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**.

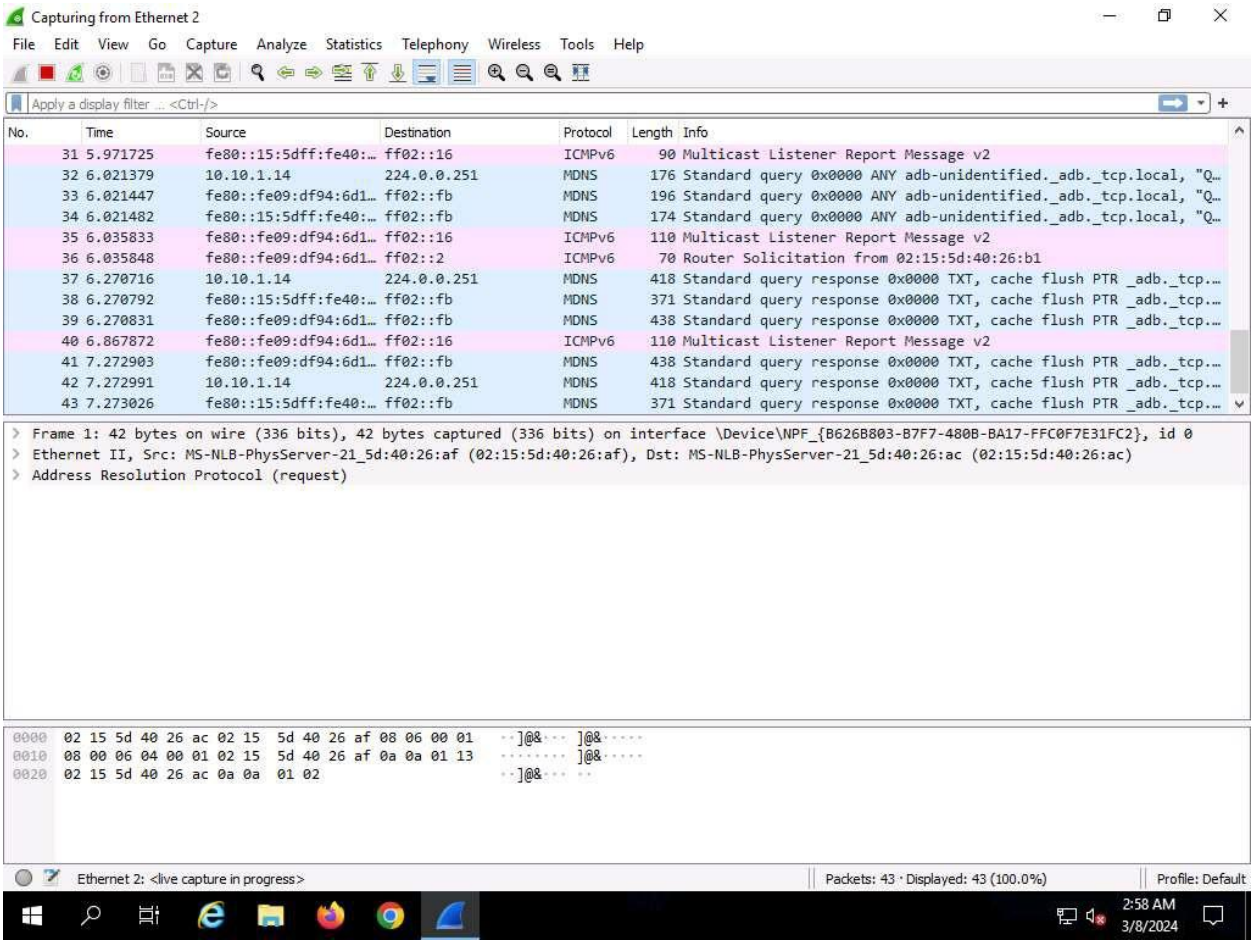
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

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.



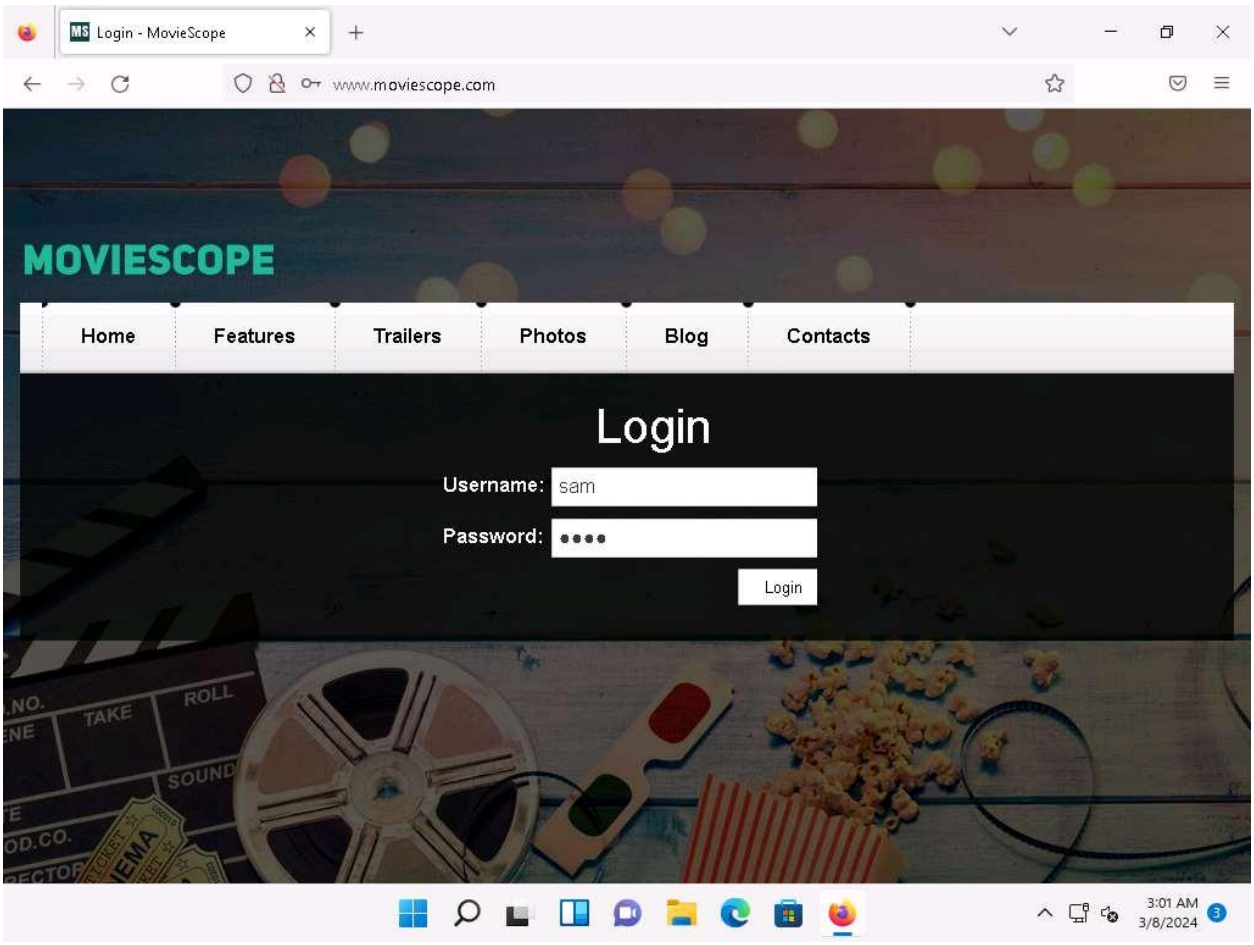
5. Now, click Windows 11 to switch to the **Windows 11** machine, login using **Admin/Pa$$w0rd**.

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

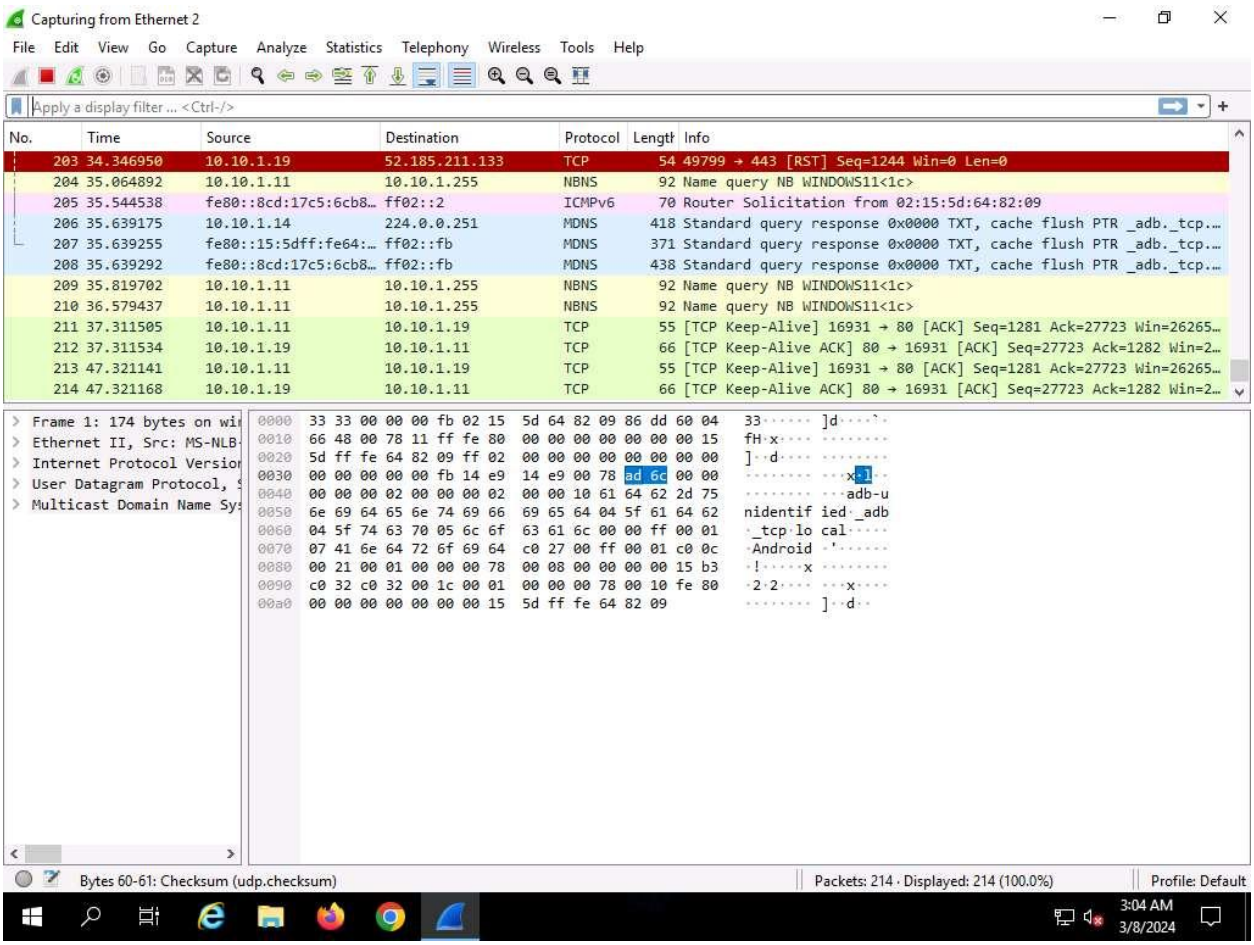
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

