

Contents

Abstract.....	1
Module 08: Sniffing.....	2
Lab 1: Perform Active Sniffing	2
Task 1: Perform MAC Flooding using macof.....	2
Task 2: Perform a DHCP Starvation Attack using Yersinia	7
Task 3: Perform ARP Poisoning using Arp spoof.....	14
Task 4: Perform a Man-in-the-Middle (MITM) Attack using Cain & Abel.....	19
Task 5: Spoof a MAC Address using TMAC and SMAC.....	29
Lab 2: Perform Network Sniffing using Various Sniffing Tools	40
Task 1: Perform Password Sniffing using Wireshark	40
Task 2: Analyze a Network using the Omnipacket Network Protocol Analyzer	54
Task 3: Analyze a Network using the SteelCentral Packet Analyzer	67
Lab 3: Detect Network Sniffing	Error! Bookmark not defined.
Task 1: Detect ARP Poisoning in a Switch-Based Network	Error! Bookmark not defined.
Task 2: Detect ARP Attacks using XArp	Error! Bookmark not defined.
Task 3: Detect Promiscuous Mode using Nmap and NetScanTools Pro.....	Error! Bookmark not defined.

Abstract

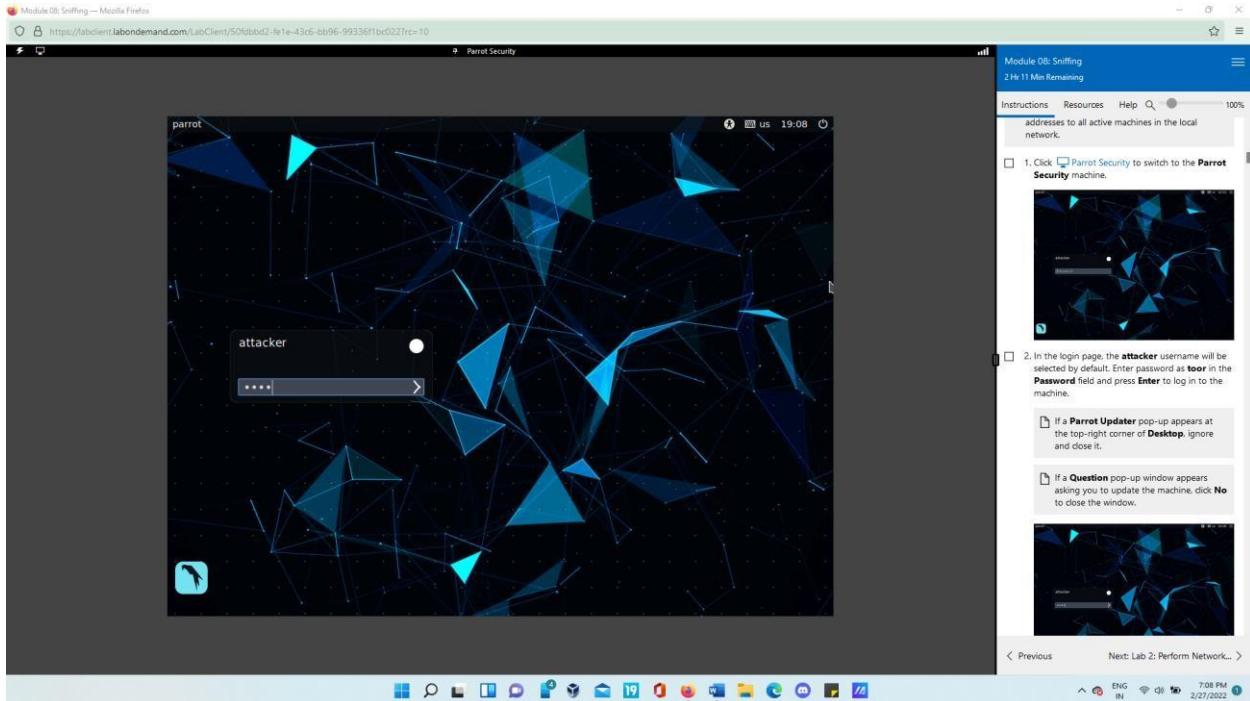
In this Assignment, we have performed two attacks namely, network sniffing and social engineering. Basically, sniffing is a technique through which a person gets access on overall traffic in the network while leaving or entering the network. Here, we are going to sniff the packets and perform MAC flooding, 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

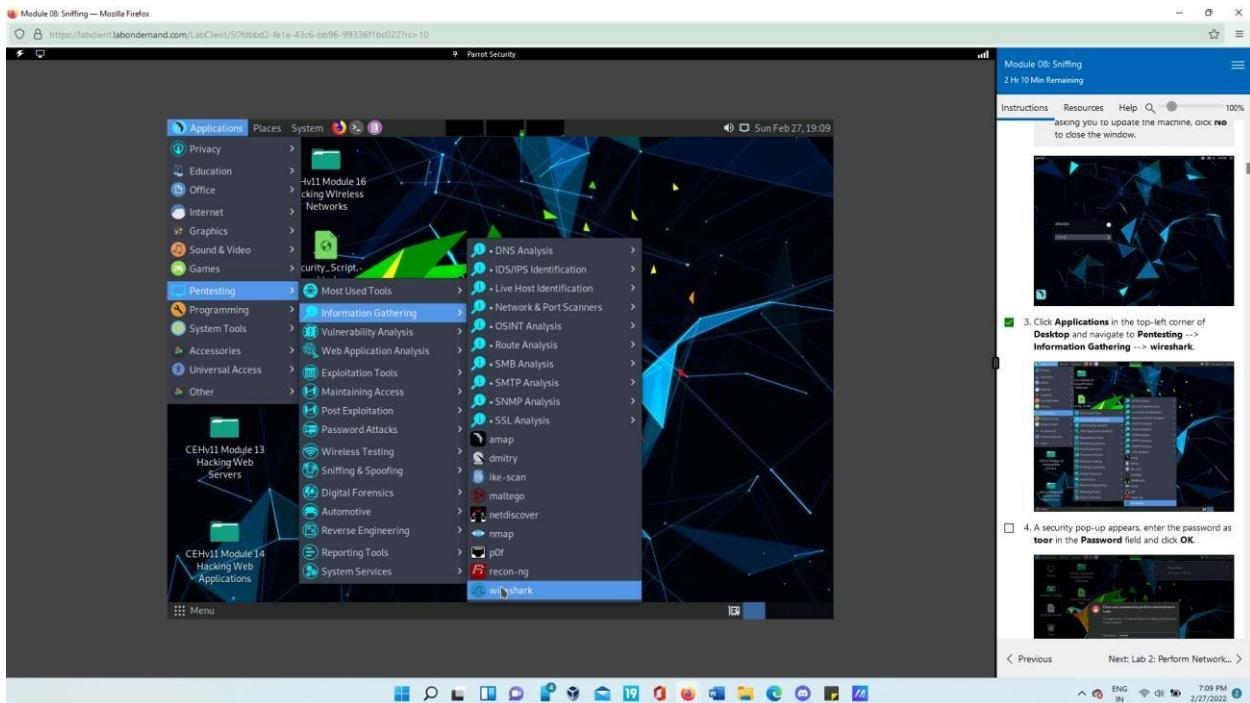
Lab 1: Perform Active Sniffing

Task 1: Perform MAC Flooding using macof

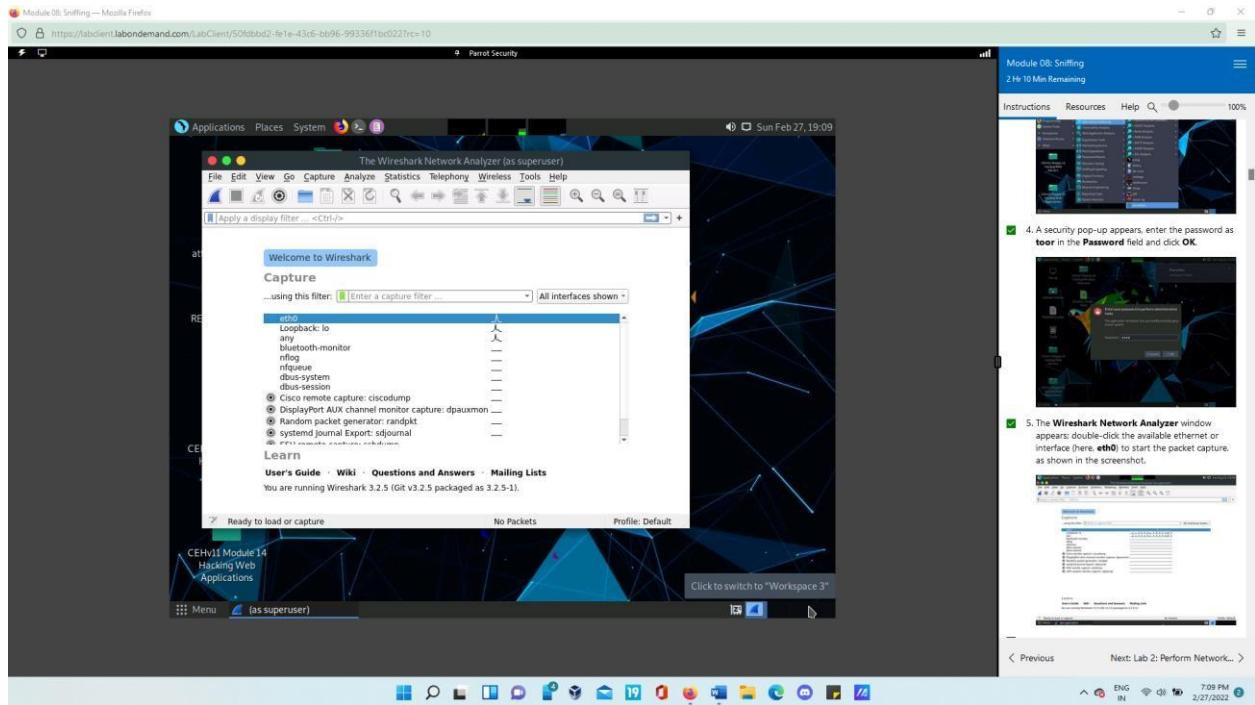
- First, we need to switch to the ParrotOS



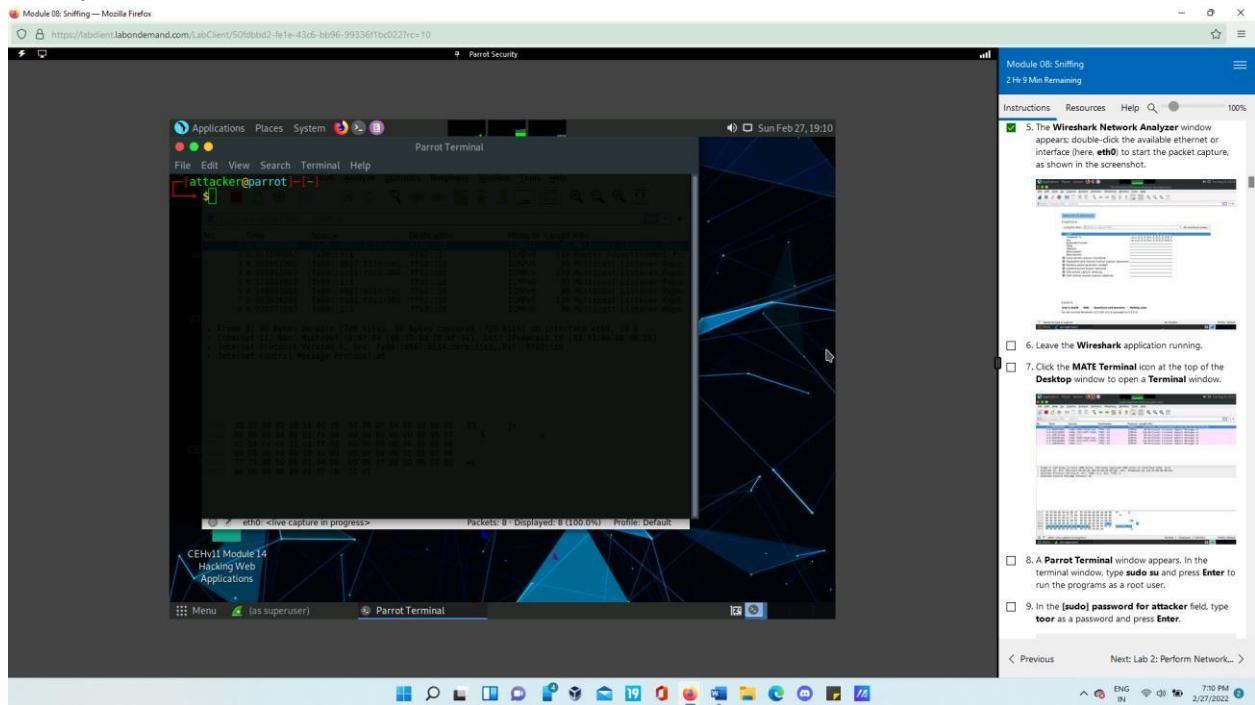
- Open Wireshark by navigating from the applications drop down menu.



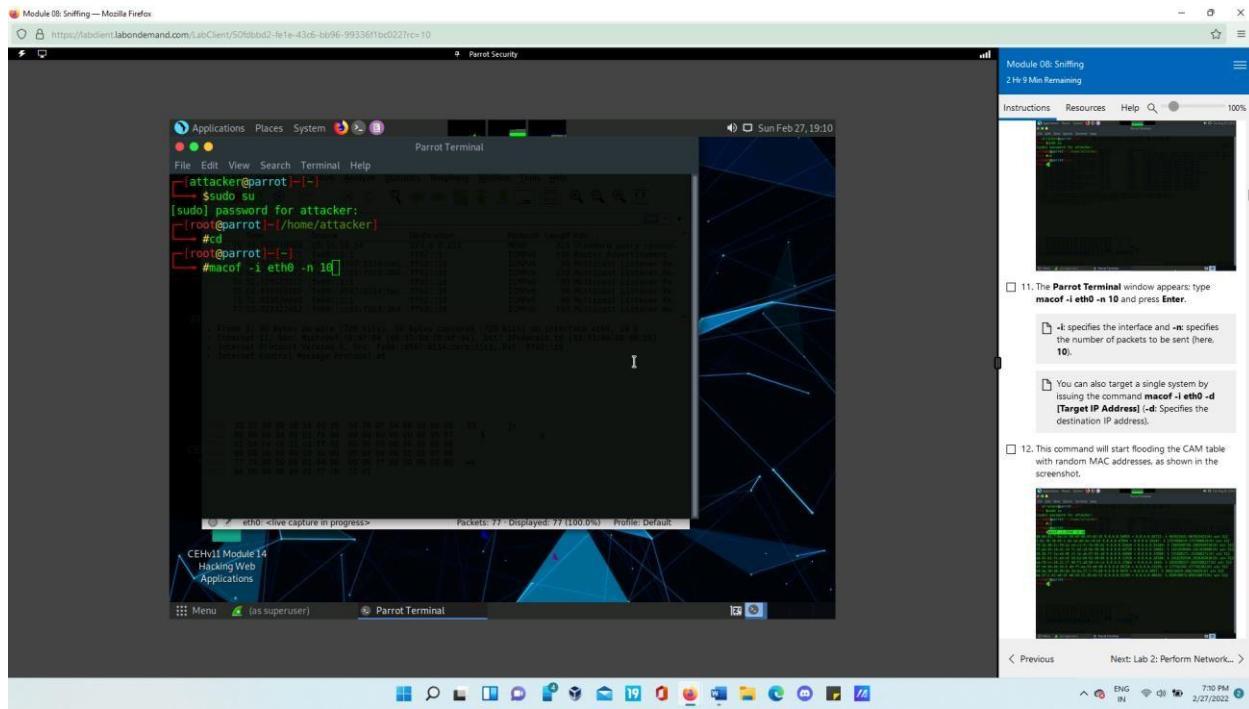
- Wireshark Network Analyzer opens and select Ethernet/eth0 to start packet capture.



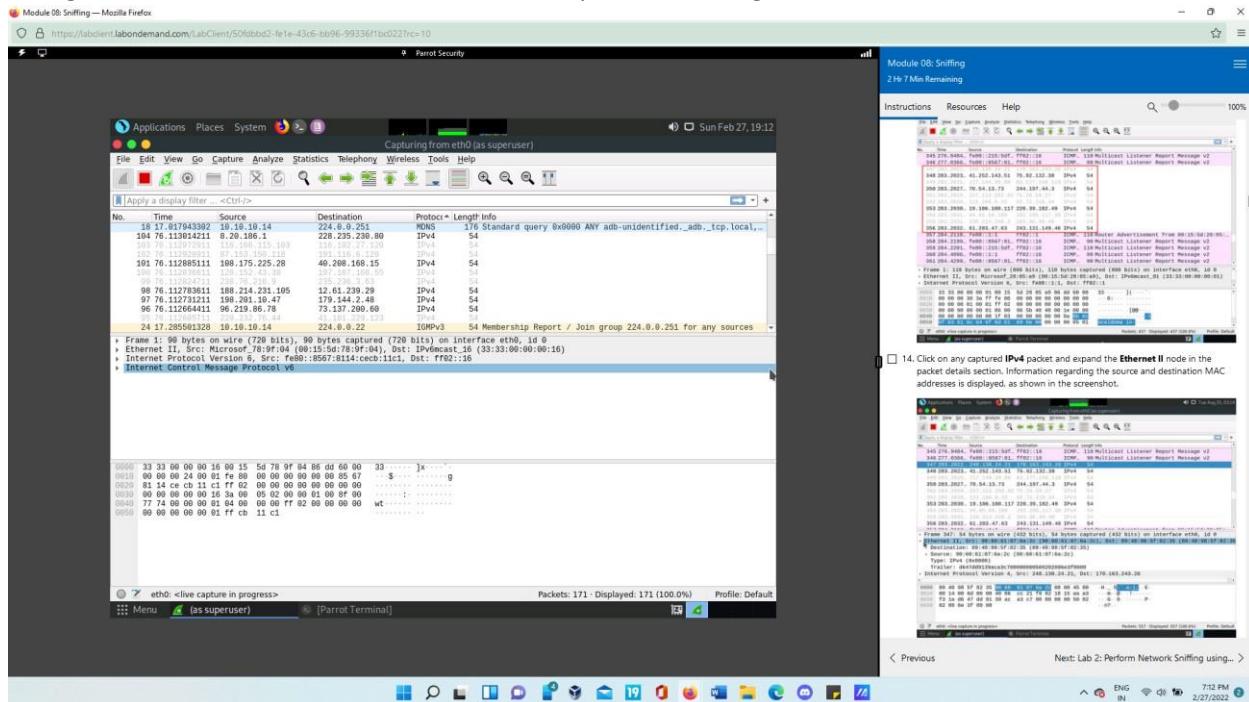
- Now open a new terminal window.



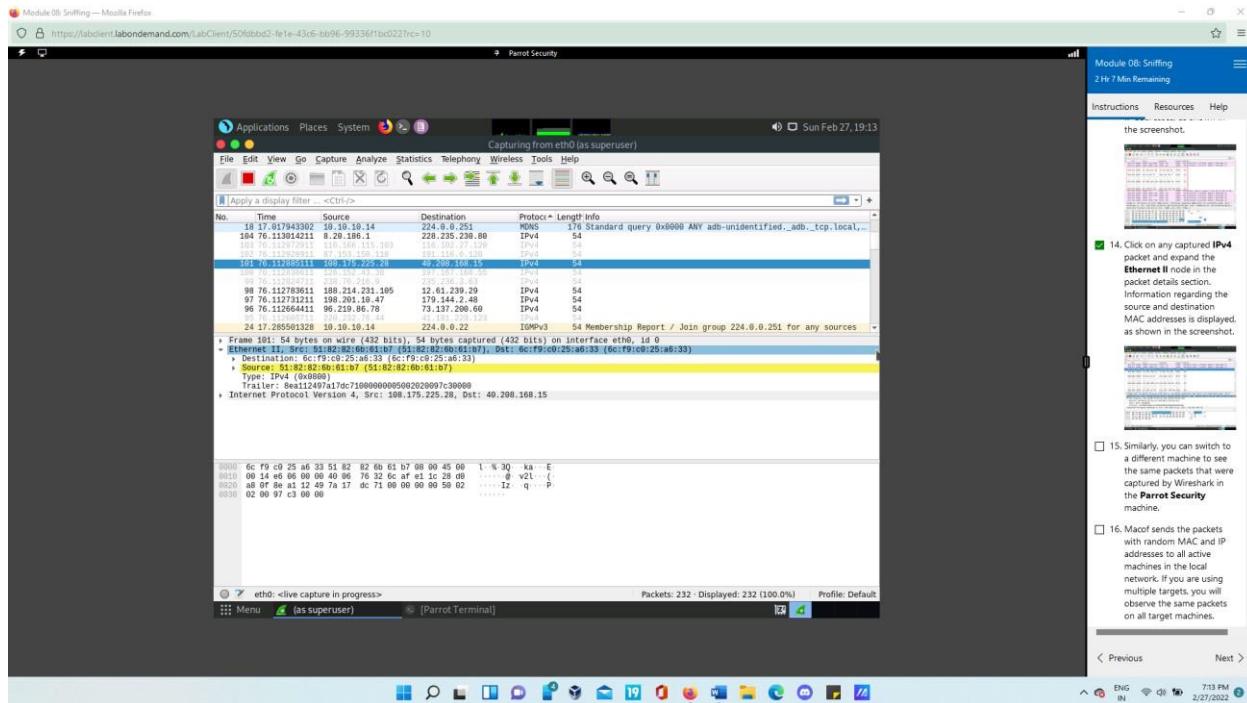
- Obtain Sudo privileges and go to root directory, now type macof -i eth0 -n 10 to start sending random MAC addresses.



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

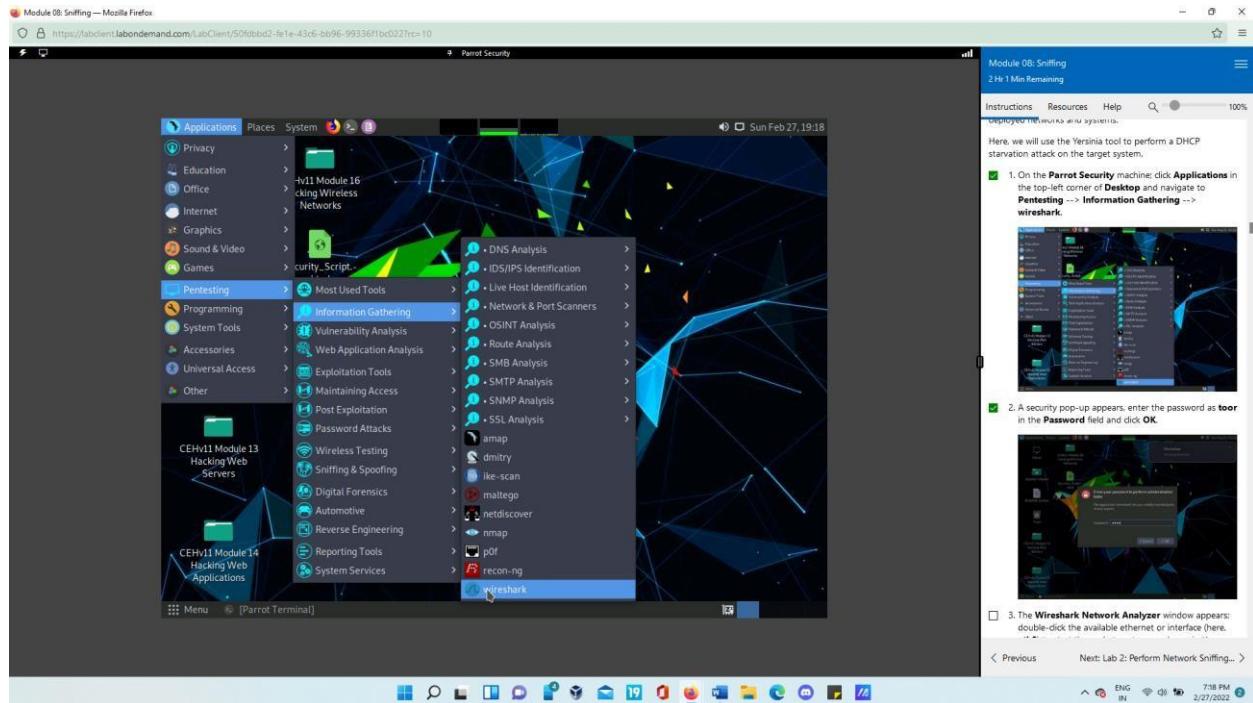


- Select any IPv4 packet and expand to packet details section to see source and destination MAC address.

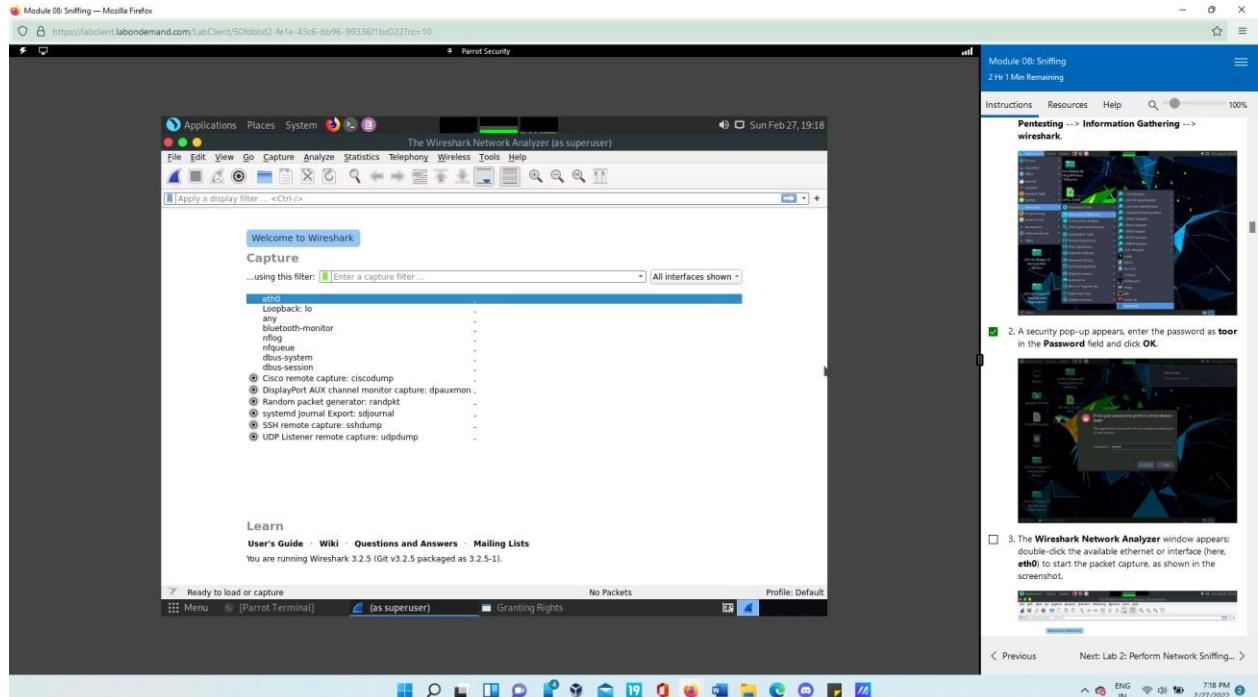


Task 2: Perform a DHCP Starvation Attack using Yersinia

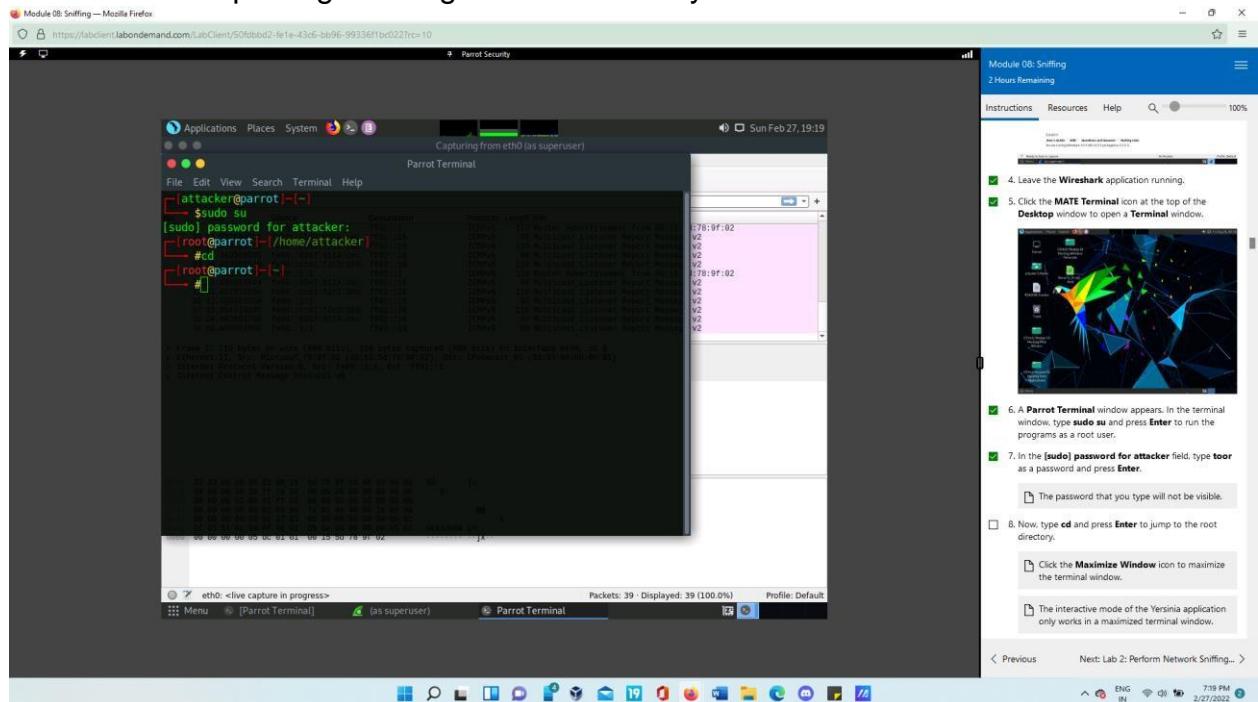
- Open Wireshark by navigating from the applications drop down menu.



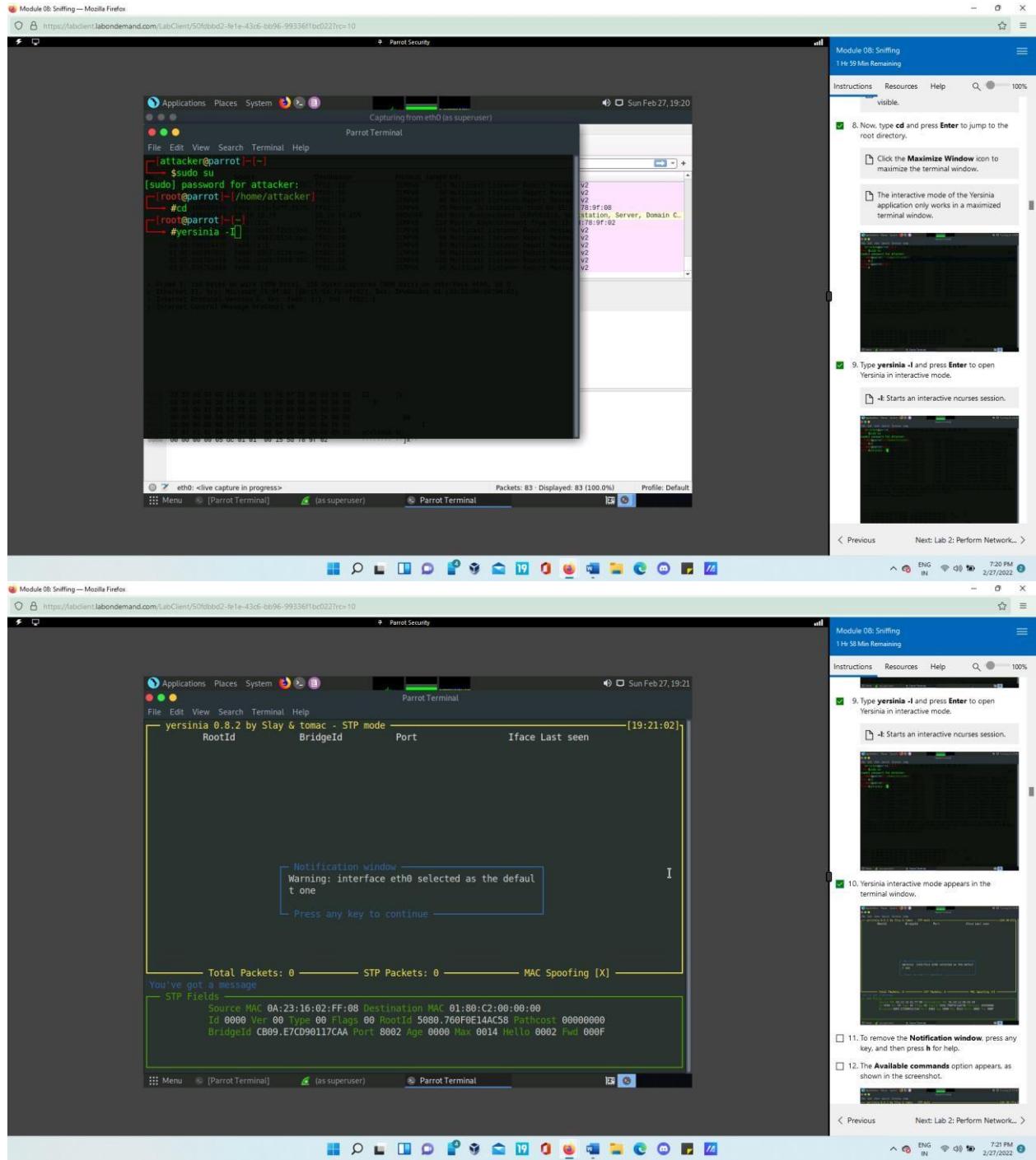
- Wireshark Network Analyzer opens and select Ethernet/eth0 to start packet capture.

