Module 08: Sniffing

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.

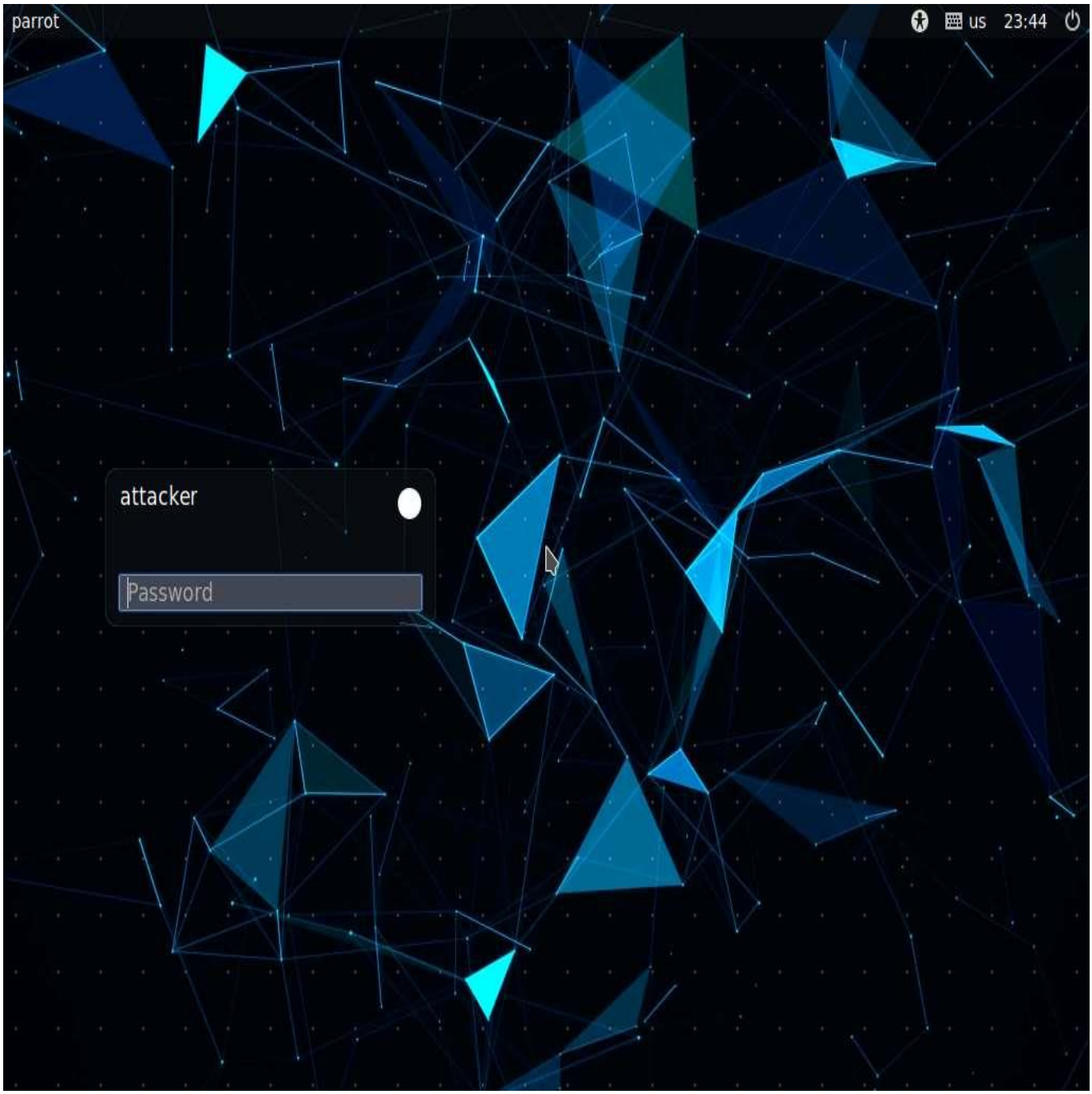
macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating

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.

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.

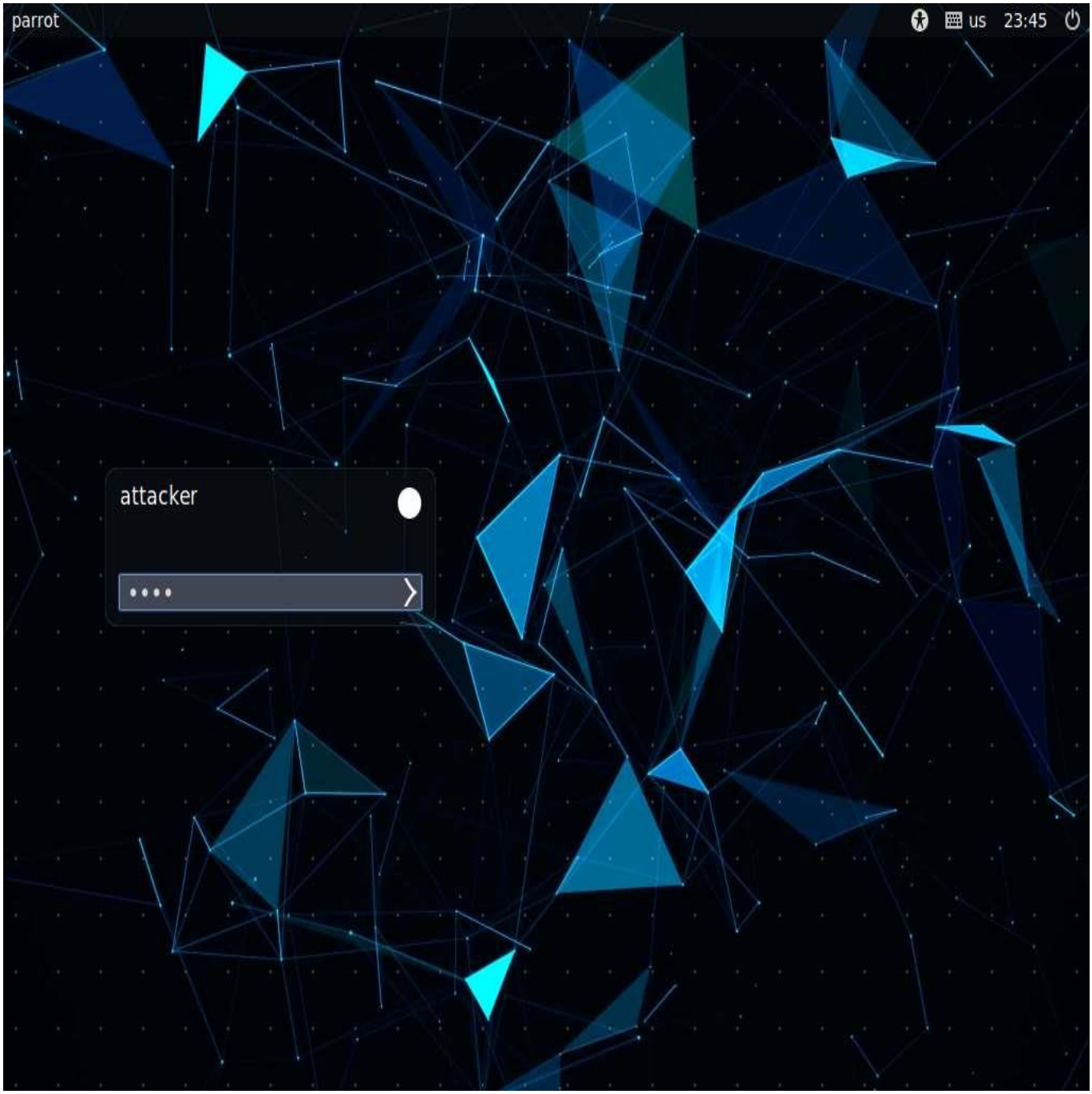
1. Click Parrot Security to switch to the **Parrot Security** machine.



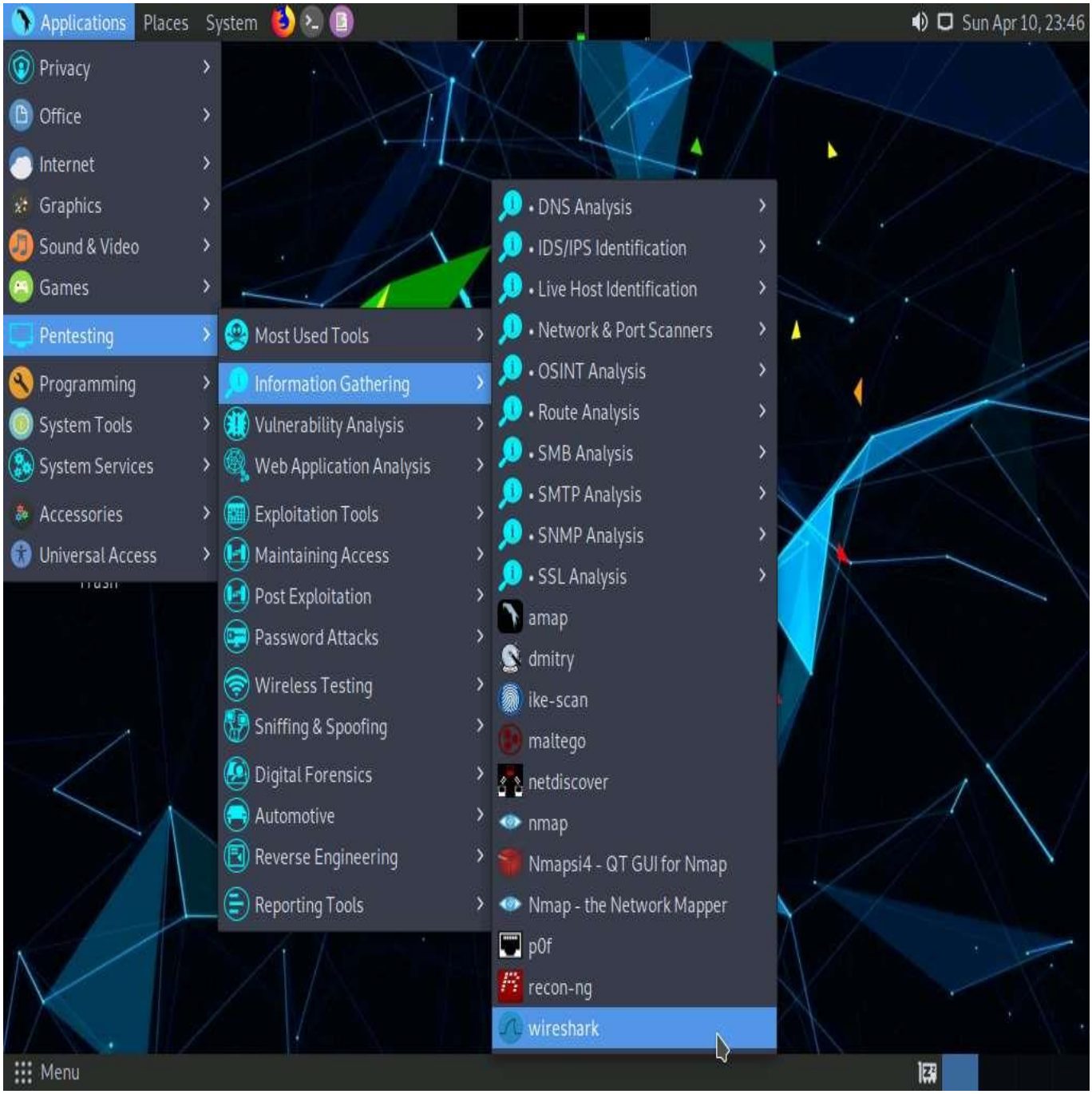
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

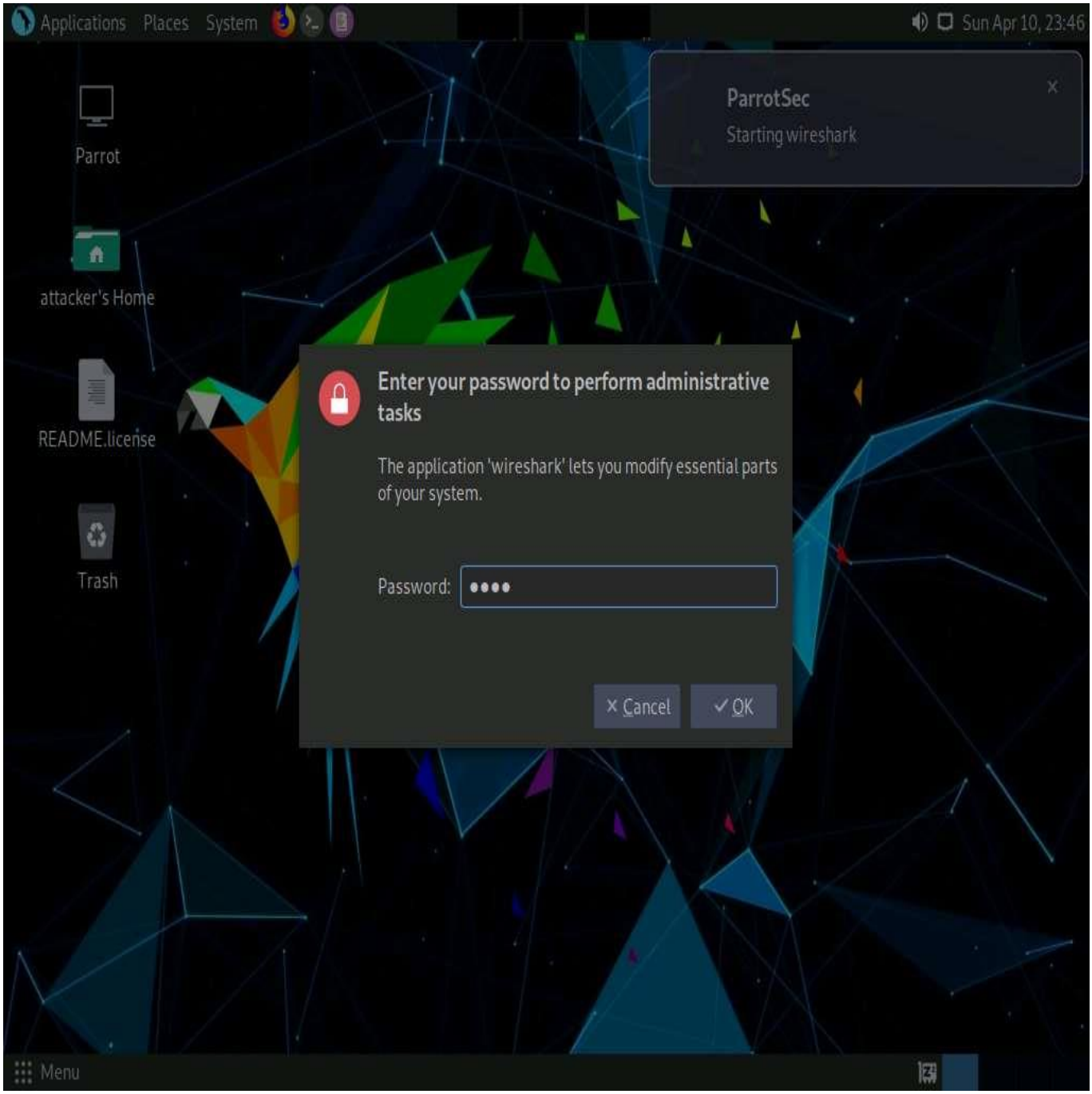
If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



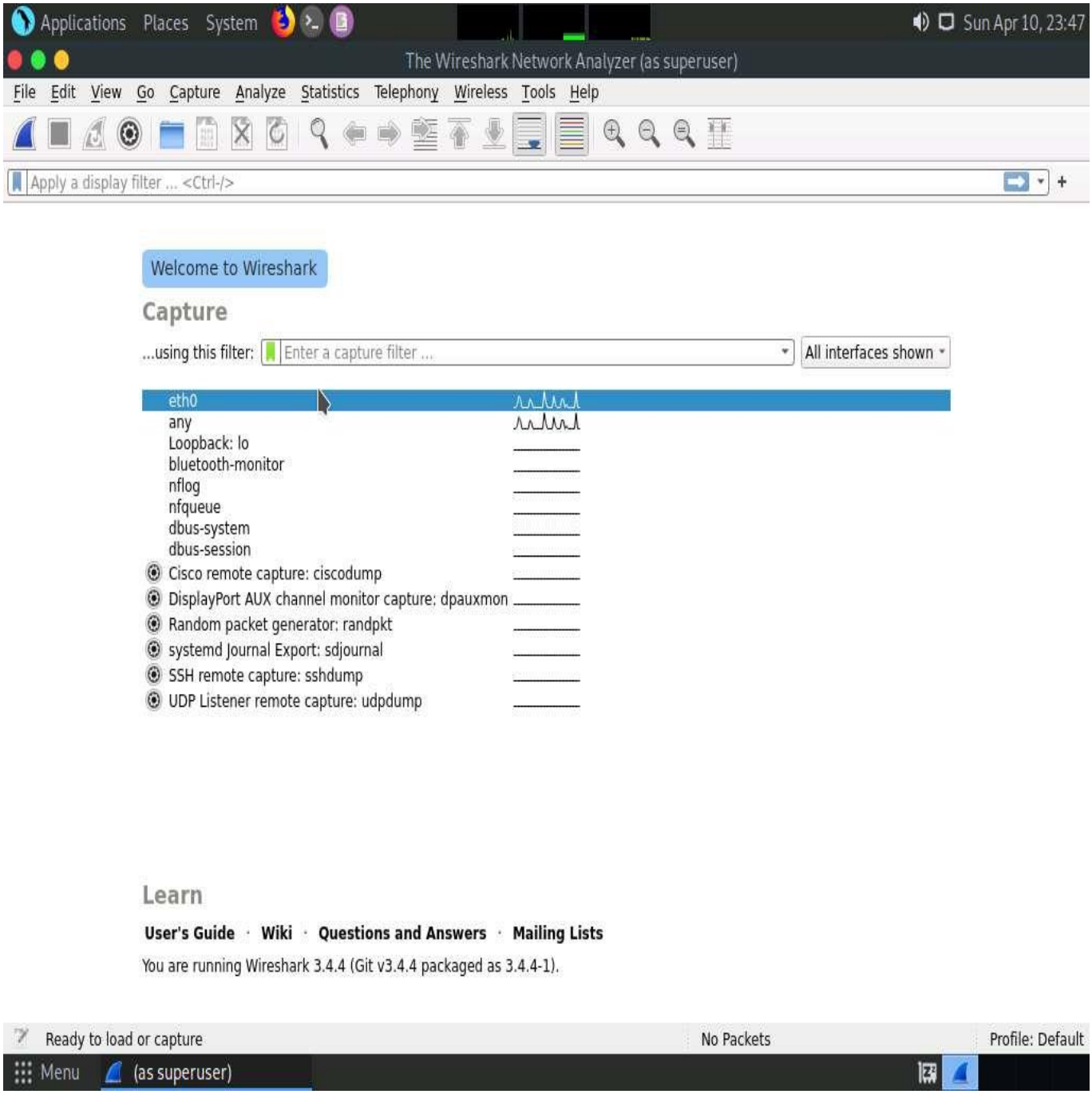
3. ☐ Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



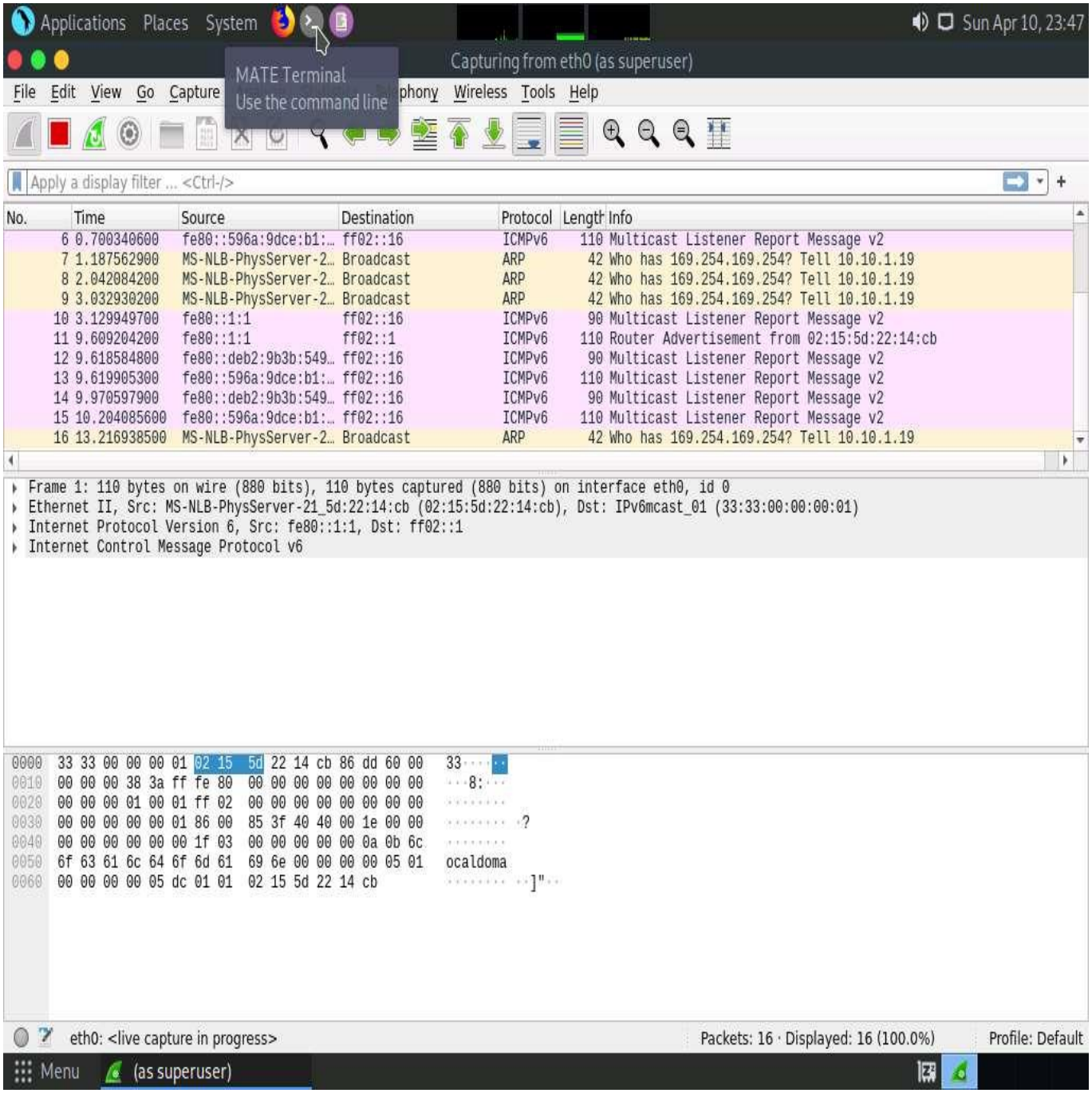
4. ☐ A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



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



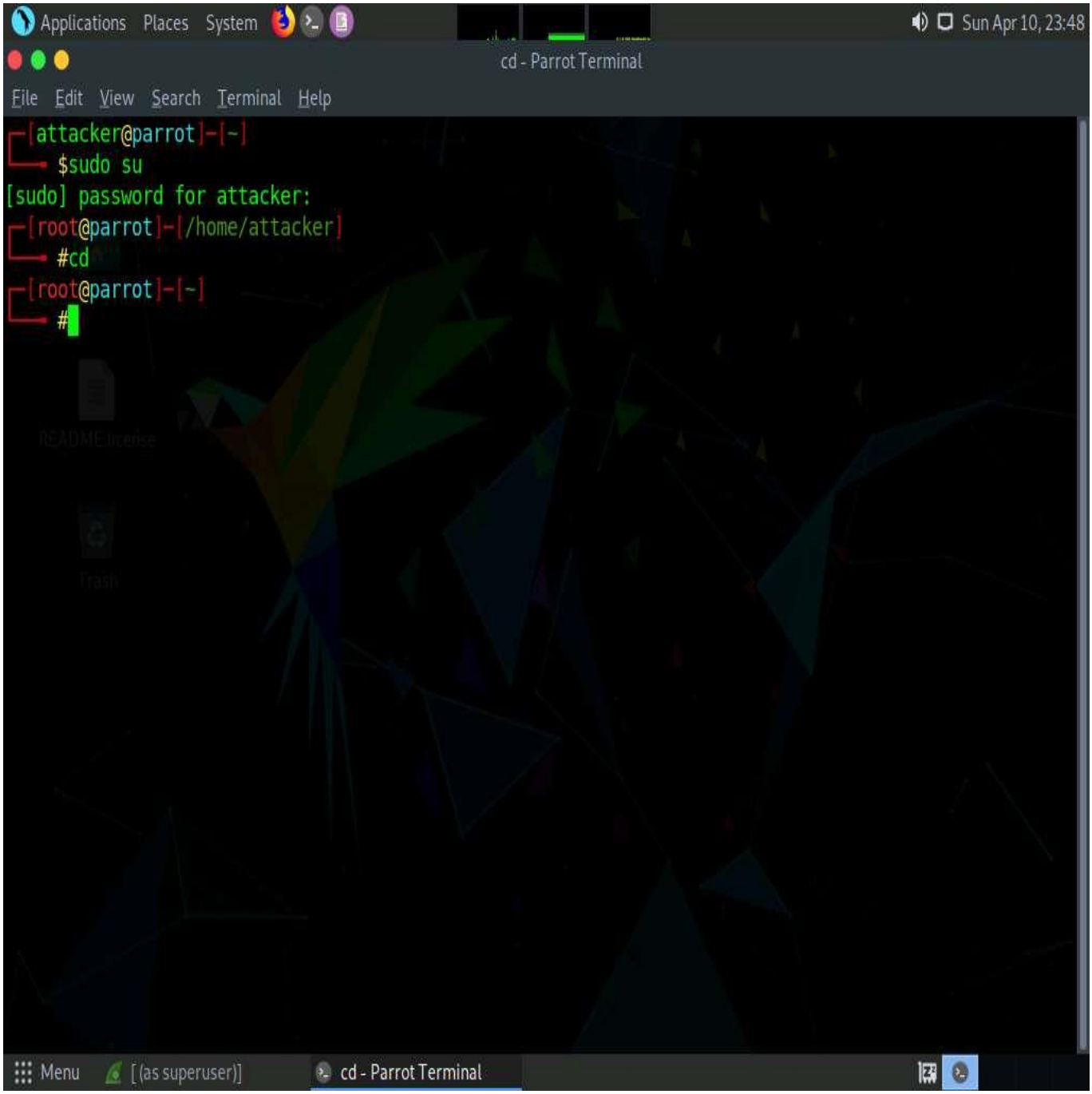
6. ☐ Leave the **Wireshark** application running.
7. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

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

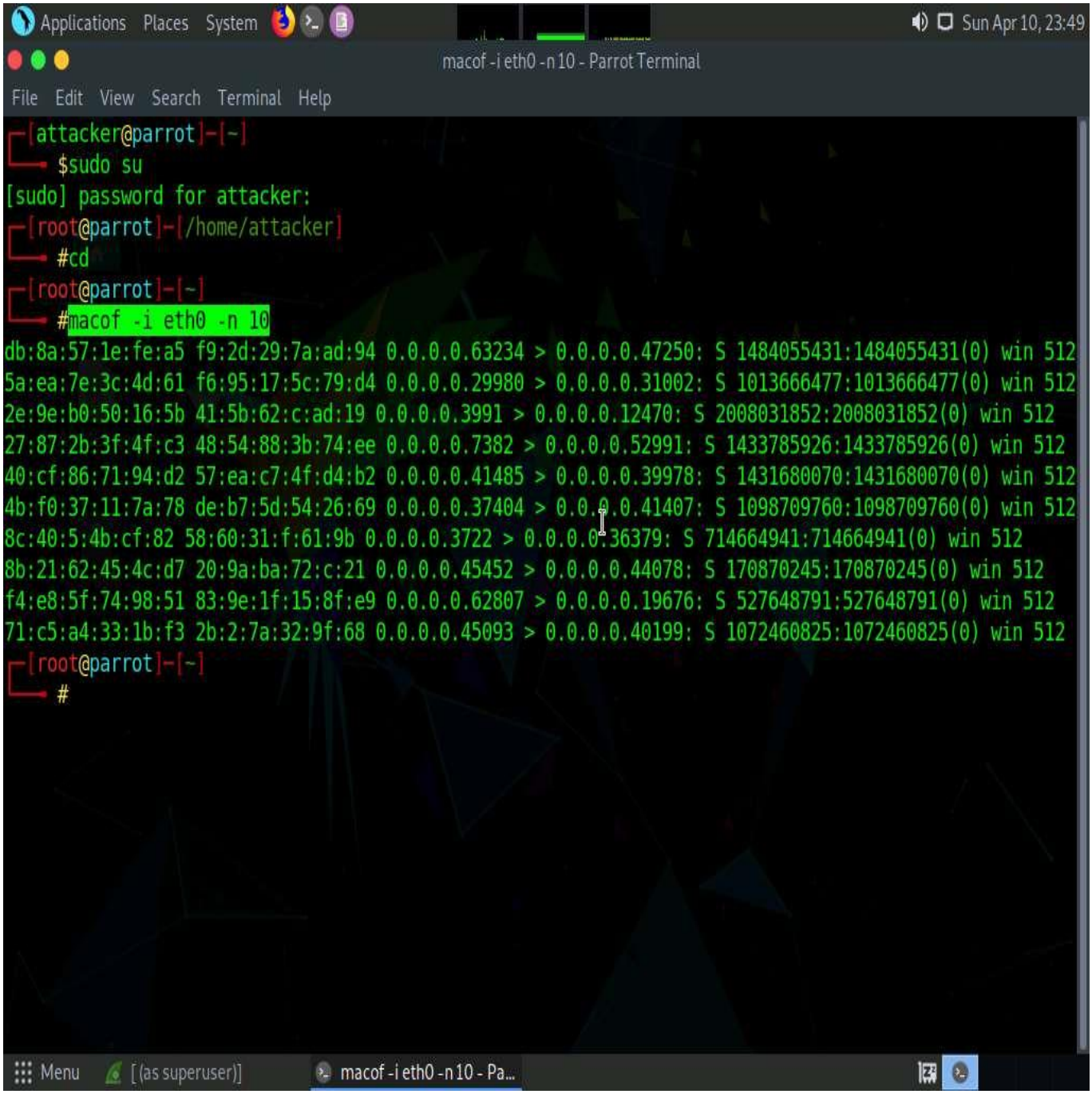


11. ☐ The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.

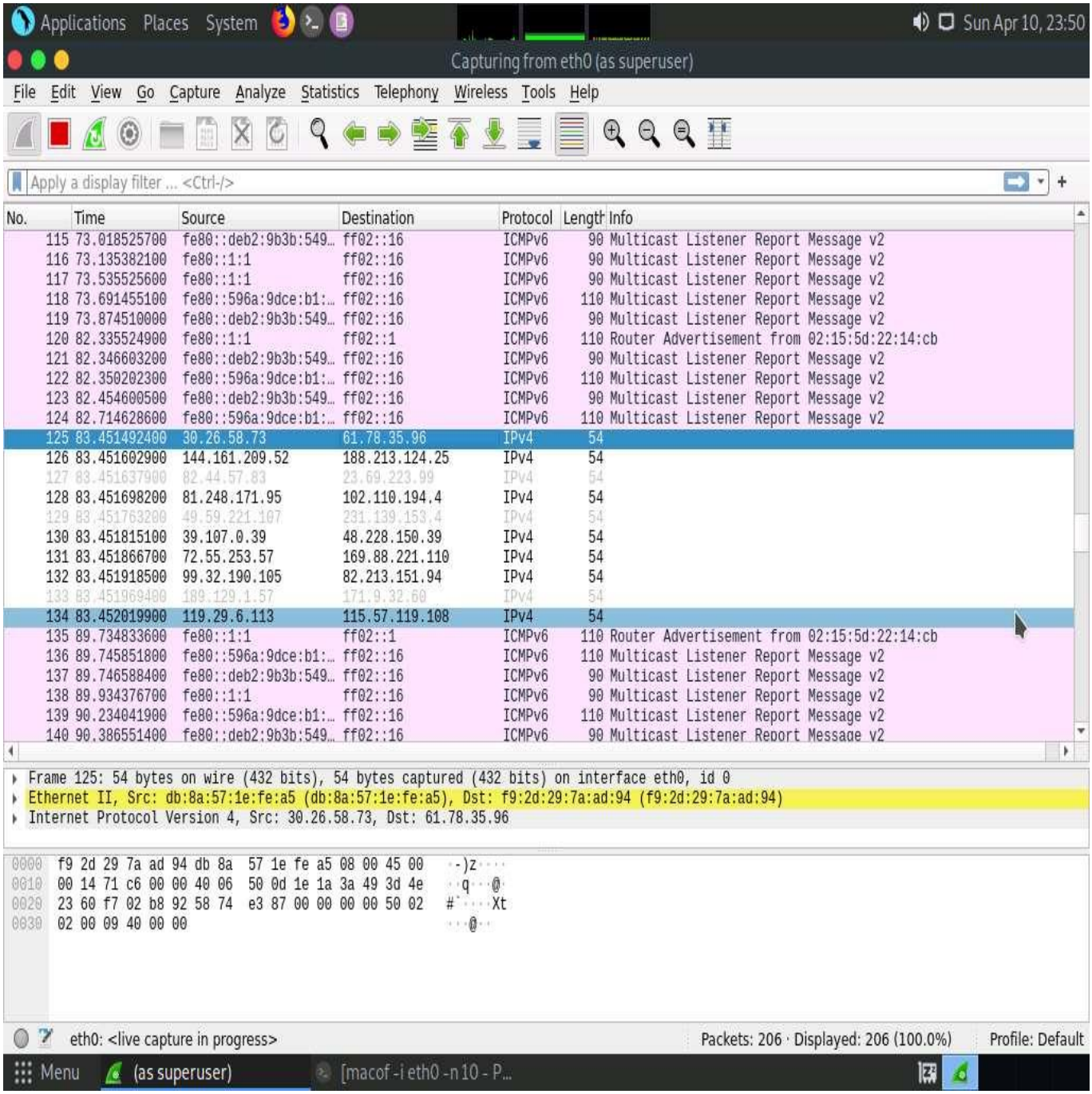
-i: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).

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

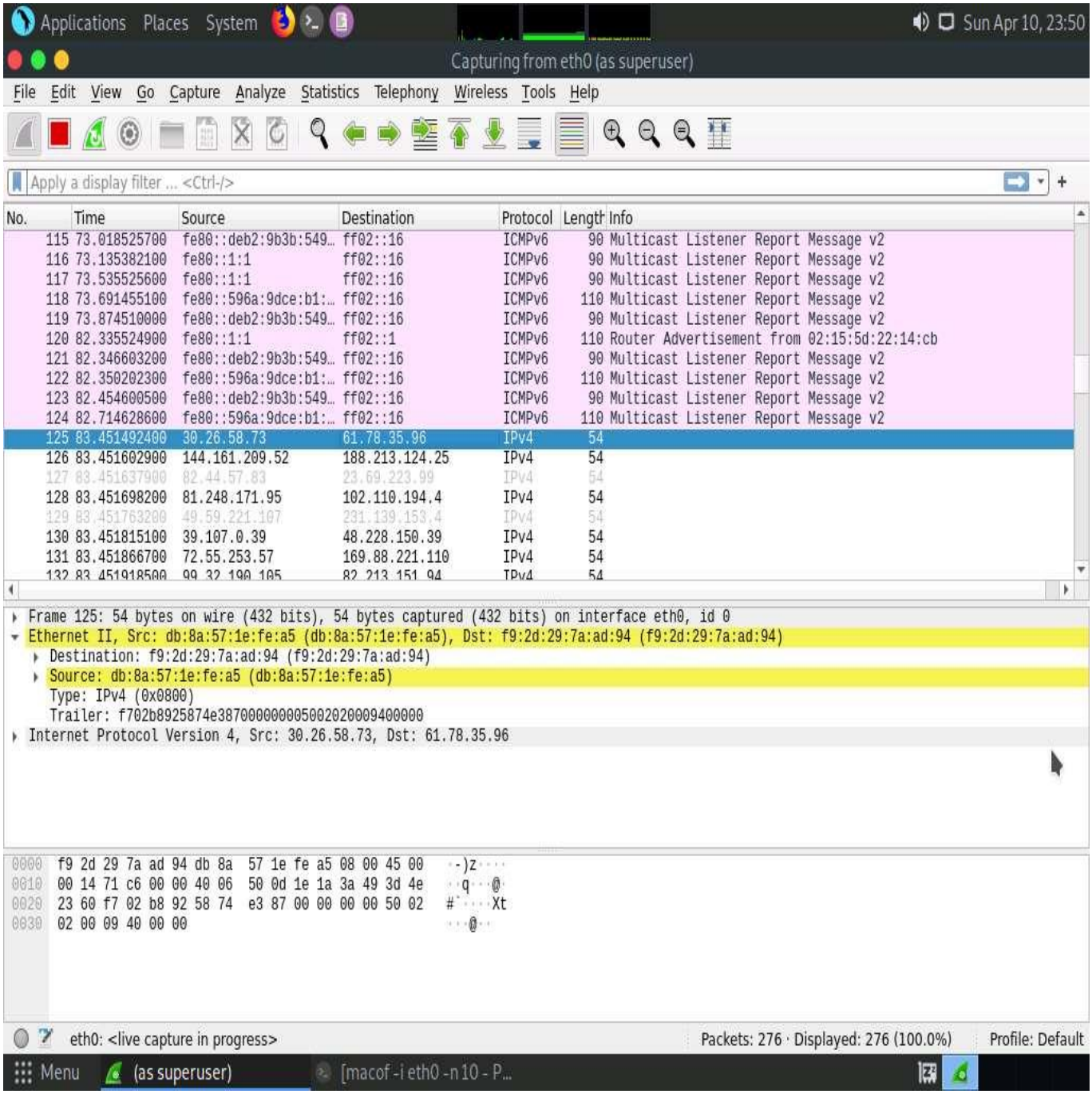
12. ☐ This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.



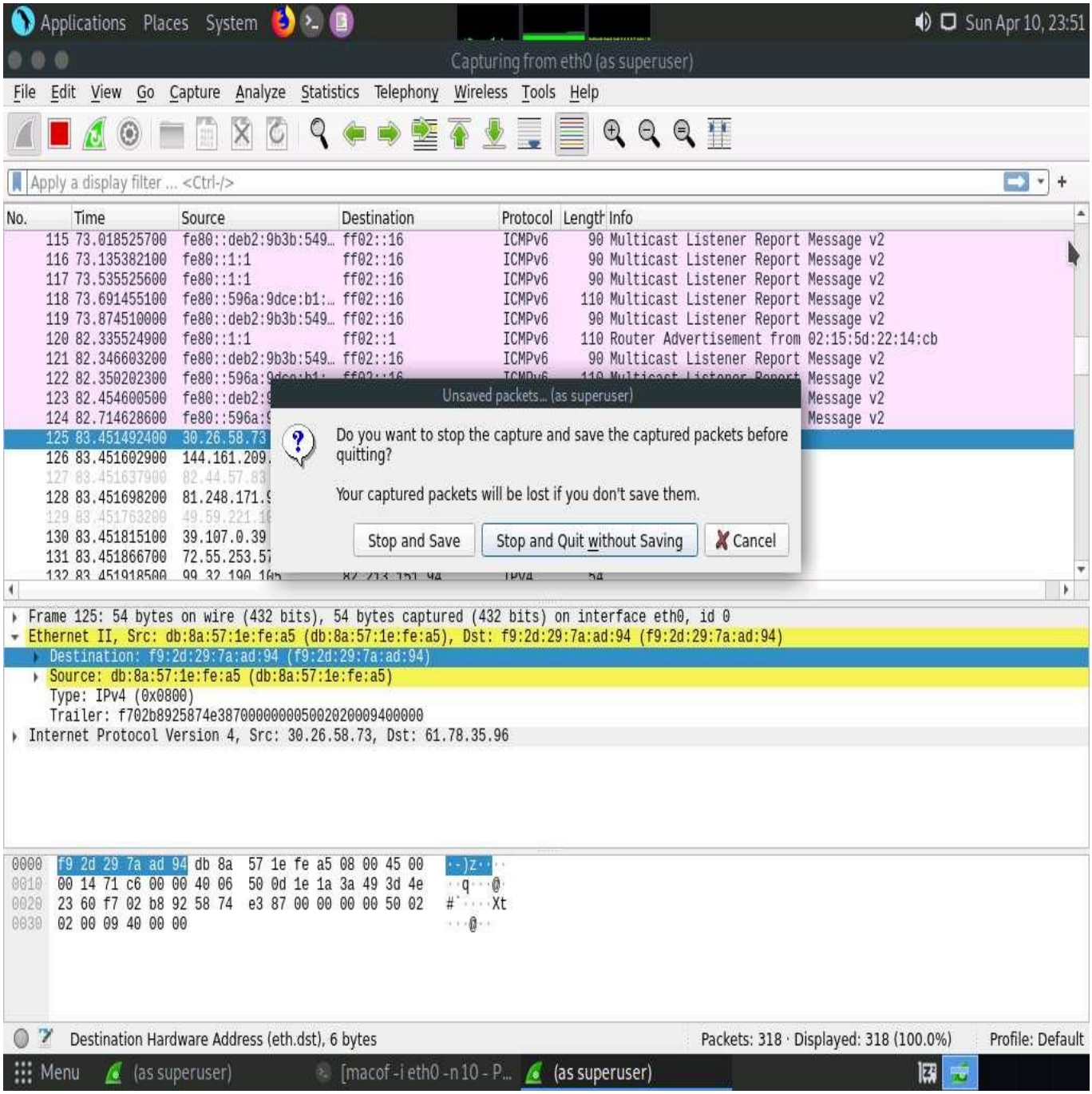
13. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.