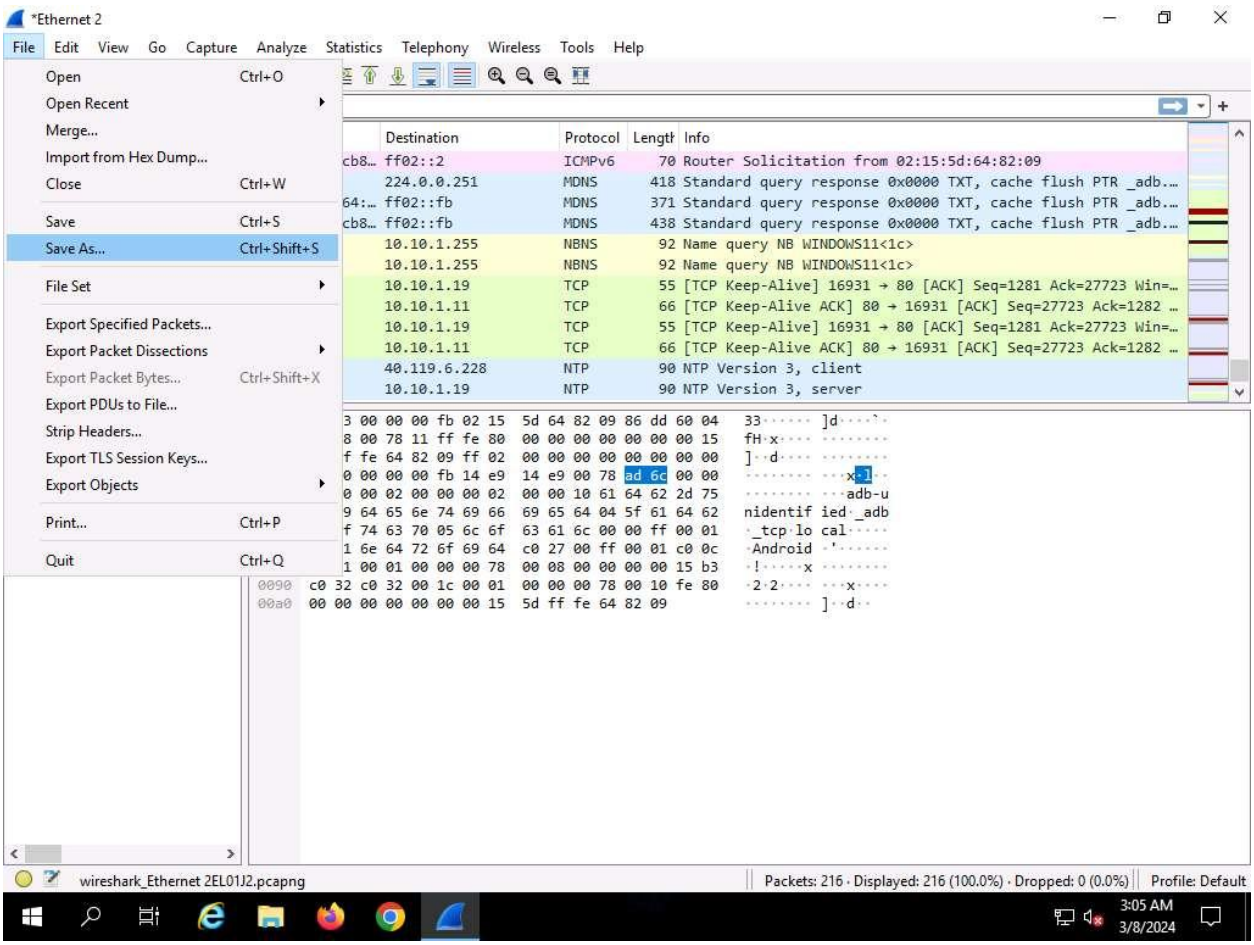
6. Open any web browser, and go to **http://www.moviescope.com/** (here, we are using **Mozilla Firefox**).
7. The **MOVIESCOPE** home page appears; login using **sam**/**test**.



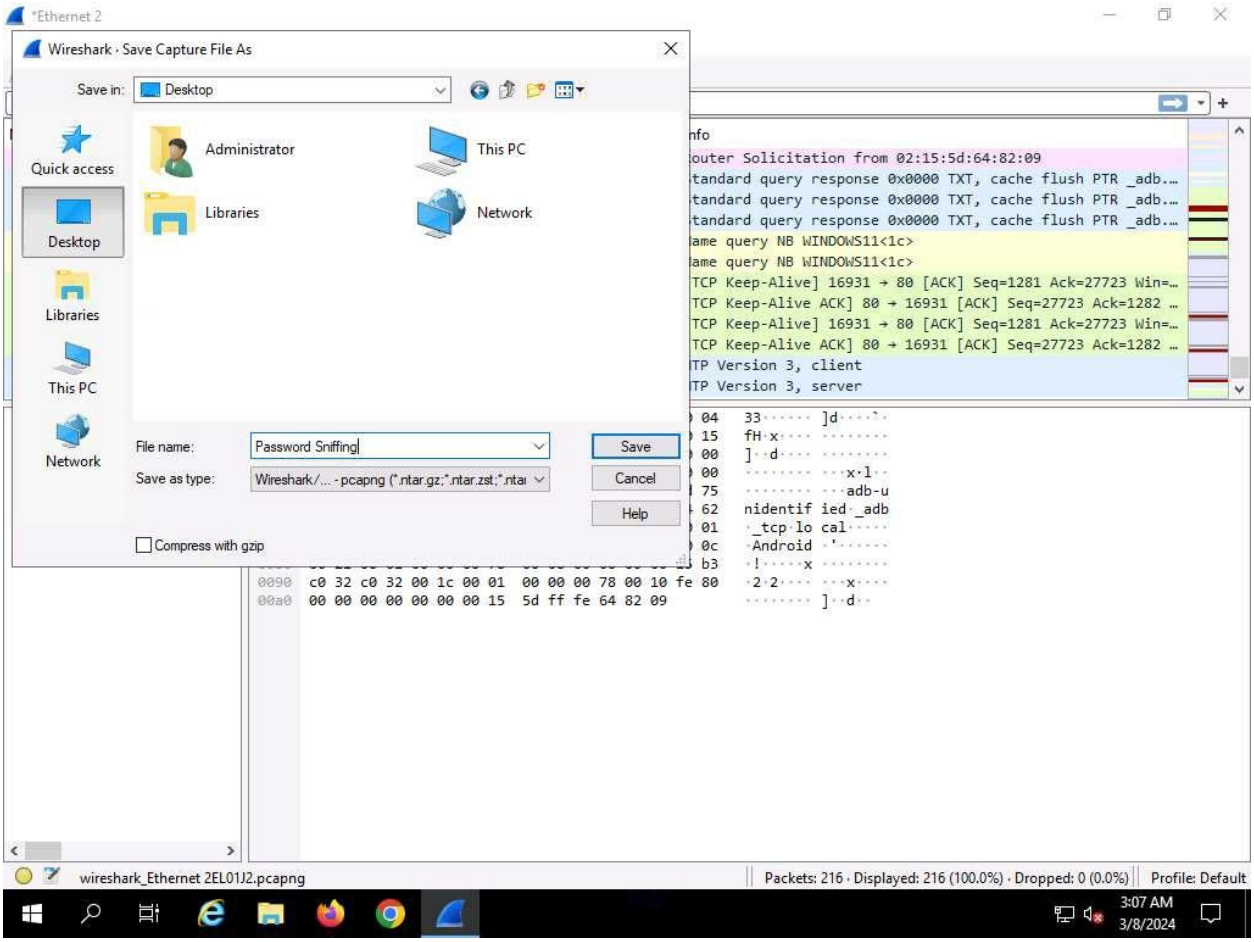
8. Click Windows Server 2019 to switch back to **Windows Server 2019** machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.



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



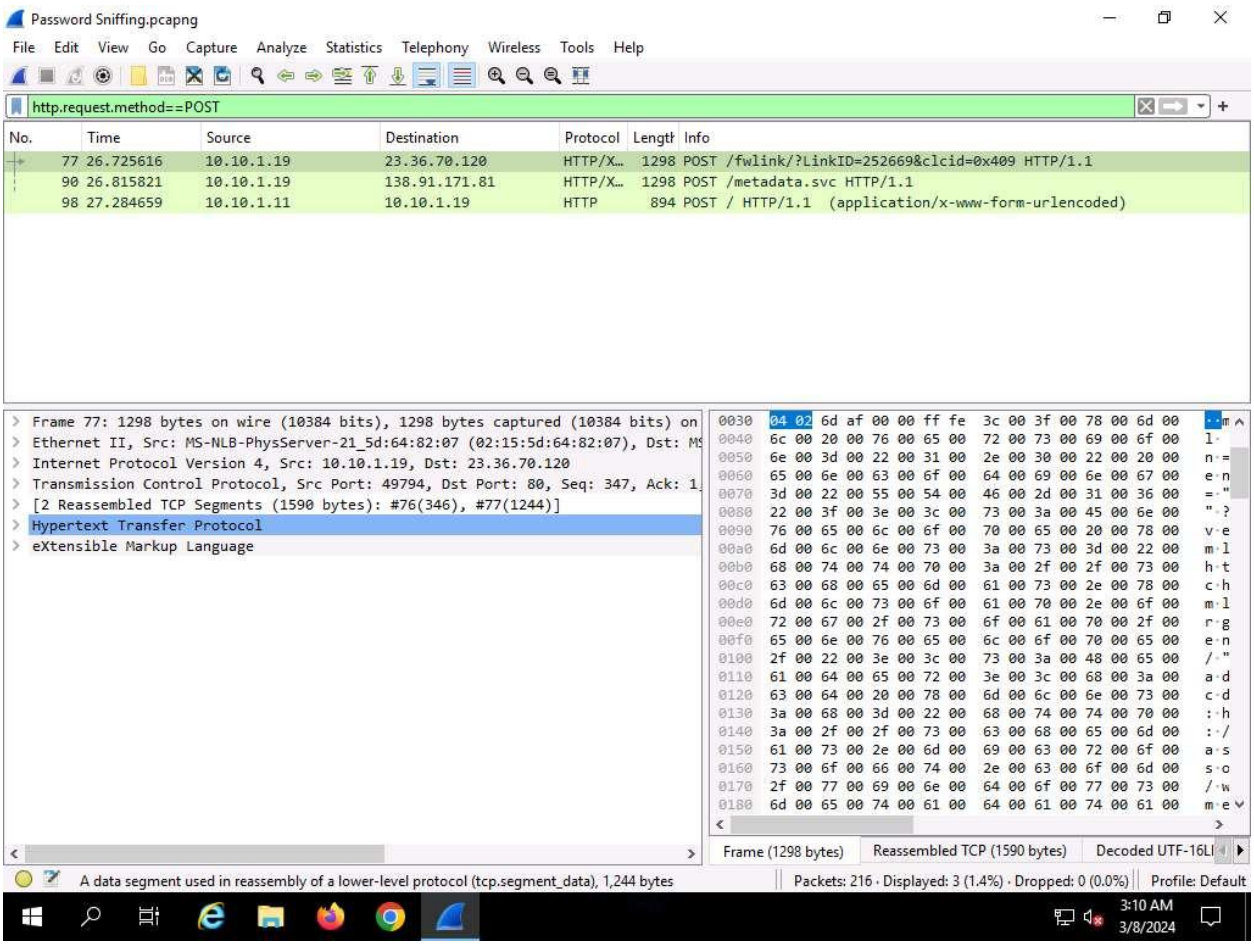
10. The **Wireshark: Save Capture File As** window appears. Select any location to save the file, specify **File name** as **Password Sniffing**, and click **Save**.



