows 11** machine.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/** in the address bar, and press **Enter**.

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

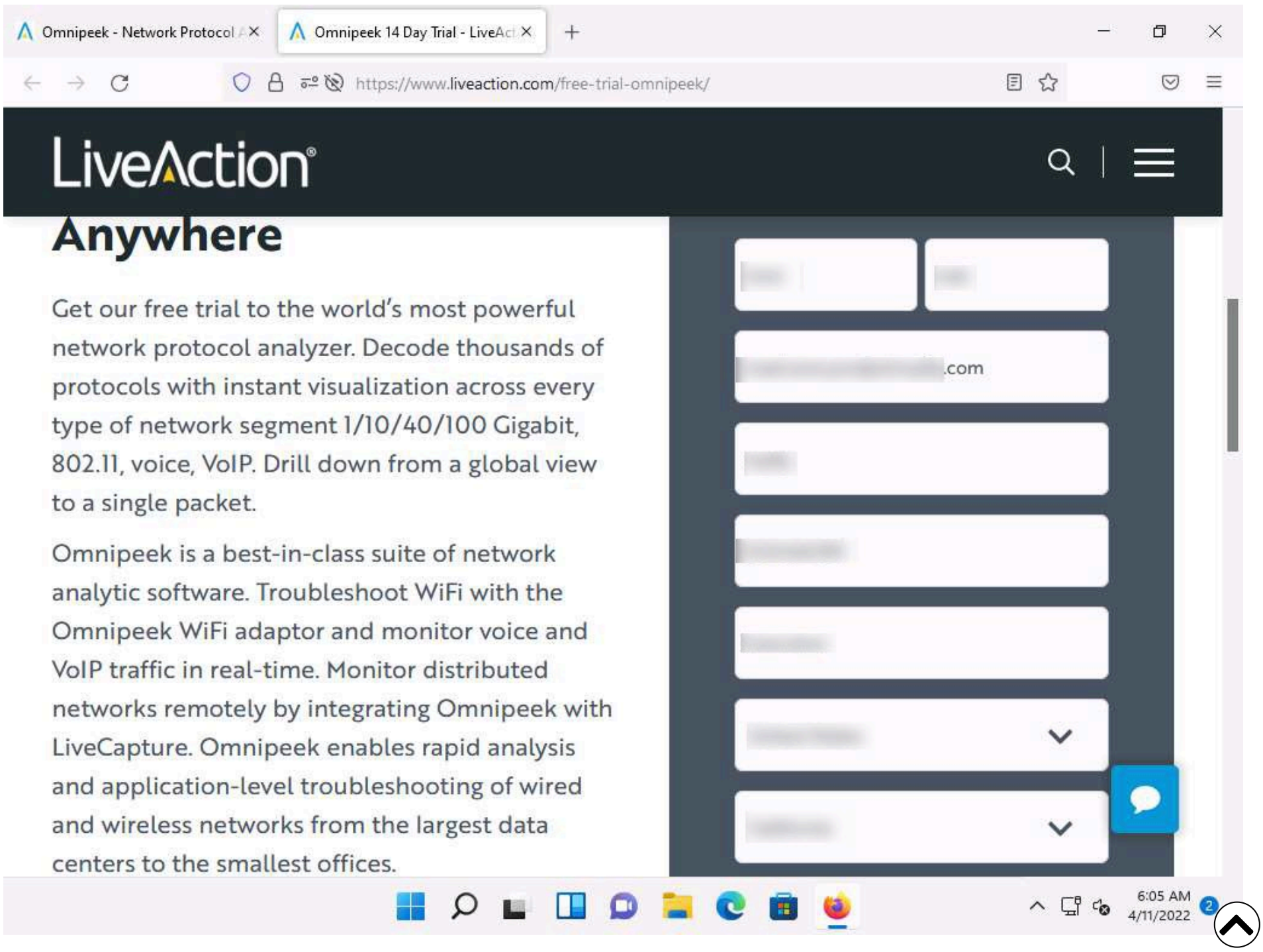
3. The **LiveAction** website appears; click the **Free Trial** button.

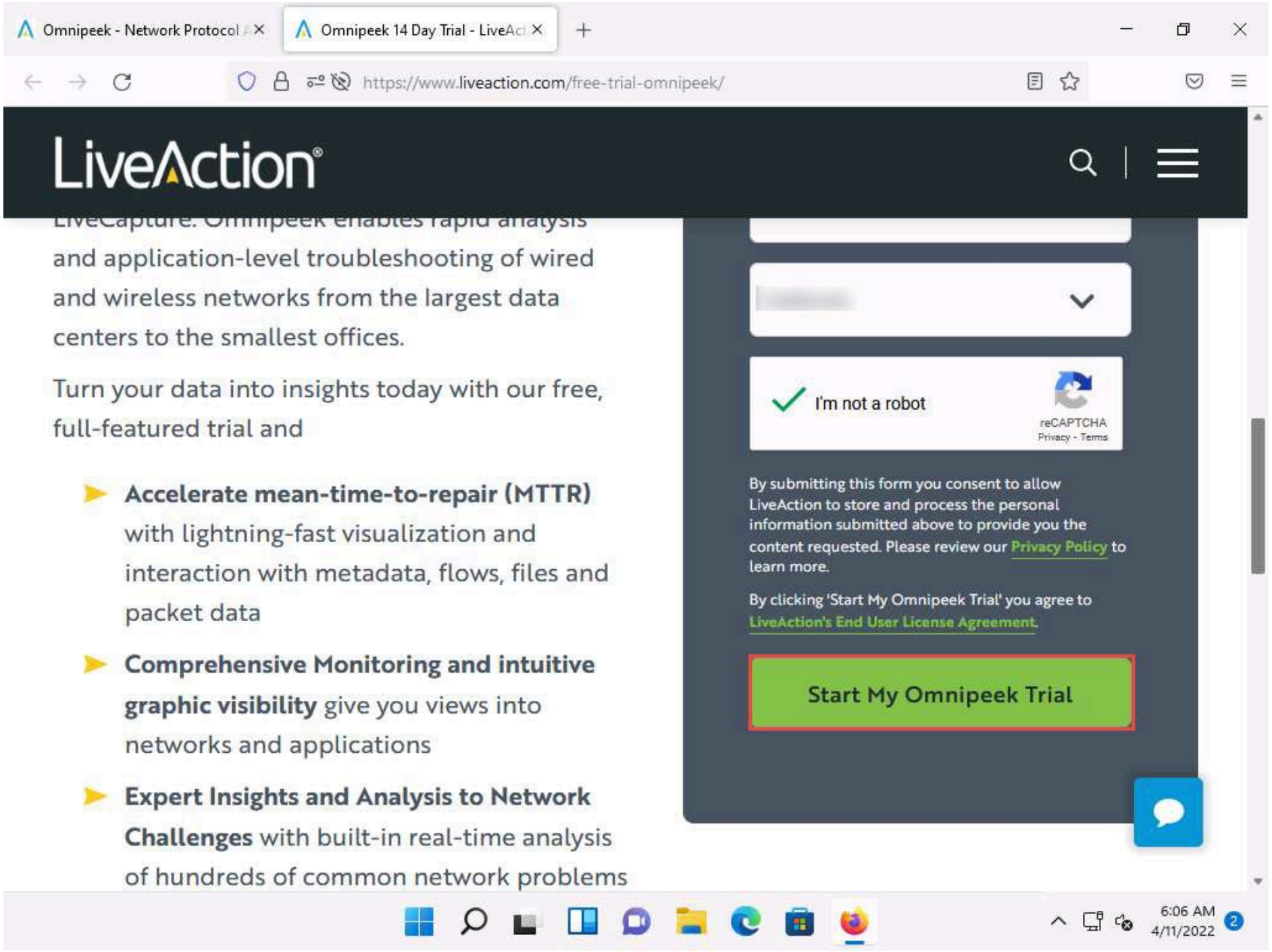
> Note: If **Warning: Potential Security Risk Ahead** page appears, click **Advanced**, and click **Accept the Risk and Continue**.
>
> Note: You will be redirected to a cart in live action, click checkout.



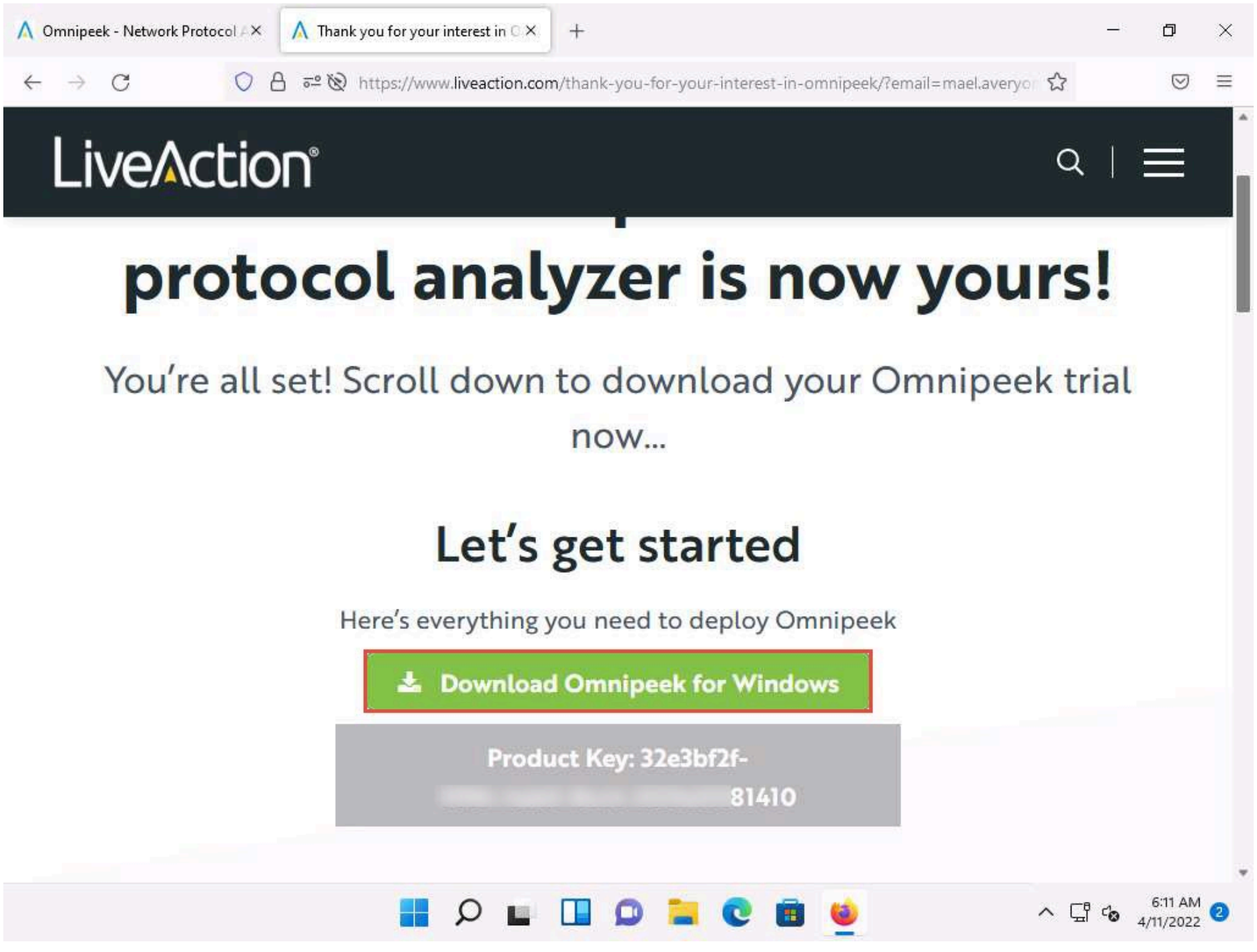
4. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **Start My Omnipeek Trial** button.

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





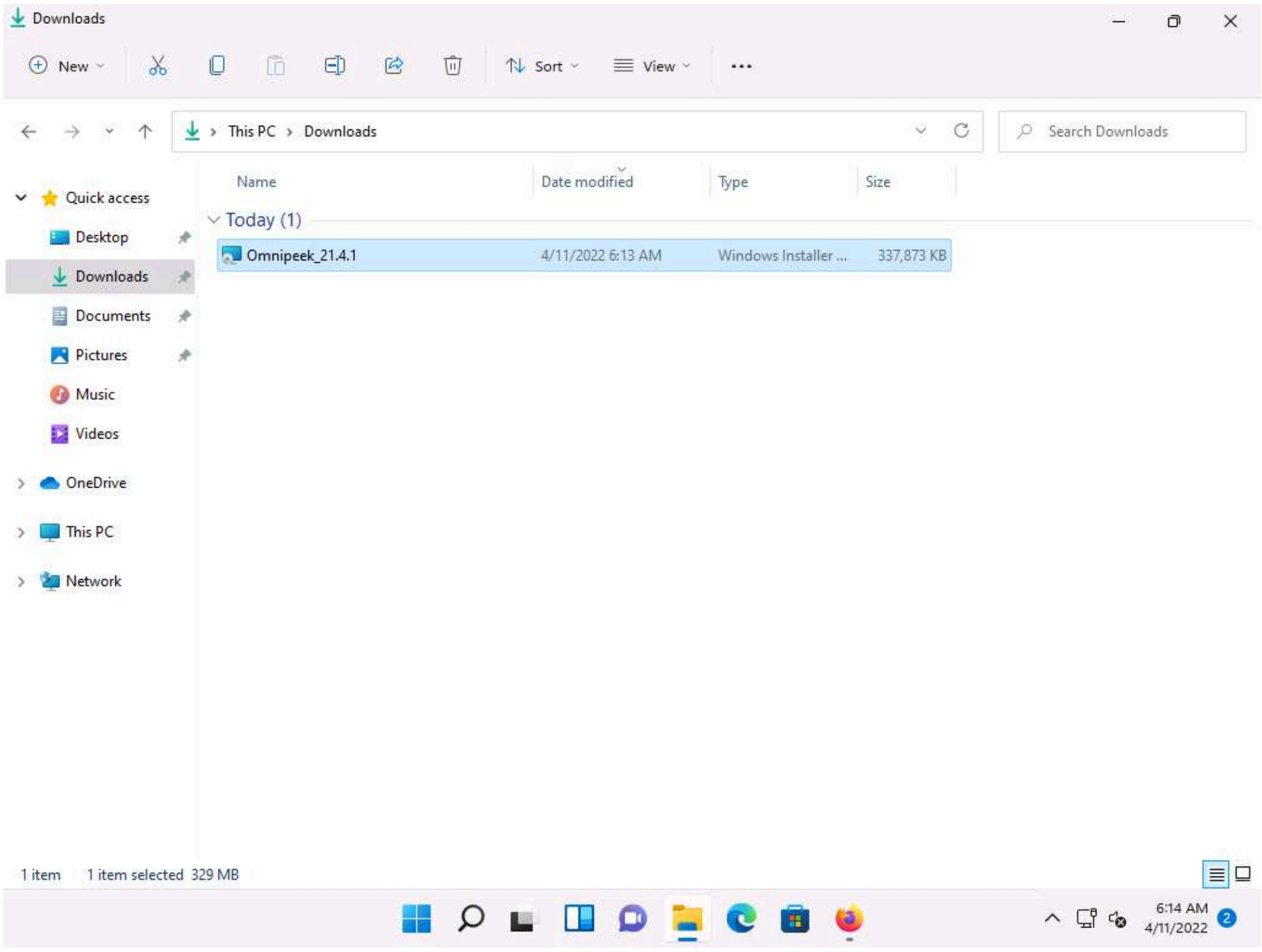
5. The **Let's get started** webpage appears, displaying the License Key and download link for Omnipeek. Click on the **Download Omnipeek for Windows** button to begin the download.



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

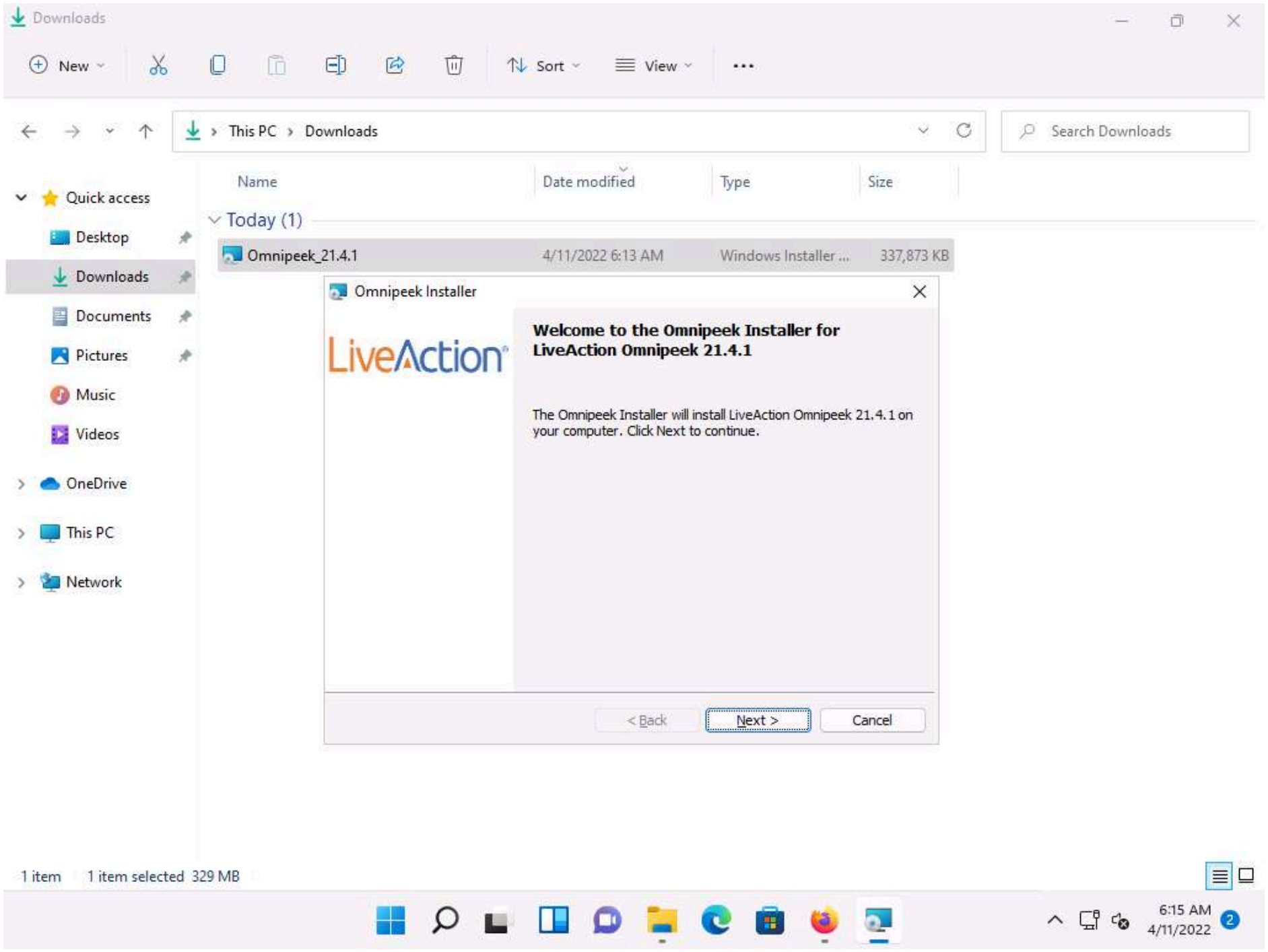
6. On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek_21.4.1msi**.

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

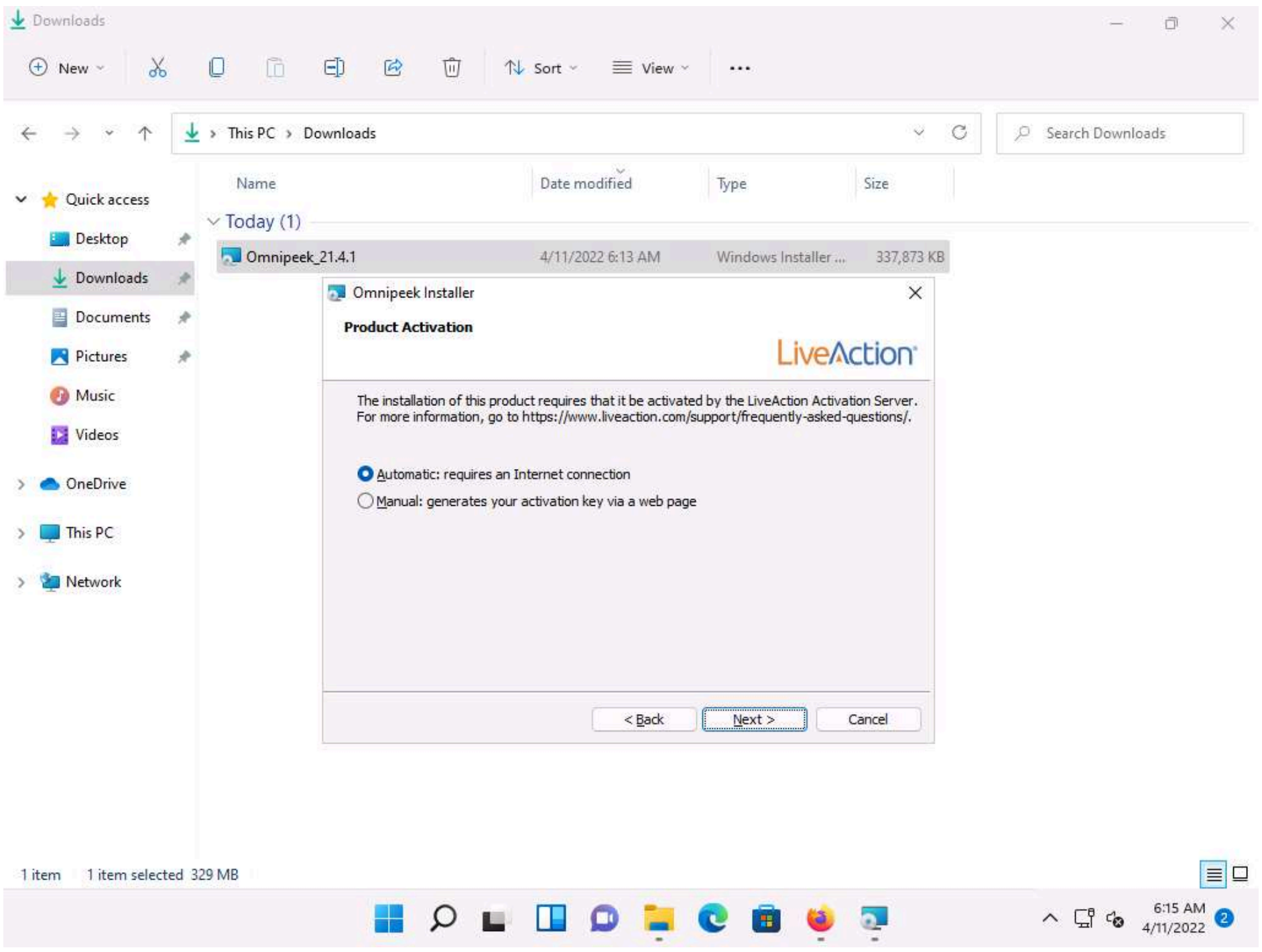


7. If an **Open File - Security Warning** pop-up appears, click **Run**.

8. The **OmniPeek Installer** wizard appears; click **Next**.

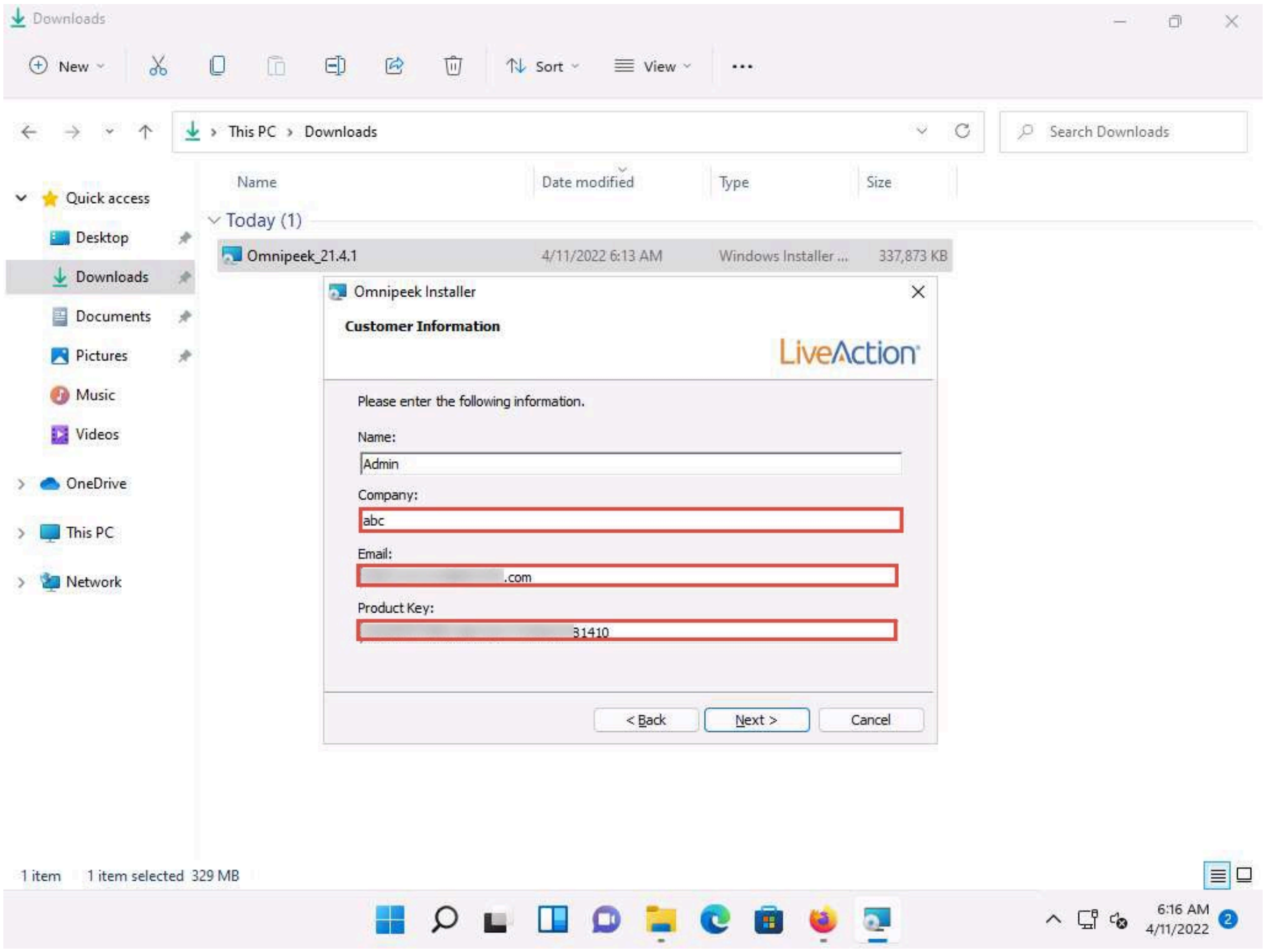


9. In the **Product Activation** wizard, ensure that the **Automatic**: **requires an Internet connection** radio-button is selected and click **Next**.



10. The **Customer Information** wizard appears; type a **Company Name** (here, **abc**) and **Email** (provided at the time of registration). For the serial number field, switch to the **Mozilla Firefox** browser and copy the **License Key**. Close the browser.

11. Switch back to the **Ompnipeek Installer** window, paste the **License Key** in the **Serial Number or Product Key** field, and then click **Next**.

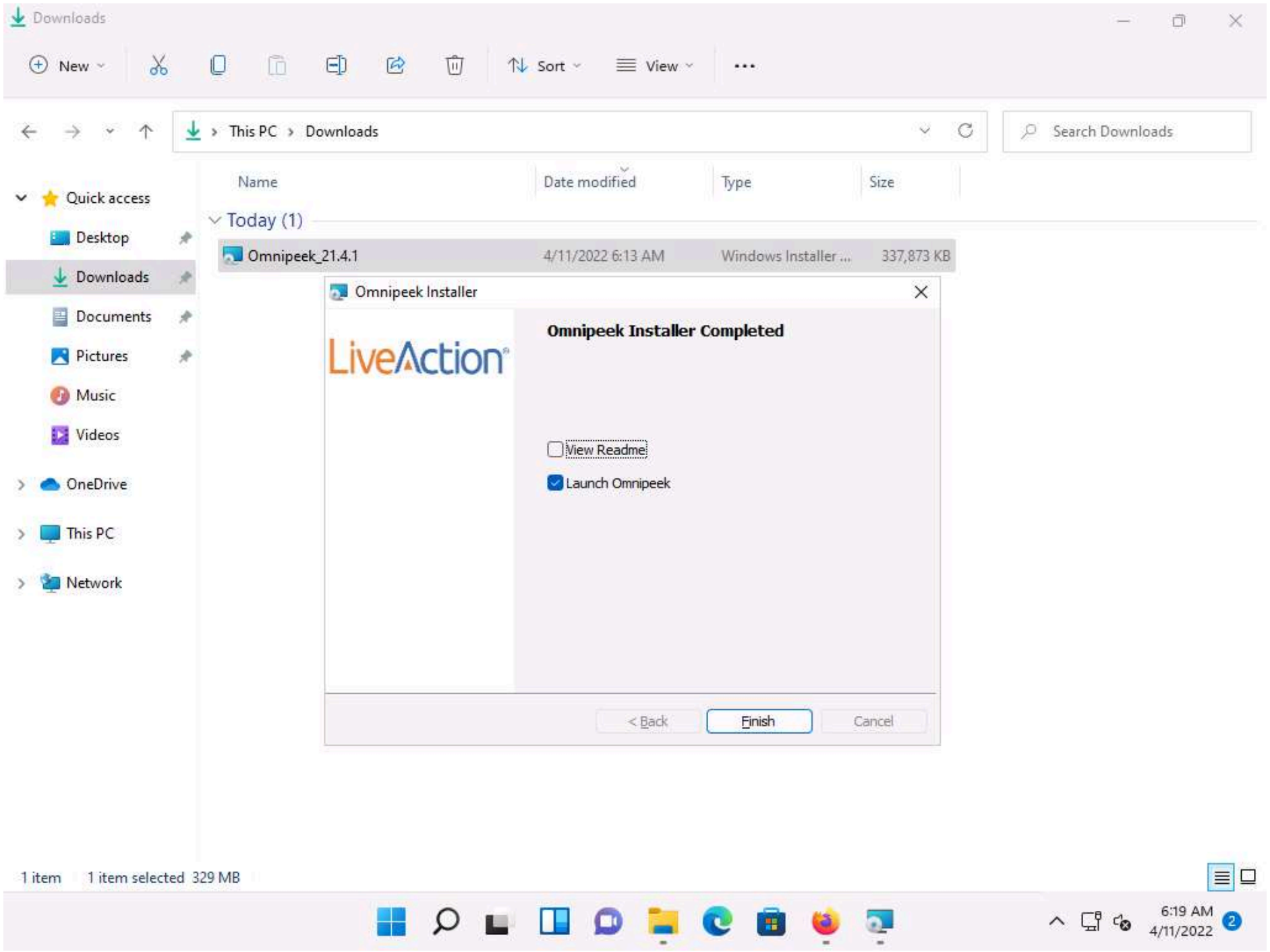


12. Follow the wizard-driven installation steps to install Omnipeek using the default settings.

13. While **Installing LiveAction Omnipeek**, if a **User Account Control** pop-up appears, click **Yes**.

14. On completion of the installation, the **Omnipeek Installer Completed** wizard appears; uncheck **View Readme**, ensure that the **Launch Omnipeek** option is checked, and click **Finish**.

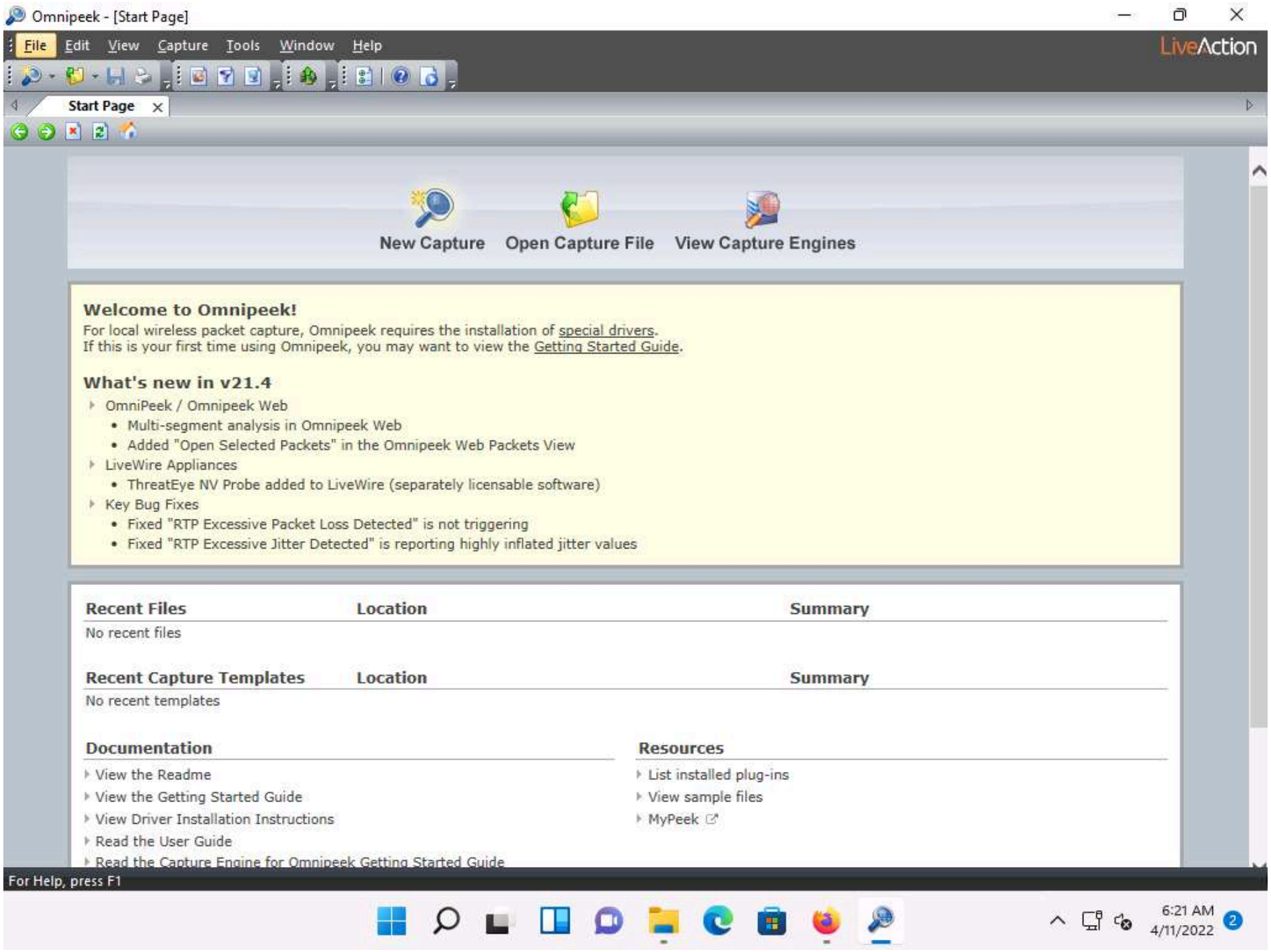
> Note: If a **User Account Control** pop-up appears, click **Yes**.



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

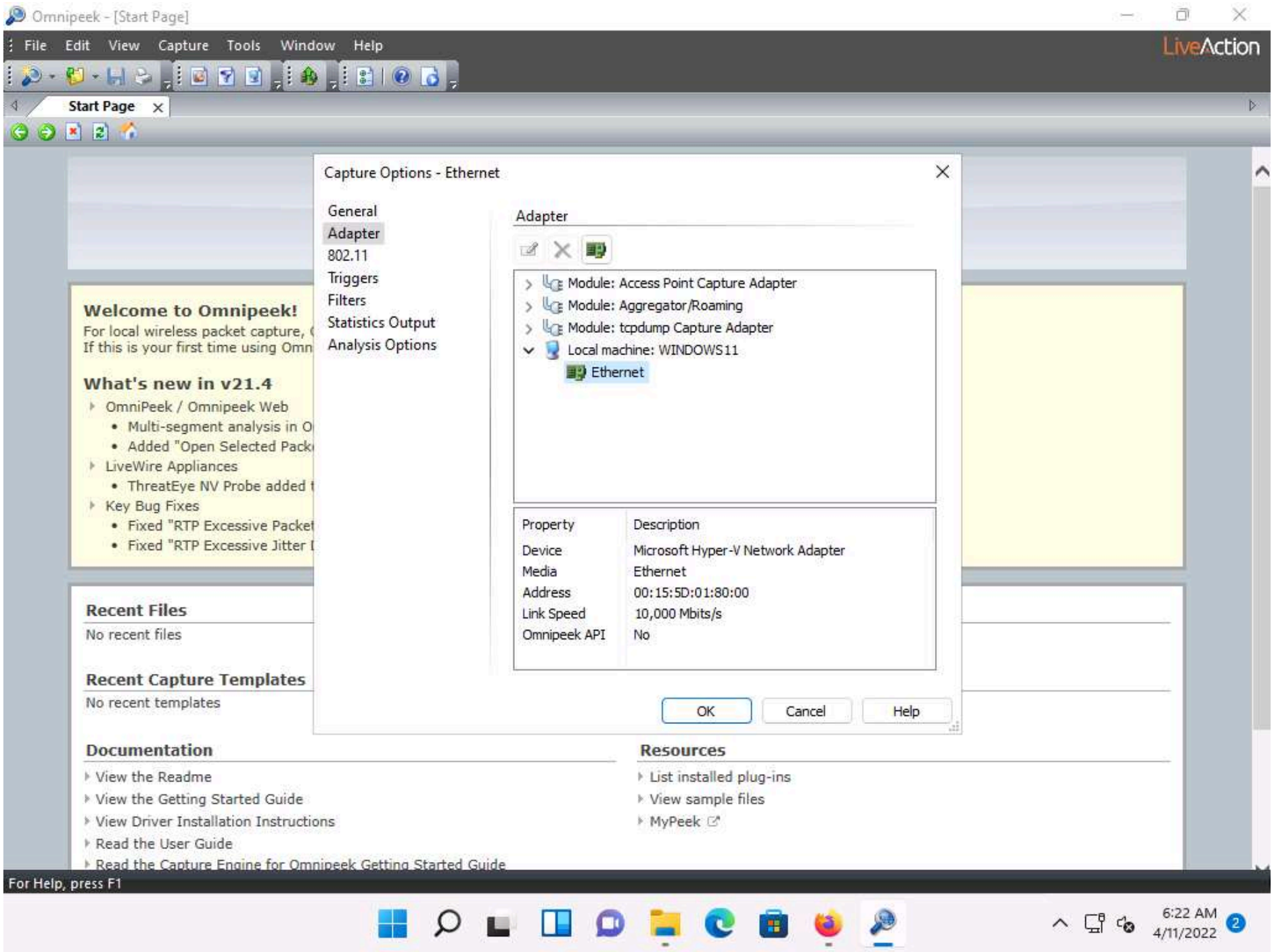
16. The **Omnipeek** main window appears, as shown in the screenshot.

17. Click on the **New Capture** option from the Omnipeek's main screen to create an Omnipeek capture window.

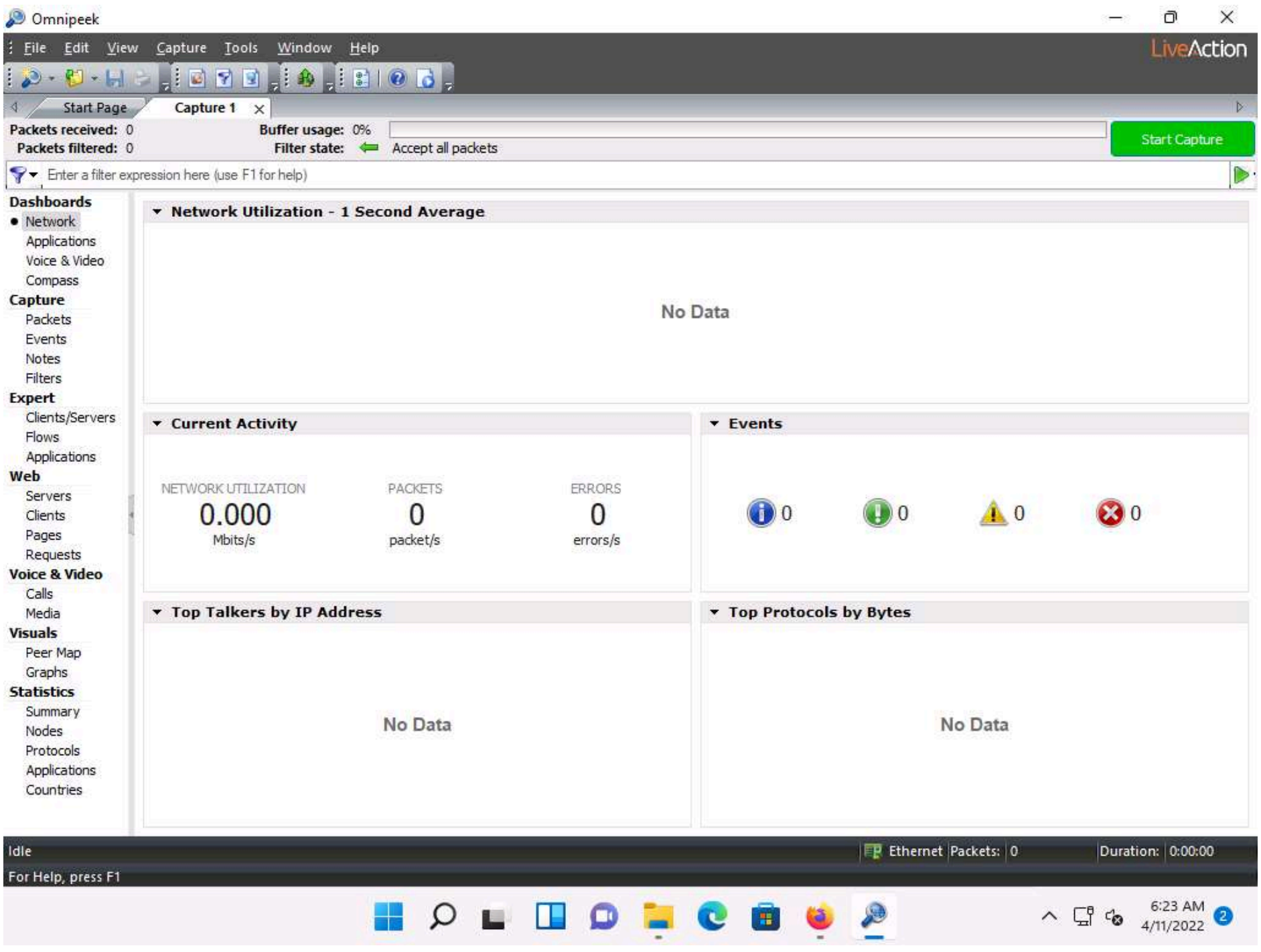


18. The **Capture Options** window appears; by default, the **Adapter** option opens-up.

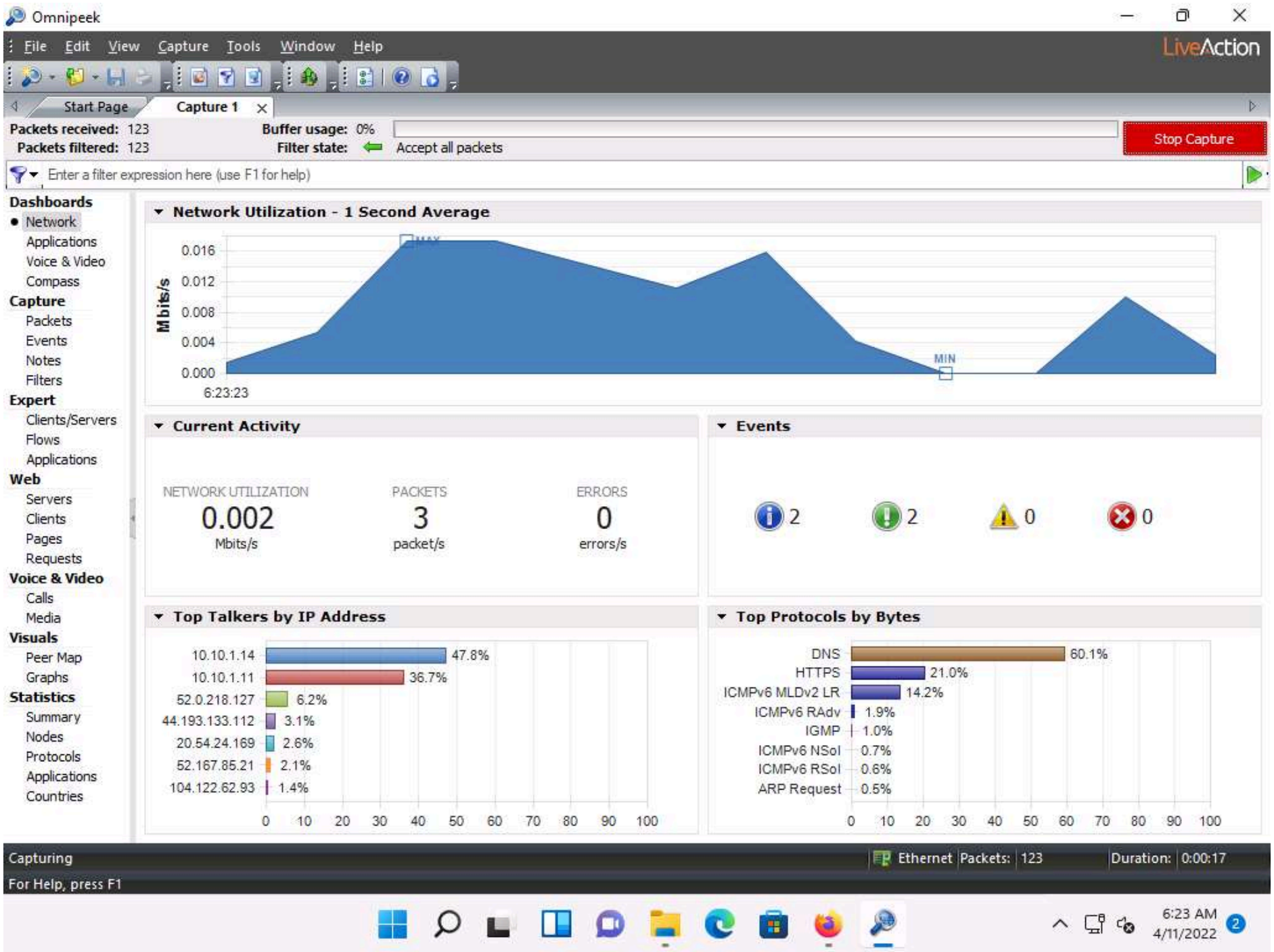
19. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS11** node, select **Ethernet**, and click **OK**.



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



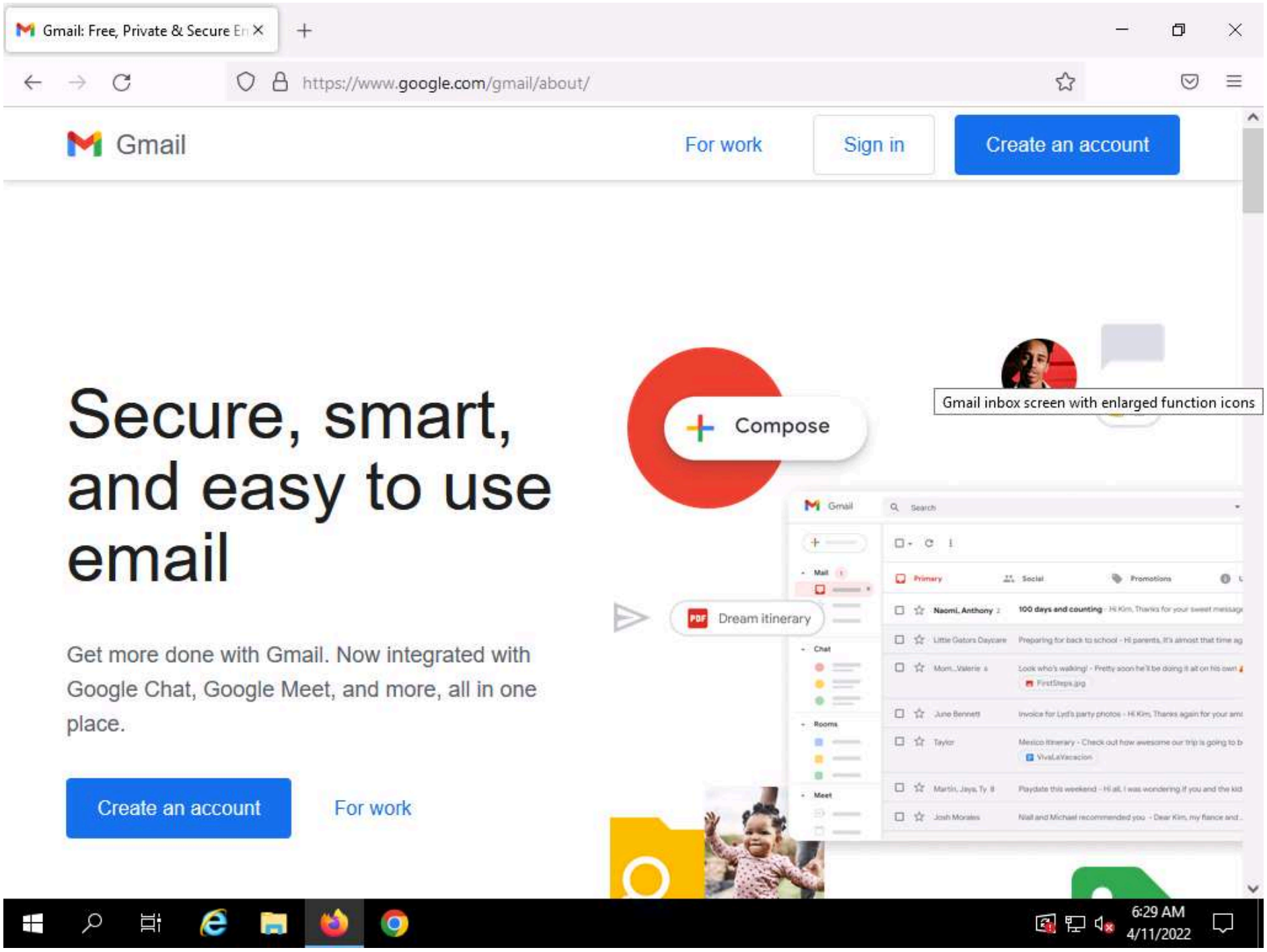
21. The **Start Capture** button changes to read "**Stop Capture**" and traffic statistics begin to populate **Network** under the **Dashboards** section, as shown in the screenshot.



22. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

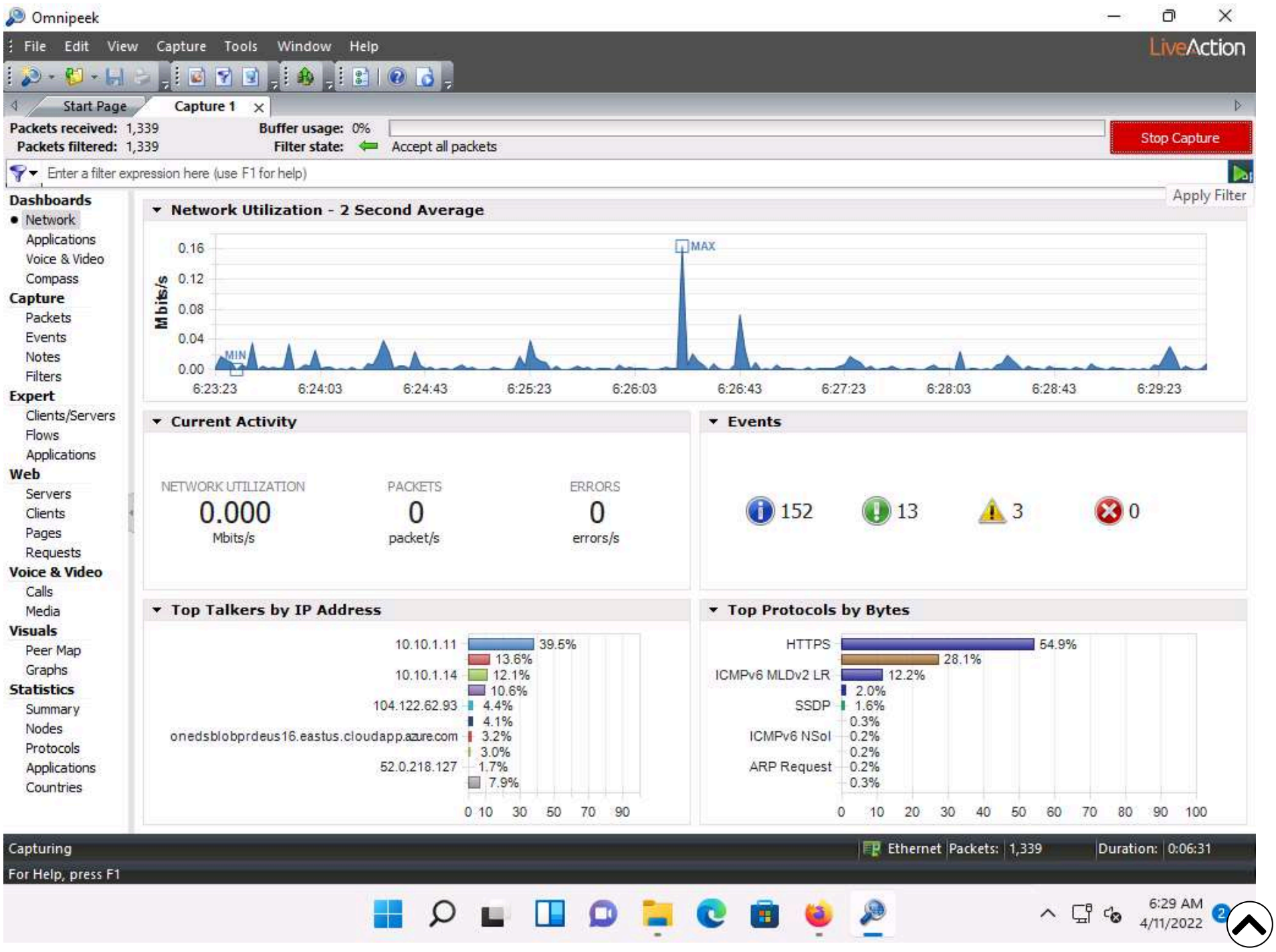
23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **https://www.gmail.com**).