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



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



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

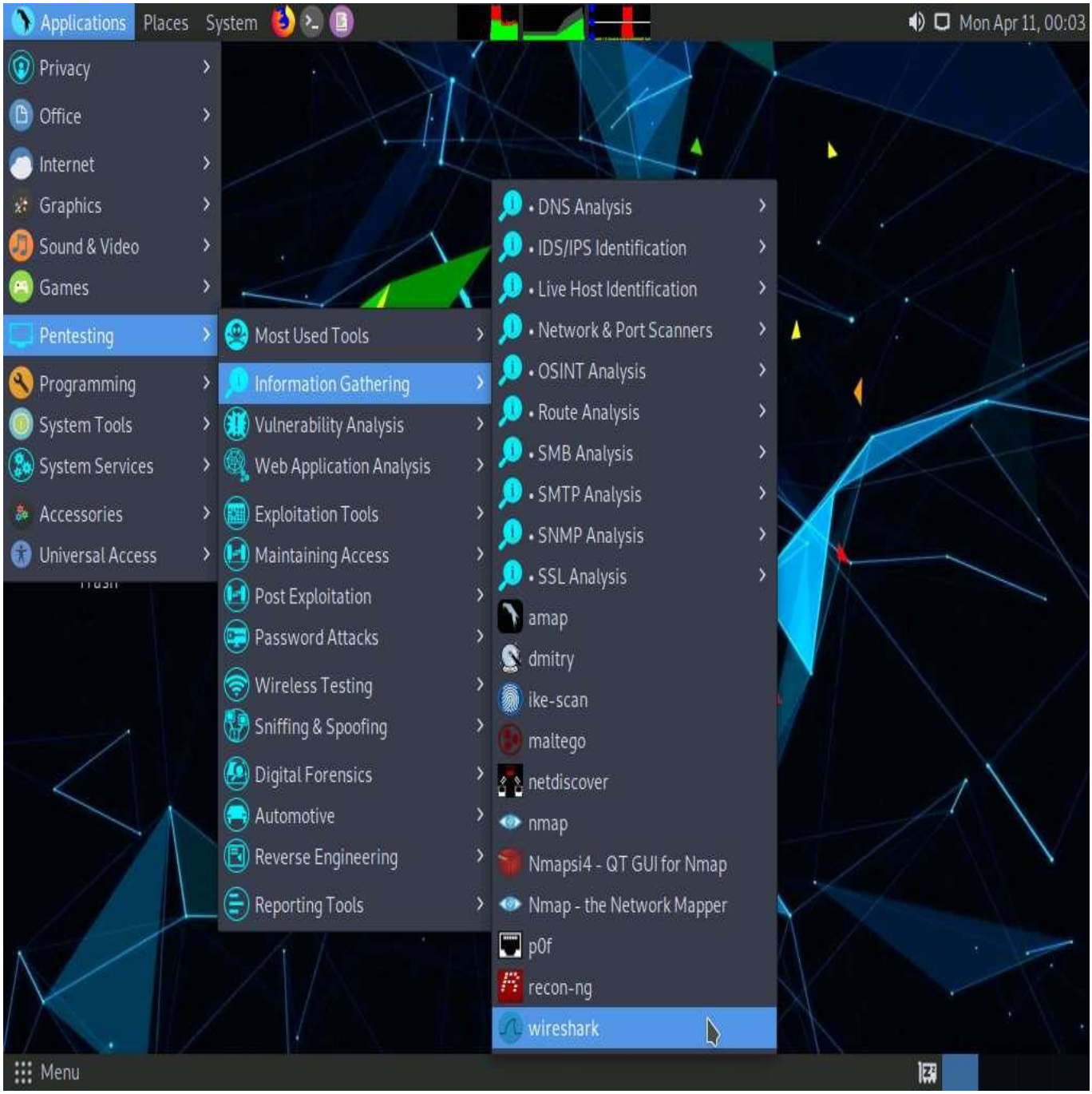
Task 2: Perform a DHCP Starvation Attack using Yersinia

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

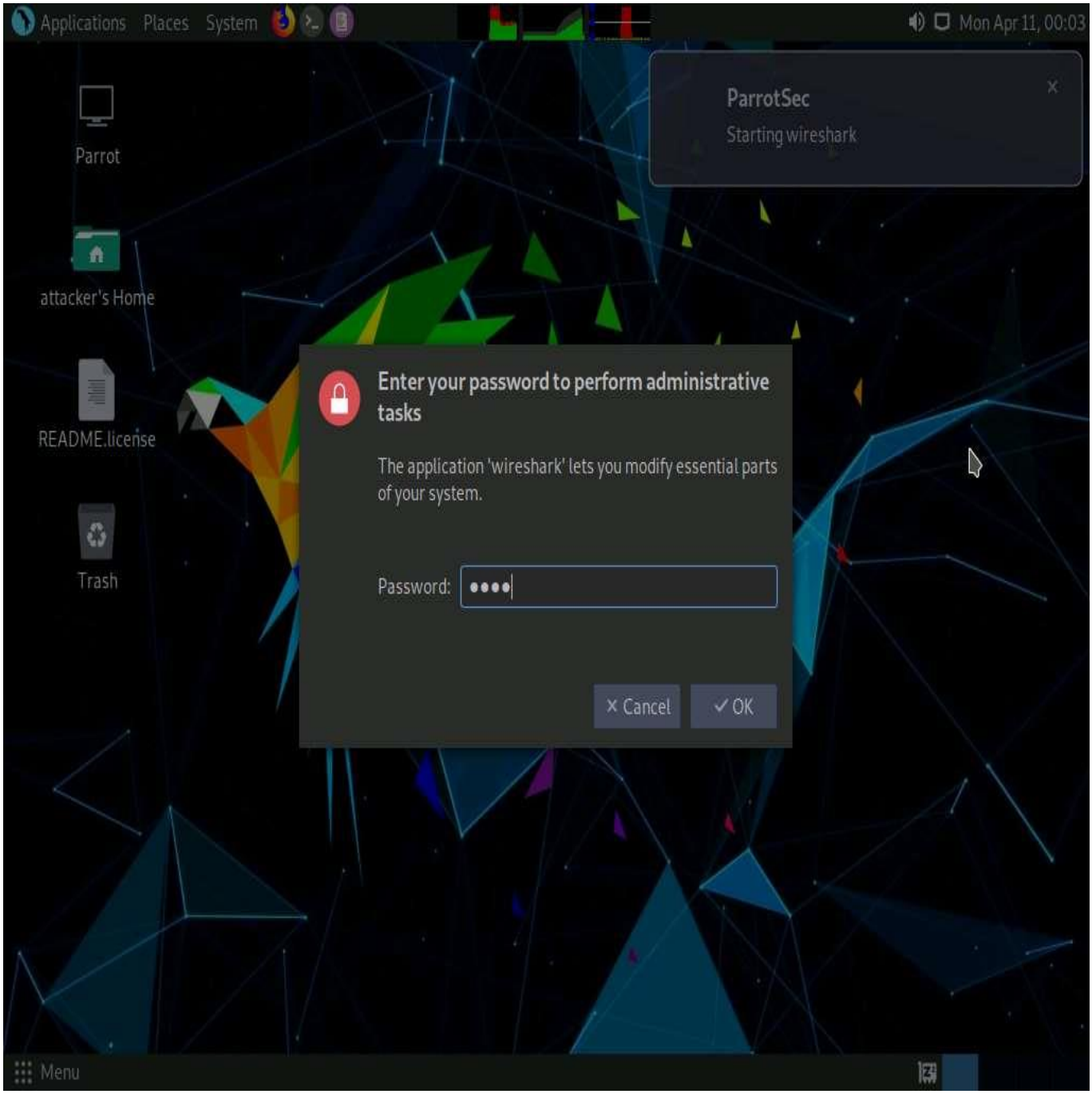
Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

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

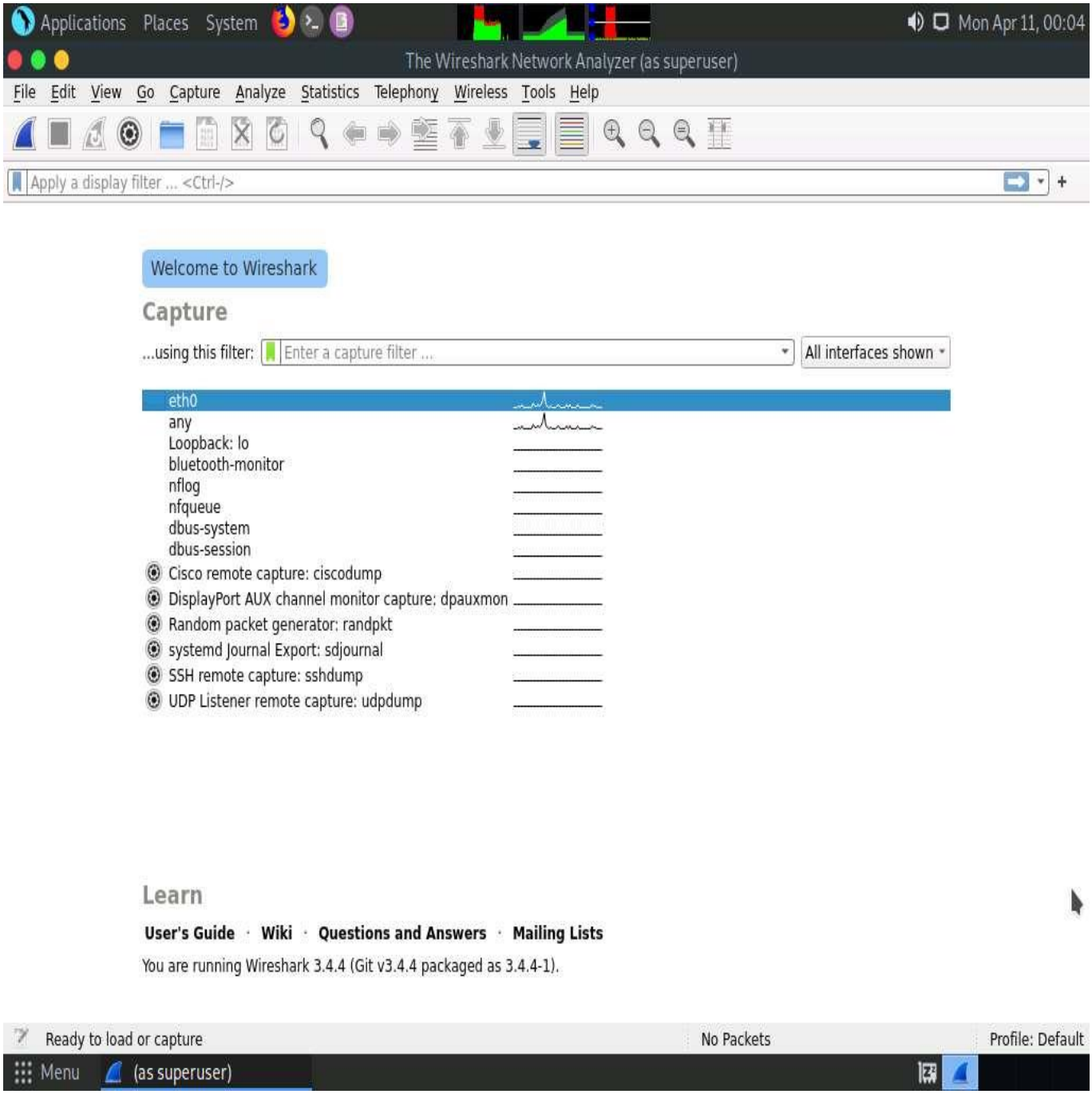
1. On the **Parrot Security** machine; click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



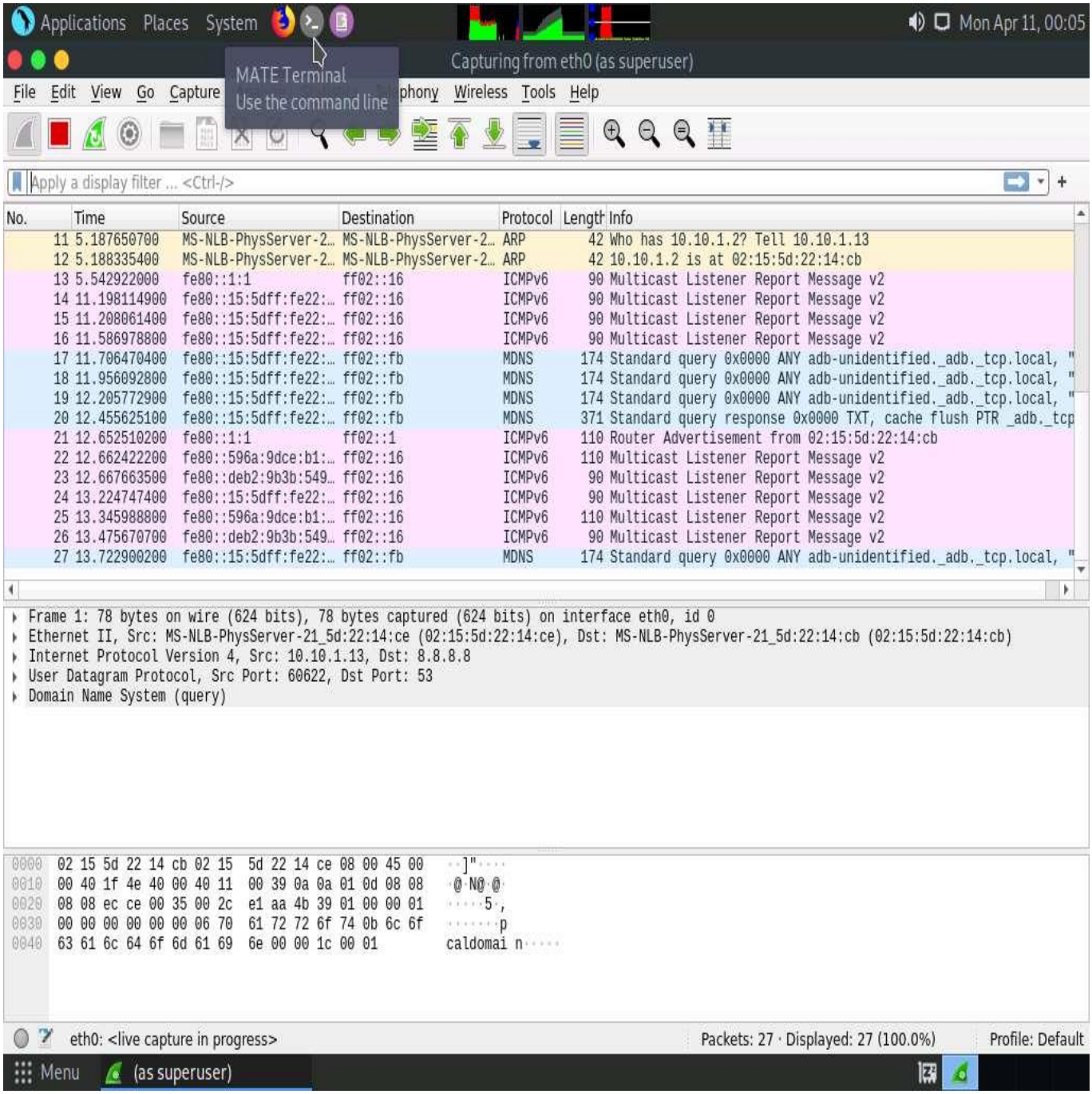
2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



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



4. ☐ Leave the **Wireshark** application running.
5. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



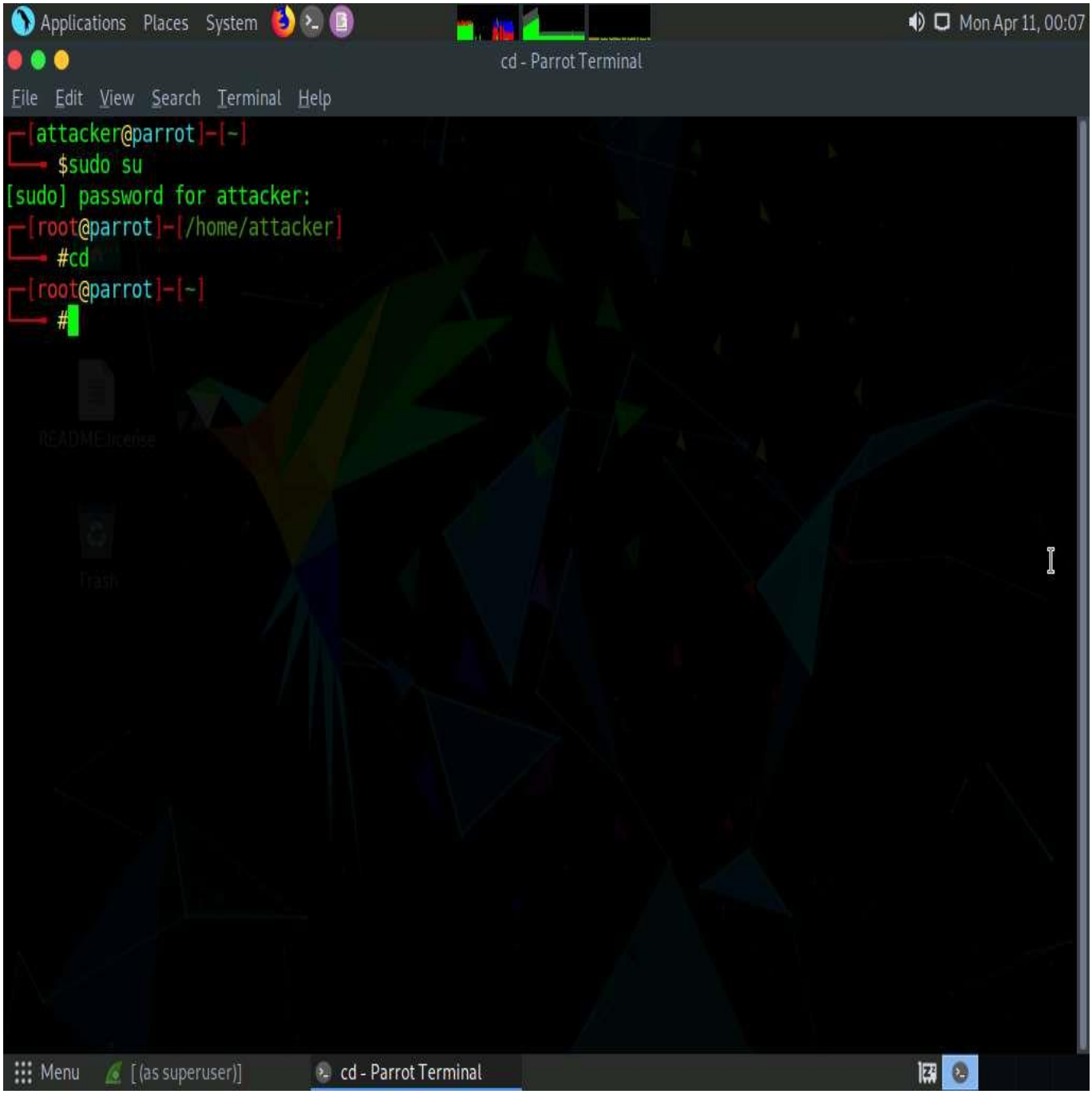
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

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

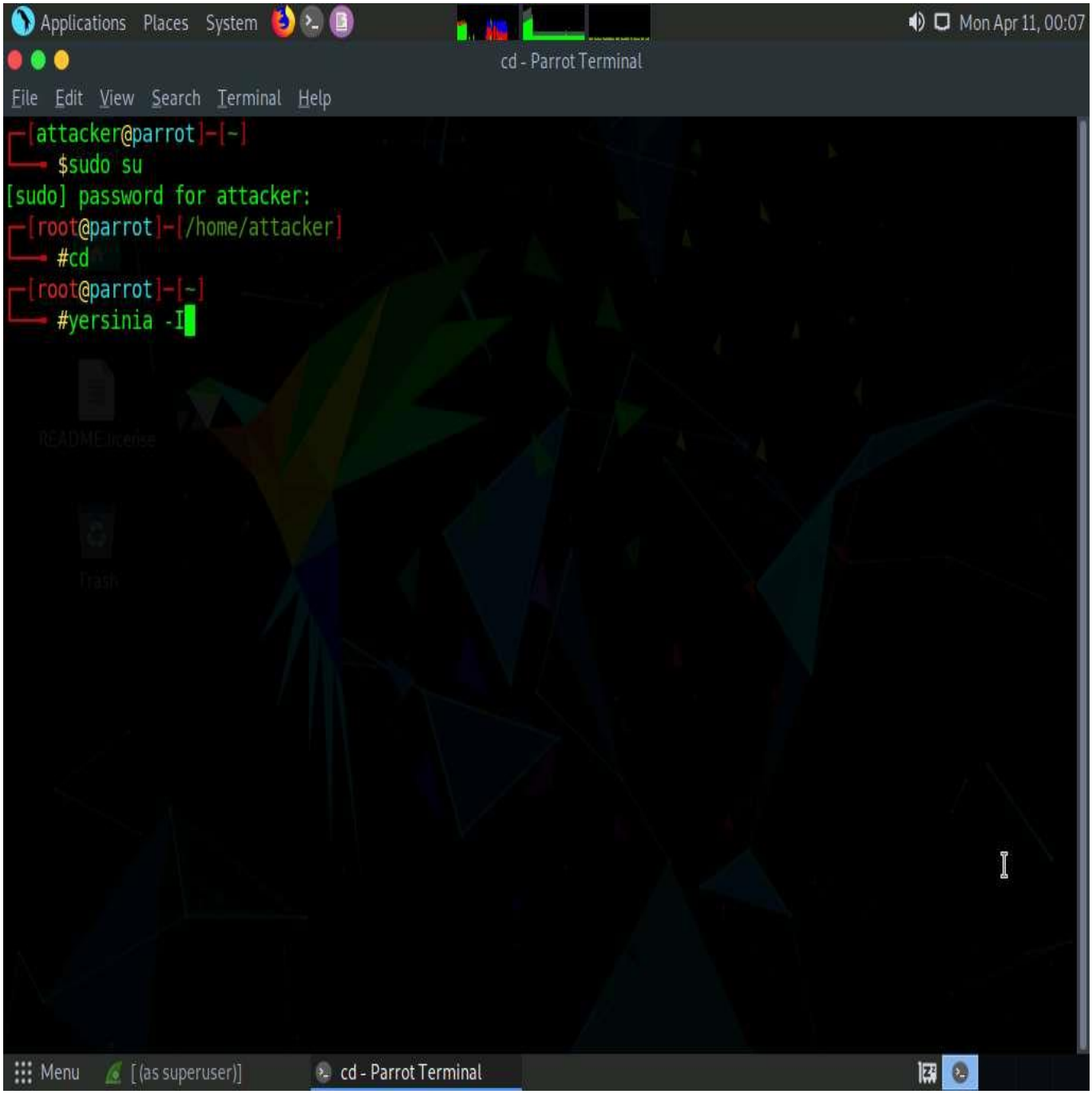
Click the **Maximize Window** icon to maximize the terminal window.

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

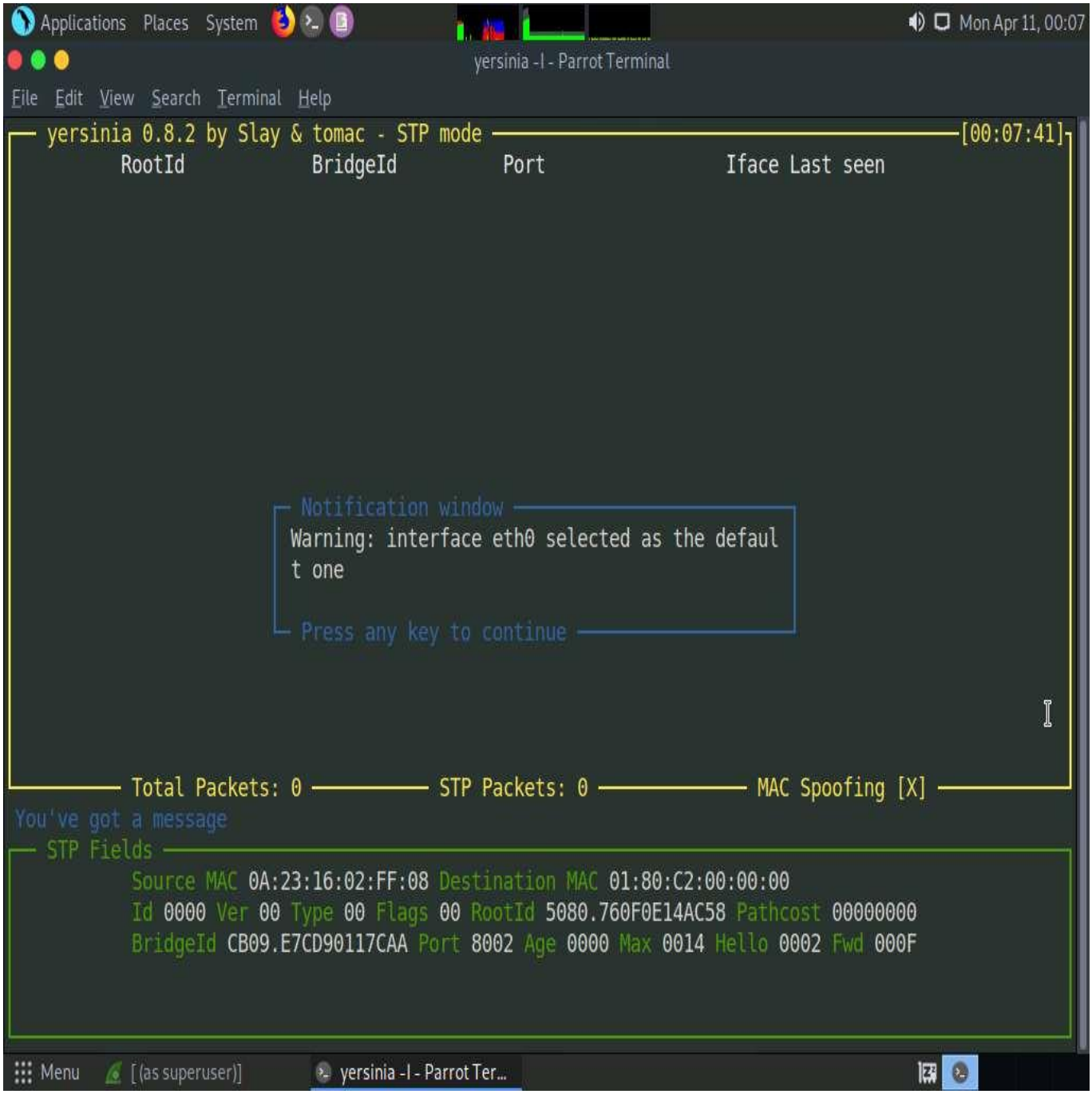


9. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.

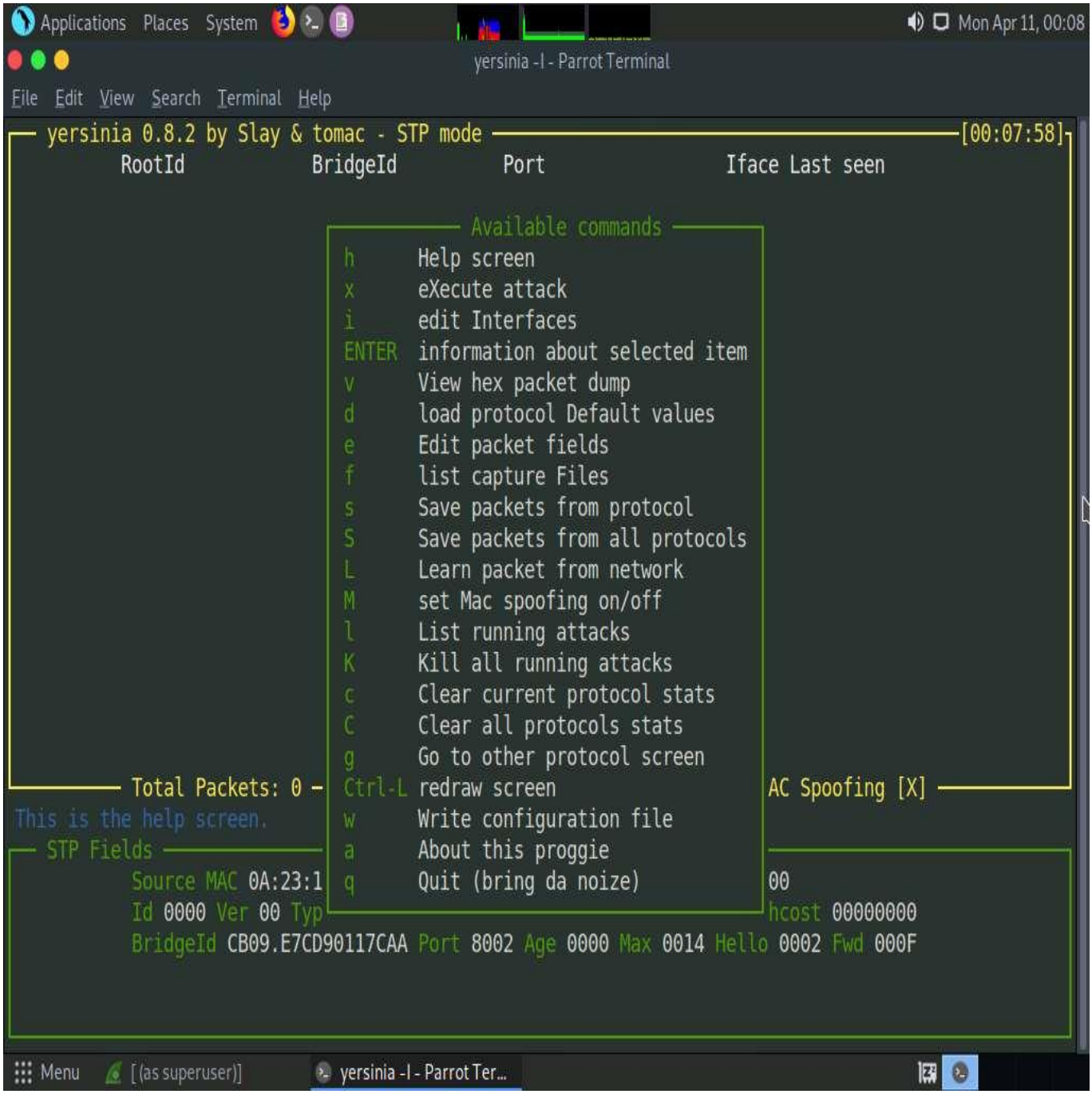
-I: Starts an interactive ncurses session.



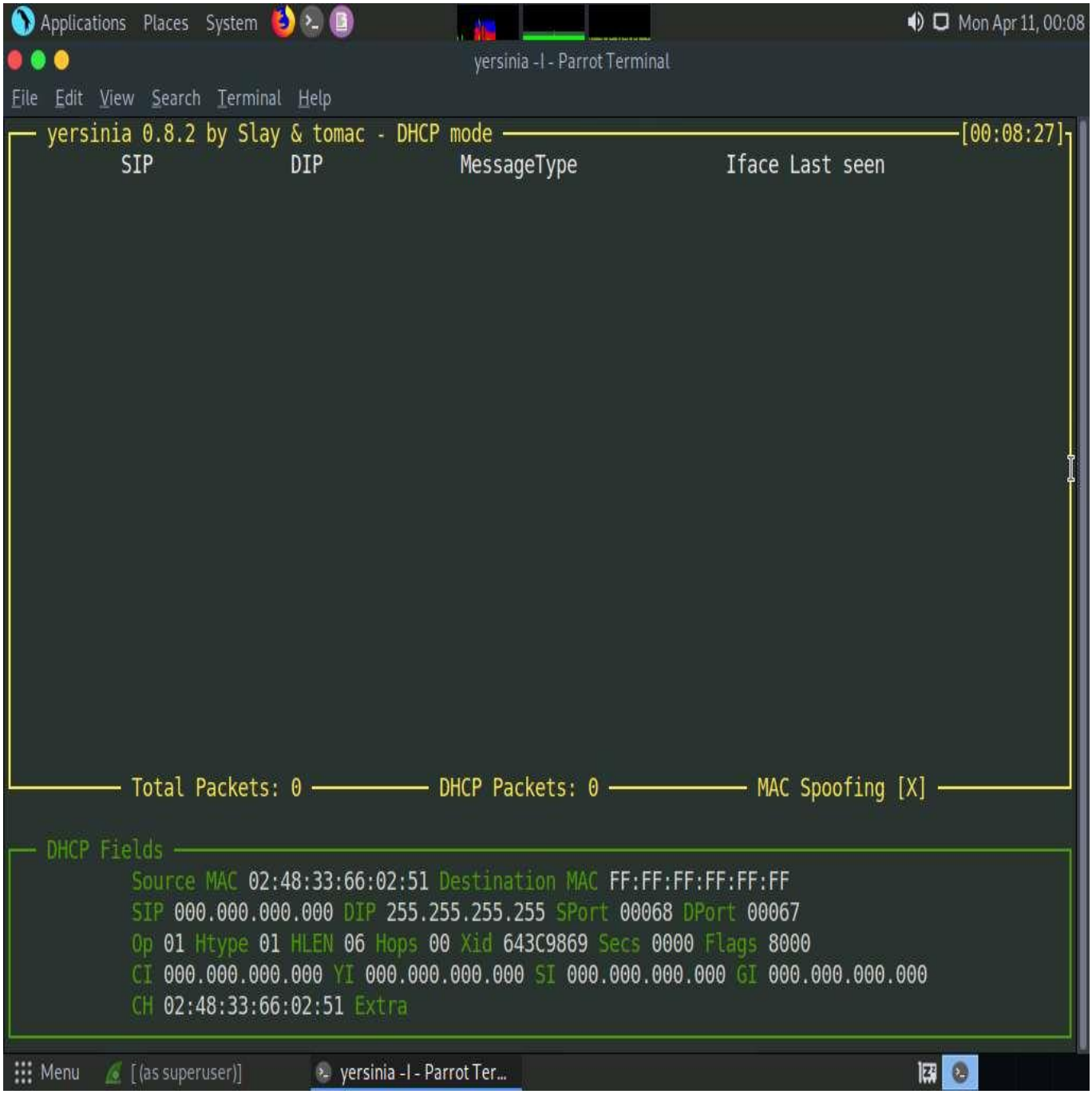
10. ☐ Yersinia interactive mode appears in the terminal window.



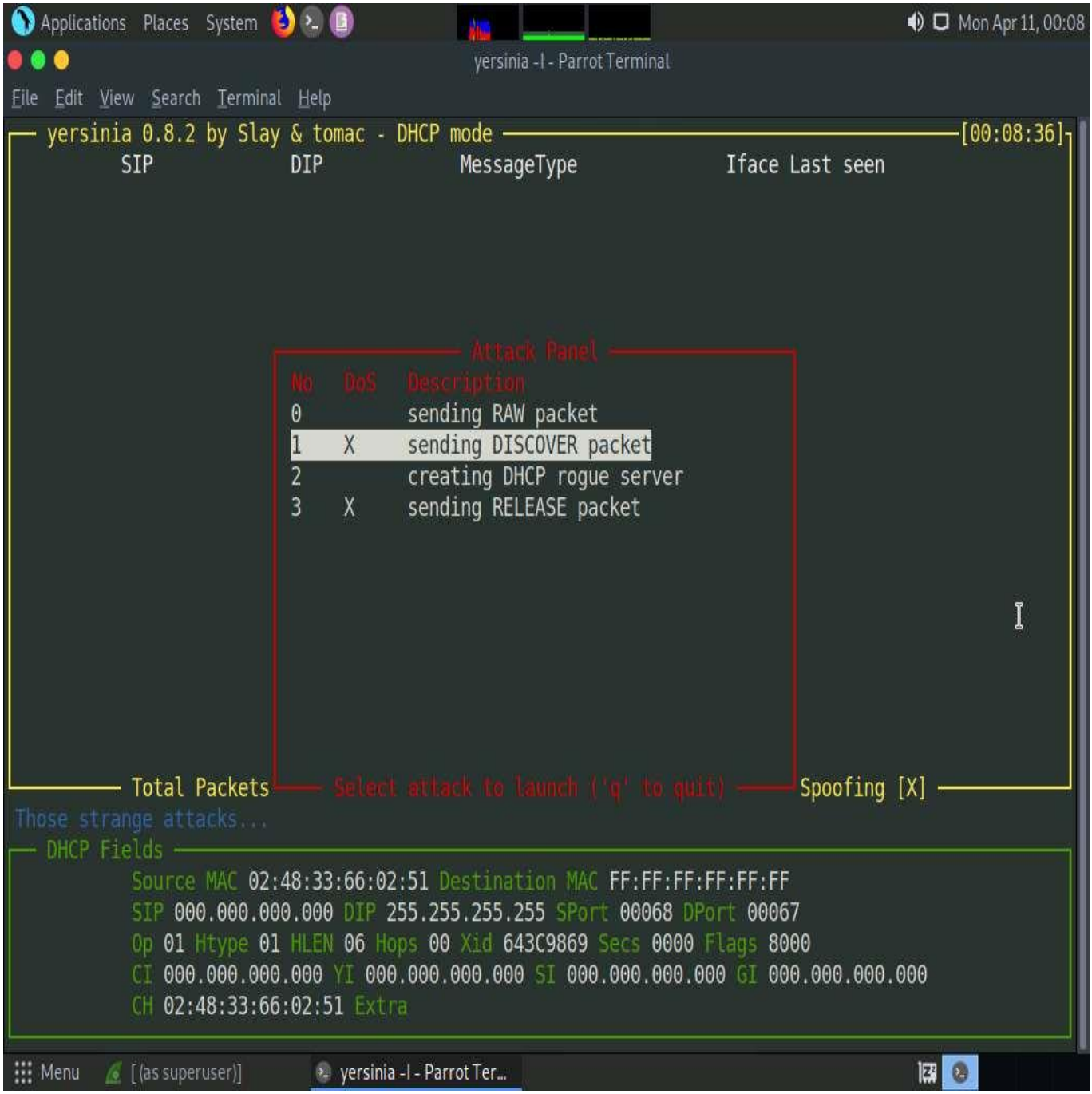
11. To remove the **Notification window**, press any key, and then press **h** for help.
12. The **Available commands** option appears, as shown in the screenshot.



13. ☐ Press **q** to exit the help options.
14. ☐ Press **F2** to select DHCP mode. In DHCP mode, **STP Fields** in the lower section of the window change to **DHCP Fields**, as shown in the screenshot.

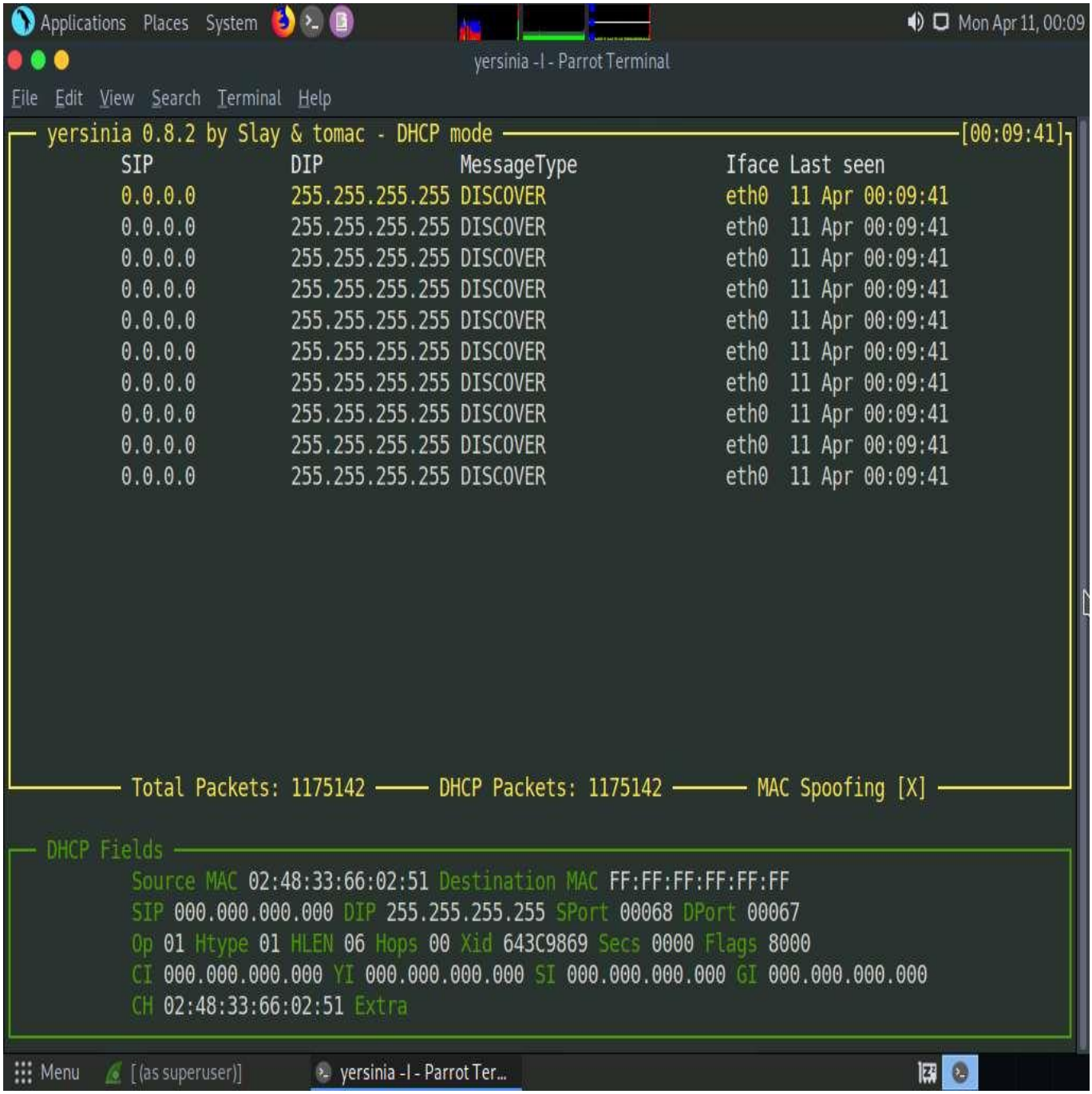


15. ☐ Press **x** to list available attack options.
16. ☐ The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.

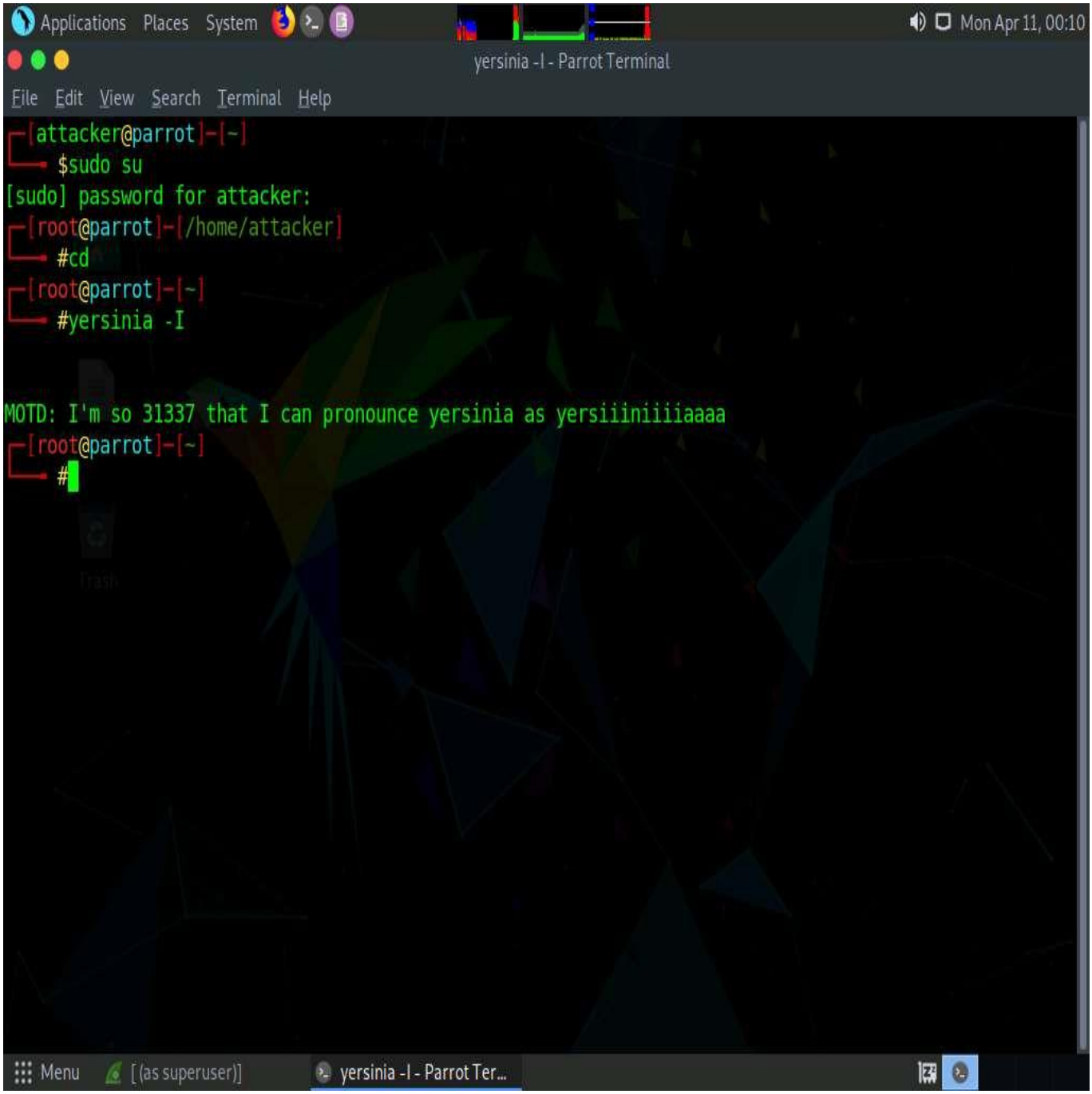


17. **Yersinia** starts sending DHCP packets to the network adapter and all active machines in the local network, as shown in the screenshot.

