Contents

Abstract

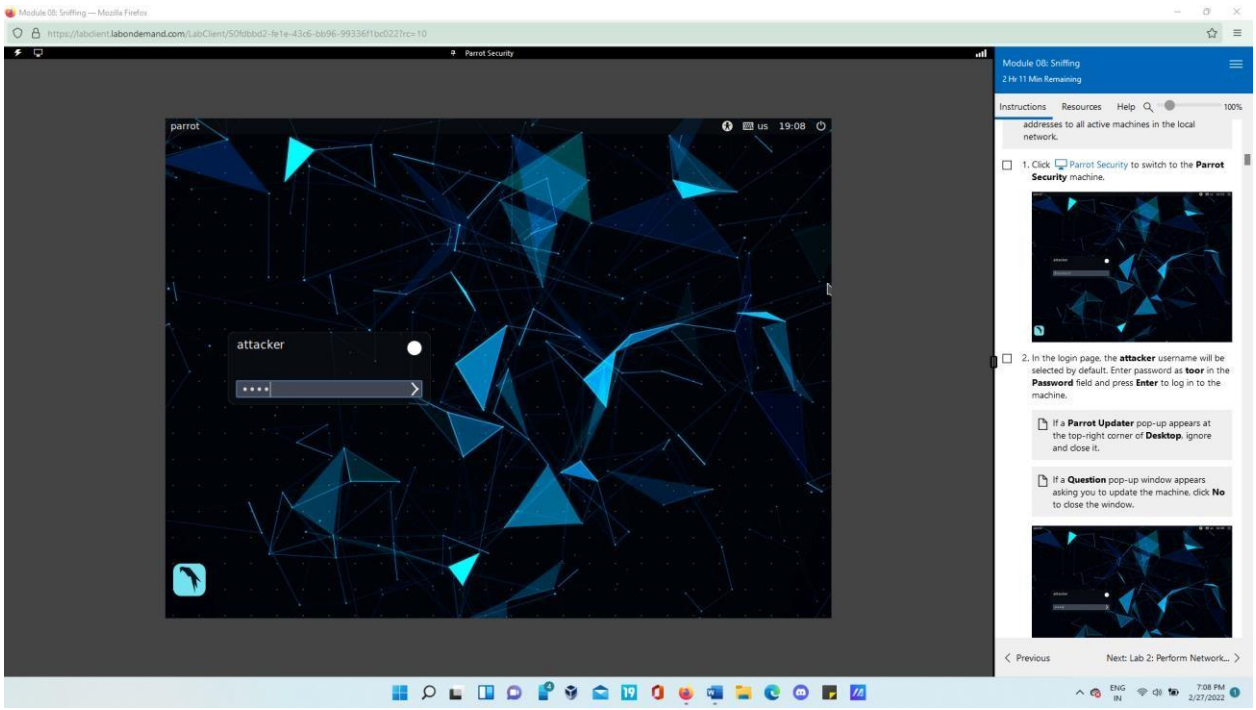
In this Assignment, we have performed two attacks namely, network sniffing and social engineering. Basically, sniffing is a technique through which a person gets access on overall traffic in the network while leaving or entering the network. Here, we are going to sniff the packets and perform MAC flooding, MITM attack, password sniffing and many more. On the other hand, social engineering is one of the best techniques nowadays to attack target by sending phishing emails and fake sites. Today we will be going to detect usernames, passwords, personal details, and other important information with social engineering toolkit, and also perform and detect phishing using Netcraft, PhishTank.

Module 08: Sniffing

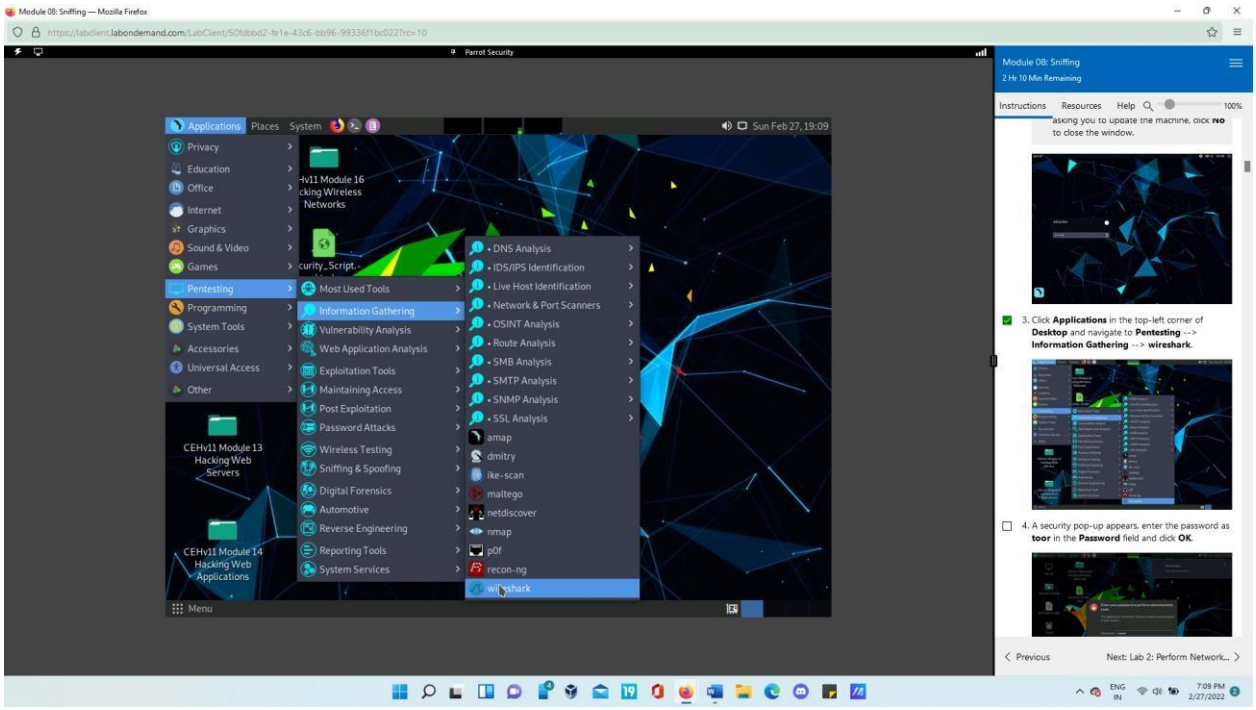
Lab 1: Perform Active Sniffing

Task 1: Perform MAC Flooding using macof

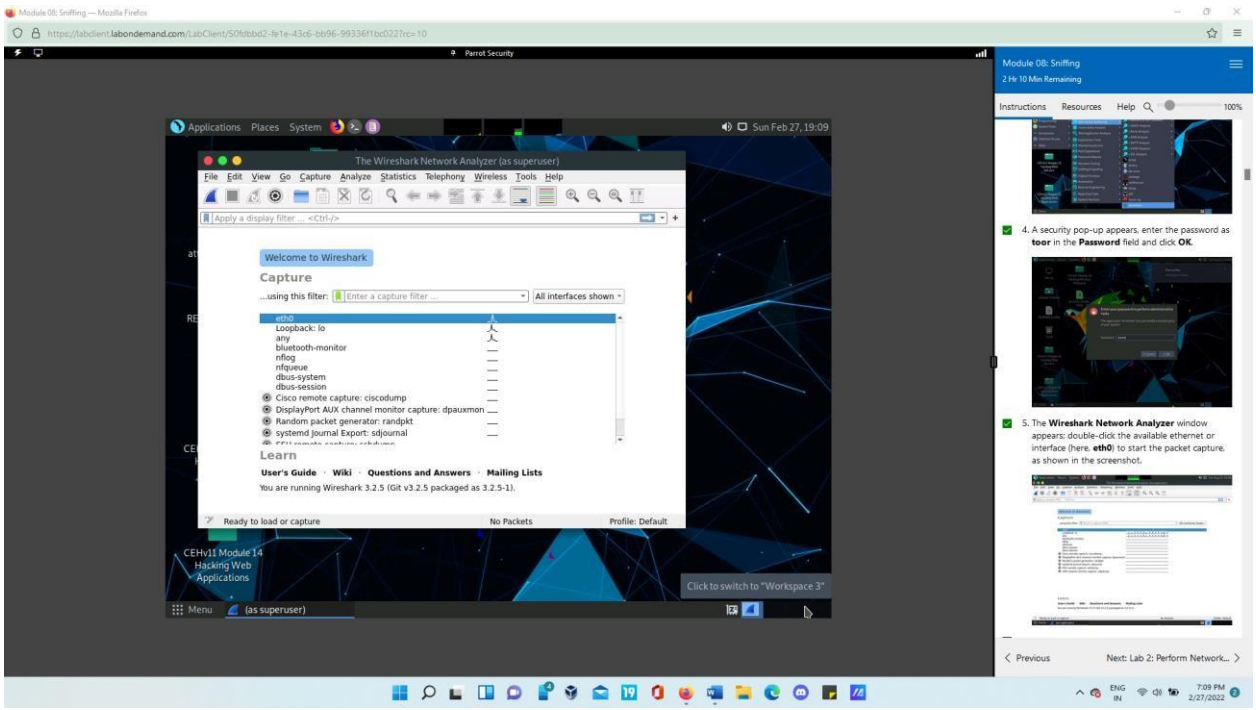
- First, we need to switch to the ParrotOS



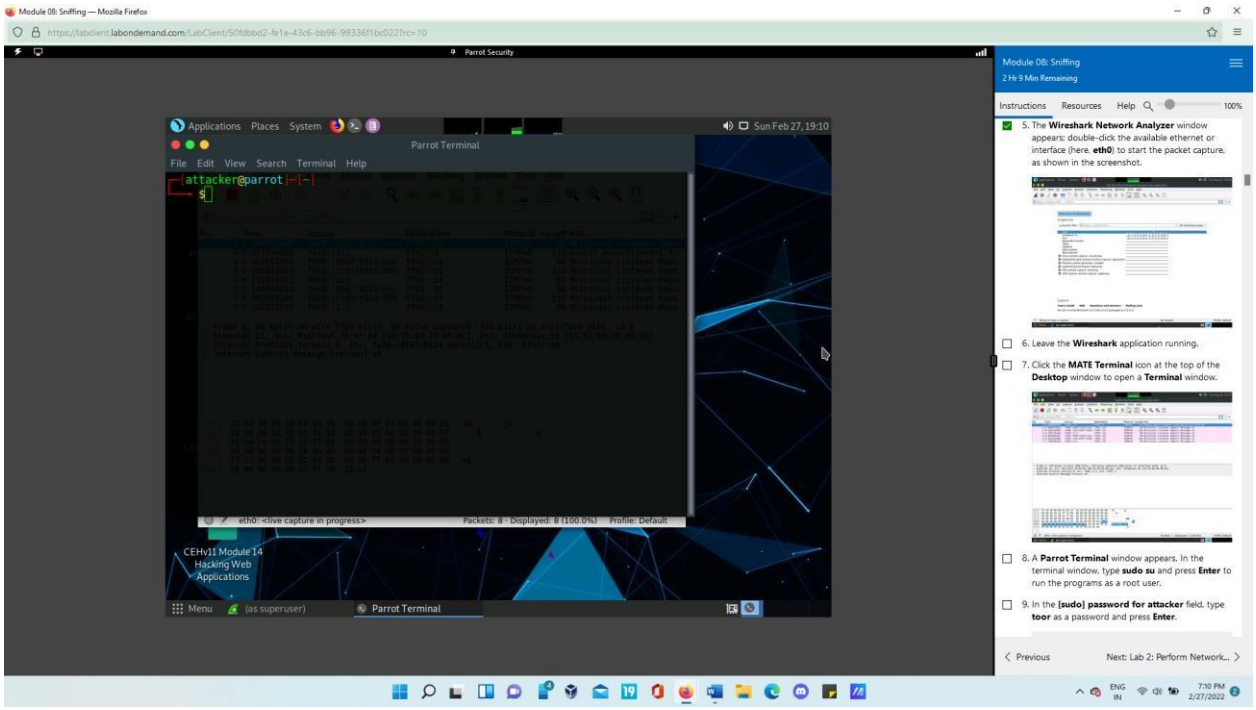
- Open Wireshark by navigating from the applications drop down menu.



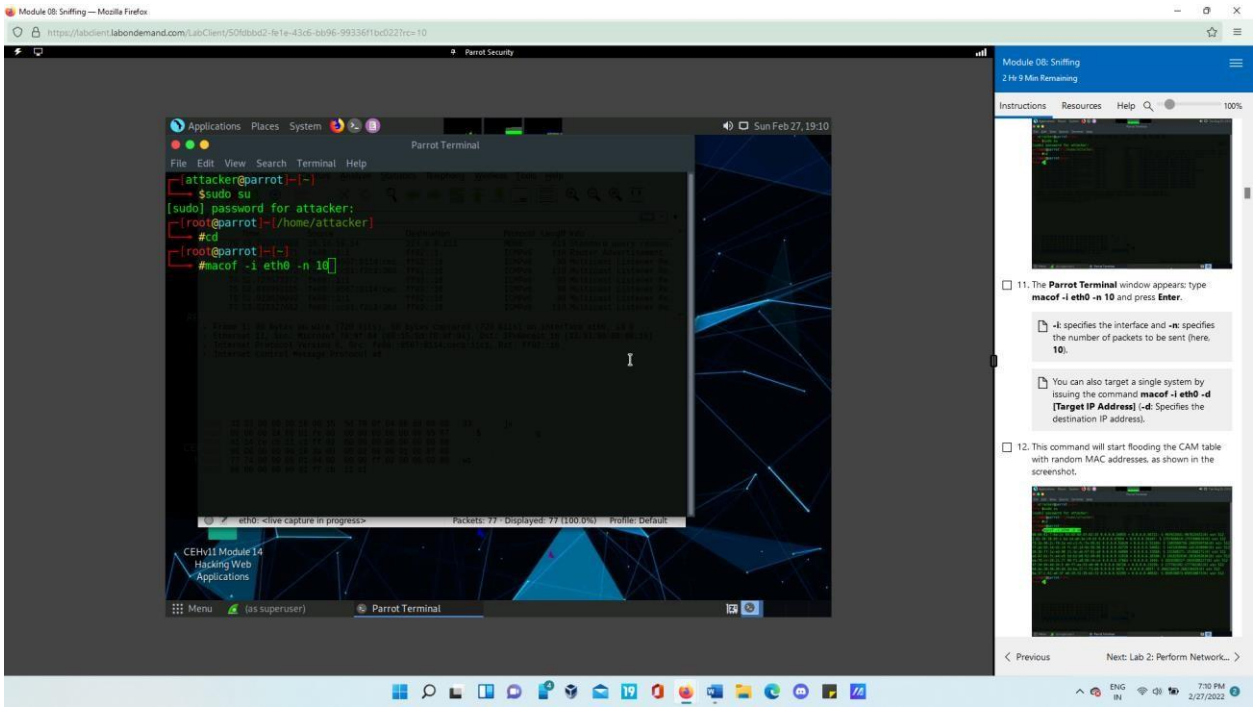
- Wireshark Network Analyzer opens and select Ethernet/eth0 to start packet capture.



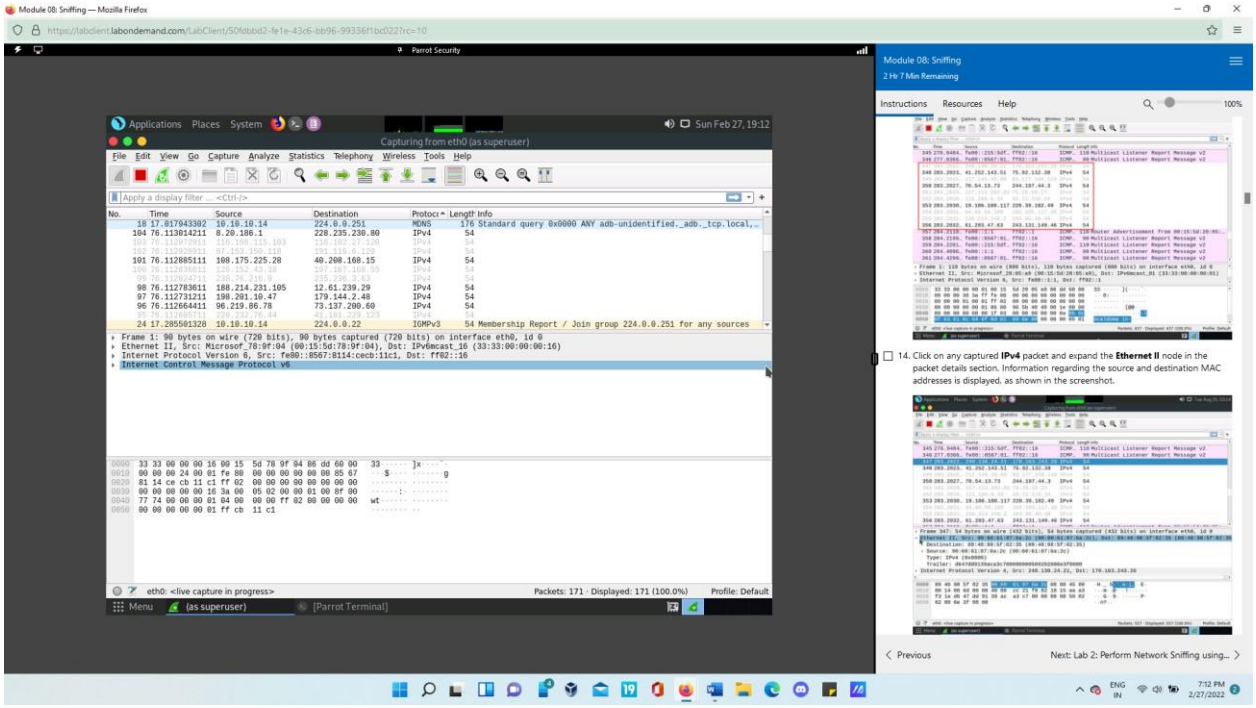
- Now open a new terminal window.



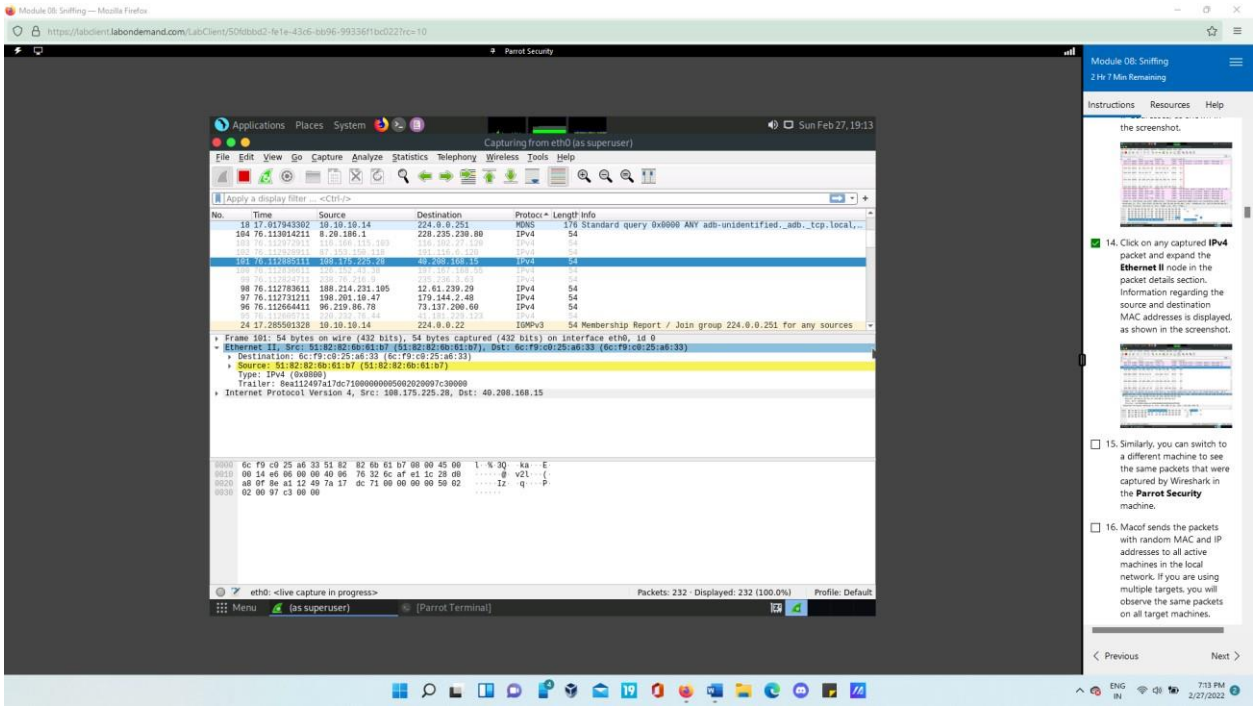
- Obtain Sudo privileges and go to root directory, now type macof -i eth0 -n 10 to start sending random MAC addresses.



- Now go back to Wireshark and observe the IPv4 packets coming from random IP addresses.

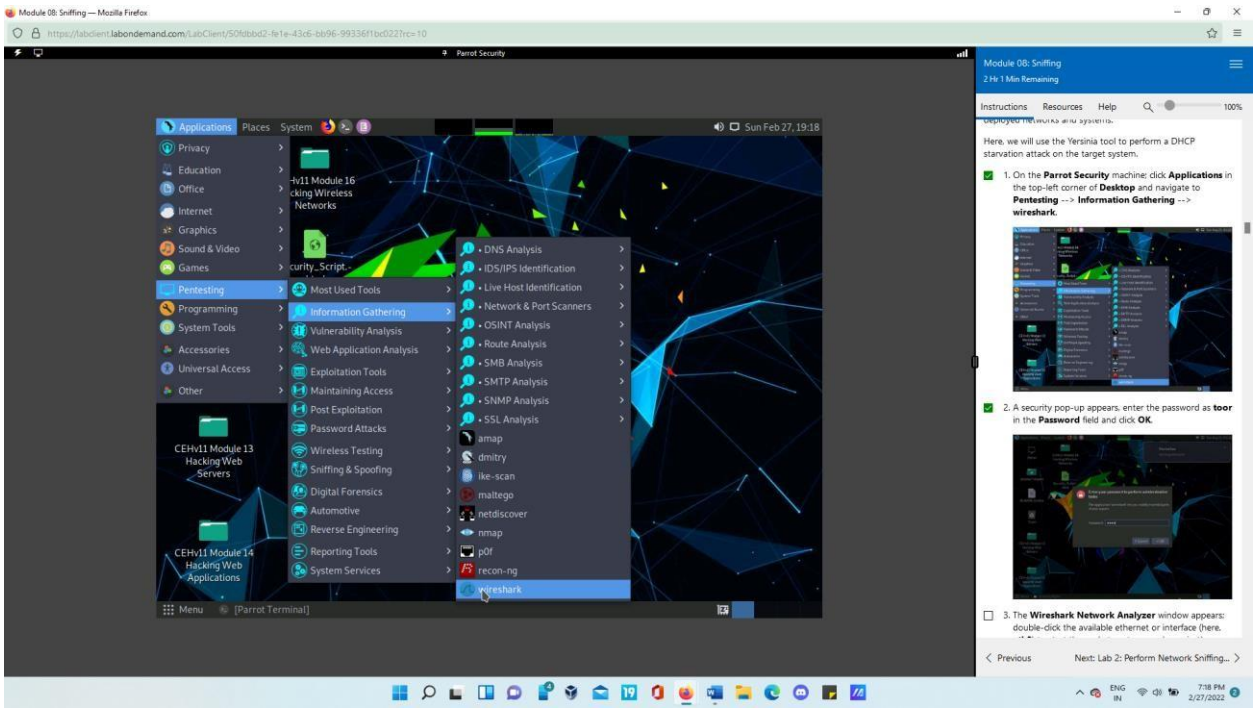


- Select any IPv4 packet and expand to packet details section to see source and destination MAC address.

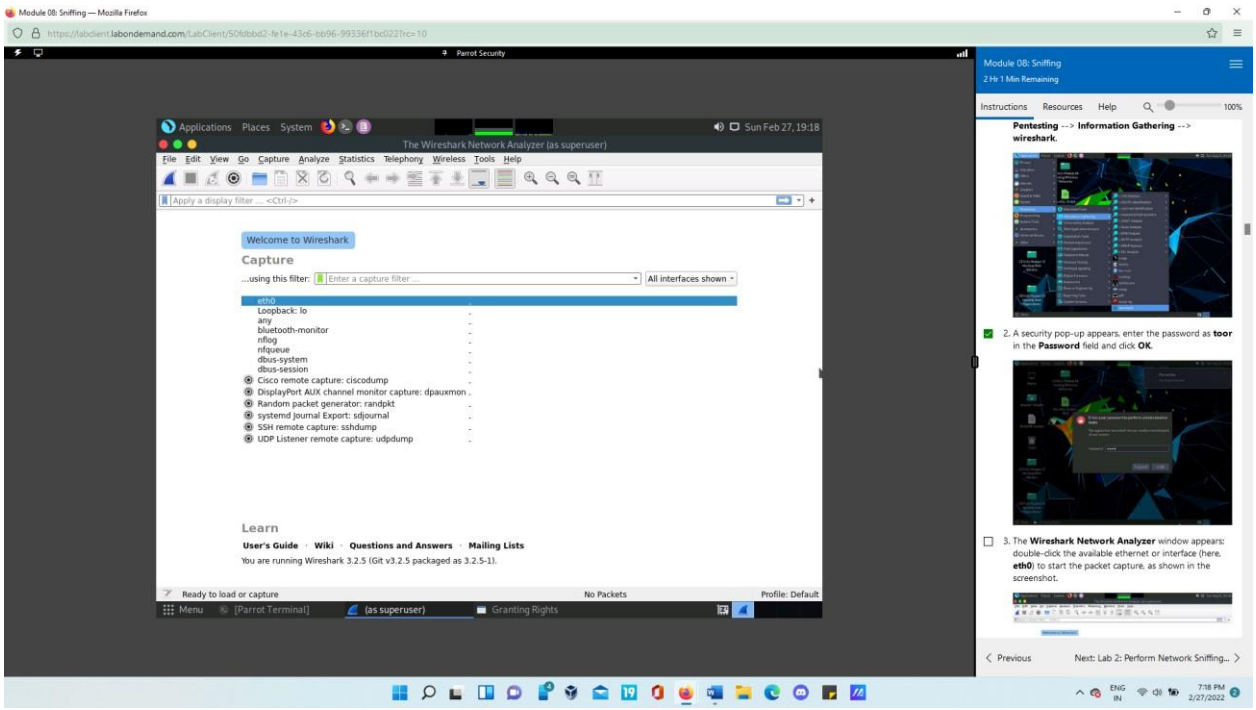


Task 2: Perform a DHCP Starvation Attack using Yersinia

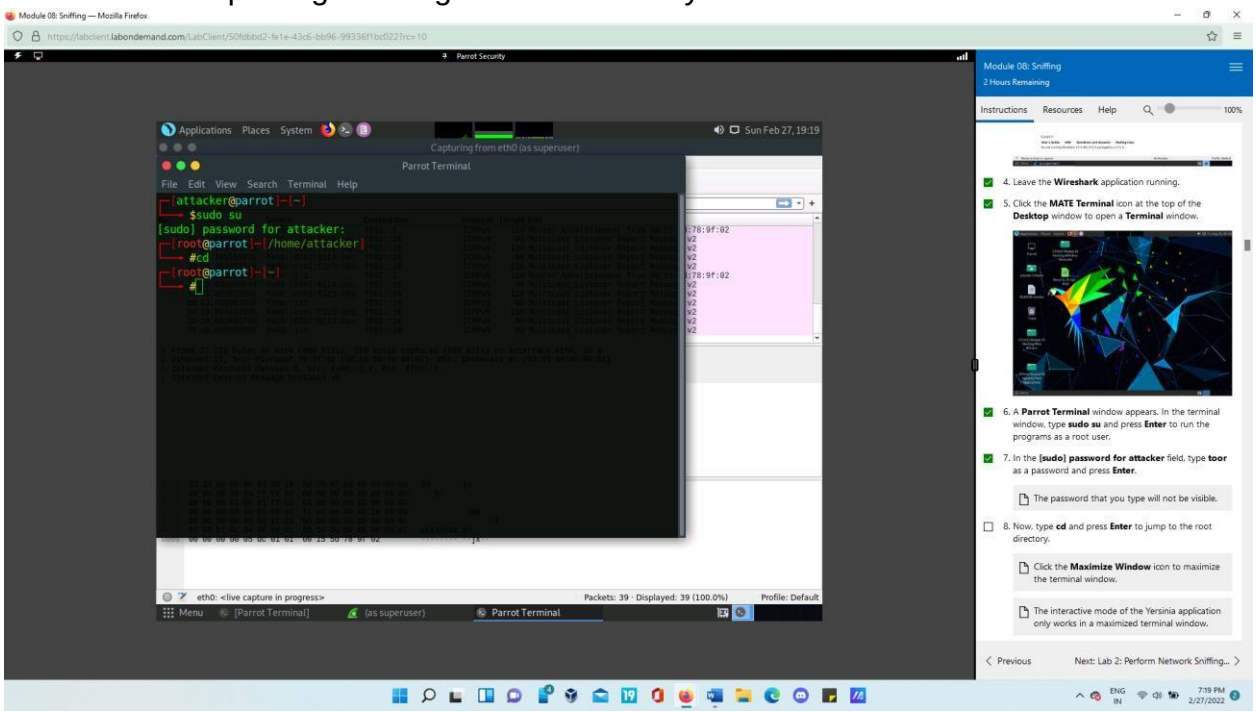
- Open Wireshark by navigating from the applications drop down menu.



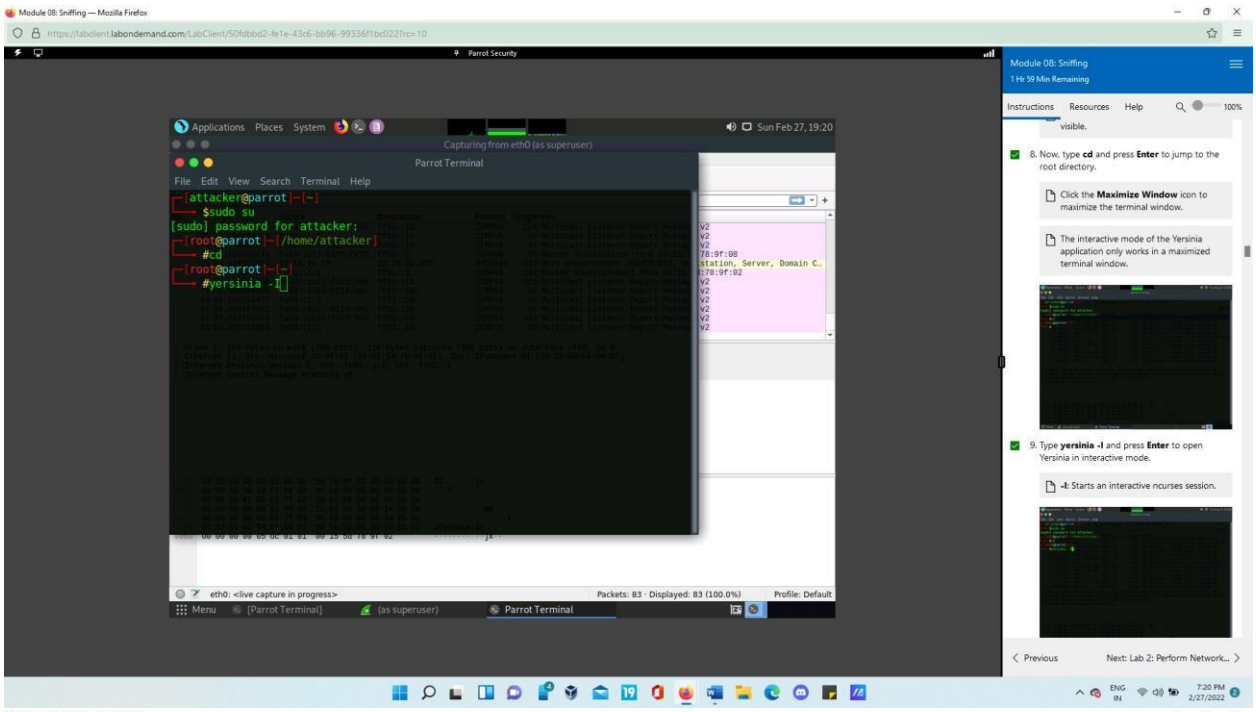
- Wireshark Network Analyzer opens and select Ethernet/eth0 to start packet capture.

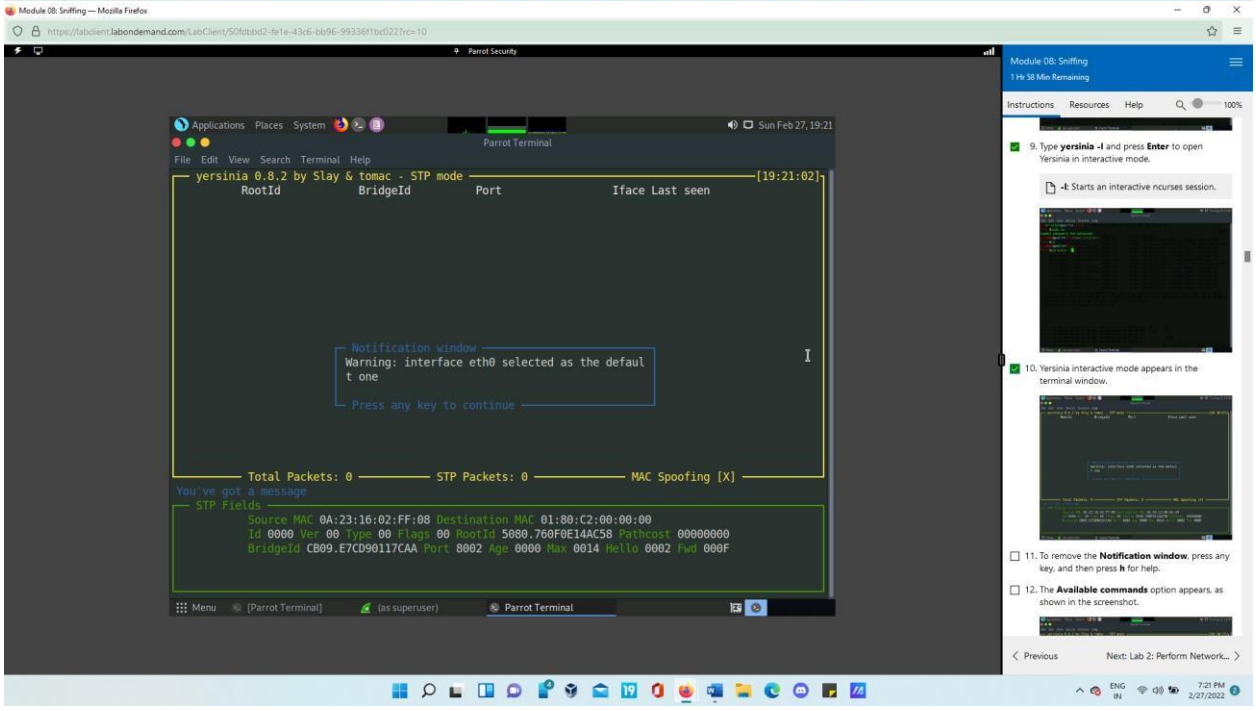


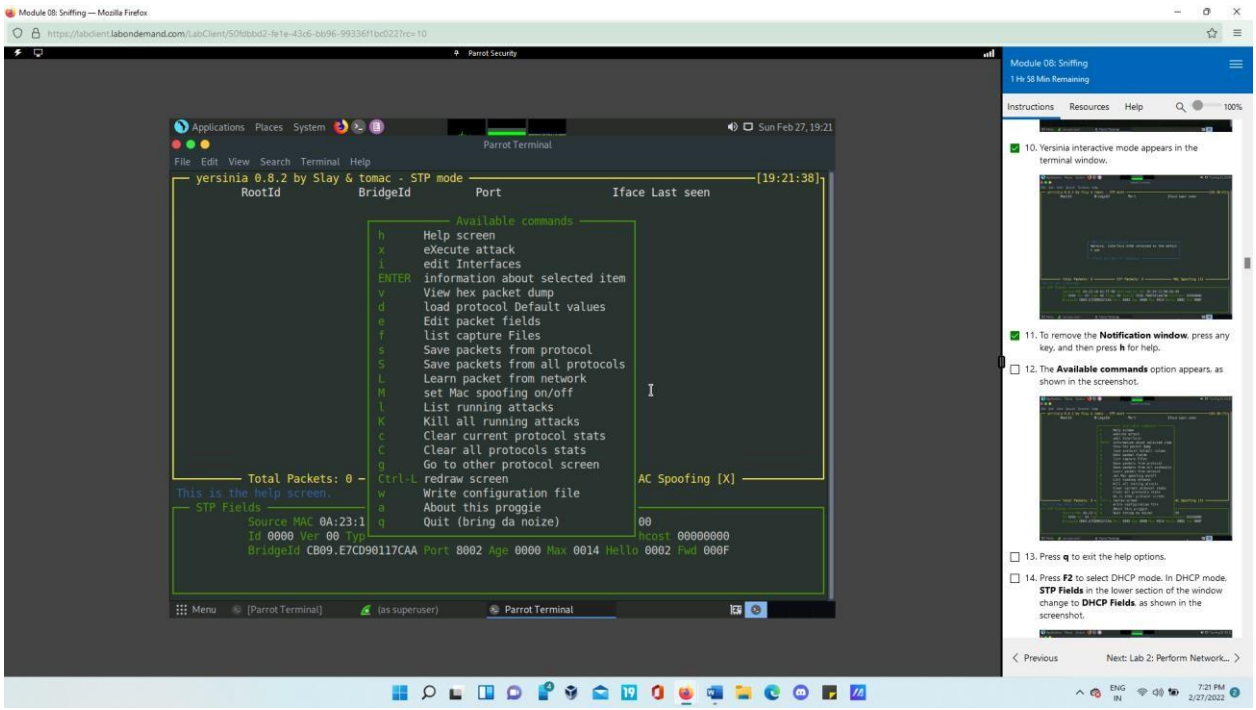
- Obtain Sudo privileges and go to root directory



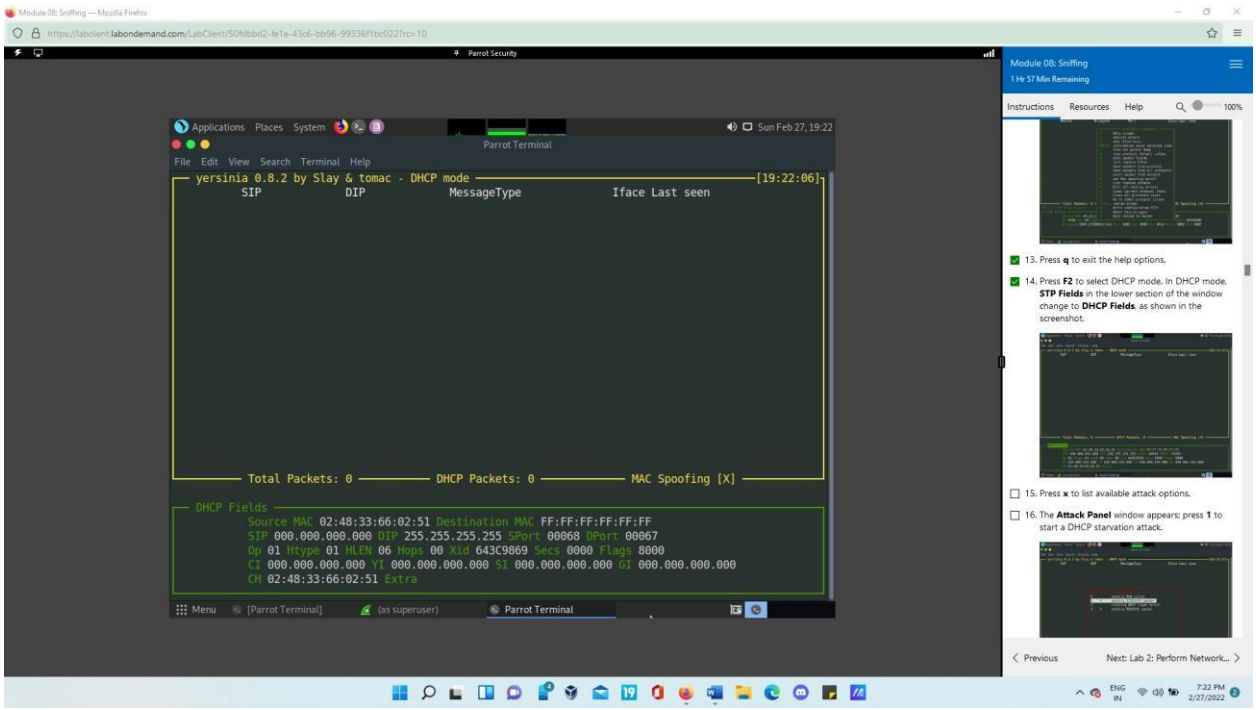
- To open Yersinia in interactive mode type yersinia -I and enter. Press q to exit from help options.

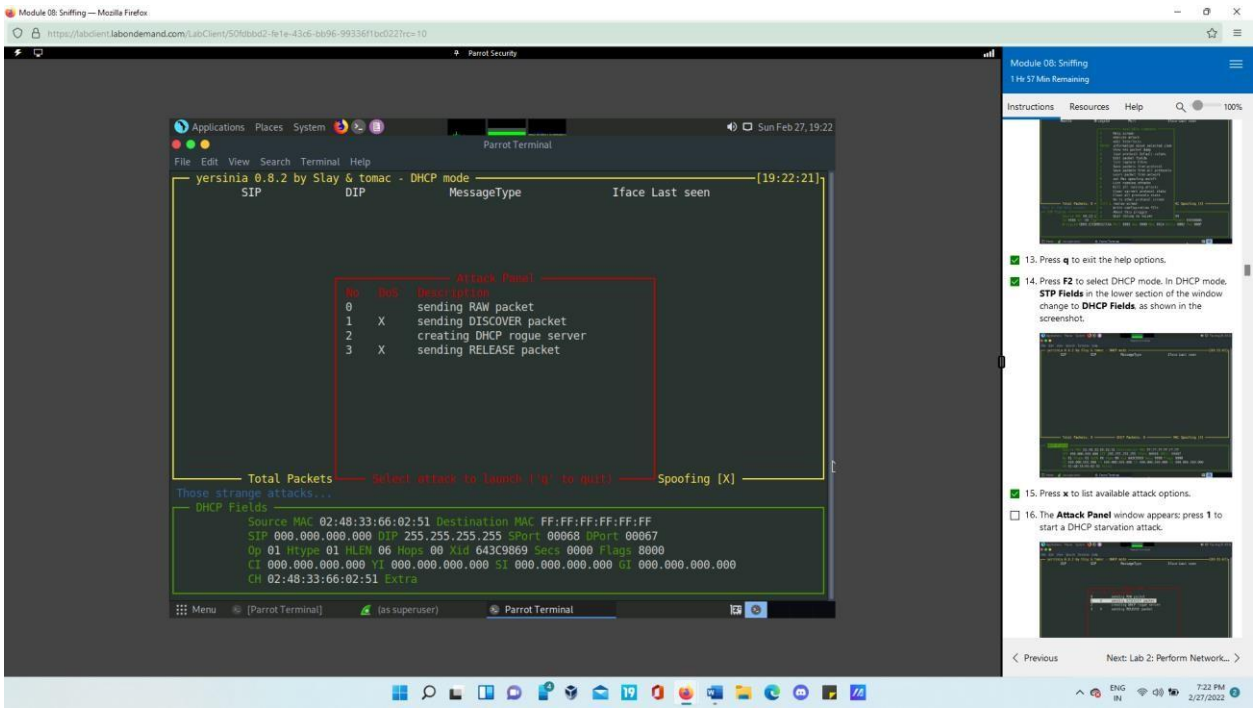

Module 08: Sniffing — Mozilla Firefox
Parrot Security
Applications Places System
Sun Feb 27, 19:20
Capturing from eth0 (as superuser)
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#versinia -I
eth0: <live capture in progress>
Packets: 83 · Displayed: 83 (100.0%)
Profile: Default
Menu [Parrot Terminal] (as superuser) Parrot Terminal
Module 08: Sniffing
1 Hr 59 Min Remaining
Instructions Resources Help
8. Now, type cd and press Enter to jump to the root directory.
Click the Maximize Window icon to maximize the terminal window.
The interactive mode of the Yersinia application only works in a maximized terminal window.
9. Type yersinia -I and press Enter to open Yersinia in interactive mode.
-I: Starts an interactive ncurses session.
Previous
Next: Lab 2: Perform Network...


Module 08: Sniffing — Mozilla Firefox
Parrot Security
Applications Places System
Sun Feb 27, 19:21
Parrot Terminal
File Edit View Search Terminal Help
yersinia 0.8.2 by Slay & tomac - STP mode
[19:21:02]
RootId BridgeId Port Iface Last seen
Notification window
Warning: interface eth0 selected as the defaul
t one
Press any key to continue
Total Packets: 0
STP Packets: 0
MAC Spoofing [X]
You've got a message
STP Fields
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
Menu [Parrot Terminal] (as superuser) Parrot Terminal
Module 08: Sniffing
1 Hr 58 Min Remaining
Instructions Resources Help
9. Type yersinia -I and press Enter to open Yersinia in interactive mode.
-I: Starts an interactive ncurses session.
10. Yersinia interactive mode appears in the terminal window.
11. To remove the Notification window, press any key, and then press h for help.
12. The Available commands option appears, as shown in the screenshot.
Previous
Next: Lab 2: Perform Network...

