

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.

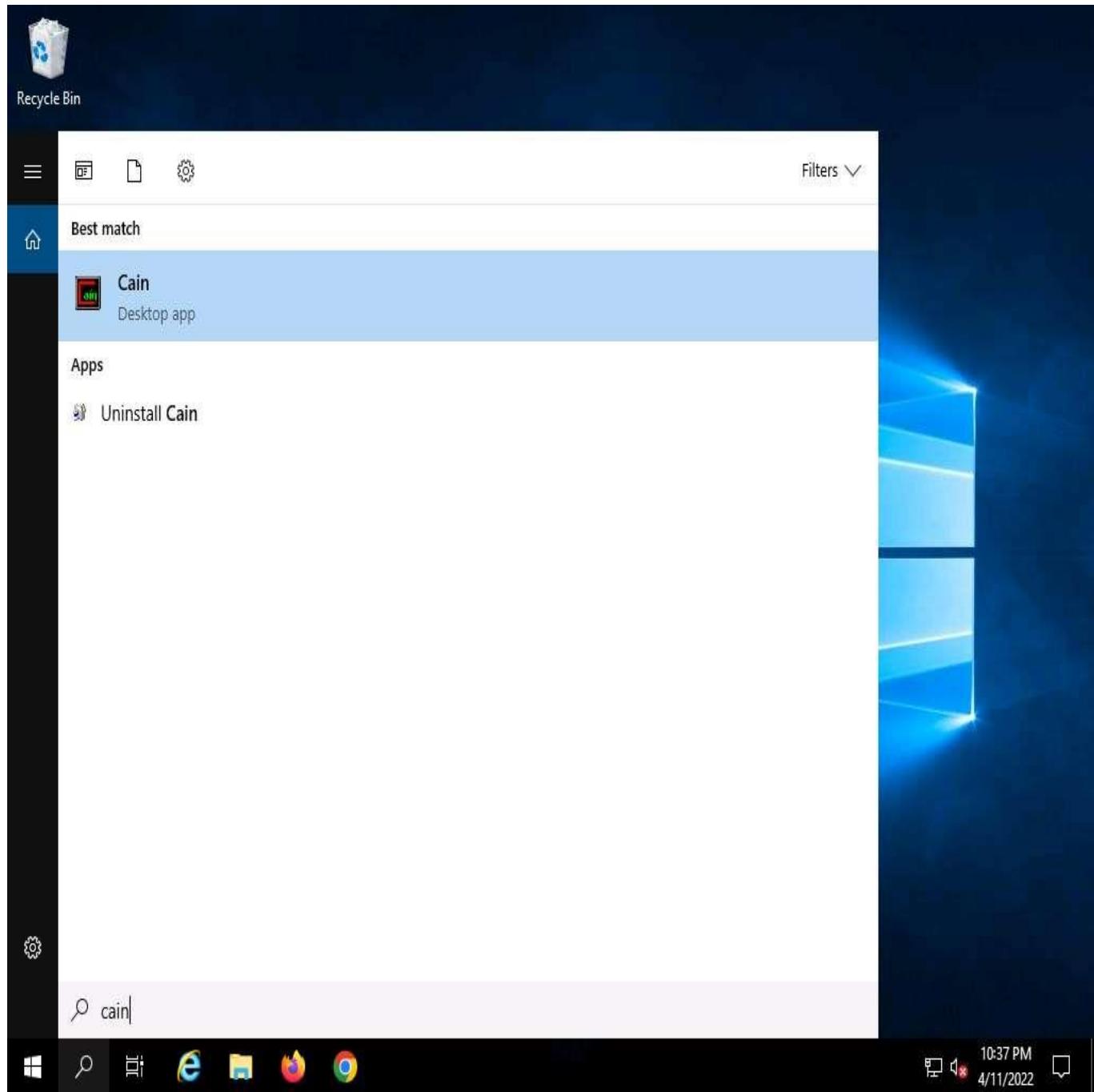
The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

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.

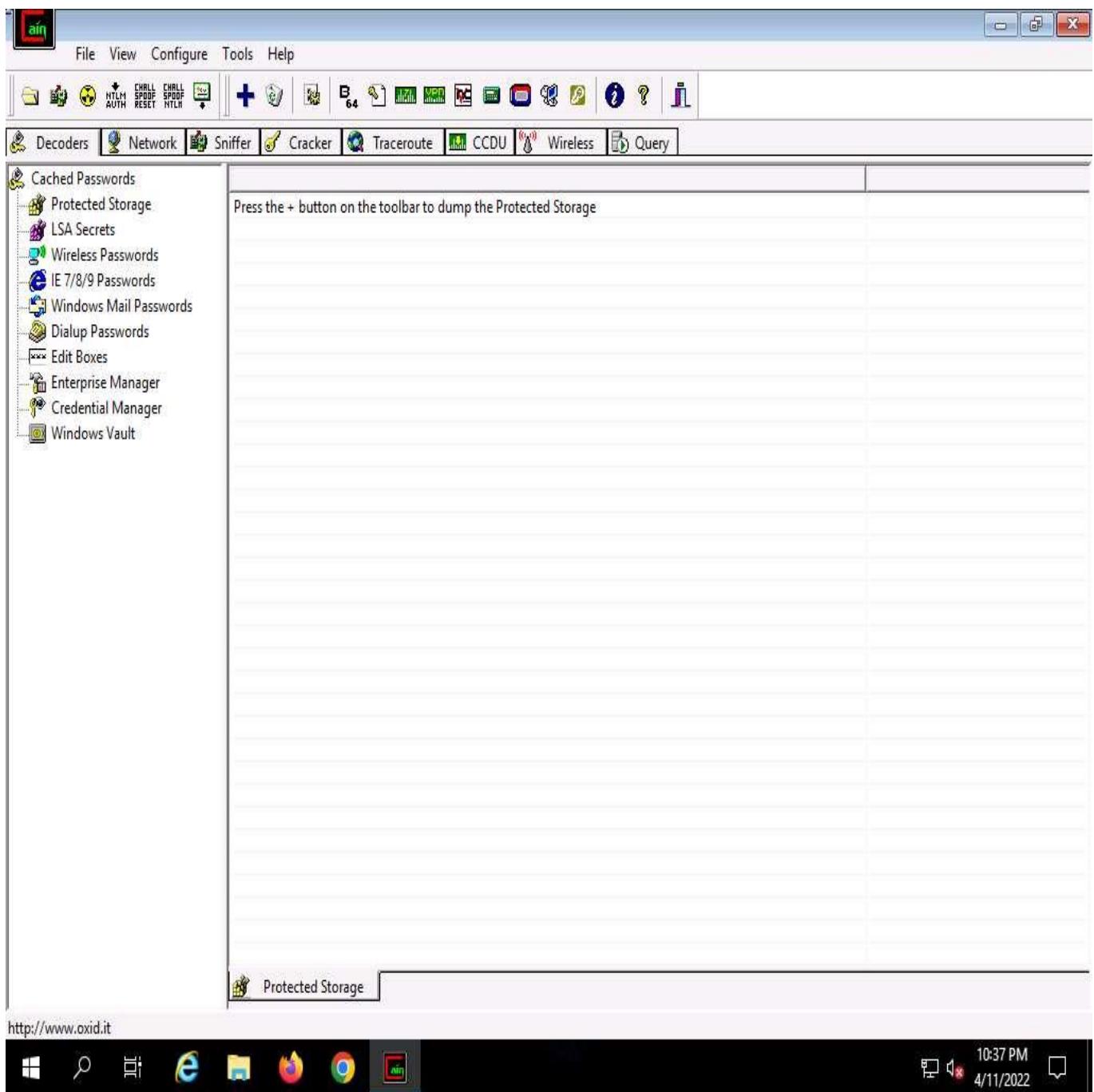
In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 11** and **Parrot Security** machines. We will use the same machine

(Windows Server 2019) to detect ARP poisoning and use the Windows 11 machine to detect promiscuous mode in the network.

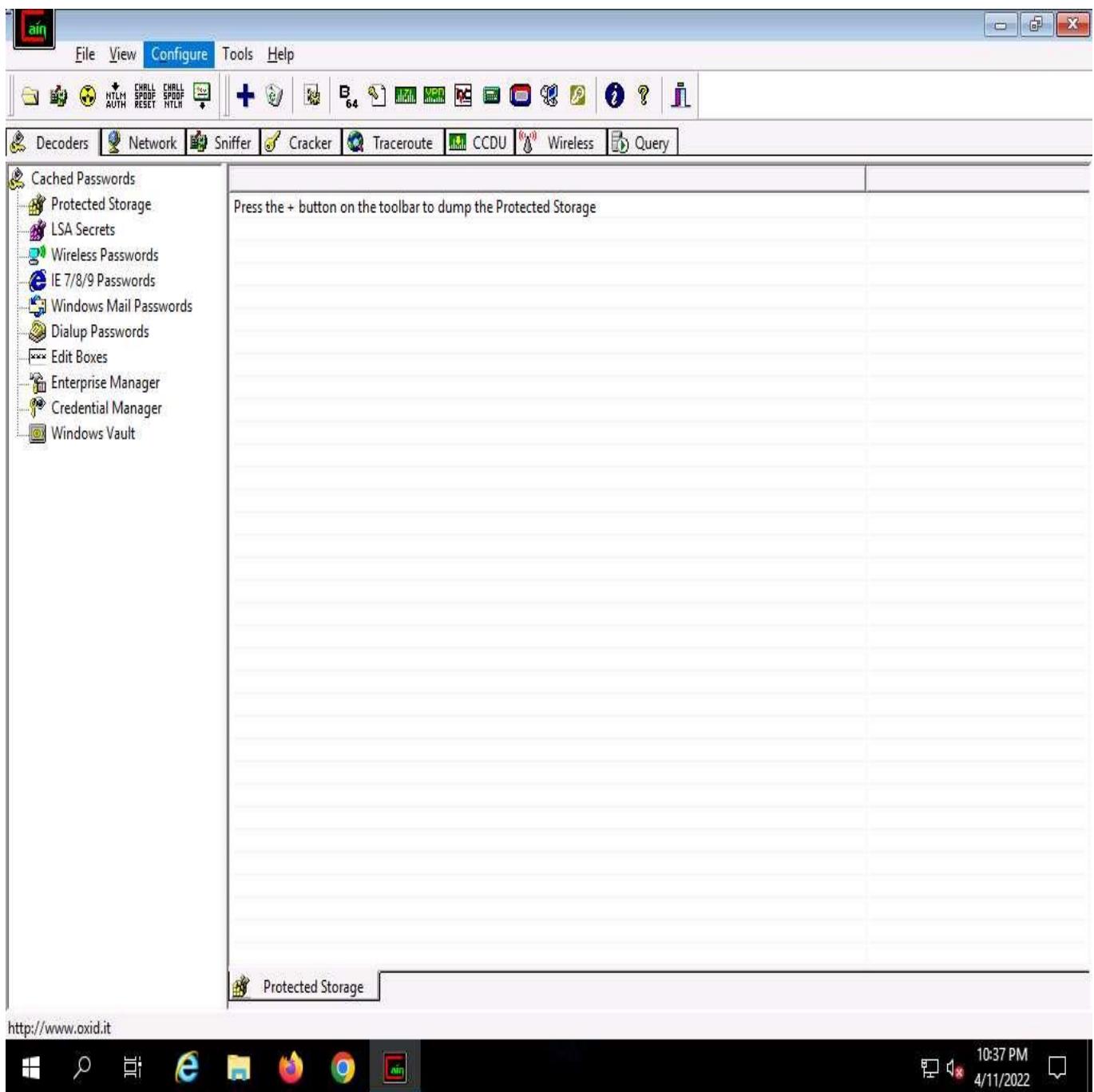
1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine.
2. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



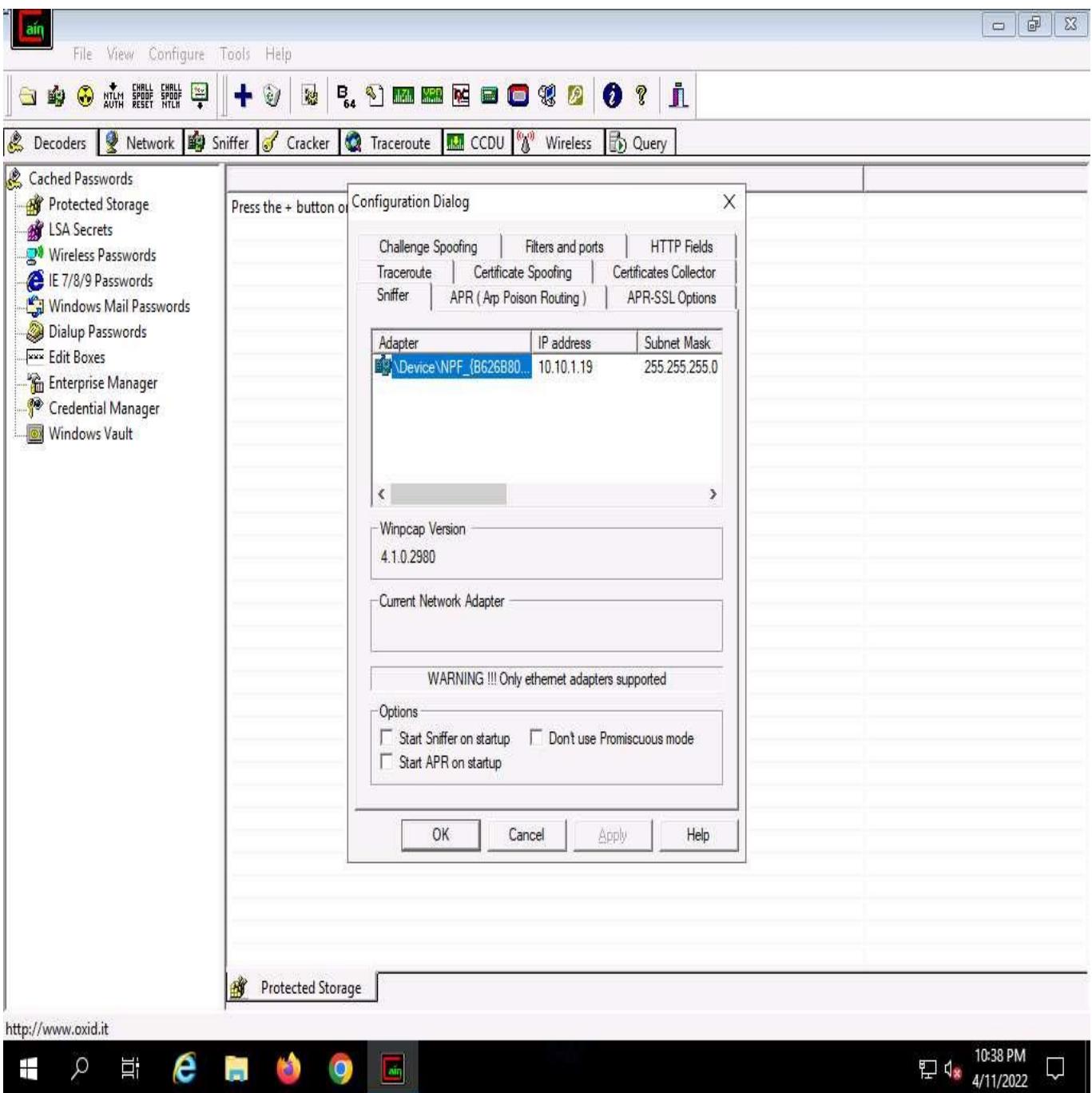
3. The **Cain & Abel** main window appears, as shown in the screenshot.



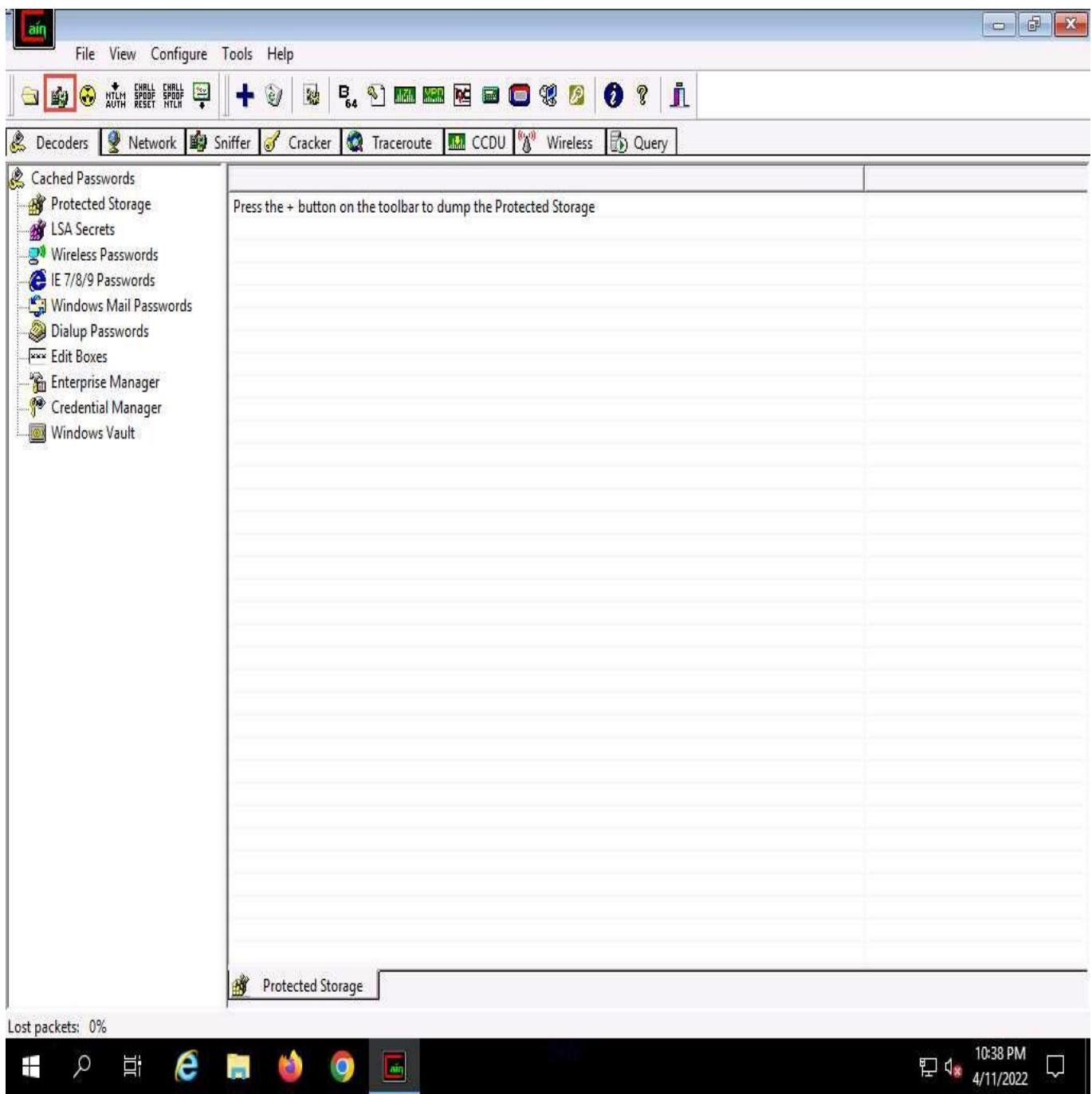
4. Click **Configure** from the menu bar to configure an ethernet card.



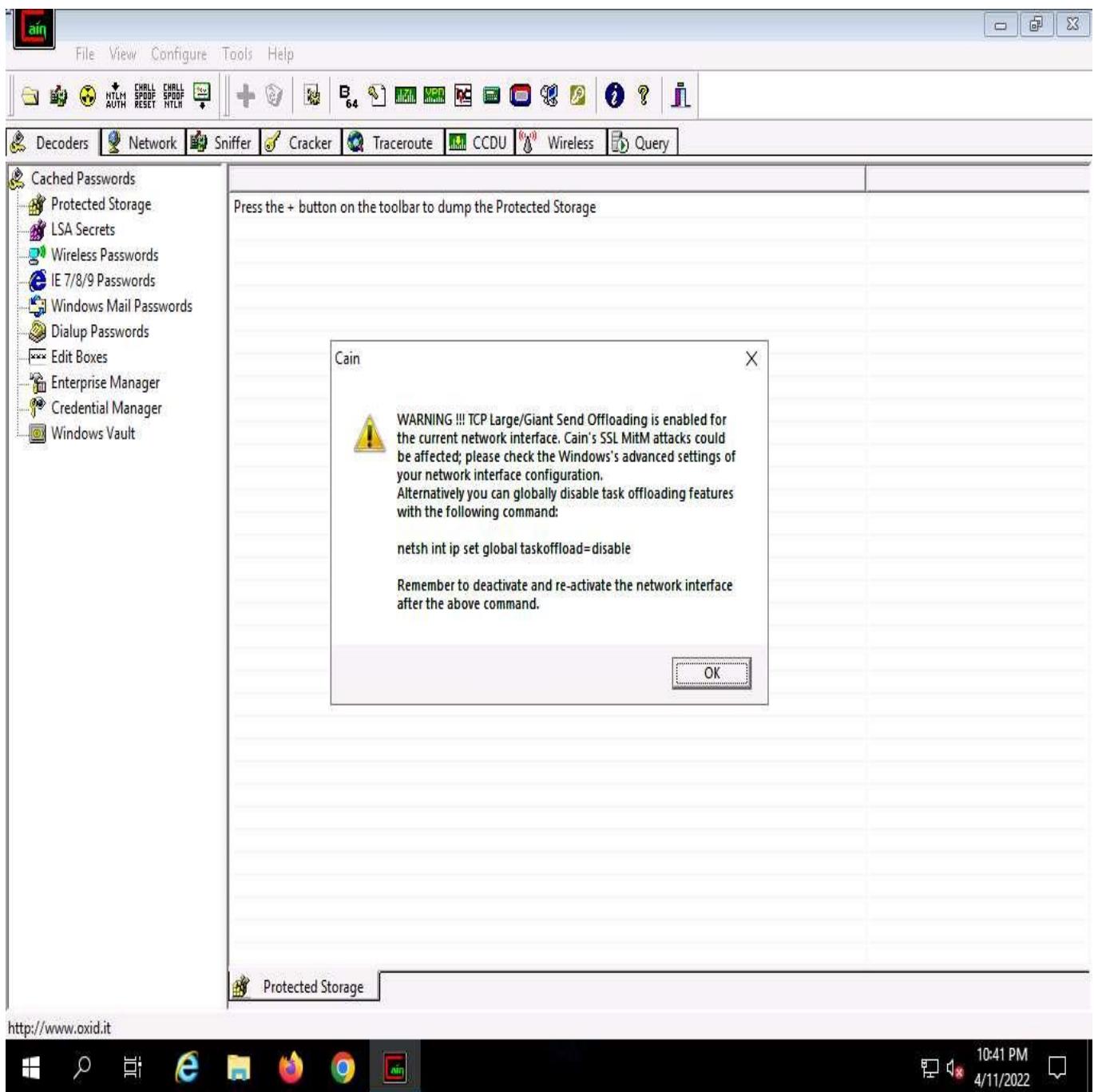
5. The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.



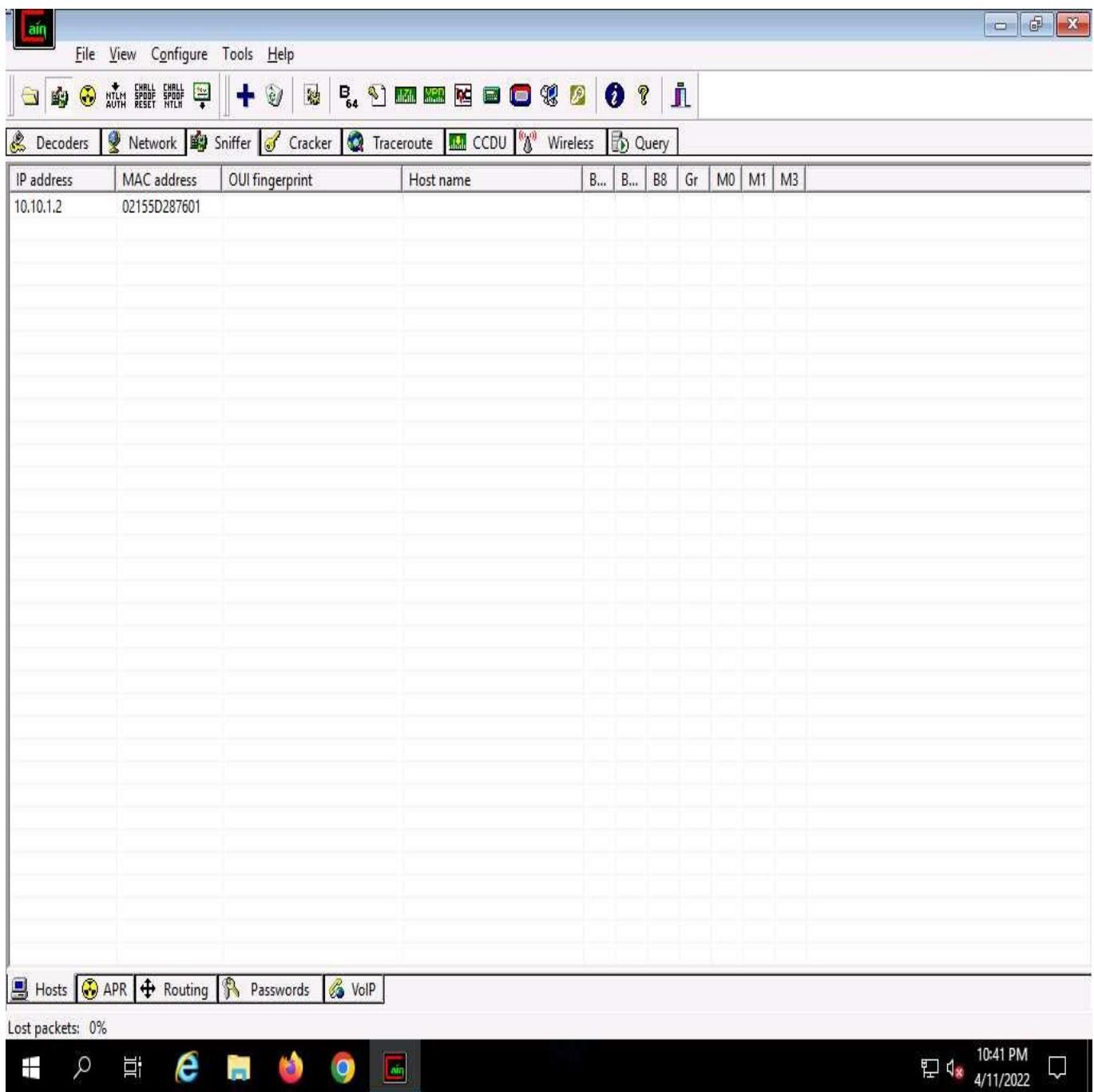
6. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



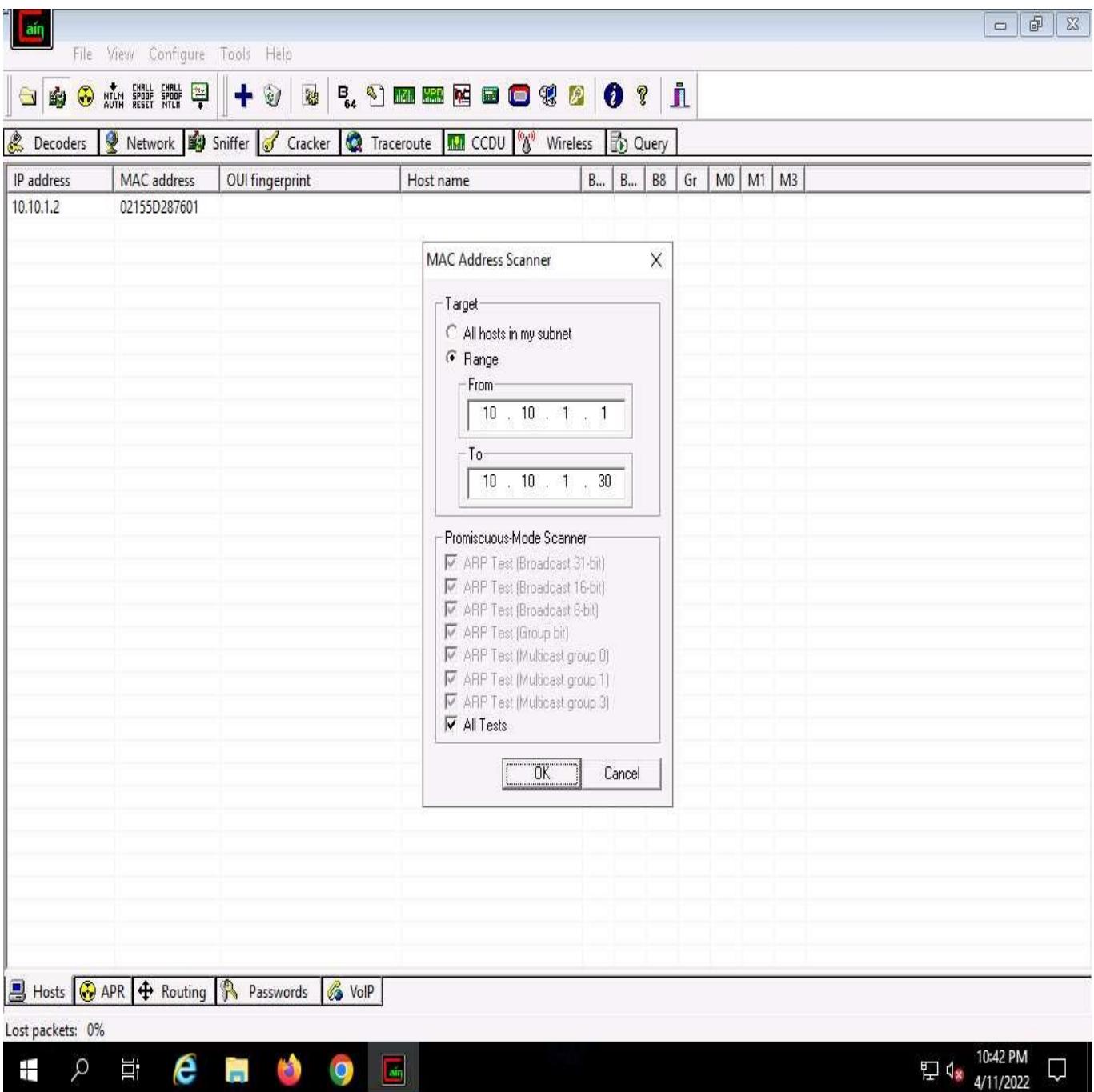
7. The **Cain** pop-up appears with a **Warning** message, click **OK**.