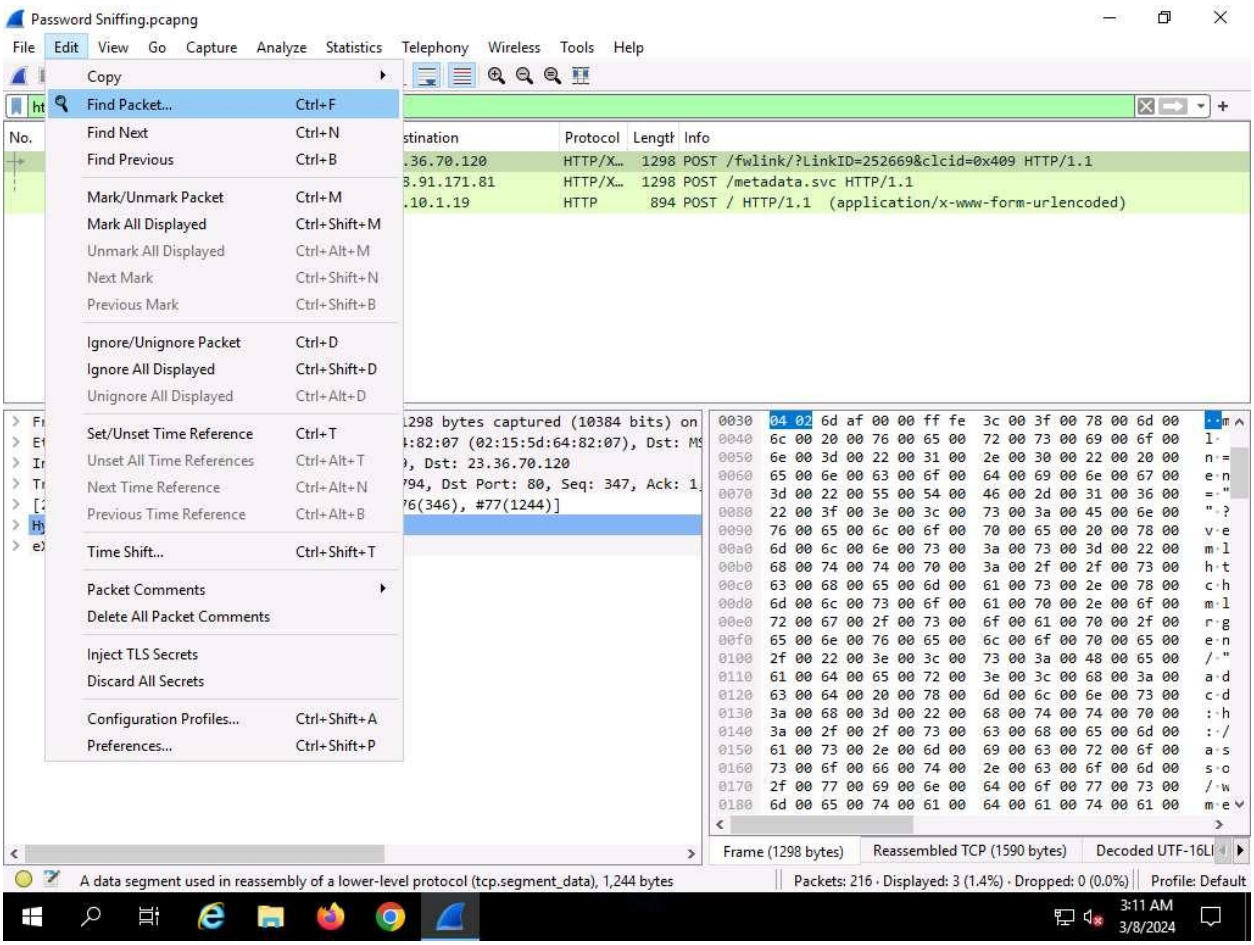
11. In the **Apply a display filter field**, type **http.request.method == POST** and click the arrow icon (**-->**) to apply the filter.

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.



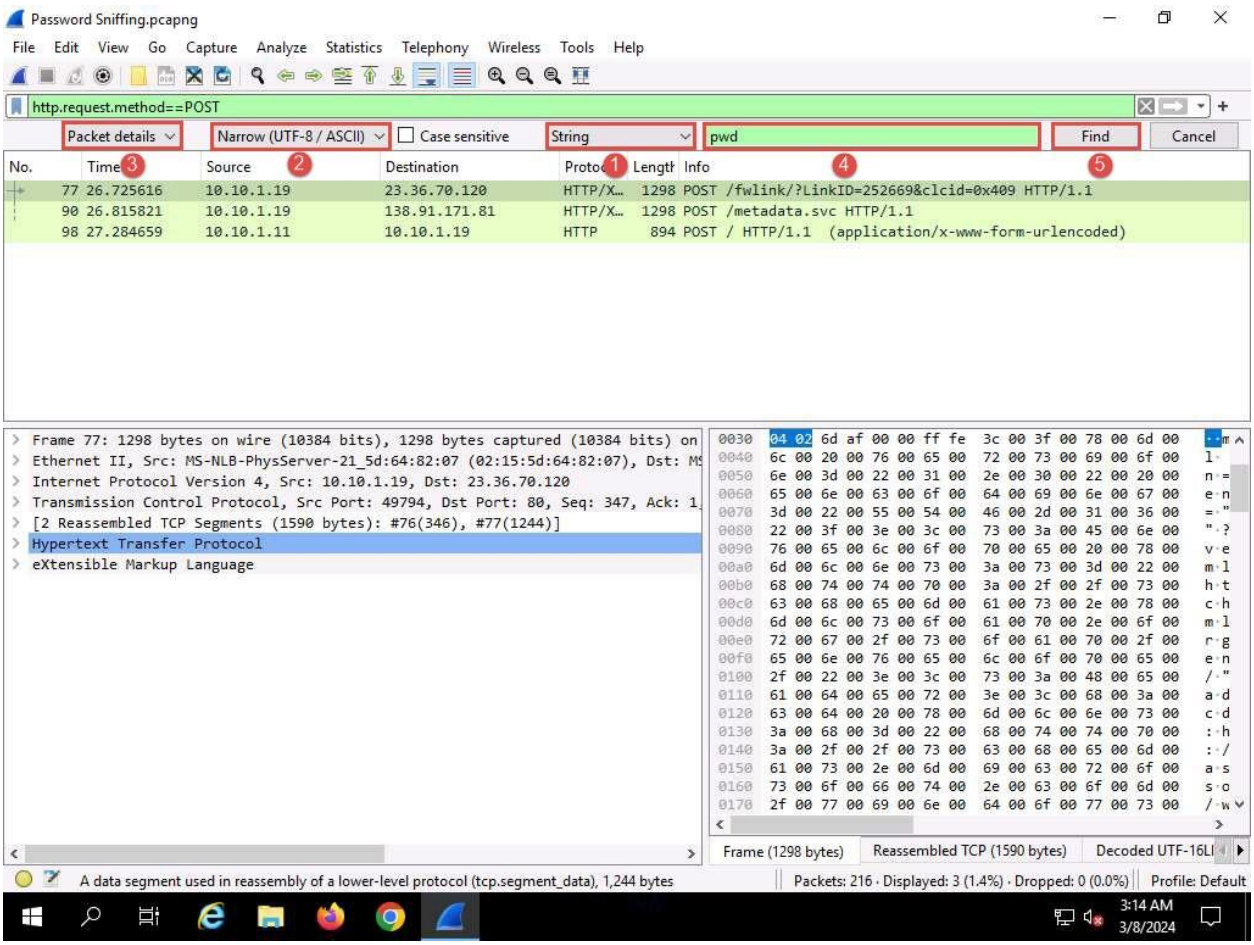
13. Now, navigate to **Edit** --> **Find Packet** from menu bar.



14. The **Find Packet** section appears below the display filter field.

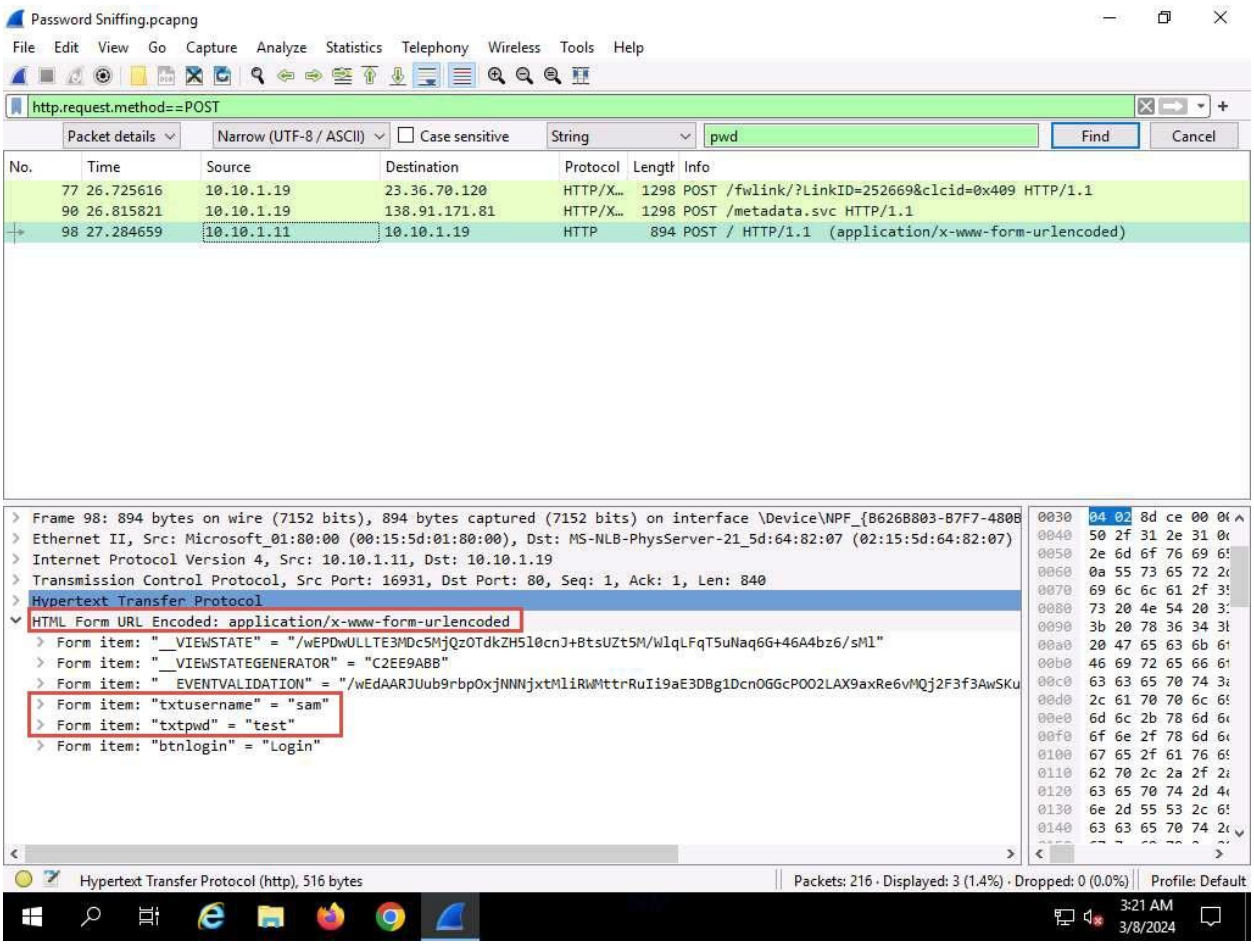
15. Click **Display filter**, select **String** from the drop-down options, click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options and click **Packet list**, select **Packet details** from the drop-down options.