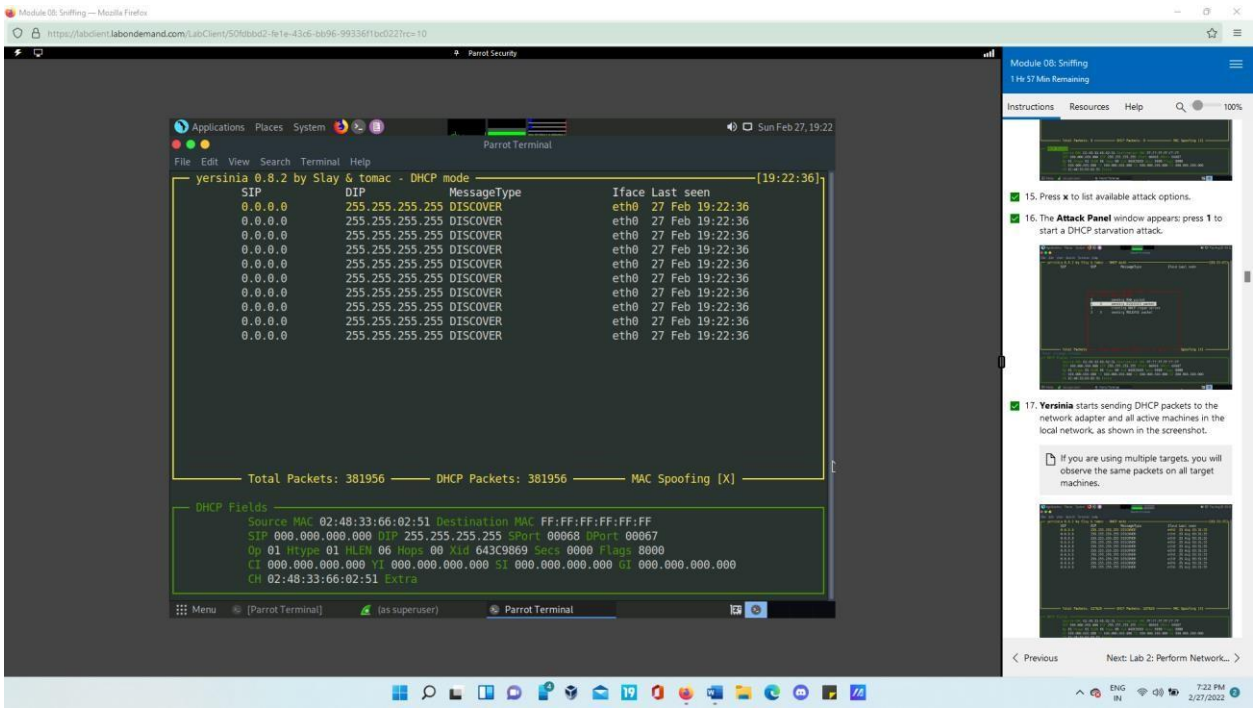


- Select DHCP mode by pressing F2. Now the STP fields will change to DHCP fields. To see a list of available attack options, press x.

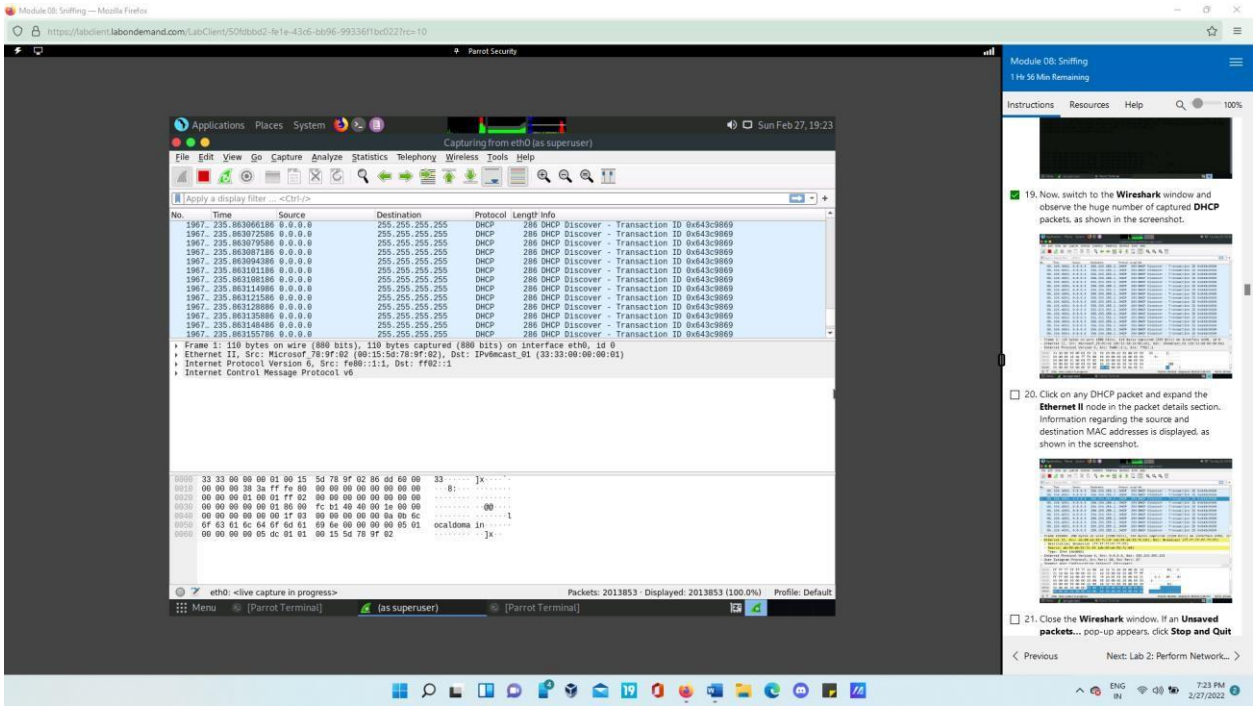




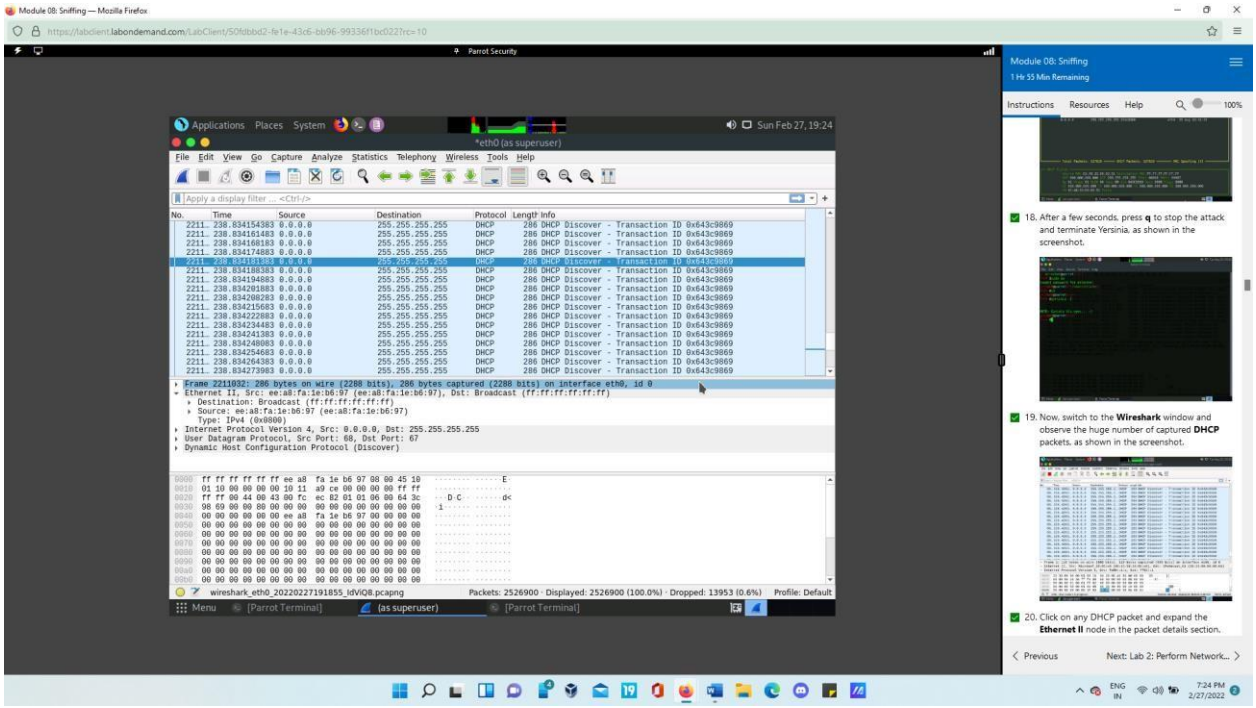
- Press 1 to launch a DHCP starvation attack in the Attack Panel window.



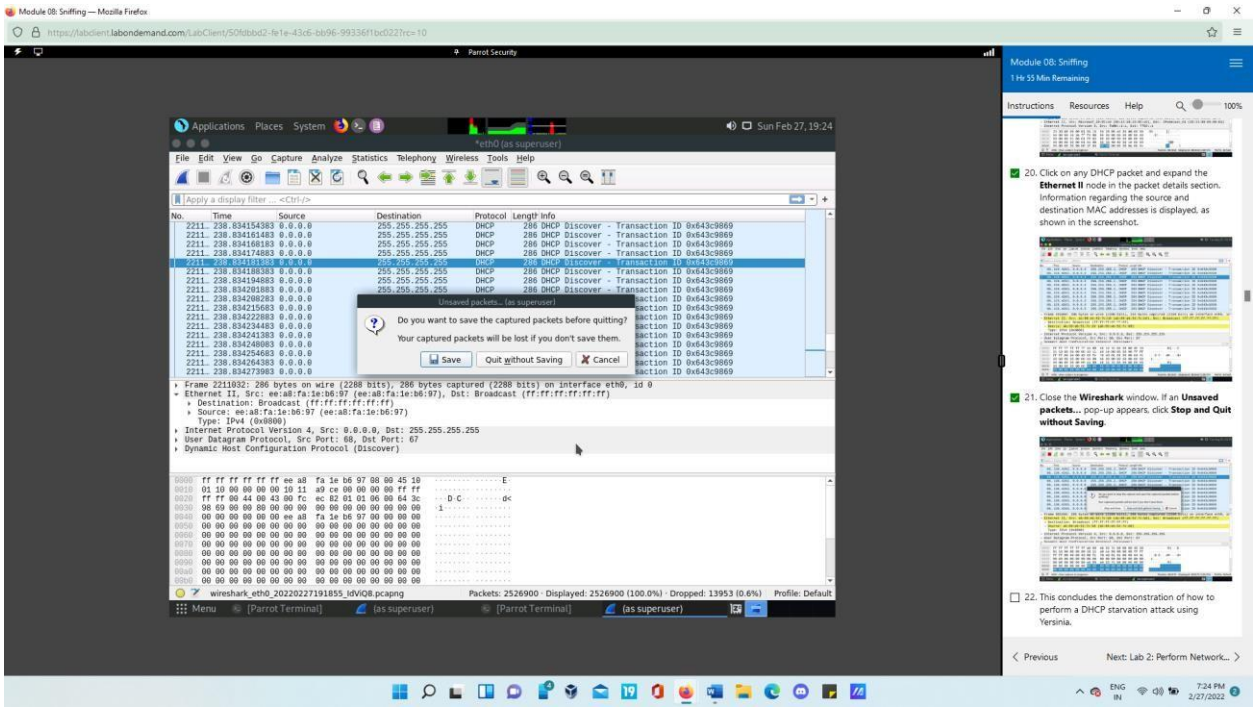
- Yersinia begins to transmit DHCP packets to the network adapter as well as all active machines in the local network. After some time, press **q** to terminate the attack and shutdown Yersinia.
- Now go back to Wireshark to observe large amount of DHCP packets.



- Select any DHCP packet and expand to packet details section to see source and destination MAC address.

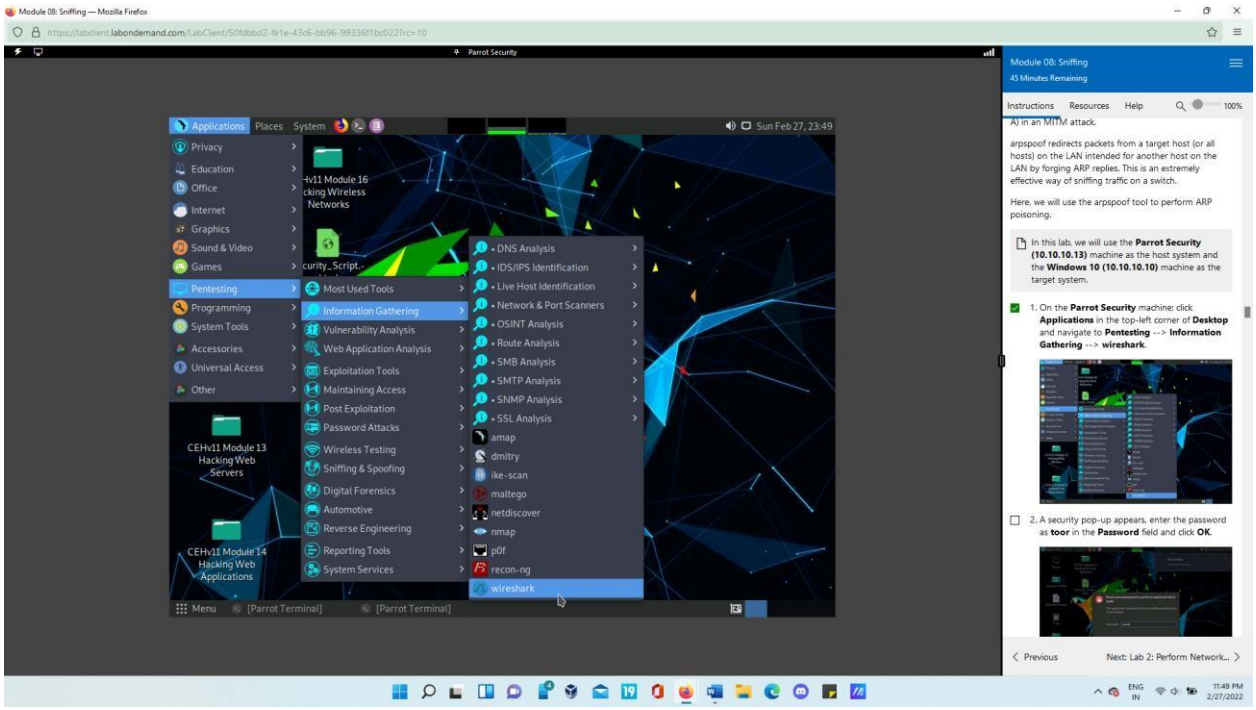


- Now close the Wireshark window.

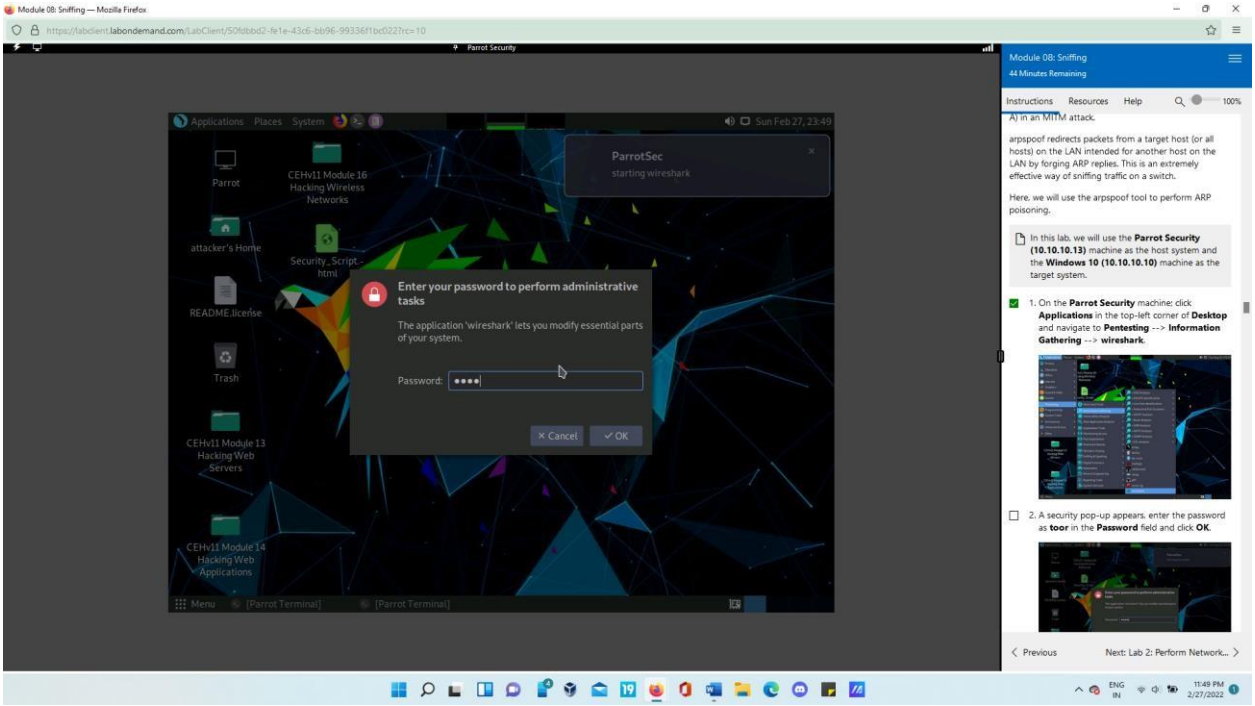


Task 3: Perform ARP Poisoning using Arp spoof

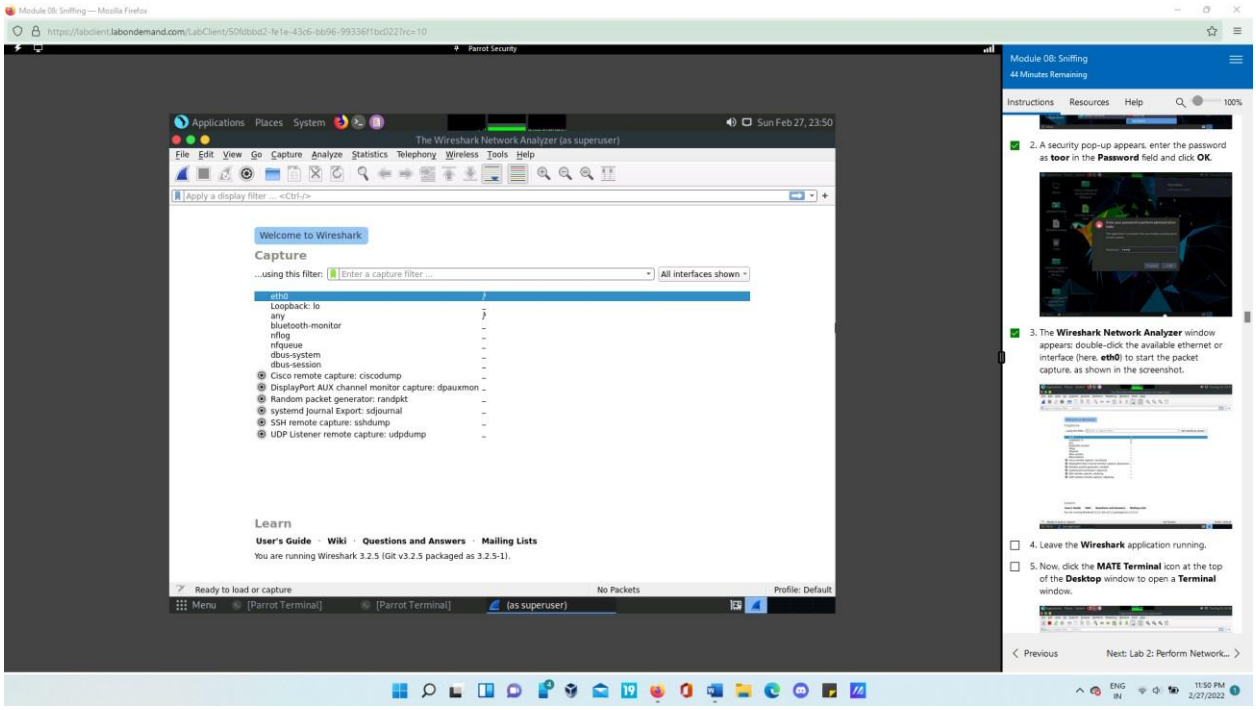
- Open Wireshark by navigating from the applications drop down menu.



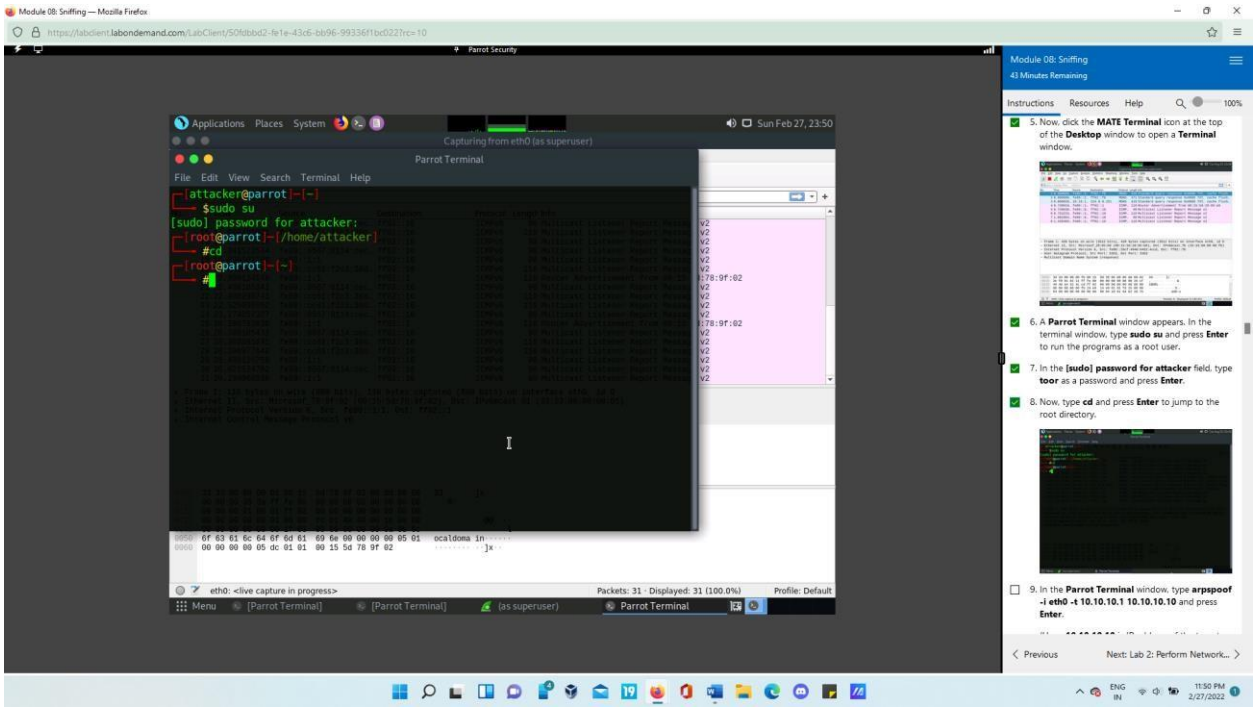
- Type password as toor and open Wireshark



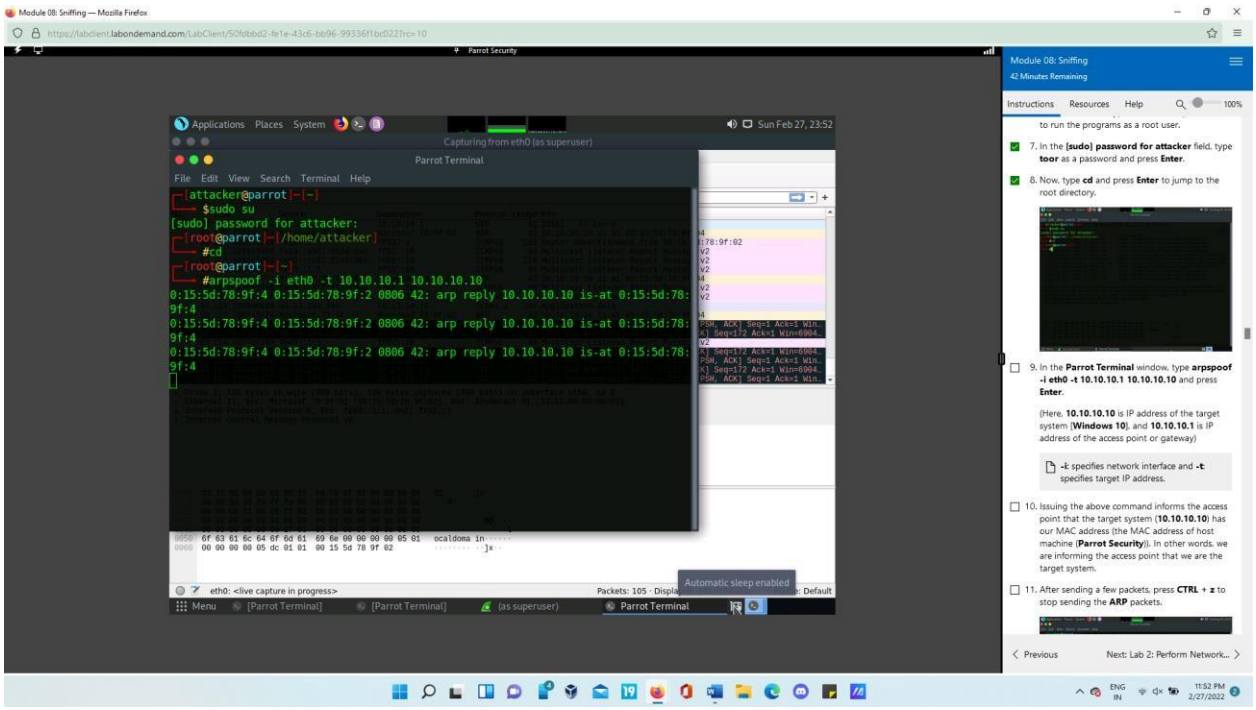
- Wireshark Network Analyzer opens and select Ethernet/eth0 to start packet capture.



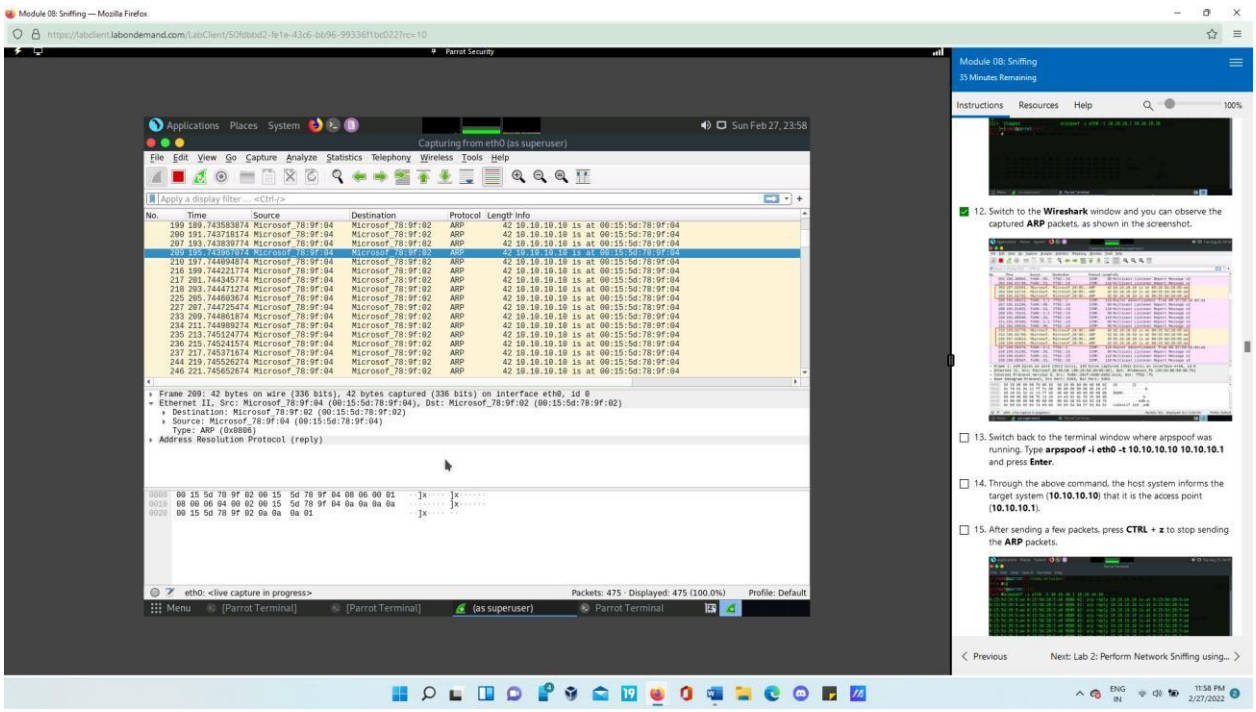
- In Mate terminal, obtain Sudo privileges and go to root directory.



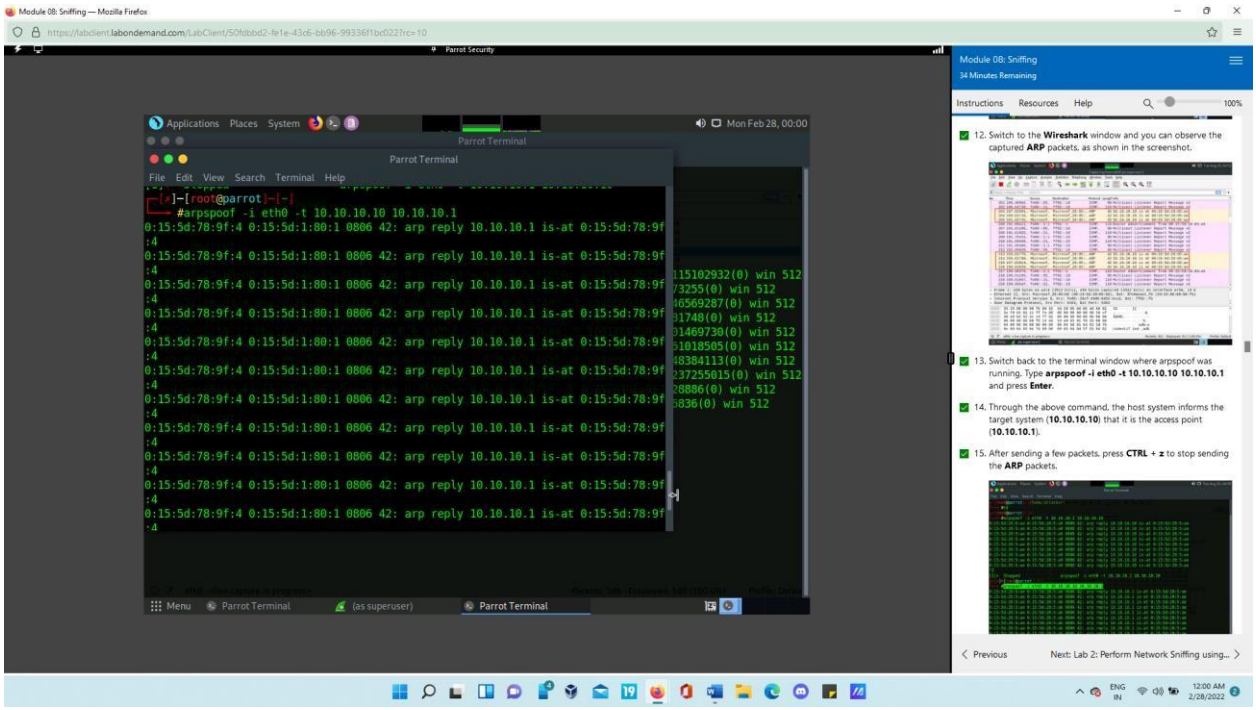
- Now in the terminal, type the command arpspoof -i eth0 -t 10.10.10.1 10.10.10.10 to send ARP packets, after few packets has been sent abort it by pressin ctrl+z.



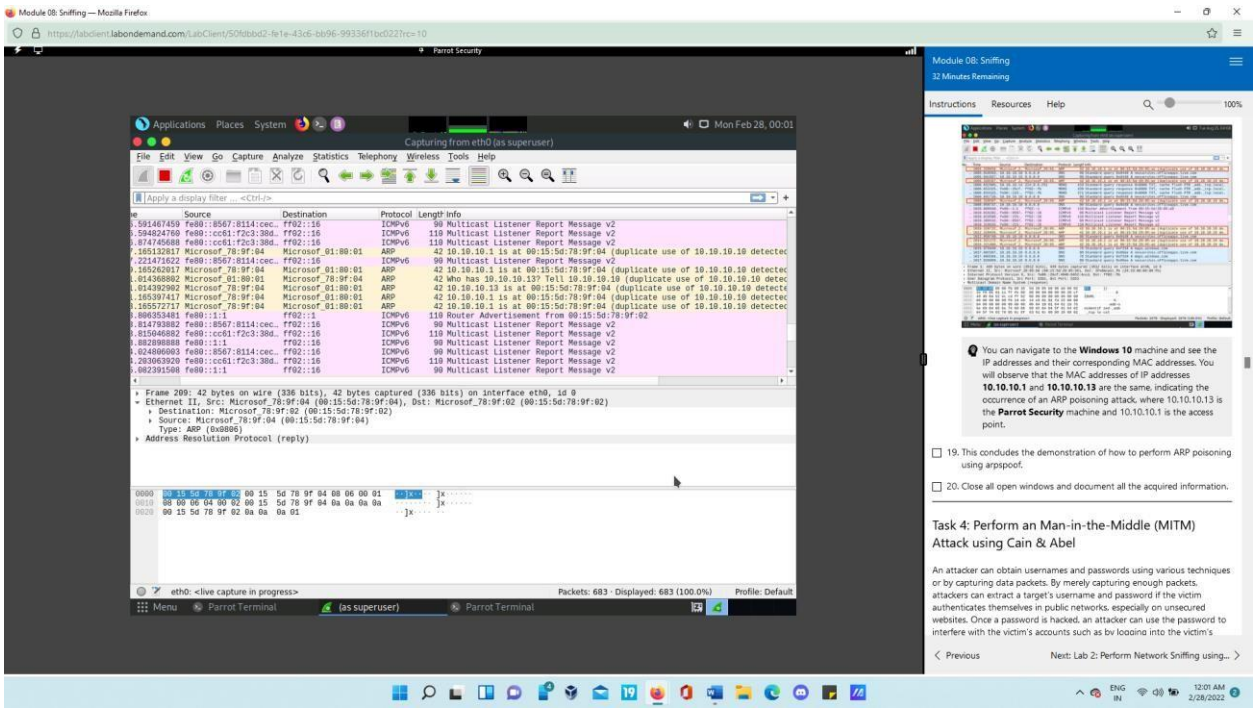
- Now go back to Wireshark to observe the ARP packets.



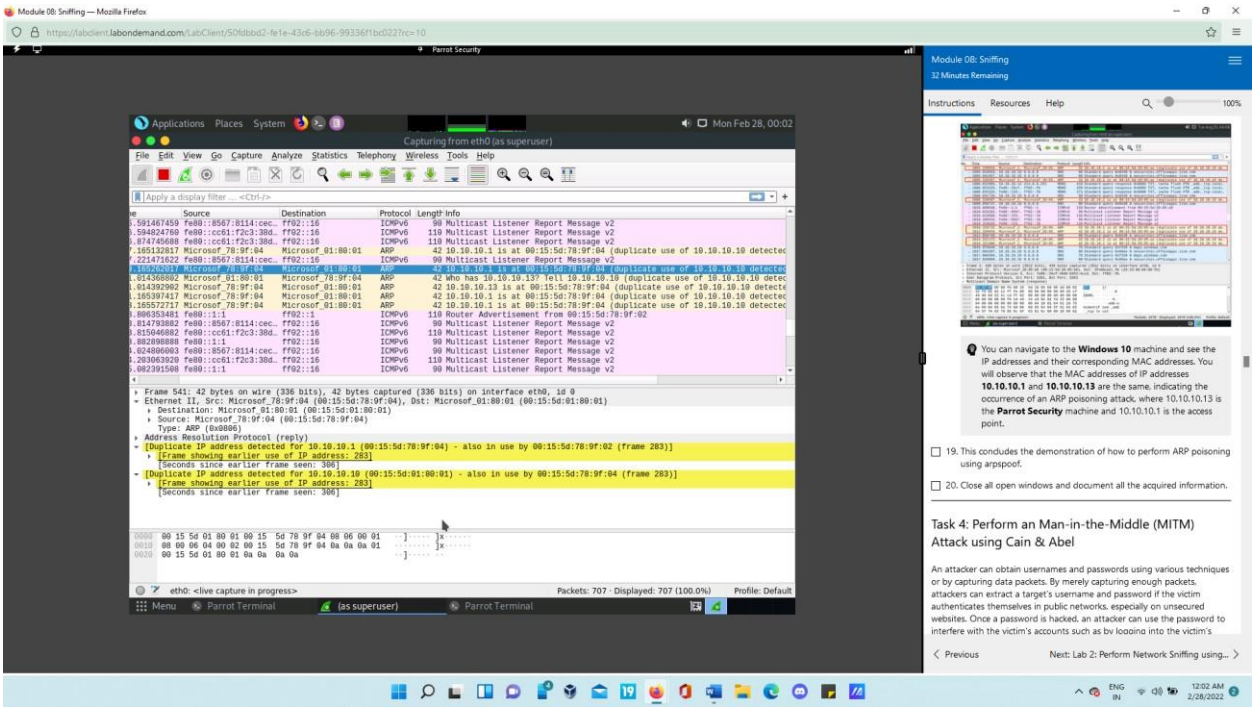
- Now switch back to terminal and type arpspoof -i eth0 -t 10.10.10.10 10.10.10.1. After sending few packets abort it by pressing ctrl+z.



- So, in Wireshark you can now see ARP packets with an alert “duplicate use of 10.10.10.10 detected”. Click on any ARP packet and go to packet details section to observe the MAC addresses of IP addresses 10.10.10.10 and 10.10.10.10.

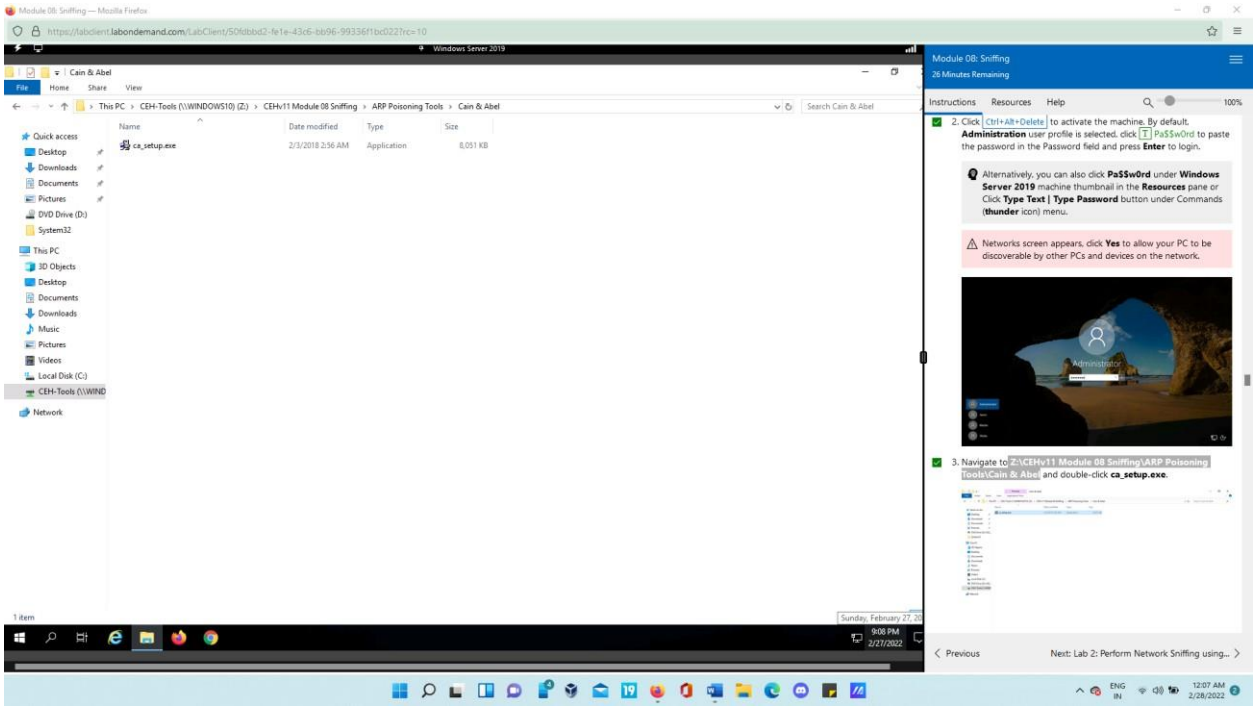


- Hence by using arpspoof, we assigned the MAC address of the host machine to the target machine and access point. Thereby, alert warning for a duplicate use of 10.10.10.10 was displayed.

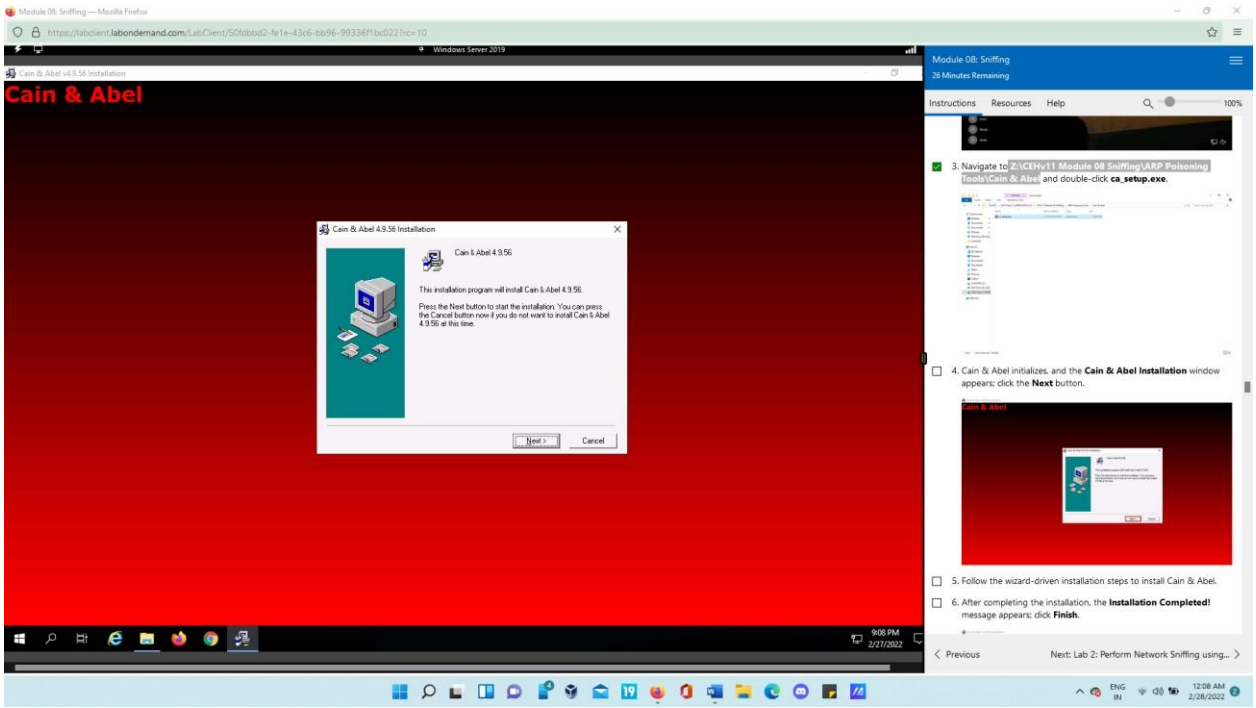


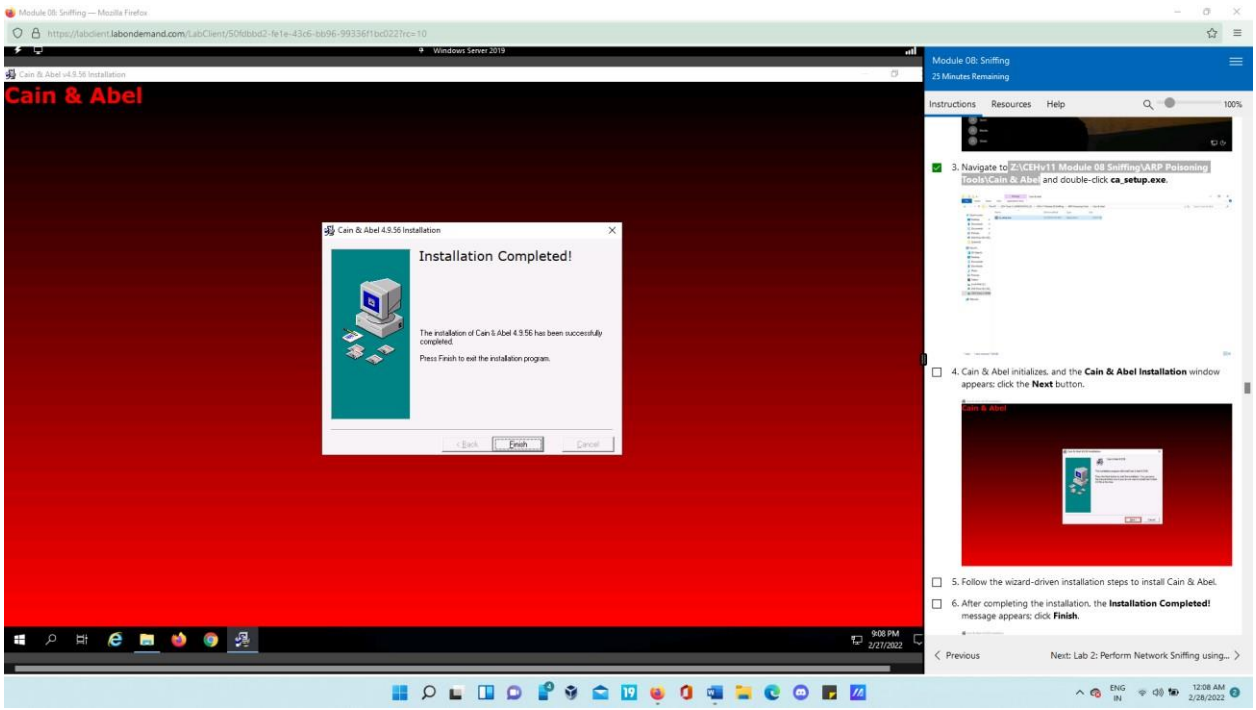
Task 4: Perform a Man-in-the-Middle (MITM) Attack using Cain & Abel

- Open Windows server 2019 and go to Z:\CEHv11 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel, then open the file ca_setup.exe.