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



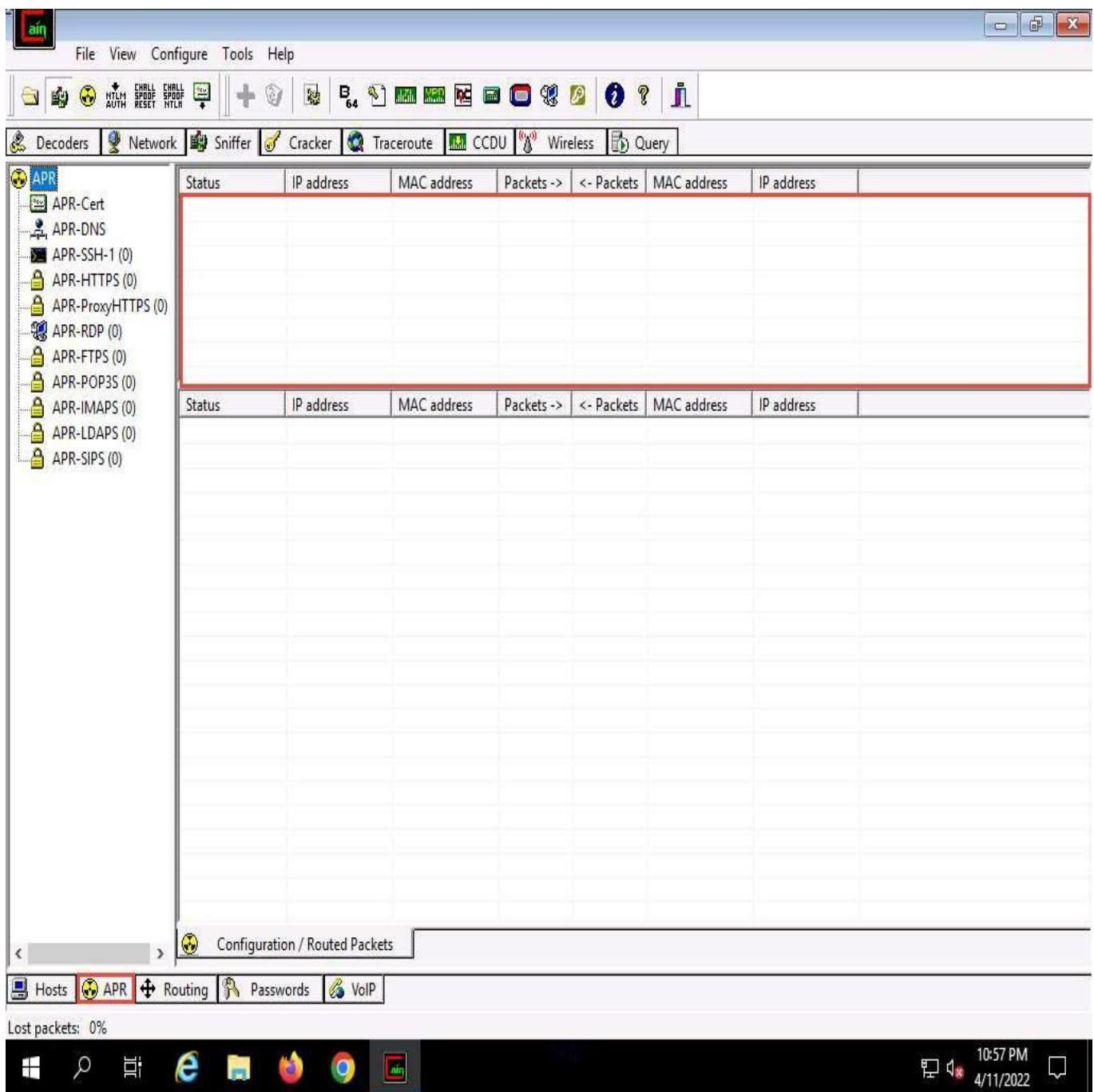
9. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
10. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.1.1-10.10.1.30**. Select the **All Tests** checkbox; then, click **OK**.



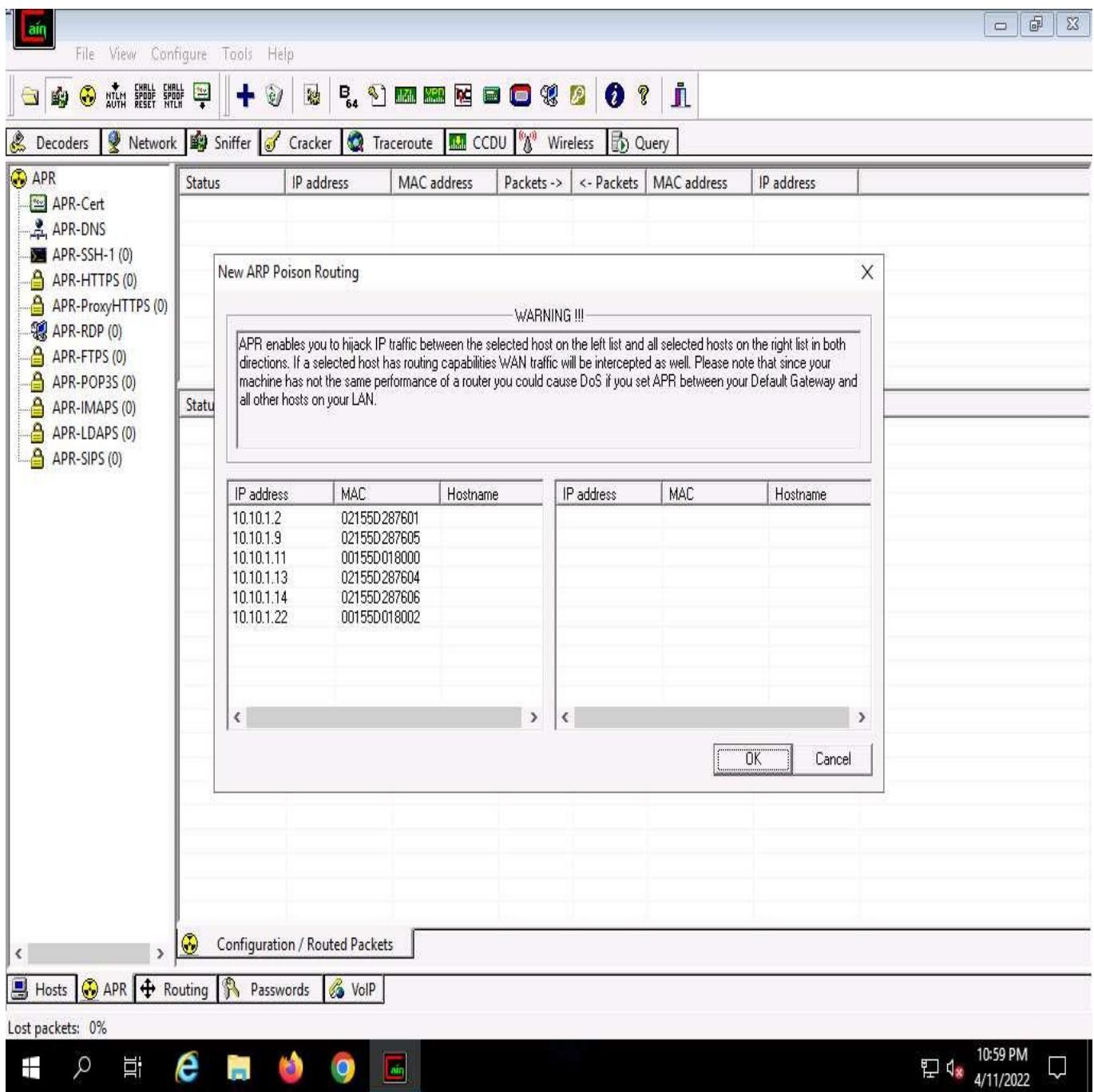
11. Cain & Abel starts scanning for MAC addresses and lists all those found.
12. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

The screenshot shows the Cain & Abel network analysis tool. The main window displays a table of network hosts with columns for IP address, MAC address, OUI fingerprint, Host name, and various wireless parameters (B1, B2, B8, Gr, M0, M1, M3). Several hosts are listed, mostly with Microsoft Corporation as the manufacturer. Below the table is a large, empty white area. At the bottom of the interface, there is a navigation bar with tabs for Hosts, APR, Routing, Passwords, and VoIP. The taskbar at the bottom of the screen shows several open application icons, including Windows File Explorer, a search icon, Task View, Internet Explorer, FileZilla, Mozilla Firefox, Google Chrome, and the Cain & Abel icon. The system tray shows the date and time as 10:48 PM on 4/11/2022.

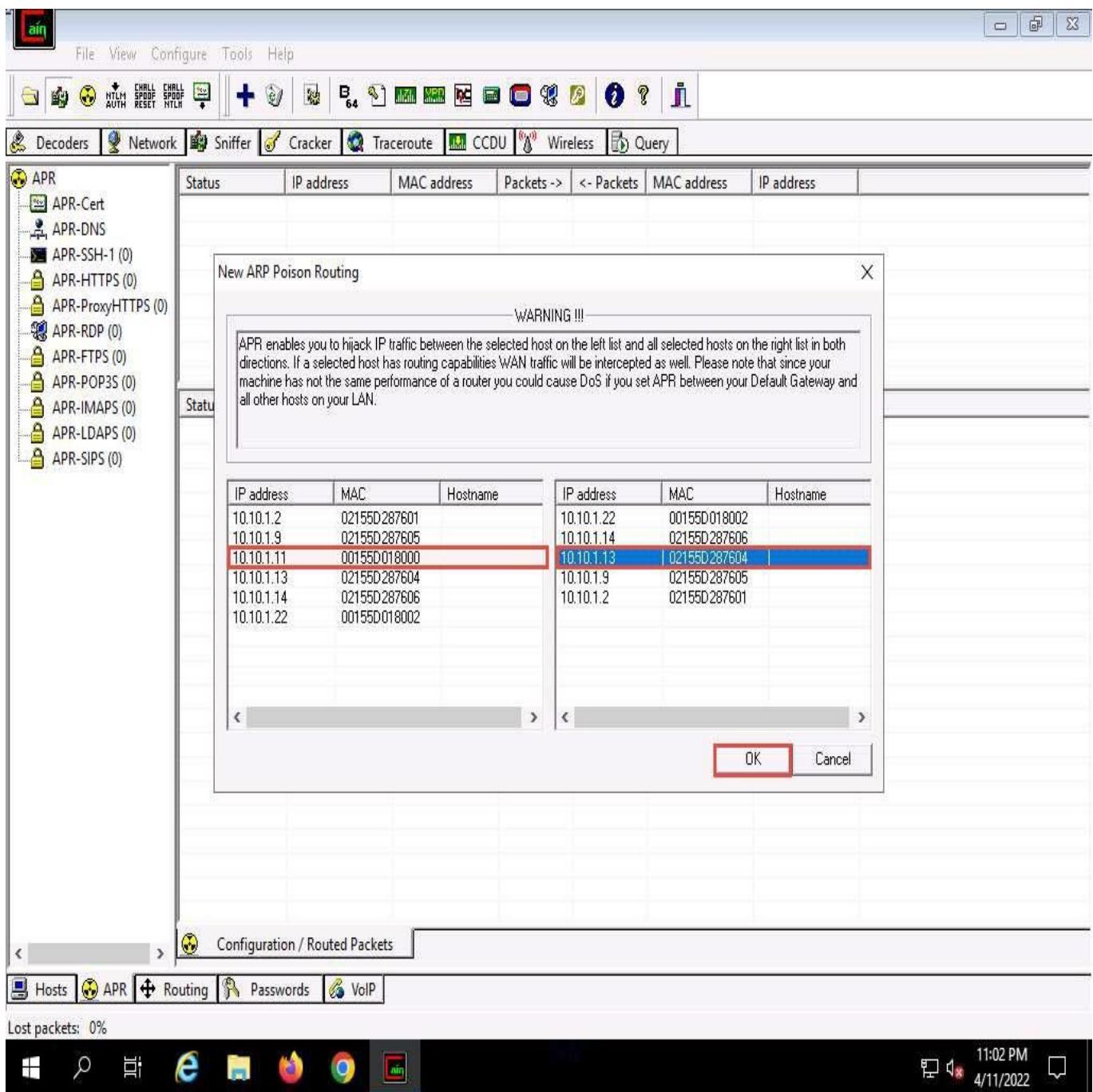
13. Now, click the **APR** tab at the bottom of the window.
14. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.



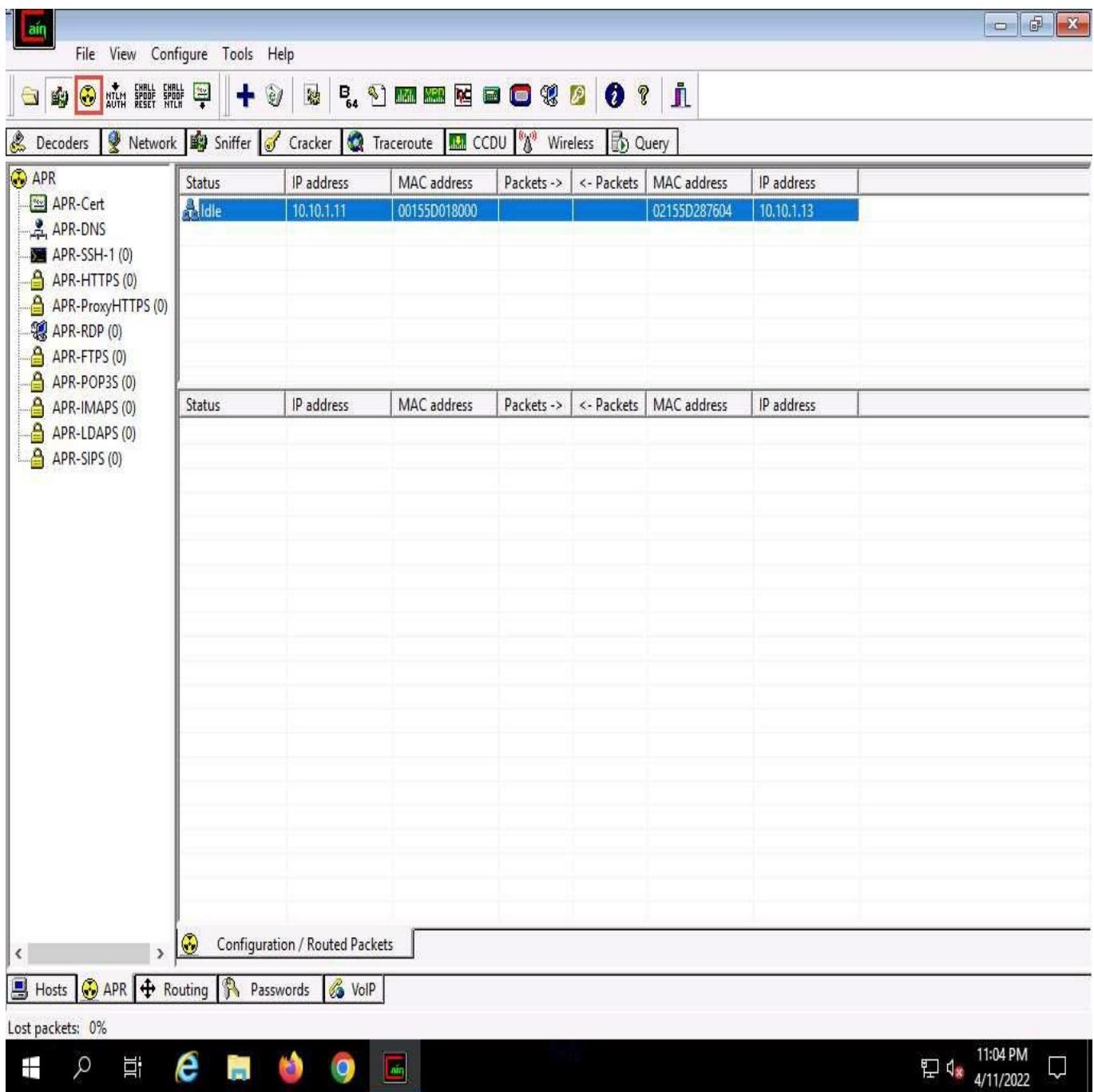
15. Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.



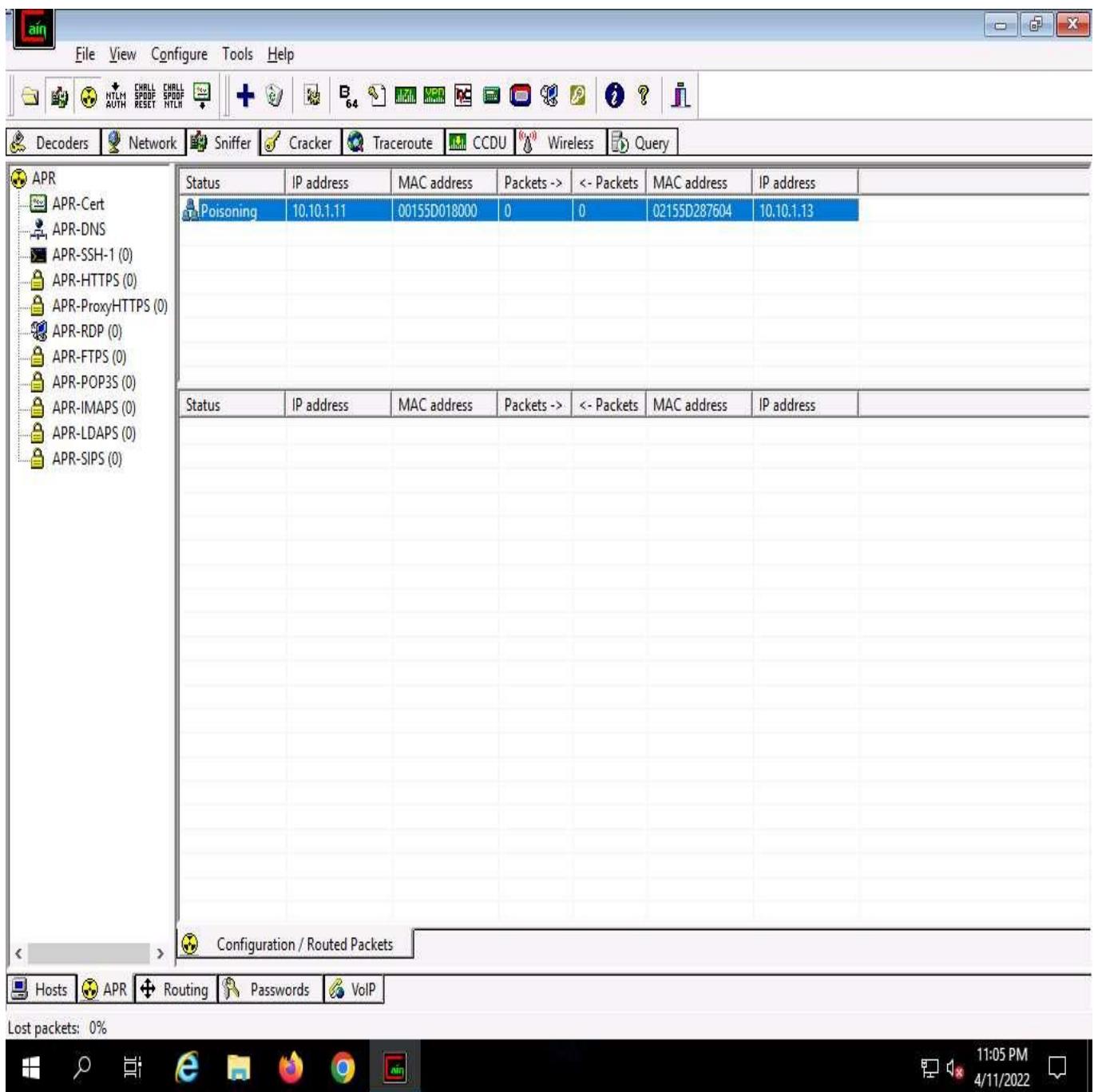
16. To monitor the traffic between two systems (here, **Windows 11** and **Parrot Security**), from the left-hand pane, click to select **10.10.1.11 (Windows 11)** and from the right-hand pane, click **10.10.1.13 (Parrot Security)**; click **OK**. By doing so, you are setting Cain to perform ARP poisoning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



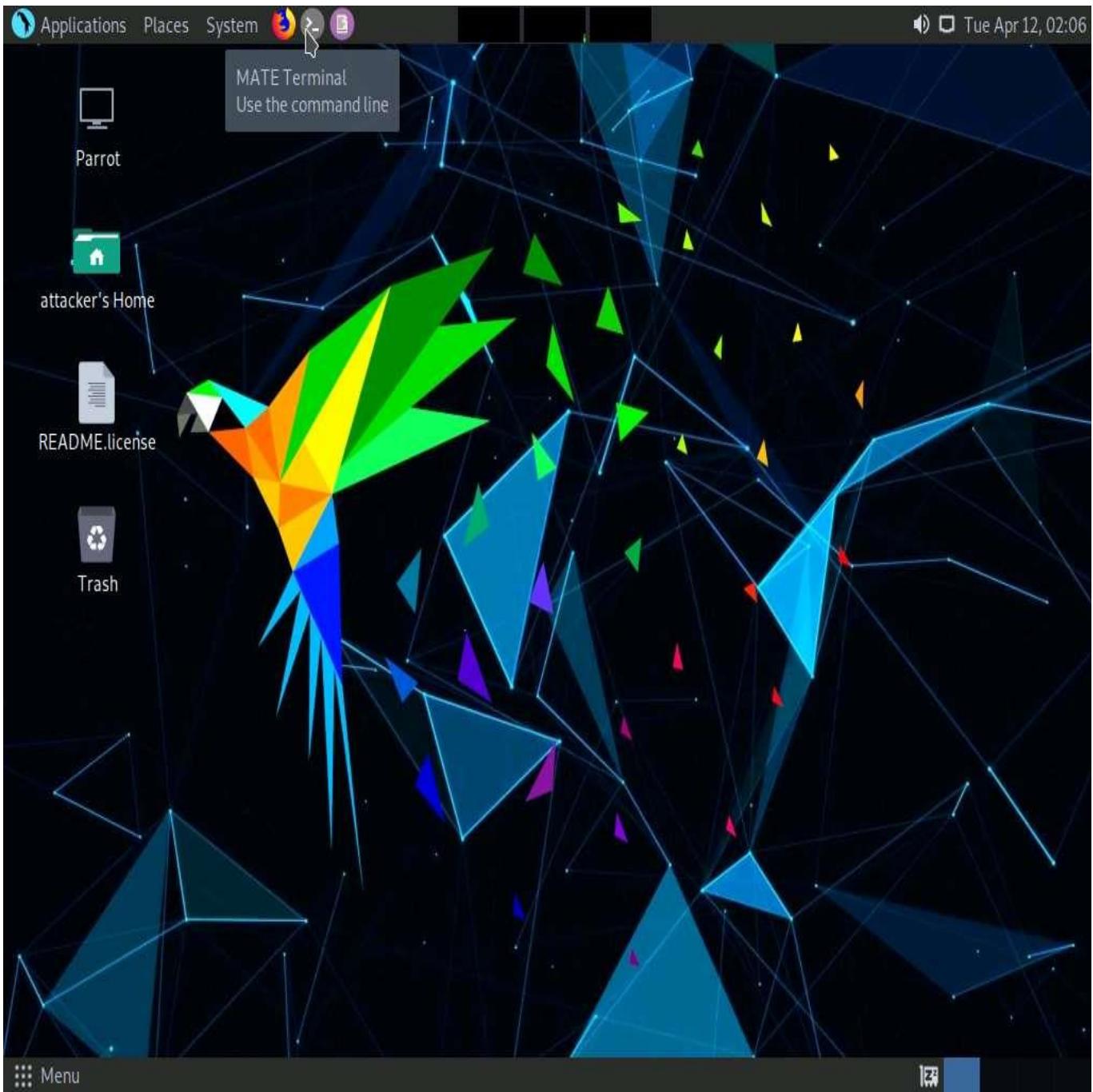
17. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.
18. Click on the **Start/Stop APR** icon to start capturing ARP packets.



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.



