

Your lab environment is being built
Your lab will be ready in about 40 seconds.
[Close Window](#)

1

[Close](#)

2

3

- Reconnect
- Power On
- Pause
- Resume
- Reset/Reboot
- Power Off
- Fit Window to Machine
- Fit Machine To Window
- Open in New Window
- Split Windows
- Revert Machine
- Reset Internet Gateway

4

- Ctrl+Alt+Delete
- ALT+Tab
- Windows Key

- Windows Key
- Windows Key + D
- Windows Key + E
- Windows Key + F
- Windows Key + M
- Windows Key + R
- Windows Key + X
- Windows Key + ...

- Windows Key
- Type Text

- Type Username
- Type Password
- Type Clipboard Text

- Virtual Keyboard

Windows 11⁵

Windows 11
Windows Server 2022
Windows Server 2019
Parrot Security
Ubuntu

Poor Connection

Full Screen
Power and Display
Keyboard
Machine Selection

This machine must be controlled outside of your browser via Remote Desktop.

Launch Remote Desktop

Username:

Password:

The selected machine is off.

Start

Machine is open in a separate window. [Close Window](#)

X

- Esc

- F1

- F2

- F3

- F4

- F5

- F6

- F7

- F8

- F9

- F10

- F11

- F12

- PrtSc

- ScrLk

- Pause

- `

- 1

- 2

- 3

- 4

- 5

- 6

- 7

- 8

- 9

- 0

- -

- =

- ← Backspace

- Insert

- Home
- P Up

- NLock

- /
- *
- -
- Tab
- q
- w
- e
- r
- t
- y
- u
- i
- o
- p
- [
-]
- \
- Delete
- End
- P Down

- 7

- 8
- 9
- +
- Caps
- a
- s
- d
- f
- g
- h
- j
- k
- l
- ;
- '
- ↲ Enter

- 4

- 5
- 6
- Shift
- z
- x
- c

- v
 - b
 - n
 - m
 - ,
 - .
 - /
 - Shift
 - ↑
 - 1
 - 2
 - 3
 - Enter
 - Ctrl
 - Win
 - Alt
 - Alt
 - Win
 - Ctrl
 - ←
 - ↓
 - →
- 0
 - .

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

6

Password

7

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

- Not Connected

Username

Password

Reconnect

Sniffing⁸

[Exit Lab](#)

Save Progress And Exit

End Lab

[Instructions](#)[Resources](#)

Module 08: Sniffing Scenario

Type Text

Type Text

Sniffing

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

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

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

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

Thus, an ethical hacker or pen tester needs to assess the security of the network's infrastructure, find the loopholes in the network using various network auditing tools, and patch them up to ensure a secure network environment.

The labs in this module provide real-time experience in performing packet sniffing on the target network using various packet sniffing techniques and tools.

Objective

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

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

Overview of Network Sniffing

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

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

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

Lab Tasks

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

1. Perform active sniffing
 - o Perform MAC flooding using macof
 - o Perform a DHCP starvation attack using Yersinia
2. Perform network sniffing using various sniffing tools
 - o Perform password sniffing using Wireshark
3. Detect network sniffing
 - o Detect ARP poisoning and promiscuous mode in a switch-based network

Lab 1: Perform Active Sniffing

Lab Scenario

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active

sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden.

An ethical hacker or pen tester needs to ensure that the organization's network is secure from various active sniffing attacks by analyzing incoming and outgoing packets for any attacks.

Lab Objectives

- Perform MAC flooding using macof
- Perform a DHCP starvation attack using Yersinia

Overview of Active Sniffing

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

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

Task 1: Perform MAC Flooding using macof

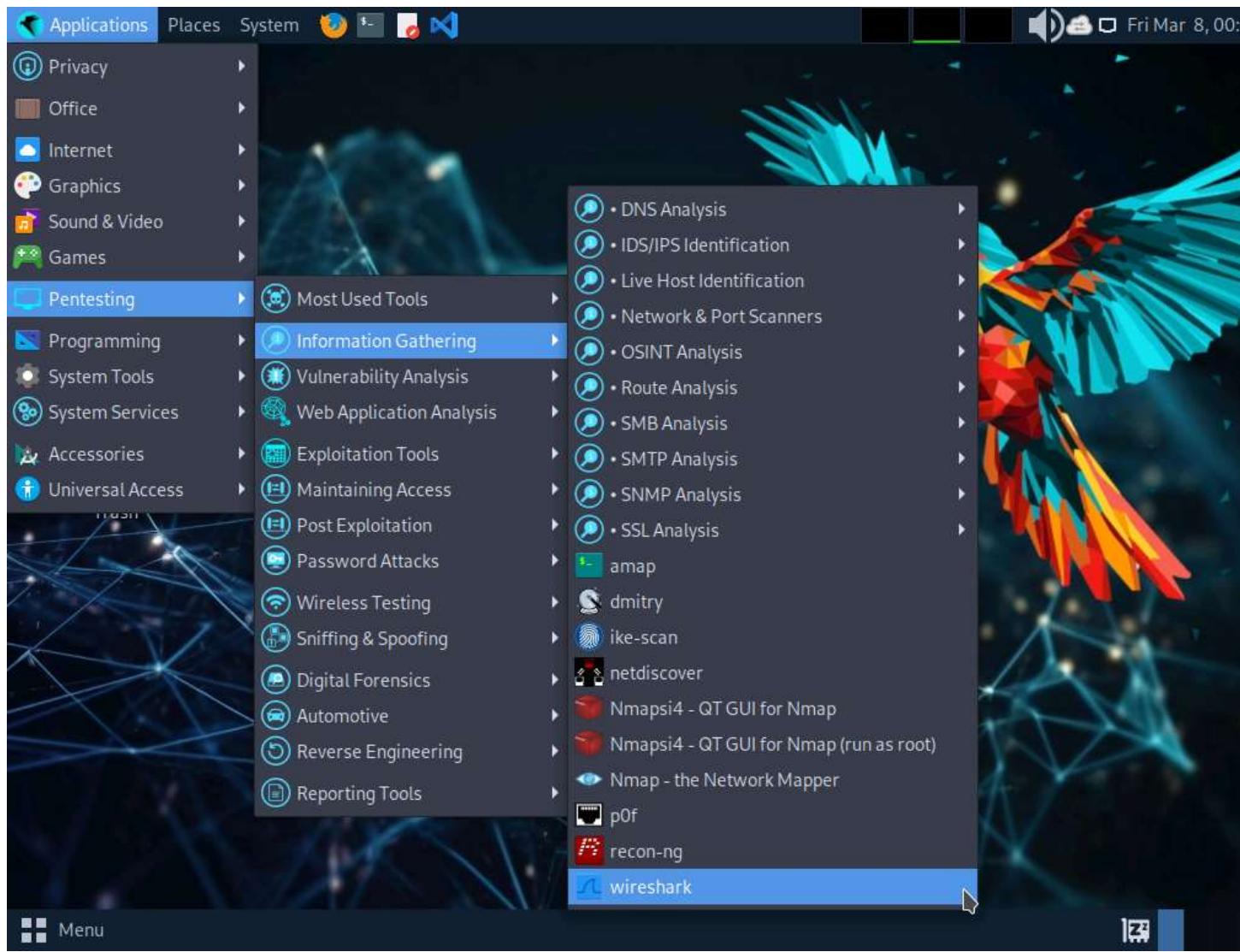
MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

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

1. By default Windows 11 machine selected, to launch **Parrot Security** machine, click [Parrot Security](#) and login with **attacker/toor**.
2. If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
3. If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
4. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting --> Information Gathering --> wireshark**.

5.



6. A security pop-up appears, authenticate by providing **toor** as a password.
7. **Wireshark Network Analyzer** window appears, start capturing the network traffic on the primary network interface (here, **eth0**).

8.

The screenshot shows the Wireshark application interface. At the top, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations like Open, Save, Print, and zoom. The main window displays a table of captured network frames. The columns are labeled: No., Time, Source, Destination, Protocol, Length, and Info. The table lists 18 frames, mostly NTP and ICMPv6 packets, with some MDNS and User Datagram Protocol entries. Frame 1 is highlighted in pink. The details pane at the bottom provides a detailed breakdown of Frame 1, including its bytes on wire and captured length, source and destination MAC addresses, protocol, port numbers, and a summary of the packet's content. The bottom status bar indicates "eth0: <live capture in progress>" and shows statistics: Packets: 63 · Displayed: 63 (100.0%).

9. Leave the **Wireshark** application running.
10. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
11. The password that you type will not be visible.
12. Now, run **cd** command to jump to the root directory.

13.

The screenshot shows a Parrot OS desktop environment. In the top right corner, there is a system tray with icons for battery, signal strength, and date/time (Fri Mar 8, 00:00). The main window is a terminal titled "cd - Parrot Terminal". The terminal window has a dark background with a green parrot logo watermark. It displays the following command-line session:

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~#
```

The desktop background features a dark, abstract geometric pattern. The taskbar at the bottom shows the "cd - Parrot Terminal" window is active. Other icons on the taskbar include "Menu", "[Capturing from eth0 (...]", and a file manager icon.

14. Execute **macof -i eth0 -n 10** in the root directory.
15. **-i**: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).
16. You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d**: Specifies the destination IP address).
17. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.

18.

```
Applications Places System Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~#cd
[root@parrot]~#macof -i eth0 -n 10
[root@parrot]~#
```

eth0: <live capture in progress>

Packets: 803 - Displayed: 803 (100.0%)

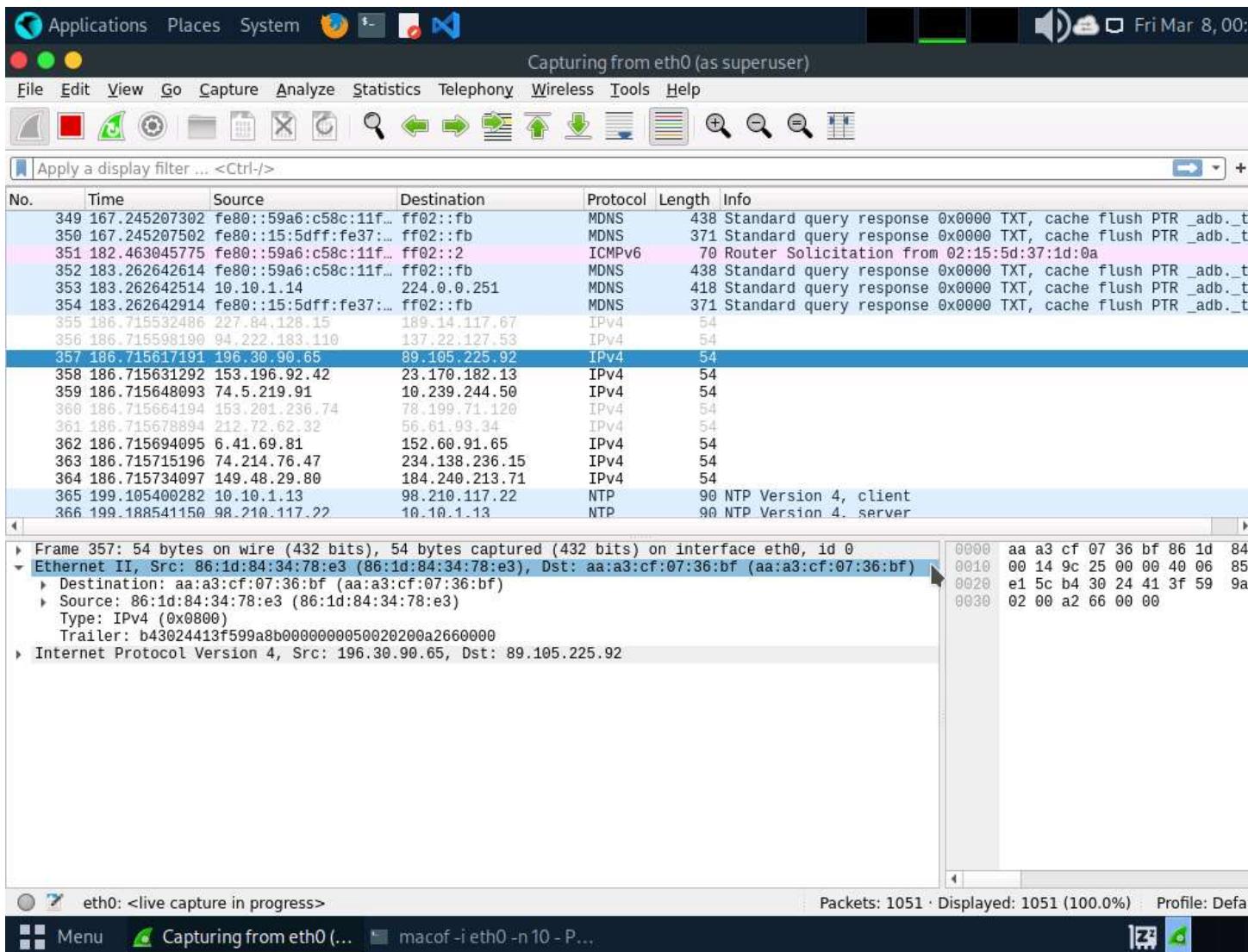
Profile: Default

Macof - i eth0 -n 10 - Parrot Terminal

Destination	Protocol	Length	Info
ff:ff:ff:ff:ff:ff	MDNS	438	standard query response 0x0000 TXT, cache flush PTR add
ff:ff:ff:ff:ff:ff	MDNS	371	standard query response 0x0002 TXT, cache flush PTR add
ff:ff:ff:ff:ff:ff	ICMPv6	79	Router Solicitation from 02:15:54:07:fd:8a
ff:ff:ff:ff:ff:ff	MDNS	438	standard query response 0x0003 TXT, cache flush PTR add
ff:ff:ff:ff:ff:ff	MDNS	371	standard query response 0x0004 TXT, cache flush PTR add

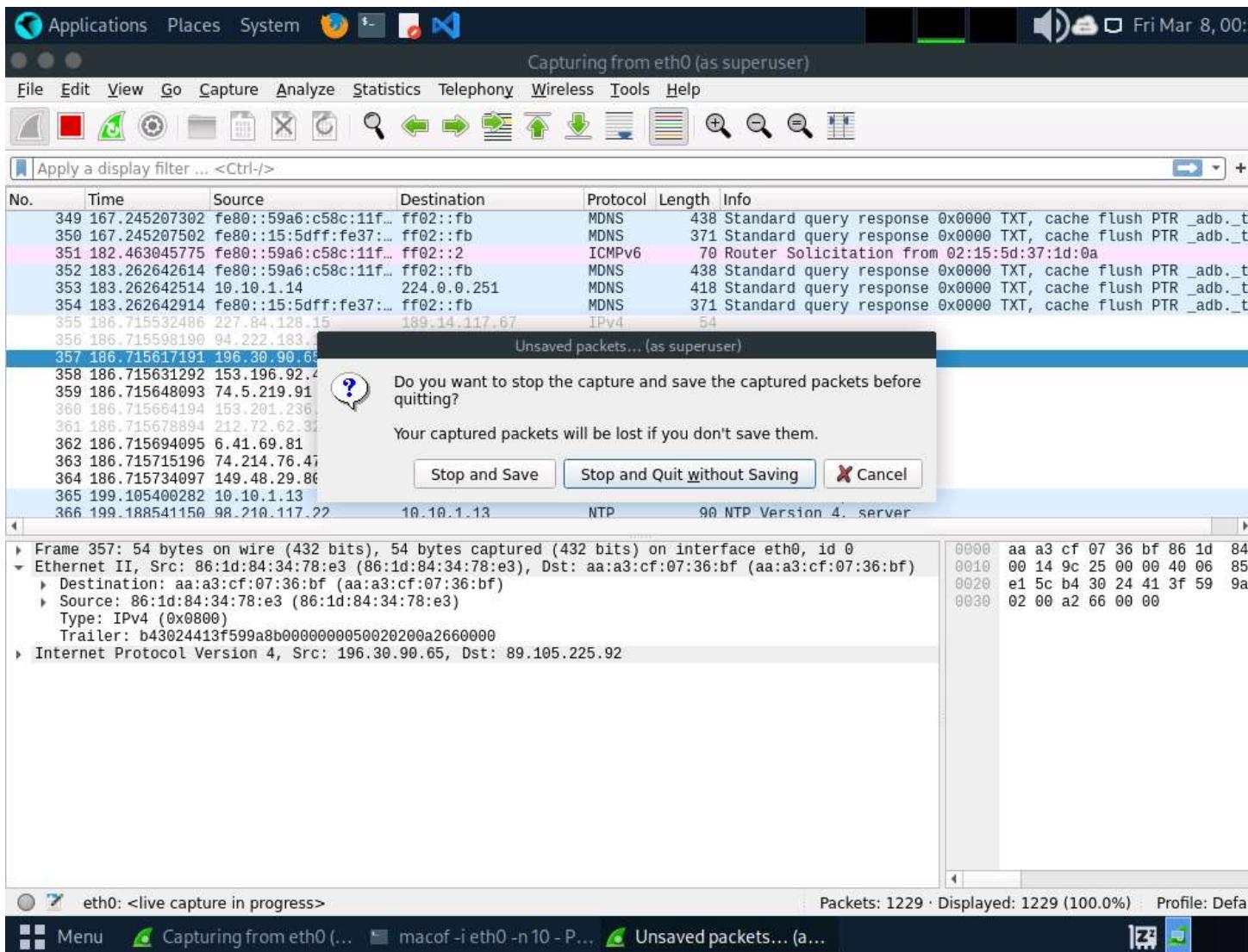
19. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses.
20. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section.
Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.

21.



22. Similarly, you can switch to a different machine to see the same packets that were captured by Wireshark in the **Parrot Security** machine.
23. 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.
24. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application.

25.



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

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

Question 8.1.1.1

Use macof on the Parrot Security machine to perform MAC flooding on the Windows 11 target machine. What is the default size of the IP packets that macof uses to flood the CAM table with random MAC addresses?

Score

Task 2: Perform a DHCP Starvation Attack using Yersinia

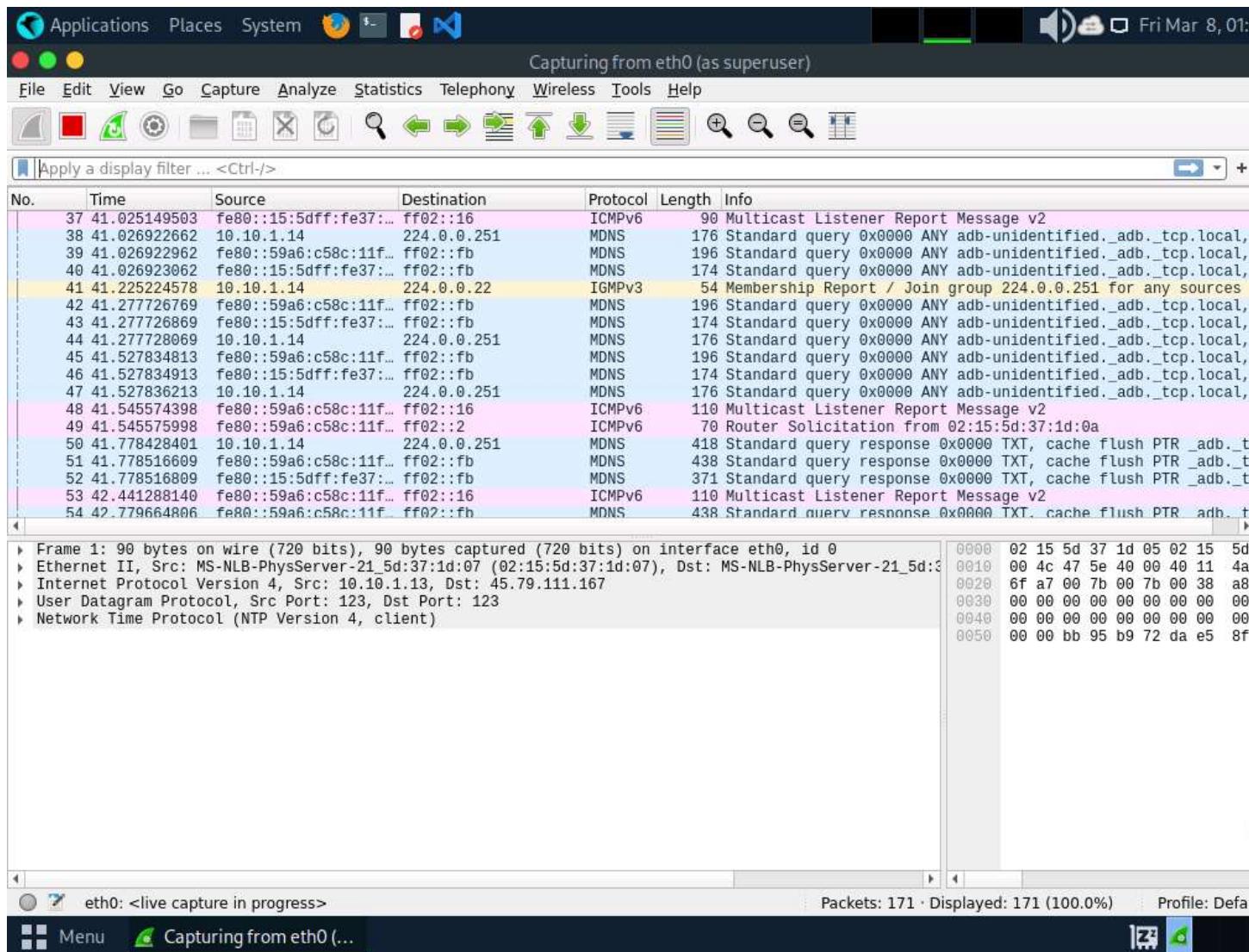
In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue,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

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

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

1. In Parrot Security machine, launch **Wireshark** and start packet capturing on available ethernet or interface (here,**eth0**).

2.



3. Leave the **Wireshark** application running.
4. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**). Run **cd** to navigate to the root directory.
5. Click the **Maximize Window** icon to maximize the terminal window.
6. The interactive mode of the Yersinia application only works in a maximized terminal window.
7. Run **yersinia -I** to open Yersinia in interactive mode.
8. **-I:** Starts an interactive session.

9.

The screenshot shows a Parrot OS desktop environment. In the top right corner, there is a system tray icon for capturing from eth0. The main window is a terminal titled "cd - Parrot Terminal". The terminal output is as follows:

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

The desktop background features a dark, abstract network-like pattern. The taskbar at the bottom shows the "Menu" button, a notification for "Capturing from eth0 (...)", and the "cd - Parrot Terminal" window.

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

13.

The screenshot shows a terminal window titled "yersinia -l - Parrot Terminal". The window displays the Yersinia 0.8.2 help screen. The help menu includes the following commands:

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

Below the help menu, there is a section for "STP Fields" which lists:

- Source MAC 0A:23:1
- Id 0000 Ver 00 Typ
- BridgeId CB09.E7CD

On the right side of the terminal window, there is a status bar with the text "[02:01:49]" and a section labeled "AC Spoofing [X]" containing the values "00", "hcost 00000000", and "0002 Fwd 000F".

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.

16.

