

# 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 snuffed 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 Omnipacket 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

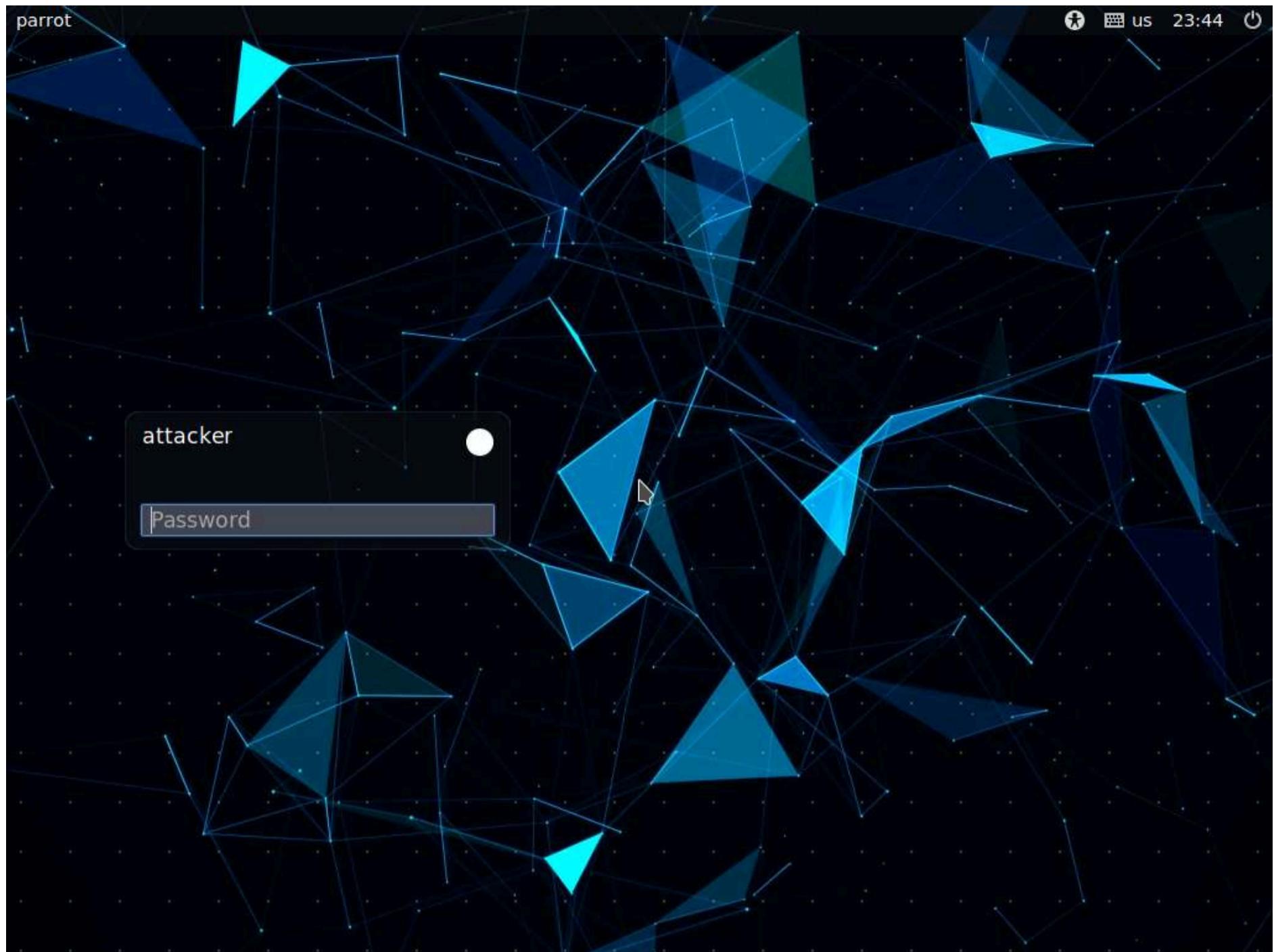
MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

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.

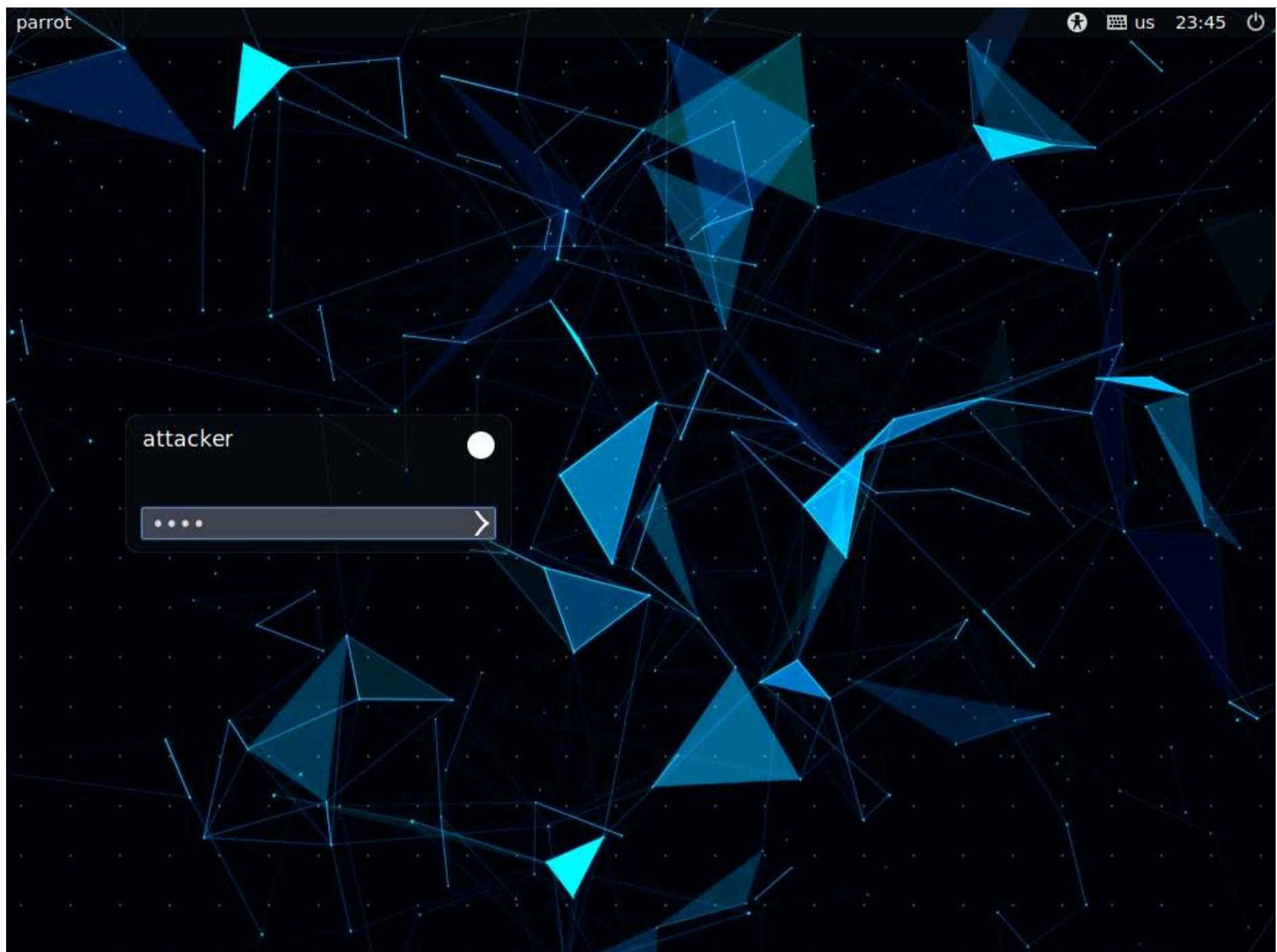


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

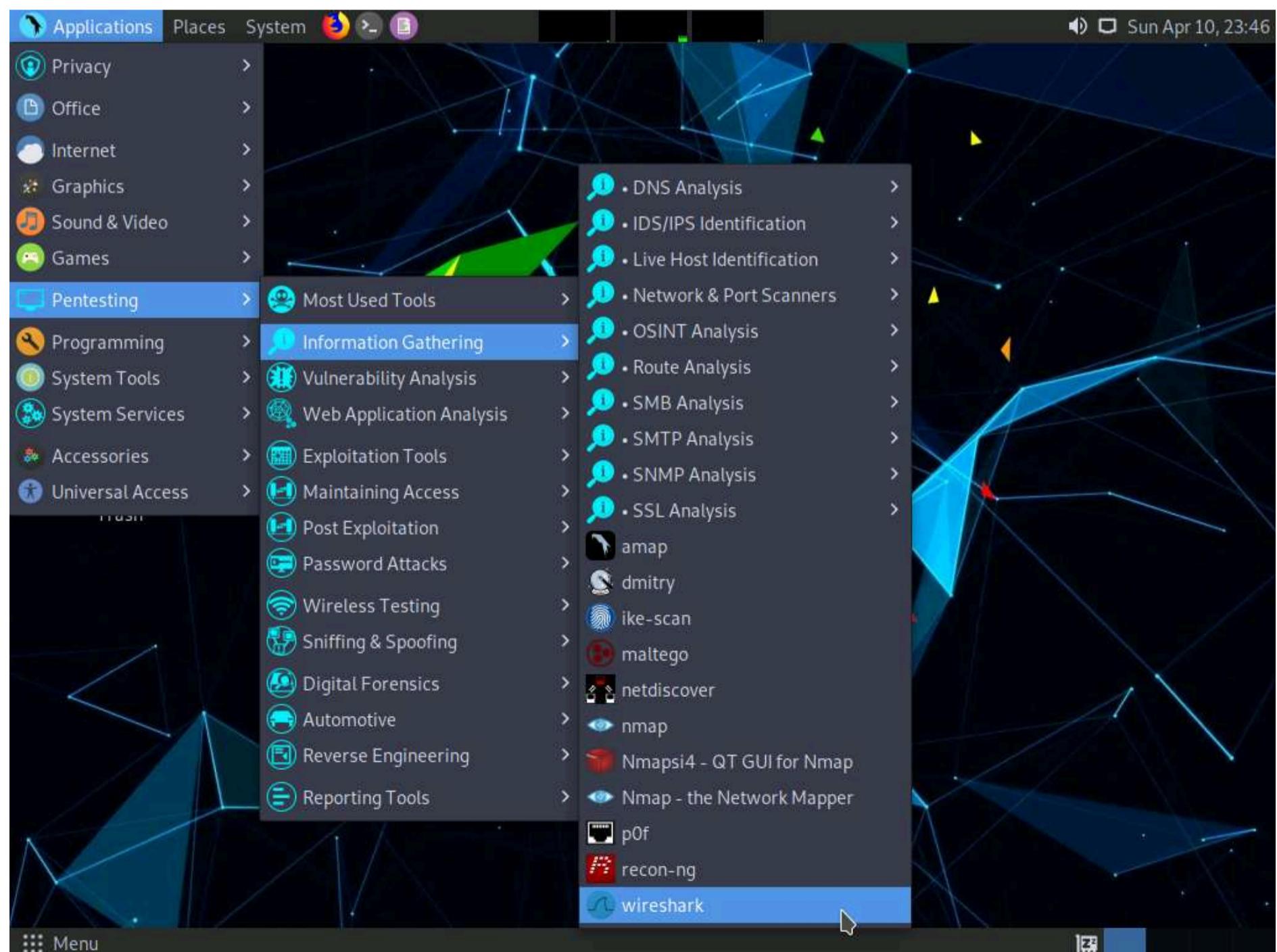
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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

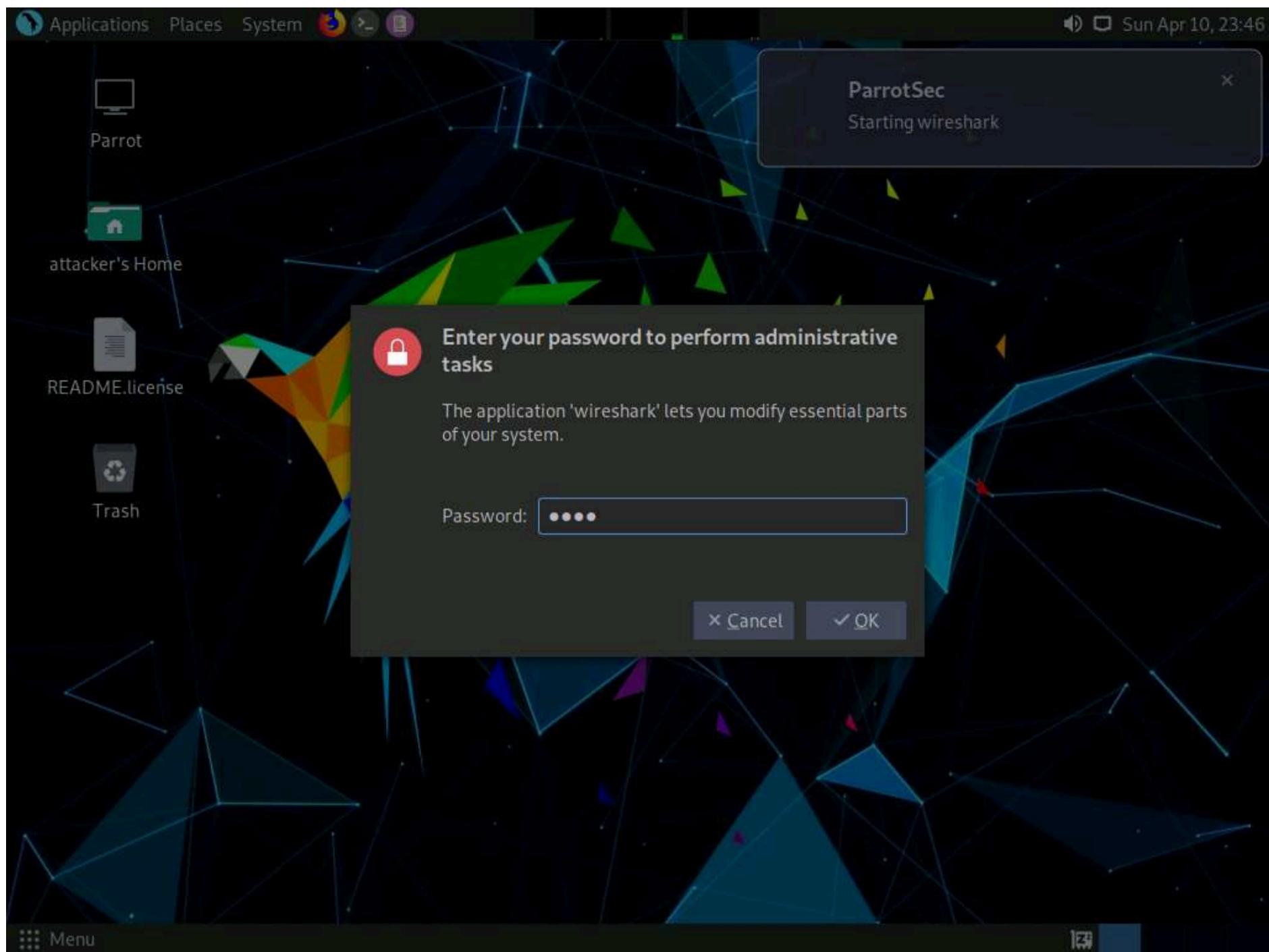




3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



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

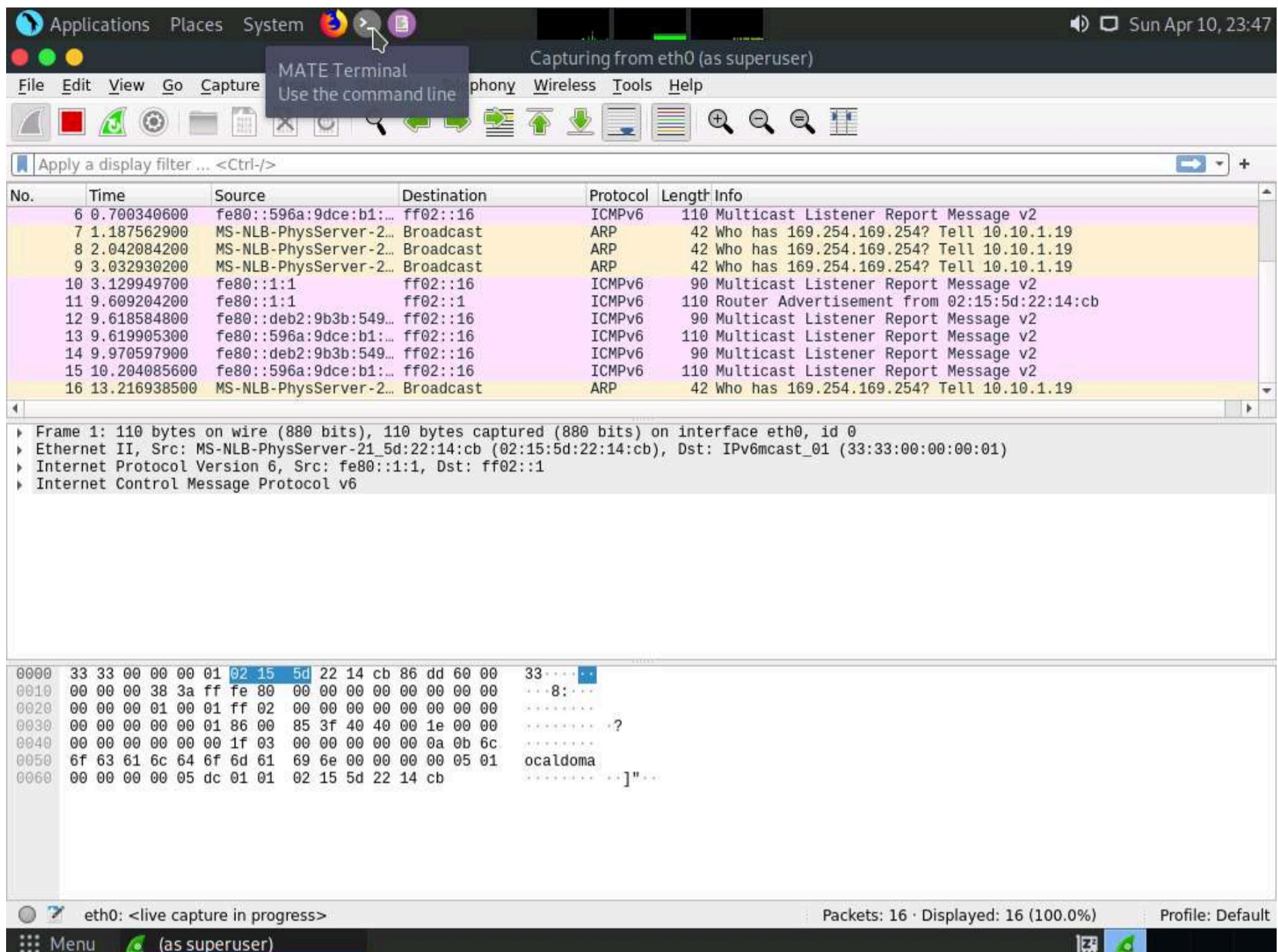


5. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

The screenshot shows the Wireshark Network Analyzer window titled "The Wireshark Network Analyzer (as superuser)". The window includes a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A search bar at the top right contains the text "Apply a display filter ... <Ctrl-/>". The main area is titled "Welcome to Wireshark" and "Capture". It features a list of available interfaces: "eth0", "any", "Loopback: lo", "bluetooth-monitor", "nflog", "nfqueue", "dbus-system", "dbus-session", and several remote capture options like "Cisco remote capture: ciscodump", "DisplayPort AUX channel monitor capture: dpauxmon", etc. At the bottom, there is a "Learn" section with links to "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". The status bar at the bottom indicates "Ready to load or capture", "No Packets", "Profile: Default", and "(as superuser)".

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

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

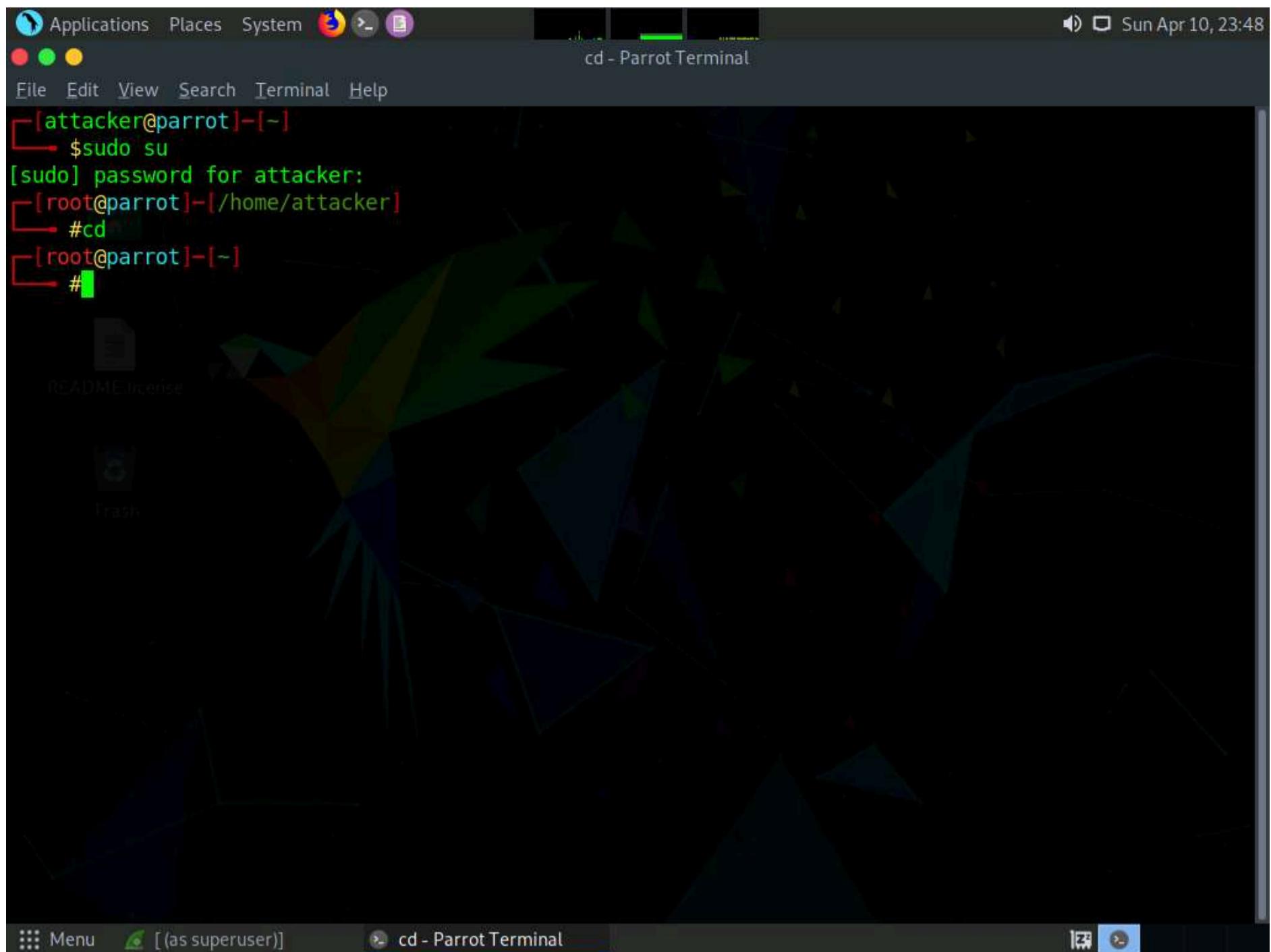


8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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.

The screenshot shows a terminal window titled "macof -i eth0 -n 10 - Parrot Terminal". The terminal session starts with the user switching to root using "sudo su". The password is entered, and the user navigates to their home directory with "#cd". They then run the command "#macof -i eth0 -n 10" which begins capturing traffic on interface eth0. The terminal displays numerous captured IPv4 packets, each with source and destination MAC addresses and IP addresses, along with protocol information like ICMPv6 or ICMPv4.

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

The screenshot shows the Wireshark application window titled "Capturing from eth0 (as superuser)". The main pane displays a list of network packets. The 125th packet is selected, highlighted in blue. This packet is an IPv4 packet from 30.26.58.73 to 61.78.35.96. The details pane at the bottom shows the packet structure, including the Ethernet II header, Internet Protocol Version 4 header, and the payload. The bytes pane shows the raw hex and ASCII data of the selected packet. The status bar at the bottom indicates "Packets: 206 · Displayed: 206 (100.0%) · Profile: Default".

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.

Frame 125: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0

Ethernet II, Src: db:8a:57:1e:fe:a5 (db:8a:57:1e:fe:a5), Dst: f9:2d:29:7a:ad:94 (f9:2d:29:7a:ad:94)

- Destination: f9:2d:29:7a:ad:94 (f9:2d:29:7a:ad:94)
- Source: db:8a:57:1e:fe:a5 (db:8a:57:1e:fe:a5)
- Type: IPv4 (0x0800)
- Trailer: f702b8925874e3870000000005002020009400000

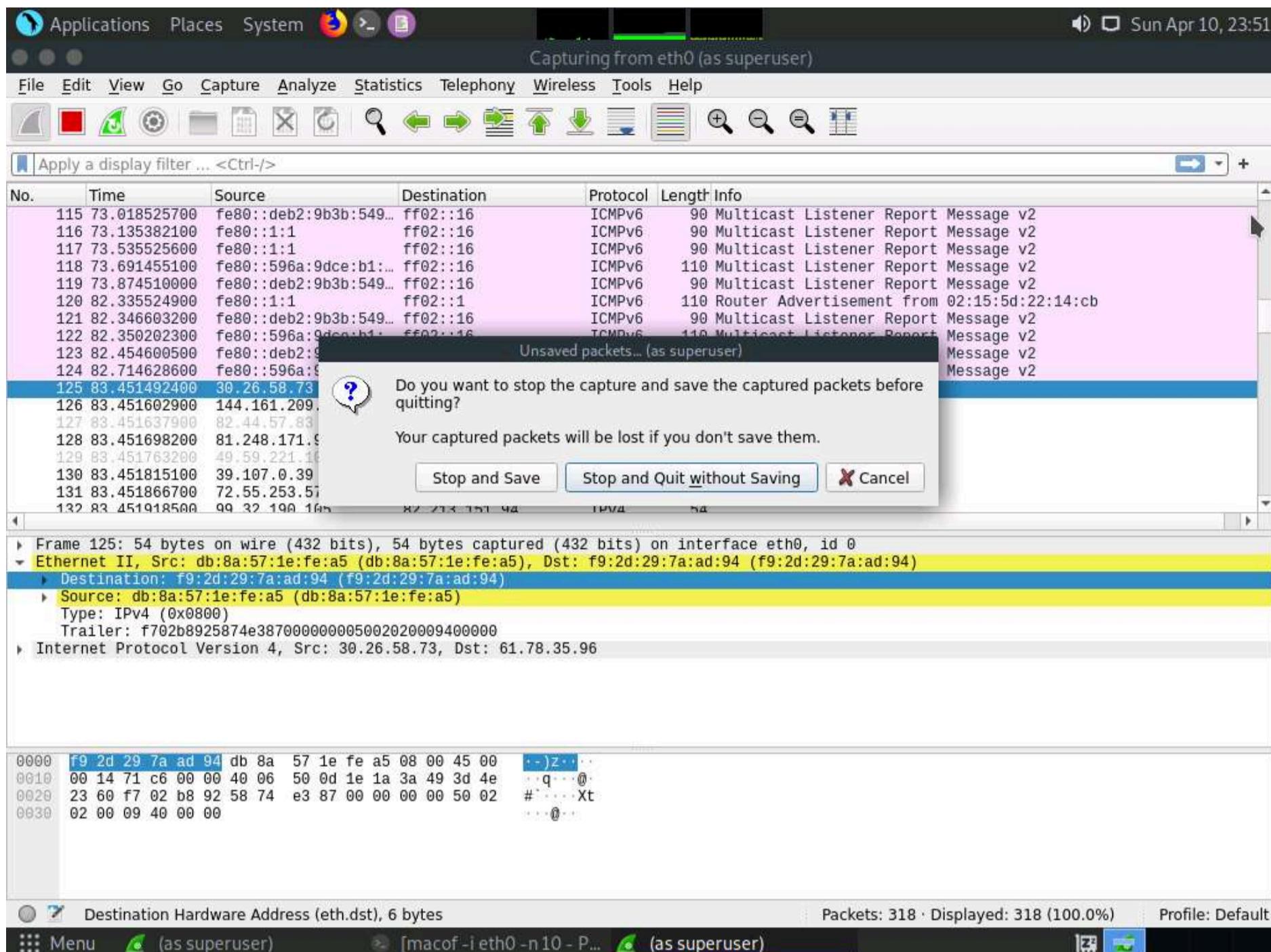
Internet Protocol Version 4, Src: 30.26.58.73, Dst: 61.78.35.96

No.	Time	Source	Destination	Protocol	Length	Info
115	73.018525700	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
116	73.135382100	fe80::1:1	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
117	73.535525600	fe80::1:1	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
118	73.691455100	fe80::596a:9dce:b1...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
119	73.874510000	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
120	82.335524900	fe80::1:1	ff02::1	ICMPv6	110	Router Advertisement from 02:15:5d:22:14:cb
121	82.346603200	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
122	82.350202300	fe80::596a:9dce:b1...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
123	82.454600500	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
124	82.714628600	fe80::596a:9dce:b1...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
125	83.451492400	30.26.58.73	61.78.35.96	IPv4	54	
126	83.451602900	144.161.209.52	188.213.124.25	IPv4	54	
127	83.451637900	82.44.57.83	23.69.223.99	IPv4	54	
128	83.451698200	81.248.171.95	102.110.194.4	IPv4	54	
129	83.451763200	49.59.221.107	231.139.153.4	IPv4	54	
130	83.451815100	39.107.0.39	48.228.150.39	IPv4	54	
131	83.451866700	72.55.253.57	169.88.221.110	IPv4	54	
132	83.451918500	99.32.190.105	82.213.151.94	IPv4	54	

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.

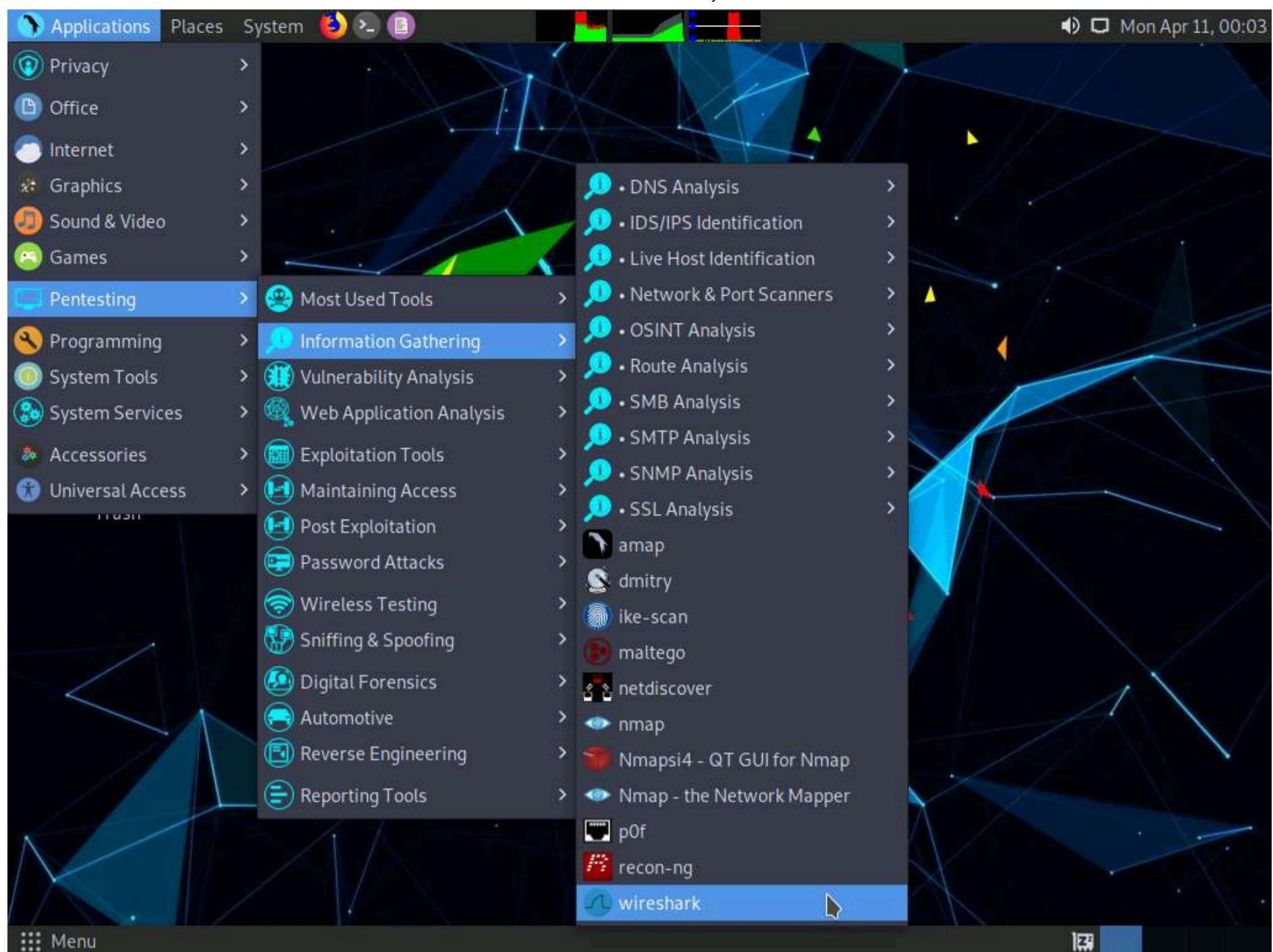
## Task 2: Perform a DHCP Starvation Attack using Yersinia

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.

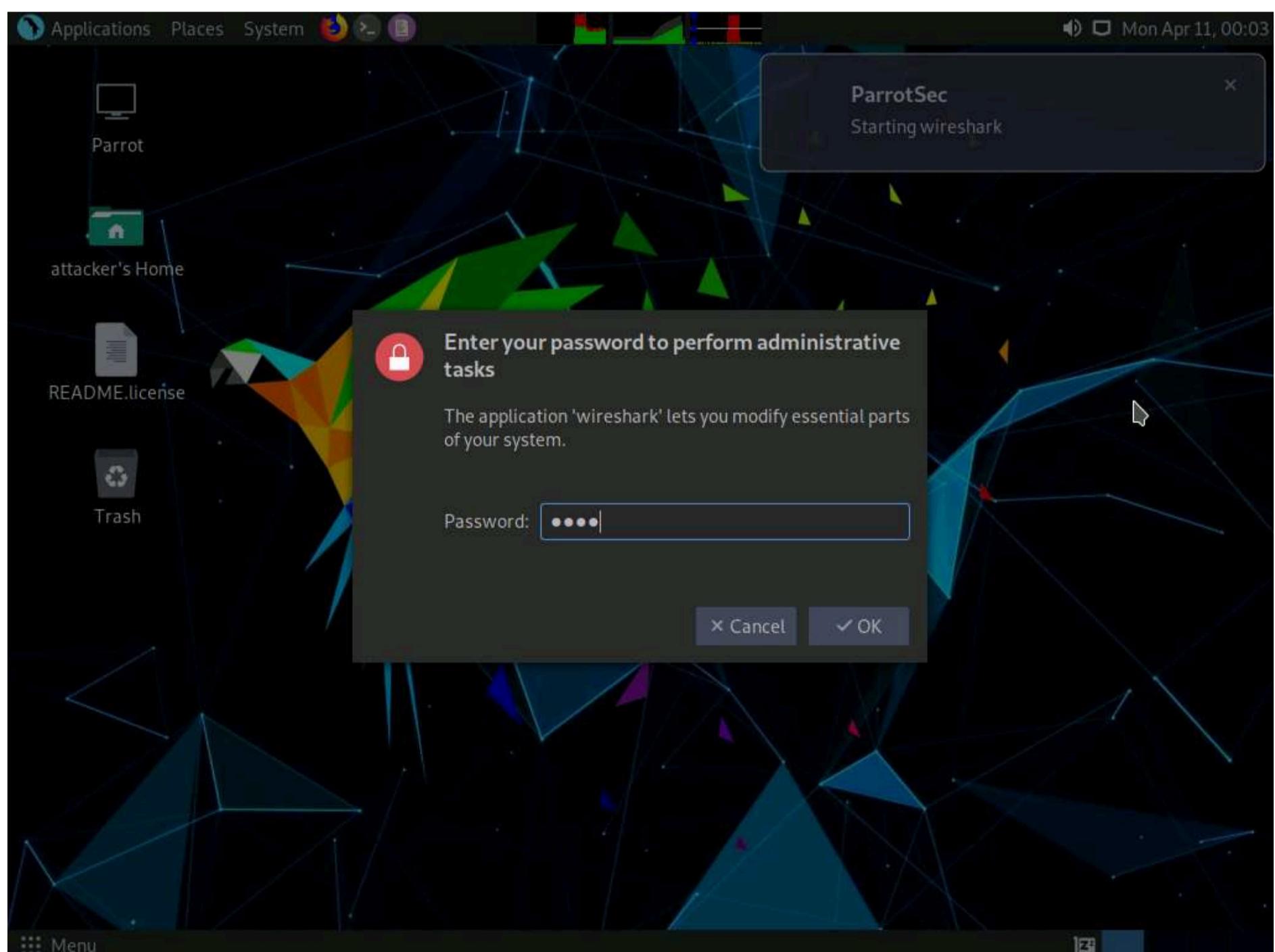
Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

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

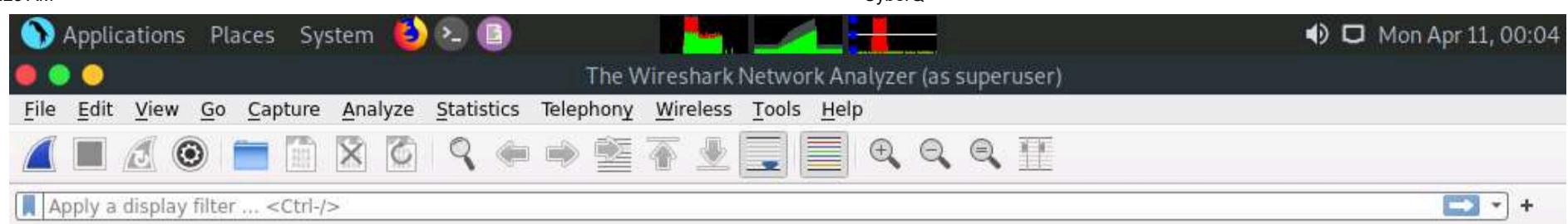
1. On the **Parrot Security** machine; click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting --> Information Gathering --> wireshark**.



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.



## Welcome to Wireshark

### Capture

...using this filter:  Enter a capture filter ...

All interfaces shown ▾

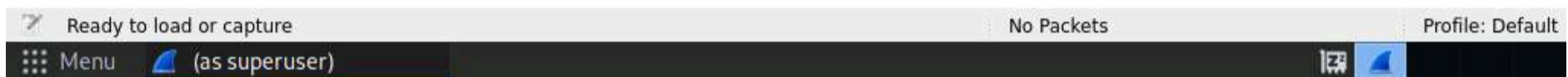
eth0

- any
- Loopback: lo
- bluetooth-monitor
- nflog
- nfqueue
- dbus-system
- dbus-session
- Cisco remote capture: ciscodump
- DisplayPort AUX channel monitor capture: dpauxmon
- Random packet generator: randpkt
- systemd Journal Export: sdjournal
- SSH remote capture: sshdump
- UDP Listener remote capture: udpdump

### Learn

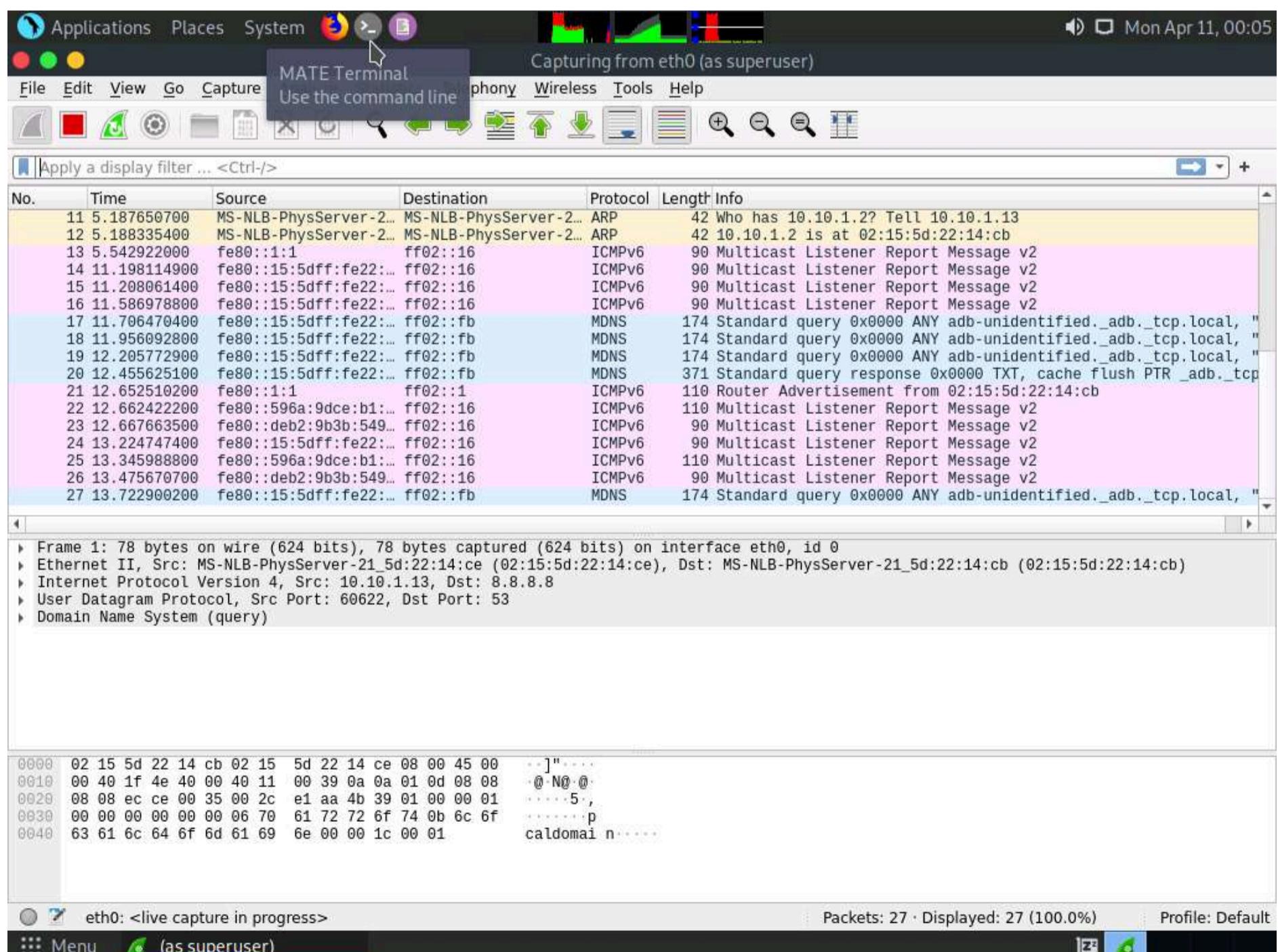
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.4.4 (Git v3.4.4 packaged as 3.4.4-1).



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.

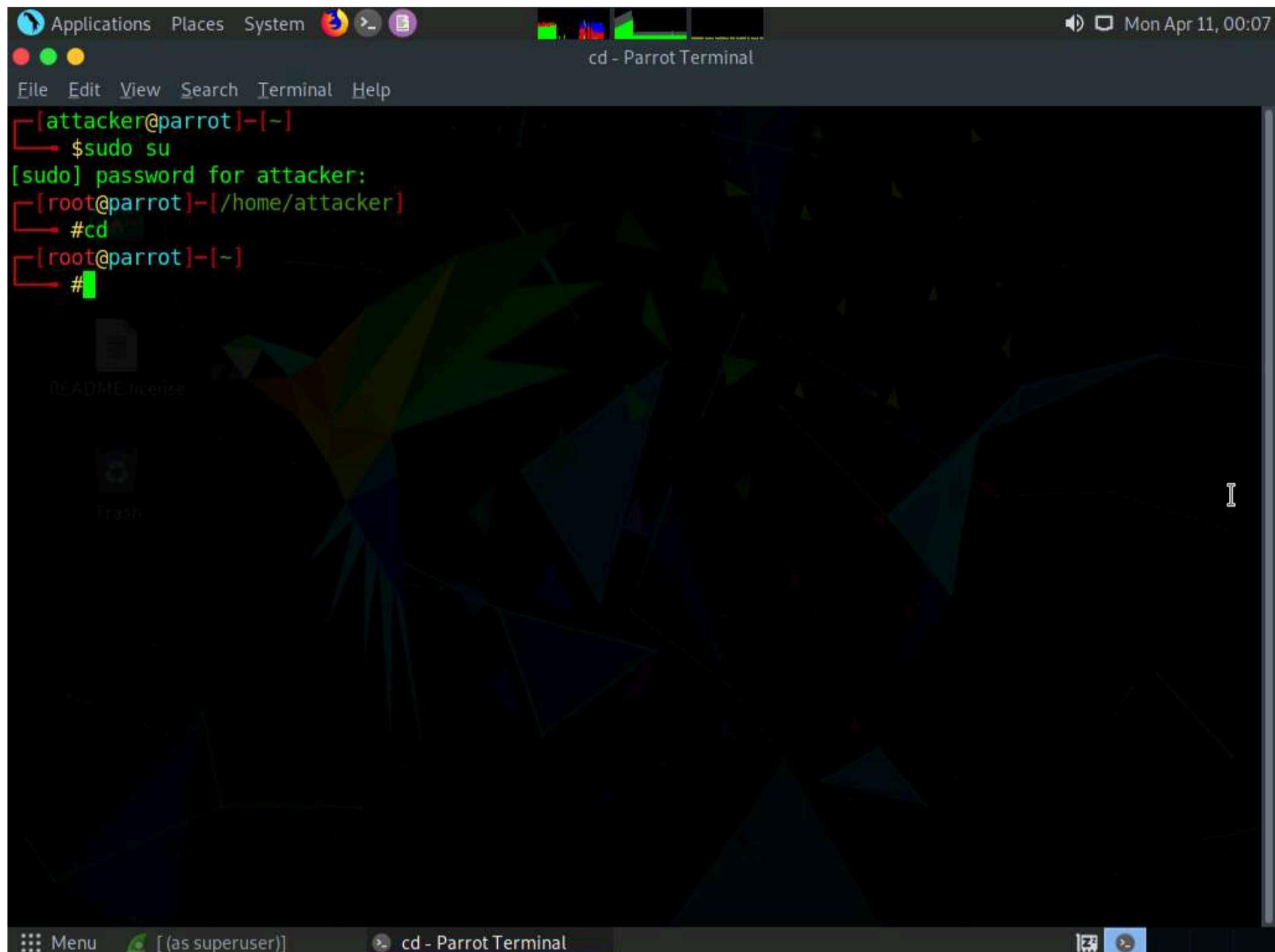
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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

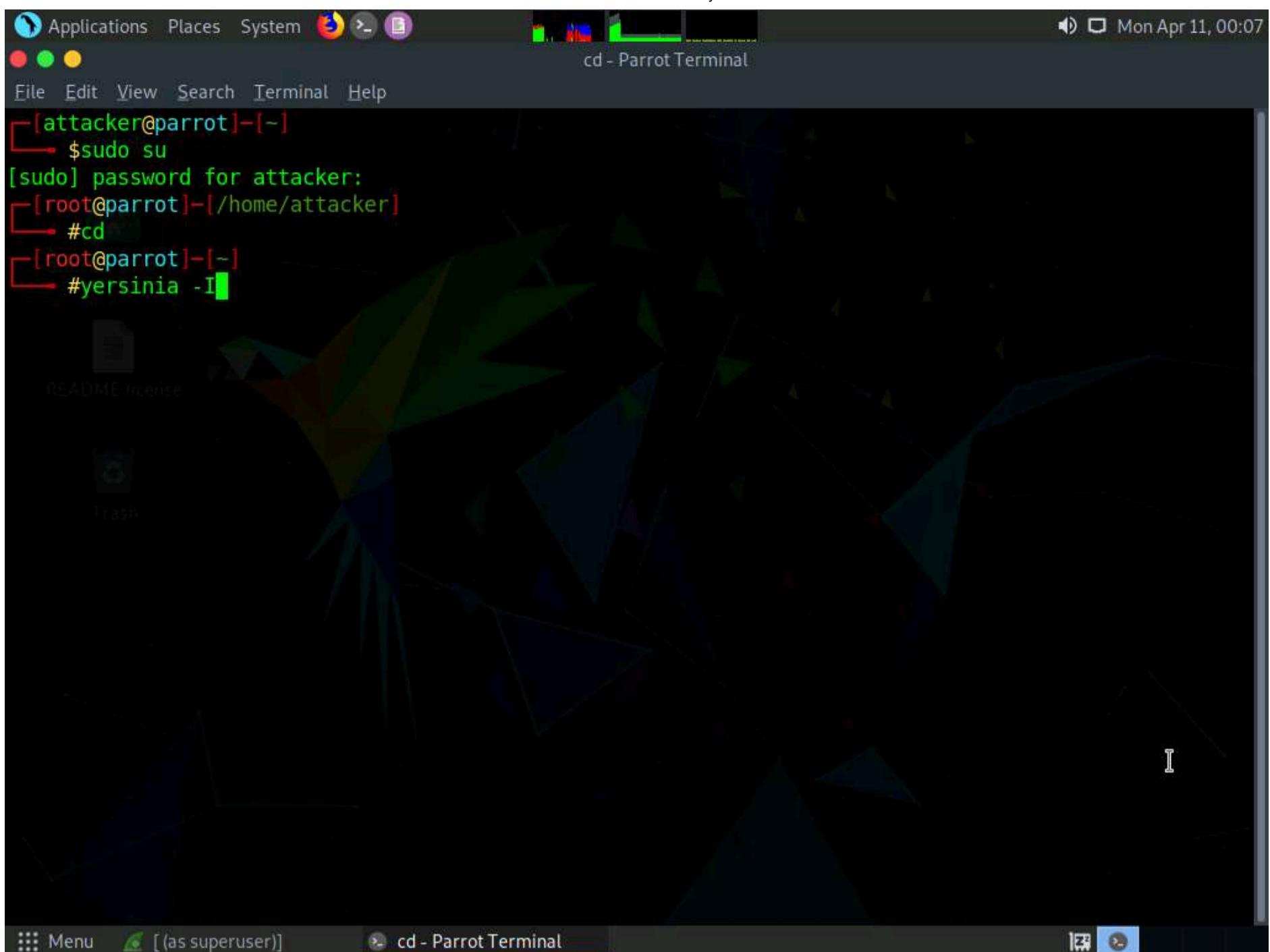
Note: Click the **Maximize Window** icon to maximize the terminal window.

Note: The interactive mode of the Yersinia application only works in a maximized terminal window.

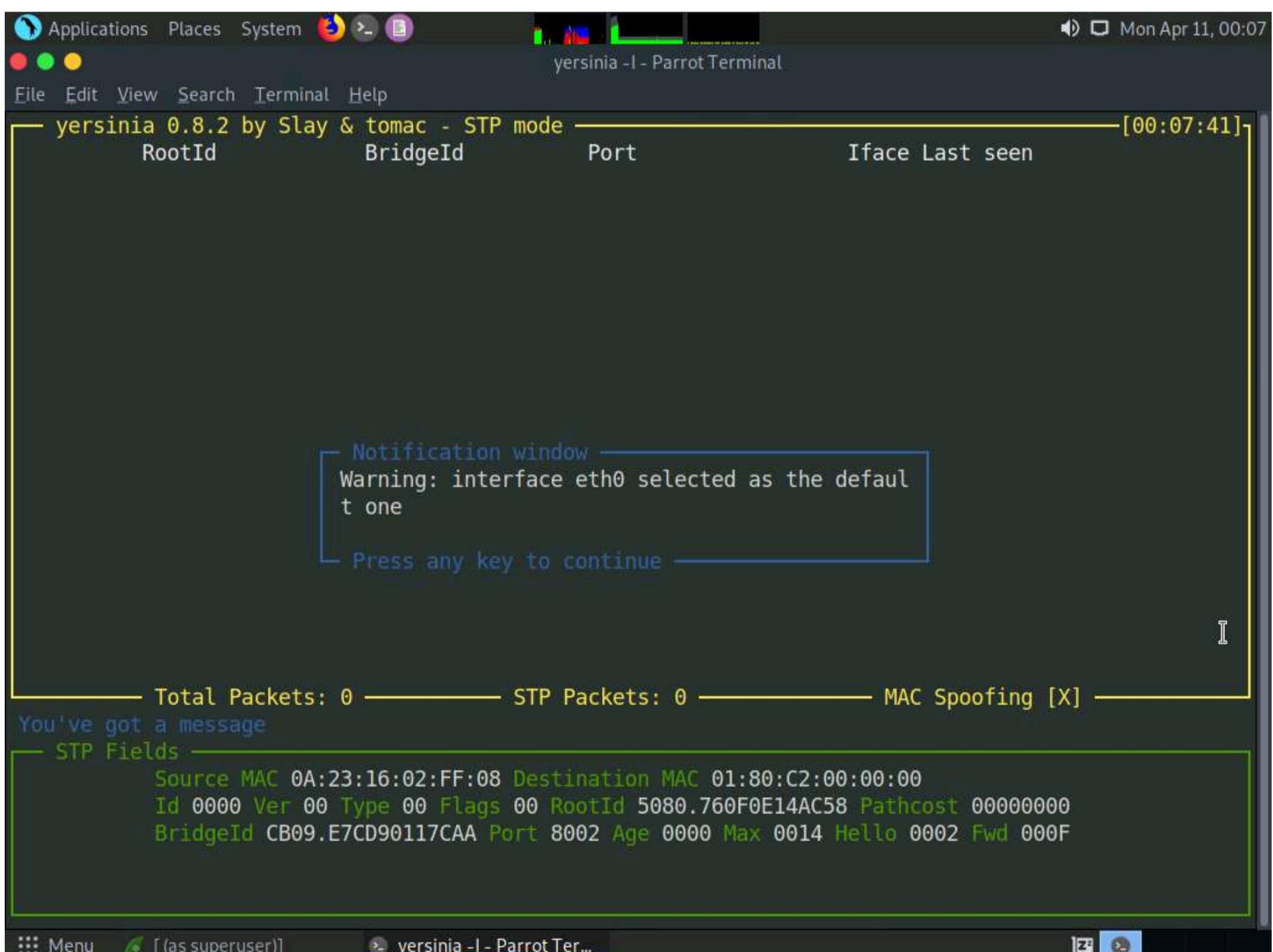


9. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.

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.

The screenshot shows a terminal window titled "yersinia -l - Parrot Terminal". The title bar also displays "CyberQ" and the date/time "Mon Apr 11, 00:08". The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". A status bar at the bottom shows "yersinia -l - Parrot Ter...". The main content of the terminal is the yersinia help screen:

```
yersinia 0.8.2 by Slay & tomac - STP mode [00:07:58]
RootId      BridgeId      Port      Iface Last seen
Total Packets: 0 -
This is the help screen.
STP Fields
  Source MAC 0A:23:1
  Id 0000 Ver 00 Typ
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
AC Spoofing [X] -
```

A large green box highlights the "Available commands" section, which lists various commands with their descriptions:

- h Help screen
- x eXecute attack
- i edit Interfaces
- ENTER information about selected item
- v View hex packet dump
- d load protocol Default values
- e Edit packet fields
- f list capture Files
- s Save packets from protocol
- S Save packets from all protocols
- L Learn packet from network
- M set Mac spoofing on/off
- L List running attacks
- K Kill all running attacks
- c Clear current protocol stats
- C Clear all protocols stats
- g Go to other protocol screen
- Ctrl-L redraw screen
- w Write configuration file
- a About this proggie
- q Quit (bring da noize)

At the bottom right of the terminal window, there is a small green box containing the text "00 hcost 00000000".

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.

File Edit View Search Terminal Help

yersinia 0.8.2 by Slay & tomac - DHCP mode [00:08:27]

SIP	DIP	MessageType	Iface	Last seen
-----	-----	-------------	-------	-----------

Total Packets: 0    DHCP Packets: 0    MAC Spoofing [X]

**DHCP Fields**

```
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
```

Menu [as superuser] yersinia -l - Parrot Ter... [x] [?] [x]

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

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

File Edit View Search Terminal Help

yersinia 0.8.2 by Slay & tomac - DHCP mode [00:08:36]

No	DoS	Description
0		sending RAW packet
1	X	sending DISCOVER packet
2		creating DHCP rogue server
3	X	sending RELEASE packet

Total Packets Select attack to launch ('q' to quit) Spoofing [X]

Those strange attacks...

**DHCP Fields**

```
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
```

Menu [as superuser] yersinia -l - Parrot Ter... [x] [?] [x]

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.



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

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

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

No.	Time	Source	Destination	Protocol	Length	Info
2265...	287.963104600	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963109600	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963114800	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963119800	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963124800	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963129900	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963135000	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963142900	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963148100	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963153100	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963158800	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963163900	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963168900	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963174000	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963179000	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963184000	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963189100	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963194200	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963199200	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963204200	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963209300	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963214300	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963219500	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963227400	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2265...	287.963237000	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0  
Ethernet II, Src: MS-NLB-PhysServer-21\_5d:22:14:ce (02:15:5d:22:14:ce), Dst: MS-NLB-PhysServer-21\_5d:22:14:cb (02:15:5d:22:14:cb)  
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 8.8.8.8  
User Datagram Protocol, Src Port: 60622, Dst Port: 53  
Domain Name System (query)

0000 02 15 5d 22 14 cb 02 15 5d 22 14 ce 08 00 45 00 ... ]"...
0010 00 40 1f 4e 40 00 40 11 00 39 0a 0a 01 0d 08 08 ... @·N@·@·
0020 08 08 ec ce 00 35 00 2c e1 aa 4b 39 01 00 00 01 ... 5 ,
0030 00 00 00 00 00 00 06 70 61 72 72 6f 74 0b 6c 6f ... .p
0040 63 61 6c 64 6f 6d 61 69 6e 00 00 1c 00 01 caldomai n....

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.



Capturing from eth0 (as superuser)

No. Time Source Destination Protocol Length Info

2899...	292.849653700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849659400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849665000 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849670900 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849676800 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849682800 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849688300 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849693800 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849699100 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849704700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849710000 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849715300 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849720500 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849725900 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849731100 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849736400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849741700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849747200 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849752400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849757700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849762900 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849768200 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849773600 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849779000 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849784400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

Frame 2899280: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth0, id 0

Ethernet II, Src: dd:13:a2:33:ac:c7 (dd:13:a2:33:ac:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: dd:13:a2:33:ac:c7 (dd:13:a2:33:ac:c7)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff dd 13 a2 33 ac c7 08 00 45 10 .....  
0010 01 10 00 00 00 00 10 11 a9 ce 00 00 00 00 ff ff .....

Packets: 2899449 · Displayed: 2899449 (100.0%) · Profile: Default

eth0: <live capture in progress>

Menu (as superuser) yersinia -l - Parrot Ter...

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

Capturing from eth0 (as superuser)

No. Time Source Destination Protocol Length Info

2899...	292.849653700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849659400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849665000 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849670900 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849676800 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849682800 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849688300 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849693800 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849699100 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849704700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849710000 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849715300 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849720500 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849725900 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849731100 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849736400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849741700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849747200 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849752400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849757700 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849762900 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849768200 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849773600 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849779000 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
2899...	292.849784400 0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

Frame 2899280: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth0, id 0

Ethernet II, Src: dd:13:a2:33:ac:c7 (dd:13:a2:33:ac:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: dd:13:a2:33:ac:c7 (dd:13:a2:33:ac:c7)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff dd 13 a2 33 ac c7 08 00 45 10 .....  
0010 01 10 00 00 00 00 10 11 a9 ce 00 00 00 00 ff ff .....

Packets: 2899529 · Displayed: 2899529 (100.0%) · Profile: Default

eth0: <live capture in progress>

Menu (as superuser) yersinia -l - Parrot Ter... (as superuser)

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

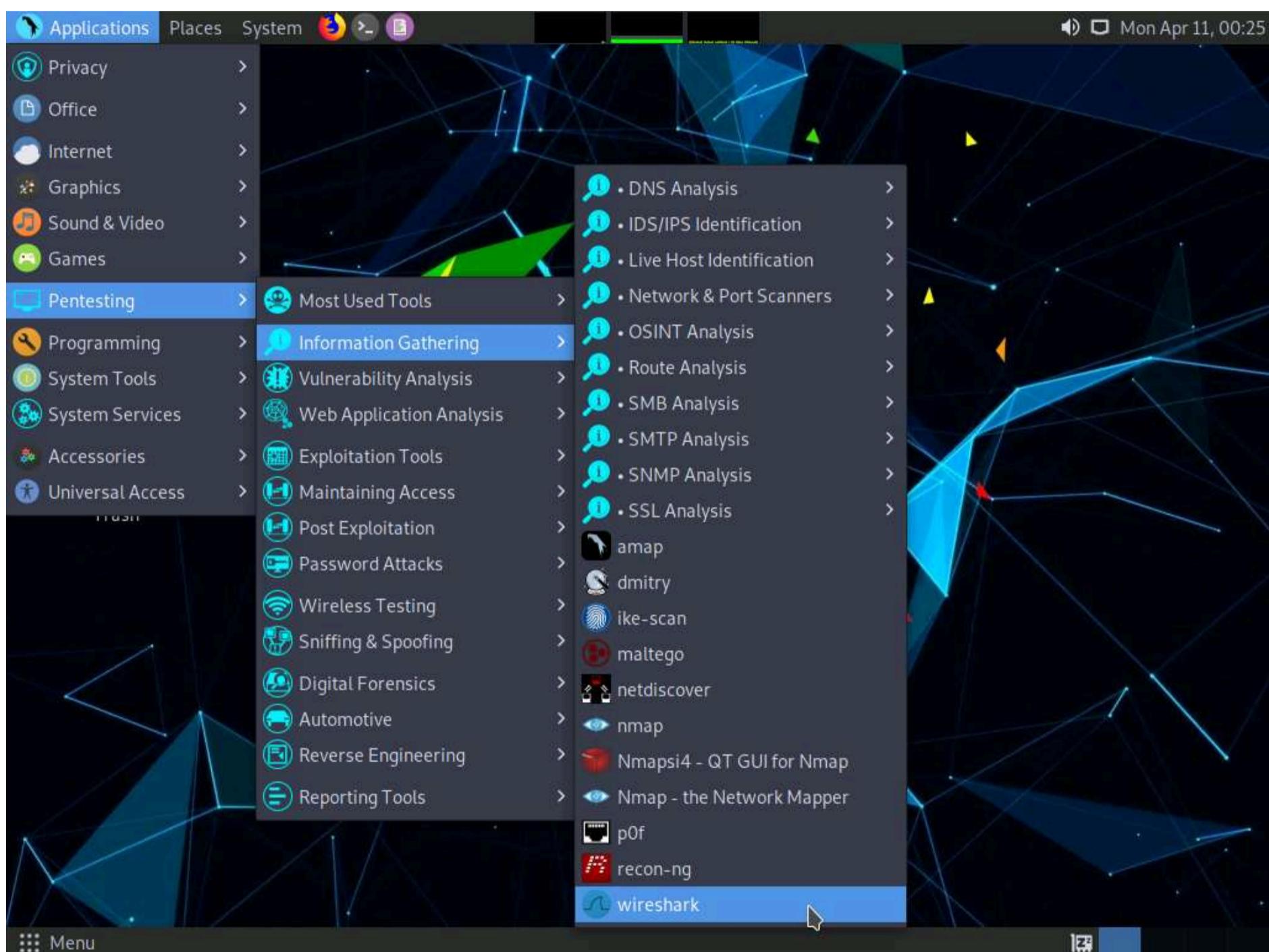
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the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

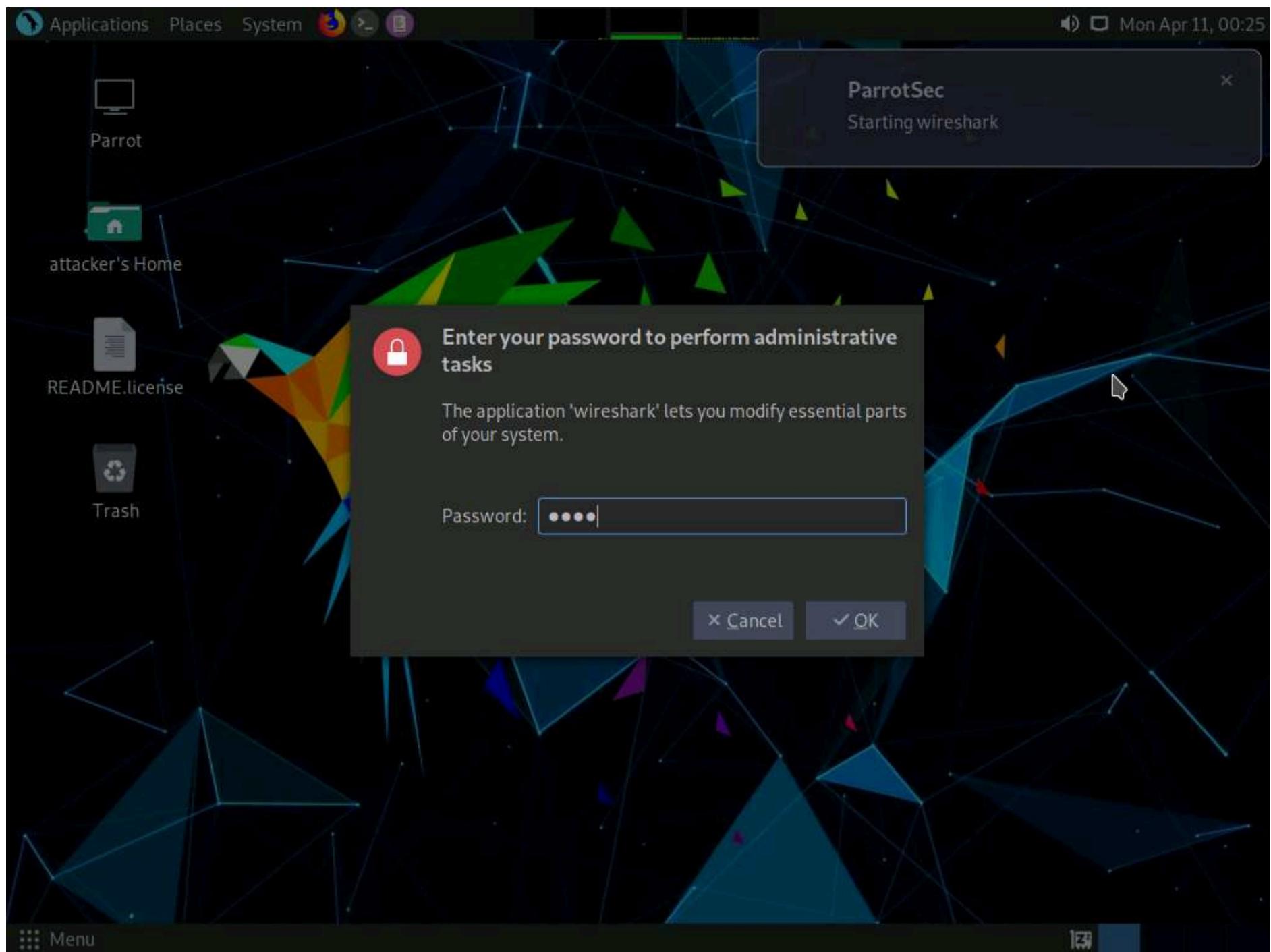
Here, we will use the arpspoof tool to perform ARP poisoning.

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**.

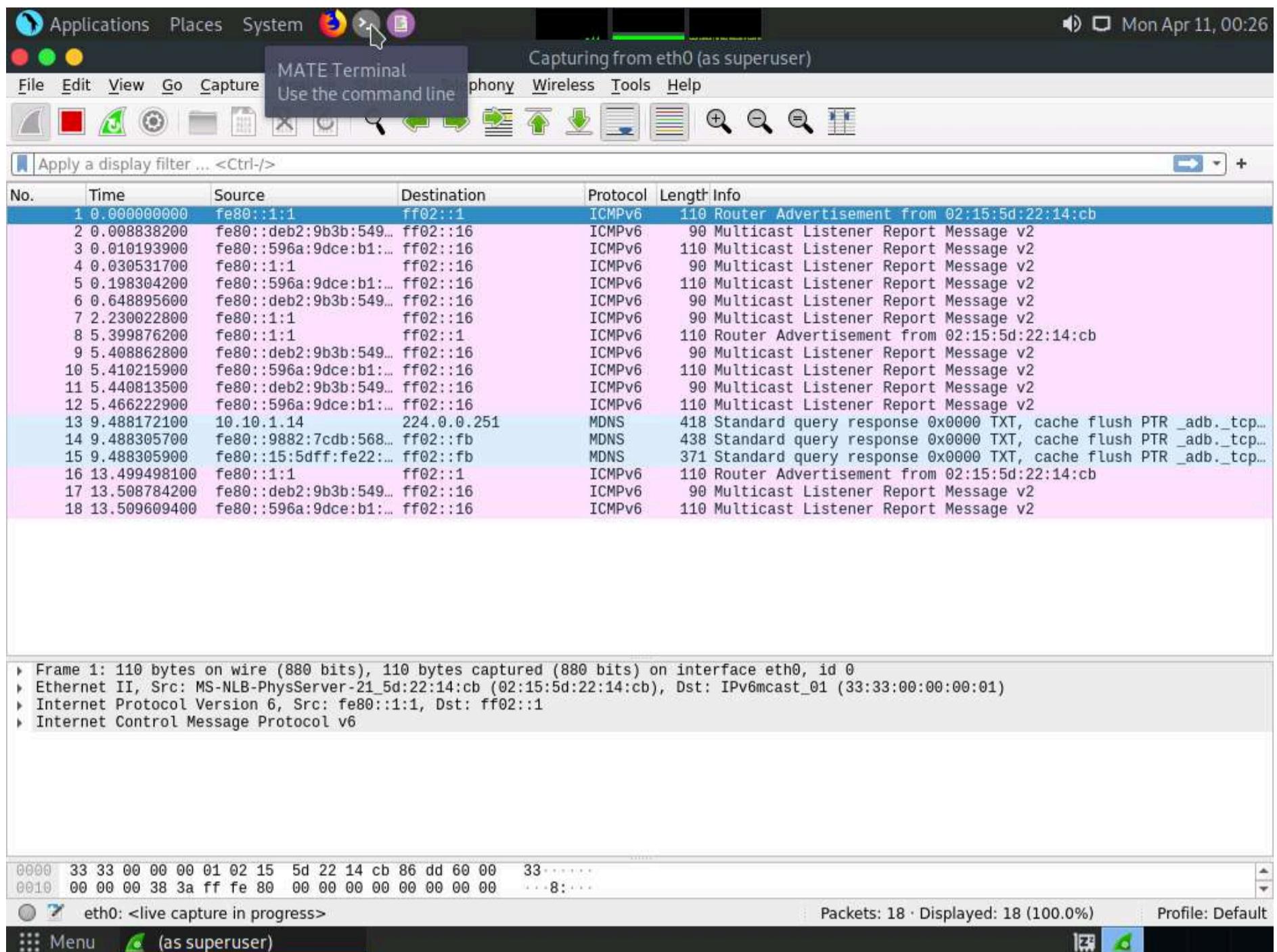


3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

The screenshot shows the Wireshark Network Analyzer window titled "The Wireshark Network Analyzer (as superuser)". The window includes a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A search bar at the top right contains the text "Apply a display filter ... <Ctrl-/>". The main area is titled "Welcome to Wireshark" and "Capture". It features a dropdown menu for filters with the placeholder "Enter a capture filter ...". Another dropdown menu shows "All interfaces shown". A list of available interfaces is displayed, with "eth0" selected and highlighted in blue. Other listed interfaces include any, Loopback: lo, bluetooth-monitor, nflog, nfqueue, dbus-system, dbus-session, Cisco remote capture: ciscodump, DisplayPort AUX channel monitor capture: dpauxmon, Random packet generator: randpkt, systemd Journal Export: sdjournal, SSH remote capture: sshdump, and UDP Listener remote capture: udpdump. At the bottom of the window, there is a "Learn" section with links to User's Guide, Wiki, Questions and Answers, and Mailing Lists. The status bar at the bottom indicates "Ready to load or capture", "No Packets", "Profile: Default", and "(as superuser)".

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

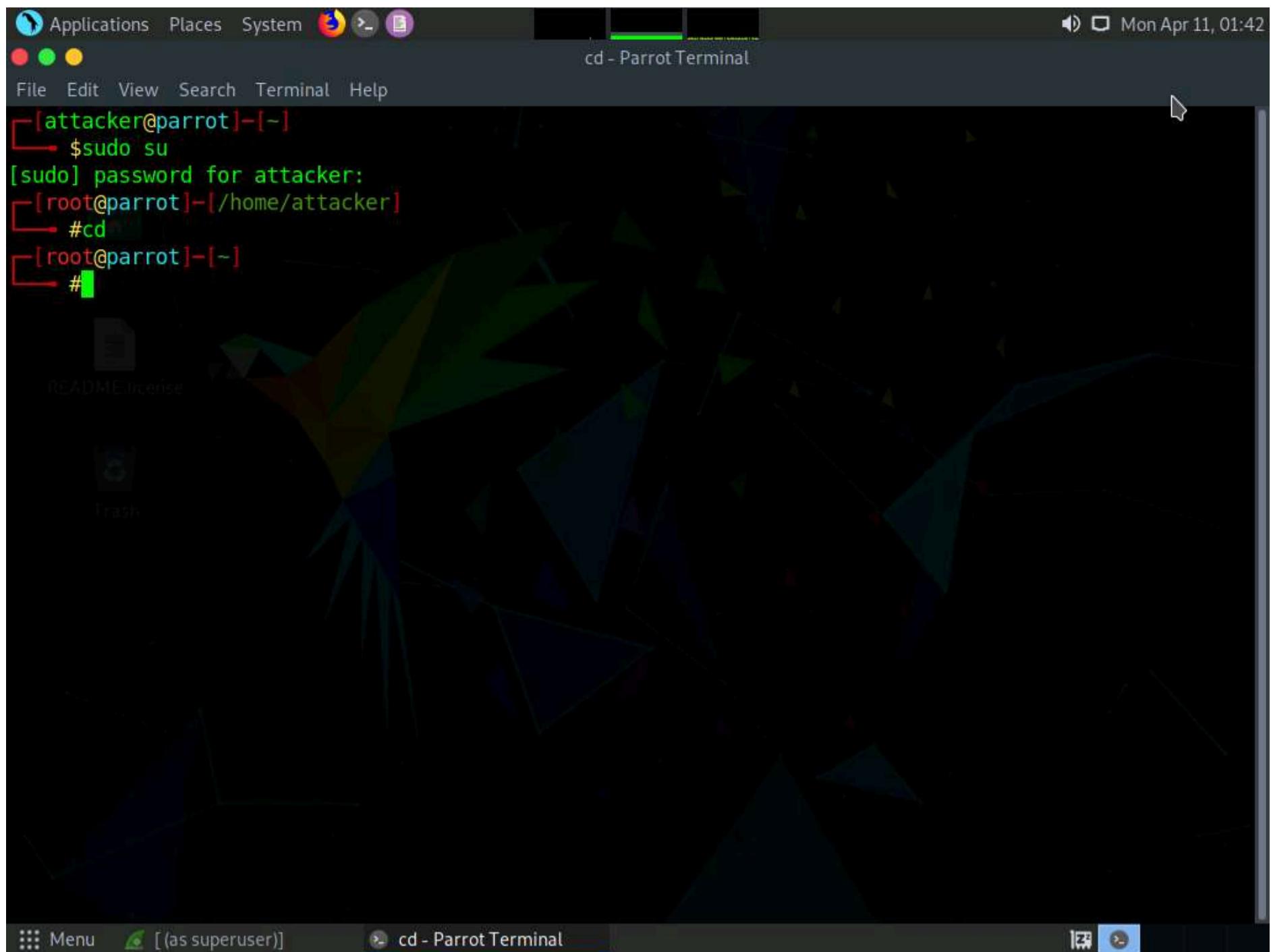
5. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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 **arp spoof -i eth0 -t 10.10.1.1 10.10.1.11** and press **Enter**.

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

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

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.

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

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

No.	Time	Source	Destination	Protocol	Length	Info
6775	4680.4092098...	fe80::1:1	ff02::1	ICMPv6	110	Router Advertisement from 02:15:5d:22:14:cb
6776	4680.4180880...	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6777	4680.4247700...	fe80::596a:9dce:b1...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
6778	4680.9250811...	fe80::596a:9dce:b1...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
6779	4681.0061033...	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6780	4683.0948938...	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.1? Tell 10.10.1.13
6781	4684.0945387...	MS-NLB-PhysServer-2...	00:00:00_00:00:00	ARP	42	10.10.1.11 is at 02:15:5d:22:14:ce (duplicate use of 10.10.1...
6782	4684.1101274...	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.1? Tell 10.10.1.13
6783	4685.1341094...	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.1? Tell 10.10.1.13
6784	4685.9721045...	fe80::15:5dff:fe22...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6785	4685.9794606...	fe80::15:5dff:fe22...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6786	4686.0947104...	MS-NLB-PhysServer-2...	00:00:00_00:00:00	ARP	42	10.10.1.11 is at 02:15:5d:22:14:ce (duplicate use of 10.10.1...
6787	4686.3715881...	fe80::15:5dff:fe22...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6788	4686.4767742...	fe80::15:5dff:fe22...	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "
6789	4686.7265559...	fe80::15:5dff:fe22...	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "
6790	4686.9772763...	fe80::15:5dff:fe22...	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "
6791	4687.2290890...	fe80::15:5dff:fe22...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp
6792	4687.9977501...	fe80::15:5dff:fe22...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6793	4688.0949087...	MS-NLB-PhysServer-2...	00:00:00_00:00:00	ARP	42	10.10.1.11 is at 02:15:5d:22:14:ce (duplicate use of 10.10.1...
6794	4688.1777121...	fe80::15:5dff:fe22...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6795	4688.4951958...	fe80::15:5dff:fe22...	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "
6796	4688.7452714...	fe80::15:5dff:fe22...	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "
6797	4688.9963831...	fe80::15:5dff:fe22...	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "
6798	4689.2452485...	fe80::15:5dff:fe22...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp
6799	4689.7878940...	fe80::1:1	ff02::1	ICMPv6	110	Router Advertisement from 02:15:5d:22:14:cb

Frame 6783: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21\_5d:22:14:ce (02:15:5d:22:14:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 02 15 5d 22 14 ce 08 06 00 01 .....
0010 08 00 06 04 00 01 02 15 5d 22 14 ce 0a 0a 01 0d .....
eth0: <live capture in progress>

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.



Wireshark screenshot showing network traffic capture from eth0. The packet list displays various types of network traffic, including DNS (MDNS), ICMPv6, and ARP. A yellow highlight box on the right side of the interface details pane indicates a 'Duplicate IP address detected for 10.10.1.11 (02:15:5d:22:14:ce) - also in use by 00:15:5d:01:80:00 (frame 6239)'.

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.

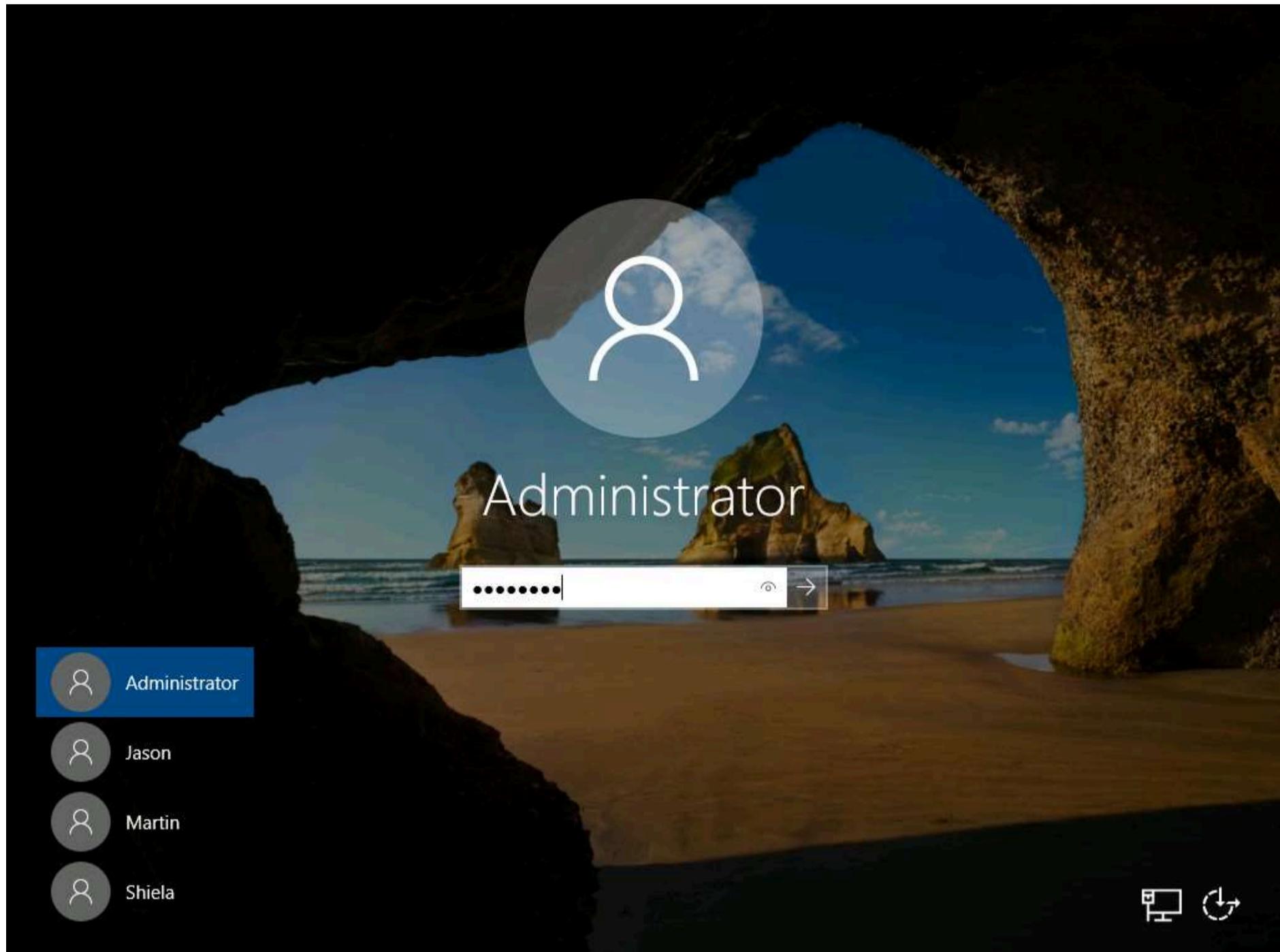
MITM attacks are varied and can be carried out on a switched LAN. MITM attacks can be performed using various tools such as Cain & Abel.

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.