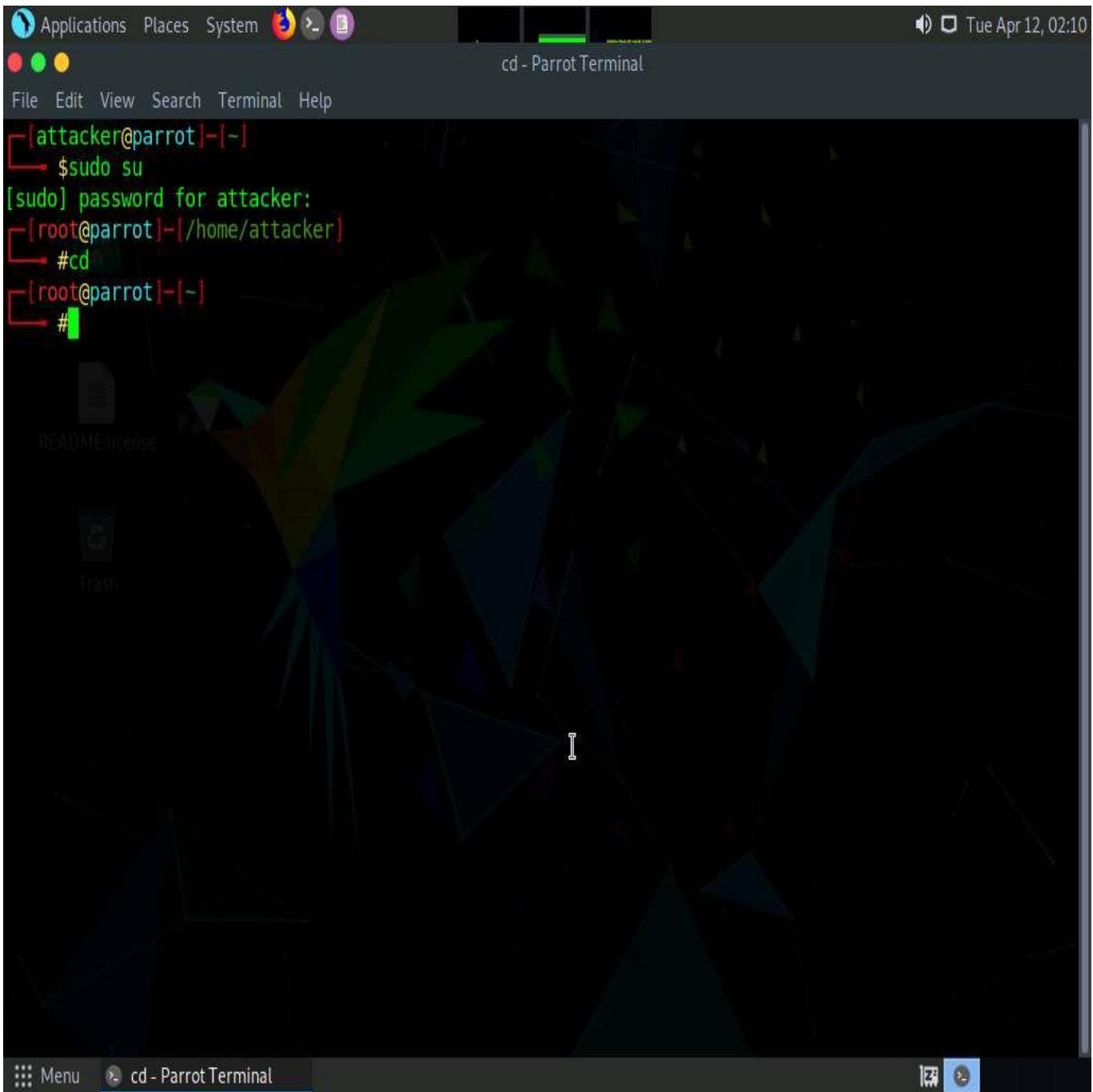
20. Cain & Abel intercepts the traffic traversing between these two machines.
21. To generate traffic between the machines, you need to ping one target machine using the other.
22. Click **Parrot Security** to switch to the **Parrot Security** machine.
23. Click the **MATE Terminal** icon at the top 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**.

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**.

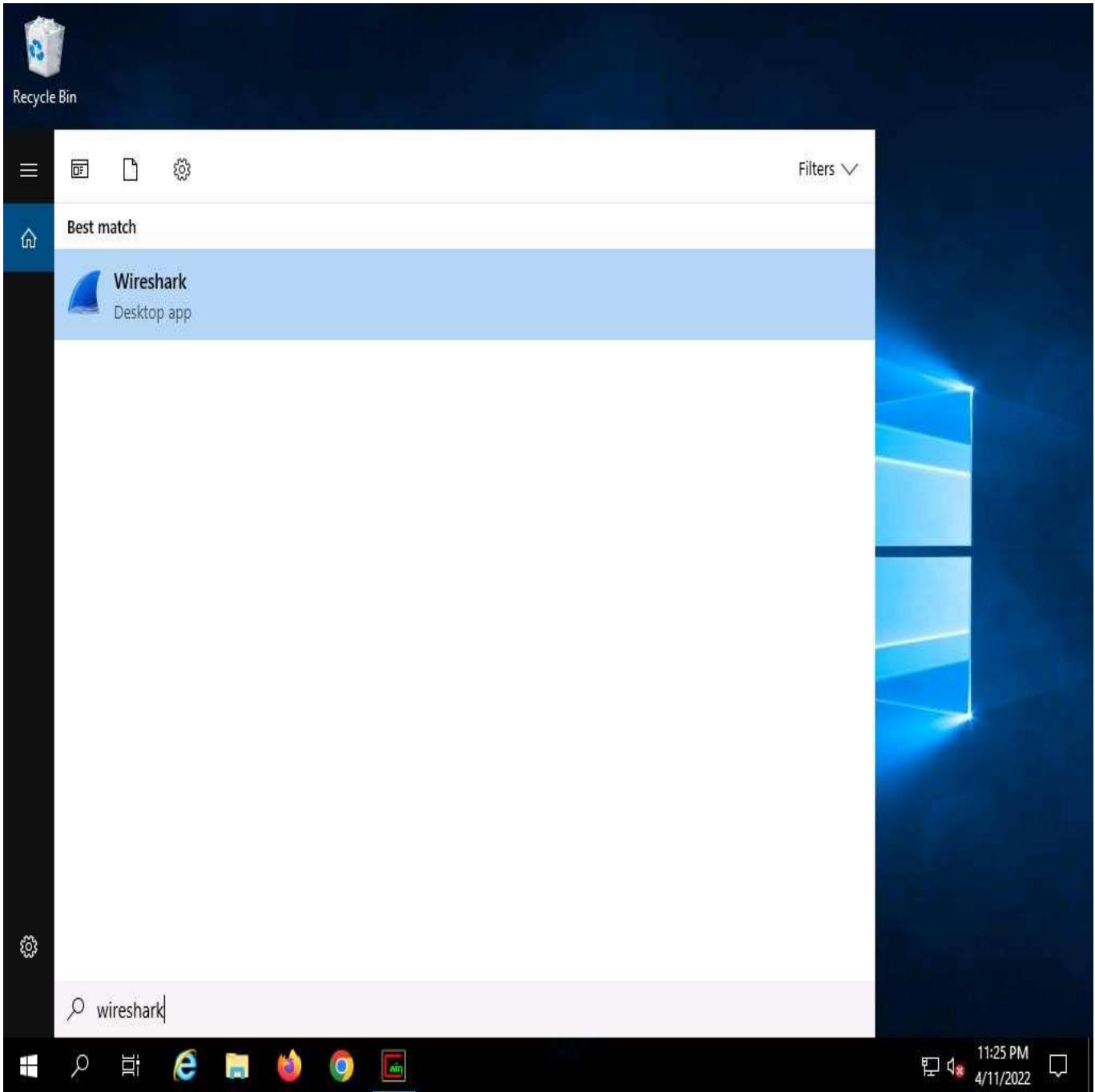
-c: specifies the packet count.

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

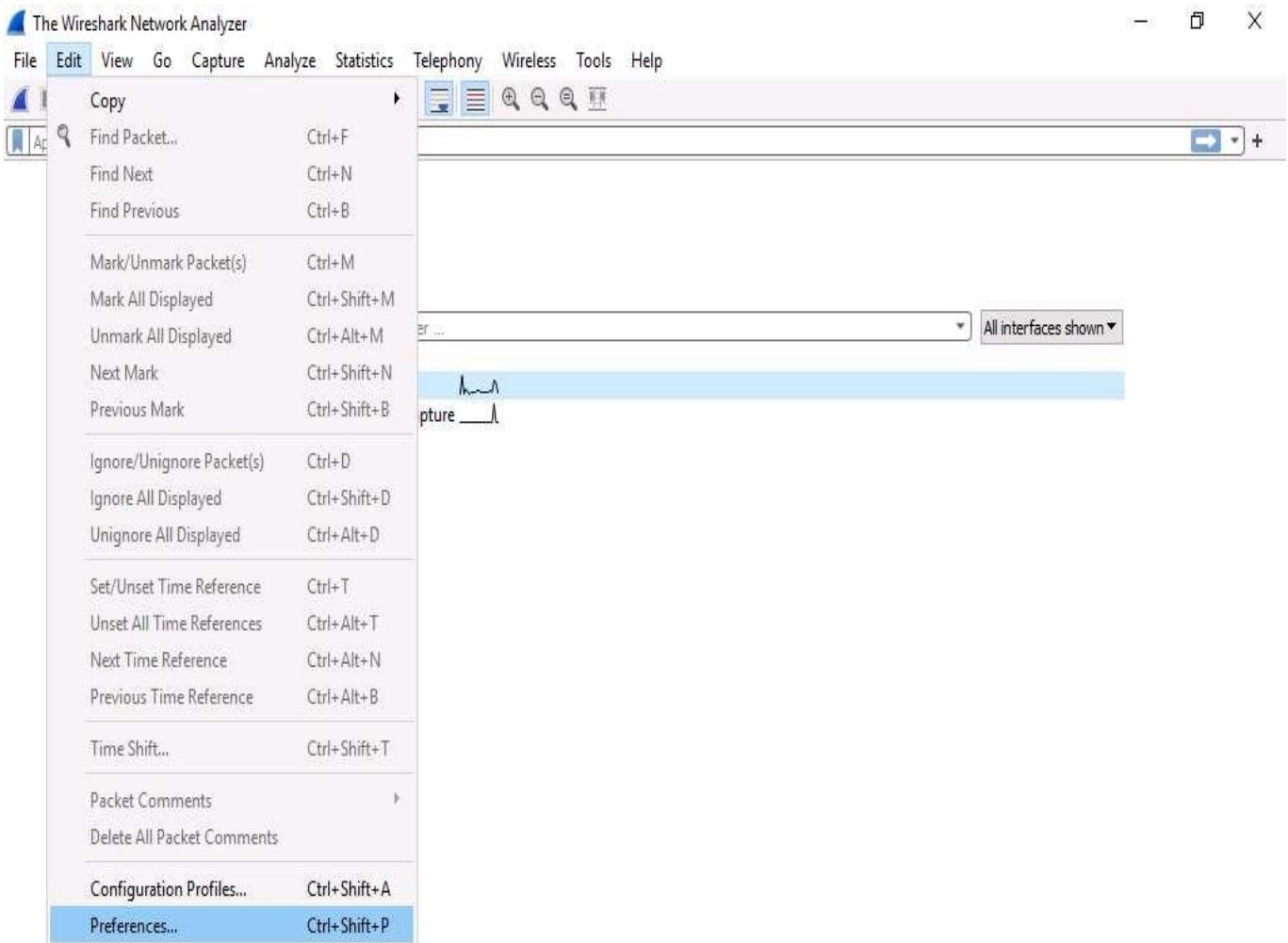
The screenshot shows a terminal window titled "hping3 10.10.1.11 -c 100000 - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command entered was "#hping3 10.10.1.11 -c 100000". The output shows 16 ICMP echo requests (RA) being sent to the target IP address. Each packet has a length of 40 bytes, DF set, TTL of 128, and a sequence number (seq) from 0 to 15. The round-trip time (RTT) for each packet ranges from 2.2 ms to 10.0 ms.

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# 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 **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....**



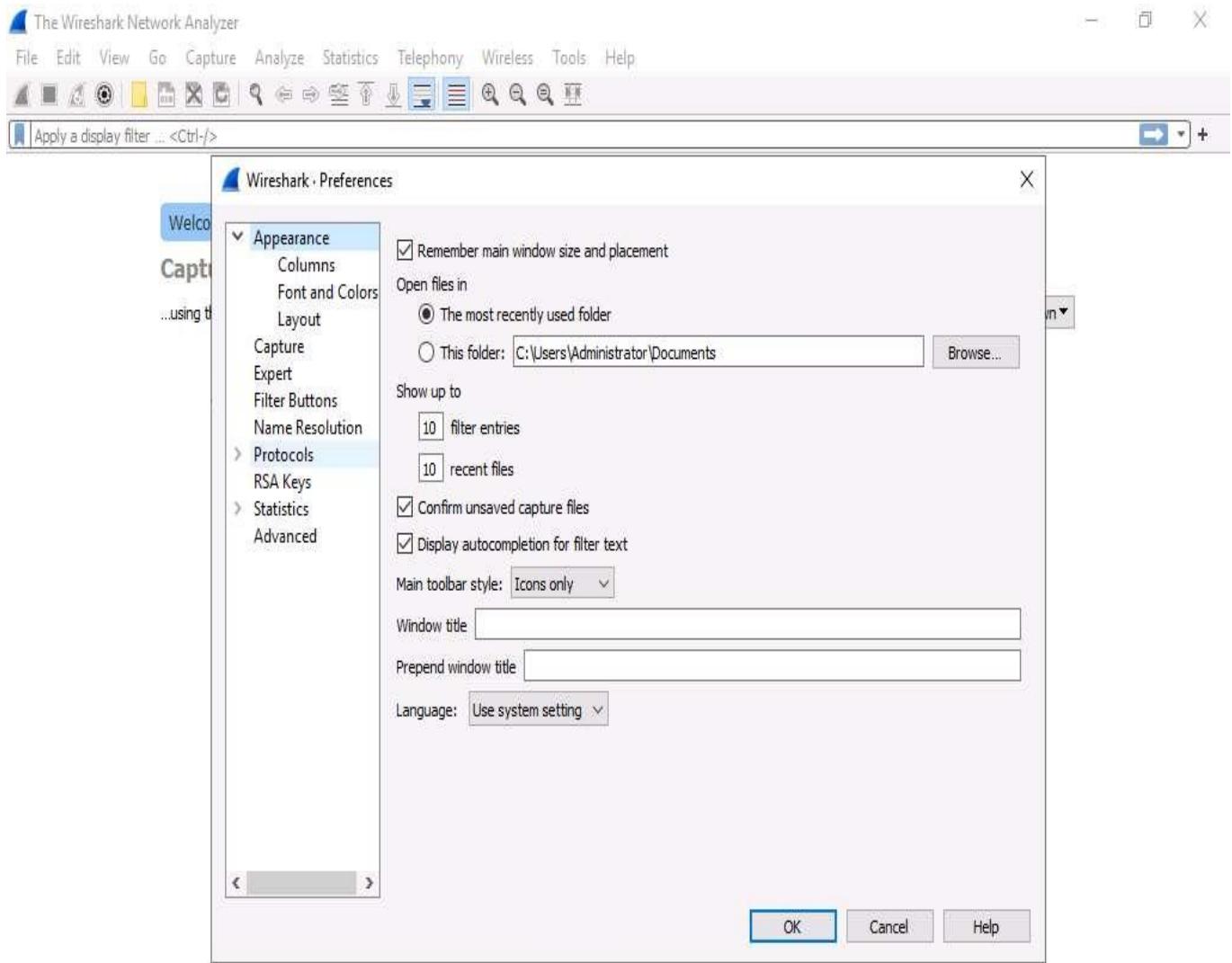
Learn

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

You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e4611e2). You receive automatic updates.



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



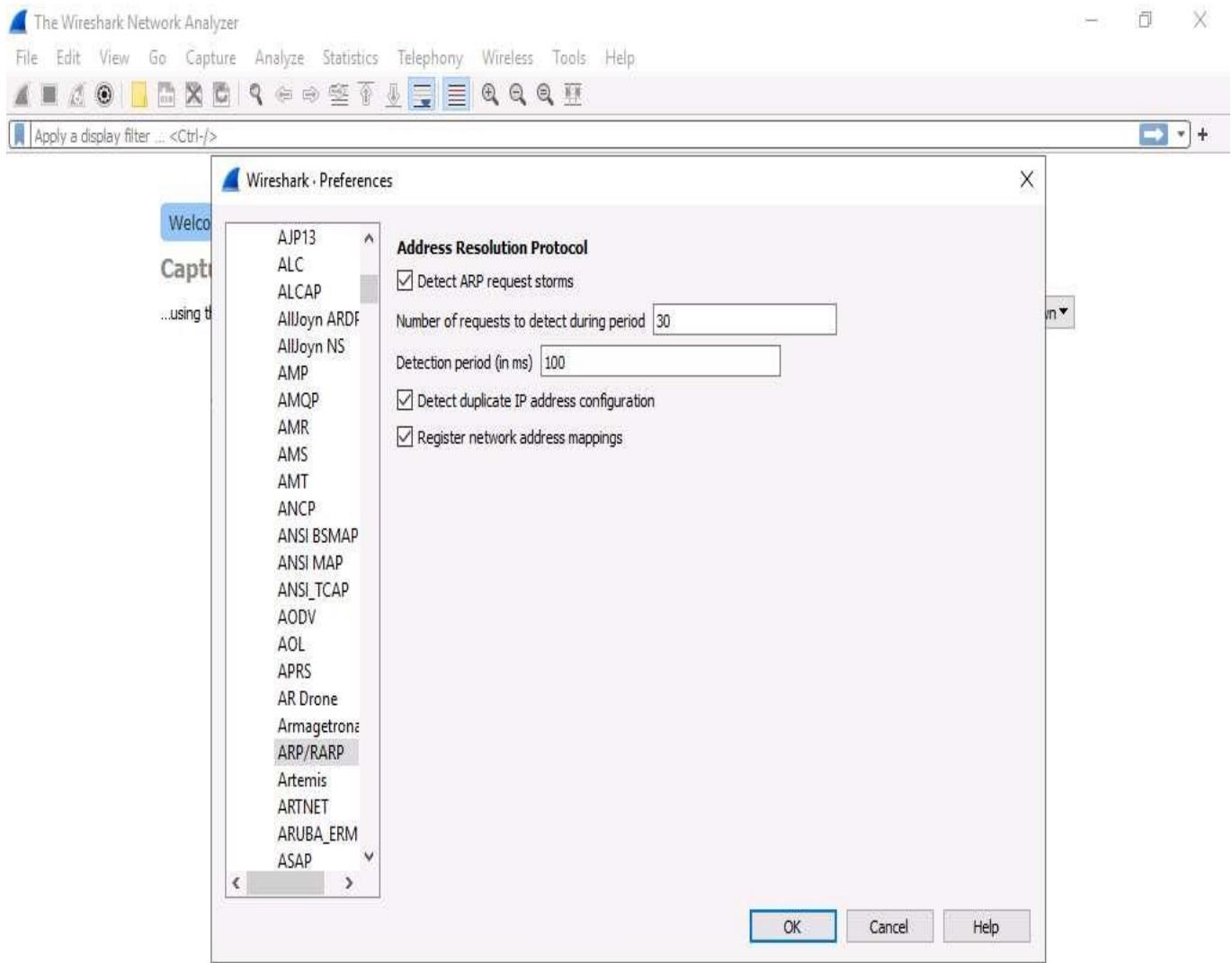
Learn

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

You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e4611e2). 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**.



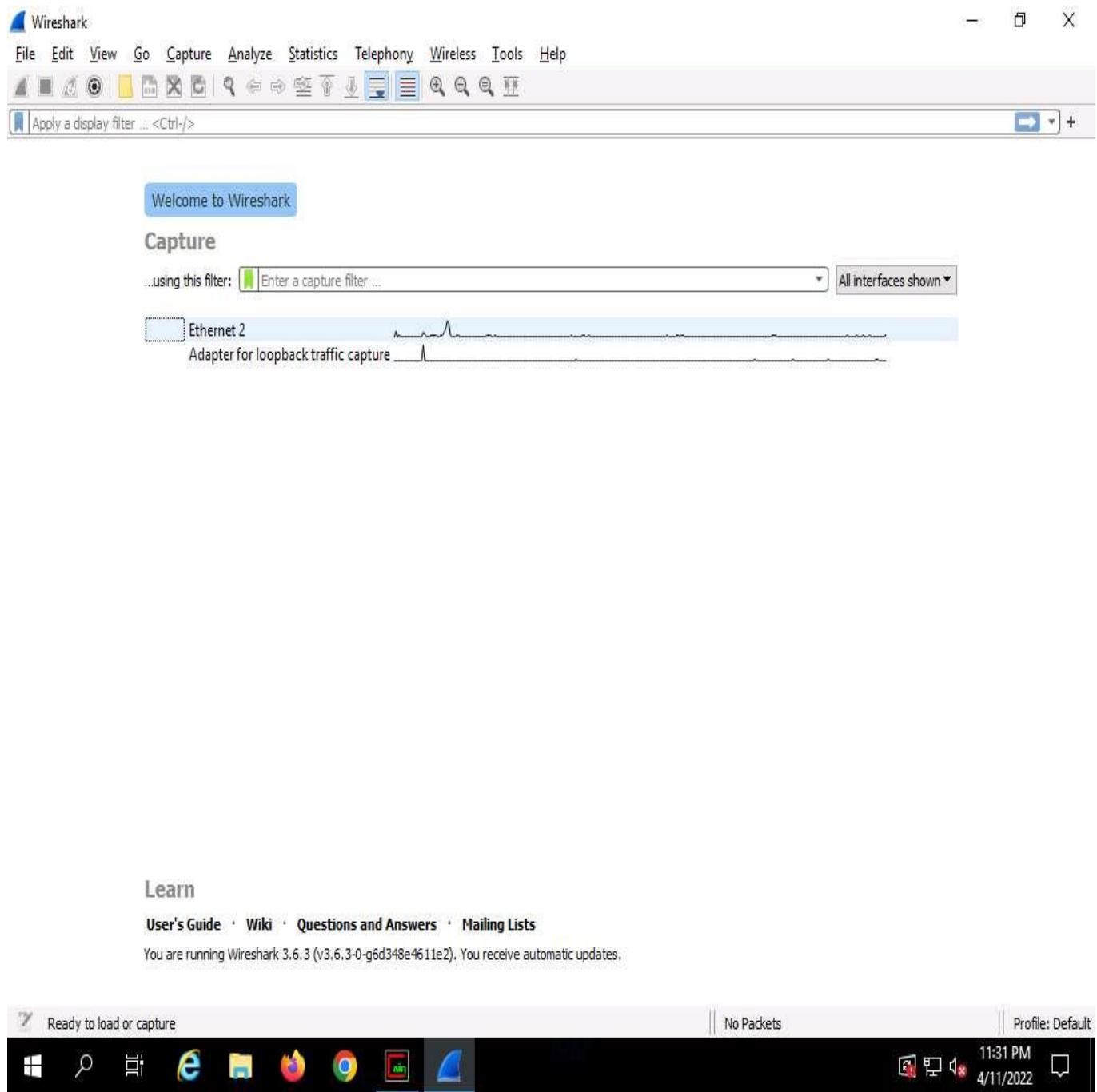
Learn

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

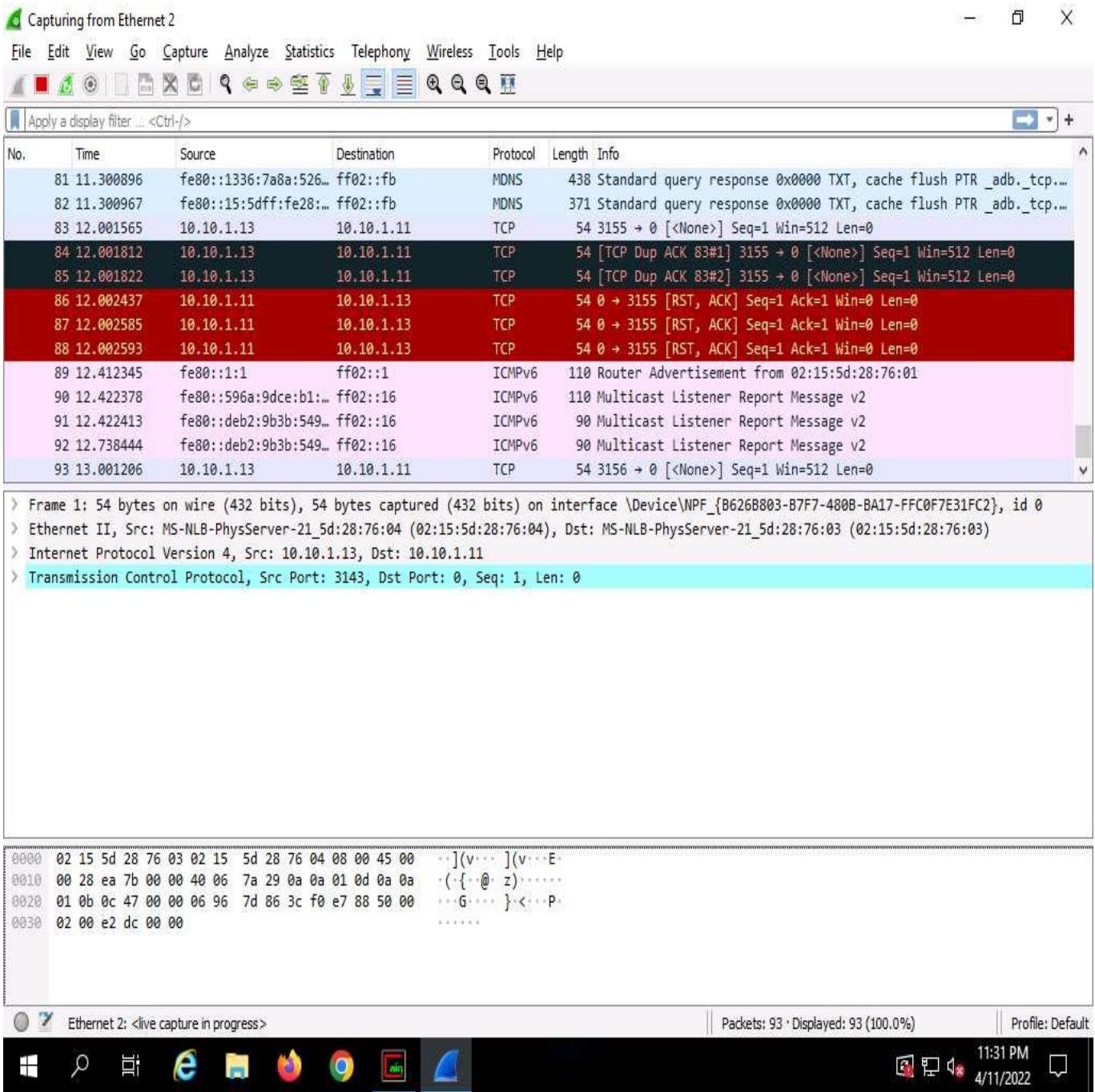
You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e4611e2). You receive automatic updates.



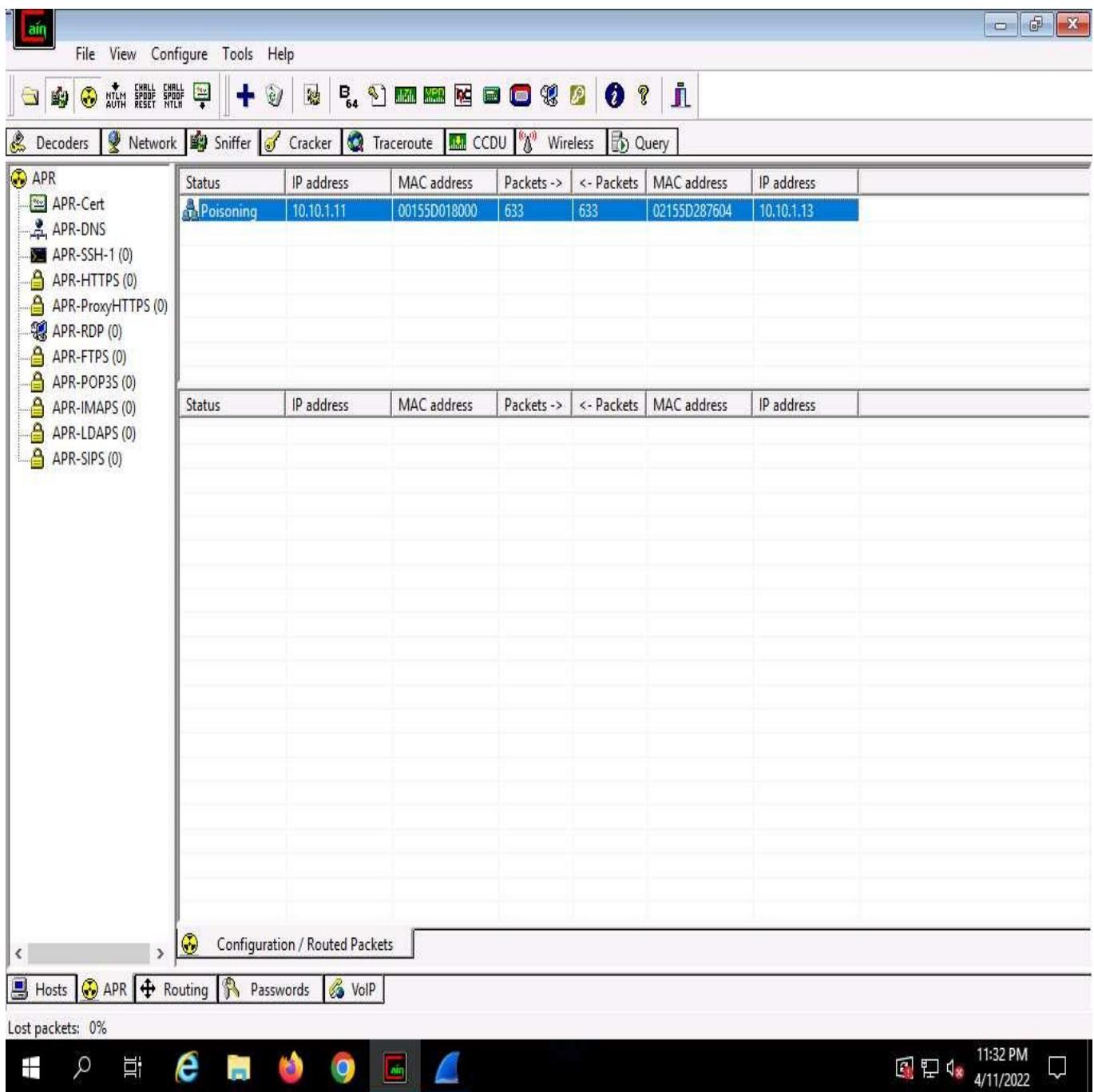
35. Now, double-click on the adapter associated with your network (here, **Ethernet2**) to start capturing the network packets.