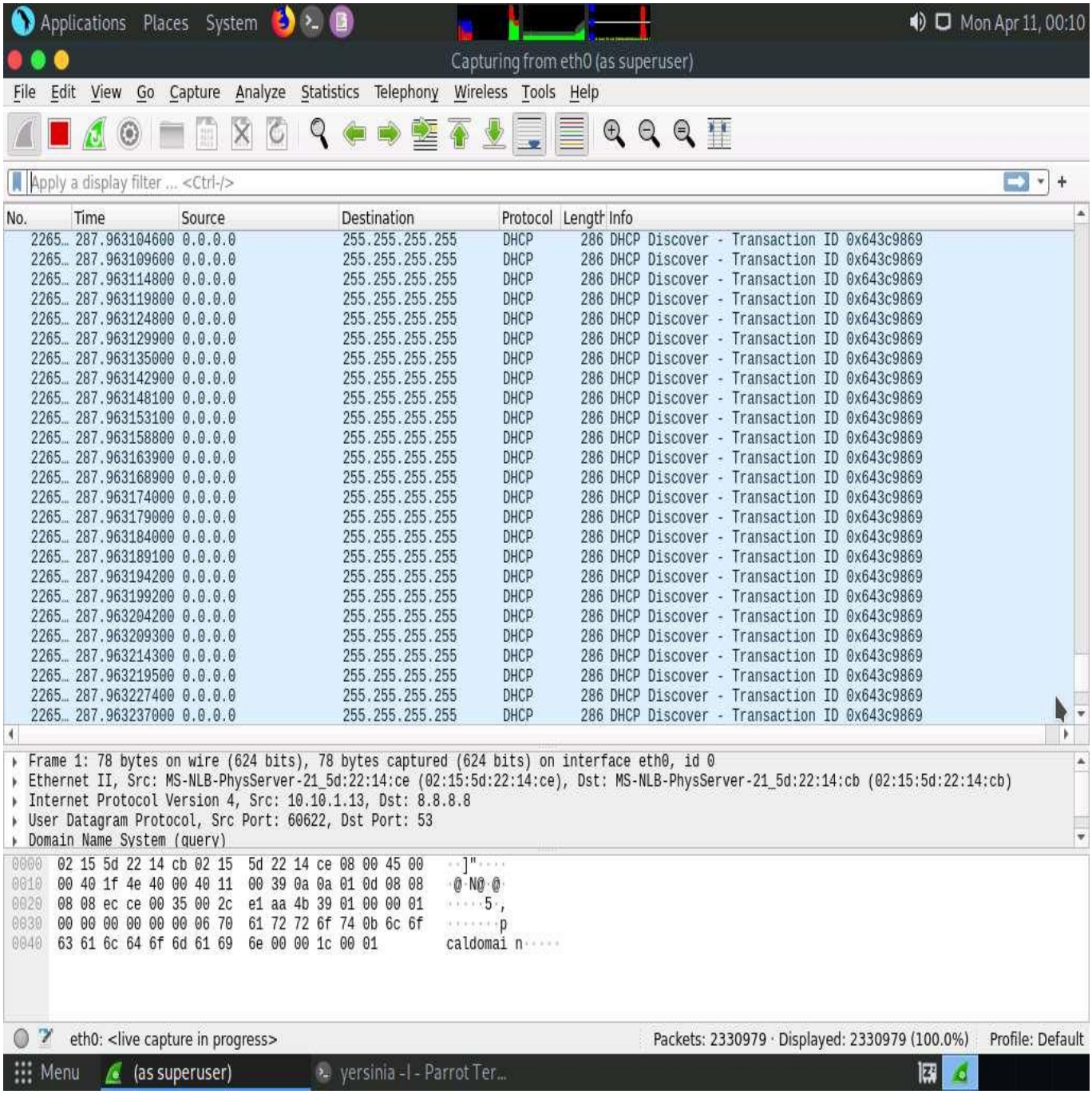
If you are using multiple targets, you will observe the same packets on all target machines.



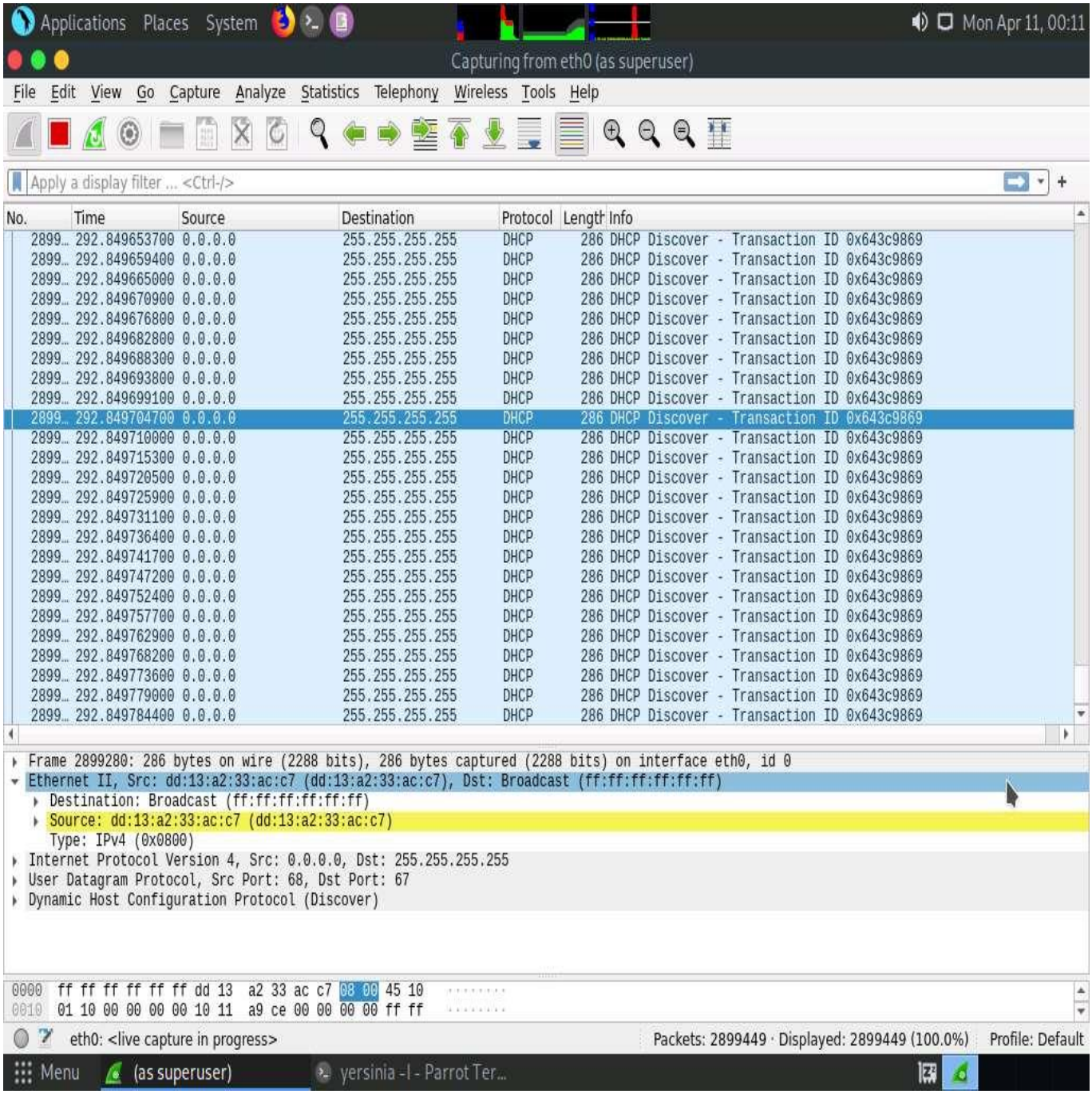
18. ☐ After a few seconds, press **q** to stop the attack and terminate Yersinia, as shown in the screenshot.



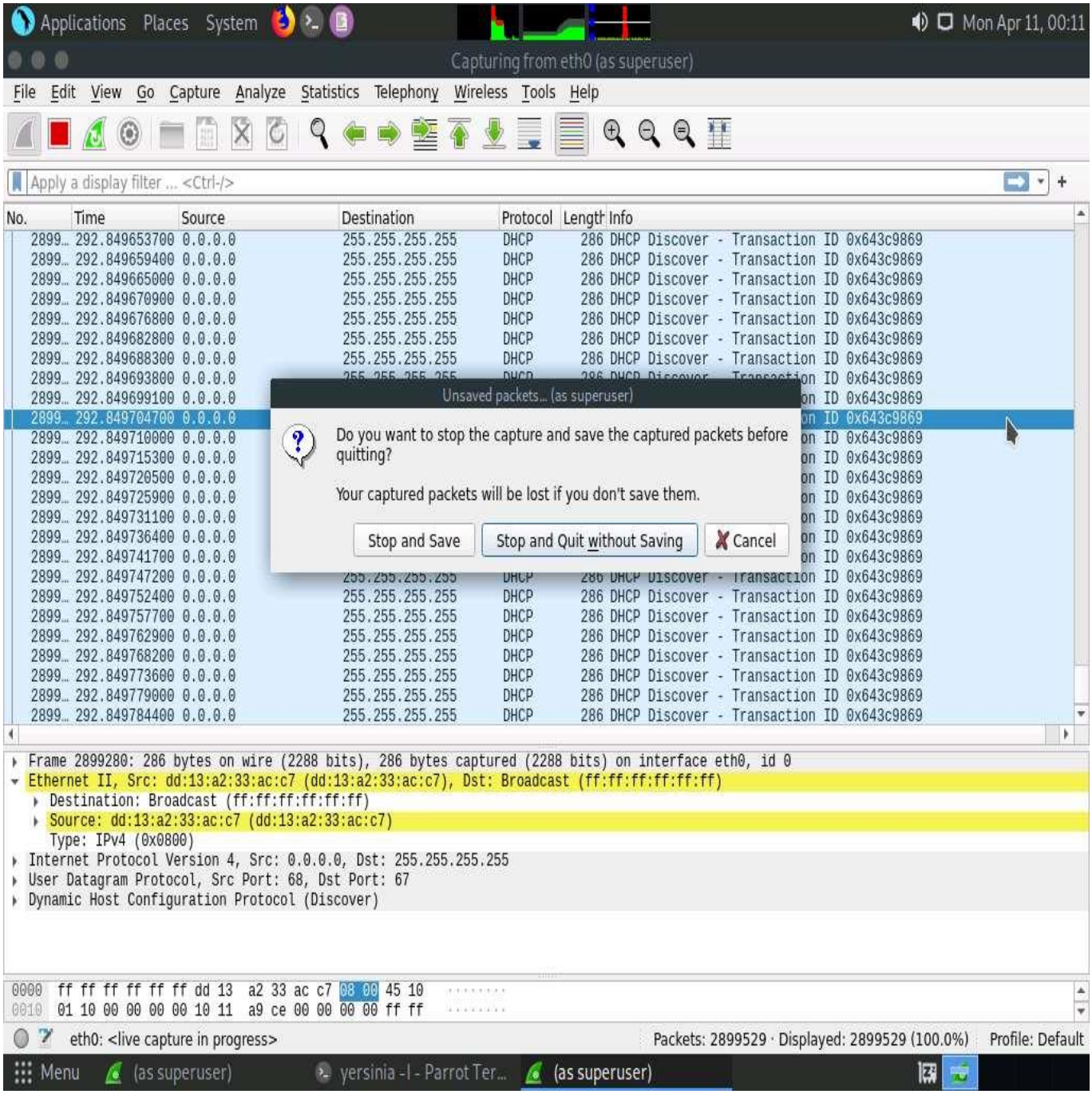
19. ☐ Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.



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



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



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

Task 3: Perform ARP Poisoning using arpspoof

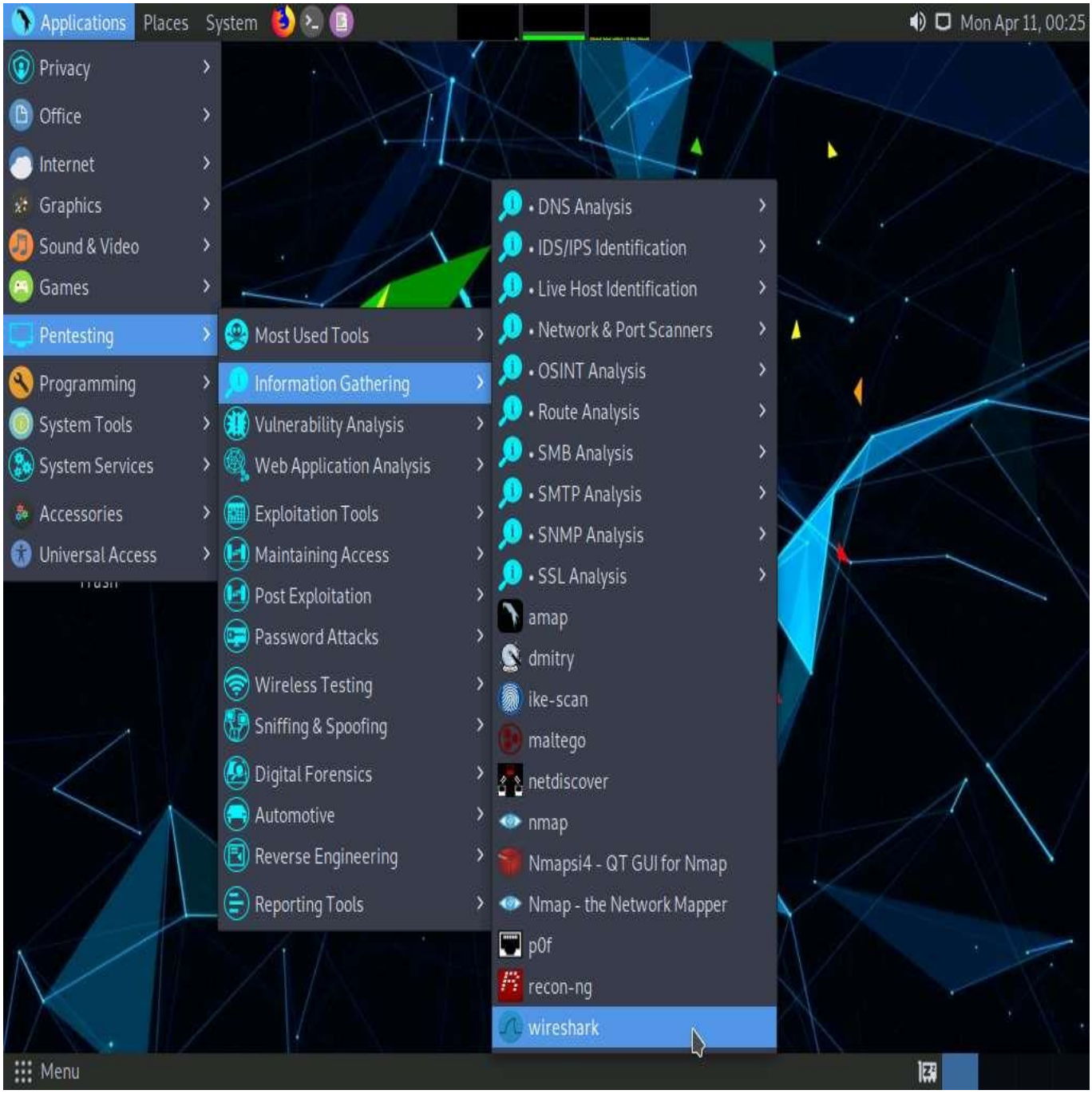
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the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

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

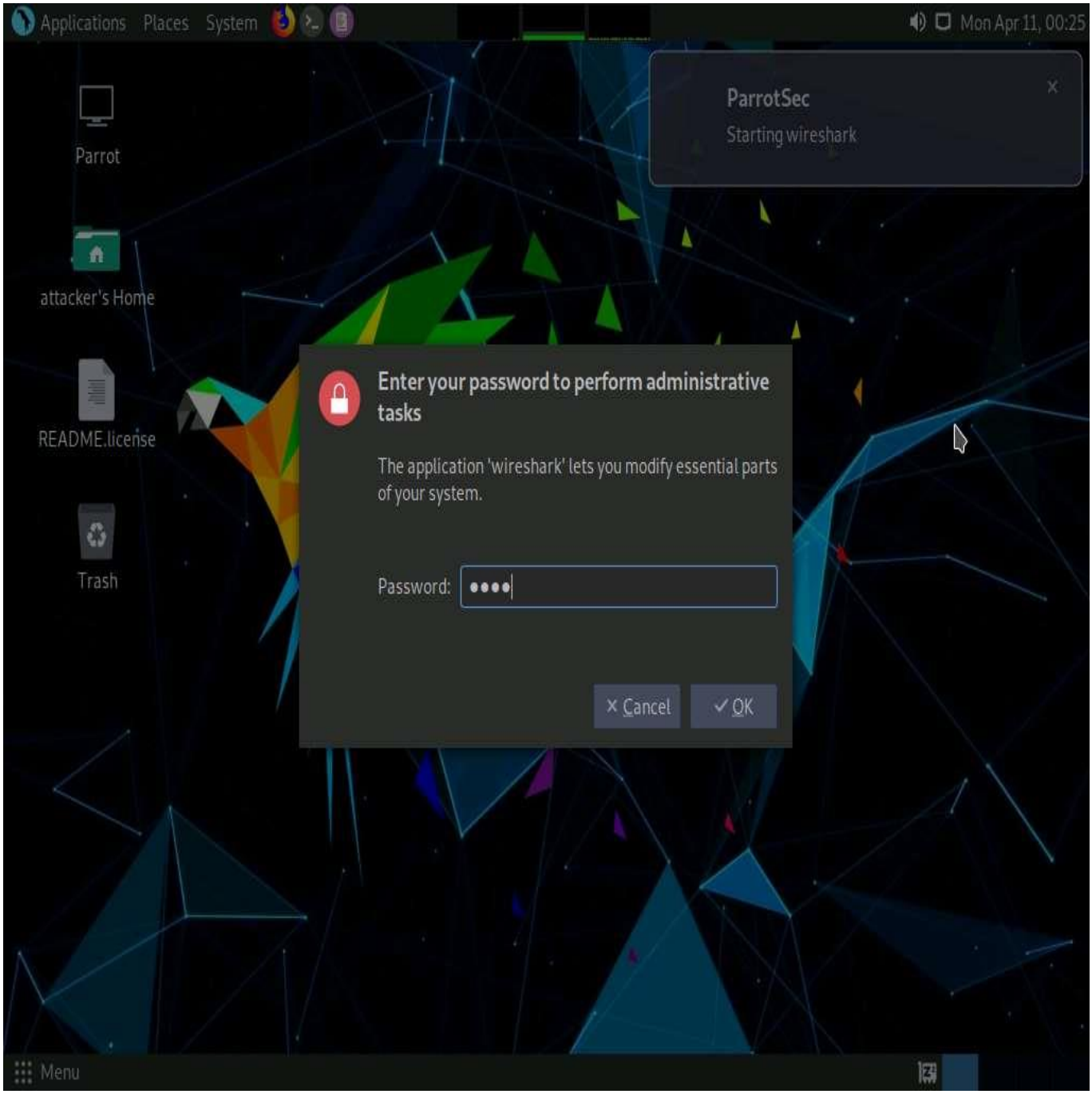
Here, we will use the arpspoof tool to perform ARP poisoning.

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

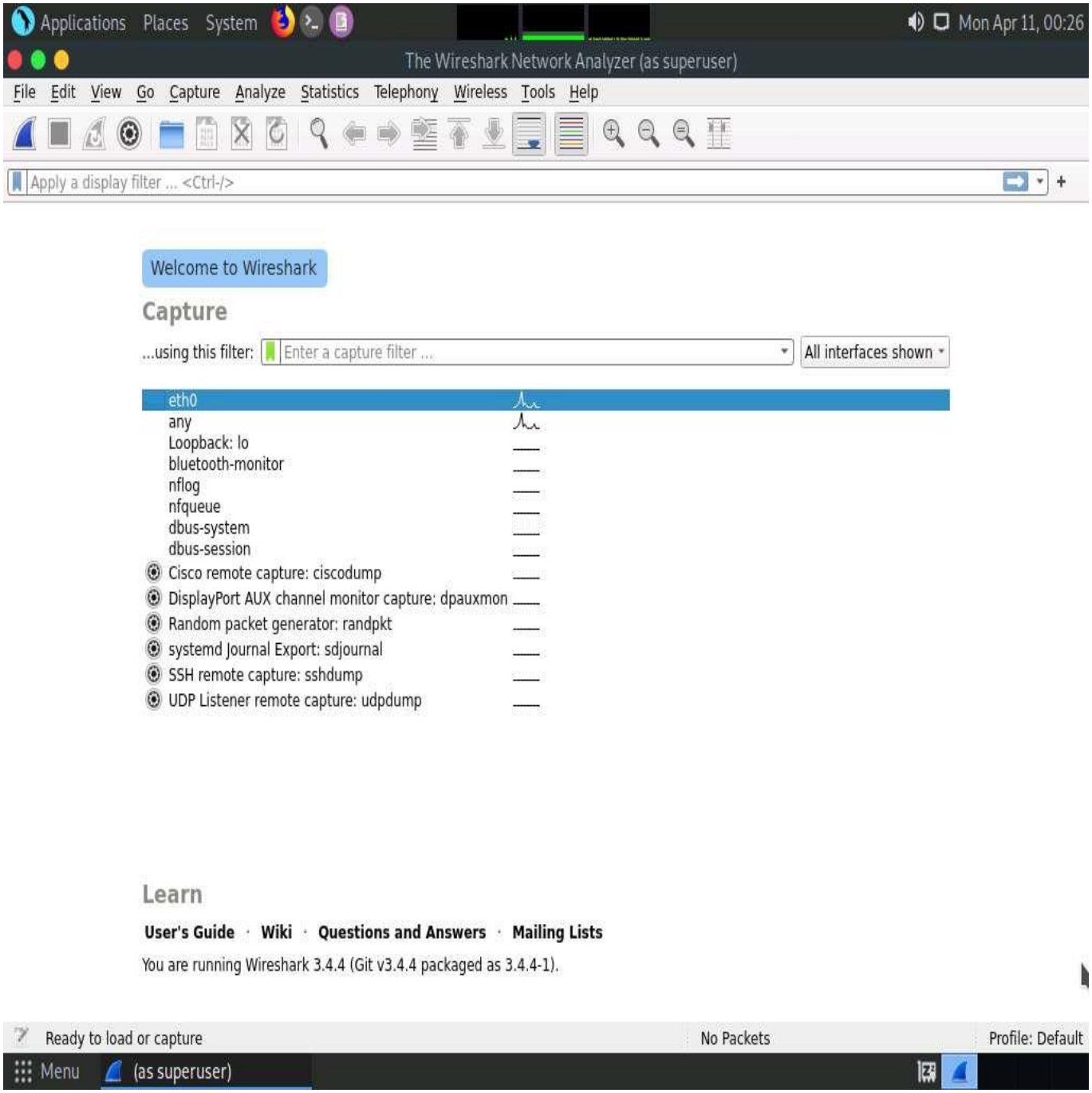
1. On the **Parrot Security** machine; click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



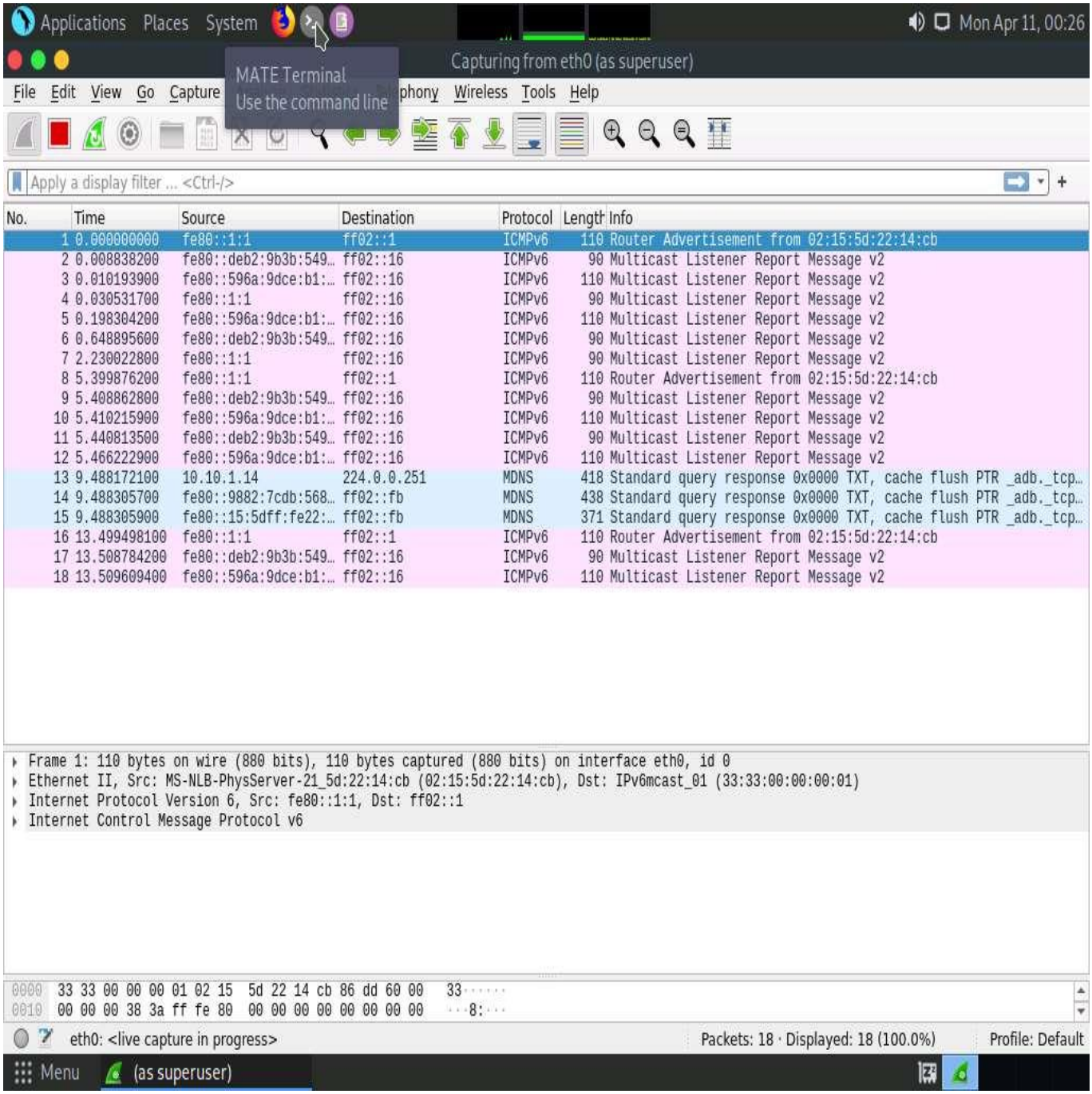
2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



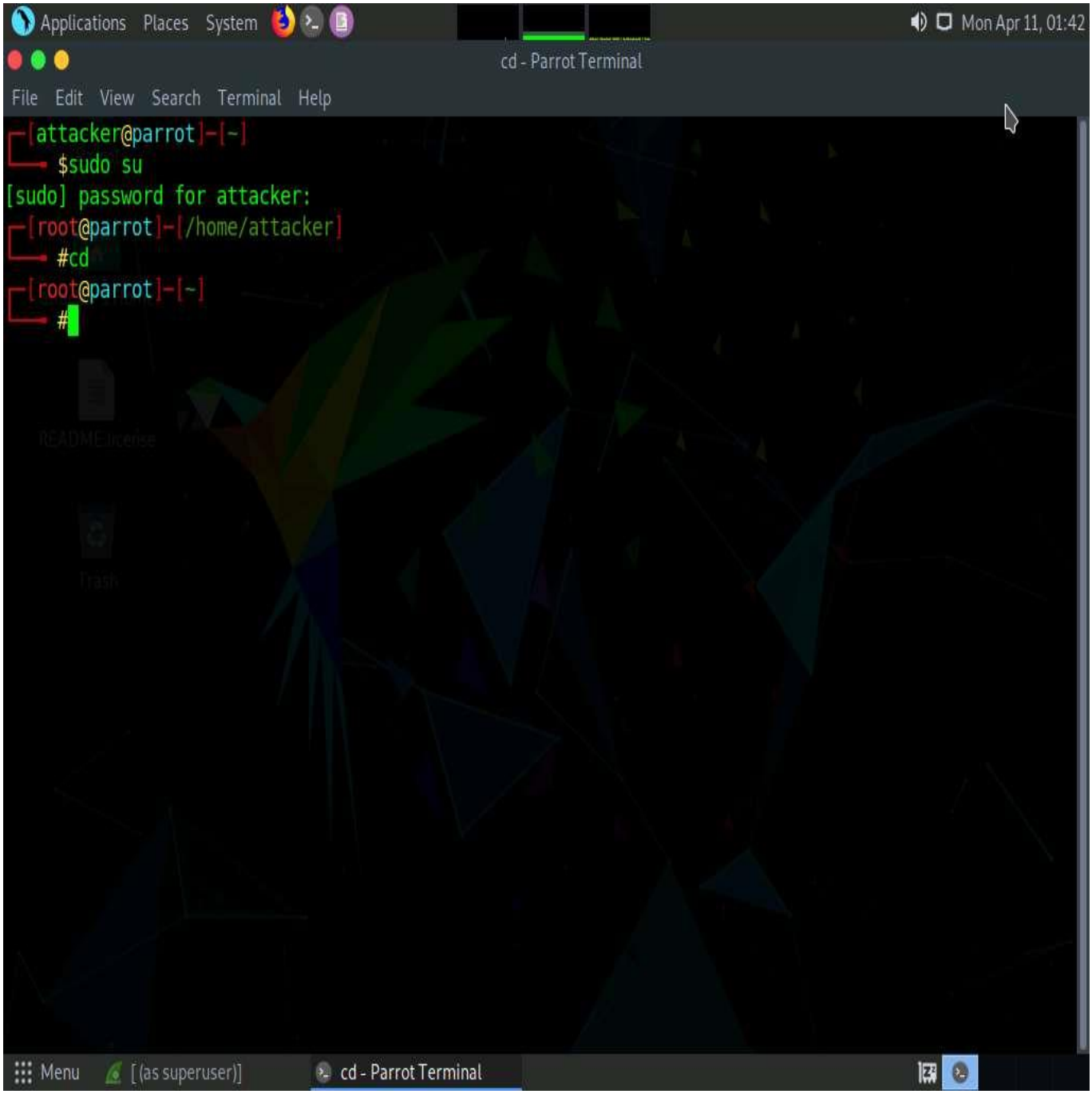
3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



4. ☐ Leave the **Wireshark** application running.
5. ☐ Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
8. Now, type **cd** and press **Enter** to jump to the root directory.

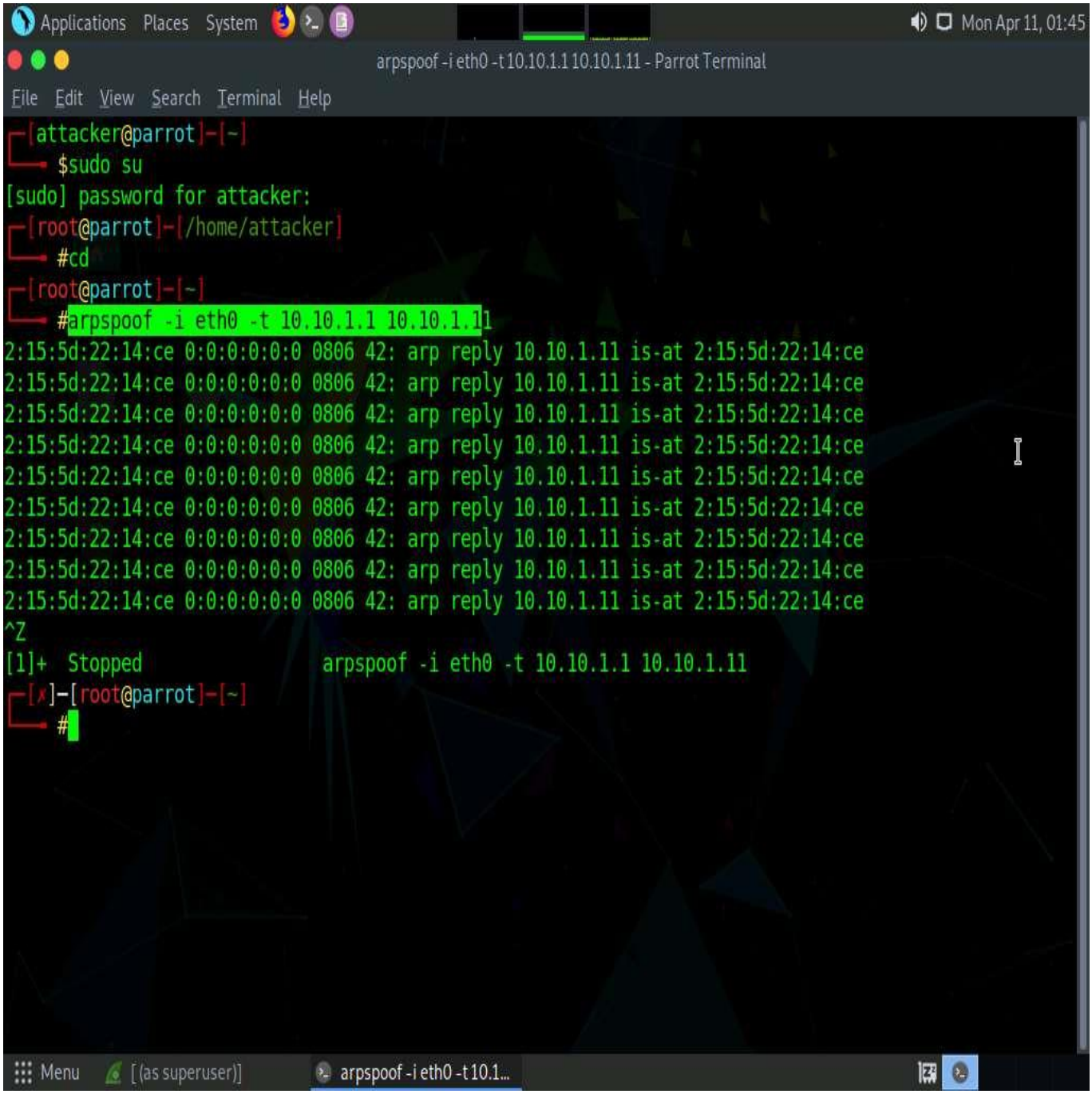


9. ☐ In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.1.1 10.10.1.11** and press **Enter**.

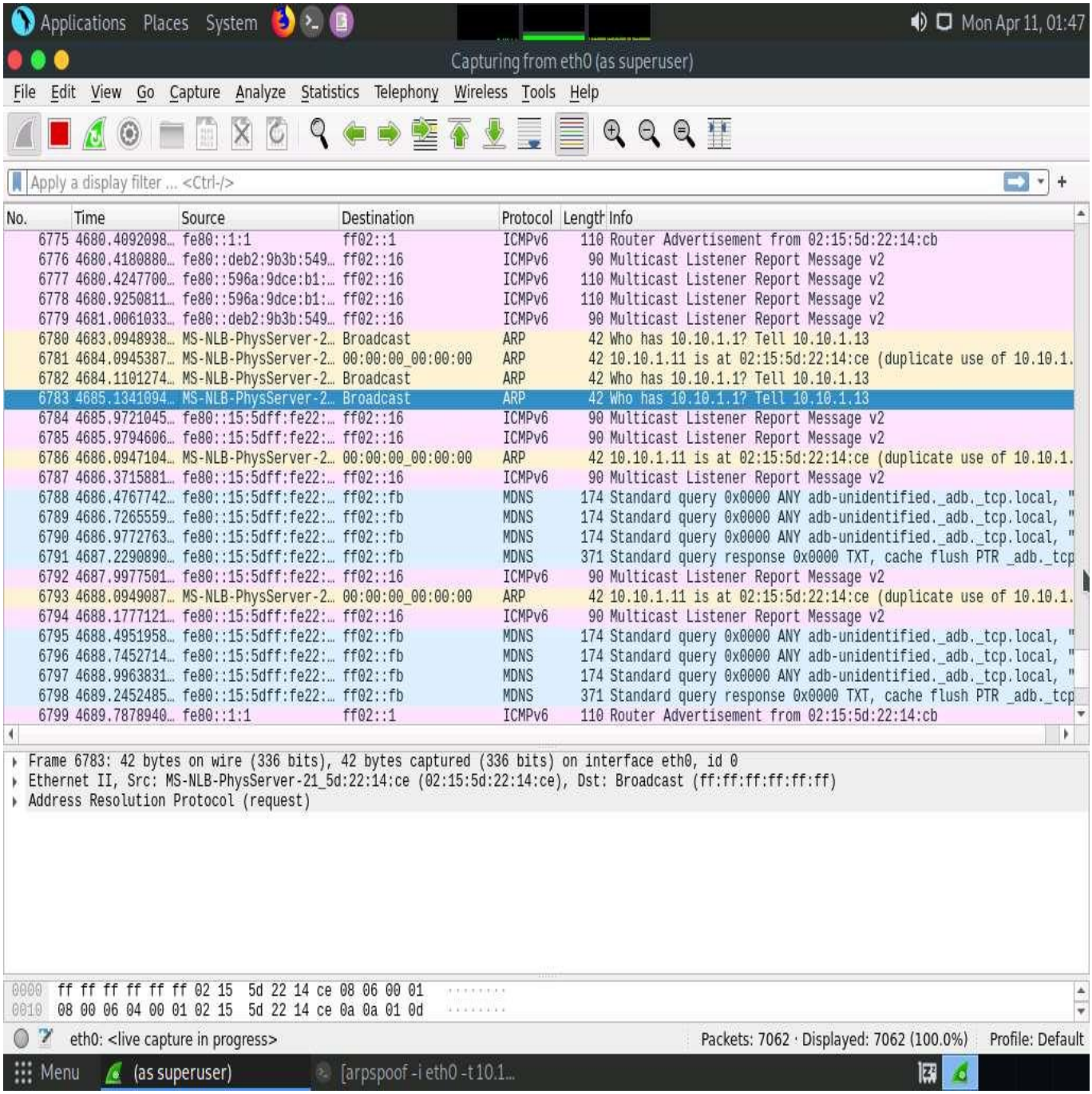
   (Here, **10.10.1.11** is IP address of the target system [**Windows 11**], and **10.10.1.1** is IP address of the access point or gateway)

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

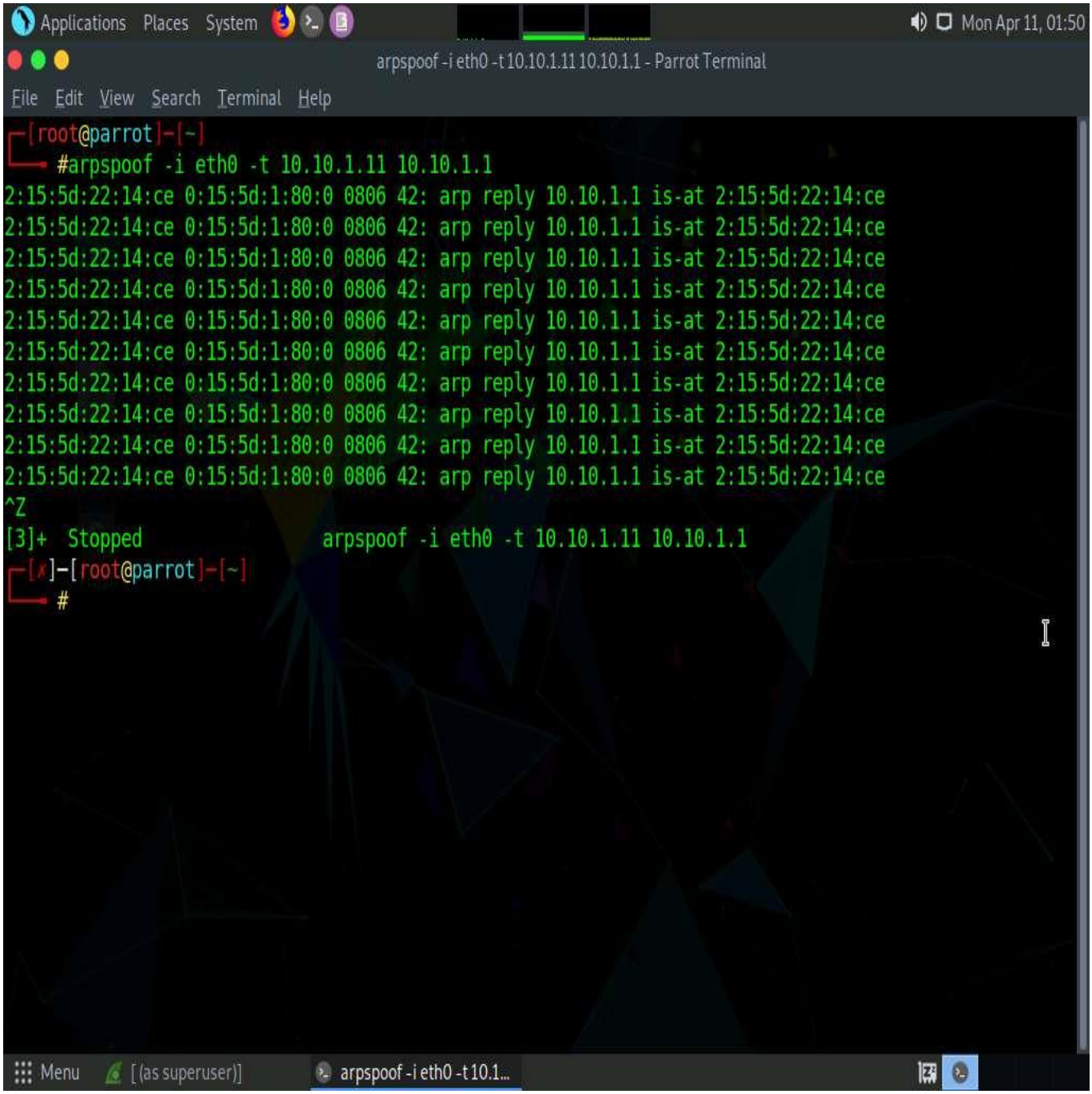
10. ☐ Issuing the above command informs the access point that the target system (**10.10.1.11**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.
11. ☐ After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.