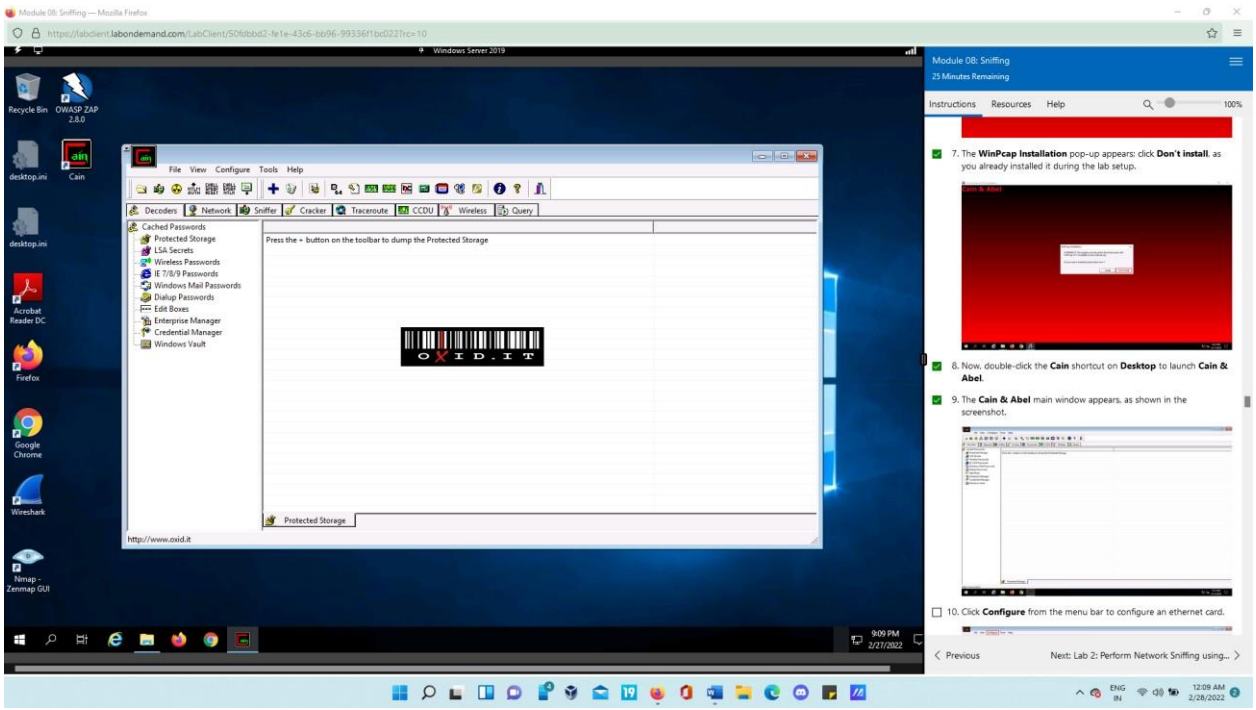


- Installation starts and by clicking next and accepting terms, complete the installation process.



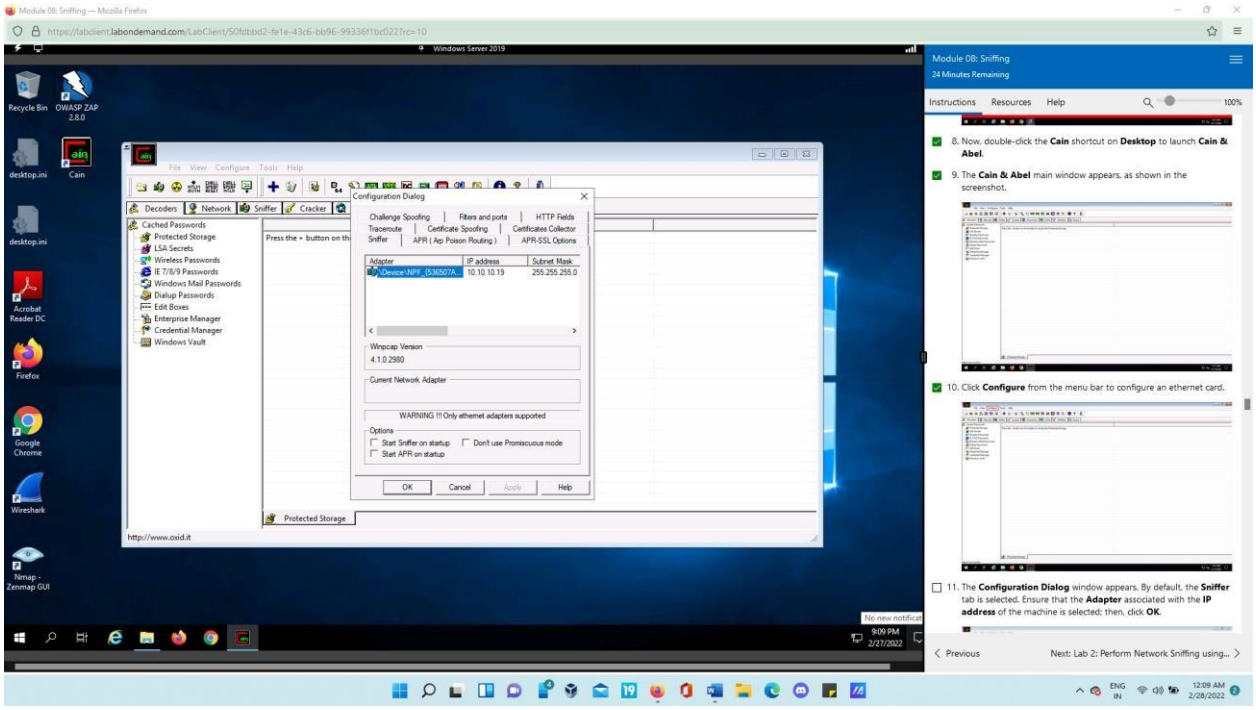


- In main window, click configure button to configure menu bar.

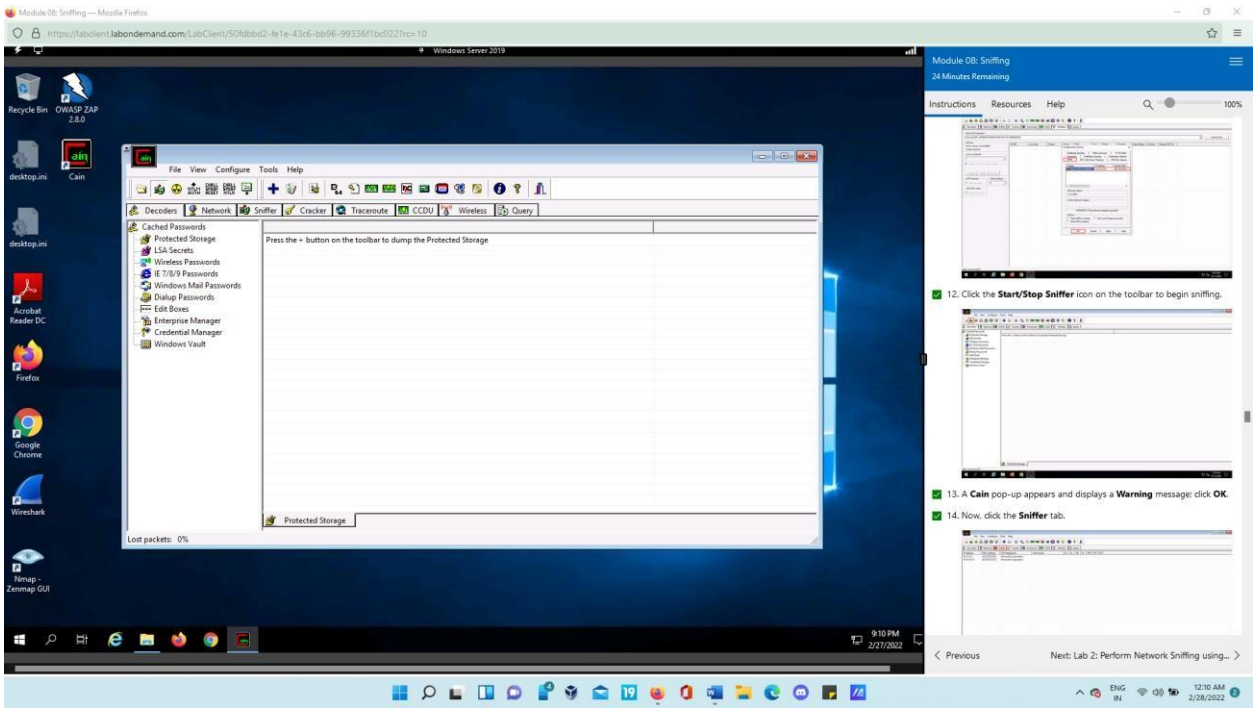


-

Configuration Dialog window opens, now by default Sniffer tab will be selected. We must make sure that the Adapter associated with the IP address of the machine is selected, then press ok.

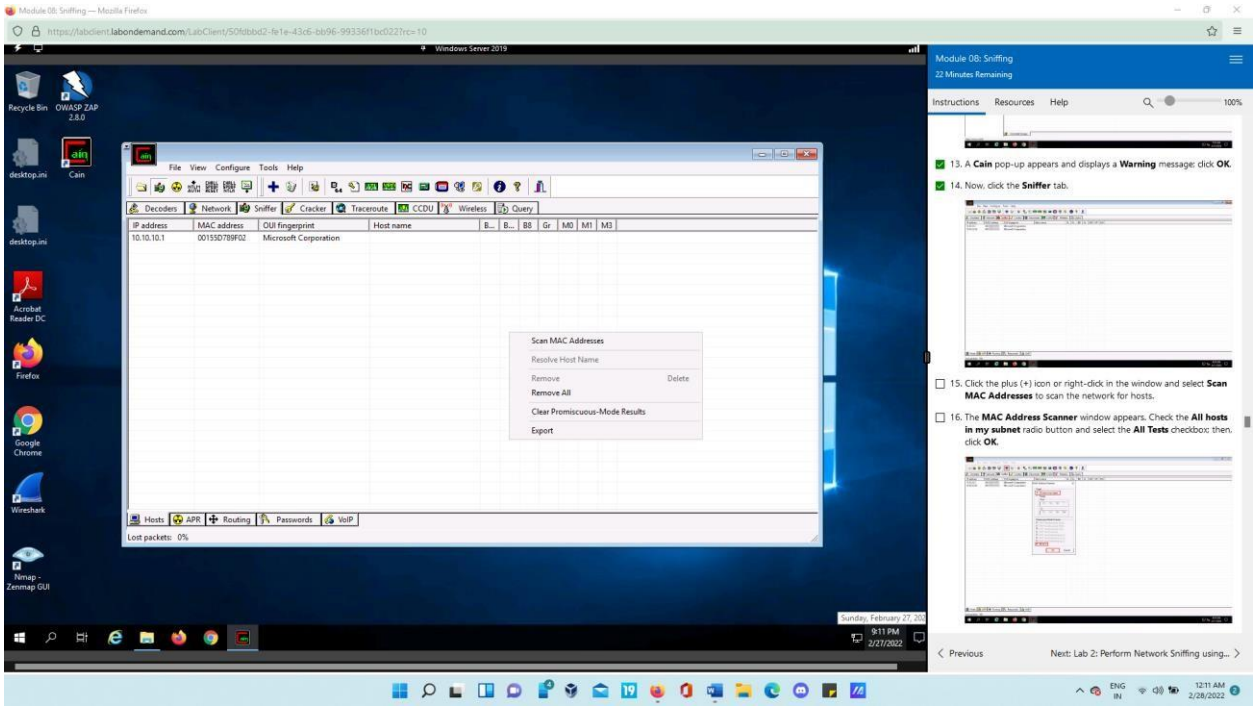


- To start sniffing, press start/stop sniffer button.

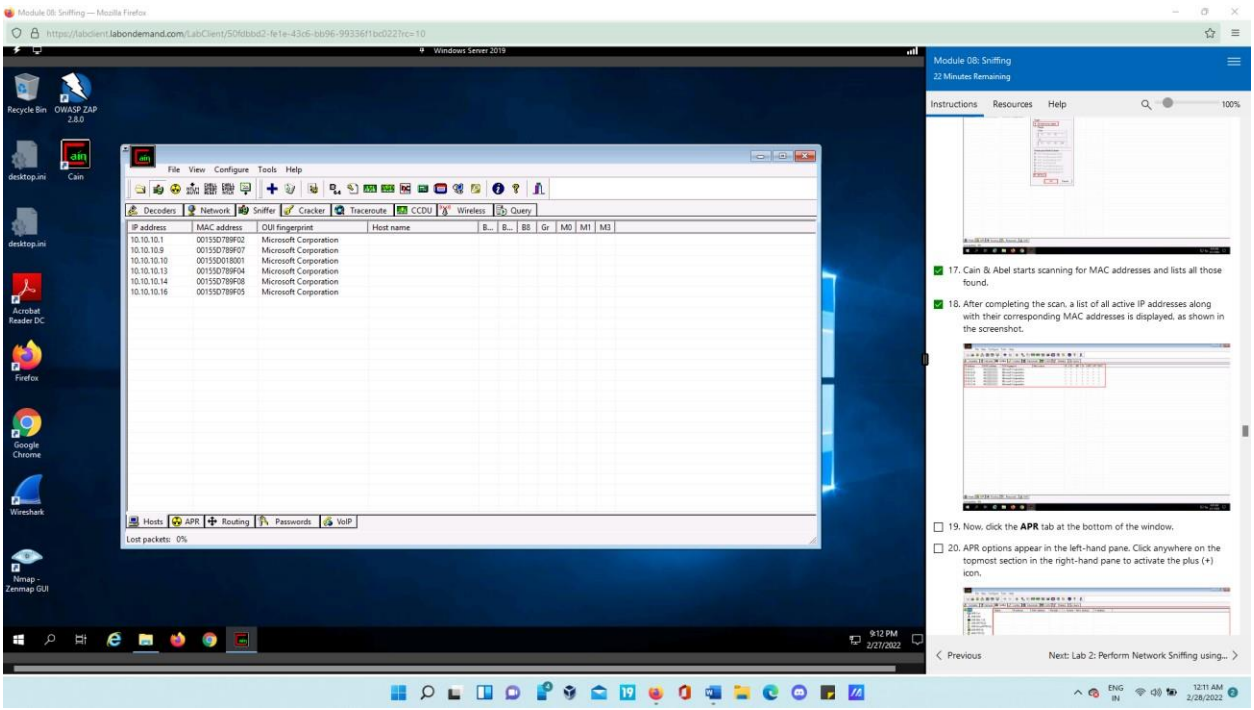


-

- Press sniffer tab and click + icon to select Scan MAC Addresses to scan host in the network.

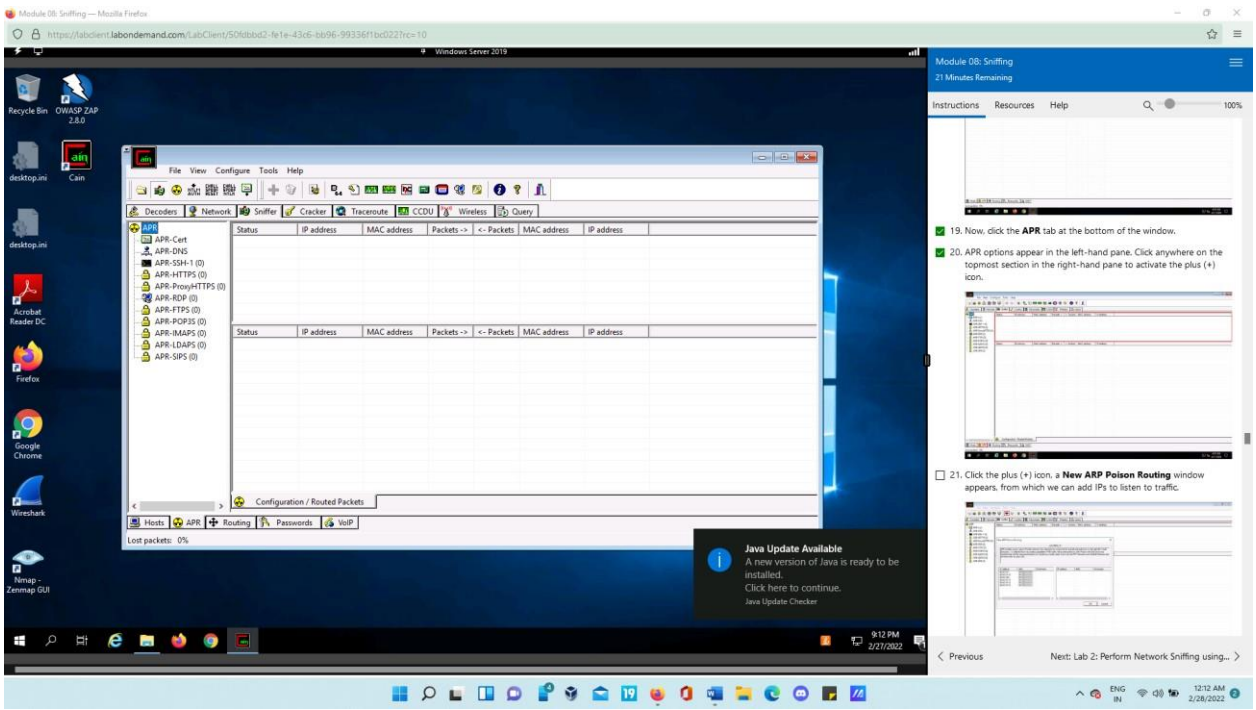


- Now MAC address scanner dialog box opens. Here, check all hosts in my subnet radio button, then press ok. Cain & Abel starts scanning for MAC addresses. When the scan in completed, all the active IP addresses and their MAC addresses are listed.



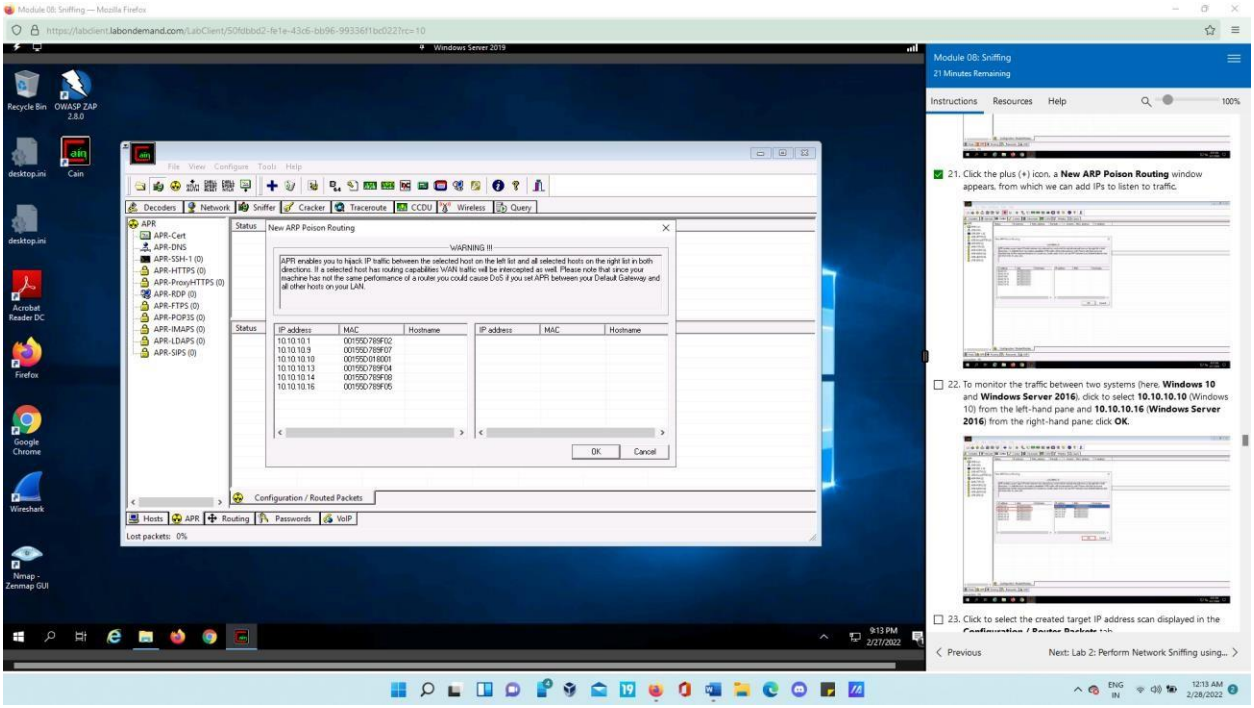
Now when you press APR button at the bottom of the window, APR options will appear.

- Now, click the **APR** tab at the bottom of the window. APR options appear in the left-hand pane.



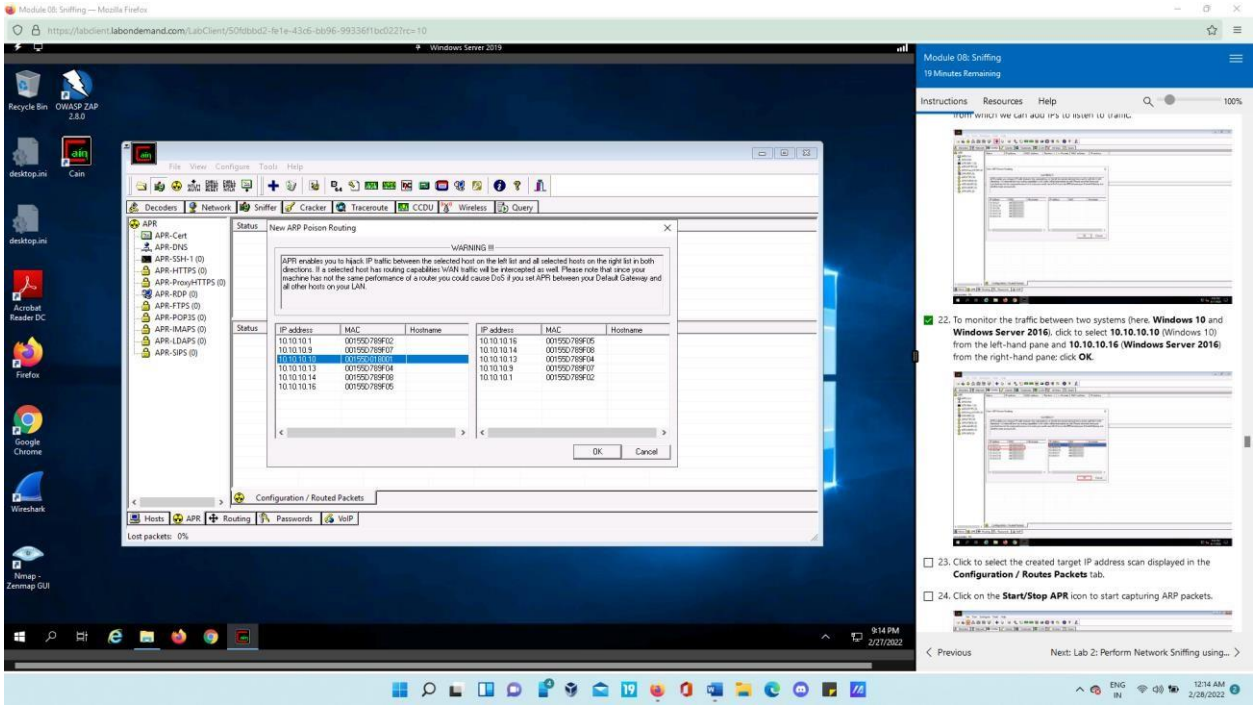
-

- Now press + icon, so that a new ARP poison routing window appears, from that we can add Ips to listen network traffic.



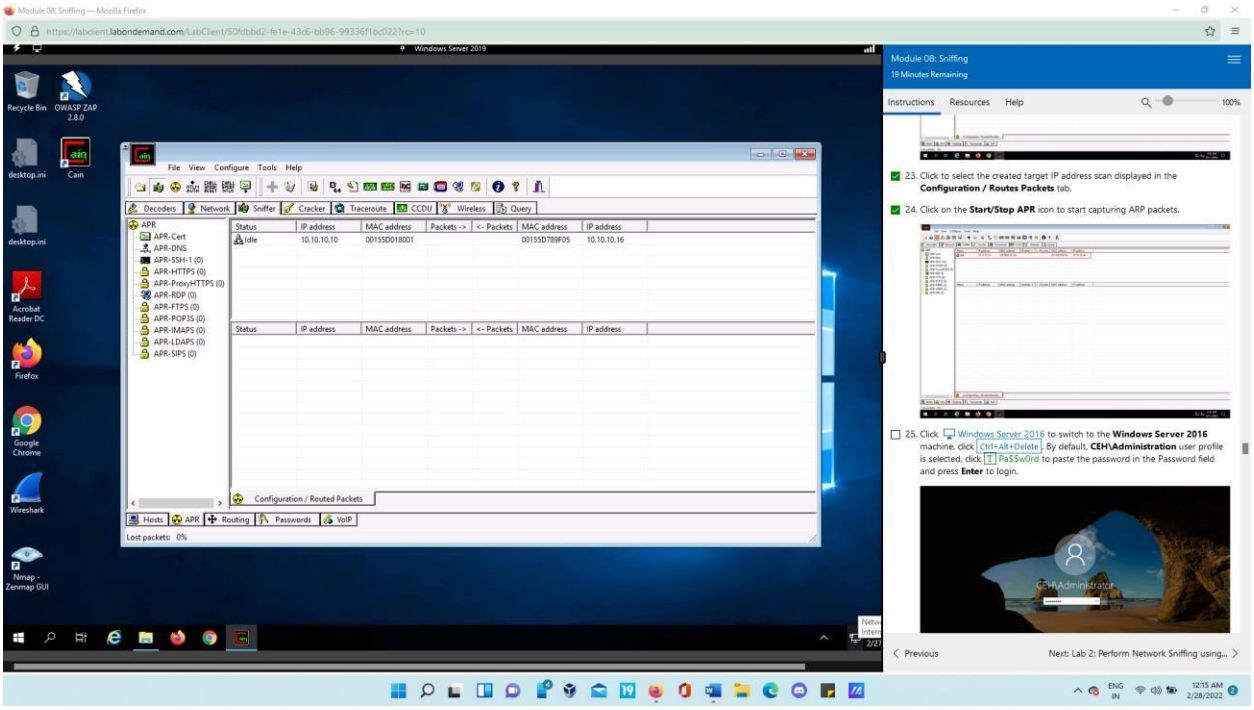
-

  Click 10.10.10.10 from the left-hand pane to view traffic coming from windows 10 and windows server 2016, and from the right-hand pane select 10.10.10.16, which is windows server 2016, then press ok.

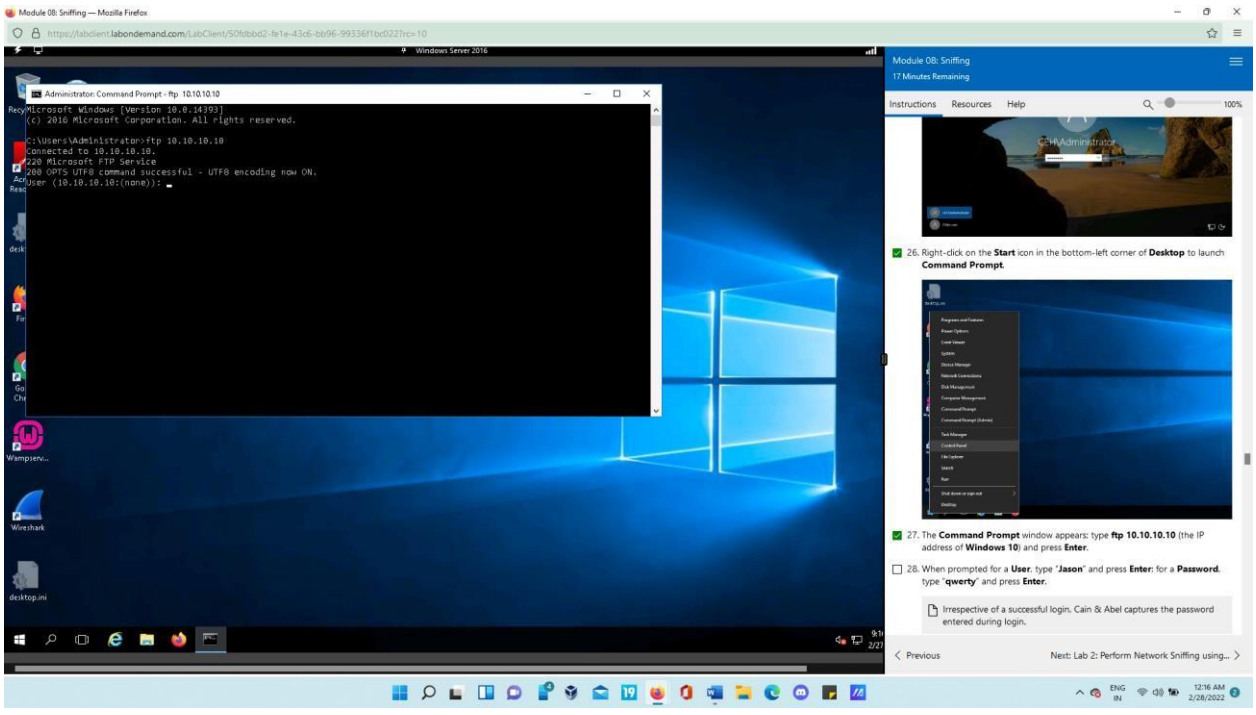


- Select the target IP address and start capturing ARP packets

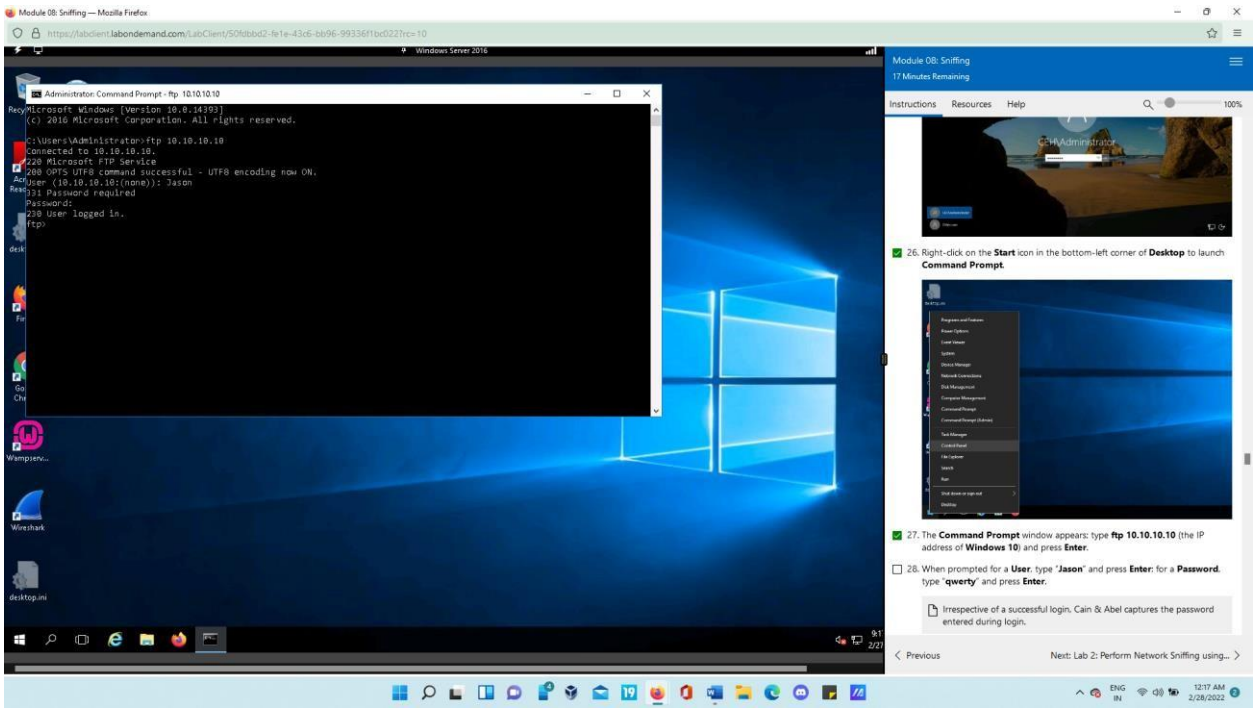
•



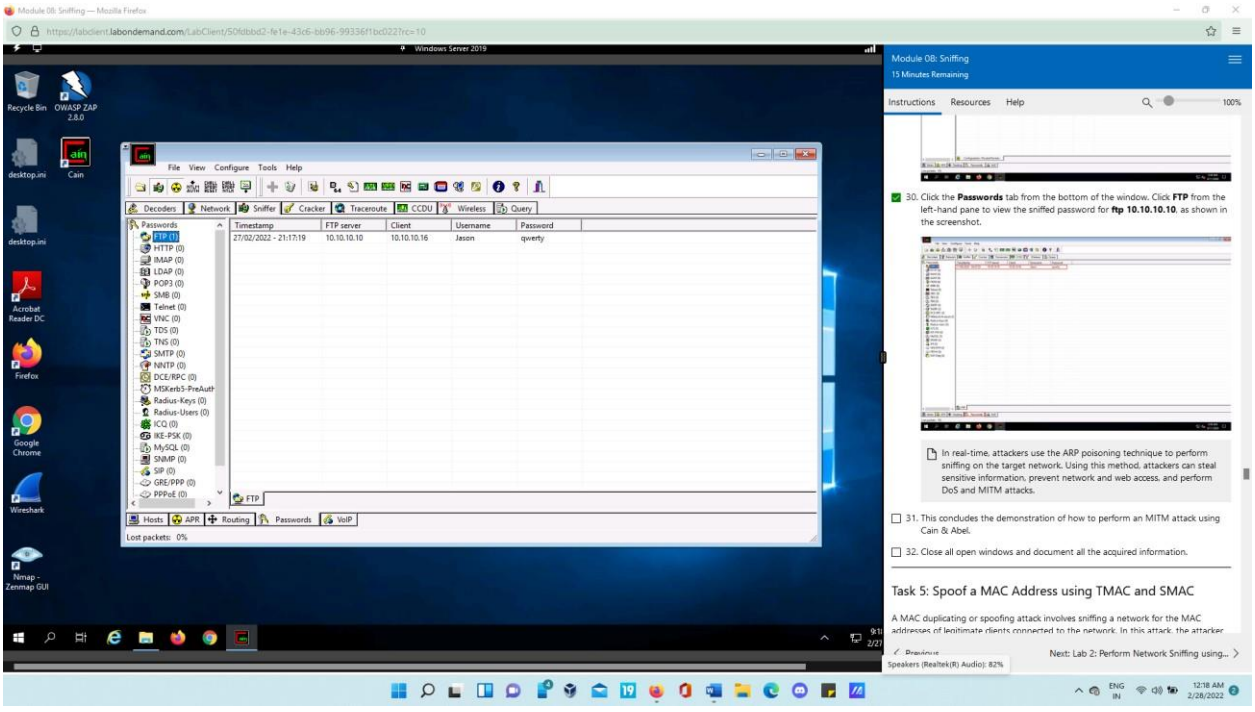
Now switch to Windows server 2016, and open command prompt. Then type ftp 10.10.10.10



- Type “Jason” for user and press enter for password, when asked.



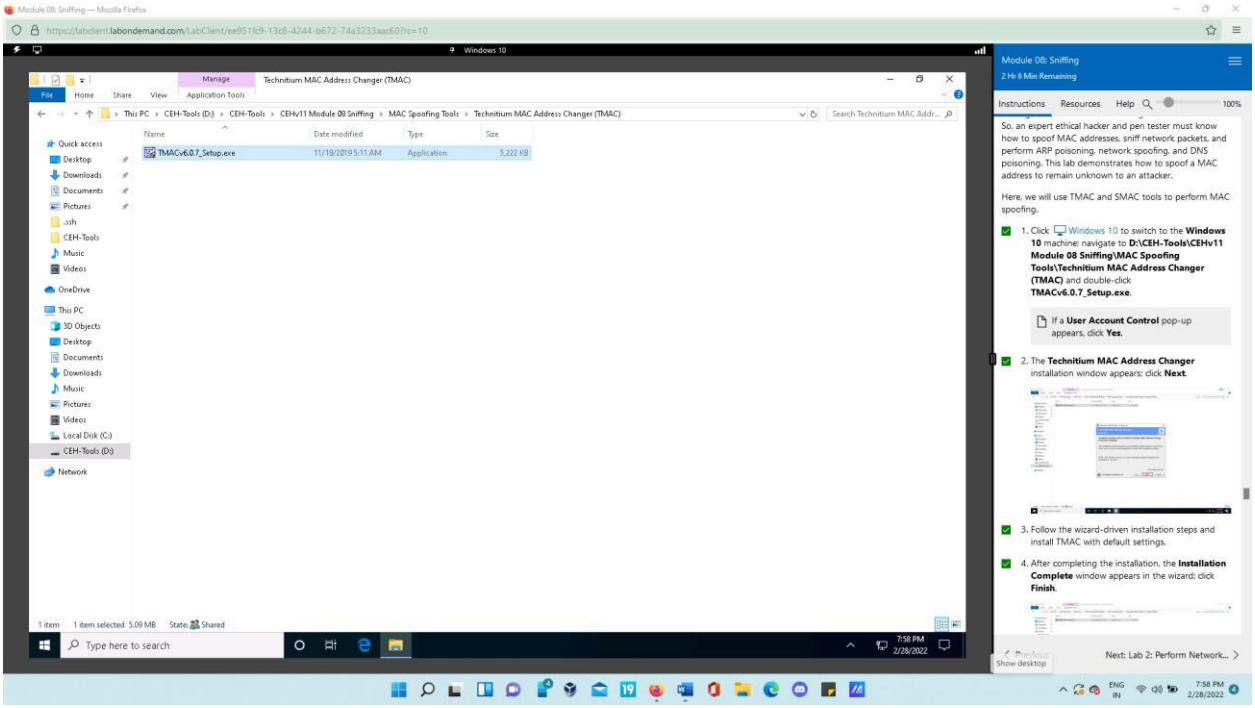
- Now go back to windows server 2019 and select FTP from the left-hand pane to observe the sniffed password for ftp 10.10.10.10.



•

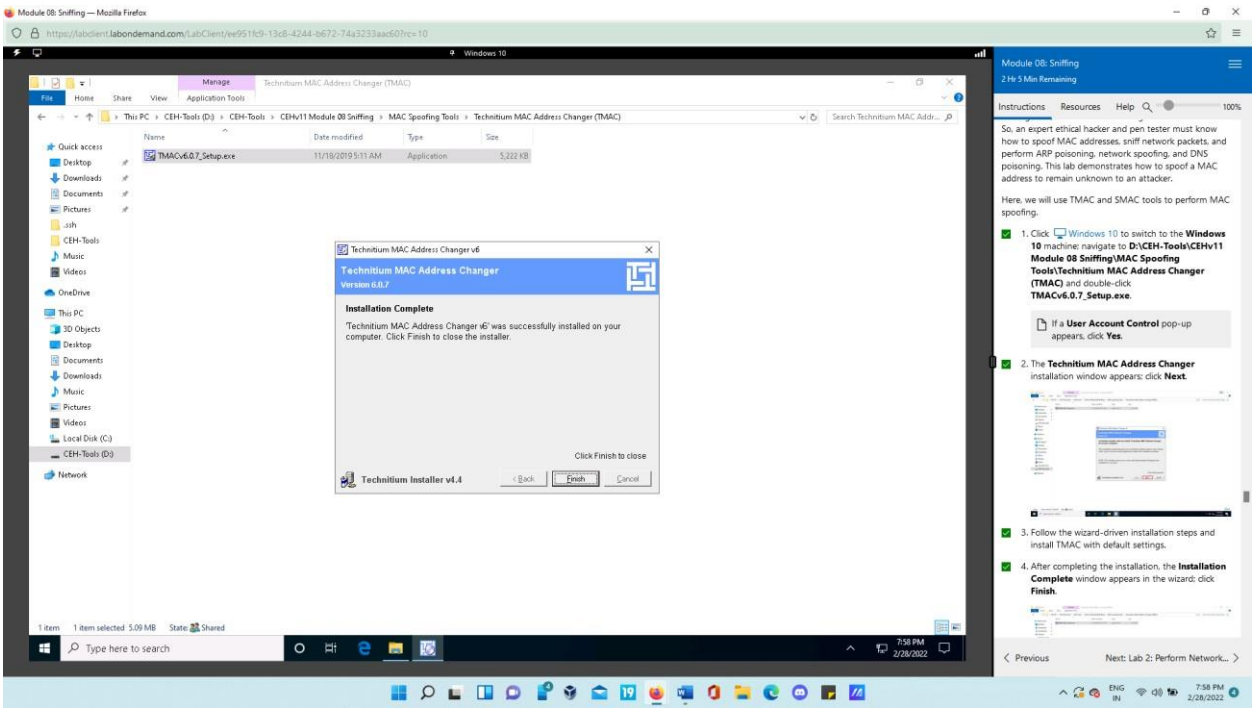
Task 5: Spoof a MAC Address using TMAC and SMAC

- Go to Windows10 machine, navigate to D:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC) and open file TMACv6.0.7_Setup.exe and install the Technitium MAC address changer.

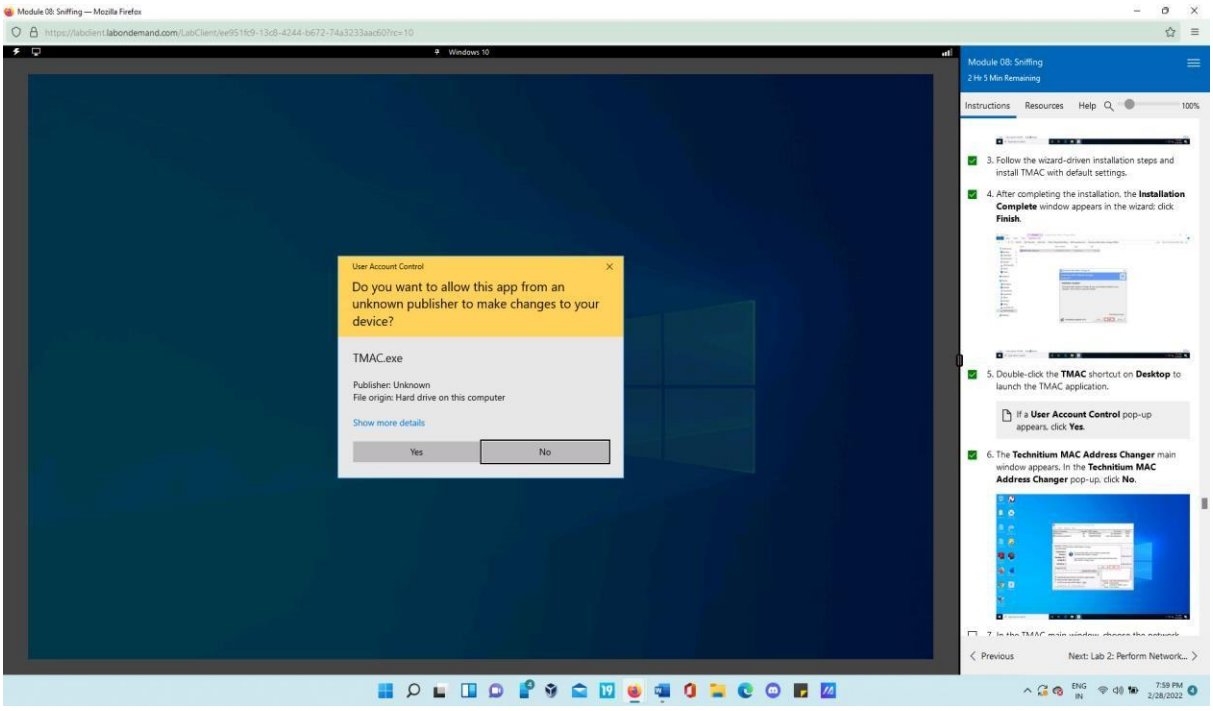


- Press finish to complete the installation.