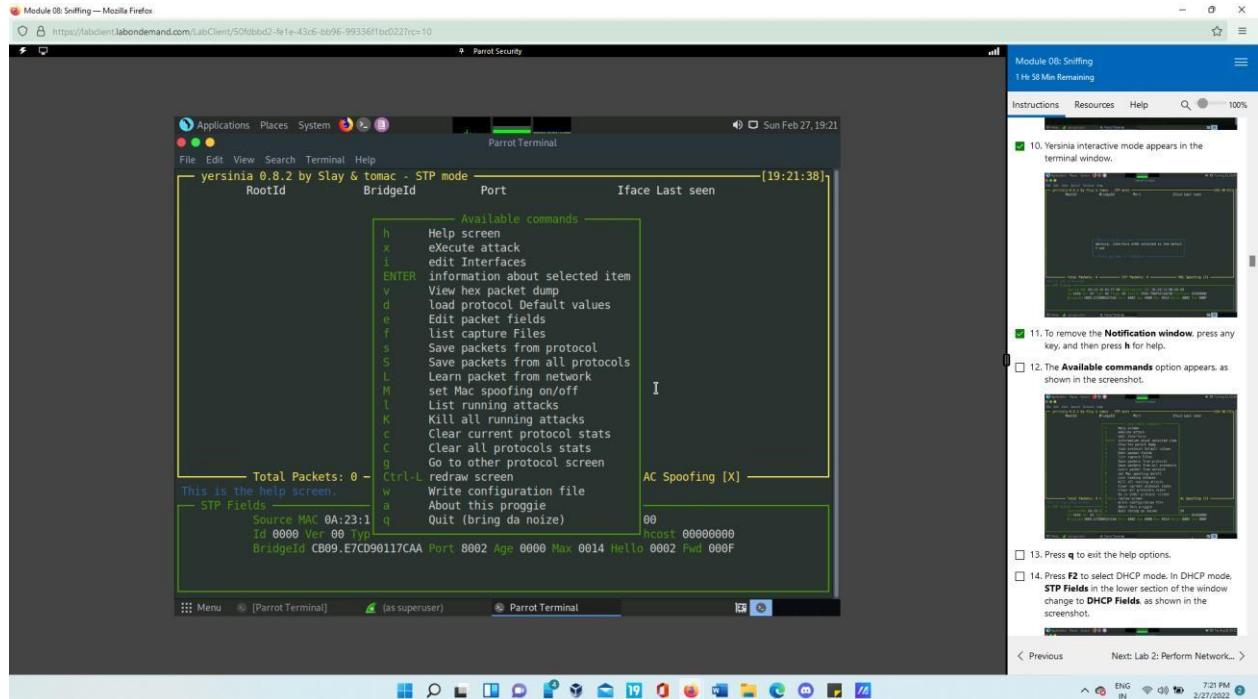


- Obtain Sudo privileges and go to root directory

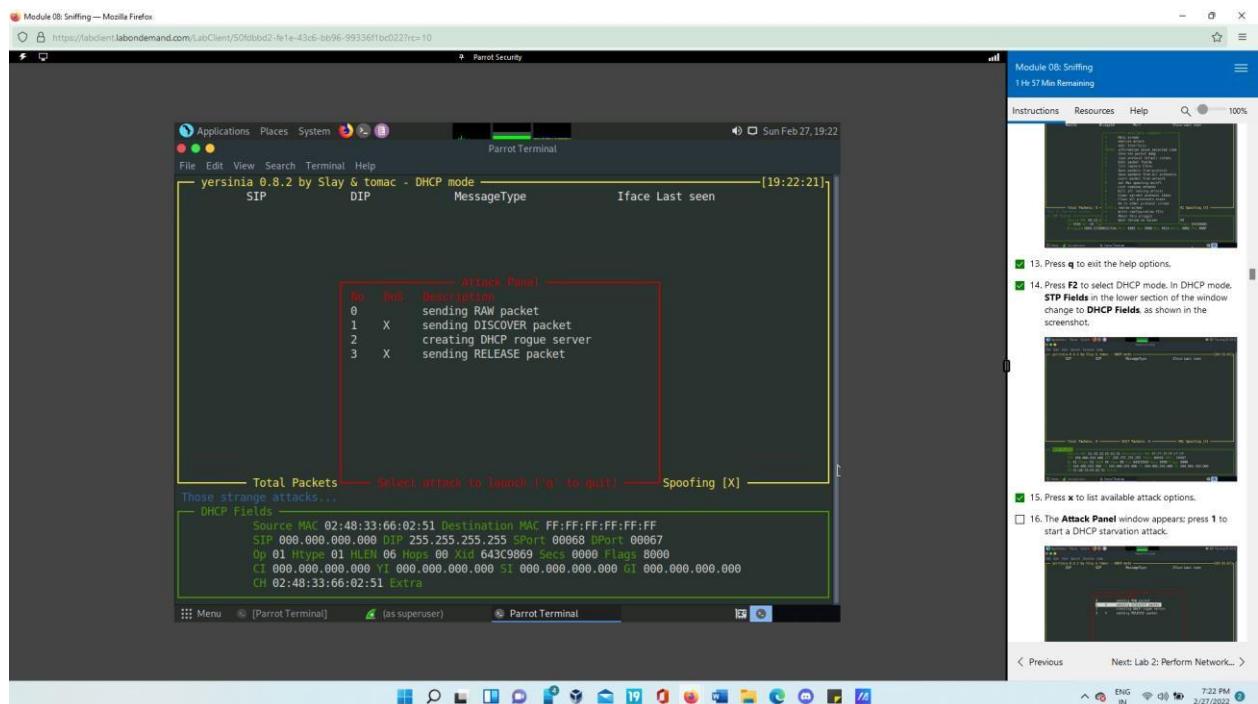
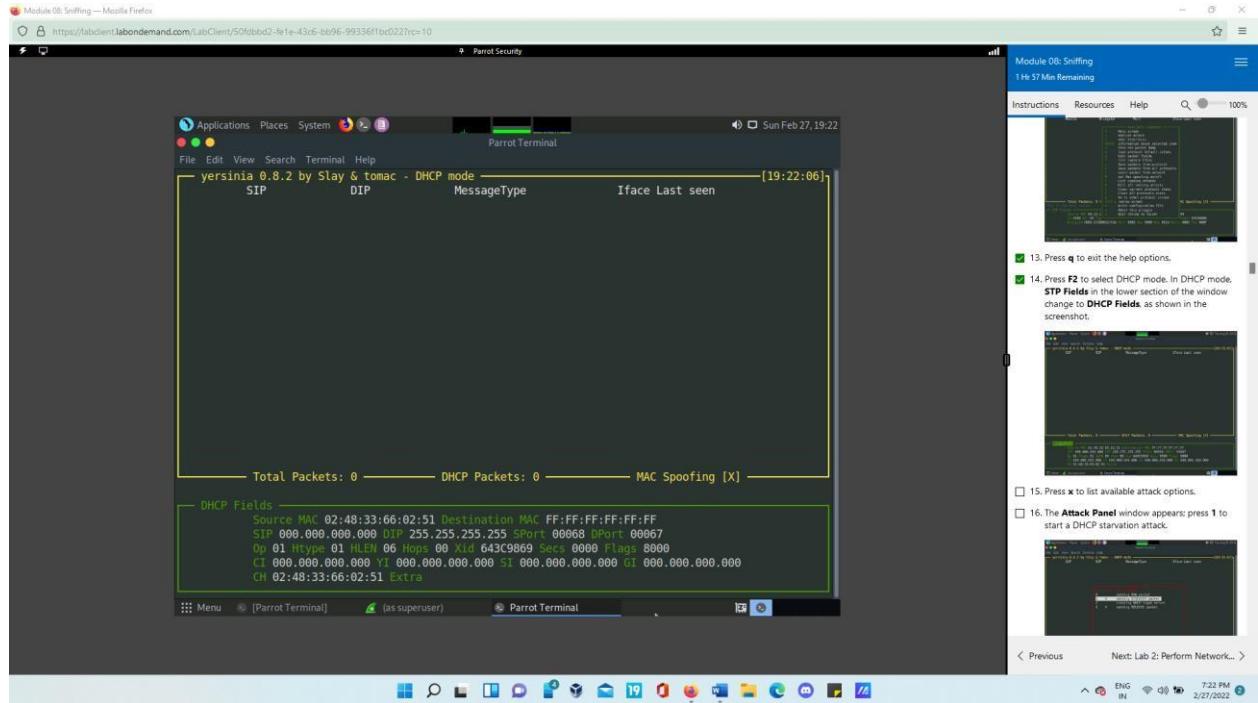


- To open Yersinia in interactive mode type yersinia -l and enter. Press q to exit from help options.

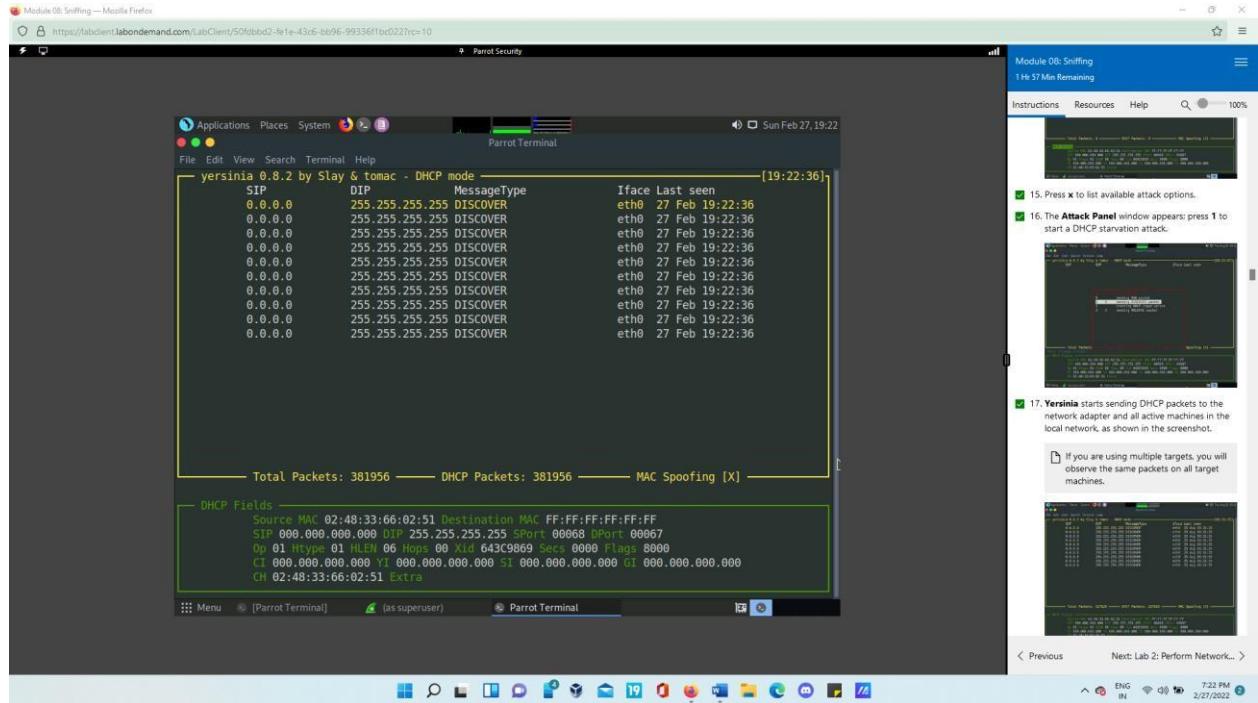




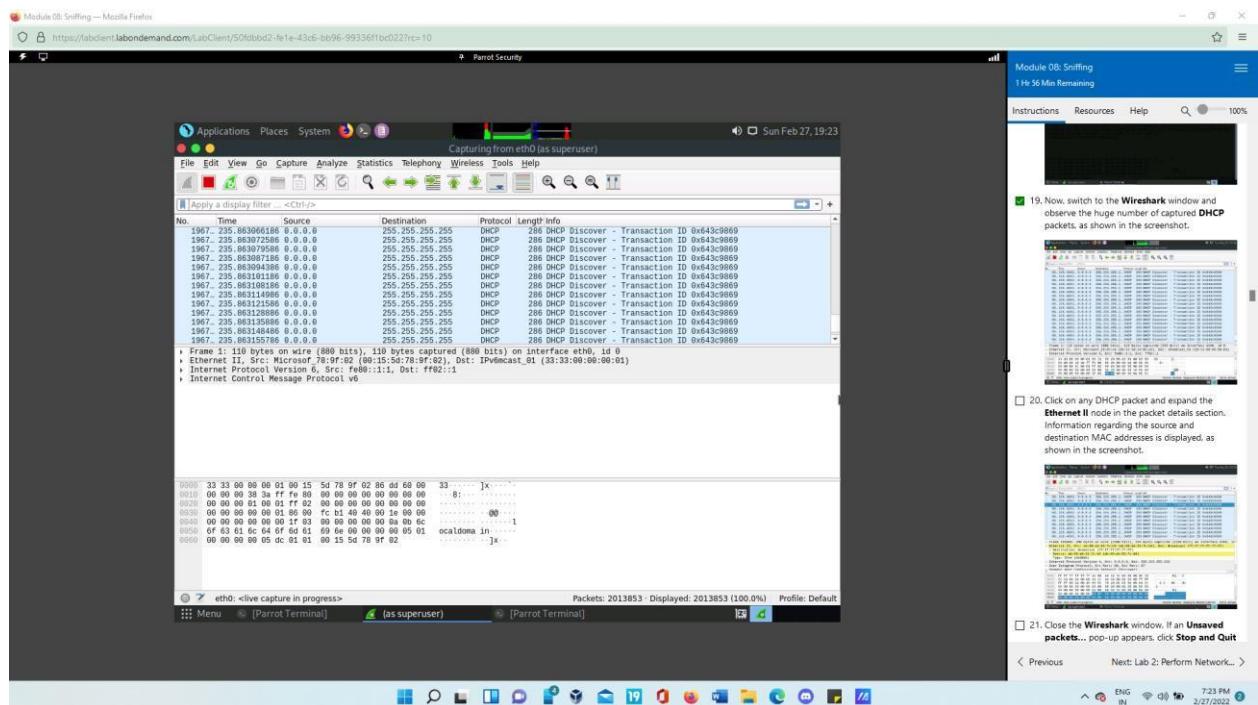
- Select DHCP mode by pressing F2. Now the STP fields will change to DHCP fields. To see a list of available attack options, press x.



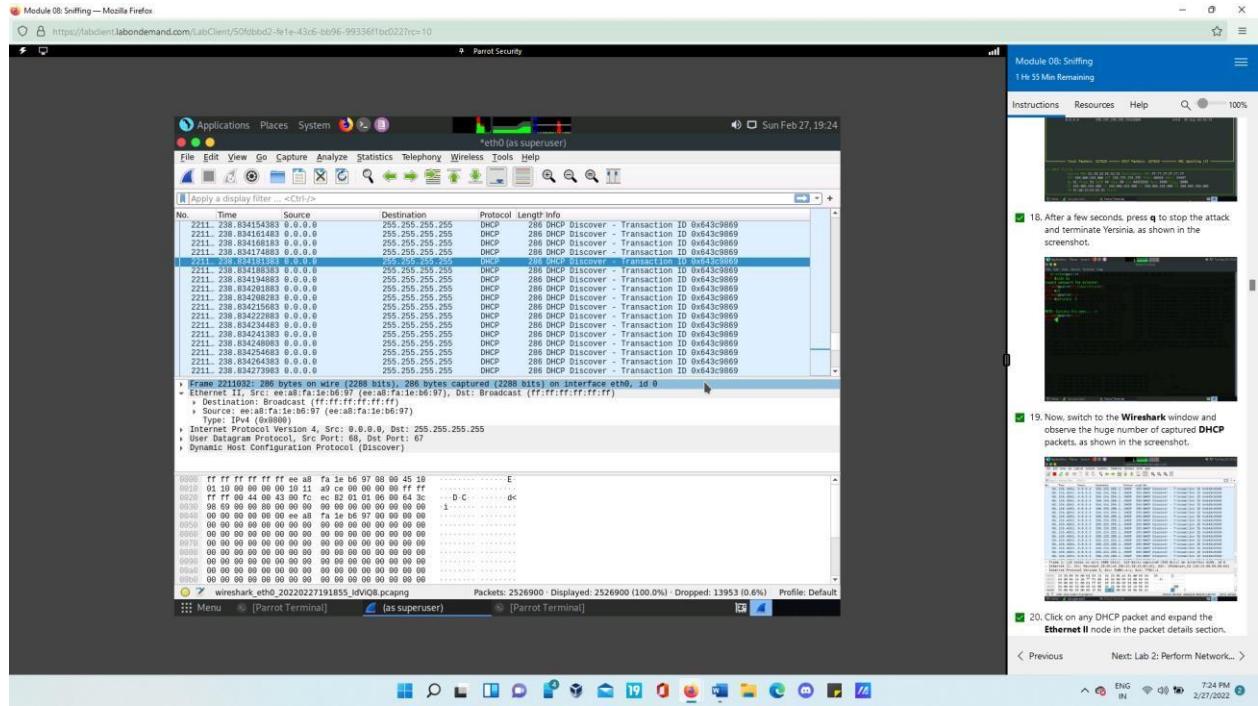
- Press **1** to launch a DHCP starvation attack in the Attack Panel window.



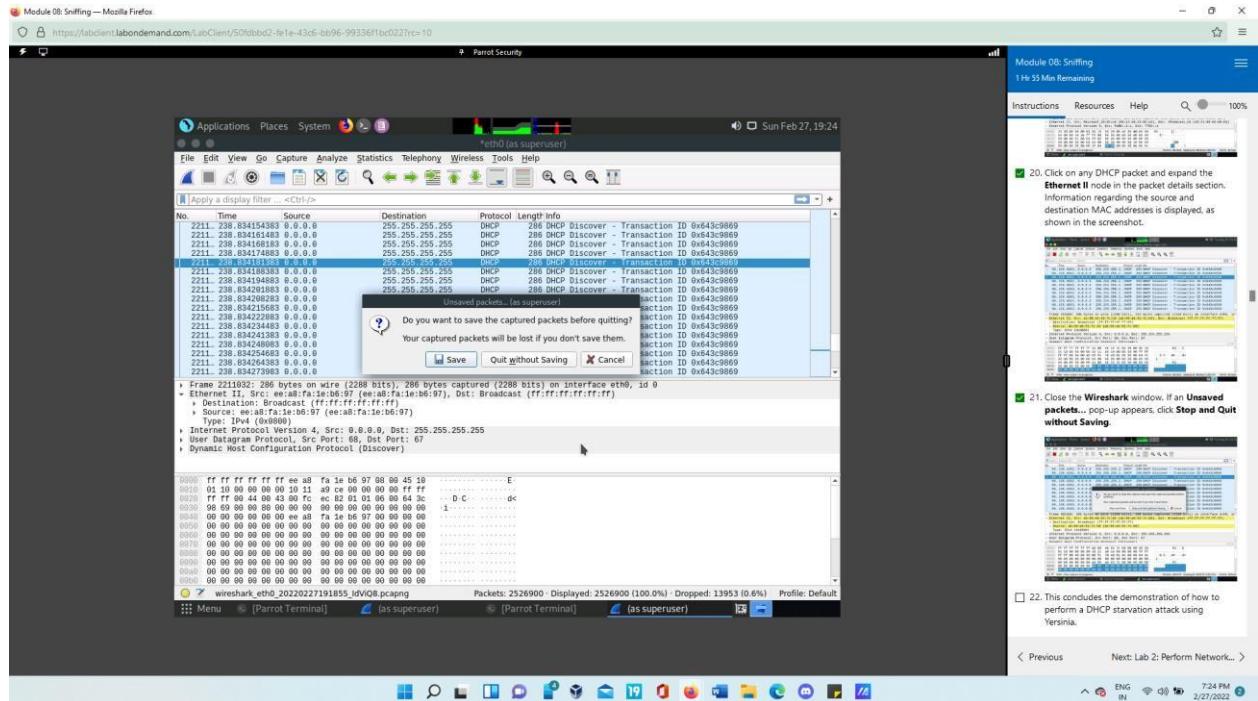
- Yersinia begins to transmit DHCP packets to the network adapter as well as all active machines in the local network. After some time, press **q** to terminate the attack and shutdown Yersinia.
- Now go back to Wireshark to observe large amount of DHCP packets.



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

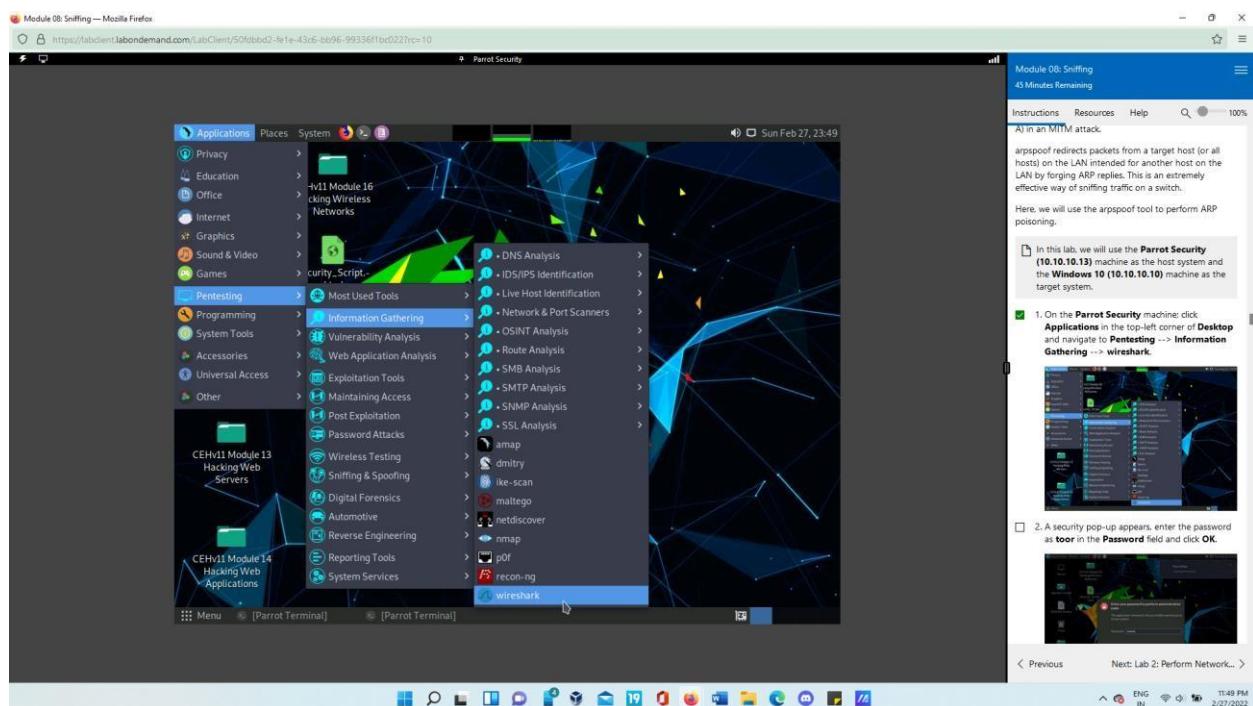


- Now close the Wireshark window.

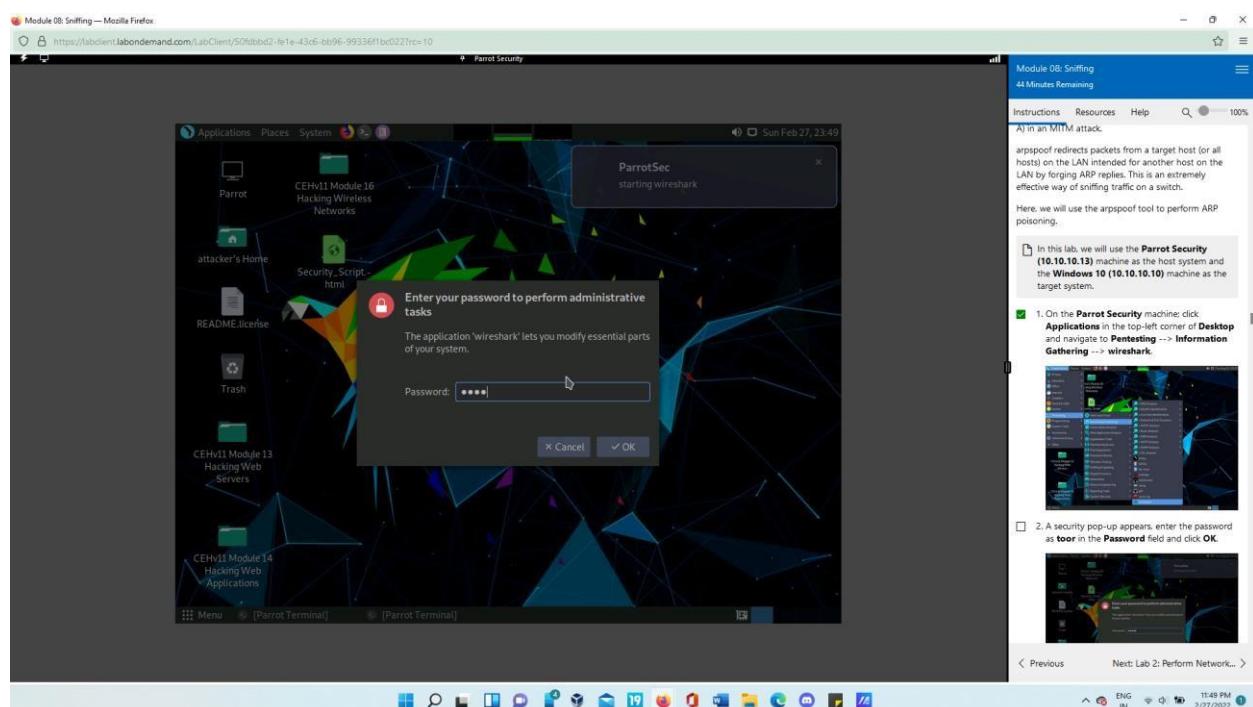


Task 3: Perform ARP Poisoning using Arp spoof

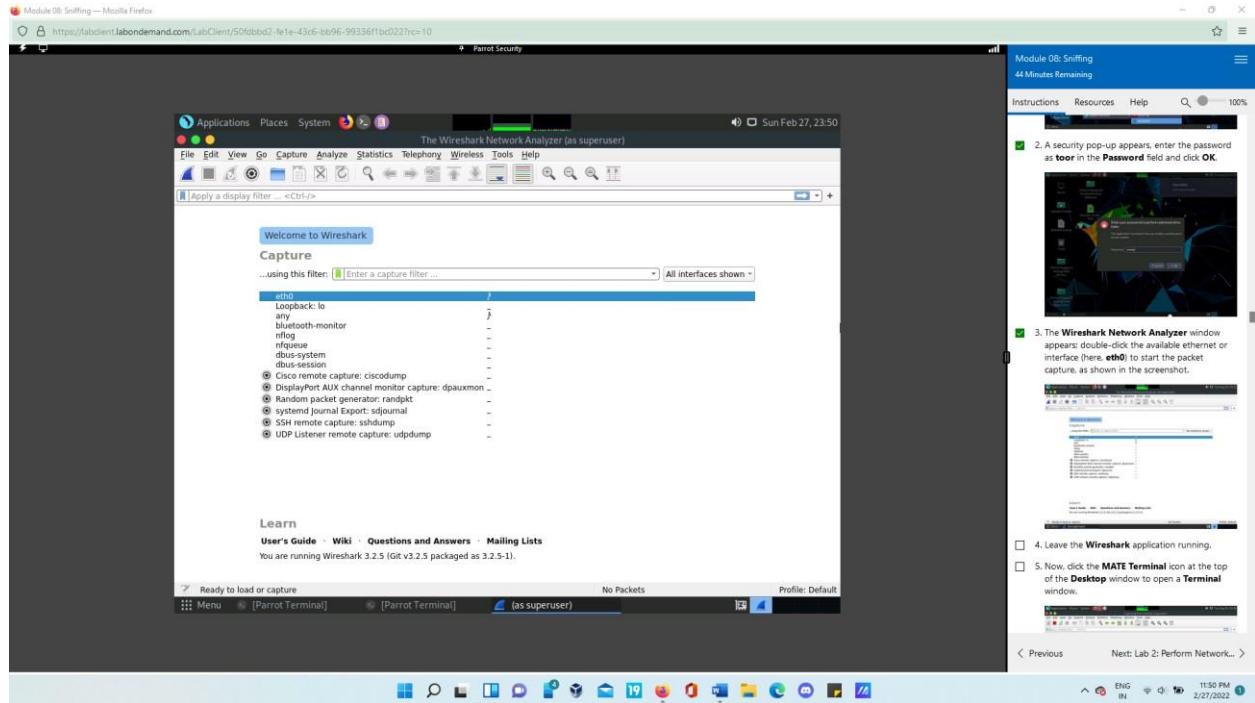
- Open Wireshark by navigating from the applications drop down menu.



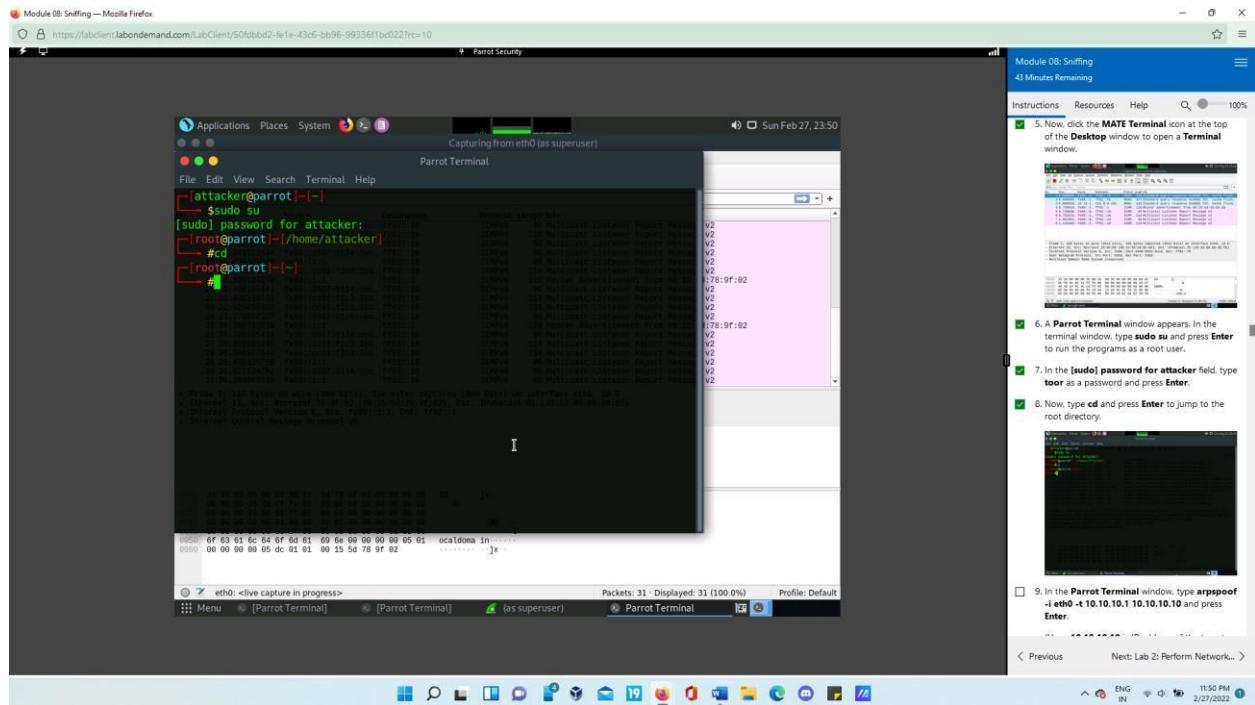
- Type password as toor and open Wireshark



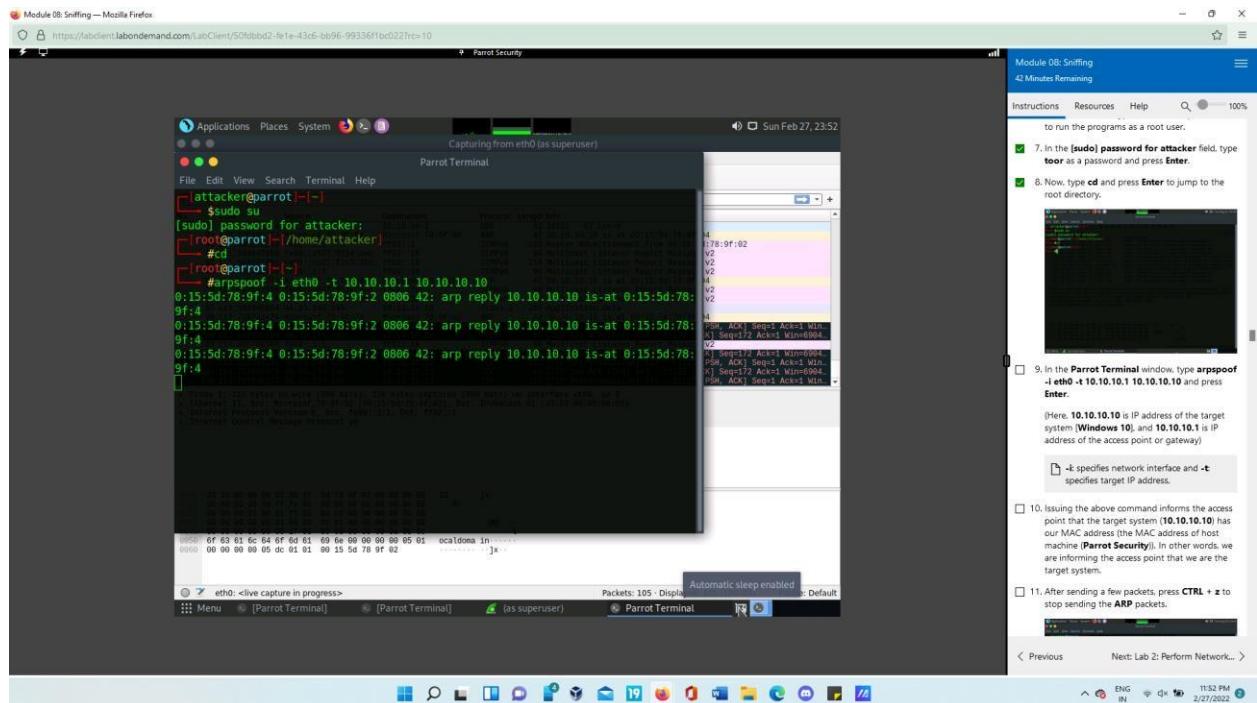
- Wireshark Network Analyzer opens and select Ethernet/eth0 to start packet capture.