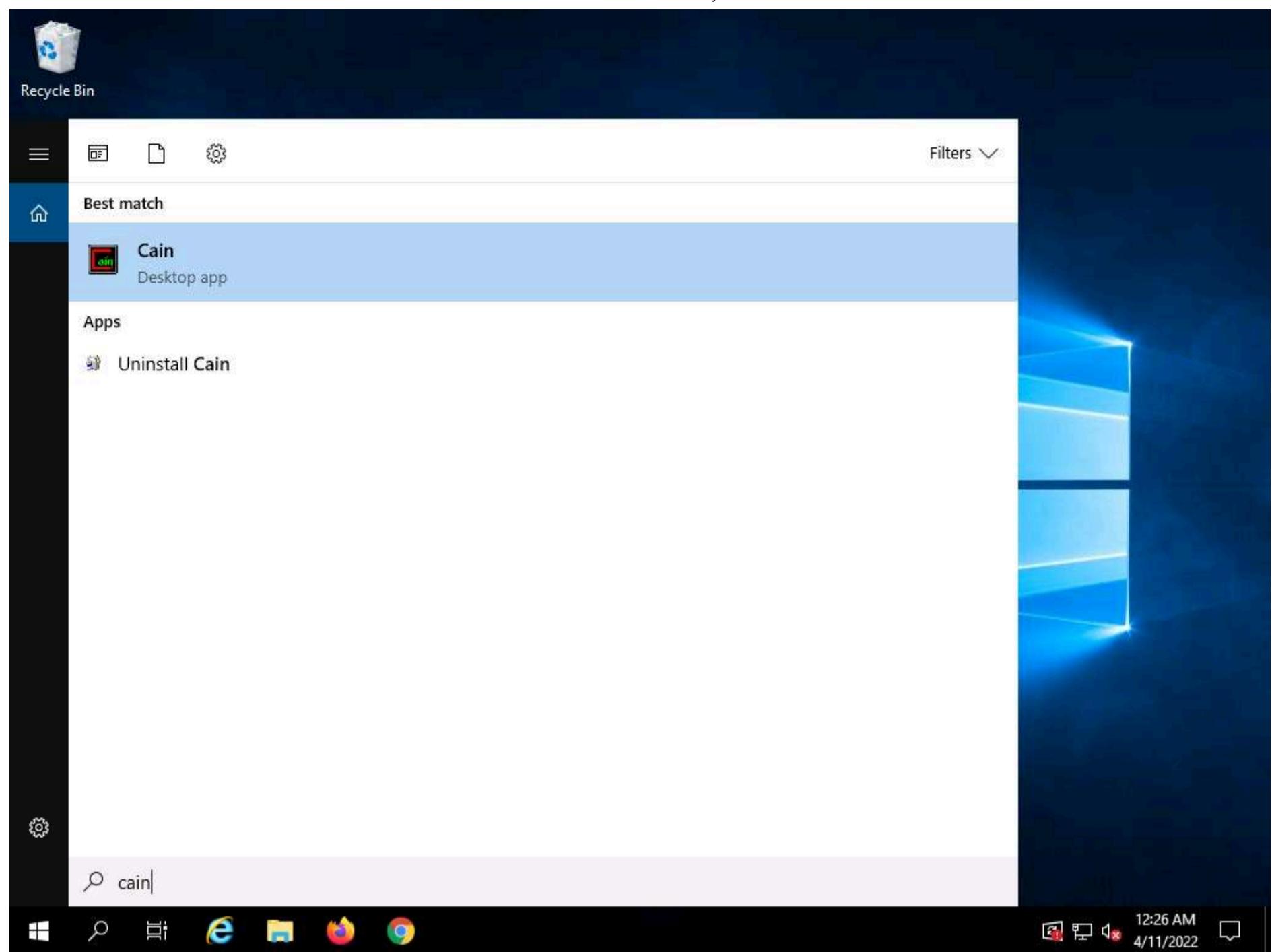
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

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

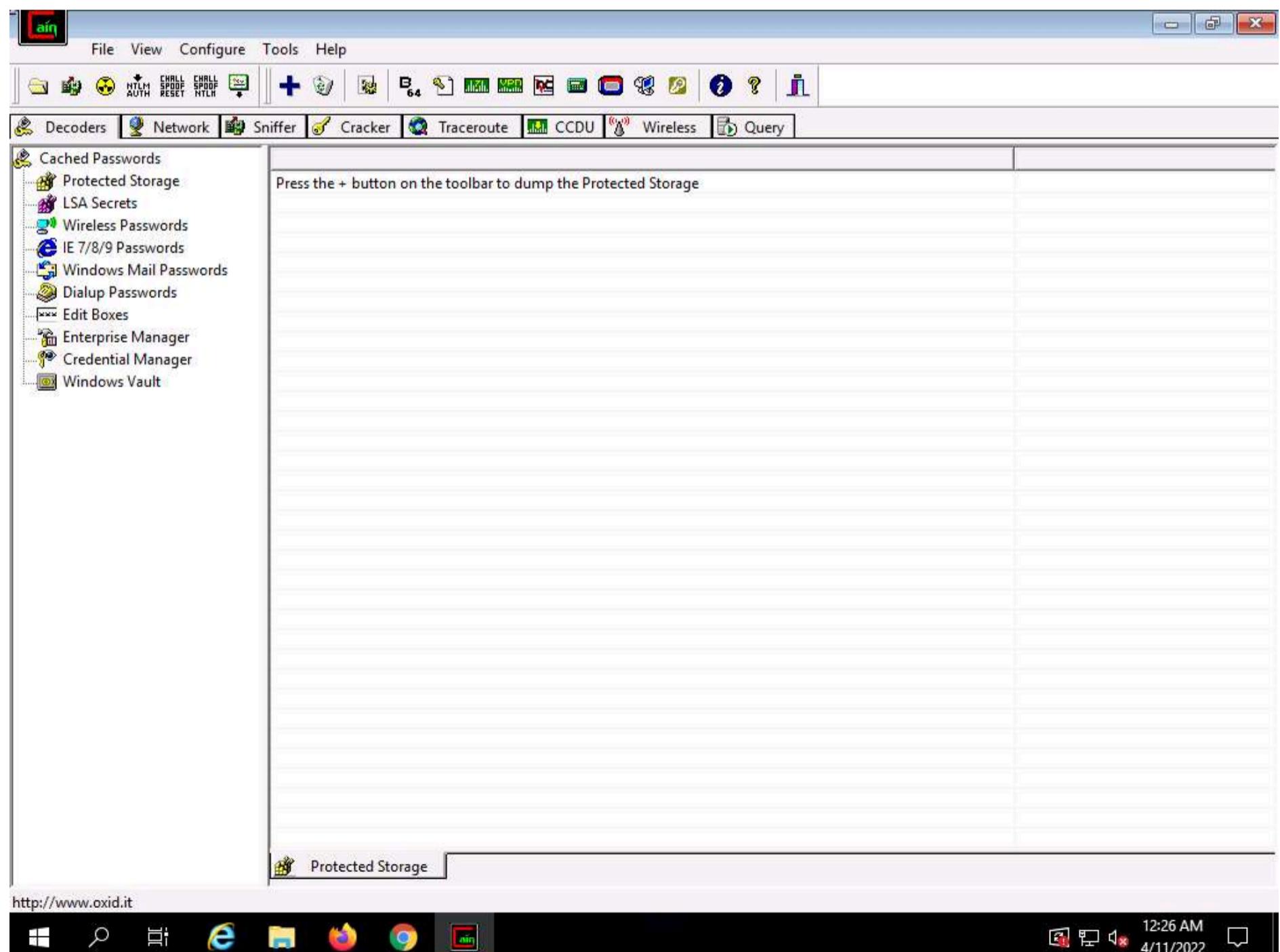


3. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



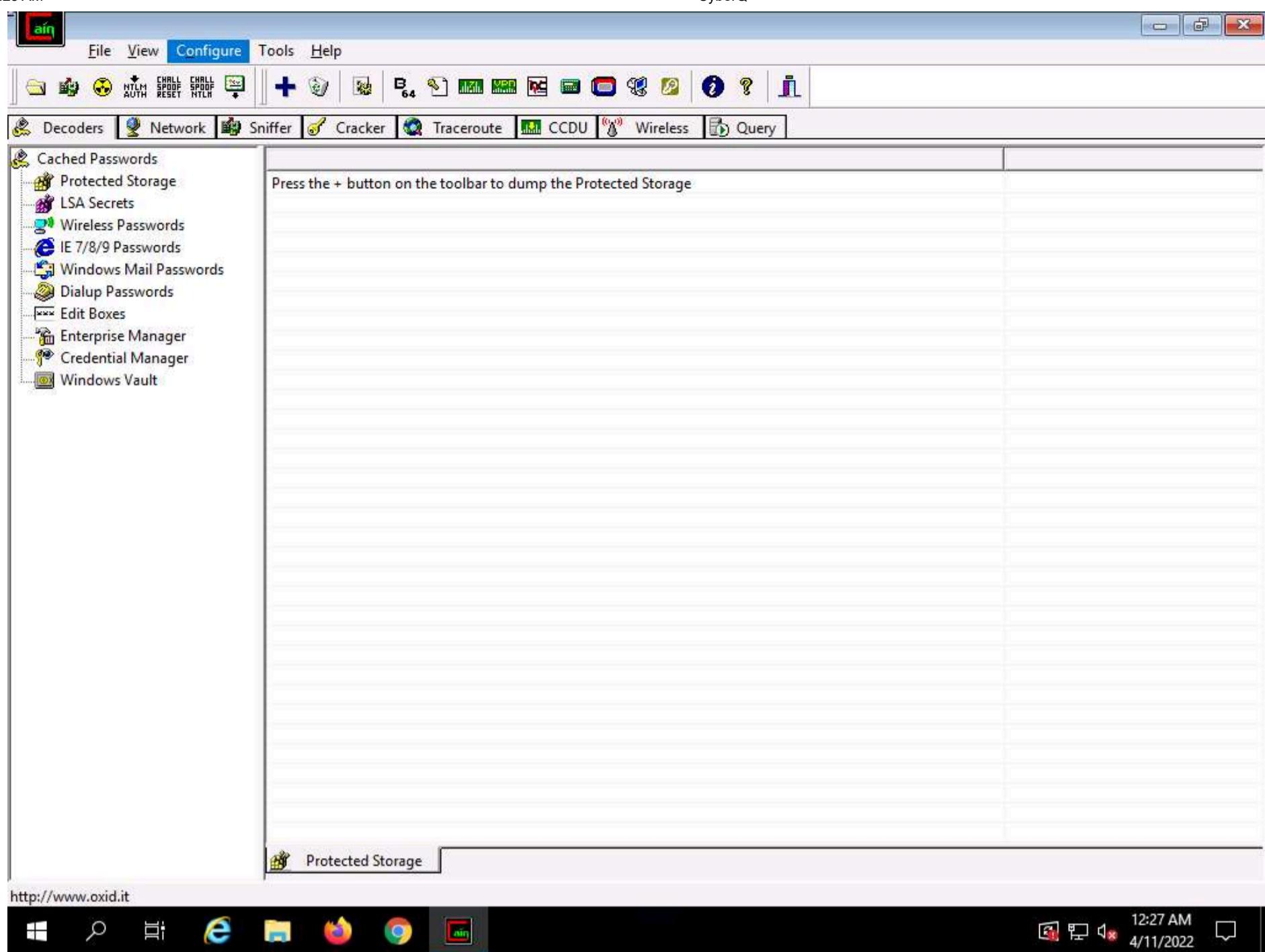


4. The **Cain & Abel** main window appears, as shown in the screenshot.

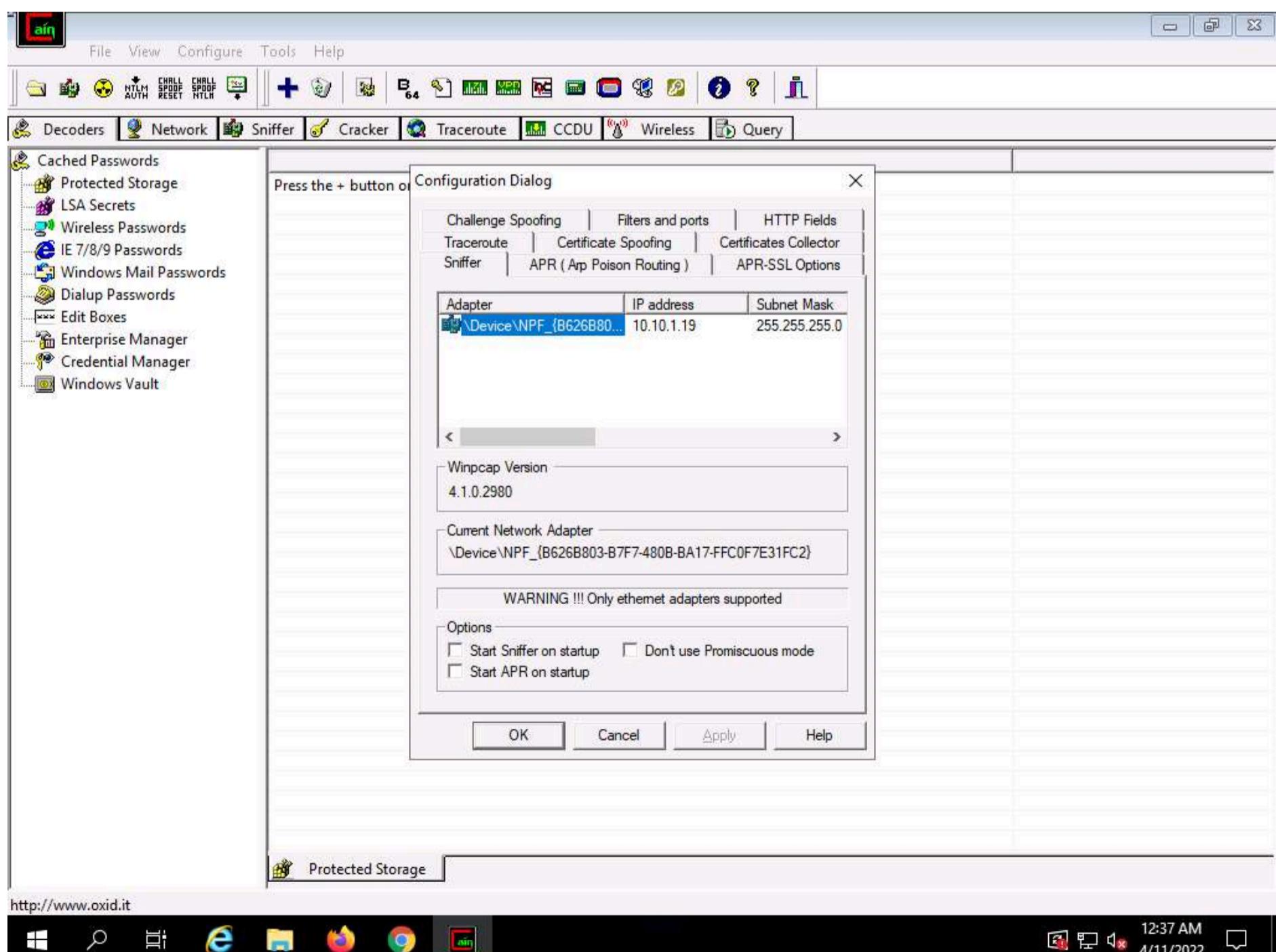


5. Click **Configure** from the menu bar to configure an ethernet card.



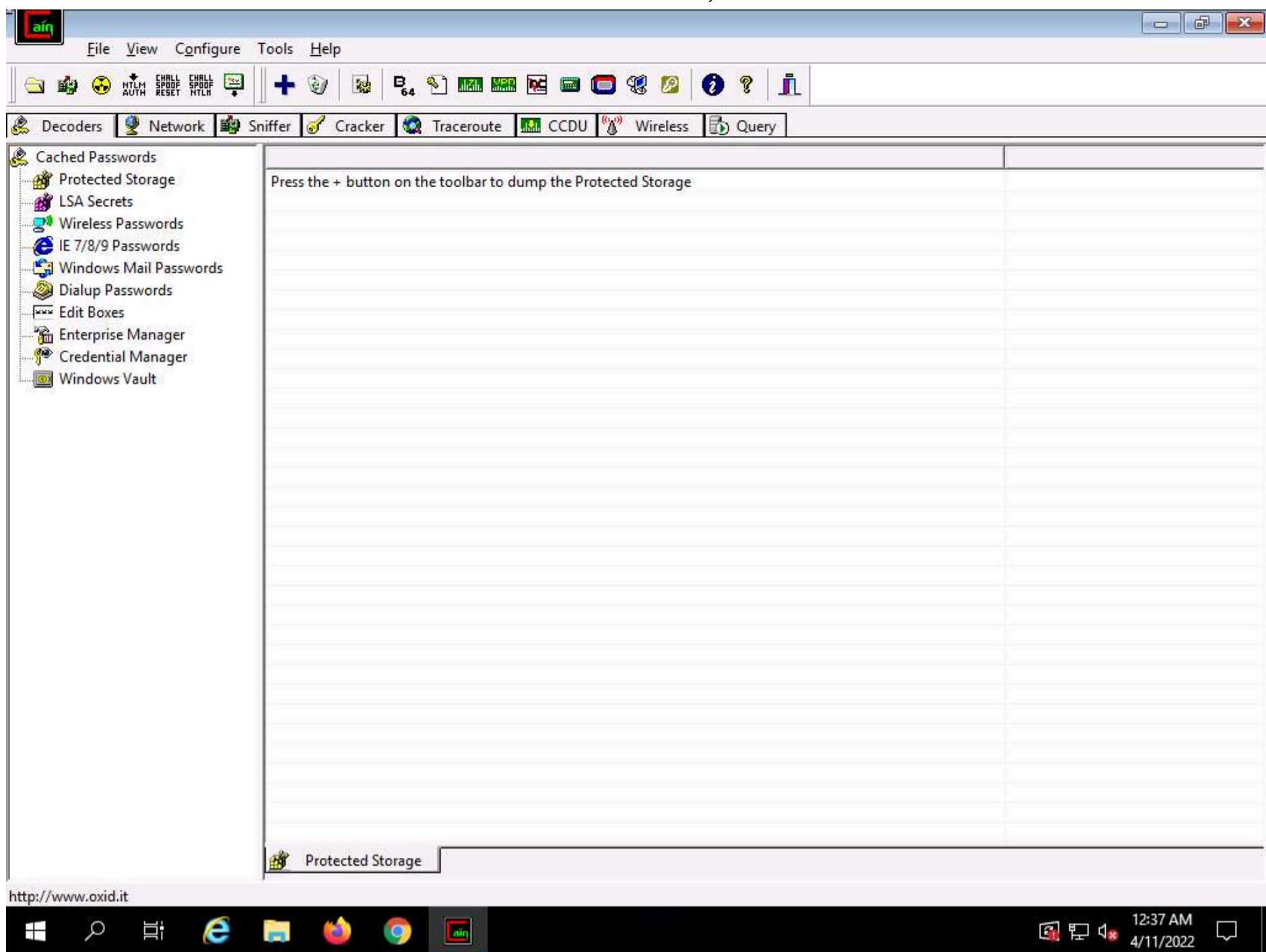


6. The Configuration Dialog window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.

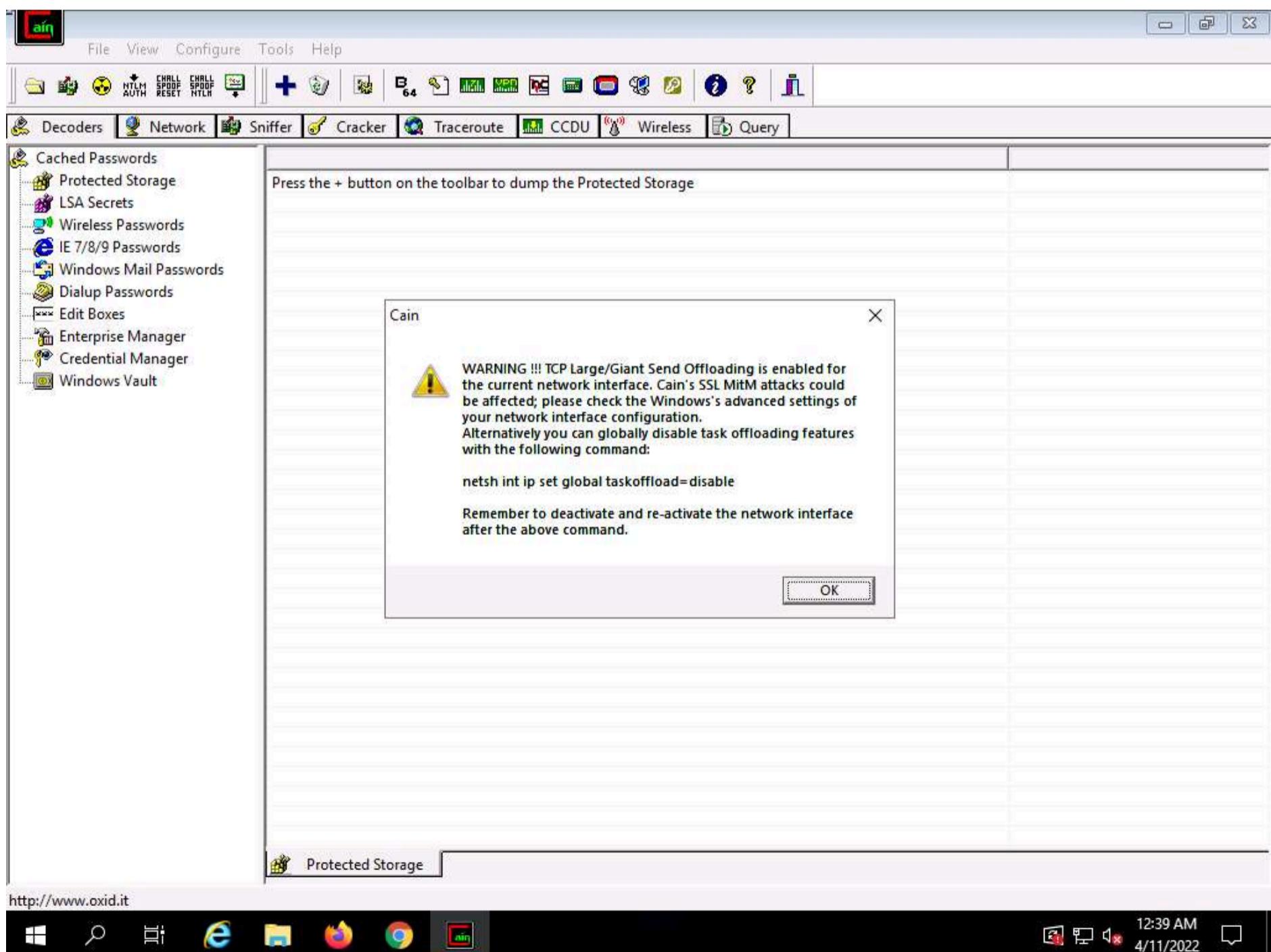


7. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.

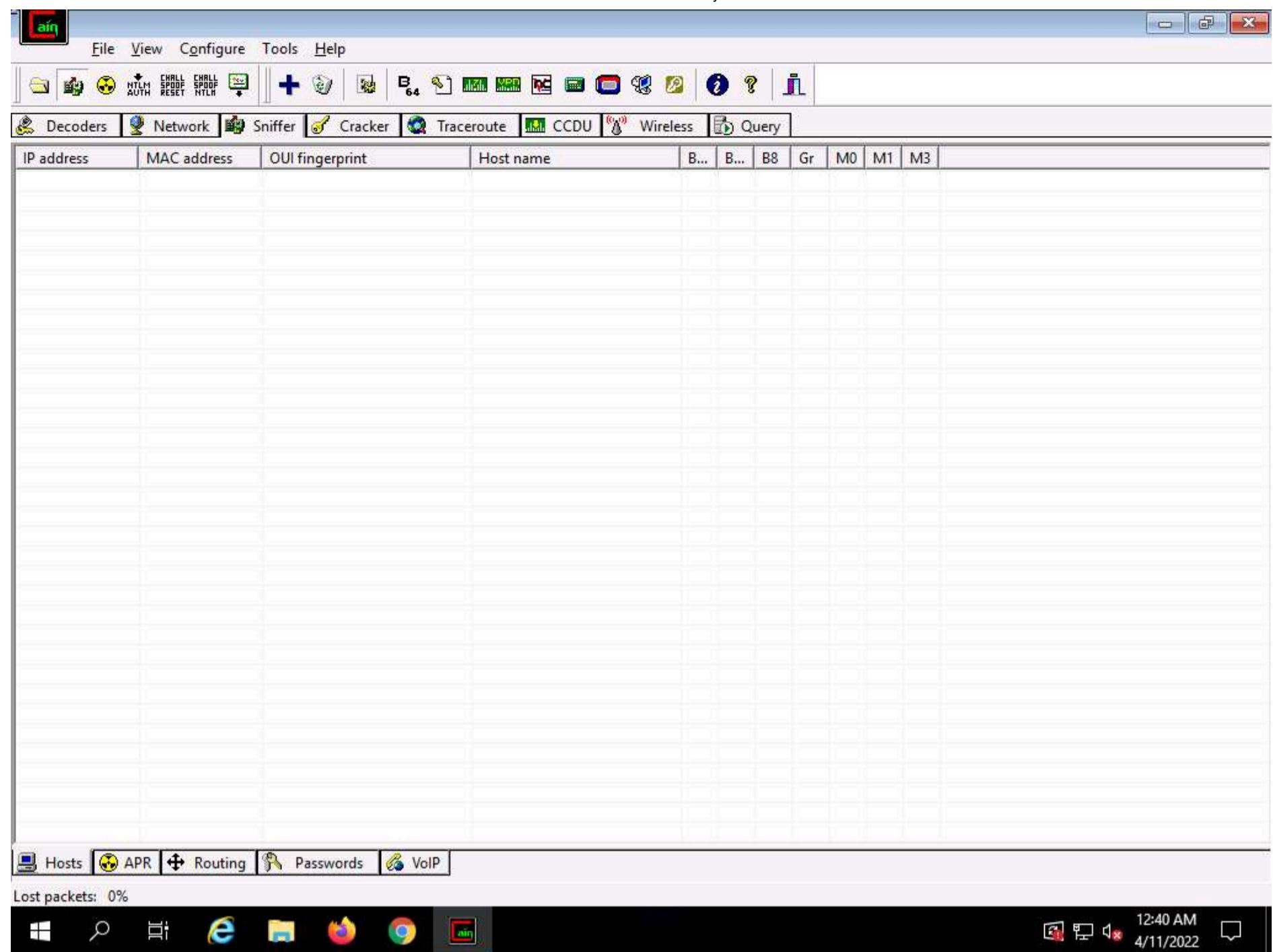




8. A Cain pop-up appears and displays a Warning message; click OK.

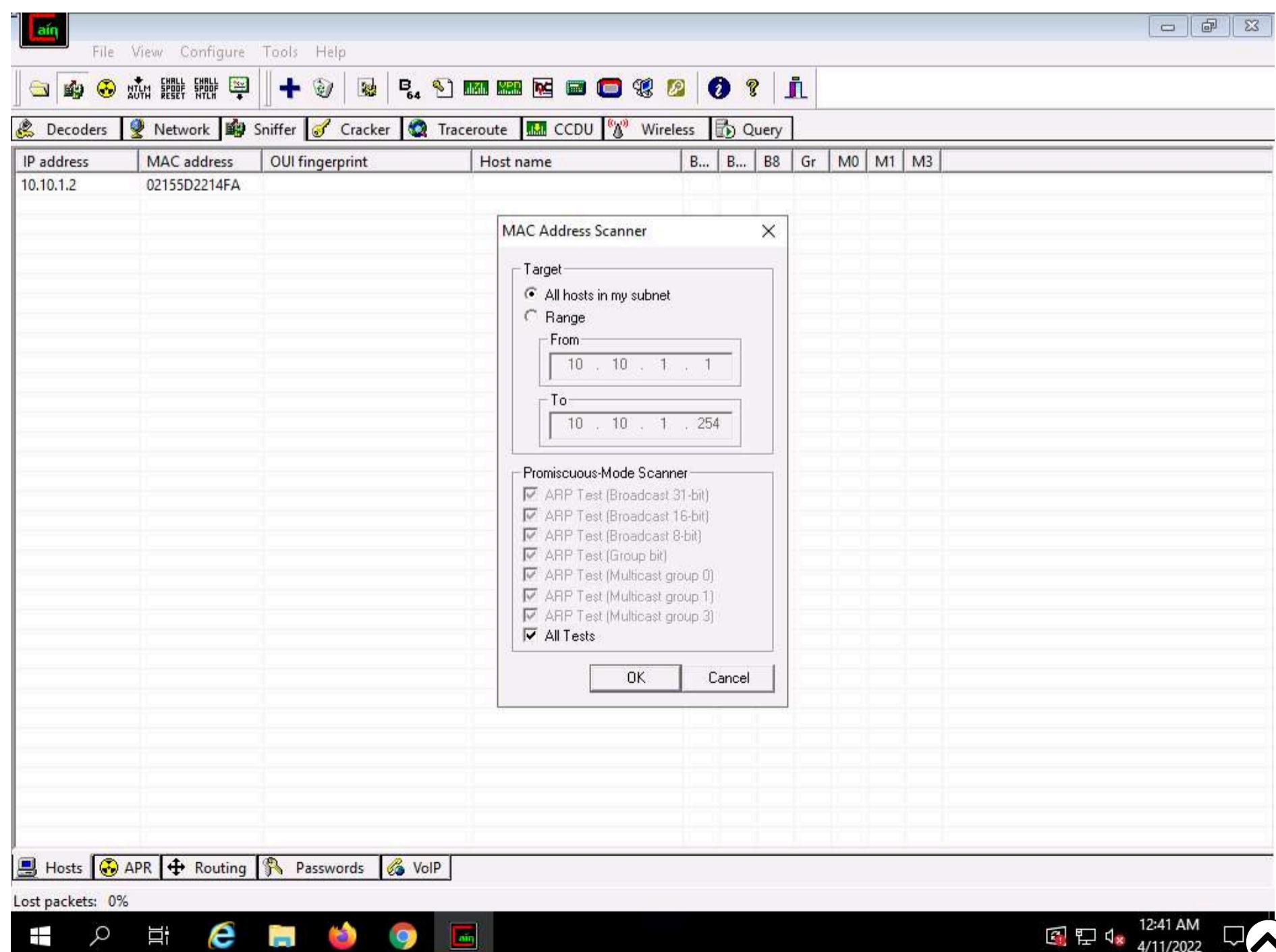


9. Now, click the Sniffer tab.



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.

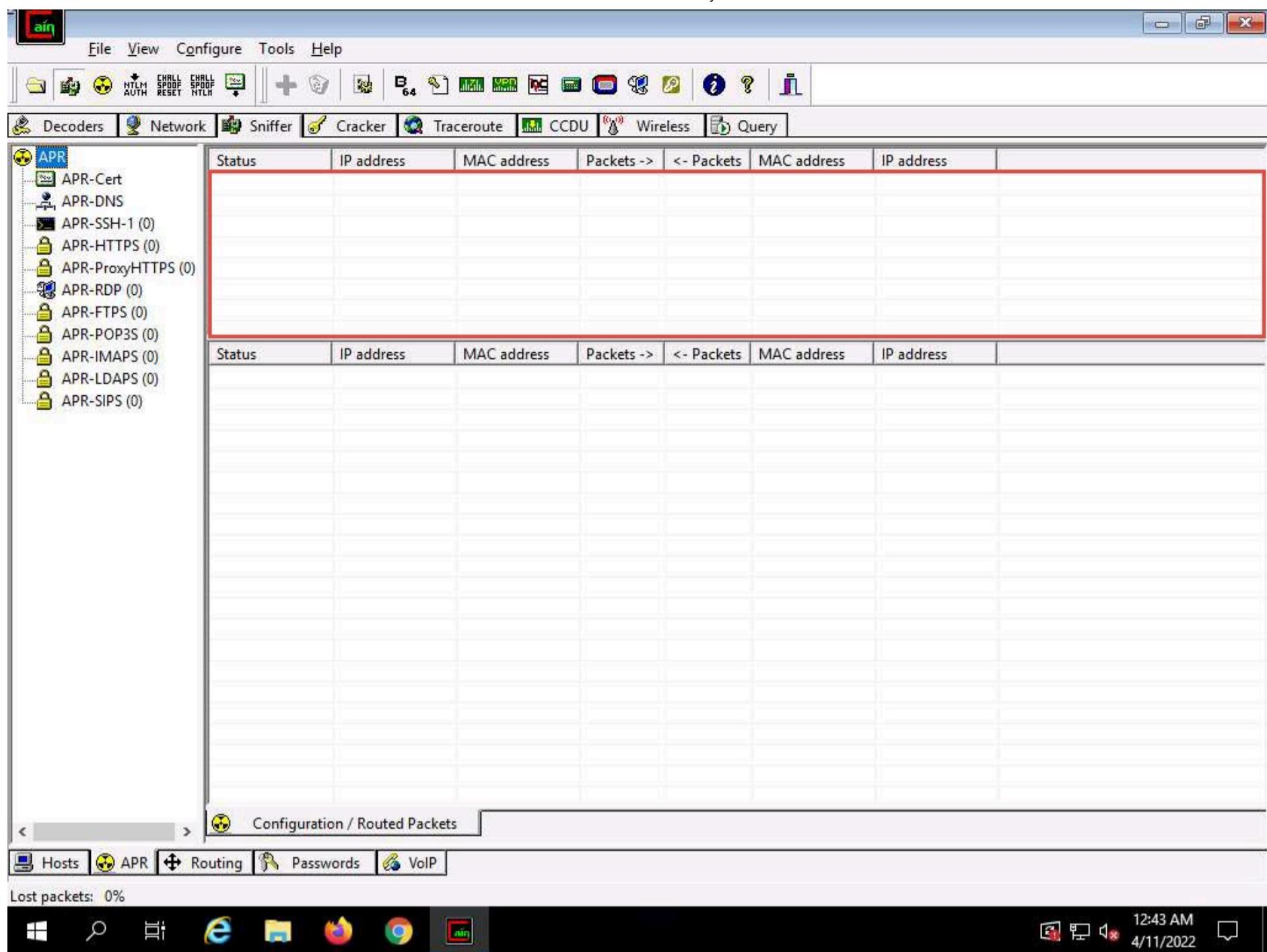
13. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

The screenshot shows the Cain & Abel interface. At the top is a menu bar with File, View, Configure, Tools, and Help. Below the menu is a toolbar with various icons for NTLM auth, CHALL auth, CHALL spoof, Nmap, and other tools. The main window has tabs for Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, and Query. The Network tab is selected, displaying a table of scanned hosts. The columns are IP address, MAC address, OUI fingerprint, Host name, and several status indicators (B..., B8, Gr, M0, M1, M3). The table shows six hosts, mostly Microsoft Corporation devices with MAC addresses like 02155D2214FA and 02155D2214FE. Below the table is a navigation bar with Hosts, APR, Routing, Passwords, and VoIP. The APR tab is highlighted. At the bottom is a taskbar with icons for Windows, search, file explorer, browser, and Cain & Abel. The system tray shows the date and time as 12:42 AM on 4/11/2022.

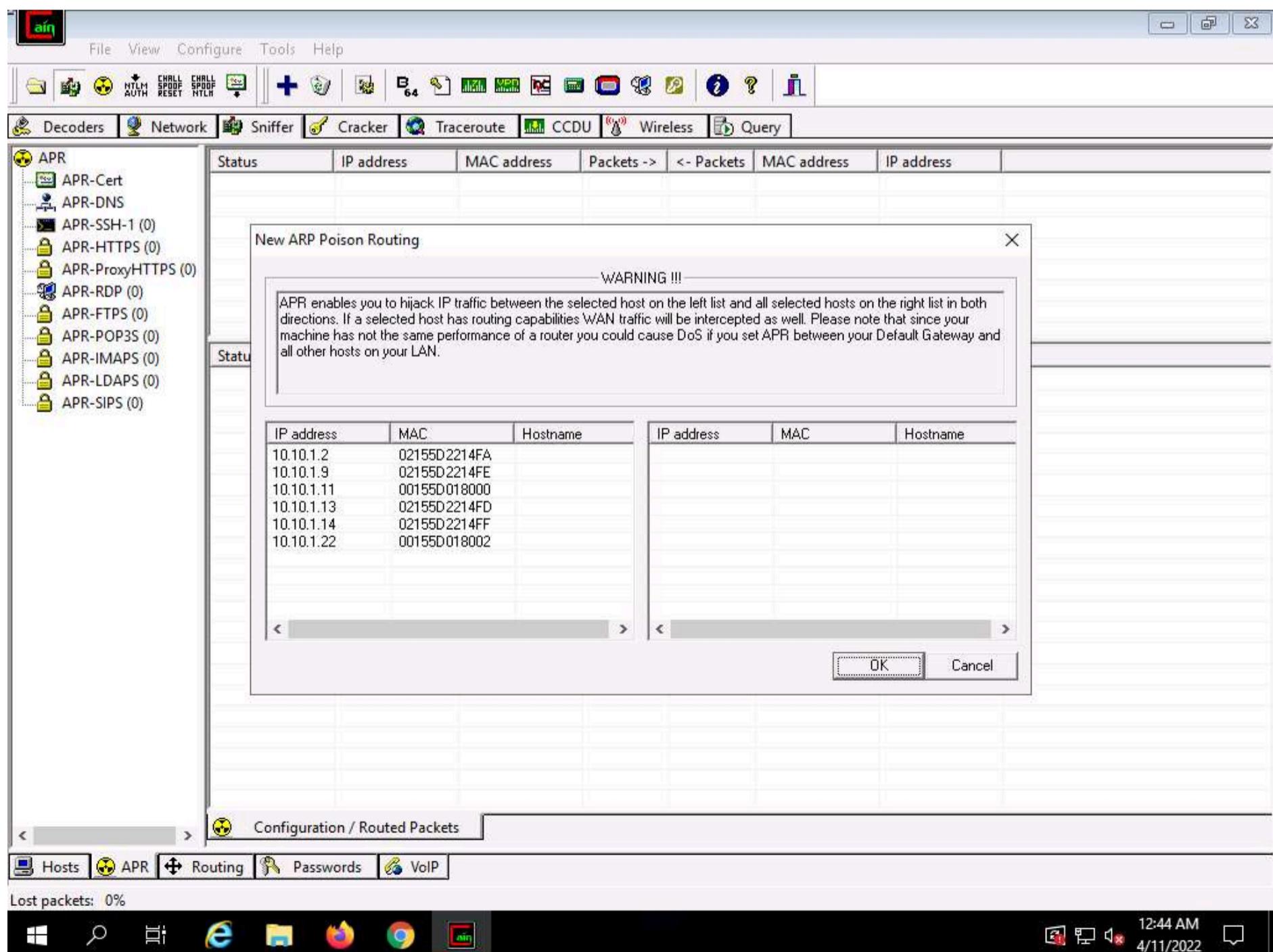
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.2	02155D2214FA			*	*	*	*	*	*	*
10.10.1.9	02155D2214FE			*	*	*	*	*	*	*
10.10.1.11	00155D018000	Microsoft Corporation		*	*	*	*	*	*	*
10.10.1.13	02155D2214FD			*	*	*	*	*	*	*
10.10.1.14	02155D2214FF			*	*	*	*	*	*	*
10.10.1.22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

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

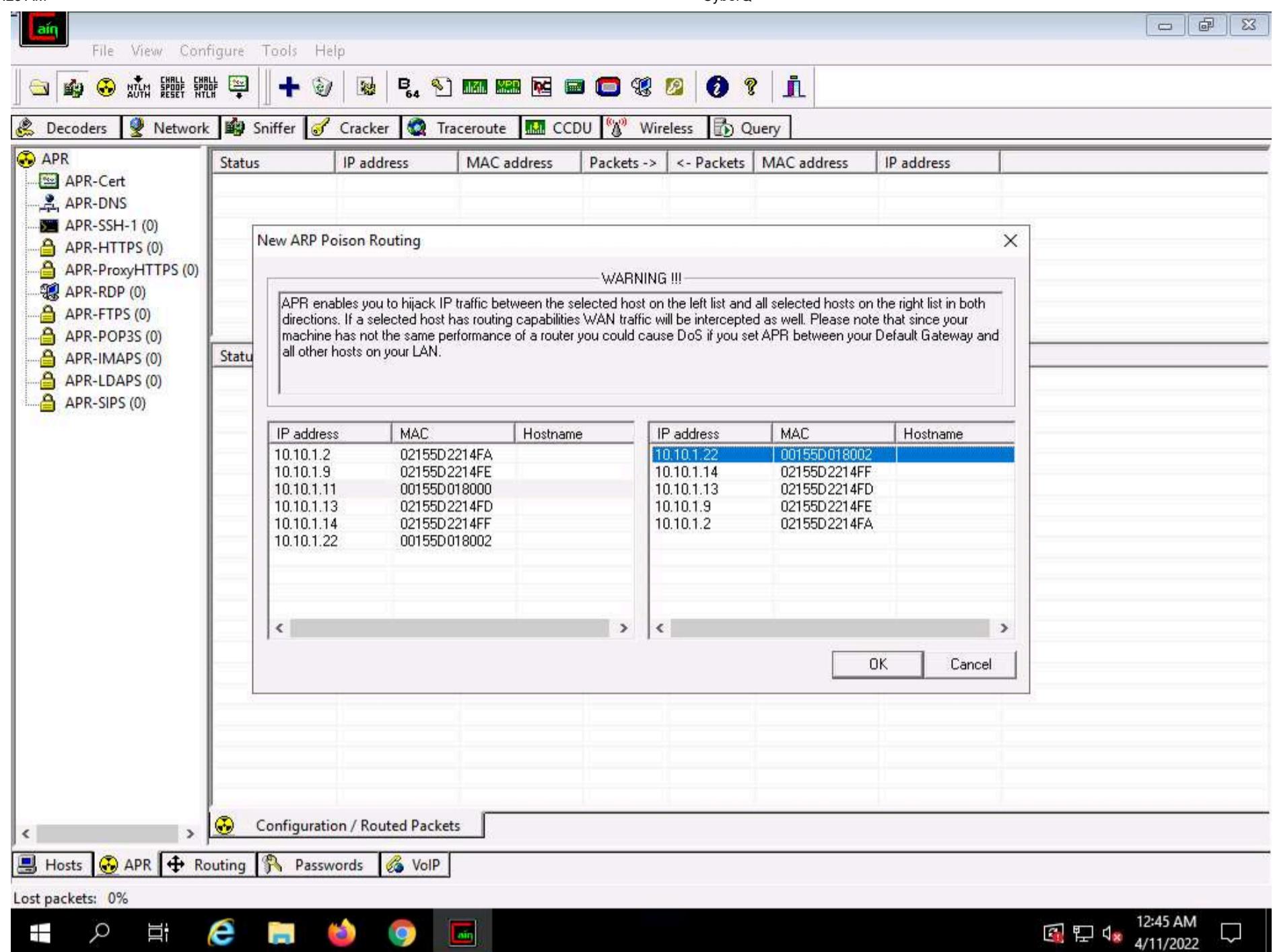
15. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.



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

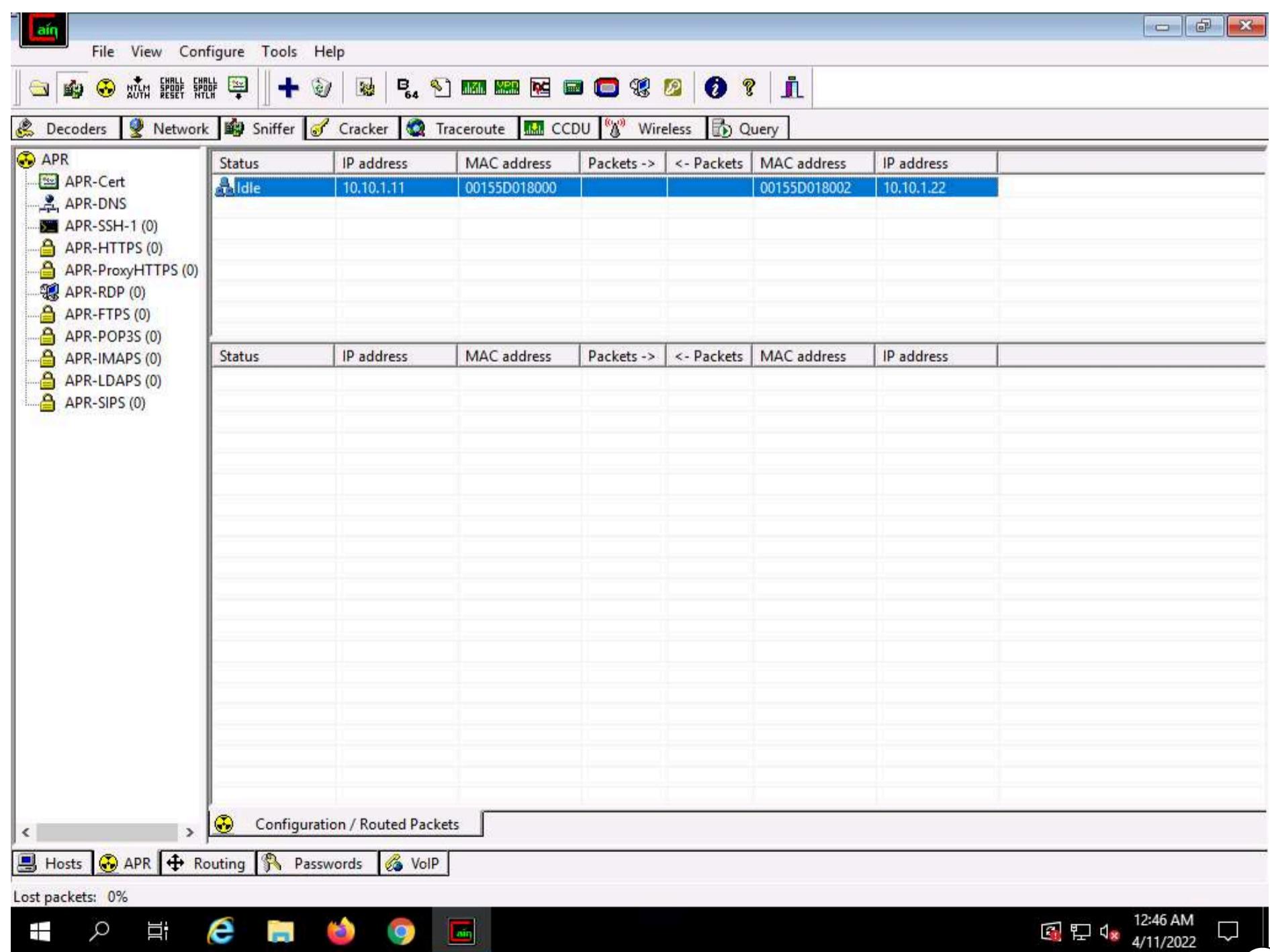


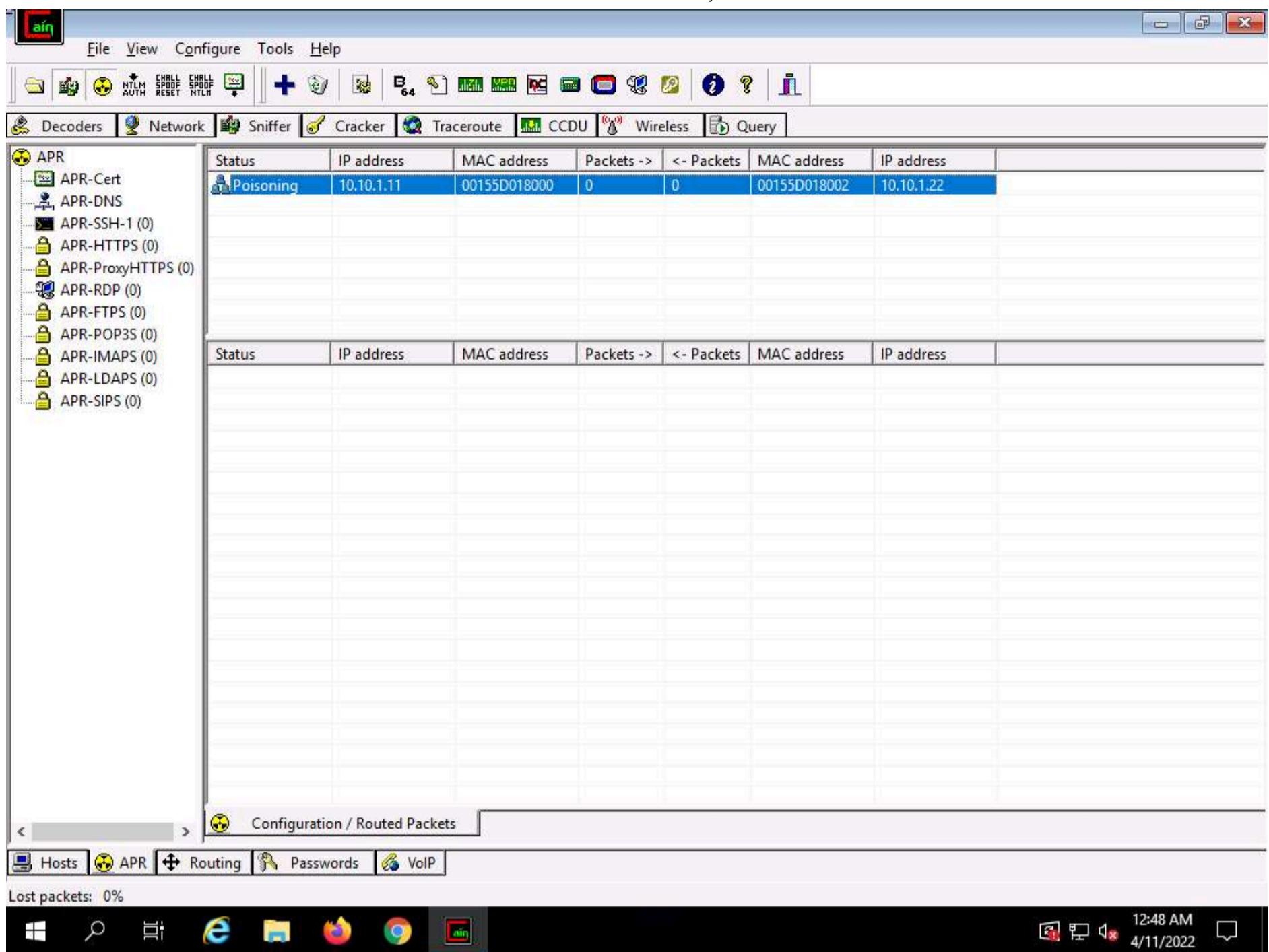
17. To monitor the traffic between two systems (here, Windows 11 and Windows Server 2022), click to select **10.10.1.11** (Windows 11) from the left-hand pane and **10.10.1.22** (Windows Server 2022) from the right-hand pane; click **OK**.



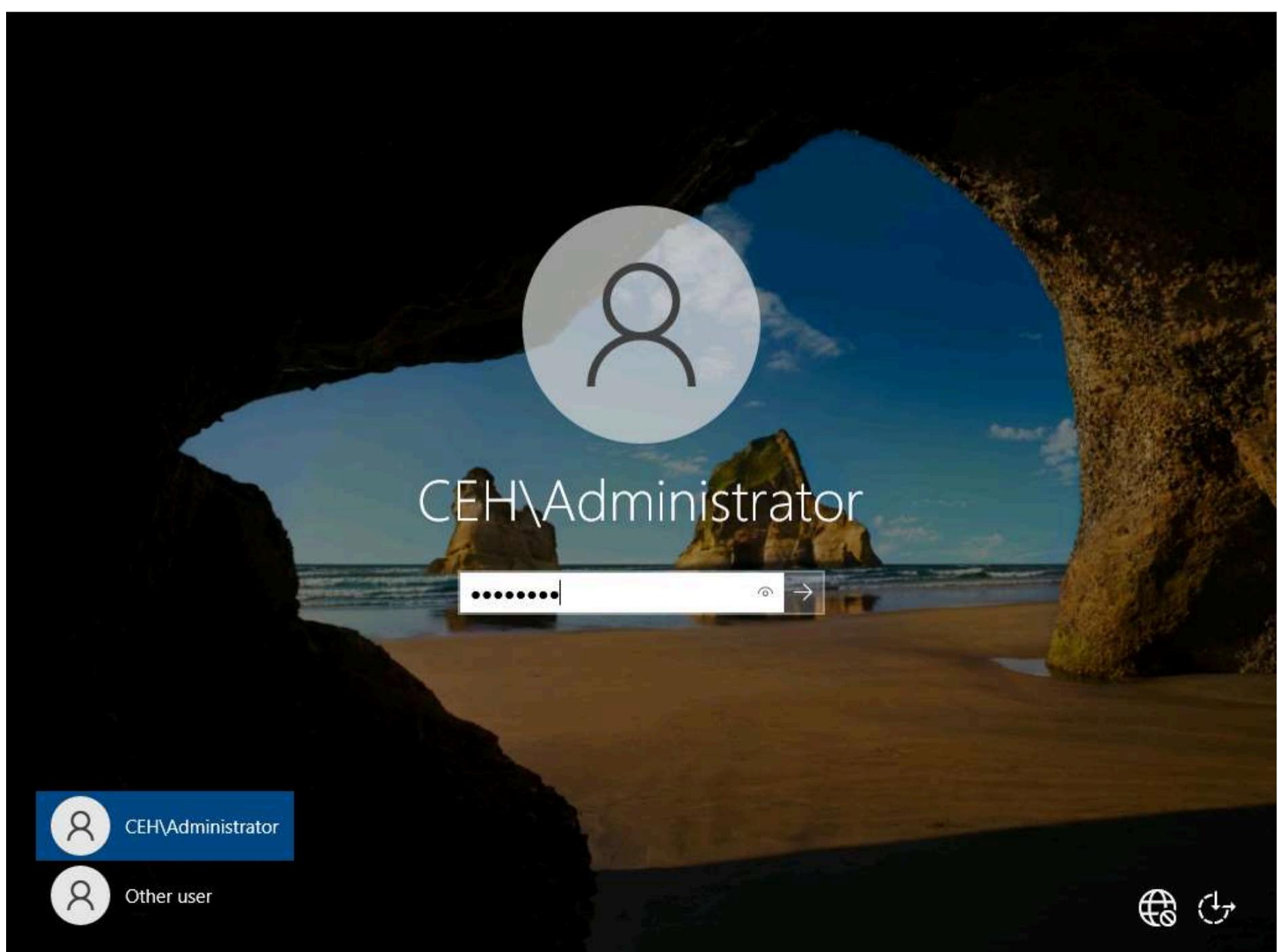
18. Click to select the created target IP address scan displayed in the Configuration / Routes Packets tab.

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

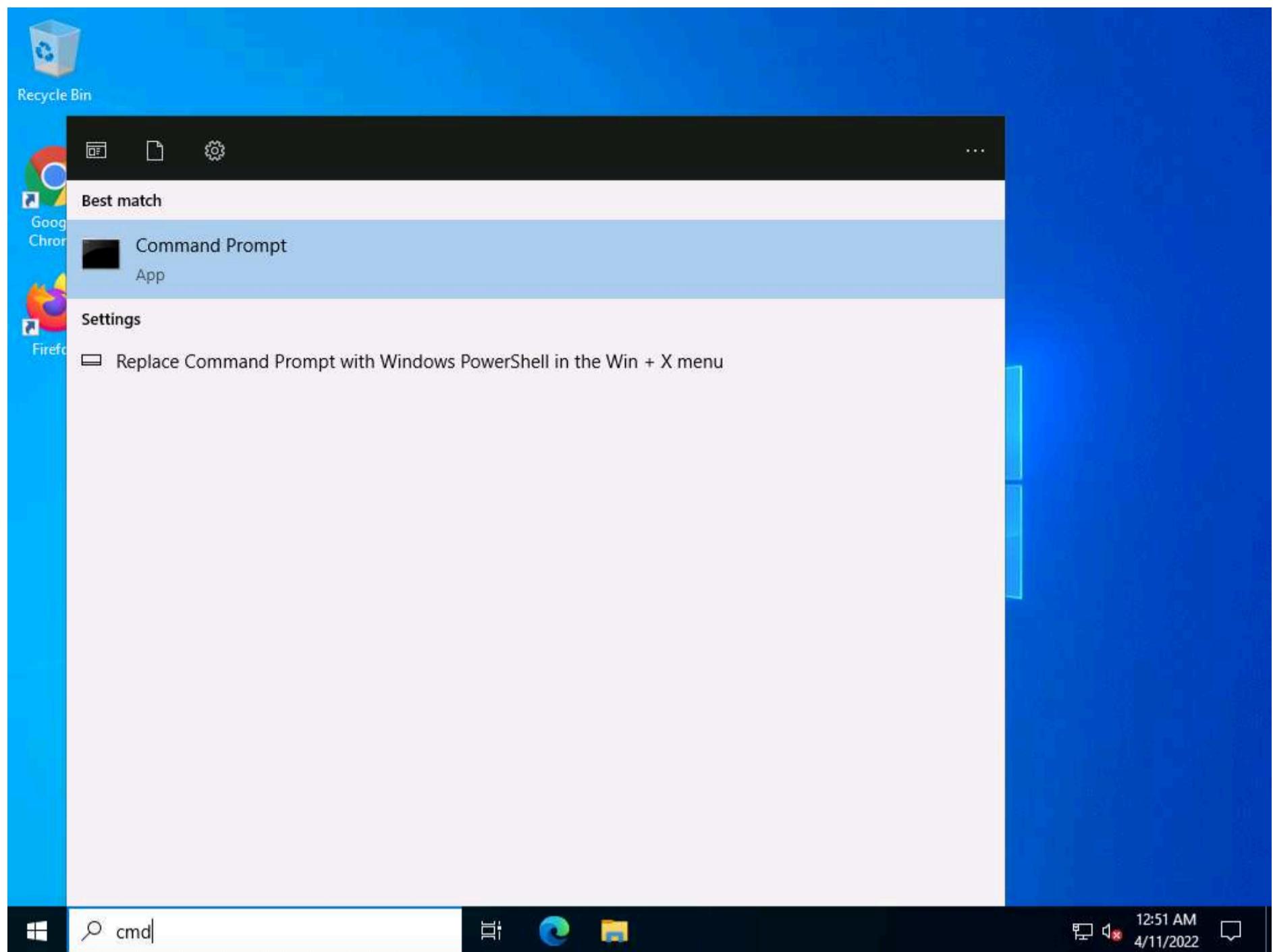




20. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine, click **Ctrl+Alt+Del**. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



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.