16. In the field next to **String**, type **pwd** and click the **Find** button.

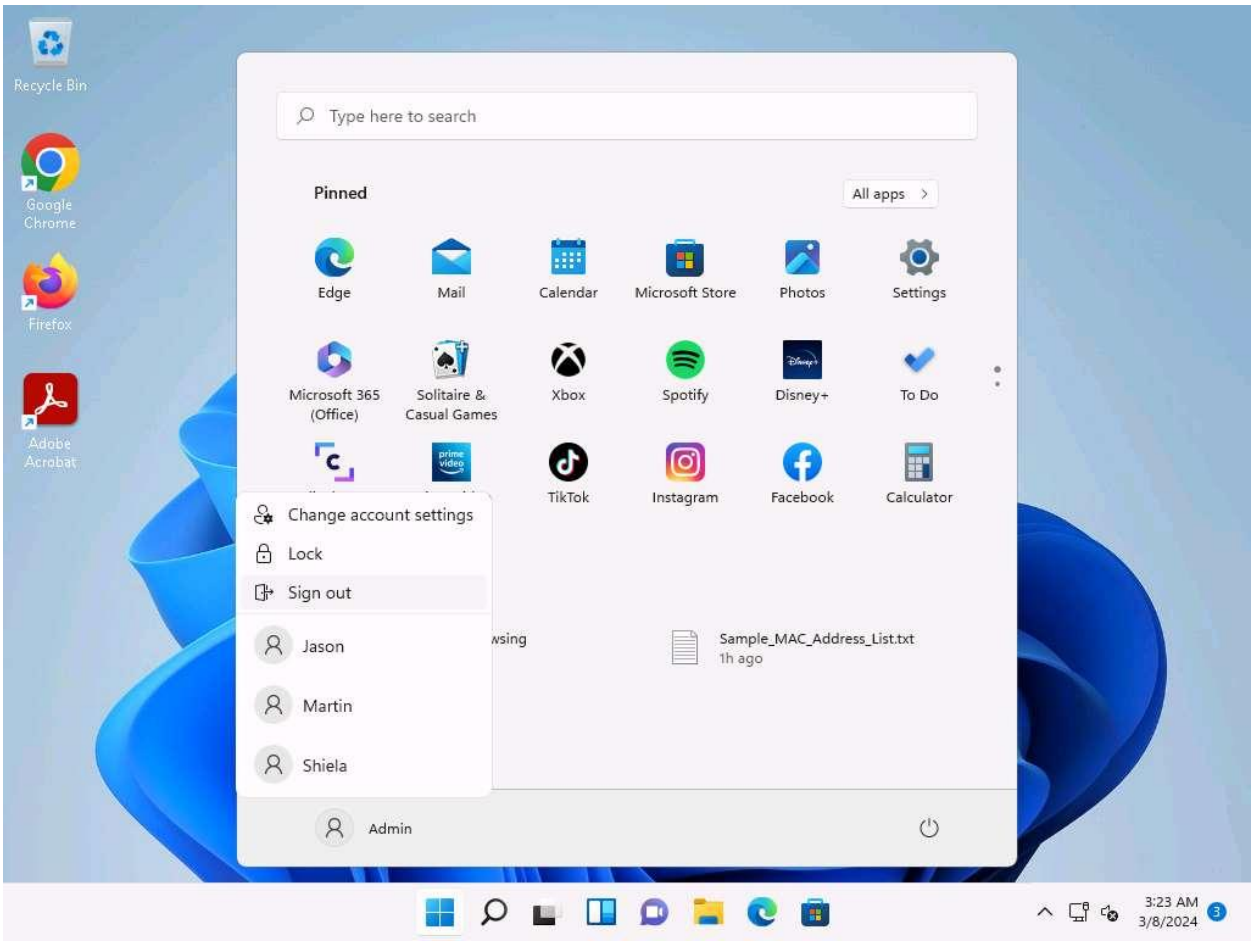


17. **Wireshark** will now display the sniffed password from the captured packets.

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.

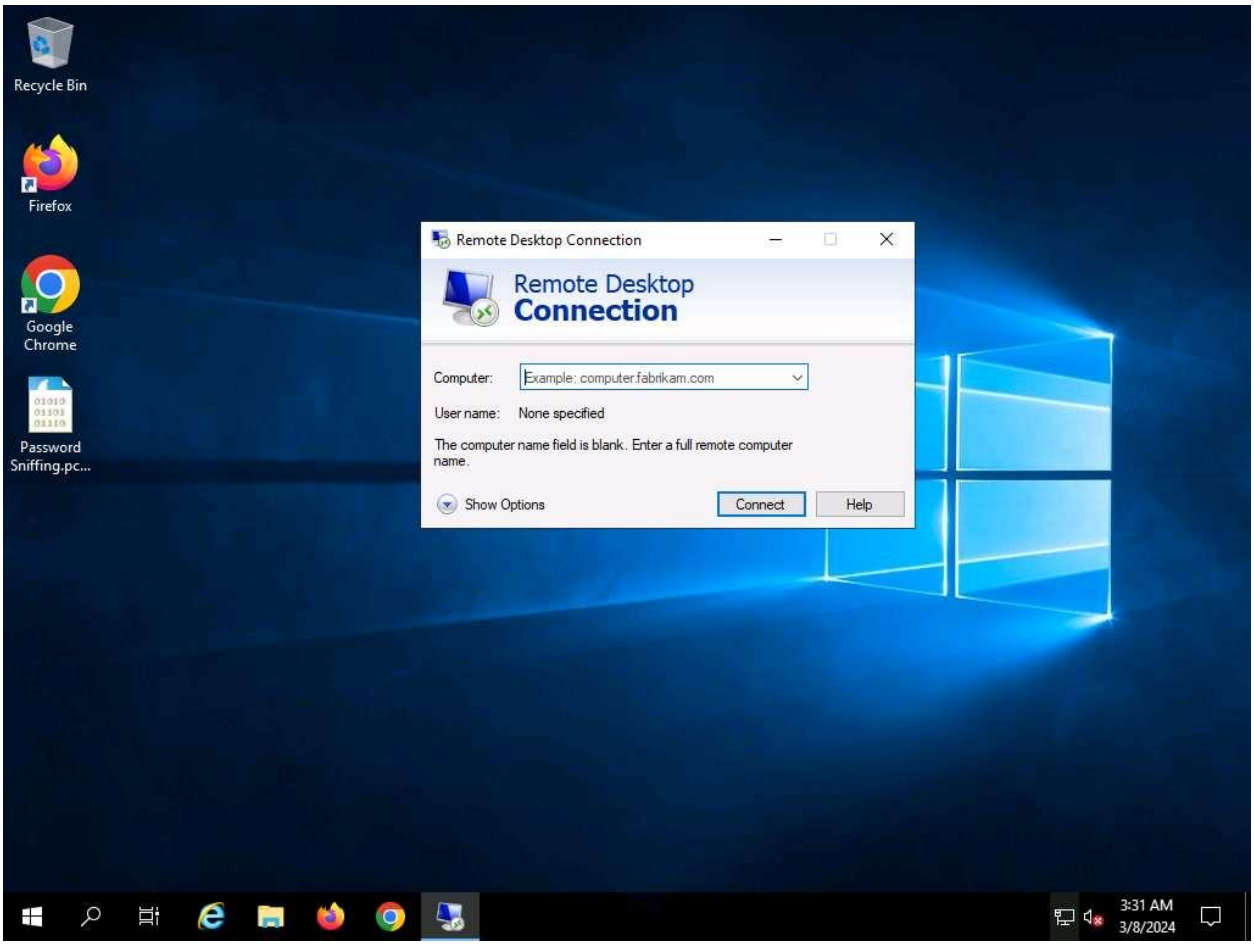


19. Close the **Wireshark** window.
20. Click Windows 11 to switch to the **Windows 11** machine, close the web browser, and sign out from the **Admin** account.



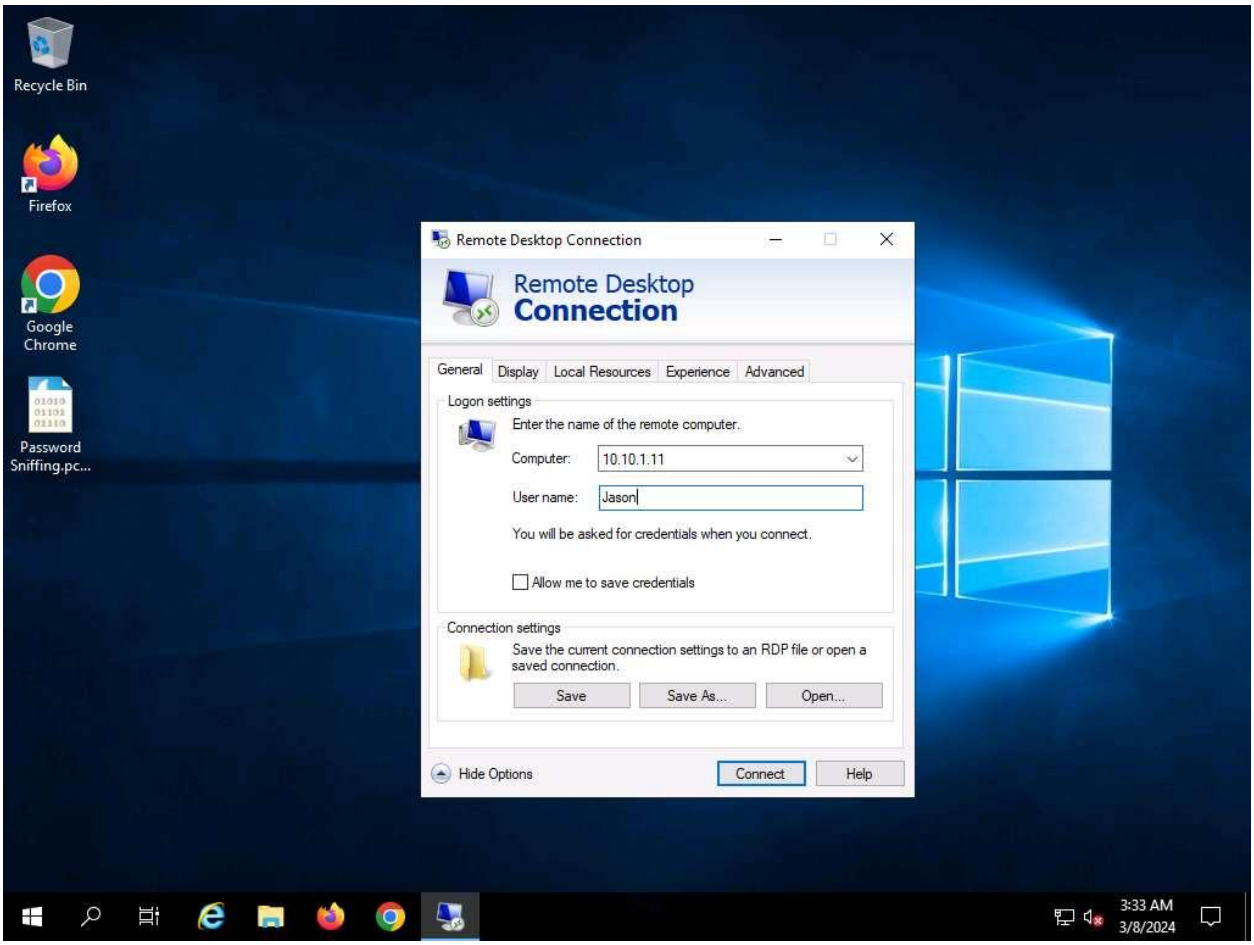
21. Click Windows Server 2019 to switch back to the **Windows Server 2019** machine.
22. Search **Remote Desktop Connection** from search bar and launch it.
23. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