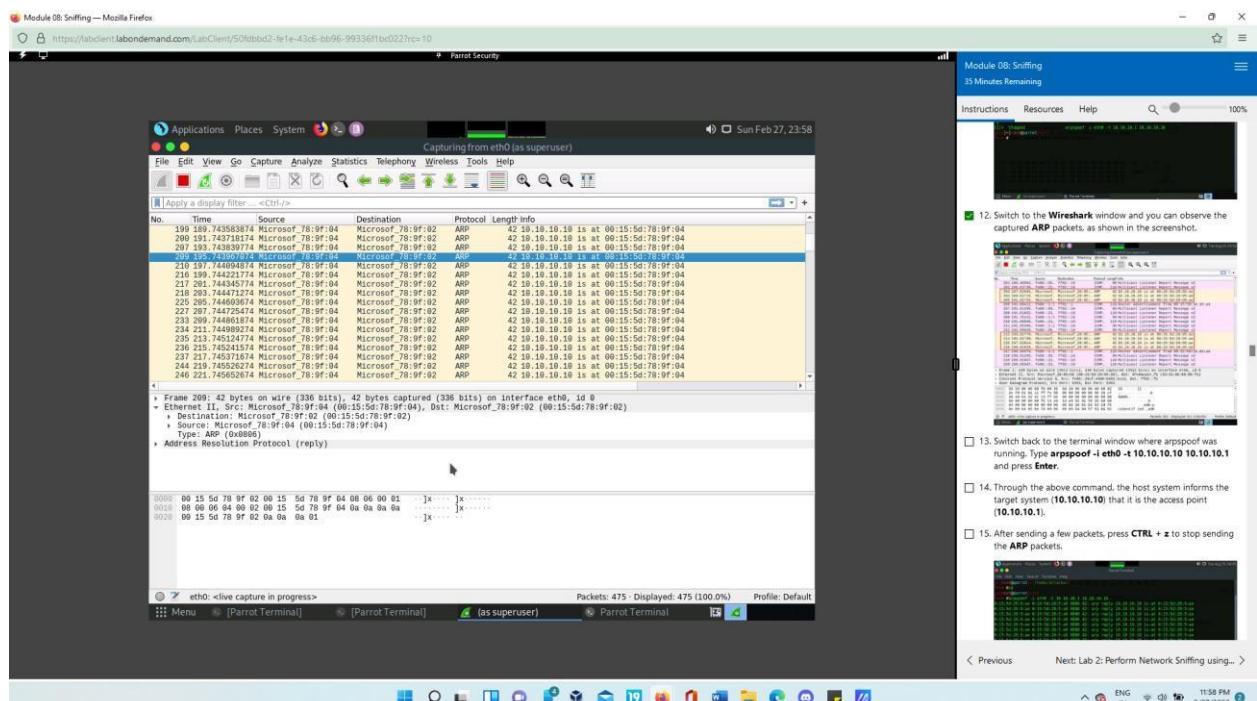
- In Mate terminal, obtain Sudo privileges and go to root directory.



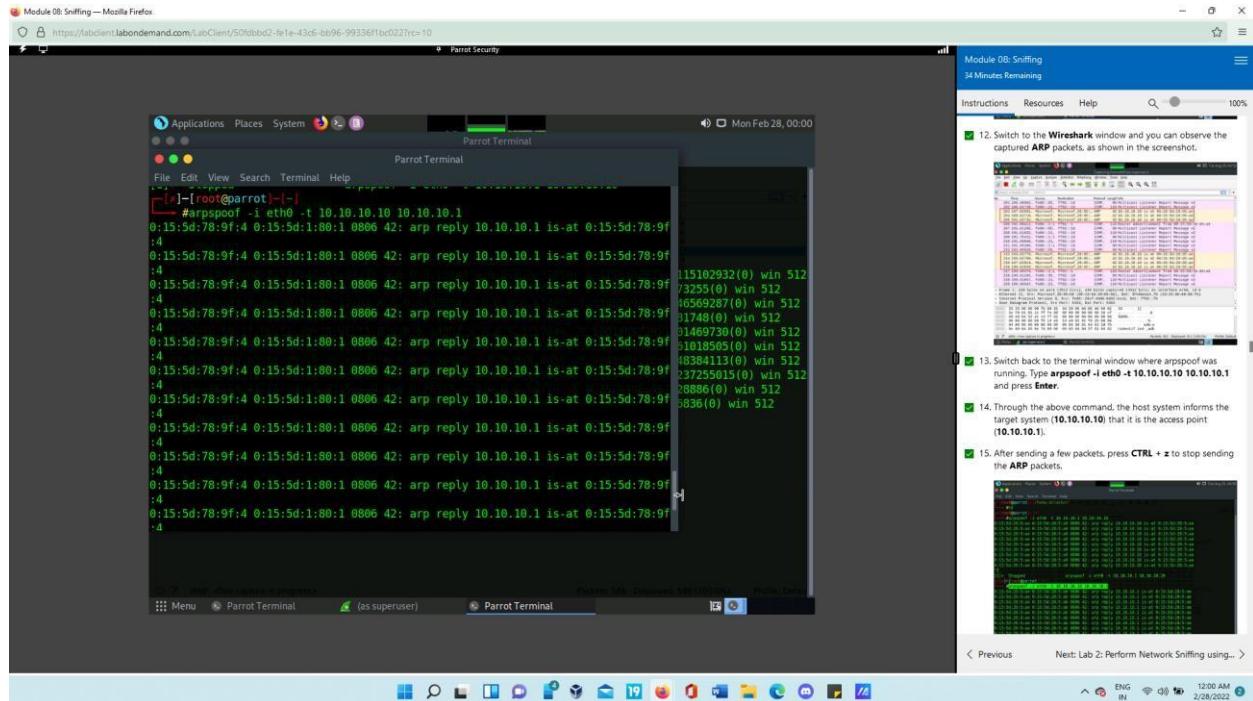
- Now in the terminal, type the command arpspoof -i eth0 -t 10.10.10.1 10.10.10.10 to send ARP packets, after few packets has been sent abort it by pressin ctrl+z.



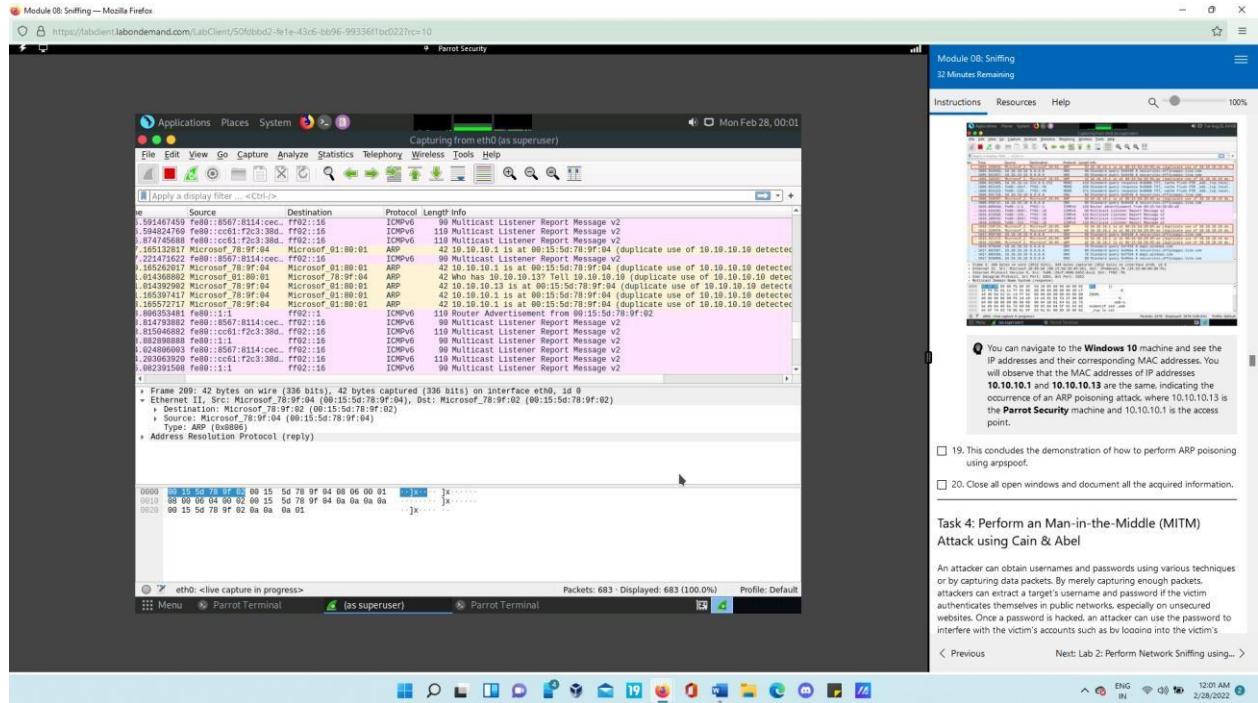
- Now go back to Wireshark to observe the ARP packets.



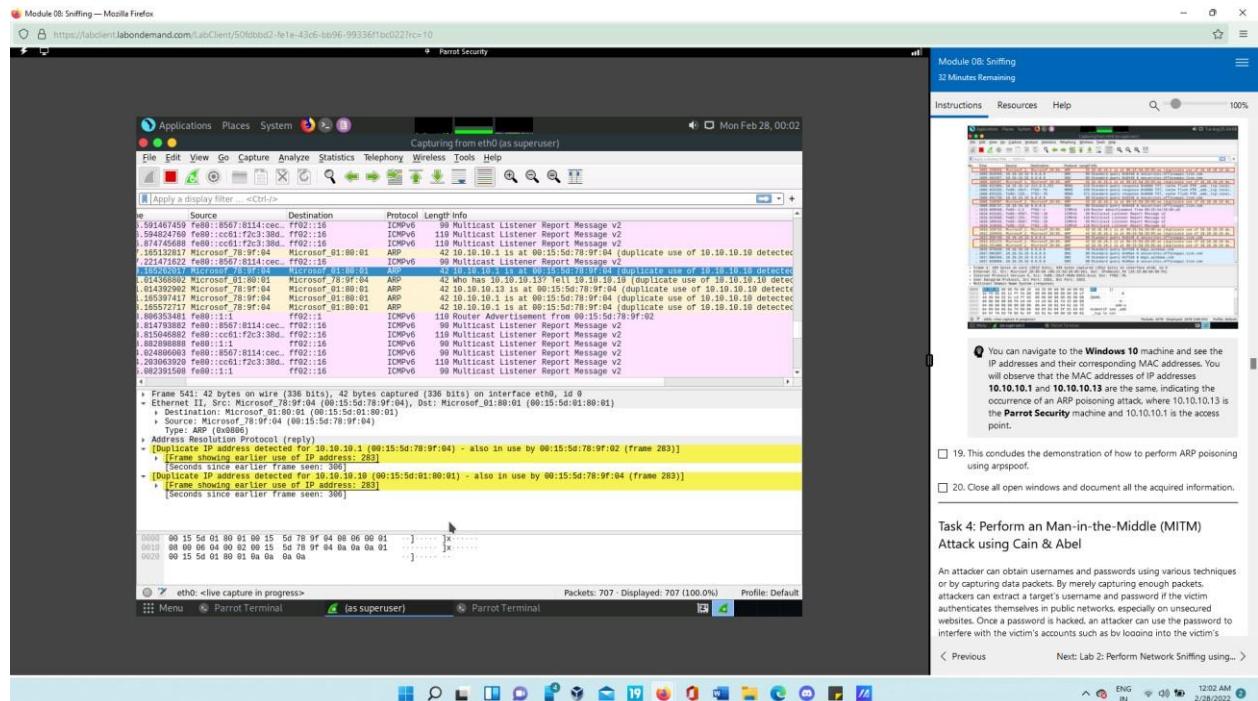
- Now switch back to terminal and type arpspoof -i eth0 -t 10.10.10.10 10.10.10.1. After sending few packets abort it by pressing ctrl+z.



- 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.

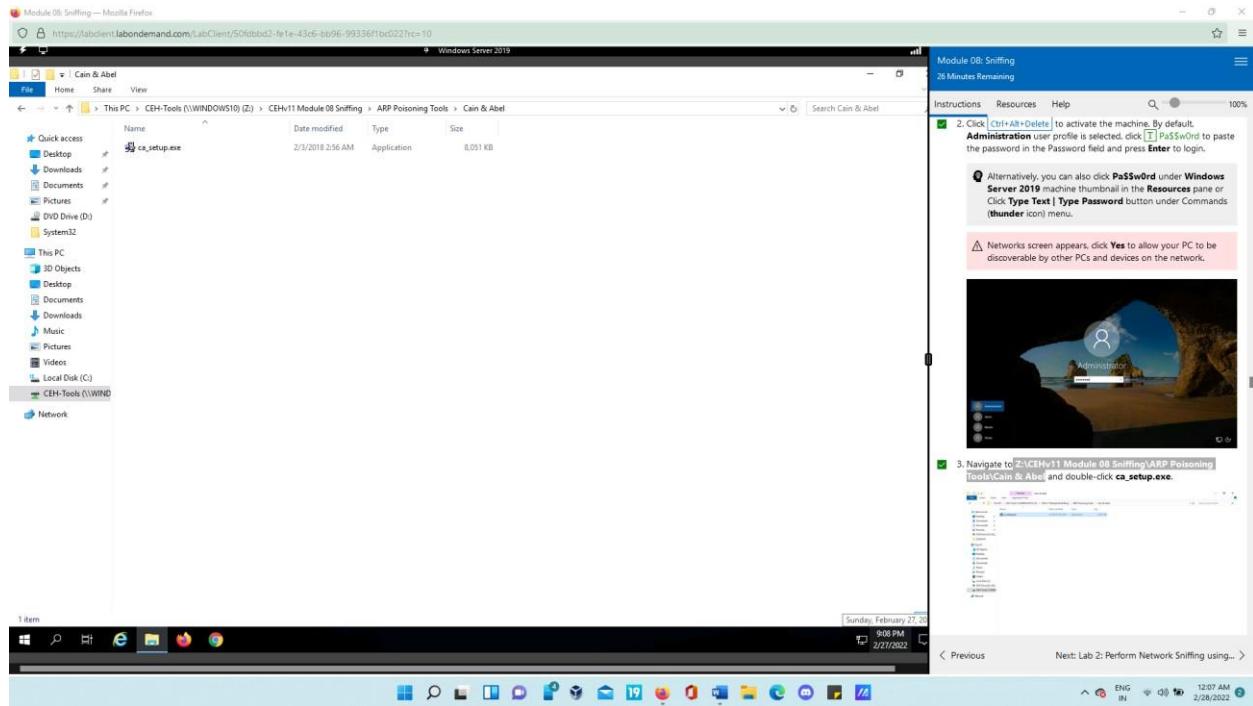


- Hence by using arpspoof, we assigned the MAC address of the host machine to the target machine and access point. Thereby, alert warning for a duplicate use of 10.10.10.10 was displayed.

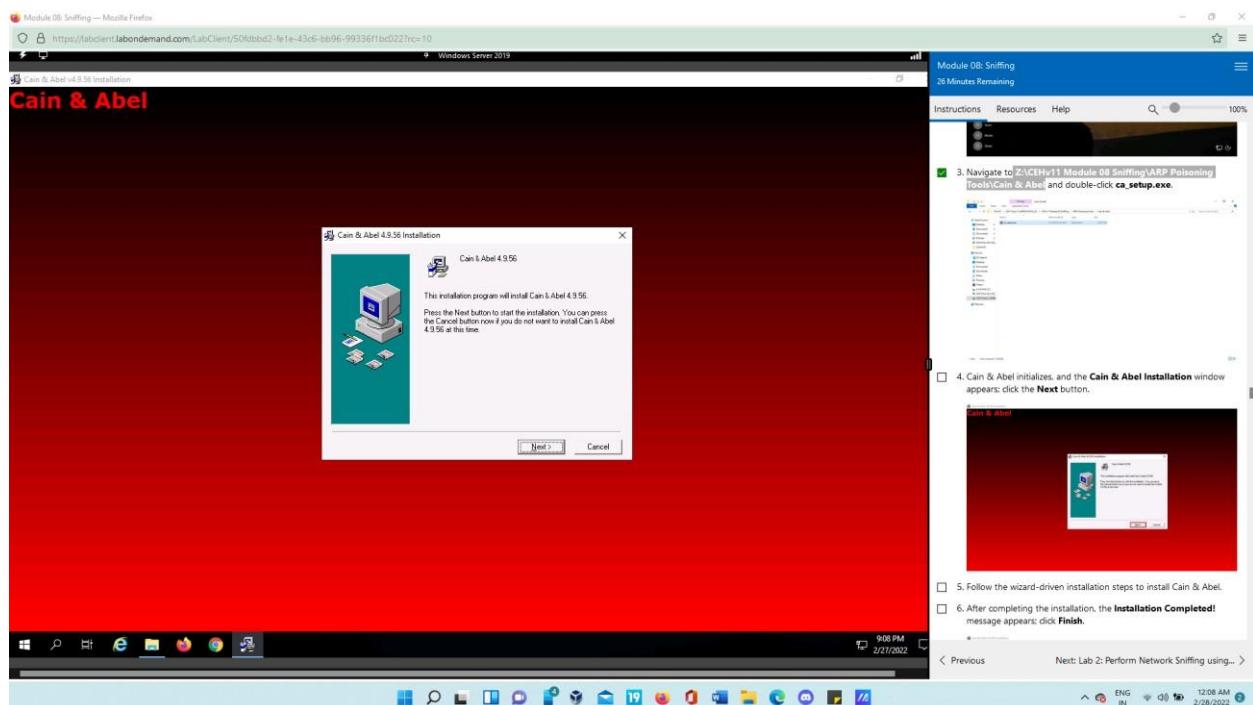


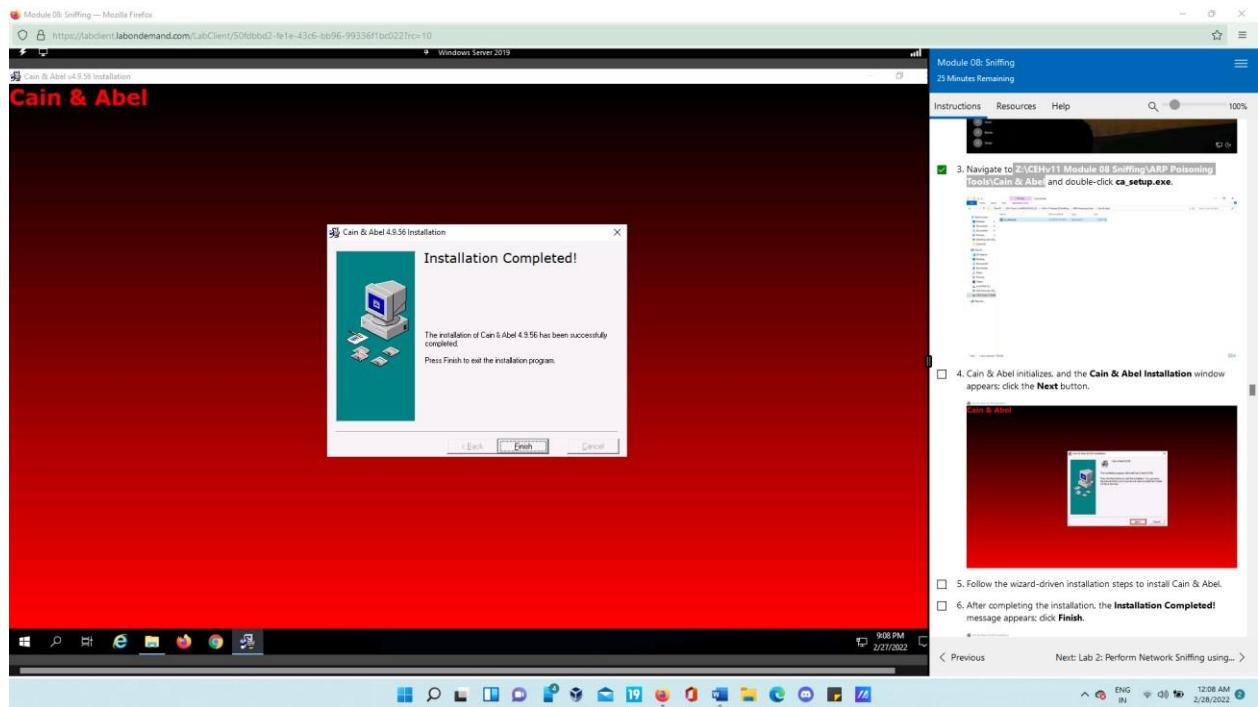
Task 4: Perform a Man-in-the-Middle (MITM) Attack using Cain & Abel

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

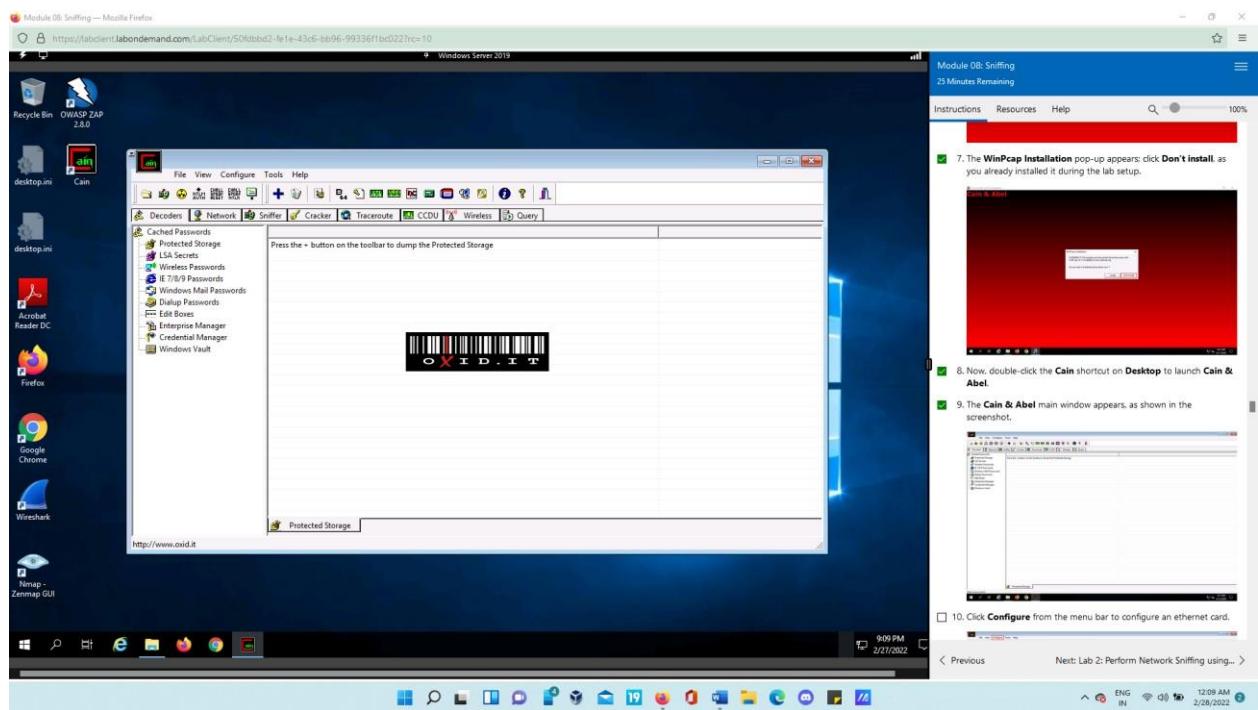


- Installation starts and by clicking next and accepting terms, complete the installation process.

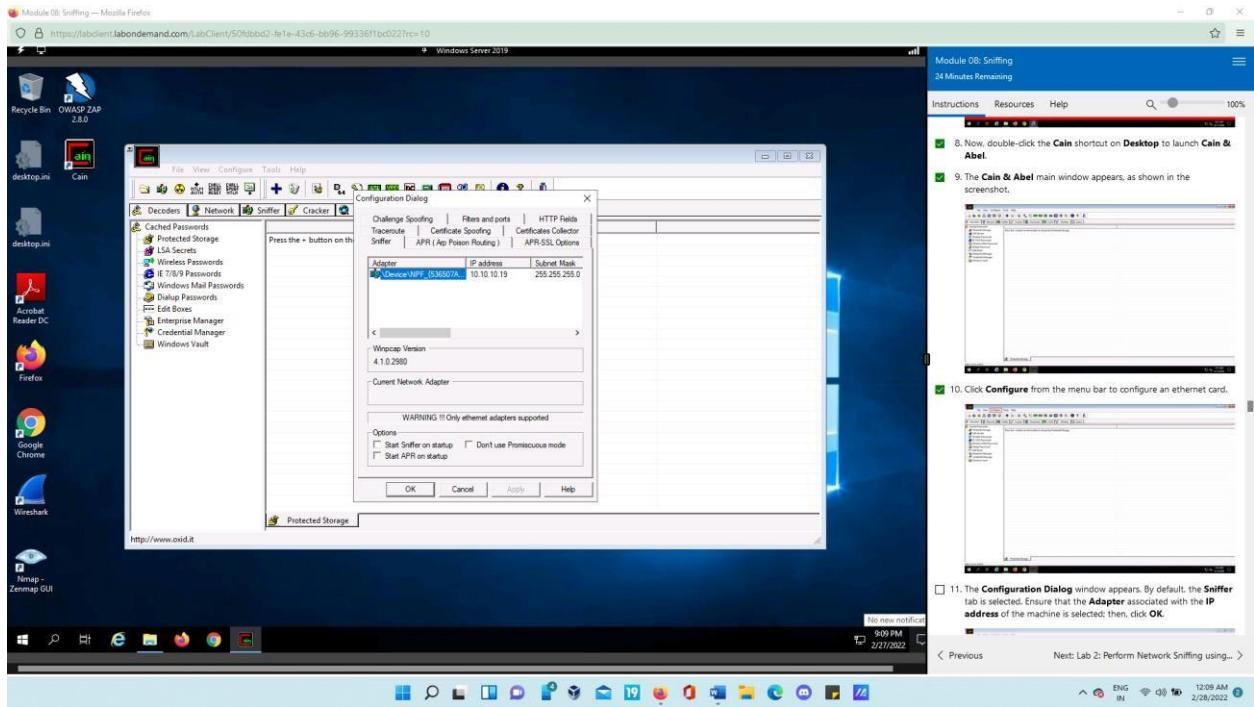




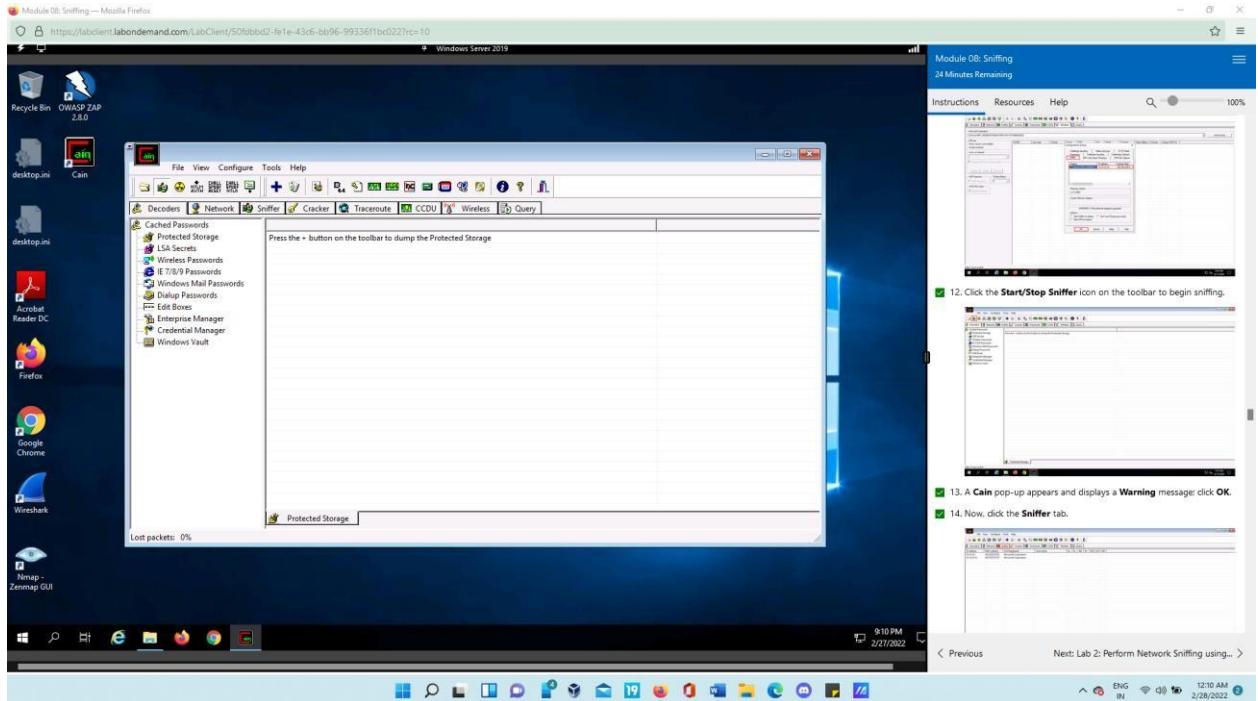
- In main window, click configure button to configure menu bar.



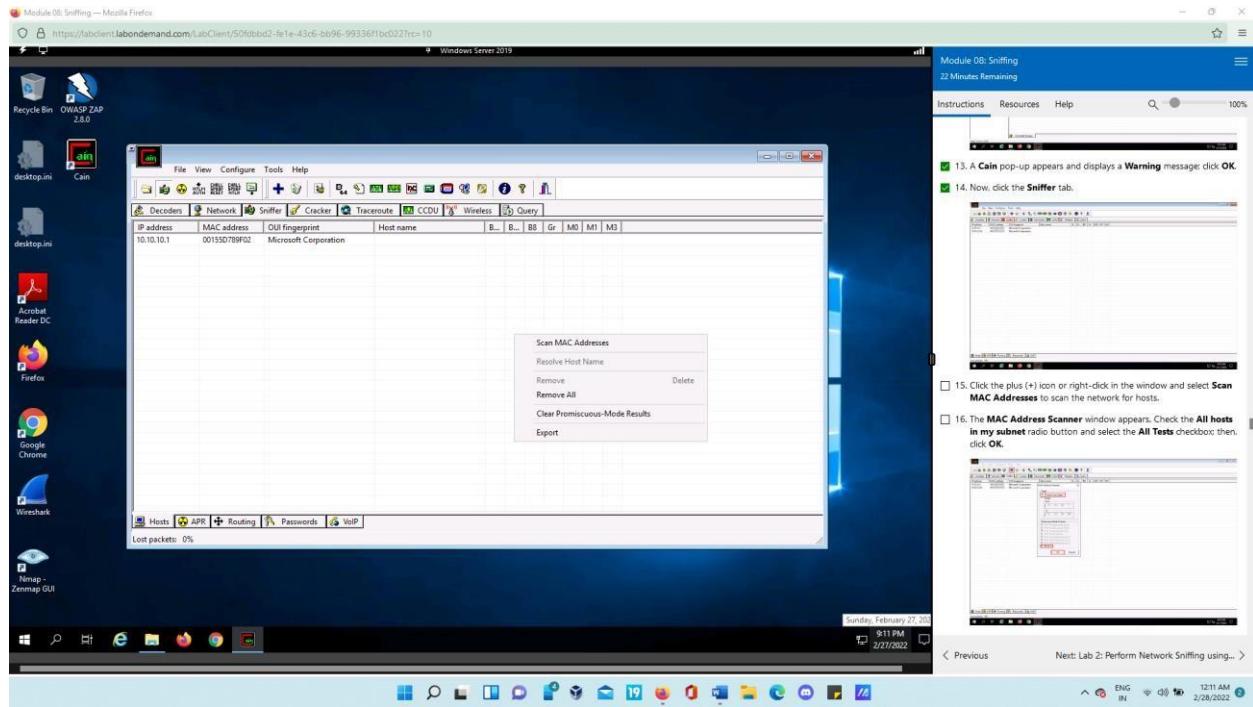
Configuration Dialog window opens, now by default Sniffer tab will be selected. We must make sure that the Adapter associated with the IP address of the machine is selected, then press ok.