```
yersinia 0.8.2 by Slay & tomac - DHCP mode [02:03:46]
SIP          DIP          MessageType      Iface Last seen
Total Packets: 0   DHCP Packets: 0   MAC Spoofing [X]

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

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

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

19.

```
yersinia 0.8.2 by Slay & tomac - DHCP mode [02:03:55]
File Edit View Search Terminal Help
yersinia -l - Parrot Terminal
yersinia 0.8.2 by Slay & tomac - DHCP mode
SIP          DIP          MessageType        Iface Last seen
[Attack Panel]
No  DoS  Description
0   sending RAW packet
1   X    sending DISCOVER packet
2   creating DHCP rogue server
3   X    sending RELEASE packet
[Total Packets]
[Those strange attacks...]
[DHCP Fields]
Source MAC 02
Select attack to launch ('q' to quit)
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
```

20. **Yersinia** starts sending DHCP packets to the network interface as shown in the screenshot.

21.

```
yersinia 0.8.2 by Slay & tomac - DHCP mode [02:04:55]
  SIP           DIP           MessageType      Iface Last seen
  0.0.0.0       255.255.255.255 DISCOVER      eth0   08 Mar 02:04:55
  0.0.0.0       255.255.255.255 DISCOVER      eth0   08 Mar 02:04:55

Total Packets: 3306566 — DHCP Packets: 3306566 — MAC Spoofing [X]

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

Menu [Capturing from eth0 (...)] yersinia -l - Parrot Ter... [Icons]

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

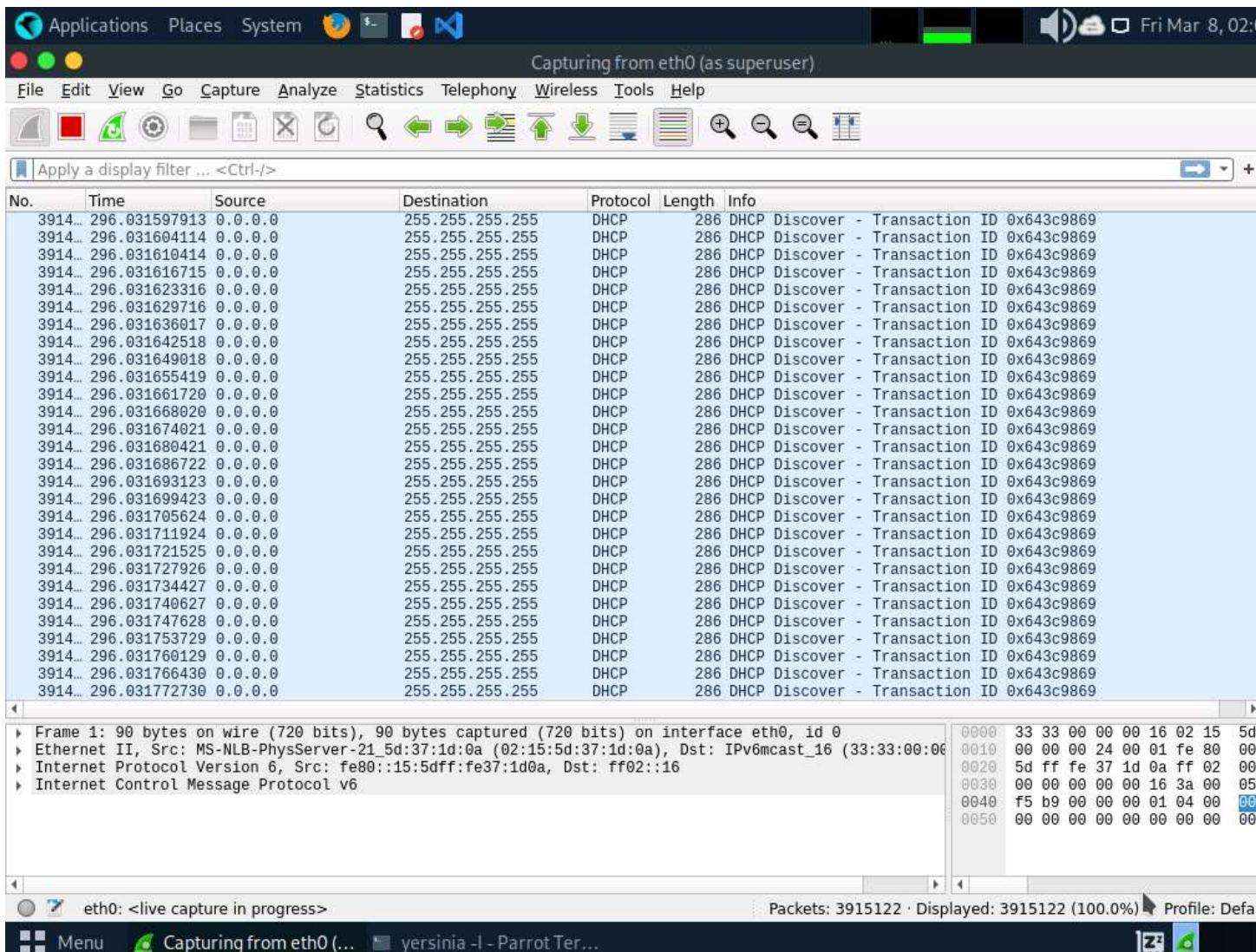
23.

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

MOTD: Snowboard on the winter, MBK on the summer :)
[root@parrot]~$ #
```

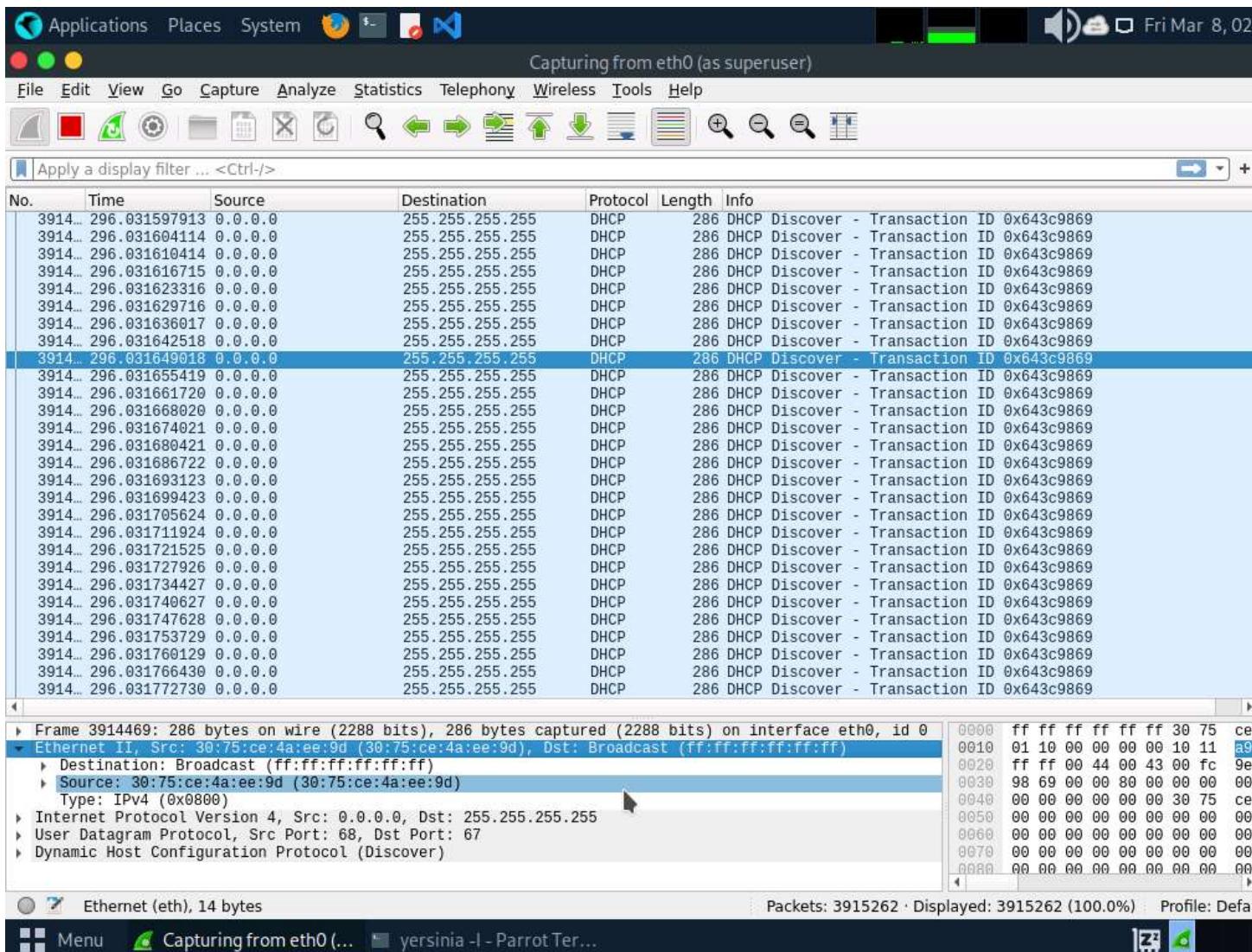
24. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.

25.



26. 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.

27.



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

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

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

Question 8.1.2.1

Use Yersinia on the Parrot Security machine to perform a DHCP starvation attack. What is the default source port used by Yersinia in the DHCP mode?

Score

Lab 2: Perform Network Sniffing using Various Sniffing Tools

Lab Scenario

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

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can only capture data packets from within a given subnet, which means that it

cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises leave their switch ports open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

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

Lab Objectives

- Perform password sniffing using Wireshark

Overview of Network Sniffing Tools

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

Task 1: Perform Password Sniffing using Wireshark

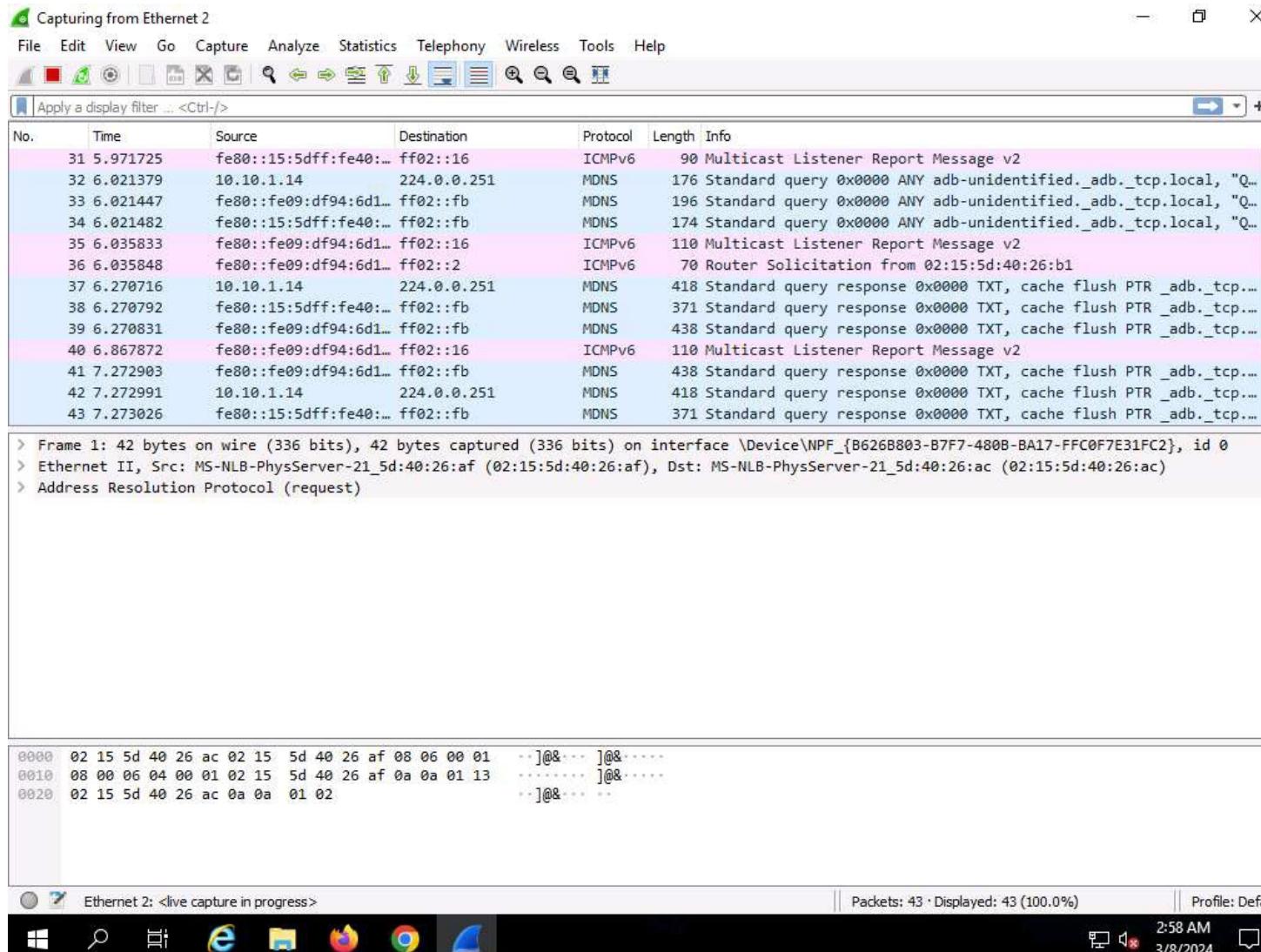
Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. The captured files can be programmatically edited via the command-line. A set of filters for customized data displays can be refined using a display filter.

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

In this task, we will use the **Windows Server 2019 (10.10.1.19)** machine as the host machine and the **Windows 11 (10.10.1.11)** machine as the target machine.

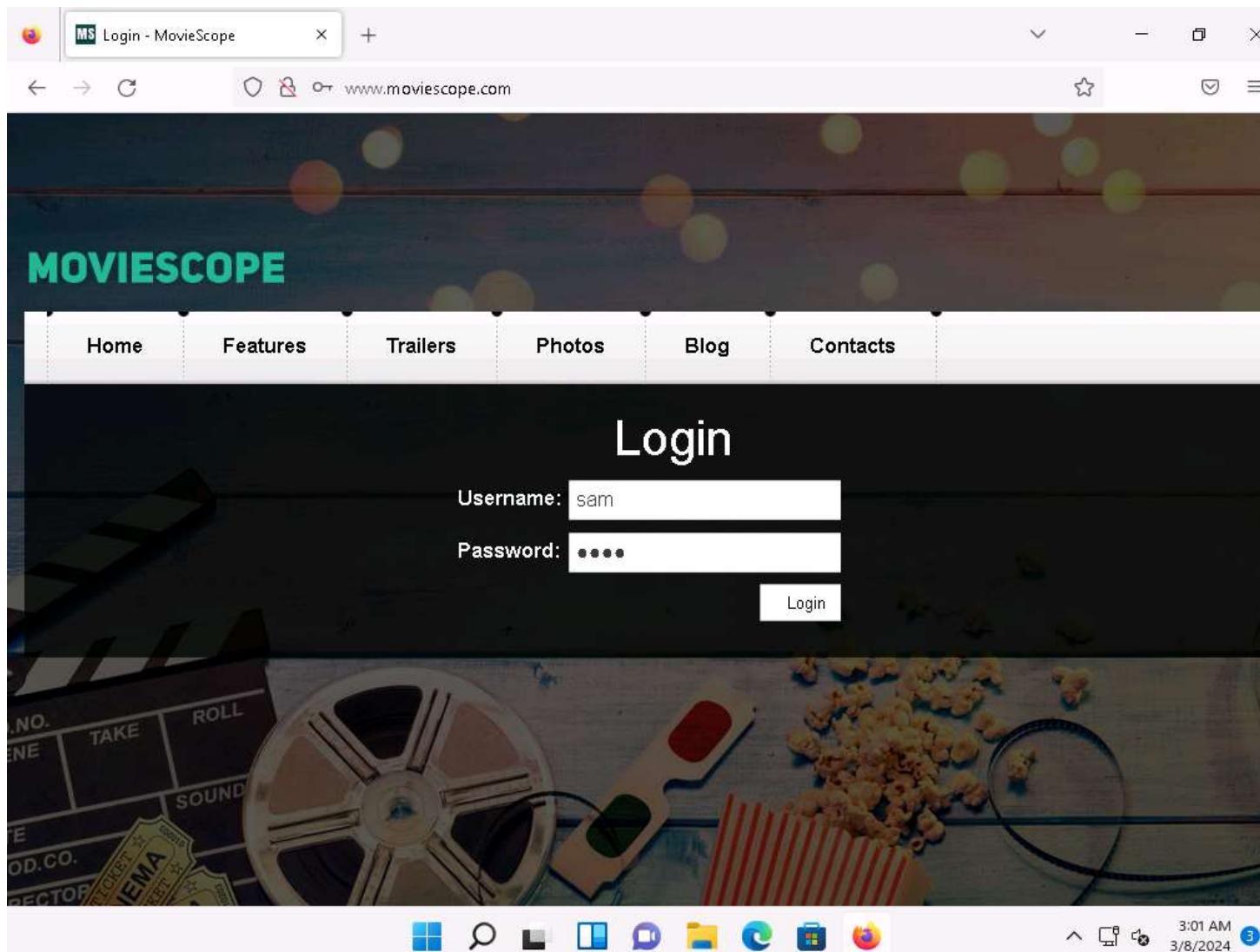
1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine and login with **Administrator/Pa\$\$w0rd**.
2. Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Search **Wireshark** from search bar and launch it.
4. If the **Software update** window appears, click **Remind me later**.
5. The **Wireshark Network Analyzer** window appears, start capturing the network traffic on the primary network interface (here, **Ethernet 2**).
6. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.

7.



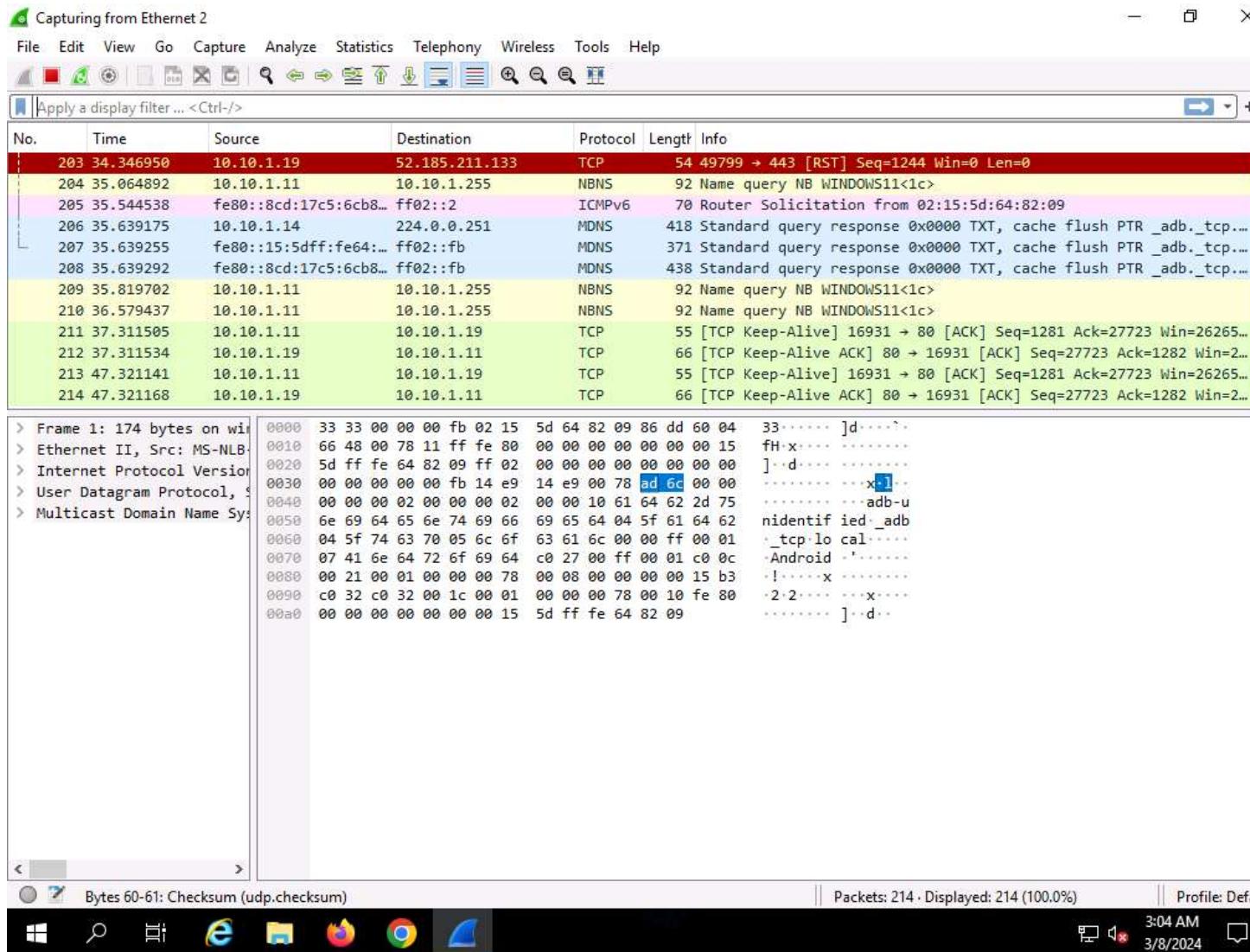
8. Now, click [Windows 11](#) to switch to the **Windows 11** machine, login using **Admin/Pa\$\$w0rd**.
9. Alternatively, you can also click **Pa\$\$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.
- [10. more...](#)
11. If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.
12. Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
13. Open any web browser, and go to <http://www.moviescope.com/> (here, we are using **Mozilla Firefox**).
14. The **MOVIESCOPE** home page appears; login using **sam/test**.

15.