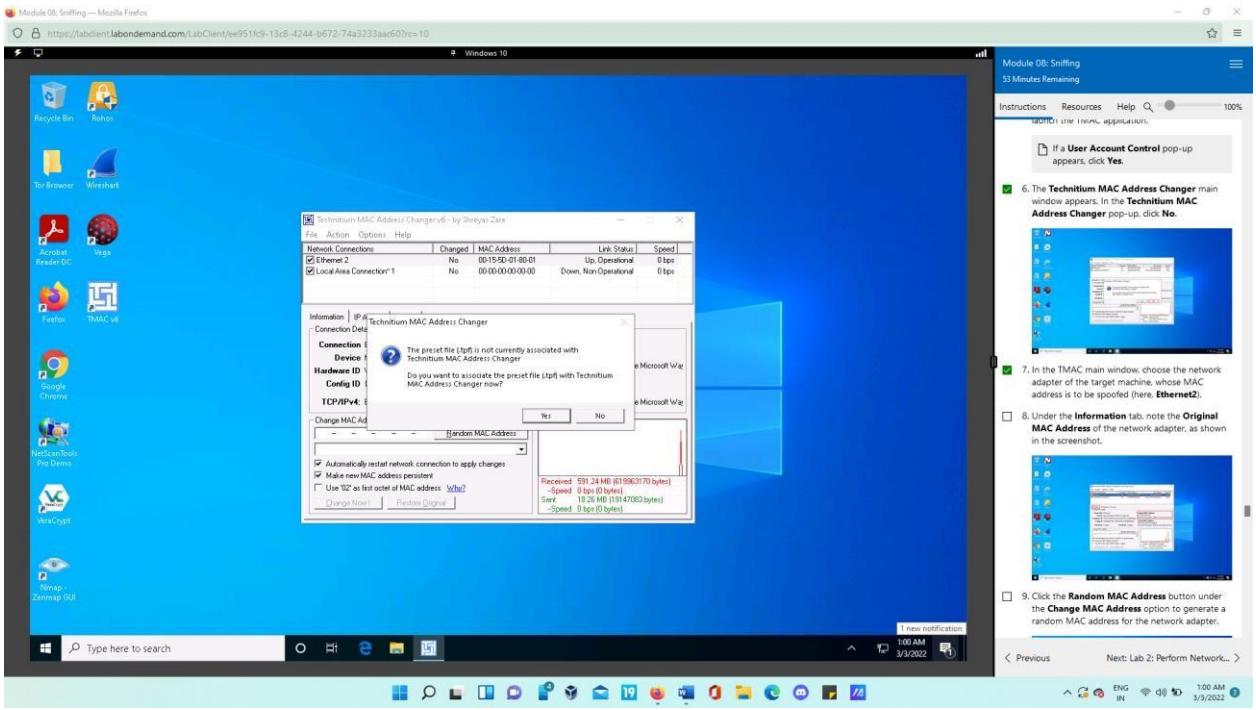
•



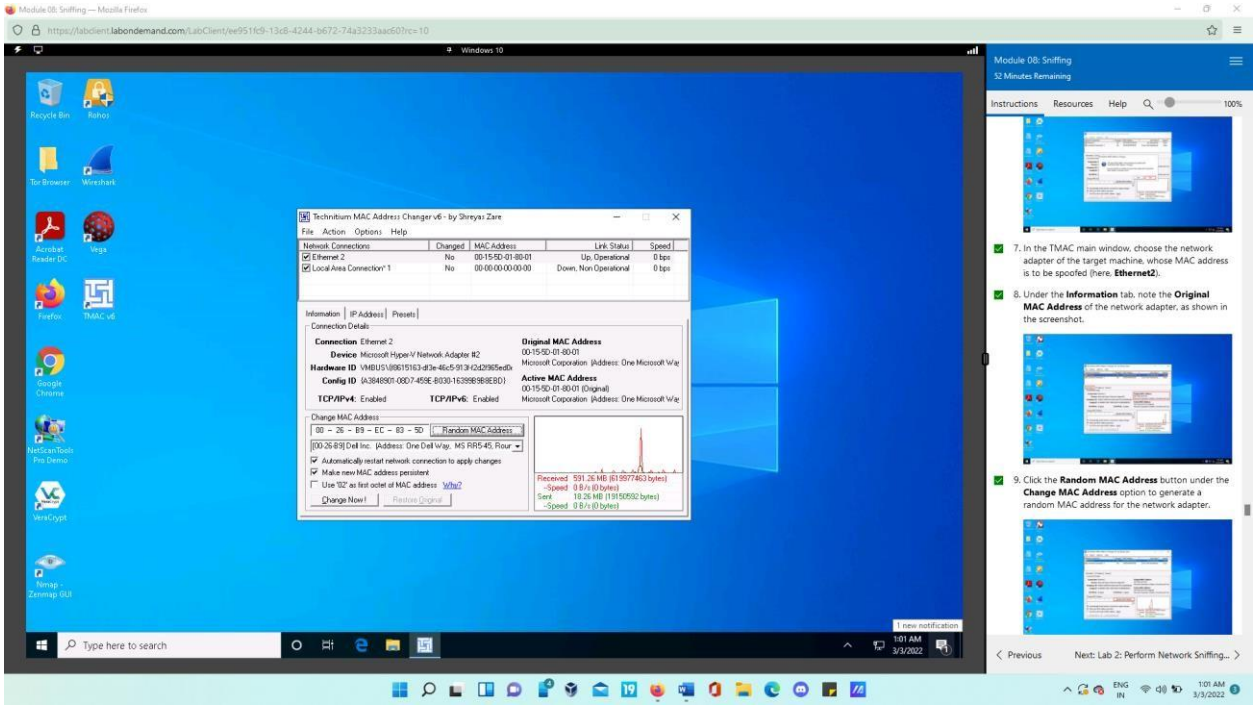
- Open TMAC from Desktop.



- Click No in the pop-up window.

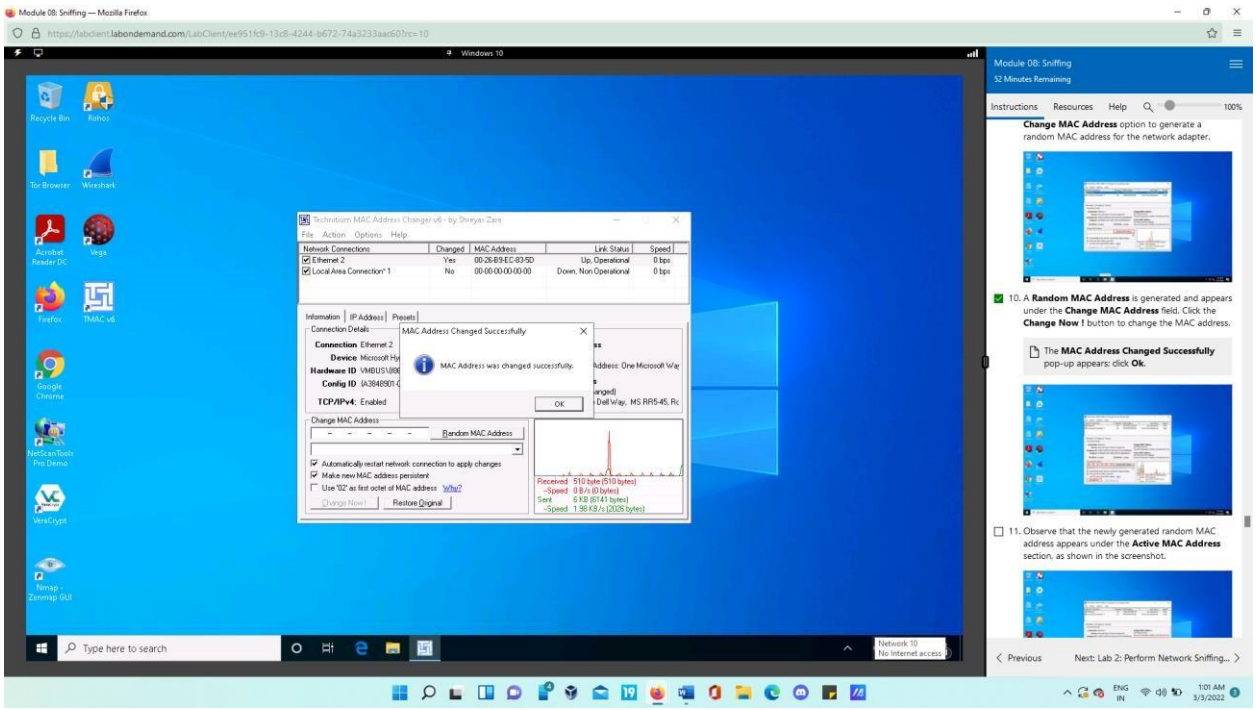


Note the Original MAC Address of the network adapter under the Information tab, as shown in the screenshot. To generate a random MAC address for the network adapter, click the Random MAC Address button beneath the Change MAC Address option.



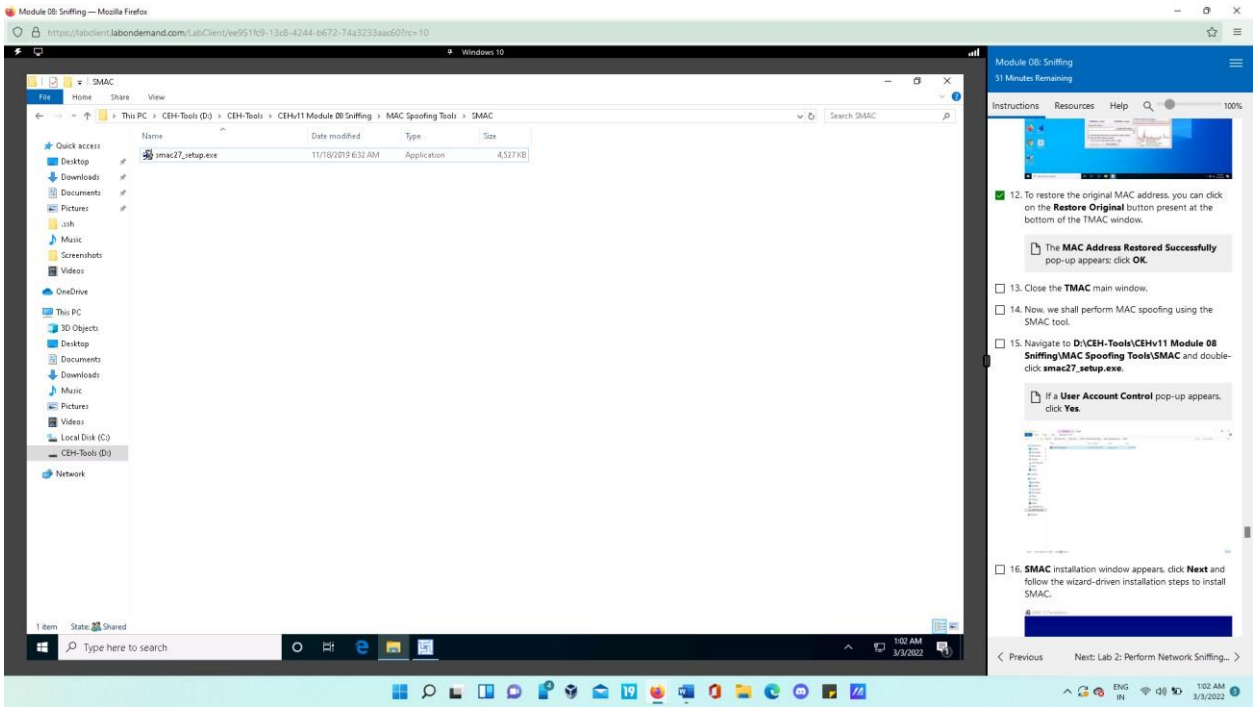
- Generated random MAC address will appear in the change MAC address field. Press “change now” to change the address.

•

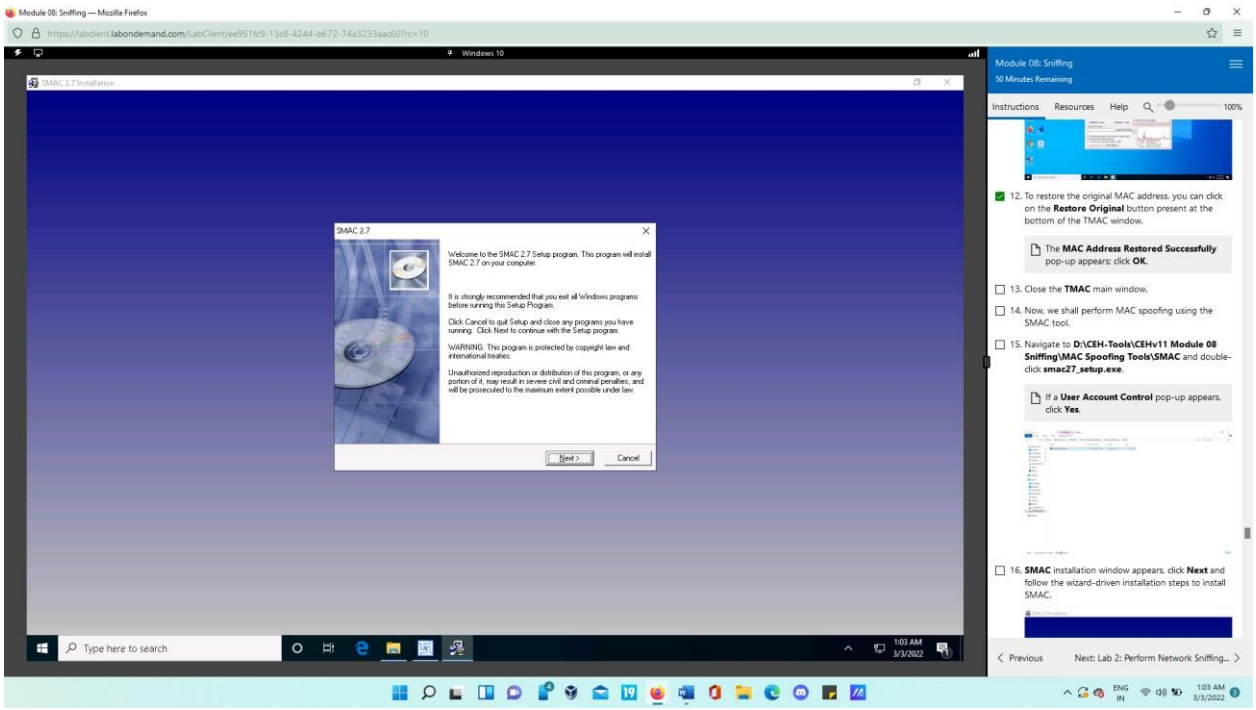

Module 08: Sniffing — Mozilla Firefox
Windows 10
Module 08: Sniffing
52 Minutes Remaining
Instructions
Resources
Help
Change MAC Address option to generate a random MAC address for the network adapter.
10. A Random MAC Address is generated and appears under the Change MAC Address field. Click the Change Now ! button to change the MAC address.
The MAC Address Changed Successfully pop-up appears: click Ok.
11. Observe that the newly generated random MAC address appears under the Active MAC Address section, as shown in the screenshot.
Previous
Next: Lab 2: Perform Network Sniffing...
MAC Address Changed Successfully
MAC Address was changed successfully.
OK
Random MAC Address
Change Now!
Restore Original
Type here to search

-

Navigate to D:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC and execute smac27_setup.exe.

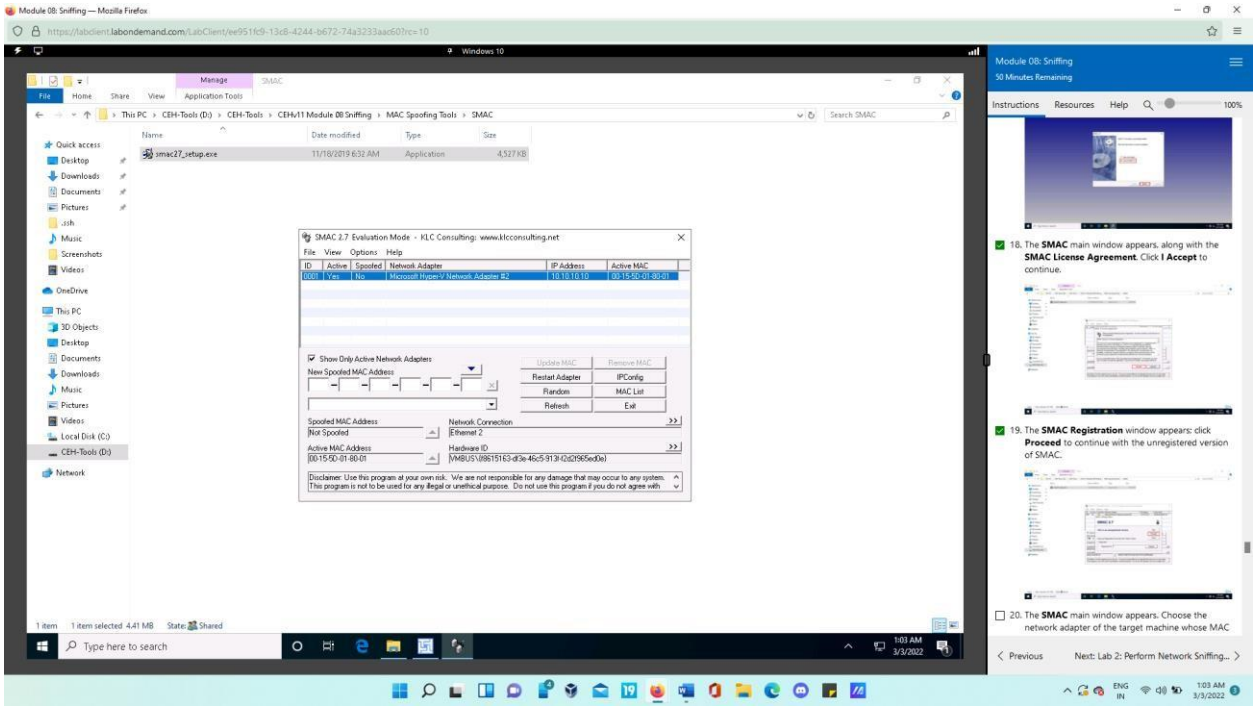


- Press next and finish the installation process



•

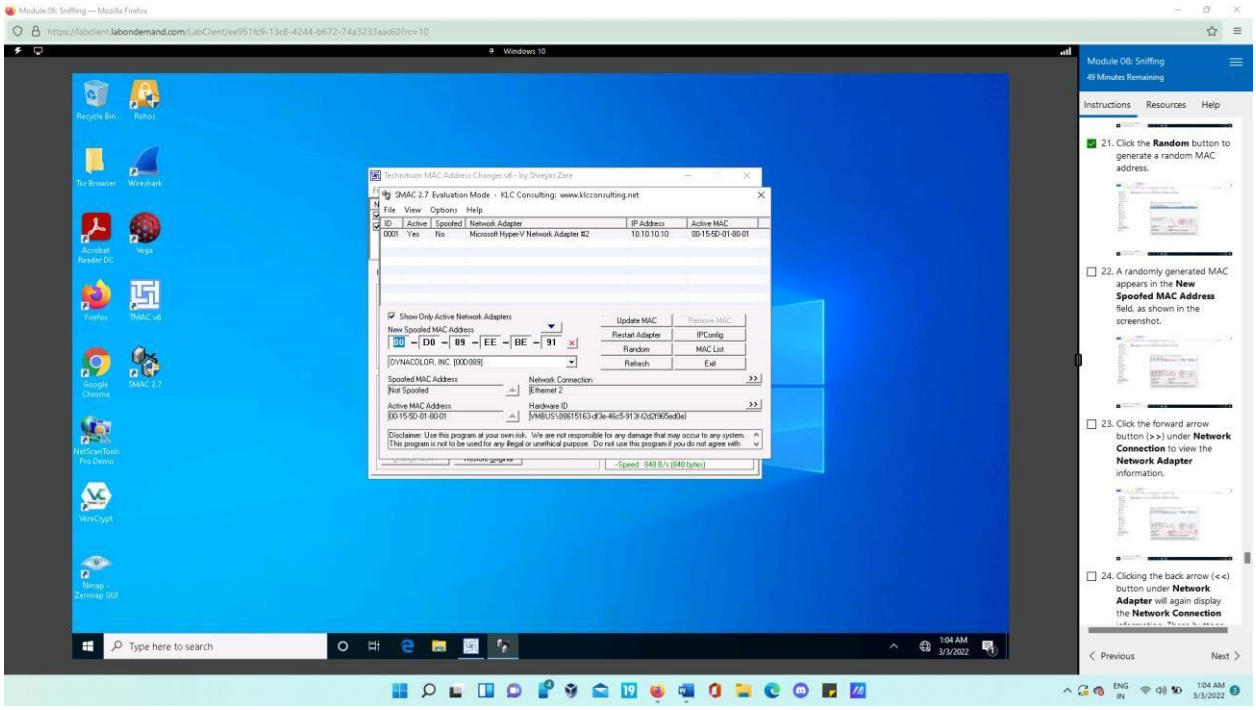
Now launch the SMAC.



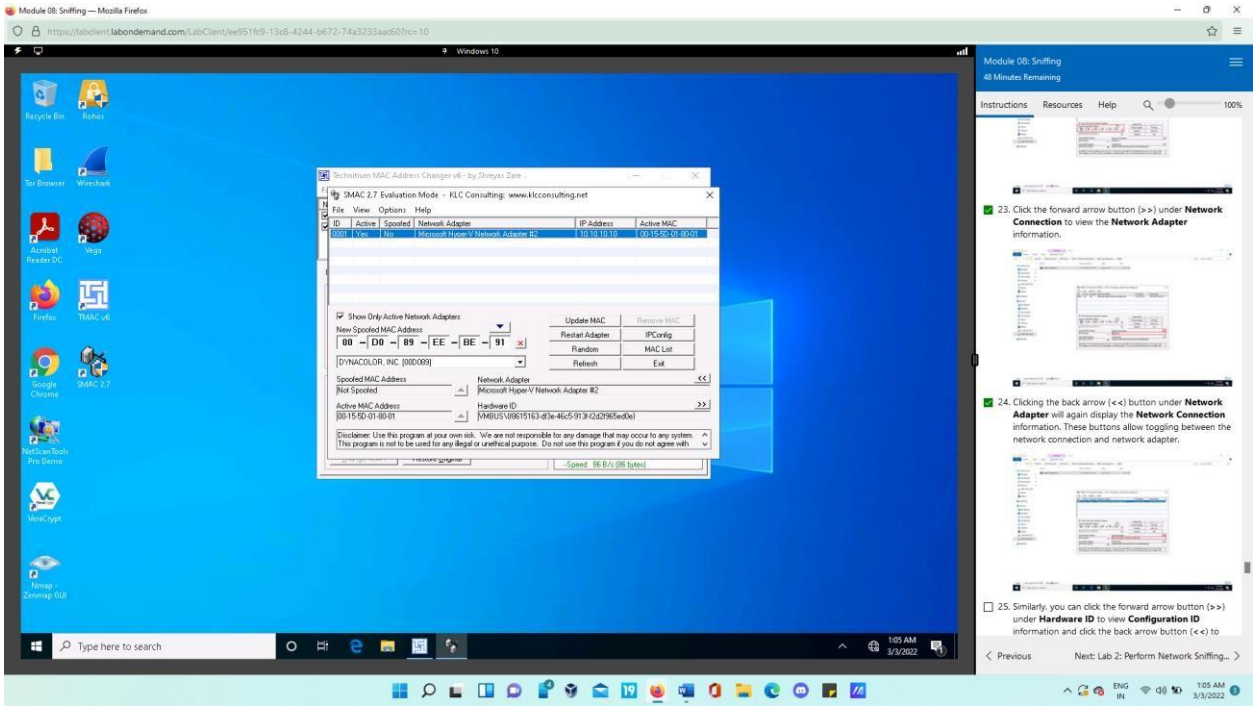
- Now in the SMAC main window, we will select the network adapter of the target machine whose MAC address we want to spoof.

- Here, press “random” button to list out random MAC address. Then, a randomly generated MAC address will be appeared in New spoofed MAC address field.

•

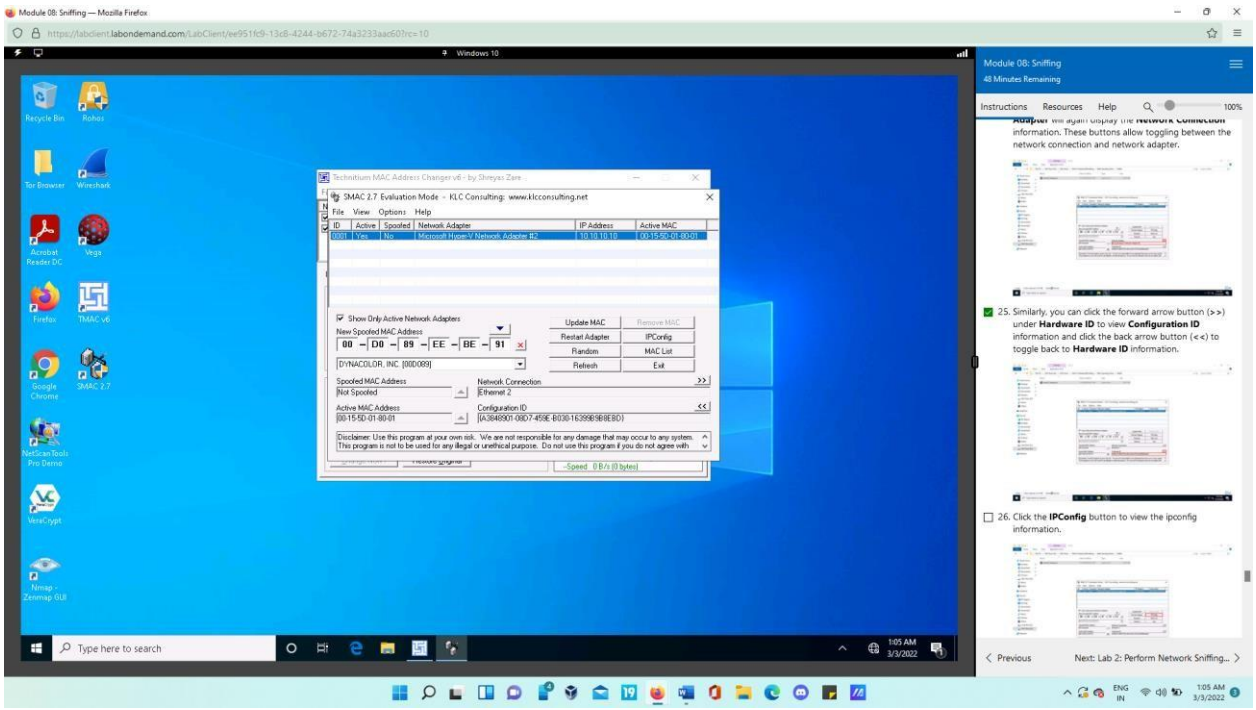


After that, view Network Adapter information by pressing (>>) button under Network connection.

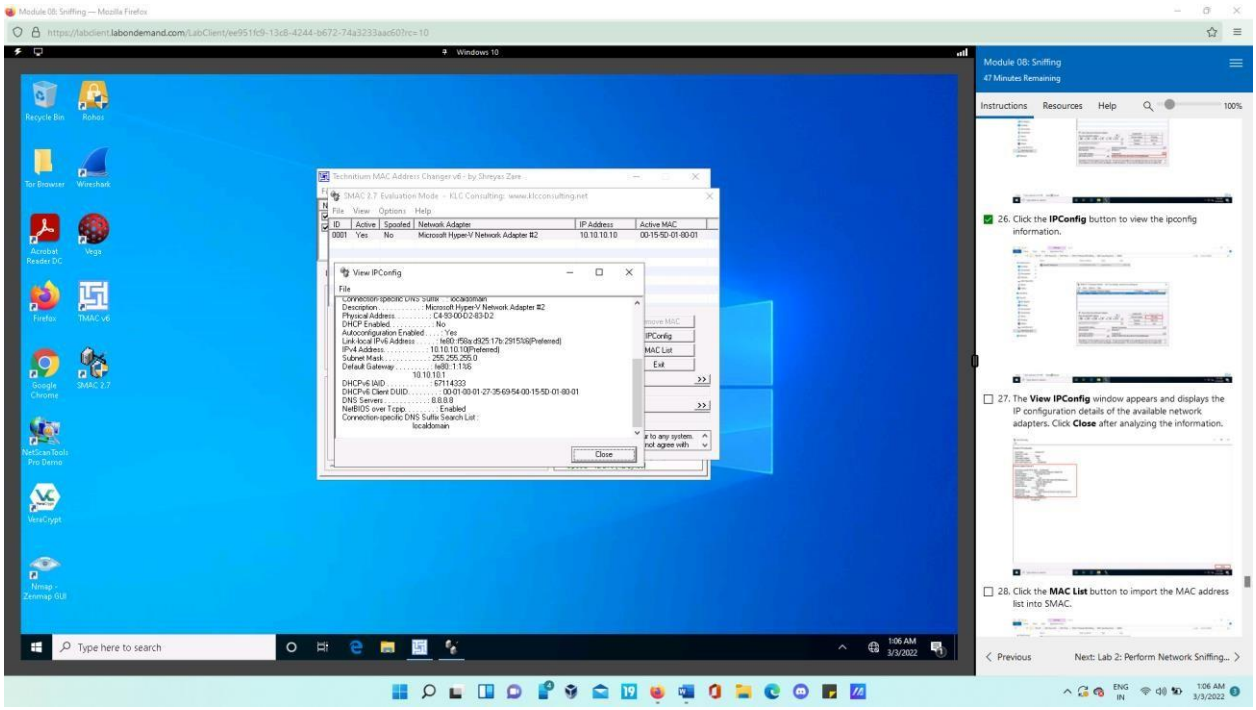


- Also, we can use (>>) option in Hardware ID to display the Configuration ID.

•

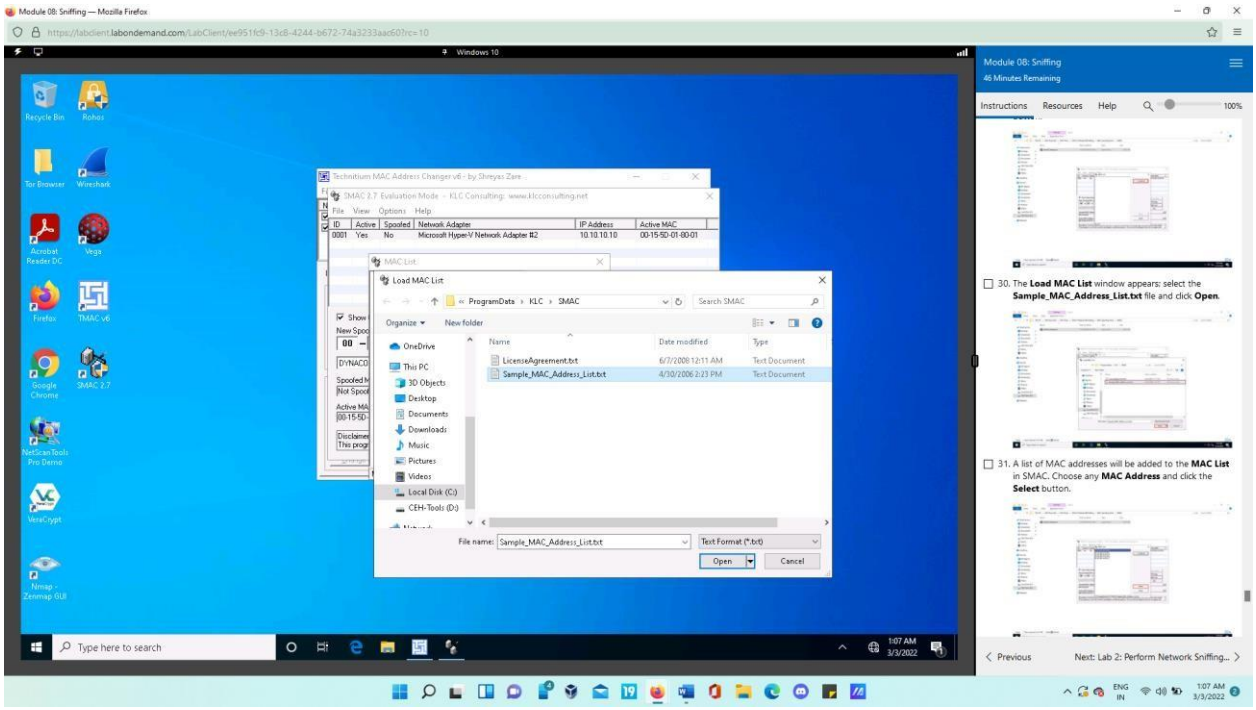


Use IPConfig option to view ipconfig information.



-

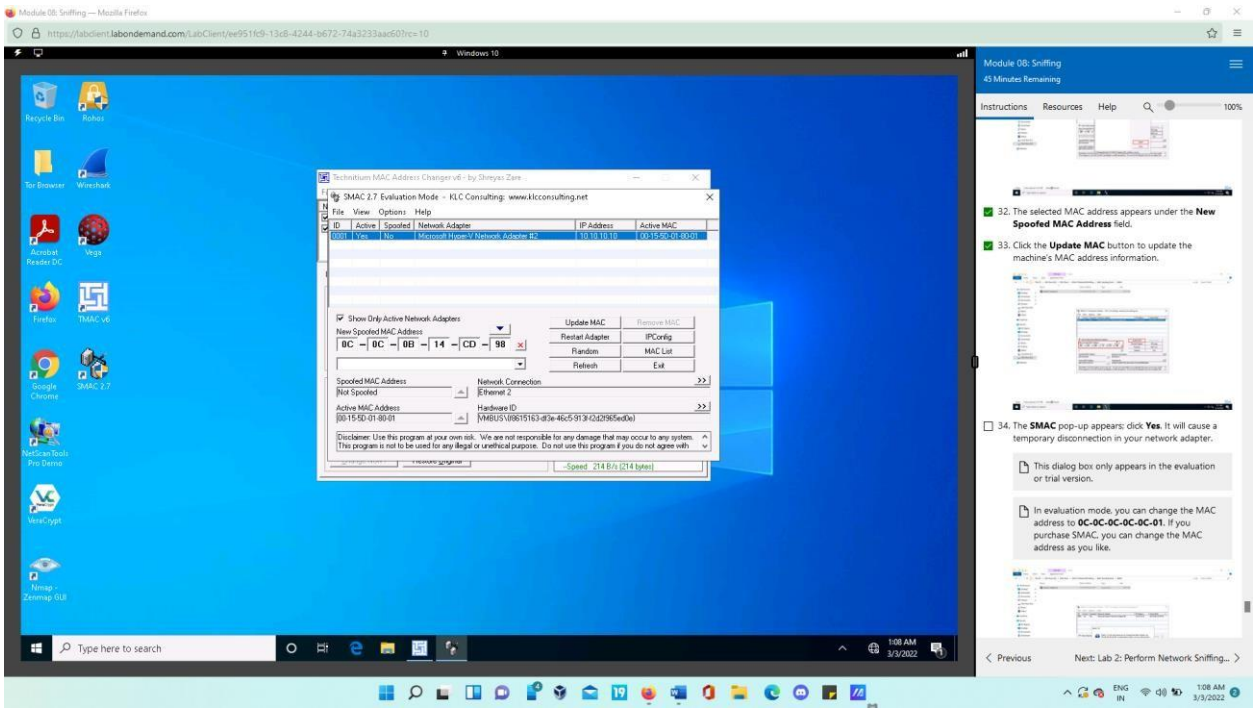
- Open the Sample_MAC_Address_List.txt file to import the MAC address list to SMAC by using load list feature.



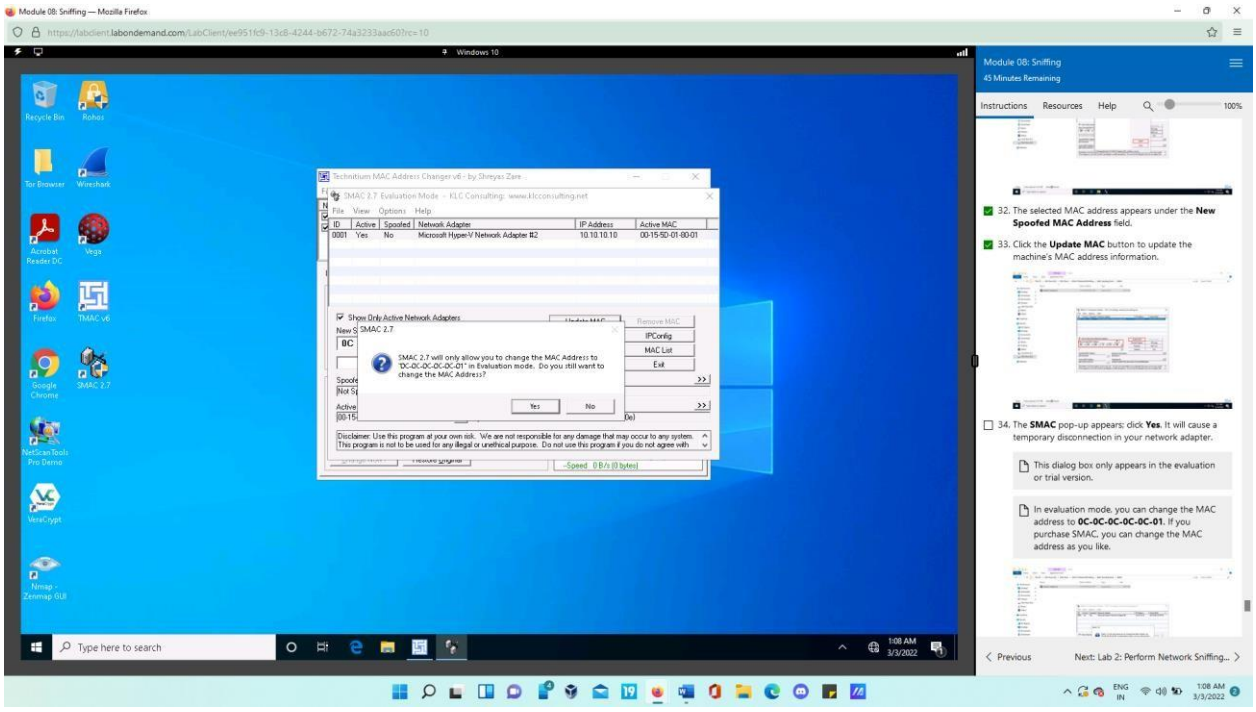
After adding the list, choose any random address and press select button. Under new spoofed MAC address field, the selected MAC address will appear.

- Now we will update the Machine's MAC address information by pressing update MAC button.

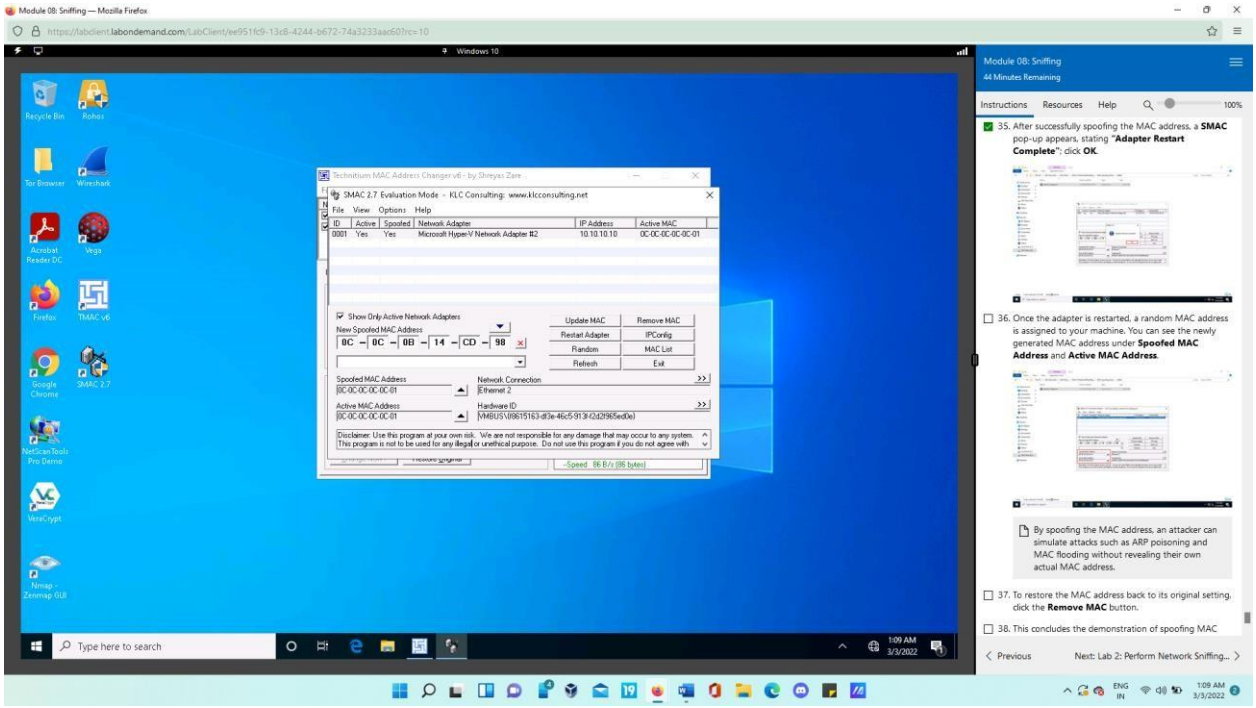
•



- Choose ‘yes’ in the dialog box. This will restart the network adapter.



- After it is finished, we have completed spoofing the machine's MAC address as we can see under the spoofed MAC address and Active MAC Address.

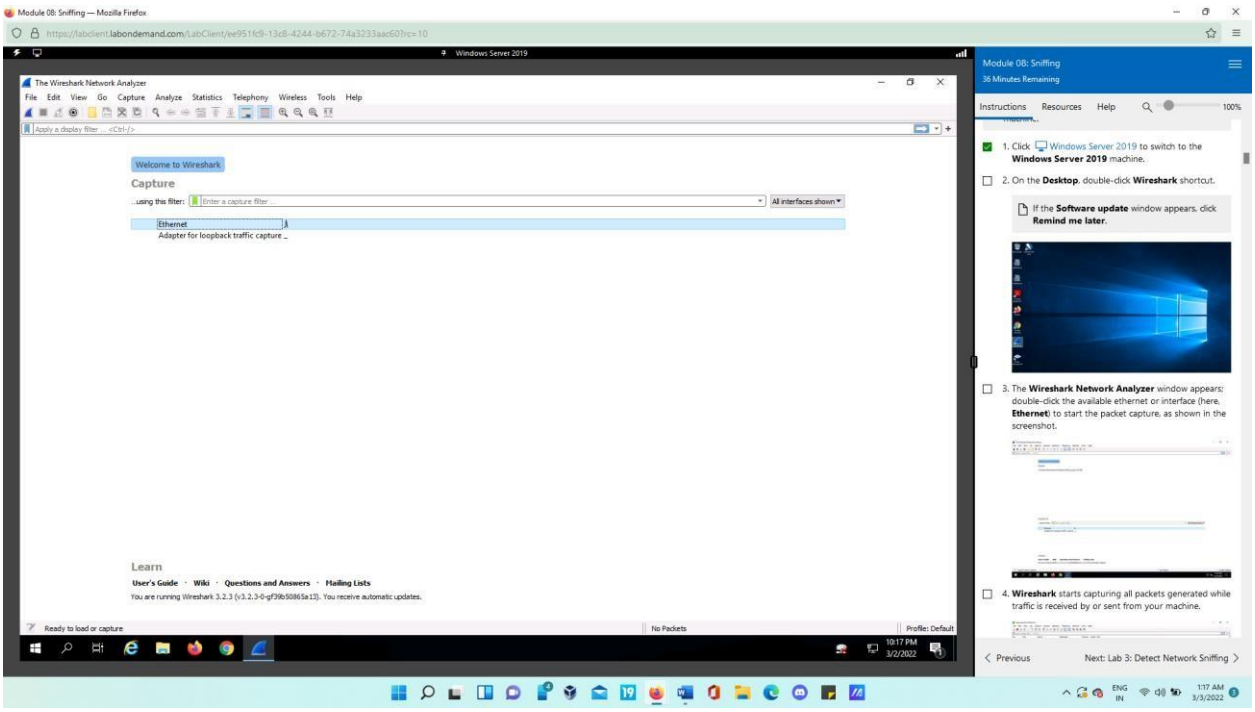


•

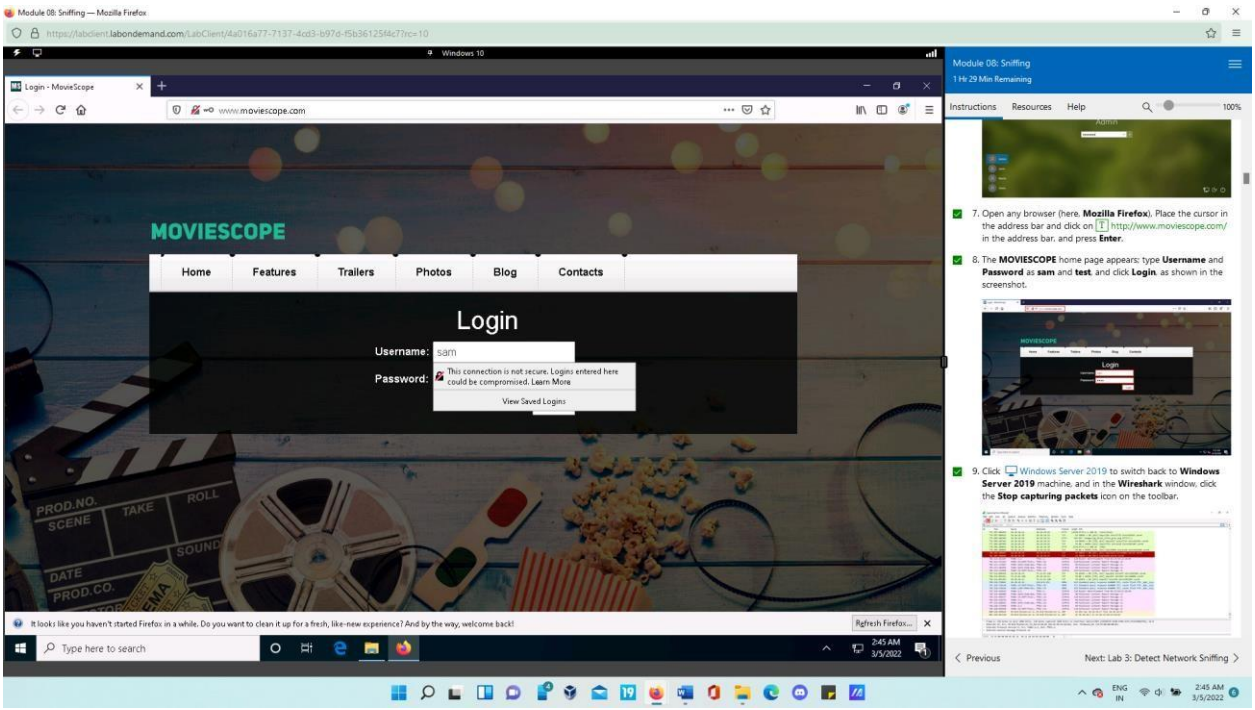
Lab 2: Perform Network Sniffing using Various Sniffing Tools

Task 1: Perform Password Sniffing using Wireshark

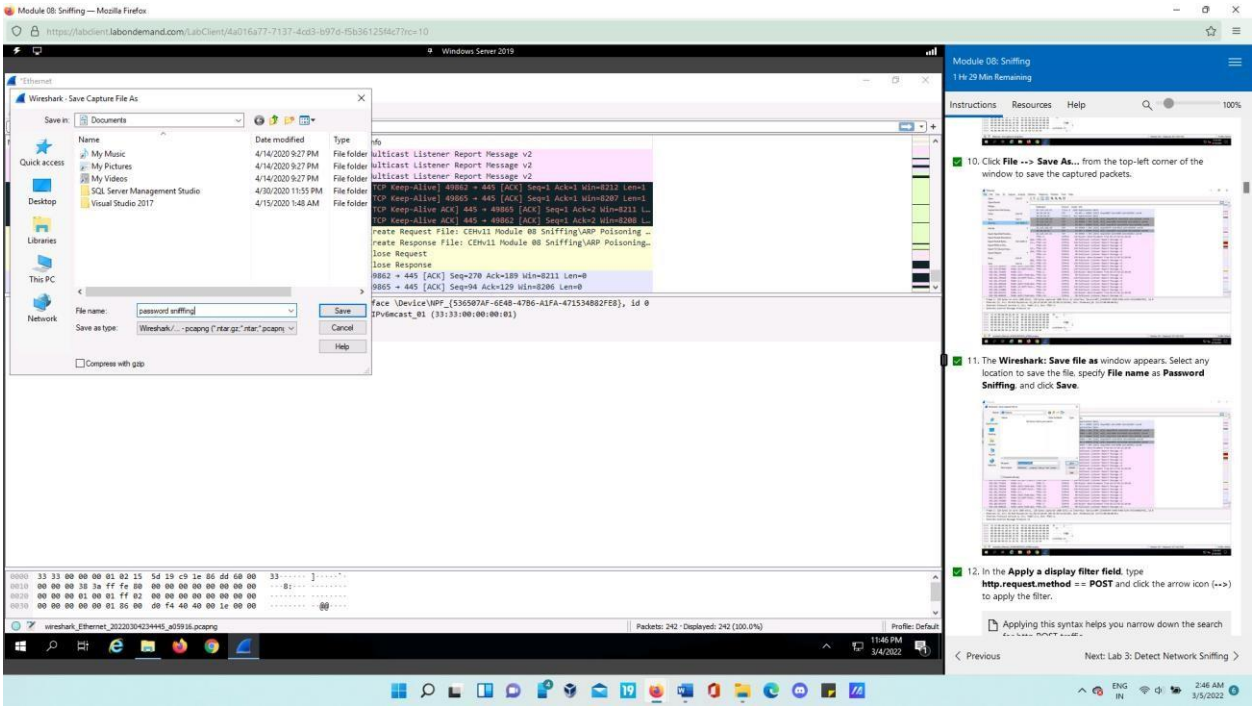
- In windows server 2019, open Wireshark from Desktop and select Ethernet. Wireshark will start packet capture.