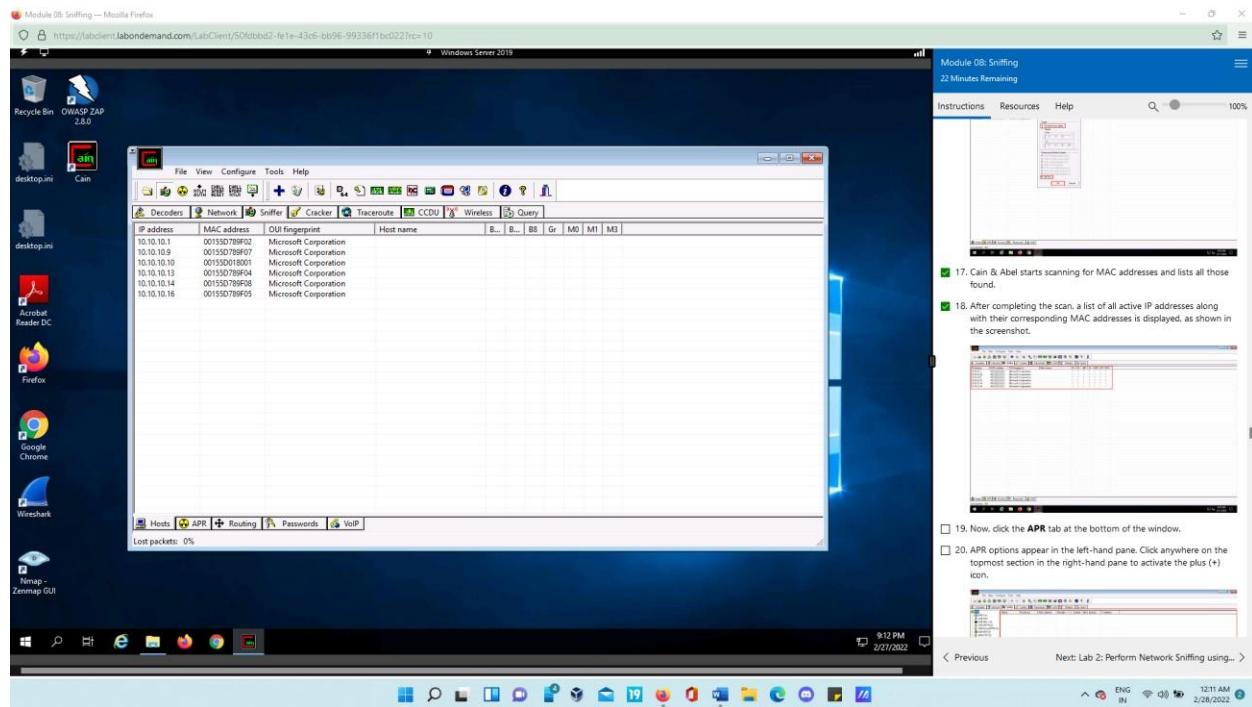
- To start sniffing, press start/stop sniffer button.



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

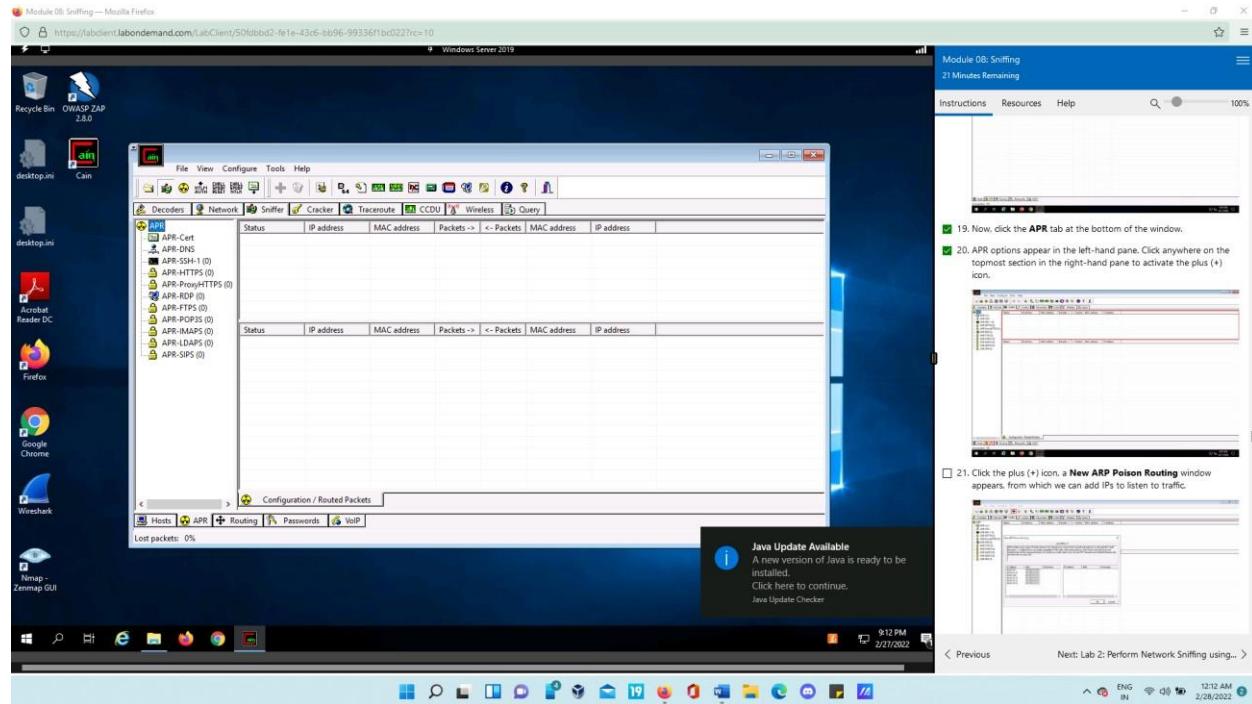


- Now MAC address scanner dialog box opens. Here, check all hosts in my subnet radio button, then press ok. Cain & Abel starts scanning for MAC addresses. When the scan is completed, all the active IP addresses and their MAC addresses are listed.

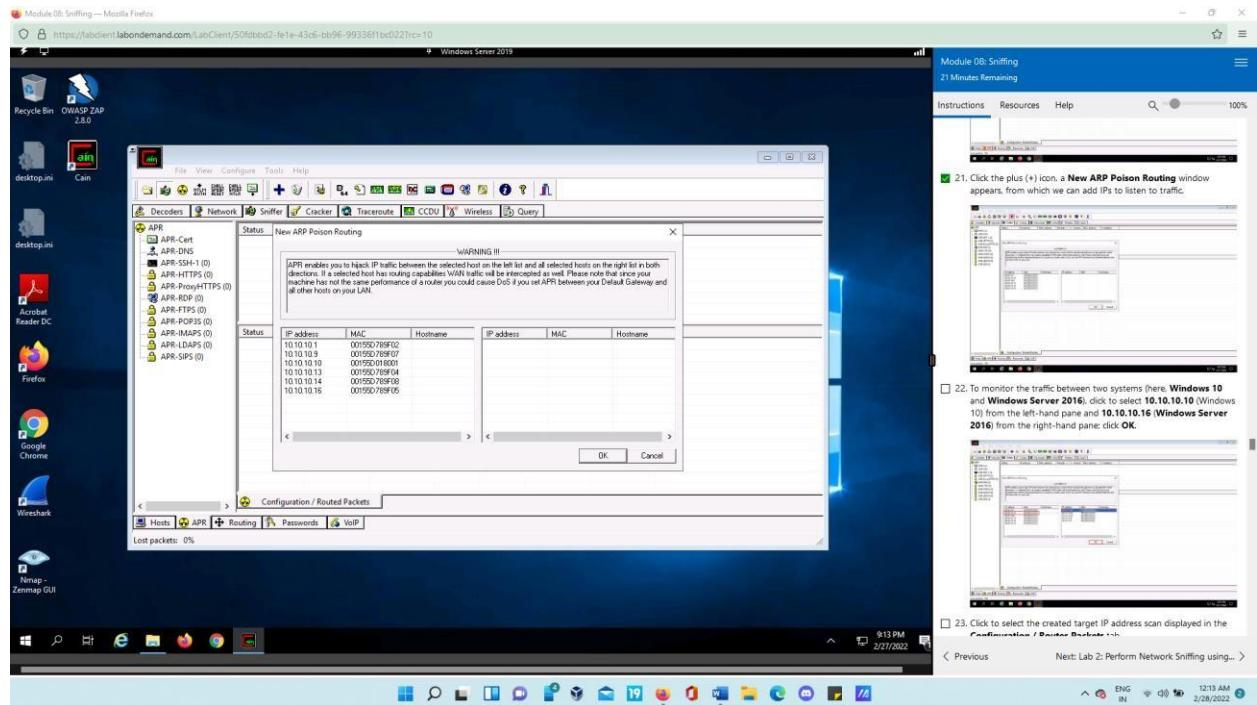


Now when you press APR button at the bottom of the window, APR options will appear.

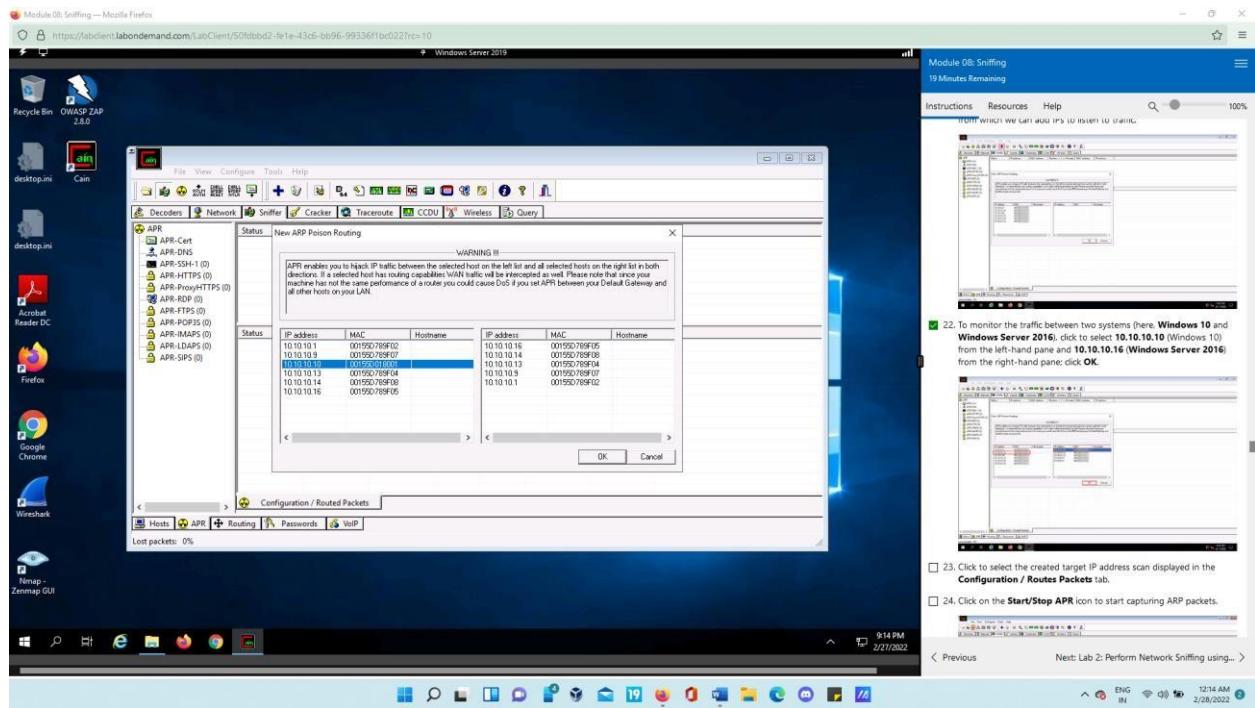
- Now, click the **APR** tab at the bottom of the window. APR options appear in the left-hand pane.



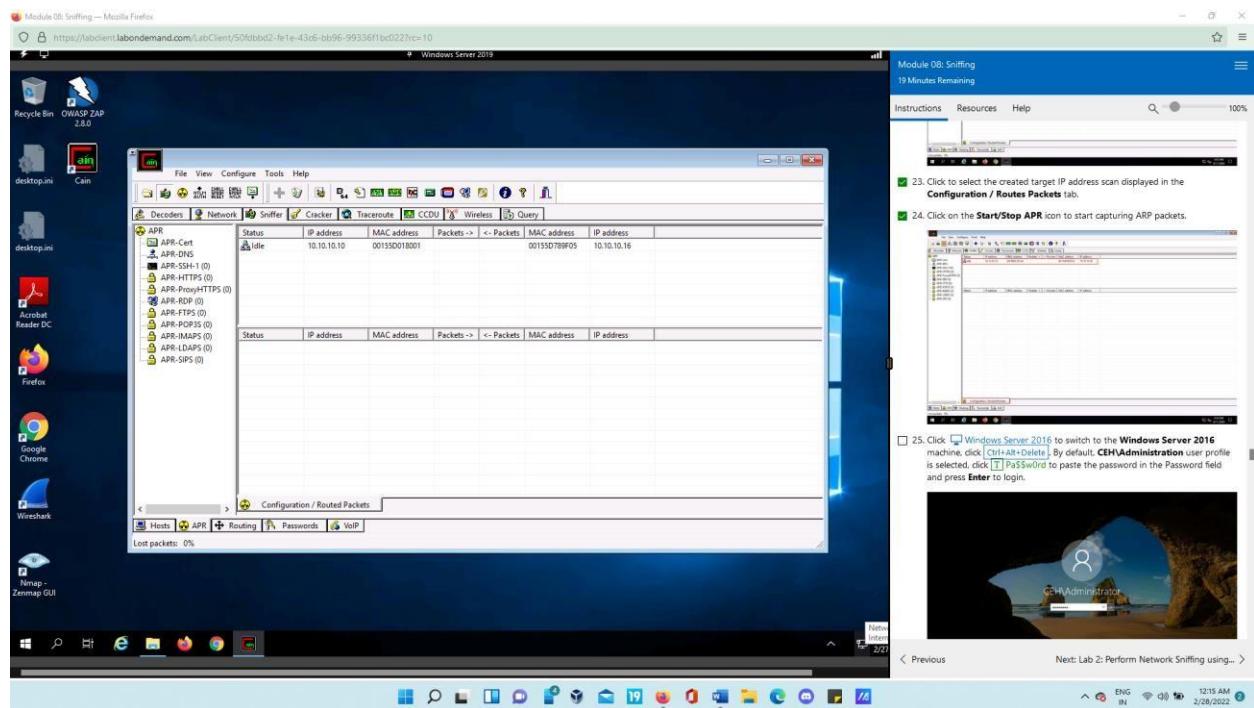
- Now press + icon, so that a new ARP poison routing window appears, from that we can add IPs to listen network traffic.



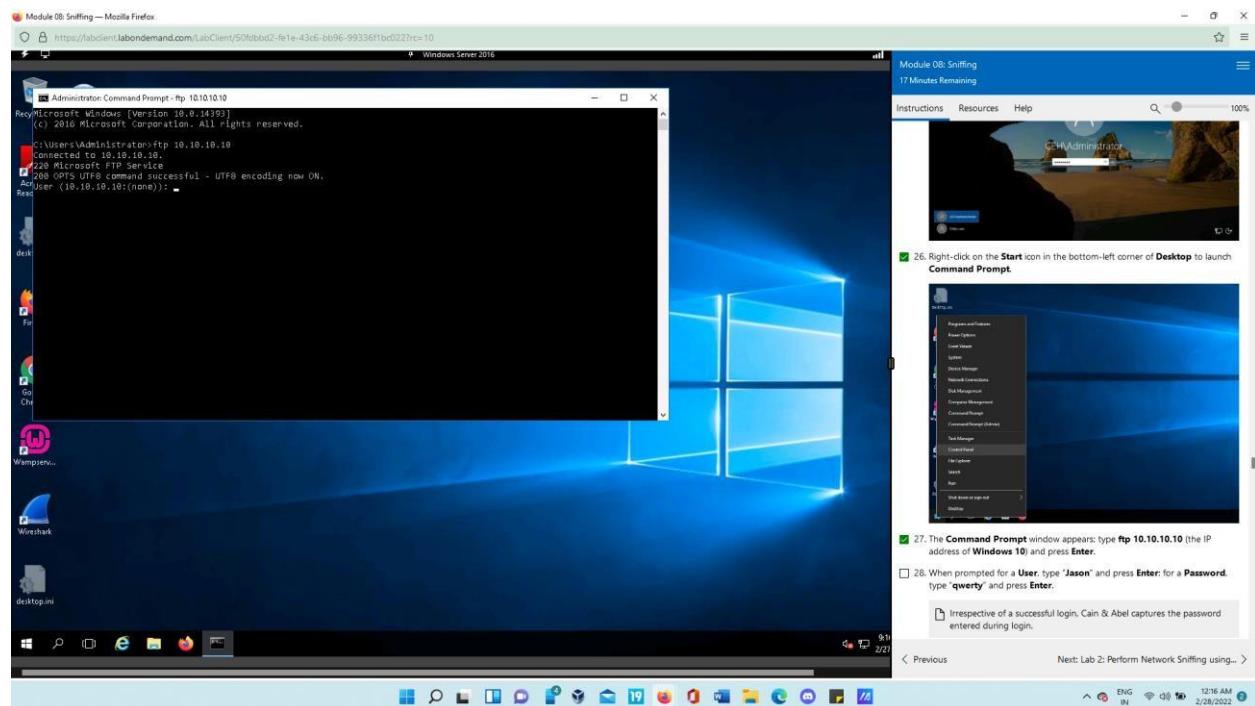
- Click 10.10.10.10 from the left-hand pane to view traffic coming from windows 10 and windows server 2016, and from the right-hand pane select 10.10.10.16, which is windows server 2016, then press ok.



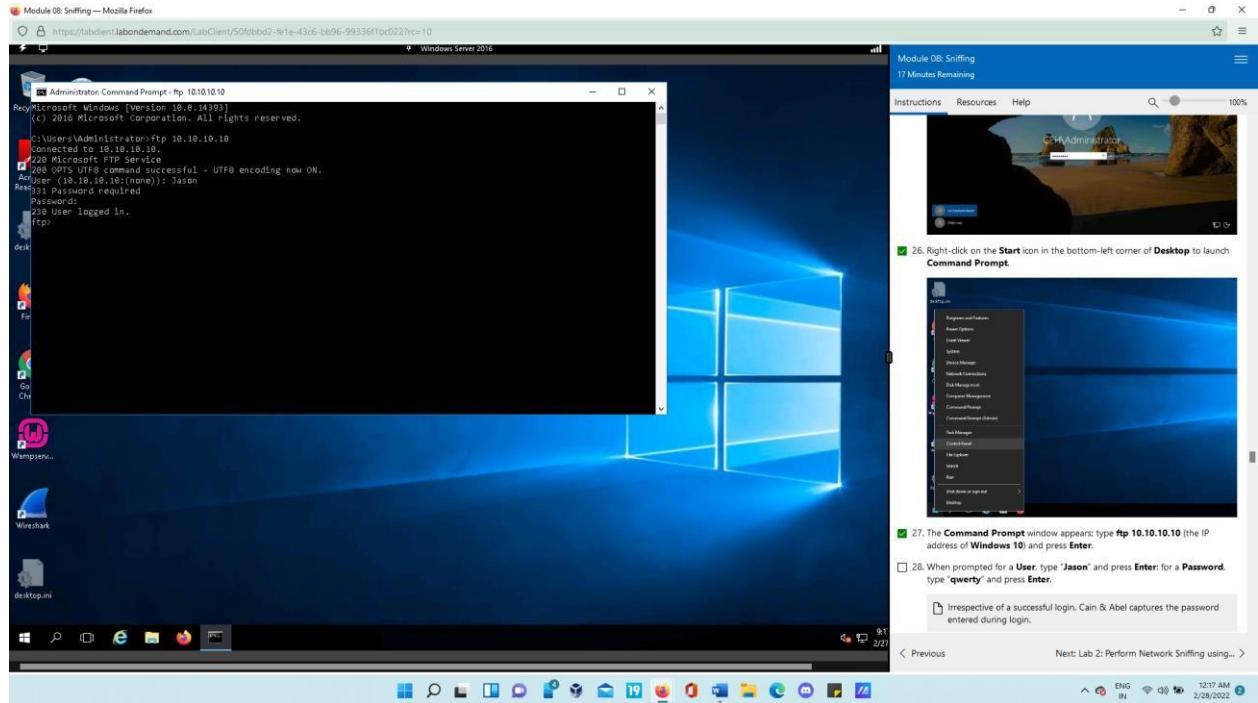
- Select the target IP address and start capturing ARP packets



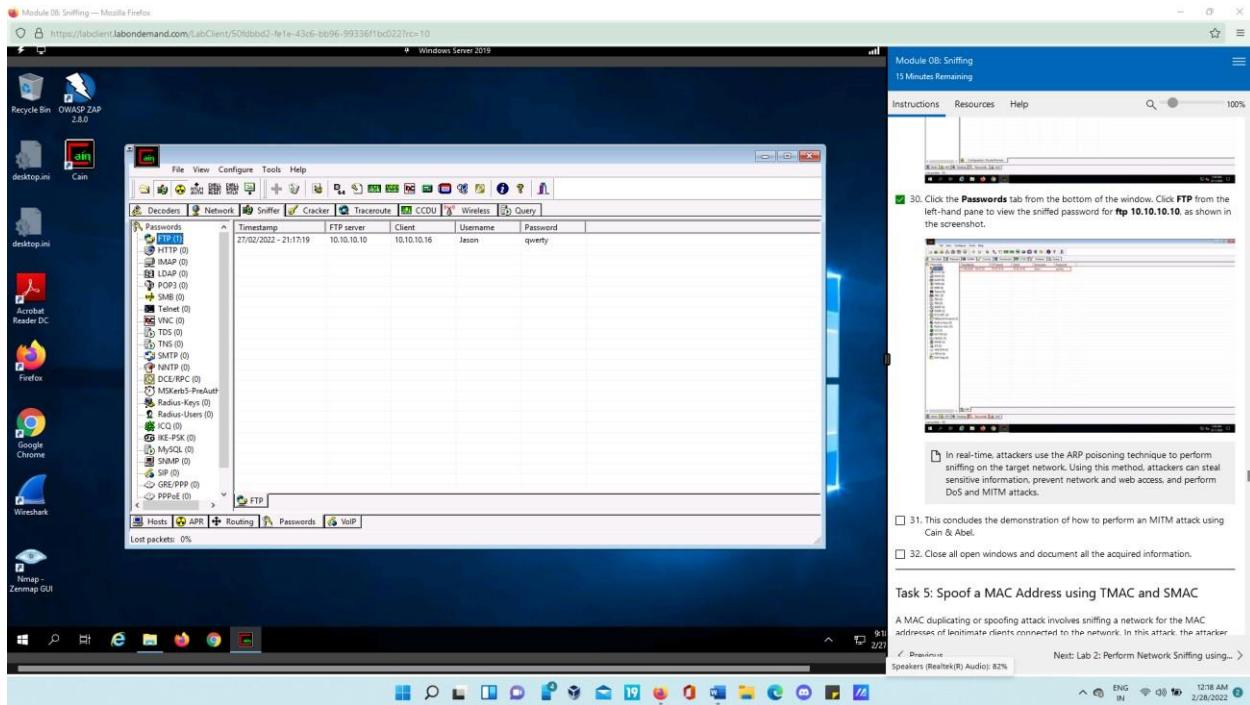
Now switch to Windows server 2016, and open command prompt. Then type `ftp 10.10.10.10`



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

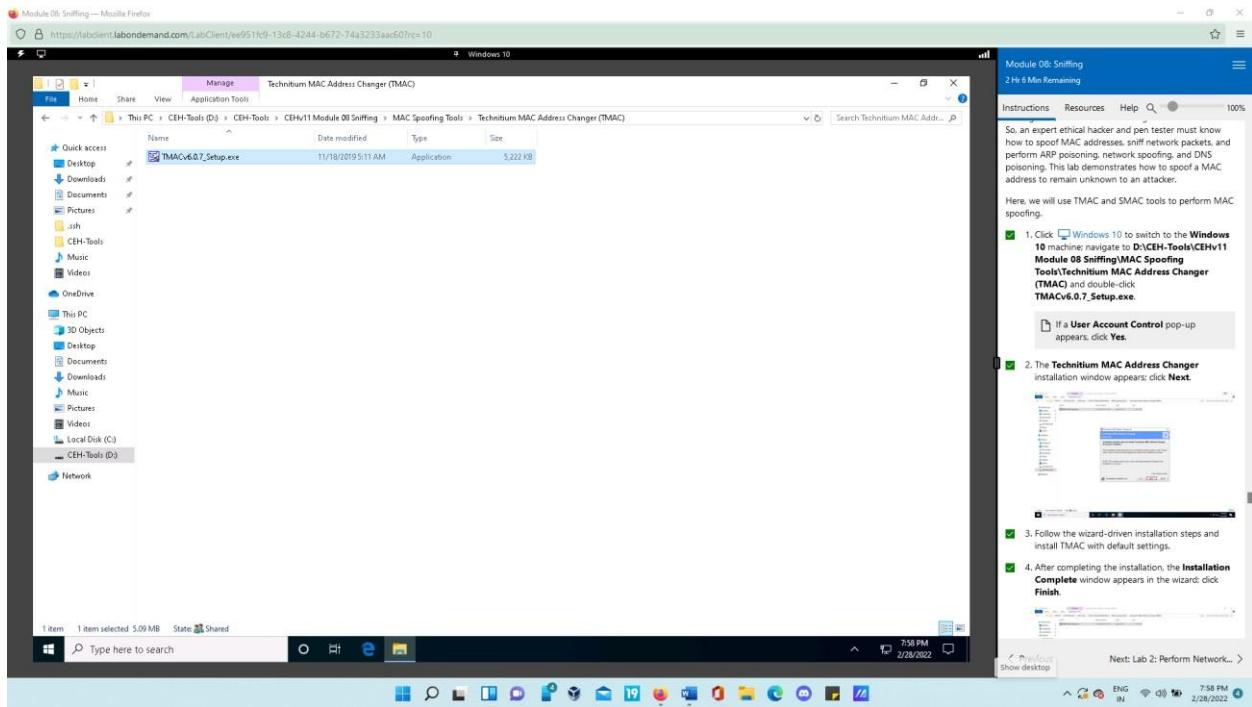


- Now go back to windows server 2019 and select FTP from the left-hand pane to observe the sniffed password for ftp 10.10.10.10.

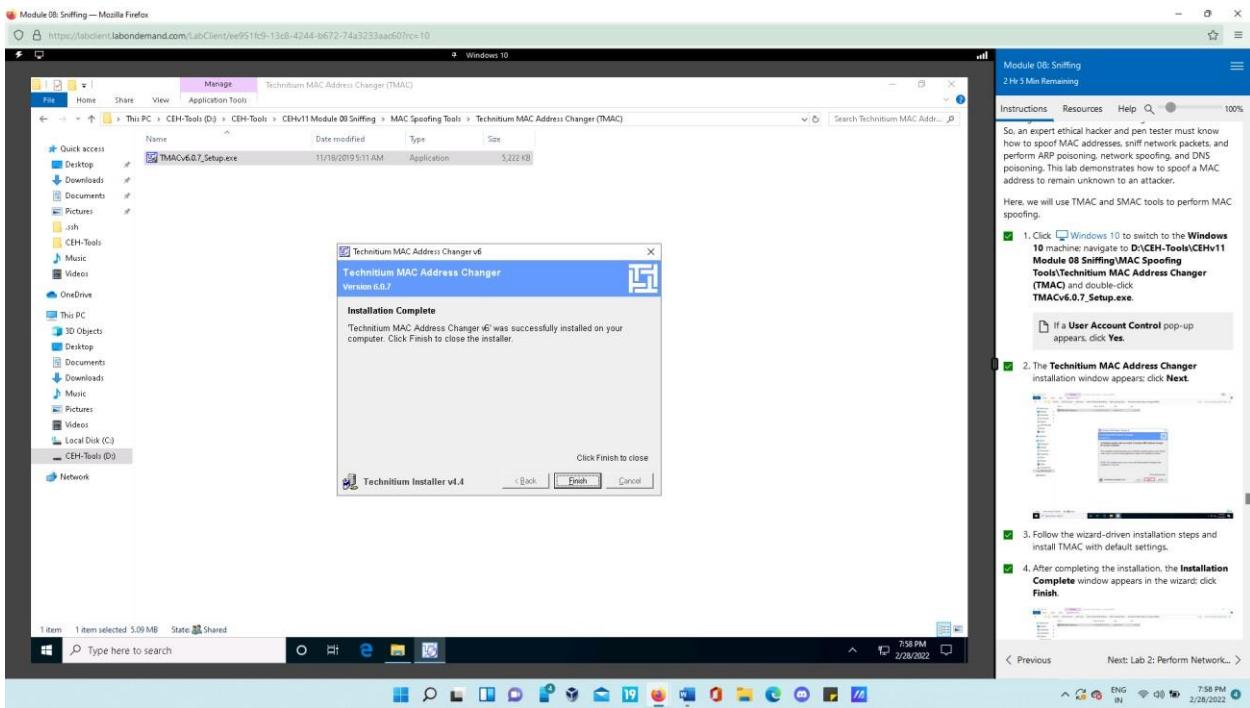


Task 5: Spoof a MAC Address using TMAC and SMAC

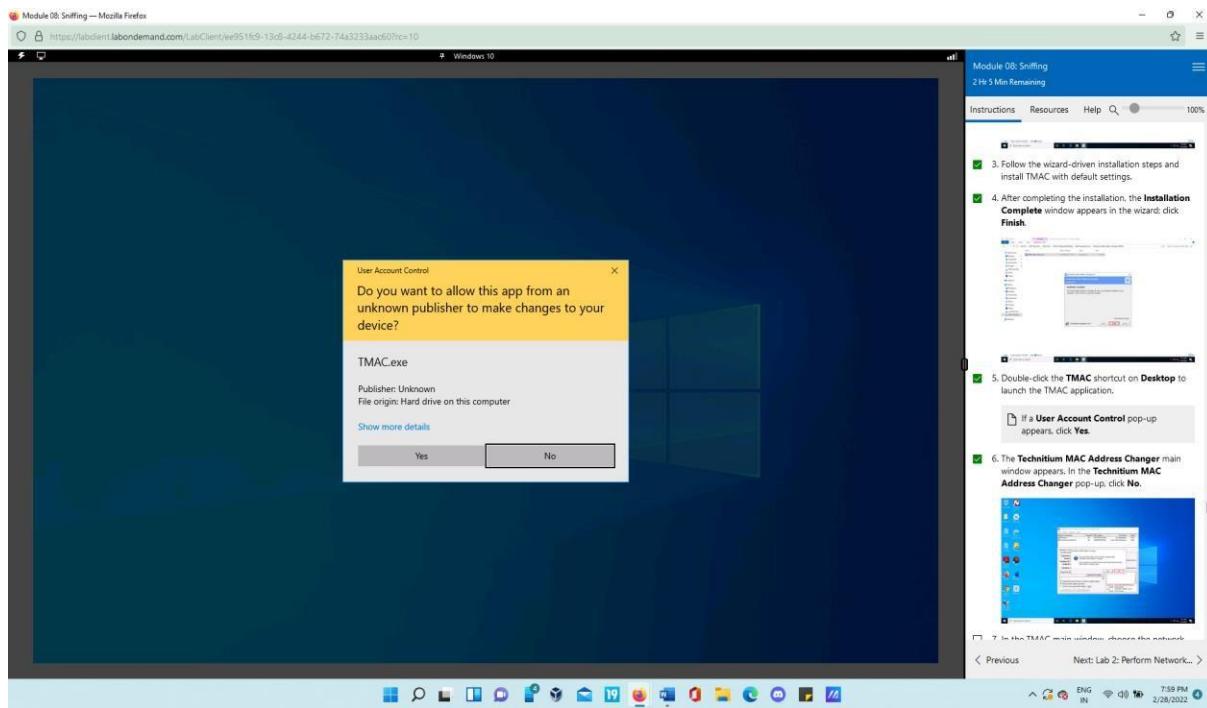
- Go to Windows10 machine, navigate to D:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC) and open file TMACv6.0.7_Setup.exe and install the Technitium MAC address changer.