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



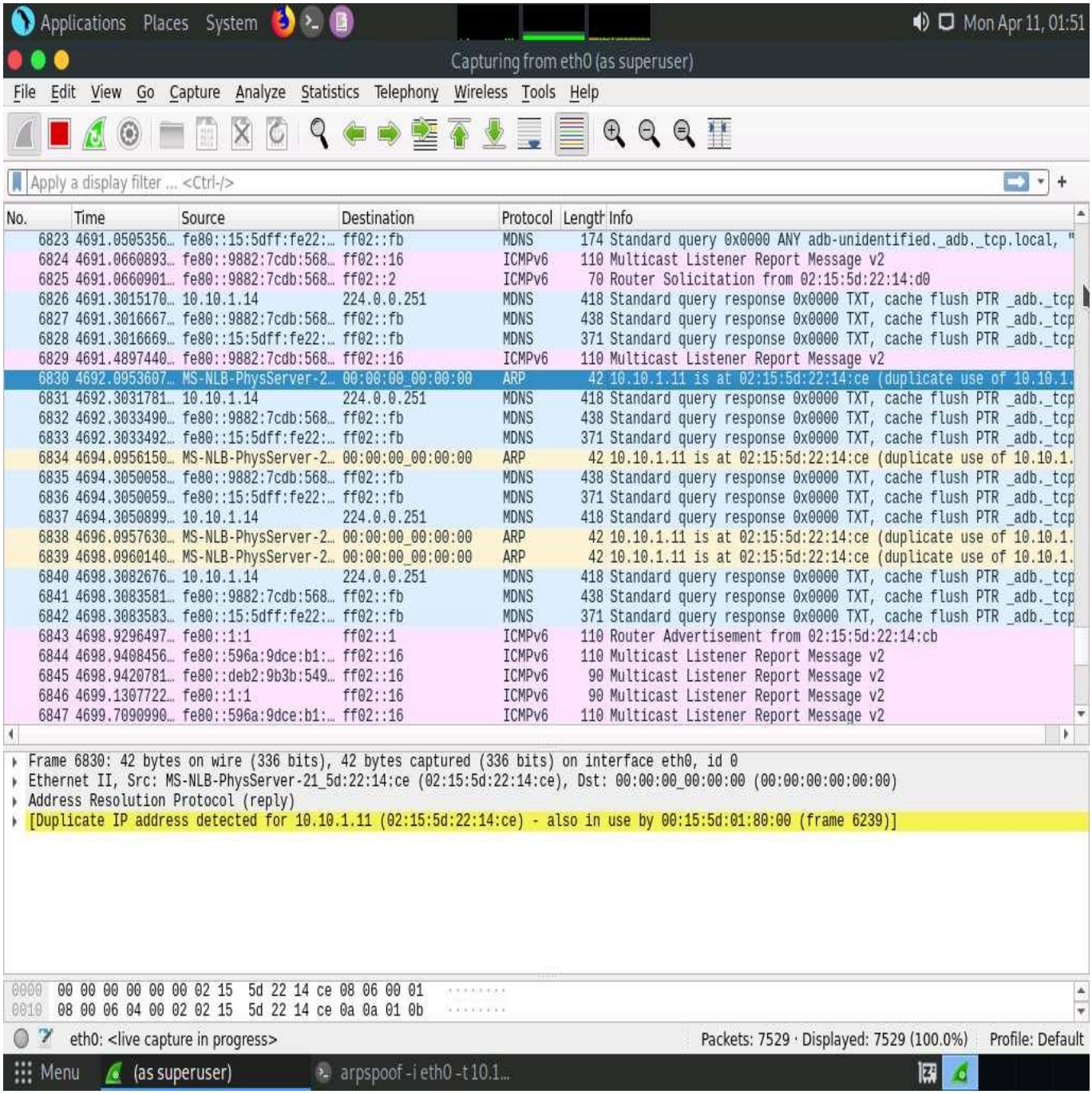
13. ☐ Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.1.11 10.10.1.1** and press **Enter**.
14. ☐ Through the above command, the host system informs the target system (**10.10.1.11**) that it is the access point (**10.10.1.1**).
15. ☐ After sending a few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



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

    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.



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.

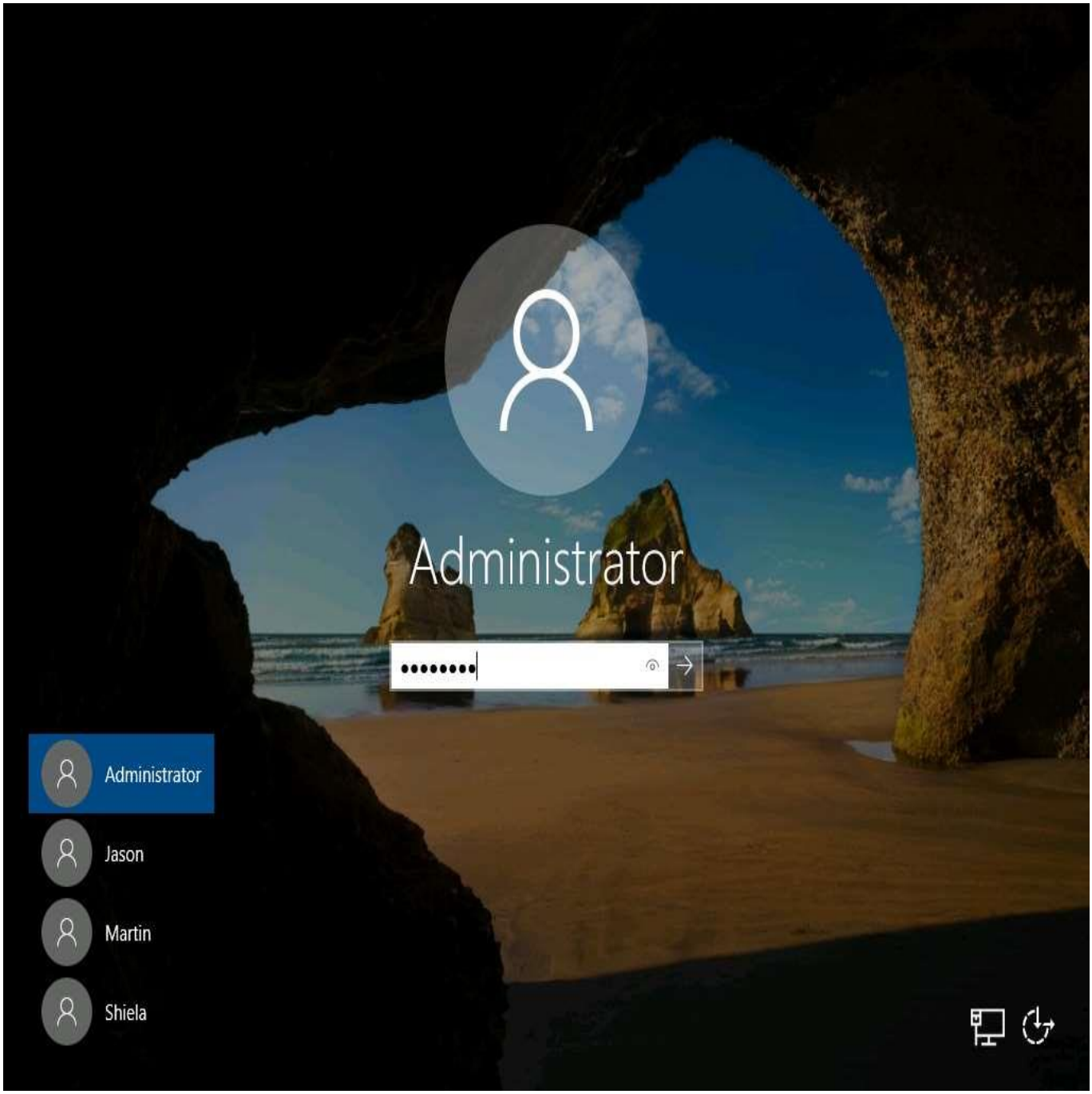
Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

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

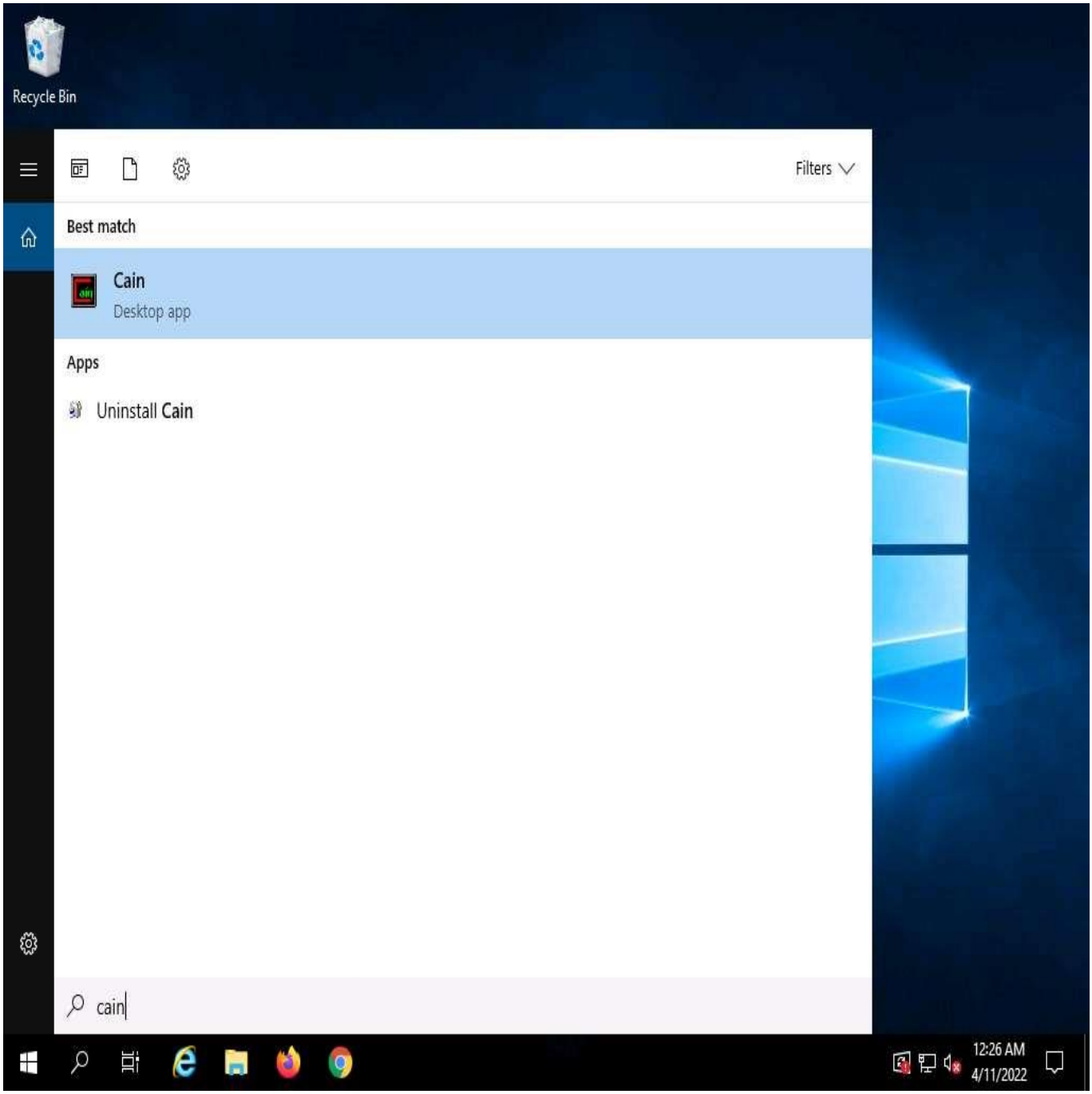
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. Click Ctrl+Alt+Delete to activate the machine. By default, **Administrator** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

   Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

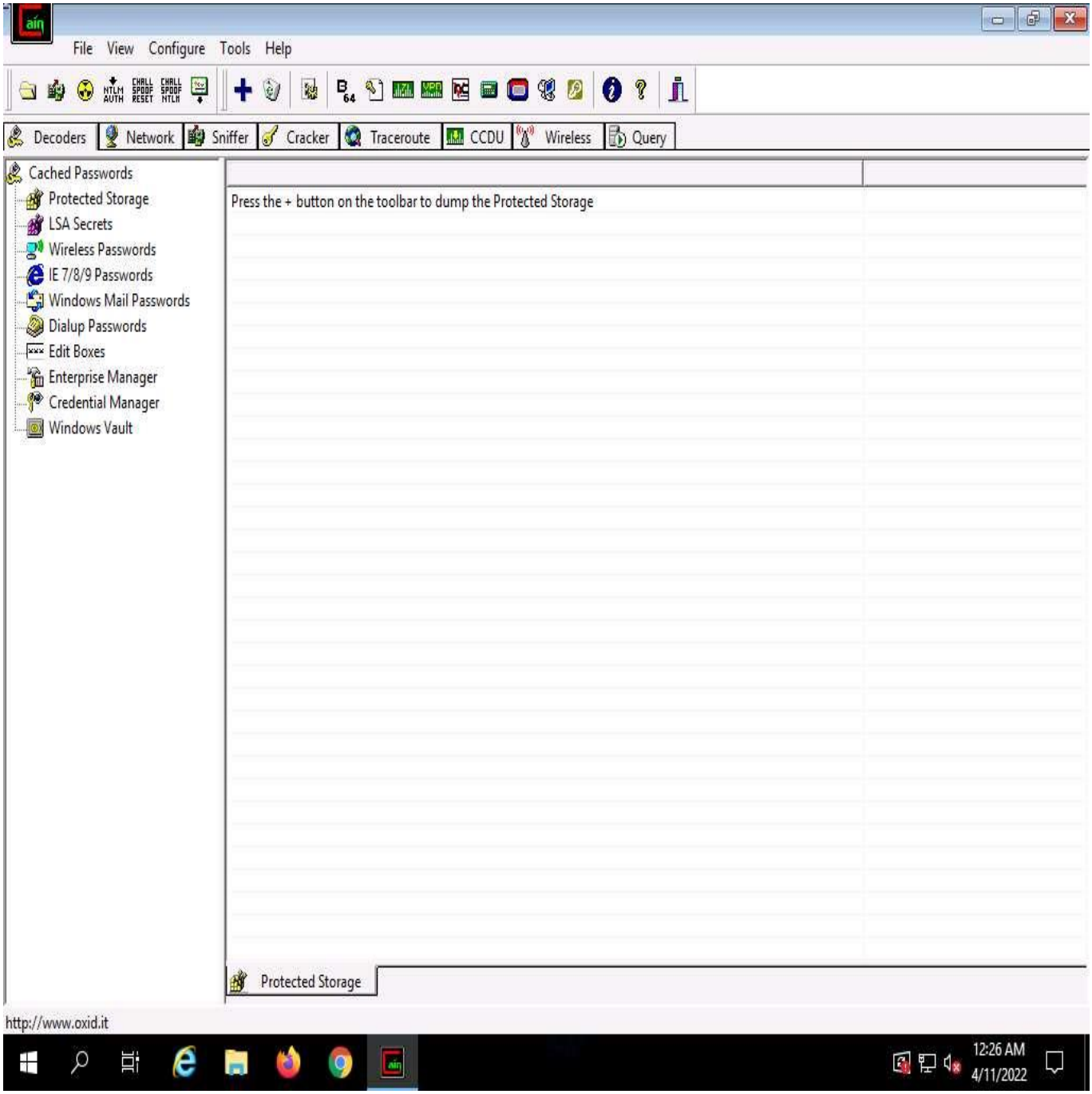
   Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



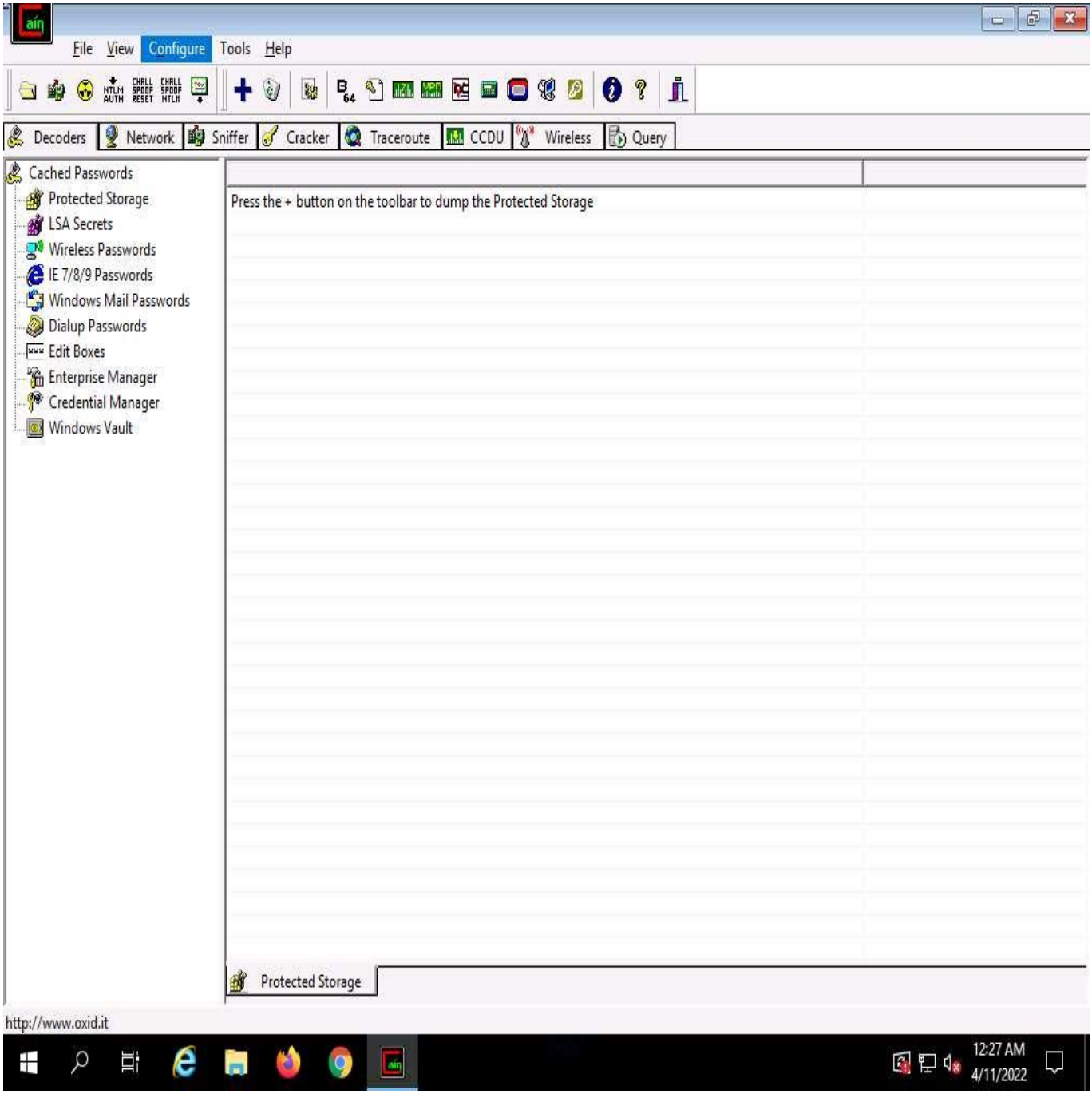
3. ☐ Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



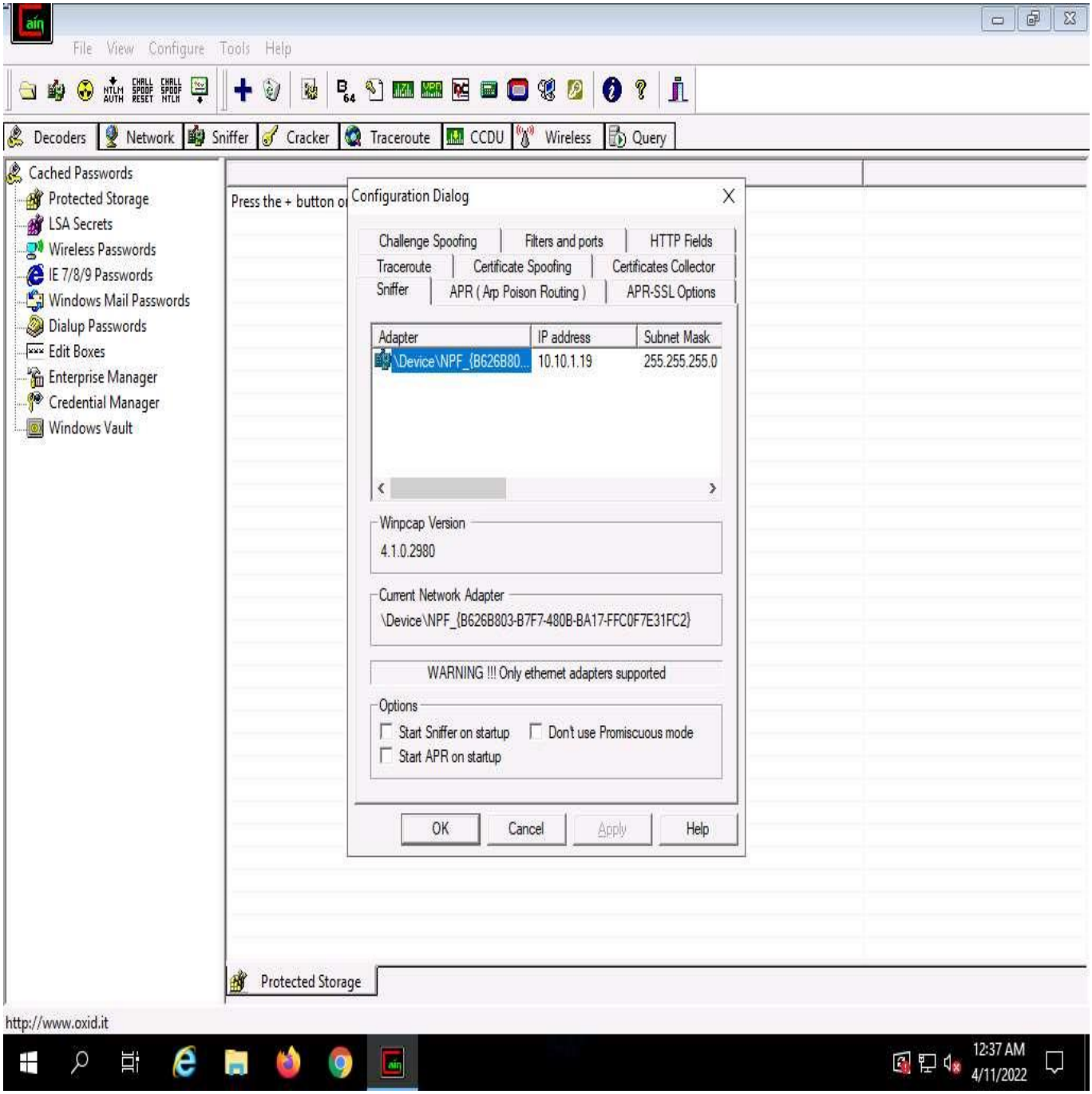
4. ☐ The **Cain & Abel** main window appears, as shown in the screenshot.



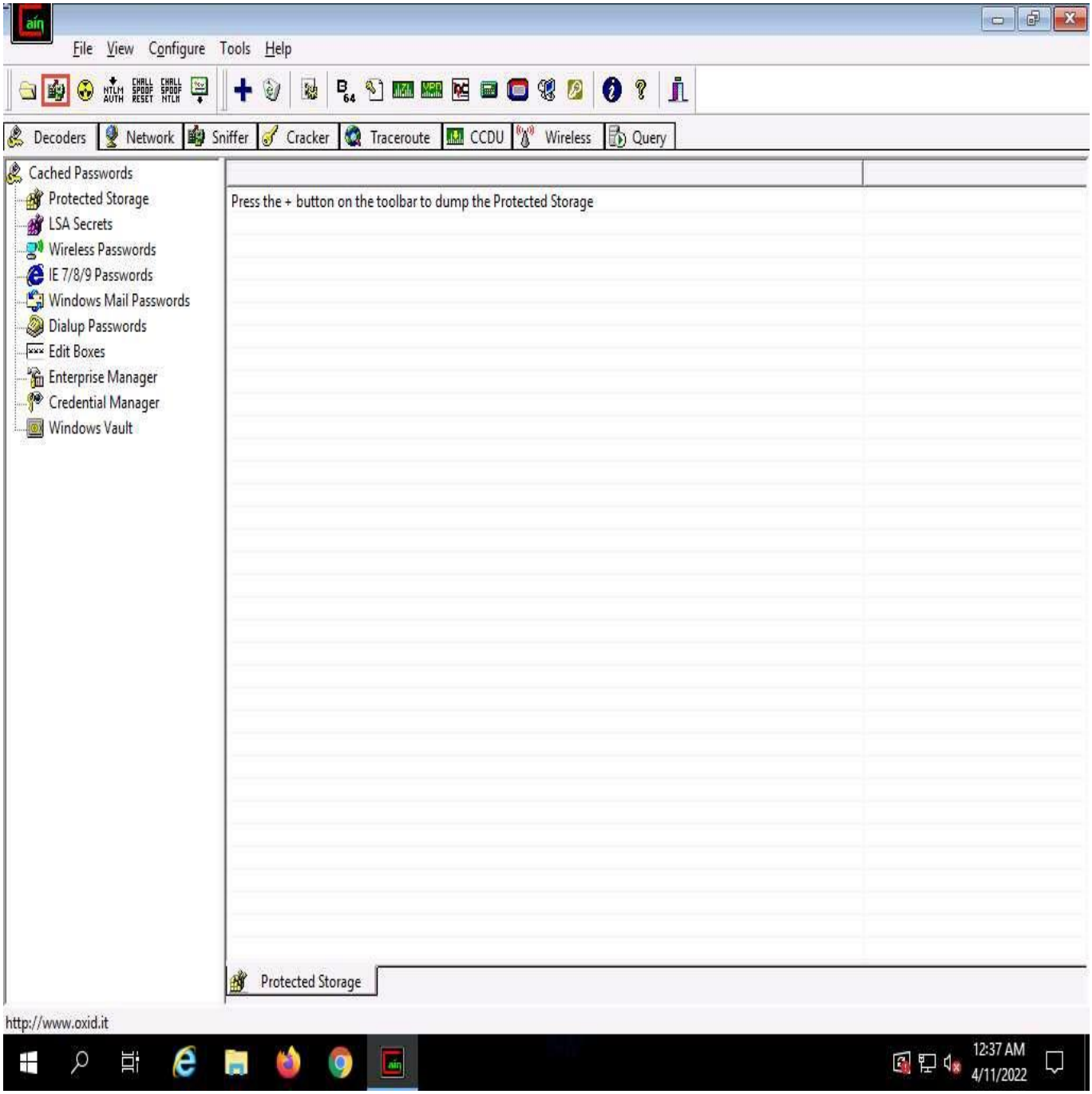
5. ☐ Click **Configure** from the menu bar to configure an ethernet card.



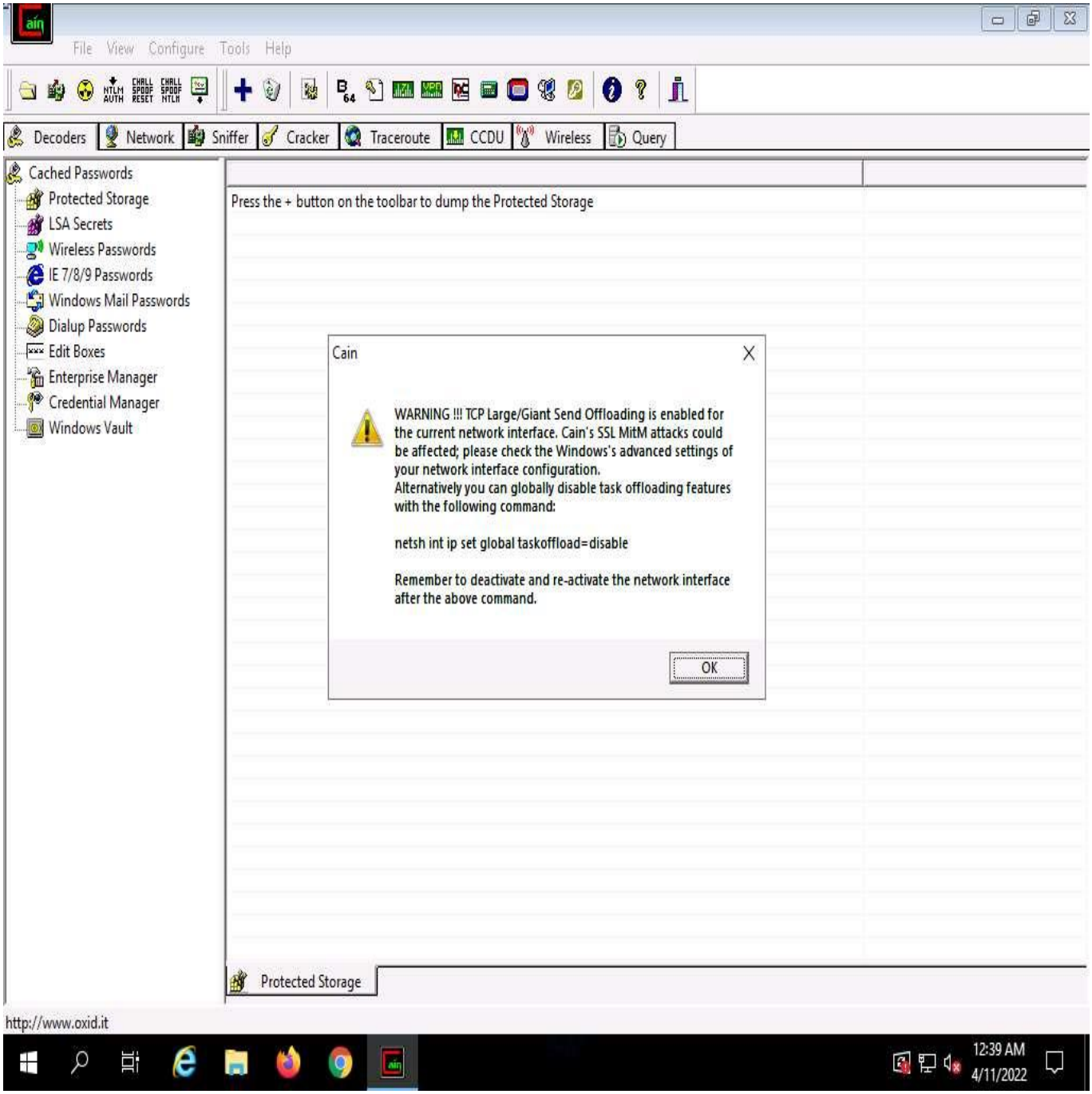
6. ☐ The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.



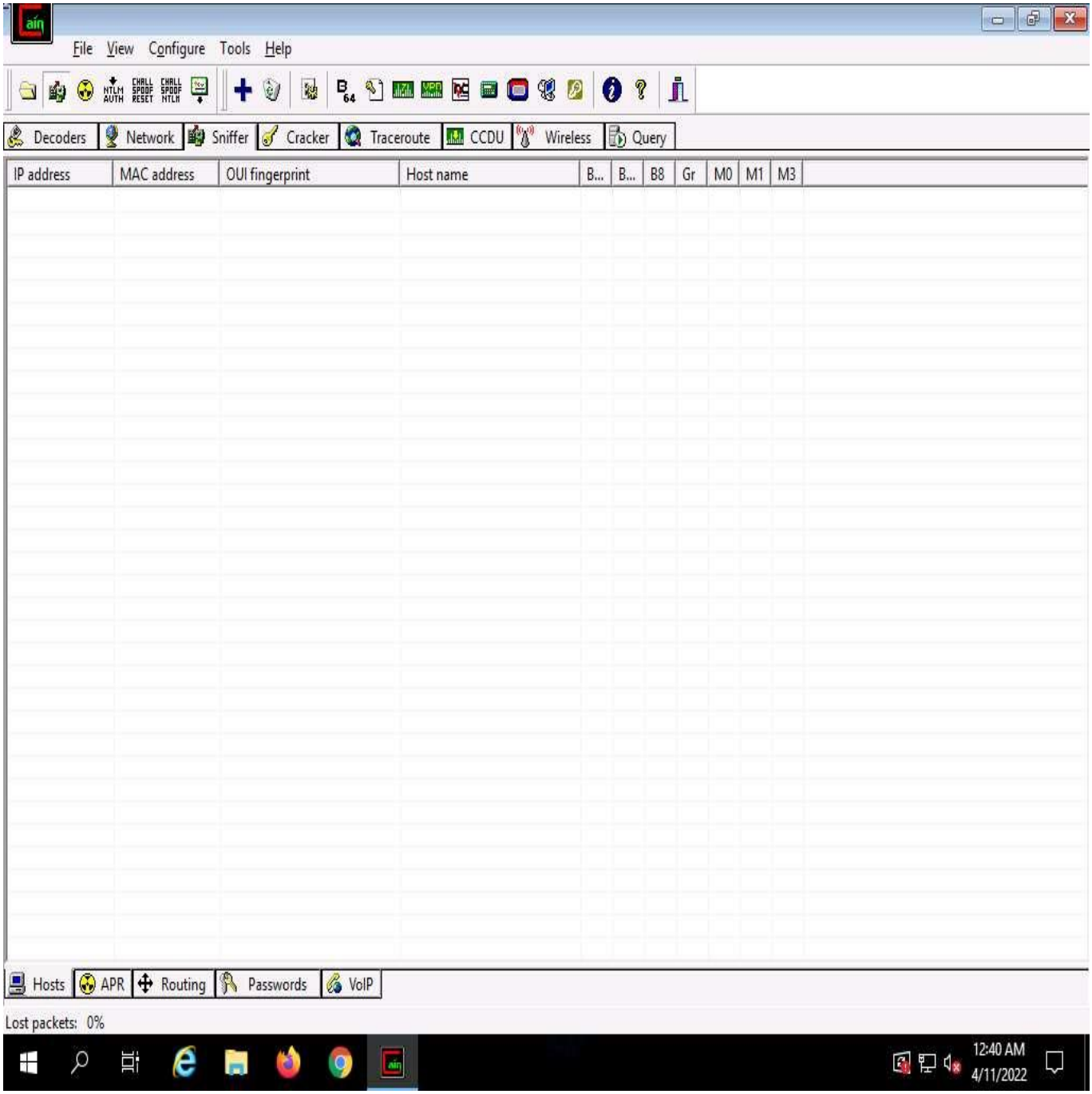
7. ☐ Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



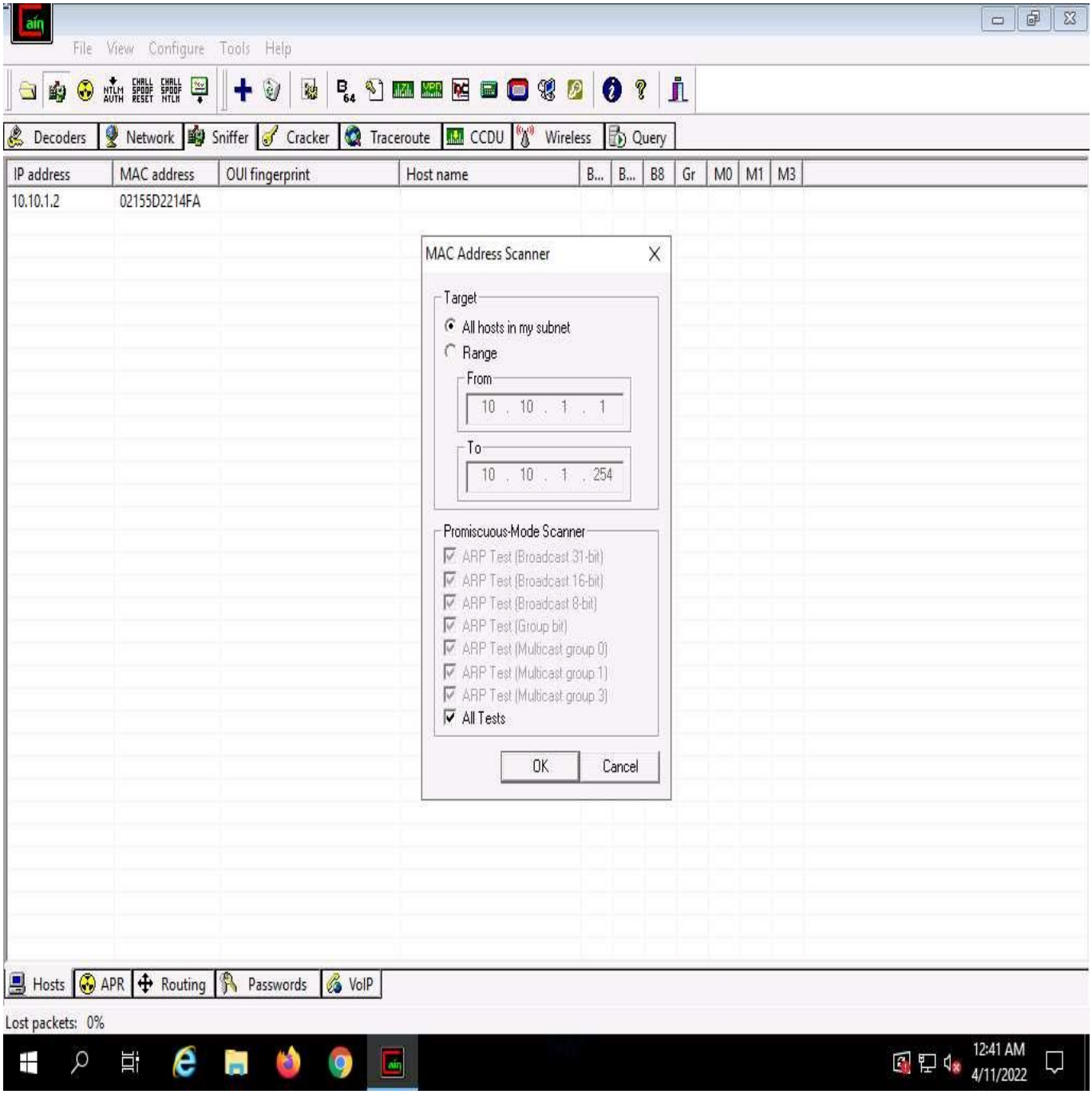
8. ☐ A **Cain** pop-up appears and displays a **Warning** message; click **OK**.



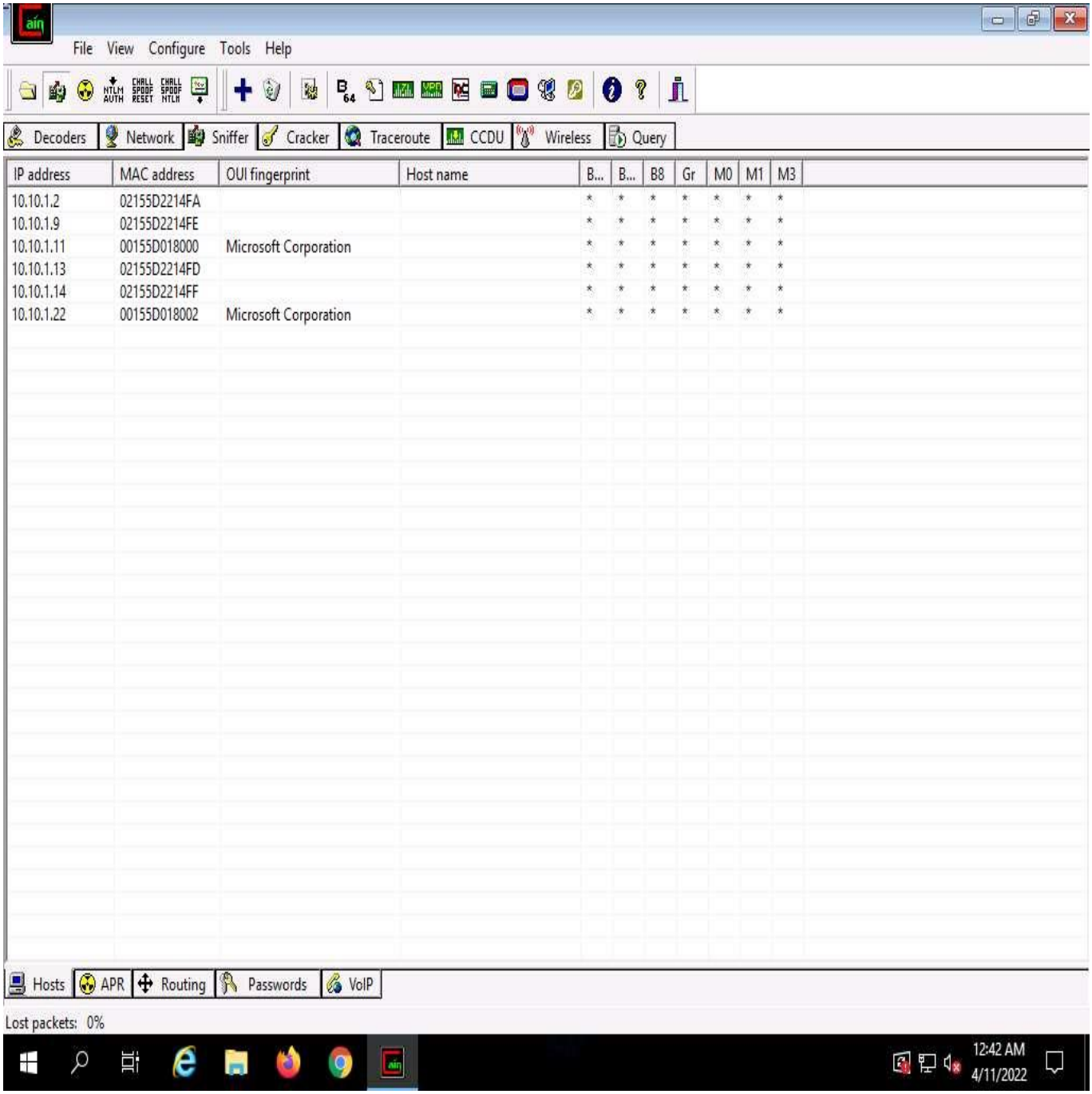
9. ☐ Now, click the **Sniffer** tab.



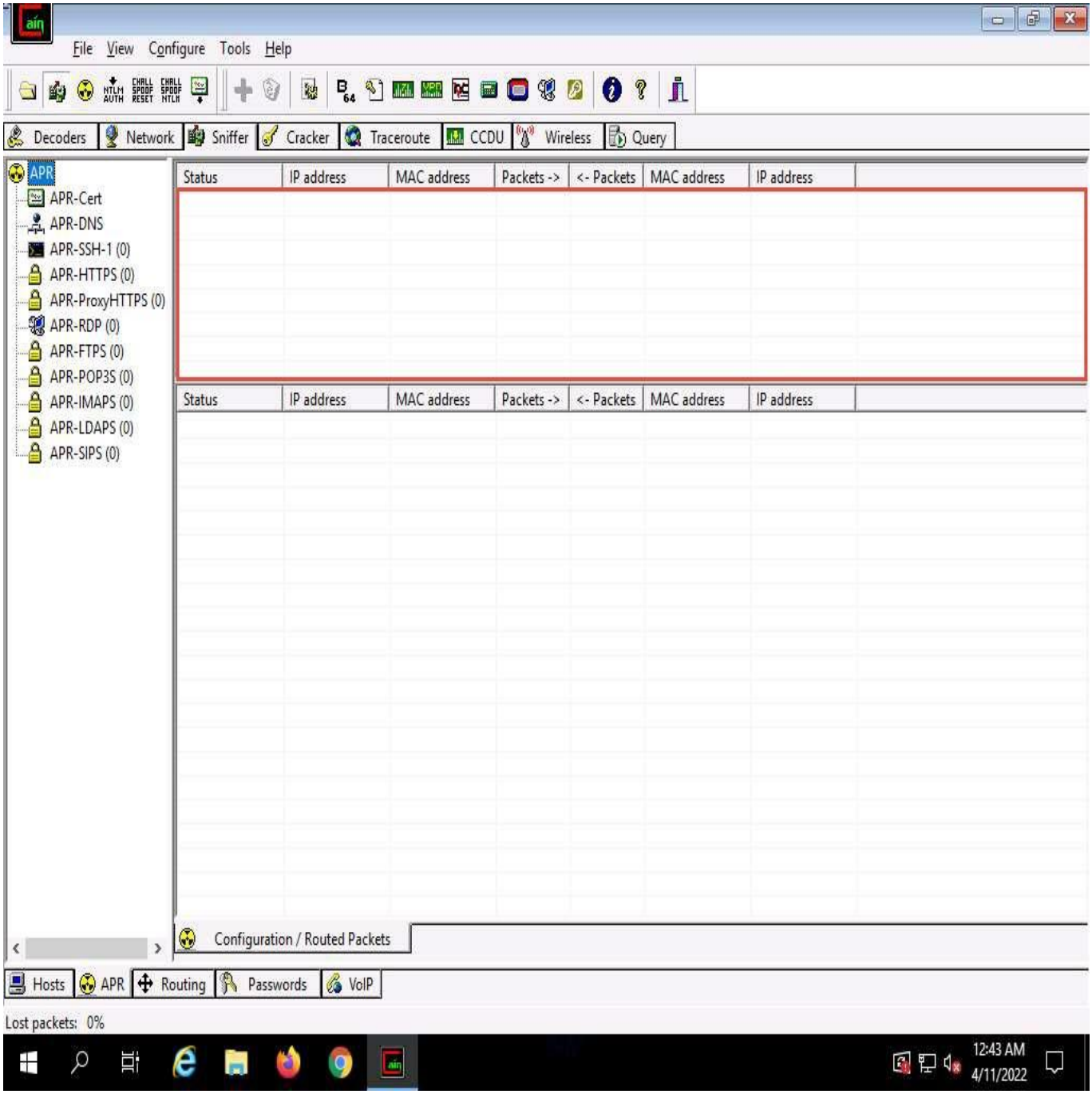
10. ☐ Click the plus (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
11. ☐ The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.