- Now in Windows1) navigate to http://www.moviescope.com from the web browser. Login by using Sam and test as username and password respectively.

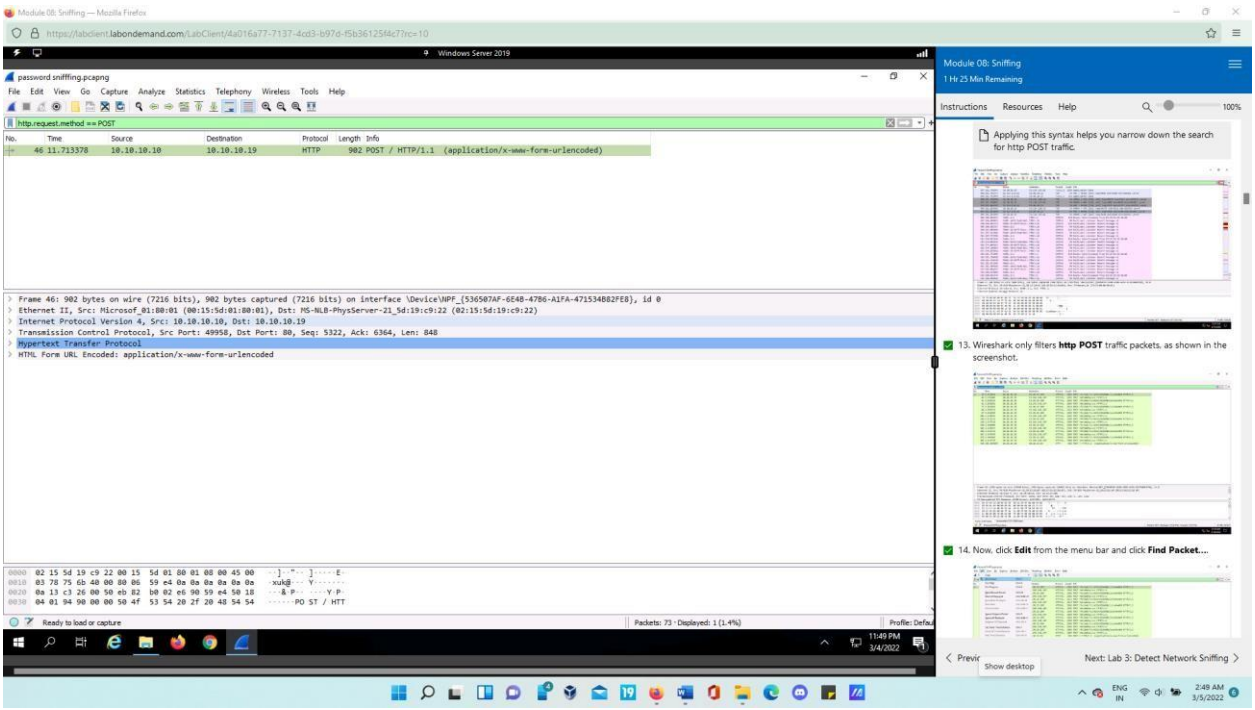


In windows server 2019, stop capturing packets in Wireshark and save the packet capture file at any location.



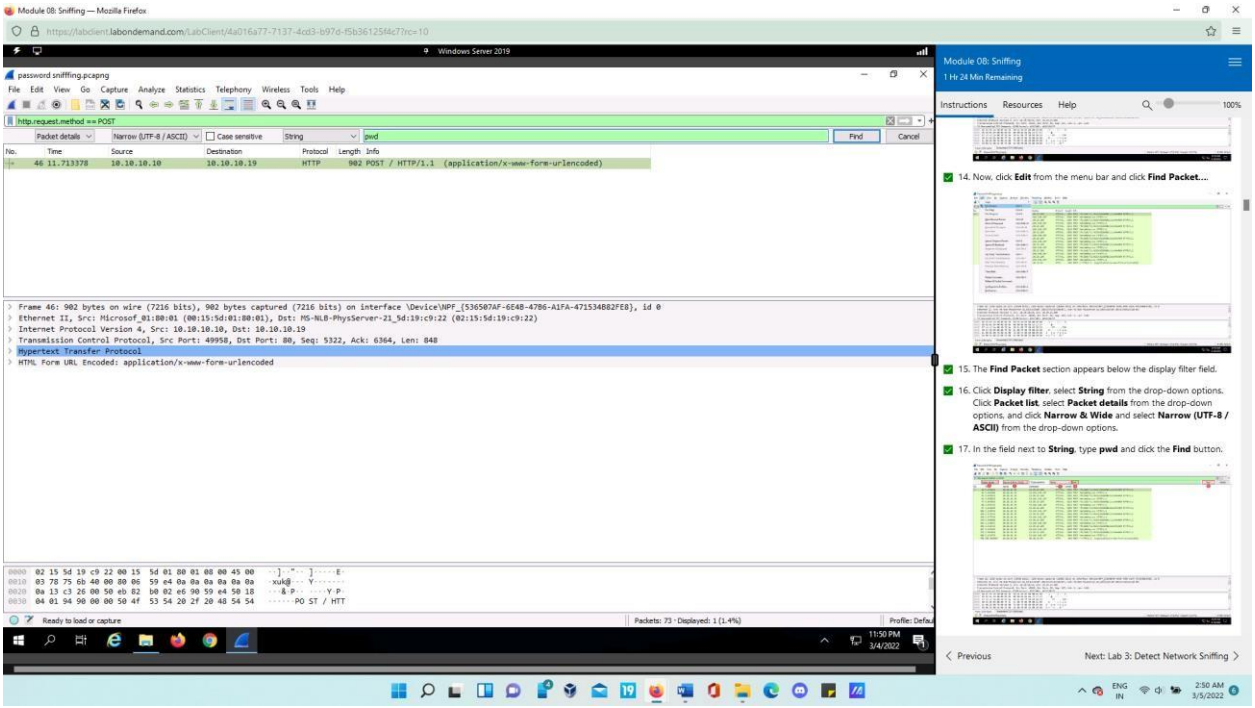
- Now filter the packet display for viewing only HTTP POST packets by using ‘http.request.method == POST’ filter.

•

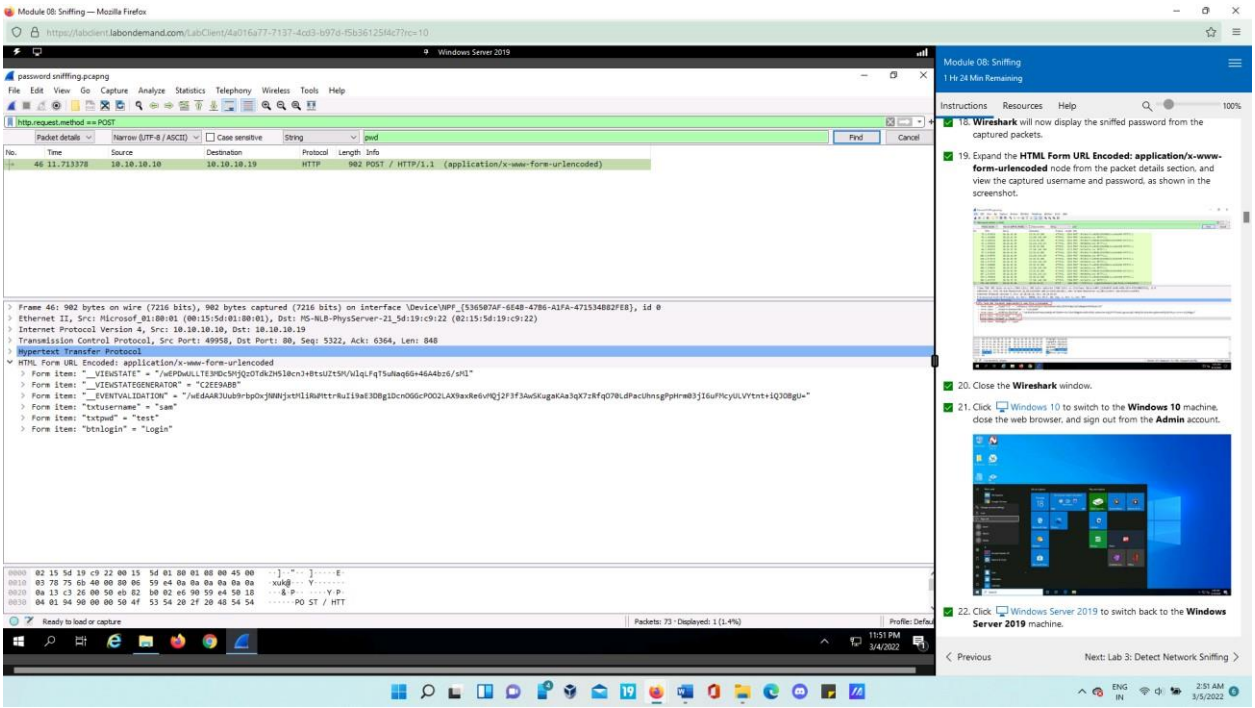

Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows Server 2019
password sniffing.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == POST
No. Time Source Destination Protocol Length Info
46 11.713378 10.10.10.10 10.10.10.19 HTTP 902 POST / HTTP/1.1 (application/x-www-form-urlencoded)
Frame 46: 902 bytes on wire (7216 bits), 902 bytes captured (7216 bits) on interface \Device\NPF_{536507AF-6E48-47B6-A1FA-471534B82FE8}, id 0
Ethernet II, Src: Microsof_01:80:01 (00:15:5d:01:80:01), Dst: MS-NLB-PhysServer-21_5d:19:c9:22 (02:15:5d:19:c9:22)
Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.10.10.19
Transmission Control Protocol, Src Port: 49958, Dst Port: 80, Seq: 5322, Ack: 6364, Len: 848
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Ready to load or capture
Packets: 73 · Displayed: 1 (1.4%)
11:49 PM 3/4/2022
Module 08: Sniffing
1 Hr 25 Min Remaining
Instructions Resources Help
100%
Applying this syntax helps you narrow down the search for http POST traffic.
13. Wireshark only filters http POST traffic packets, as shown in the screenshot.
14. Now, click Edit from the menu bar and click Find Packet...
Show desktop
Next: Lab 3: Detect Network Sniffing
ENG IN
2:49 AM 3/5/2022

•

Then press edit > find packet > display filter > string > packet list > packet details > narrow & wide > narrow (UTF-8 / ASCII). In the field next to string, type in pwd and click find.

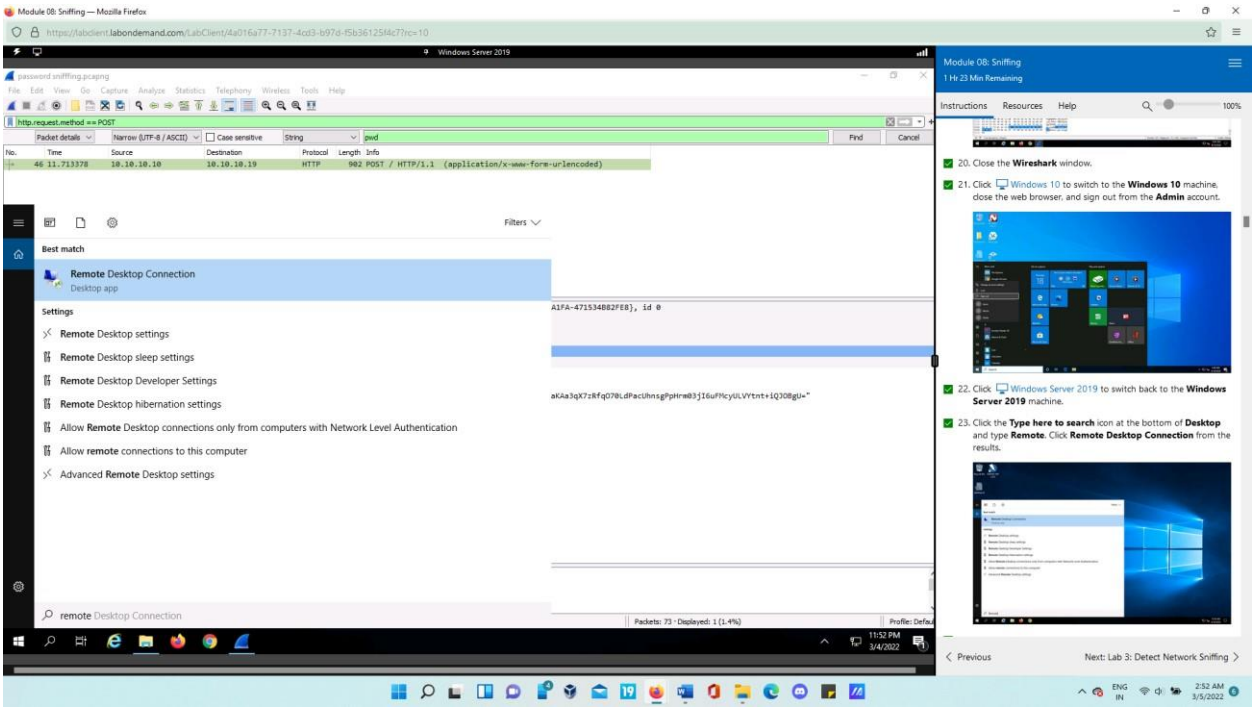


- The sniffed password from the captured packets will be displayed in wireshark.
- In the packet information section, expand the HTML Form URL Encoded: application/x-www-formurlencoded node to see the captured login and password.

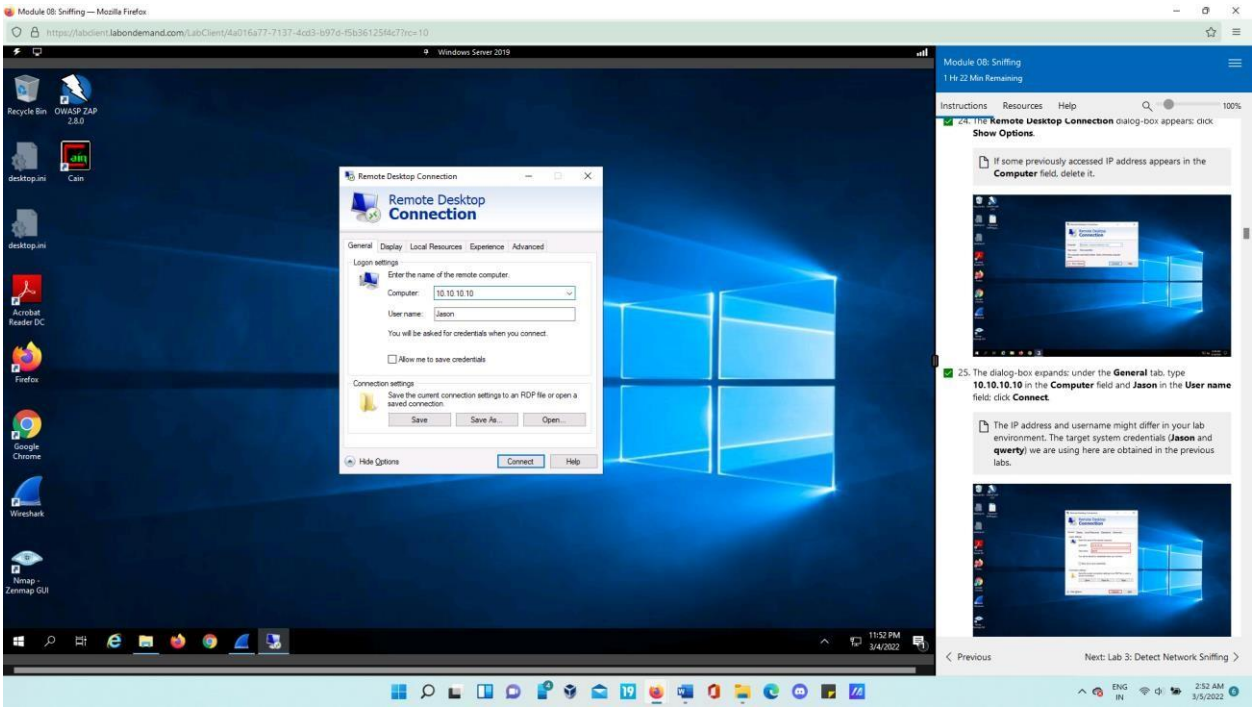


-

Open remote desktop connection application in Windows server 2019.

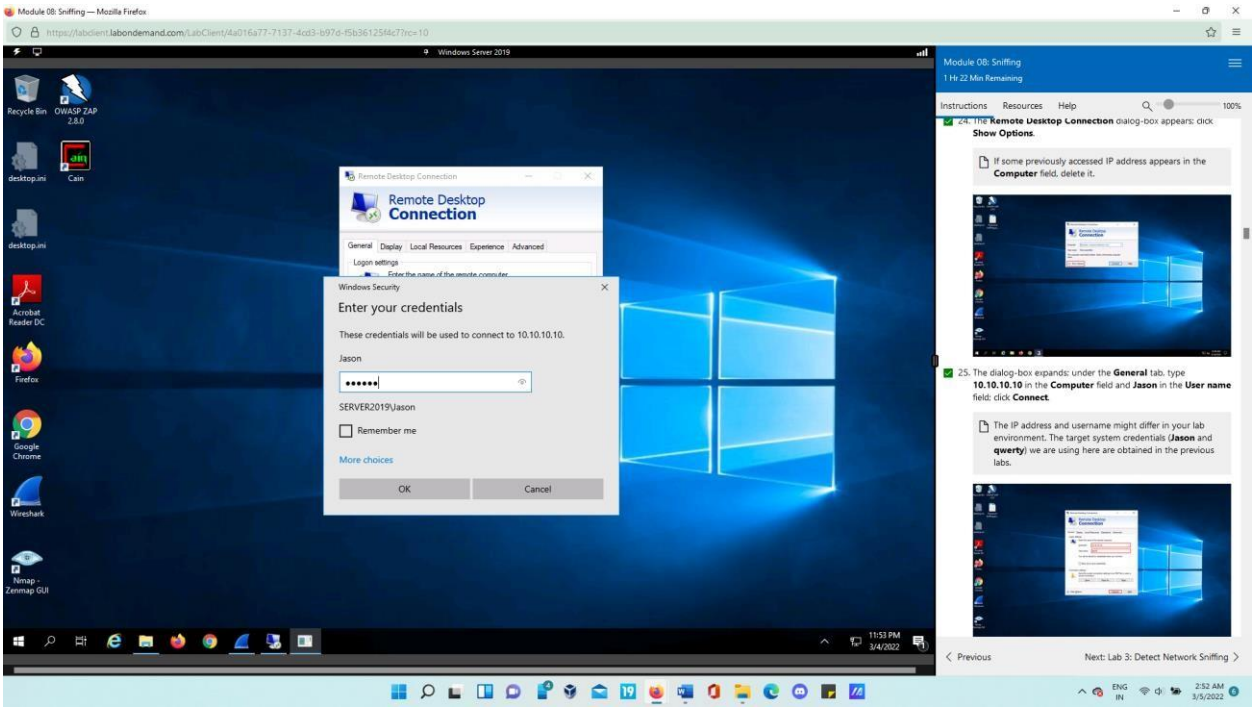


- The **Remote Desktop Connection** dialog-box appears; click **Show Options**
- The dialogue box expands; in the computer field, type 10.10.10.10, and in the Username field, type Jason; click Connect.



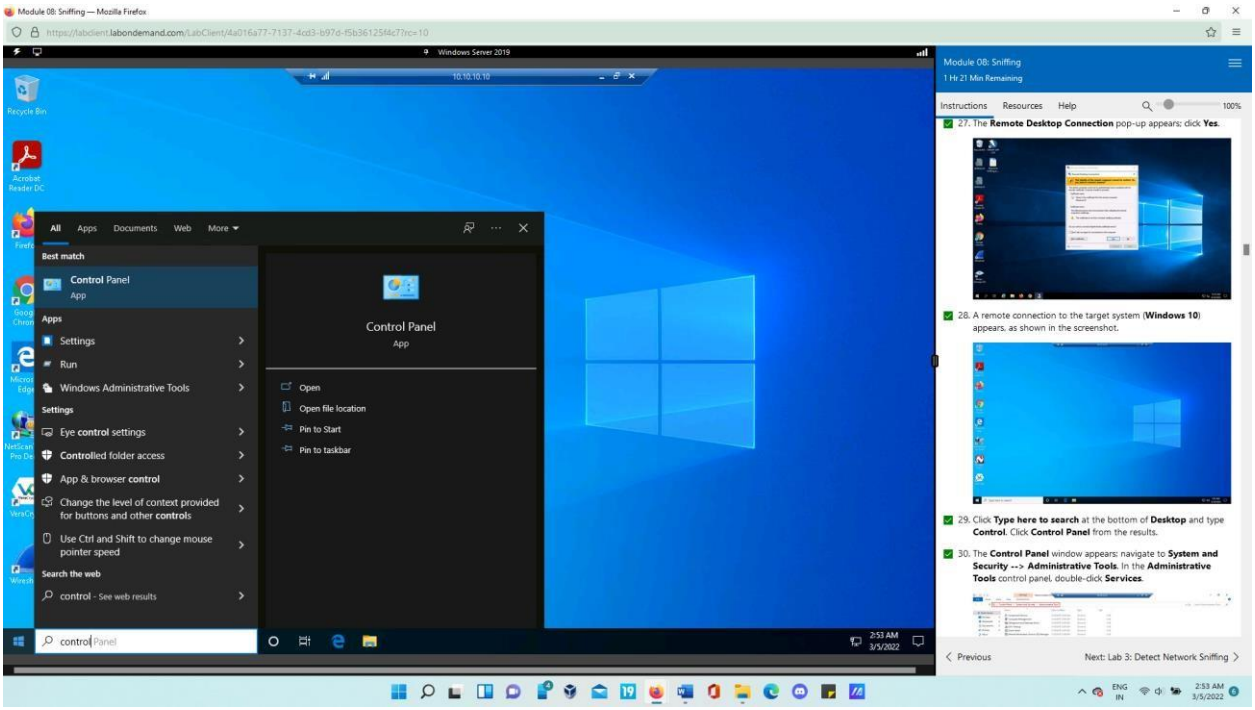
•

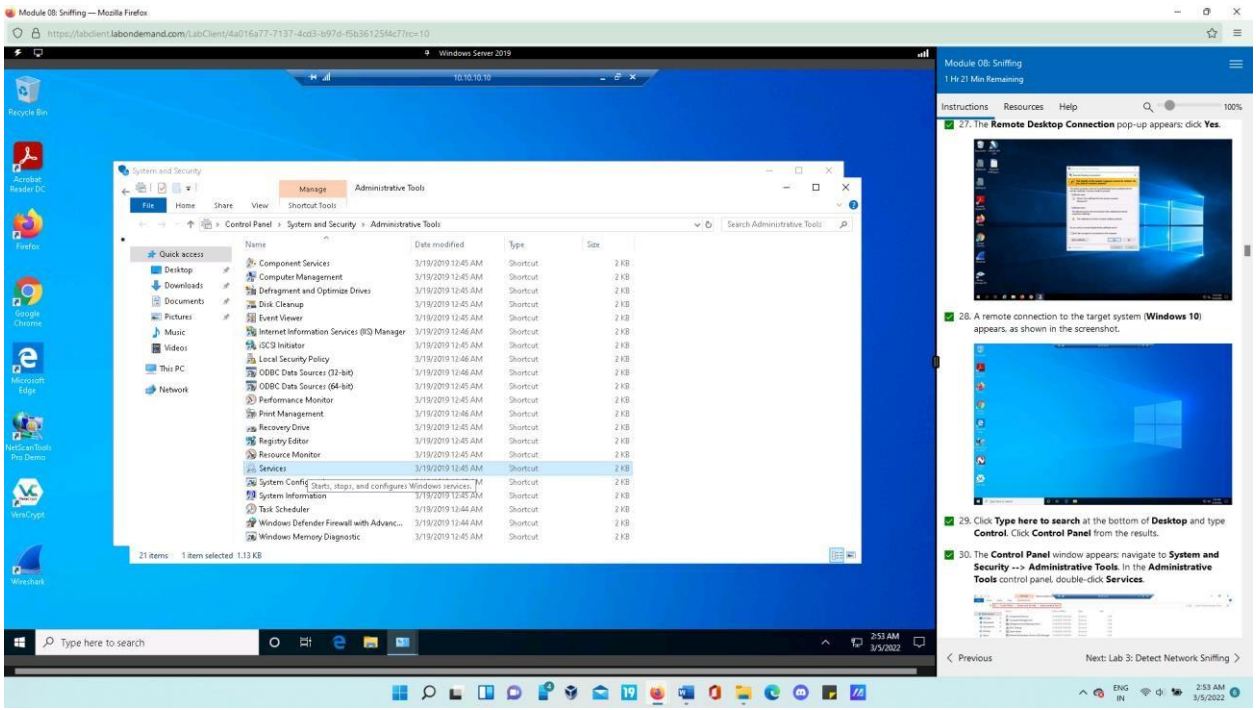
Here type in password as ‘qwerty’ and click ok.



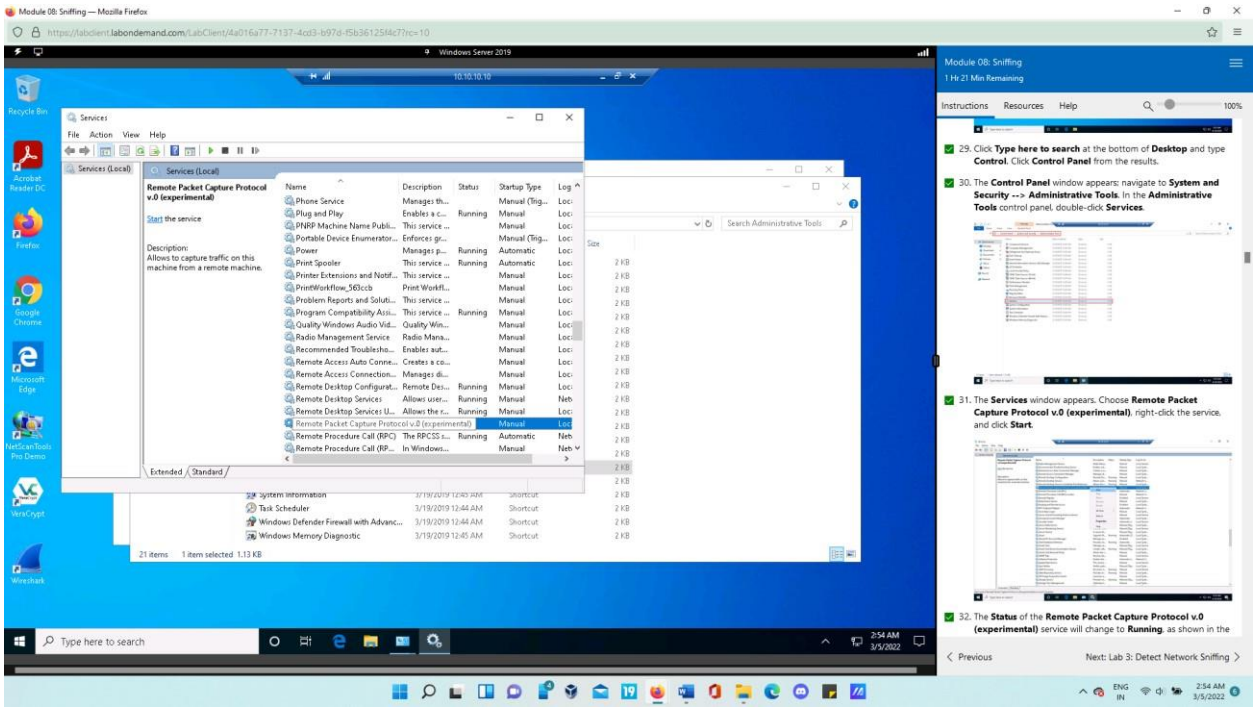
- The **Remote Desktop Connection** pop-up appears; click **Yes**.

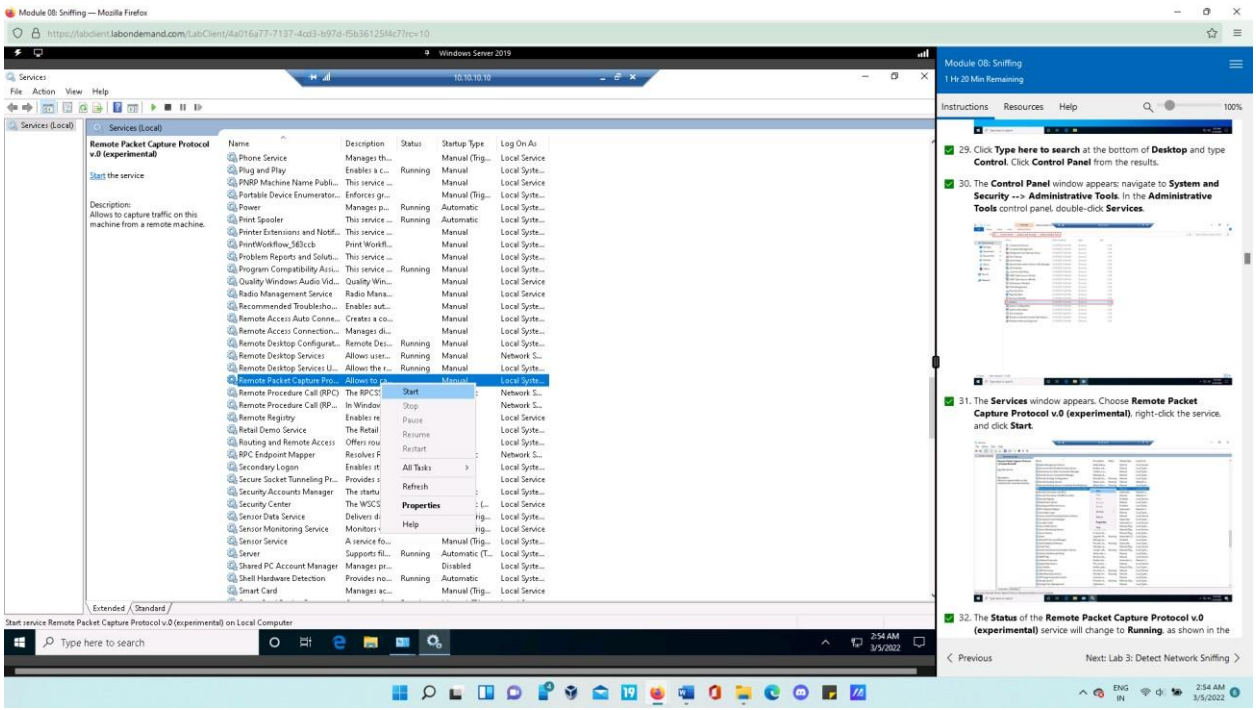
- Then navigate to Control Panel > System and security > Administrative tools > services



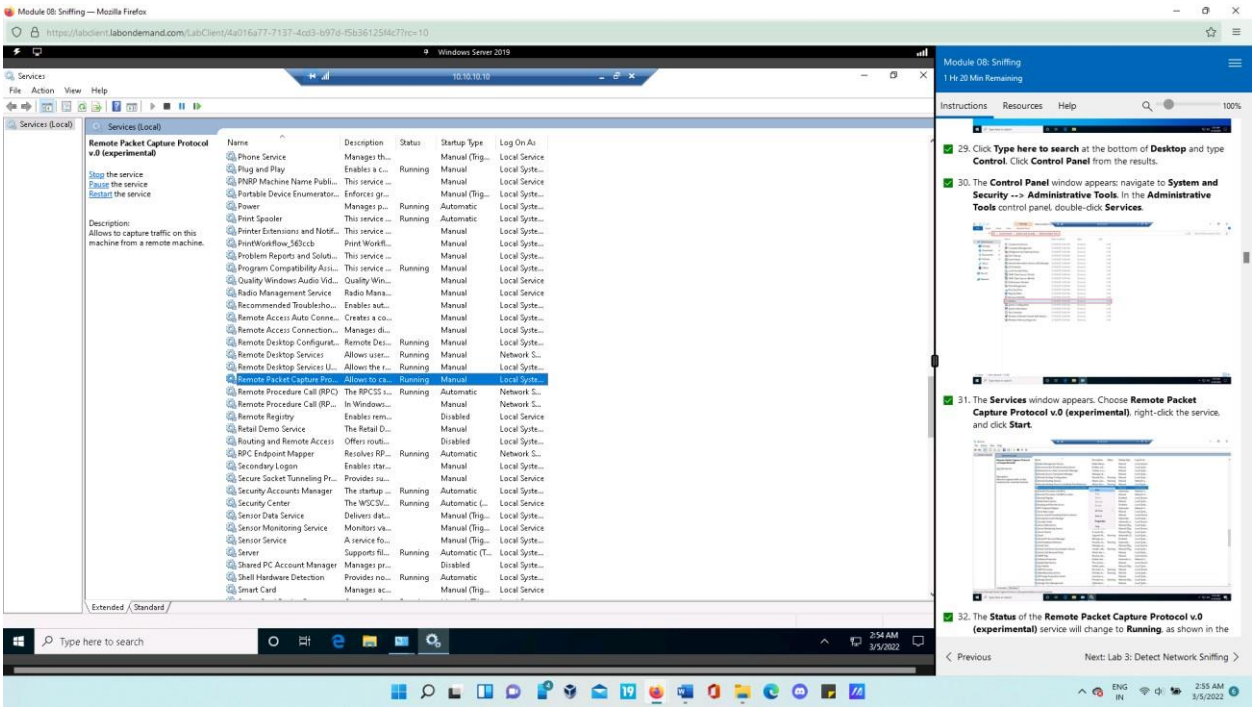


- The Services window is displayed. Select Remote Packet Capture Protocol v.0 (experimental) and double click services option to start it.



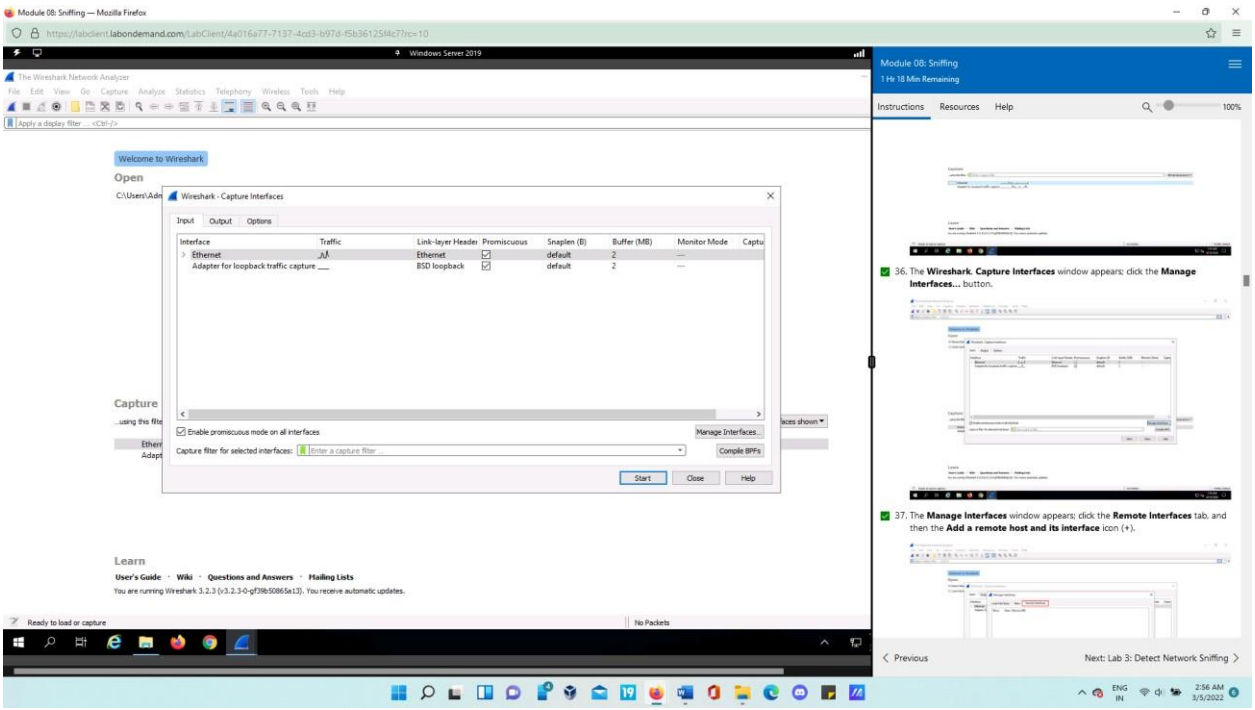


- The Remote Packet Capture Protocol v.0 (experimental) service's status will be updated to Running.

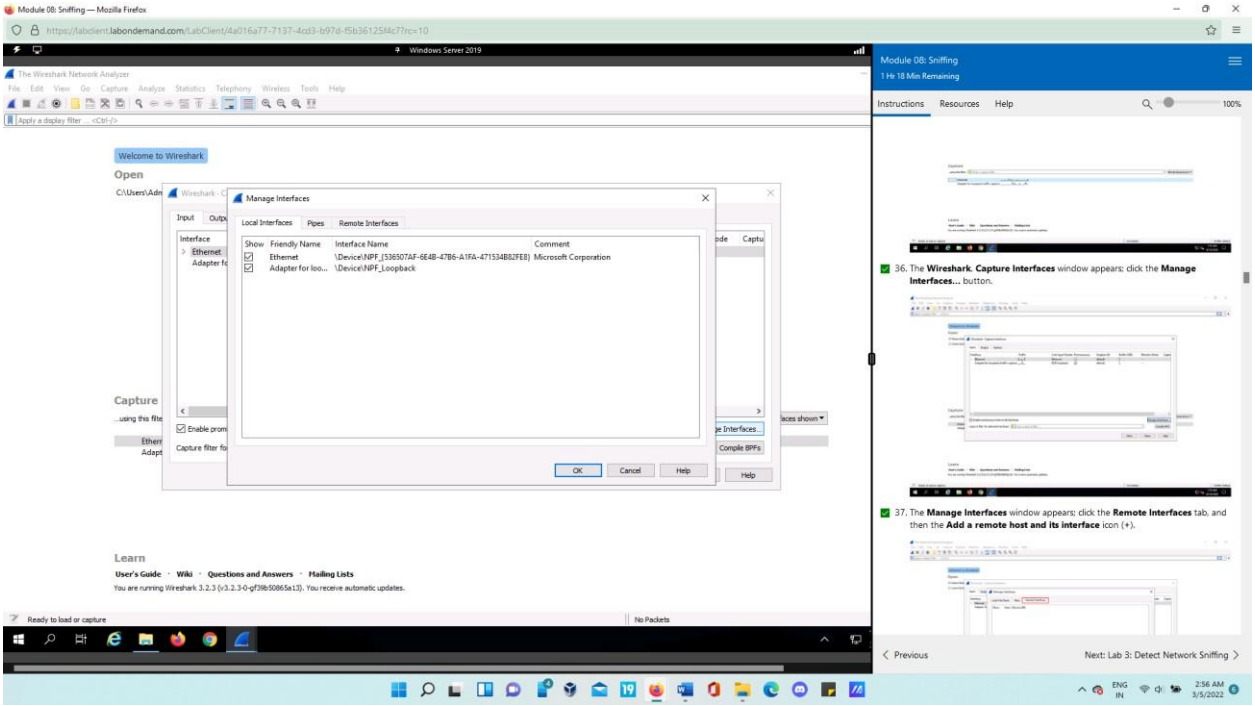


•

Close all open windows in Windows10 machine and now launch Wireshark from desktop. The Wireshark Network Analyzer window displays; from the toolbar, select Capture options.

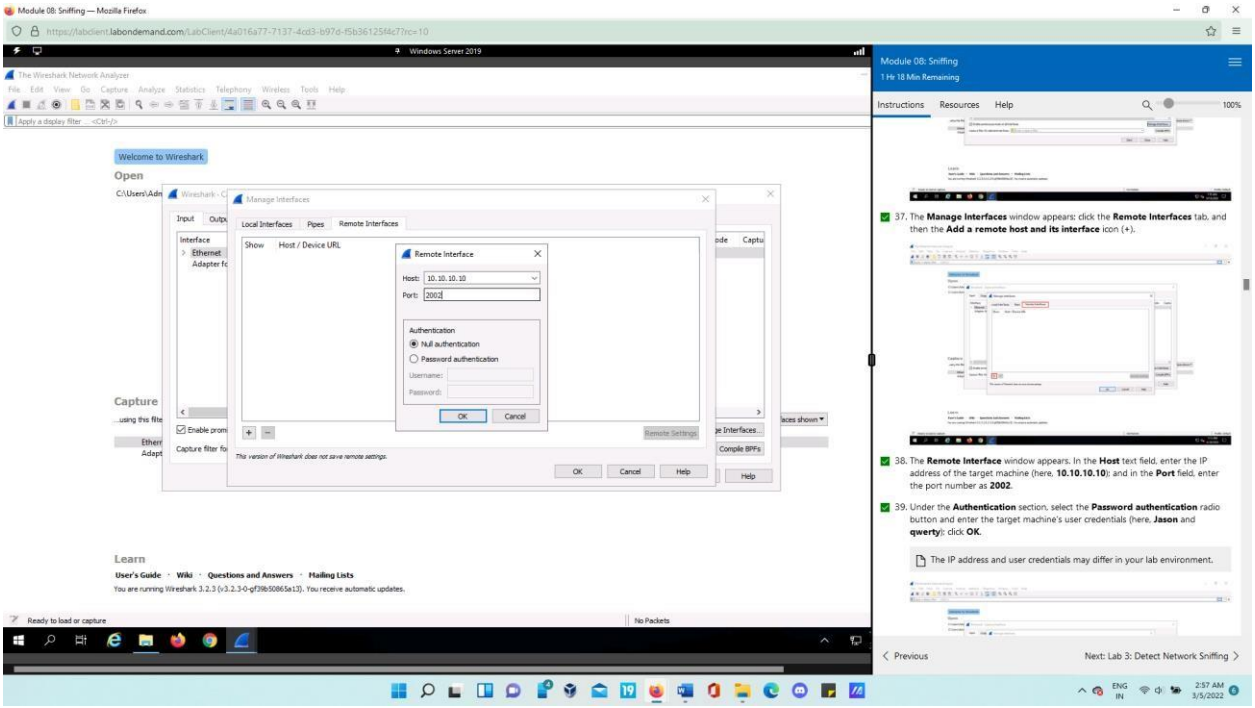


- Choose manages interfaces option from Wireshark capture interfaces window.