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



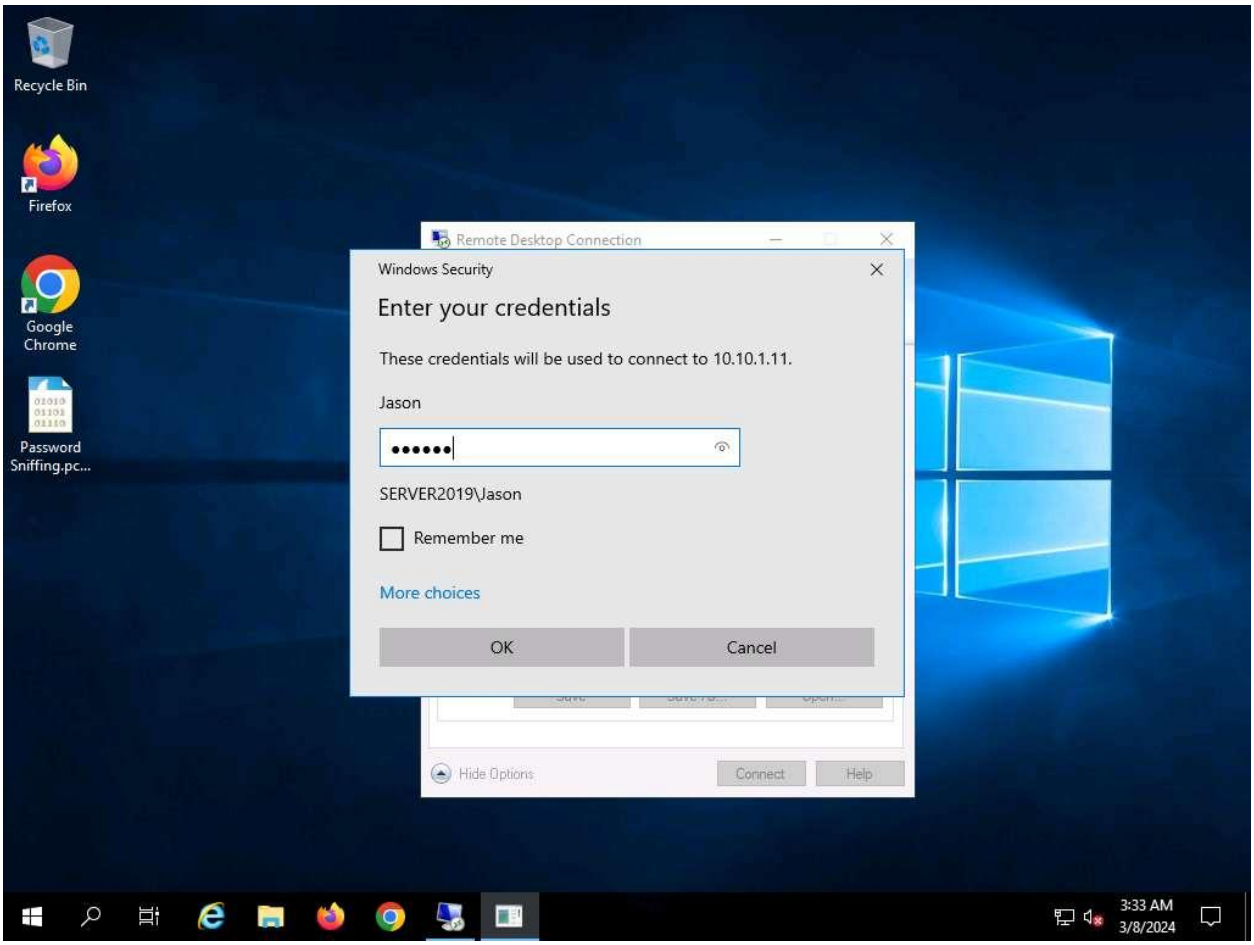
24. The dialog-box expands; under the **General** tab, type **10.10.1.11** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

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.

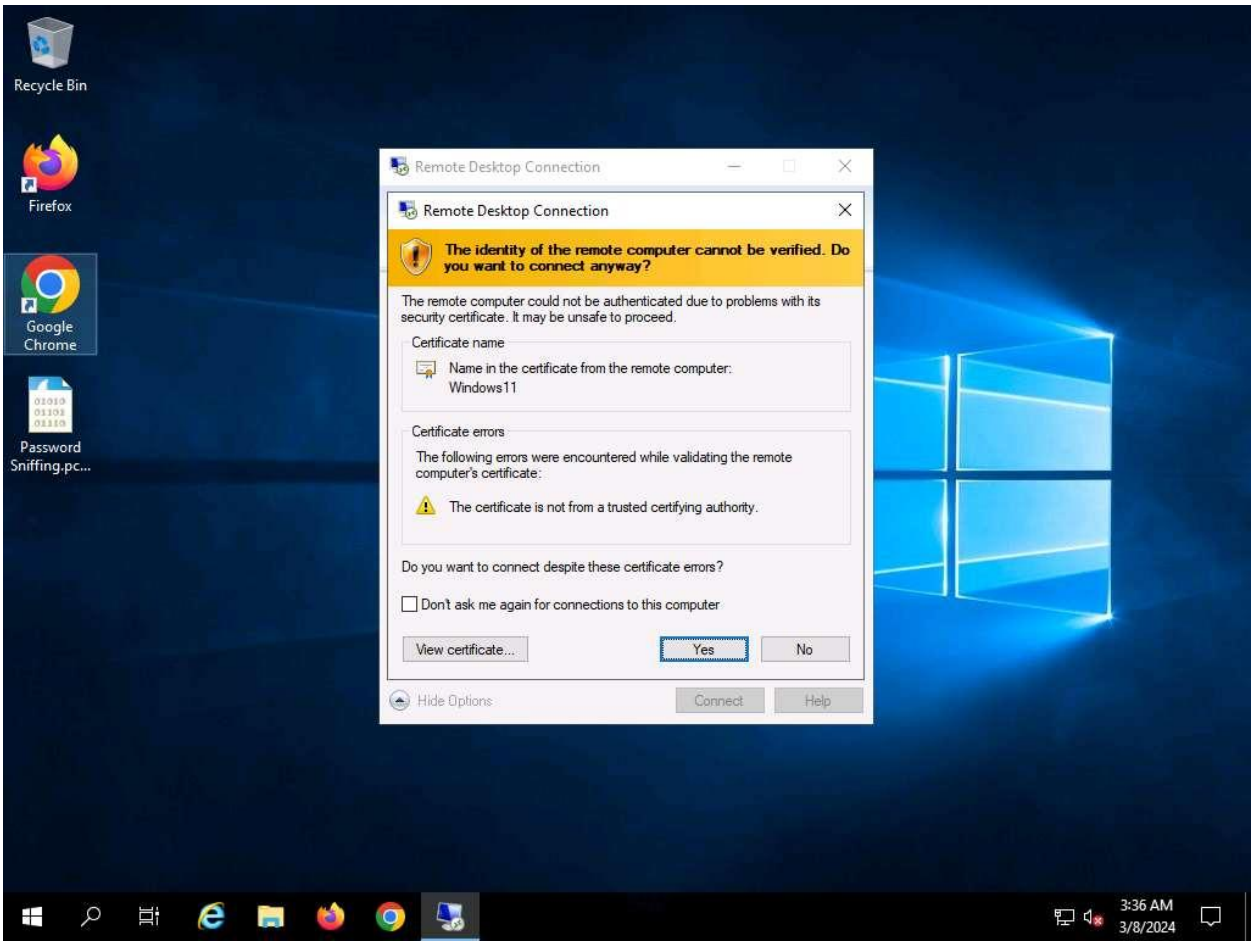


25. The **Windows Security** pop-up appears. Enter **Password** (**qwerty**) and click **OK**.

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



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

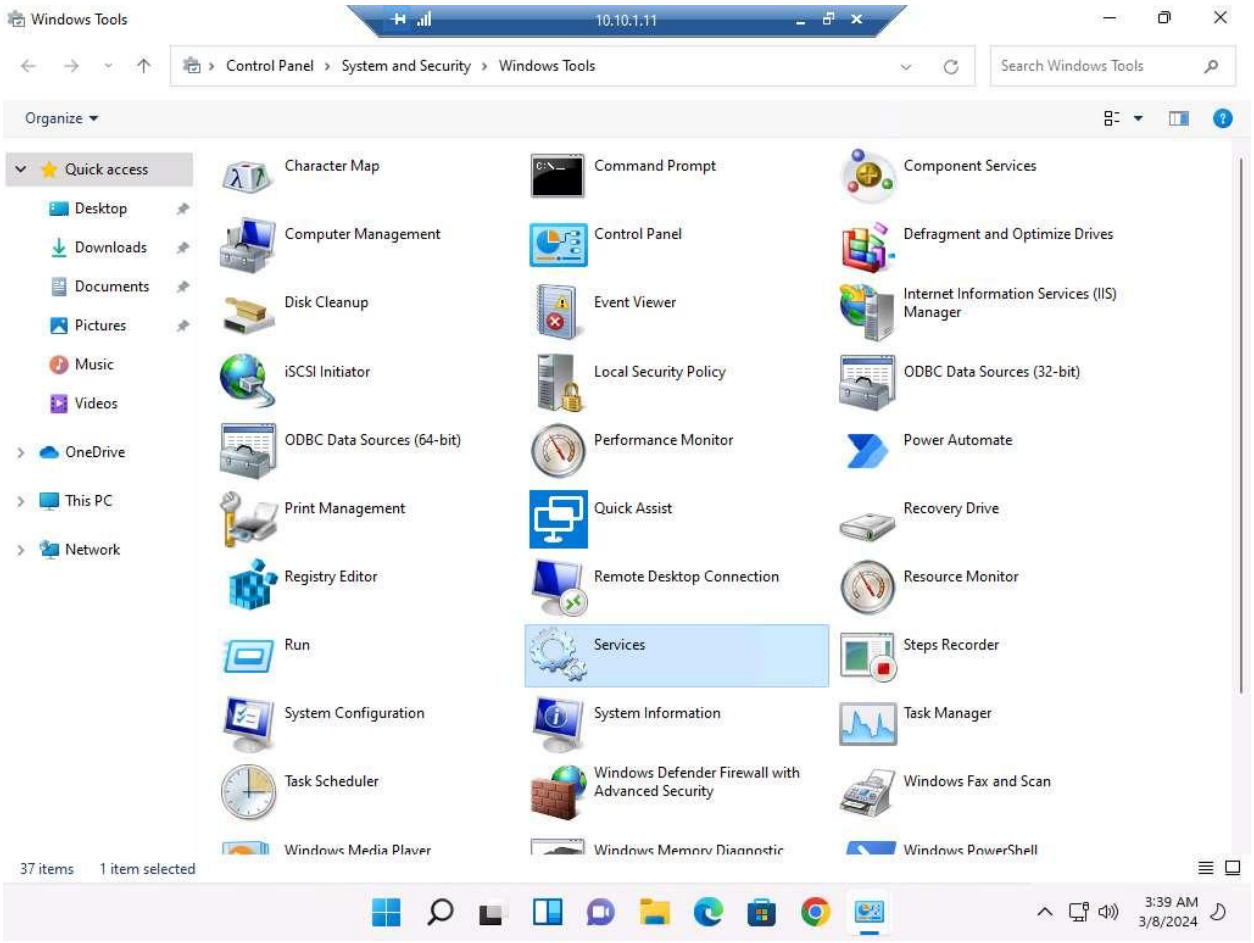


27. A remote connection to the target system (**Windows 11**) appears.

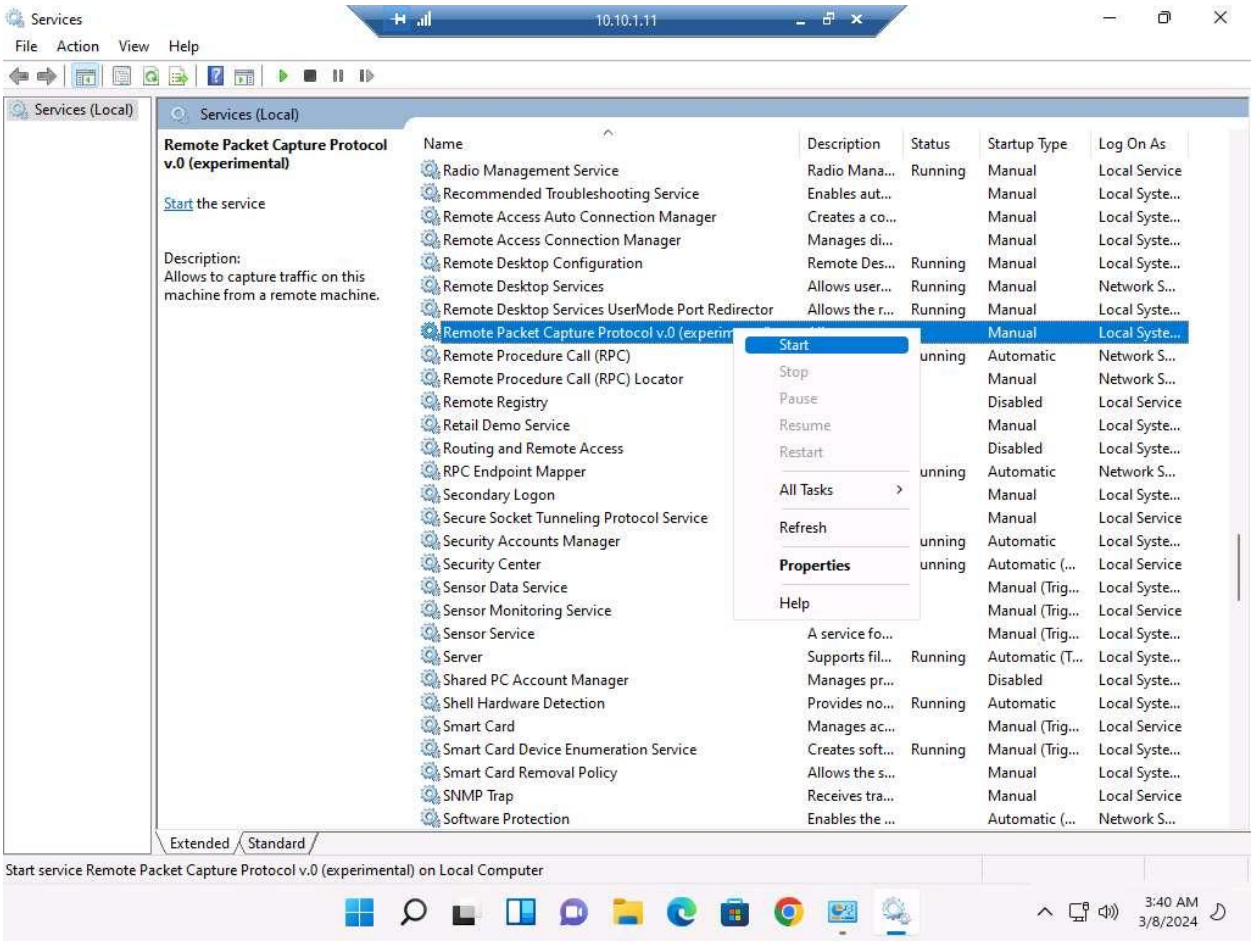
If a **Choose privacy settings for your device** window appears, click on **Next** in the next window click on **Next** and in the next window click on **Accept**.