> 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.

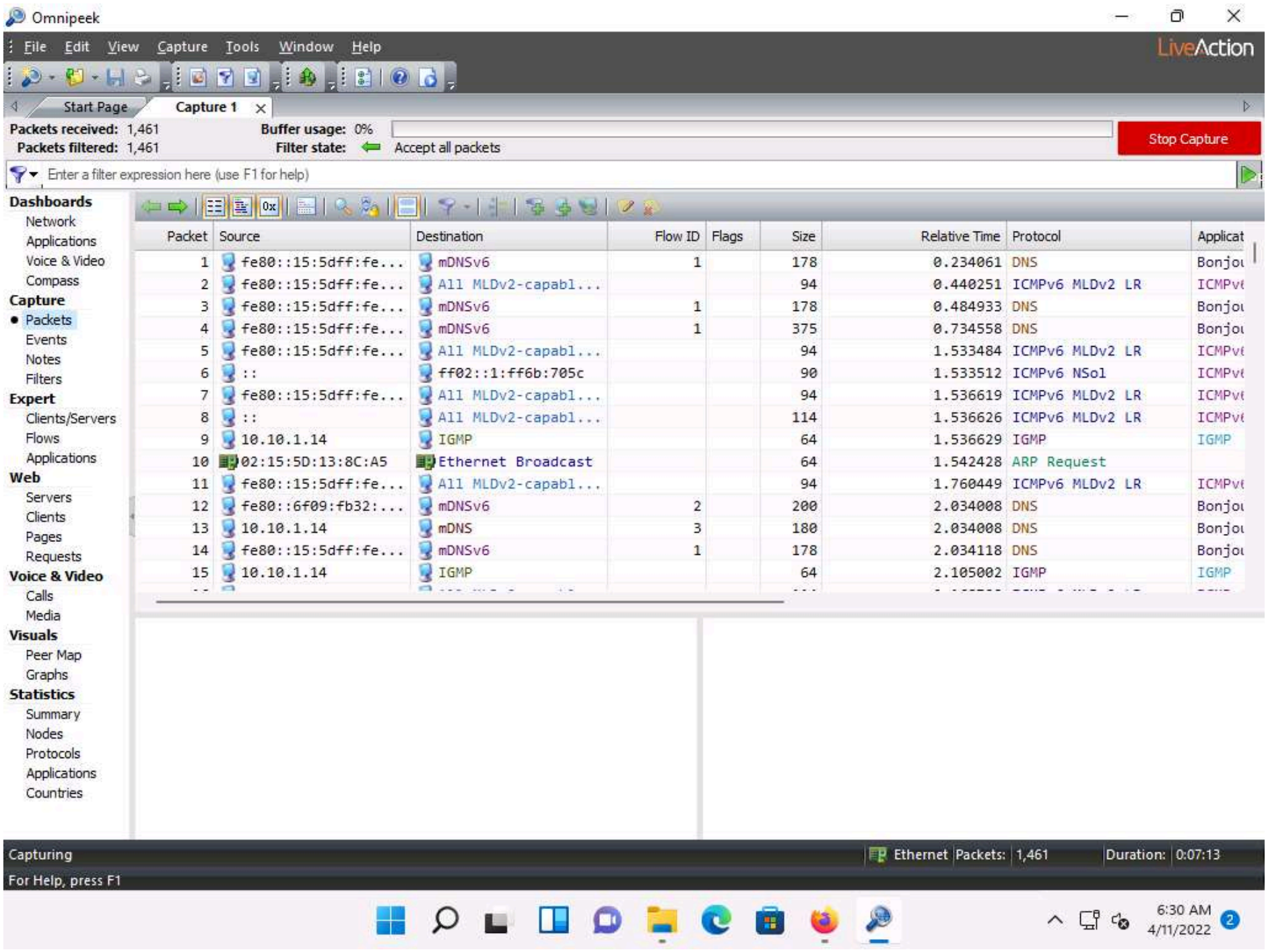


24. Now, click **CEHv12 Windows 11** to switch back to the **Windows 11** machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.

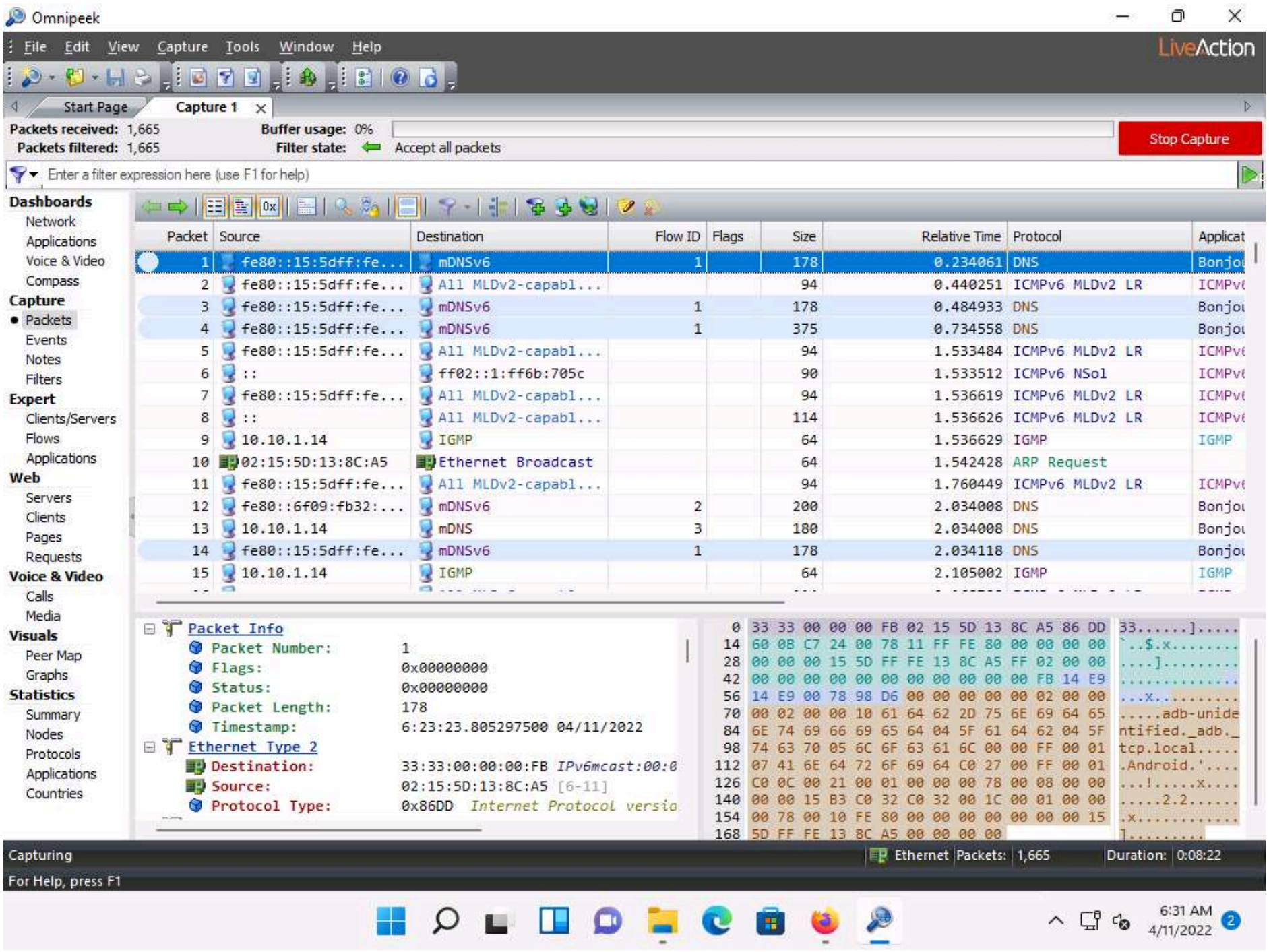
25. You can observe the network traffic along with the websites visited by the target machine.



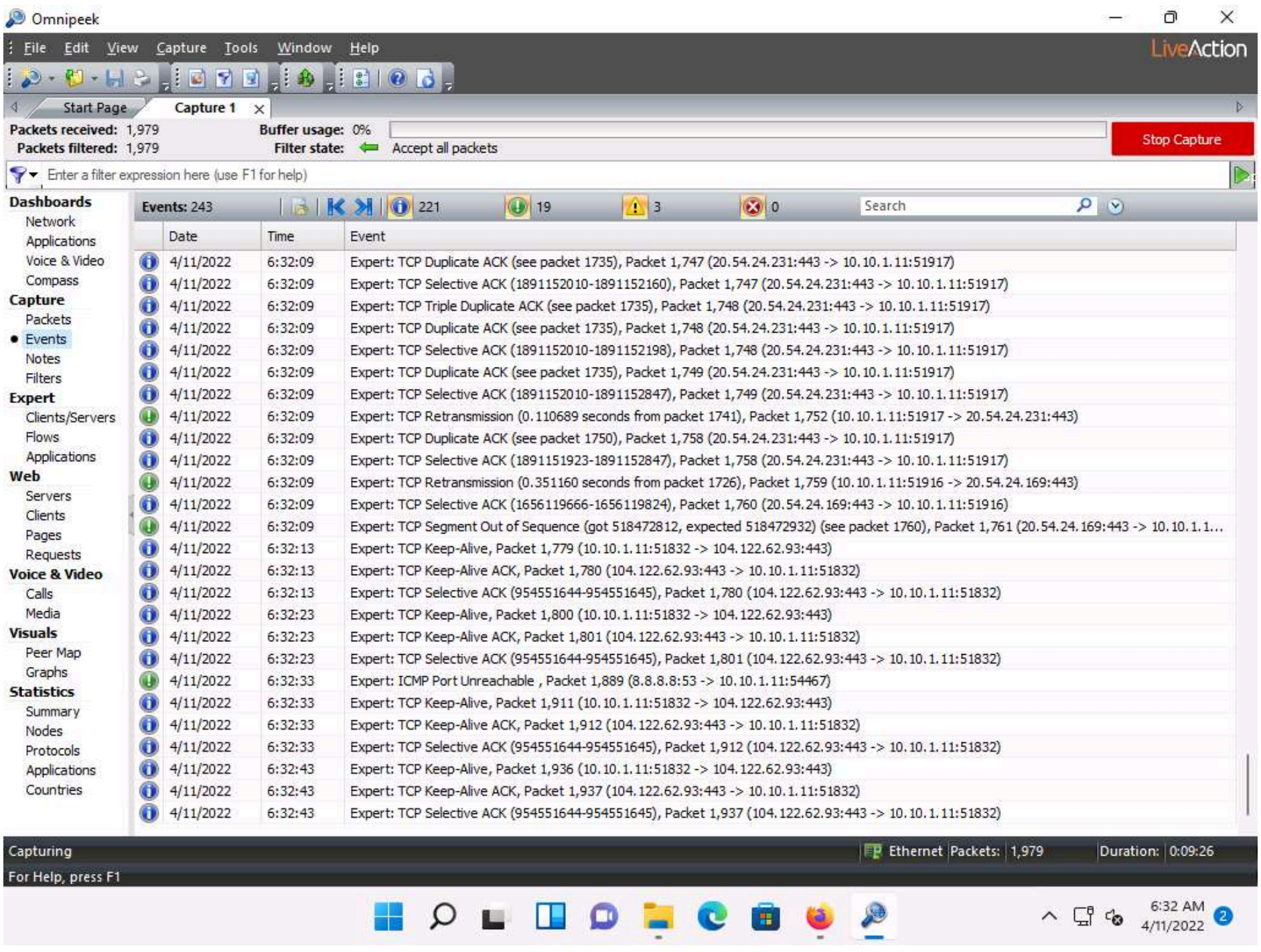
26. To view the captured packets, select **Packets** under the **Capture** section in the left-hand pane. You can observe the outgoing and incoming network packets of the target system.



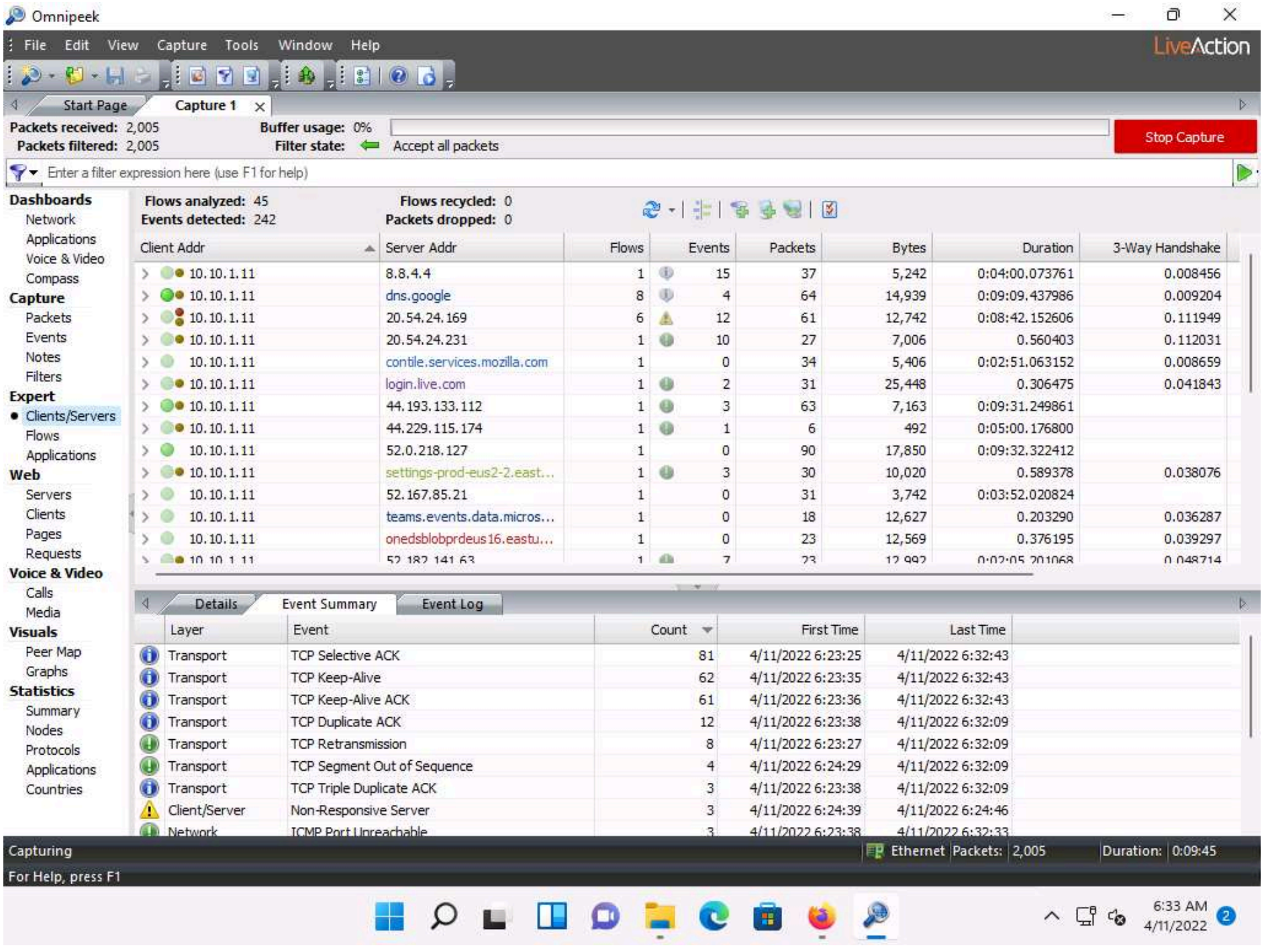
27. You can further click the **Show Decode View** and **Show Hex View** icons to view detailed information regarding any selected packet.



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



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

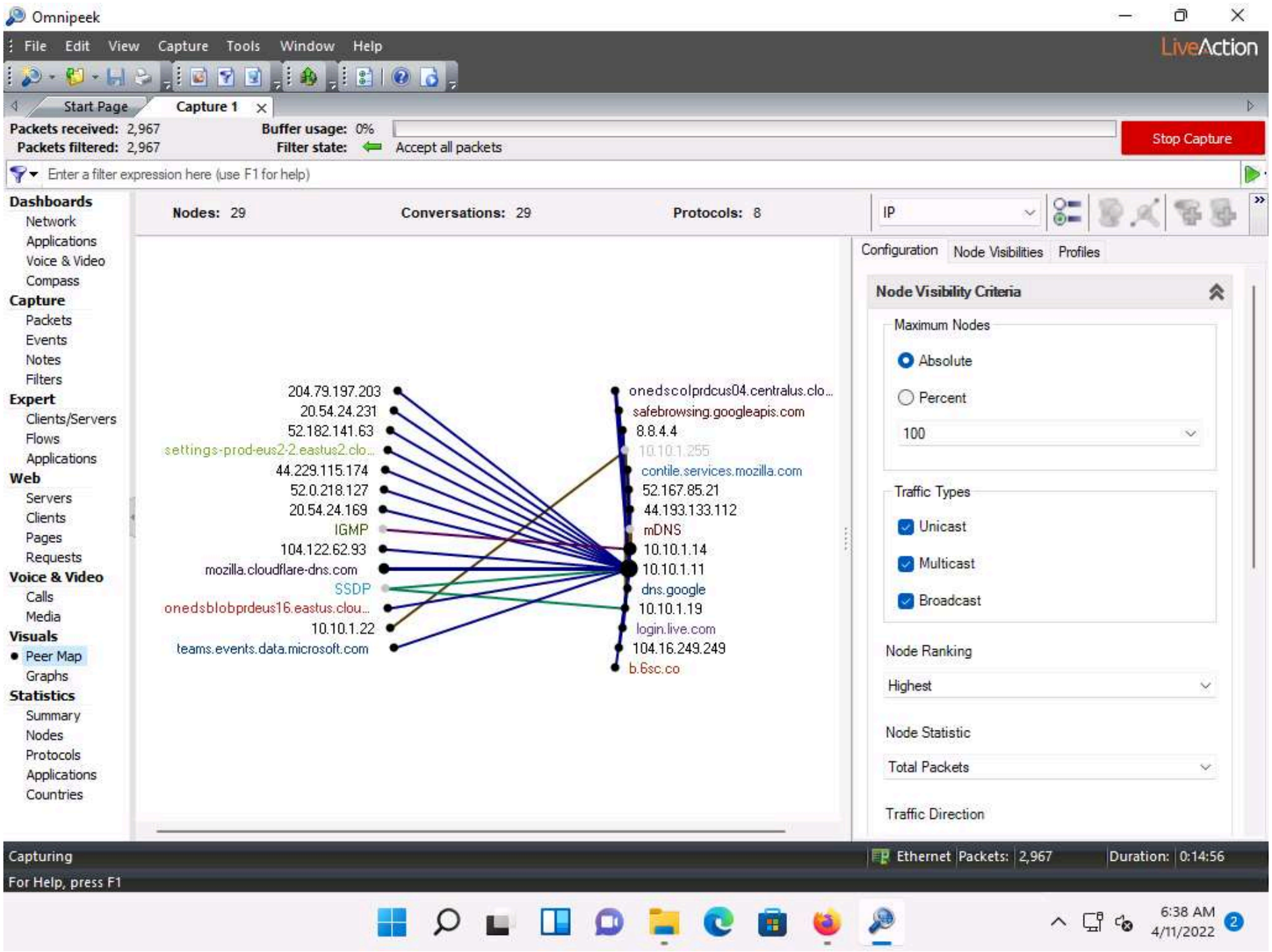


30. Similarly, under the **Flows** and **Applications** options, you can view the packet flow and applications running on the systems in the local network.

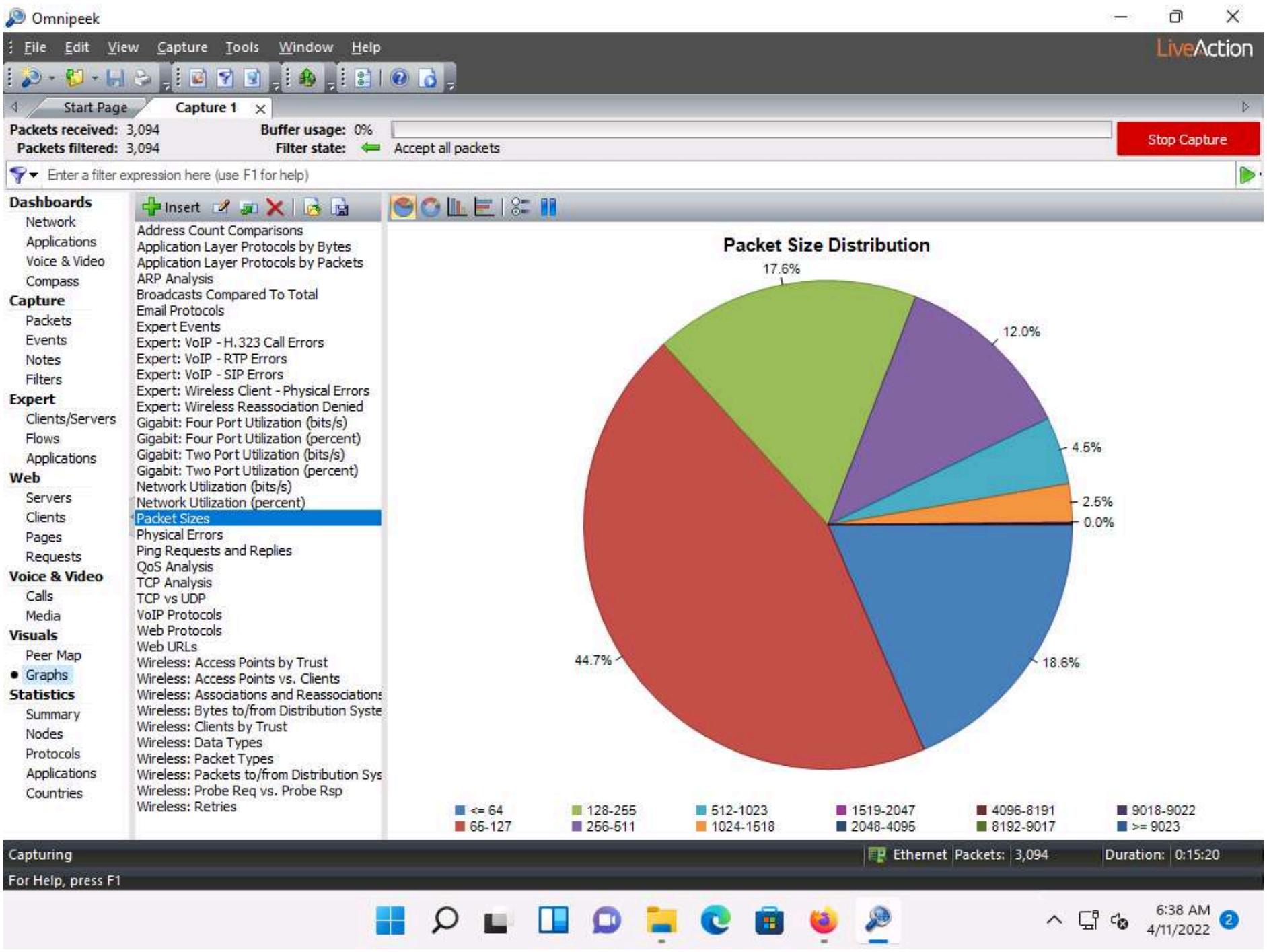
31. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.

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

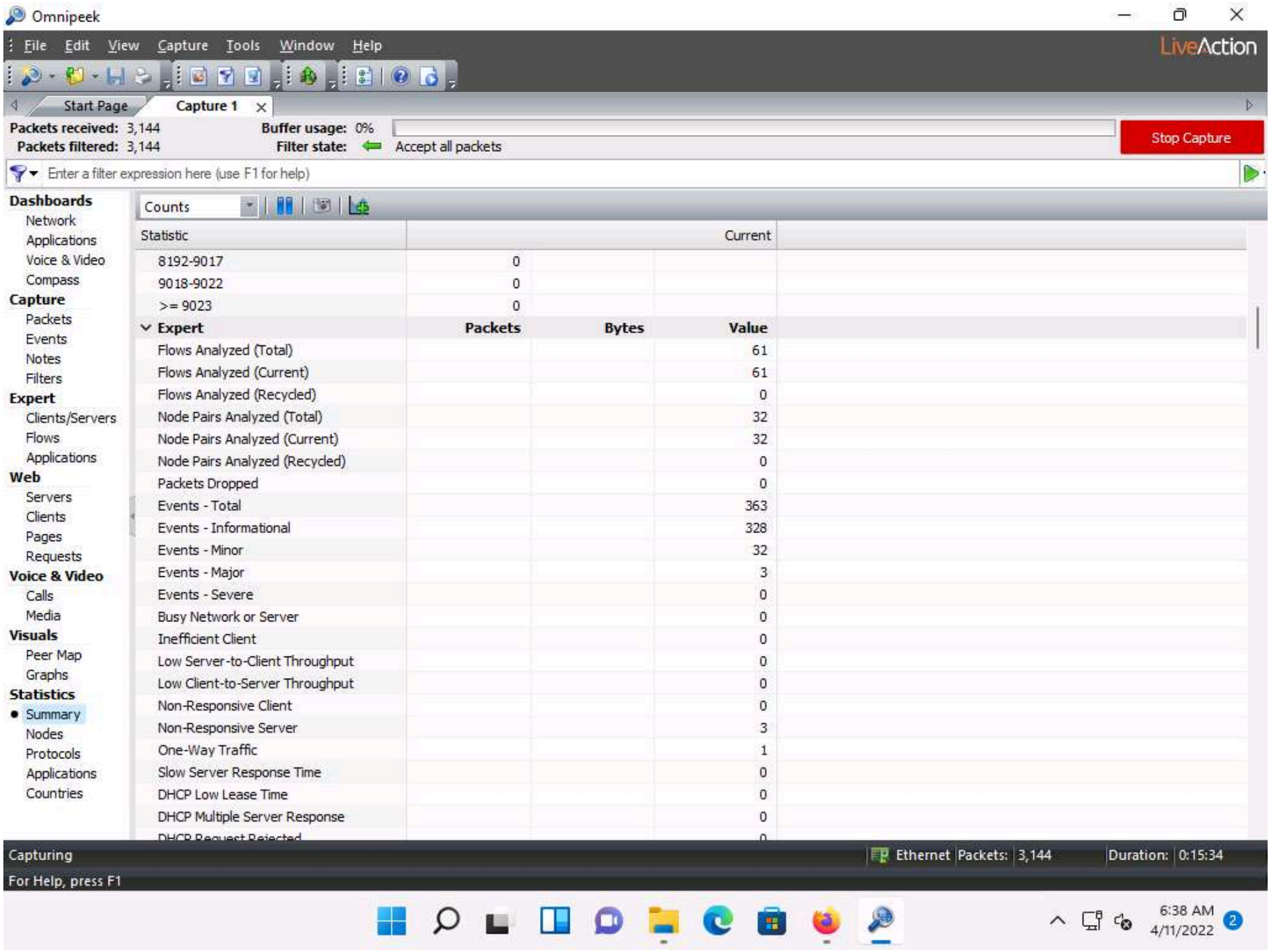
> Note: You can select any traffic according to your purpose.



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

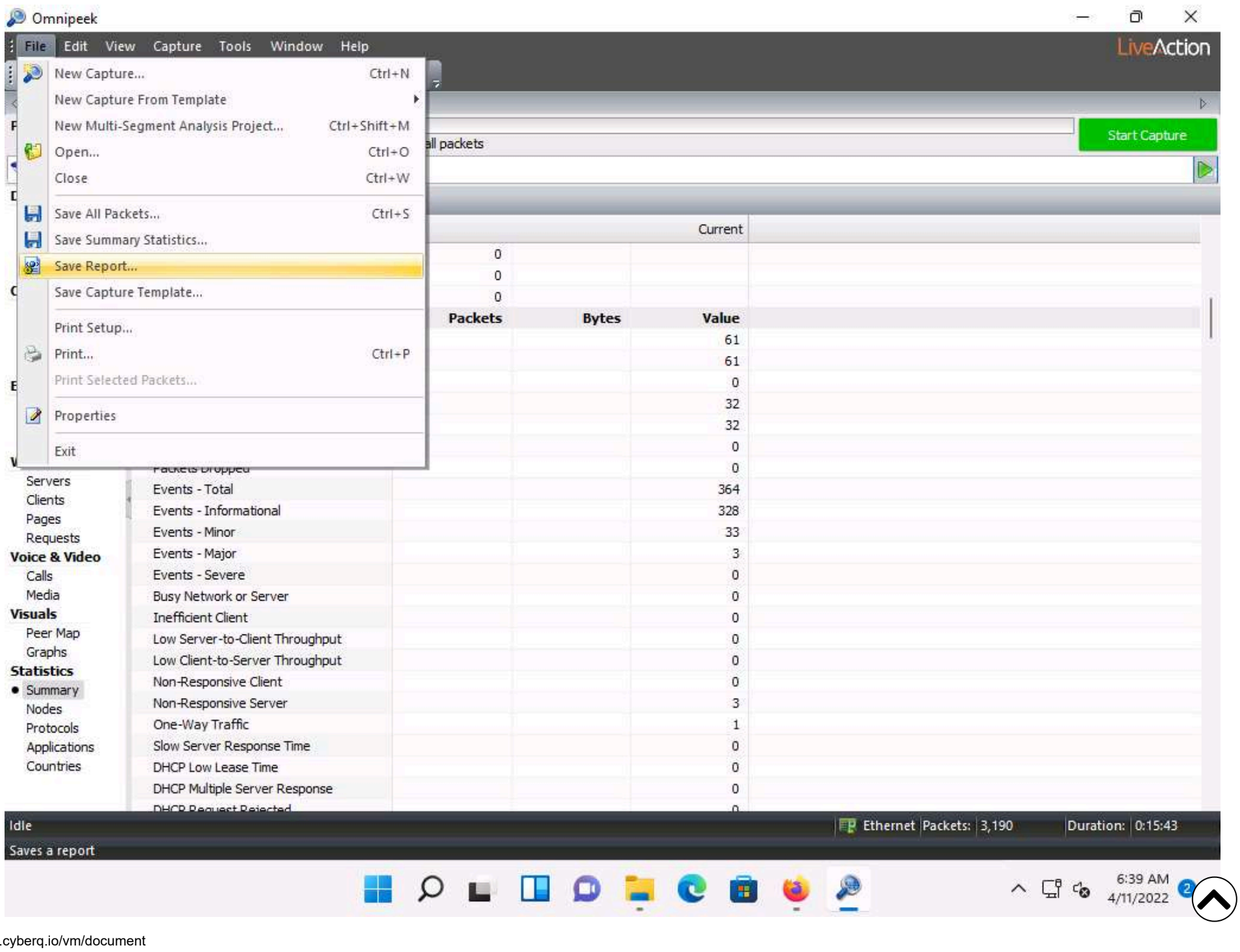


34. Click on the **Summary** option under the **Statistics** section in the left-hand pane to view a summary report of the network analysis.

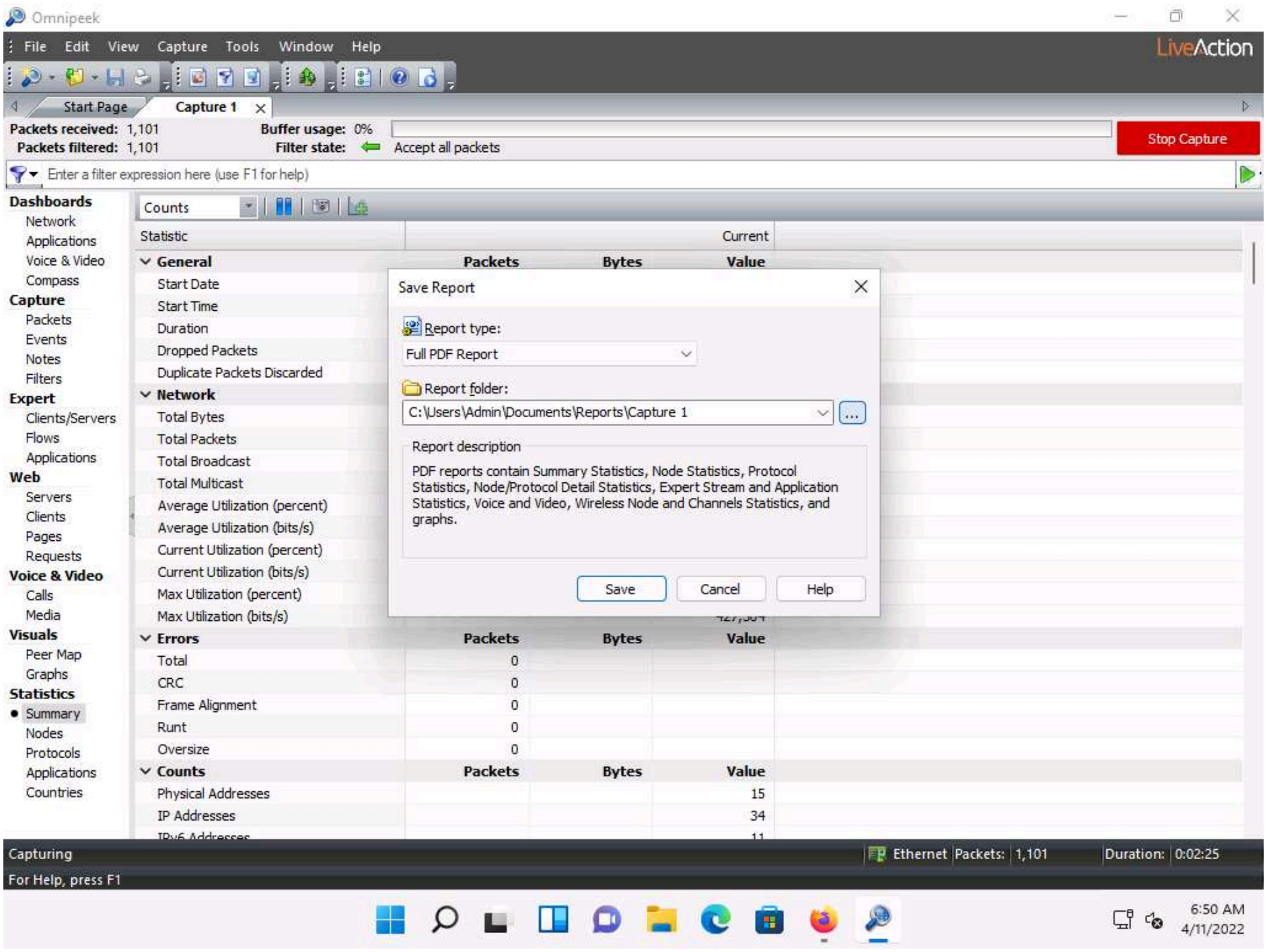


35. Stop the packet capturing by clicking on the **Stop Capture** button in the right-hand corner of the window. The **Stop Capture** button will toggle back to the **Start Capture** button.

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

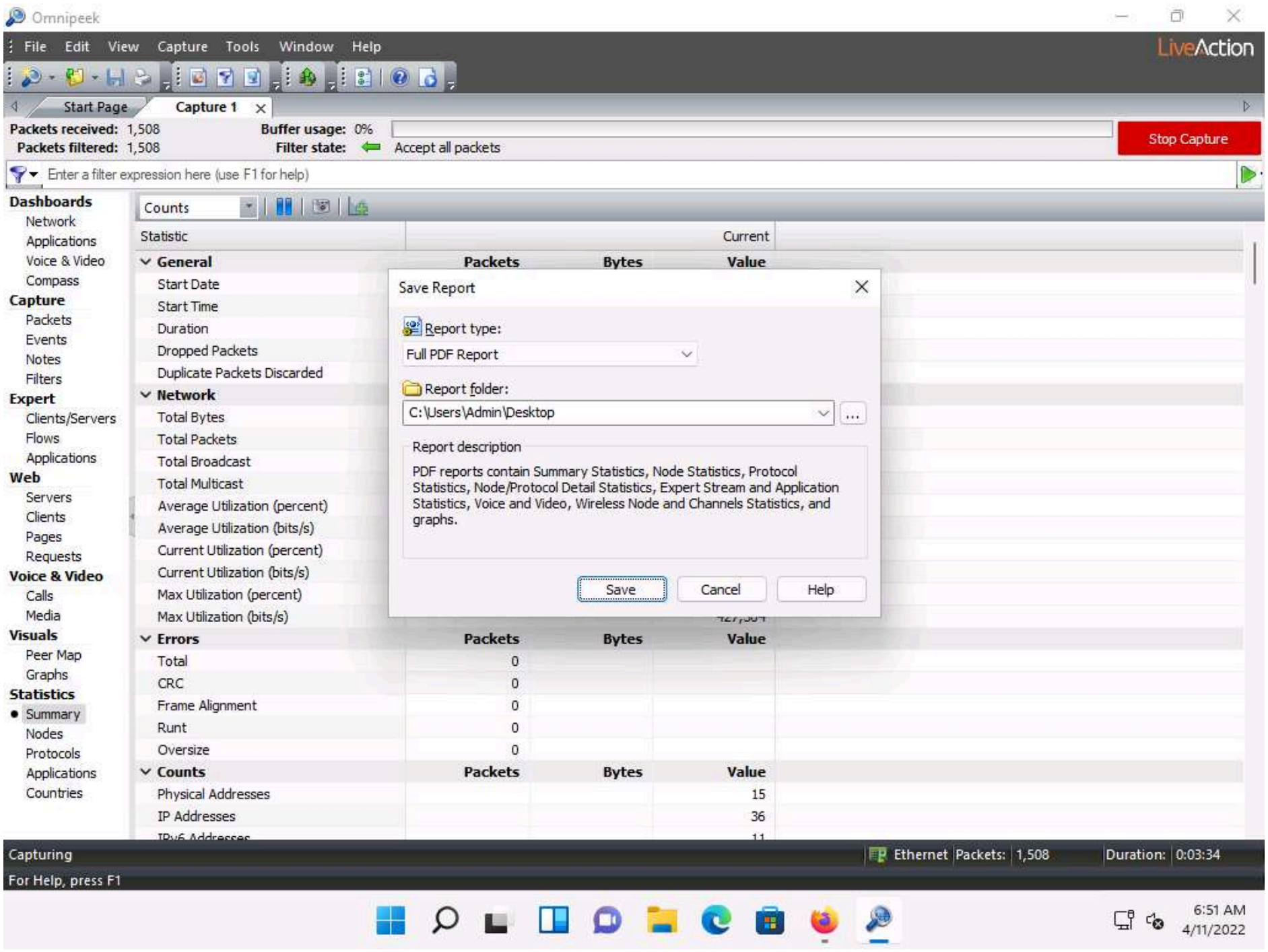


37. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon to change the download location.



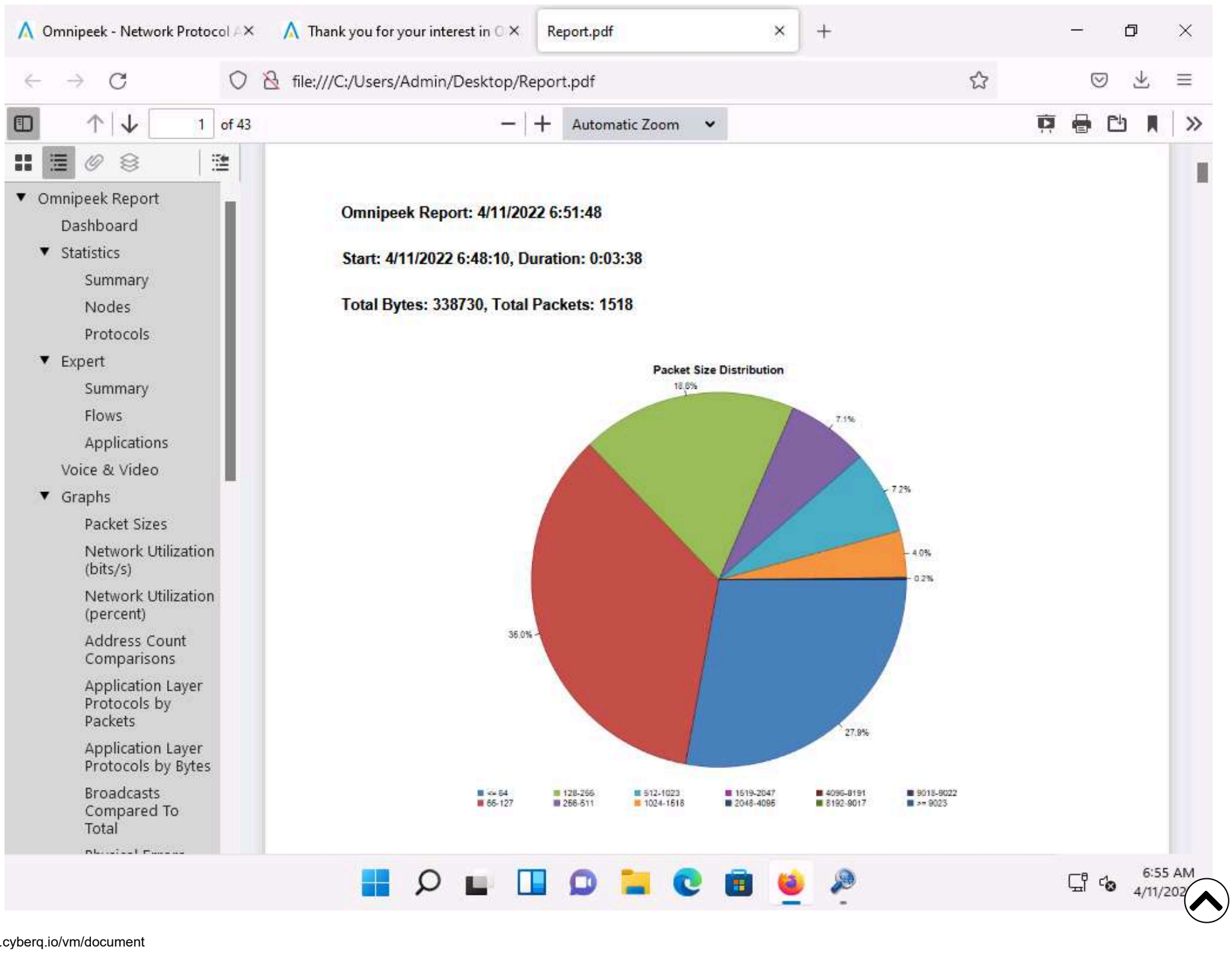
38. The **Browse For Folder** window appears; select the **Desktop** as your save location and click **OK**.

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

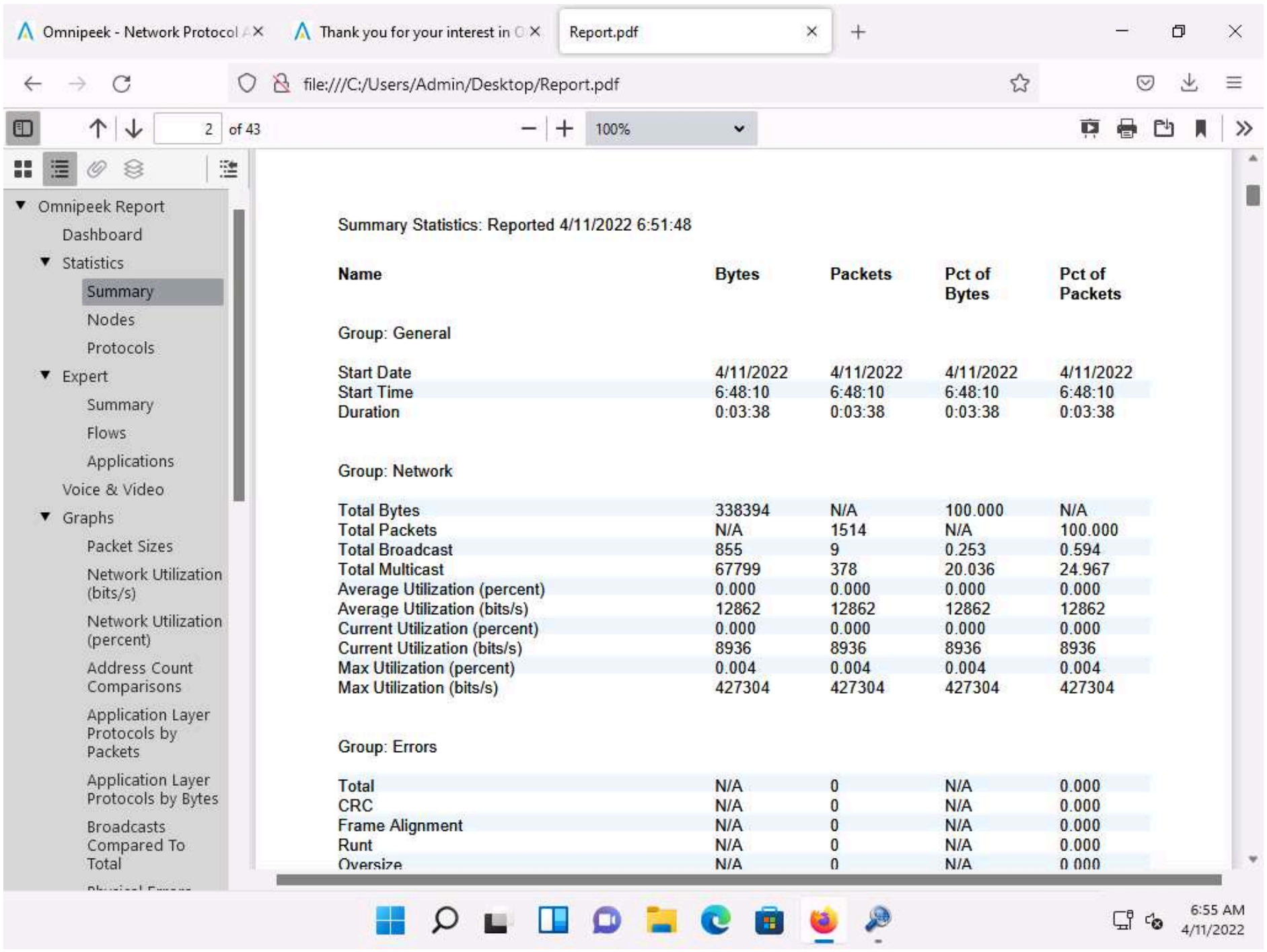


40. The saved report automatically appears, as shown in the screenshot.

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



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



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

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

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

Task 3: Analyze a Network using the SteelCentral Packet Analyzer

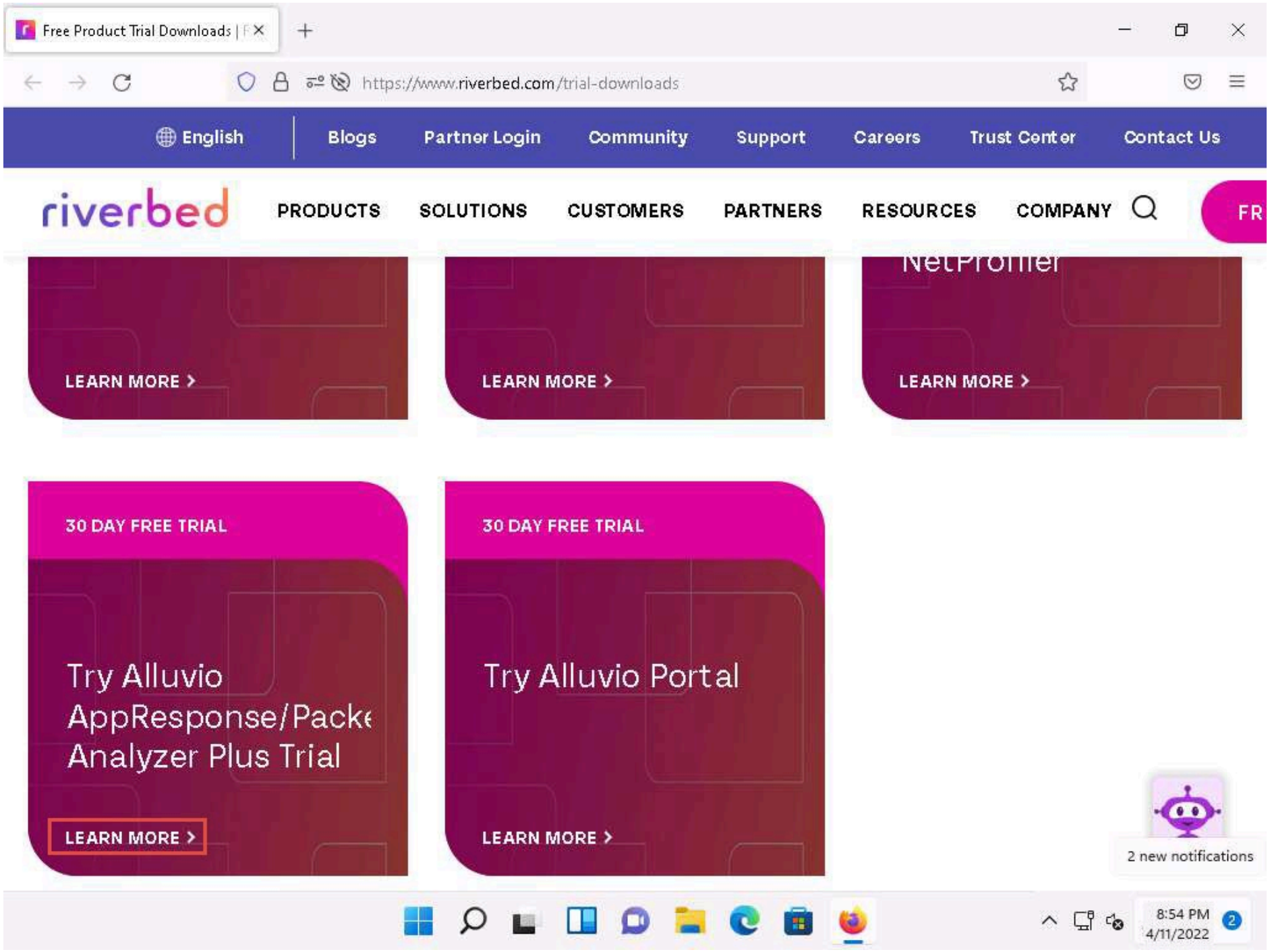
SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes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

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

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, open any web browser (here, **Mozilla Firefox**) now type **https://www.riverbed.com/trial-downloads** in the address bar; press **Enter**.
2. The **riverbed** website appears, displaying **TRIAL DOWNLOADS**. Scroll down and click on **LEARN MORE** under **Try Alluvio AppResponse/Packet Analyzer Plus Trial**.

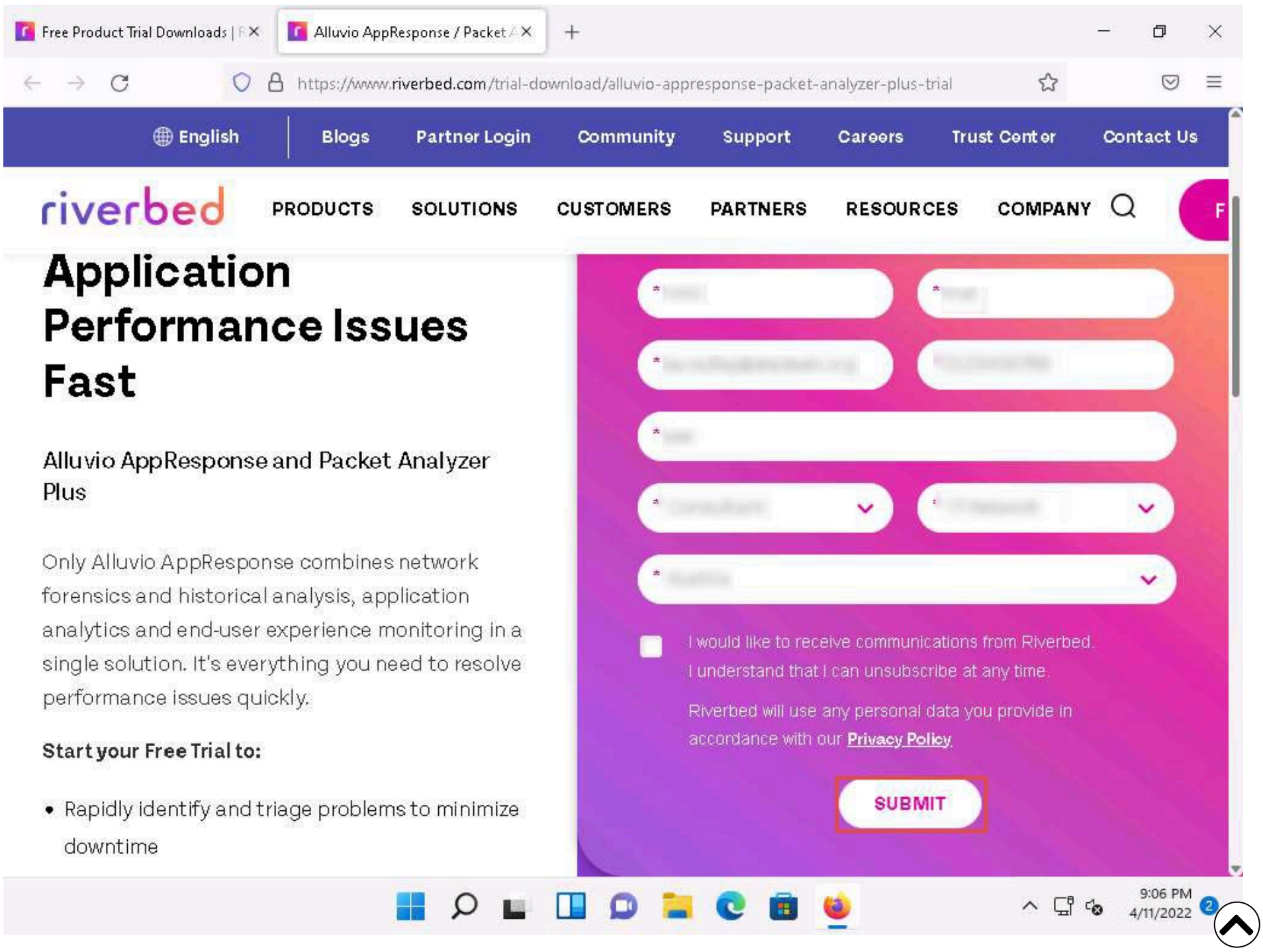
Note: The tool version might differ in your lab environment.