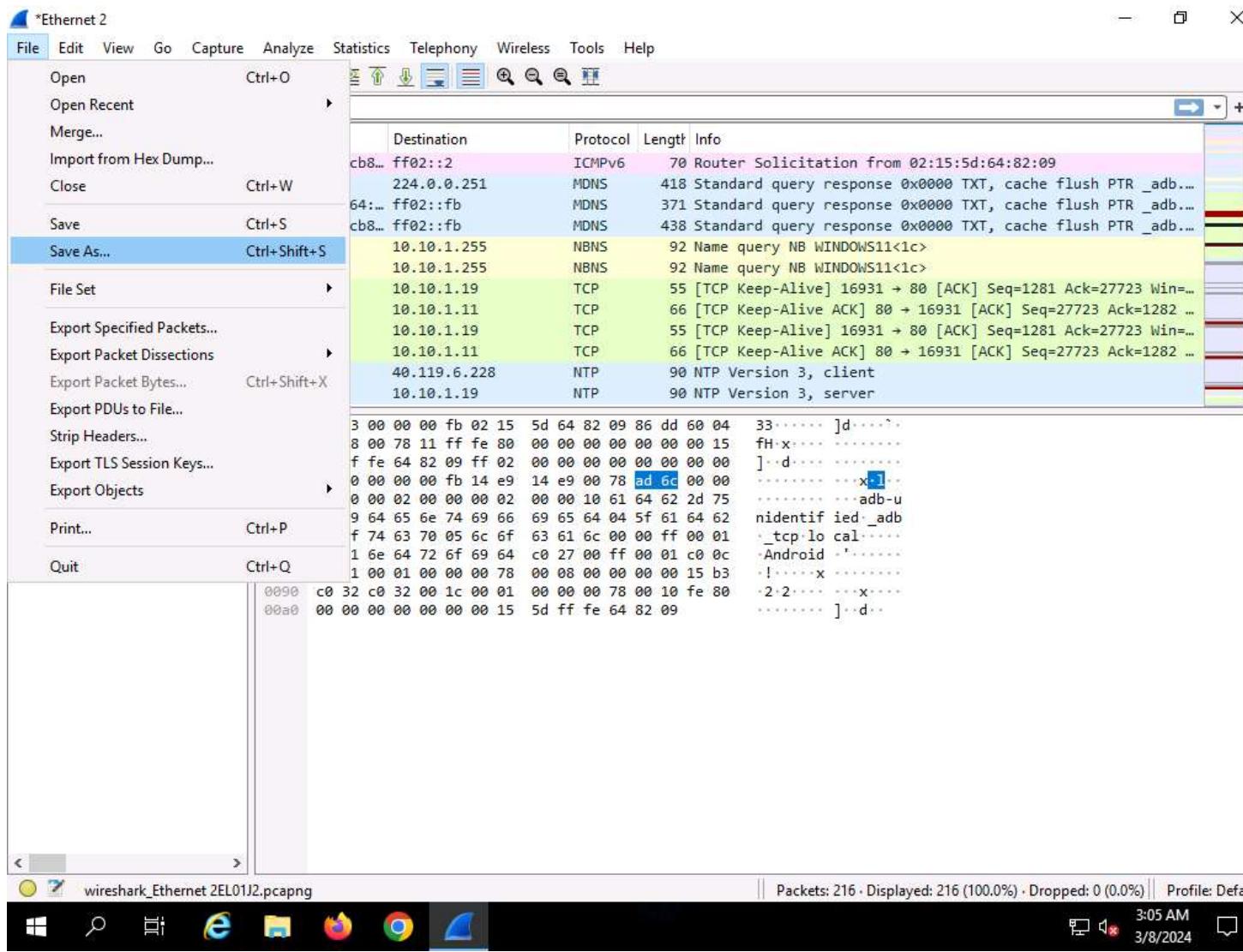
16. Click [Windows Server 2019](#) to switch back to **Windows Server 2019** machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.

17.



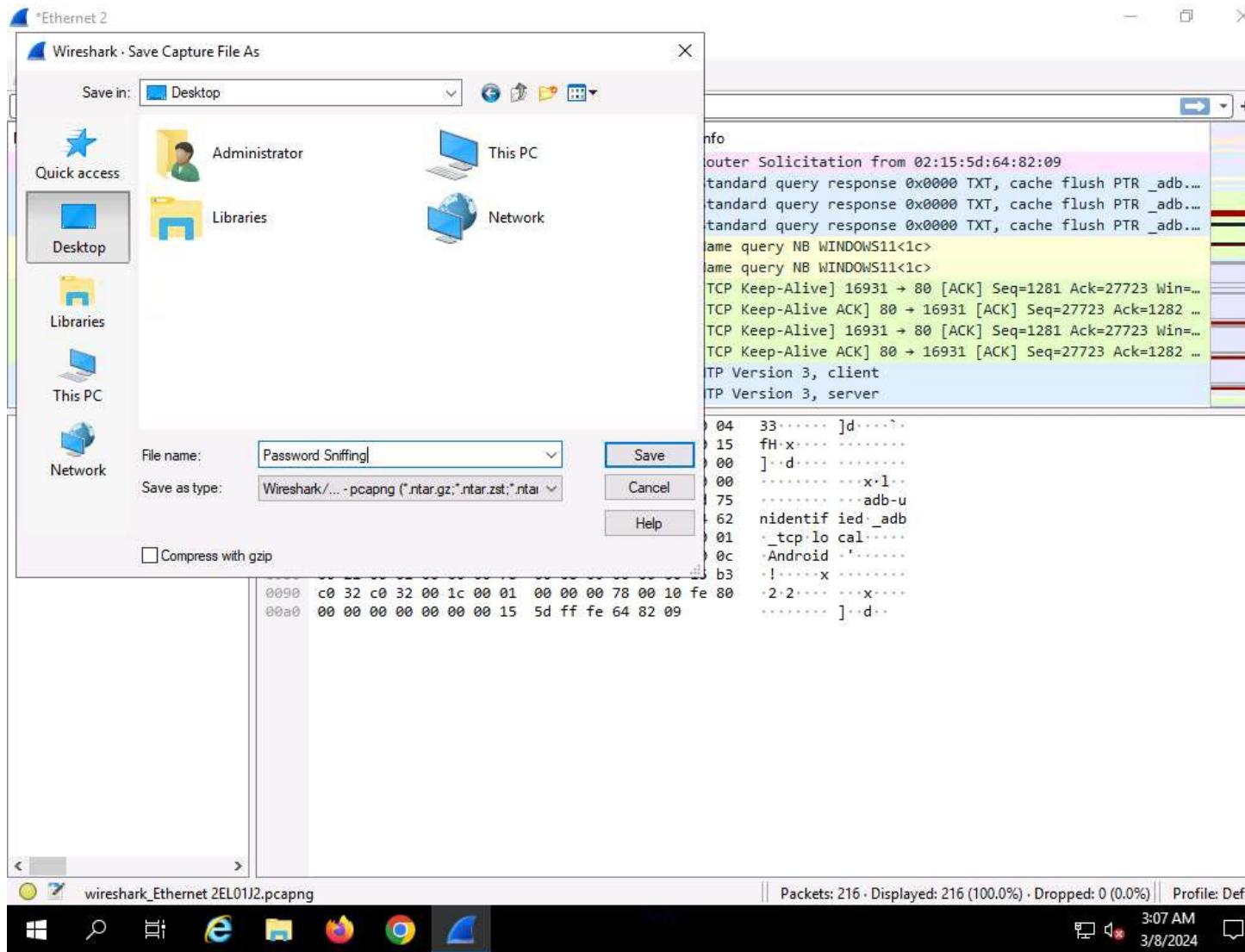
18. Click **File --> Save As...** from the top-left corner of the window to save the captured packets.

19.



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

21.



22. In the **Apply a display filter field**, type **http.request.method == POST** and click the arrow icon (=>) to apply the filter.
23. Applying this syntax helps you narrow down the search for http POST traffic.
24. Wireshark only filters **http POST** traffic packets, as shown in the screenshot.

25.

Wireshark Screenshot:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method==POST

No.	Time	Source	Destination	Protocol	Length	Info
77	26.725616	10.10.1.19	23.36.70.120	HTTP/X...	1298	POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1
90	26.815821	10.10.1.19	138.91.171.81	HTTP/X...	1298	POST /metadata.svc HTTP/1.1
98	27.284659	10.10.1.11	10.10.1.19	HTTP	894	POST / HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 77: 1298 bytes on wire (10384 bits), 1298 bytes captured (10384 bits) on
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:64:82:07 (02:15:5d:64:82:07), Dst: MS
> Internet Protocol Version 4, Src: 10.10.1.19, Dst: 23.36.70.120
> Transmission Control Protocol, Src Port: 49794, Dst Port: 80, Seq: 347, Ack: 1
> [2 Reassembled TCP Segments (1590 bytes): #76(346), #77(1244)]
> Hypertext Transfer Protocol
> eXtensible Markup Language

0030 04 02 6d af 00 00 ff fe 3c 00 3f 00 78 00 6d 00
0040 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00
0050 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00
0060 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00
0070 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00
0080 22 00 3f 00 3e 00 3c 00 73 00 3a 00 45 00 6e 00
0090 76 00 65 00 6c 00 6f 00 70 00 65 00 20 00 78 00
00a0 6d 00 6c 00 6e 00 73 00 3a 00 73 00 3d 00 22 00
00b0 68 00 74 00 74 00 70 00 3a 00 2f 00 2f 00 73 00
00c0 63 00 68 00 65 00 6d 00 61 00 73 00 2e 00 78 00
00d0 6d 00 6c 00 73 00 6f 00 61 00 70 00 2e 00 6f 00
00e0 72 00 67 00 2f 00 73 00 6f 00 61 00 70 00 2f 00
00f0 65 00 6e 00 76 00 65 00 6c 00 6f 00 70 00 65 00
0100 2f 00 22 00 3e 00 3c 00 73 00 3a 00 48 00 65 00
0110 61 00 64 00 65 00 72 00 3e 00 3c 00 68 00 3a 00
0120 63 00 64 00 20 00 78 00 6d 00 6c 00 6e 00 73 00
0130 3a 00 68 00 3d 00 22 00 68 00 74 00 74 00 70 00
0140 3a 00 2f 00 2f 00 73 00 63 00 68 00 65 00 6d 00
0150 61 00 73 00 2e 00 6d 00 69 00 63 00 72 00 6f 00
0160 73 00 6f 00 66 00 74 00 2e 00 63 00 6f 00 6d 00
0170 2f 00 77 00 69 00 6e 00 64 00 6f 00 77 00 73 00
0180 6d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00

Frame (1298 bytes) Reassembled TCP (1590 bytes) Decoded UTF-16LE

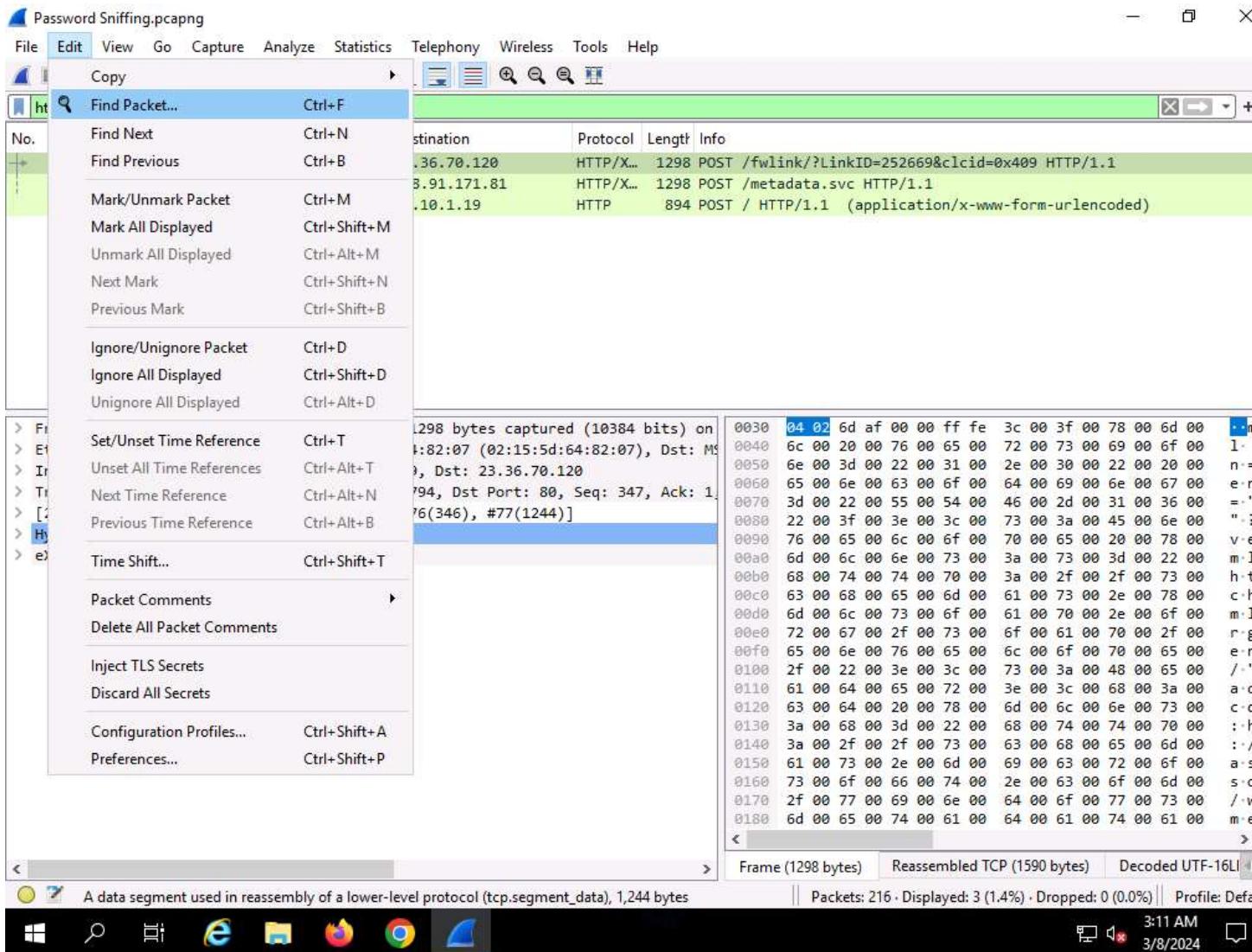
A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1,244 bytes

Packets: 216 · Displayed: 3 (1.4%) · Dropped: 0 (0.0%) · Profile: Default

3:10 AM 3/8/2024

26. Now, navigate to **Edit --> Find Packet** from menu bar.

27.



28. The **Find Packet** section appears below the display filter field.
29. Click **Display filter**, select **String** from the drop-down options, click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options and click **Packet list**, select **Packet details** from the drop-down options.
30. In the field next to **String**, type **pwd** and click the **Find** button.

31.

The screenshot shows the Wireshark interface with the following details:

- File menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Search Bar:** Shows the search string "pwd".
- Table Headers:** No., Time (3), Source (2), Destination, Proto (1), Length, Info (4).
- Table Data:** Three rows of network traffic. Row 1: 77 26.725616, 10.10.1.19, 23.36.70.120, HTTP/X..., 1298 POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1. Row 2: 90 26.815821, 10.10.1.19, 138.91.171.81, HTTP/X..., 1298 POST /metadata.svc HTTP/1.1. Row 3: 98 27.284659, 10.10.1.11, 10.10.1.19, HTTP, 894 POST / HTTP/1.1 (application/x-www-form-urlencoded).
- Packet Details:** A large pane showing the raw bytes of the selected packet (Frame 77) in hex, ASCII, and EBCDIC formats.
- Selected Hex Dump:** The bytes 0030 04 02 6d af 00 00 ff fe 3c 00 3f 00 78 00 6d 00 are highlighted in blue.
- Selected ASCII Dump:** The ASCII representation of the highlighted bytes: "40 26 725616 10.10.1.19 23.36.70.120 HTTP/X... 1298 POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1".
- Selected EBCDIC Dump:** The EBCDIC representation of the highlighted bytes: "40 26 725616 10.10.1.19 23.36.70.120 HTTP/X... 1298 POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1".
- Bottom Status Bar:** Frame (1298 bytes), Reassembled TCP (1590 bytes), Decoded UTF-16LE, Packets: 216 · Displayed: 3 (1.4%) · Dropped: 0 (0.0%), Profile: Default, 3:14 AM, 3/8/2024.

32. Wireshark will now display the sniffed password from the captured packets.
33. 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.

34.

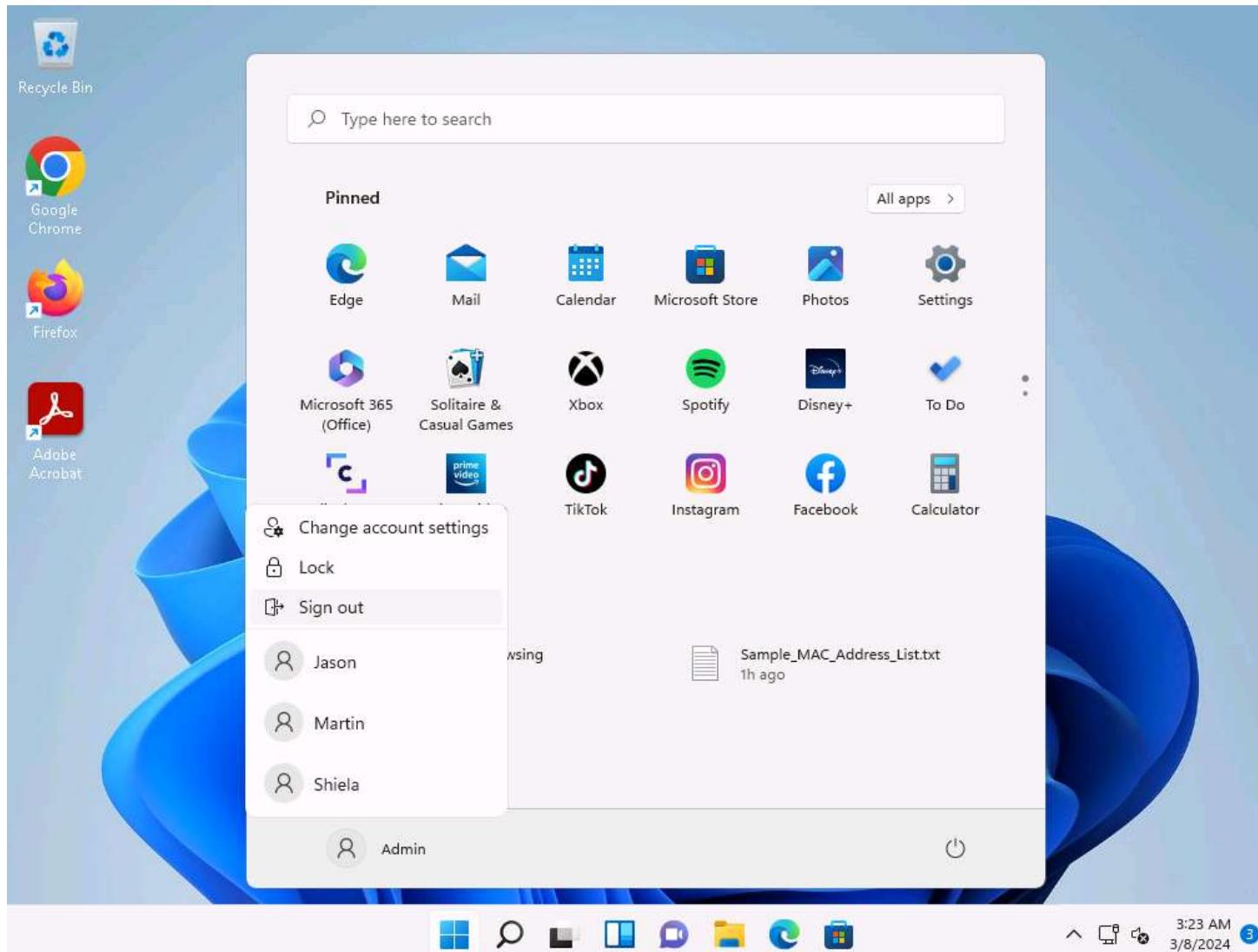
The screenshot shows the Wireshark interface with the following details:

- File menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Search Bar:** http.request.method==POST
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info.
- Table Data:** Three rows of network traffic:
 - No. 77: 26.725616, Source 10.10.1.19, Destination 23.36.70.120, HTTP/X..., Length 1298, Info: POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1
 - No. 90: 26.815821, Source 10.10.1.19, Destination 138.91.171.81, HTTP/X..., Length 1298, Info: POST /metadata.svc HTTP/1.1
 - No. 98: 27.284659, Source 10.10.1.11, Destination 10.10.1.19, HTTP, Length 894, Info: POST / HTTP/1.1 (application/x-www-form-urlencoded)
- Packet Details View:** Shows the structure of the selected packet (Frame 98).
 - Frame 98: 894 bytes on wire (7152 bits), 894 bytes captured (7152 bits) on interface \Device\NPF_{B6268803-B7F7-480B}
 - Ethernet II, Src: Microsoft_01:80:00 (00:15:5d:01:80:00), Dst: MS-NLB-PhysServer-21_5d:64:82:07 (02:15:5d:64:82:07)
 - Internet Protocol Version 4, Src: 10.10.1.11, Dst: 10.10.1.19
 - Transmission Control Protocol, Src Port: 16931, Dst Port: 80, Seq: 1, Ack: 1, Len: 840
 - Hypertext Transfer Protocol**
 - HTML Form URL Encoded: application/x-www-form-urlencoded**
 - Form item: "__VIEWSTATE" = "/wEPDwULLTE3Mdc5MjQzOTdkZH5l0cnJ+BtsUZt5M/WlqLFqT5uNaq6G+46A4bz6/sM1"
 - Form item: "__VIEWSTATEGENERATOR" = "C2EE9ABB"
 - Form item: "__EVENTVALIDATION" = "/wEdAARJUub9rbp0xjNNNjxtMliRWMtrRuIi9aE3DBG1DcnOGGcP002LAX9axRe6vMQj2F3f3AwSKu"
 - Form item: "txtusername" = "sam" (highlighted with a red box)
 - Form item: "txtpwd" = "test" (highlighted with a red box)
 - Form item: "btnlogin" = "Login"
- Bottom Status Bar:** Hypertext Transfer Protocol (http), 516 bytes | Packets: 216 · Displayed: 3 (1.4%) · Dropped: 0 (0.0%) | Profile: Default | 3:21 AM | 3/8/2024

35. Close the **Wireshark** window.

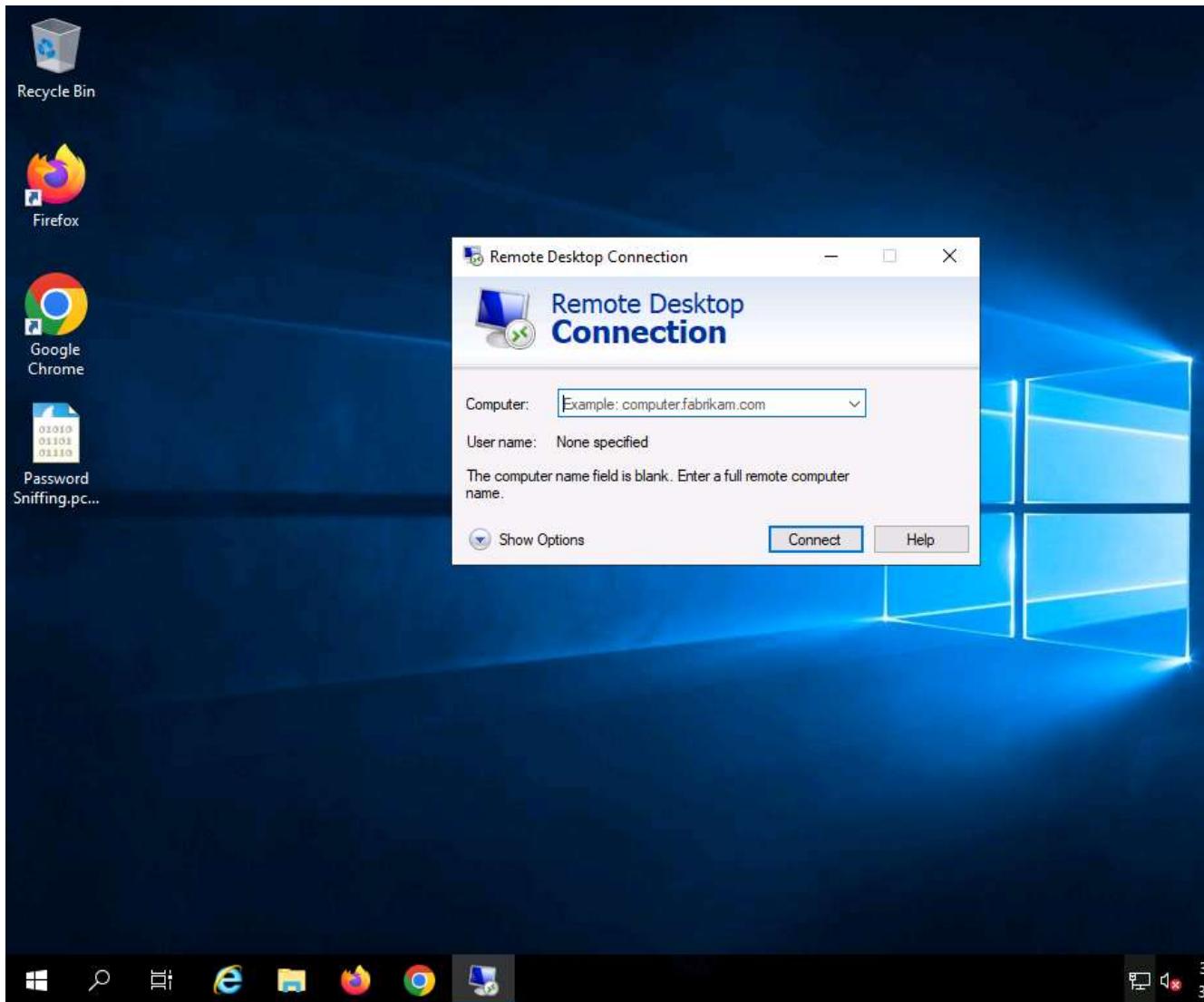
36. Click [Windows 11](#) to switch to the **Windows 11** machine, close the web browser, and sign out from the **Admin** account.