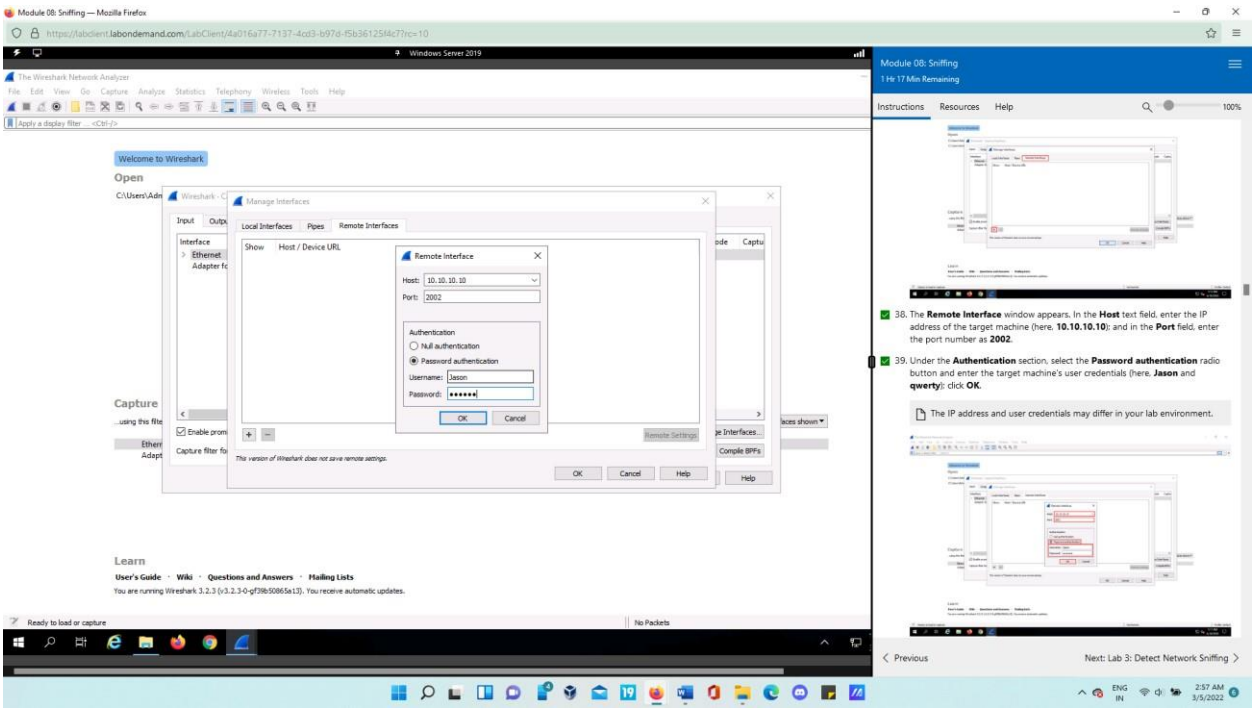


•

Now click remote interfaces > add remote host and its interface. Then in remote interface window, type 10.10.10.10 in host field and 2002 in port field.

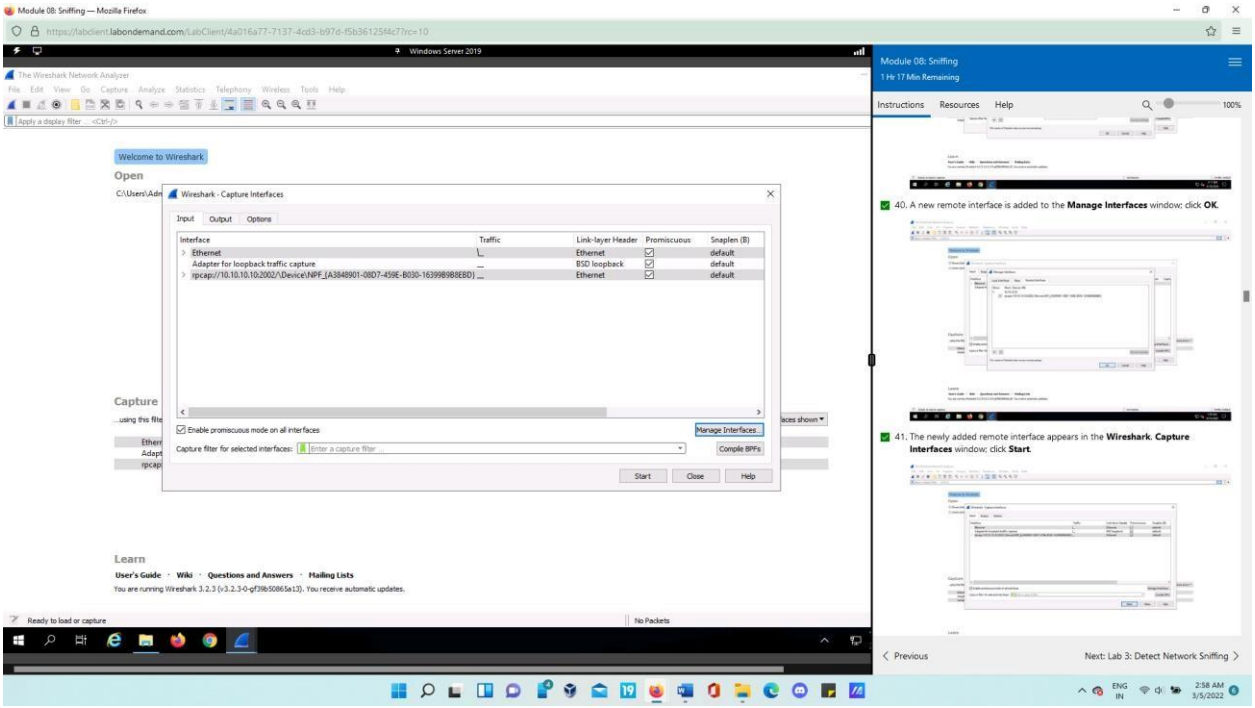


• Now use Jason and qwerty as username and password respectively for password authentication. After press ok.



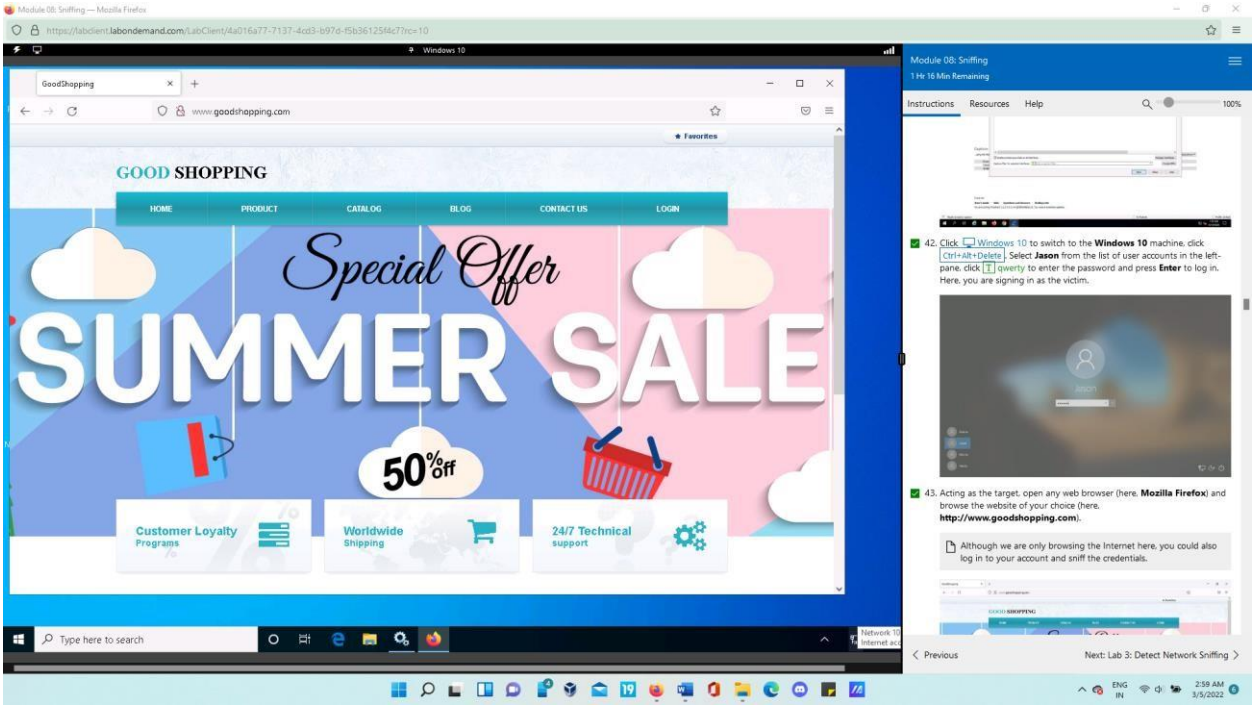
-

In manage interfaces, a new remote interface is added. Now choose newly added remote interface and press start.

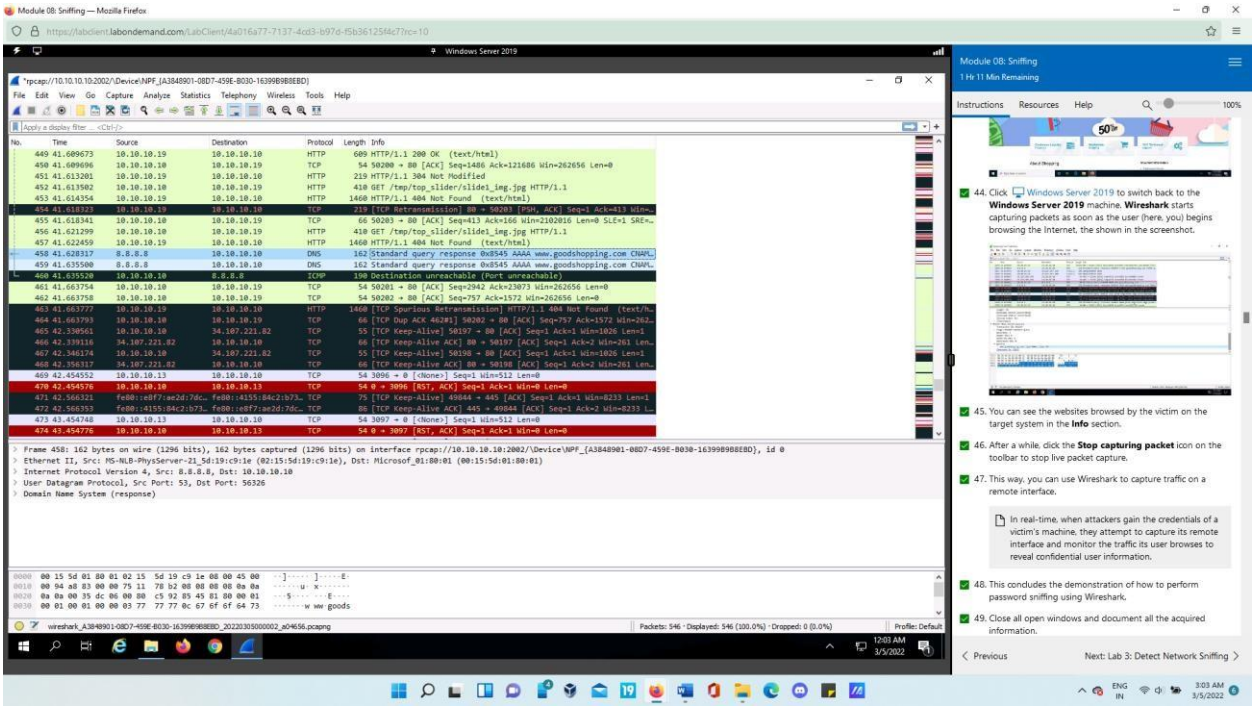


- Then, switch back to Windows10, login to Jason account. Here, we are logging in as victim.

- Then upon acting as a target, navigate to any website from the web browser, here we will navigate to www.goodshopping.com



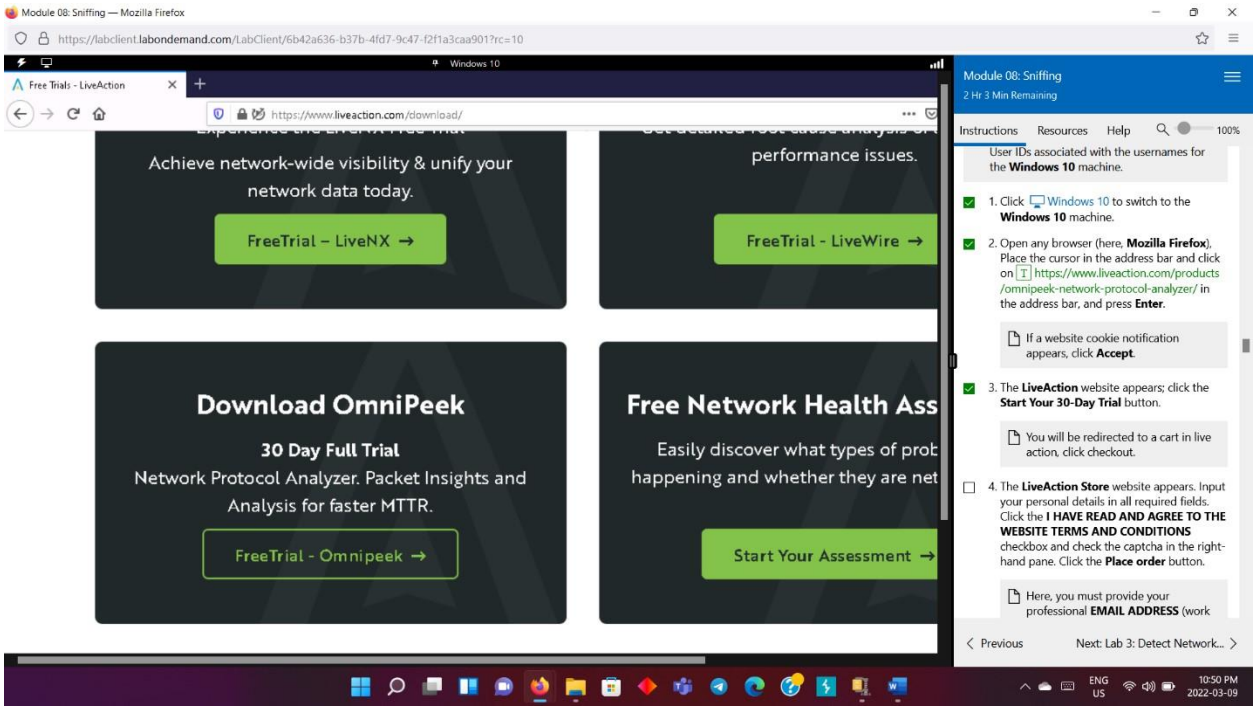
Now open Wireshark in Windows server 2019, you can see Wireshark starts capturing packets as the user begins browsing the web. In the Info area, you can see which websites the victim visited on the target system.

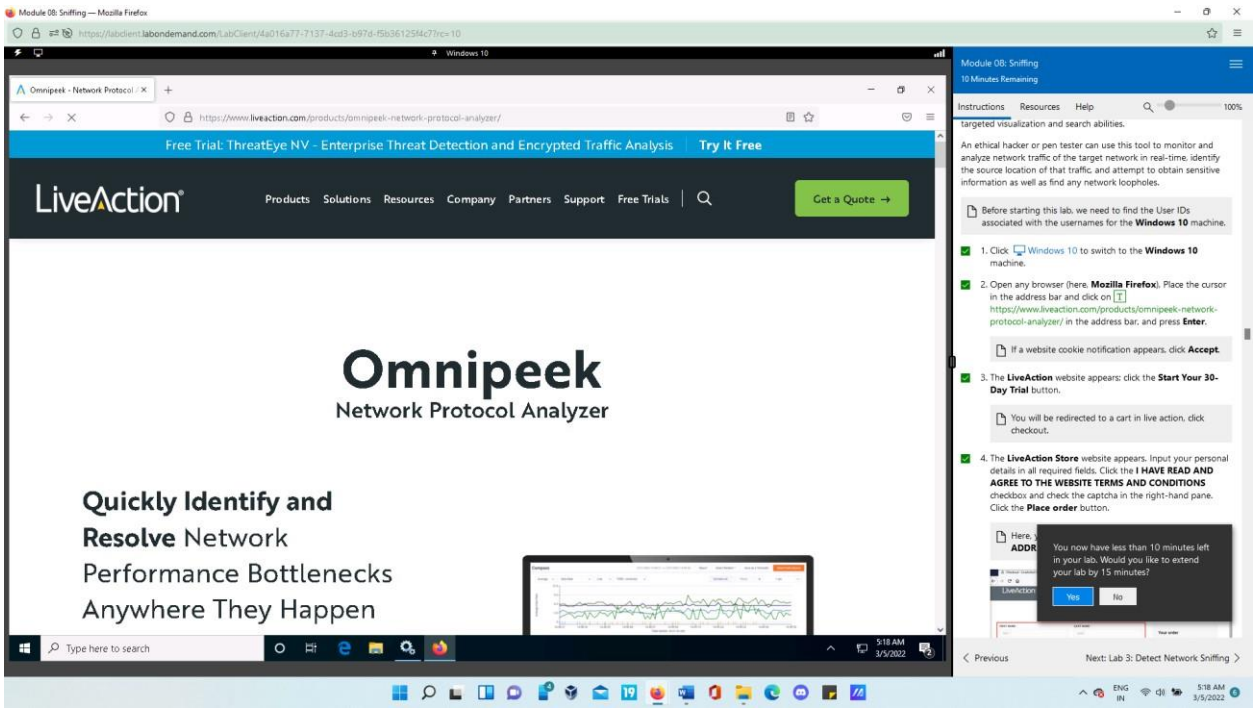


•

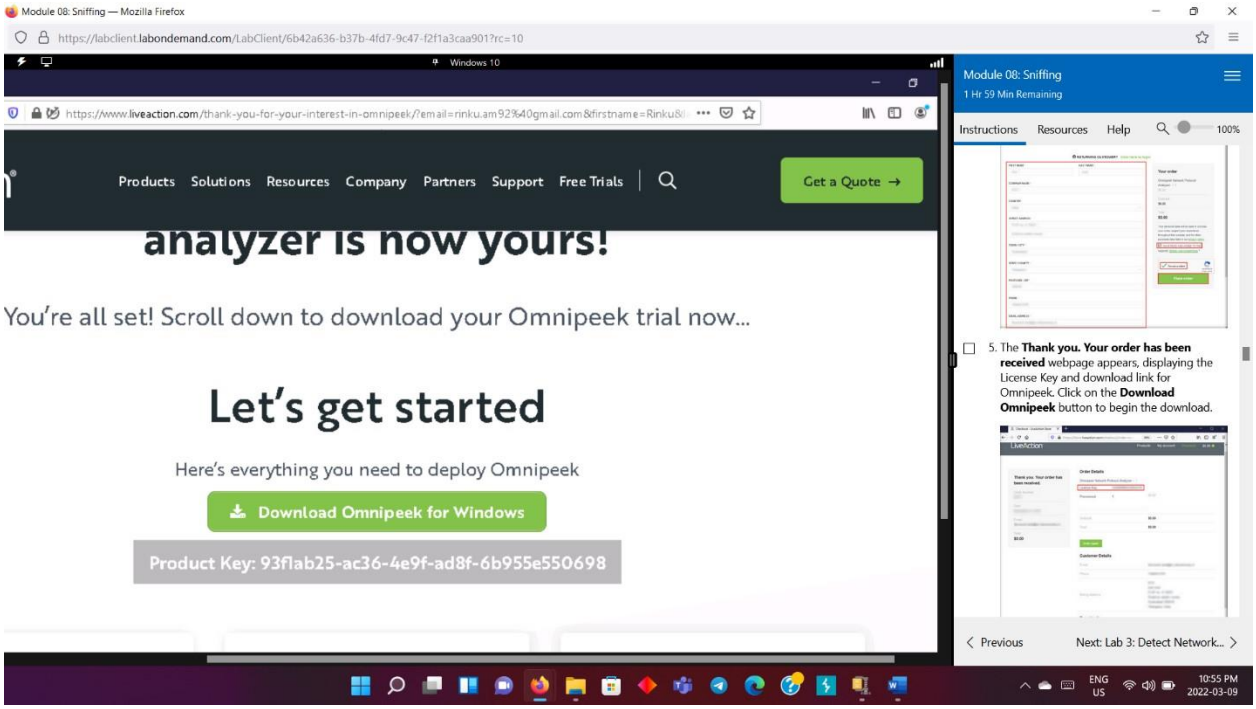
Task 2: Analyze a Network using the Omnipeek Network Protocol Analyzer

- Launch windows 10 OS and open a browser and paste the link : https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/ and click on enter.

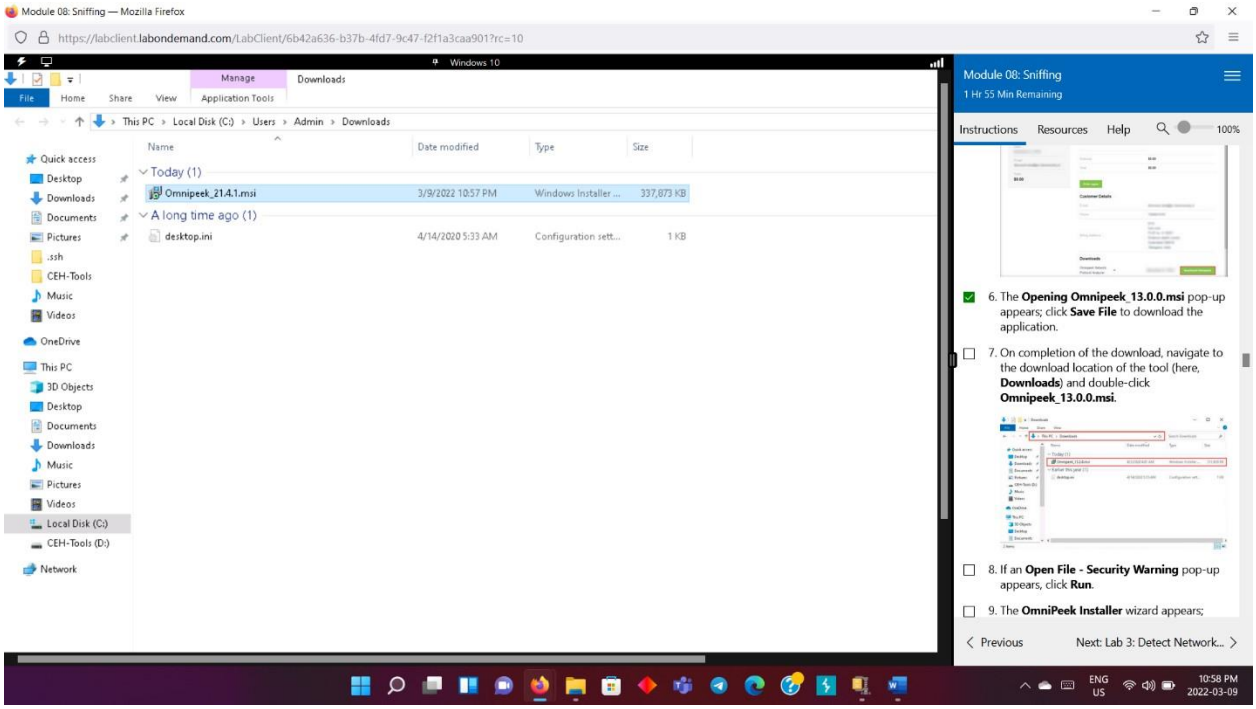


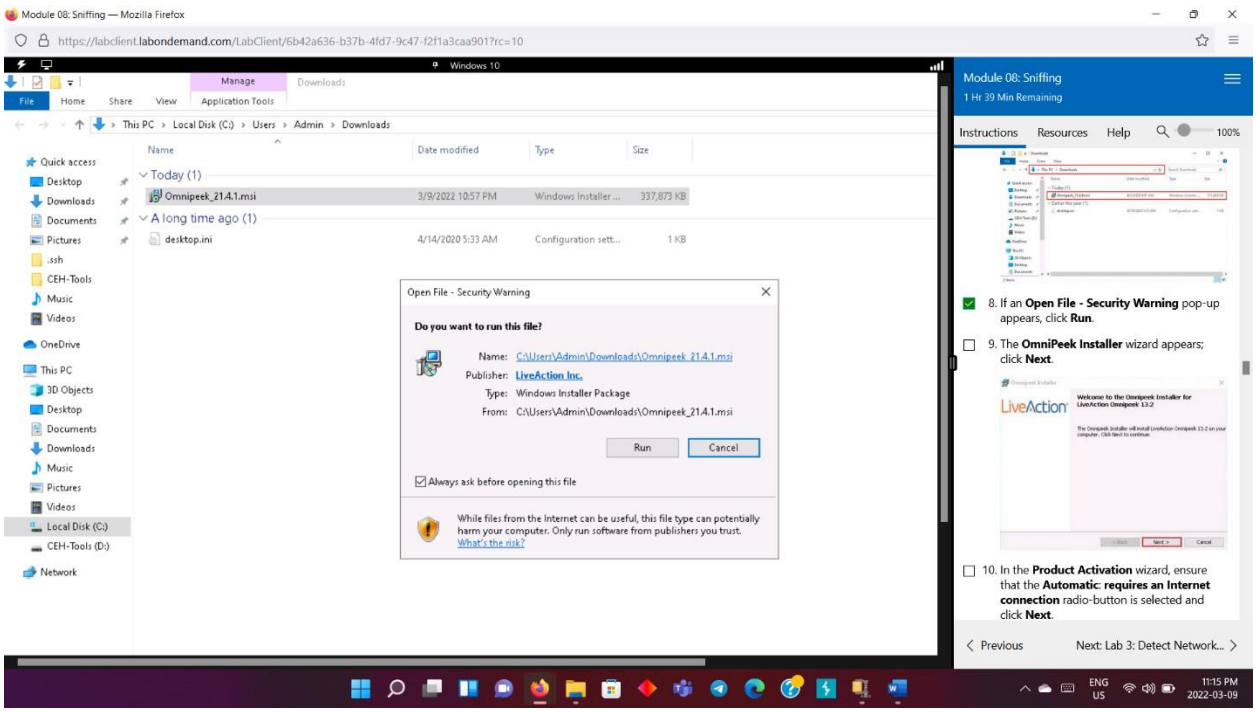


- Once the website is up, click on the trial button. Fill in the details and click on place order. Download the Omnipeek button and start the download.

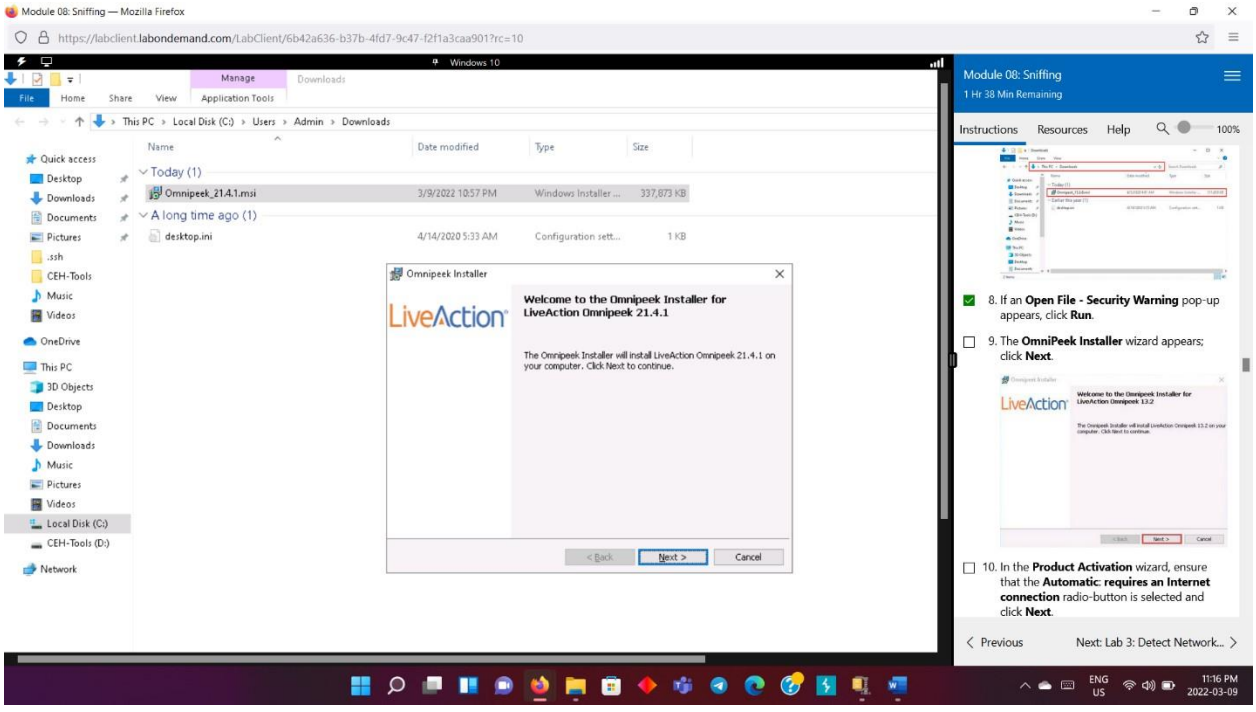


- Double click on the downloaded file to start the installation.

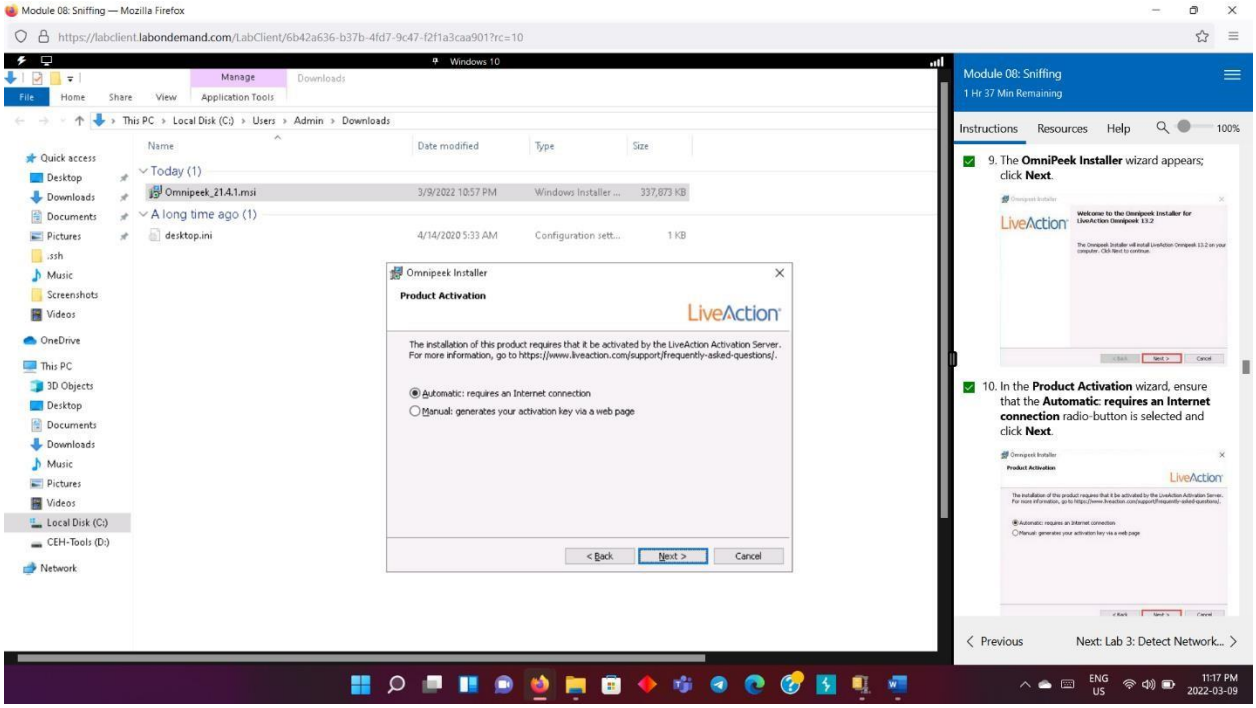




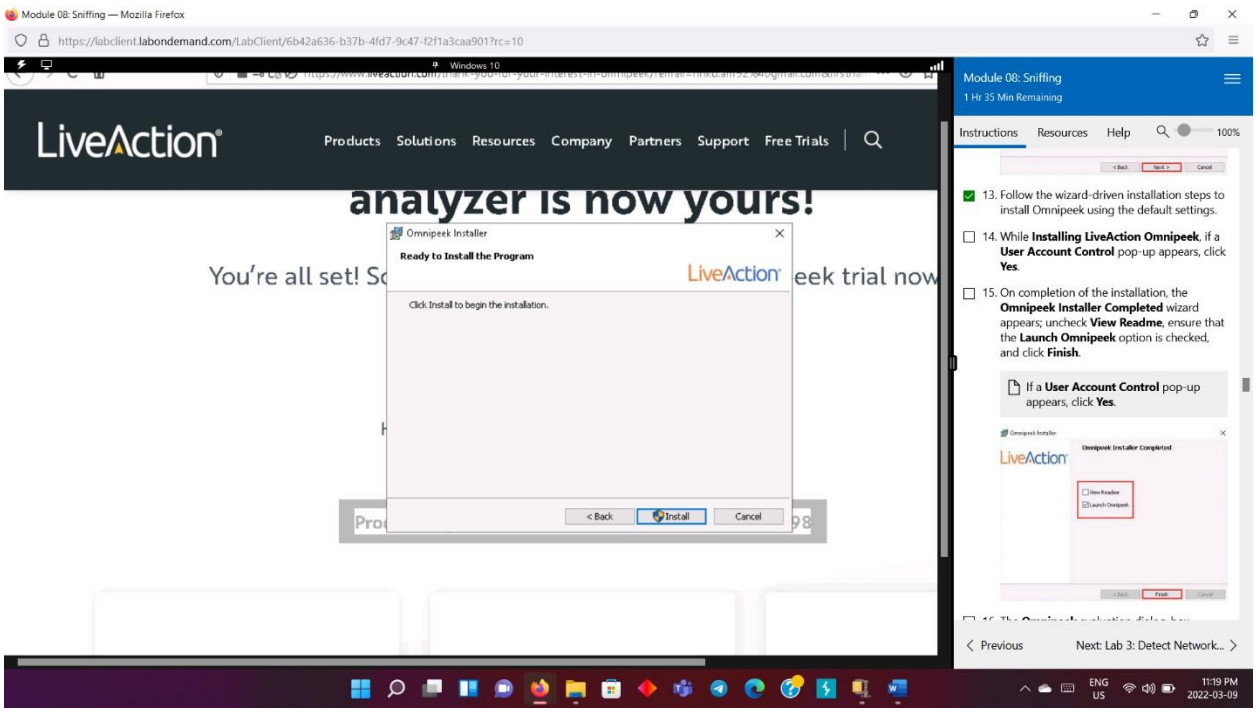
- Click on next and proceed.



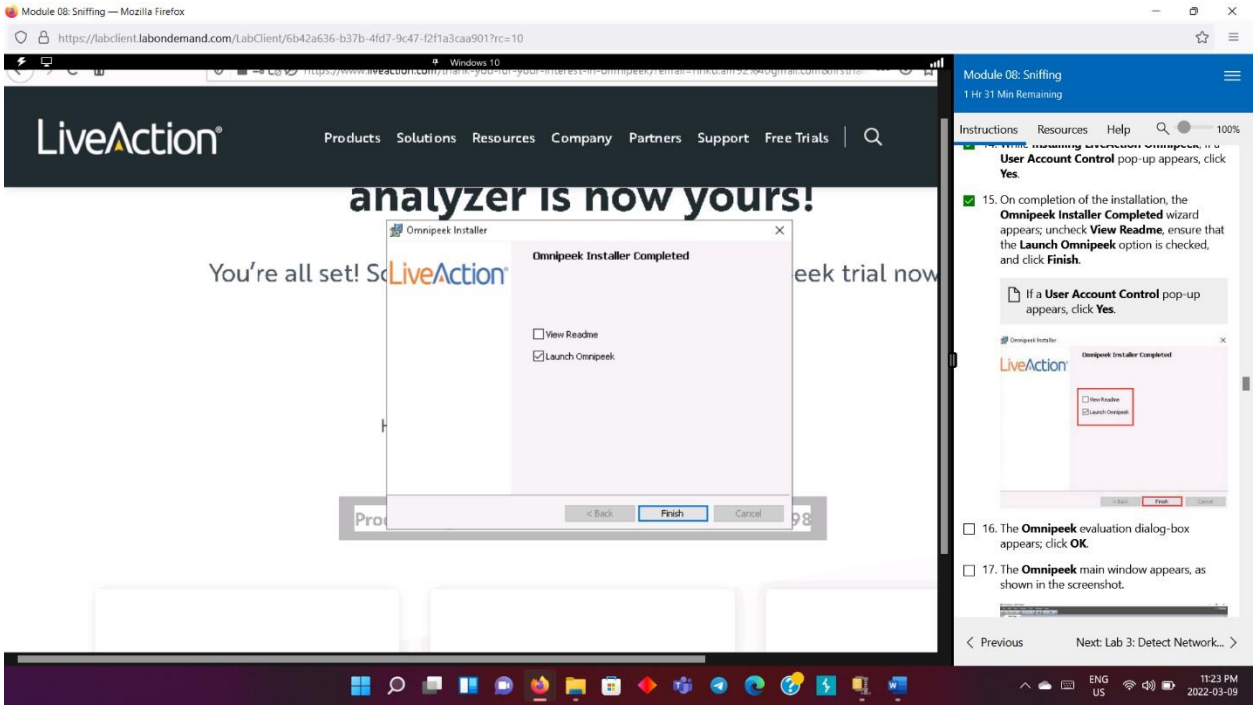
- Select the radio button and click next.



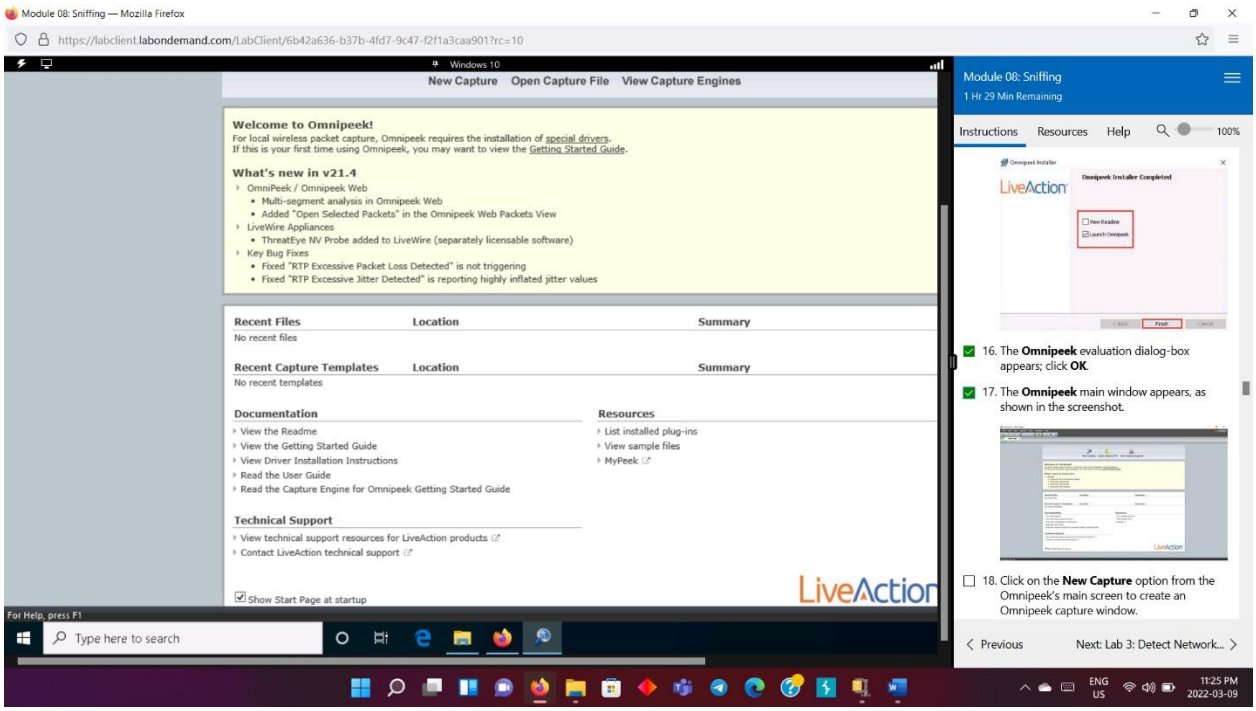
- Copy - paste the license key and click next.



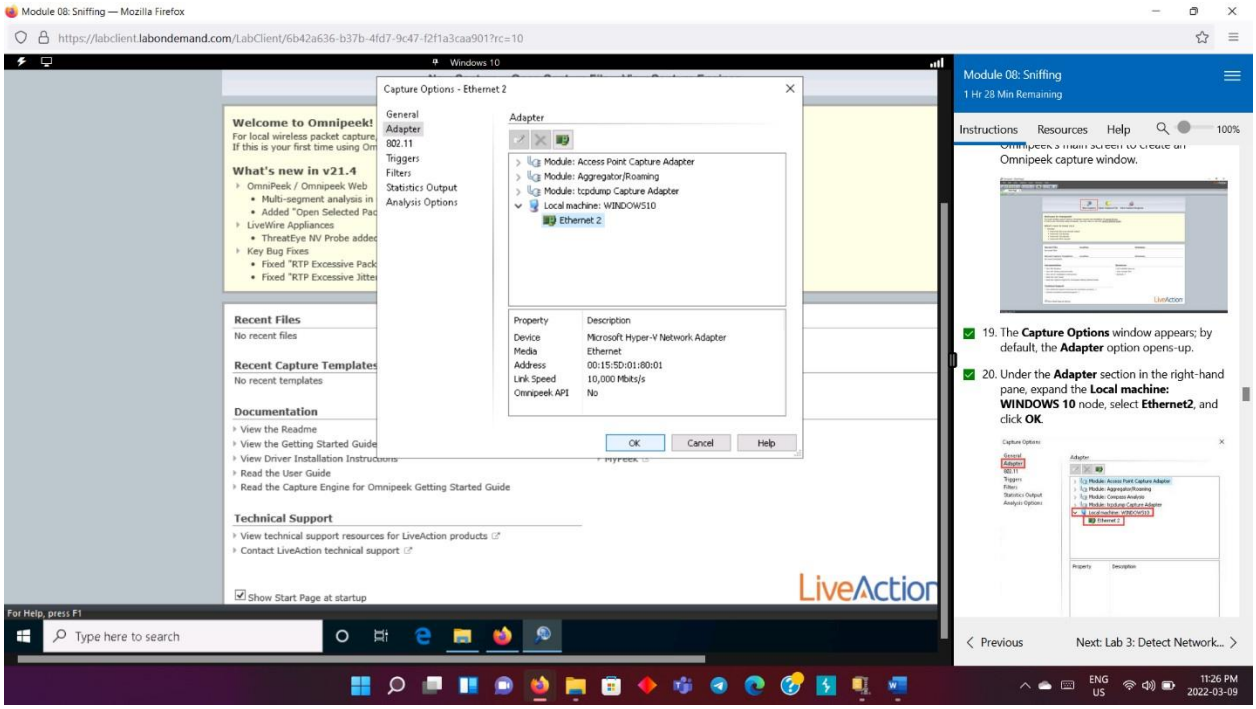
- Once the installation is complete, select the option launch Omnipeek and click on finish button.



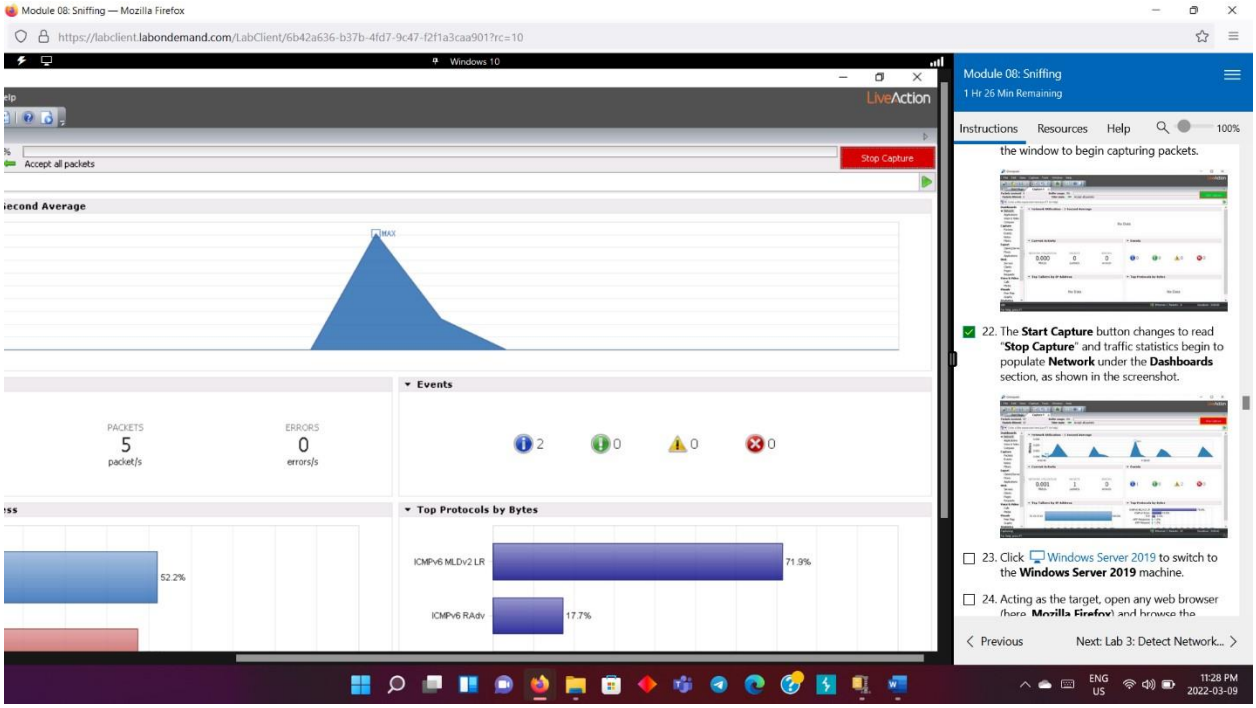
- The Omnipeek window appears.