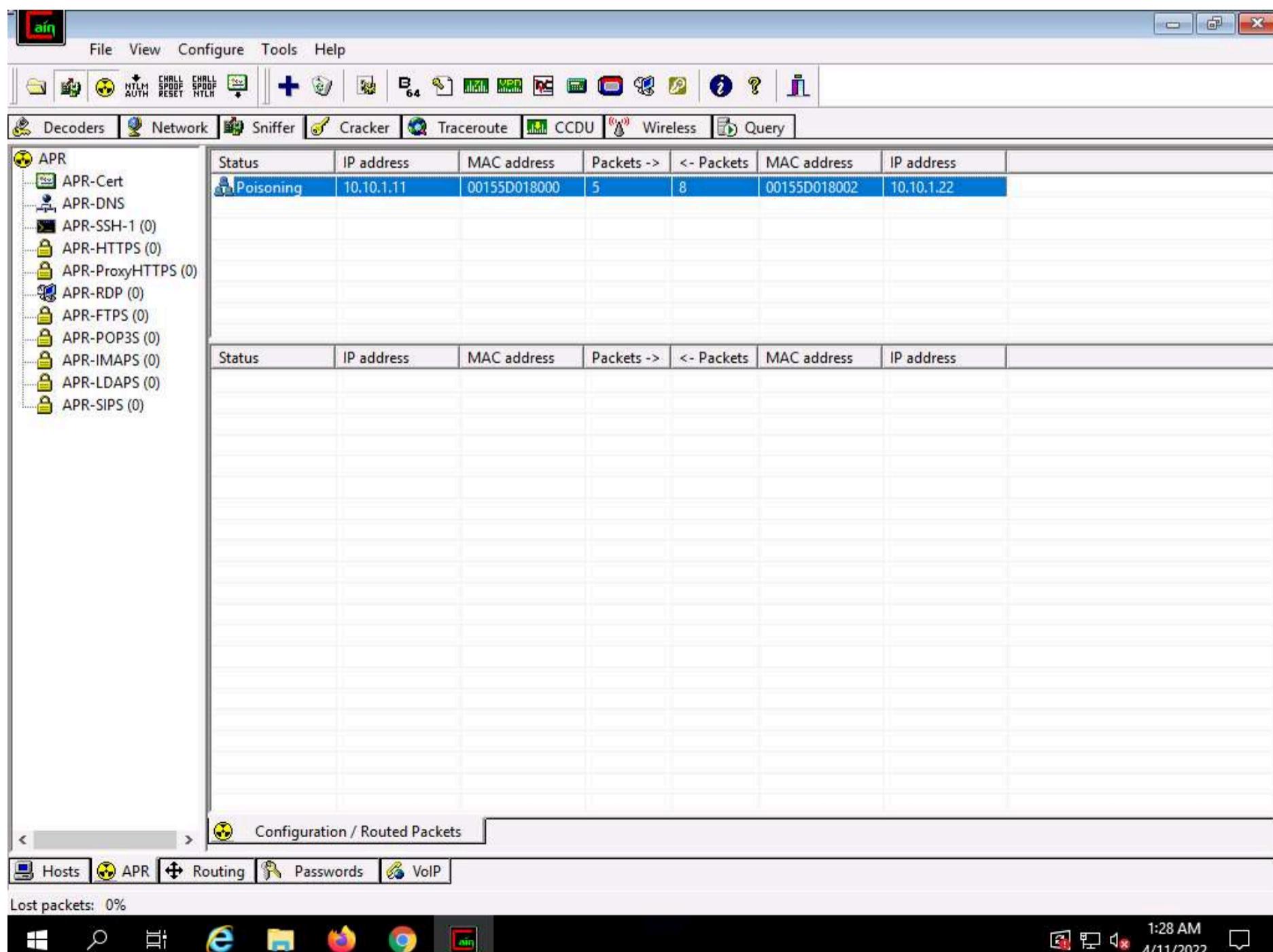


```
C:\ Select Administrator: Command Prompt - ftp 10.10.1.11
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

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



24. 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.

The screenshot shows the Cain & Abel interface. On the left, a sidebar lists various protocols with their counts: FTP (1), HTTP (0), IMAP (0), LDAP (0), POP3 (0), SMB (0), Telnet (0), VNC (0), TDS (0), TNS (0), SMTP (0), NNTP (0), DCE/RPC (0), MSKerb5-PreAuth (0), Radius-Keys (0), Radius-Users (0), ICQ (0), IKE-PSK (0), MySQL (0), SNMP (0), SIP (0), GRE/PPP (0), PPPoE (0), and SAP Diag (0). The main pane displays a table with the following data:

	Timestamp	FTP server	Client	Username	Password
FTP (1)	11/04/2022 - 01:26:01	10.10.1.11	10.10.1.22	Jason	qwerty

Below the table, the sidebar shows the **FTP** tab is selected. At the bottom, the taskbar includes icons for Hosts, APR, Routing, Passwords, VoIP, and Cain. The system tray shows the date and time as 1:28 AM, 4/11/2022.

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.

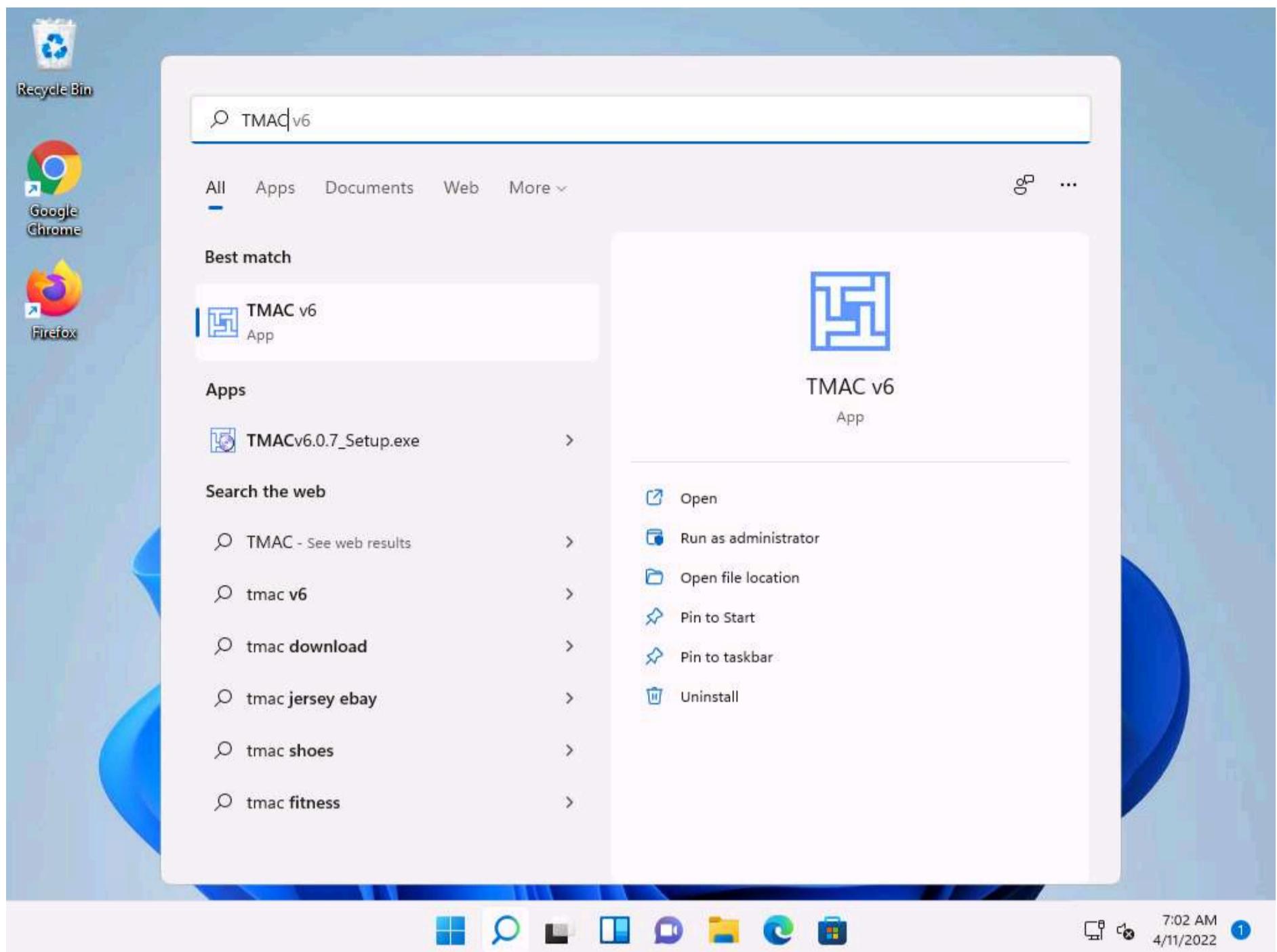
Here, we will use TMAC and SMAC tools to perform MAC spoofing.

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

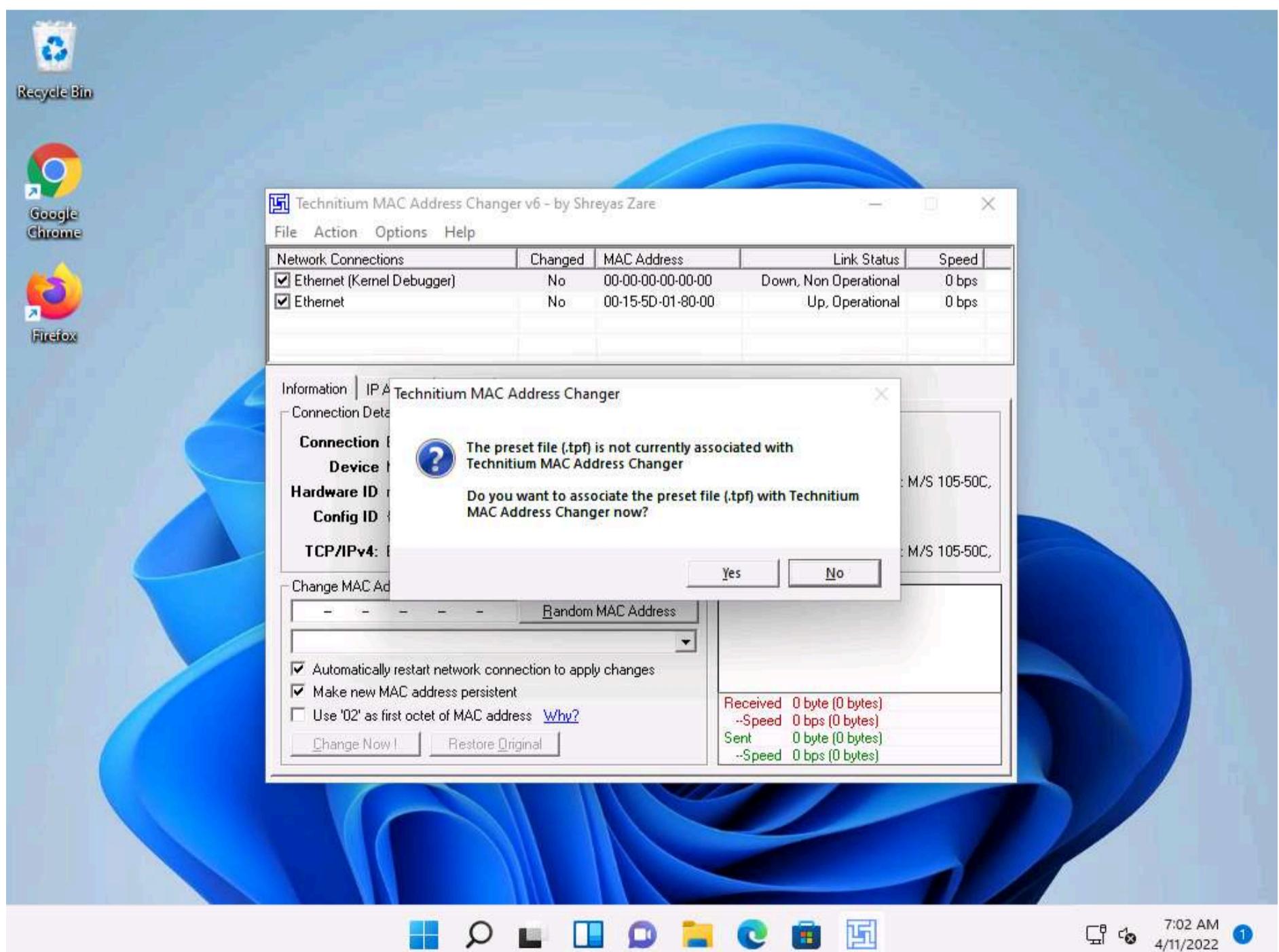
Note: If a **User Account Control** pop-up appears, click **Yes**.

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**.

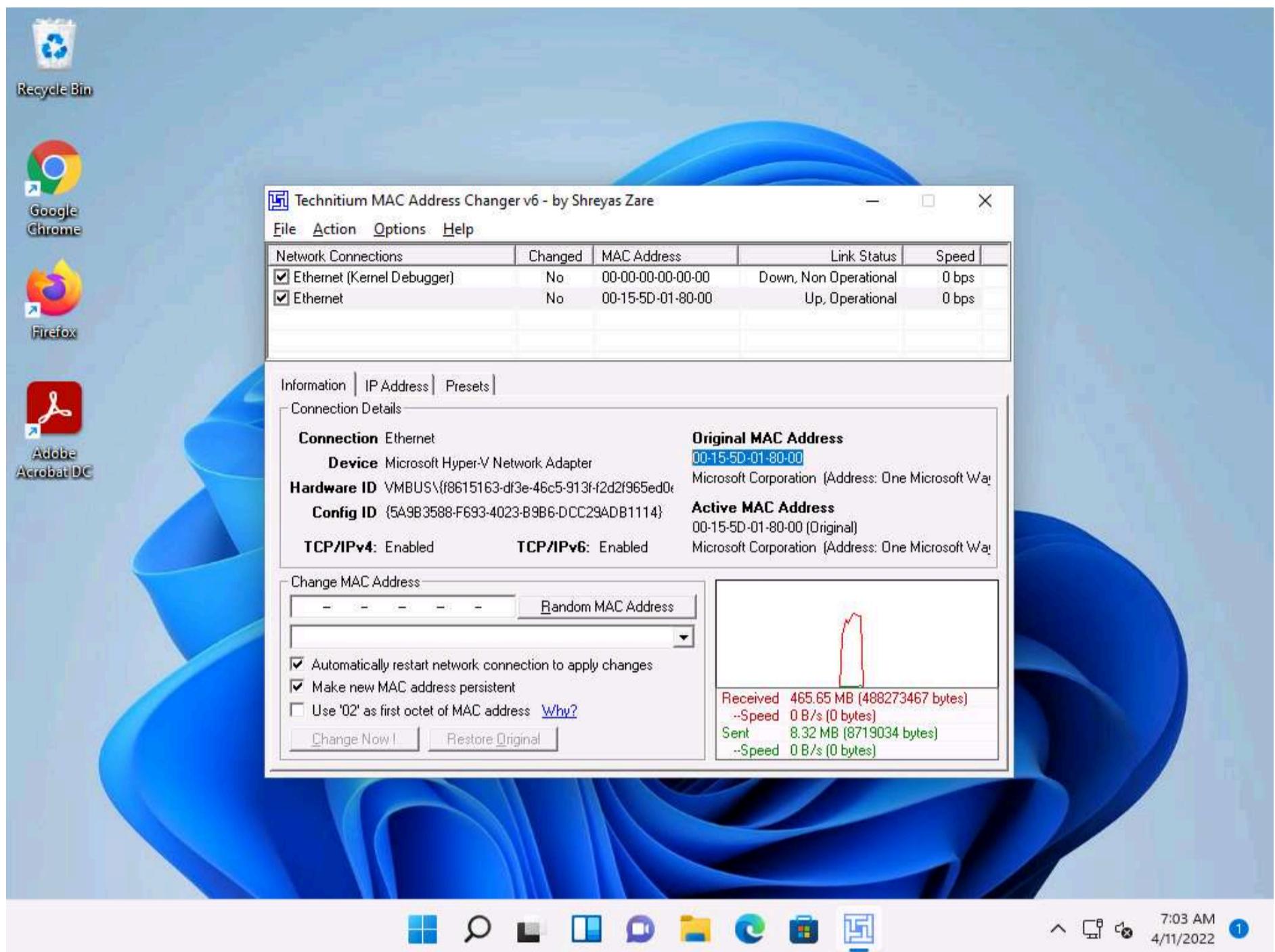


3. The Technitium MAC Address Changer main window appears. In the Technitium MAC Address Changer pop-up, click **No**.

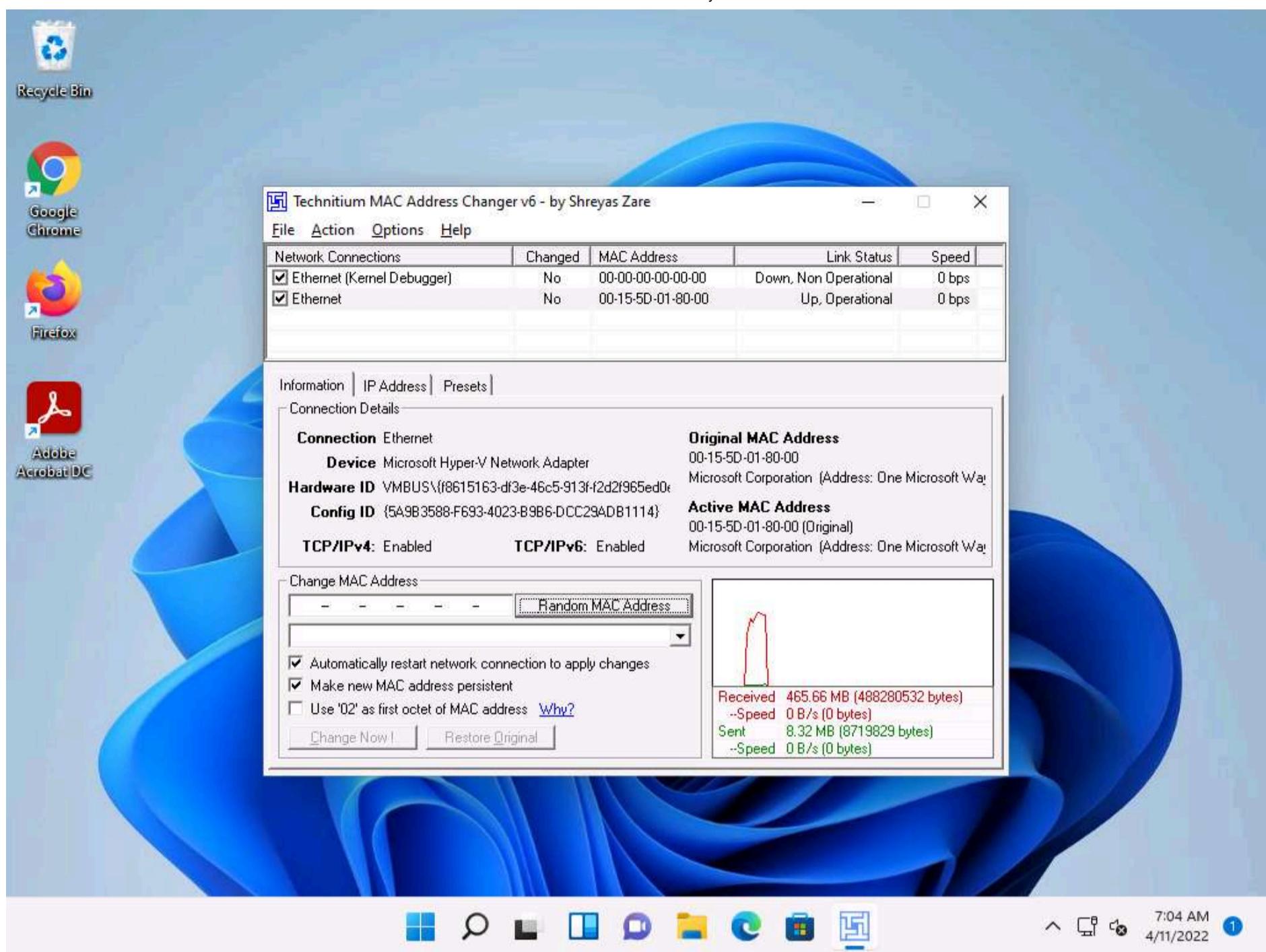


4. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet**).

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

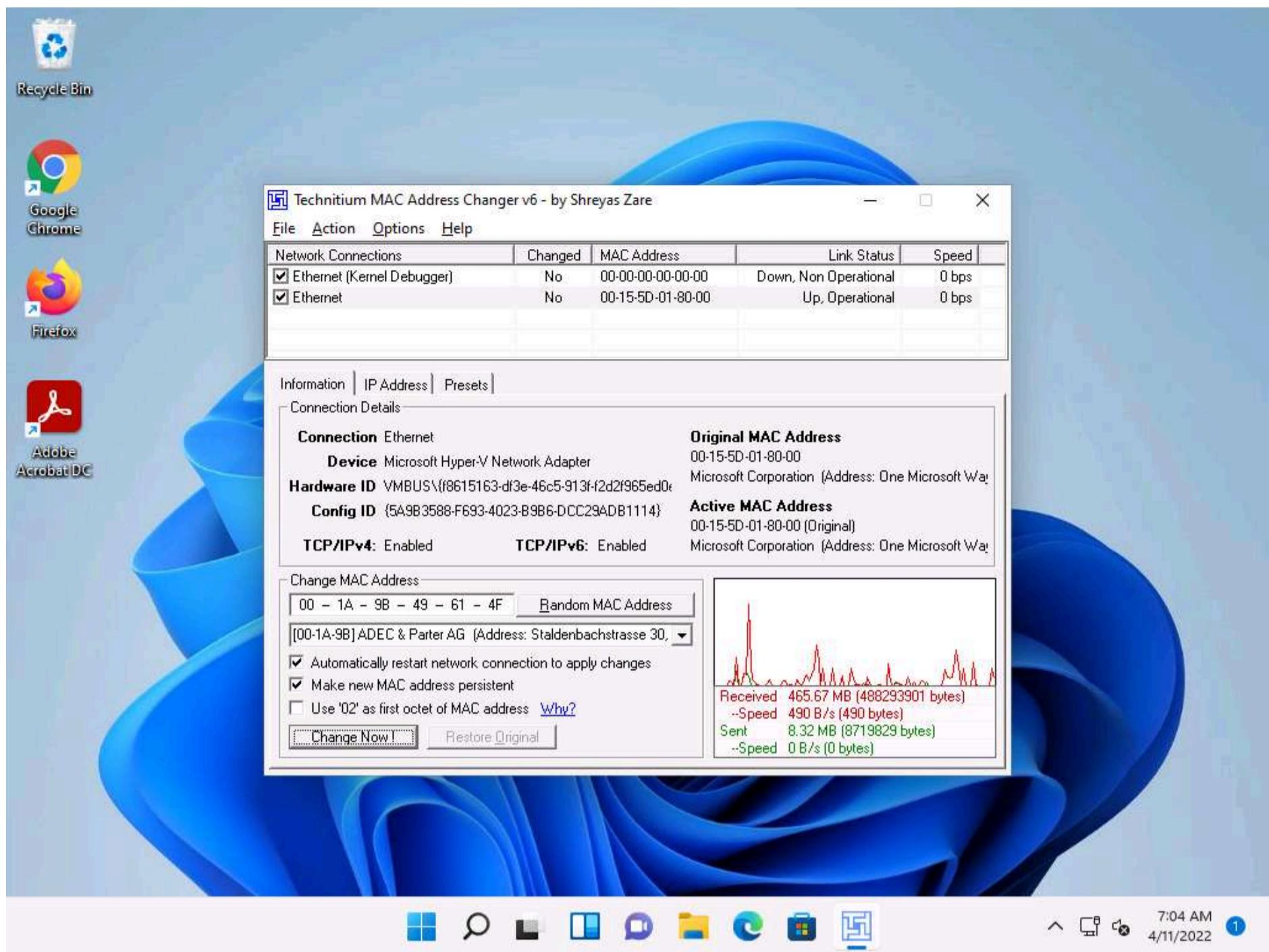


6. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

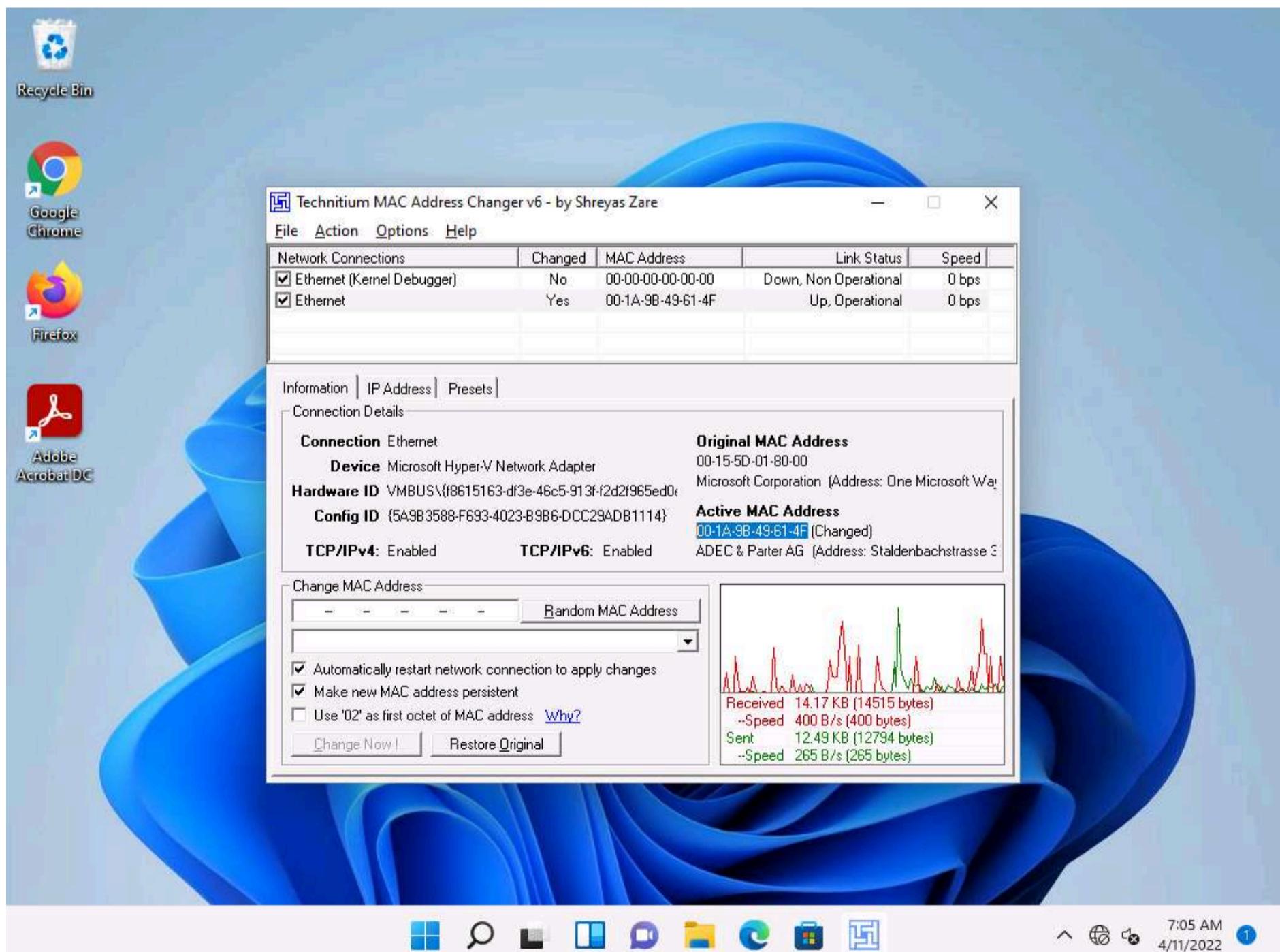


7. A Random MAC Address is generated and appears under the Change MAC Address field. Click the Change Now! button to change the MAC address.

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

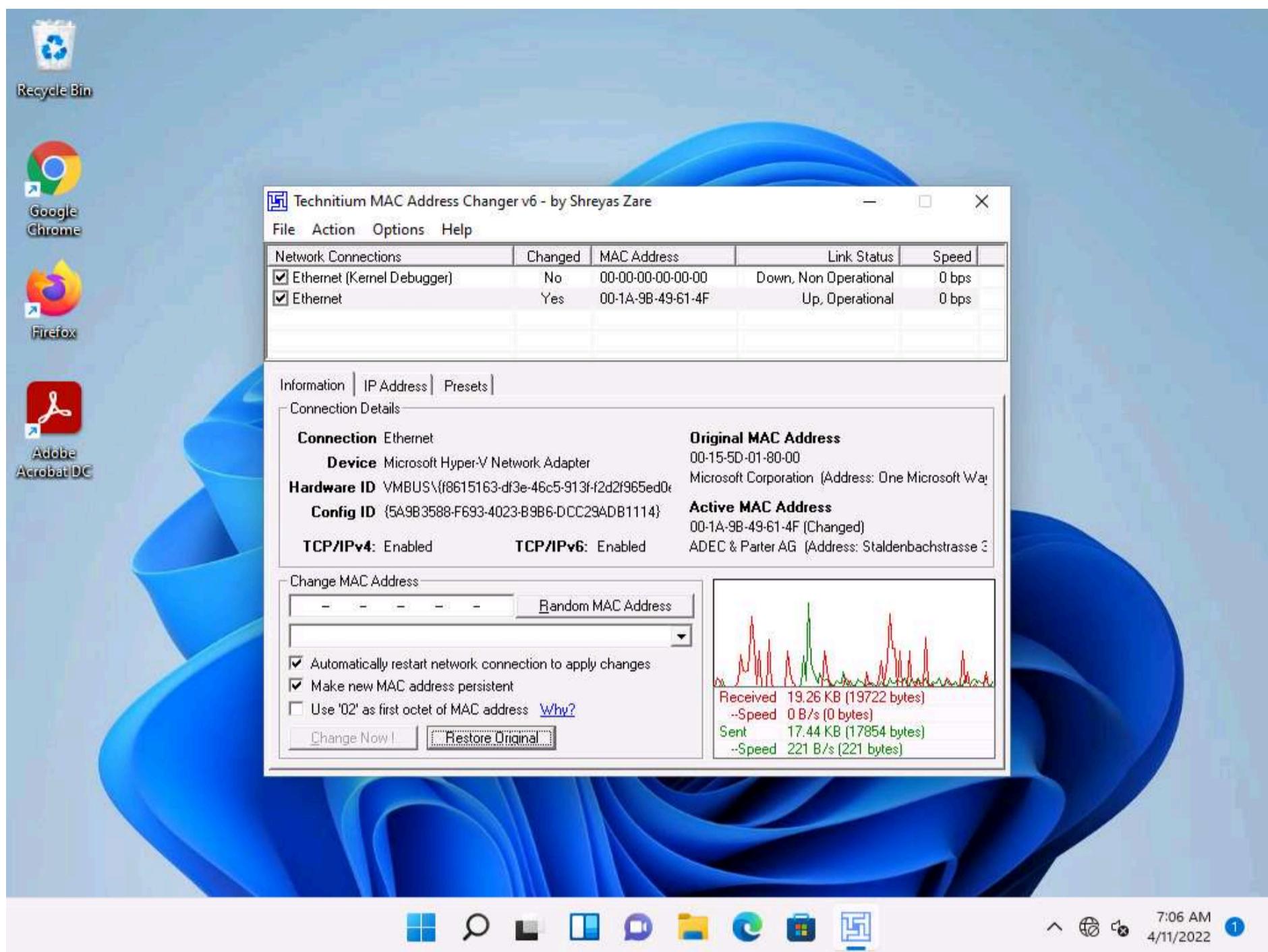


8. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.



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**.

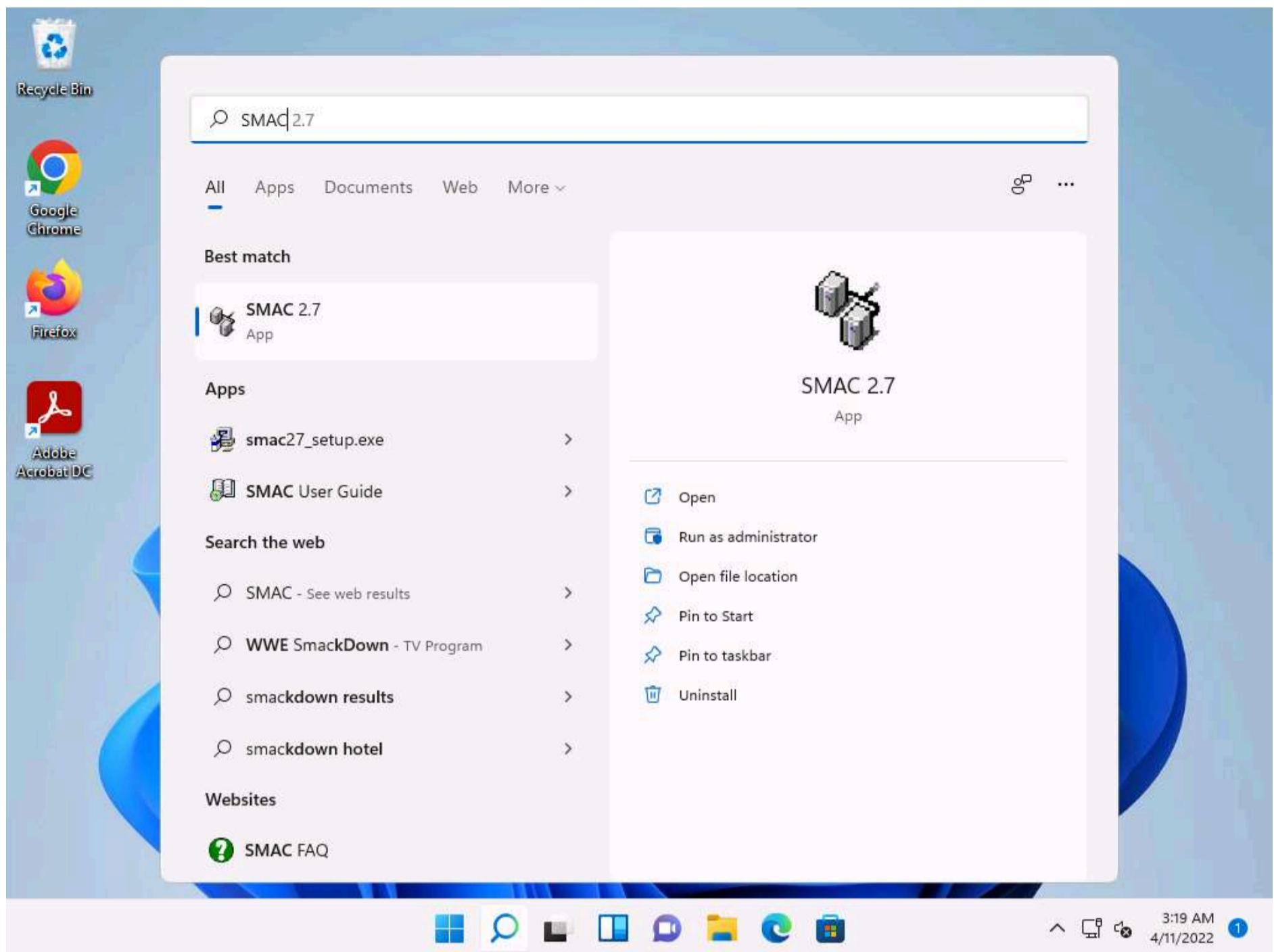


10. Close the **TMAC** main window.

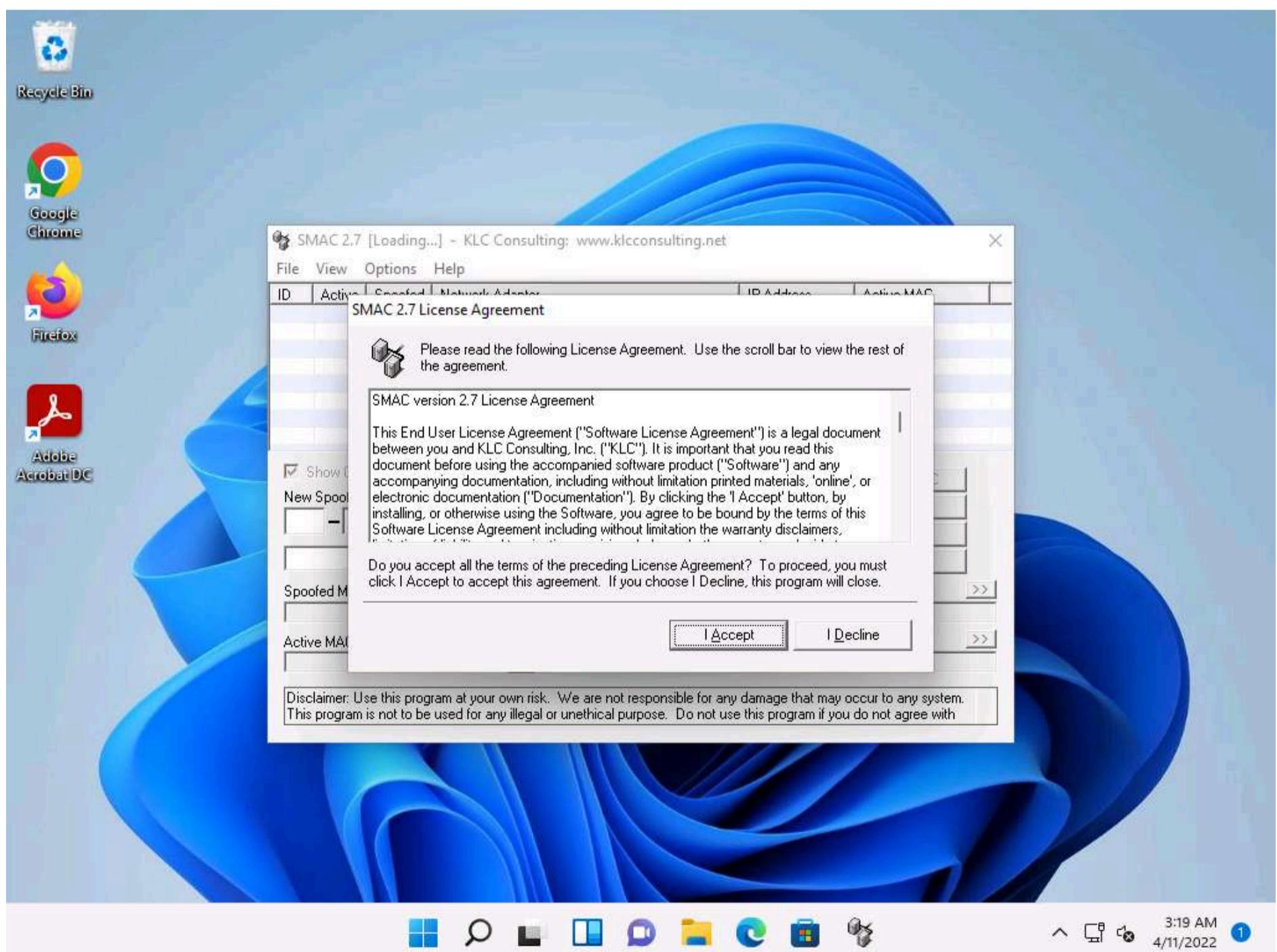
11. Now, we shall perform MAC spoofing using the SMAC tool.

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.

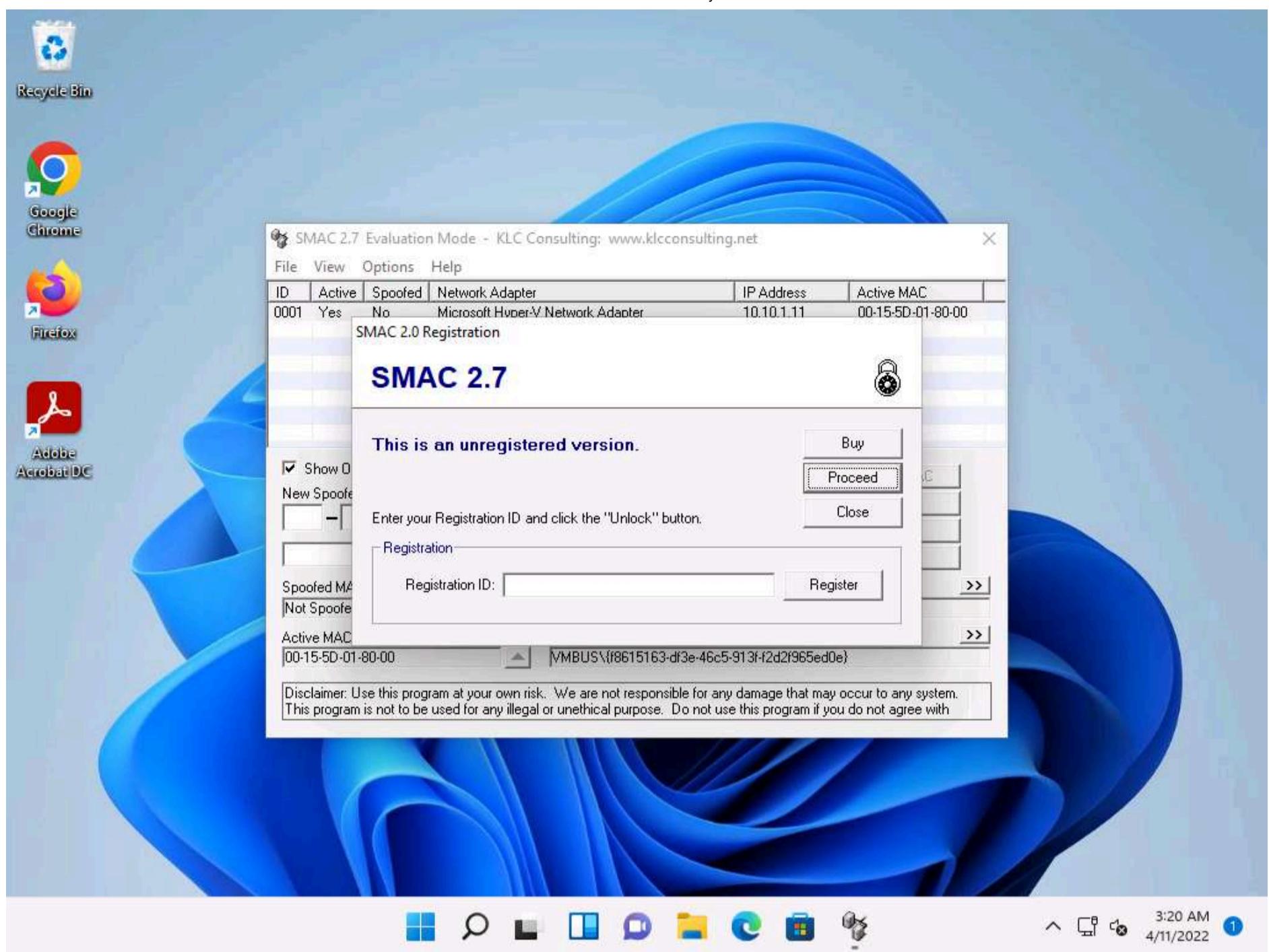
Note: If a **User Account Control** pop-up appears, click **Yes**.



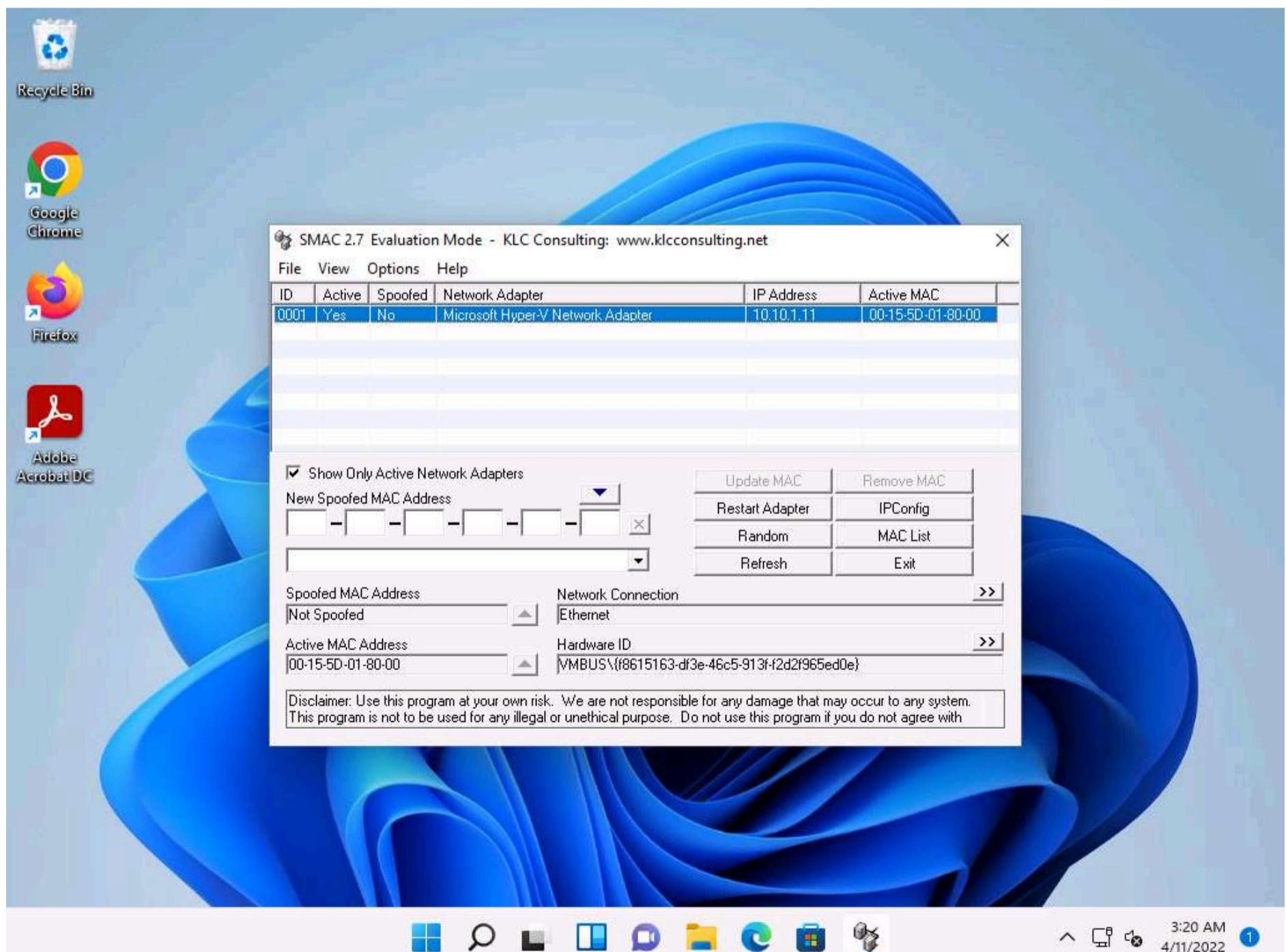
13. The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.



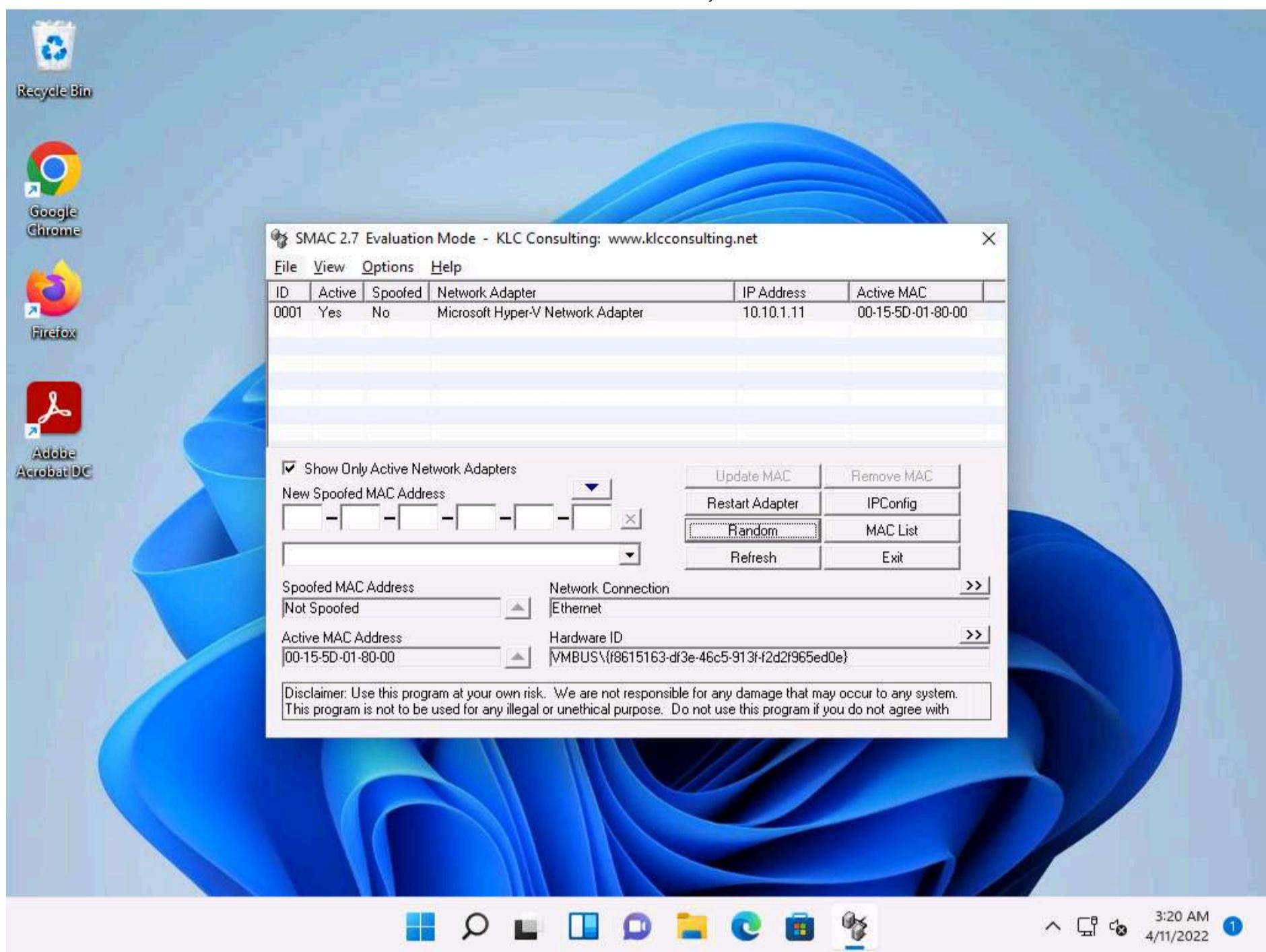
14. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.



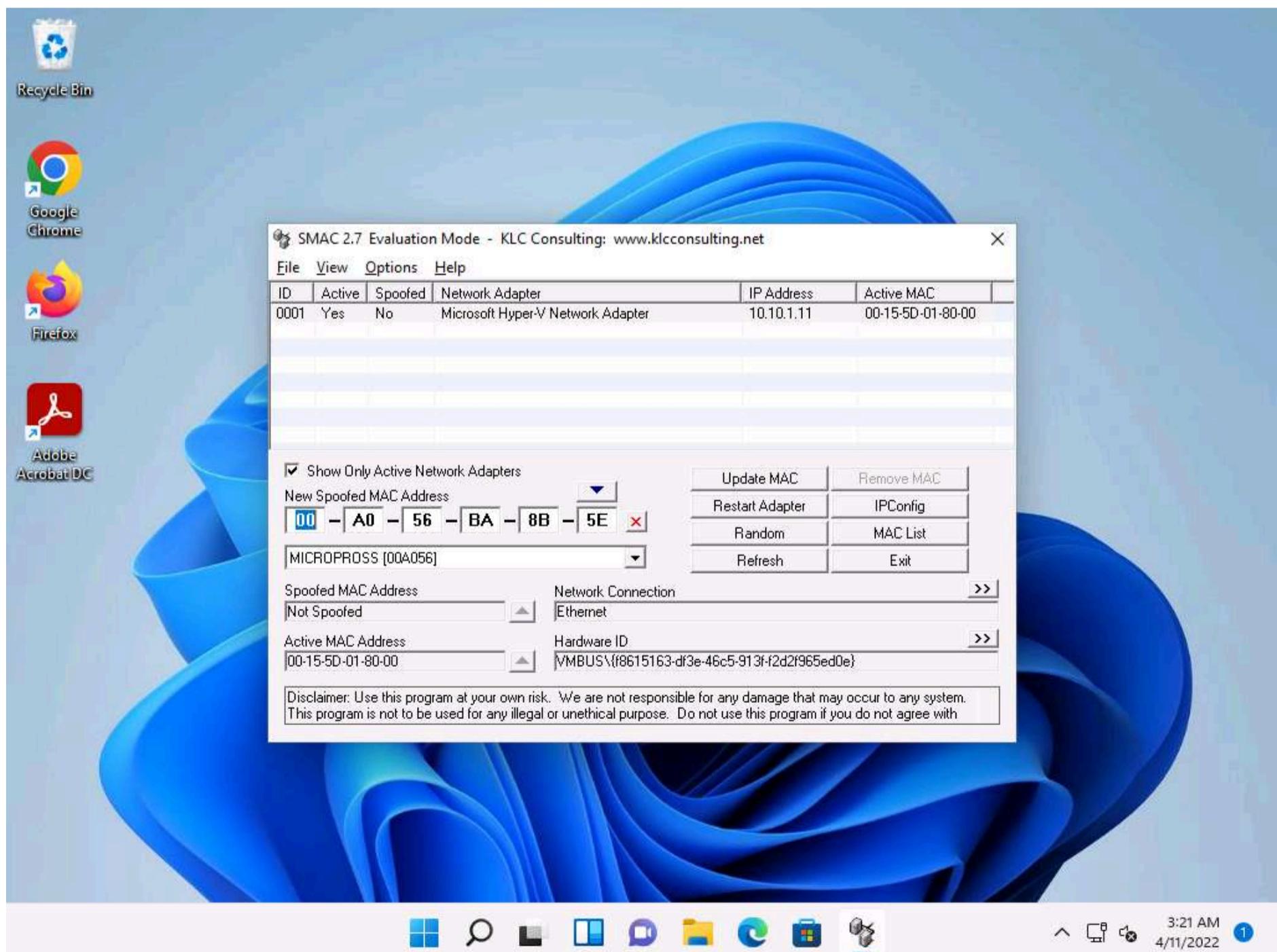
15. The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.



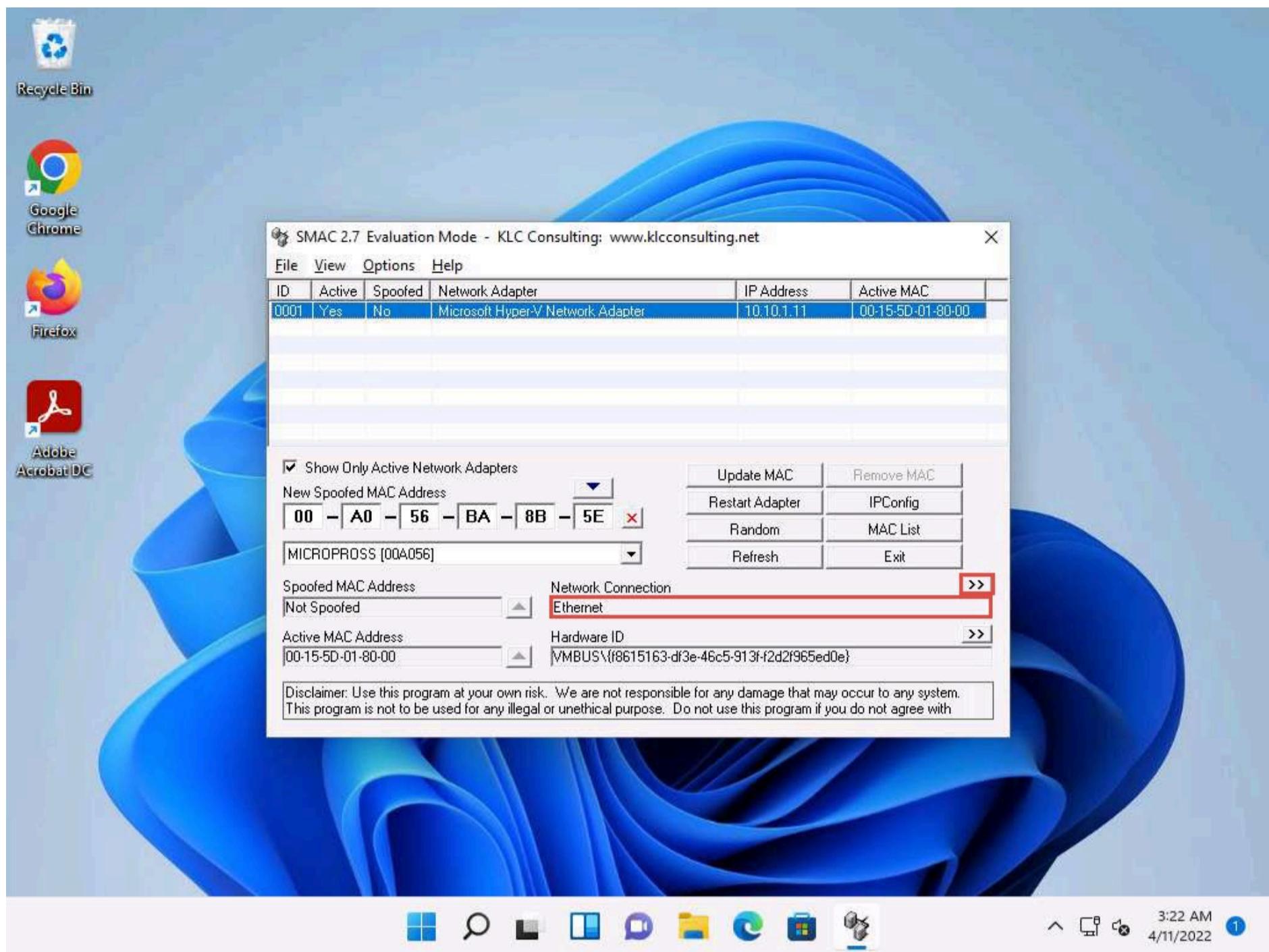
16. Click the **Random** button to generate a random MAC address.



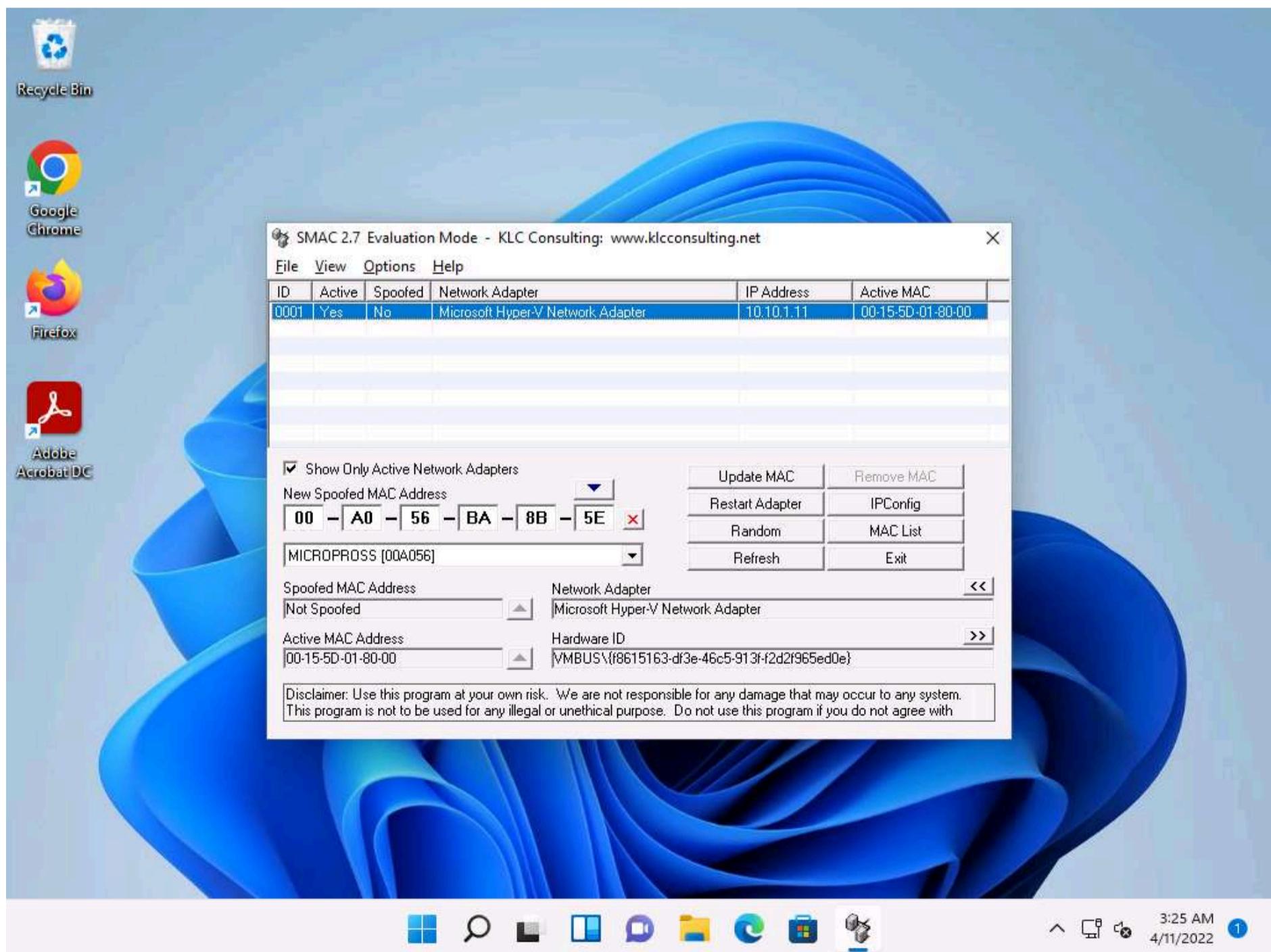
17. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.



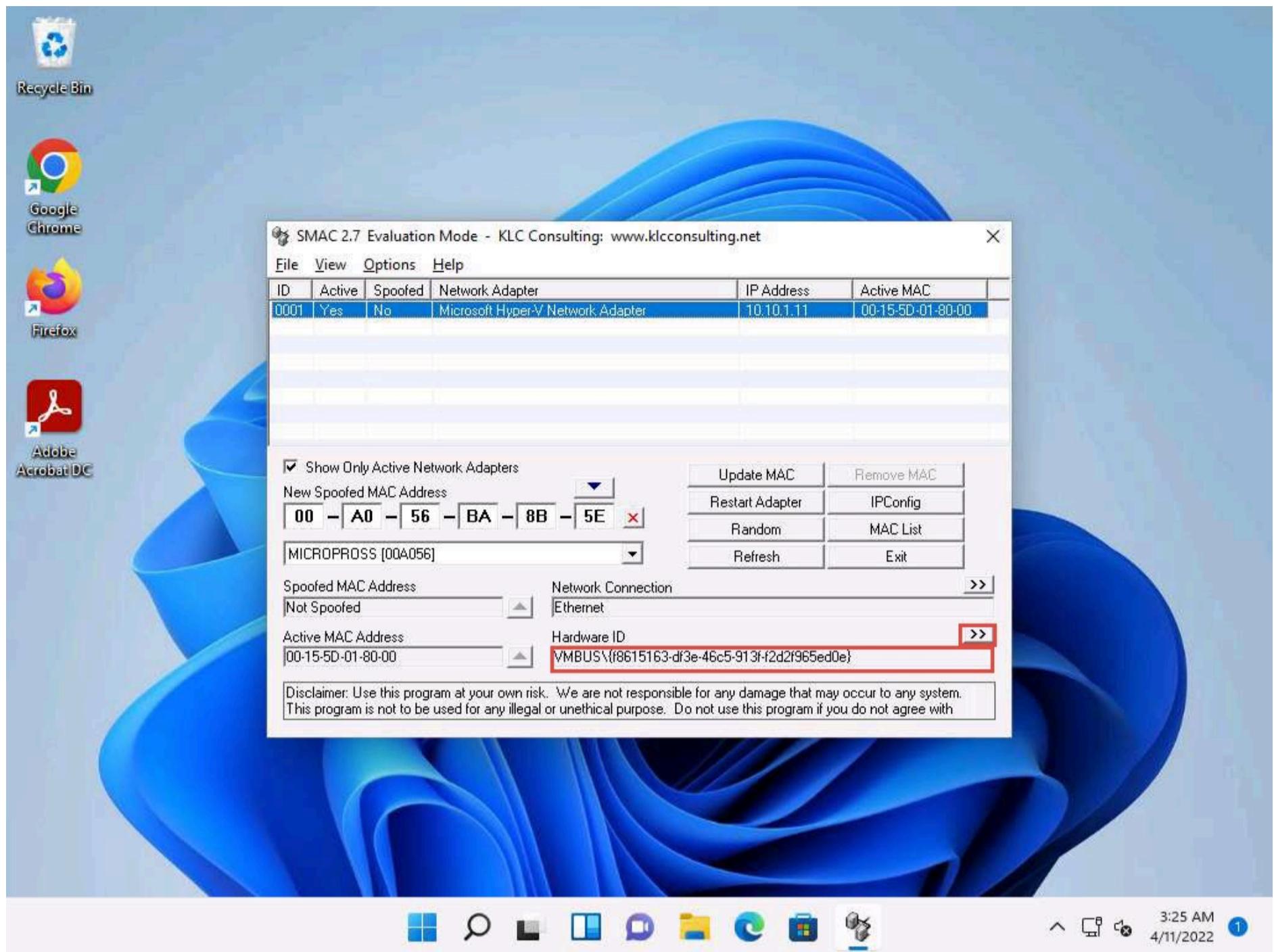
18. Click the forward arrow button (>>) under **Network Connection** to view the **Network Adapter** information.



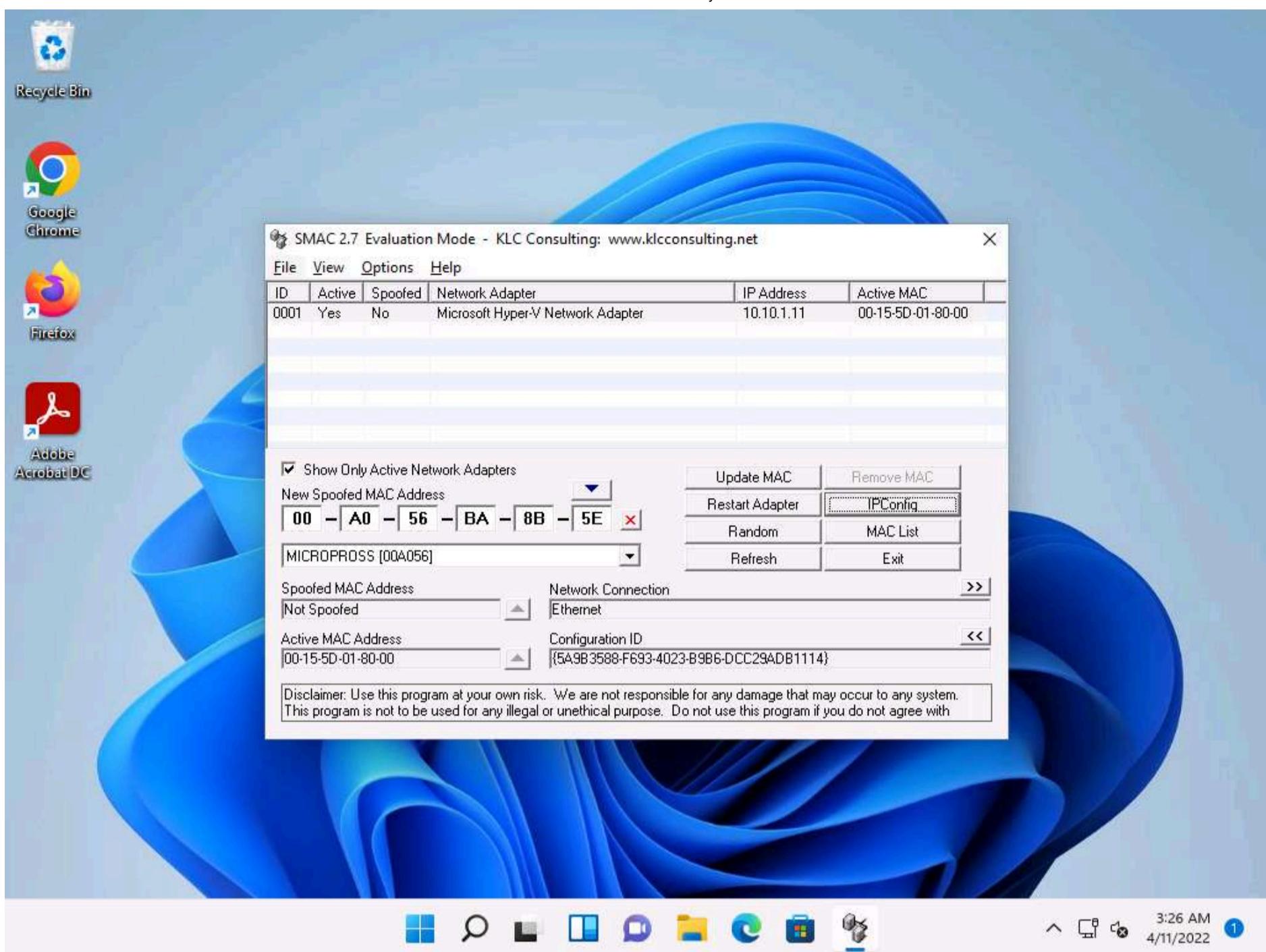
19. Clicking the back arrow (<<) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.



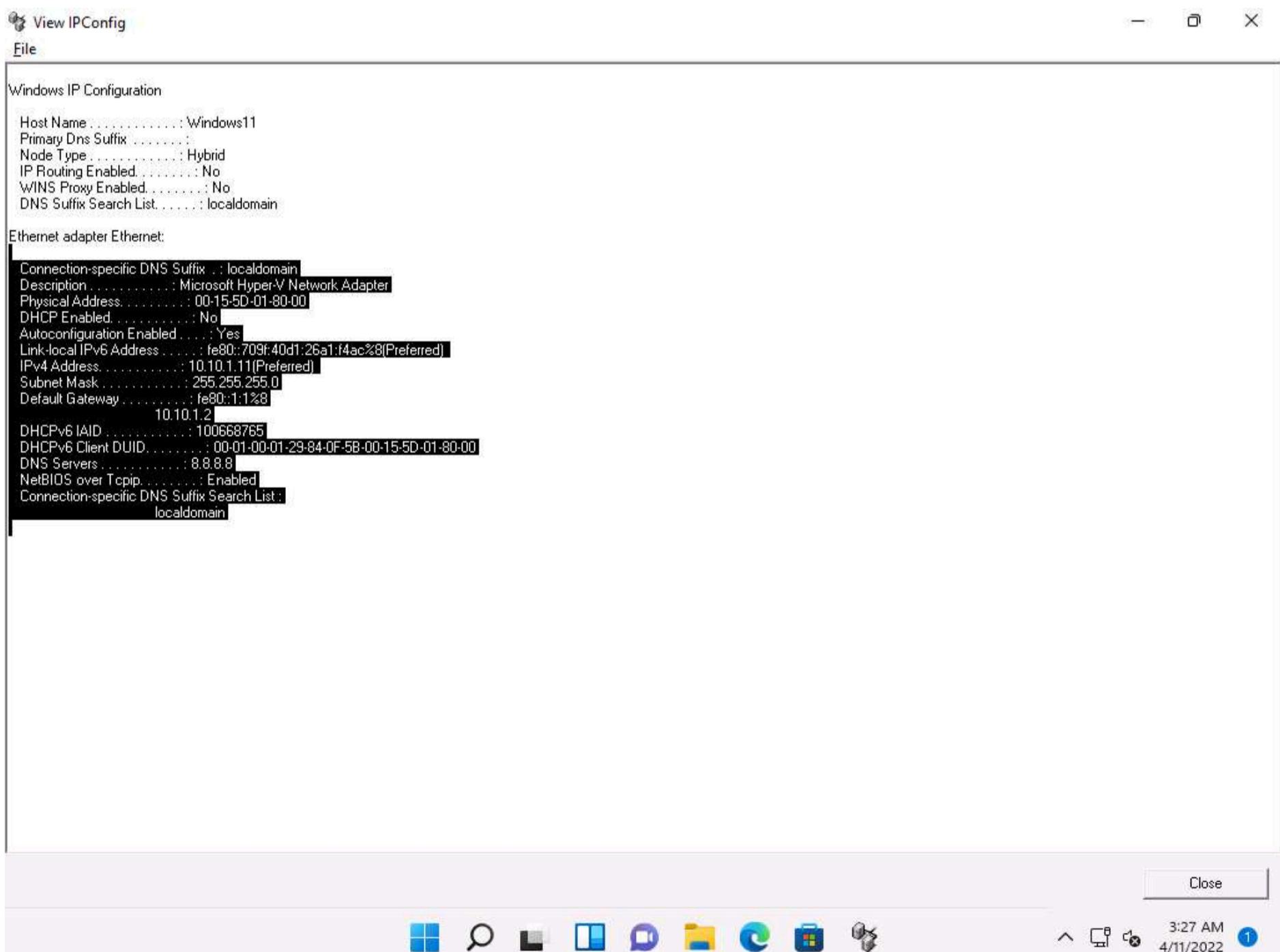
20. Similarly, you can click the forward arrow button (>>) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (<<) to toggle back to **Hardware ID** information.



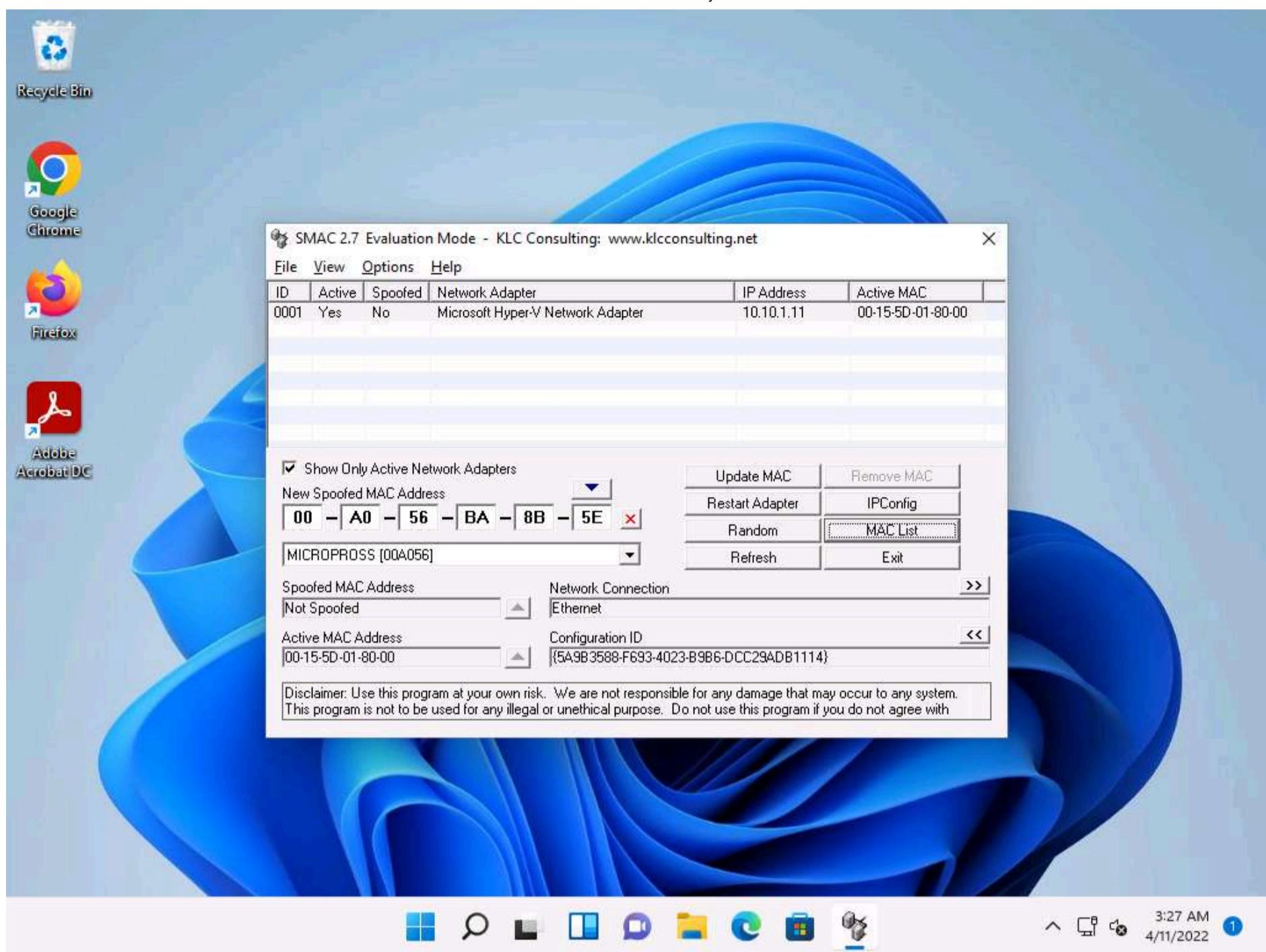
21. Click the **IPConfig** button to view the ipconfig information.



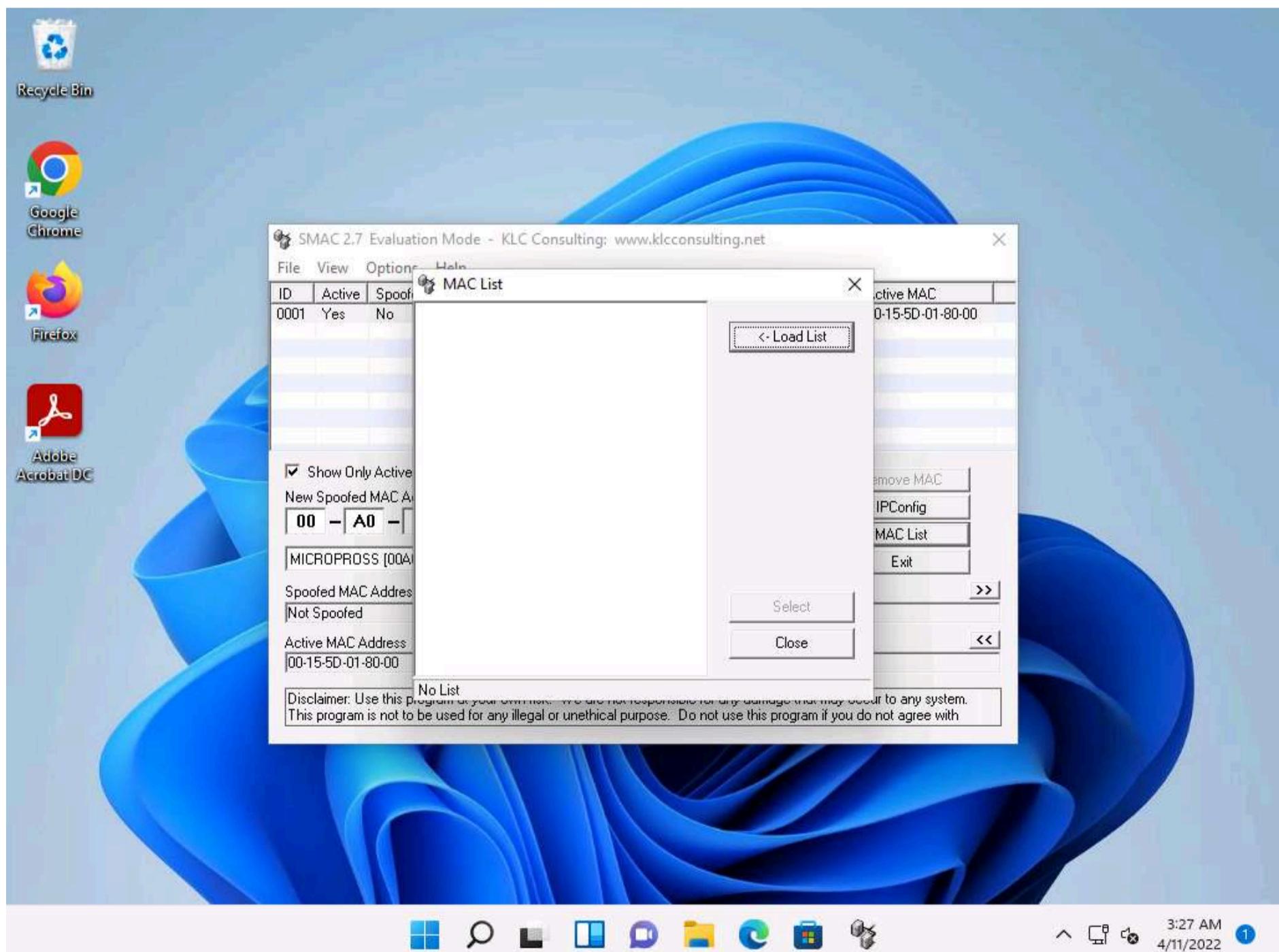
22. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.



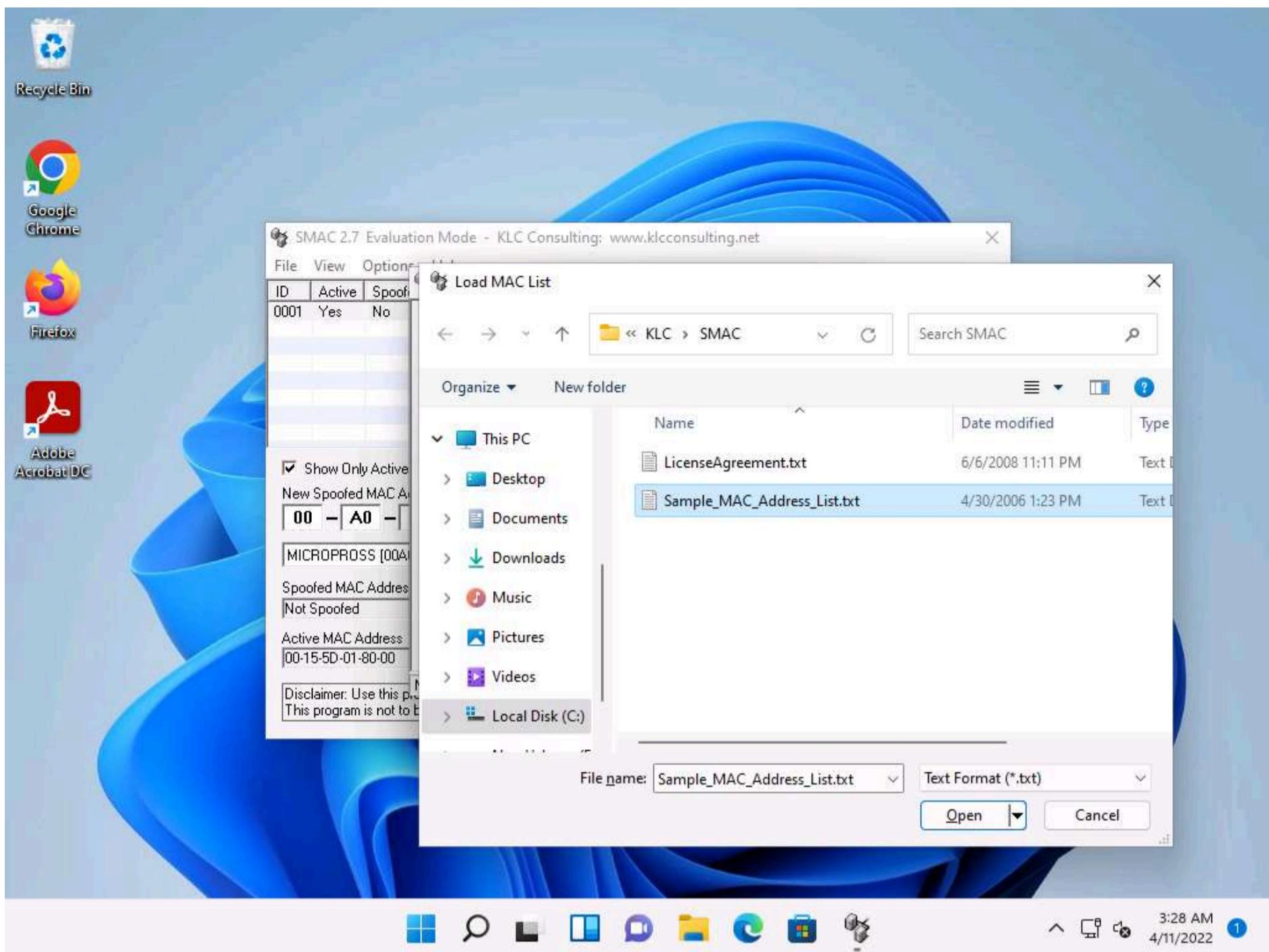
23. Click the **MAC List** button to import the MAC address list into SMAC.



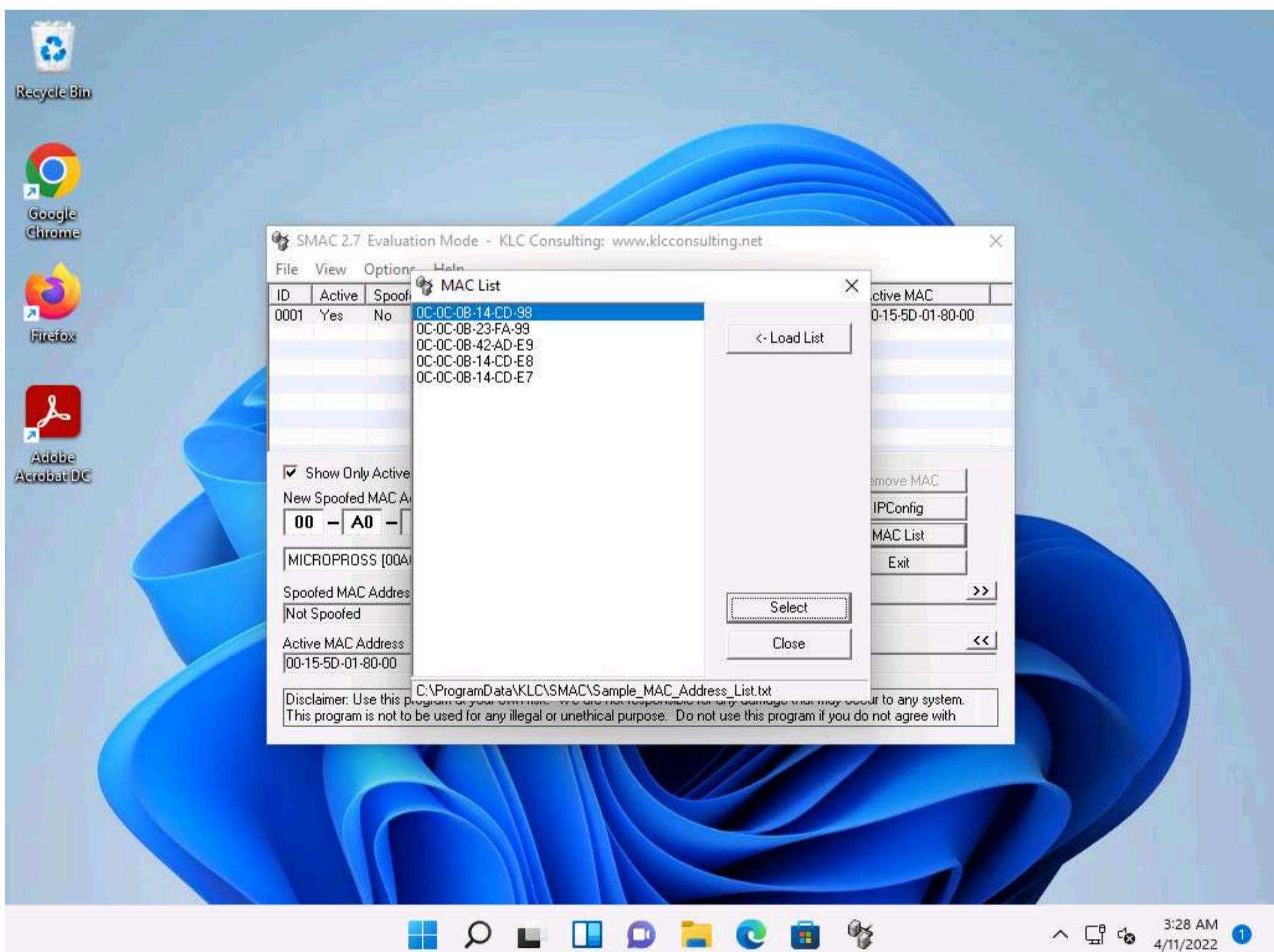
24. The **MAC List** window appears; click the **Load List** button.



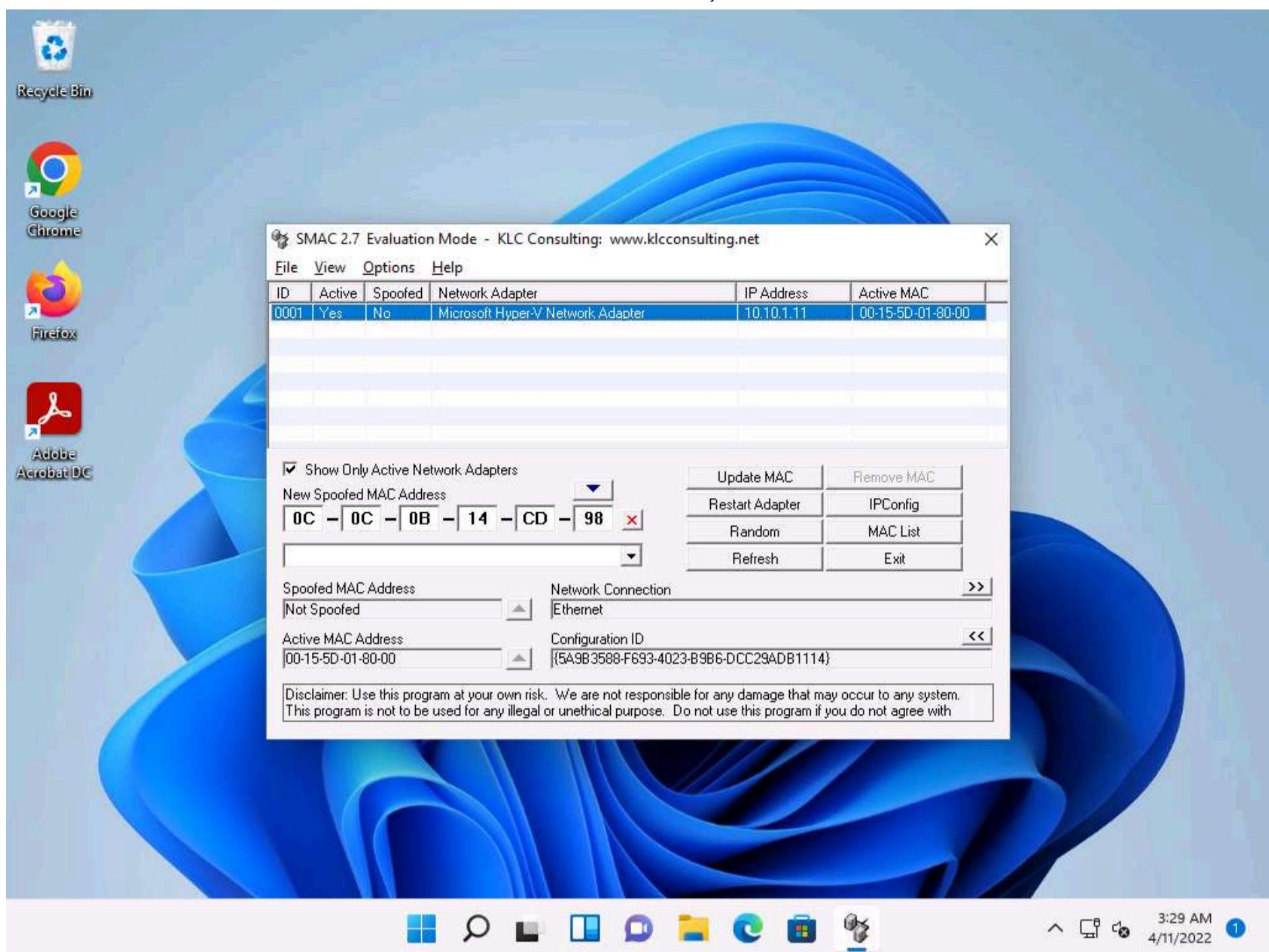
25. The **Load MAC List** window appears; select the **Sample\_MAC\_Address\_List.txt** file and click **Open**.



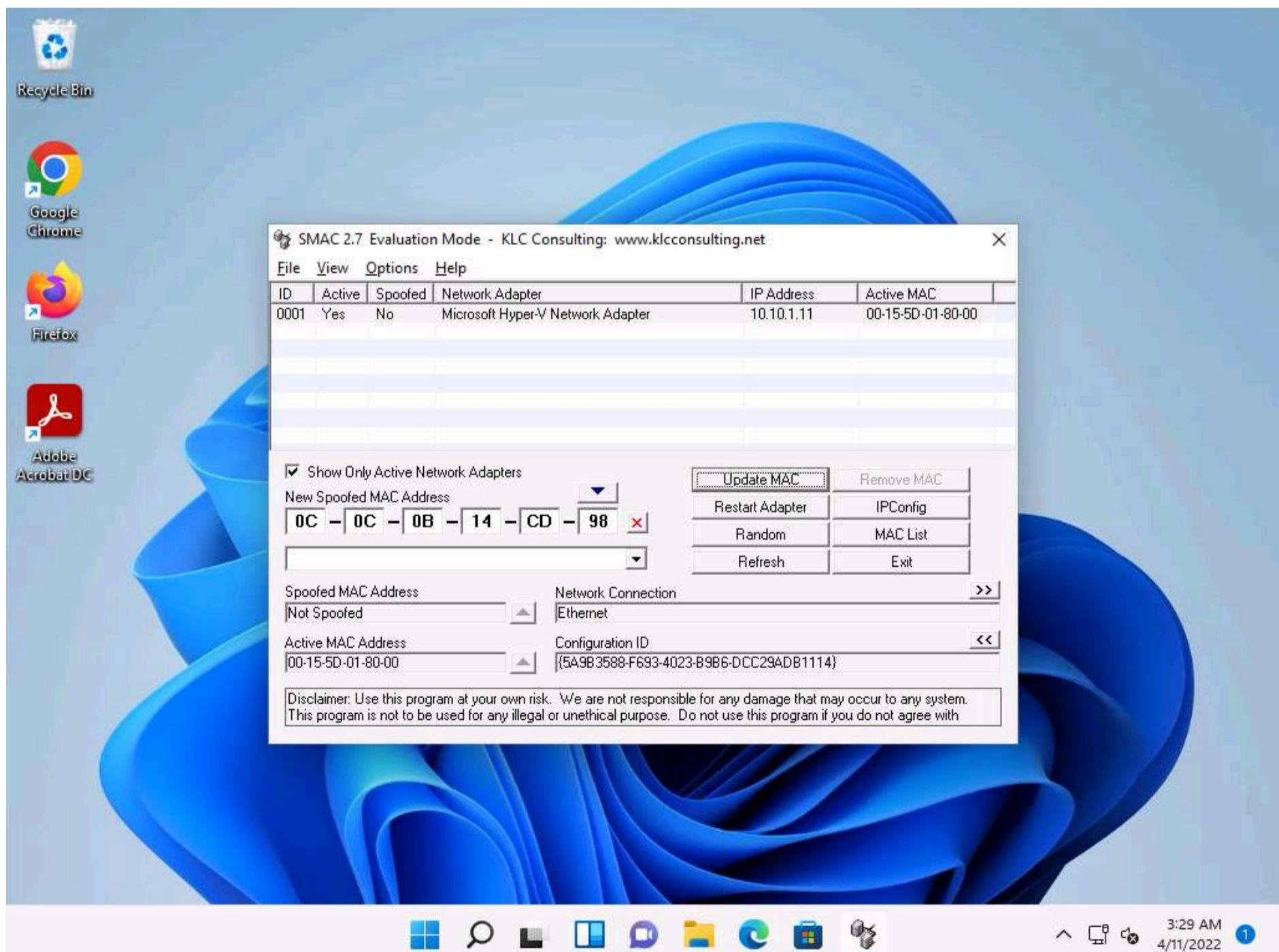
26. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.



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



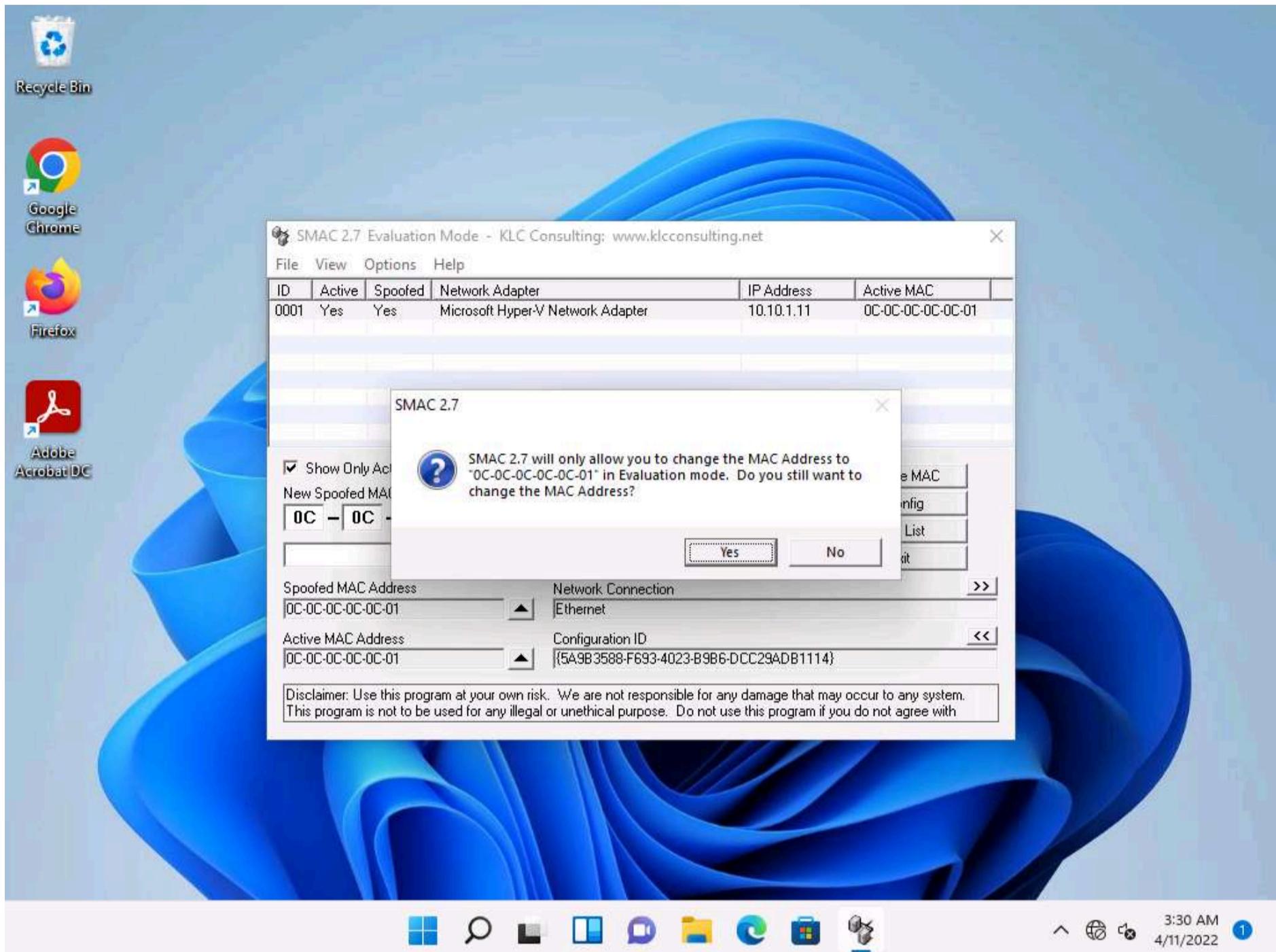
28. Click the **Update MAC** button to update the machine's MAC address information.



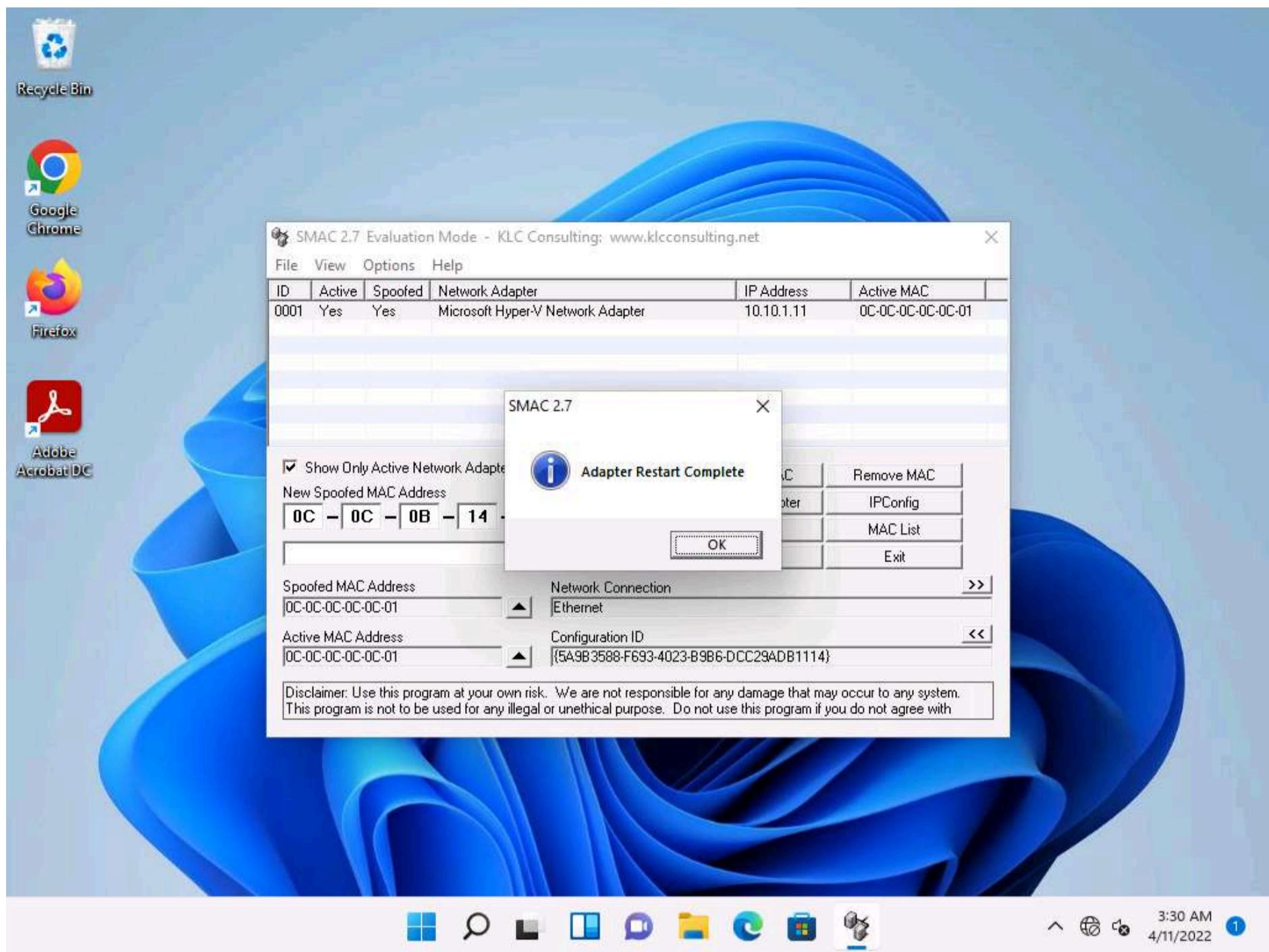
29. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

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

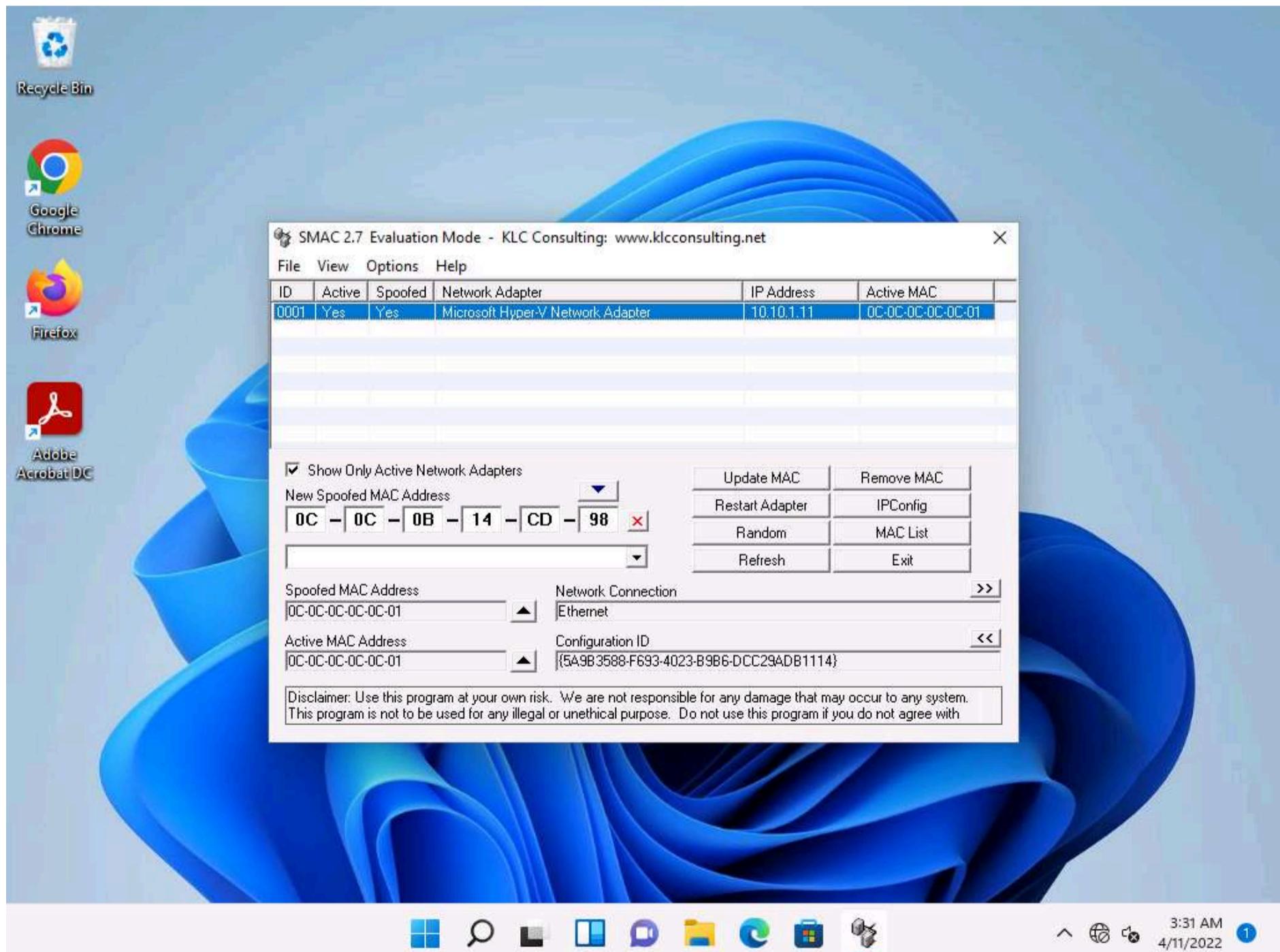
Note: In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.



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.

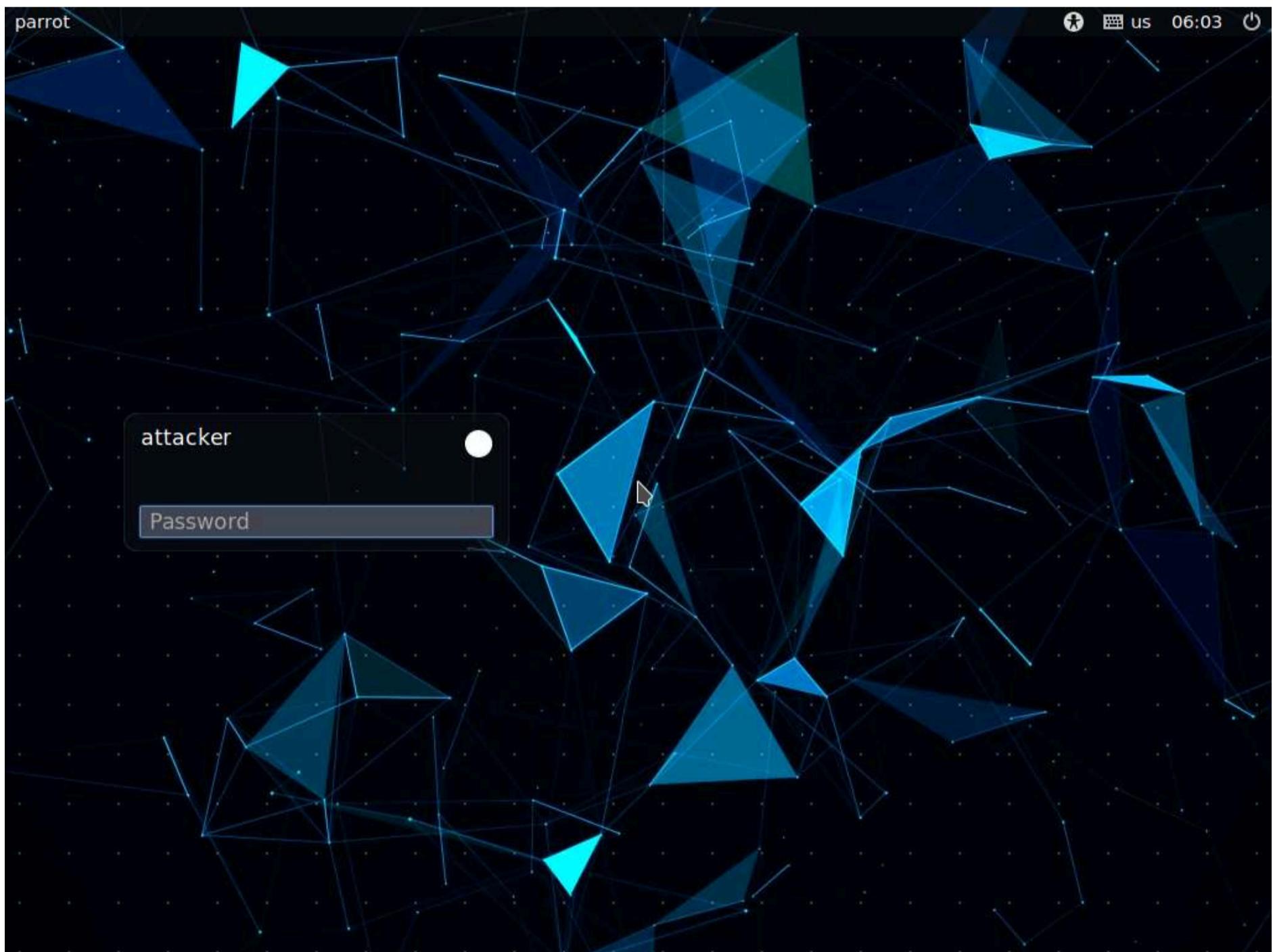
34. Close all open windows and document all the acquired information.

## 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 controller). However many drivers allow the MAC address to be changed. Some tools can make the operating system believe that the NIC has the MAC address of user's choice. Masking of the MAC address is known as MAC spoofing and involves changing the computer's identity. MAC spoofing can be performed using numerous tools.

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

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

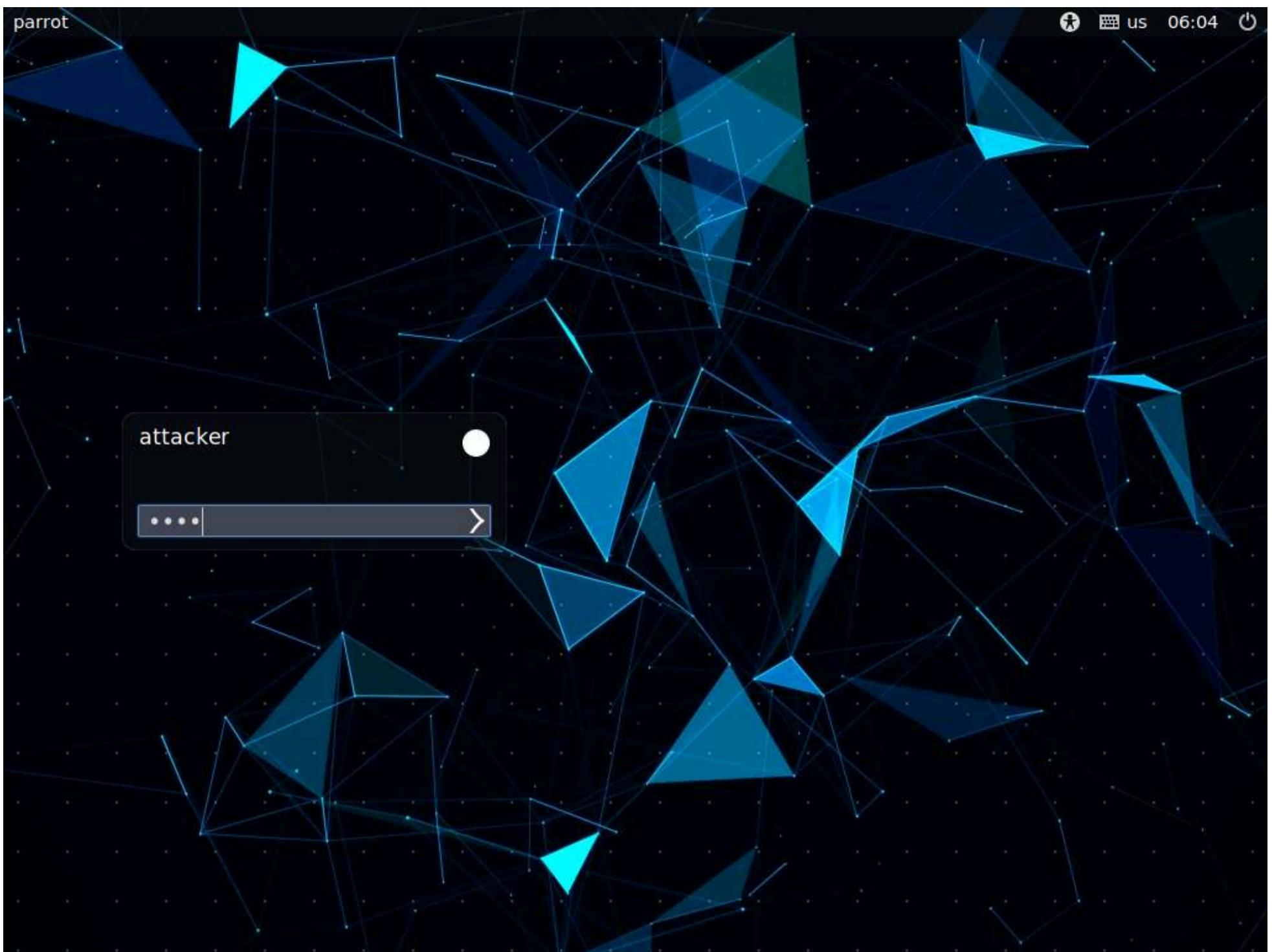


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

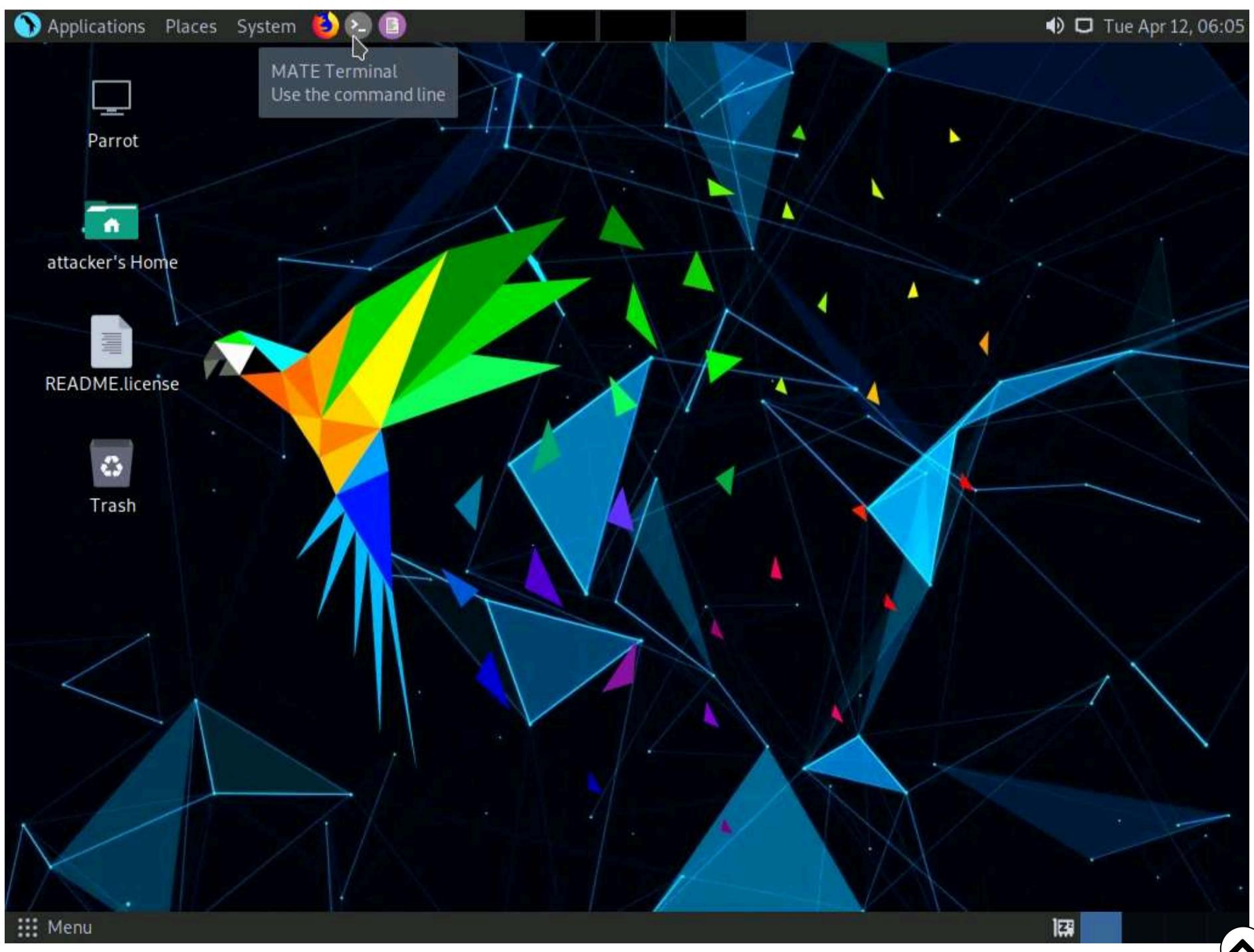
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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.

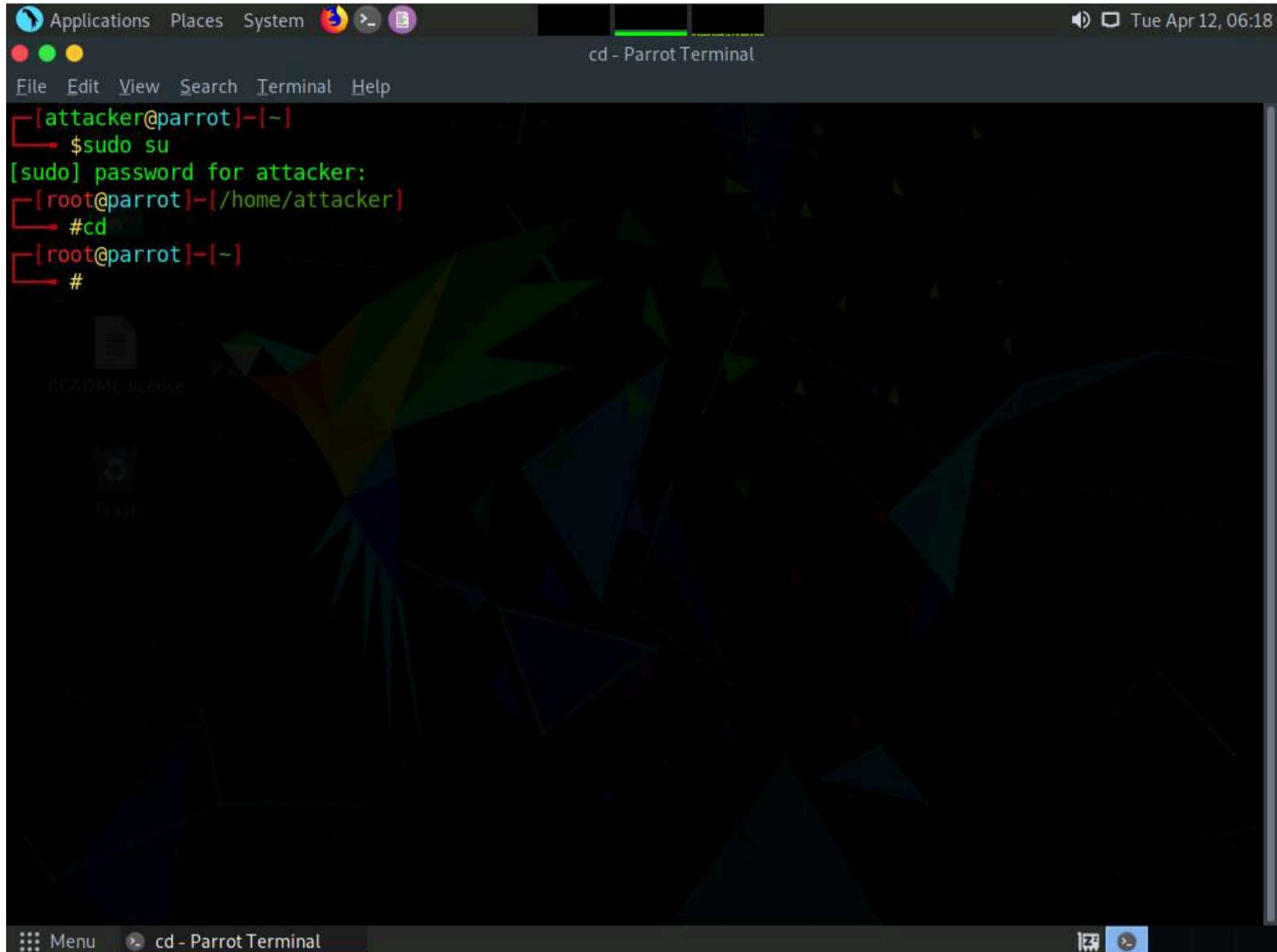


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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.



```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~(/home/attacker)
└─#cd
[root@parrot]~[-]
└─#
```

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.



The screenshot shows a terminal window titled "ifconfig eth0 down - Parrot Terminal". The terminal session starts with the user "attacker" at the root prompt. The user runs "sudo su" to become root, then changes to the home directory of the attacker user, and finally runs the command "#ifconfig eth0 down". The terminal has a dark background with a green and blue geometric pattern. The title bar and menu bar are visible at the top.

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

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

The screenshot shows a terminal window titled "macchanger --help - Parrot Terminal". The user has already run the "ifconfig eth0 down" command. Now, they type "#macchanger --help" and press Enter. The terminal displays the help documentation for the macchanger tool, listing various options and their descriptions. The terminal window has a dark background with a green and blue geometric pattern.

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

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

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

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

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

The terminal window shows the following session:

```
[sudo] password for attacker:  
[root@parrot]~[/home/attacker]  
[root@parrot]#cd  
[root@parrot]~[-]  
[root@parrot]#ifconfig eth0 down  
[root@parrot]~[-]  
[root@parrot]#macchanger --help  
GNU MAC Changer  
Usage: macchanger [options] device  
  
-h, --help          Print this help  
-V, --version       Print version and exit  
-s, --show          Print the MAC address and exit  
-e, --ending         Don't change the vendor bytes  
-a, --another        Set random vendor MAC of the same kind  
-A                  Set random vendor MAC of any kind  
-p, --permanent     Reset to original, permanent hardware MAC  
-r, --random         Set fully random MAC  
-l, --list[=keyword] Print known vendors  
-b, --bia            Pretend to be a burned-in-address  
-m, --mac=XX:XX:XX:XX:XX:XX  
      --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX  
  
Report bugs to https://github.com/alobbs/macchanger/issues  
[root@parrot]~[-]  
[root@parrot]#macchanger -s eth0  
Current MAC: 02:15:5d:26:62:a6 (unknown)  
Permanent MAC: 02:15:5d:26:62:a6 (unknown)  
[root@parrot]~[-]  
[root@parrot]#
```

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

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

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

```
[root@parrot]~[-]
└─#macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

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

Report bugs to https://github.com/alobbs/macchanger/issues
```

[root@parrot]~[-]
└─#macchanger -s eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)

[root@parrot]~[-]
└─#macchanger -a eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
New MAC: 00:30:a0:27:e2:f1 (TYCO SUBMARINE SYSTEMS, LTD.)

[root@parrot]~[-]
└─#

Click to switch to "Workspace 3"

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

```
[root@parrot]~[-]
└─#macchanger -r eth0
Current MAC: 00:30:a0:27:e2:f1 (TYCO SUBMARINE SYSTEMS, LTD.)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
New MAC: da:ef:95:36:55:44 (unknown)
```

[root@parrot]~[-]
└─#

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

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

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

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

[~]#
```

16. You can observe that a random MAC address is set to the network interface.

17. This concludes the demonstration of how to spoof a MAC address of Linux machine using macchanger

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

19. 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

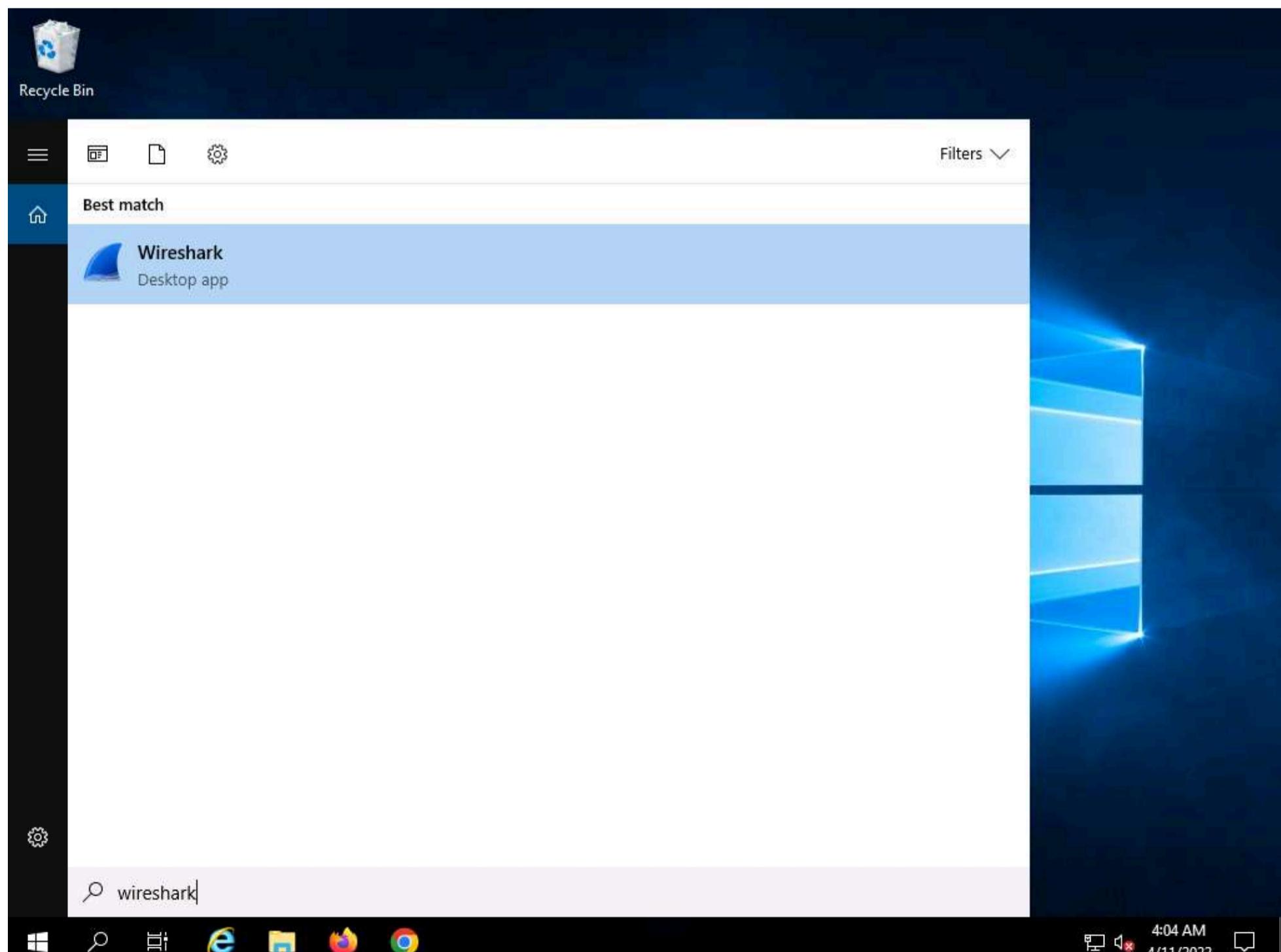
Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI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

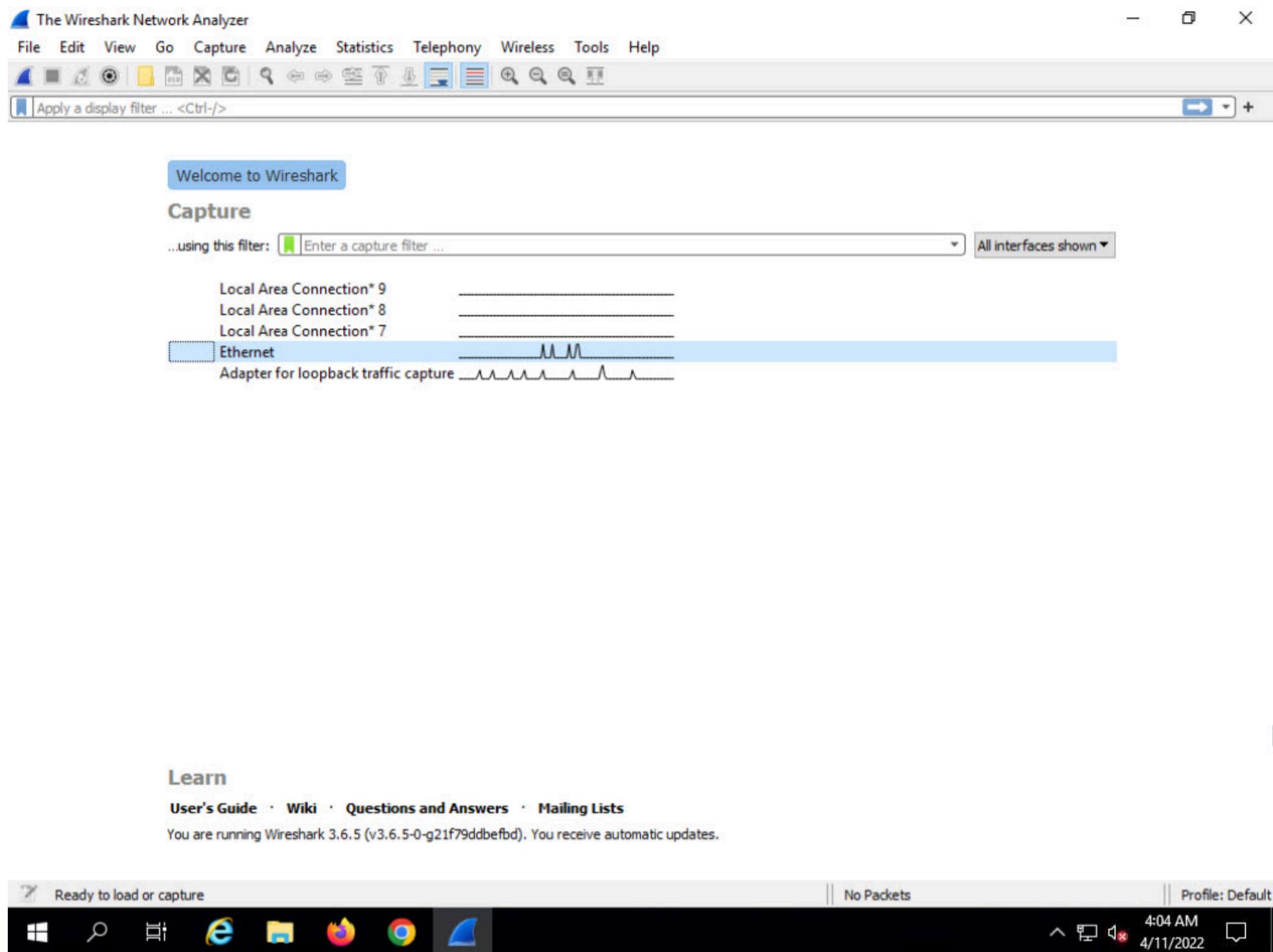
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
3. Click the **Type here to search**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

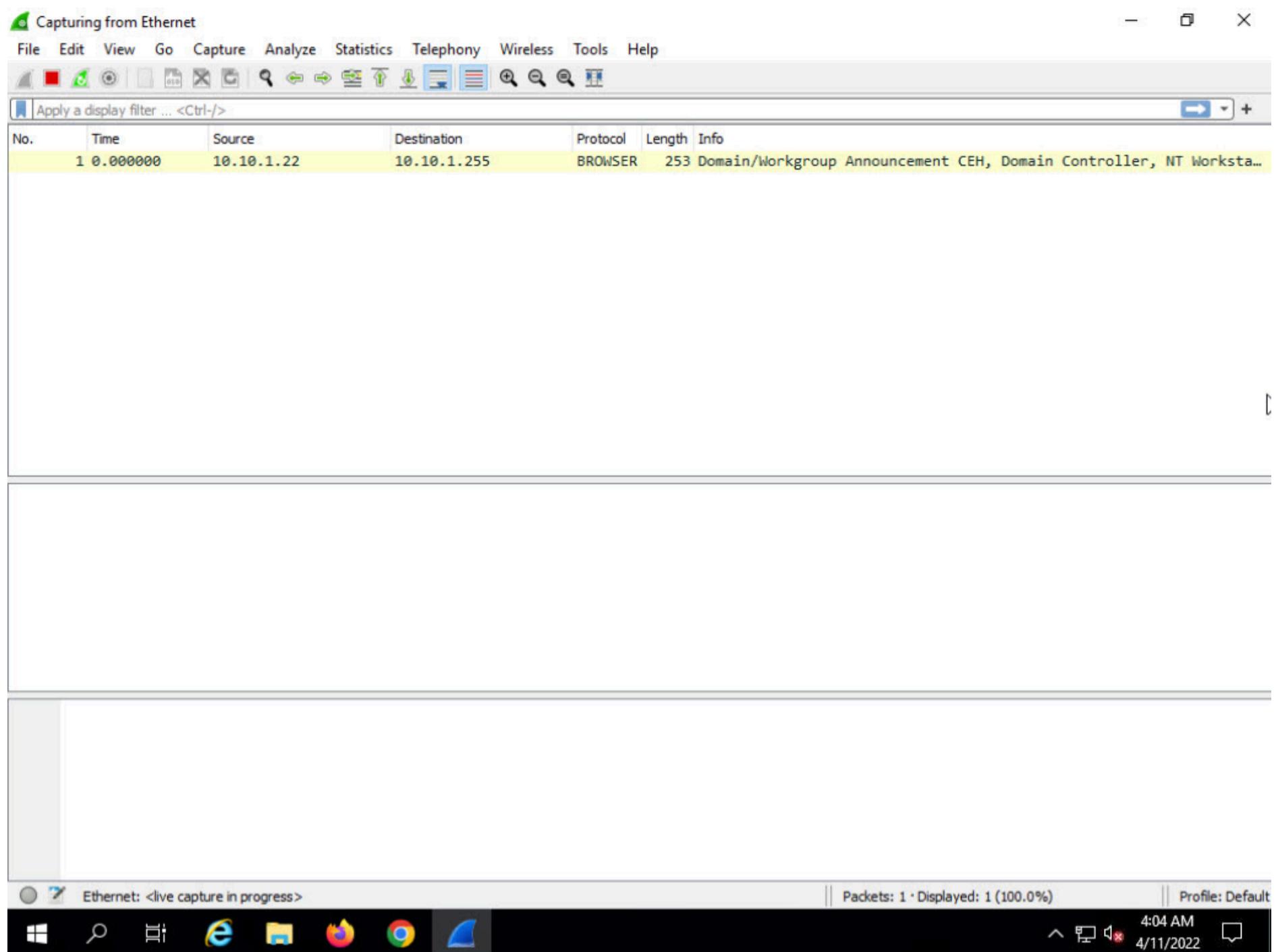


4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

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.



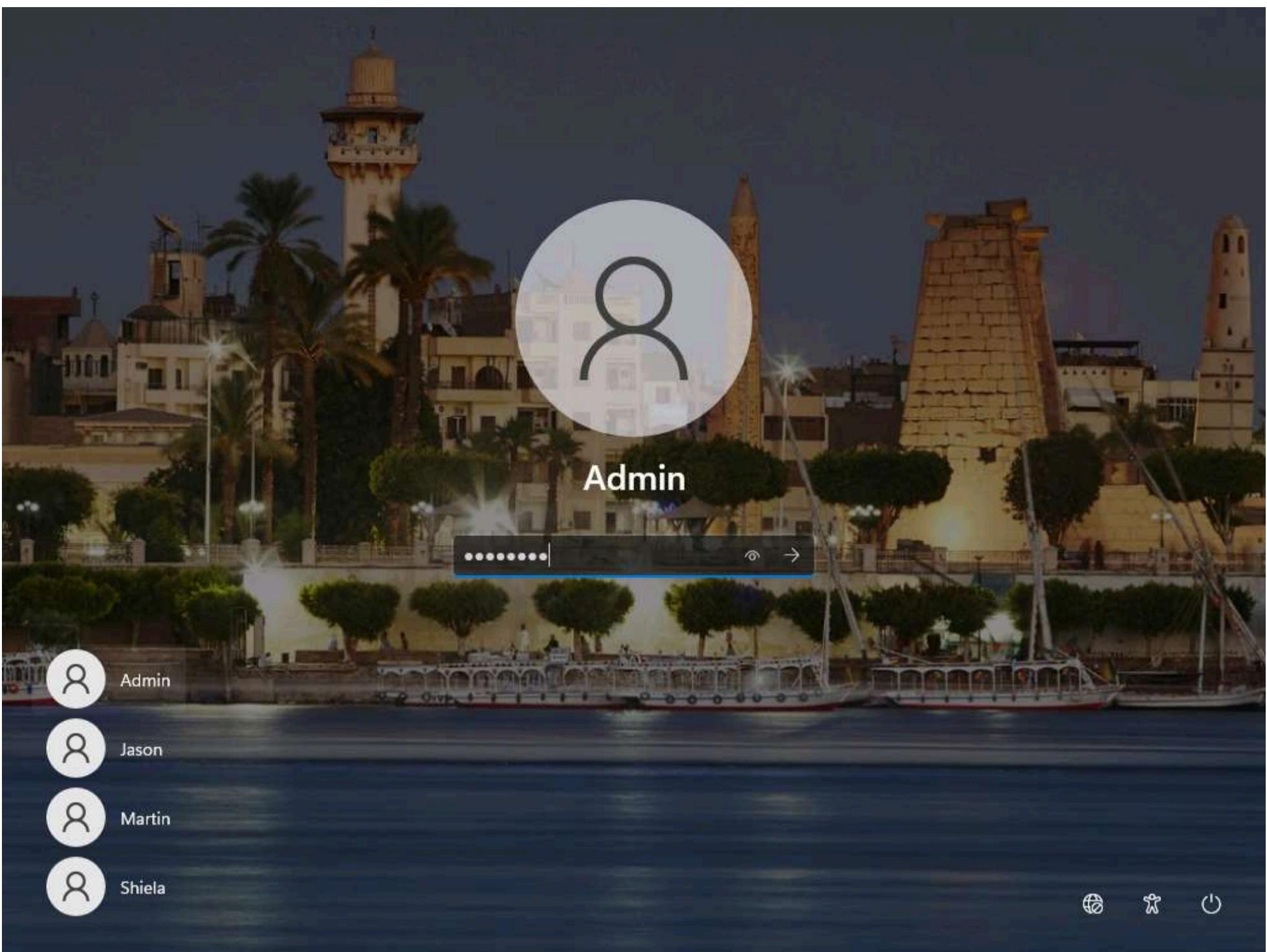
6. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**.