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



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



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

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Stop capturing packets

No.	Time	Source	Destination	Protocol	Length	Info
499	63.011792	10.10.1.11	10.10.1.13	TCP	54	0 → 3206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
500	63.011800	10.10.1.11	10.10.1.13	TCP	54	0 → 3206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
501	64.010936	10.10.1.13	10.10.1.11	TCP	54	3207 → 0 [<None>] Seq=1 Win=512 Len=0
502	64.011161	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 501#1] 3207 → 0 [<None>] Seq=1 Win=512 Len=0
503	64.011178	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 501#2] 3207 → 0 [<None>] Seq=1 Win=512 Len=0
504	64.012045	10.10.1.11	10.10.1.13	TCP	54	0 → 3207 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
505	64.012219	10.10.1.11	10.10.1.13	TCP	54	0 → 3207 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
506	64.012226	10.10.1.11	10.10.1.13	TCP	54	0 → 3207 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
507	65.011135	10.10.1.13	10.10.1.11	TCP	54	3208 → 0 [<None>] Seq=1 Win=512 Len=0
508	65.011383	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 507#1] 3208 → 0 [<None>] Seq=1 Win=512 Len=0
509	65.011394	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 507#2] 3208 → 0 [<None>] Seq=1 Win=512 Len=0
510	65.012193	10.10.1.11	10.10.1.13	TCP	54	0 → 3208 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
511	65.012855	10.10.1.11	10.10.1.13	TCP	54	0 → 3208 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
512	65.012865	10.10.1.11	10.10.1.13	TCP	54	0 → 3208 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
513	66.012003	10.10.1.13	10.10.1.11	TCP	54	3209 → 0 [<None>] Seq=1 Win=512 Len=0
514	66.012218	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 513#1] 3209 → 0 [<None>] Seq=1 Win=512 Len=0
515	66.012230	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 513#2] 3209 → 0 [<None>] Seq=1 Win=512 Len=0
516	66.013766	10.10.1.11	10.10.1.13	TCP	54	0 → 3209 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
517	66.014615	10.10.1.11	10.10.1.13	TCP	54	0 → 3209 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
518	66.014625	10.10.1.11	10.10.1.13	TCP	54	0 → 3209 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:28:76:04 (02:15:5d:28:76:04), Dst: MS-NLB-PhysServer-21_5d:28:76:03 (02:15:5d:28:76:03)
> Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.11
> Transmission Control Protocol, Src Port: 3143, Dst Port: 0, Seq: 1, Len: 0

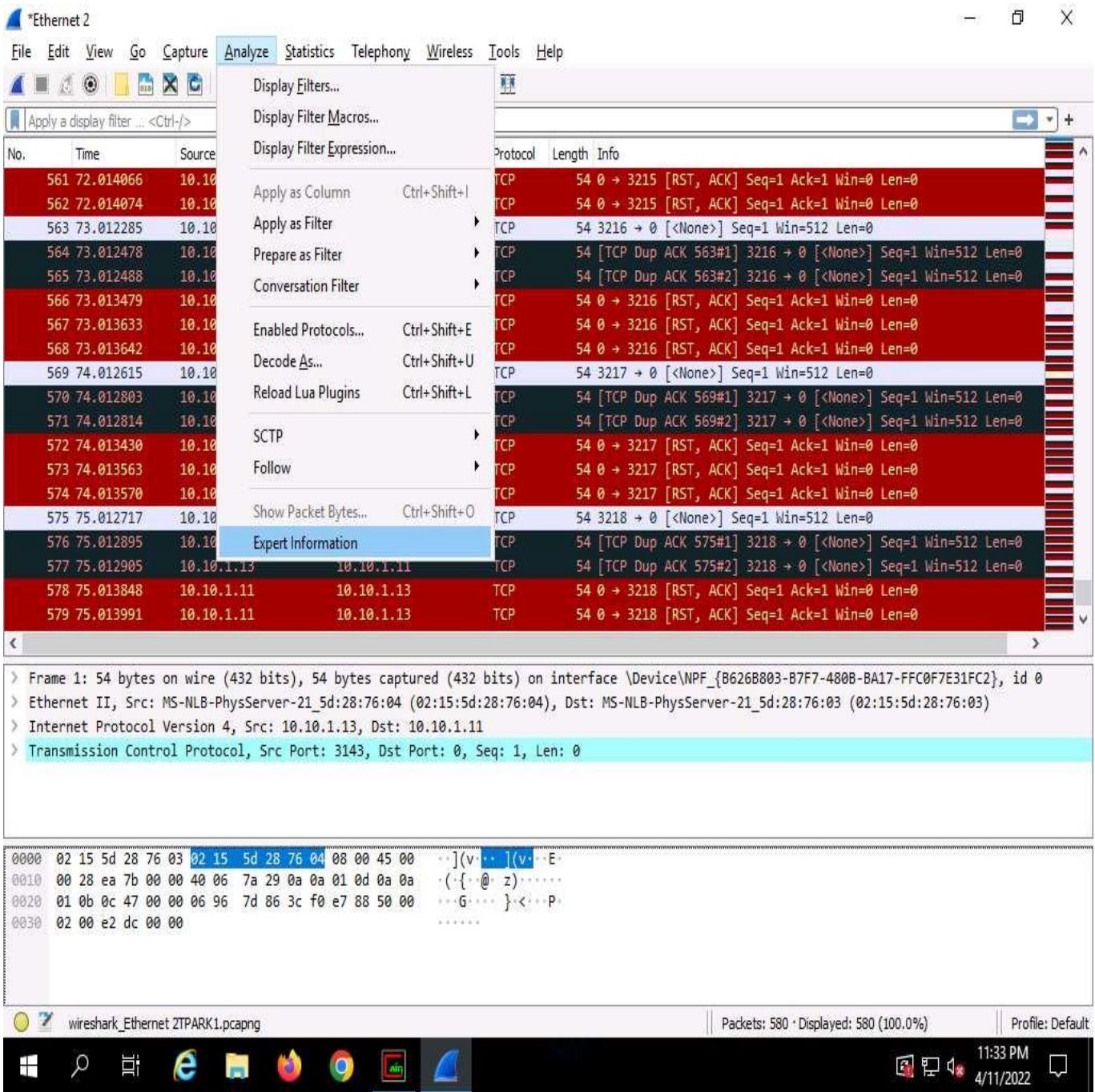
```

0000	02	15	5d	28	76	03	02	15	5d	28	76	04	08	00	45	00	...](v...](v... E...
0010	00	28	ea	7b	00	00	40	06	7a	29	0a	0a	01	0d	0a	0a	...({@ z).....
0020	01	0b	0c	47	00	00	06	96	7d	86	3c	f0	e7	88	50	00	...G... }<--P...
0030	02	00	e2	dc	00	00	00	00	00	00	00	00	00	00	00	00

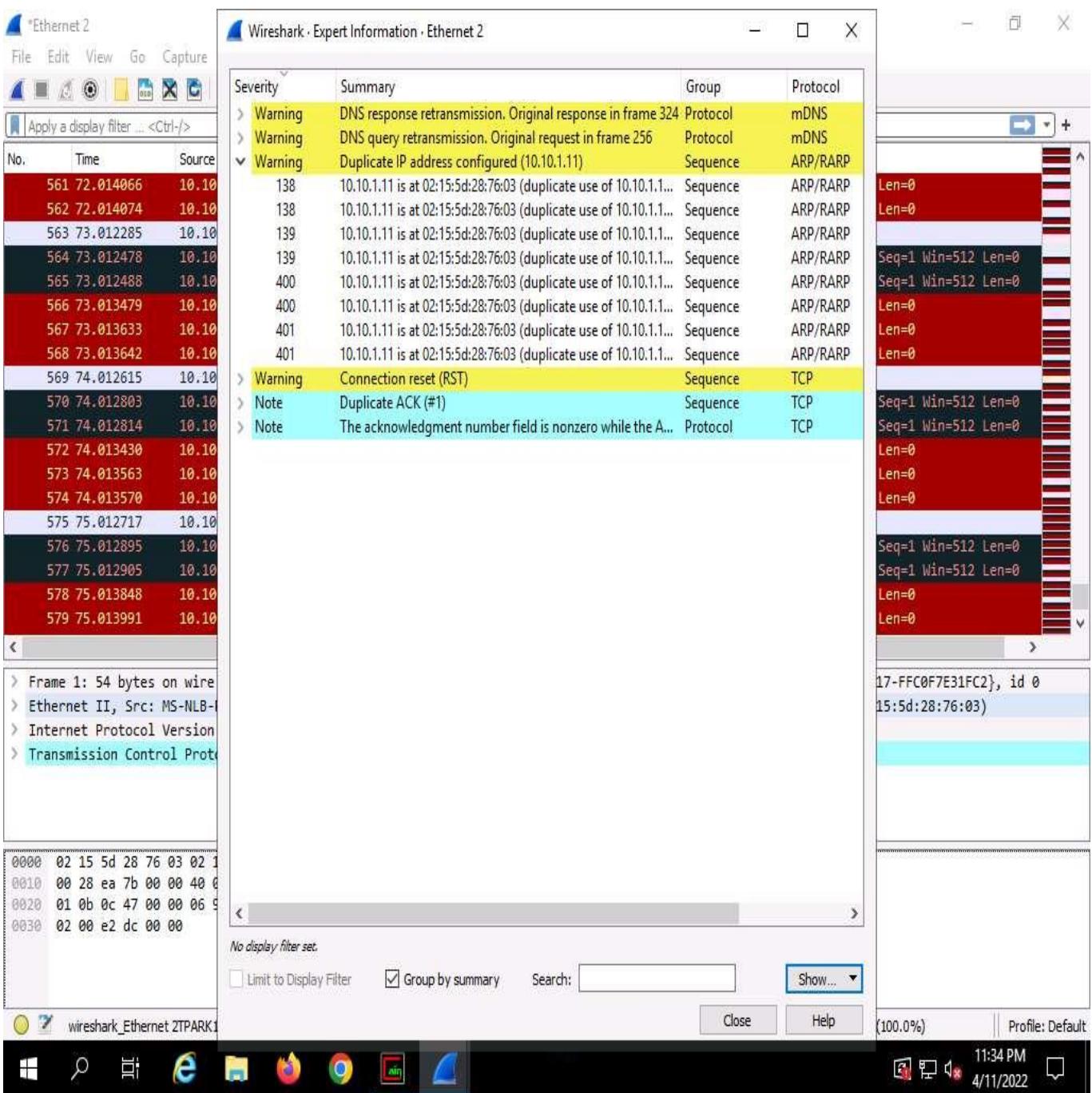
Ethernet 2: <live capture in progress> | Packets: 518 · Displayed: 518 (100.0%) | Profile: Default

11:32 PM 4/11/2022

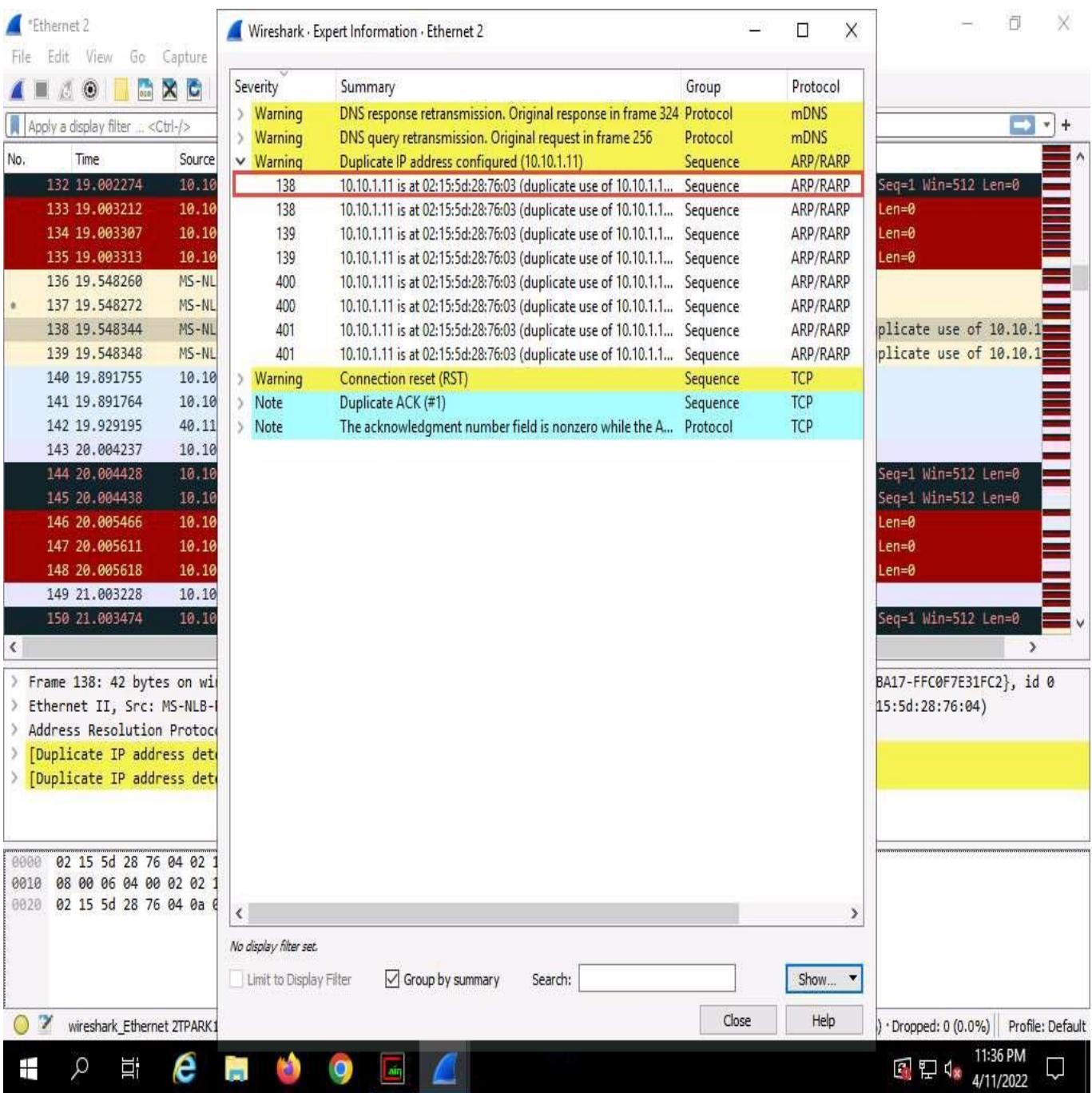
39. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.



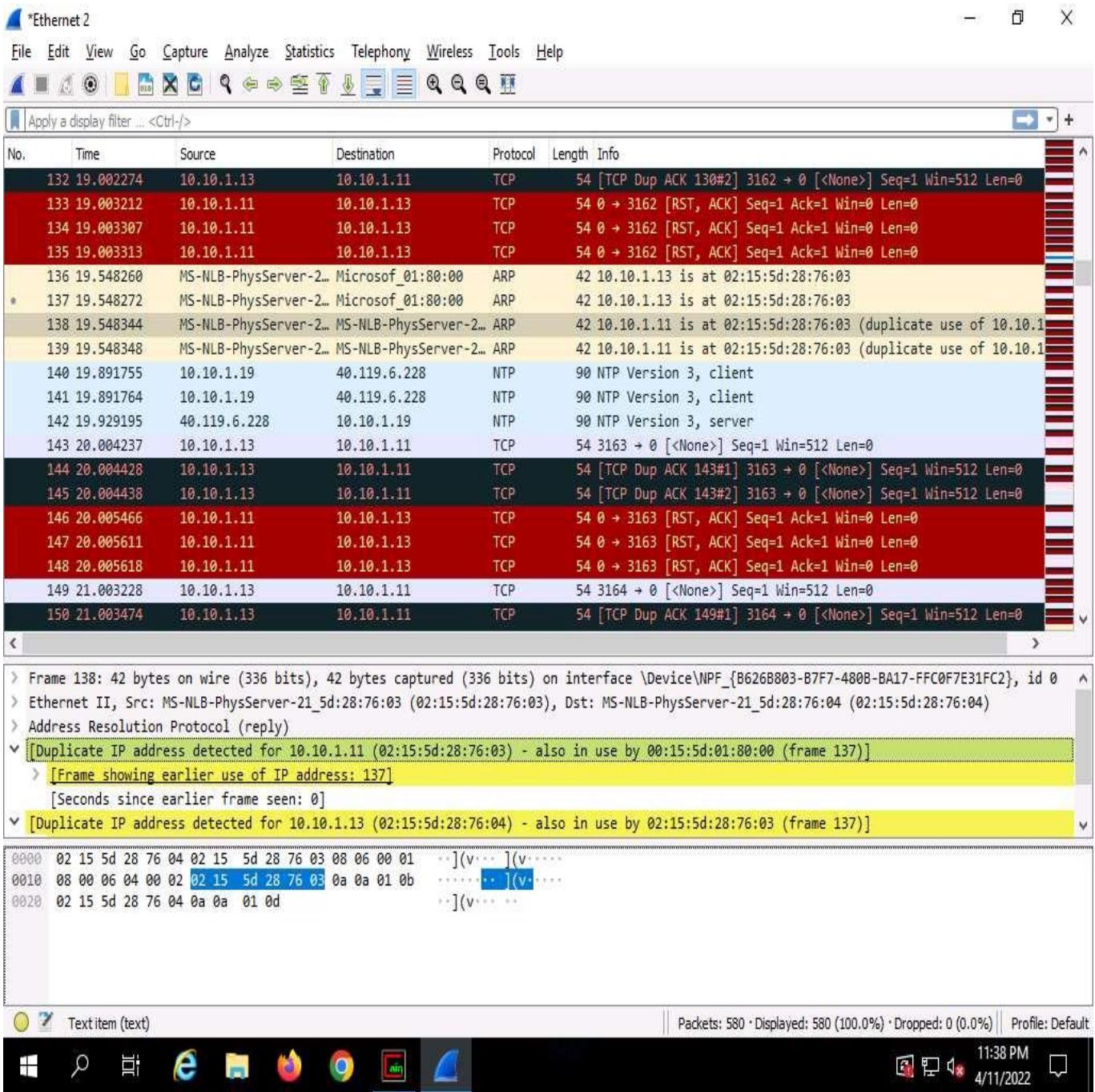
40. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.11)**, running on the **ARP/RARP** protocol.



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).

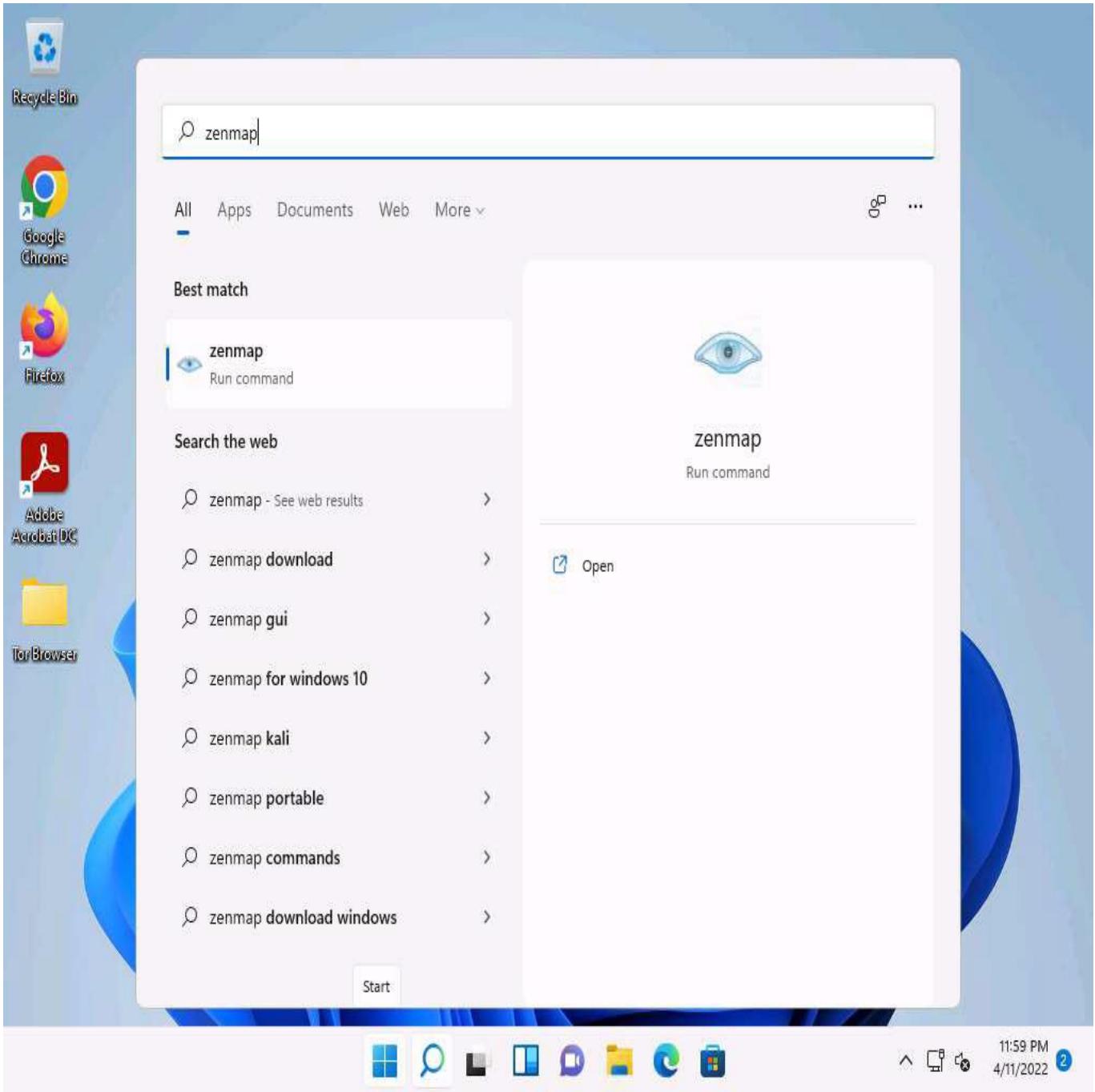


43. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close the **Wireshark . Expert Information** window.
44. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.



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 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.

- This concludes the demonstration of detecting ARP poisoning in a switch-based network.
- Close the **Wireshark** window and leave all other windows running.
- Now, we shall perform promiscuous mode detection using Nmap.
- Now, Click **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.

```

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-12 00:01 Pacific Daylight Time
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.002s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
636/tcp   open  ldapssl
990/tcp   open  ftps
993/tcp   open  imaps
995/tcp   open  pop3s
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5061/tcp  open  sip-tls
5357/tcp  open  wsapi
8080/tcp  open  http-proxy
MAC Address: 02:15:5D:28:76:03 (Unknown)

Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap done: 1 IP address (1 host up) scanned in 2.50 seconds

```

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

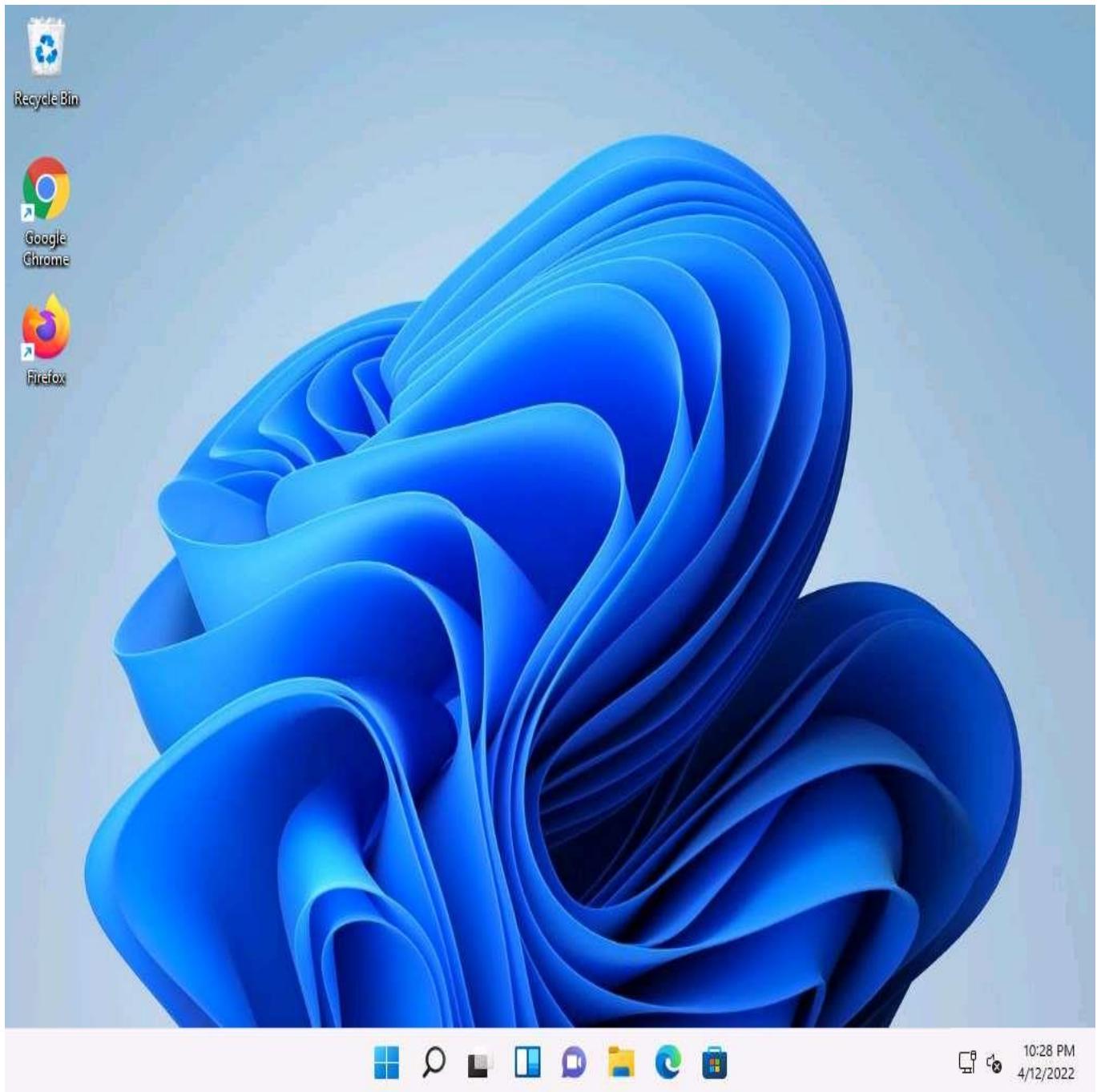
Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy to use interface that allows users to protect and monitor networks in a critical business environment. It helps ethical hackers or pentesters in quickly detecting ARP poisoning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

Habu

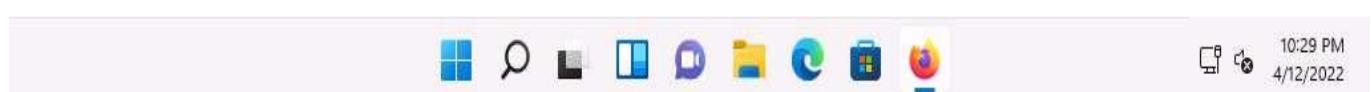
Habu is an open source penetration testing toolkit that can perform various tasks such as ARP poisoning, ARP sniffing, DHCP starvation and DHCP discover.

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 **Windows 11** to switch to the **Windows 11** machine.



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



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

Quick detect ARP poisoning & ... X

https://www.colasoft.com/download/arp_flood_arp_spoofing_arp_poisoning_attack_solution_with_Capsa_Network_Analyzer

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...

Colasoft Maximize Network Value

PRODUCTS SOLUTIONS PURCHASE SUPPORT COMPANY PARTNER

TRIAL DOWNLOADS

Colasoft Capsa - Quick detect ARP poisoning & ARP flooding

This demo will demonstrate how to quickly detect ARP poisoning and ARP flooding attack and locate attack source with Colasoft Capsa - a professional network analyzer from Colasoft.

Buy Now

Download Free Trial

Contact Sales

Download this demo

Watch Other Live Demo

- Quick detect ARP poisoning & ARP flooding
- Monitor realtime network utilization
- Monitor Network Traffic
- Track Down BitTorrent Protocol
- Find out top 10 network traffic hosts
- Deploy Colasoft Capsa

QUICK LINKS

Capsa Network Analyzer

DOWNLOADS

Capsa Network Analyzer

COMPANY

About Colasoft

FOLLOW US

10:32 PM
4/12/2022

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**.

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

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

- Title Bar:** "Thank you for downloading Capsa" and a "+" button.
- Address Bar:** URL: https://www.colasoft.com/download/products/download_capsa.php
- Message Bar:** "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!" with "Refresh Firefox..." button.
- Header:** Colasoft logo, followed by navigation menus: PRODUCTS, SOLUTIONS, PURCHASE, SUPPORT, COMPANY, and PARTNER.
- Section:** TRIAL DOWNLOADS
- Form Fields (Left):**
 - Version: 13.0 (02/26/2020)
 - Requirements: Windows Server 2008/2012/7/8/10
 - Limitations: Fully functional for 30 days
- Form Fields (Right):**
 - First Name: [Redacted]
 - Last Name: [Redacted]
 - Country/Region: [Redacted]
 - State: [Redacted]
 - Company: [Redacted]
 - Email: [Redacted]
 - Phone: [Redacted]
- Checkboxes:**
 - Subscribe to our newsletter.
 - I'm not a robot
- Image:** reCAPTCHA logo with "Privacy - Terms".
- Buttons:** A large blue "30-Day Trial Download" button.
- Taskbar:** Shows various pinned icons and system status: 10:39 PM, 4/12/2022, and a notification badge with the number 1.

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 a Firefox browser window with the address bar pointing to https://www.colasoft.com/download/products/api/process_demo_download.ent.php. A message at the top of the page says, "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!" Below this, there are links for "Customer Portal", "Blog", and "Contact Us".

The main content of the page is a "Thank You for Downloading" message for Colasoft Capsa Enterprise. It includes a link to "Your Free Trial License for Capsa Enterprise". A download dialog box is overlaid on the page, titled "Opening capsa_ent_13.0.1.13110_x64.zip". The dialog shows the file path as "capsa_ent_13.0.1.13110_x64.zip", describes it as a "WinRAR ZIP archive", and provides the source URL "from: https://www.colasoft.com". It asks, "What should Firefox do with this file?", with two options: "Open with WinRAR archiver (default)" (radio button unselected) and "Save File" (radio button selected). There is also a checkbox "Do this automatically for files like this from now on." At the bottom are "OK" and "Cancel" buttons.