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



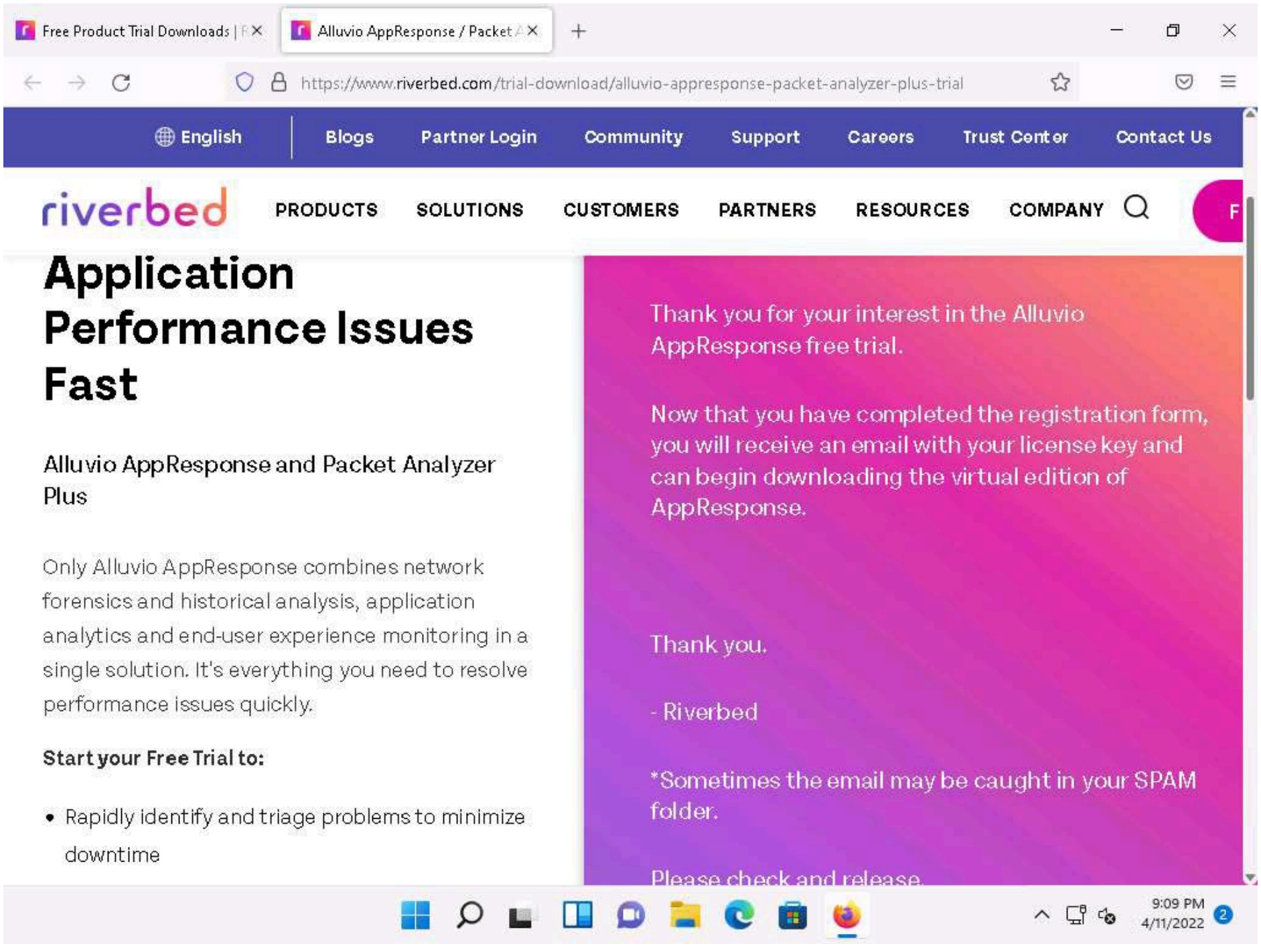
3. A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.

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



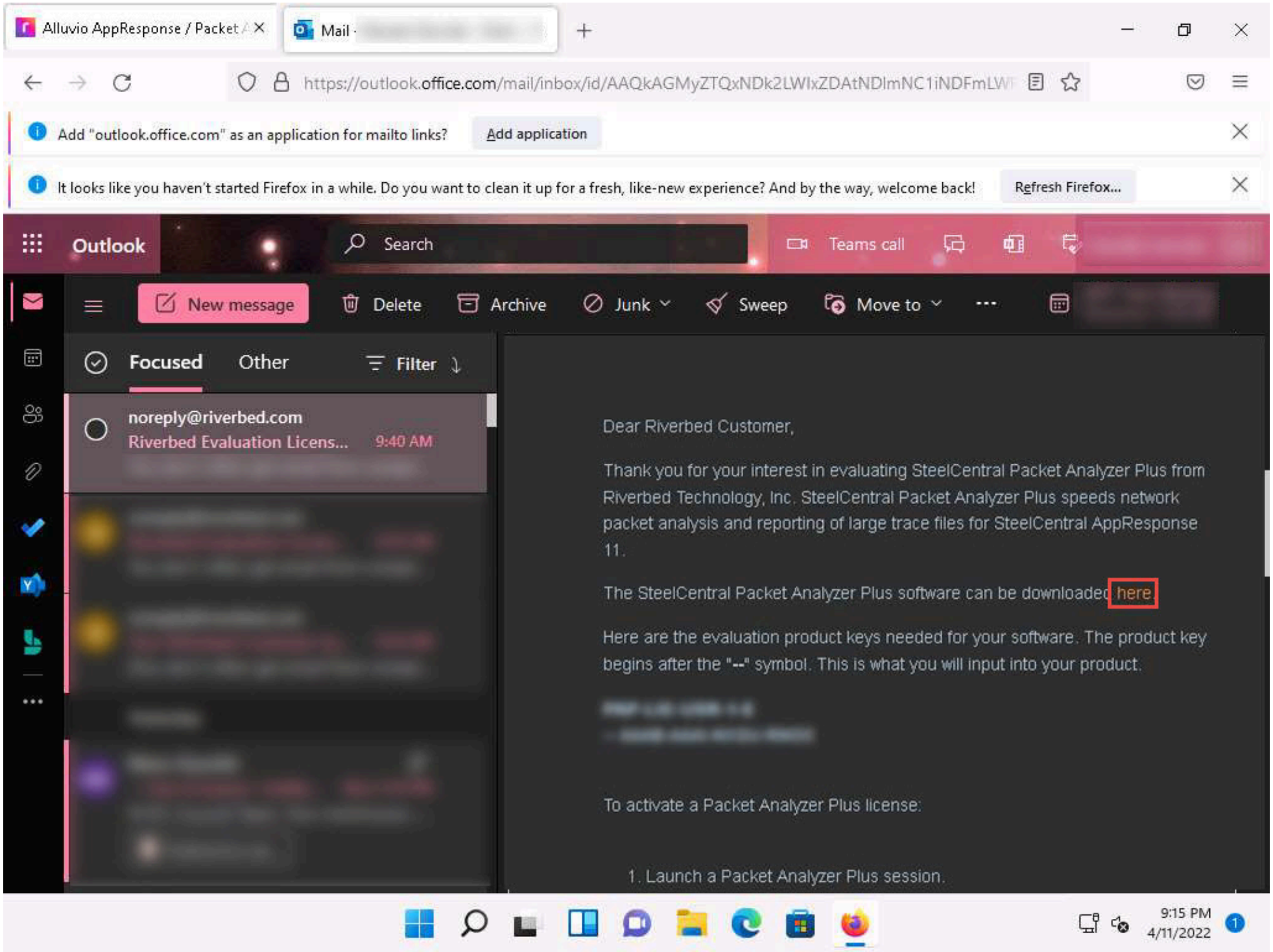
Note: If a **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

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

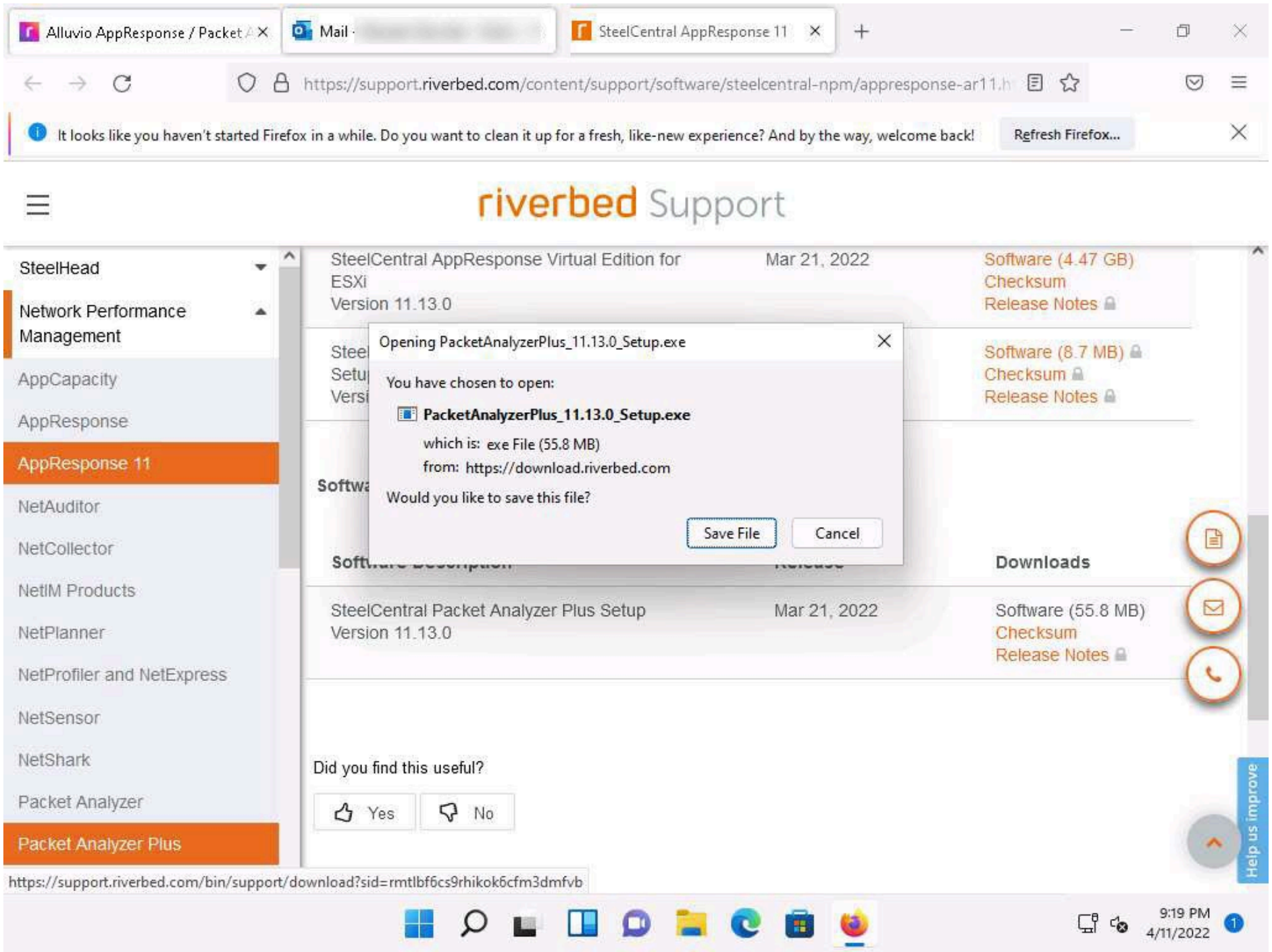


5. Open a new tab and log in to the email account you provided during registration. Open the email from **Riverbed Evaluation License Request for your SteelCentral PacketAnalyzer Plus**, and click the **Software** link to download SteelCentral Packet Analyzer.

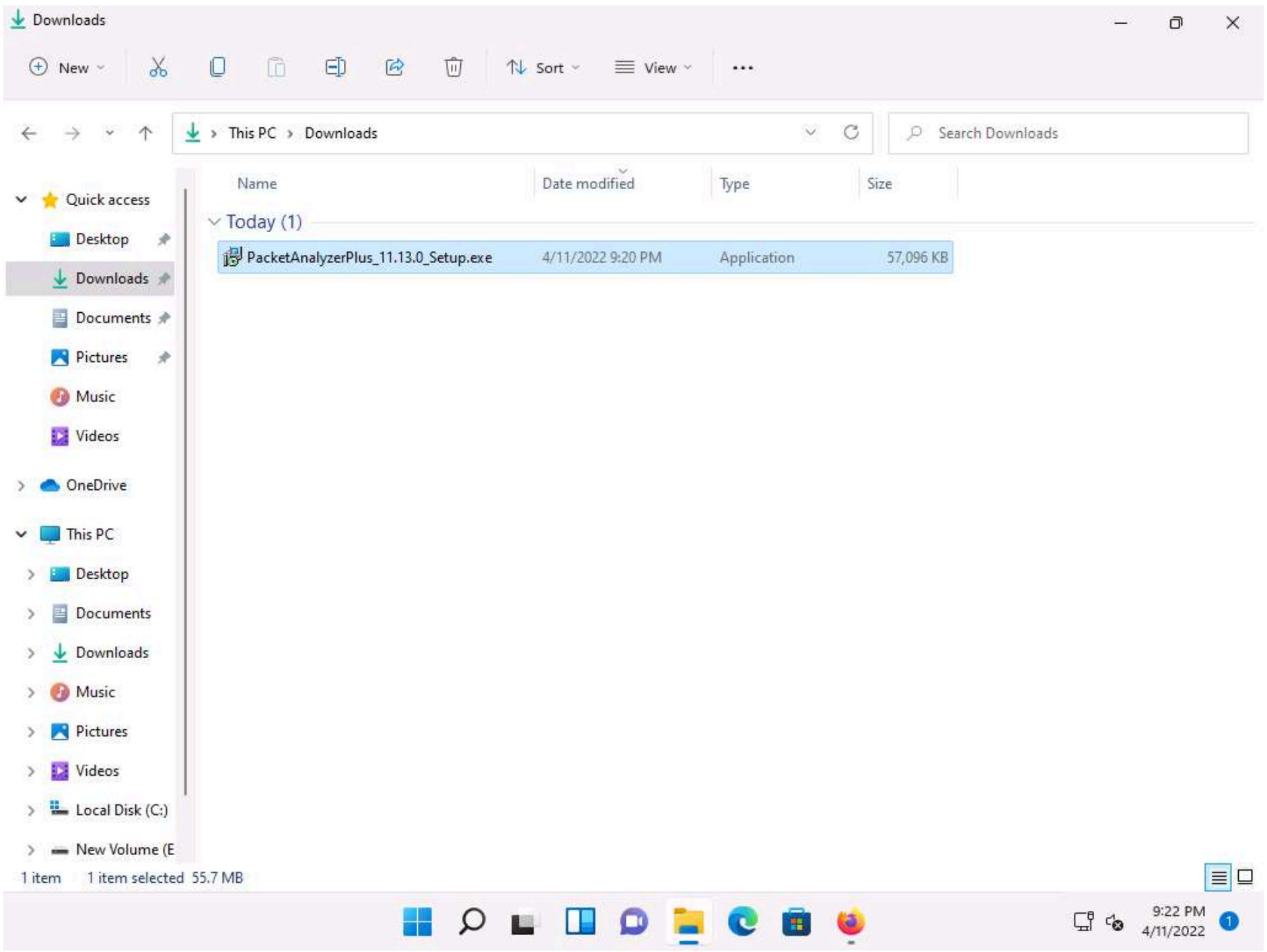
Note: It might take some time to receive the mail.



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

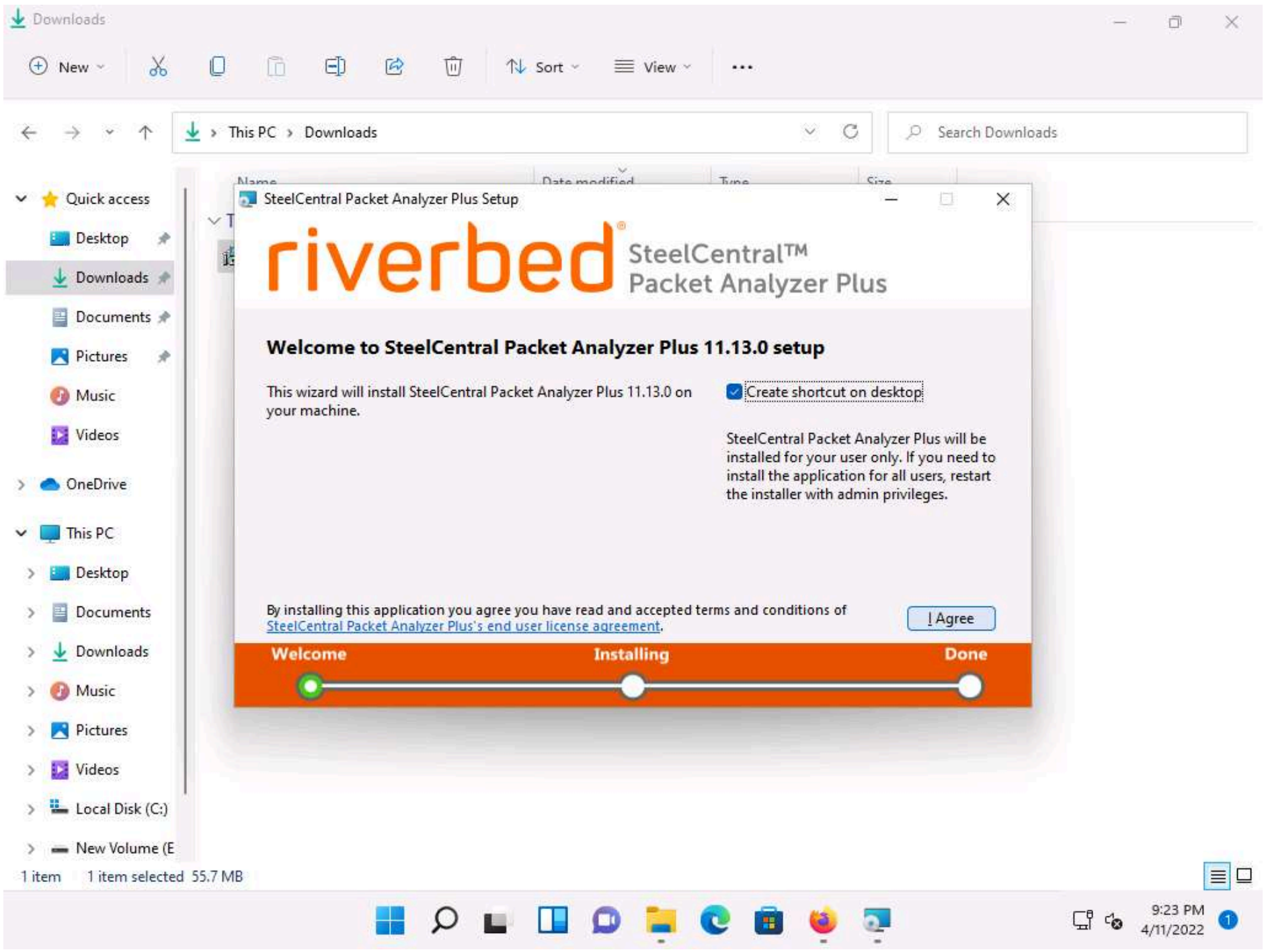


7. On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer_11.13.0_Setup.exe**.

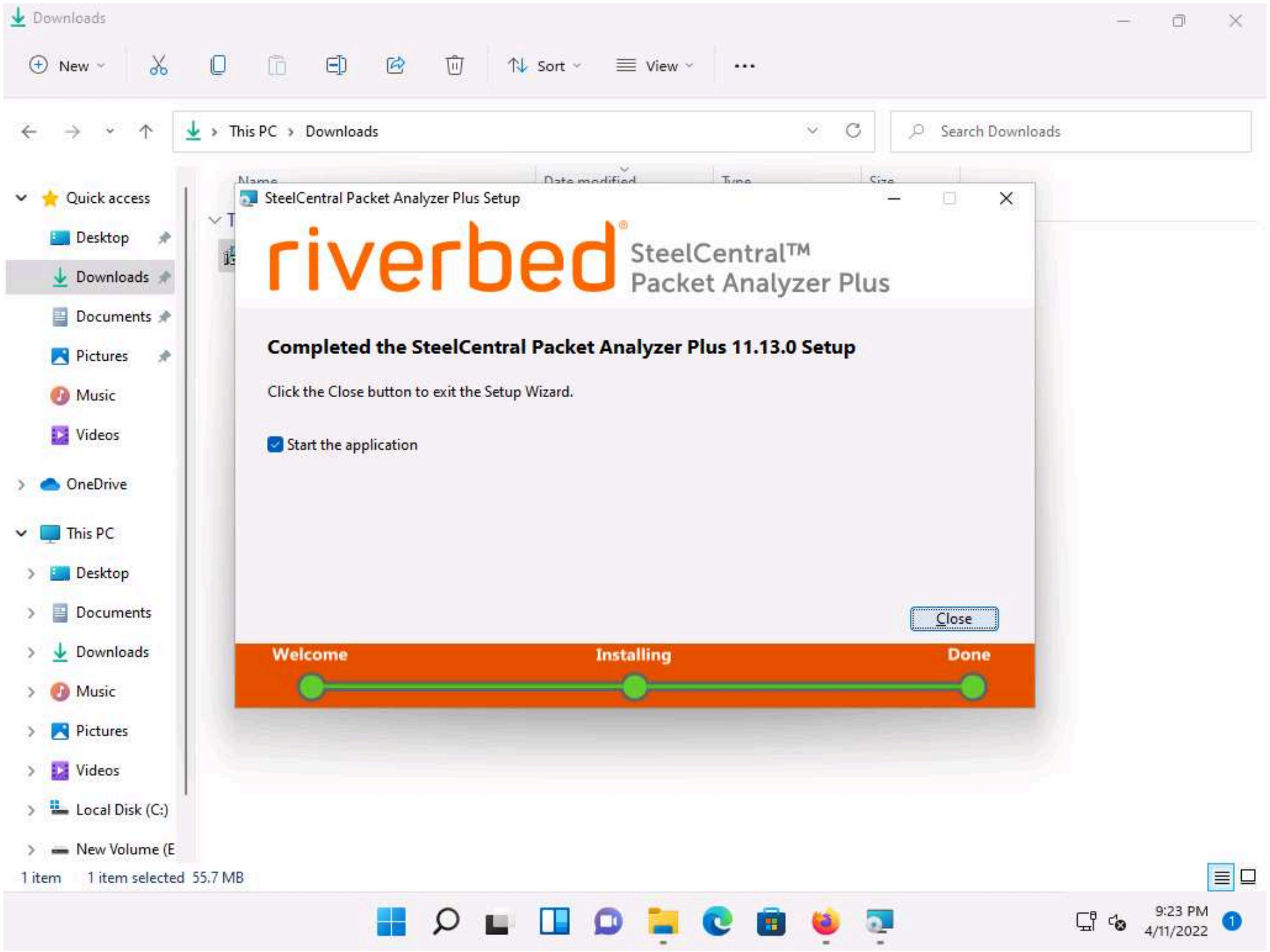


8. The **Open File - Security Warning** window appears; click **Run**.

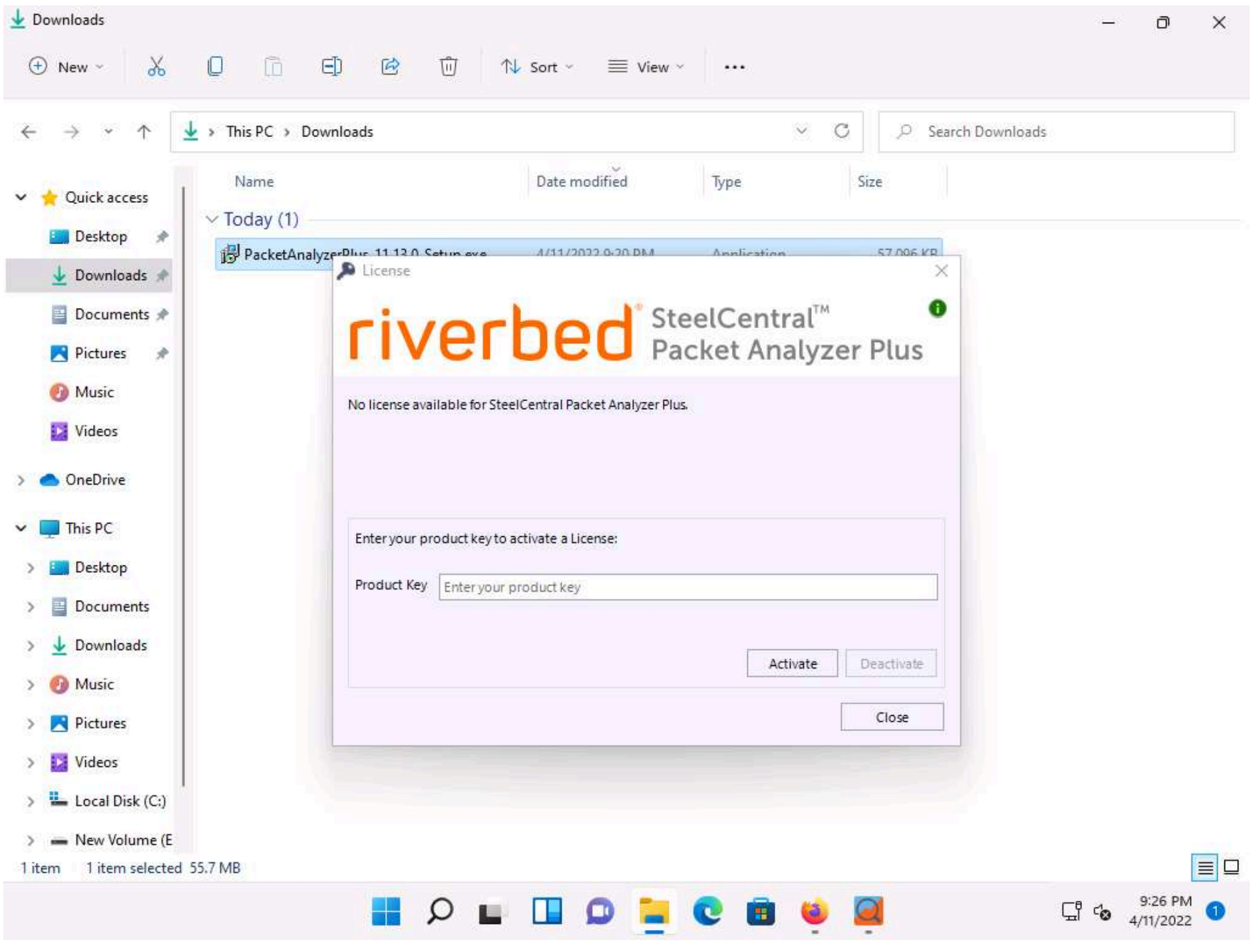
9. The **SteelCentral Packet Analyzer Plus Setup** window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.



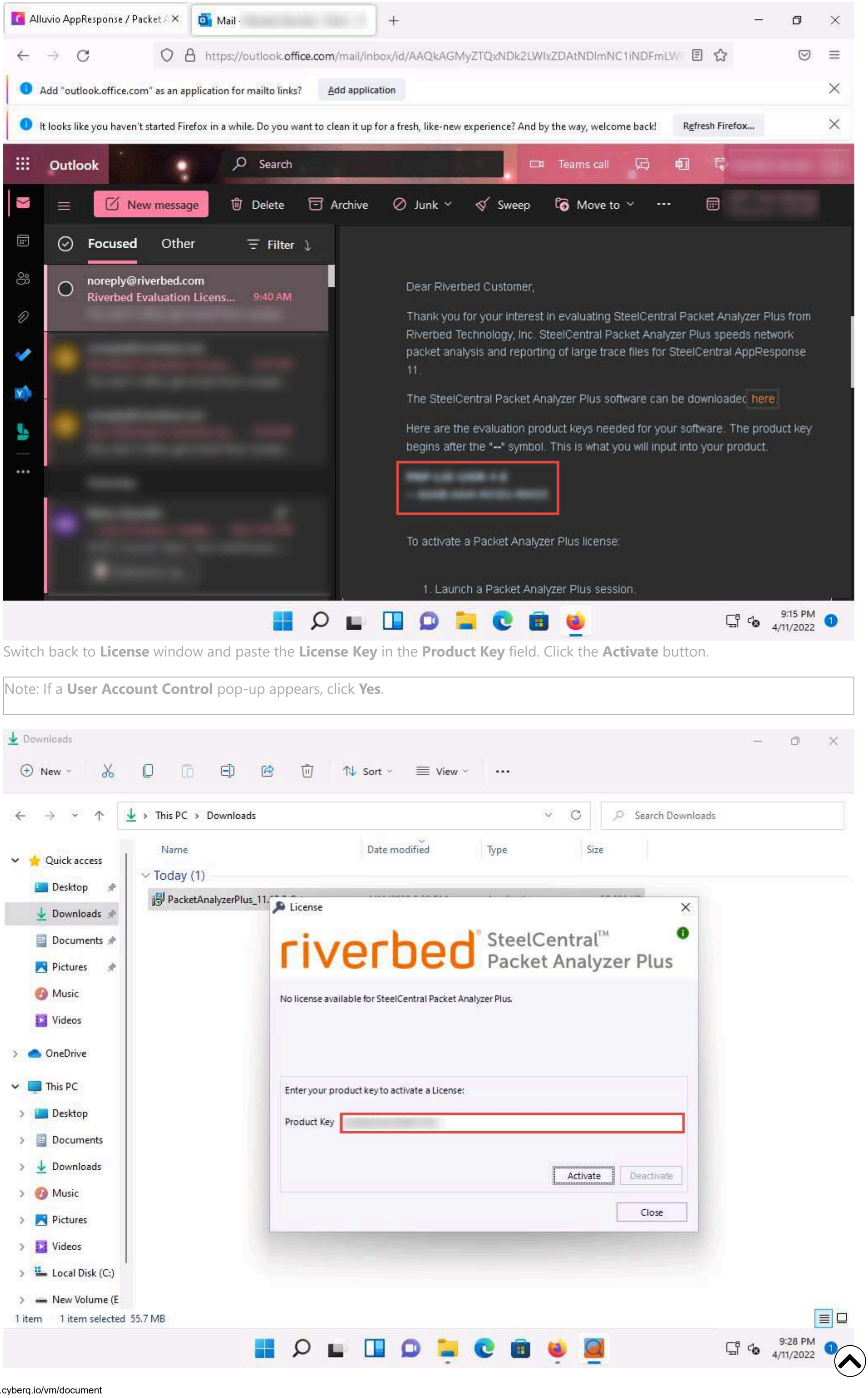
10. SteelCentral Packet Analyzer starts installing, and after the completion of the installation, the **Completed the SteelCentral Packet Analyzer Plus Setup** wizard appears. Ensure that the **Start the application** checkbox is selected and click **Close**.



11. The **License** window appears. Leave this window running.



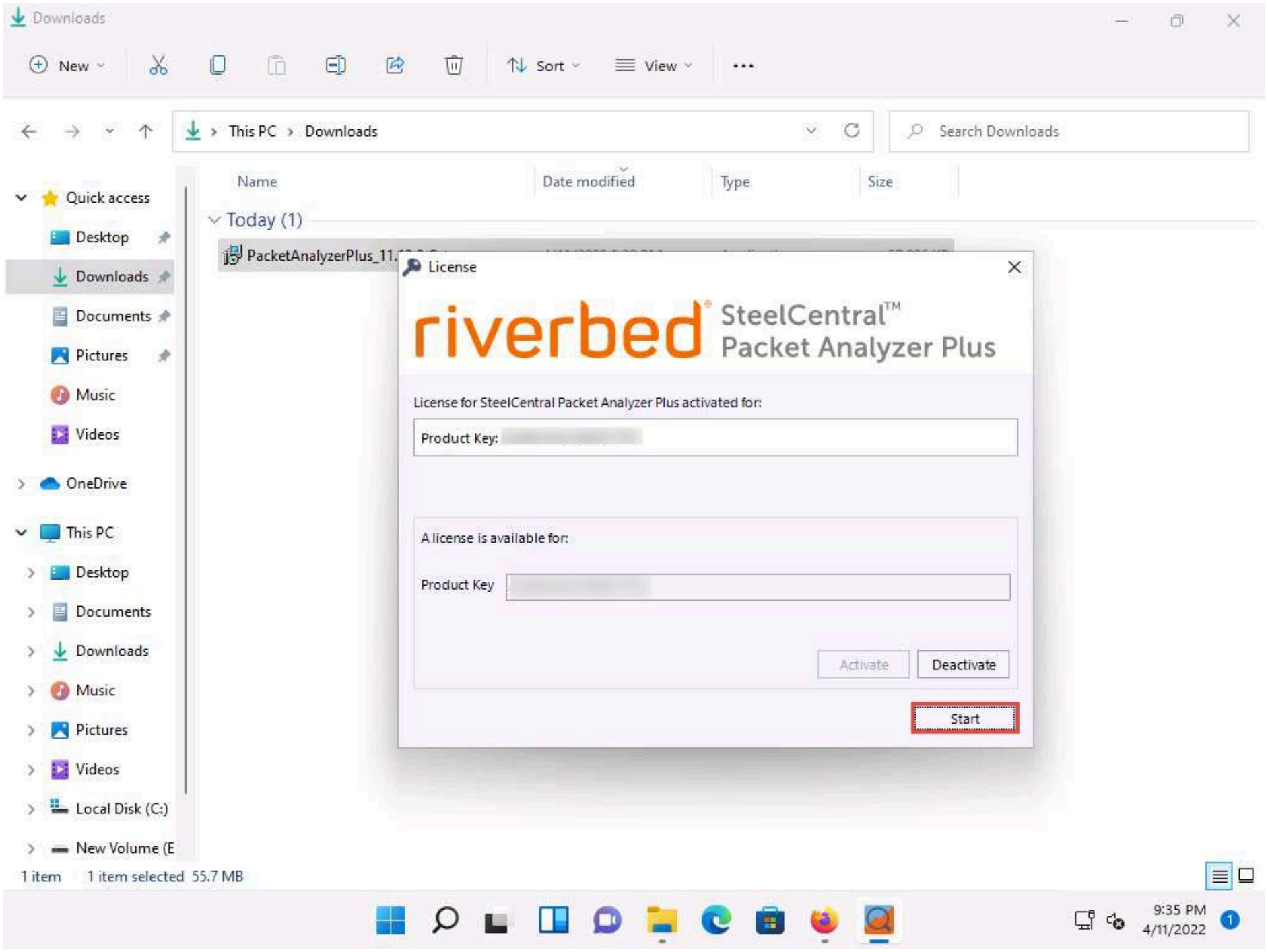
12. Switch to your browser (here, **Mozilla Firefox**). Navigate to the tab where the **Riverbed Evaluation License Request for SteelCentral PacketAnalyzer Plus** email is open and copy the **License Key** provided in the email.



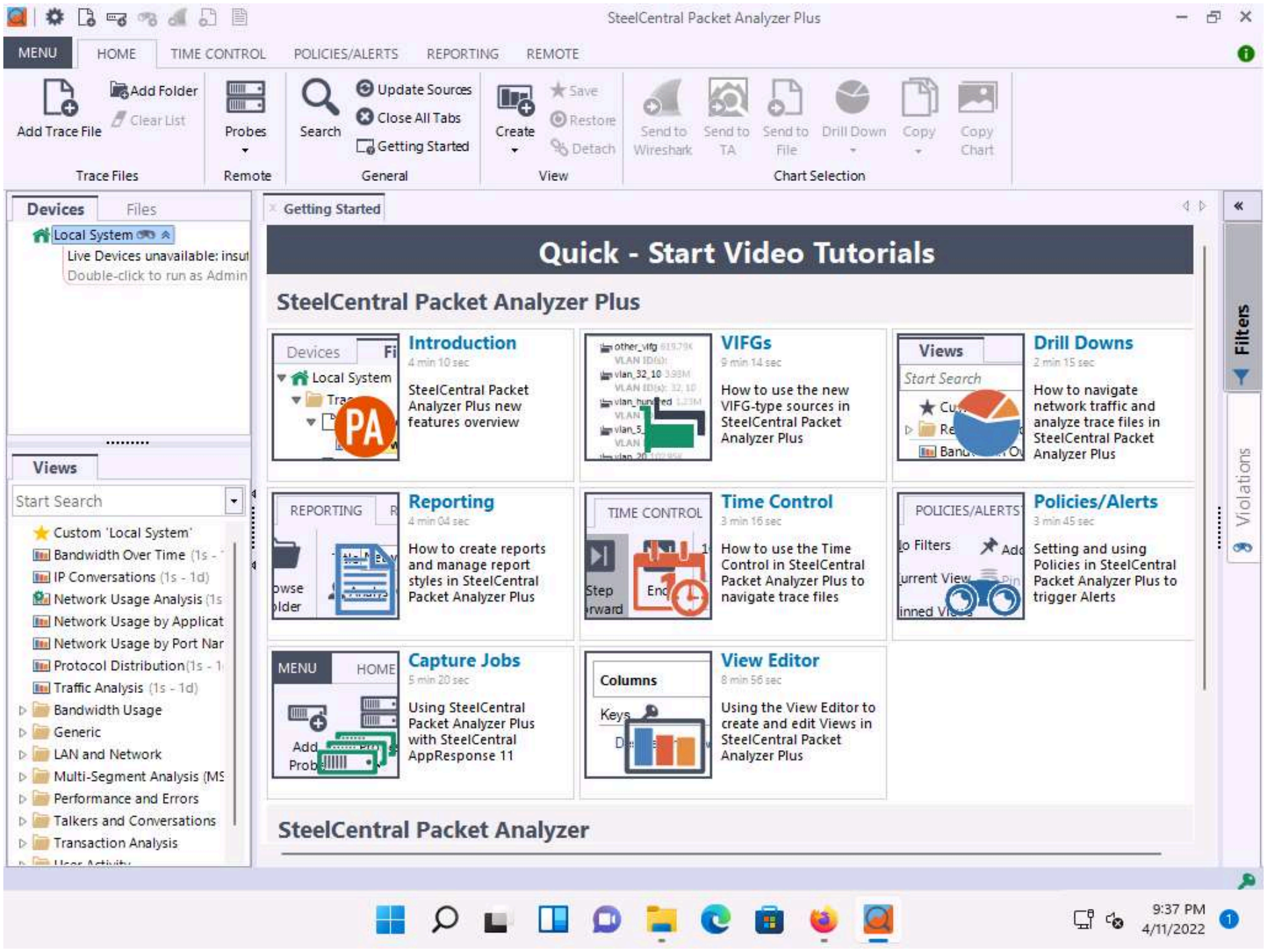
13. Switch back to **License** window and paste the **License Key** in the **Product Key** field. Click the **Activate** button.

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

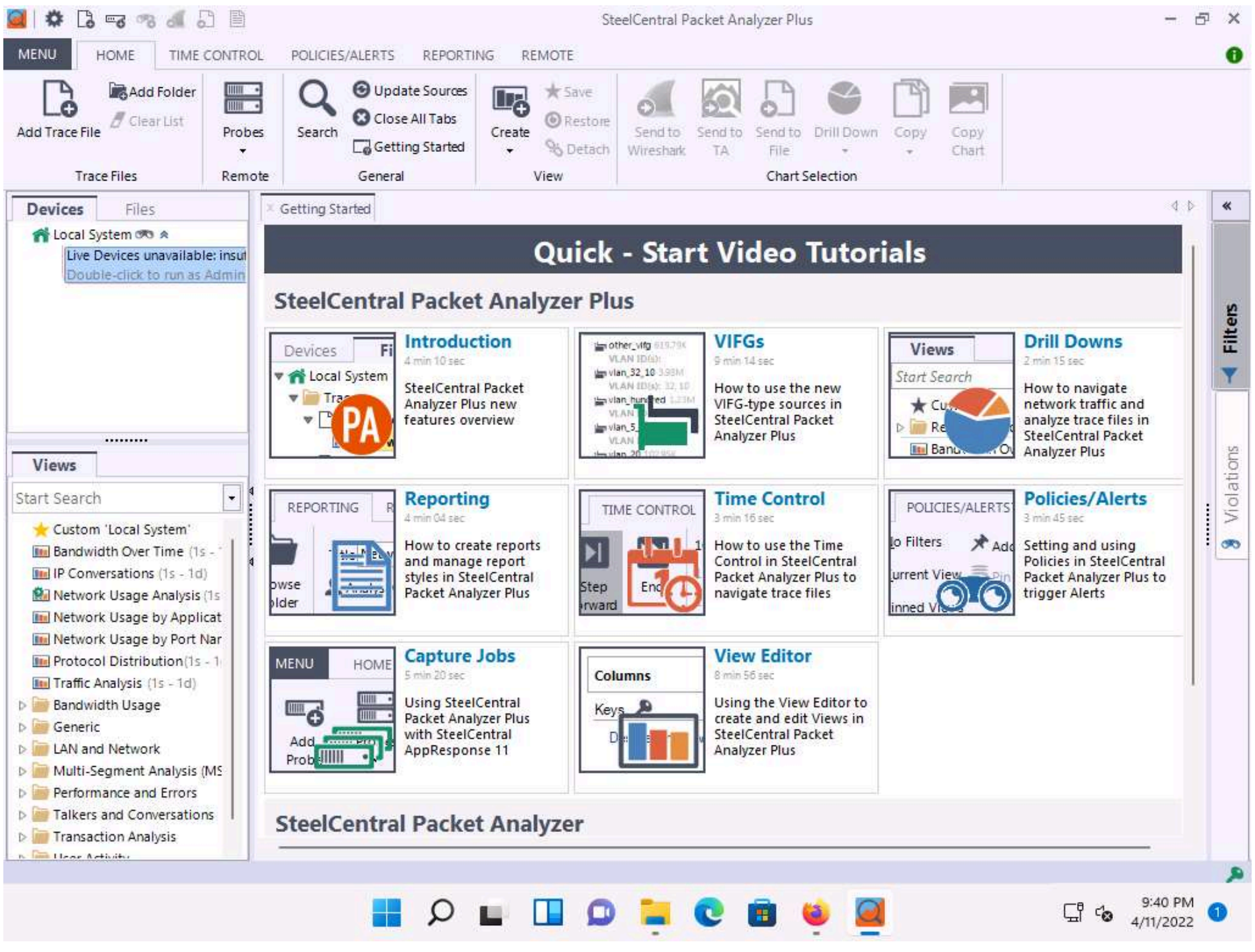
14. The **SteelCentral Packet Analyzer Plus license activated** notification appears; click the **Start** button to start the application.



15. The **SteelCentral Packet Analyzer Plus** main window appears, displaying the **Getting Started** tab options, as shown in the screenshot.

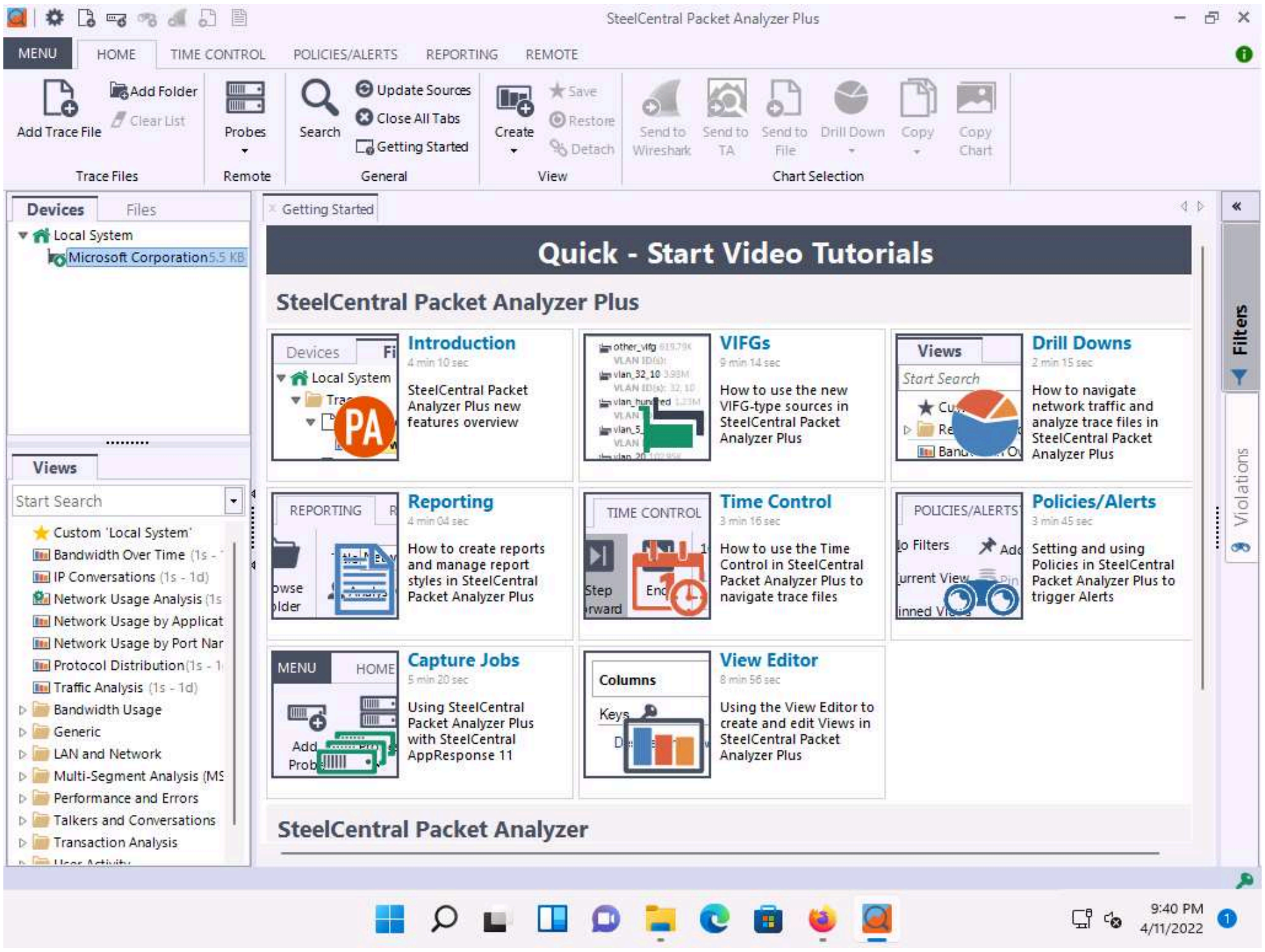


16. Observe that under the **Devices** tab in the left-hand pane, the application is unable to detect any **Local System** as it requires admin privileges. Therefore, double-click **Live Devices unavailable: Insufficient privileges** to run the application as an **Administrator**.



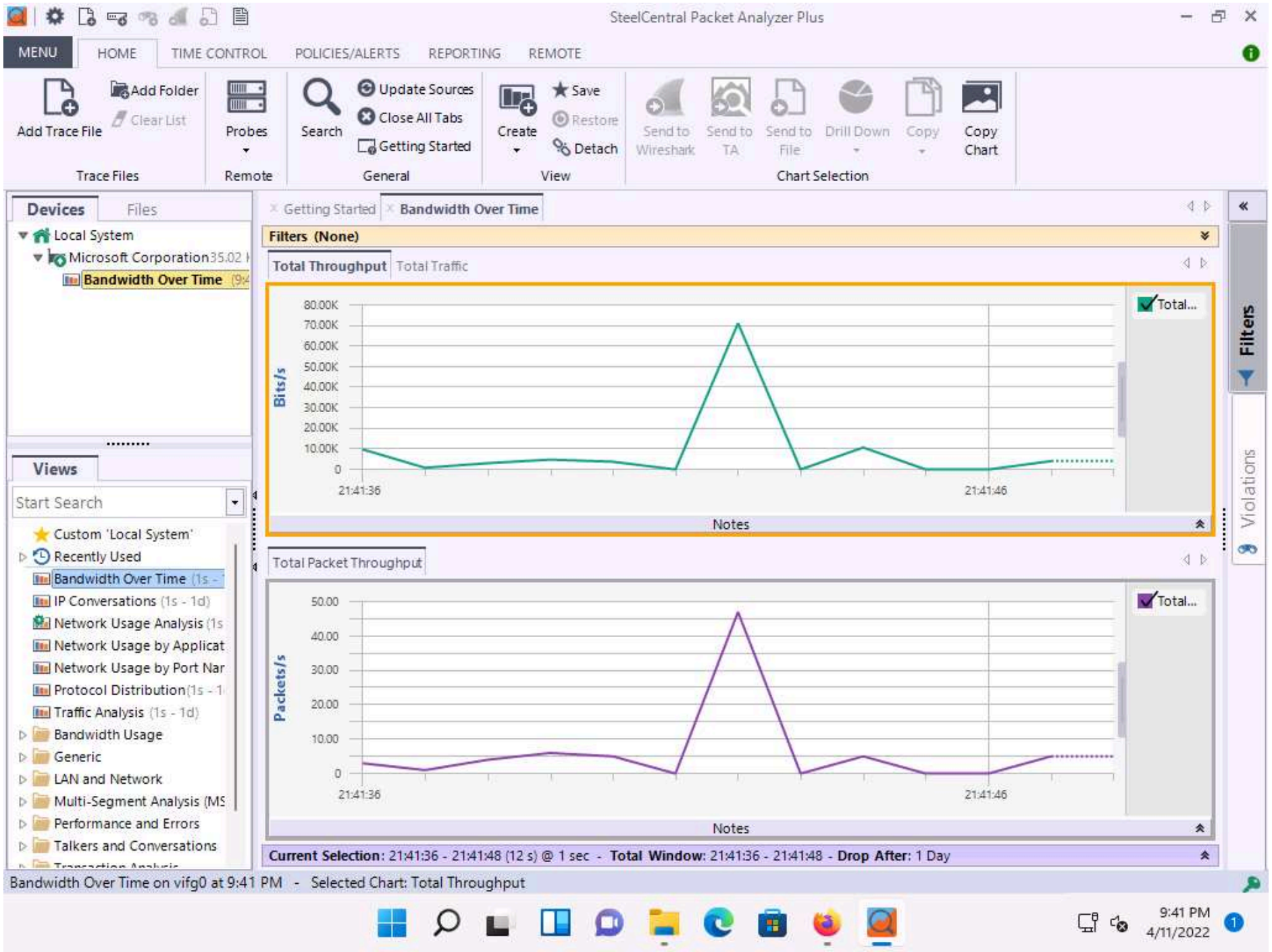
17. A **User Account Control** pop-up appears; click **Yes**.

18. Ethernet adapter appear under **Local System** in the left-hand pane. Click the **Microsoft Corporation** adapter.



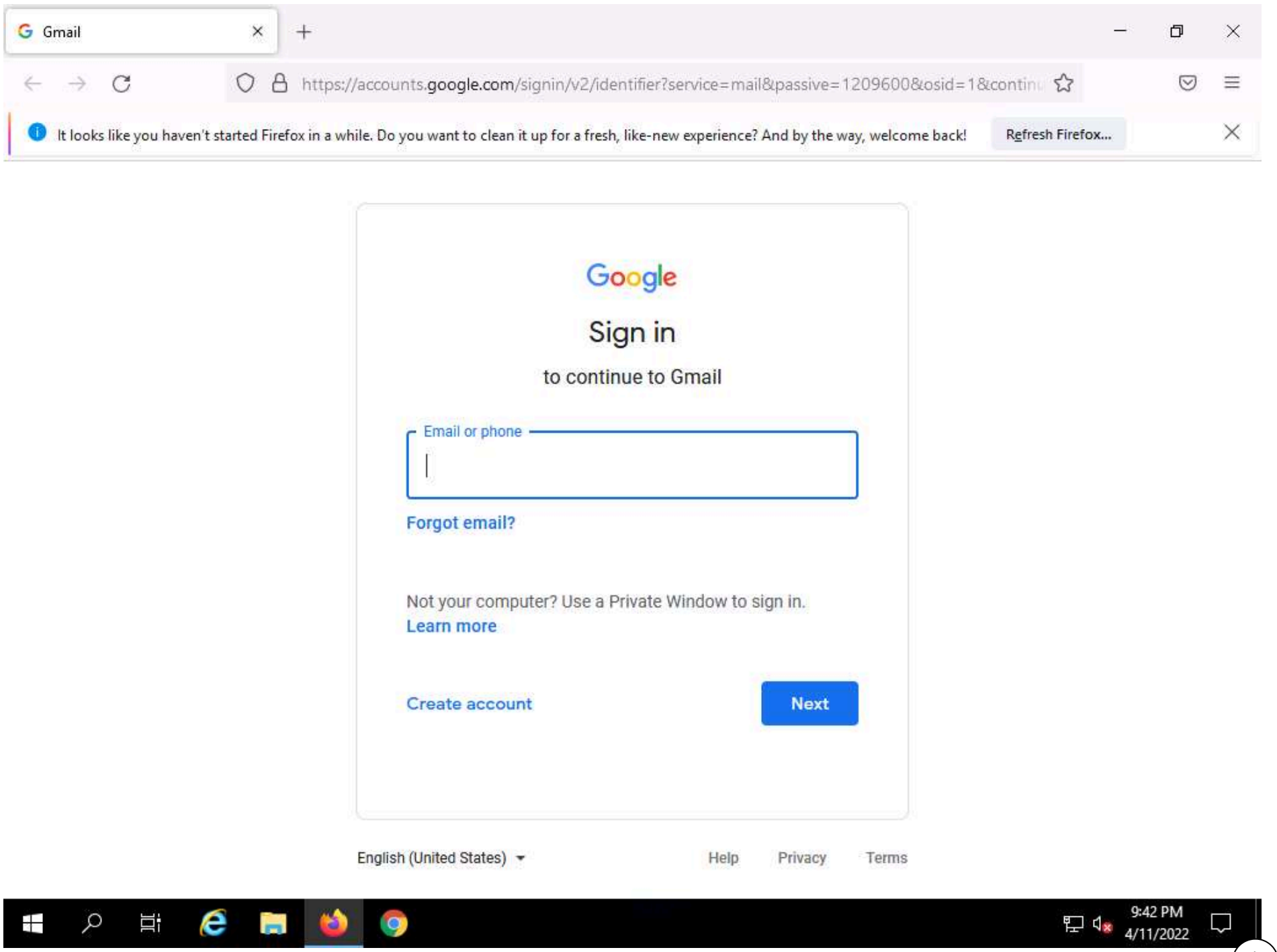
19. Double-click the **Bandwidth Over Time** option under the **Recently Used** node in the left-hand pane under the **Views** section.