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

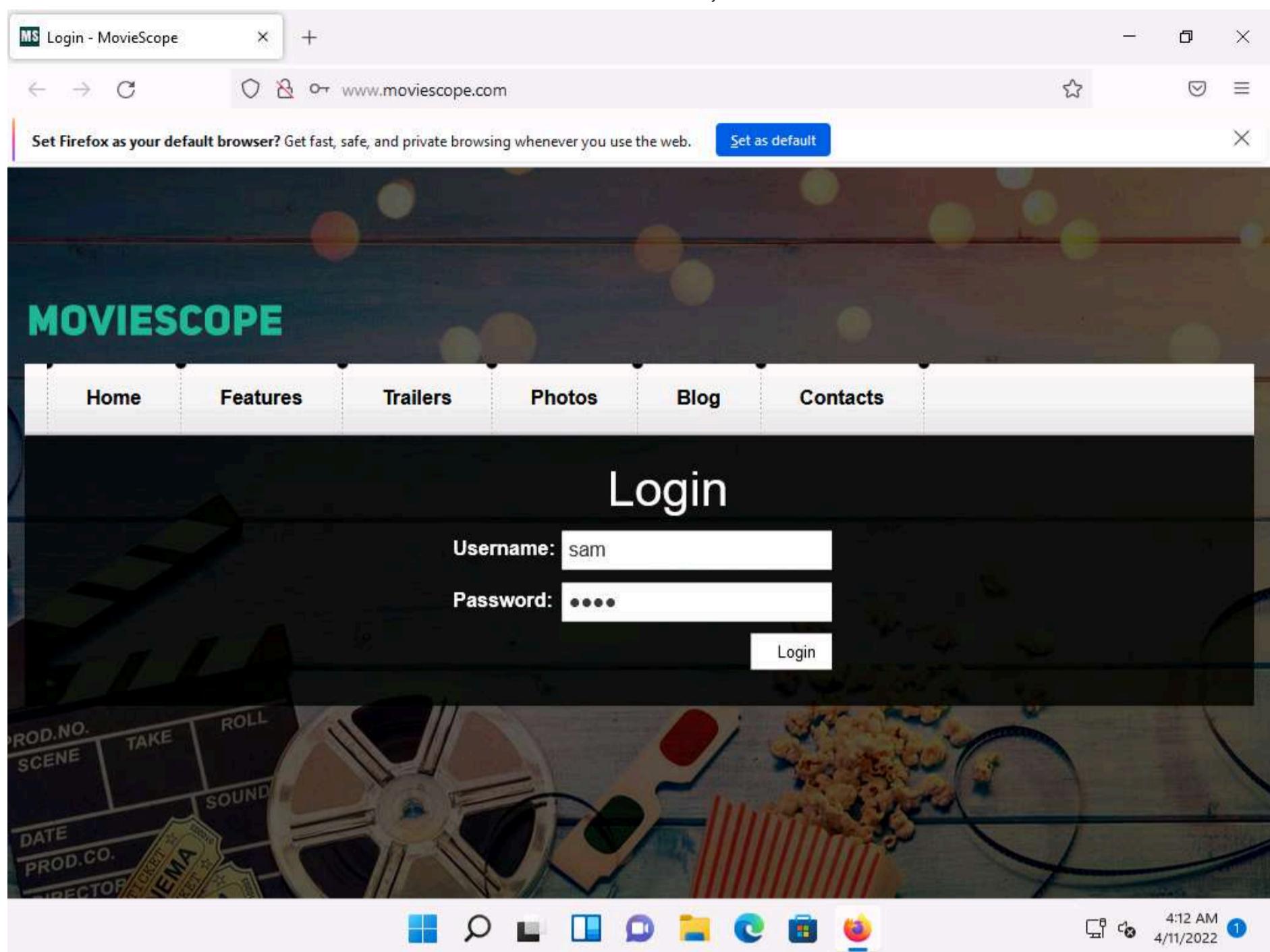
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

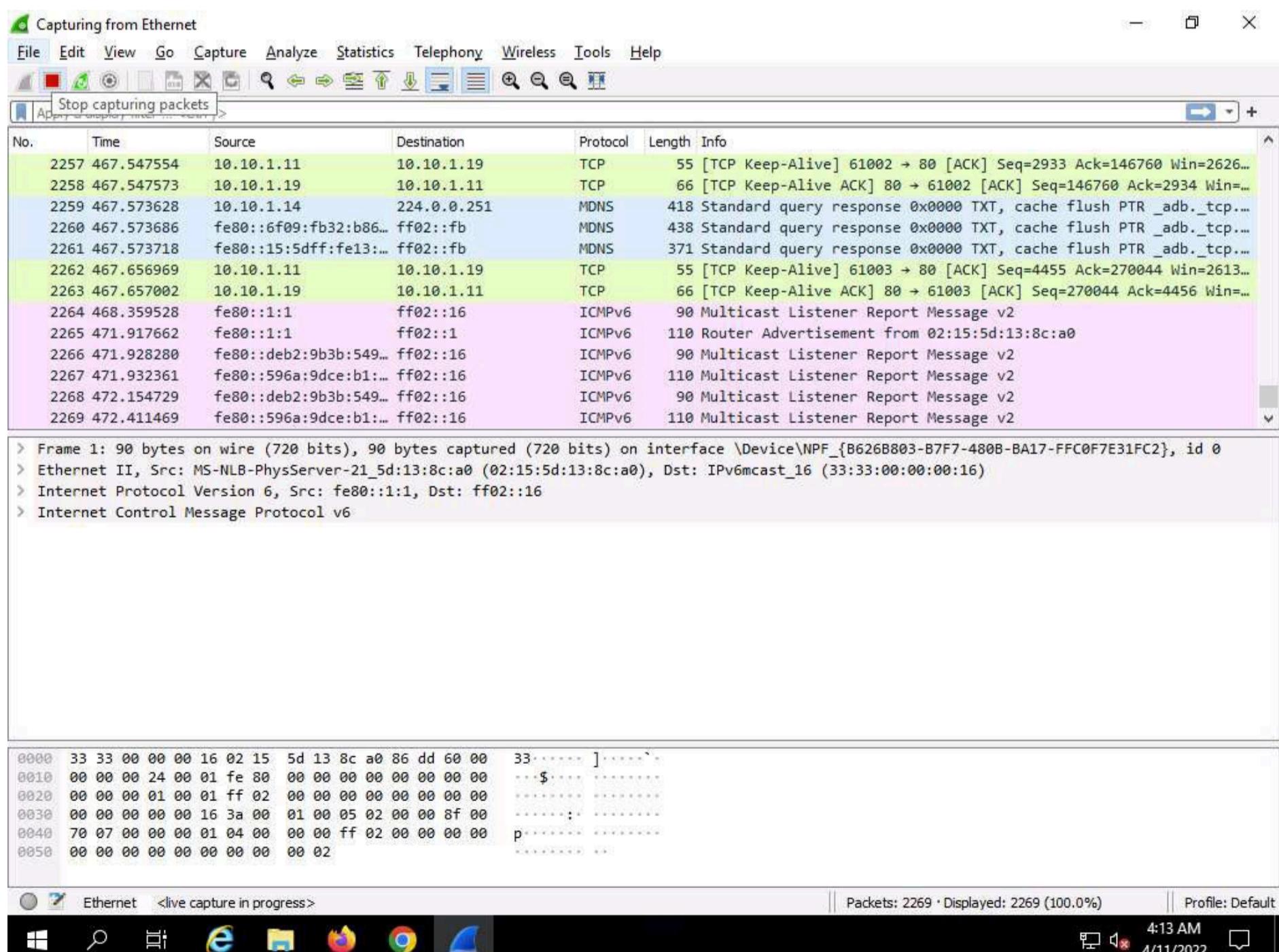




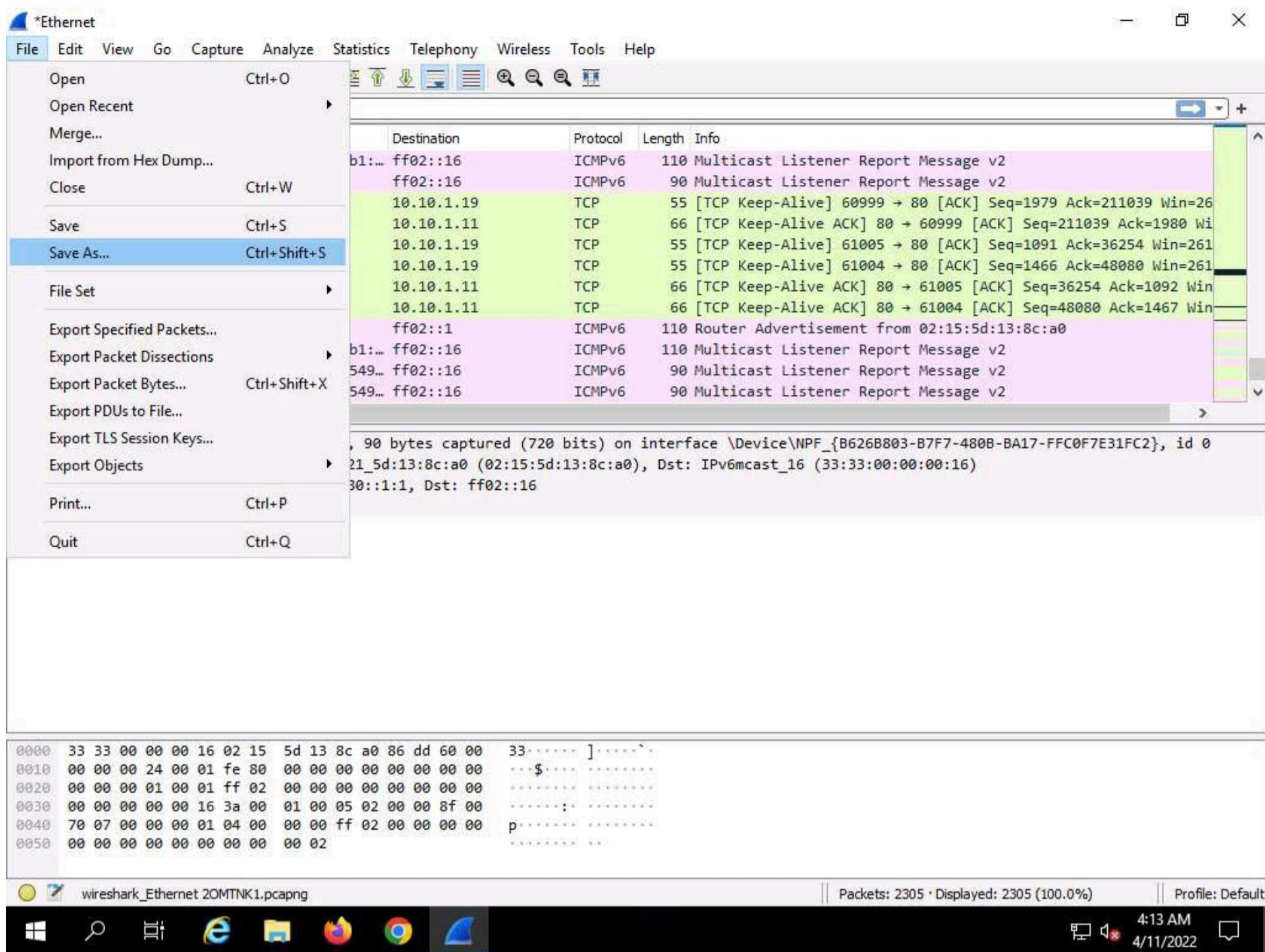
8. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on <http://www.moviescope.com/> in the address bar, and press **Enter**.
9. The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in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



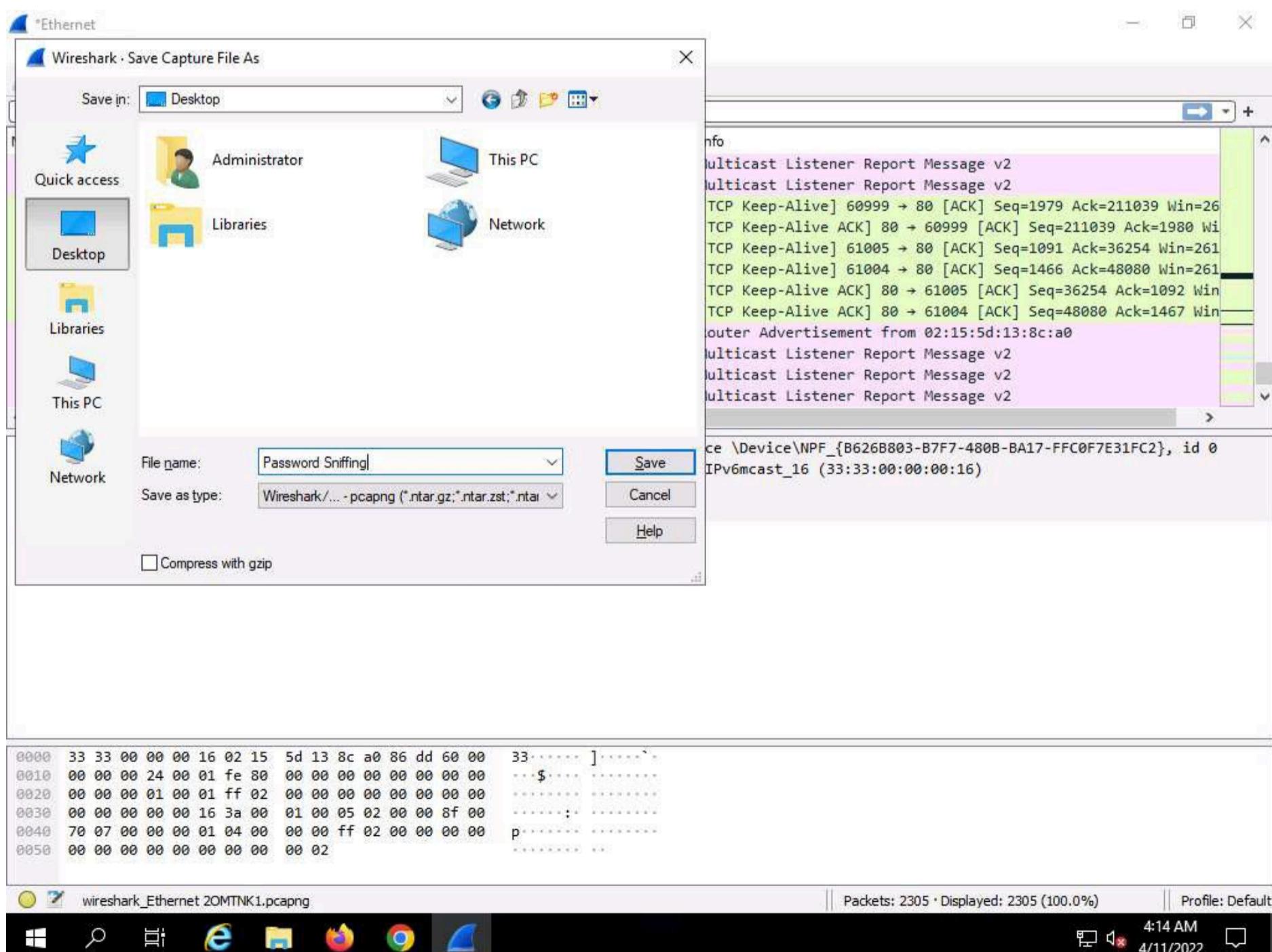
10. Click **CEHv12 Windows Server 2019** to switch back to **Windows Server 2019** machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.



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.

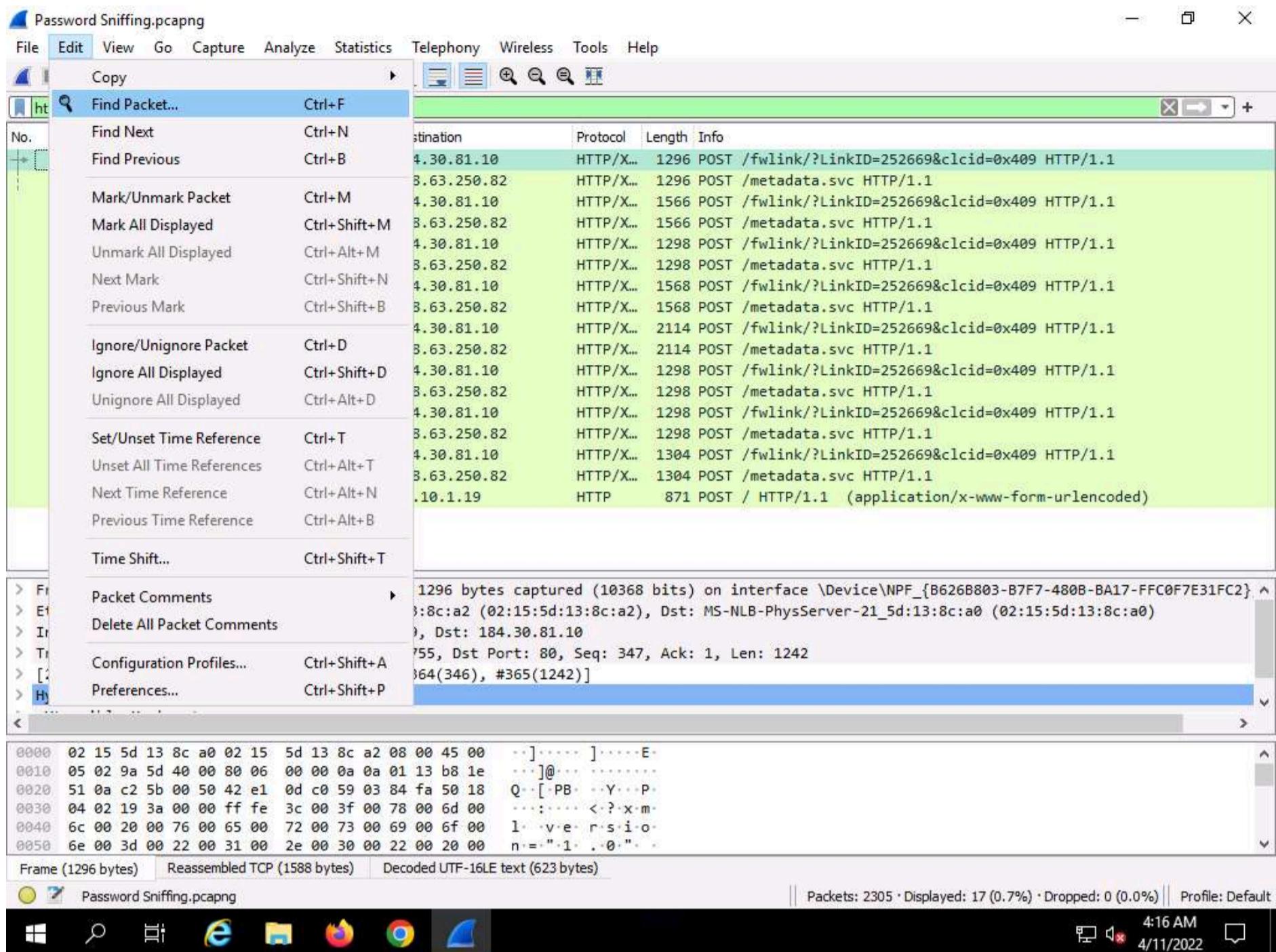
Note: Applying this syntax helps you narrow down the search for http POST traffic.

Wireshark screenshot showing captured traffic. A search filter 'http.request.method == POST' is applied, resulting in only 17 POST requests being displayed. The packet list shows various TCP and ICMPv6 frames, with the first few being Multicast Listener Report Message v2. The details and bytes panes show the captured data for each selected packet.

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

Wireshark screenshot showing captured traffic. A search filter 'http.request.method == POST' is applied, resulting in only 17 POST requests being displayed. The packet list shows various TCP and HTTP frames, with the first few being POST requests to fwlink and metadata.svc. The details and bytes panes show the captured data for each selected packet.

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.

Frame 365: 1296 bytes on wire (10368 bits), 1296 bytes captured (10368 bits) on interface \Device\NPF\_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2} ^

> Ethernet II, Src: MS-NLB-PhysServer-21\_5d:13:8c:a2 (02:15:5d:13:8c:a2), Dst: MS-NLB-PhysServer-21\_5d:13:8c:a0 (02:15:5d:13:8c:a0)

> Internet Protocol Version 4, Src: 10.10.1.19, Dst: 184.30.81.10

> Transmission Control Protocol, Src Port: 49755, Dst Port: 80, Seq: 347, Ack: 1, Len: 1242

> [2 Reassembled TCP Segments (1588 bytes): #364(346), #365(1242)]

> Hypertext Transfer Protocol

Frame (1296 bytes) | Reassembled TCP (1588 bytes) | Decoded UTF-16LE text (623 bytes)

Packets: 2305 · Displayed: 17 (0.7%) · Dropped: 0 (0.0%) · Profile: Default

4:17 AM 4/11/2022

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.

Frame 2064: 871 bytes on wire (6968 bits), 871 bytes captured (6968 bits) on interface \Device\NPF\_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}, id 0

> Ethernet II, Src: Microsoft\_01:80:00 (00:15:5d:01:80:00), Dst: MS-NLB-PhysServer-21\_5d:13:8c:a2 (02:15:5d:13:8c:a2)

> Internet Protocol Version 4, Src: 10.10.1.11, Dst: 10.10.1.19

> Transmission Control Protocol, Src Port: 60999, Dst Port: 80, Seq: 1, Ack: 1, Len: 817

> Hypertext Transfer Protocol

> HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "\_\_VIEWSTATE" = "/wEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ+BtsUZt5M/WlqLFqTSuNaq6G+46A4bz6/sM1"
- > Form item: "\_\_VIEWSTATEGENERATOR" = "C2EE9ABB"
- > Form item: "\_\_EVENTVALIDATION" = "/wEdAARJUub9rbp0xjNNNjxtMliRWMttrRuIi9aE3DBg1DcnOGGcP002LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfq070LdPacUhns...
- > Form item: "txtusername" = "sam"
- > Form item: "txtpwd" = "test"
- > Form item: "btnlogin" = "Login"

0030 04 02 c0 14 00 00 50 4f 53 54 20 2f 20 48 54 54 .....POST / HTTP/1.1

0040 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 P/1.1 Host: www

0050 2e 6d 6f 76 69 65 73 63 6f 70 65 2e 63 6f 6d 0d .moviesc ope.com.

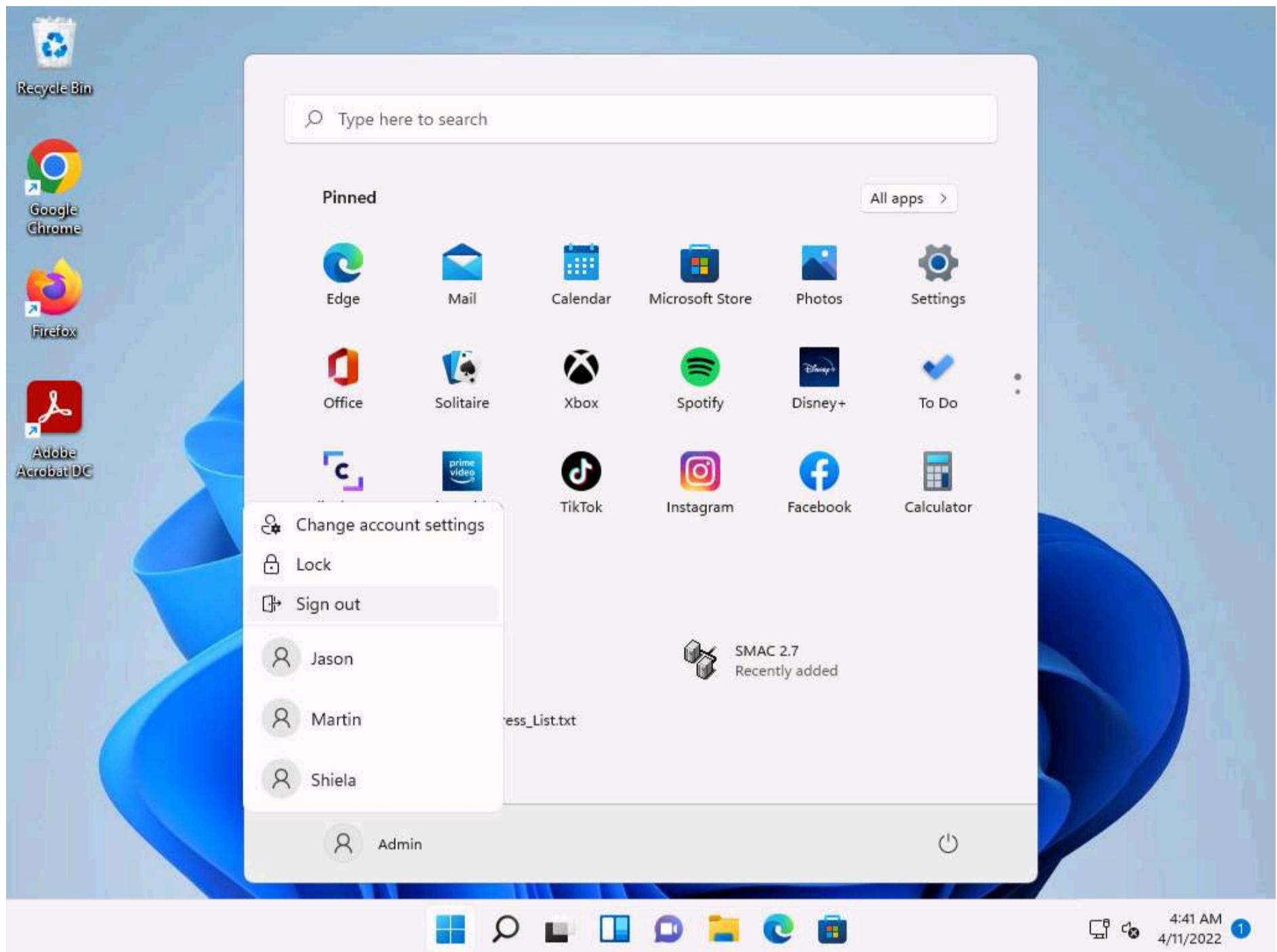
Hypertext Transfer Protocol (http), 493 bytes

Packets: 2305 · Displayed: 17 (0.7%) · Dropped: 0 (0.0%) · Profile: Default

4:28 AM 4/11/2022

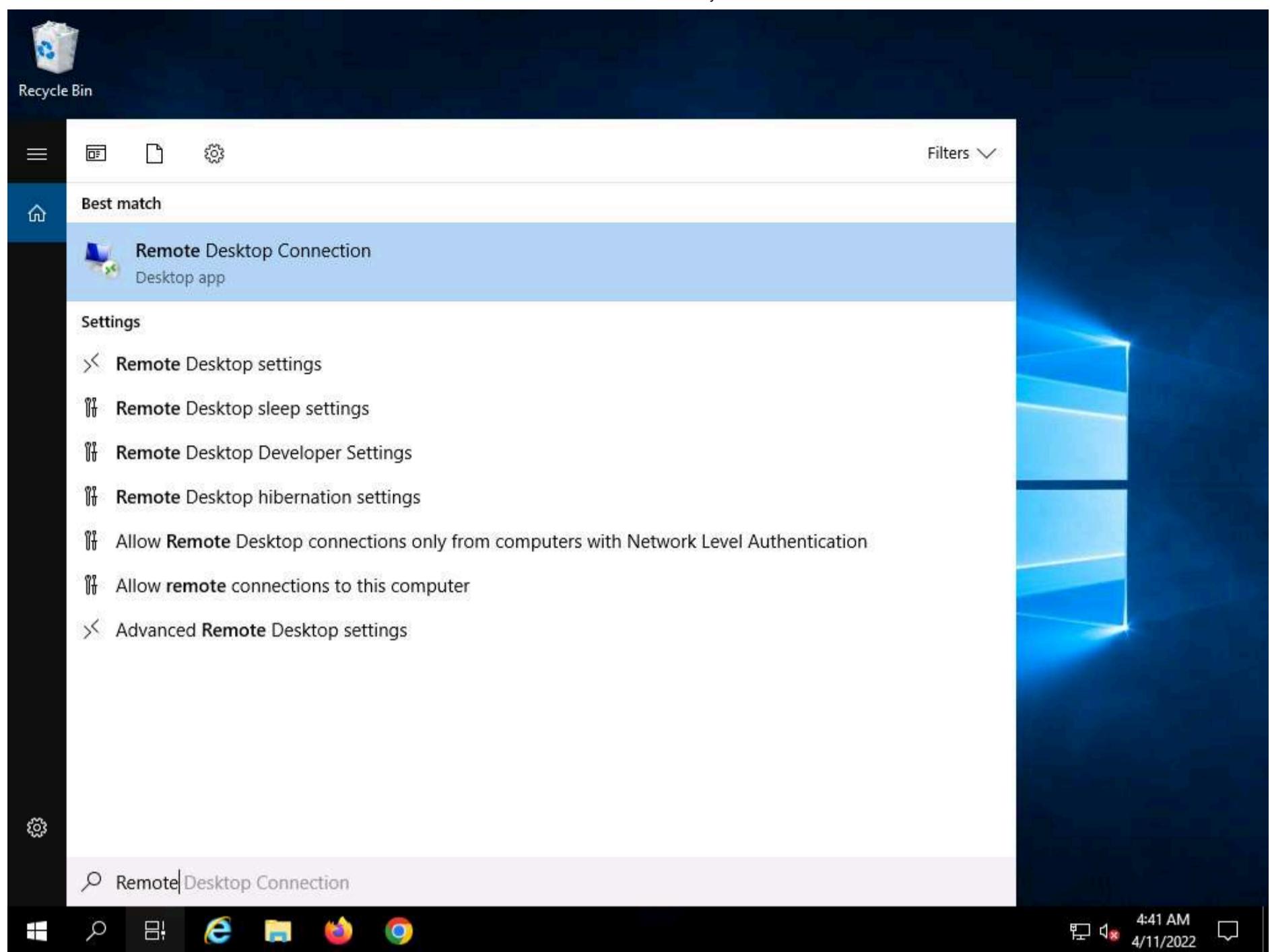
21. Close the **Wireshark** window.

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



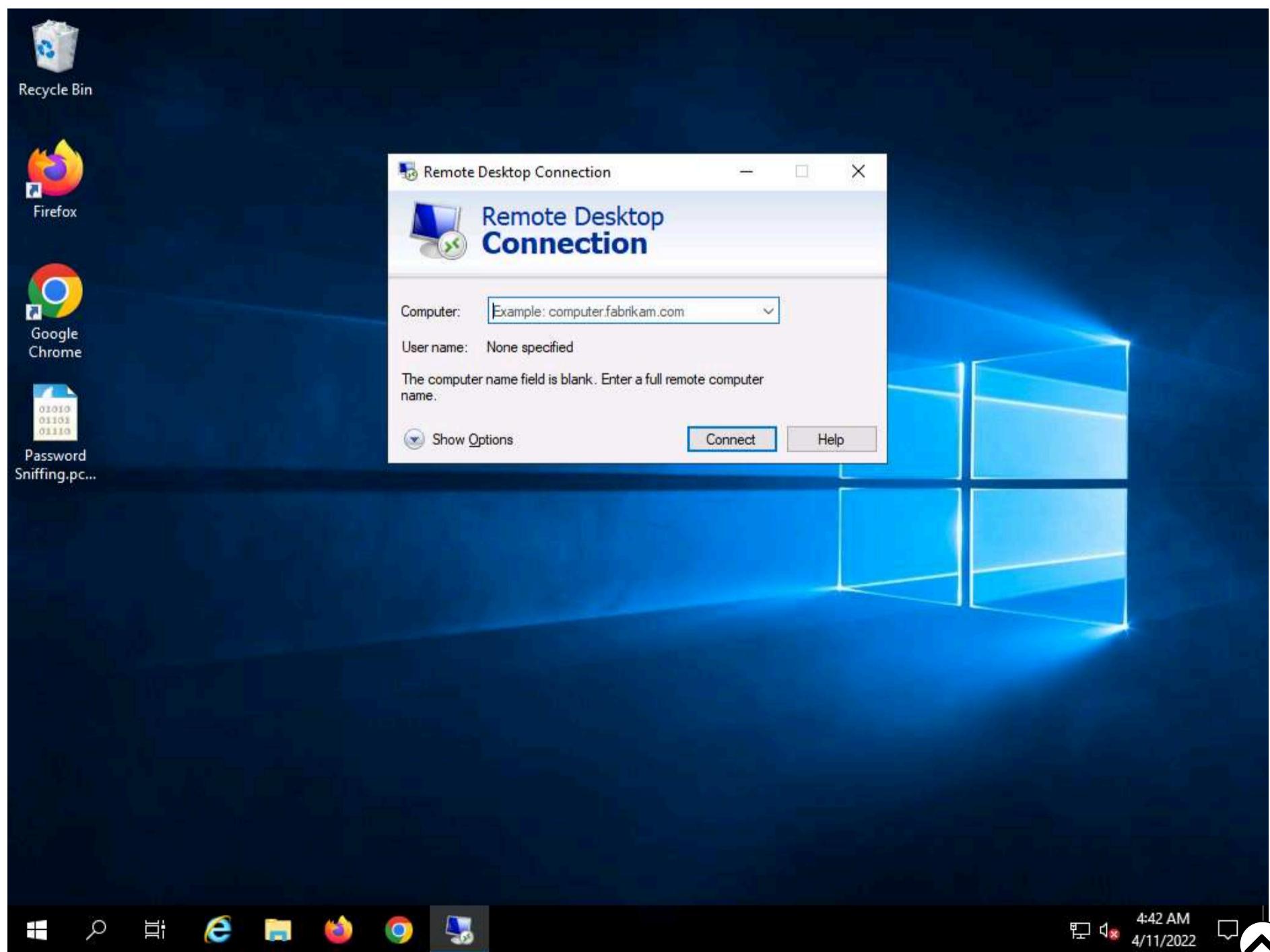
23. Click **CEHv12 Windows Server 2019** to switch back to the **Windows Server 2019** machine.

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



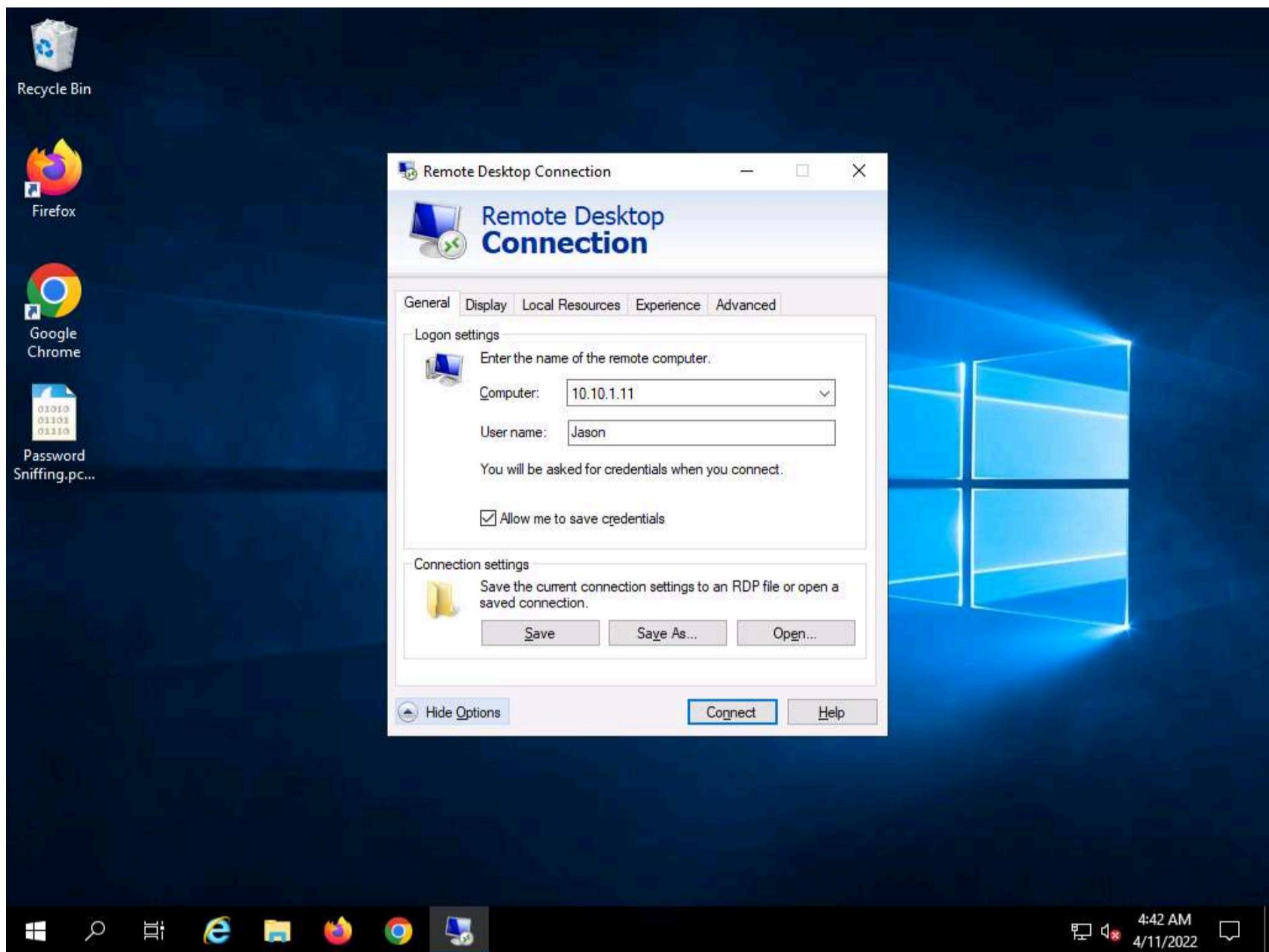
25. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

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**.

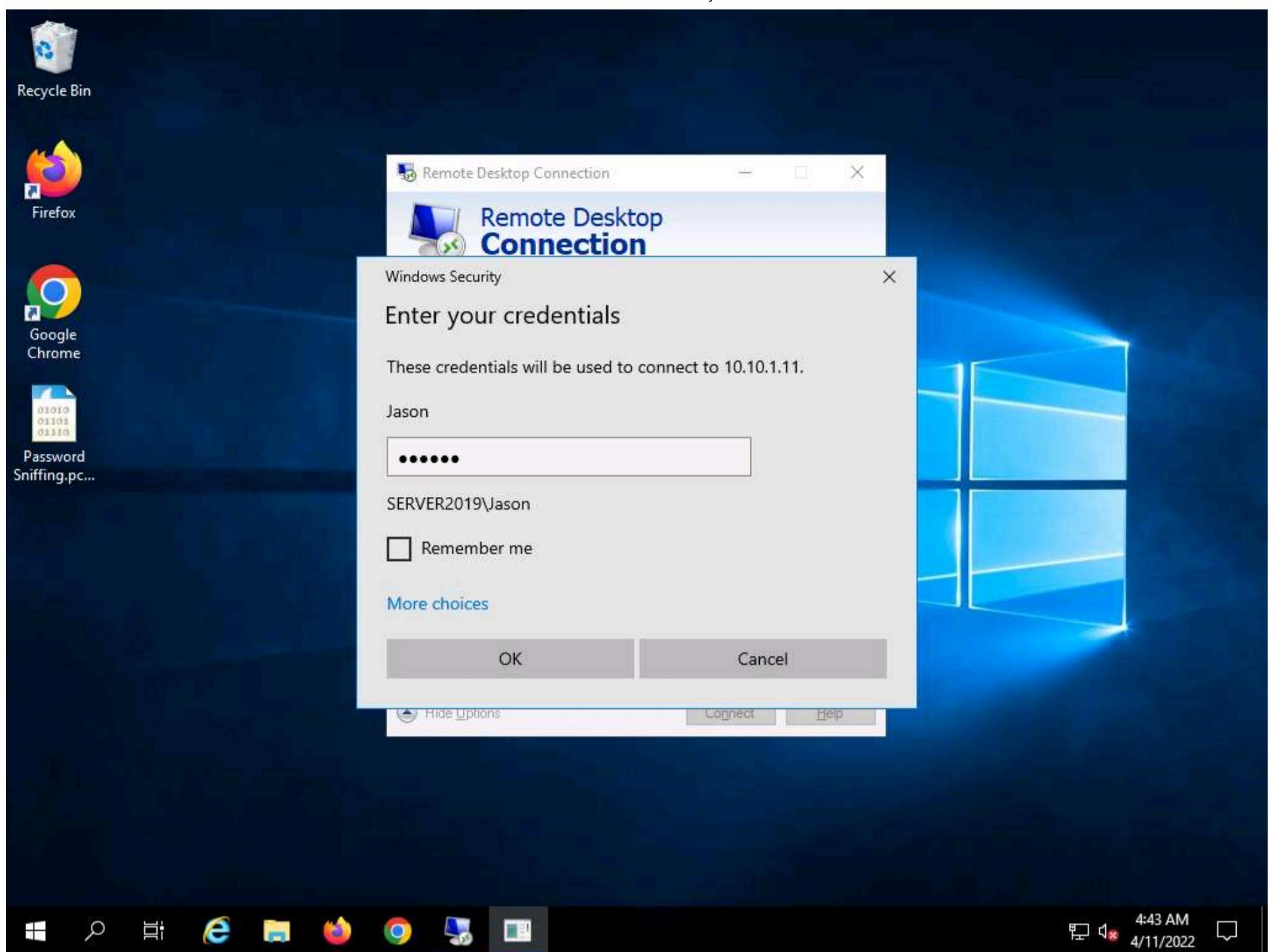
Note: The IP address and username might differ in your lab environment. The target system credentials (**Jason** and **qwerty**) we are using here are obtained in the previous labs.



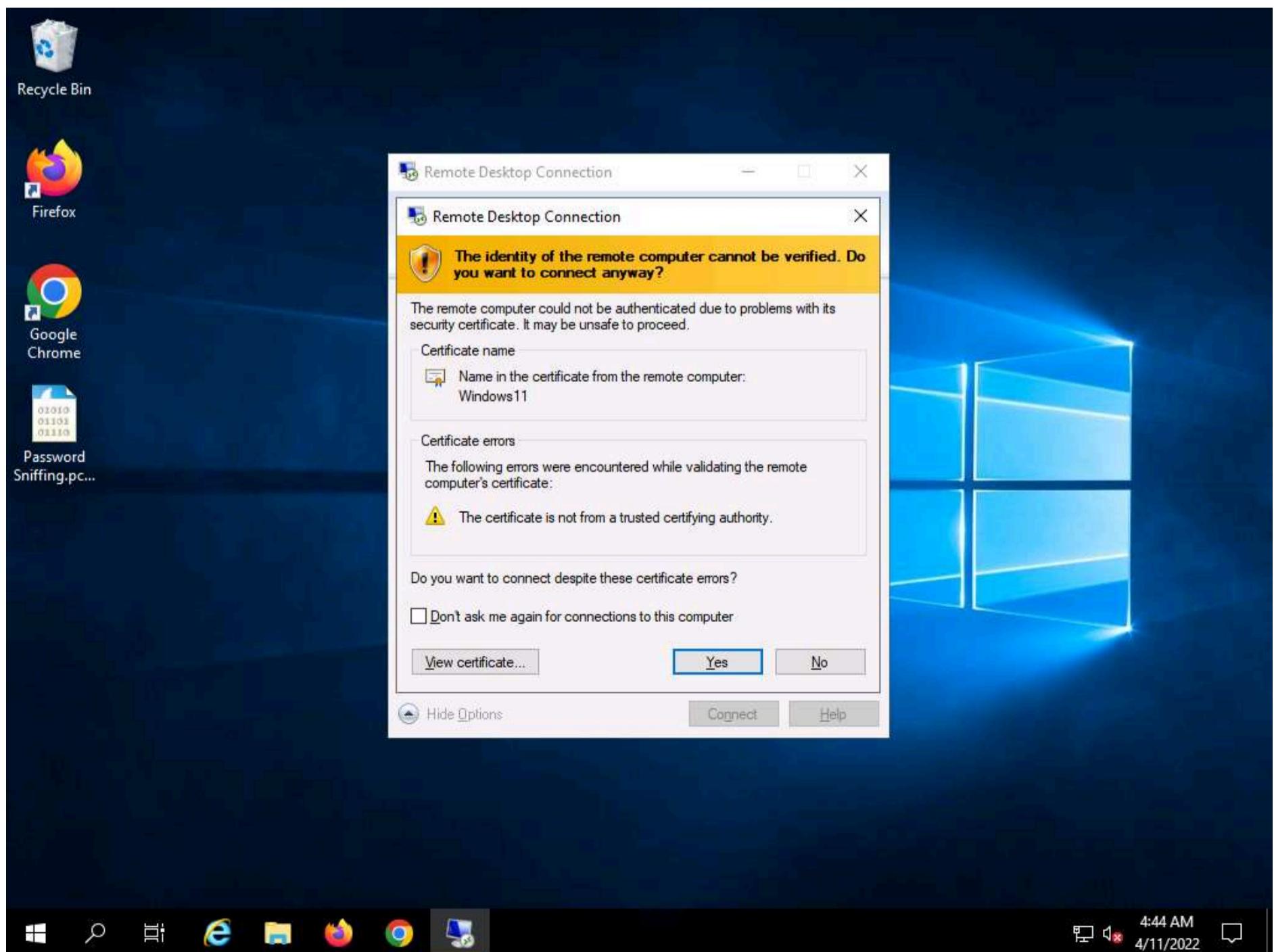
27. The **Windows Security** pop-up appears. Enter **Password (qwerty)** and click **OK**.

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



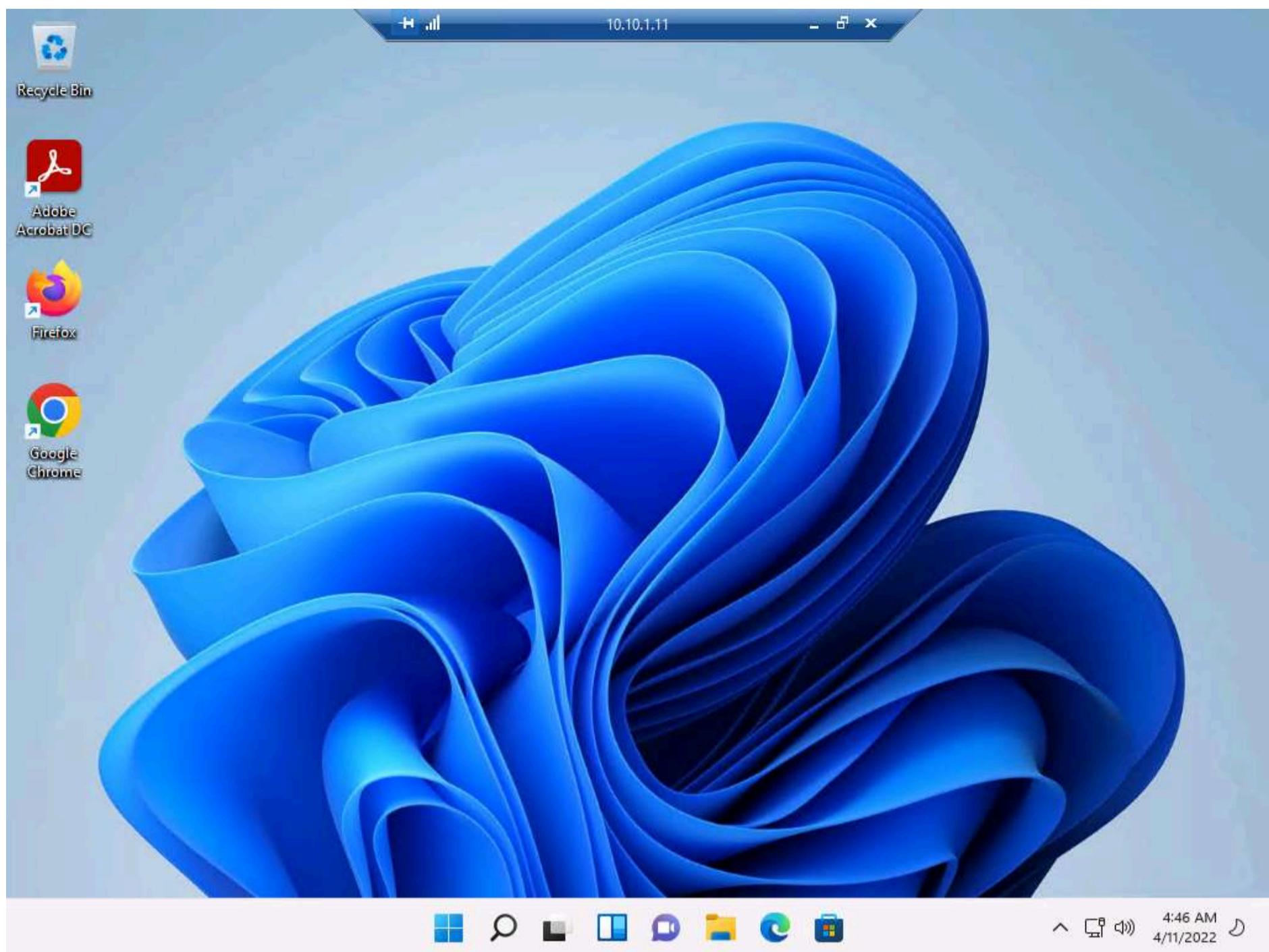


28. The **Remote Desktop Connection** pop-up appears; click **Yes**.



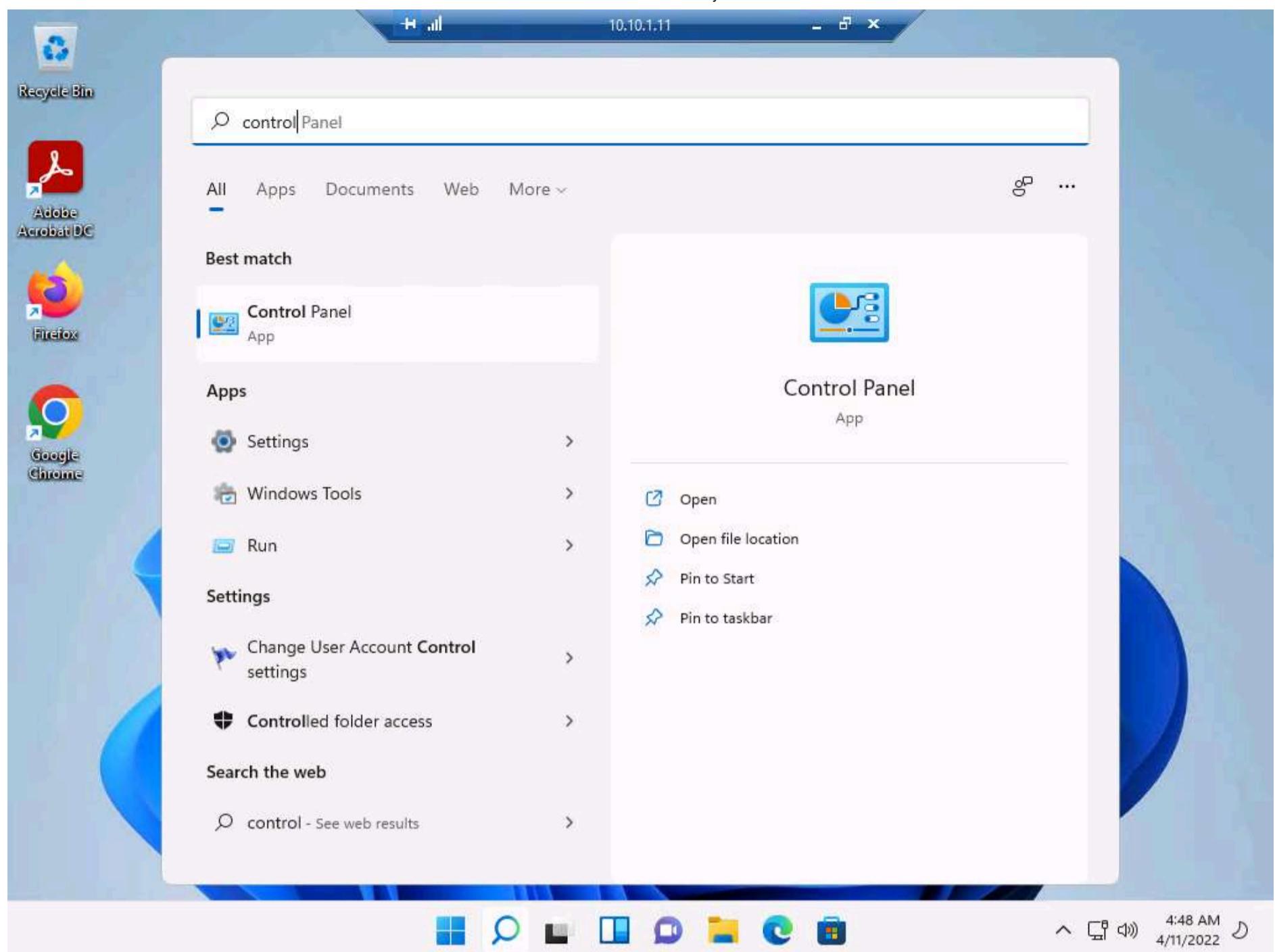
29. A remote connection to the target system (**Windows 11**) appears, as shown in the screenshot.

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**.

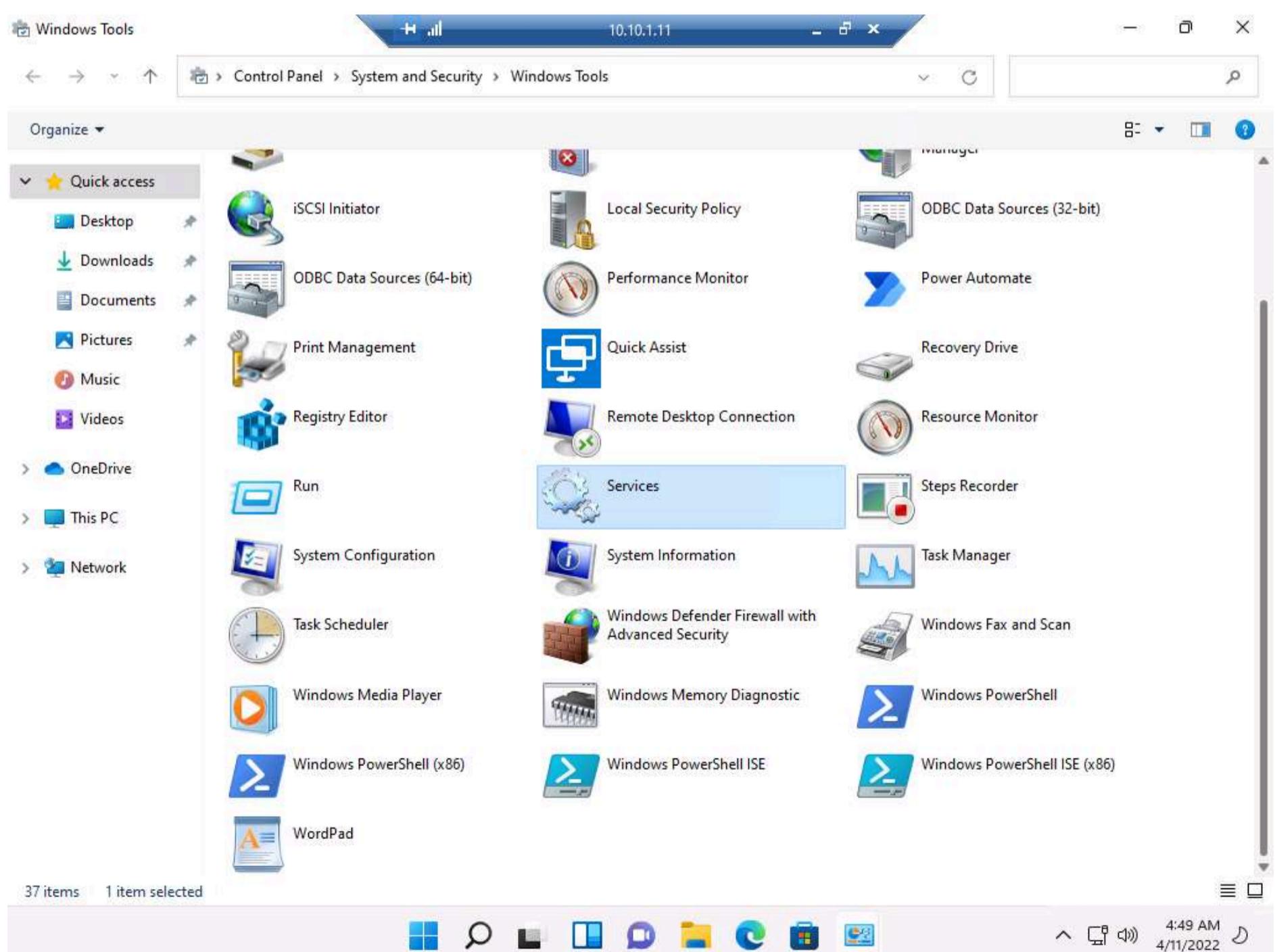


30. Click **Search** icon (  ) on the **Desktop**. Type **Control** in the search field, the **Control Panel** appears in the results, click **Open** to launch it.





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 **Start** 

The screenshot shows the Windows Services window. On the left, the 'Remote Packet Capture Protocol v.0 (experimental)' service is selected. A context menu is open over this service, with 'Start' highlighted. The main table lists various Windows services with their names, descriptions, statuses, startup types, and log on accounts.

Name	Description	Status	Startup Type	Log On As
Program Compatibility Assistant Service	This service ...	Running	Automatic (...)	Local Syste...
Quality Windows Audio Video Experience	Quality Win...	Manual	Local Service	Local Service
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troubleshooting Service	Enables aut...	Manual	Local Syste...	Local Syste...
Remote Access Auto Connection Manager	Creates a co...	Manual	Local Syste...	Local Syste...
Remote Access Connection Manager	Manages di...	Running	Manual	Local Syste...
Remote Desktop Configuration	Remote Des...	Running	Manual	Local Syste...
Remote Desktop Services	Allows user...	Running	Manual	Network S...
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local Syste...
<b>Remote Packet Capture Protocol v.0 (experimental)</b>	<b>Allows to ca...</b>	<b>Running</b>	<b>Manual</b>	<b>Local Syste...</b>
Remote Procedure Call (RPC)	Start	Automatic	Network S...	
Remote Procedure Call (RPC) Locator	Stop	Manual	Network S...	
Remote Registry	Pause	Disabled	Local Service	
Retail Demo Service	Resume	Manual	Local Syste...	
Routing and Remote Access	Restart	Disabled	Local Syste...	
RPC Endpoint Mapper	All Tasks >	Automatic	Network S...	
Secondary Logon	Refresh	Manual	Local Syste...	
Secure Socket Tunneling Protocol Service	Properties	Automatic	Local Service	
Security Accounts Manager	Help	Manual (Trig...)	Local Syste...	
Security Center	A service to...	Manual (Trig...)	Local Service	
Sensor Data Service	Supports fil...	Automatic (T...	Local Syste...	
Sensor Monitoring Service	Manages pr...	Disabled	Local Syste...	
Sensor Service	Provides no...	Running	Automatic	Local Syste...
Server	Manages ac...	Manual (Trig...)	Local Service	
Shared PC Account Manager	Creates soft...	Running	Manual (Trig...)	Local Syste...
Shell Hardware Detection	Allows the s...	Manual	Local Syste...	
Smart Card				
Smart Card Device Enumeration Service				
Smart Card Removal Policy				

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

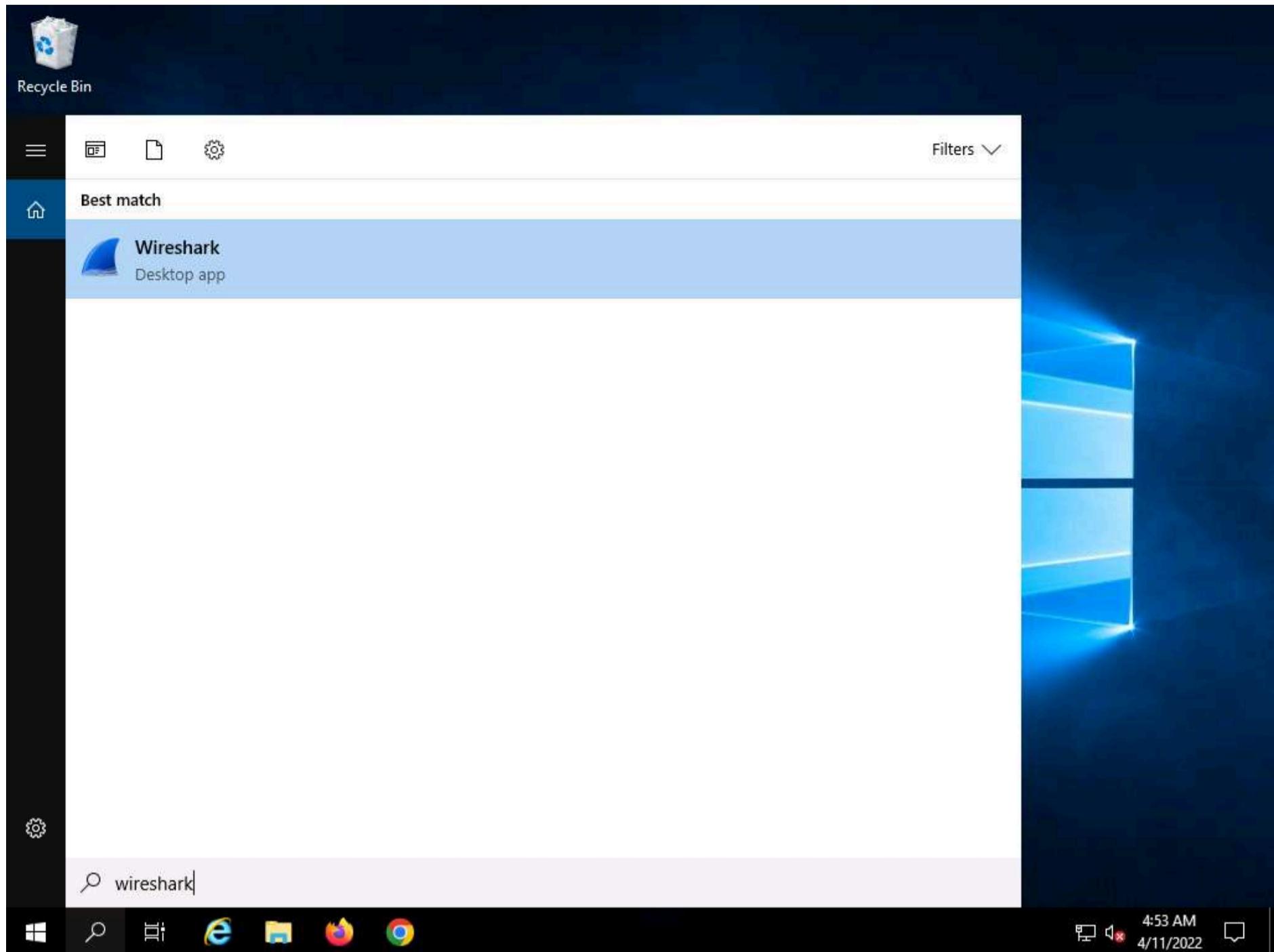
The screenshot shows the Windows Services window. The 'Remote Packet Capture Protocol v.0 (experimental)' service is now listed with a status of 'Running'. The context menu is no longer open.

Name	Description	Status	Startup Type	Log On As
Program Compatibility Assistant Service	This service ...	Running	Automatic (...)	Local Syste...
Quality Windows Audio Video Experience	Quality Win...	Manual	Local Service	Local Service
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troubleshooting Service	Enables aut...	Manual	Local Syste...	Local Syste...
Remote Access Auto Connection Manager	Creates a co...	Manual	Local Syste...	Local Syste...
Remote Access Connection Manager	Manages di...	Running	Manual	Local Syste...
Remote Desktop Configuration	Remote Des...	Running	Manual	Local Syste...
Remote Desktop Services	Allows user...	Running	Manual	Network S...
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local Syste...
<b>Remote Packet Capture Protocol v.0 (experimental)</b>	<b>Allows to ca...</b>	<b>Running</b>	<b>Manual</b>	<b>Local Syste...</b>
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network S...
Remote Procedure Call (RPC) Locator	In Windows...	Manual	Network S...	
Remote Registry	Enables rem...	Disabled	Local Service	
Retail Demo Service	The Retail D...	Manual	Local Syste...	
Routing and Remote Access	Offers routi...	Disabled	Local Syste...	
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Secondary Logon	Enables star...	Manual	Local Syste...	
Secure Socket Tunneling Protocol Service	Provides su...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
Security Center	The WSCSV...	Running	Automatic (...)	Local Service
Sensor Data Service	Delivers dat...	Manual	Local Syste...	
Sensor Monitoring Service	Monitors va...	Manual (Trig...)	Local Service	
Sensor Service	A service fo...	Manual (Trig...)	Local Syste...	
Server	Supports fil...	Running	Automatic (T...	Local Syste...
Shared PC Account Manager	Manages pr...	Disabled	Local Syste...	
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syste...
Smart Card	Manages ac...	Manual (Trig...)	Local Service	
Smart Card Device Enumeration Service	Creates soft...	Running	Manual (Trig...)	Local Syste...
Smart Card Removal Policy	Allows the s...	Manual	Local Syste...	

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**.

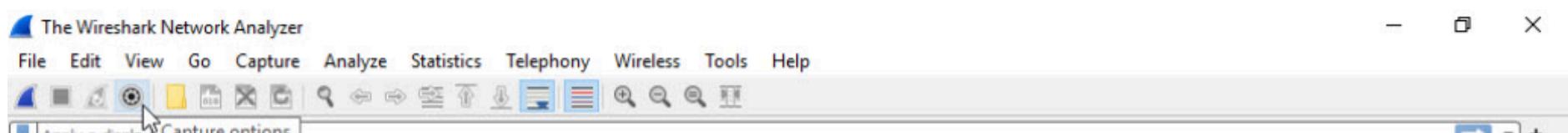
35. Now, in **Windows Server 2019**, click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results, to launch **Wireshark**.



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**.





## Welcome to Wireshark

## Capture

...using this filter:  Enter a capture filter ...

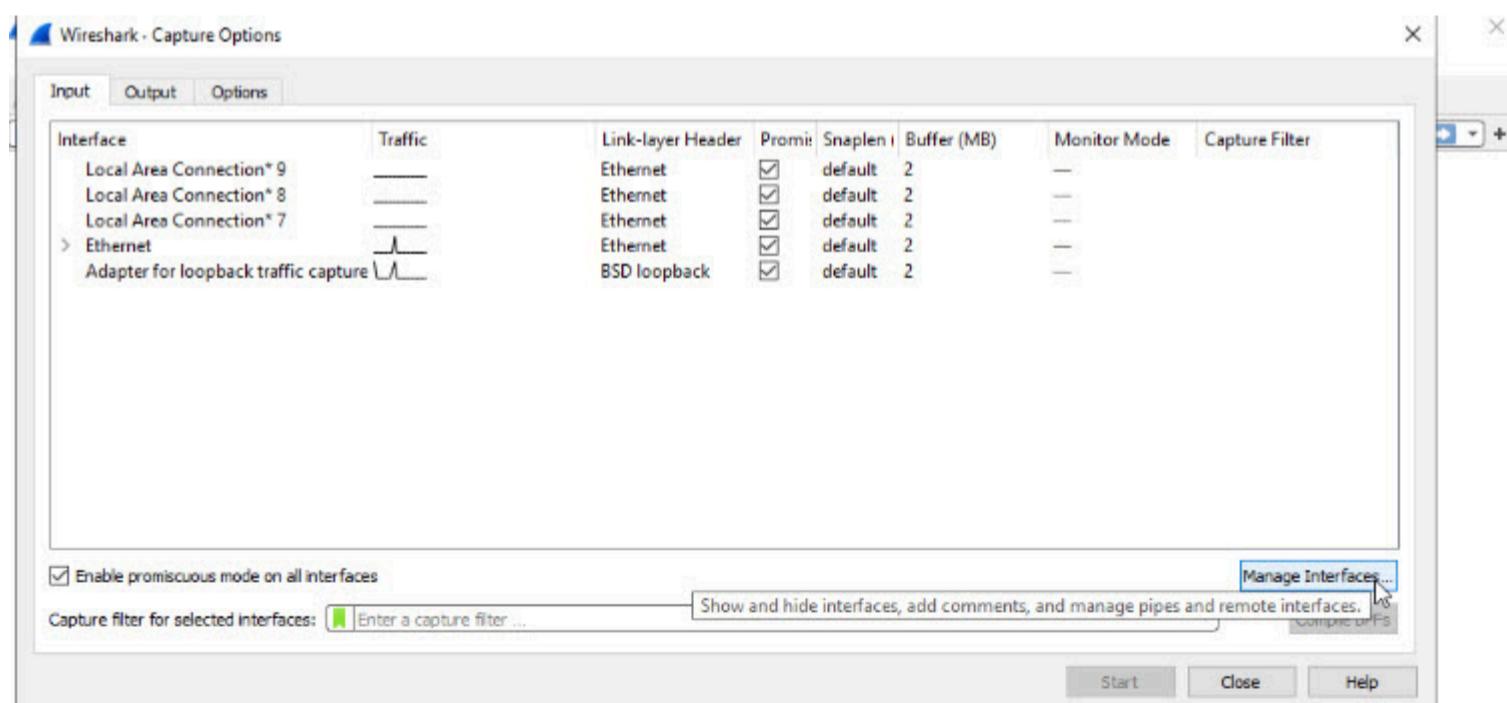
All interfaces shown ▾

- Local Area Connection\* 9
- Local Area Connection\* 8
- Local Area Connection\* 7
- Ethernet
- Adapter for loopback traffic capture

## Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.

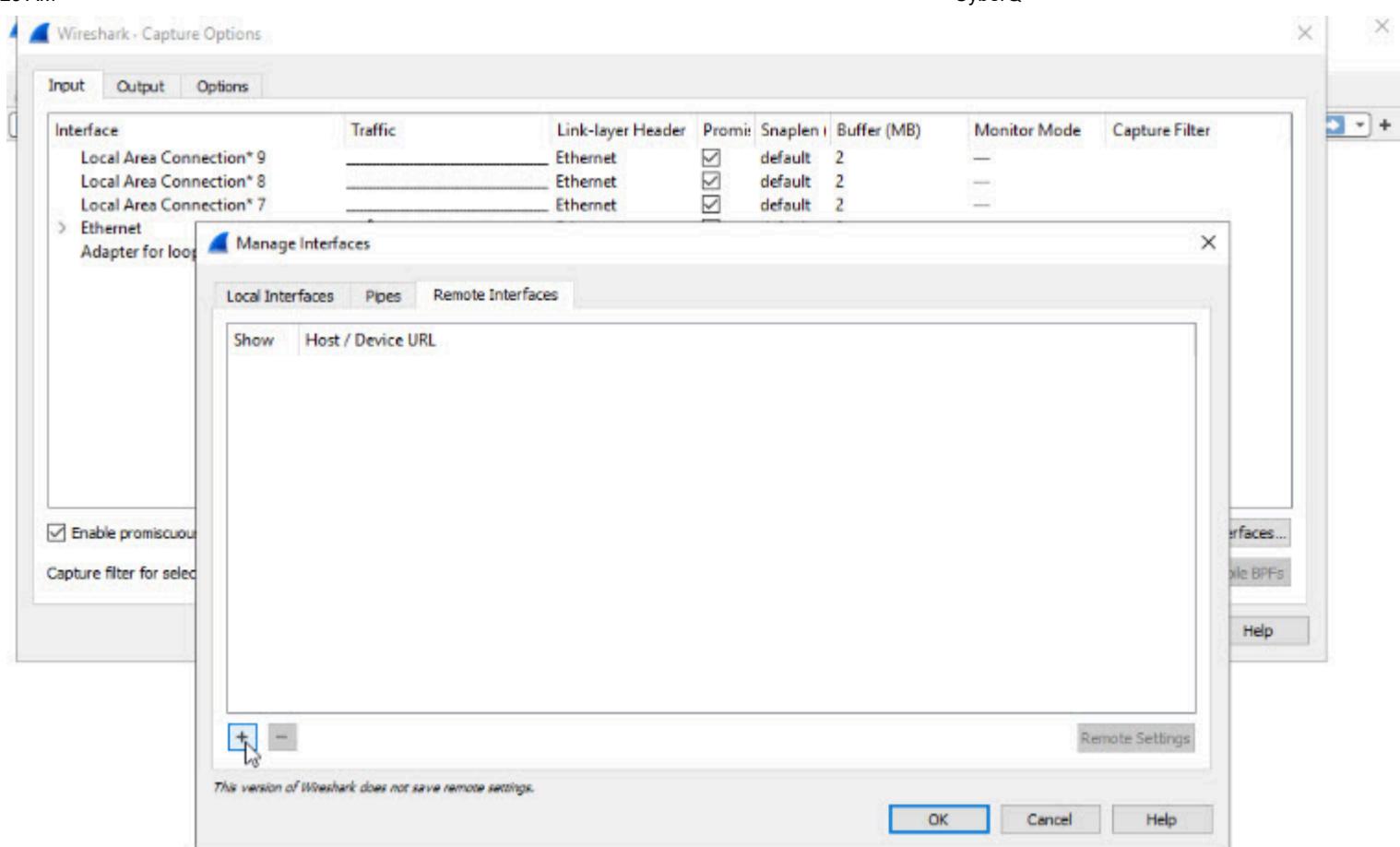
37. The Wireshark. Capture Options window appears; click the **Manage Interfaces...** button.

## Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.

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

**Learn**[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

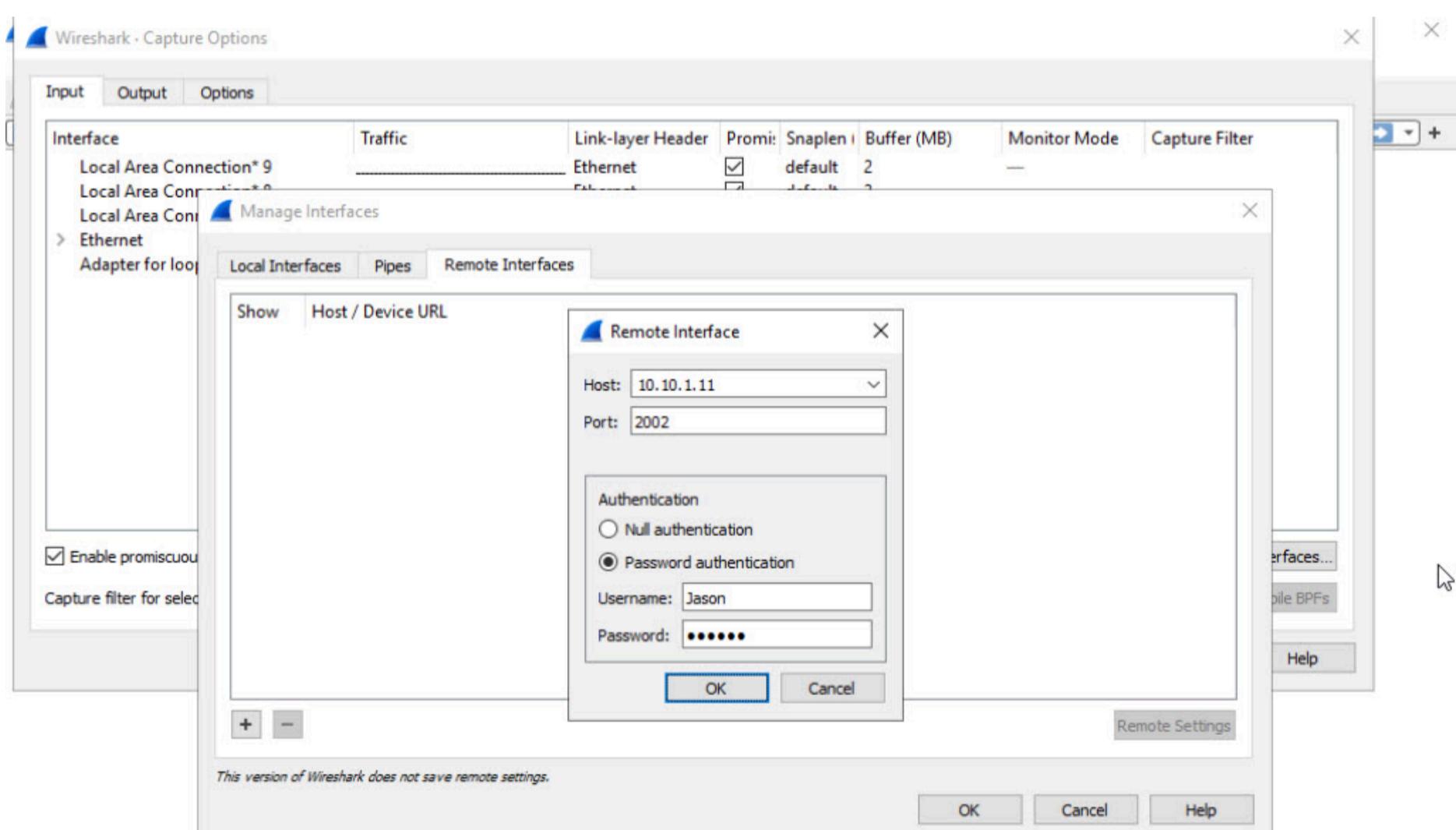
You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.



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

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

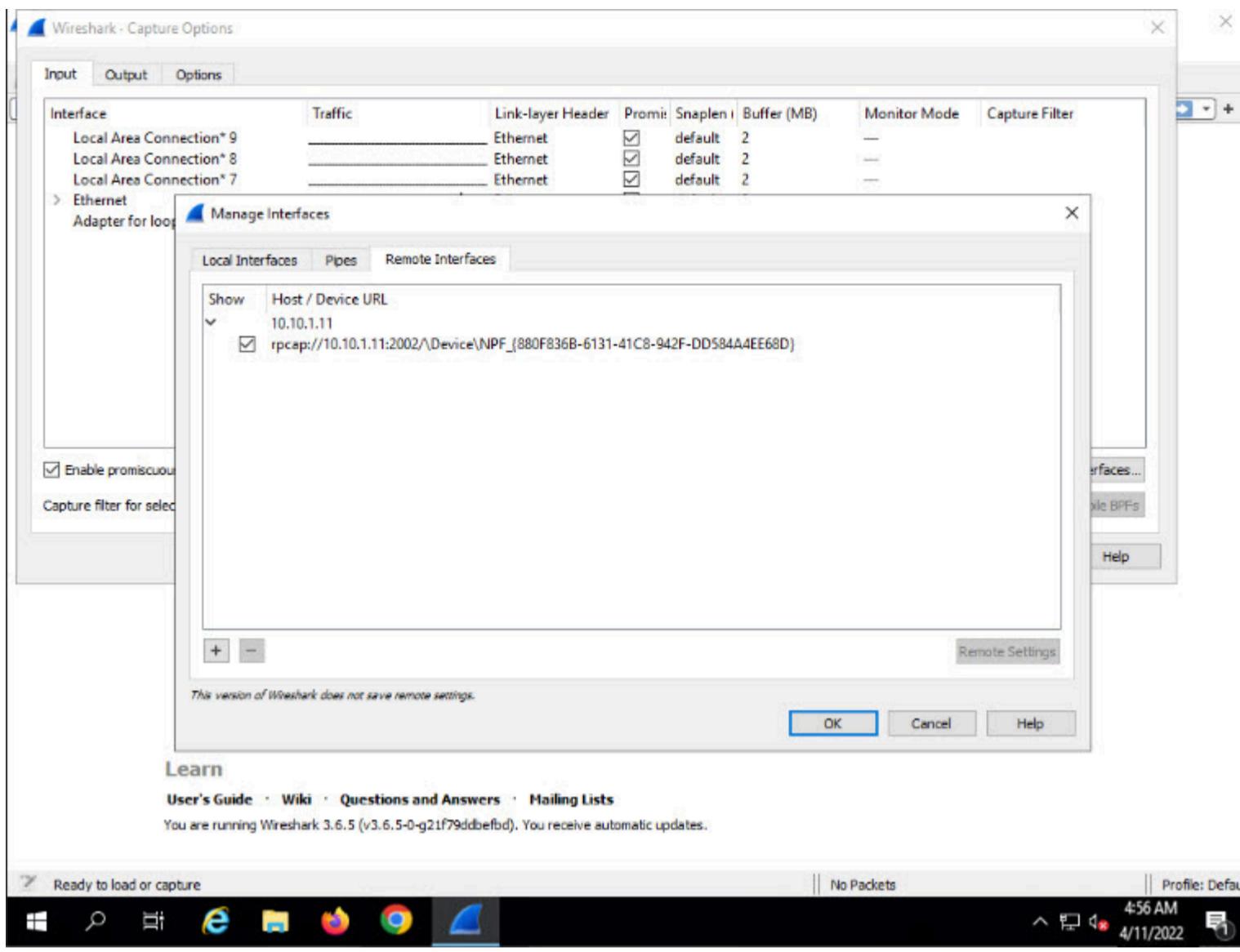
Note: The IP address and user credentials may differ when you perform this task.

**Learn**[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.

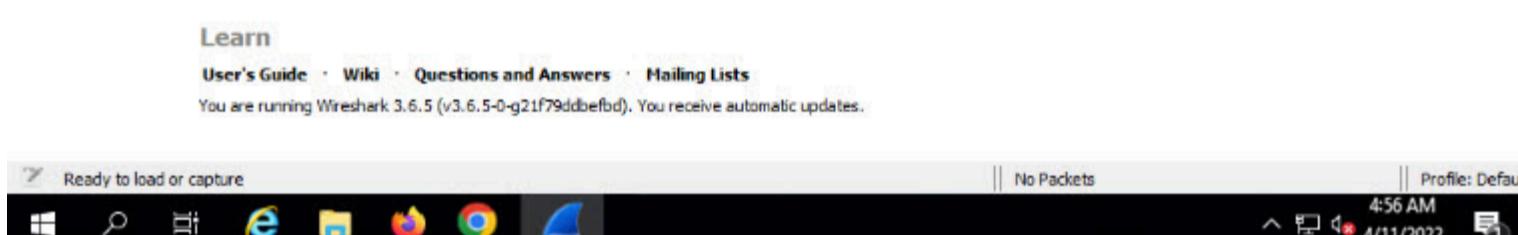
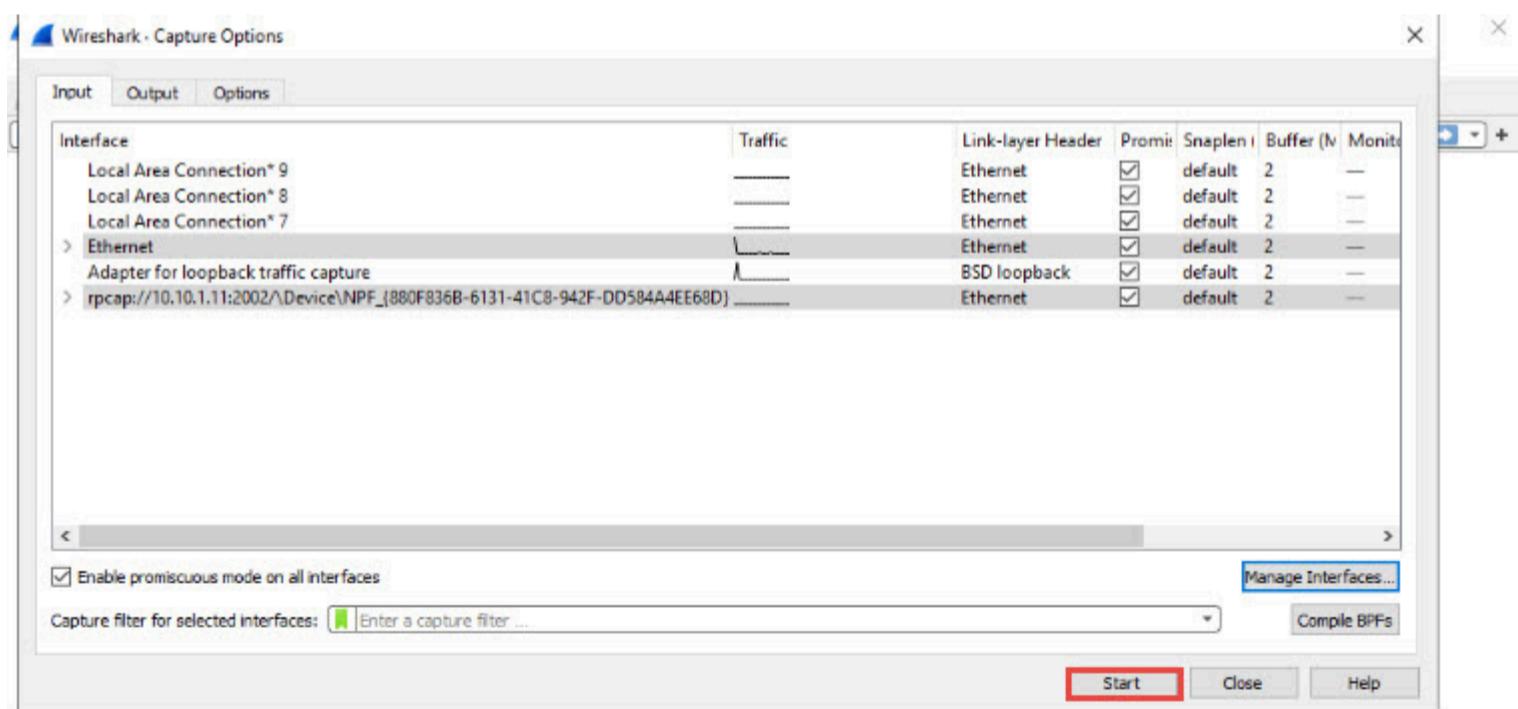


41. A new remote interface is added to the **Manage Interfaces** window; click **OK**.

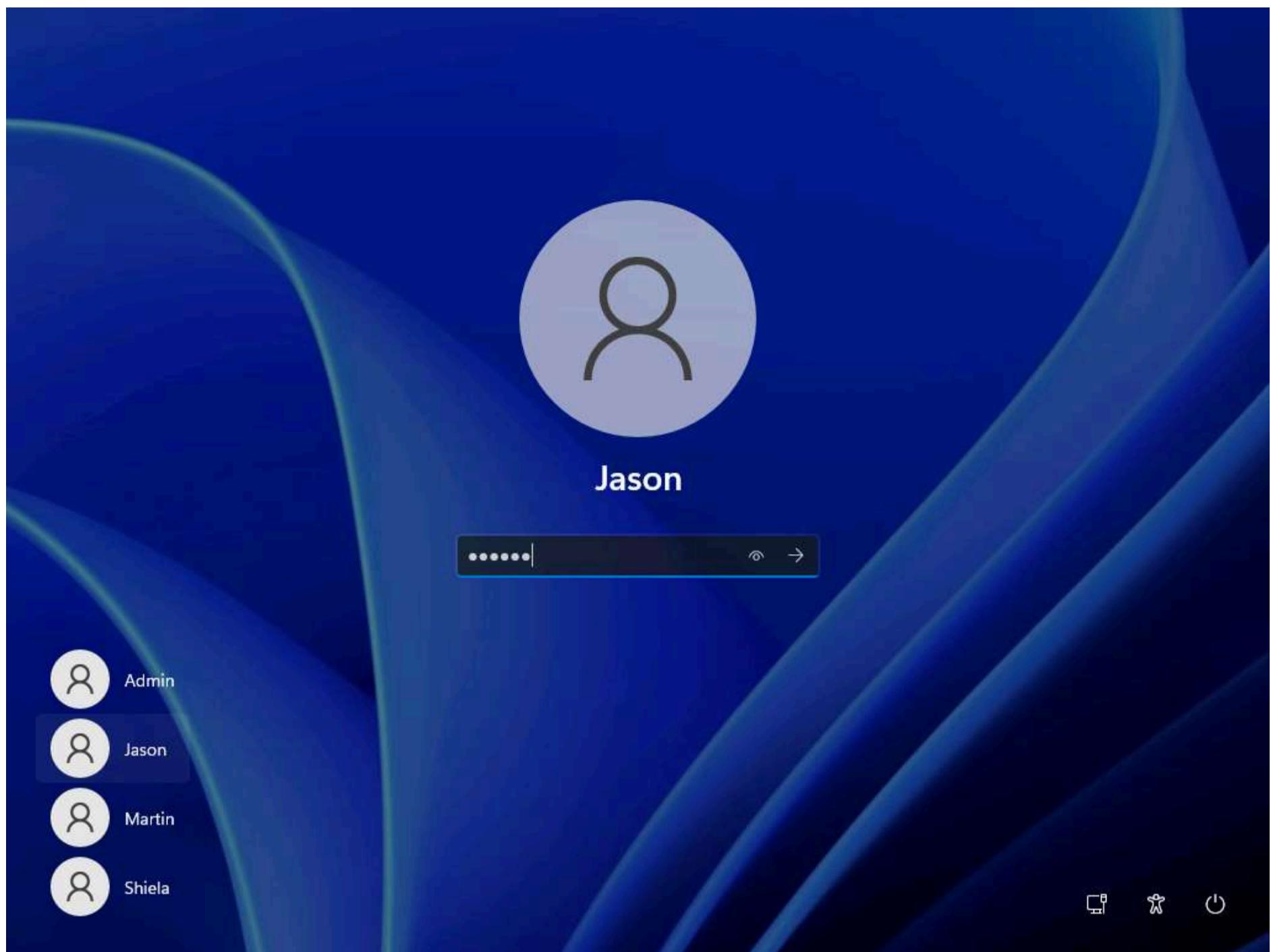


42. The newly added remote interface appears in the **Wireshark. Capture Options** window; click **Start**.

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



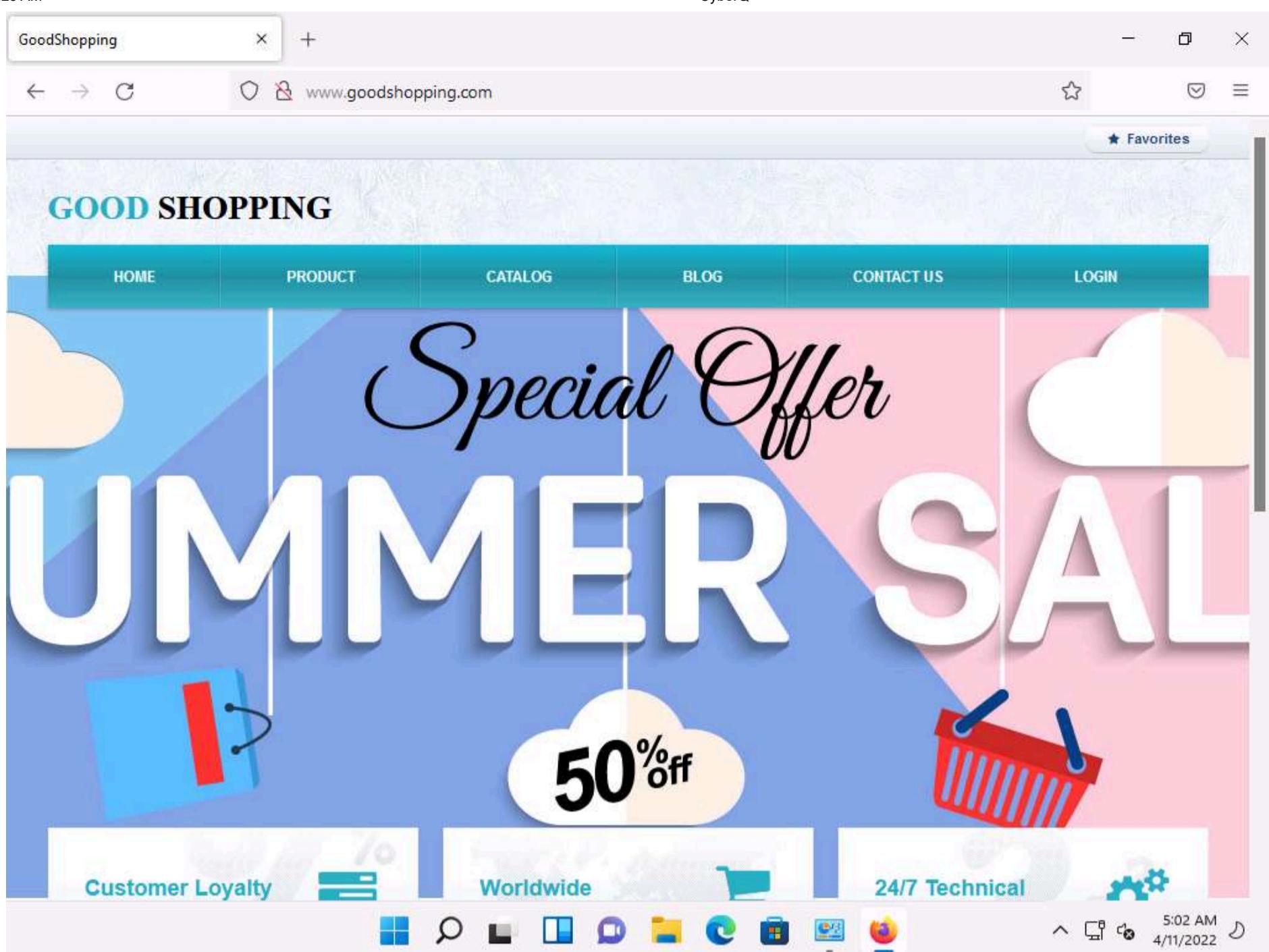
43. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**. Select **Jason** from the list of user accounts in the left-pane, click **qwerty** to enter the password and press **Enter** to log in. Here, you are signing in as the victim.



