Sniffing

Module 08

Network Sniffing

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Earlier modules taught how to damage target systems by infecting them using malware, which gives limited or full control of the target systems to further perform data exfiltration.

Now, as an ethical hacker or pen tester, it is important to understand network sniffing. Packet sniffing allows a person to observe and access the entire network's traffic from a given point. It monitors any bit of information entering or leaving the network. There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network.

Although passive sniffing was once predominant, proper network-securing architecture has been implemented (switch-based network) to mitigate this kind of attack. However, there are a few loopholes in switch-based network implementation that can open doors for an attacker to sniff the network traffic.

Attackers hack the network using sniffers, where they mainly target the protocols vulnerable to sniffing. Some of these vulnerable protocols include HTTP, FTP, SMTP, POP, Telnet, IMAP, and NNTP. The sniffed traffic comprises data such as FTP and Telnet passwords, chat sessions, email and web traffic, and DNS traffic. Once attackers obtain such sensitive information, they might attempt to impersonate target user sessions.

Thus, an ethical hacker or pen tester needs to assess the security of the network's infrastructure, find the loopholes in the network using various network auditing tools, and patch them up to ensure a secure network environment. The labs in this module provide real-time experience in performing packet sniffing on the target network using various packet sniffing techniques and tools.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

The objective of the lab is to perform network sniffing and other tasks that include, but are not limited to:

- Sniff the network
- Analyze incoming and outgoing packets for any attacks
- Troubleshoot the network for performance
- Secure the network from attacks

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 140 Minutes

Overview of Network Sniffing

Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

Packet sniffers are used to convert the host system's NIC to promiscuous mode. The NIC in promiscuous mode can then capture the packets addressed to the specific network. There are two types of sniffing. Each is used for different types of networks. The two types are:

- **Passive Sniffing**: Passive sniffing involves sending no packets. It only captures and monitors the packets flowing in the network
- **Active Sniffing**: Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN; it also refers to sniffing through a switch

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform network sniffing. Recommended labs that assist in learning various network sniffing techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Active Sniffing	√	√	√
	1.1 Perform MAC Flooding using macof	√		√
	1.2 Perform a DHCP Starvation Attack using Yersinia	√		√
	1.3 Perform ARP Poisoning using arpspoof		√	√

	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel		√	√
	1.5 Spoof a MAC Address using TMAC and SMAC		√	√
2	Perform Network Sniffing using Various Sniffing Tools	√	√	√
	2.1 Perform Password Sniffing using Wireshark	√		√
	2.2 Analyze a Network using the Capsa Network Analyzer		√	
	2.3 Analyze a Network using the Omnipeek Network Protocol Analyzer		√	√
	2.4 Analyze a Network using the SteelCentral Packet Analyzer		√	√
3	Detect Network Sniffing	√		√
	3.1 Detect ARP Poisoning in a Switch-Based Network	√		√
	3.2 Detect ARP Attacks using Xarp	√		√
	3.3 Detect Promiscuous Mode using Nmap and NetScanTools Pro	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Perform Active Sniffing

Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

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.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

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

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine

- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- TMAC located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC)**
- SMAC located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 50 Minutes

Overview of Active Sniffing

Active sniffing involves sending out multiple network probes to identify access points. The following is the list of different active sniffing techniques:

- **MAC Flooding**: Involves flooding the CAM table with fake MAC address and IP pairs until it is full
- **DNS Poisoning**: Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not
- **ARP Poisoning**: Involves constructing a large number of forged ARP request and reply packets to overload a switch
- **DHCP Attacks**: Involves performing a DHCP starvation attack and a rogue DHCP server attack
- **Spoofing Attack**: Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Lab Tasks

TASK 1

Perform MAC Flooding using macof

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

Here, we will use the macof tool to perform MAC flooding:

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

Note: For demonstration purposes, we are using only one target machine (namely, **Windows 10**). 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.

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

Note:

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

TASK 1.1

Launch Wireshark

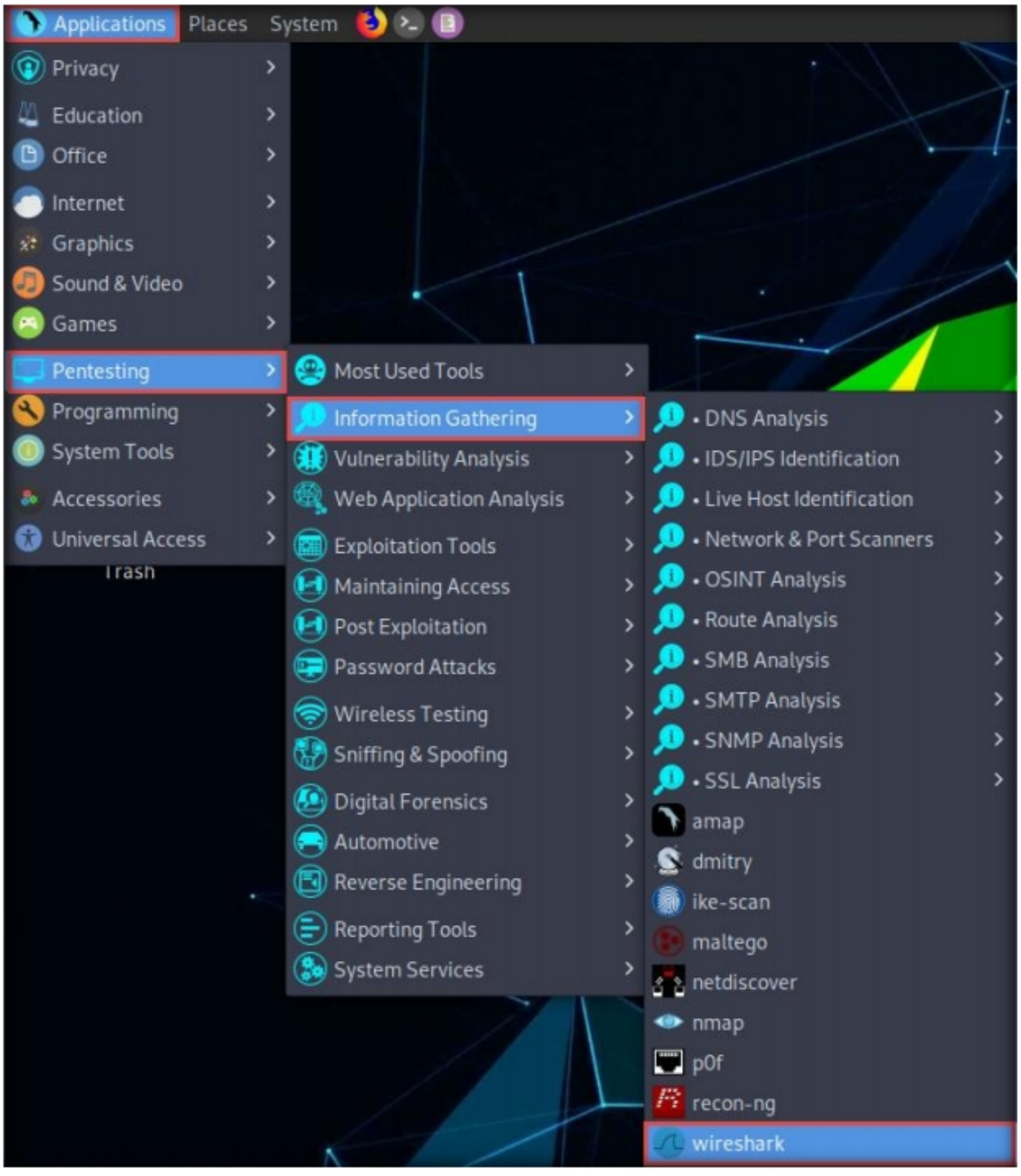


Figure 1.1.1: Launching Wireshark

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

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.

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.

Note: The network adapter might differ in your lab environment.

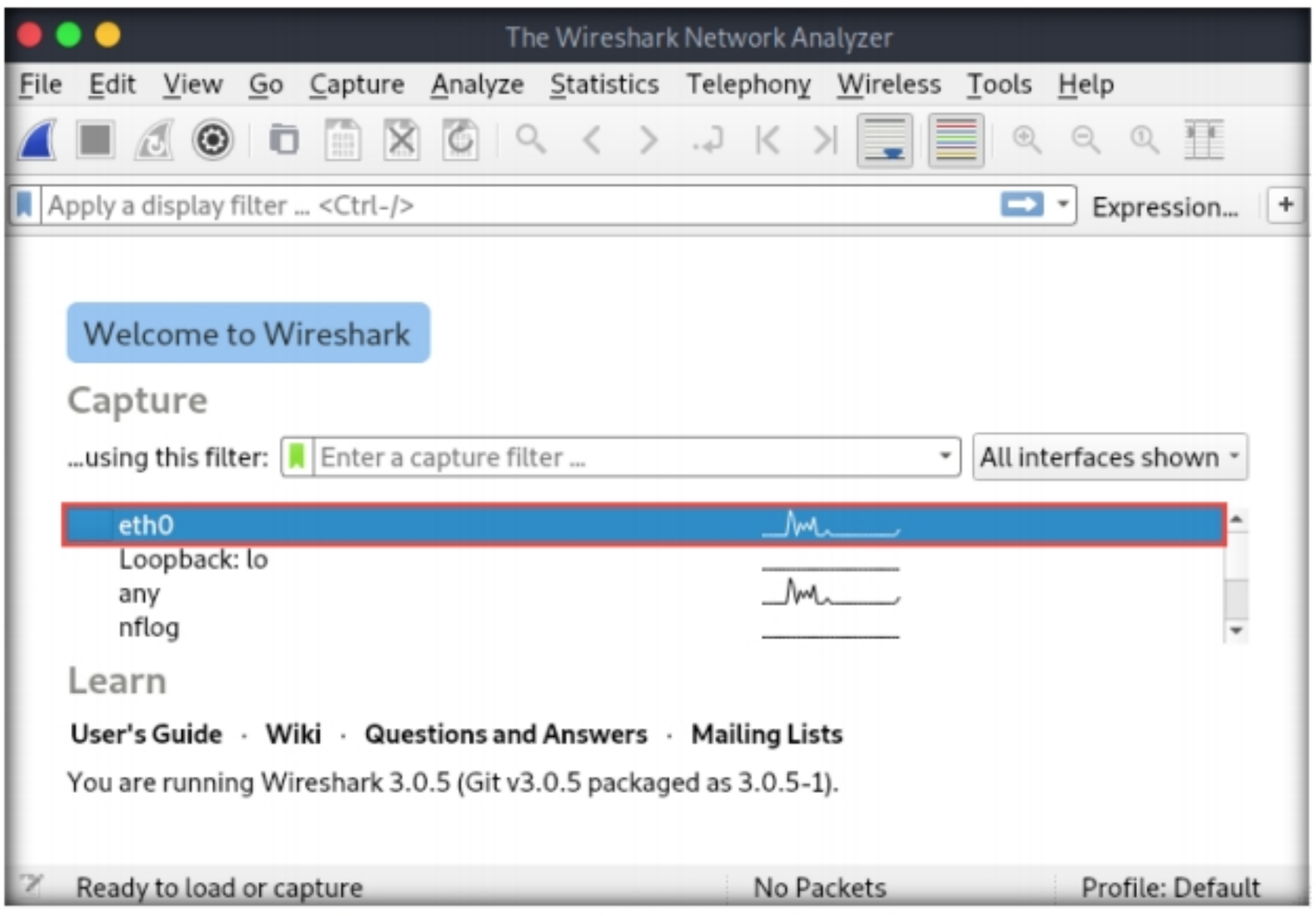


Figure 1.1.2: Wireshark Main Window with Interface Option

6. Leave the **Wireshark** application running.
7. Navigate to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
8. Open the **Wireshark** application and double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.
9. Now, switch back to the **Parrot Security** virtual machine.
10. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
11. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
12. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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

TASK 1.2

Launch MAC Flooding Attack

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

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

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

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

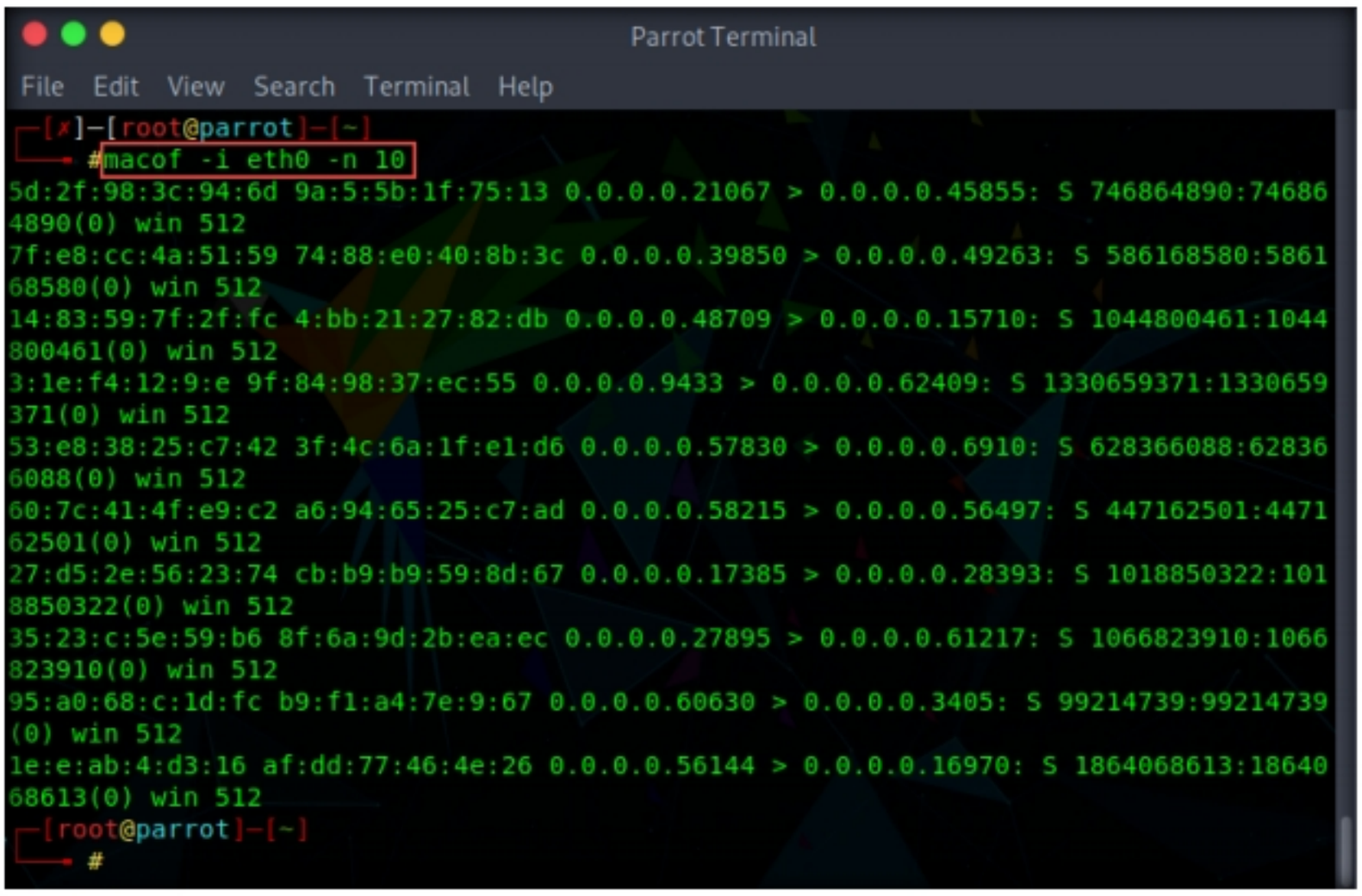


Figure 1.1.3: Command to flood the CAM table

TASK 1.3

Analyze Captured Packets

16. Open the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.

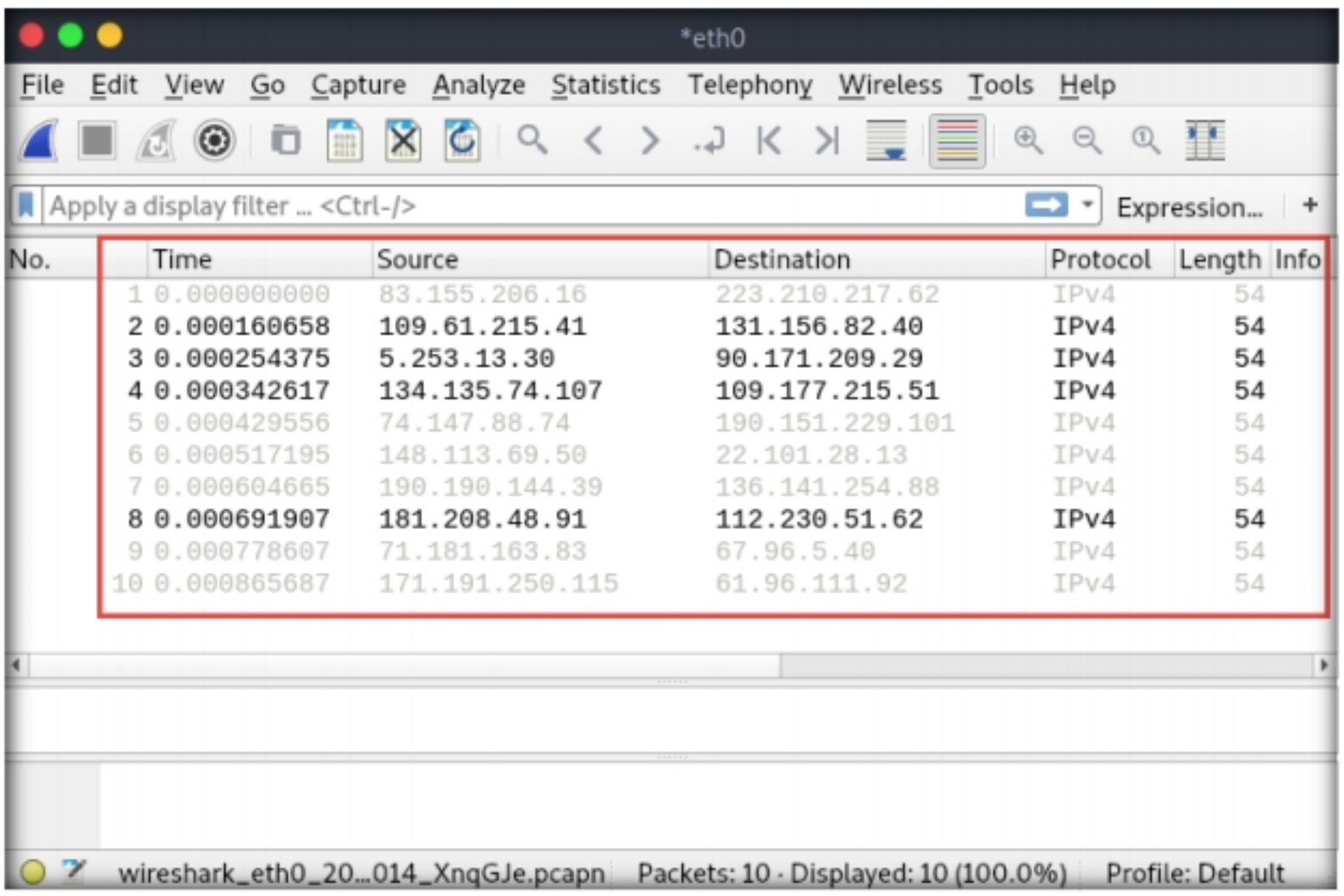


Figure 1.1.4: Wireshark captured packets

17. 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.

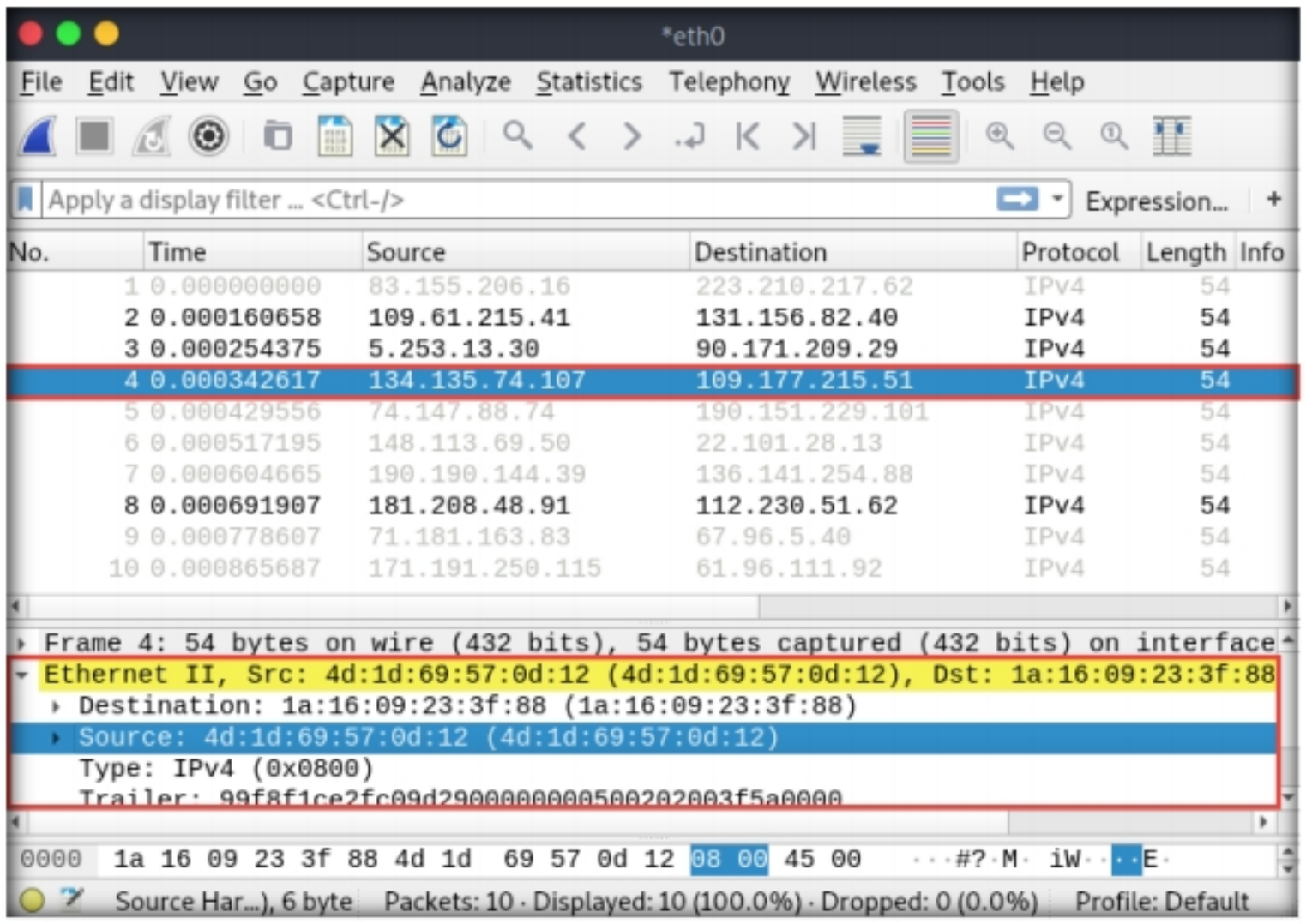


Figure 1.1.5: Viewing packet content in Wireshark

18. Now, switch to the **Windows 10** virtual machine and observe the packets captured by Wireshark.

19. You will find the same packets that were captured by Wireshark in the **Parrot Security** virtual machine.

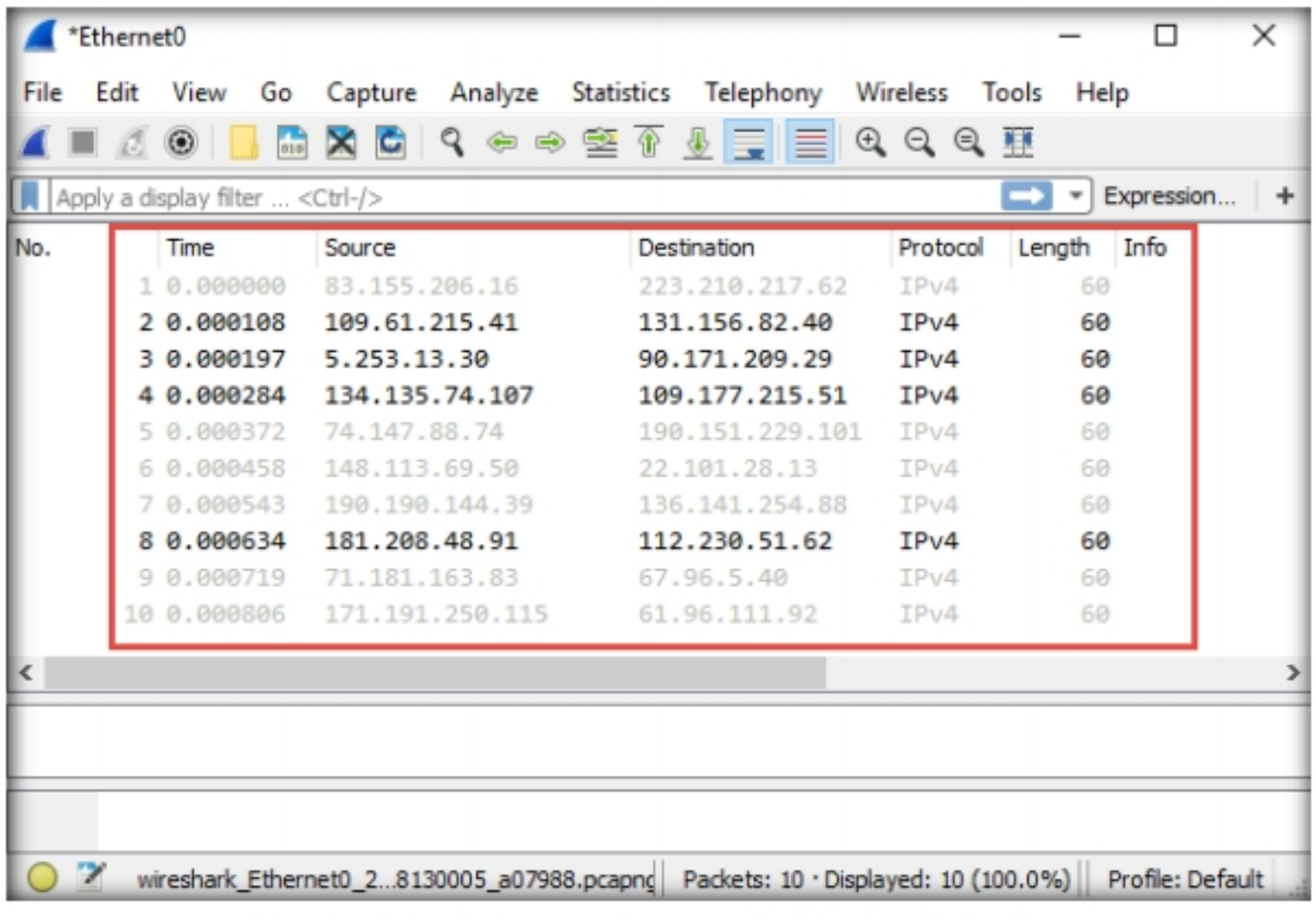


Figure 1.1.6: Wireshark captured the target machine's packets (Windows 10)

20. 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.
21. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Quit without Saving** to close the Wireshark application.
22. This concludes the demonstration of how to perform MAC flooding using macof.
23. Close all open windows and document all the acquired information.

TASK 2 Perform a DHCP Starvation Attack using Yersinia

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

TASK 2.1 Launch Wireshark

1. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.
2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

Note: The network adapter might differ in your lab environment.

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.

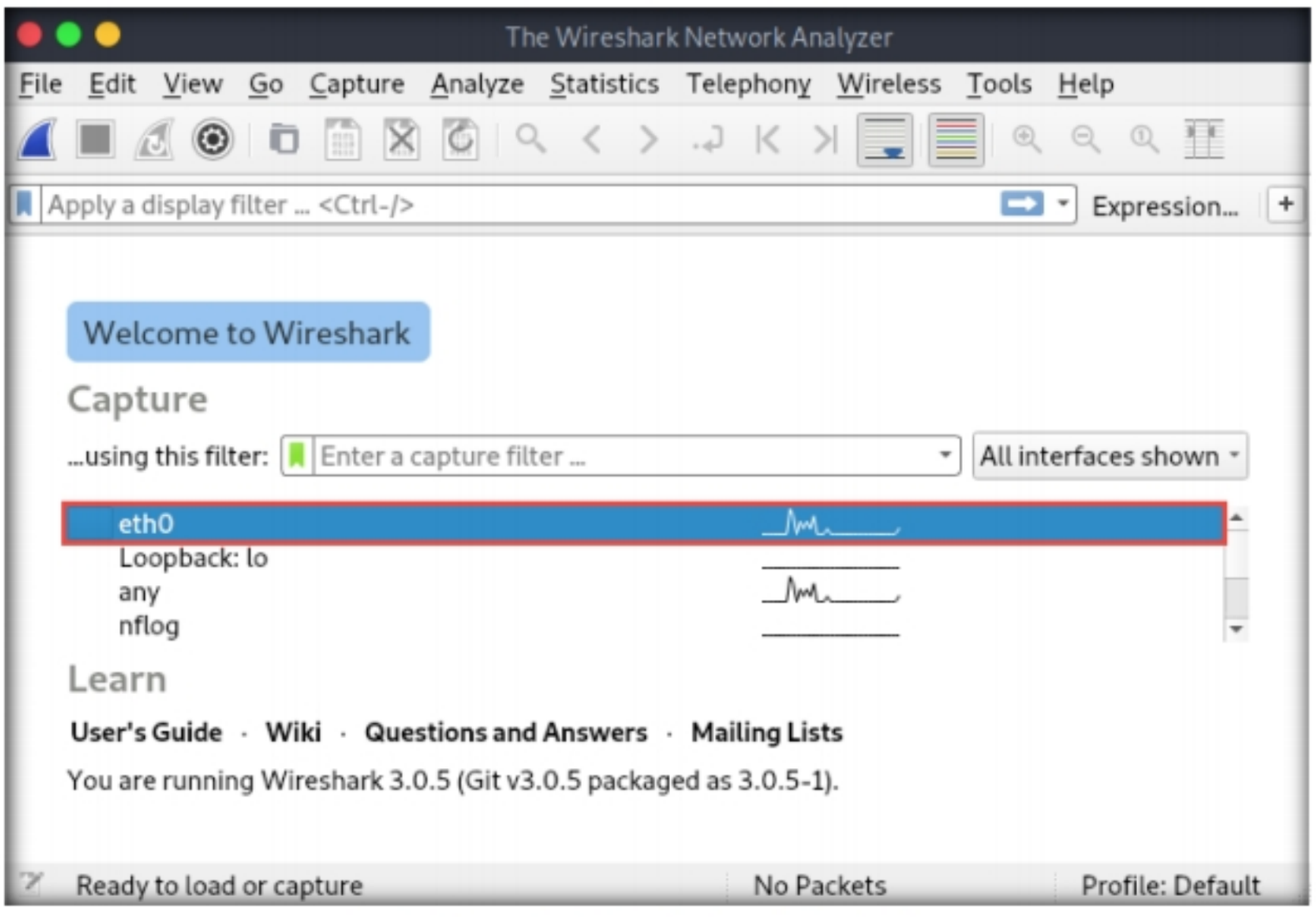


Figure 1.2.1: Wireshark Main Window with Interface Option

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**.

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

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

TASK 2.2

Launch and Configure Yersinia

9. In the terminal window, click the **Maximize Window** icon ( ) to maximize the terminal window.

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

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

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

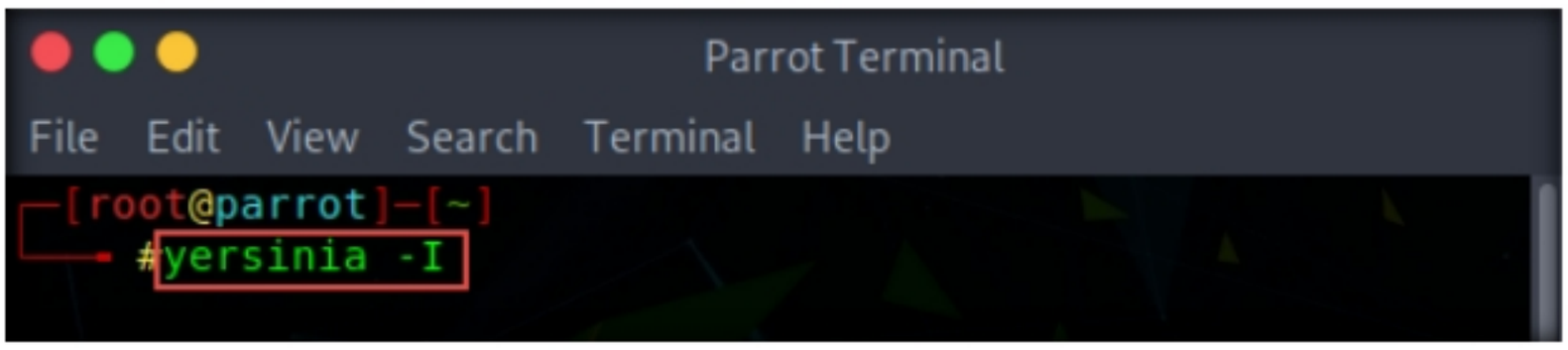


Figure 1.2.2: Issue command to open Yersinia in interactive mode

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.

11. Yersinia interactive mode appears in the terminal window.

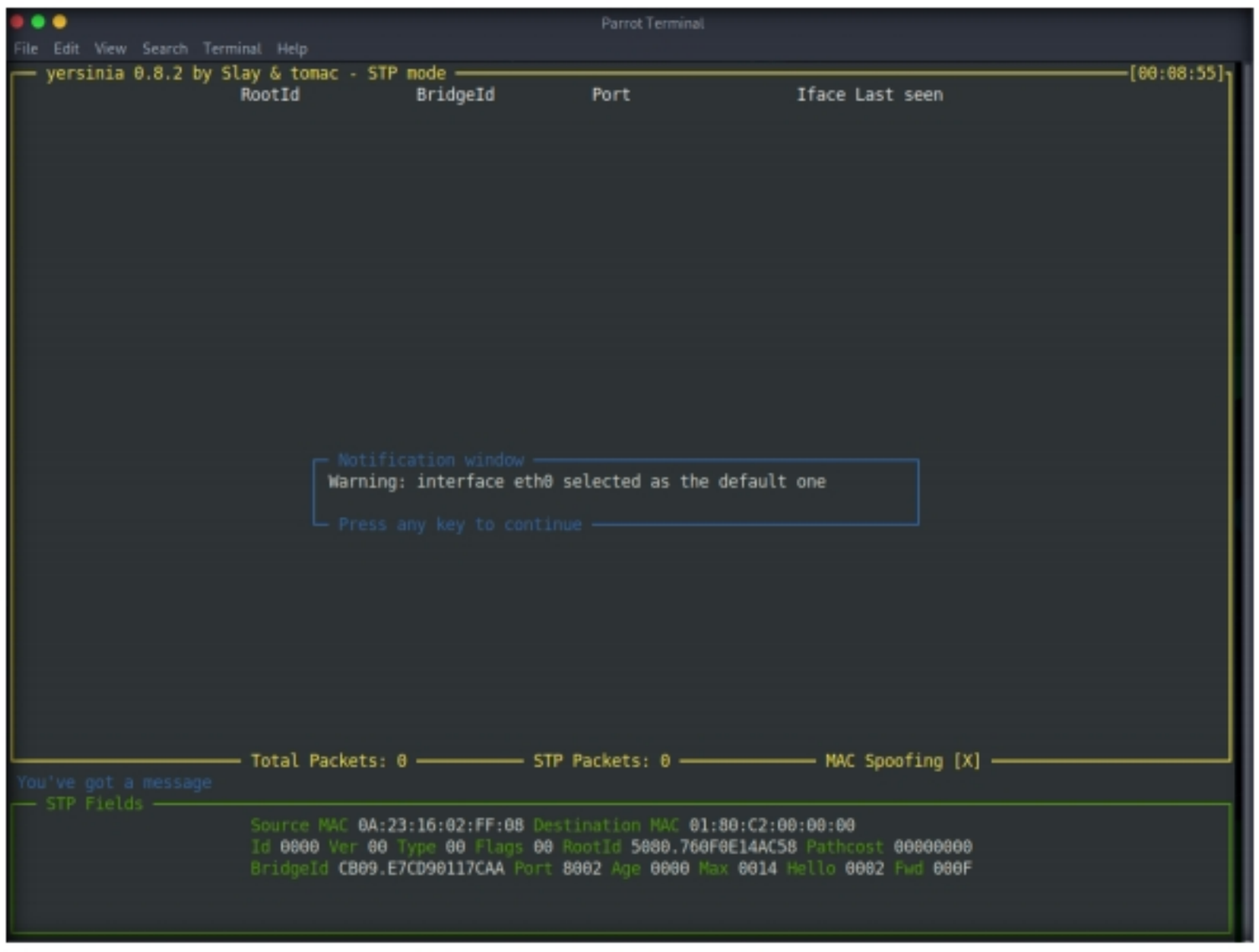


Figure 1.2.3: Yersinia interactive mode

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

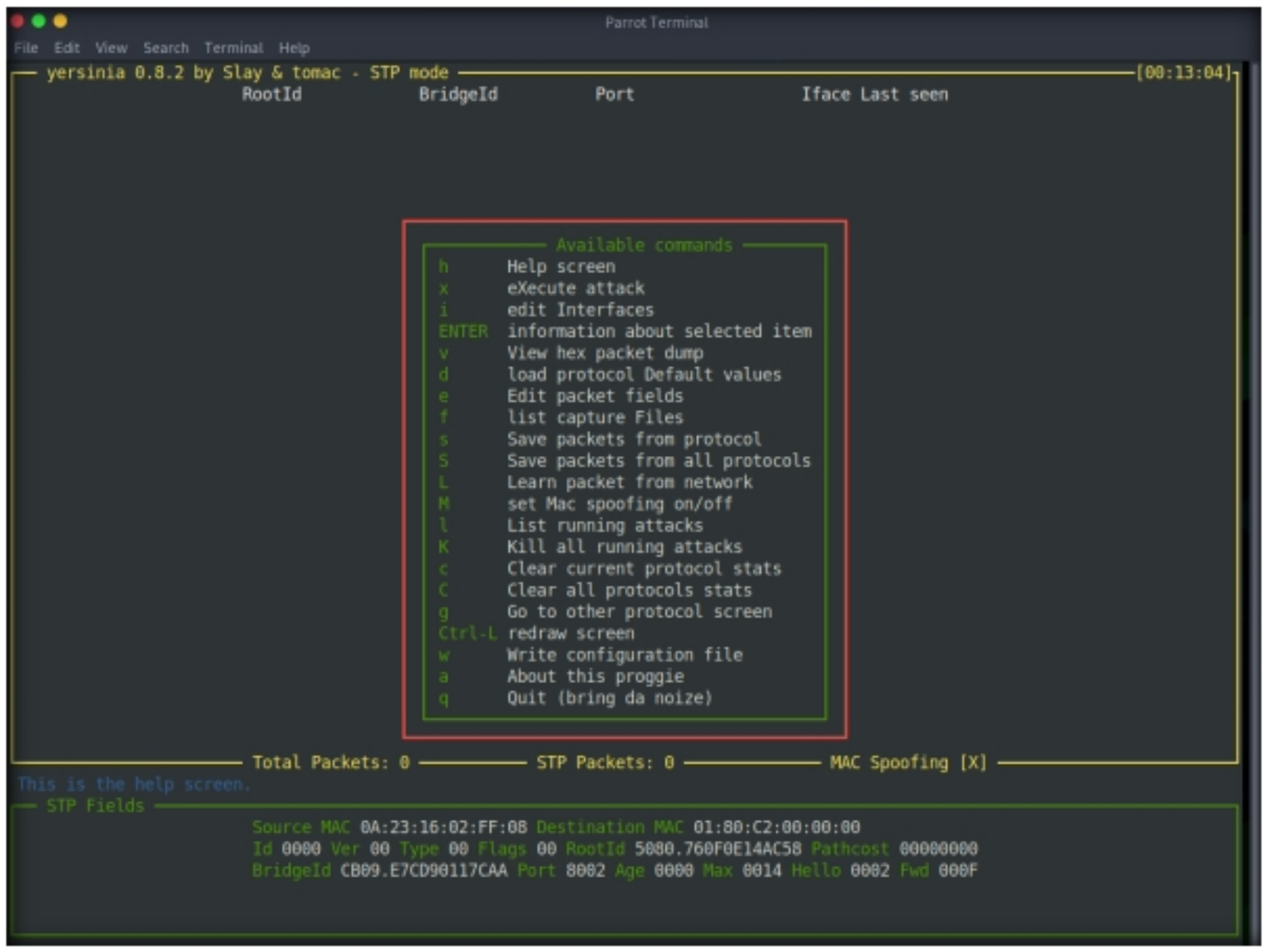


Figure 1.2.4: Yersinia help

14. Press **q** to exit the help options.
15. 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.

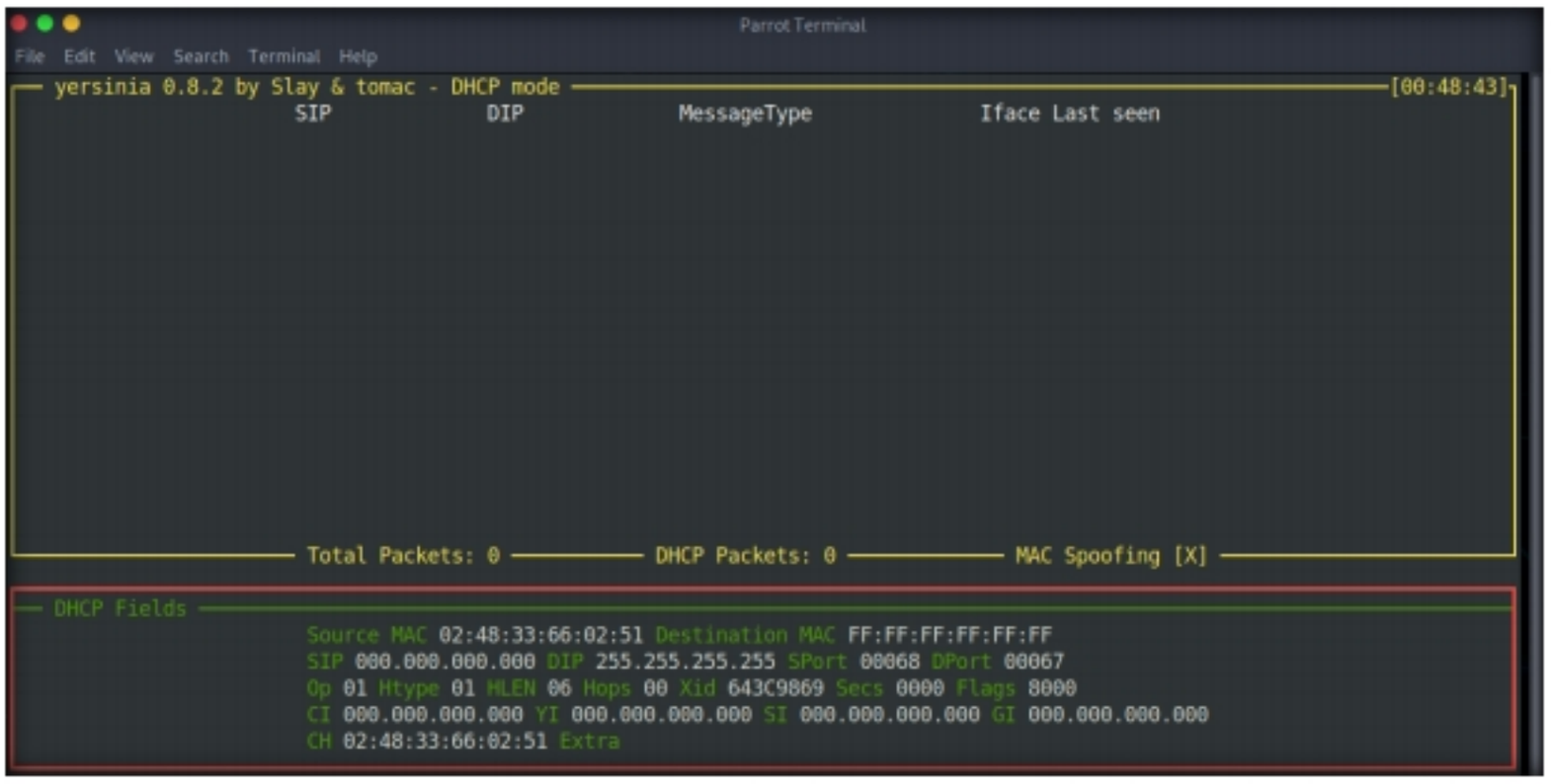


Figure 1.2.5: Yersinia: Execute DHCP mode

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

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

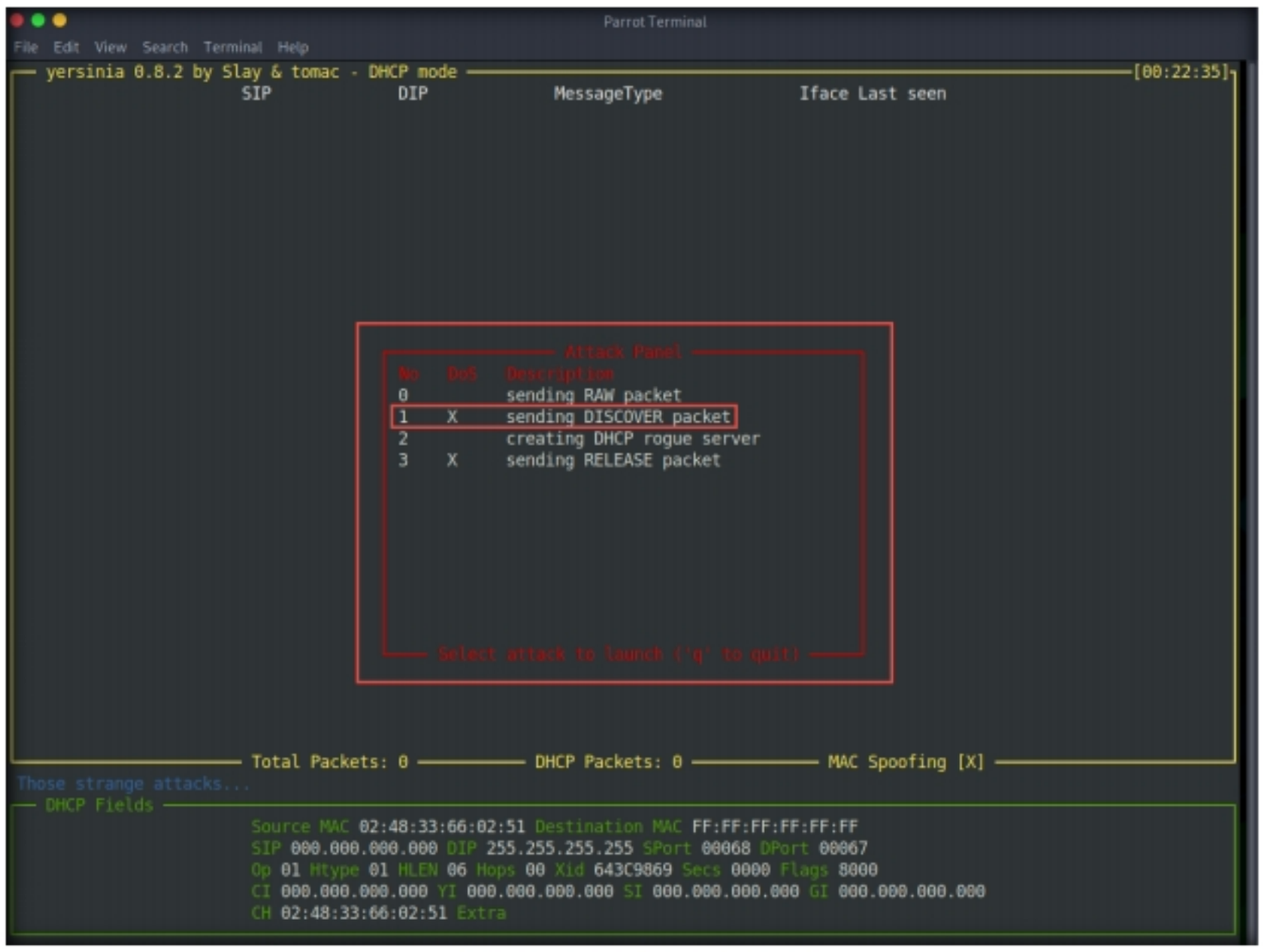


Figure 1.2.6: Yersinia attack panel

TASK 2.3

Launch DHCP Starvation Attack

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

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

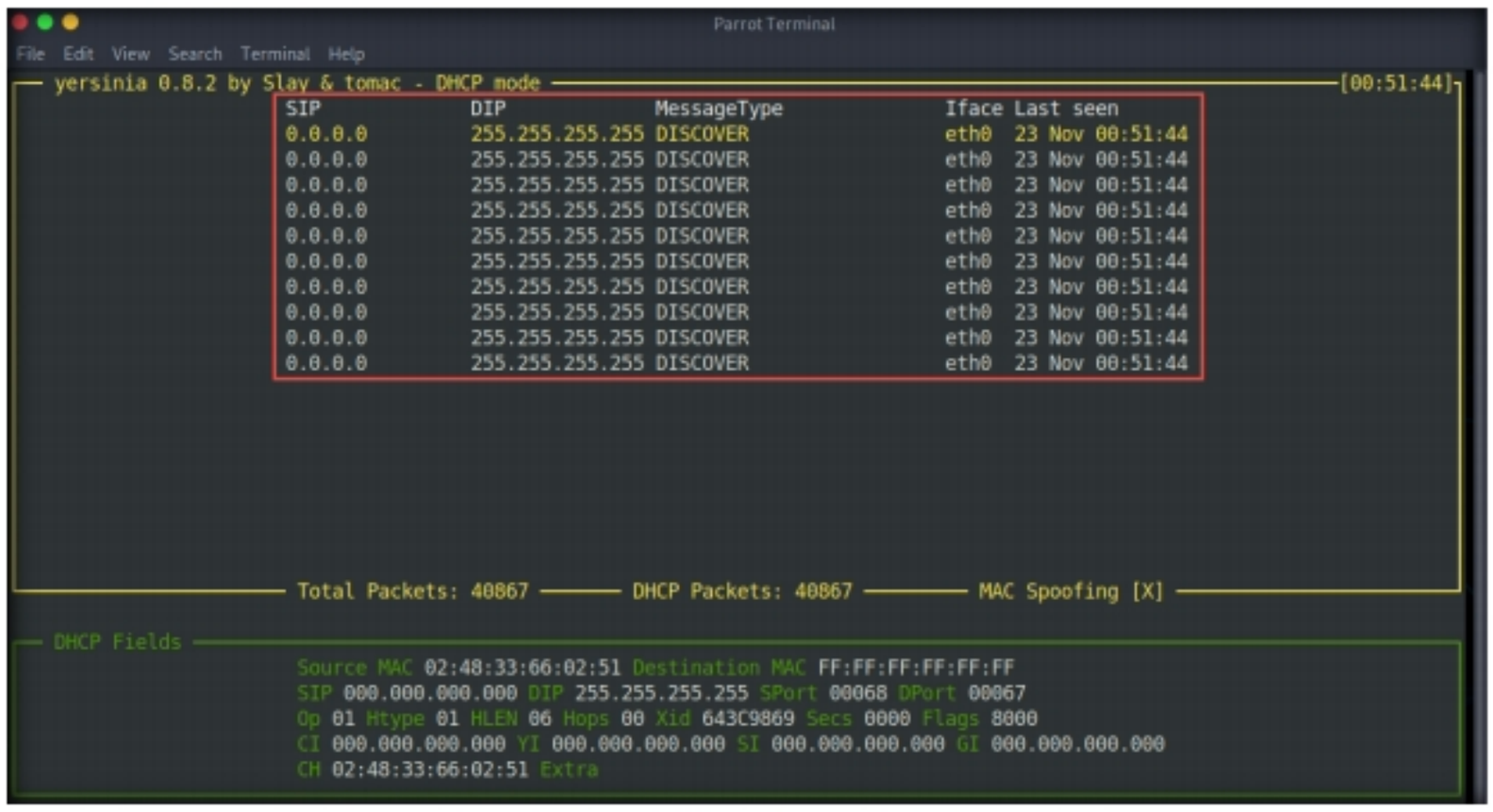


Figure 1.2.7: Yersinia sending DHCP packets

19. After a few seconds, press **q** to stop the attack.

TASK 2.4

Analyze Captured Packets

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

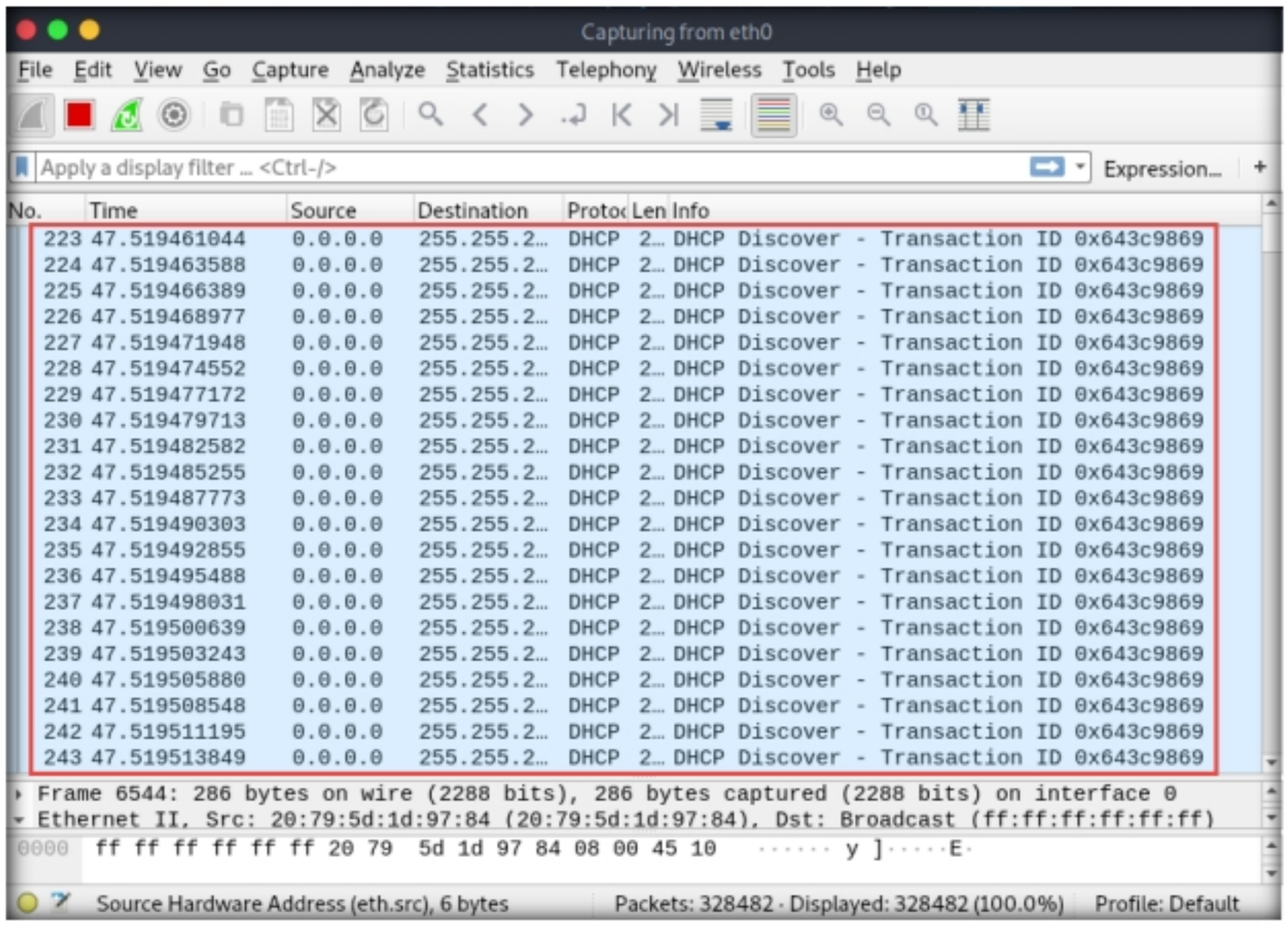


Figure 1.2.8: Wireshark: DHCP packets

You can also use other DHCP starvation attack tools such as **Hyenae** (https://sourceforge.net), **dhcpstarv** (https://github.com), **Gobbler** (https://sourceforge.net), or **DHCPig** (https://github.com) to perform DHCP starvation attack.

21. 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.

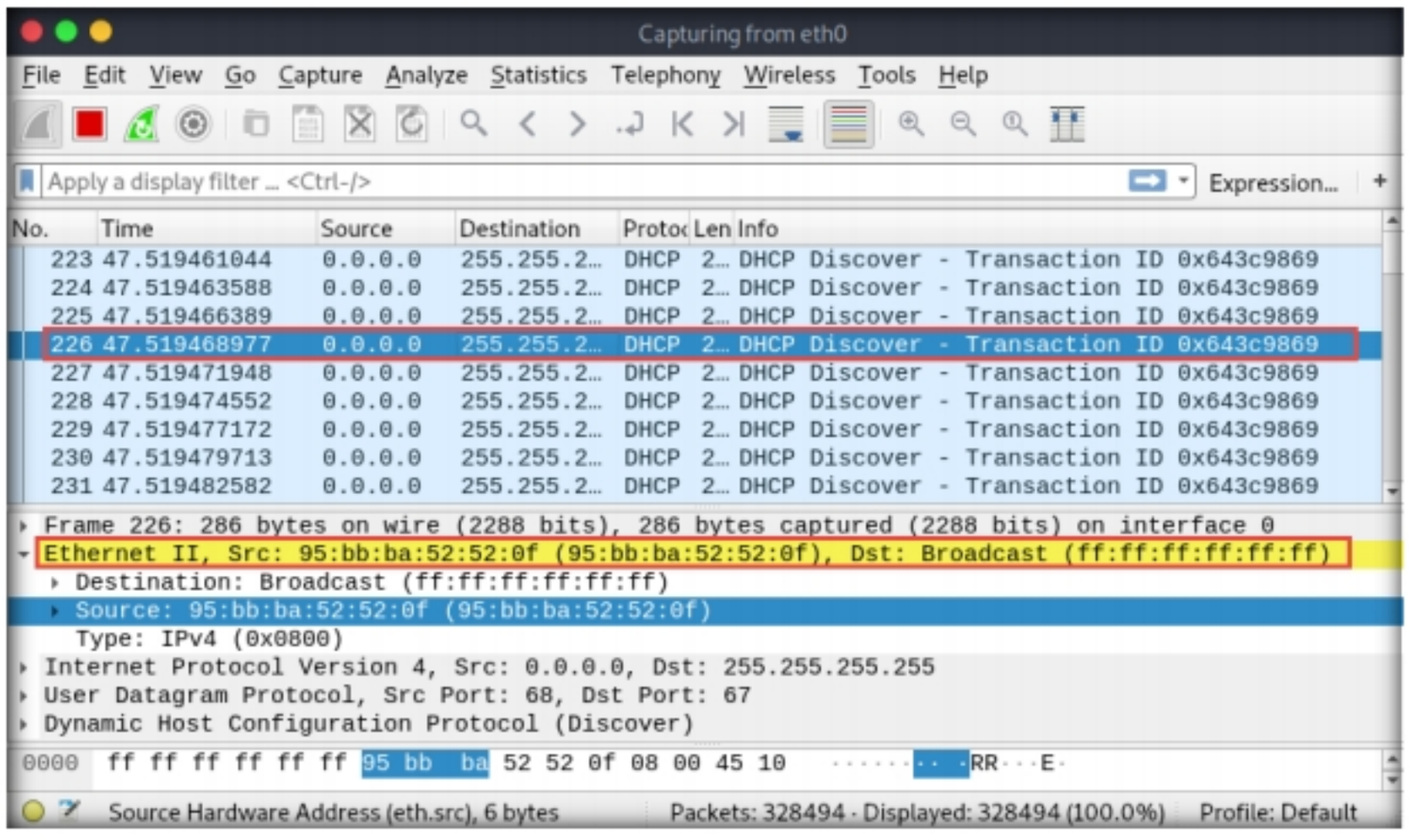


Figure 1.2.9: Viewing packet content

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

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

TASK 3 Perform ARP Poisoning using arpspoof

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

Note: In this lab, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

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

TASK 3.1

Launch 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.

Note: The network adapter might differ in your lab environment.

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.

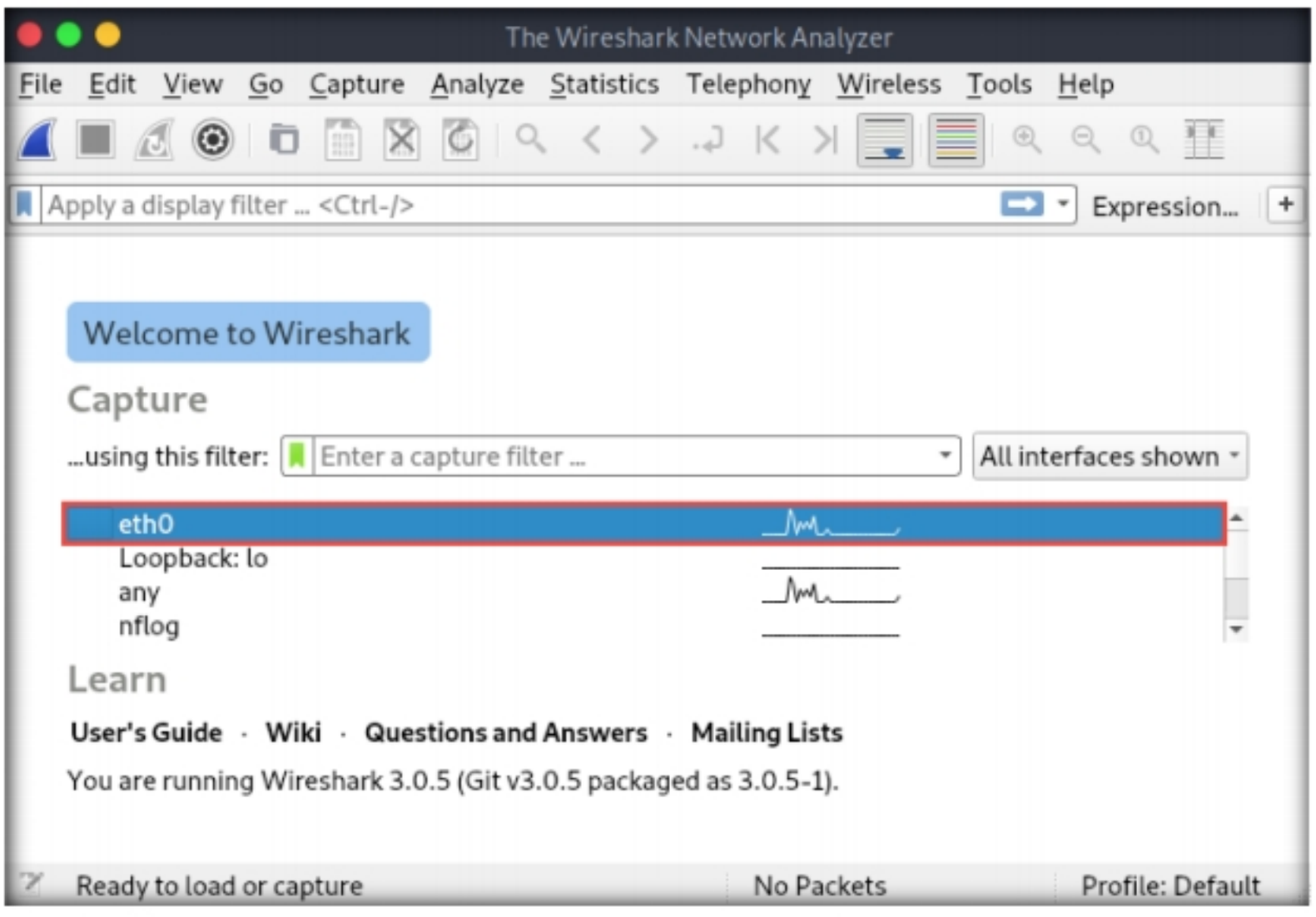


Figure 1.3.1: Wireshark Main Window with Interface Option

4. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

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

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

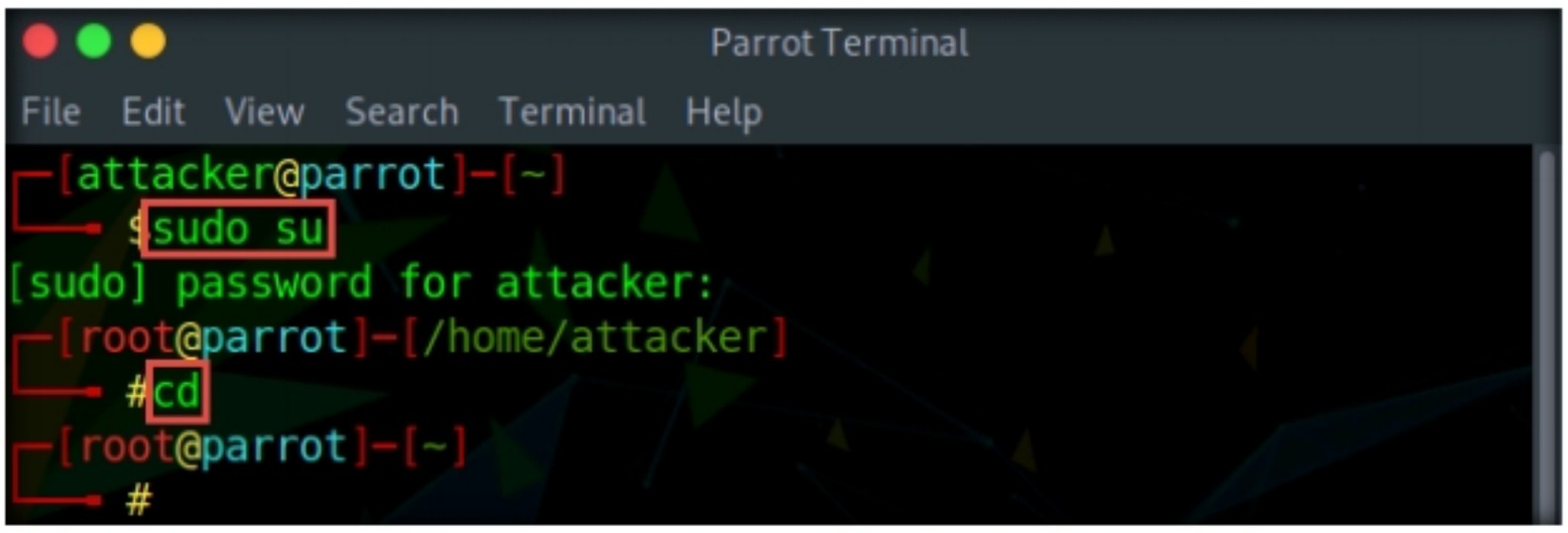


Figure 1.3.2: Running the programs as a root user

TASK 3.2

Spoof as a Target Host

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.

8. In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.10.2 10.10.10.10** and press **Enter**.

   (Here, **10.10.10.10** is IP address of the target system [**Windows 10**], and **10.10.10.2** is IP address of the access point or gateway)

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

Note: The IP addresses might differ in your lab environment.

9. Issuing the above command informs the access point that the target system (**10.10.10.10**) 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.

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

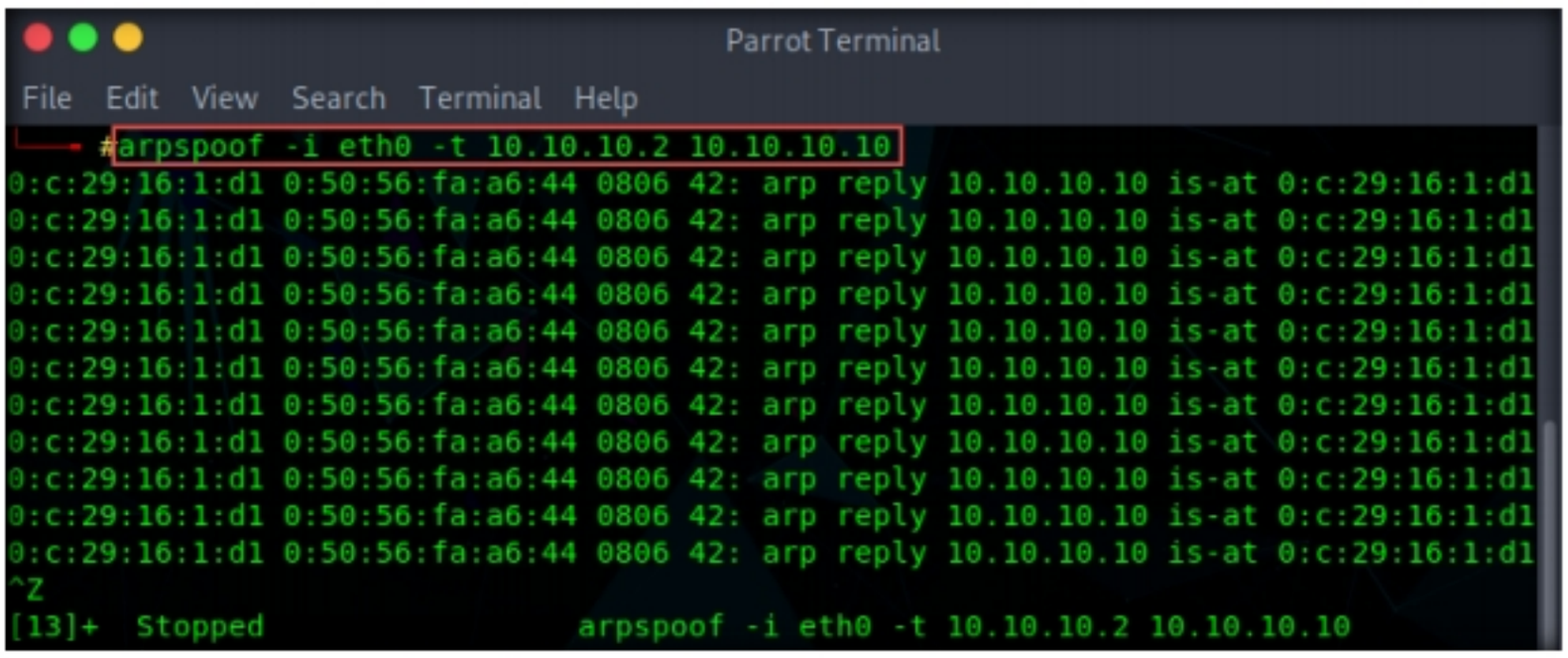


Figure 1.3.3: arpspoof command to spoof as a target system

11. As shown in the screenshot, you can observe the **ARP** packets captured by **Wireshark**.

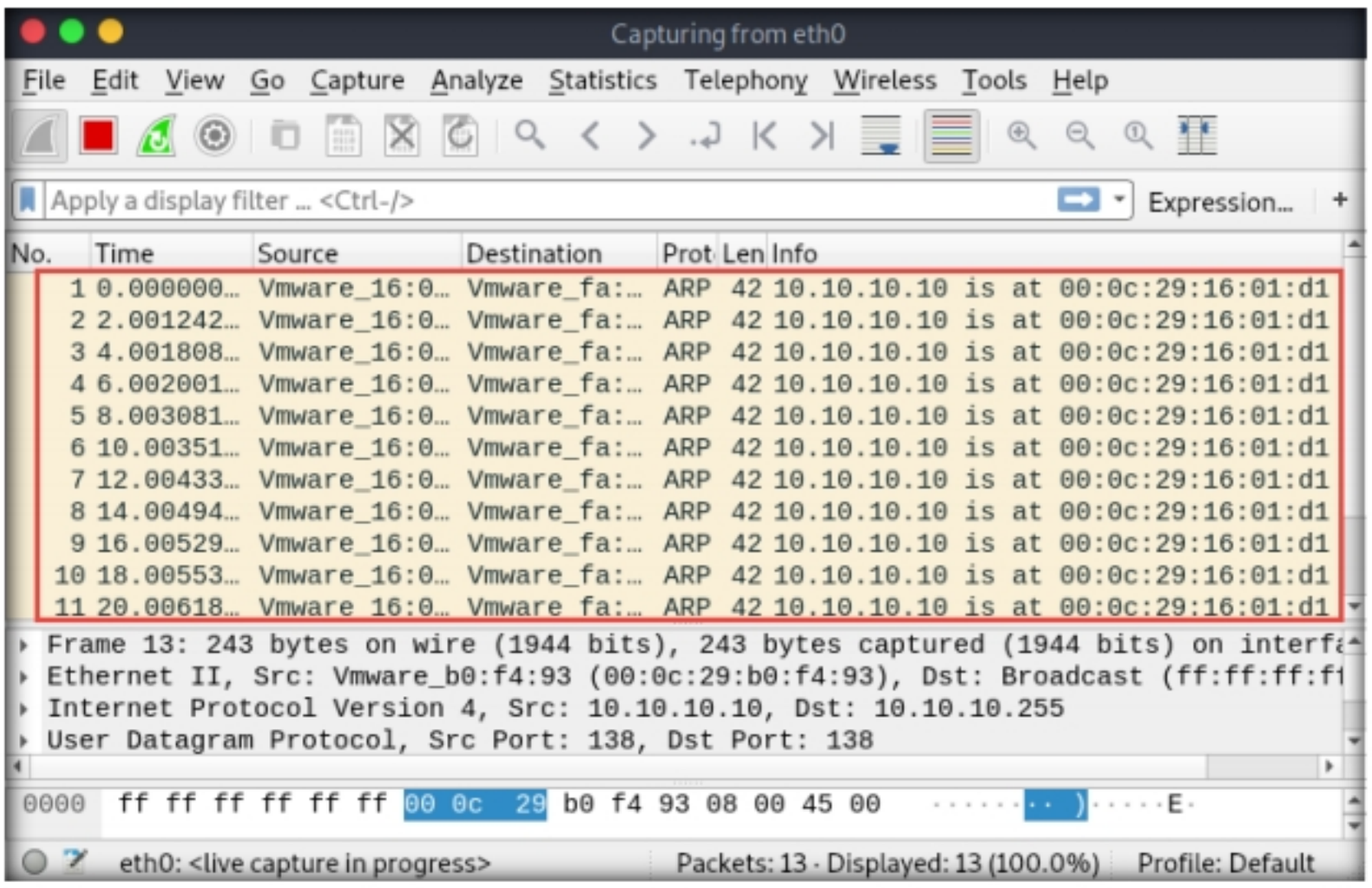


Figure 1.3.4: Wireshark captured ARP packets

TASK 3.3

Spoof as an Access Point

12. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.10.10 10.10.10.2** and press **Enter**.
13. Through the above command, the host system informs the target system (**10.10.10.10**) that it is the access point (**10.10.10.2**).
14. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

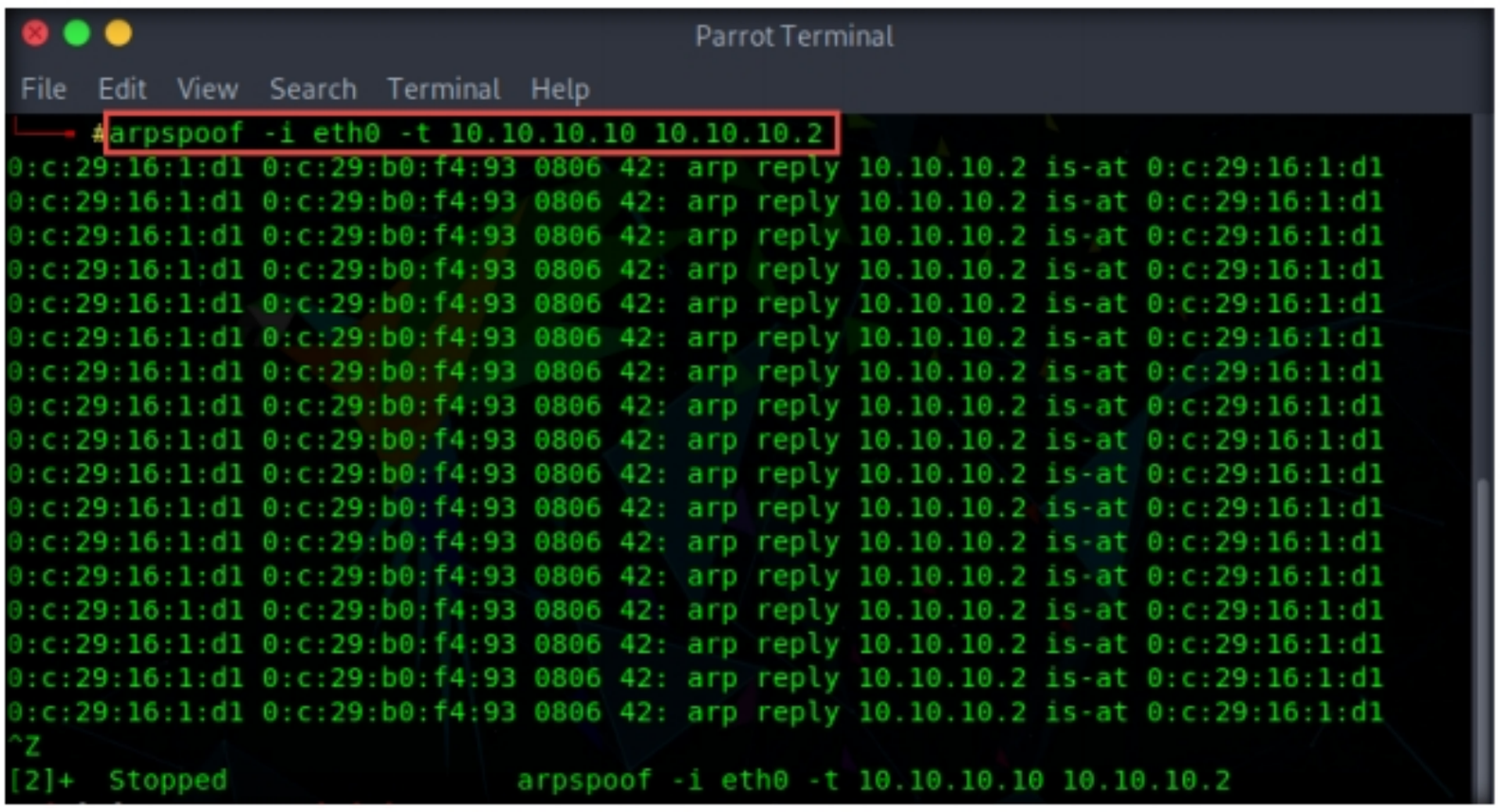


Figure 1.3.5: arpspoof command to spoof as an access point

TASK 3.4

Analyze Captured Packets

15. In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.10.10 detected!**"
16. 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 **10.10.10.2** and **10.10.10.10**.

Note: Here, the MAC address of the host system (**Parrot Security**) is **00:0c:29:16:01:d1**.

Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 10**) and access point. Therefore, the alert warning of a duplicate use of **10.10.10.10** is displayed.

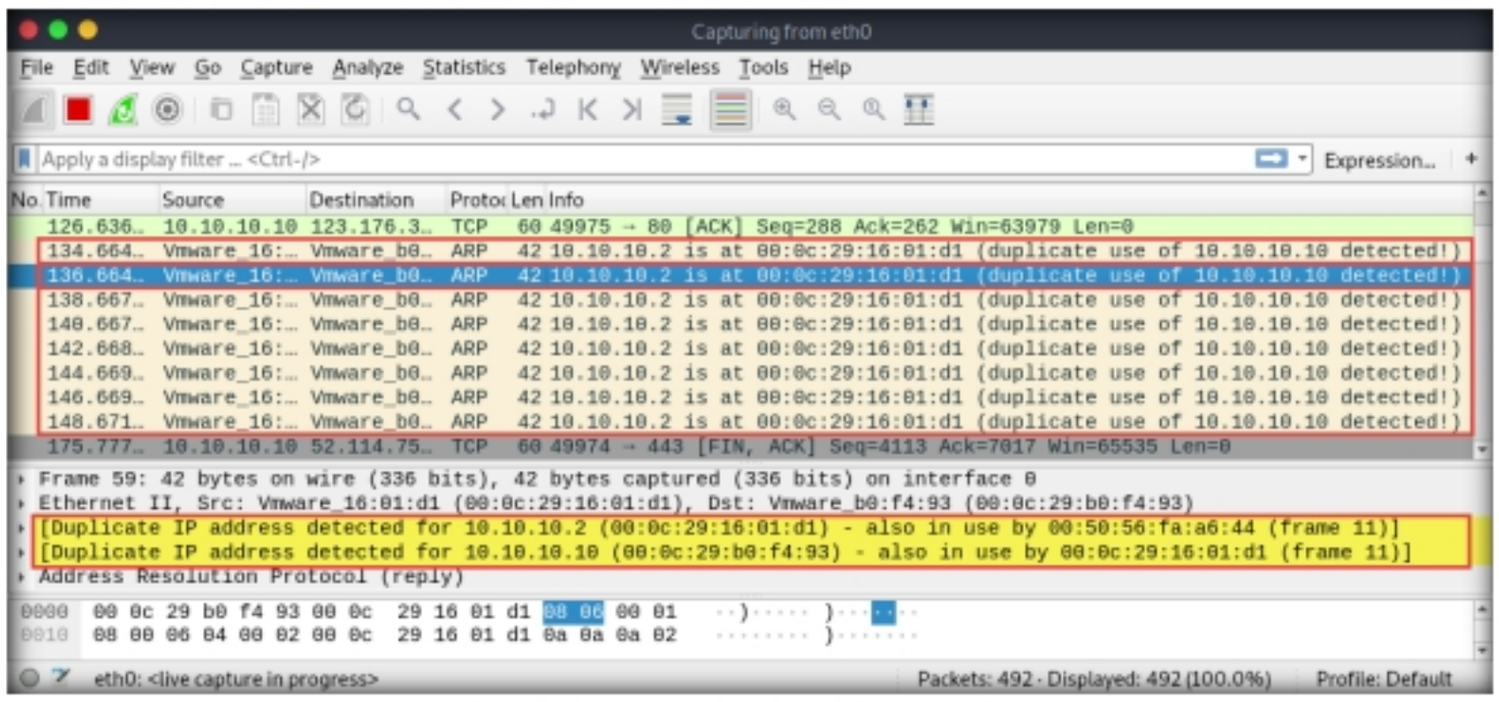


Figure 1.3.6: Wireshark captured ARP packets

TASK 3.5

View ARP Cache

17. Now, switch to the **Windows 10** virtual machine; click the **Type here to search field** at the bottom of **Desktop**. Type **cmd** and click **Command Prompt** from the results.
18. In the **Command Prompt** window, type **arp -a** and press **Enter** to view the ARP cache.
19. The results appear, displaying the IP addresses and their corresponding MAC addresses. Observe that the MAC addresses of IP addresses **10.10.10.2** and **10.10.10.13** are the same, indicating the occurrence of an ARP poisoning attack, where 10.10.10.13 is the **Parrot Security** machine and 10.10.10.2 is the access point.

You can also use other ARP poisoning tools such as **BetterCAP** (https://www.bettercap.org), **Ettercap** (http://www.ettercap-project.org), **dsniff** (https://www.monkey.org), or **MITMf** (https://github.com) to perform ARP poisoning attack.

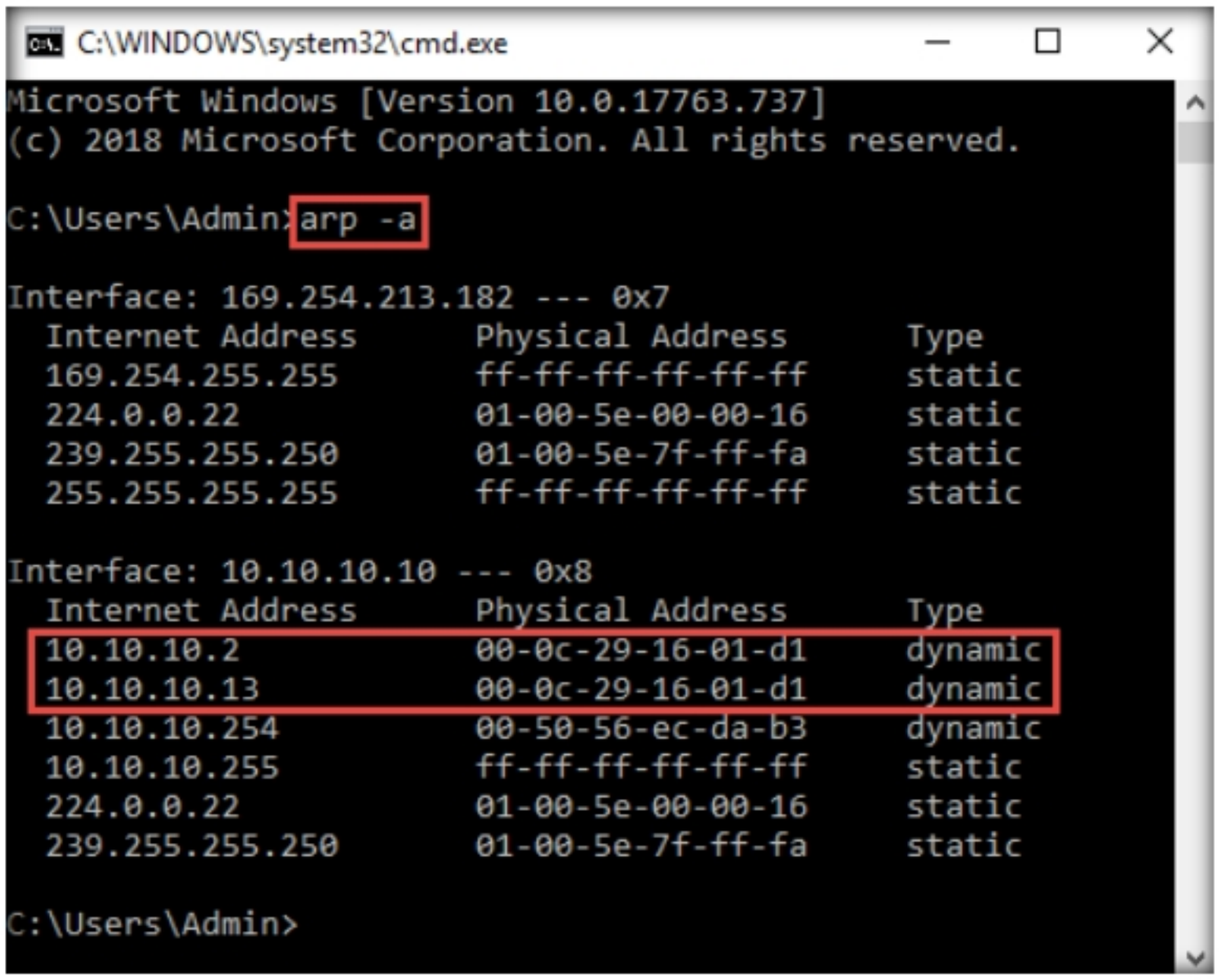


Figure 1.3.7: Command Prompt window: arp -a results

20. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
21. Close all open windows and document all the acquired information.
22. Turn off the **Parrot Security** virtual machine.

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

An attacker can obtain user names 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.

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

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Install and Configure Cain & Abel

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.

1. Turn on the **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel** and double-click **ca_setup.exe**.
4. Cain & Abel initializes, and the **Cain & Abel Installation** window appears; click the **Next** button.

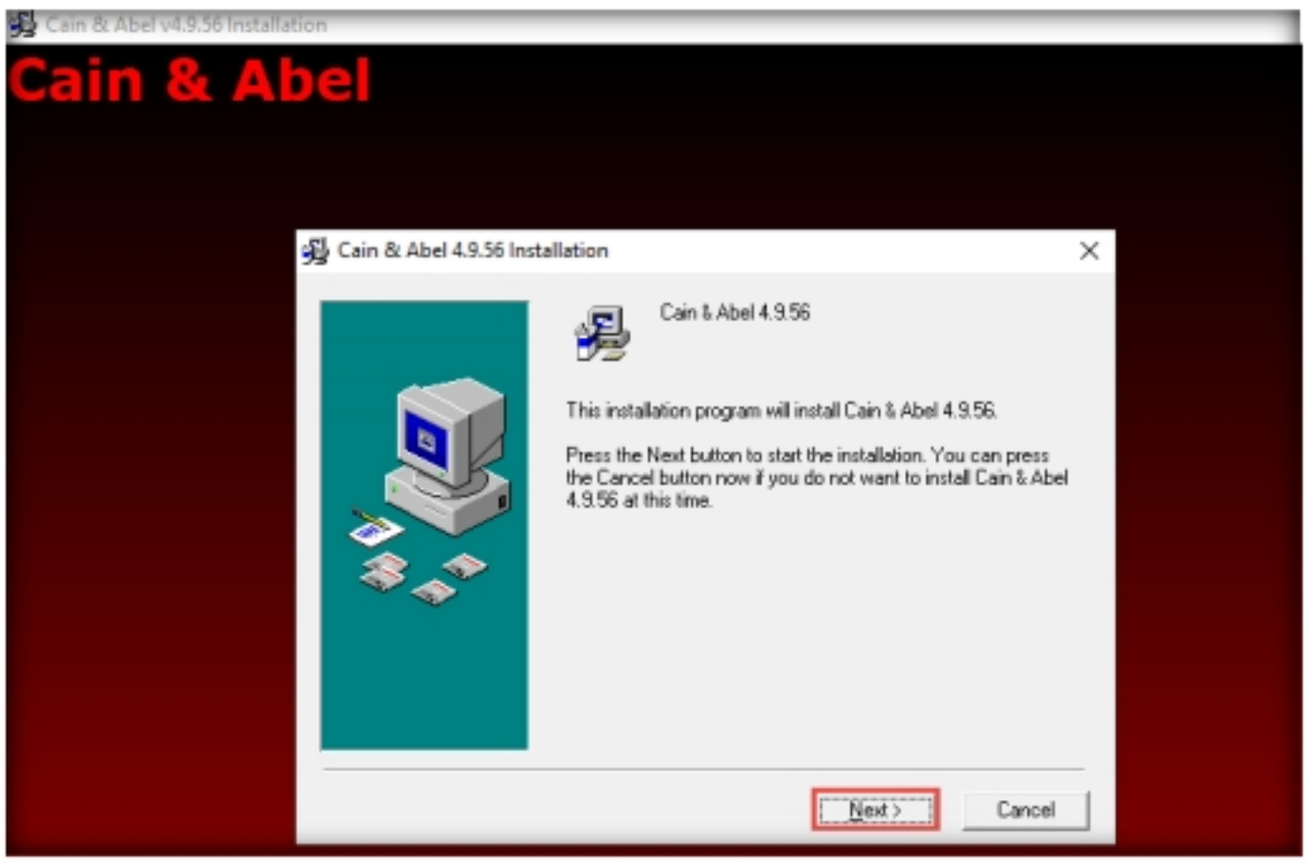


Figure 1.4.1: Cain & Abel installation

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.

5. Follow the wizard-driven installation steps to install Cain & Abel.
6. After completing the installation, the **Installation Completed!** message appears; click **Finish**.

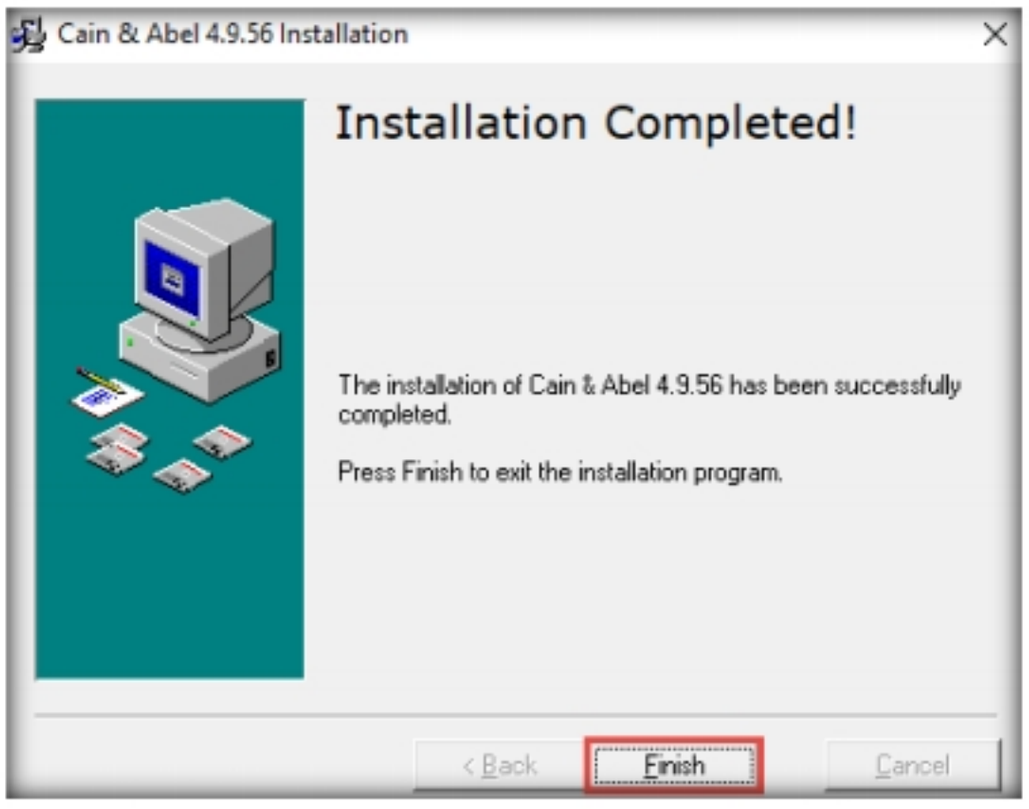


Figure 1.4.2: Cain & Abel installation complete message

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.

7. The **WinPcap Installation** pop-up appears; click **Don't install**, as you already installed it during the lab setup.

Figure 1.4.3: WinPcap Installation pop-up

8. Now, double-click the **Cain** shortcut on **Desktop** to launch **Cain & Abel**.
9. The **Cain & Abel** main window appears, as shown in the screenshot.

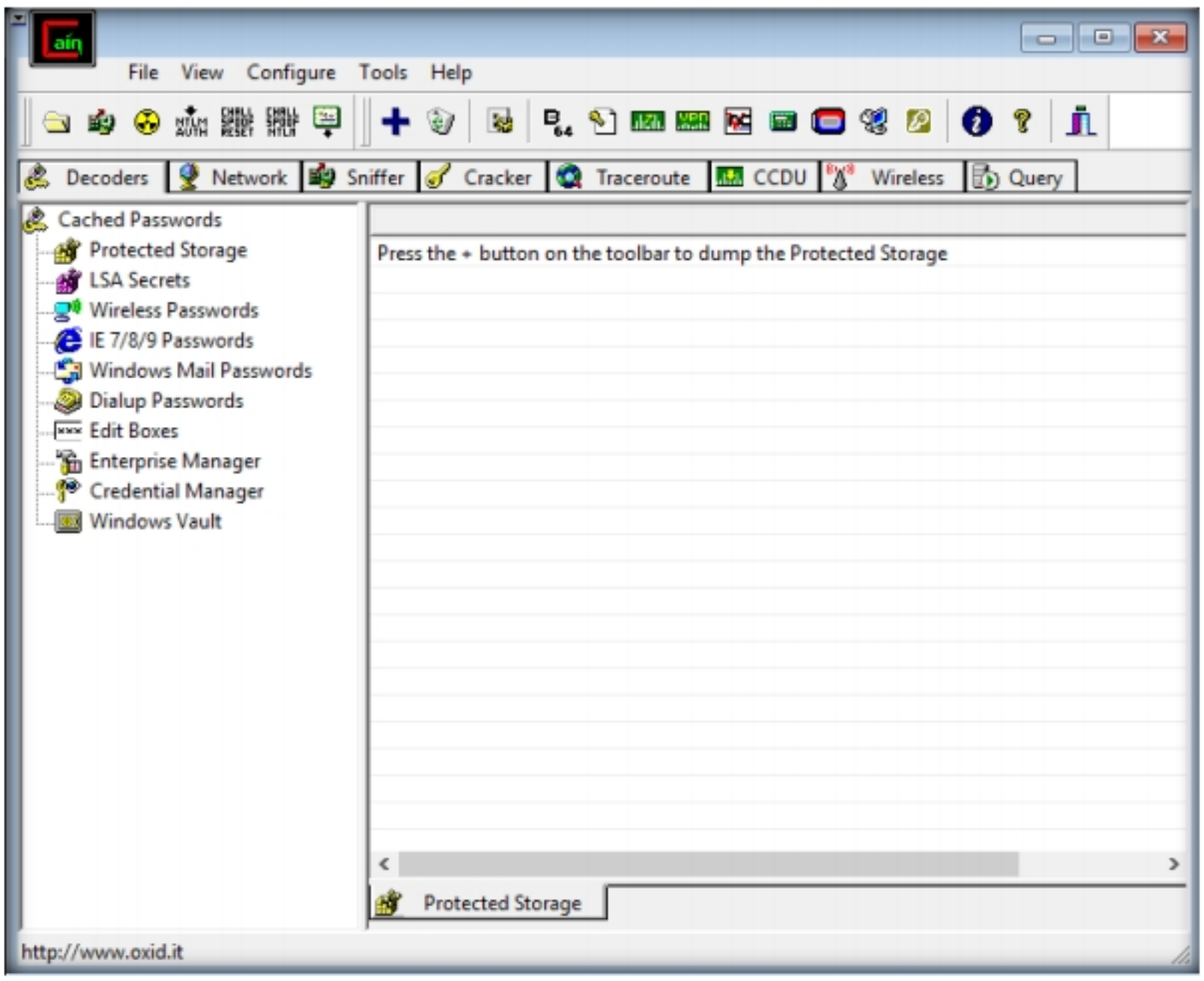


Figure 1.4.4: Cain & Abel Main Window

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

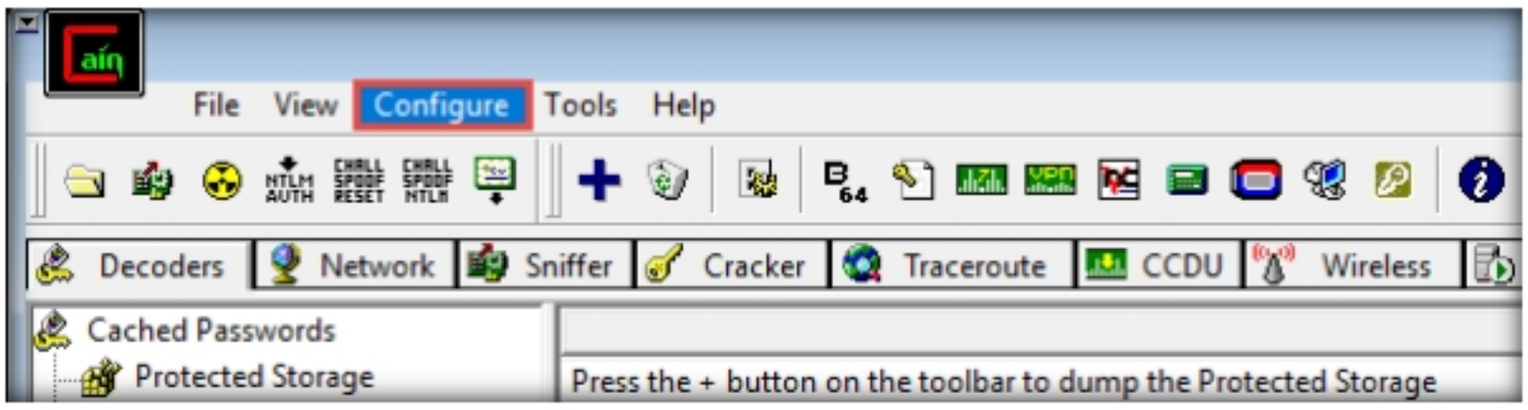


Figure 1.4.5: Cain & Abel Configuration Option

11. 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**.

Note: The adapter might differ in your lab environment.