20. A new **Bandwidth Over Time** tab appears, and SteelCentral Packet Analyzer Plus starts capturing the network traffic, as shown in the screenshot.

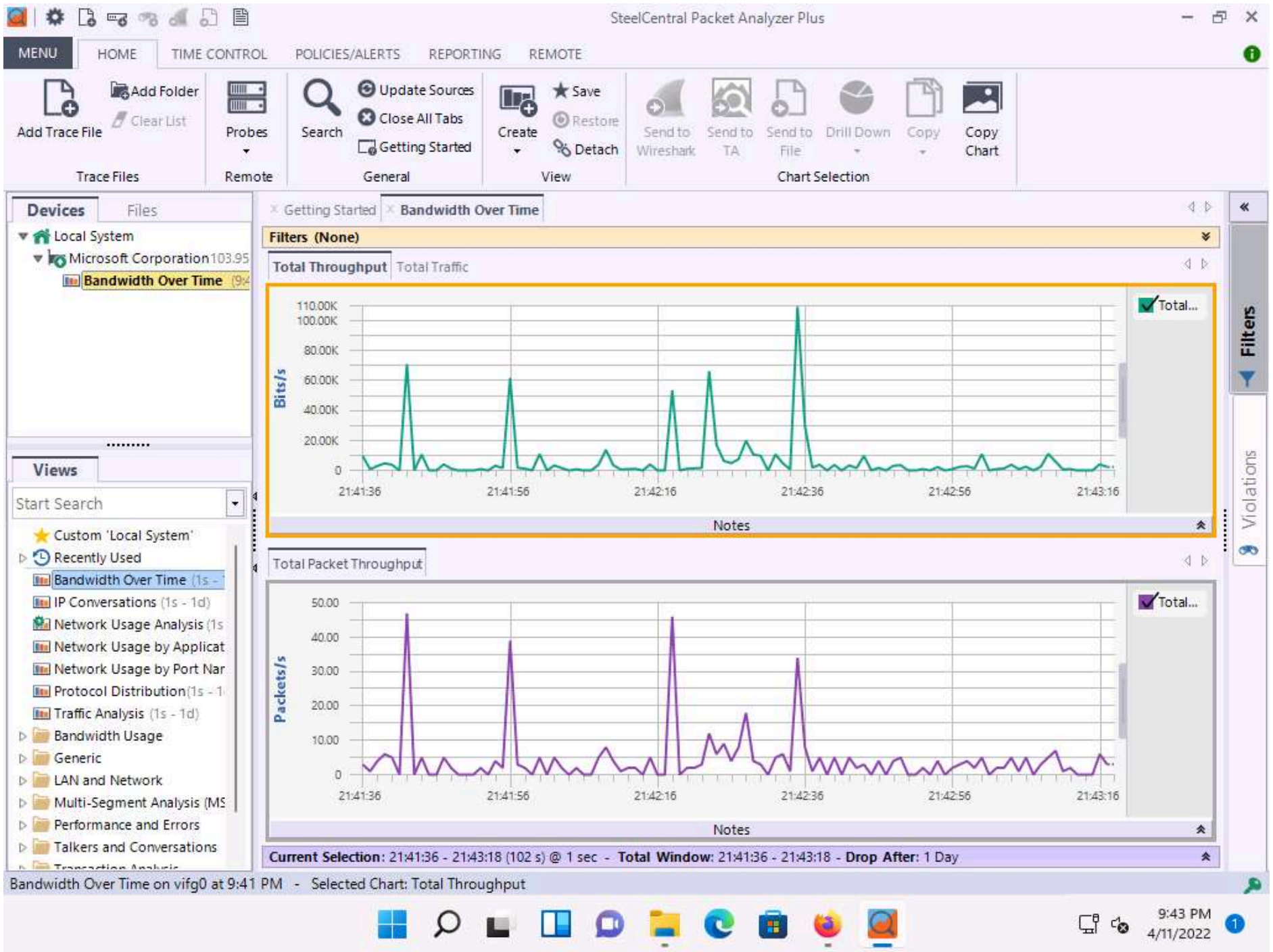


21. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

22. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.gmail.com**).

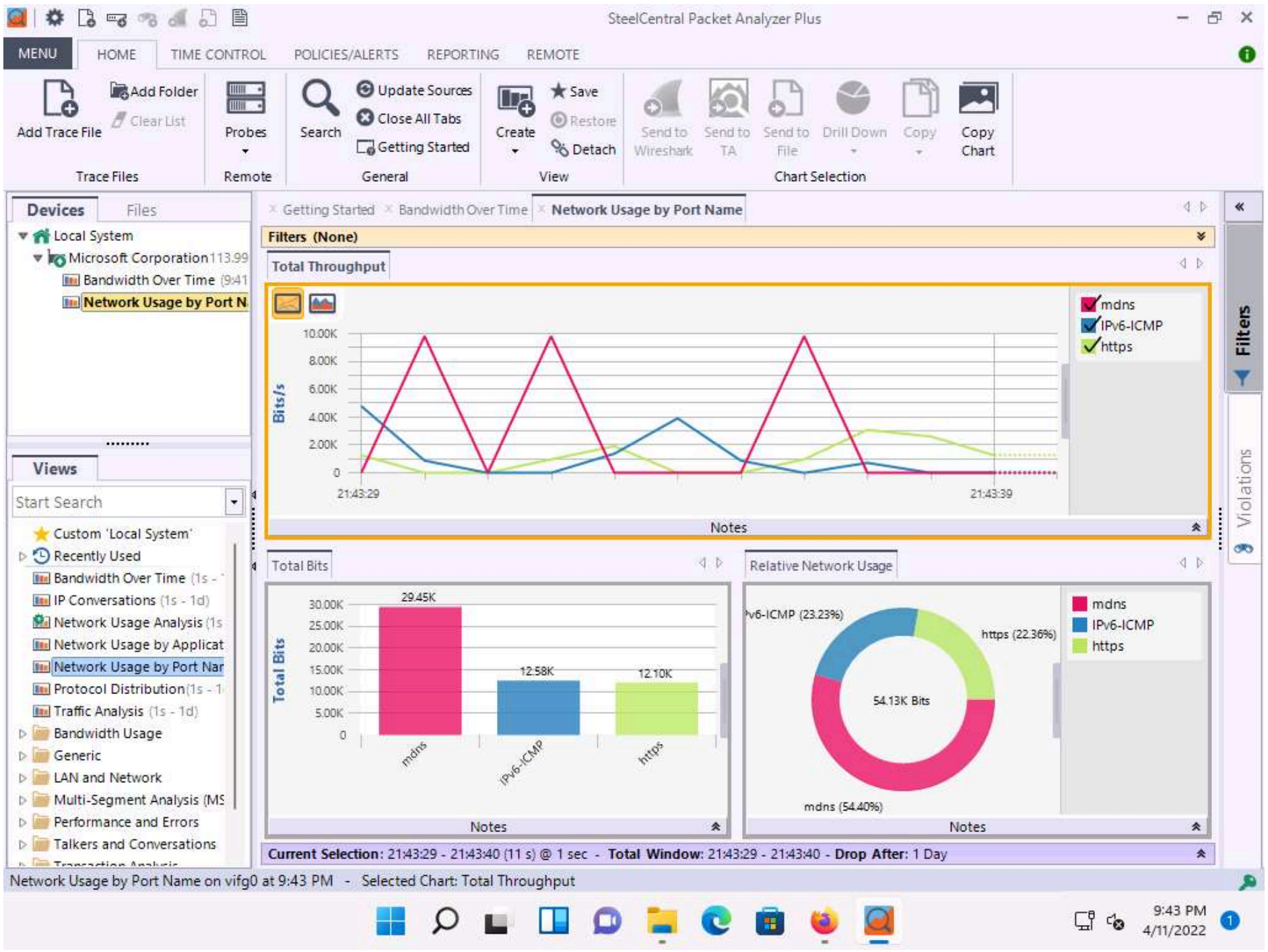


23. Click **CEHv12 Windows 11** to switch back to the **Windows 11** machine and observe the network traffic captured by **SteelCentral Packet Analyzer**, as shown in the screenshot.



24. Double-click the **Network Usage by Port Name** option under the **Recently Used** node in the left-hand pane under the **Views** section.

25. A new **Network Usage by Port Name** tab appears, and **SteelCentral Packet Analyzer Plus** displays the captured network traffic.

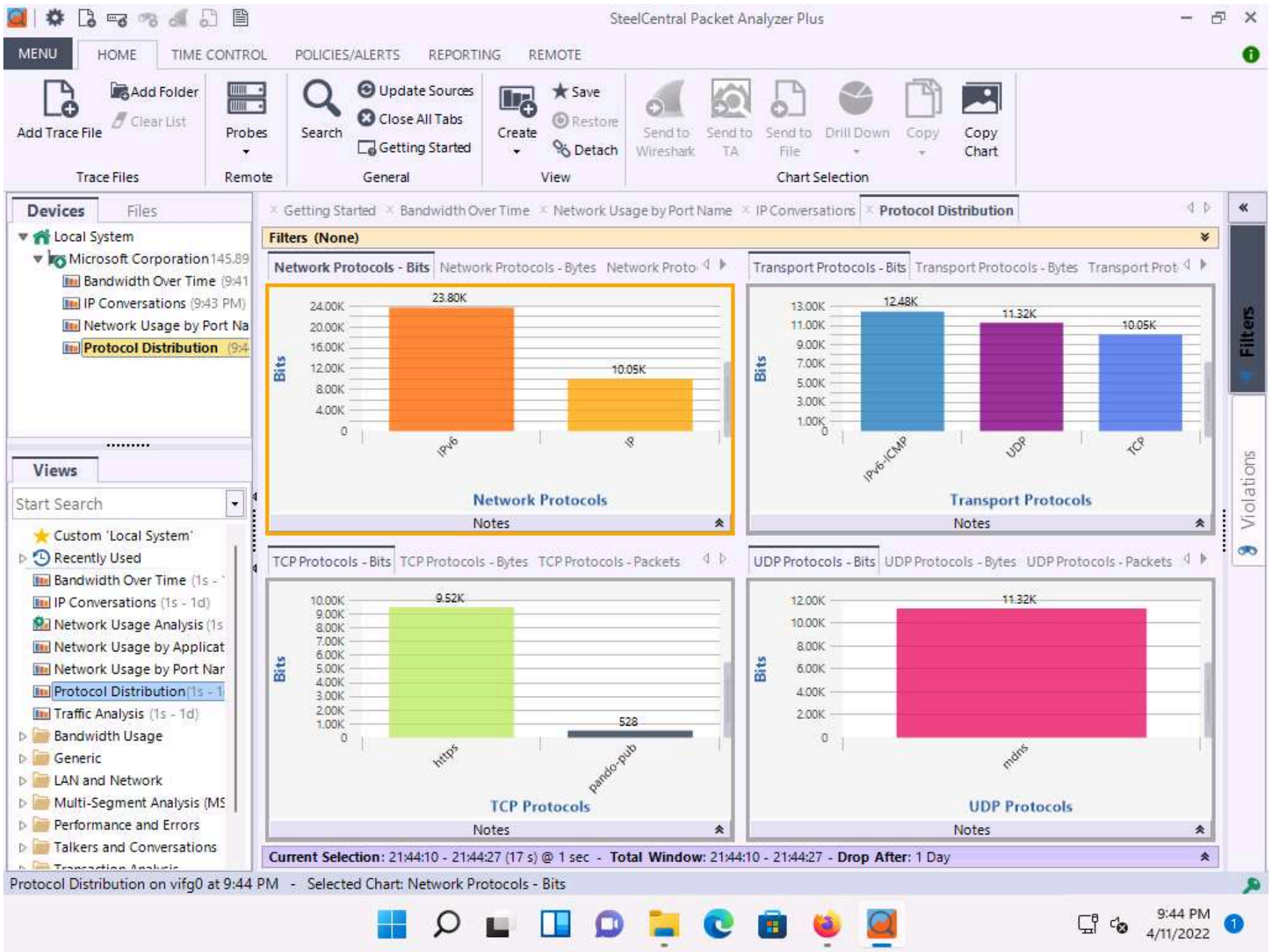


26. Double-click the **IP Conversations** option under the **Recently Used** node in the left-hand pane under the **Views** section.

27. A new **IP Conversations** tab appears, displaying conversations between different IP addresses in a map view.

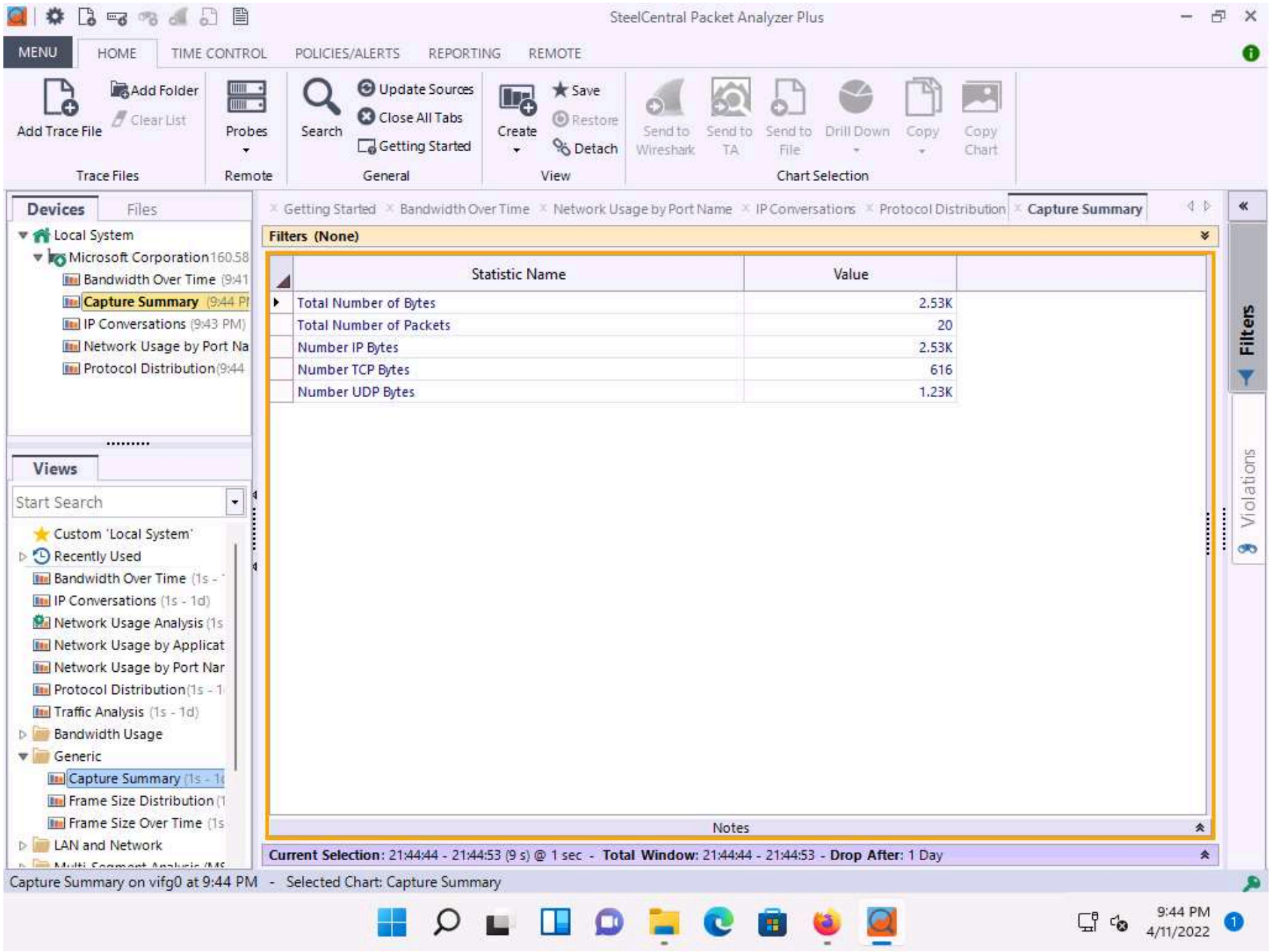
28. Double-click the **Protocol Distribution** option under the **Recently Used** node in the left-hand pane under the **Views** section.

29. A new **Protocol Distribution** tab appears, displaying **Network Protocols**, **Transport Protocols**, **TCP Protocols**, **UDP Protocols**, and other information, as shown in the screenshot.



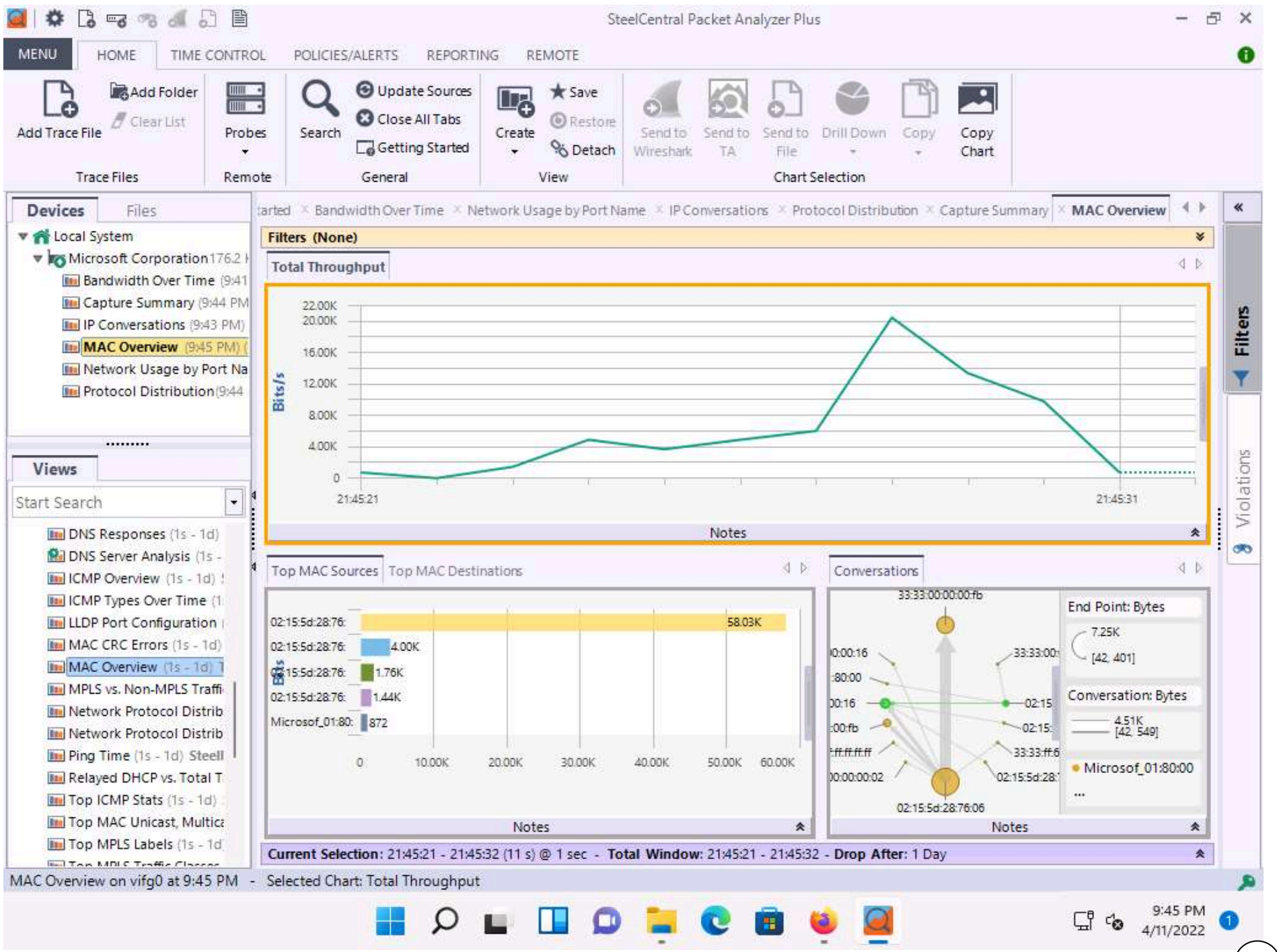
30. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.

31. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.



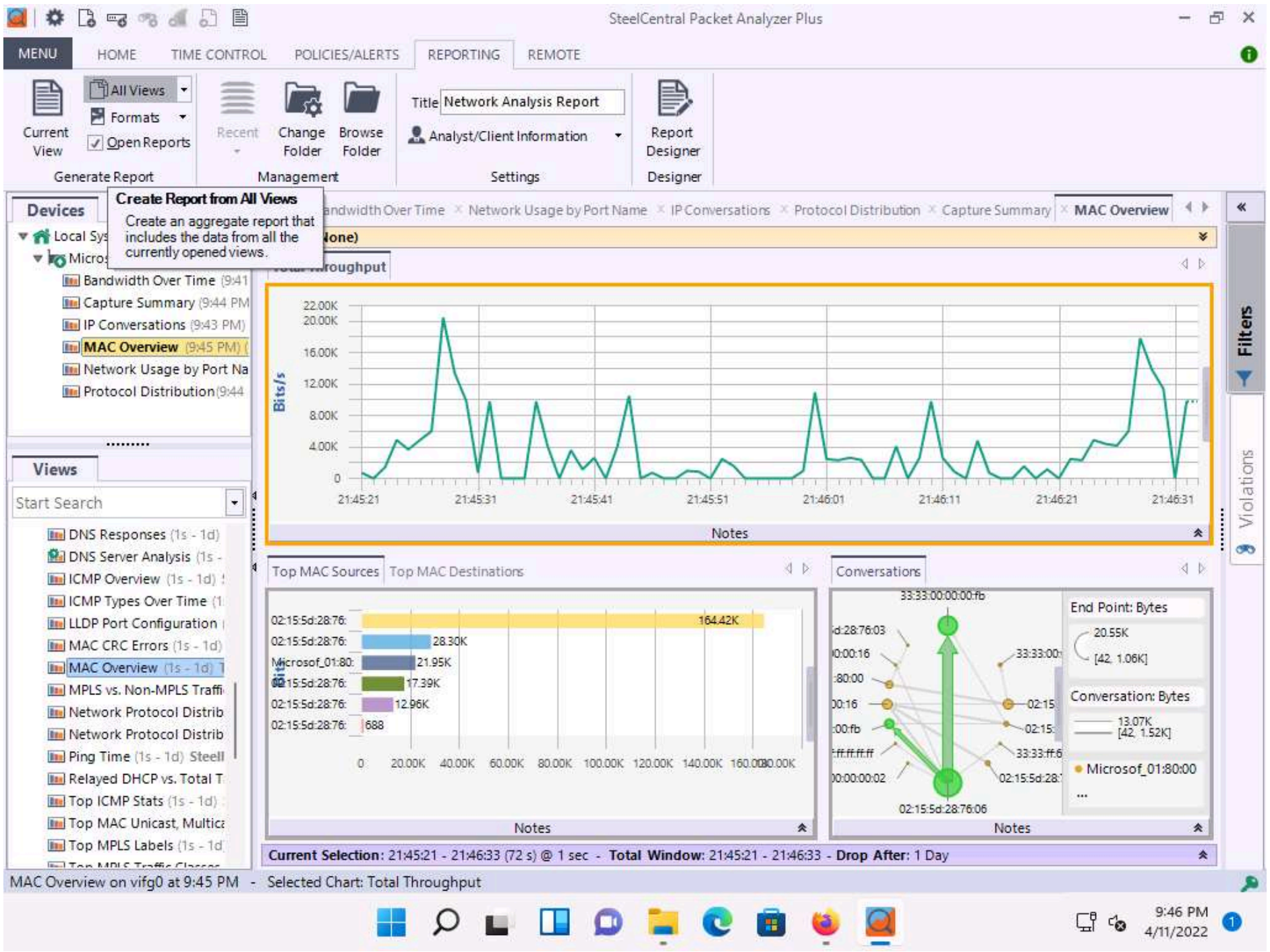
32. Expand the **LAN and Network** node and double-click the **MAC Overview** option in the left-hand pane.

33. A new **MAC Overview** tab appears, displaying information about MAC sources and destinations and MAC conversations.

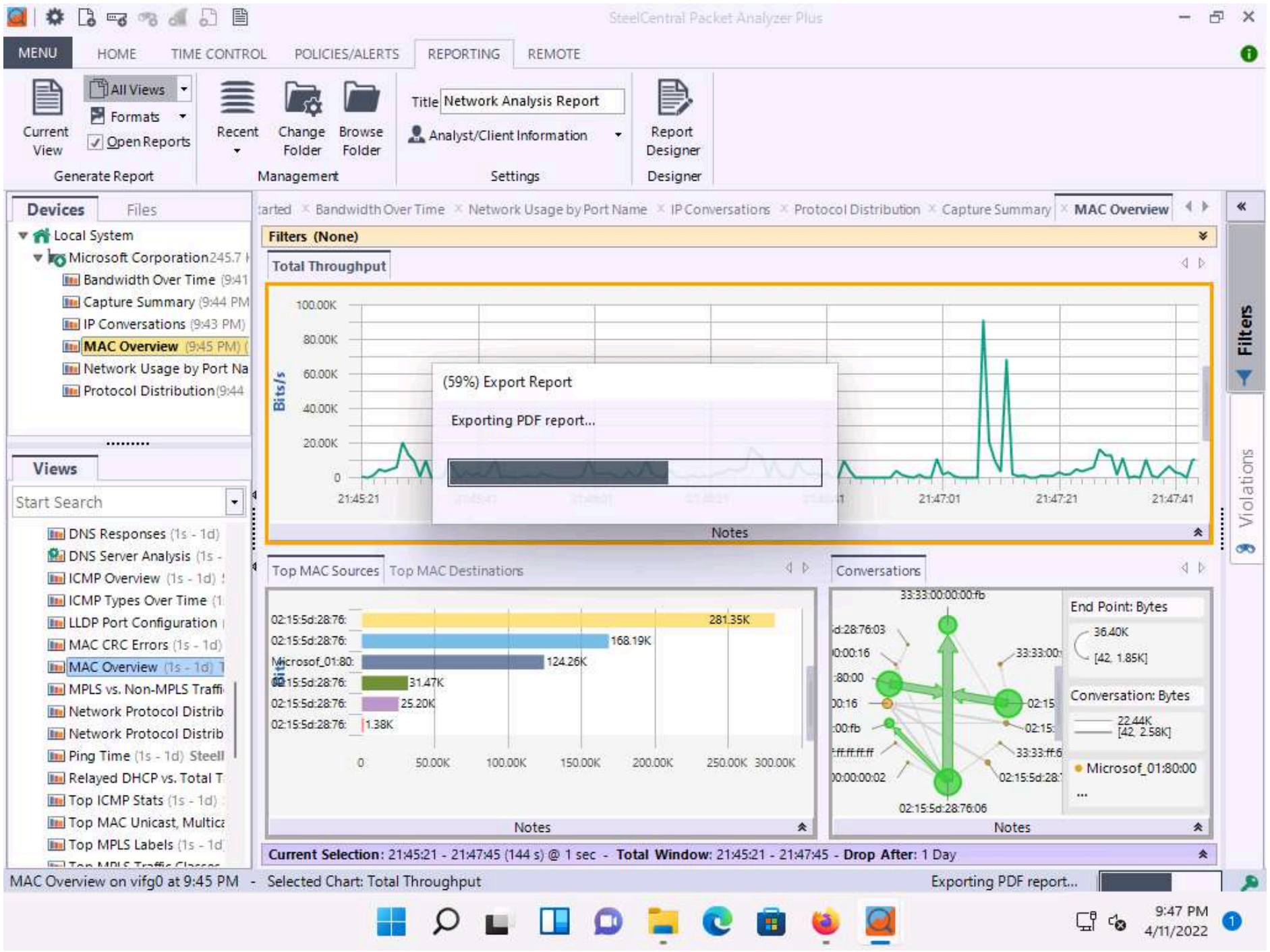


34. Similarly, you can explore various options in other nodes such as VLAN, MPLS, ARP, ICMP, and DHCP.

35. Click **Reporting** from the menu bar. Click on the **All Views** option to generate a report that includes all views.

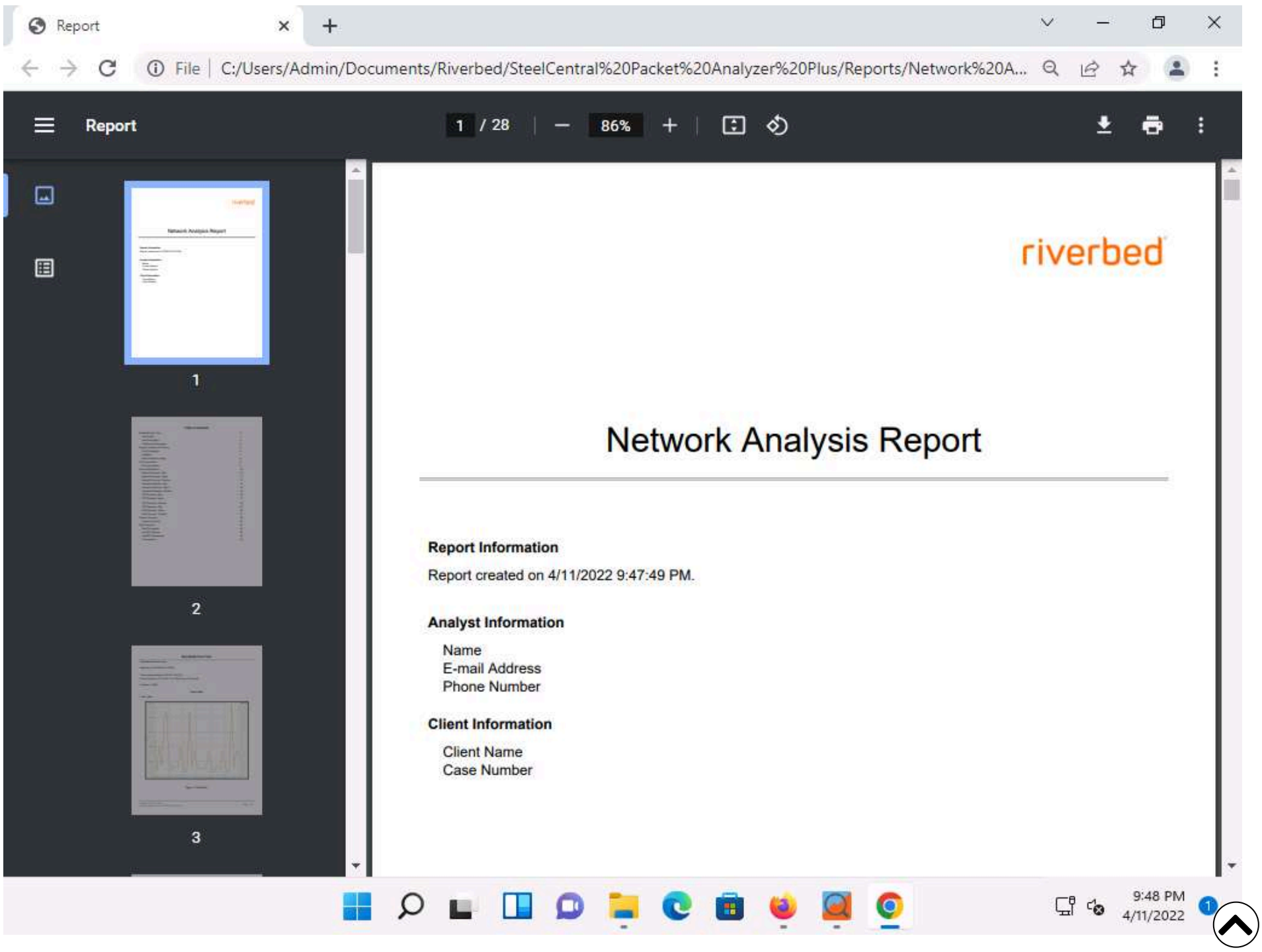


36. An **Export Report** pop-up appears, and the report starts exporting.

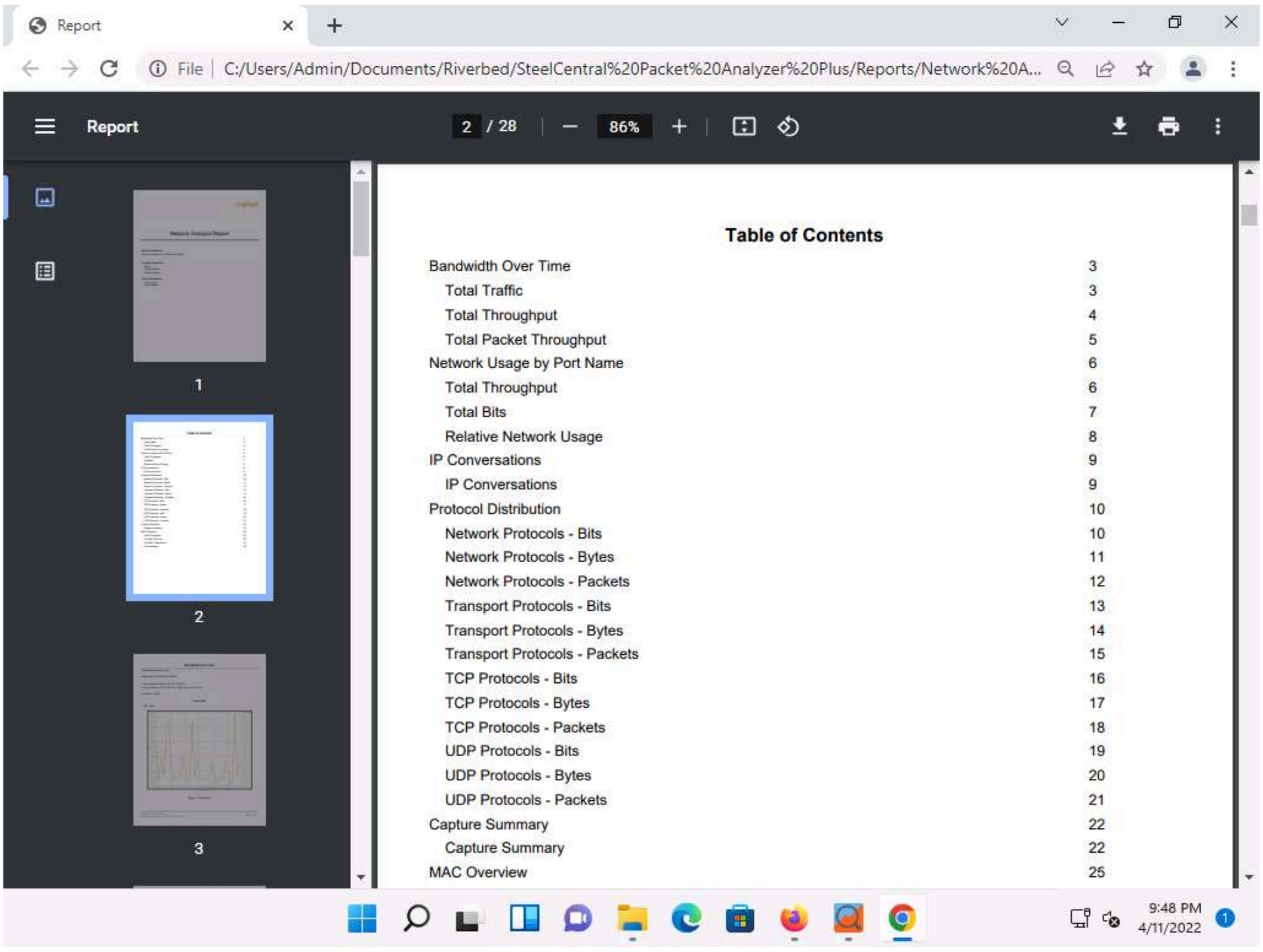


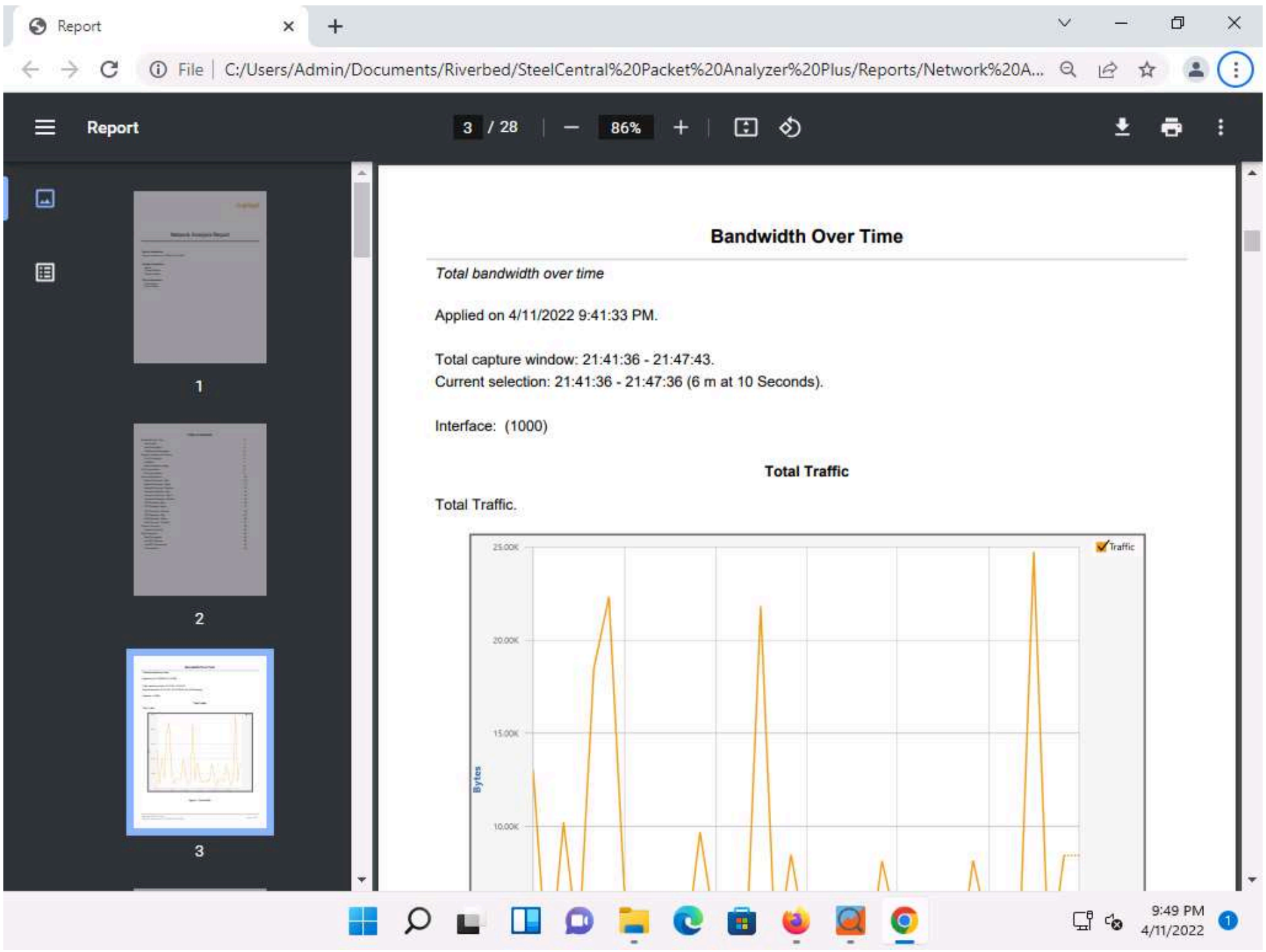
37. After completing the extraction, the generated report appears, as shown in the screenshot.

Note: If a **How do you want to open this file?** pop up appears, click on **Google Chrome** and press **OK**



38. Scroll down to view detailed information on each option shown in **Table of Contents**.





39. This concludes the demonstration of analyzing a network using SteelCentral Packet Analyzer.

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

Lab 3: Detect Network Sniffing

Lab Scenario

The previous labs demonstrated how an attacker carries out sniffing with different techniques and tools. This lab helps you understand possible defensive techniques used to defend a target network against sniffing attacks.

A professional ethical hacker or pen tester should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the various network sniffing detection techniques and tools discussed in this lab.

Lab Objectives

- Detect ARP poisoning and promiscuous mode in a switch-based network
- Detect ARP poisoning using the Capsa Network Analyzer

Overview of Detecting Network Sniffing

Network sniffing involves using sniffer tools that enable the real-time monitoring and analysis of data packets flowing over computer networks. These network sniffers can be detected by using various techniques such as:

- **Ping Method**: Identifies if a system on the network is running in promiscuous mode
- **DNS Method**: Identifies sniffers in the network by analyzing the increase in network traffic
- **ARP Method**: Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

Task 1: Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network

ARP poisoning involves forging many ARP request and reply packets to overload a switch. ARP cache poisoning is the method of attacking a LAN network by updating the target computer's ARP cache with both forged ARP request and reply packets designed to change the Layer 2 Ethernet MAC address (that of the network card) to one that the attacker can monitor. Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

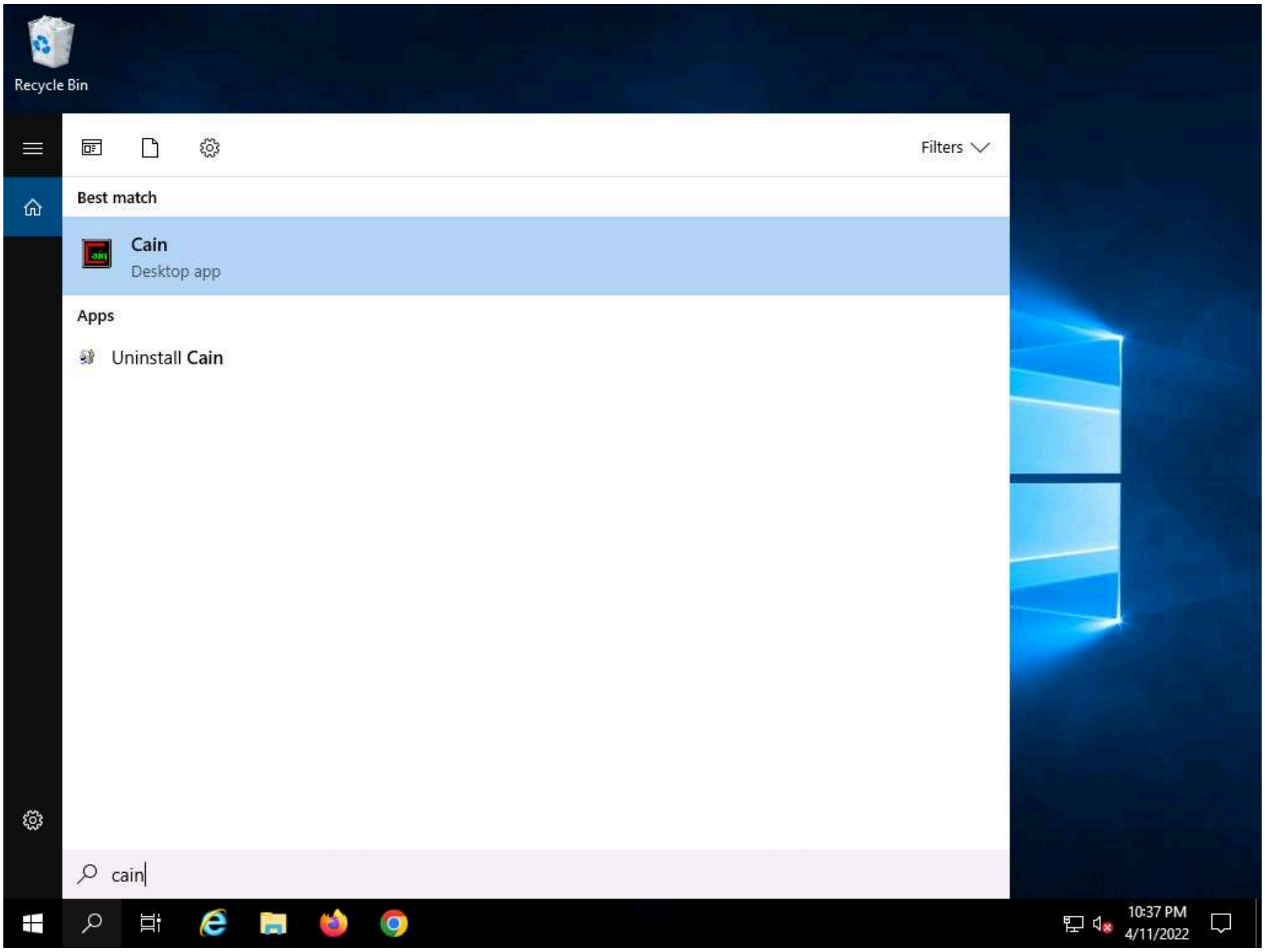
Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools.

The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

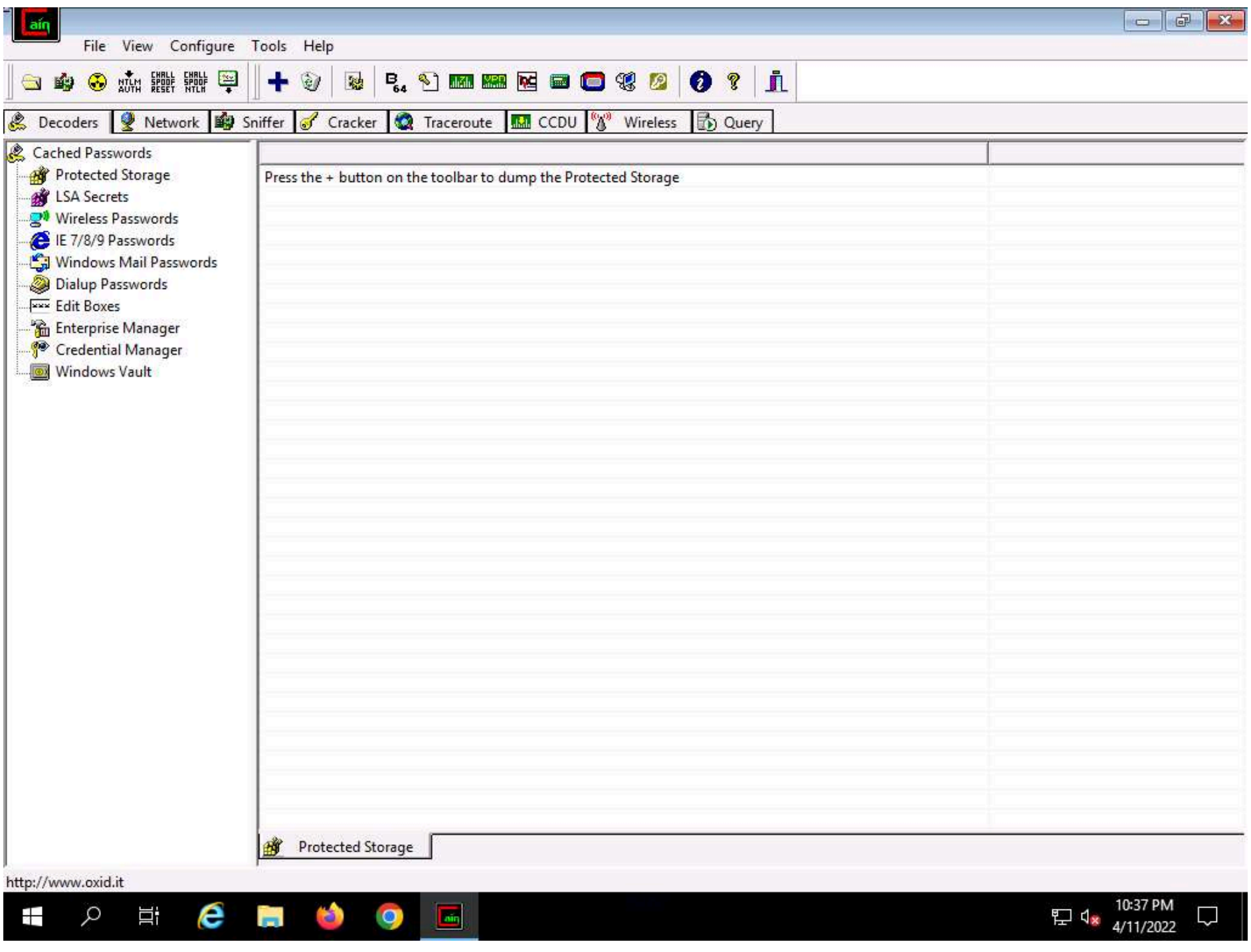
Here, we will detect ARP poisoning in a switch-based network using Wireshark and we will use the Nmap Scripting Engine (NSE) to check if a system on a local Ethernet has its network card in promiscuous mode.

> Note: In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 11** and **Parrot Security** machines. We will use the same machine (**Windows Server 2019**) to detect ARP poisoning and use the Windows 11 machine to detect promiscuous mode in the in the network.

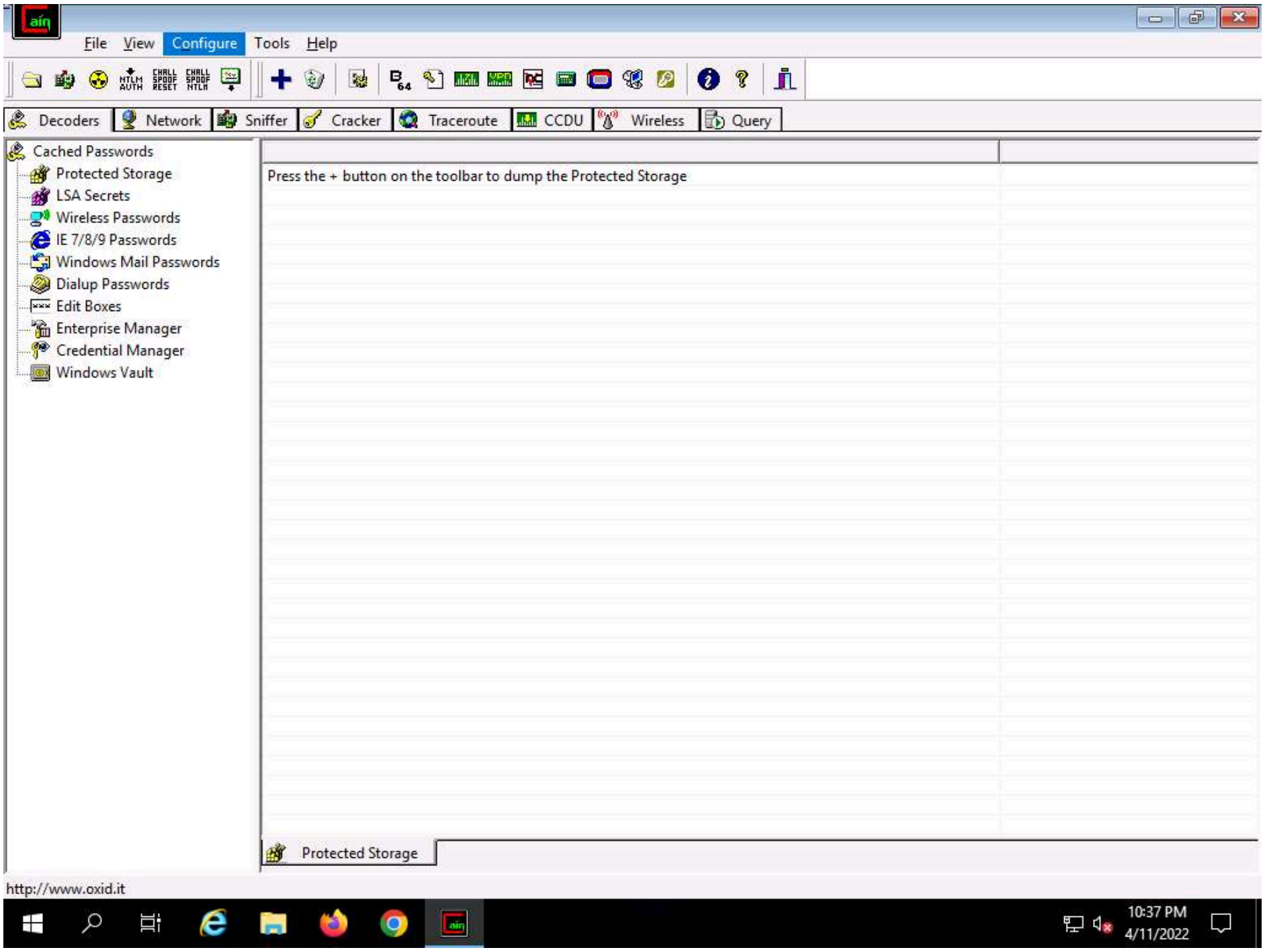
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



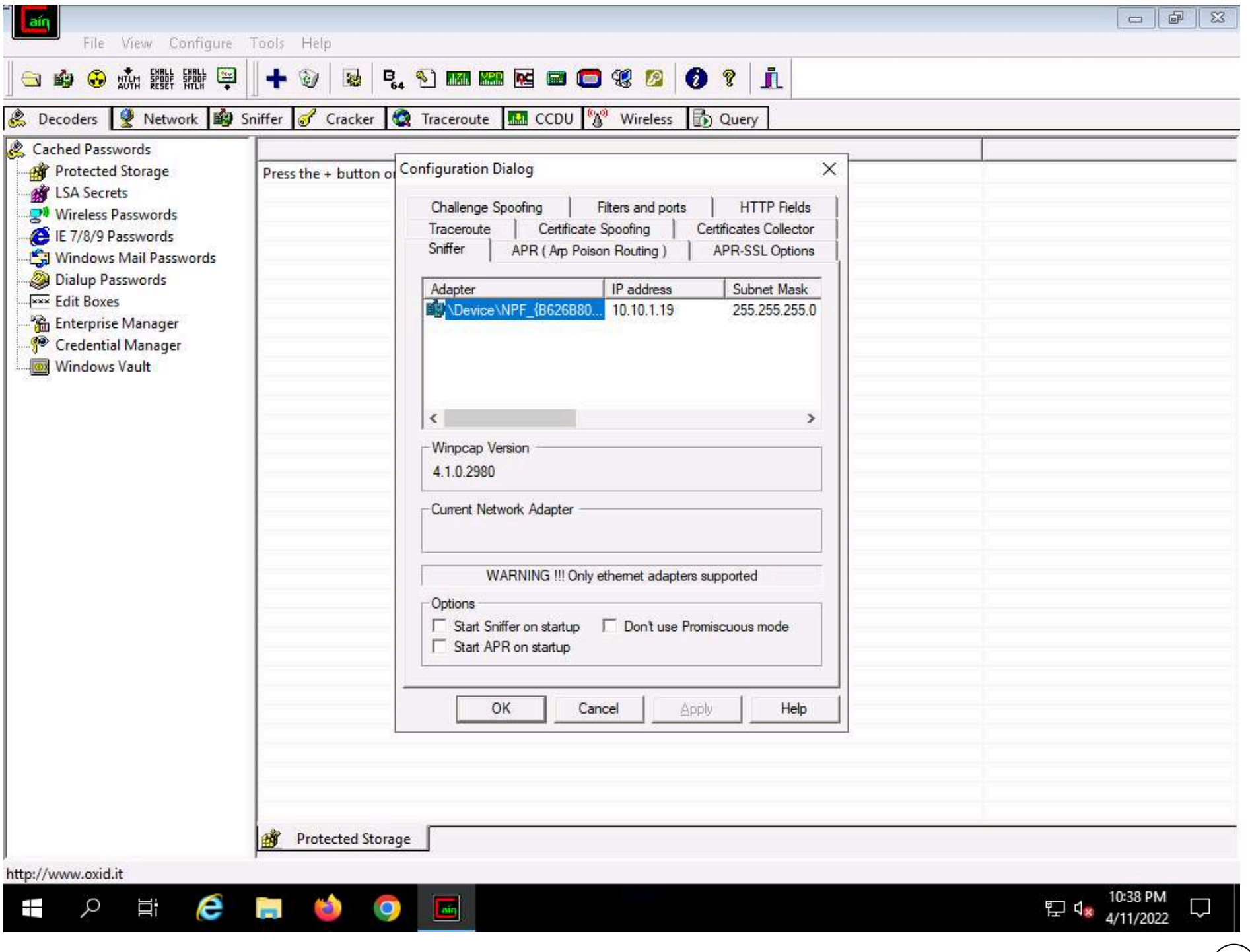
3. The **Cain & Abel** main window appears, as shown in the screenshot.