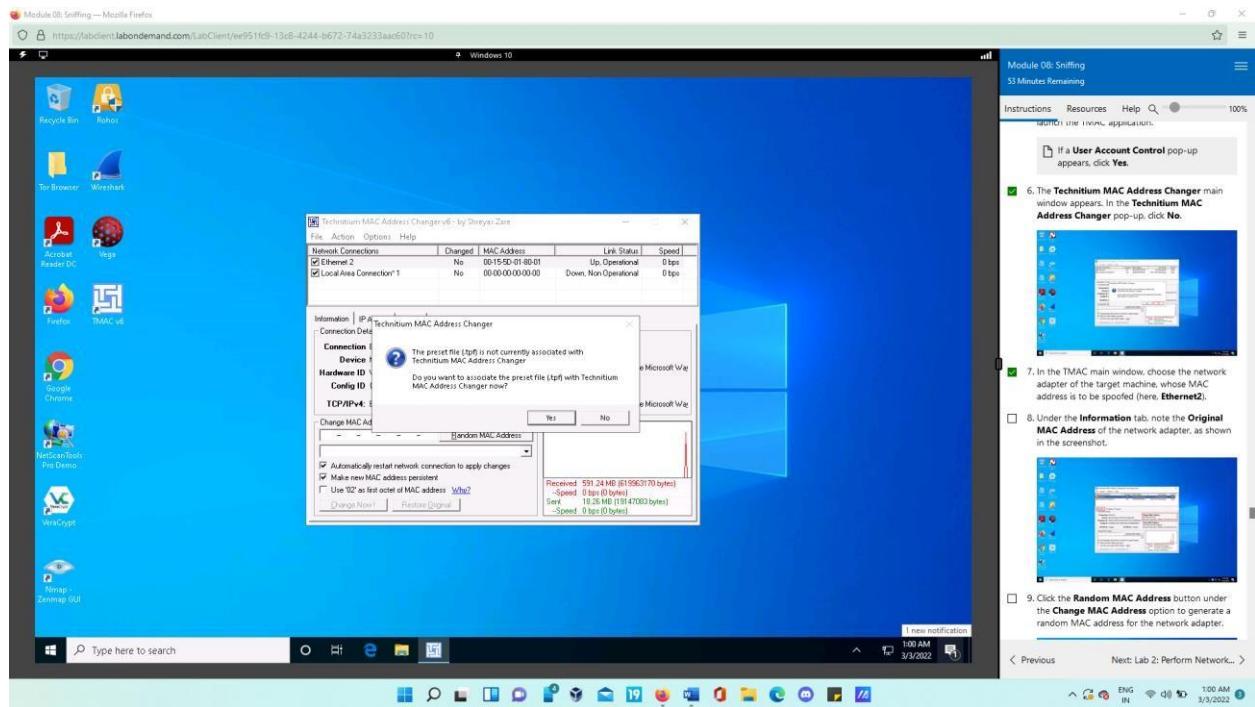
- Press finish to complete the installation.



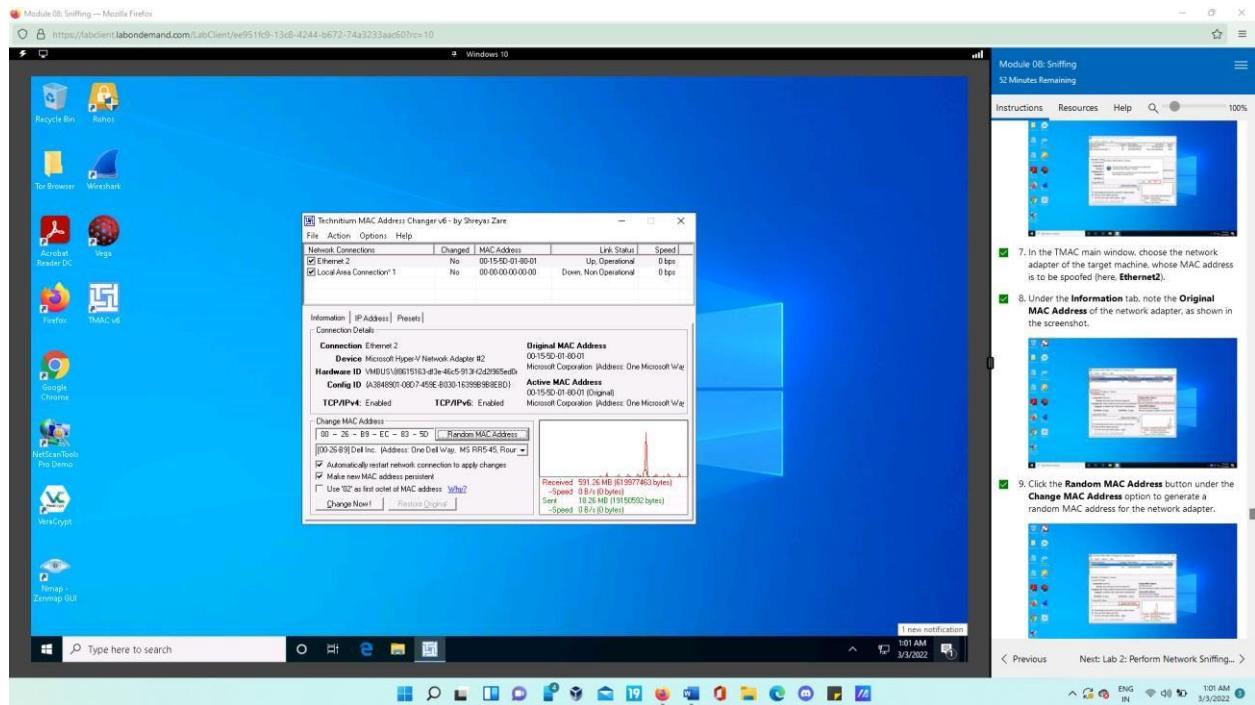
- Open TMAC from Desktop.



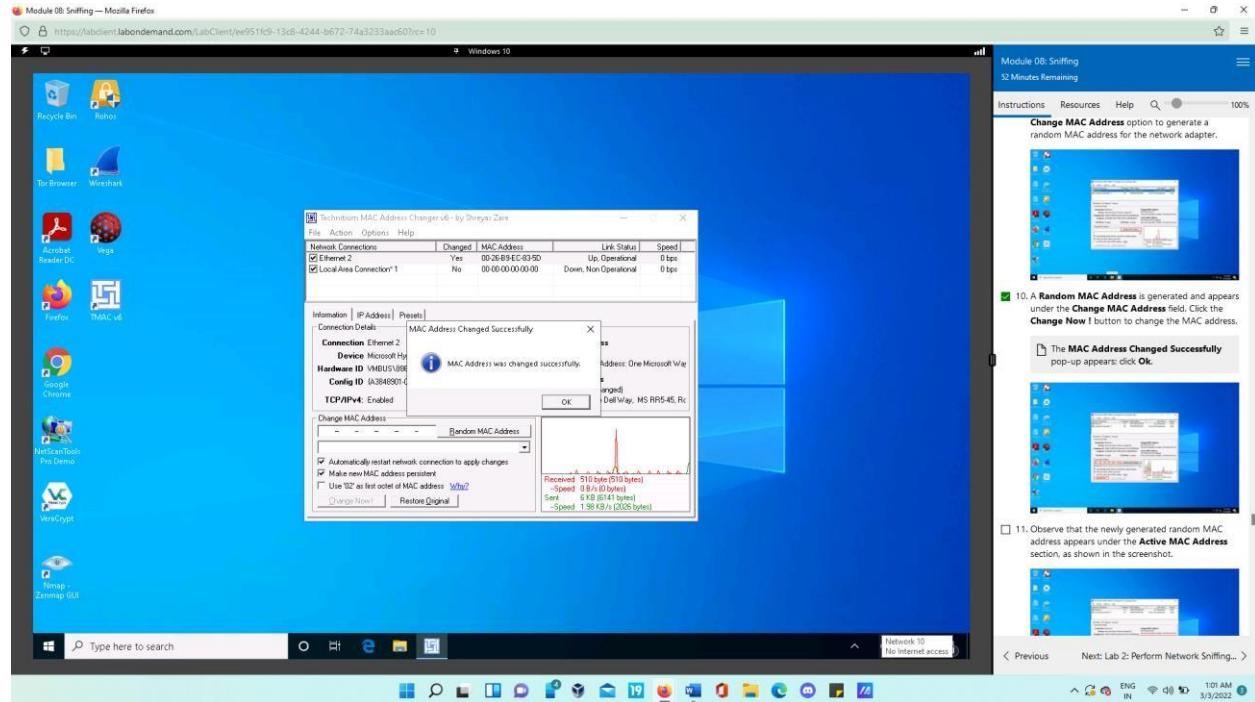
- Click No in the pop-up window.



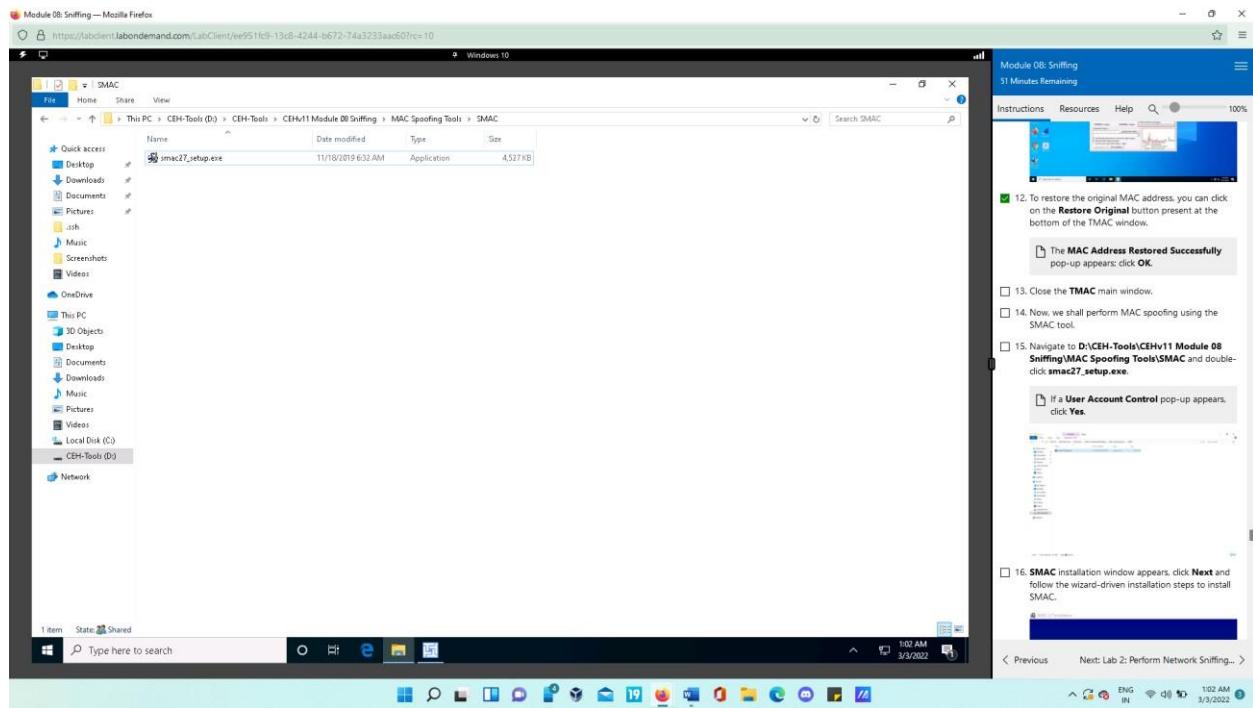
Note the Original MAC Address of the network adapter under the Information tab, as shown in the screenshot. To generate a random MAC address for the network adapter, click the Random MAC Address button beneath the Change MAC Address option.



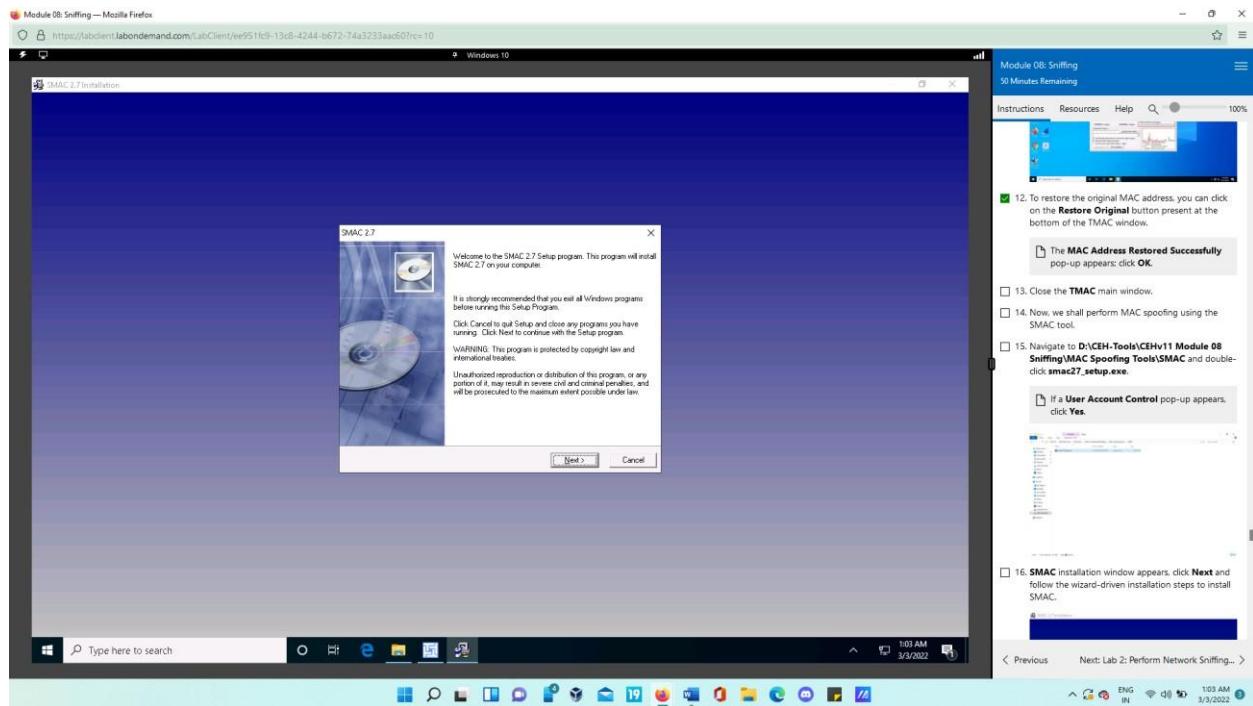
- Generated random MAC address will appear in the change MAC address field. Press “change now” to change the address.



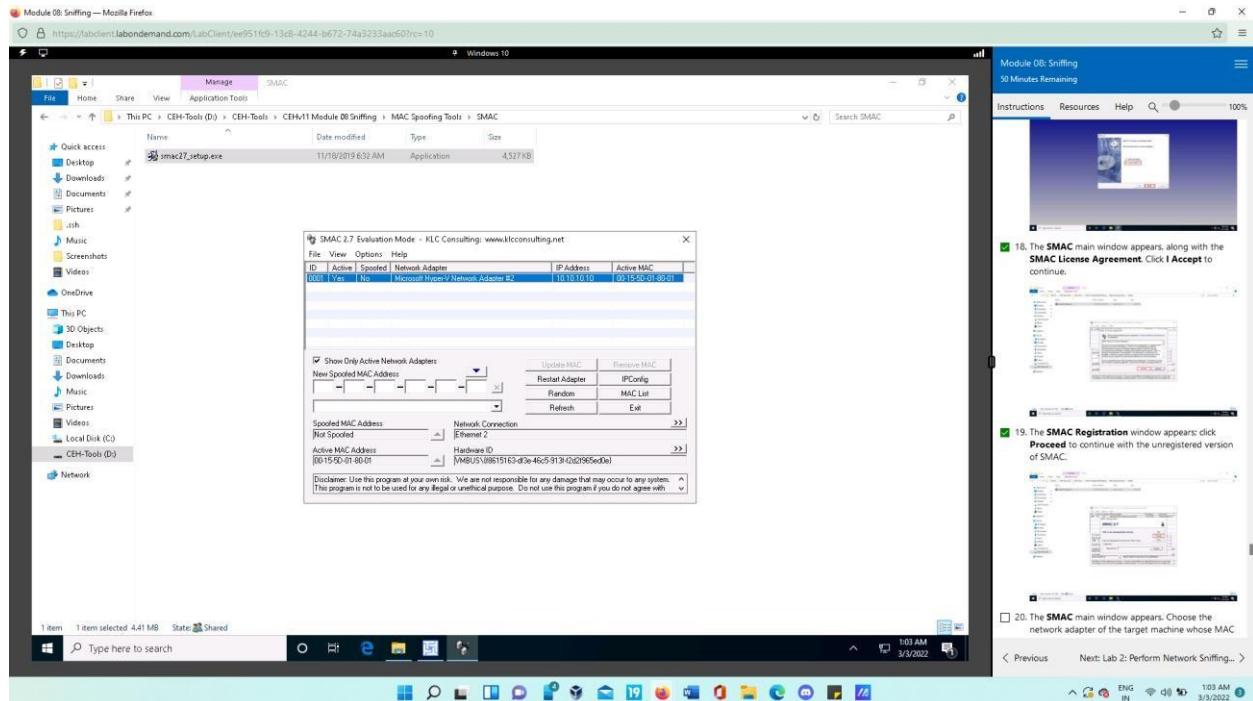
• Navigate to D:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC and execute smac27_setup.exe.



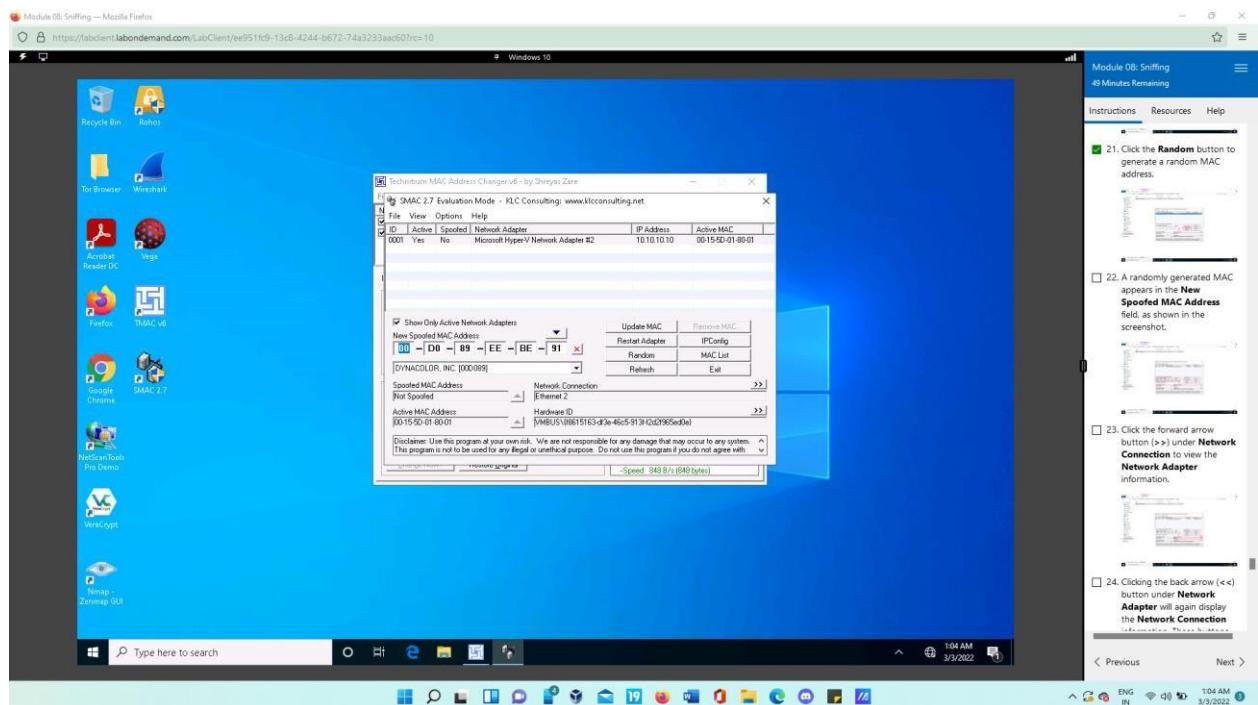
- Press next and finish the installation process



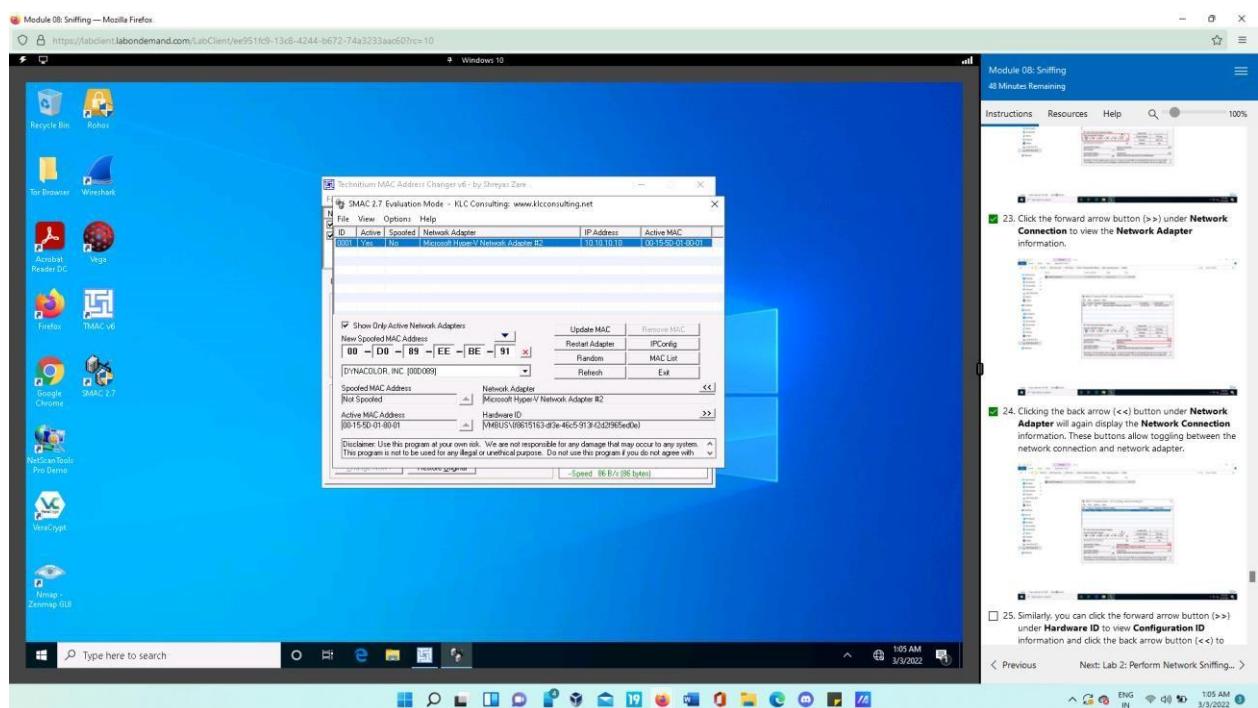
Now launch the SMAC.



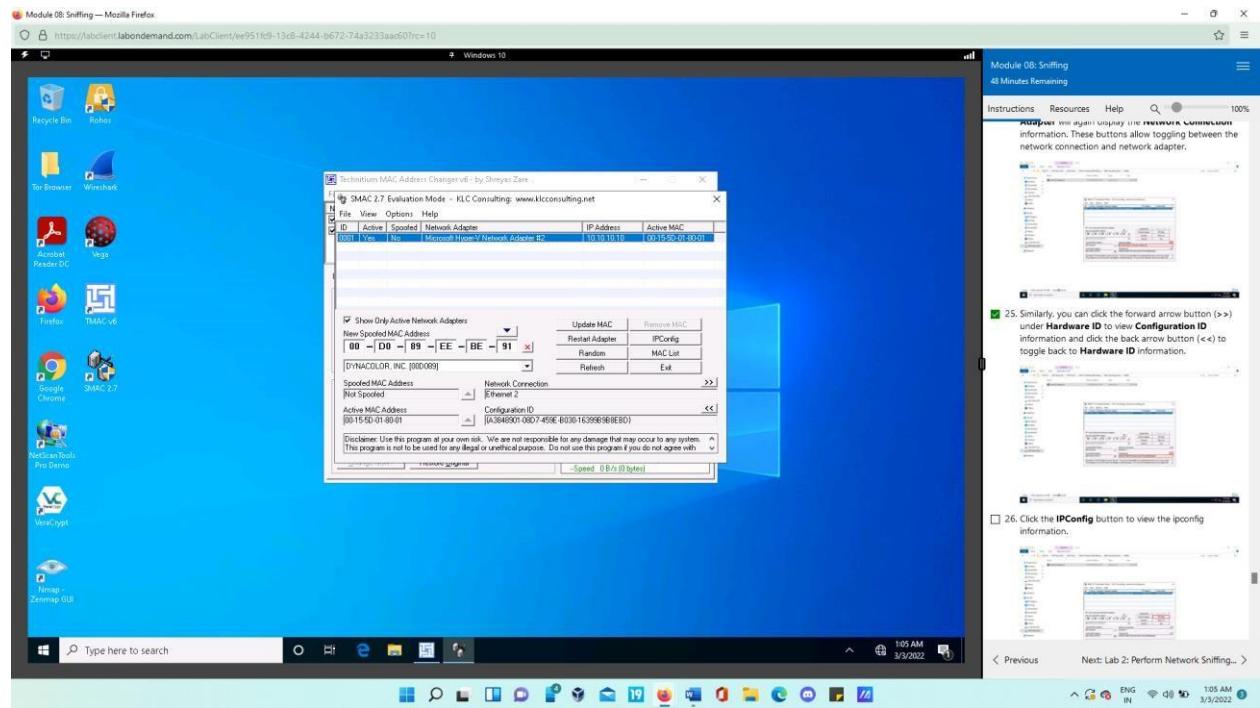
- Now in the SMAC main window, we will select the network adapter of the target machine whose MAC address we want to spoof.
- Here, press “random” button to list out random MAC address. Then, a randomly generated MAC address will be appeared in New spoofed MAC address field.



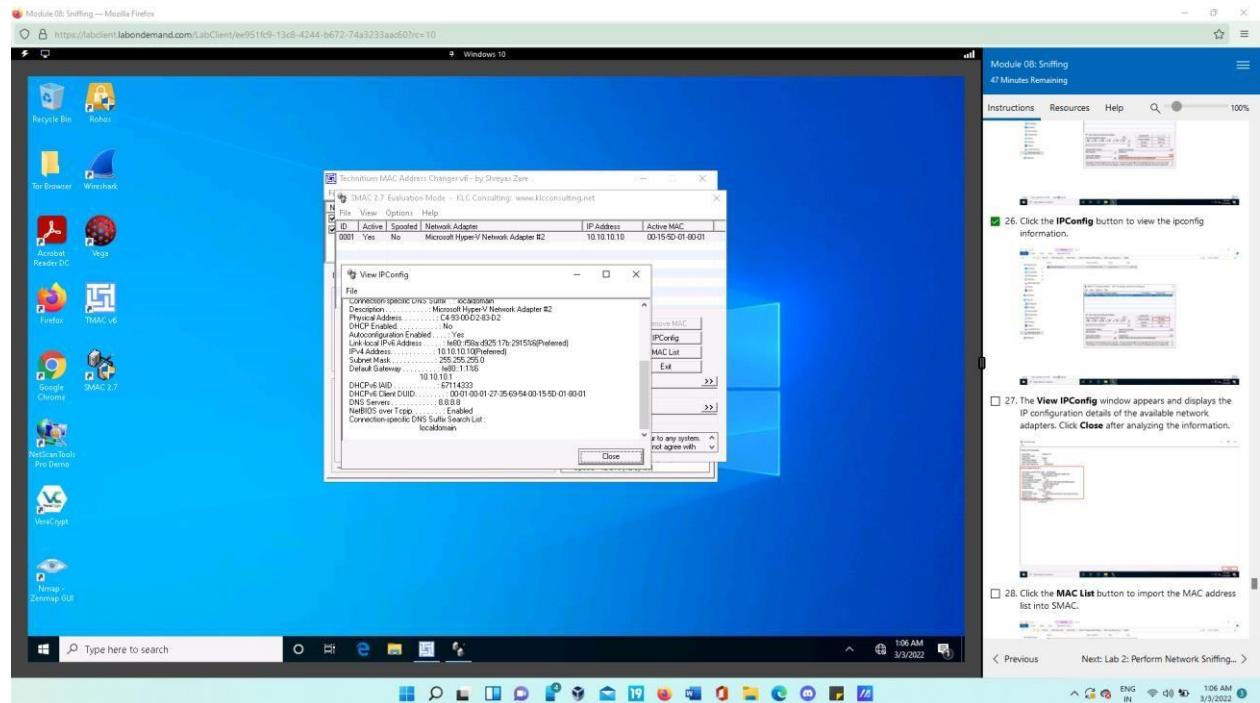
After that, view Network Adapter information by pressing (>) button under Network connection.



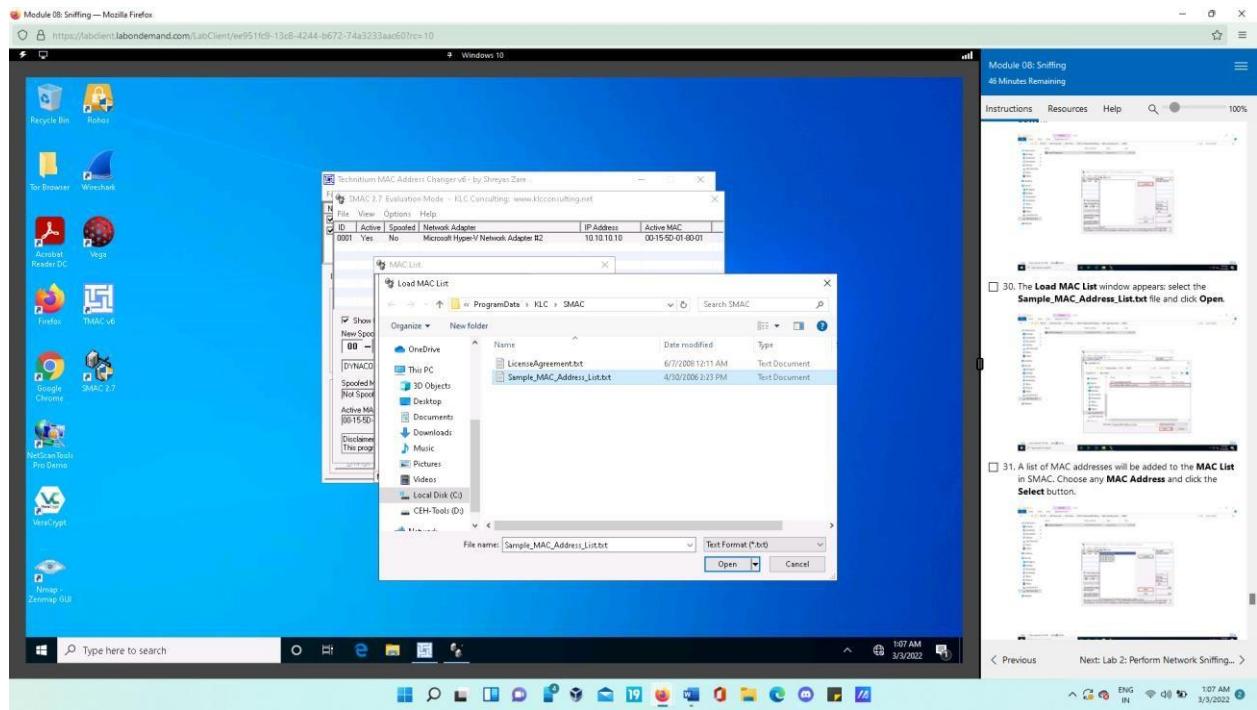
- Also, we can use (>) option in Hardware ID to display the Configuration ID.



Use IPConfig option to view ipconfig information.

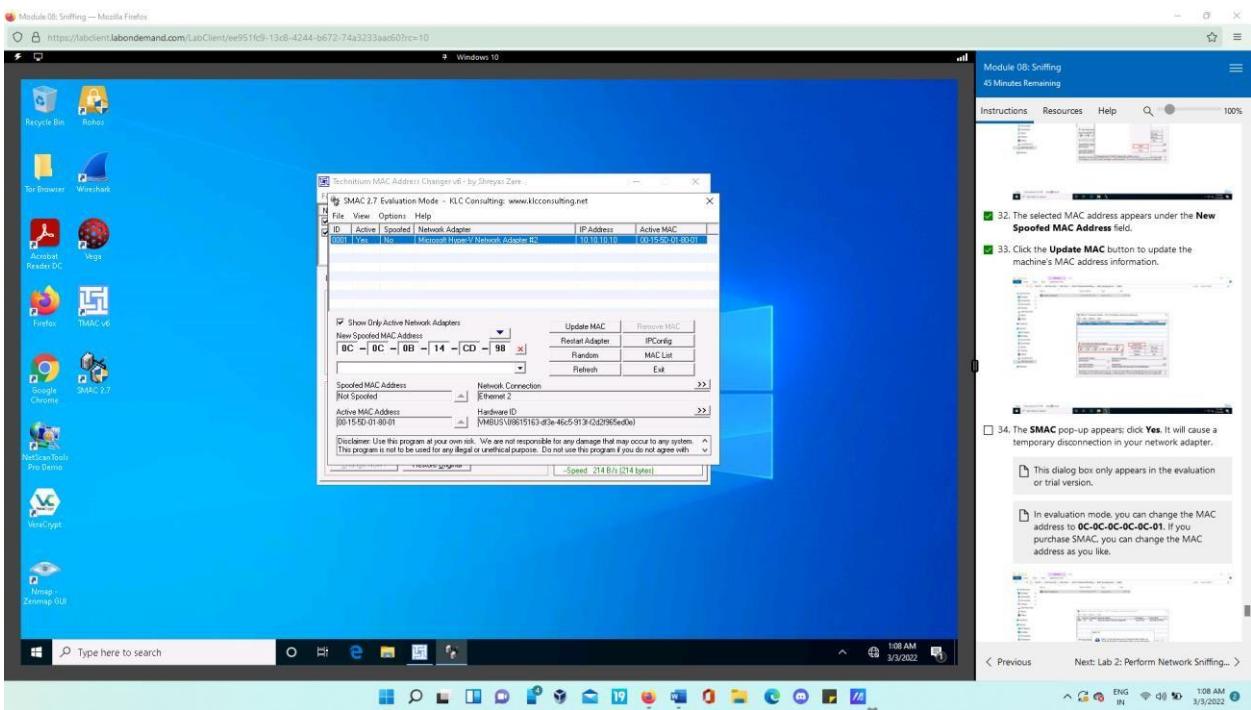


- Open the Sample_MAC_Address_List.txt file to import the MAC address list to SMAC by using load list feature.