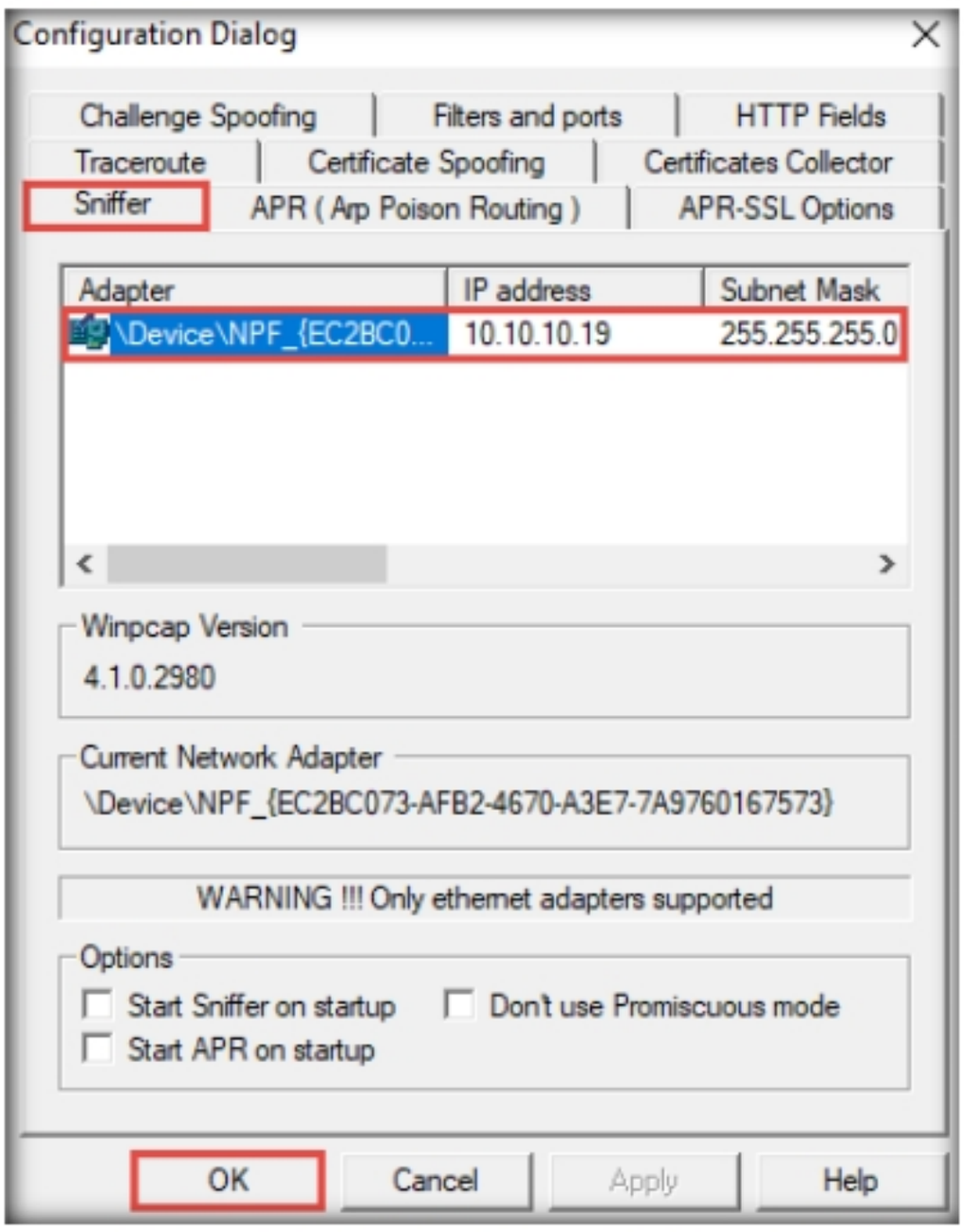


Figure 1.4.6: Cain & Abel Configuration Dialog Window

12. Click the **Start/Stop Sniffer** icon ( ) on the toolbar to begin sniffing.

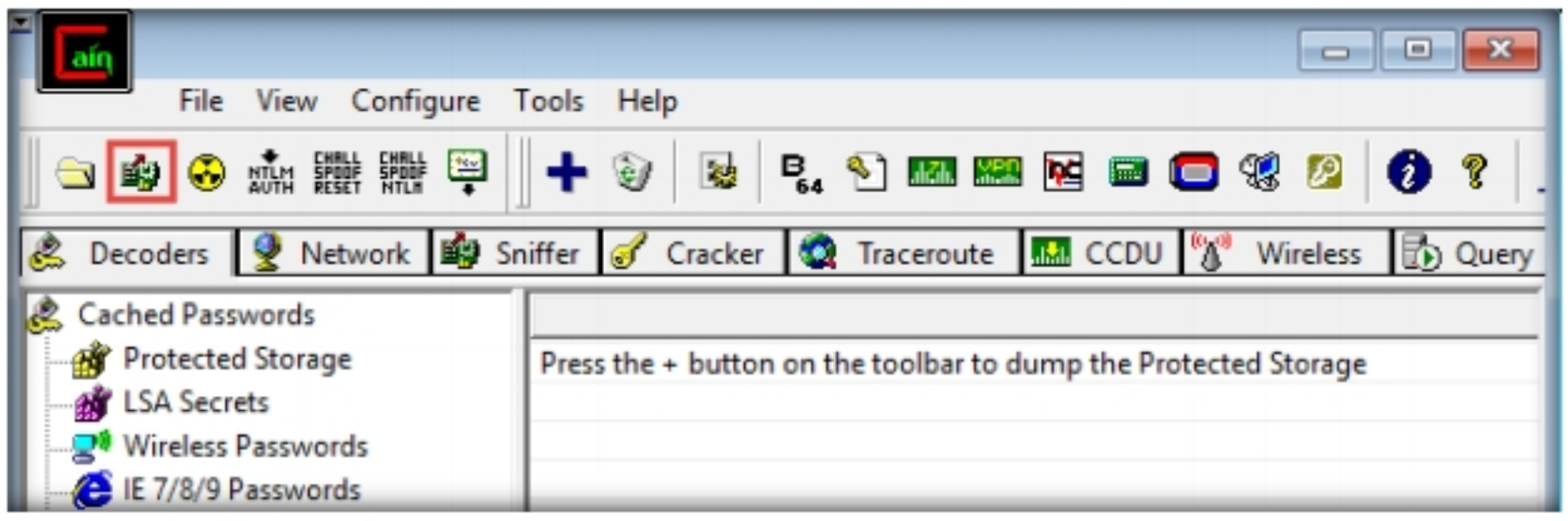


Figure 1.4.7: Starting a sniffer

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

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

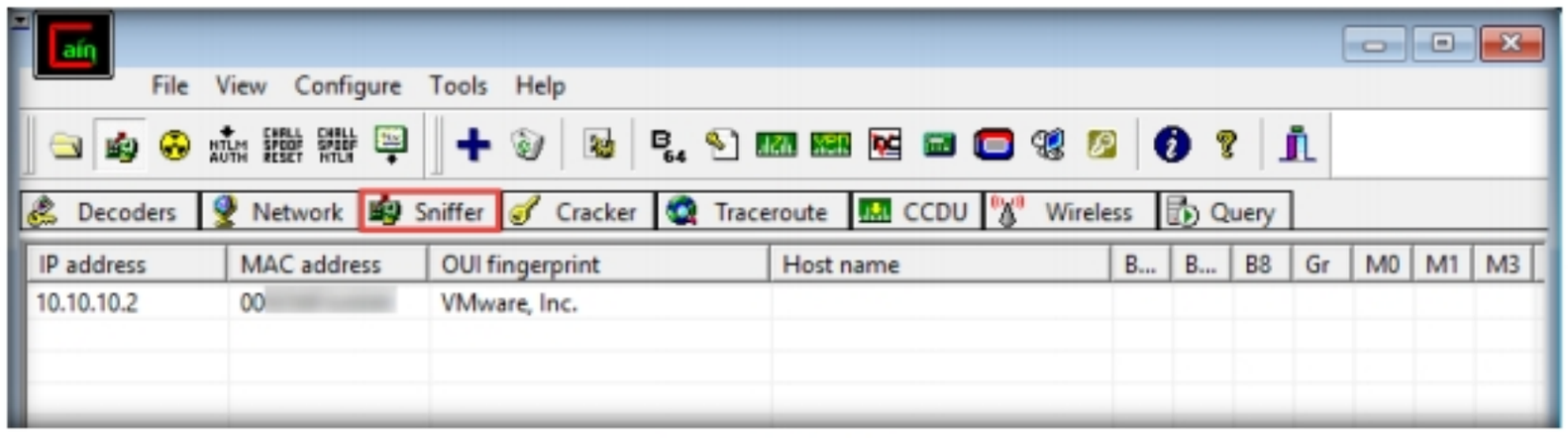


Figure 1.4.8: Sniffer tab

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

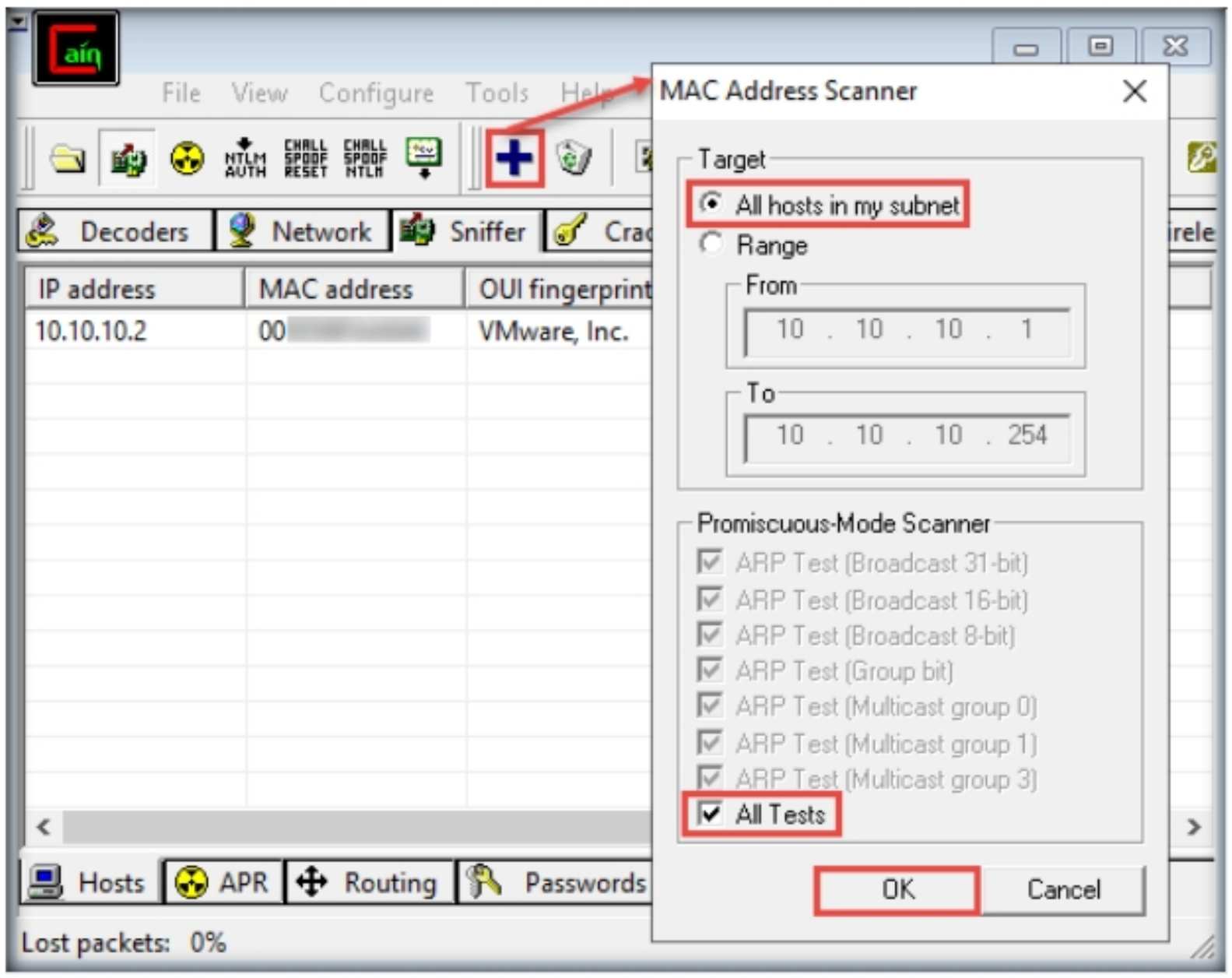


Figure 1.4.9: Cain & Abel: MAC Address Scanner Window

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

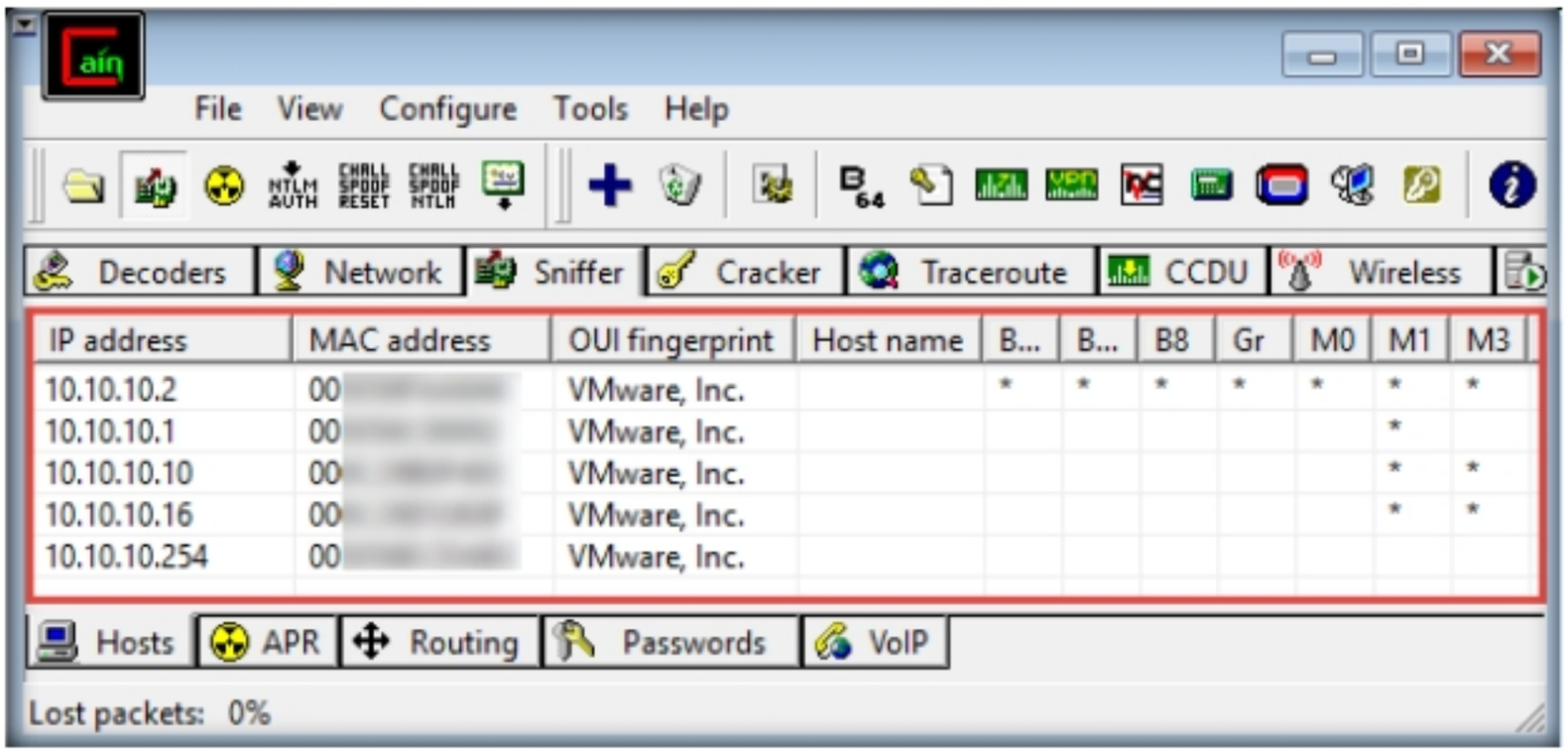


Figure 1.4.10: Cain & Abel: MAC Address Scanned

TASK 4.2

Perform ARP Poisoning

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

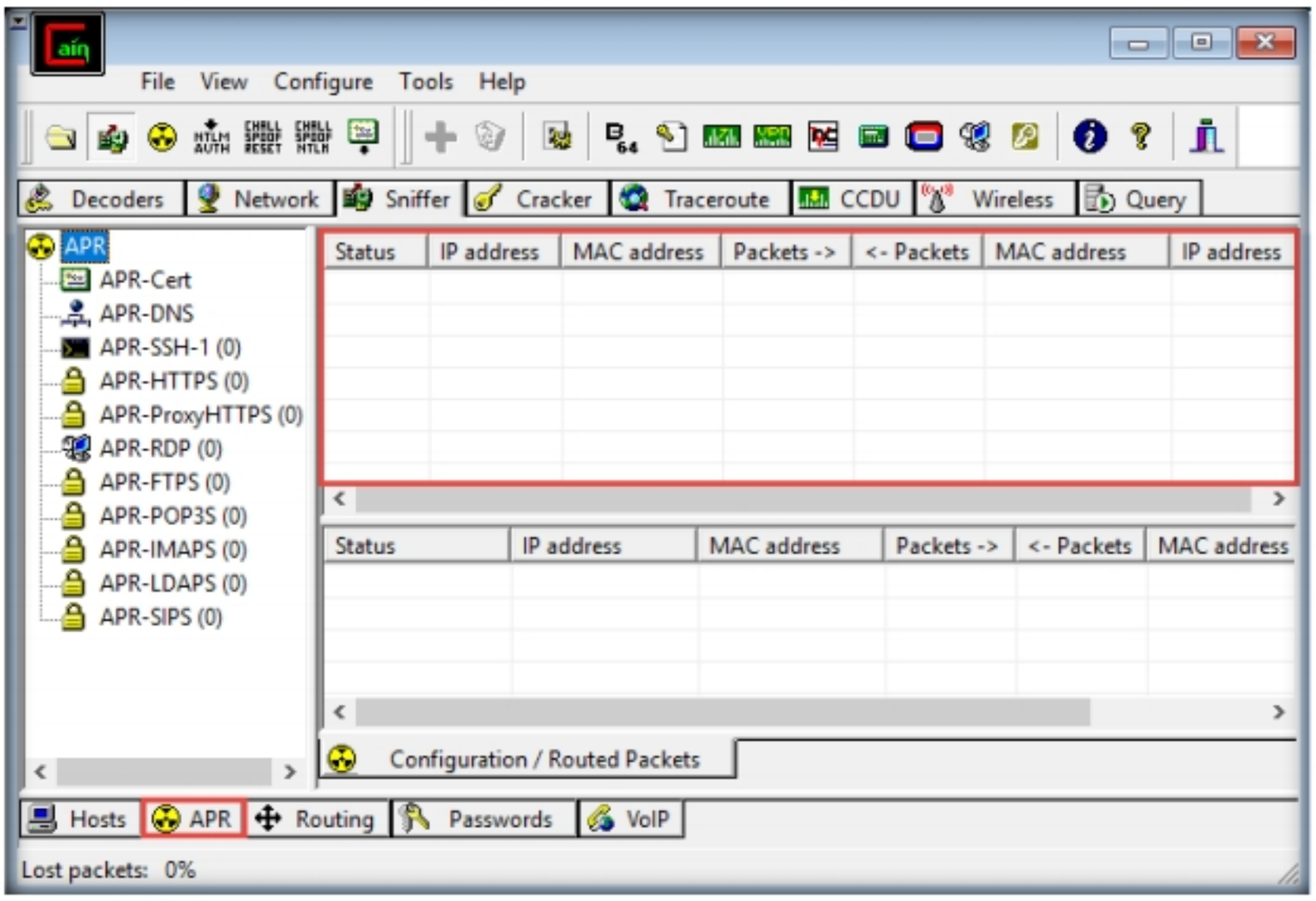


Figure 1.4.11: Cain & Abel ARP Tab

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

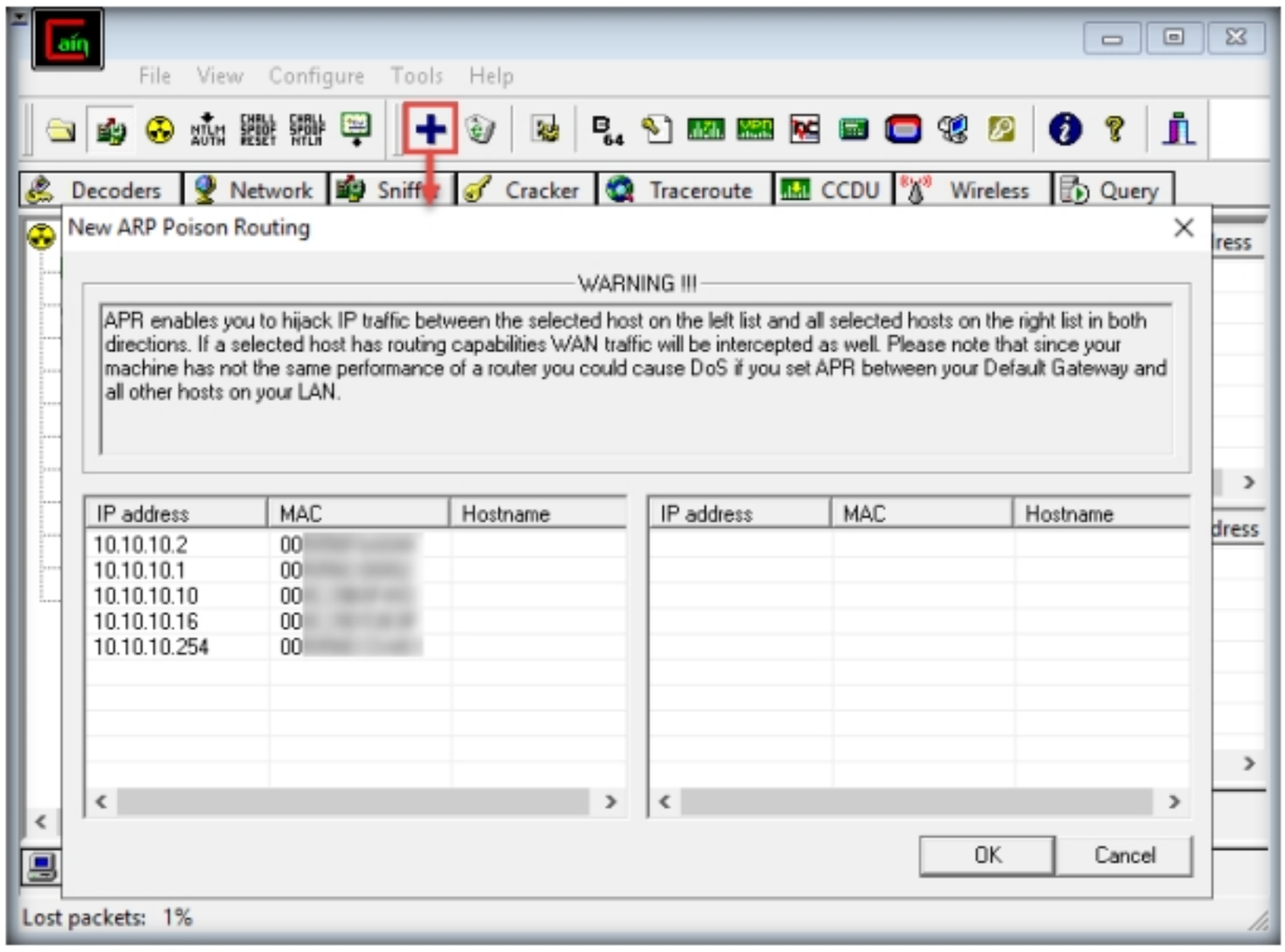


Figure 1.4.12: New ARP Poison Routing window

22. To monitor the traffic between two systems (here, **Windows 10** and **Windows Server 2016**), click to select **10.10.10.10** (**Windows 10**) from the left-hand pane and **10.10.10.16** (**Windows Server 2016**) from the right-hand pane; click **OK**.

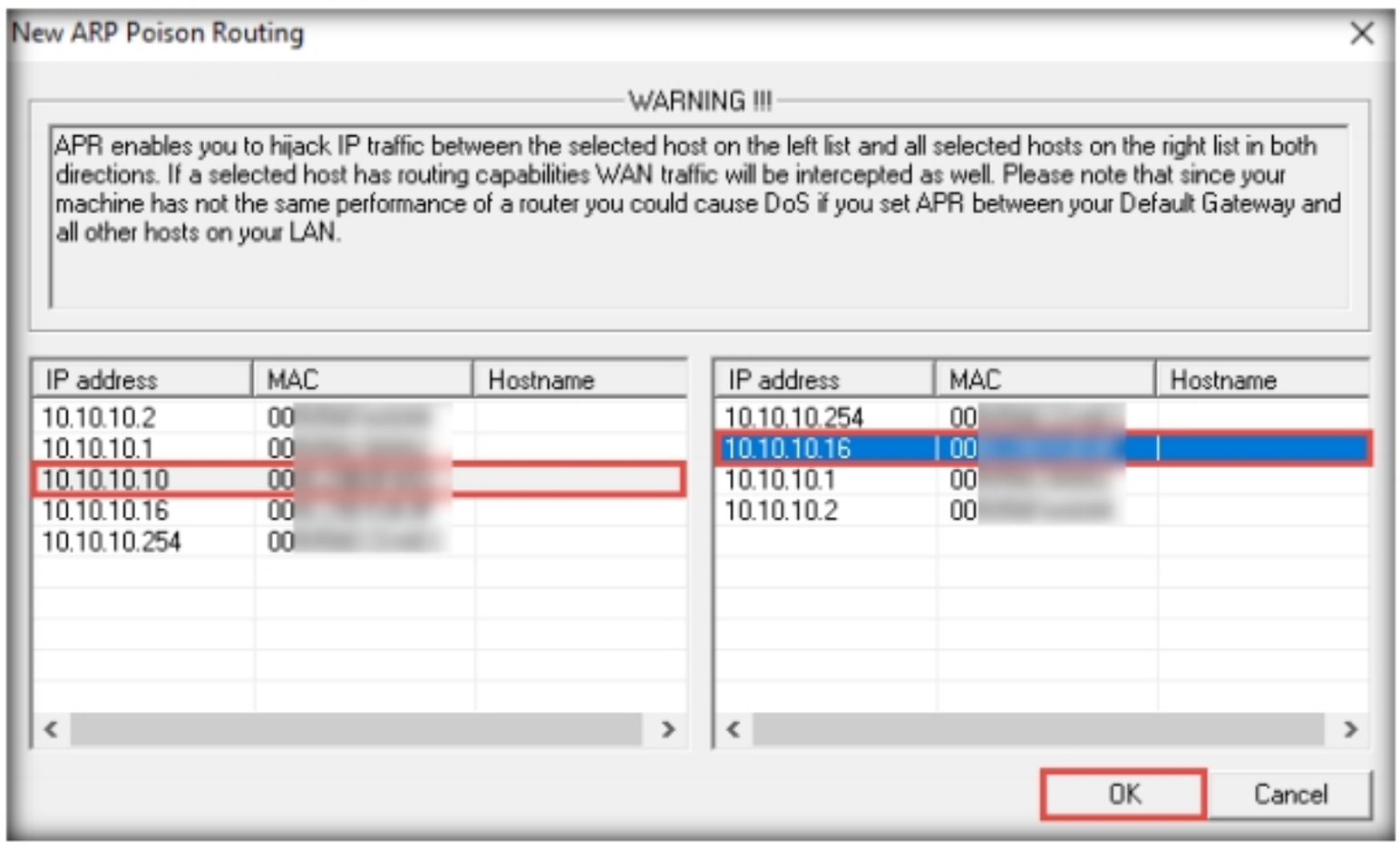


Figure 1.4.13: Monitoring traffic between two computers

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

24. Click on the **Start/Stop APR** icon ( ) to start capturing ARP packets.

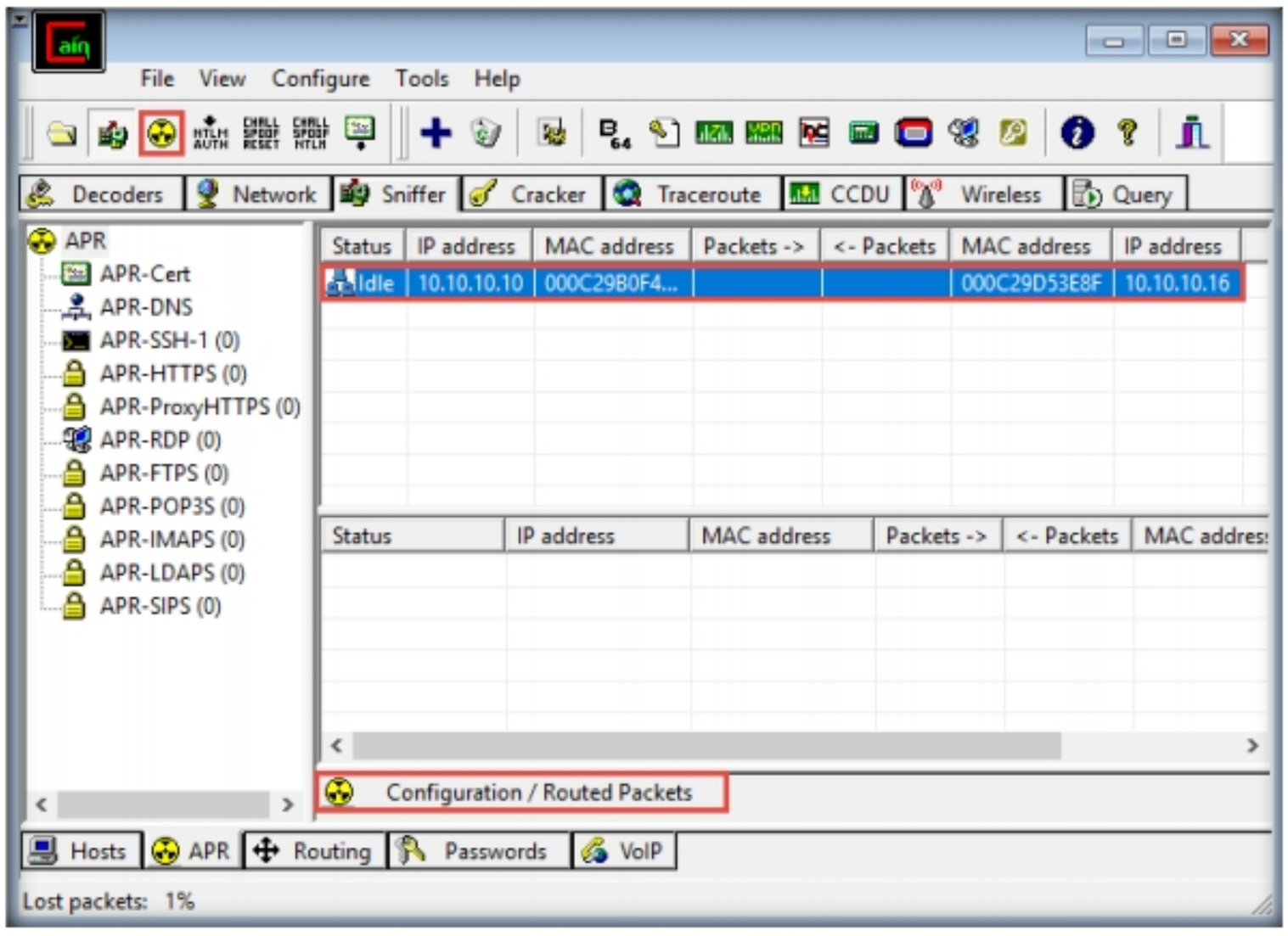


Figure 1.4.14: Cain & Abel ARP Poisoning

25. Now, switch to the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
26. Right-click on the **Start** icon in the bottom-left corner of **Desktop** to launch **Command Prompt**.
27. The **Command Prompt** window appears; type **ftp 10.10.10.10** (the IP address of **Windows 10**) and press **Enter**.
28. When prompted for a **User**, type "**Jason**" and press **Enter**; for a **Password**, type "**qwerty**" and press **Enter**.

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

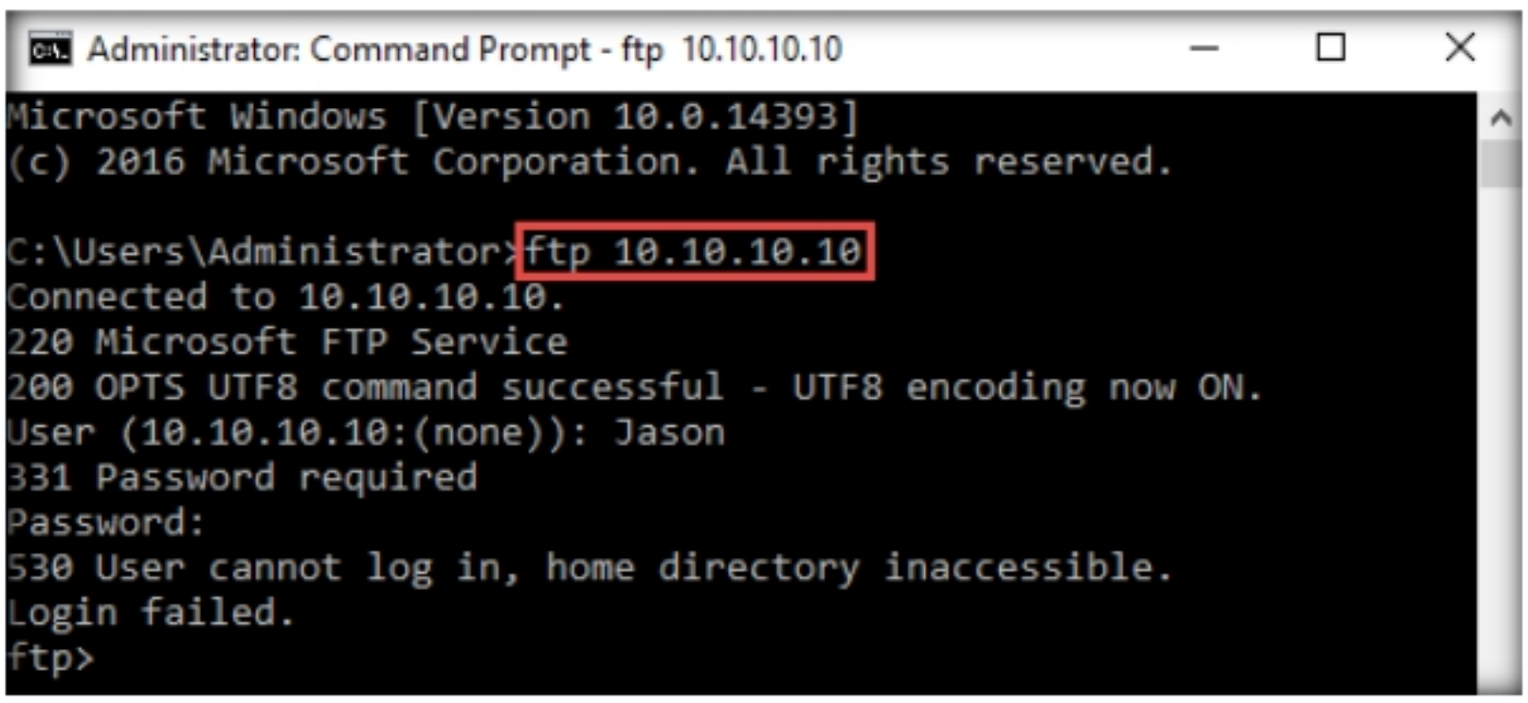


Figure 1.4.15: Start ftp://10.10.10.10

TASK 4.3

Analyze the Result

29. Switch back to the **Windows Server 2019** virtual machine; observe that the tool lists packet exchange.

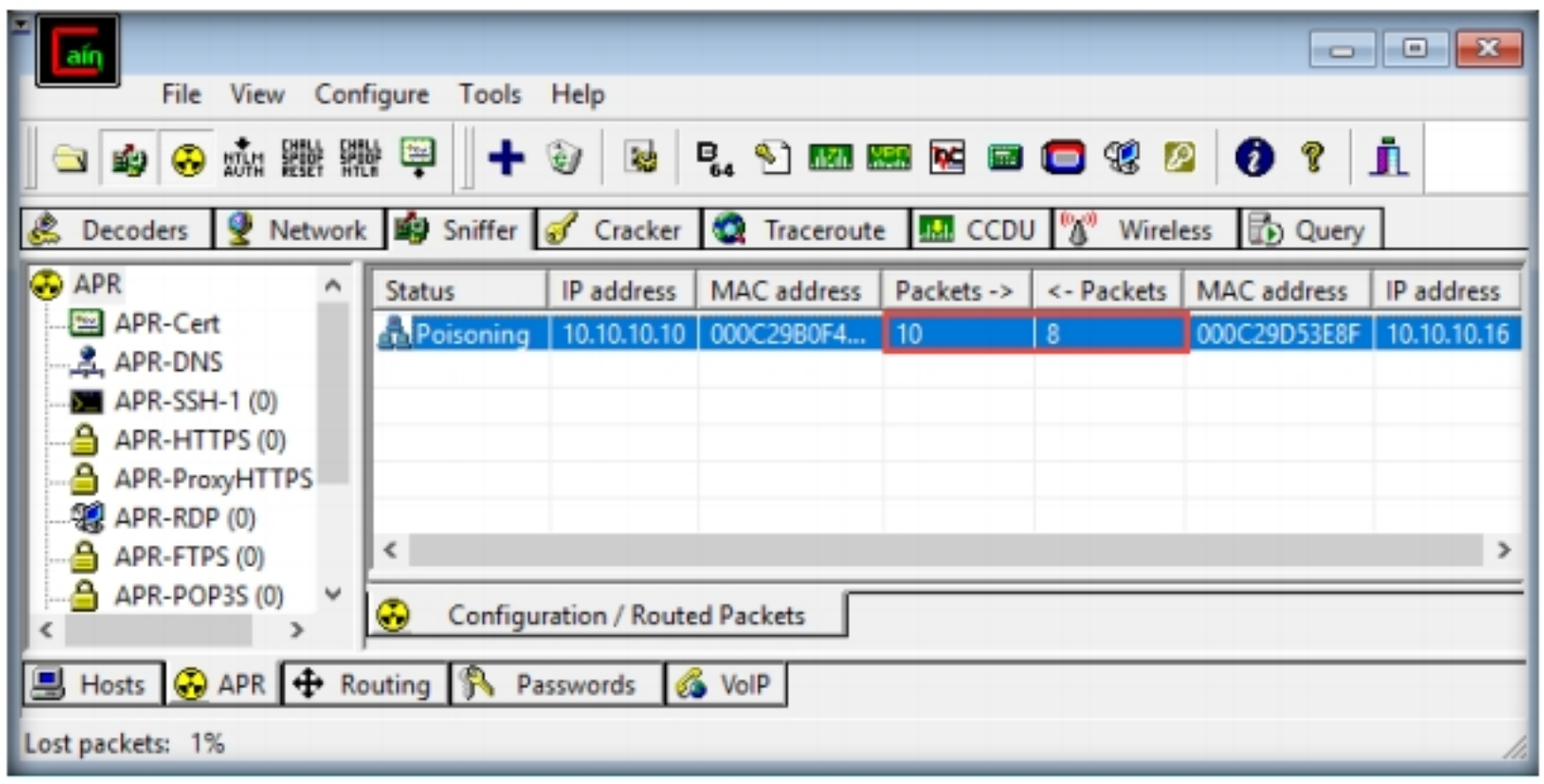


Figure 1.4.16: Sniffer window with more packets exchanged

30. Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the sniffed password for **ftp 10.10.10.10**, as shown in the screenshot.

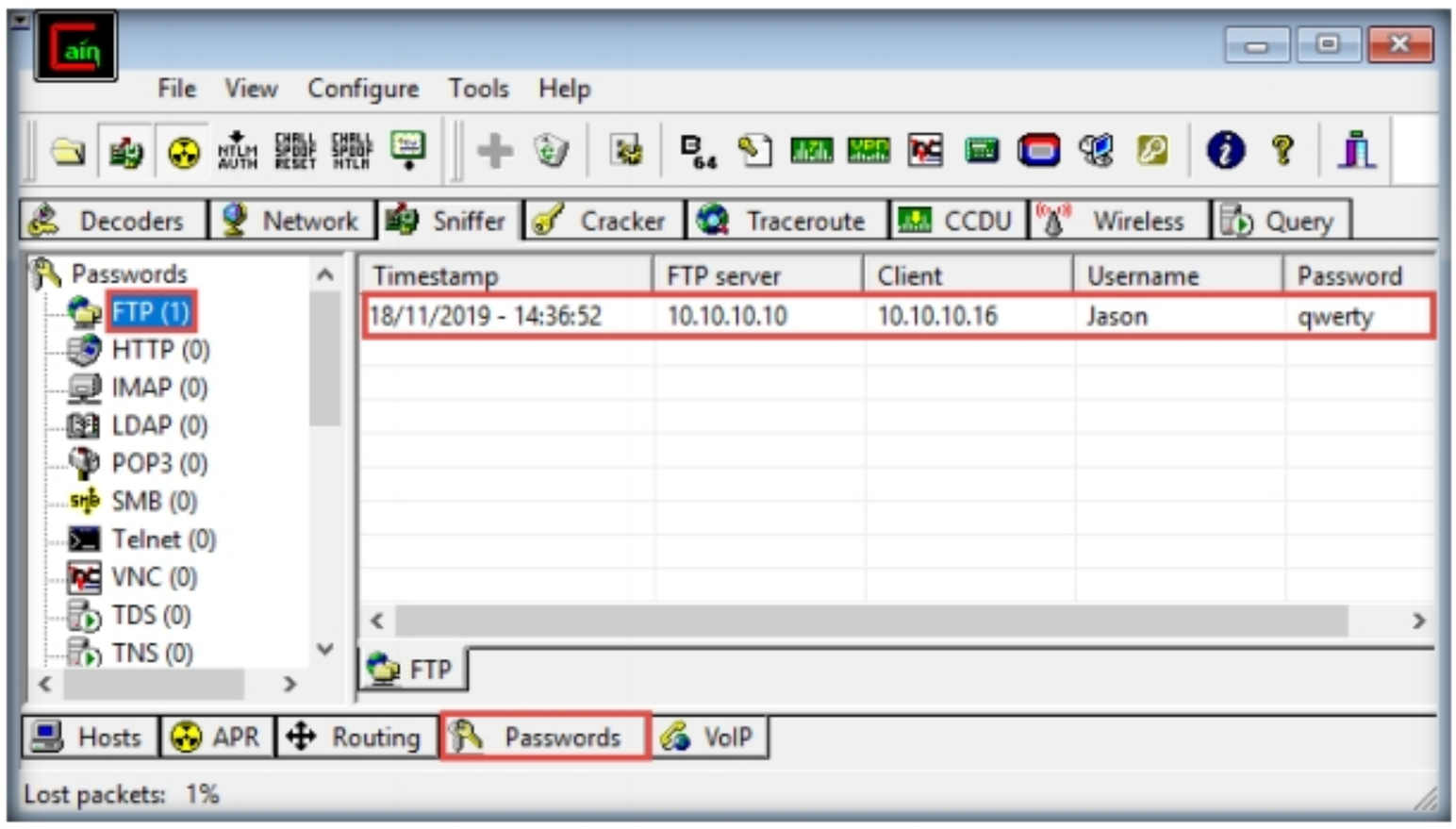


Figure 1.4.17: Passwords displayed in plain text

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

31. This concludes the demonstration of how to perform an MITM attack using Cain & Abel.
32. Close all open windows and document all the acquired information.
33. Turn off the **Windows Server 2019** and **Windows Server 2016** virtual machines.

Spoof a MAC Address using TMAC and SMAC

TASK 5

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.

TASK 5.1

Install TMAC

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC)** and double-click **TMACv6.0.7_Setup.exe**.

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

2. The **Technitium MAC Address Changer** installation window appears; click **Next**.

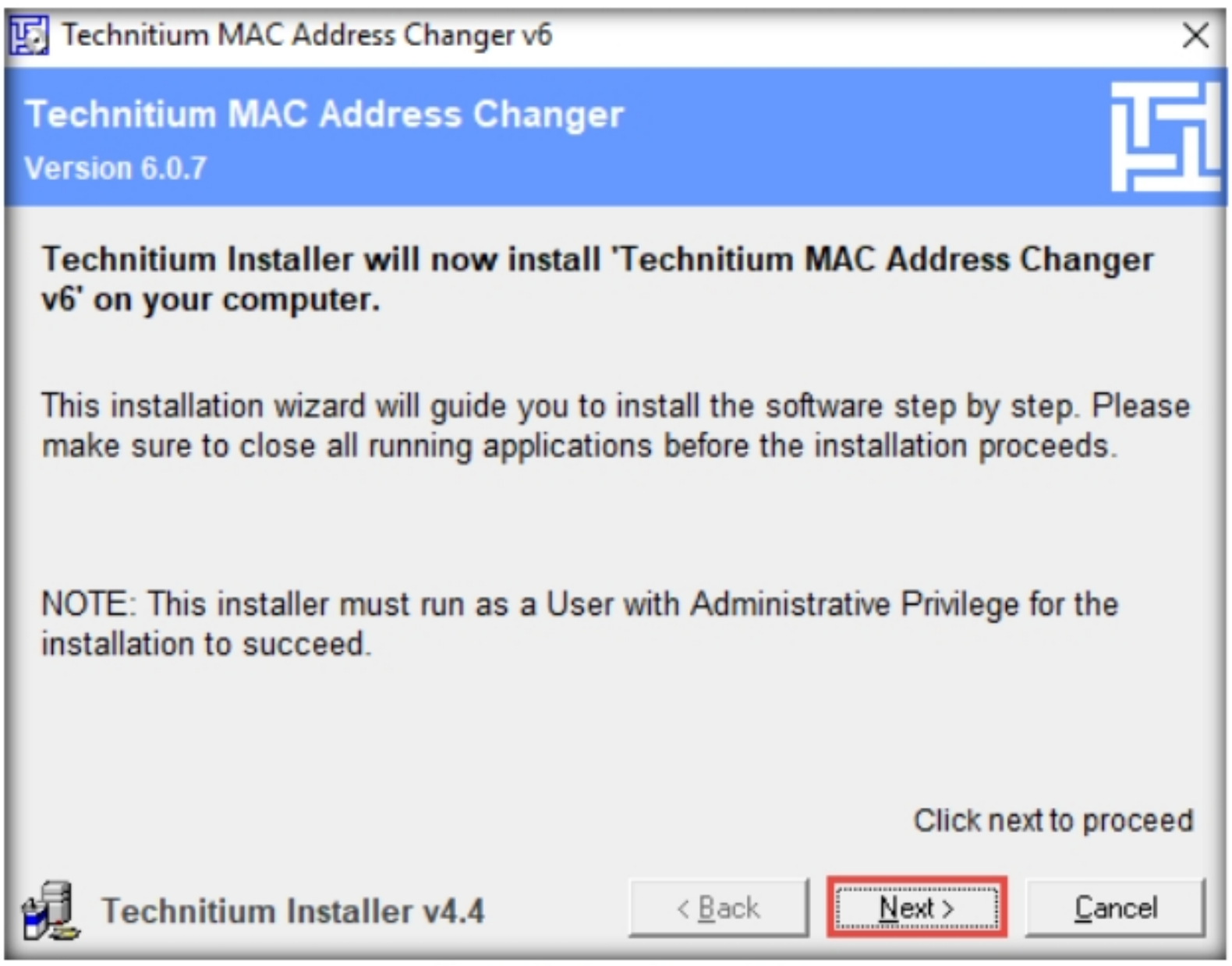


Figure 1.5.1: TMAC installation wizard

3. Follow the wizard-driven installation steps and install TMAC with default settings.
4. After completing the installation, the **Installation Complete** window appears in the wizard; click **Finish**.

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.

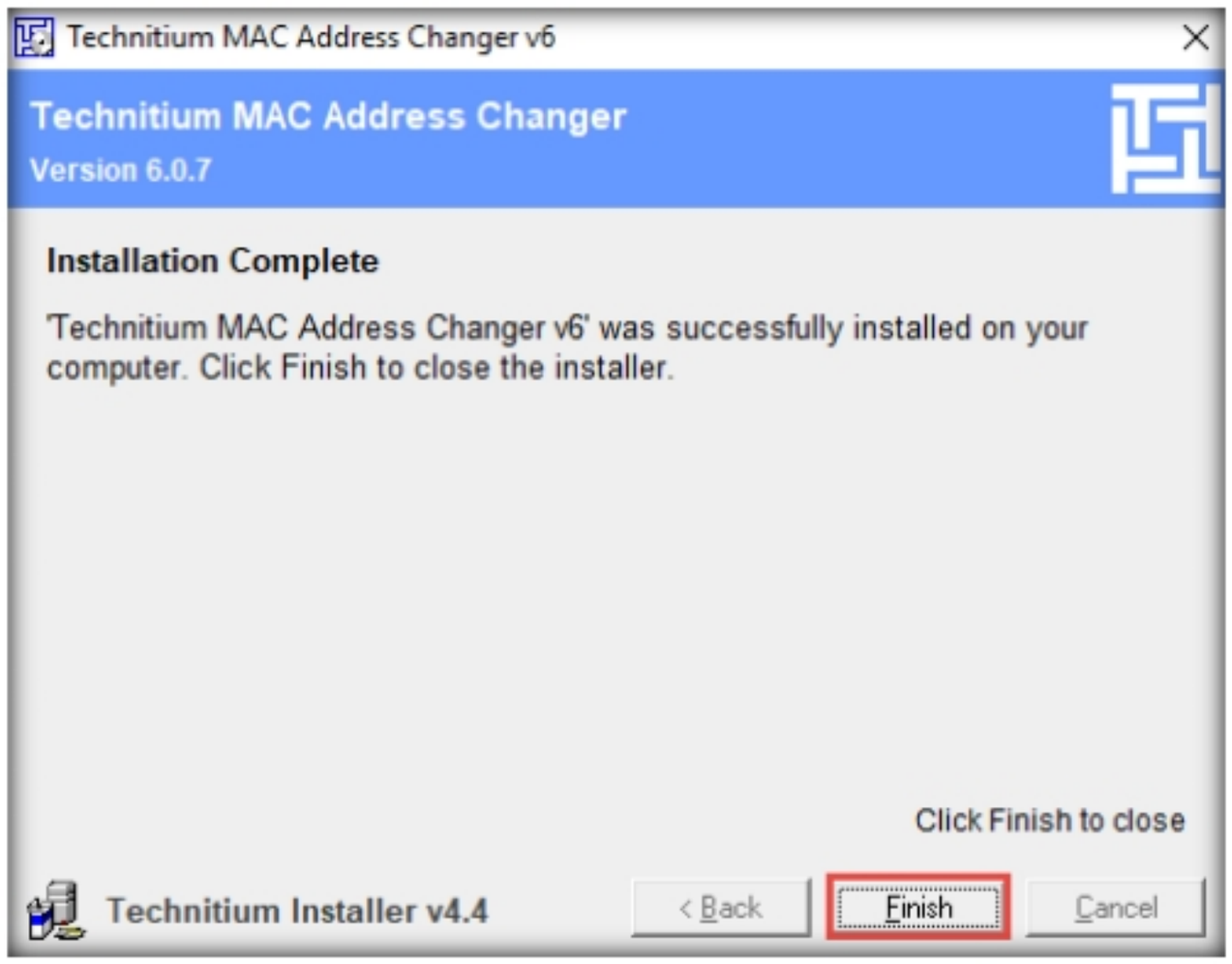


Figure 1.5.2: TMAC installation wizard

5. Double-click the **TMAC** shortcut on **Desktop** to launch the TMAC application.

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

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

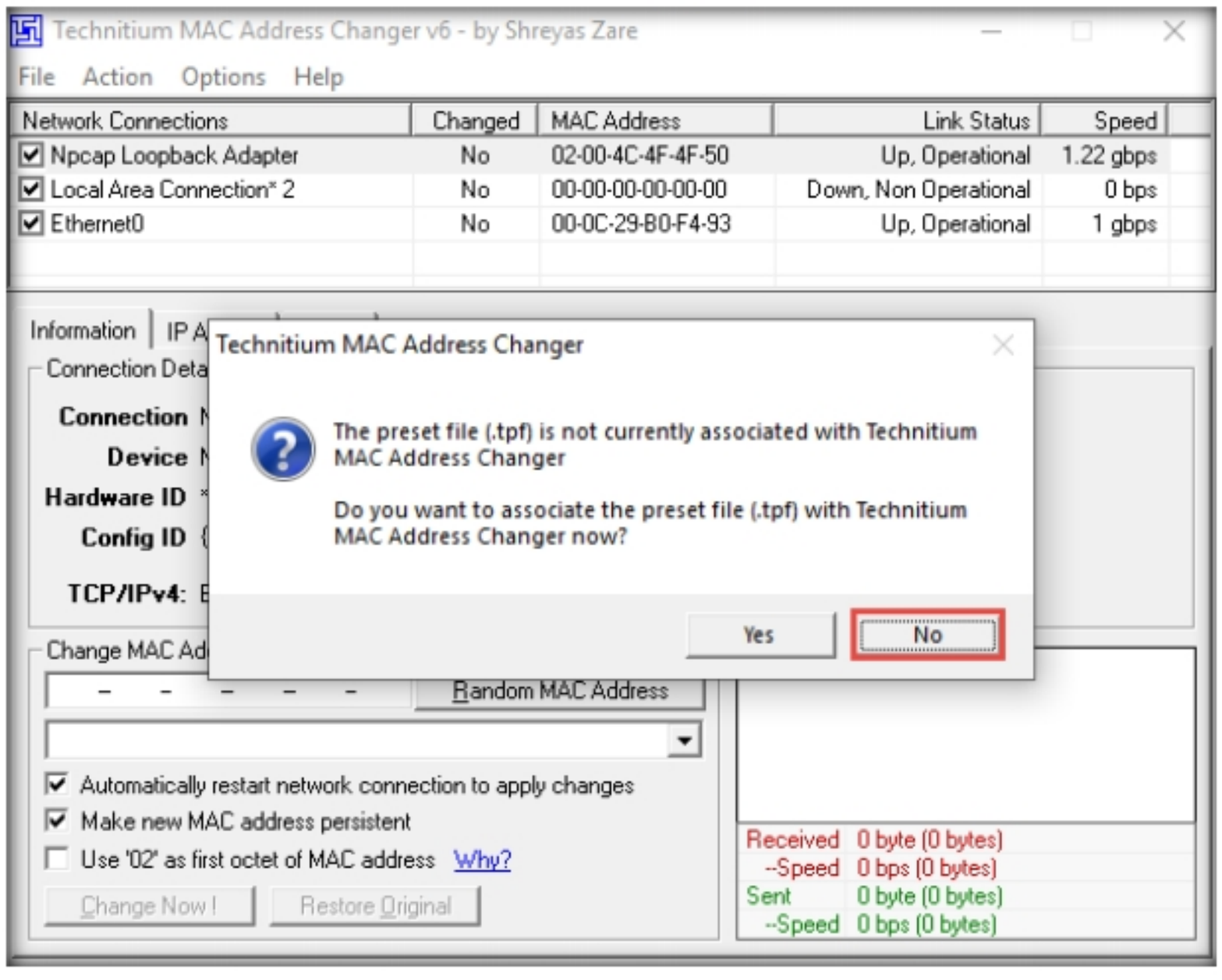


Figure 1.5.3: TMAC main window

7. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet0**).

Note: The network adapter might differ in your lab environment.

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

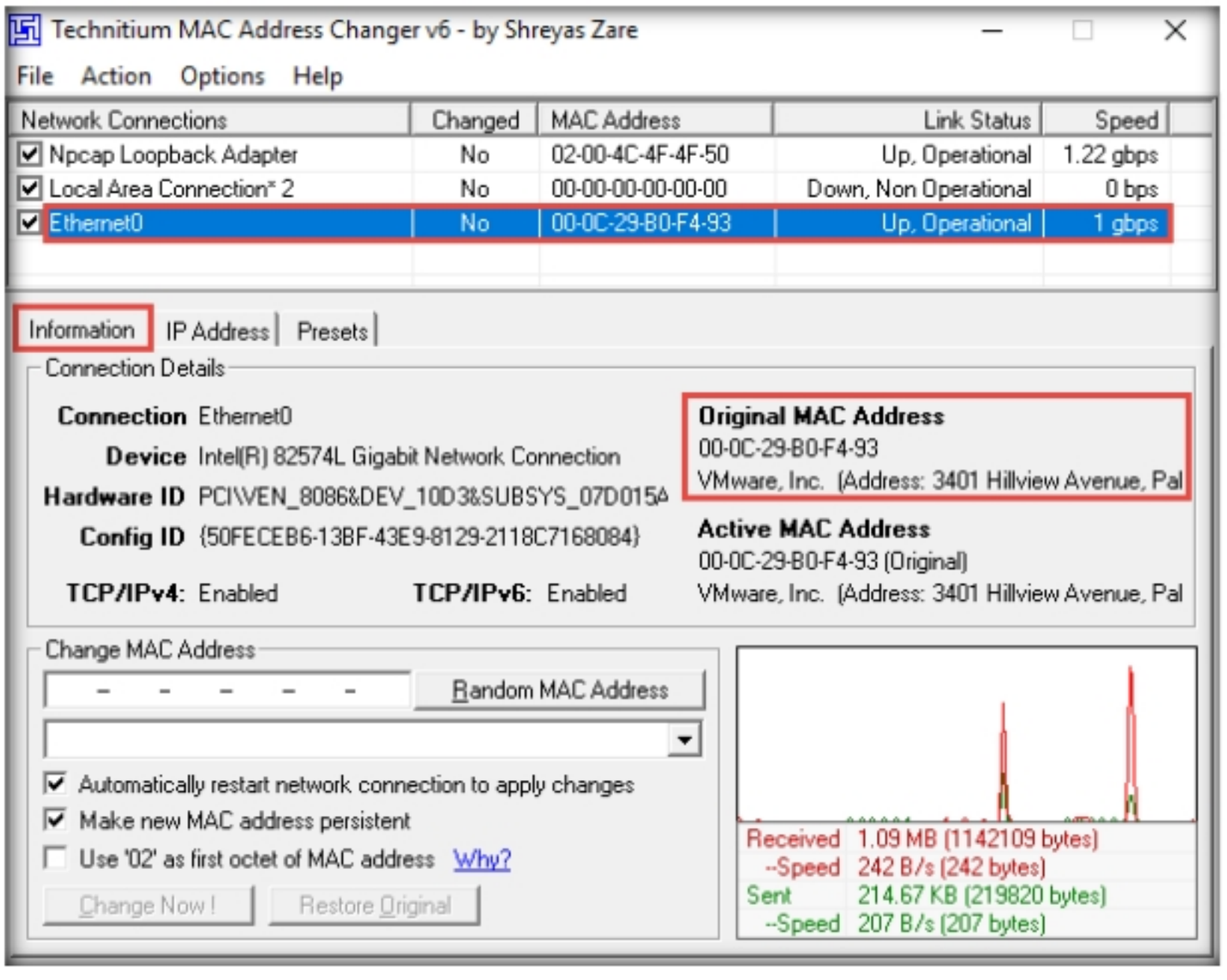


Figure 1.5.4: TMAC main window: Original MAC Address

TASK 5.2

Perform MAC Spoofing Using TMAC

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

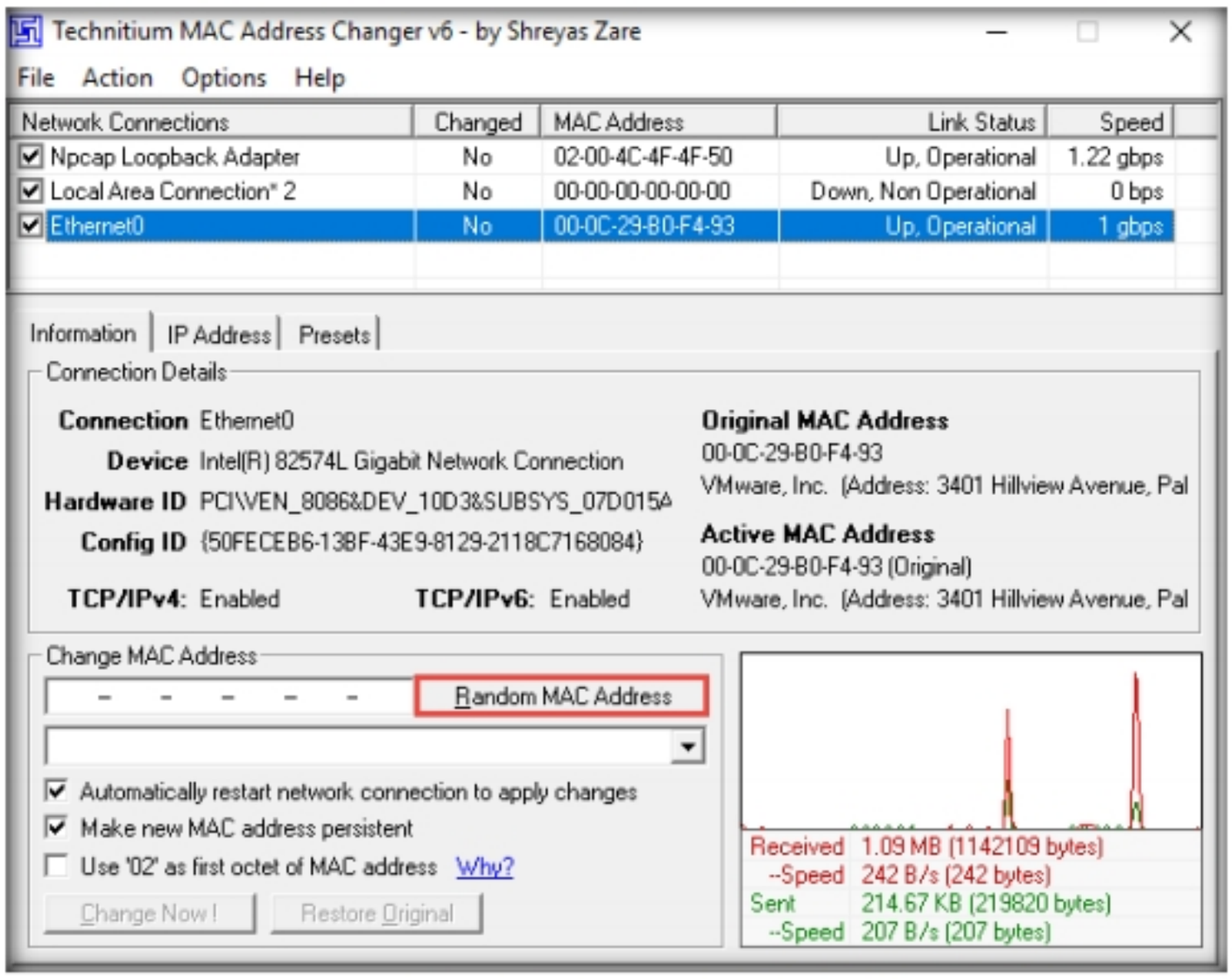


Figure 1.5.5: TMAC main window: Original MAC Address

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

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

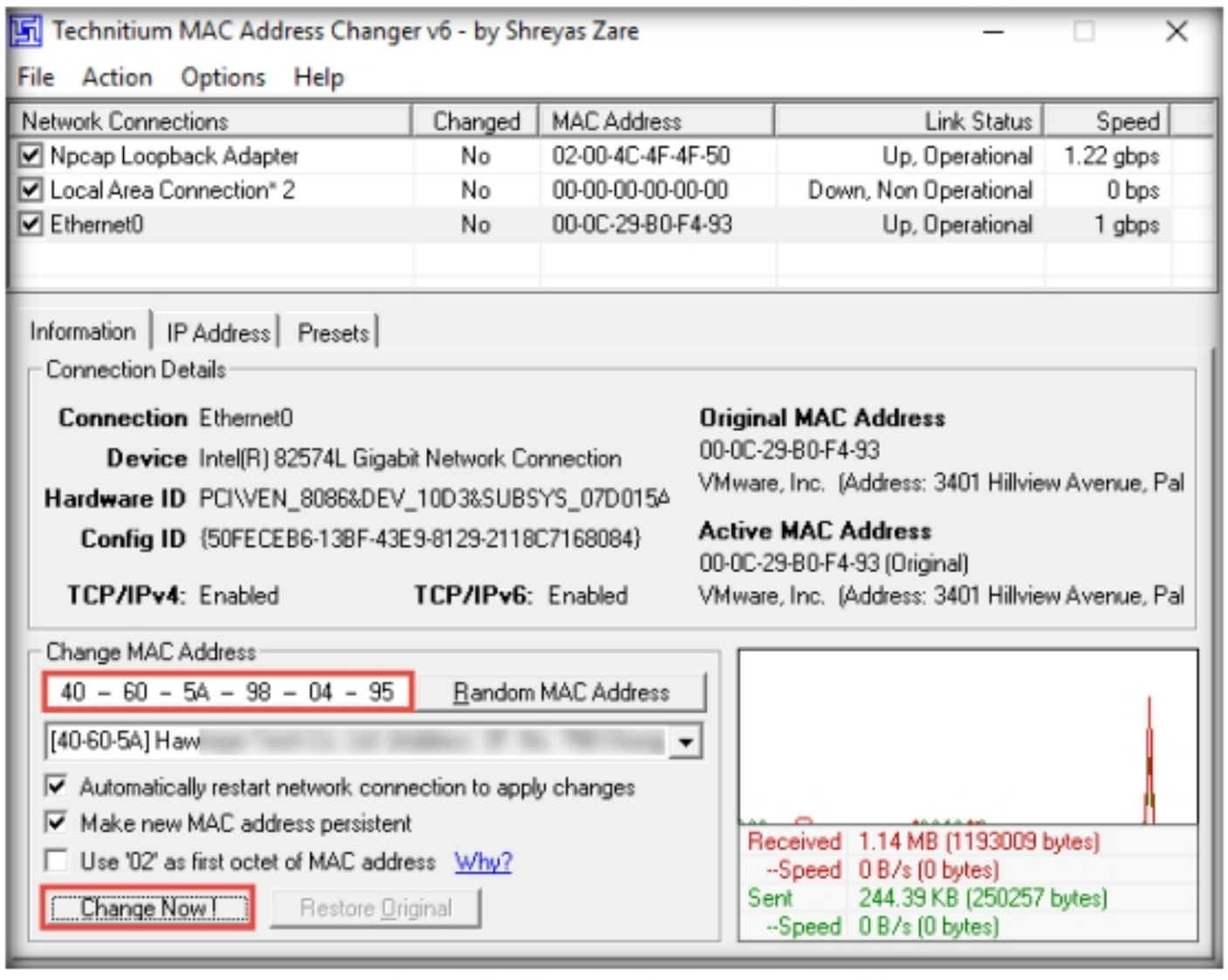


Figure 1.5.6: TMAC main window: Change MAC Address

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

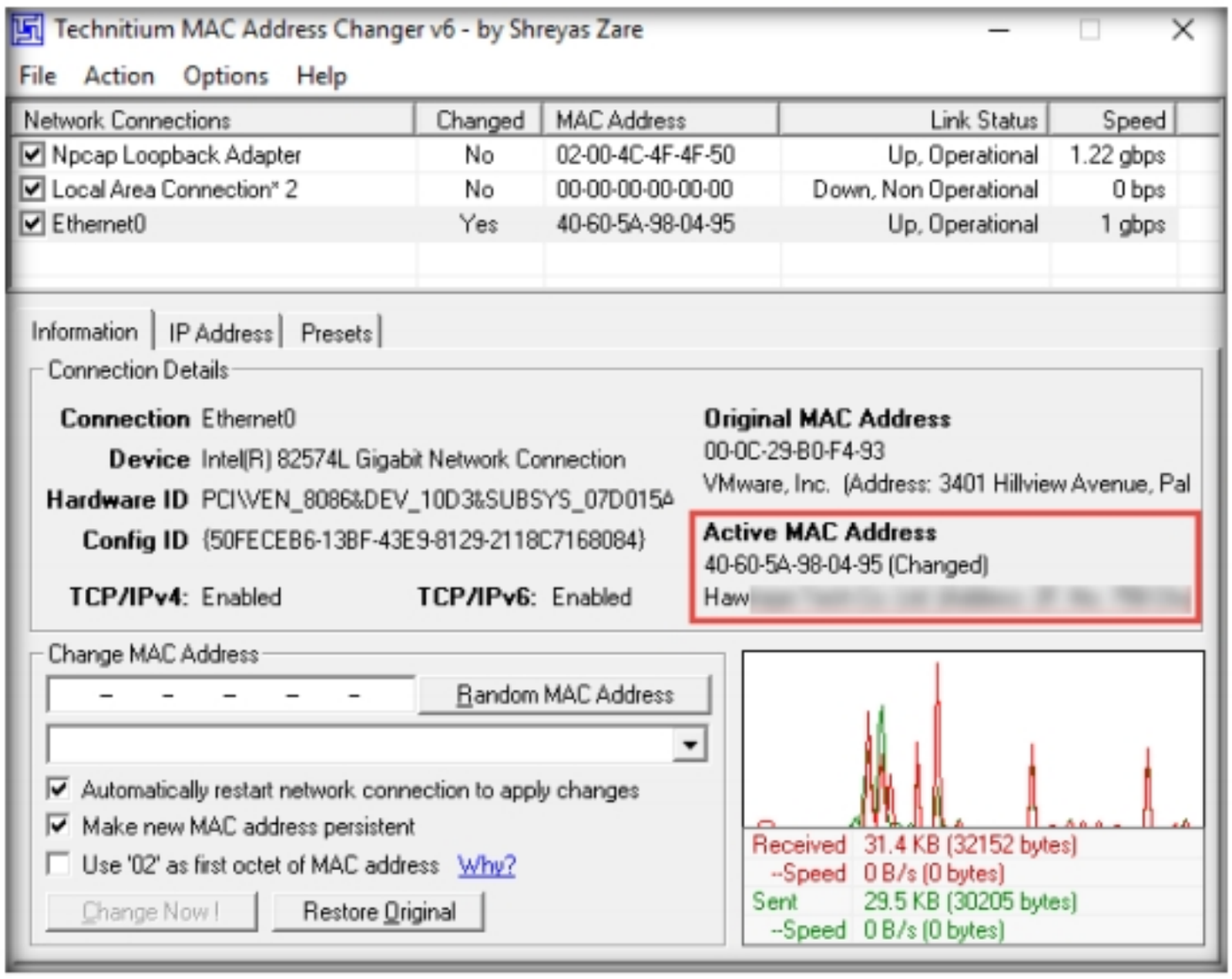


Figure 1.5.7: TMAC main window: Active MAC Address

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

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

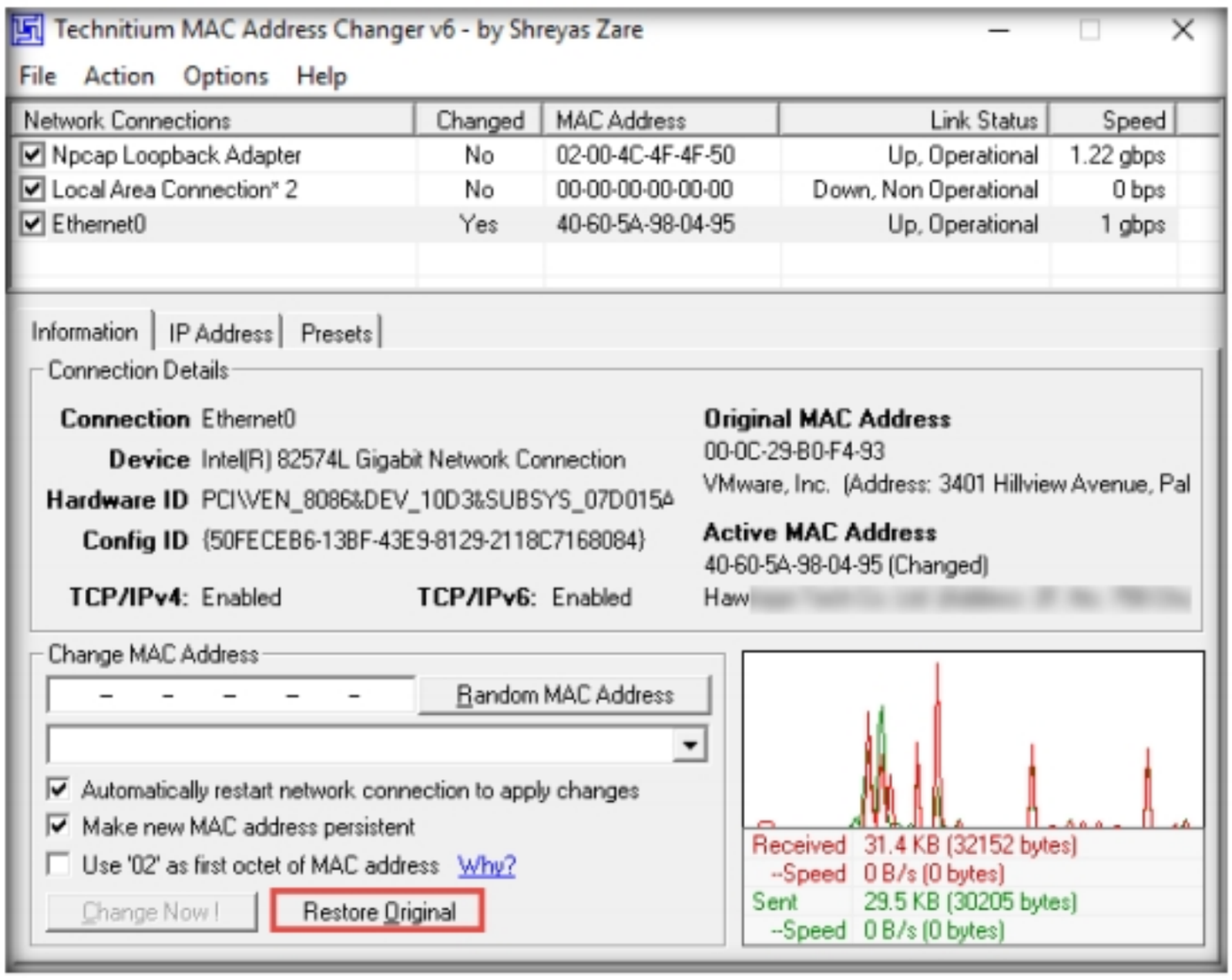


Figure 1.5.8: TMAC main window: Restore MAC Address

TASK 5.3

Install and Configure SMAC

13. Close the **TMAC** main window.
14. Now, we shall perform MAC spoofing using the SMAC tool.
15. Navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC** and double-click **smac27_setup.exe**.

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

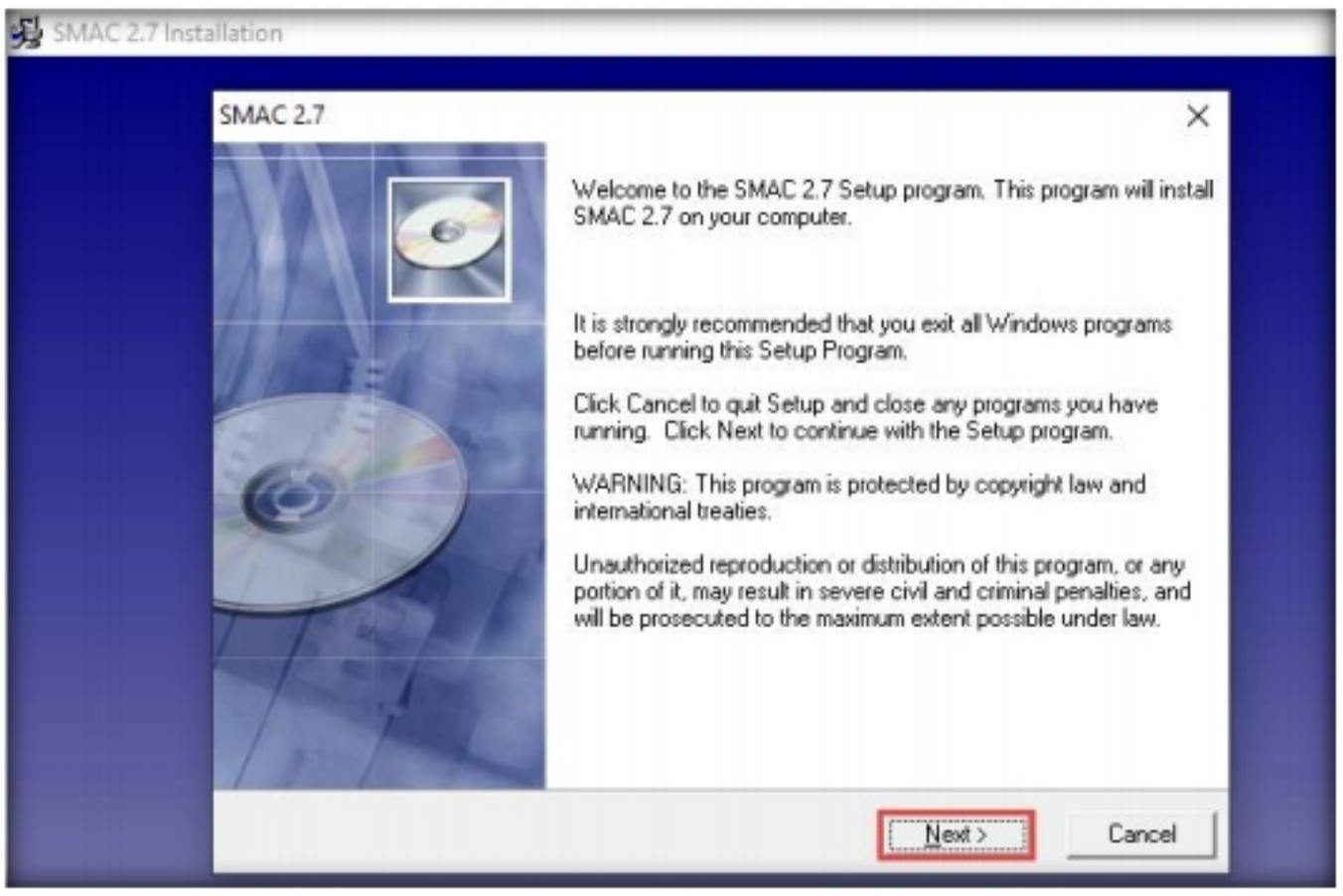


Figure 1.5.9: SMAC installation wizard

16. Follow the wizard-driven installation steps to install SMAC.
17. After the completion of the installation, the **SMAC has been successfully installed** message appears. Ensure that the **Launch SMAC** checkbox is selected; click **Finish**.

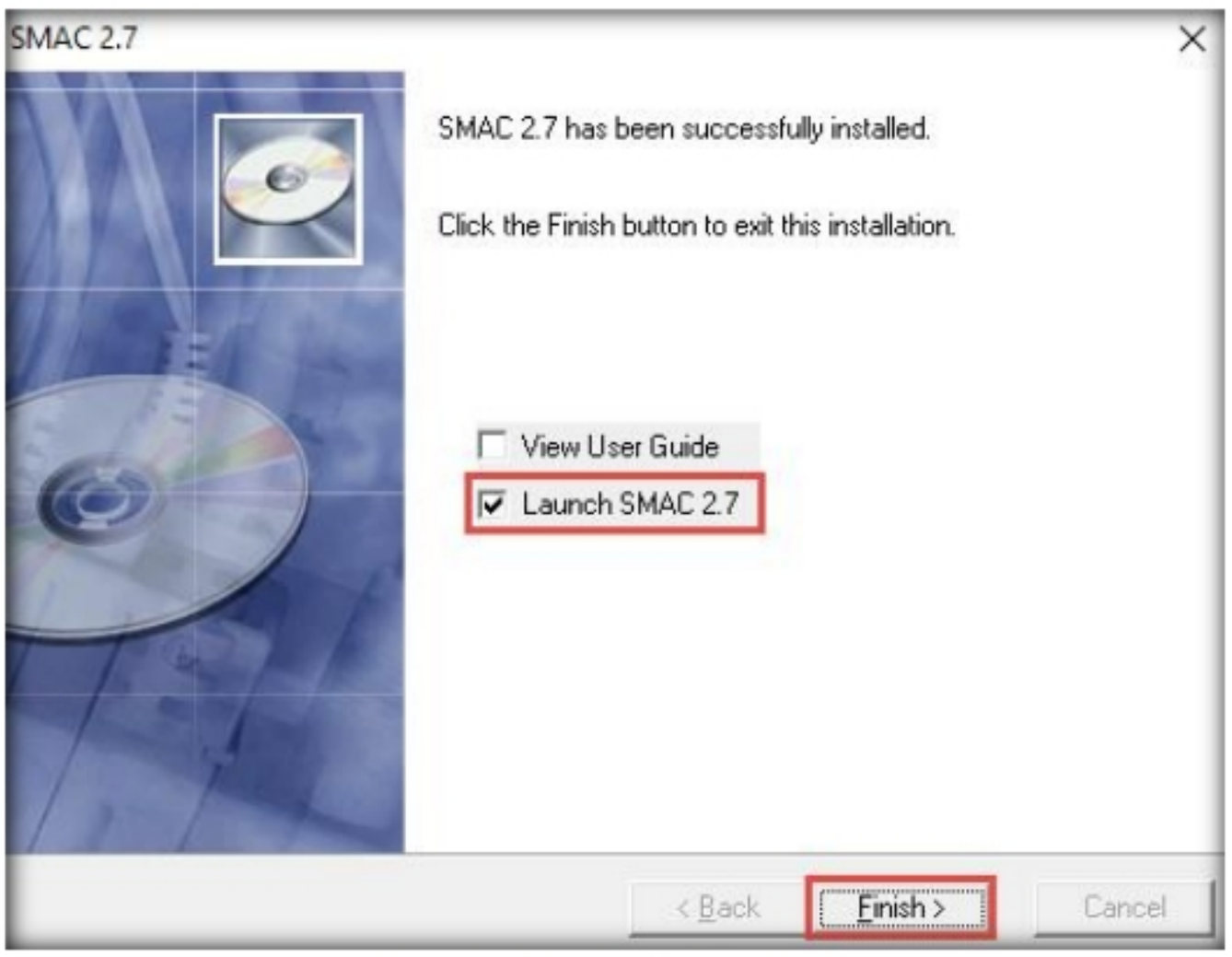


Figure 1.5.10: SMAC installation wizard

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

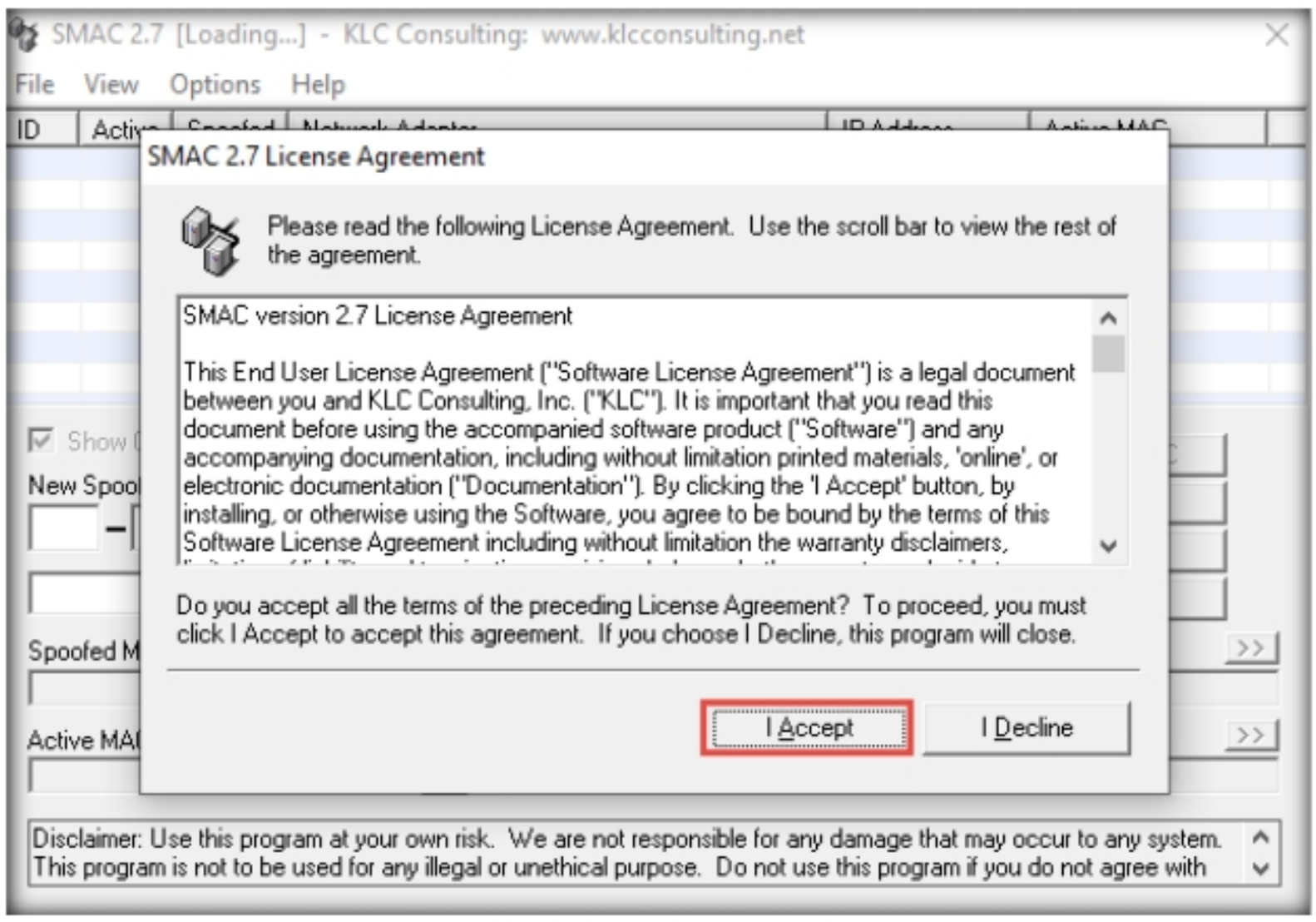


Figure 1.5.11: SMAC License Agreement window

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

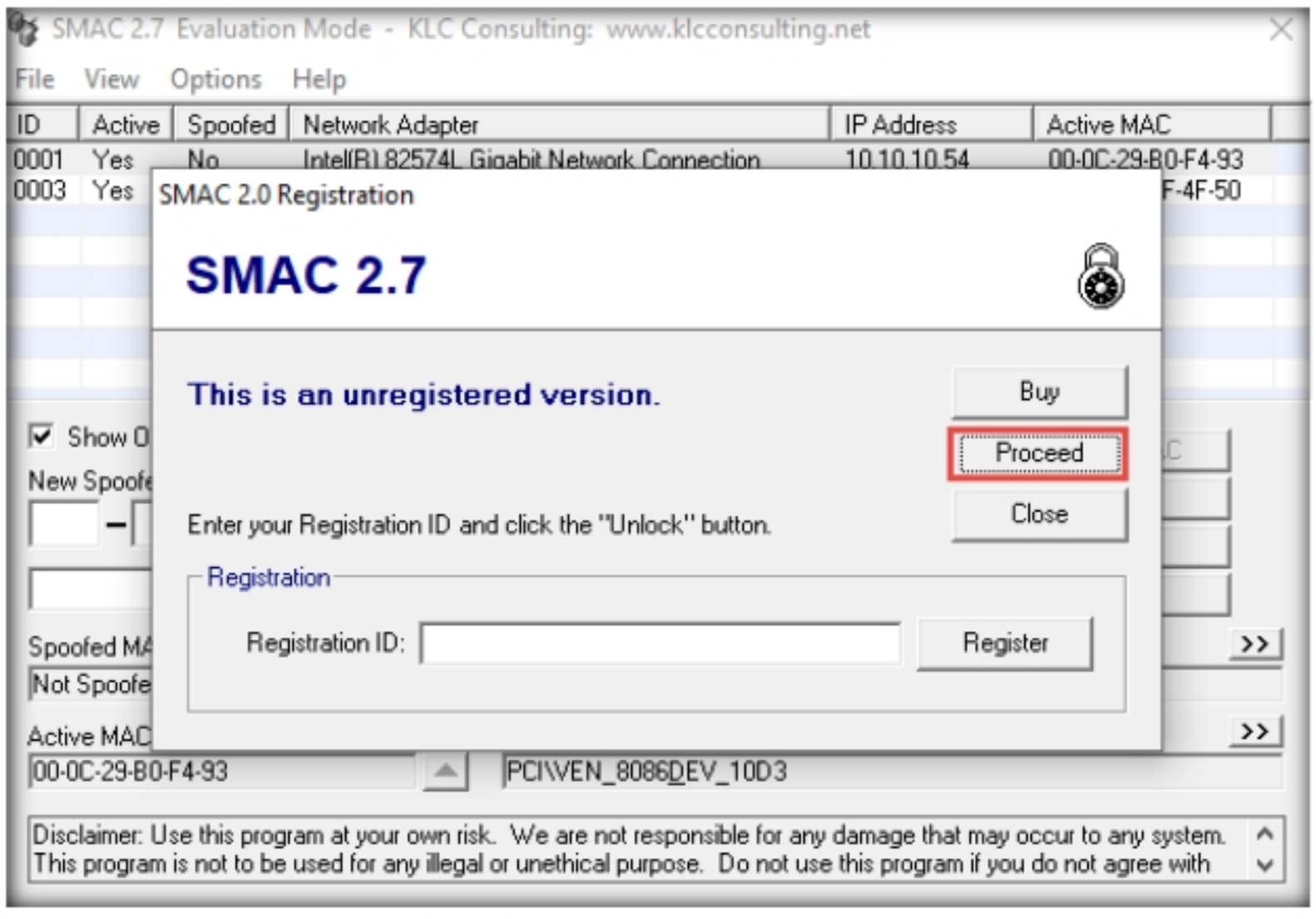


Figure 1.5.12: SMAC Registration window

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

Note: The network adapter might differ in your lab environment.

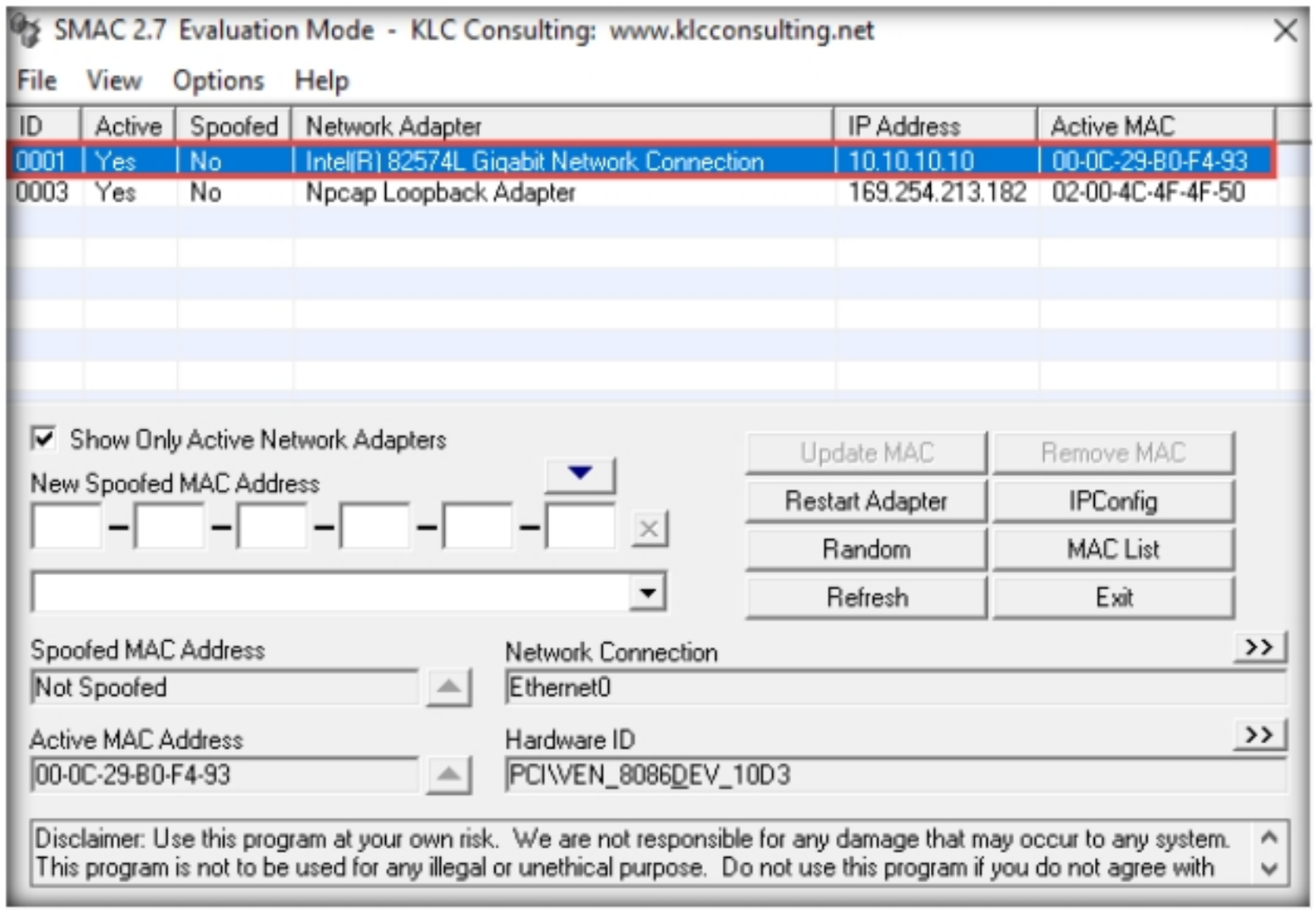


Figure 1.5.13: SMAC main window

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

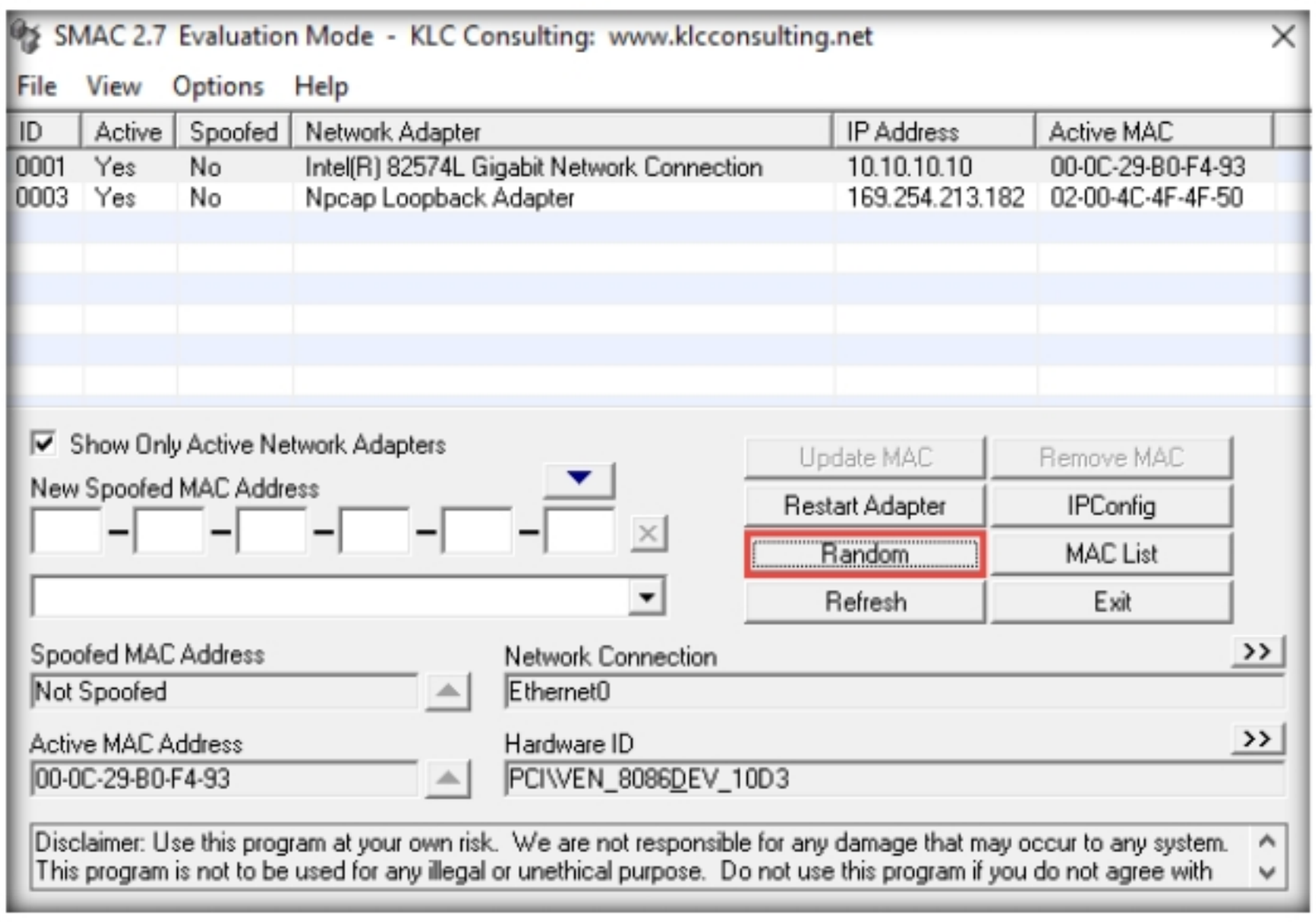


Figure 1.5.14: SMAC Random button to generate MAC addresses

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

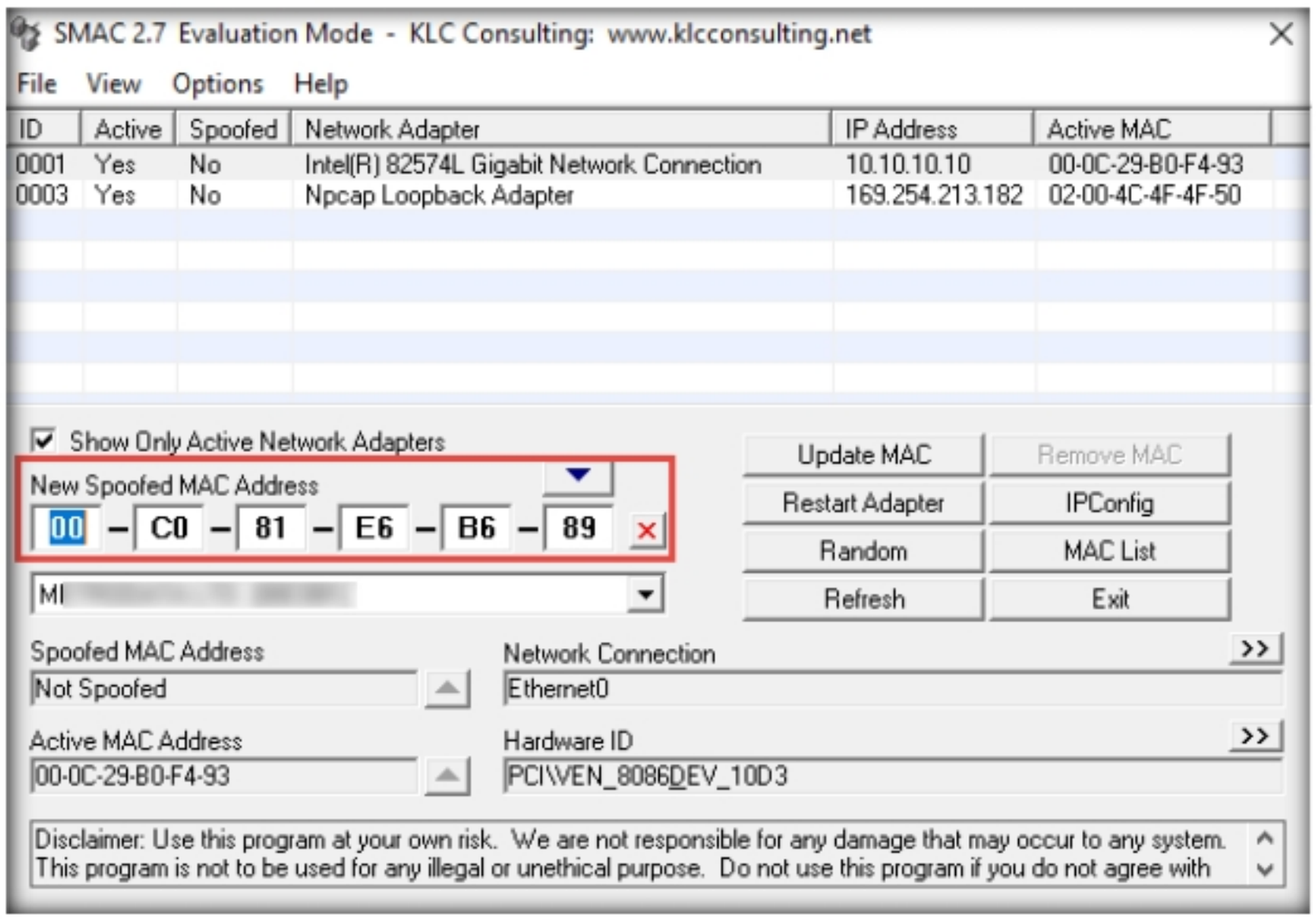


Figure 1.5.15: SMAC selecting a new spoofed MAC address

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

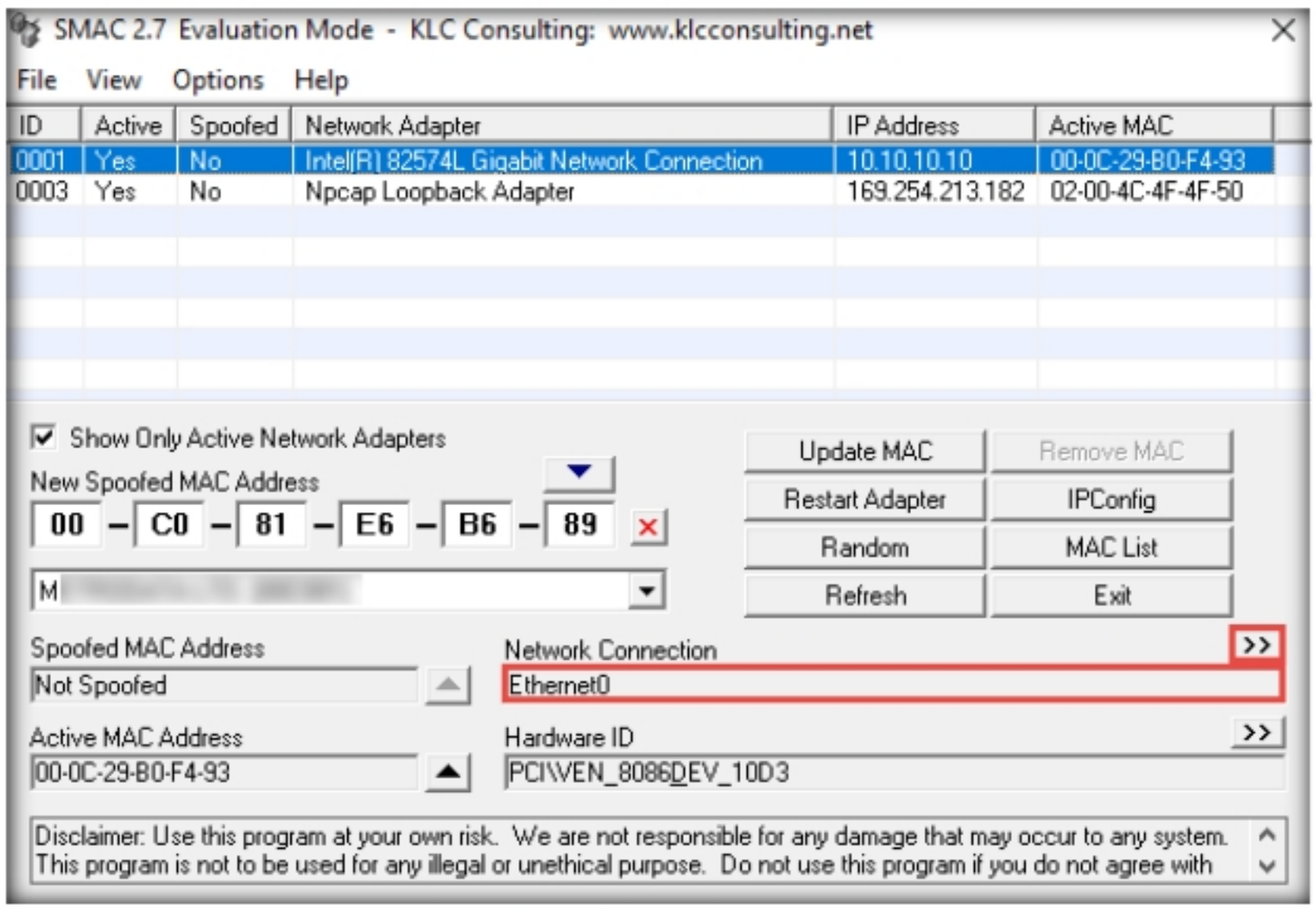


Figure 1.5.16: SMAC Network Connection information

24. 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.