37.



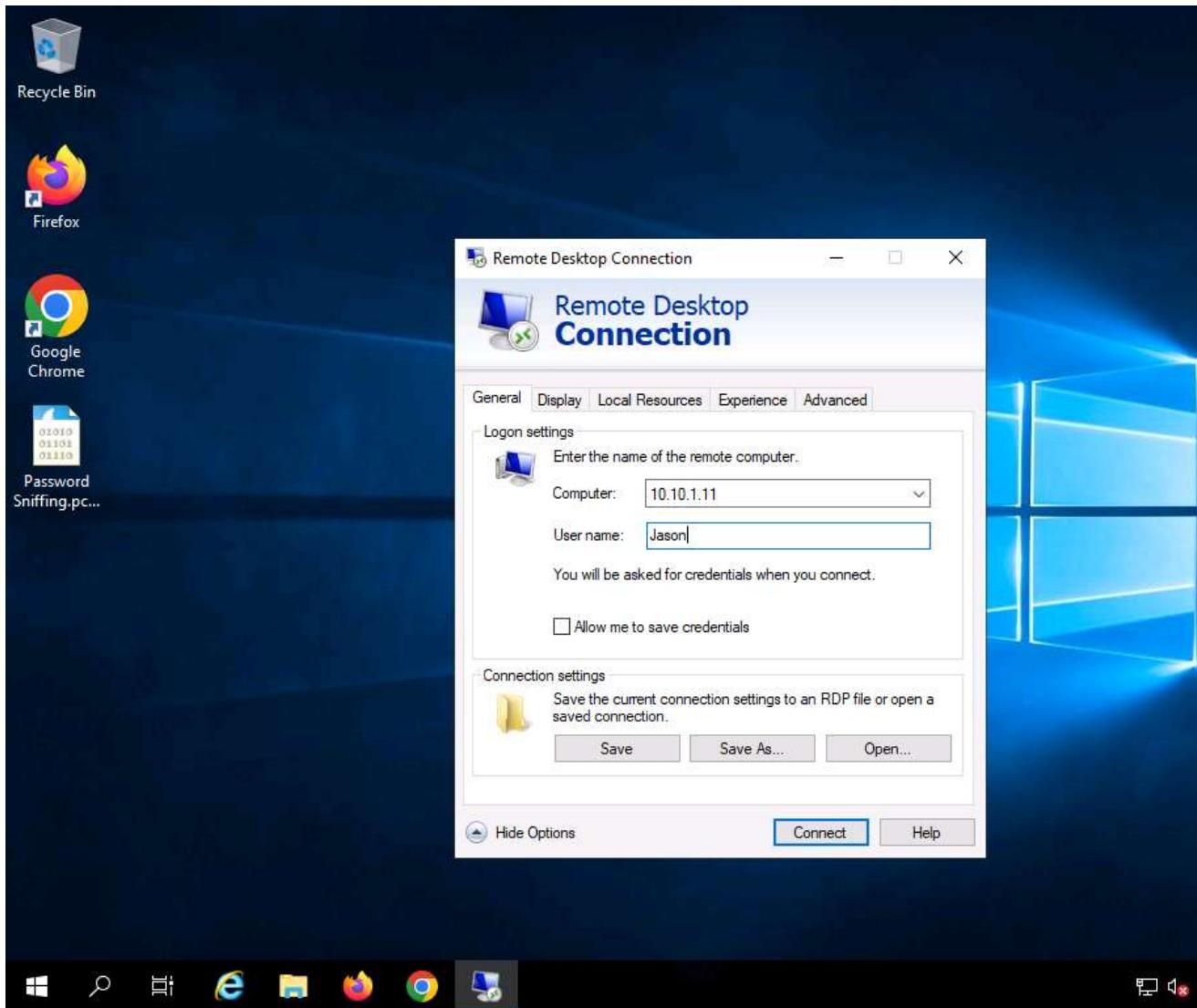
38. Click [Windows Server 2019](#) to switch back to the **Windows Server 2019** machine.
39. Search **Remote Desktop Connection** from search bar and launch it.
40. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.
41. If some previously accessed IP address appears in the **Computer** field, delete it.

42.



43. The dialog-box expands; under the **General** tab, type **10.10.1.11** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.
44. 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.

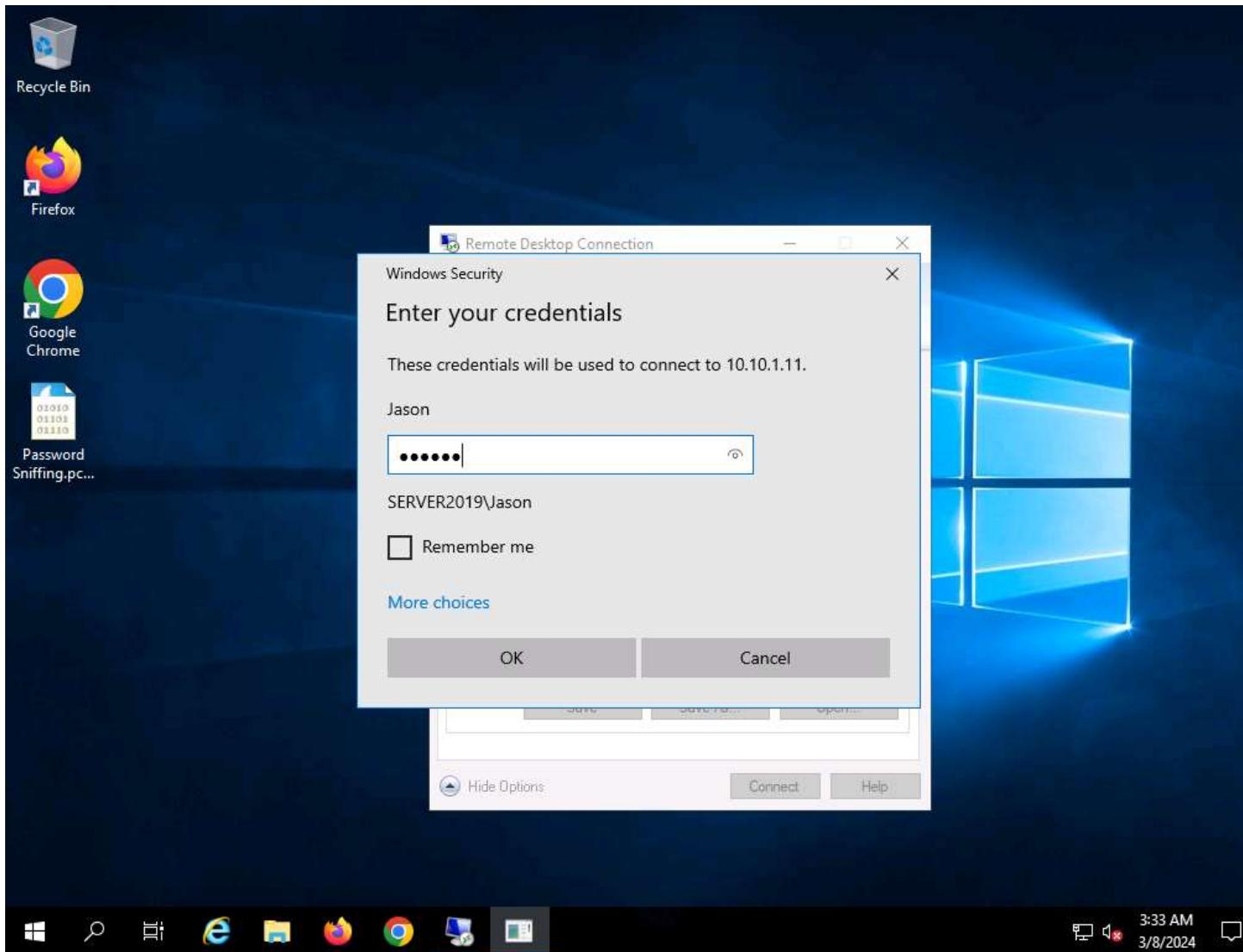
45.



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

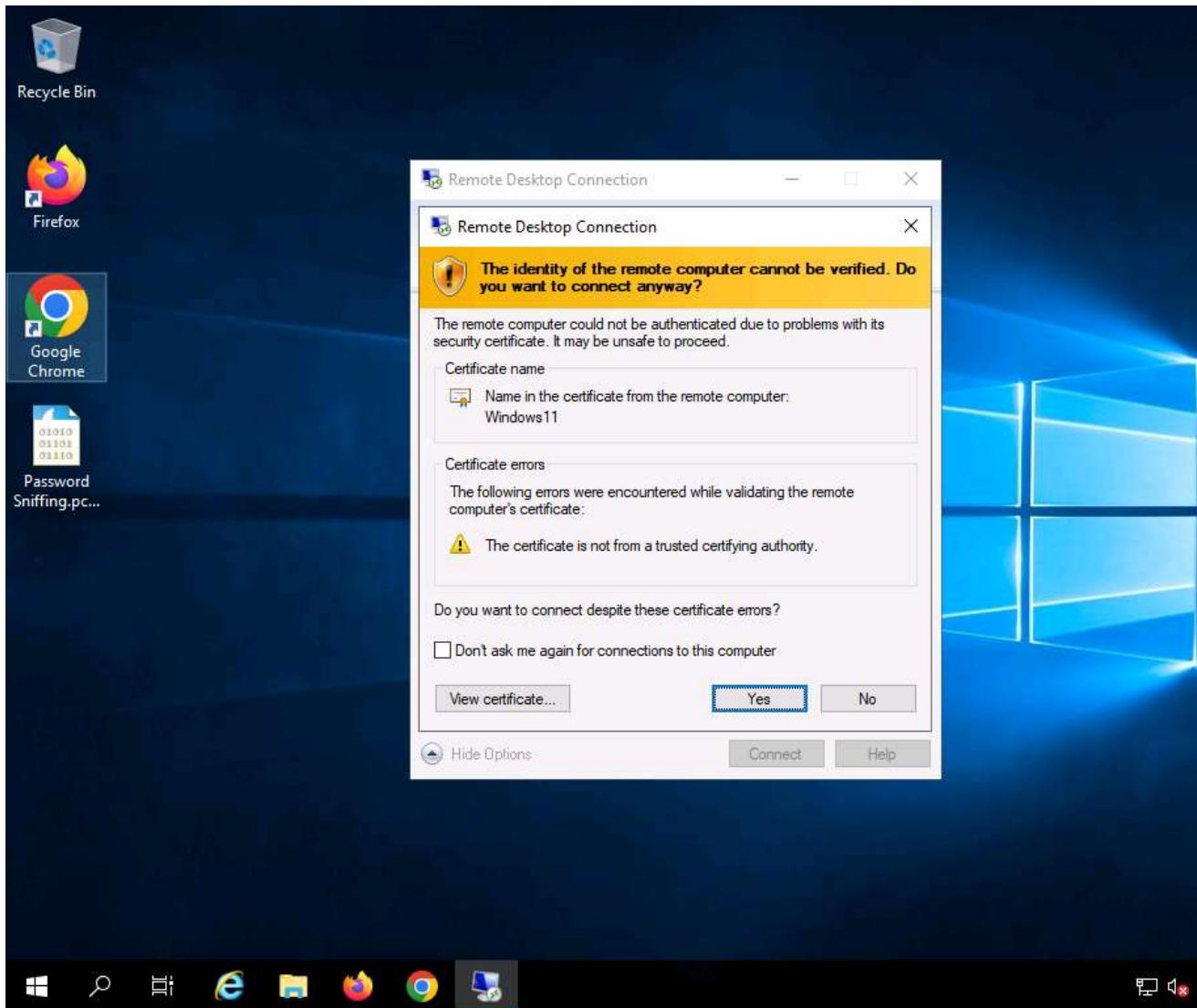
47. If **Remember me** option is checked uncheck it.

48.



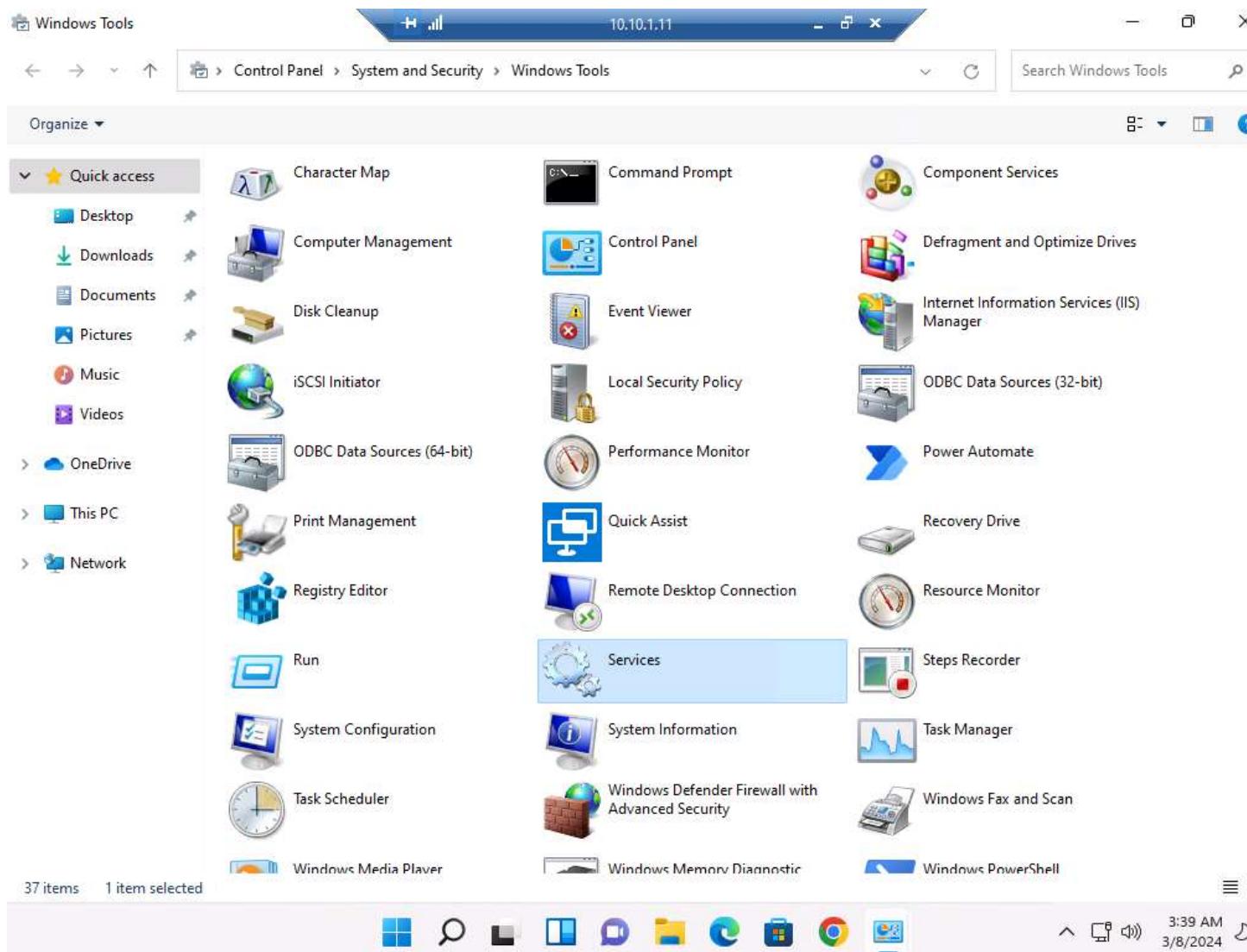
49. The **Remote Desktop Connection** pop-up appears; click **Yes**.

50.



51. A remote connection to the target system (**Windows 11**) appears.
52. If a **Choose privacy settings for your device** window appears, click on **Next** in the next window click on **Next** and in the next window click on **Accept**.
53. In the **Desktop** window, click windows **Search** icon and search for **Control Panel** in the search bar and launch it.
54. The **Control Panel** window appears; navigate to **System and Security --> Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.

55.



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

57.

The screenshot shows the Windows Services console window titled "Services (Local)". The "Remote Packet Capture Protocol v.0 (experimental)" service is selected. A context menu is open over this service, with the "Start" option highlighted. The service details pane on the left shows its description: "Allows to capture traffic on this machine from a remote machine." The main pane lists all system services, and the status column for the selected service shows it is "Running".

Name	Description	Status	Startup Type	Log On As
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troubleshooting Service	Enables aut...	Running	Manual	Local Syste...
Remote Access Auto Connection Manager	Creates a co...	Running	Manual	Local Syste...
Remote Access Connection Manager	Manages di...	Running	Manual	Local Syste...
Remote Desktop Configuration	Remote Des...	Running	Manual	Local Syste...
Remote Desktop Services	Allows user...	Running	Manual	Network S...
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local Syste...
Remote Packet Capture Protocol v.0 (experimental)	Start	Running	Manual	Local Syste...
Remote Procedure Call (RPC)	Stop	Automatic	Network S...	
Remote Procedure Call (RPC) Locator	Manual	Network S...		
Remote Registry	Disabled	Local Service		
Retail Demo Service	Manual	Local Syste...		
Routing and Remote Access	Disabled	Local Syste...		
RPC Endpoint Mapper	Automatic	Network S...		
Secondary Logon	Manual	Local Syste...		
Secure Socket Tunneling Protocol Service	Manual	Local Service		
Security Accounts Manager	Automatic	Local Syste...		
Security Center	Automatic (...)	Local Service		
Sensor Data Service	Manual (Trig...)	Local Syste...		
Sensor Monitoring Service	Manual (Trig...)	Local Service		
Sensor Service	Manual (Trig...)	Local Syste...		
Server	Automatic (T...)	Local Syste...		
Shared PC Account Manager	Disabled	Local Syste...		
Shell Hardware Detection	Automatic	Local Syste...		
Smart Card	Manual (Trig...)	Local Service		
Smart Card Device Enumeration Service	Creates soft...	Running		
Smart Card Removal Policy	Allows the s...	Manual		
SNMP Trap	Receives tra...	Manual		
Software Protection	Enables the ...	Automatic (...)		

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

59.

The screenshot shows the Windows Services console window titled "Services (Local)". The main pane displays a list of services, with the "Remote Packet Capture Protocol v.0 (experimental)" service selected and highlighted. The service details pane on the left provides information about the selected service, stating it allows capturing traffic from a remote machine. The status bar at the bottom right shows the date and time as 3/8/2024 3:42 AM.