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.

No.	Time	Source	Destination	Protocol	Length	Info
88	29.004642	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
89	29.011226	fe80::596a:9dce:b1...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
90	29.600781	fe80::deb2:9b3b:549...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
91	29.723407	fe80::596a:9dce:b1...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
92	33.313449	10.10.1.11	10.10.1.19	TCP	66	50872 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PEE...
93	33.313526	10.10.1.19	10.10.1.11	TCP	66	80 → 50872 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=...
94	33.313926	10.10.1.11	10.10.1.19	TCP	54	50872 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
95	33.313926	10.10.1.11	10.10.1.19	HTTP	406	[GET / HTTP/1.1]
96	33.316544	10.10.1.19	10.10.1.11	HTTP	13749	HTTP/1.1 200 OK (text/html)
97	33.317124	10.10.1.11	10.10.1.19	TCP	54	50872 → 80 [ACK] Seq=253 Ack=12606 Win=262656 Len=0

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.



The screenshot shows a web browser window with the URL <https://www.liveaction.com/products/omnipipek-network-protocol-analyzer/>. The page features the LiveAction logo at the top left. Below it, a text block reads: "decoding thousands of protocols for fast network troubleshooting and diagnostics, anywhere network issues happen." To the right, there's a screenshot of the software interface showing various network protocol analysis tools. At the bottom left are two buttons: "Get a Demo →" and "Free Trial →". A large blue banner in the center says "Meet the World's Most Powerful Protocol Analyzer". On the right side of the banner is a white speech bubble with the text "Hey there! 🌟 Want to talk about your network?" and a blue icon of a person with a speech bubble.

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

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

The screenshot shows a web browser window with the URL <https://www.liveaction.com/free-trial-omnipipek/>. The page has a dark header with the LiveAction logo and a search bar. The main content area features the text "Anywhere" in large letters. Below it, a paragraph describes the benefits of the free trial: "Get our free trial to the world's most powerful network protocol analyzer. Decode thousands of protocols with instant visualization across every type of network segment 1/10/40/100 Gigabit, 802.11, voice, VoIP. Drill down from a global view to a single packet." To the right, there's a sidebar with several input fields, some containing blurred text, and a blue button with a speech bubble icon. At the bottom, there's a row of Windows taskbar icons and a system tray showing the date and time.

LiveCapture. Omnipoke enables rapid analysis and application-level troubleshooting of wired and wireless networks from the largest data centers to the smallest offices.

Turn your data into insights today with our free, full-featured trial and

- ▶ Accelerate mean-time-to-repair (MTTR) with lightning-fast visualization and interaction with metadata, flows, files and packet data
- ▶ Comprehensive Monitoring and intuitive graphic visibility give you views into networks and applications
- ▶ Expert Insights and Analysis to Network Challenges with built-in real-time analysis of hundreds of common network problems

I'm not a robot reCAPTCHA Privacy - Terms

By submitting this form you consent to allow LiveAction to store and process the personal information submitted above to provide you the content requested. Please review our [Privacy Policy](#) to learn more.

By clicking 'Start My Omnipoke Trial' you agree to [LiveAction's End User License Agreement](#).

**Start My Omnipoke Trial**

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

protocol analyzer is now yours!

You're all set! Scroll down to download your Omnipoke trial now...

**Let's get started**

Here's everything you need to deploy Omnipoke

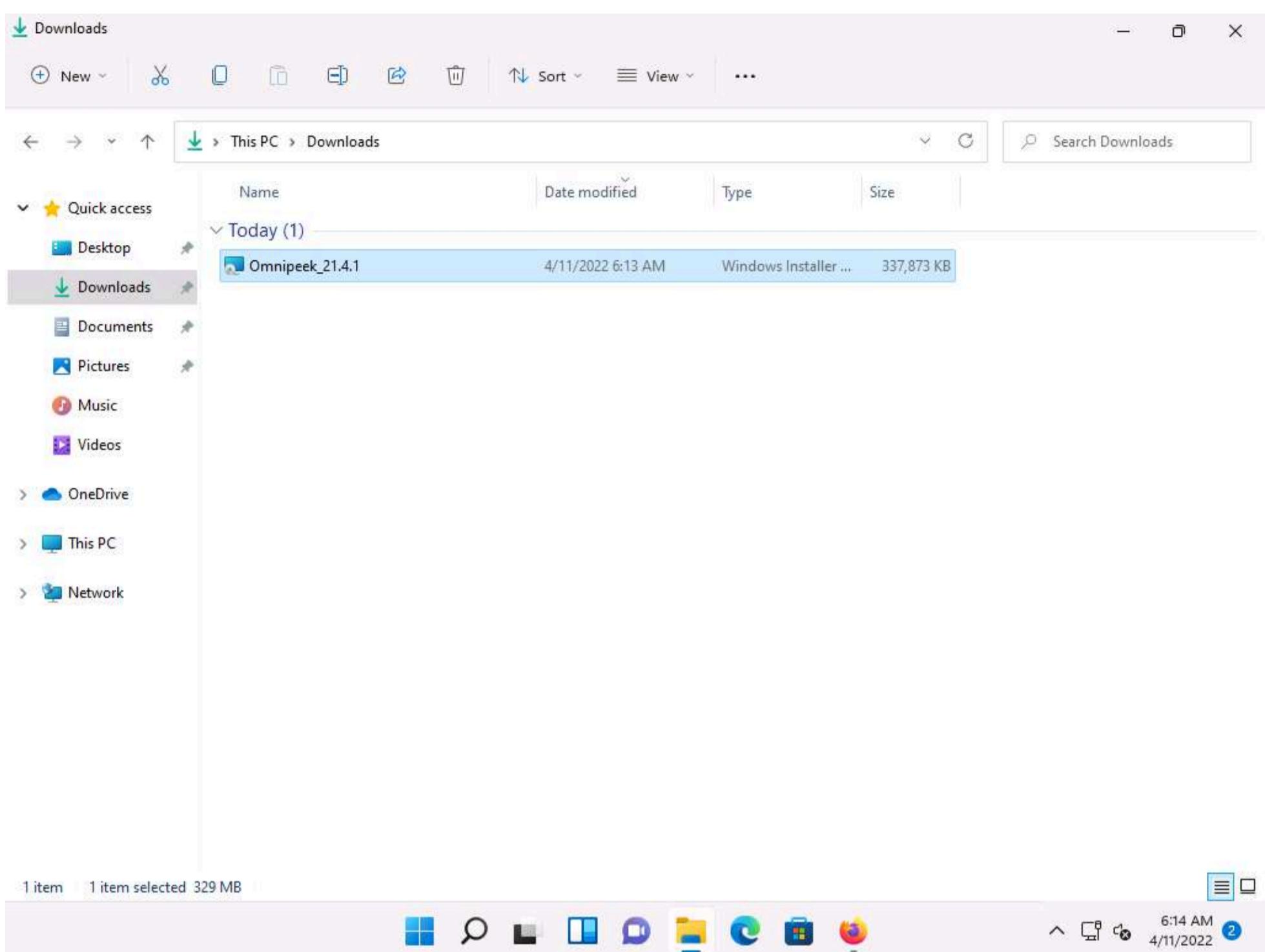
**Download Omnipoke for Windows**

Product Key: 32e3bf2f-  
81410

Note: If **Opening Omnipipe\_21.4.1msi** pop-up appears; click **Save File** to download the application.

6. On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek\_21.4.1msi**.

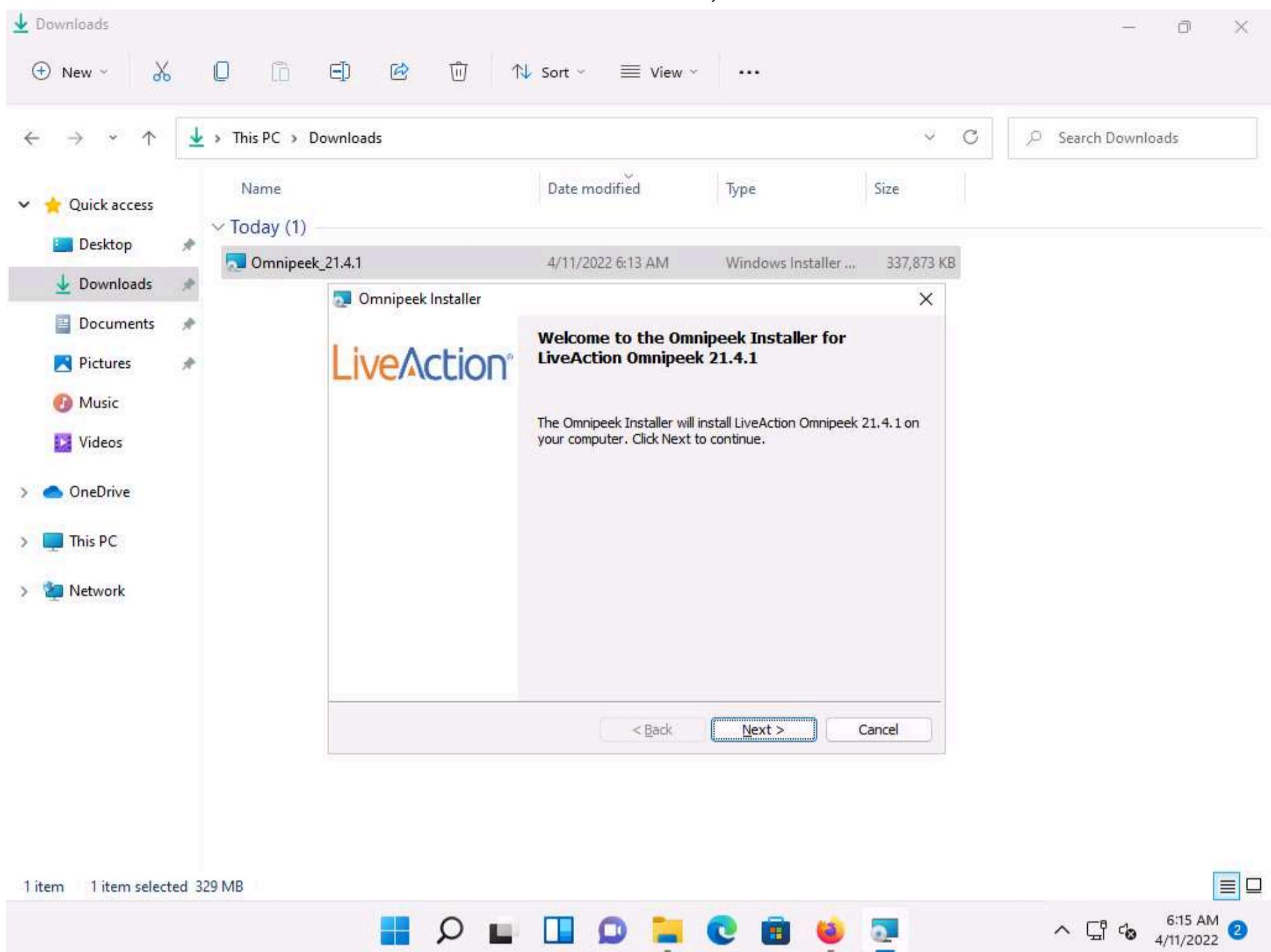
Note: The version of **Omnipeek** might differ when you perform the task.



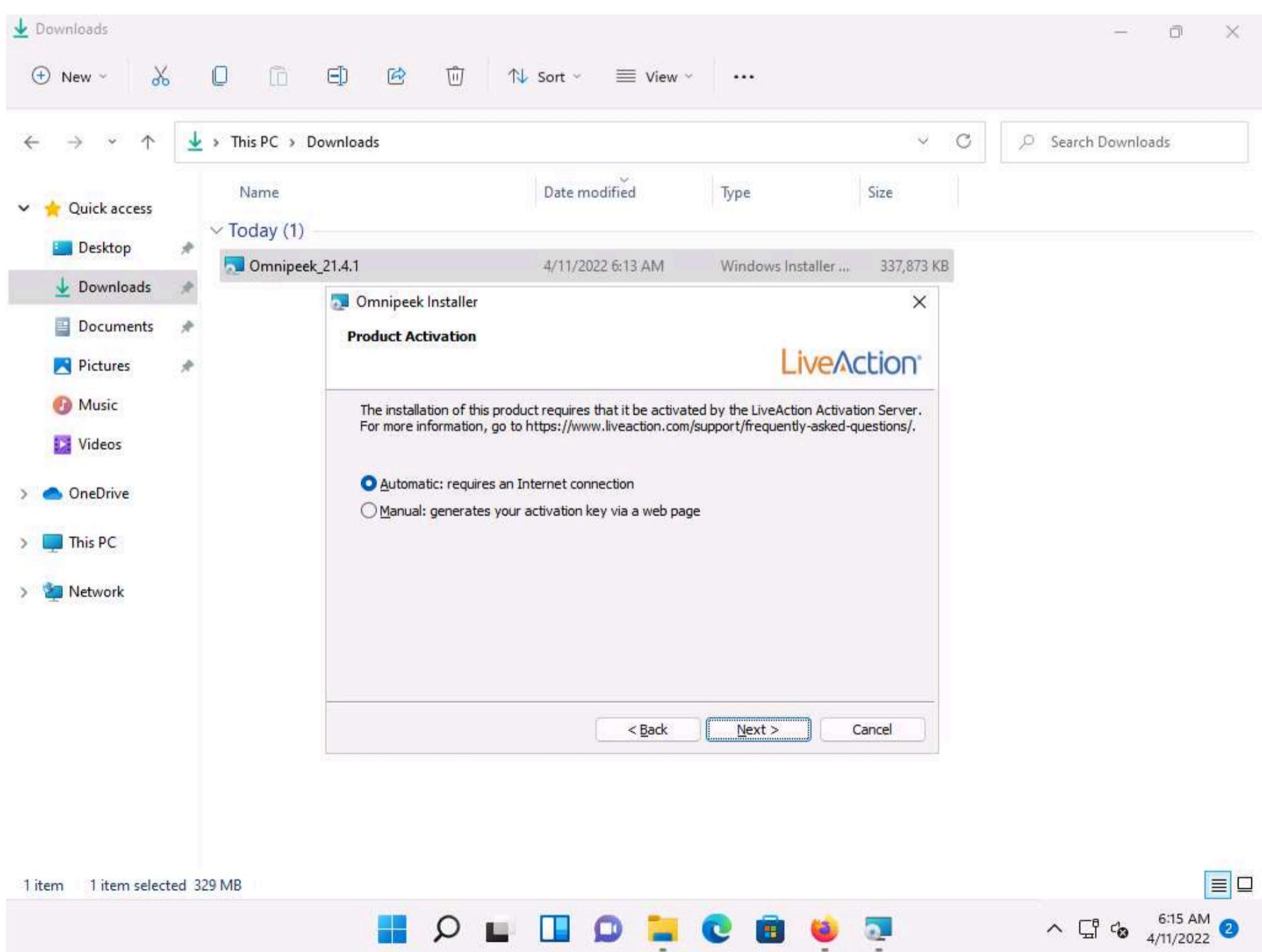
7. If an **Open File - Security Warning** pop-up appears, click **Run**.

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



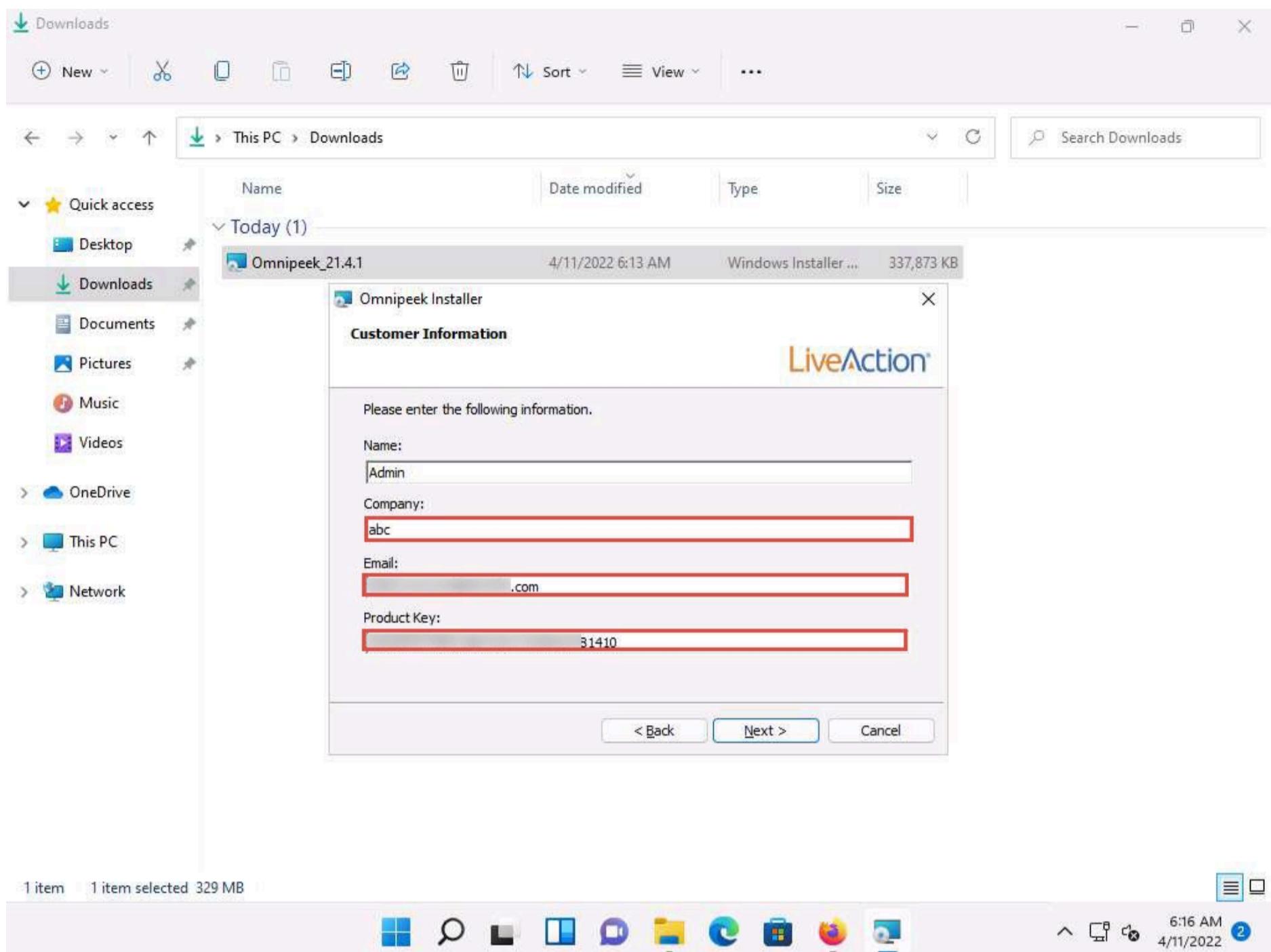


9. In the **Product Activation** wizard, ensure that the **Automatic: requires an Internet connection** radio-button is selected and click **Next**.



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

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

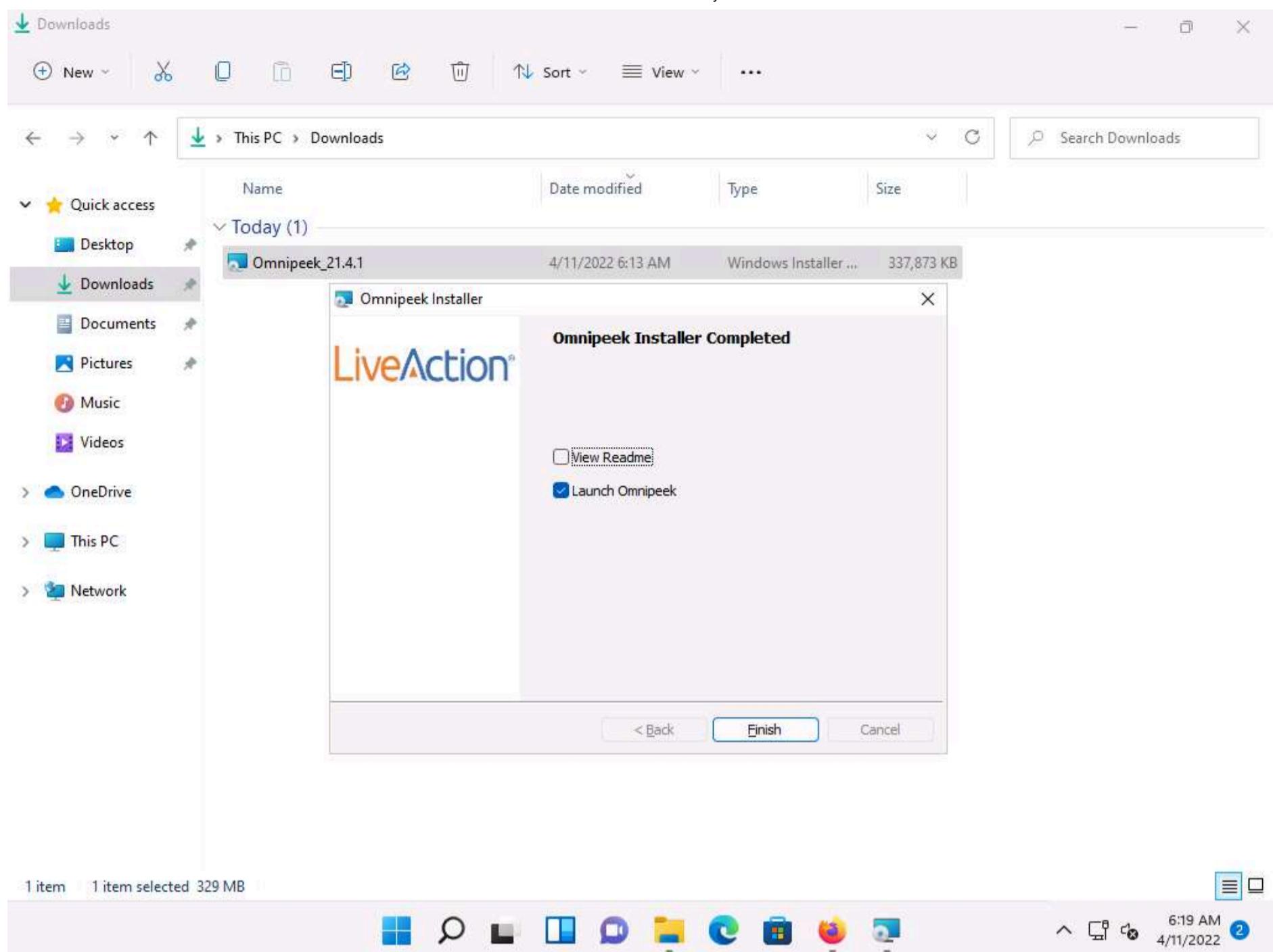


12. Follow the wizard-driven installation steps to install Omnipipek using the default settings.

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

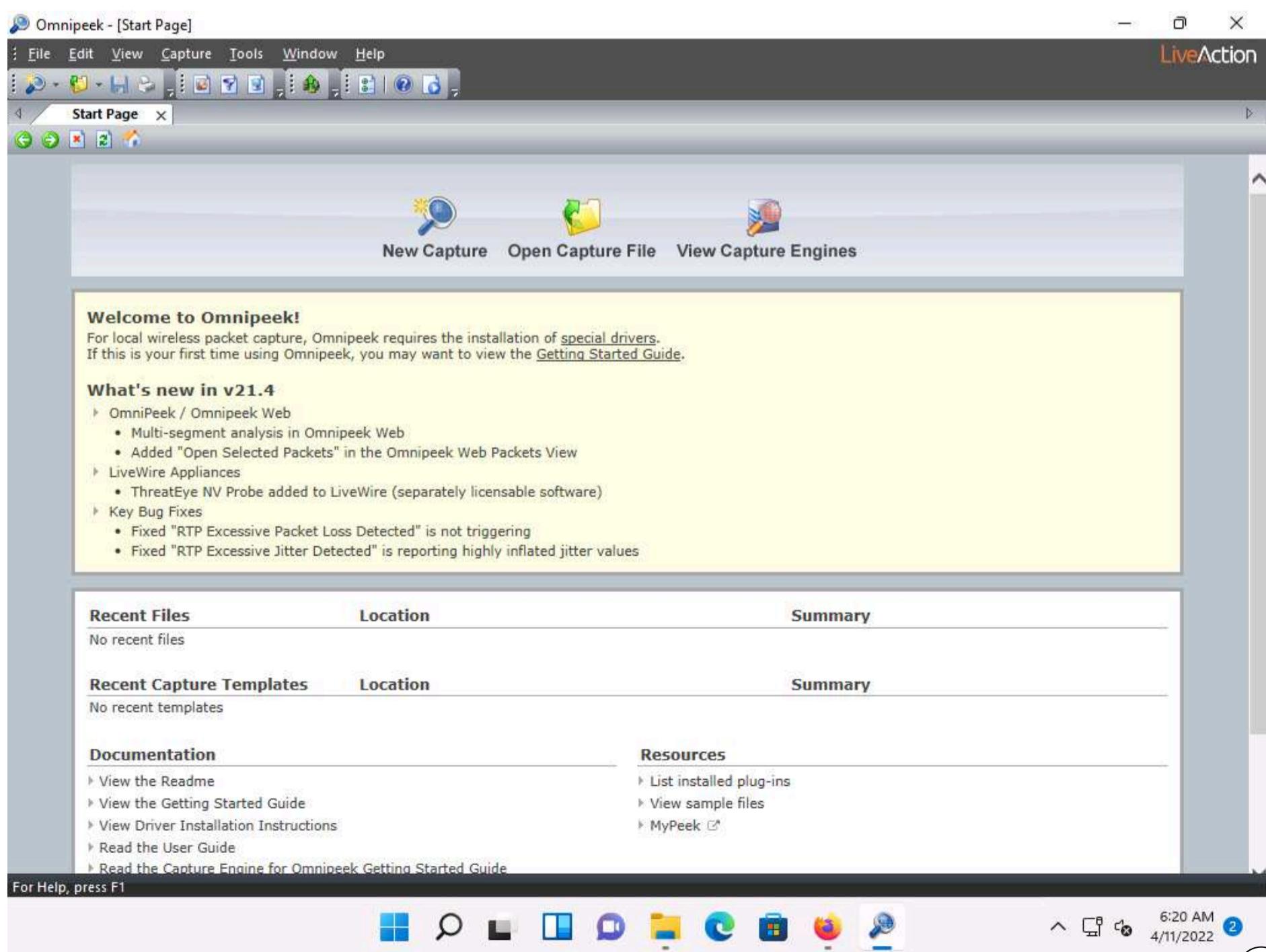
14. On completion of the installation, the **Omnipeek Installer Completed** wizard appears; uncheck **View Readme**, ensure that the **Launch Omnipipek** option is checked, and click **Finish**.

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

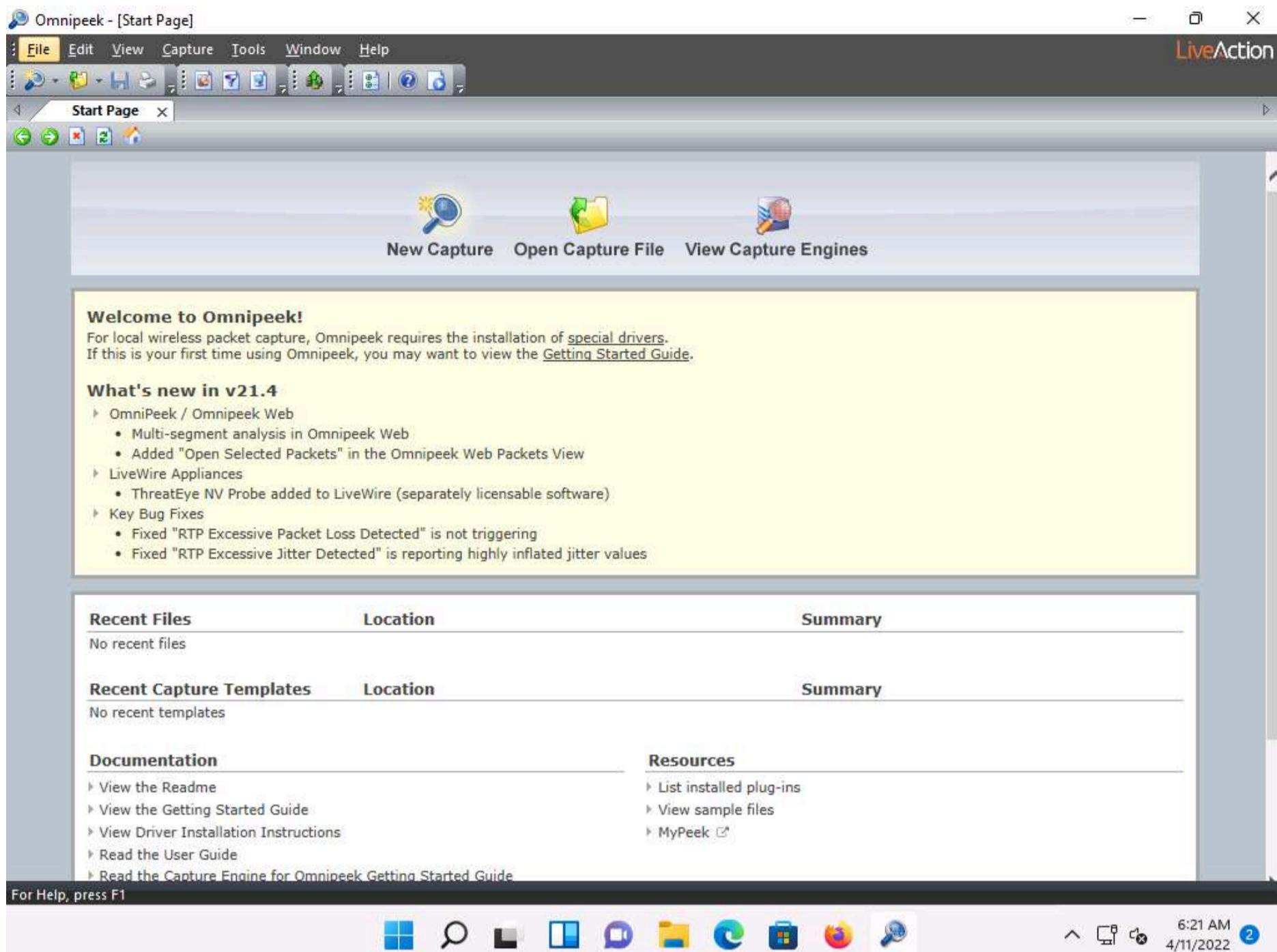


15. The **Omnipeek** evaluation dialog-box appears; click **OK**.

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

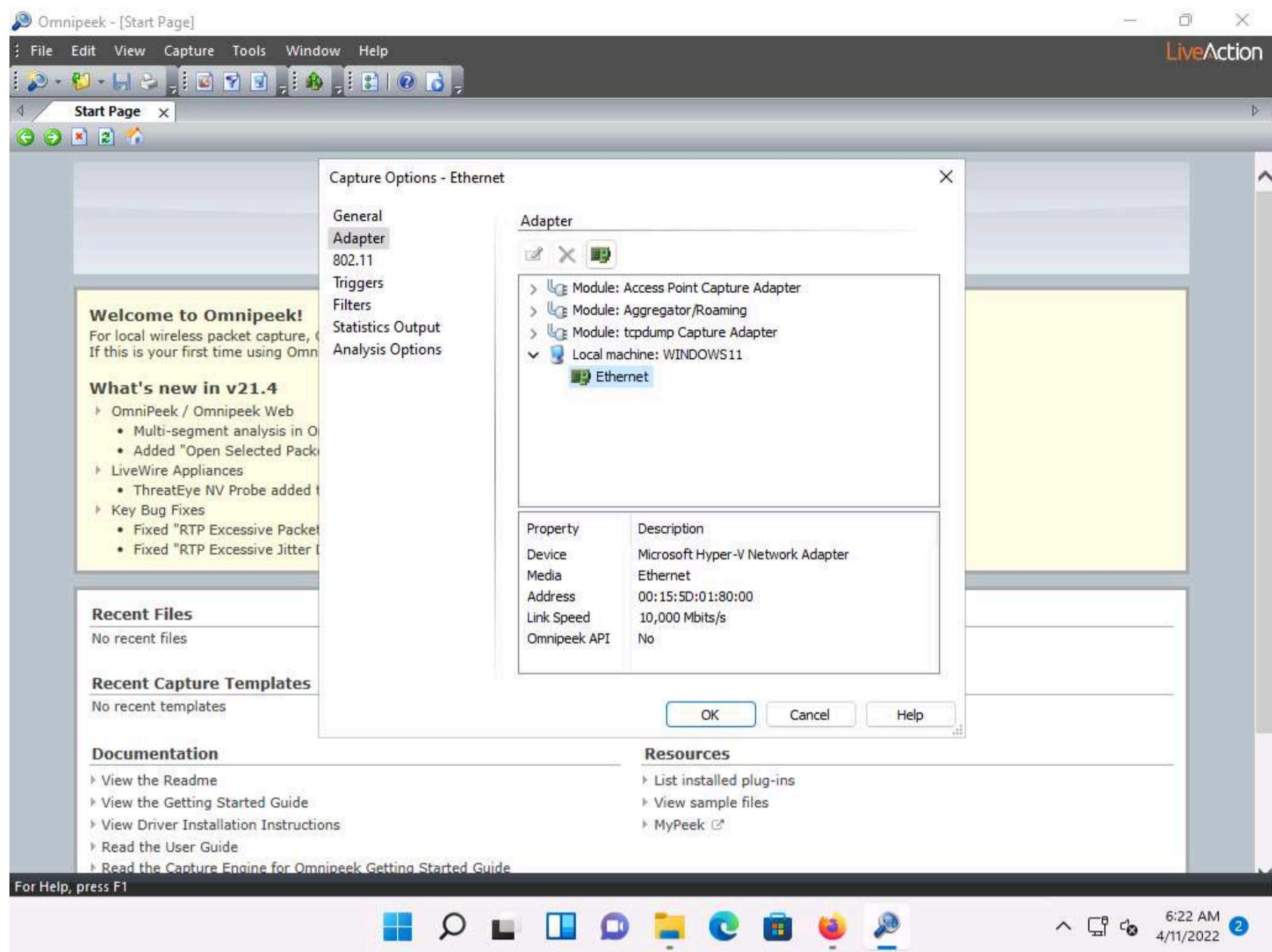


17. Click on the **New Capture** option from the Omnipacket's main screen to create an Omnipacket capture window.

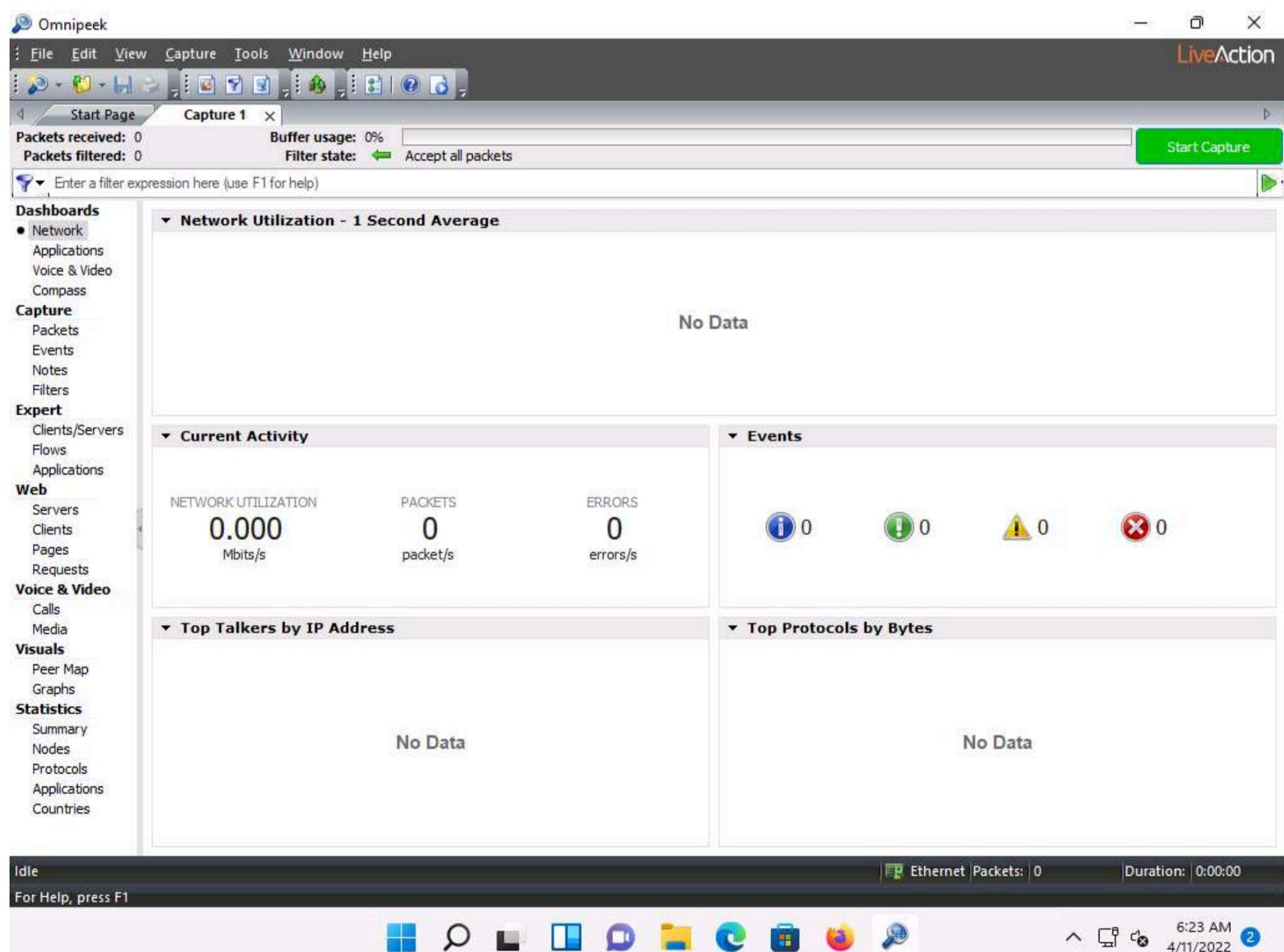


18. The **Capture Options** window appears; by default, the **Adapter** option opens-up.

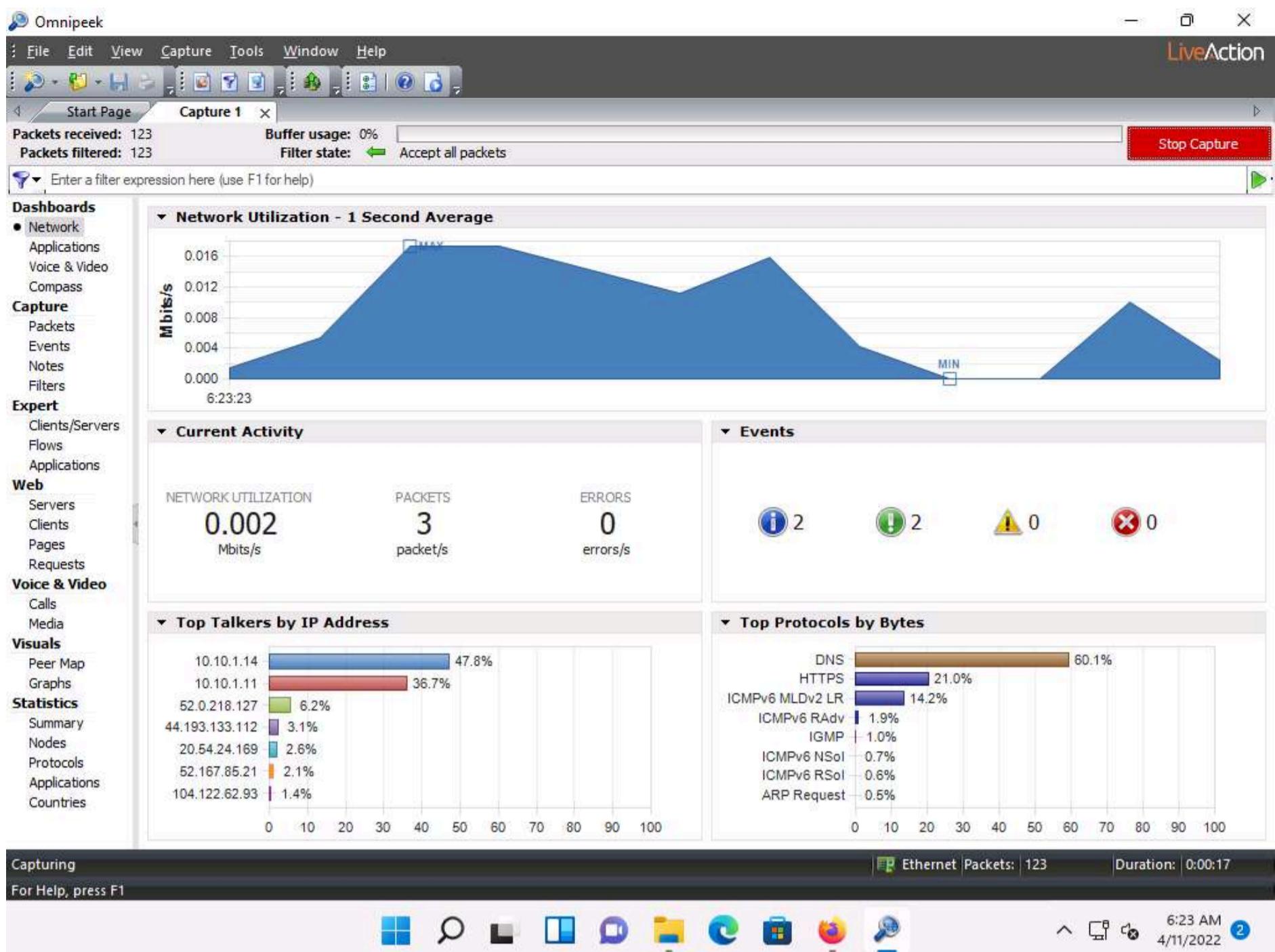
19. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS11** node, select **Ethernet**, and click **OK**.



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



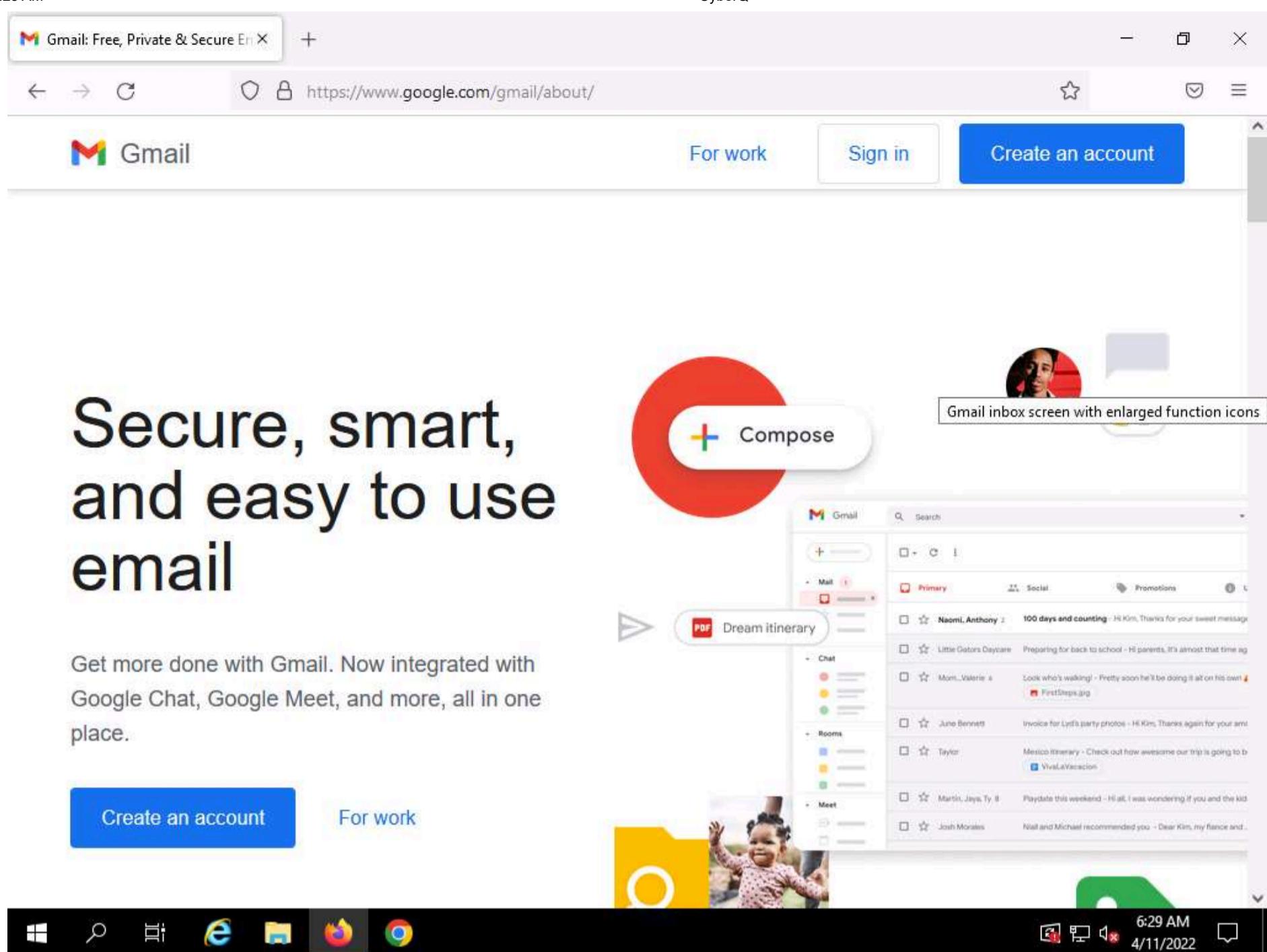
21. The **Start Capture** button changes to read "**Stop Capture**" and traffic statistics begin to populate **Network** under the **Dashboards** section, as shown in the screenshot.



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

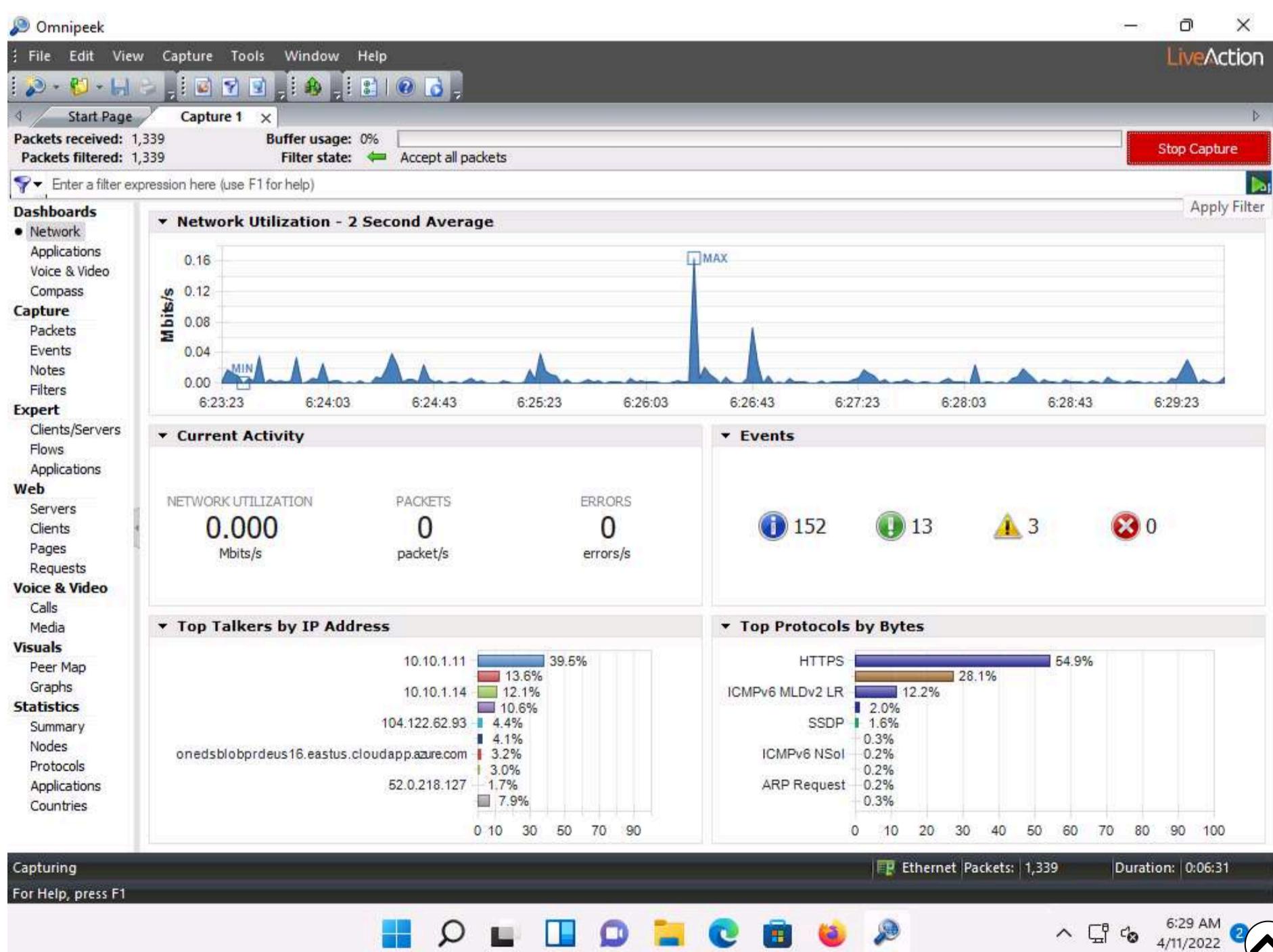
23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, <https://www.gmail.com>).

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.

Packet	Source	Destination	Flow ID	Flags	Size	Relative Time	Protocol	Application
1	fe80::15:5dff:fe...	mDNSv6			178	0.234061	DNS	Bonjour
2	fe80::15:5dff:fe...	A11 MLDv2-capabl...			94	0.440251	ICMPv6 MLDv2 LR	ICMPv6
3	fe80::15:5dff:fe...	mDNSv6	1		178	0.484933	DNS	Bonjour
4	fe80::15:5dff:fe...	mDNSv6	1		375	0.734558	DNS	Bonjour
5	fe80::15:5dff:fe...	A11 MLDv2-capabl...			94	1.533484	ICMPv6 MLDv2 LR	ICMPv6
6	::	ff02::1:ff6b:705c			90	1.533512	ICMPv6 NSol	ICMPv6
7	fe80::15:5dff:fe...	A11 MLDv2-capabl...			94	1.536619	ICMPv6 MLDv2 LR	ICMPv6
8	::	A11 MLDv2-capabl...			114	1.536626	ICMPv6 MLDv2 LR	ICMPv6
9	10.10.1.14	IGMP			64	1.536629	IGMP	IGMP
10	02:15:5D:13:8C:A5	Ethernet Broadcast			64	1.542428	ARP Request	
11	fe80::15:5dff:fe...	A11 MLDv2-capabl...			94	1.760449	ICMPv6 MLDv2 LR	ICMPv6
12	fe80::6f09:fb32:...	mDNSv6	2		200	2.034008	DNS	Bonjour
13	10.10.1.14	mDNS	3		180	2.034008	DNS	Bonjour
14	fe80::15:5dff:fe...	mDNSv6	1		178	2.034118	DNS	Bonjour
15	10.10.1.14	IGMP			64	2.105002	IGMP	IGMP

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

The screenshot shows the Omnipacket interface with the following details:

- Header:** File, Edit, View, Capture, Tools, Window, Help.
- Toolbar:** Start Page, Capture 1, Stop Capture.
- Packets Received:** 1,665.
- Buffer Usage:** 0%.
- Filter State:** Accept all packets.
- Dashboards:** Network, Applications, Voice & Video, Compass.
- Capture:** Packets (selected), Events, Notes, Filters.
- Expert:** Clients/Servers, Flows, Applications.
- Web:** Servers, Clients, Pages, Requests.
- Voice & Video:** Calls, Media.
- Visuals:** Peer Map, Graphs.
- Statistics:** Summary, Nodes, Protocols, Applications, Countries.
- Table:** Shows a list of 15 captured packets. The first few rows include:
  - Packet 1: Source fe80::15:5dff:fe..., Destination mDNSv6, Flow ID 1, Flags 0x00000000, Size 178, Relative Time 0.234061, Protocol DNS, Application Bonjour.
  - Packet 2: Source fe80::15:5dff:fe..., Destination A11 MLDv2-capabl..., Flow ID 1, Flags 0x00000000, Size 94, Relative Time 0.440251, Protocol ICMPv6 MLDv2 LR, Application ICMPv6.
  - Packet 3: Source fe80::15:5dff:fe..., Destination mDNSv6, Flow ID 1, Flags 0x00000000, Size 178, Relative Time 0.484933, Protocol DNS, Application Bonjour.
  - Packet 4: Source fe80::15:5dff:fe..., Destination mDNSv6, Flow ID 1, Flags 0x00000000, Size 375, Relative Time 0.734558, Protocol DNS, Application Bonjour.
  - Packet 5: Source fe80::15:5dff:fe..., Destination A11 MLDv2-capabl..., Flow ID 1, Flags 0x00000000, Size 94, Relative Time 1.533484, Protocol ICMPv6 MLDv2 LR, Application ICMPv6.
  - Packet 6: Source ::, Destination ff02::1:ff6b:705c, Flow ID 1, Flags 0x00000000, Size 90, Relative Time 1.533512, Protocol ICMPv6 NSol, Application ICMPv6.
  - Packet 7: Source fe80::15:5dff:fe..., Destination A11 MLDv2-capabl..., Flow ID 1, Flags 0x00000000, Size 94, Relative Time 1.536619, Protocol ICMPv6 MLDv2 LR, Application ICMPv6.
  - Packet 8: Source ::, Destination A11 MLDv2-capabl..., Flow ID 1, Flags 0x00000000, Size 114, Relative Time 1.536626, Protocol ICMPv6 MLDv2 LR, Application ICMPv6.
  - Packet 9: Source 10.10.1.14, Destination IGMP, Flow ID 1, Flags 0x00000000, Size 64, Relative Time 1.536629, Protocol IGMP, Application IGMP.
  - Packet 10: Source 02:15:5D:13:8C:A5, Destination Ethernet Broadcast, Flow ID 1, Flags 0x00000000, Size 64, Relative Time 1.542428, Protocol ARP Request, Application ARP.
  - Packet 11: Source fe80::15:5dff:fe..., Destination A11 MLDv2-capabl..., Flow ID 1, Flags 0x00000000, Size 94, Relative Time 1.760449, Protocol ICMPv6 MLDv2 LR, Application ICMPv6.
  - Packet 12: Source fe80::6f09:fb32:..., Destination mDNSv6, Flow ID 2, Flags 0x00000000, Size 200, Relative Time 2.034008, Protocol DNS, Application Bonjour.
  - Packet 13: Source 10.10.1.14, Destination mDNS, Flow ID 3, Flags 0x00000000, Size 180, Relative Time 2.034008, Protocol DNS, Application Bonjour.
  - Packet 14: Source fe80::15:5dff:fe..., Destination mDNSv6, Flow ID 1, Flags 0x00000000, Size 178, Relative Time 2.034118, Protocol DNS, Application Bonjour.
  - Packet 15: Source 10.10.1.14, Destination IGMP, Flow ID 1, Flags 0x00000000, Size 64, Relative Time 2.105002, Protocol IGMP, Application IGMP.
- Packet Info:** Shows detailed information for Packet 1, including its number (1), flags (0x00000000), status (0x00000000), length (178), timestamp (6:23:23.805297500 04/11/2022), and Ethernet Type 2 details (Destination: 33:33:00:00:FB, Source: 02:15:5D:13:8C:A5 [6-11], Protocol Type: 0x86DD Internet Protocol versia).
- Hex View:** Displays the raw hex and ASCII representation of the selected packet (Packet 1).
- Bottom Bar:** Capturing, Ethernet, Packets: 1,665, Duration: 0:08:22.

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

The screenshot shows the Omnipacket interface with the following details:

- Header:** File, Edit, View, Capture, Tools, Window, Help.
- Toolbar:** Start Page, Capture 1, Stop Capture.
- Packets received:** 1,979.
- Buffer usage:** 0%.
- Filter state:** Accept all packets.
- Dashboards:** Network, Applications, Voice & Video, Compass.
- Capture:** Packets, Events (selected), Notes, Filters.
- Expert:** Clients/Servers, Flows, Applications.
- Web:** Servers, Clients, Pages, Requests.
- Voice & Video:** Calls, Media.
- Visuals:** Peer Map, Graphs.
- Statistics:** Summary, Nodes, Protocols, Applications, Countries.
- Table:** Shows a list of 243 events. The first few rows include:
  - Event 1: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Duplicate ACK (see packet 1735), Packet 1,747 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 2: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Selective ACK (1891152010-1891152160), Packet 1,747 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 3: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Triple Duplicate ACK (see packet 1735), Packet 1,748 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 4: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Duplicate ACK (see packet 1735), Packet 1,748 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 5: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Selective ACK (1891152010-1891152198), Packet 1,748 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 6: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Duplicate ACK (see packet 1735), Packet 1,749 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 7: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Selective ACK (1891152010-1891152847), Packet 1,749 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 8: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Retransmission (0.110689 seconds from packet 1741), Packet 1,752 (10.10.1.11:51917 -> 20.54.24.231:443).
  - Event 9: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Duplicate ACK (see packet 1750), Packet 1,758 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 10: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Selective ACK (1891151923-1891152847), Packet 1,758 (20.54.24.231:443 -> 10.10.1.11:51917).
  - Event 11: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Retransmission (0.351160 seconds from packet 1726), Packet 1,759 (10.10.1.11:51916 -> 20.54.24.169:443).
  - Event 12: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Selective ACK (1656119666-1656119824), Packet 1,760 (20.54.24.169:443 -> 10.10.1.11:51916).
  - Event 13: Date 4/11/2022, Time 6:32:09, Event: Expert: TCP Segment Out of Sequence (got 518472812, expected 518472932) (see packet 1760), Packet 1,761 (20.54.24.169:443 -> 10.10.1.11:51916).
  - Event 14: Date 4/11/2022, Time 6:32:13, Event: Expert: TCP Keep-Alive, Packet 1,779 (10.10.1.11:51832 -> 104.122.62.93:443).
  - Event 15: Date 4/11/2022, Time 6:32:13, Event: Expert: TCP Keep-Alive ACK, Packet 1,780 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 16: Date 4/11/2022, Time 6:32:13, Event: Expert: TCP Selective ACK (954551644-954551645), Packet 1,780 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 17: Date 4/11/2022, Time 6:32:23, Event: Expert: TCP Keep-Alive, Packet 1,800 (10.10.1.11:51832 -> 104.122.62.93:443).
  - Event 18: Date 4/11/2022, Time 6:32:23, Event: Expert: TCP Keep-Alive ACK, Packet 1,801 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 19: Date 4/11/2022, Time 6:32:23, Event: Expert: TCP Keep-Alive ACK, Packet 1,801 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 20: Date 4/11/2022, Time 6:32:23, Event: Expert: TCP Selective ACK (954551644-954551645), Packet 1,801 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 21: Date 4/11/2022, Time 6:32:33, Event: Expert: ICMP Port Unreachable , Packet 1,889 (8.8.8.8:53 -> 10.10.1.11:54467).
  - Event 22: Date 4/11/2022, Time 6:32:33, Event: Expert: TCP Keep-Alive, Packet 1,911 (10.10.1.11:51832 -> 104.122.62.93:443).
  - Event 23: Date 4/11/2022, Time 6:32:33, Event: Expert: TCP Keep-Alive ACK, Packet 1,912 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 24: Date 4/11/2022, Time 6:32:33, Event: Expert: TCP Selective ACK (954551644-954551645), Packet 1,912 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 25: Date 4/11/2022, Time 6:32:43, Event: Expert: TCP Keep-Alive, Packet 1,936 (10.10.1.11:51832 -> 104.122.62.93:443).
  - Event 26: Date 4/11/2022, Time 6:32:43, Event: Expert: TCP Keep-Alive ACK, Packet 1,937 (104.122.62.93:443 -> 10.10.1.11:51832).
  - Event 27: Date 4/11/2022, Time 6:32:43, Event: Expert: TCP Selective ACK (954551644-954551645), Packet 1,937 (104.122.62.93:443 -> 10.10.1.11:51832).
- Bottom Bar:** Capturing, Ethernet, Packets: 1,979, Duration: 0:09:26.

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

The screenshot shows the CyberQ interface with the following details:

- Top Bar:** Omnipack (with a magnifying glass icon), File, Edit, View, Capture, Tools, Window, Help, CyberQ, LiveAction.
- Packets Received:** 2,005, **Buffer Usage:** 0%, **Filter State:** Accept all packets, **Stop Capture** button.
- Dashboards:** Network, Applications, Voice & Video, Compass.
- Capture:** Packets, Events, Notes, Filters.
- Expert:** Clients/Servers, Flows, Applications.
- Web:** Servers, Clients, Pages, Requests.
- Voice & Video:** Calls, Media.
- Visuals:** Peer Map, Graphs.
- Statistics:** Summary, Nodes, Protocols, Applications, Countries.
- Flows Analyzed:** 45, **Events Detected:** 242, **Flows Recycled:** 0, **Packets Dropped:** 0.
- Table (Flows):**| Client Addr | Server Addr | Flows | Events | Packets | Bytes | Duration | 3-Way Handshake |
| --- | --- | --- | --- | --- | --- | --- | --- |
| > 10.10.1.11 | 8.8.4.4 | 1 | 15 | 37 | 5,242 | 0:04:00.073761 | 0.008456 |
| > 10.10.1.11 | dns.google | 8 | 4 | 64 | 14,939 | 0:09:09.437986 | 0.009204 |
| > 10.10.1.11 | 20.54.24.169 | 6 | 12 | 61 | 12,742 | 0:08:42.152606 | 0.111949 |
| > 10.10.1.11 | 20.54.24.231 | 1 | 10 | 27 | 7,006 | 0.560403 | 0.112031 |
| > 10.10.1.11 | contile.services.mozilla.com | 1 | 0 | 34 | 5,406 | 0:02:51.063152 | 0.008659 |
| > 10.10.1.11 | login.live.com | 1 | 2 | 31 | 25,448 | 0.306475 | 0.041843 |
| > 10.10.1.11 | 44.193.133.112 | 1 | 3 | 63 | 7,163 | 0:09:31.249861 |  |
| > 10.10.1.11 | 44.229.115.174 | 1 | 1 | 6 | 492 | 0:05:00.176800 |  |
| > 10.10.1.11 | 52.0.218.127 | 1 | 0 | 90 | 17,850 | 0:09:32.322412 |  |
| > 10.10.1.11 | settings-prod-eus2-2.east... | 1 | 3 | 30 | 10,020 | 0.589378 | 0.038076 |
| > 10.10.1.11 | 52.167.85.21 | 1 | 0 | 31 | 3,742 | 0:03:52.020824 |  |
| > 10.10.1.11 | teams.events.data.micros... | 1 | 0 | 18 | 12,627 | 0.203290 | 0.036287 |
| > 10.10.1.11 | onedsblobprdeus16.east... | 1 | 0 | 23 | 12,569 | 0.376195 | 0.039297 |
| > 10.10.1.11 | 52.182.141.63 | 1 | 7 | 73 | 12,997 | 0:02:05.201068 | 0.048714 |
- Event Log:**

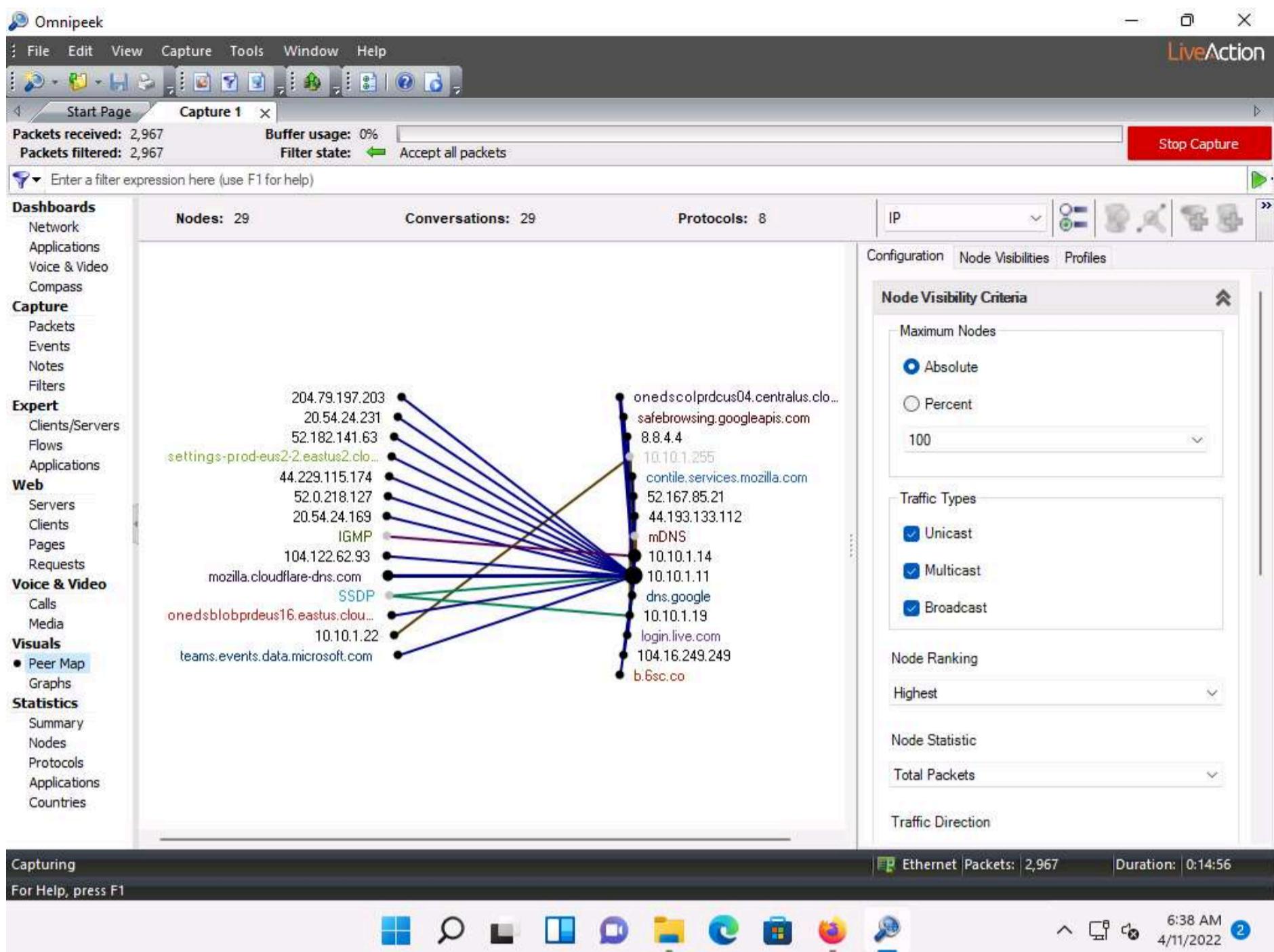
Layer	Event	Count	First Time	Last Time
Transport	TCP Selective ACK	81	4/11/2022 6:23:25	4/11/2022 6:32:43
Transport	TCP Keep-Alive	62	4/11/2022 6:23:35	4/11/2022 6:32:43
Transport	TCP Keep-Alive ACK	61	4/11/2022 6:23:36	4/11/2022 6:32:43
Transport	TCP Duplicate ACK	12	4/11/2022 6:23:38	4/11/2022 6:32:09
Transport	TCP Retransmission	8	4/11/2022 6:23:27	4/11/2022 6:32:09
Transport	TCP Segment Out of Sequence	4	4/11/2022 6:24:29	4/11/2022 6:32:09
Transport	TCP Triple Duplicate ACK	3	4/11/2022 6:23:38	4/11/2022 6:32:09
Client/Server	Non-Responsive Server	3	4/11/2022 6:24:39	4/11/2022 6:24:46
Network	ICMP Port Unreachable	3	4/11/2022 6:23:38	4/11/2022 6:32:33
- Capturing:** Ethernet, Packets: 2,005, Duration: 0:09:45.
- Bottom Bar:** Icons for File, Edit, View, Capture, Tools, Window, Help, and a search bar.

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

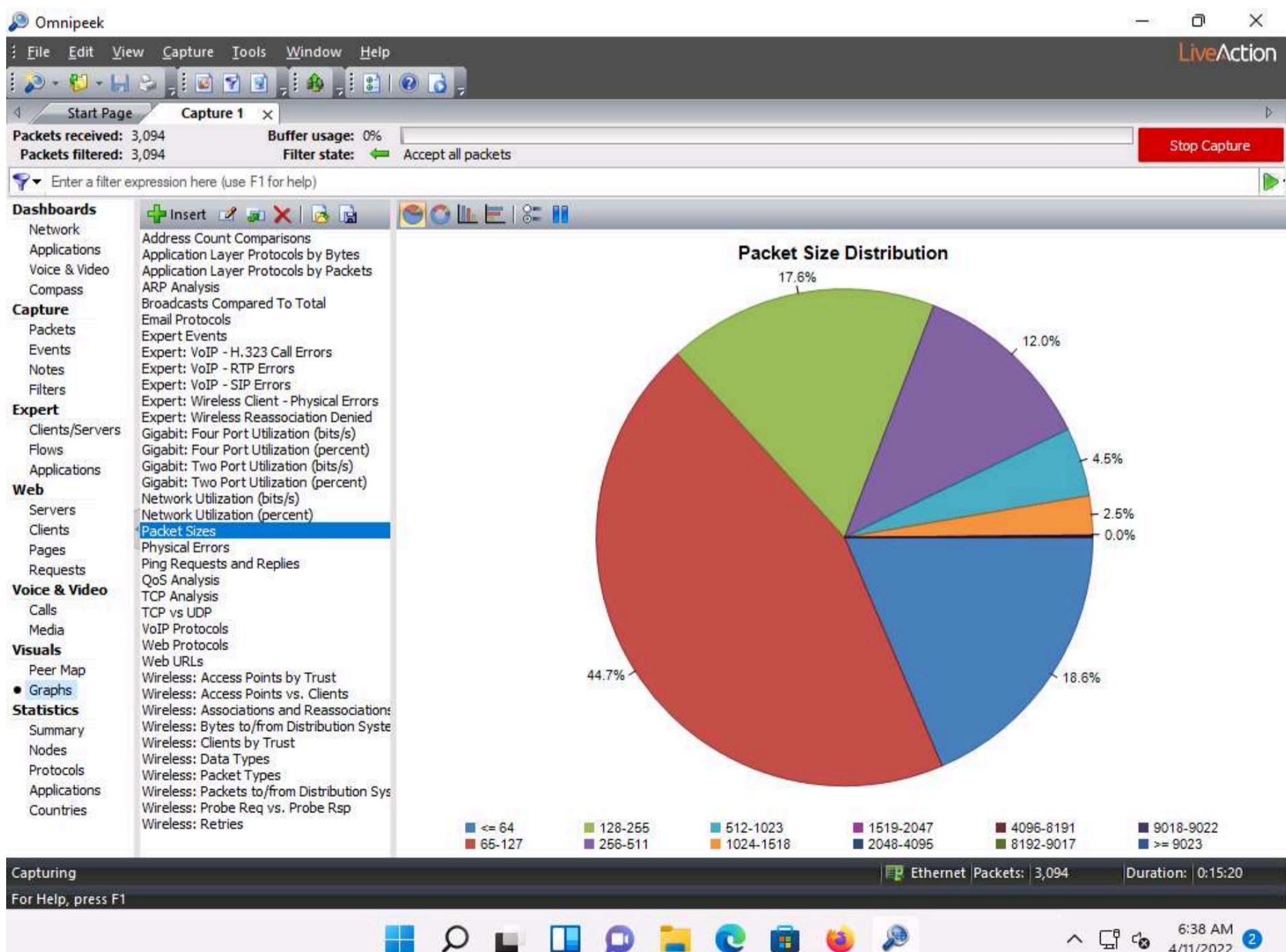
31. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.

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.

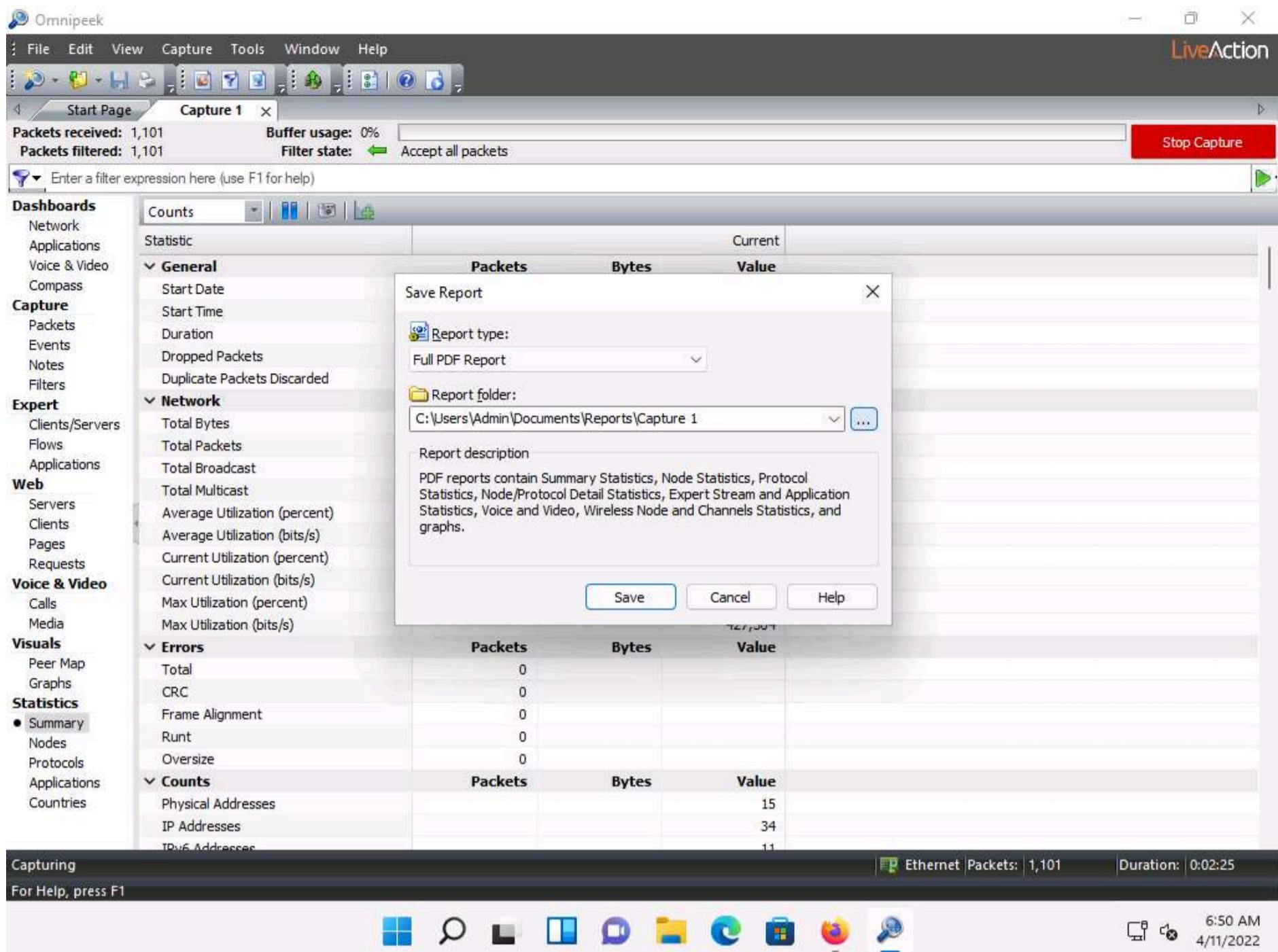
The screenshot shows the Omnipacket software interface. The main window displays a summary of packet captures. At the top, it says "Packets received: 3,144" and "Packets filtered: 3,144". The "Buffer usage: 0%" is shown as 0%. The "Filter state" is set to "Accept all packets". A red "Stop Capture" button is visible in the top right corner. Below the summary, there's a search bar with the placeholder "Enter a filter expression here (use F1 for help)". On the left, a sidebar lists various monitoring categories: Dashboards, Capture, Expert, Web, Voice & Video, Visuals, and Statistics. Under "Statistics", the "Summary" tab is selected. The main pane shows a table of statistics with columns "Statistic", "Packets", "Bytes", and "Value". Some entries include "Flows Analyzed (Total)", "Events - Total", and "Events - Severe". The table also includes sections for "Expert" and "Capture" statistics.

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.

The screenshot shows the Omnipacket software interface with the "File" menu open. The "Save Report..." option is highlighted with a yellow selection bar. The menu also includes options like "New Capture...", "Open...", "Save All Packets...", "Print Setup...", "Print...", "Properties", and "Exit". The main workspace shows a table of statistics with columns "Packets", "Bytes", and "Value". The table includes rows for "Events - Total", "Events - Informational", and "Events - Minor". The bottom status bar indicates "Idle" and "Saves a report".

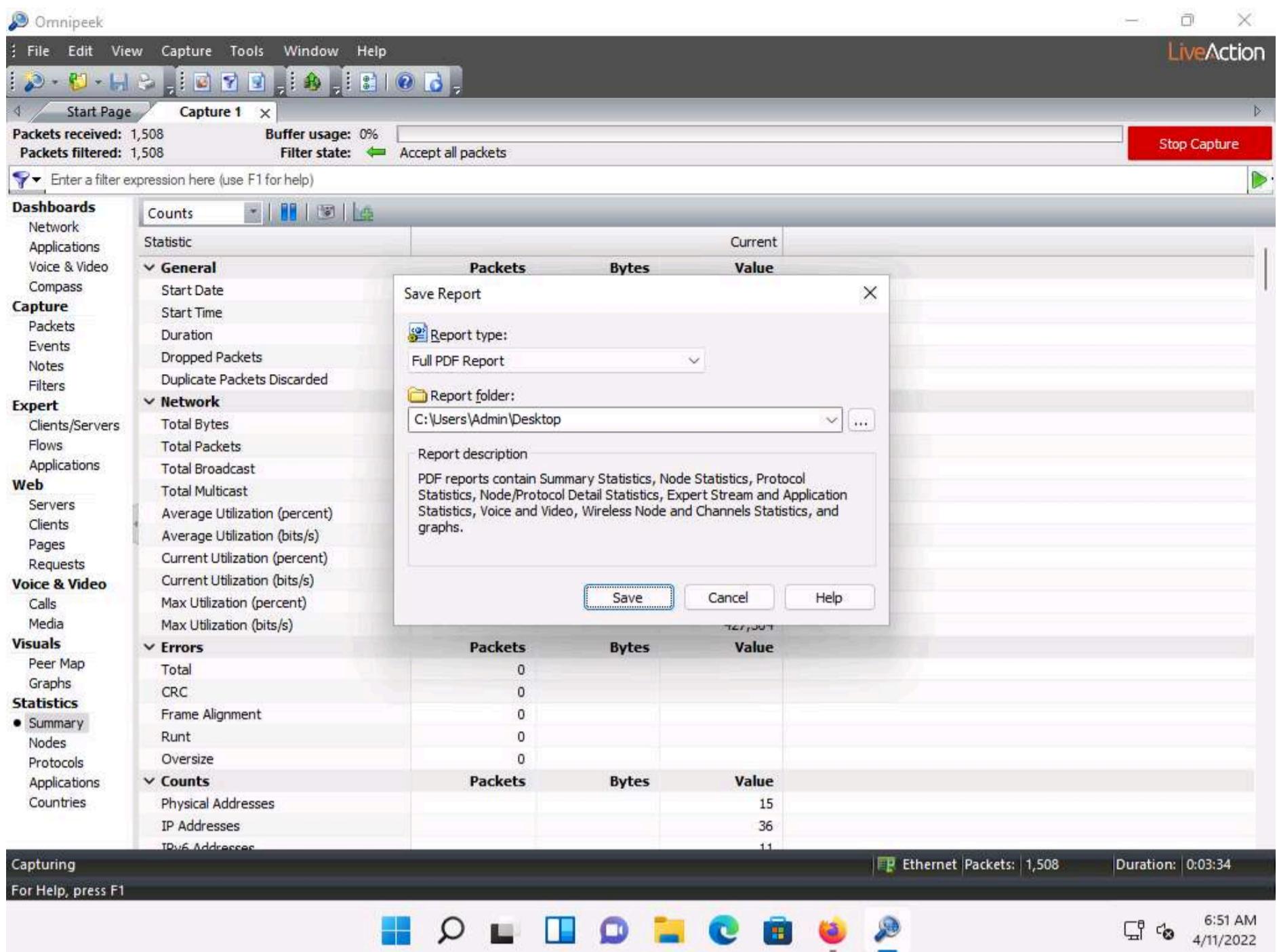
37. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon to change the download location.



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

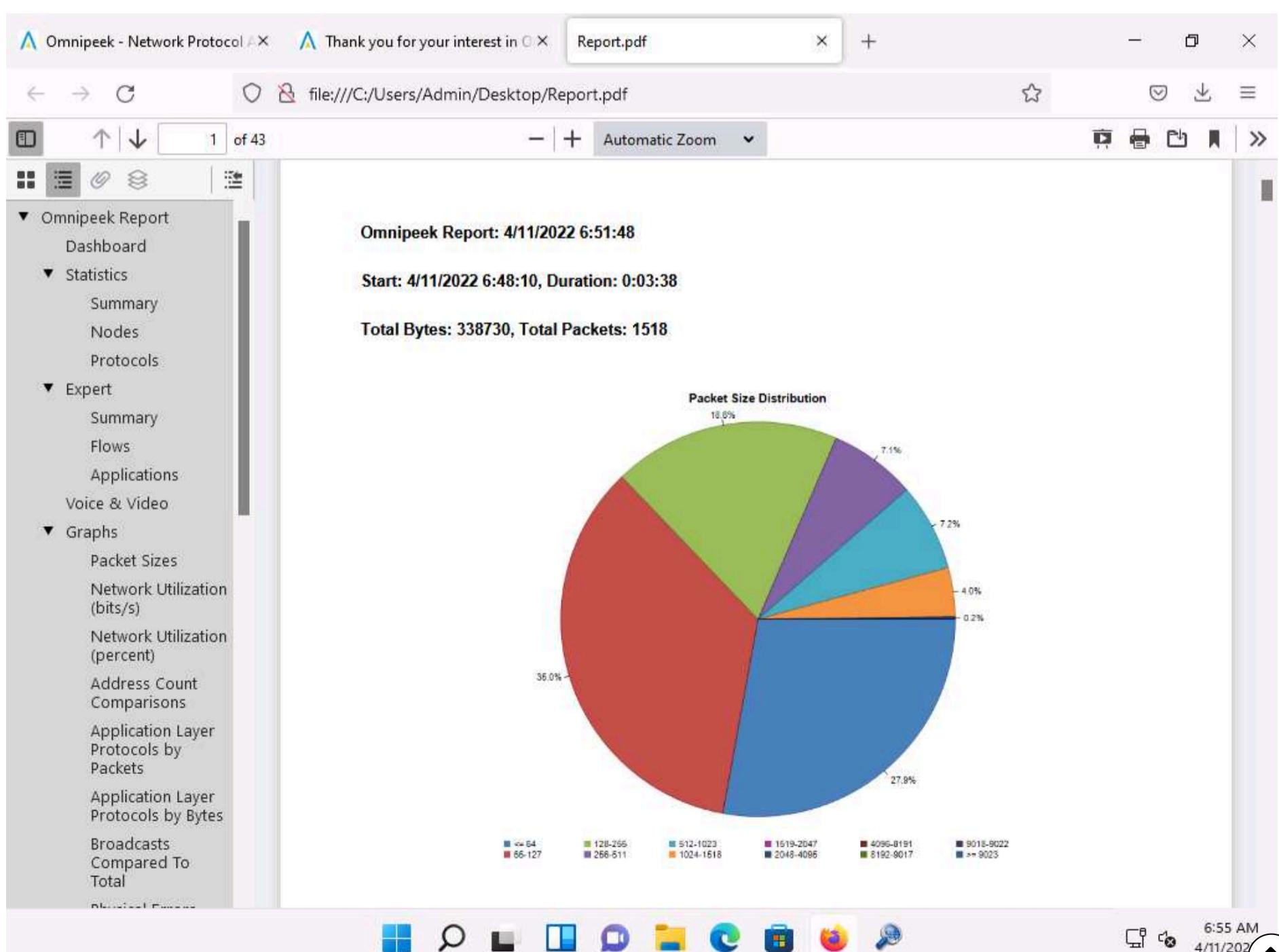
39. The changed save location appears in the **Report folder** field; click the **Save** button to save the report.





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

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



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

**Summary Statistics: Reported 4/11/2022 6:51:48**

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

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

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

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

## Task 3: Analyze a Network using the SteelCentral Packet Analyzer

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

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

- 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**.
- 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**.

The screenshot shows the Riverbed website with several promotional banners for different products:

- NetPromoter**: LEARN MORE >
- Alluvio AppResponse / Packet Analyzer Plus Trial**: 30 DAY FREE TRIAL, Try Alluvio AppResponse/Packet Analyzer Plus Trial, LEARN MORE >
- Alluvio Portal**: 30 DAY FREE TRIAL, Try Alluvio Portal, LEARN MORE >

A notification bar at the top right indicates "2 new notifications". The taskbar at the bottom shows various open applications.

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.

The screenshot shows the "Alluvio AppResponse / Packet Analyzer Plus" trial download page. The main content includes:

## Application Performance Issues Fast

**Alluvio AppResponse and Packet Analyzer Plus**

Only Alluvio AppResponse combines network forensics and historical analysis, application analytics and end-user experience monitoring in a single solution. It's everything you need to resolve performance issues quickly.

**Start your Free Trial to:**

- Rapidly identify and triage problems to minimize downtime

The right side features a registration form with fields for name, company, address, city, state, zip, and country. There are also dropdown menus for phone number and fax number. A checkbox for receiving communications from Riverbed is present, along with a note about unsubscribe rights and a link to the Privacy Policy. A large red "SUBMIT" button is at the bottom.

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.

The screenshot shows a web browser window with the following details:

- Title Bar:** Free Product Trial Downloads | X and Alluvio AppResponse / Packet X.
- Address Bar:** https://www.riverbed.com/trial-download/alluvio-appresponse-packet-analyzer-plus-trial
- Header:** English, Blogs, Partner Login, Community, Support, Careers, Trust Center, Contact Us.
- Main Content:**
  - Section Header:** Application Performance Issues Fast.
  - Text:** Alluvio AppResponse and Packet Analyzer Plus.
  - Description:** Only Alluvio AppResponse combines network forensics and historical analysis, application analytics and end-user experience monitoring in a single solution. It's everything you need to resolve performance issues quickly.
  - Call-to-Action:** Start your Free Trial to:
    - Rapidly identify and triage problems to minimize downtime
  - Right Column:** Thank you for your interest in the Alluvio AppResponse free trial. Now that you have completed the registration form, you will receive an email with your license key and can begin downloading the virtual edition of AppResponse.
  - Sign-off:** Thank you,  
- Riverbed
  - Footnote:** \*Sometimes the email may be caught in your SPAM folder.
  - Bottom:** Please check and release, 9:09 PM, 4/11/2022, 2 notifications.

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.

The screenshot shows an Outlook inbox with several notifications at the top:

- Add "outlook.office.com" as an application for mailto links? [Add application](#)
- It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! [Refresh Firefox...](#)

The main interface includes a search bar, a Teams call button, and various message management buttons (New message, Delete, Archive, Junk, Sweep, Move to). The inbox list shows one item from "noreply@riverbed.com" titled "Riverbed Evaluation Licens..." received at 9:40 AM. The message body is as follows:

Dear Riverbed Customer,

Thank you for your interest in evaluating SteelCentral Packet Analyzer Plus from Riverbed Technology, Inc. SteelCentral Packet Analyzer Plus speeds network packet analysis and reporting of large trace files for SteelCentral AppResponse 11.

The SteelCentral Packet Analyzer Plus software can be downloaded [here](#).

Here are the evaluation product keys needed for your software. The product key begins after the "--" symbol. This is what you will input into your product:

[REDACTED]

To activate a Packet Analyzer Plus license:

1. Launch a Packet Analyzer Plus session.

6. The Opening **PacketAnalyzer\_11.13.0\_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.



SteelHead

Network Performance Management

AppCapacity

AppResponse

**AppResponse 11**

NetAuditor

NetCollector

NetIM Products

NetPlanner

NetProfiler and NetExpress

NetSensor

NetShark

Packet Analyzer

**Packet Analyzer Plus**

SteelCentral AppResponse Virtual Edition for ESXi Version 11.13.0

Opening PacketAnalyzerPlus\_11.13.0\_Setup.exe

You have chosen to open:  
PacketAnalyzerPlus\_11.13.0\_Setup.exe  
which is: exe File (55.8 MB)  
from: https://download.riverbed.com

Would you like to save this file?

Save File Cancel

SteelCentral Packet Analyzer Plus Setup Version 11.13.0 Mar 21, 2022

Software (55.8 MB) Checksum Release Notes

Downloads

Help us improve

Did you find this useful?  
Yes No

https://support.riverbed.com/bin/support/download?sid=rmtlbf6cs9rhikok6cfm3dmfvb

9:19 PM 4/11/2022 1

- On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer\_11.13.0\_Setup.exe**.

Downloads

New Sort View ...