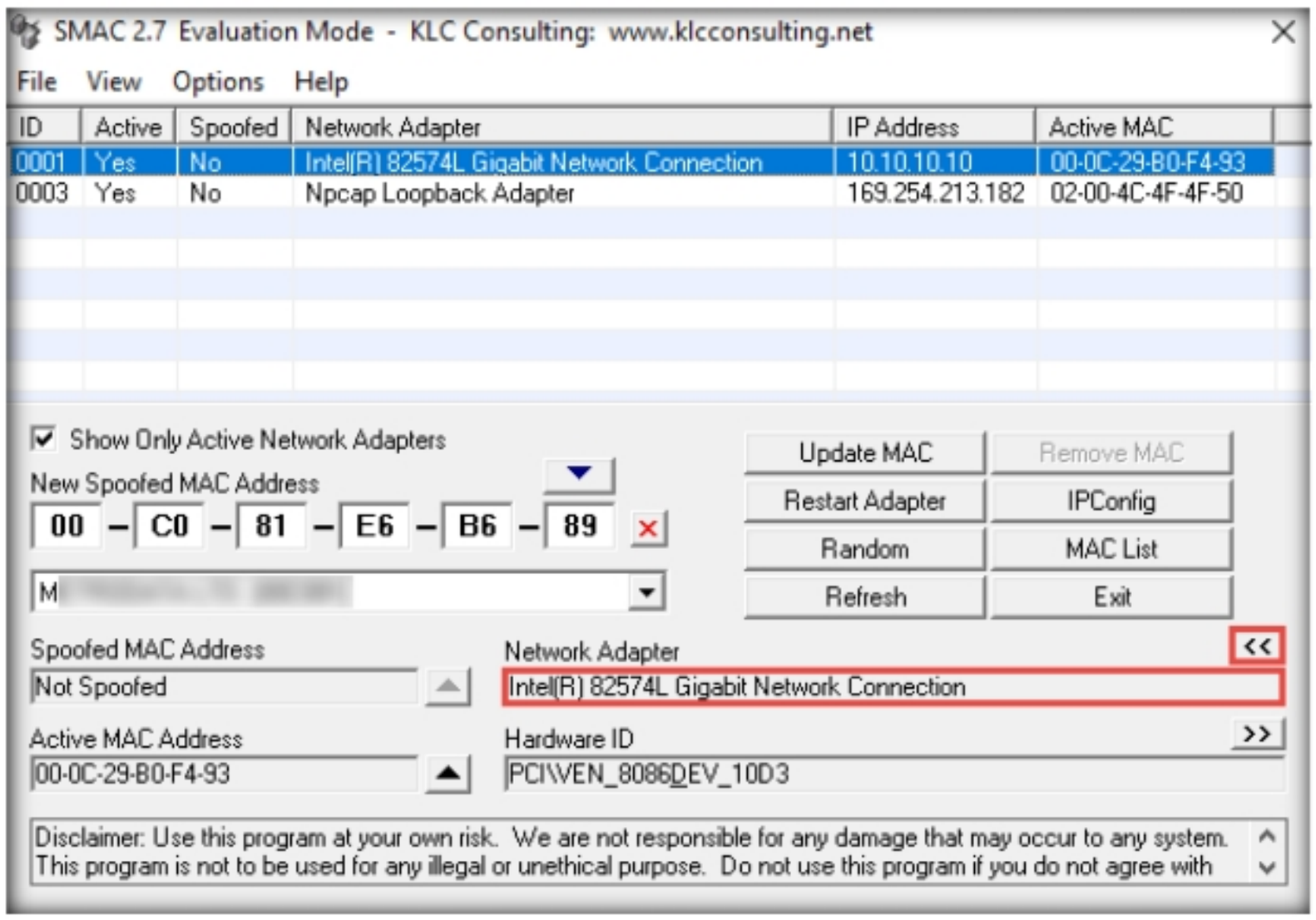


Figure 1.5.17: SMAC Network Adapter information

25. 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.

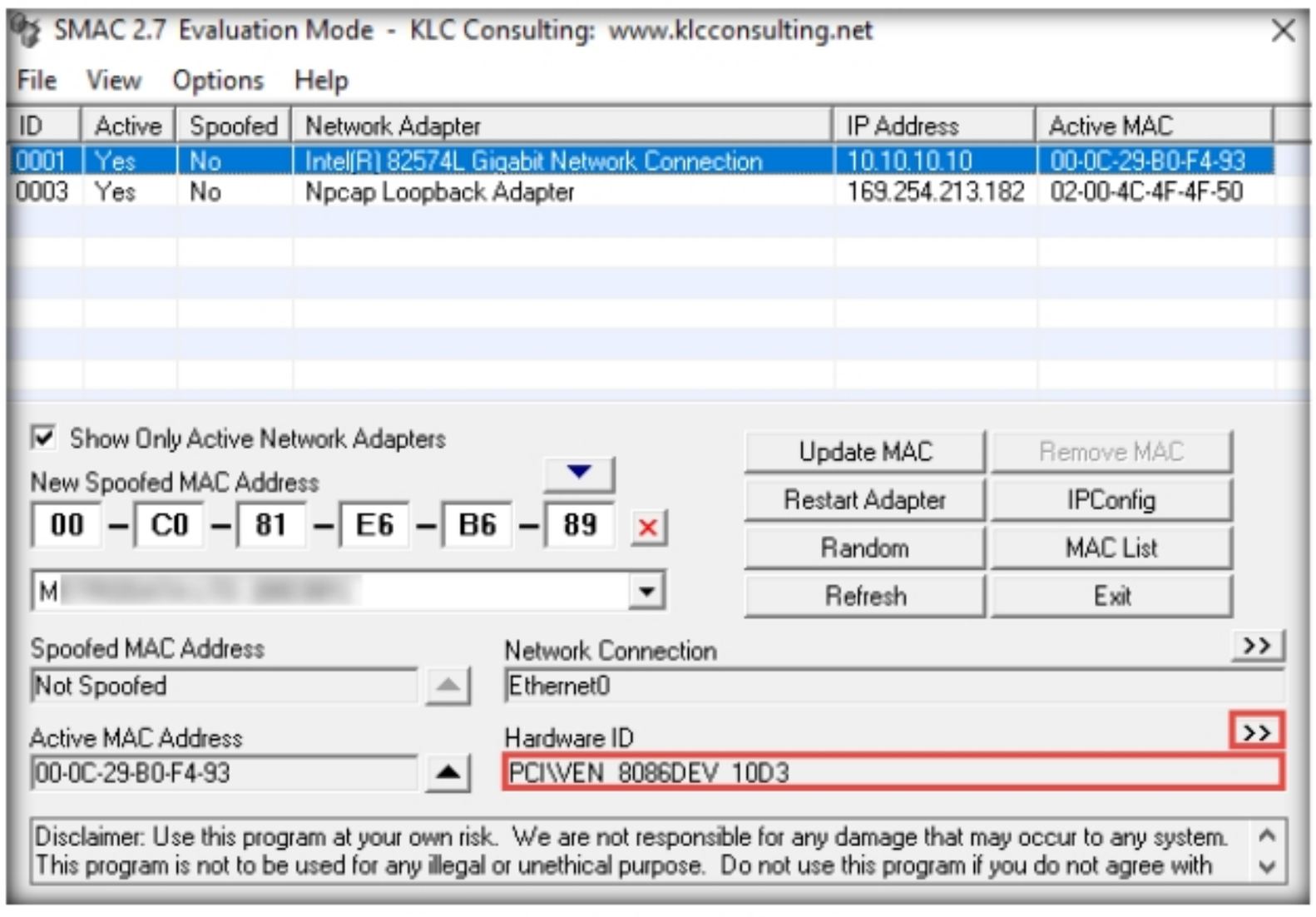


Figure 1.5.18: SMAC Hardware ID information

TASK 5.4

View IPConfig Information

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

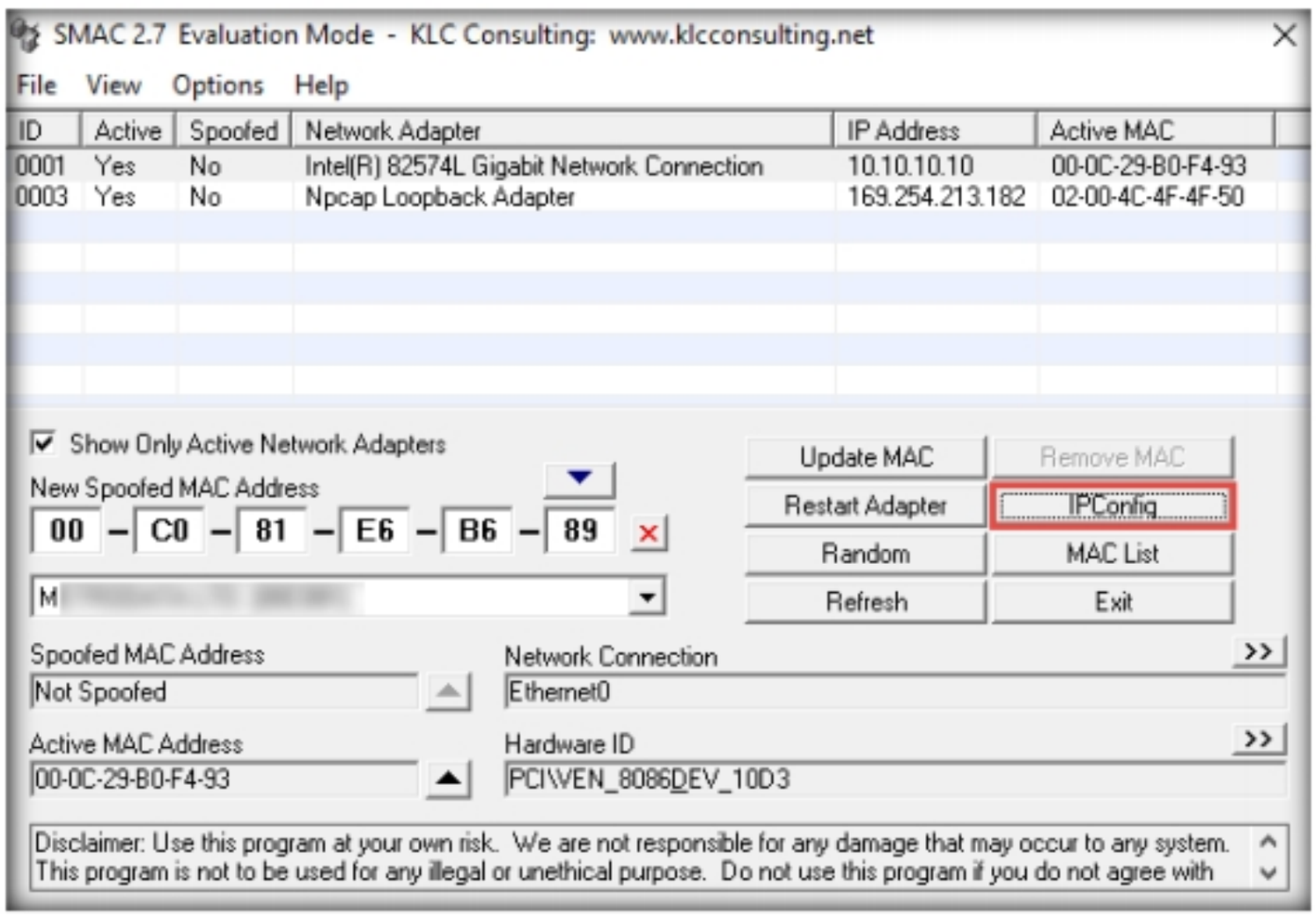


Figure 1.5.19: SMAC to view the information of IPConfig

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

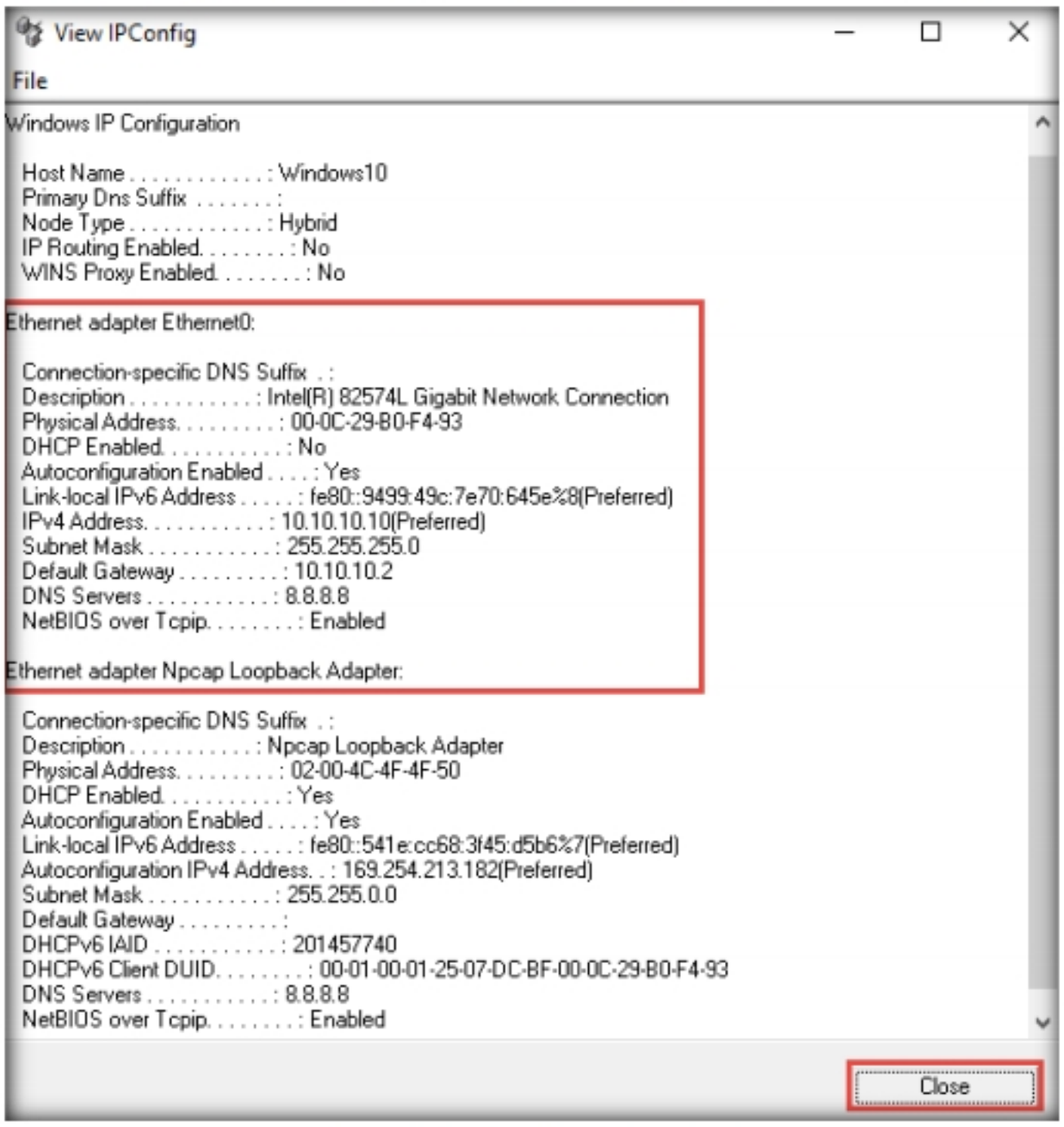


Figure 1.5.20: SMAC IPConfig information

TASK 5.5

Perform MAC Spoofing Using SMAC

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

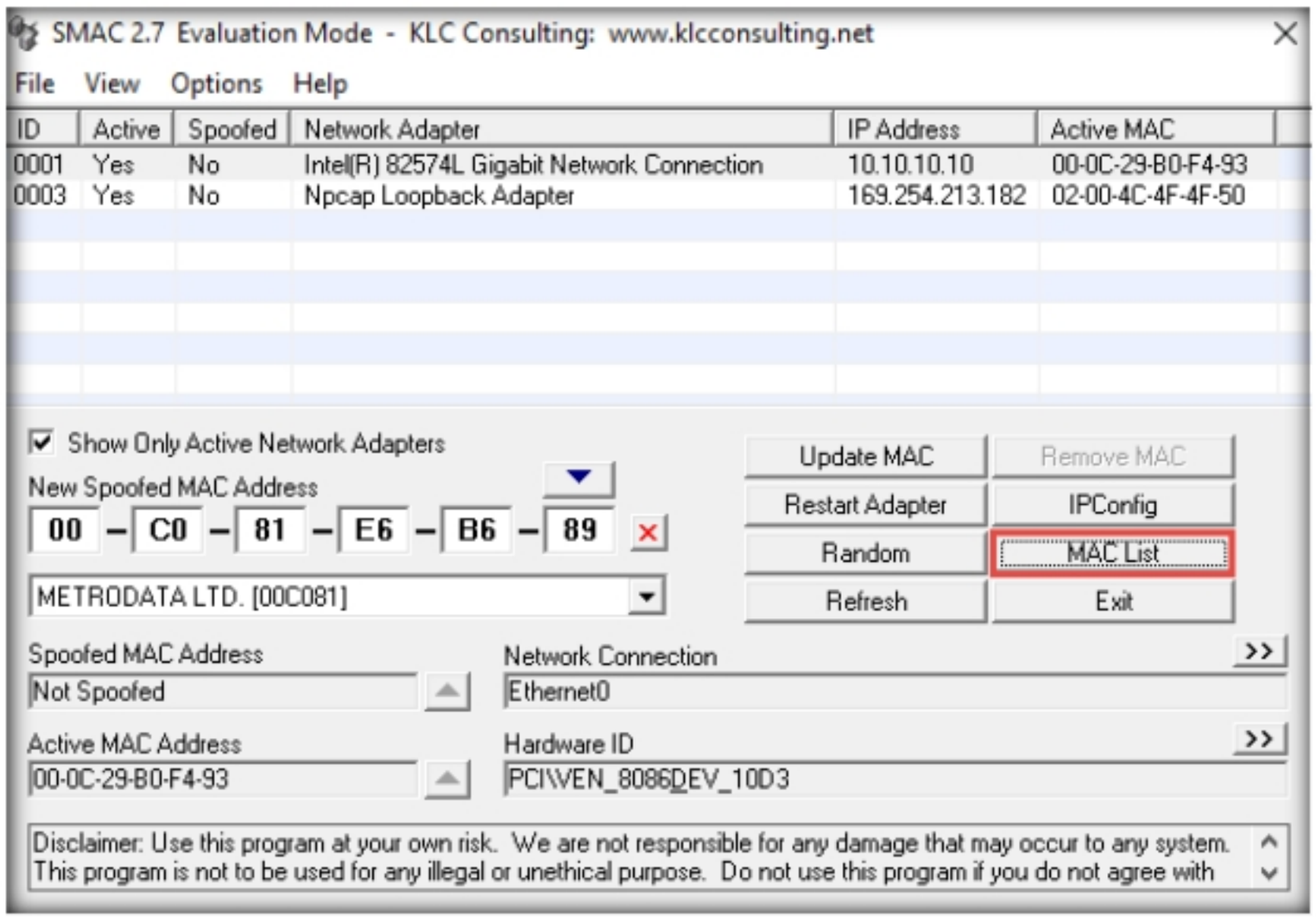


Figure 1.5.21: SMAC listing MAC addresses

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

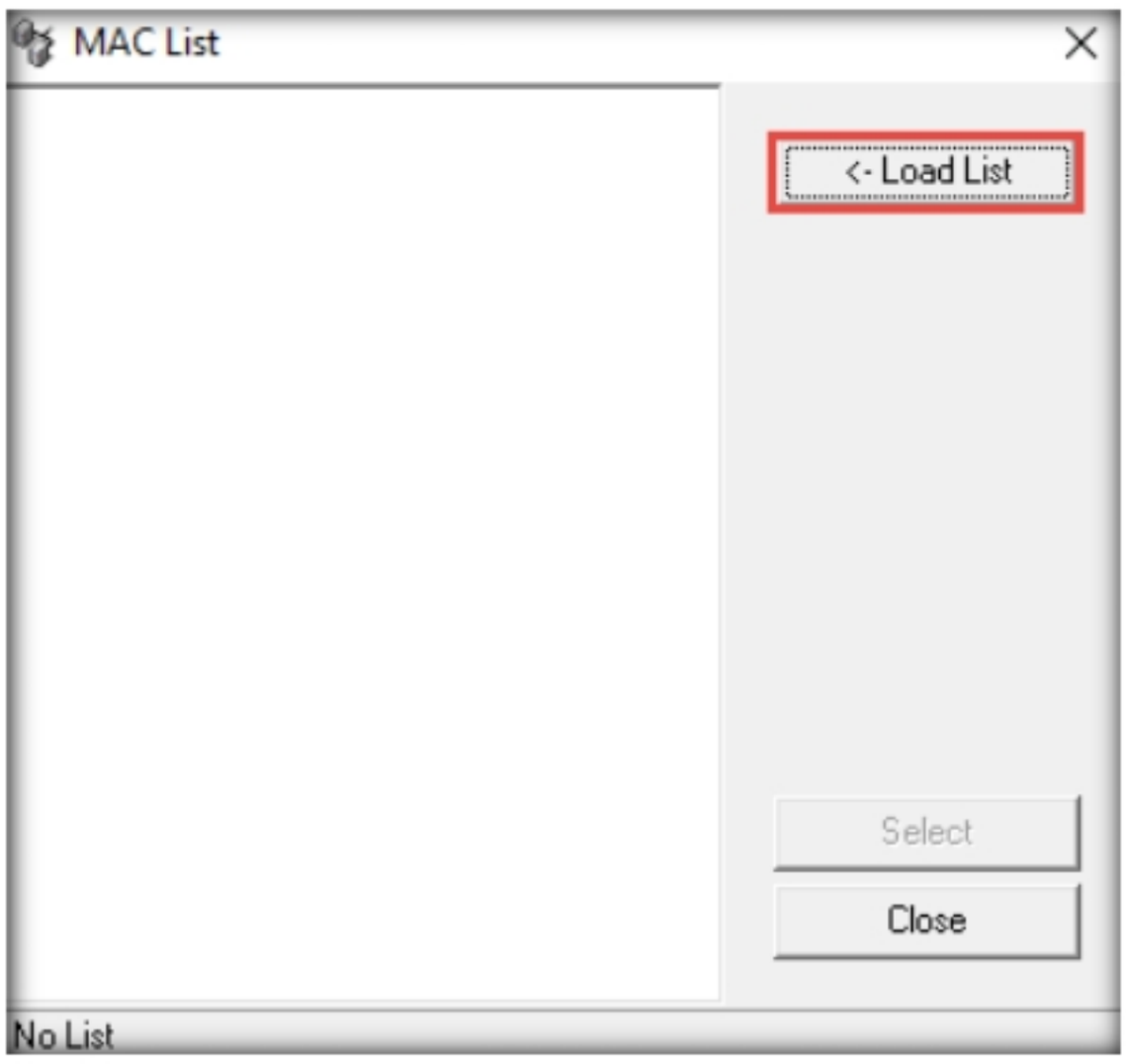


Figure 1.5.22: SMAC MAC List window

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

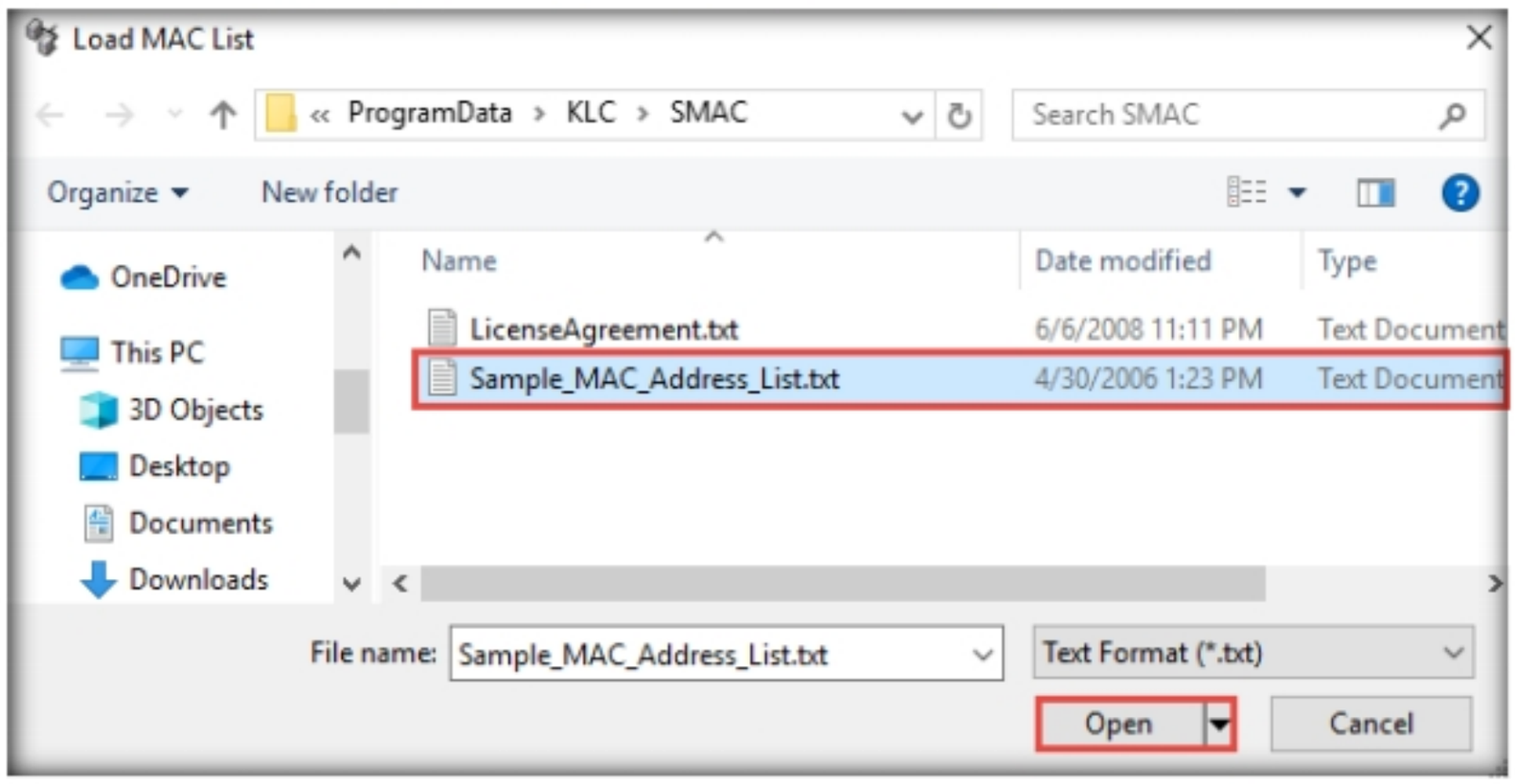


Figure 1.5.23: SMAC MAC List window

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

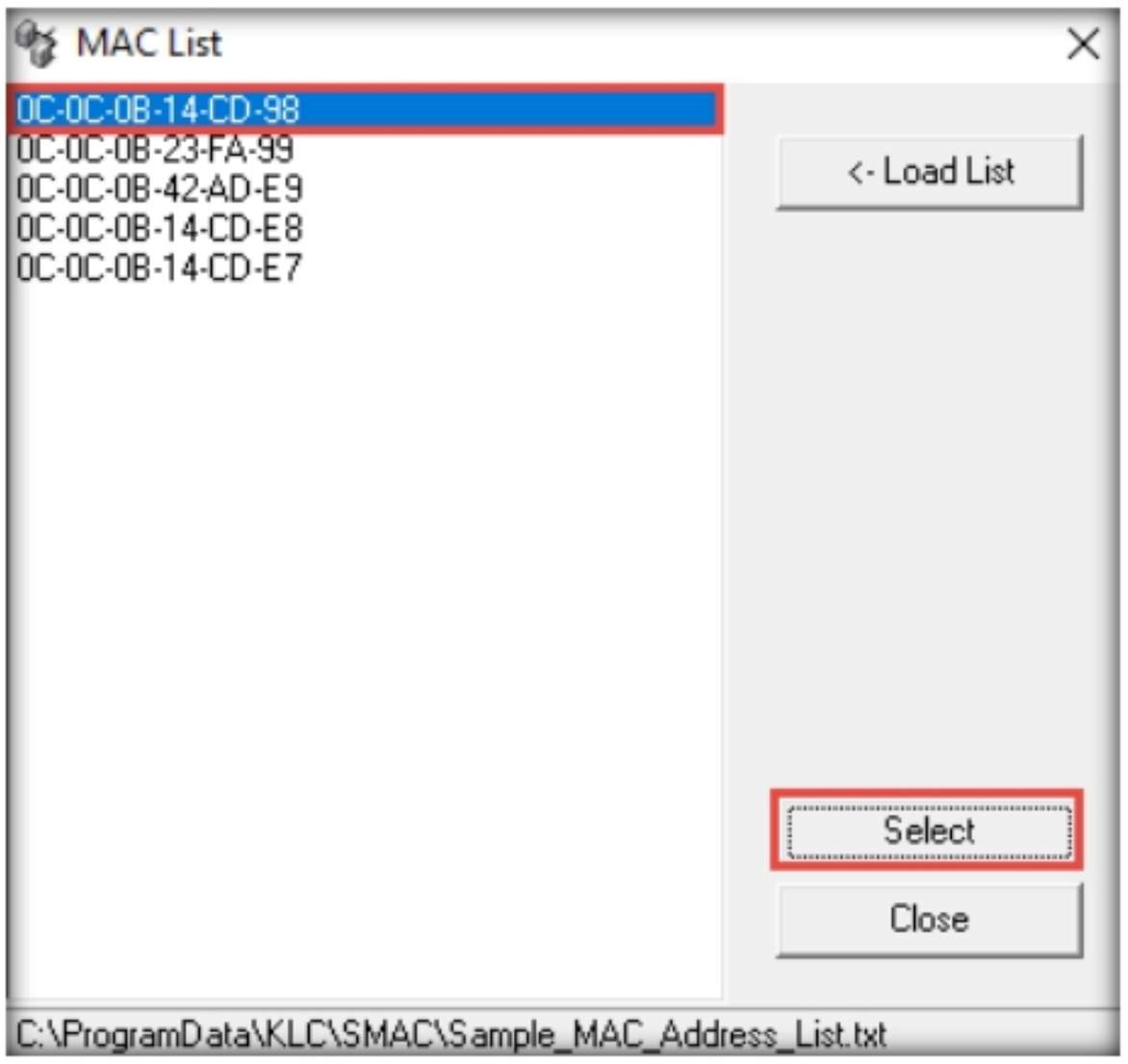


Figure 1.5.24: SMAC MAC List window

32. The selected MAC address appears under the **New Spoofed MAC Address** field.
33. Click the **Update MAC** button to update the machine's MAC address information.

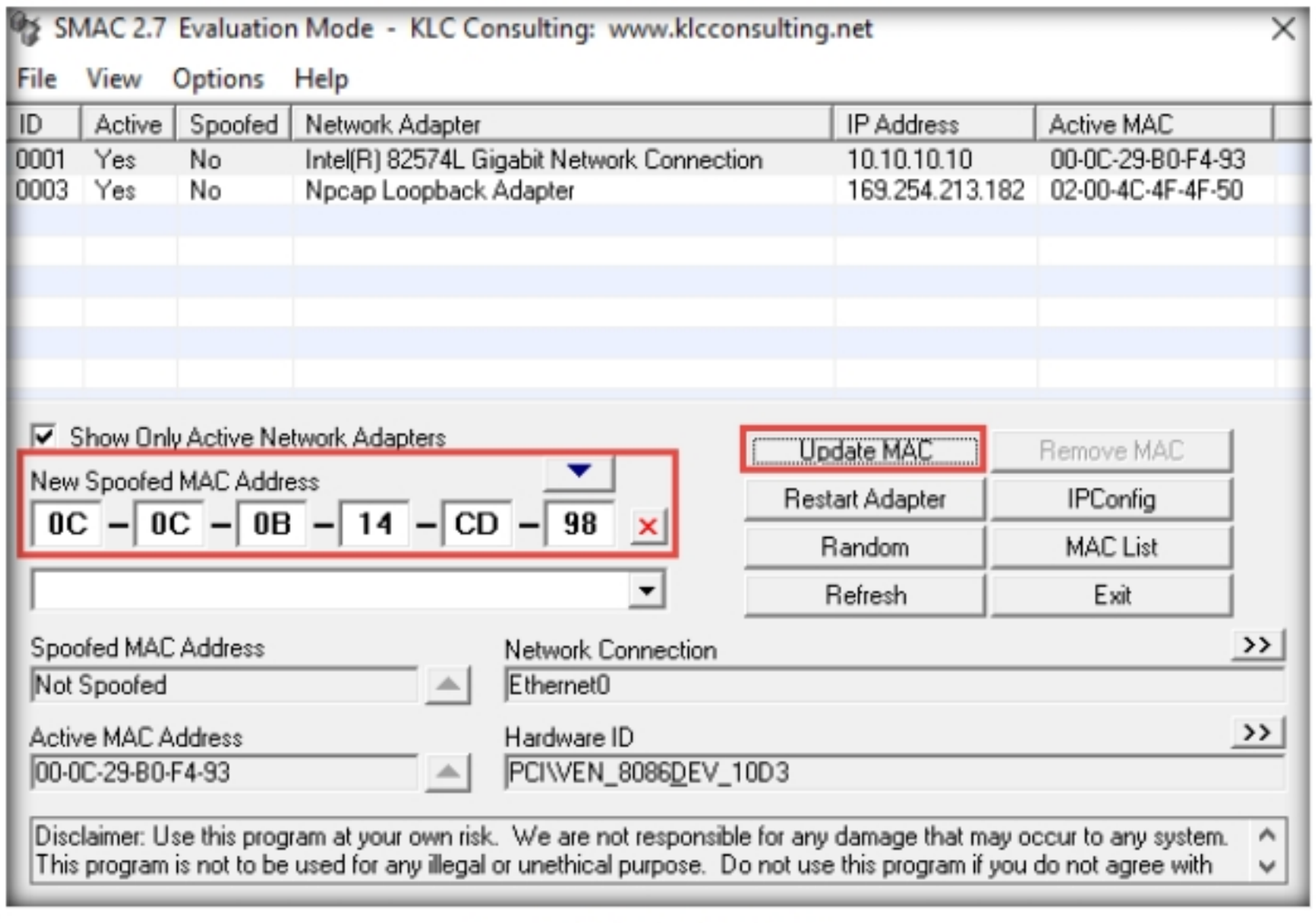


Figure 1.5.25: Updating MAC address

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

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

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

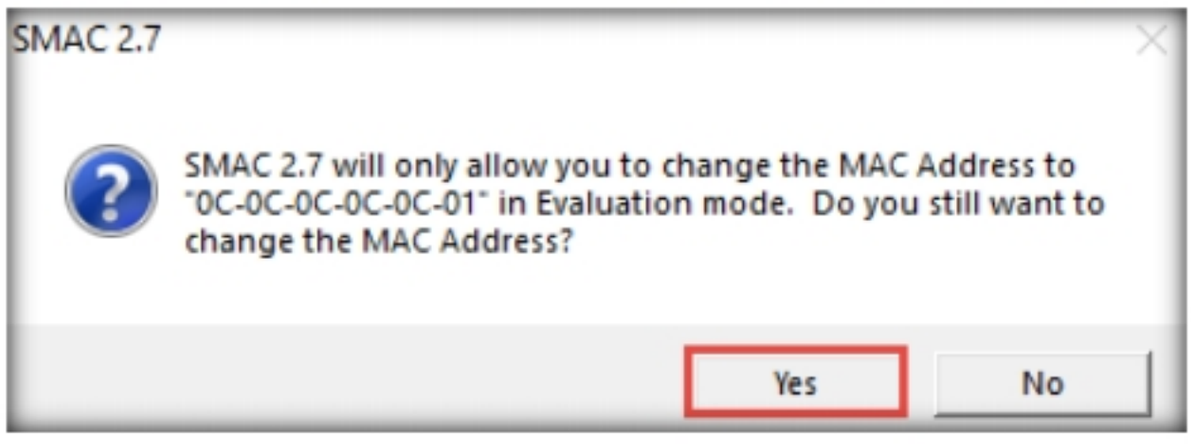


Figure 1.5.26: SMAC 2.0 dialog box

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

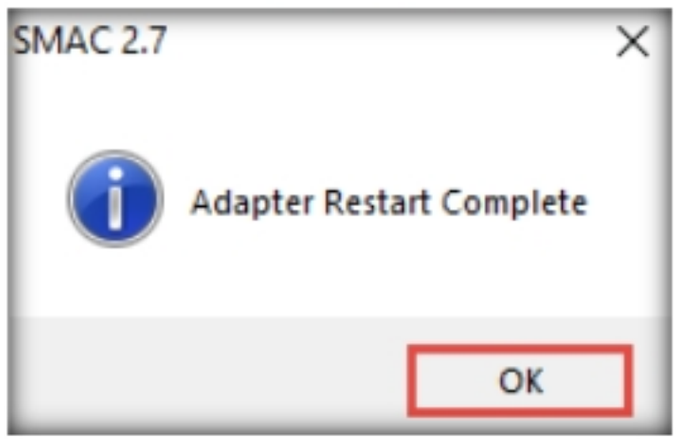


Figure 1.5.27: SMAC dialog box

36. 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**.

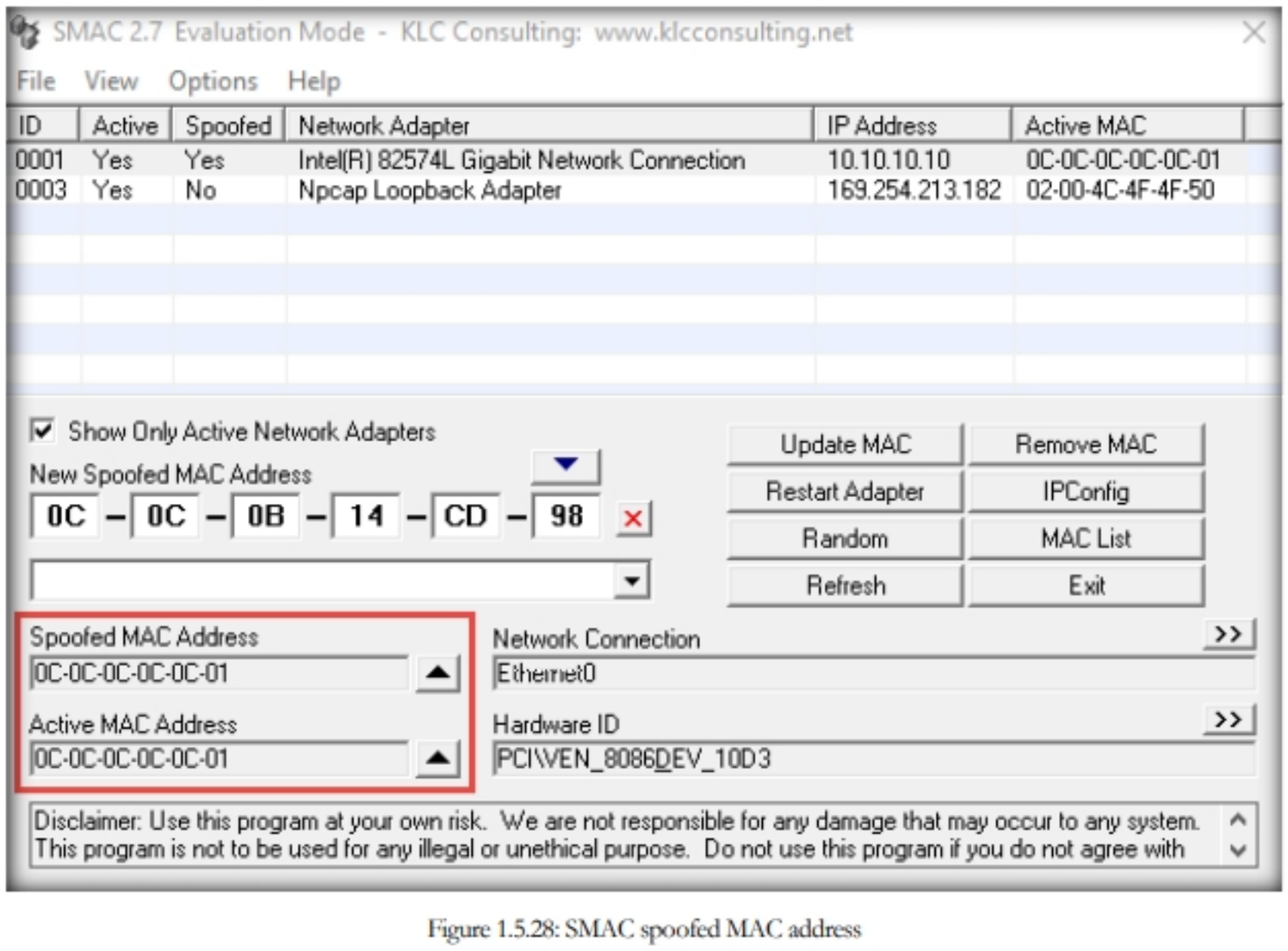


Figure 1.5.28: SMAC spoofed MAC address

You can also use other MAC address changer tools such as **MAC Address Changer** (https://www.novirusthanks.org), **Change MAC Address** (https://lizardsystems.com), **Easy Mac Changer** (https://github.com), or **Spoof-Me-Now** (https://sourceforge.net) to change the MAC address of the machine.

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

37. To restore the MAC address back to its original setting, click the **Remove MAC** button.
38. This concludes the demonstration of spoofing MAC addresses using TMAC and SMAC.
39. Close all open windows and document all the acquired information.
40. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Perform Network Sniffing using Various Sniffing Tools

Ethical hackers and pen testers are aided in network sniffing by various tools that make it an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Data traversing an HTTP channel flows in plain-text format and is therefore prone to MITM attacks. Network administrators can use sniffers for helpful purposes such as to troubleshoot network problems, examine security problems, and debug protocol implementations. However, an attacker can use sniffing tools such as Wireshark to sniff the traffic flowing between the client and the server. The traffic obtained by the attacker might contain sensitive information such as login credentials, which can then be used to perform malicious activities such as user-session impersonation.

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can only capture data packets from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises leave their switch ports open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

The information gathered in the previous step may be insufficient to reveal the potential vulnerabilities of the target. There may be more information to help find loopholes in the target. An ethical hacker needs to perform network security assessments and suggest proper troubleshooting techniques to mitigate attacks. This lab provides hands-on experience of how to use sniffing tools to sniff network traffic and capture it on a remote interface.

Lab Objectives

- Perform password sniffing using Wireshark

- Analyze a network using the Capsa Network Analyzer
- Analyze a network using the Omnipeek Network Protocol Analyzer
- Analyze a network using the SteelCentral Packet Analyzer

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- A business Email ID to download the tool
- Administrator privileges to run the tools

Lab Duration

Time: 60 Minutes

Overview of Network Sniffing Tools

System administrators use automated tools to monitor their networks, but attackers misuse these tools to sniff network data. Network sniffing tools can be used to perform a detailed network analysis. When protecting a network, it is important to have as many details about the packet traffic as possible. By actively scanning the network, a threat hunter can stay vigilant and respond quickly to attacks.

Lab Tasks

TASK 1

Perform Password Sniffing using Wireshark

Here, we will use the Wireshark tool to perform password sniffing.

Note: In this task, we will use the **Windows Server 2019** (**10.10.10.19**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

Launch Wireshark

3. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wireshark**. Select **Wireshark** from the results.
4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture, as shown in the screenshot.

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

Note: The network adapter might differ in your lab environment.

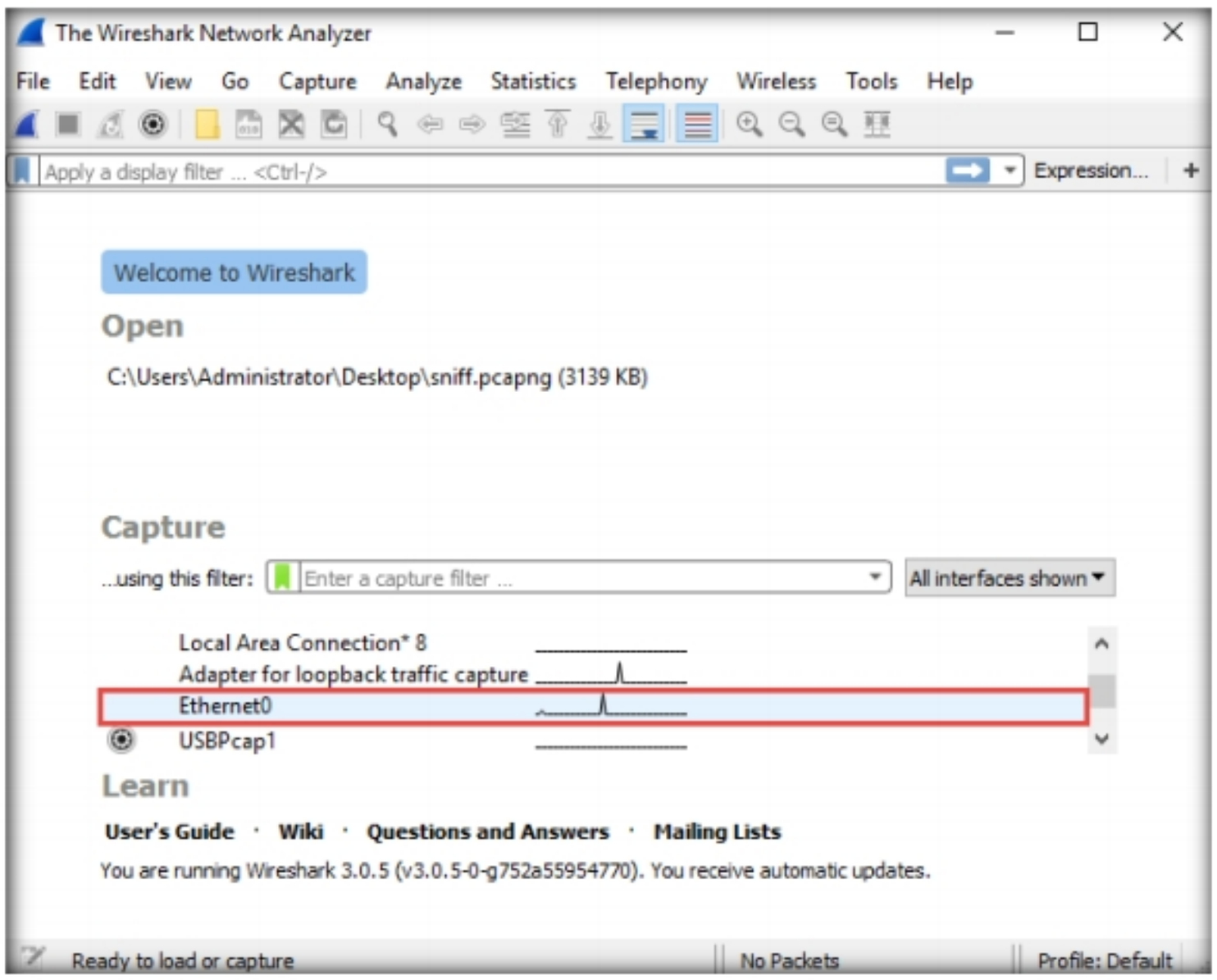


Figure 2.1.1: Wireshark Main Window with Interface Option

The captured Wireshark files can be programmatically edited via the command-line. A set of filters for customized data displays can be refined using a display filter.

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

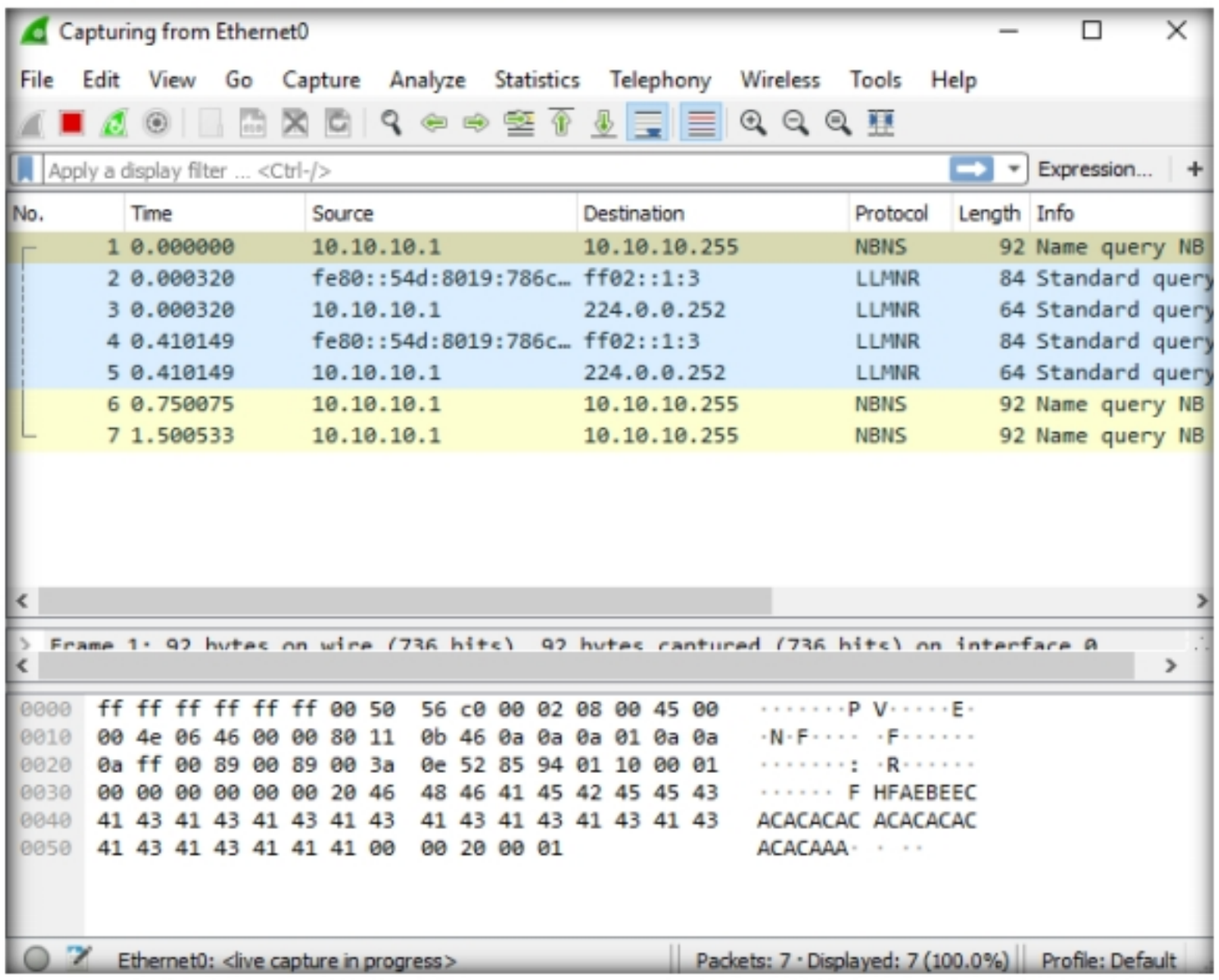


Figure 2.1.2: Wireshark Window with Packets Captured

TASK 1.2

Open Moviescope Website and Login

6. Now, switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
7. Open any browser (here, **Mozilla Firefox**), type **http://www.moviescope.com/** in the address bar, and press **Enter**.
8. The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in the screenshot.

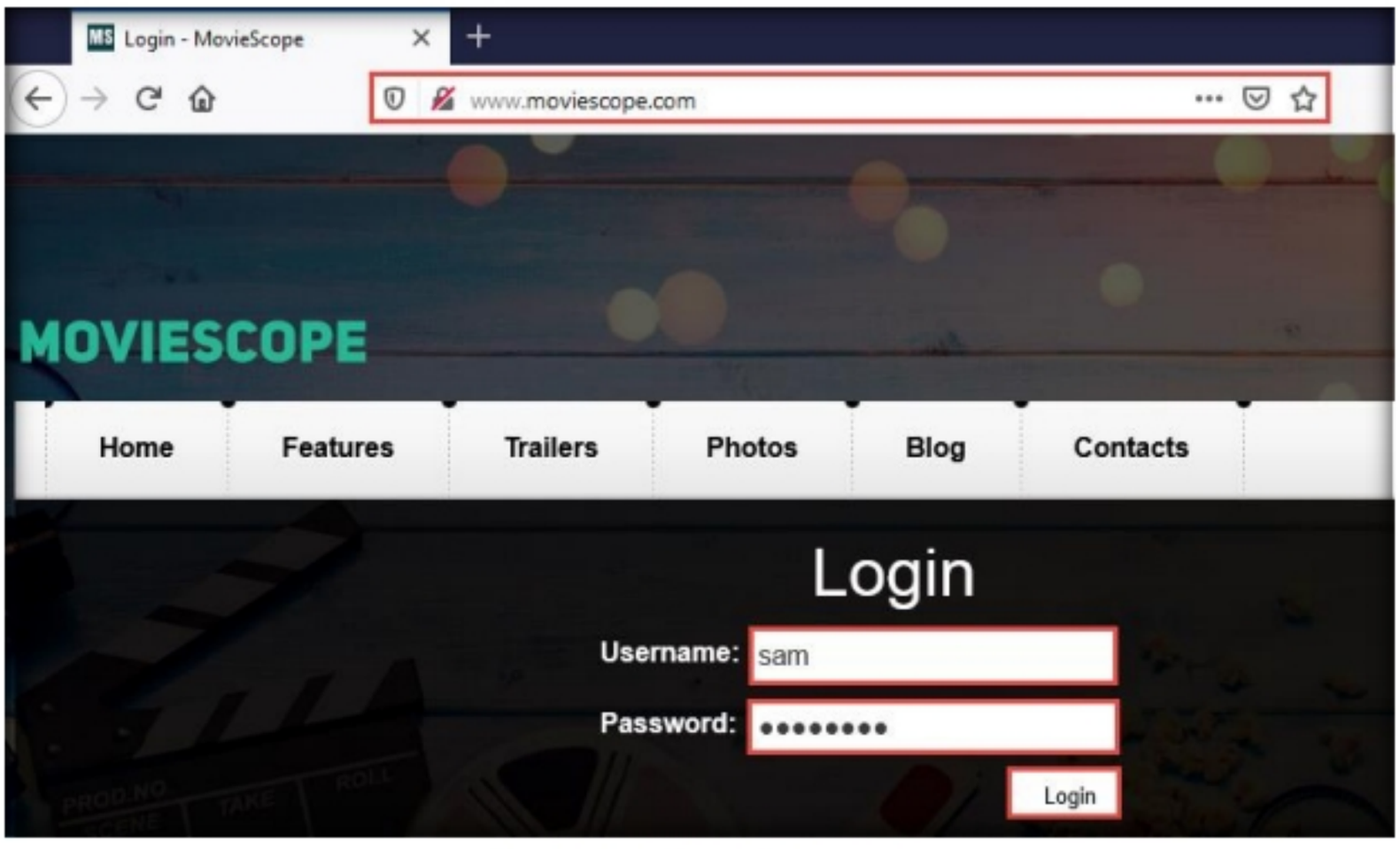


Figure 2.1.3: Moviescope login page

TASK 1.3

Stop Live Capturing

9. Switch to **Windows Server 2019**, and in the **Wireshark** window, click the **Stop capturing packets** icon ( ) on the toolbar.

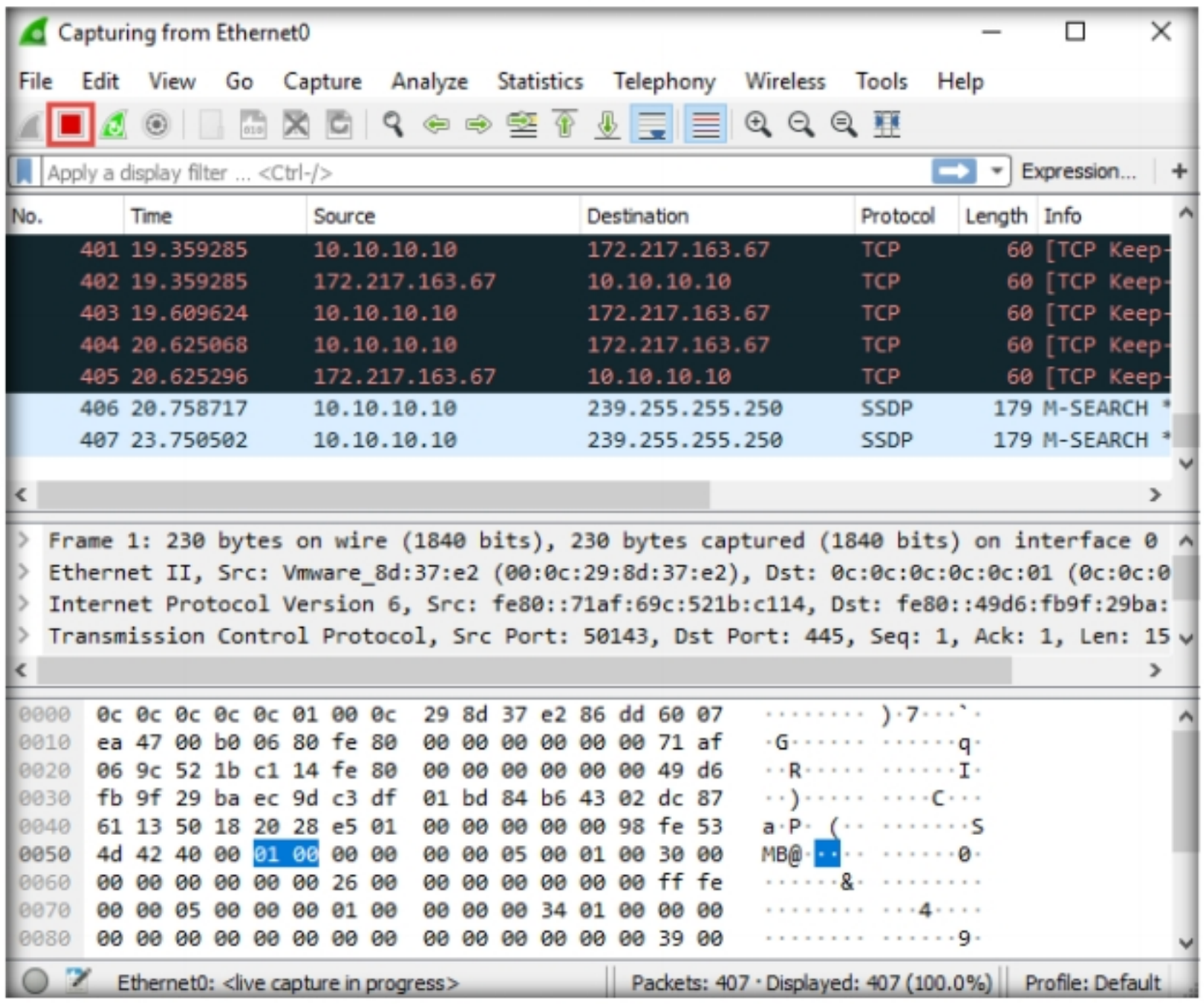


Figure 2.1.4: Wireshark Window: Stopping Live Capture

TASK 1.4

Save Captured Packets File

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

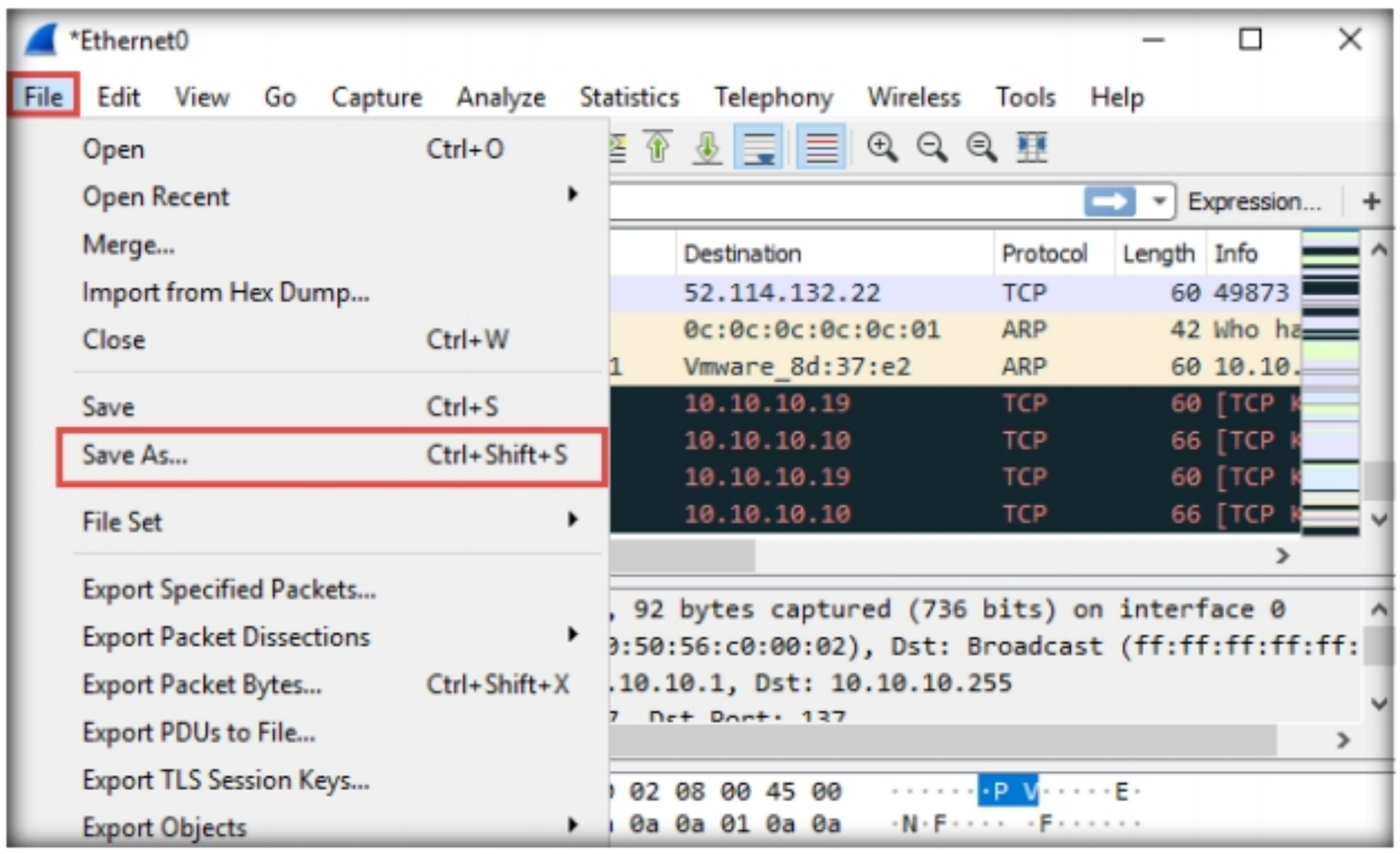


Figure 2.1.5: Wireshark: Saving the Captured Packets

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

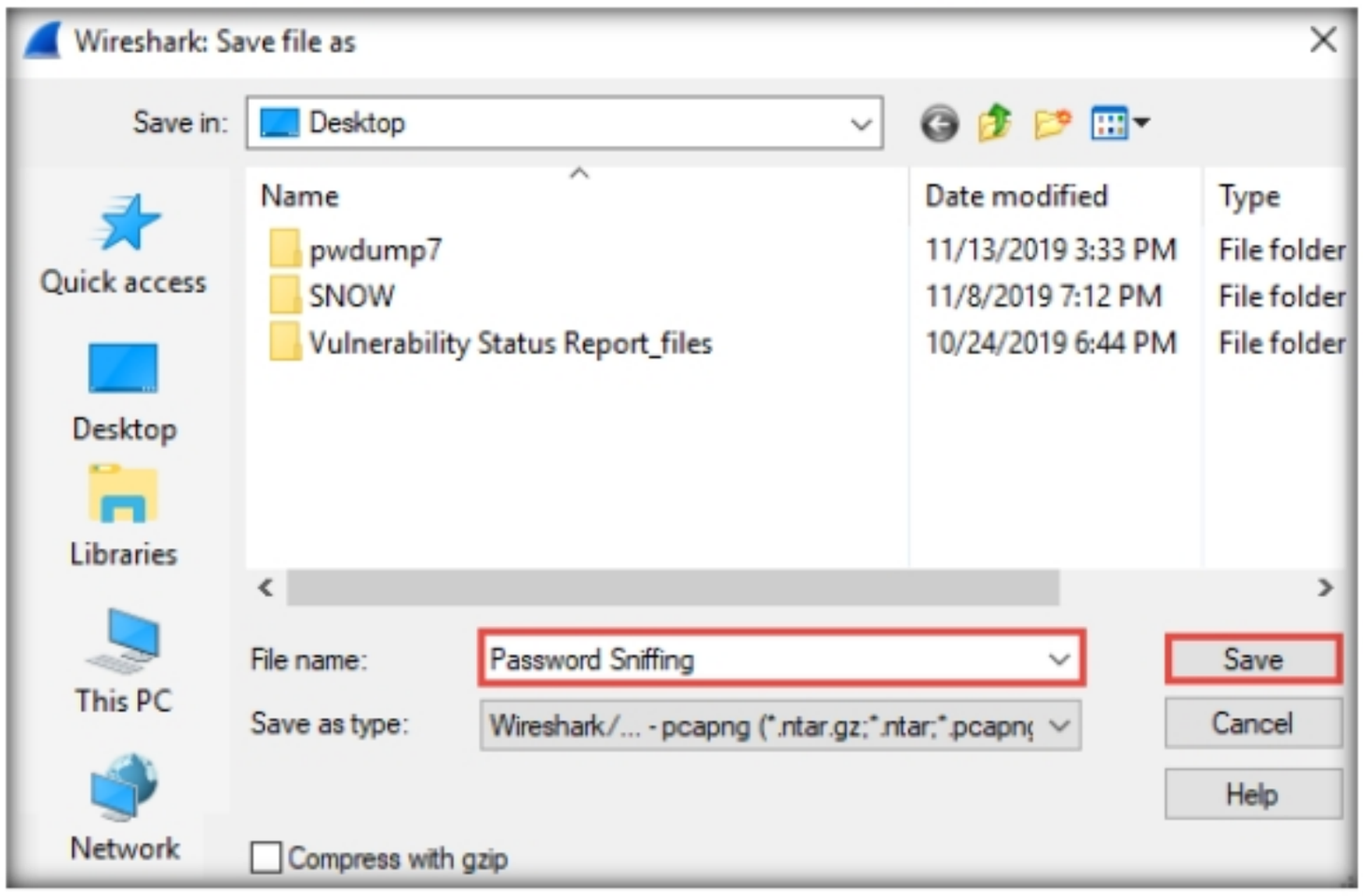


Figure 2.1.6: Wireshark Saving a packet capture

TASK 1.5

Look for Passwords

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

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

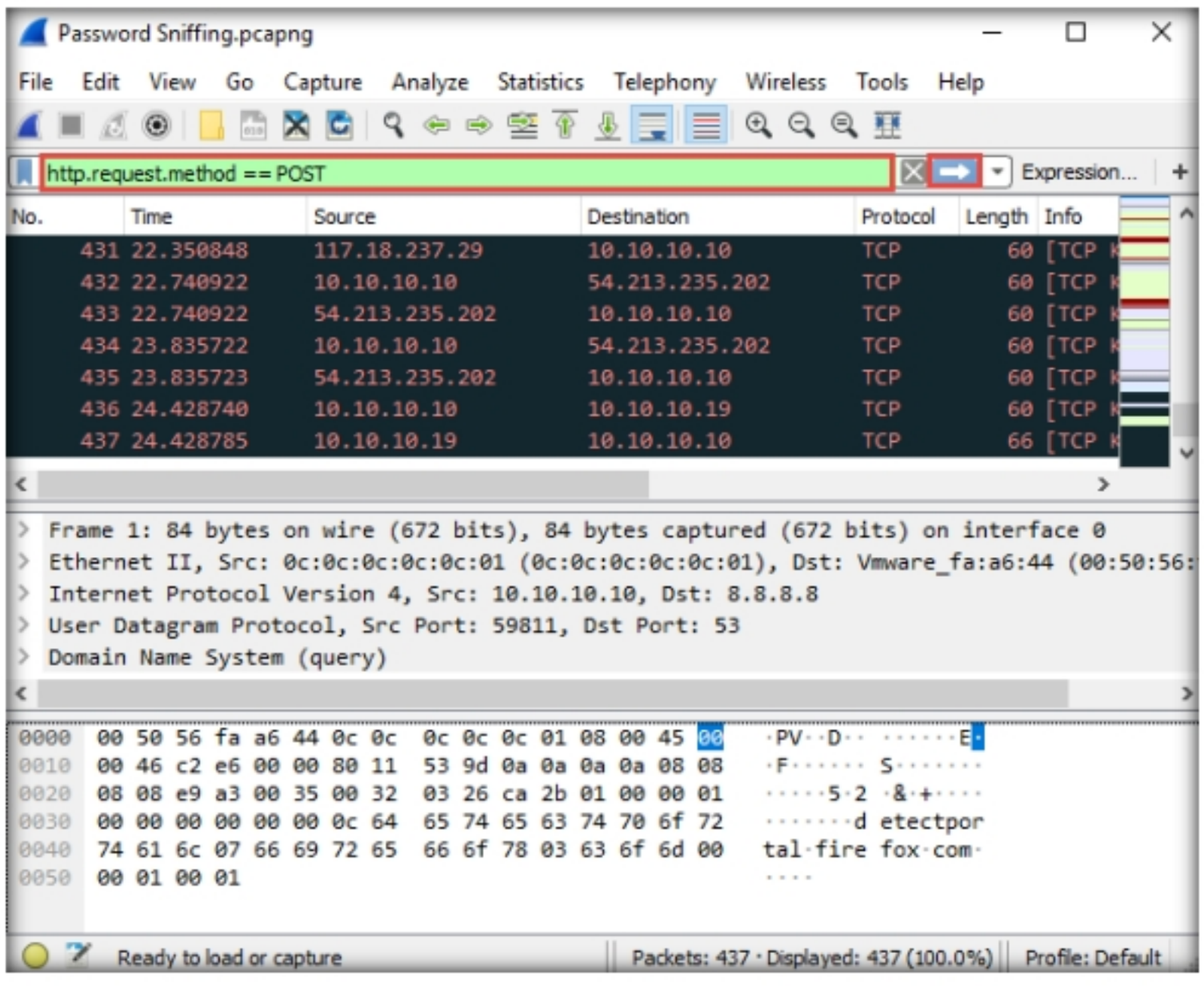


Figure 2.1.7: Wireshark: Filtering http traffic

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

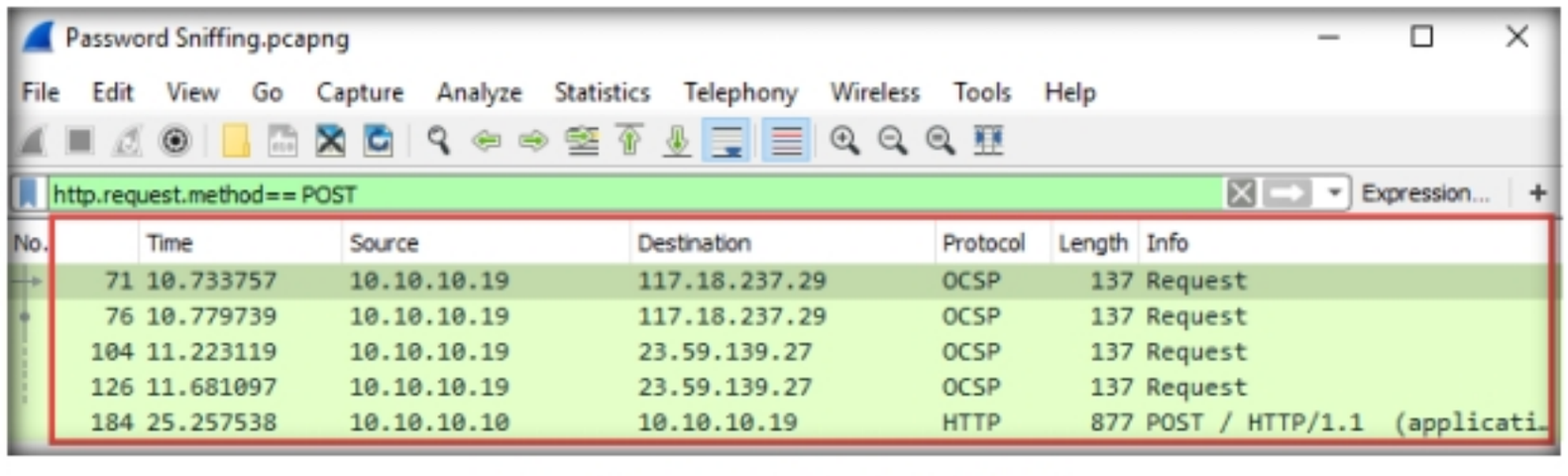


Figure 2.1.8: Wireshark: Filtering http traffic

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

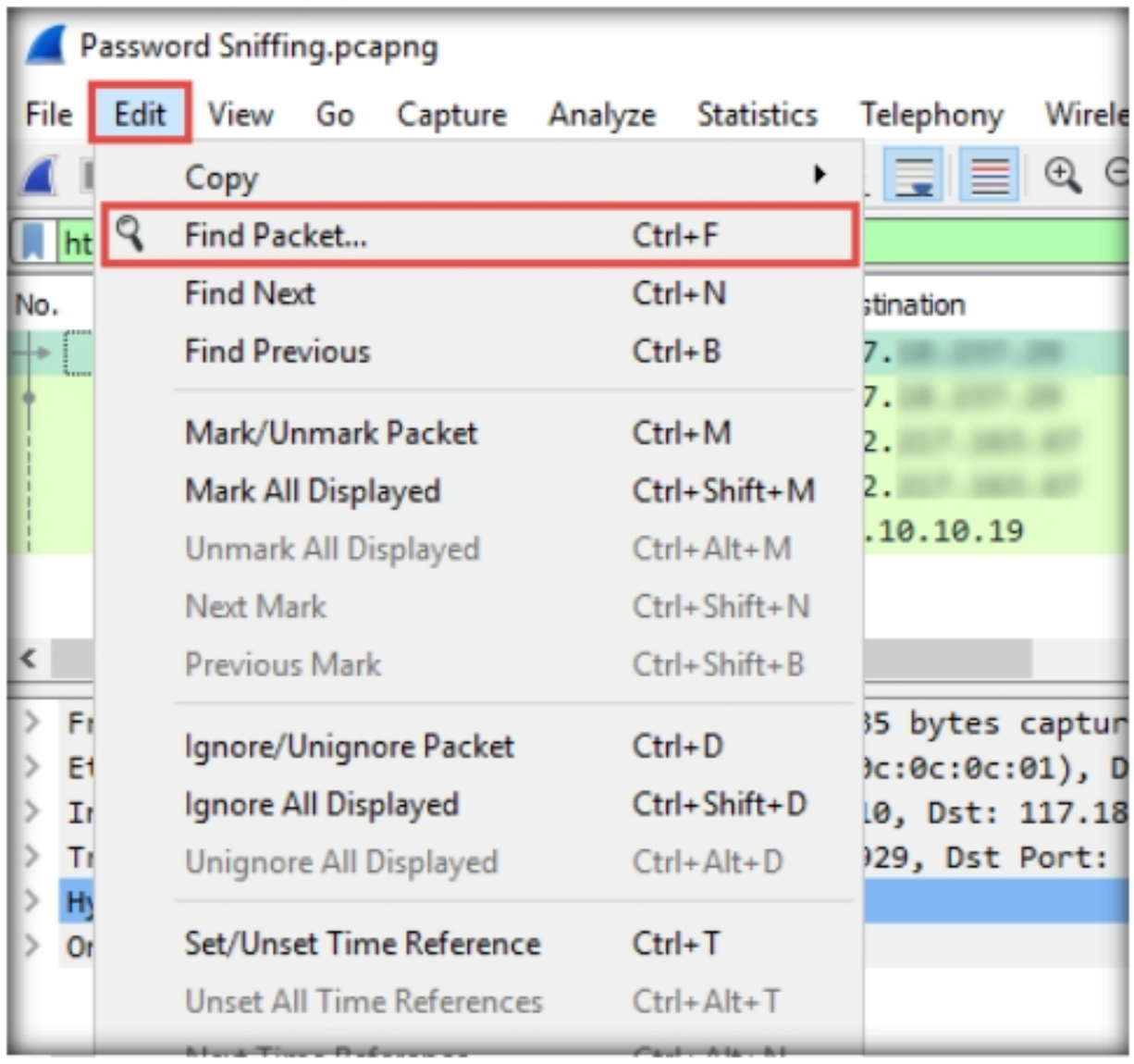


Figure 2.1.9: Wireshark: Finding Packet Option

15. The **Find Packet** section appears below the display filter field, as shown in the screenshot.

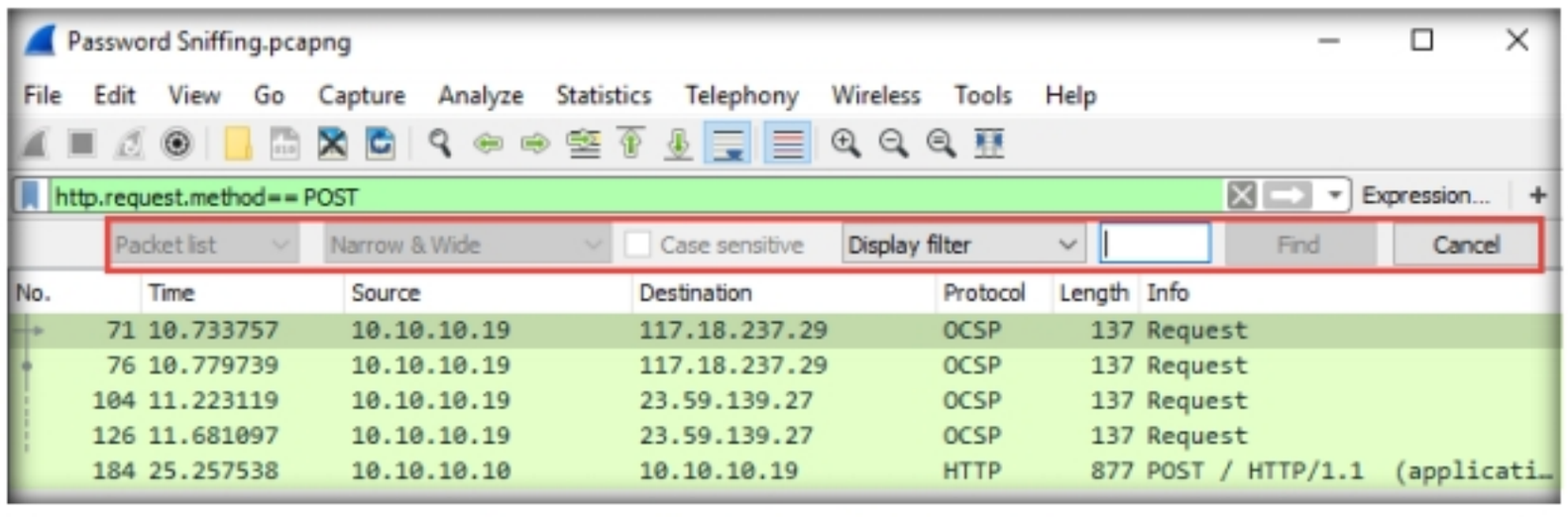


Figure 2.1.10: Wireshark: Find Packet Window

16. Click **Display filter**, select **String** from the drop-down options. Click **Packet list**, select **Packet details** from the drop-down options, and click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options.
17. In the field next to **String**, type **pwd** and click the **Find** button.

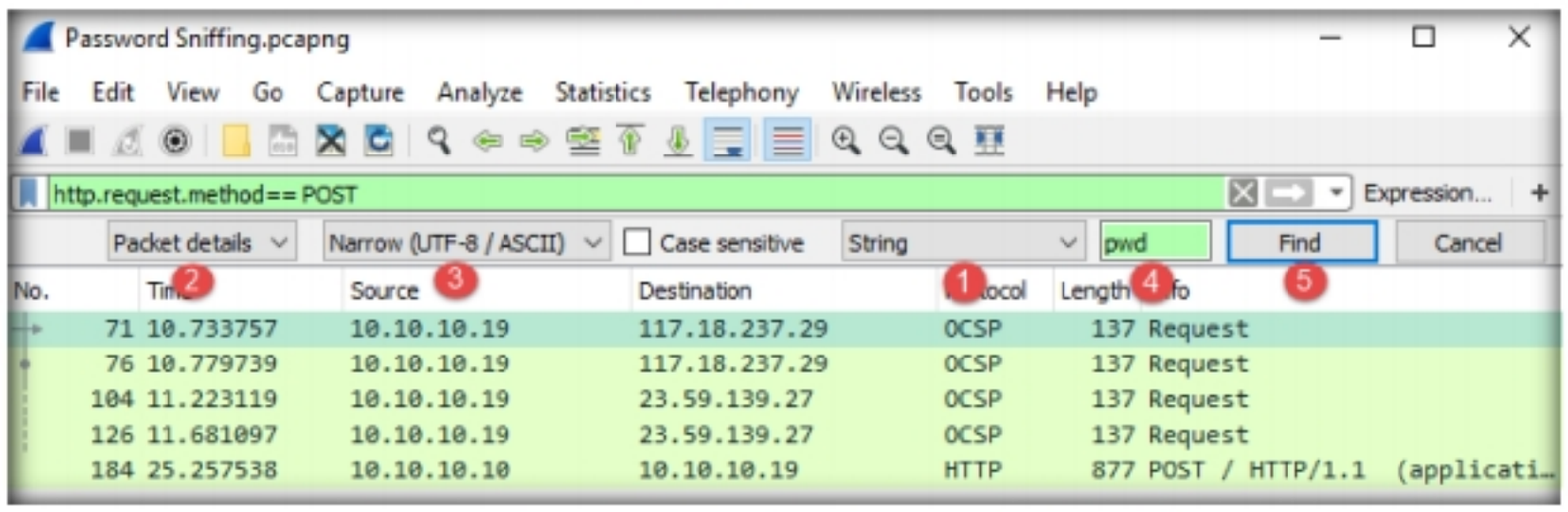


Figure 2.1.11: Wireshark: Selecting Options in Find Packet Window

18. **Wireshark** will now display the sniffed password from the captured packets.
19. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** node from the packet details section, and view the captured username and password, as shown in the screenshot.

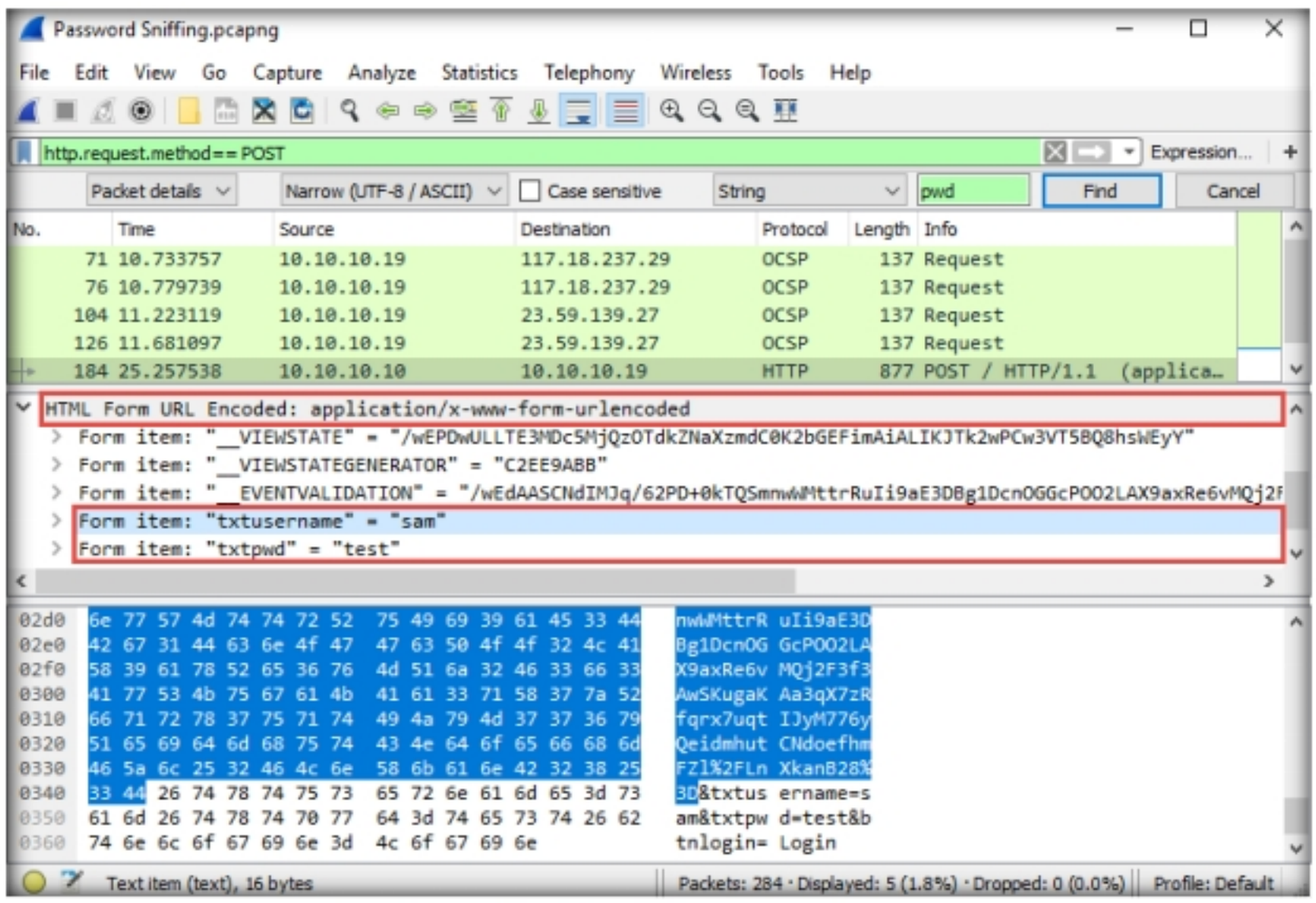


Figure 2.1.12: Wireshark: displaying the captured password

20. Close the **Wireshark** window.
21. Navigate to the **Windows 10** virtual machine, close the web browser, and sign out from the **Admin** account.

TASK 1.6

Capture Remote Network Traffic Using Wireshark

22. Switch back to the **Windows Server 2019** virtual machine.
23. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

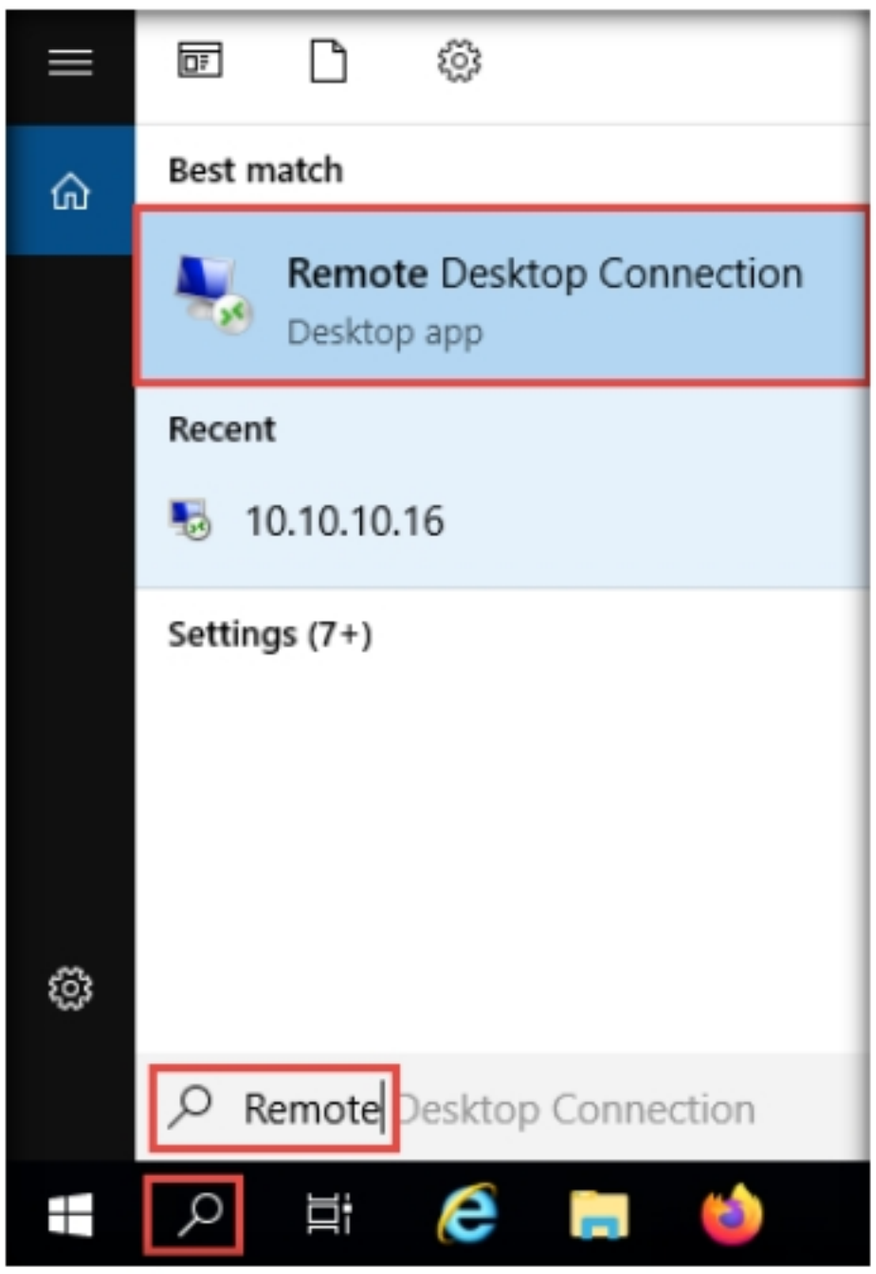


Figure 2.1.13: Selecting Search

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

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

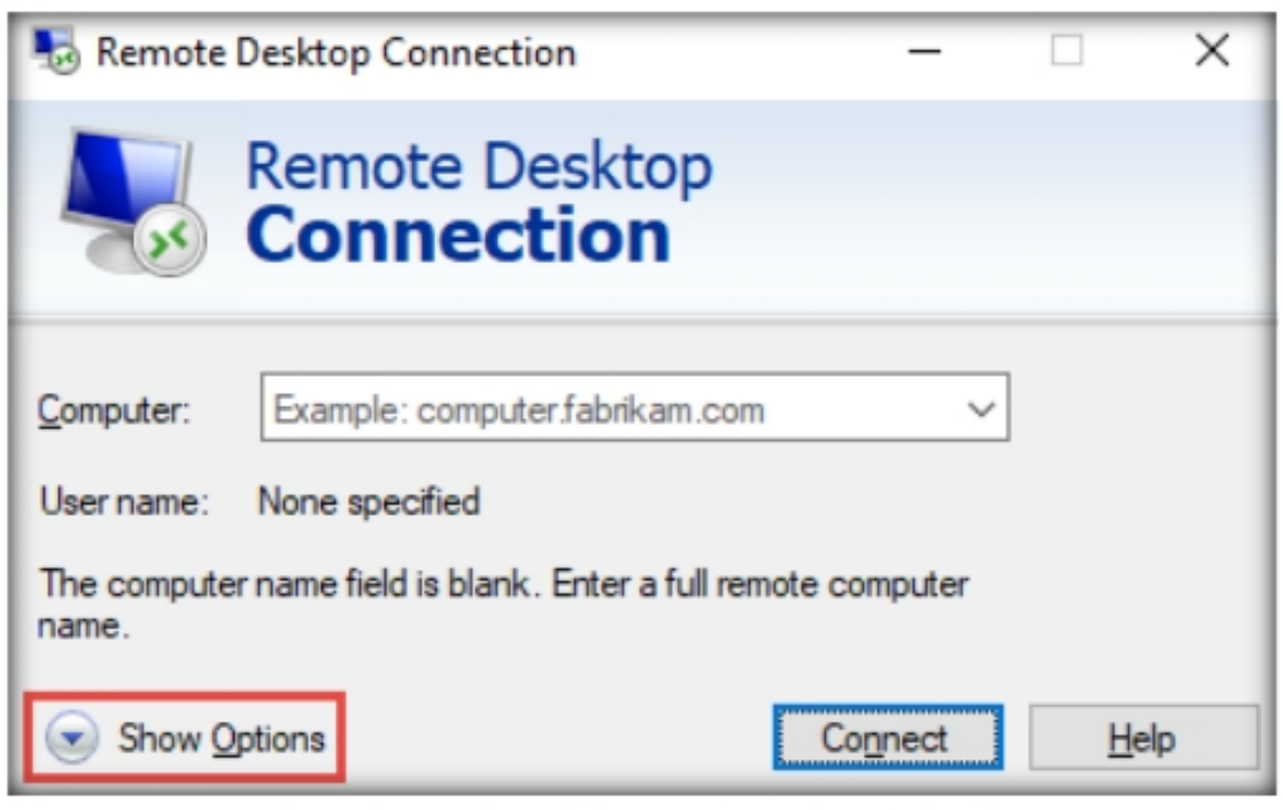


Figure 2.1.14: Remote Desktop Connection dialog box

25. The dialog-box expands; under the **General** tab, type **10.10.10.10** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

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

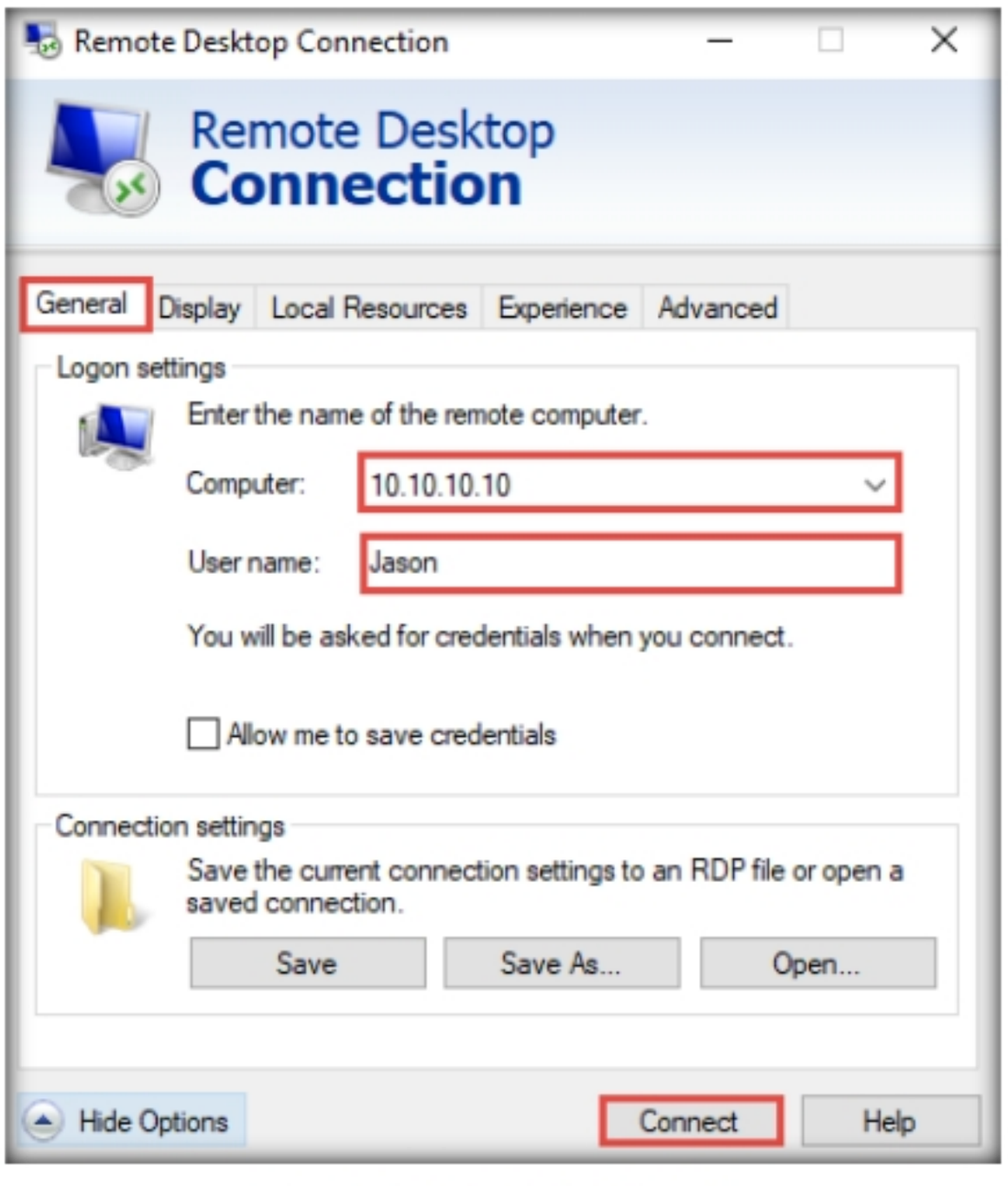


Figure 2.1.15: Connecting to remote desktop

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

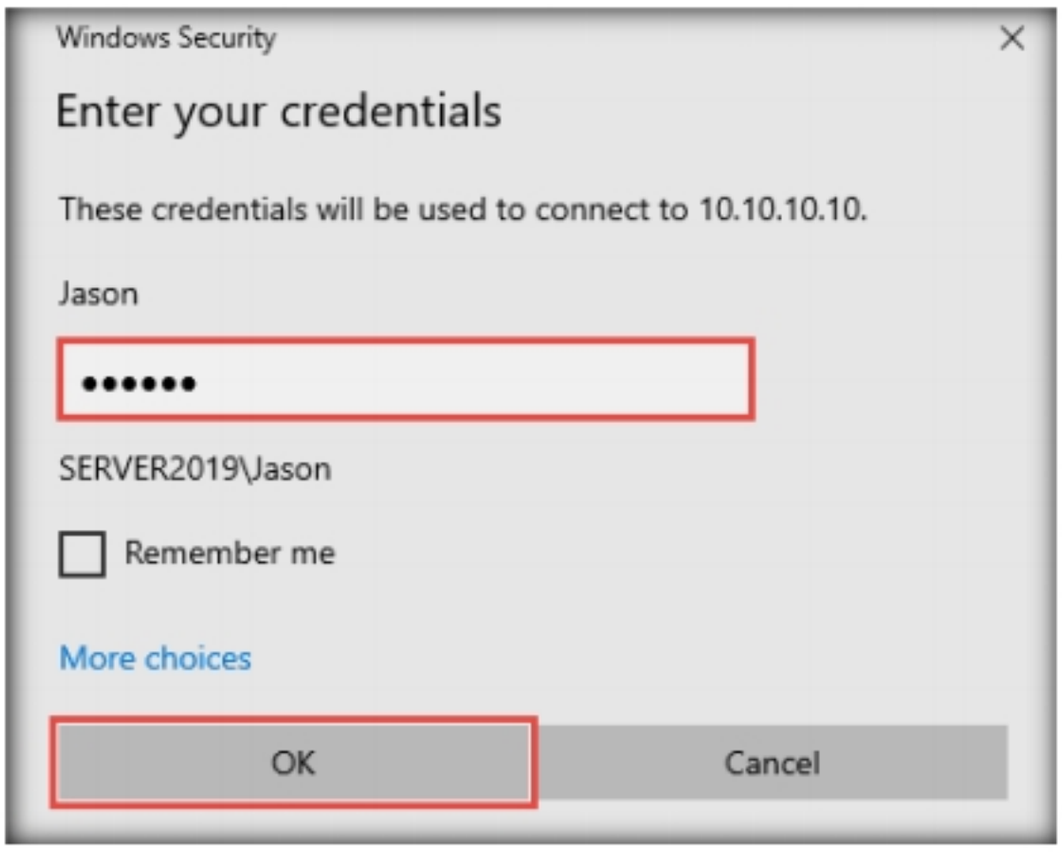


Figure 2.1.16: Entering credentials

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

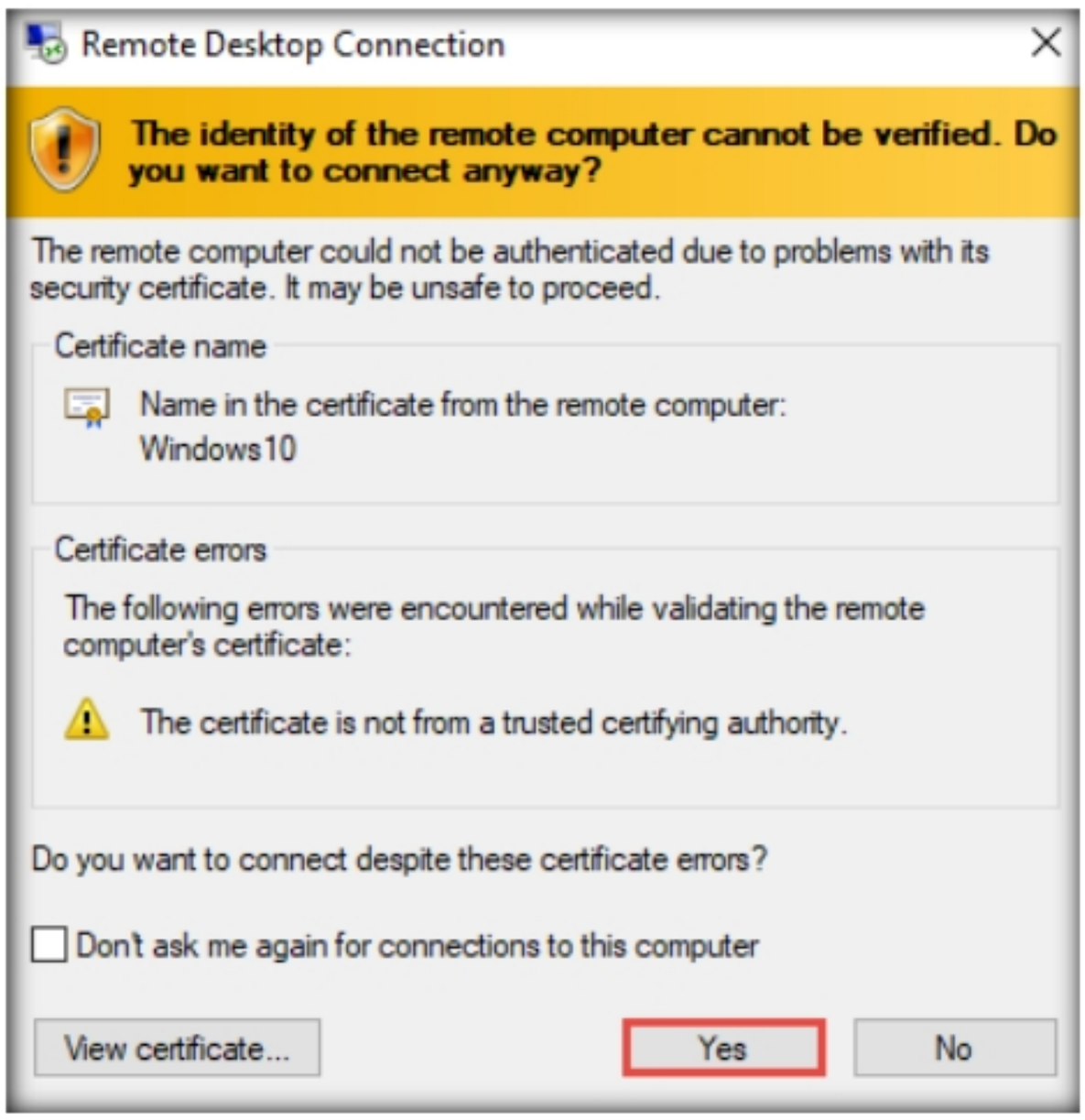


Figure 2.1.17: Establishing Remote Desktop Connection

28. A remote connection to the target system (**Windows 10**) appears, as shown in the screenshot.

Figure 2.1.18: Remote Desktop Connection successfully established

29. Click **Type here to search** at the bottom of **Desktop** and type **Control**. Click **Control Panel** from the results.