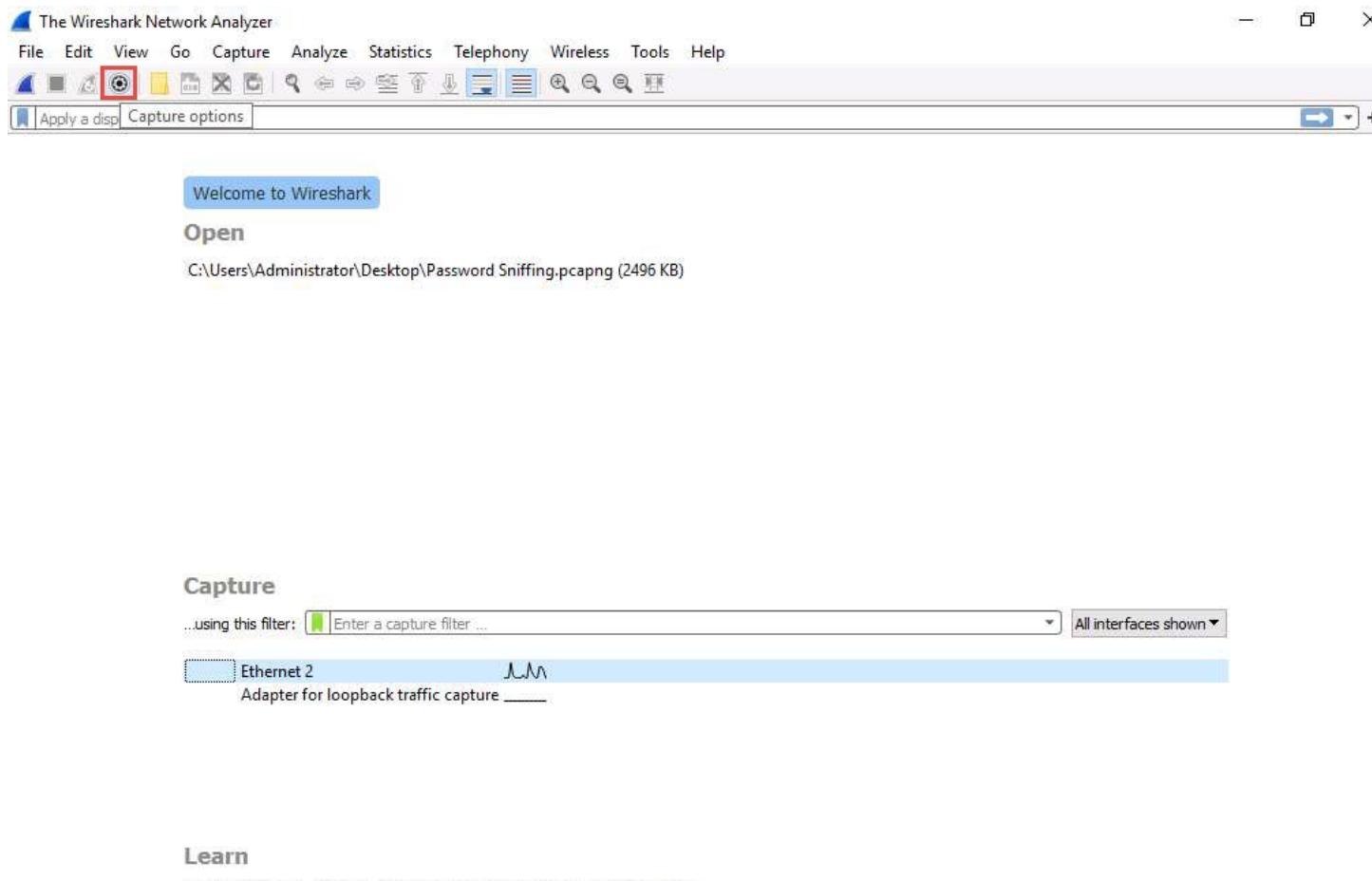
Name	Description	Status	Startup Type	Log On As
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troubleshooting Service	Enables aut...	Manual	Manual	Local Syst...
Remote Access Auto Connection Manager	Creates a co...	Manual	Manual	Local Syst...
Remote Access Connection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

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

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

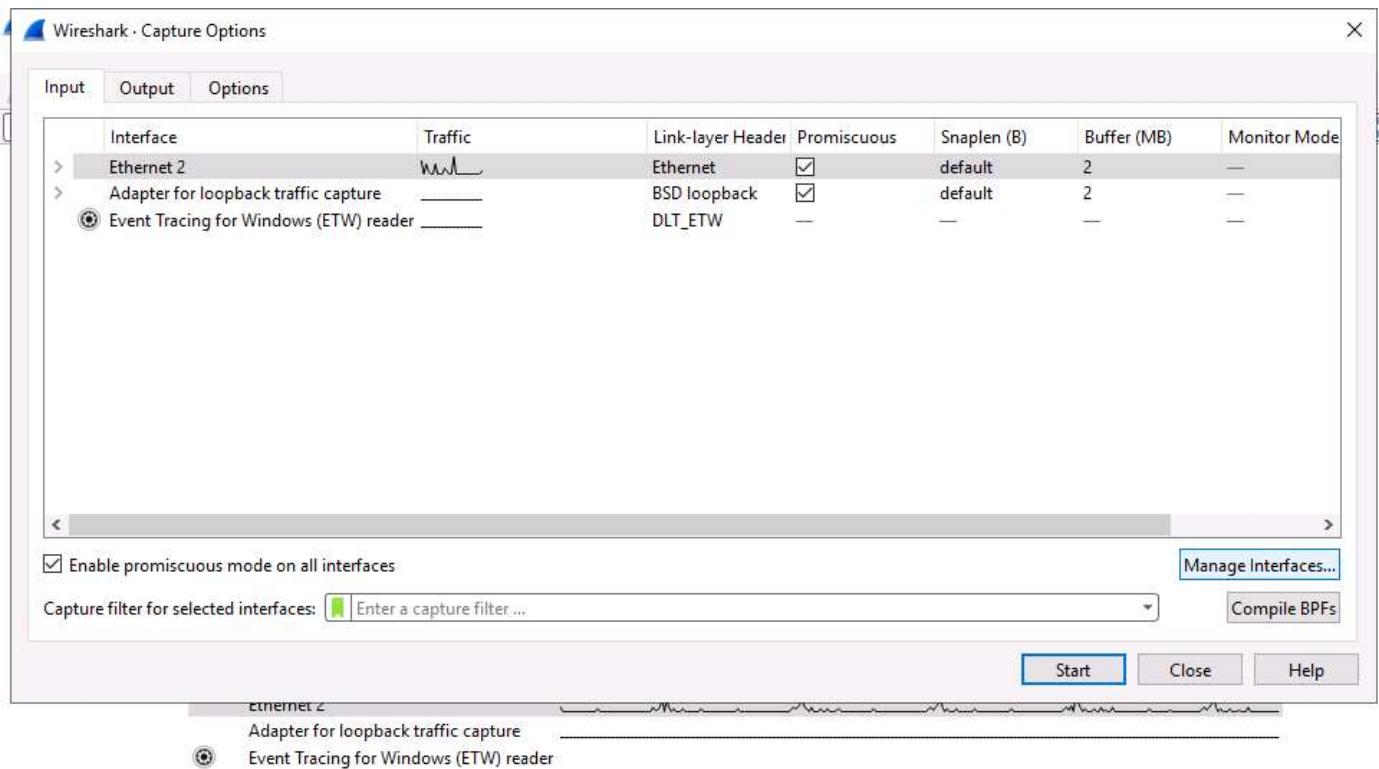
62. Now, in **Windows Server 2019**, launch **Wireshark** and click on **Capture options** icon from the toolbar.

63.



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

65.



Learn

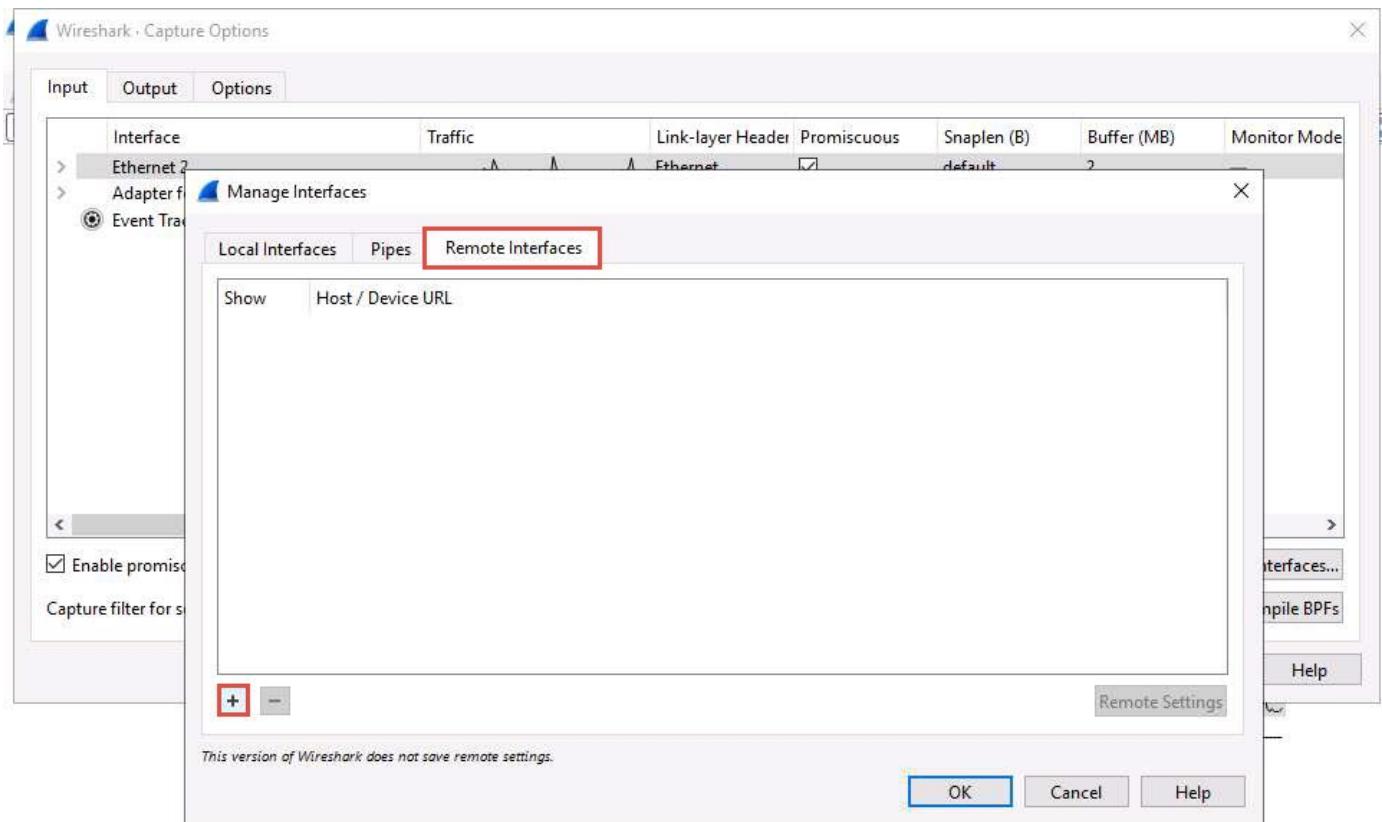
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.



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

67.



Learn

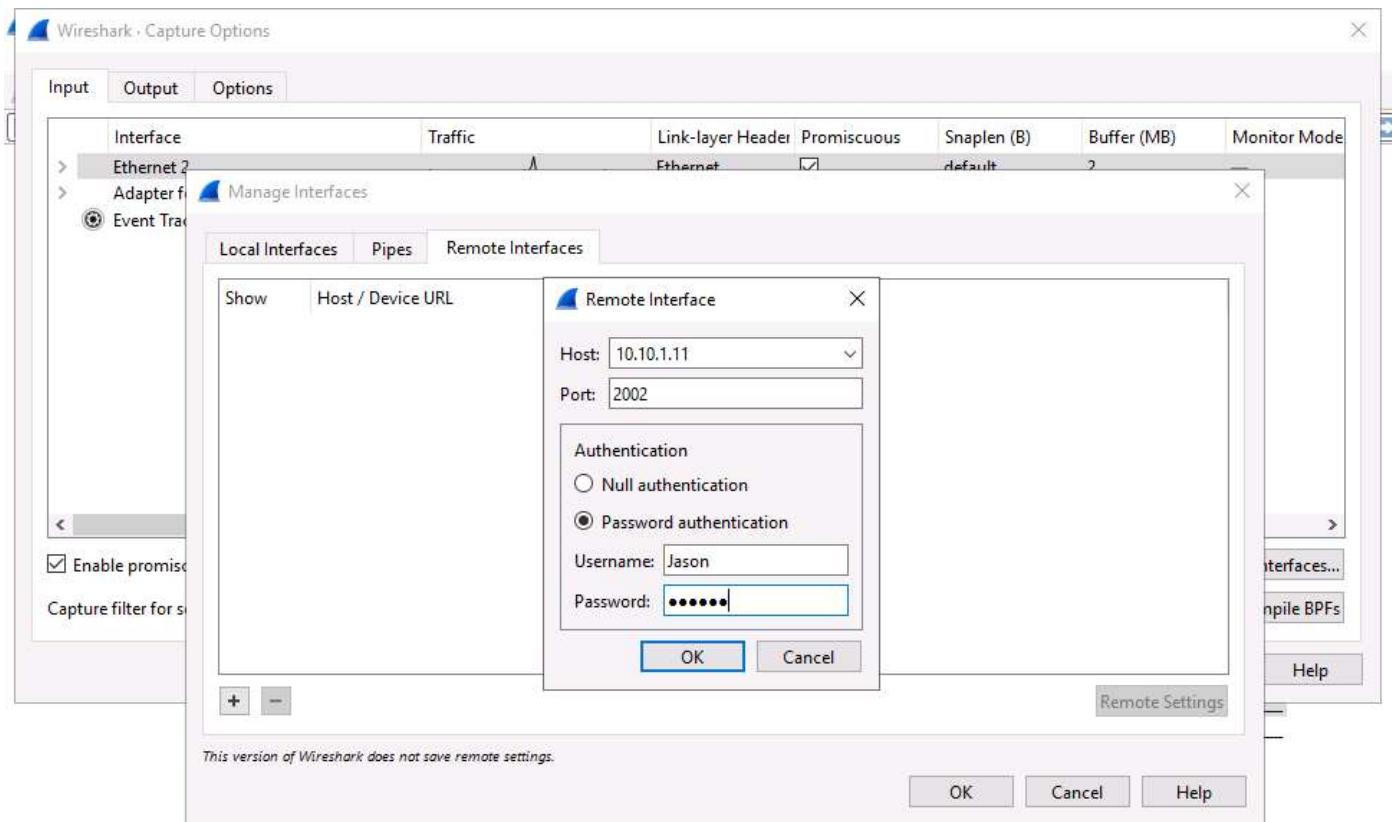
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.



68. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.1.11**); and in the **Port** field, enter the port number as **2002**.
69. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwertys**); click **OK**.
70. The IP address and user credentials may differ when you perform this task.

71.



Learn

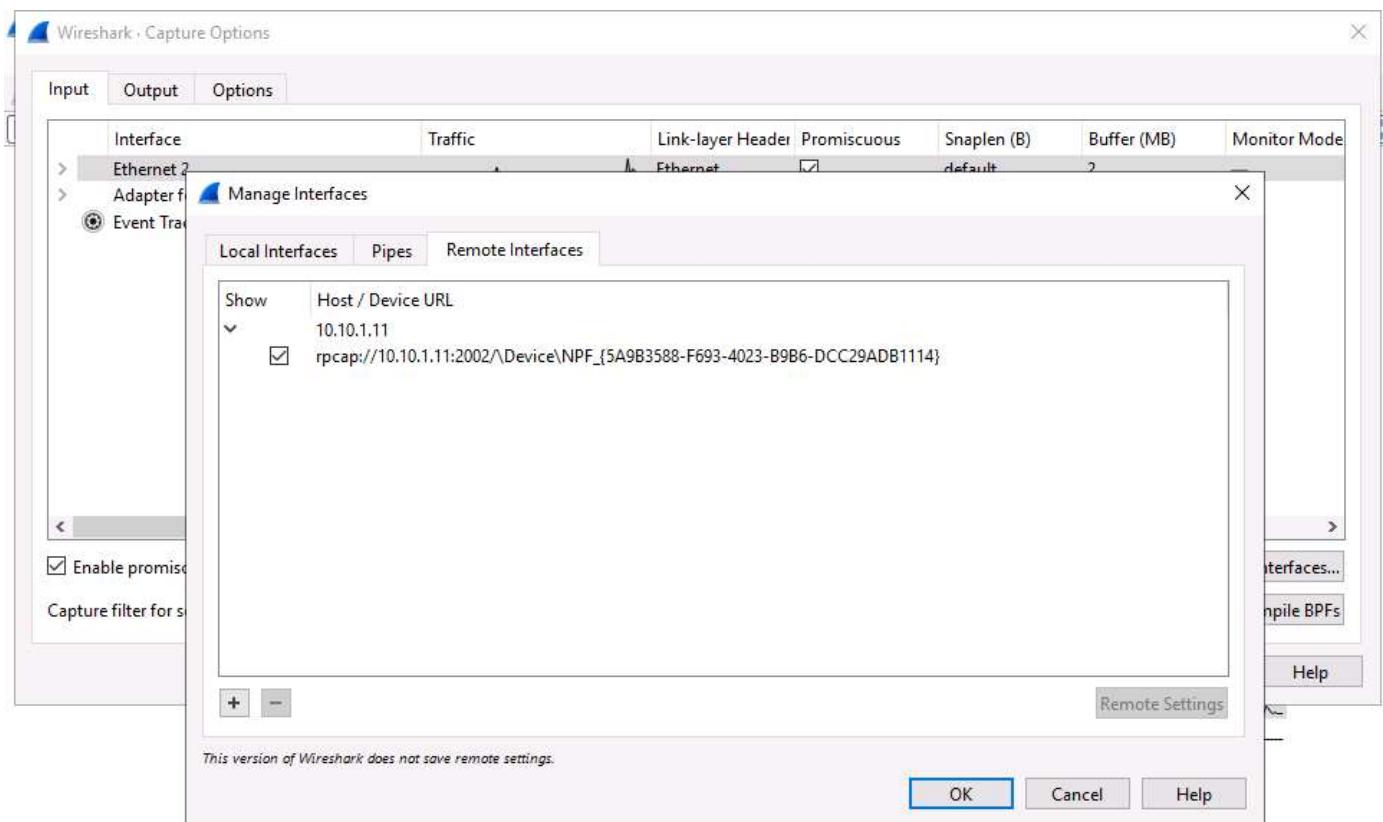
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.



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

73.



Learn

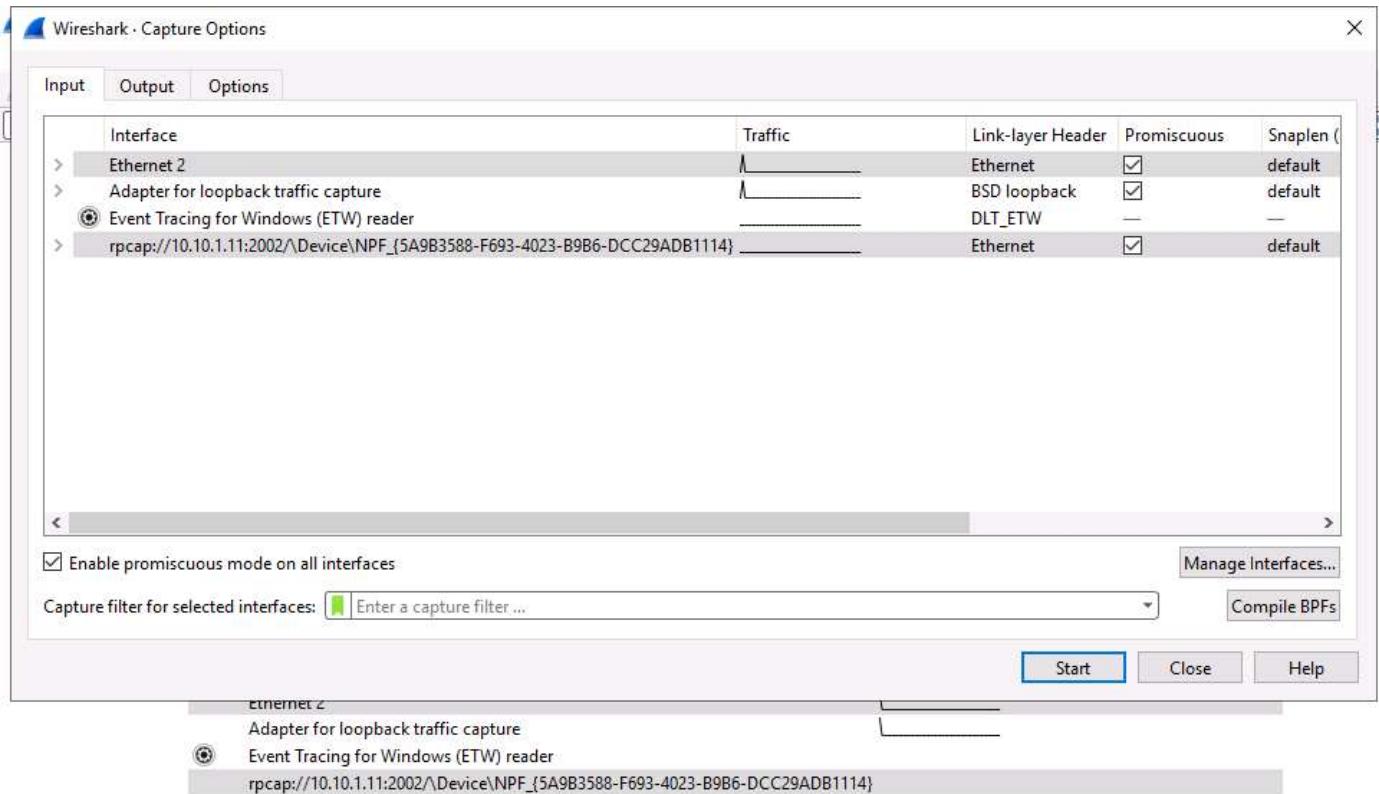
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.



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

75.



Learn

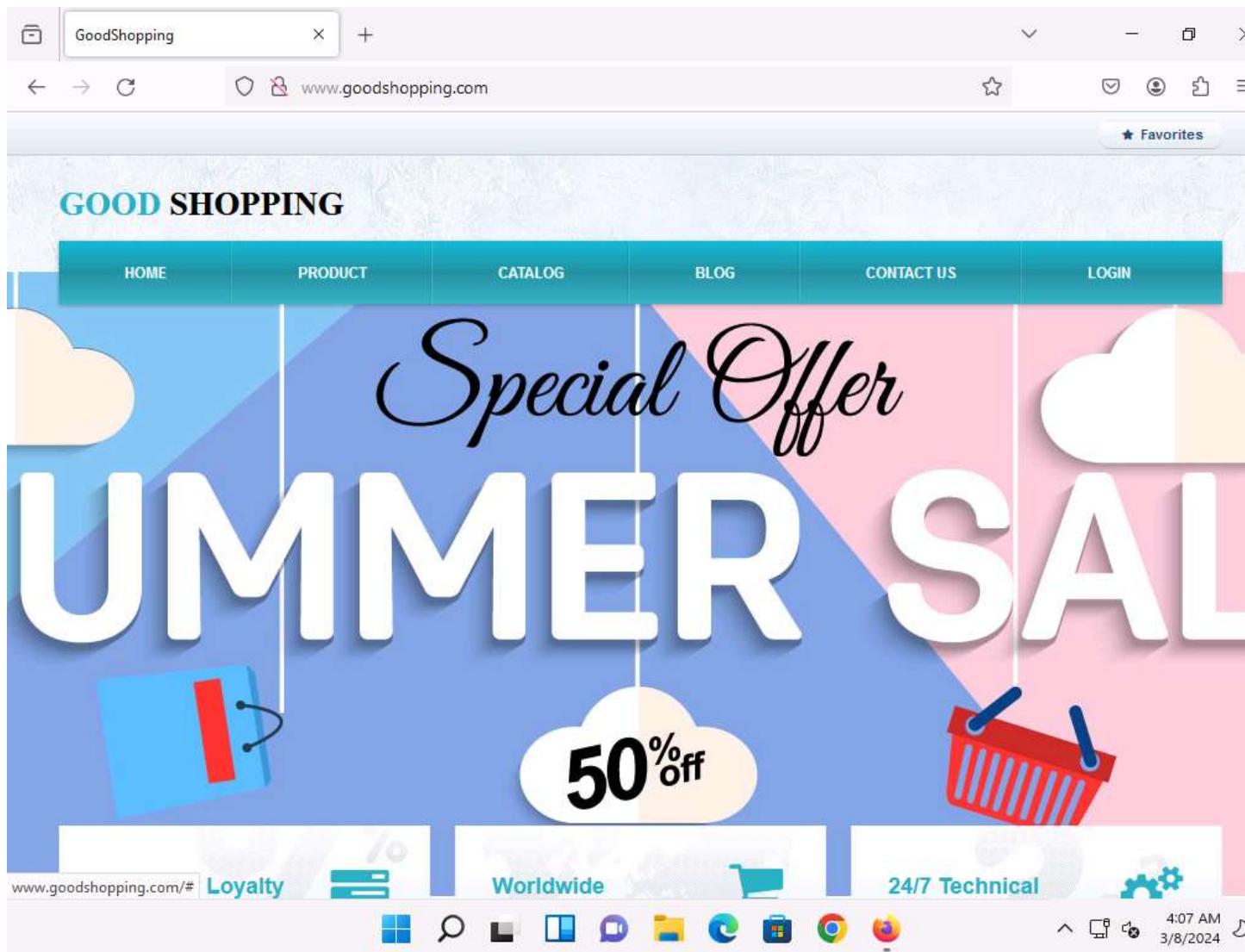
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.



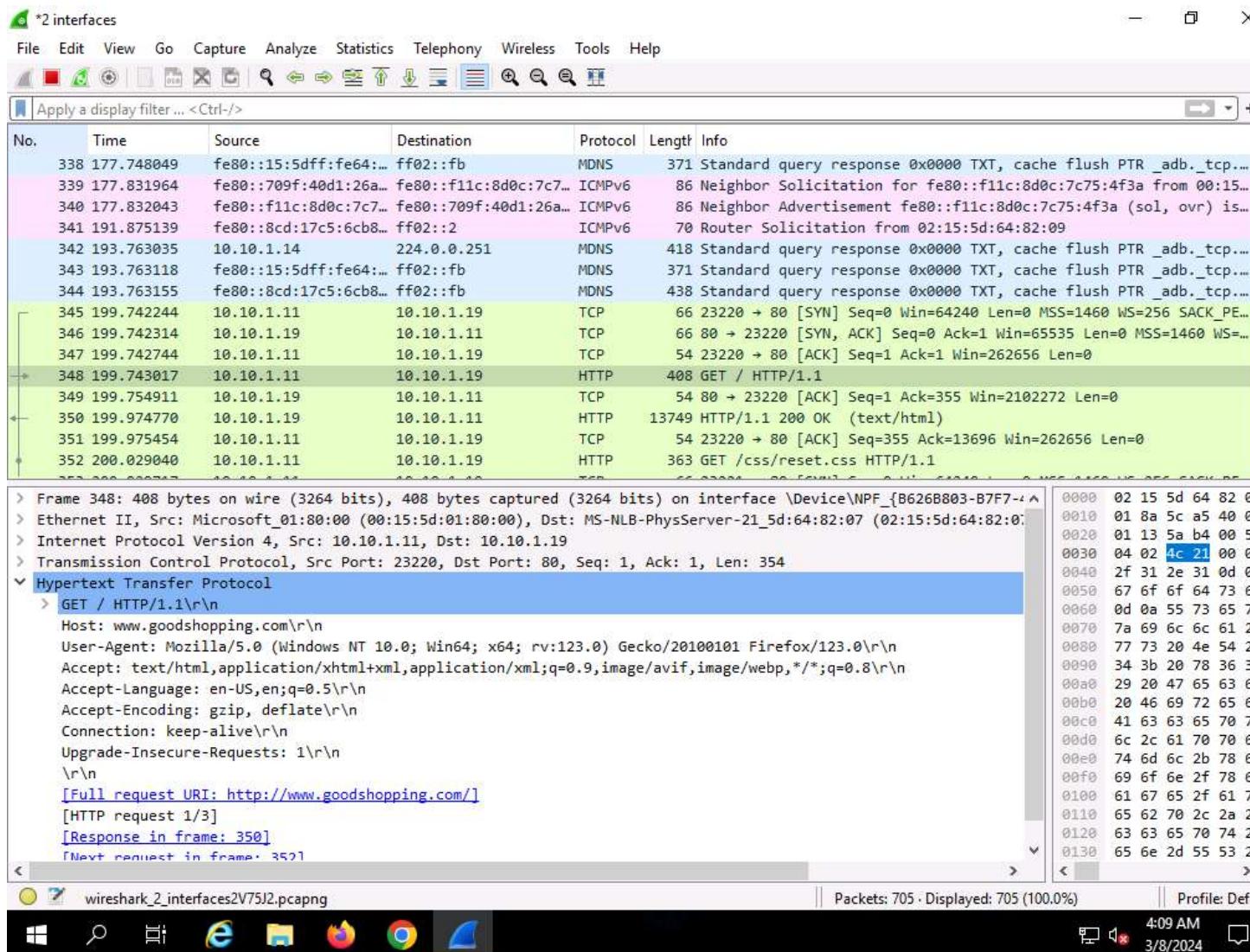
76. Click [Windows 11](#) to switch to the **Windows 11** machine, and login using **Jason/qwerty**. Here, you are signing in as the victim.
77. Acting as the target, open any web browser go to <http://www.goodshopping.com> (here, we are using **Mozilla Firefox**).
78. Although we are only browsing the Internet here, you could also log in to your account and sniff the credentials.

79.



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

81.



82. After a while, click the **Stop capturing packet** icon on the toolbar to stop live packet capture.
 83. This way, you can use Wireshark to capture traffic on a remote interface.
 84. 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.
 85. This concludes the demonstration of how to perform password sniffing using Wireshark.
 86. Close all open windows and document all the acquired information.

Question 8.2.1.1

Use the Wireshark tool to perform password sniffing. Which Wireshark display filter shows HTTP POST traffic?
Score

Lab 3: Detect Network Sniffing

Lab Scenario

The previous labs demonstrated how an attacker carries out sniffing with different techniques and tools. This lab helps you understand possible defensive techniques used to defend a target network against sniffing attacks. A professional ethical hacker or pen tester should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the various network sniffing detection techniques and tools discussed in this lab.

Lab Objectives

- Detect ARP poisoning and promiscuous mode in a switch-based network

Overview of Detecting Network Sniffing

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

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

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

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

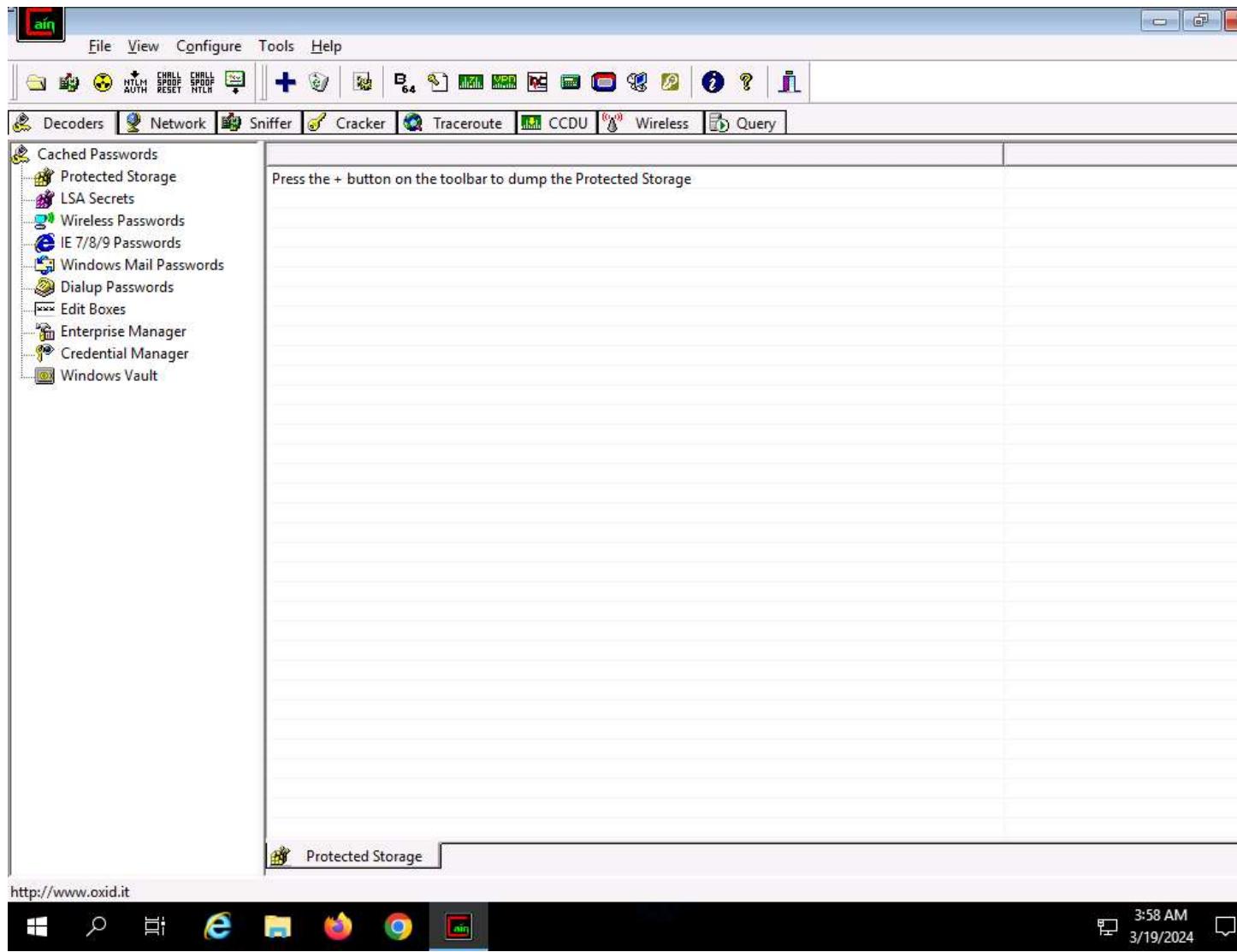
Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools. The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

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

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

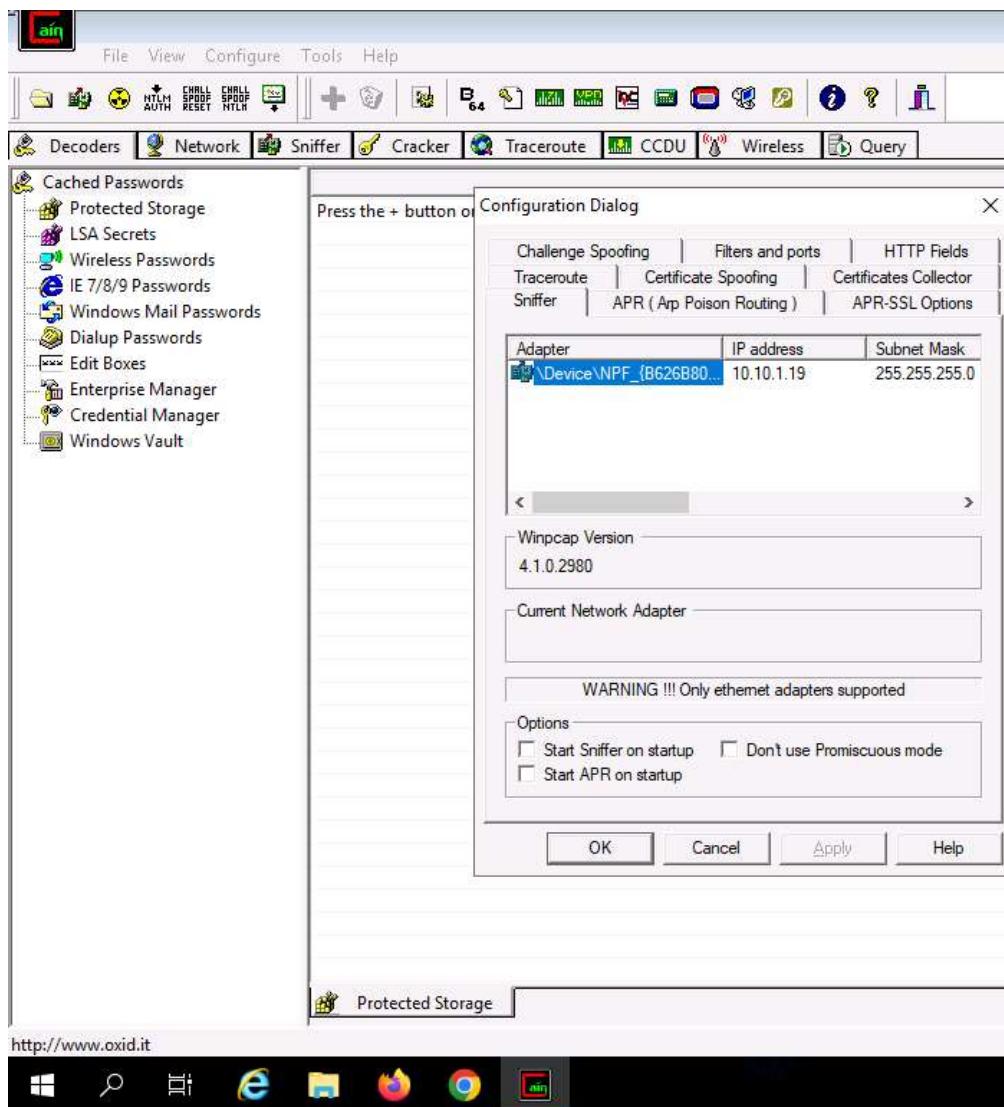
1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine.
2. In the **Desktop** window, click windows **Search** icon and search for **cain** in the search bar and launch it.
3. The **Cain & Abel** main window appears, click **Configure** from the menu bar to configure an ethernet card.

4.



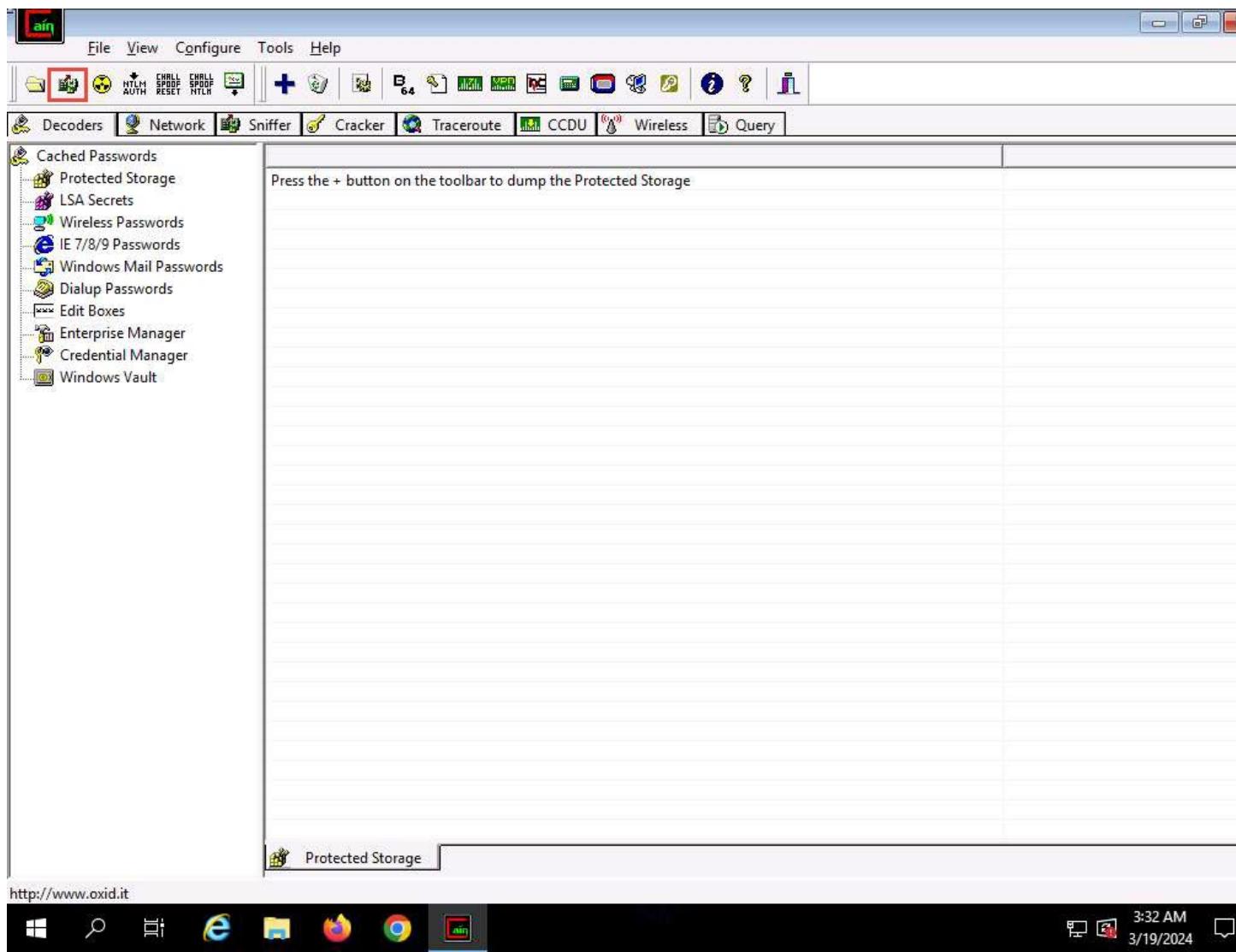
5. The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.

6.



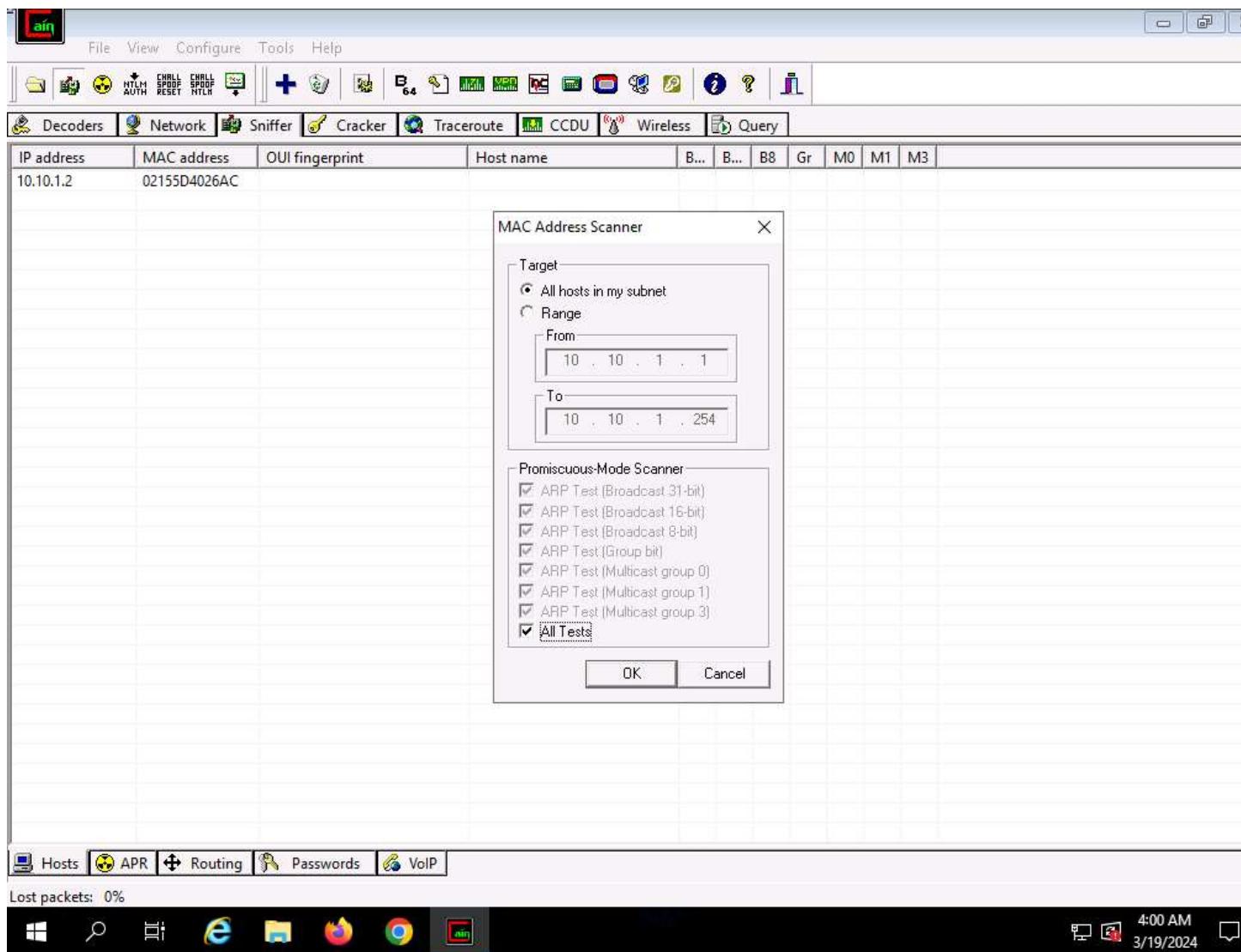
7. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.

8.



9. The **Cain** pop-up appears with a **Warning** message, click **OK**.
10. Now, click the **Sniffer** tab.
11. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
12. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button. Select the **All Tests** checkbox; then, click **OK**.

13.



14. Cain & Abel starts scanning for MAC addresses and lists all those found.
15. 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.

16.

The screenshot shows a Windows desktop environment with a network analysis application running in the foreground. The application has a toolbar at the top with various icons for decoding, sniffing, cracking, and wireless analysis. Below the toolbar is a menu bar with File, View, Configure, Tools, and Help. A tab bar includes Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, and Query, with Decoders currently selected. The main area is a table displaying network hosts:

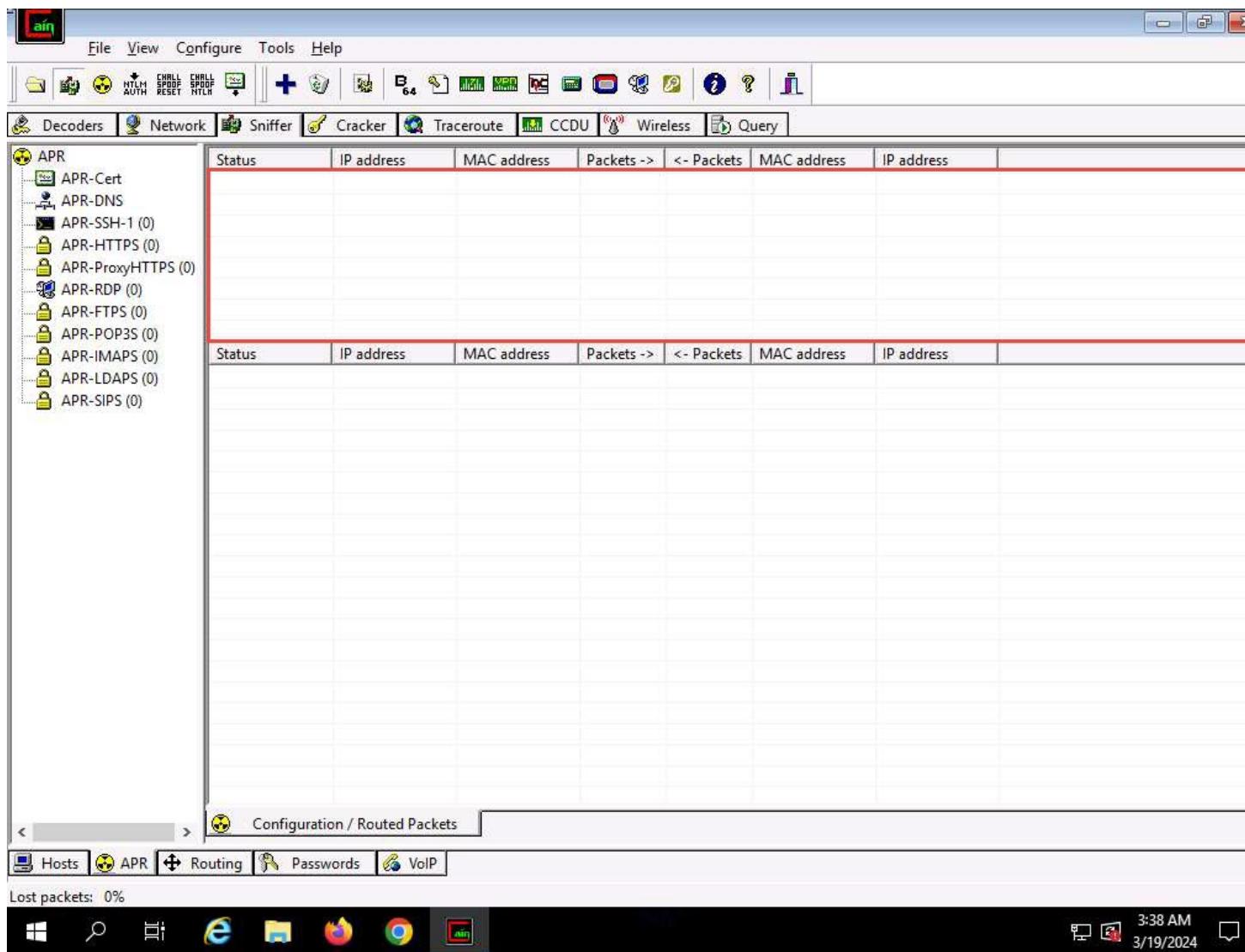
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.2	02155D4026AC			*	*	*	*	*	*	*
10.10.1.9	02155D4026B0			*	*	*	*	*	*	*
10.10.1.11	00155D018000	Microsoft Corporation		*	*	*	*	*	*	*
10.10.1.13	02155D4026AE			*	*	*	*	*	*	*
10.10.1.14	02155D4026B1			*	*	*	*	*	*	*
10.10.1.22	00155D018002	Microsoft Corporation		*	*	*	*	*	*	*

At the bottom of the application window, there is a navigation bar with tabs for Hosts, APR, Routing, Passwords, and VoIP, with APR currently selected. The taskbar at the bottom of the screen shows several open applications, including a browser, file explorer, and the network tool. The system tray indicates the date and time as 4:01 AM on 3/19/2024.

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

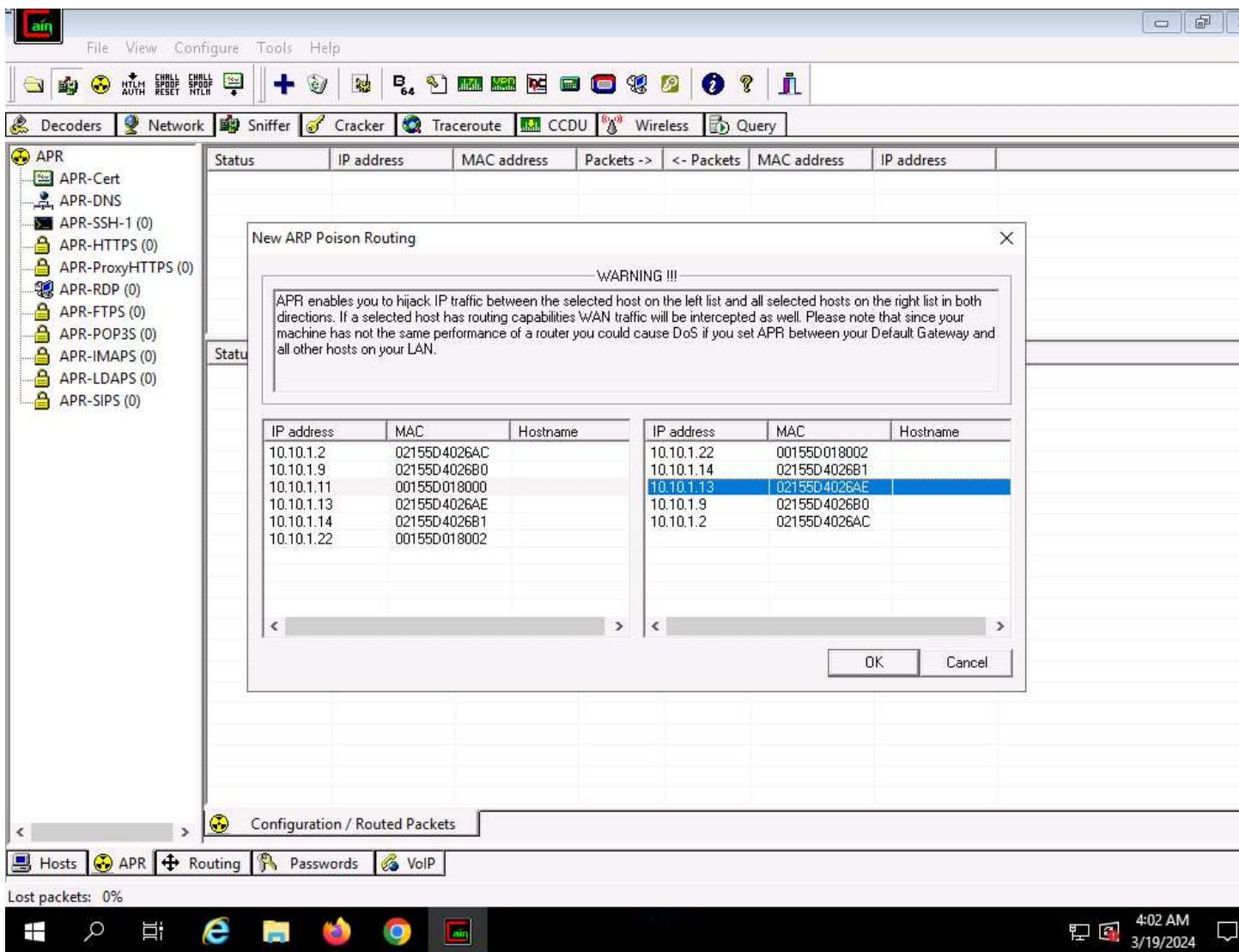
18. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.

19.



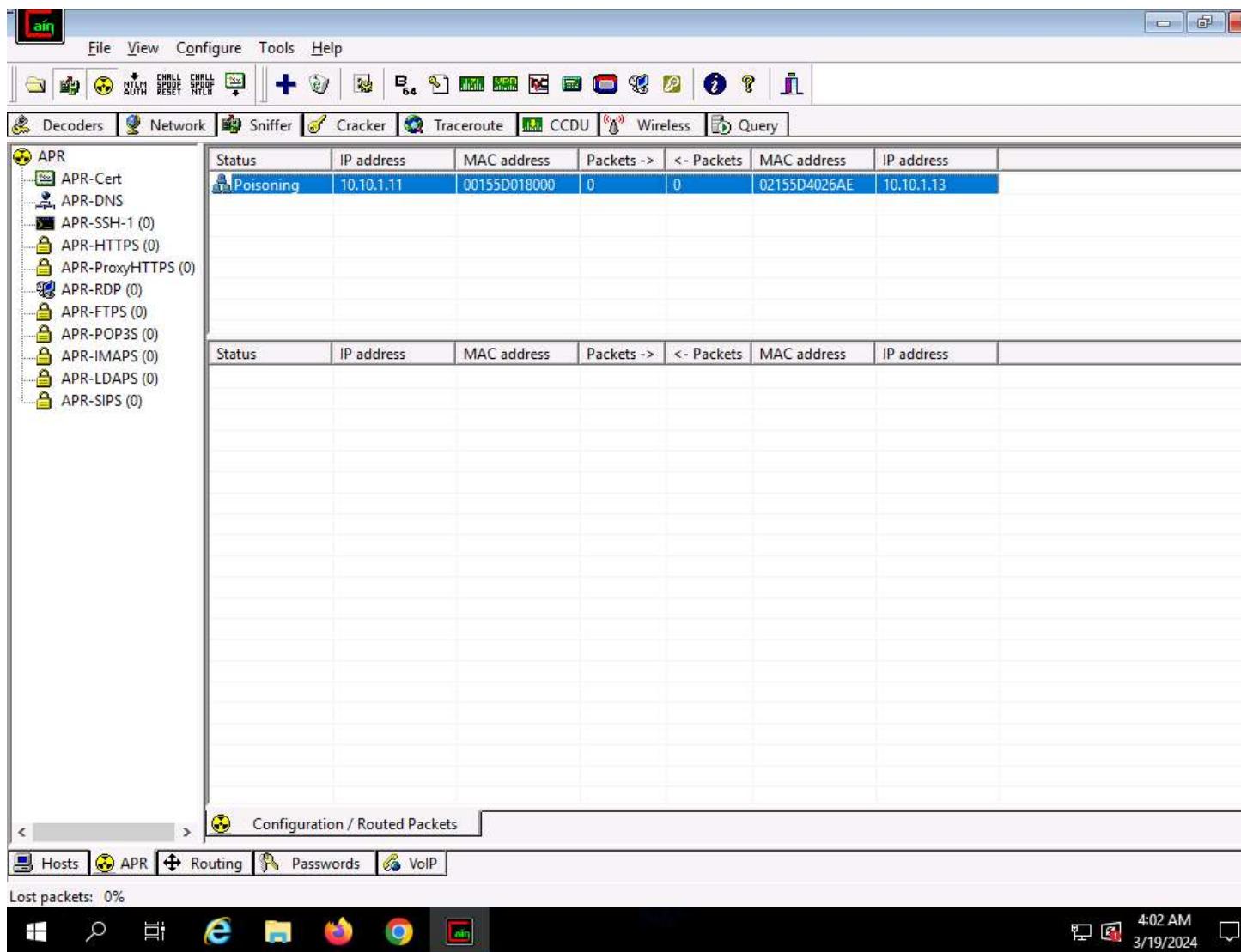
20. Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.
21. To monitor the traffic between two systems (here, **Windows 11** and **Parrot Security**), from the left-hand pane, click to select **10.10.1.11 (Windows 11)** and from the right-hand pane, click **10.10.1.13 (Parrot Security)**; click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

22.



23. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.
24. Click on the **Start/Stop APR** icon to start capturing ARP packets.
25. 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.

26.



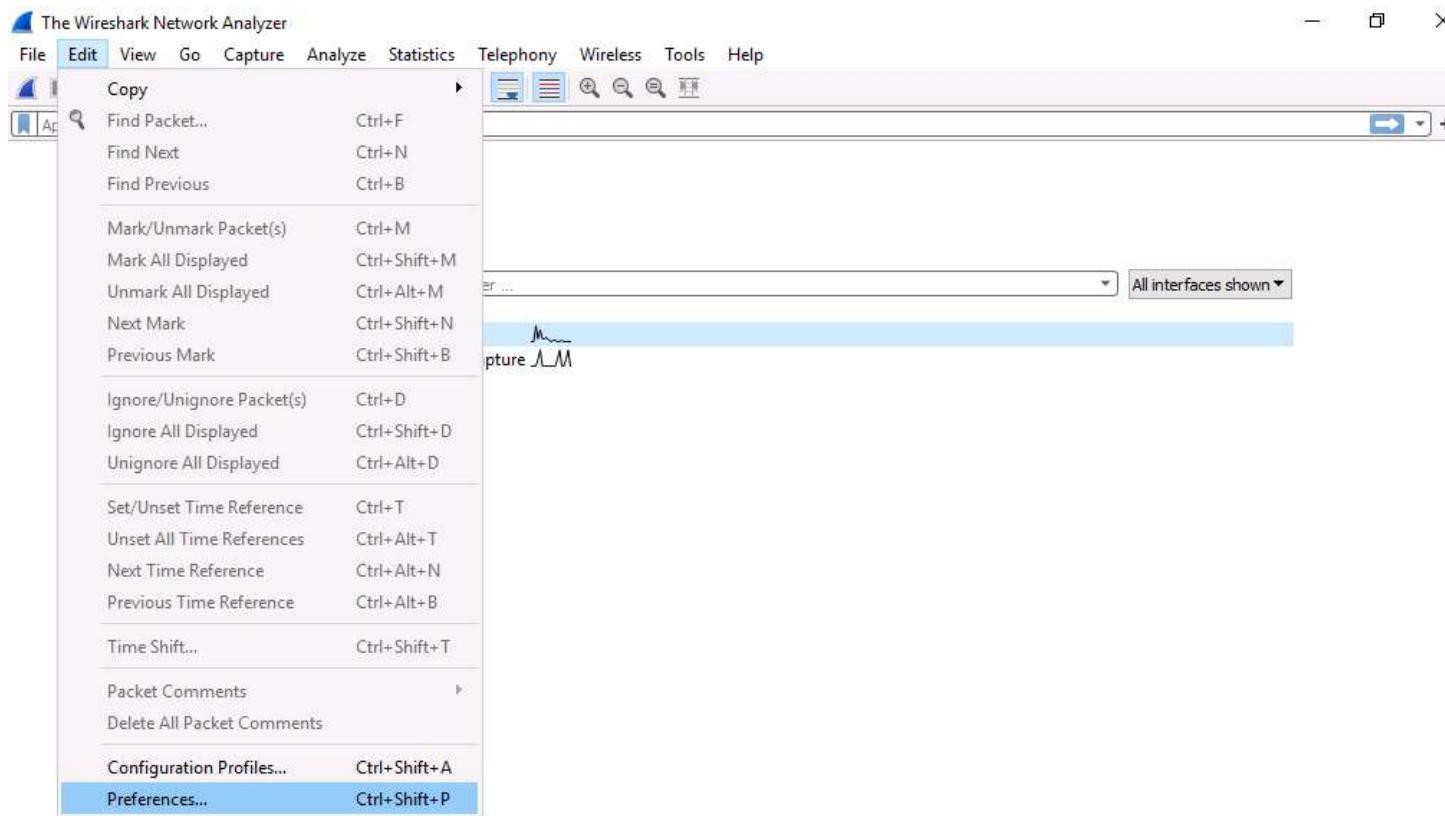
27. Cain & Abel intercepts the traffic traversing between these two machines.
28. To generate traffic between the machines, you need to ping one target machine using the other.
29. Click [Parrot Security](#) to switch to the **Parrot Security** machine.
30. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**). Run **cd** command to jump to root directory.
31. Run **hping3 [Target IP Address] -c 100000** command (here, target IP address is **10.10.1.11 [Windows 11]**).
32. **-c:** specifies the packet count.
33. This command will start pinging the target machine (**Windows 11**) with 100,000 packets.

34.

```
Applications Places System hping3 10.10.1.11 -c 100000 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~ 
$ sudo su
[sudo] password for attacker:
[root@parrot]~ 
#cd
[root@parrot]~ 
#hping3 10.10.1.11 -c 100000
HPING 10.10.1.11 (eth0 10.10.1.11): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=10.10.1.11 ttl=128 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=3.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=1 sport=0 flags=RA seq=1 win=0 rtt=3.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=2 sport=0 flags=RA seq=2 win=0 rtt=6.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=3 sport=0 flags=RA seq=3 win=0 rtt=2.9 ms
len=40 ip=10.10.1.11 ttl=128 DF id=4 sport=0 flags=RA seq=4 win=0 rtt=6.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=5 sport=0 flags=RA seq=5 win=0 rtt=6.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=6 sport=0 flags=RA seq=6 win=0 rtt=6.0 ms
len=40 ip=10.10.1.11 ttl=128 DF id=7 sport=0 flags=RA seq=7 win=0 rtt=2.6 ms
len=40 ip=10.10.1.11 ttl=128 DF id=8 sport=0 flags=RA seq=8 win=0 rtt=2.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=9 sport=0 flags=RA seq=9 win=0 rtt=2.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=10 sport=0 flags=RA seq=10 win=0 rtt=5.5 ms
len=40 ip=10.10.1.11 ttl=128 DF id=11 sport=0 flags=RA seq=11 win=0 rtt=5.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=12 sport=0 flags=RA seq=12 win=0 rtt=2.0 ms
len=40 ip=10.10.1.11 ttl=128 DF id=13 sport=0 flags=RA seq=13 win=0 rtt=1.7 ms
len=40 ip=10.10.1.11 ttl=128 DF id=14 sport=0 flags=RA seq=14 win=0 rtt=5.0 ms
len=40 ip=10.10.1.11 ttl=128 DF id=15 sport=0 flags=RA seq=15 win=0 rtt=4.9 ms
len=40 ip=10.10.1.11 ttl=128 DF id=16 sport=0 flags=RA seq=16 win=0 rtt=1.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=17 sport=0 flags=RA seq=17 win=0 rtt=1.3 ms
```

35. Leave the command running and immediately click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine.
36. In the **Desktop** window, click windows **Search** icon and search for **wireshark** in the search bar and launch it.
37. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences....**

38.



Learn

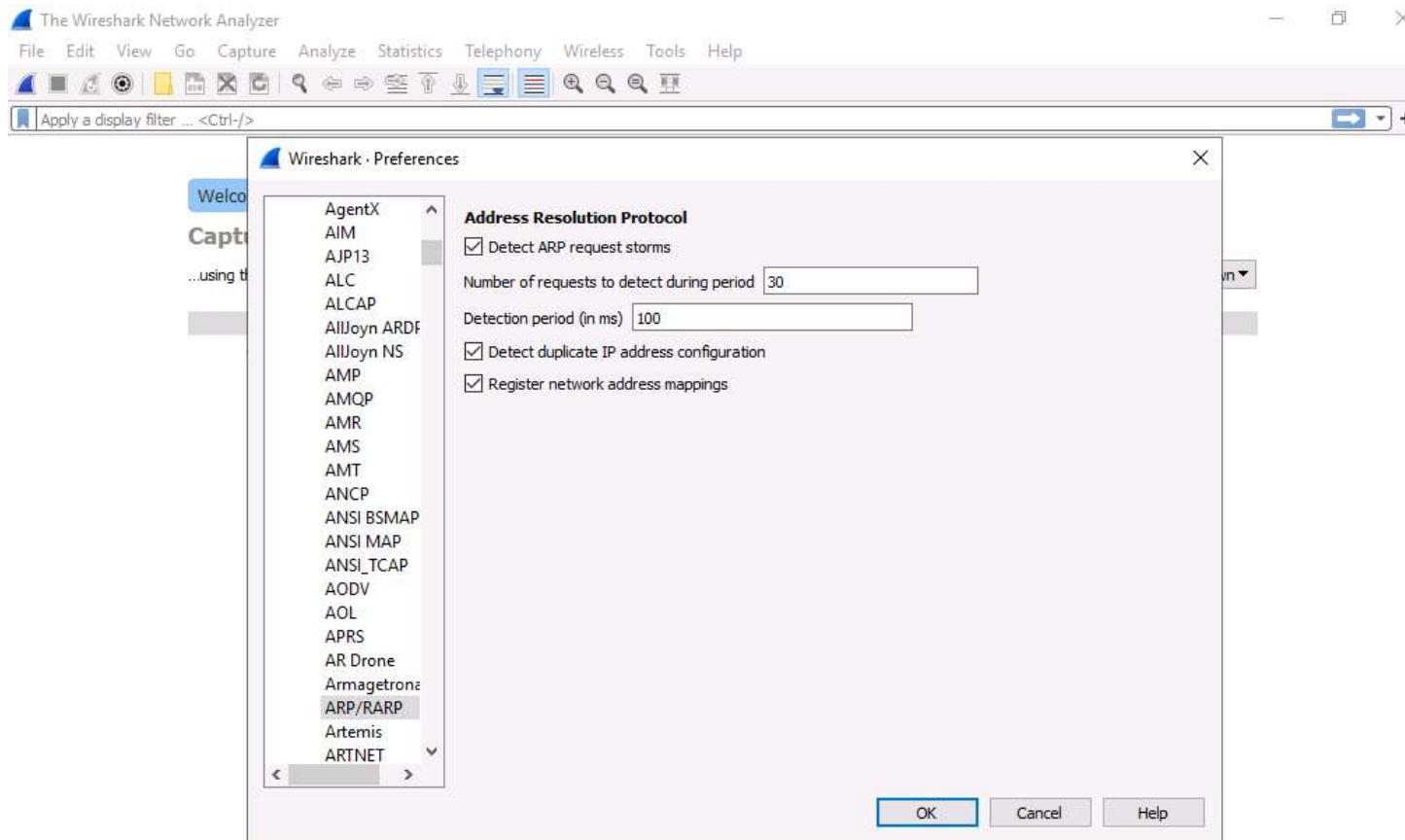
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

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



39. The **Wireshark . Preferences** window appears; expand the **Protocols** node.
40. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.
41. 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**.

42.



Learn

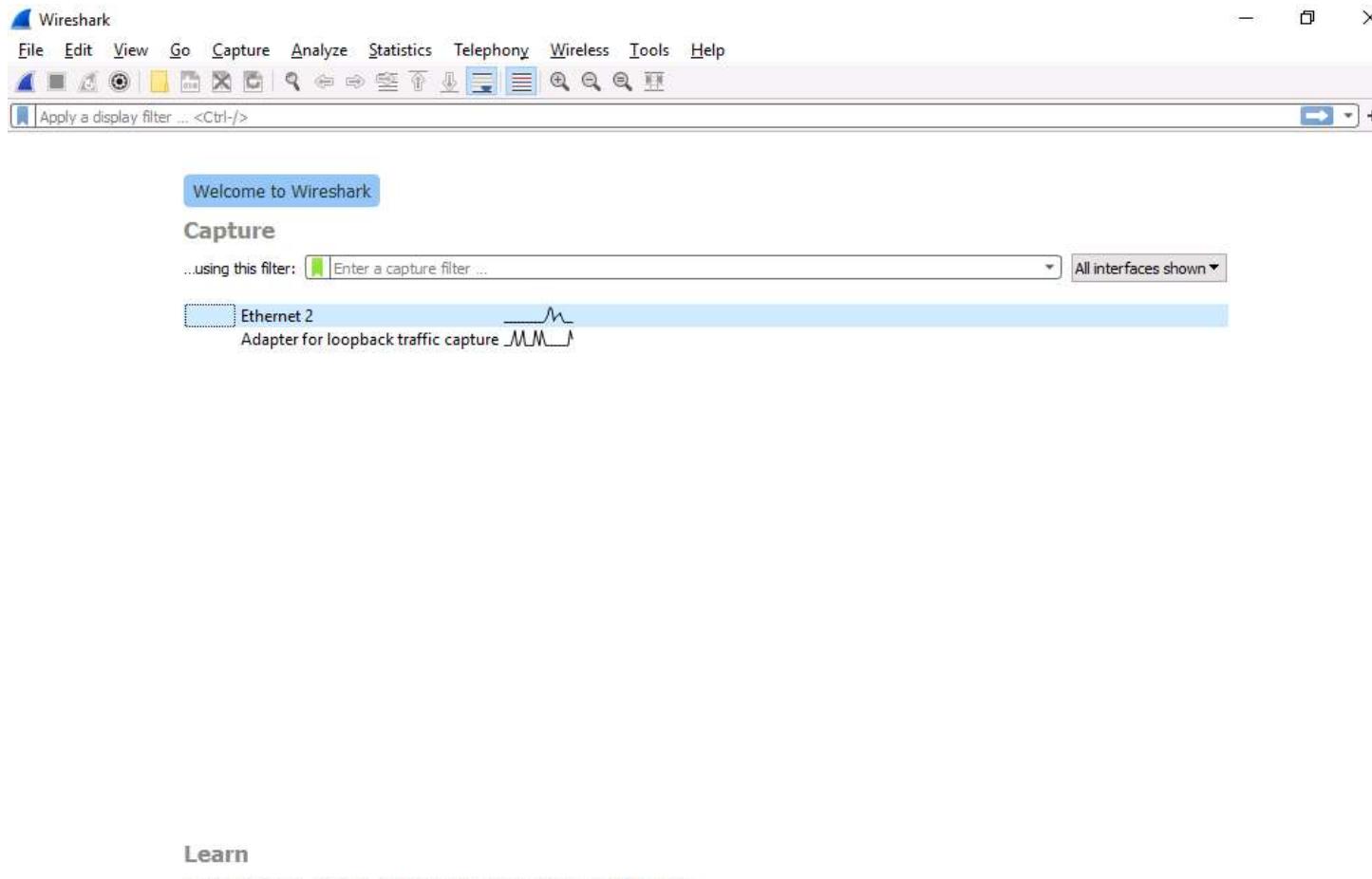
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

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



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

44.



Learn

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

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



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

46.

The screenshot shows the Wireshark interface capturing traffic from 'Ethernet 2'. The packet list pane displays 618 total packets, with 618 displayed. The columns include No., Time, Source, Destination, Protocol, Length, and Info. Most packets are TCP, primarily ACK and RST segments, indicating a connection reset or cleanup process. The packet details pane shows hex and ASCII representations of the captured bytes. The bottom status bar indicates the capture is live on 'Ethernet 2' and shows system information like the date and time.

No.	Time	Source	Destination	Protocol	Length	Info
335	10.260845	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 334#1] 1988 + 0 [<None>] Seq=1 Win=512 Len=0
336	10.260857	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 334#2] 1988 + 0 [<None>] Seq=1 Win=512 Len=0
337	10.261326	10.10.1.11	10.10.1.13	TCP	54	0 → 1988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
338	10.261389	10.10.1.11	10.10.1.13	TCP	54	0 → 1988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
339	10.261392	10.10.1.11	10.10.1.13	TCP	54	0 → 1988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
340	11.259940	10.10.1.13	10.10.1.11	TCP	54	1989 → 0 [<None>] Seq=1 Win=512 Len=0
341	11.260081	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 340#1] 1989 + 0 [<None>] Seq=1 Win=512 Len=0
342	11.260086	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 340#2] 1989 + 0 [<None>] Seq=1 Win=512 Len=0
343	11.260388	10.10.1.11	10.10.1.13	TCP	54	0 → 1989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
344	11.260438	10.10.1.11	10.10.1.13	TCP	54	0 → 1989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
345	11.260441	10.10.1.11	10.10.1.13	TCP	54	0 → 1989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
346	12.260692	10.10.1.13	10.10.1.11	TCP	54	1990 → 0 [<None>] Seq=1 Win=512 Len=0
347	12.260774	10.10.1.13	10.10.1.11	TCP	54	[TCP Dup ACK 346#1] 1990 + 0 [<None>] Seq=1 Win=512 Len=0

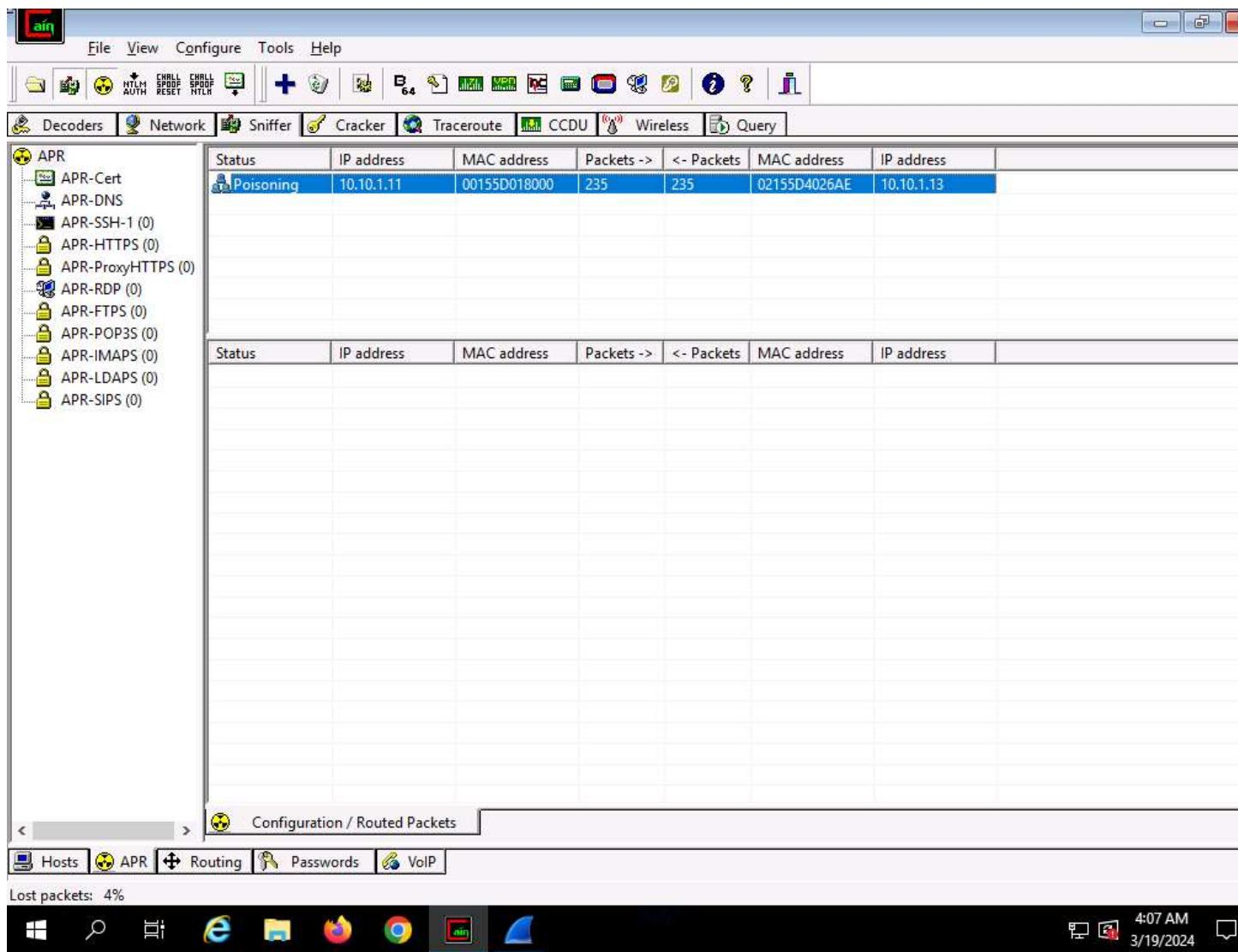
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:40:26:b2 (02:15:5d:40:26:b2), Dst: Microsoft_01:80:00 (00:15:5d:01:80:00)
> Address Resolution Protocol (reply)

0000 00 15 5d 01 80 00 02 15 5d 40 26 b2 08 06 00 01 ..].....]@&.....
0010 08 00 06 04 00 02 02 15 5d 40 26 b2 0a 0a 01 0d]@&.....
0020 00 15 5d 01 80 00 0a 0a 01 0b ..]..... ..

Ethernet 2: <live capture in progress> | Packets: 618 · Displayed: 618 (100.0%) | Profile: Default
4:07 AM 3/19/2024

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

48.



49. Now, switch to Wireshark and click the **Stop packet capturing** icon to stop the packet capturing.
50. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.11)**, running on the **ARP/RARP** protocol.

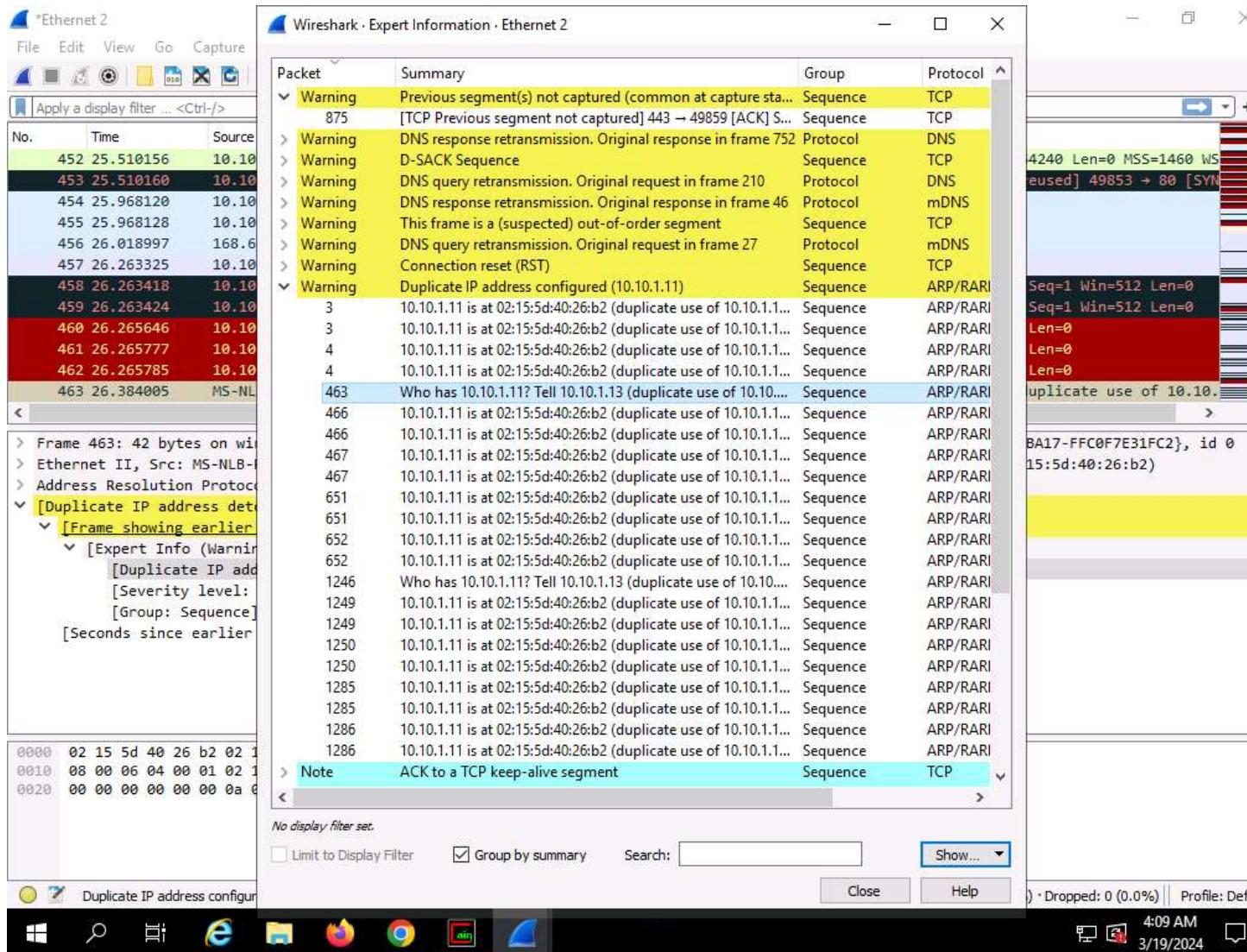
51.

The screenshot shows the Wireshark application interface. The main window displays a list of network packets captured on 'Ethernet 2'. The second window, titled 'Wireshark - Expert Information - Ethernet 2', is overlaid on the main window. This expert information window lists various warnings and notes related to the captured packets. A specific note for packet 463 is highlighted in yellow, indicating it is an ACK to a TCP keep-alive segment. The status bar at the bottom right shows the time as 4:08 AM and the date as 3/19/2024.

Severity	Summary	Group	Protocol
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP
875	[TCP Previous segment not captured] 443 → 49859 [ACK] S...	Sequence	TCP
> Warning	DNS response retransmission. Original response in frame 752	Protocol	DNS
> Warning	D-SACK Sequence	Sequence	TCP
> Warning	DNS query retransmission. Original request in frame 210	Protocol	DNS
> Warning	DNS response retransmission. Original response in frame 46	Protocol	mDNS
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP
> Warning	DNS query retransmission. Original request in frame 27	Protocol	mDNS
> Warning	Connection reset (RST)	Sequence	TCP
> Warning	Duplicate IP address configured (10.10.1.11)	Sequence	ARP/RARI
3	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
3	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
4	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
4	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
463	Who has 10.10.1.11? Tell 10.10.1.13 (duplicate use of 10.10....)	Sequence	ARP/RARI
466	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
466	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
467	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
467	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
651	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
651	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
652	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
652	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1246	Who has 10.10.1.11? Tell 10.10.1.13 (duplicate use of 10.10....)	Sequence	ARP/RARI
1249	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1249	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1250	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1250	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1285	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1285	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1286	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
1286	10.10.1.11 is at 02:15:5d:40:26:b2 (duplicate use of 10.10.1.1...)	Sequence	ARP/RARI
> Note	ACK to a TCP keep-alive segment	Sequence	TCP

52. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.
53. In the **Wireshark . Expert Information** window, click any packet (here, 463).

54.



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

57.

The screenshot shows a Wireshark capture window for interface "Ethernet 2". The packet list pane shows several TCP and NTP packets between 10.10.1.19 and 10.10.1.13. A yellow highlight covers a section of the packet details and bytes panes, specifically focusing on frame 463 which is an ARP request. The details pane shows the ARP request with source MAC 02:15:5d:40:26:b2 and destination MAC 0a:0a:01:0d. The bytes pane shows the raw hex and ASCII data of the ARP frame. Below the Wireshark window, the Windows taskbar is visible with icons for File Explorer, Edge, and other applications. The system tray shows the date and time as 3/19/2024 at 4:09 AM.

Frame 463: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}, id 0

Ethernet II, Src: MS-NLB-PhysServer-21_5d:40:26:ae (02:15:5d:40:26:ae), Dst: MS-NLB-PhysServer-21_5d:40:26:b2 (02:15:5d:40:26:b2)

Address Resolution Protocol (request)

[Duplicate IP address detected for 10.10.1.13 (02:15:5d:40:26:ae) - also in use by 02:15:5d:40:26:b2 (frame 2)]

[Frame showing earlier use of IP address: 2]

[Expert Info (Warning/Sequence): Duplicate IP address configured (10.10.1.13)]

[Duplicate IP address configured (10.10.1.13)]

[Severity level: Warning]

[Group: Sequence]

[Seconds since earlier frame seen: 26]

0000 02 15 5d 40 26 b2 02 15 5d 40 26 ae 08 06 00 01 ..]@&...]@&....

0010 08 00 06 04 00 01 02 15 5d 40 26 ae 0a 0a 01 0d]@&....

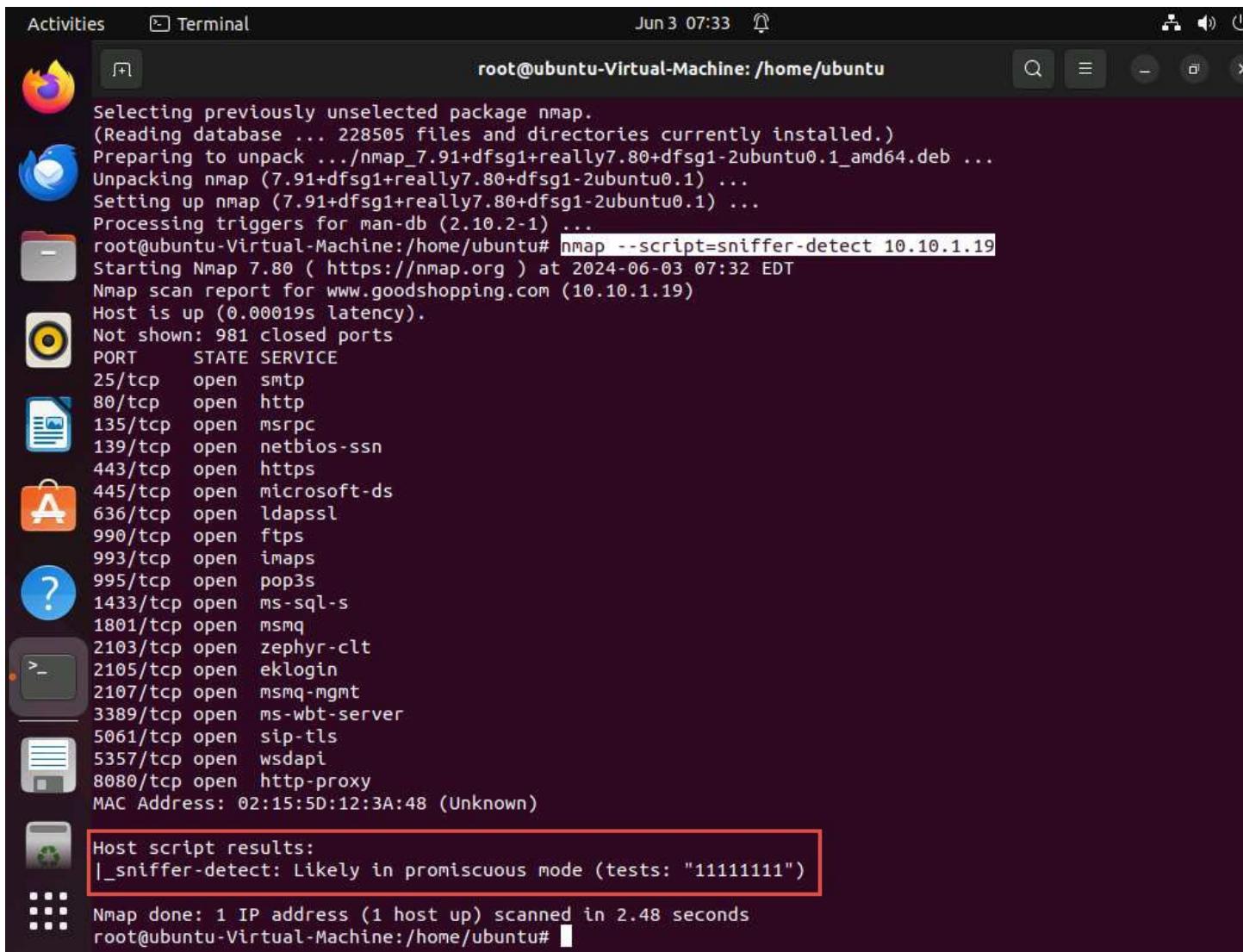
0020 00 00 00 00 00 00 0a 0a 01 0b

Duplicate IP address configured (arp.duplicate-address-detected) | Packets: 1335 • Displayed: 1335 (100.0%) • Dropped: 0 (0.0%) | Profile: Default

4:09 AM 3/19/2024

58. 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.
59. This concludes the demonstration of detecting ARP poisoning in a switch-based network.
60. Close the **Wireshark** window and leave all other windows running.
61. Now, we shall perform promiscuous mode detection using Nmap.
62. Now, Click [Ubuntu](#) to switch to the **Ubuntu** machine and login with **Ubuntu/toor**.
63. In the **Ubuntu** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**)
64. Run **nmap --script=sniffer-detect [Target IP Address/ IP Address Range]** (here, target IP address is **10.10.1.19 [Windows Server 2019]**) to start scanning.
65. 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.

66.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@ubuntu-Virtual-Machine: /home/ubuntu". The terminal content shows the following Nmap command and its output:

```
Selecting previously unselected package nmap.  
(Reading database ... 228505 files and directories currently installed.)  
Preparing to unpack .../nmap_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_amd64.deb ...  
Unpacking nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...  
Setting up nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...  
Processing triggers for man-db (2.10.2-1) ...  
root@ubuntu-Virtual-Machine:/home/ubuntu# nmap --script=sniffer-detect 10.10.1.19  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-03 07:32 EDT  
Nmap scan report for www.goodshopping.com (10.10.1.19)  
Host is up (0.00019s latency).  
Not shown: 981 closed ports  
PORT      STATE SERVICE  
25/tcp    open  smtp  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
636/tcp   open  ldapssl  
990/tcp   open  ftps  
993/tcp   open  imaps  
995/tcp   open  pop3s  
1433/tcp  open  ms-sql-s  
1801/tcp  open  msmq  
2103/tcp  open  zephyr-clt  
2105/tcp  open  eklogin  
2107/tcp  open  msmq-mgmt  
3389/tcp  open  ms-wbt-server  
5061/tcp  open  sip-tls  
5357/tcp  open  wsdapi  
8080/tcp  open  http-proxy  
MAC Address: 02:15:5D:12:3A:48 (Unknown)  
  
Host script results:  
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")  
  
Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds  
root@ubuntu-Virtual-Machine:/home/ubuntu#
```

67. Close the terminal window and document all the acquired information.

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

Question 8.3.1.1

Use Cain and Abel on the Windows Server 2019 machine to perform ARP poisoning, and sniff traffic between the Windows 11 and Parrot Security machines. Further, use Wireshark on the same Windows Server 2019 machine to detect ARP poisoning. What is the severity level of ARP/RARP packets as shown in the expert information window of Wireshark?

Score

Question 8.3.1.2

Use the Nmap Scripting Engine (NSE) to check if a system on the local Ethernet has its network card in the promiscuous mode. Which Nmap NSE script detects if a network interface is in the promiscuous mode?

Score

- Check this box to confirm completion of this module.

Previous⁹**Next**¹⁰

22 Minutes Remaining

Thumbnail screenshot of virtual machineLab52682610-Windows 11

Windows 11

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Admin¹²

Password

Pa\$\$w0rd¹³

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52682610-Windows Server 2022

Windows Server 2022

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Administrator¹⁴

Password

Pa\$\$w0rd¹⁵

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52682610-Windows Server 2019

Windows Server 2019

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Administrator¹⁶

Password

Pa\$\$w0rd¹⁷

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52682610-Parrot Security

Parrot Security

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Attacker¹⁸

Password

toor¹⁹

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52682610-Ubuntu

Ubuntu

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Ubuntu²⁰

Password

toor²¹

Next: Lab 3: Detect Network Sniffing

0/129 (0%) Tasks Complete

Type Text

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

[Help](#)

Support Information

ID	52682610
Host	EU-HV27
Datacenter	EU North (London)

FAQs

[Frequently asked questions about the lab interface](#)

Other Help Options

[Submit a Support Request](#)

Powered by [Skillable](#) • [Review Us](#)

Notifications

Settings

Text Size

100 Standard

150 Large Text

200 Extra Large Text

Color Mode

- Light
- Dark
- High Contrast

Actions

[Split Windows](#)

Close Window

Close Window