This PC > Downloads

Search Downloads

Quick access

Desktop

**Downloads**

Documents

Pictures

Music

Videos

OneDrive

This PC

Desktop

Documents

Downloads

Music

Pictures

Videos

Local Disk (C:)

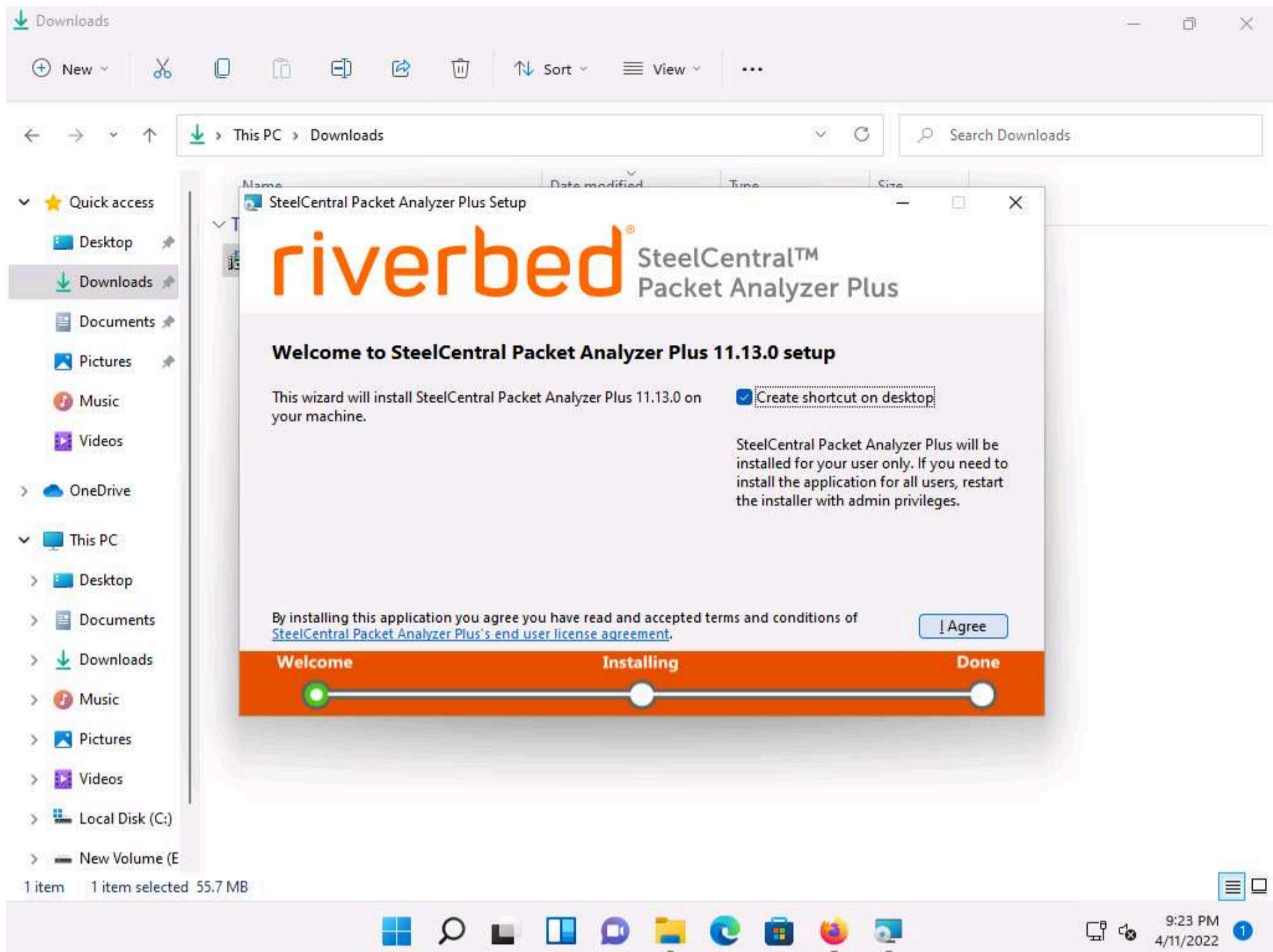
New Volume (E)

1 item 1 item selected 55.7 MB

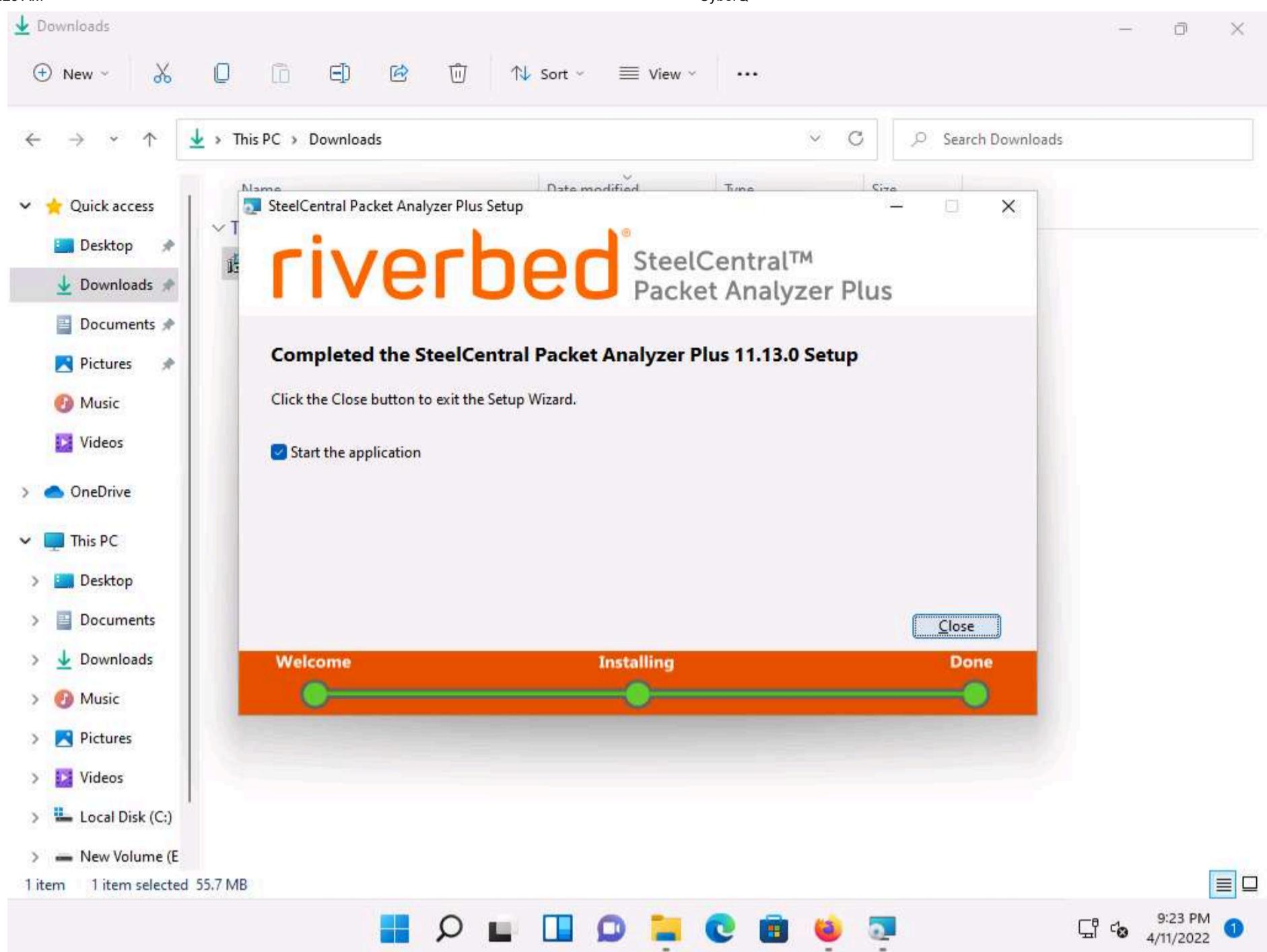
9:22 PM 4/11/2022 1

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

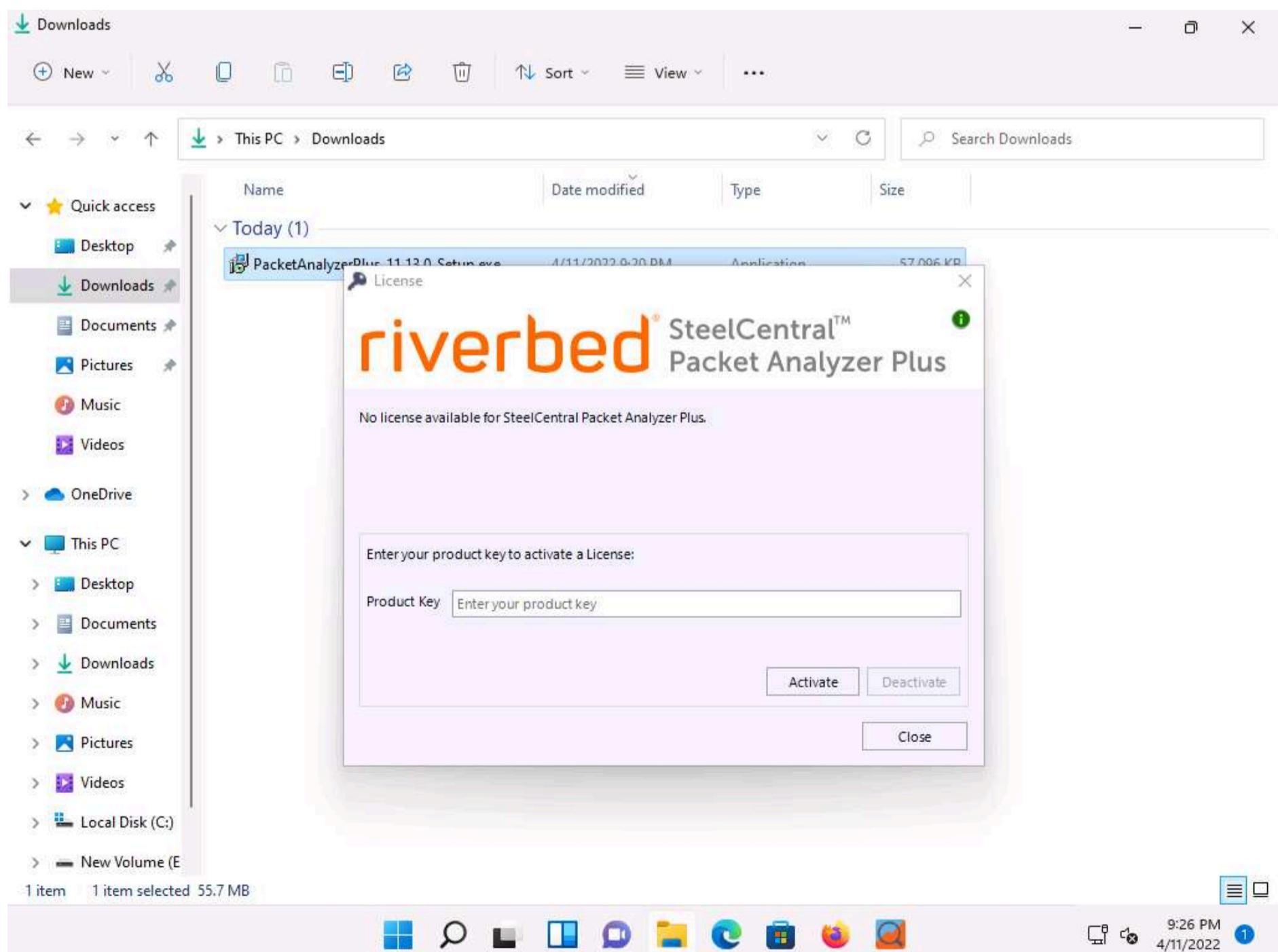
9. The SteelCentral Packet Analyzer Plus Setup window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.



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.

Dear Riverbed Customer,

Thank you for your interest in evaluating SteelCentral Packet Analyzer Plus from Riverbed Technology, Inc. SteelCentral Packet Analyzer Plus speeds network packet analysis and reporting of large trace files for SteelCentral AppResponse 11.

The SteelCentral Packet Analyzer Plus software can be downloaded [here](#).

Here are the evaluation product keys needed for your software. The product key begins after the "--" symbol. This is what you will input into your product.

**--PAP-1000-1000  
--PAP-1000-1000**

To activate a Packet Analyzer Plus license:

1. Launch a Packet Analyzer Plus session.

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**.

Downloads

This PC > Downloads

Name	Date modified	Type	Size
PacketAnalyzerPlus_11.1.0.1000.license			

**riverbed® SteelCentral™  
Packet Analyzer Plus**

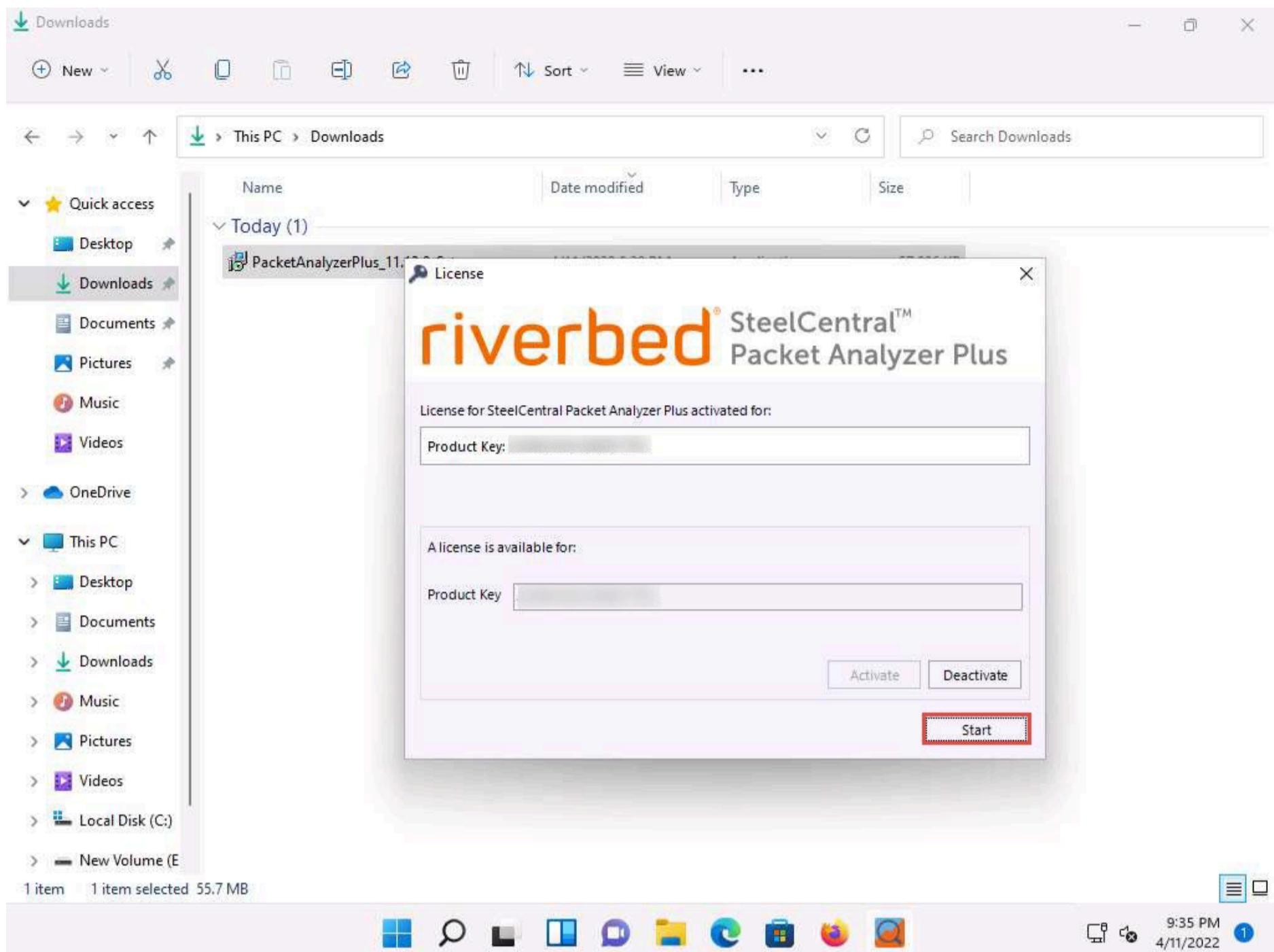
No license available for SteelCentral Packet Analyzer Plus.

Enter your product key to activate a License:

Product Key

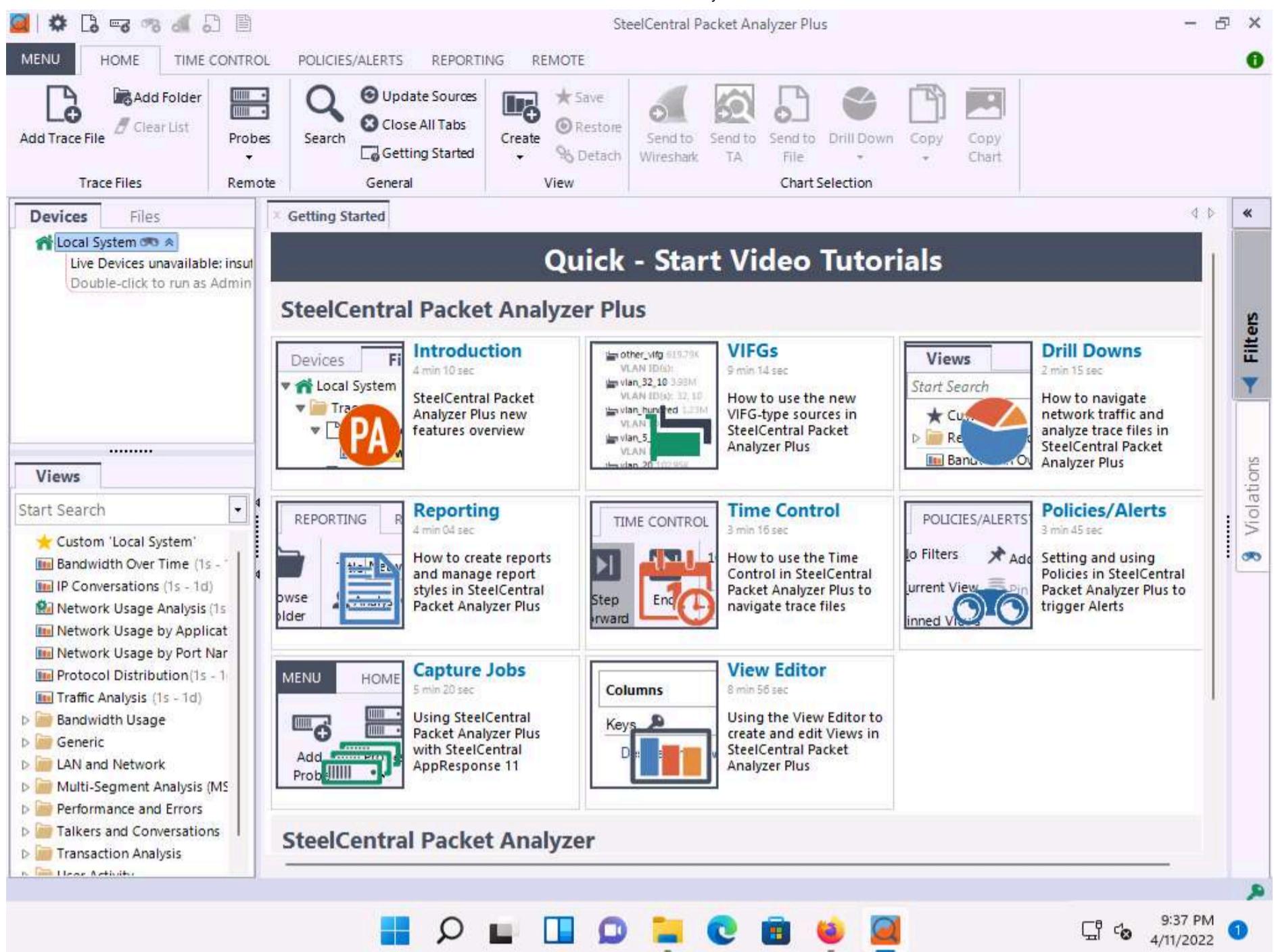
Activate Deactivate Close

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

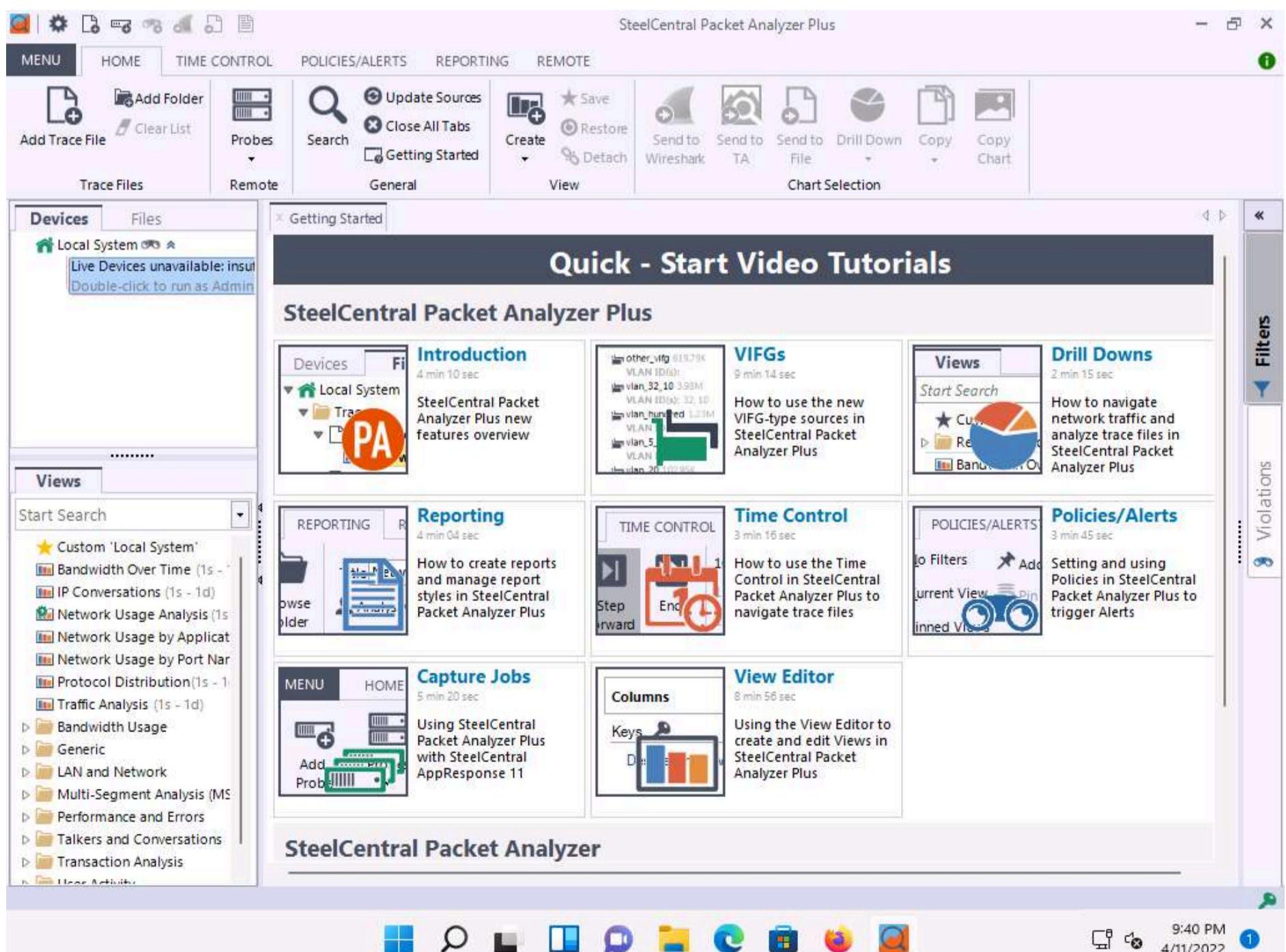


15. The SteelCentral Packet Analyzer Plus main window appears, displaying the Getting Started tab options, as shown in the screenshot.



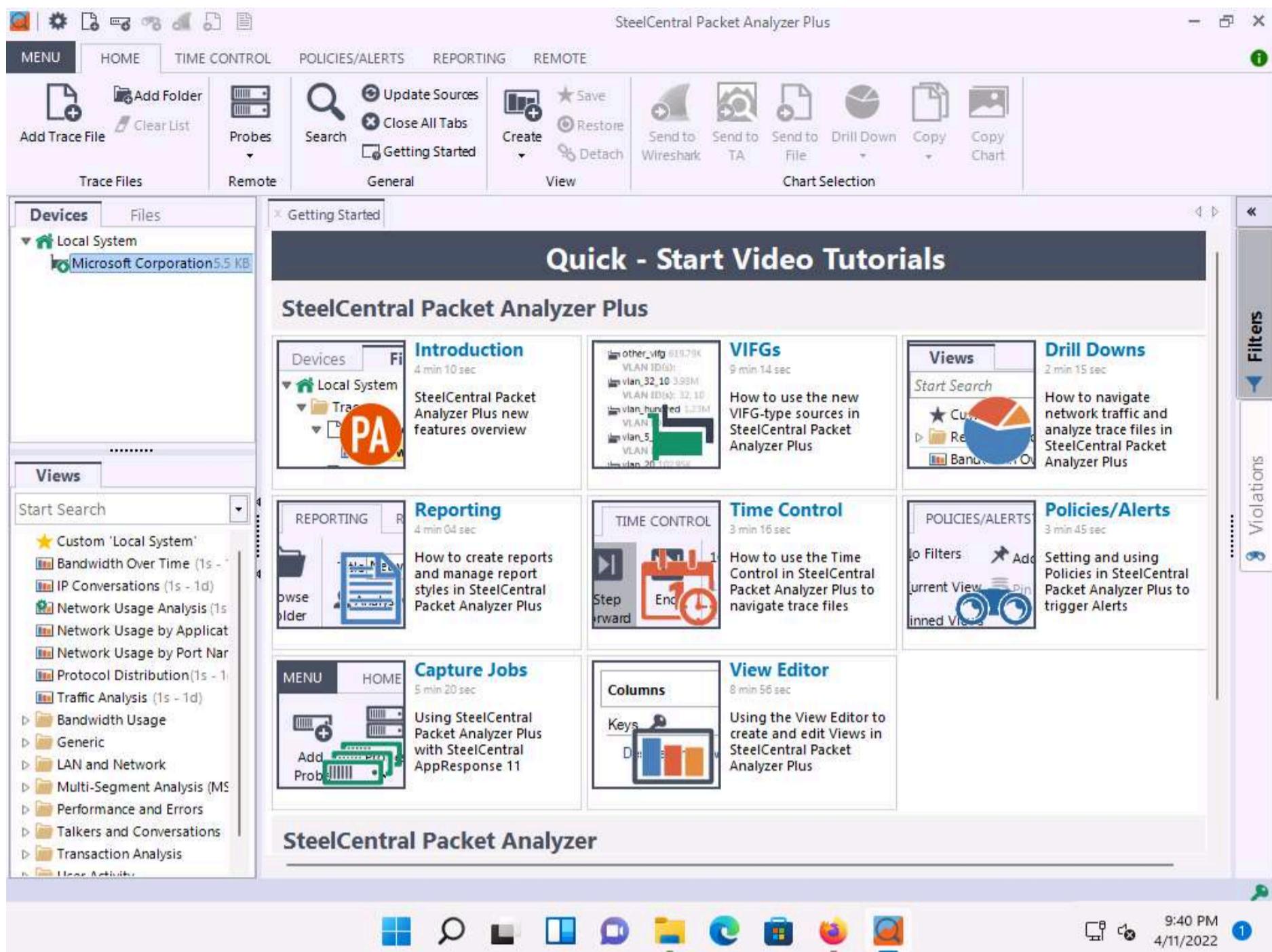


16. Observe that under the **Devices** tab in the left-hand pane, the application is unable to detect any **Local System** as it requires admin privileges. Therefore, double-click **Live Devices unavailable: Insufficient privileges** to run the application as an **Administrator**.



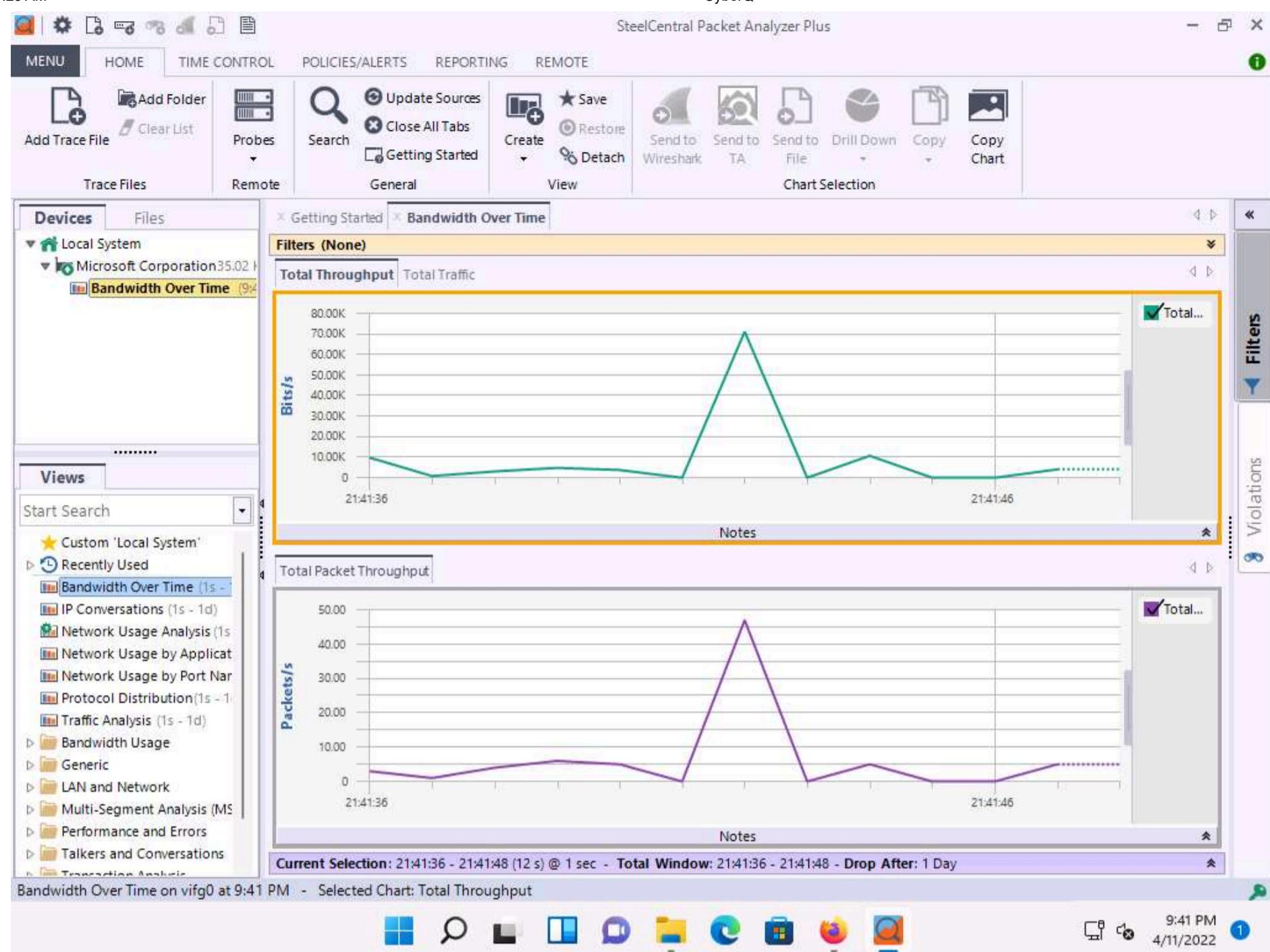
17. A **User Account Control** pop-up appears; click **Yes**.

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



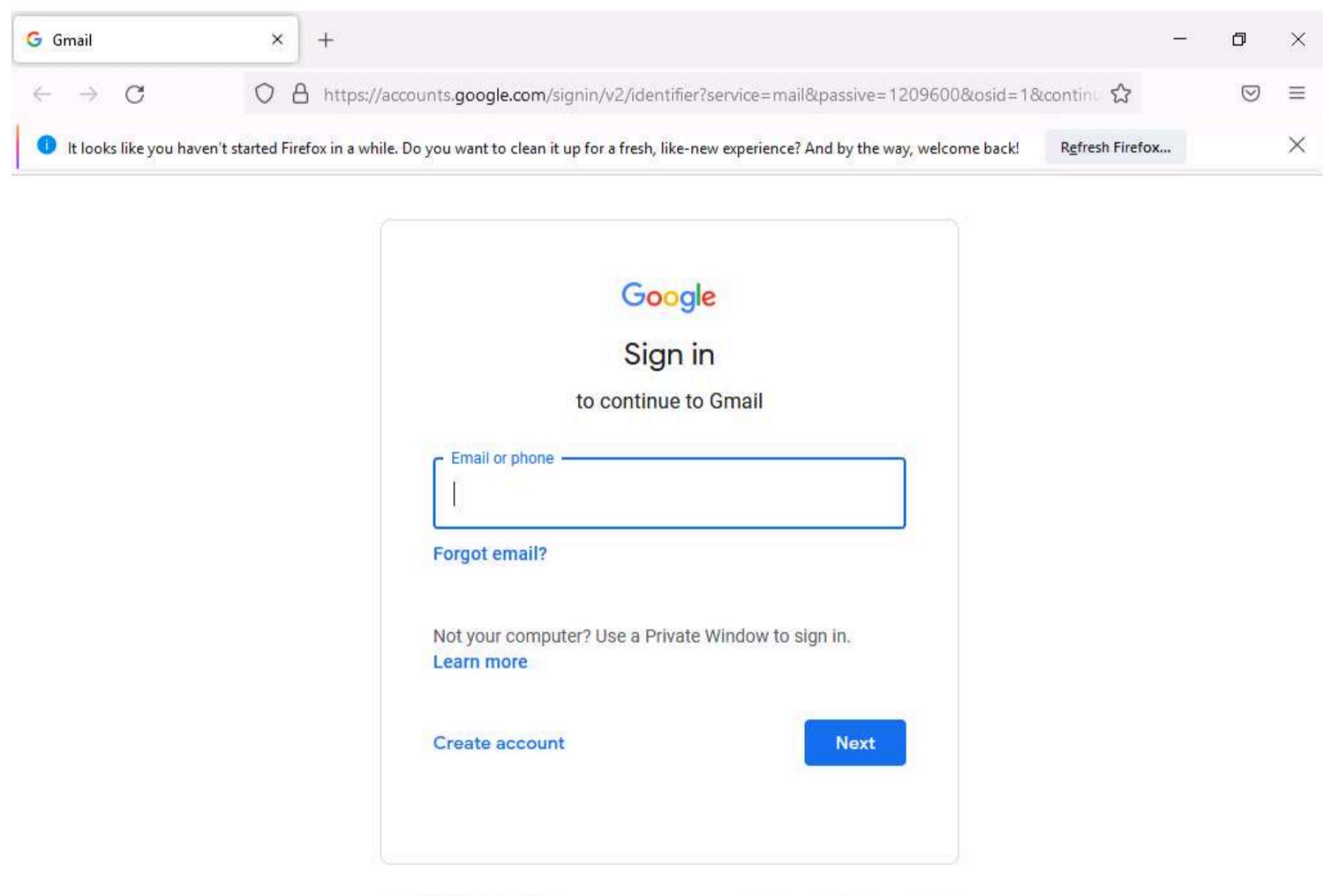
19. Double-click the **Bandwidth Over Time** option under the **Recently Used** node in the left-hand pane under the **Views** section.

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

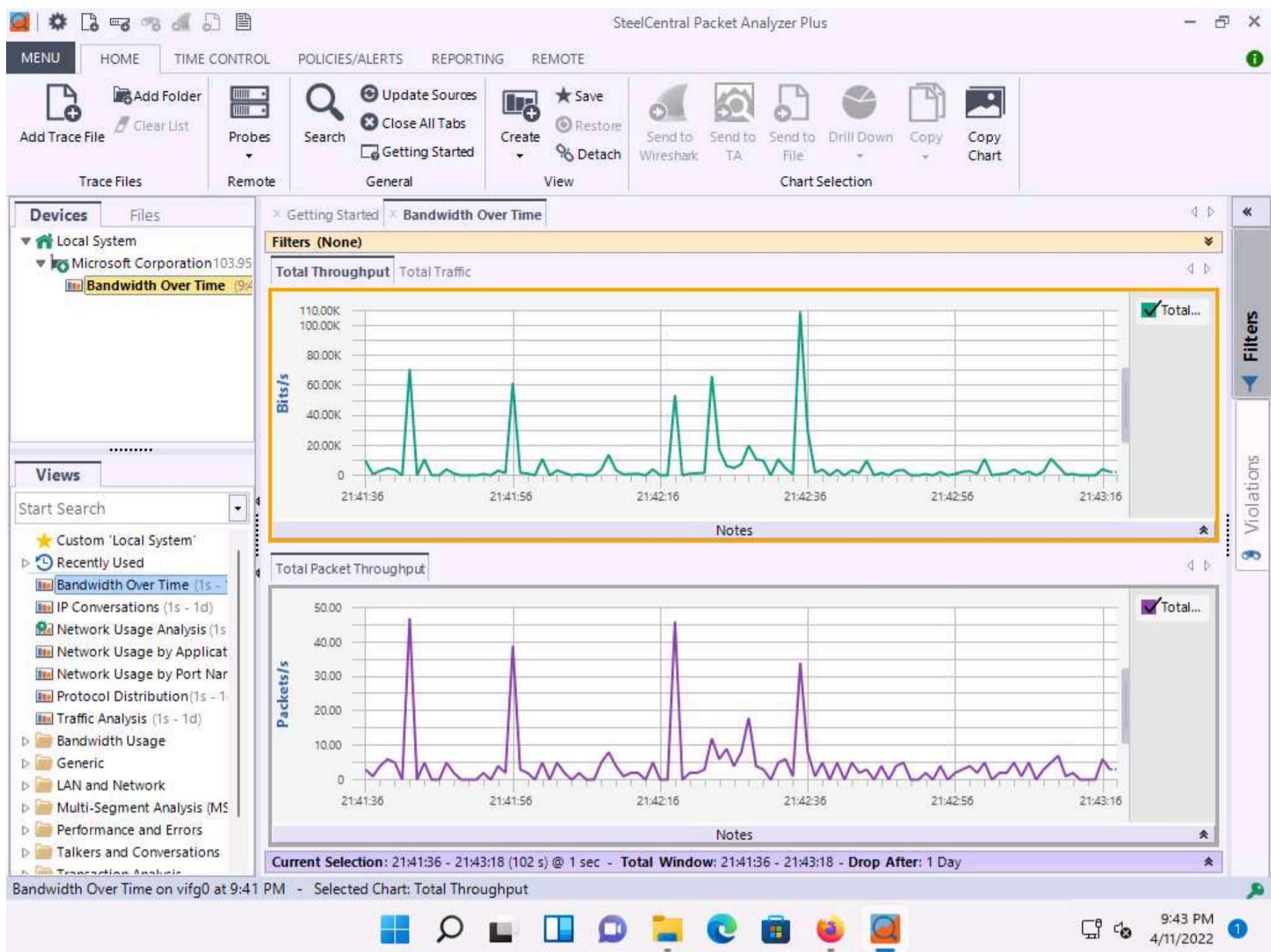


21. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

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

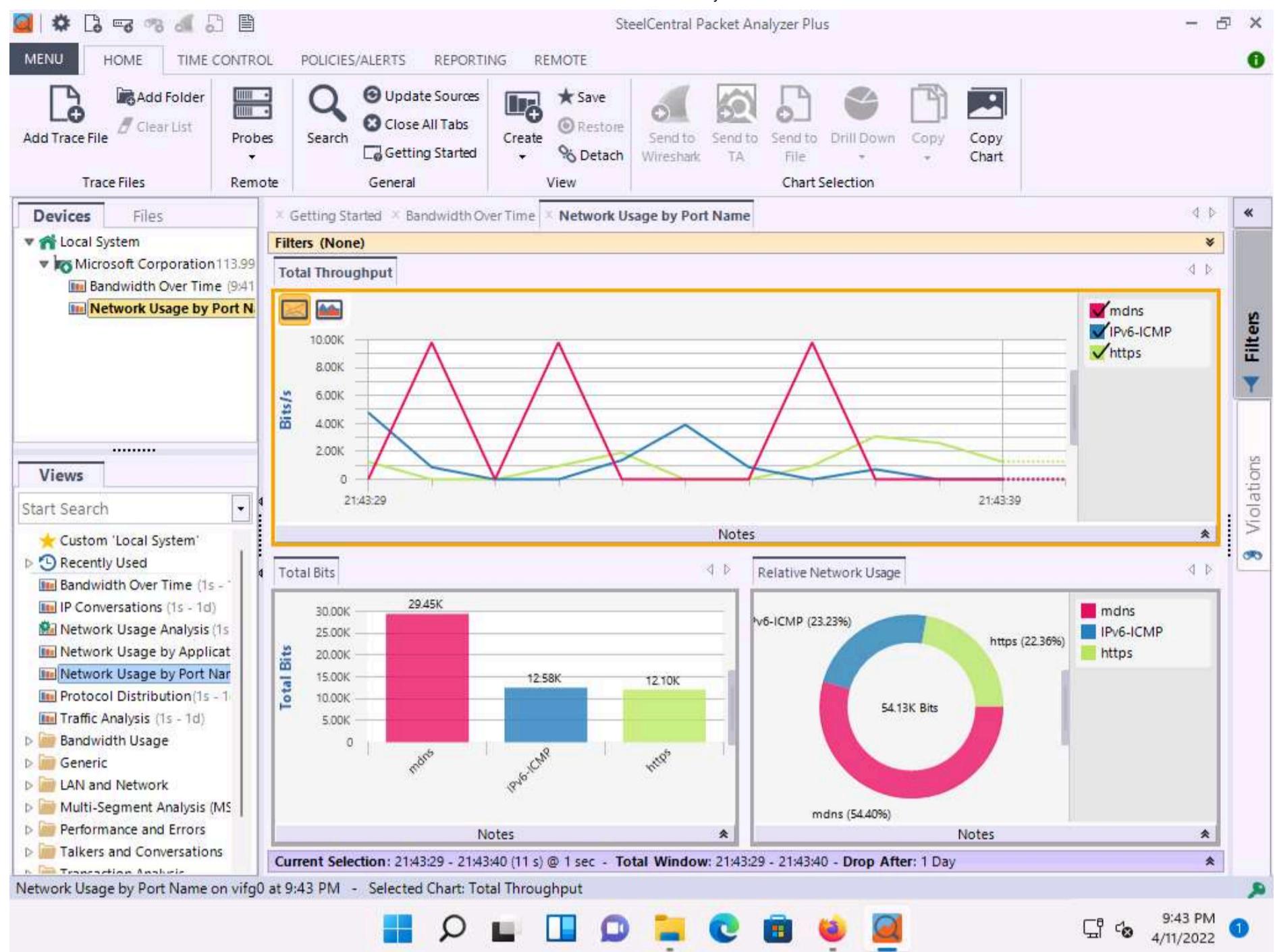


23. Click **CEHv12 Windows 11** to switch back to the **Windows 11** machine and observe the network traffic captured by **SteelCentral Packet Analyzer**, as shown in the screenshot.



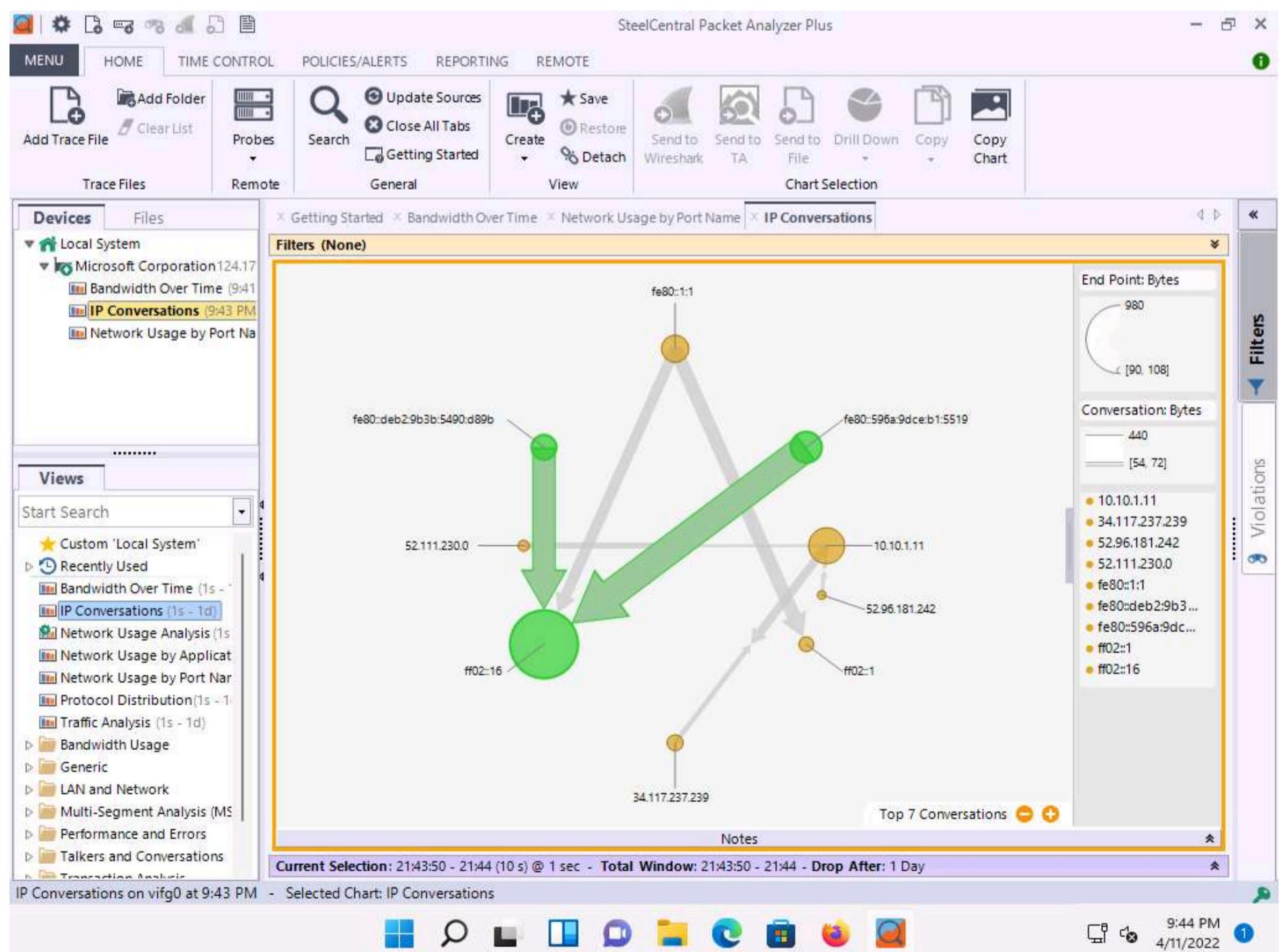
24. Double-click the **Network Usage by Port Name** option under the **Recently Used** node in the left-hand pane under the **Views** section.

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



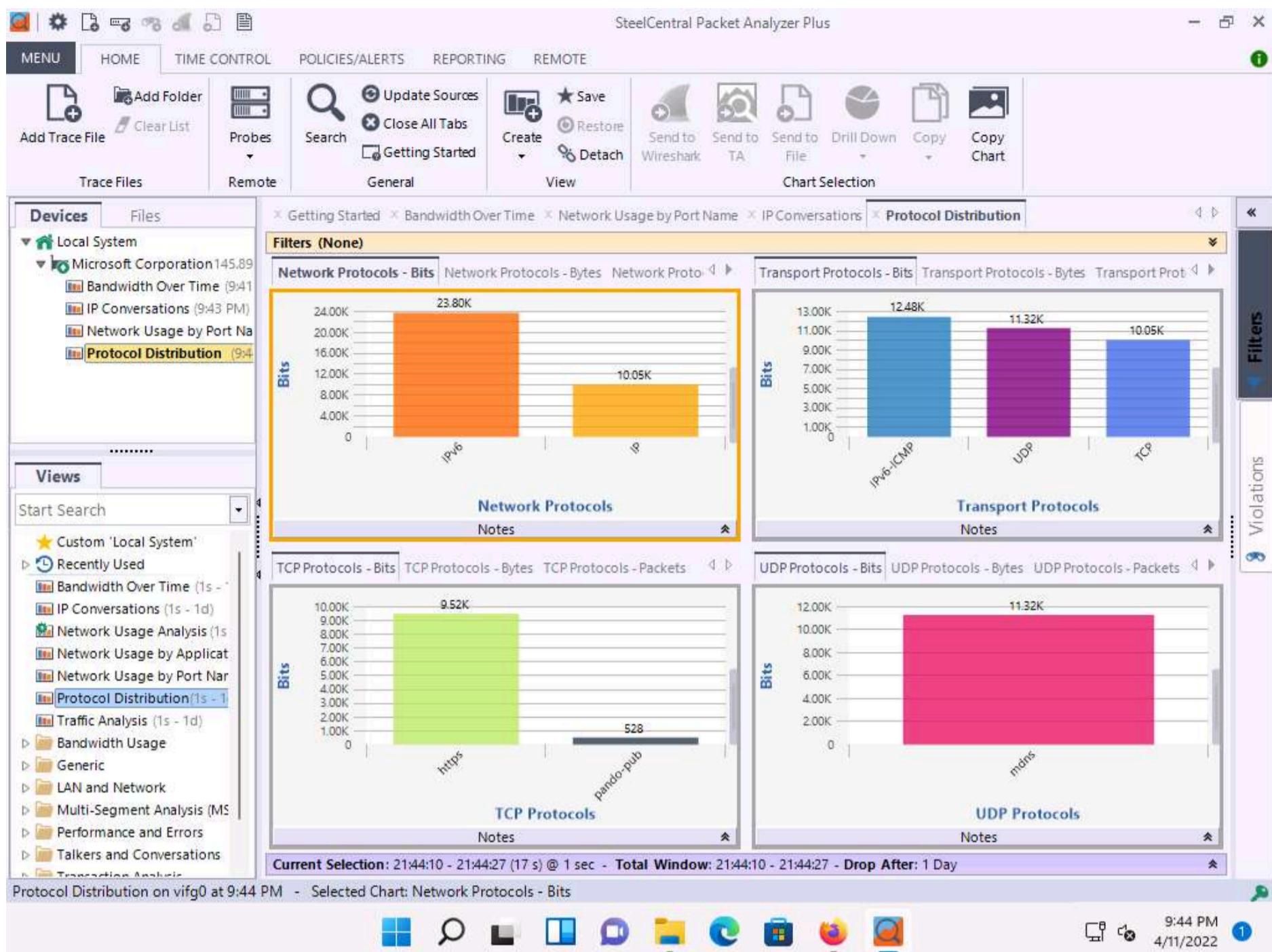
26. Double-click the **IP Conversations** option under the **Recently Used** node in the left-hand pane under the **Views** section.

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.

SteelCentral Packet Analyzer Plus

**HOME** TIME CONTROL POLICIES/ALERTS REPORTING REMOTE

Add Trace File Add Folder Probes Search Update Sources Close All Tabs Save Restore Create Detach Send to Wireshark Send to TA Send to File Drill Down Copy Copy Chart

Trace Files Remote General View Chart Selection

**Devices** Files

Local System Microsoft Corporation 160.58

- Bandwidth Over Time (9:41)
- Capture Summary (9:44 PM)**
- IP Conversations (9:43 PM)
- Network Usage by Port Name
- Protocol Distribution (9:44)

Views Start Search

- Custom 'Local System'
- Recently Used
  - Bandwidth Over Time (1s - 1d)
  - IP Conversations (1s - 1d)
  - Network Usage Analysis (1s)
  - Network Usage by Application
  - Network Usage by Port Name
  - Protocol Distribution (1s - 1d)
  - Traffic Analysis (1s - 1d)
- Bandwidth Usage
- Generic
  - Capture Summary (1s - 1d)**
  - Frame Size Distribution (1s)
  - Frame Size Over Time (1s)
- LAN and Network
- Multi-Comment Analysis (MAC)

**Capture Summary**

**Filters (None)**

Statistic Name	Value
Total Number of Bytes	2.53K
Total Number of Packets	20
Number IP Bytes	2.53K
Number TCP Bytes	616
Number UDP Bytes	1.23K

Notes

Current Selection: 21:44:44 - 21:44:53 (9 s) @ 1 sec - Total Window: 21:44:44 - 21:44:53 - Drop After: 1 Day

9:44 PM 4/11/2022

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.

SteelCentral Packet Analyzer Plus

**HOME** TIME CONTROL POLICIES/ALERTS REPORTING REMOTE

Add Trace File Add Folder Probes Search Update Sources Close All Tabs Save Restore Create Detach Send to Wireshark Send to TA Send to File Drill Down Copy Copy Chart

Trace Files Remote General View Chart Selection

**Devices** Files

Local System Microsoft Corporation 176.2

- Bandwidth Over Time (9:41)
- Capture Summary (9:44 PM)
- IP Conversations (9:43 PM)
- MAC Overview (9:45 PM)**
- Network Usage by Port Name
- Protocol Distribution (9:44)

Views Start Search

- DNS Responses (1s - 1d)
- DNS Server Analysis (1s - 1d)
- ICMP Overview (1s - 1d)
- ICMP Types Over Time (1s)
- LLDP Port Configuration (1s)
- MAC CRC Errors (1s - 1d)
- MAC Overview (1s - 1d)**
- MPLS vs. Non-MPLS Traffic (1s)
- Network Protocol Distribution (1s)
- Network Protocol Distribution (1s)
- Ping Time (1s - 1d) Steel
- Relayed DHCP vs. Total T
- Top ICMP Stats (1s - 1d)
- Top MAC Unicast, Multicast (1s - 1d)
- Top MPLS Labels (1s - 1d)
- Top MPLS Traffic Classes (1s - 1d)

**MAC Overview**

**Filters (None)**

**Total Throughput**

Bits/s

21:45:21 21:45:31

**Top MAC Sources** Top MAC Destinations

Source MAC Address	Bytes
02:15:5d:28:76	58.03K
02:15:5d:28:76	4.00K
02:15:5d:28:76	1.76K
02:15:5d:28:76	1.44K
Microsoft_01:80:00	872

**Conversations**

End Point: Bytes

- 7.25K [42, 401]
- 4.51K [42, 549]
- Microsof\_01:80:00 ...

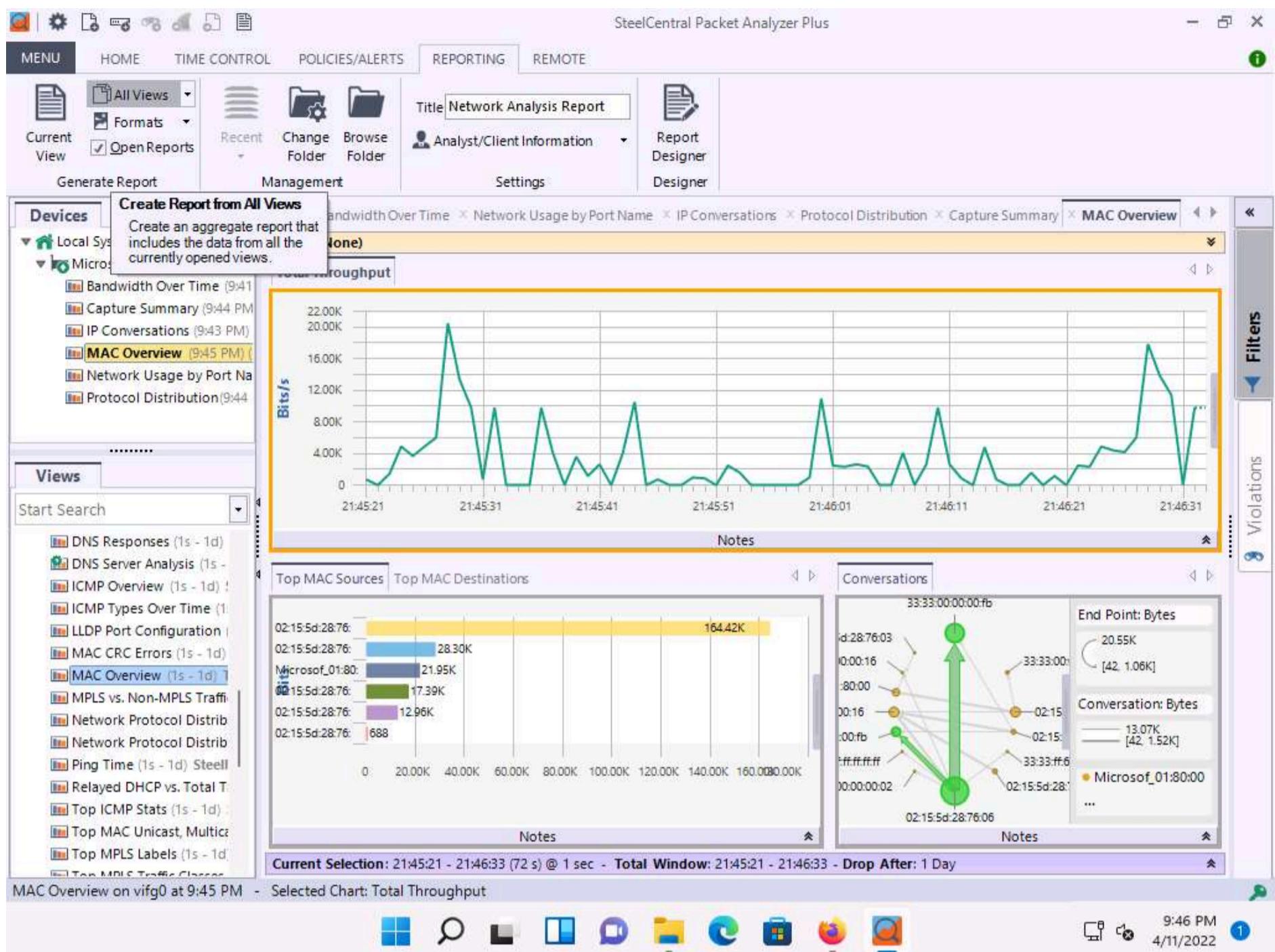
Conversation: Bytes

Current Selection: 21:45:21 - 21:45:32 (11 s) @ 1 sec - Total Window: 21:45:21 - 21:45:32 - Drop After: 1 Day

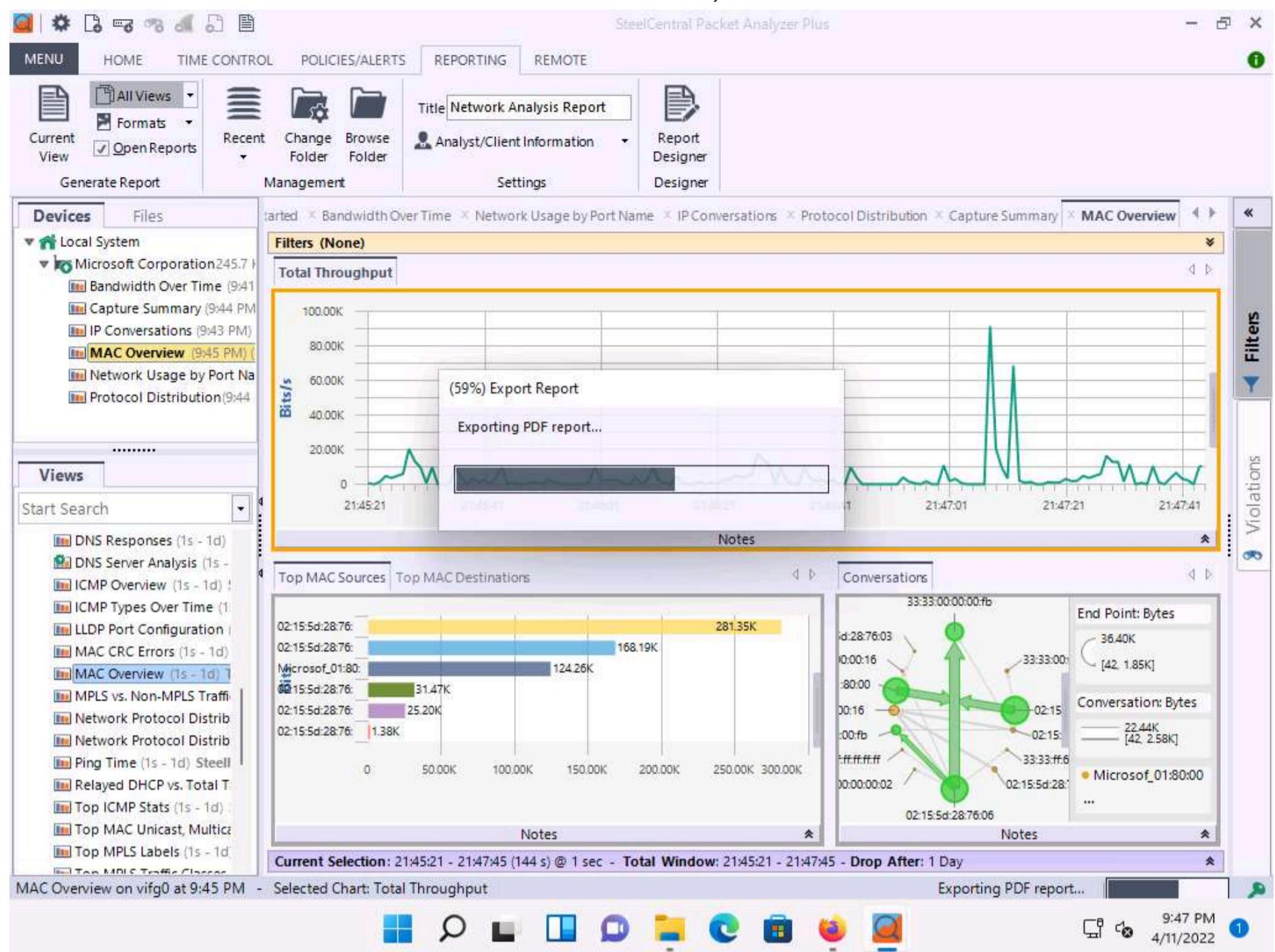
9:45 PM 4/11/2022

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.

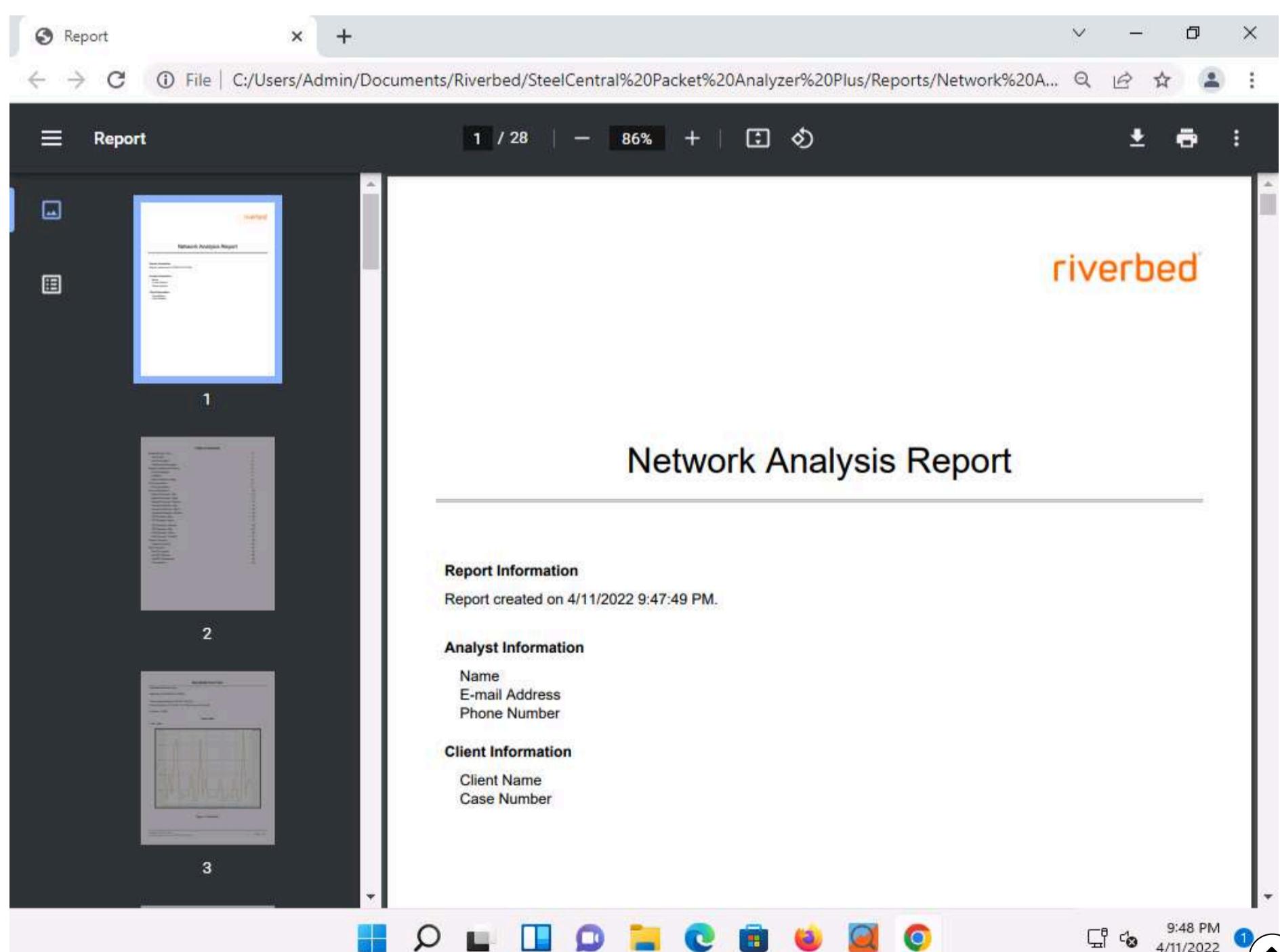


36. An **Export Report** pop-up appears, and the report starts exporting.



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**.

The screenshot shows the SteelCentral Packet Analyzer interface with the 'Report' tab selected. On the left, there is a navigation pane with three items labeled 1, 2, and 3. Item 2 is highlighted with a blue border. The main content area displays the 'Table of Contents' for the report, which includes sections like Bandwidth Over Time, Total Traffic, Total Throughput, and Network Usage by Port Name, along with their corresponding page numbers.

Section	Page Number
Bandwidth Over Time	3
Total Traffic	3
Total Throughput	4
Total Packet Throughput	5
Network Usage by Port Name	6
Total Throughput	6
Total Bits	7
Relative Network Usage	8
IP Conversations	9
IP Conversations	9
Protocol Distribution	10
Network Protocols - Bits	10
Network Protocols - Bytes	11
Network Protocols - Packets	12
Transport Protocols - Bits	13
Transport Protocols - Bytes	14
Transport Protocols - Packets	15
TCP Protocols - Bits	16
TCP Protocols - Bytes	17
TCP Protocols - Packets	18
UDP Protocols - Bits	19
UDP Protocols - Bytes	20
UDP Protocols - Packets	21
Capture Summary	22
Capture Summary	22
MAC Overview	25

The screenshot shows the SteelCentral Packet Analyzer interface with the 'Report' tab selected. On the left, there is a navigation pane with three items labeled 1, 2, and 3. Item 2 is highlighted with a blue border. The main content area displays the 'Bandwidth Over Time' section, which includes a sub-section for 'Total bandwidth over time' applied on 4/11/2022 9:41:33 PM. It also shows the total capture window (21:41:36 - 21:47:43) and current selection (21:41:36 - 21:47:36). A graph titled 'Total Traffic' shows traffic volume in bytes over time, with several sharp peaks reaching up to 25.00K bytes.

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.

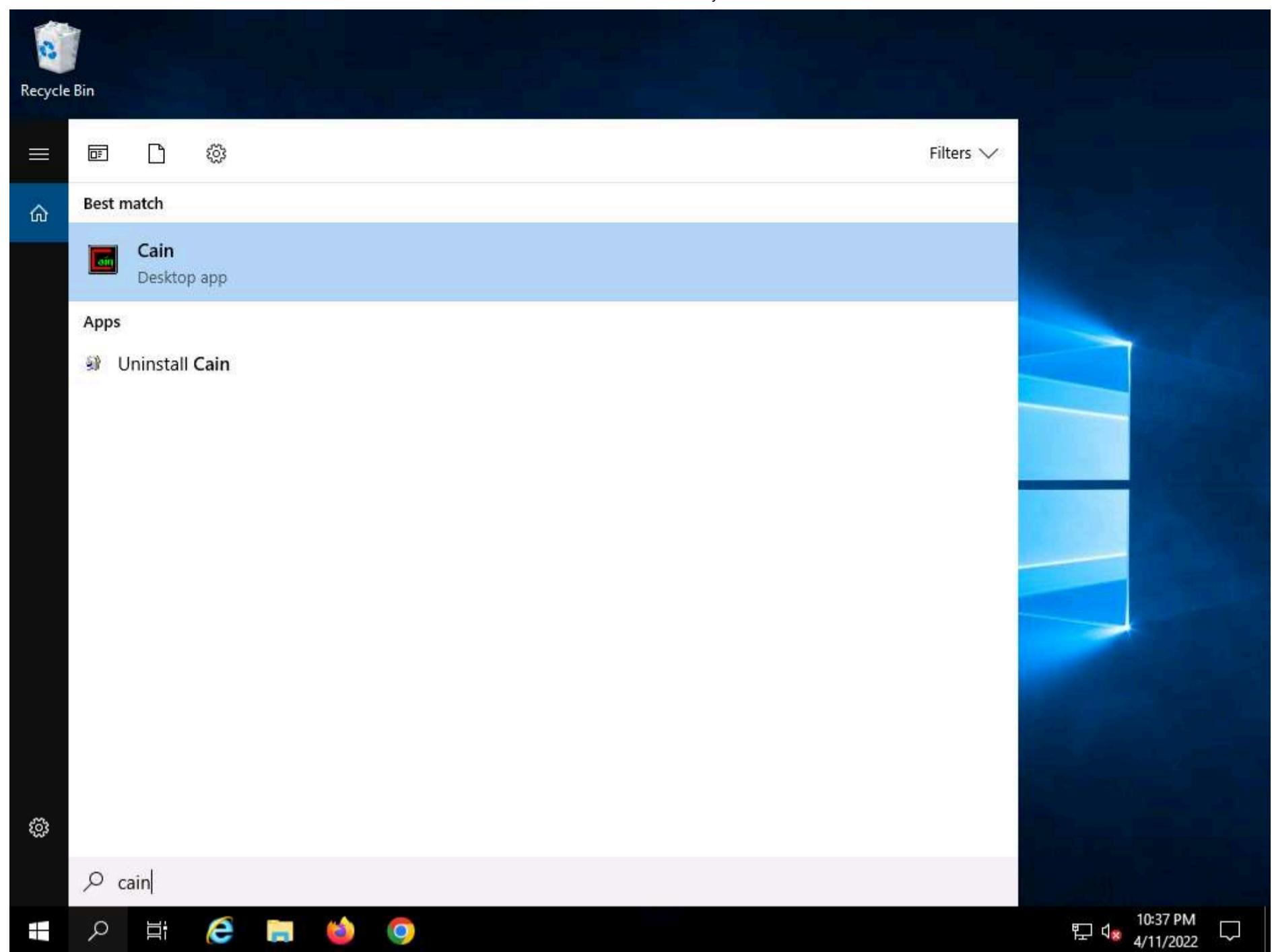
The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

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.

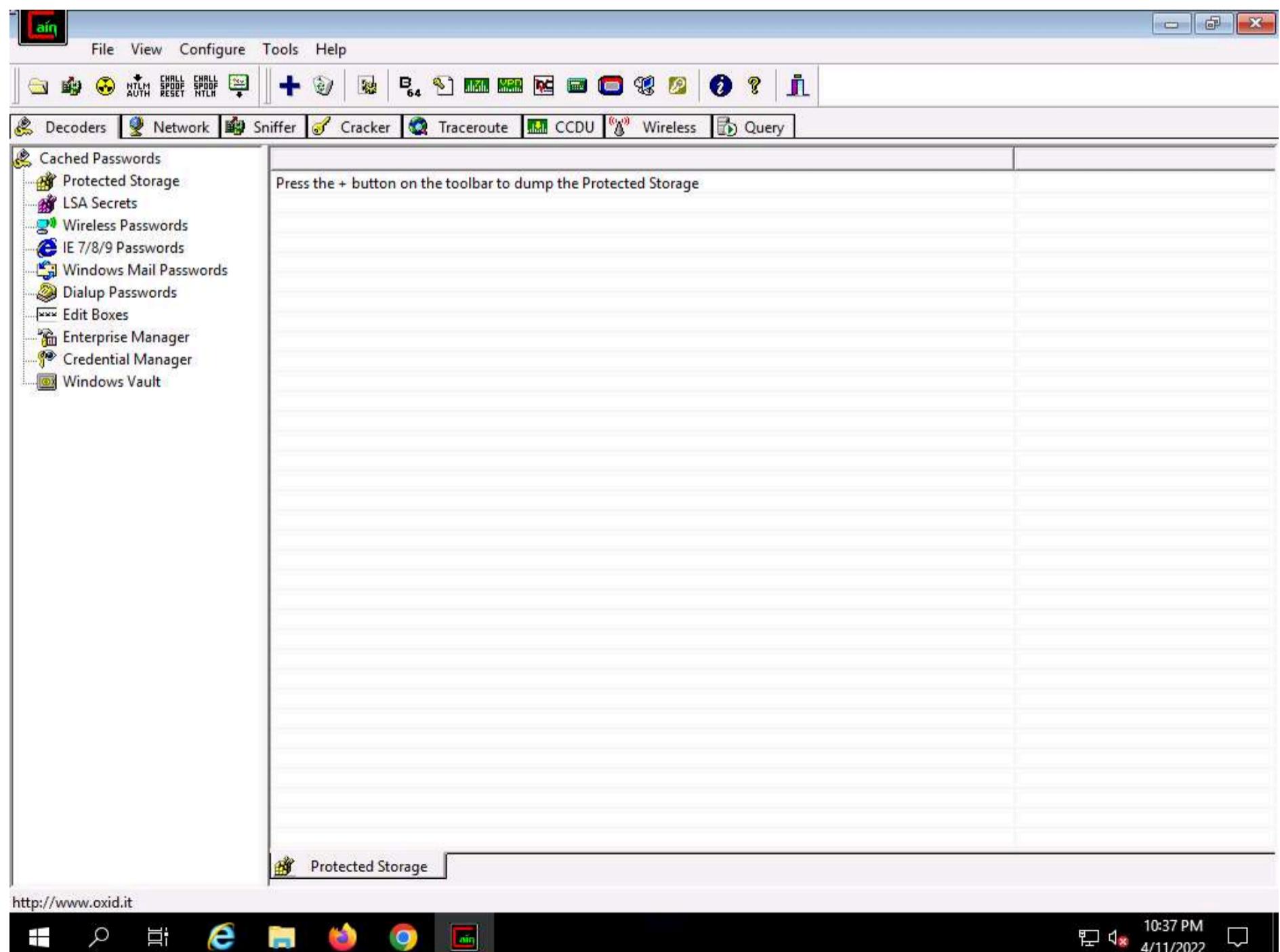
Note: In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 11** and **Parrot Security** machines. We will use the same machine (**Windows Server 2019**) to detect ARP poisoning and use the Windows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

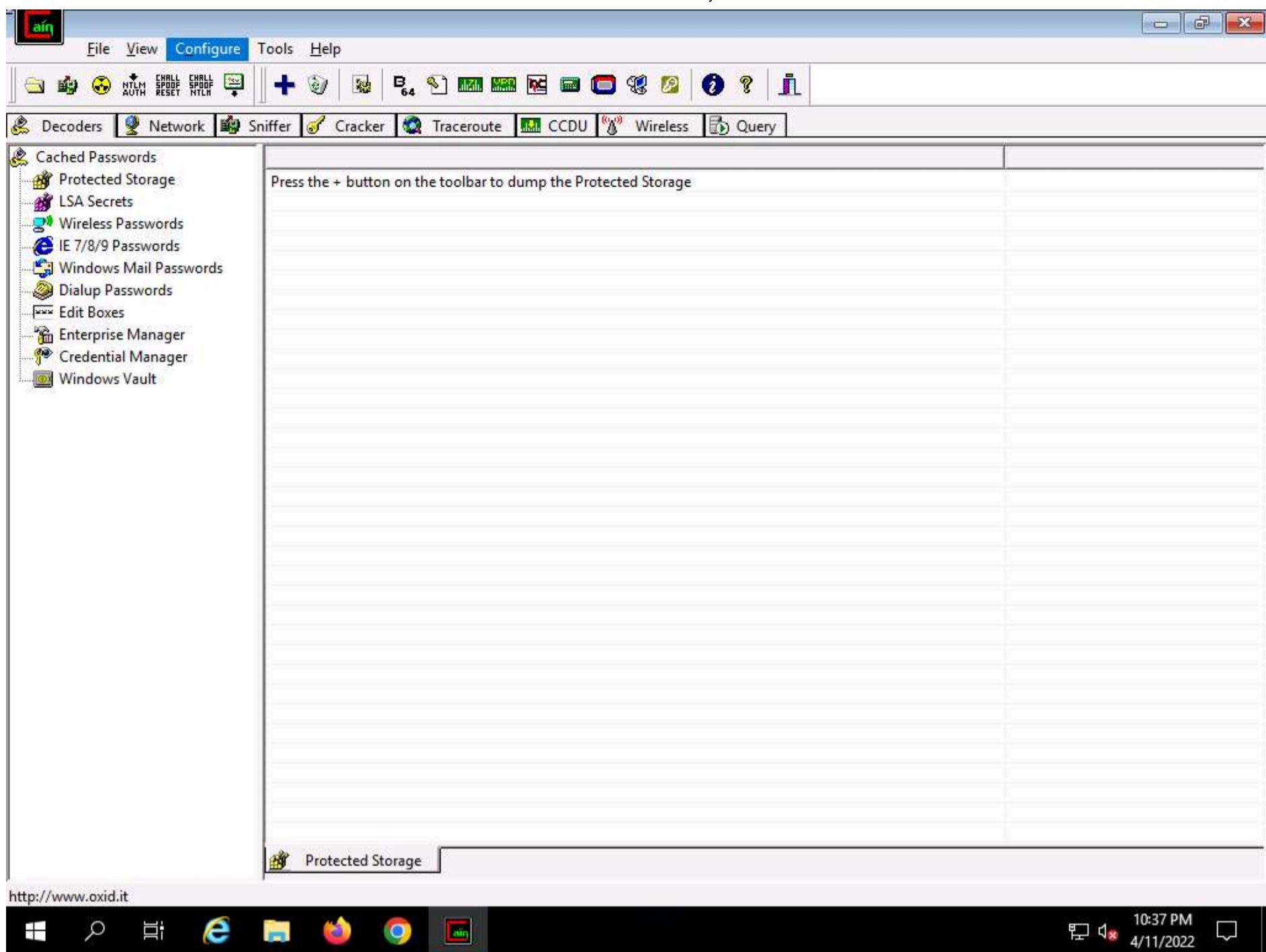




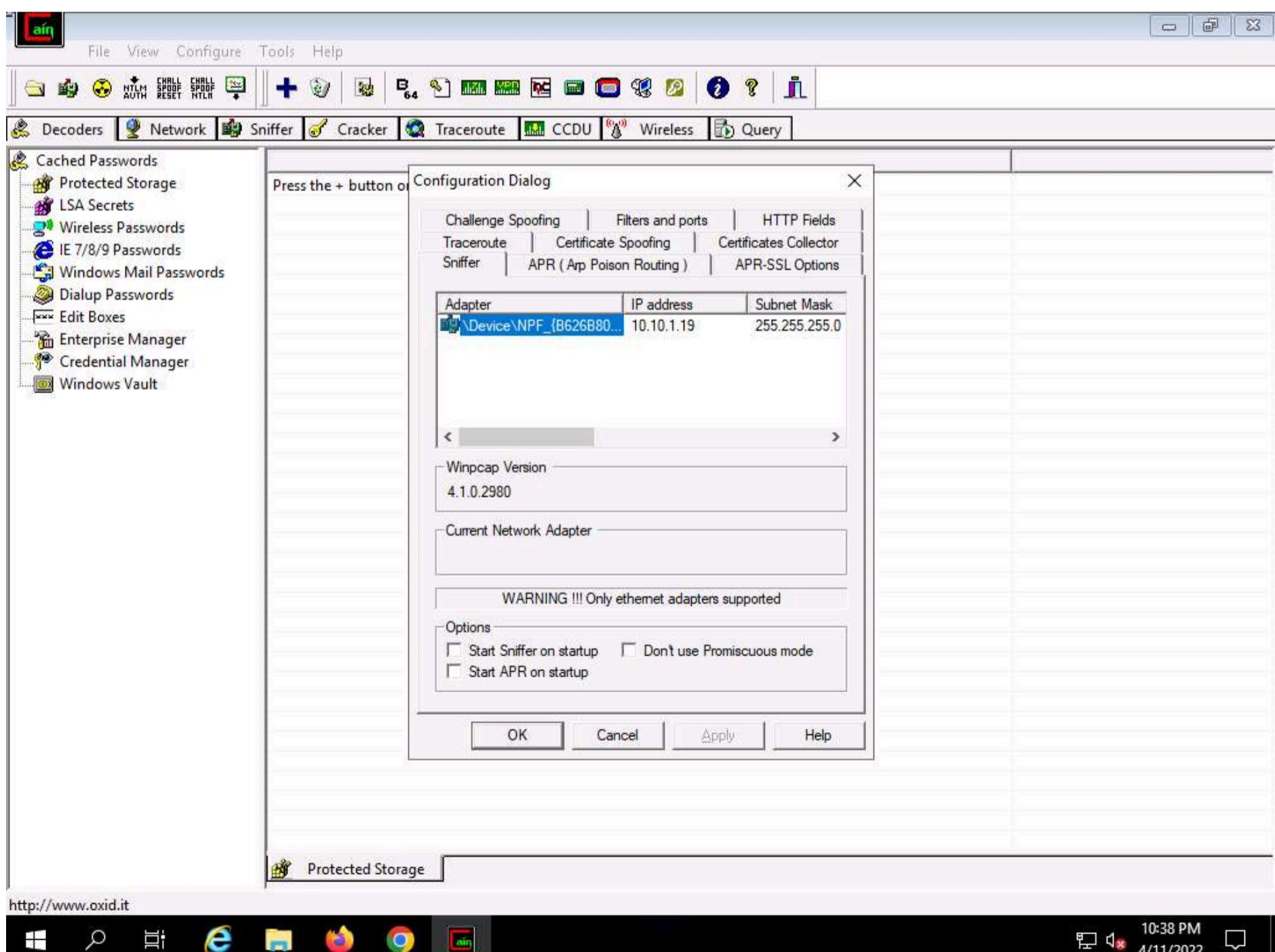
3. The **Cain & Abel** main window appears, as shown in the screenshot.



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

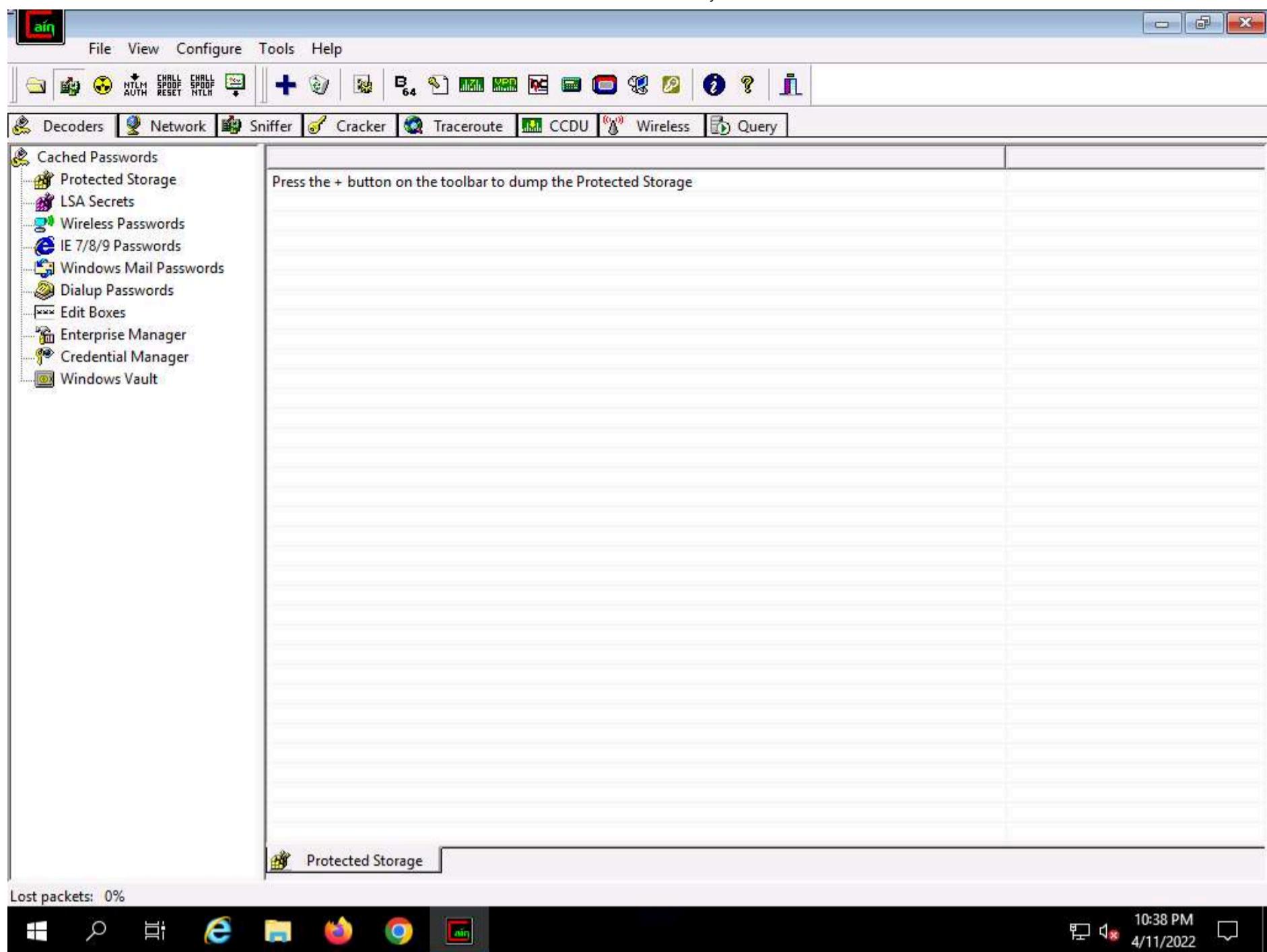


5. The Configuration Dialog window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.

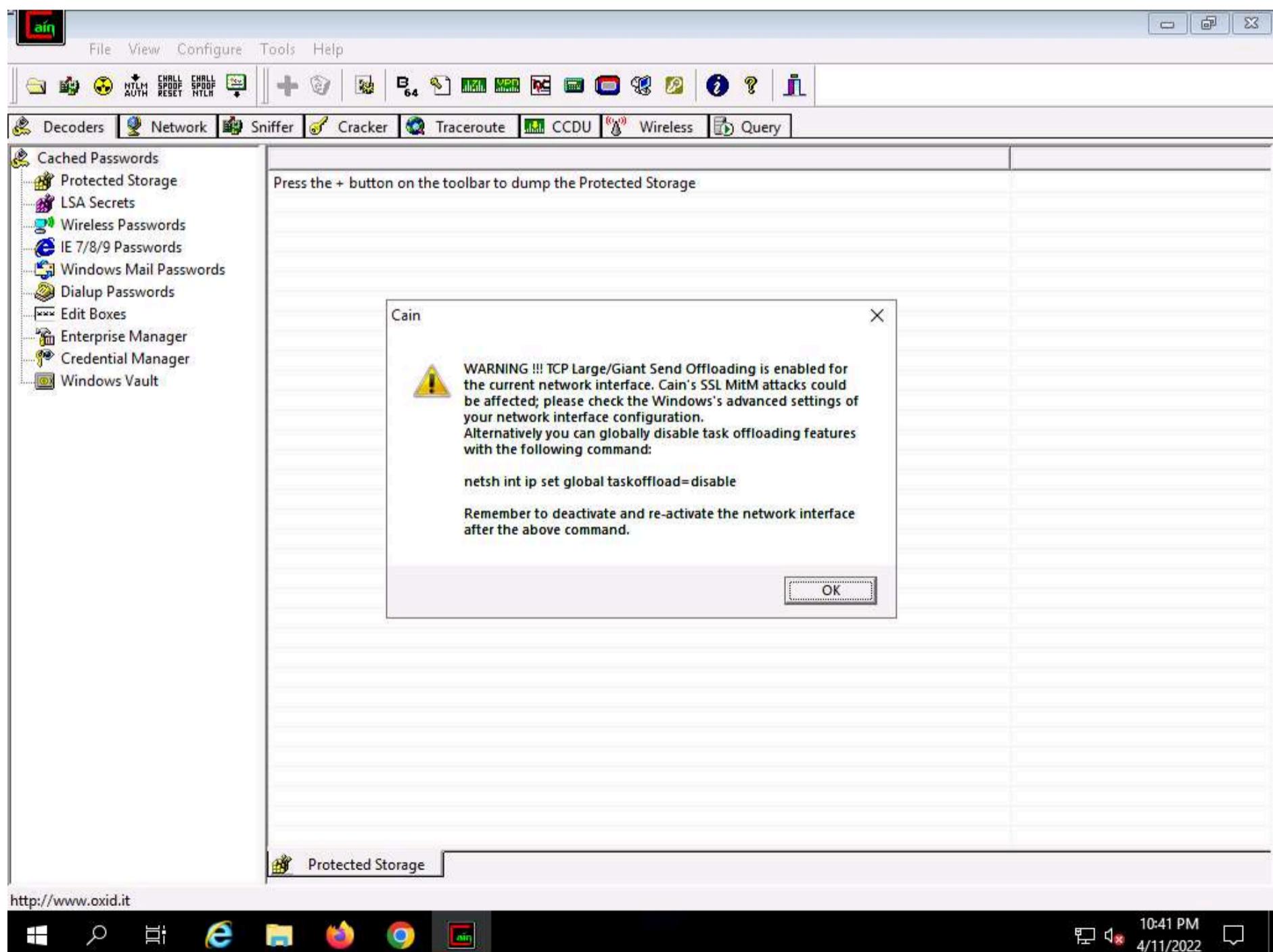


6. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.

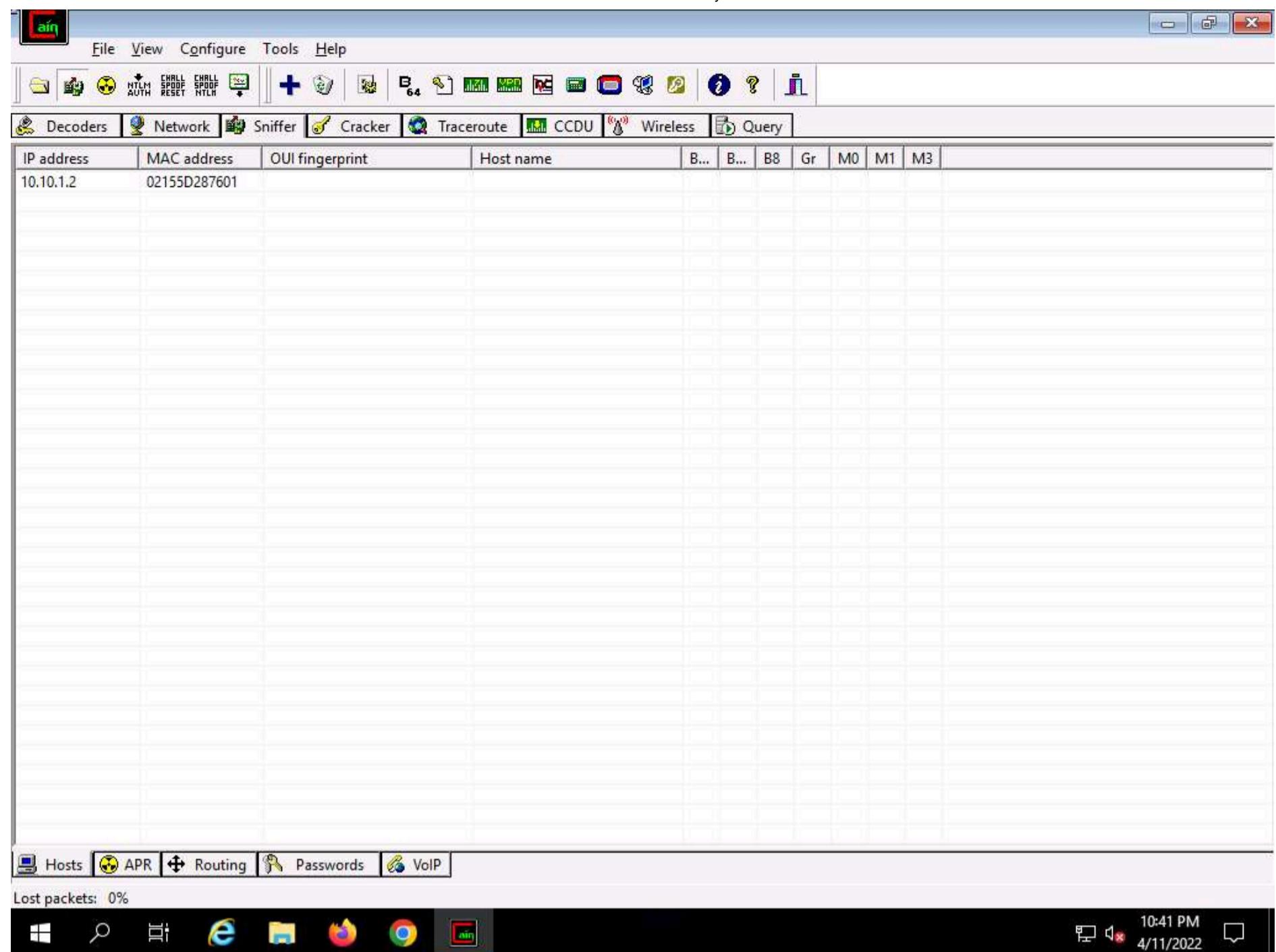




7. The Cain pop-up appears with a **Warning** message, click **OK**.

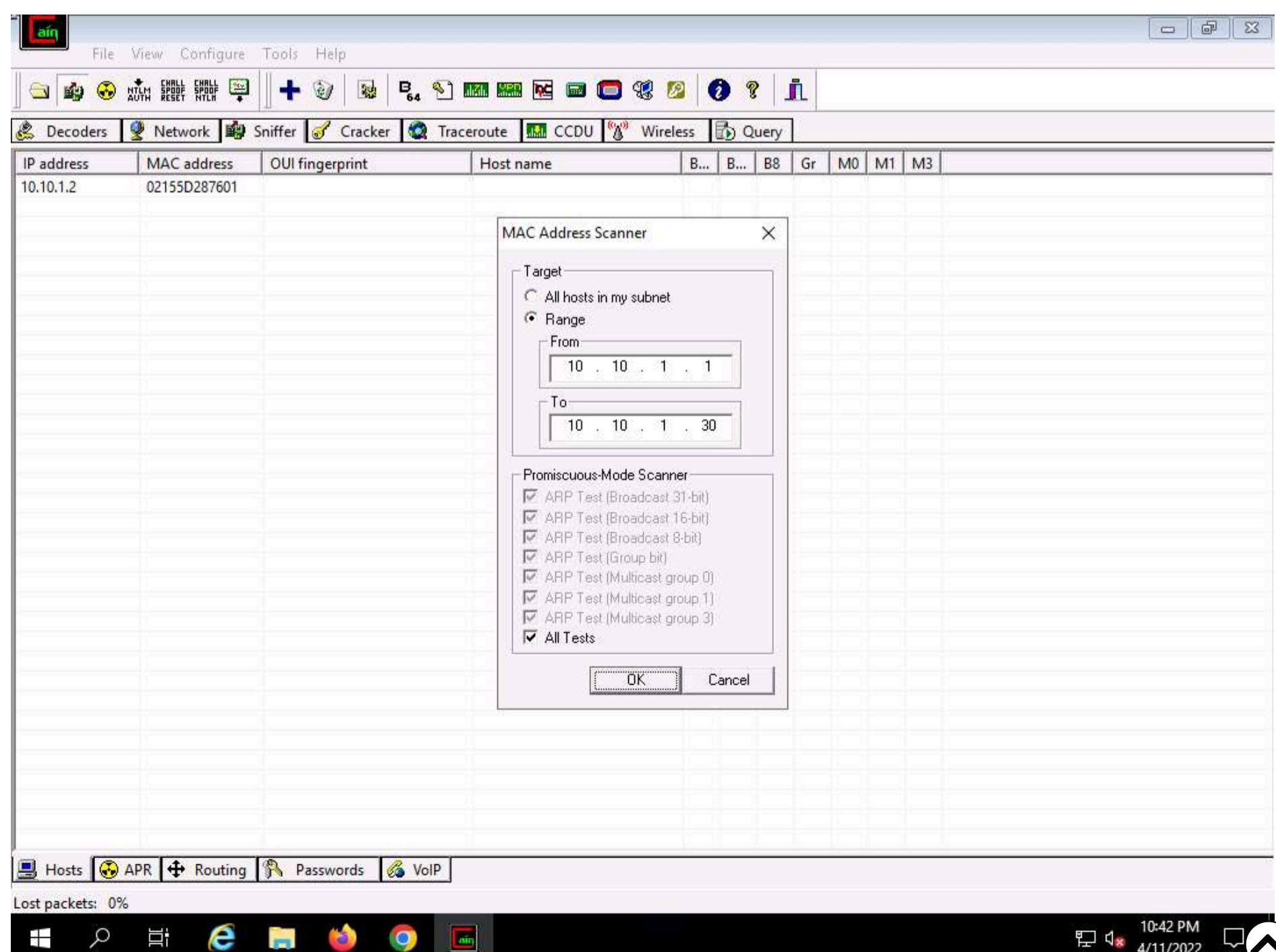


8. Now, click the **Sniffer** tab.



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.