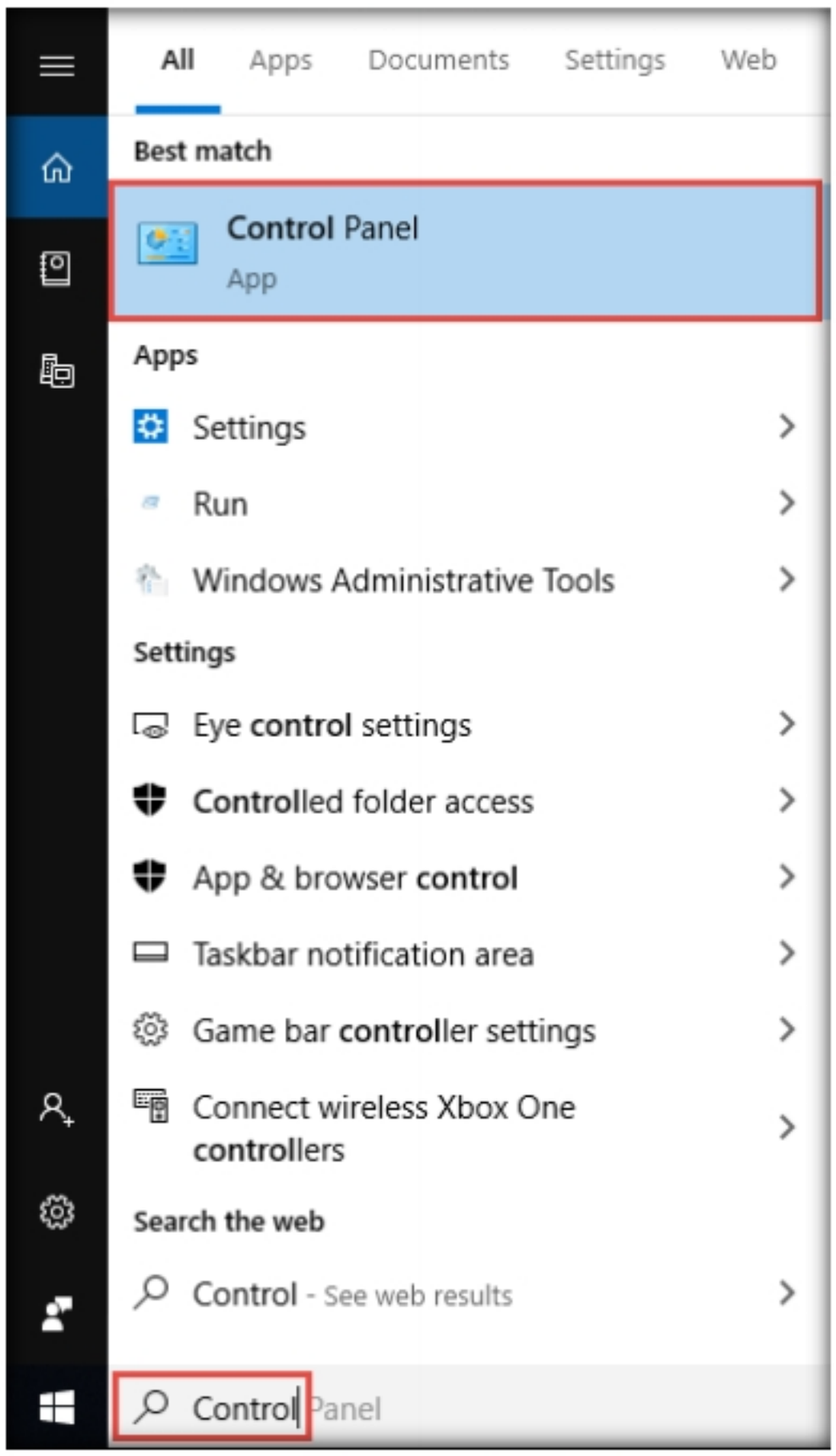


Figure 2.1.19: Selecting a Control Panel

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

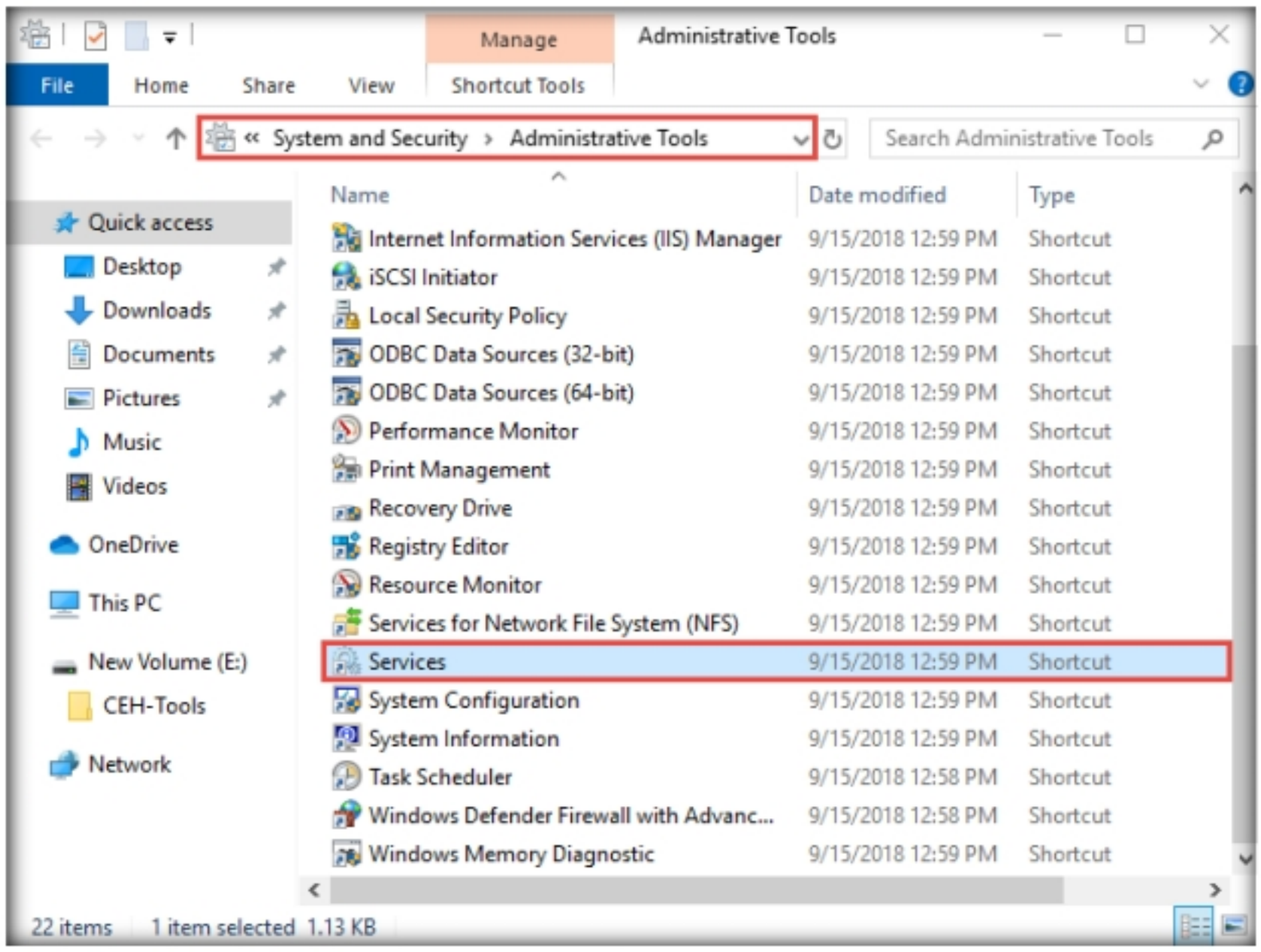


Figure 2.1.20: Administrative Tools: selecting Services

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

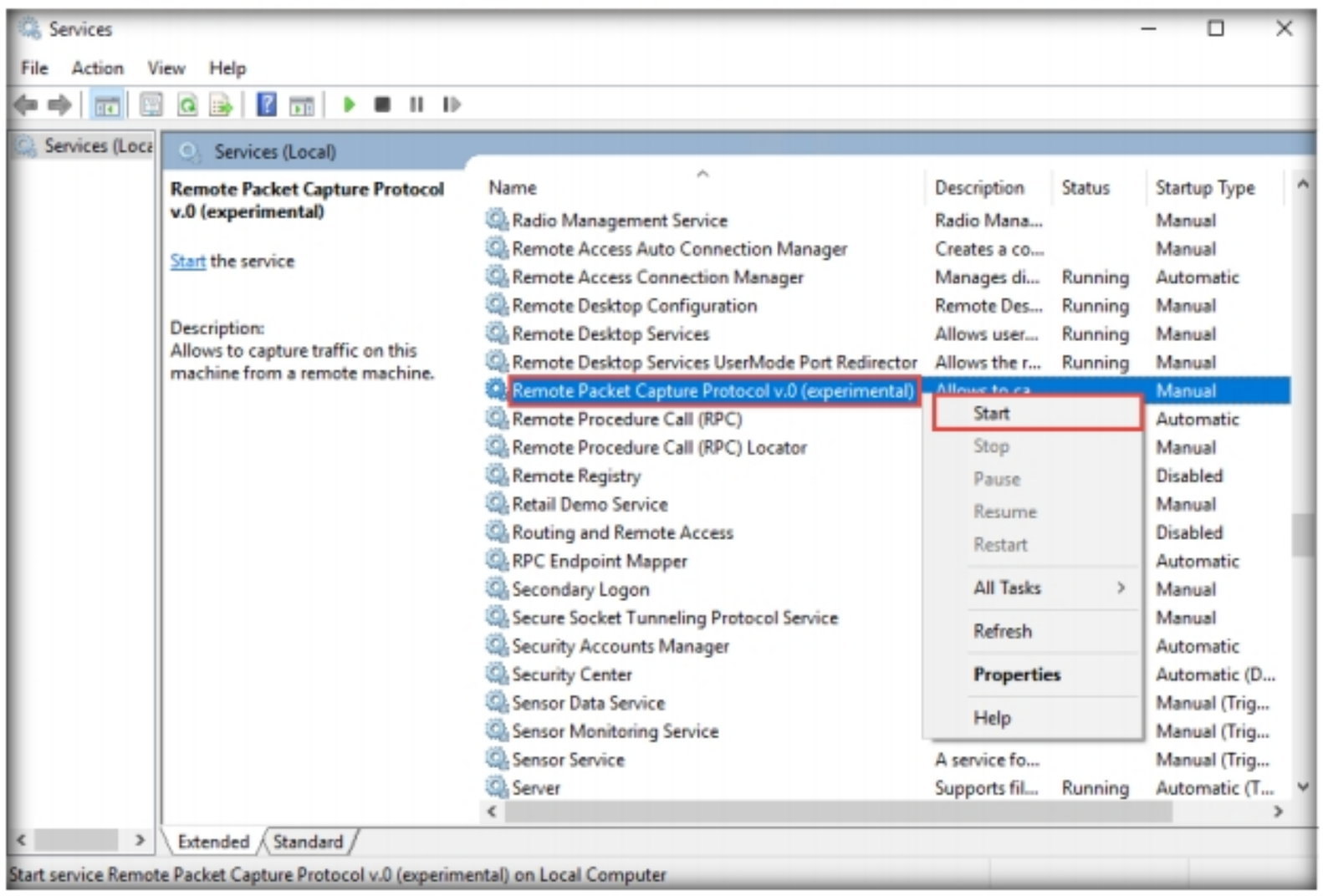


Figure 2.1.21: Starting Remote Packet Capture Protocol v.0

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

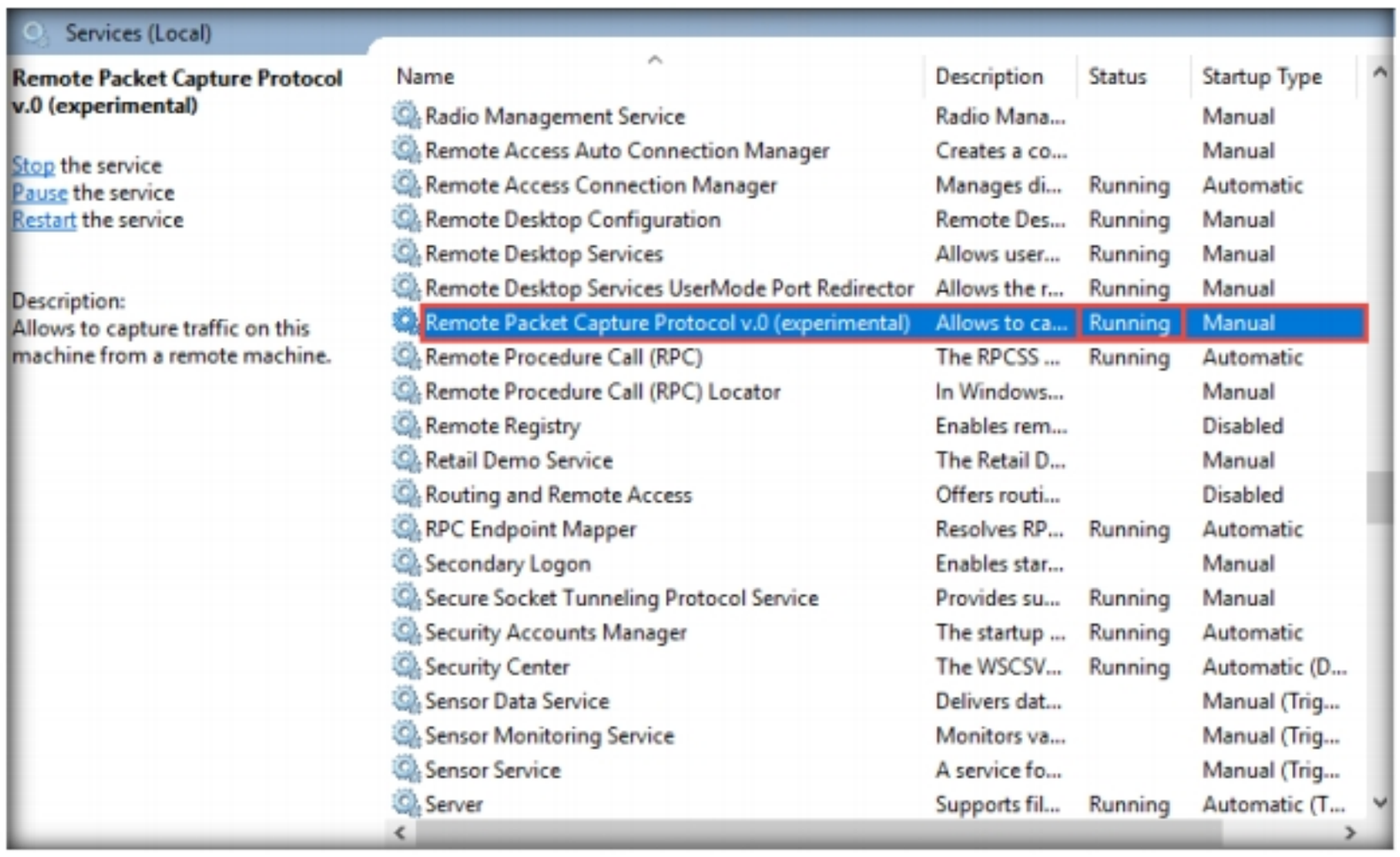


Figure 2.1.22: Running Remote Packet Capture Protocol v.0

33. Close all open windows on the **Windows 10** virtual machine and close **Remote Desktop Connection**.

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

34. Now, launch **Wireshark** by clicking the **Type here to search** icon ( ) at the bottom of **Desktop** and typing **wireshark**. Click **Wireshark** from the results.

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

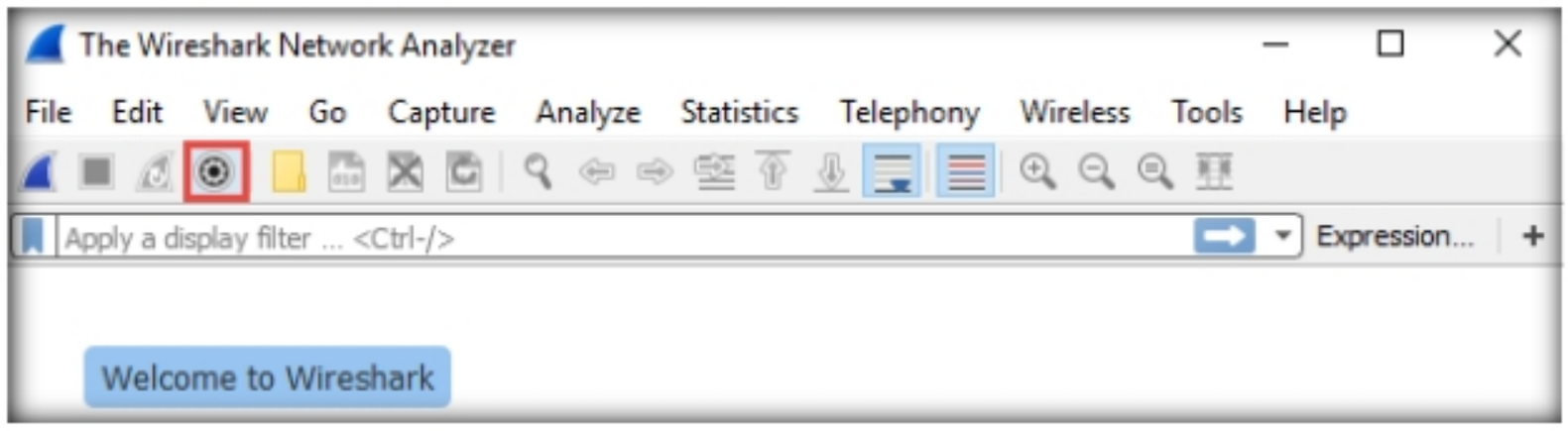


Figure 2.1.23: Selecting Options from Wireshark

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

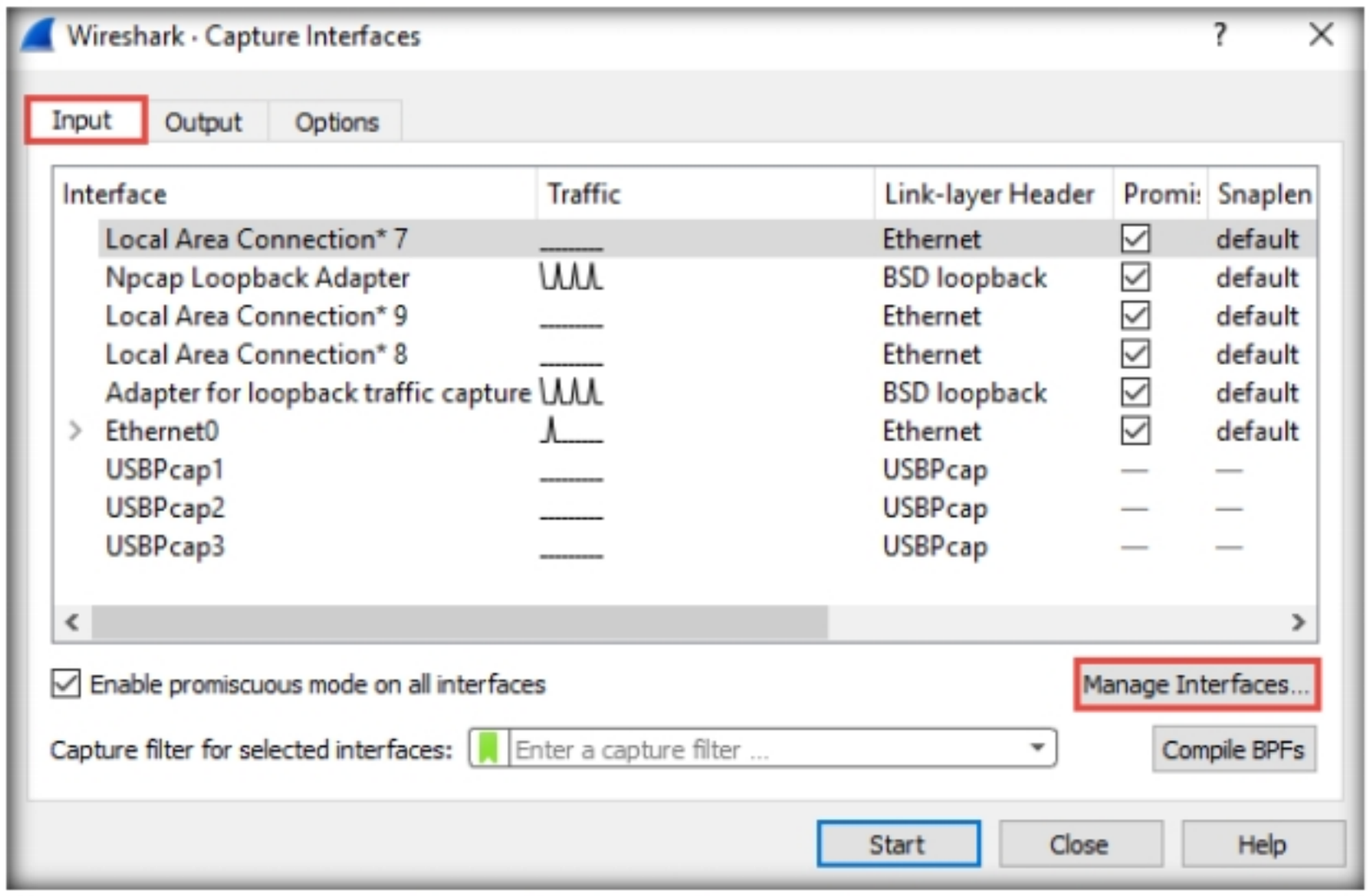


Figure 2.1.24: Selecting Options from Wireshark

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

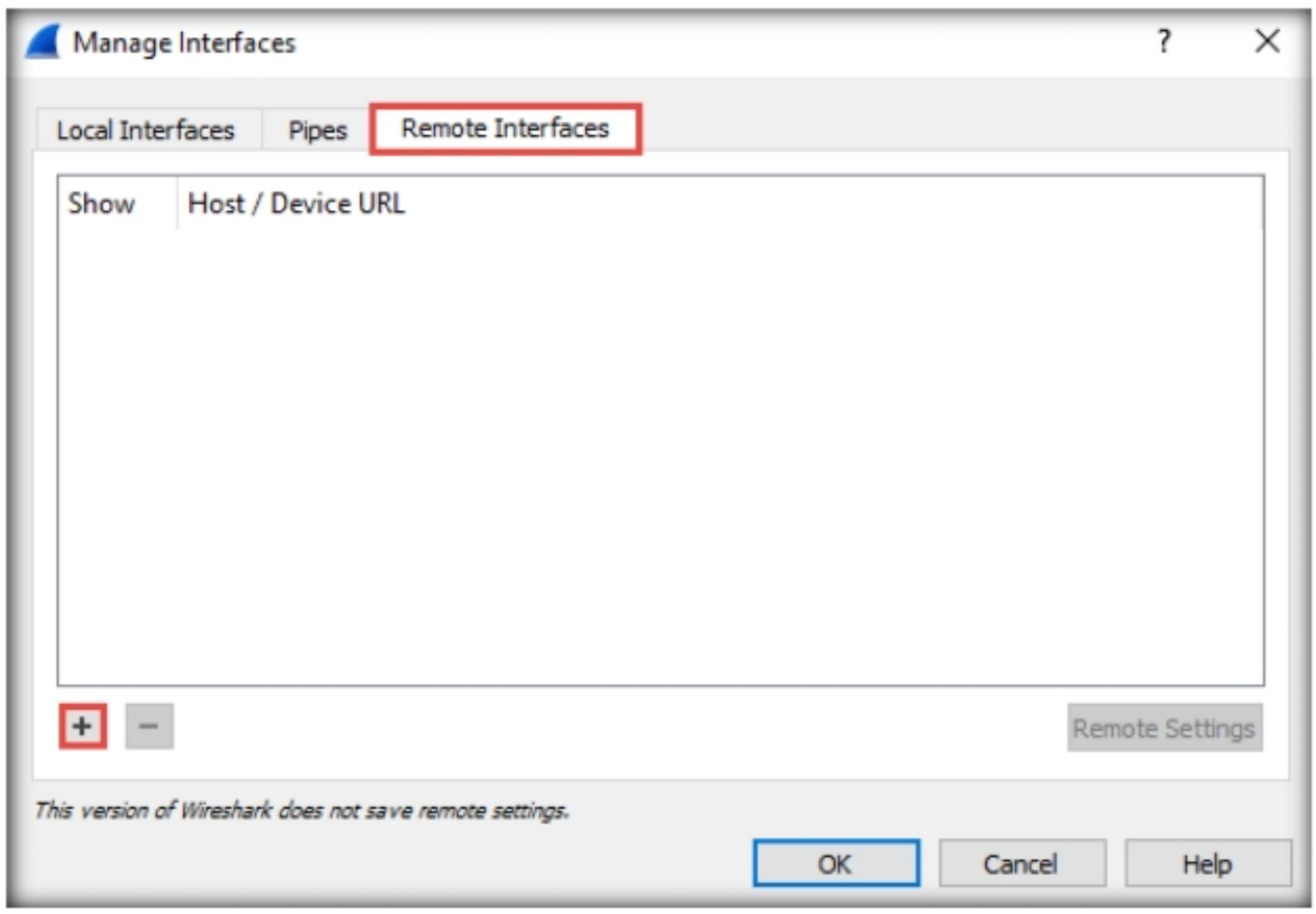


Figure 2.1.25: Interface Management window

38. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.10.10**); and in the **Port** field, enter the port number as **2002**.
39. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.

Note: The IP address and user credentials may differ in your lab environment.

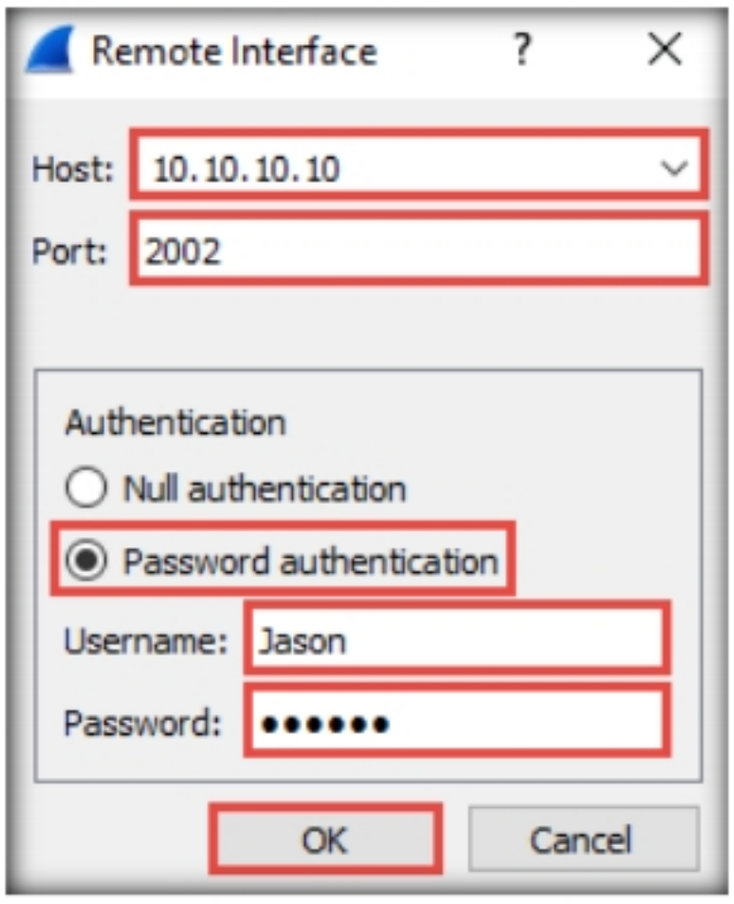


Figure 2.1.26: Wireshark: Remote Interface window

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

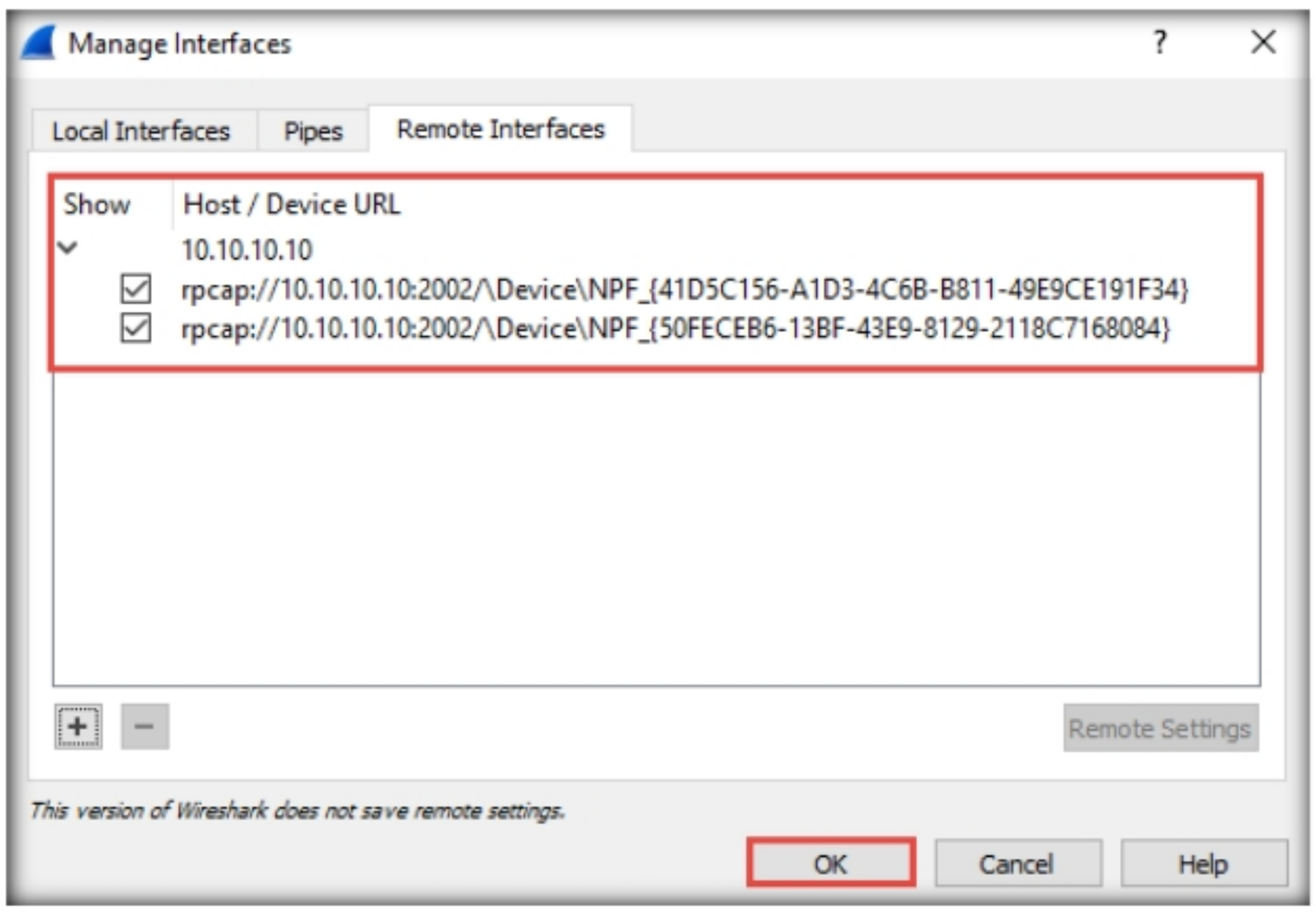


Figure 2.1.27: Applying the newly added interface

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

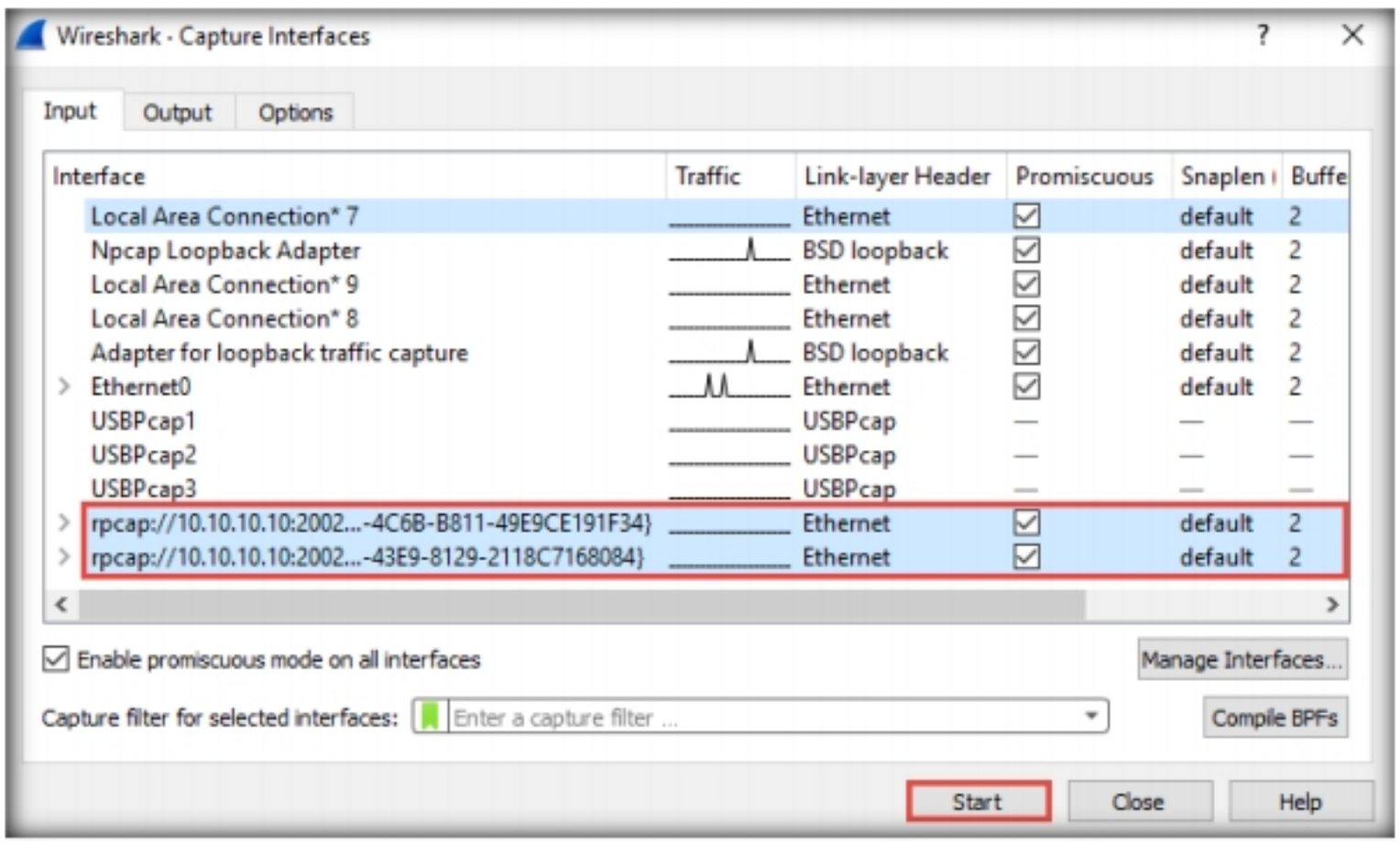


Figure 2.1.28: Wireshark: Capture Options window

42. Switch to the **Windows 10** virtual machine and sign in to the user account **Jason** with the password **qwerty**. Here, you are signing in as the victim.
43. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

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

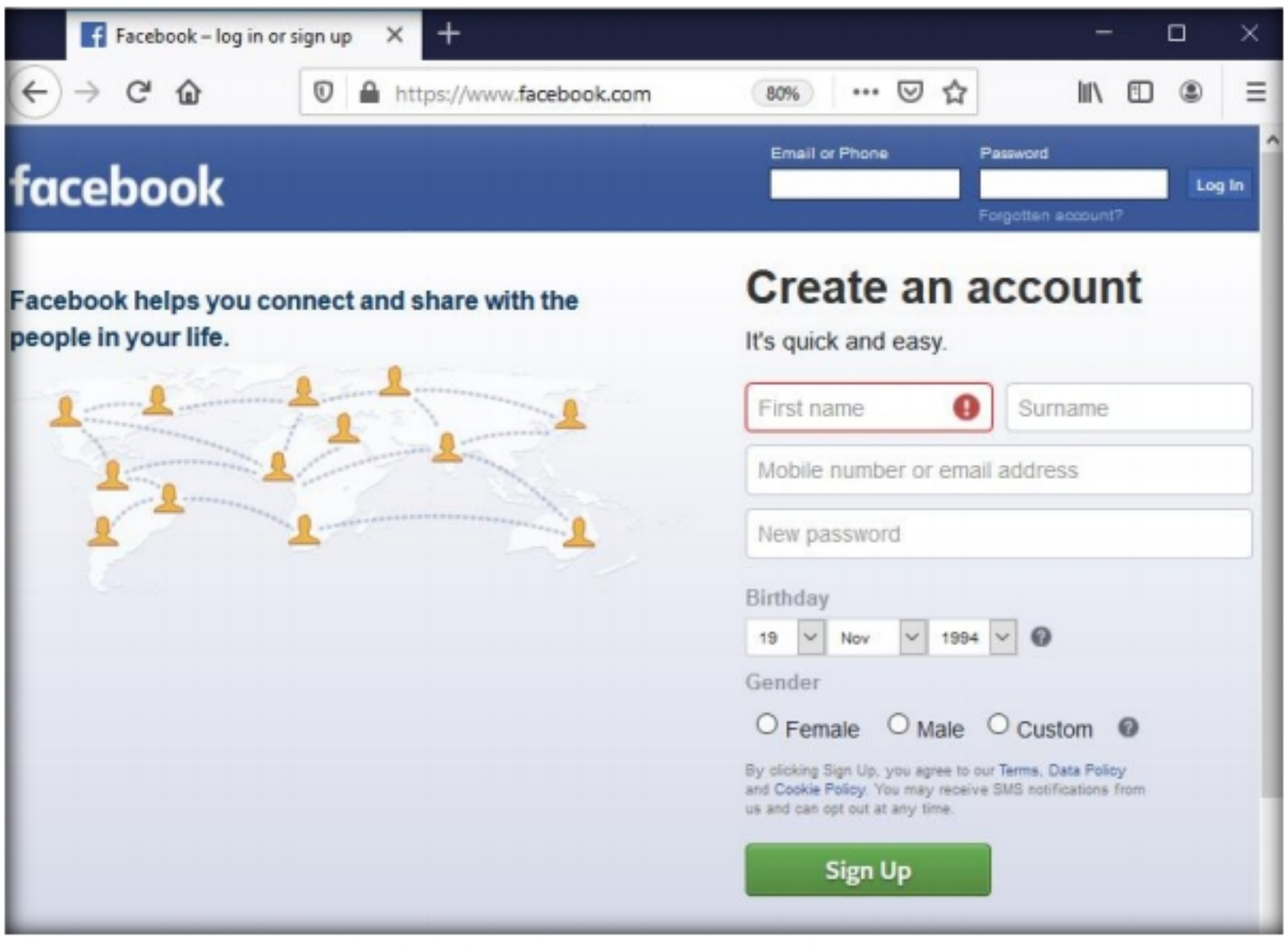


Figure 2.1.29: Browsing the Internet on Windows 10

44. Switch back to the **Windows Server 2019** virtual machine. **Wireshark** starts capturing packets as soon as the user (here, you) begins browsing the Internet, the shown in the screenshot.

45. You can see the websites browsed by the victim on the target system in the **Info** section.

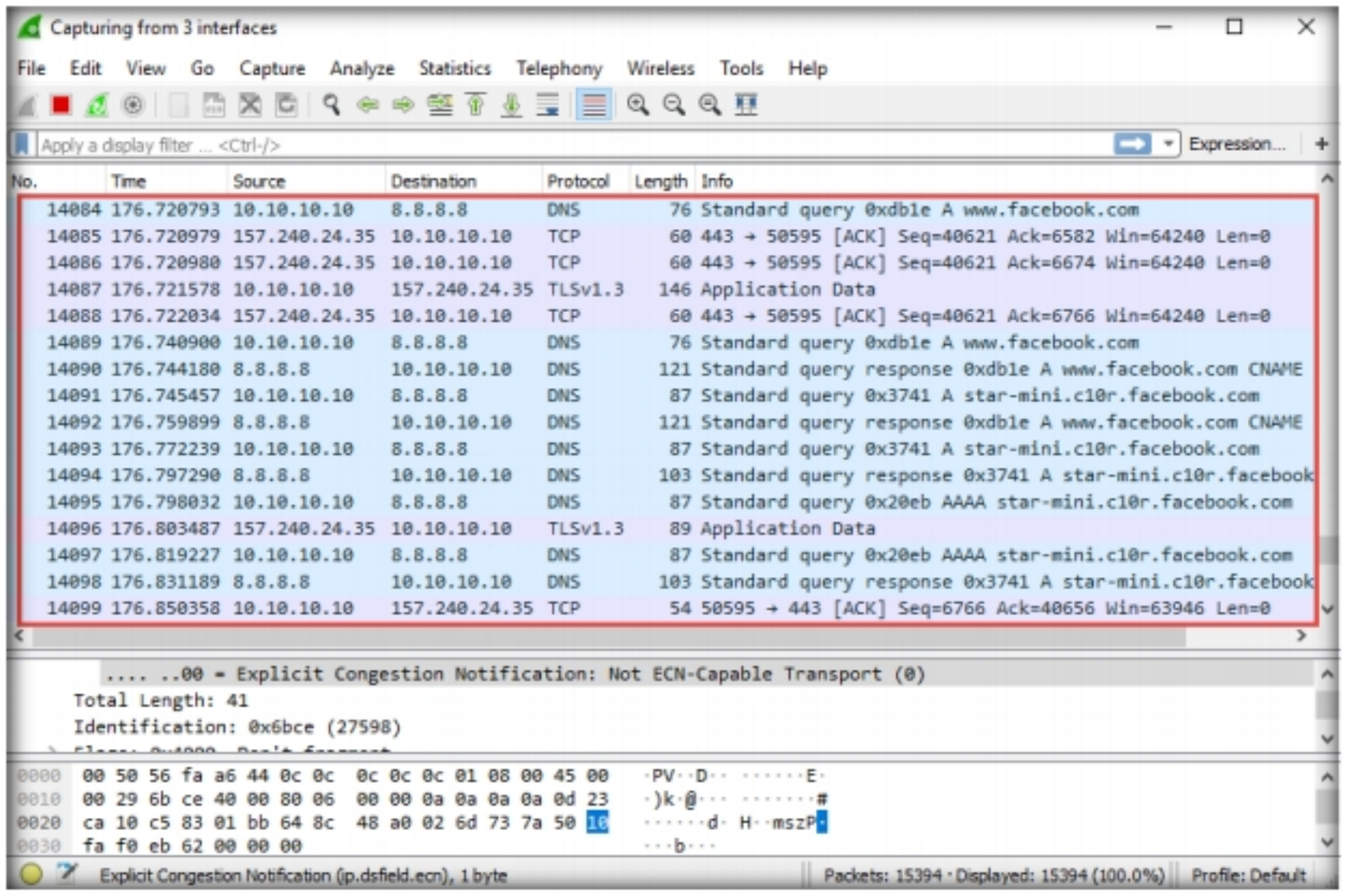


Figure 2.1.30: Wireshark Window with Packets Captured

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

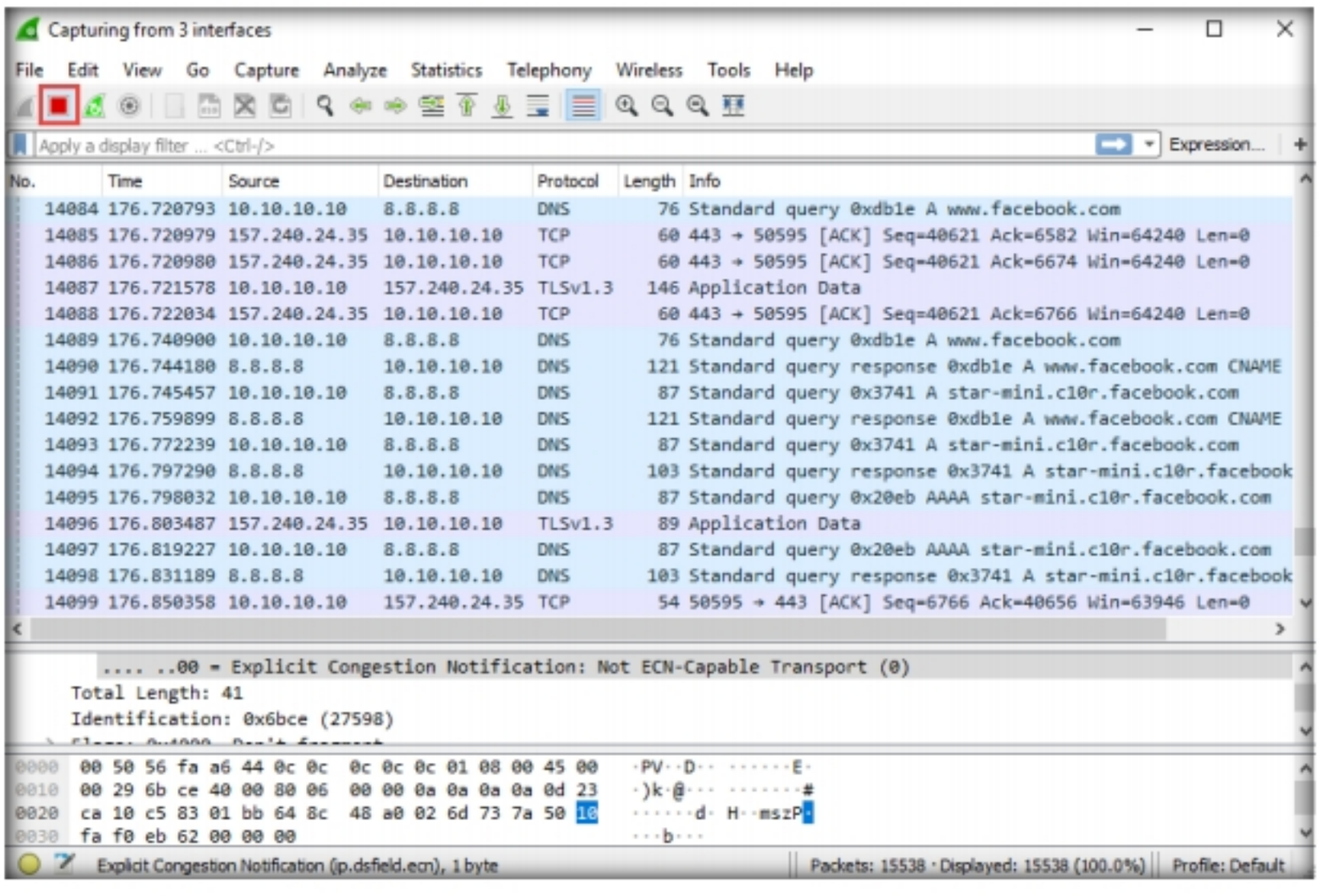


Figure 2.1.31: Stopping the running live capture

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

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

48. This concludes the demonstration of how to perform password sniffing using Wireshark.
49. Close all open windows and document all the acquired information.
50. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

TASK 2 — Analyze a Network using the Capsa Network Analyzer

Here, we will use the Capsa Network Analyzer tool to analyze the network.

Note: Capsa Network Analyzer requires a large amount of memory to analyze the network successfully. Therefore, before starting this task, we must increase the **Memory** (RAM) of the **Windows 10** virtual machine from **2 GB** to **6 GB**. To do so, perform **Steps # 1-4**.

TASK 2.1 — Increase Windows 10 Memory (RAM)

1. In your main system, open the **VMware Workstation Pro** application, and click on the **Windows 10** operating system from the left-hand pane.
2. A **Windows 10** node appears. Under the **Devices** section, click the **Memory** option.

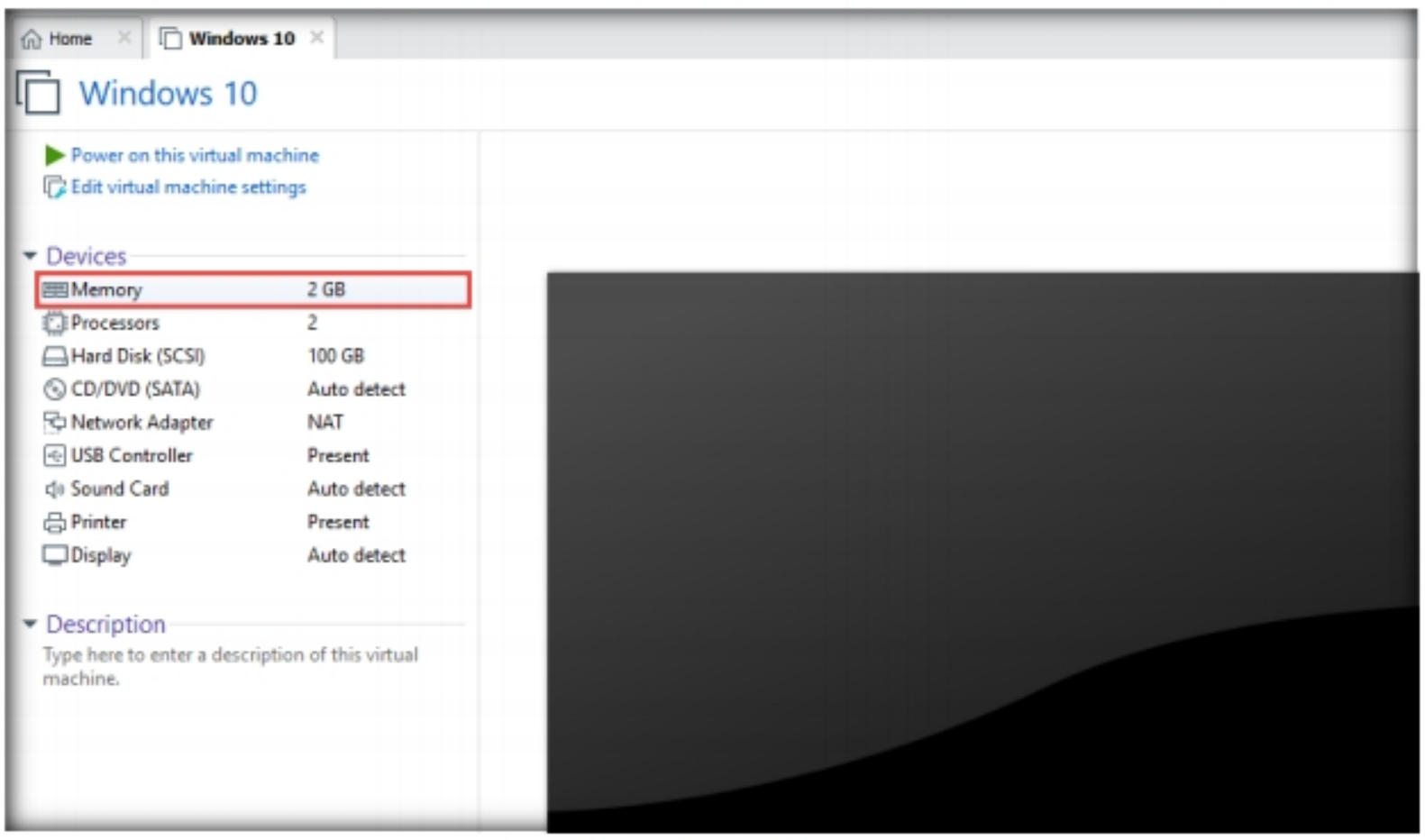


Figure 2.2.1: Windows 10 settings

Capsa is a portable network analysis application for both LANs and WLANs, which performs real-time packet capturing, 24x7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It goes one step ahead of sniffing by intuitively analyzing network packets and generating meaningful information.

3. The **Virtual Machine Settings** window appears. In the right-hand pane, toggle the slide bar in the **Memory** section to change **Memory for this virtual machine** to **6 GB** or **6144 MB**, and click **OK**.

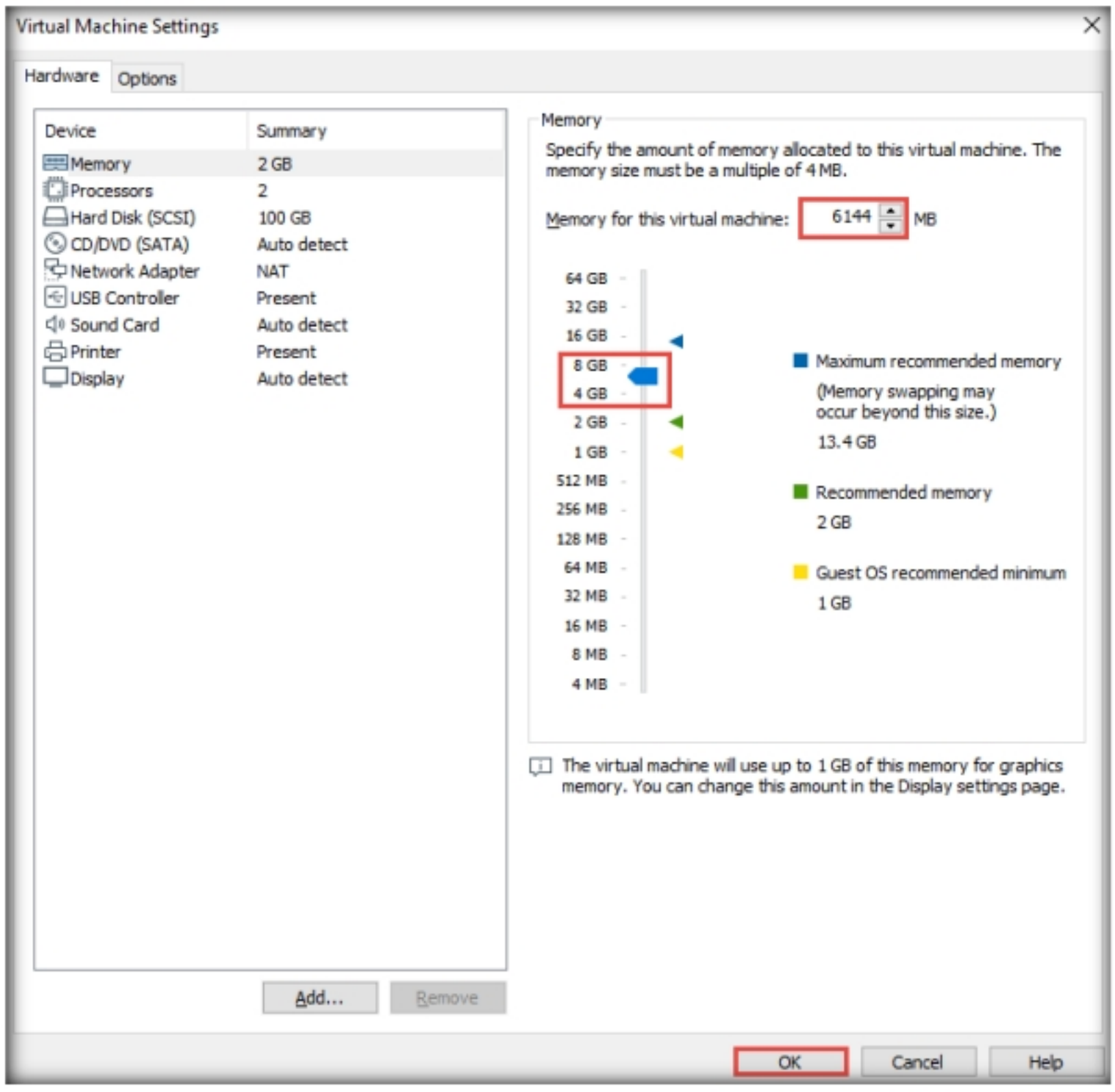


Figure 2.2.2: Windows 10: Increasing memory

Capsa's comprehensive high-level window view of the entire network gives network administrators and engineers quick insight, allowing them to pinpoint and resolve application problems rapidly.

4. Check the **Memory** option in the **Devices** section. It should have upgraded to **6 GB** from **2 GB**.

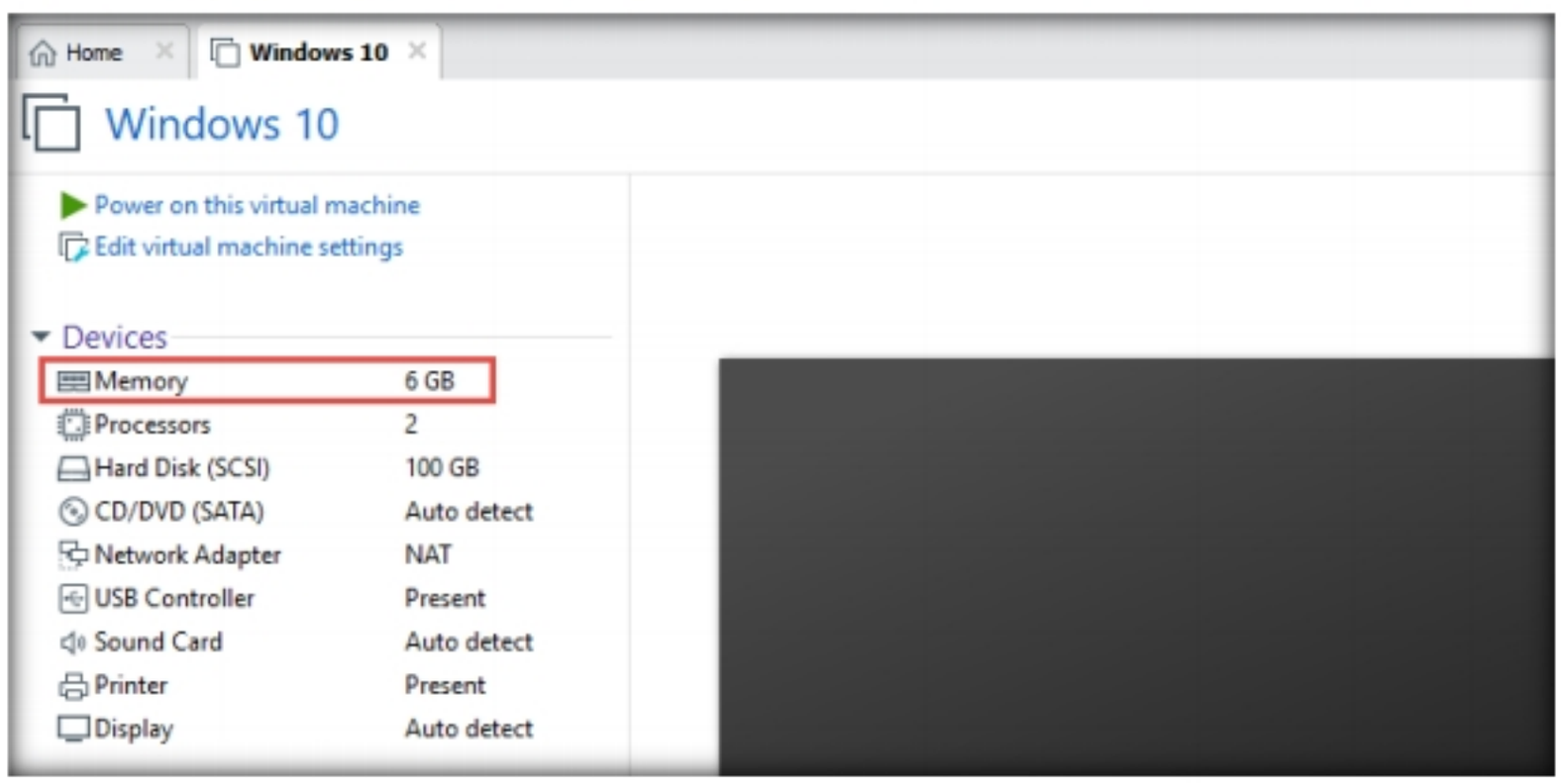


Figure 2.2.3: Windows 10: Memory

TASK 2.2

Download and Install Capsa Network Analyzer

5. Turn on the **Windows 10** and **Windows Server 2016** virtual machines.
6. Log on to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.
7. Open any web browser (here, **Mozilla Firefox**), type **https://www.colasoft.com/download/products/download_capsa.php** into the address bar, and press **Enter**.
8. The **Download Capsa Enterprise Trial** webpage appears; scroll down to the registration form and enter your personal details, as shown in the screenshot.

Note: You must give a **Valid, Non-Personal Email** (work or school accounts) during registration.

9. Untick the **Subscribe to our newsletter** checkbox and click the **30-Day Trial Download** button.

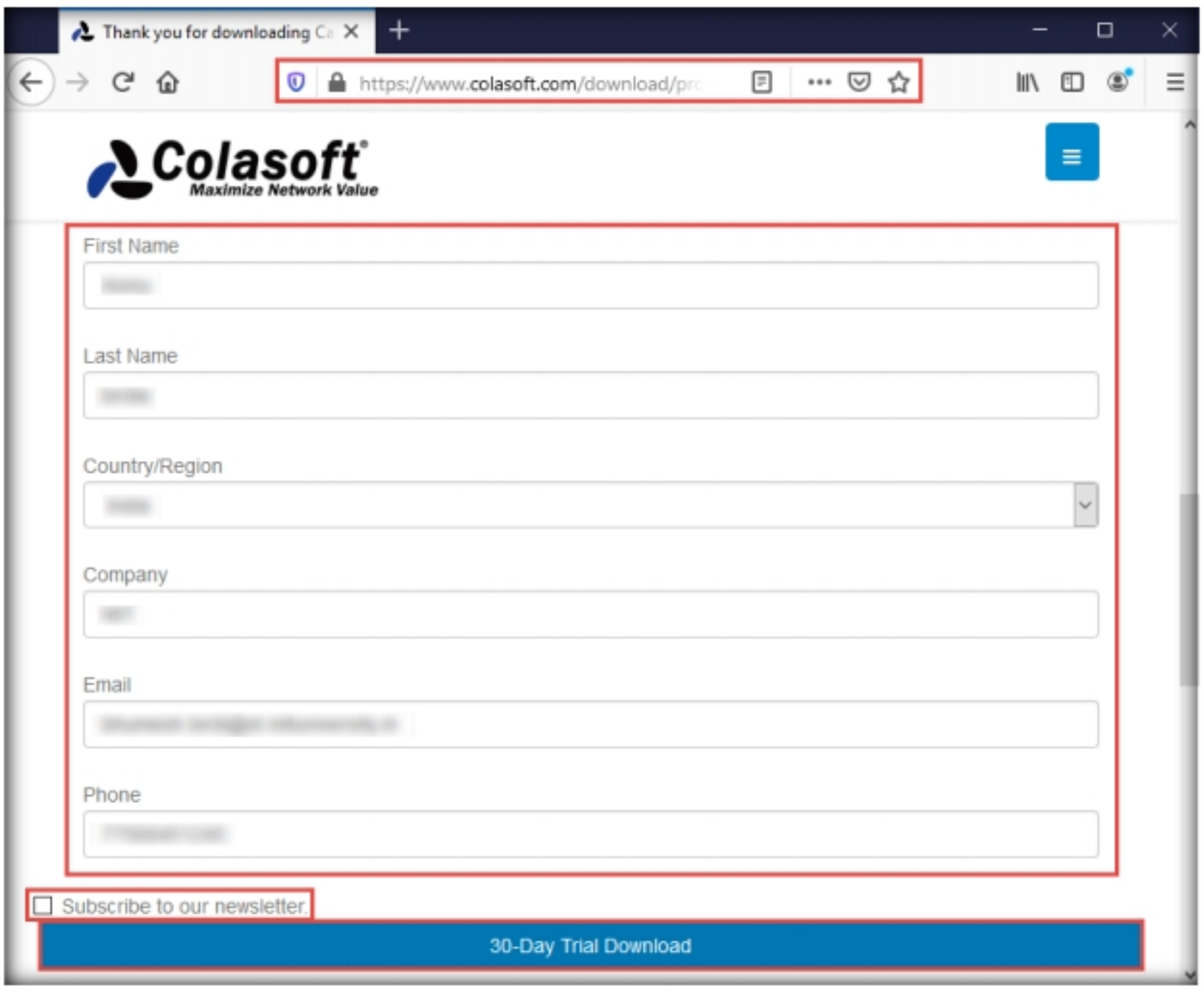


Figure 2.2.4: Colasoft Capsa online registration

10. The **Thank You for Downloading Our Product** page appears, along with the **Opening capsa_ent_12.0.6.12621_x64.exe** pop-up; click **Save**.
11. The **Capsa Network Analyzer** setup file starts to download.

12. After the file downloads, navigate to the download location (here, **Downloads**) and double-click on **capsa_ent_12.0.6.12621_x64.exe**.

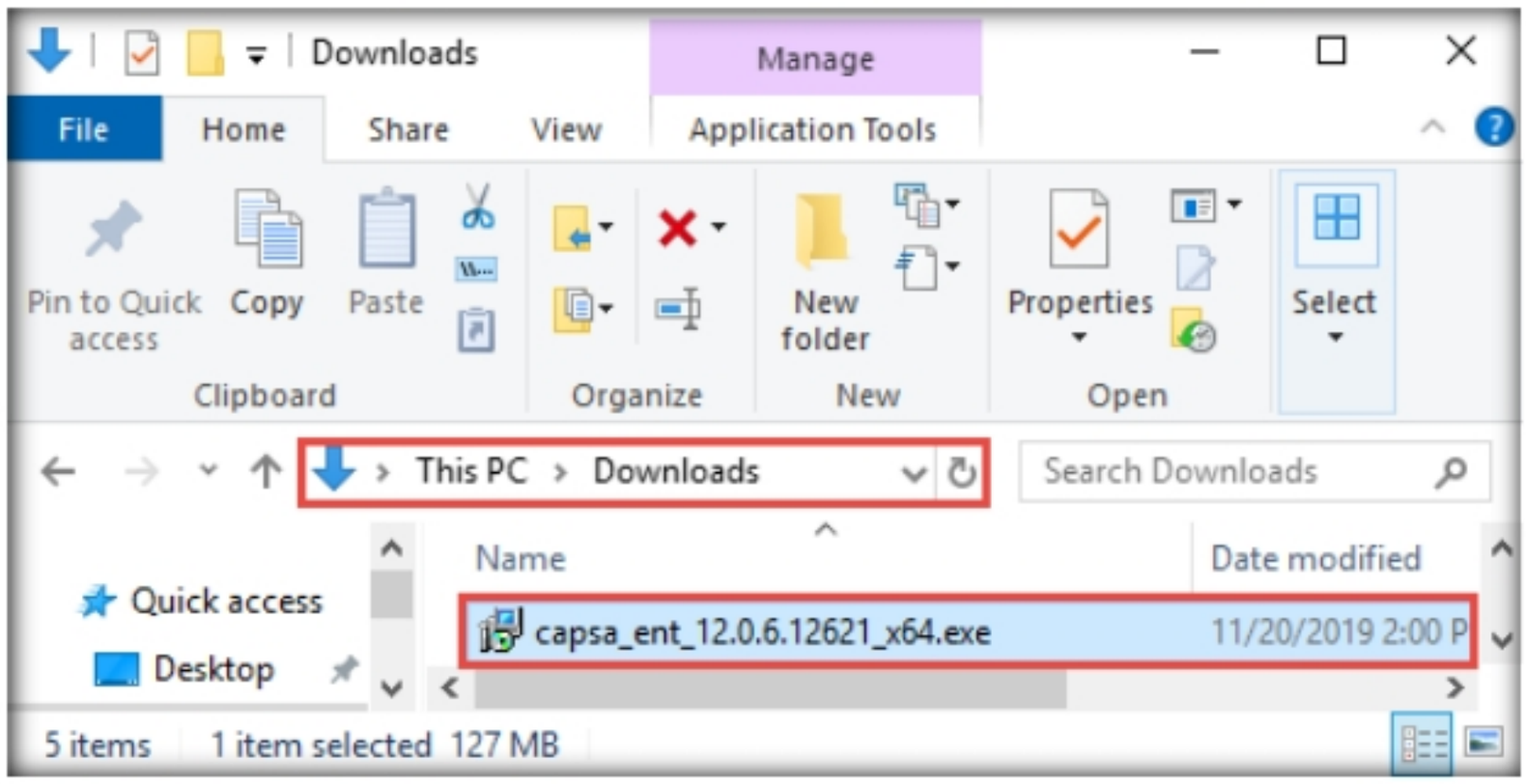


Figure 2.2.5: Colasoft Capsa setup

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

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

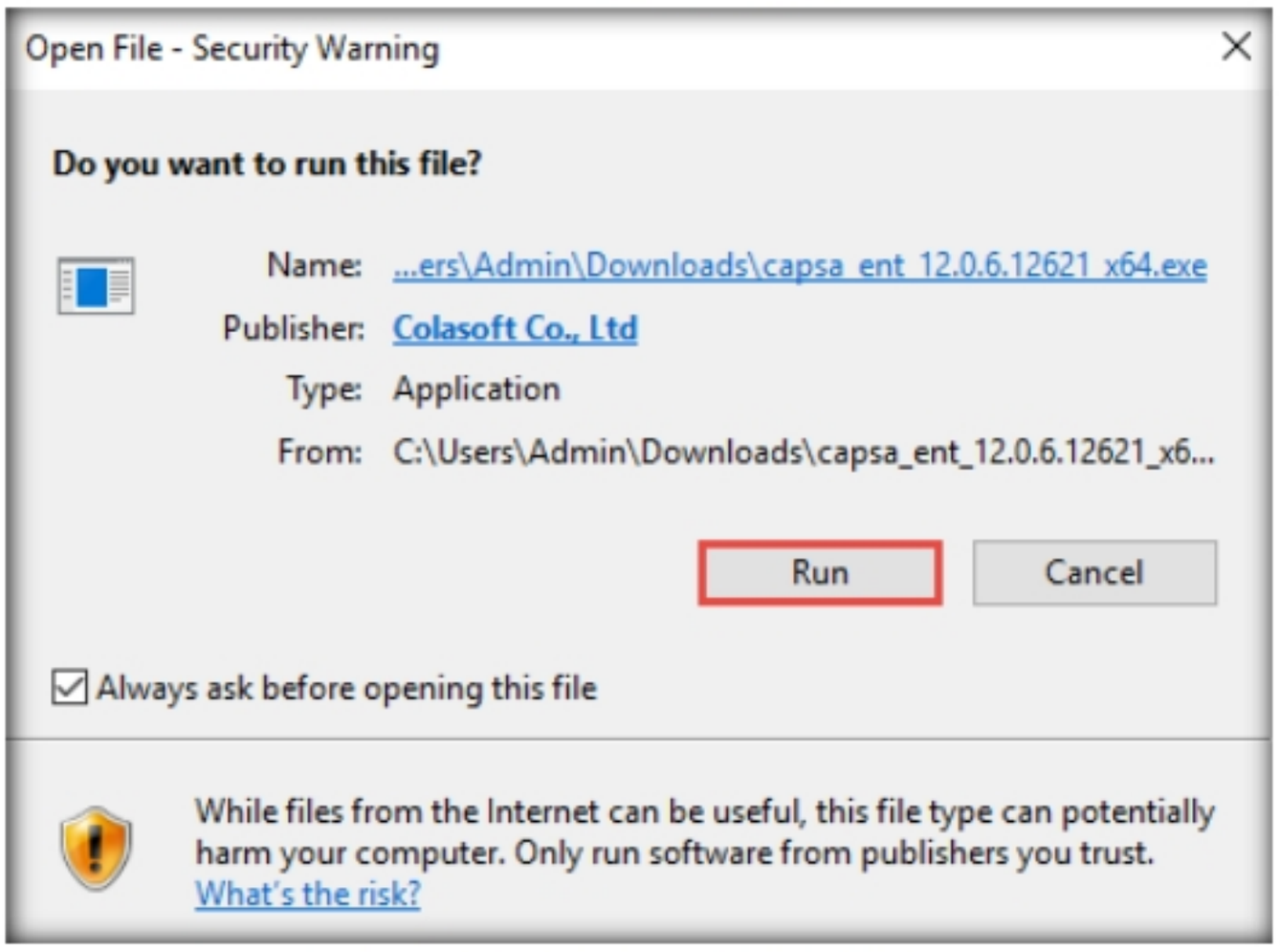


Figure 2.2.6: Open File: Security Warning window

14. The **Setup - Colasoft Capsa Enterprise** window appears; click **Next**.

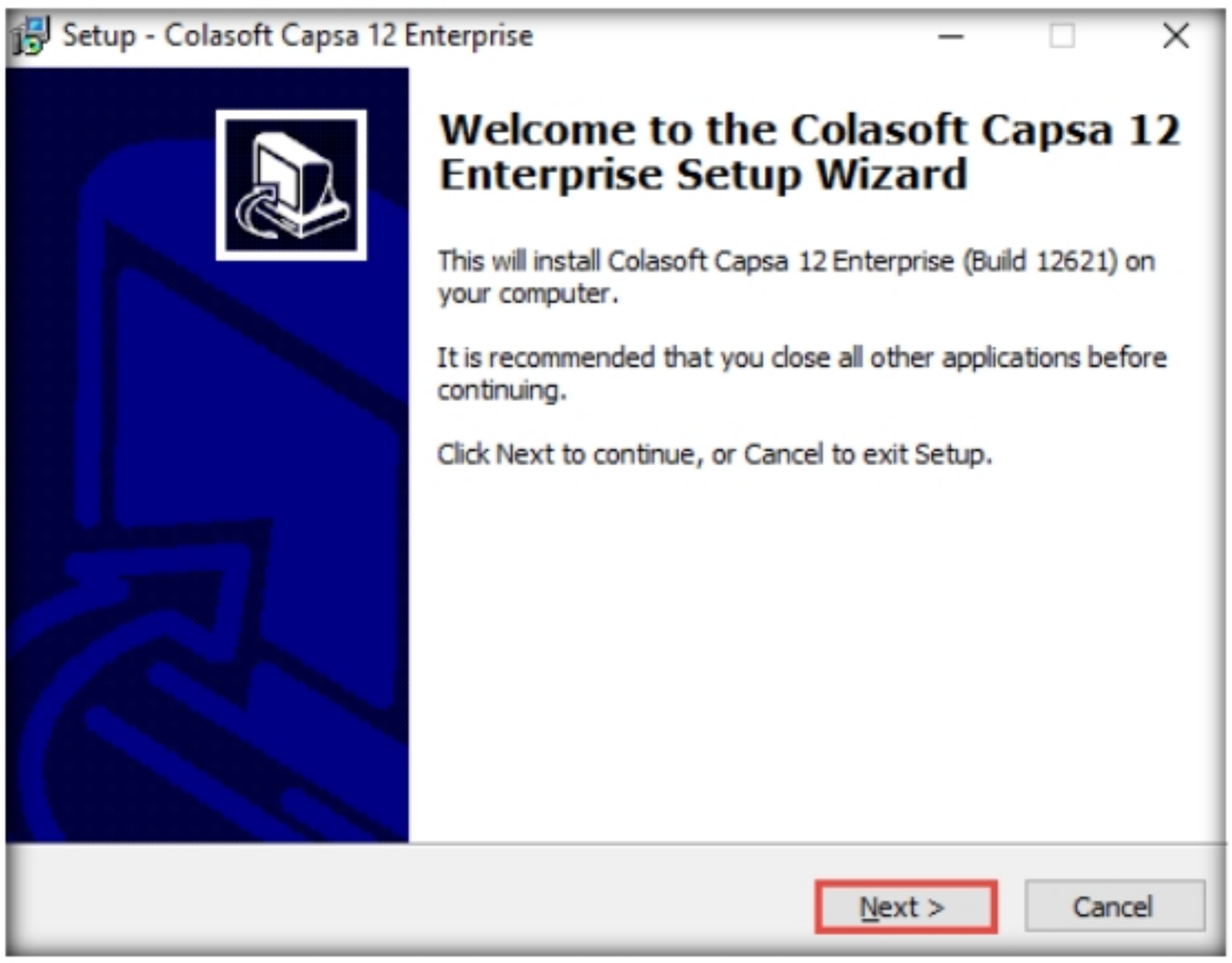


Figure 2.2.7: Colasoft Capsa installation wizard

15. Follow the wizard-driven installation steps to install Capsa Network Analyzer using the default settings.

16. On completion of the installation, the **Completing the Colasoft Capsa Enterprise Setup Wizard** screen appears. Ensure that the **Launch Program** checkbox is selected and click **Finish**.

Figure 2.2.8: Completion of Colasoft Capsa Setup

17. The **Colasoft Software Activation Wizard** window appears; click **Next**.

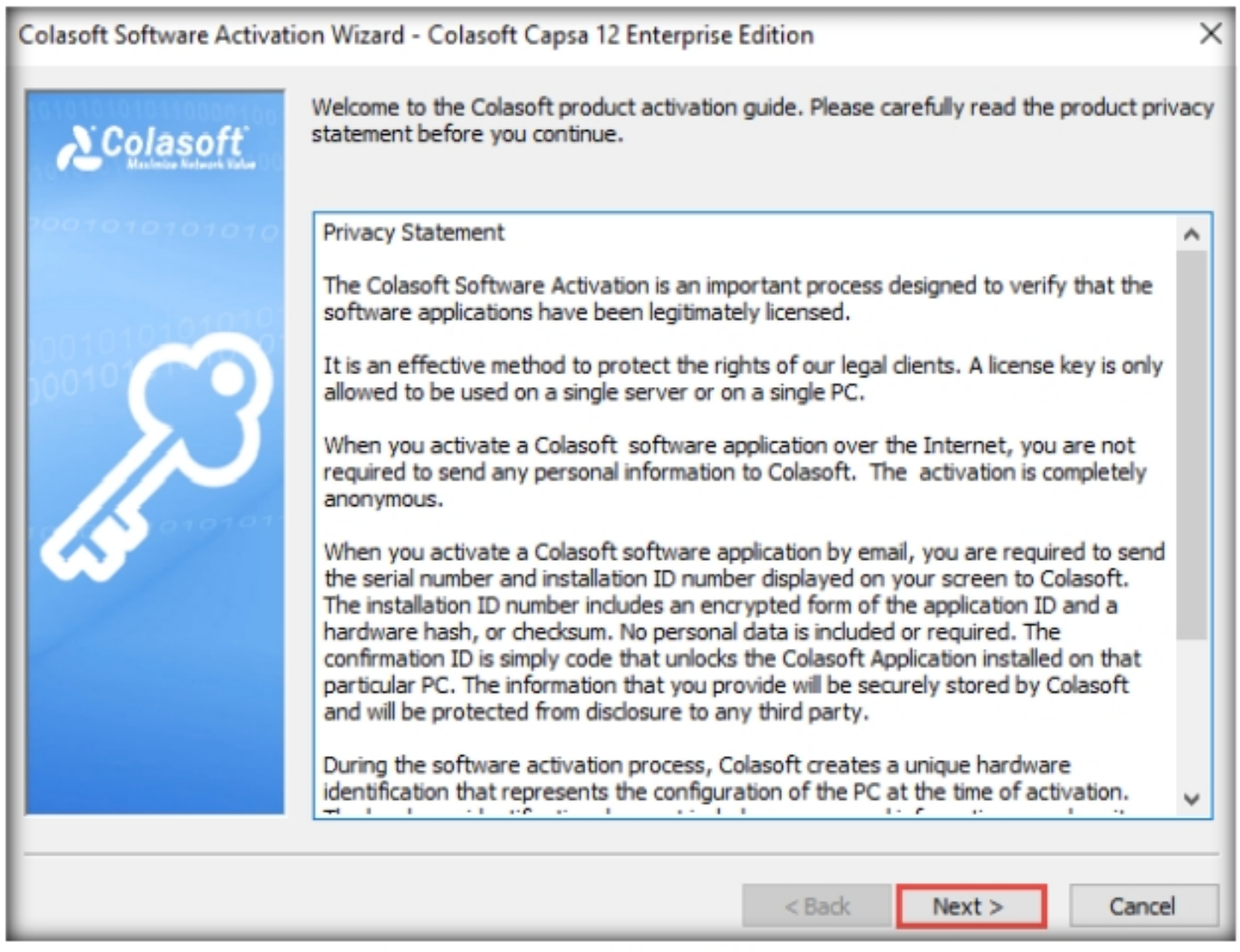


Figure 2.2.9: Colasoft Software Activation Wizard

18. Switch to the **Mozilla Firefox** browser, open a new tab, and log in to the email account you provided during registration. Open the mail from **Colasoft Capsa Packet Analyzer** and copy **Trial Serial Number**.

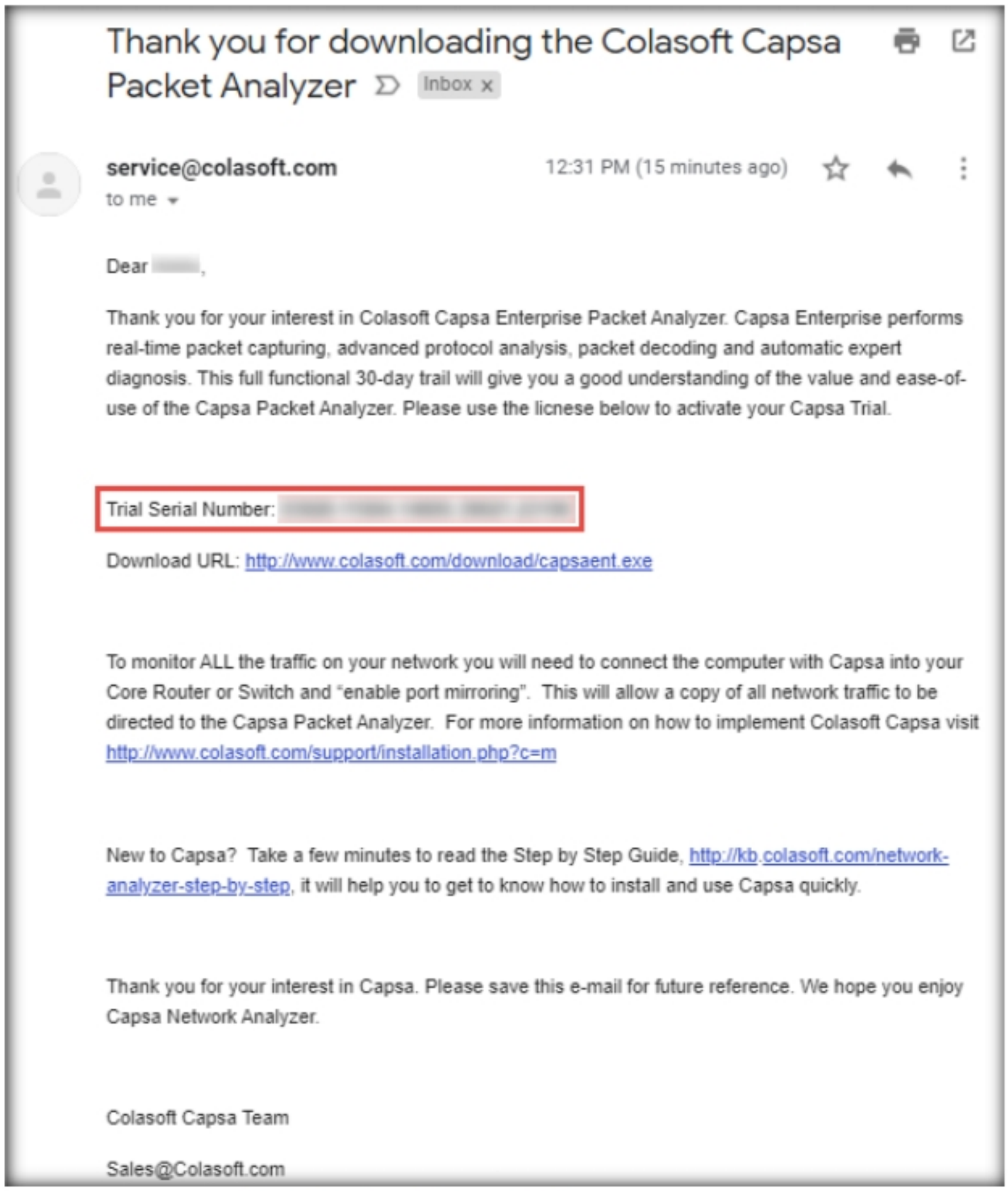


Figure 2.2.10: Colasoft Capsa Packet Analyzer: copy the trial key

TASK 2.3

Enter the Activation Code

19. Switch back to **Colasoft Software Activation Wizard** and paste the copied trial serial number into the **Serial Number** field. Ensure that the **Activate Online (Recommended)** radio button is selected; click **Next**.

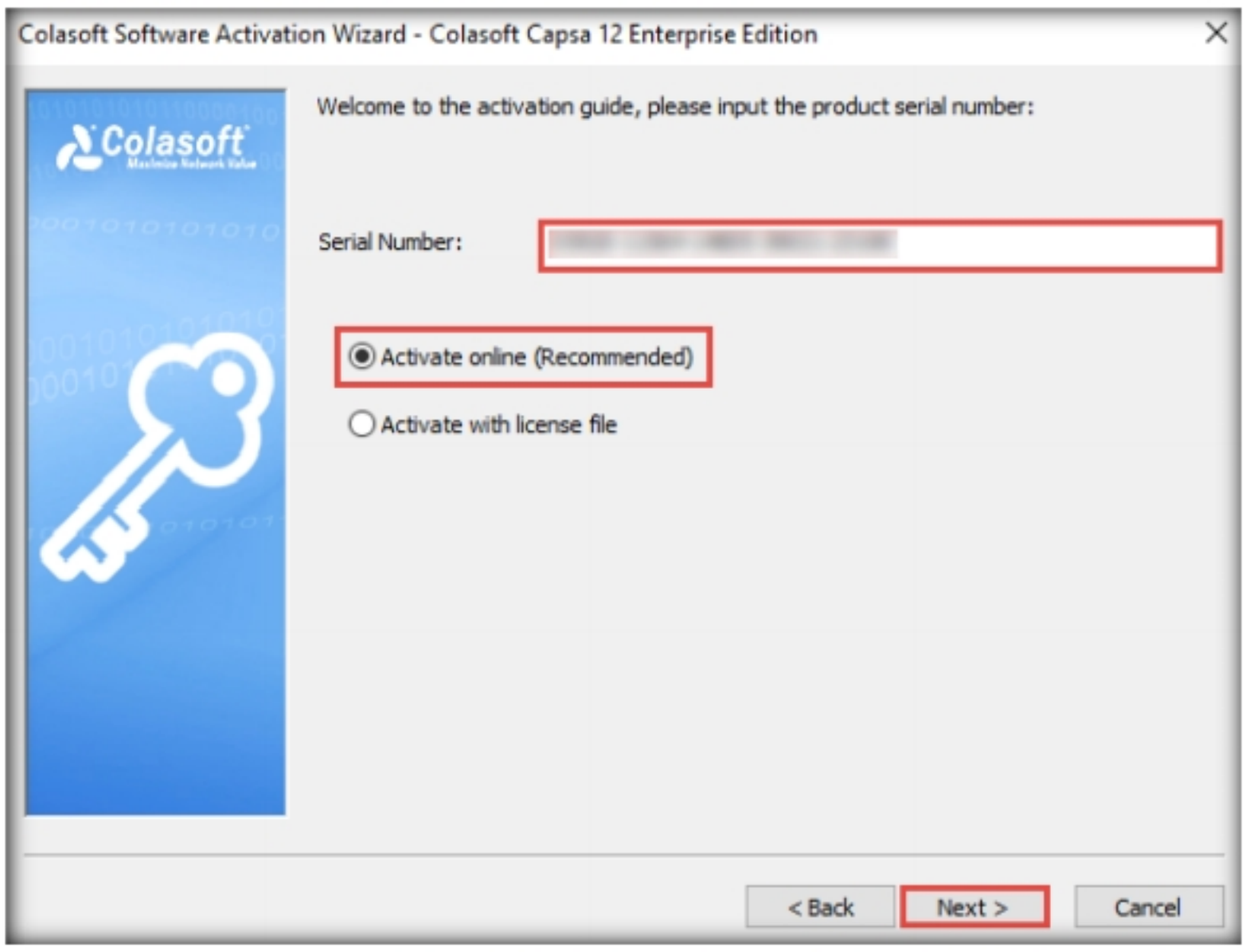


Figure 2.2.11: Colasoft Software Activation Wizard: paste the trial key

20. A "**The software has been successfully activated**" message appears; click **Finish**.

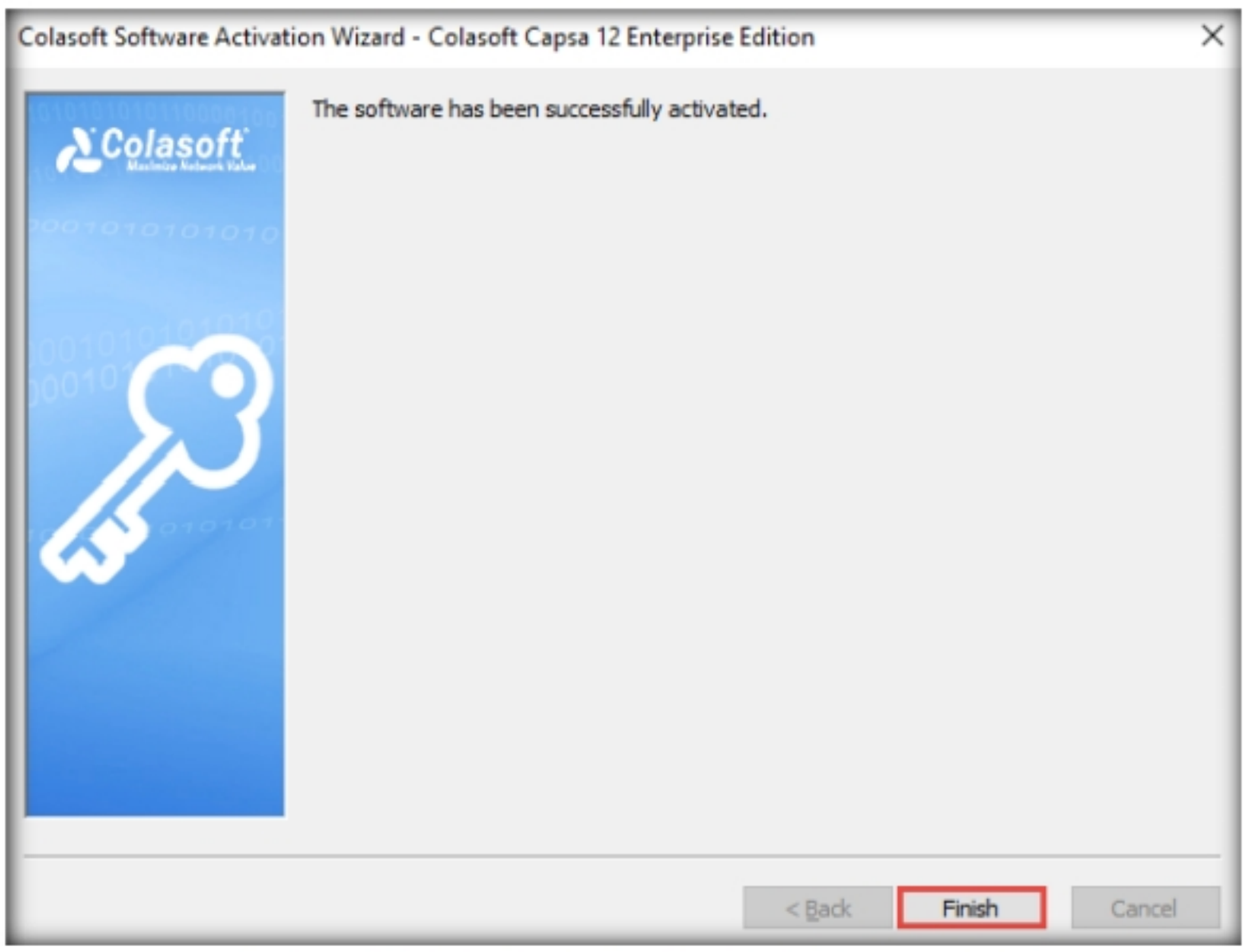


Figure 2.2.12: Colasoft Software Activation Wizard: activation successful

21. The **Colasoft Capsa Enterprise** main window appears, as shown in the screenshot.

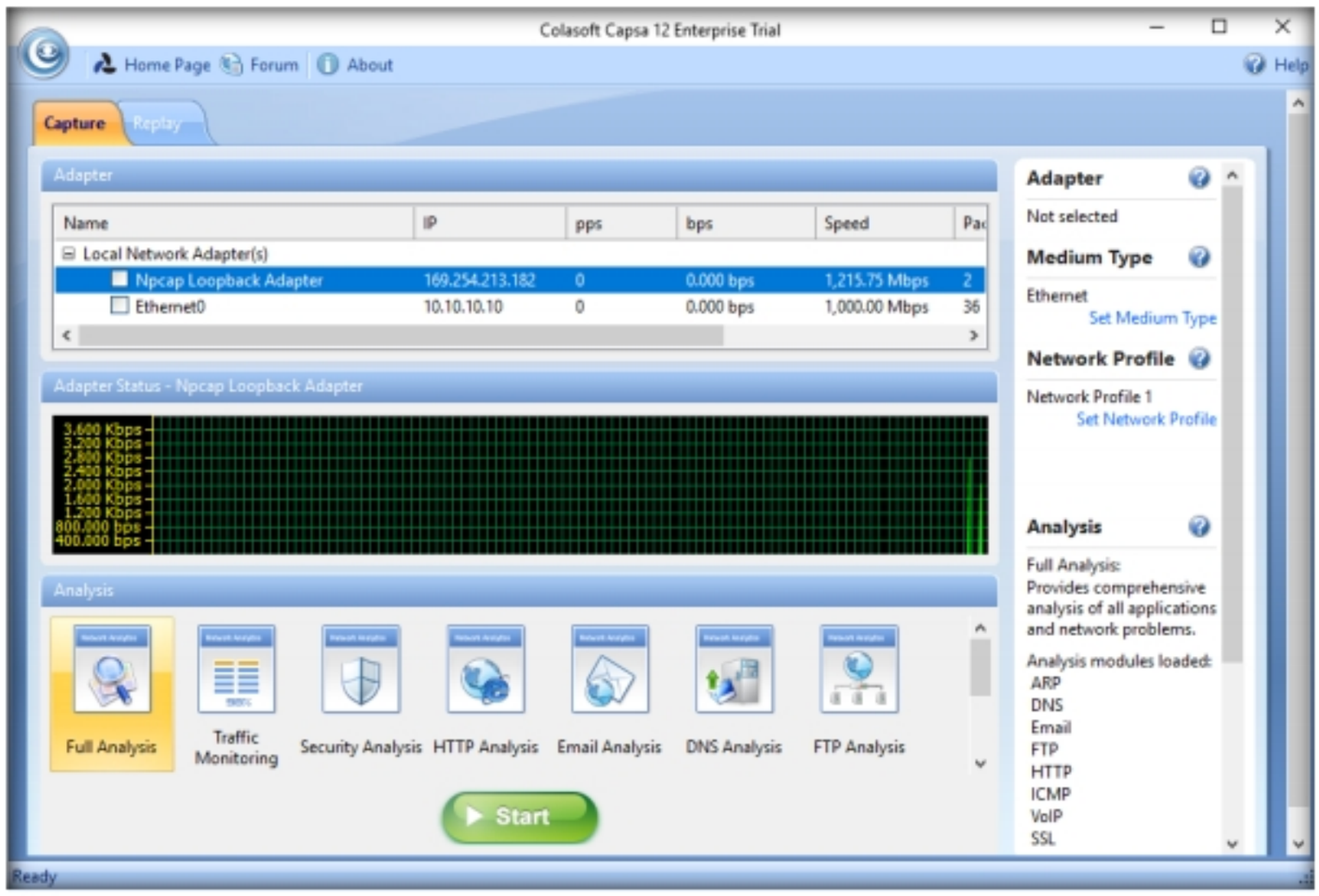


Figure 2.2.13: Colasoft Capsa Network Analyzer main window

TASK 2.4

Begin Packet Analysis

22. In the **Adapter** section, click the **Ethernet0** adapter checkbox. Ensure that the **Full Analysis** option is selected under the **Analysis** section. Click the **Start** button to create a New Project.

Note: The adapter might differ in your lab environment.

Note: If a **Security Warning** pop-up appears, click **Yes**.

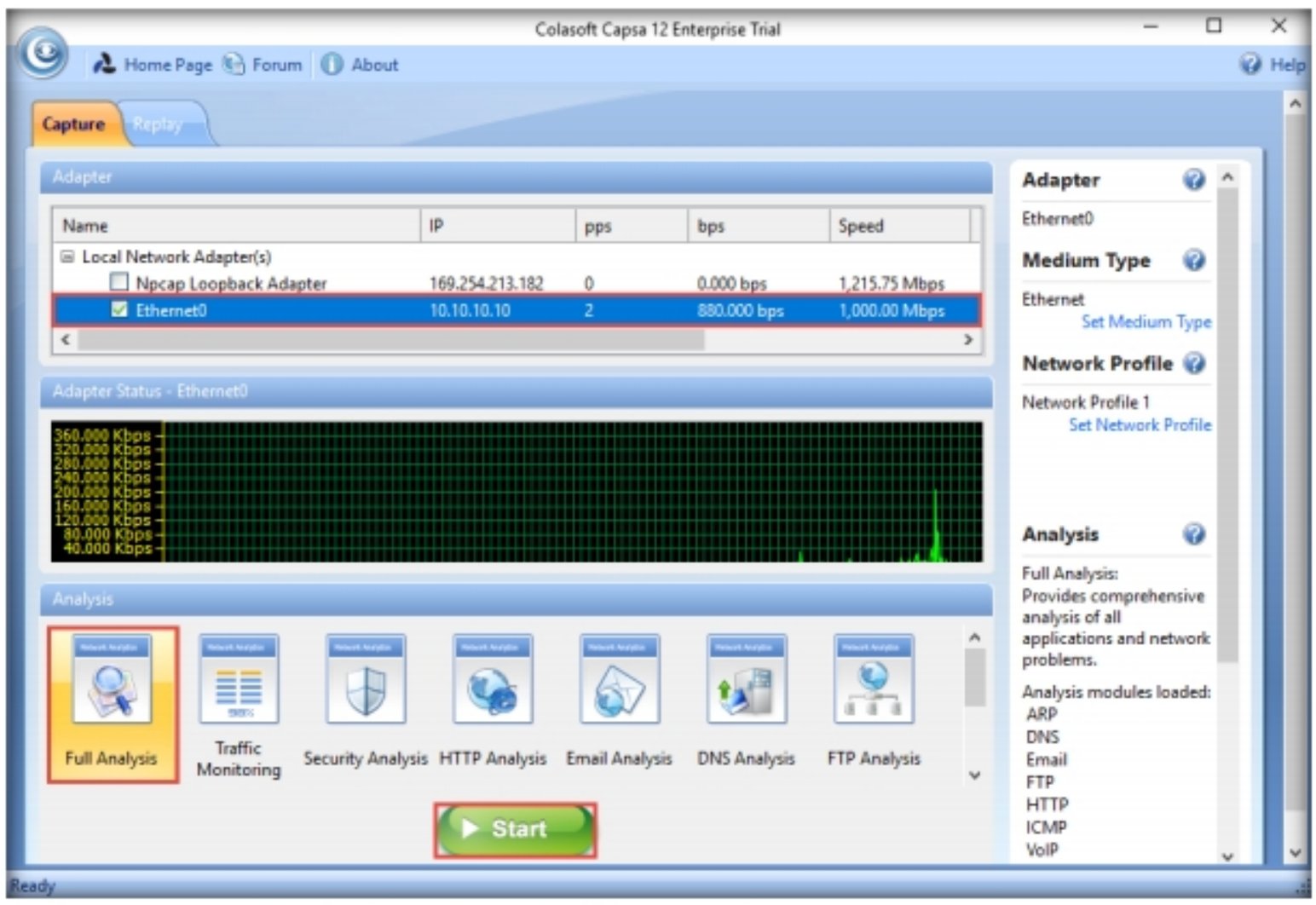


Figure 2.2.14: Colasoft Capsa Network Analyzer creating a New Project

TASK 2.5

Analyze the Dashboard Information

23. The **Analysis Project 1** window appears, displaying a **Dashboard** containing statistical graphs and charts.

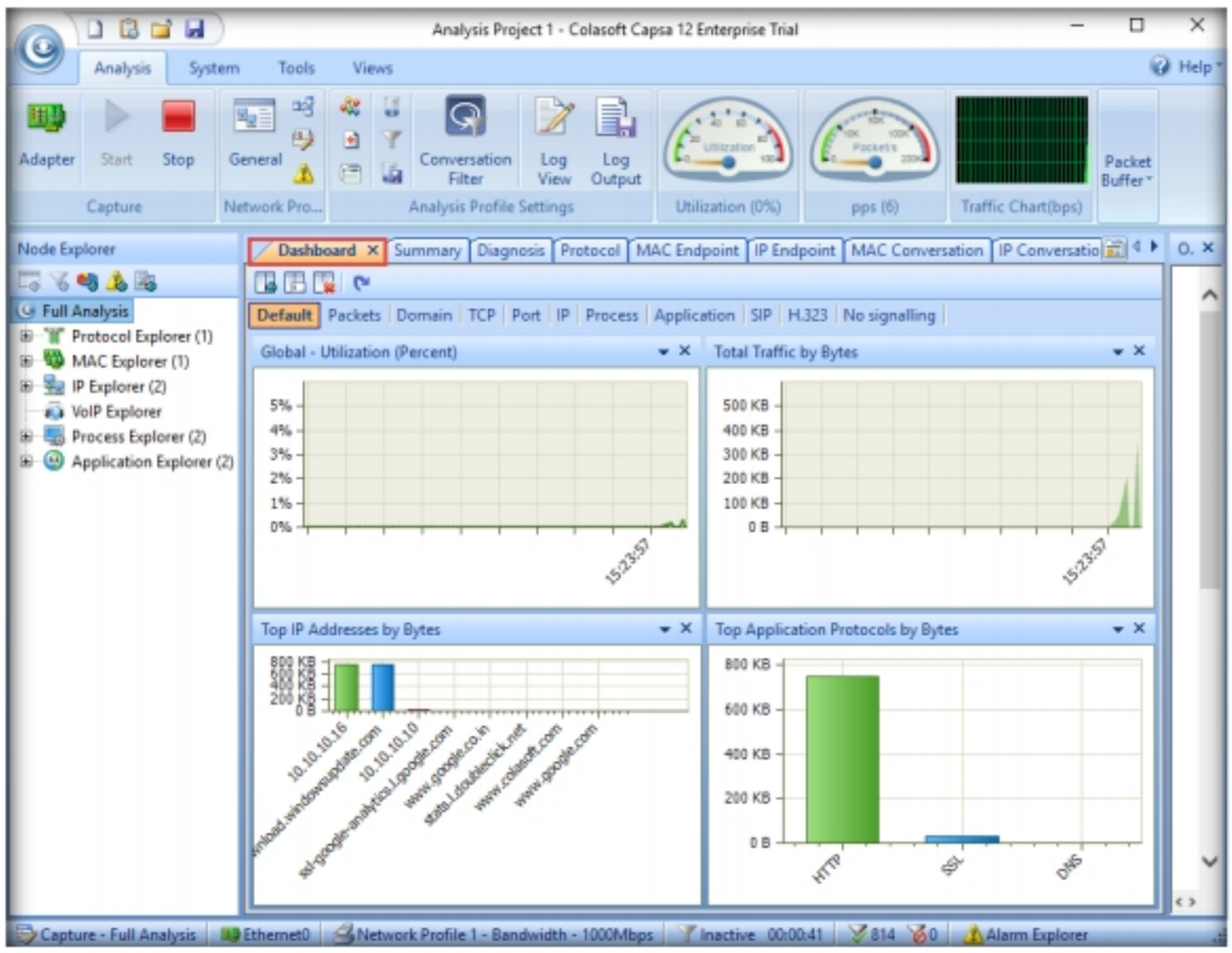


Figure 2.2.15: Colasoft Capsa Network Analyzer Dashboard

TASK 2.6

Examine the Summary Information

24. The **Summary** tab provides full general analysis and statistical information for the selected node in the **Node Explorer** section of the right-hand pane.