The Next Steps You Need to

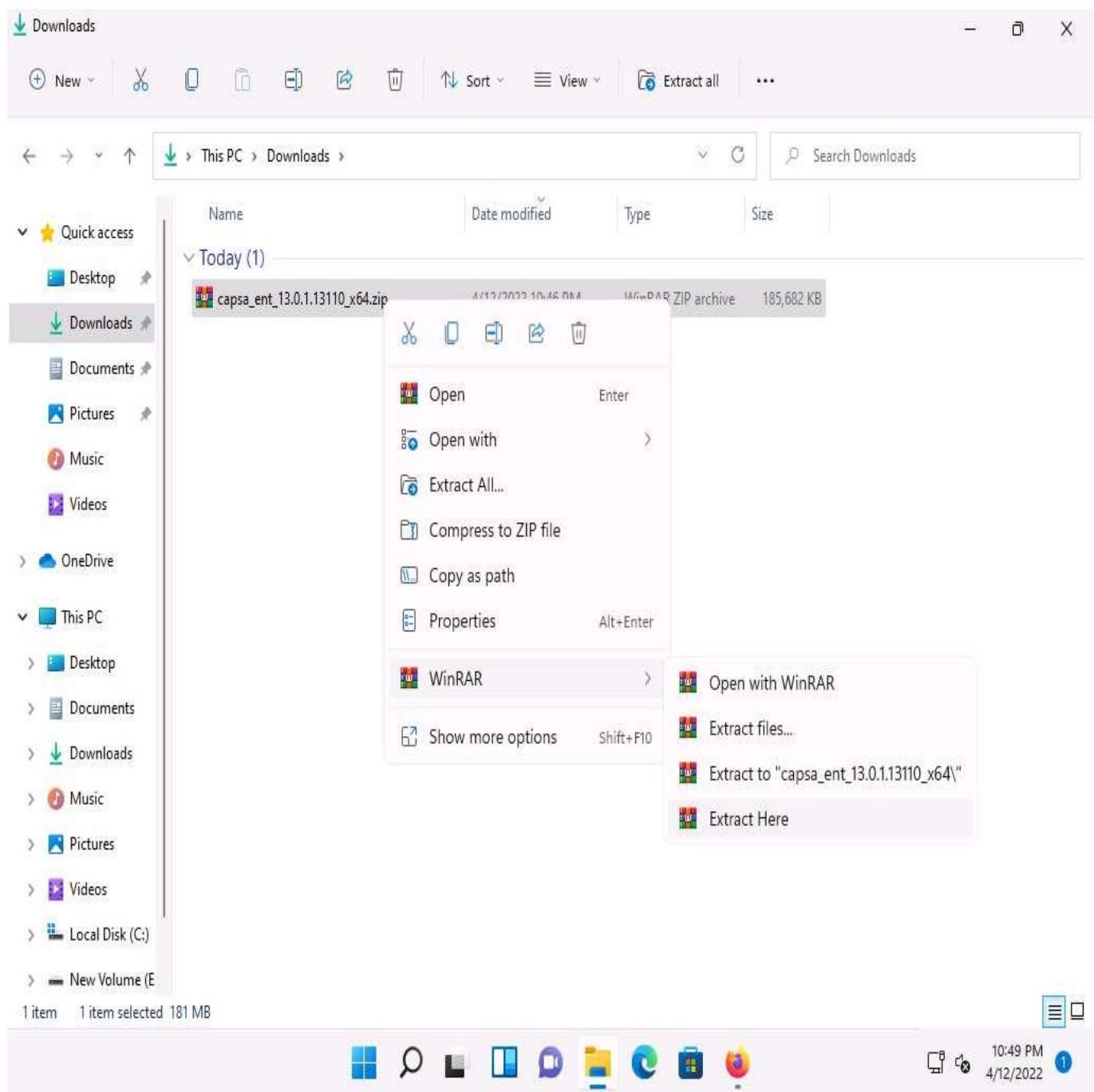
- Take a look at our [deployment guide](#) for Capsa network analyzer.

You May Need More...

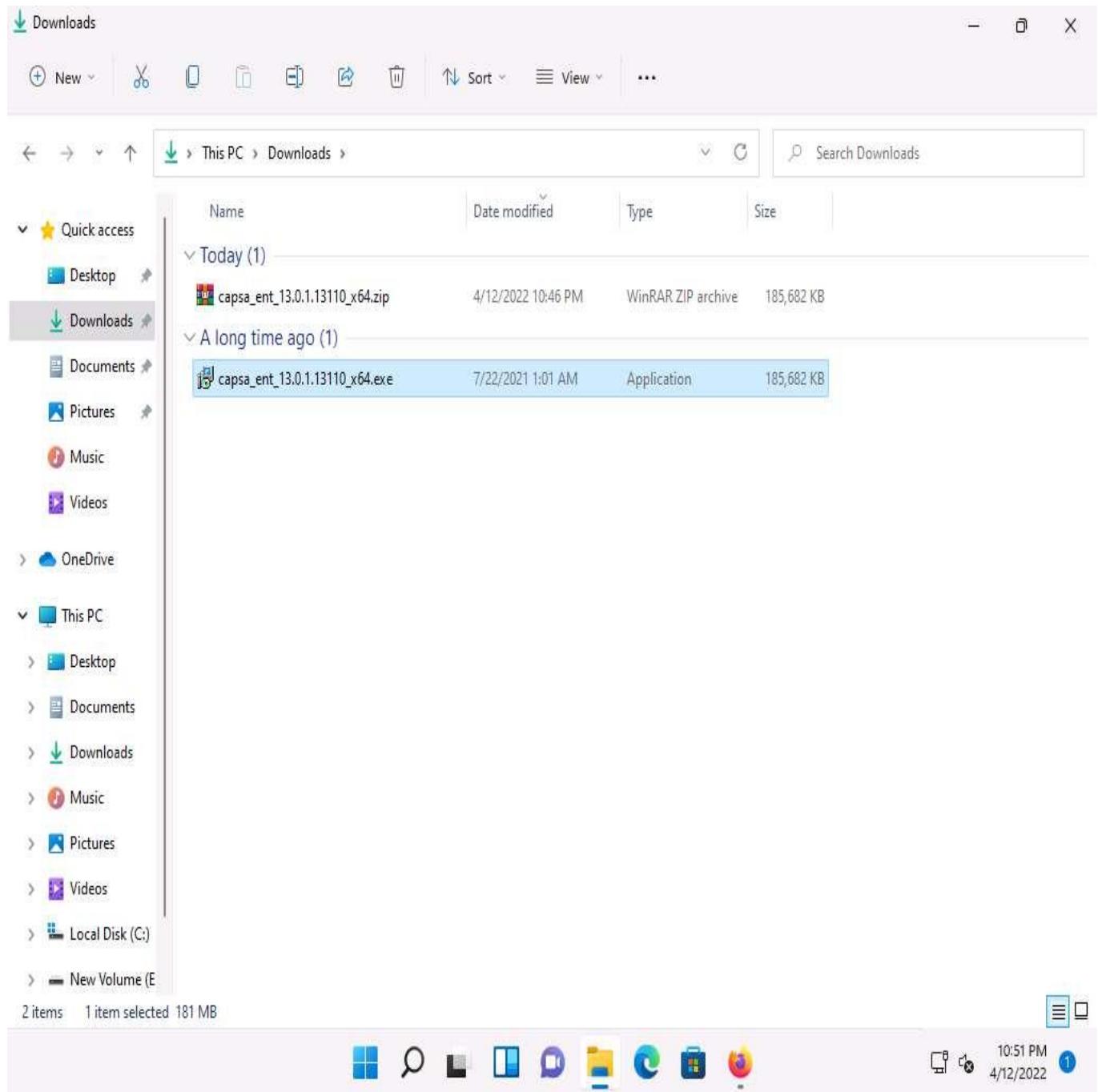


10:42 PM
4/12/2022 1

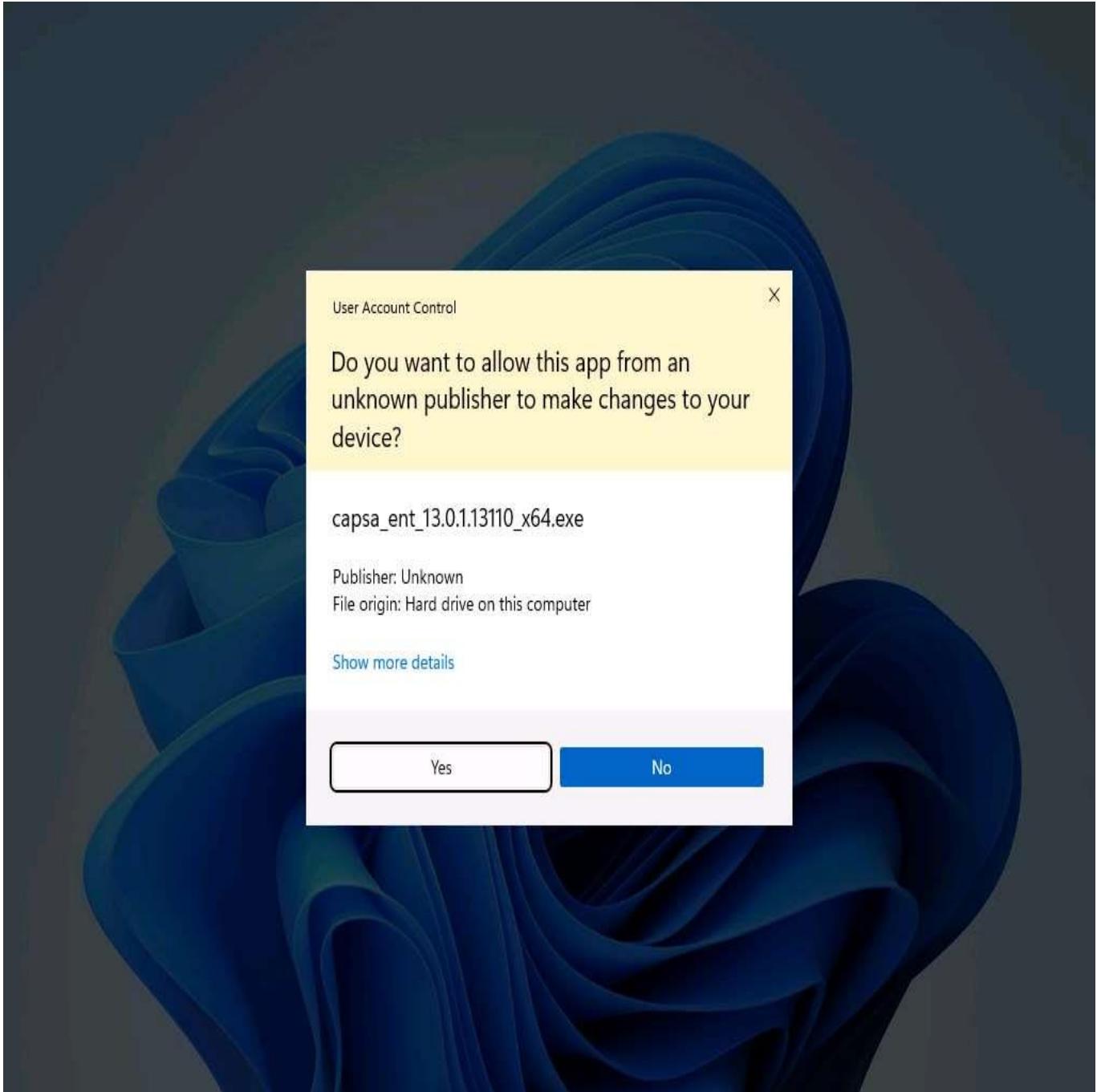
- The **capsa_ent_13.0.1.13110_x64.zip** file starts downloading, it will take approximately **5** minutes for the download.
- Once the download completes, navigate to the **Downloads** folder and right-click on **capsa_ent_13.0.1.13110_x64.zip** file and hover the cursor over **WinRAR** and select **Extract Here** option from the list.



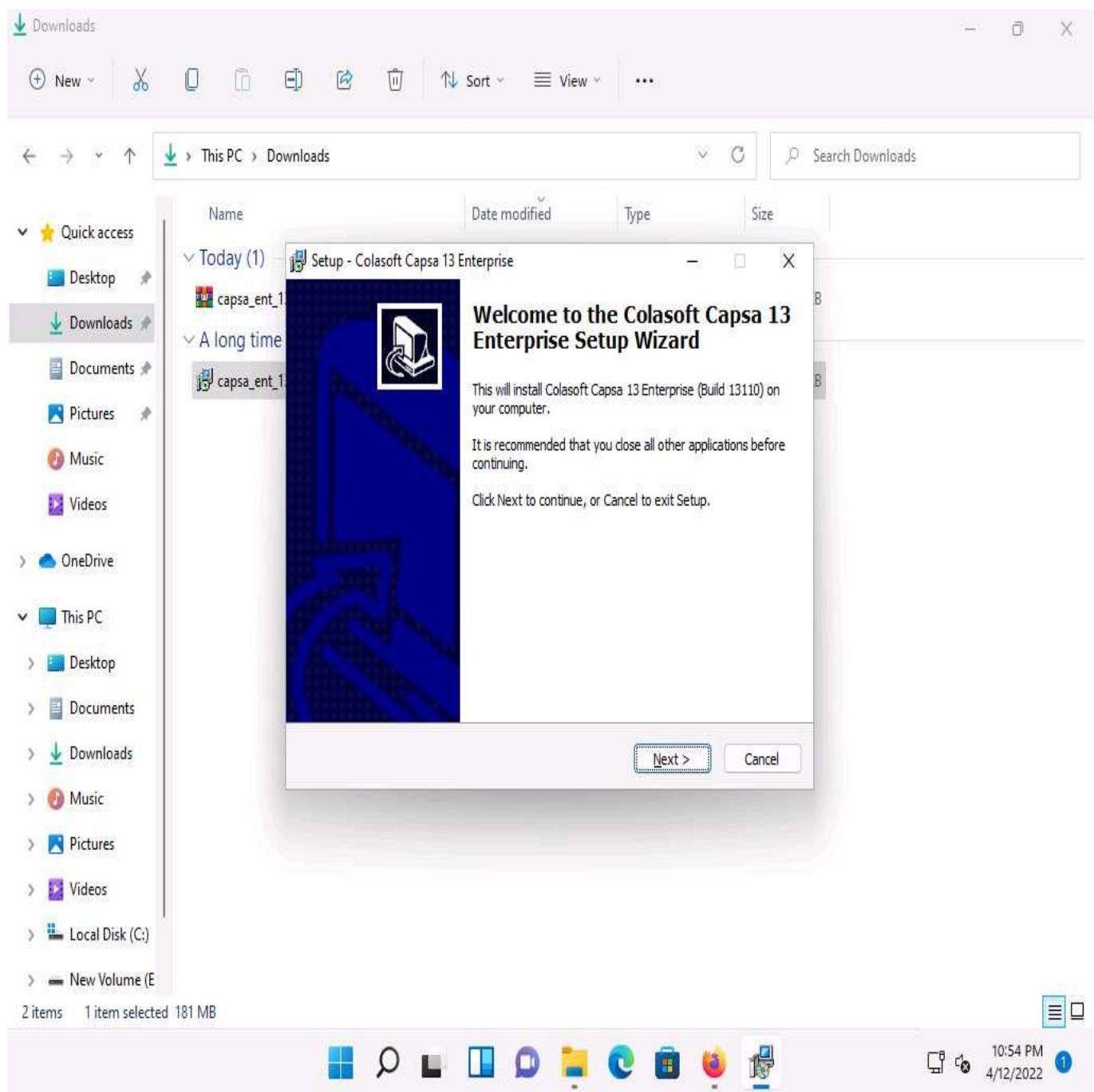
8. Once the extraction is completed, double-click the **capsa_ent_13.0.1.13110_x64.exe** file.



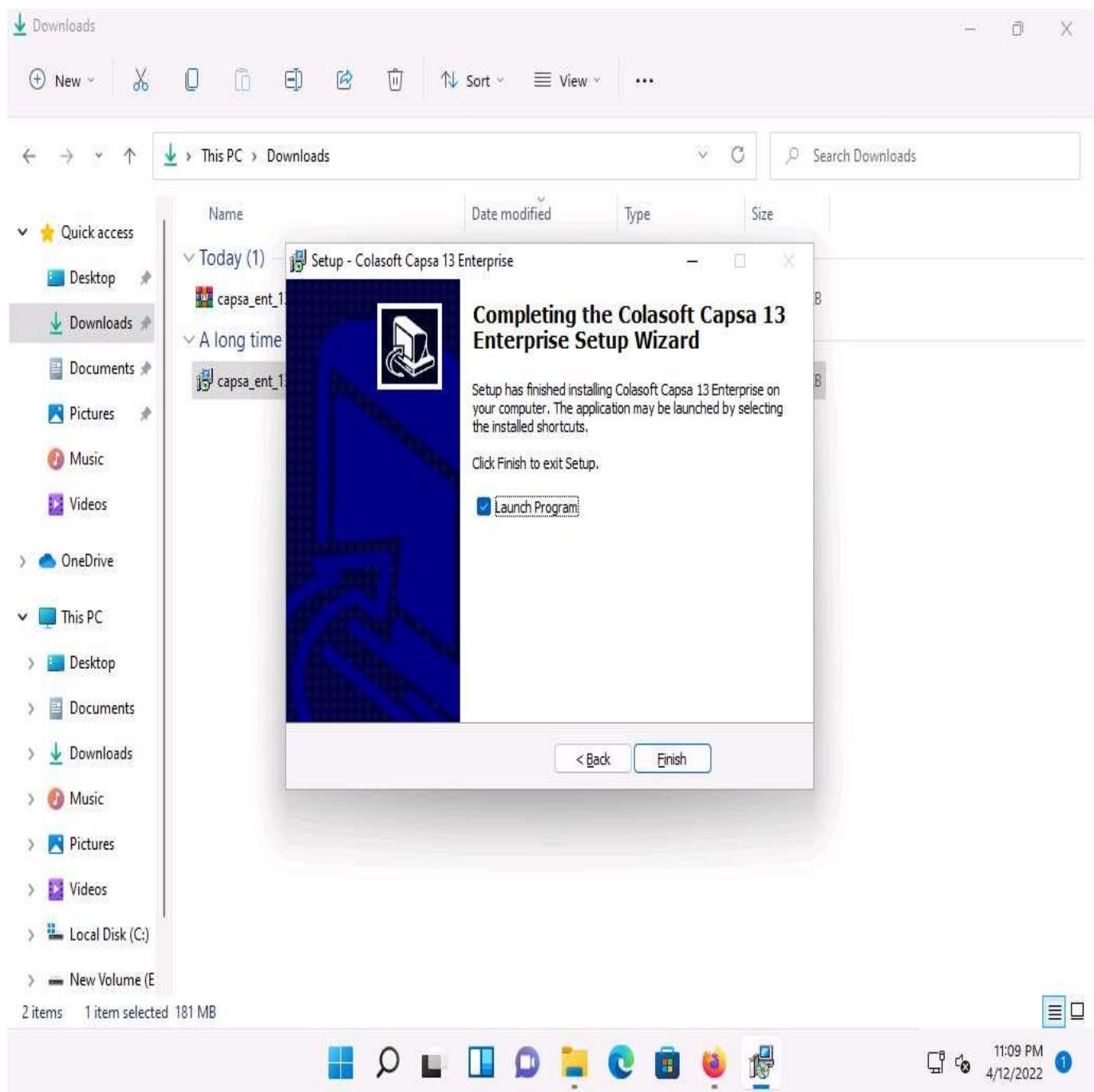
9. A **User Account Control** pop-up appears; click **Yes**.



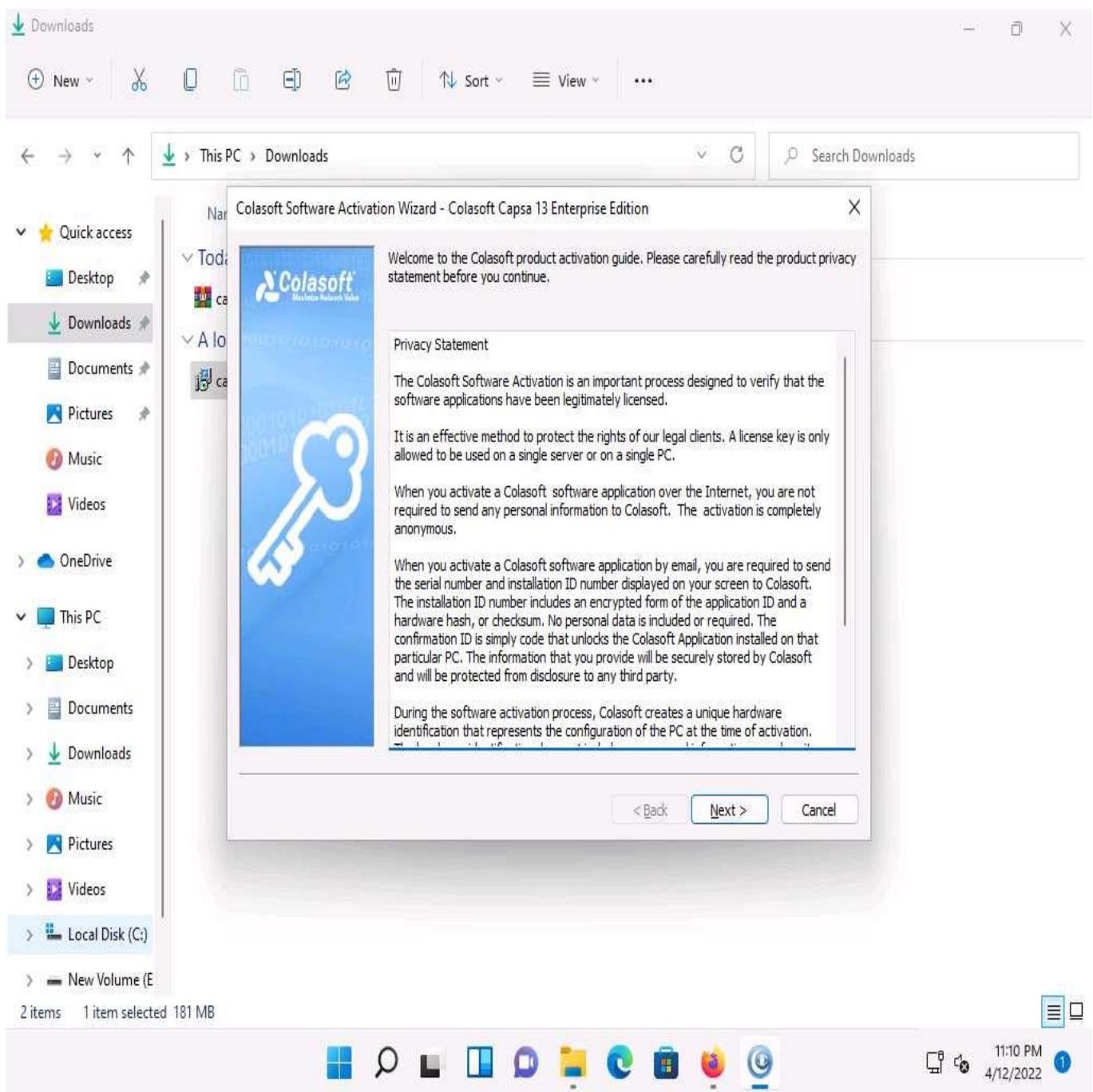
10. **Setup - Colasoft Capsa 13 Enterprise** window appears, click **Next** and follow the wizard driven steps to install **Colasoft Capsa 13 Enterprise** tool.



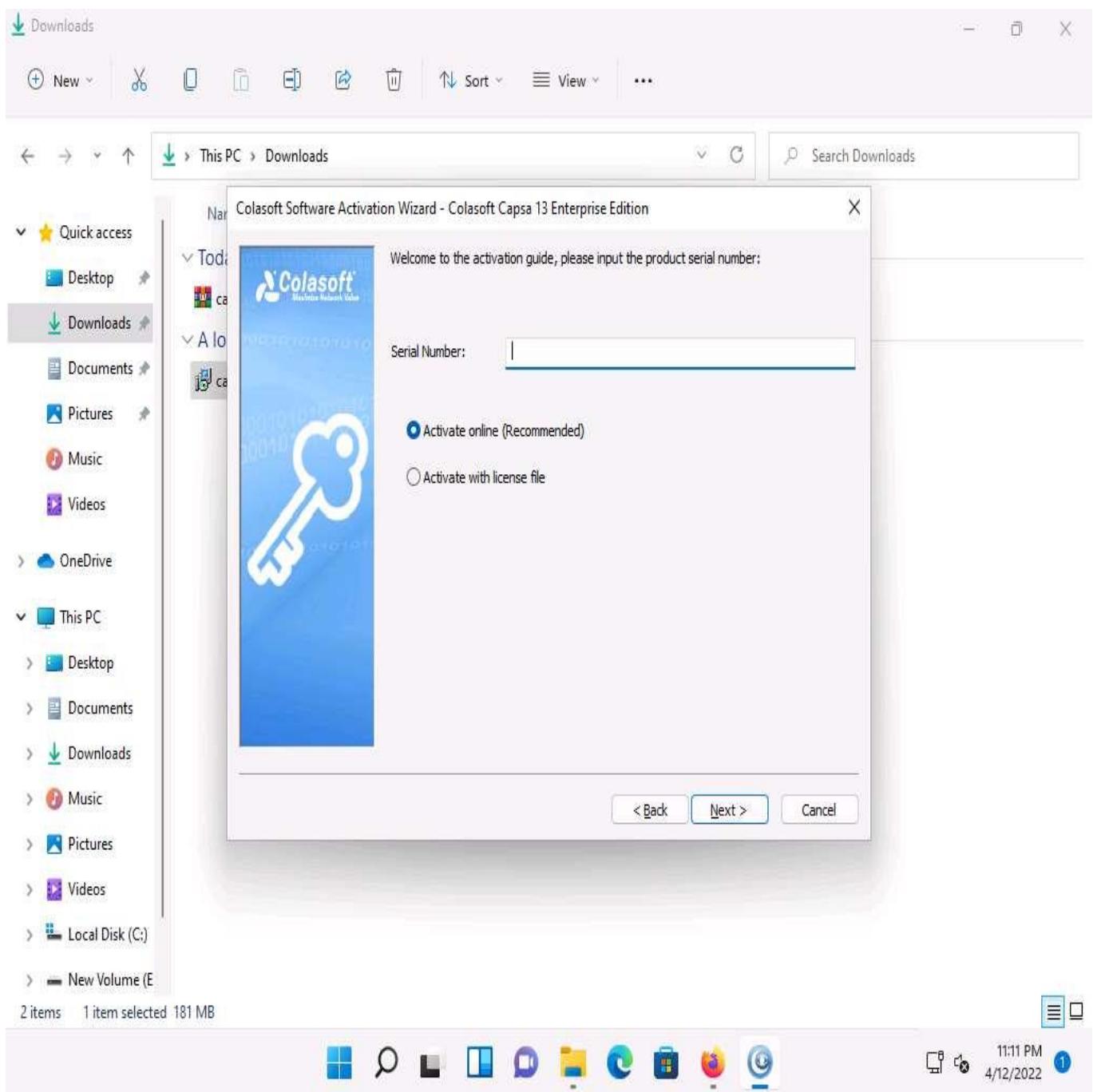
11. In the **Completing the Colasoft Capsa 13 Enterprise Setup** Wizard, ensure that **Launch Program** checkbox is checked and click on **Finish**.



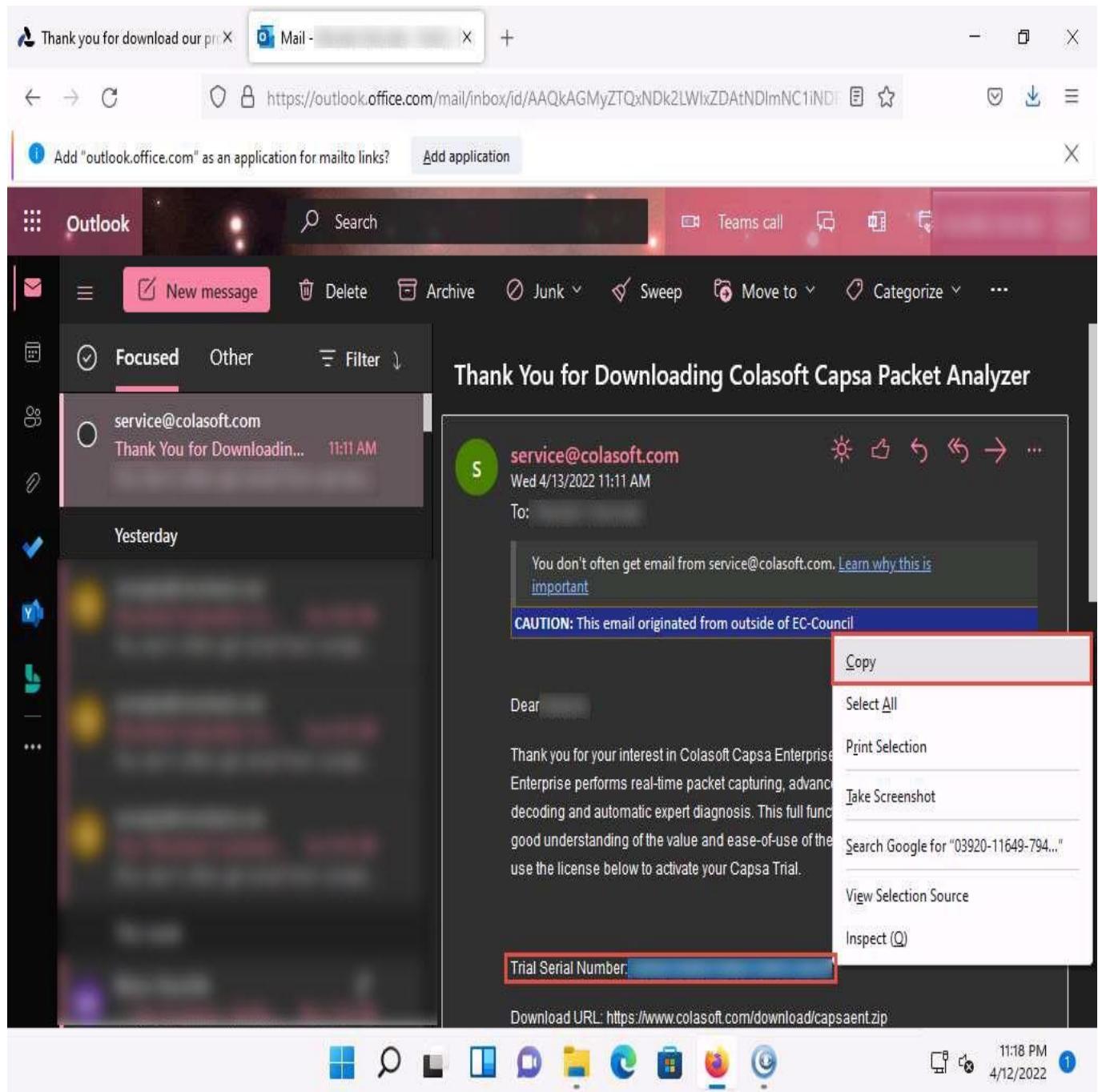
12. In the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window, click **Next**.



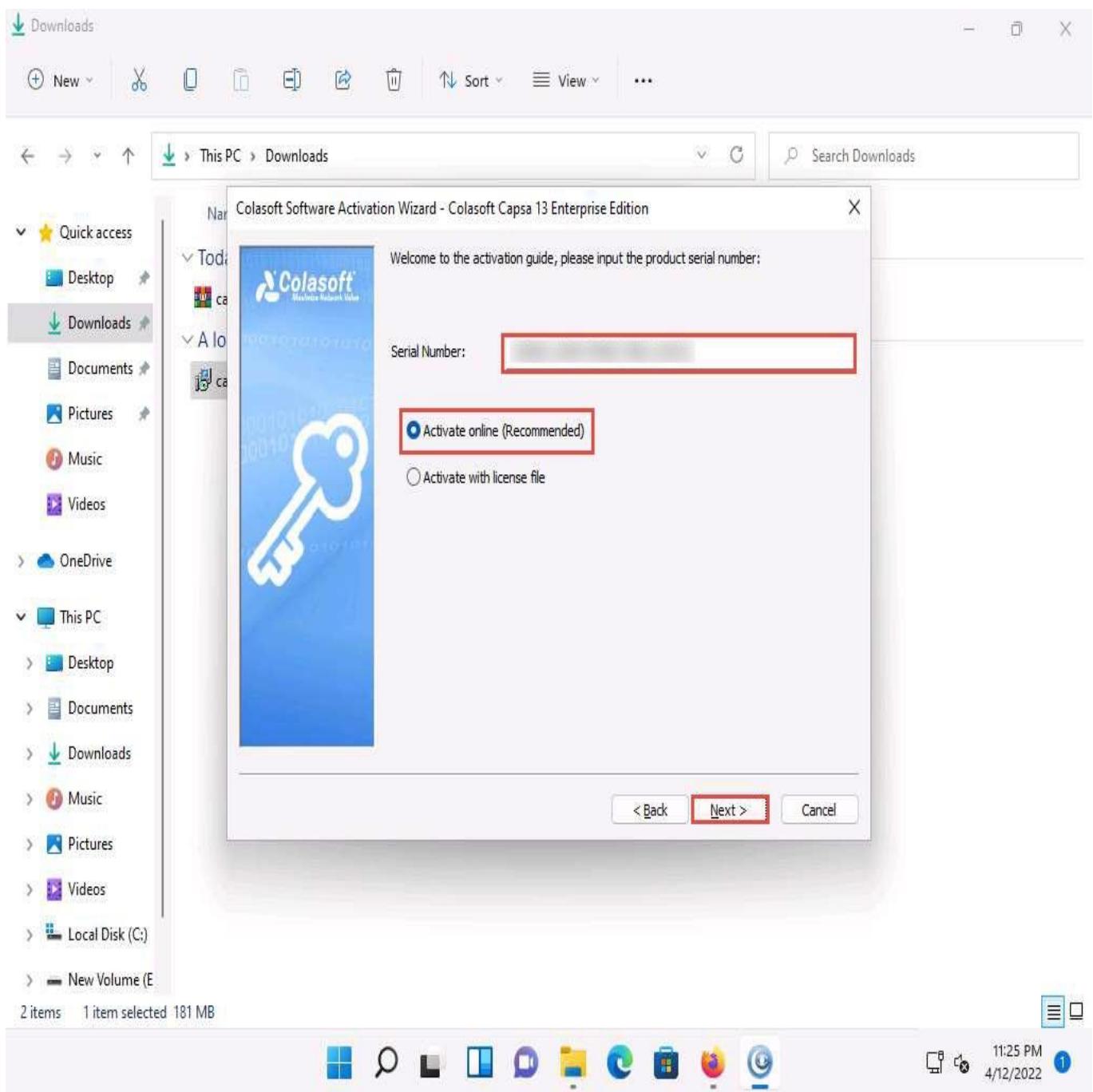
13. In the next window we need to enter the serial number to activate the license.



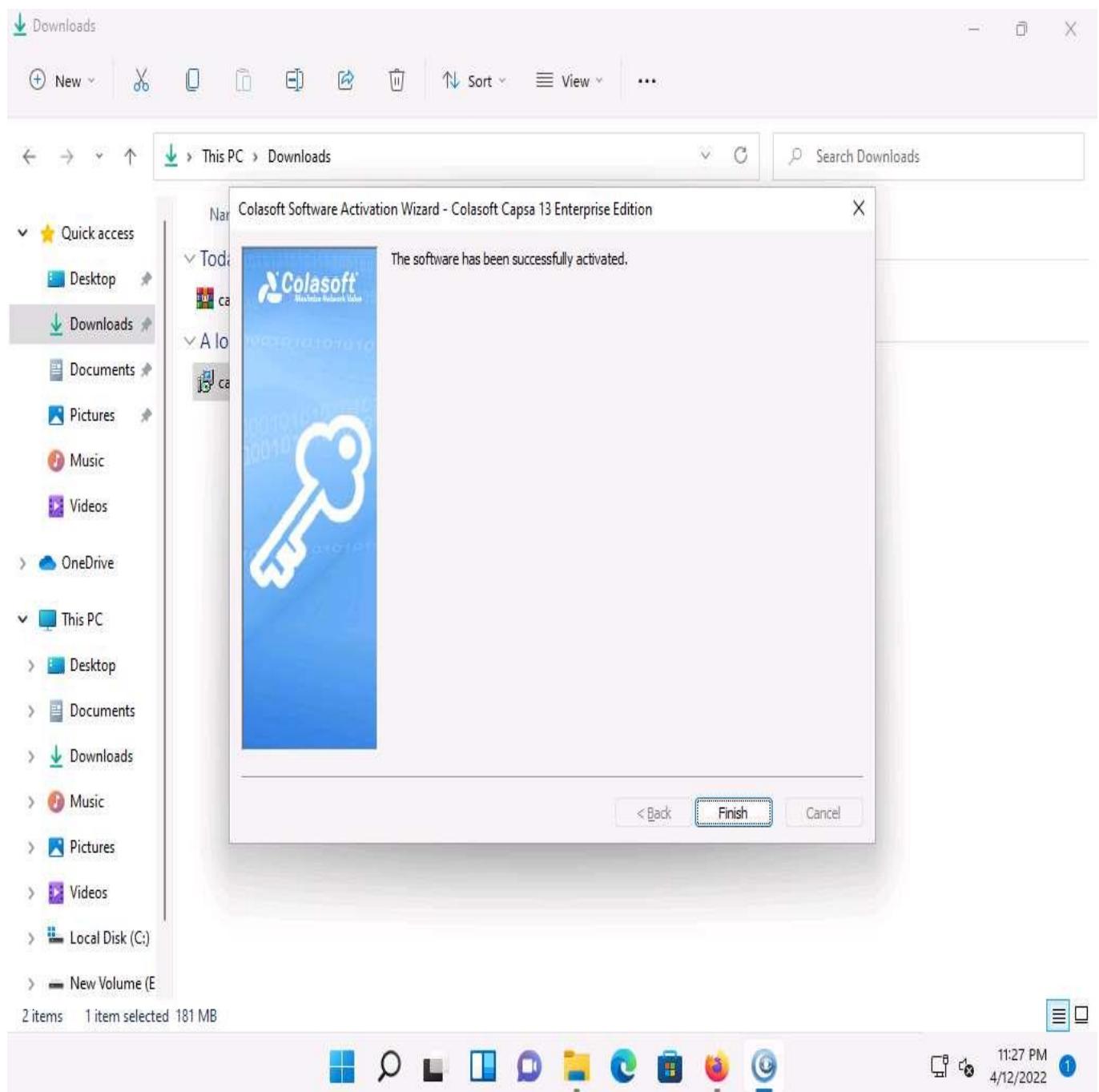
14. Leave the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** as it is and switch to the browser.
15. Open a new tab in the browser and log in to the email account you provided during registration. Open the email from **service@colasoft.com** and copy the **Trial Serial Number** as shown in the screenshot.



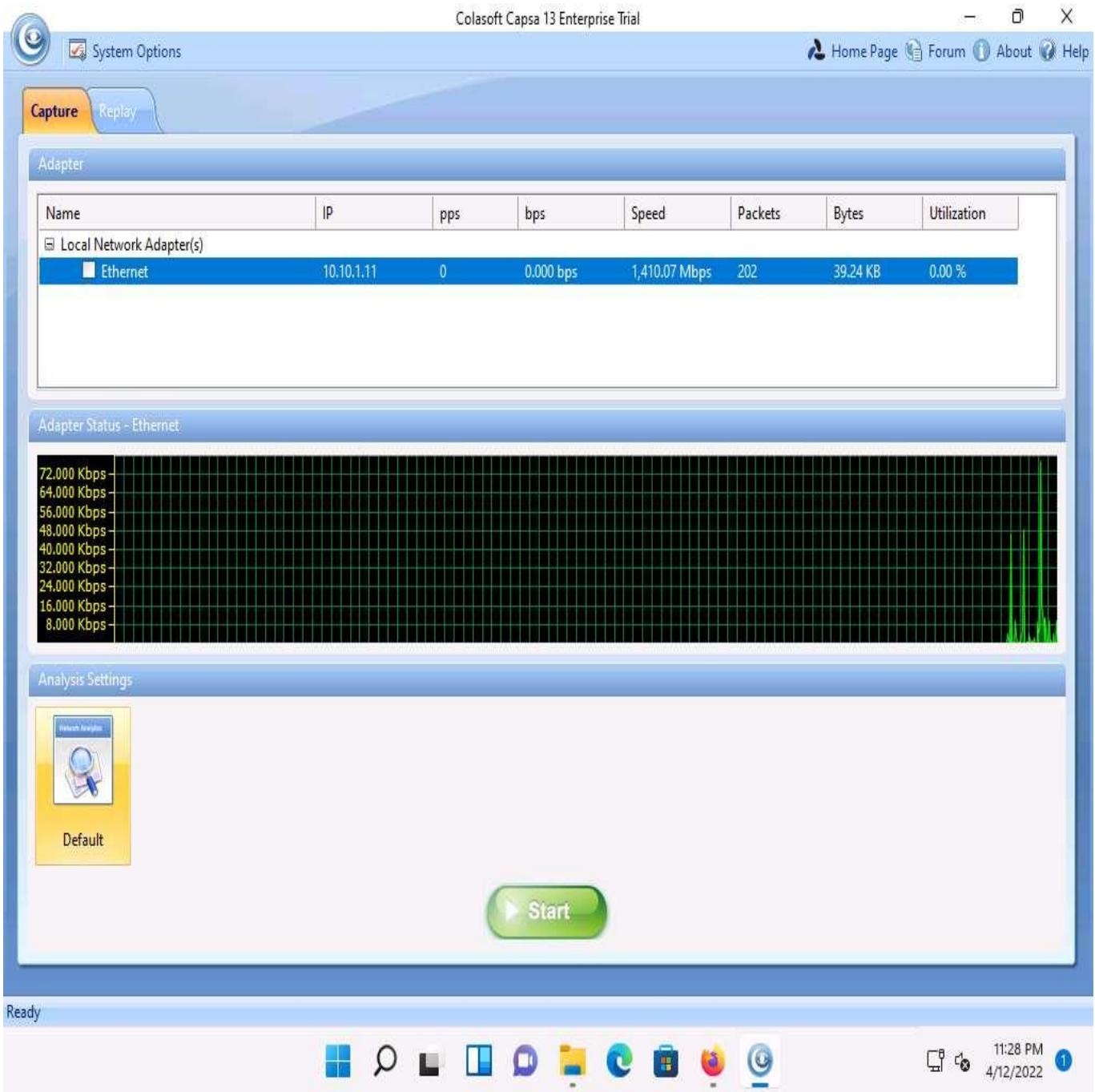
16. Now, minimize the browser window and switch to the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window and paste the copied serial number in the **Serial Number** field. Ensure that **Activate online (Recommended)** radio button is selected and click on **Next**.



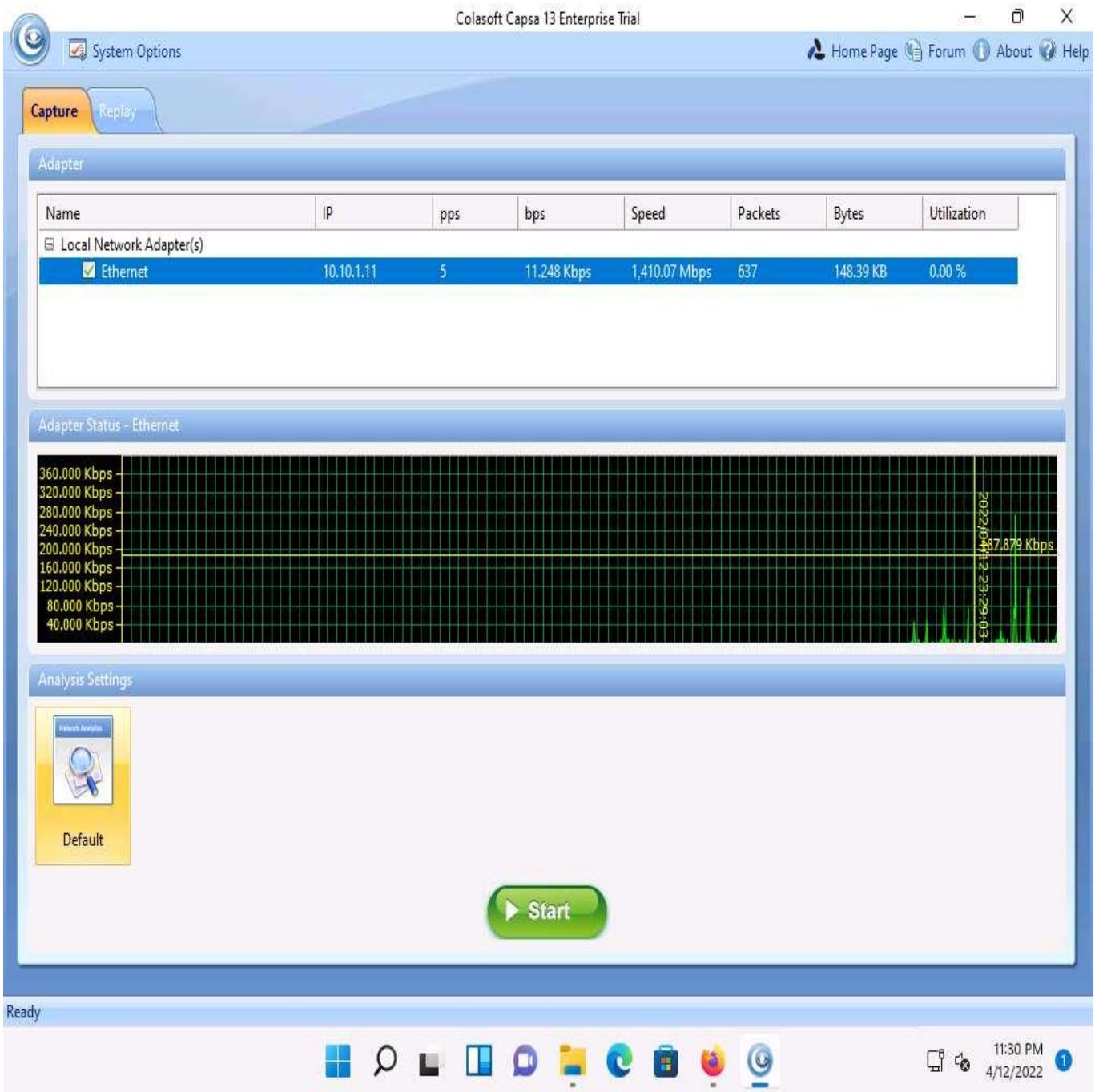
17. A **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window appears, showing that the software has been successfully activated, click on **Finish**.



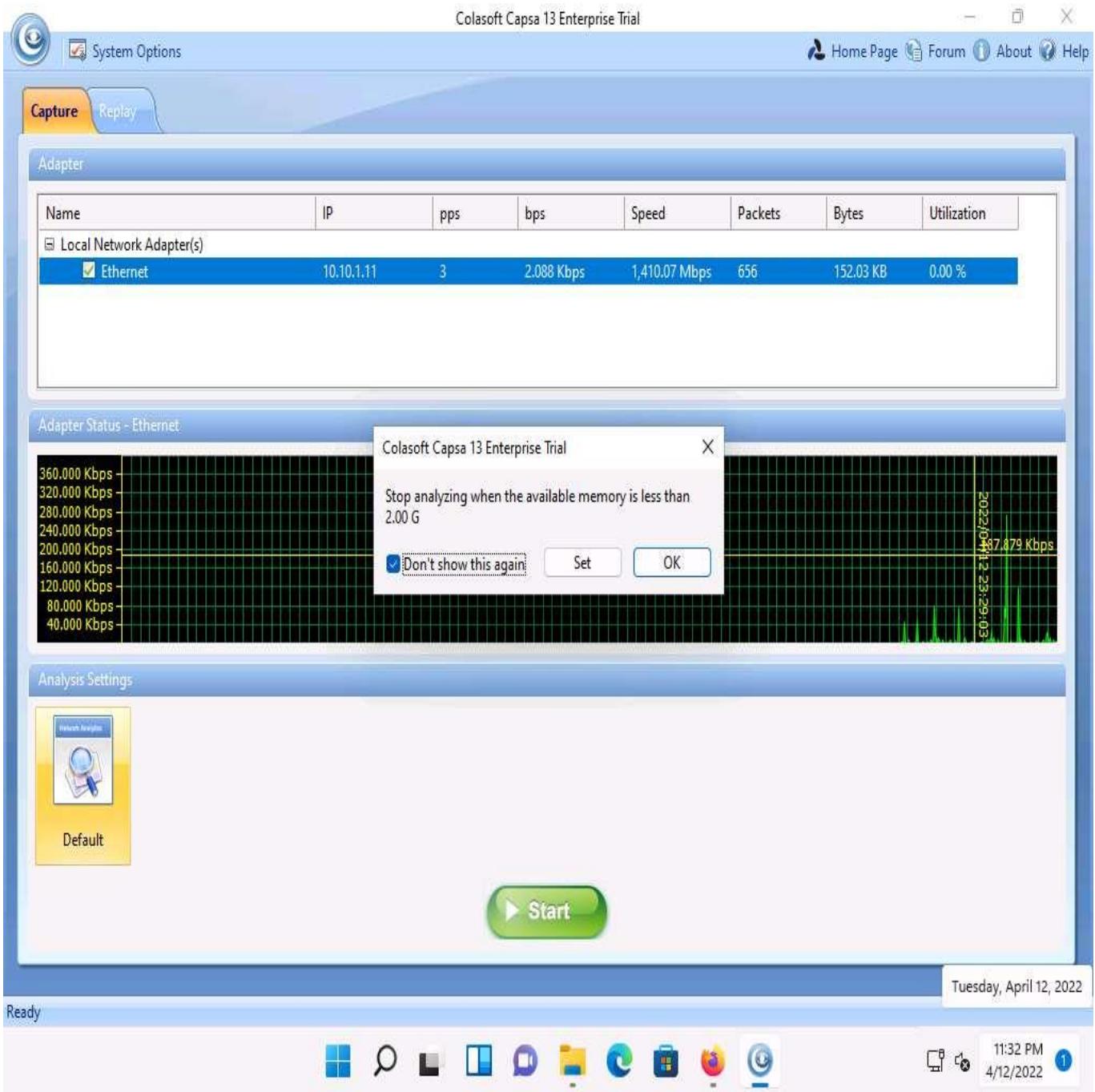
18. After successful installation, A **Colasoft Capsa 13 Enterprise Trial** window appears.



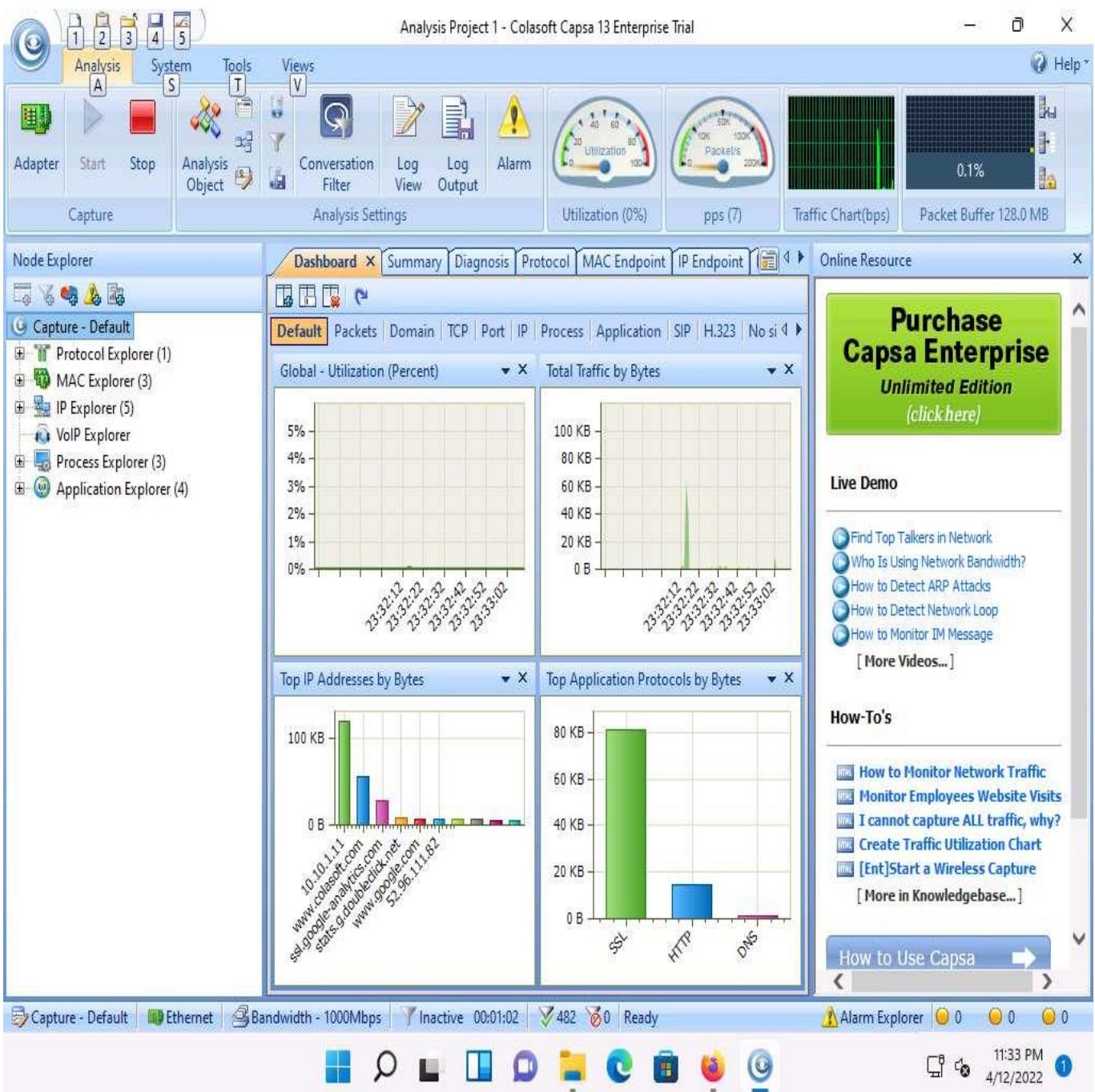
19. In the **Colasoft Capsa 13 Enterprise Trial** window check the checkbox beside the available adapter (here, **Ethernet**) and click on **Start**.



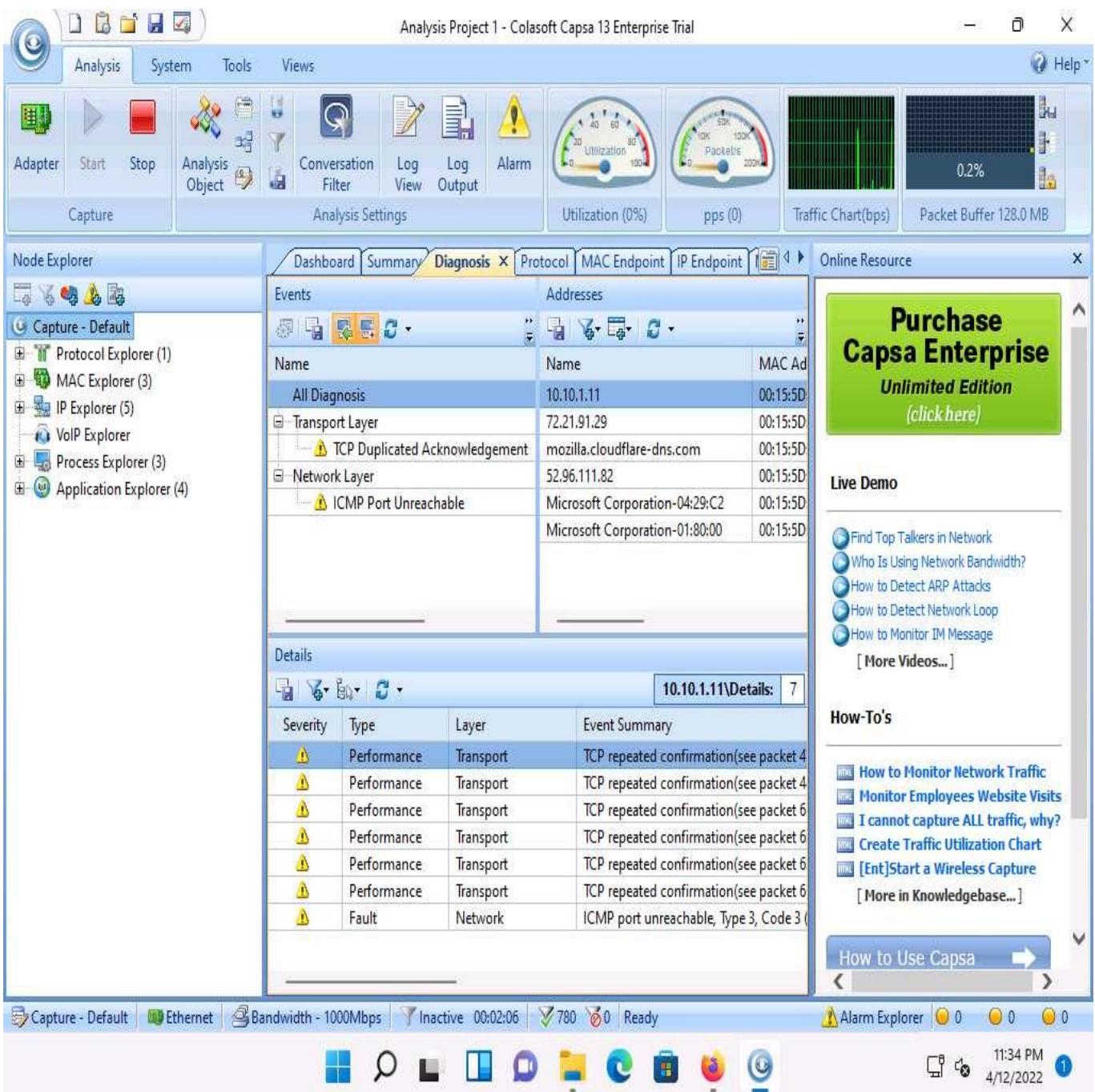
20. If a **Colasoft Capsa 13 Enterprise Trial** pop-up appears, select **Don't show this again** checkbox and click on **OK**.



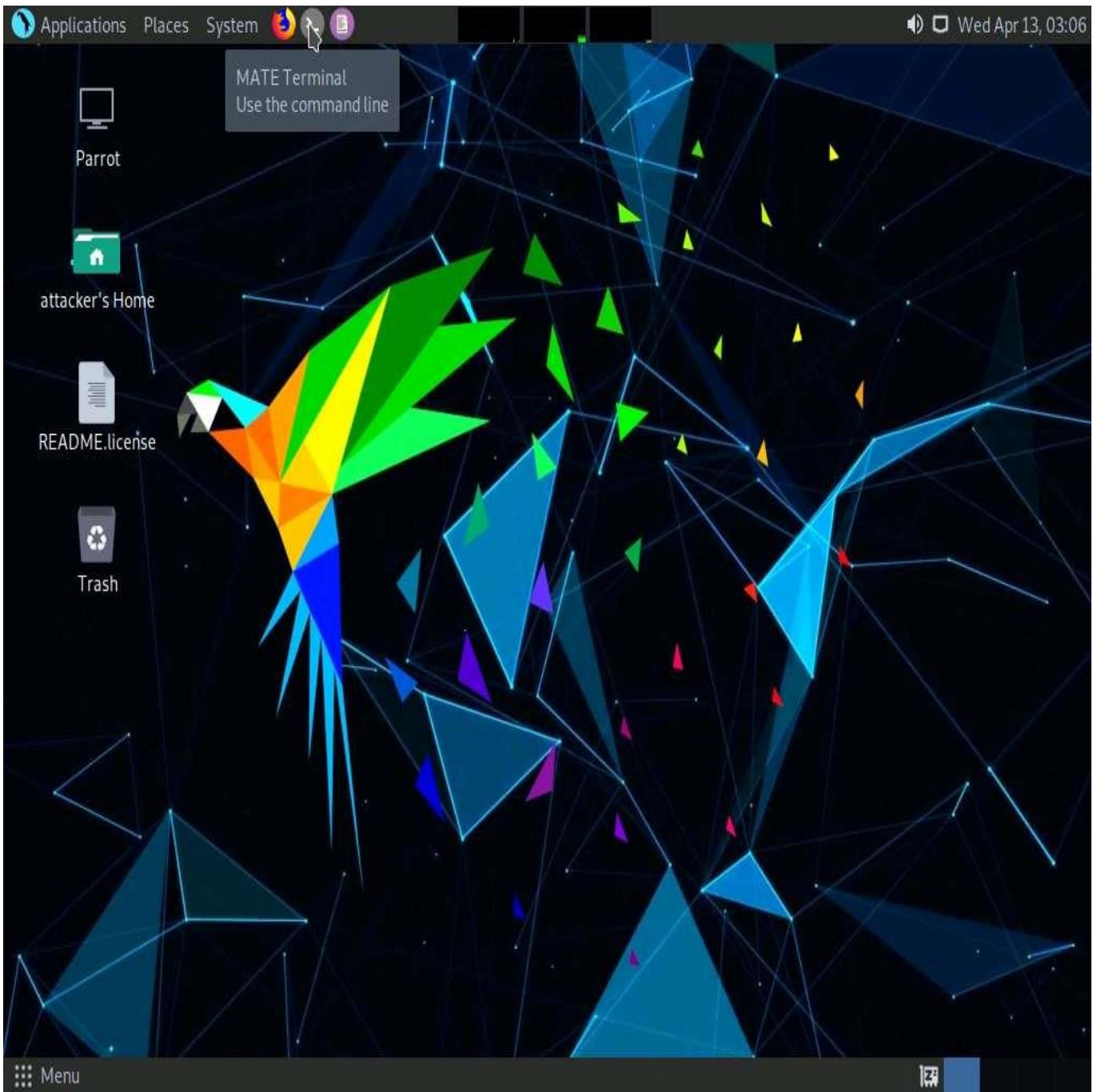
21. The **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window appears, as shown in the screenshot.



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

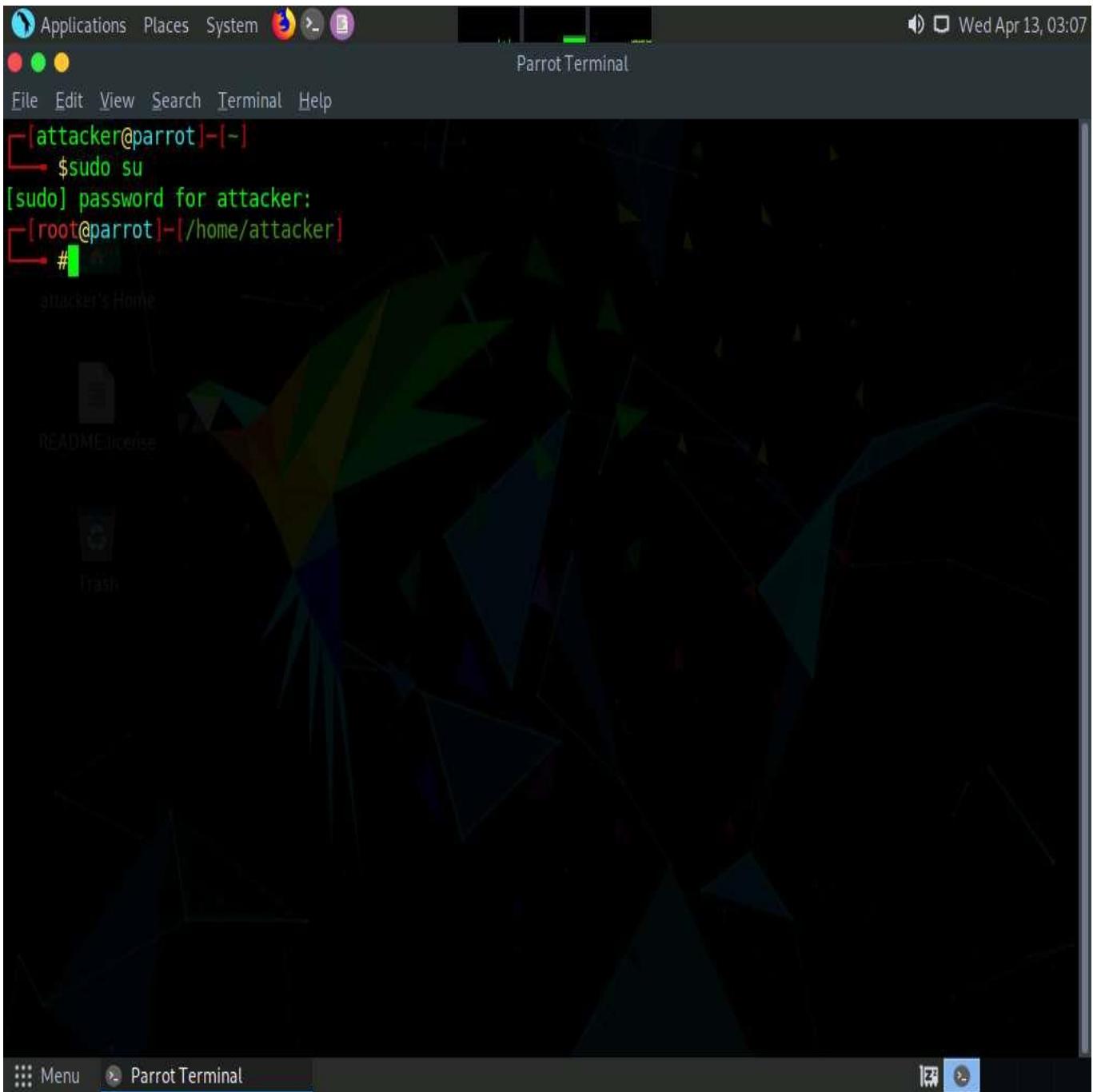


23. Click on **Parrot Security** to switch to **Parrot Security** machine.
24. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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**.

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.

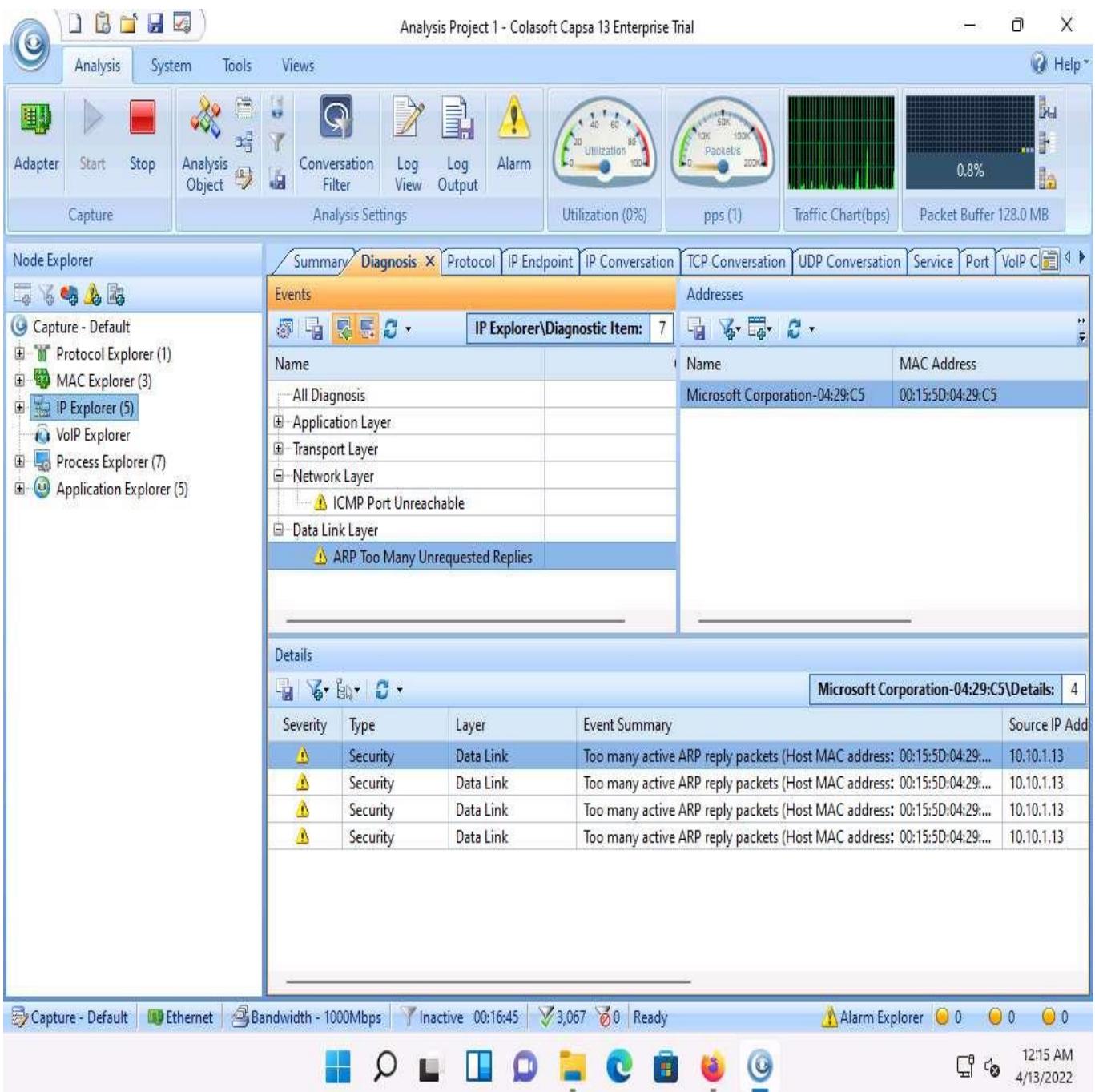
The above command sends ARP '**is-at**' packets to the specified victim(s), poisoning their ARP tables to send their traffic to the attacker system.

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

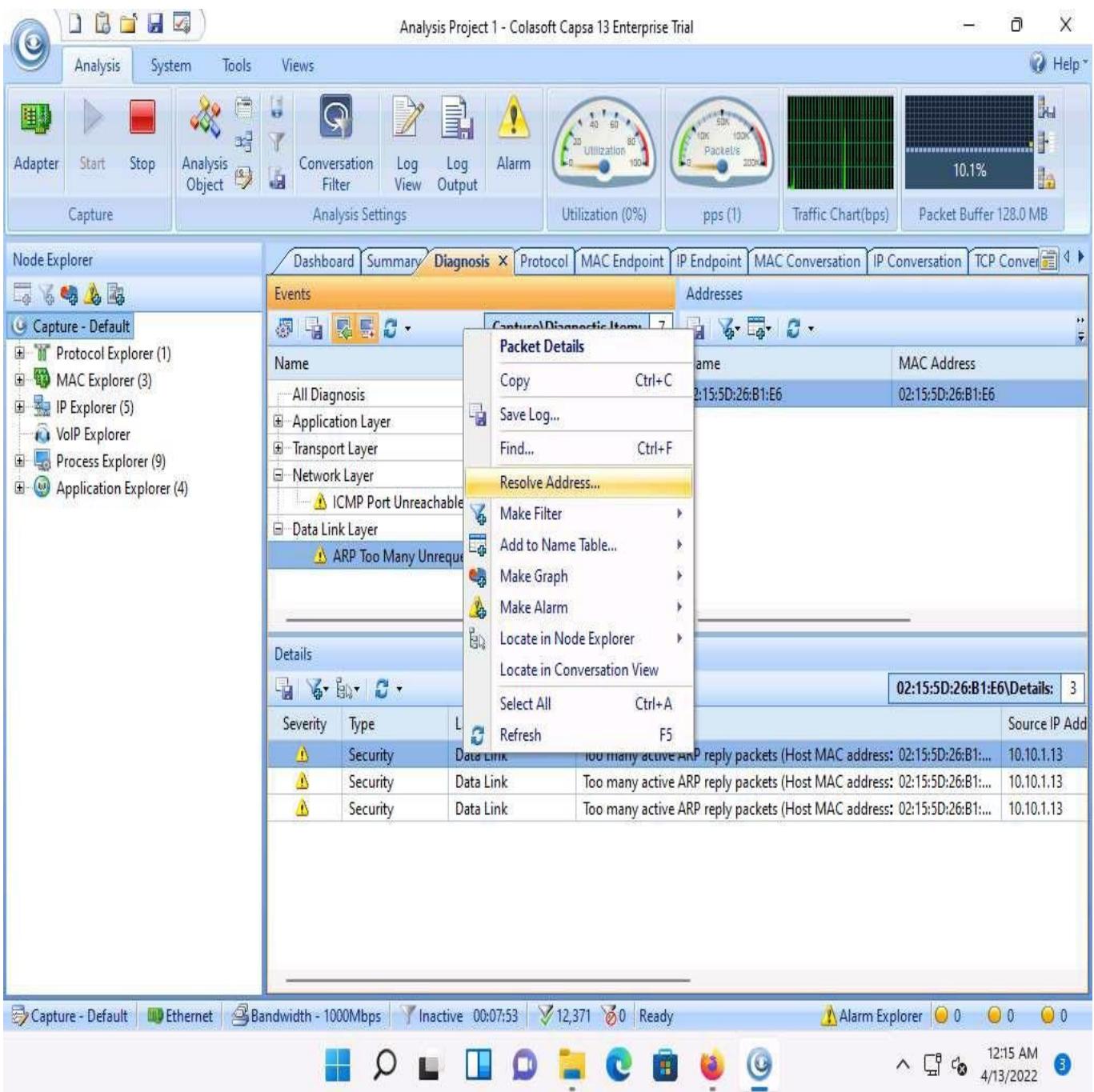
```
[attacker@parrot] ~ [~]
$ sudo su
[sudo] password for attacker:
[root@parrot] ~ [/home/attacker]
# habu.arp.poison 10.10.1.11 10.10.1.13
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether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