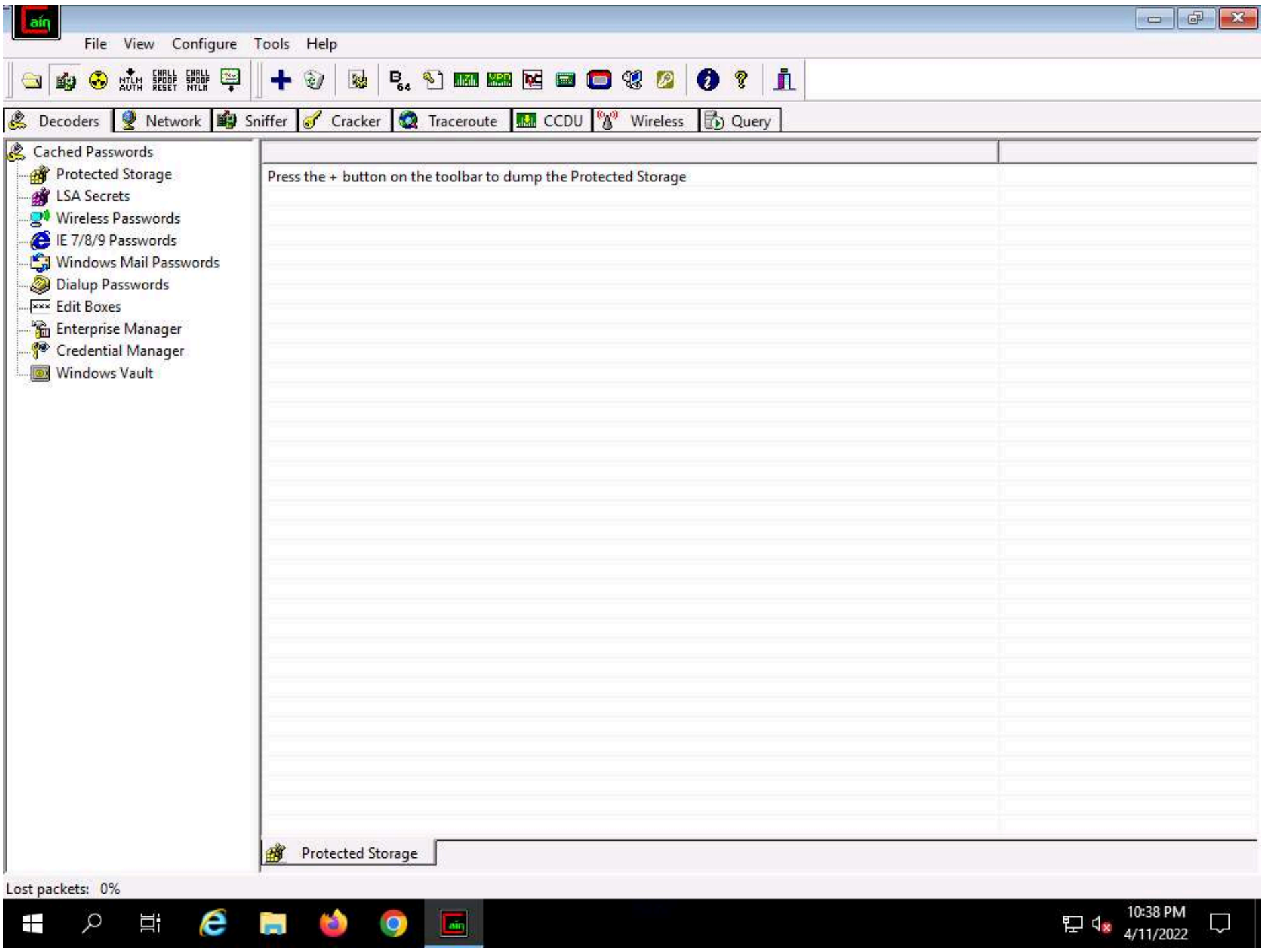
4. Click **Configure** from the menu bar to configure an ethernet card.



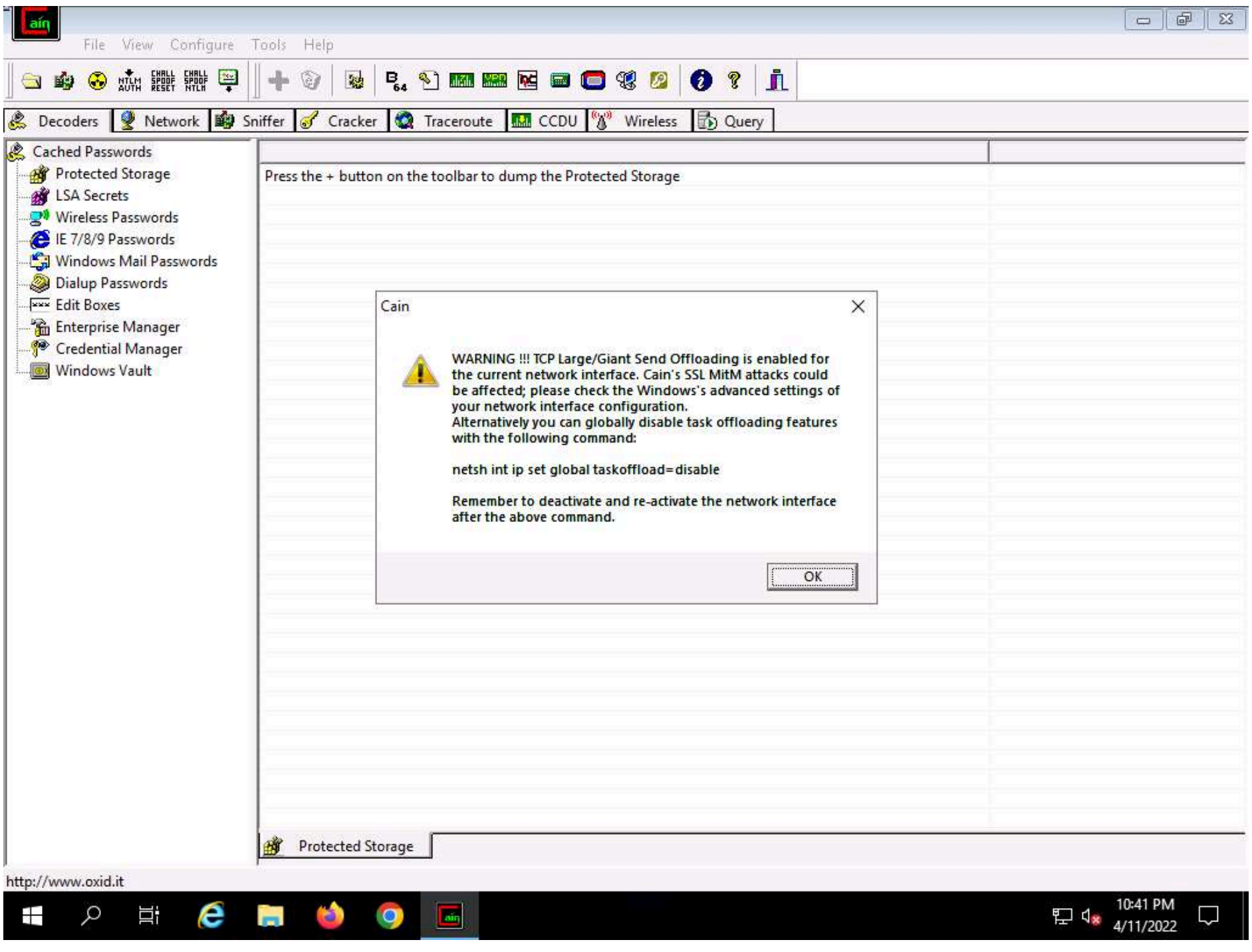
5. The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.



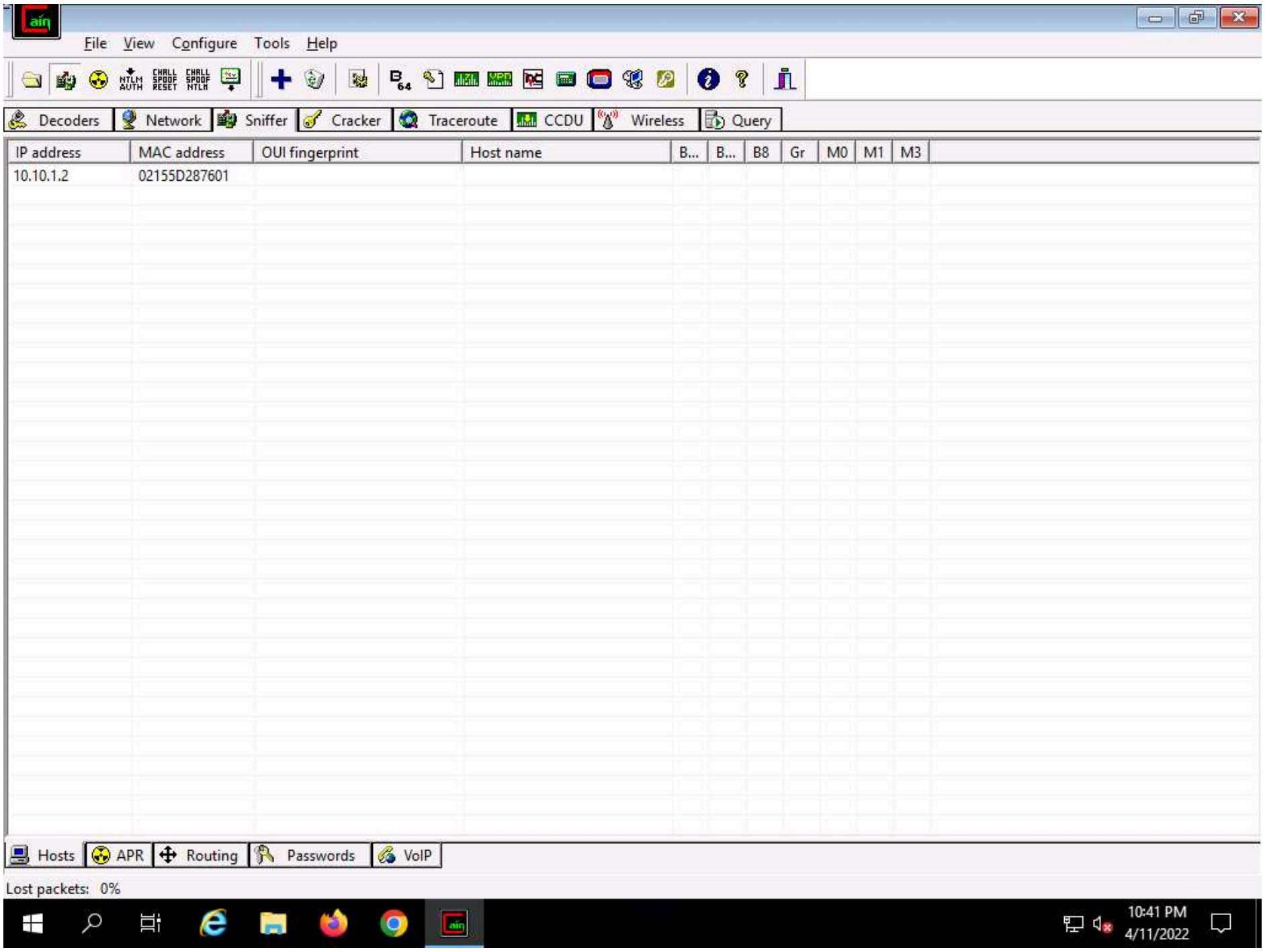
6. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



7. The **Cain** pop-up appears with a **Warning** message, click **OK**.

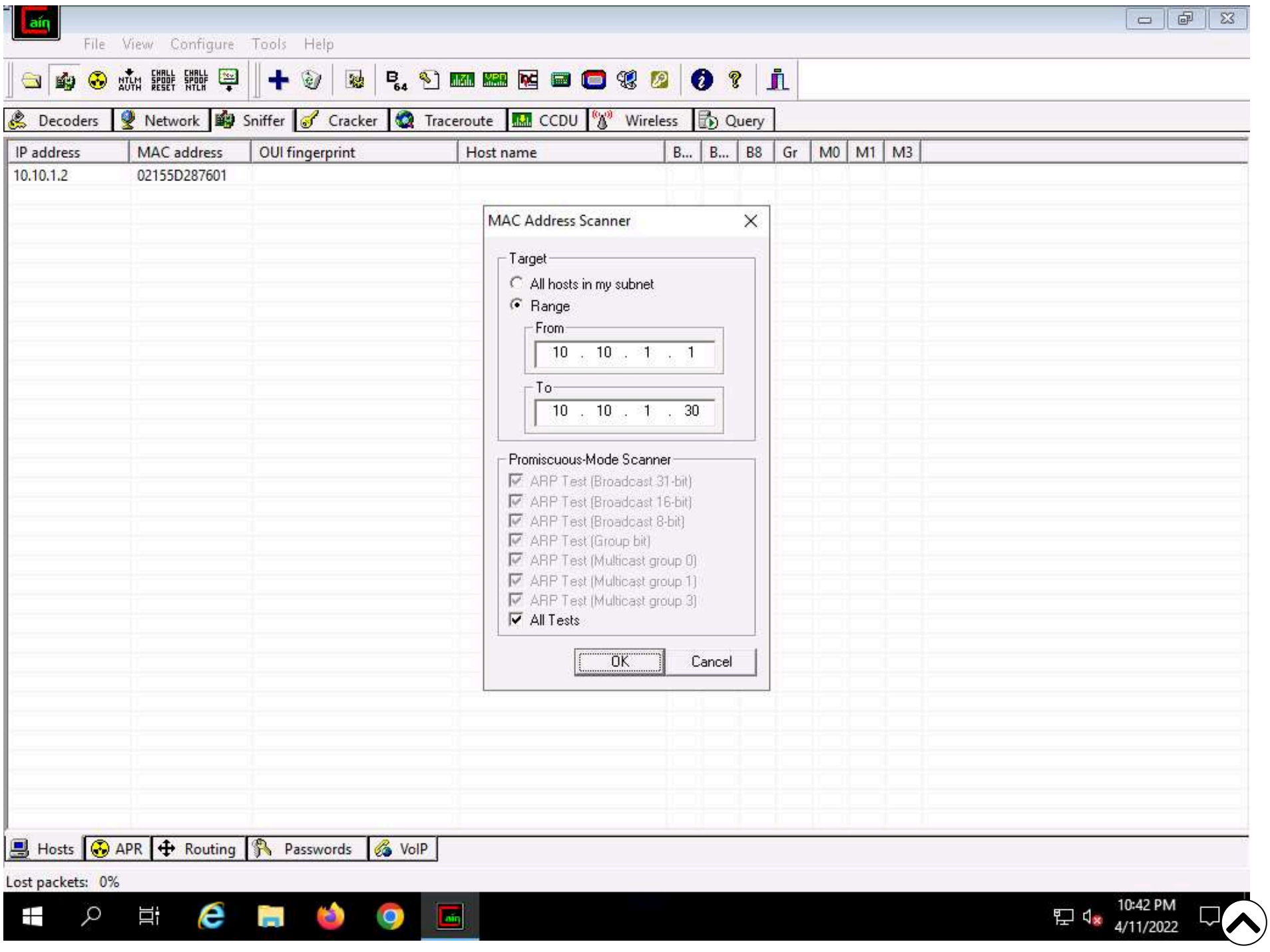


8. Now, click the **Sniffer** tab.



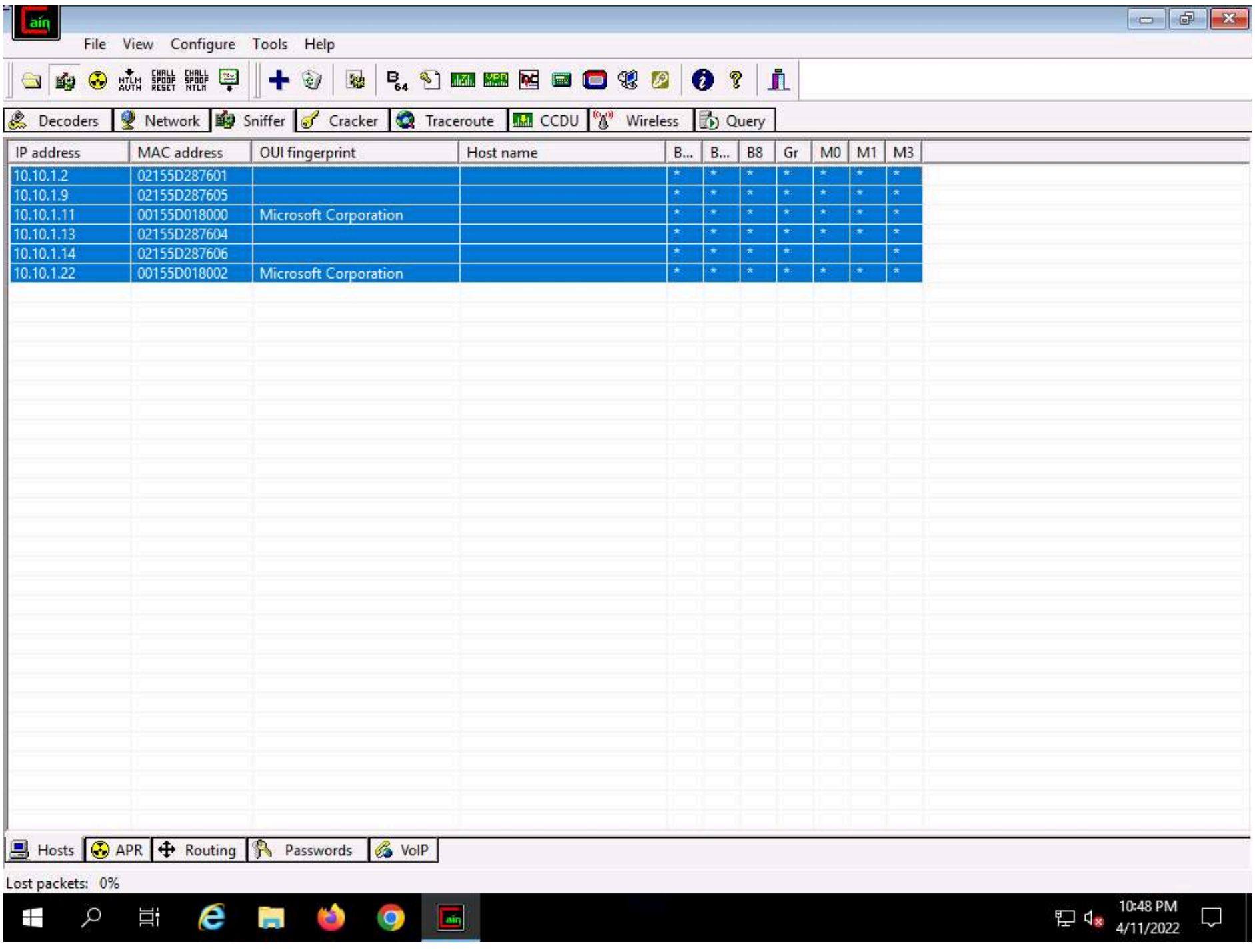
9. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

10. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.1.1-10.10.1.30**. Select the **All Tests** checkbox; then, click **OK**.



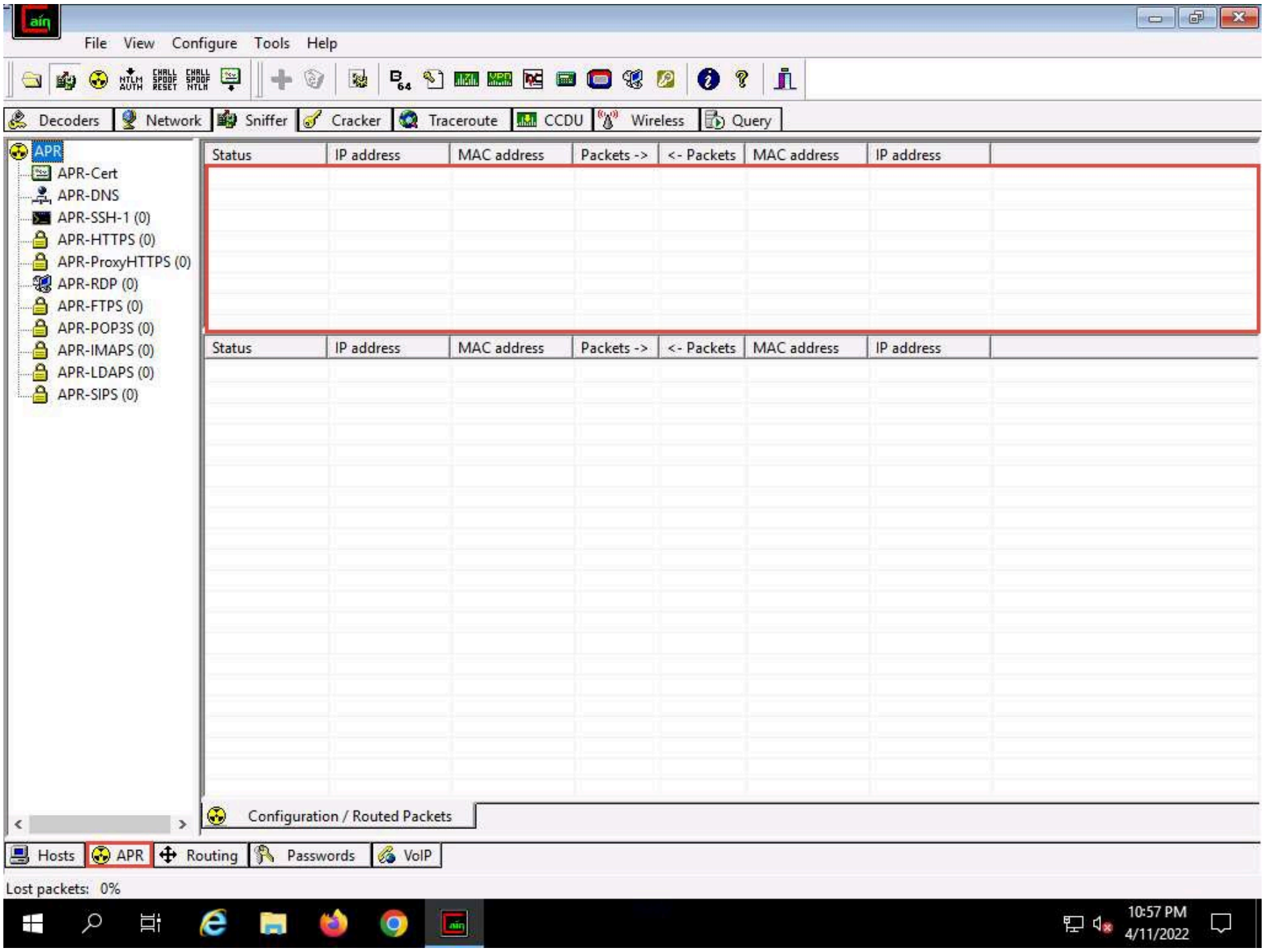
11. Cain & Abel starts scanning for MAC addresses and lists all those found.

12. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

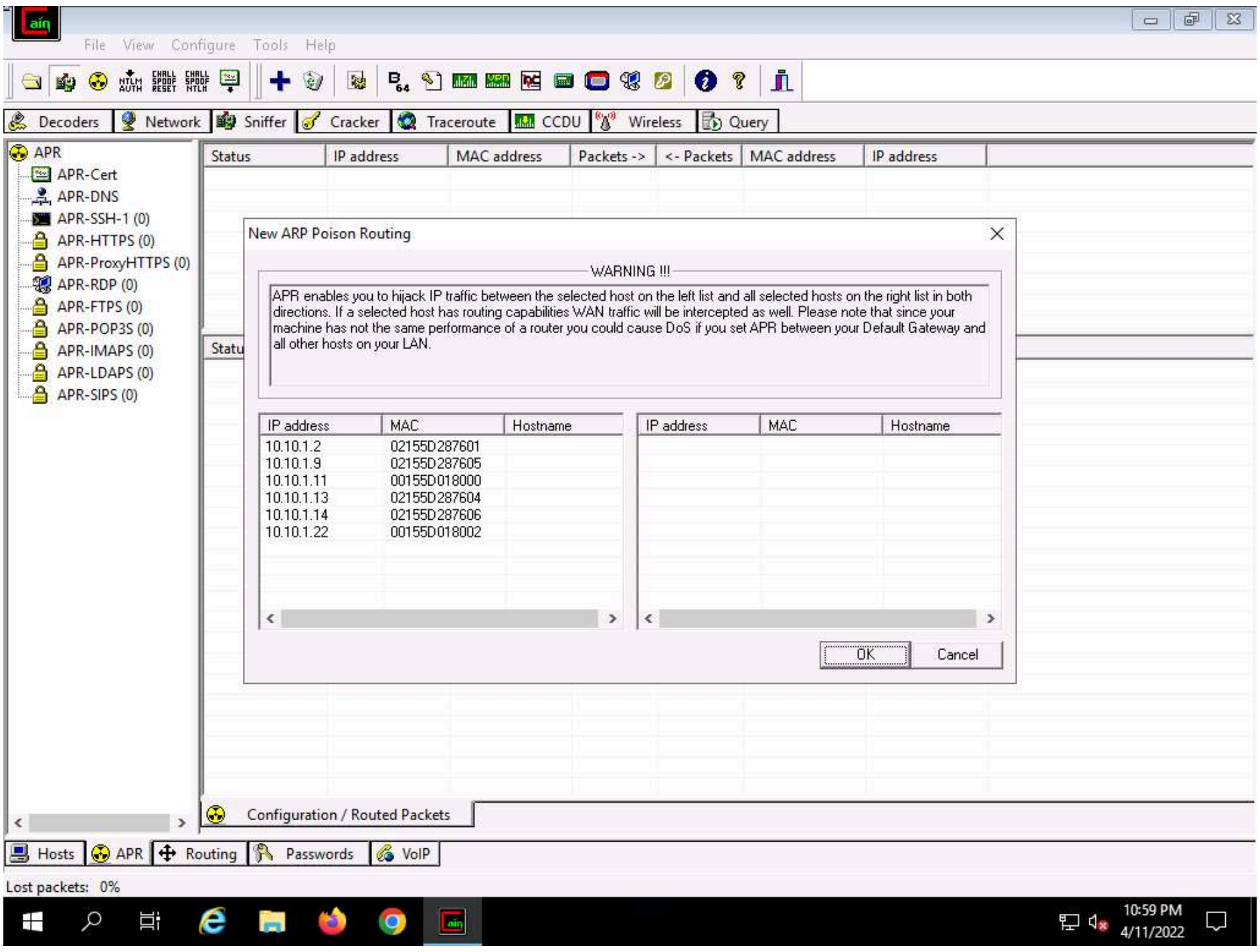


13. Now, click the **APR** tab at the bottom of the window.

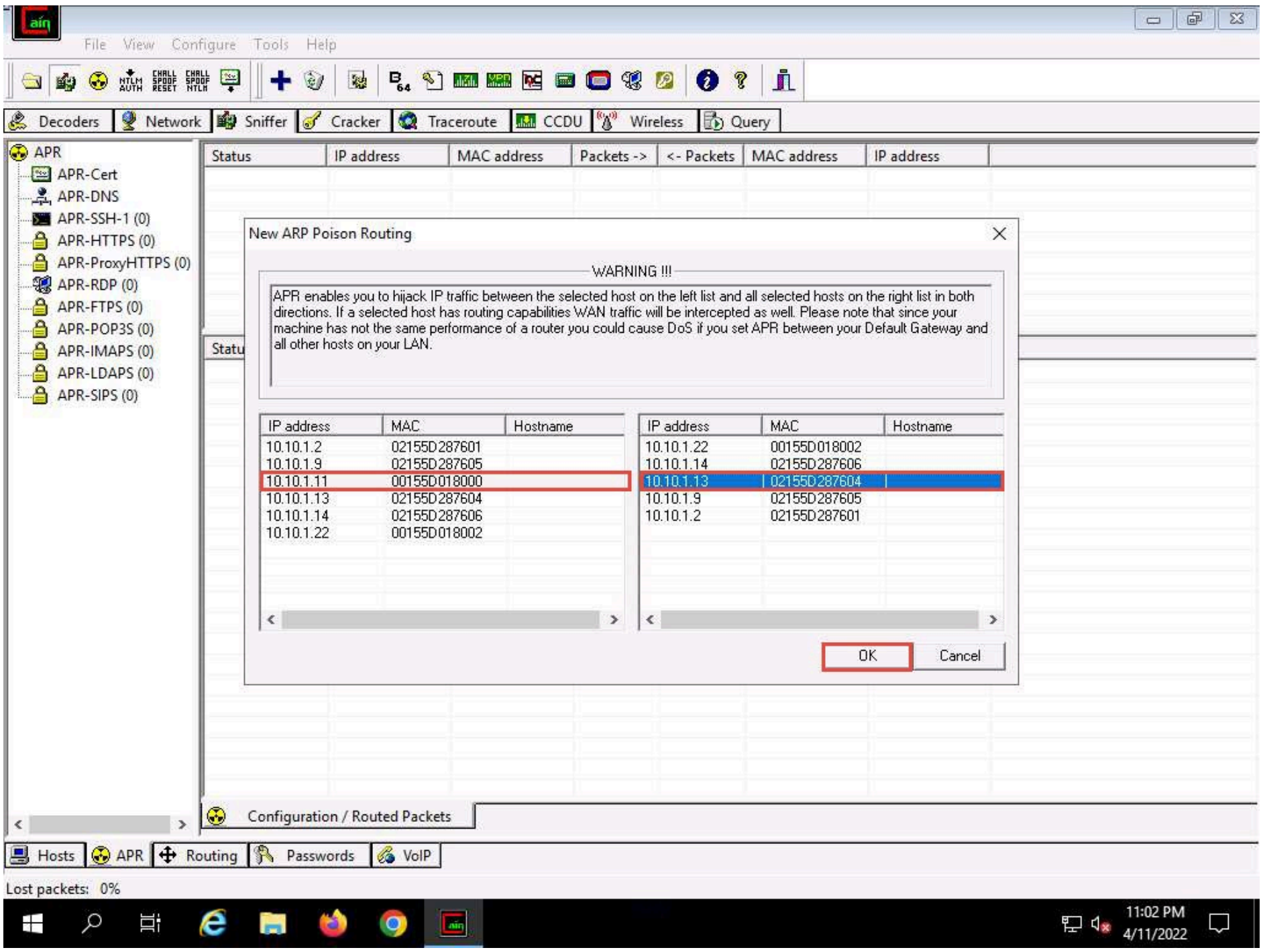
14. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (**+**) icon.



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

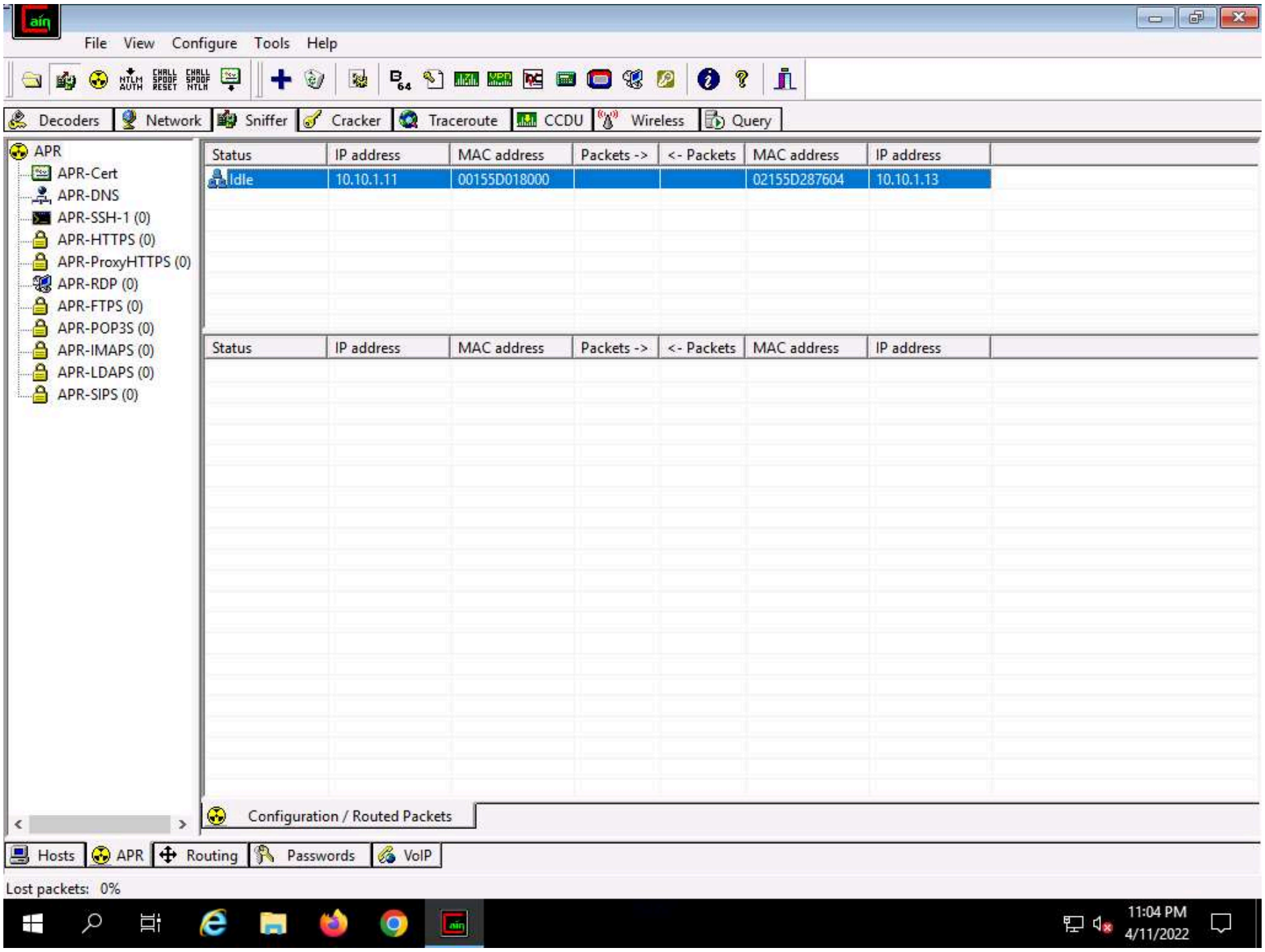


16. To monitor the traffic between two systems (here, **Windows 11** and **Parrot Security**), from the left-hand pane, click to select **10.10.1.11** (**Windows 11**) and from the right-hand pane, click **10.10.1.13** (**Parrot Security**); click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

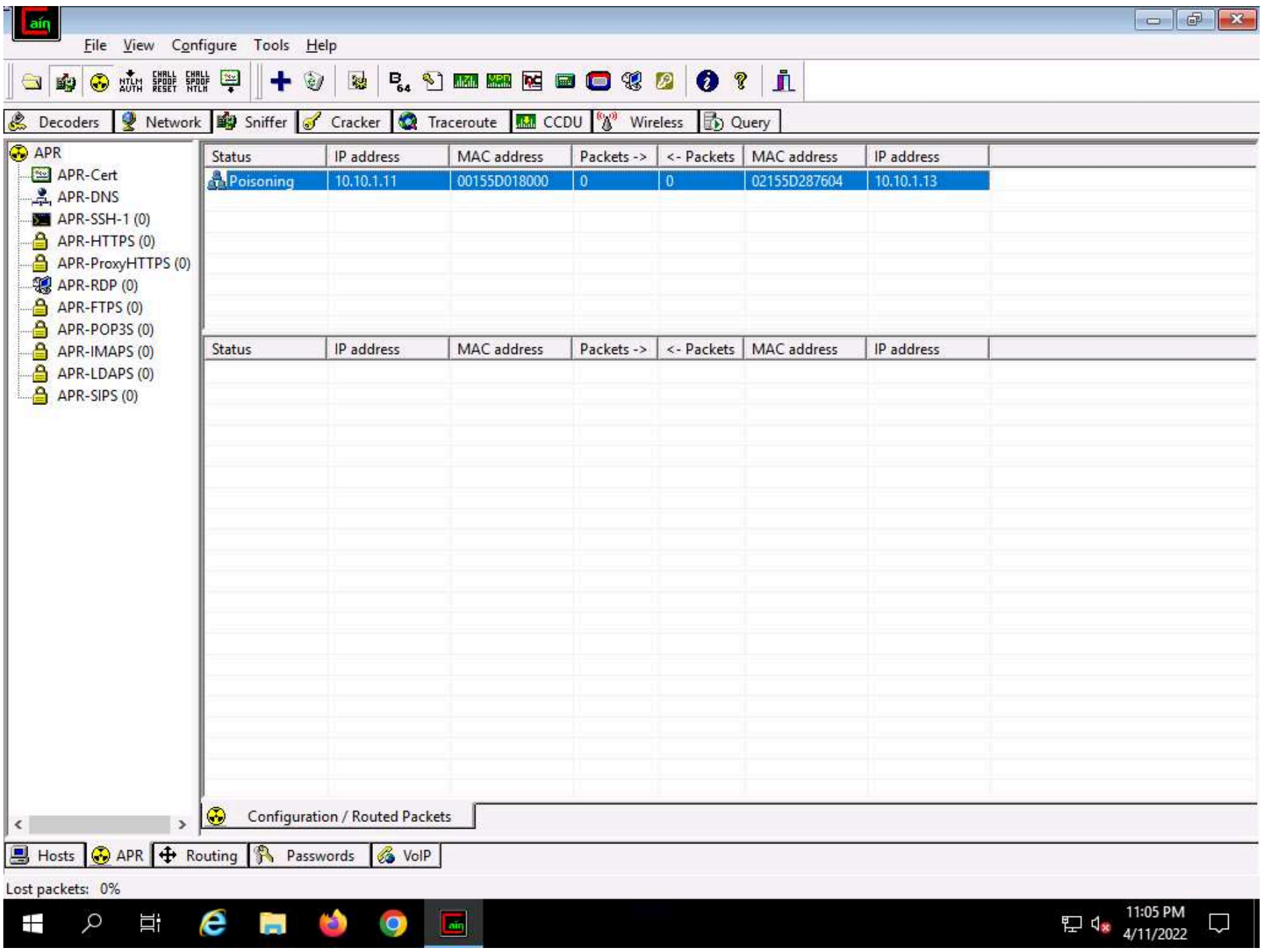


17. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.

18. Click on the **Start/Stop APR** icon to start capturing ARP packets.



19. After clicking on the **Start/Stop APR** icon, Cain & Abel starts ARP **poisoning** and the status of the scan changes to Poisoning, as shown in the screenshot.

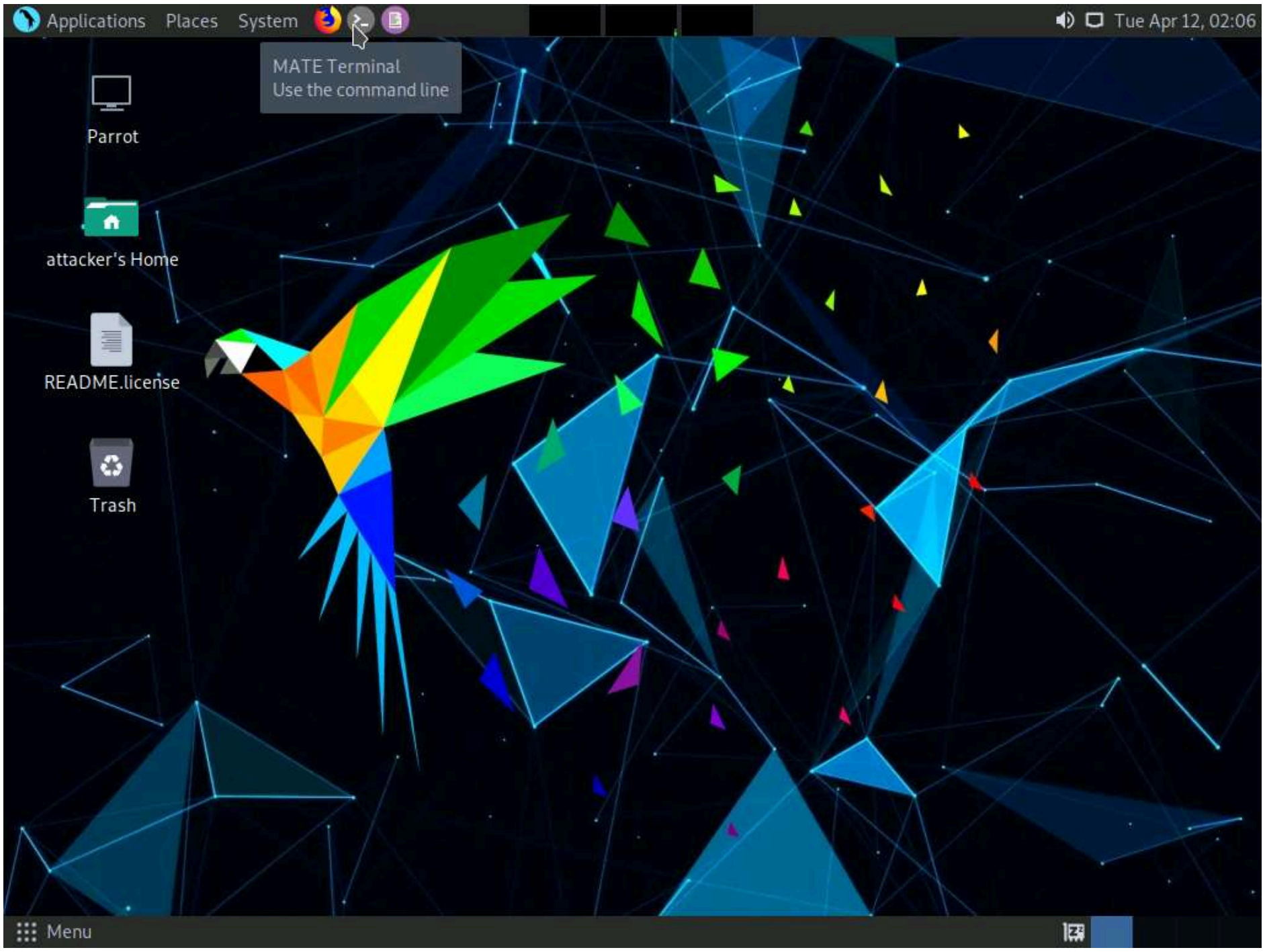


20. Cain & Abel intercepts the traffic traversing between these two machines.

21. To generate traffic between the machines, you need to ping one target machine using the other.

22. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

23. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

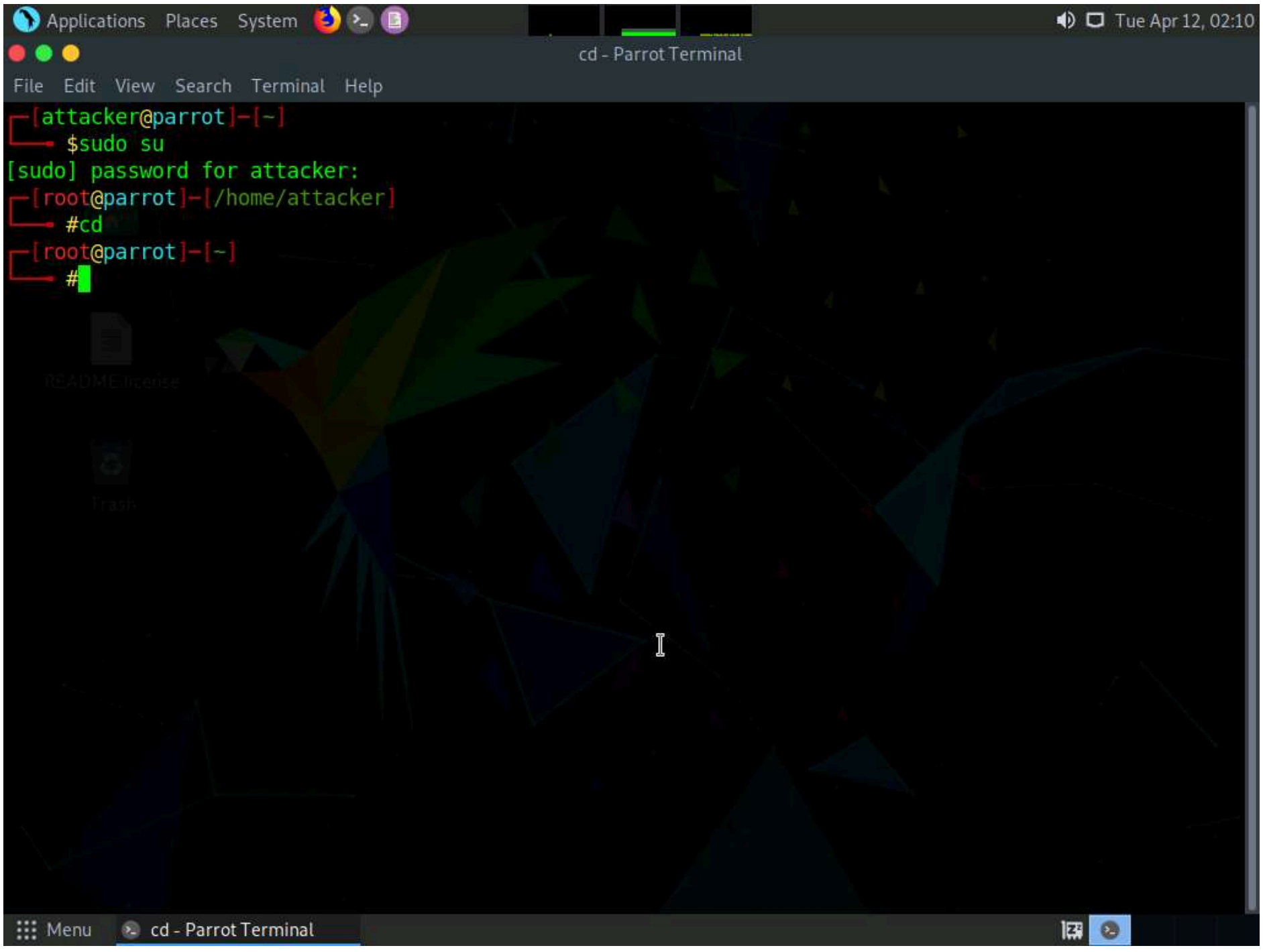


24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

25. 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.

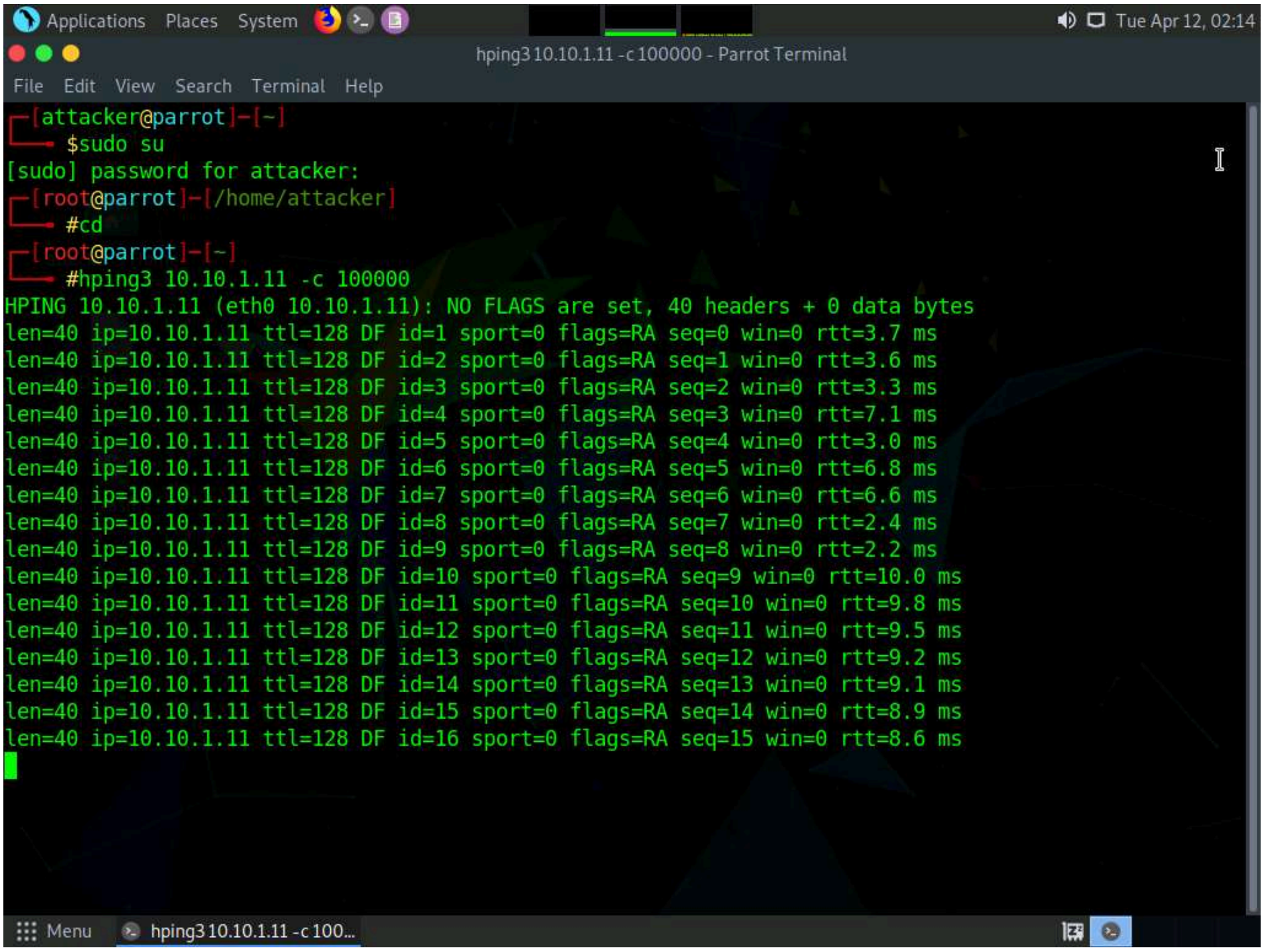
26. Now, type **cd** and press **Enter** to jump to the root directory.