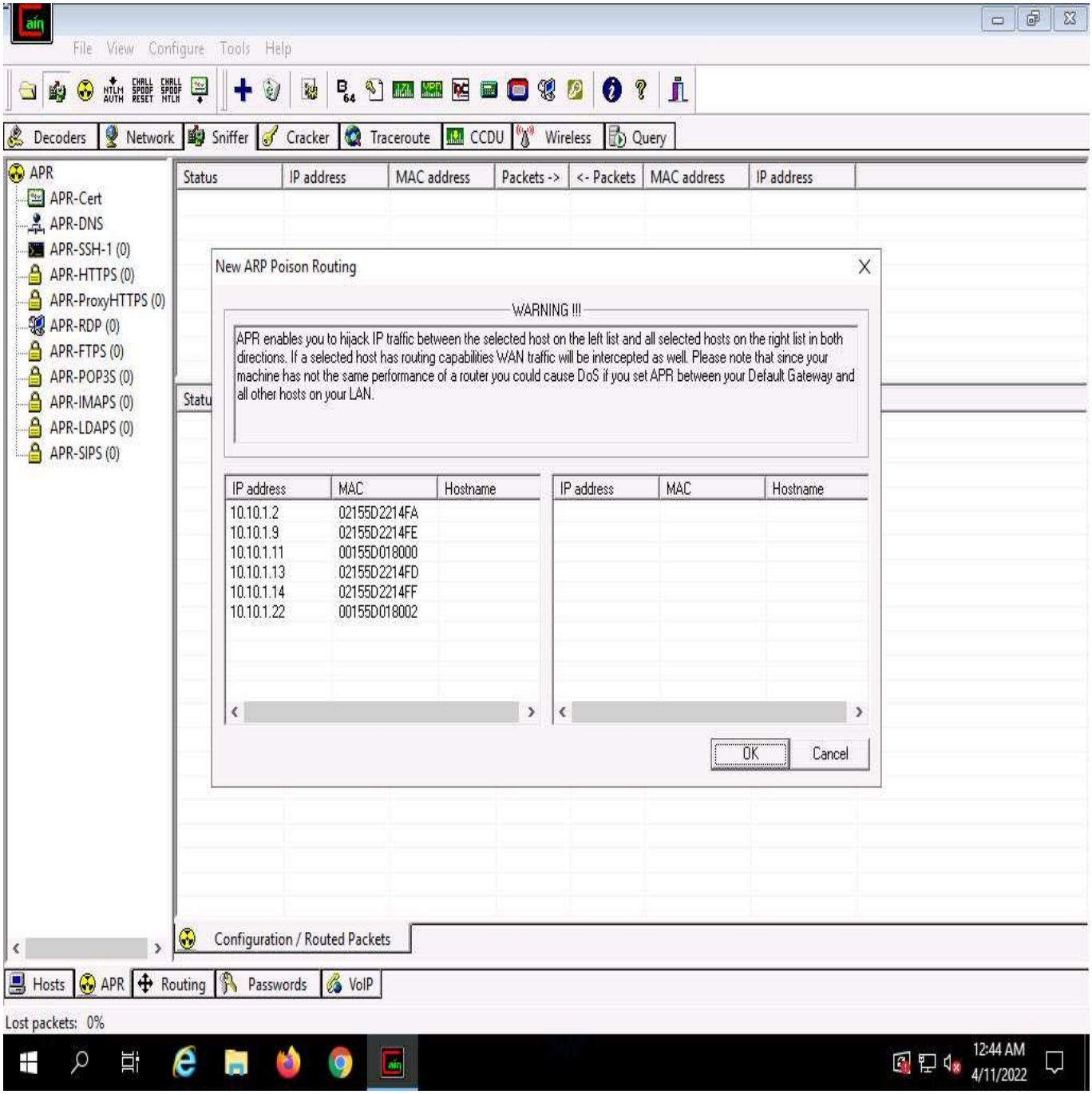
12. ☐ Cain & Abel starts scanning for MAC addresses and lists all those found.
13. ☐ After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.



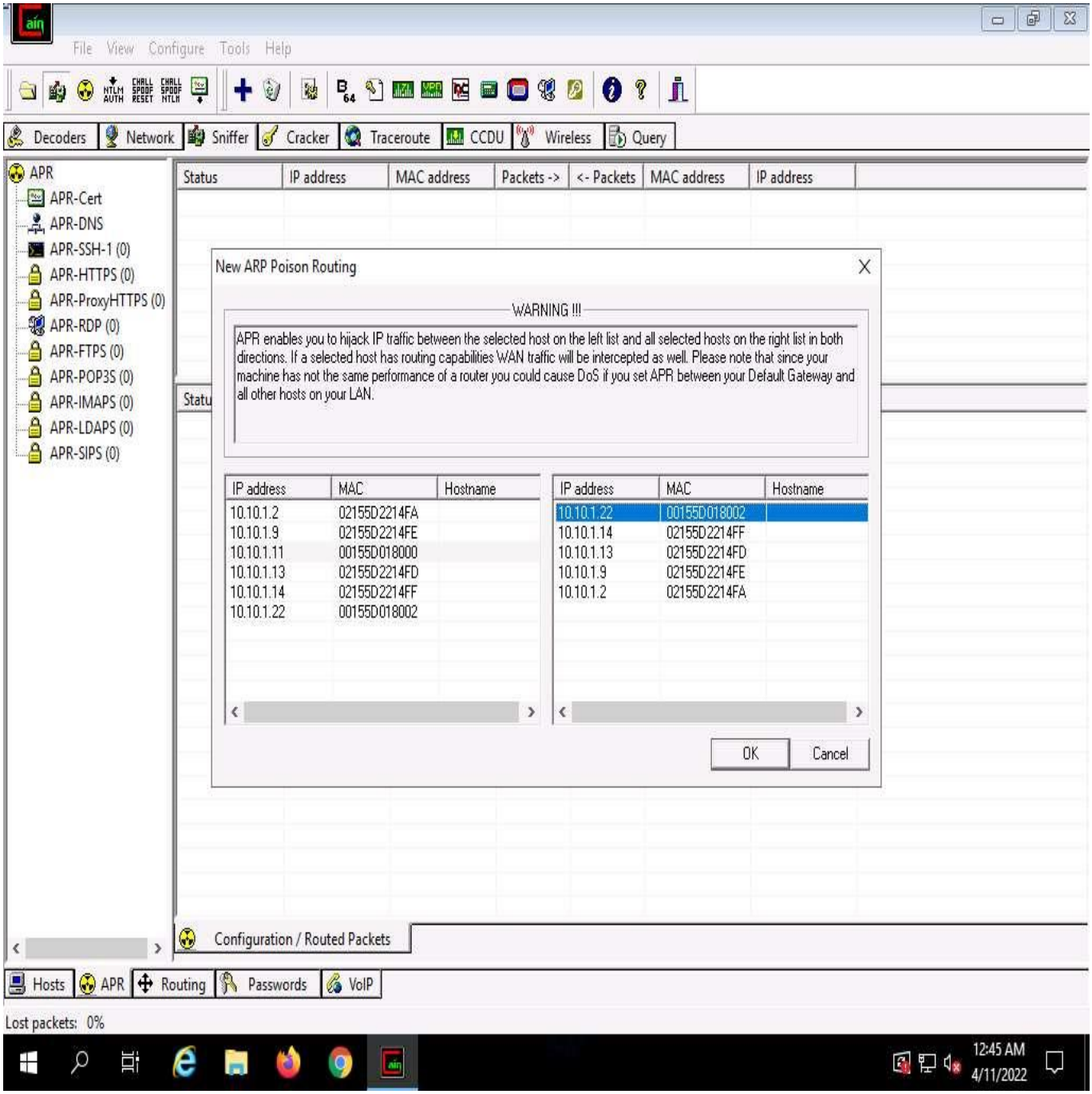
14. ☐ Now, click the **APR** tab at the bottom of the window.
15. ☐ APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (**+**) icon.



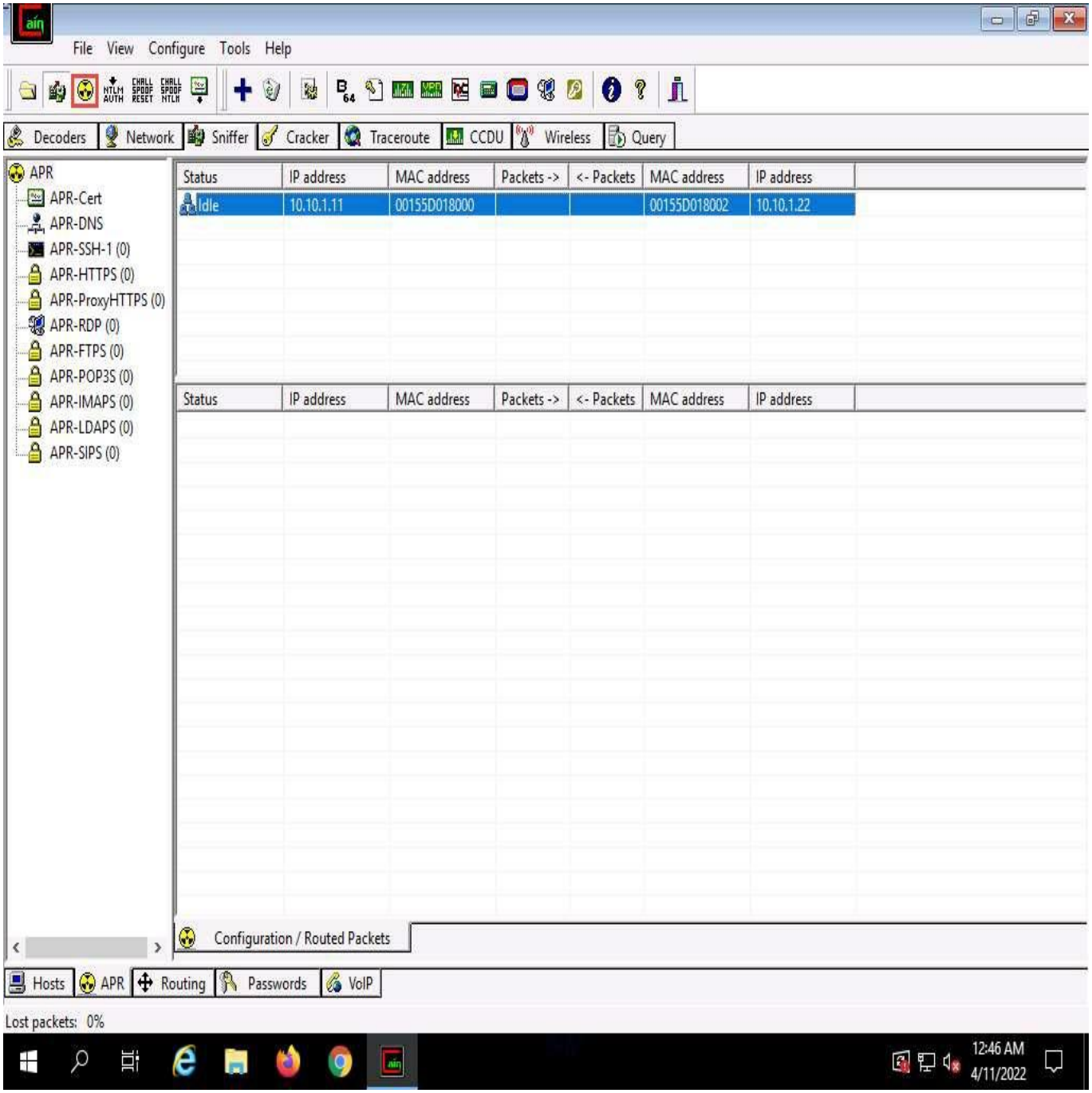
16. ☐ Click the plus (**+**) icon, a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.

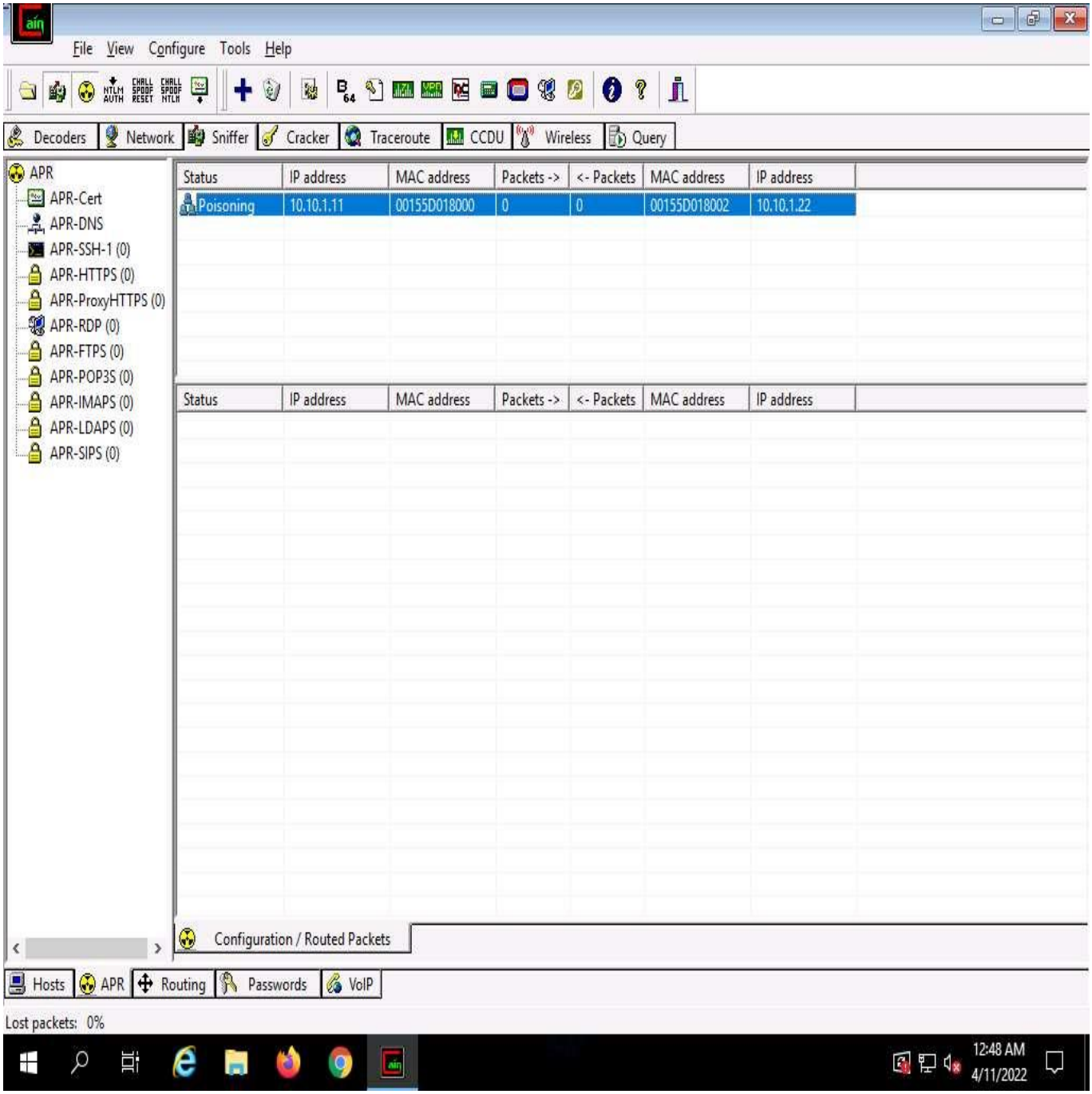


17. ☐ To monitor the traffic between two systems (here, **Windows 11** and **Windows Server 2022**), click to select **10.10.1.11** (Windows 11) from the left-hand pane and **10.10.1.22** (**Windows Server 2022**) from the right-hand pane; click **OK**.

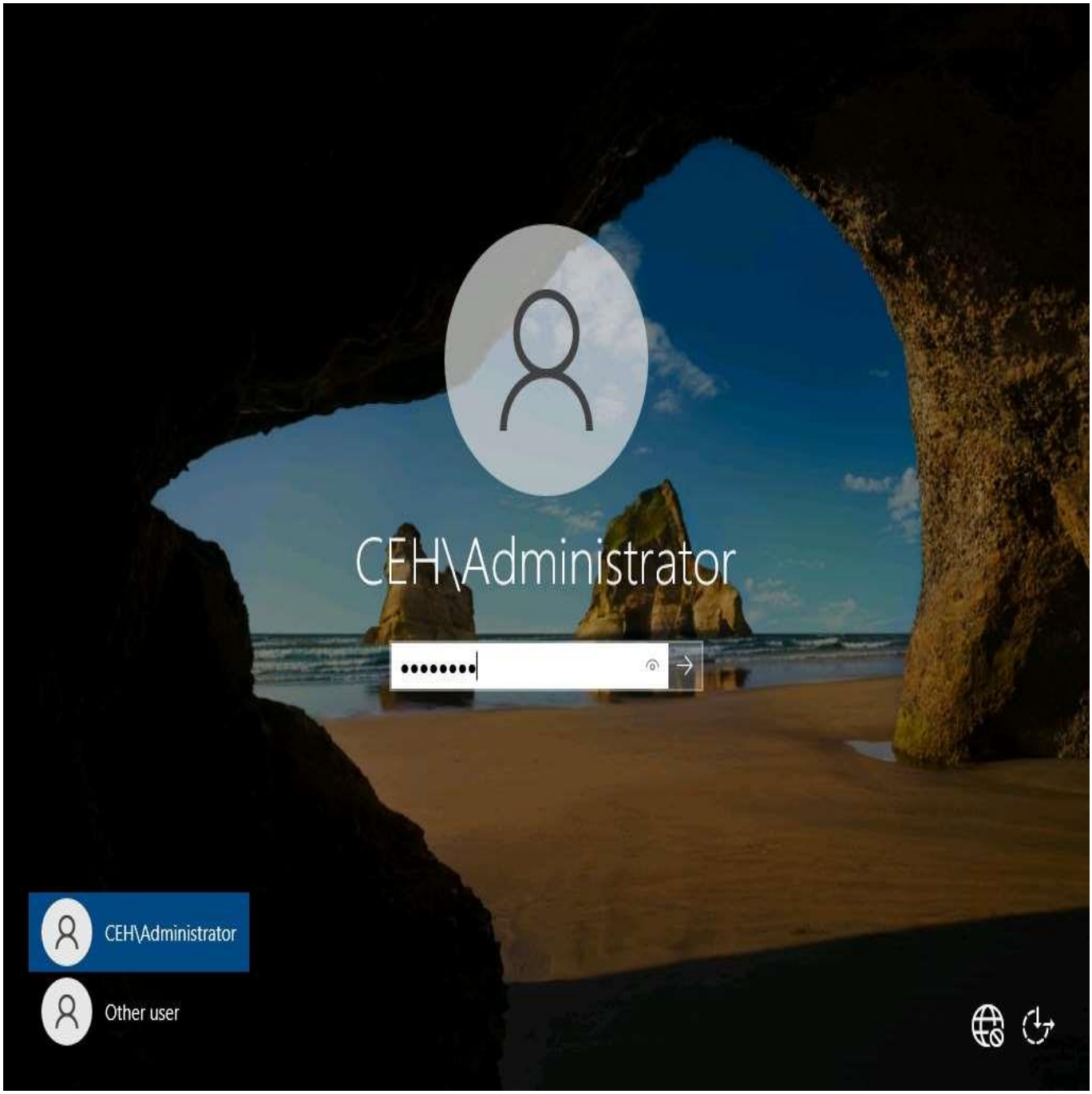


18. ☐ Click to select the created target IP address scan displayed in the **Configuration / Routes Packets** tab.
19. ☐ Click on the **Start/Stop APR** icon to start capturing ARP packets. The **Status** will change from **Idle** to **Poisoning**.

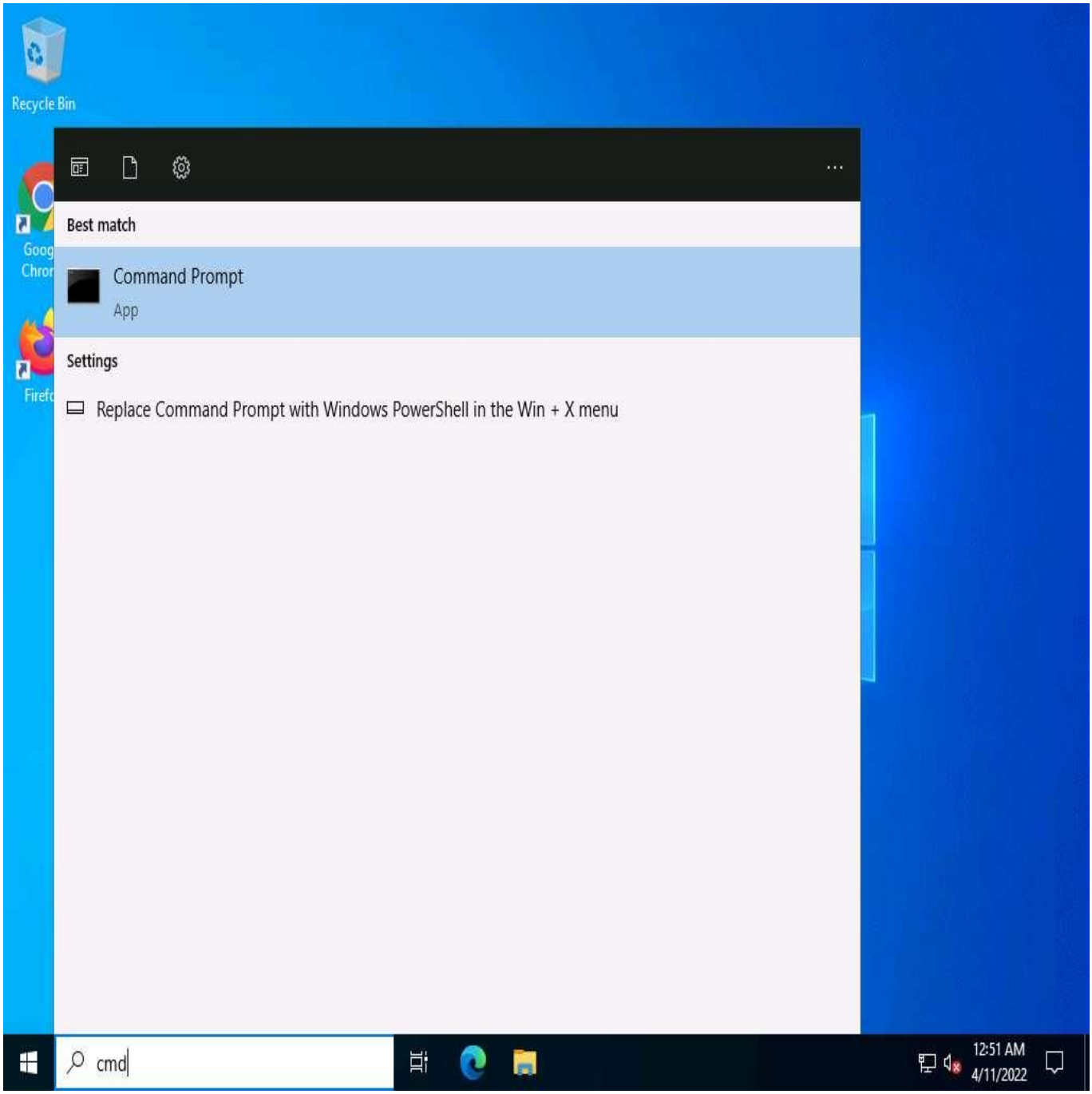

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 10.10.1.11 00155D018000 00155D018002 10.10.1.22
Status IP address MAC address Packets -> <- Packets MAC address IP address
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
12:46 AM
4/11/2022



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

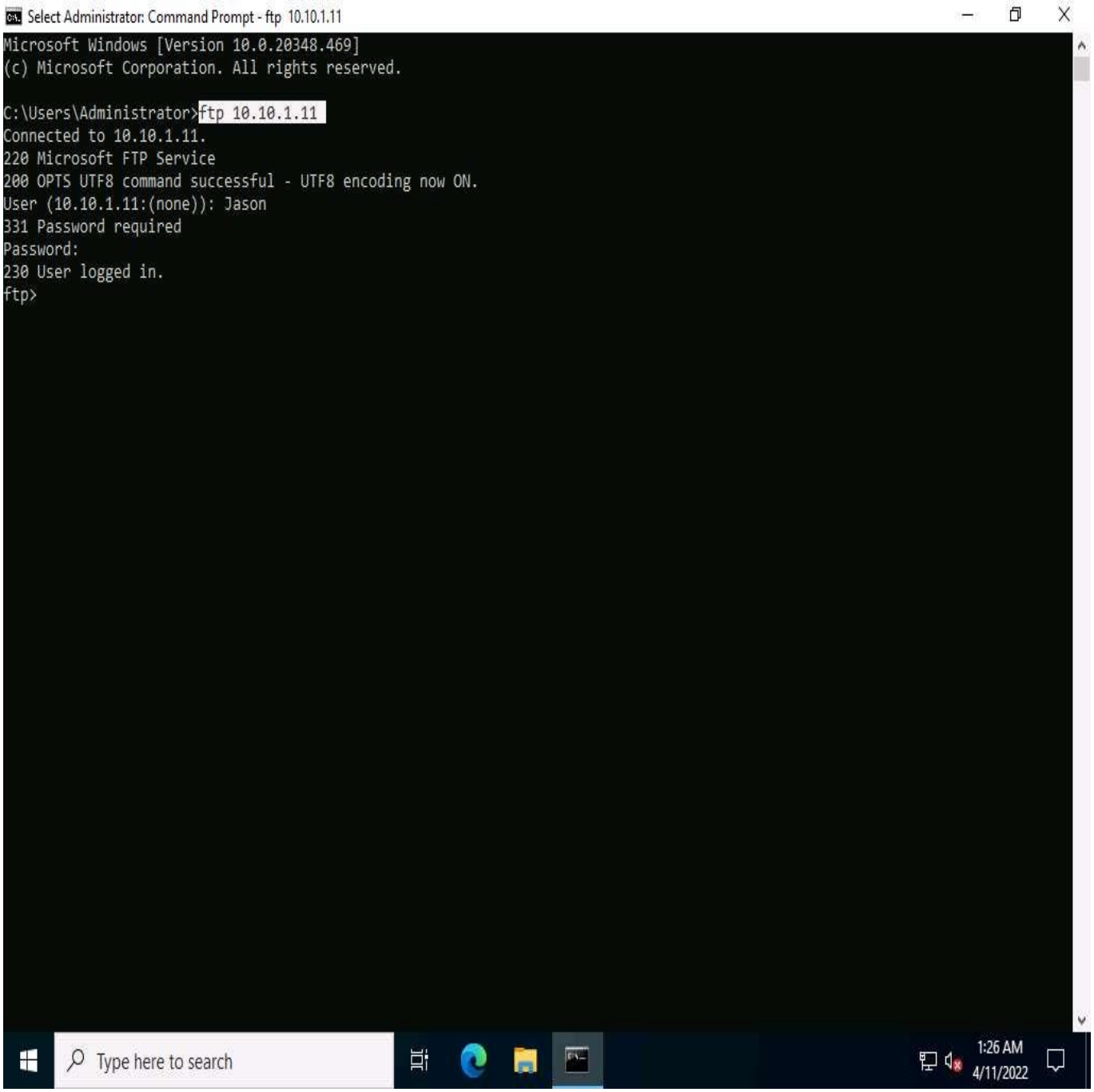


21. ☐ Click the **Type here to search** icon at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.

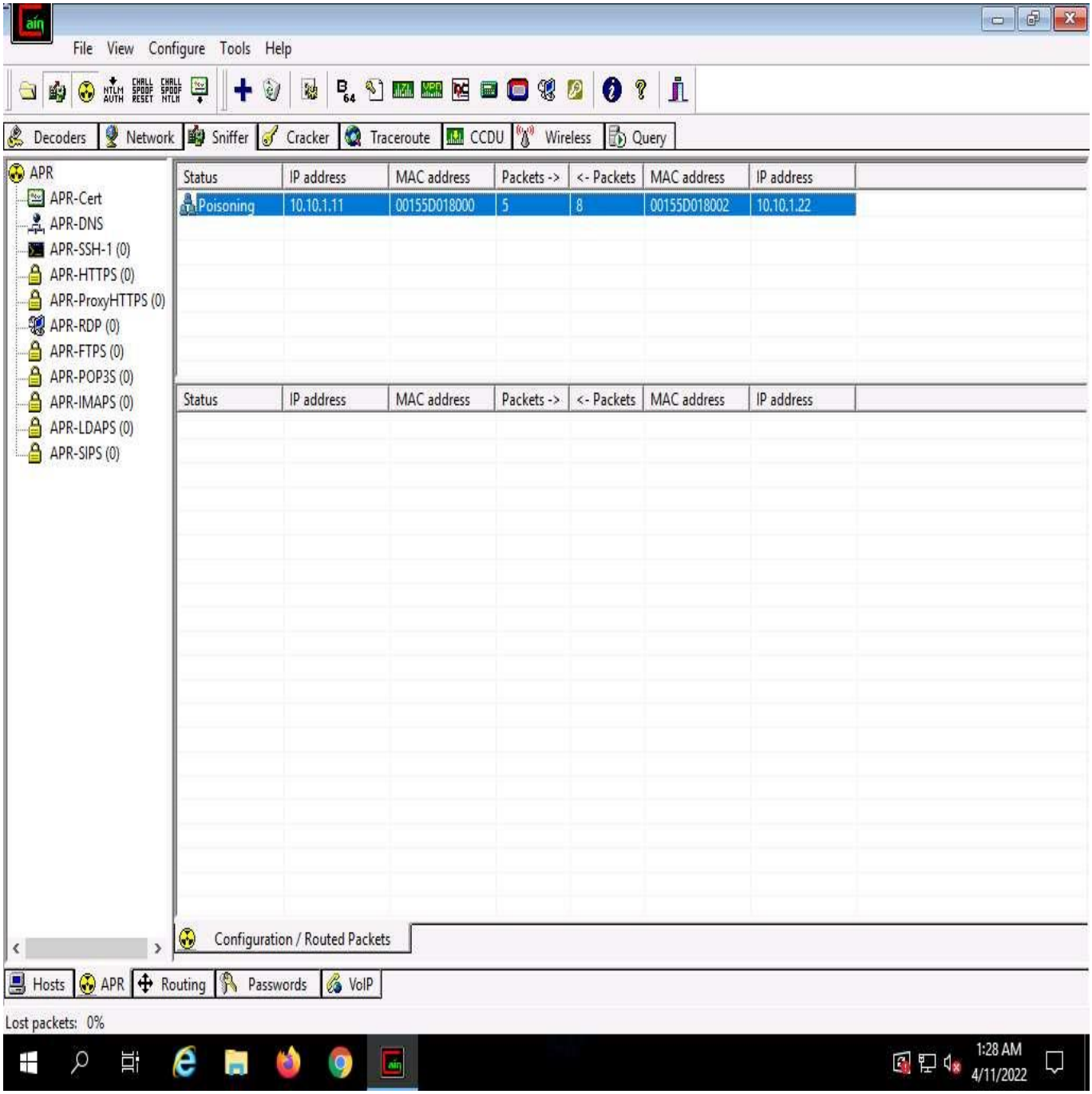


22. ☐ The **Command Prompt** window appears; type **ftp 10.10.1.11** (the IP address of **Windows 11**) and press **Enter**.
23. ☐ When prompted for a **User**, type "**Jason**" and press **Enter**; for a **Password**, type "**qwerty**" and press **Enter**.

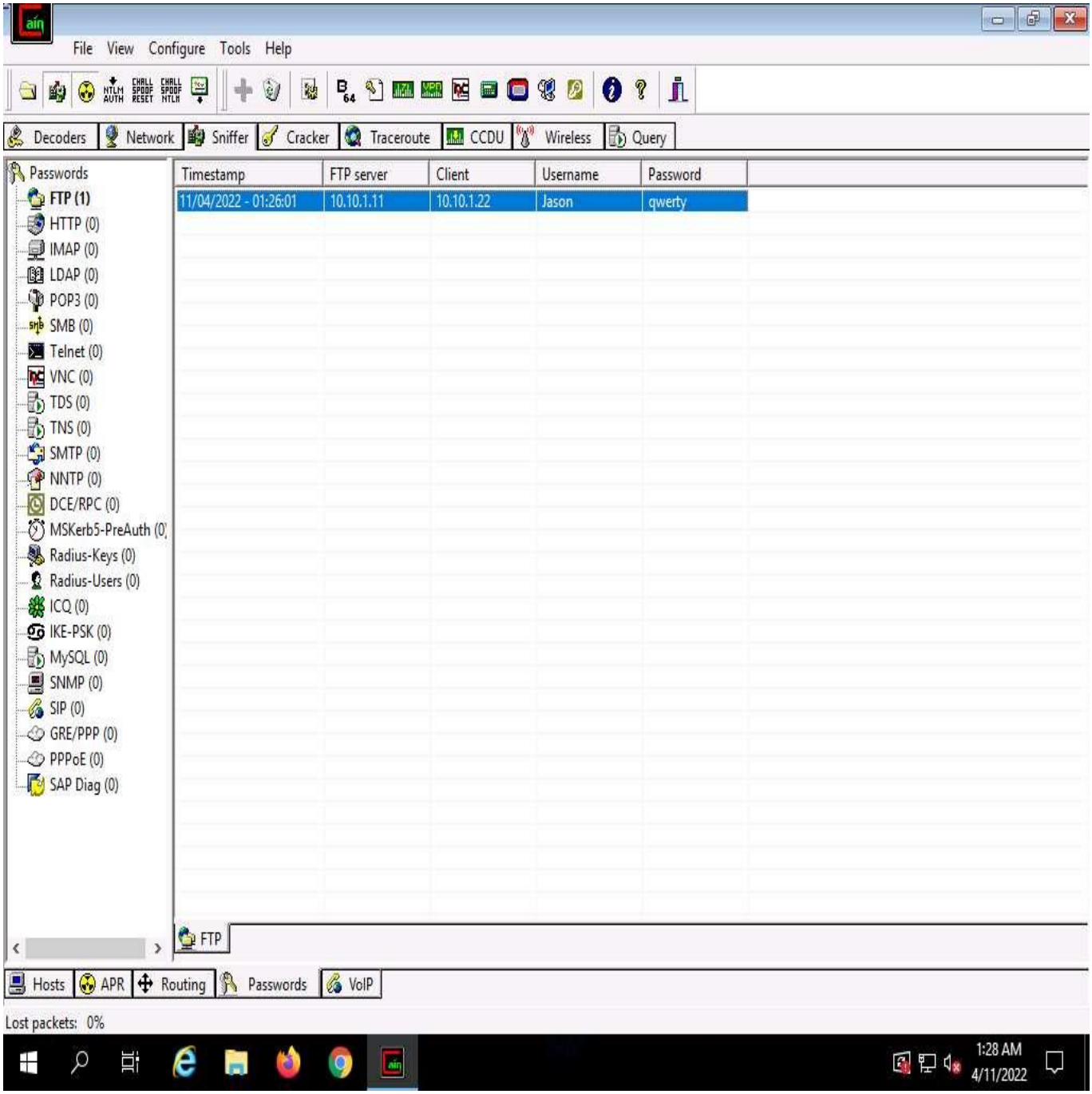
Irrespective of a successful login, Cain & Abel captures the password entered during login.



24. ☐ Click 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.



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.

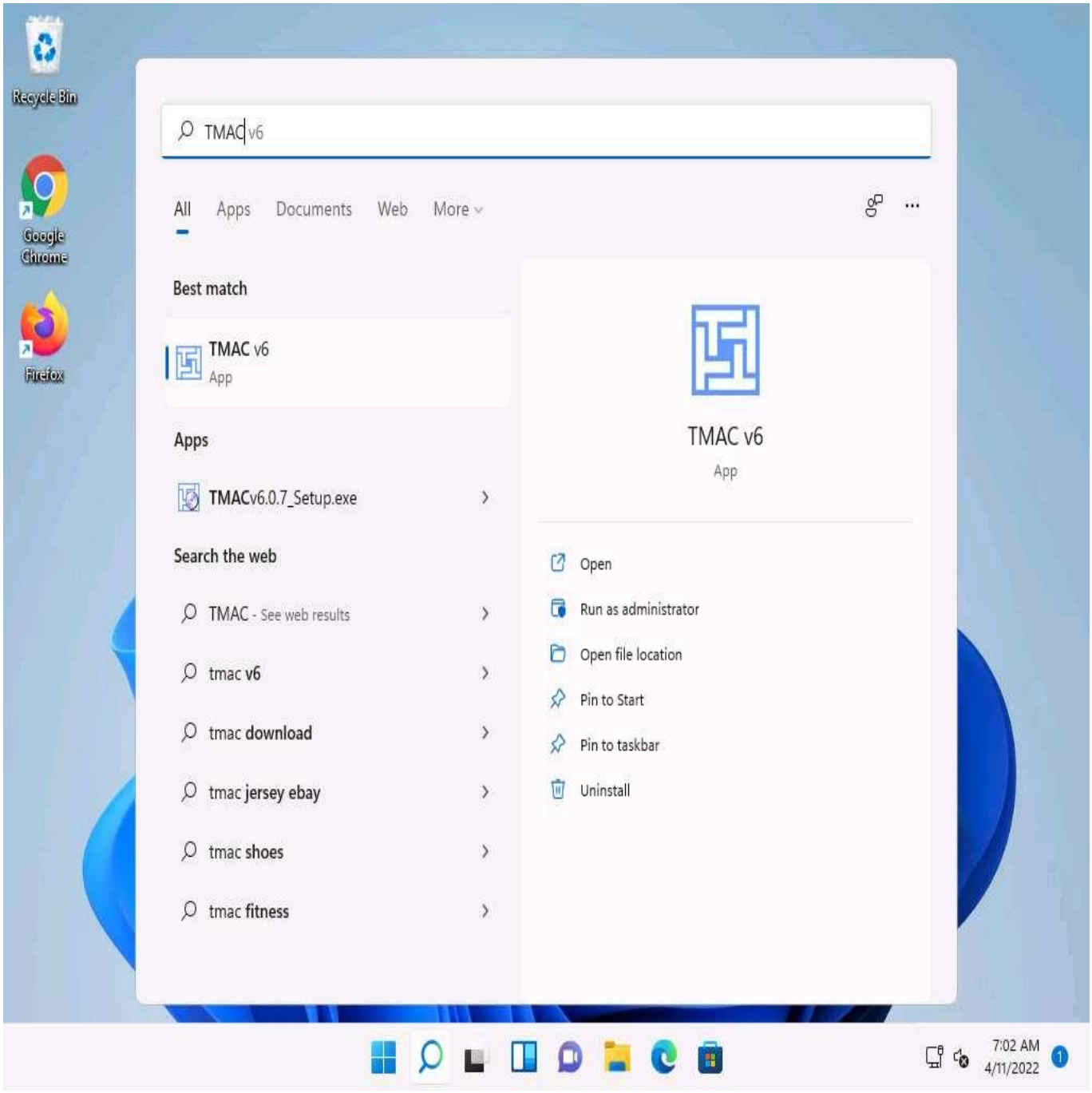
Here, we will use TMAC and SMAC tools to perform MAC spoofing.

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

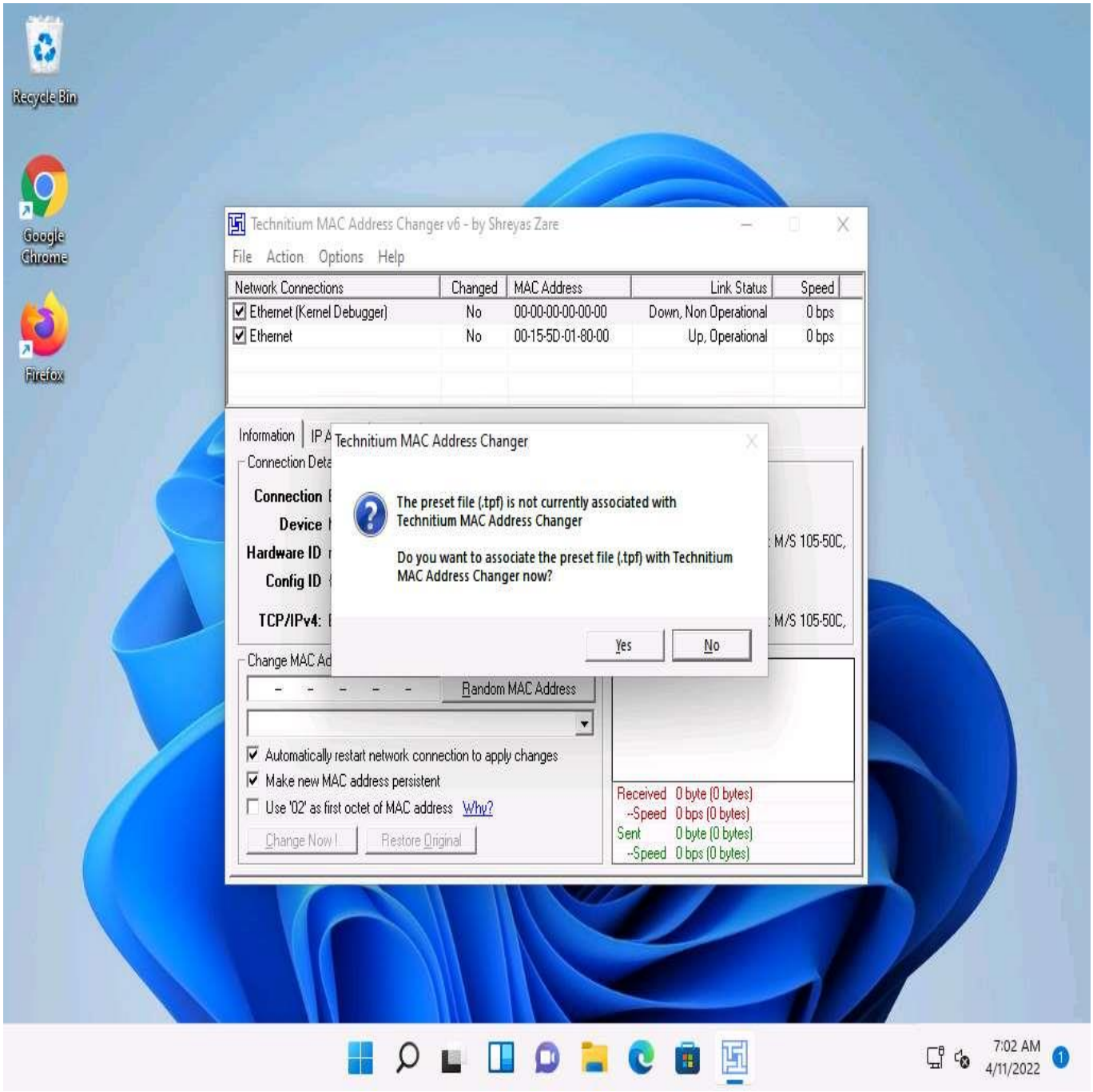
   If a **User Account Control** pop-up appears, click **Yes**.

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.