- Now click on the button new capture from the main screen to create a new omnipeek capture window.
- The adapter option opens. Below the adapter option, expand the local machine: windows 10 node. Then select ethernet 2 and select Ok.

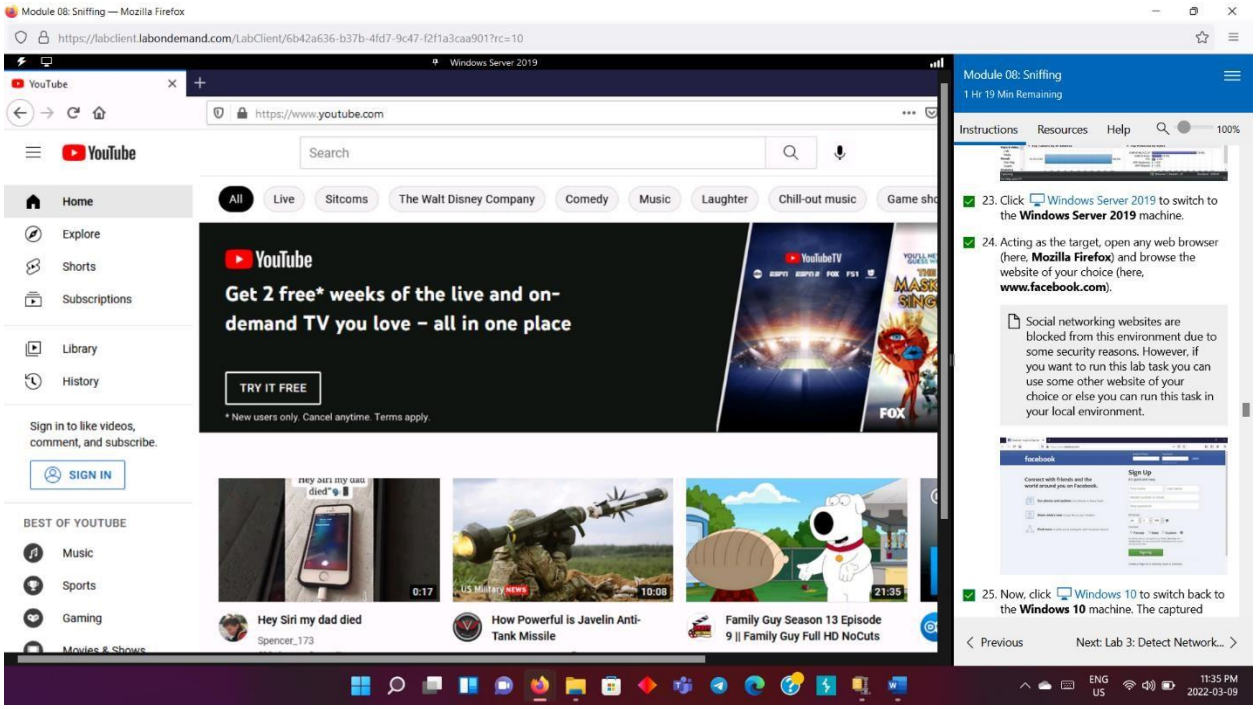


- The capture 1-tab pops up. Now click on the start capture button to start capturing packets.

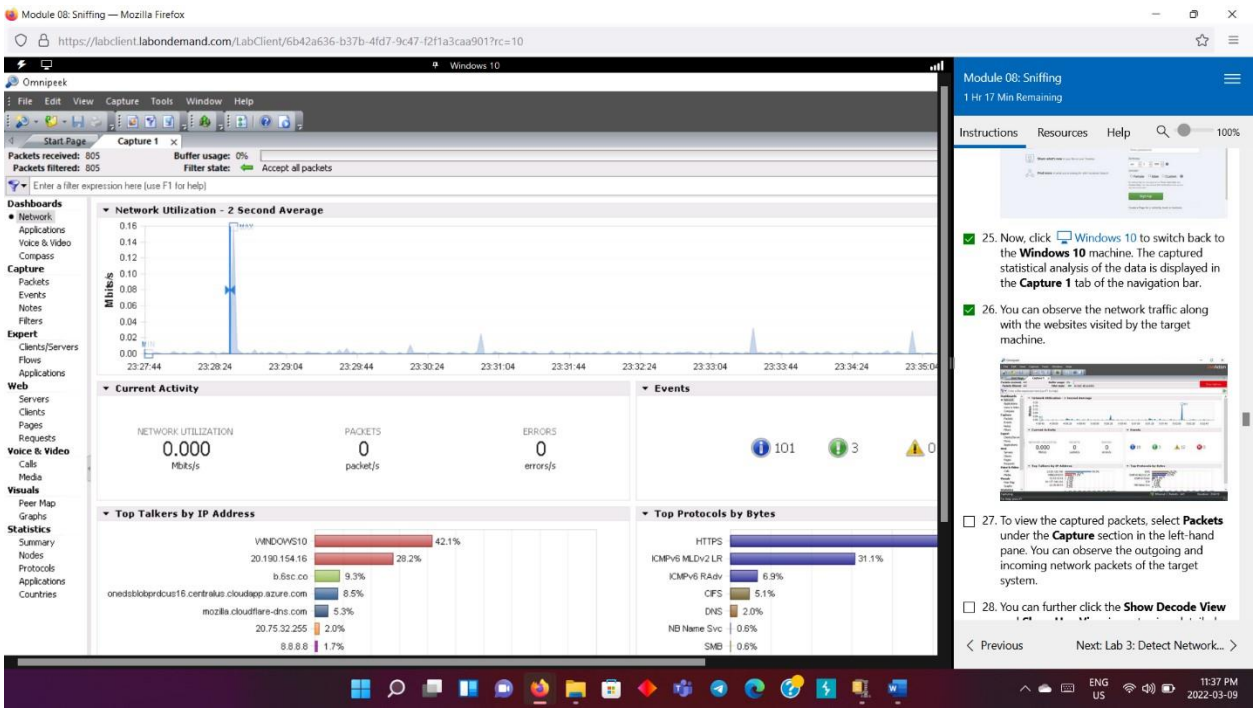


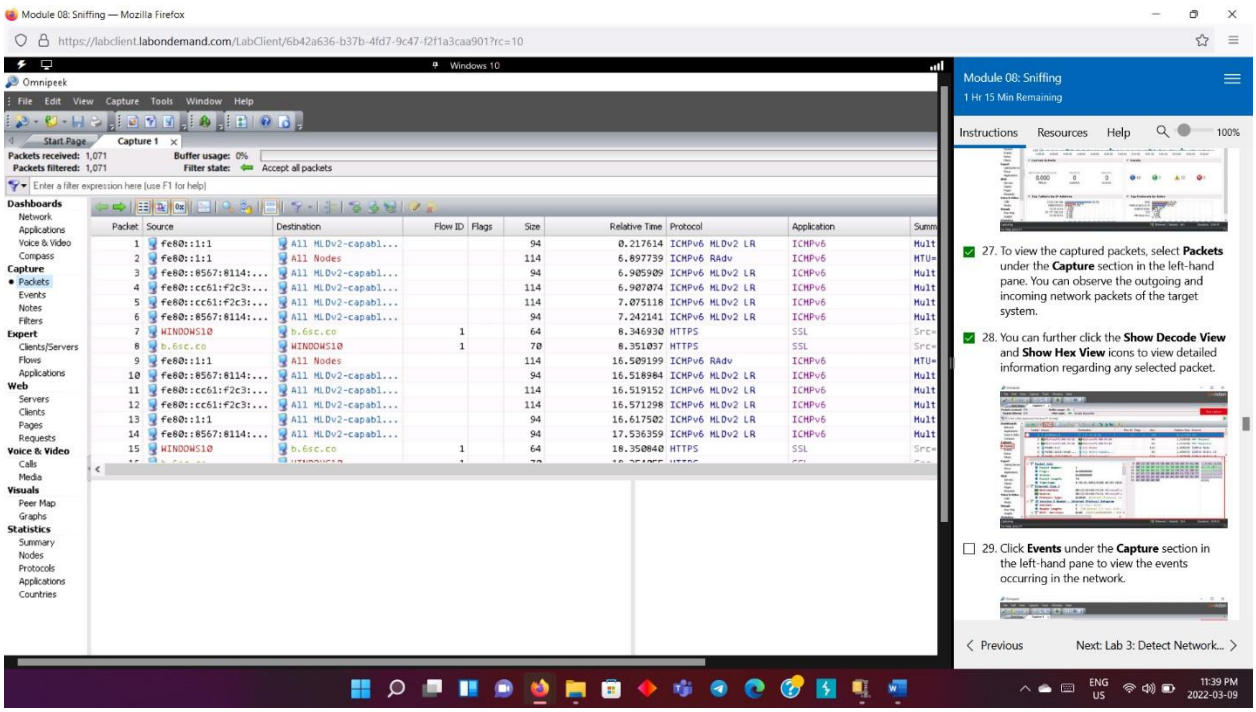
-

Now switch to the windows server 2019 and open a browser and launch any website.

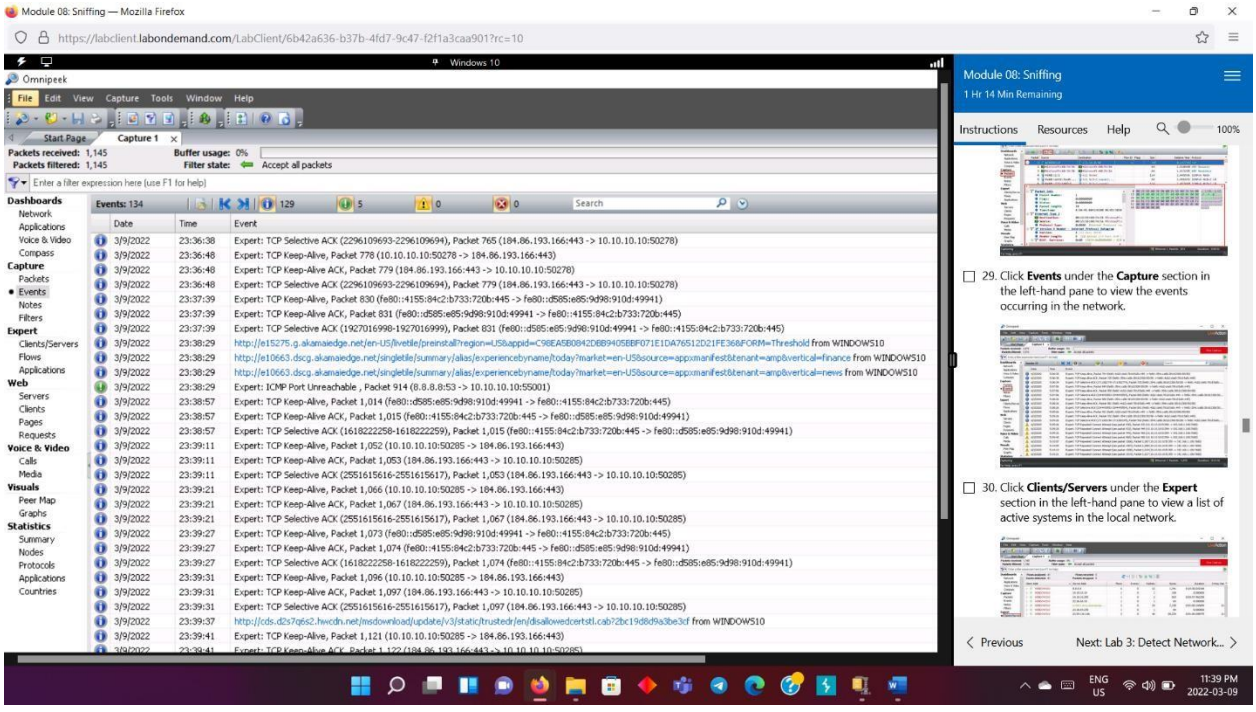


- Get back to the windows 10 machine the packets are captured and the graph bar gets displayed.



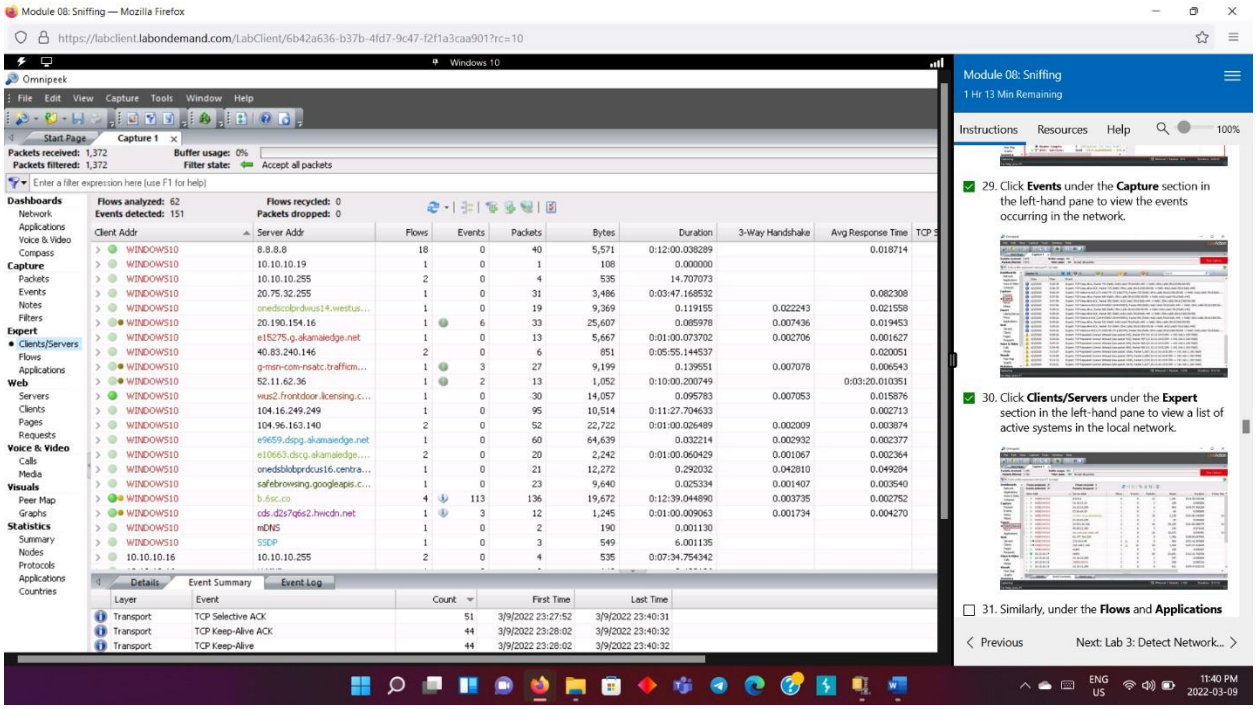


- Select events option to view all the events on the network.

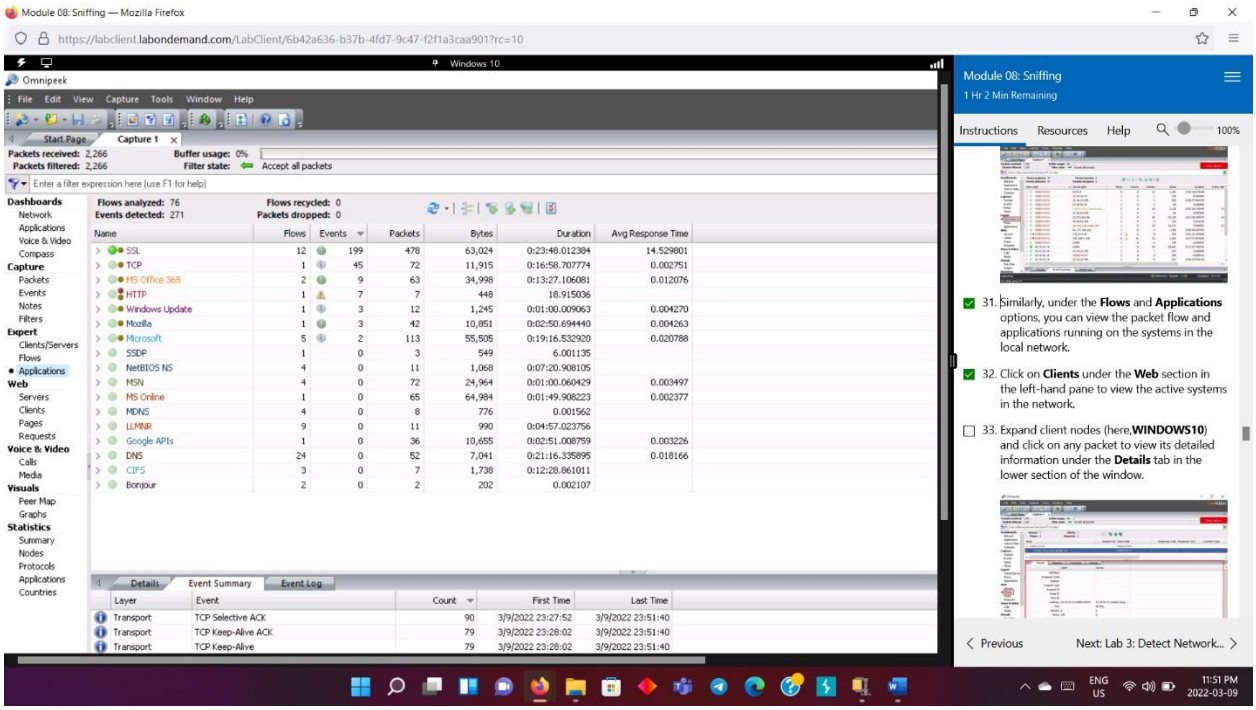


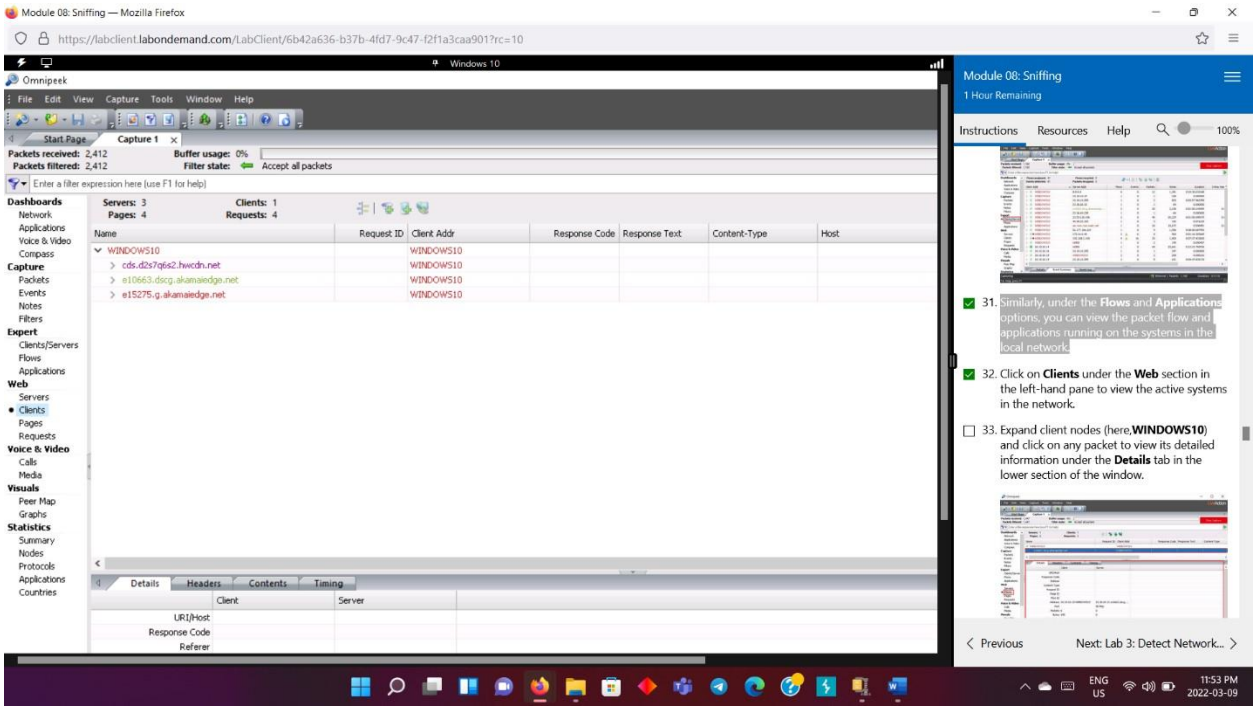
-

Select the client/server option to view all the active systems on the network.

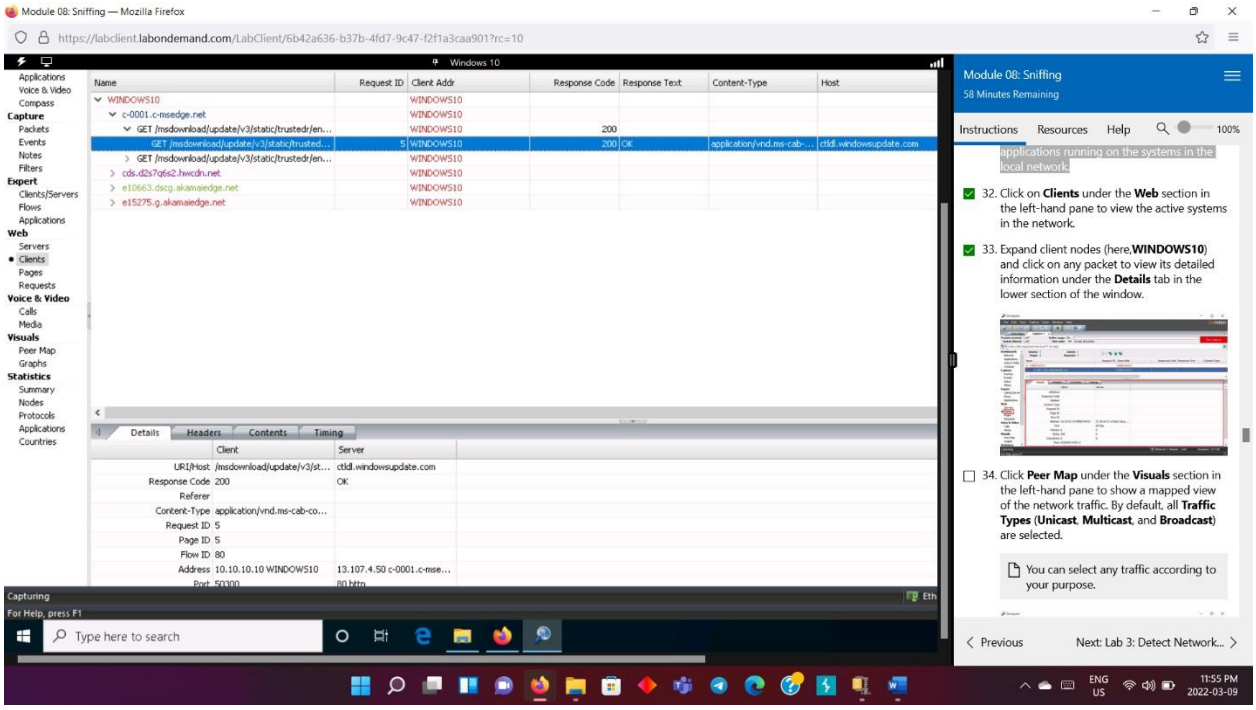


- Select flows and applications to view the packet flow.



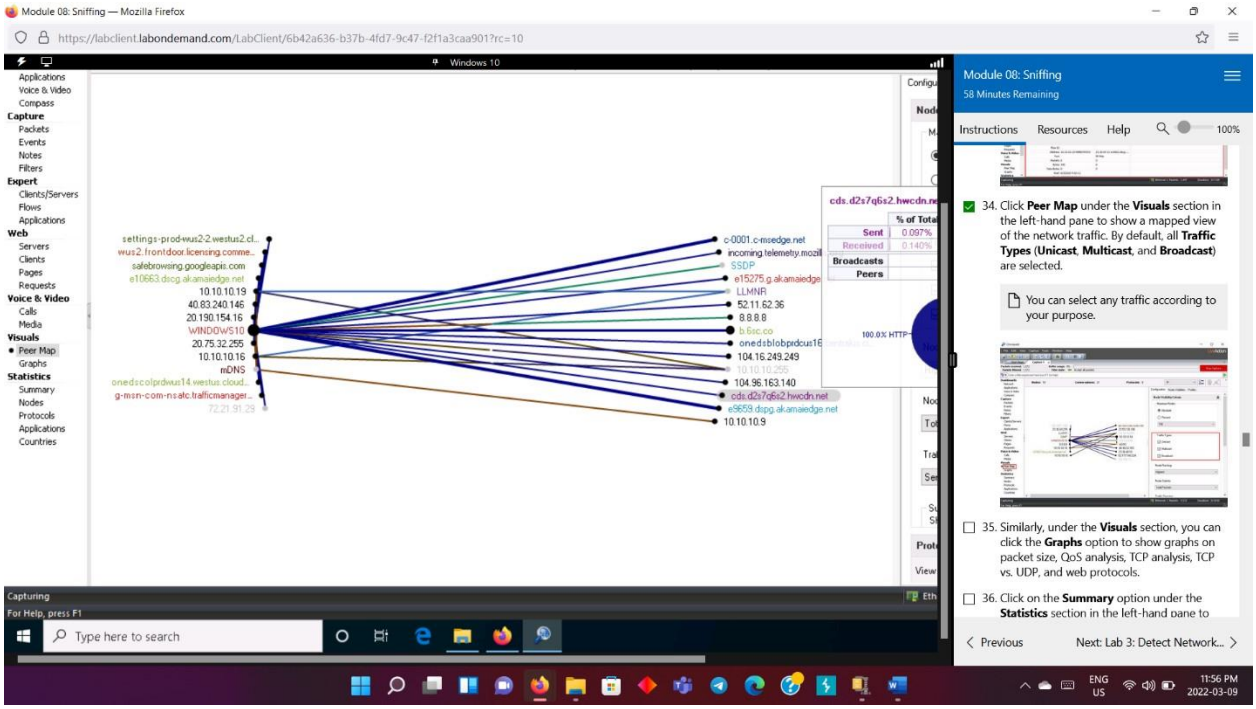


- Choose any packet to get the detailed information.

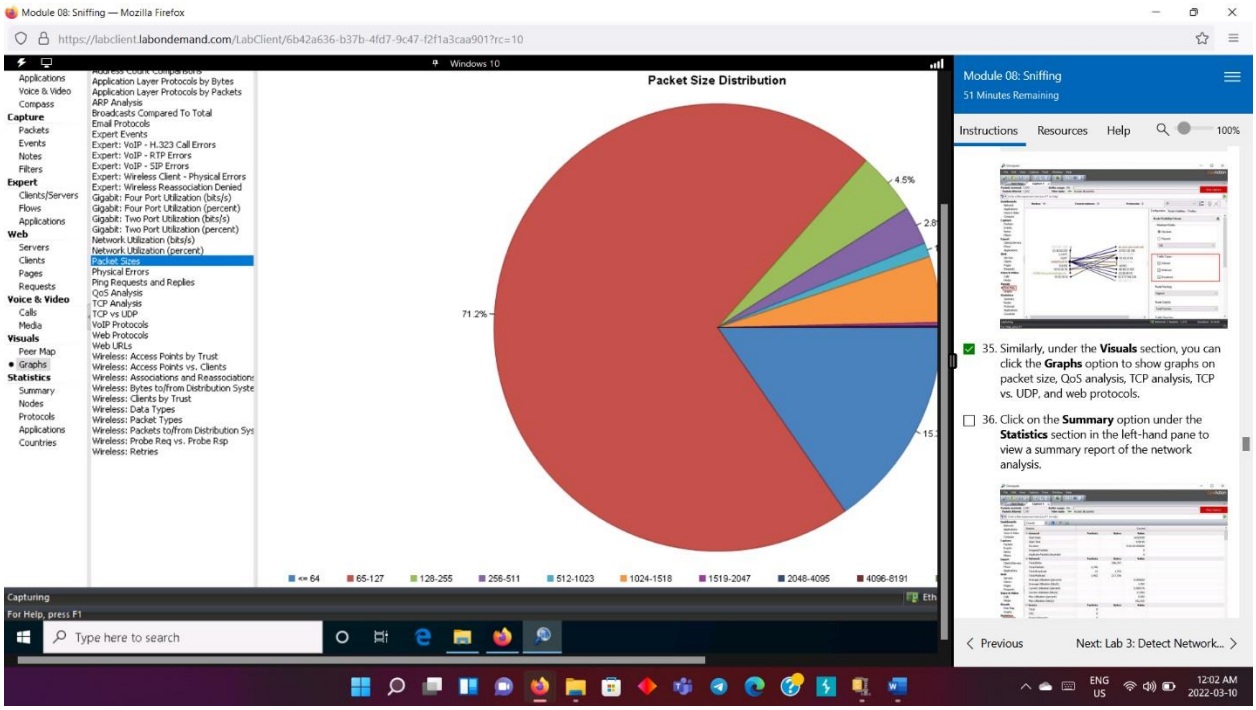


-

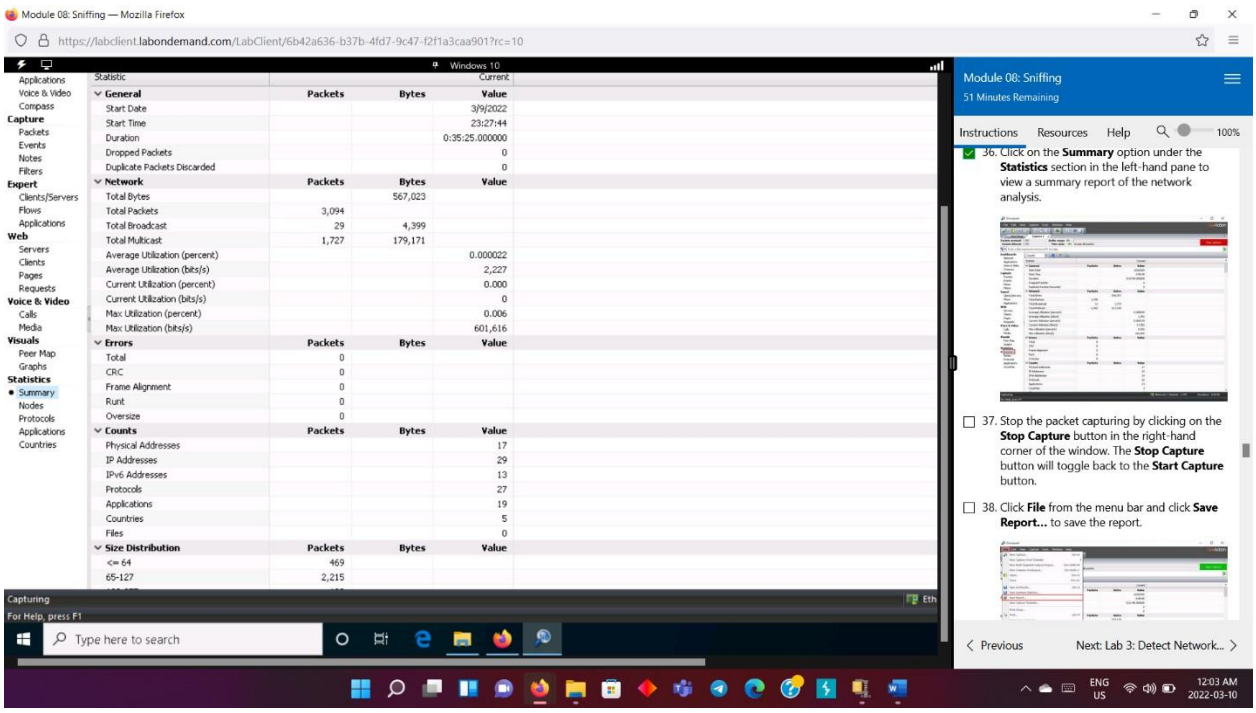
Select the peer map option to get a map view.



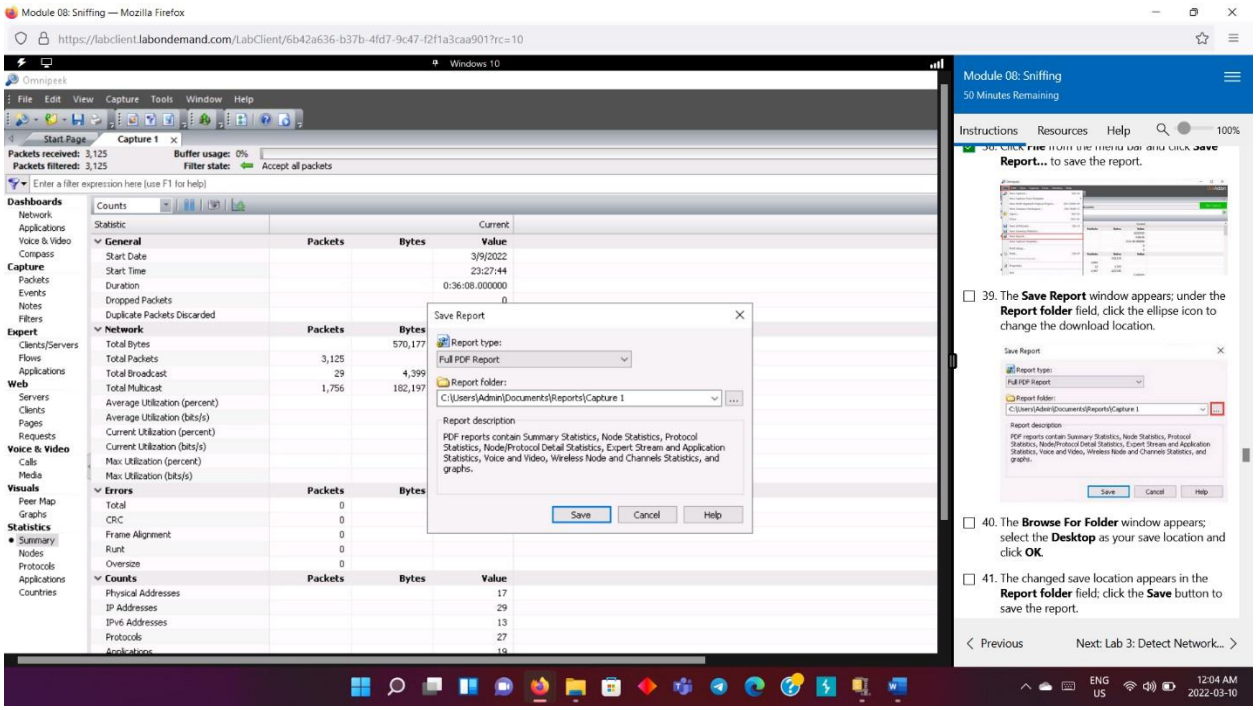
- Under visuals, select the graph option to get the details of QoS analysis, TCP analysis , TCP vs UDP and web protocols.



- Select summary option under the statistics section to view the summary report.

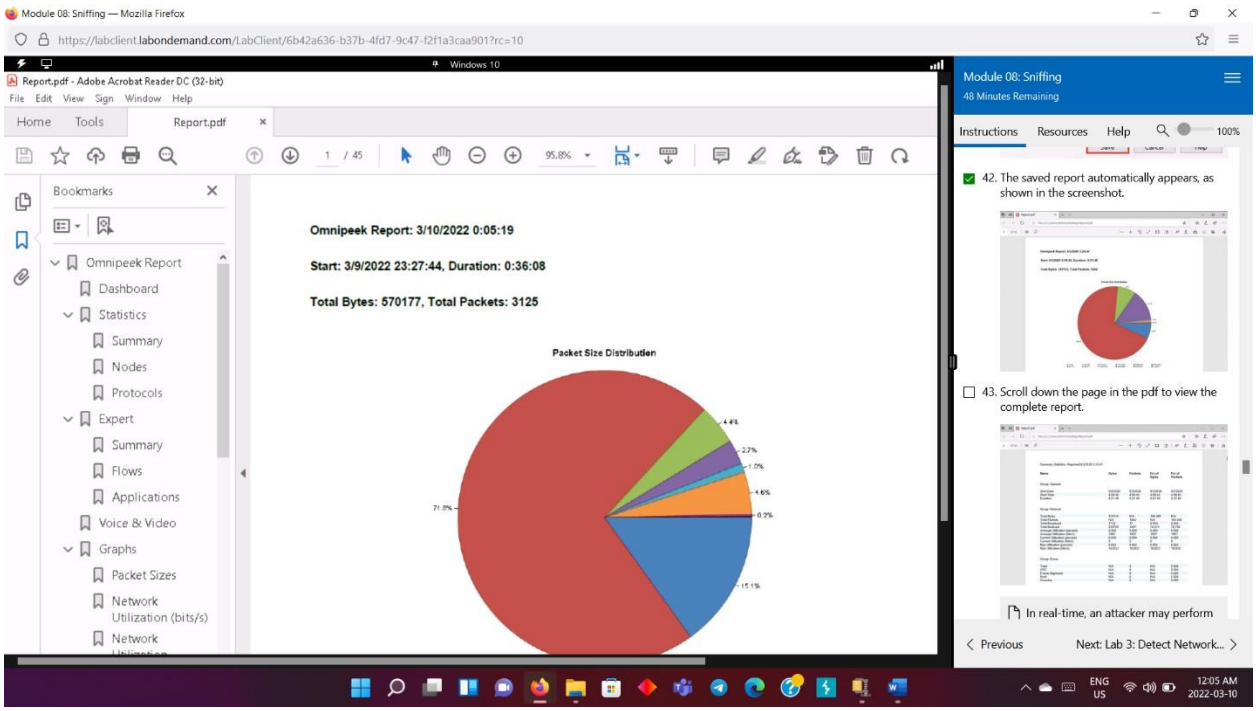


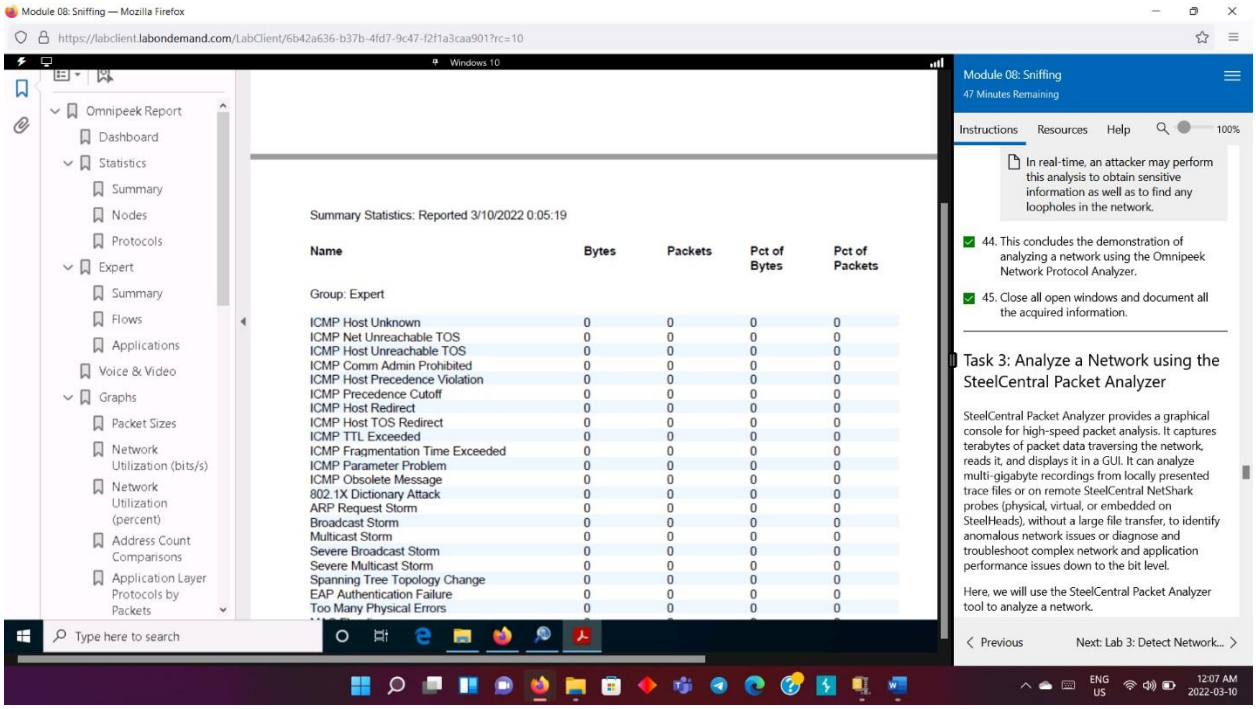
- Select stop capture and go to file and select save report and download the report.



-

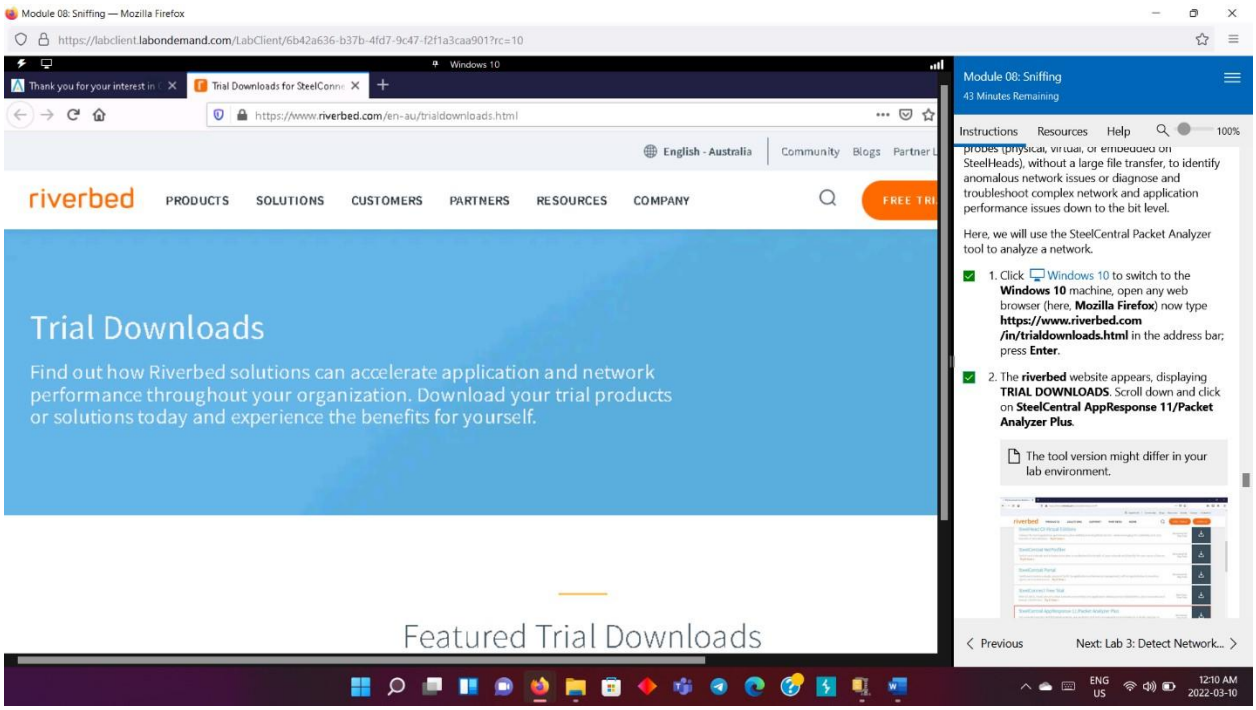
The saved report opens and scroll down to view the complete report.