27. A **Parrot Terminal** window appears; type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

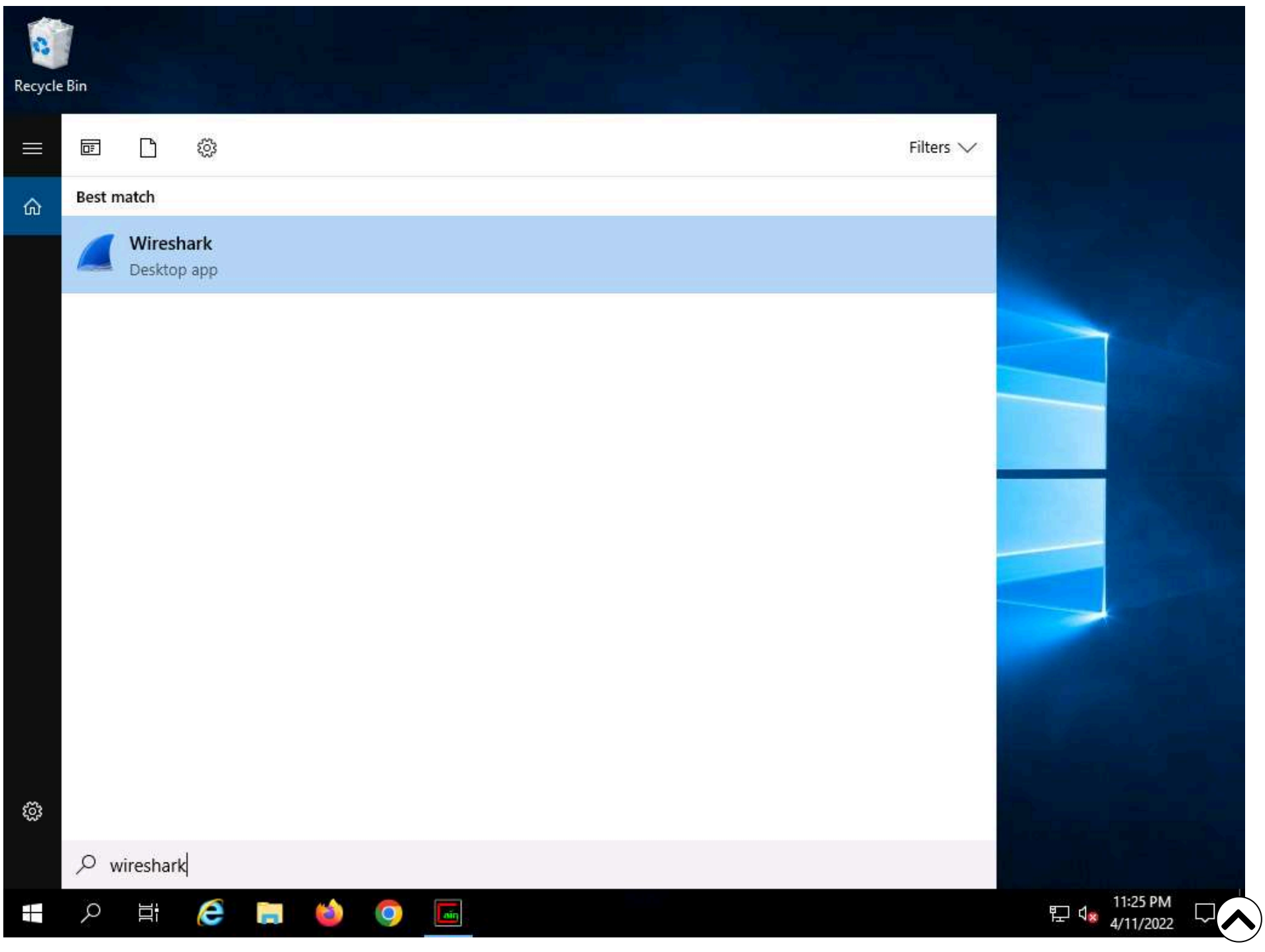
> Note: **-c**: specifies the packet count.

28. This command will start pinging the target machine (**Windows 11**) with 100,000 packets.

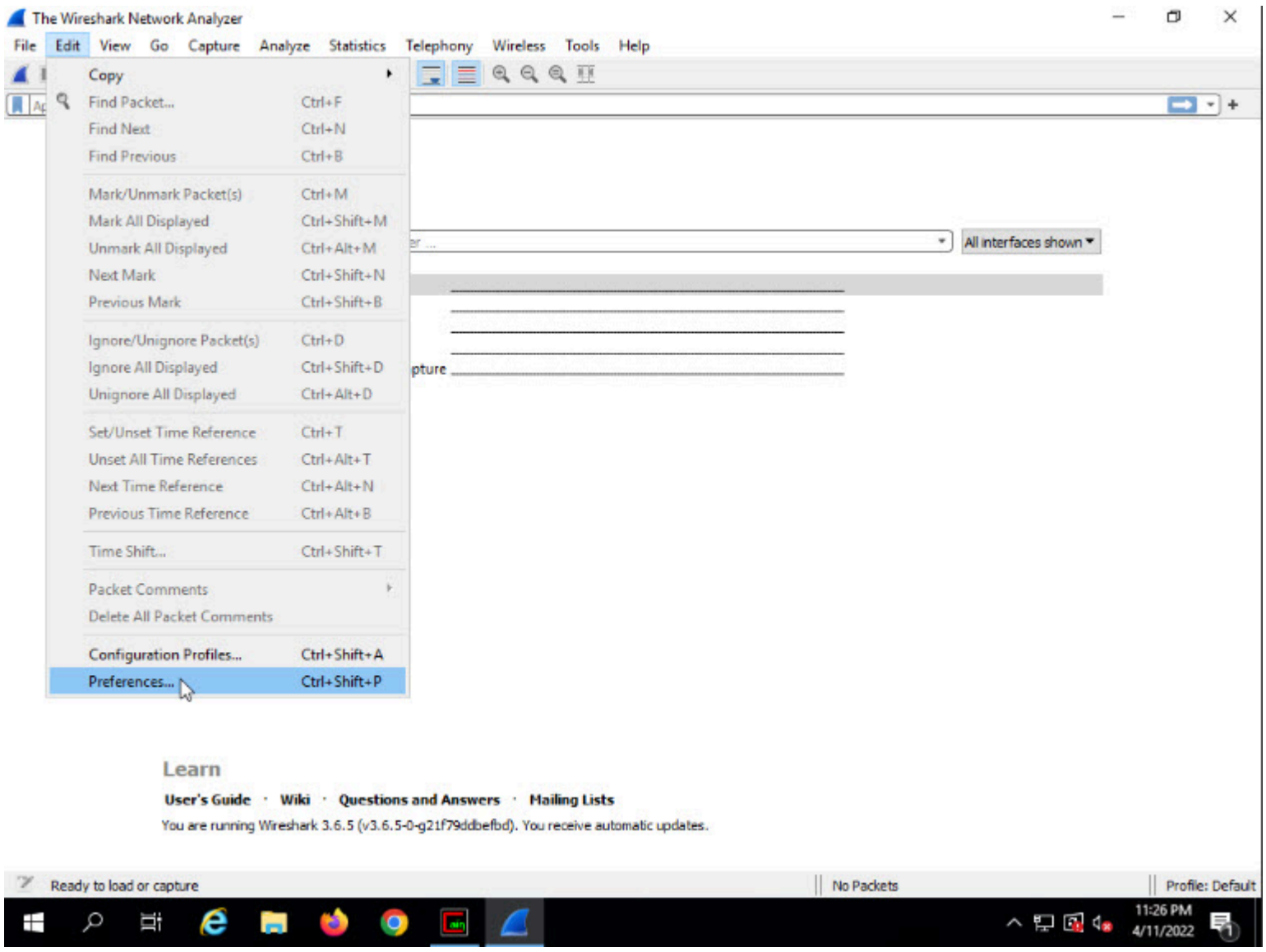


29. Leave the command running and immediately click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

30. Click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.



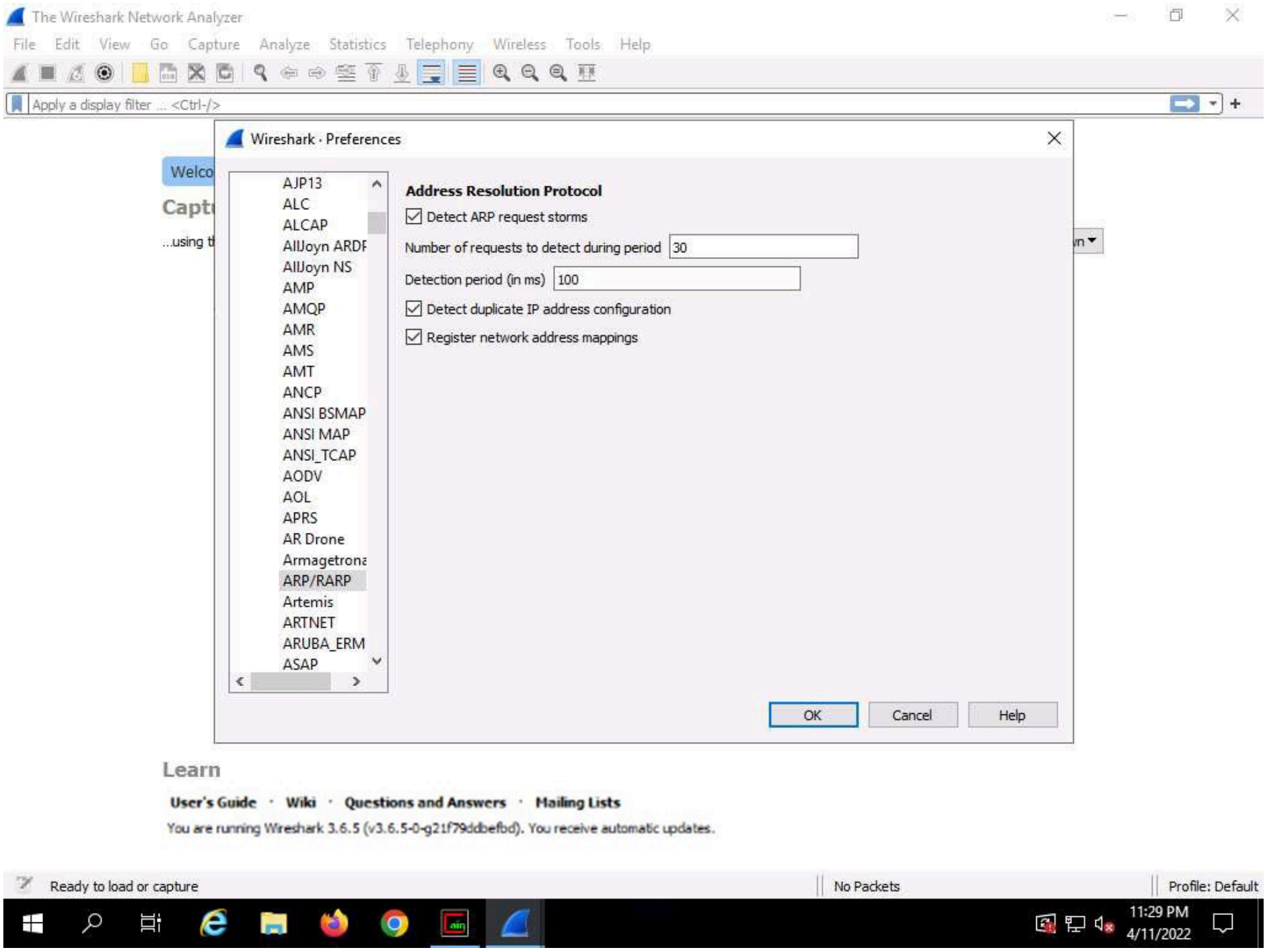
31. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences...**.



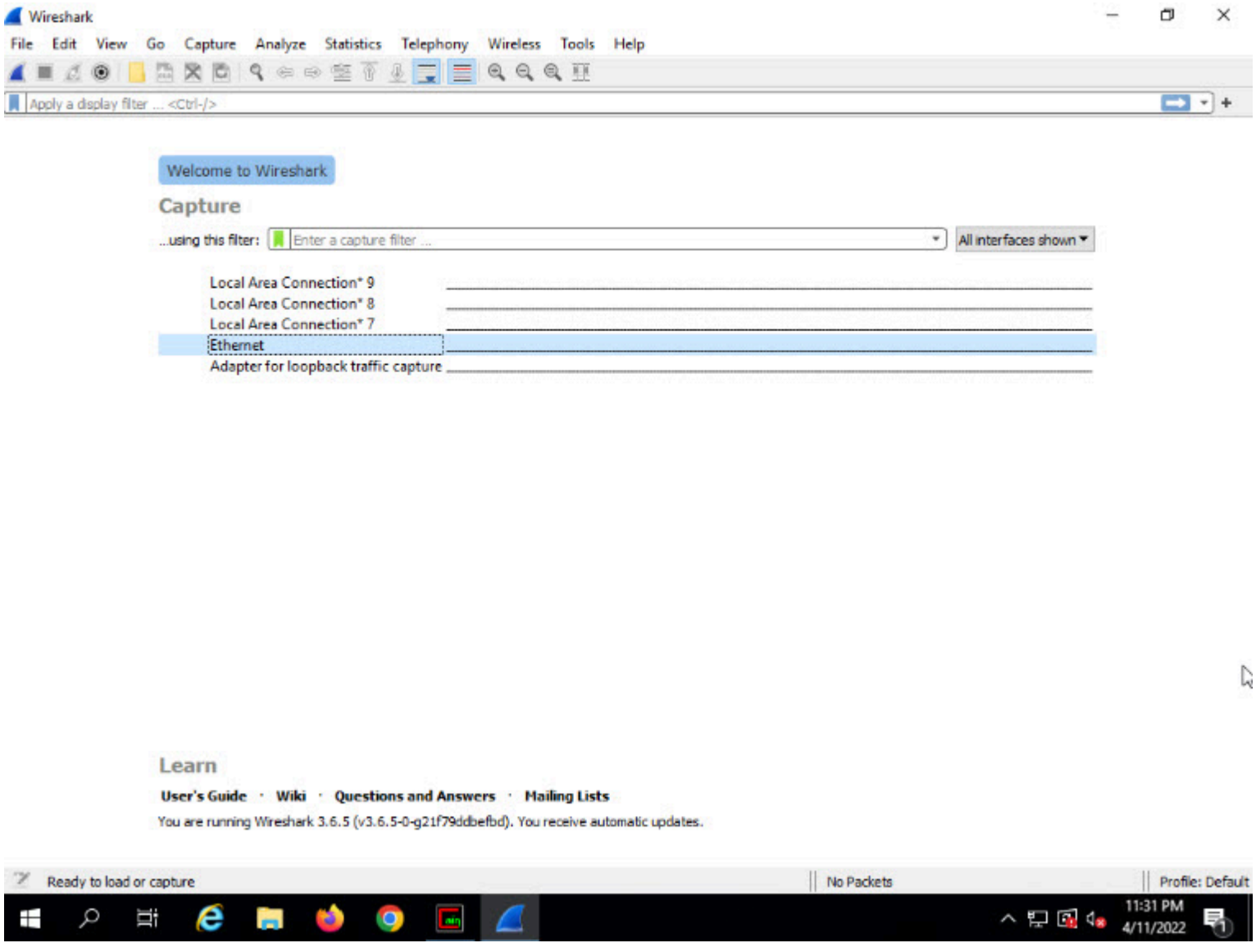
32. The **Wireshark . Preferences** window appears; expand the **Protocols** node.

33. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.

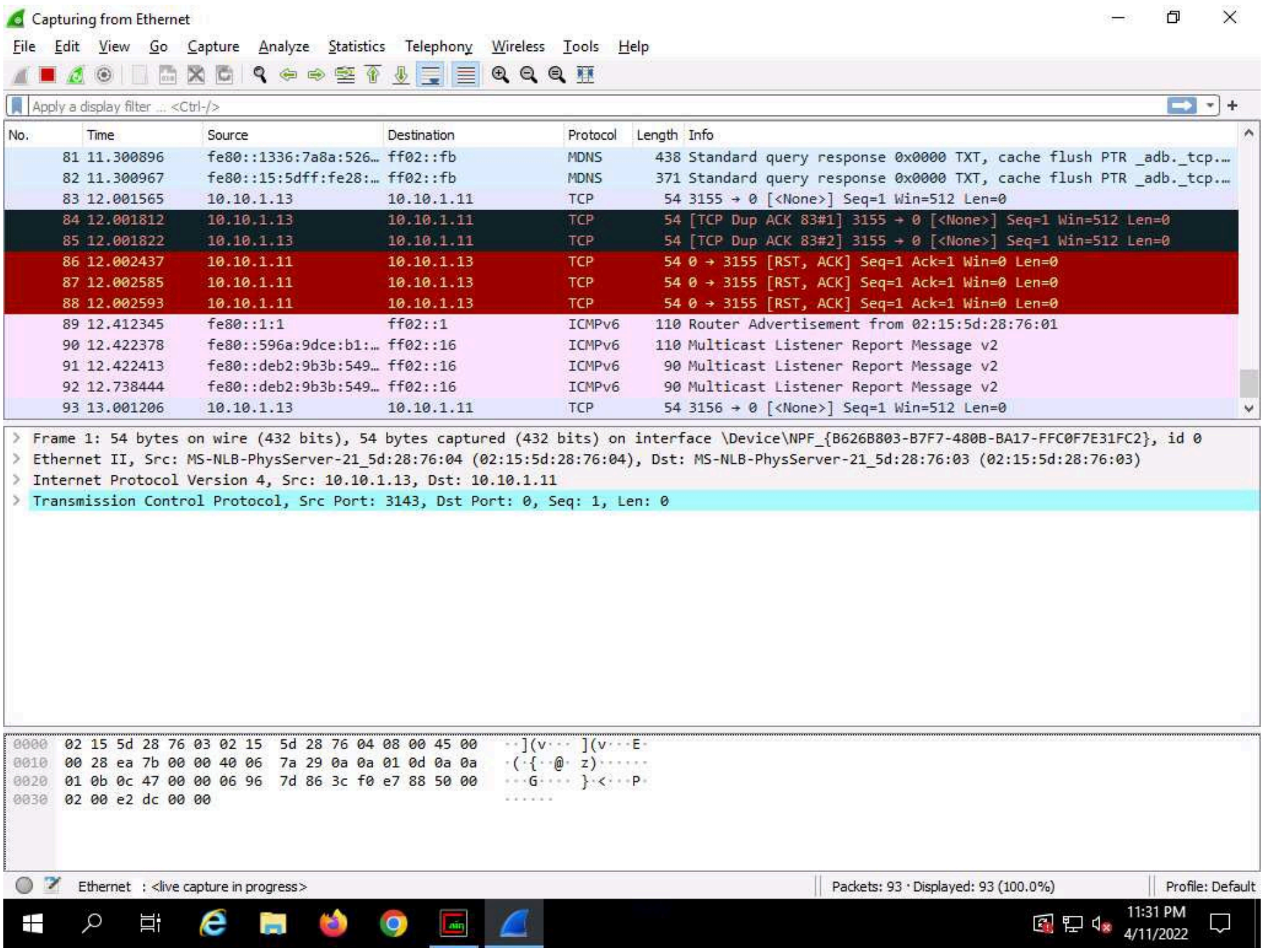
34. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.



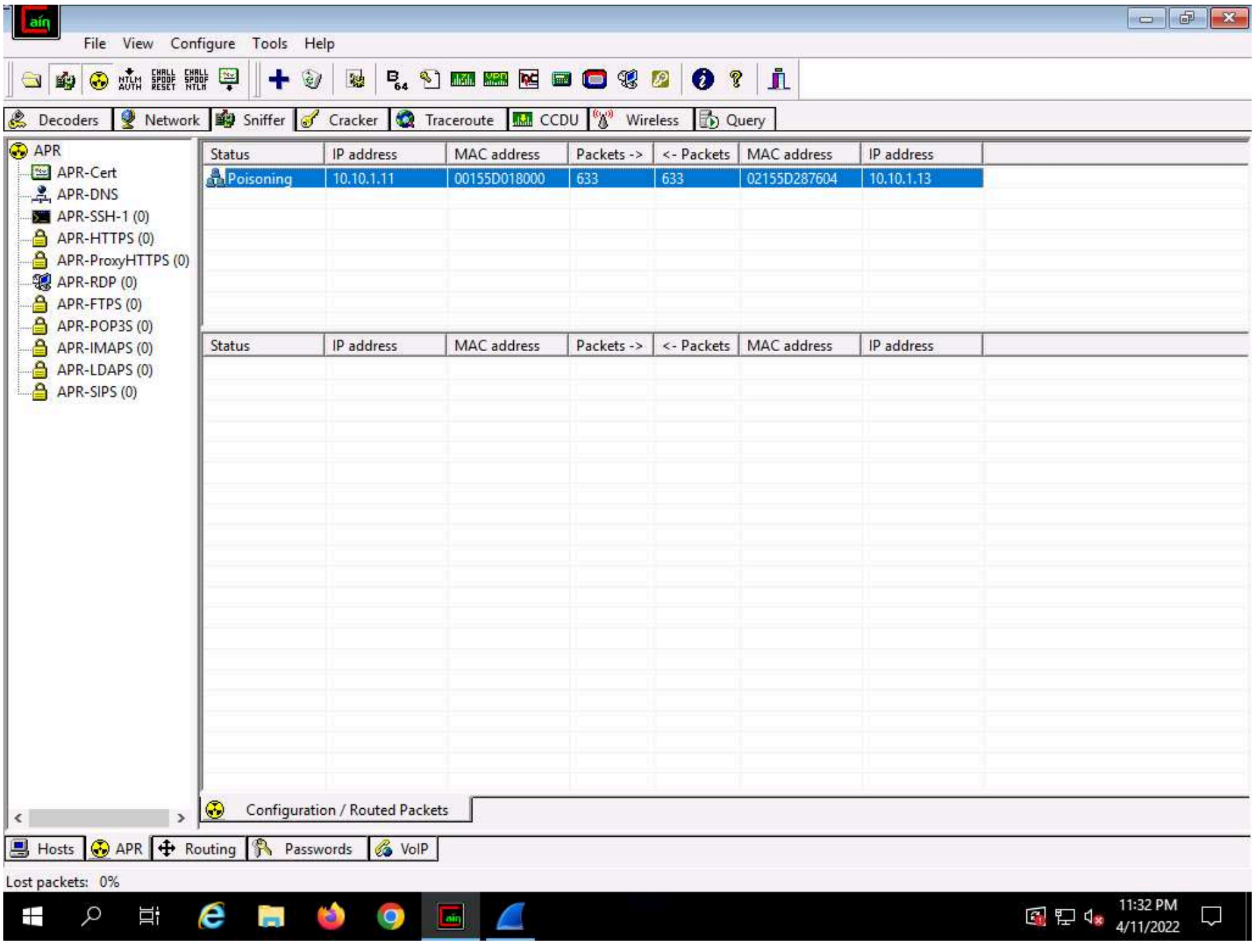
35. Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.



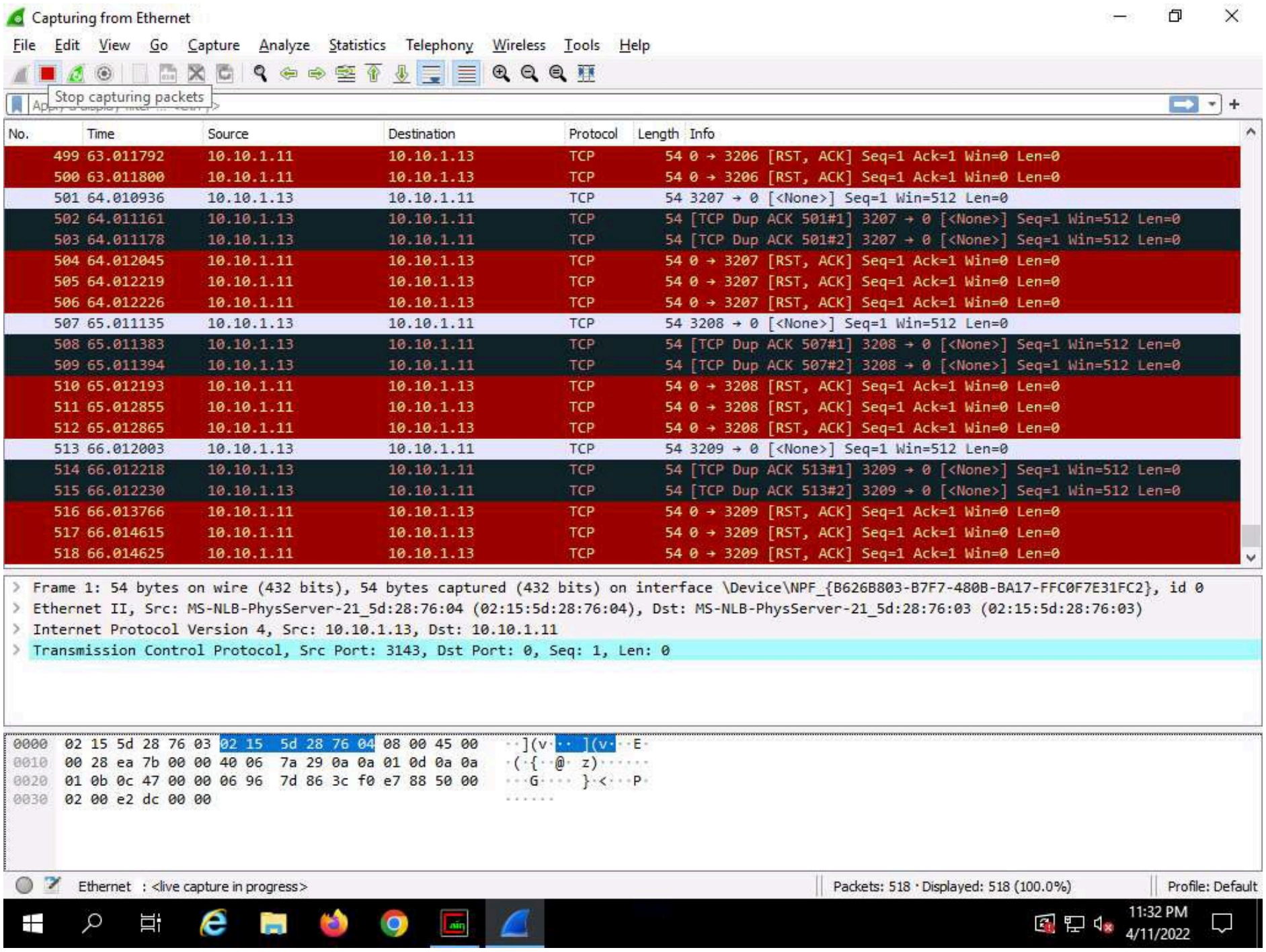
36. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.



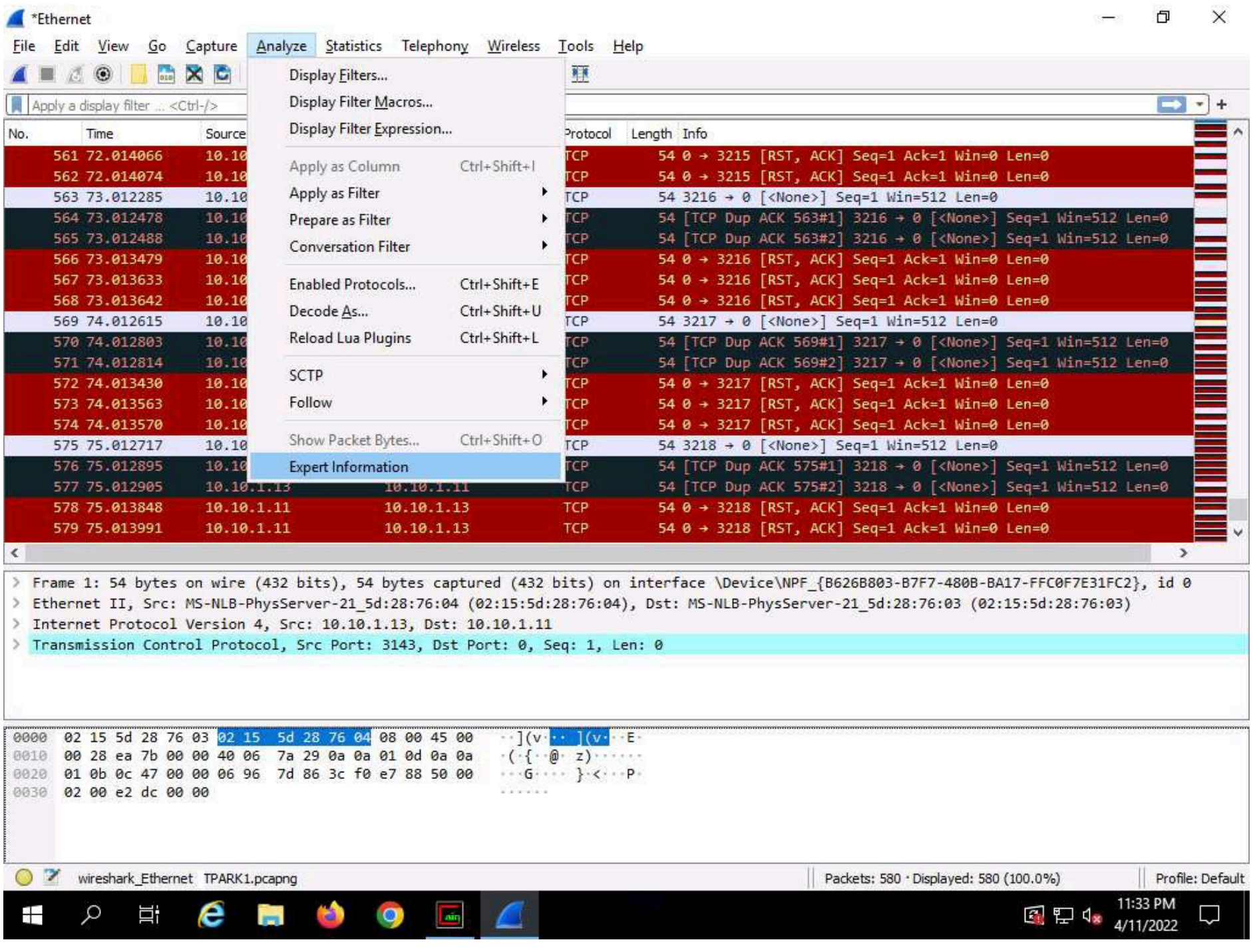
37. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.



38. Now, switch to **Wireshark** and click the **Stop packet capturing** icon to stop the packet capturing.



39. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.



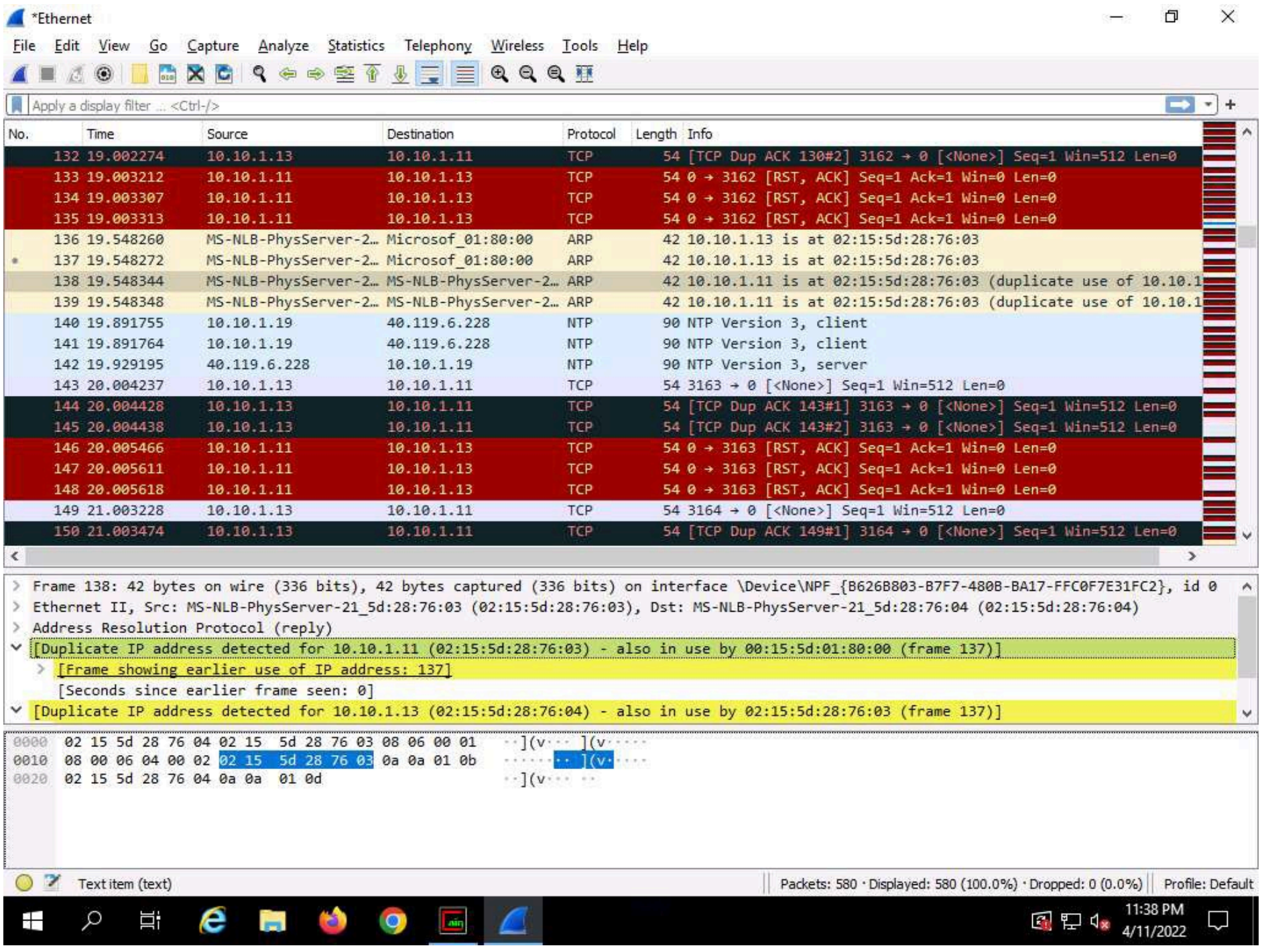
40. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.11)**, running on the **ARP/RARP** protocol.

41. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

42. In the **Wireshark . Expert Information** window, click any packet (here, **138**).

43. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close the **Wireshark . Expert Information** window.

44. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.



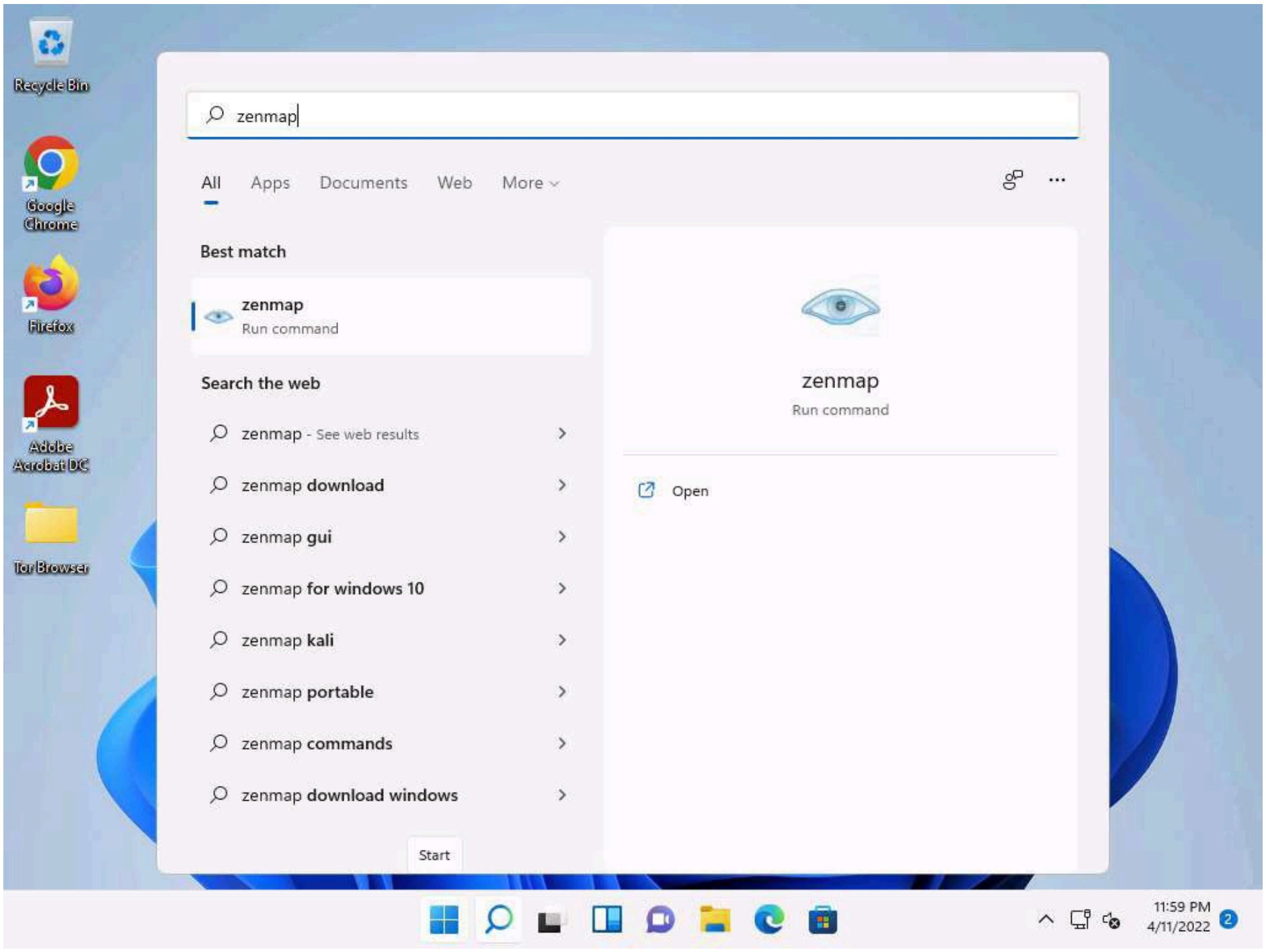
Note: ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. At this point, the attacker can launch a DoS attack by associating a non-existent MAC address with the IP address of the gateway or may passively sniff the traffic, and then forward it to the target destination.

45. This concludes the demonstration of detecting ARP poisoning in a switch-based network.

46. Close the **Wireshark** window and leave all other windows running.

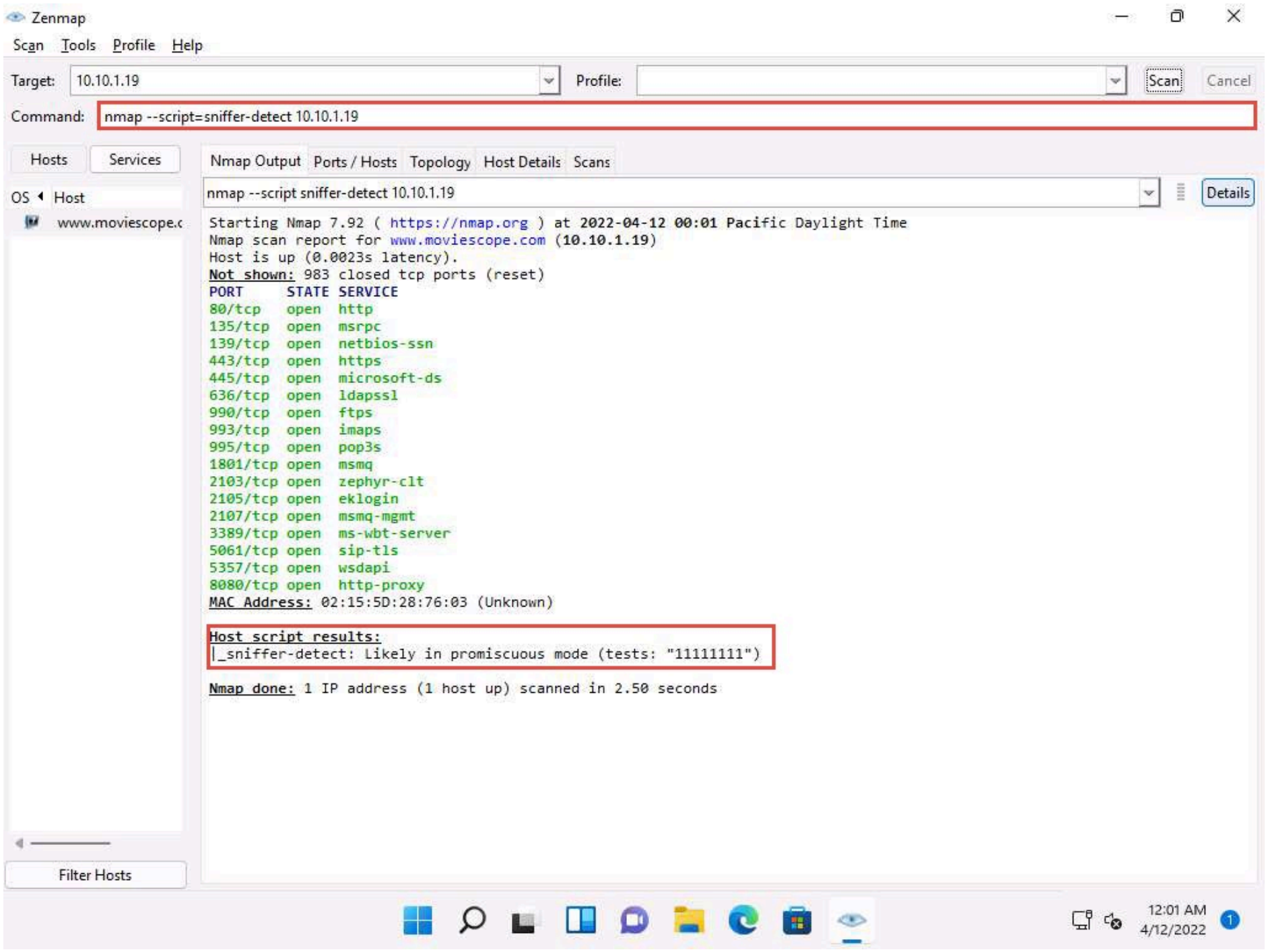
47. Now, we shall perform promiscuous mode detection using **Nmap**.

48. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine. Click **Search** icon ( ) on the **Desktop**. Type **zenmap** in the search field, the **Nmap - Zenmap GUI** appears in the results, click **Open** to launch it.



49. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect [Target IP Address/ IP Address Range]** (here, target IP address is **10.10.1.19 [Windows Server 2019]**) and click **Scan**.

50. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates that the target system is in promiscuous mode.



51. Close the **Nmap** tool window and document all the acquired information.

52. Close all open windows in all machines (ensure that ARP poisoning is not running in **Windows Server 2019**), and document all the acquired information.

Task 2: Detect ARP Poisoning using the Capsa Network Analyzer

Capsa Network Analyzer

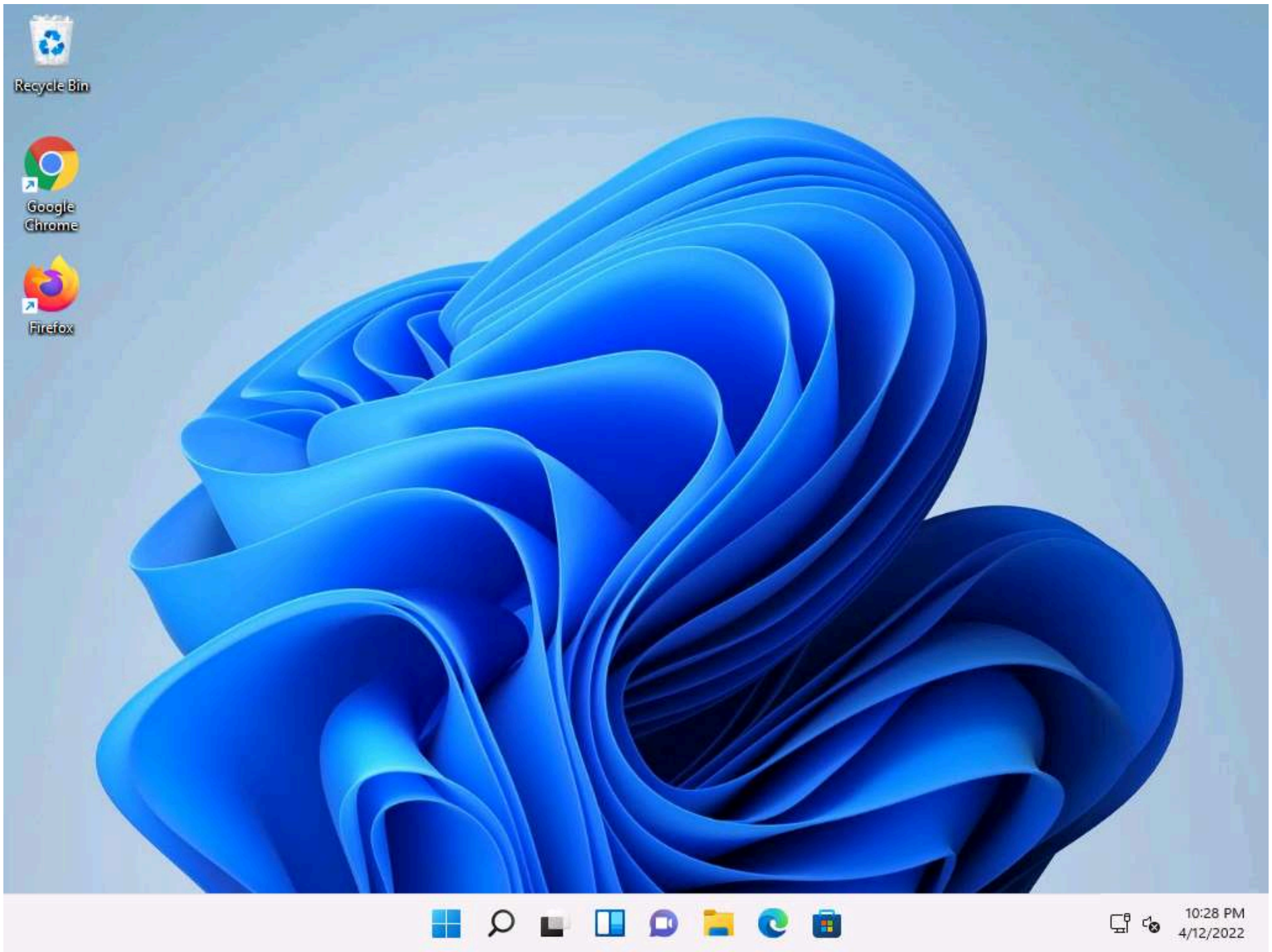
Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy to use interface that allows users to protect and monitor networks in a critical business environment. It helps ethical hackers or pentesters in quickly detecting ARP poisoning and ARP flooding attack and in locating attack source.

Habu

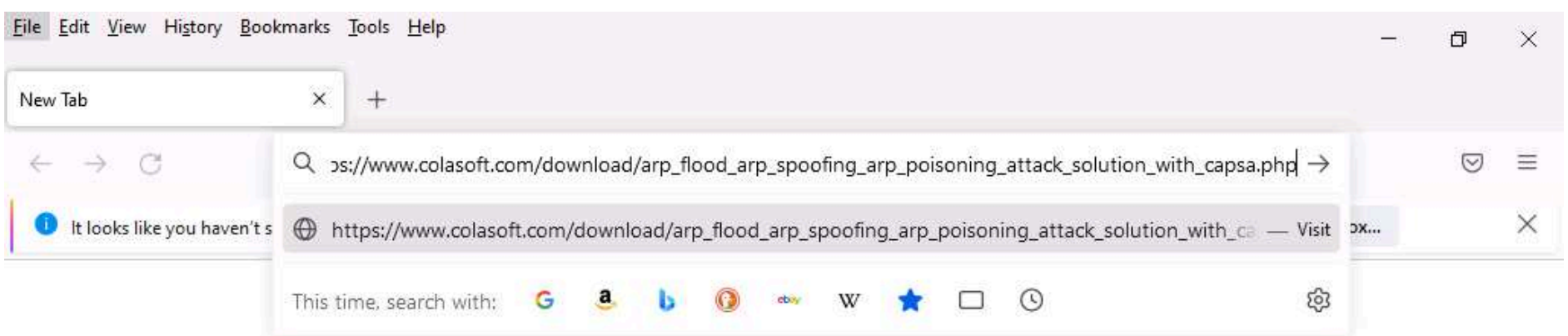
Habu is an open source penetration testing toolkit that can perform various tasks such as ARP poisoning, ARP sniffing, DHCP starvation and DHCP discovers.

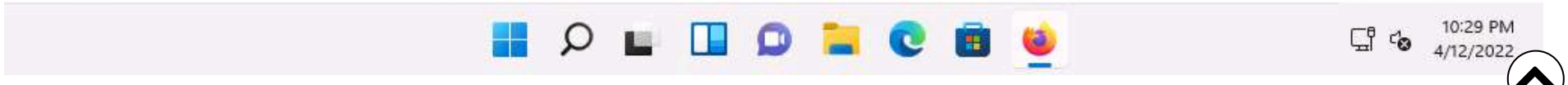
Here, we will use Habu tool to perform ARP poisoning attack on the target system and use Capsa Network Analyser to detect the attack.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

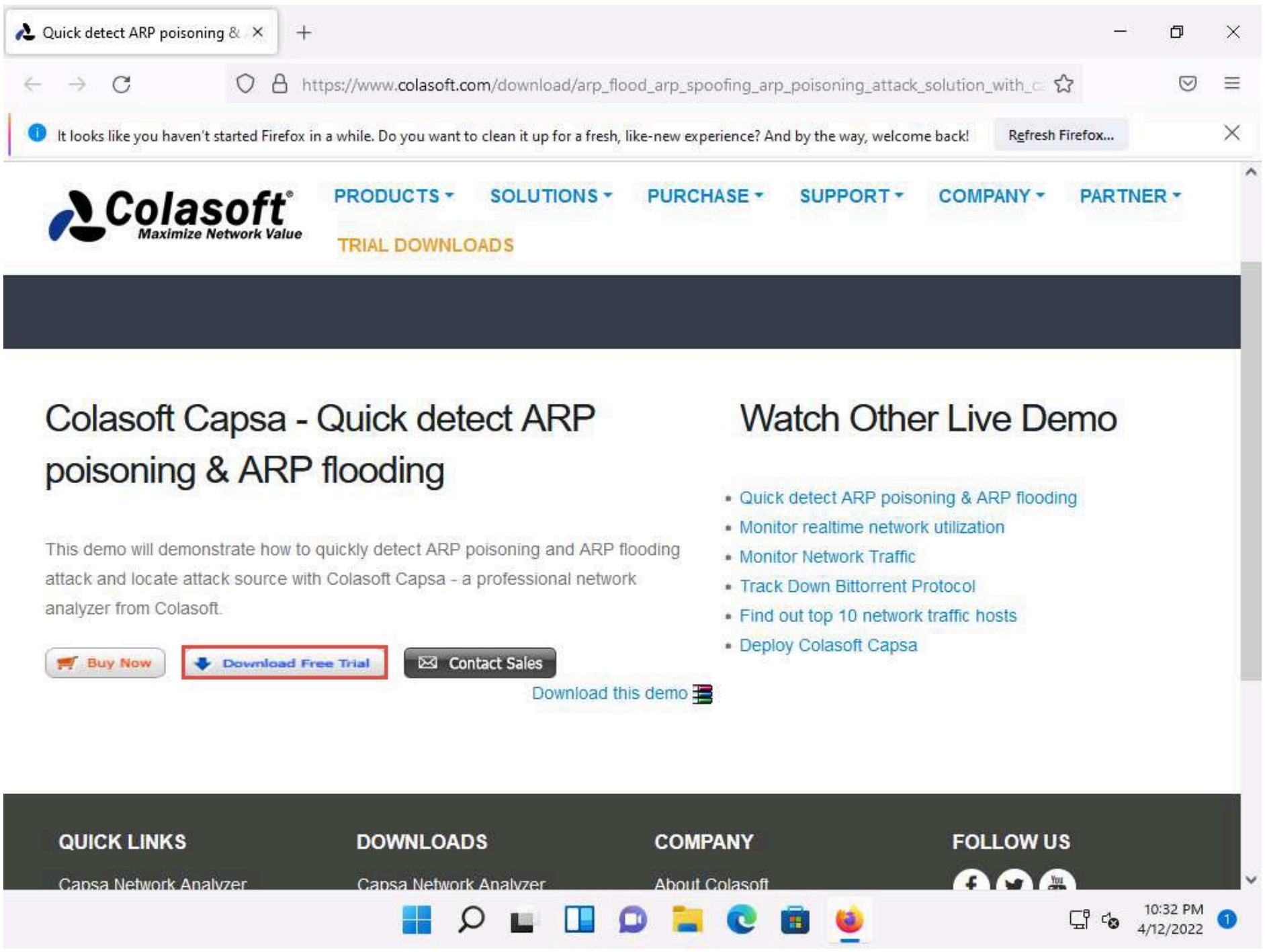


2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar, type **https://www.colasoft.com/download/arp_flood_arp_spoofing*arp*poisoning_attack_solution_with_capsa.php** in the address bar, and press **Enter**.



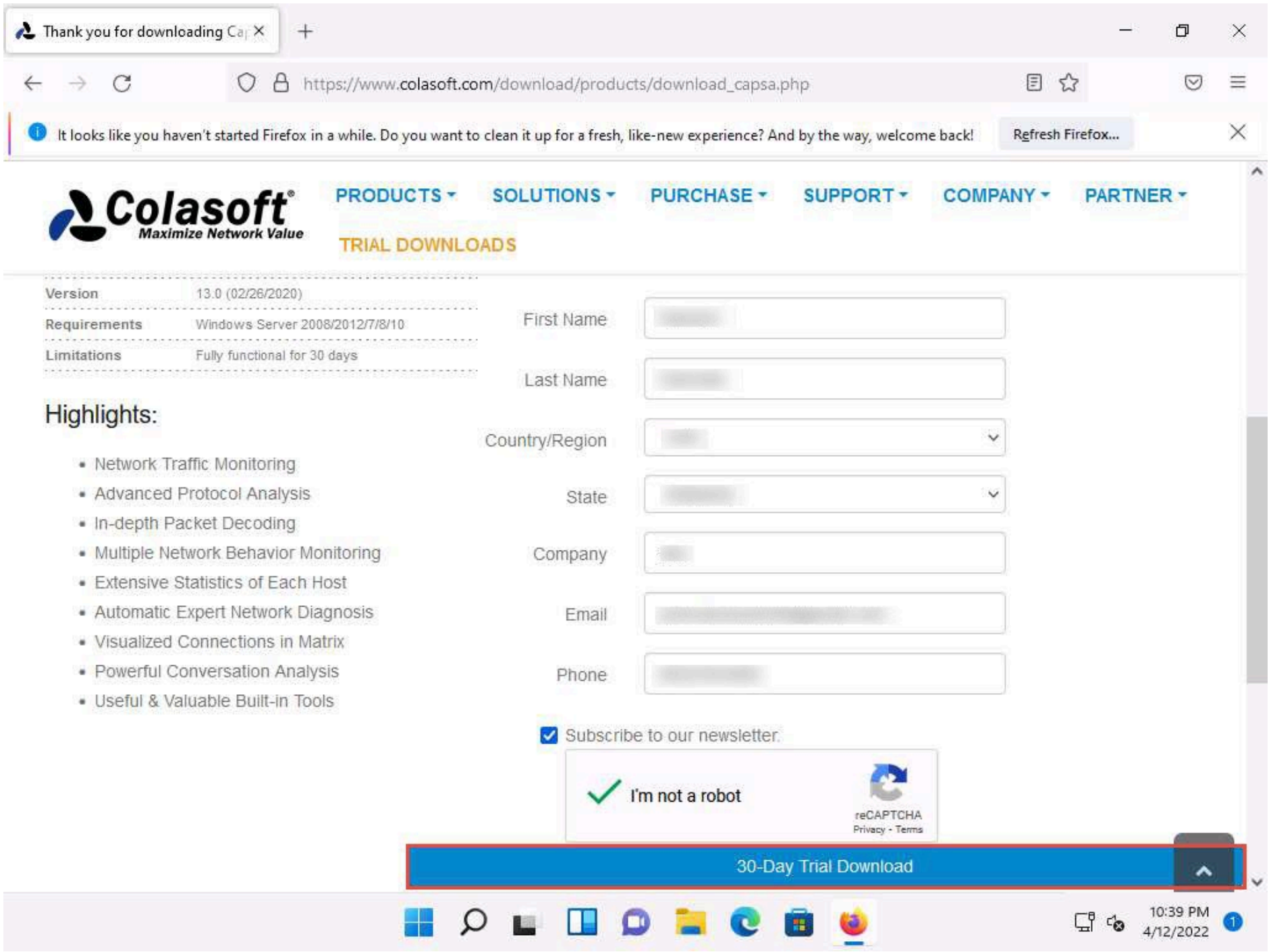


3. In the **Colasoft Capsa - Quick detect ARP poisoning & ARP flooding** window, click on **Download Free Trial** button.

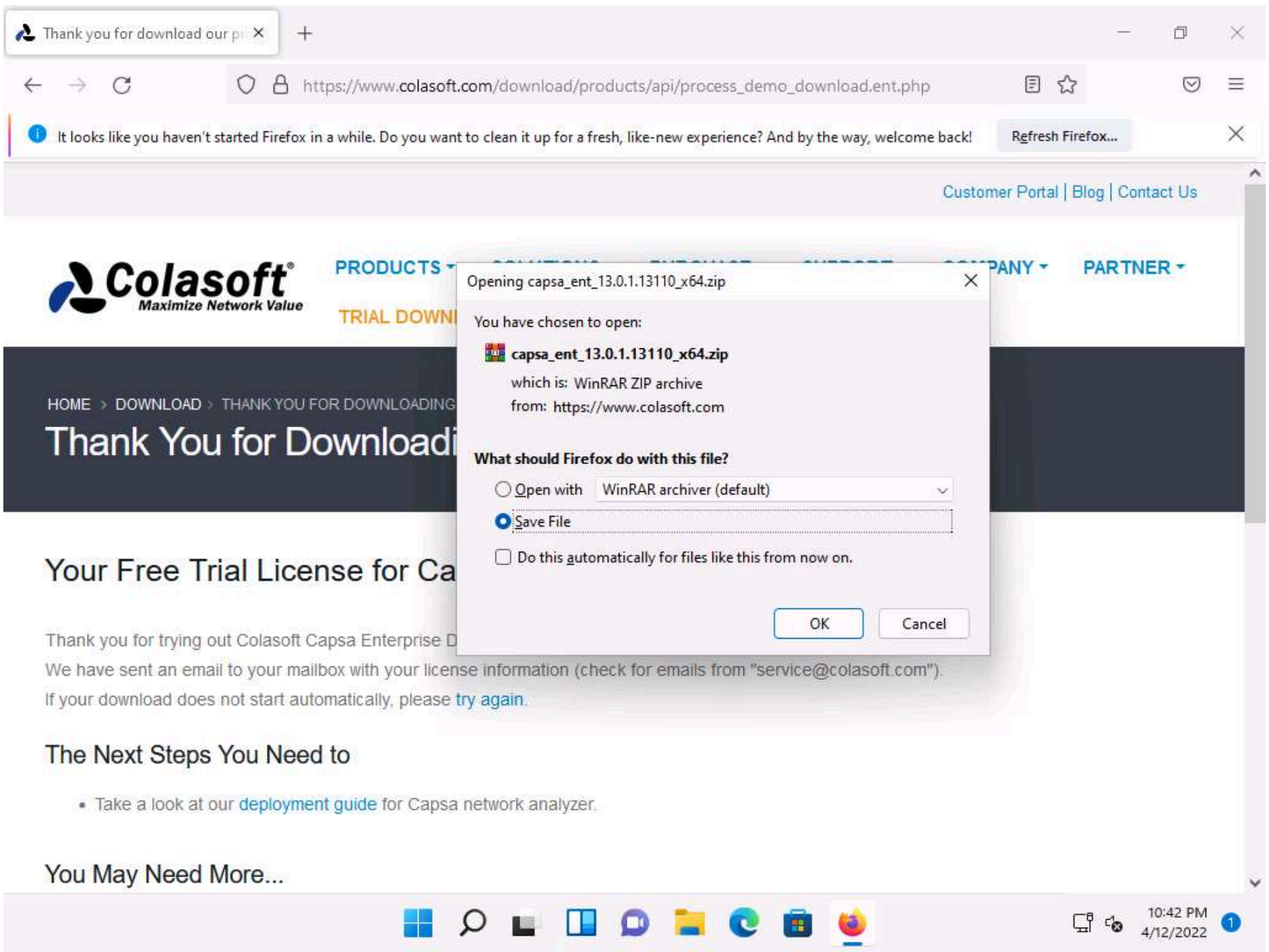


4. You will be redirected to **Download Capsa Enterprise Trial** window, scroll-down and fill all the required personal details and click on **30-Day Trial Download**.

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

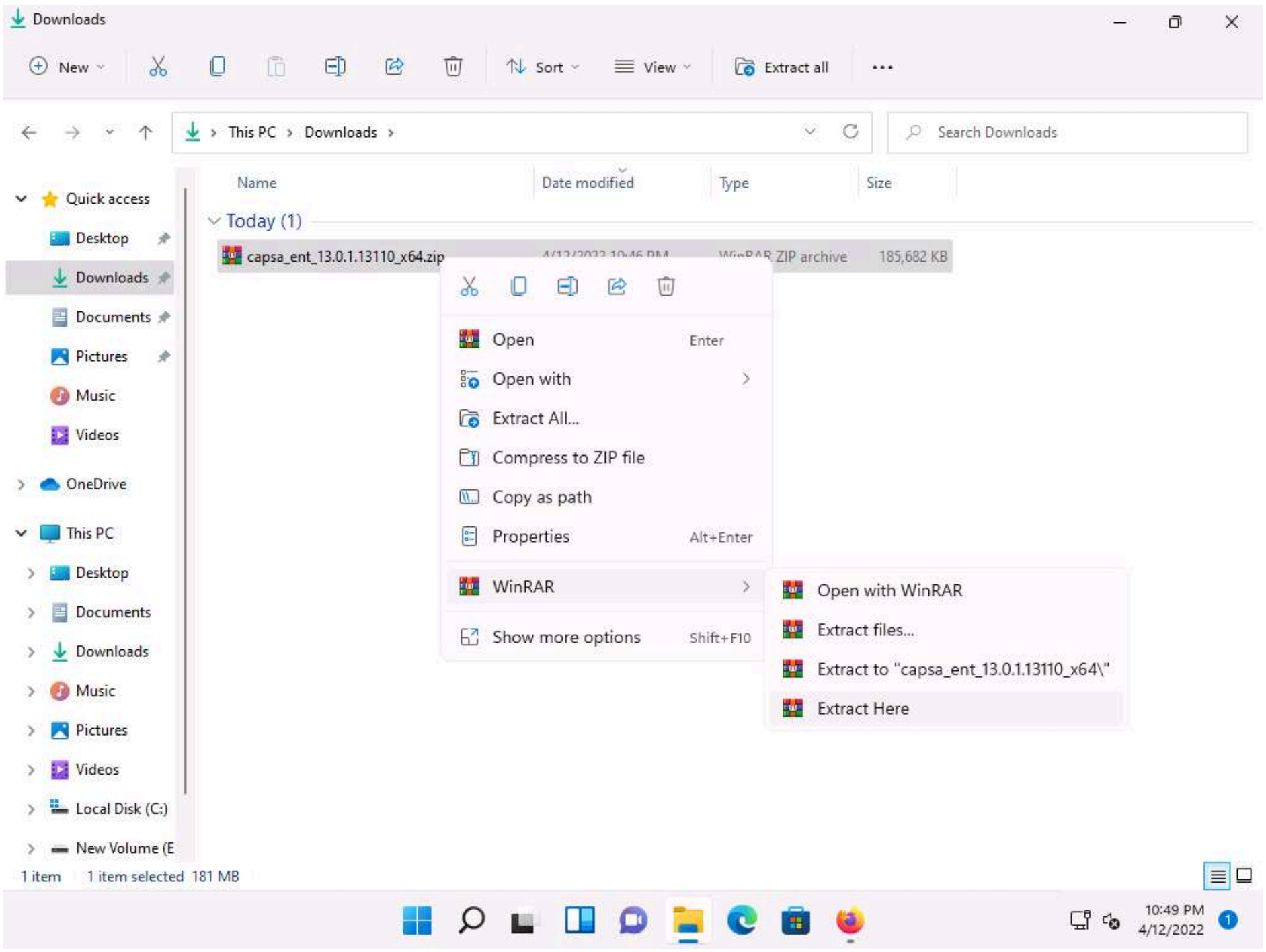


5. You will be redirected to download page, if **Opening capsa_ent_13.0.1.13110_x64.zip** pop-up appears select **Save File** radio button and click on **OK**.

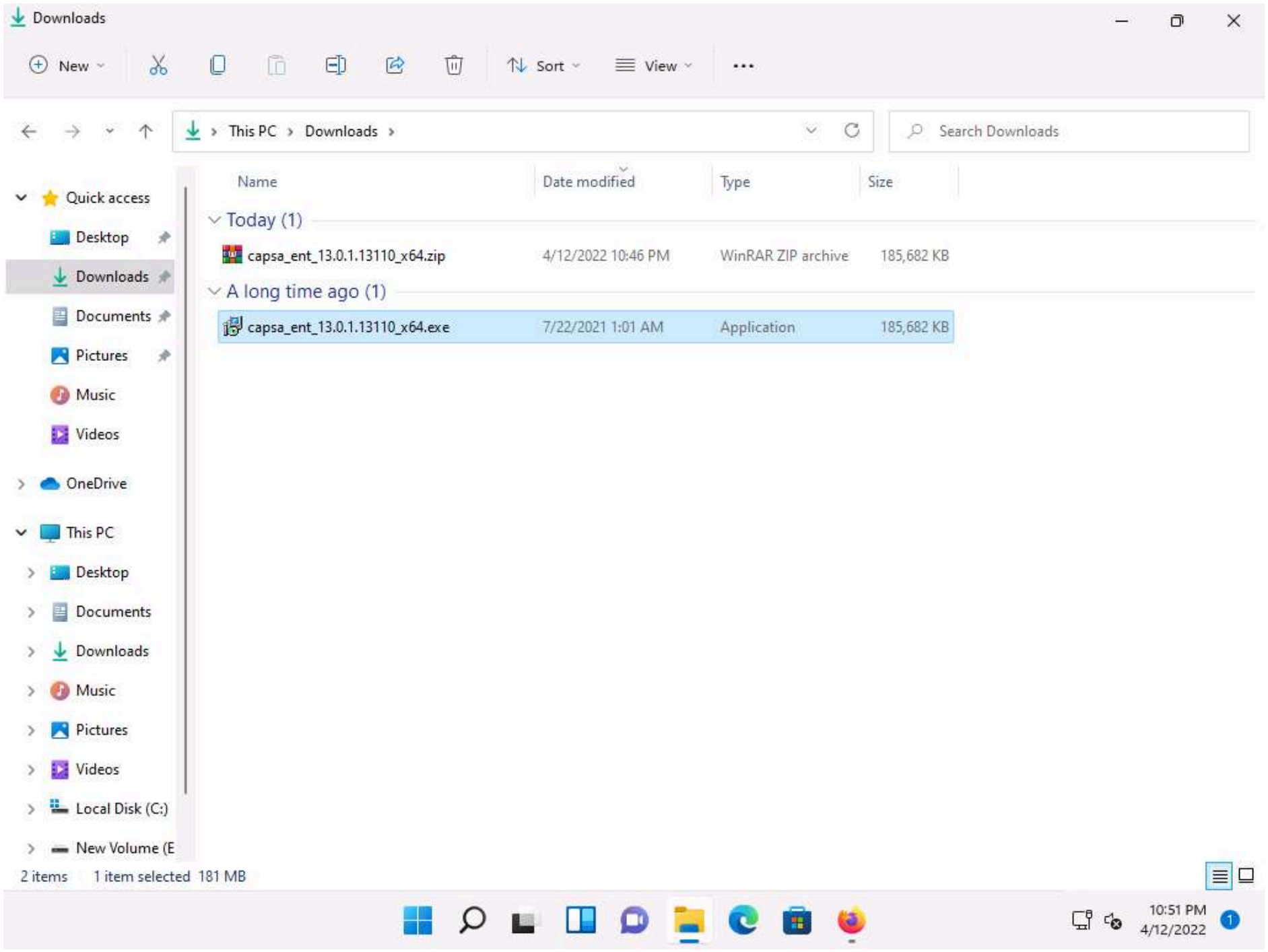


6. The **capsa_ent_13.0.1.13110_x64.zip** file starts downloading, it will take approximately **5** minutes for the download.

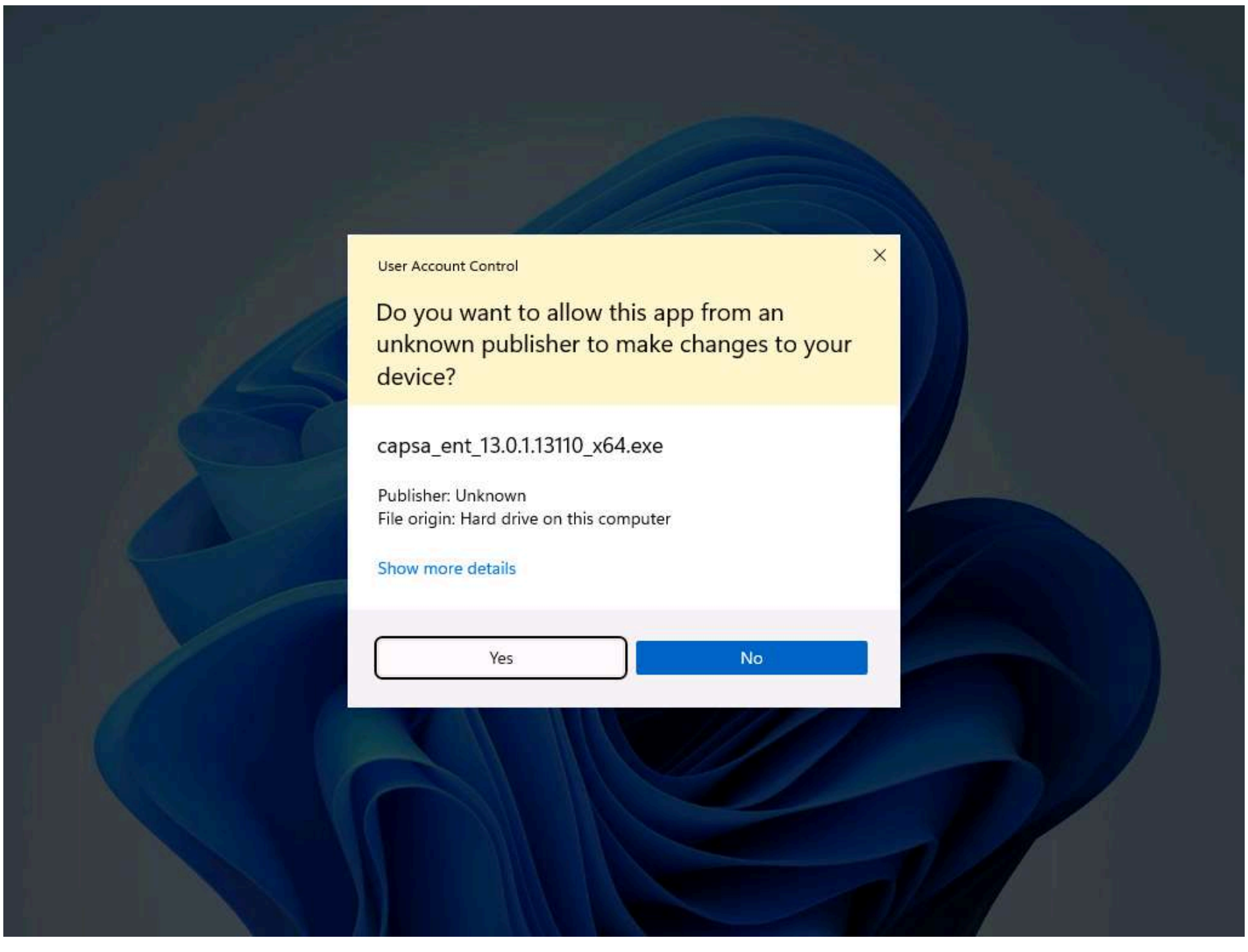
7. Once the download completes, navigate to the **Downloads** folder and right-click on **capsa_ent_13.0.1.13110_x64.zip** file and hover the cursor over **WinRAR** and select **Extract Here** option from the list.



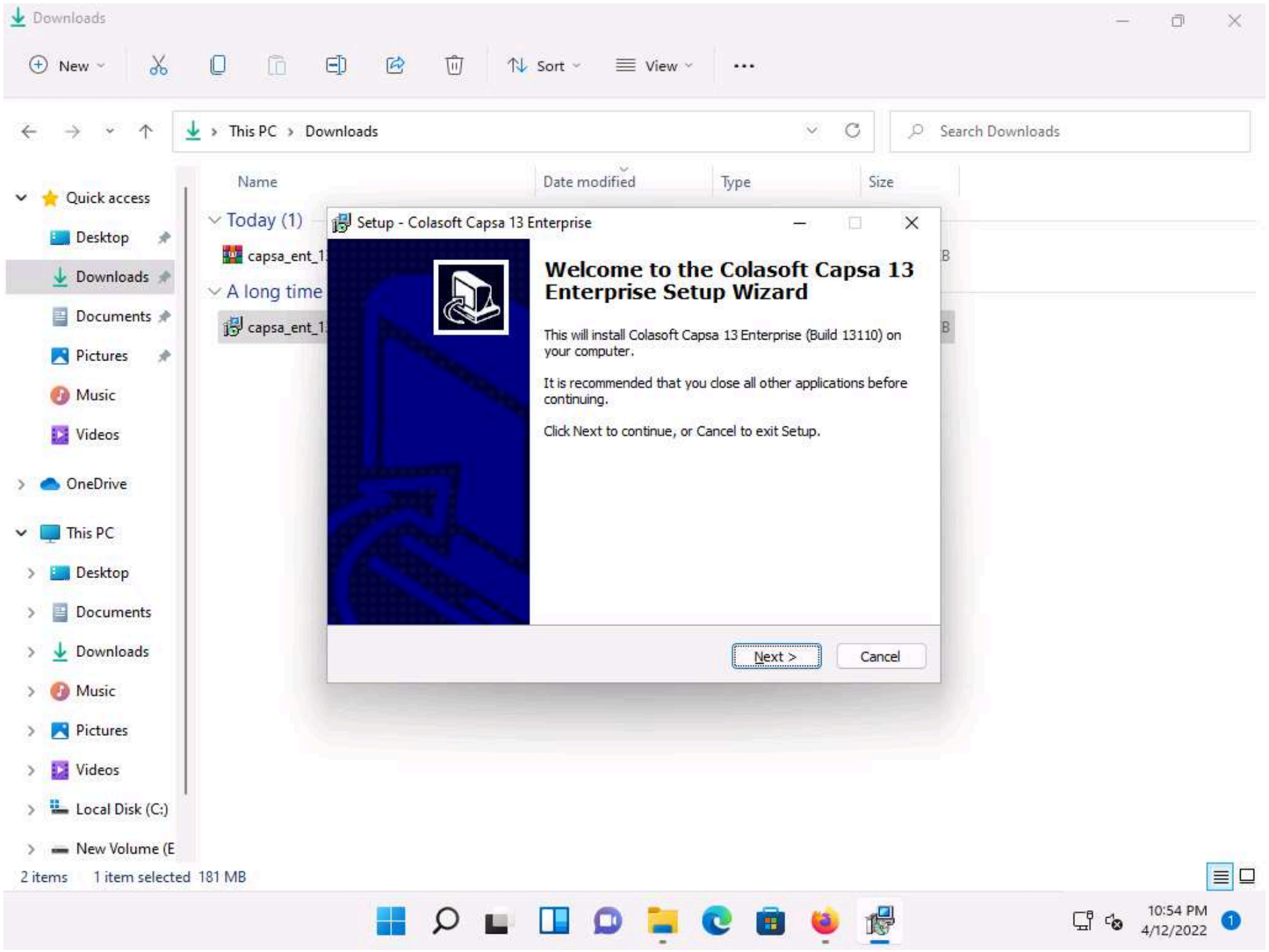
8. Once the extraction is completed, double-click the **capsa_ent_13.0.1.13110_x64.exe** file.



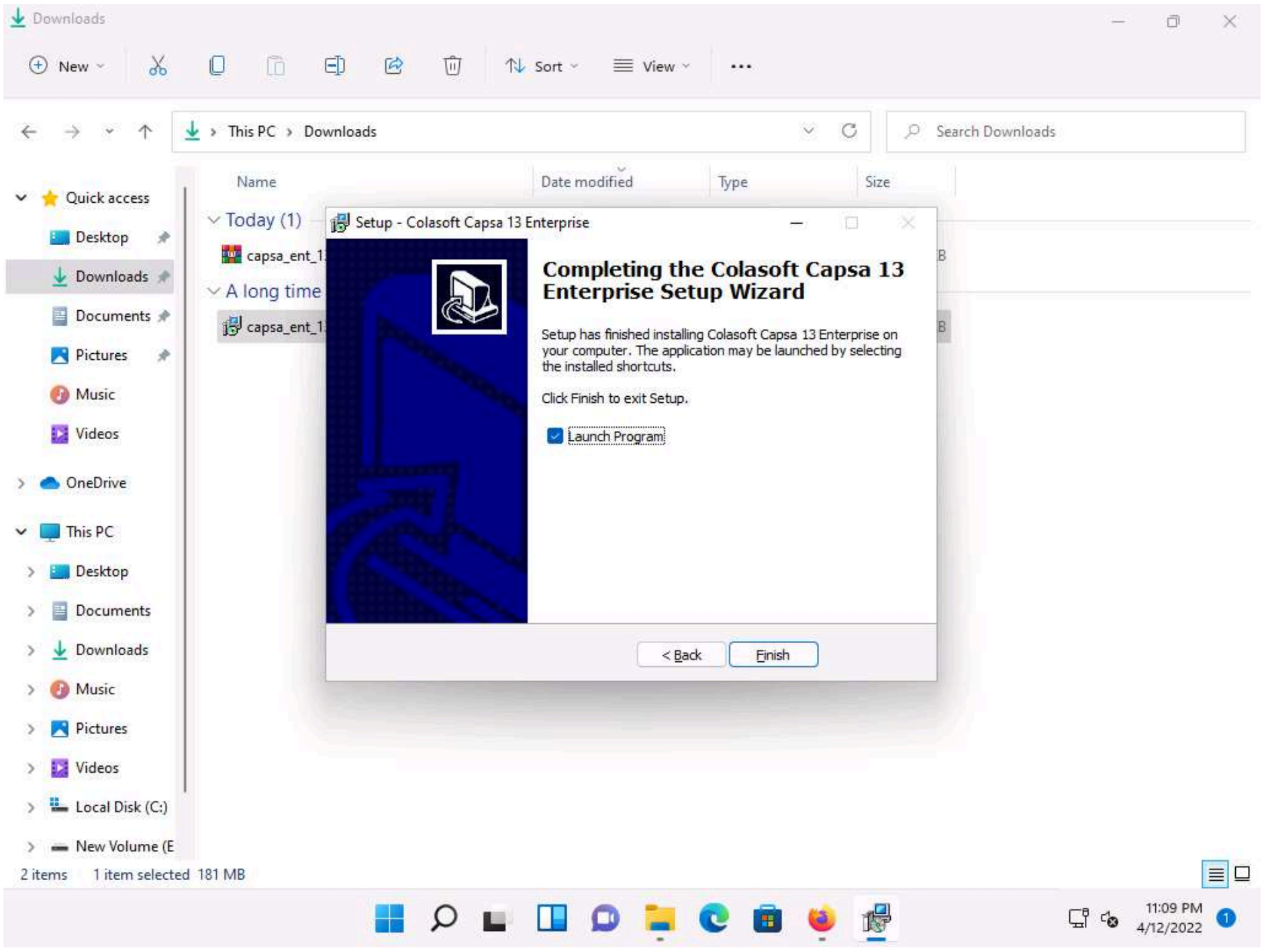
9. A **User Account Control** pop-up appears; click **Yes**.



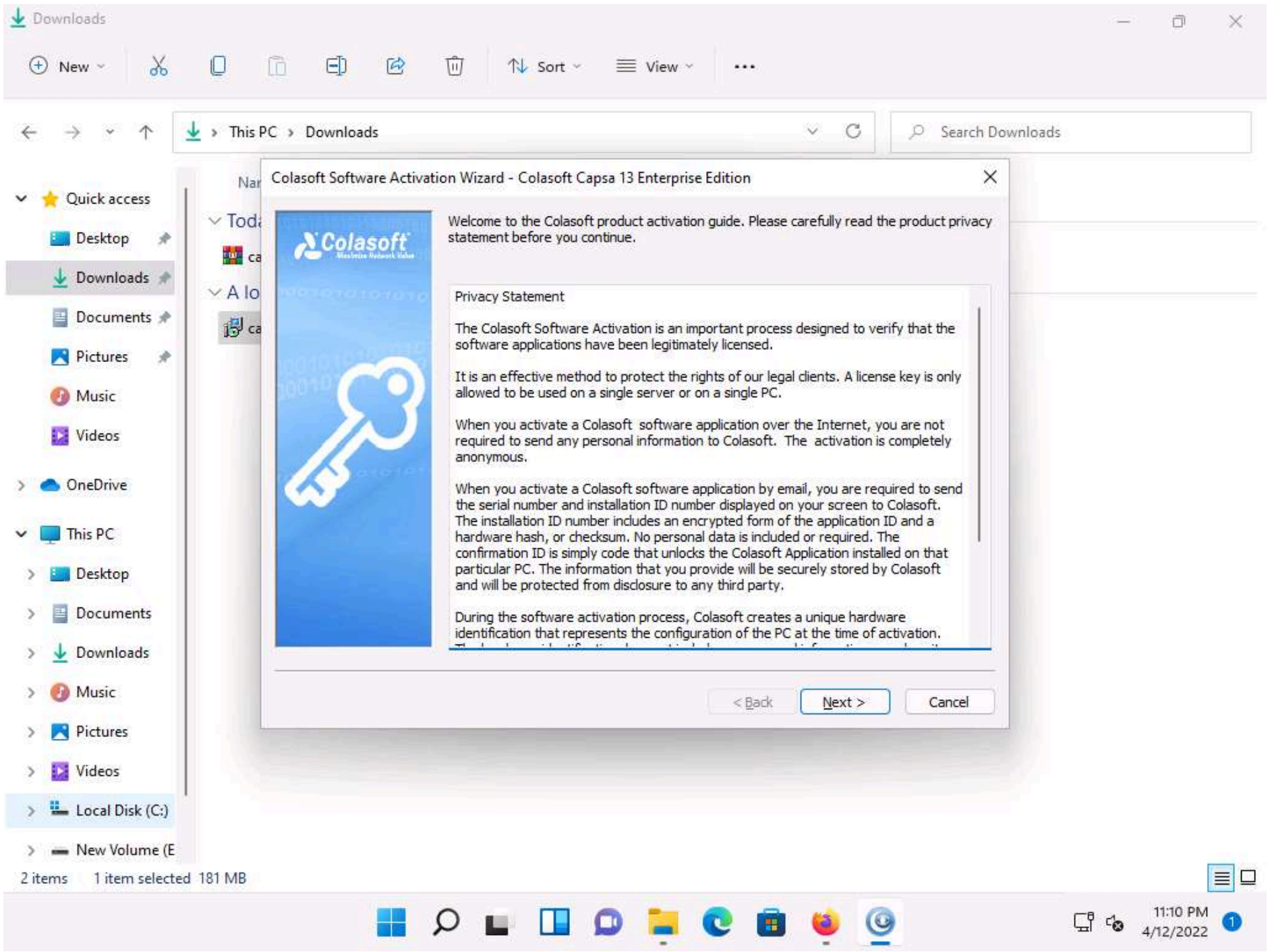
10. **Setup - Colasoft Capsa 13 Enterprise** window appears, click **Next** and follow the wizard driven steps to install **Colasoft Capsa 13 Enterprise** tool.



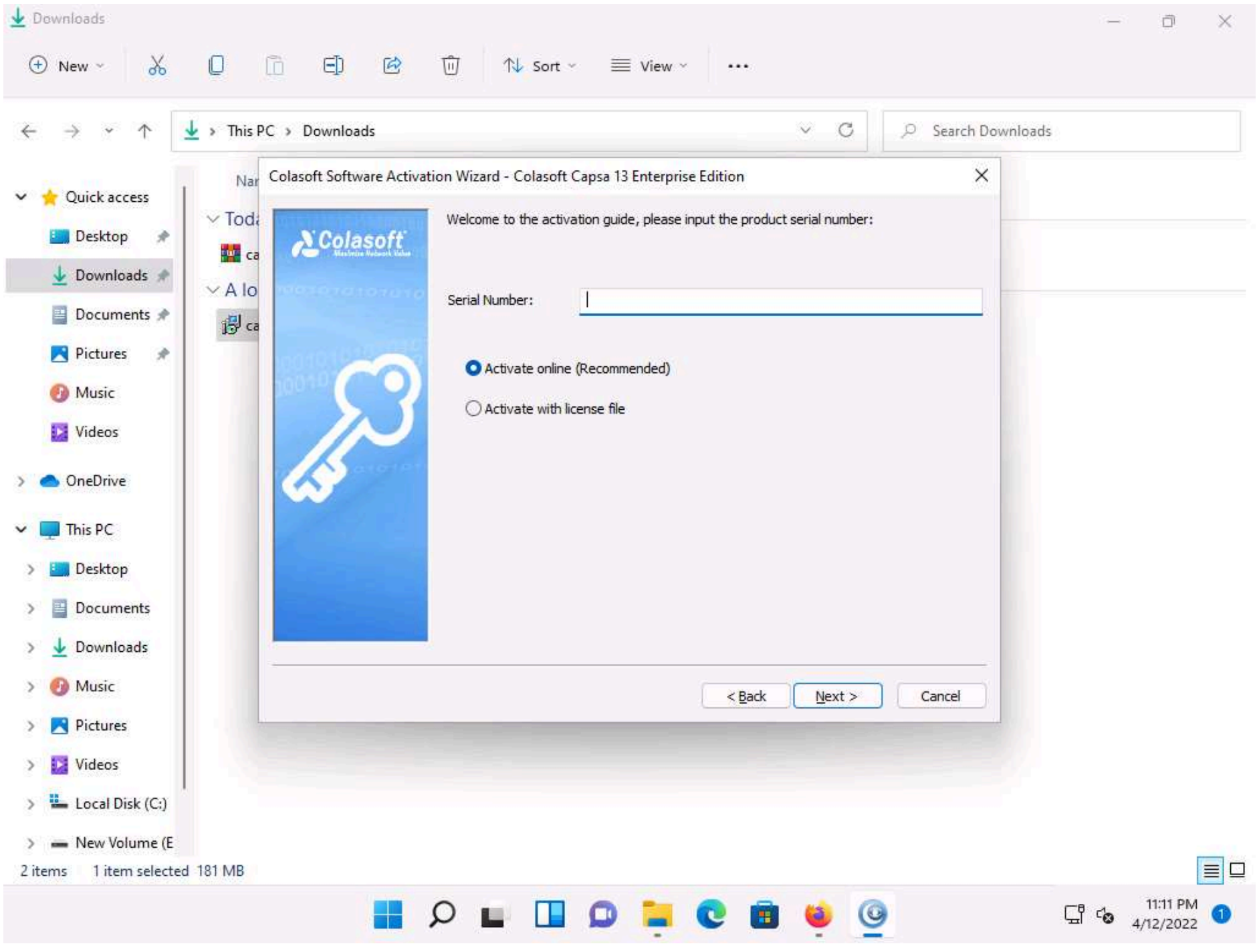
11. In the **Completing the Colasoft Capsa 13 Enterprise Setup** Wizard, ensure that **Launch Program** checkbox is checked and click on **Finish**.



12. In the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window, click **Next**.

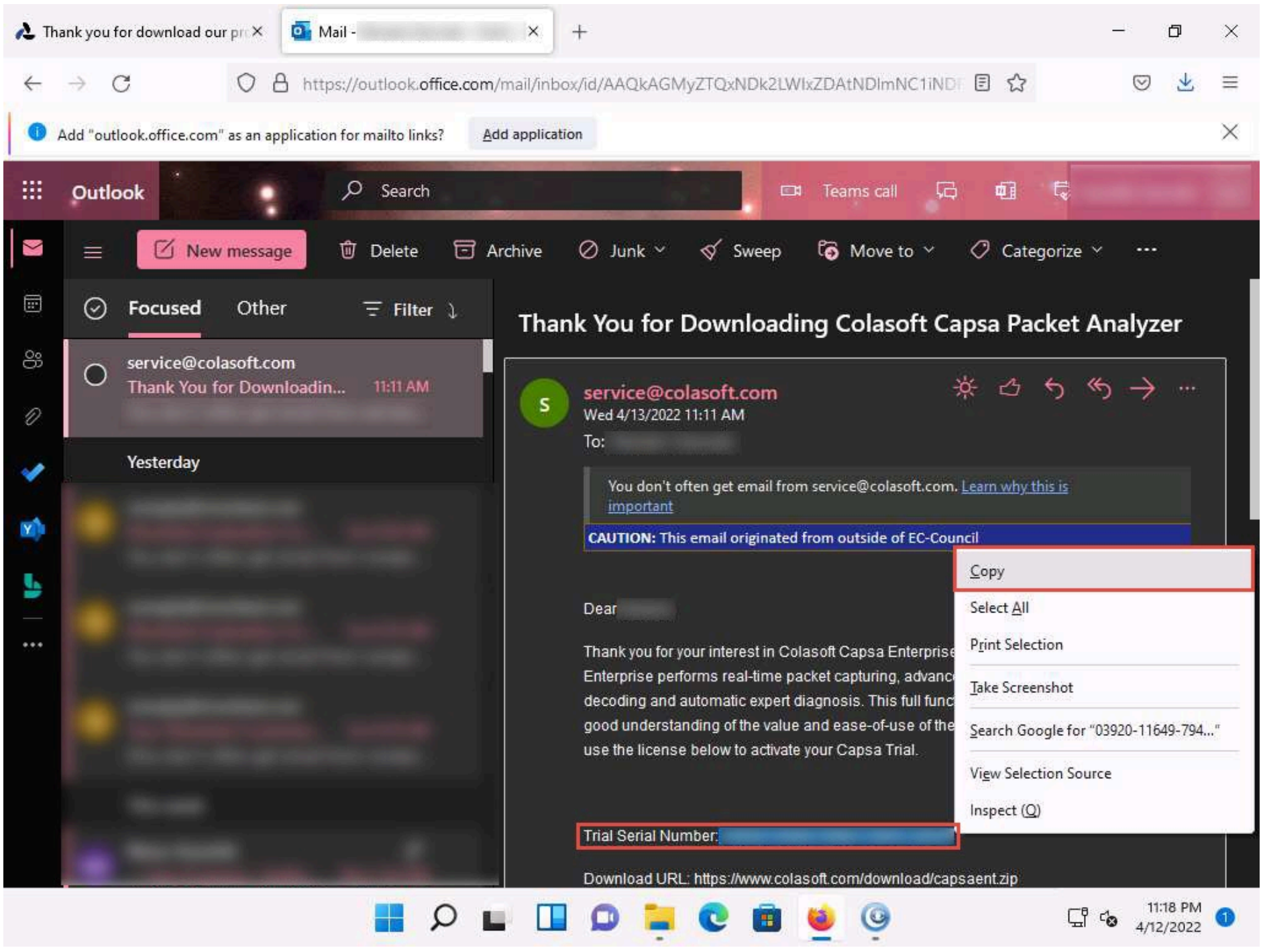


13. In the next window we need to enter the serial number to activate the license.

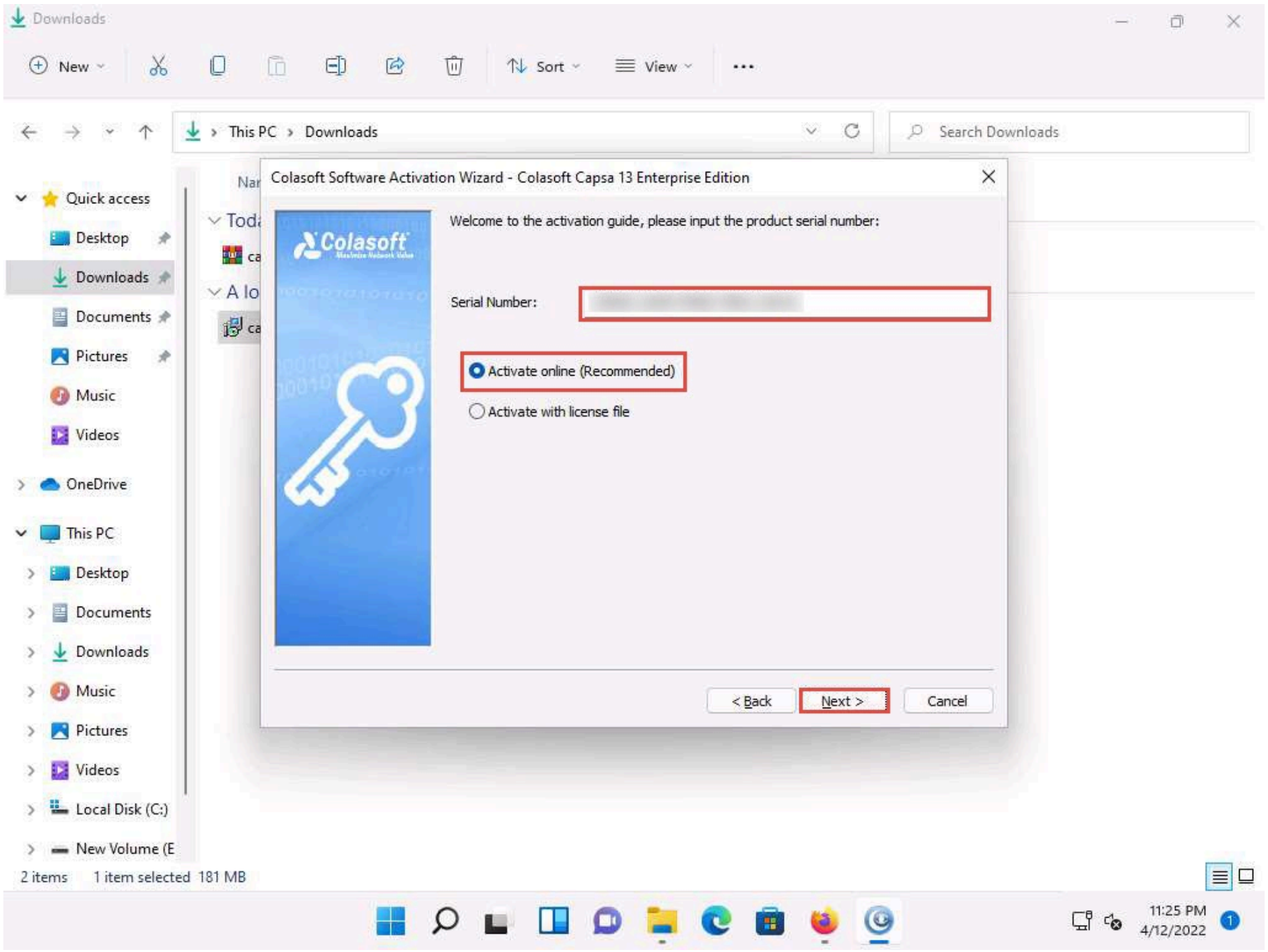


14. Leave the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** as it is and switch to the browser.

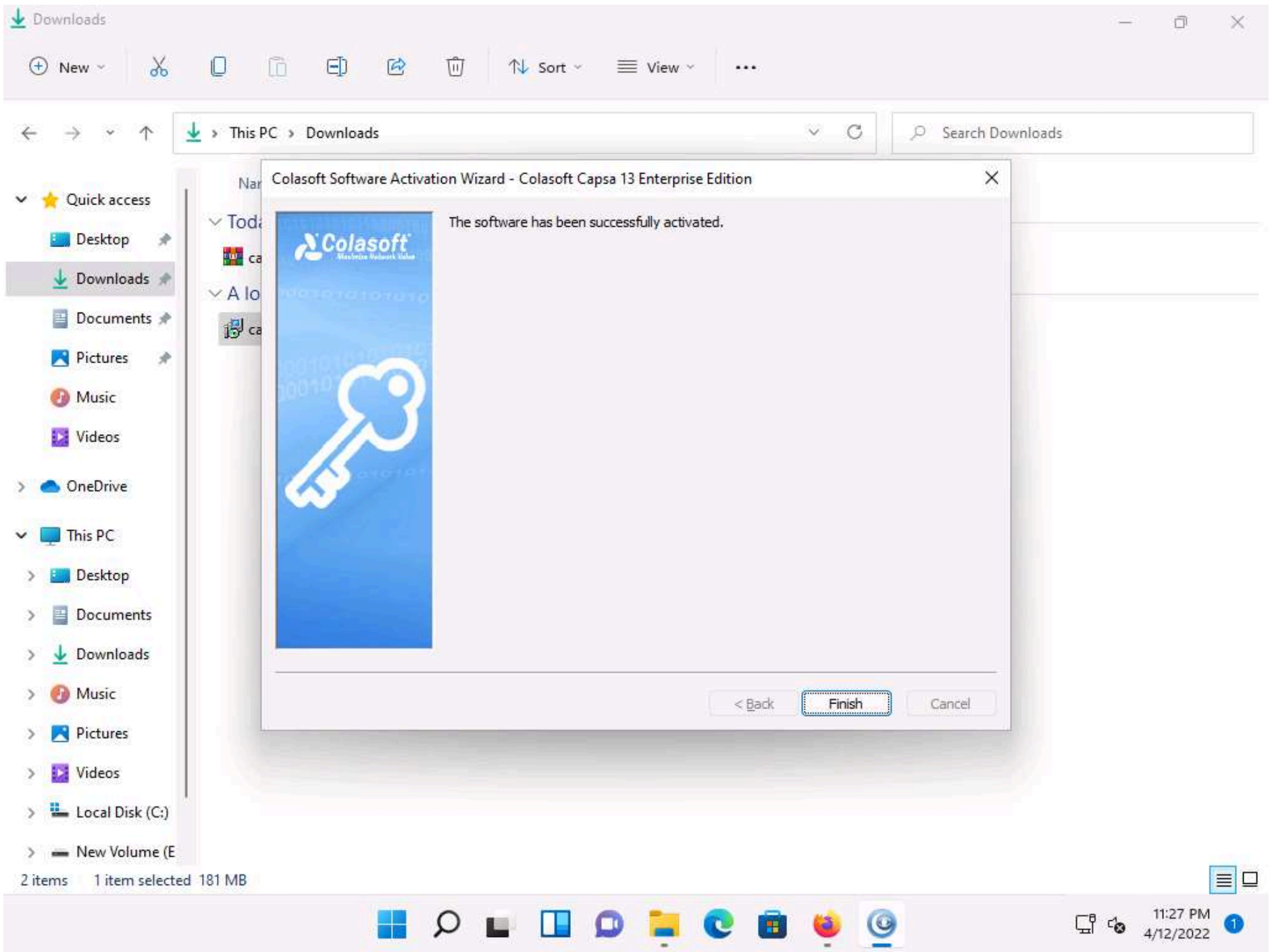
15. Open a new tab in the browser and log in to the email account you provided during registration. Open the email from **service@colasoft.com** and copy the **Trial Serial Number** as shown in the screenshot.



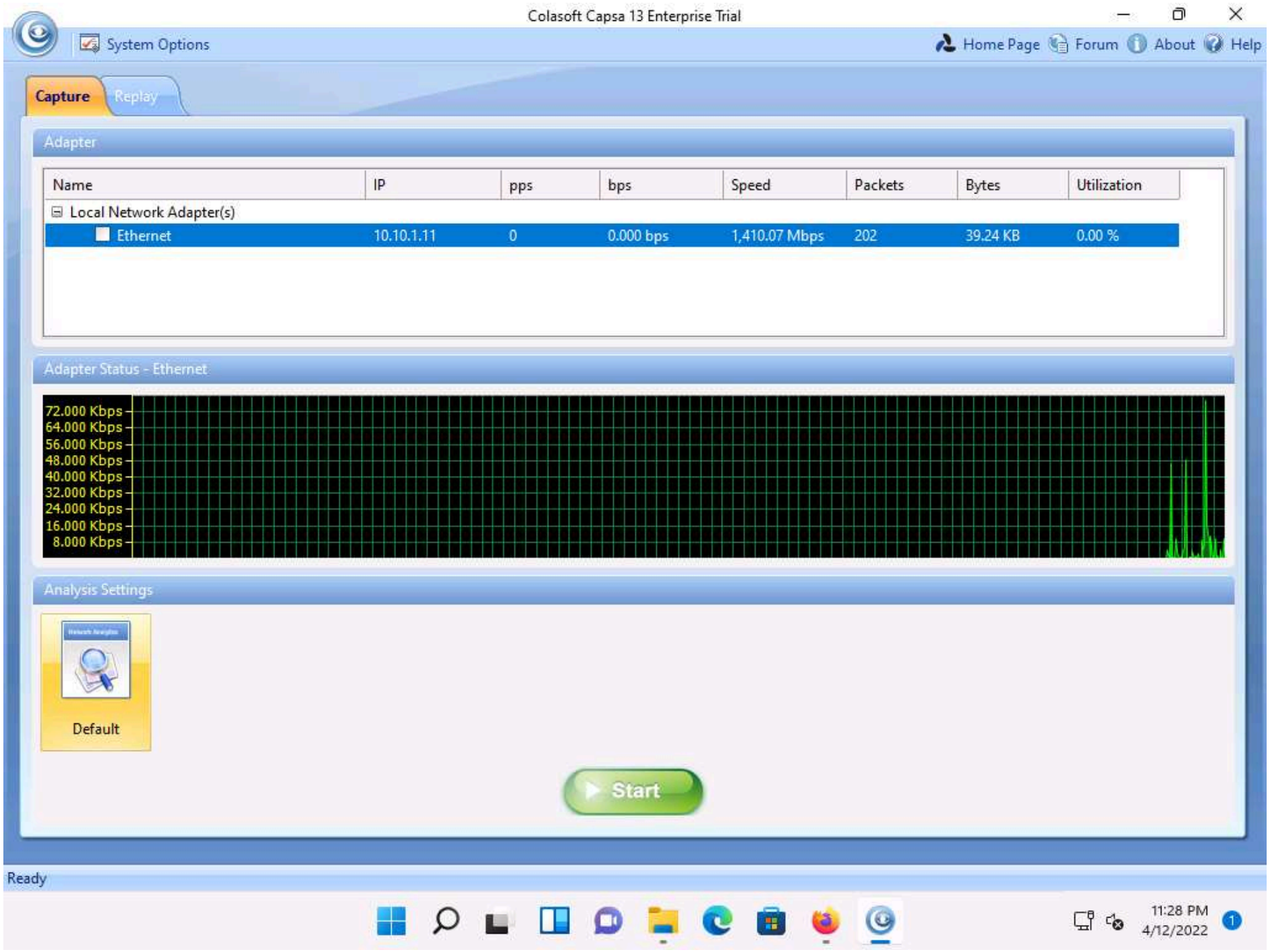
16. Now, minimize the browser window and switch to the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window and paste the copied serial number in the **Serial Number** field. Ensure that **Activate online (Recommended)** radio button is selected and click on **Next**.



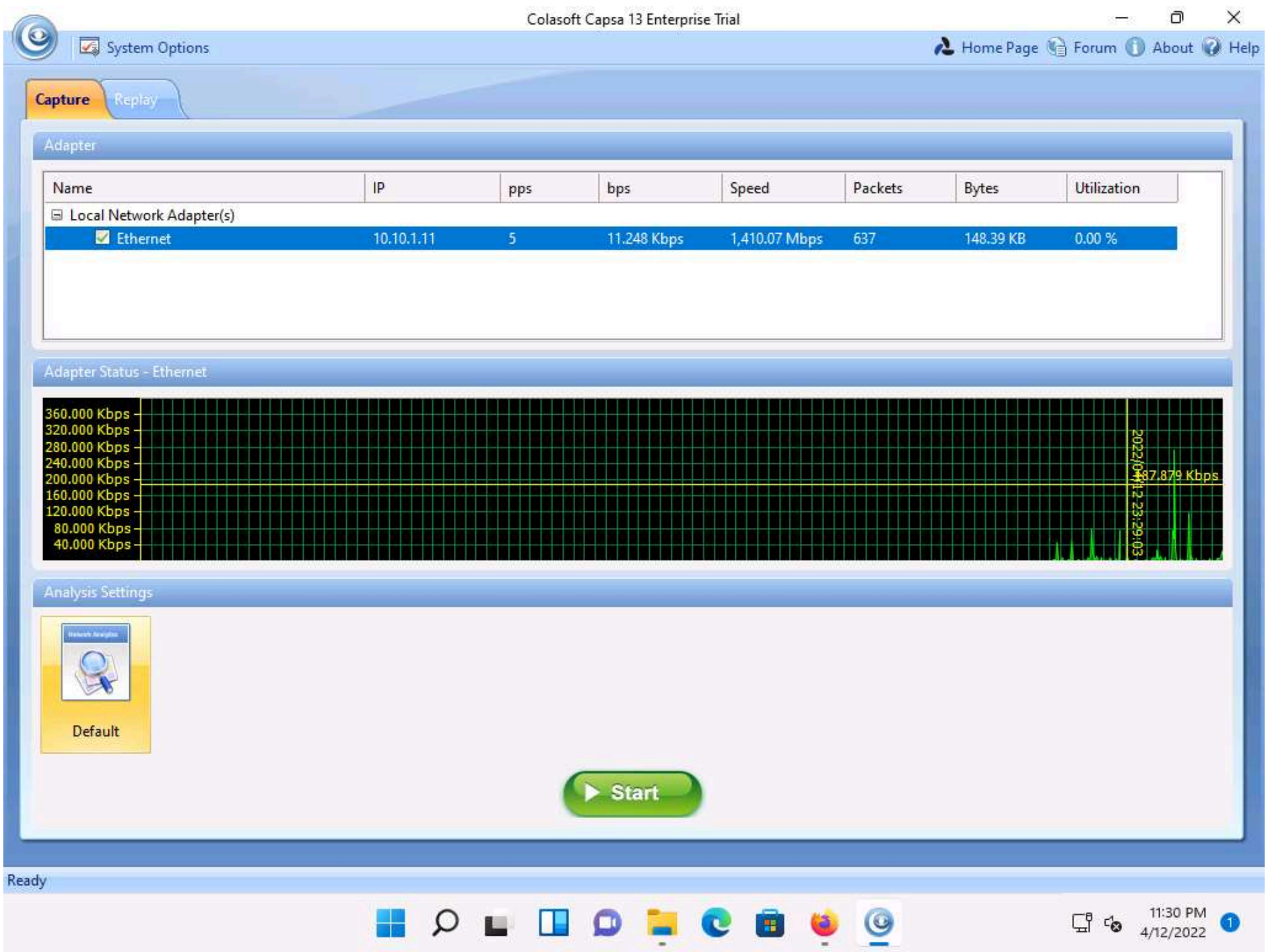
17. A **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window appears, showing that the software has been successfully activated, click on **Finish**.