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

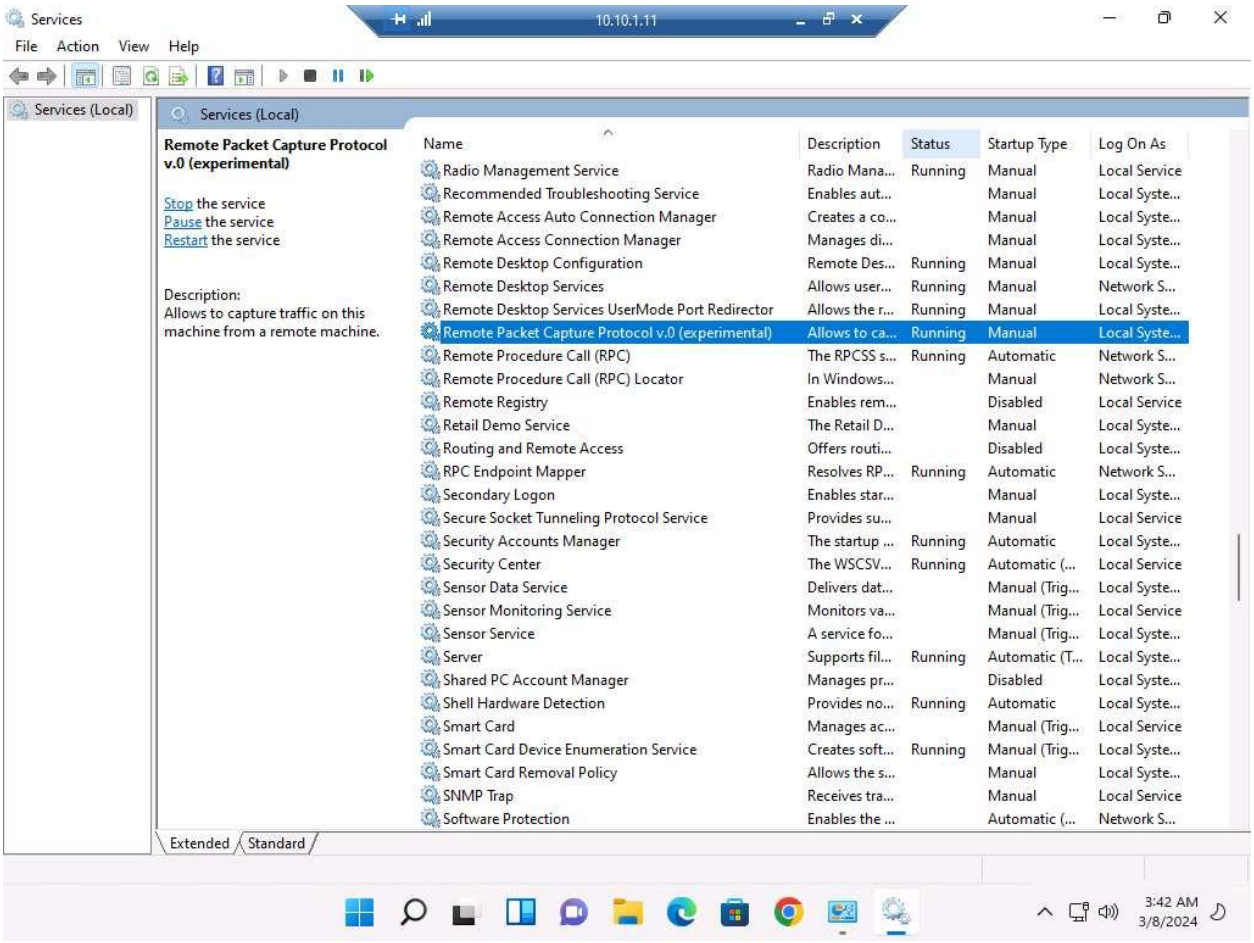
29. The **Control Panel** window appears; navigate to **System and Security --> Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.



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



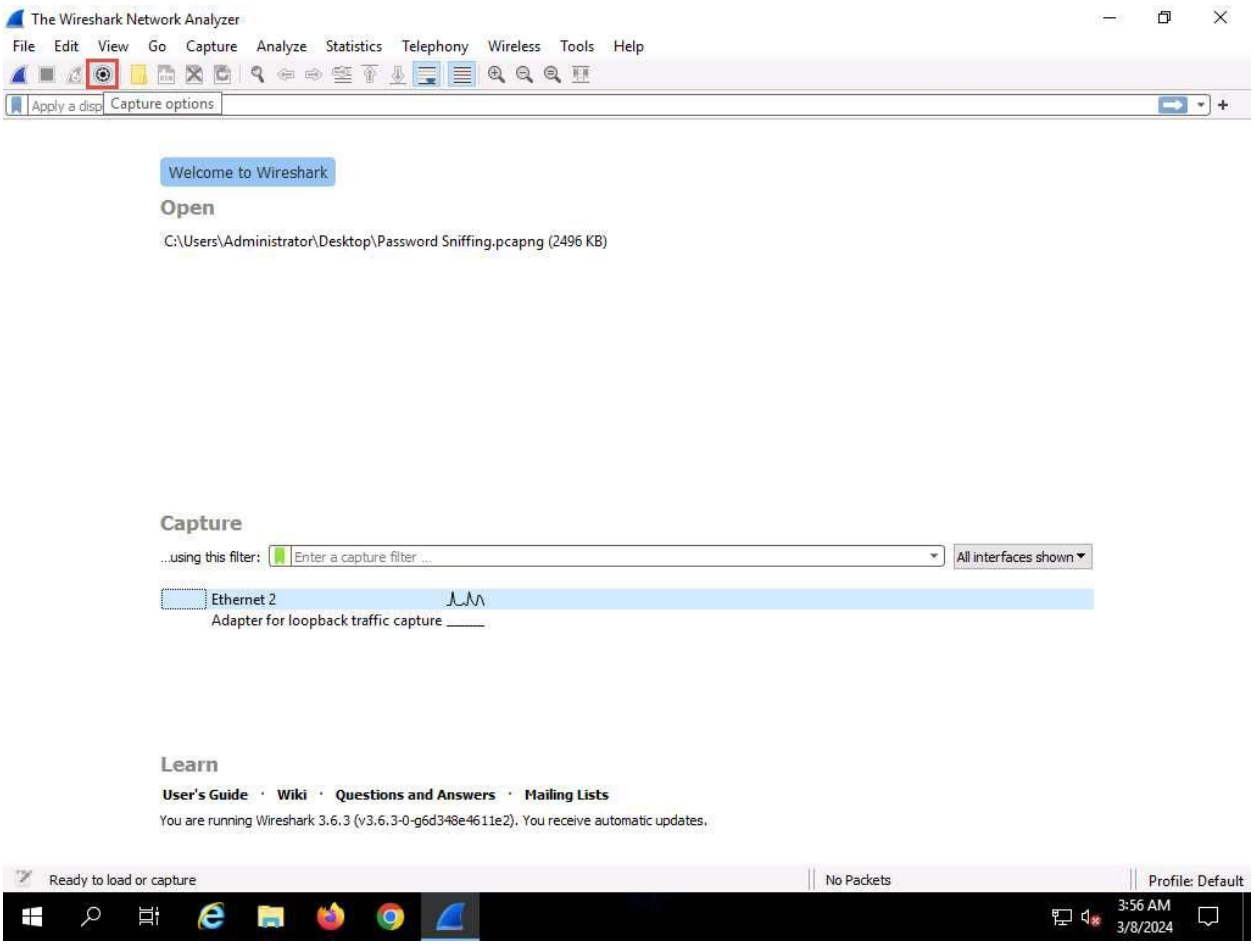
31. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.



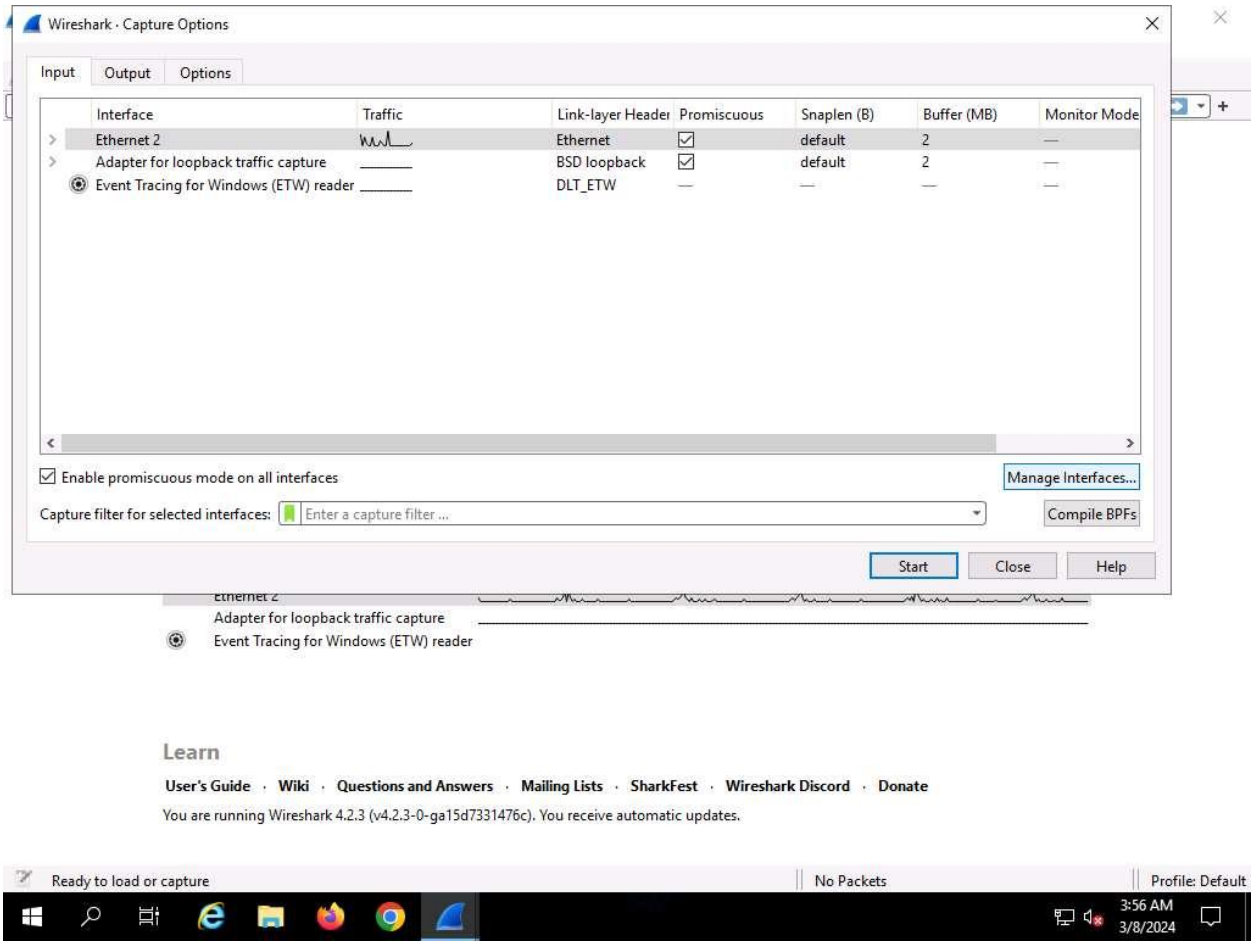
32. Close all open windows on the **Windows 11** machine and close **Remote Desktop Connection**.