The screenshot shows the Cain & Abel interface. At the top is a menu bar with File, View, Configure, Tools, and Help. Below the menu is a toolbar with various icons for NTLM auth, CHALL auth, CHALL spoof, B64, and others. The main window has tabs for Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, and Query. The Network tab is selected. A table displays the results of the scan:

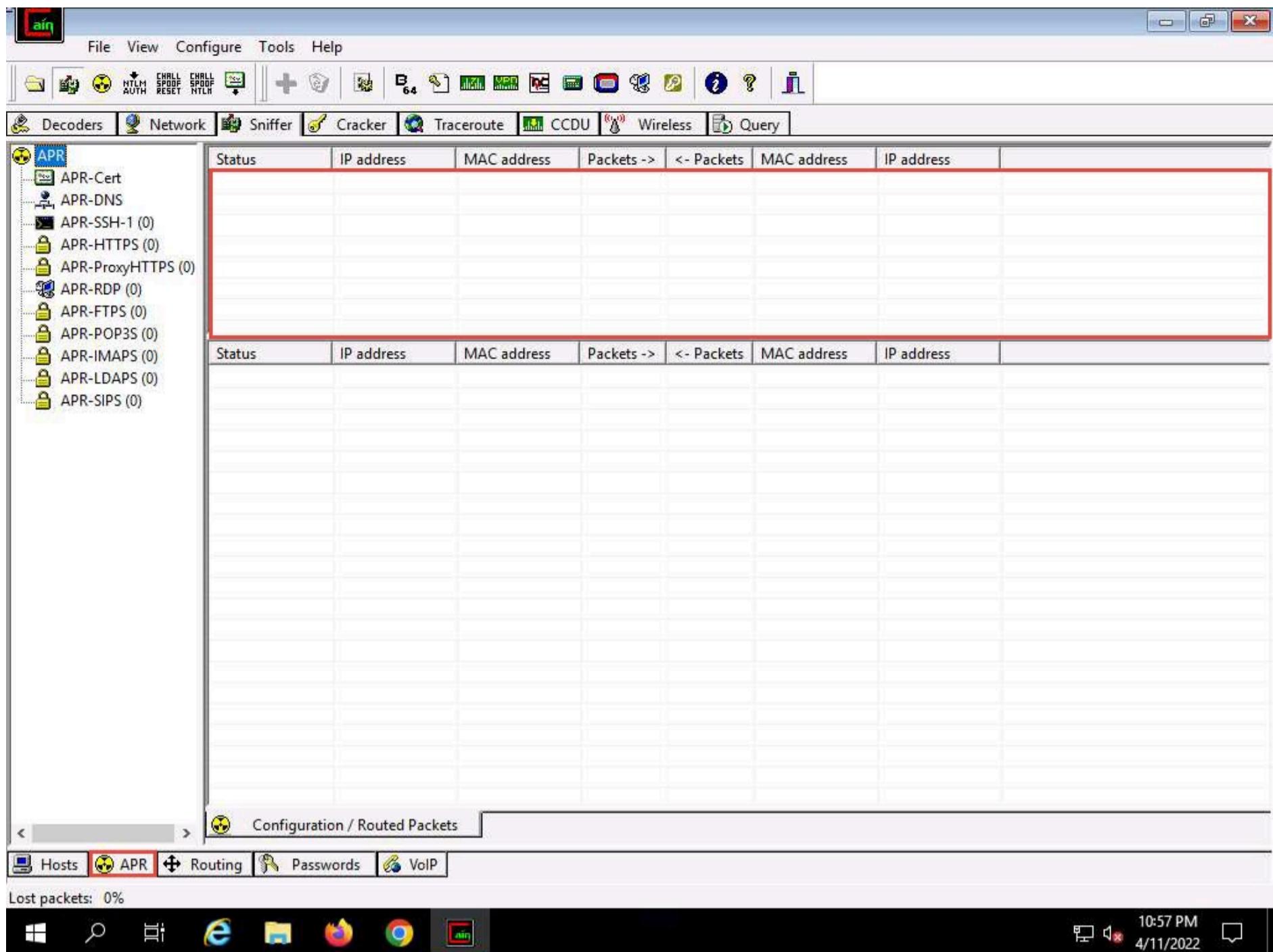
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.2	02155D287601			*	*	*	*	*	*	*
10.10.1.9	02155D287605			*	*	*	*	*	*	*
10.10.1.11	00155D018000	Microsoft Corporation		*	*	*	*	*	*	*
10.10.1.13	02155D287604			*	*	*	*	*	*	*
10.10.1.14	02155D287606			*	*	*	*			*
10.10.1.22	00155D018002	Microsoft Corporation		*	*	*	*	*	*	*

At the bottom of the interface, there are tabs for Hosts, APR, Routing, Passwords, and VoIP. The APR tab is currently selected. The status bar at the bottom shows "Lost packets: 0%" and the system clock "10:48 PM 4/11/2022".

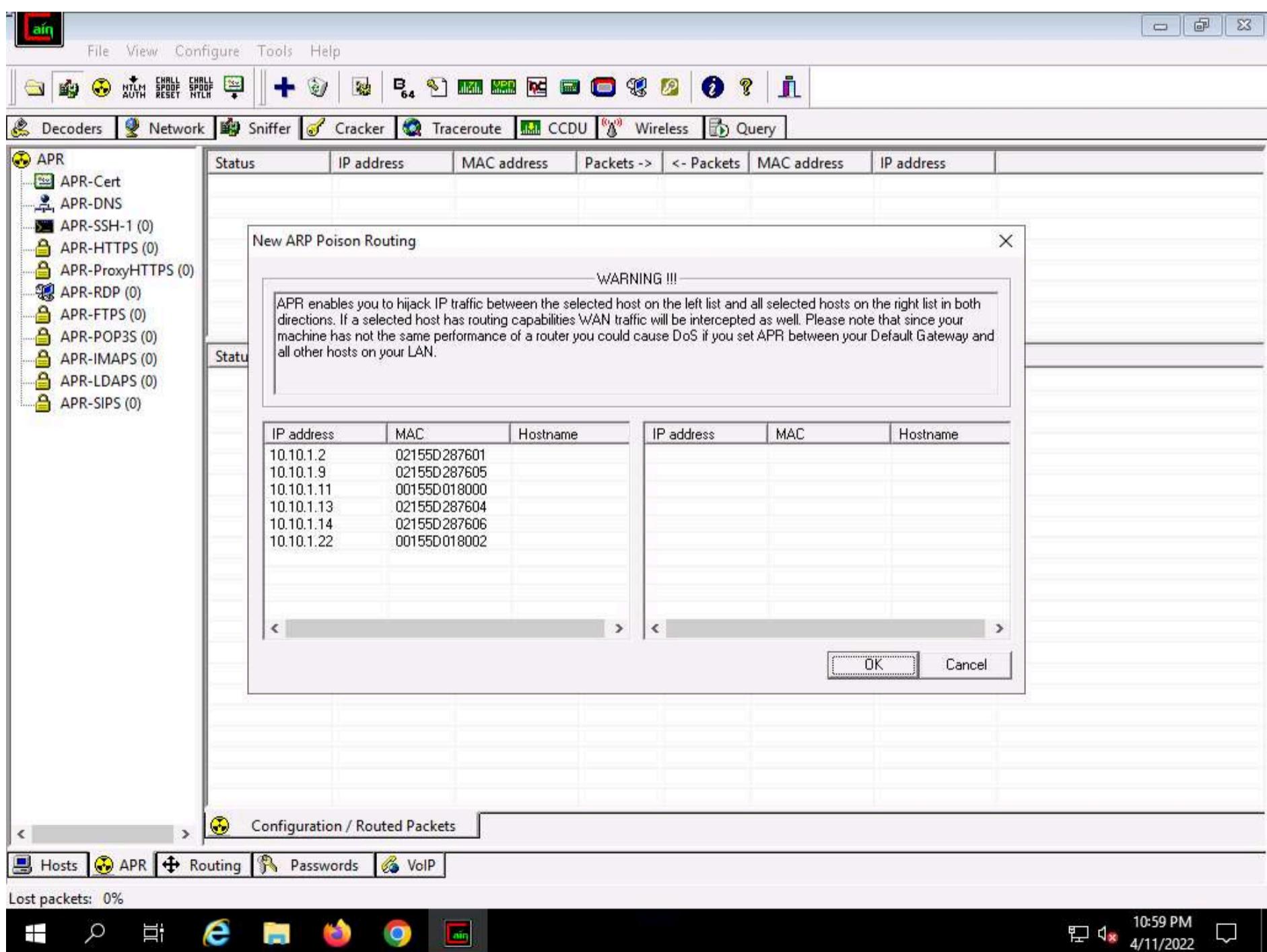
13. Now, click the **APR** tab at the bottom of the window.

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.

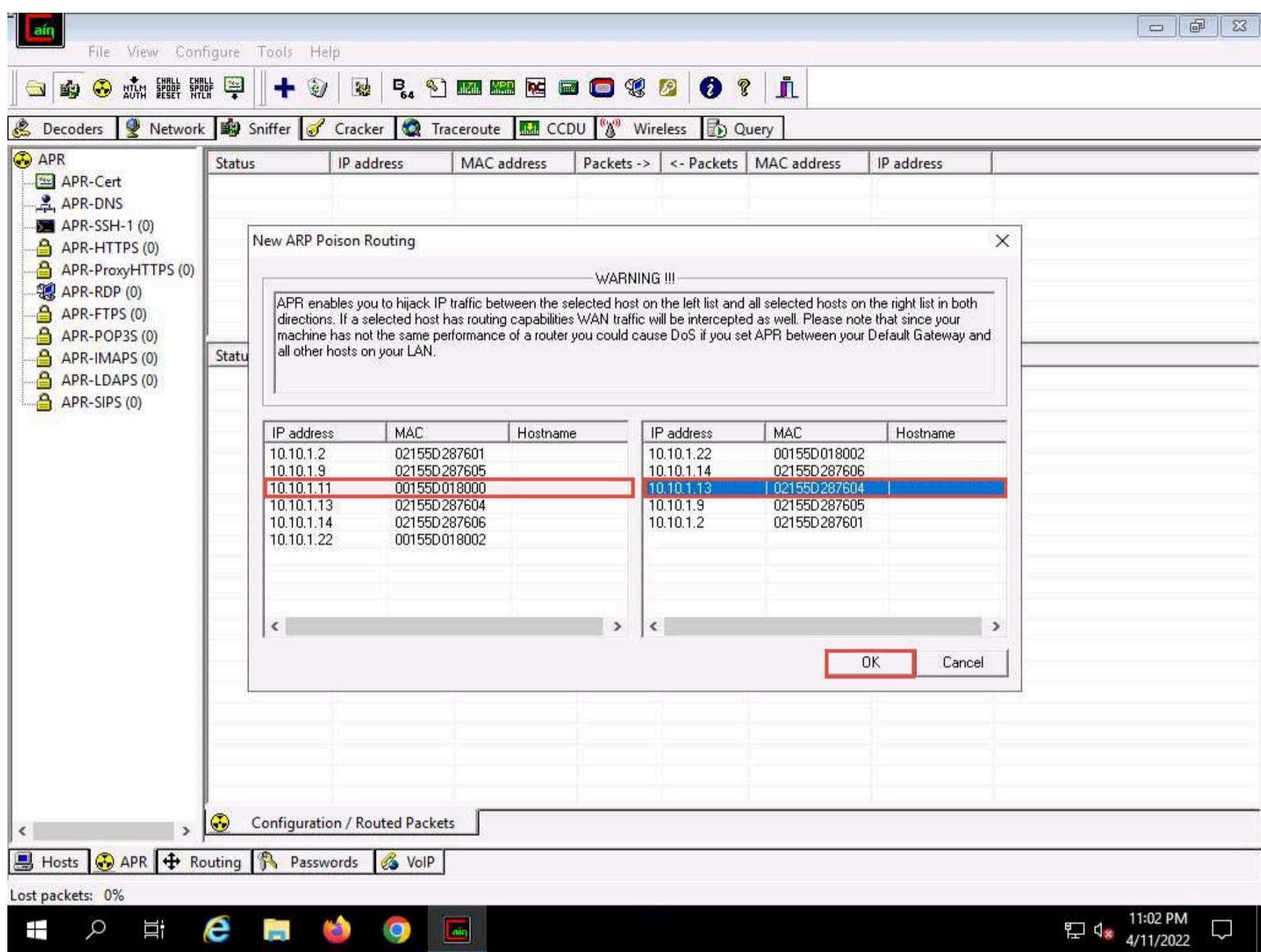




15. Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.



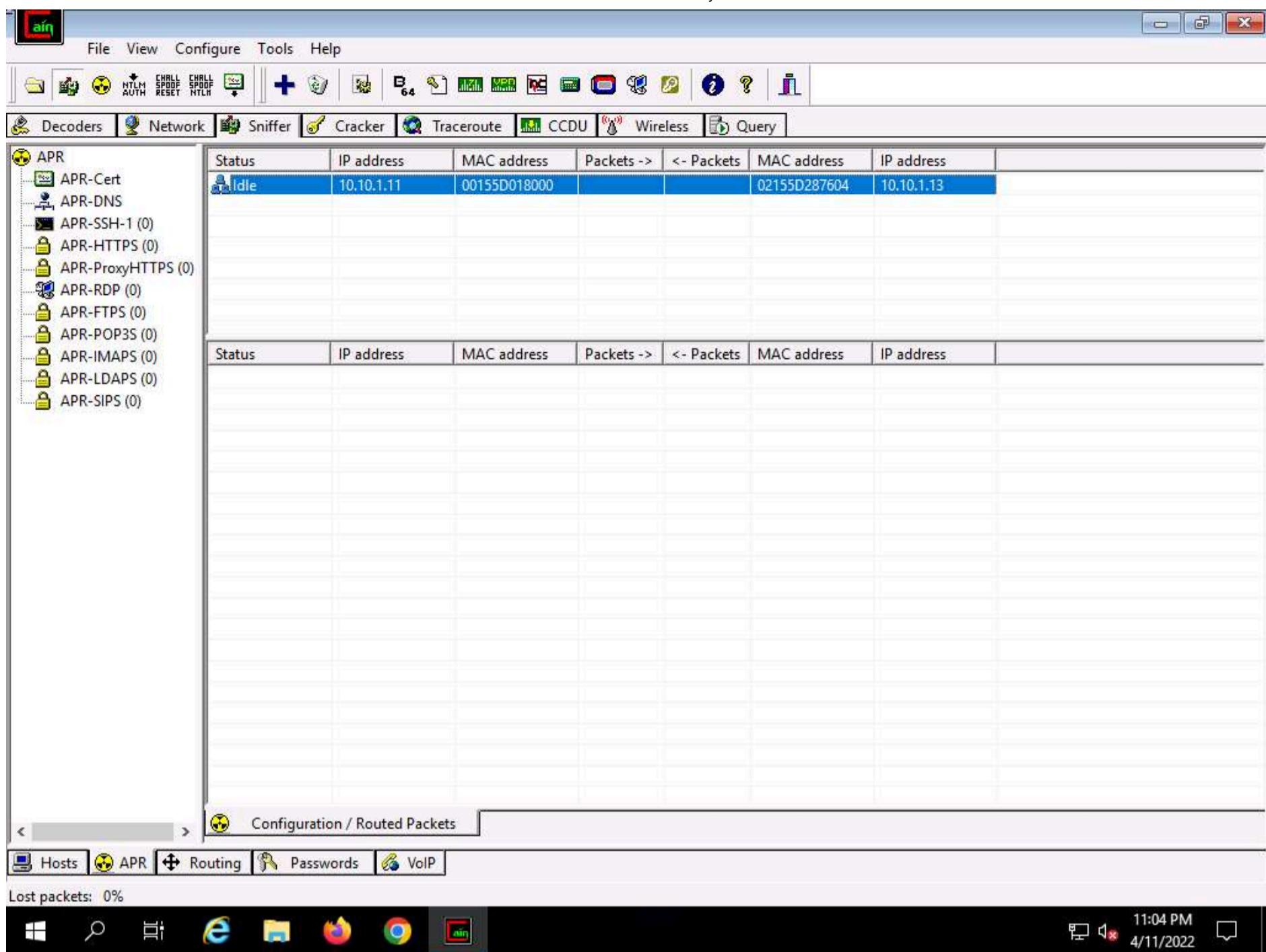
16. To monitor the traffic between two systems (here, **Windows 11** and **Parrot Security**), from the left-hand pane, click to select **10.10.1.11 (Windows 11)** and from the right-hand pane, click **10.10.1.13 (Parrot Security)**; click **OK**. By doing so, you are setting Cain to perform ARP poisoning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



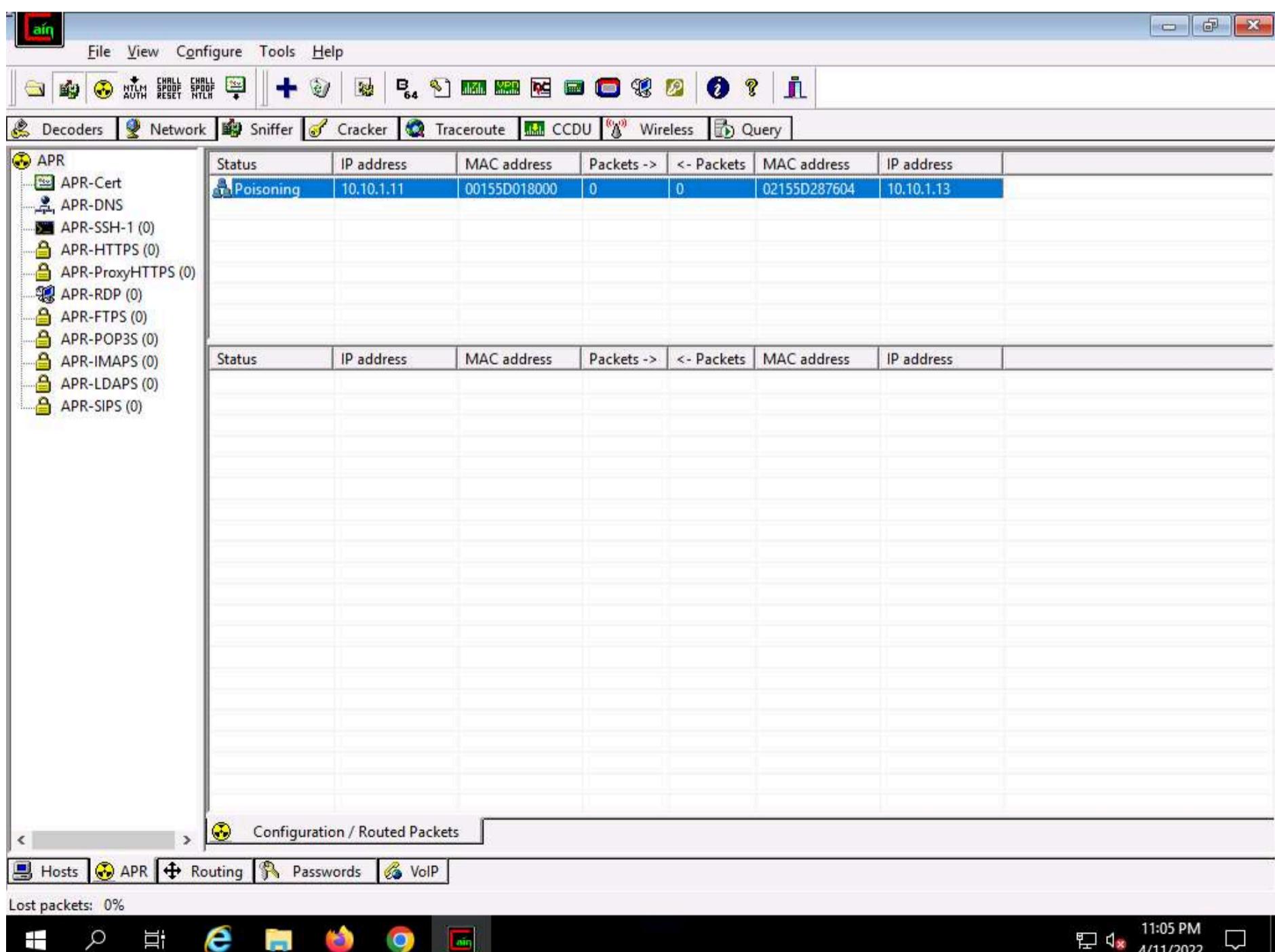
17. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.

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.

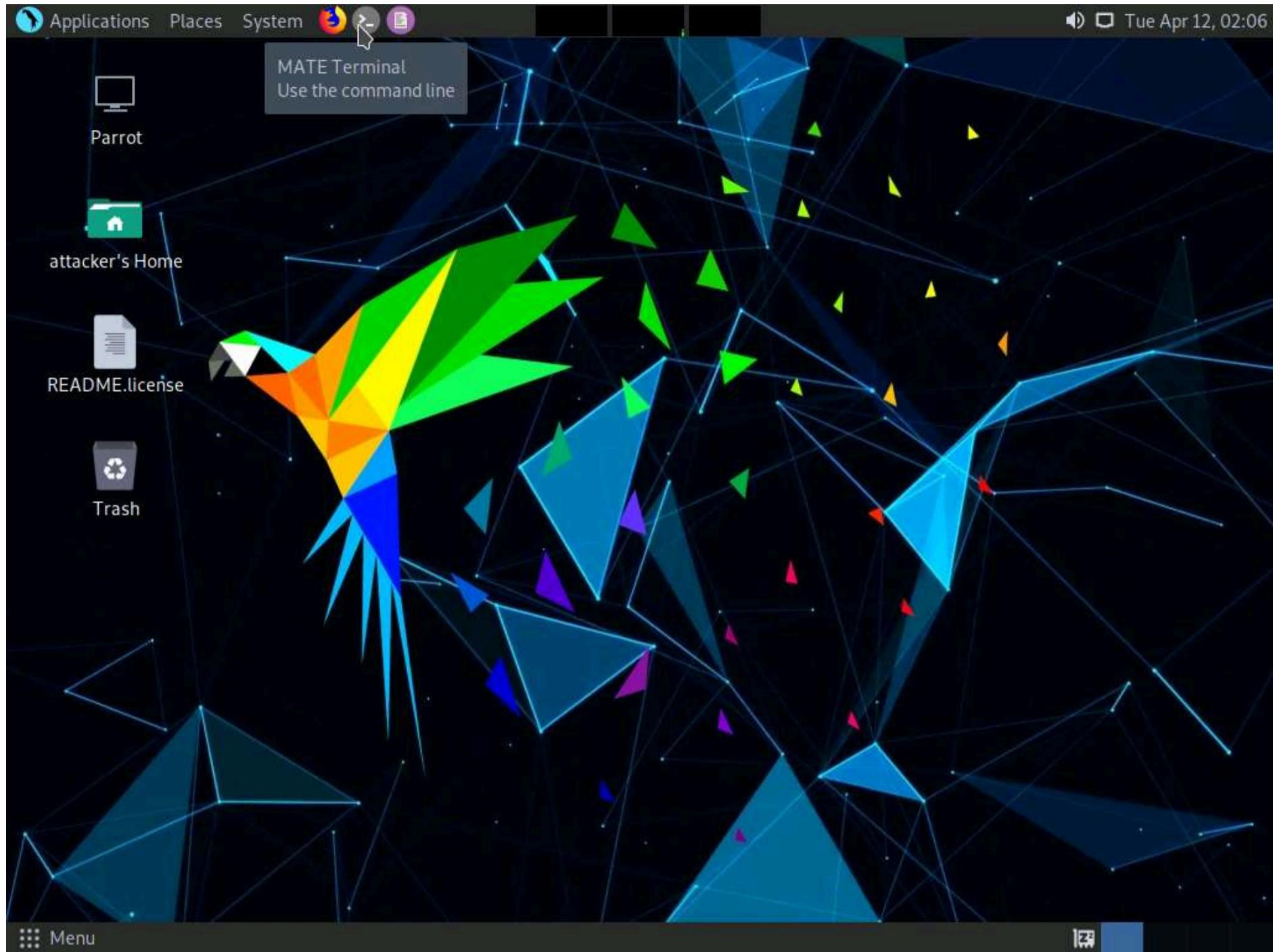


20. Cain & Abel intercepts the traffic traversing between these two machines.

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.



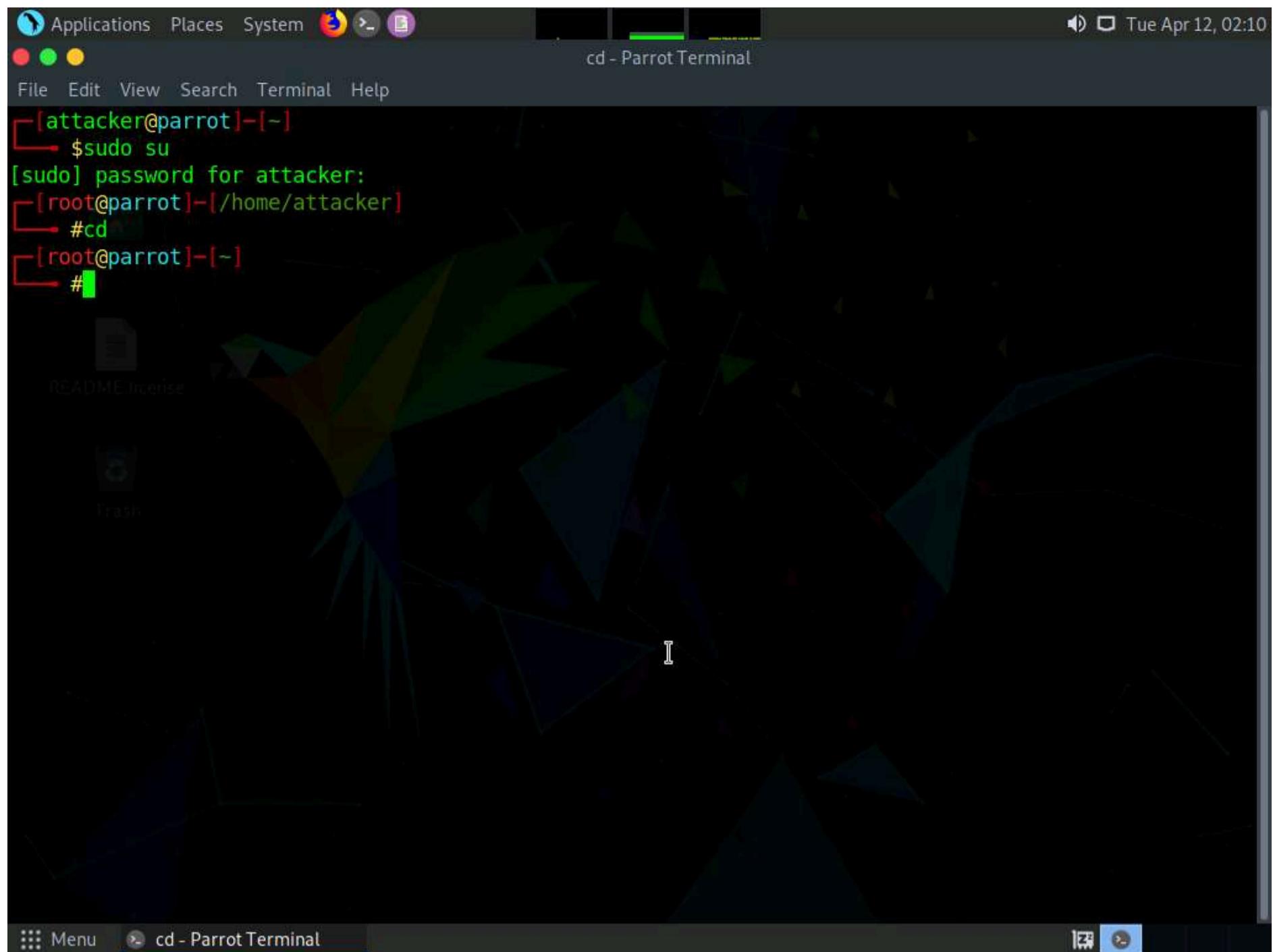
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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.

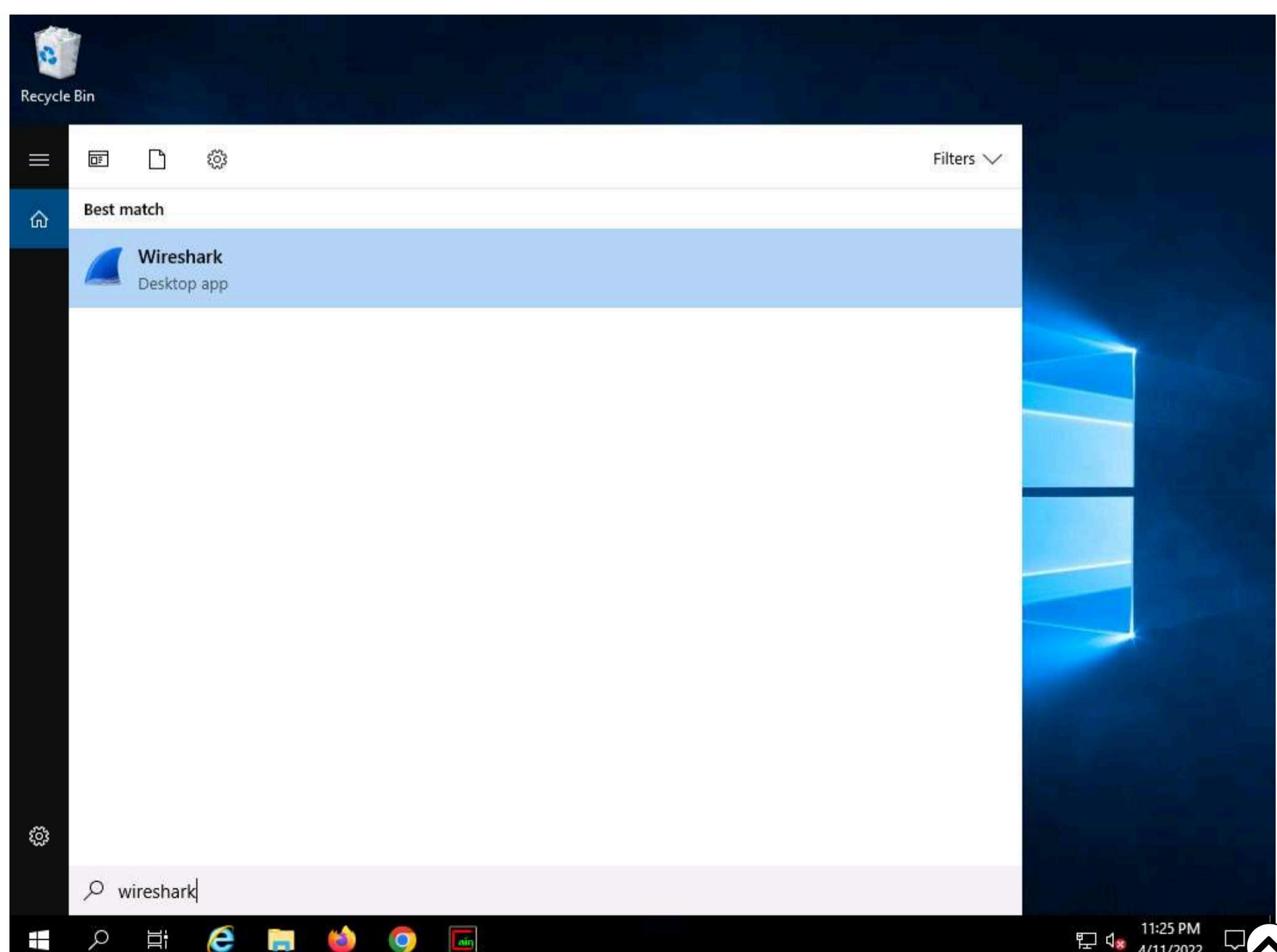


The screenshot shows a terminal window titled "hping3 10.10.1.11 -c 100000 - Parrot Terminal". The terminal output shows the command being run and the resulting traffic. The traffic consists of 16 ICMP echo requests (RA) sent to the target IP address 10.10.1.11 over interface eth0. Each packet has a TTL of 128, sequence number 0, and flags set to RA.

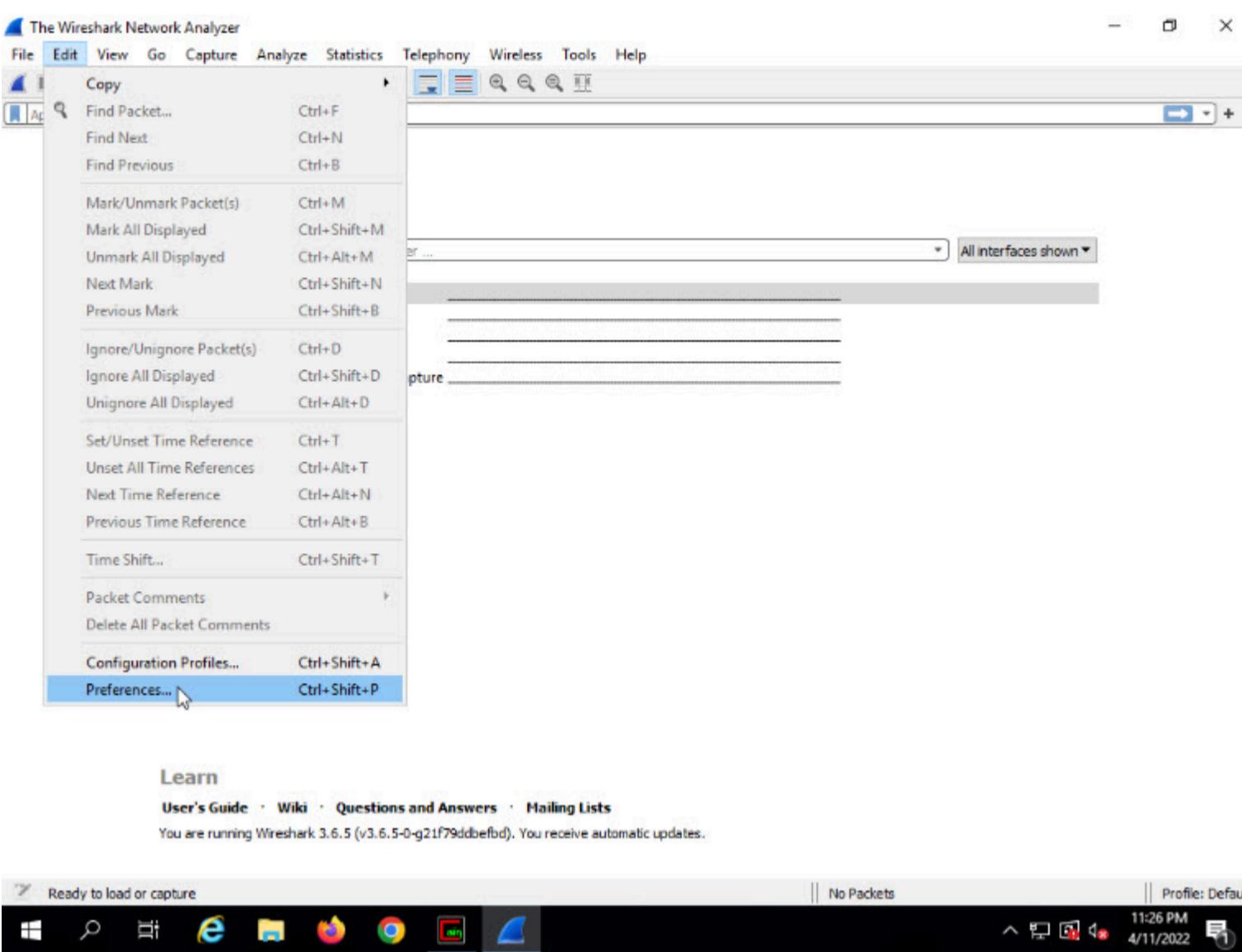
```
[attacker@parrot]~[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#hping3 10.10.1.11 -c 100000
HPING 10.10.1.11 (eth0 10.10.1.11): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=10.10.1.11 ttl=128 DF id=1 sport=0 flags=RA seq=0 win=0 rtt=3.7 ms
len=40 ip=10.10.1.11 ttl=128 DF id=2 sport=0 flags=RA seq=1 win=0 rtt=3.6 ms
len=40 ip=10.10.1.11 ttl=128 DF id=3 sport=0 flags=RA seq=2 win=0 rtt=3.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=4 sport=0 flags=RA seq=3 win=0 rtt=7.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=5 sport=0 flags=RA seq=4 win=0 rtt=3.0 ms
len=40 ip=10.10.1.11 ttl=128 DF id=6 sport=0 flags=RA seq=5 win=0 rtt=6.8 ms
len=40 ip=10.10.1.11 ttl=128 DF id=7 sport=0 flags=RA seq=6 win=0 rtt=6.6 ms
len=40 ip=10.10.1.11 ttl=128 DF id=8 sport=0 flags=RA seq=7 win=0 rtt=2.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=9 sport=0 flags=RA seq=8 win=0 rtt=2.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=10 sport=0 flags=RA seq=9 win=0 rtt=10.0 ms
len=40 ip=10.10.1.11 ttl=128 DF id=11 sport=0 flags=RA seq=10 win=0 rtt=9.8 ms
len=40 ip=10.10.1.11 ttl=128 DF id=12 sport=0 flags=RA seq=11 win=0 rtt=9.5 ms
len=40 ip=10.10.1.11 ttl=128 DF id=13 sport=0 flags=RA seq=12 win=0 rtt=9.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=14 sport=0 flags=RA seq=13 win=0 rtt=9.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=15 sport=0 flags=RA seq=14 win=0 rtt=8.9 ms
len=40 ip=10.10.1.11 ttl=128 DF id=16 sport=0 flags=RA seq=15 win=0 rtt=8.6 ms
```

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

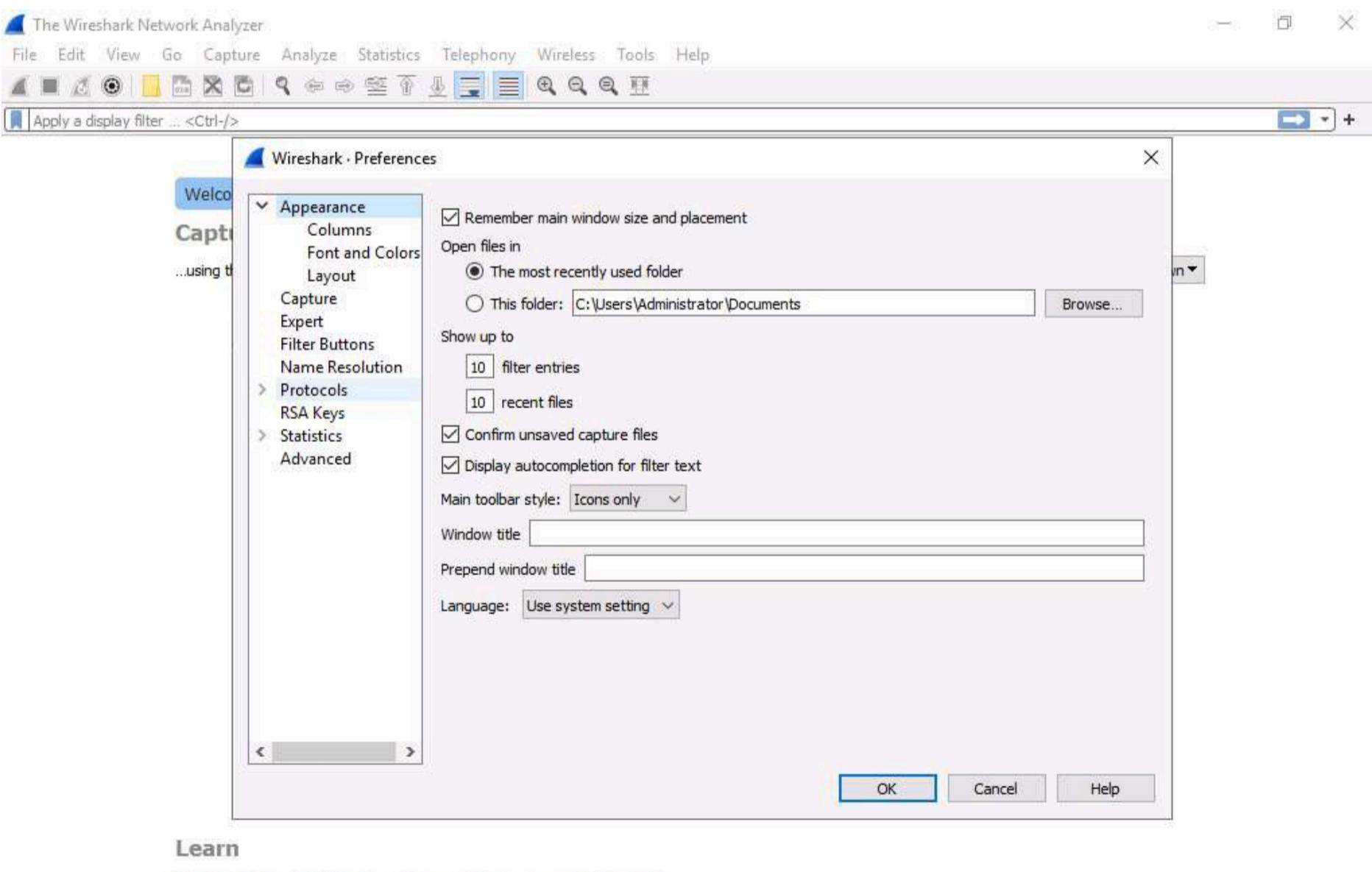
30. Click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.



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.



### Learn

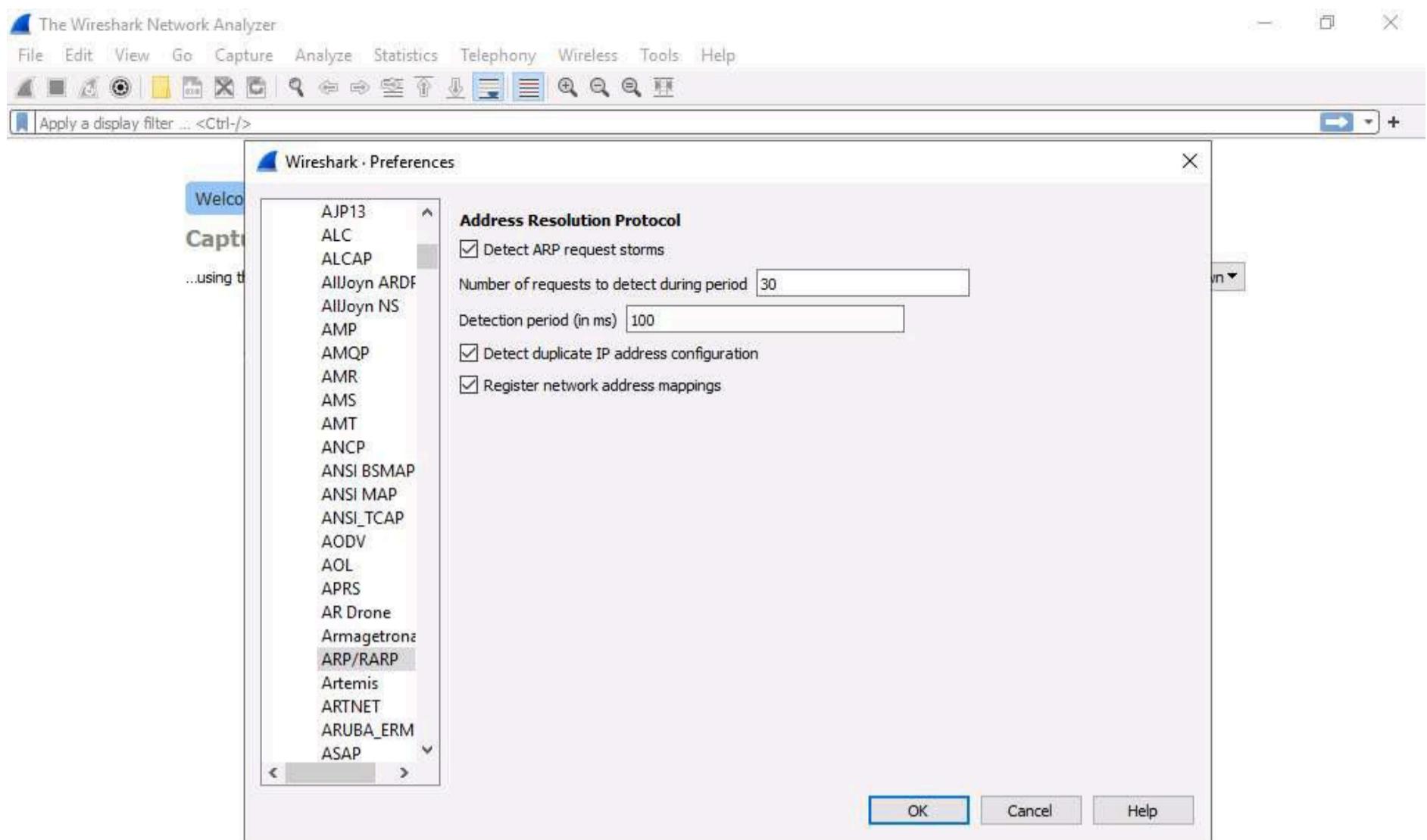
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.



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**.



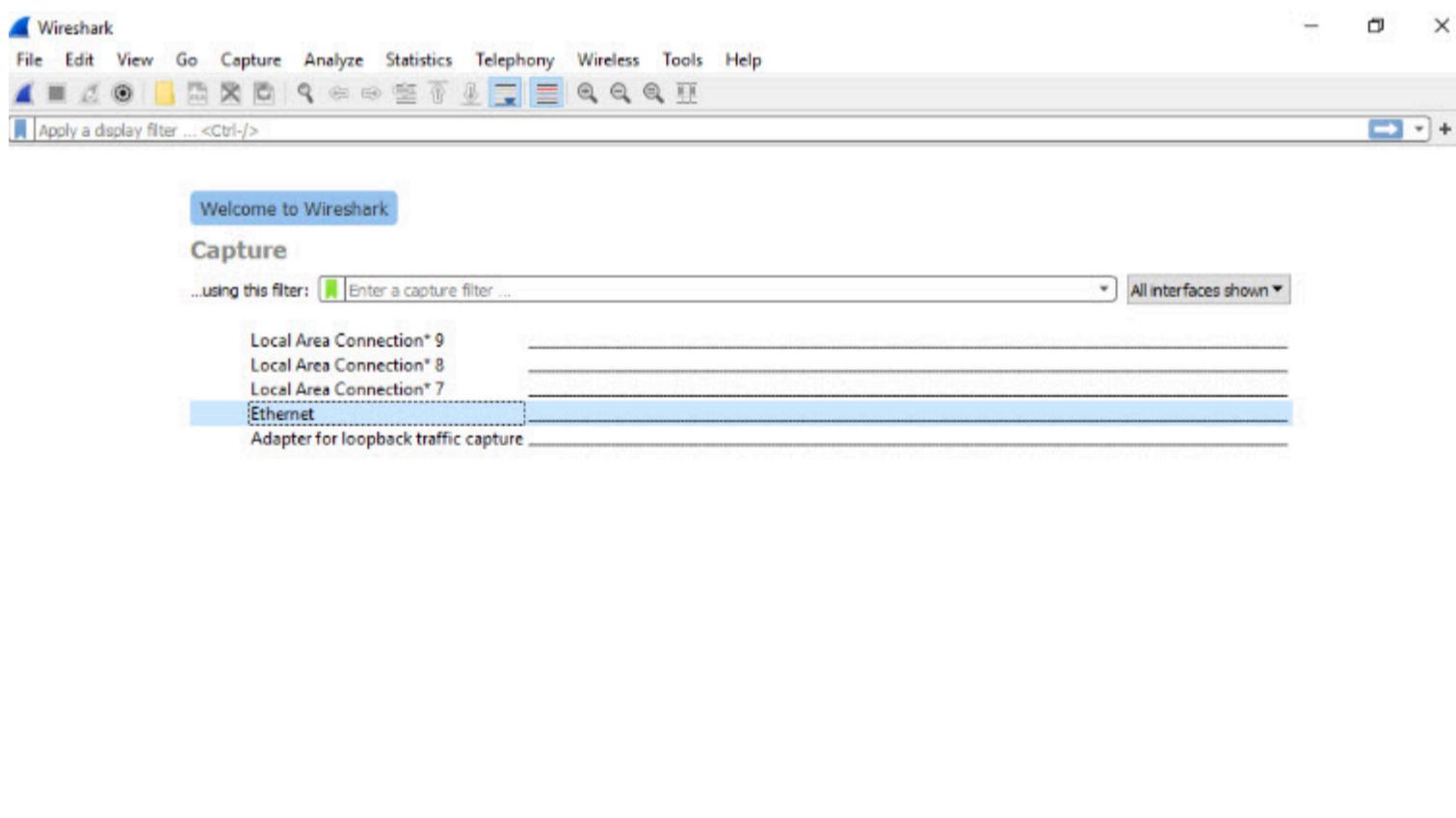
### Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.



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



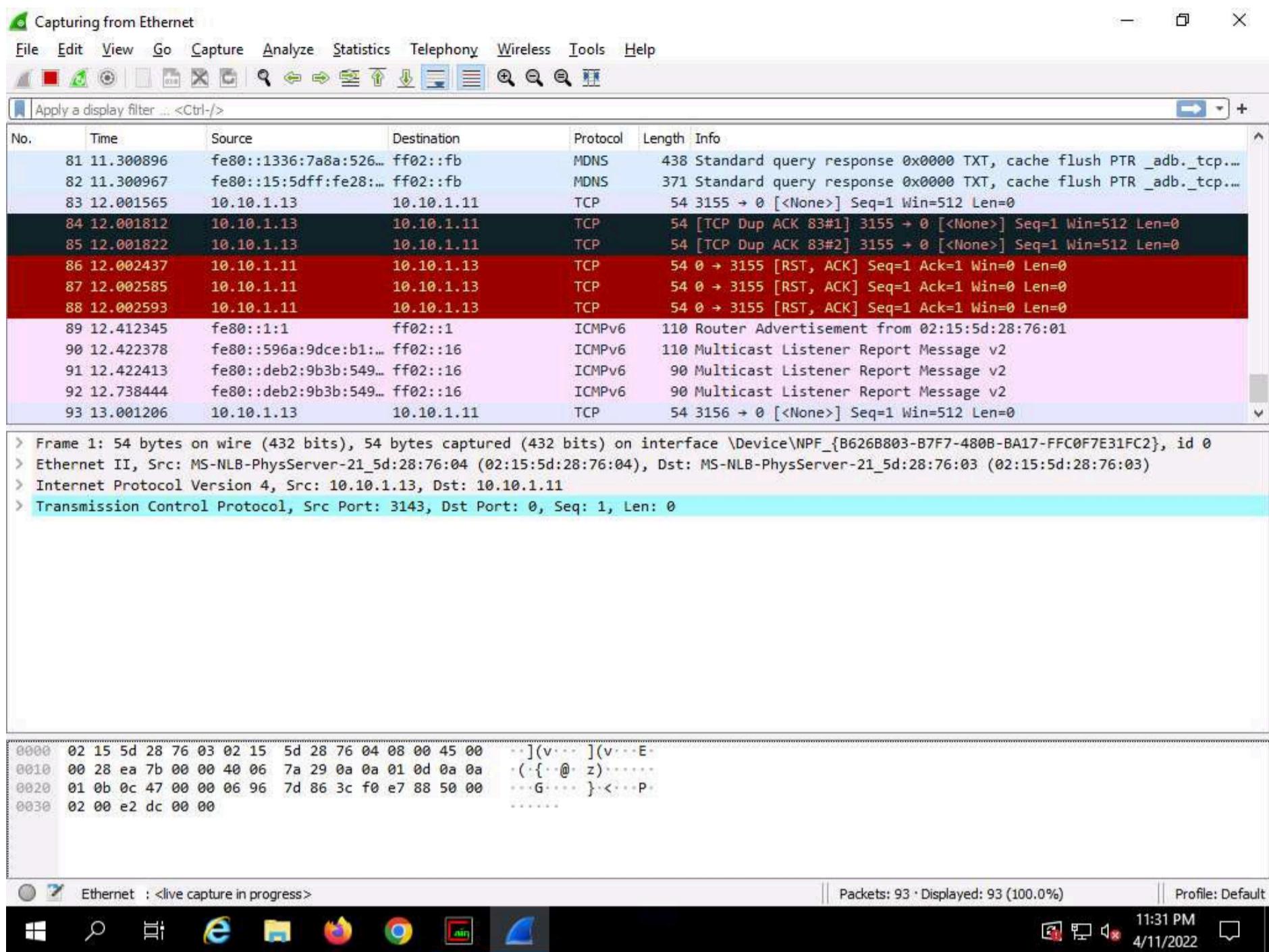
### Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

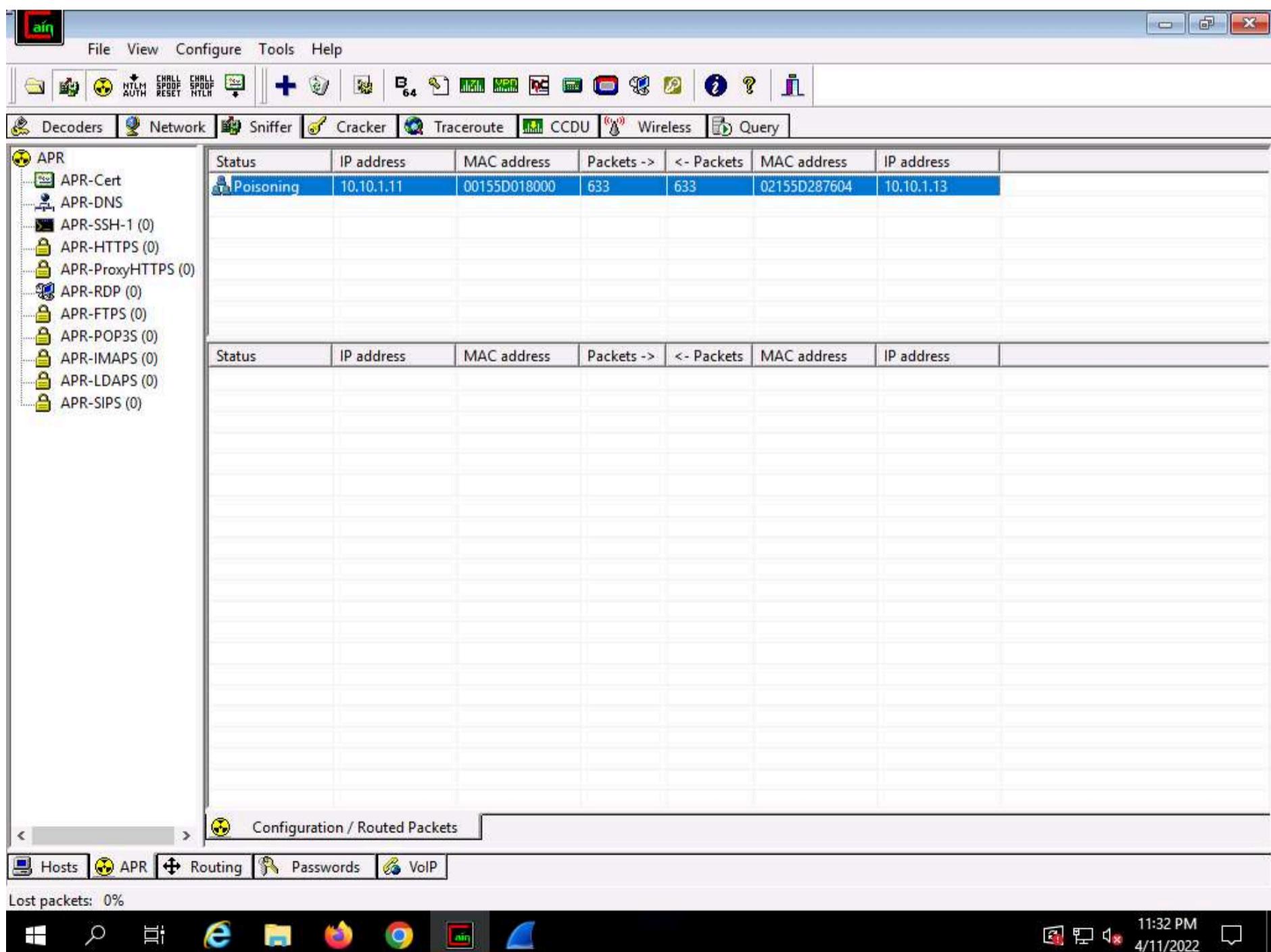
You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.



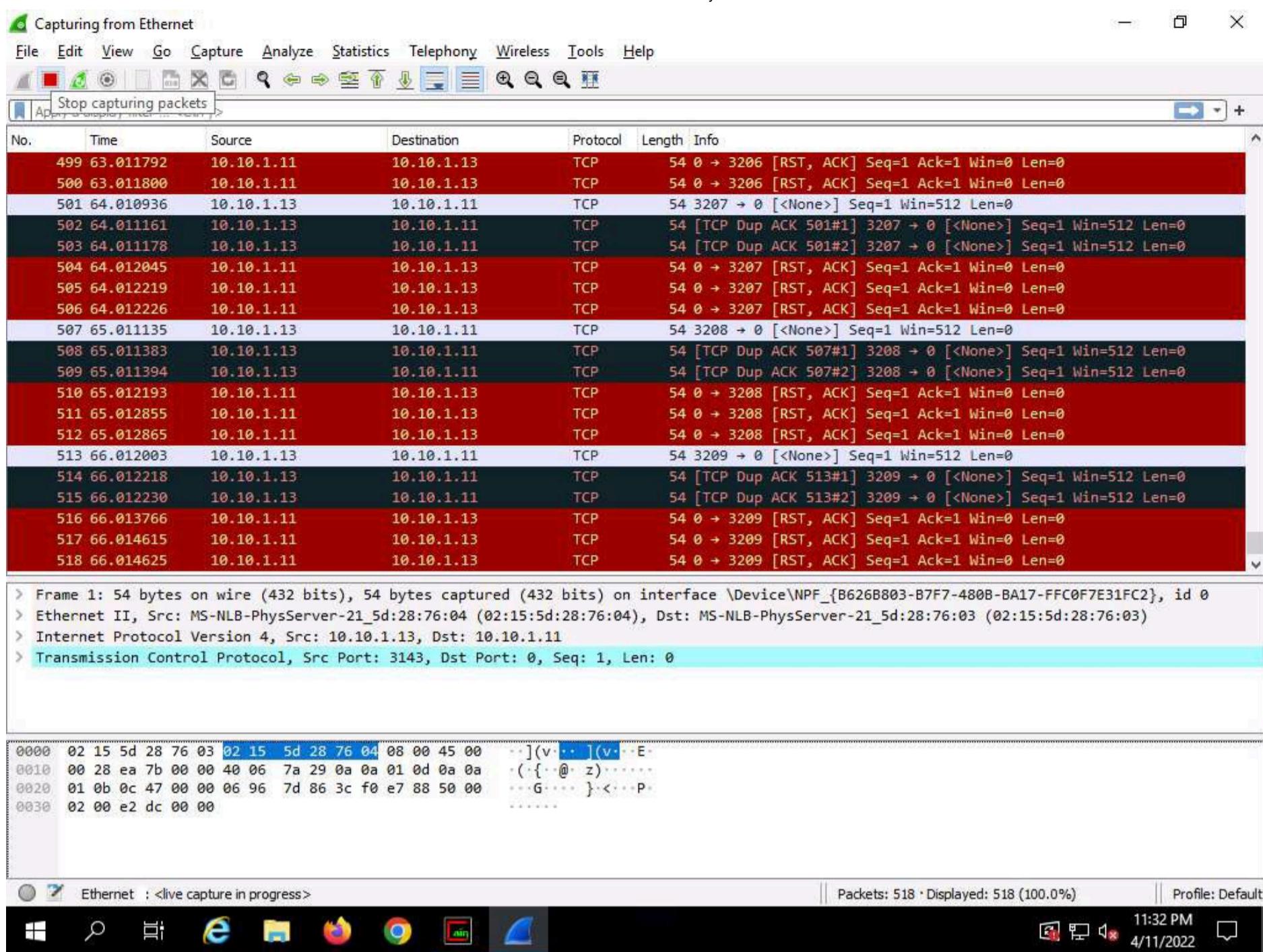
36. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.



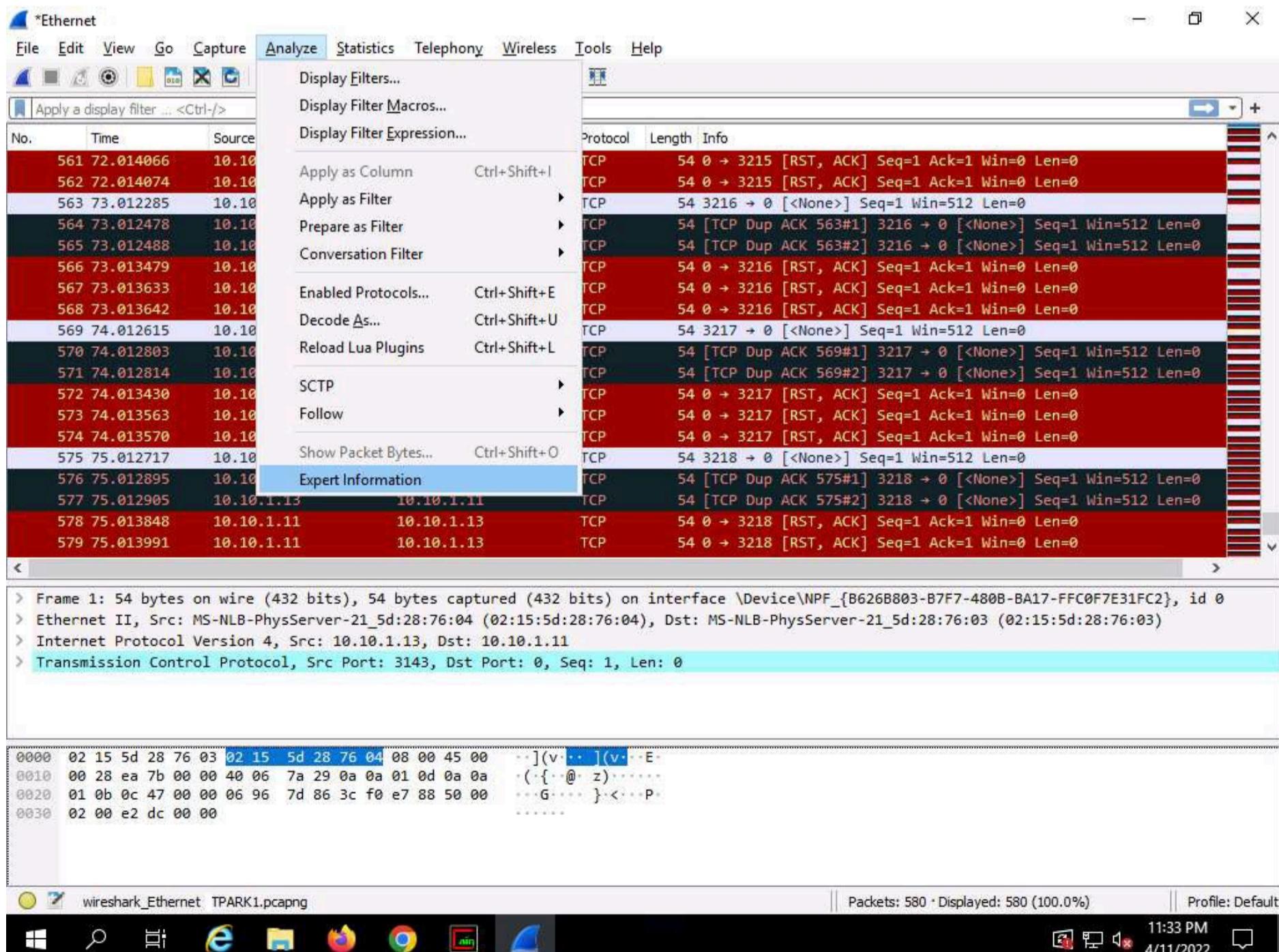
37. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.



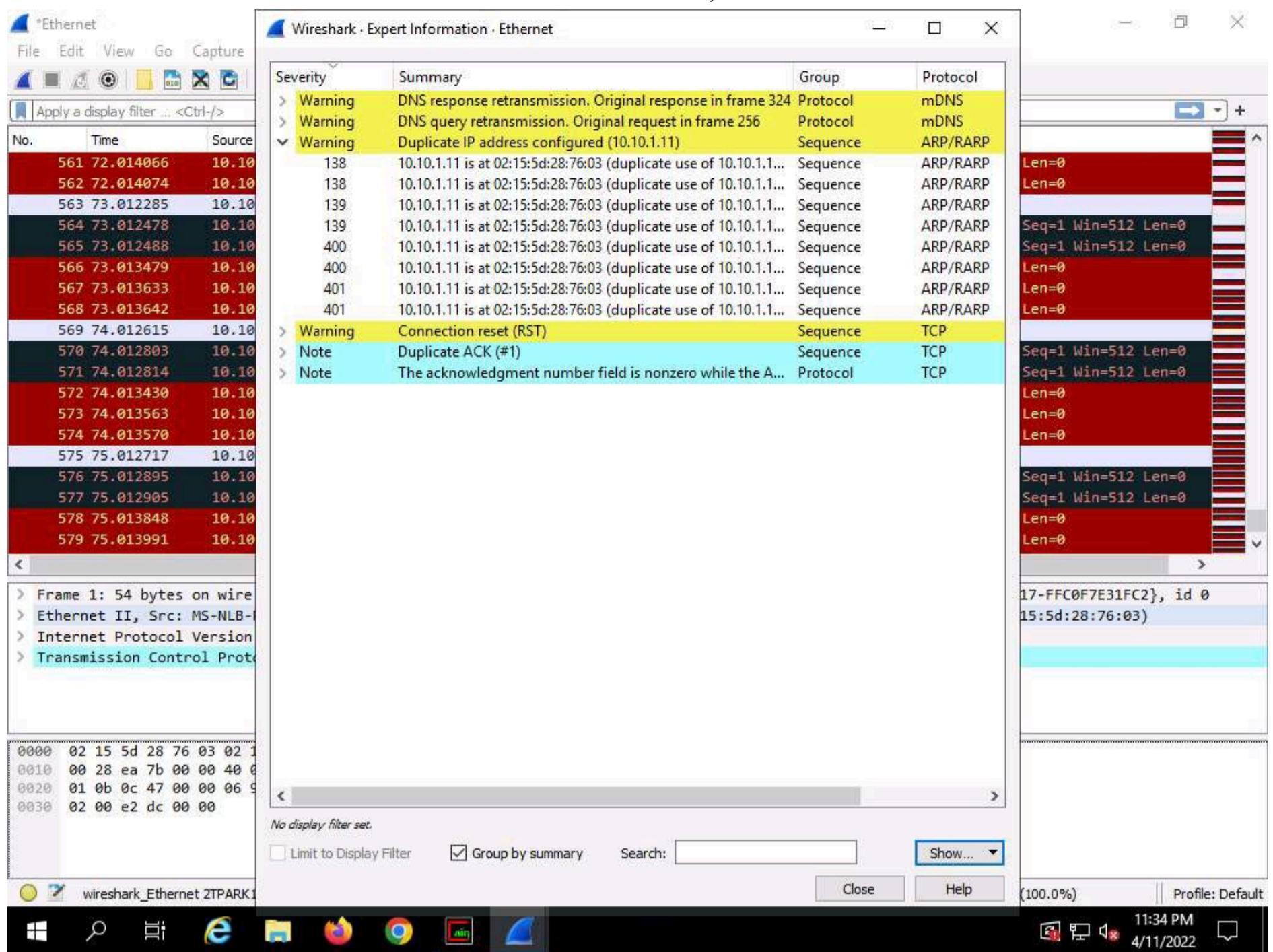
38. Now, switch to **Wireshark** and click the **Stop packet capturing** icon to stop the packet capturing.



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

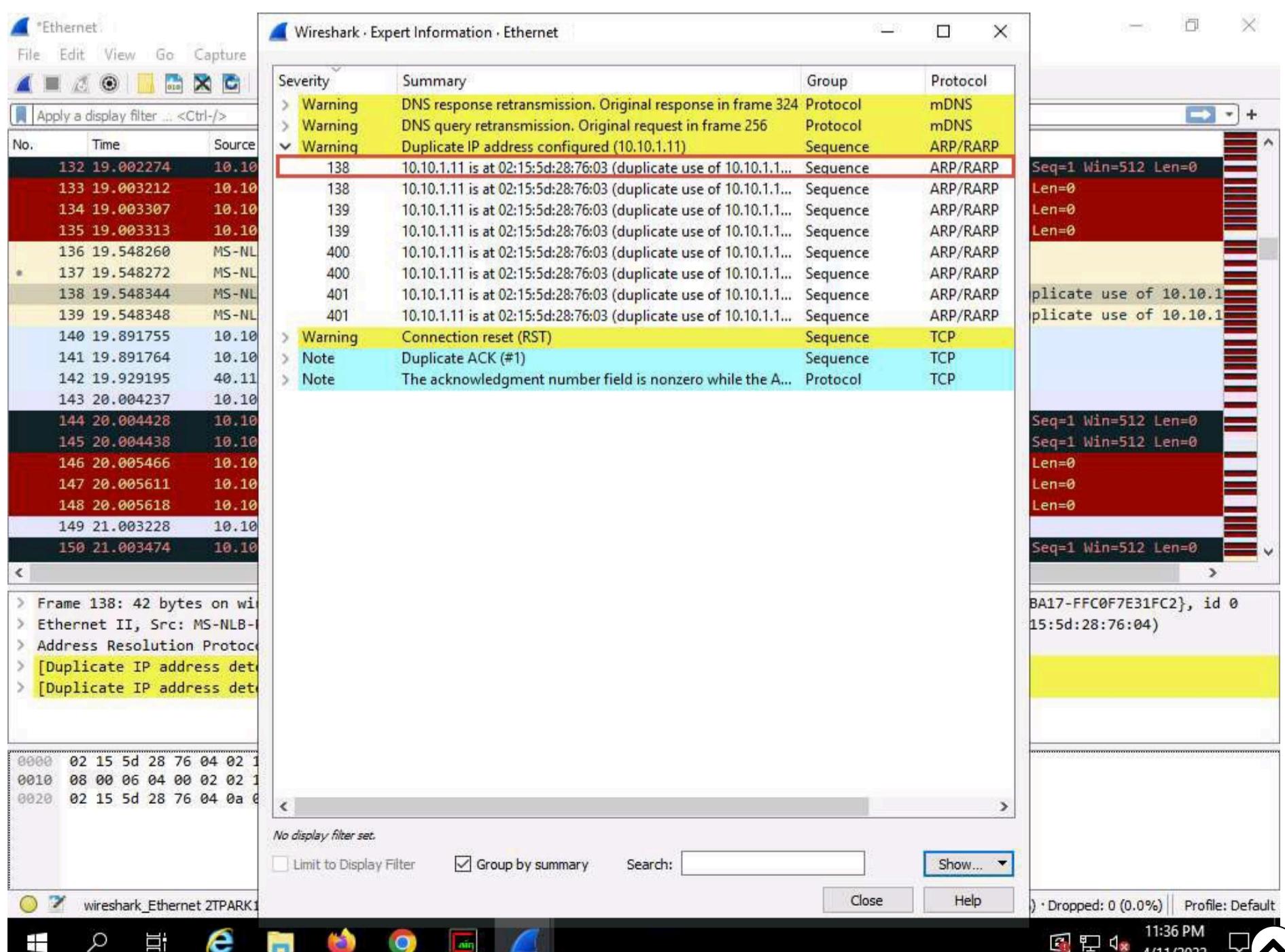


40. The Wireshark . Expert Information window appears; click to expand the Warning node labeled **Duplicate IP address configured (10.10.1.11)**, running on the ARP/RARP protocol.



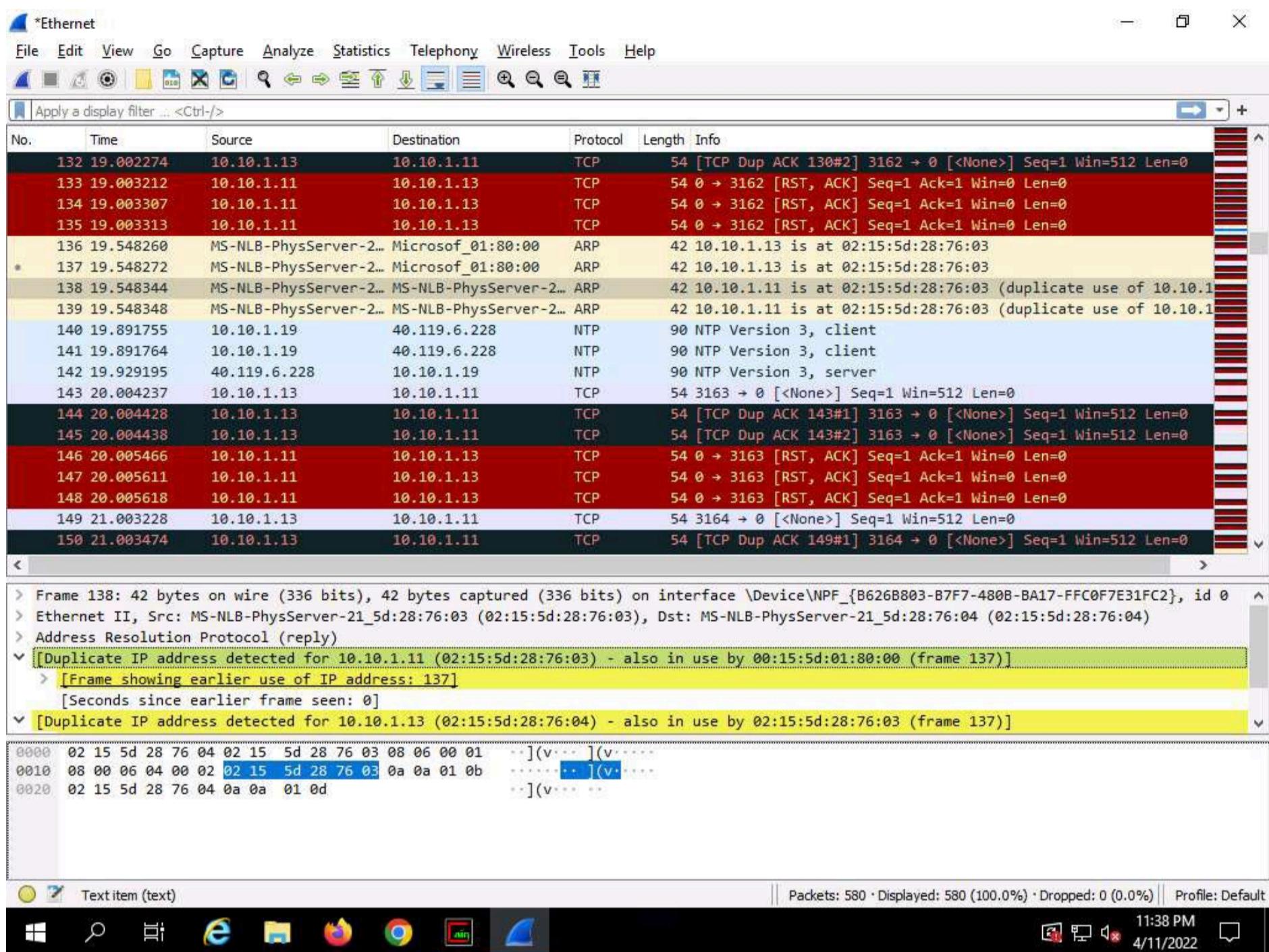
41. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

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.



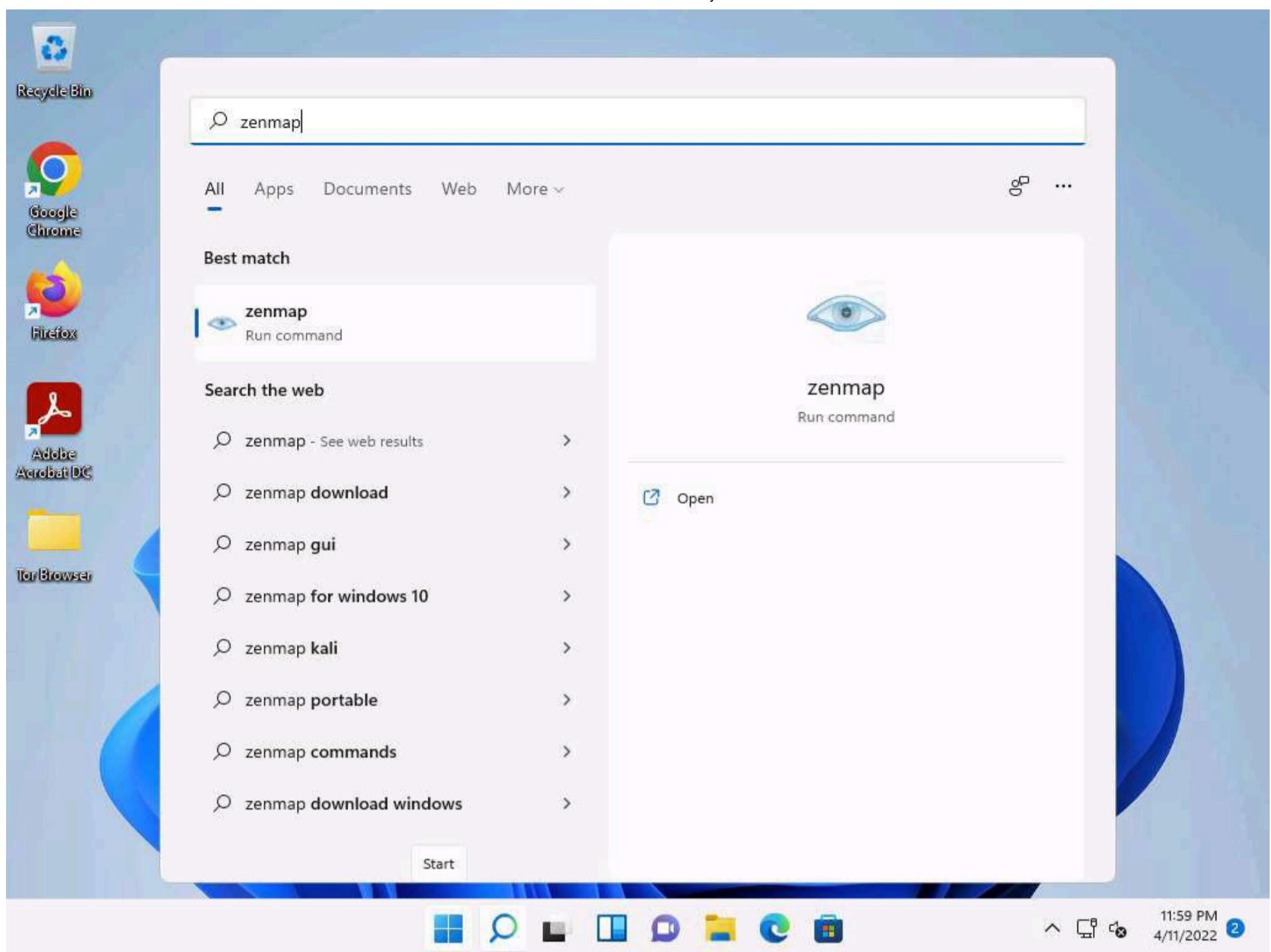
Note: ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the 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.

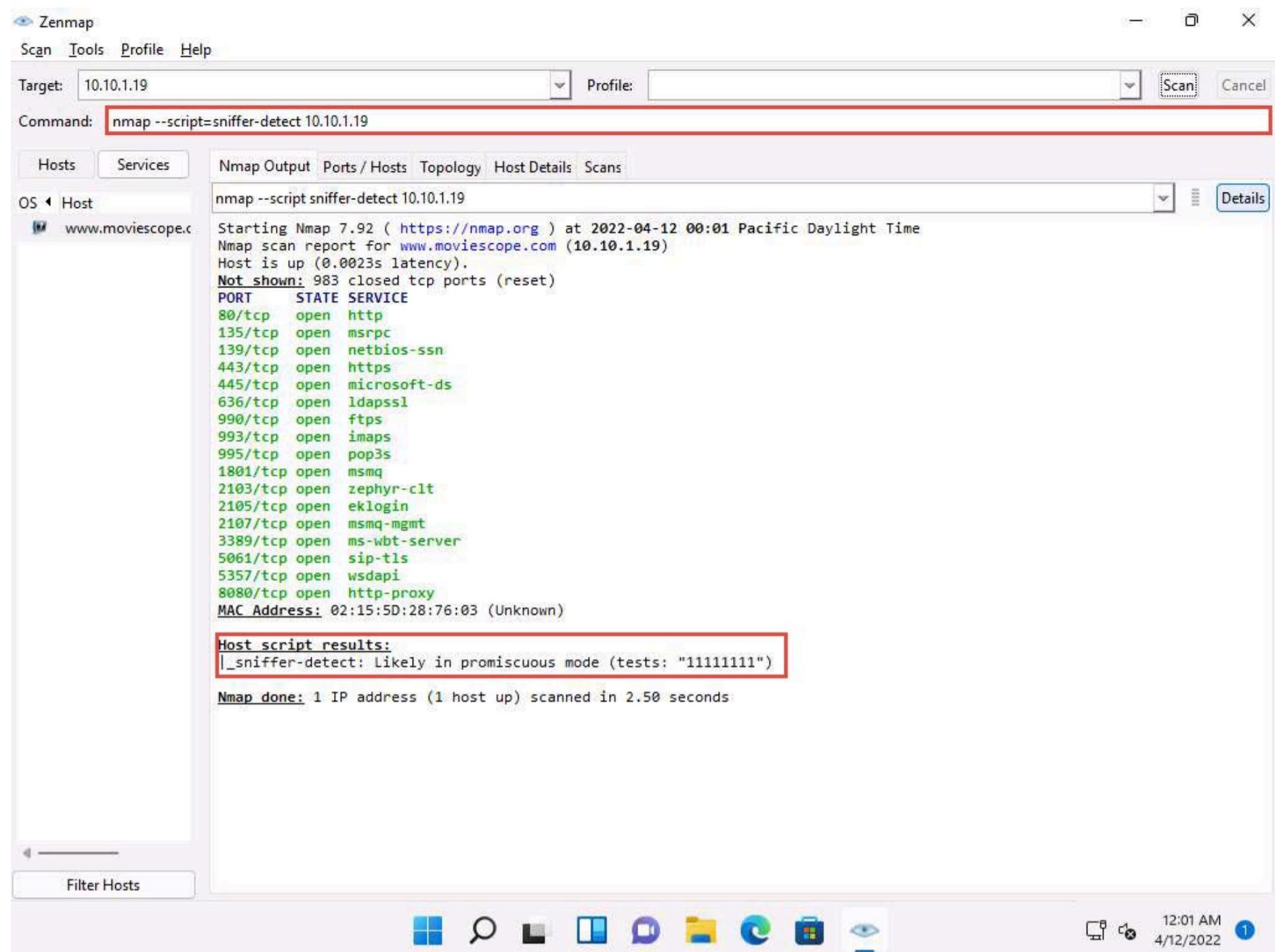
47. Now, we shall perform promiscuous mode detection using **Nmap**.

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

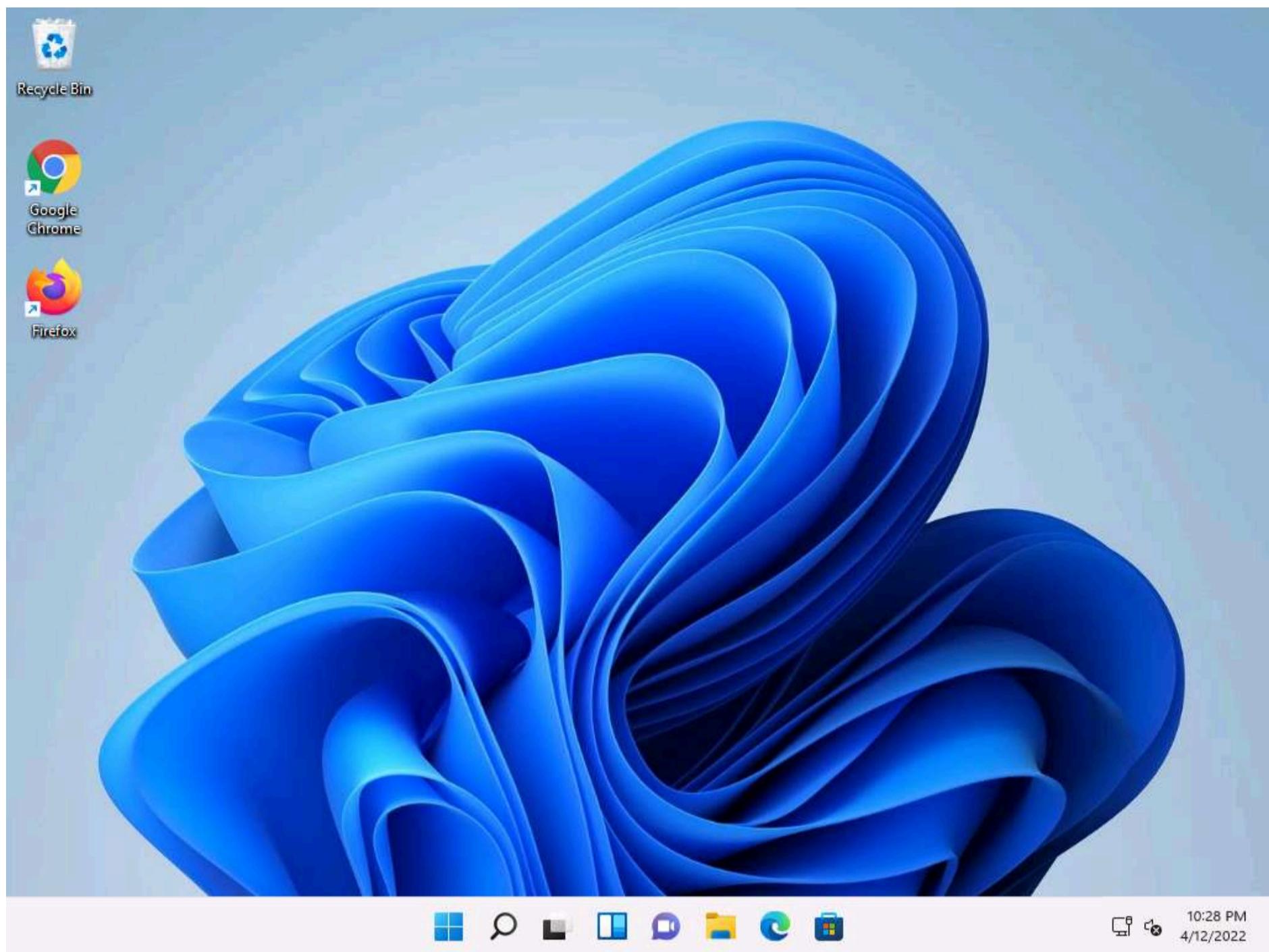
Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy to use interface that allows users to protect and monitor networks in a critical business environment. It helps ethical hackers or pentesters in quickly detecting ARP poisoning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

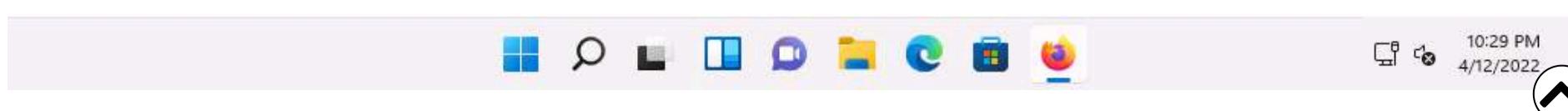
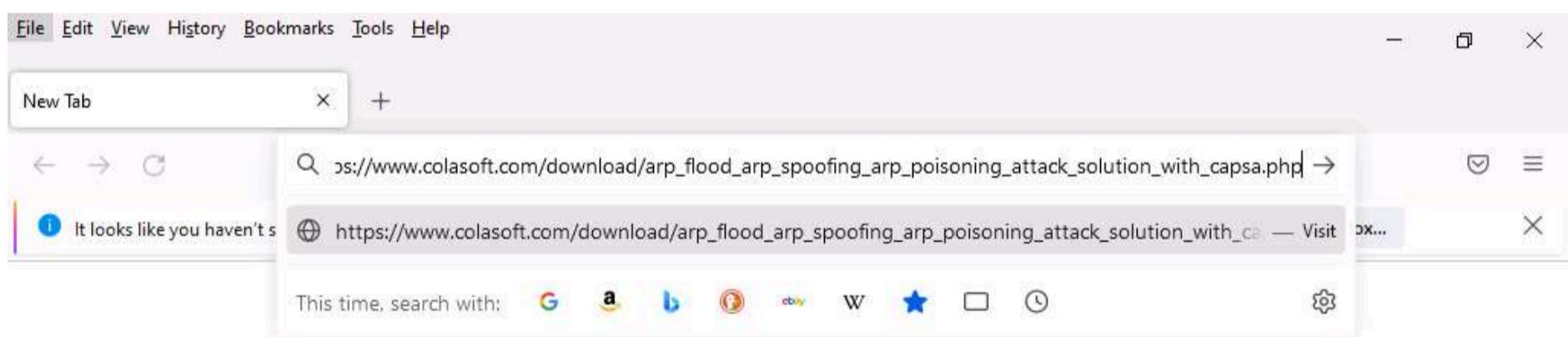
Here, we will use Habu tool to perform ARP poisoning attack on the target system and use Capsa Network Analyser to detect the attack.

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](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).



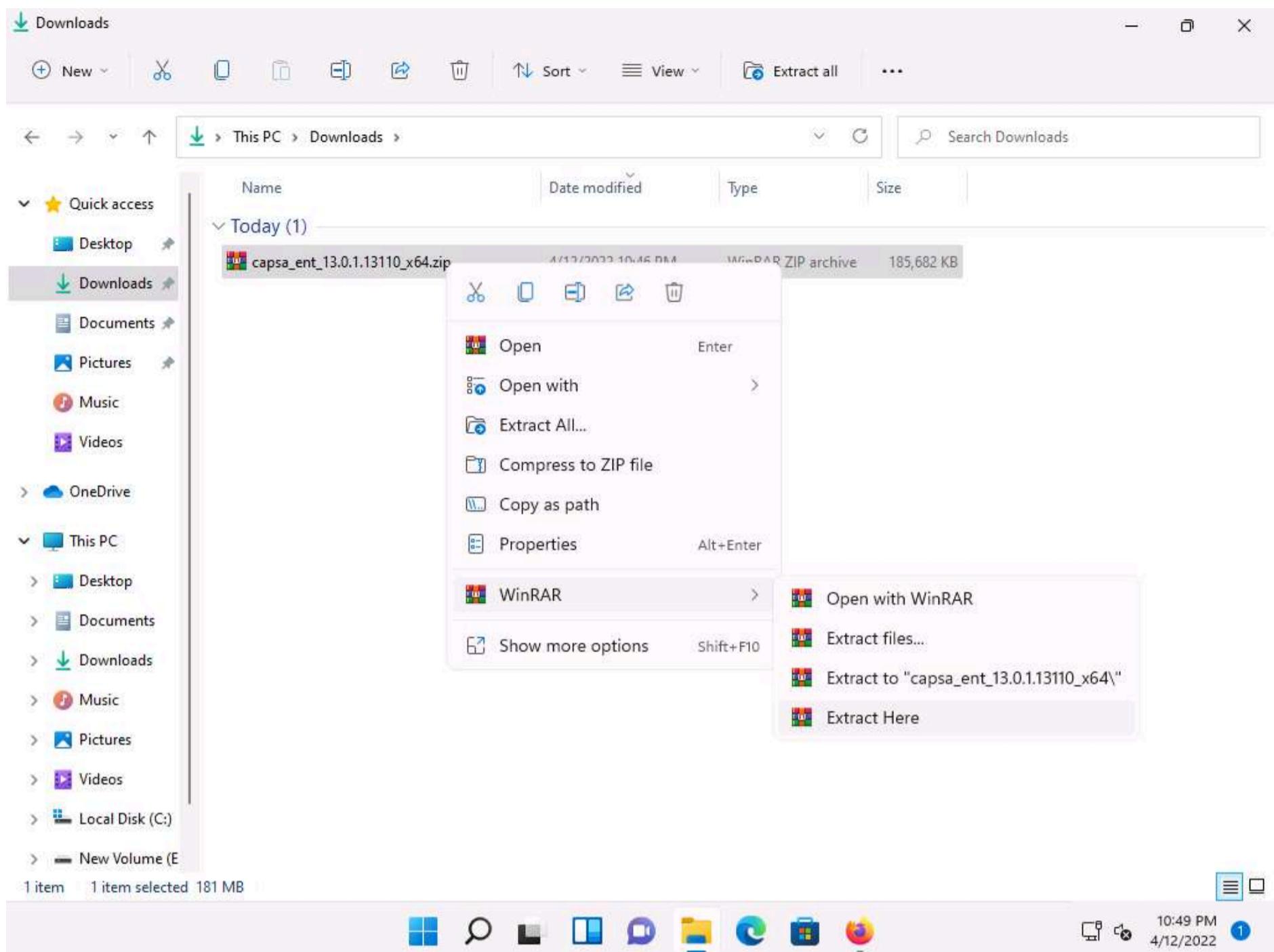
The screenshot shows the Colasoft website at [https://www.colasoft.com/download/products/download\\_capsa.php](https://www.colasoft.com/download/products/download_capsa.php). The page displays a 'TRIAL DOWNLOADS' section with fields for First Name, Last Name, Country/Region, State, Company, Email, and Phone. A checkbox for 'Subscribe to our newsletter' is checked, and a reCAPTCHA box with 'I'm not a robot' is present. A large blue button labeled '30-Day Trial Download' is centered below the form.