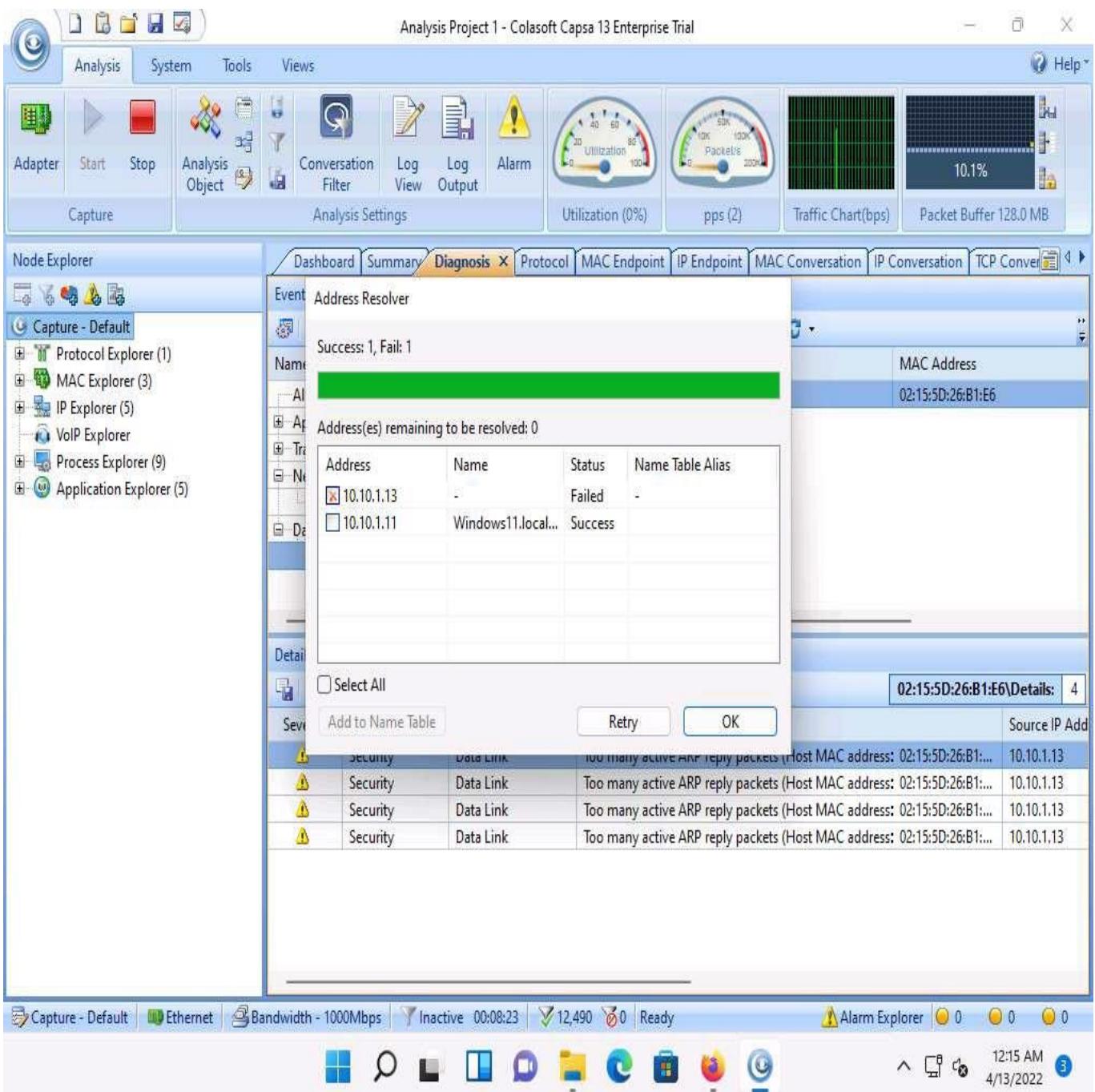
It will take approximately **10** minutes for the tool to capture the **ARP** requests.