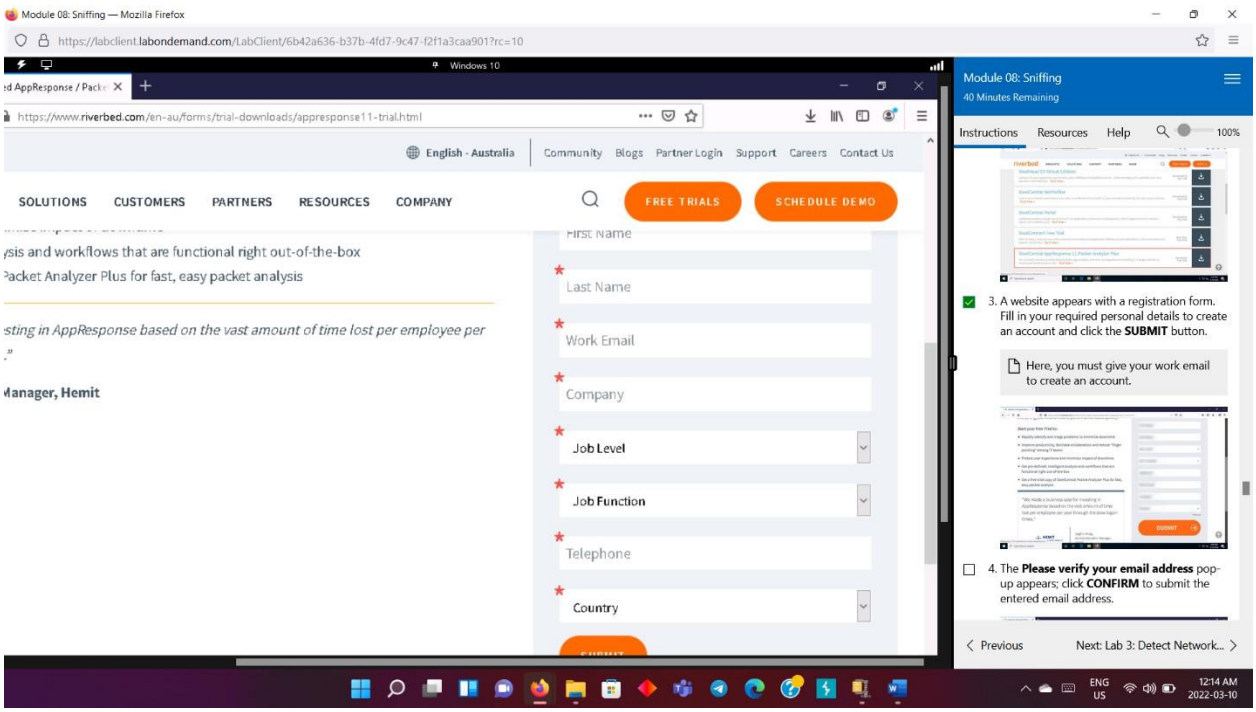
Task 3: Analyze a Network using the SteelCentral Packet Analyzer

- Launch the windows 10 OS, and open any browser and copy paste the link **https://www.riverbed.com/in/trialdownloads.html** and click on enter.

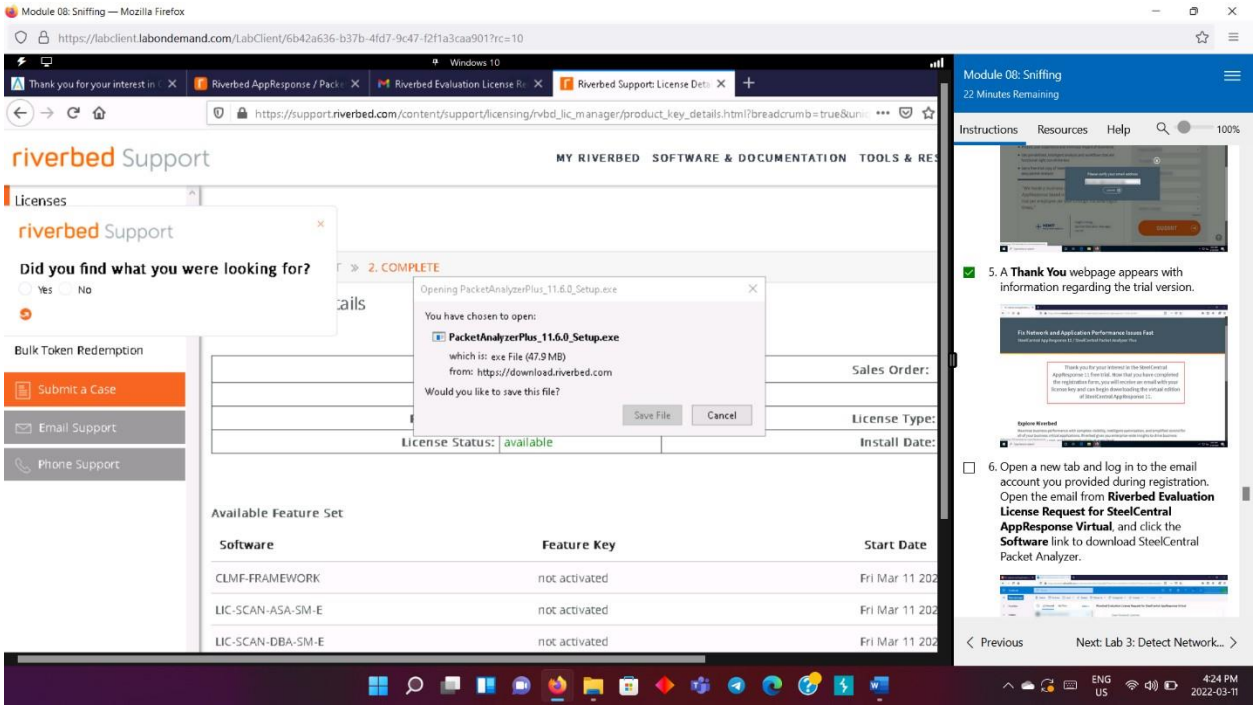


- The website launches, select steel central packet analyzer. Now fill the form and click on submit.

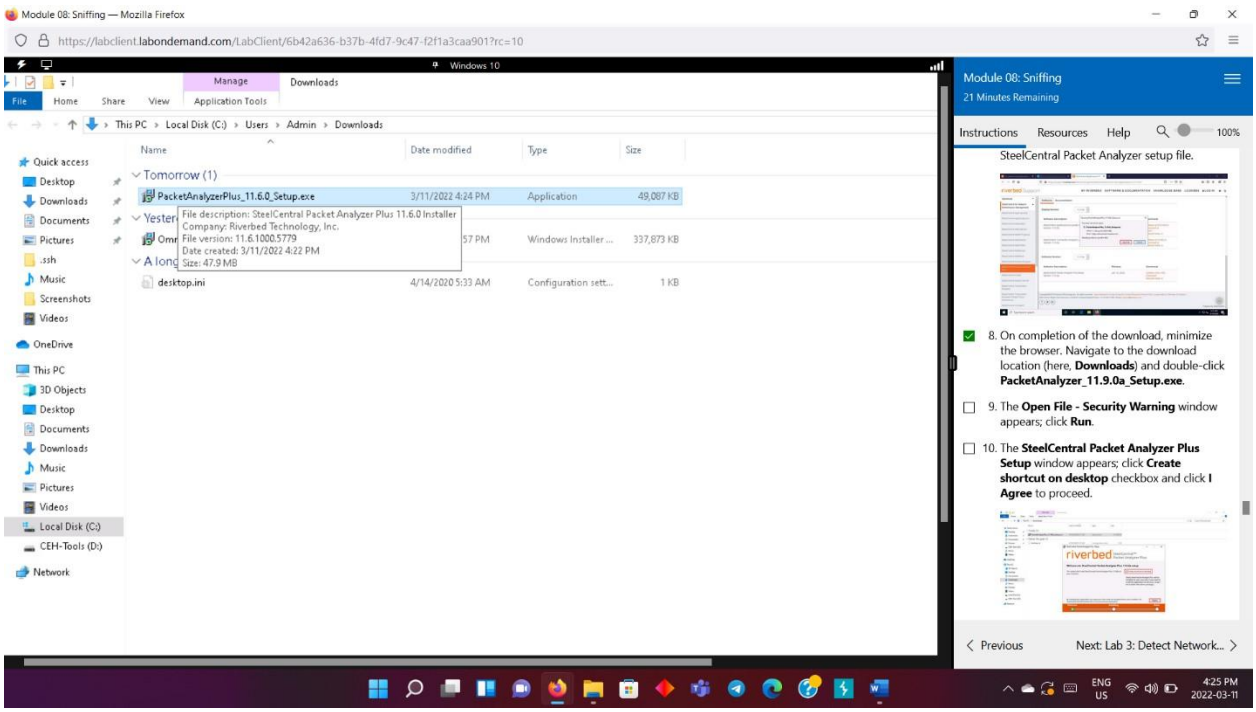
•

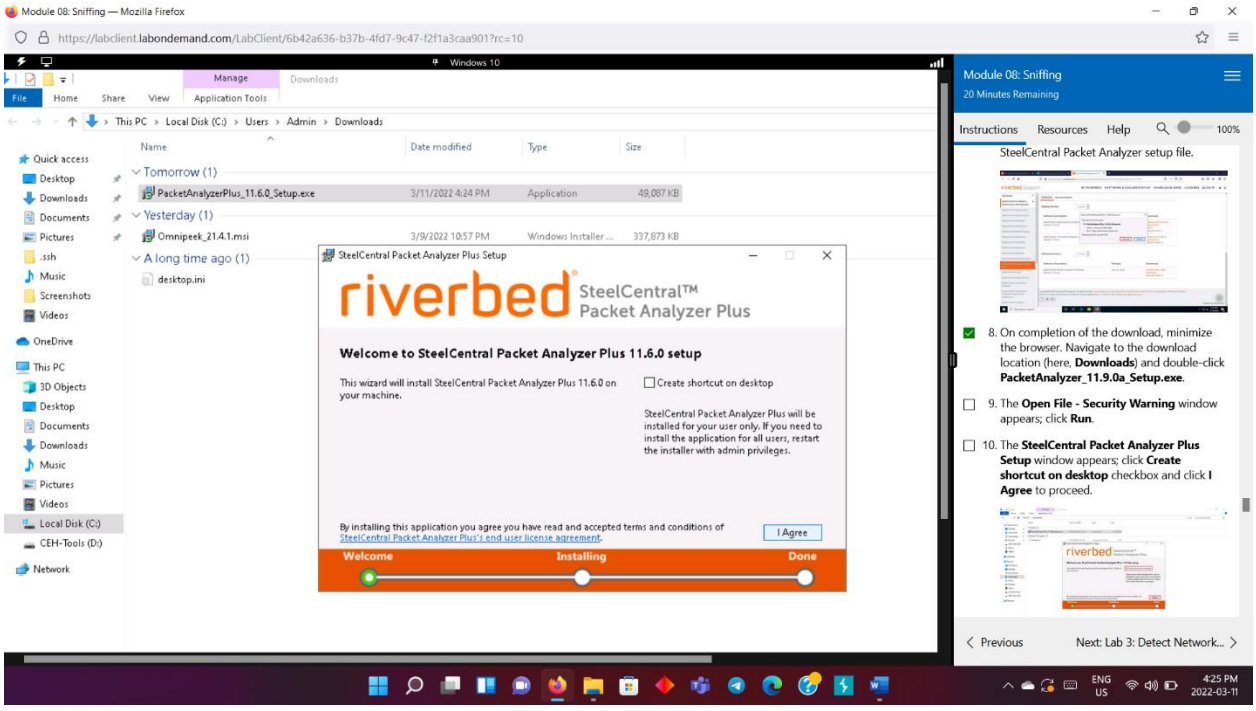


Confirm the email address. Launch the email received and select the link to download the software.

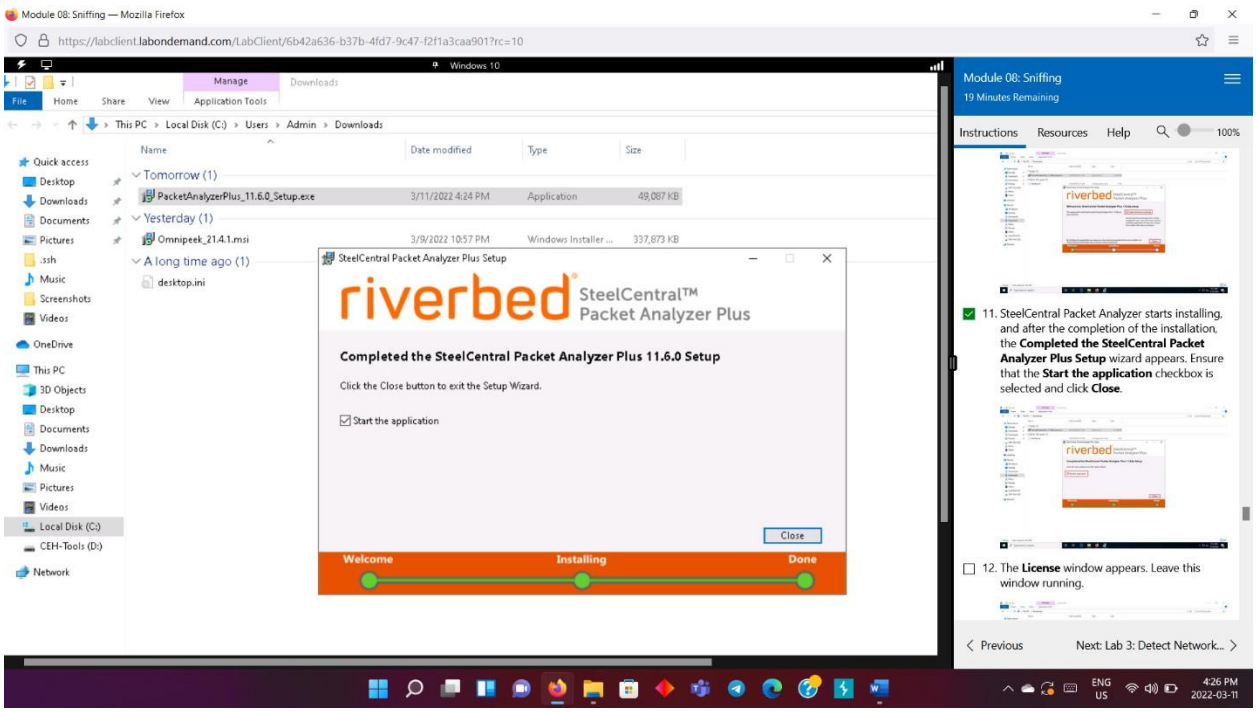


- The exe file pops up, save the file in the folder.

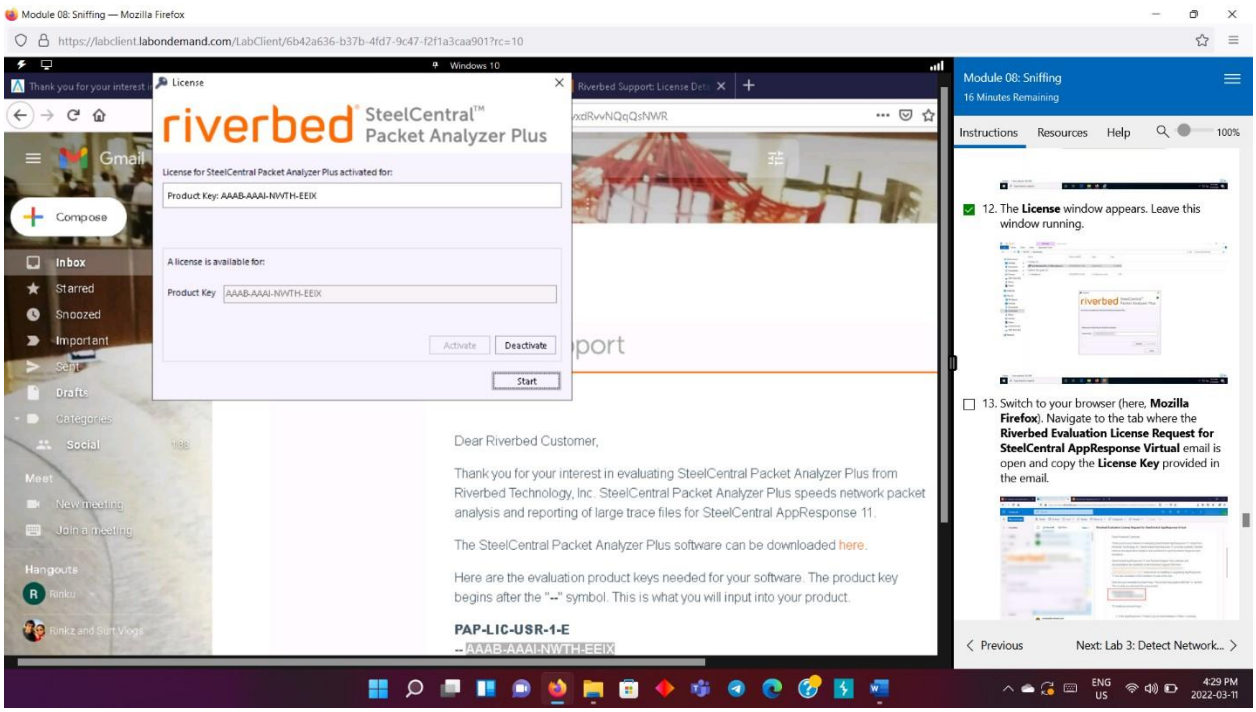




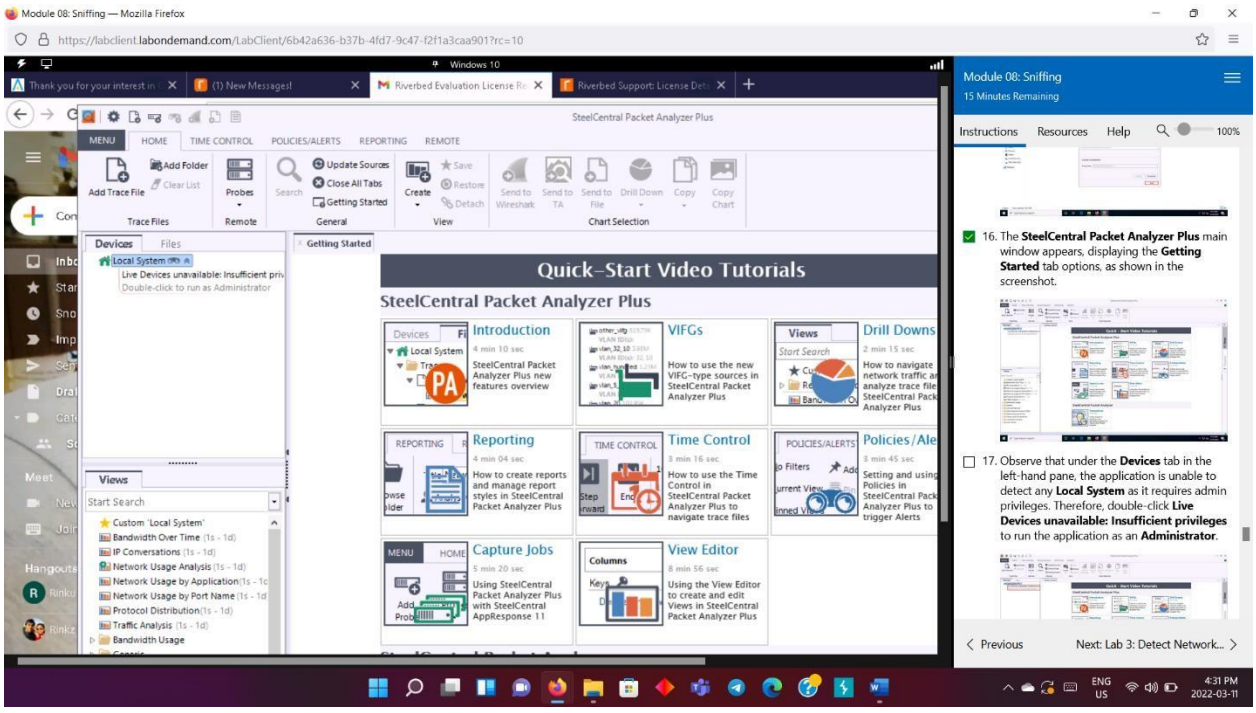
- Once the installation is complete, check the start the application option and click on close button.



Copy & paste the license key from the email received and then click on the activate button.

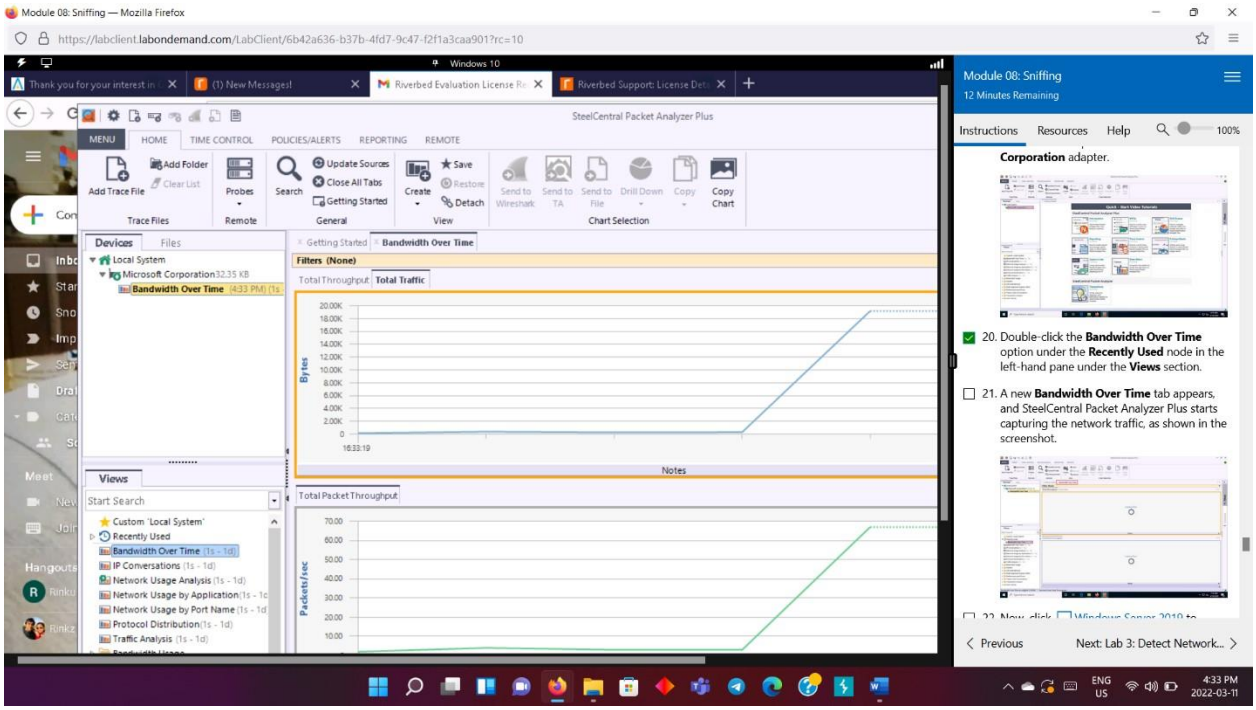


- Click on start button to start the application.



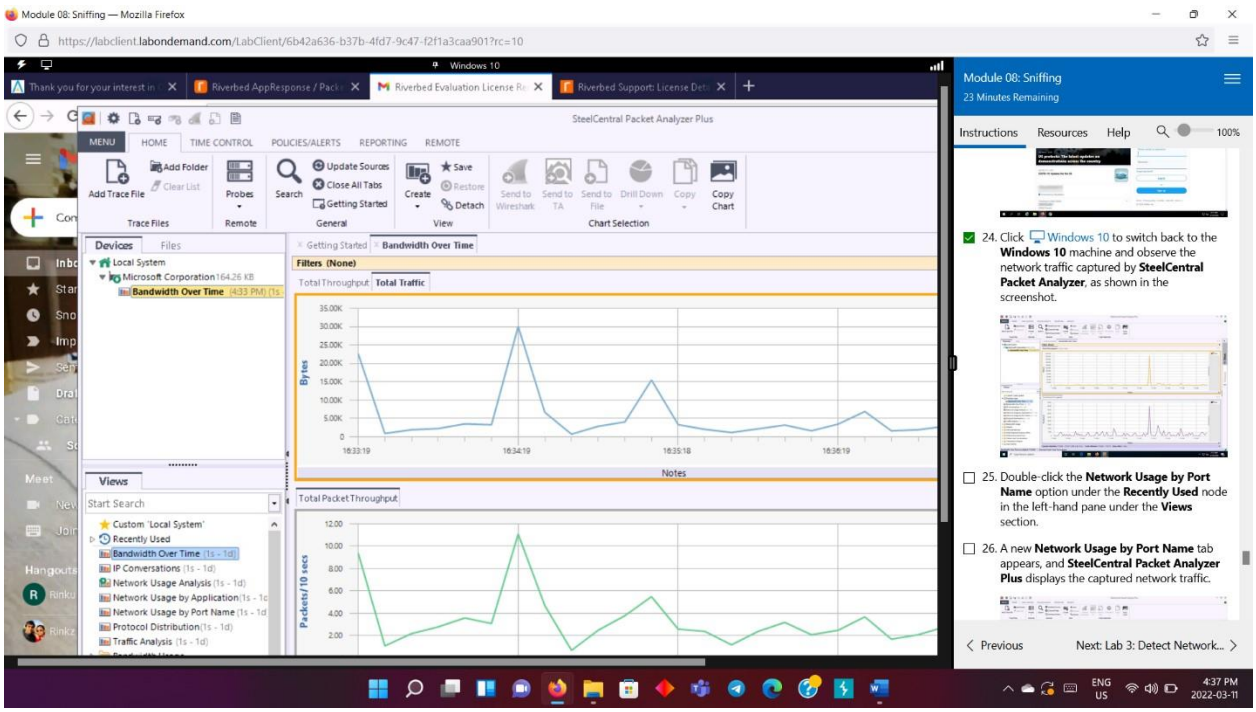
-

Run the application as administrator by double clicking the live devices unavailable: insufficient privileges. Select Microsoft corporation under ethernet. The bandwidth over time tab appears, now it starts capturing network traffic.

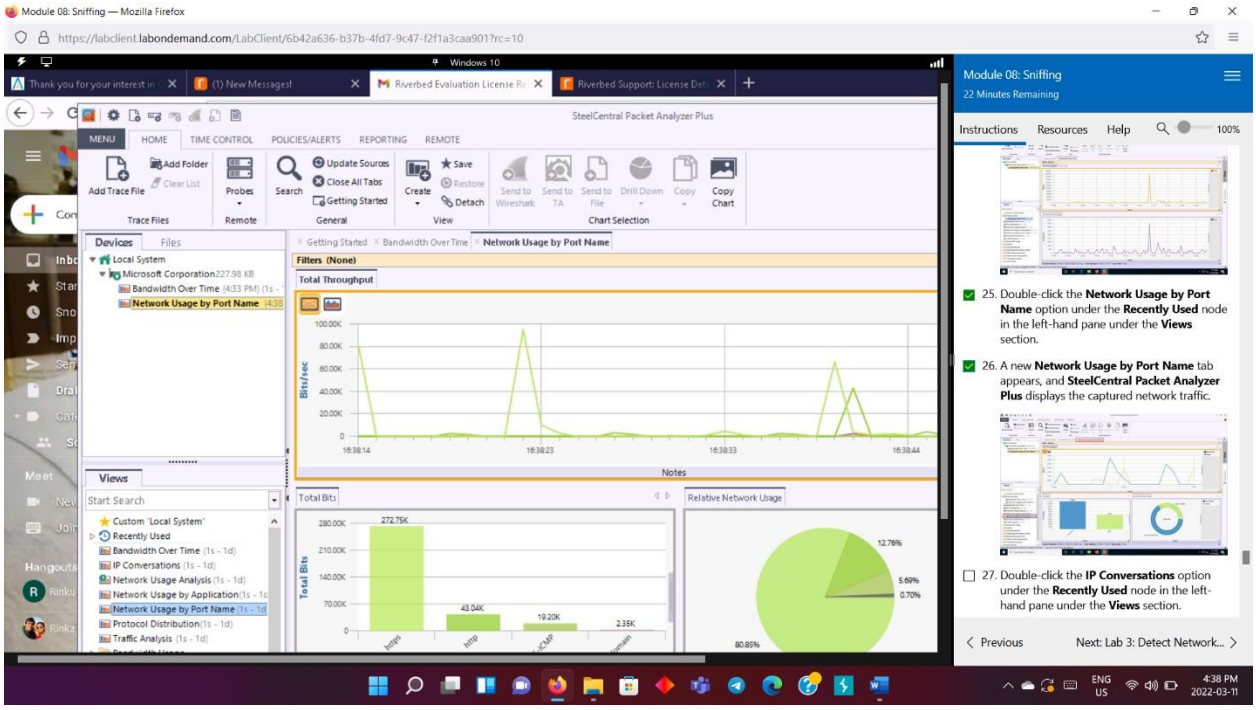


- Switch back to windows server 2019, since the machine acts as the target, launch any web browser and search for twitter.

Go back to windows 10 OS and observe the packets captured.

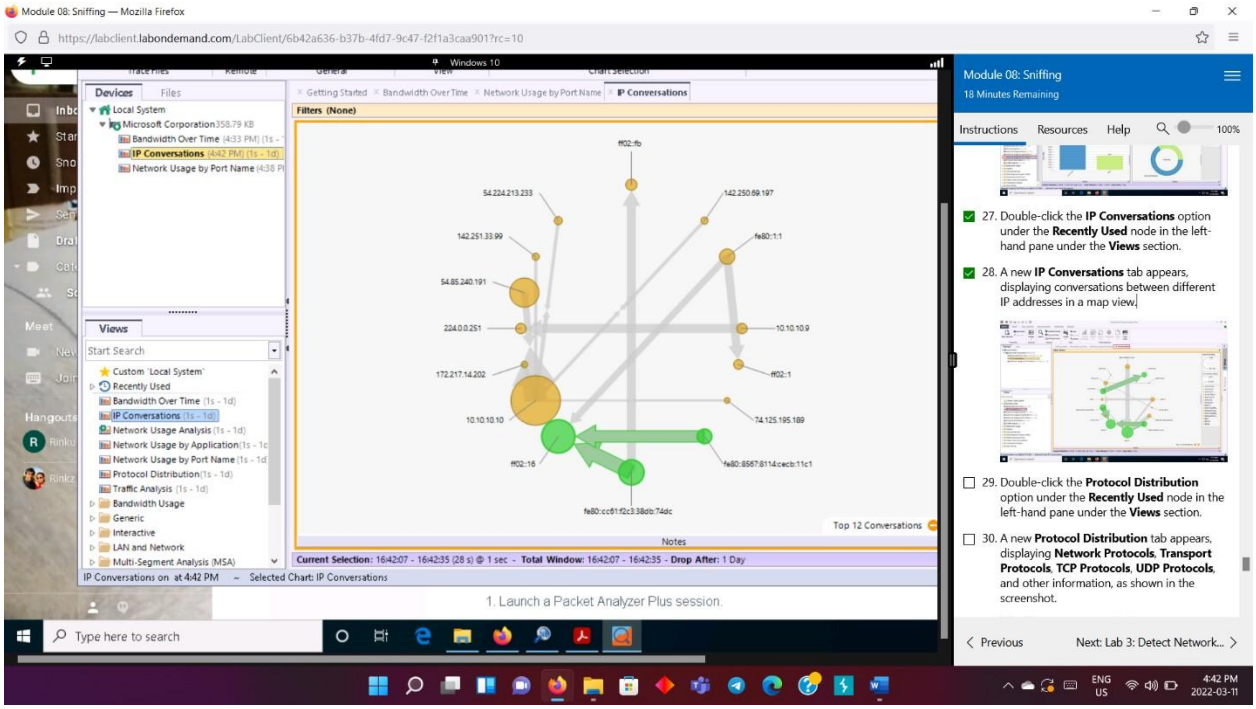


- Now a new network usage port appears, and it displays the captured network traffic. The IP conversation tab appears to display the conversation among different IP address. Double click on the IP conversation under the view option.

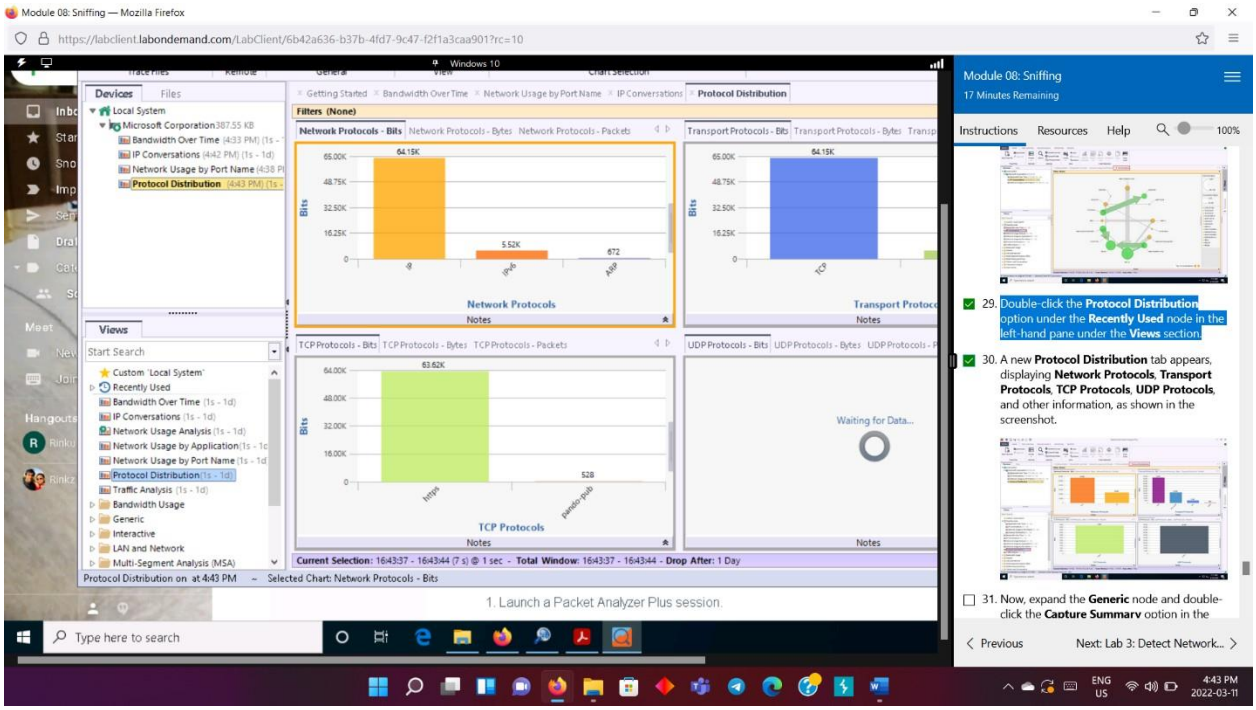


-

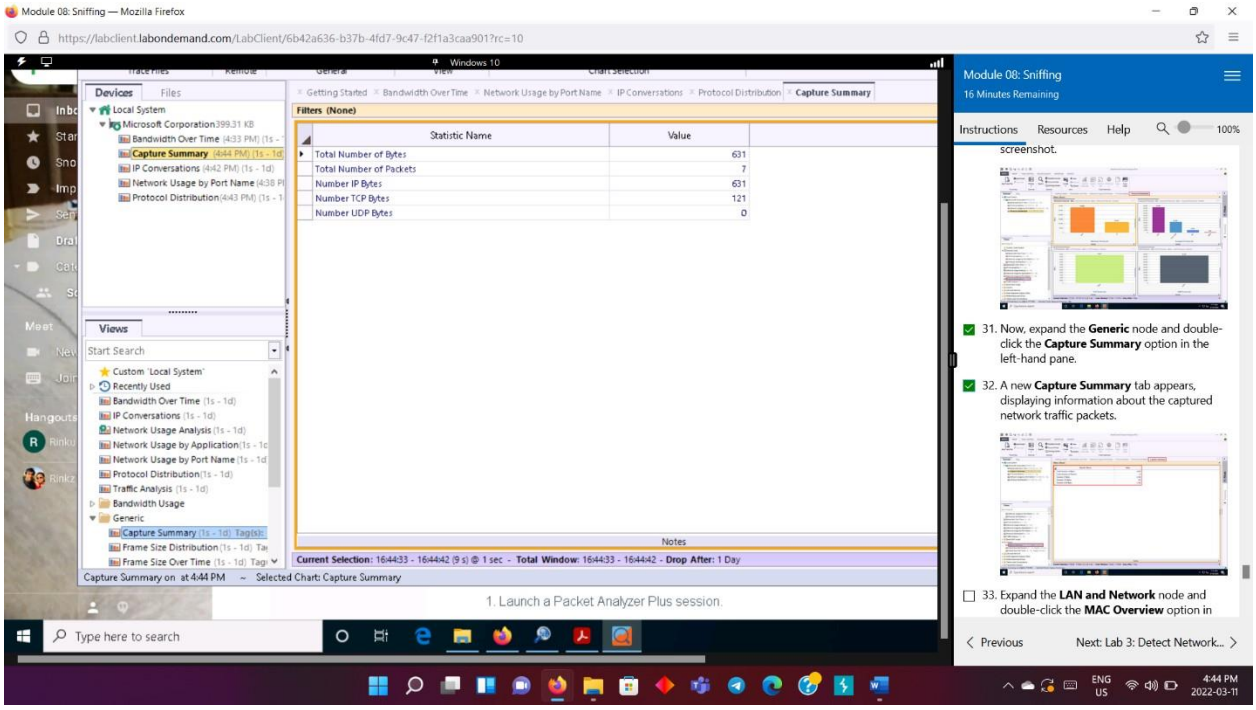
- A new IP conversation appears, it displays the map view of the conversation.



- Now double click on the protocol distribution under recently used node.

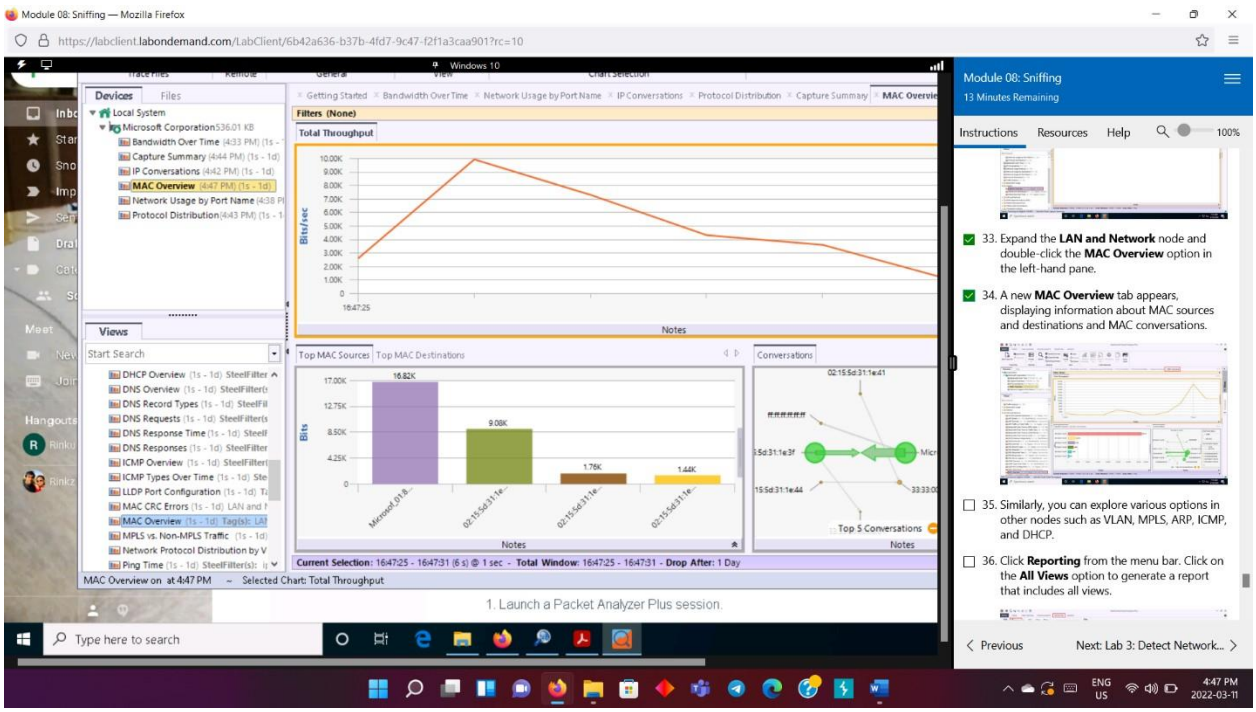


The new protocol distribution tab appears, displaying the network protocols, transport protocols, TCP protocols, UDP protocols etc. Now the capture summary option appears to view the information of the captured network traffic.

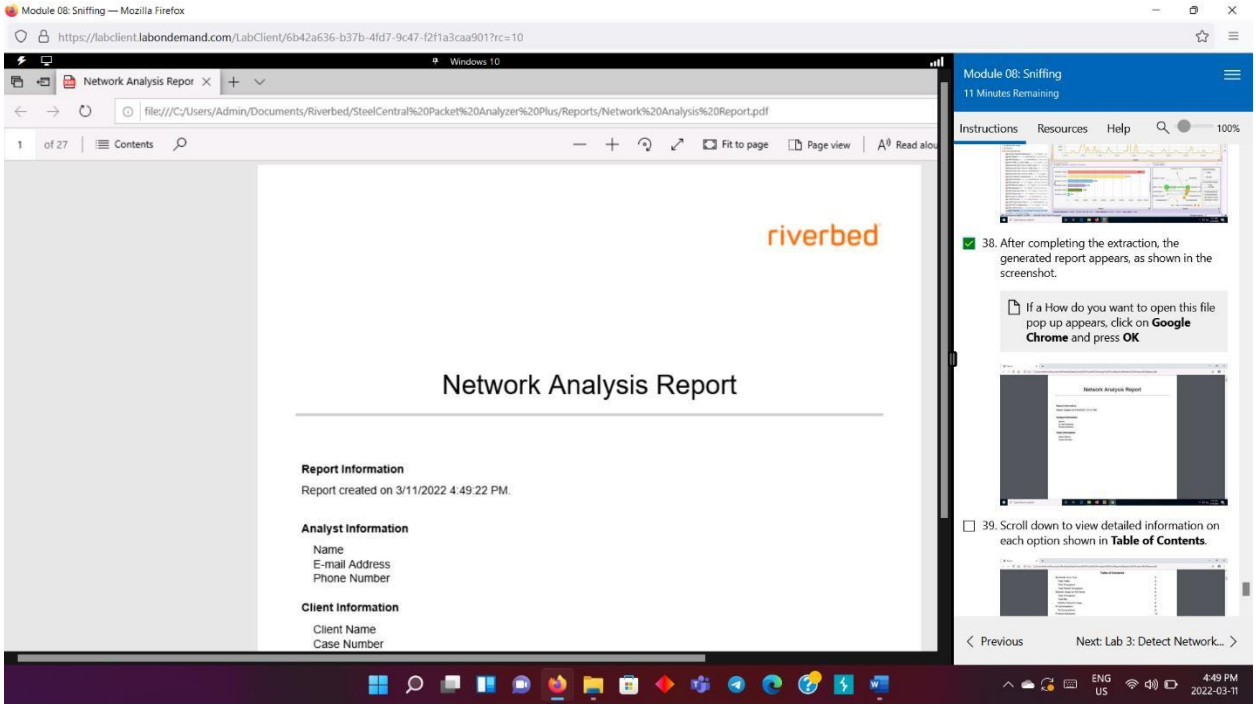


- Select MAC overview, it provides the MAC source and MAC conversations.

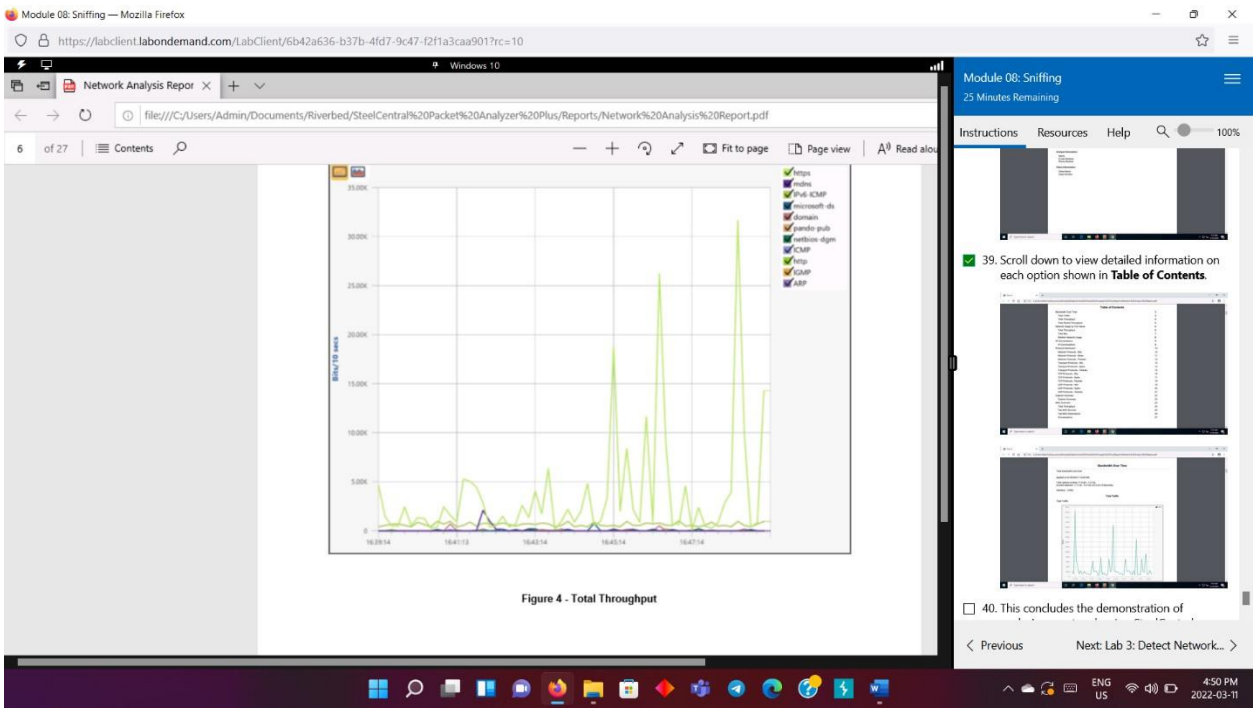
•



- Finally, select reporting from the main menu bar and then select all views to generate report.



- Scroll down and expand the full report to get the complete information.



- This concludes the demonstration.