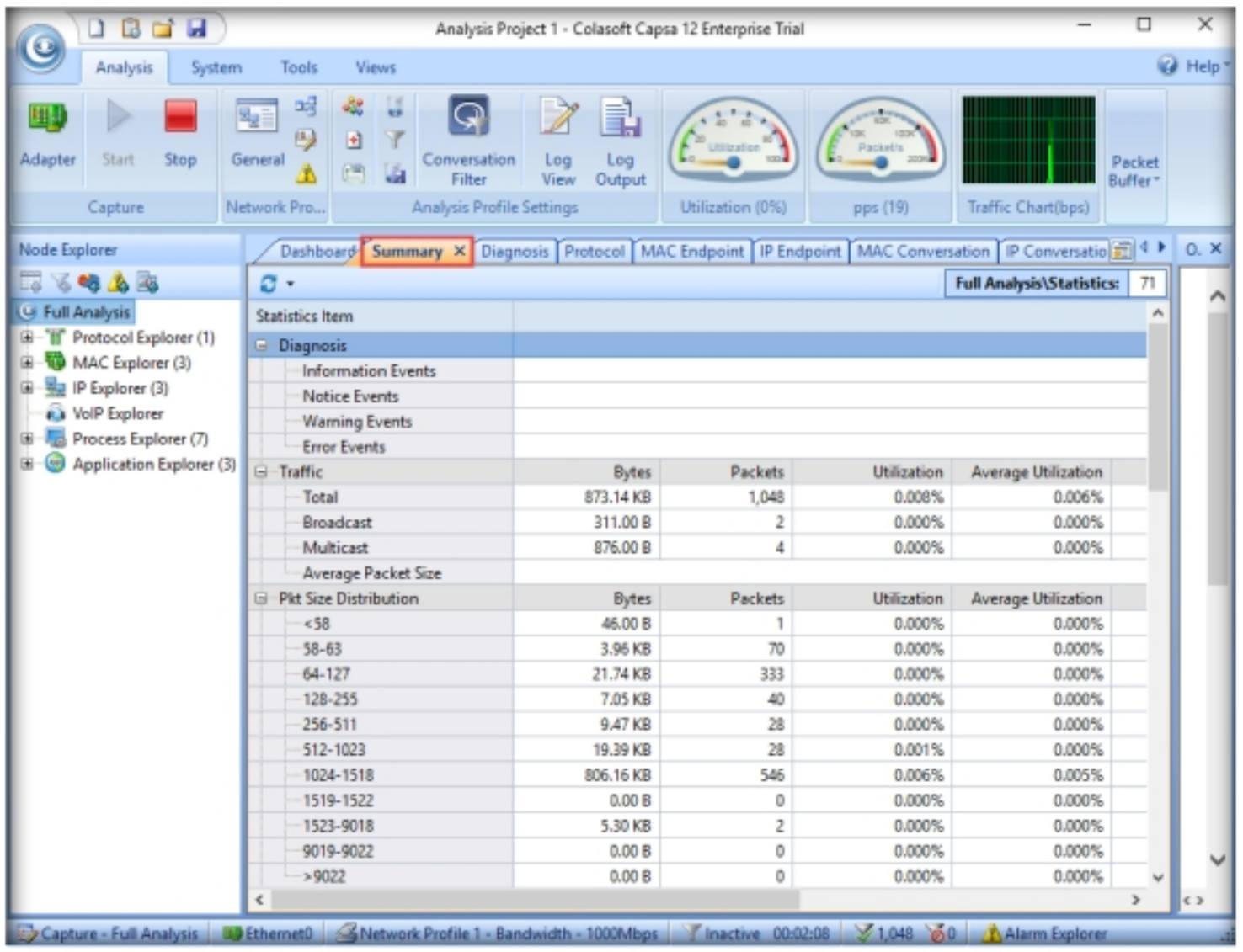


Figure 2.2.16: Colasoft Capsa Network Analyzer Summary

TASK 2.7

Analyze the Diagnosis Information

25. Click the **Diagnosis** tab. It displays the real-time diagnostic events of the global network according to groups of protocol layers or security levels. With this tab, you can view the performance of the protocols.
26. Now, click **TCP Duplicated Acknowledgement** under the **Transport Layer** node, which, in turn, will highlight **TCP repeated confirmation** under the **Details** section.
27. Double-click on the highlighted **TCP repeated confirmation** to view detailed information.

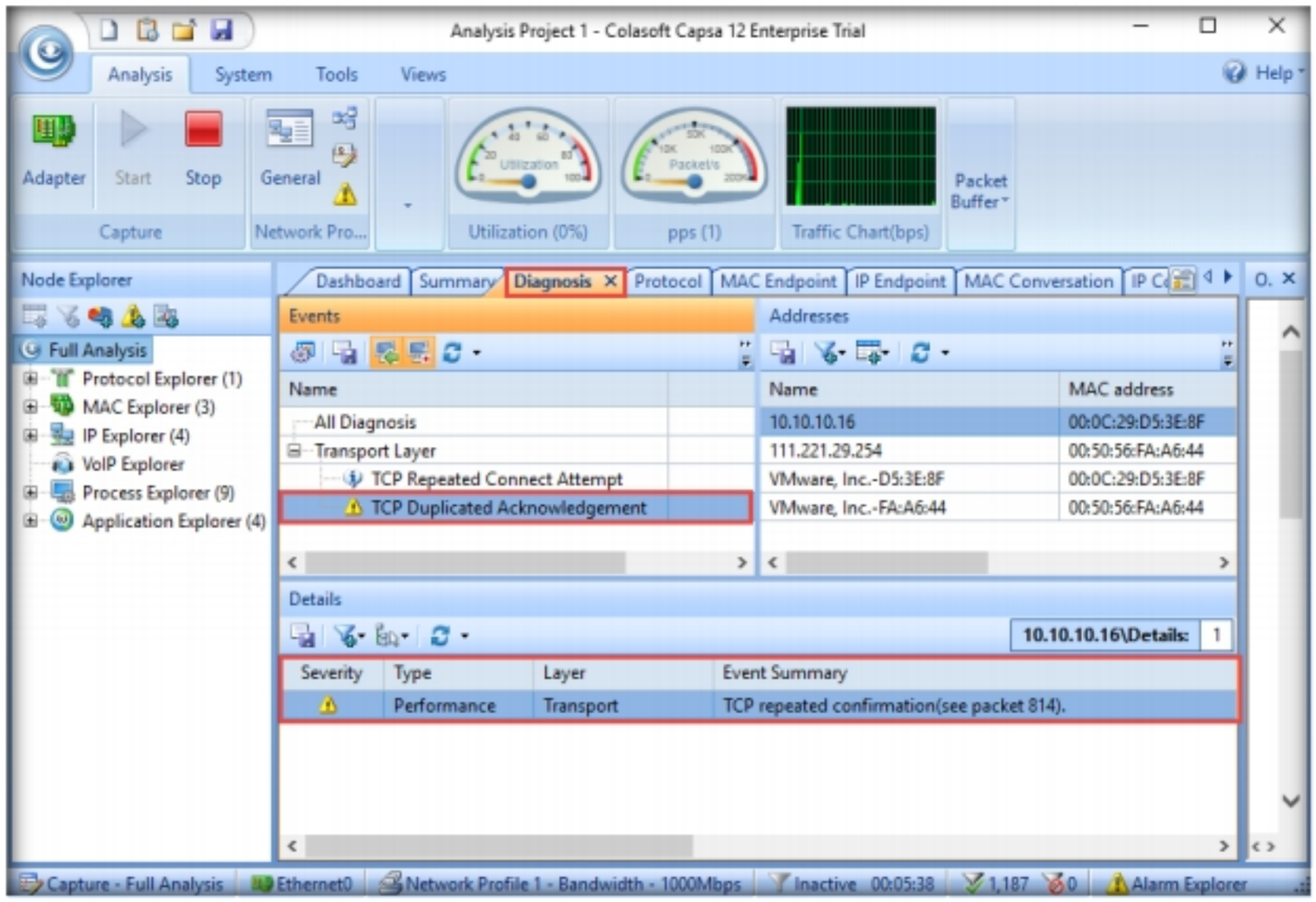


Figure 2.2.17: Colasoft Capsa Network Analyzer Diagnoses

28. The **Packet - Details - Analysis Project 1** window appears, displaying detailed information regarding captured packets such as absolute time, source, source port, source geolocation, and other information related to the event.

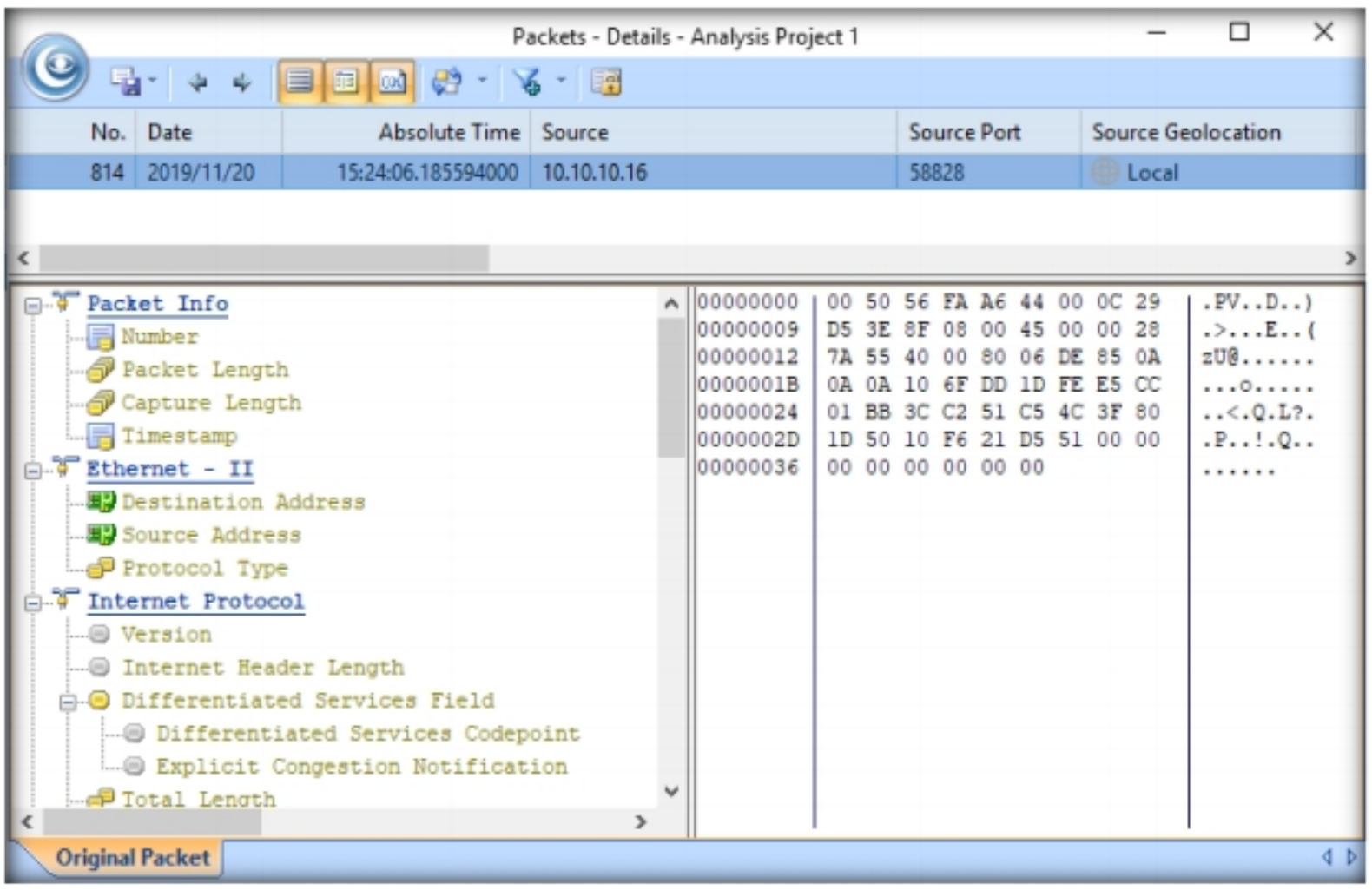


Figure 2.2.18: Packet - Details: Analysis Project window

TASK 2.8

Examine the Protocol Information

29. Close the **Packet - Details - Analysis Project** window after analyzing its results.
30. Click the **Protocol** tab. It lists the statistics of all protocols used in the network transactions hierarchically. By default, **MAC Endpoint** in the lower section of the window is selected.

Note: Here, we will analyze the packets traveling to and from the **Windows Server 2016** virtual machine.

31. Under the **MAC Endpoint** section, double-click the **10.10.10.16** IP address to analyze packets flowing through the open ports.

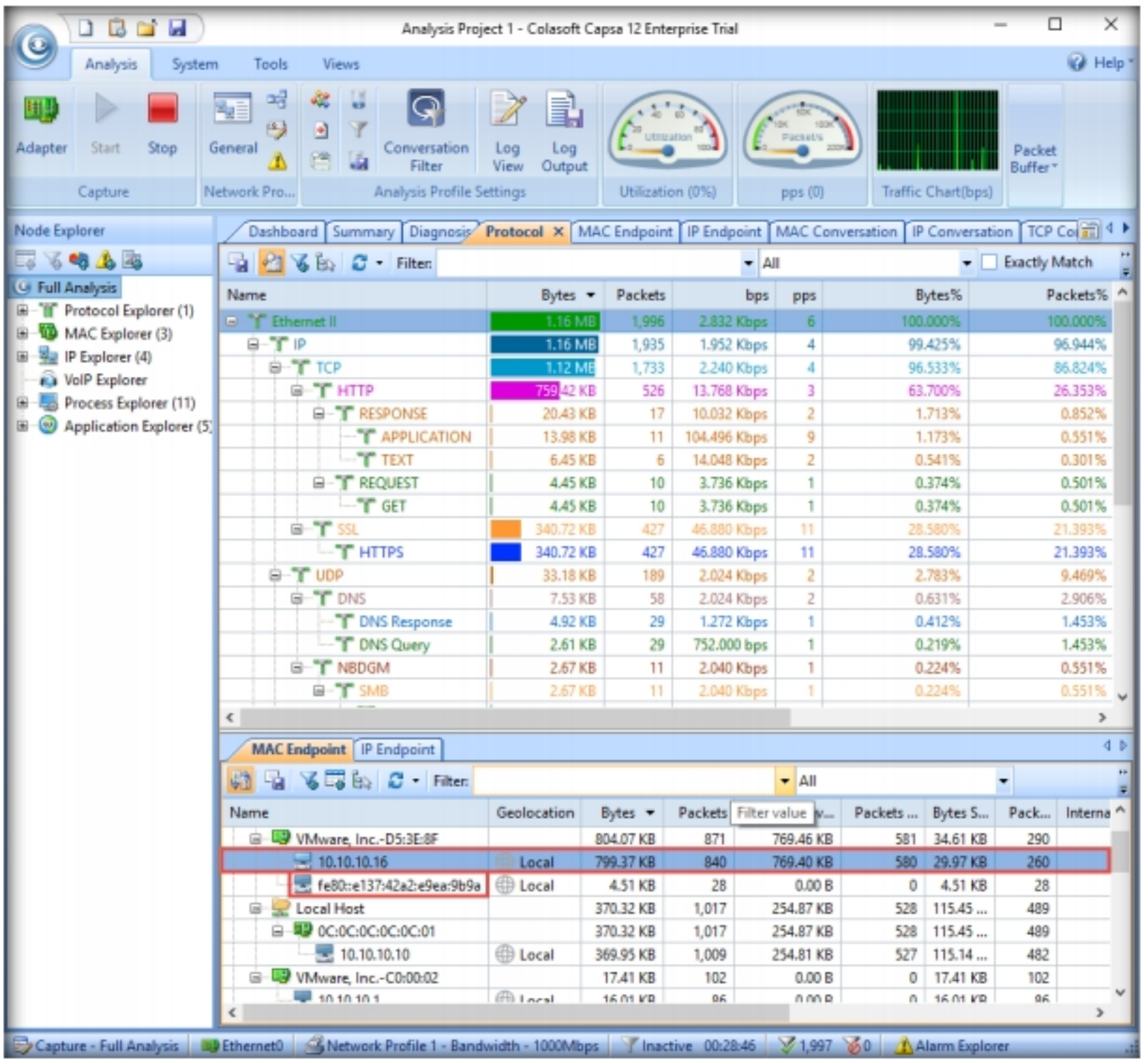


Figure 2.2.19: Colasoft Capsa Network Analyzer Protocol analysis

32. The **Packets - 10.10.10.16 - Analysis Project 1** window appears, displaying information about captured packets transmitted via open ports on the **Windows Server 2016** virtual machine.

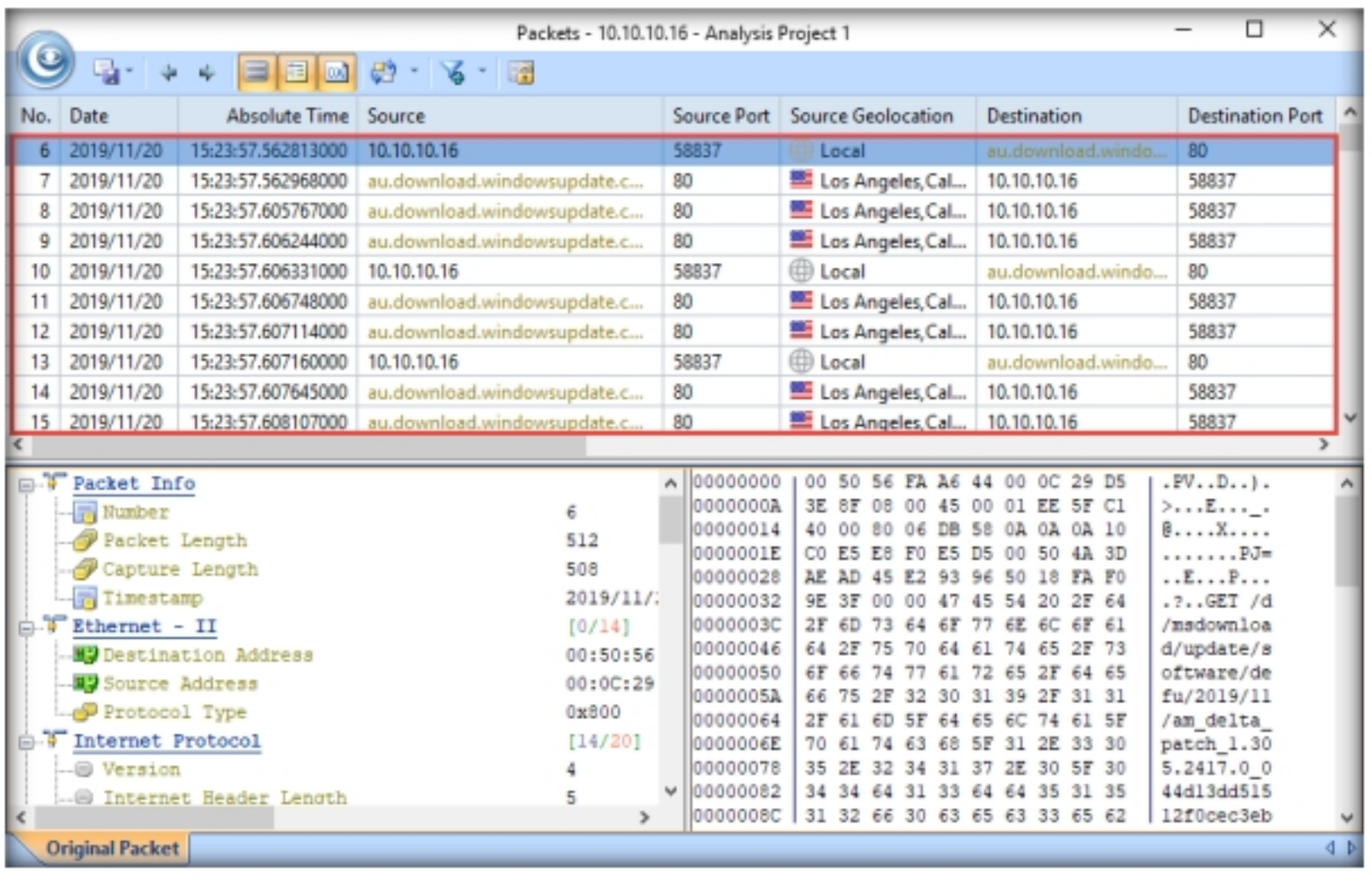


Figure 2.2.20: Packet 10.10.10.16: Analysis Project windows

TASK 2.9

Examine the Physical Endpoint Information

33. Click the **MAC Endpoint** tab. It displays the statistics of all MAC addresses that communicate in the network. The list of MAC addresses is displayed under **MAC Conversation** present in the lower pane of the window, as shown in the screenshot.

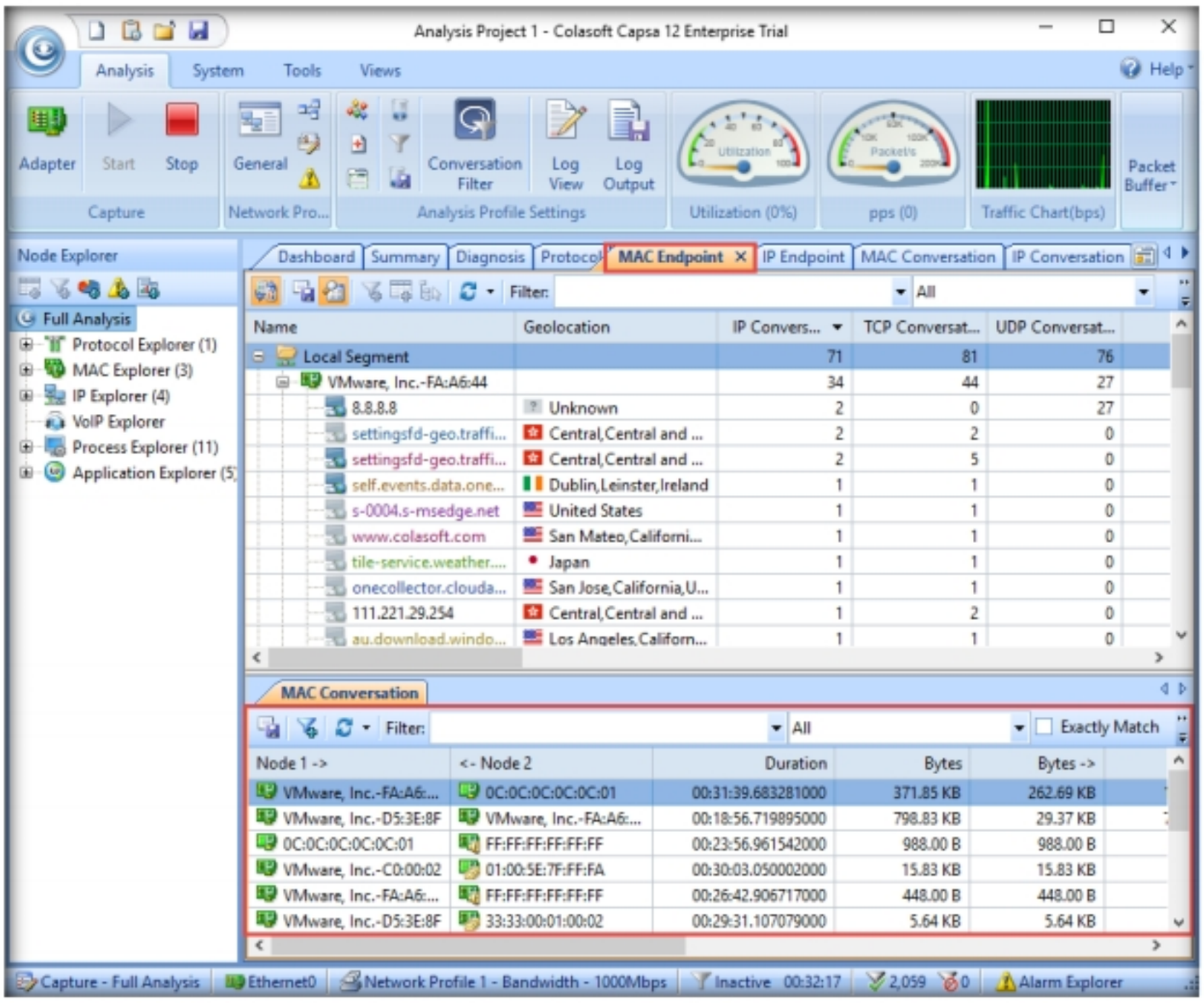


Figure 2.2.21: Colasoft Capsa Network Analyzer: MAC Endpoint analysis

TASK 2.10

Analyze the IP Endpoint Information

34. Click the **IP Endpoint** tab. It displays statistics of all IP addresses communicating in the network. You can easily find the nodes with the highest traffic volumes by analyzing the number of packets send and received, including the bytes used. You can also check if there is a multicast or broadcast storm in your network.

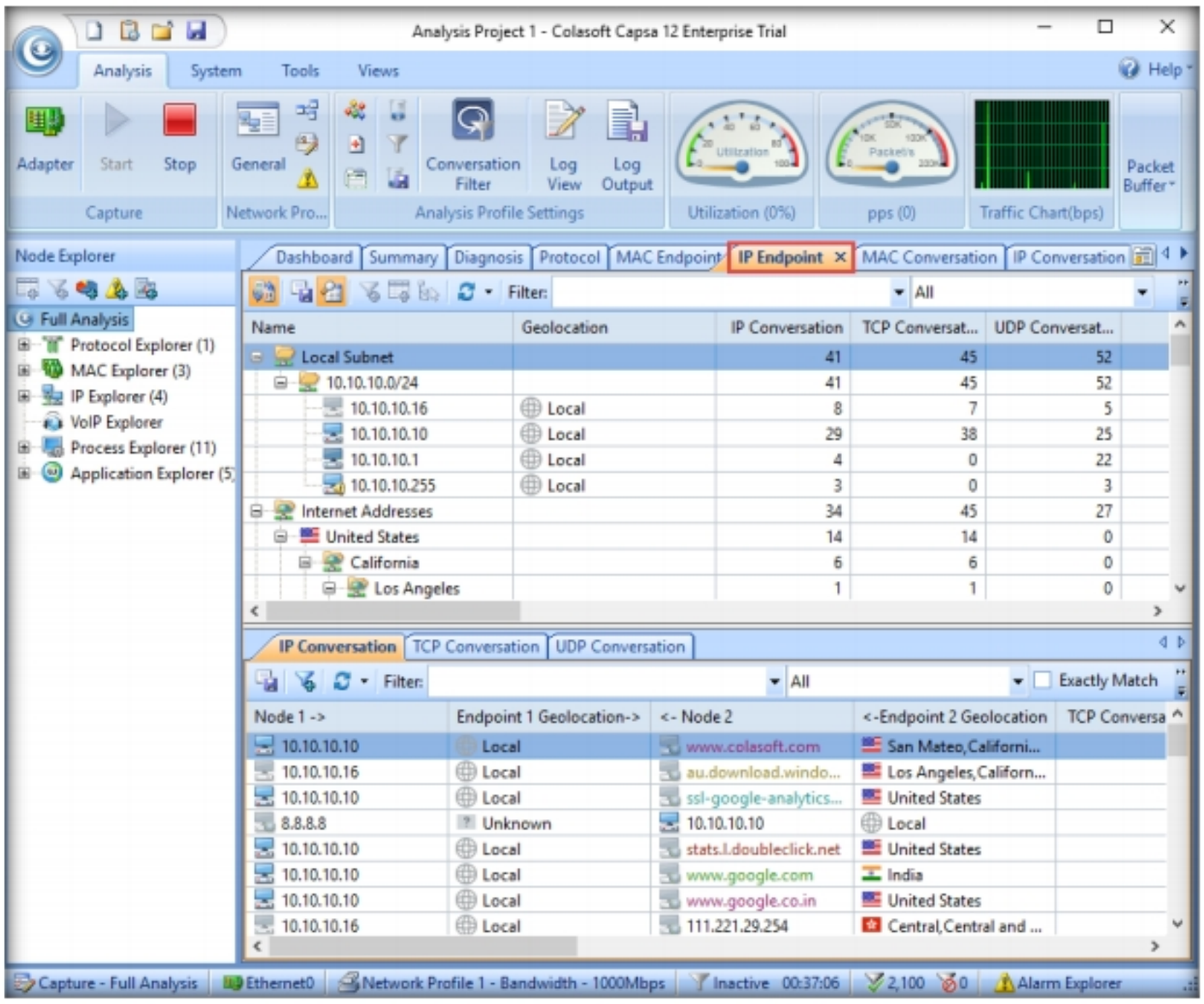


Figure 2.2.22: Colasoft Capsa Network Analyzer: IP Endpoint view

35. Click the **MAC Conversation** tab. It displays conversations between two MAC addresses.

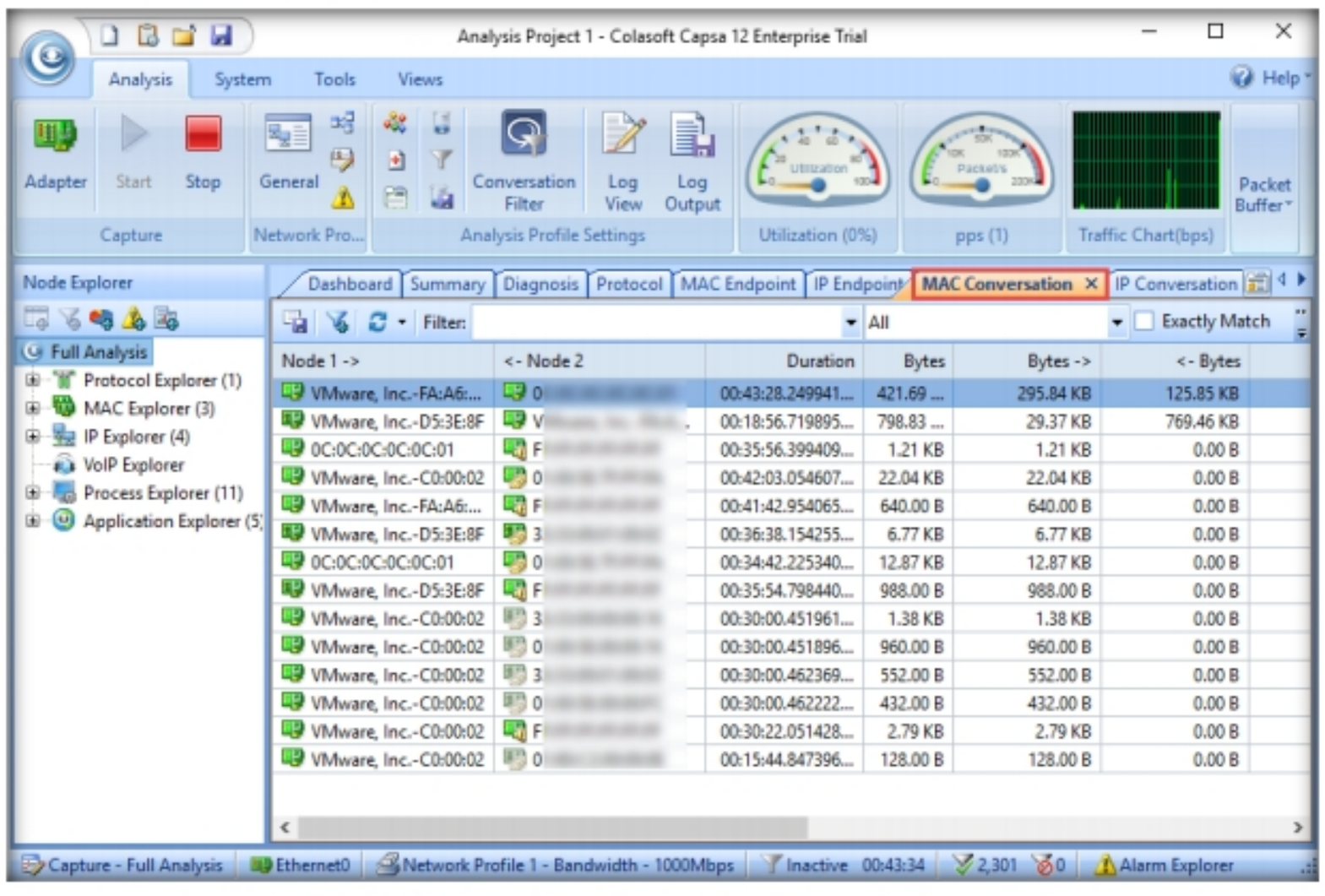


Figure 2.2.23: Colasoft Capsa Network Analyzer MAC Conversations

TASK 2.11

Examine the IP Conversation

36. Click the **IP Conversation** tab. It displays IP conversations between pairs of nodes. The lower pane of the IP Conversation section offers UDP and TCP conversations, which you can drill down to analyze.
37. Double-click any conversation in the **IP Conversation** list to view a full analysis of the packets exchanged between two IPs (here, **10.10.10.16** and **10.10.10.10**).

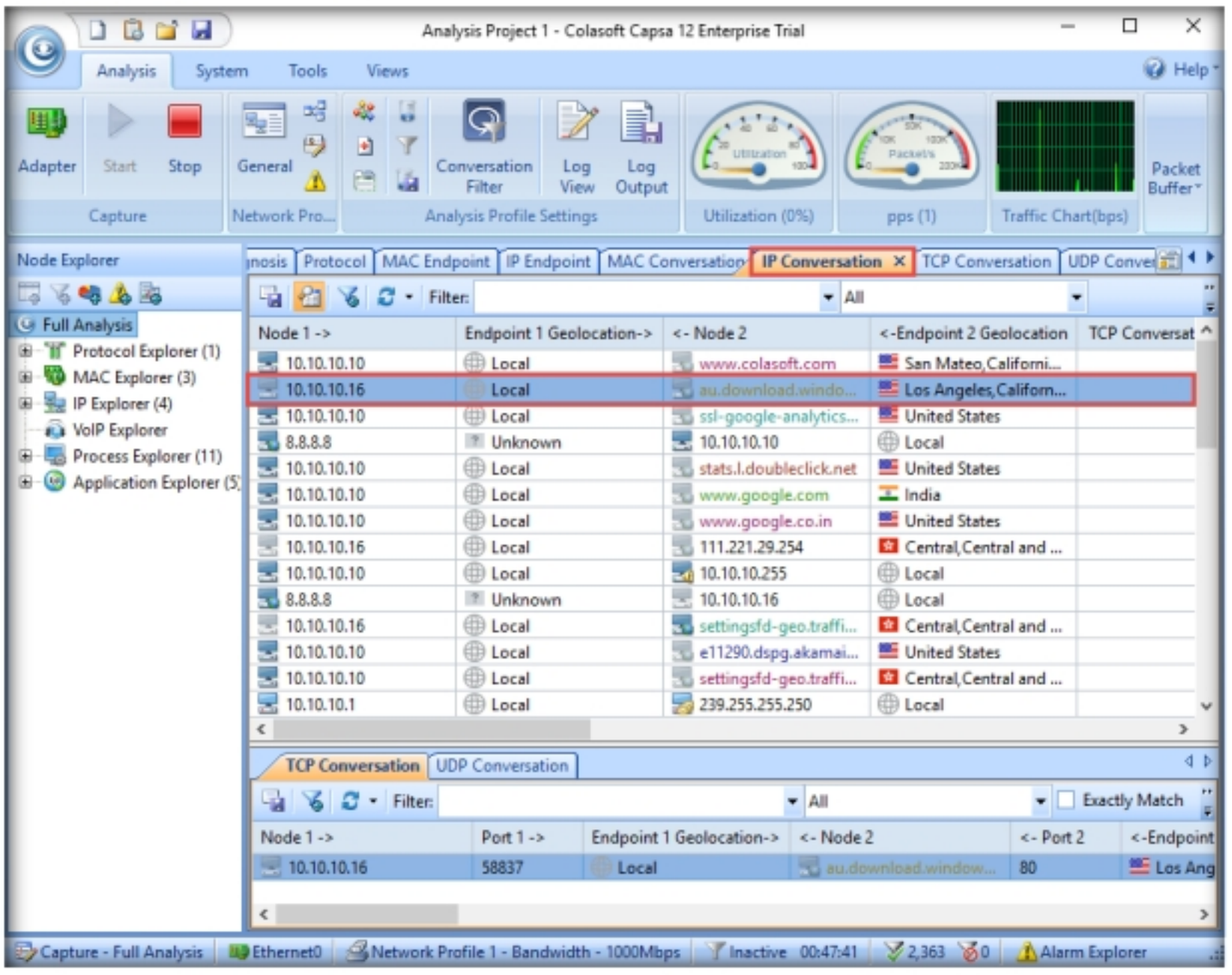


Figure 2.2.24: Colasoft Capsa Network Analyzer: IP Conversations

38. The **Packets** window appears, displaying the full packet analysis between two IP addresses.

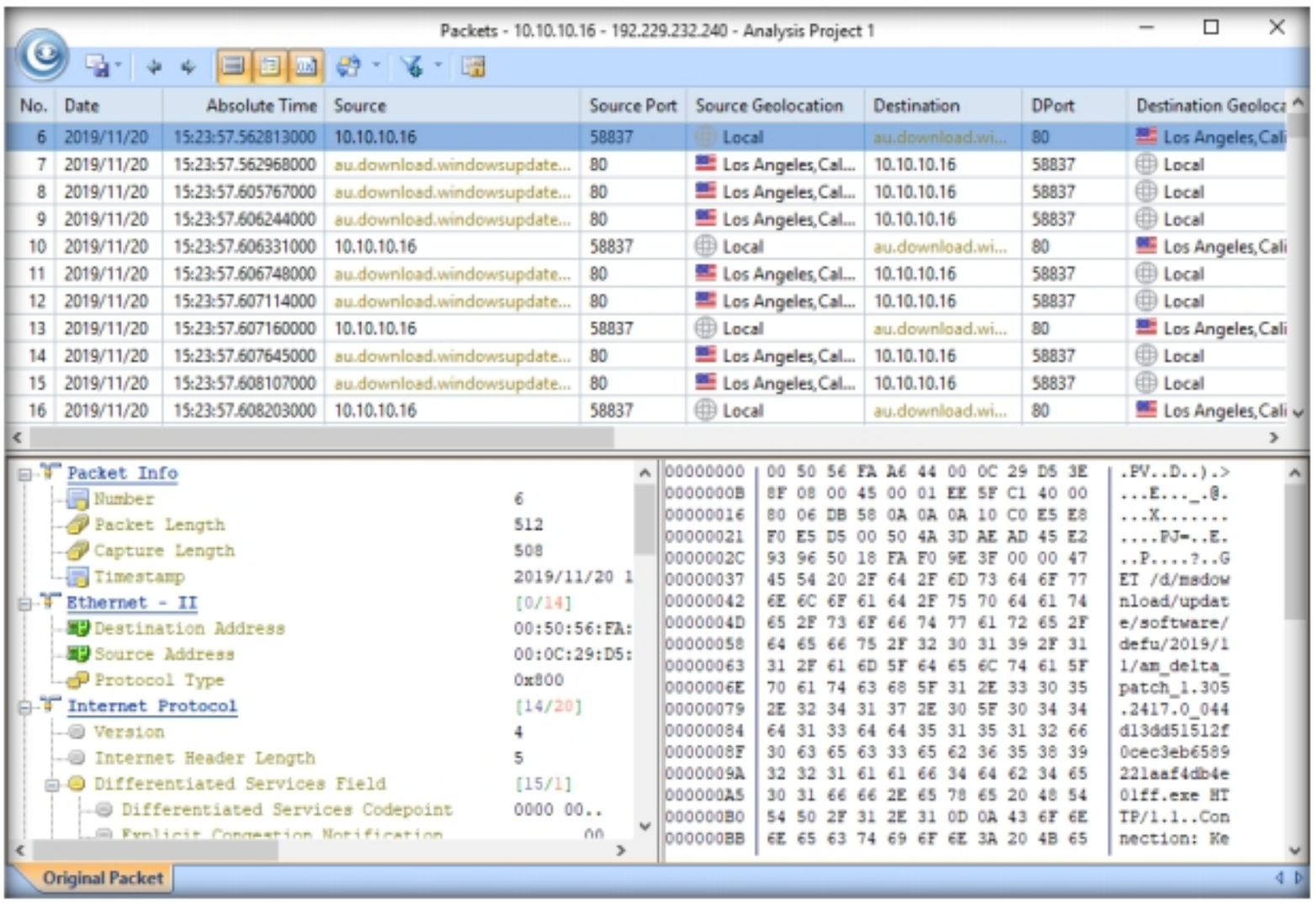


Figure 2.2.25: Full Packet Analysis of Nodes in IP Conversations

TASK 2.12

Examine the TCP Conversations

39. Click the **TCP Conversation** tab. It displays the real-time status of the TCP conversations between pairs of nodes.

40. Double-click any node (here, **10.10.10.16**) to display a full analysis of the captured packets.

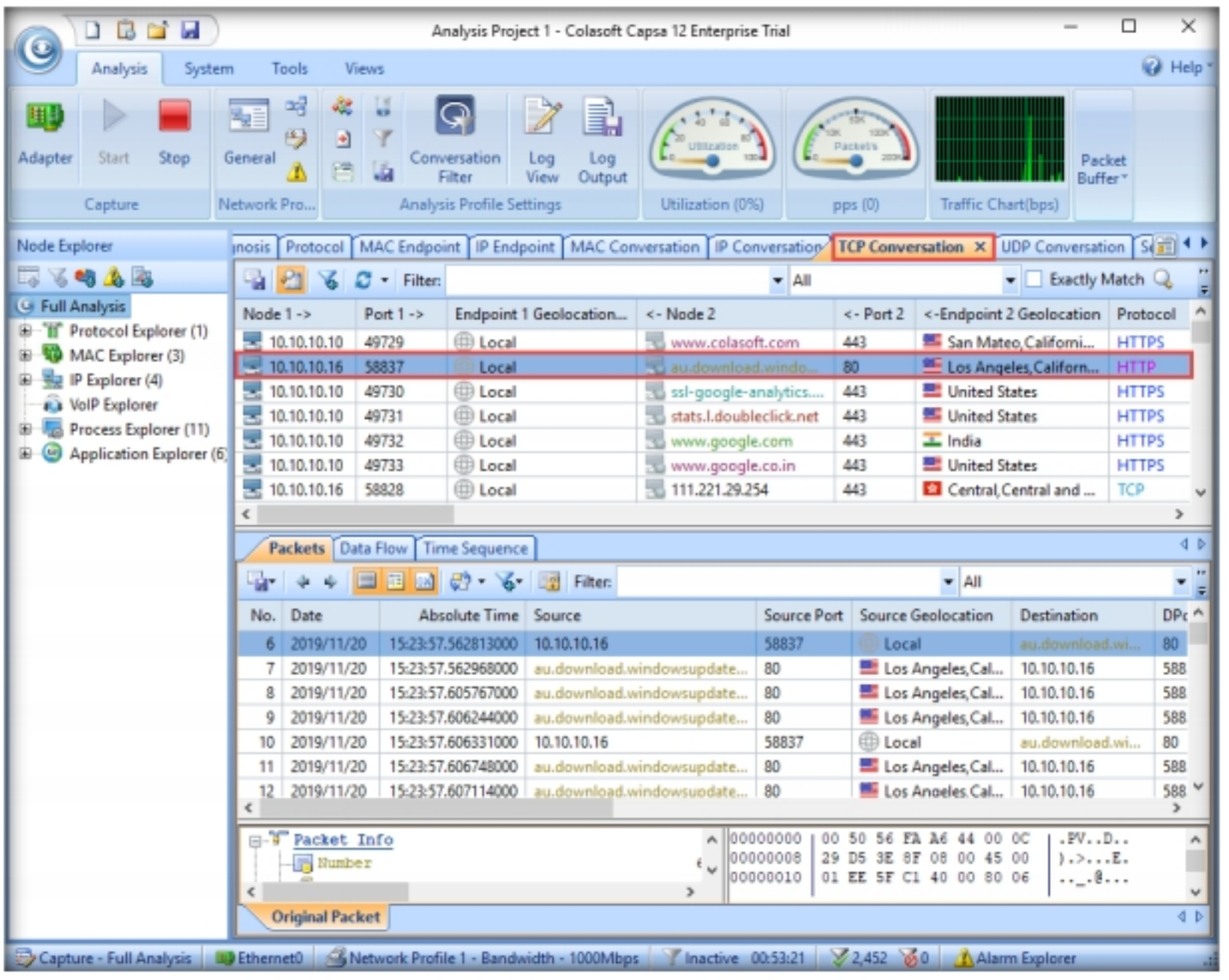


Figure 2.2.26: Colasoft Capsa Network Analyzer TCP Conversations

41. The **TCP Flow Analysis** window appears. By default, the **Packets** tab opens, displaying the TCP transactions between the selected pair of nodes.

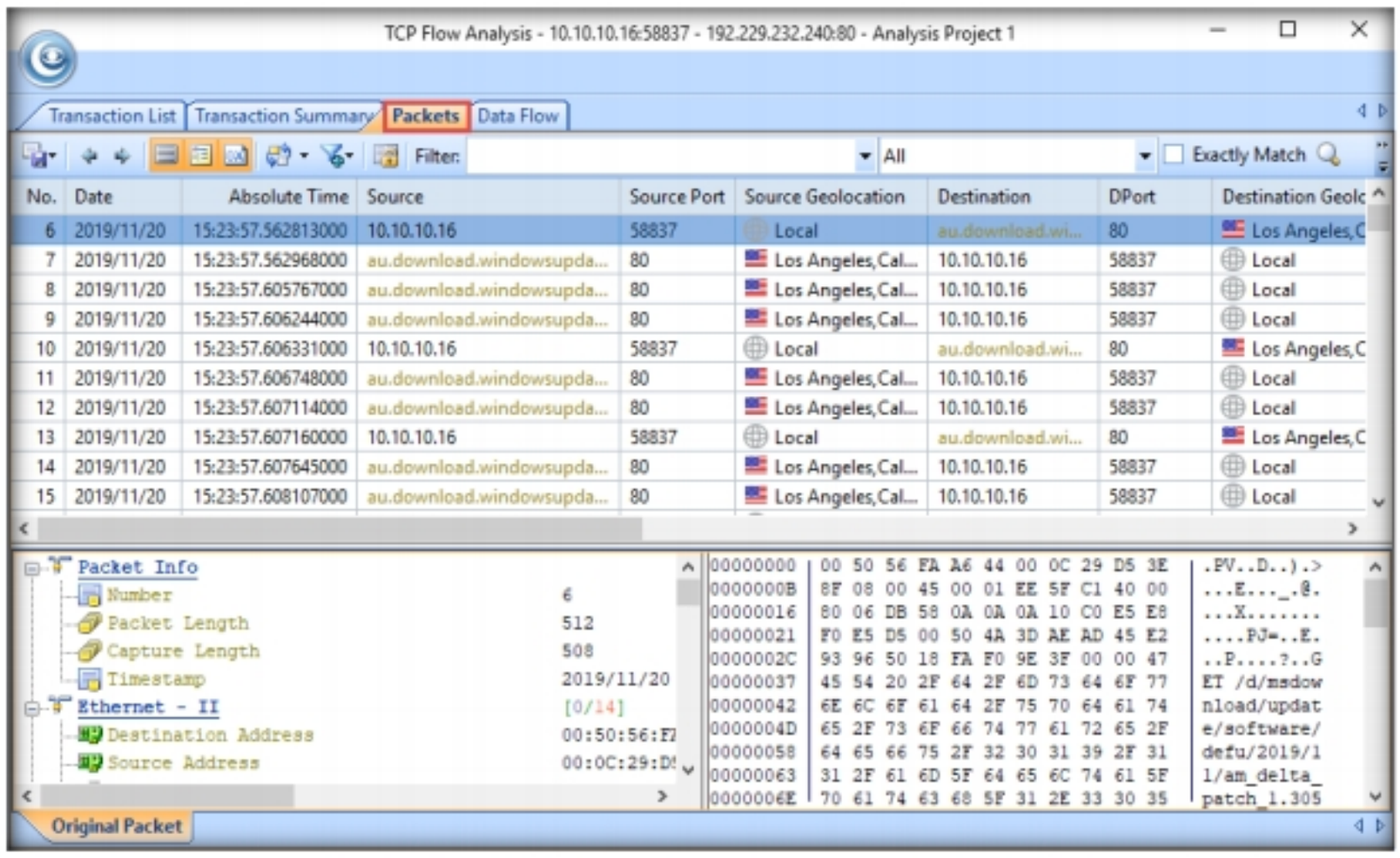


Figure 2.2.27: Colasoft Capsa Network Analyzer Transaction List

42. Click the **Transaction Summary** tab to display a summary of the transactions. After analyzing the details, close the **TCP Flow Analysis** window.

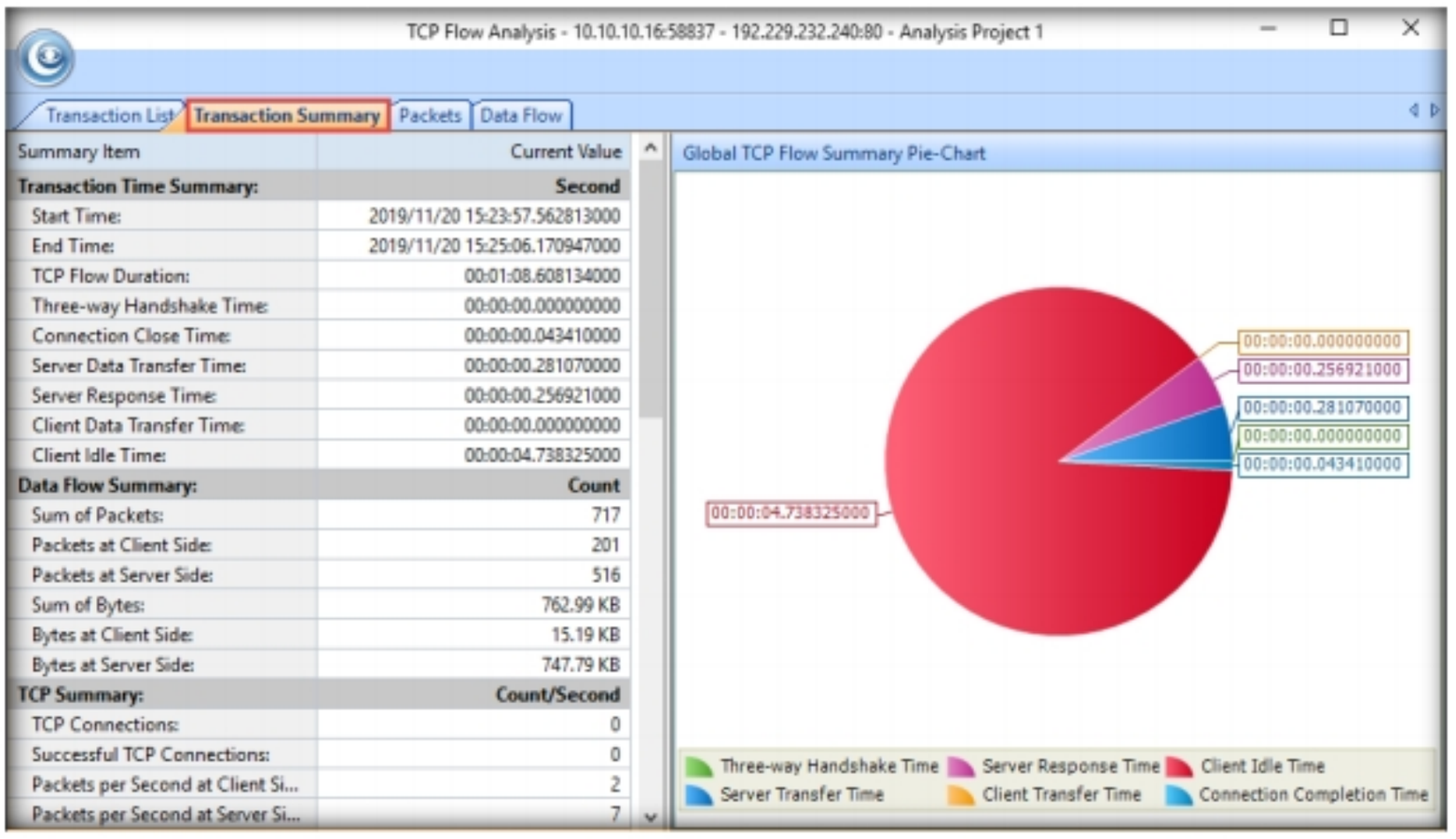


Figure 2.2.28: Colasoft Capsa Network Analyzer Transaction Summary

TASK 2.13

Examine the Matrix View

43. Click the **Matrix** tab to view the nodes communicating in the network as graphically connected with lines. The weight of each line indicates the volume of the traffic between the nodes, which are arranged into an ellipse.
44. Click the **Top 100 MAC Node** option under the **Select Matrix** section to view a network communication diagram between 100 MAC nodes.
45. Similarly, you can select other matrix options such as **Top 100 MAC Conversation**, **Top 100 IP Conversation**, and **Top 100 IP Node**.

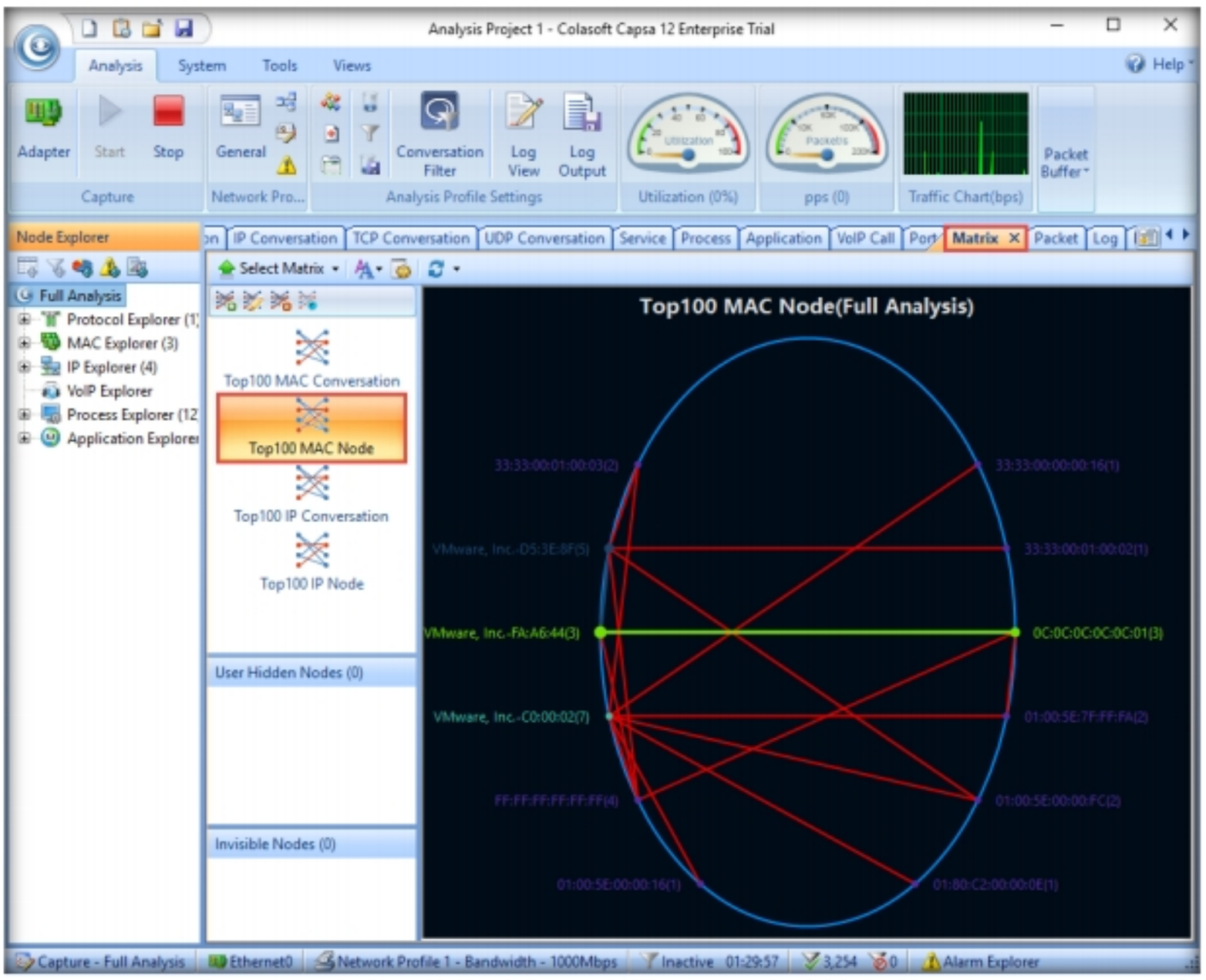


Figure 2.2.29: Colasoft Capsa Network Analyzer Matrix view

TASK 2.14

Analyze the Packet Details

46. Click the **Packet** tab to view original information for any packet. Double-click any packet to view the full analysis information of the packet decode.

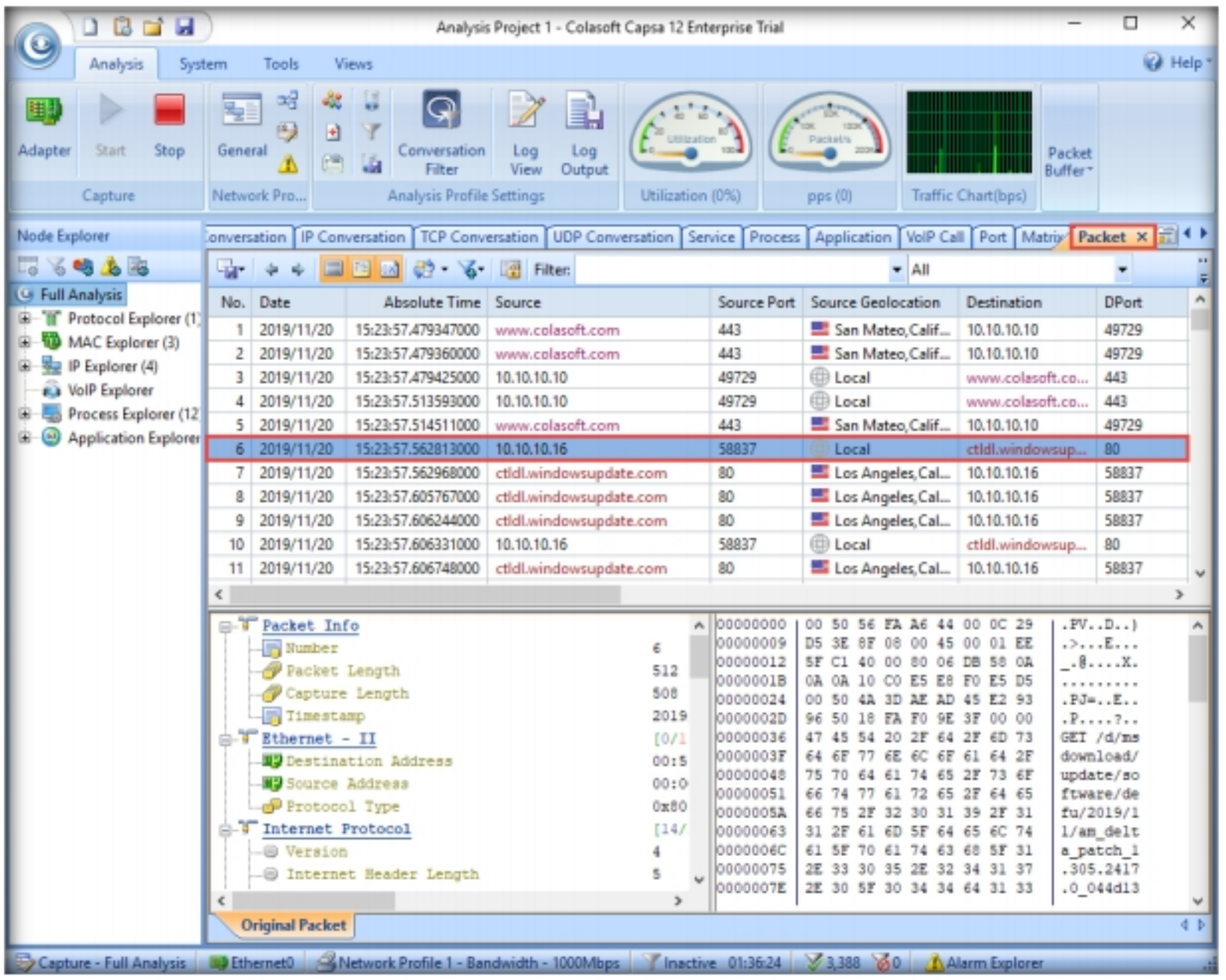


Figure 2.2.30: Colasoft Capsa Network Analyzer Packet information

47. The **Packet Decoding** window appears, displaying two major views: **Decoding View** and **Hex View**.

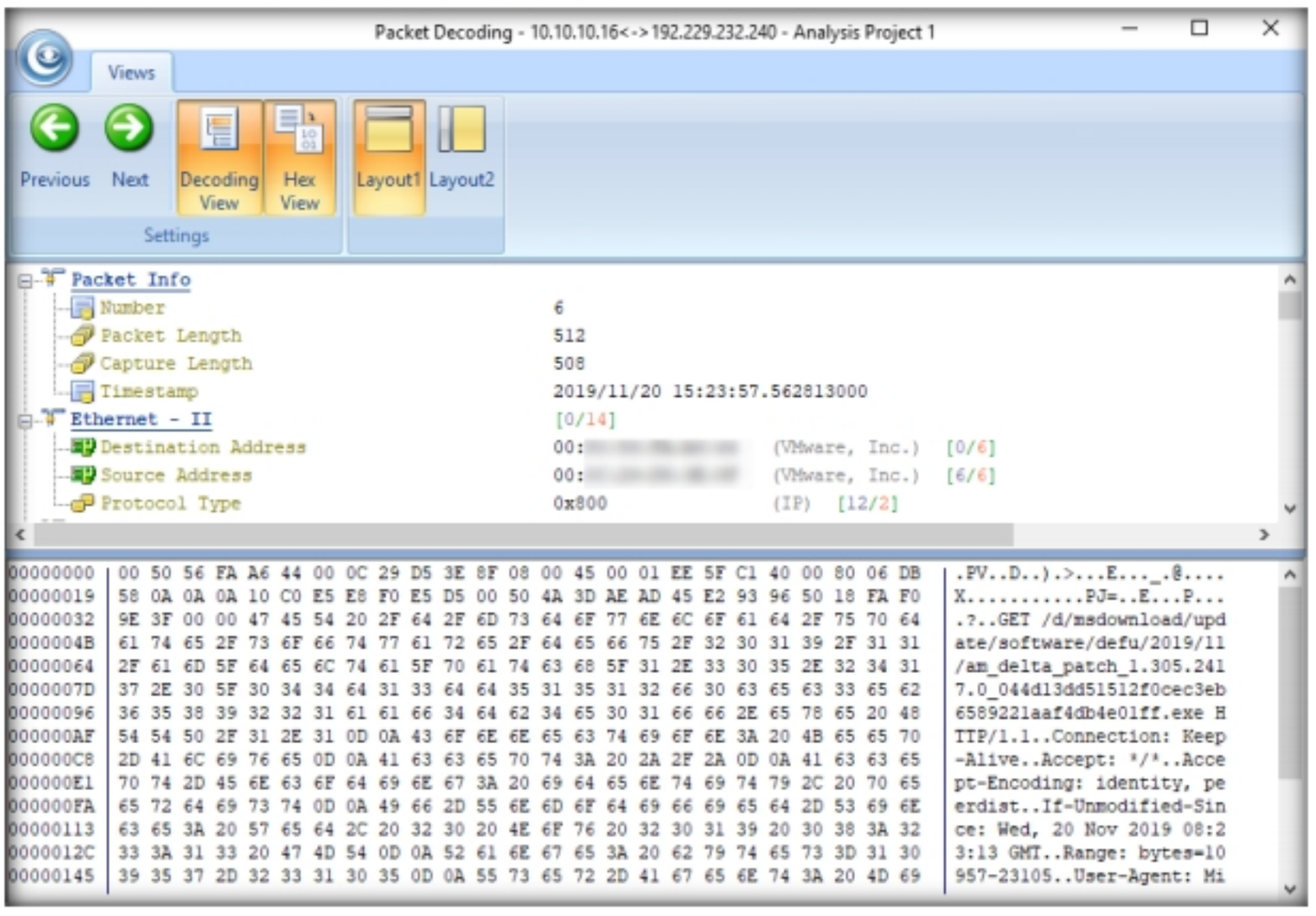


Figure 2.2.31: Full Analysis of Packet Decode

TASK 2.15

Generate Report

48. Click the **Report** tab to view various reports such as **Global**, **VoIP**, **Conversation**, **Top Traffic**, **Port**, and **Packet**.

49. Click on the **Global** option and click the **Export** icon ( ) to save the analysis report.

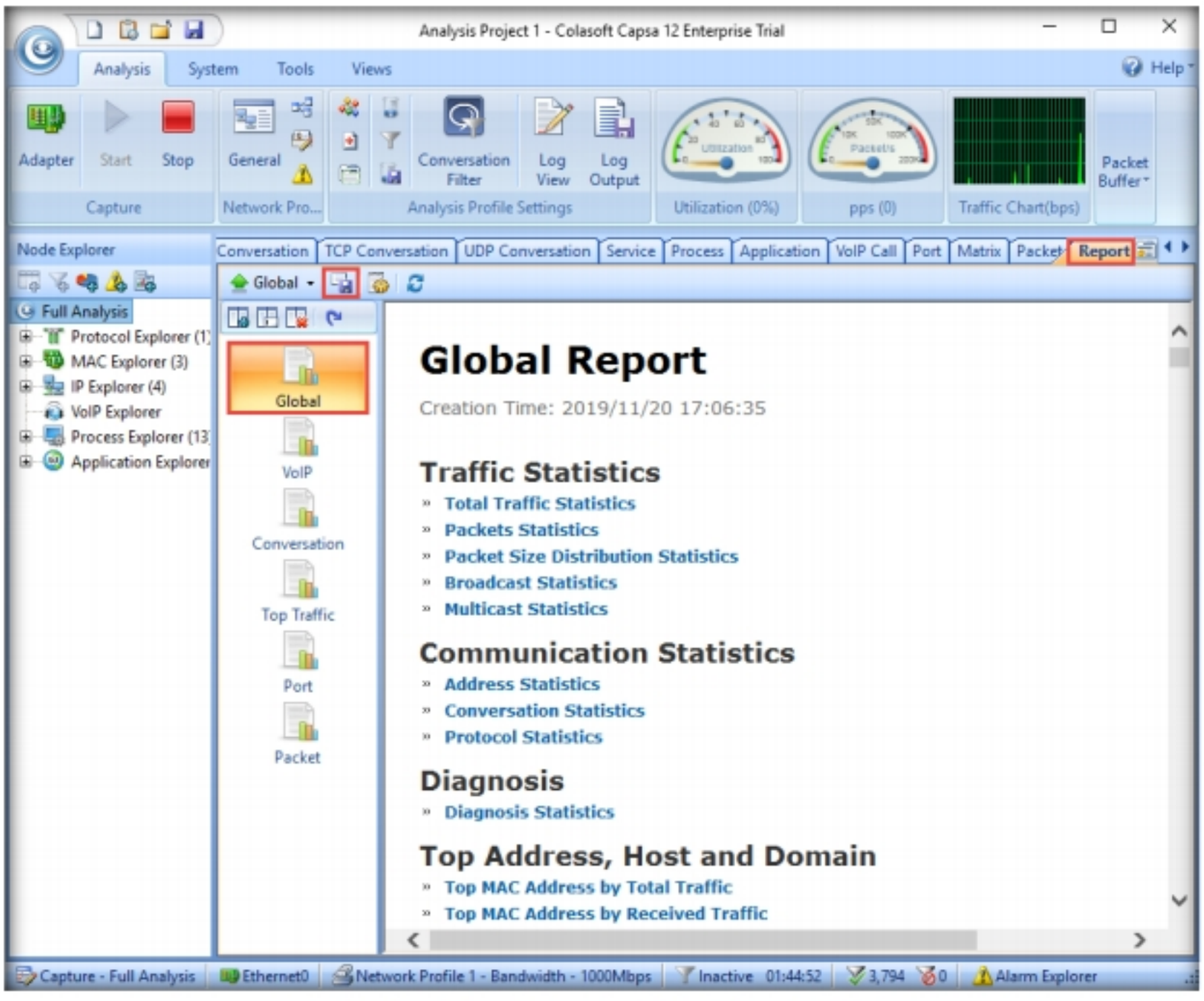


Figure 2.2.32: Colasoft Capsa Network Analyzer: Report tab

50. The **Save As** window appears; select your desired location (here, **Desktop**). In the **File name** field, type **Capsa Network Analyzer Report** and click **Save**.

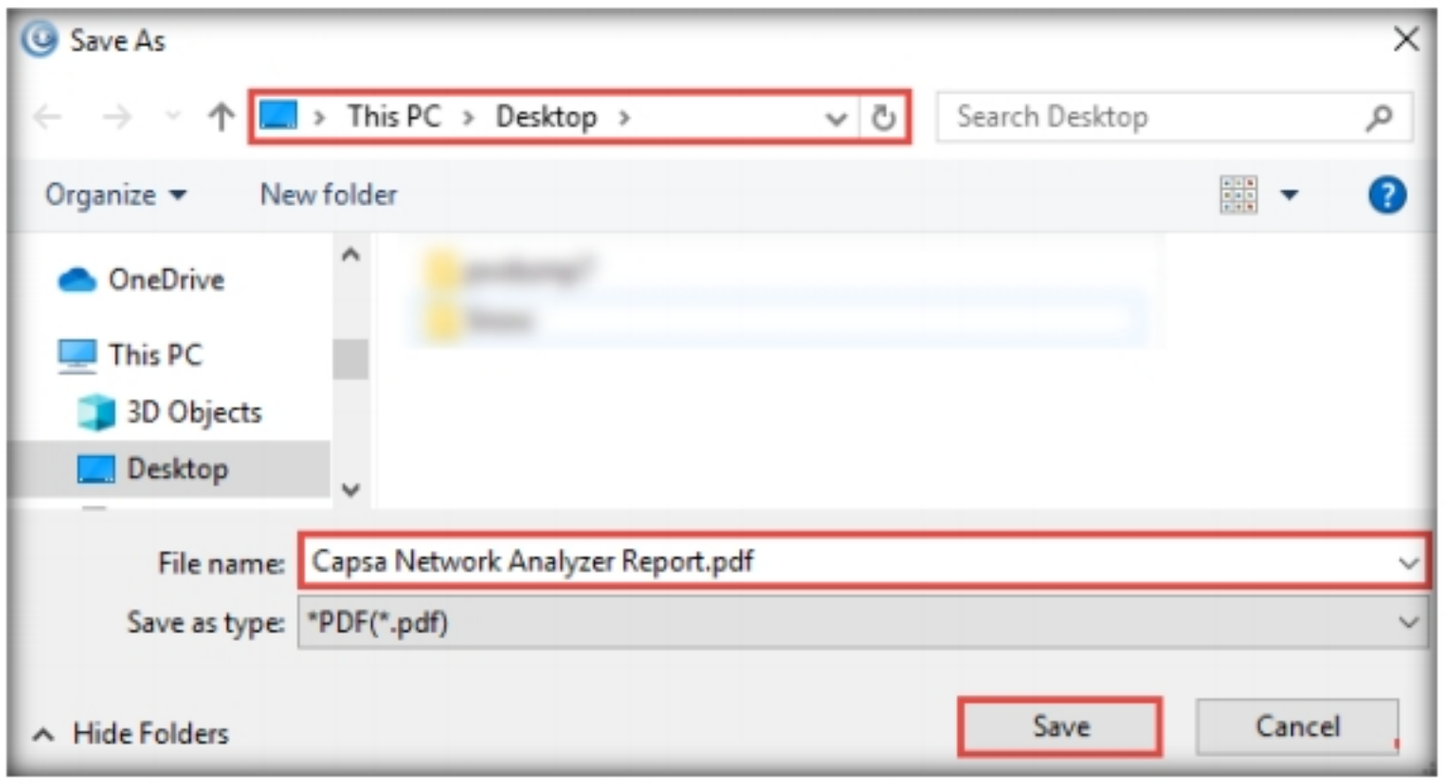


Figure 2.2.33: Save As window

51. An **Export File** pop-up appears; click **Open file** to open the exported report.

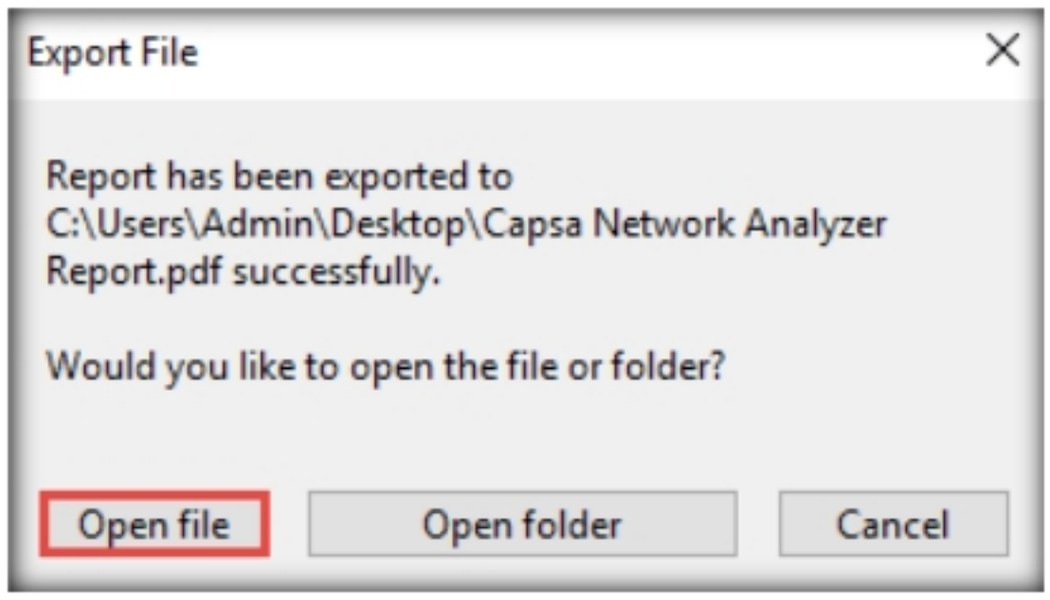


Figure 2.2.34: Export file window

52. The generated report appears in the browser, as shown in the screenshot.
53. You can click the respective hyperlinks for information, or you can scroll down to view a complete detailed report.
54. Here, we will click on the **Top MAC Address by Total Traffic** hyperlink to view the statistical information regarding MAC address traffic.

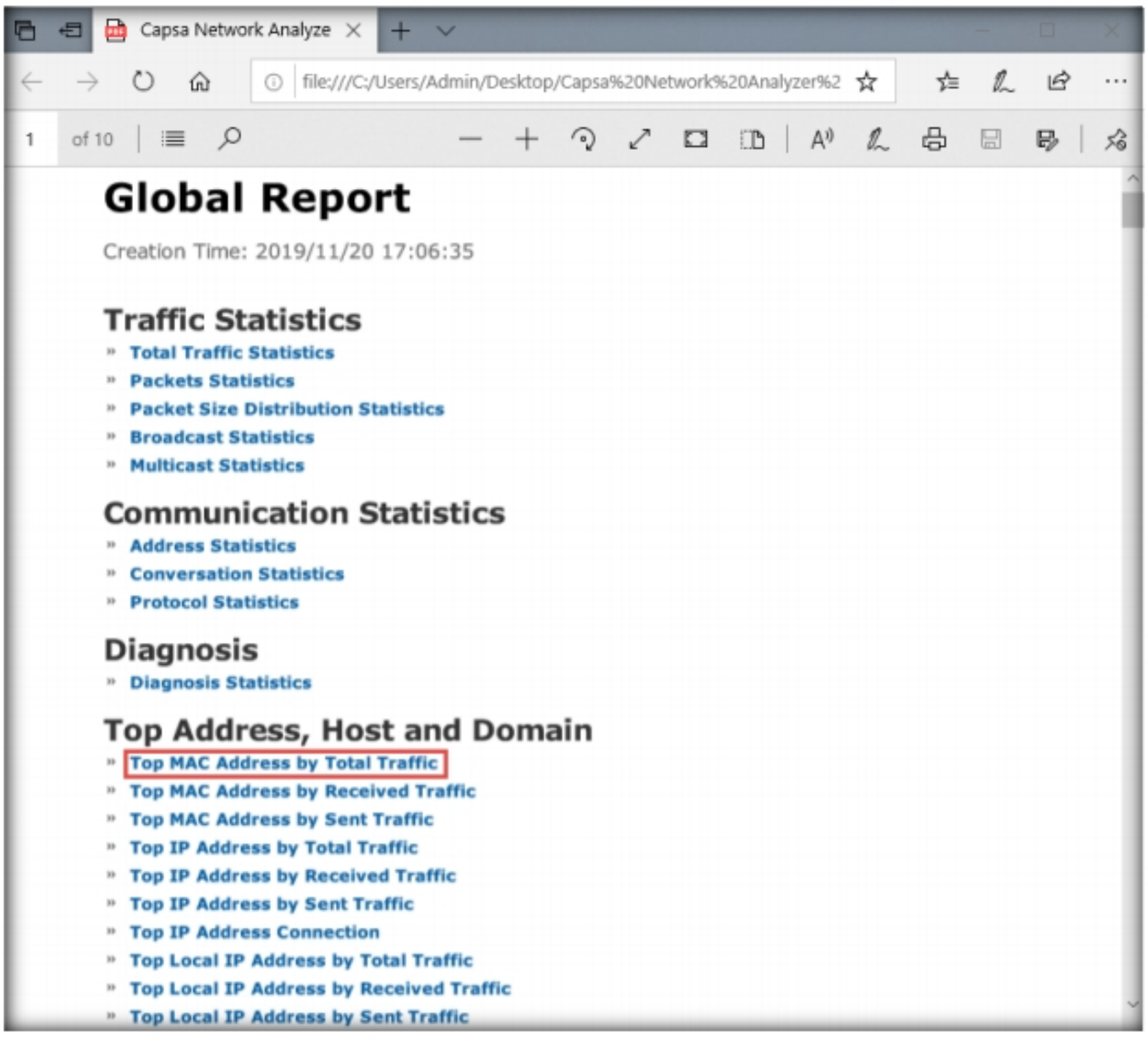


Figure 2.2.35: Global Report

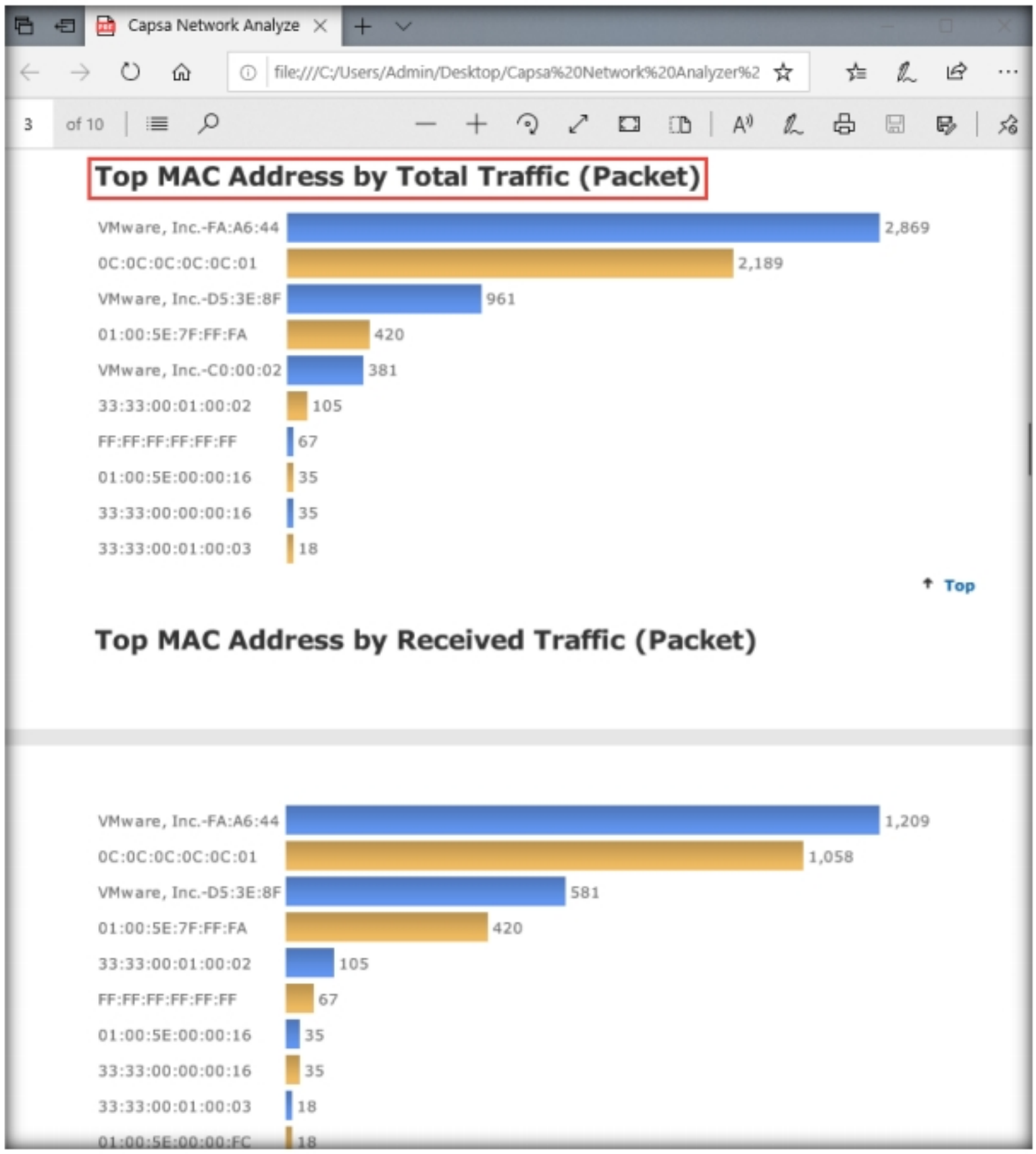


Figure 2.2.36: Top MAC Address by Total Traffic

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

55. In the **Colasoft Capsa** main window, click **Stop** on the toolbar to stop capturing network packets.

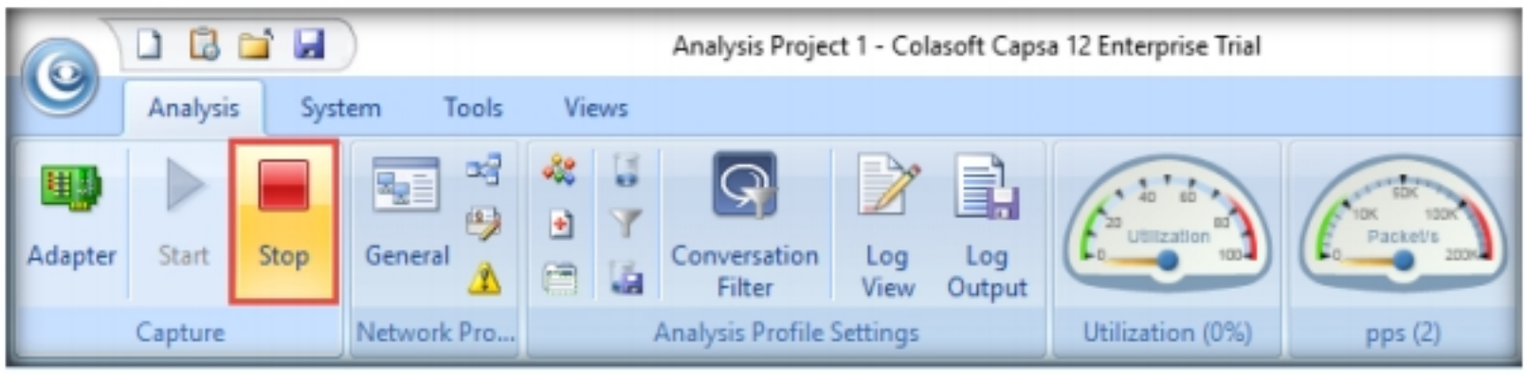


Figure 2.2.37: Stop capturing

56. This concludes the demonstration of analyzing a network using the Capsa Network Analyzer.

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

TASK 2.16

Decrease Windows 10 Memory (RAM)

58. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.
59. In the **Windows 10** operating system node, click the **Memory** option under the **Devices** section.

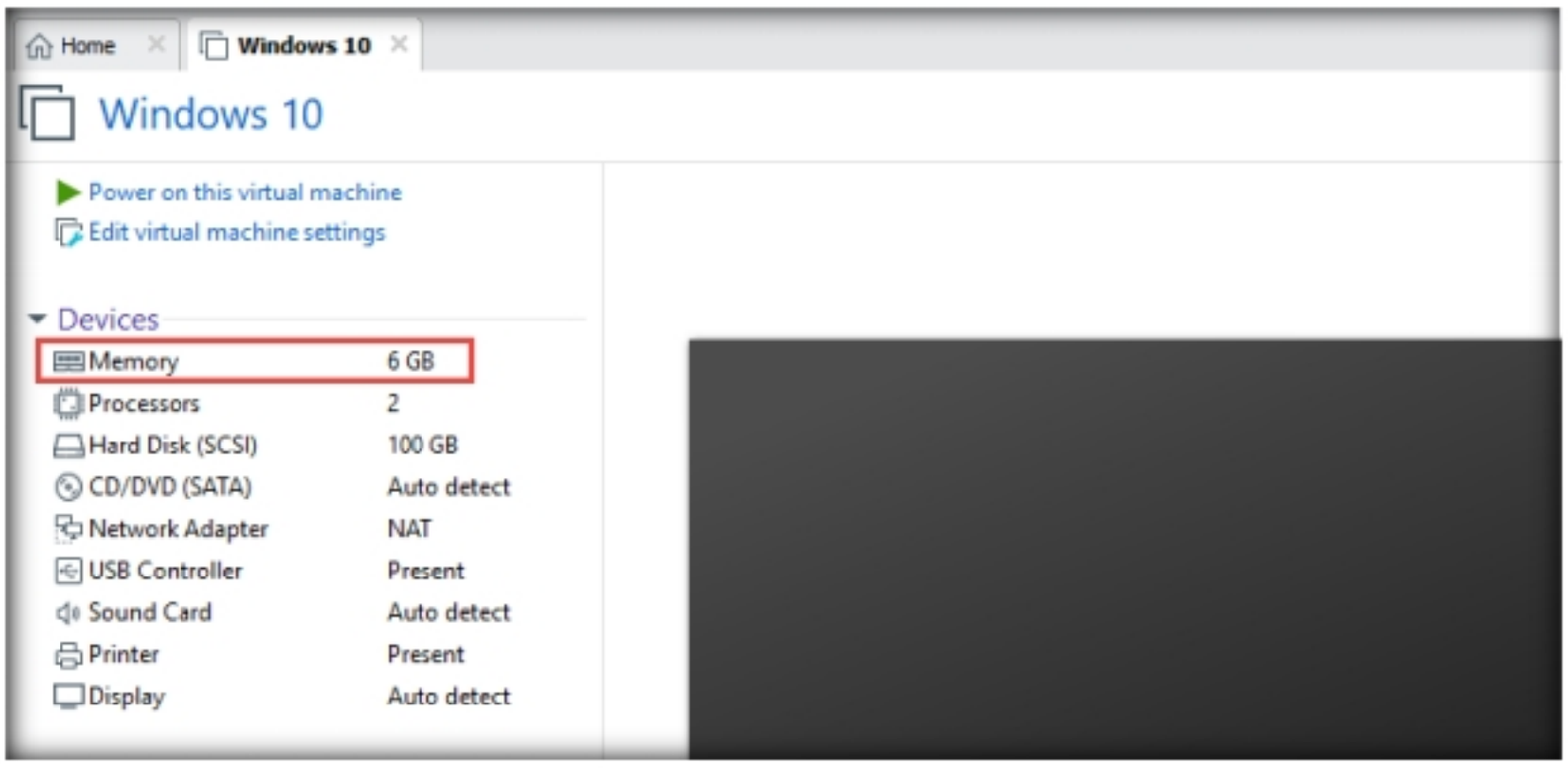


Figure 2.2.38: Windows 10 settings

60. The **Virtual Machine Settings** window appears. On the left-hand pane, toggle the slide bar in the **Memory** section to change **Memory for this virtual machine** to **2 GB** or **2048 MB** and click **OK**.

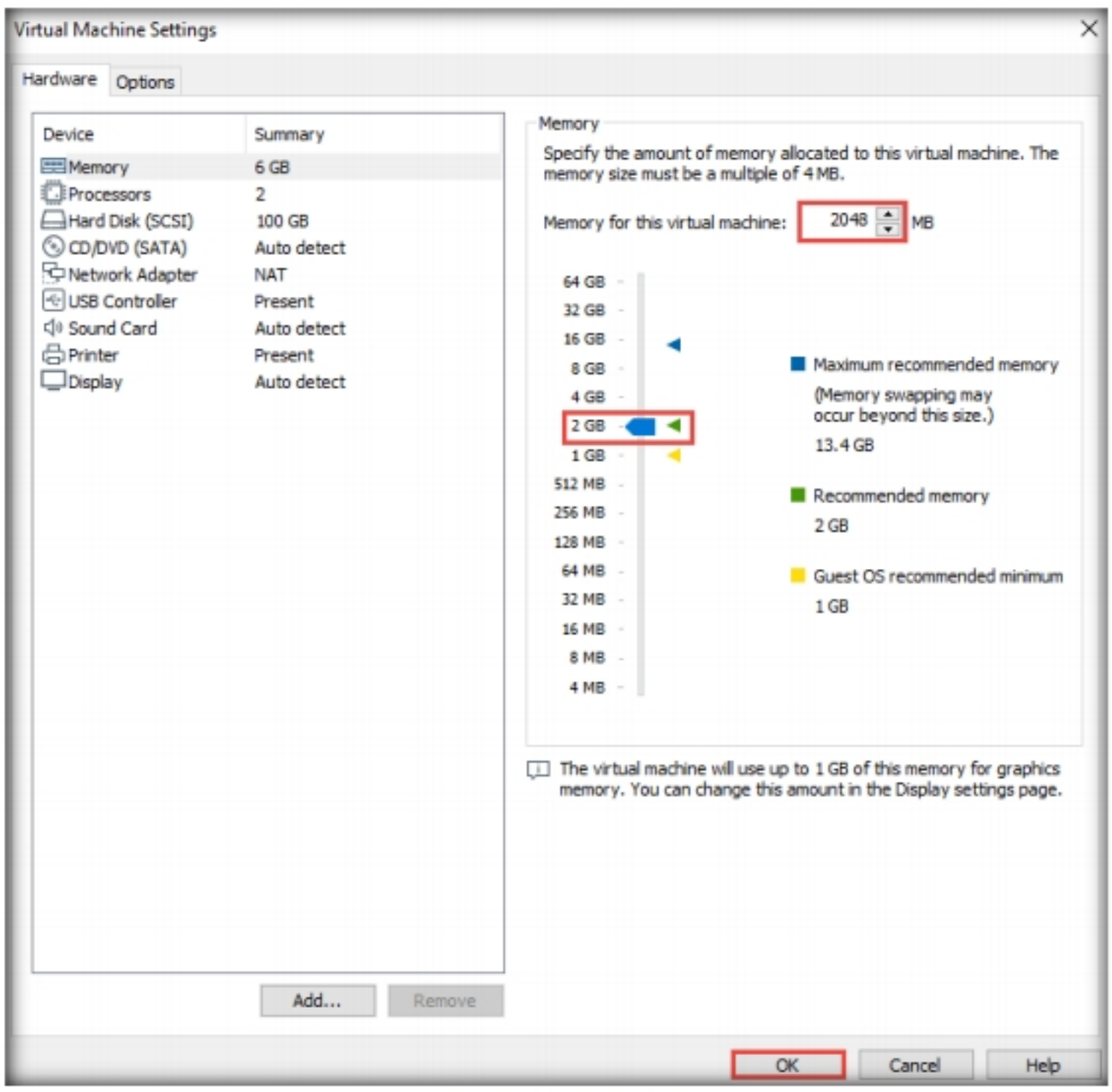


Figure 2.2.39: Windows 10: Increasing memory

61. Check the **Memory** option under the **Devices** section. It should have downgraded to **2 GB** from **6 GB**.

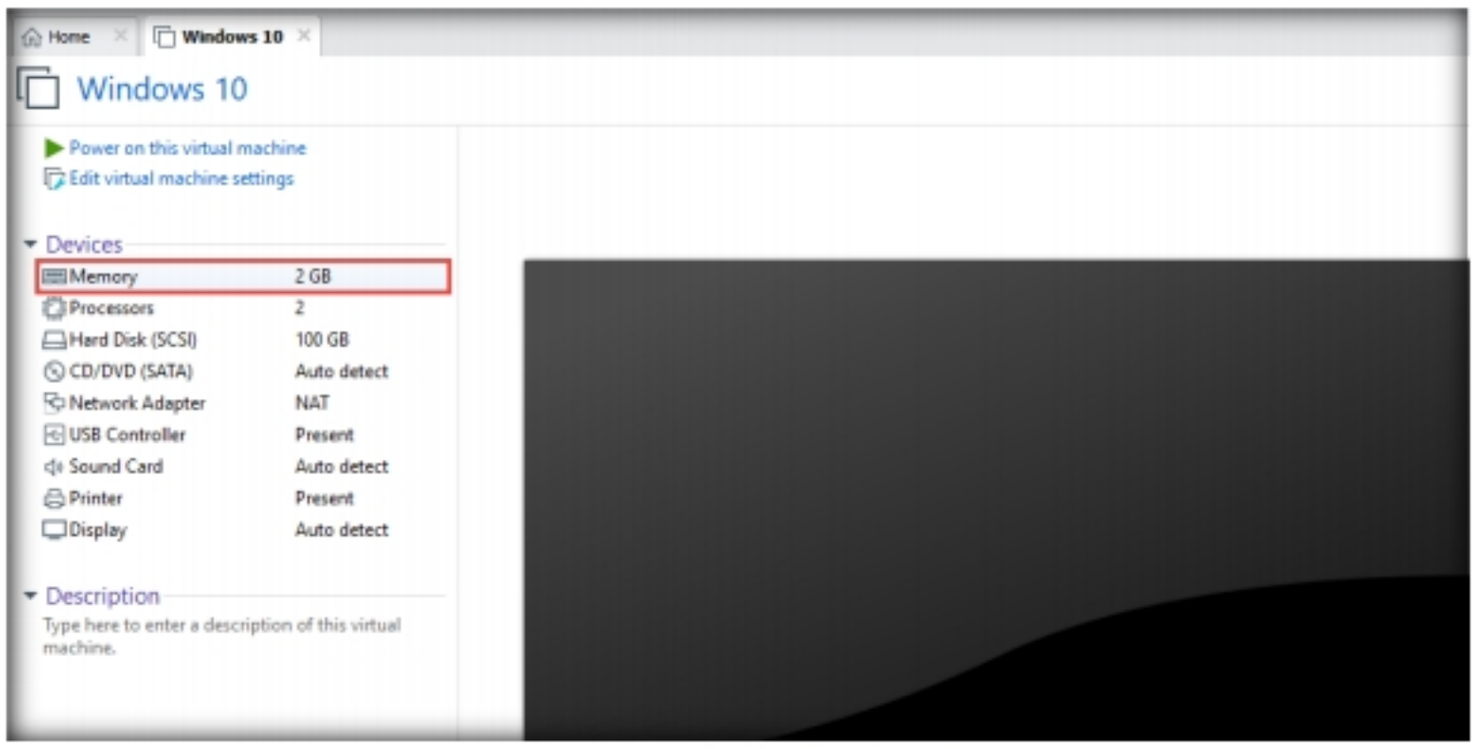


Figure 2.2.40: Windows 10: Memory

TASK 3 — Analyze a Network using the Omnipeek Network Protocol Analyzer

Note: Before starting this lab, we need to find the User IDs associated with the usernames for the **Windows 10** machine.

TASK 3.1 — Download and Install Omnipeek Network Protocol Analyzer

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with credentials **Admin** and **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**), type **https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/** into the address bar, and press **Enter**.

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

4. The **LiveAction** website appears; click the **Start Your 30-Day Trial** button.

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

5. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **I HAVE READ AND AGREE TO THE WEBSITE TERMS AND CONDITIONS** checkbox and check the captcha in the right-hand pane. Click the **Place order** button.

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

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

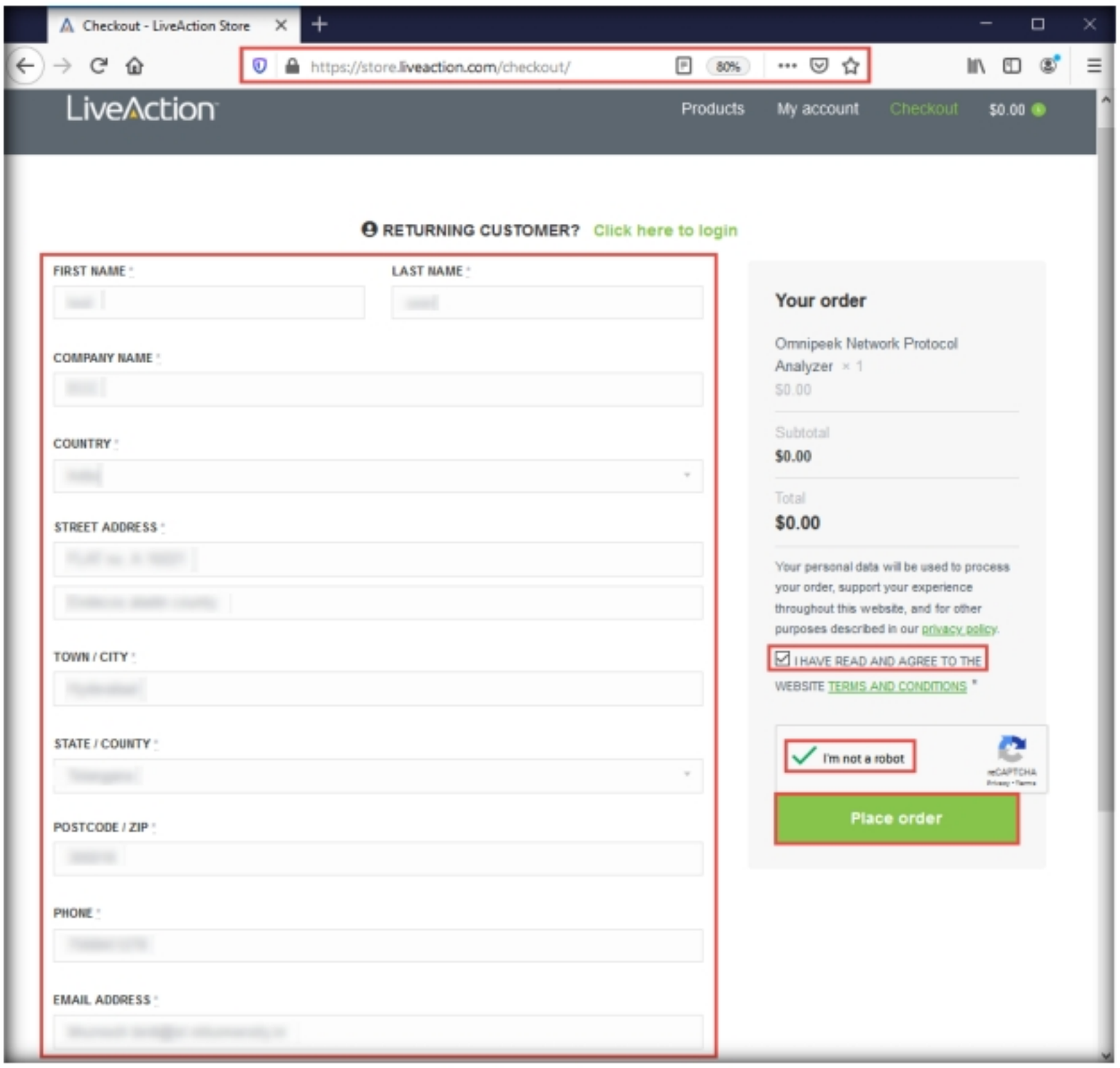


Figure 2.3.1: Omnipeek products window

6. The **Thank you. Your order has been received** webpage appears, displaying the **License Key** and download link for Omnipeek. Click on the **Download Omnipeek** button to begin the download.