30. Click on **ARP Too Many Unrequested Replies** warning under **Data Link Layer** node.
31. Right-click on **Security** warning under **Details** section and select **Resolve Address...** from the context menu.

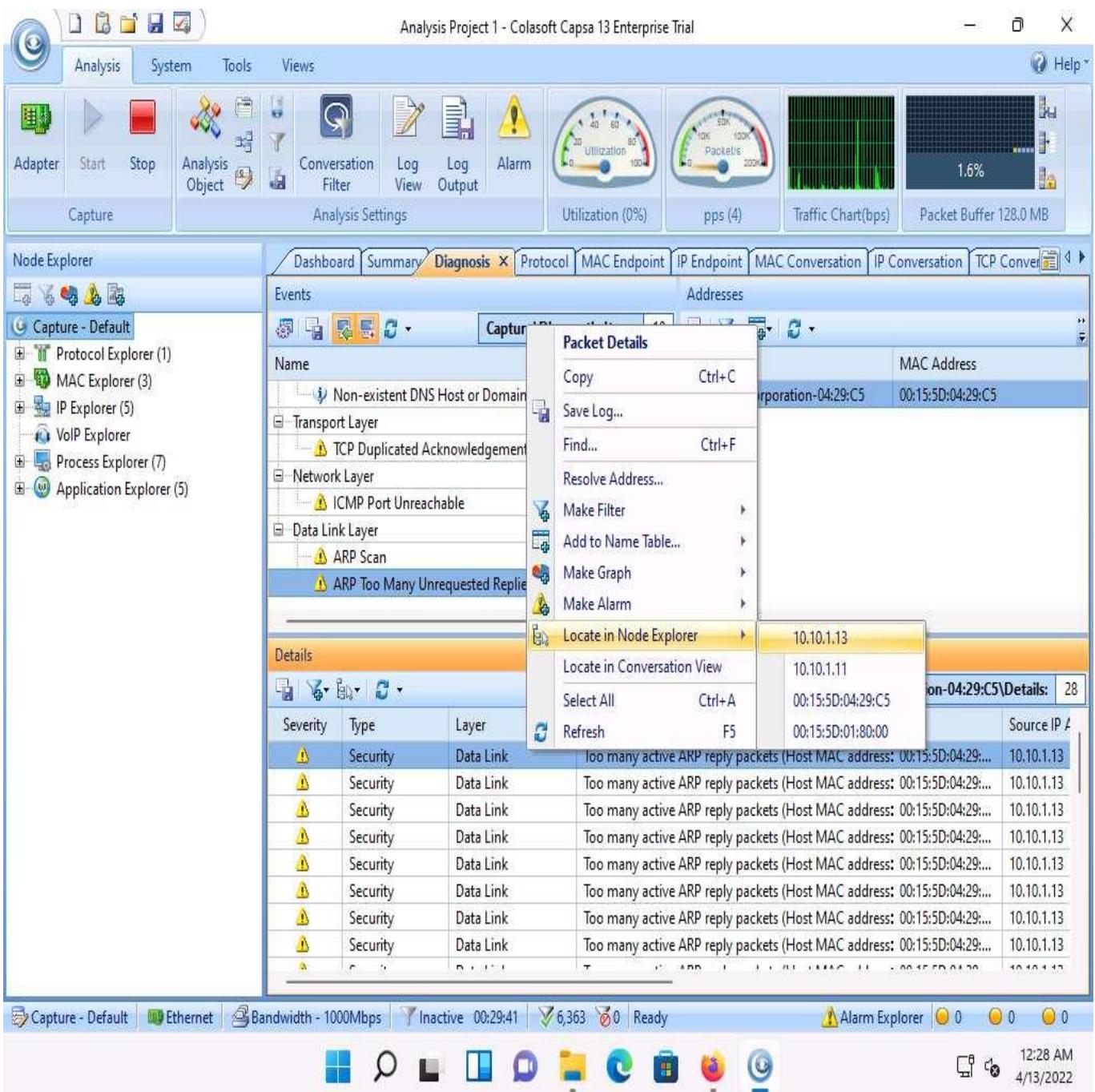


32. An **Address Resolver** pop-up appears, once the address resolving completes click on **OK**.

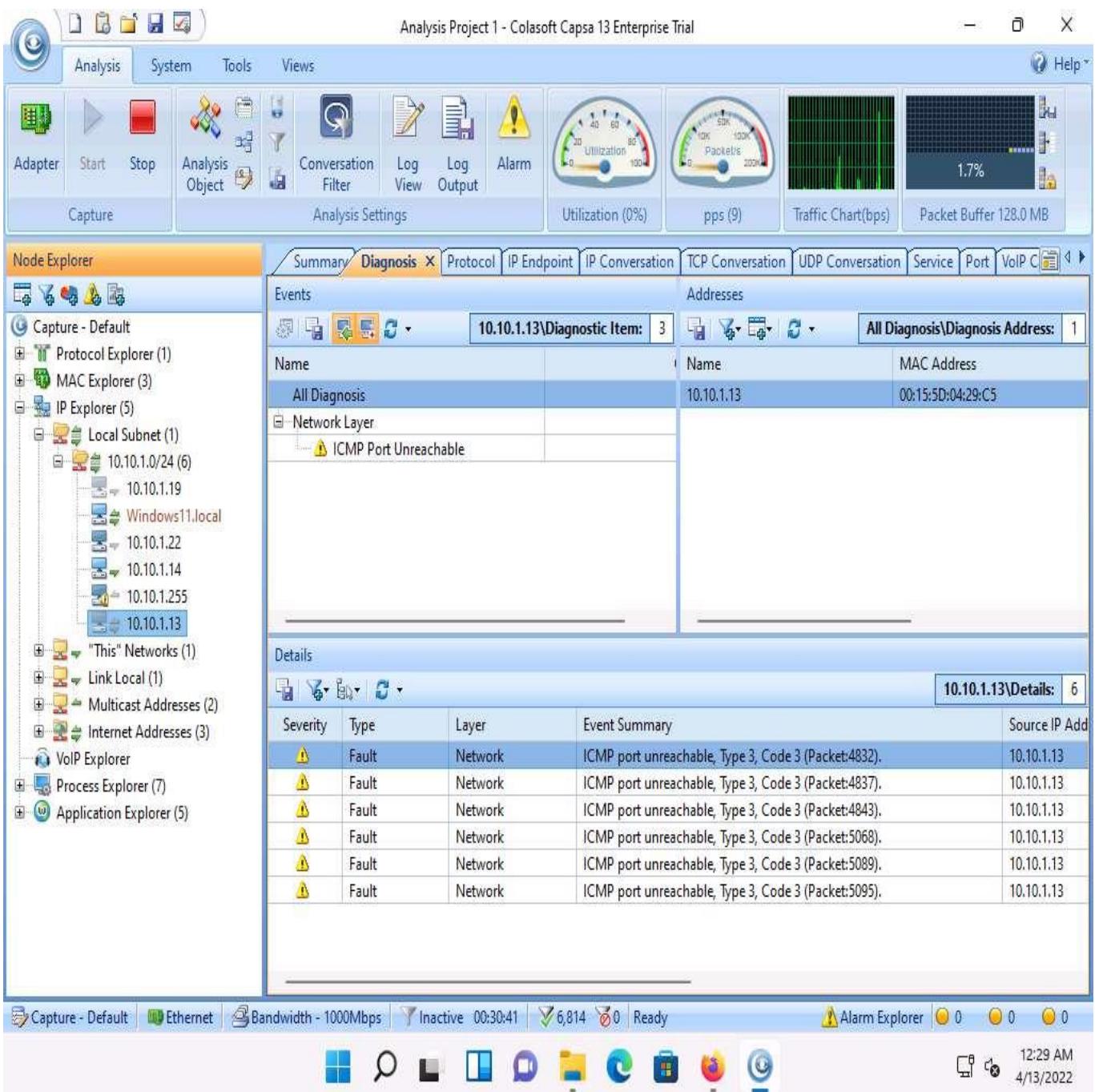


33. Now to locate the Parrot Machine's IP address click on **Capture Default** option under **Node Explorer** section in the left-pane.
34. Right-click any warning in the **Details** tab and click on **Locate in Node Explorer** and select **Parrot Security** machine's IP address from the list (here, **10.10.1.13**).

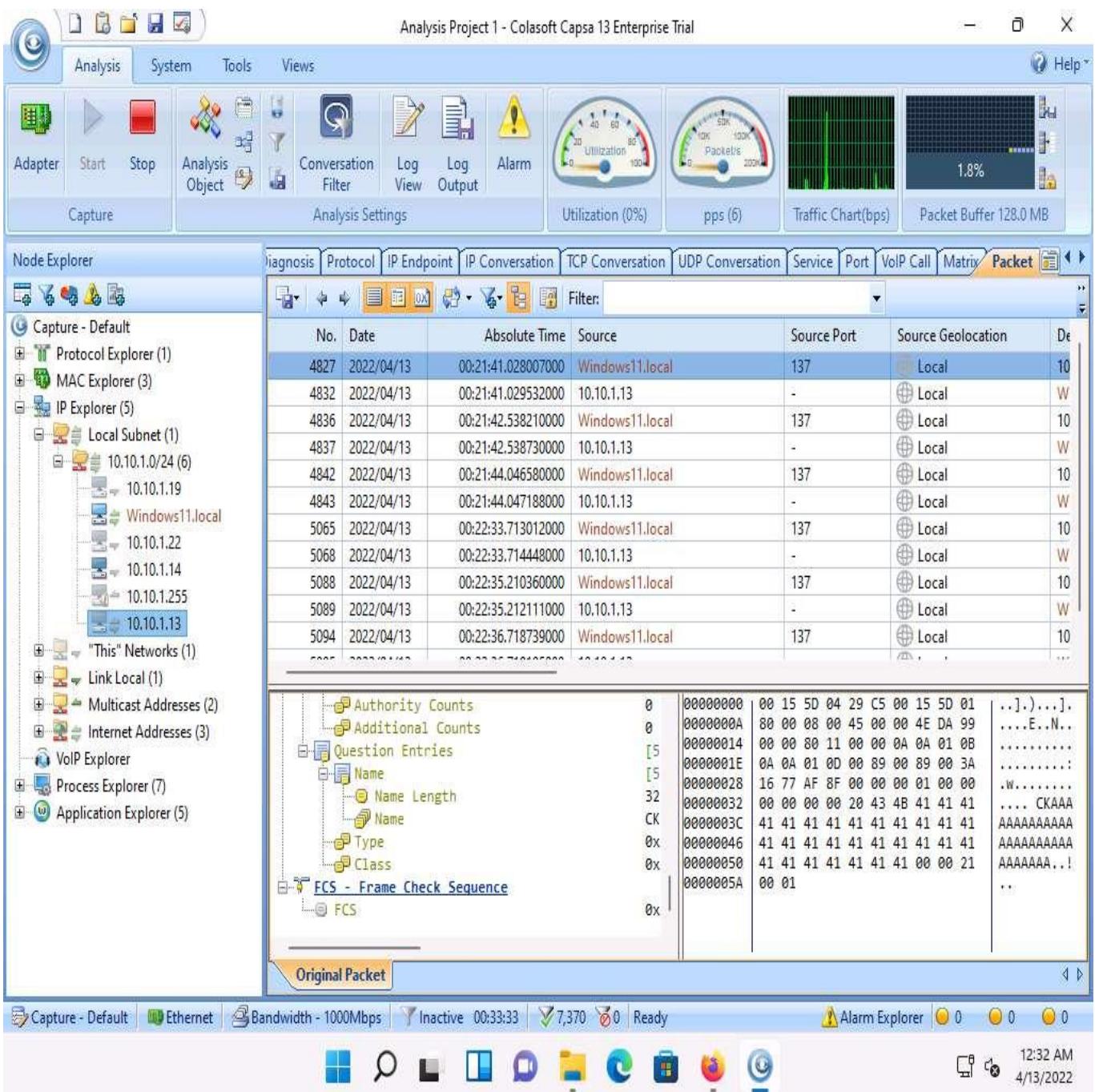
Here, the IP address of the Parrot Security machine is the attacker's IP address.



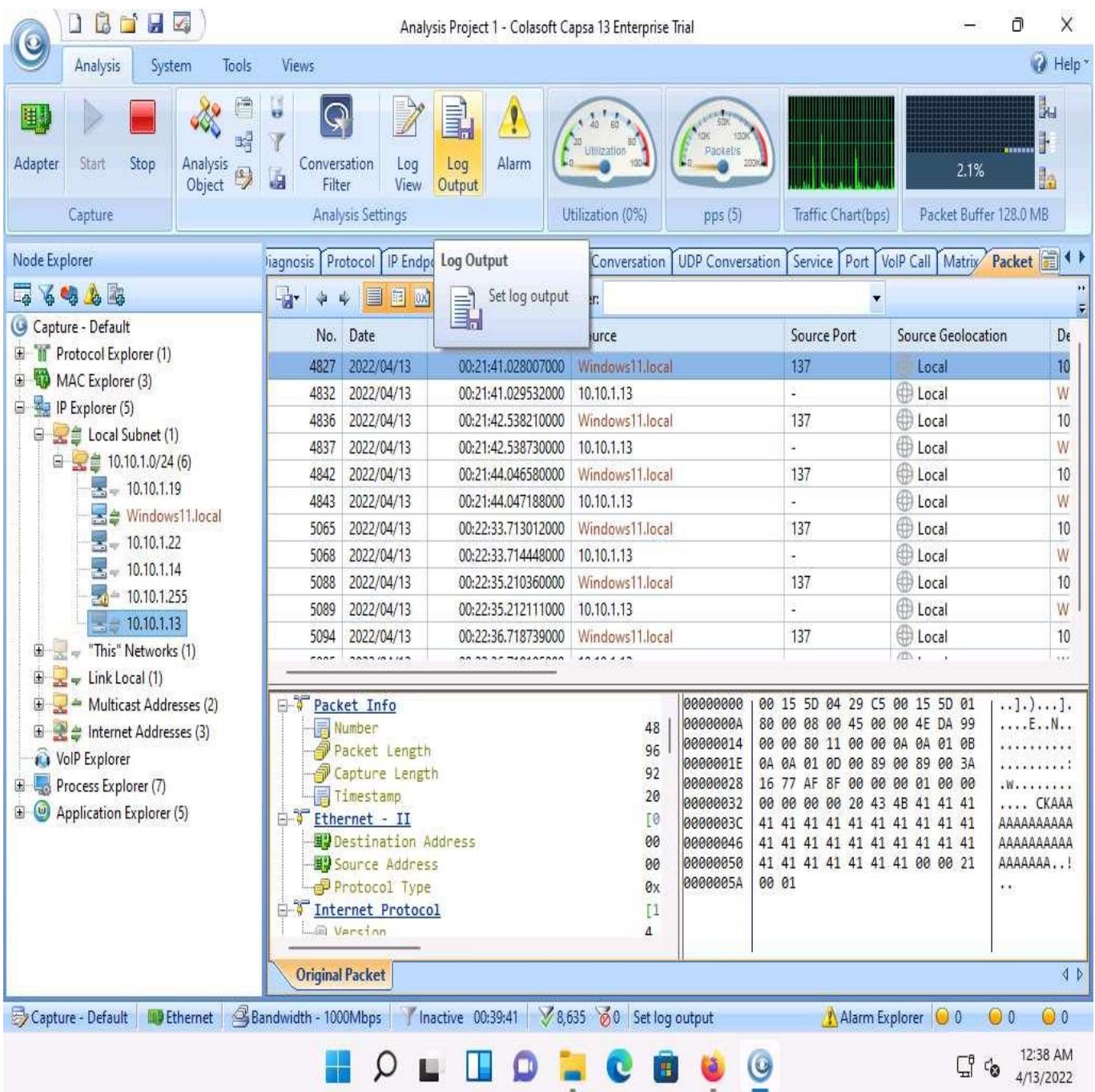
35. The IP address of the Parrot Security machine is displayed under **Node Explorer** section in the left-pane.



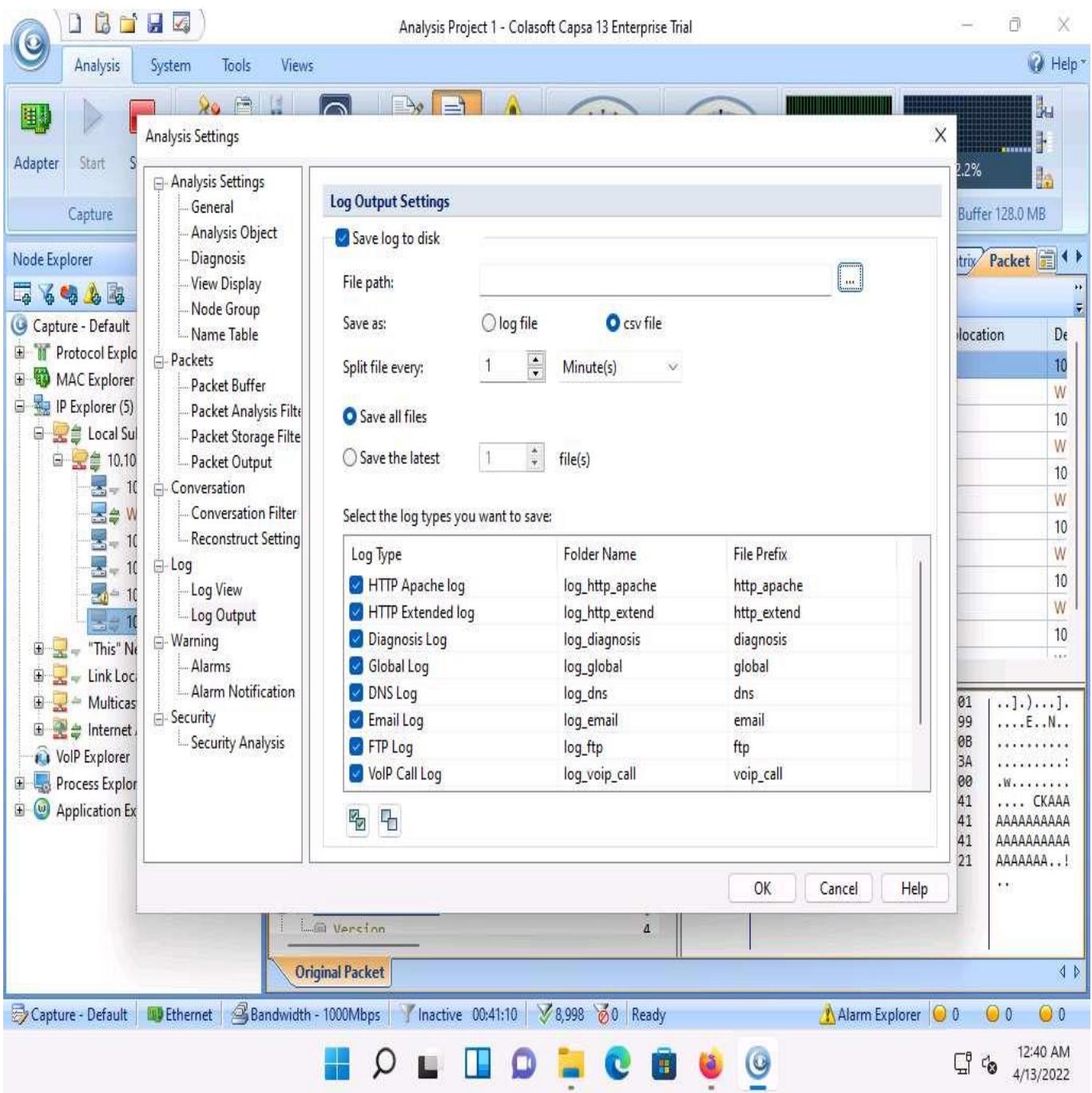
36. Now click on **Packet** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window, to check the packets transferred by the **Parrot Security** machine.



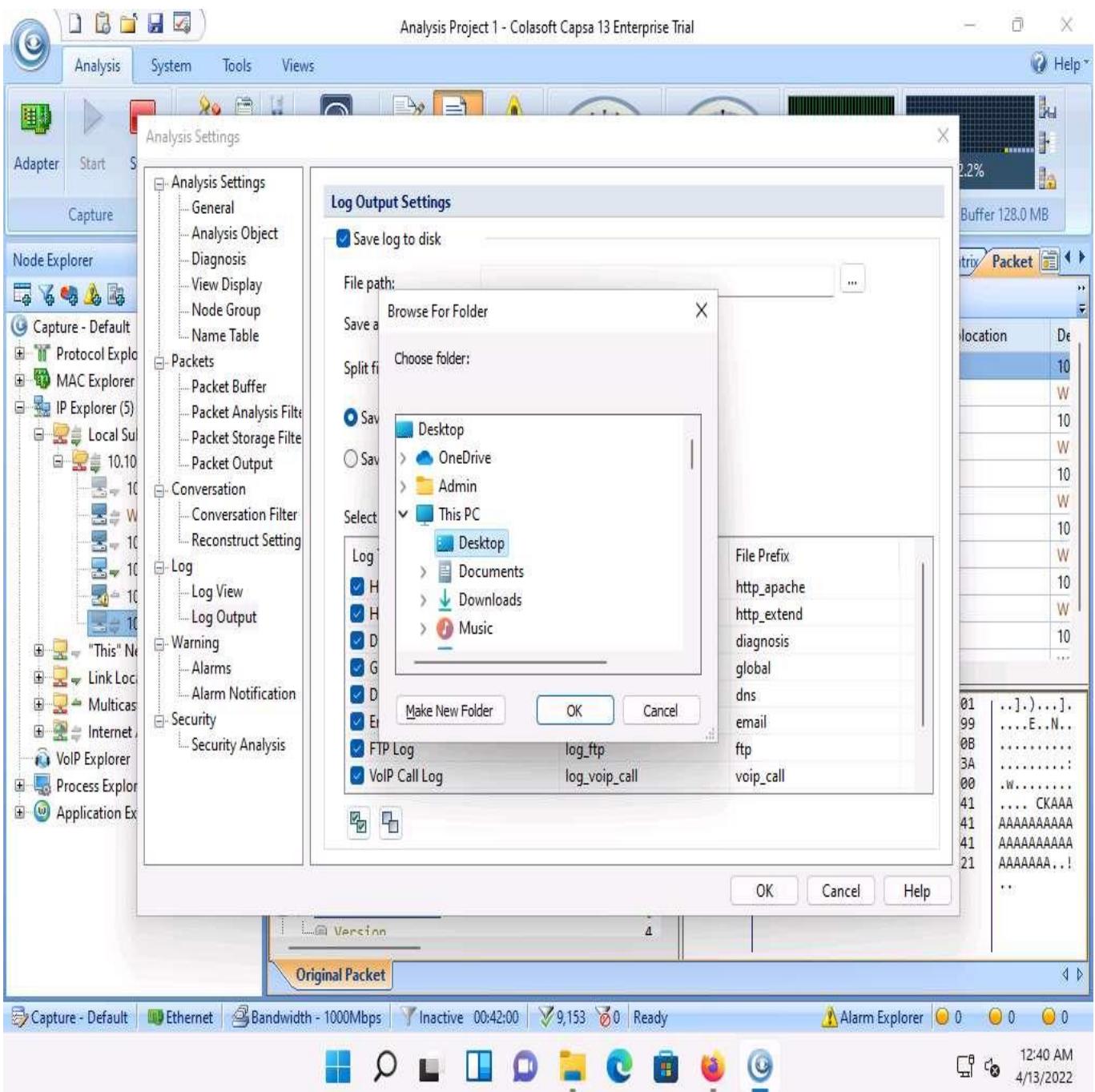
37. Similarly you can navigate to all the available tabs such as **Protocol, MAC Endpoint, IP Endpoint, MAC Conversation, IP Conversation** etc.
38. After completing the analysis click on **Log Output** option from the menubar.



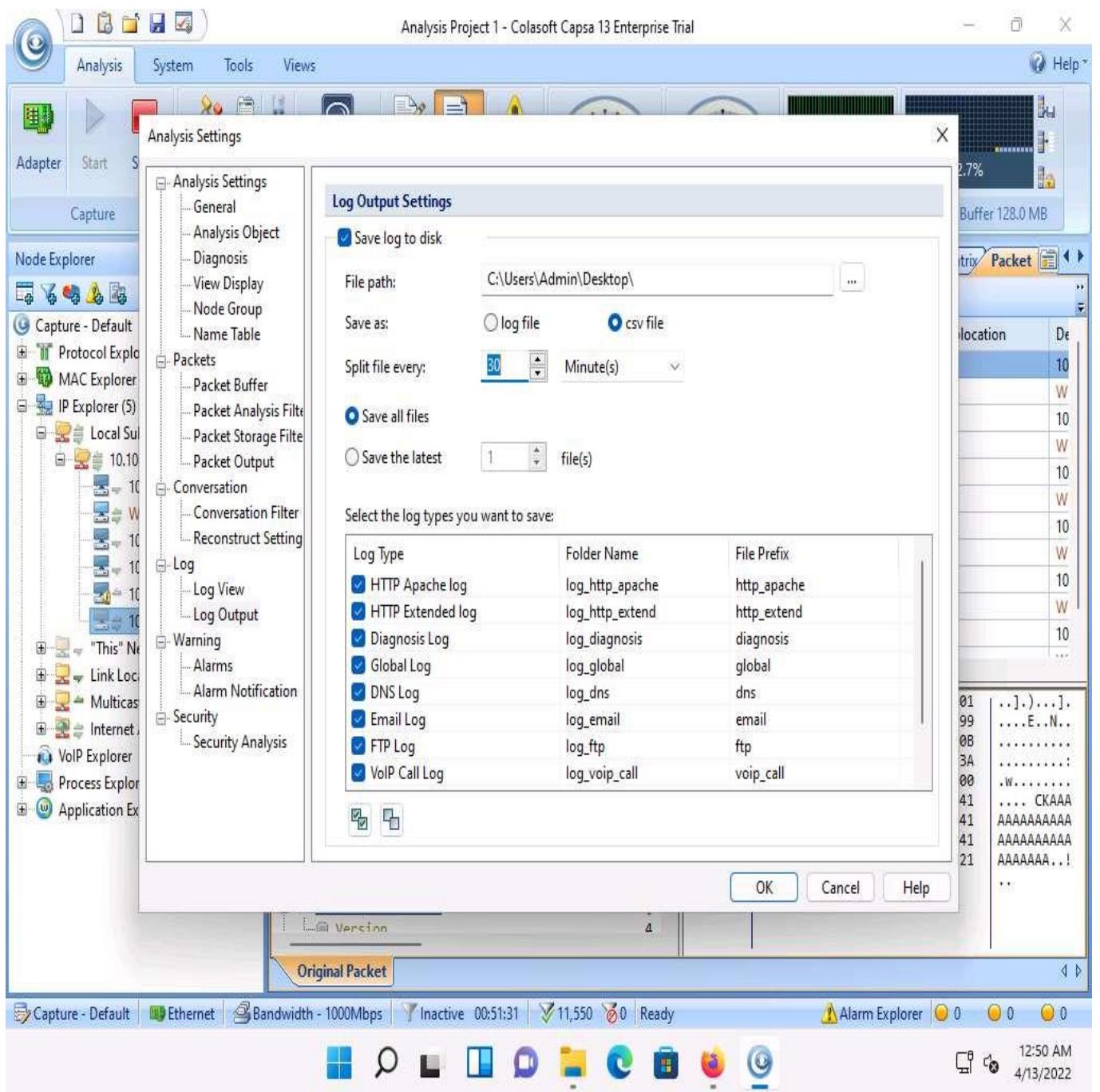
39. In the **Analysis Settings** window, check the **Save log to disk** checkbox and click the ellipsis button under **File path** option.



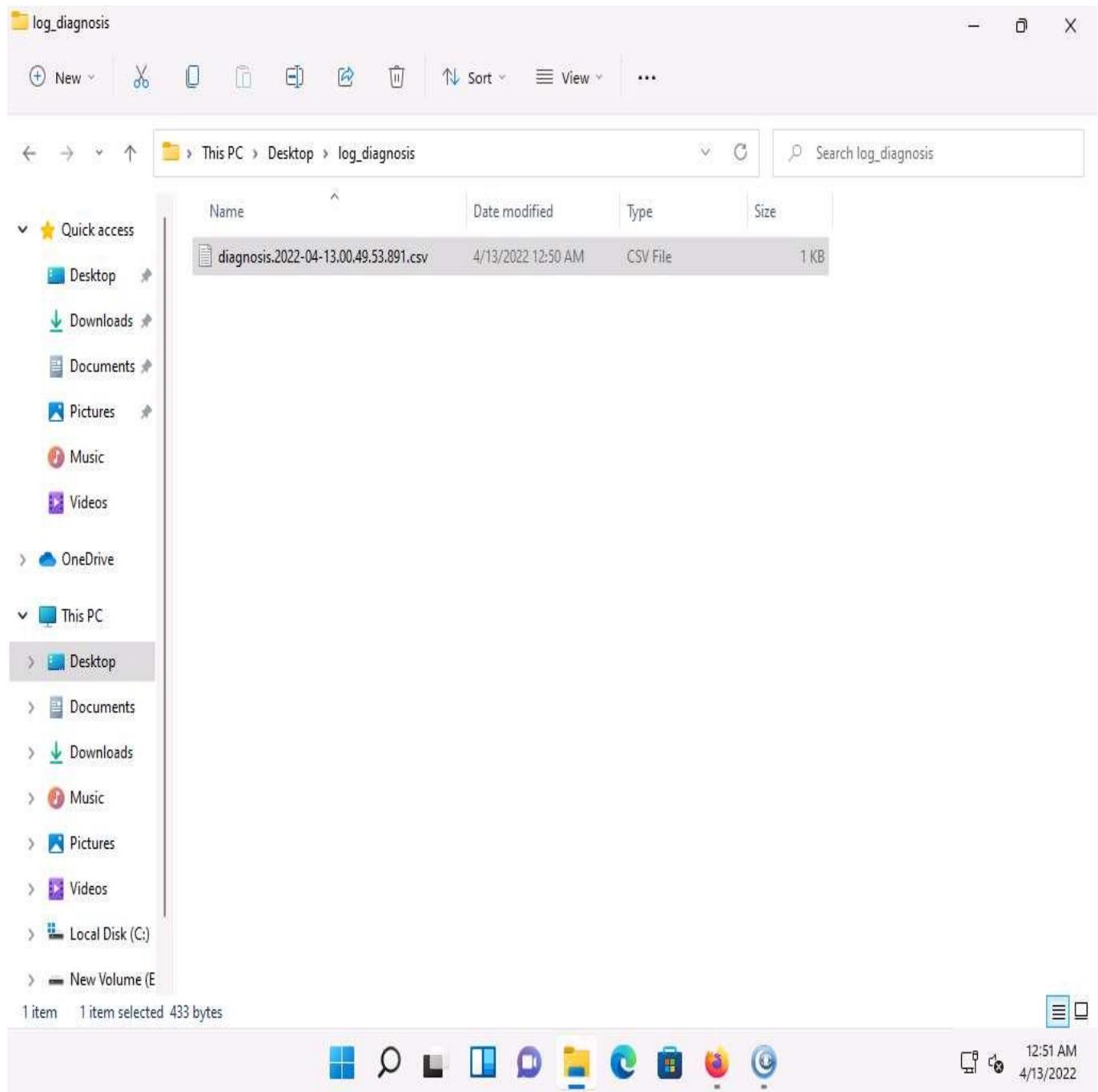
40. In the **Browse For Folder** window, select **Desktop** and click on **OK**.



41. 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**.



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



43. This concludes the demonstration of detecting ARP poisoning using the Capsa Network Analyzer.
 44. Close all open windows and document all the acquired information.
-