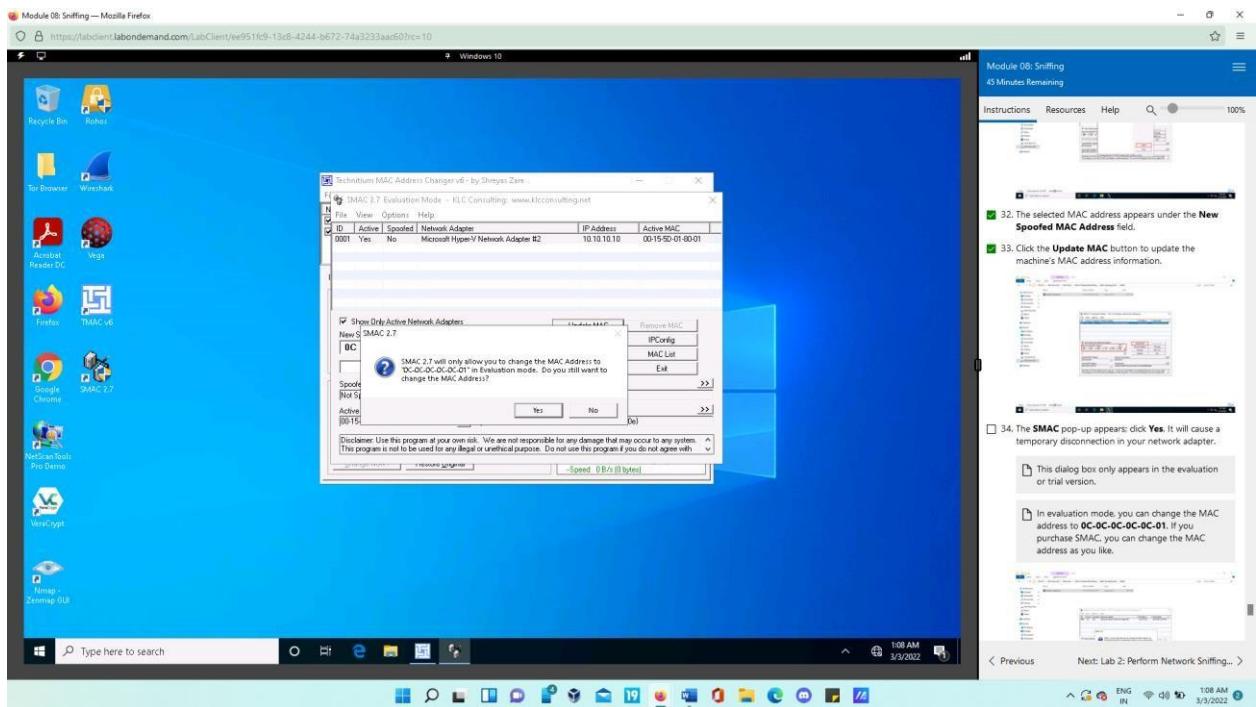


After adding the list, choose any random address and press select button. Under new spoofed MAC address field, the selected MAC address will appear.

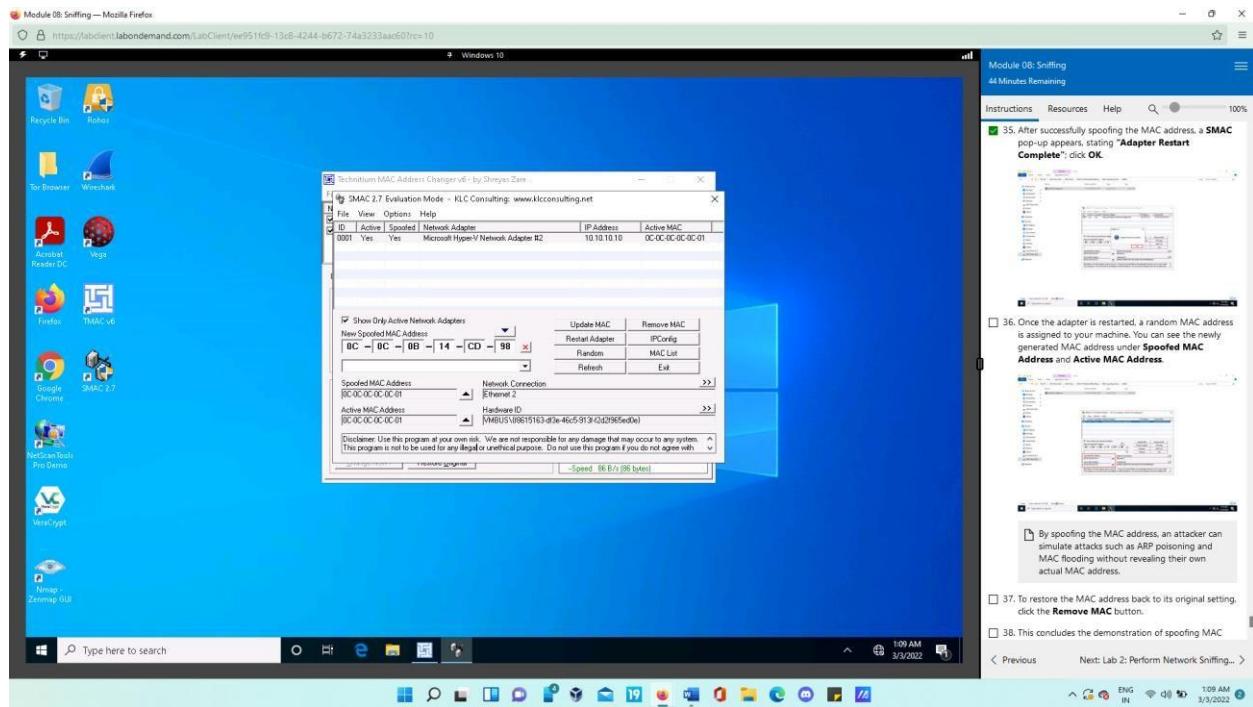
- Now we will update the Machine's MAC address information by pressing update MAC button.



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



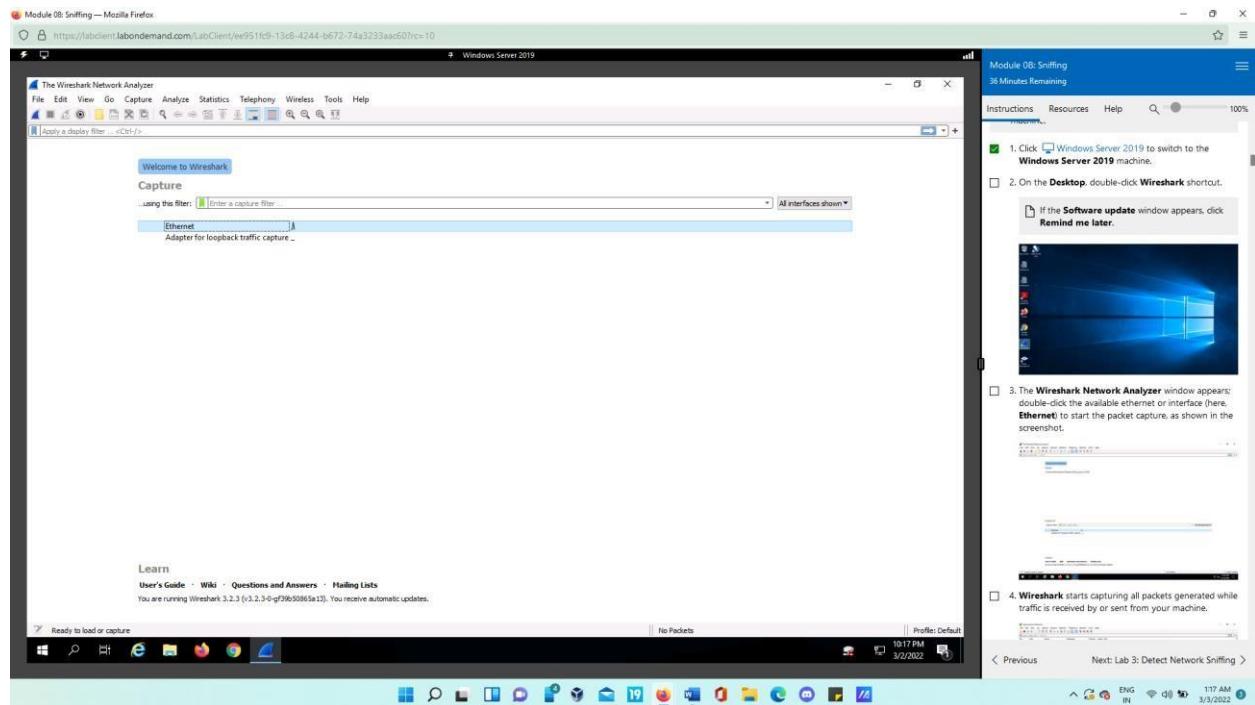
- After it is finished, we have completed spoofing the machine's MAC address as we can see under the spoofed MAC address and Active MAC Address.



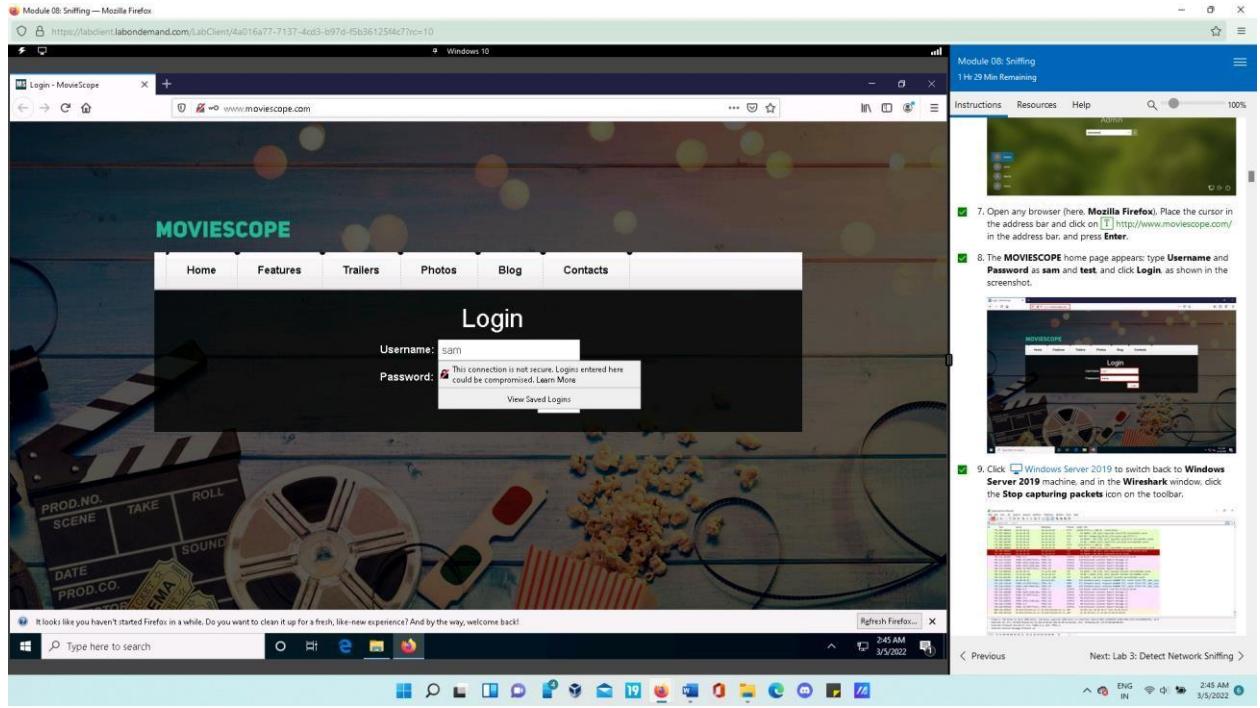
Lab 2: Perform Network Sniffing using Various Sniffing Tools

Task 1: Perform Password Sniffing using Wireshark

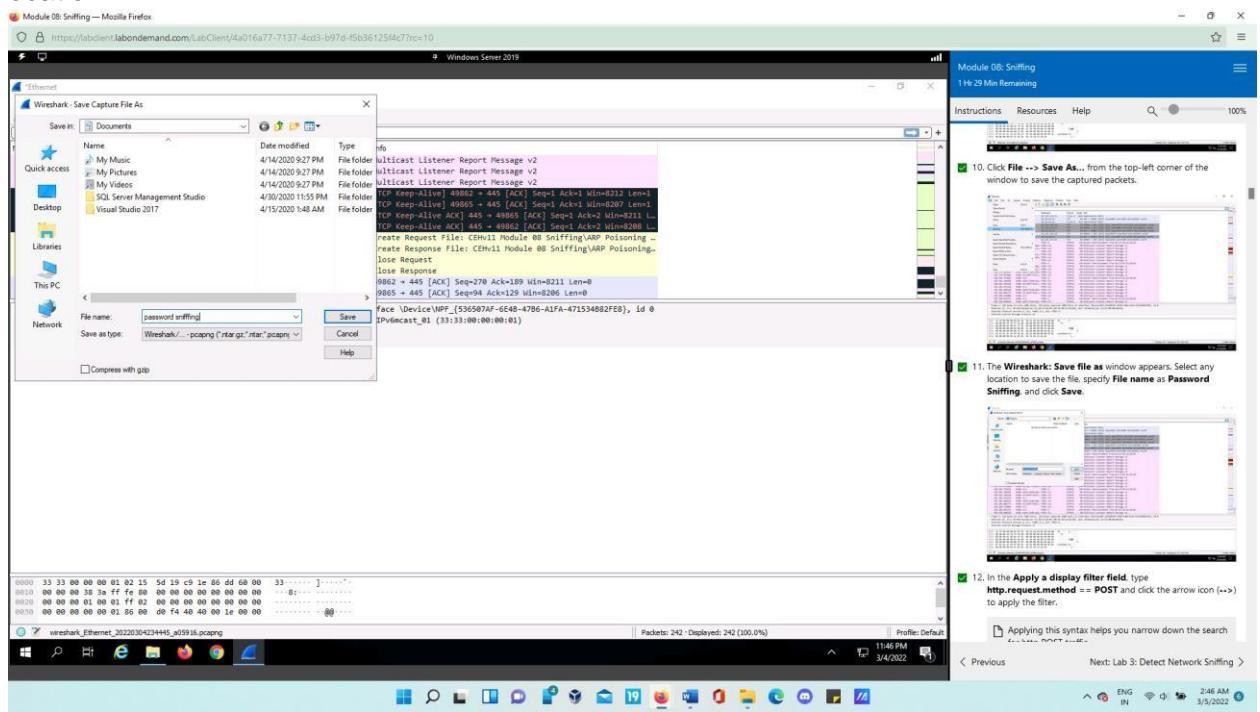
- In windows server 2019, open Wireshark from Desktop and select Ethernet. Wireshark will start packet capture.



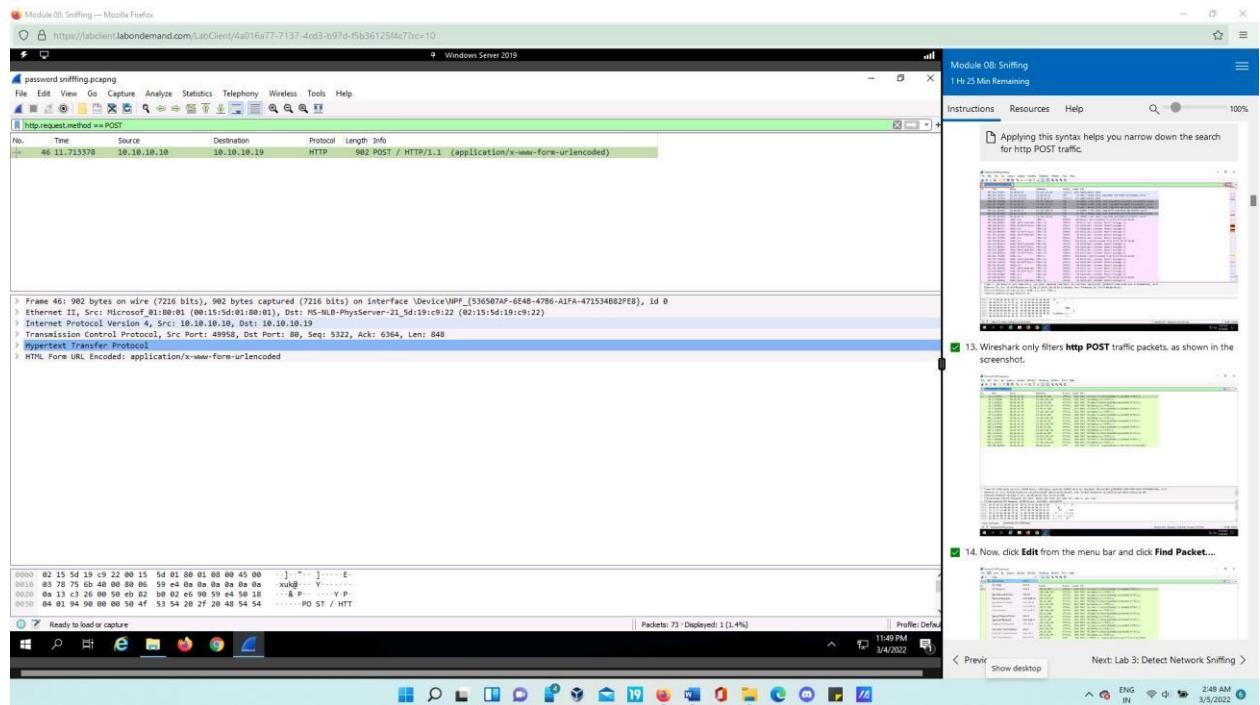
- Now in Windows1) navigate to <http://www.moviescope.com> from the web browser. Login by using Sam and test as username and password respectively.



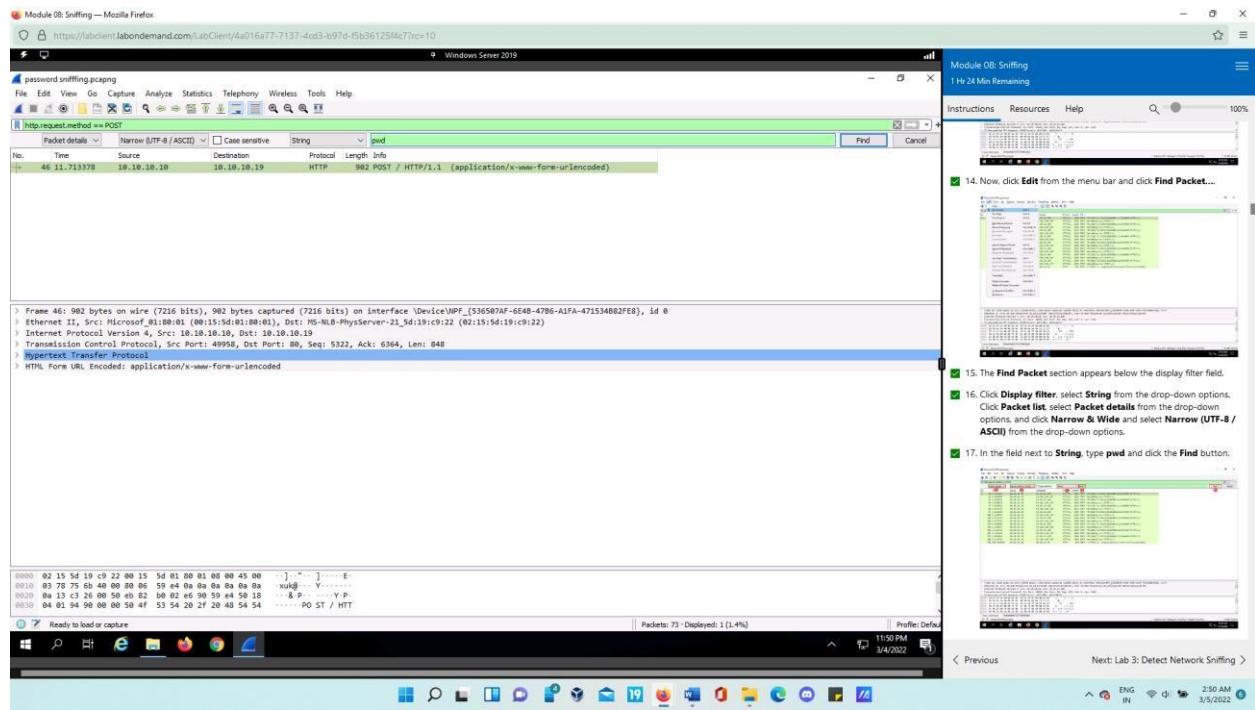
In windows server 2019, stop capturing packets in Wireshark and save the packet capture file at any location.



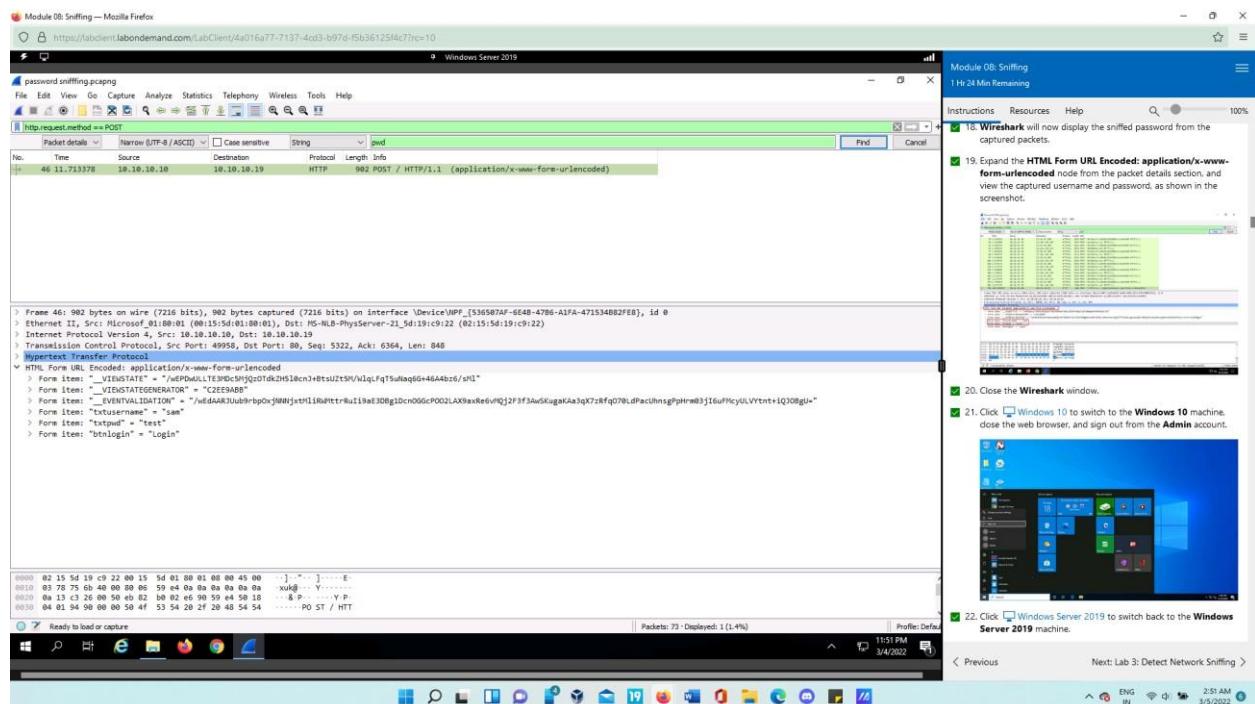
- Now filter the packet display for viewing only HTTP POST packets by using 'http.request.method == POST' filter.



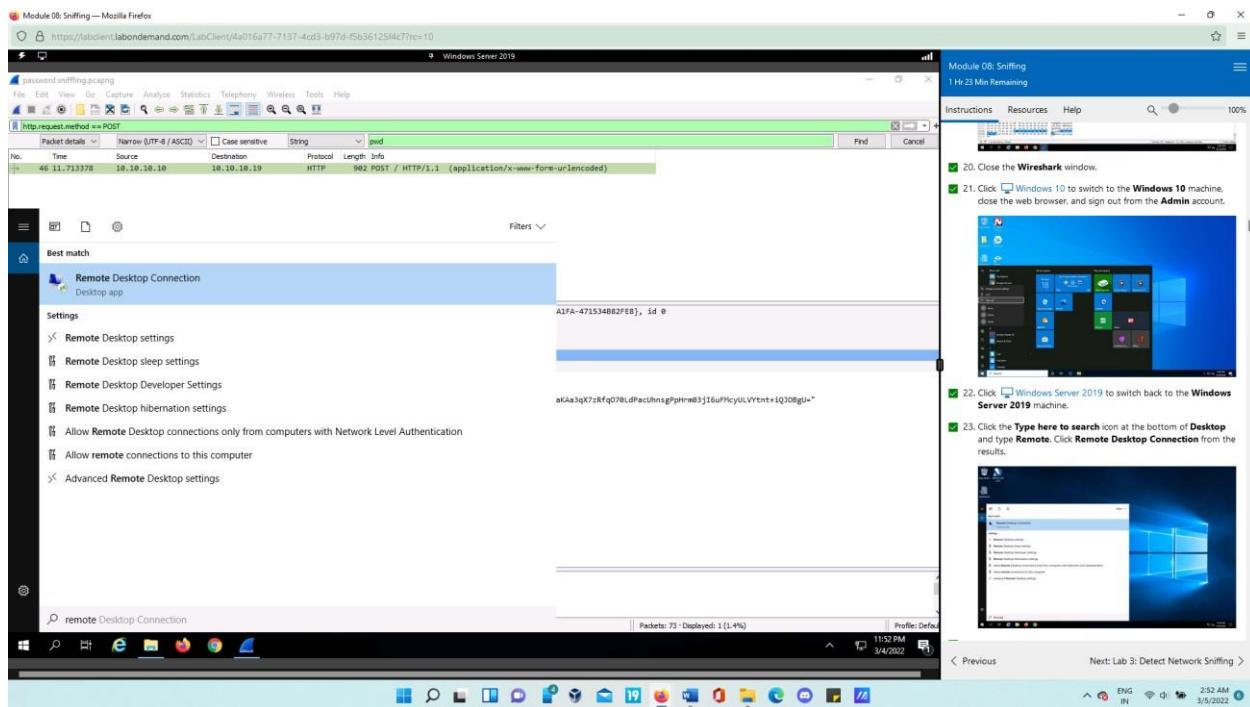
Then press edit > find packet > display filter > string > packet list > packet details > narrow & wide > narrow (UTF-8 / ASCII). In the field next to string, type in pwd and click find.



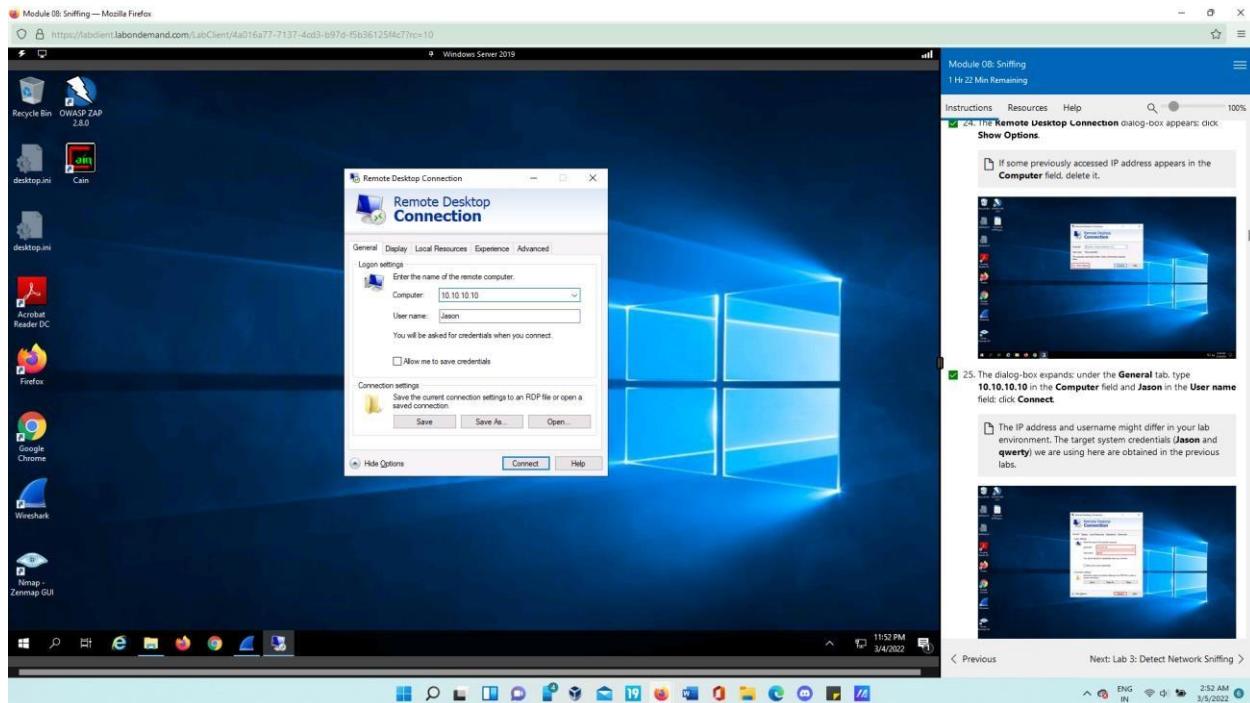
- The sniffed password from the captured packets will be displayed in wireshark.
- In the packet information section, expand the HTML Form URL Encoded: application/x-www-formurlencoded node to see the captured login and password.



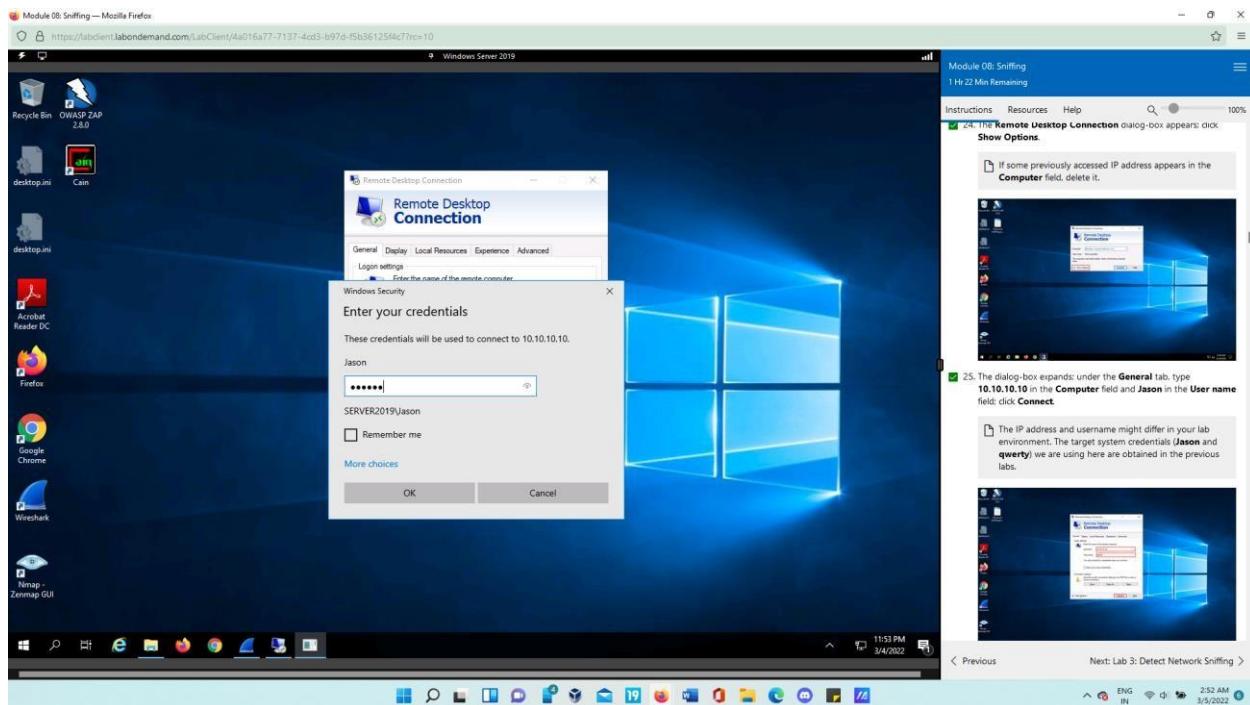
Open remote desktop connection application in Windows server 2019.