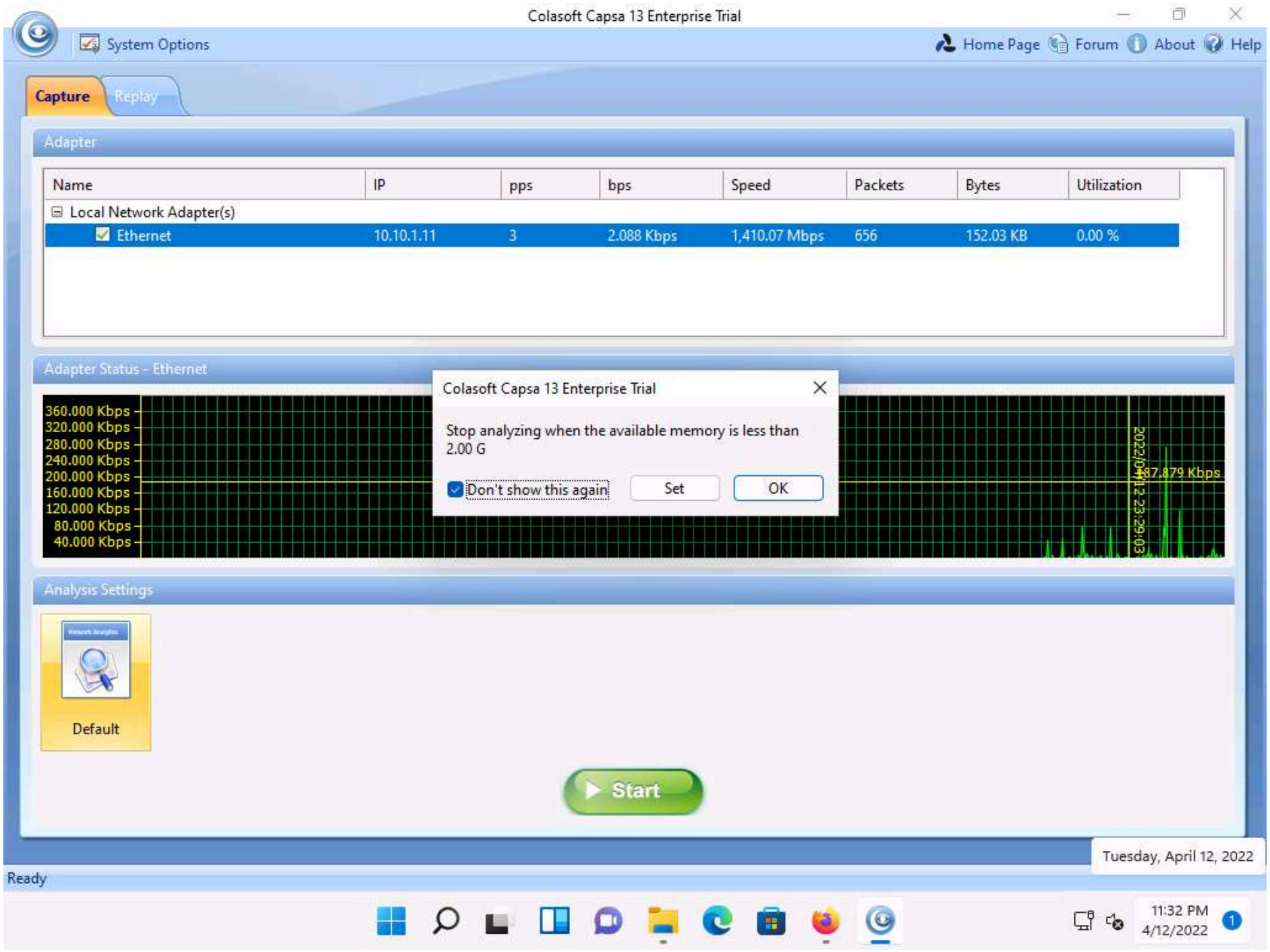
18. After successful installation, A **Colasoft Capsa 13 Enterprise Trial** window appears.



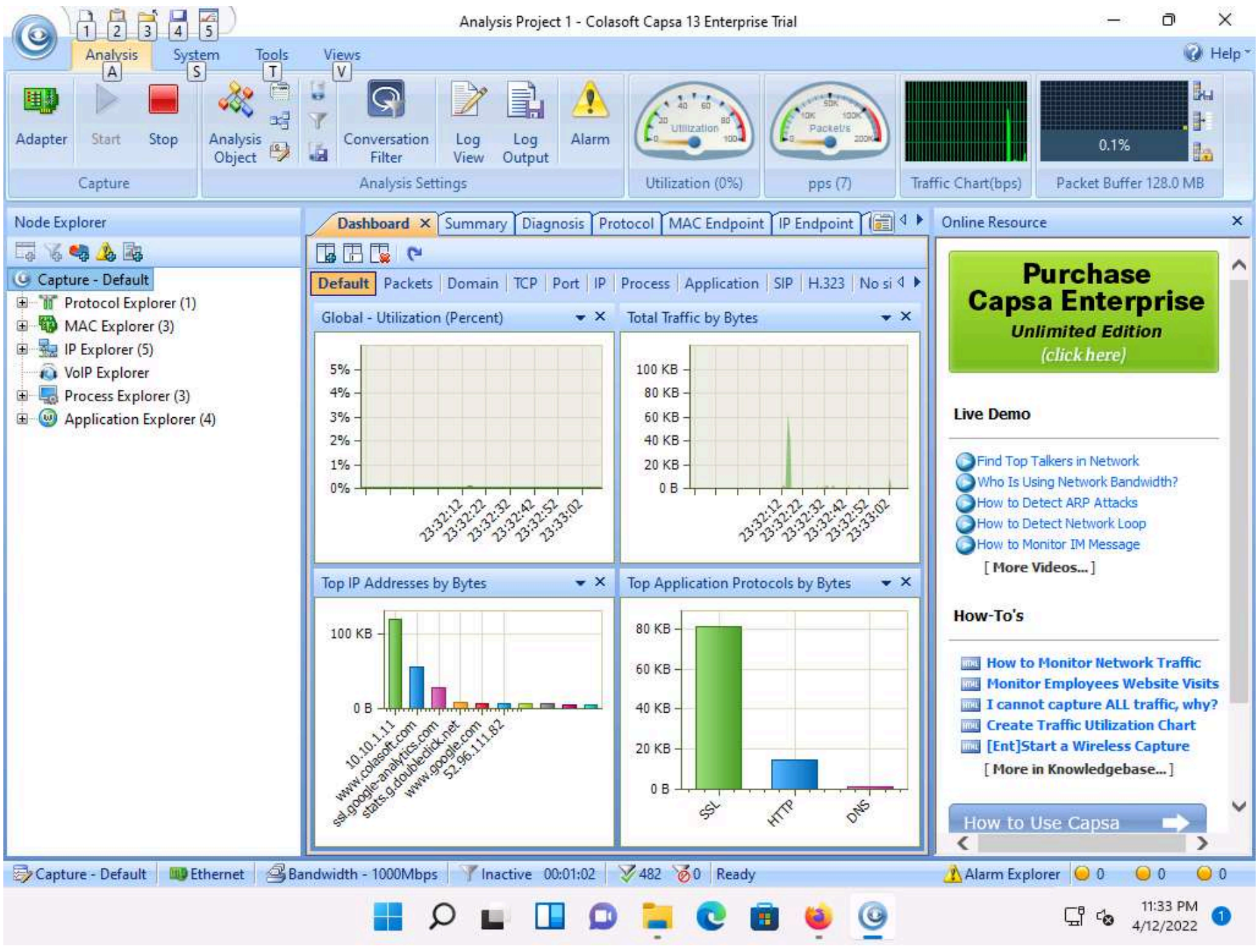
19. In the **Colasoft Capsa 13 Enterprise Trial** window check the checkbox beside the available adapter (here, **Ethernet**) and click on **Start**.



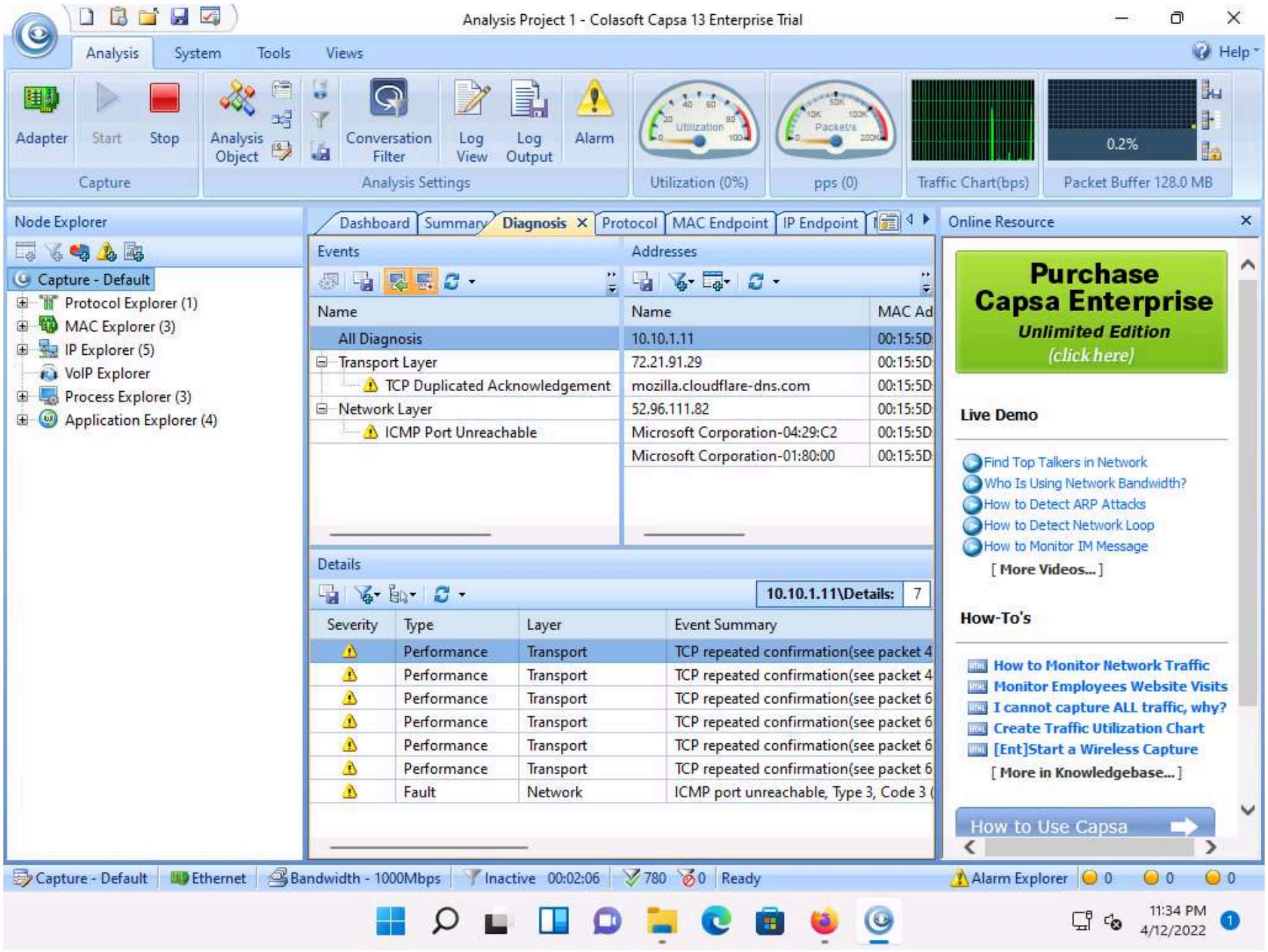
20. If a **Colasoft Capsa 13 Enterprise Trial** pop-up appears, select **Don't show this again** checkbox and click on **OK**.



21. The **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window appears, as shown in the screenshot.

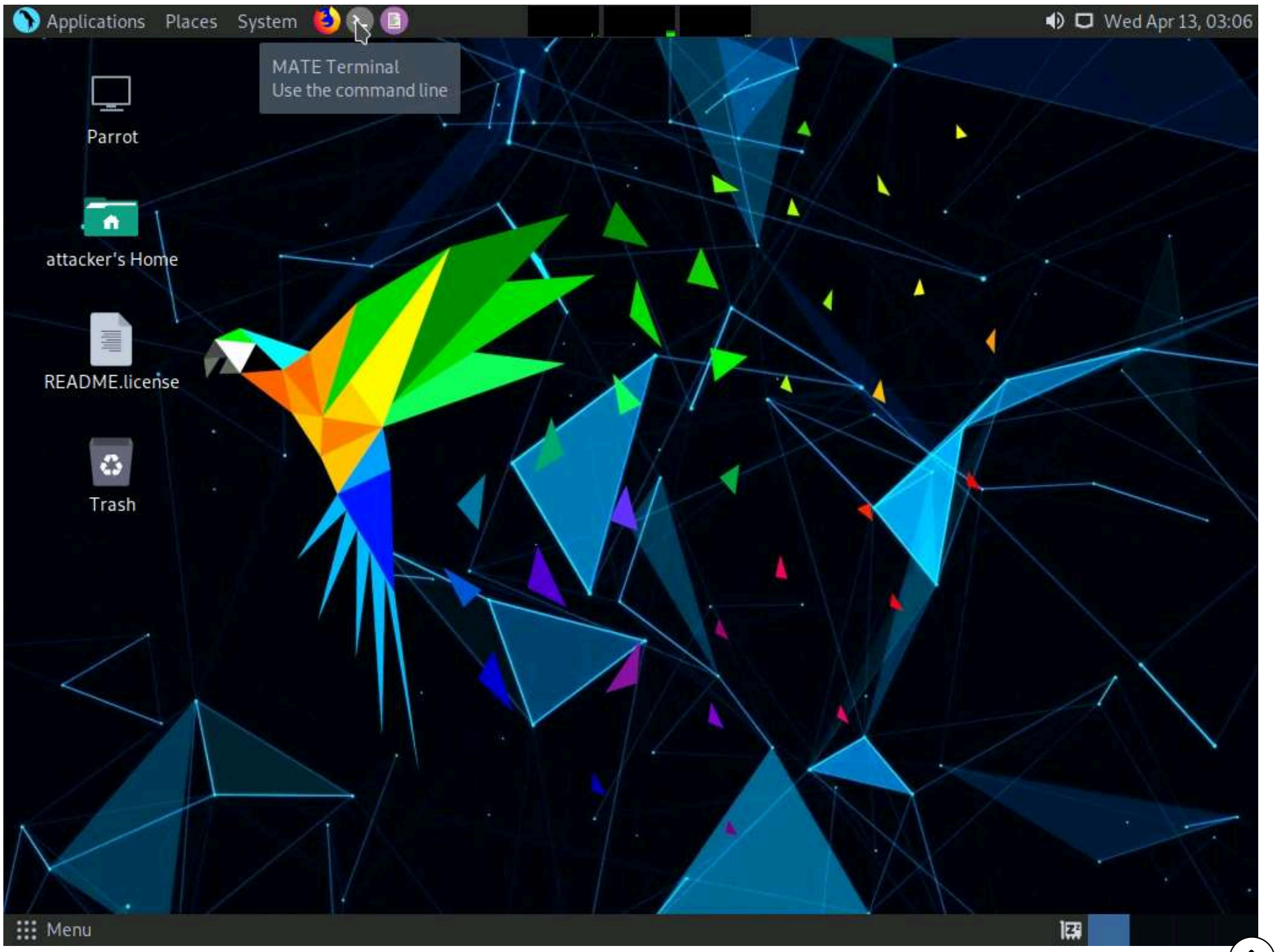


22. Navigate to the **Diagnosis** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window.



23. Click on **CEHv12 Parrot Security** to switch to **Parrot Security** machine.

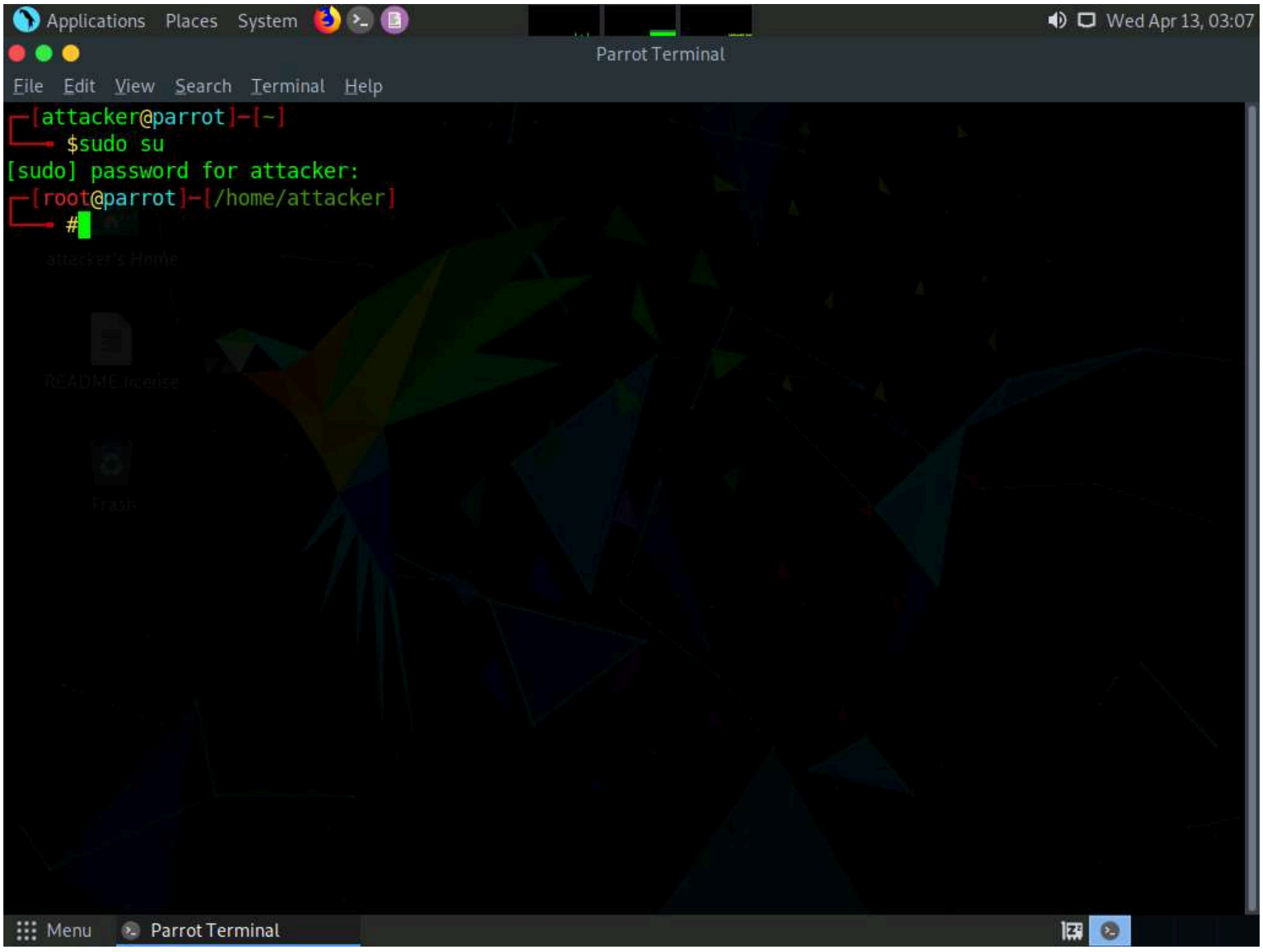
24. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



25. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

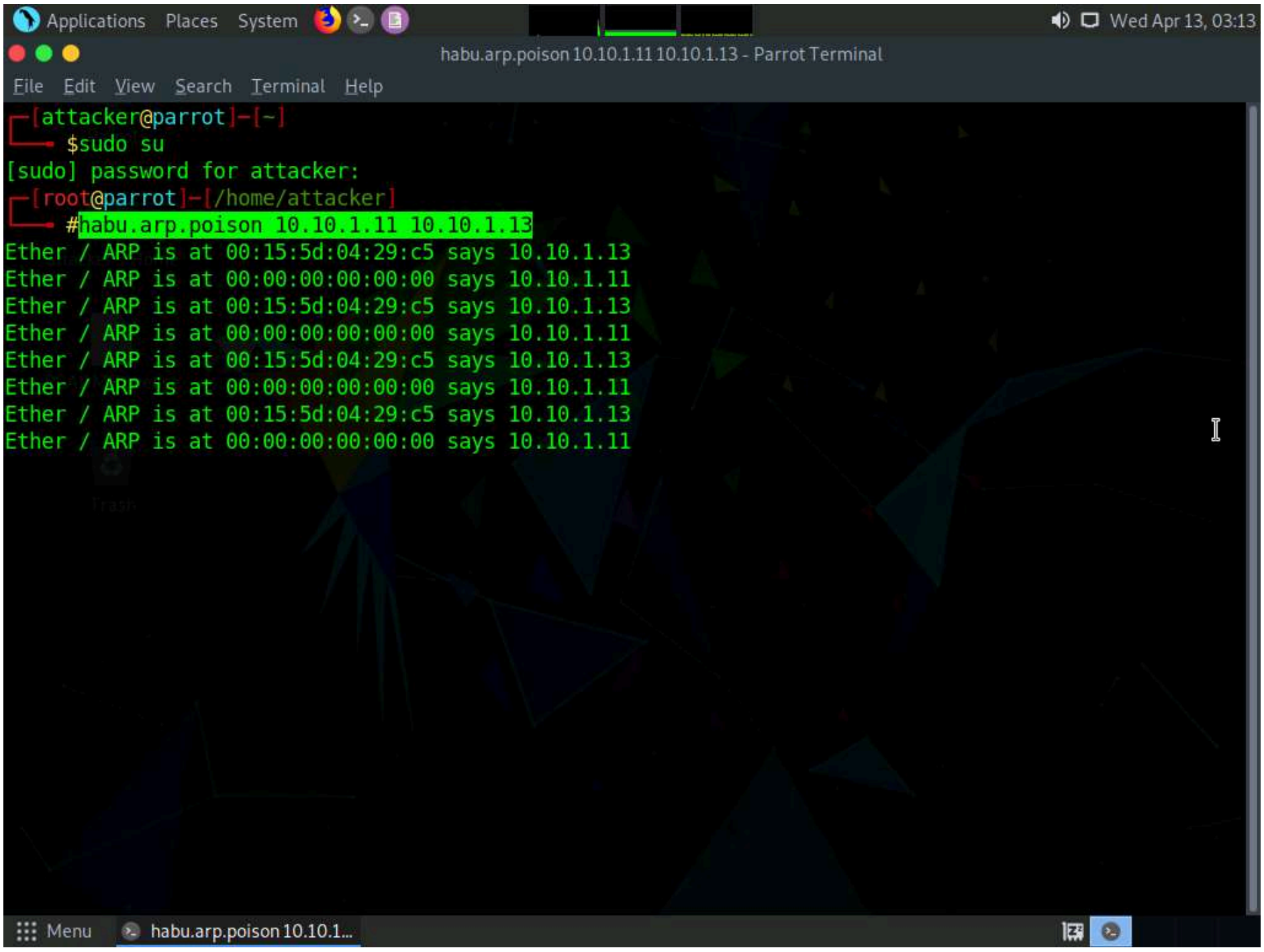
26. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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



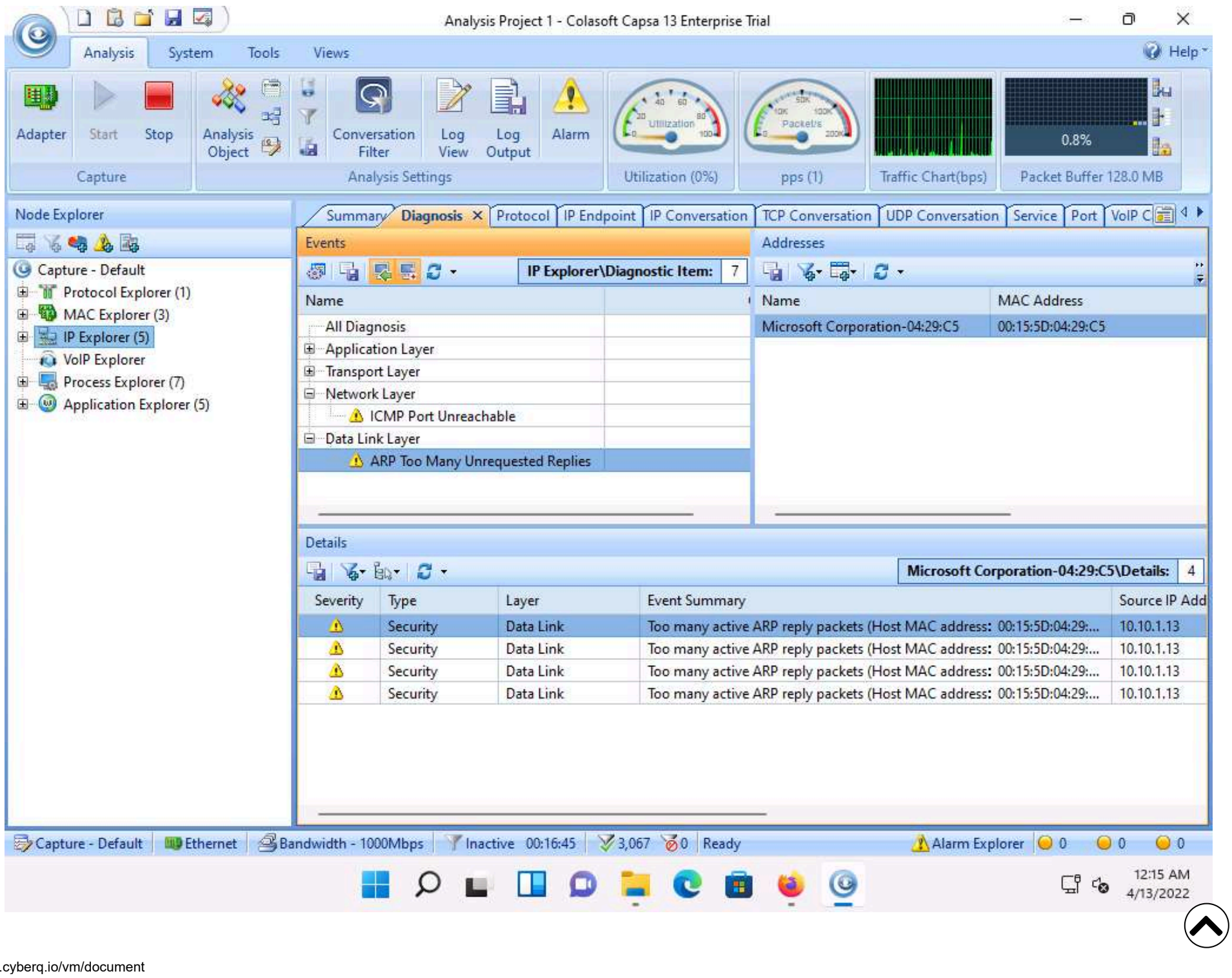
27. In the terminal window, type **habu.arp.poison 10.10.1.11 10.10.1.13** and press **Enter**, to start ARP poisoning on **Windows 11** machine.

> Note: The above command sends ARP **'is-at'** packets to the specified victim(s), poisoning their ARP tables to send their traffic to the attacker system.
>
> Note: If you receive any error while running the command ignore it.



28. Click **CEHv12 Windows 11** to switch to **Windows 11** machine.

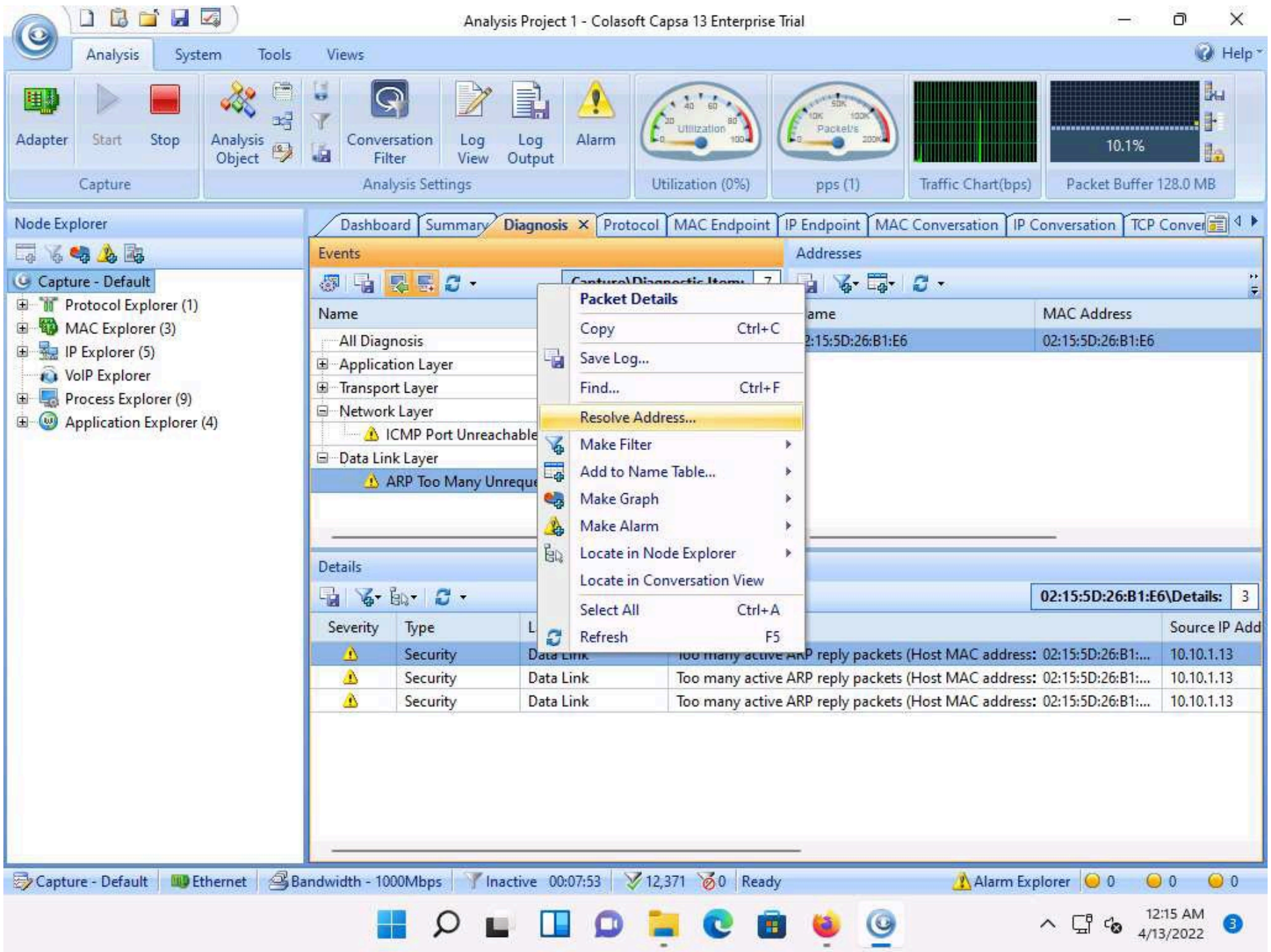
29. In the **Diagnosis** tab, expand the **Data Link Layer** node to see the **ARP Too Many Unrequested Replies** warning.



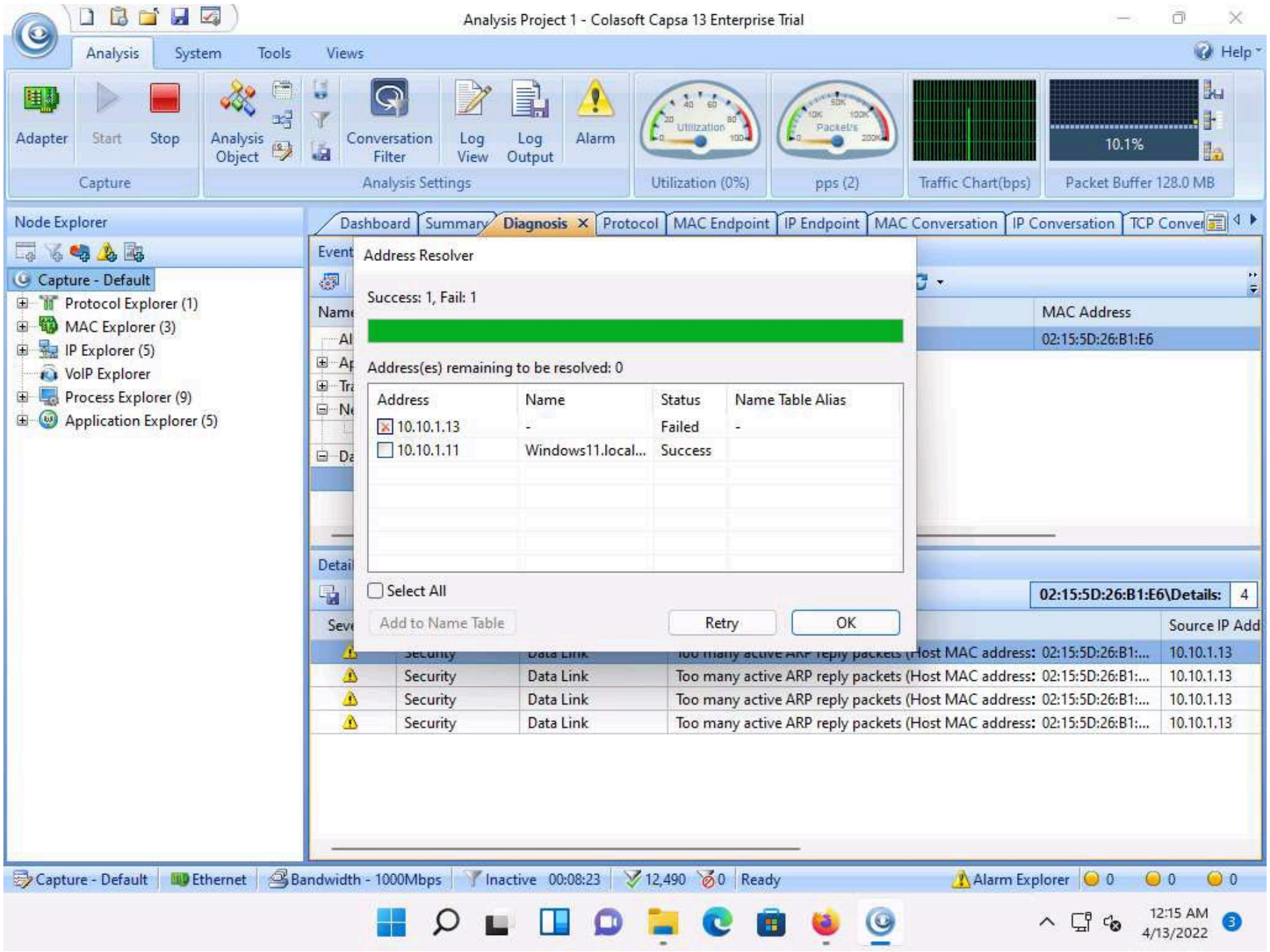
Note: It will take approximately **10** minutes for the tool to capture the **ARP** requests.

38. Click on **ARP Too Many Unrequested Replies** warning under **Data Link Layer** node.

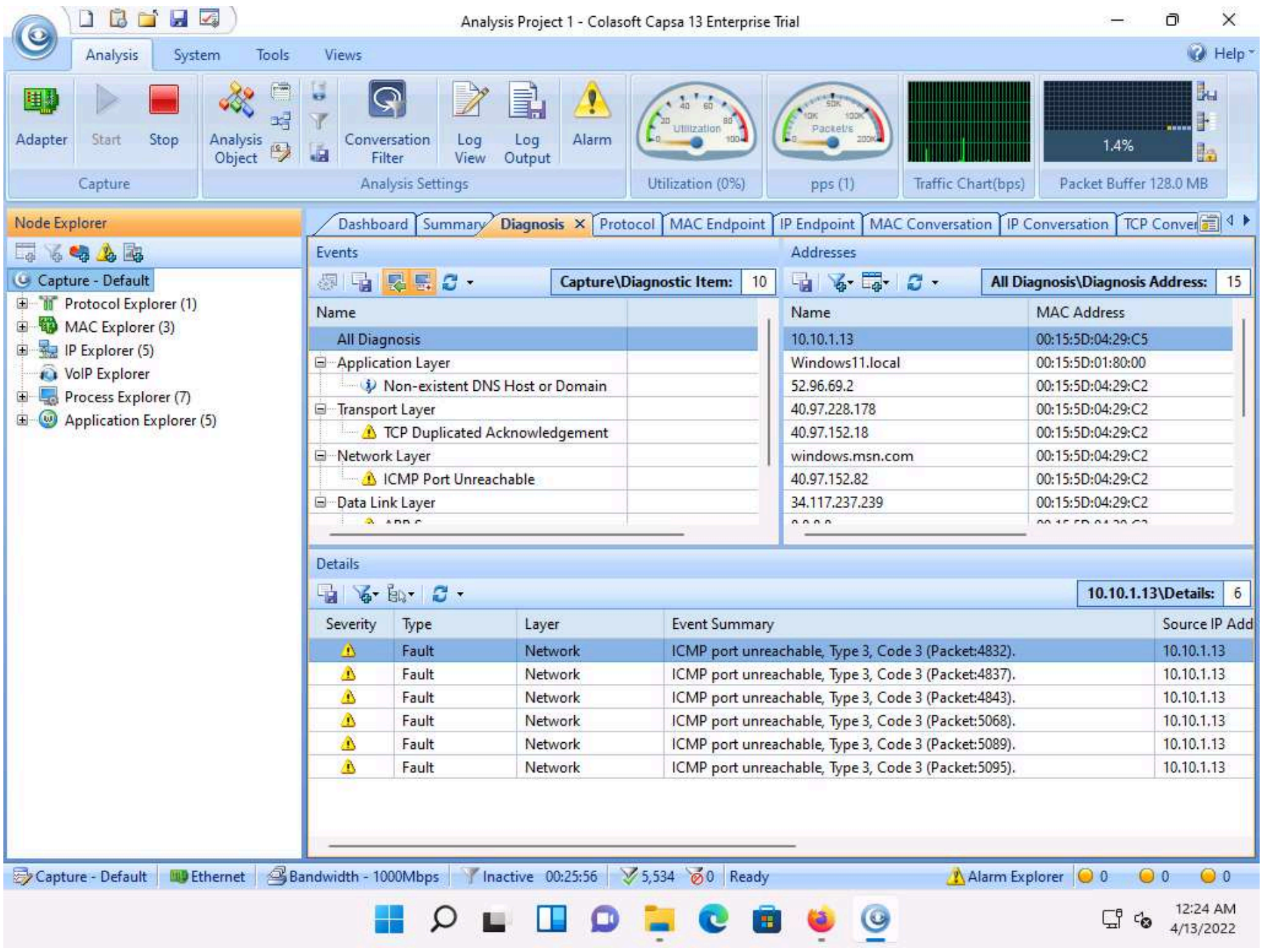
39. Right-click on **Security** warning under **Details** section and select **Resolve Address...** from the context menu.



40. An **Address Resolver** pop-up appears, once the address resolving completes click on **OK**.



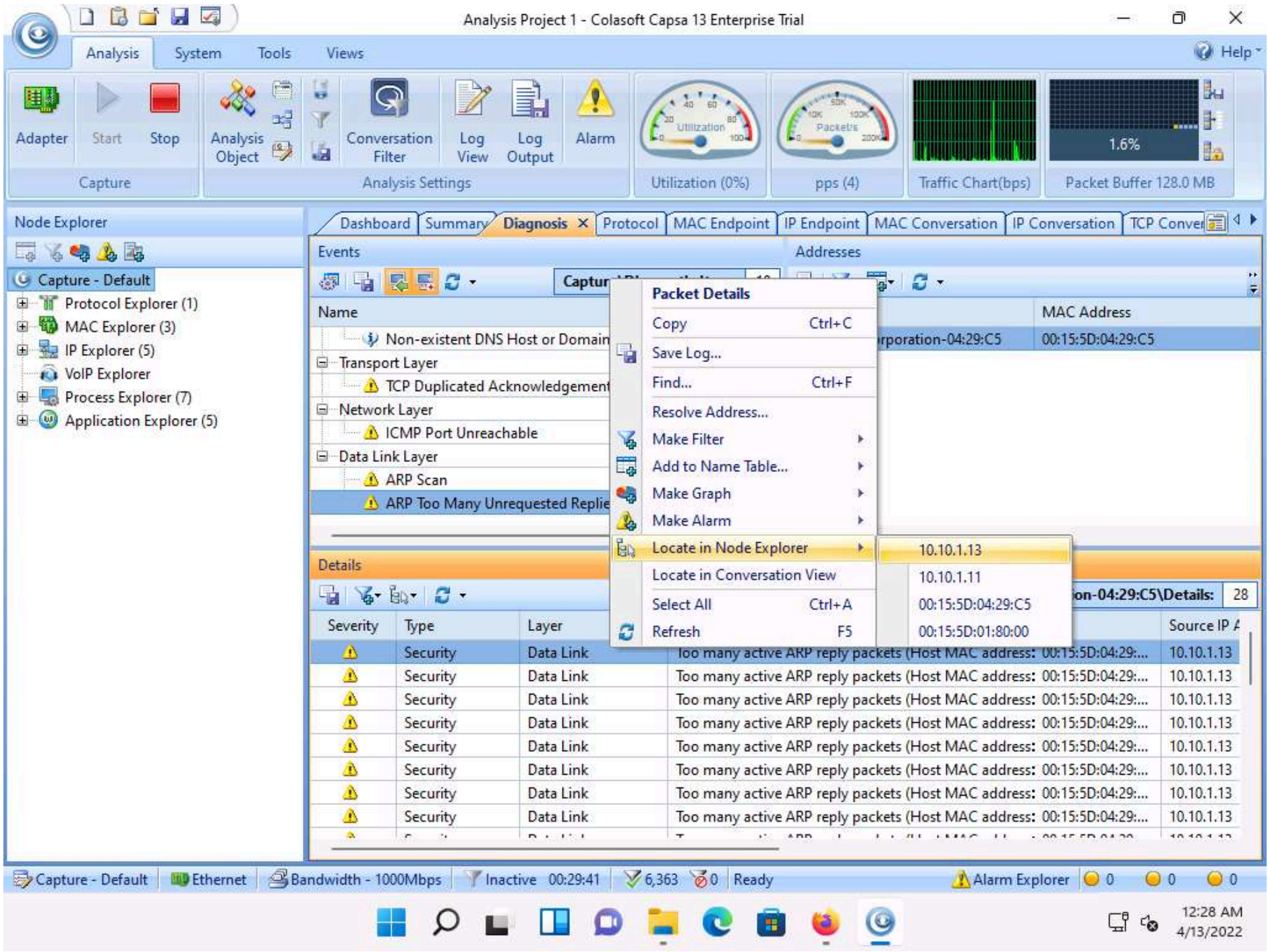
41. Now to locate the Parrot Machine's IP address click on **Capture Default** option under **Node Explorer** section in the left-pane.



42. Click on **ARP Too Many Unrequested Replies** warning under **Data Link Layer** node.

43. Now right click any warning in the **Details** tab and click on **Locate in Node Explorer** and select **Parrot Security** machine's IP address from the list (here, **10.10.1.13**).

Note: Here, the IP address of the Parrot Security machine is the attacker's IP address.

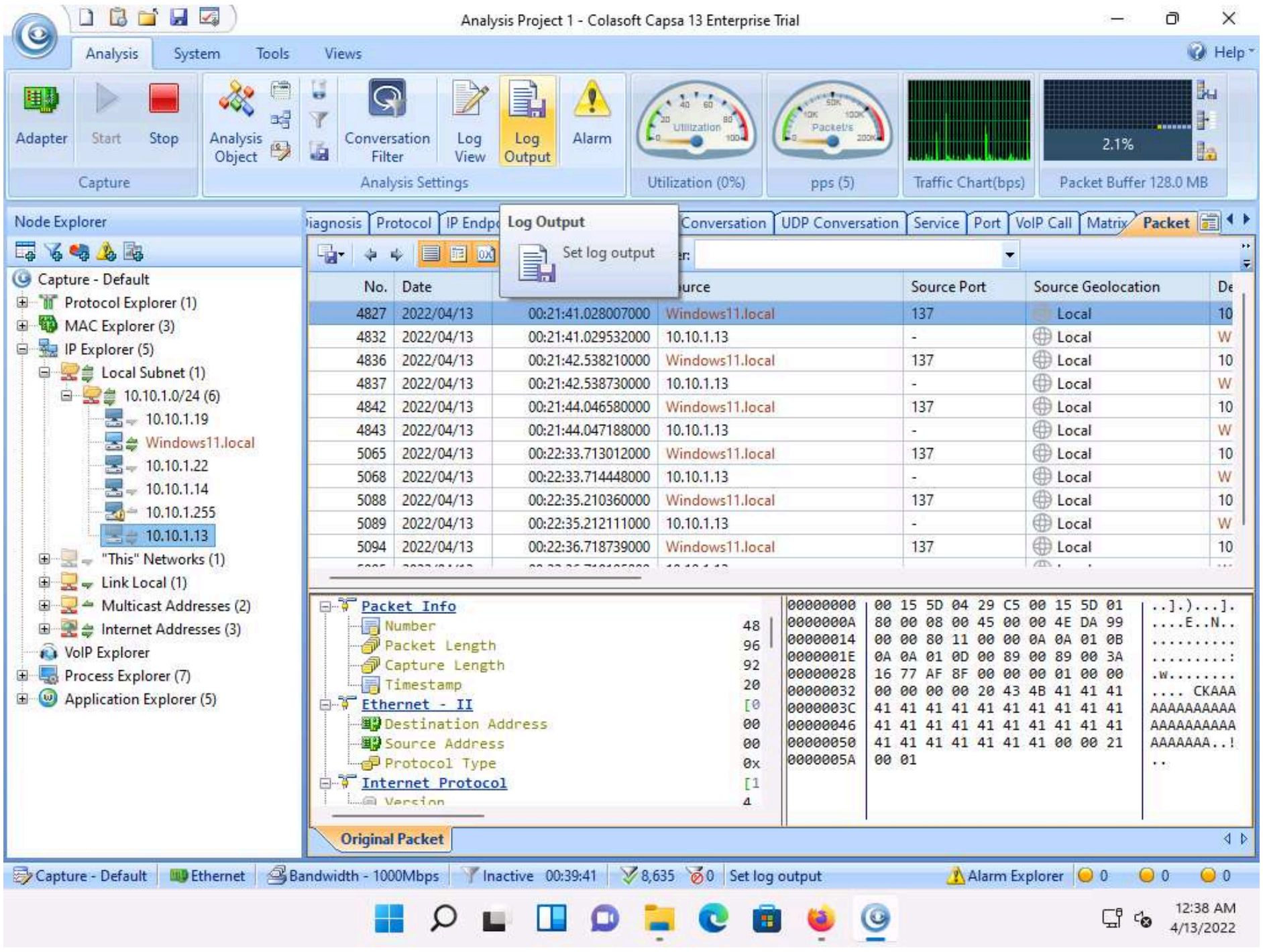


44. The IP address of the Parrot Security machine is displayed under **Node Explorer** section in the left-pane.

45. Now click on **Packet** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window, to check the packets transferred by the **Parrot Security** machine.

46. Similarly you can navigate to all the available tabs such as **Protocol**, **MAC Endpoint**, **IP Endpoint**, **MAC Conversation**, **IP Conversation** etc.

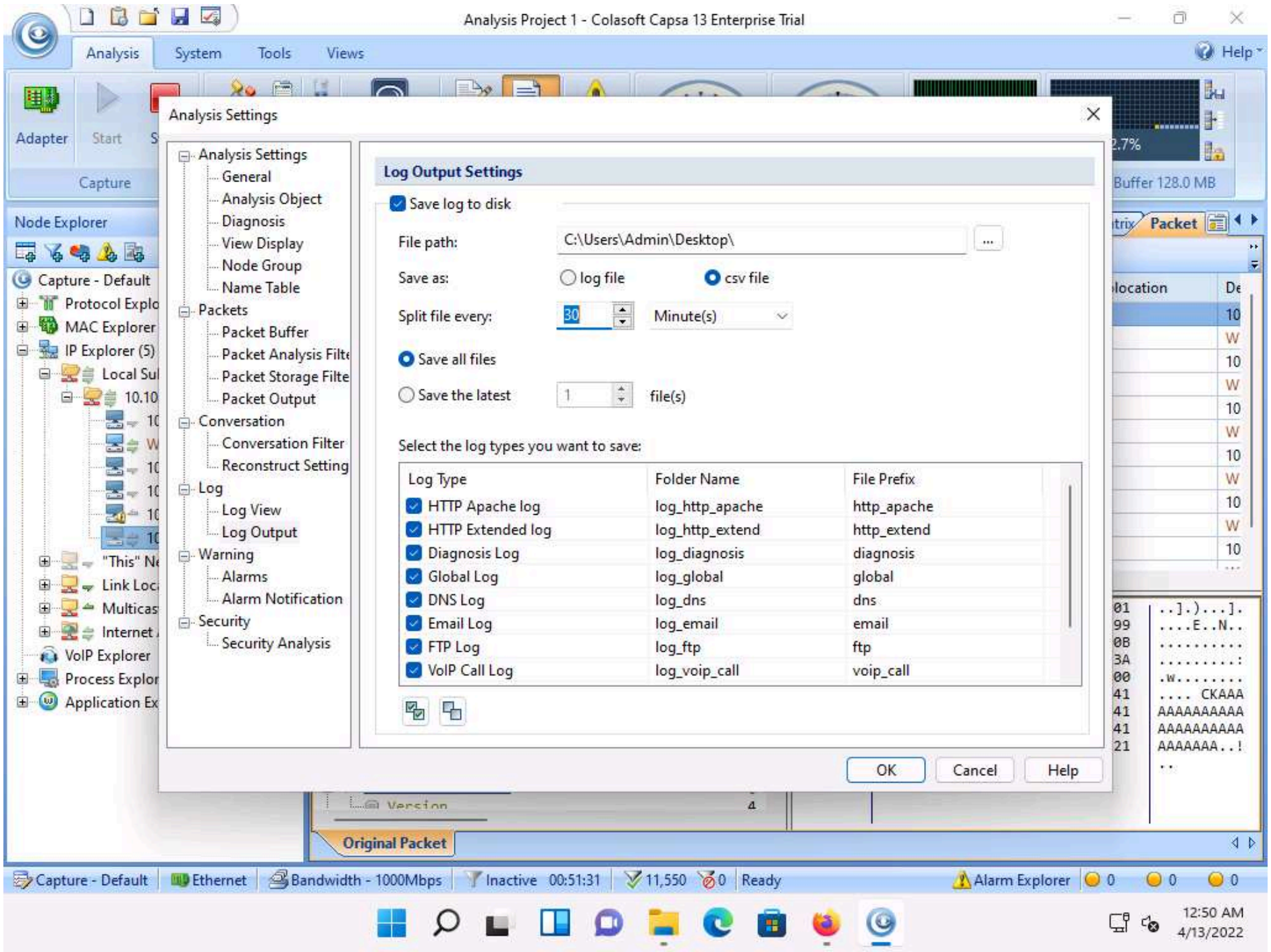
47. After completing the analysis click on **Log Output** option from the menubar.



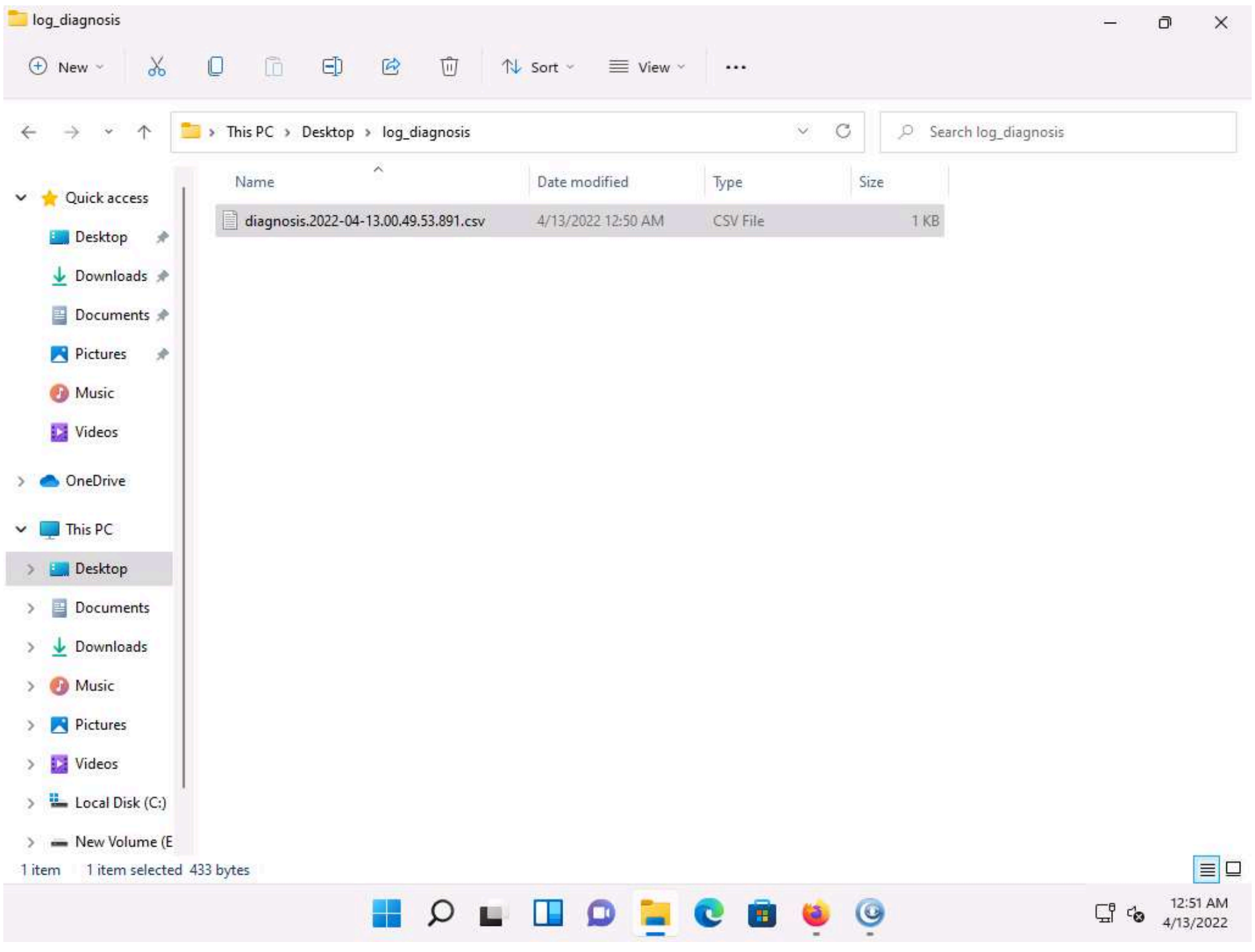
48. In the **Analysis Settings window**, check the **Save log to disk** checkbox and click the ellipsis button under **File path** option.

49. In the **Browse For Folder** window, select **Desktop** and click on **OK**.

50. Ensure that **csv** file radio button is selected under **Save As** section and select **30** seconds under **Split file every:** section (this option directly saves a new log file in the specified location for every 30 seconds), leave all the other settings as default and click **OK**.



51. We can see that the csv log file is created in **Desktop -> log_diagnosis** location.



52. This concludes the demonstration of detecting ARP poisoning using the Capsa Network Analyzer.

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