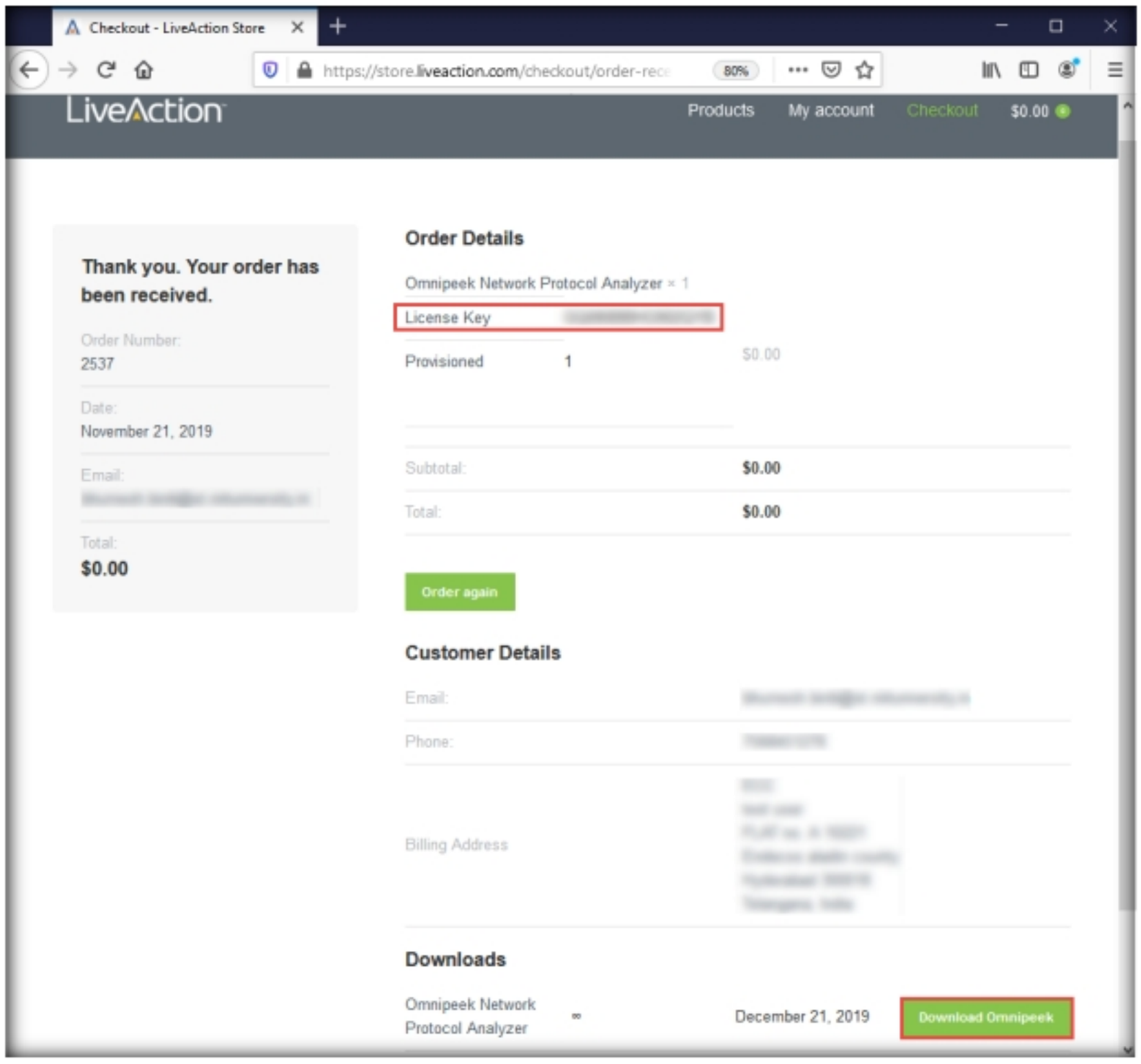


Figure 2.3.2: Thank you. Your order has been received webpage

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

7. The **Opening Omnipeek_13.0.0.msi** pop-up appears; click **Save File** to download the application.

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

8. On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek_13.0.0.msi**.

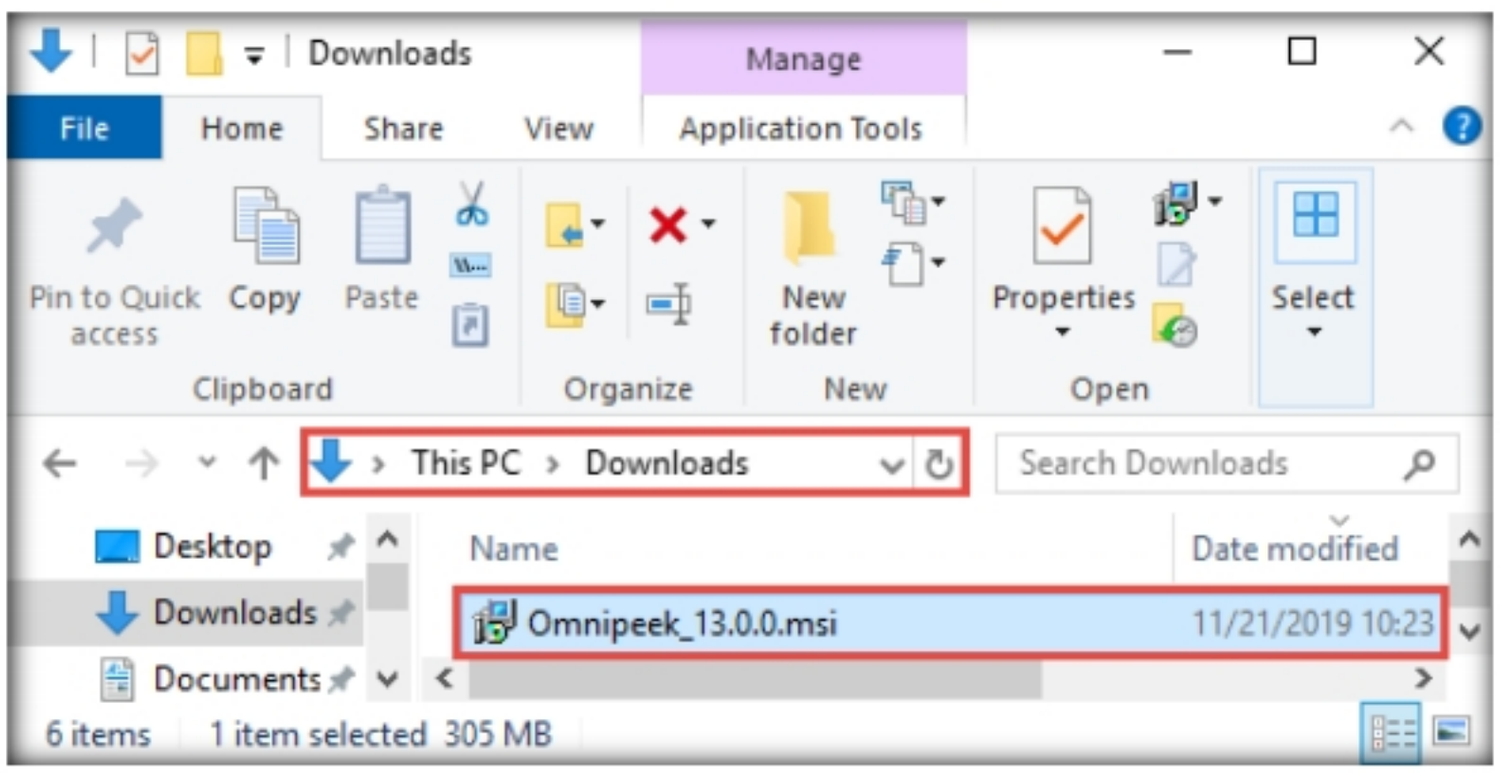


Figure 2.3.3: Double-click Omnipeek application

9. If an **Open File - Security Warning** pop-up appears, click **Run**.
10. The **OmniPeek Installer** wizard appears; click **Next**.

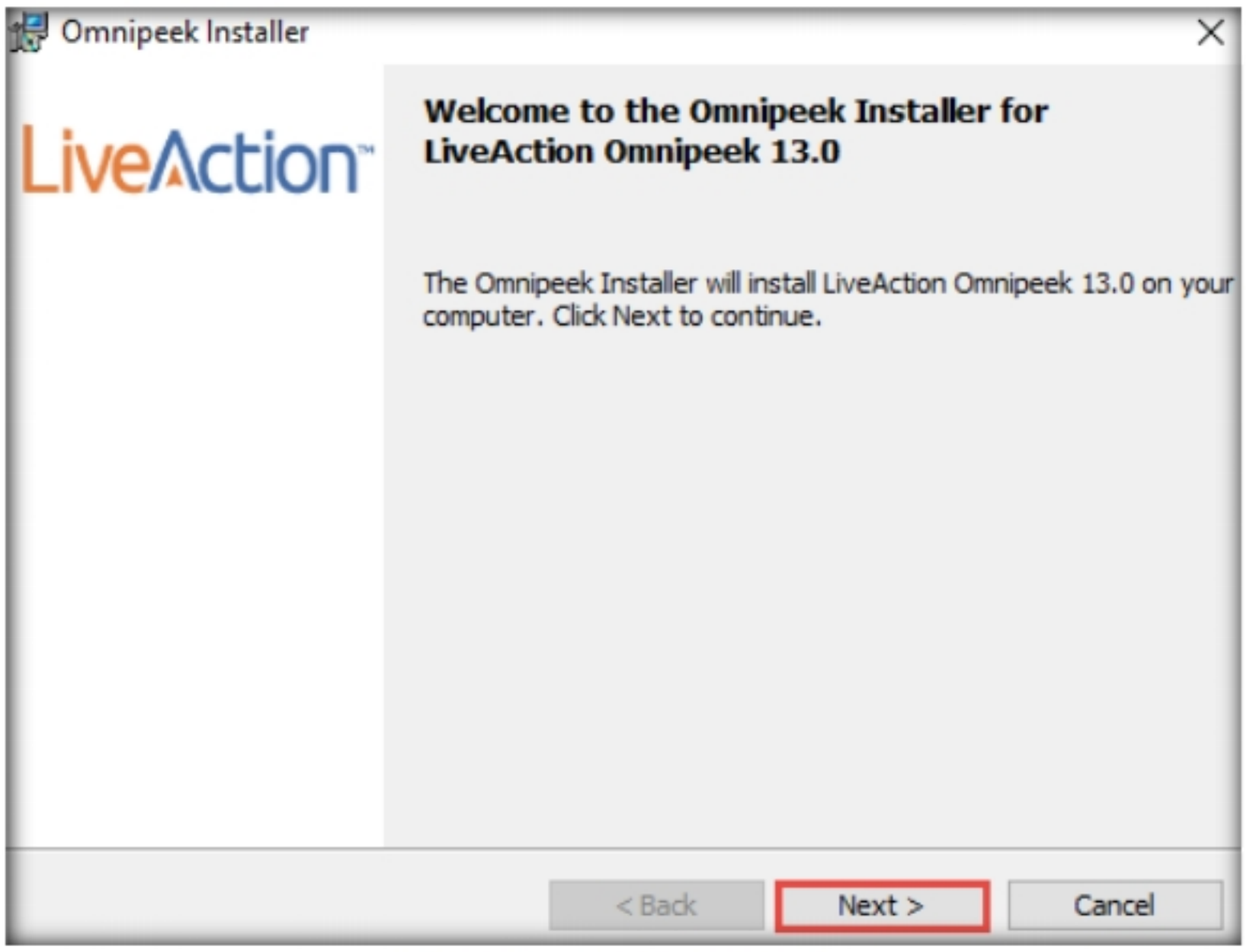


Figure 2.3.4: Omnipeek Installer Wizard

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

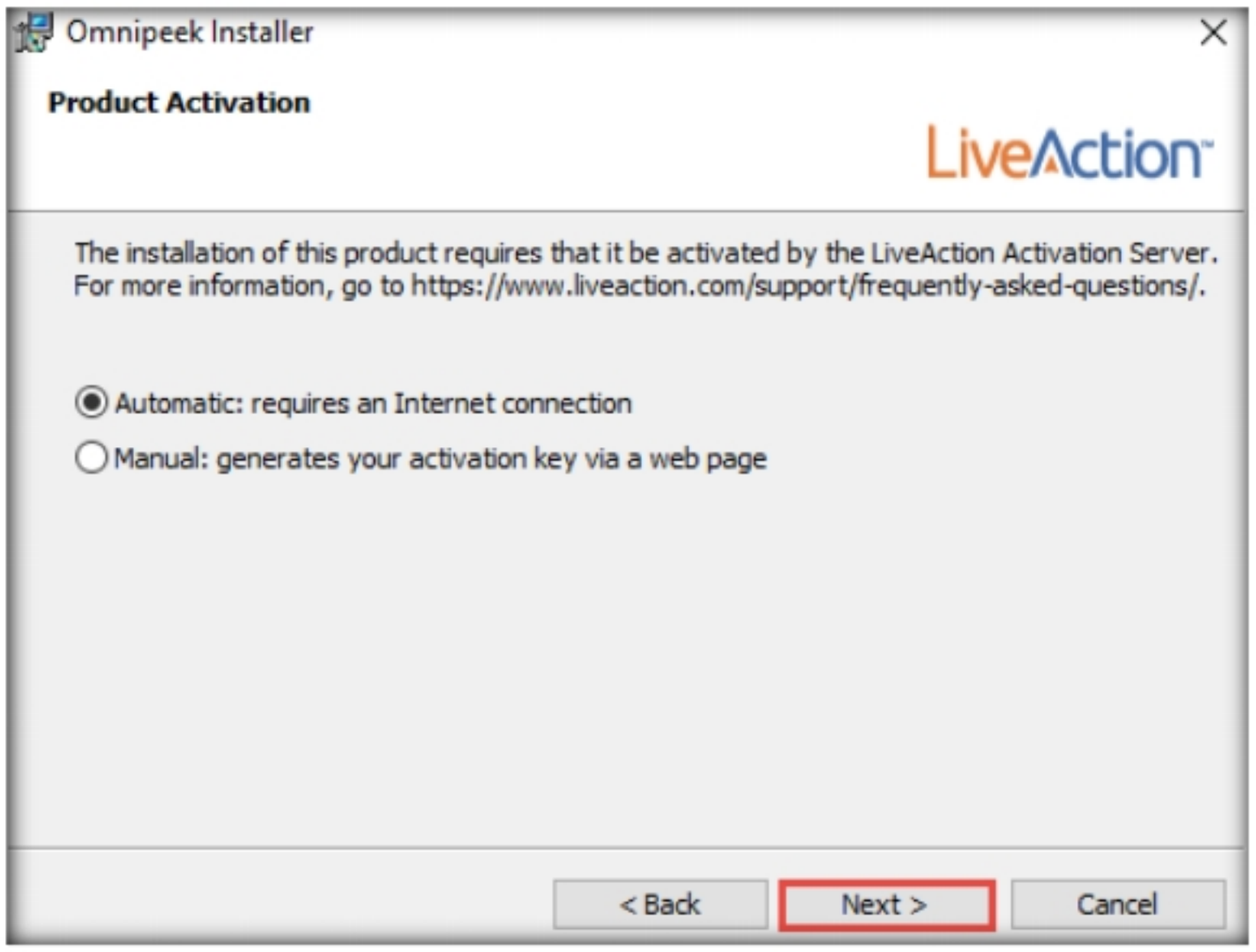


Figure 2.3.5: Omnipeek Product Activation wizard

12. The **Customer Information** wizard appears; type a **Company Name** (here, **abc**) and **Email** (provided at the time of registration). For the serial number field, switch to the **Mozilla Firefox** browser and copy the **License Key**. Close the browser.
13. Switch back to the **Ompnipeek Installer** window, paste the **License Key** in the **Serial Number or Product Key** field, and then click **Next**.

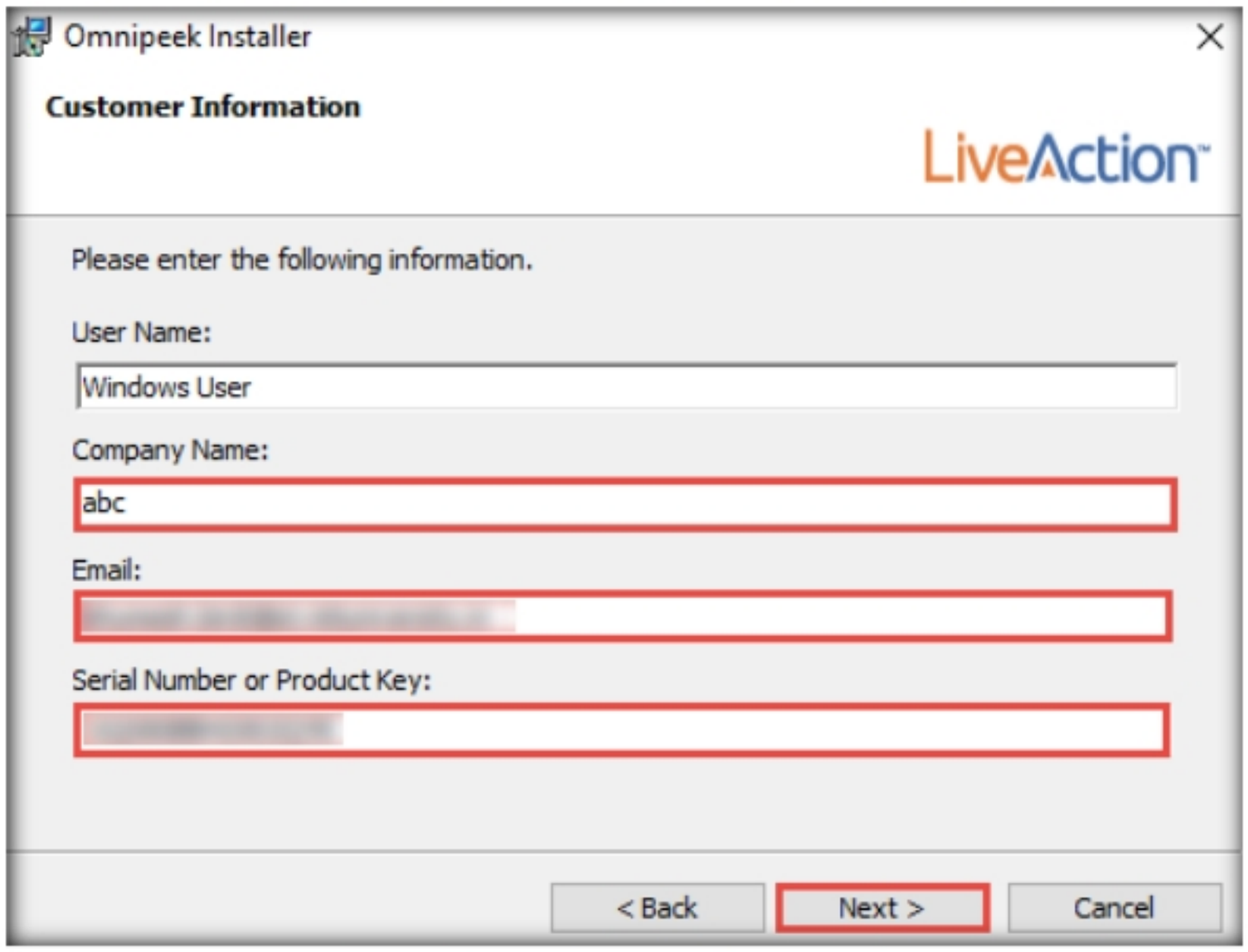


Figure 2.3.6: Omnipeek Customer Information section

14. Follow the wizard-driven installation steps to install Omnipeek using the default settings.
15. While **Installing LiveAction Omnipeek**, if a **User Account Control** pop-up appears, click **Yes**.
16. On completion of the installation, the **Omnipeek Installer Completed** wizard appears; uncheck **View Readme**, ensure that the **Launch Omnipeek** option is checked, and click **Finish**.

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

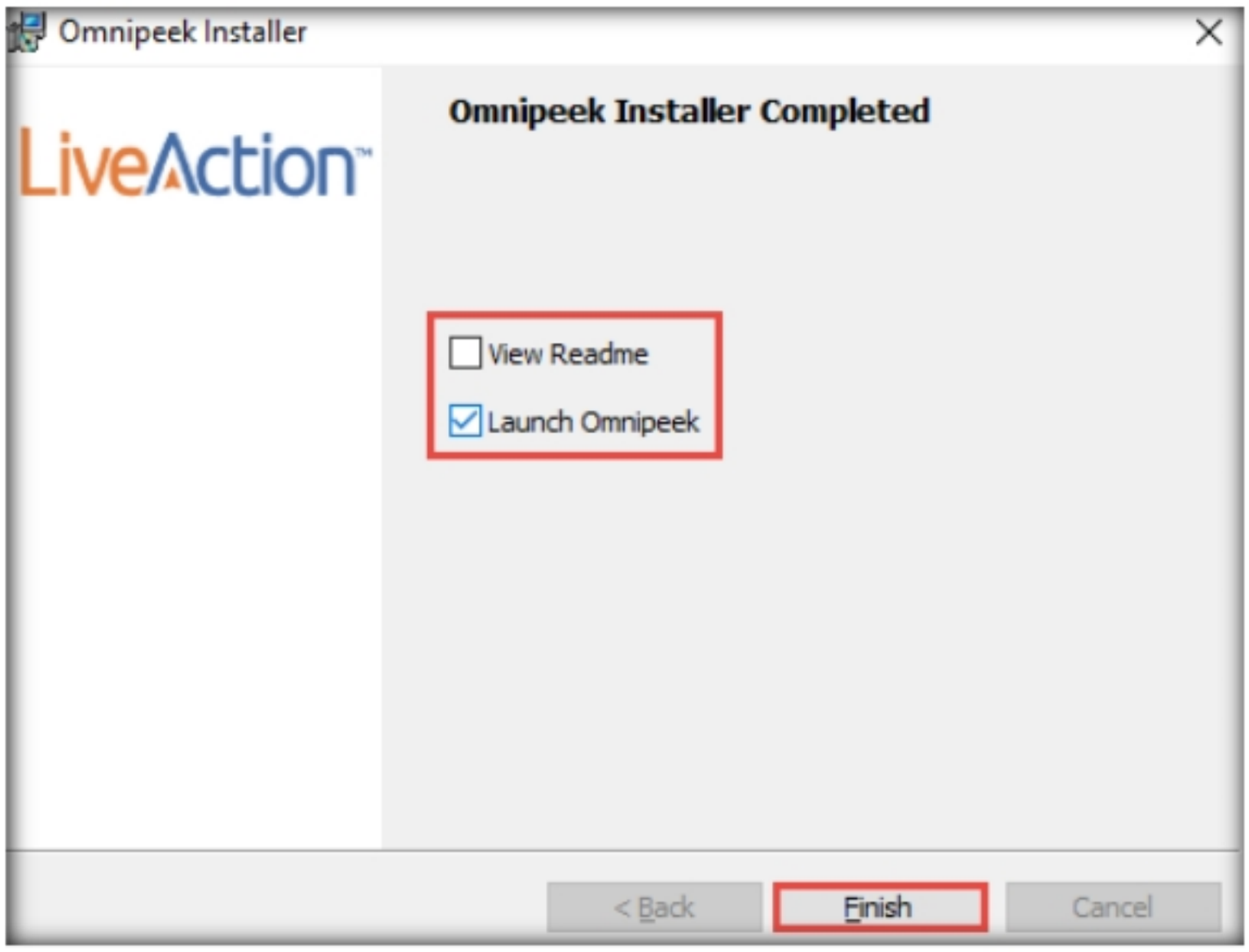


Figure 2.3.7: Omnipeek installation completed

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

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

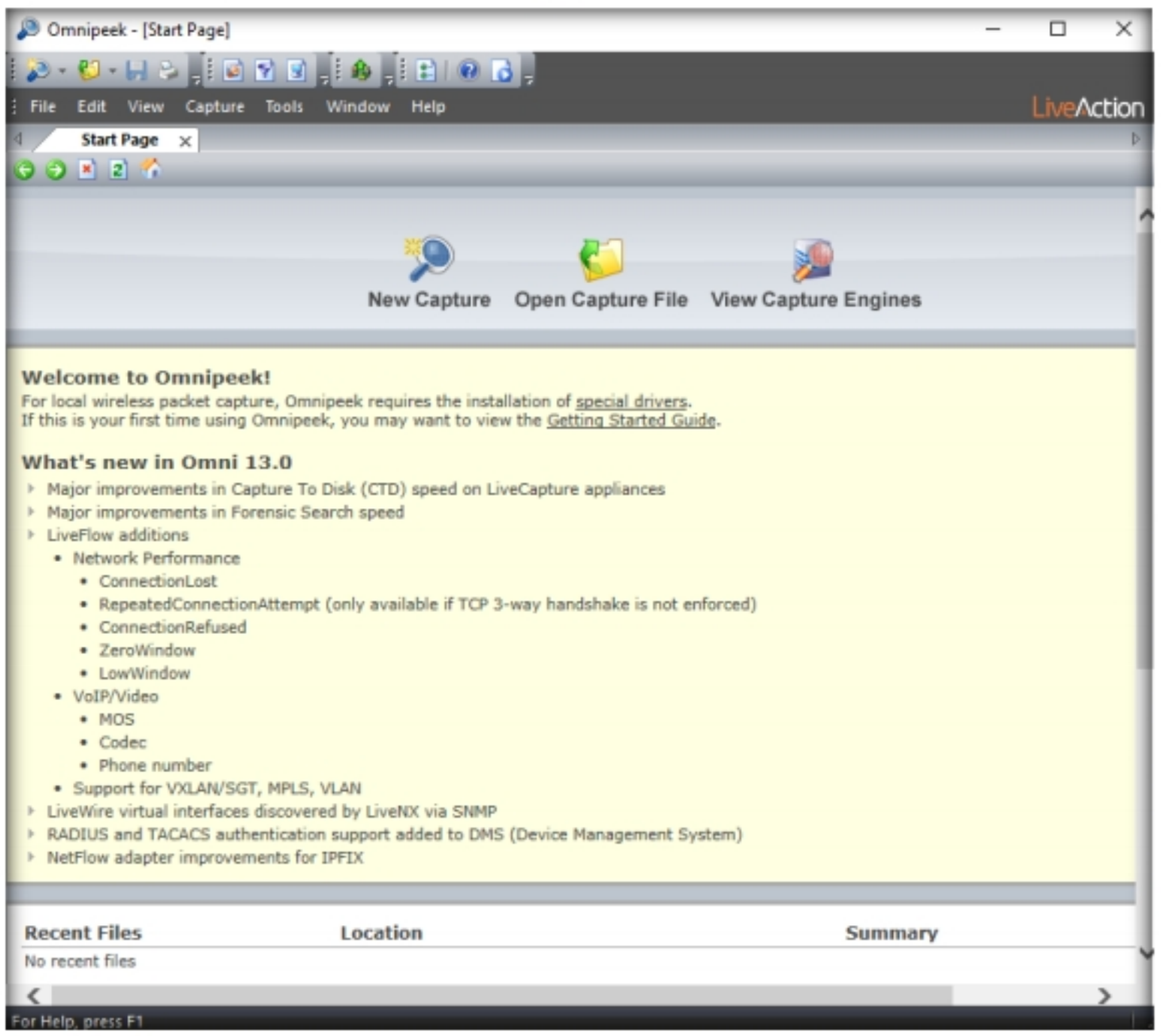


Figure 2.3.8: Omnipeek main window

TASK 3.2

Start a New Capture

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

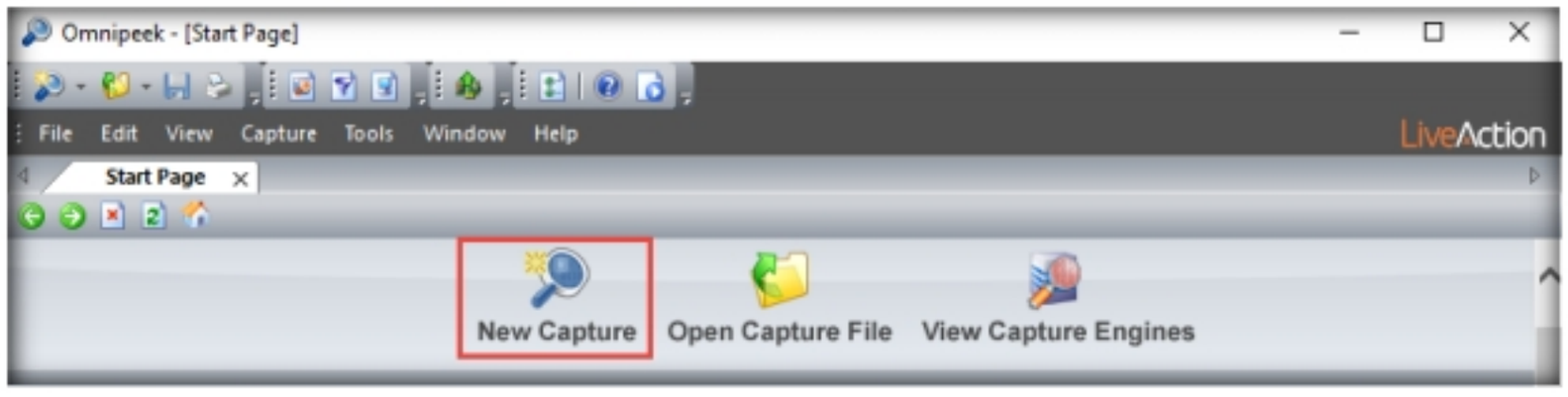


Figure 2.3.9: Starting a new capture

20. The **Capture Options** window appears; by default, the **Adapter** option opens-up.
21. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS 10** node, select **Ethernet0**, and click **OK**.

Note: The ethernet adapter will vary in your lab environment.

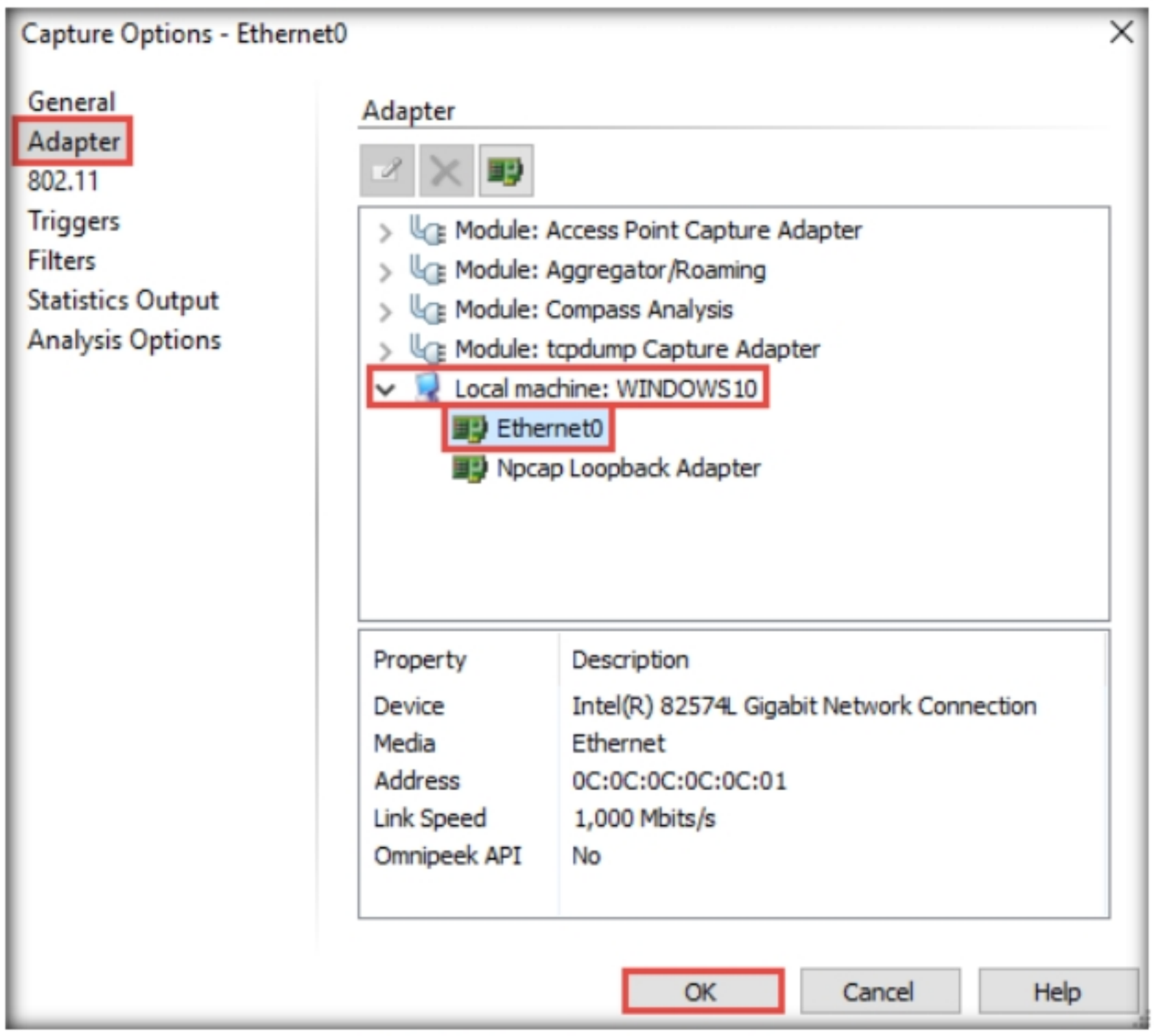


Figure 2.3.10: OmniPeek capture options: Adapter

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

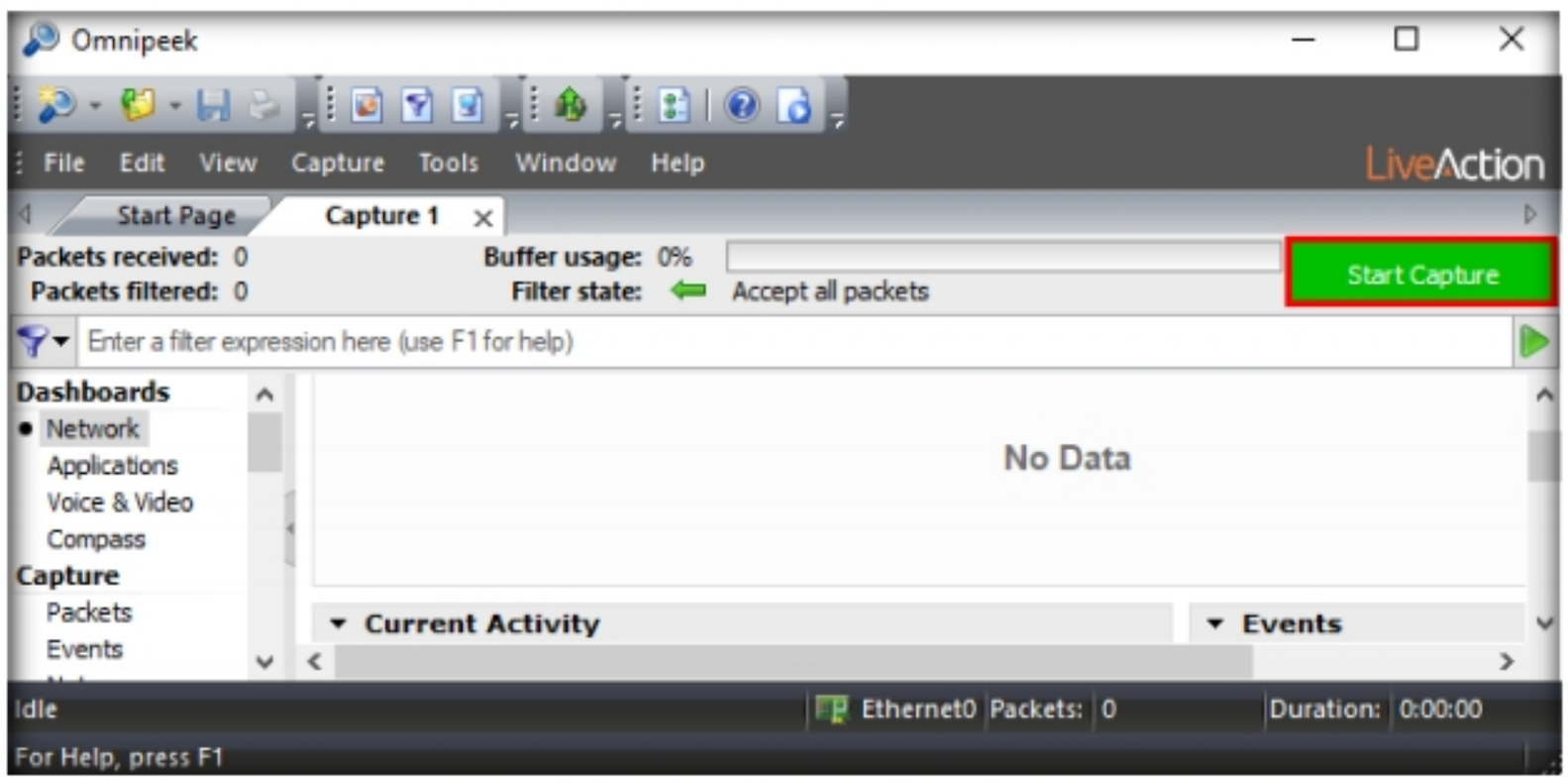


Figure 2.3.11: Starting packet capture

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

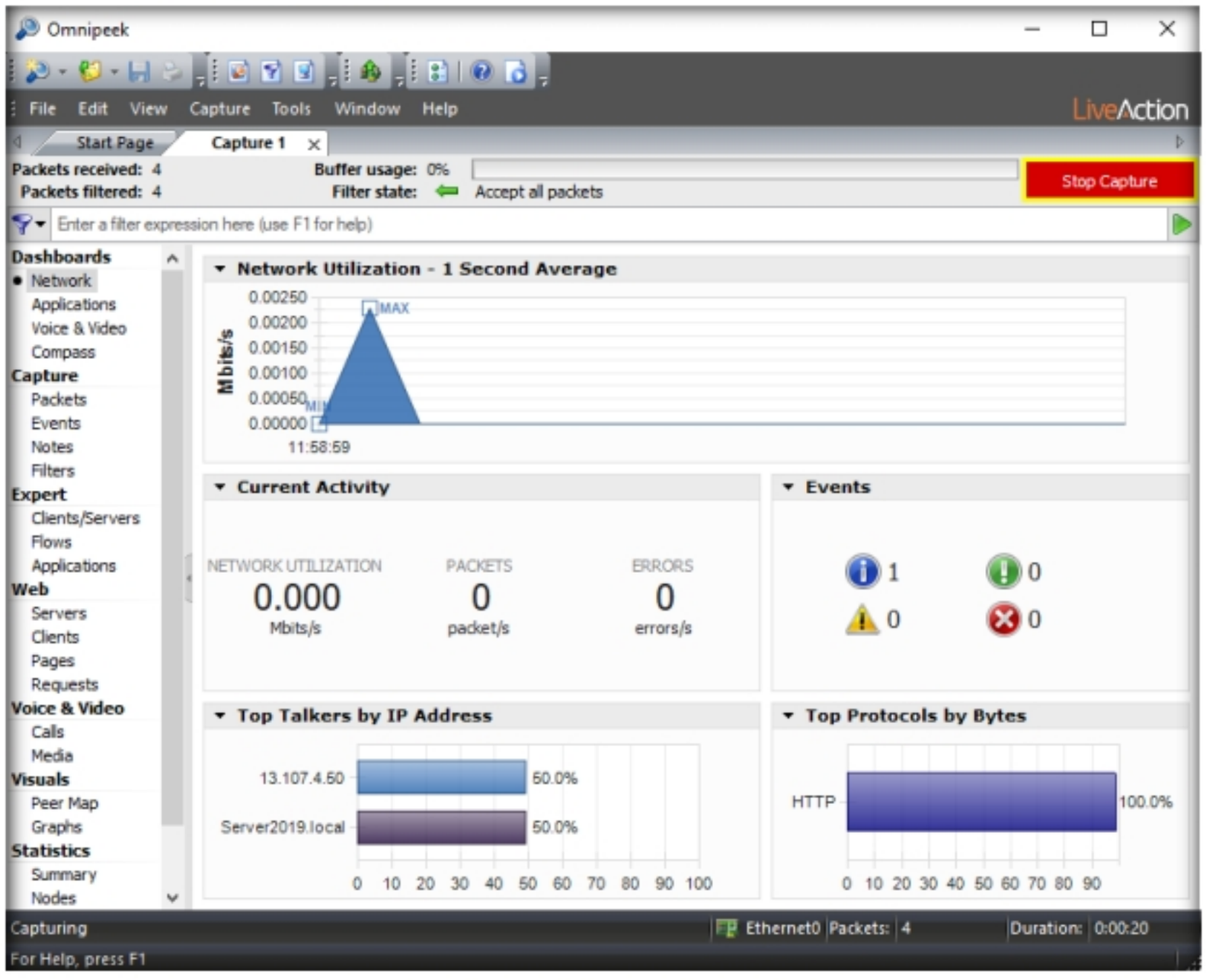


Figure 2.3.12: Start Capture tab changes to Stop Capture

TASK 3.3

Browse the Internet on the Target System

24. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
25. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

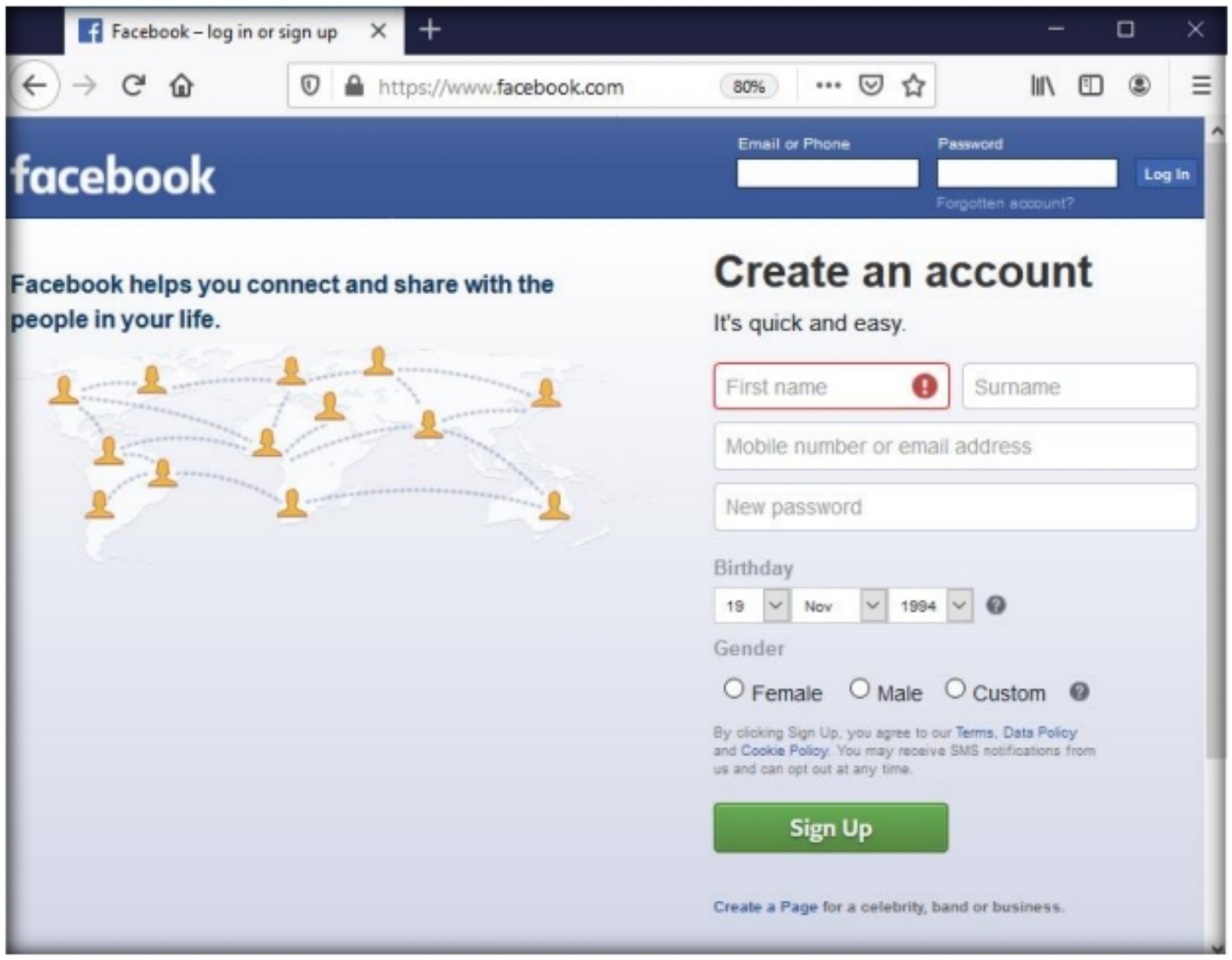


Figure 2.3.13: Browsing the Internet on Windows Server 2019

TASK 3.4

Analyze the Captured Results

26. Now, switch back to the **Windows 10** virtual machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.
27. You can observe the network traffic along with the websites visited by the target machine.

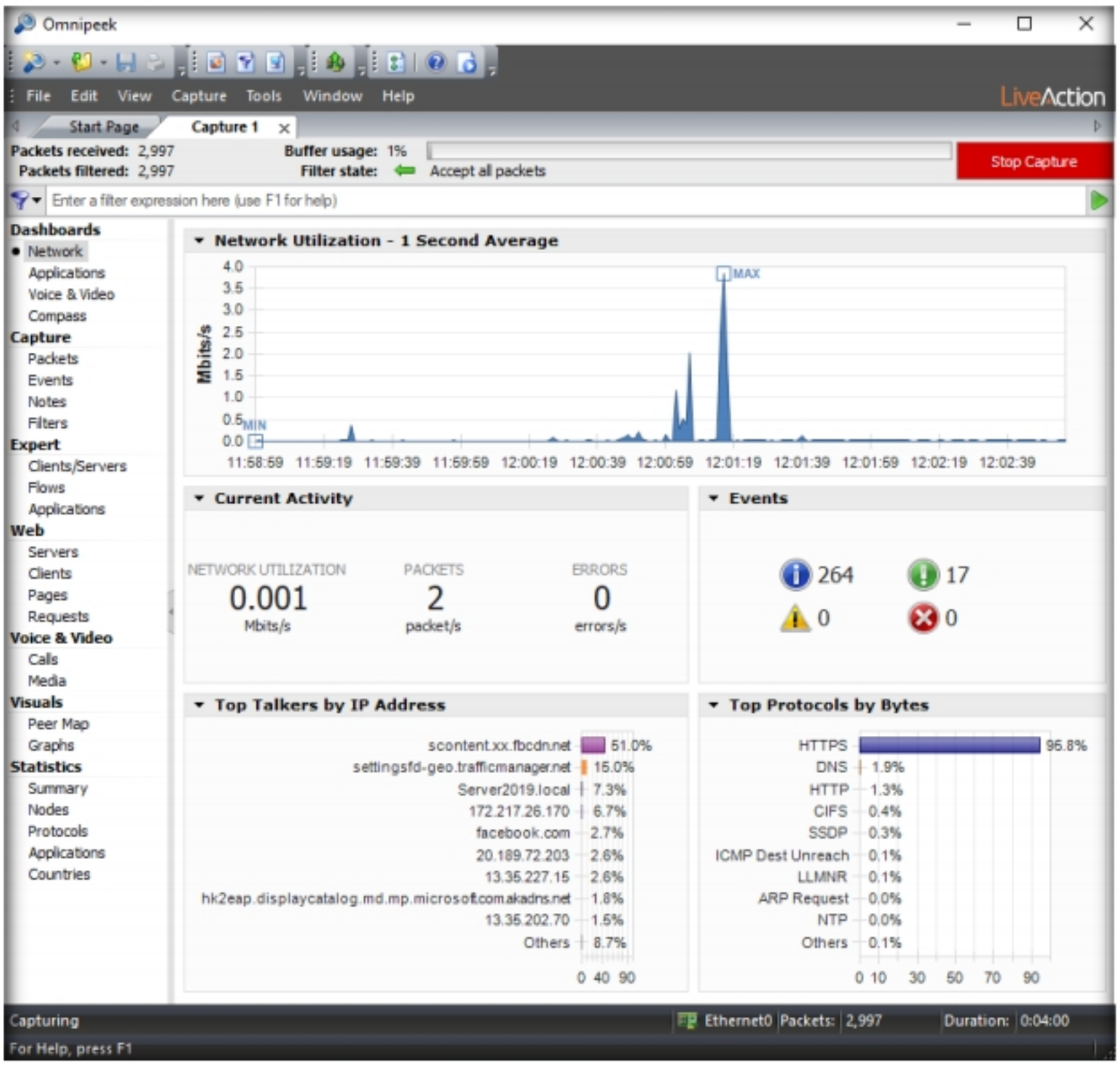


Figure 2.3.14: Omnipeek statistical analysis of the data

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

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

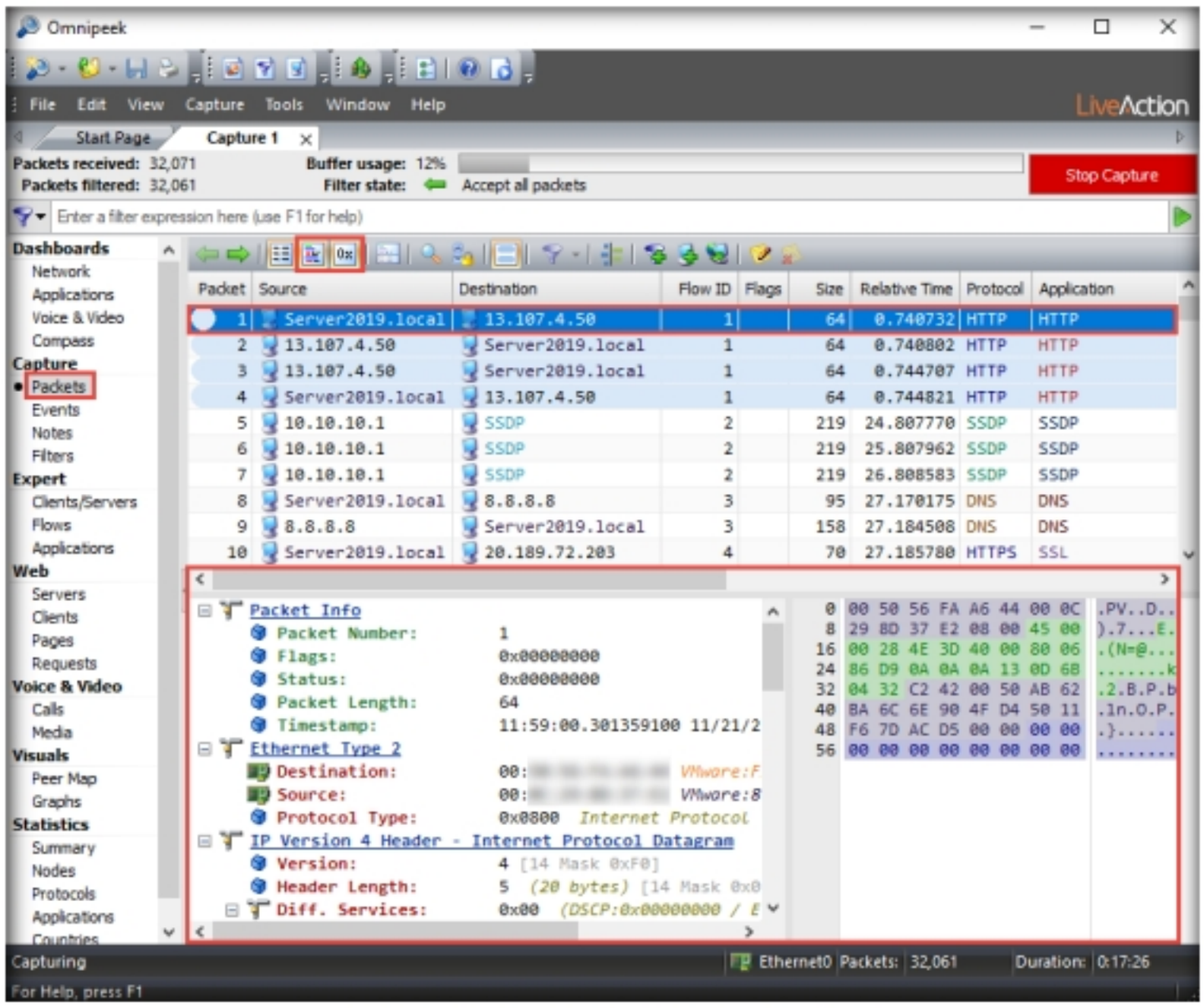


Figure 2.3.15: Omnipeek displaying captured packets

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

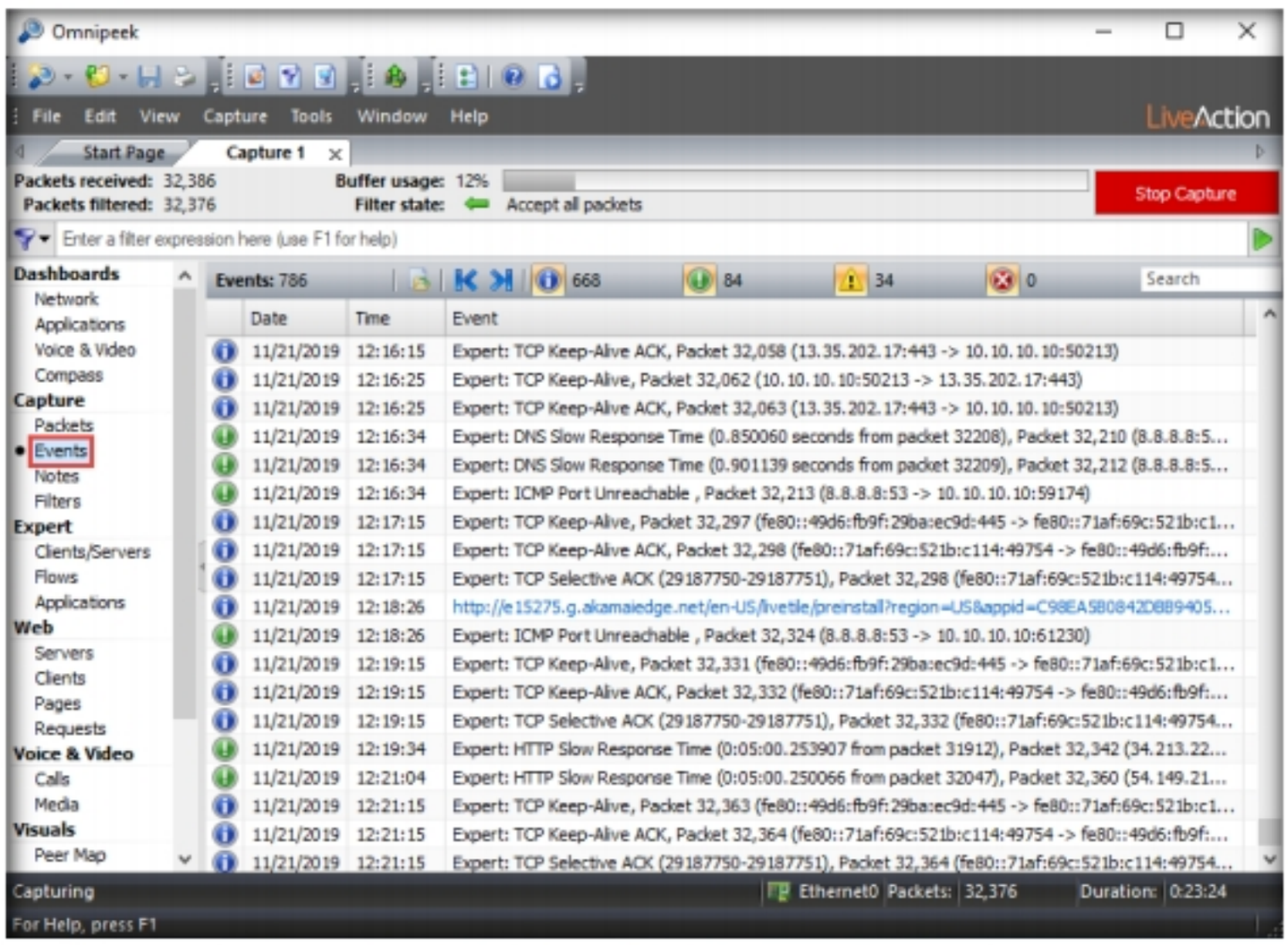


Figure 2.3.16: Omnipeek displaying captured events

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

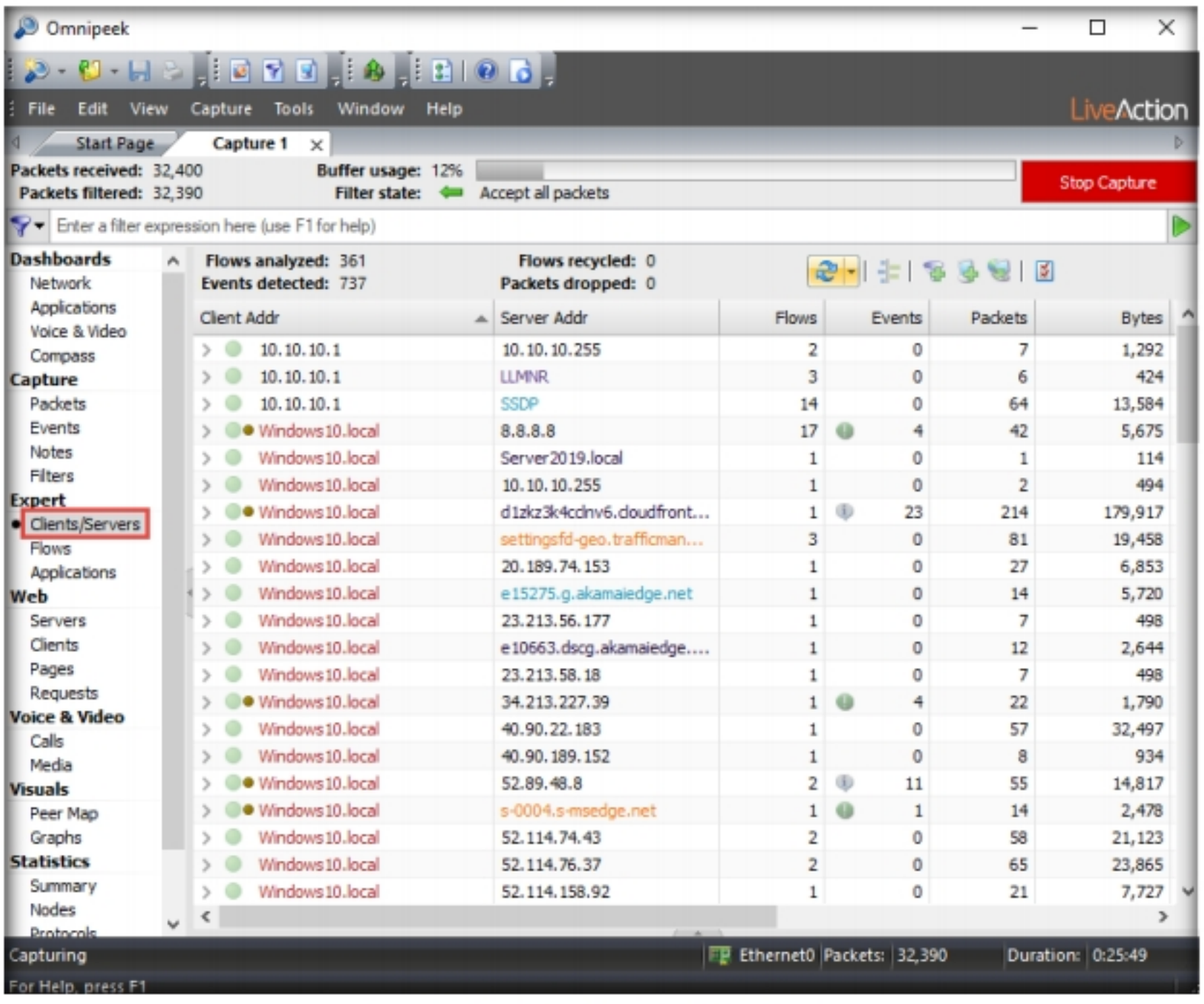


Figure 2.3.17: Omnipeek displaying Clients/Servers

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

33. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.
34. Expand both the client nodes (here, **SERVER2019.local** and **WINDOWS10.local**) and click on any packet to view its detailed information under the **Details** tab in the lower section of the window.

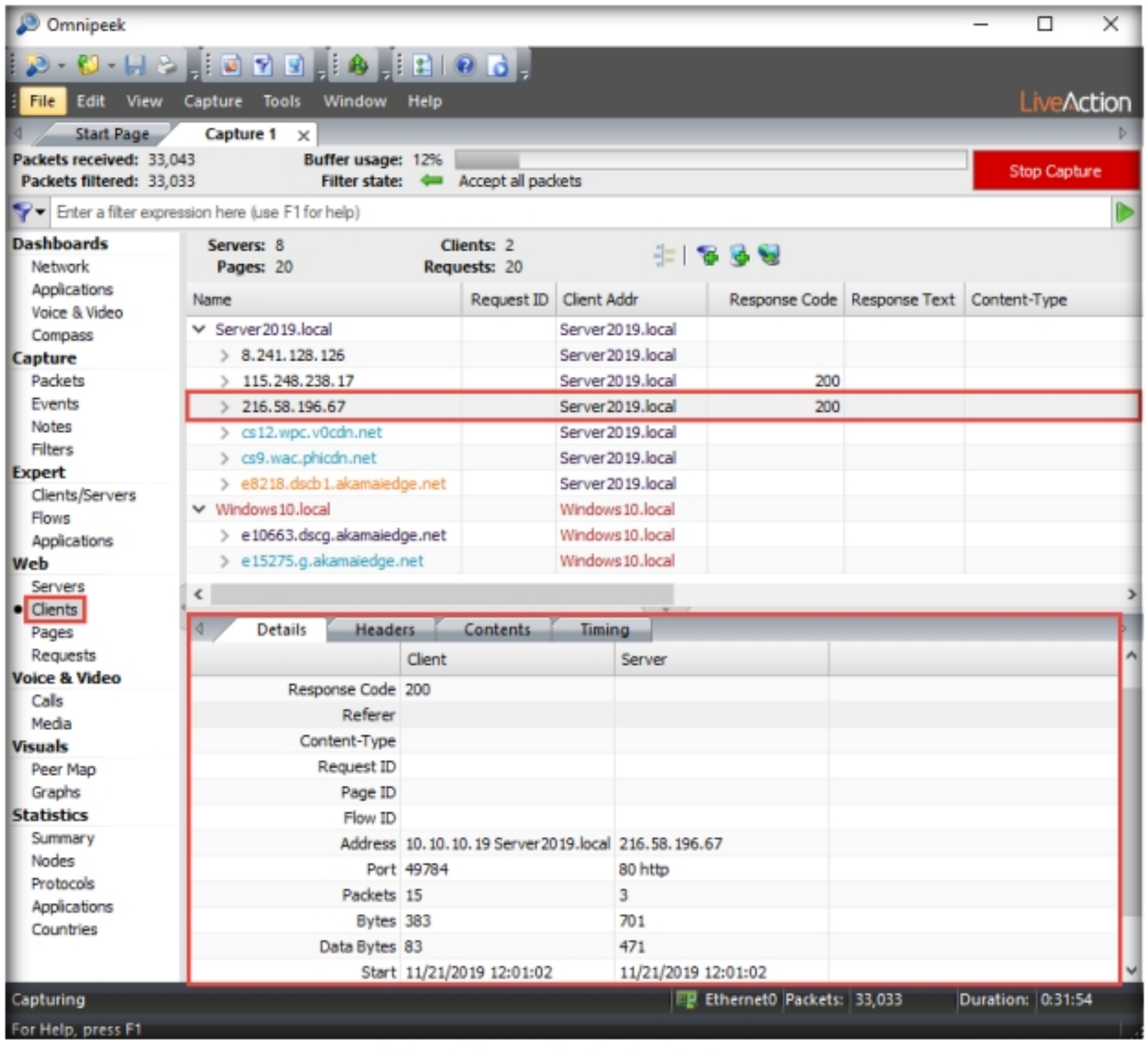


Figure 2.3.18: Omnipeek displaying Clients

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

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

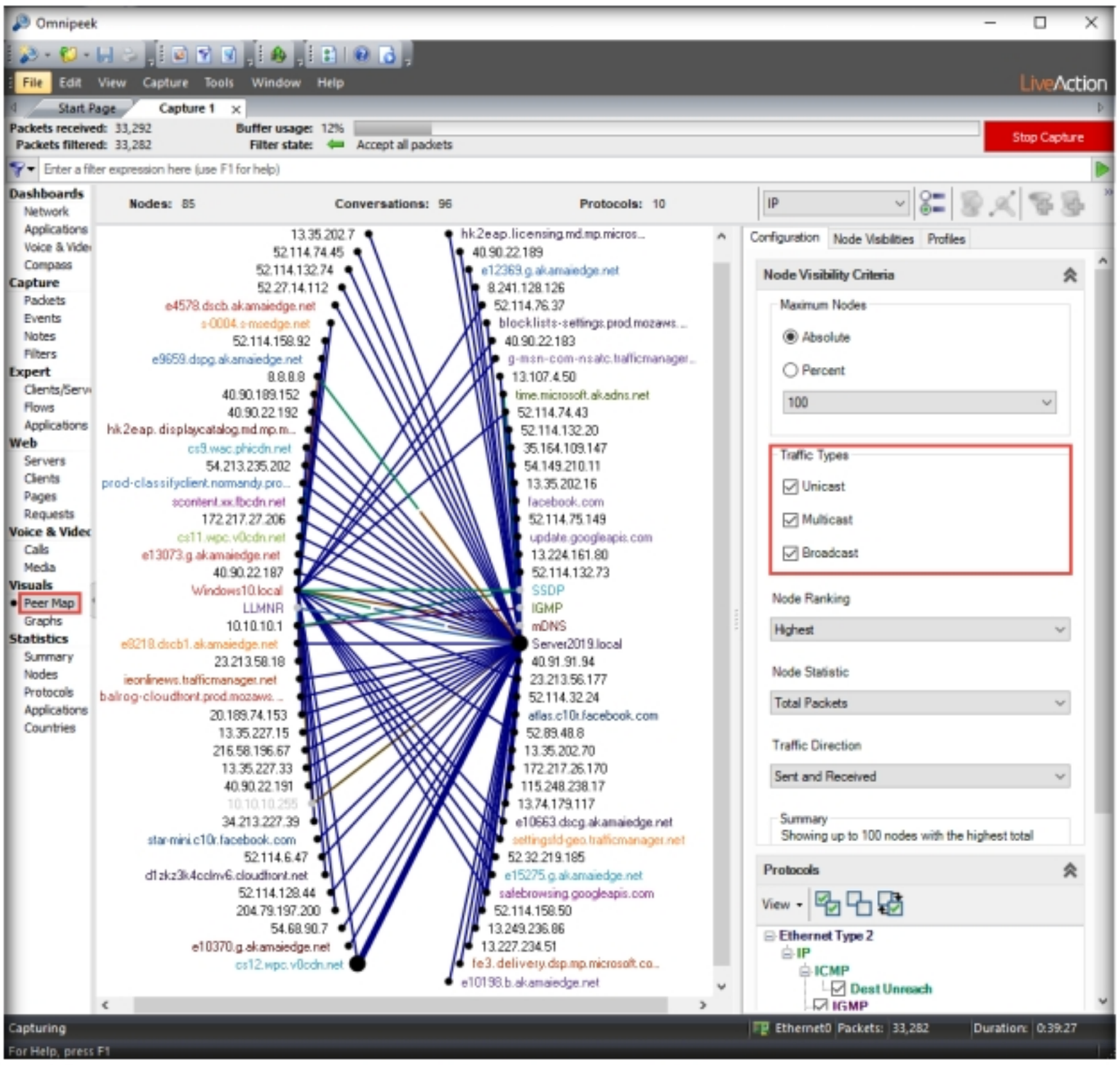


Figure 2.3.19: Omnipeek displaying Peer Map

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

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

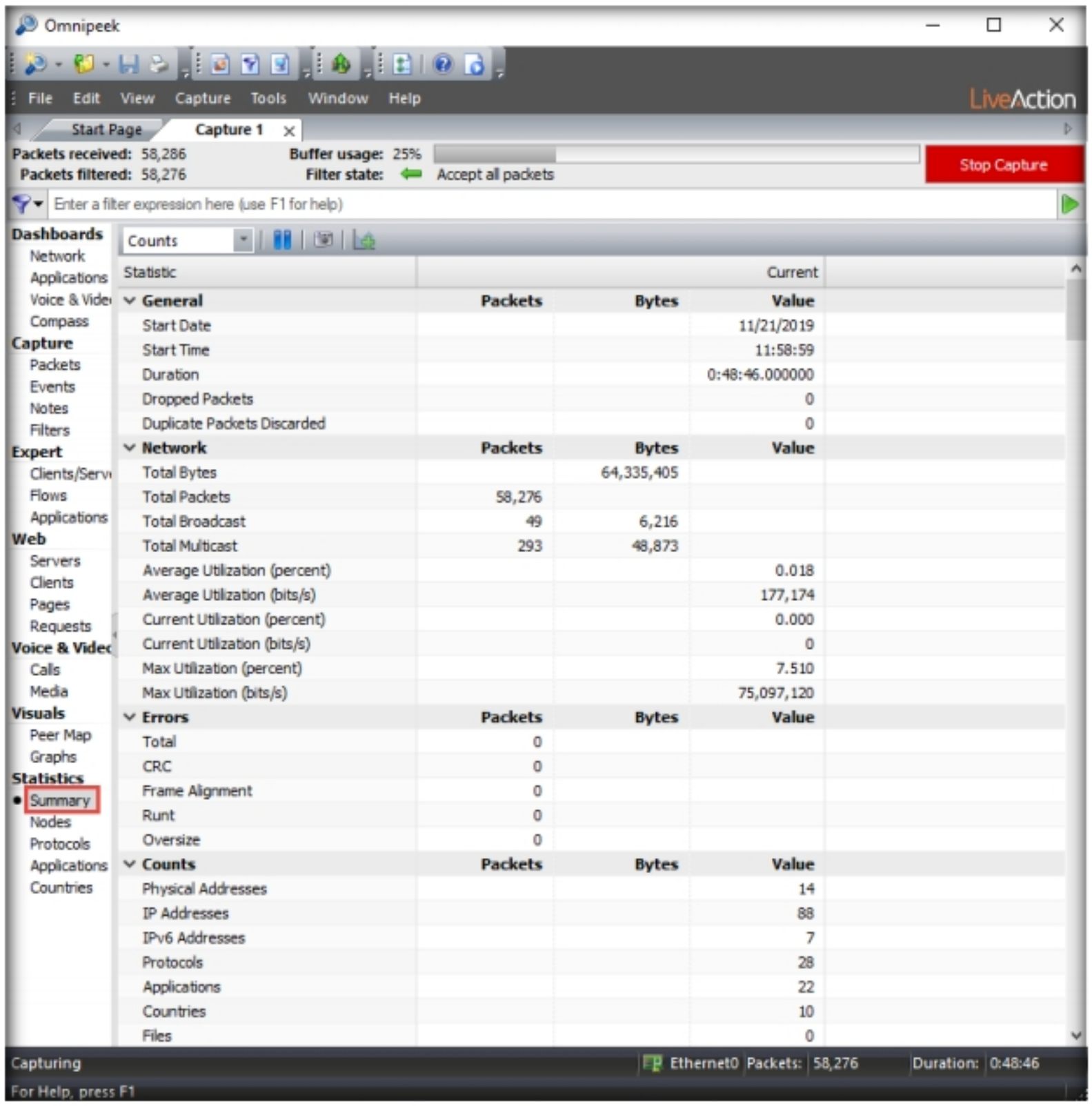


Figure 2.3.20: OmniPeek Summary details

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

TASK 3.5

Save the Captured Results

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

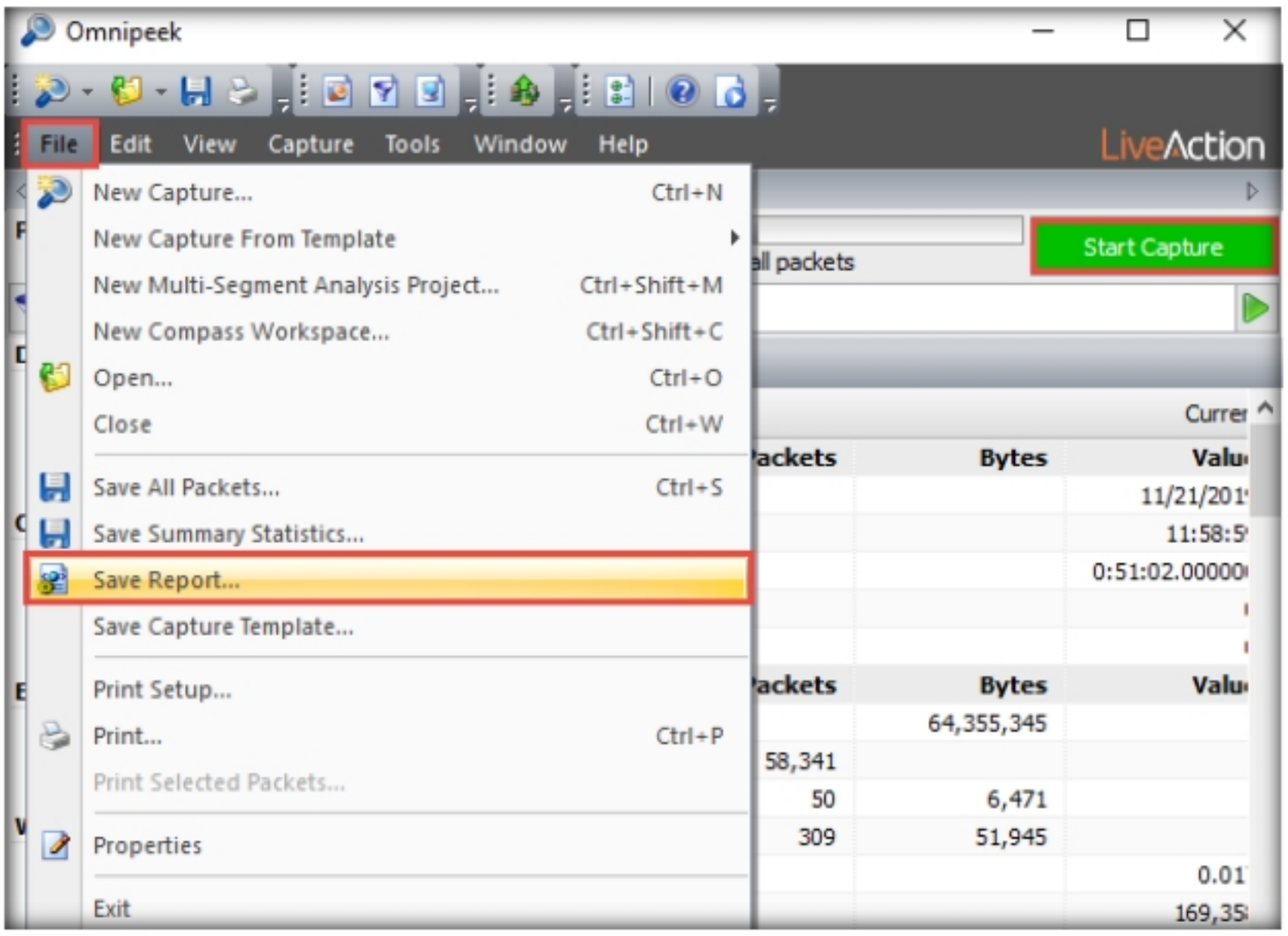


Figure 2.3.21 OmniPeek saving the results

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

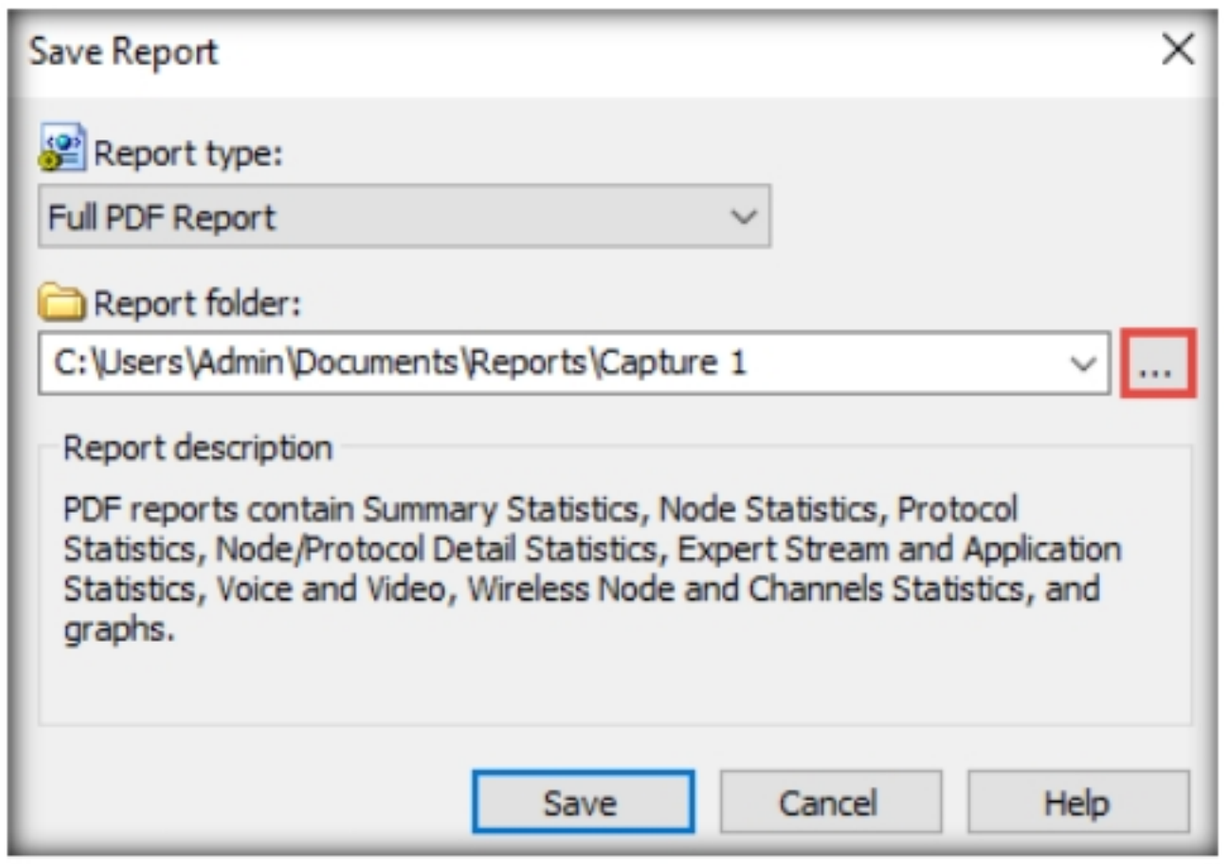


Figure 2.3.22: Save Report window

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

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

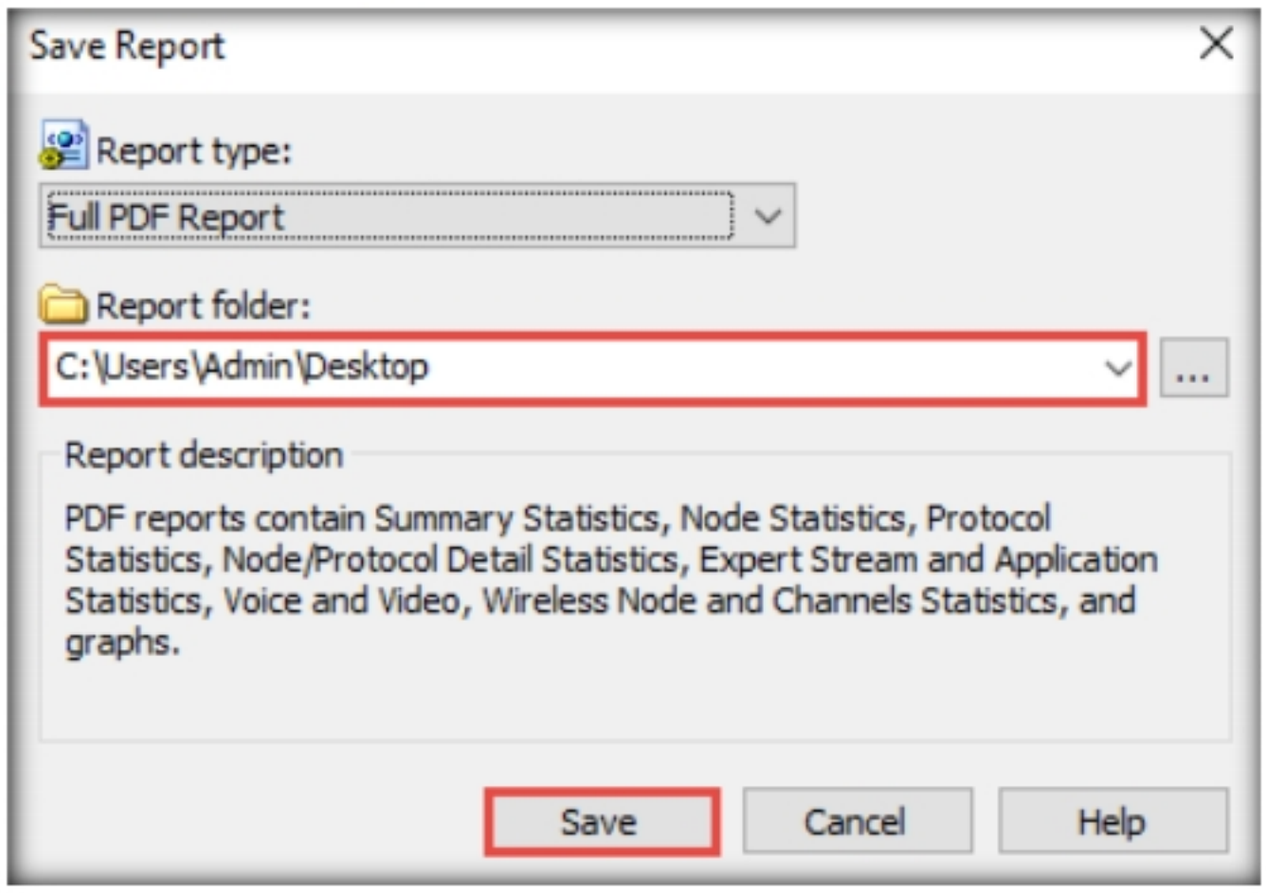


Figure 2.3.23 Save Report window

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

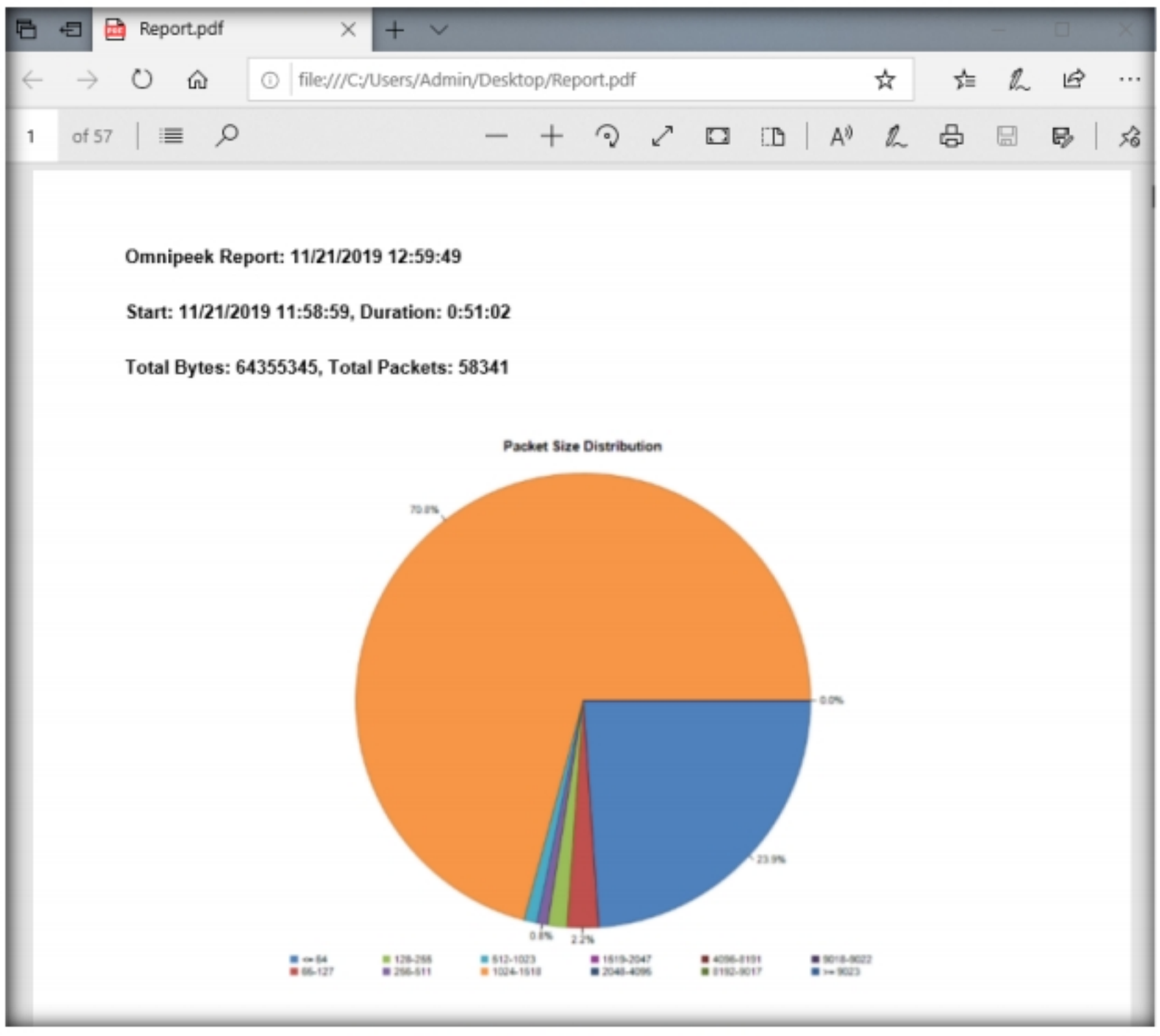
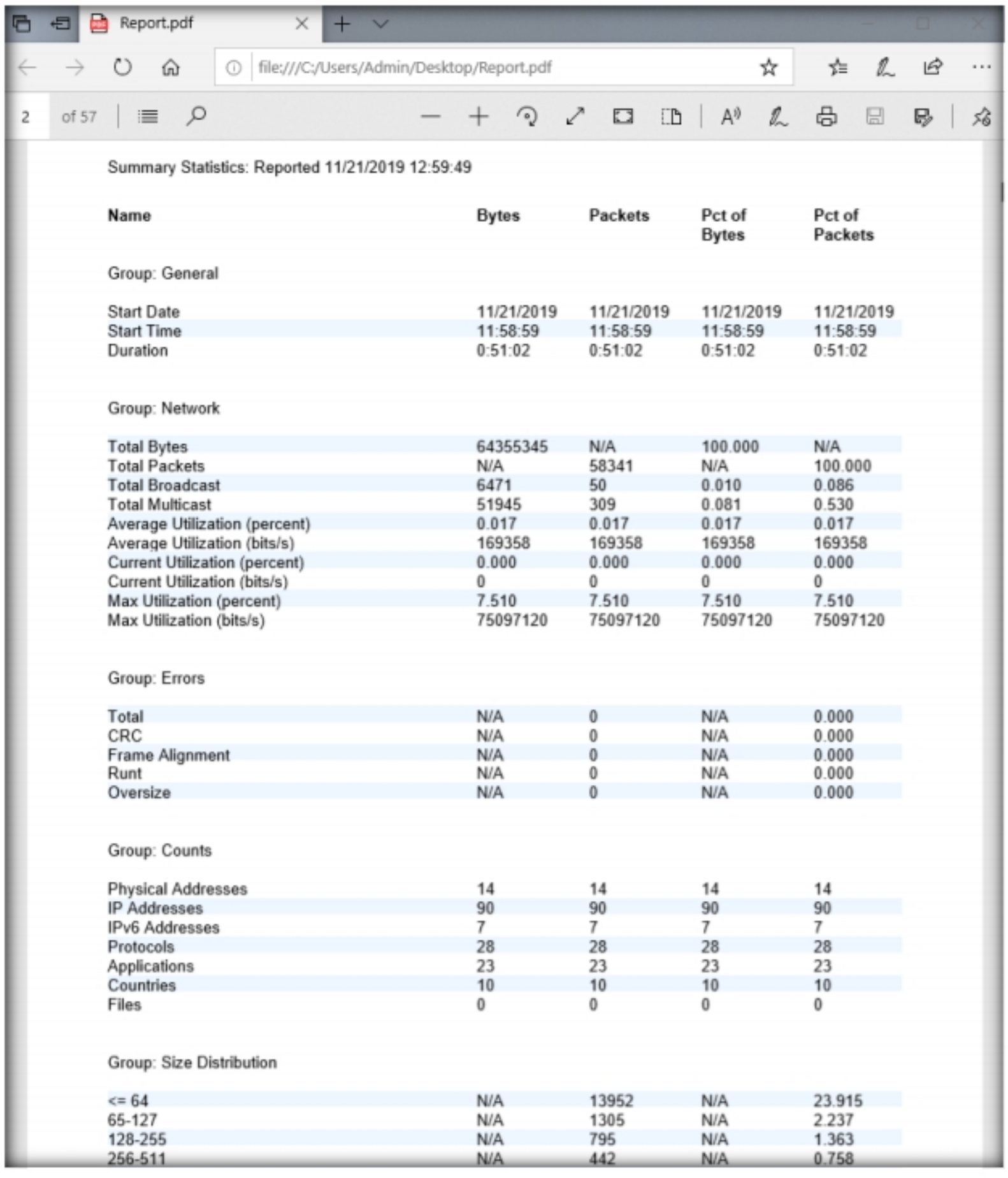


Figure 2.3.24: OmniPeek Report in PDF format

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



Name	Bytes	Packets	Pct of Bytes	Pct of Packets
Group: General				
Start Date	11/21/2019	11/21/2019	11/21/2019	11/21/2019
Start Time	11:58:59	11:58:59	11:58:59	11:58:59
Duration	0:51:02	0:51:02	0:51:02	0:51:02
Group: Network				
Total Bytes	64355345	N/A	100.000	N/A
Total Packets	N/A	58341	N/A	100.000
Total Broadcast	6471	50	0.010	0.086
Total Multicast	51945	309	0.081	0.530
Average Utilization (percent)	0.017	0.017	0.017	0.017
Average Utilization (bits/s)	169358	169358	169358	169358
Current Utilization (percent)	0.000	0.000	0.000	0.000
Current Utilization (bits/s)	0	0	0	0
Max Utilization (percent)	7.510	7.510	7.510	7.510
Max Utilization (bits/s)	75097120	75097120	75097120	75097120
Group: Errors				
Total	N/A	0	N/A	0.000
CRC	N/A	0	N/A	0.000
Frame Alignment	N/A	0	N/A	0.000
Runt	N/A	0	N/A	0.000
Oversize	N/A	0	N/A	0.000
Group: Counts				
Physical Addresses	14	14	14	14
IP Addresses	90	90	90	90
IPv6 Addresses	7	7	7	7
Protocols	28	28	28	28
Applications	23	23	23	23
Countries	10	10	10	10
Files	0	0	0	0
Group: Size Distribution				
<= 64	N/A	13952	N/A	23.915
65-127	N/A	1305	N/A	2.237
128-255	N/A	795	N/A	1.363
256-511	N/A	442	N/A	0.758

Figure 2.3.25: Omnipeek Report in PDF format

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

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

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

TASK 4 Analyze a Network using the SteelCentral Packet Analyzer

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

Note: Ensure that the **Windows 10** and **Windows Server 2019** virtual machines are running.

TASK 4.1

Download and Install SteelCentral Packet Analyzer

SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and type **https://www.riverbed.com/in/trialdownloads.html** in the address bar; press **Enter**.
2. The **riverbed** website appears, displaying **TRIAL DOWNLOADS**. Scroll down and click on **SteelCentral Packet Analyzer**.