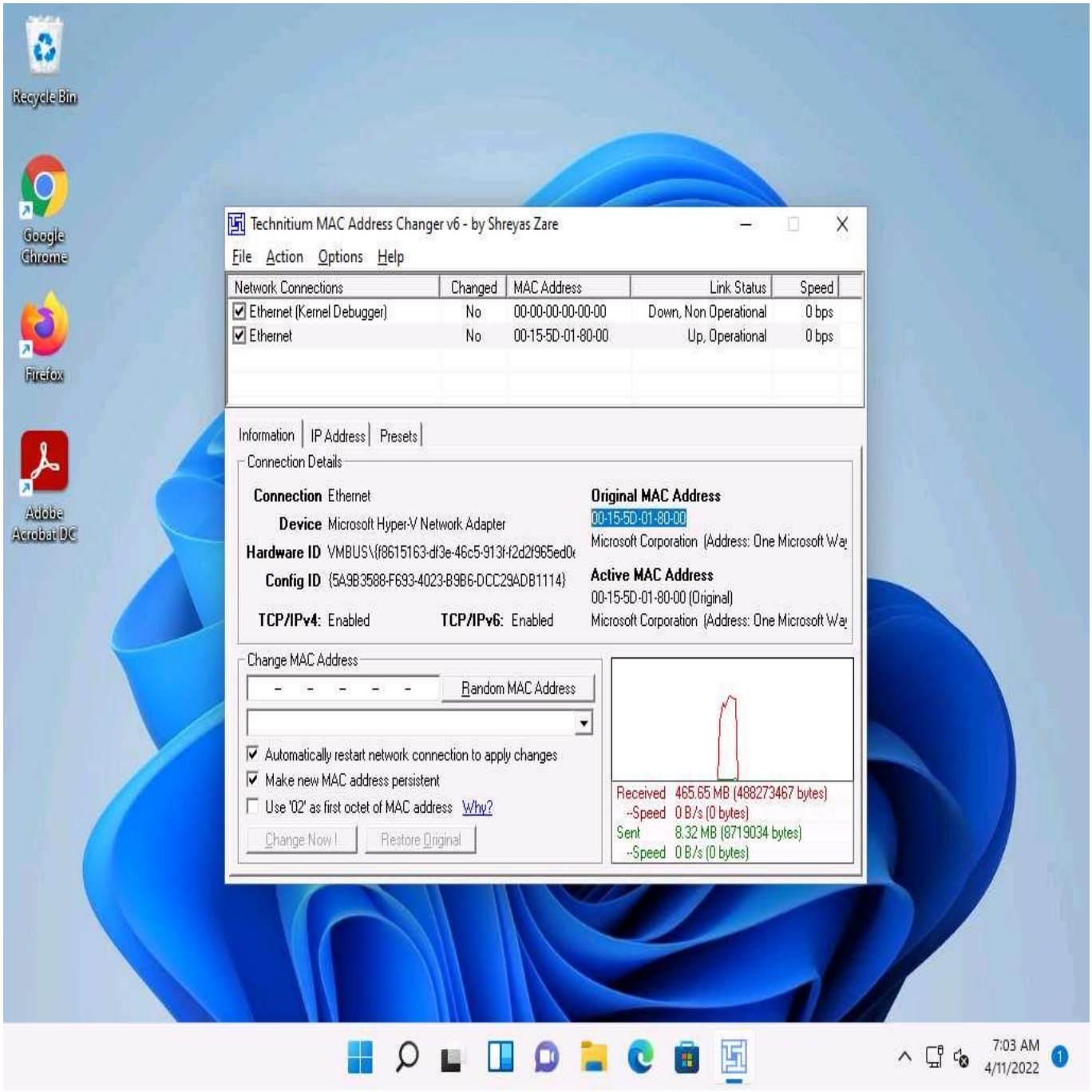
   If a **User Account Control** pop-up appears, click **Yes**.



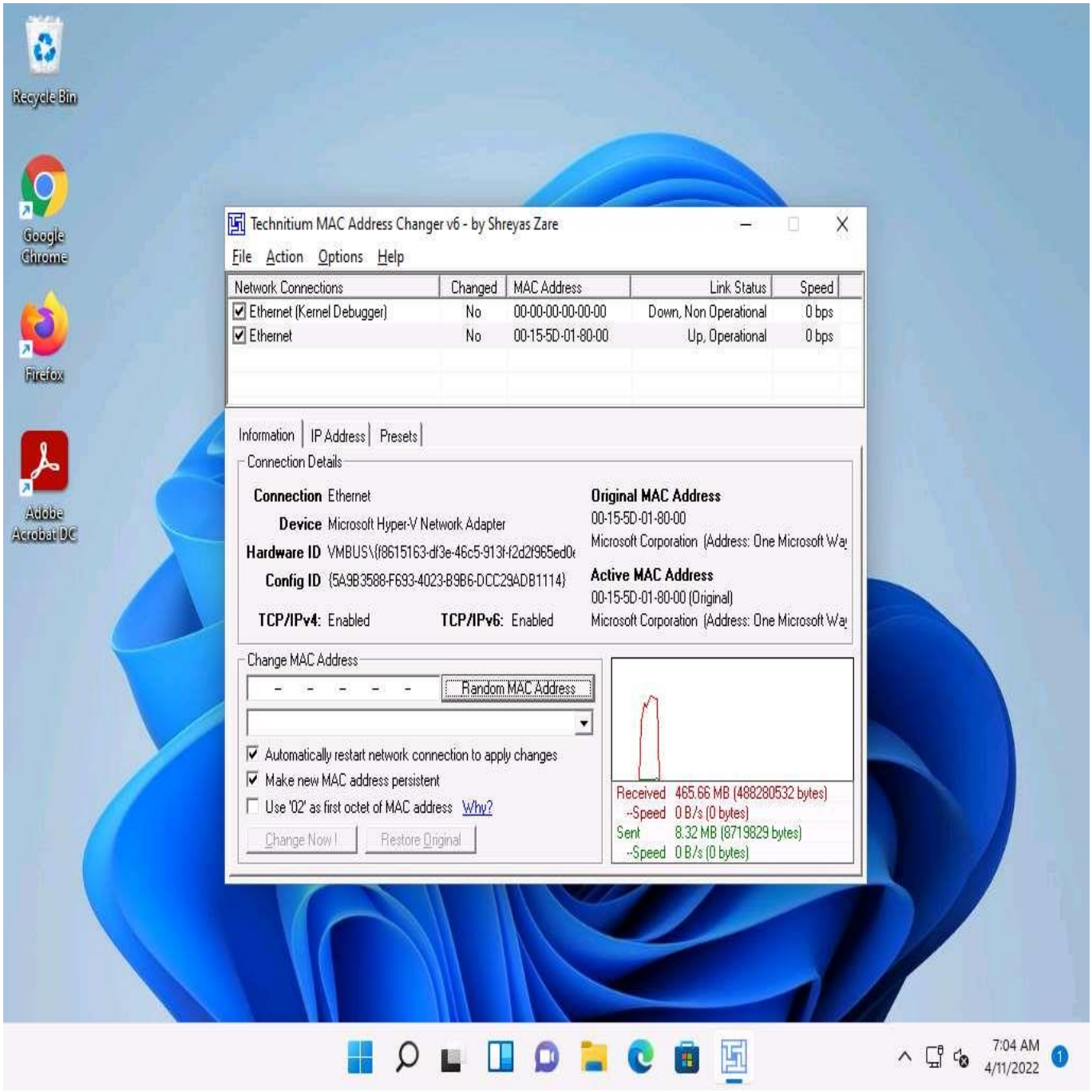
3. ☐ The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.



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.

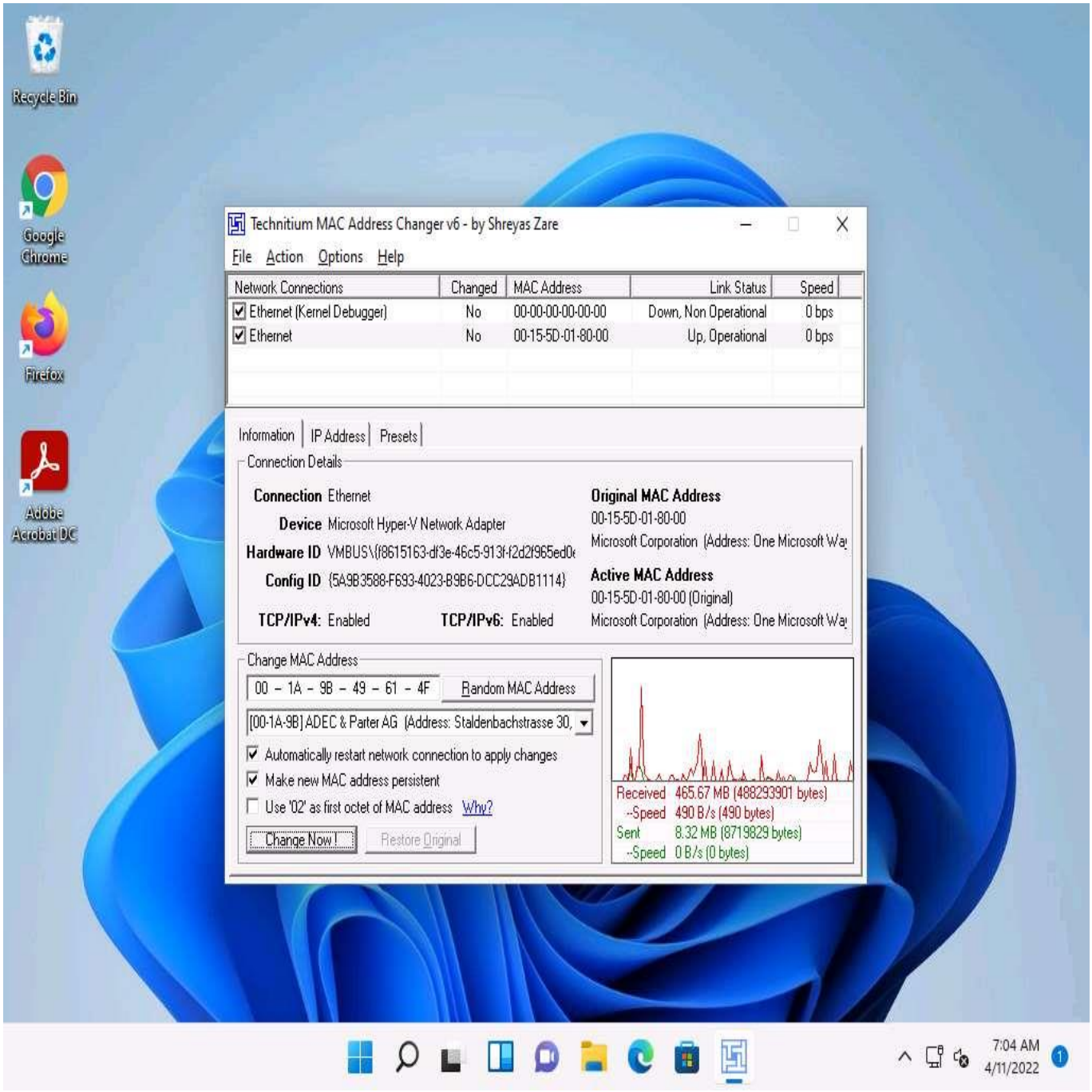


6. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

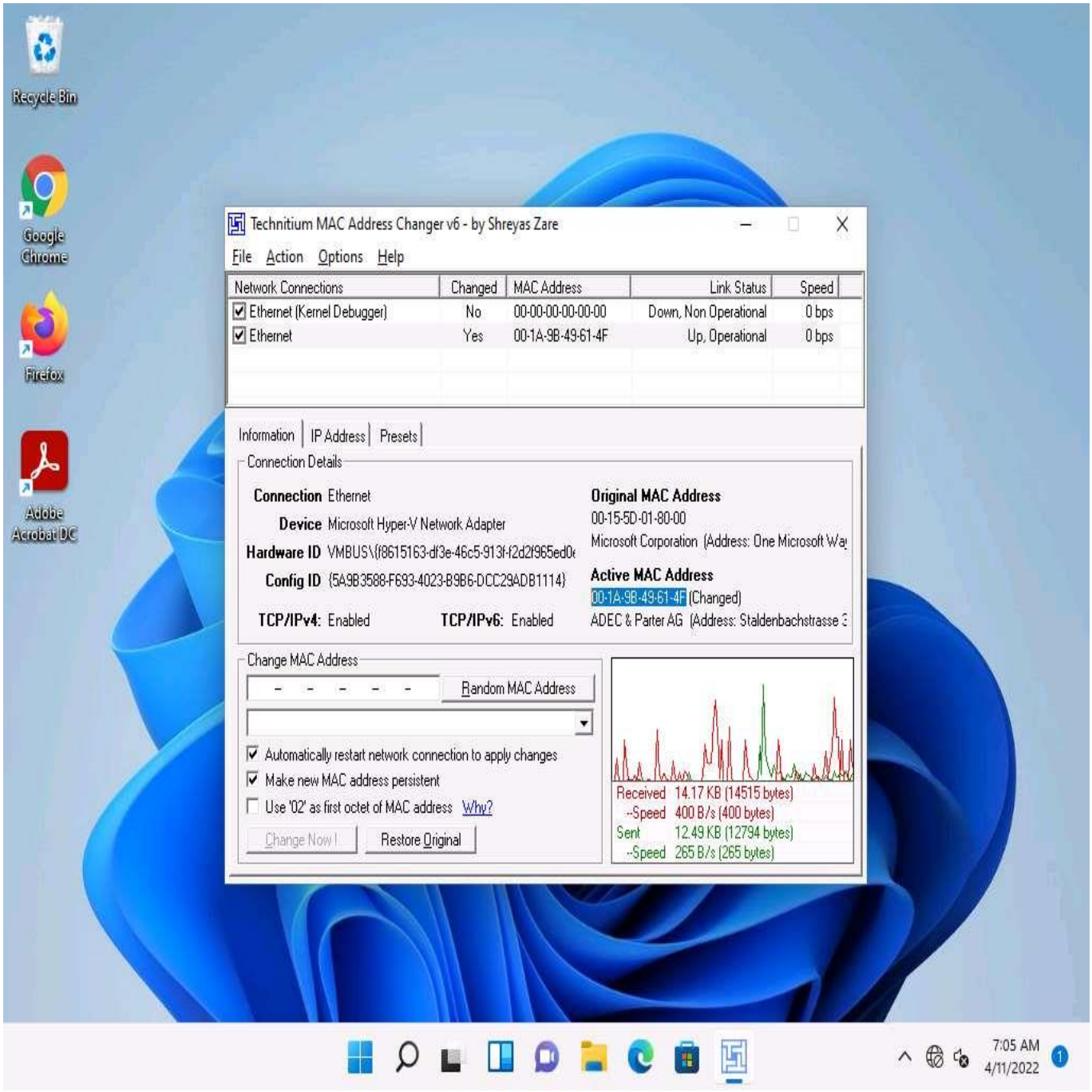


7. A **Random MAC Address** is generated and appears under the **Change MAC Address** field. Click the **Change Now !** button to change the MAC address.

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

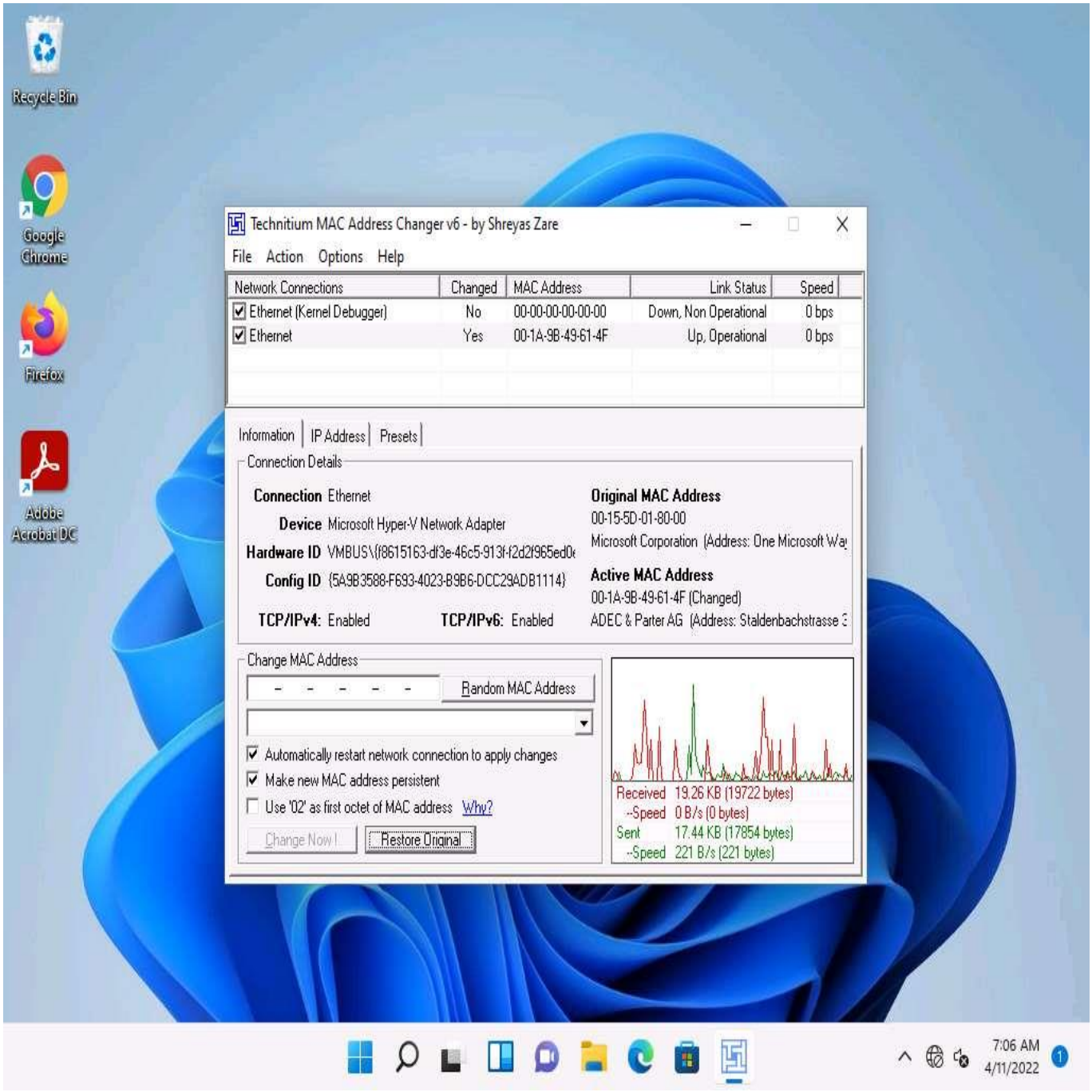


8. ☐ Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.



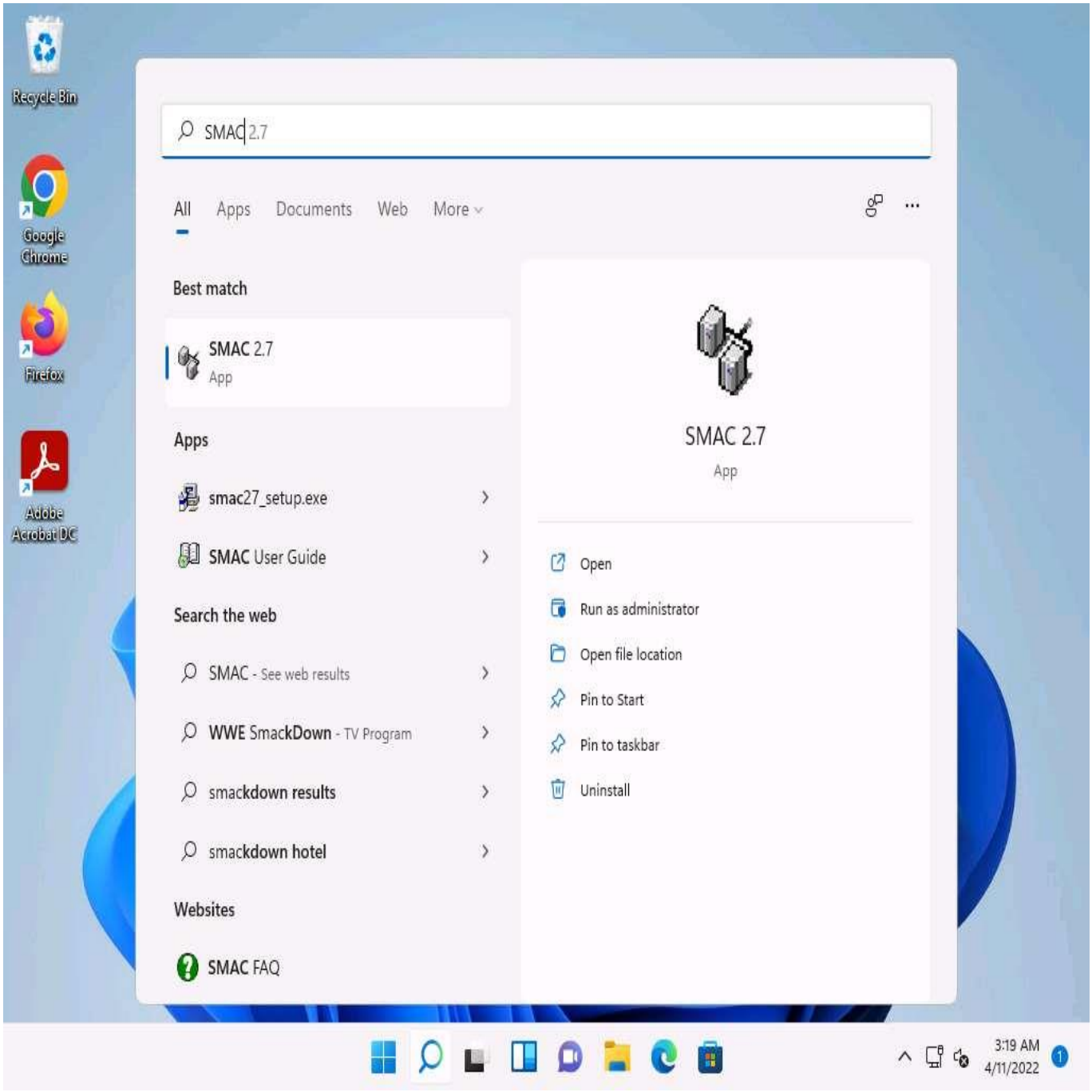
9. To restore the original MAC address, you can click on the **Restore Original** button present at the bottom of the TMAC window.

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

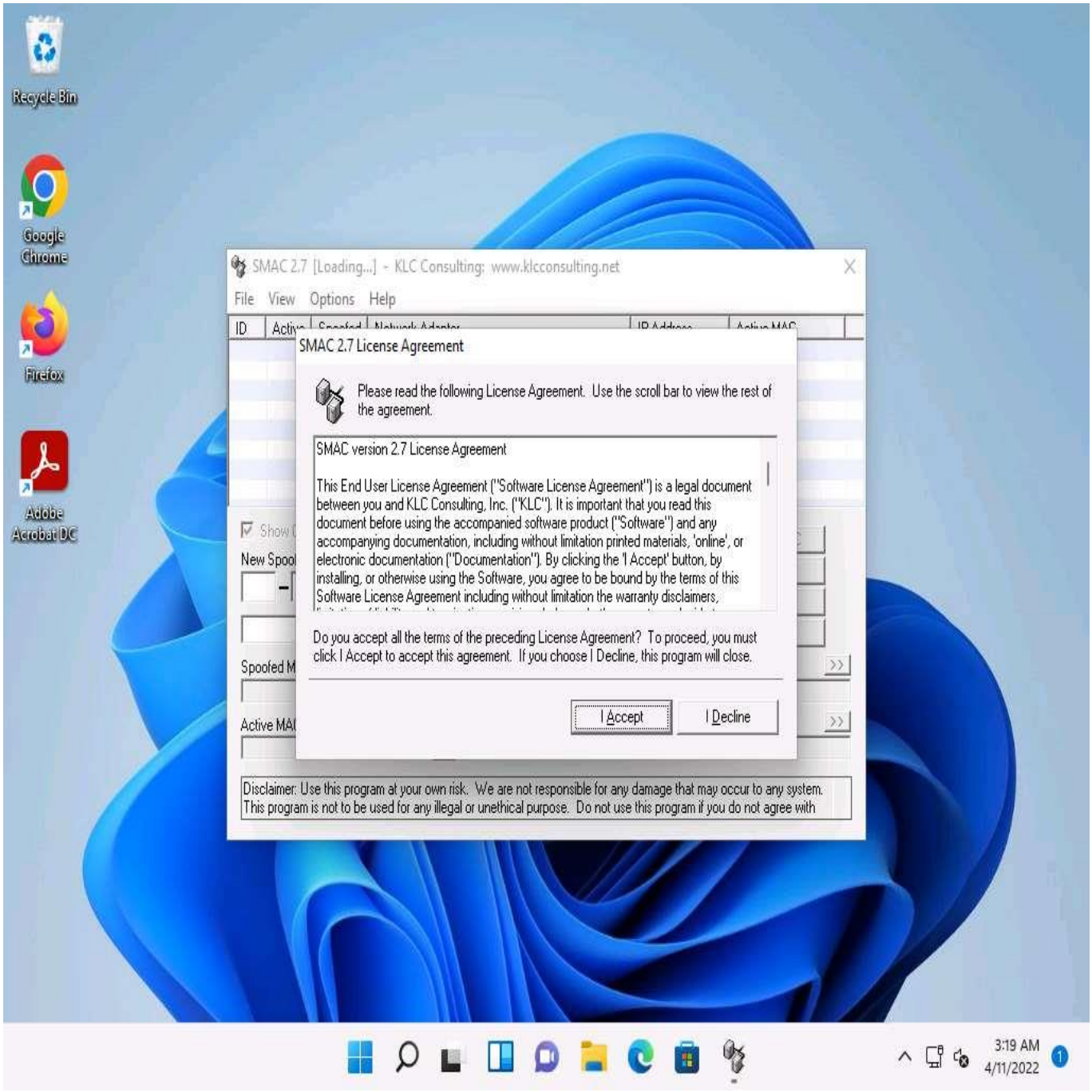


10. ☐ Close the **TMAC** main window.
11. ☐ Now, we shall perform MAC spoofing using the SMAC tool.
12. ☐ Click **Search** icon ( ) on the **Desktop**. Type **SMAC** in the search field, the **SMAC 2.7** appears in the results, click **Open** to launch it.

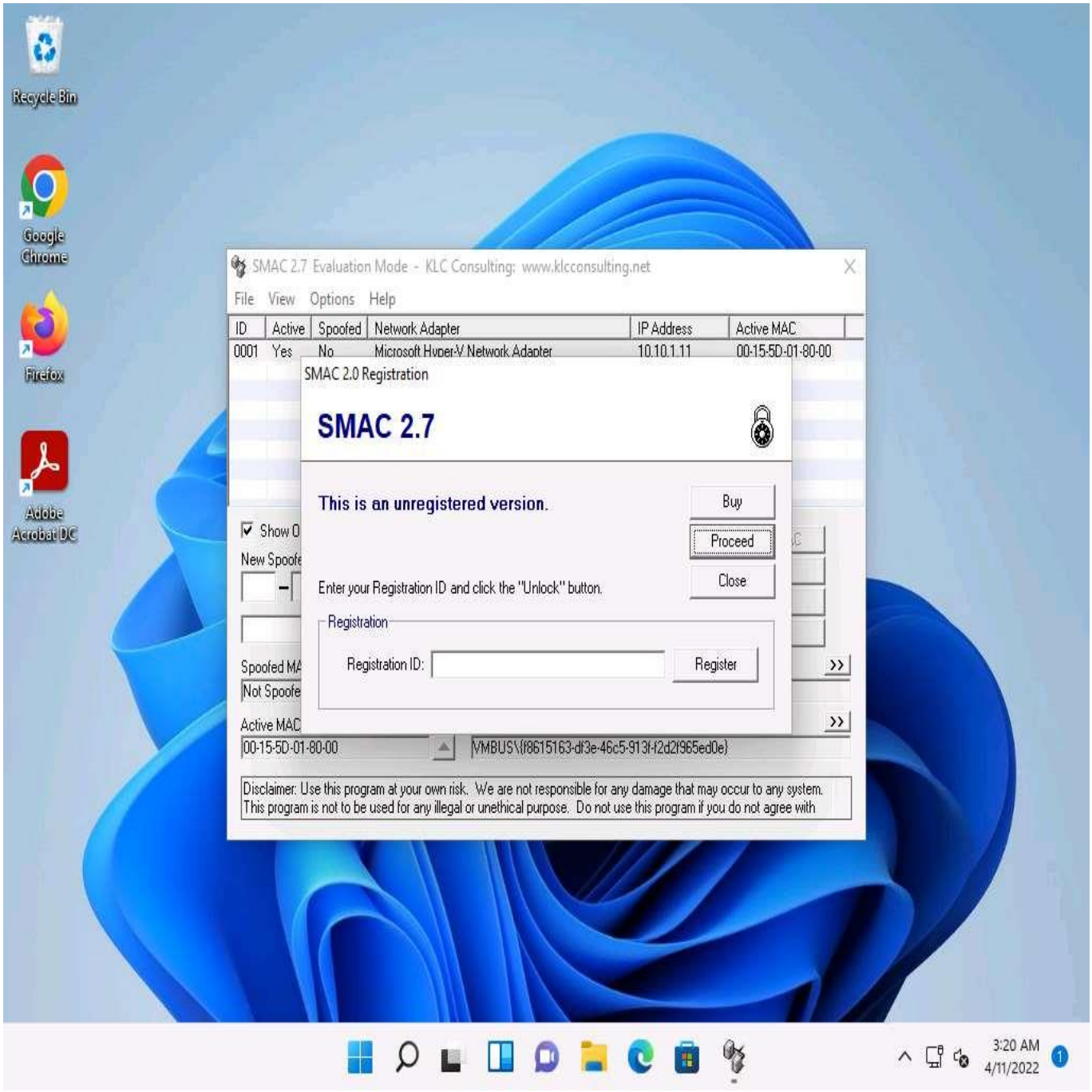
If a **User Account Control** pop-up appears, click **Yes**.



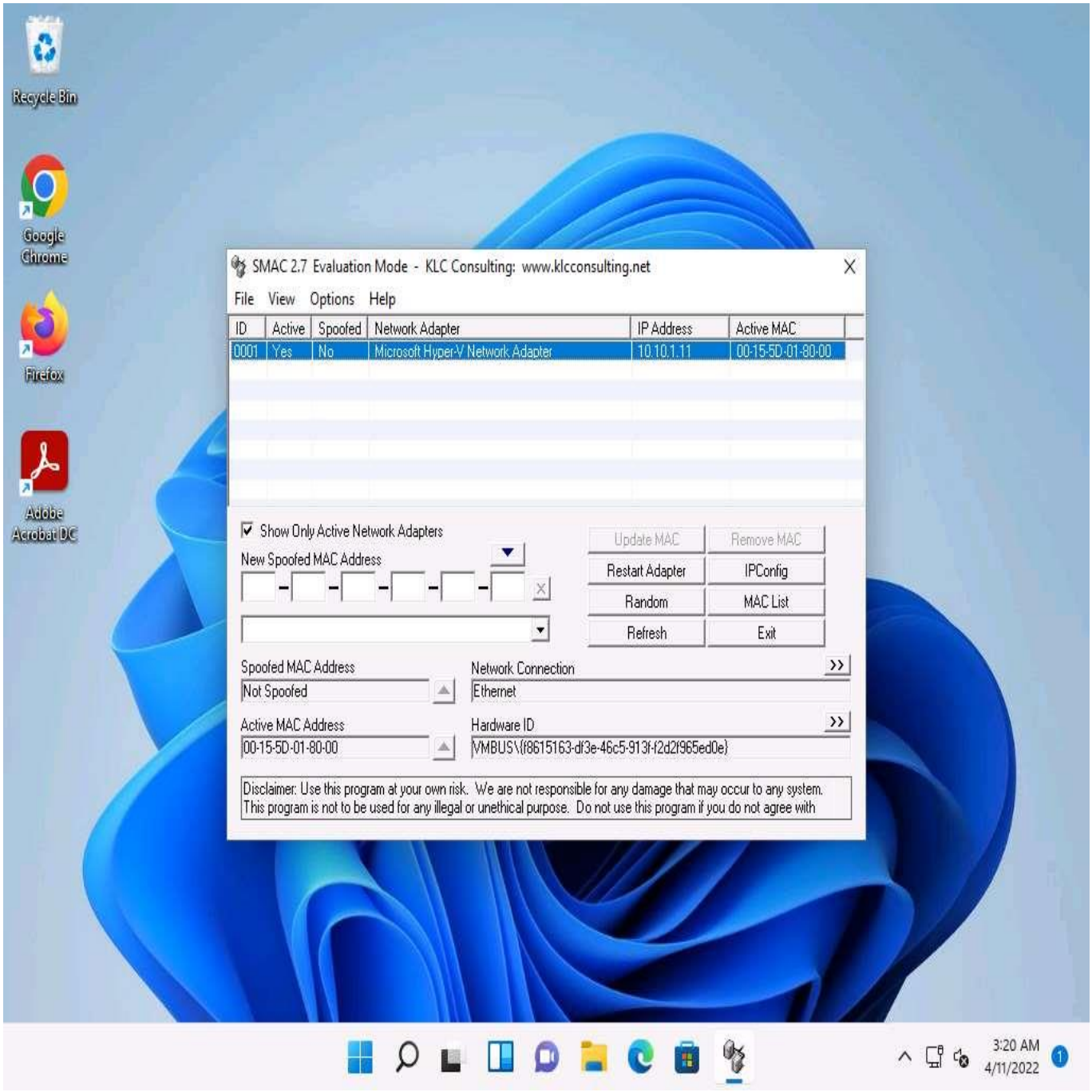
13. ☐ The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.



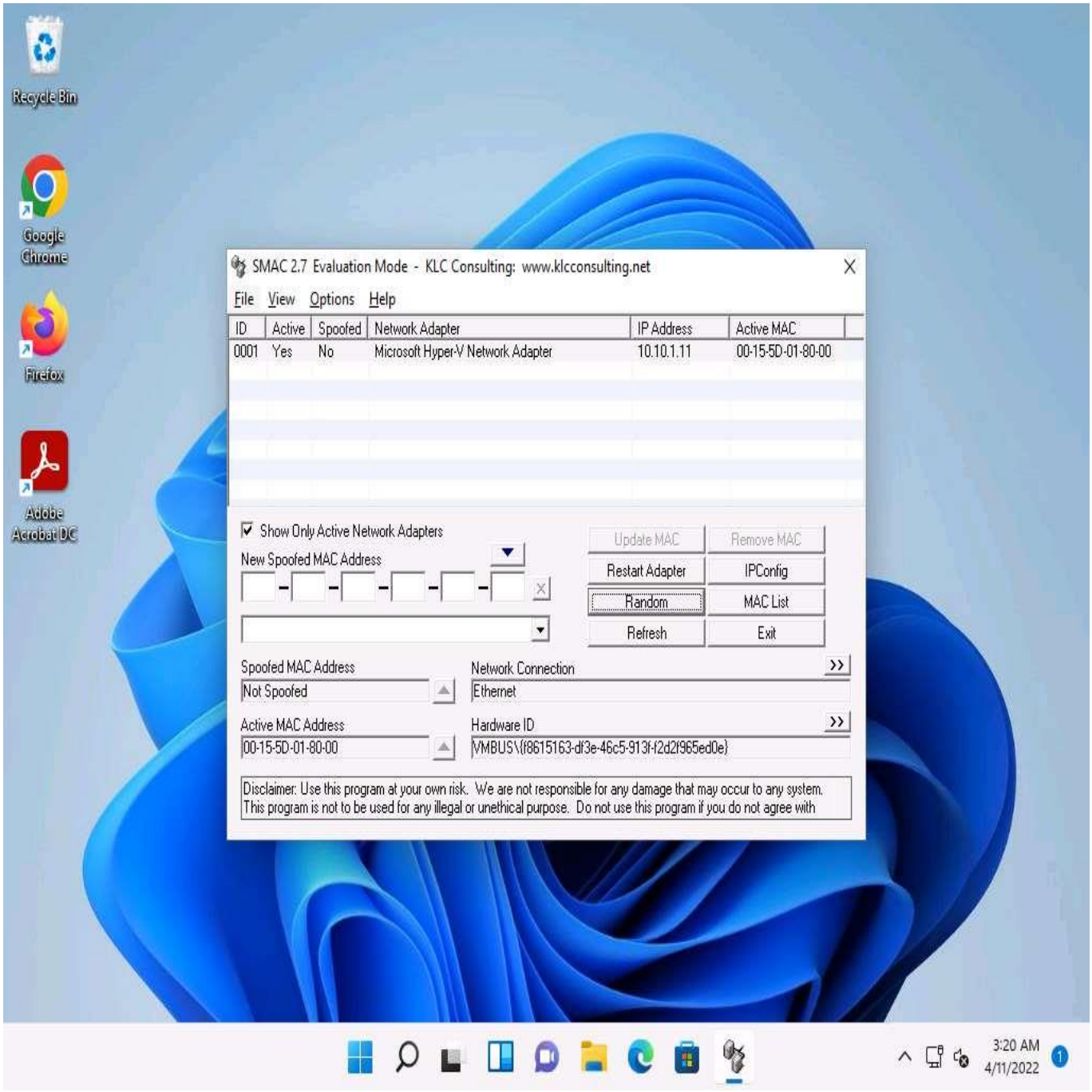
14. ☐ The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.



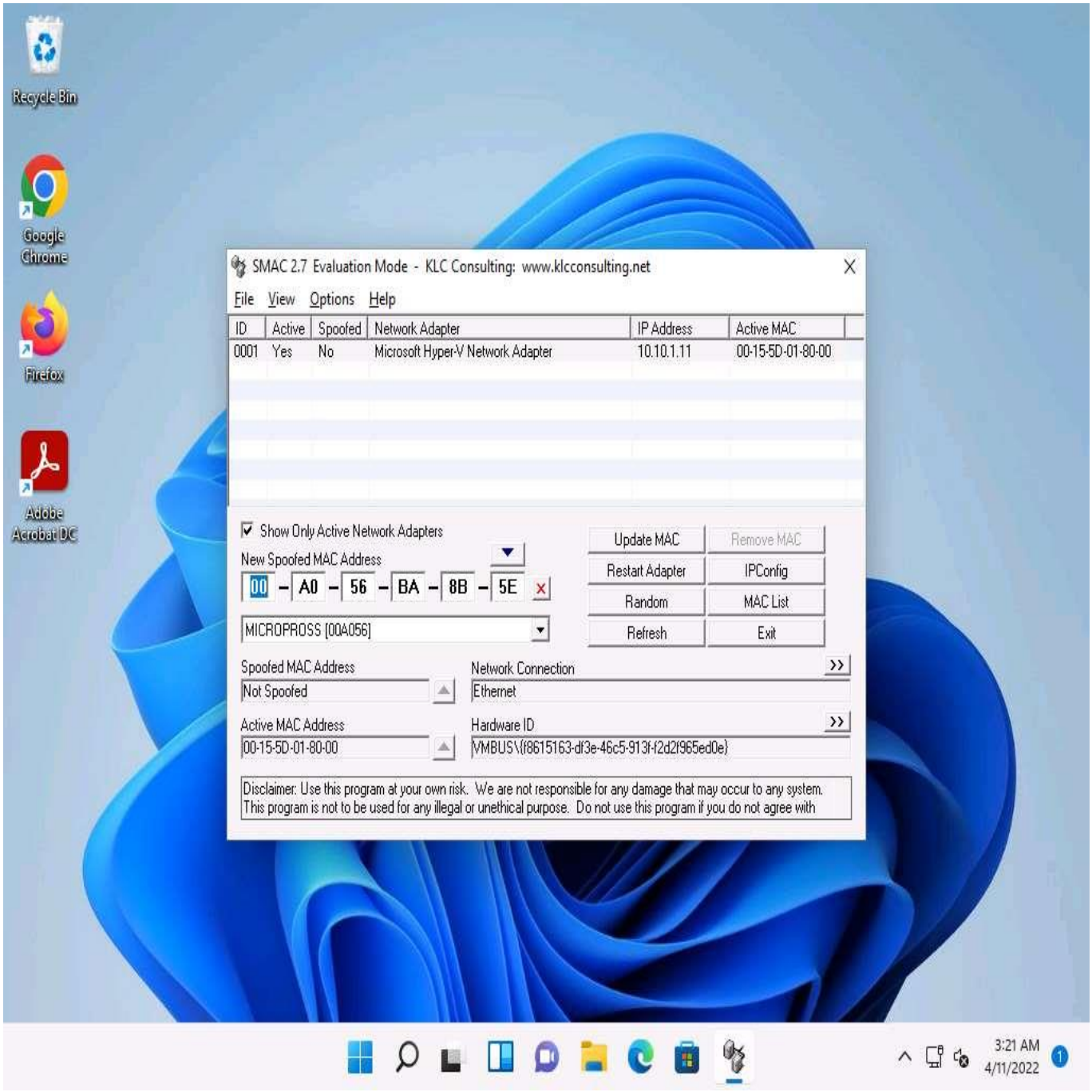
15. ☐ The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.



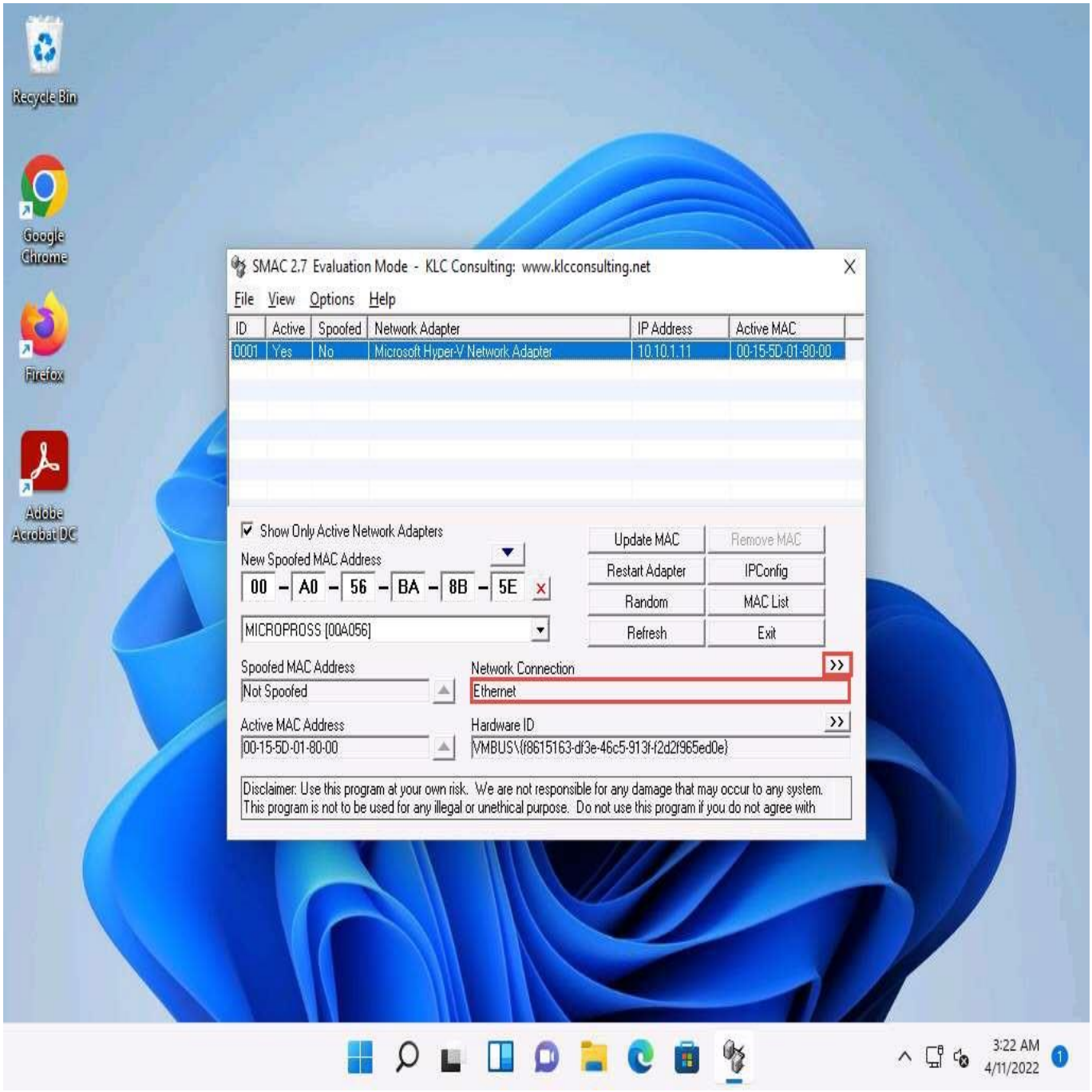
16. ☐ Click the **Random** button to generate a random MAC address.