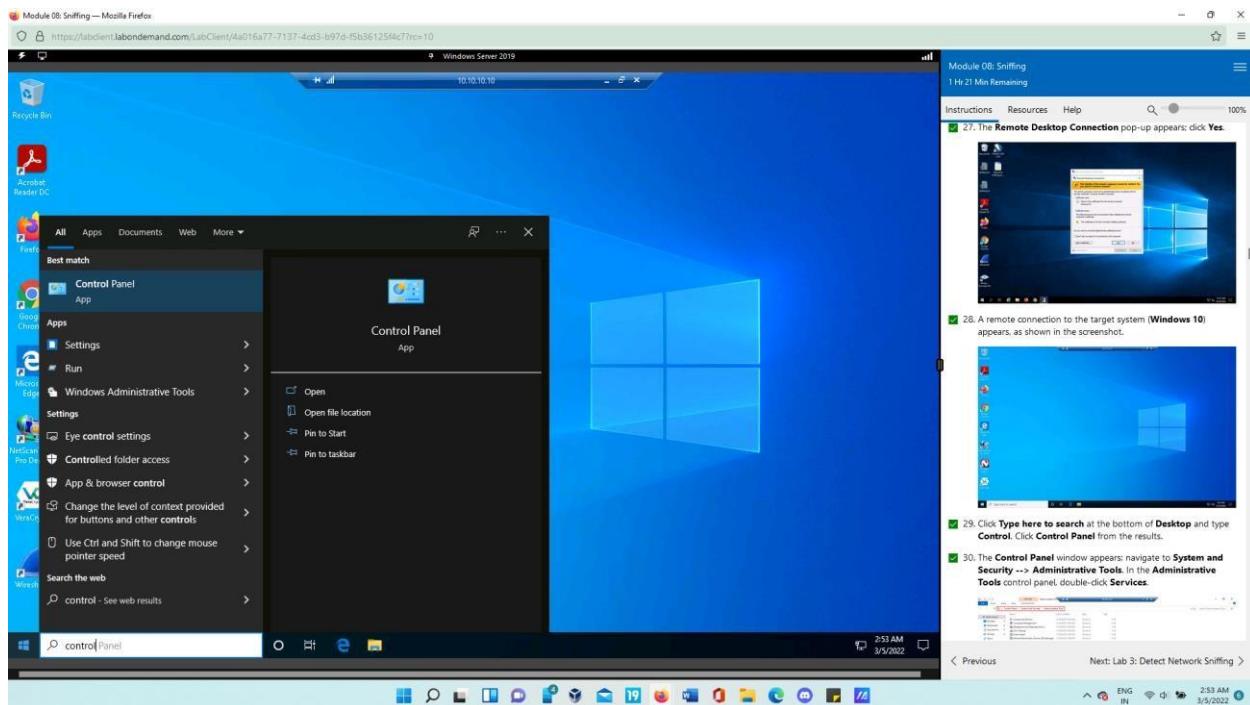
- The **Remote Desktop Connection** dialog-box appears; click **Show Options**
- The dialogue box expands; in the computer field, type 10.10.10.10, and in the Username field, type Jason; click Connect.

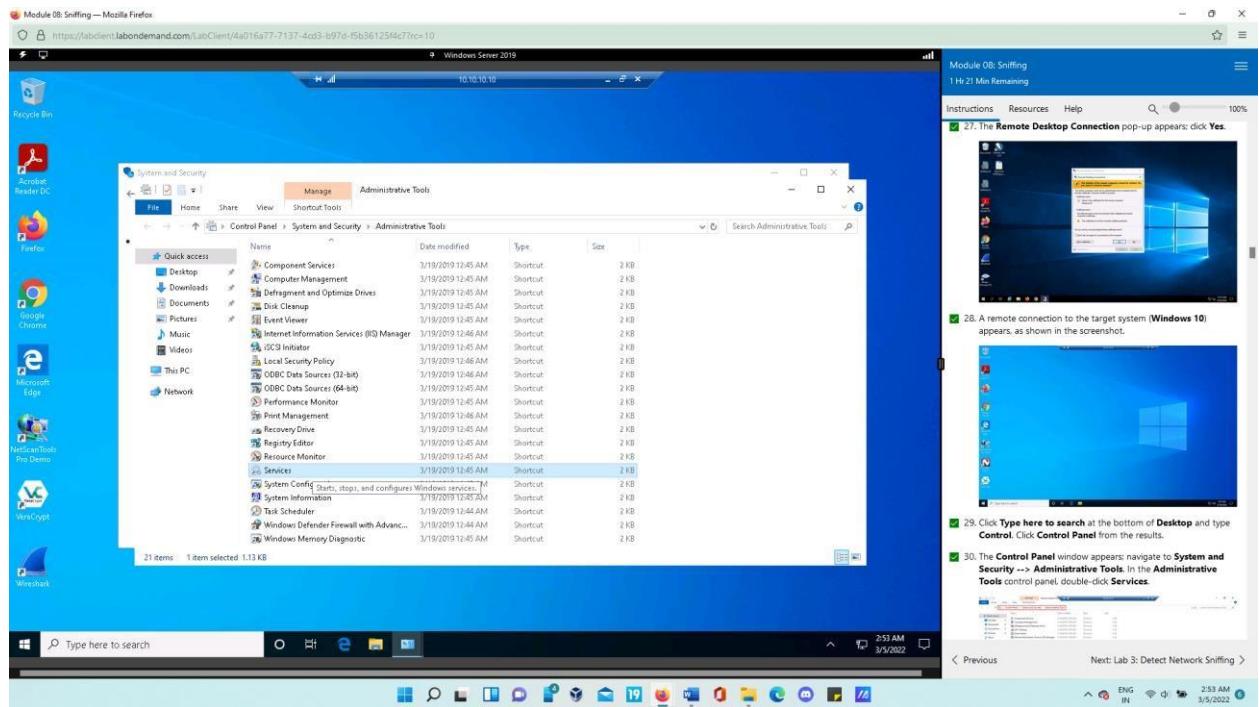


Here type in password as 'qwerty' and click ok.

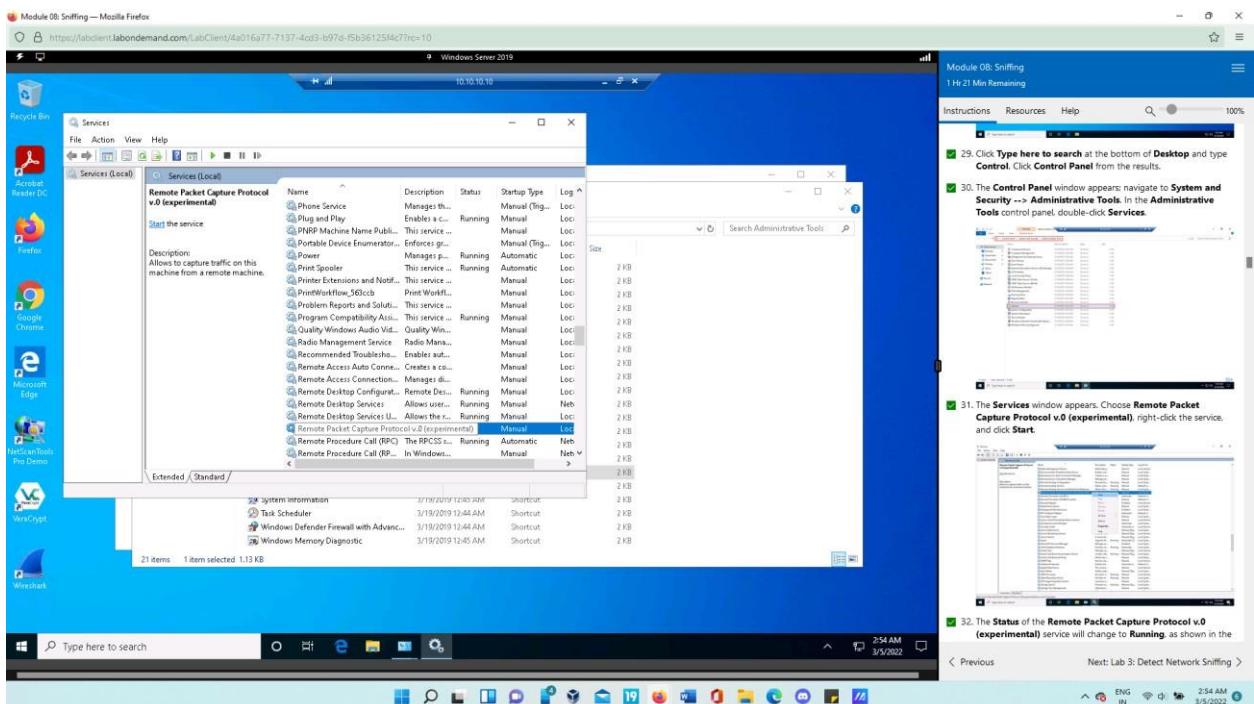


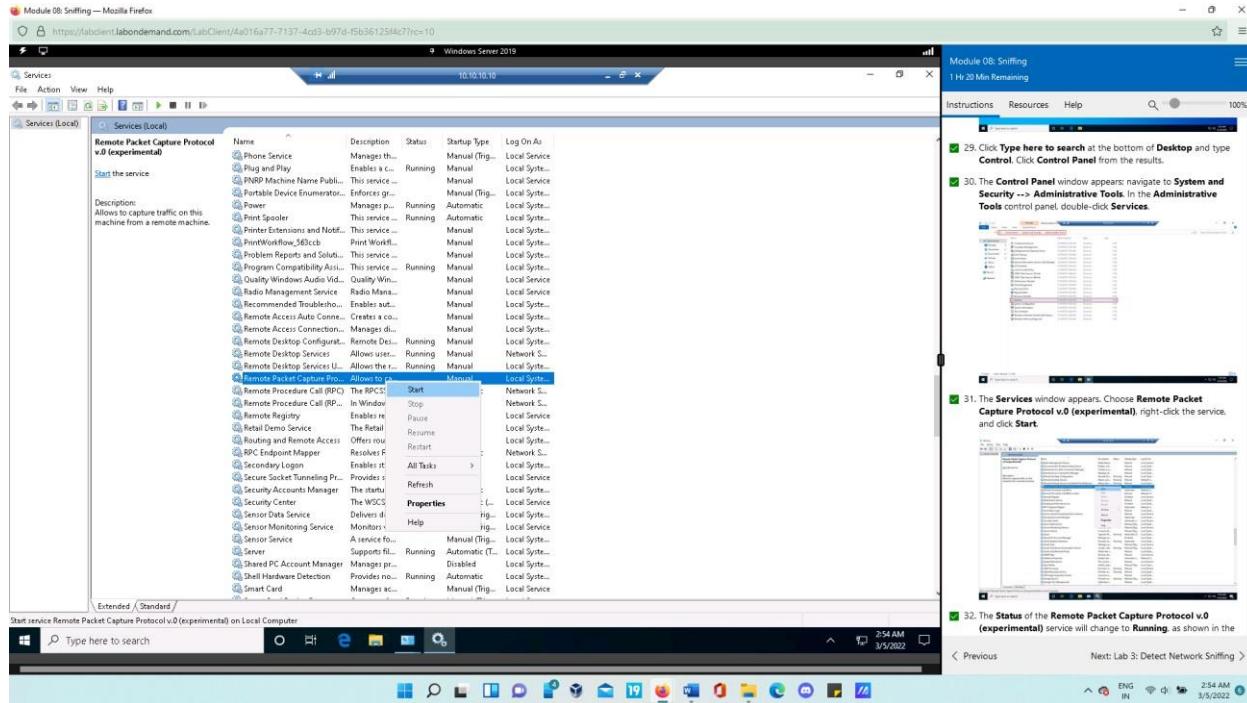
- The **Remote Desktop Connection** pop-up appears; click **Yes**.
- Then navigate to Control Panel > System and security > Administrative tools > services



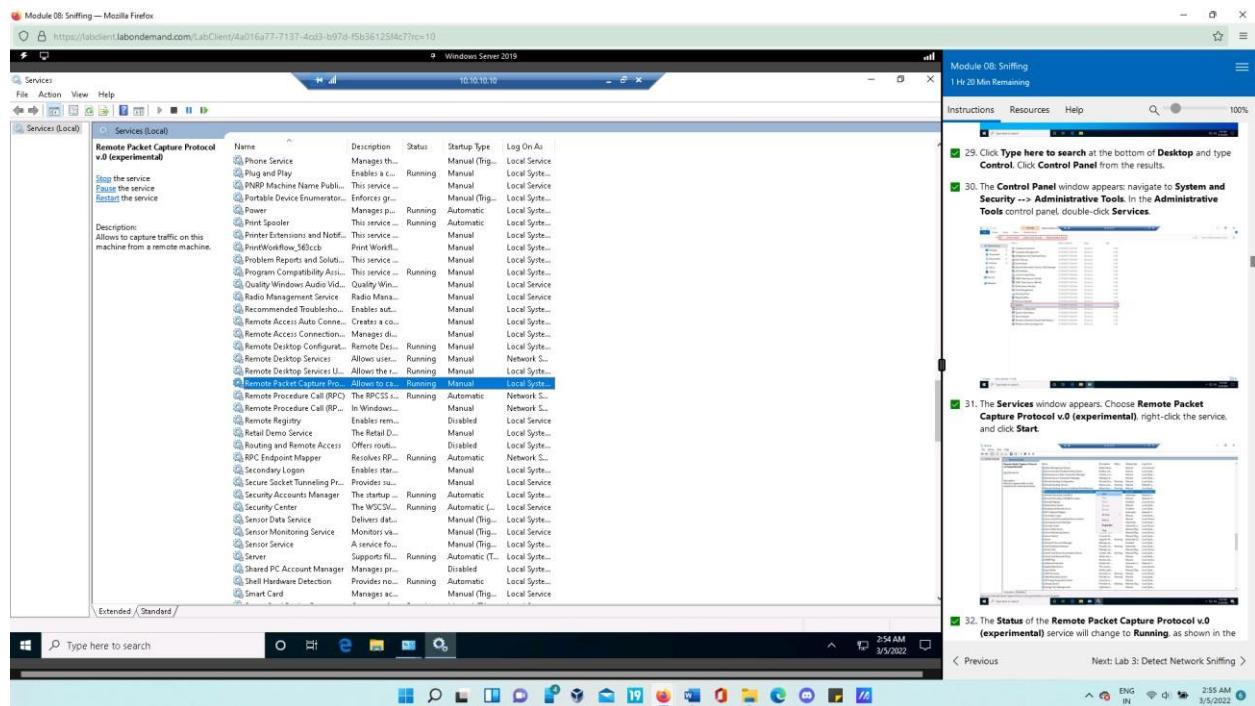


- The Services window is displayed. Select Remote Packet Capture Protocol v.0 (experimental) and double click services option to start it.

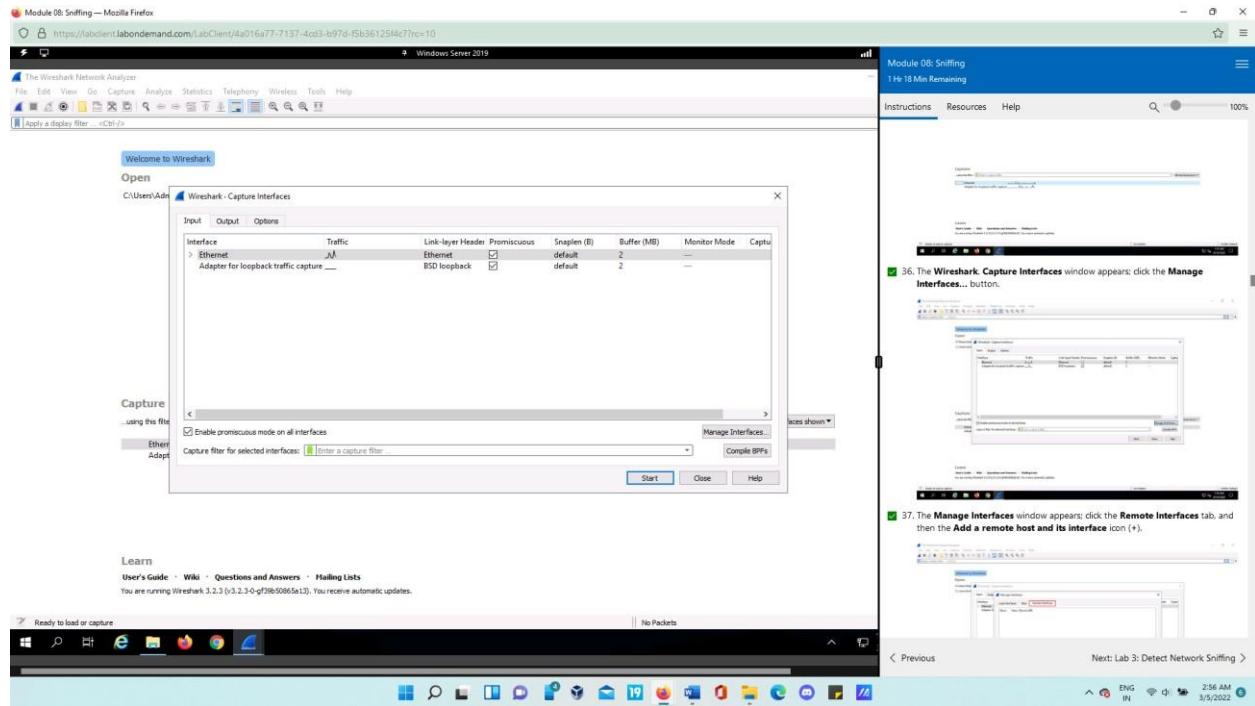




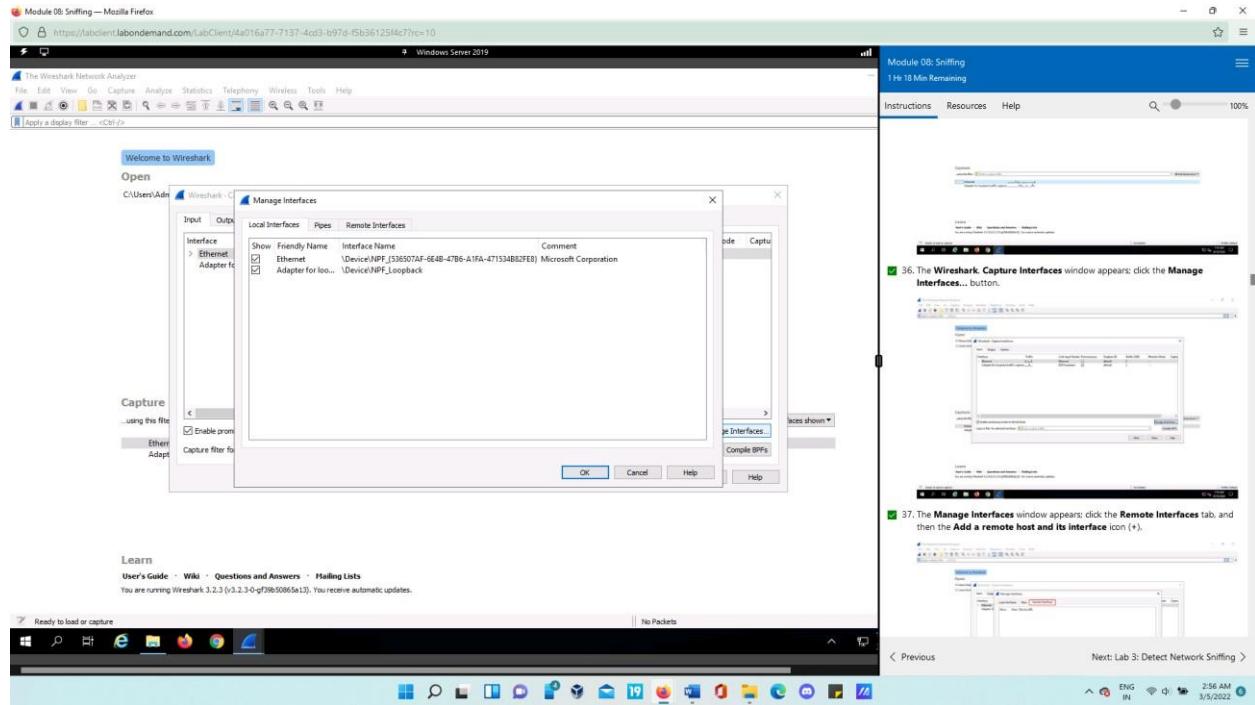
- The Remote Packet Capture Protocol v.0 (experimental) service's status will be updated to Running.



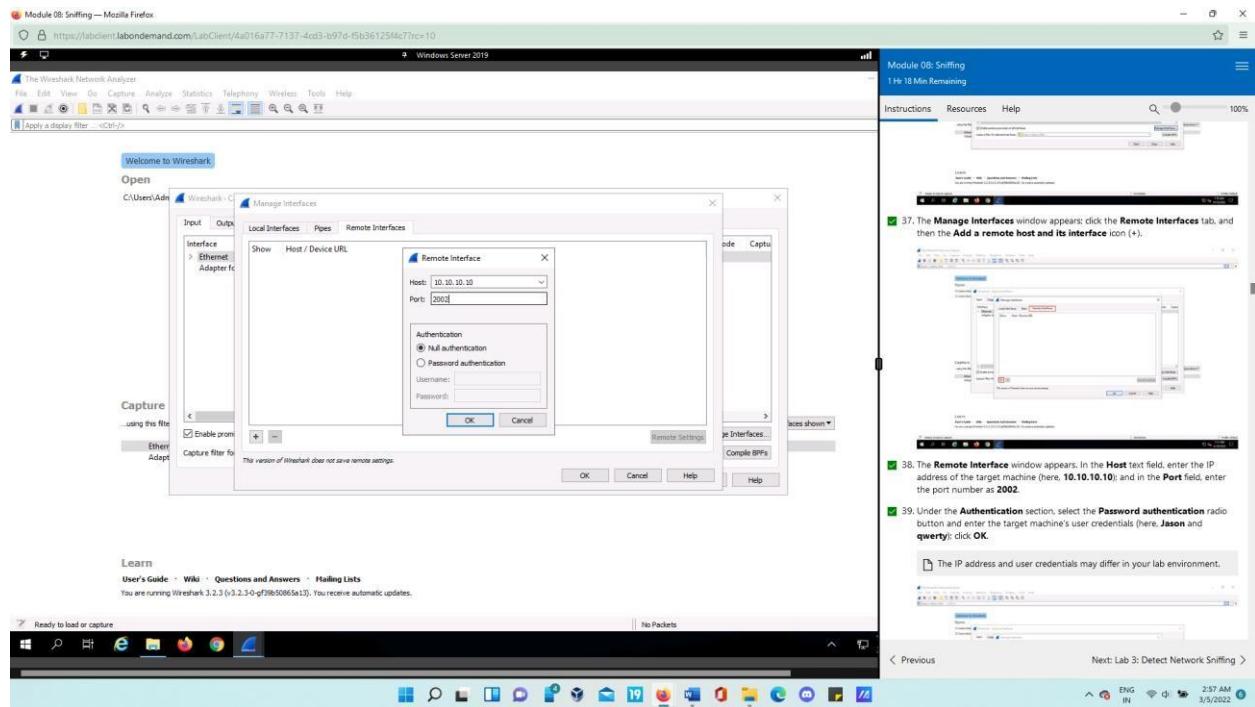
Close all open windows in Windows10 machine and now launch Wireshark from desktop. The Wireshark Network Analyzer window displays; from the toolbar, select Capture options.



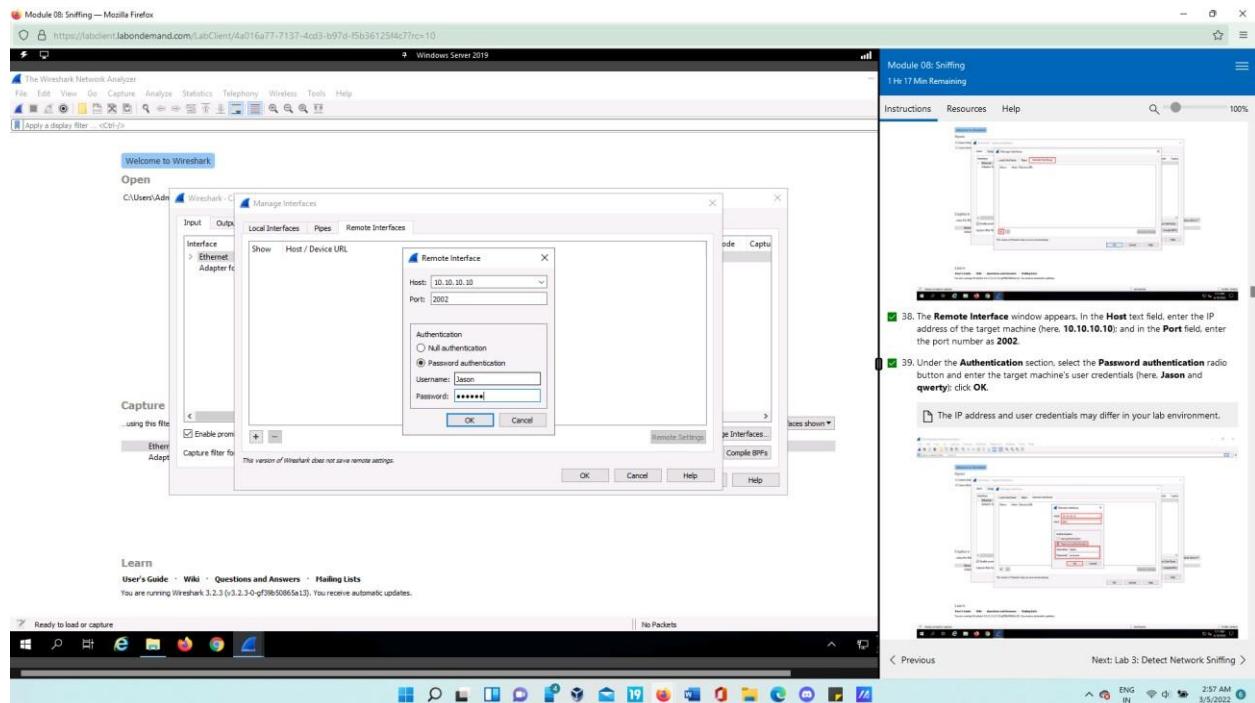
- Choose manages interfaces option from Wireshark capture interfaces window.



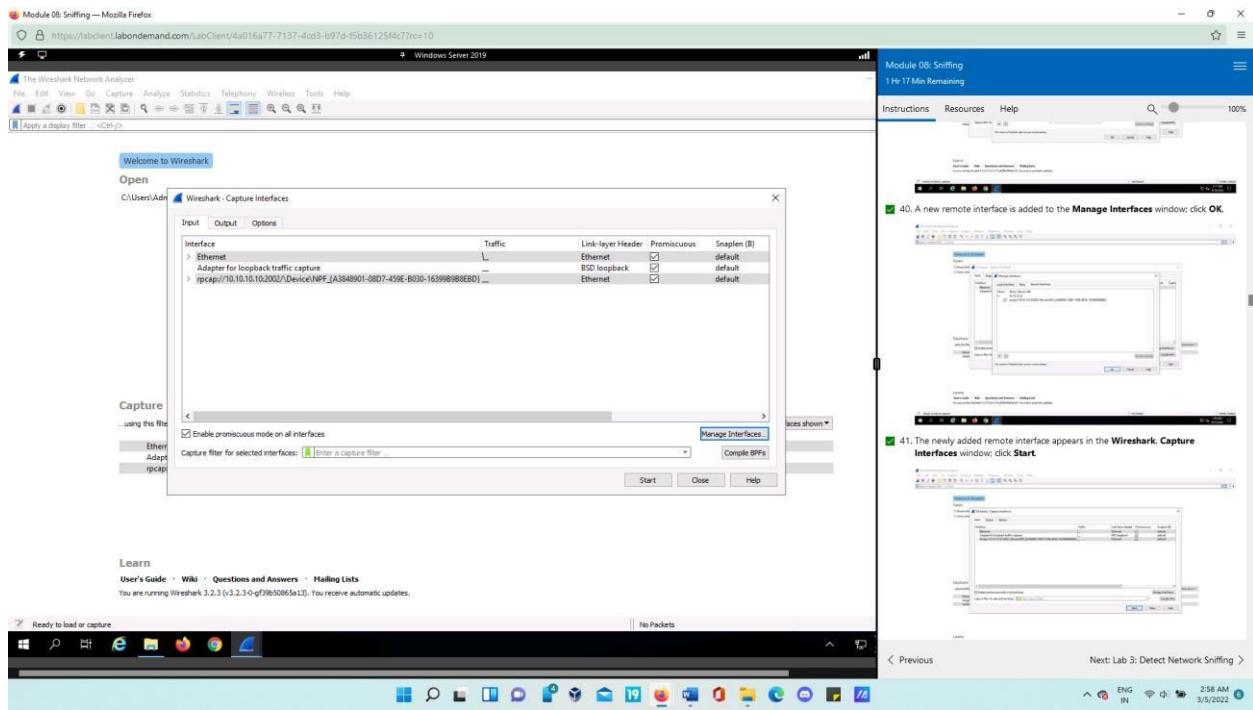
Now click remote interfaces > add remote host and its interface. Then in remote interface window, type 10.10.10.10 in host field and 2002 in port field.



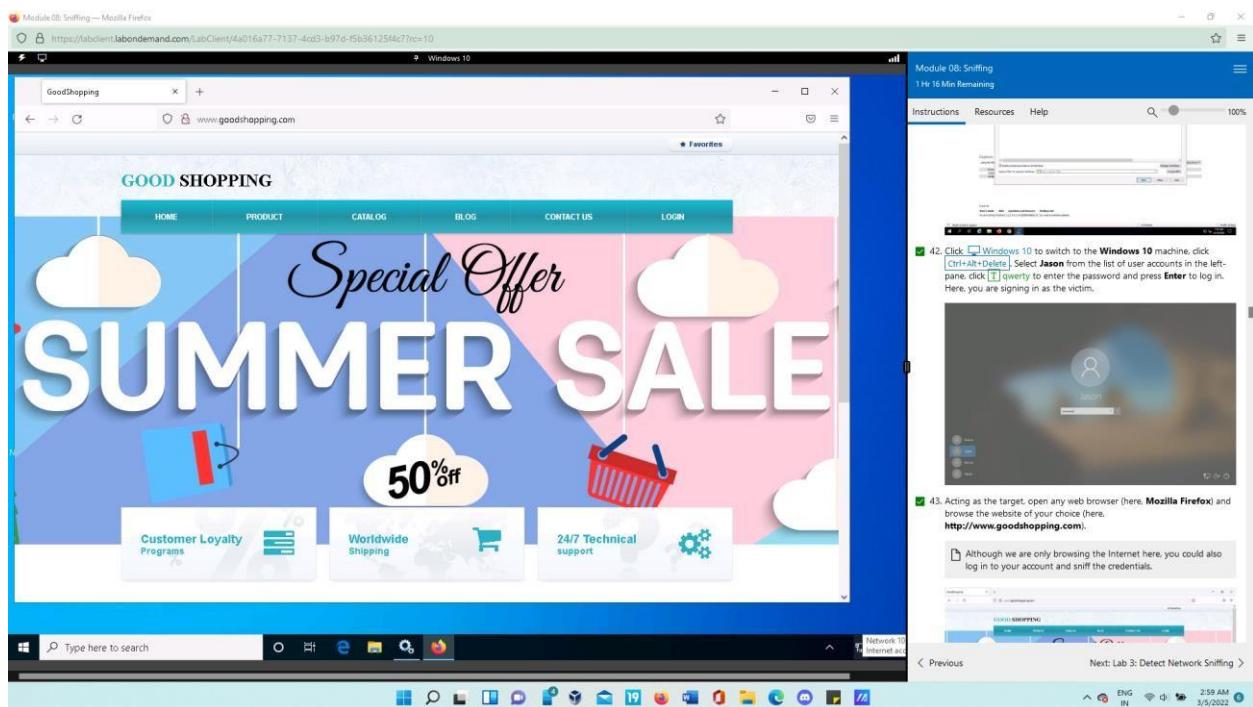
- Now use Jason and qwerty as username and password respectively for password authentication. After press ok.