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

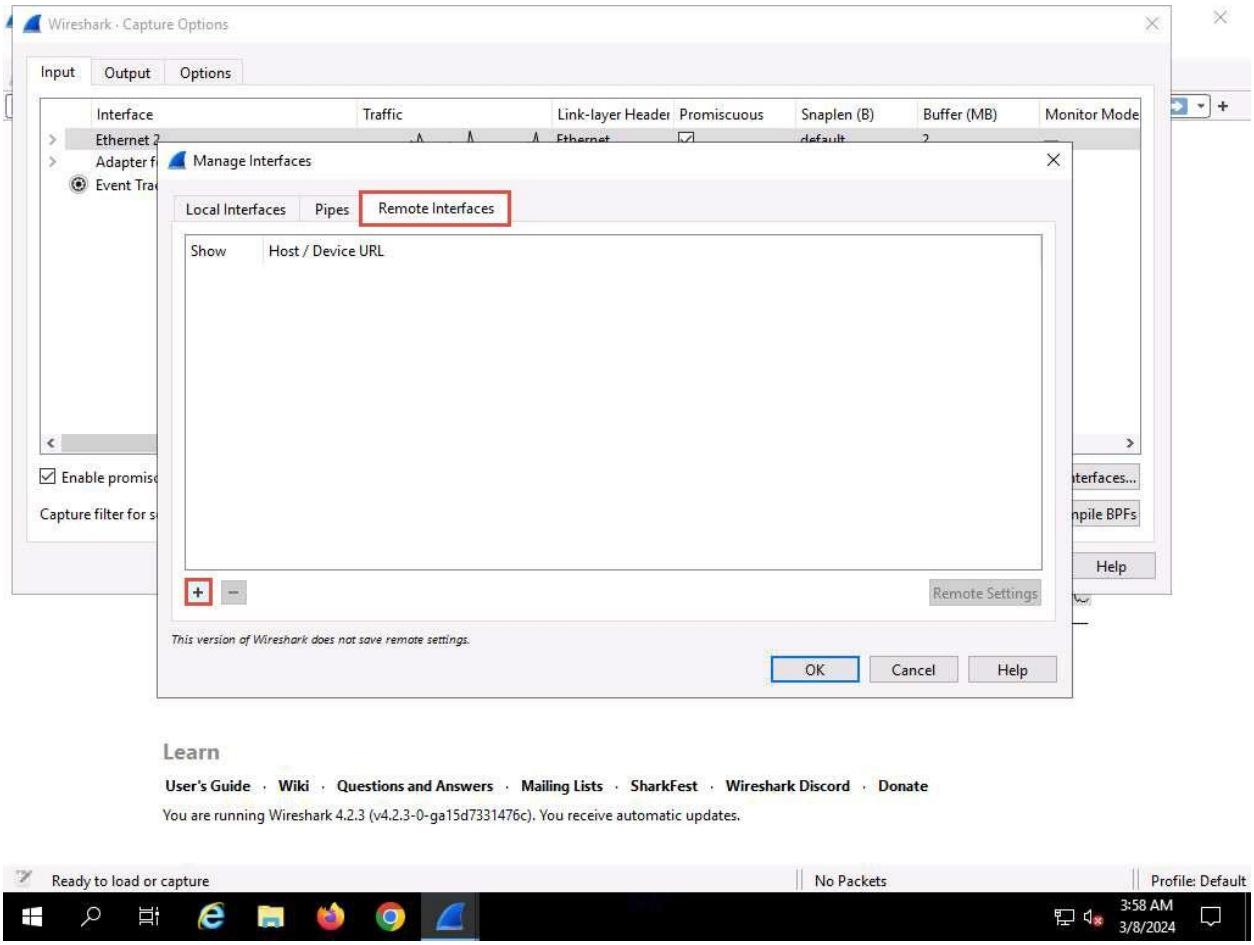
33. Now, in **Windows Server 2019**, launch **Wireshark** and click on **Capture options** icon from the toolbar.



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

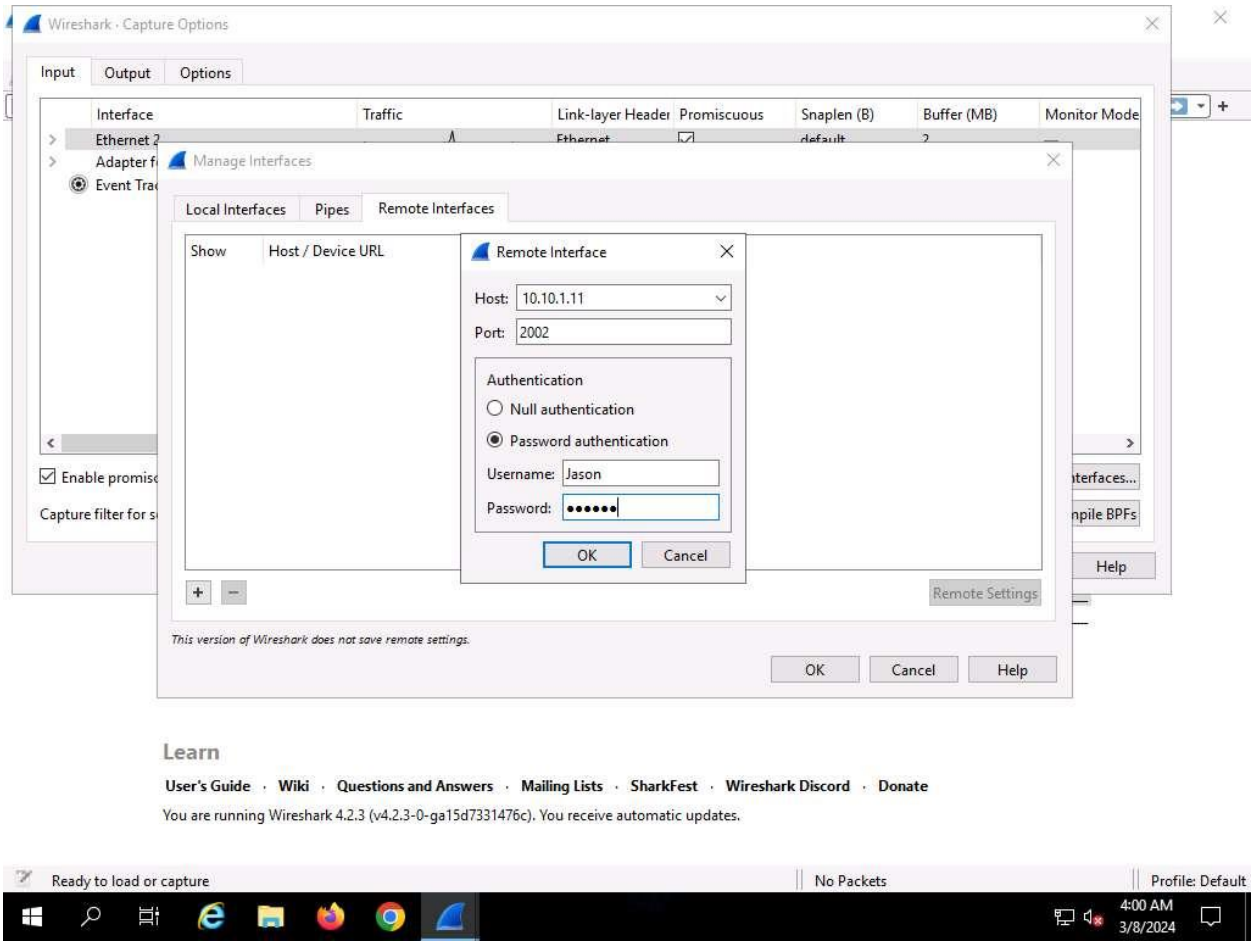


35. The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface** icon (**+**).

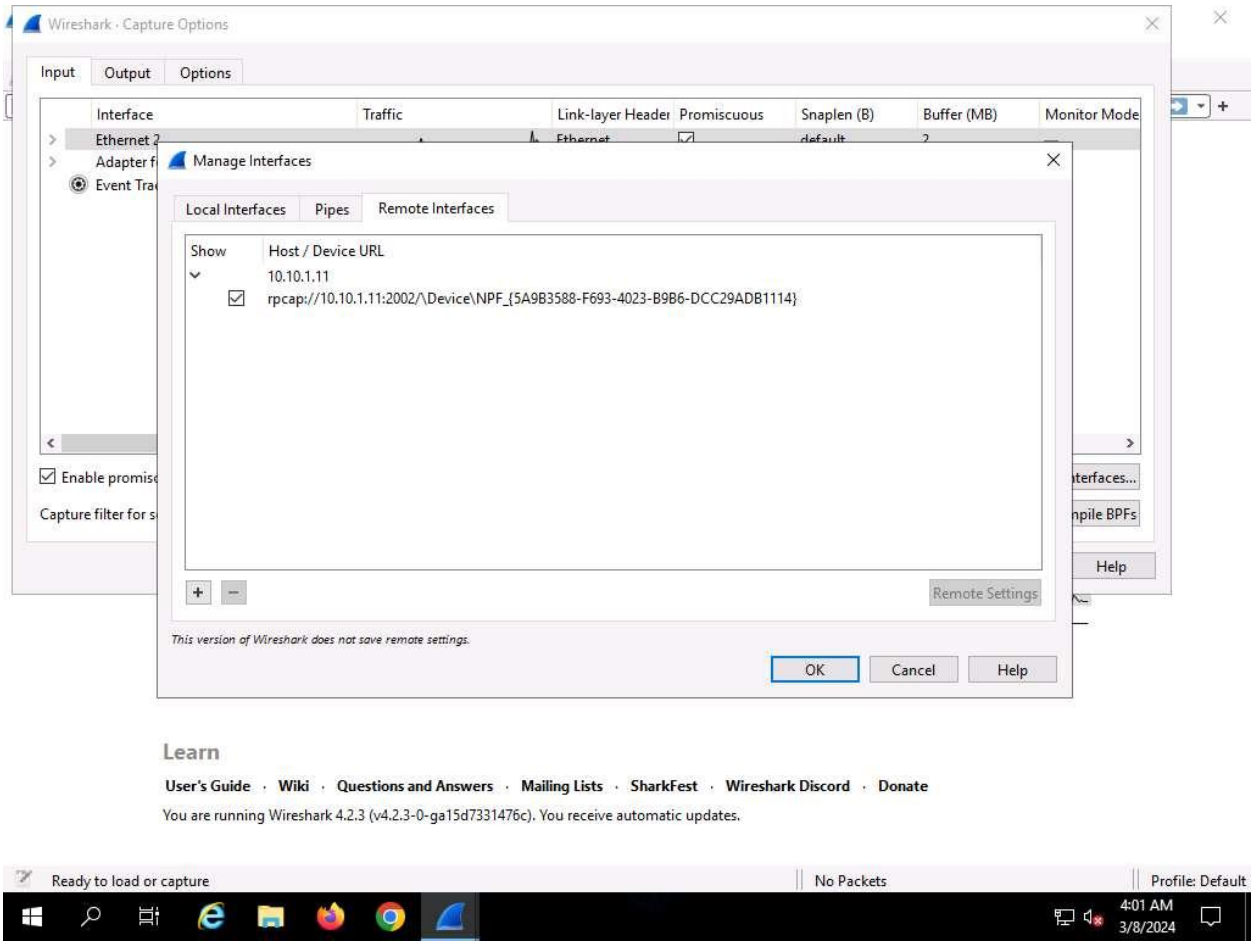


36. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.1.11**); and in the **Port** field, enter the port number as **2002**.
37. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.