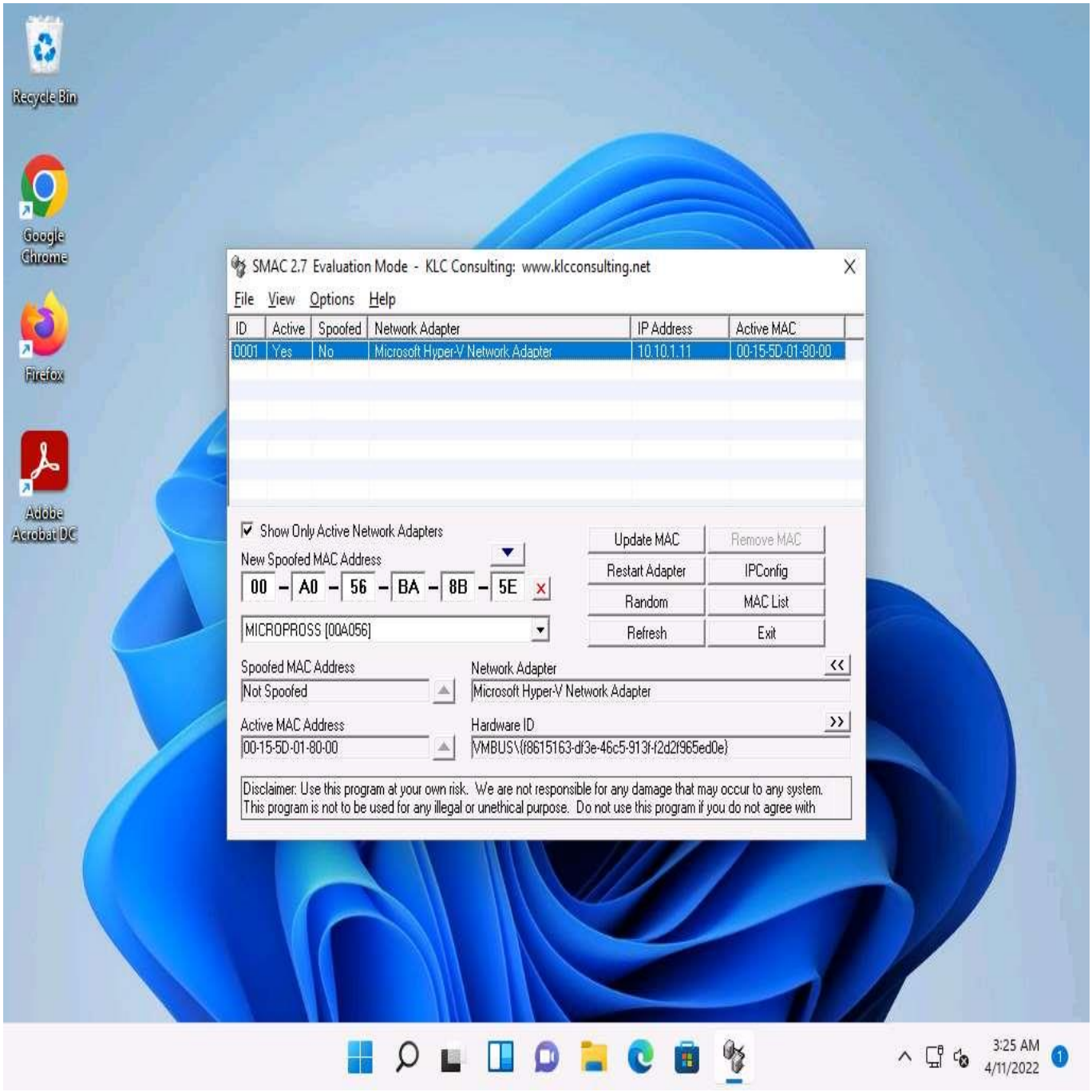
17. ☐ A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.



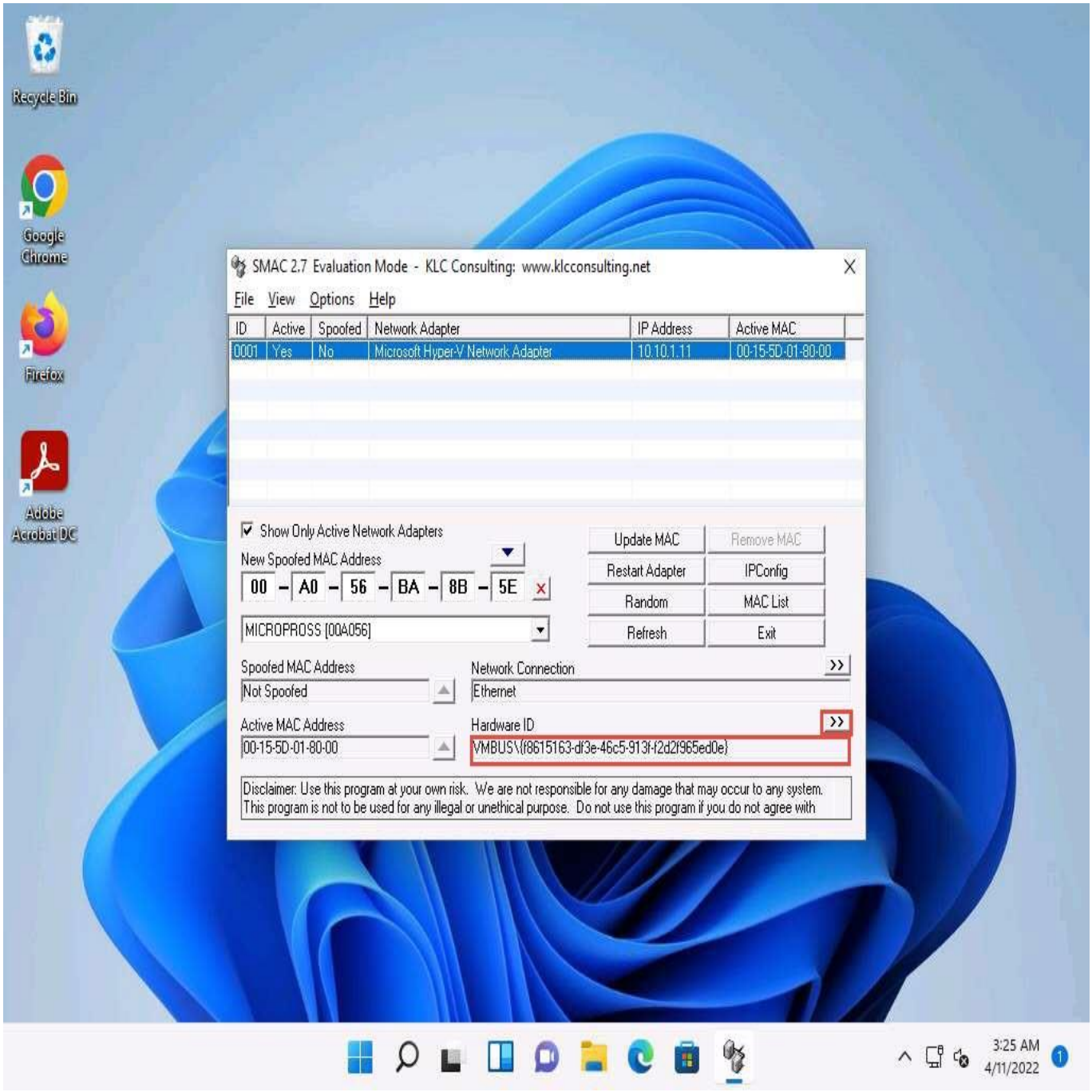
18. ☐ Click the forward arrow button (**>>**) under **Network Connection** to view the **Network Adapter** information.



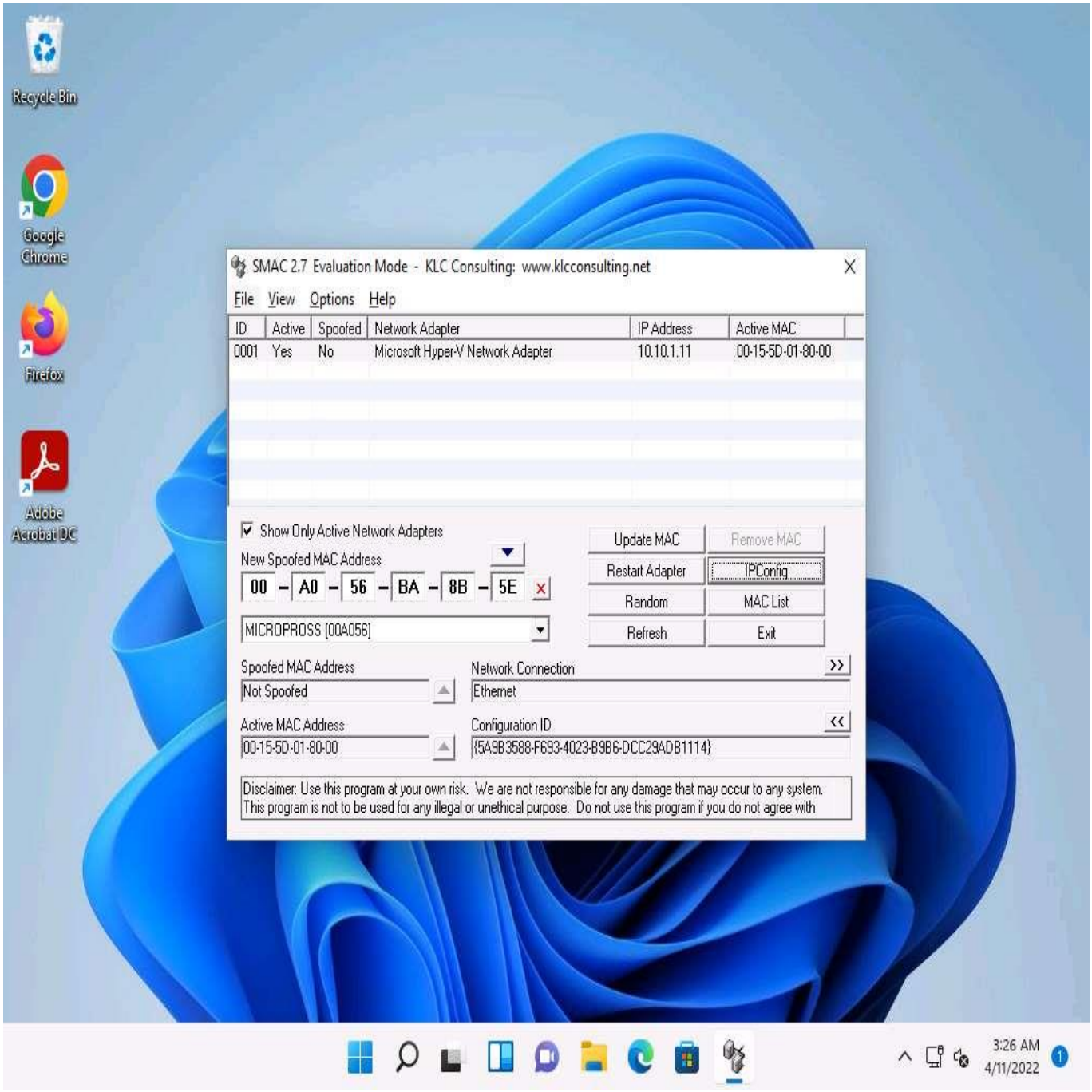
19. ☐ Clicking the back arrow (**<<**) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.



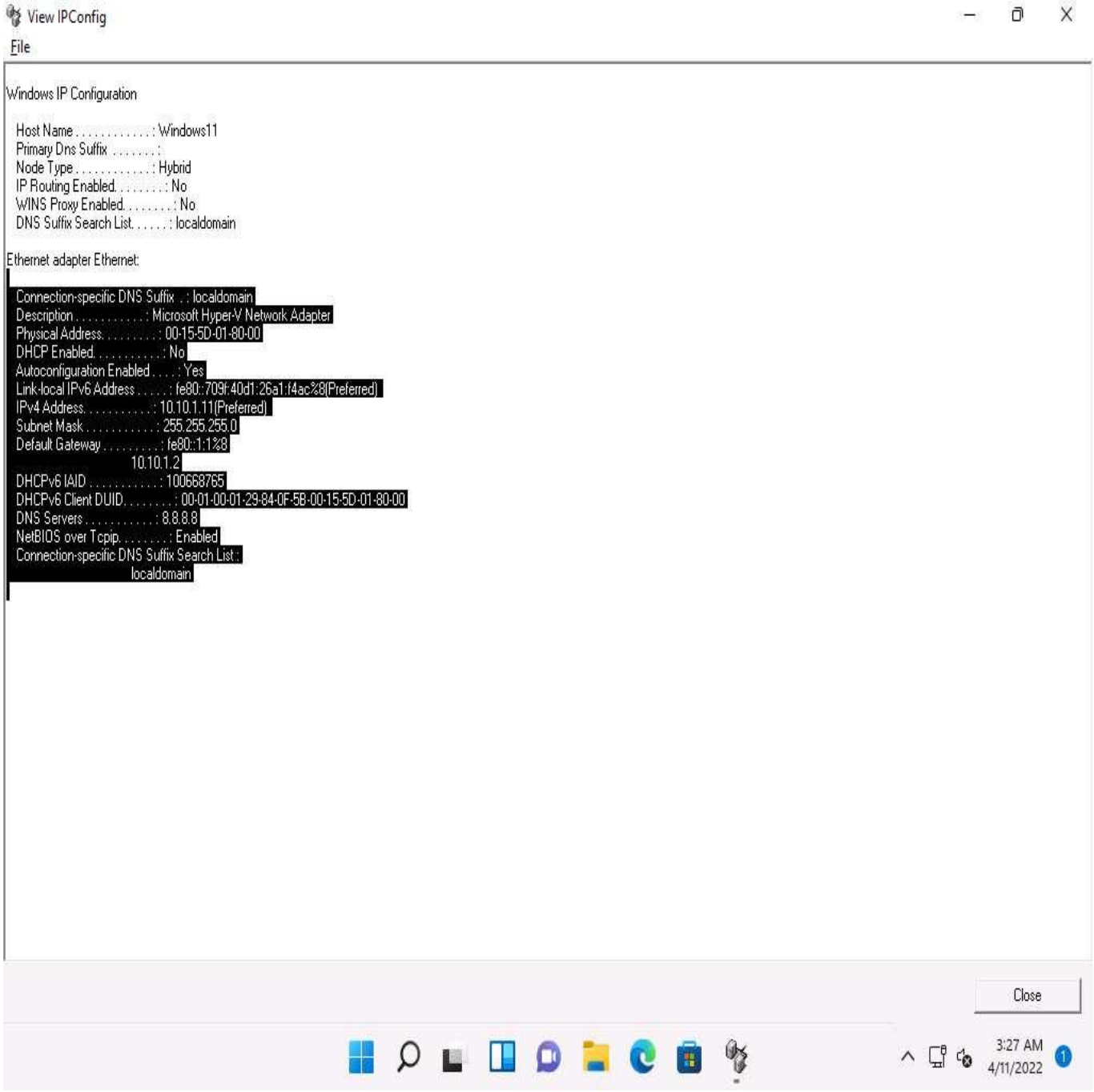
20. ☐ Similarly, you can click the forward arrow button (**>>**) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (**<<**) to toggle back to **Hardware ID** information.



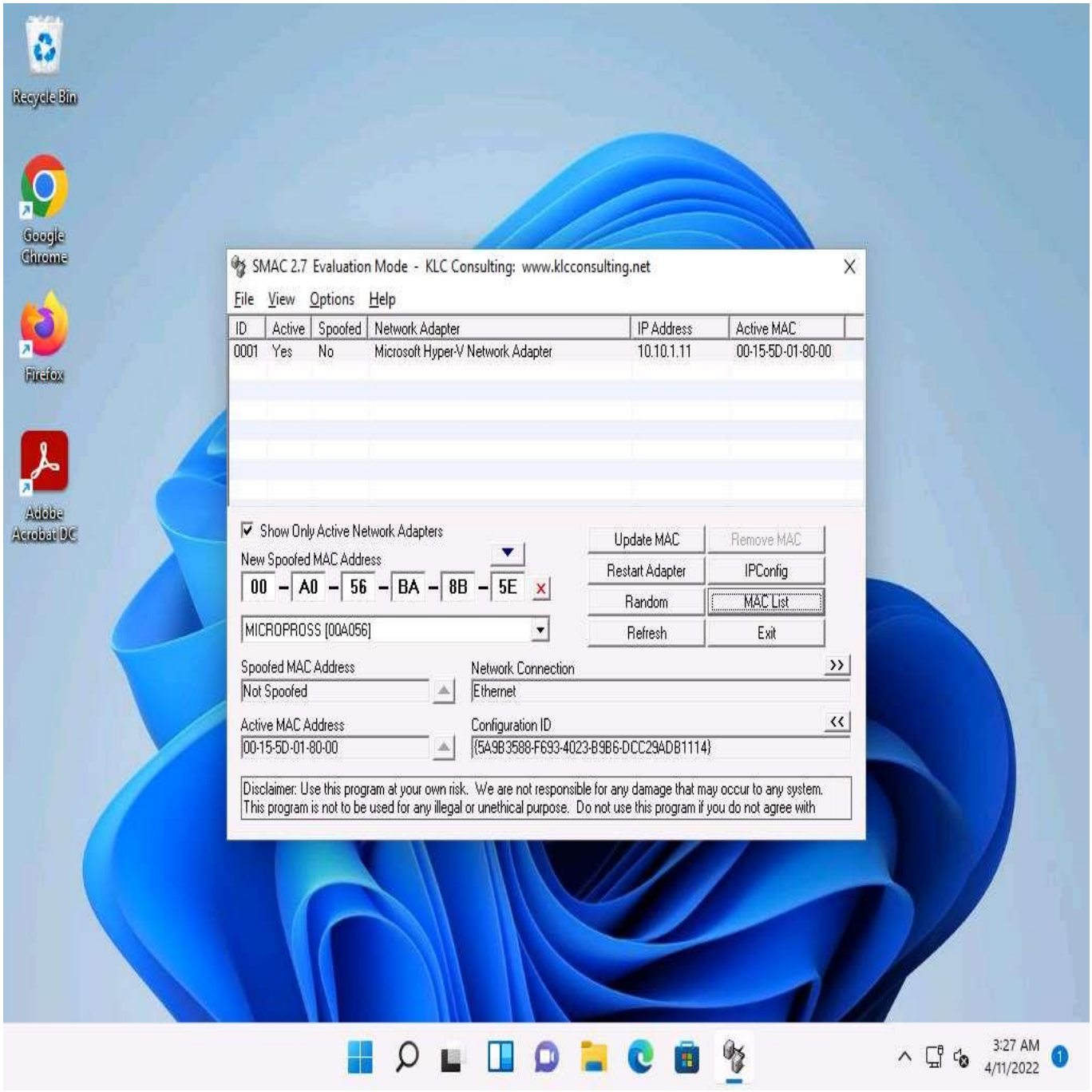
21. ☐ Click the **IPConfig** button to view the ipconfig information.



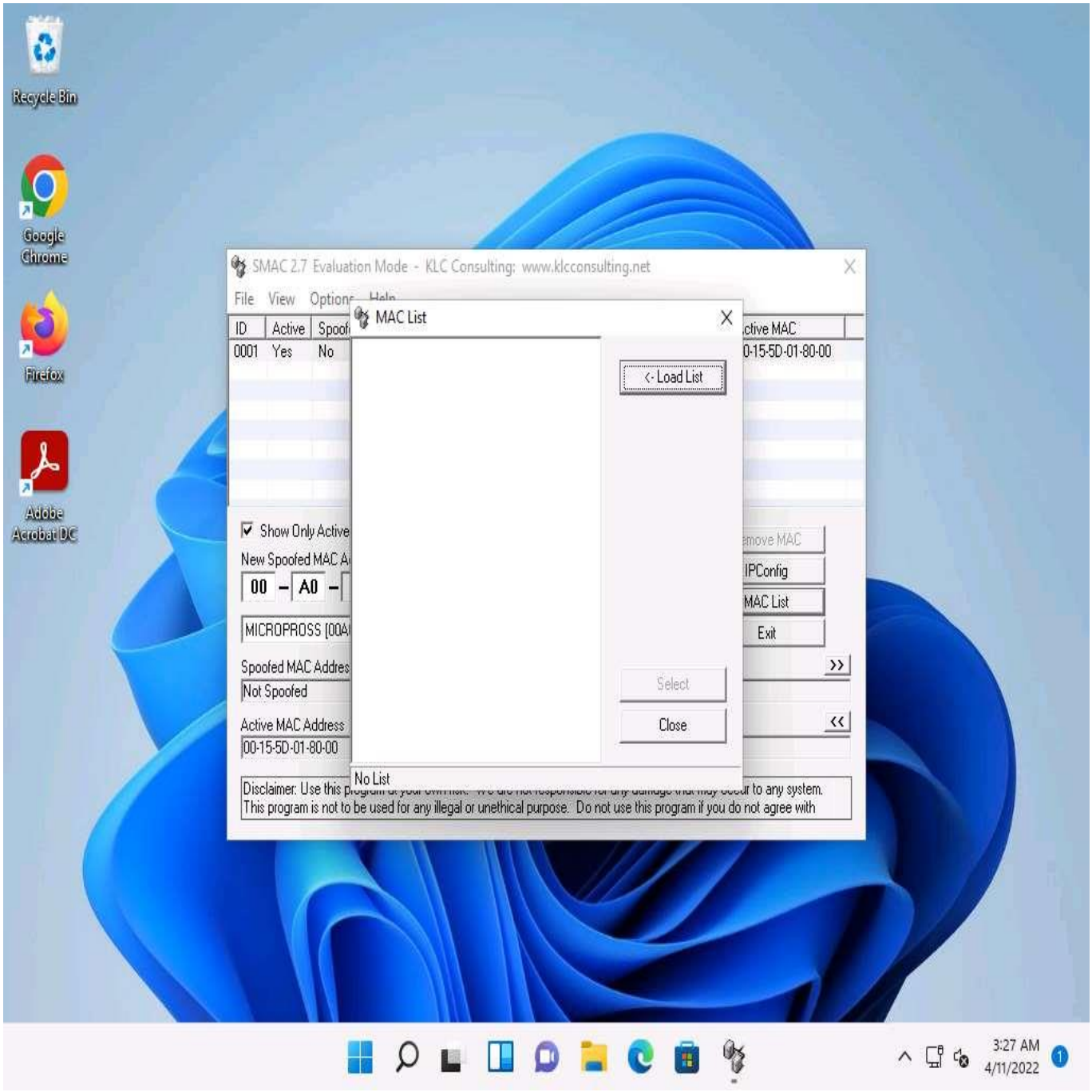
22. ☐ The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.



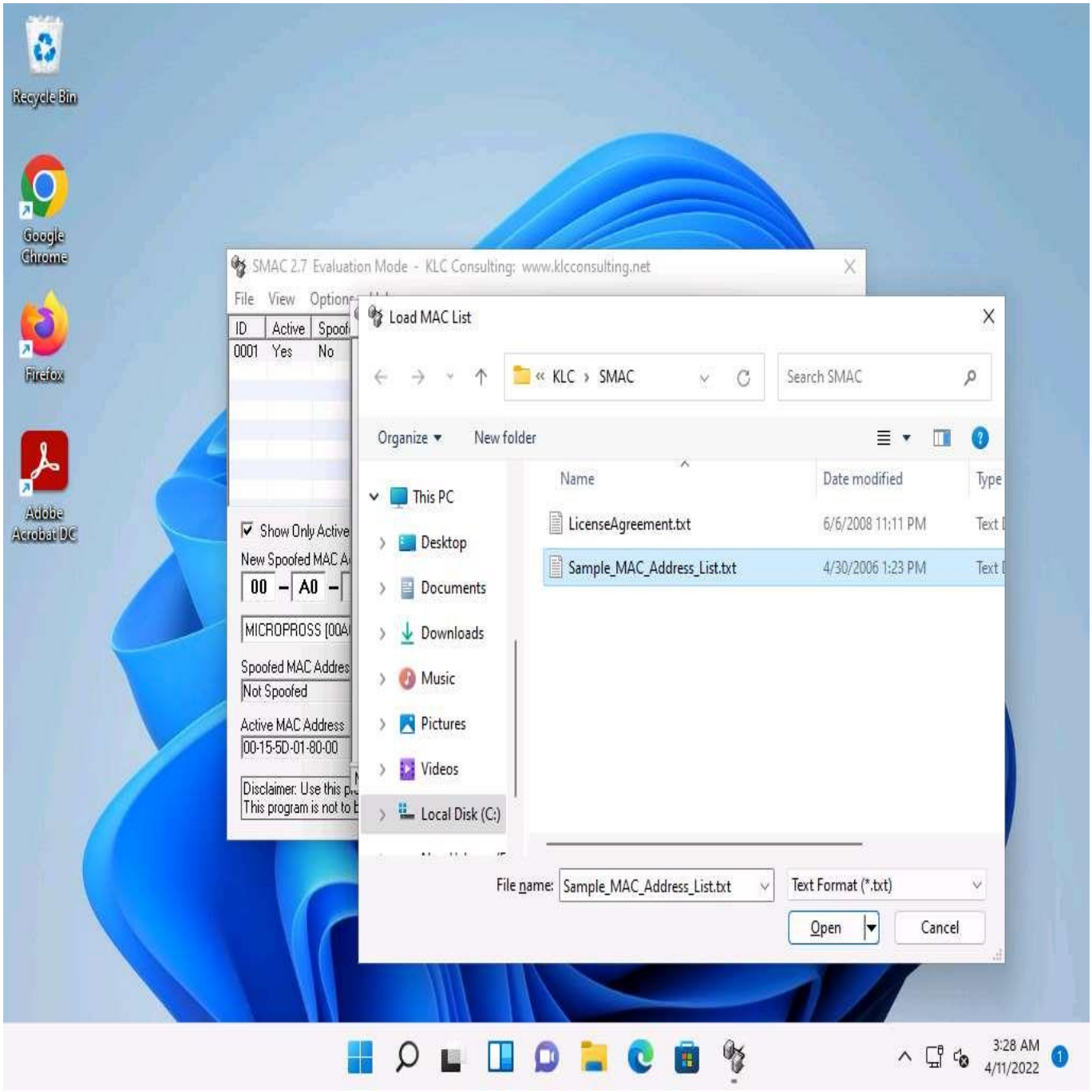
23. ☐ Click the **MAC List** button to import the MAC address list into SMAC.



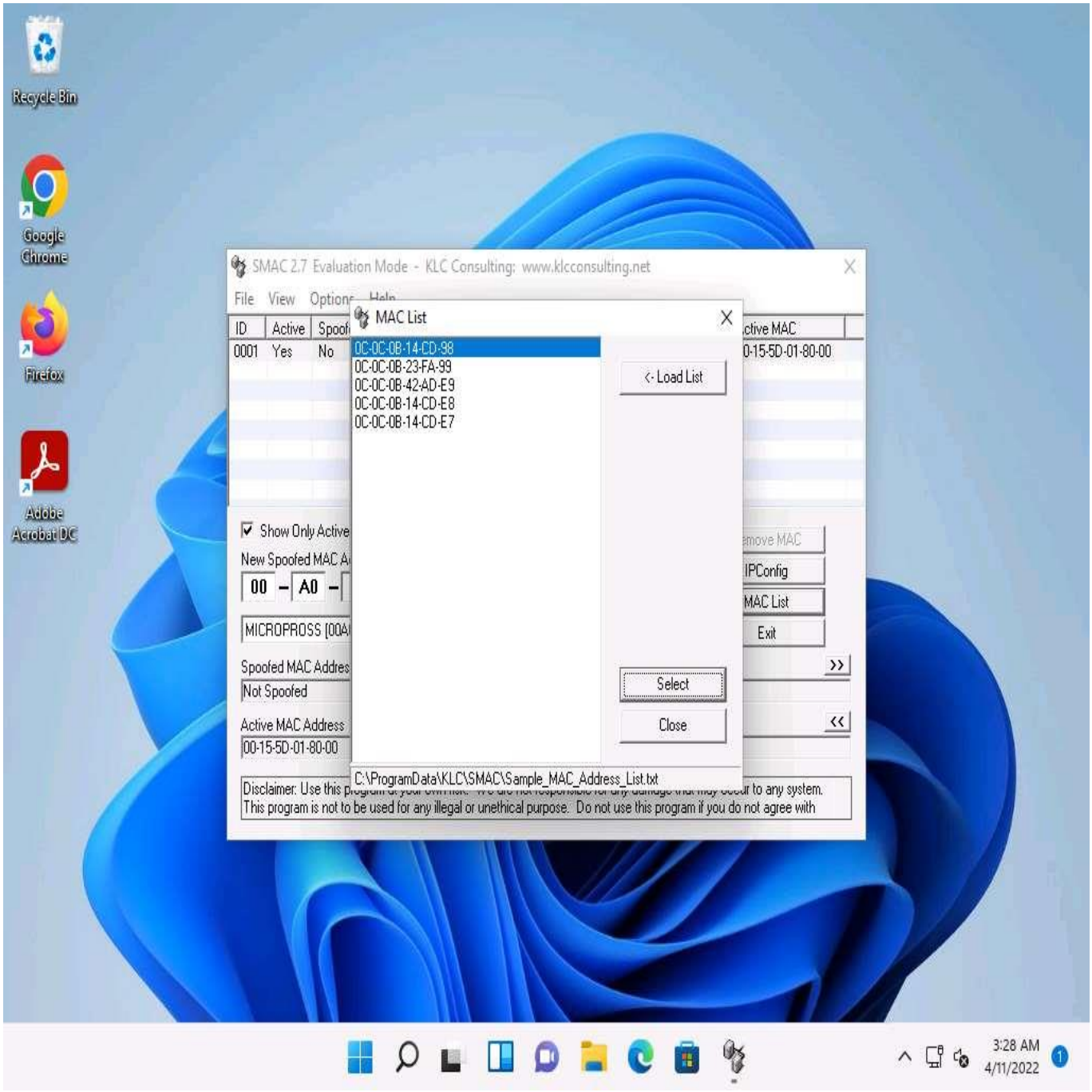
24. ☐ The **MAC List** window appears; click the **Load List** button.



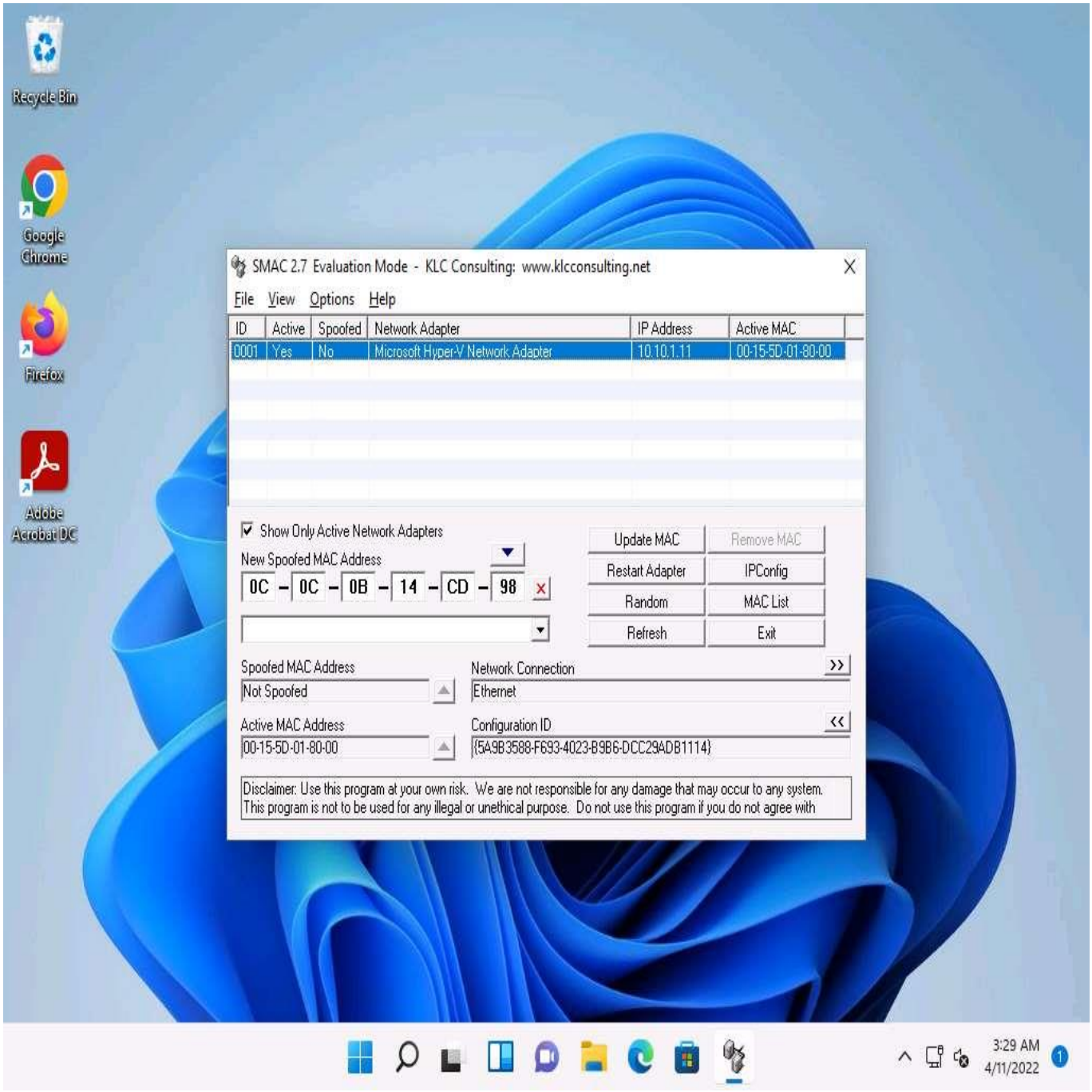
25. ☐ The **Load MAC List** window appears; select the **Sample_MAC_Address_List.txt** file and click **Open**.



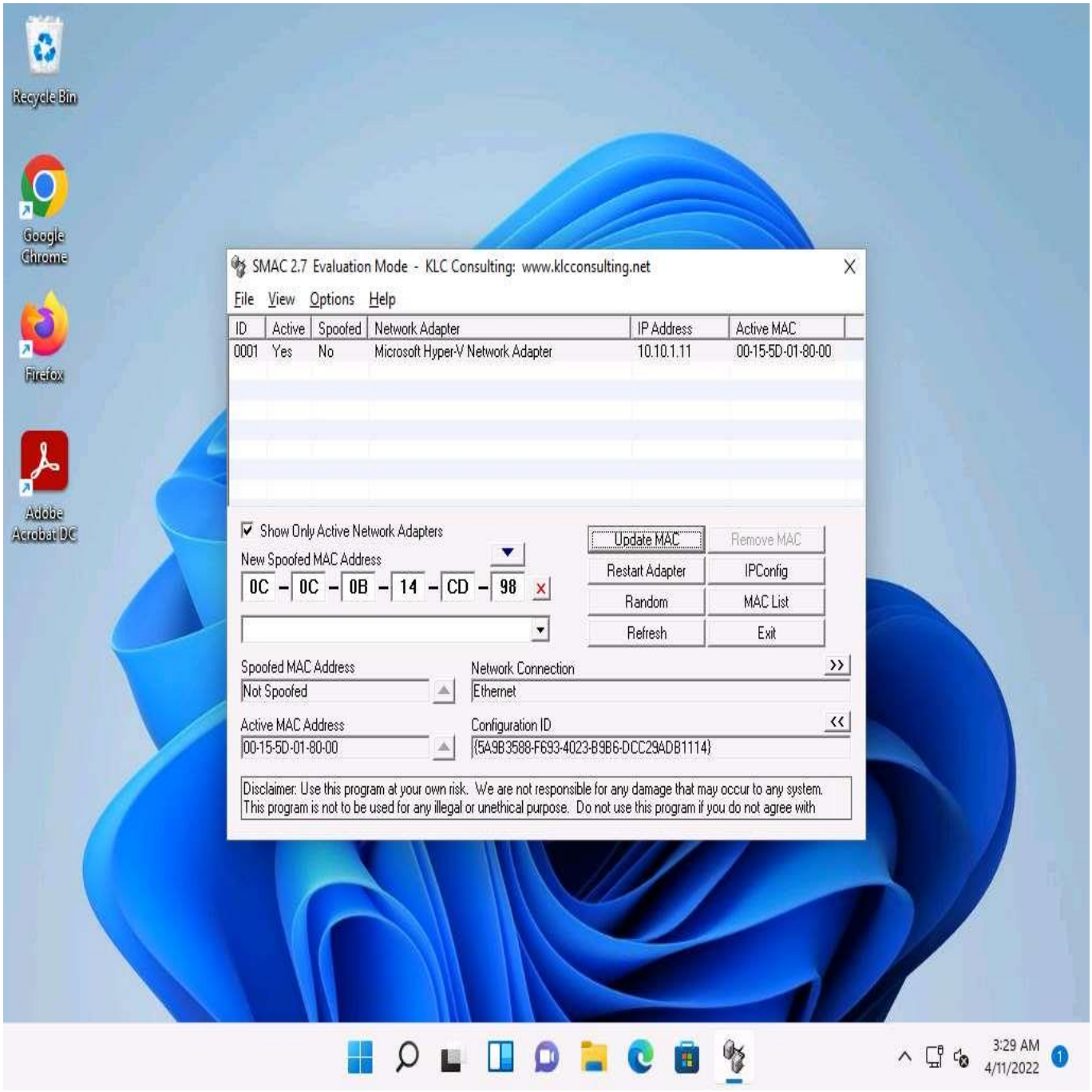
26. ☐ A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.



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



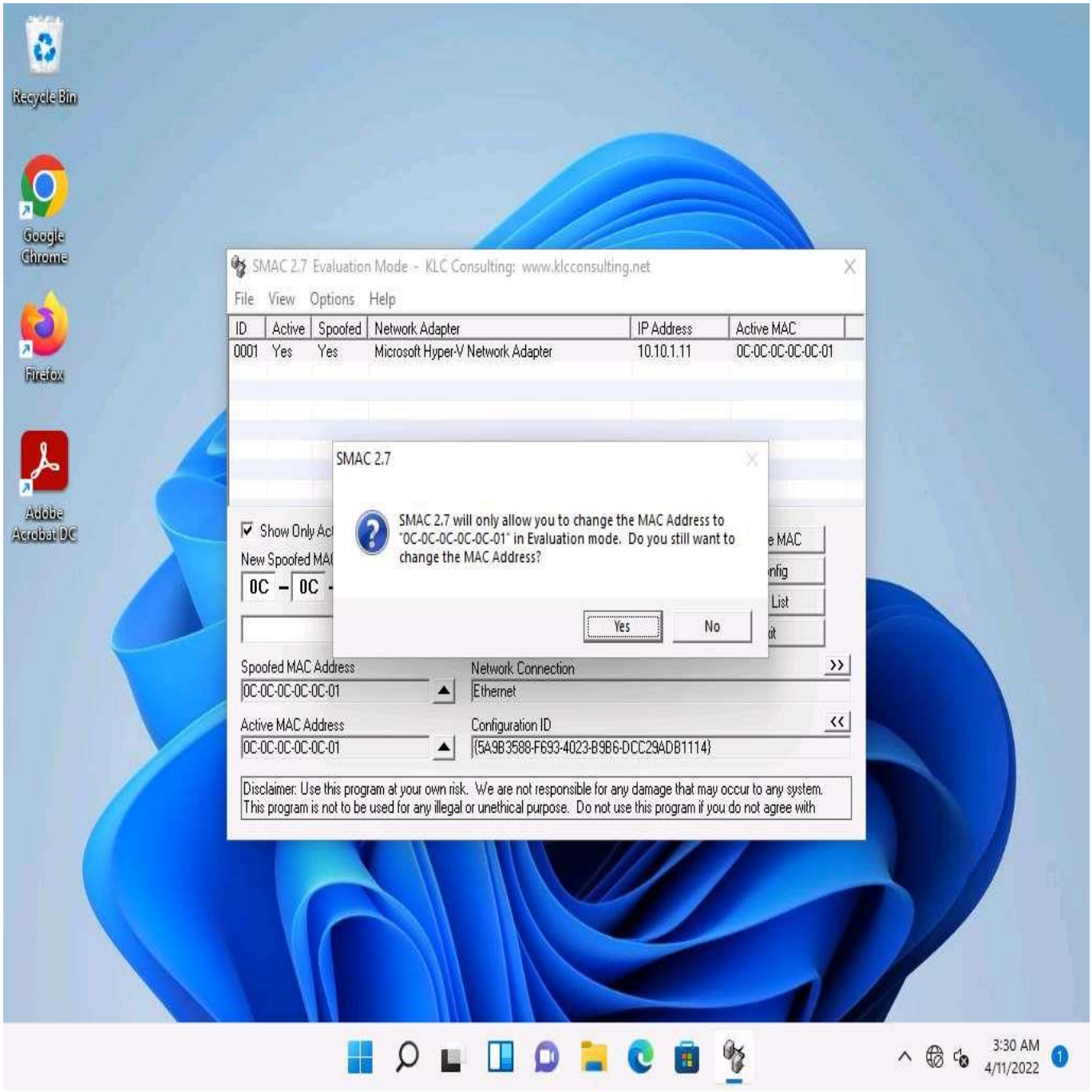
28. ☐ Click the **Update MAC** button to update the machine's MAC address information.