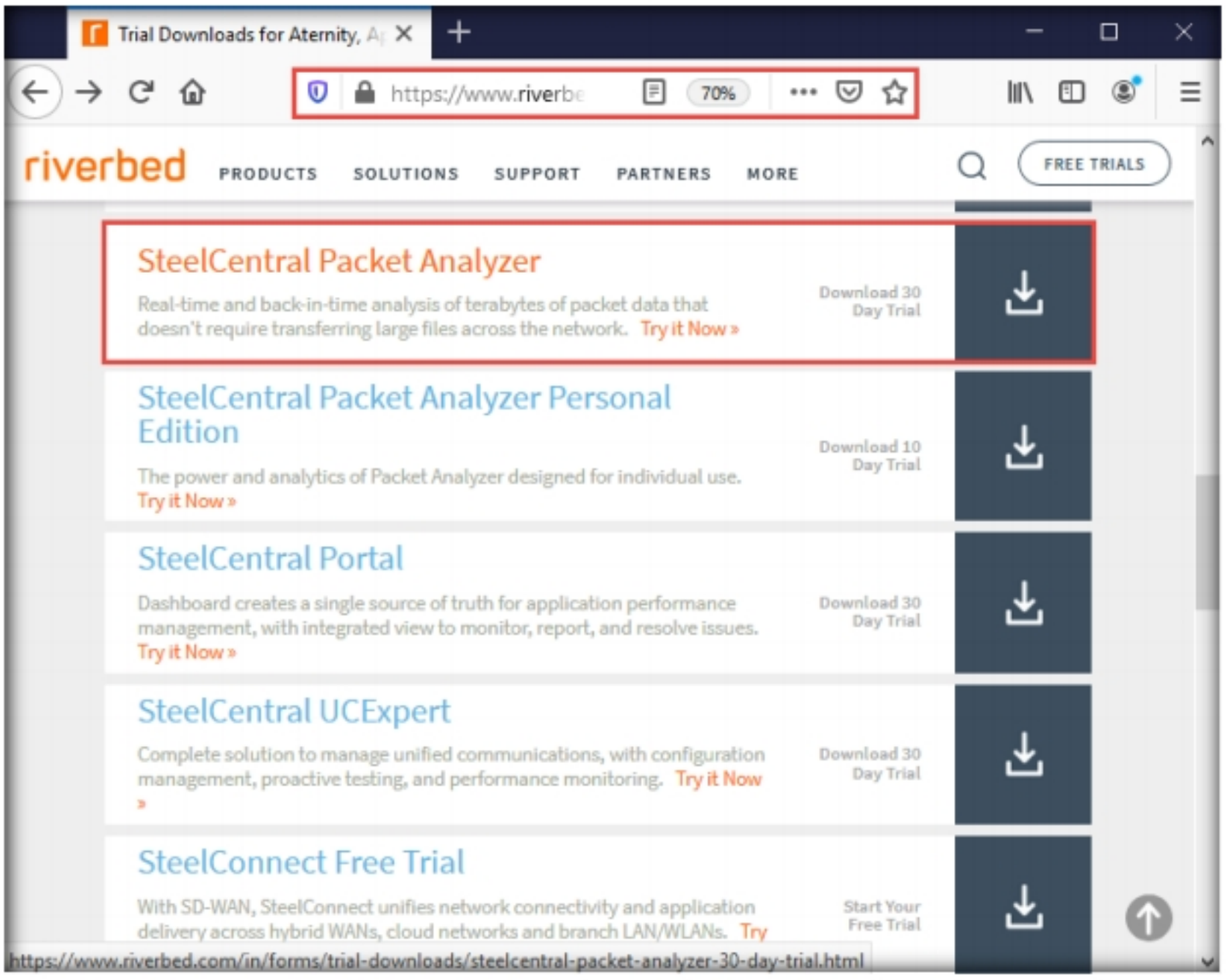


Figure 2.4.1: SteelCentral Packet Analyzer: download

SteelCentral Packet Analyzer can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

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

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

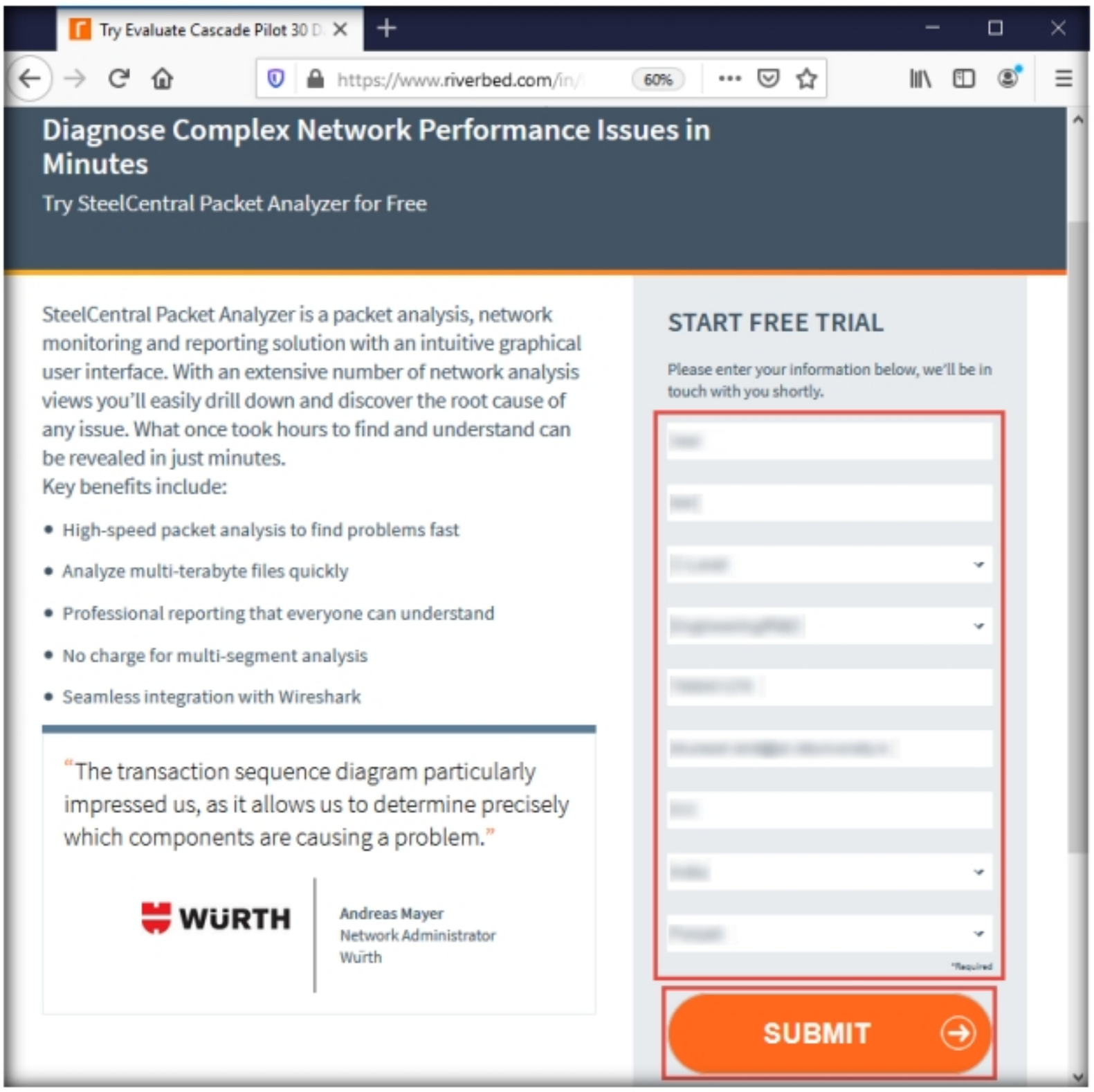


Figure 2.4.2: SteelCentral Packet Analyzer: registration form

4. The **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

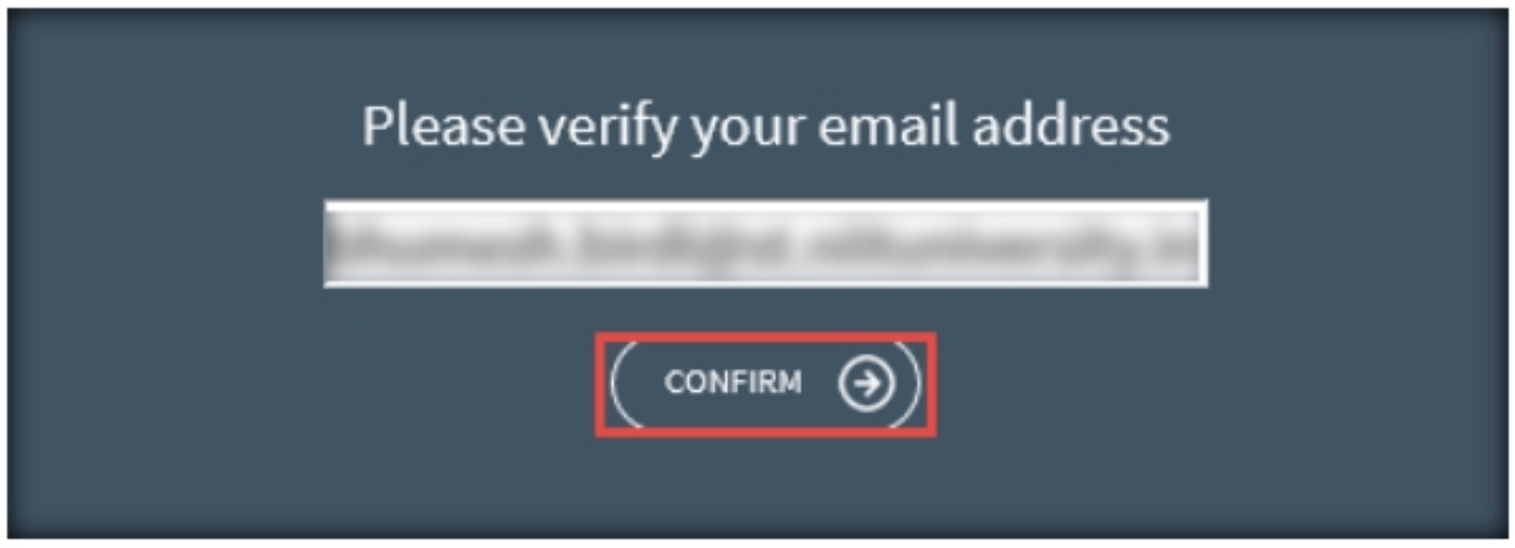


Figure 2.4.3: Confirm email address pop-up

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

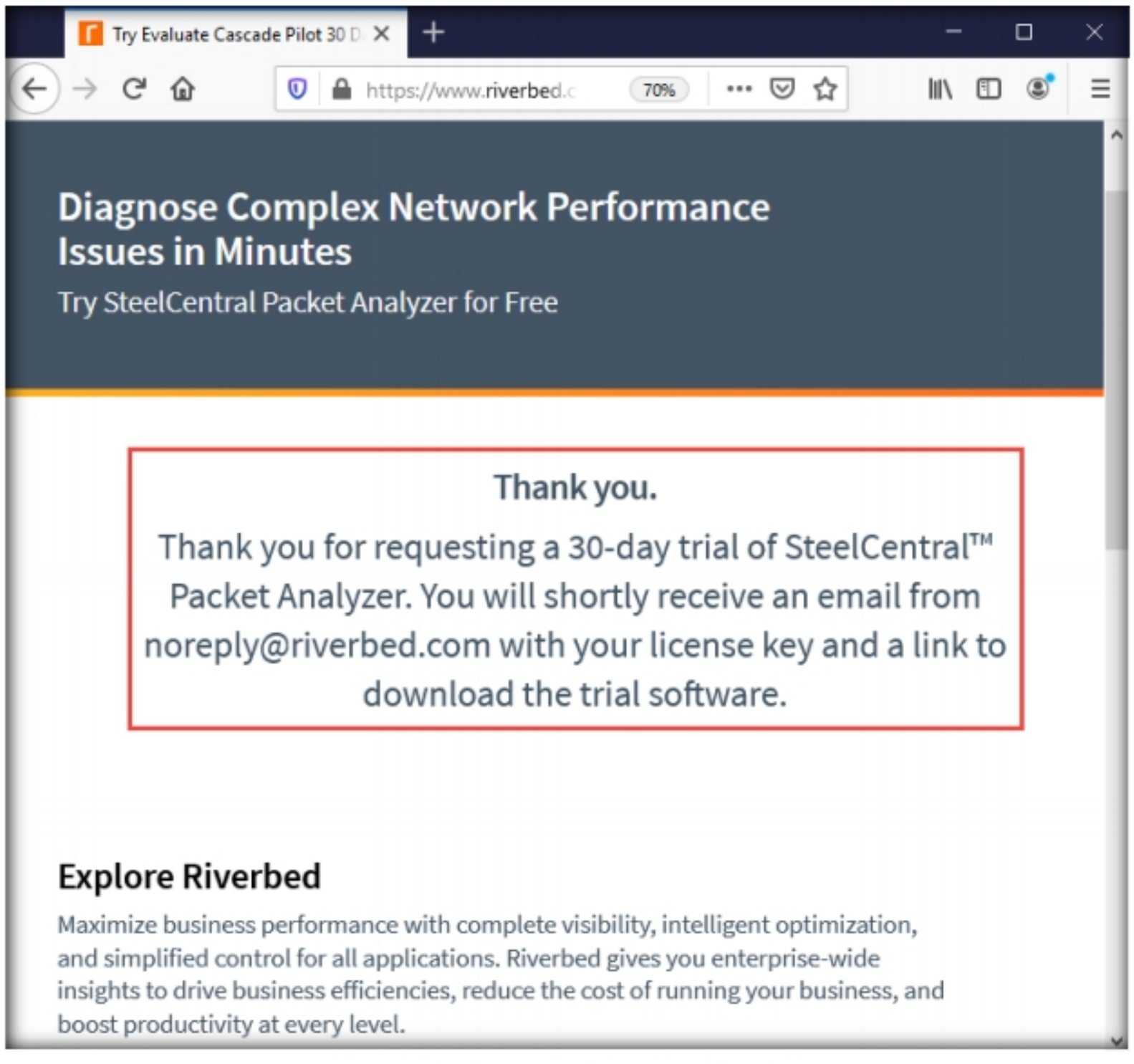
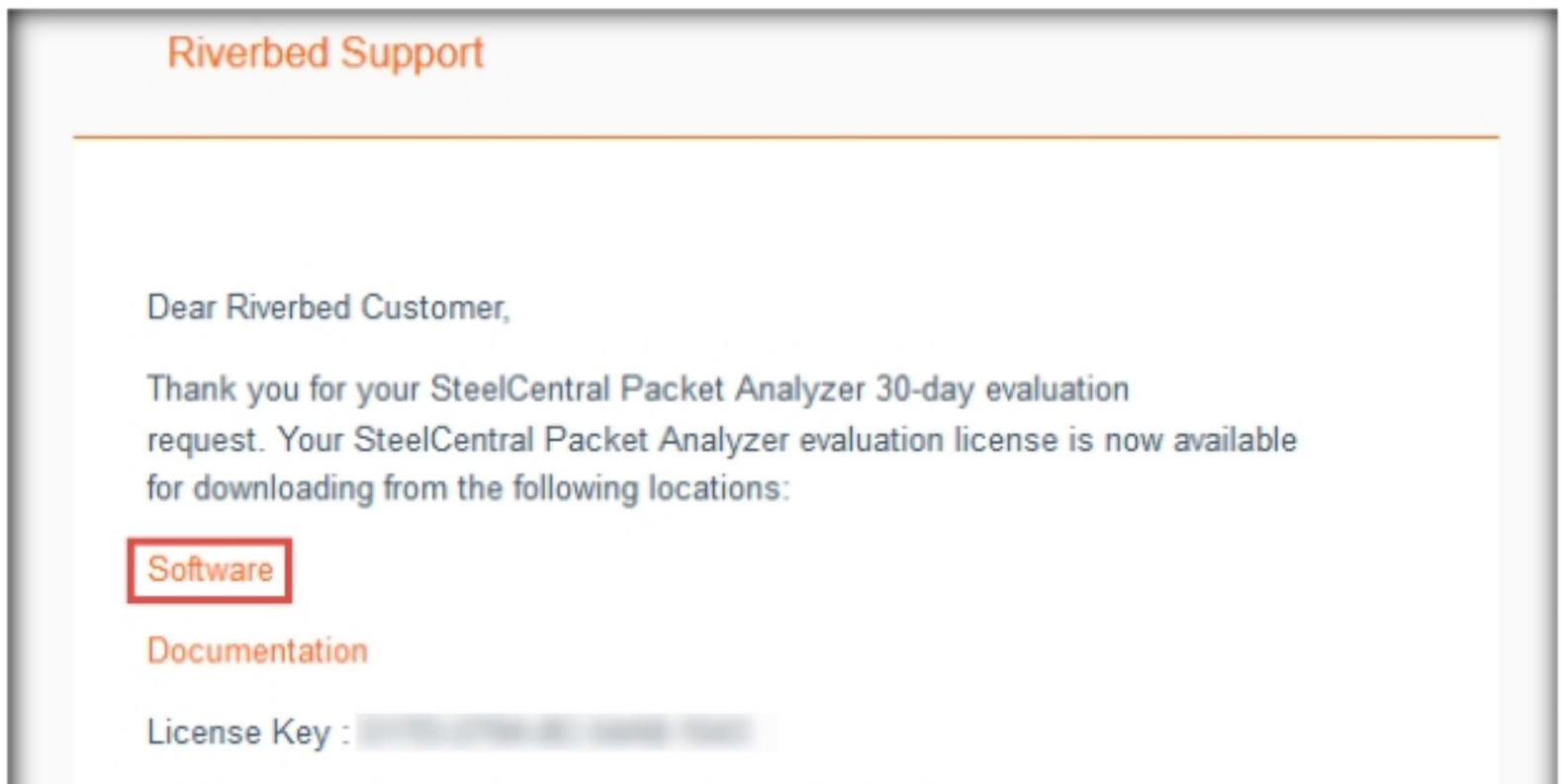


Figure 2.4.4: riverbed website Thank You webpage

6. Open a new tab and log in to the email account you provided during registration. Open the email from **SteelCentral Packet Analyzer Evaluation**, and click the **Software** link to download SteelCentral Packet Analyzer.



Riverbed Support

Dear Riverbed Customer,

Thank you for your SteelCentral Packet Analyzer 30-day evaluation request. Your SteelCentral Packet Analyzer evaluation license is now available for downloading from the following locations:

Software

Documentation

License Key :

FOR A SUCCESSFUL EVALUATION, PLEASE READ THE FOLLOWING BEFORE INSTALLING!

1. Once activated, the SteelCentral Packet Analyzer evaluation will live for 30 days.
2. The SteelCentral Packet Analyzer evaluation license provides a product activation key for two installations.
3. If you uninstall the SteelCentral Packet Analyzer evaluation software, it cannot be reinstalled.
4. The minimum recommended system configuration for SteelCentral Packet Analyzer is a Pentium dual core 2.0 GHz CPU with 2 GB RAM, 300MB free disk space on the hard drive plus additional space for capture files, a minimum of 128MB of video memory, a resolution of 1024 x 768, and Windows XP, Vista, or Windows 7.

A great next step - attended a free webinar: Introduction to the Integrated SteelCentral Network Performance Management Solution Featuring SteelCentral NetShark and SteelCentral Packet Analyzer

For more information about Riverbed Network Performance Management solutions please click here.

Figure 2.4.5: SteelCentral Packet Analyzer Evaluation mail

7. The **Opening PacketAnalyzer_10.9.3_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.

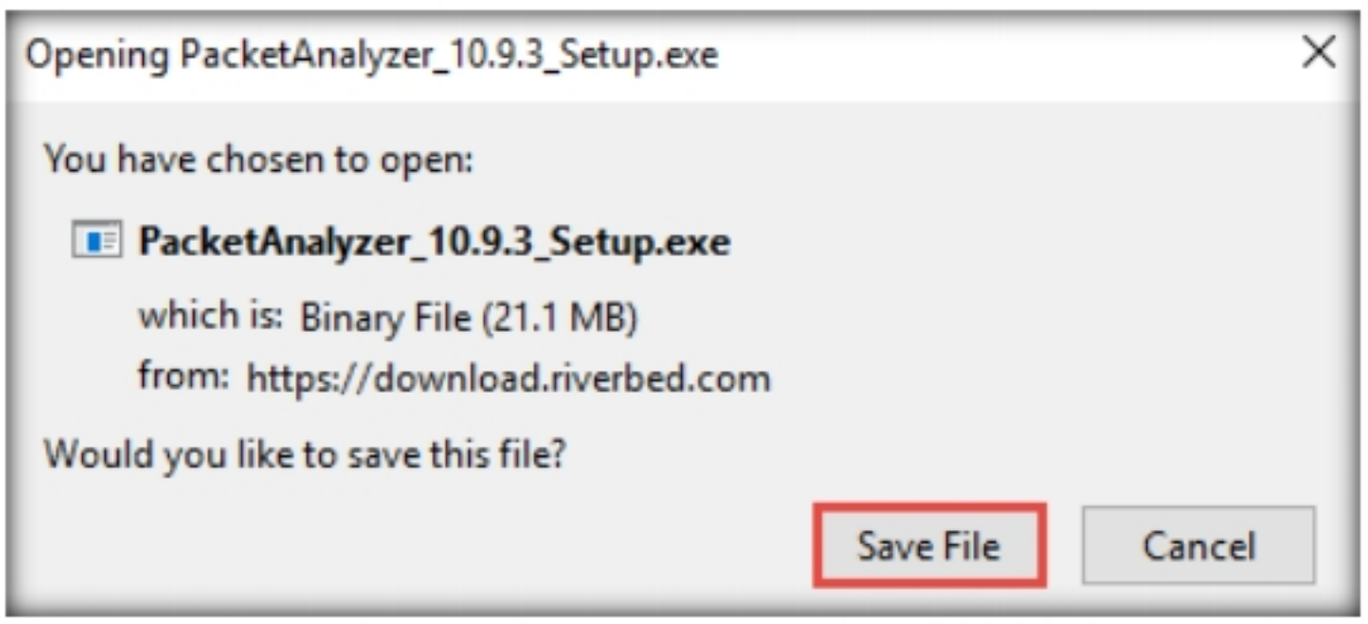


Figure 2.4.6: Downloading SteelCentral Packet Analyzer setup

8. On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer_10.9.3_Setup.exe**.
9. The **Open File - Security Warning** window appears; click **Run**.
10. The **SteelCentral Packet Analyzer Setup** window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.

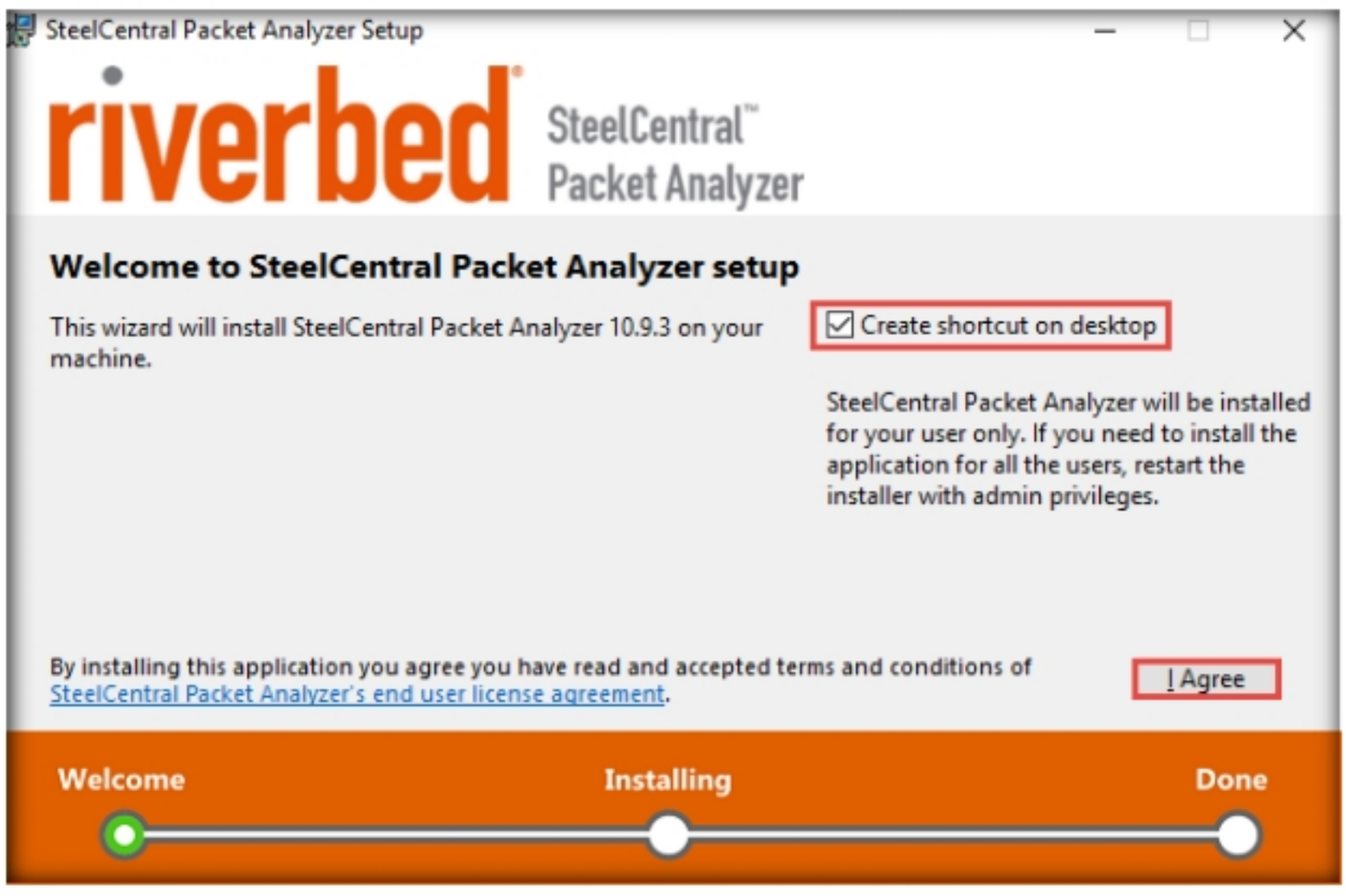


Figure 2.4.7: SteelCentral Packet Analyzer Setup window

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

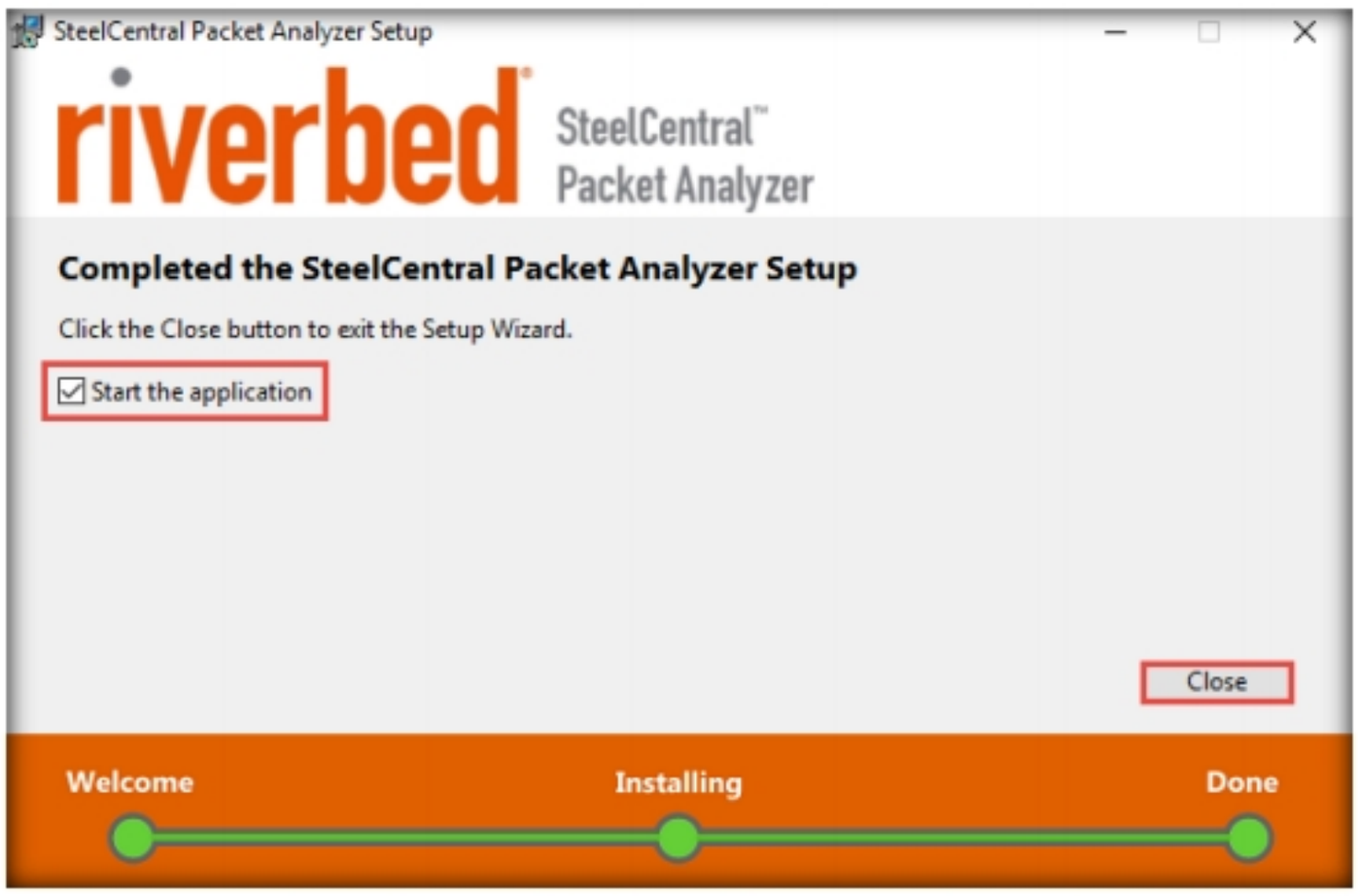


Figure 2.4.8: Completed SteelCentral Packet Analyzer Setup wizard

12. The **License** window appears, showing the **Single-Seat License** tab by default. Leave this window running.

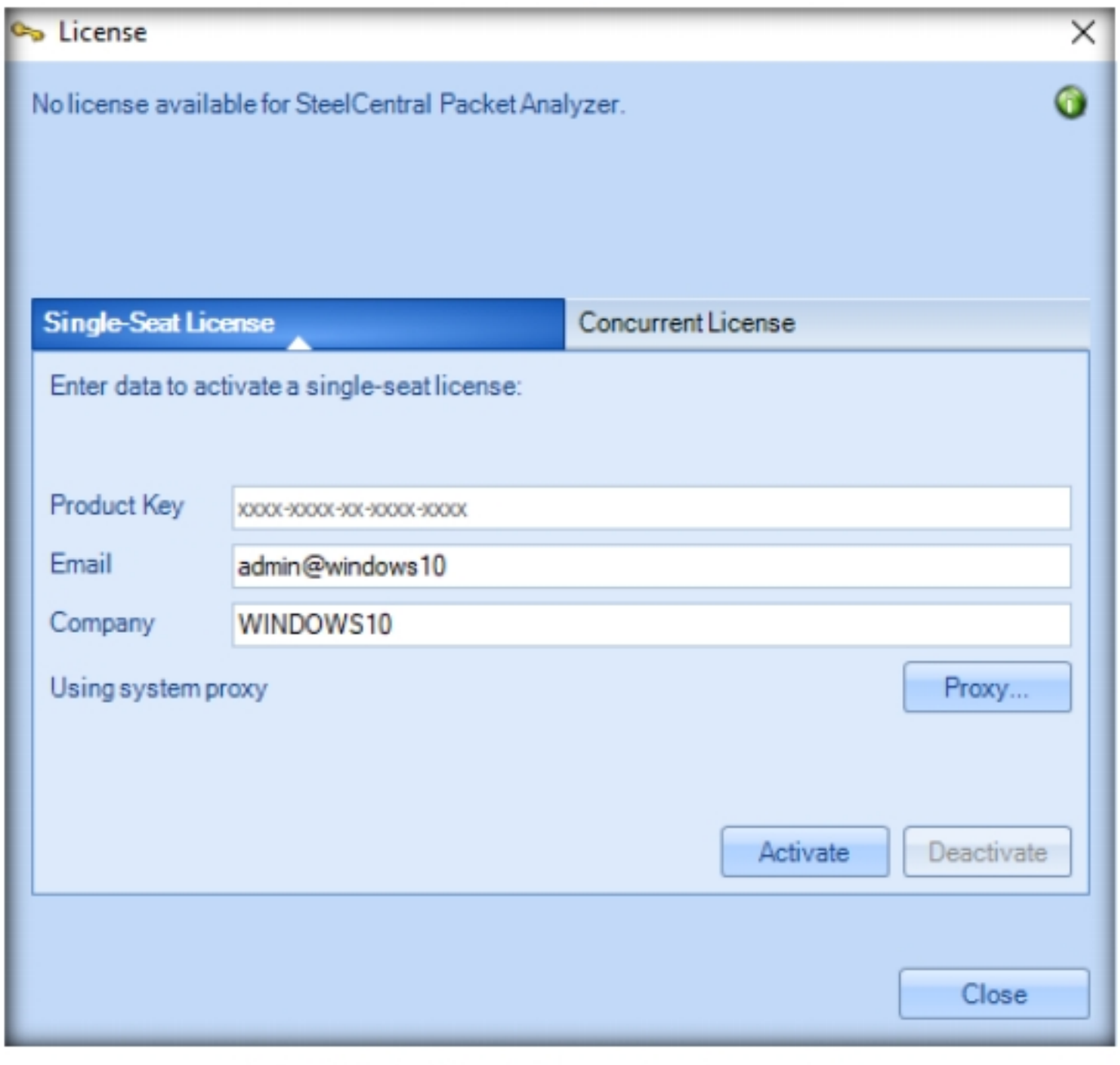
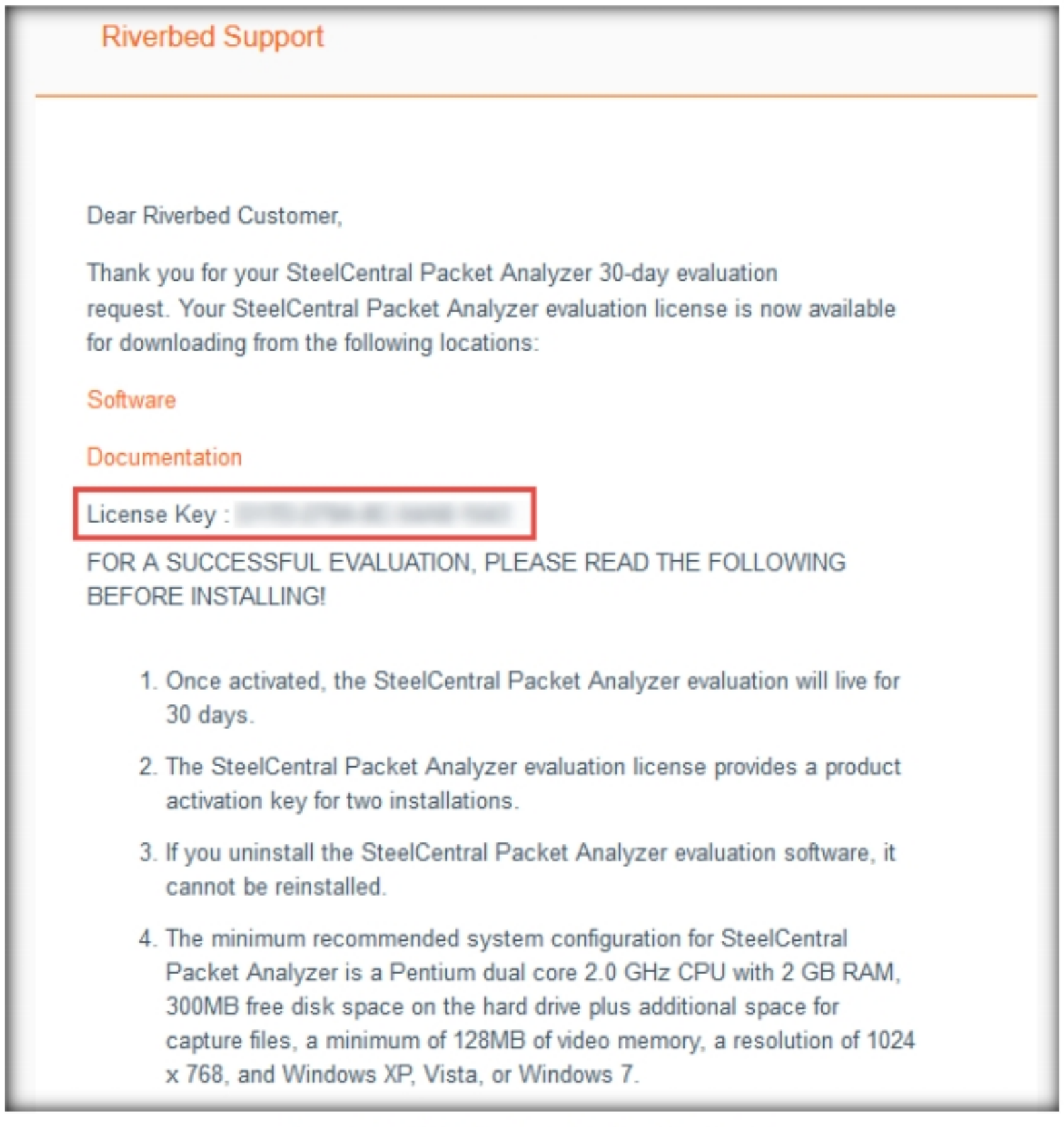


Figure 2.4.9: SteelCentral Packet Analyzer License window

13. Switch to your browser (here, **Mozilla Firefox**). Navigate to the tab where the **SteelCentral Packet Analyzer Evaluation** email is open and copy the **License Key** provided in the email.



Riverbed Support

Dear Riverbed Customer,

Thank you for your SteelCentral Packet Analyzer 30-day evaluation request. Your SteelCentral Packet Analyzer evaluation license is now available for downloading from the following locations:

Software

Documentation

License Key : [redacted]

FOR A SUCCESSFUL EVALUATION, PLEASE READ THE FOLLOWING BEFORE INSTALLING!

1. Once activated, the SteelCentral Packet Analyzer evaluation will live for 30 days.
2. The SteelCentral Packet Analyzer evaluation license provides a product activation key for two installations.
3. If you uninstall the SteelCentral Packet Analyzer evaluation software, it cannot be reinstalled.
4. The minimum recommended system configuration for SteelCentral Packet Analyzer is a Pentium dual core 2.0 GHz CPU with 2 GB RAM, 300MB free disk space on the hard drive plus additional space for capture files, a minimum of 128MB of video memory, a resolution of 1024 x 768, and Windows XP, Vista, or Windows 7.

Figure 2.4.10: SteelCentral Packet Analyzer License key

TASK 4.2

Enter the License Key

14. Switch back to **License** window and paste the **License Key** in the **Product Key** field. Leave the **Email** and **Company** fields set to default and click the **Activate** button.

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

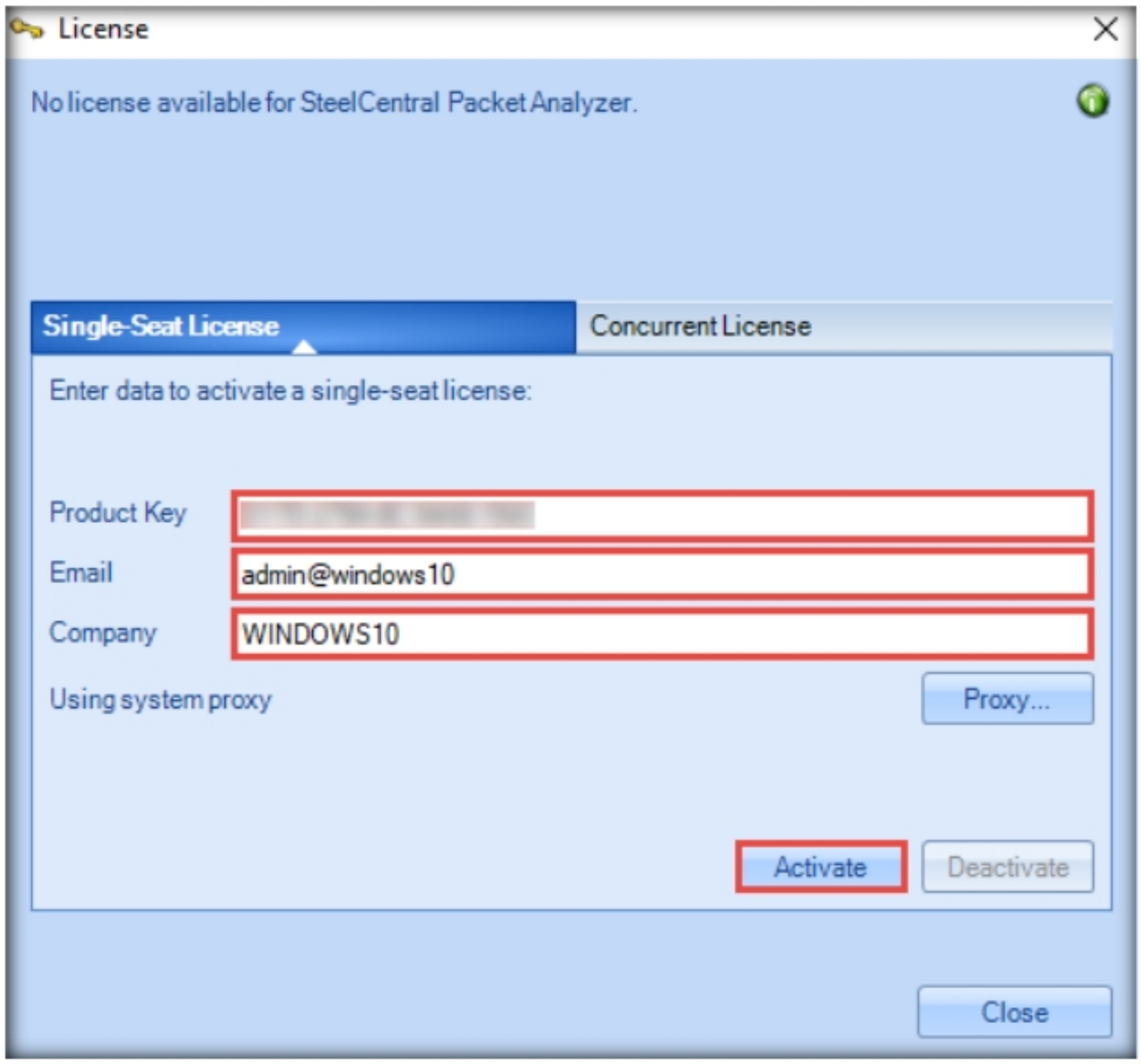


Figure 2.4.11: SteelCentral Packet Analyzer License window

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

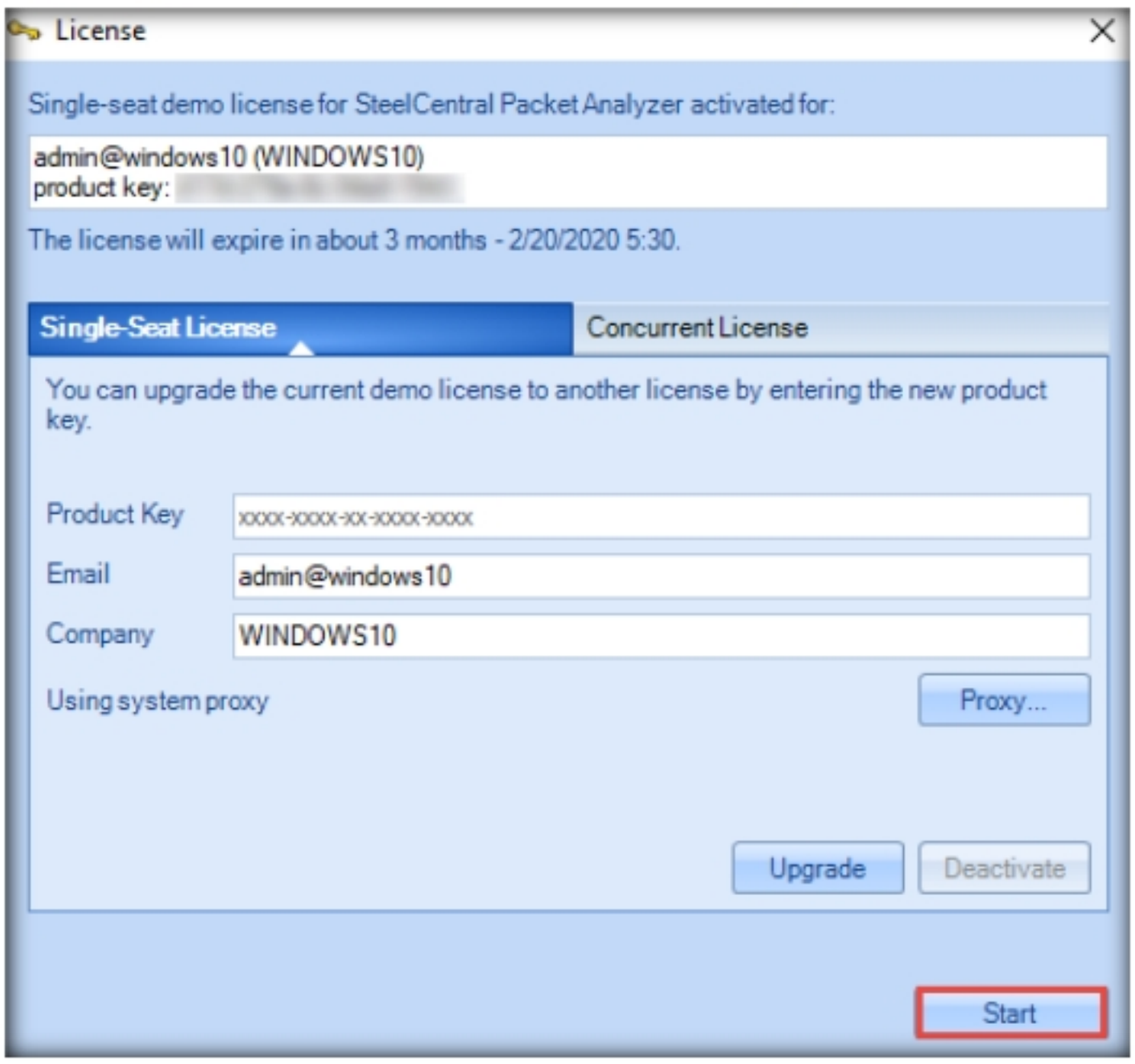


Figure 2.4.12: SteelCentral Packet Analyzer license activated

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

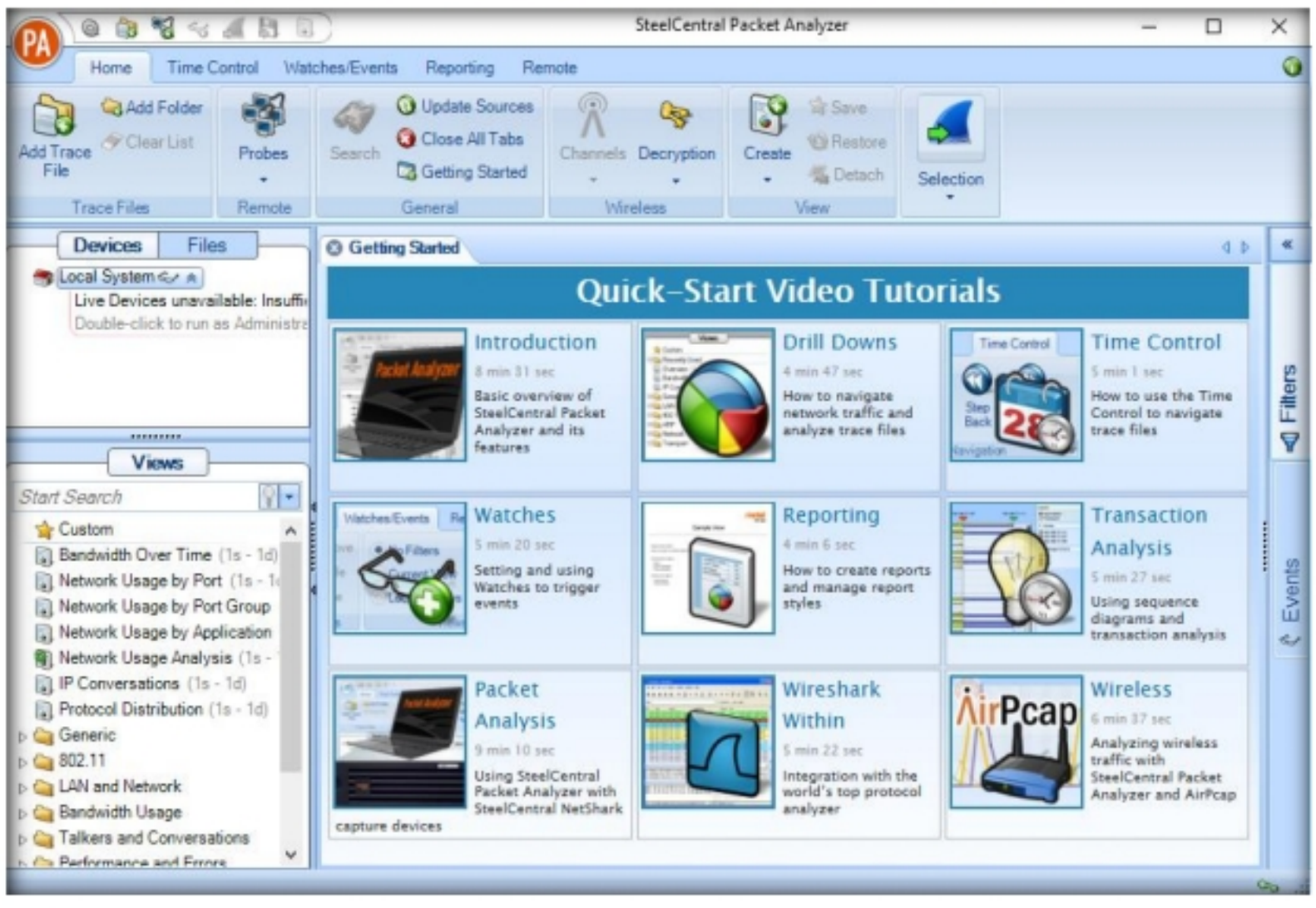


Figure 2.4.13: SteelCentral Packet Analyzer windows

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

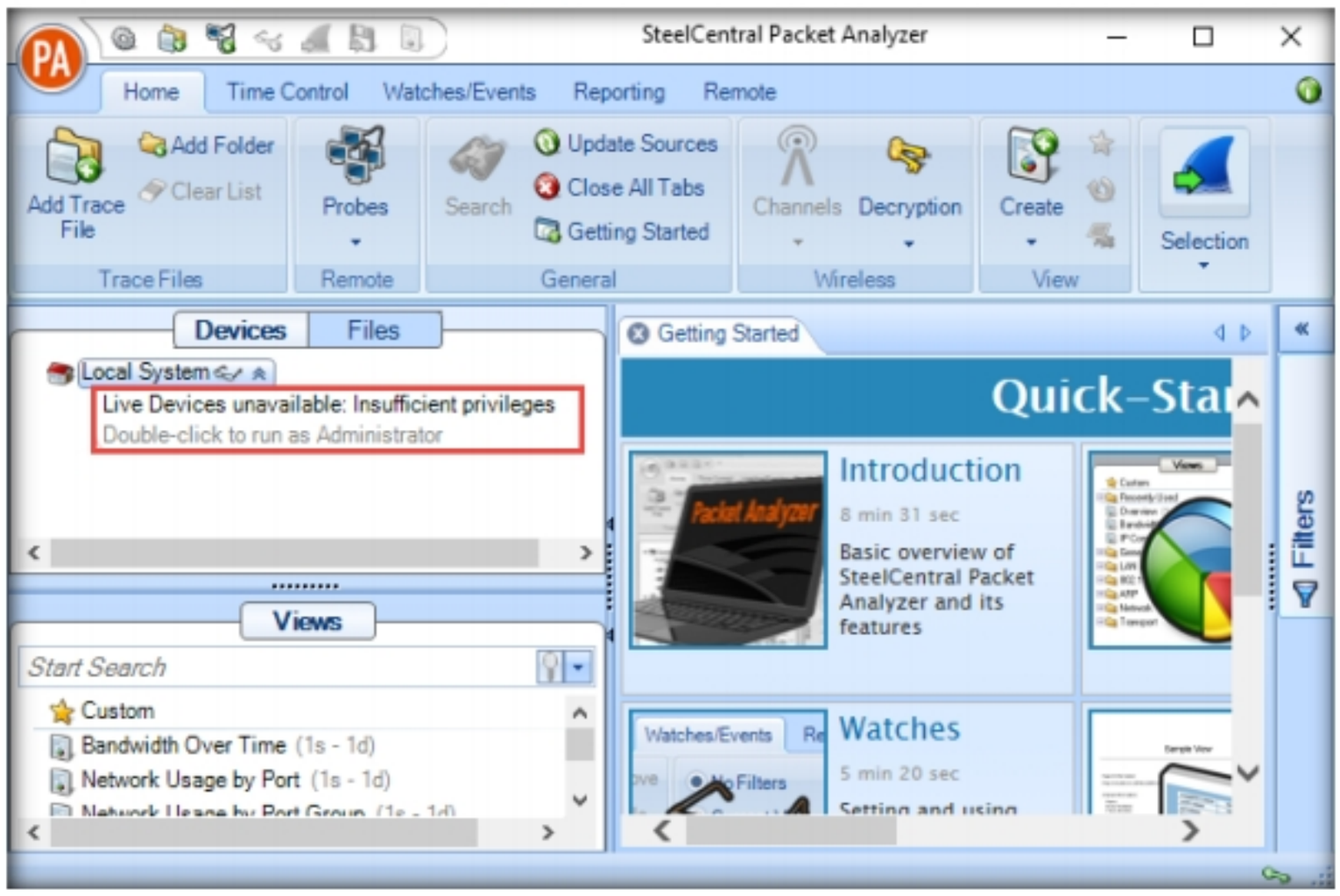


Figure 2.4.14: SteelCentral Packet Analyzer windows

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

TASK 4.3

Capture Network Traffic

19. Ethernet adapters appear under **Local System** in the right-hand pane. Click the **Intel(R) 82574L Gigabit Network Connection** adapter.

Note: The adapter might differ in your lab environment.

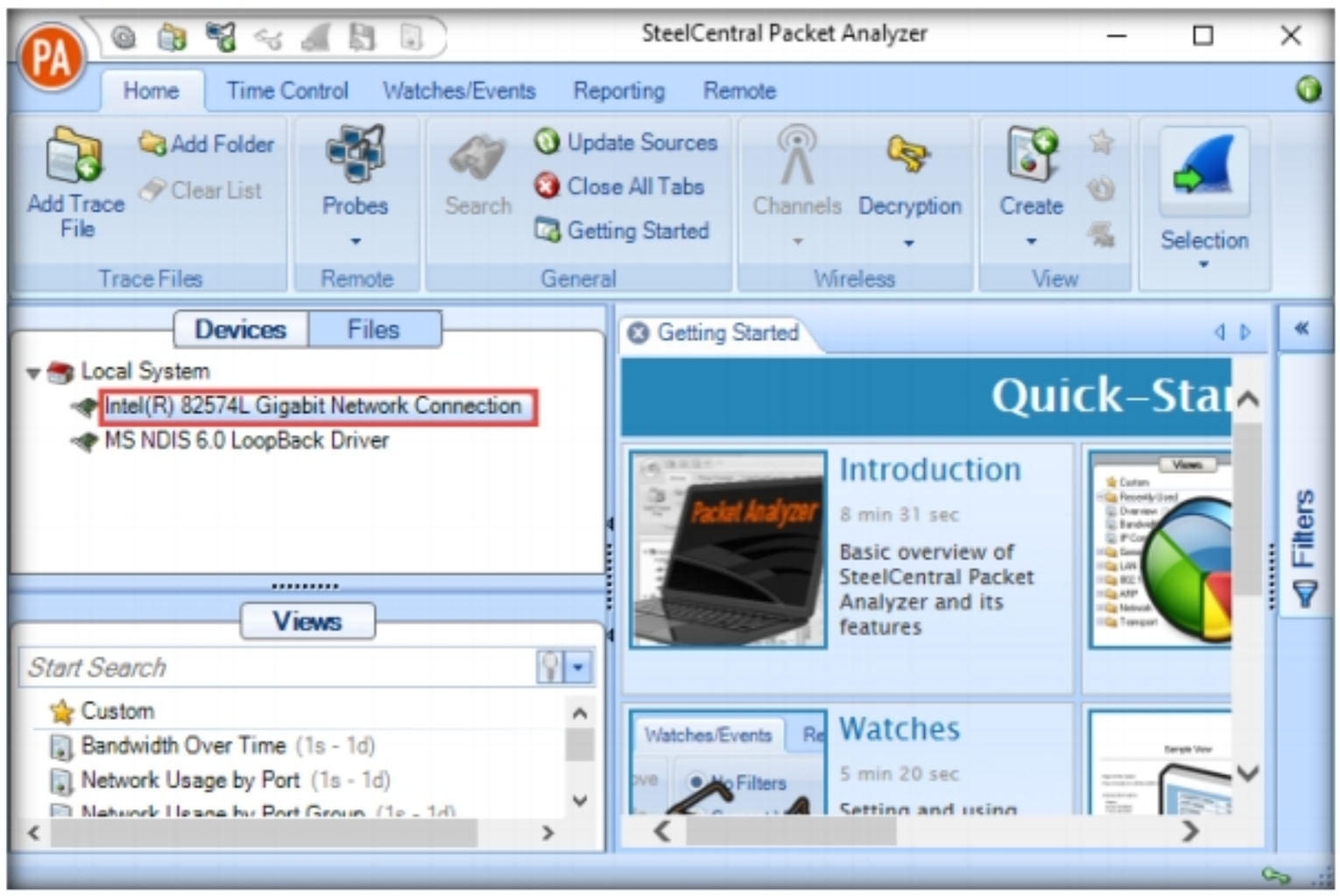


Figure 2.4.15: SteelCentral Packet Analyzer windows

20. Double-click the **Bandwidth Over Time** option under the **Recently Used** node in the left-hand pane under the **Views** section.
21. A new **Bandwidth Over Time** tab appears, and SteelCentral Packet Analyzer starts capturing the network traffic, as shown in the screenshot.

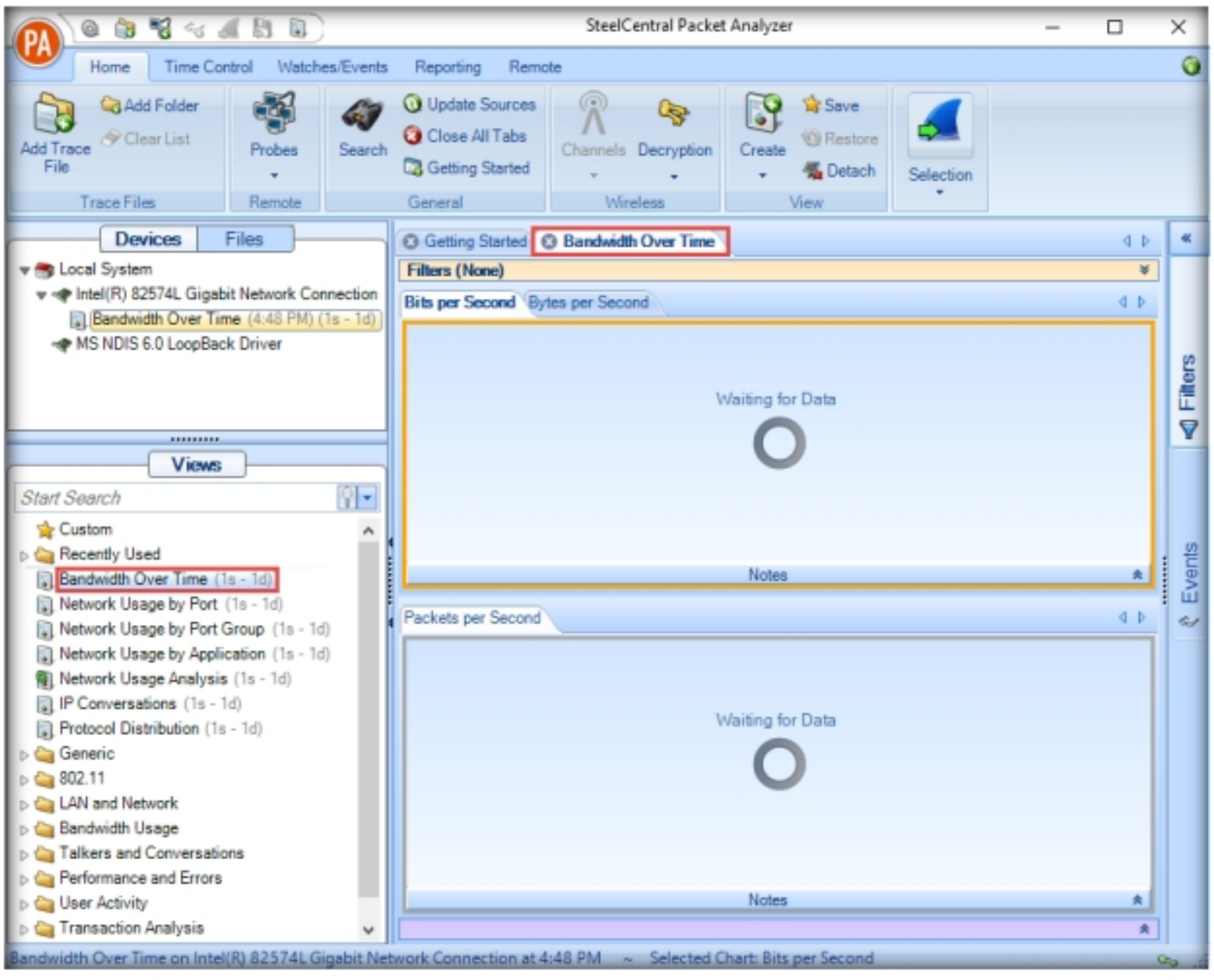


Figure 2.4.16: SteelCentral Packet Analyzer starts capturing

22. Now, navigate to the **Windows Server 2019** virtual machine.
23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

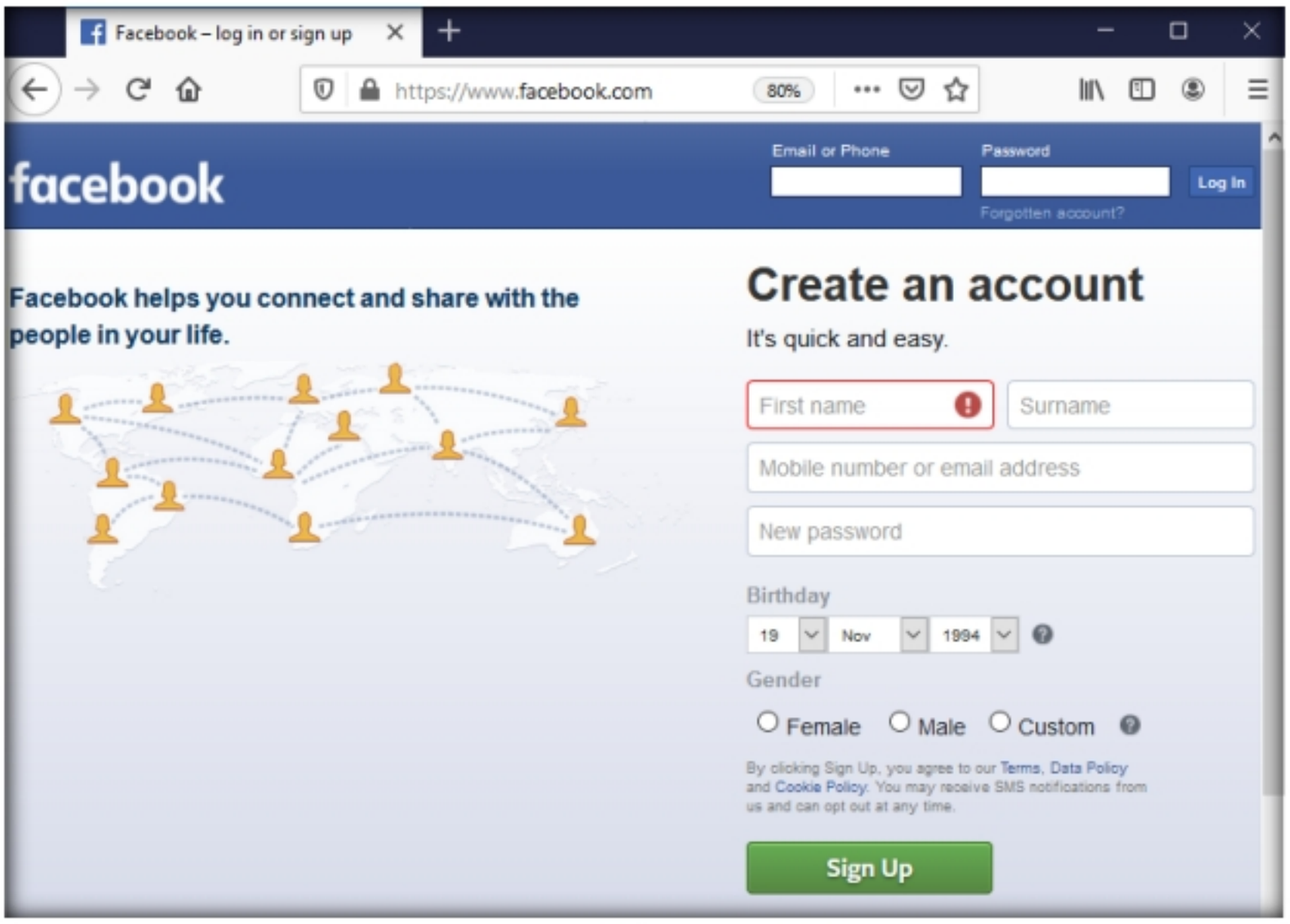


Figure 2.4.17: Browsing the Internet on Windows Server 2019

TASK 4.4

Analyze the Captured Results

24. Switch back to the **Windows 10** virtual machine and observe the network traffic captured by **SteelCentral Packet Analyzer**, as shown in the screenshot.

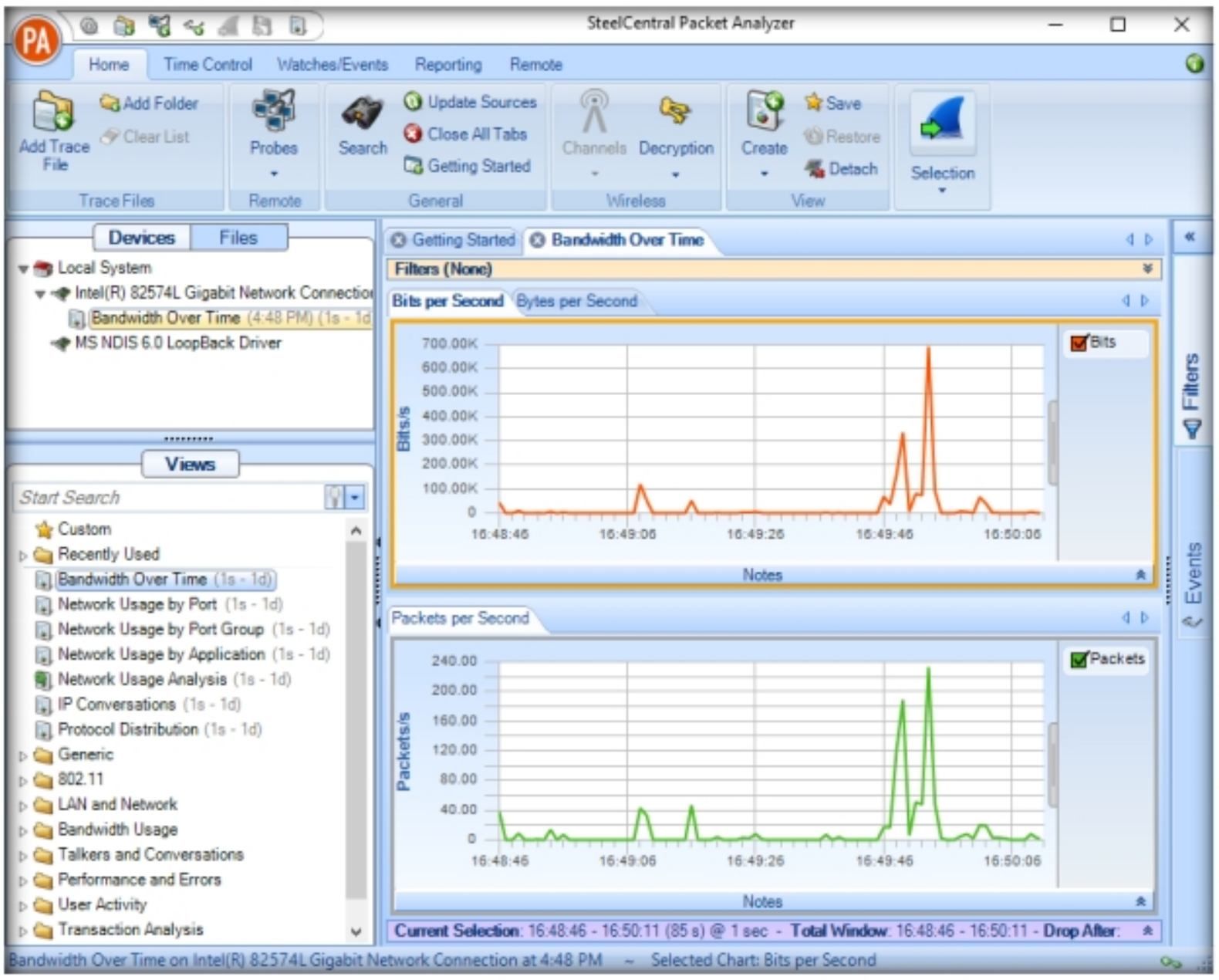


Figure 2.4.18: SteelCentral Packet Analyzer capturing Bandwidth Over Time

25. Double-click the **Network Usage by Port** option under the **Recently Used** node in the left-hand pane under the **Views** section.
26. A new **Network Usage by Port** tab appears, and **SteelCentral Packet Analyzer** displays the captured network traffic.

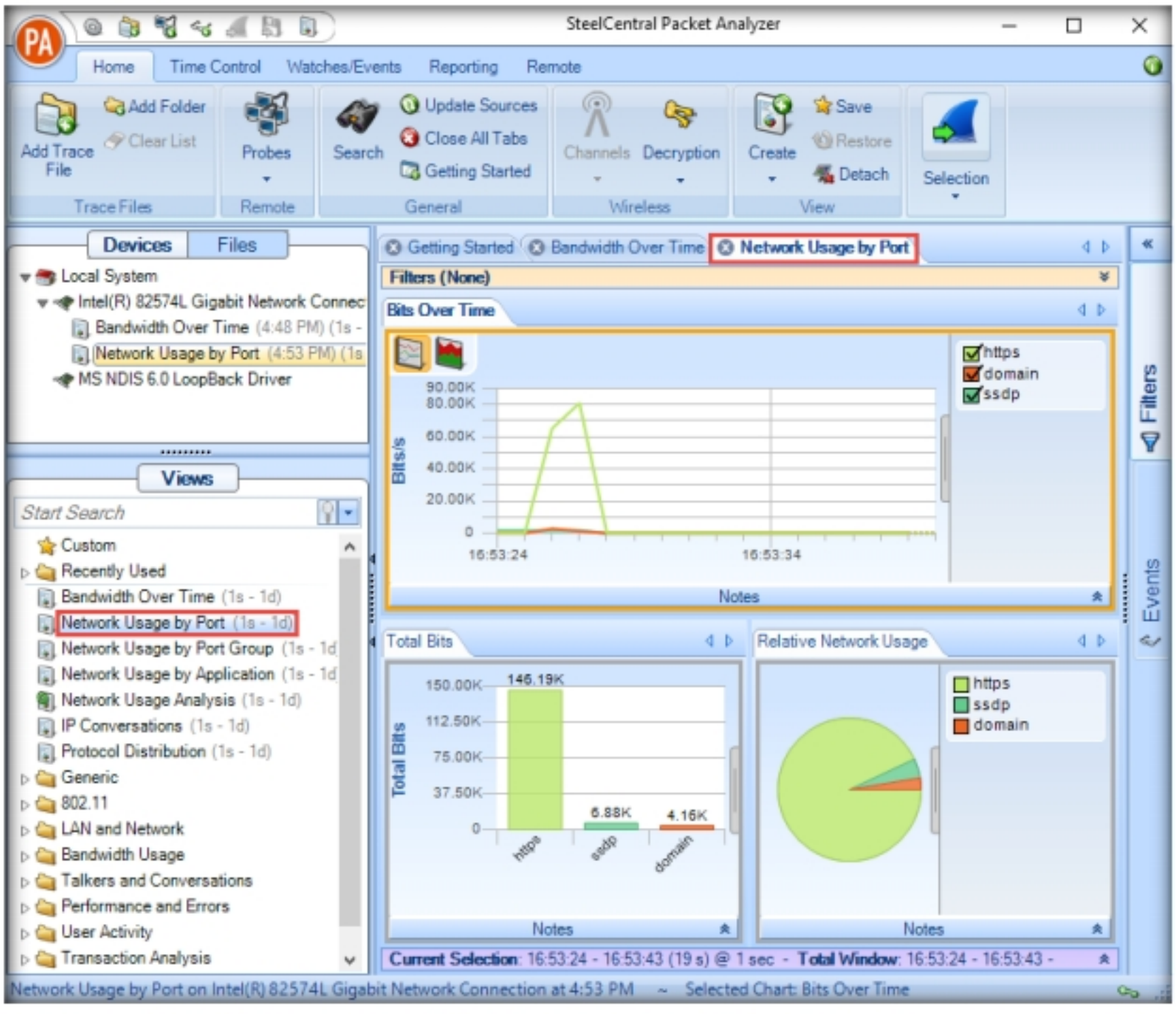


Figure 2.4.19: SteelCentral Packet Analyzer capturing Network Usage by Port

27. Double-click the **Network Usage Port by Port Group** option under the **Recently Used** node in the left-hand pane under the **Views** section.
28. A new **Network Usage by Port Group** tab appears, displaying captured network traffic protocols such as MS networking and ARP.

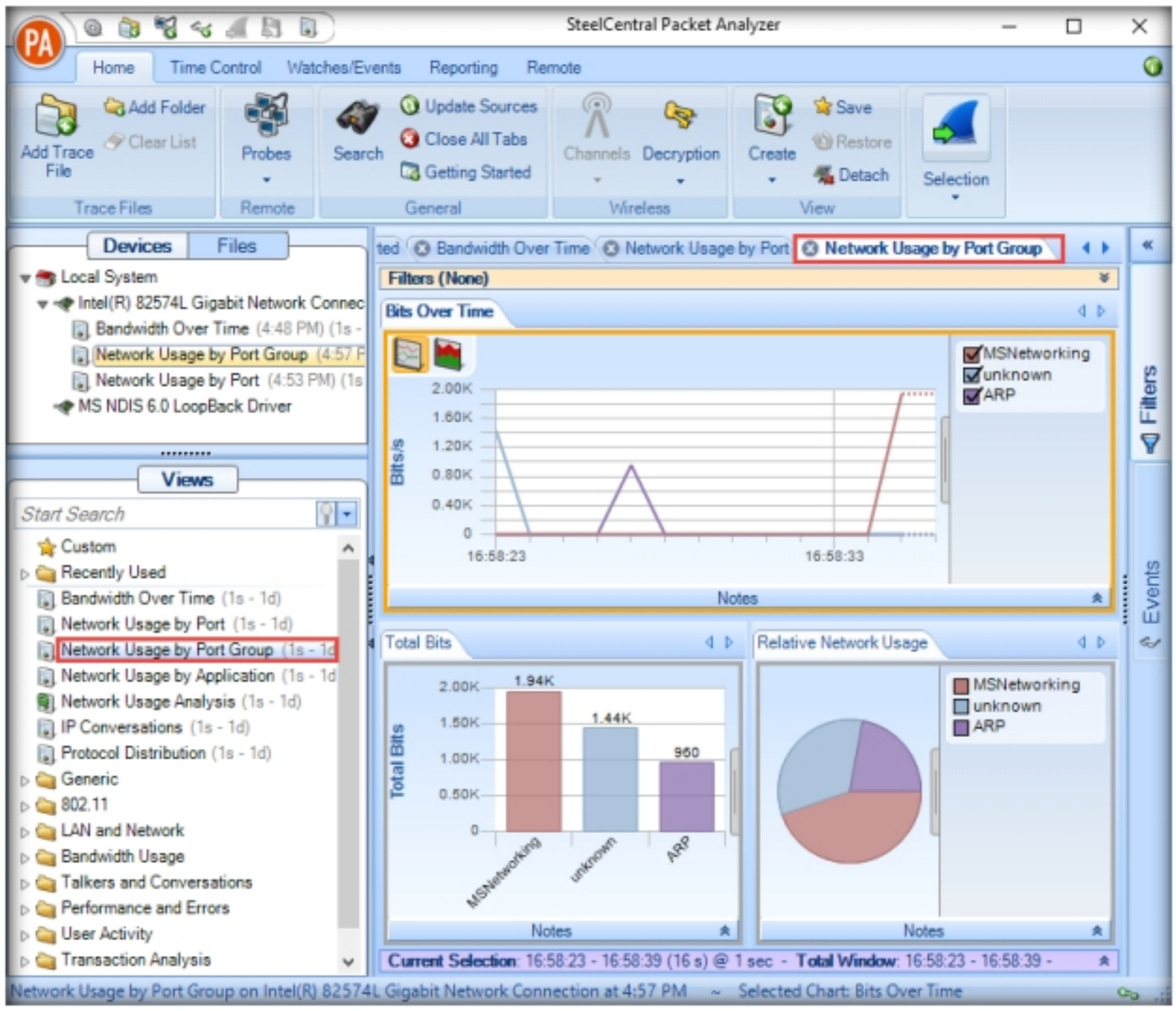


Figure 2.4.20: SteelCentral Packet Analyzer capturing Network Usage by Port Group

29. Double-click the **IP Conversations** option under the **Recently Used** node in the left-hand pane under the **Views** section.
30. A new **IP Conversations** tab appears, displaying conversations between different IP addresses in a map view.

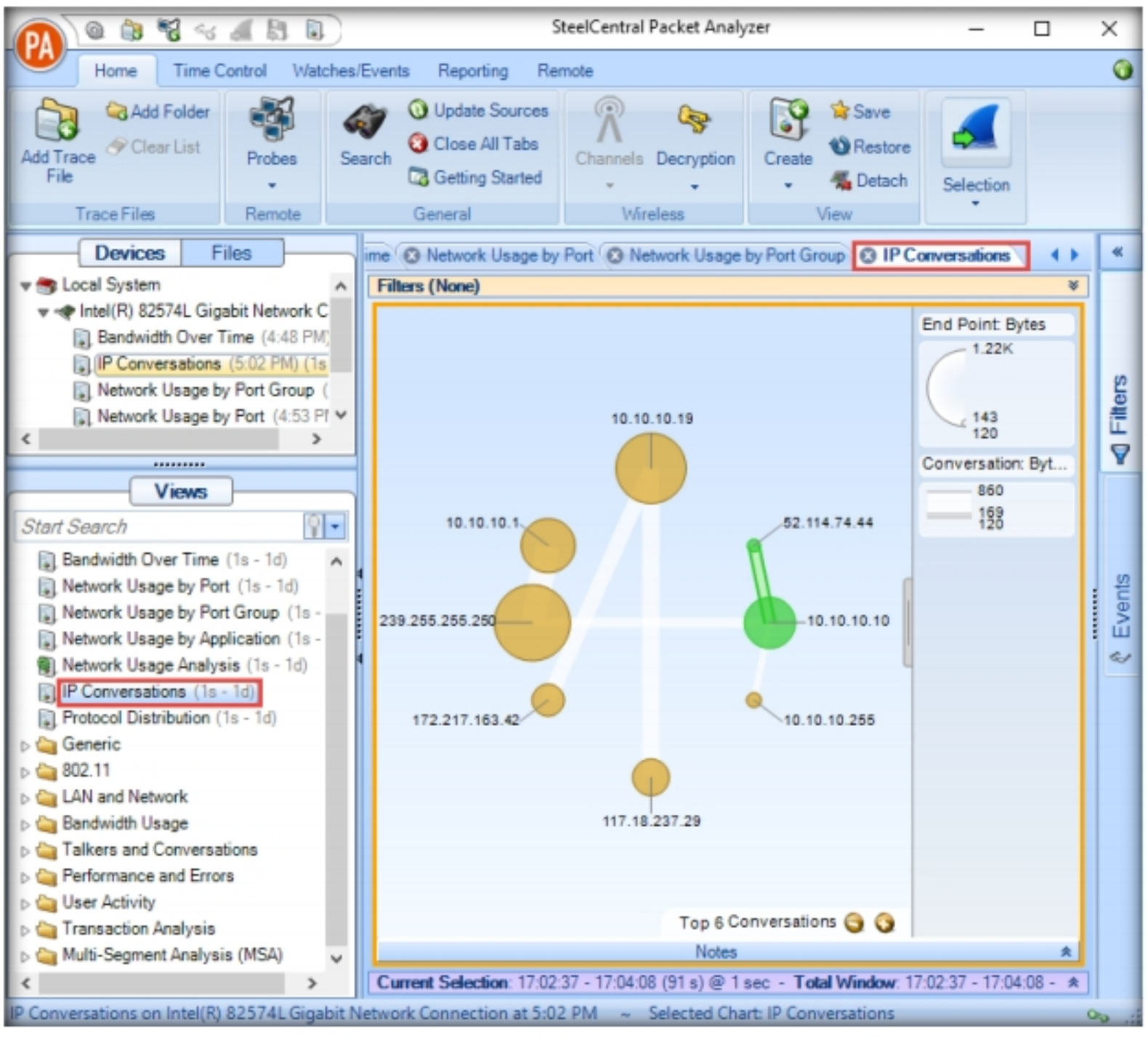


Figure 2.4.21: SteelCentral Packet Analyzer capturing IP Conversations

31. Double-click the **Protocol Distribution** option under the **Recently Used** node in the left-hand pane under the **Views** section.
32. A new **Protocol Distribution** tab appears, displaying **Network Protocols**, **Transport Protocols**, **TCP Protocols**, **UDP Protocols**, and other information, as shown in the screenshot.

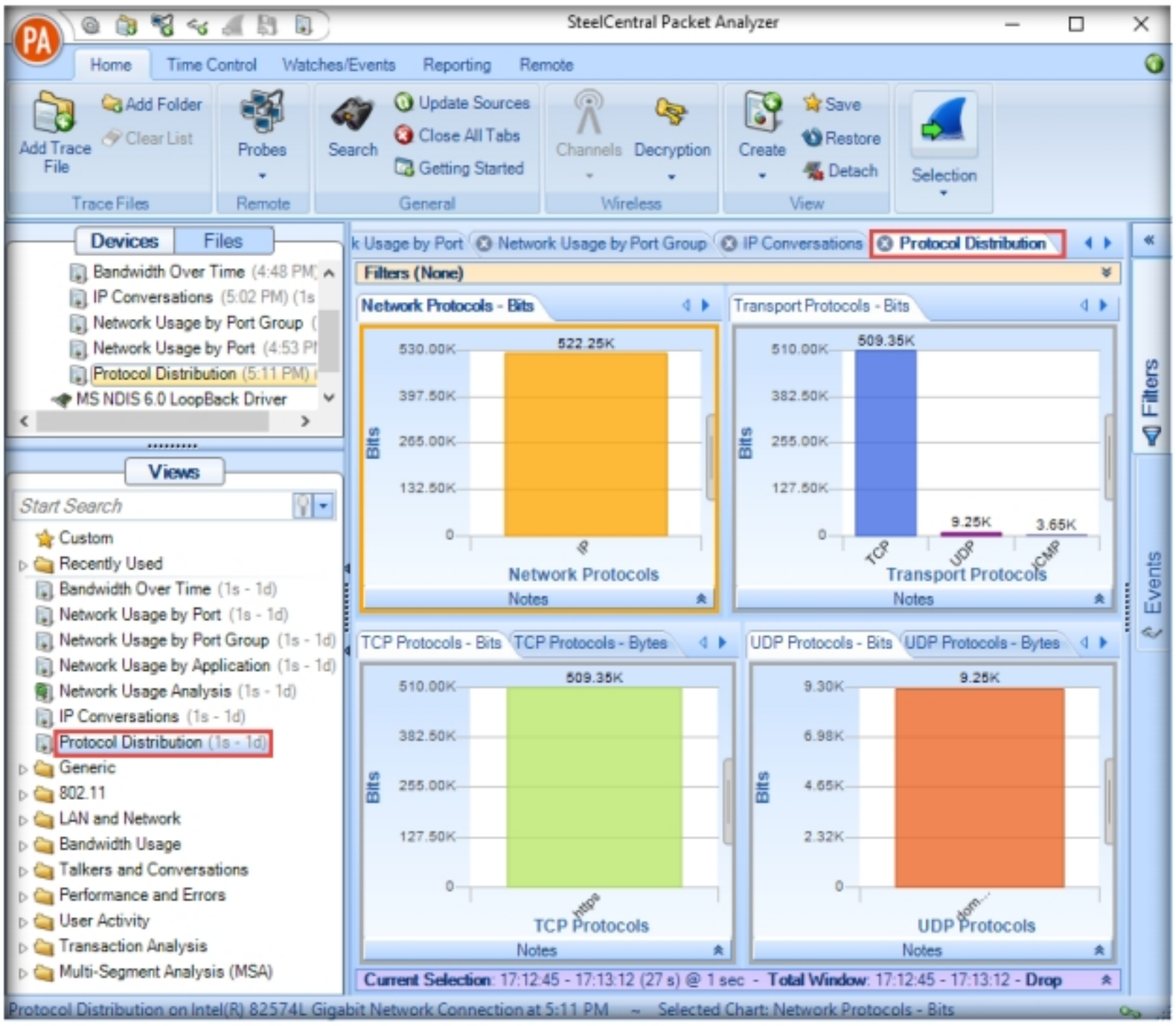


Figure 2.4.22: SteelCentral Packet Analyzer capturing Protocol Distribution

33. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.
34. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.

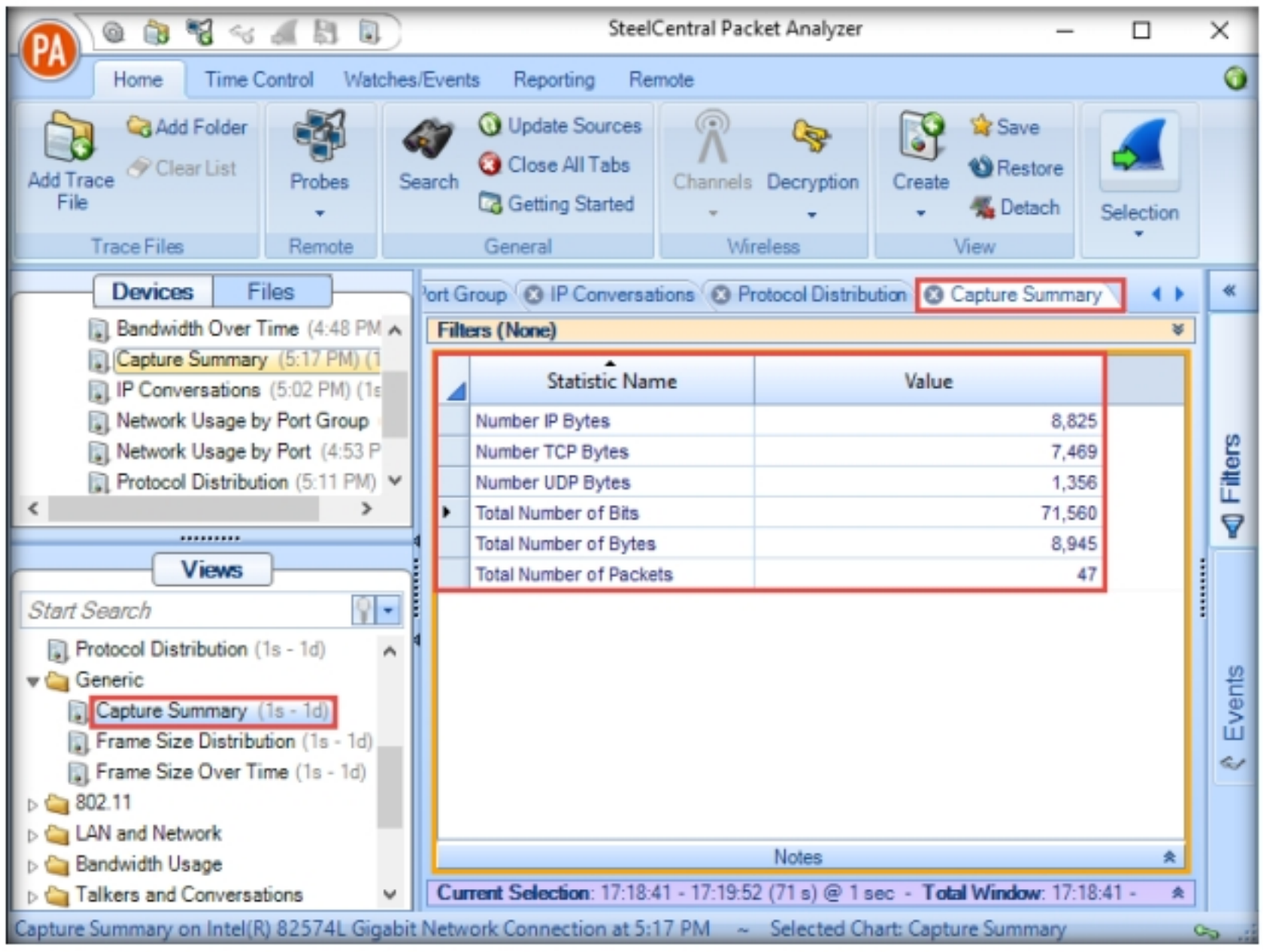


Figure 2.4.23: SteelCentral Packet Analyzer displaying Capture Summary

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

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

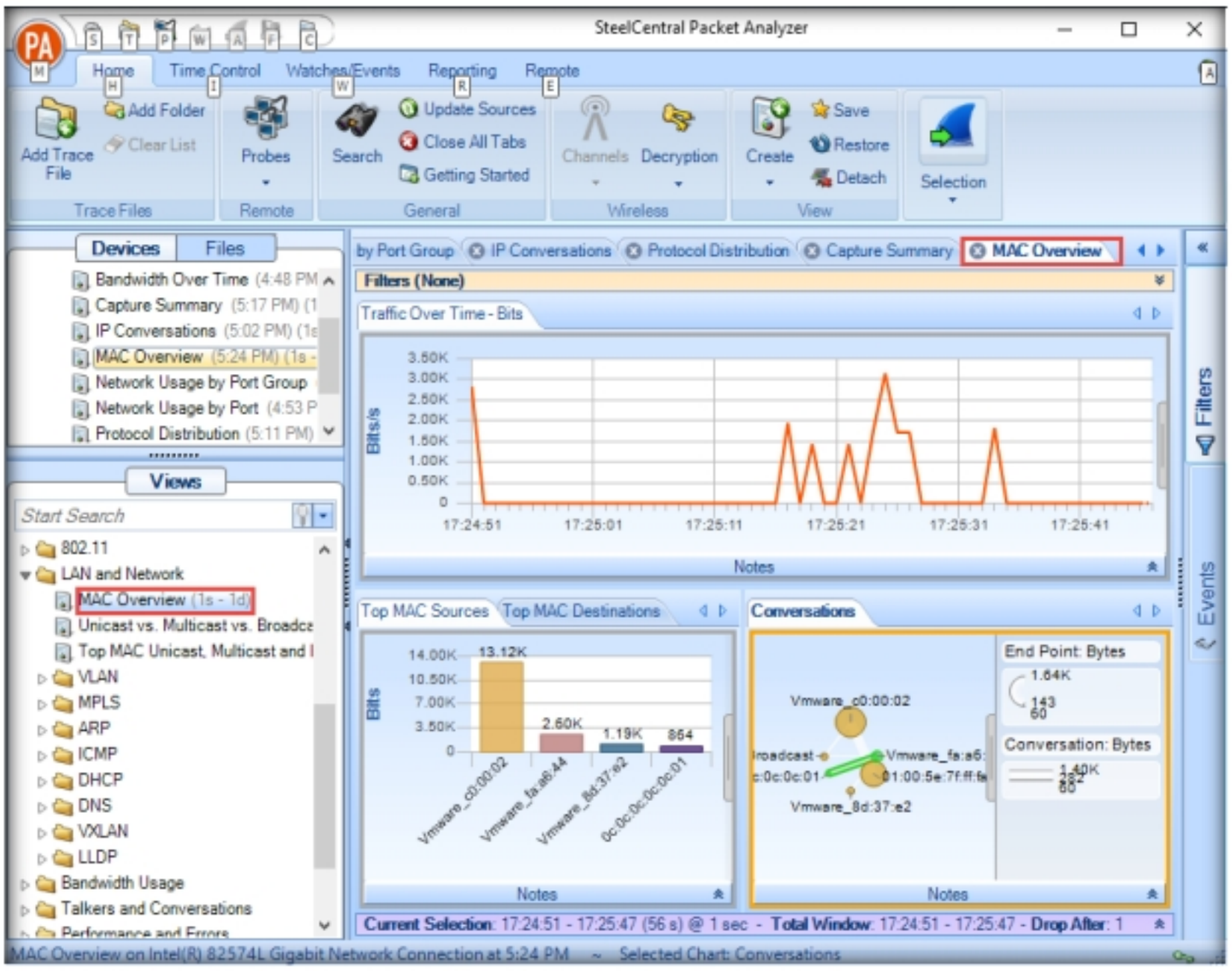


Figure 2.4.24: SteelCentral Packet Analyzer displaying MAC Overview

TASK 4.5

Generate Analysis Report

37. Similarly, you can explore various options in other nodes such as VLAN, MPLS, ARP, ICMP, and DHCP.
38. Click **Reporting** from the menu bar. Click on the **All Views** option to generate a report that includes all views.

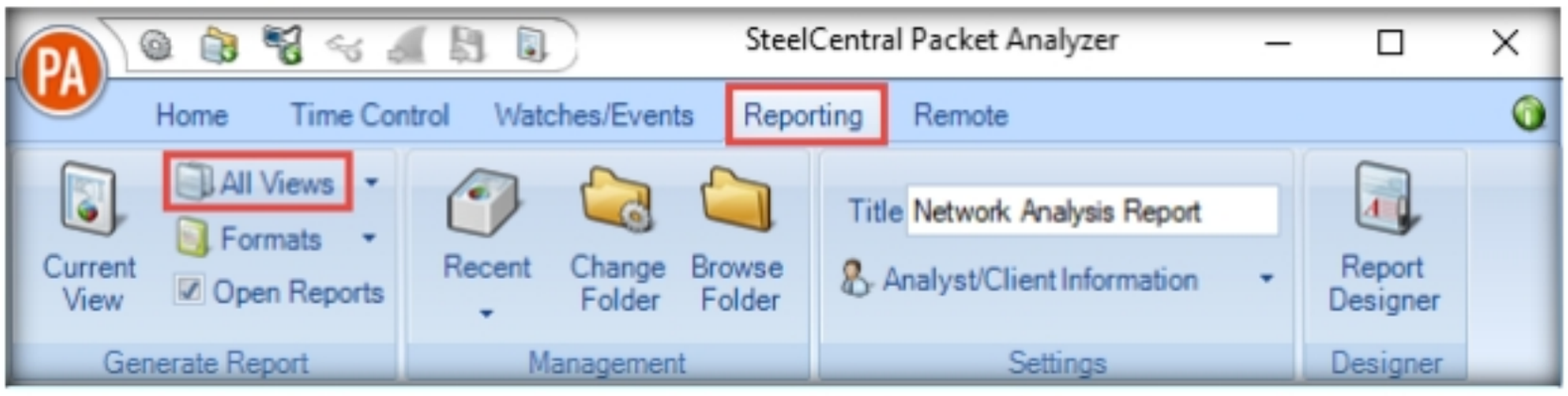


Figure 2.4.25: SteelCentral Packet Analyzer Reporting option

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

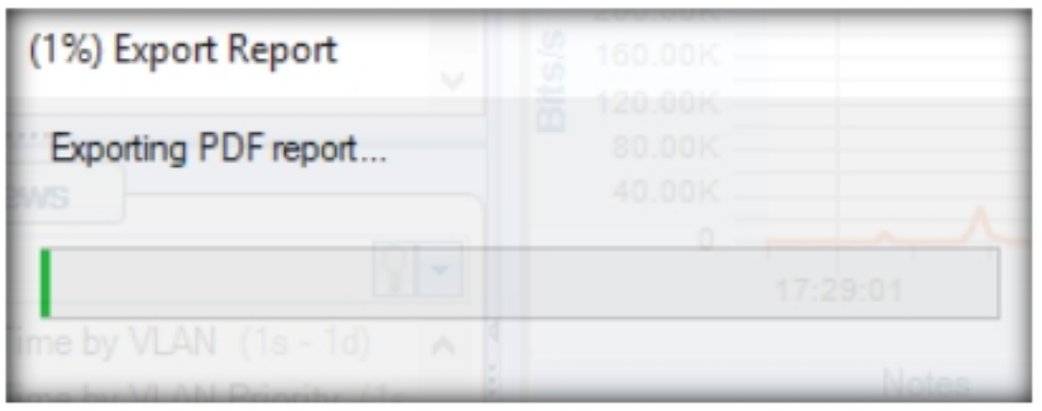


Figure 2.4.26: SteelCentral Packet Analyzer Exporting Report

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

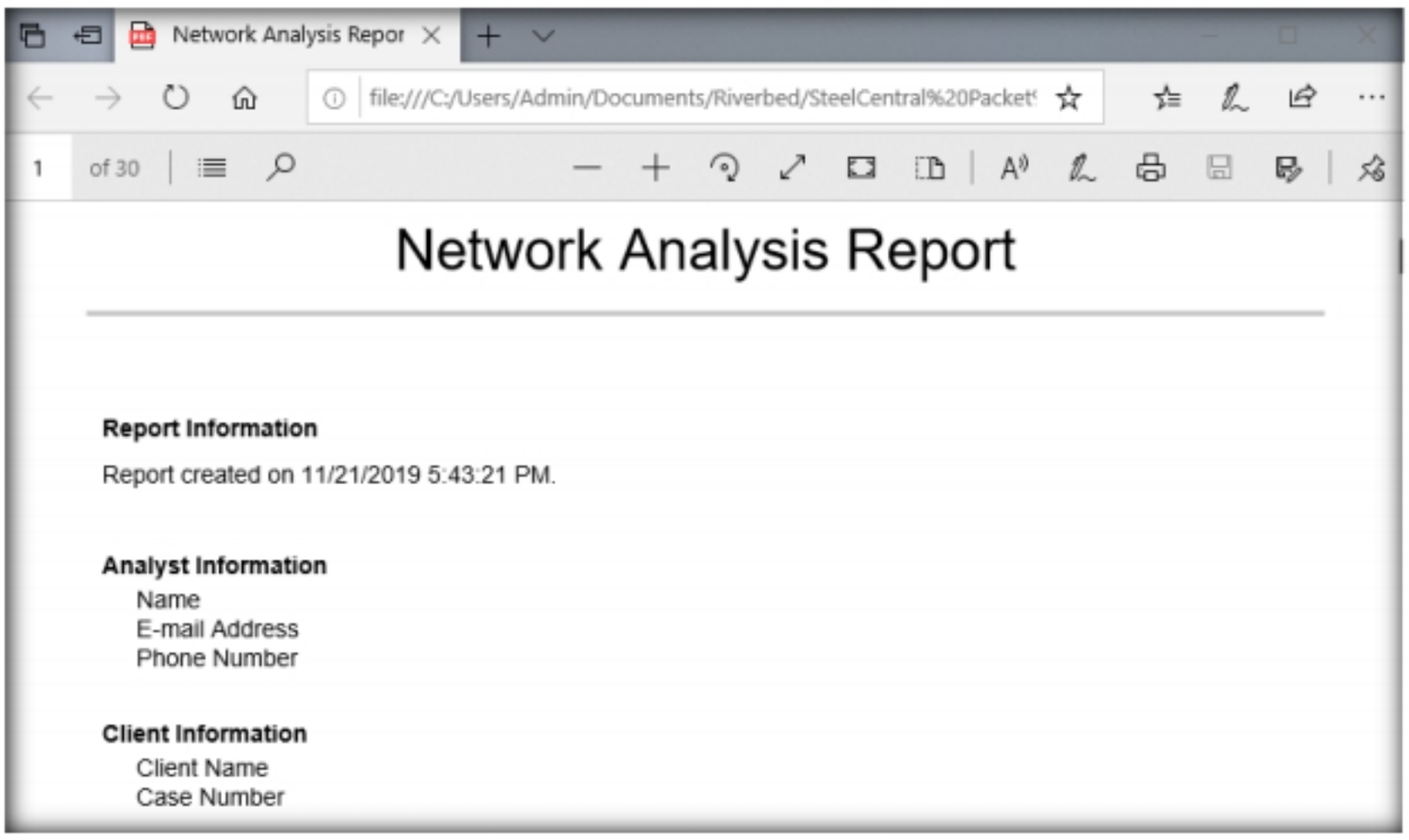


Figure 2.4.27: Network Analysis Report

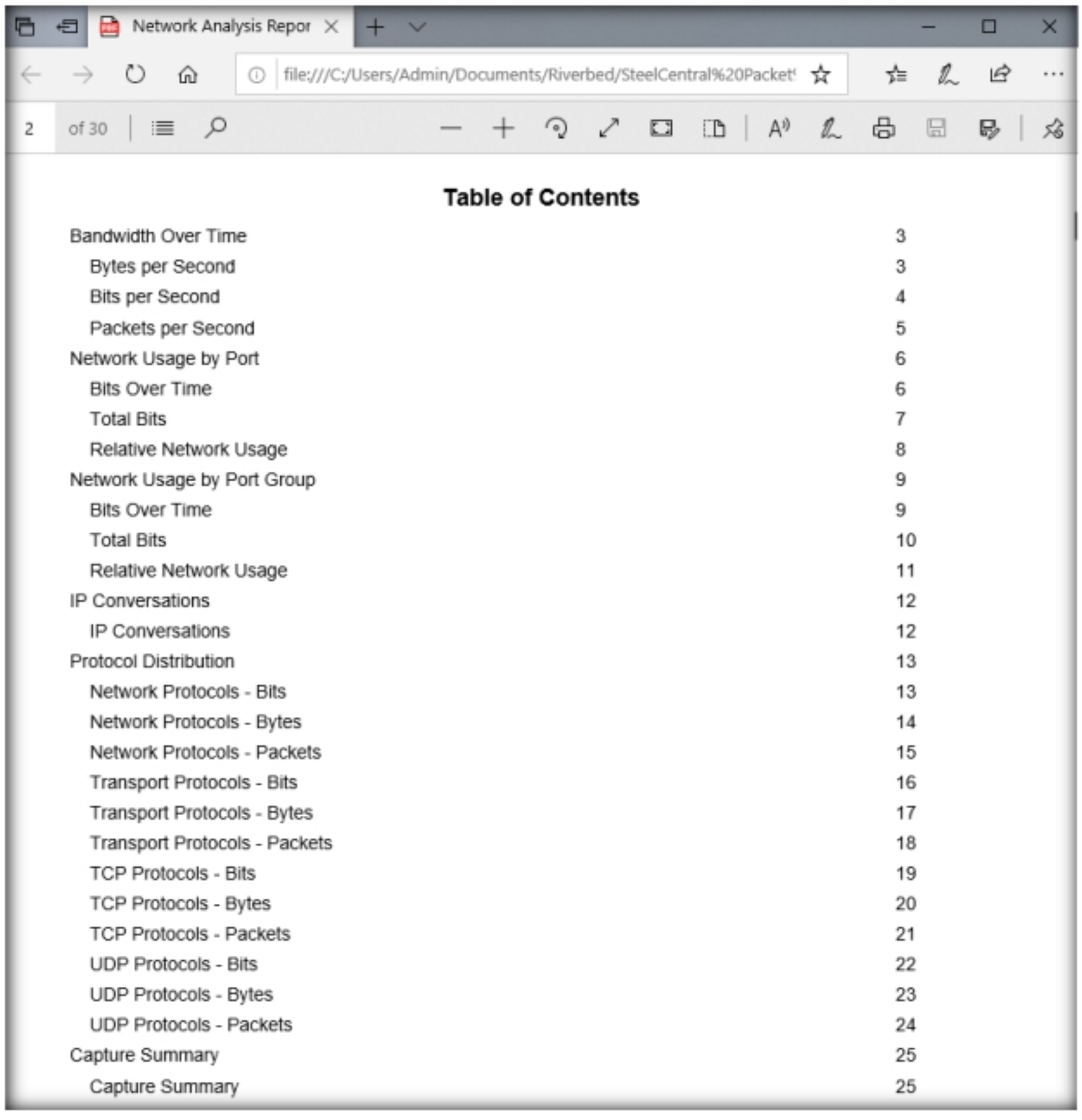


Table of Contents

Figure 2.4.28: Network Analysis Report

You can also use other sniffing tools such as **Observer Analyzer** (https://www.viavisolutions.com), **PRTG Network Monitor** (https://www.paessler.com), **SolarWinds Deep Packet Inspection and Analysis** (https://www.solarwinds.com), or **Xplico** (https://www.xplico.org) to analyze the network.

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

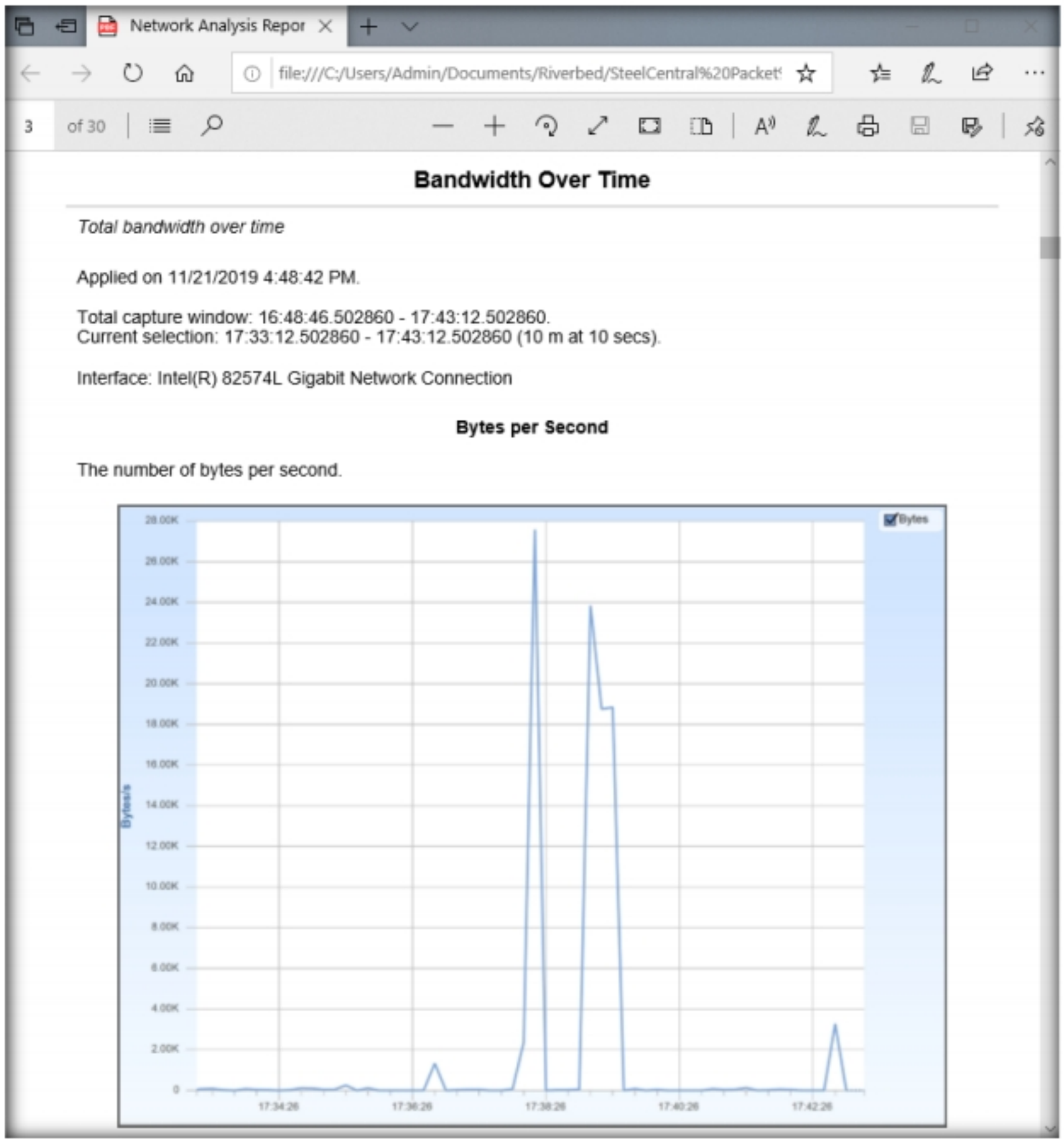


Figure 2.4.29: Network Analysis Report

42. This concludes the demonstration of analyzing a network using SteelCentral Packet Analyzer.
43. Close all open windows and document all the acquired information.
44. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Detect Network Sniffing

Ethical hackers and pen testers are aided in the detection of network sniffing by various tools that make its detection an easy task.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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 in a switch-based network
- Detect ARP attacks using XArp
- Detect promiscuous mode using Nmap and NetScanTools Pro

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- XArp located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp**

- You can also download the latest version of XArp from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 30 Minutes

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

Lab Tasks

TASK 1

Detect ARP Poisoning in a Switch-Based Network

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.

Note: In this task, we will use the **Windows Server 2019** virtual machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 10** and **Parrot Security** virtual machines. Further, we will use the same machine (**Windows Server 2019**) to detect ARP poisoning.

TASK 1.1

Launch and Configure Cain & Abel

1. Turn on the **Windows Server 2019**, **Windows 10** and **Parrot Security** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with credentials **Administrator** and **Pa$$w0rd**.
3. Double-click the **Cain** icon on **Desktop** to launch **Cain & Abel**.

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.