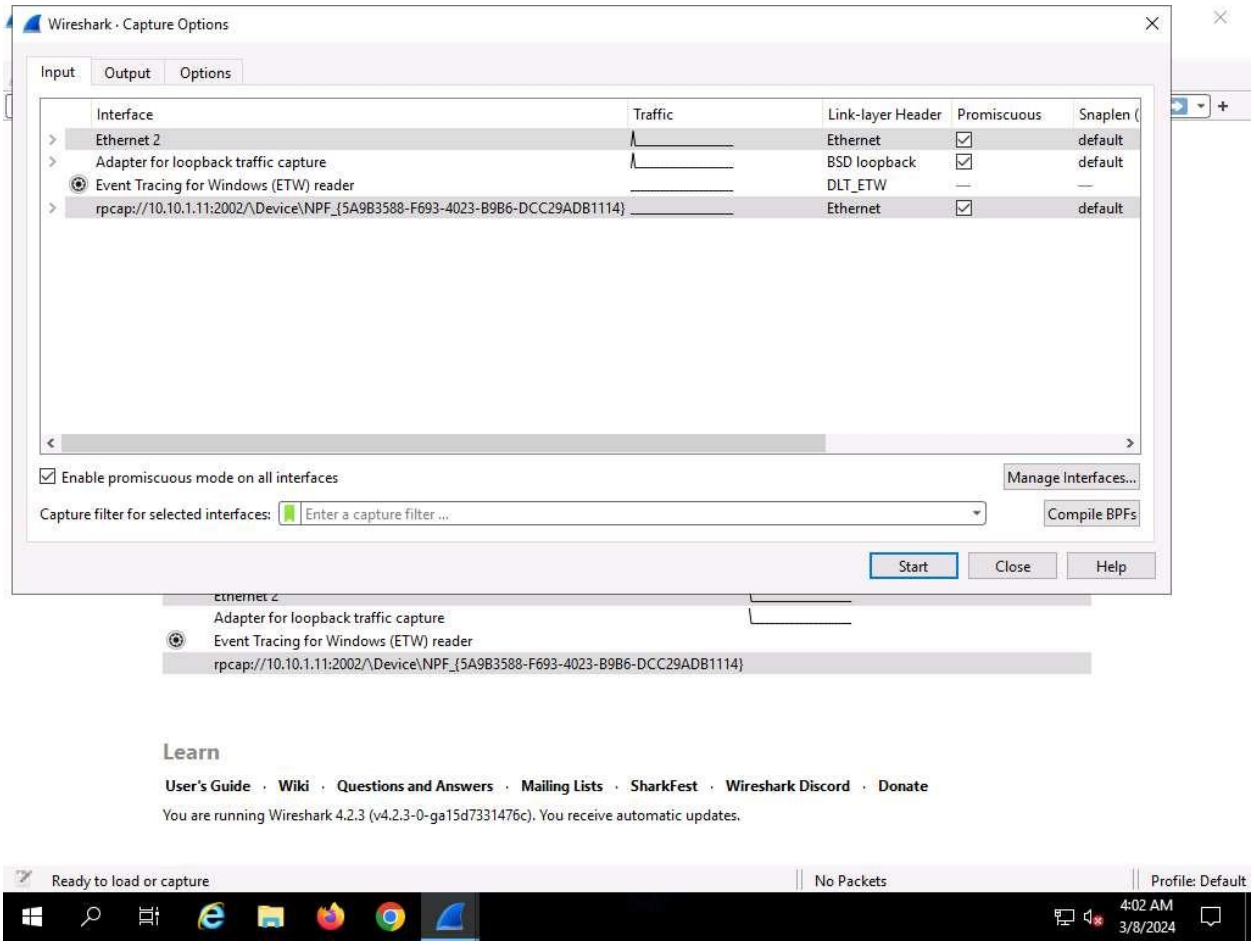
The IP address and user credentials may differ when you perform this task.



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



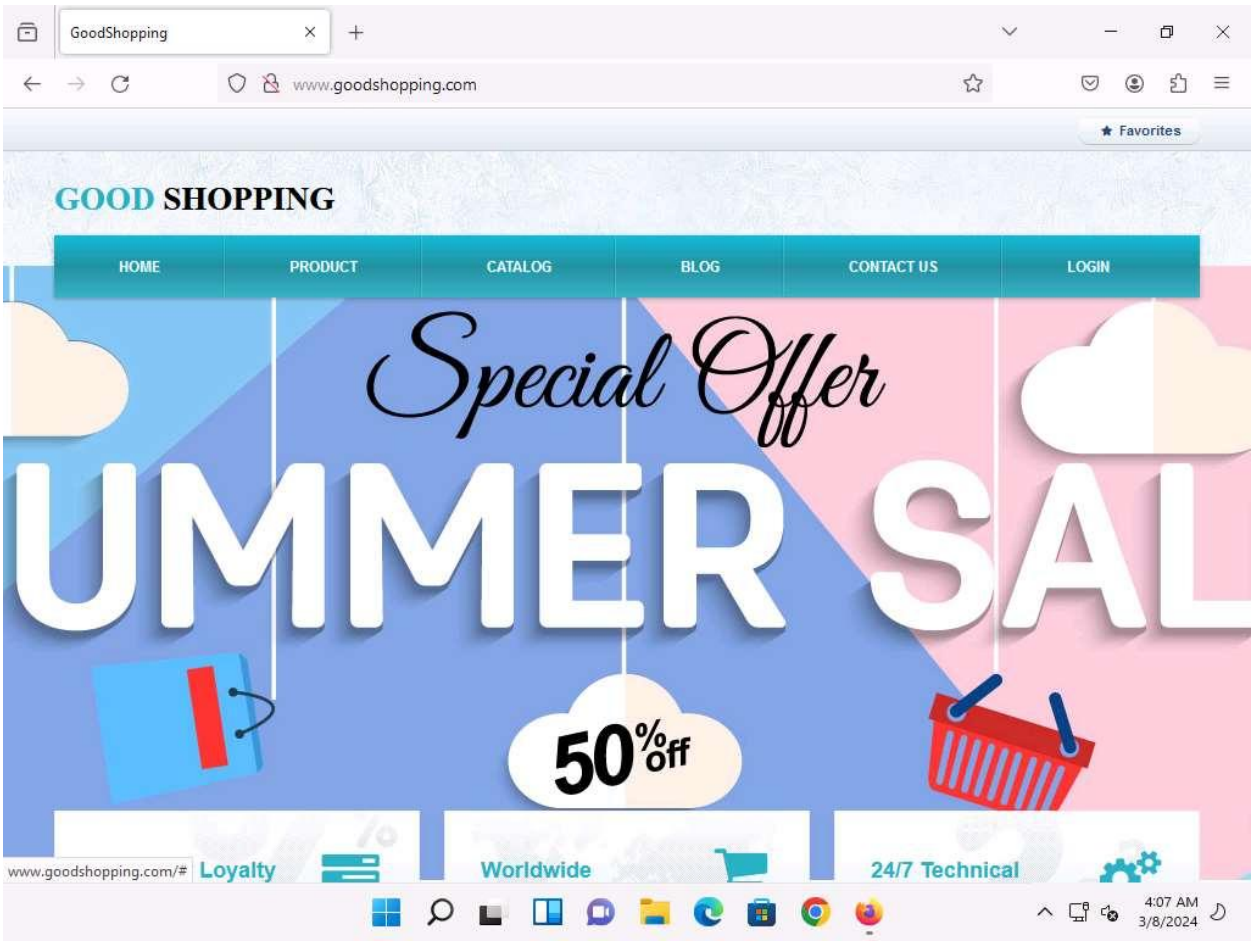
39. The newly added remote interface appears in the **Wireshark**. **Capture Options** window; click **Start**.



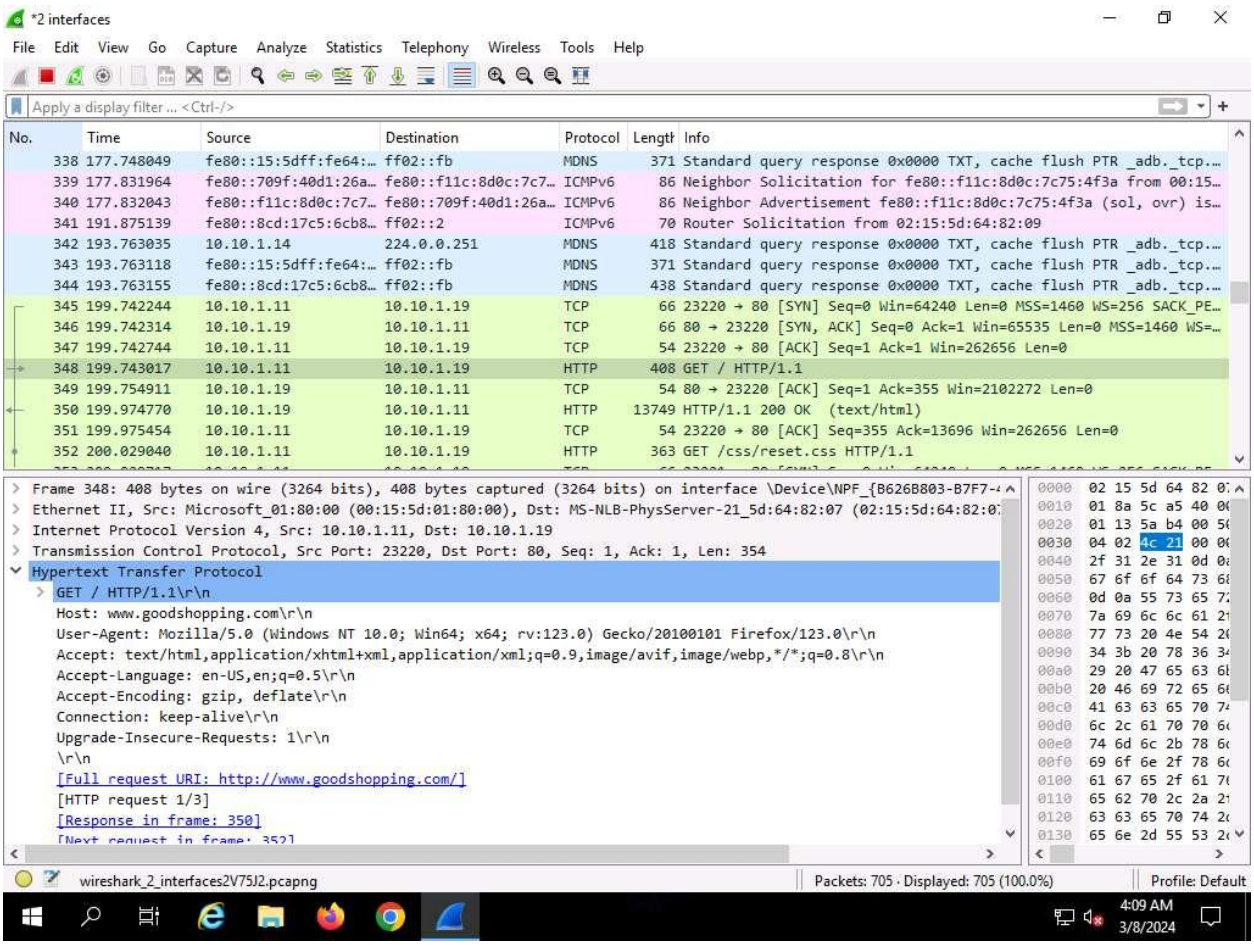
40. Click Windows 11 to switch to the **Windows 11** machine, and login using **Jason/qwerty**. Here, you are signing in as the victim.

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?