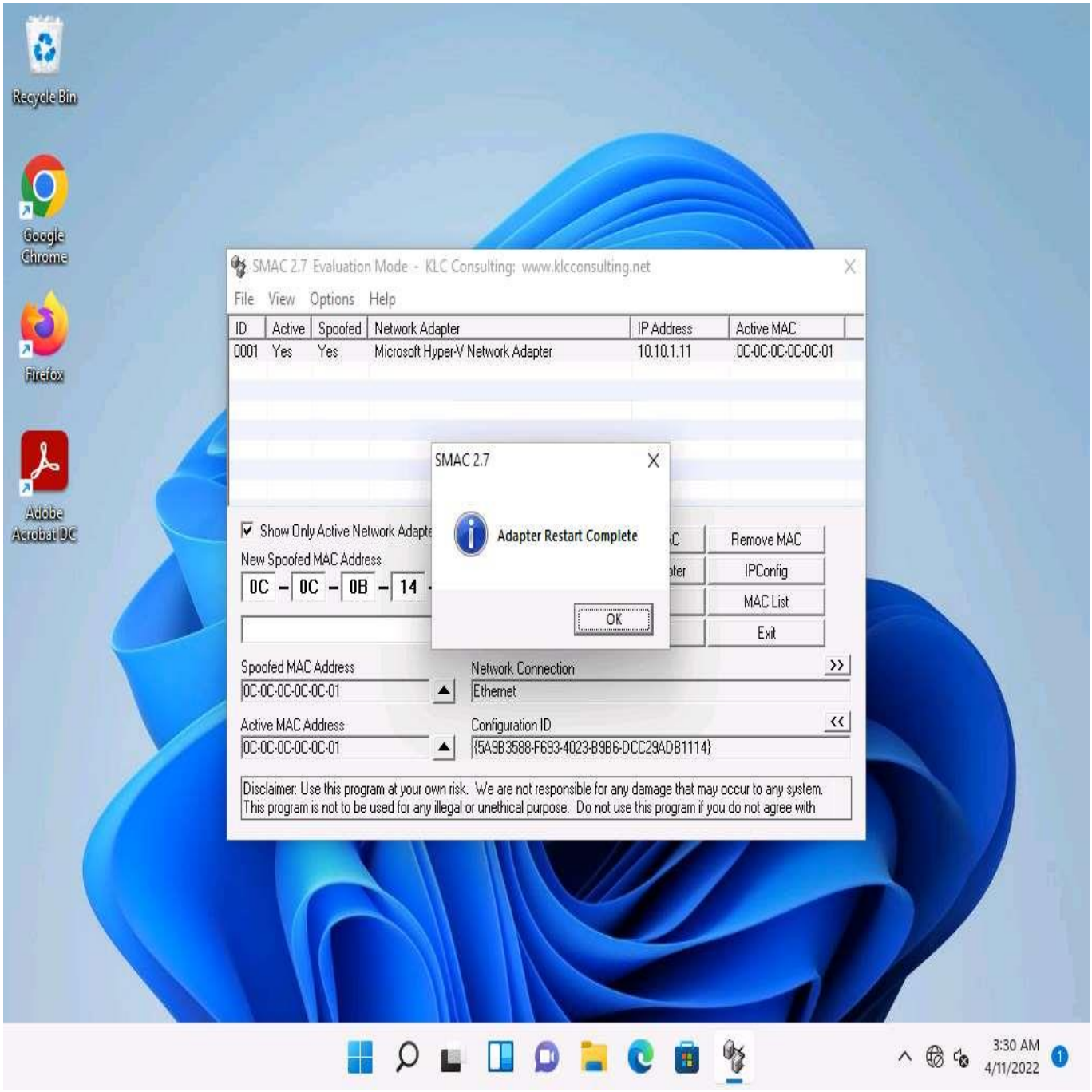
29. ☐ The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

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

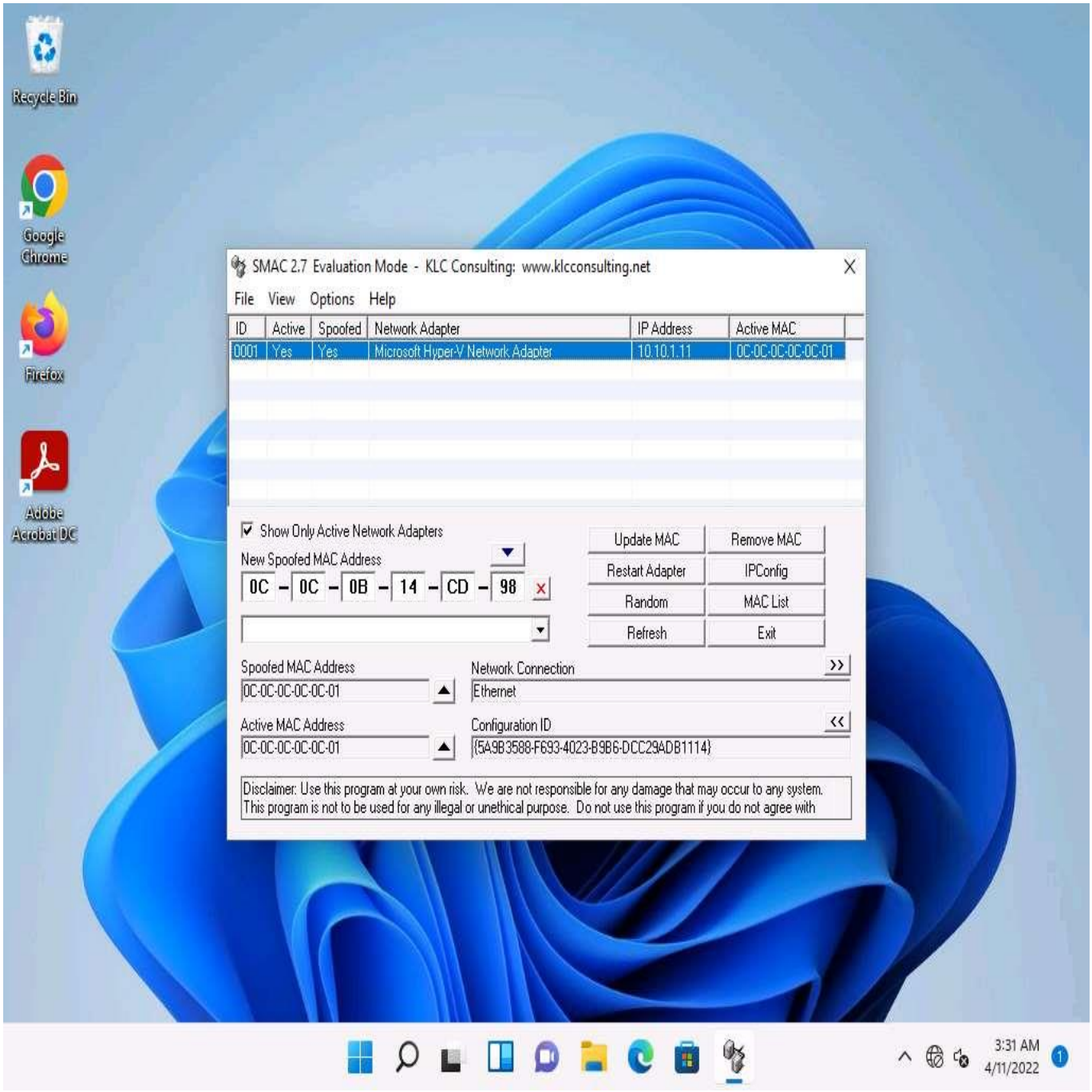
In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.



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**.



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

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

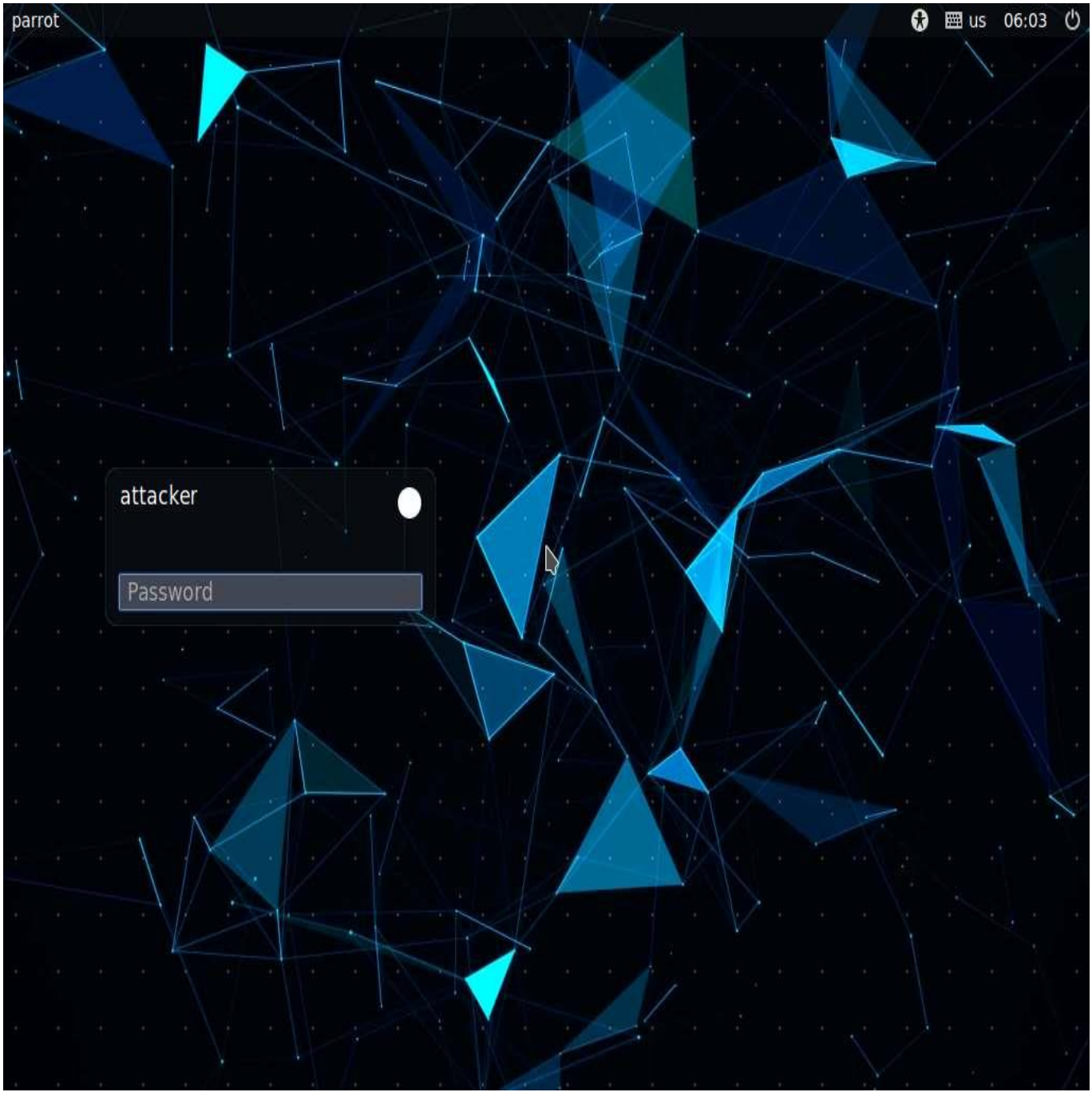
Task 6: Spoof a MAC Address of Linux Machine using macchanger

A MAC address is a unique number that can be assigned to every network interface, and it is used by various systems programs and protocols to identify a network interface. It is not possible to change MAC address that is hard-coded on the NIC (Network interface controoller). However many drivers allow the MAC address to be changed. Some tools can make the operating system believe that the NIC has the MAC address of user's choice.

Masking of the MAC address is known as MAC spoofing and involves changing the computer's identity. MAC spoofing can be performed using numerous tools.

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

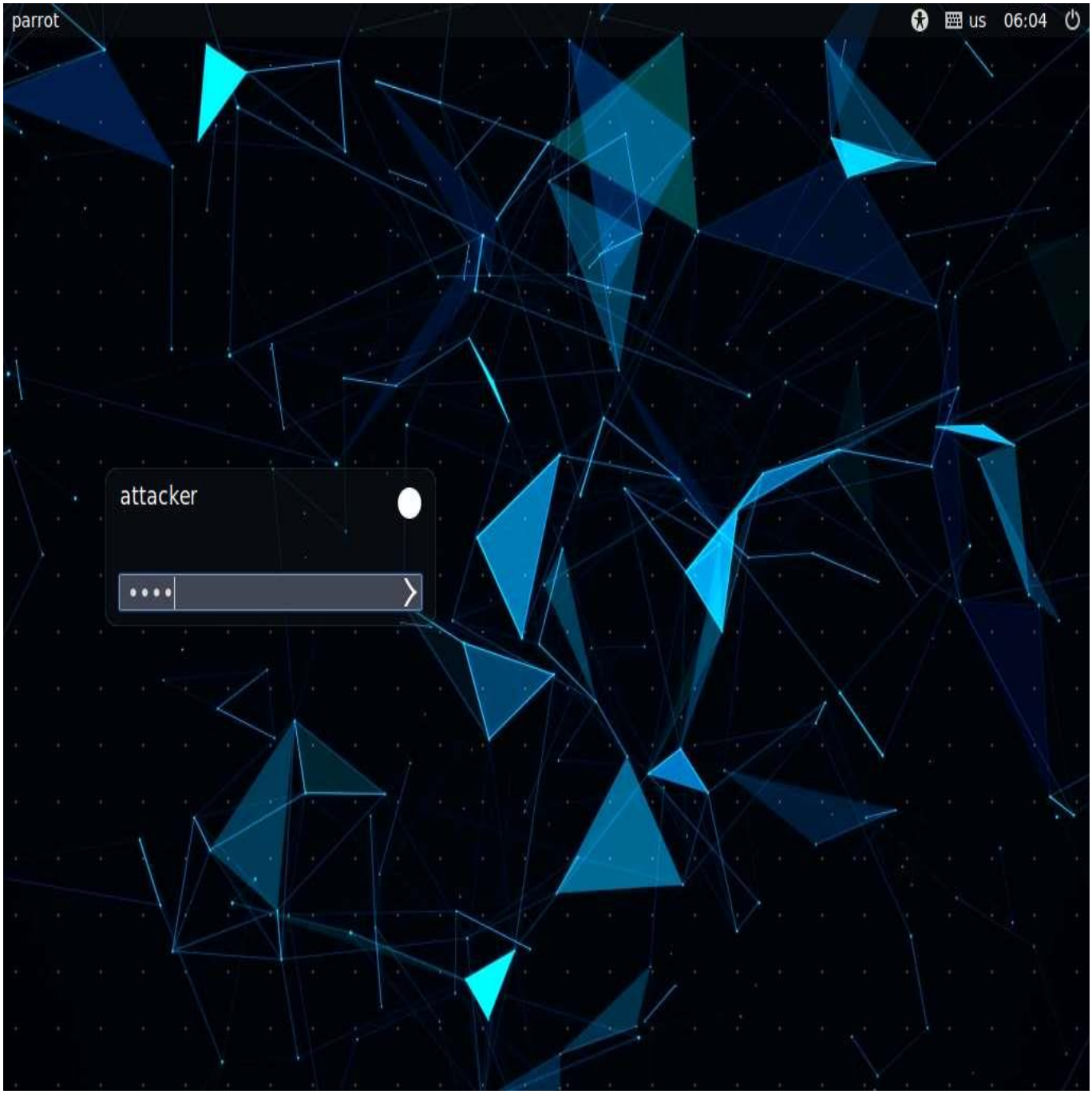
1. Click Parrot Security to switch to the **Parrot Security** machine.



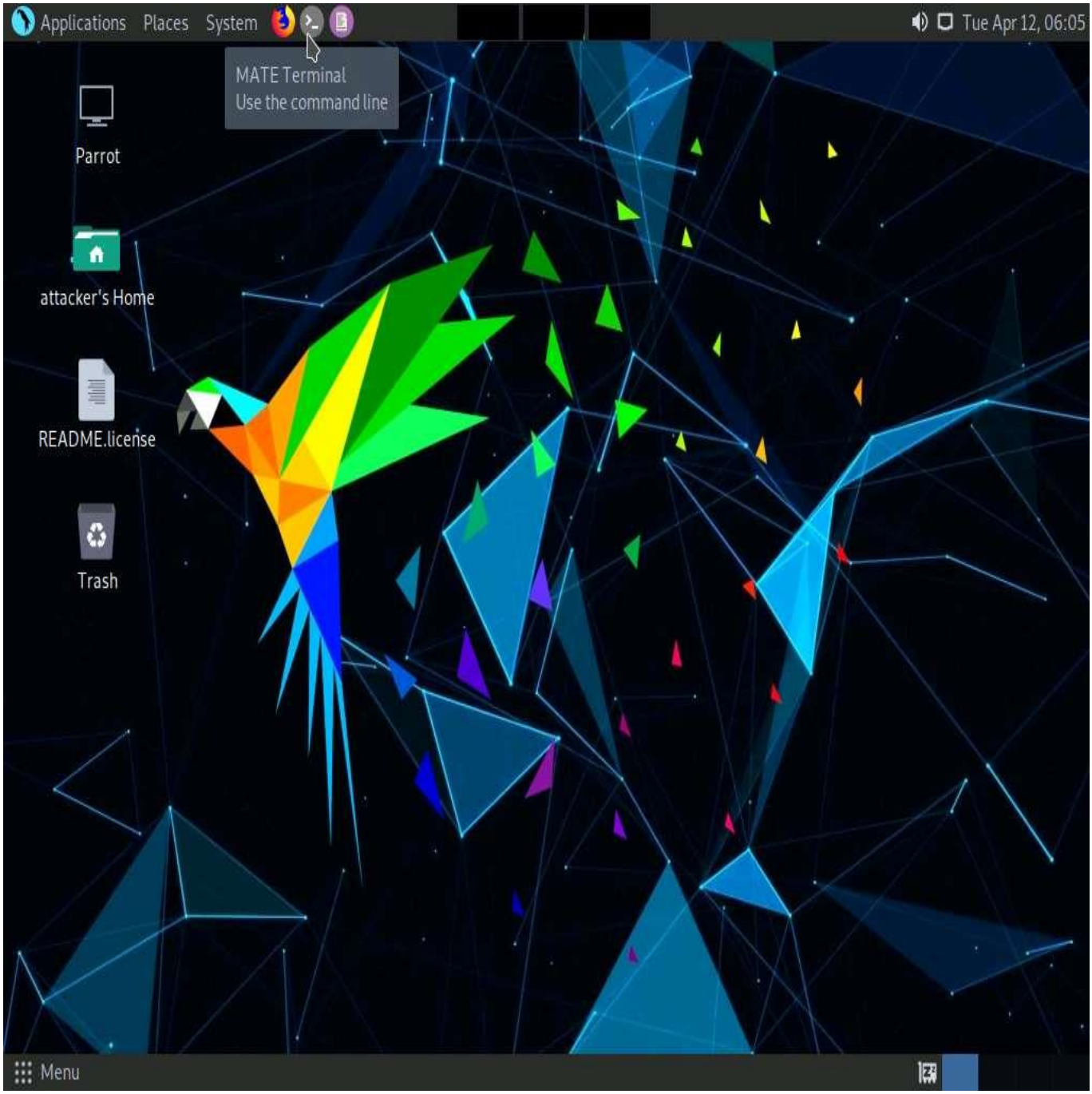
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

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



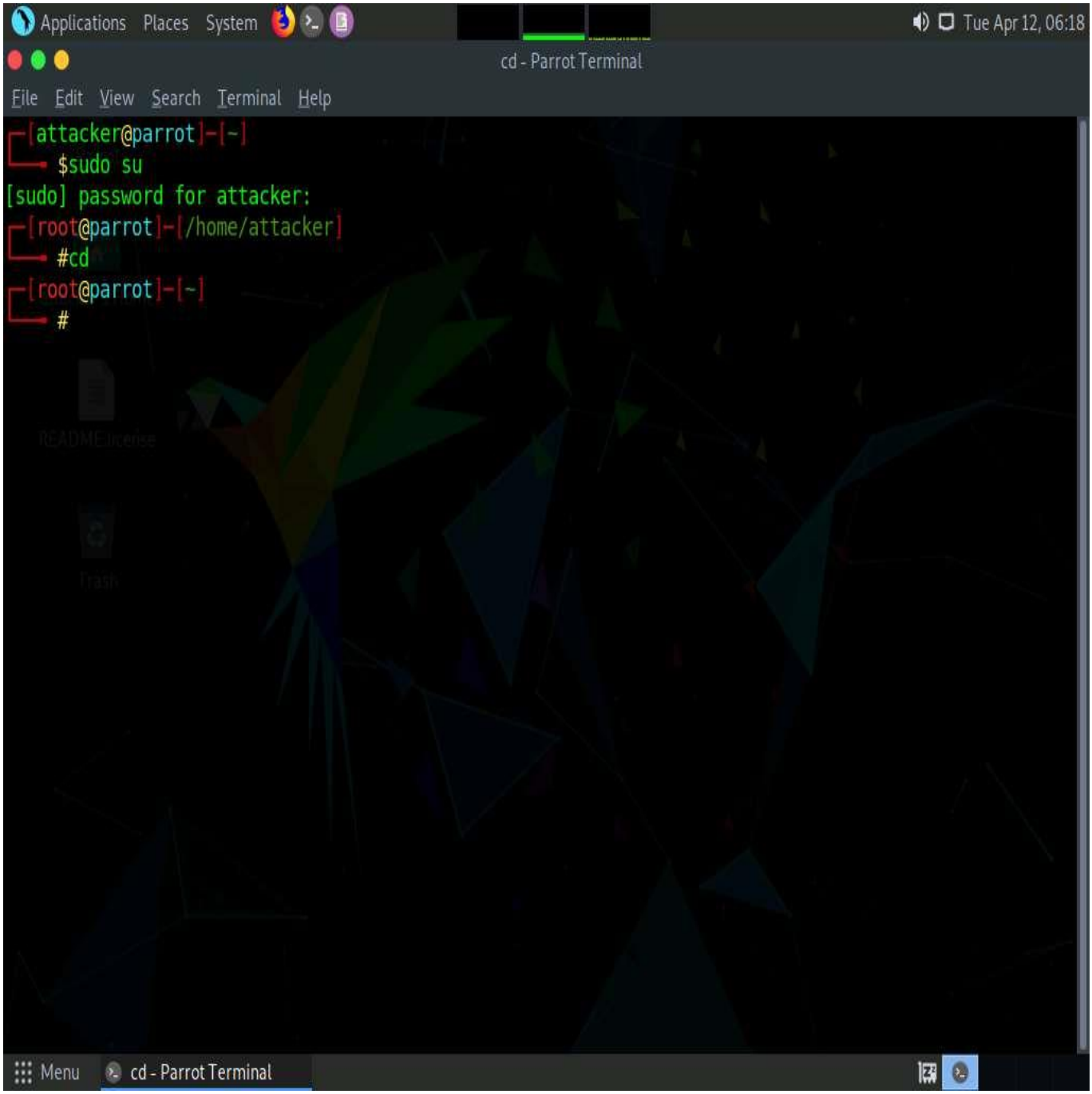
3. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



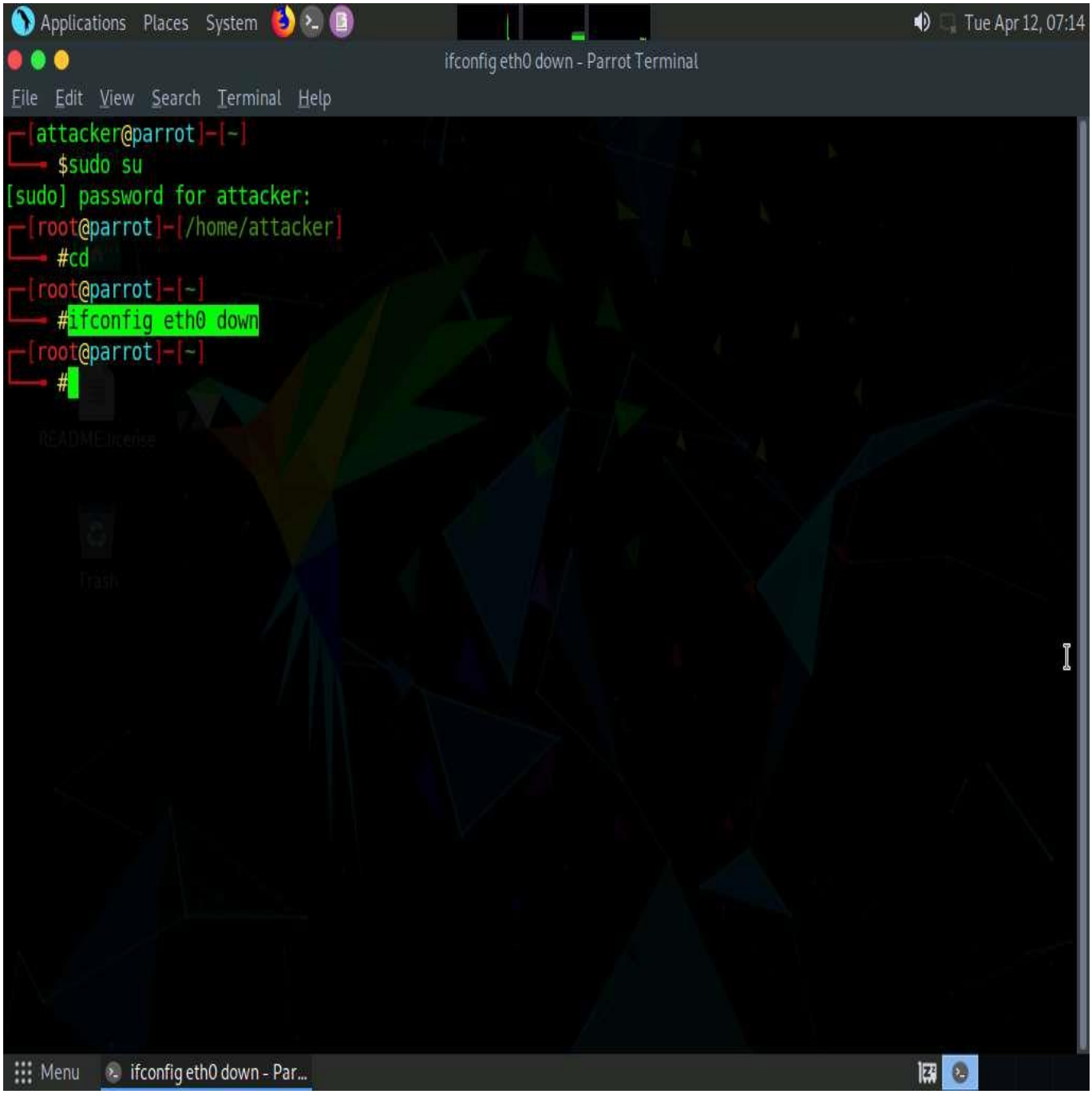
4. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. ☐ In the [sudo] password for attacker field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

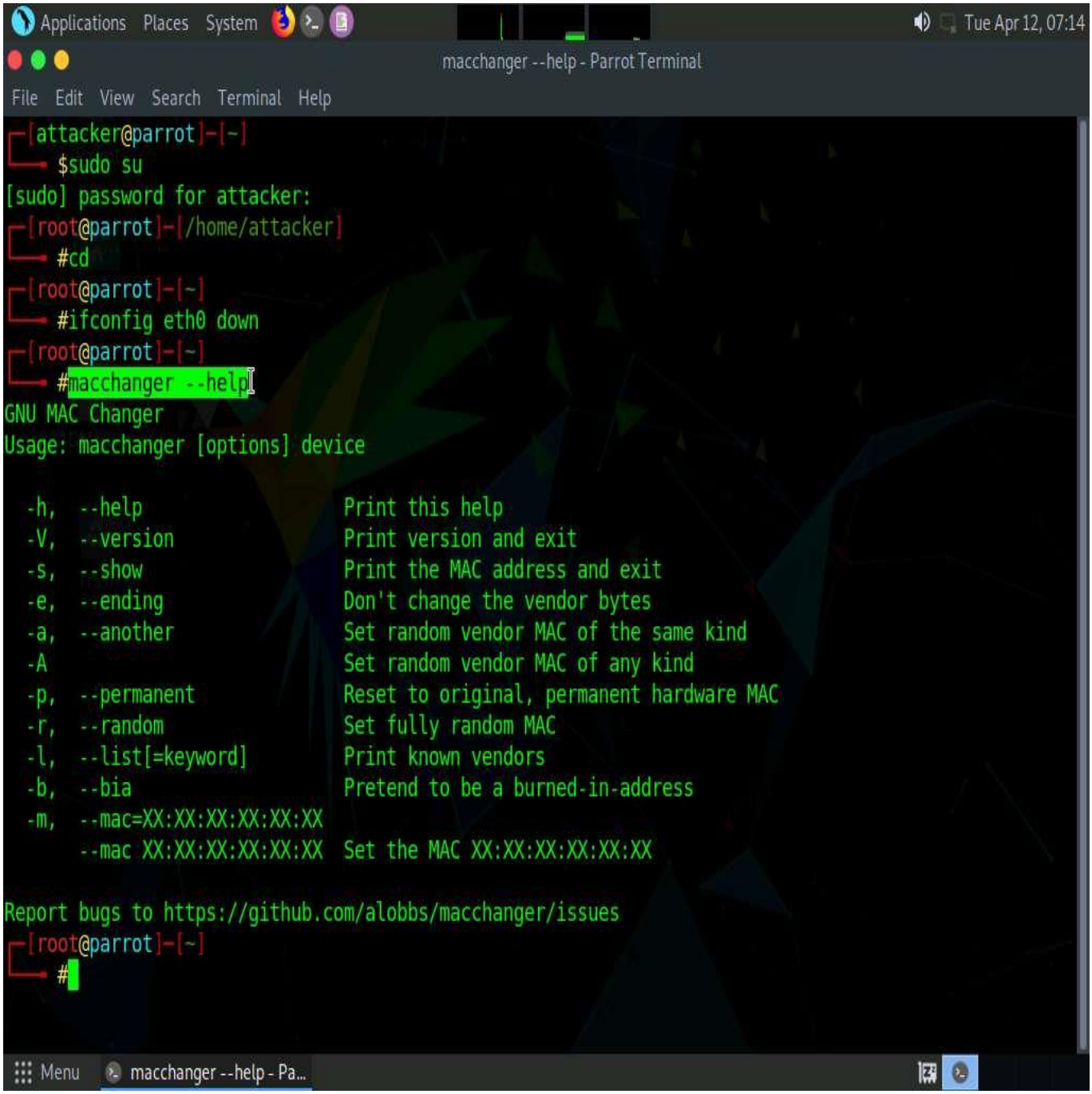
6. ☐ Now, type **cd** and press **Enter** to jump to the root directory.



7. ☐ Before changing the MAC address we need to turn off the network interface.
8. ☐ Type **ifconfig eth0 down** and press **Enter**, to turn off the network interface.

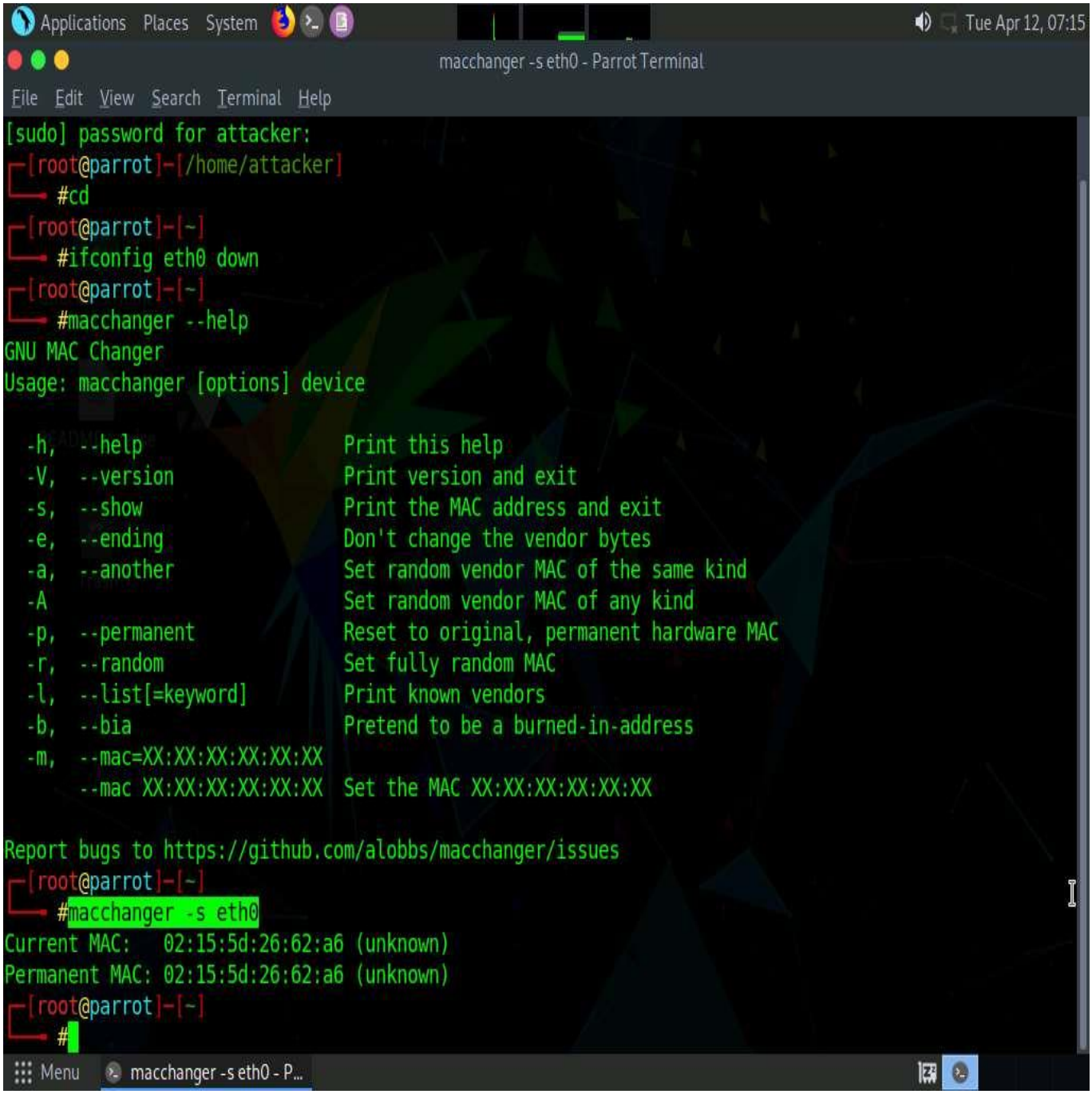


9. Type **macchanger --help** command to see the available options of macchanger tool.



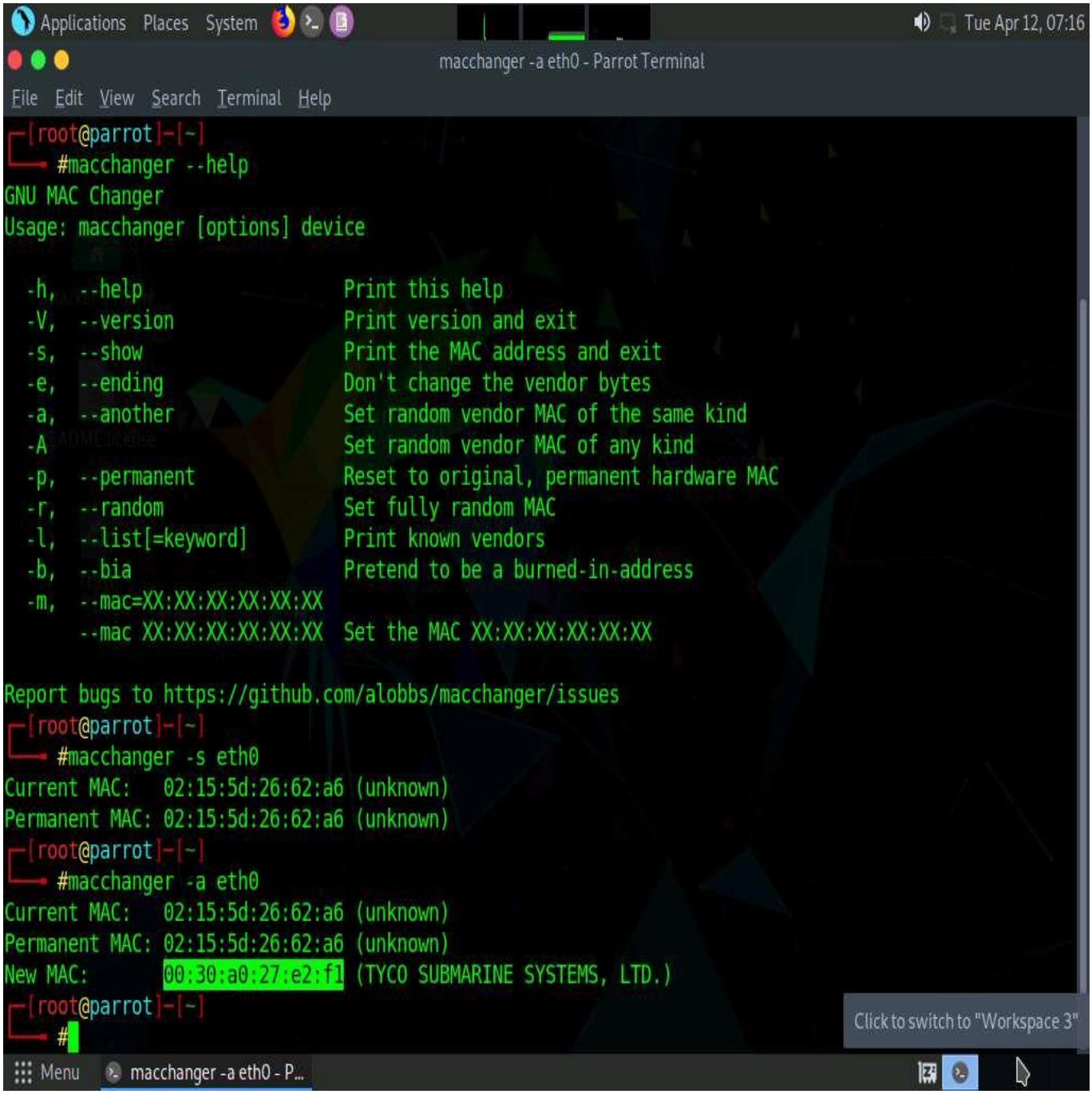
10. To see the current MAC address of the **Parrot Security** machine, type **macchanger -s eth0** and press **Enter**.

-s: prints the MAC address of the machine.

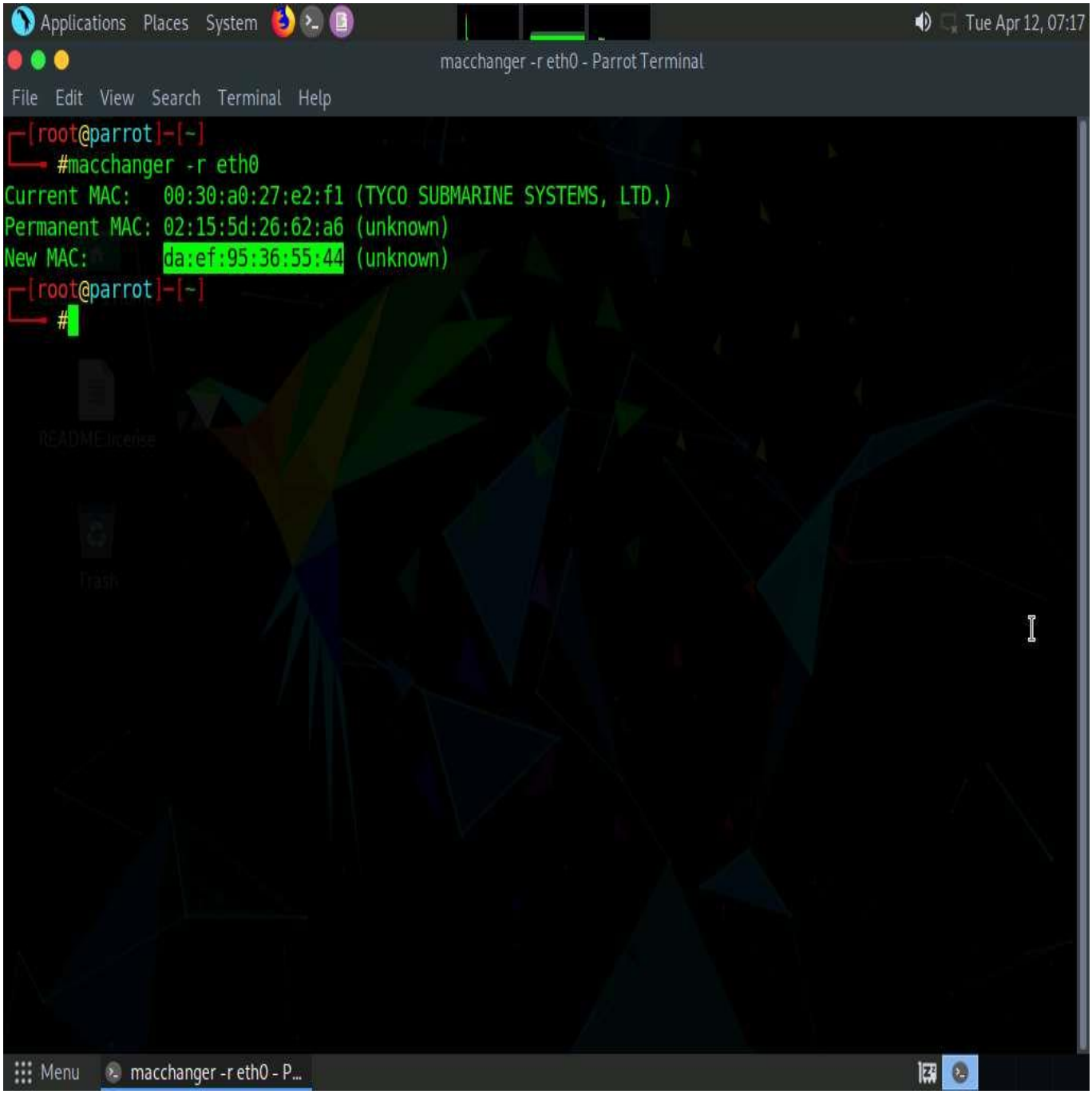


11. ☐ Now we will change the MAC address of the network interface.
12. ☐ In the terminal type, **macchanger -a eth0** and press **Enter**, to set a random vendor MAC address to the network interface.

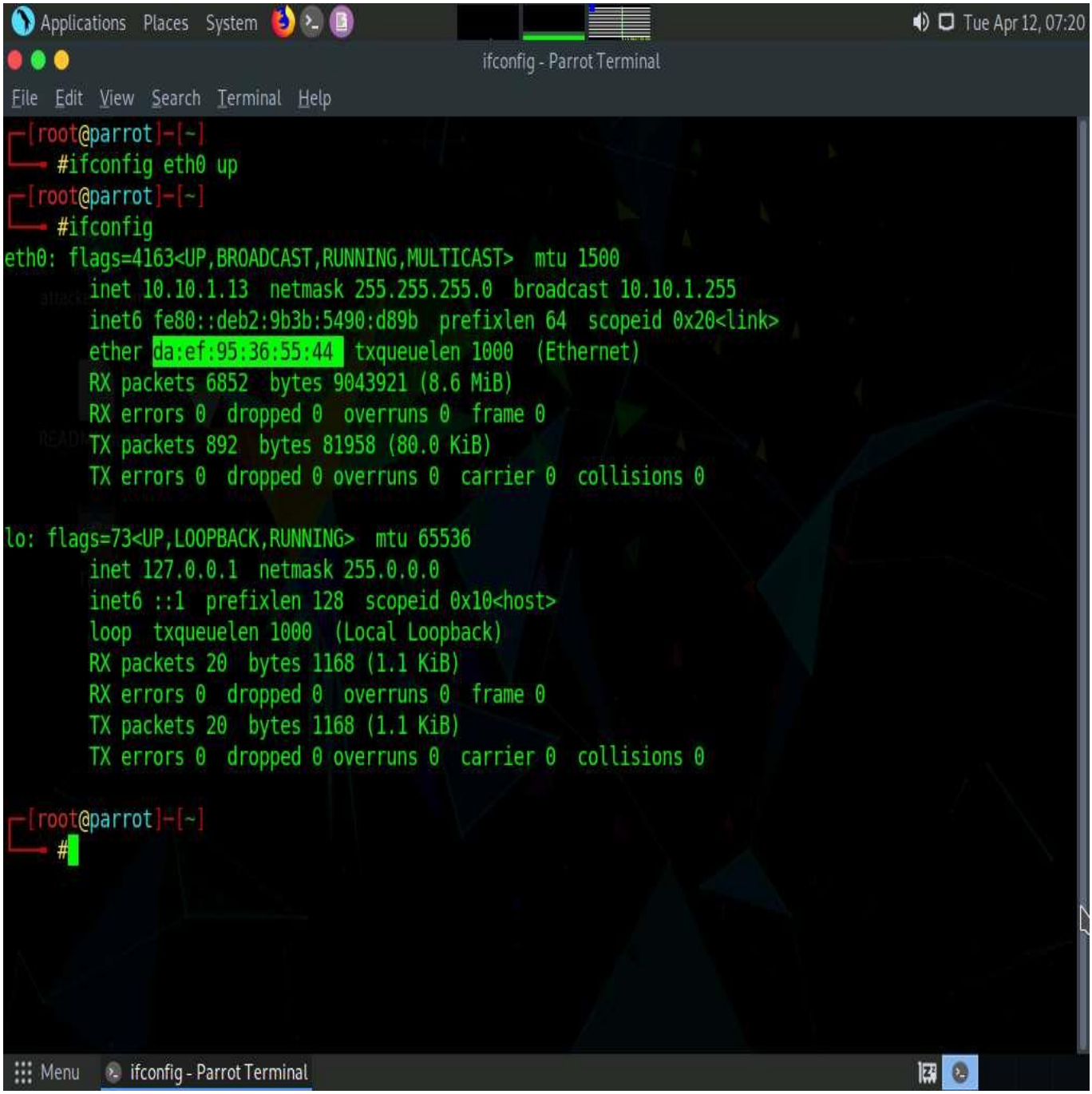
-a: sets random vendor MAC address to the network interface.



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



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



16. ☐ You can observe that a random MAC address is set to the network interface.
17. ☐ This concludes the demonstration of how to spoof a MAC address of Linux machine using macchanger
18. ☐ Close all open windows and document all the acquired information.
19. ☐ Now, before proceeding to the next task, **End** the lab and re-launch it to reset the machines. To do so, click the **Menu** icon ( ) and click **END** from the drop-down options.