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**.

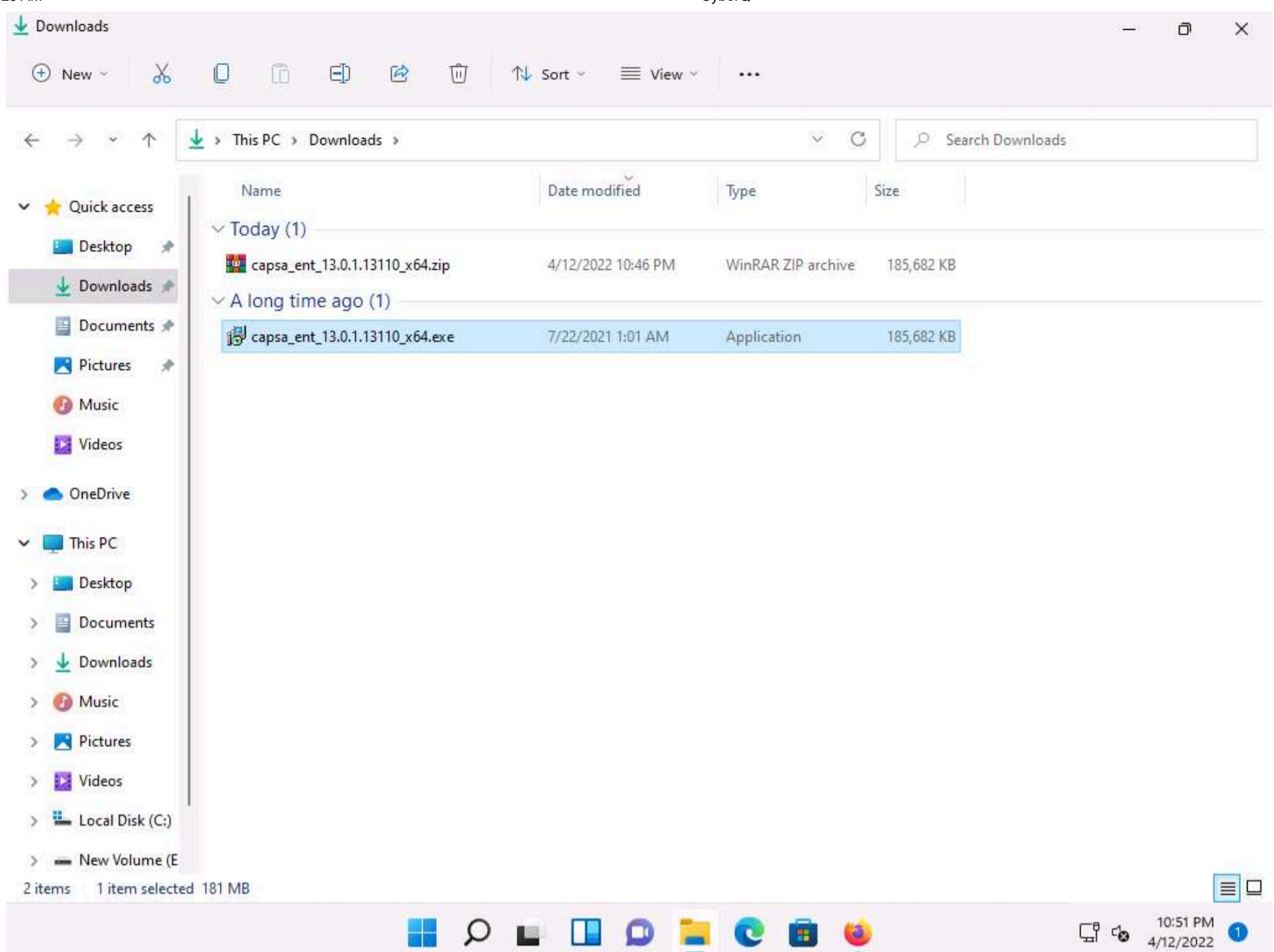
The screenshot shows the Firefox browser at [https://www.colasoft.com/download/products/api/process\\_demo\\_download.ent.php](https://www.colasoft.com/download/products/api/process_demo_download.ent.php). A download dialog box is open, showing the file 'Opening capsa\_ent\_13.0.1.13110\_x64.zip'. The dialog asks what Firefox should do with the file, with options: 'Open with WinRAR archiver (default)', 'Save File' (which is selected), and 'Do this automatically for files like this from now on.' Buttons for 'OK' and 'Cancel' are at the bottom.

6. The **capsa\_ent\_13.0.1.13110\_x64.zip** file starts downloading, it will take approximately 5 minutes for the download.

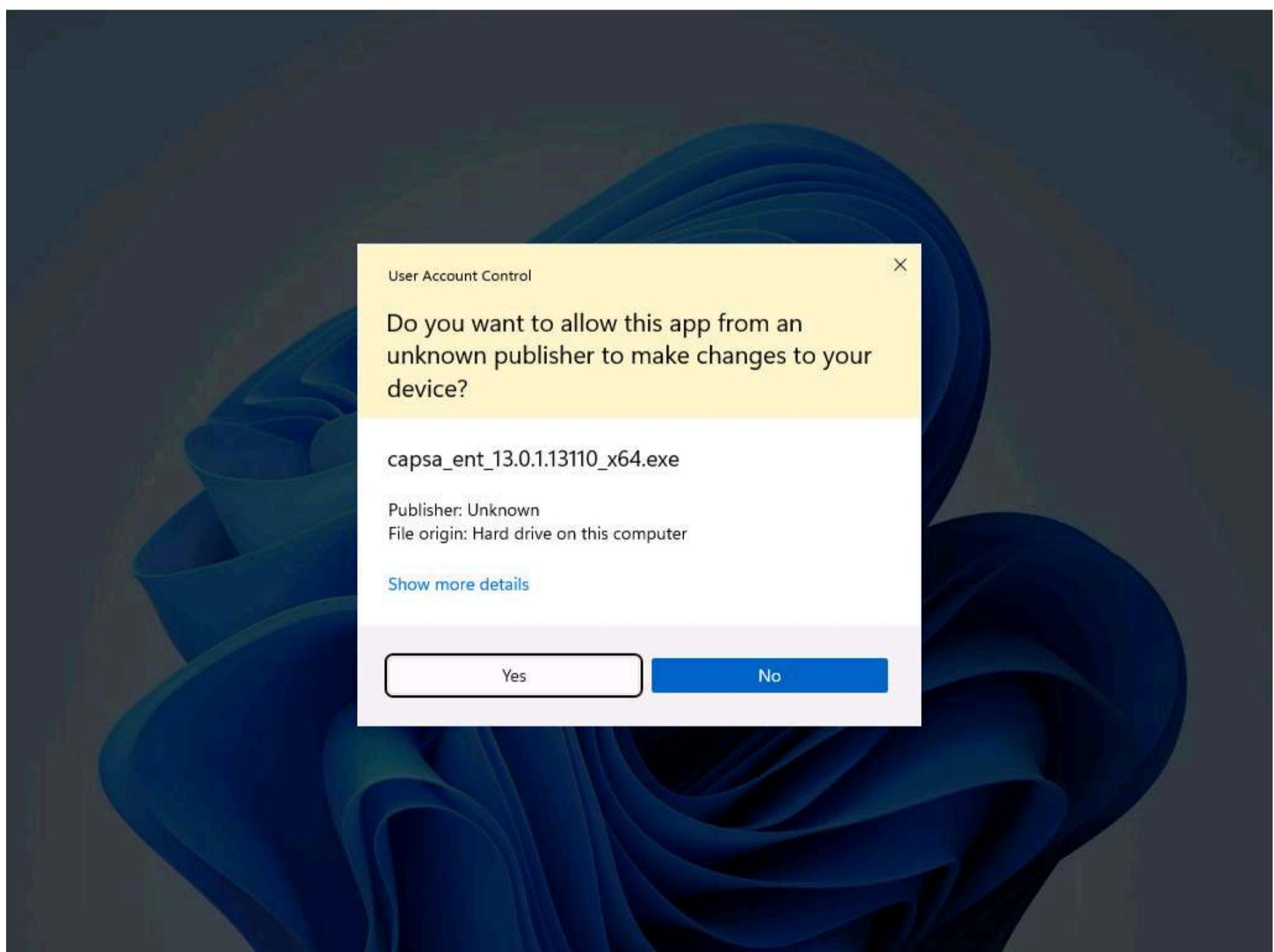
7. Once the download completes, navigate to the **Downloads** folder and right-click on **capsa\_ent\_13.0.1.13110\_x64.zip** file and hover the cursor over **WinRAR** and select **Extract Here** option from the list.



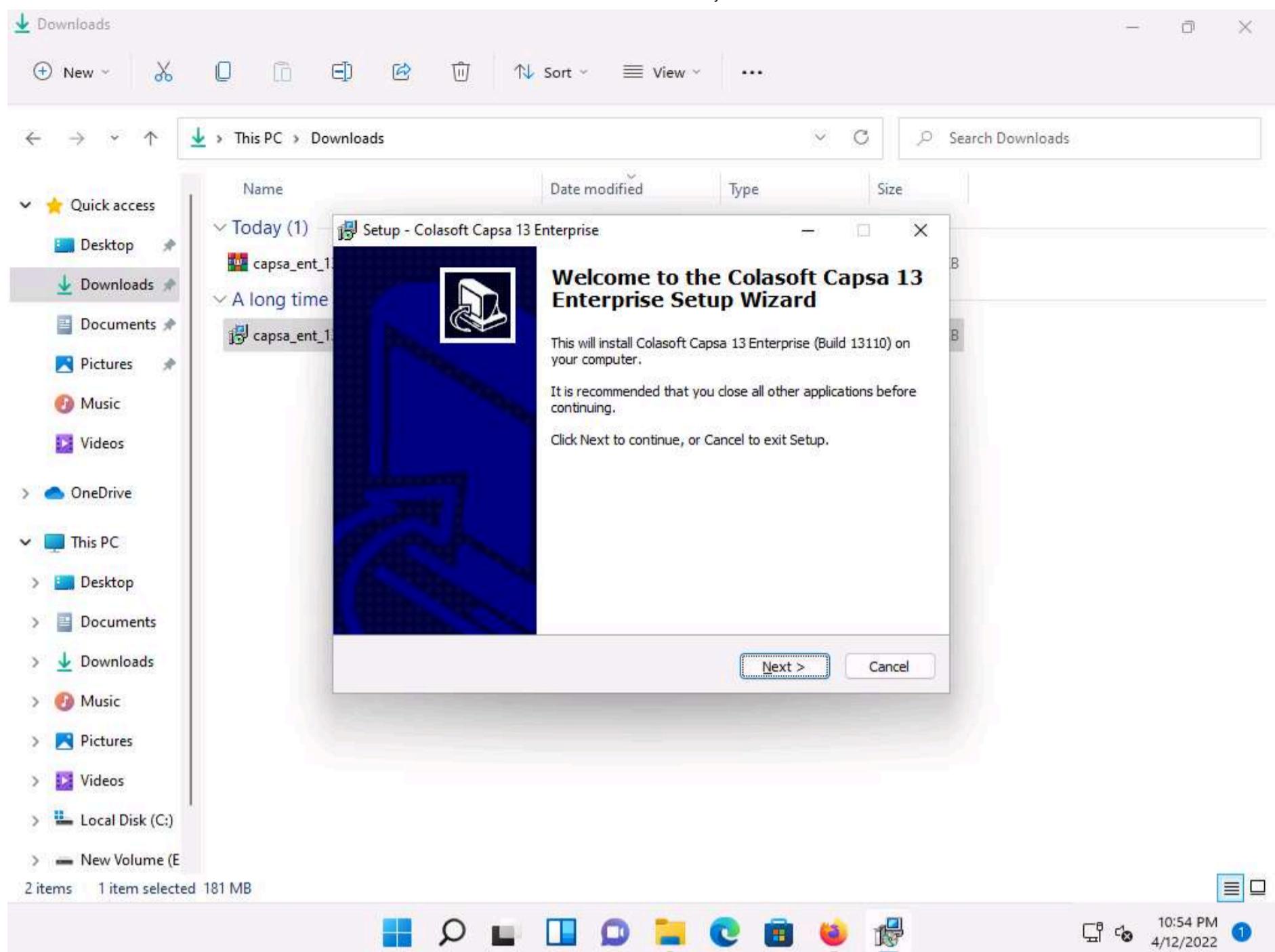
8. Once the extraction is completed, double-click the **capsa\_ent\_13.0.1.13110\_x64.exe** file.



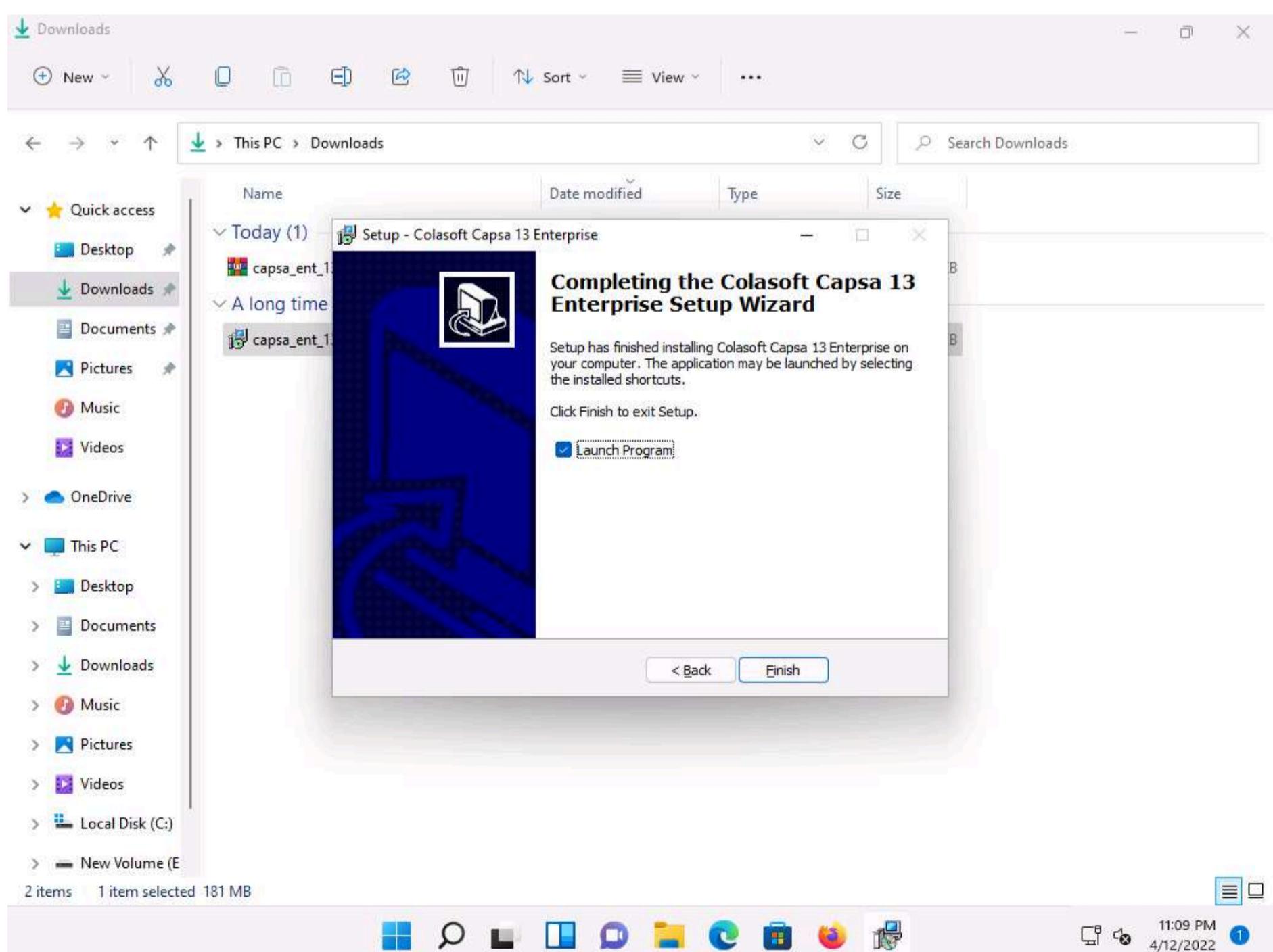
9. A User Account Control pop-up appears; click Yes.



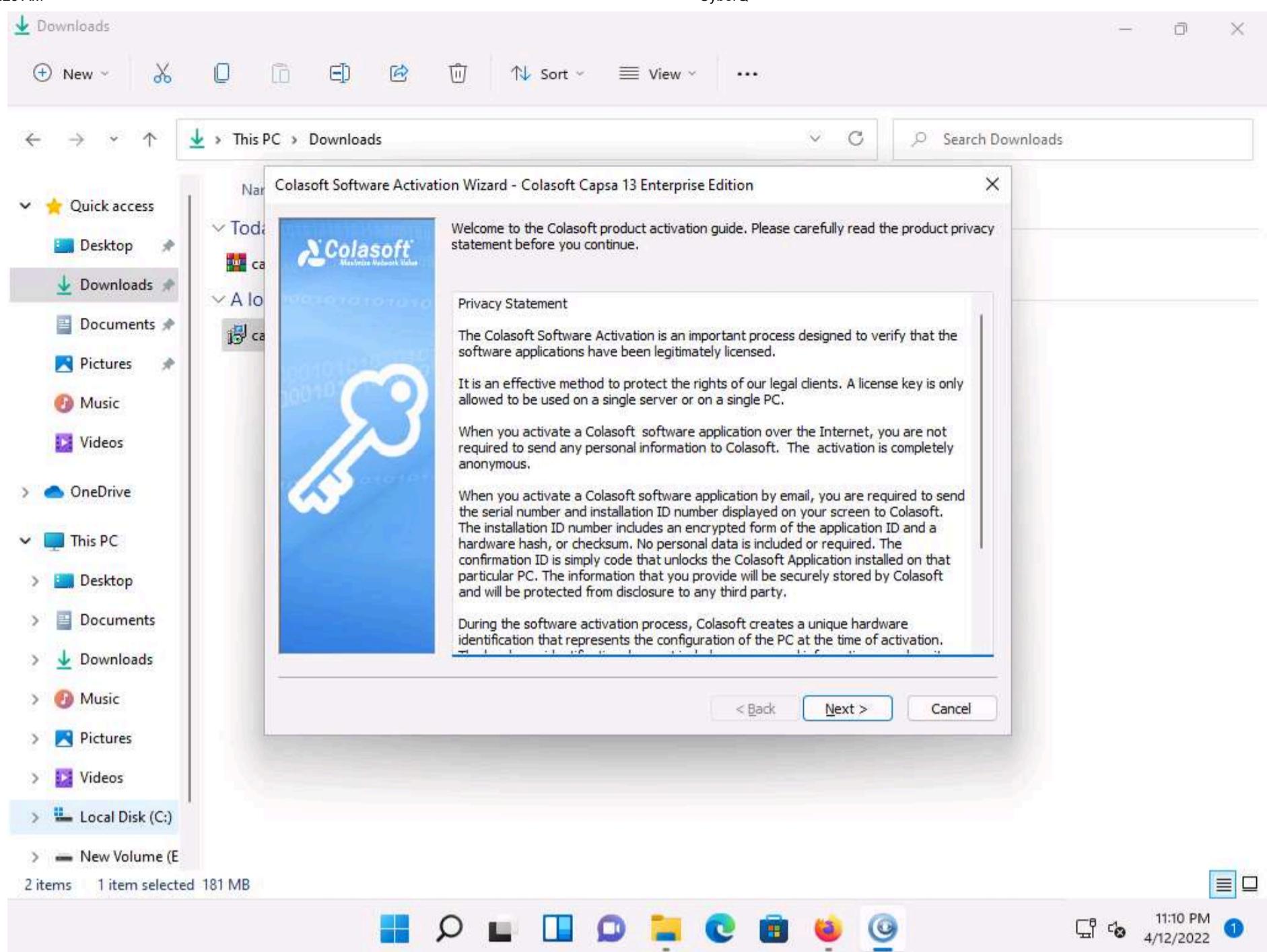
10. Setup - Colasoft Capsa 13 Enterprise window appears, click Next and follow the wizard driven steps to install **Colasoft Capsa 13 Enterprise** tool.



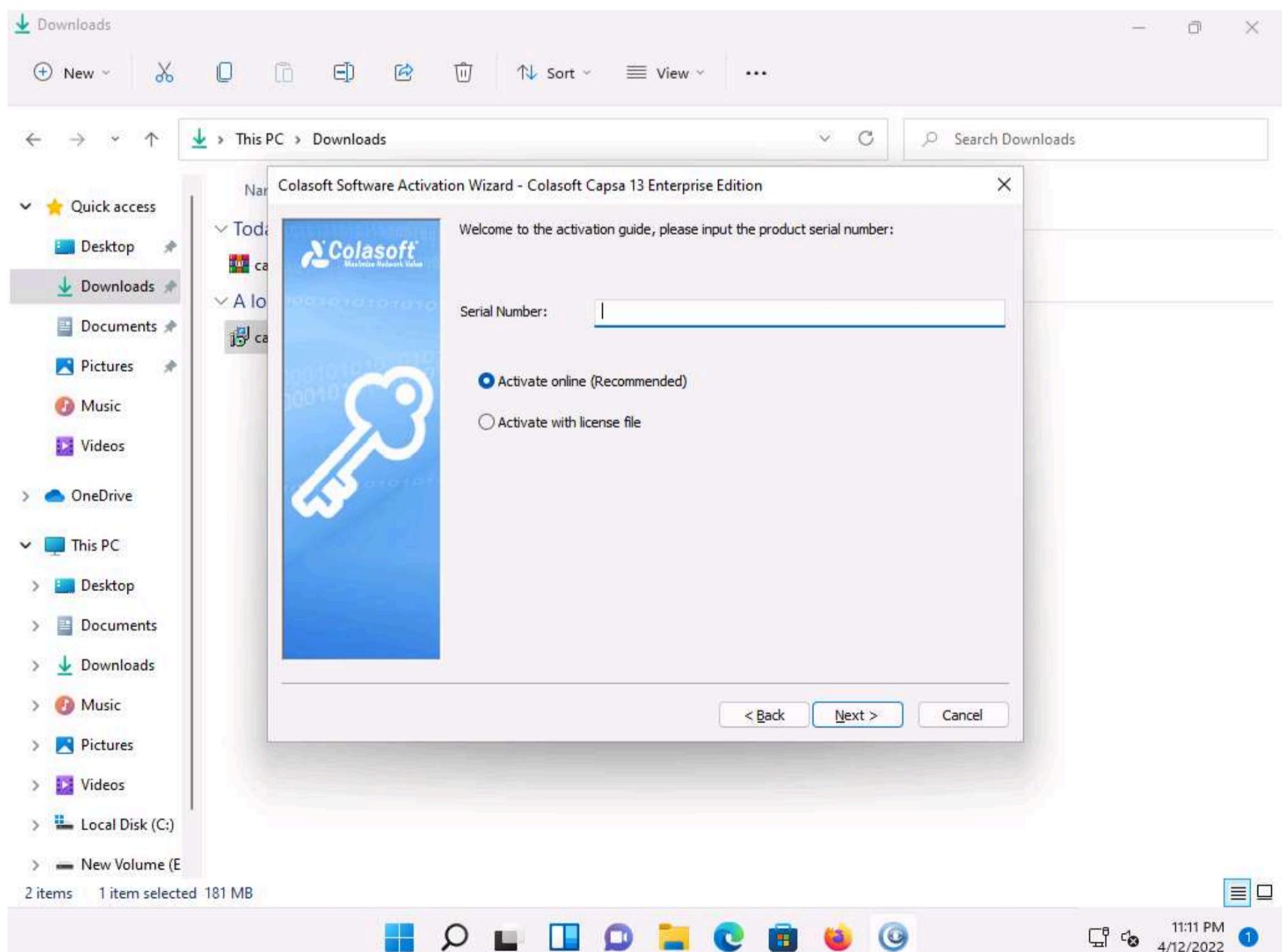
11. In the **Completing the Colasoft Capsa 13 Enterprise Setup Wizard**, ensure that **Launch Program** checkbox is checked and click on **Finish**.



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

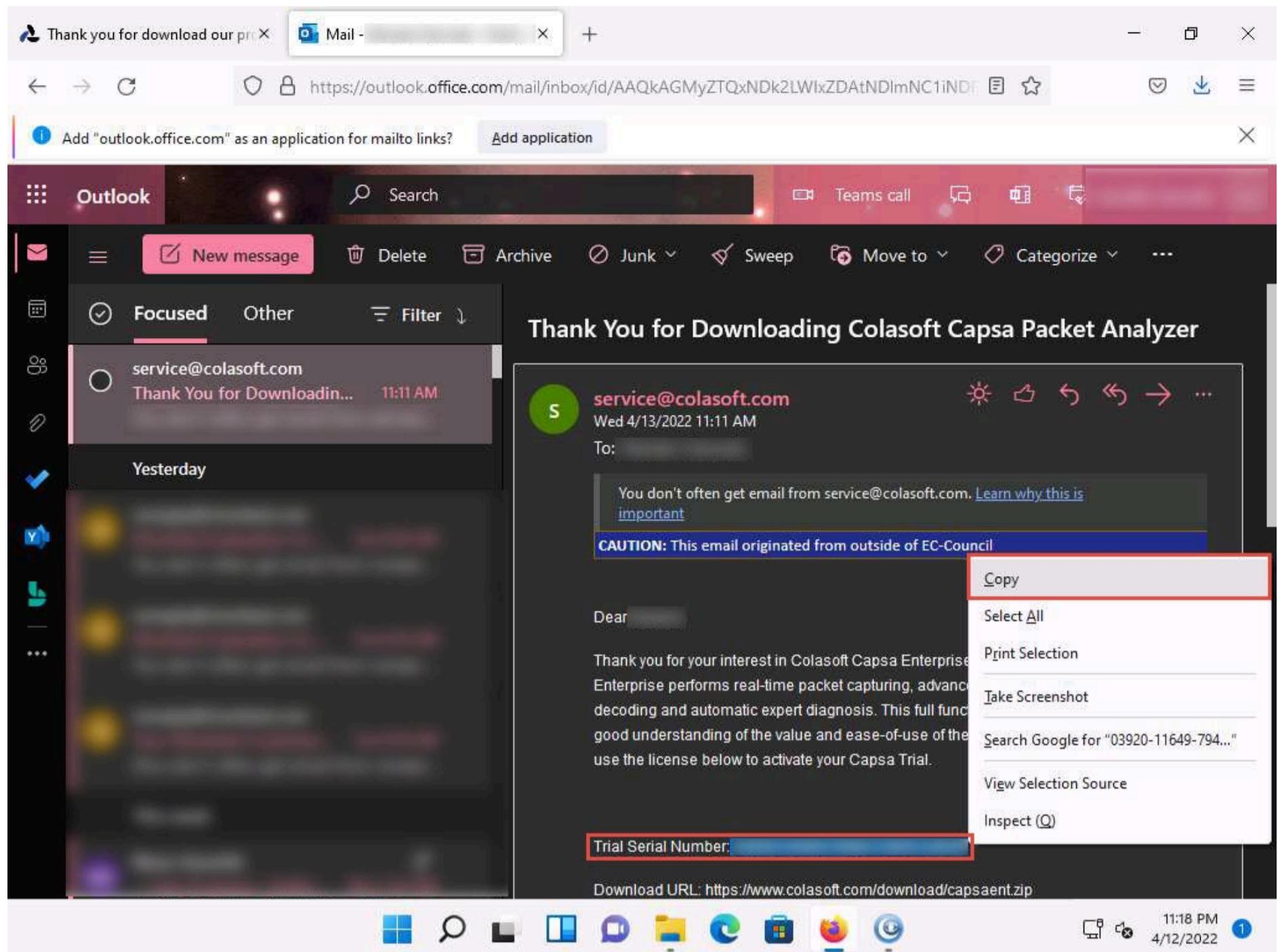


13. In the next window we need to enter the serial number to activate the license.

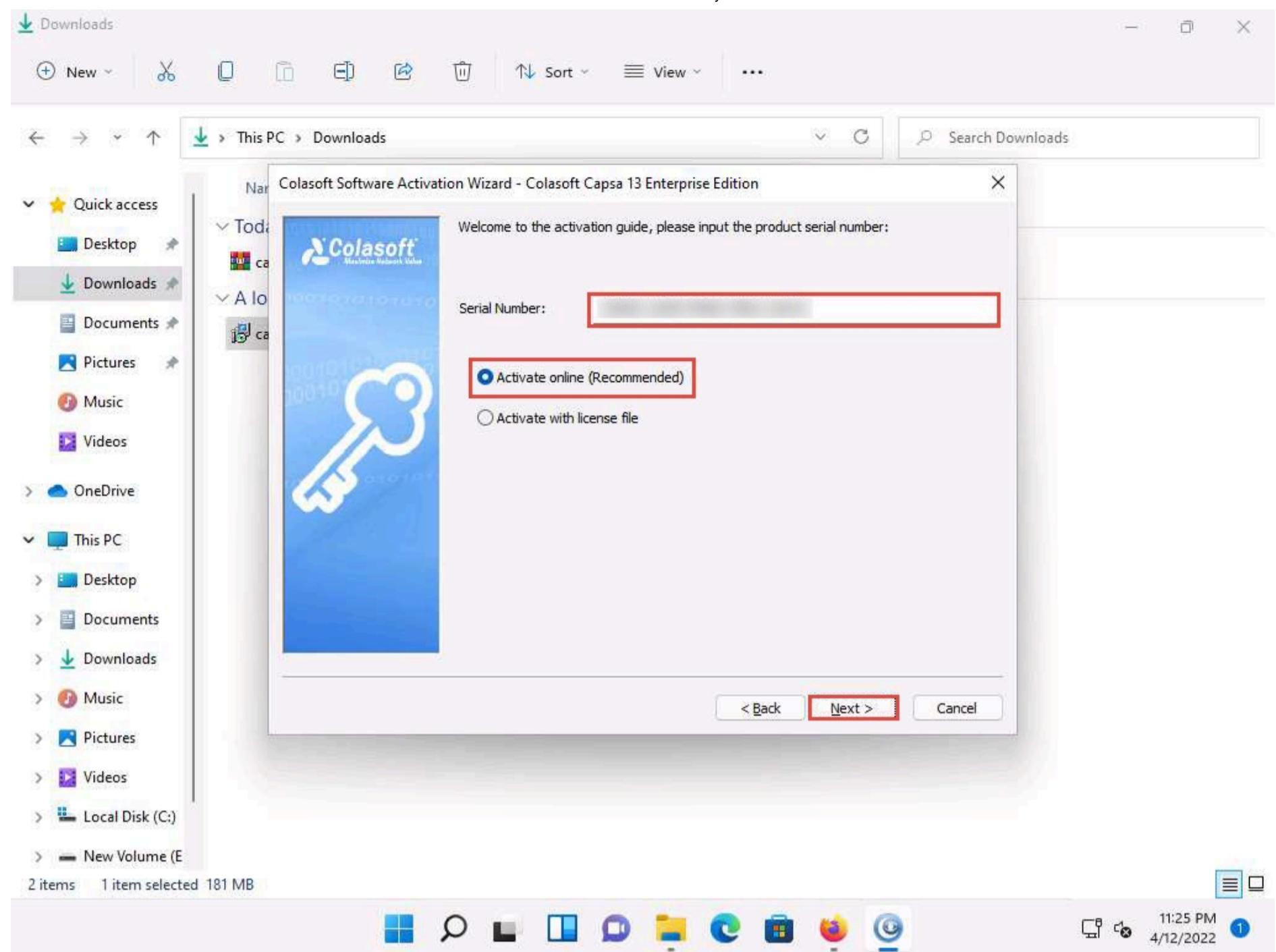


14. Leave the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** as it is and switch to the browser.

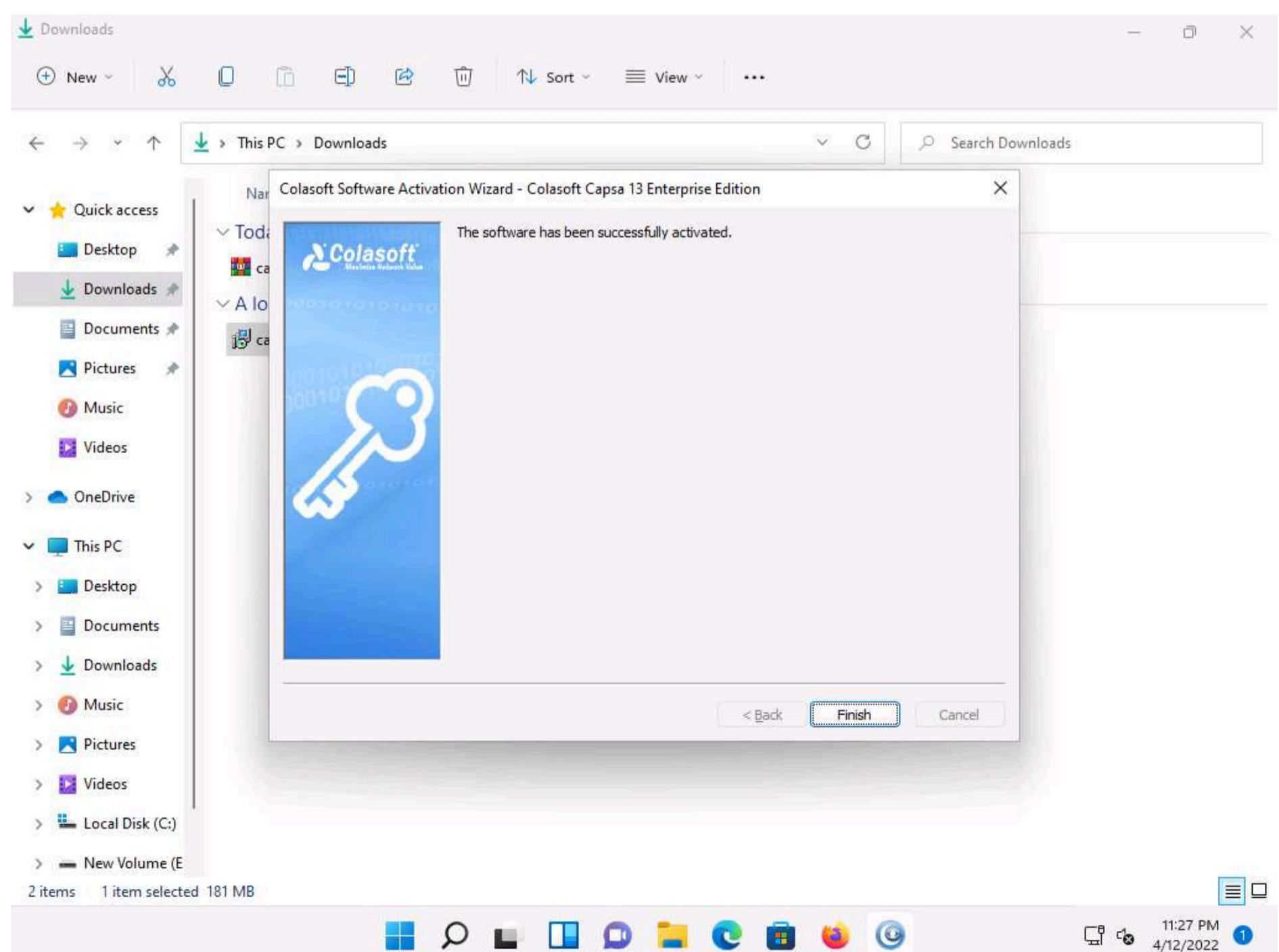
15. Open a new tab in the browser and log in to the email account you provided during registration. Open the email from **service@colasoft.com** and copy the **Trial Serial Number** as shown in the screenshot.



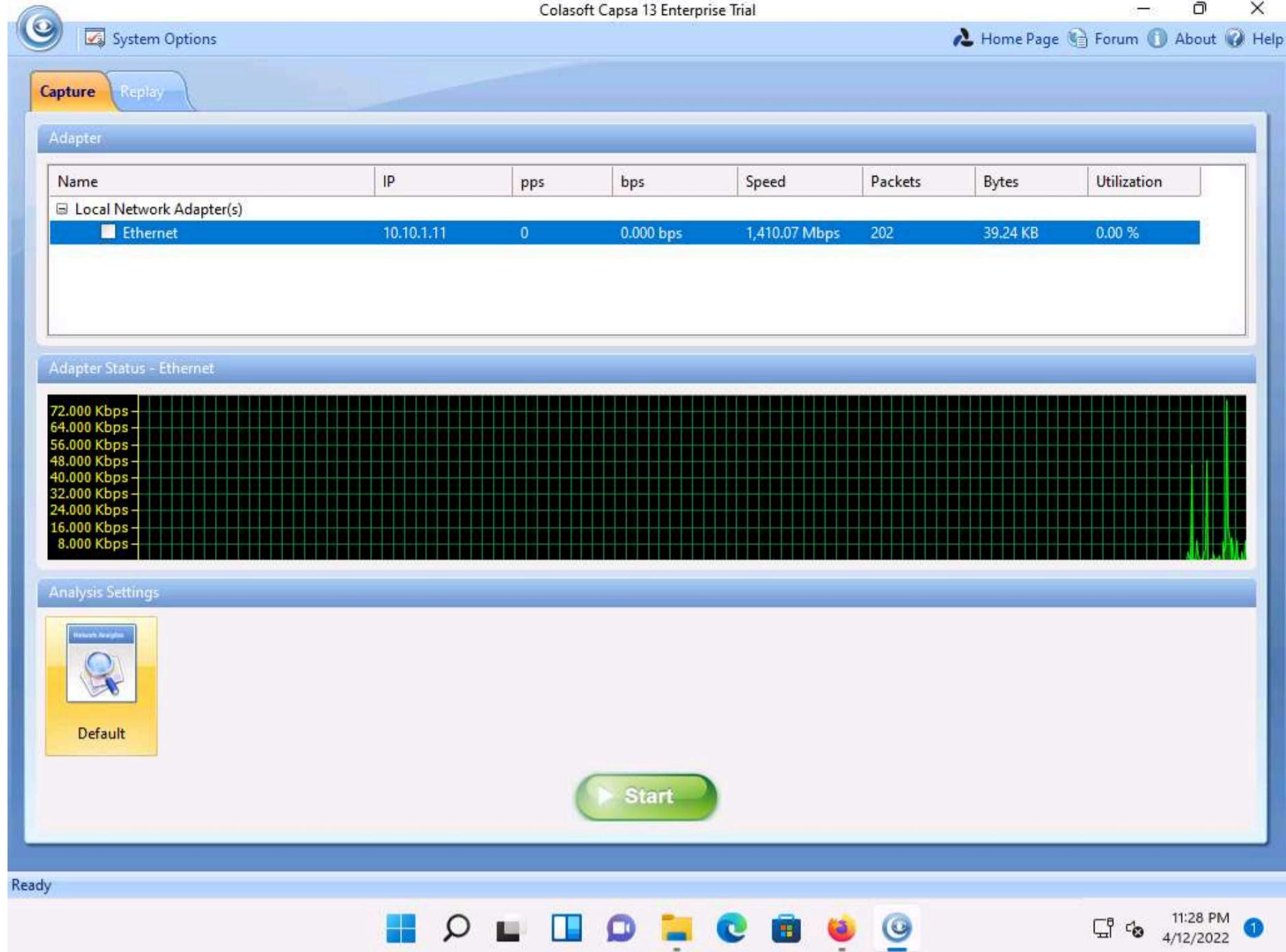
16. Now, minimize the browser window and switch to the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window and paste the copied serial number in the **Serial Number** field. Ensure that **Activate online (Recommended)** radio button is selected and click on **Next**.



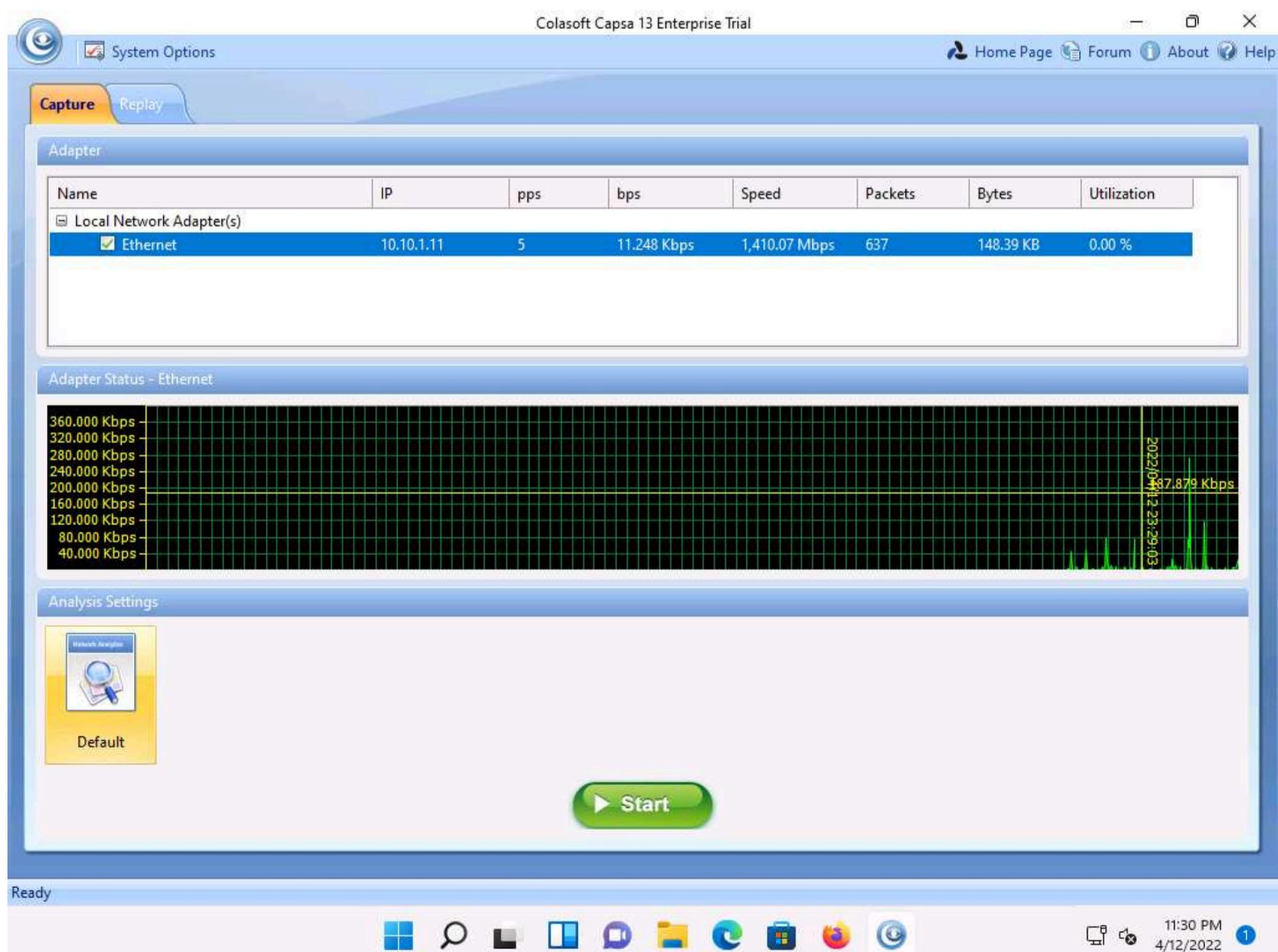
17. A **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window appears, showing that the software has been successfully activated, click on **Finish**.



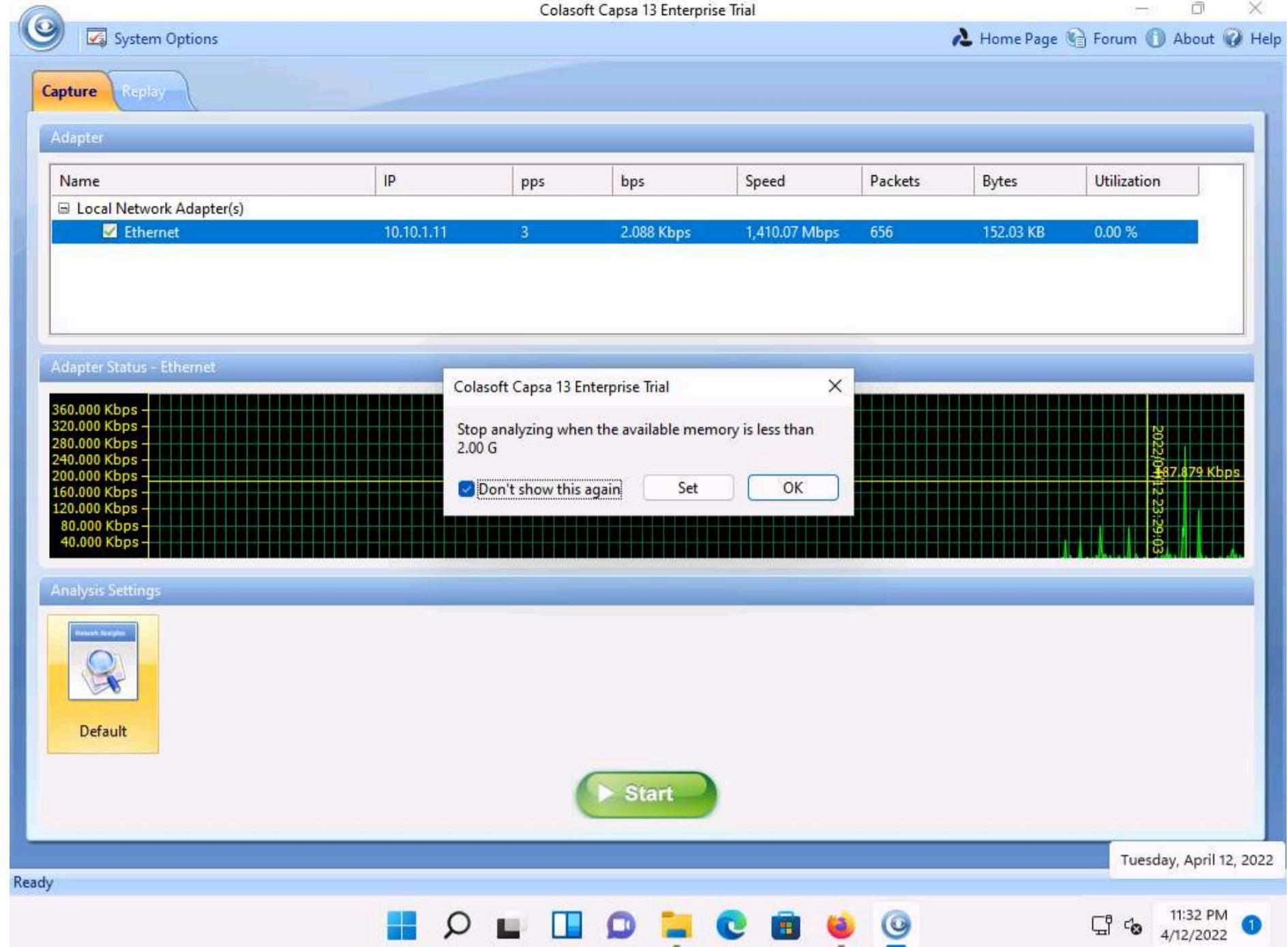
18. After successful installation, A **Colasoft Capsa 13 Enterprise Trial** window appears.



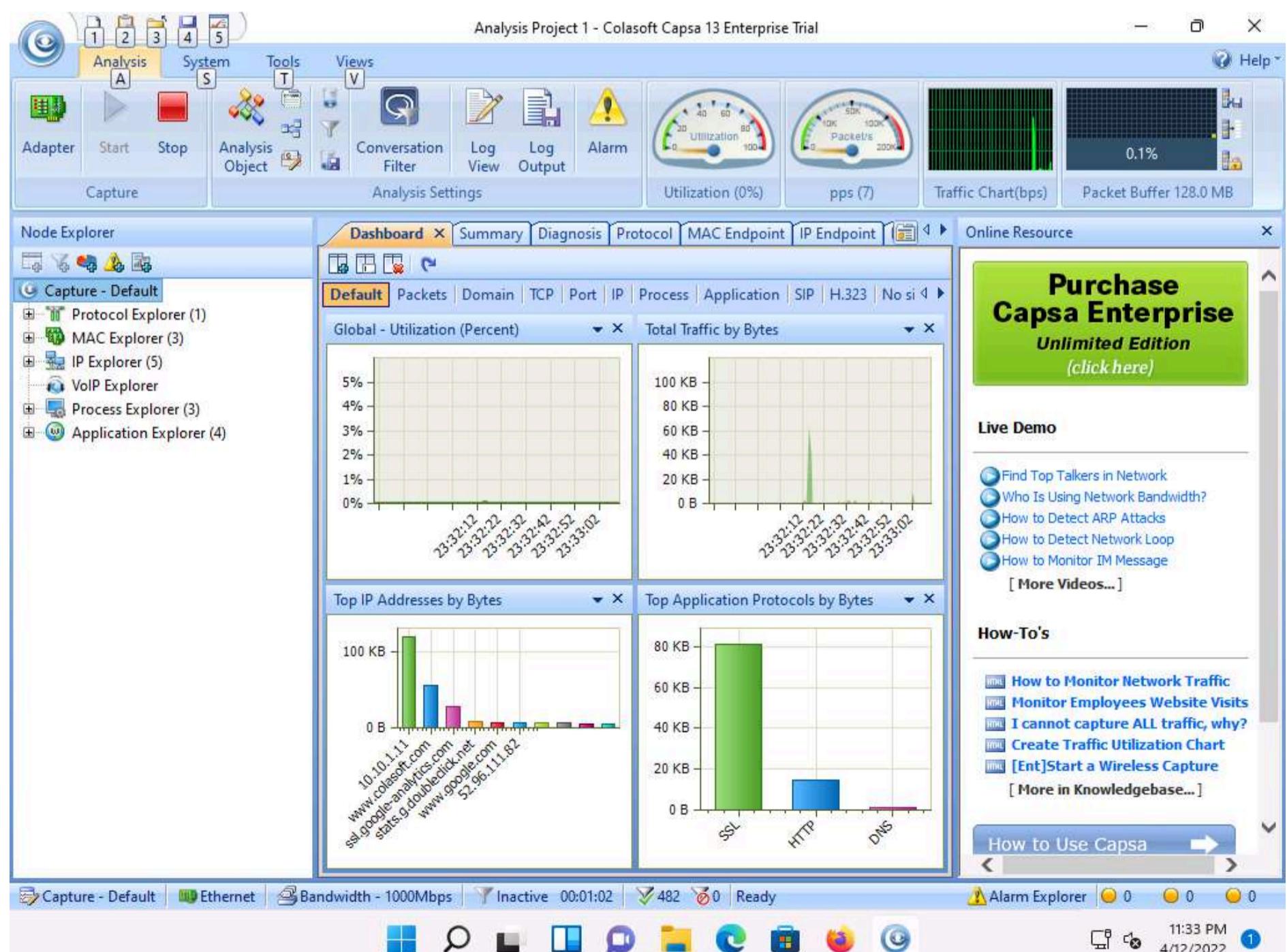
19. In the **Colasoft Capsa 13 Enterprise Trial** window check the checkbox beside the available adapter (here, **Ethernet**) and click on **Start**.



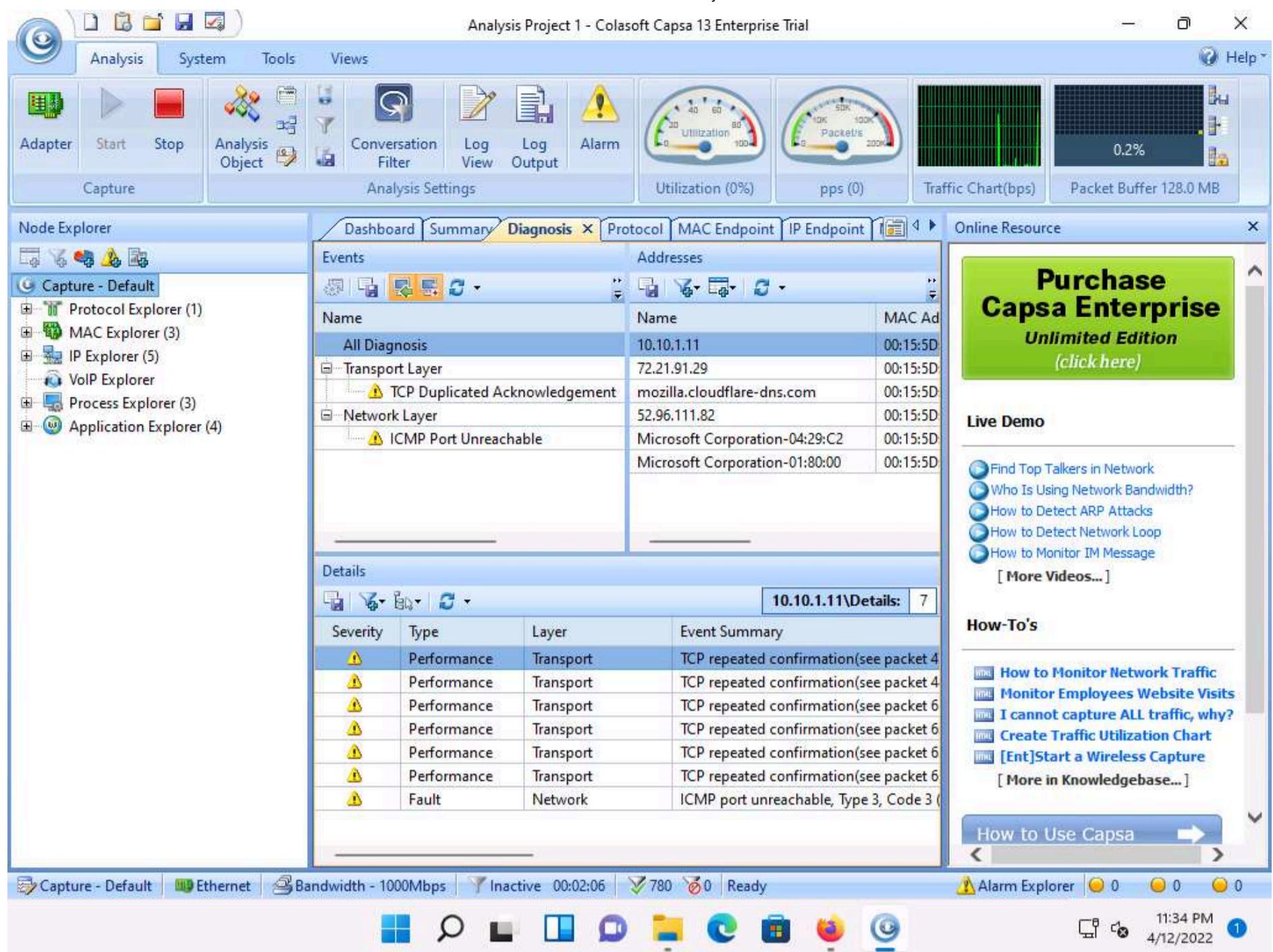
20. If a **Colasoft Capsa 13 Enterprise Trial** pop-up appears, select **Don't show this again** checkbox and click on **OK**.



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

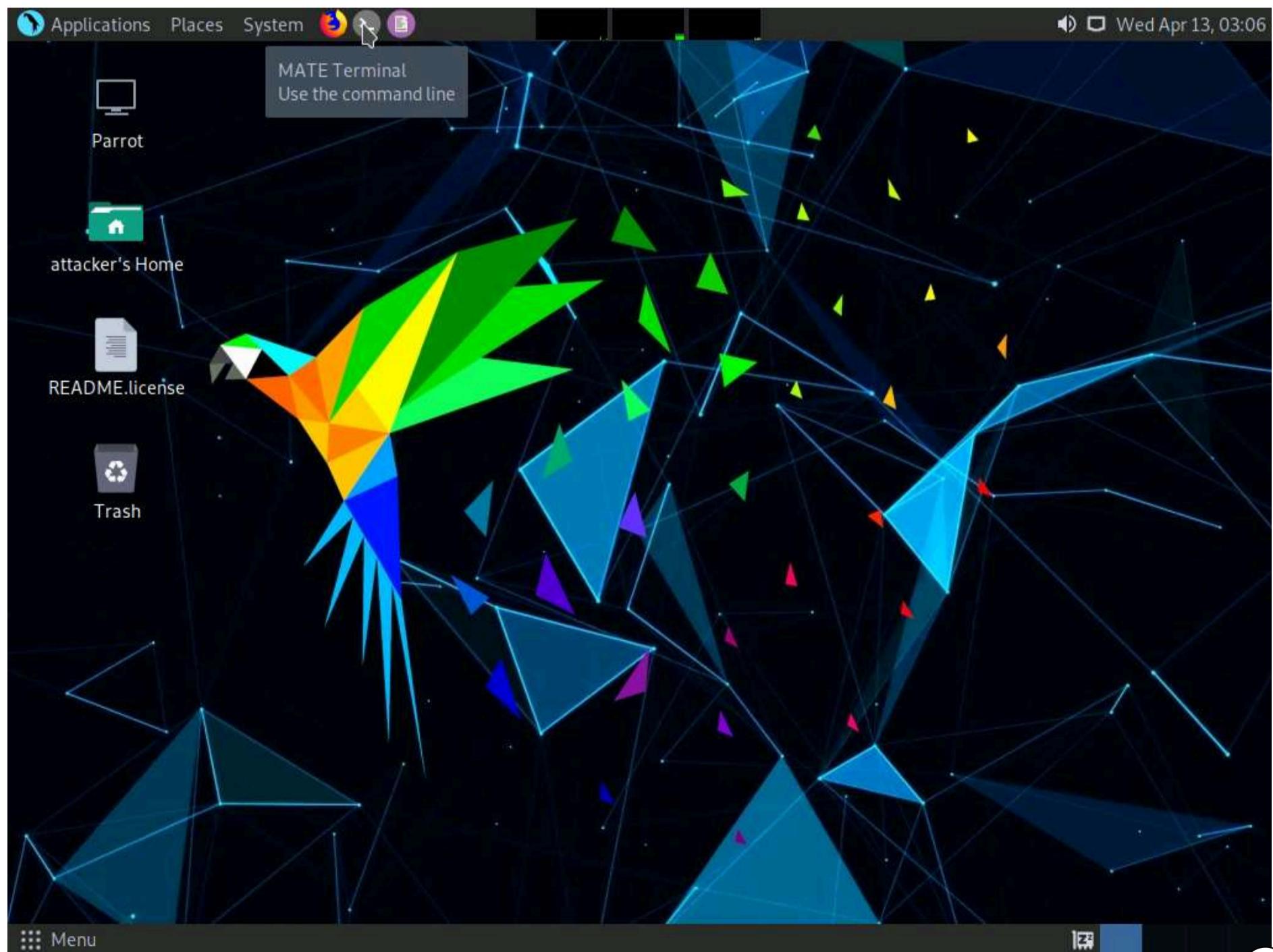


22. Navigate to the Diagnosis tab in the Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial window.



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

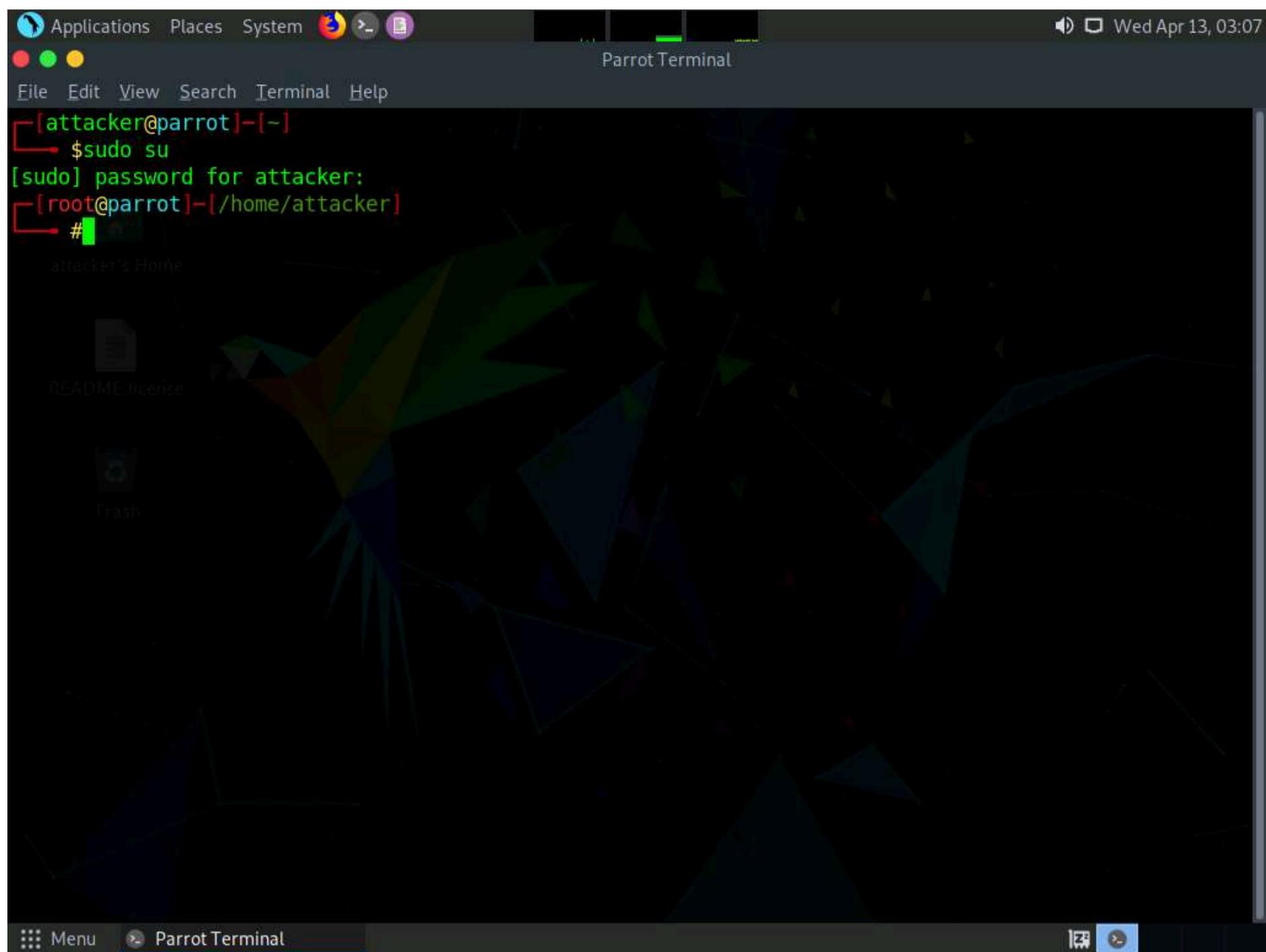
24. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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.

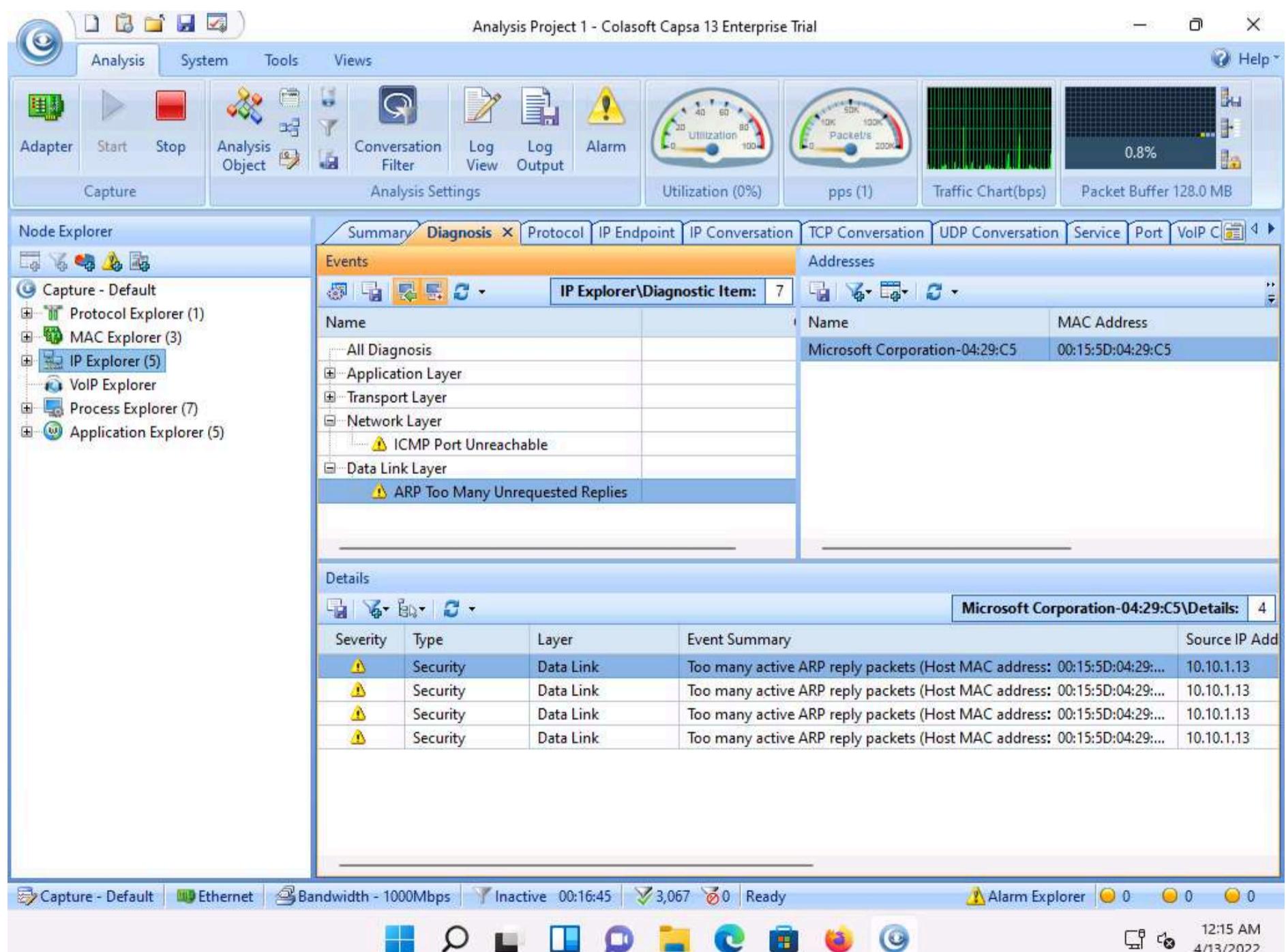
Note: If you receive any error while running the command ignore it.



```
[attacker@parrot]~[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#habu.arp.poison 10.10.1.11 10.10.1.13
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
```

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

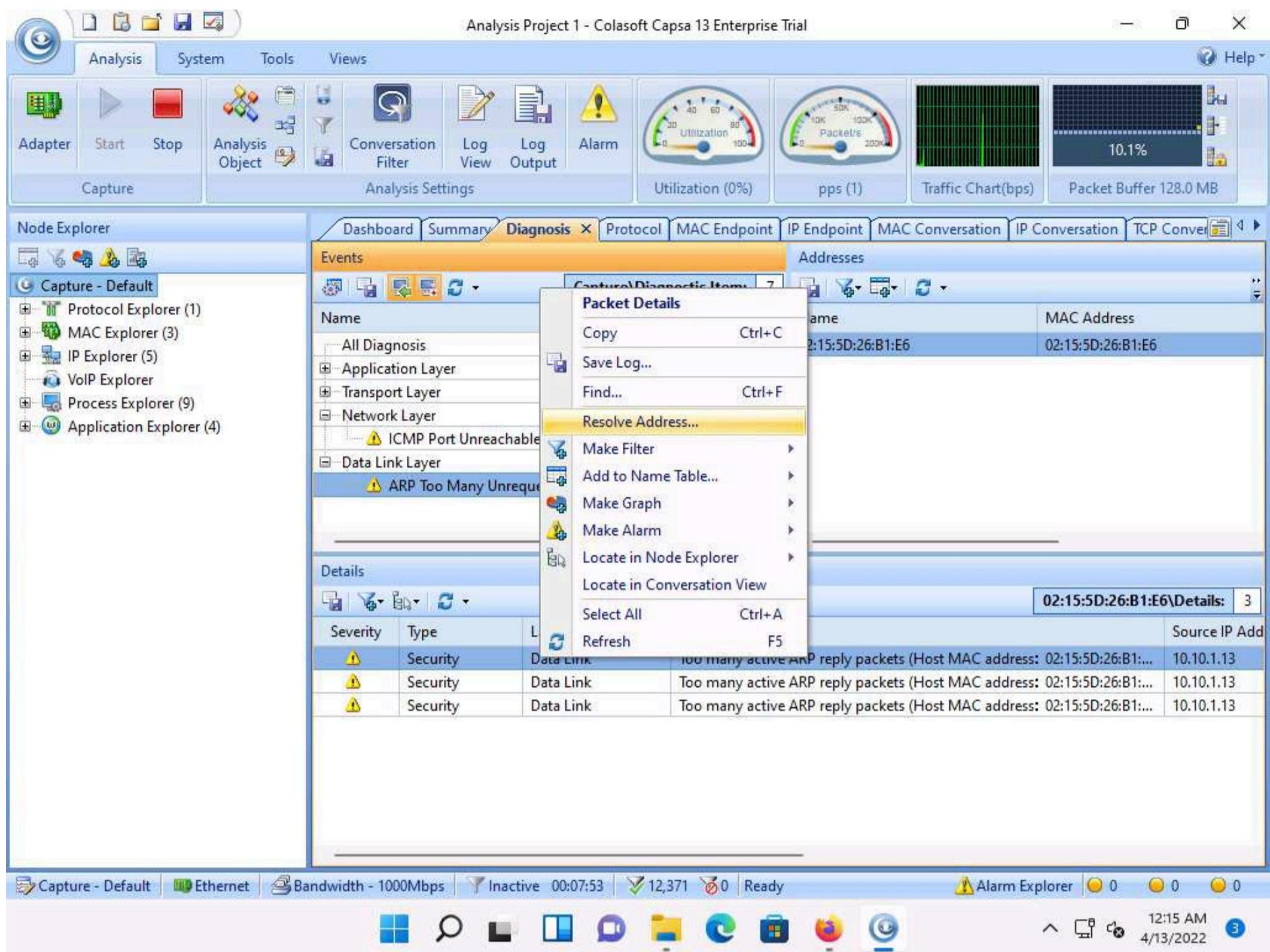
29. In the **Diagnosis** tab, expand the **Data Link Layer** node to see the **ARP Too Many Unrequested Replies** warning.



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**.

Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial

Node Explorer

Capture - Default

Event: Address Resolver

Success: 1, Fail: 1

Address	Name	Status	Name Table Alias
10.10.1.13	-	Failed	-
10.10.1.11	Windows11.local...	Success	

Select All

Severity Add to Name Table Retry OK

Severity	Data Link	Source IP Address
Security	Data Link	Too many active ARP reply packets (Host MAC address: 02:15:5D:26:B1:E6) 10.10.1.13
Security	Data Link	Too many active ARP reply packets (Host MAC address: 02:15:5D:26:B1:E6) 10.10.1.13
Security	Data Link	Too many active ARP reply packets (Host MAC address: 02:15:5D:26:B1:E6) 10.10.1.13
Security	Data Link	Too many active ARP reply packets (Host MAC address: 02:15:5D:26:B1:E6) 10.10.1.13

Capture - Default Ethernet Bandwidth - 1000Mbps Inactive 00:08:23 12,490 0 Ready Alarm Explorer 0 0 0 12:15 AM 4/13/2022

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

Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial

Node Explorer

Capture - Default

Events

Capture\Diagnostic Item: 10

Addresses

All Diagnosis

Name	MAC Address
10.10.1.13	00:15:5D:04:29:C5
Windows11.local	00:15:5D:01:80:00
52.96.69.2	00:15:5D:04:29:C2
40.97.228.178	00:15:5D:04:29:C2
40.97.152.18	00:15:5D:04:29:C2
windows.msn.com	00:15:5D:04:29:C2
40.97.152.82	00:15:5D:04:29:C2
34.117.237.239	00:15:5D:04:29:C2
...	...

Details

10.10.1.13\Details: 6

Severity	Type	Layer	Event Summary	Source IP Address
Fault	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:4832).	10.10.1.13
Fault	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:4837).	10.10.1.13
Fault	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:4843).	10.10.1.13
Fault	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:5068).	10.10.1.13
Fault	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:5089).	10.10.1.13
Fault	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:5095).	10.10.1.13

Capture - Default Ethernet Bandwidth - 1000Mbps Inactive 00:25:56 5,534 0 Ready Alarm Explorer 0 0 0 12:24 AM 4/13/2022

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.

The screenshot shows the CyberQ interface with the Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial window open. The Diagnosis tab is selected. In the Node Explorer, a local subnet is selected, showing hosts 10.10.1.19, 10.10.1.22, 10.10.1.14, 10.10.1.255, and 10.10.1.13. The Diagnosis tab displays a list of events under the Network Layer, specifically ICMP Port Unreachable errors. The Details pane provides a detailed view of these six events, each with a severity of Fault, type of Network, and source IP of 10.10.1.13. The bottom status bar shows a bandwidth of 1000Mbps and a packet count of 6,814.

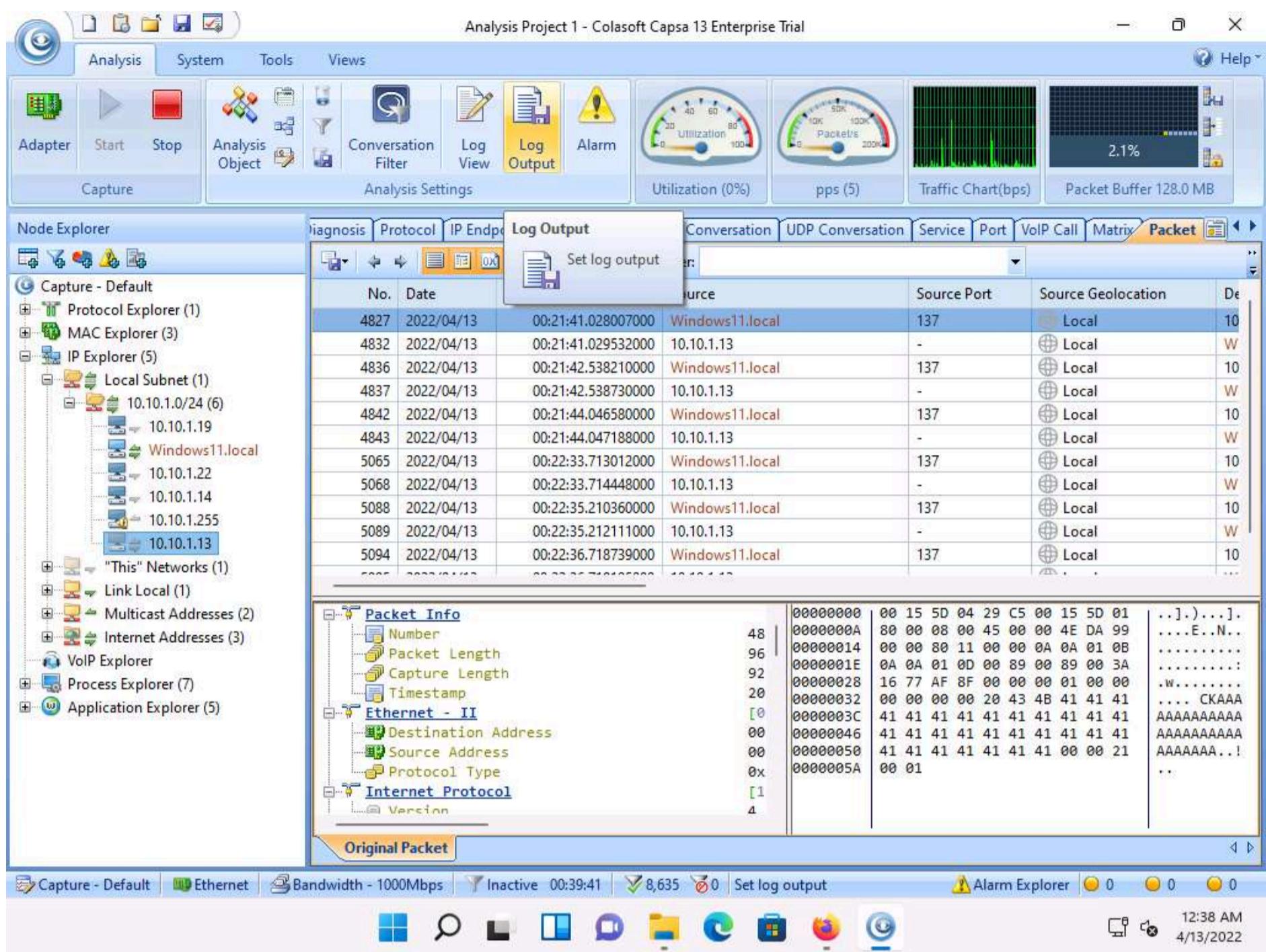
45. Now click on **Packet** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window, to check the packets transferred by the **Parrot Security** machine.

The screenshot shows the CyberQ interface with the Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial window open. The Packet tab is selected. In the Node Explorer, a local subnet is selected, showing hosts 10.10.1.19, 10.10.1.22, 10.10.1.14, 10.10.1.255, and 10.10.1.13. The Packet tab displays a list of captured packets, with the first few rows shown in the table below. The bottom status bar shows a bandwidth of 1000Mbps and a packet count of 7,370.

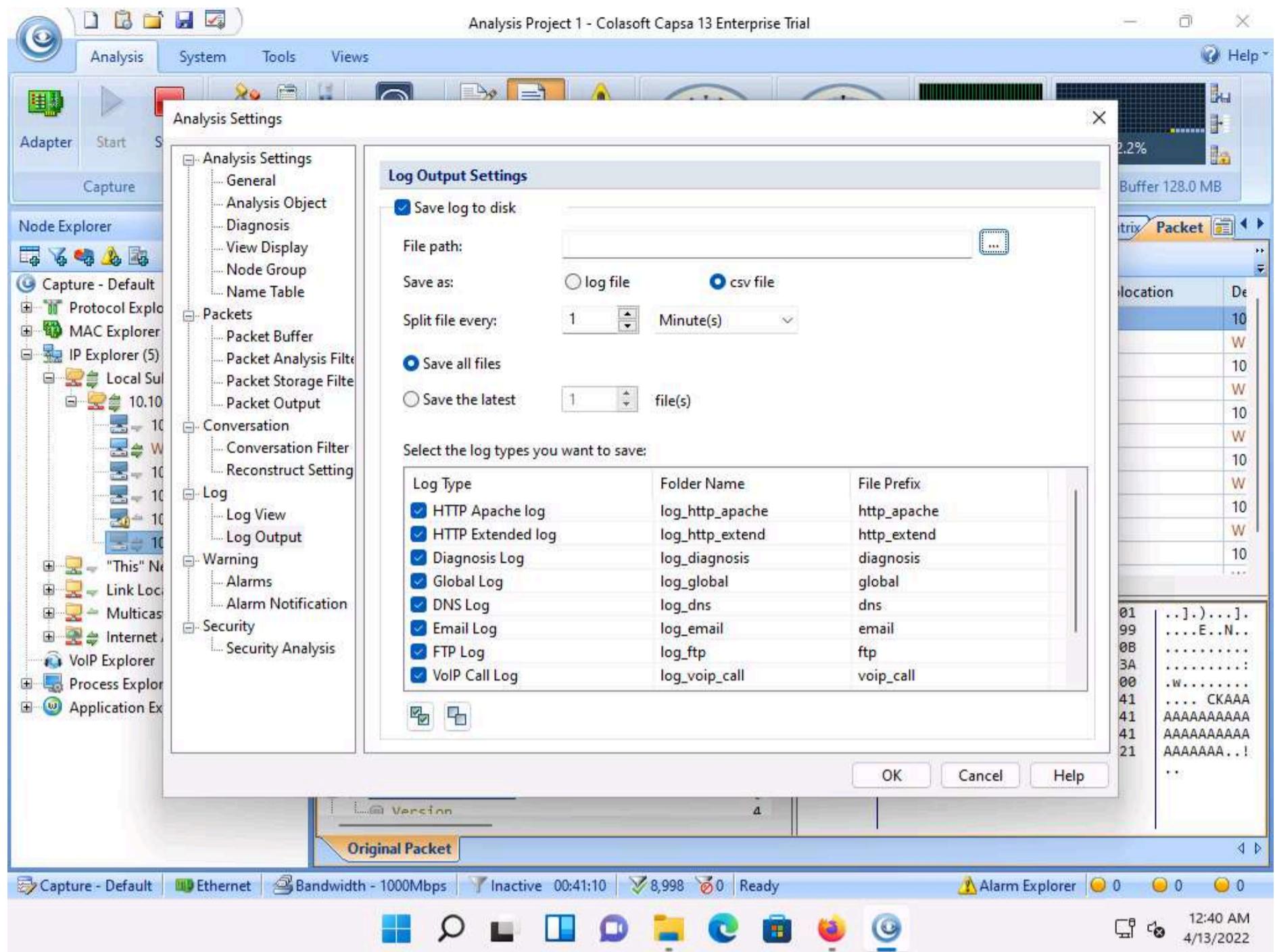
No.	Date	Absolute Time	Source	Source Port	Source Geolocation	Dest
4827	2022/04/13	00:21:41.028007000	Windows11.local	137	Local	10.10.1.13
4832	2022/04/13	00:21:41.029532000	10.10.1.13	-	Local	W
4836	2022/04/13	00:21:42.538210000	Windows11.local	137	Local	10.10.1.13
4837	2022/04/13	00:21:42.538730000	10.10.1.13	-	Local	W
4842	2022/04/13	00:21:44.046580000	Windows11.local	137	Local	10.10.1.13
4843	2022/04/13	00:21:44.047188000	10.10.1.13	-	Local	W
5065	2022/04/13	00:22:33.713012000	Windows11.local	137	Local	10.10.1.13
5068	2022/04/13	00:22:33.714448000	10.10.1.13	-	Local	W
5088	2022/04/13	00:22:35.210360000	Windows11.local	137	Local	10.10.1.13
5089	2022/04/13	00:22:35.212111000	10.10.1.13	-	Local	W
5094	2022/04/13	00:22:36.718739000	Windows11.local	137	Local	10.10.1.13

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

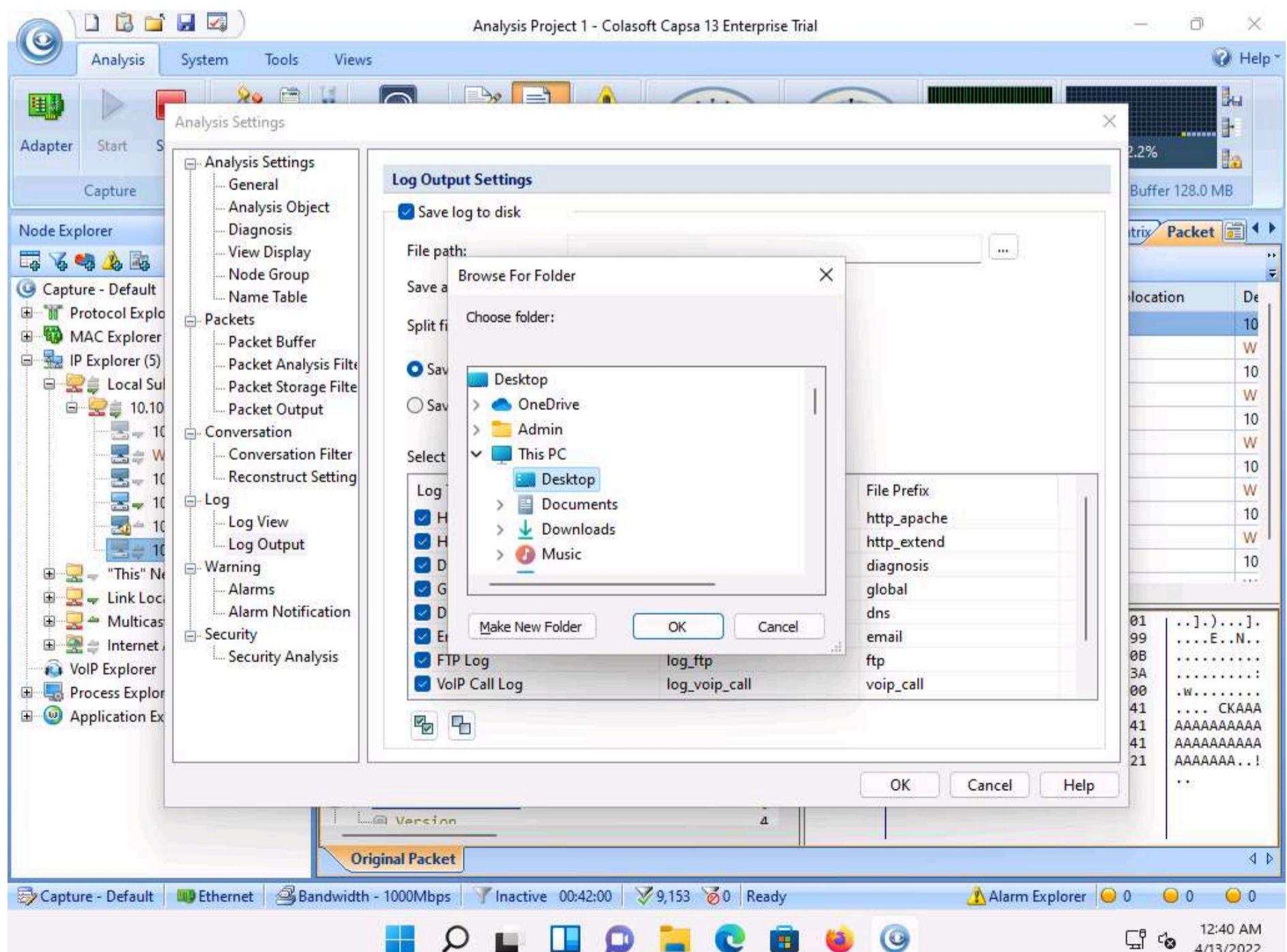
47. After completing the analysis click on **Log Output** option from the menubar.



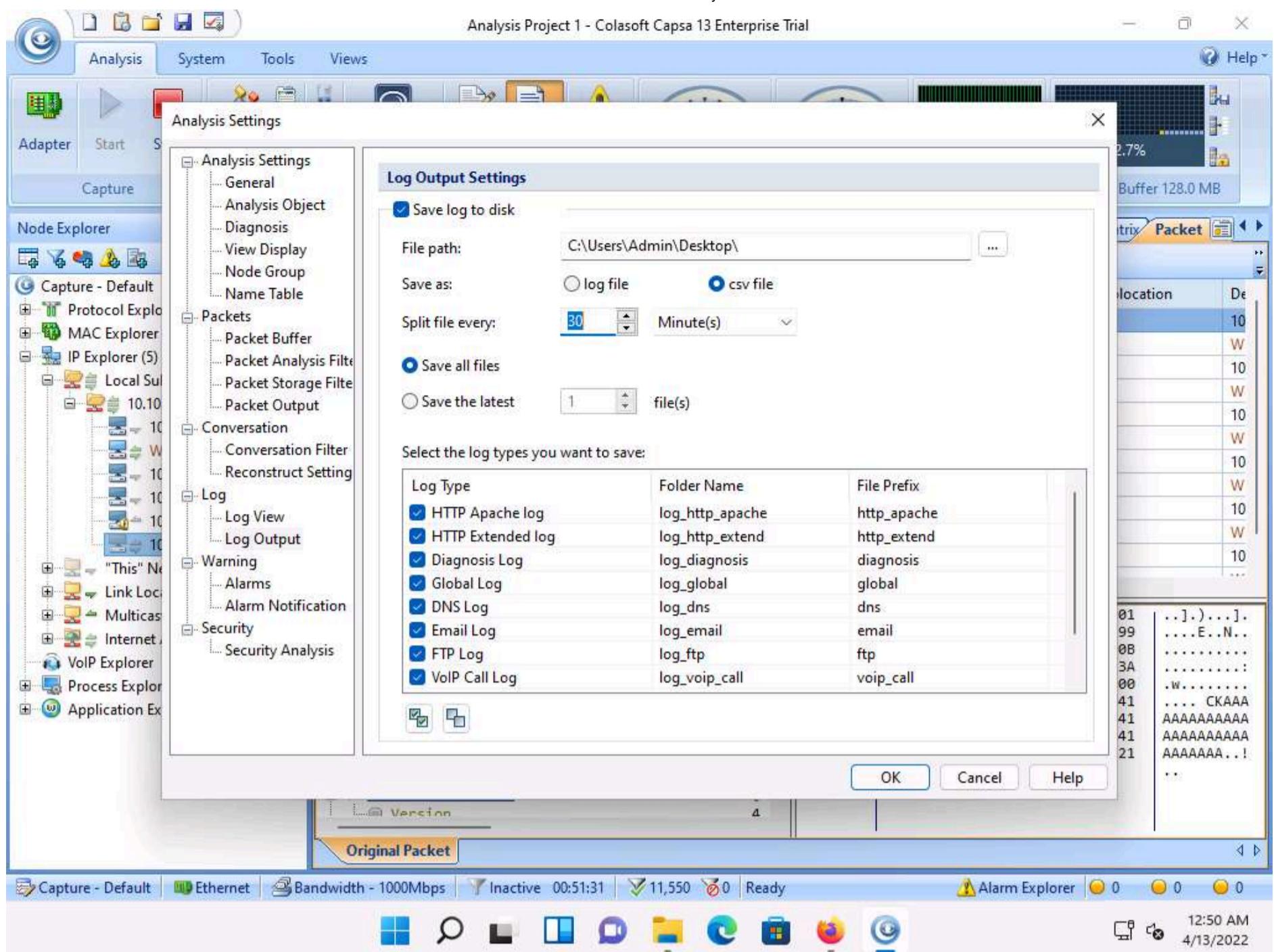
48. In the **Analysis Settings** window, check the **Save log to disk** checkbox and click the ellipsis button under **File path** option.



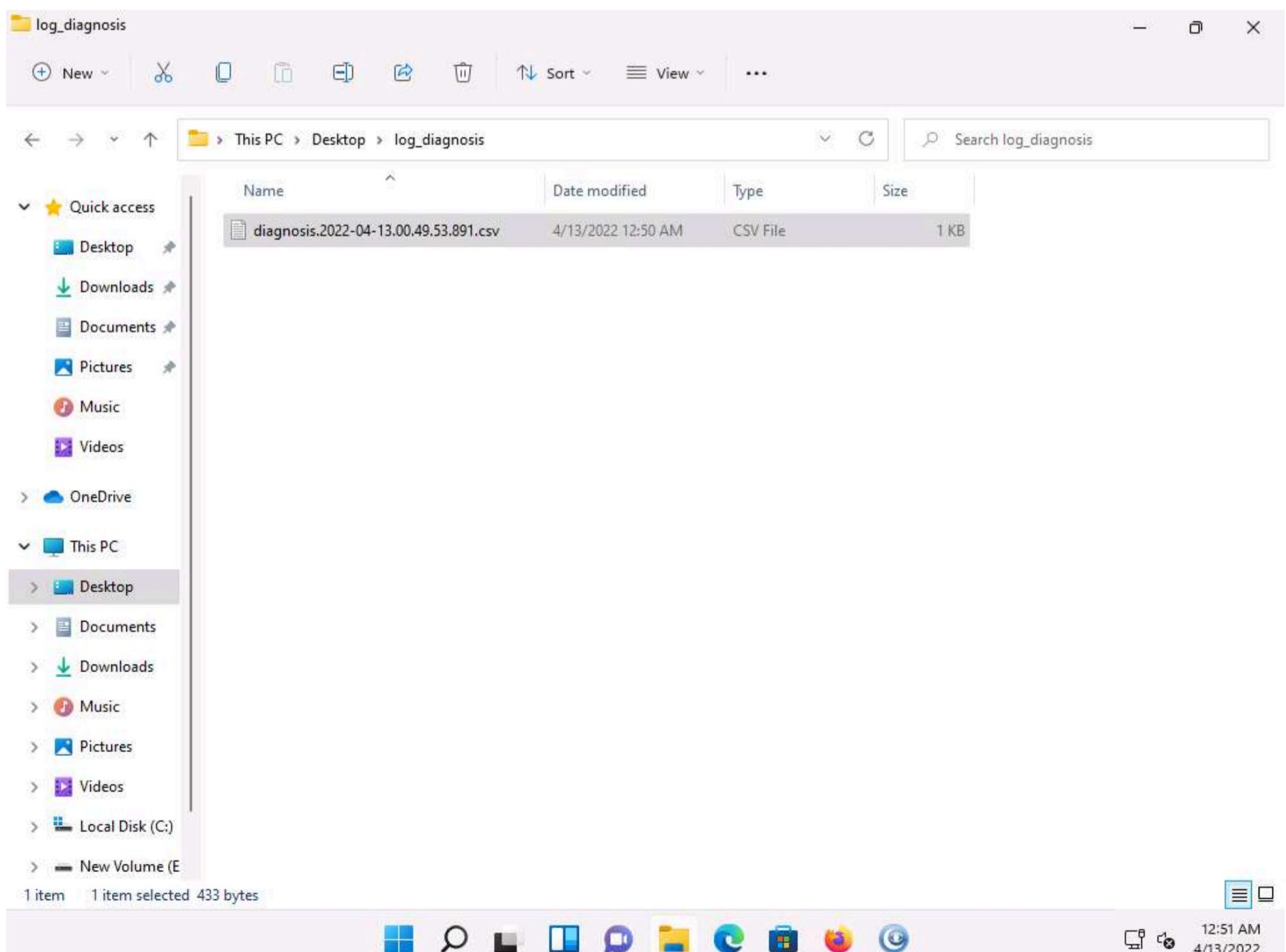
49. In the **Browse For Folder** window, select **Desktop** and click on **OK**.



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.