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

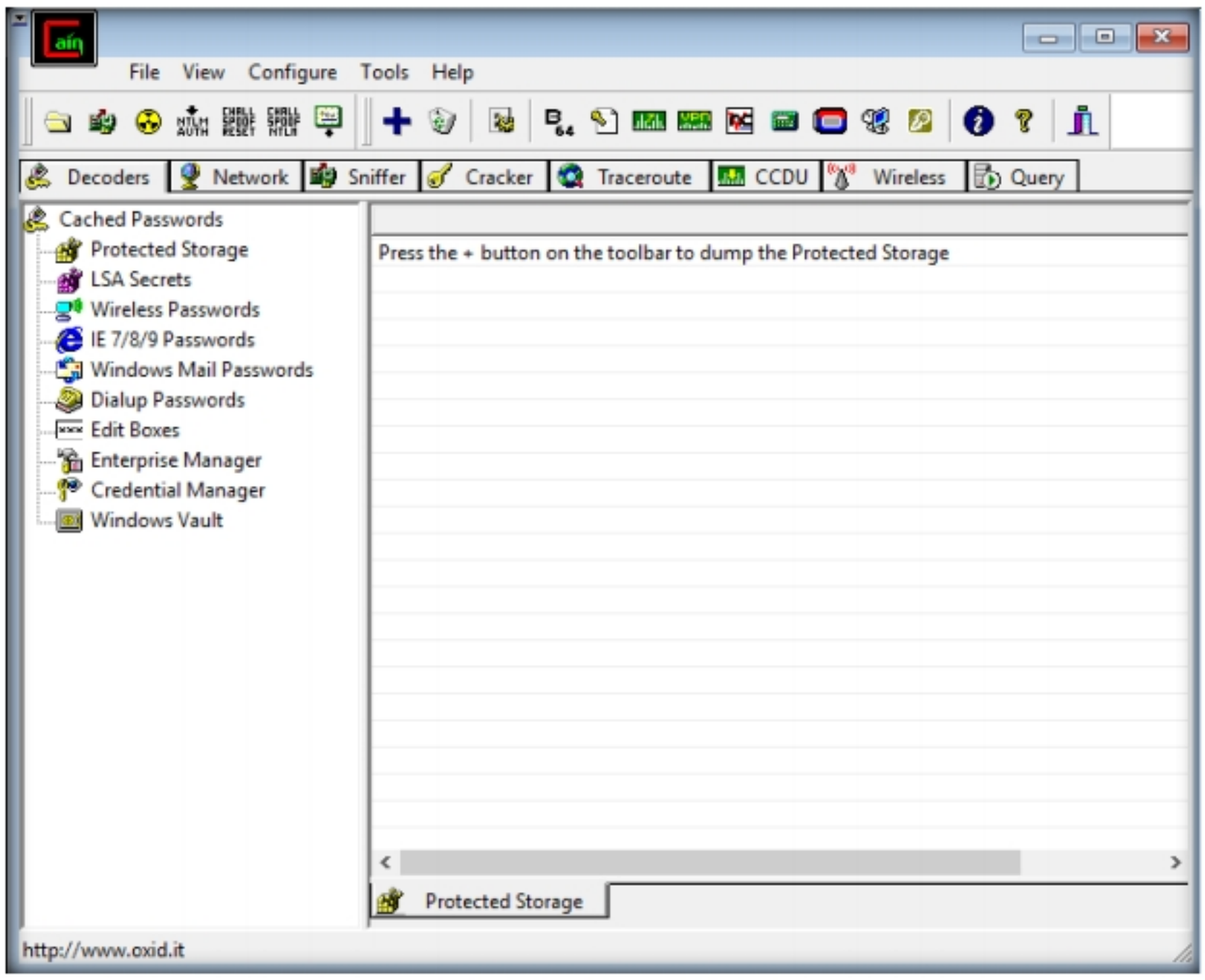


Figure 3.1.1: Cain & Abel Main Window

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.

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

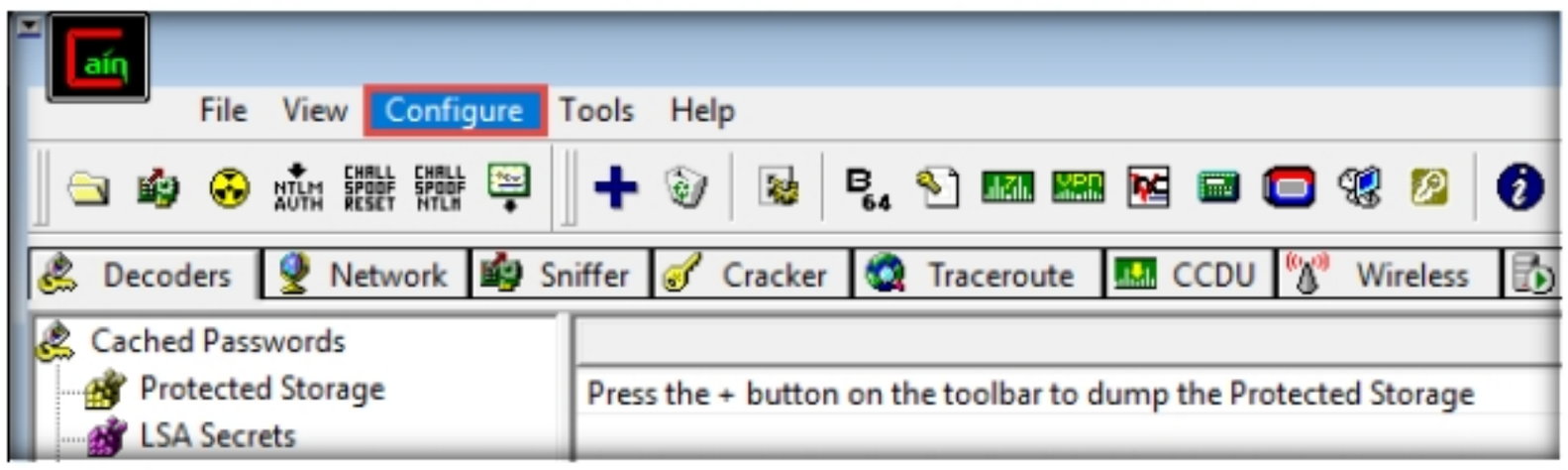


Figure 3.1.2: Cain & Abel Configuration Option

6. 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**.

Note: The adapter might differ in your lab environment.

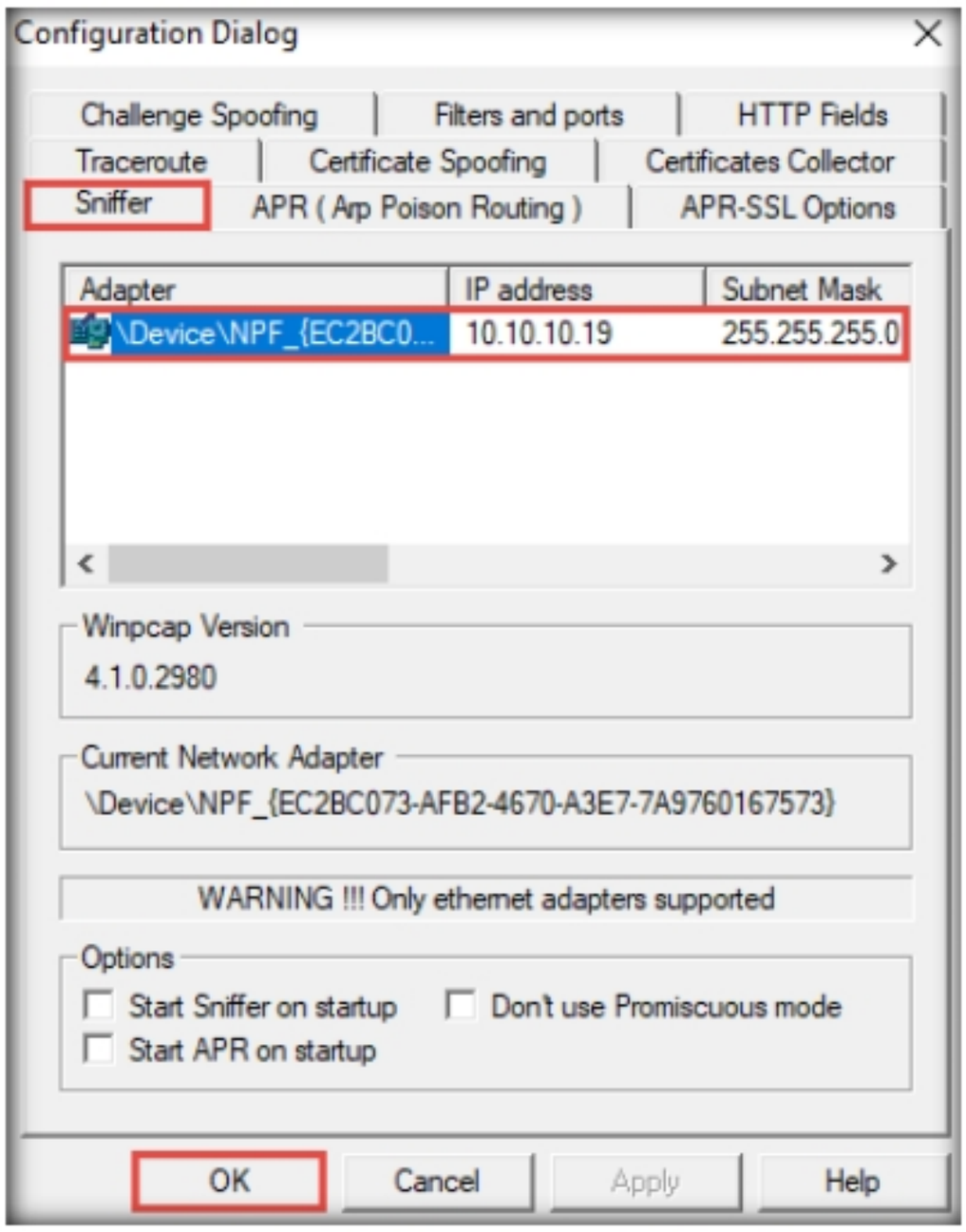


Figure 3.1.3: Cain & Abel Configuration Dialog Window

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

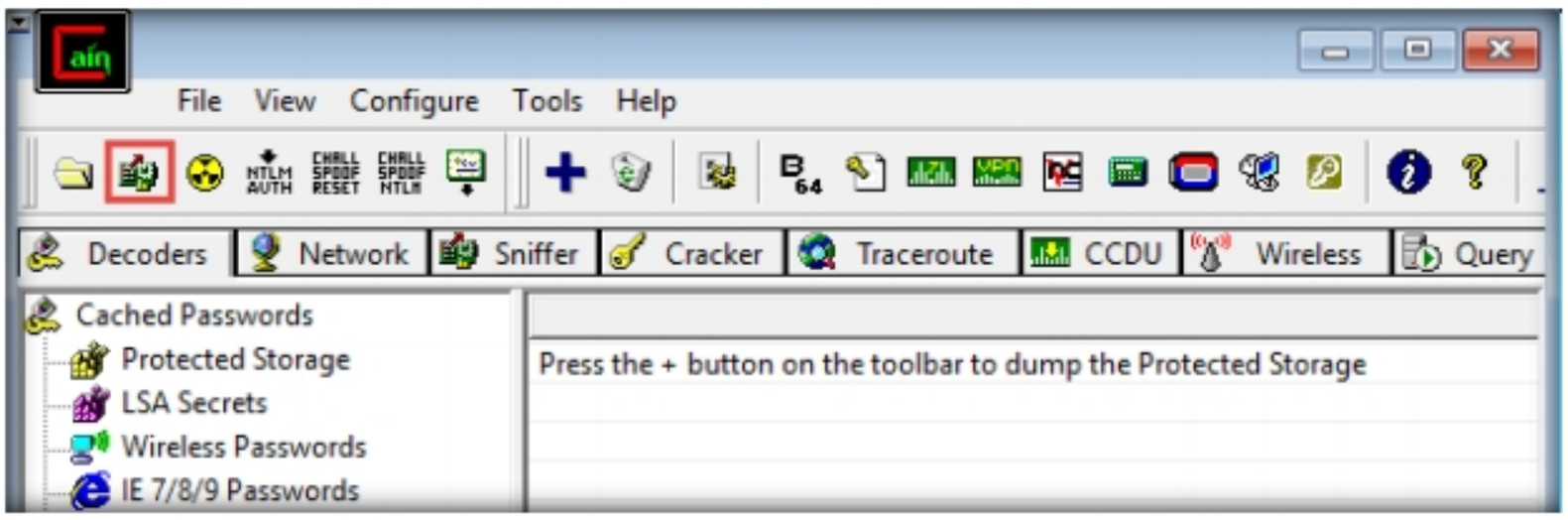


Figure 3.1.4: Starting a sniffer

8. The **Cain** pop-up appears with a **Warning** message, click **OK**.
9. Now, click the **Sniffer** tab.

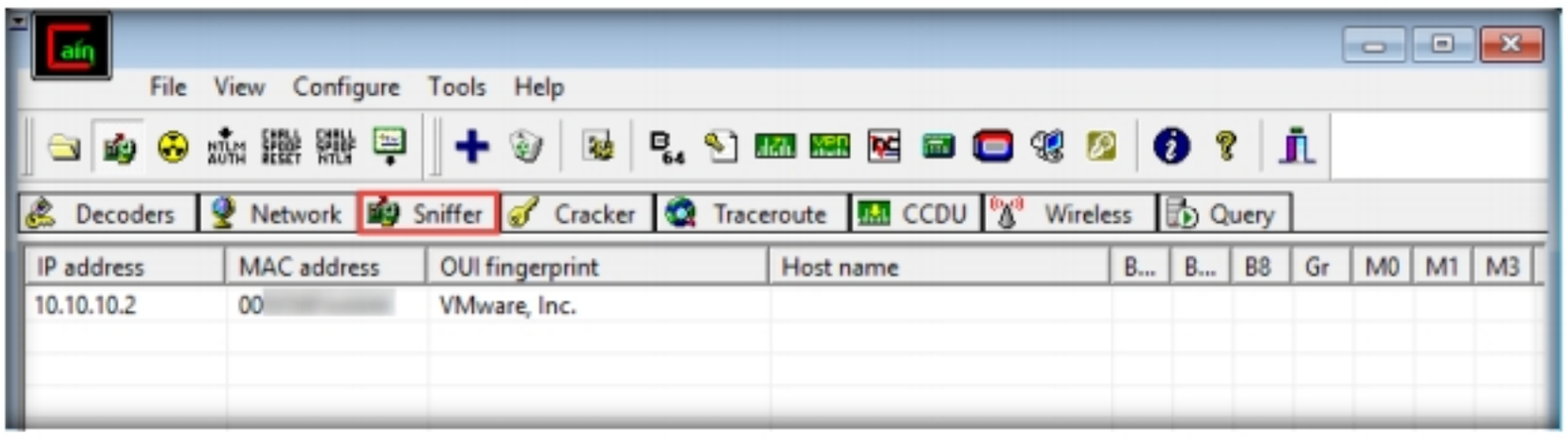


Figure 3.1.5: Sniffer tab

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 Range** radio button and specify the IP address range as **10.10.10.1-10.10.10.30**. Select the **All Tests** checkbox; then, click **OK**.

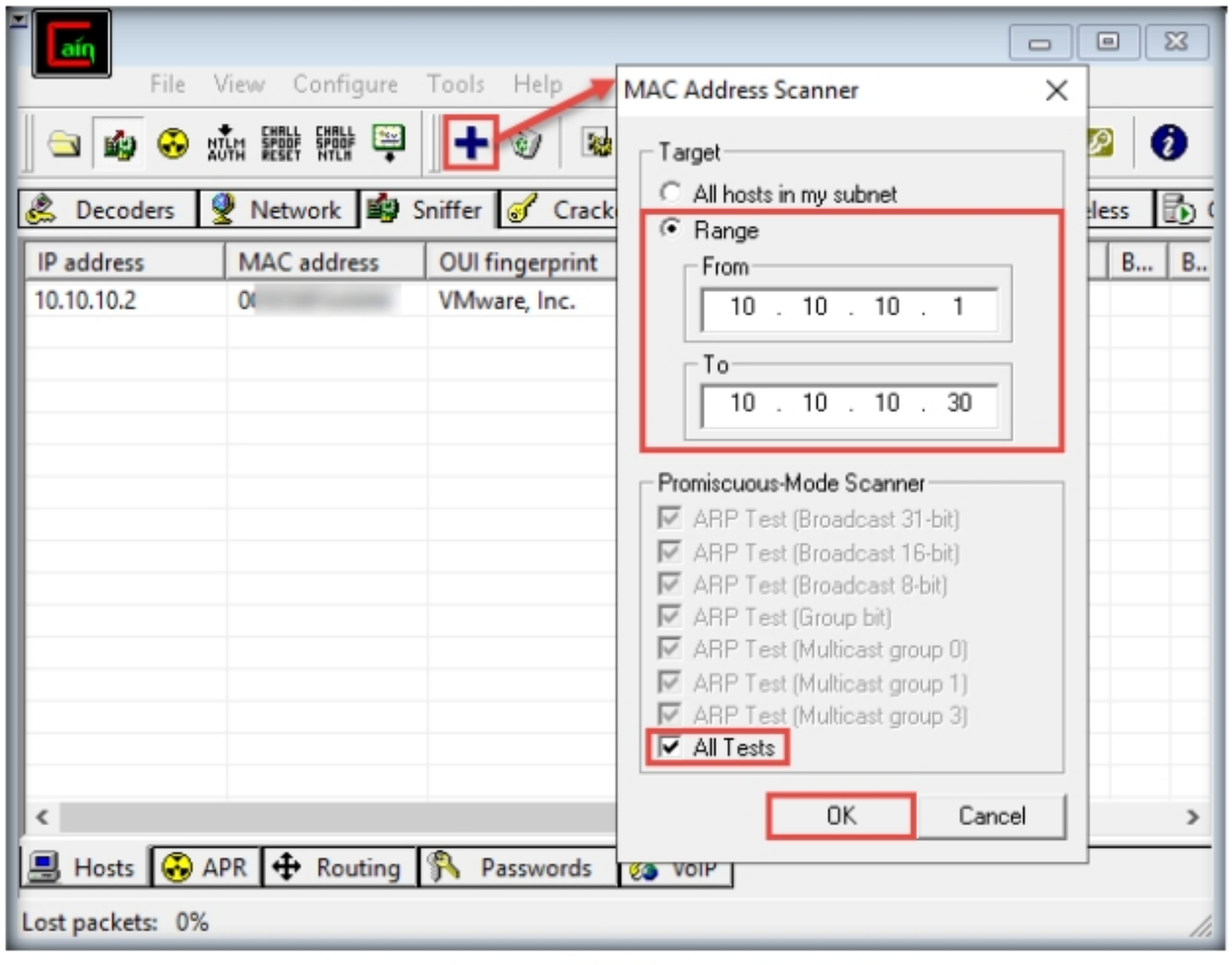


Figure 3.1.6: Cain & Abel: MAC Address Scanner Window

12. Cain & Abel starts scanning for MAC addresses and lists all those found.
13. 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.

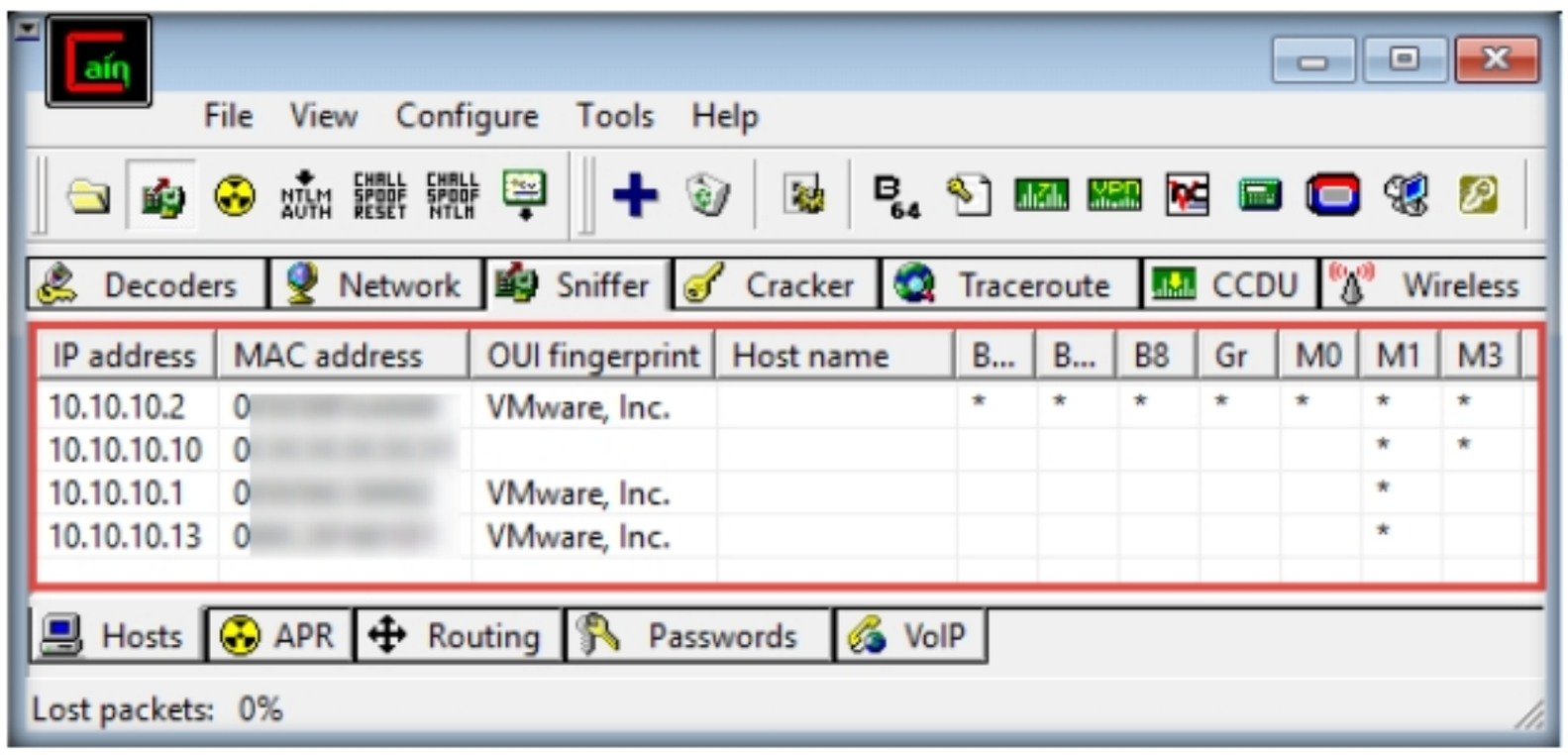


Figure 3.1.7: Cain & Abel: MAC Address Scanned

TASK 1.2

Perform ARP Poisoning

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.

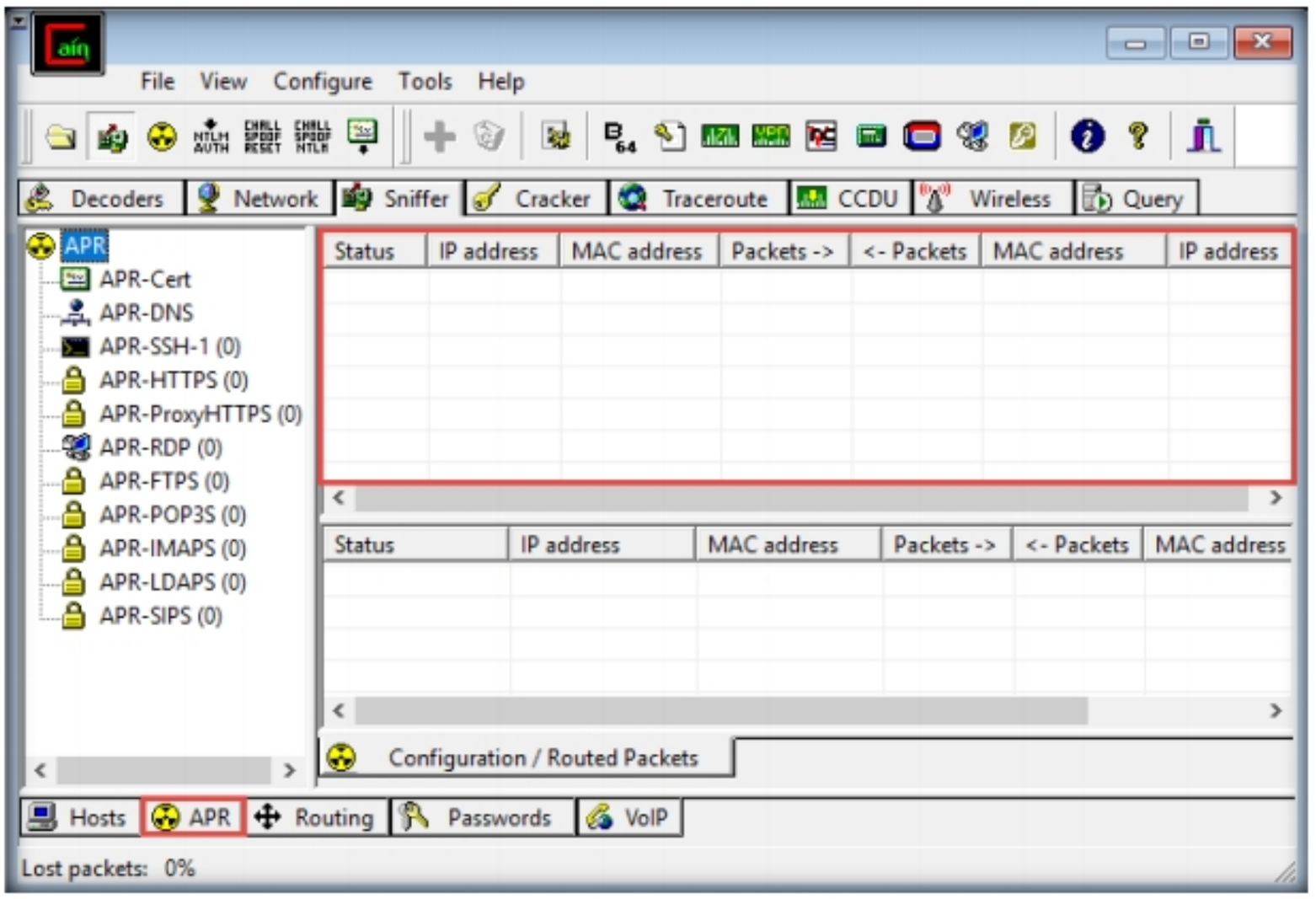


Figure 3.1.8: Cain & Abel ARP Tab

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

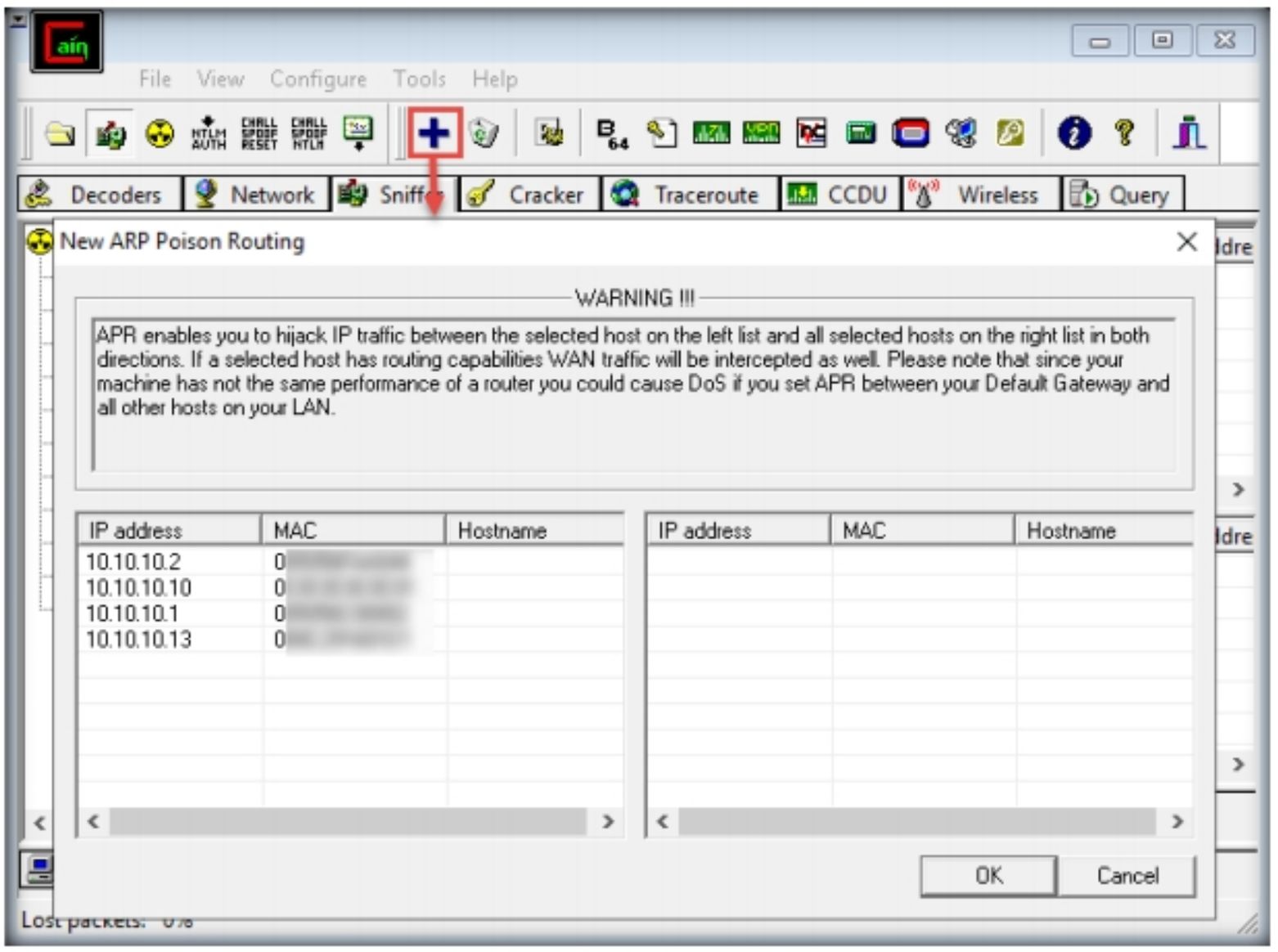


Figure 3.1.9: New ARP Poison Routing window

17. To monitor the traffic between two systems (here, **Windows 10** and **Parrot Security**), from the left-hand pane, click to select **10.10.10.10** (**Windows 10**) and from the right-hand pane, click **10.10.10.13** (**Parrot Security**); click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

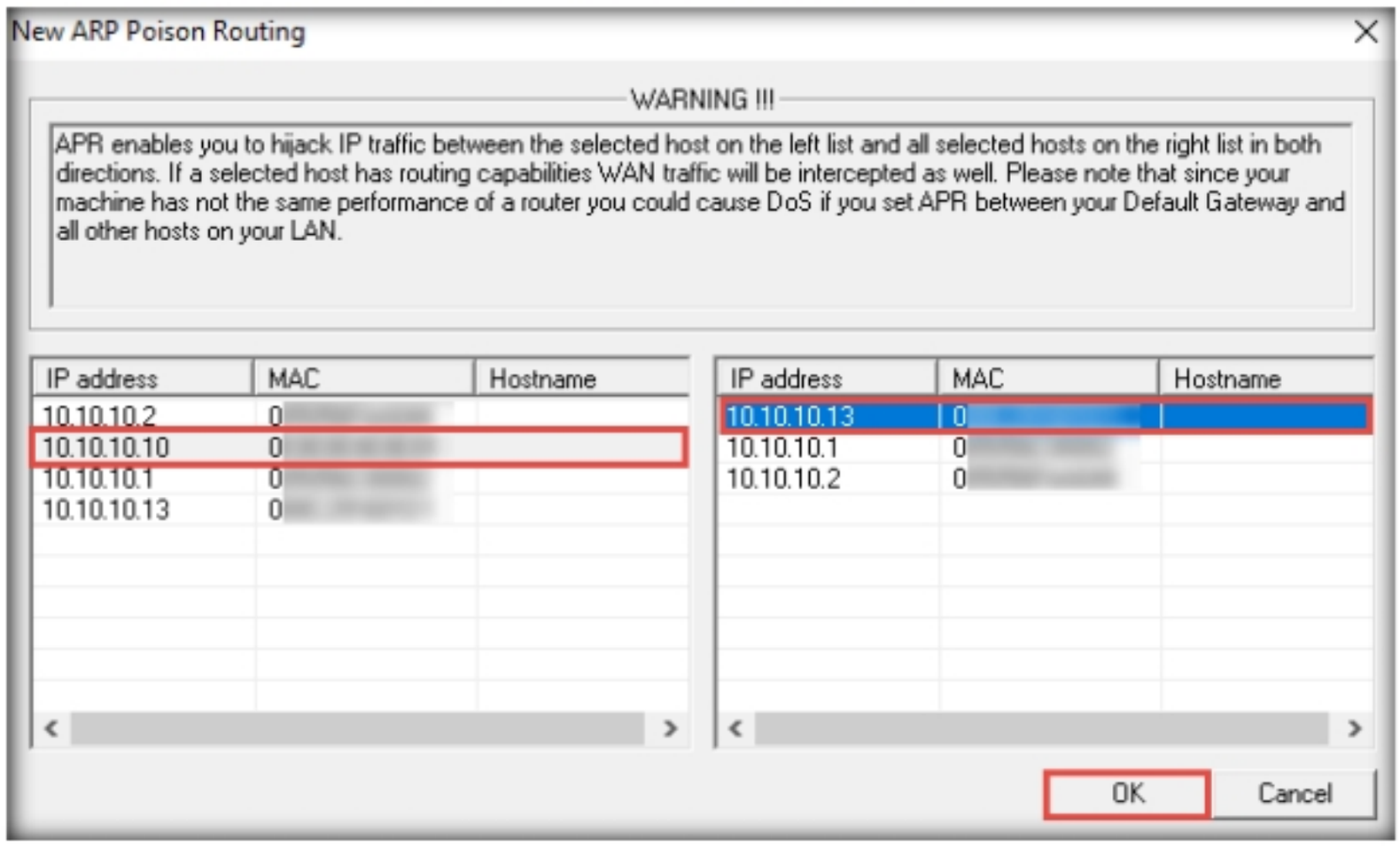


Figure 3.1.10: Monitoring traffic between two computers

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

19. Click on the **Start/Stop APR** icon ( ) to start capturing ARP packets.

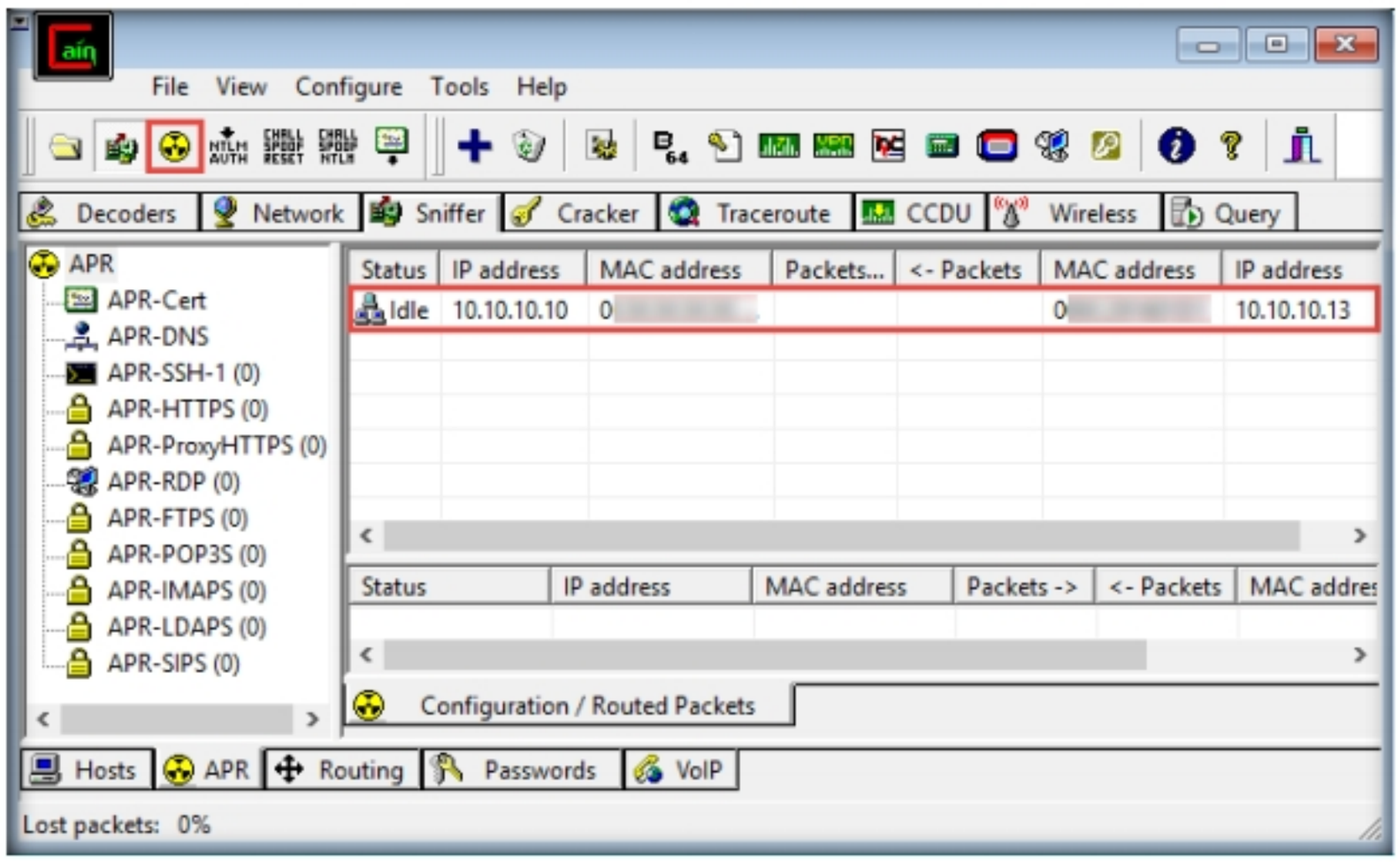


Figure 3.1.11: Click on Start/Stop APR

20. 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.

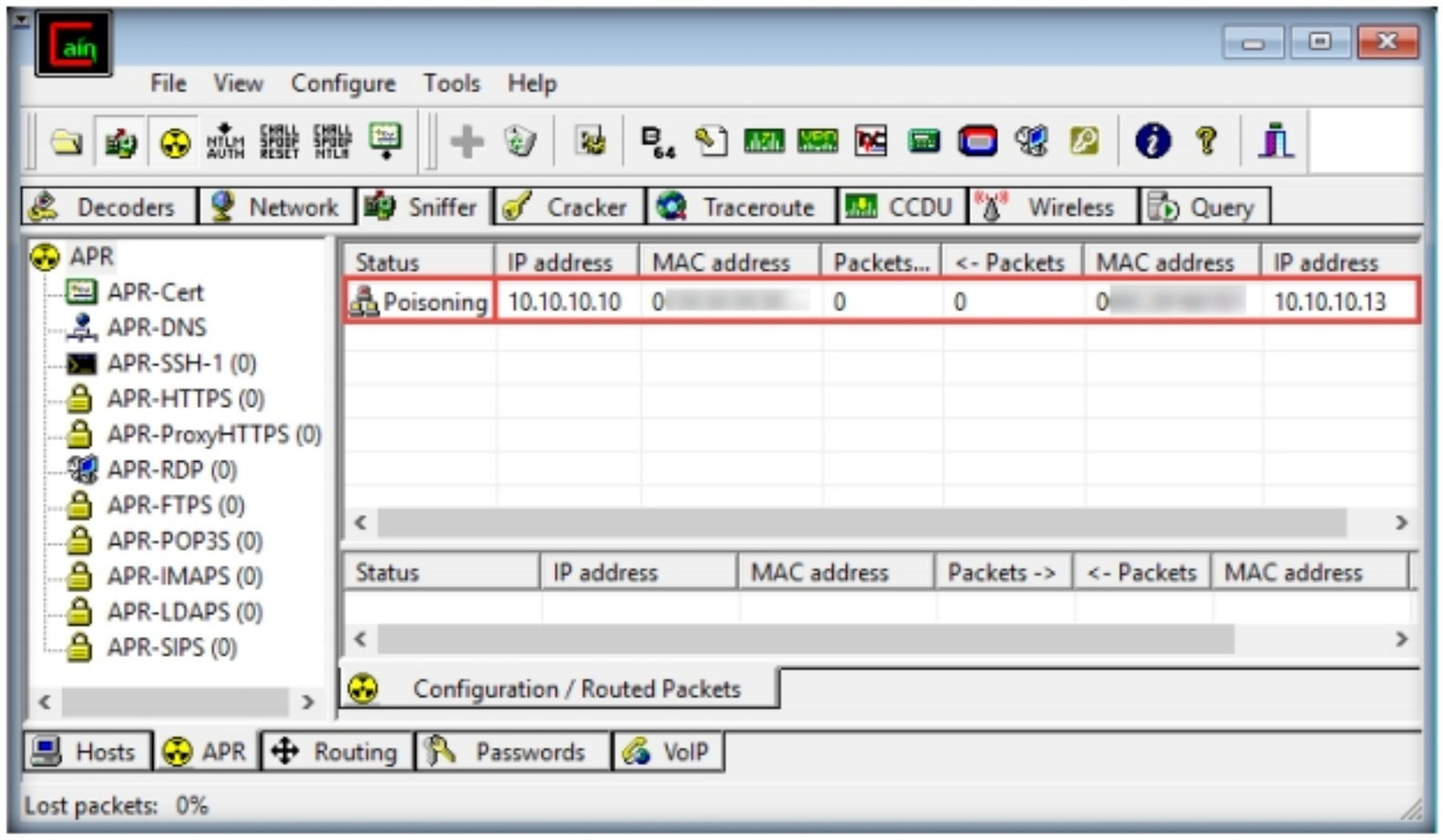


Figure 3.1.12: Performing ARP Poison Routing

21. Cain & Abel intercepts the traffic traversing between these two machines.
22. To generate traffic between the machines, you need to ping one target machine using the other.
23. Switch to the **Parrot Security** virtual machine
24. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

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

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

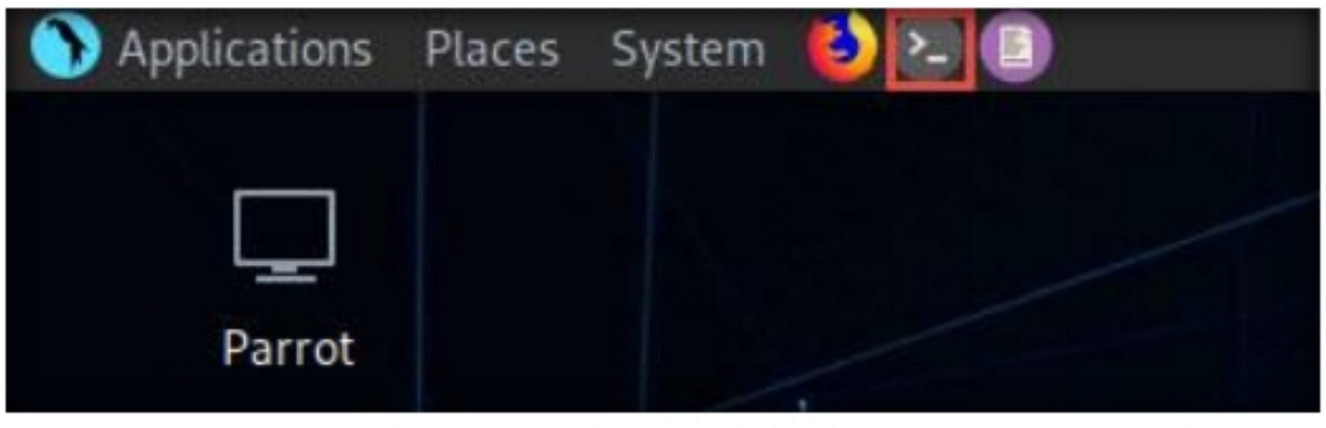


Figure 3.1.13: MATE Terminal Icon

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

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

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

TASK 1.3

Ping Windows 10 Machine

29. In the terminal window, type **hping3 <Target IP Address> -c 100000** (here, target IP address is **10.10.10.10** [**Windows 10**]) and press **Enter**.

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

30. This command will start pinging the target machine (**Windows 10**) with 100,000 packets.

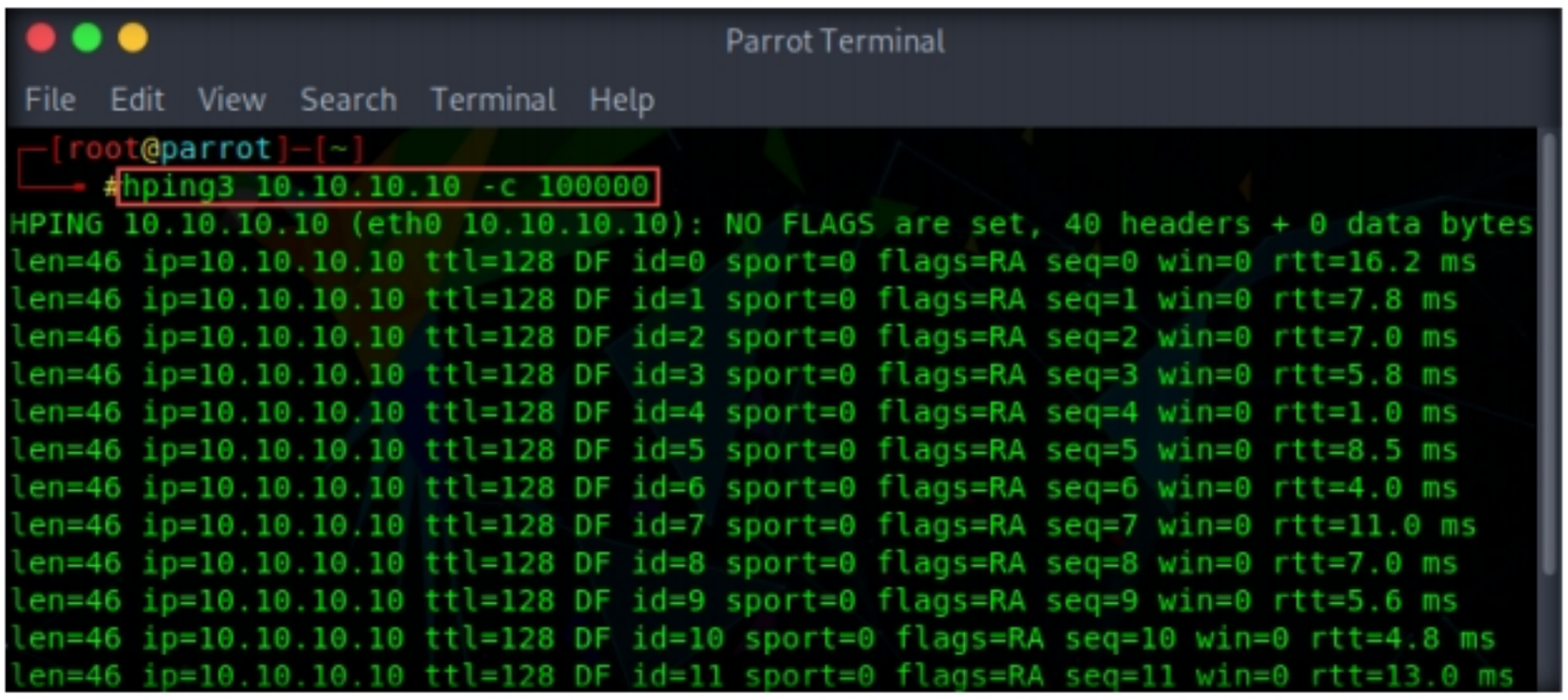


Figure 3.1.14: Ping the target machine

TASK 1.4

Detect ARP Poisoning

31. Leave the command running and immediately switch to the **Windows Server 2019** virtual machine.
32. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wire**. Click **Wireshark** from the results.

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

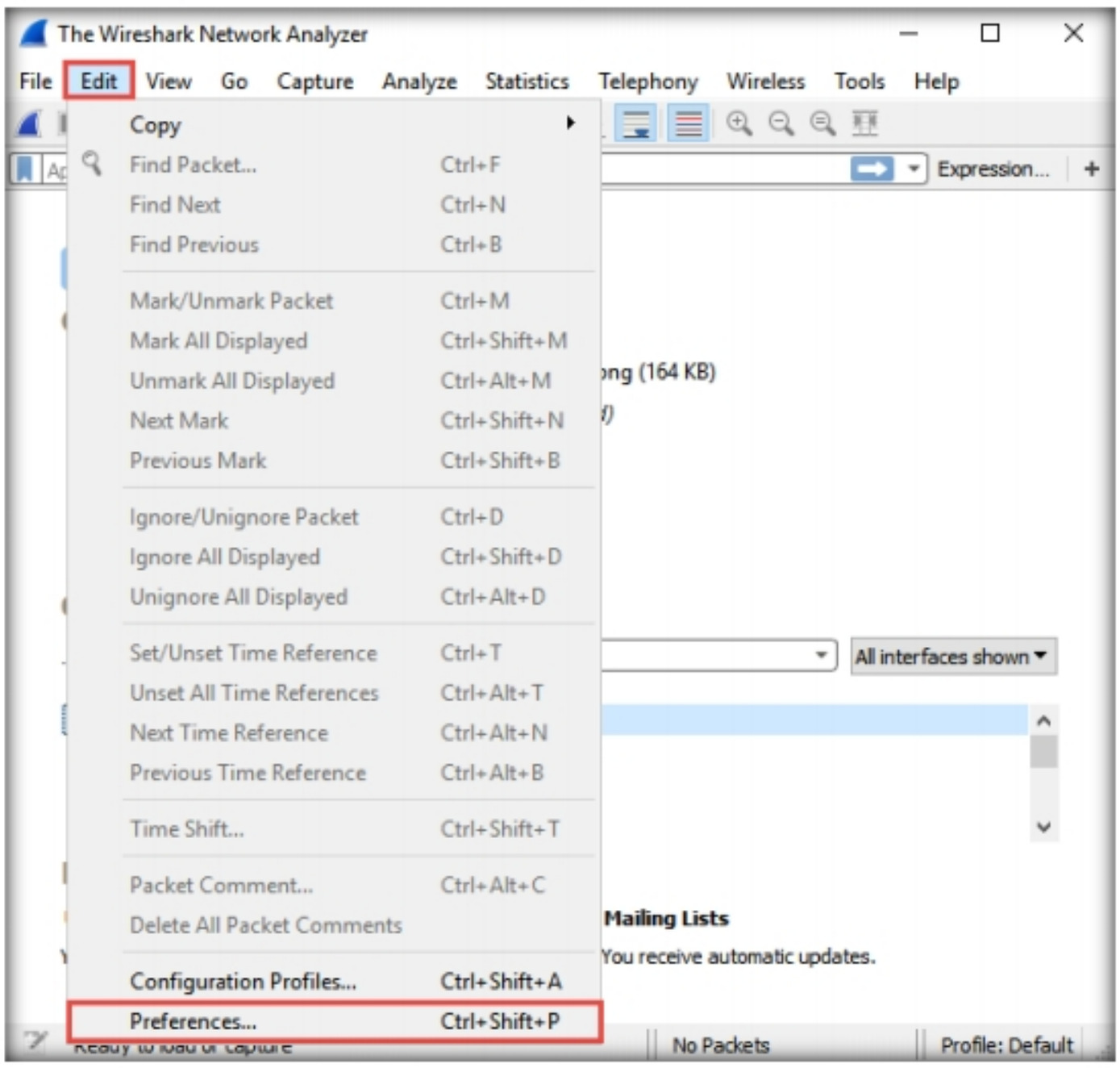


Figure 3.1.15: Launching Preferences

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

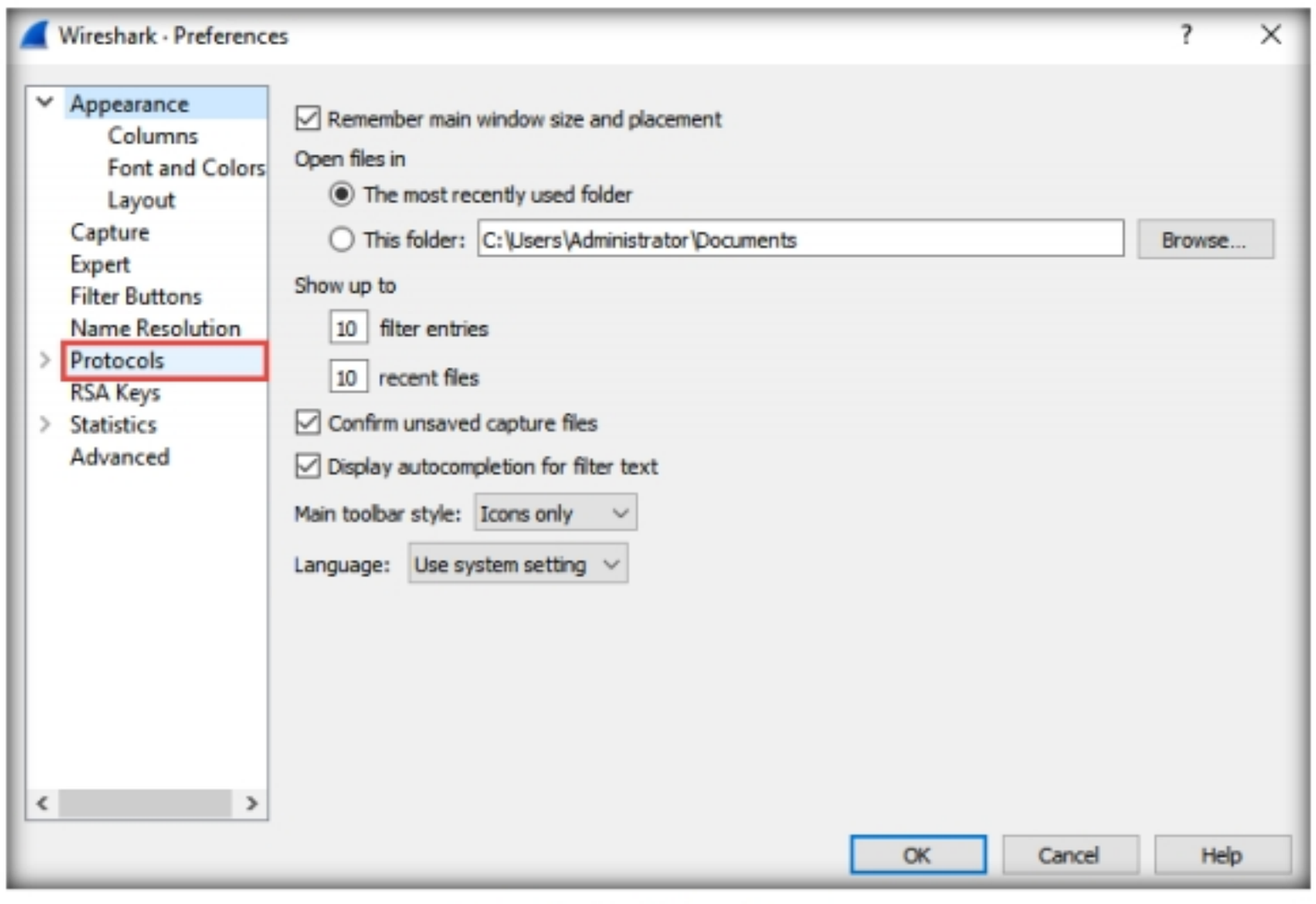


Figure 3.1.16: Viewing Protocols

35. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.
36. 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**.

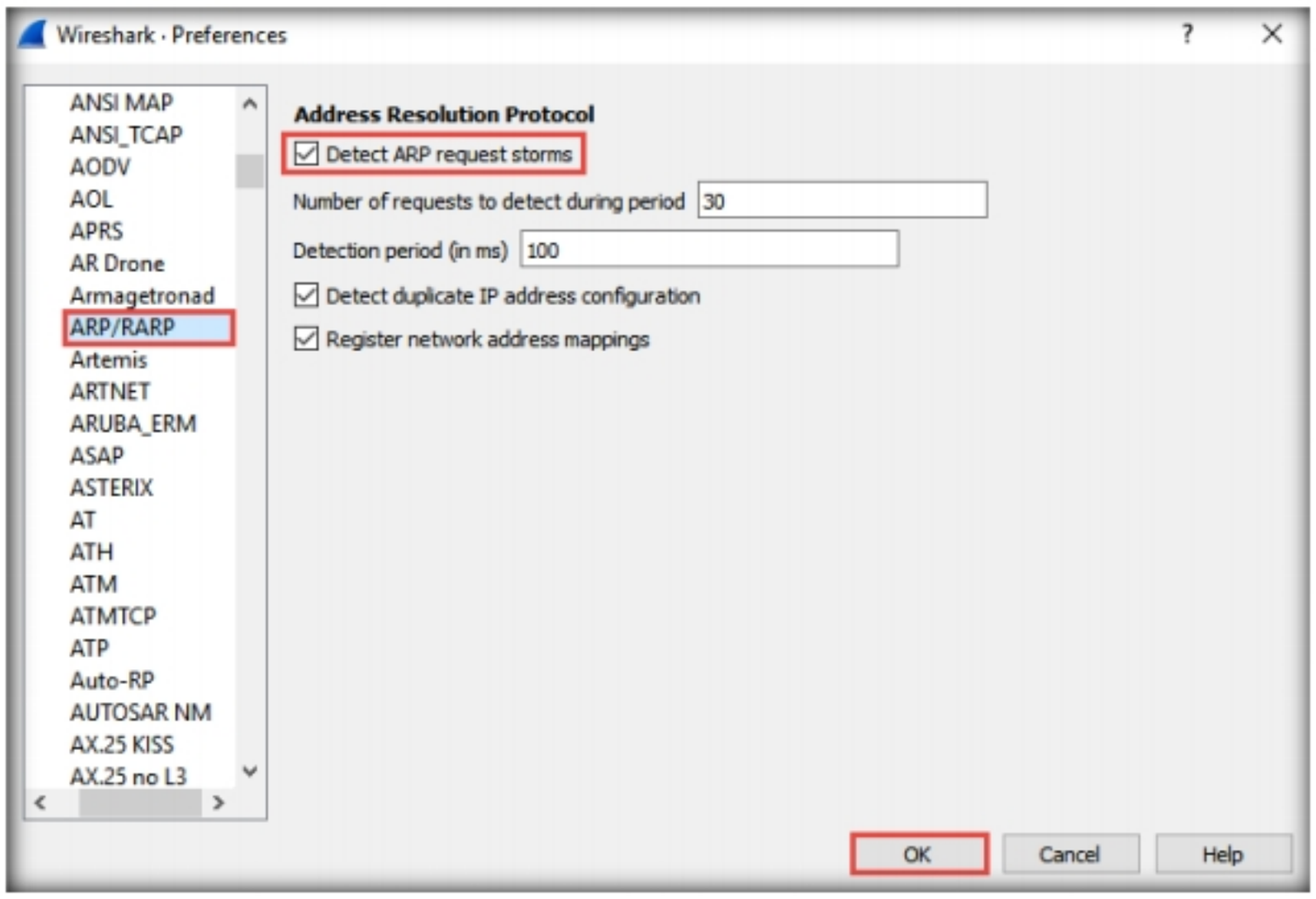


Figure 3.1.17: Configuring ARP Detection Settings

37. Now, double-click on the adapter associated with your network (here, **Ethernet0**) to start capturing the network packets.

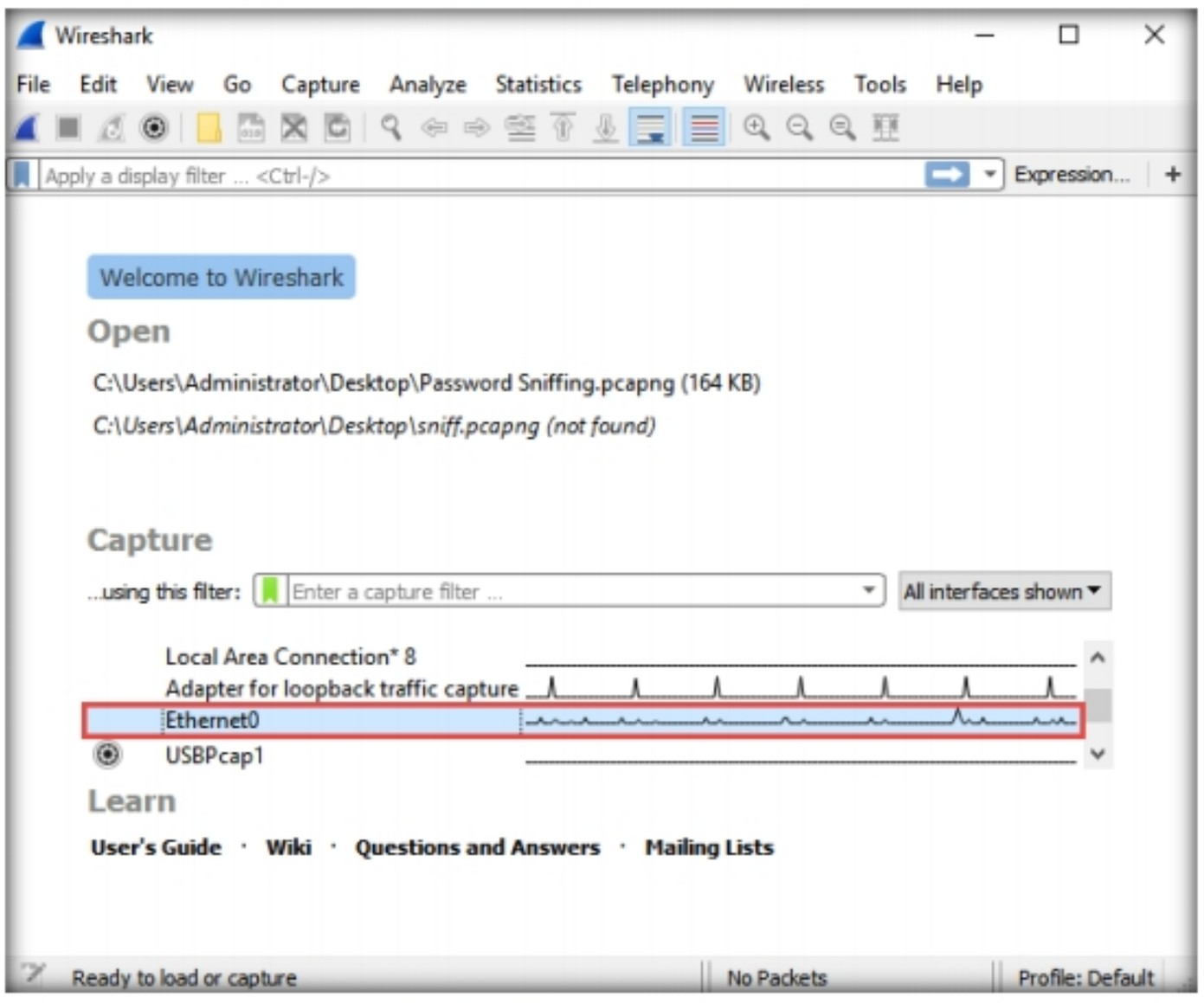


Figure 3.1.18: Starting Capture

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

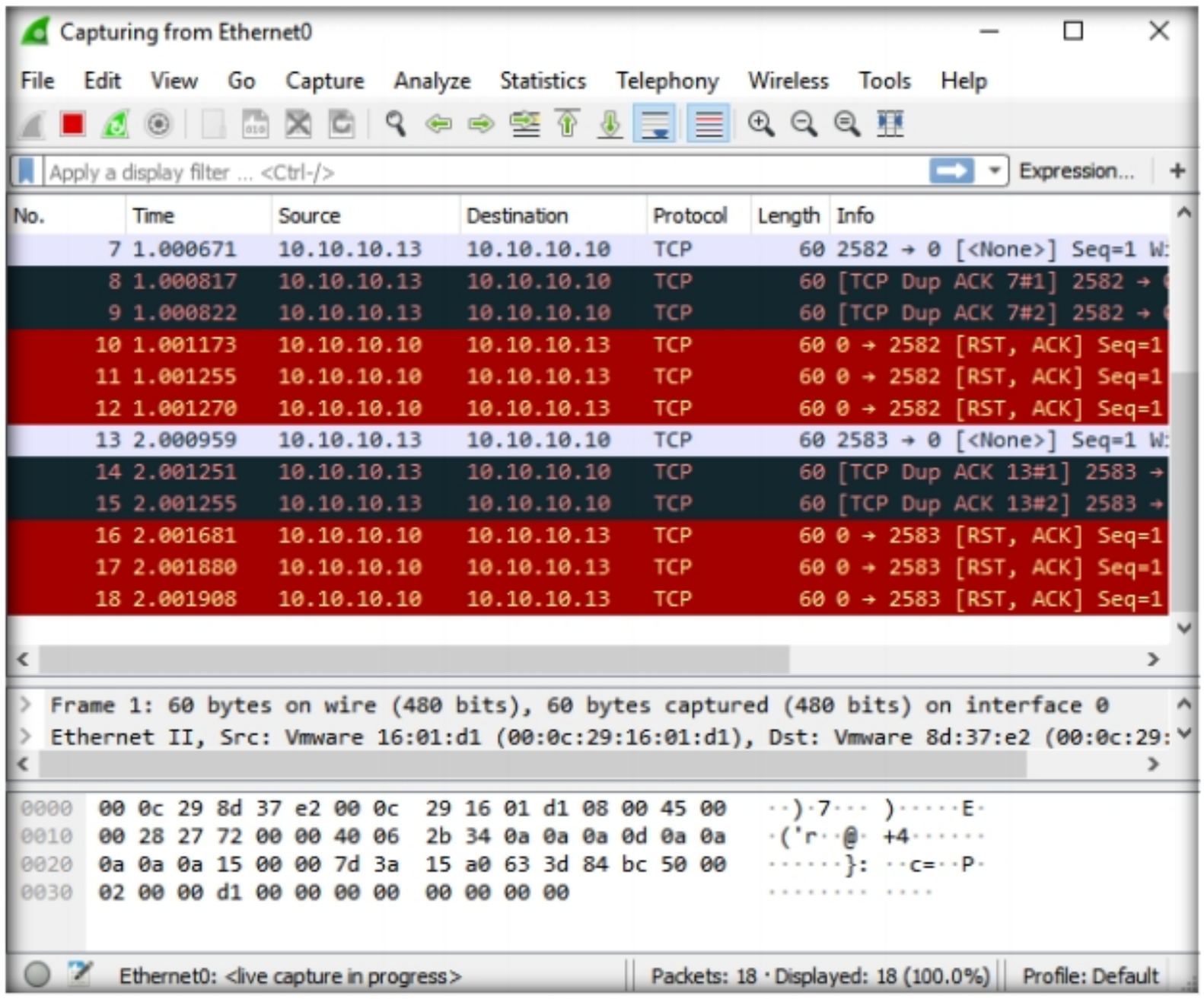


Figure 3.1.19: Wireshark Capturing Packets

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

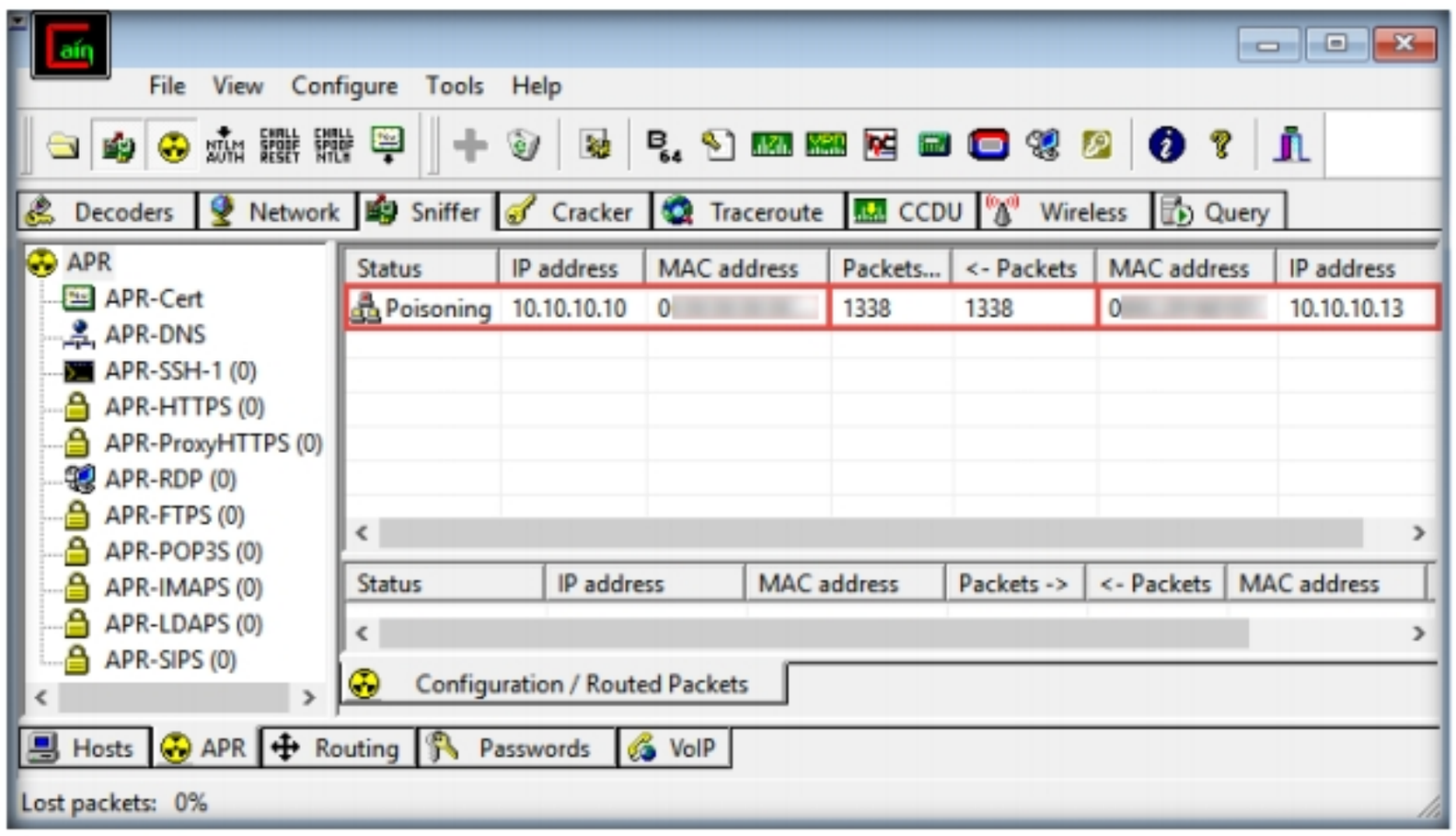


Figure 3.1.20: ARP Poisoning Detected

40. Now, switch to **Wireshark** and click the **Stop packet capturing** icon ( ) to stop the packet capturing.

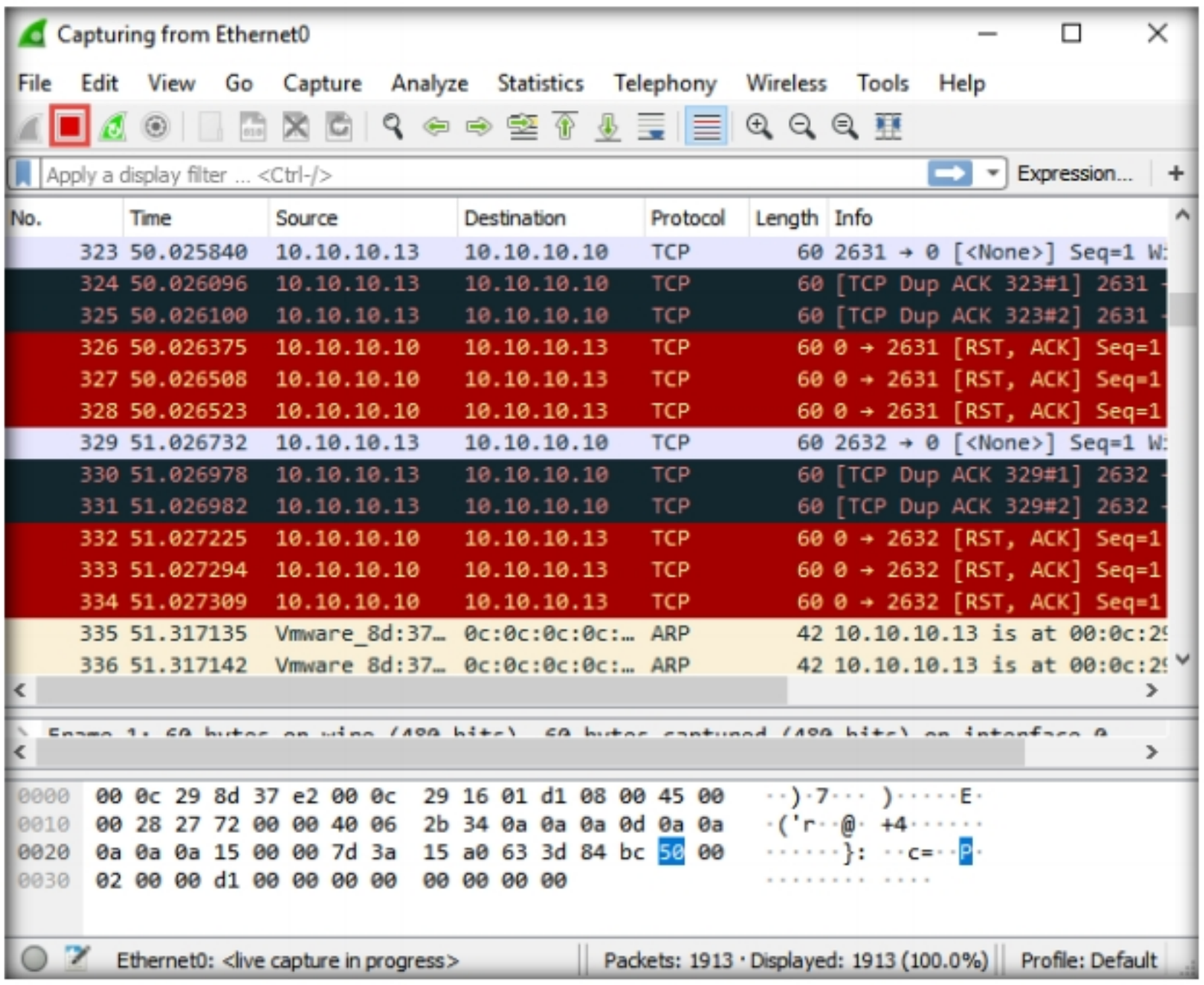


Figure 3.1.21: Stopping Packet Capture

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

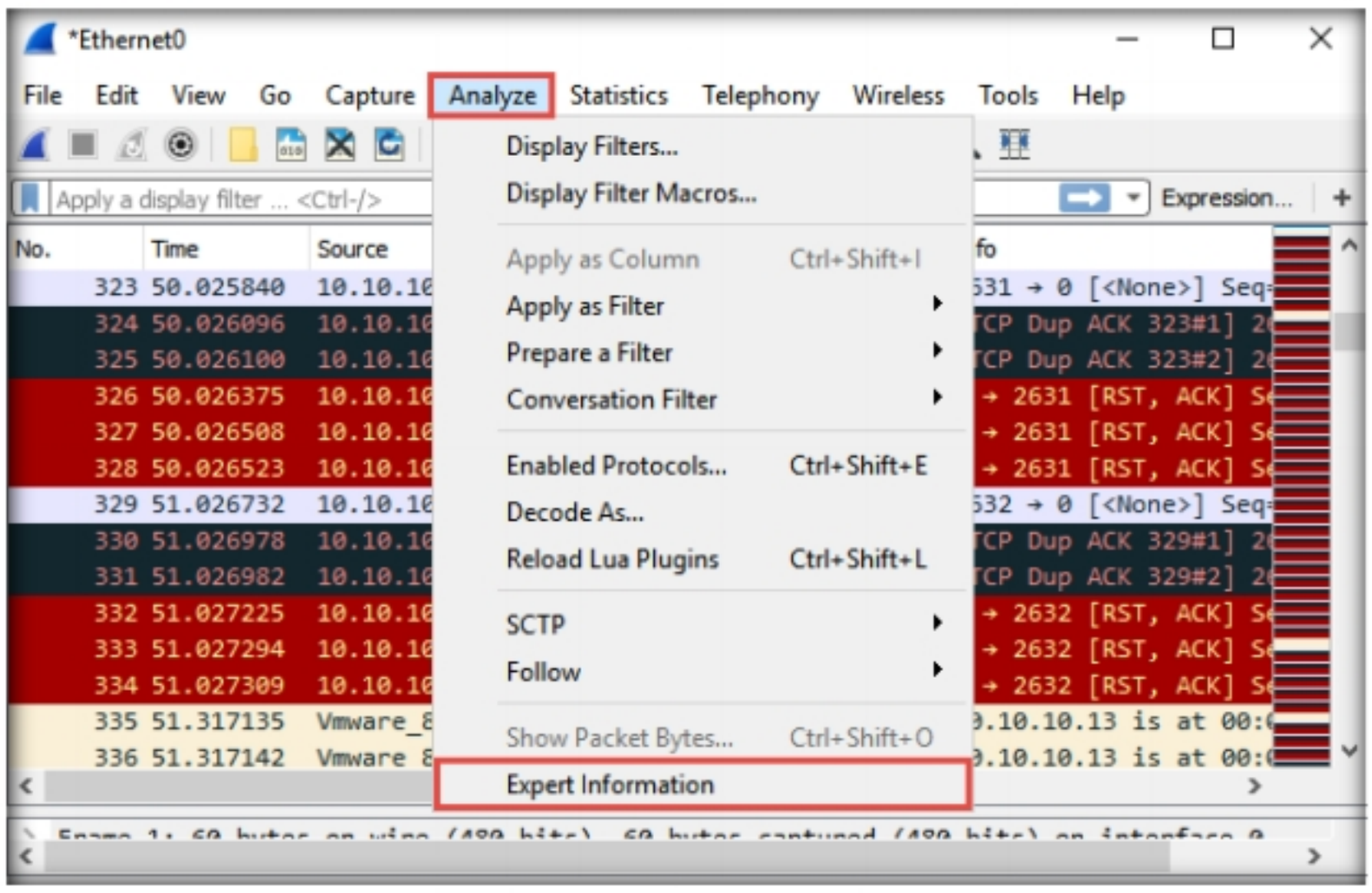


Figure 3.1.22: Analyzing Expert Information

42. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.10.10)**, running on the **ARP/RARP** protocol.

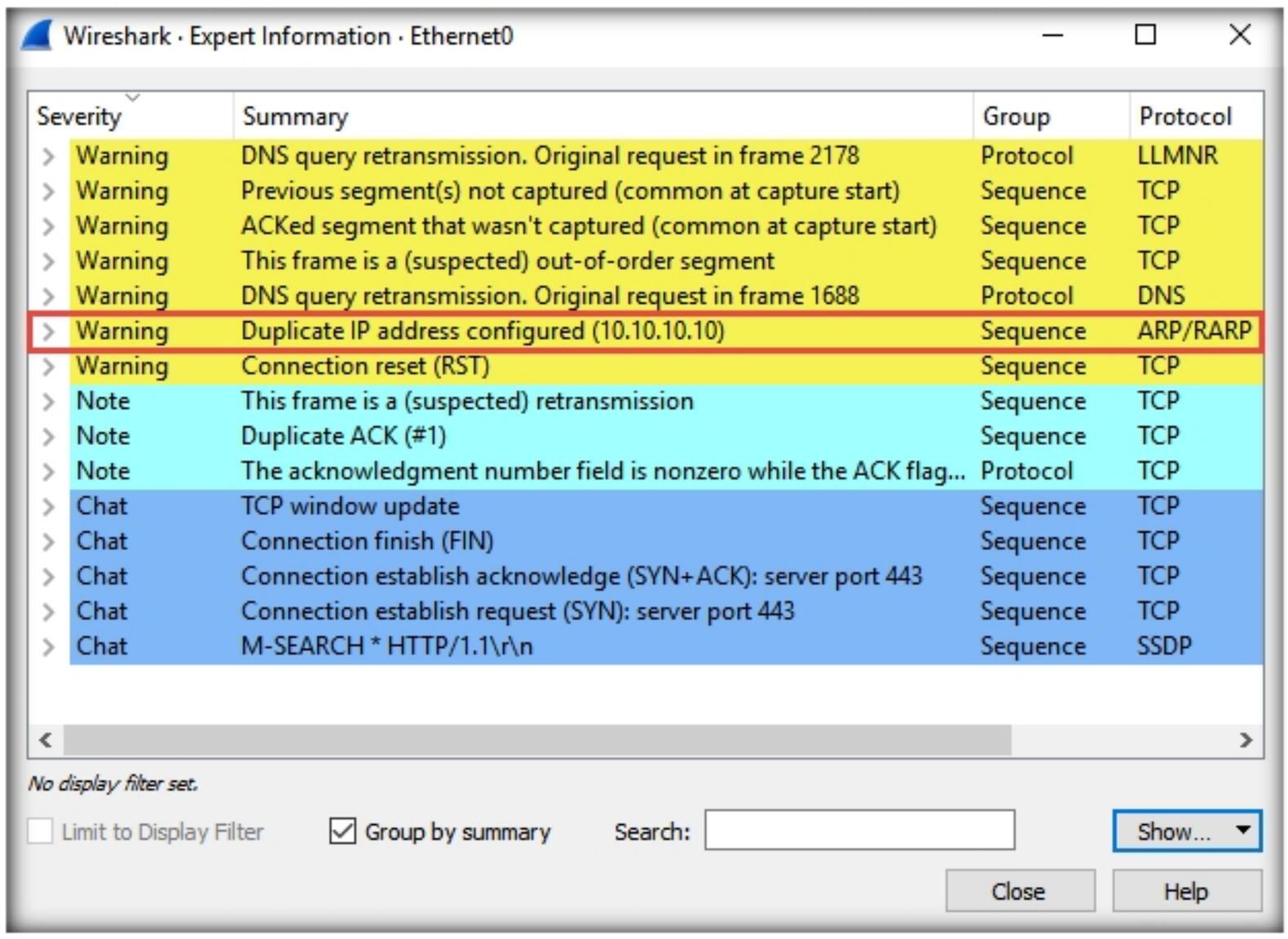


Figure 3.1.23: Viewing Warnings

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

44. In the **Wireshark . Expert Information** window, click any packet (here, **100**).

45. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section.

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

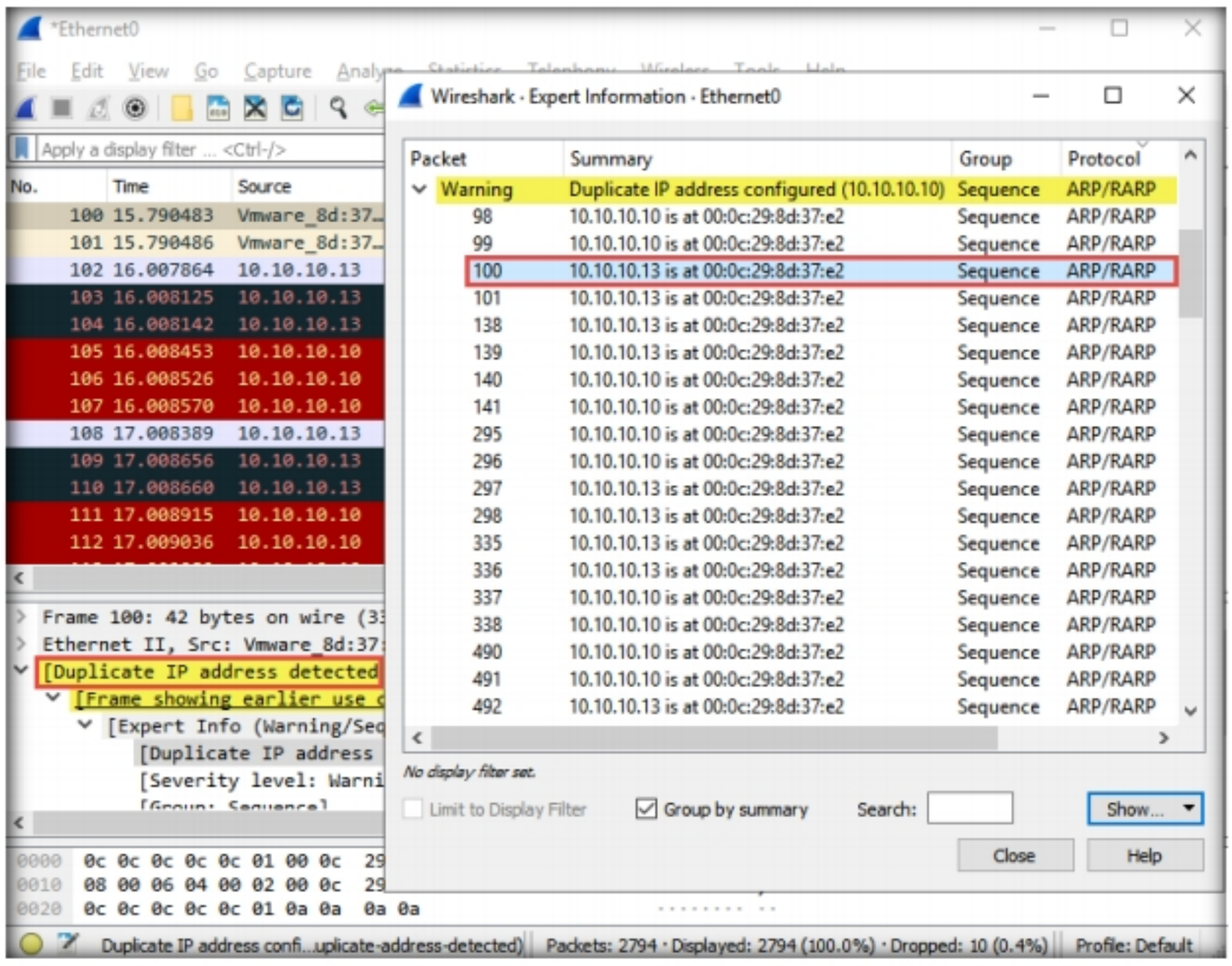


Figure 3.1.24: Duplicate IP Address Detected

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

47. This concludes the demonstration of detecting ARP poisoning in a switch-based network.
48. Close the **Wireshark** window and leave all other windows running.

TASK 2 Detect ARP Attacks using XArp

Here, we will use the XArp tool to detect ARP attacks in the network.

1. Ensure that the ARP poisoning is running from the previous task where we used the **Windows Server 2019** virtual machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** virtual machines.

TASK 2.1

Install and Launching XArp

2. Switch to the **Windows 10** virtual machine. Navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp** and double-click **xarp-2.2.2-win.exe**.

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

3. The **XArp Setup** window appears; click **Next**.
4. Follow the wizard-driven installation steps to install XArp with the default settings.

XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.

Figure 3.2.1: XArp Installation Wizard

5. On completion of the installation, the **Completing the XArp Setup Wizard** appears. Ensure that the **Run XArp** checkbox is selected and click **Finish**.

Figure 3.2.2: Completing the XArp Setup Wizard

TASK 2.2

Detect ARP Attacks

6. The XArp main window appears with a **Status** of **ARP attacks detected!** It also displays lists of the IPs, MAC addresses, hosts, and other information regarding the machines in the network.

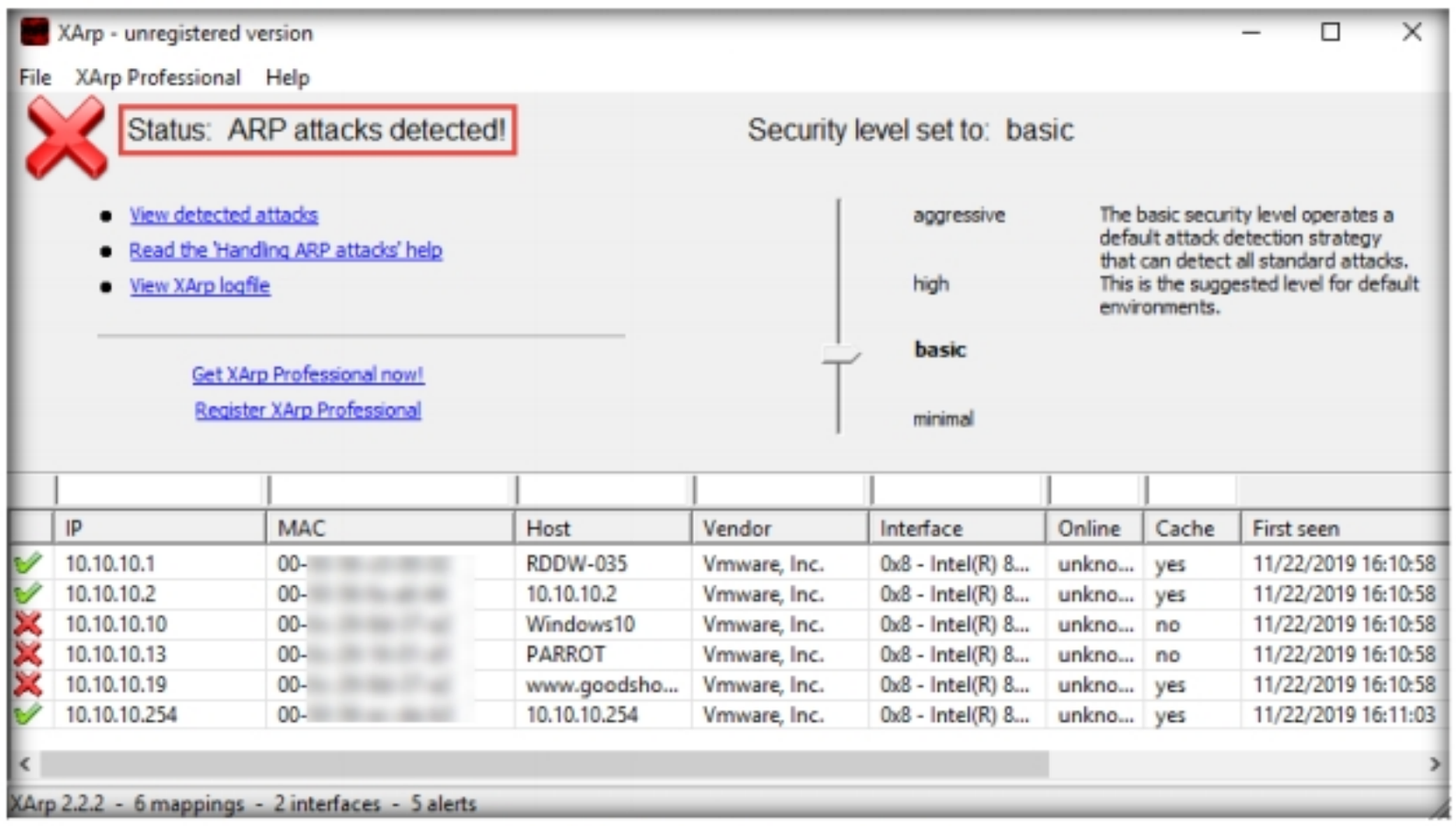


Figure 3.2.3: XArp: ARP attacks detected

You can also use other ARP spoofing detection tools such as **Capsa Network Analyzer** (https://www.colasoft.com), **ArpON** (https://sourceforge.net), **ARP AntiSpoofer** (https://sourceforge.net), or **ARPStraw** (https://github.com) to detect ARP attacks on the network.

7. The **XArp** pop-up appears in the right-hand pane of **Desktop**, displaying the **Alert**.

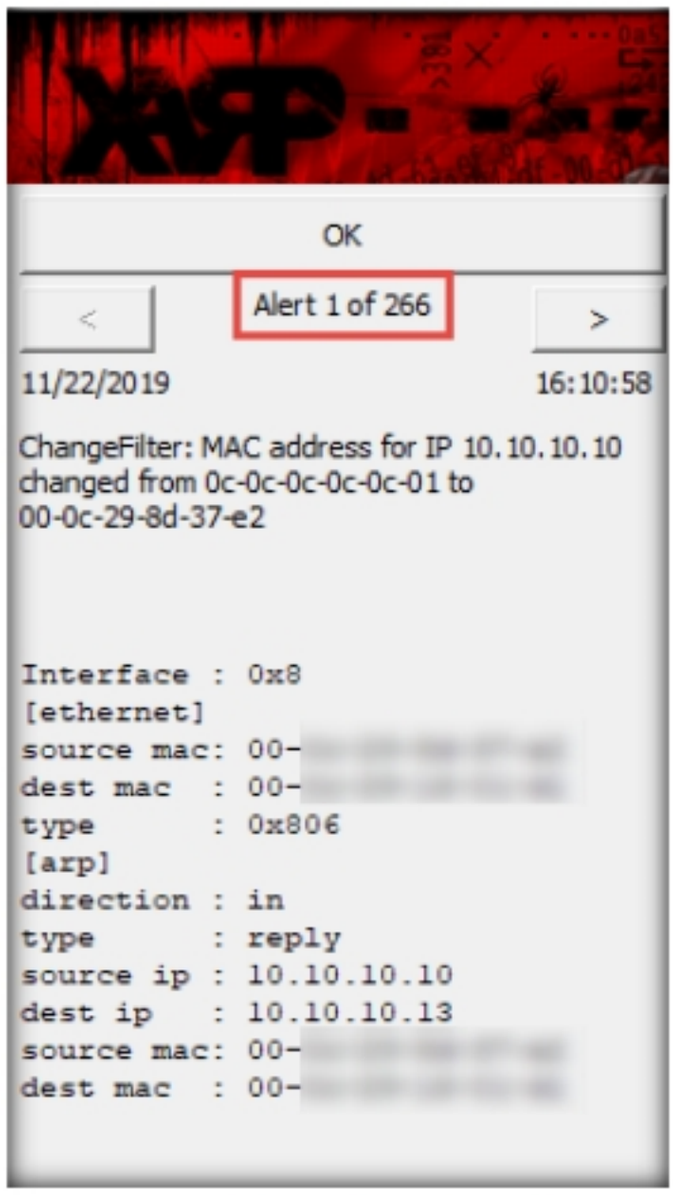


Figure 3.2.4: XArp displaying Alerts

8. This concludes the demonstration of detecting APR poisoning using XArp.

9. Close the XArp tool window and leave all other windows running.
10. Document all the acquired information.
11. Navigate to **Control Panel → Programs → Programs and Features** and uninstall **XArp**.

TASK 3 Detect Promiscuous Mode using Nmap and NetScanTools Pro

Here, we will use the Nmap Scripting Engine (NSE) and NetScan Tools Pro to check if a system on a local Ethernet has its network card in promiscuous mode.

1. Ensure that the ARP poisoning is still running from the previous task where we used the **Windows Server 2019** virtual machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** machines.

TASK 3.1

Detect Promiscuous Mode Using Nmap

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.

2. On the **Windows 10** virtual machine, double-click the **Nmap - Zenmap GUI** shortcut on **Desktop** to launch Nmap.
3. 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 **10.10.10.19** [**Windows Server 2019**]) and click **Scan**.
4. 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.

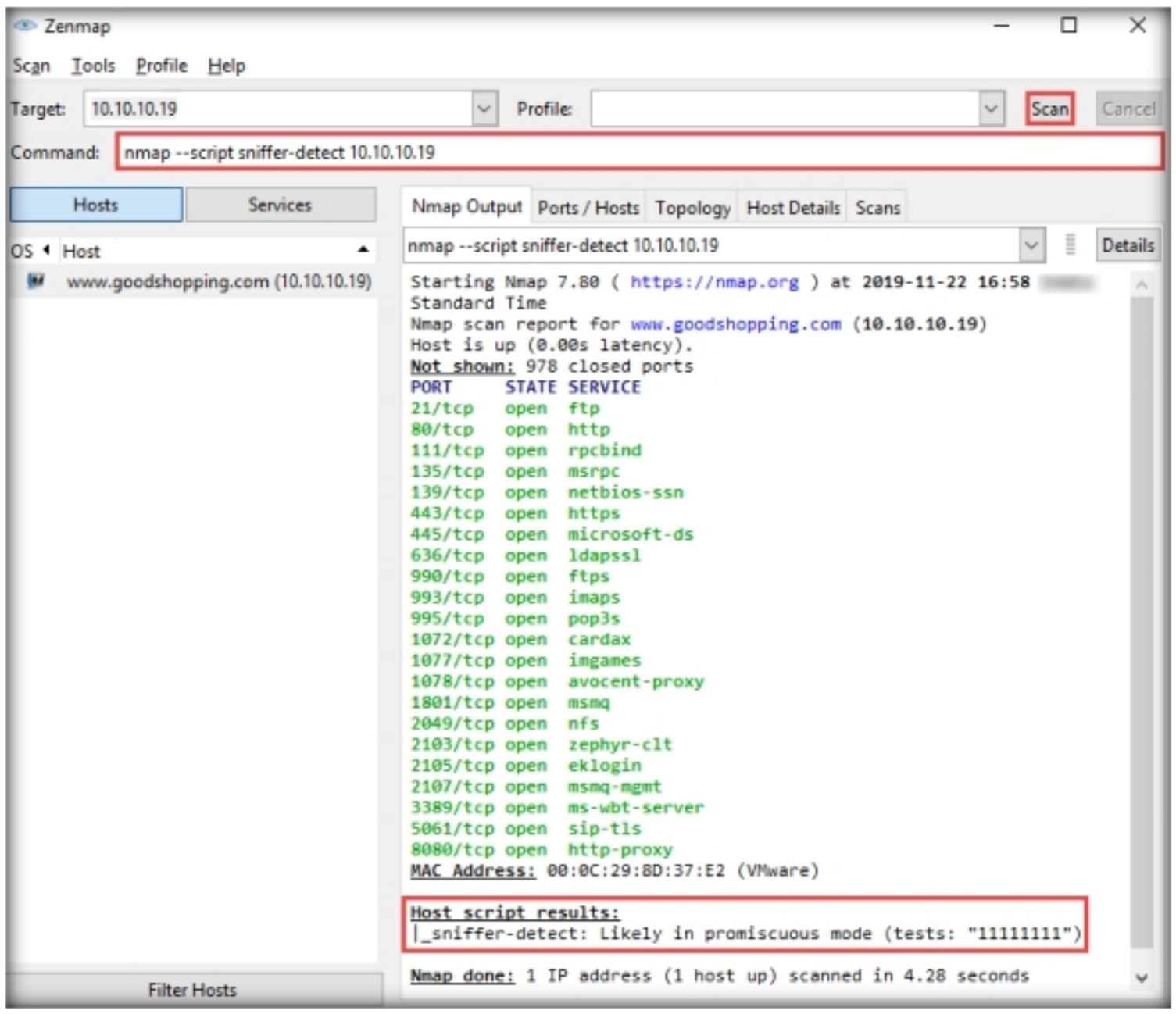


Figure 3.3.1: Zenmap scan results for promiscuous mode detection

TASK 3.2

Detect Promiscuous Mode Using NetScanTools Pro

5. Close the **Nmap** tool window and document all the acquired information.
6. Now, we shall perform promiscuous mode detection using NetScanTools Pro.
7. Double-click the **NetScanTools Pro Demo** shortcut on **Desktop** to launch **NetScanTools Pro**.
8. The **NetScanTools Pro** main window appears. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Promiscuous Mode Scanner** option.

Note: If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.
10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

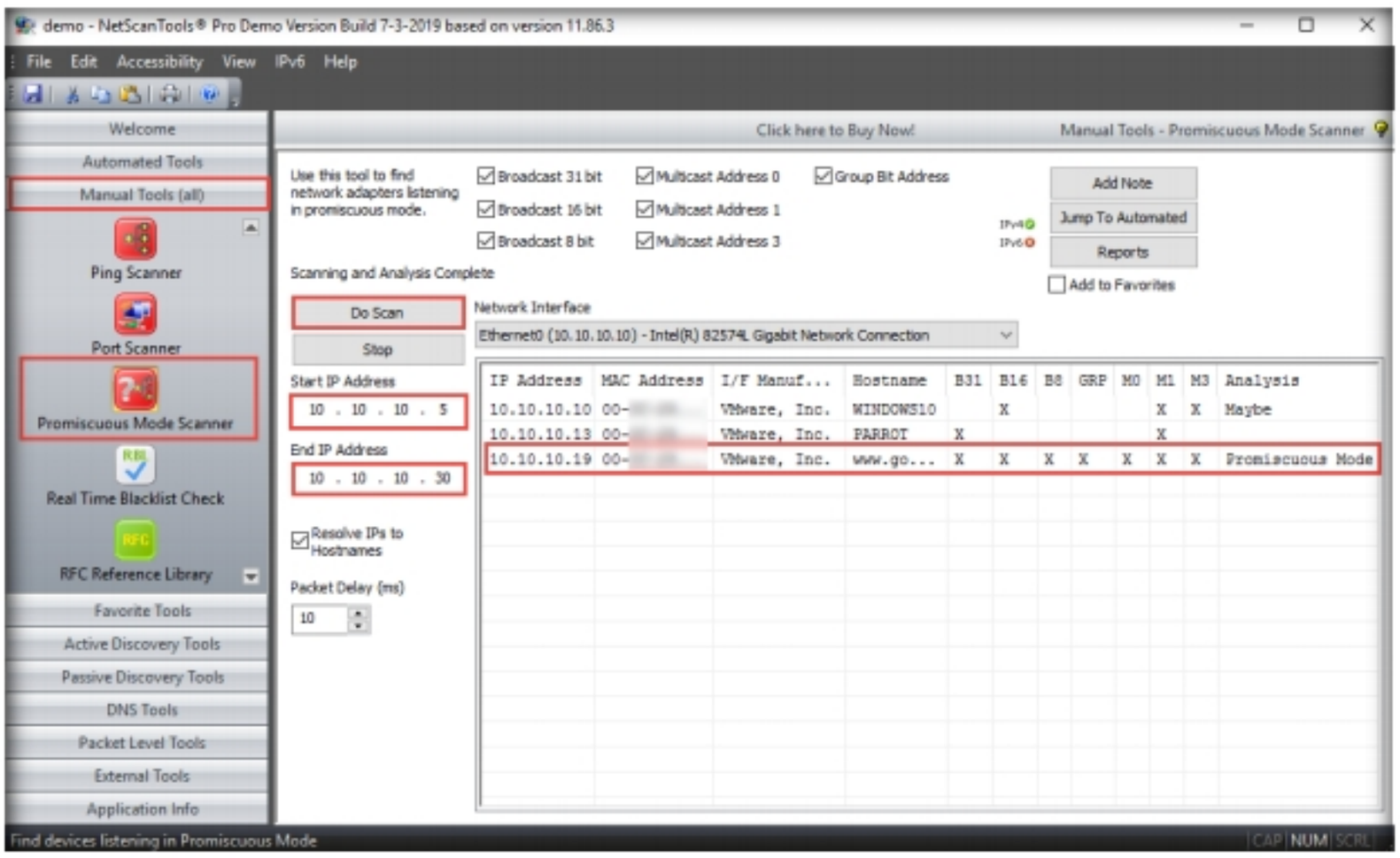


Figure 3.3.2: Zenmap scan results for promiscuous mode detection

11. This concludes the demonstration of detecting promiscuous mode using Nmap and NetScanTools Pro.
12. Close all open windows and document all the acquired information.
13. Turn off the **Windows 10**, **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs