

# **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.

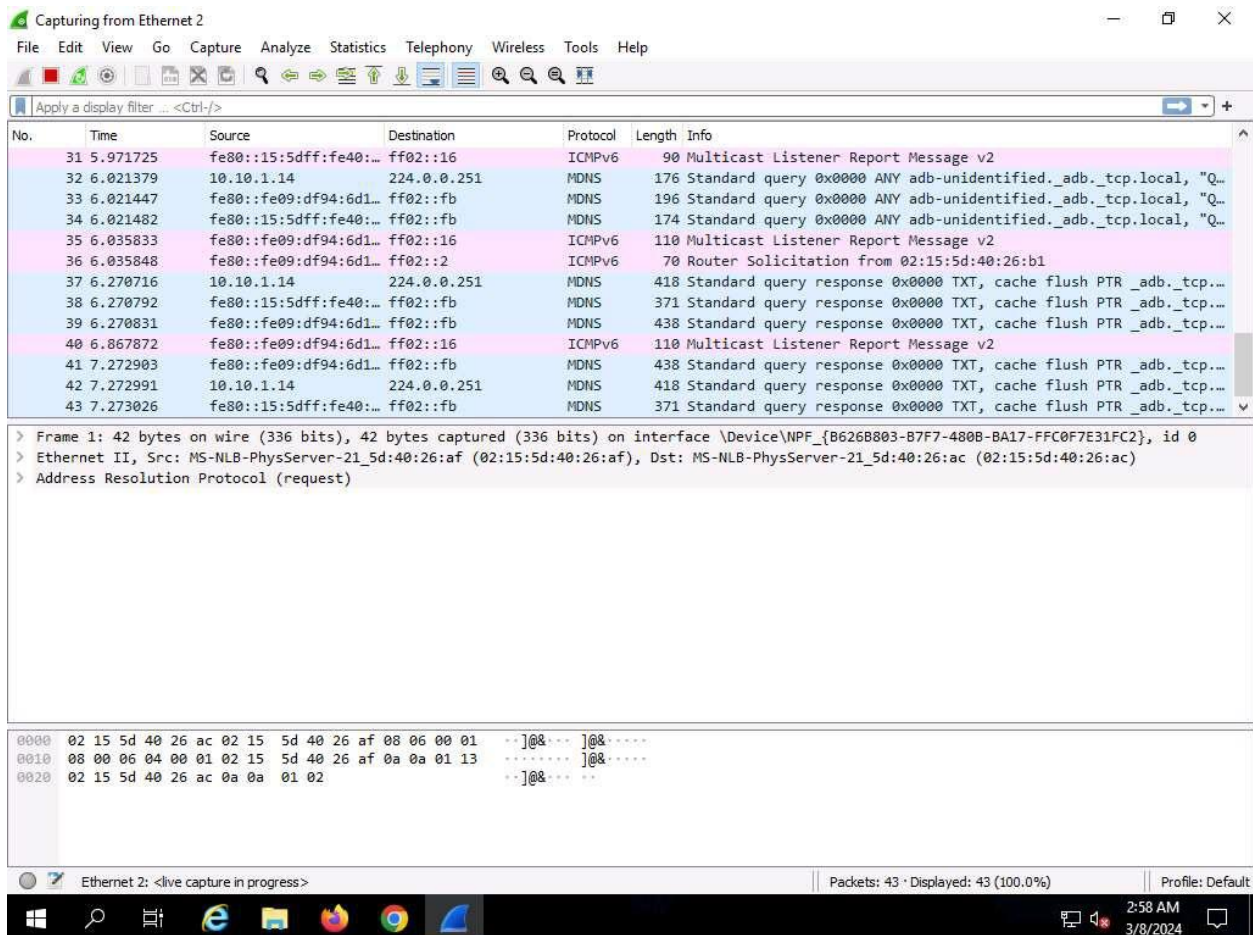
1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine and login with **Administrator/Pa\$\$w0rd**.

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

2. Search **Wireshark** from search bar and launch it.

If the **Software update** window appears, click **Remind me later**.

3. **The Wireshark Network Analyzer** window appears, start capturing the network traffic on the primary network interface (here, **Ethernet 2**).
4. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.



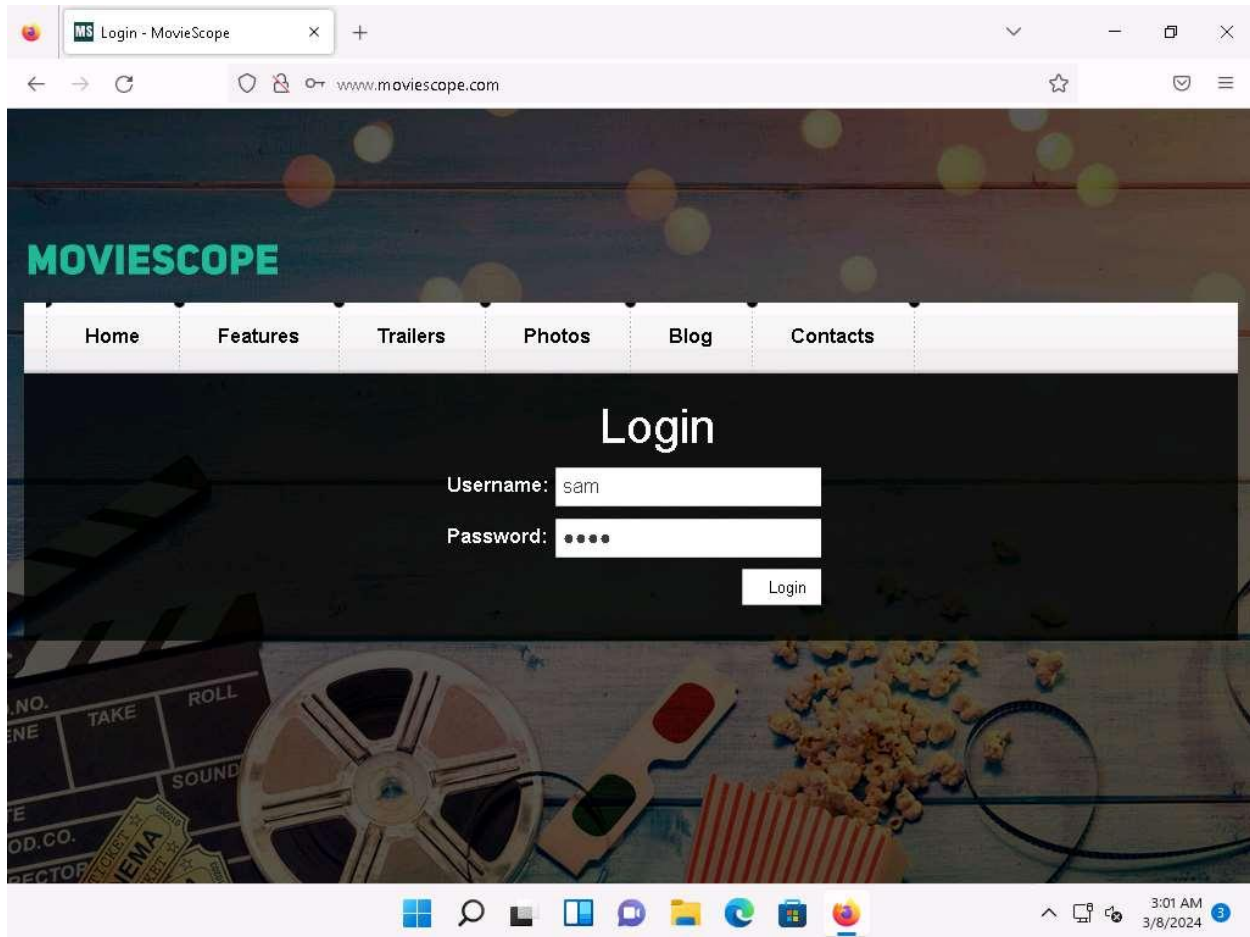
5. Now, click [Windows 11](#) to switch to the **Windows 11** machine, login using **Admin/Pa\$\$w0rd**.

Alternatively, you can also click **Pa\$\$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.

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

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

6. Open any web browser, and go to **<http://www.moviescope.com/>** (here, we are using **Mozilla Firefox**).
7. The **MOVIESCOPE** home page appears; login using **sam/test**.



8. 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.

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
203	34.346950	10.10.1.19	52.185.211.133	TCP	54	49799 → 443 [RST] Seq=1244 Win=0 Len=0
204	35.064892	10.10.1.11	10.10.1.255	NBNS	92	Name query NB WINDONS11<1c>
205	35.544538	fe80::8cd:17c5:6cb8...	ff02::2	ICMPv6	70	Router Solicitation from 02:15:5d:64:82:09
206	35.639175	10.10.1.14	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
207	35.639255	fe80::15:5dff:fe64:...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
208	35.639292	fe80::8cd:17c5:6cb8...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
209	35.819702	10.10.1.11	10.10.1.255	NBNS	92	Name query NB WINDONS11<1c>
210	36.579437	10.10.1.11	10.10.1.255	NBNS	92	Name query NB WINDONS11<1c>
211	37.311505	10.10.1.11	10.10.1.19	TCP	55	[TCP Keep-Alive] 16931 → 80 [ACK] Seq=1281 Ack=27723 Win=26265...
212	37.311534	10.10.1.19	10.10.1.11	TCP	66	[TCP Keep-Alive ACK] 80 → 16931 [ACK] Seq=27723 Ack=1282 Win=2...
213	47.321141	10.10.1.11	10.10.1.19	TCP	55	[TCP Keep-Alive] 16931 → 80 [ACK] Seq=1281 Ack=27723 Win=26265...
214	47.321168	10.10.1.19	10.10.1.11	TCP	66	[TCP Keep-Alive ACK] 80 → 16931 [ACK] Seq=27723 Ack=1282 Win=2...

> Frame 1: 174 bytes on wire (Ethernet II, Src: MS-NLBS, Dst: 01:00:00:00:00:00, Protocol: Internet Protocol Version 4, Src: 10.10.1.11, Dst: 10.10.1.19, User Datagram Protocol, Src Port: 49799, Dst Port: 443, Multicast Domain Name System, Seq: 1244, Win: 0, Len: 0)

0000 33 33 00 00 00 fb 02 15 5d 64 82 09 86 dd 60 04 33 ..... ]d .....  
0010 66 48 00 78 11 ff fe 80 00 00 00 00 00 00 15 fh x .....  
0020 5d ff fe 64 82 09 ff 02 00 00 00 00 00 00 00 ] . d .....  
0030 00 00 00 00 00 fb 14 e9 14 e9 00 78 bd 6c 00 00 ..... x .....  
0040 00 00 00 02 00 00 00 02 00 00 10 61 64 62 2d 75 ..... adb-u .....  
0050 6e 69 64 65 6e 74 69 66 69 65 64 04 5f 61 64 62 nidentif ied adb .....  
0060 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 ff 00 01 \_tcp lo cal .....  
0070 07 41 6e 64 72 6f 69 64 c0 27 00 ff 00 01 c0 0c -Android .....  
0080 00 21 00 01 00 00 78 00 08 00 00 00 15 b3 + ..... x .....  
0090 c0 32 c0 32 00 1c 00 01 00 00 78 00 10 fe 80 -2.2 ..... x .....  
00a0 00 00 00 00 00 00 15 5d ff fe 64 82 09 ..... ] . d .....

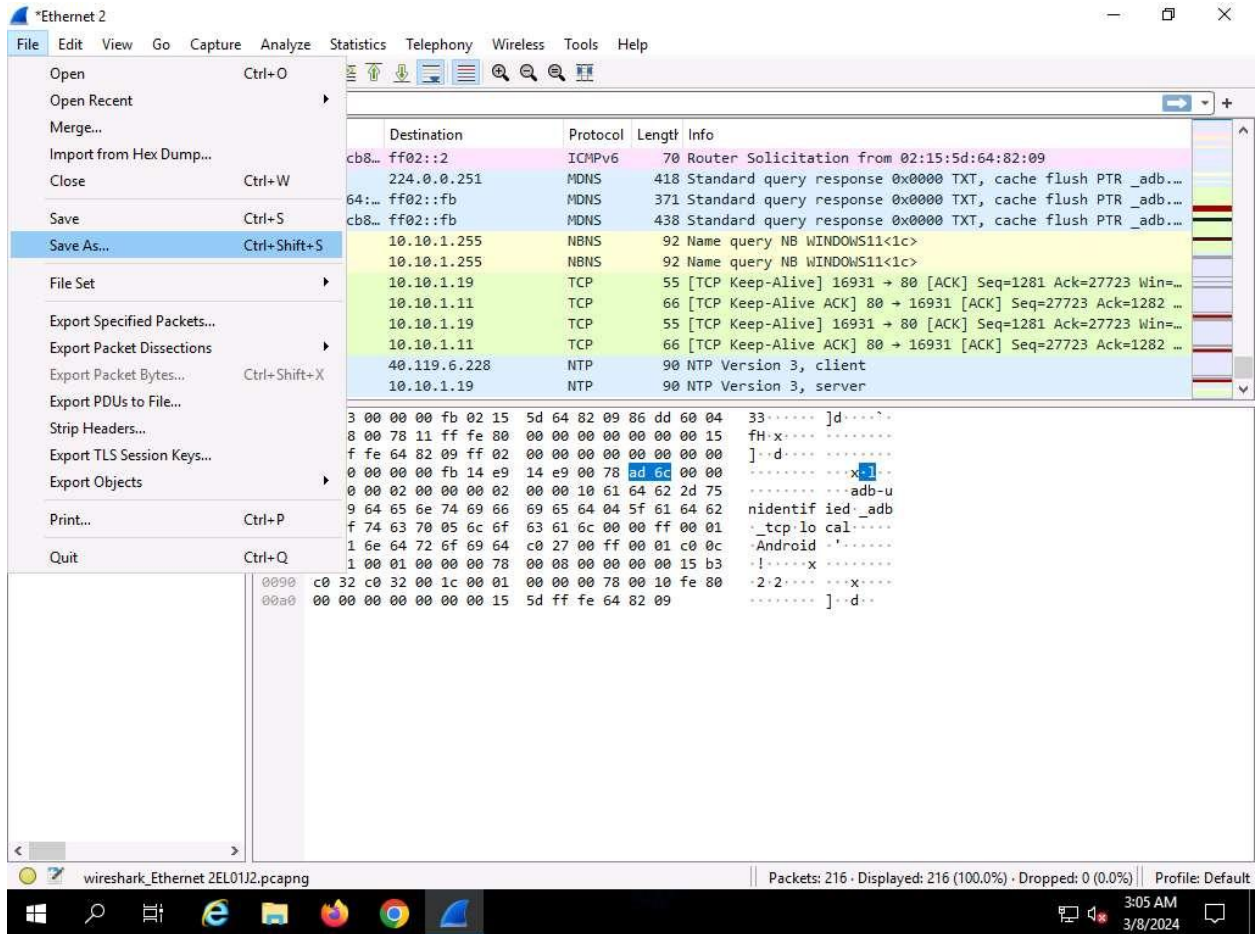
Bytes 60-61: Checksum (udp.checksum)

Packets: 214 · Displayed: 214 (100.0%)

Profile: Default

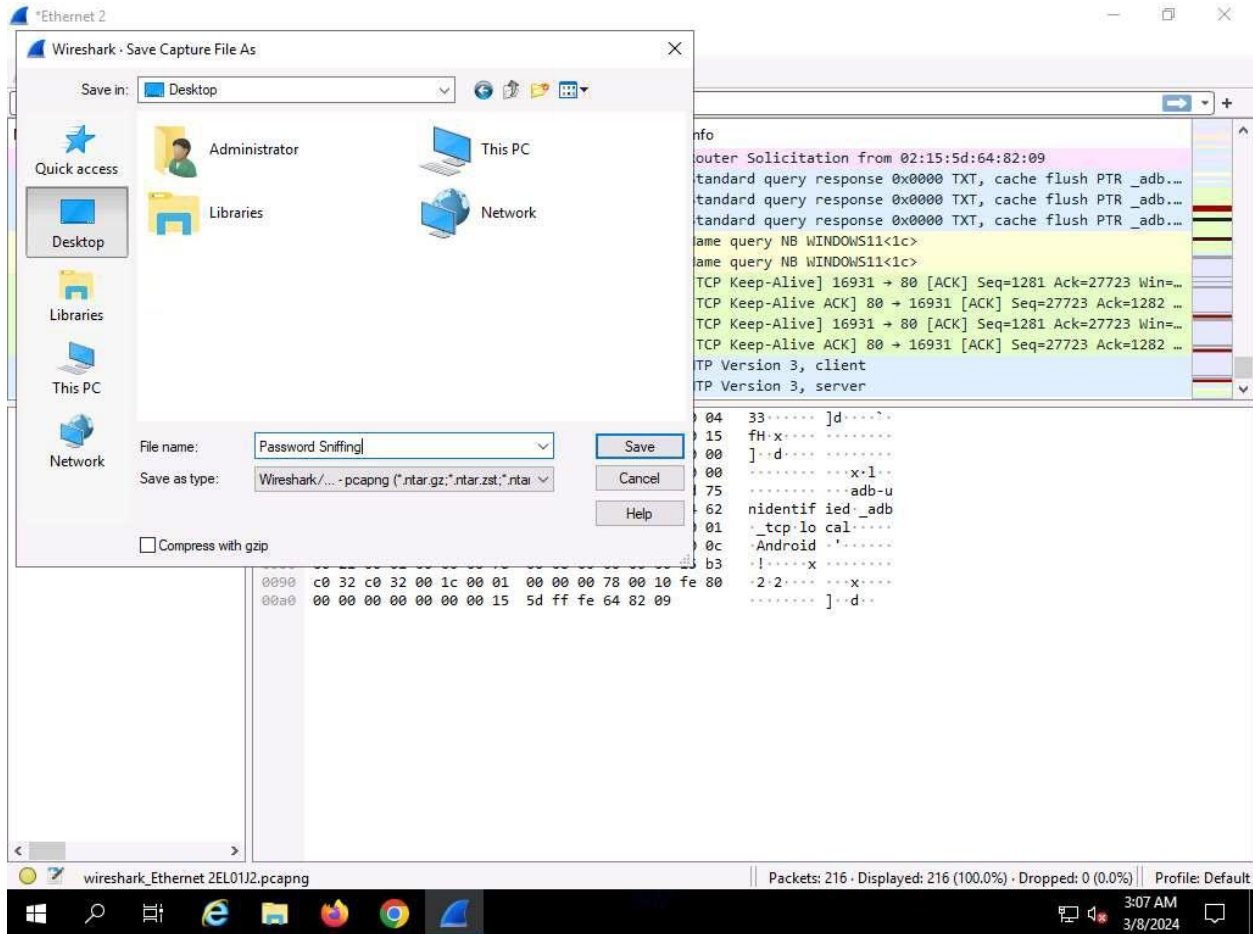
3:04 AM  
3/8/2024

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



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





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

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

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

Password Sniffing.pcapng

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&clid=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

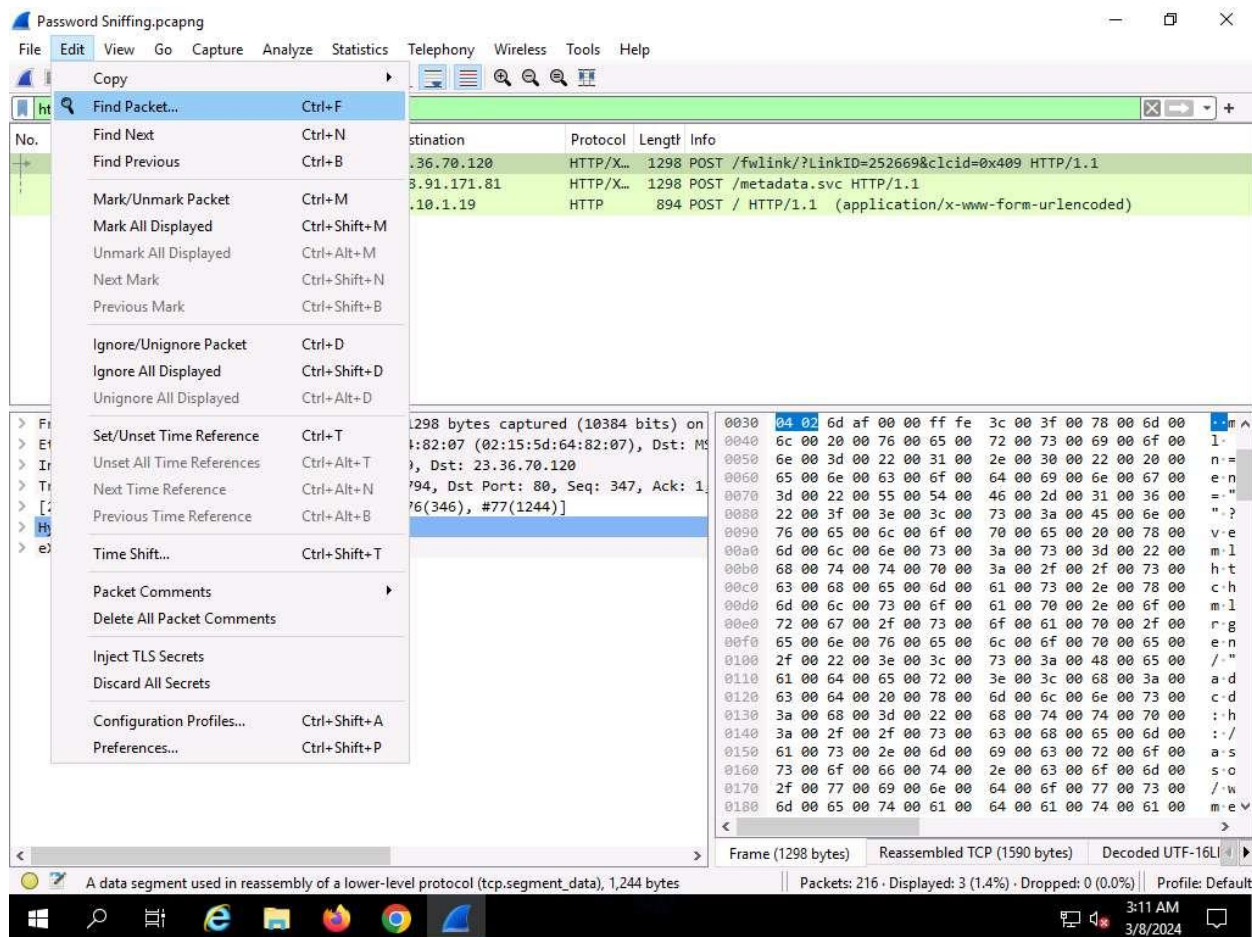
Frame (1298 bytes) Reassembled TCP (1590 bytes) Decoded UTF-16L

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

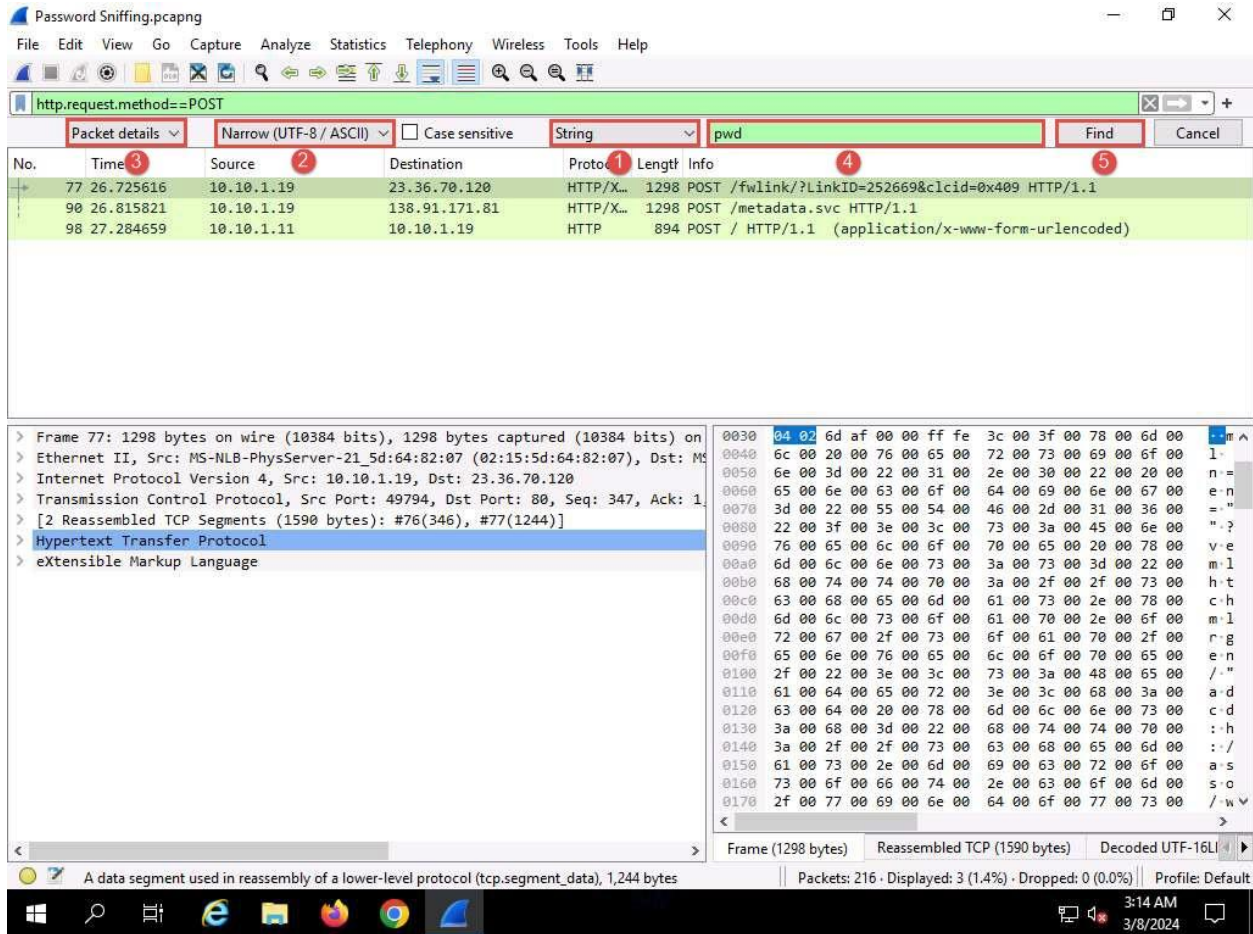
3:10 AM 3/8/2024

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

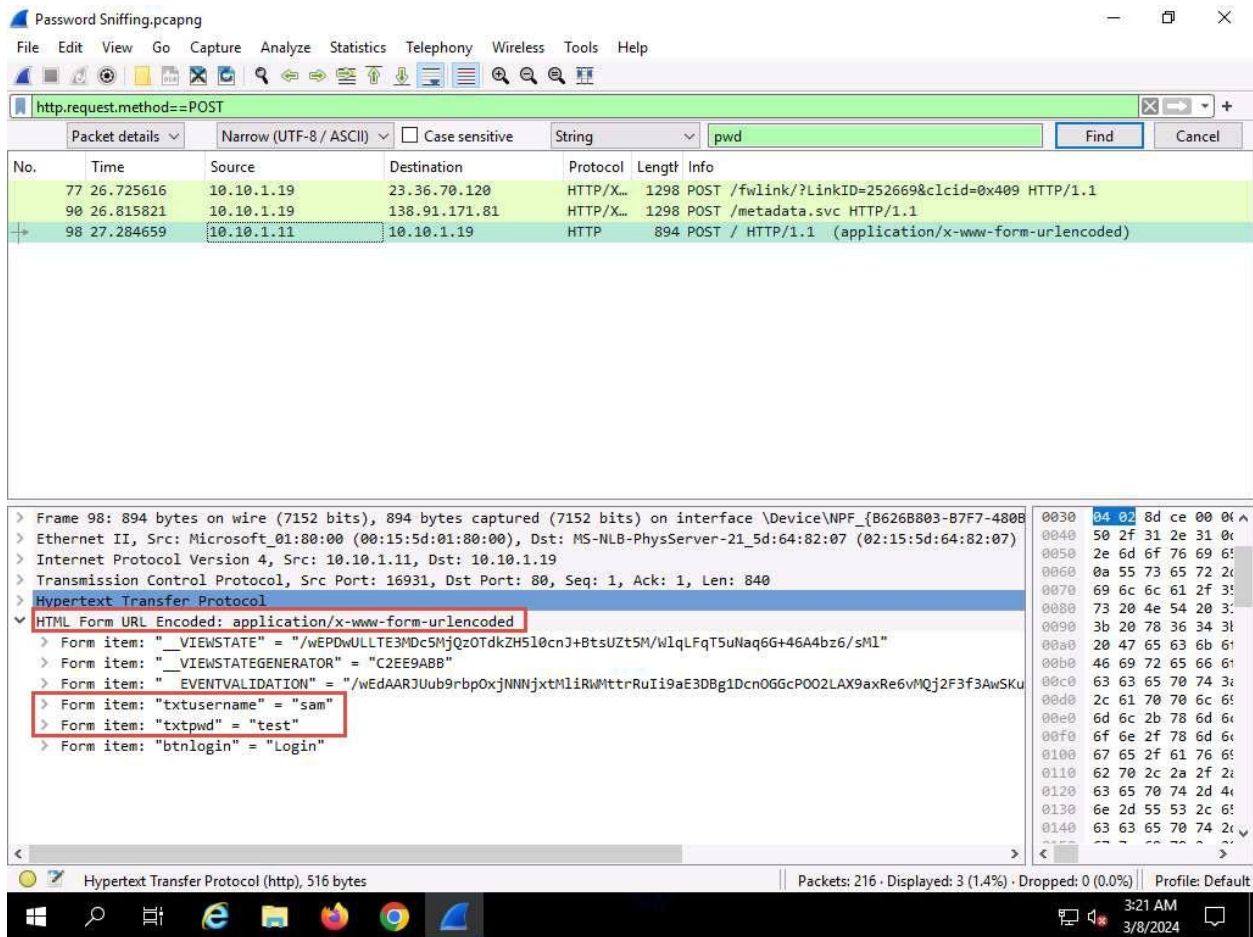


14. The **Find Packet** section appears below the display filter field.
15. Click **Display filter**, select **String** from the drop-down options, click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options and click **Packet list**, select **Packet details** from the drop-down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



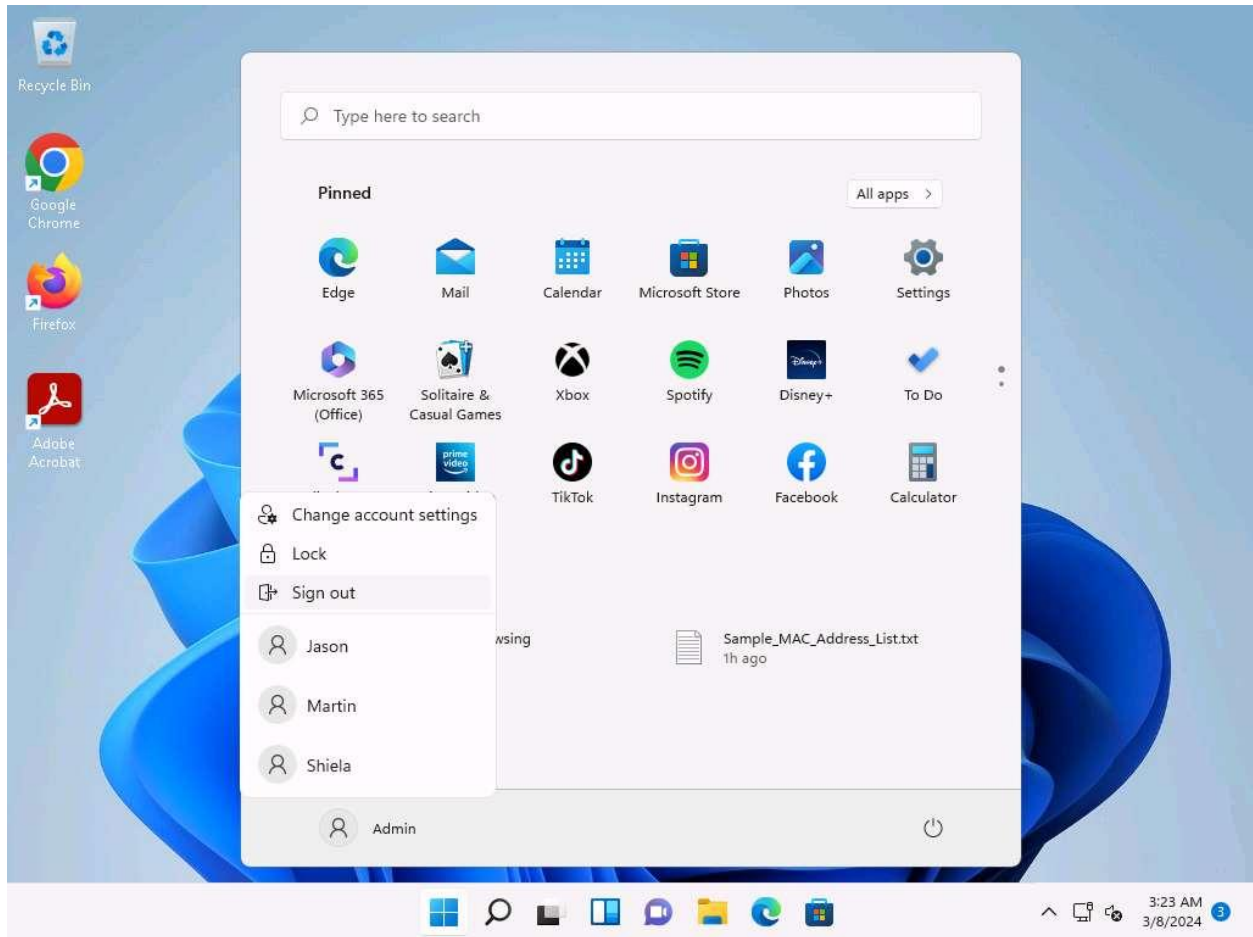


17. Wireshark will now display the sniffed password from the captured packets.
18. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** node from the packet details section, and view the captured username and password, as shown in the screenshot.



19. Close the **Wireshark** window.

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

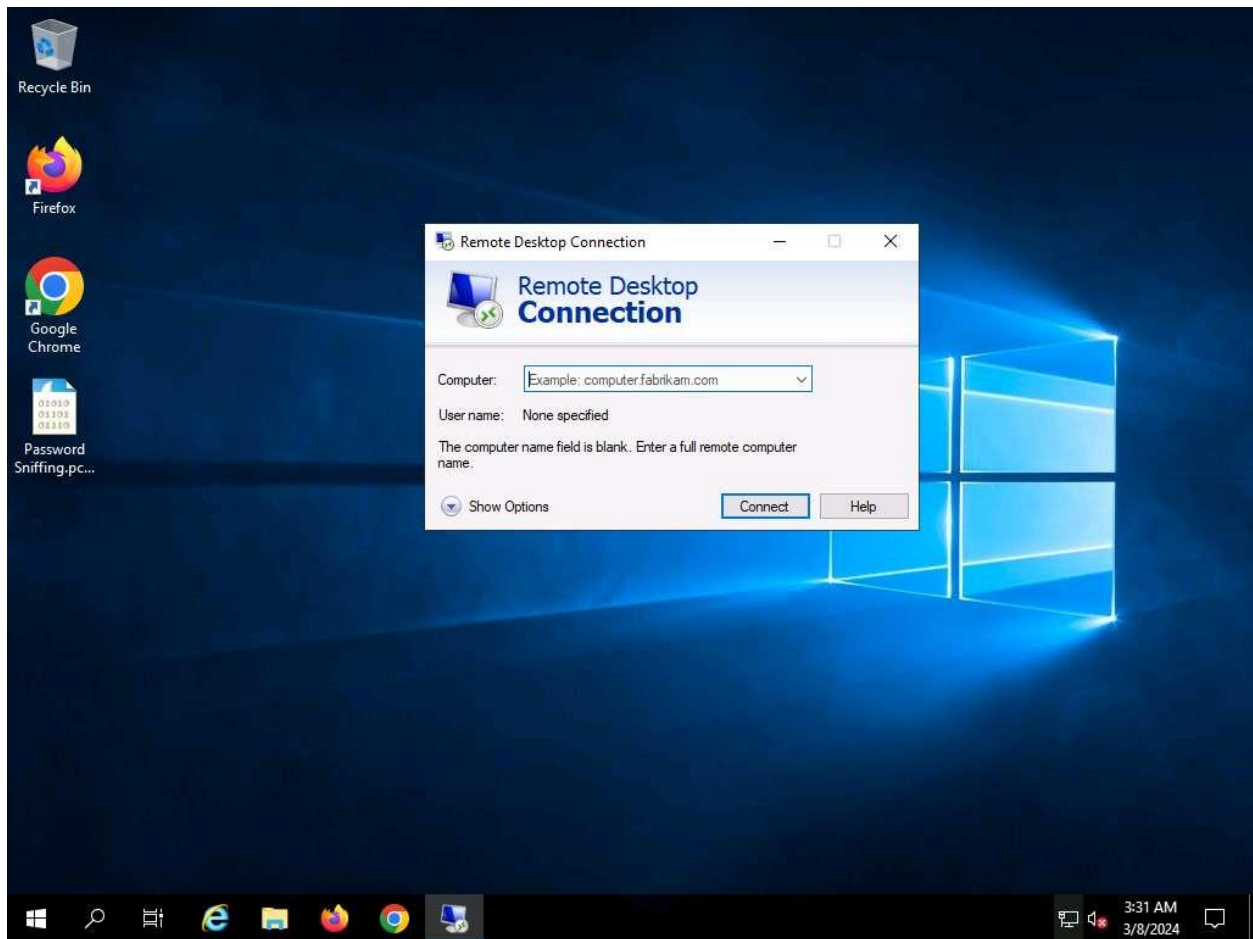


21. Click [Windows Server 2019](#) to switch back to the **Windows Server 2019** machine.

22. Search **Remote Desktop Connection** from search bar and launch it.

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

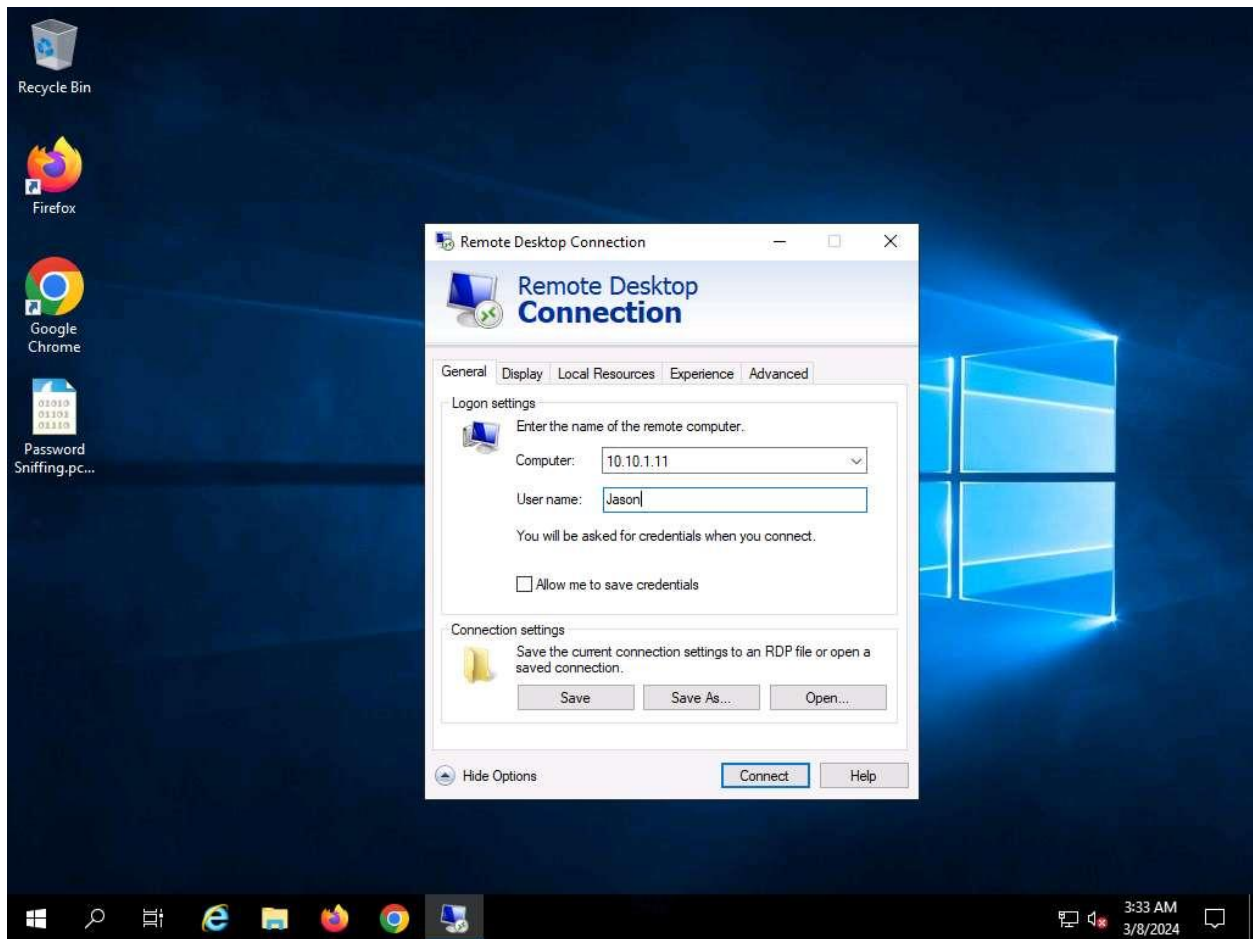
If some previously accessed IP address appears in the **Computer** field, delete it.



24. 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**.

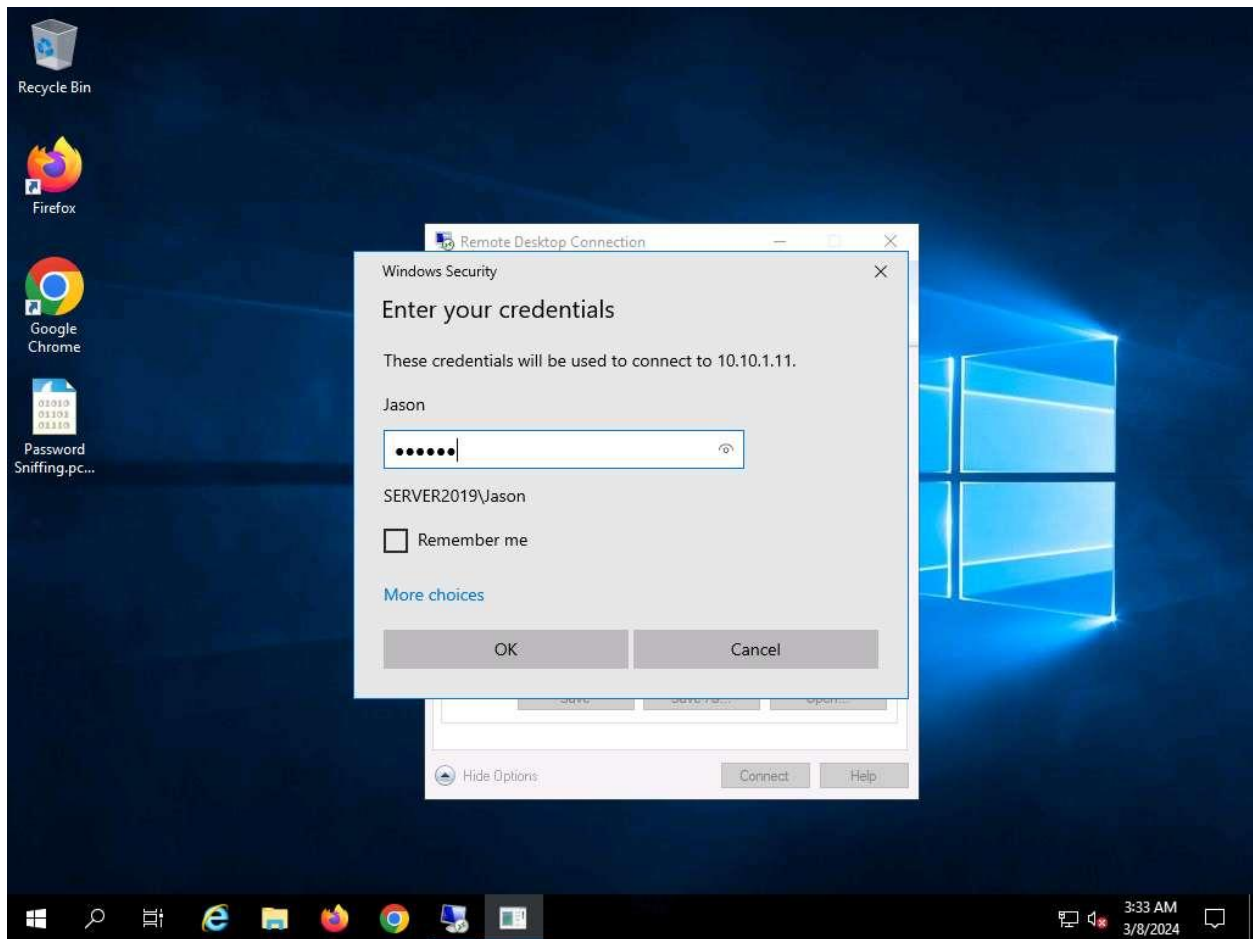
The IP address and username might differ in your lab environment. The target system credentials (**Jason** and **qwerty**) we are using here are obtained in the previous labs.



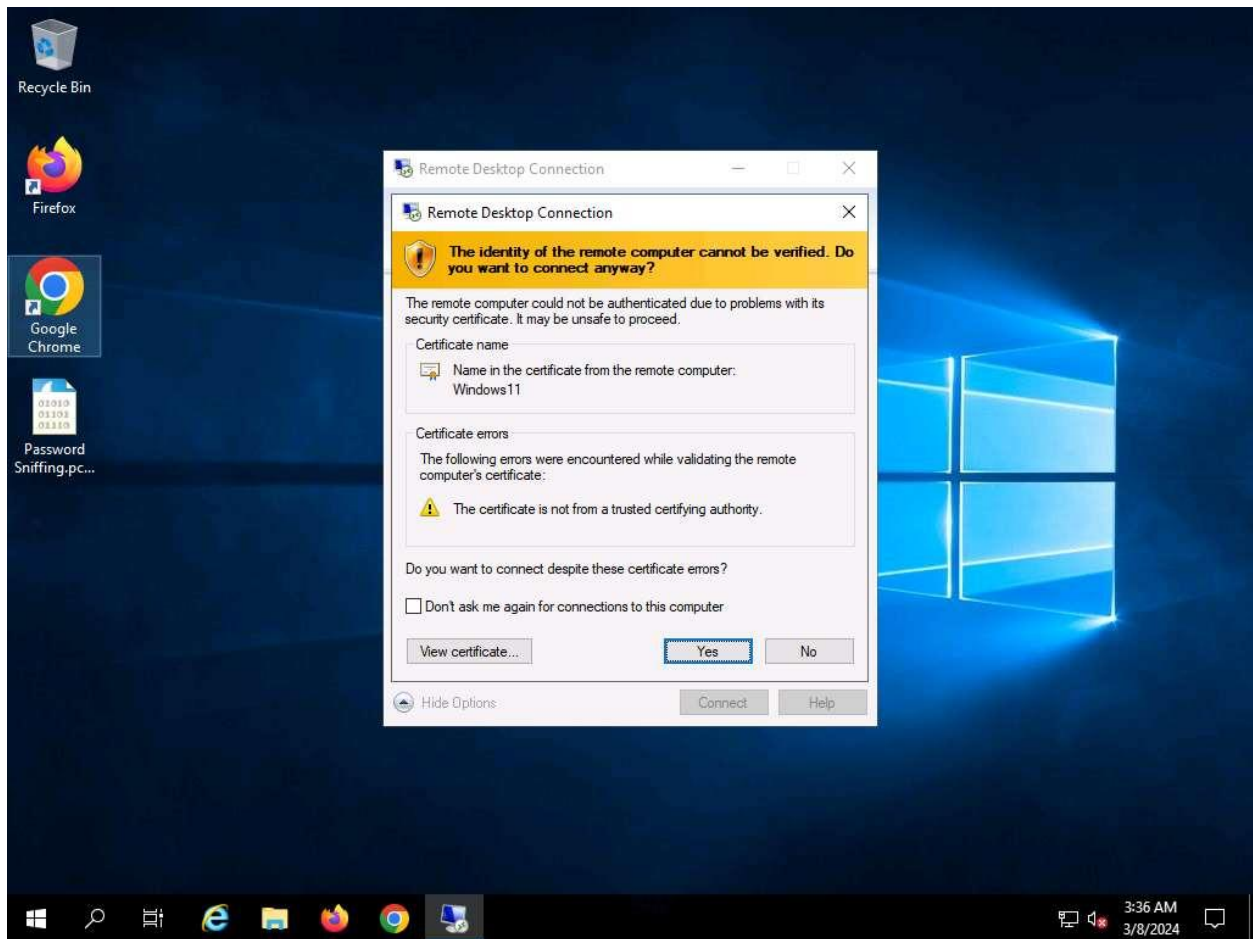


25. The **Windows Security** pop-up appears. Enter **Password (qwerty)** and click **OK**.

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



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

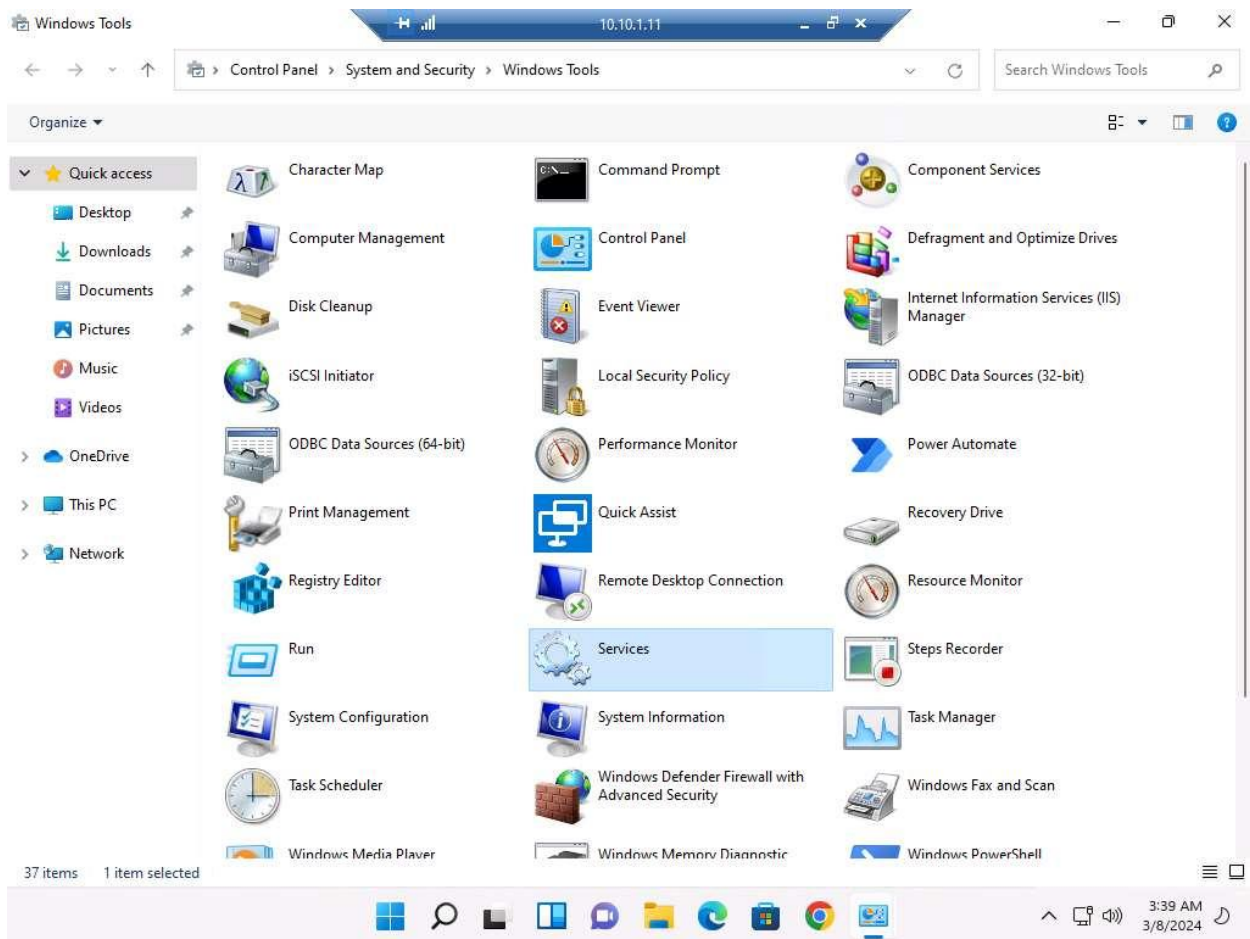


27. A remote connection to the target system (**Windows 11**) appears.

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**.

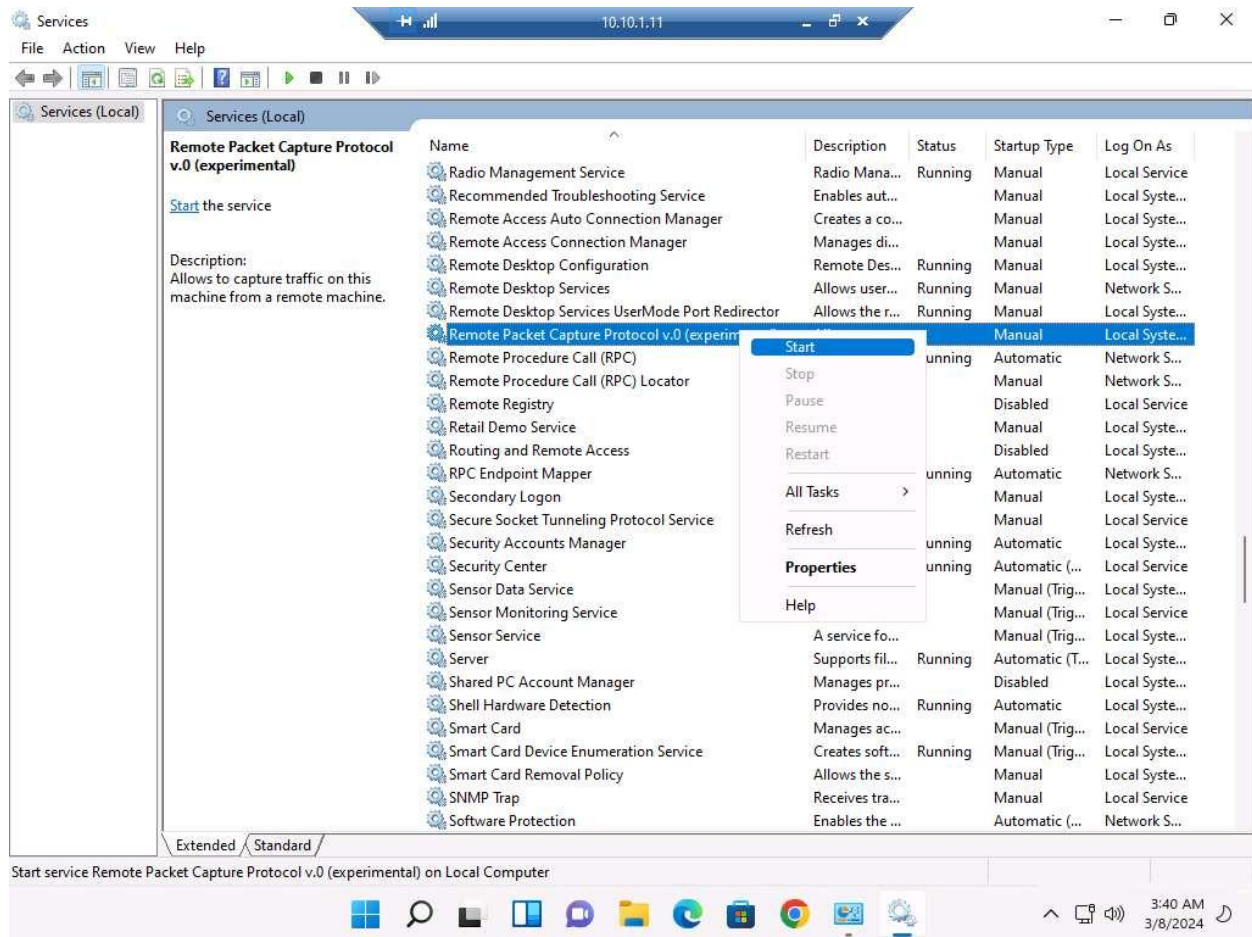
28. In the **Desktop** window, click windows **Search** icon and search for **Control Panel** in the search bar and launch it.

29. The **Control Panel** window appears; navigate to **System and Security --> Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.

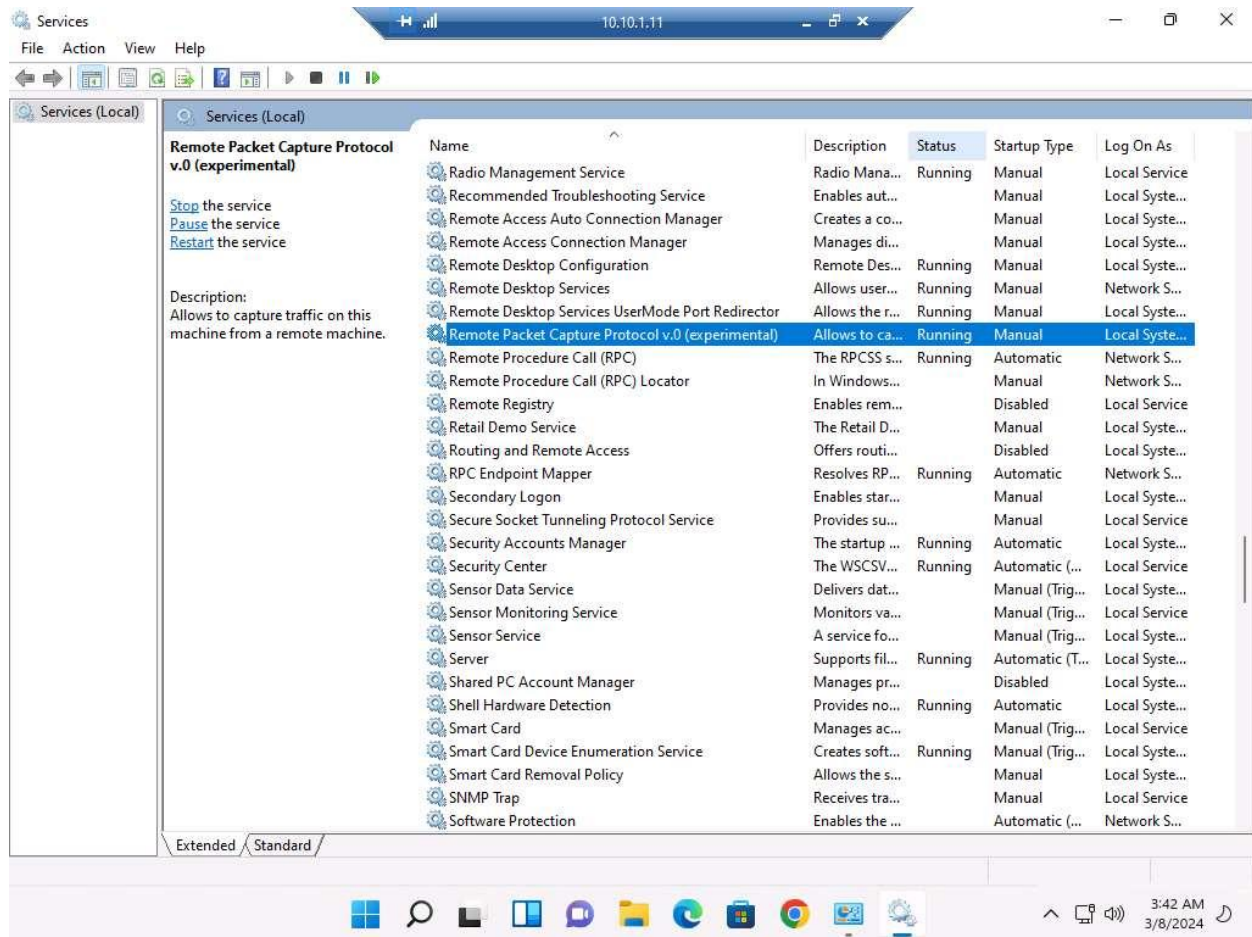


30. The **Services** window appears. Choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service, and click **Start**.





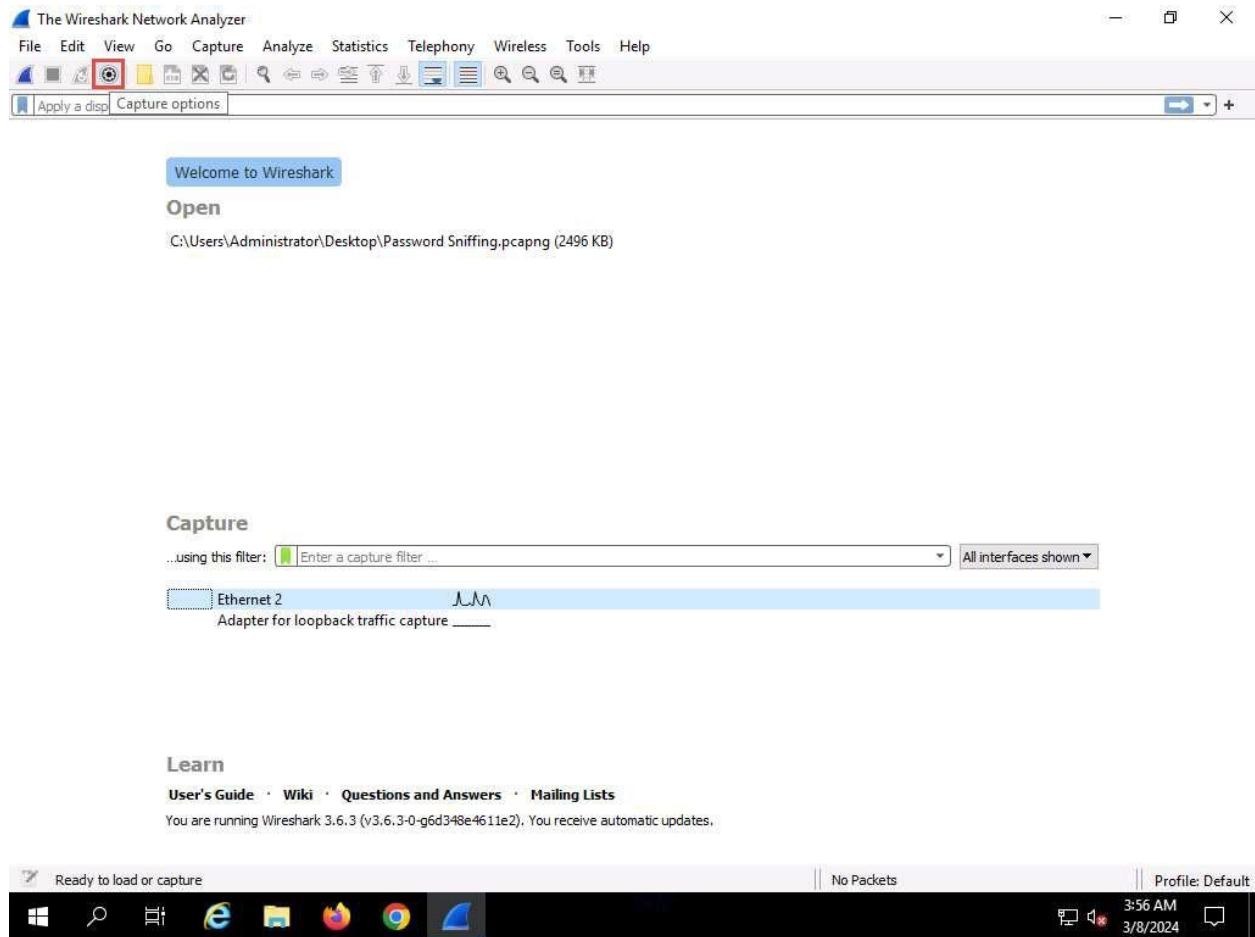
31. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.



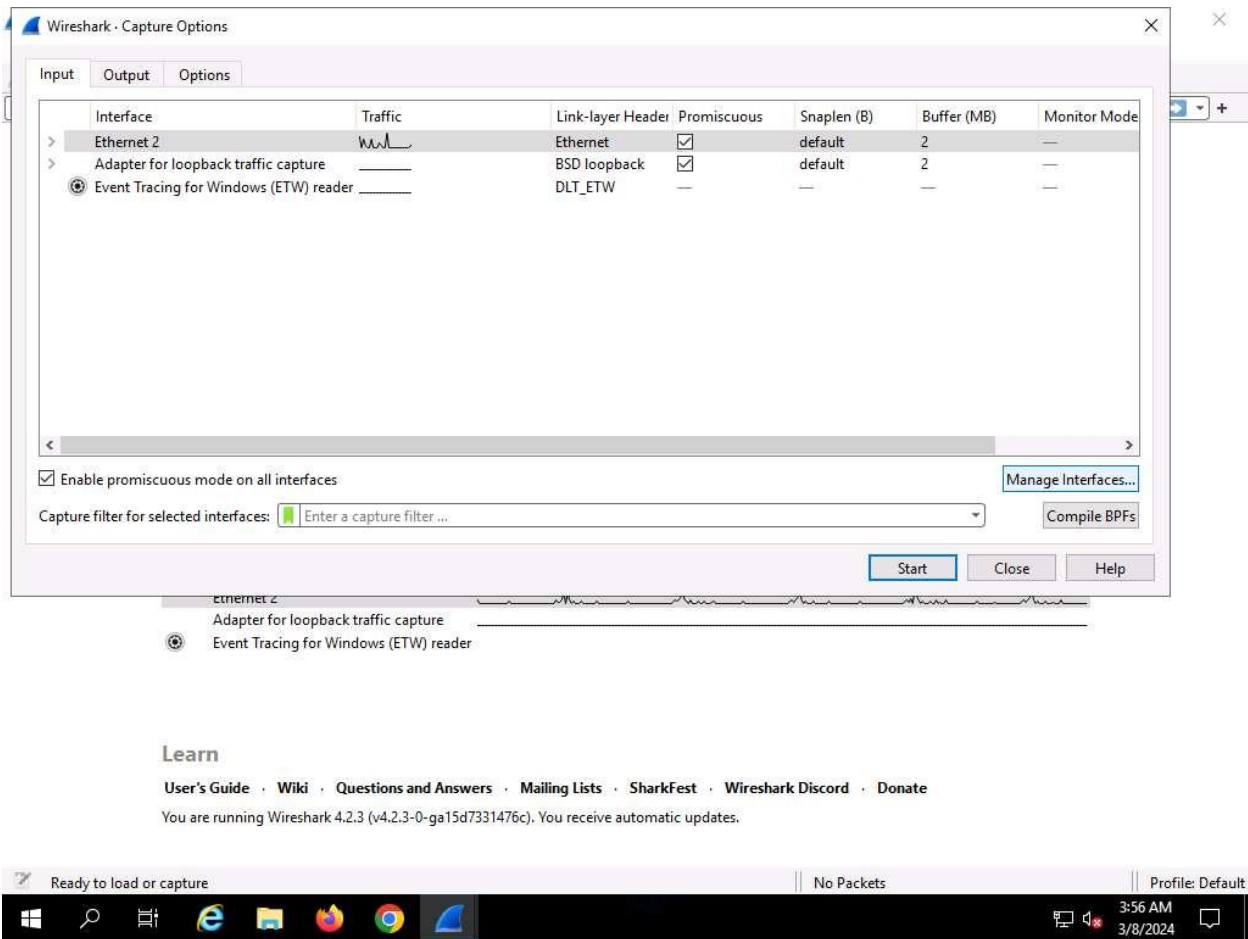
32. Close all open windows on the **Windows 11** machine and close **Remote Desktop Connection**.

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

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



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



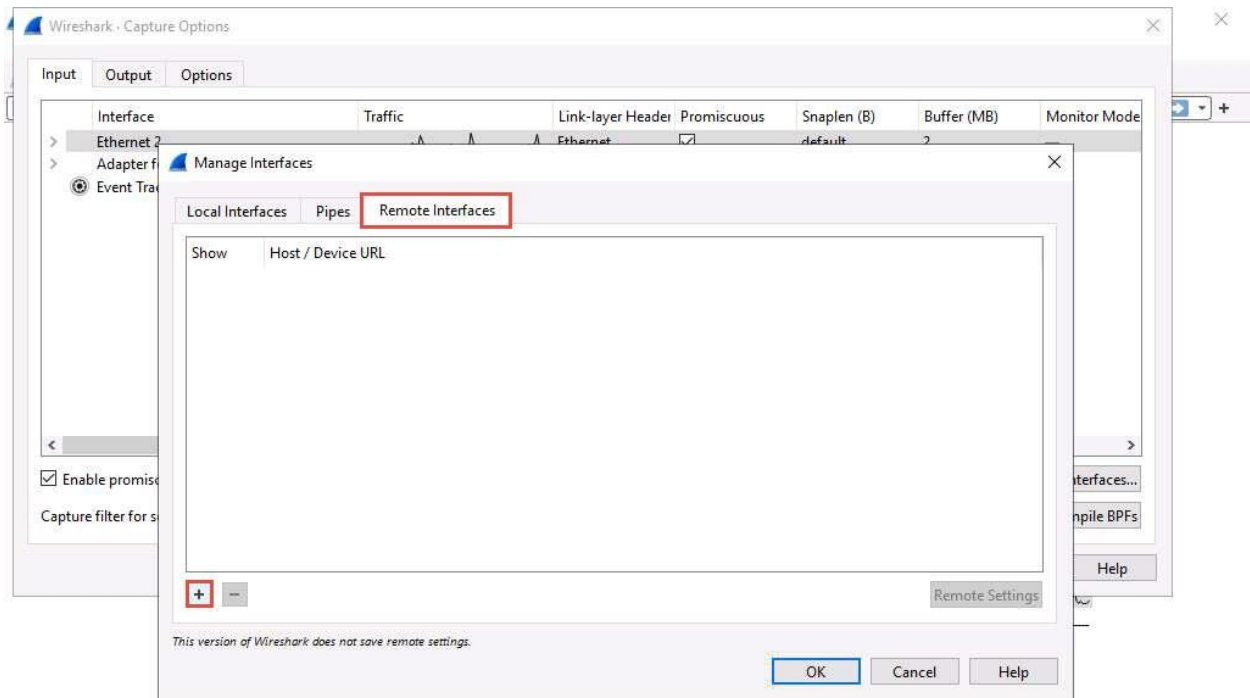
#### Learn

[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.

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





## Learn

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

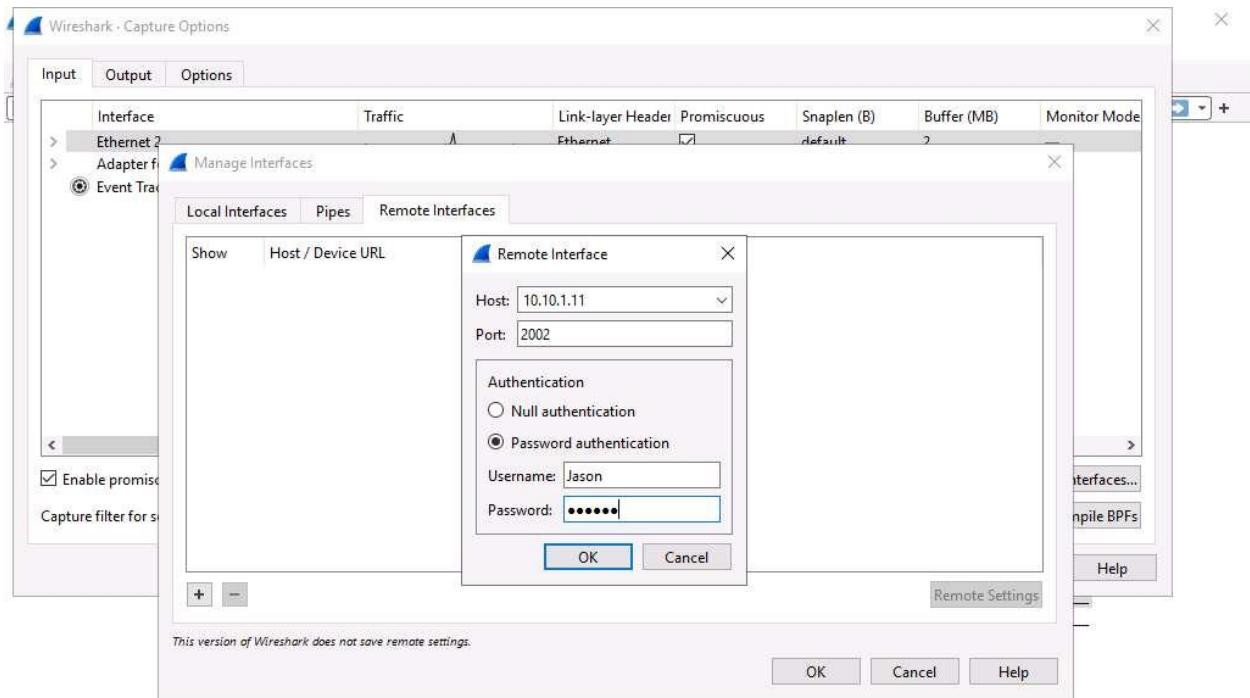
You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.



36. 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**.

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

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



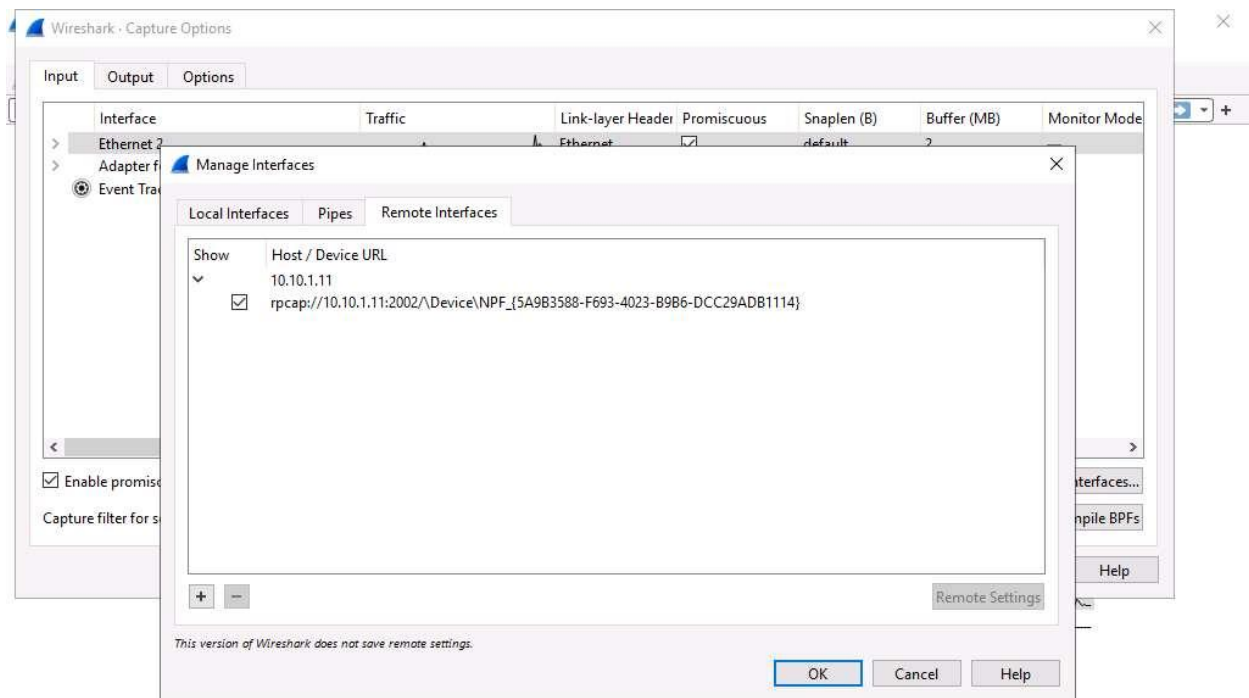
## Learn

[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.



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



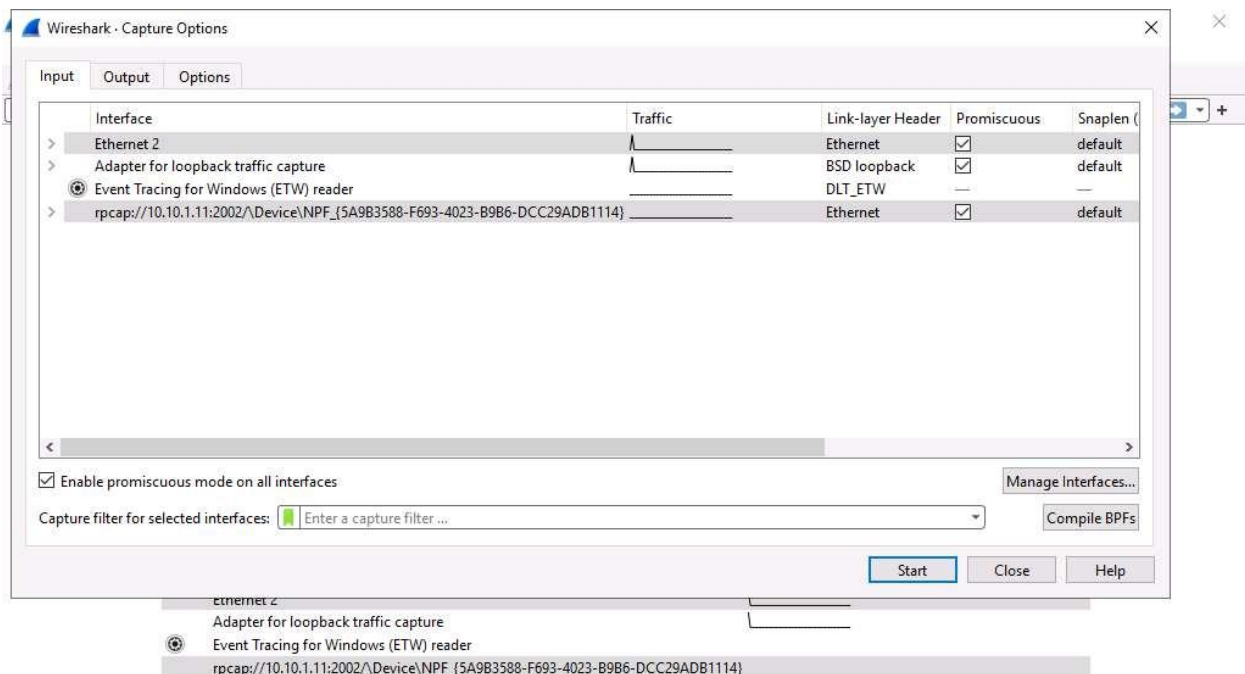
## Learn

[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.



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



## 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.

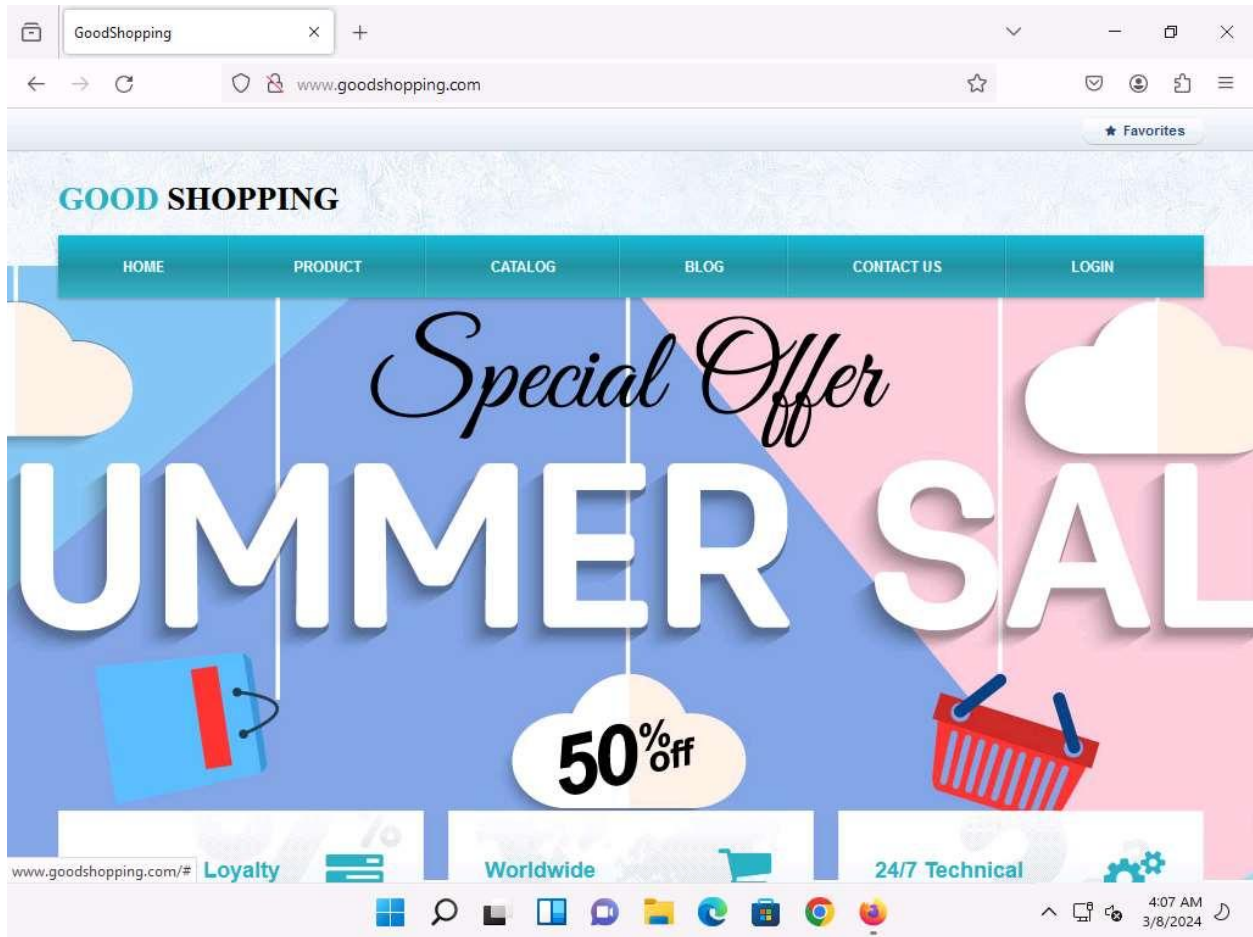


40. Click [Windows 11](#) to switch to the **Windows 11** machine, and login using **Jason/qwerty**. Here, you are signing in as the victim.

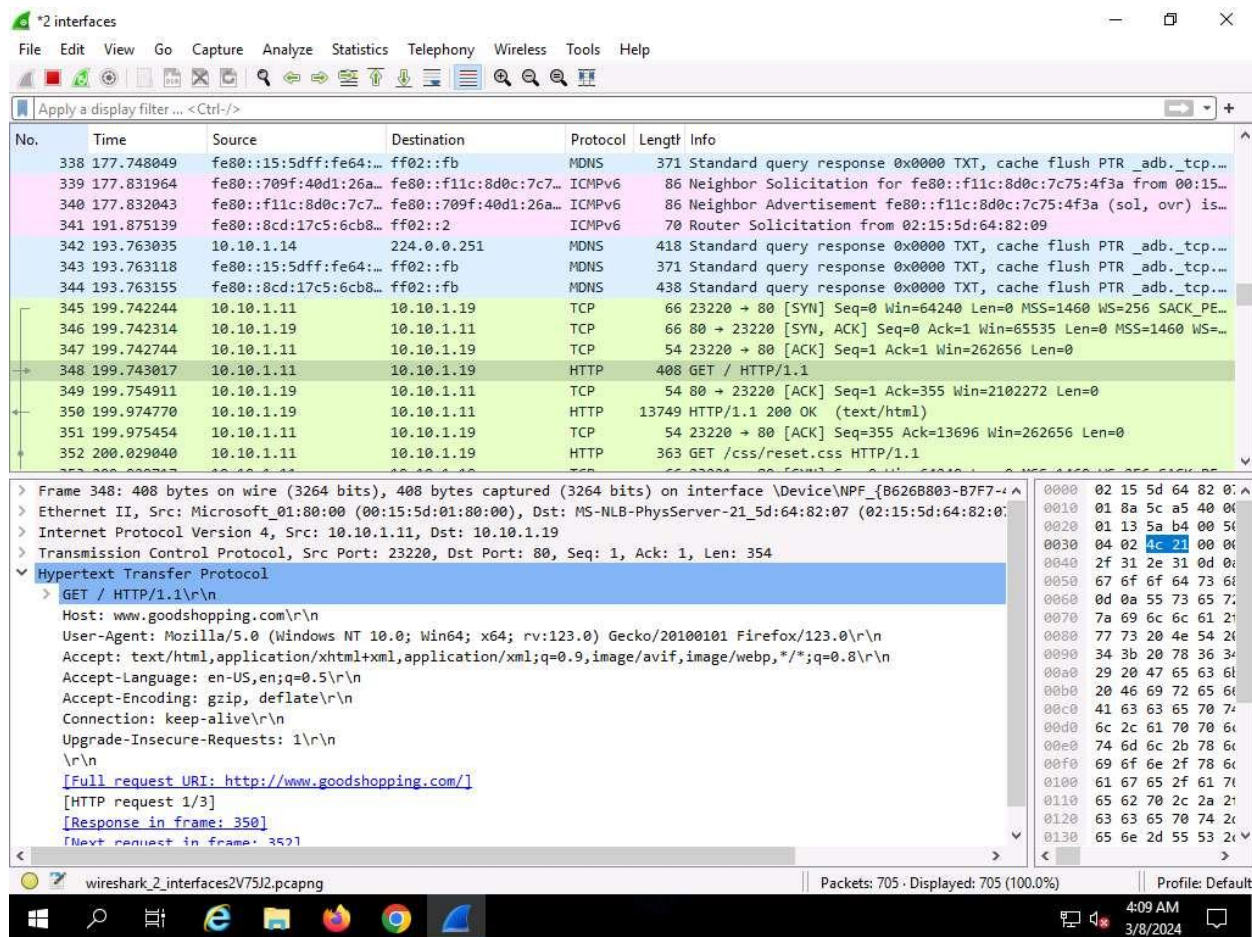
41. Acting as the target, open any web browser go to **<http://www.goodshopping.com>** (here, we are using **Mozilla Firefox**).

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





42. 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, the shown in the screenshot.



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

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

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.

45. This concludes the demonstration of how to perform password sniffing using Wireshark.

46. 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?