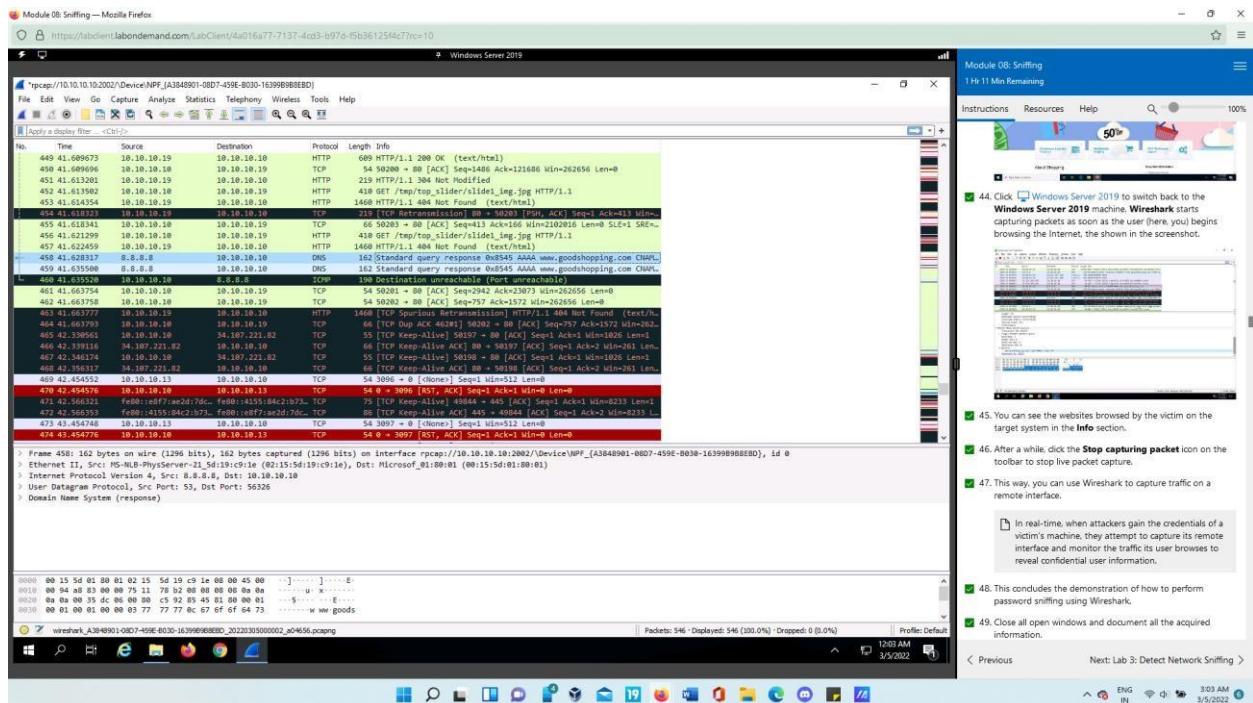
In manage interfaces, a new remote interface is added. Now choose newly added remote interface and press start.



- 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

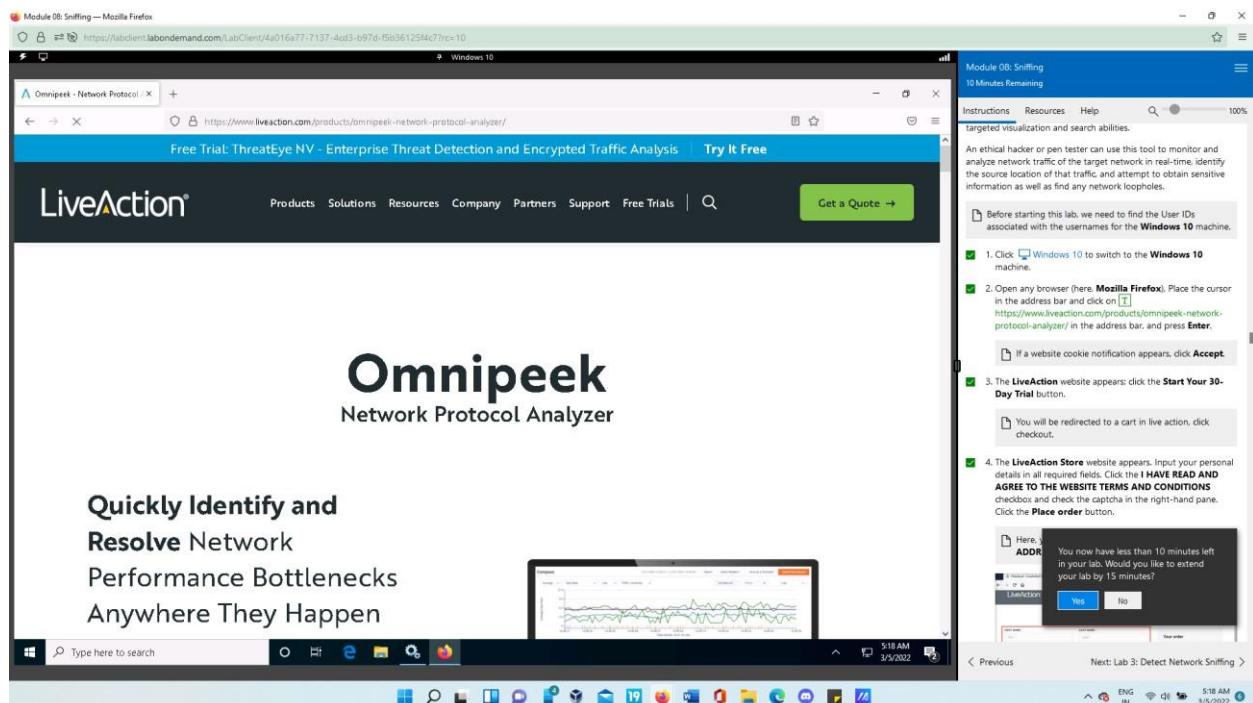
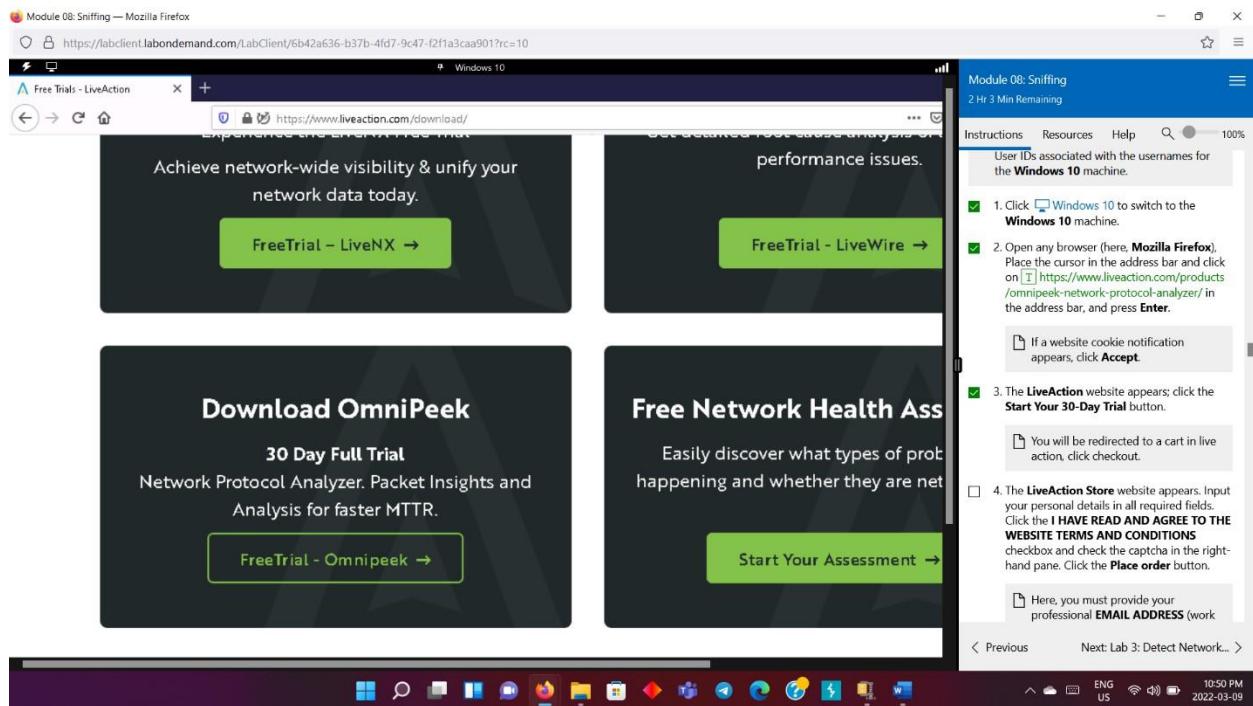


Now open Wireshark in Windows server 2019, you can see Wireshark starts capturing packets as the user begins browsing the web. In the Info area, you can see which websites the victim visited on the target system.

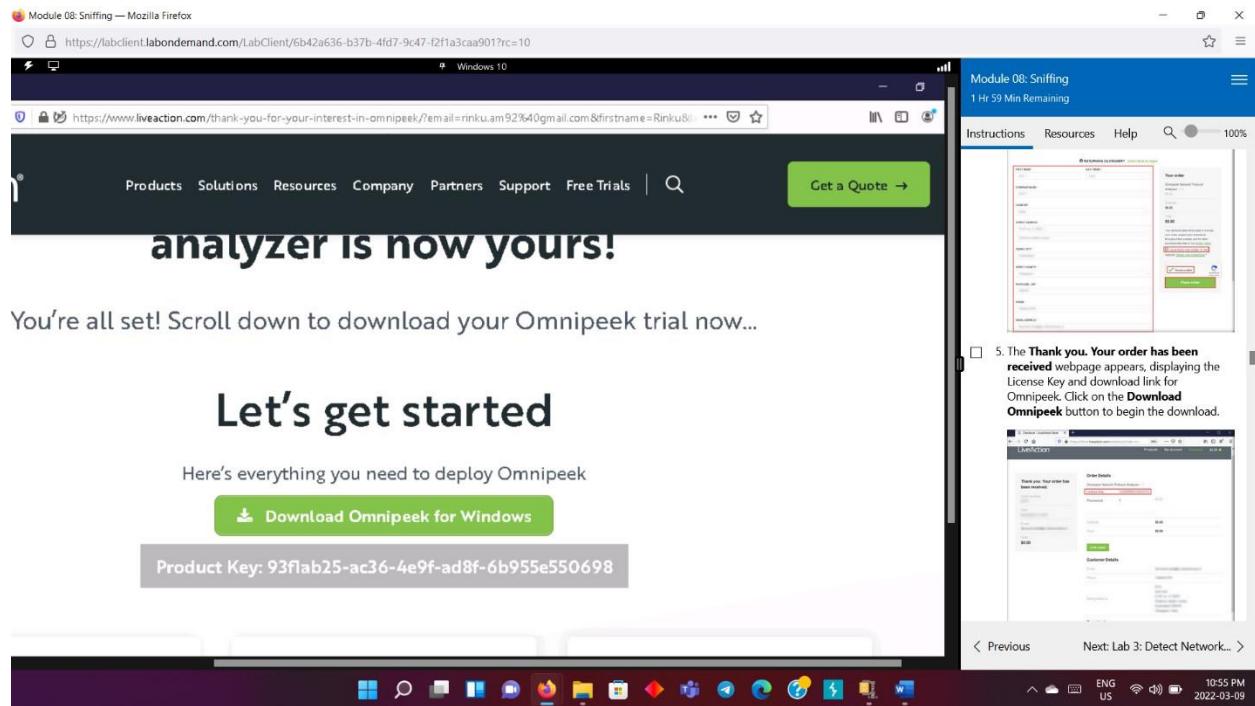


Task 2: Analyze a Network using the Omnipoke Network Protocol Analyzer

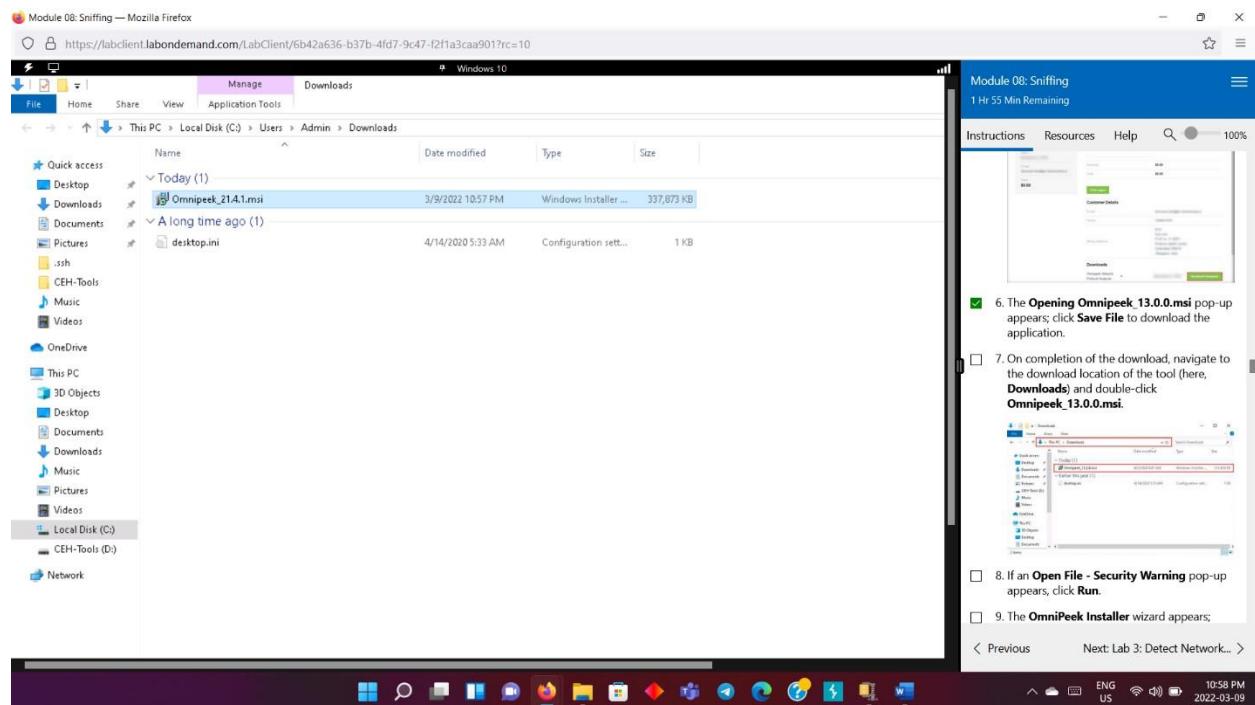
- Launch windows 10 OS and open a browser and paste the link : <https://www.liveaction.com/products/omnipoke-network-protocol-analyzer/> and click on enter.

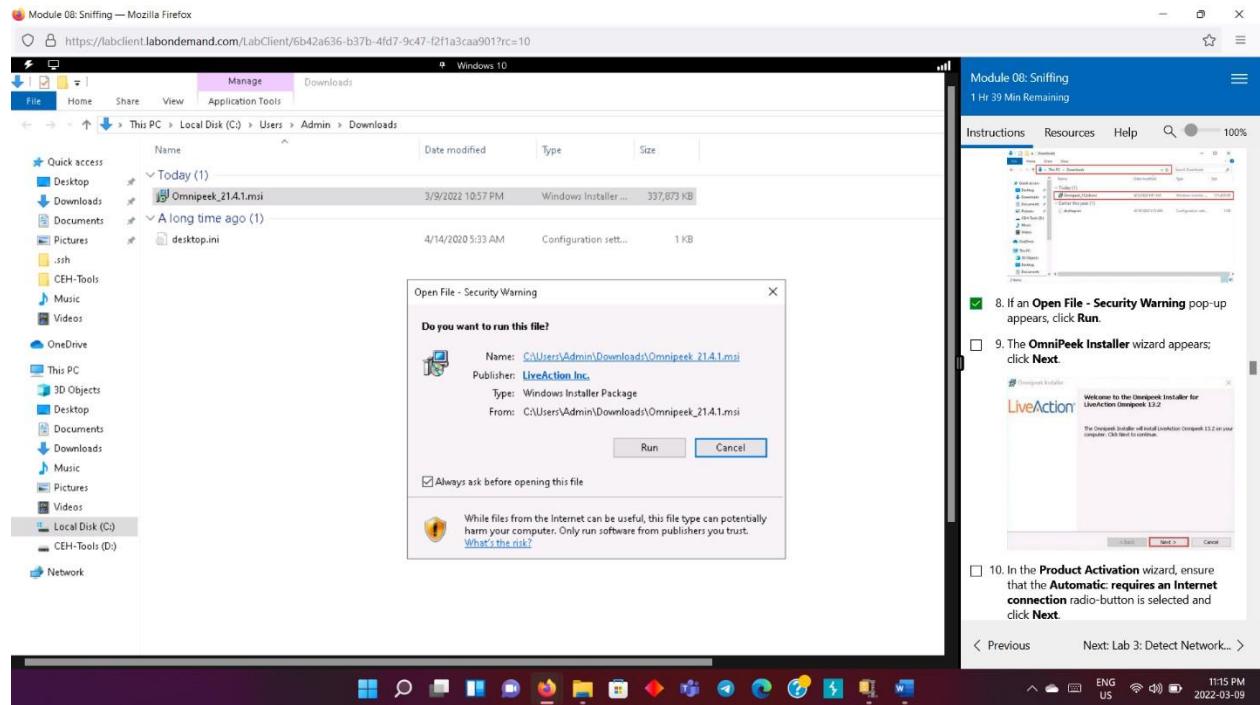


- Once the website is up, click on the trial button. Fill in the details and click on place order. Download the Omnipoke button and start the download.

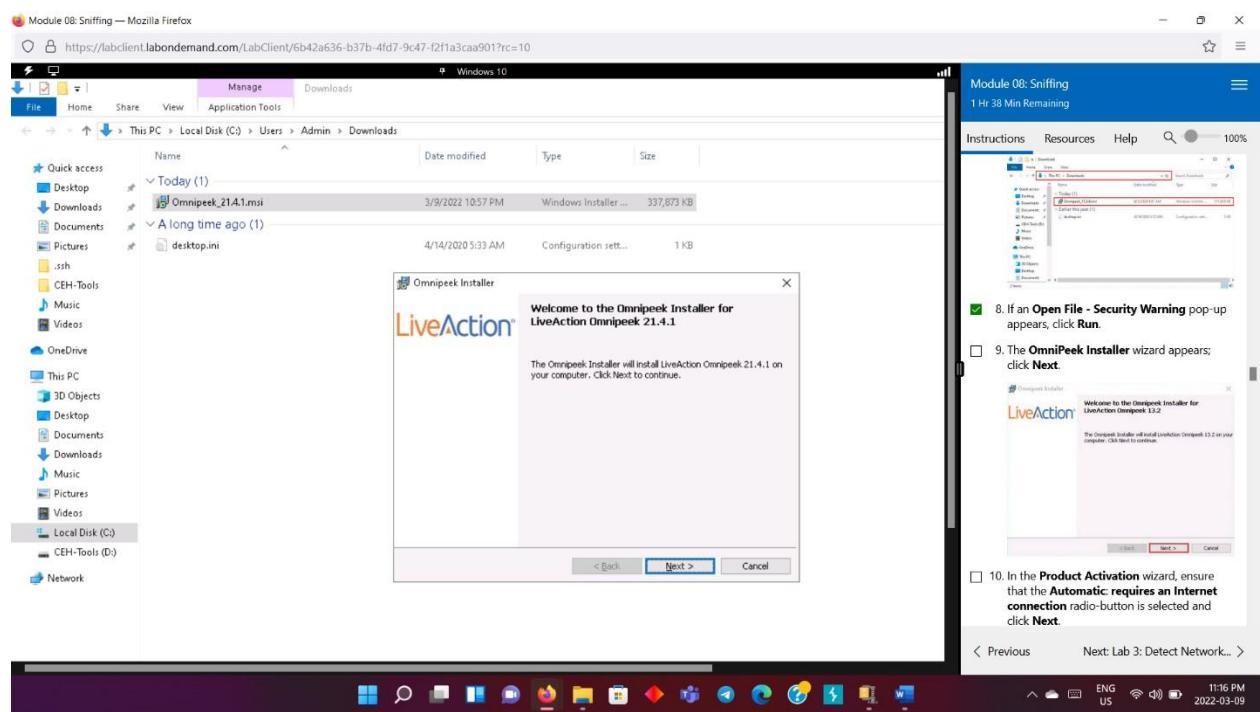


- Double click on the downloaded file to start the installation.

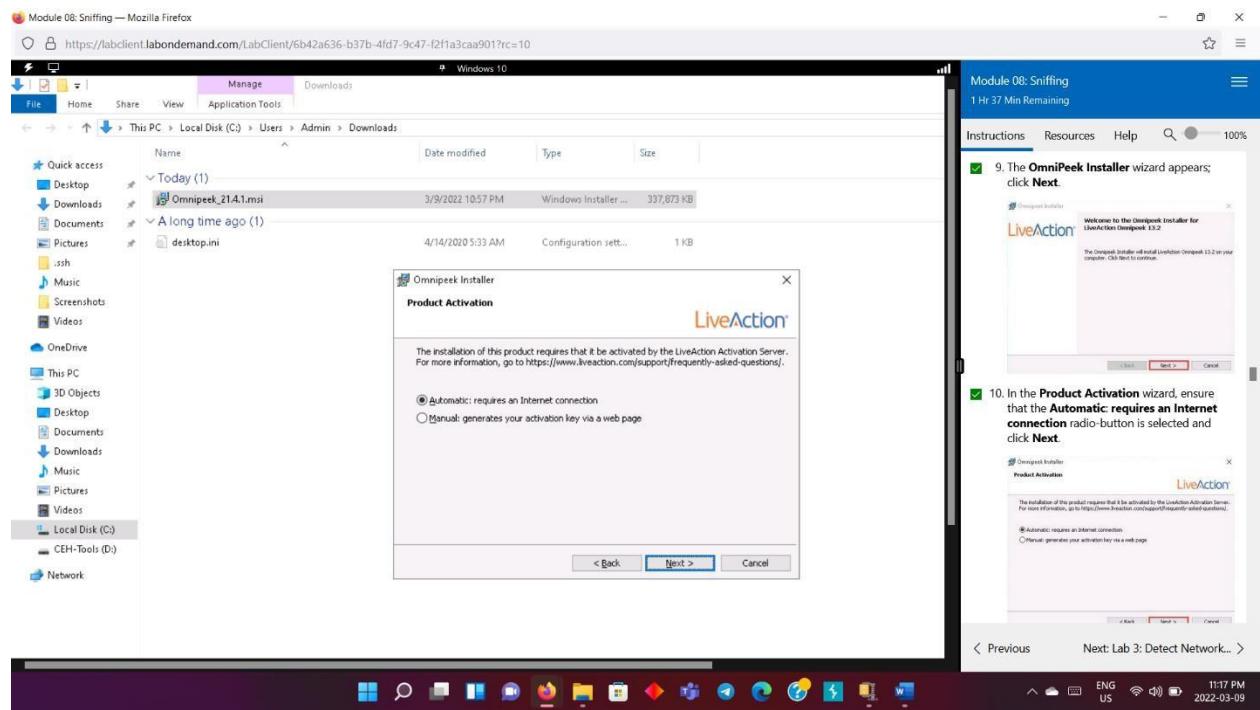




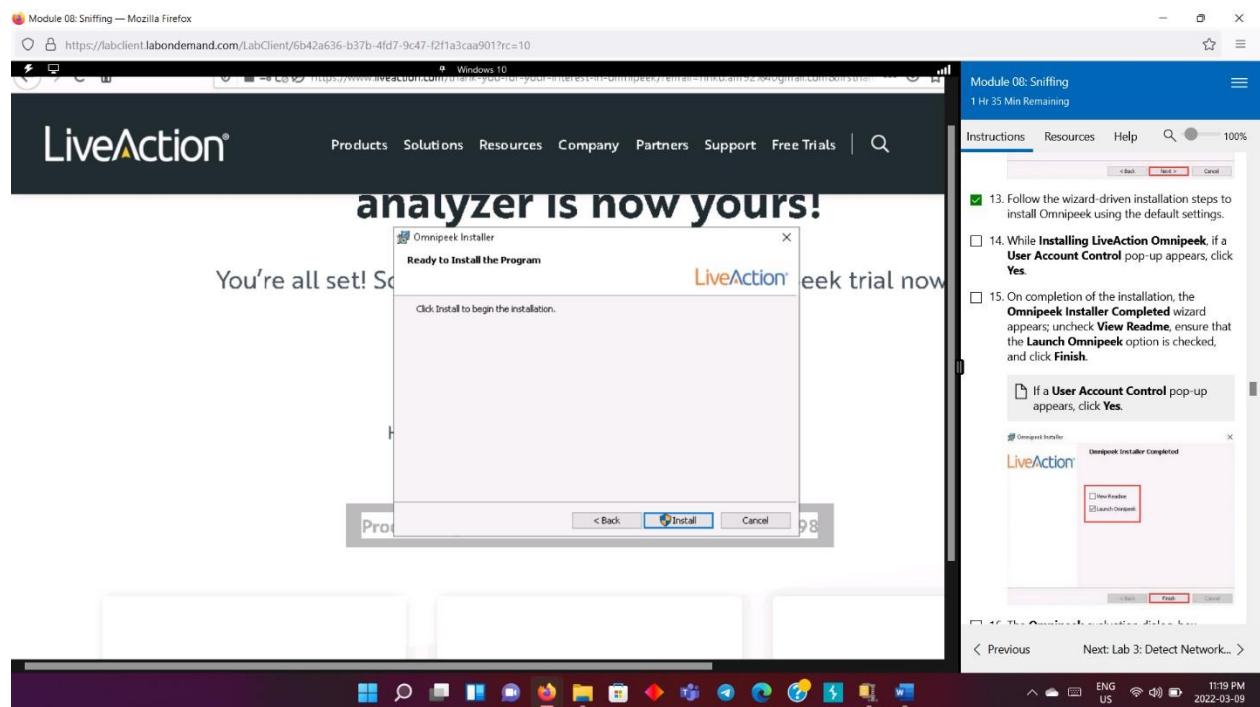
- Click on next and proceed.



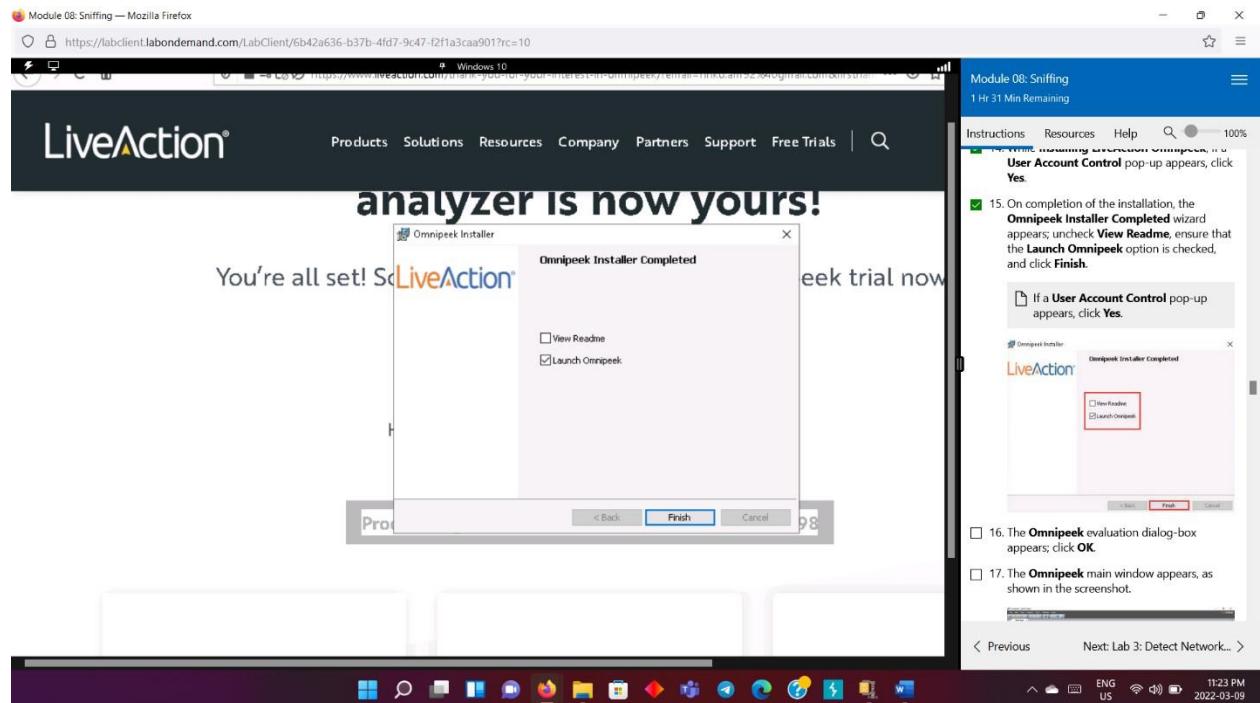
- Select the radio button and click next.



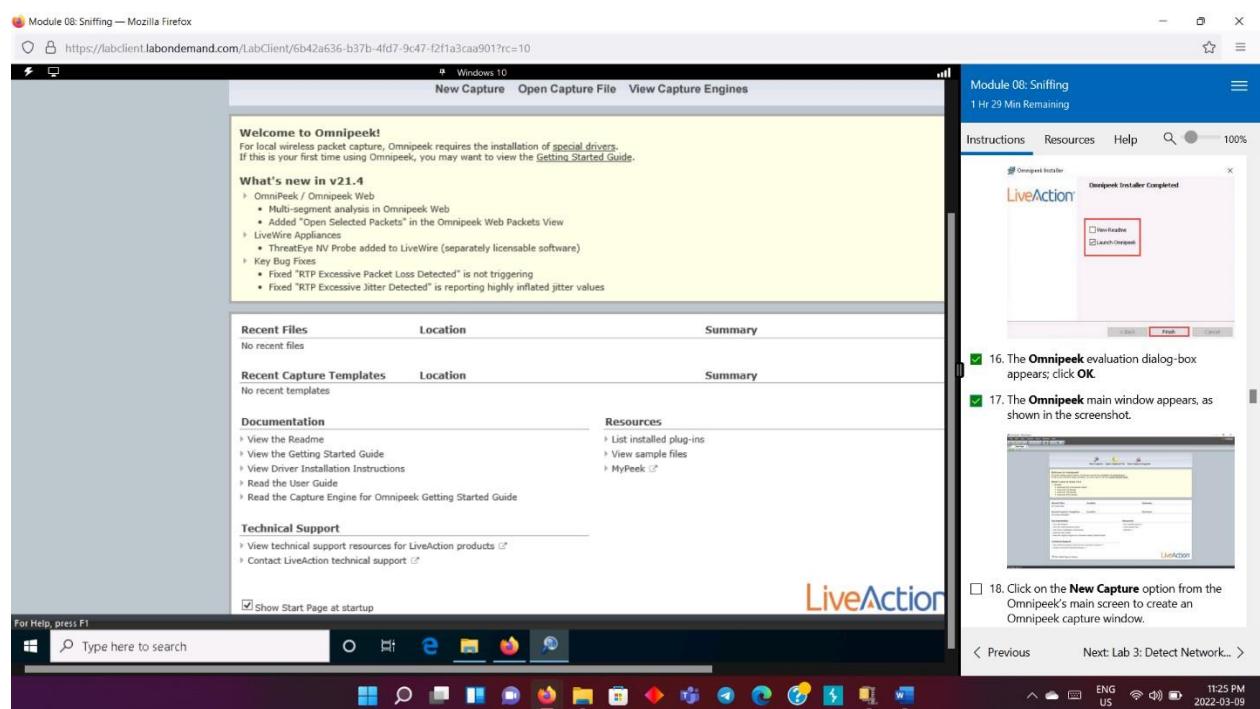
- Copy - paste the license key and click next.



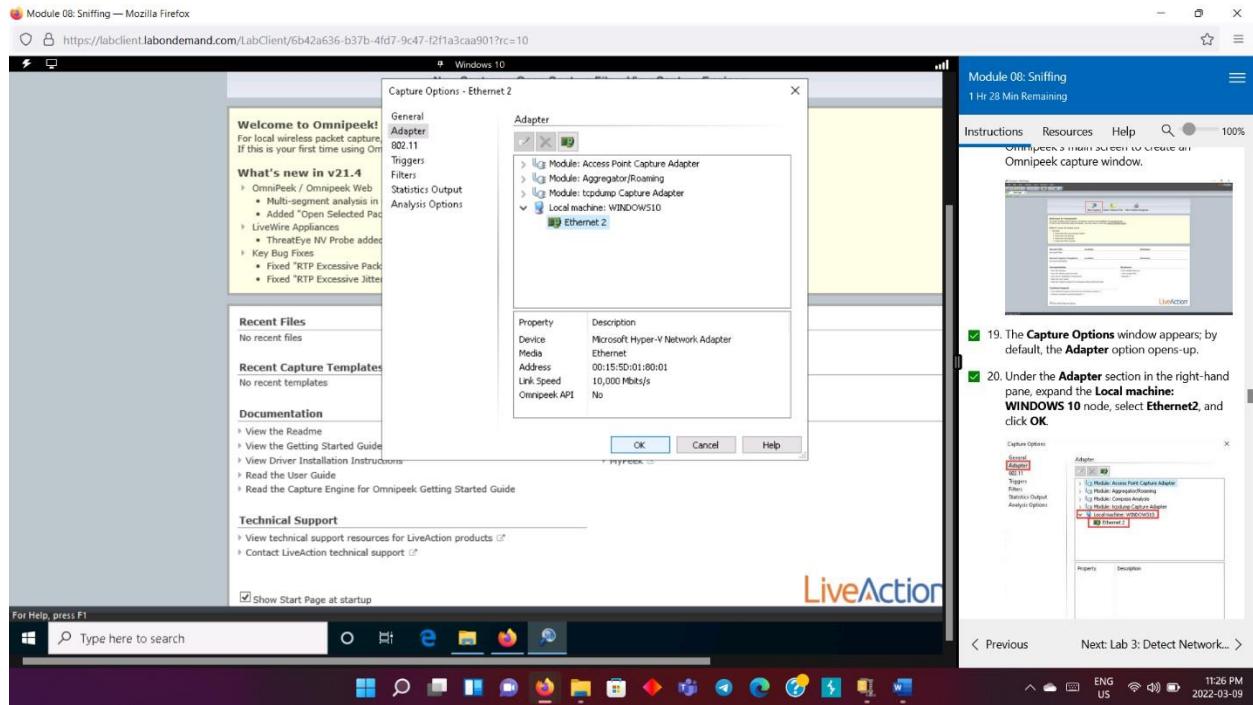
- Once the installation is complete, select the option launch Omnipipek and click on finish button.



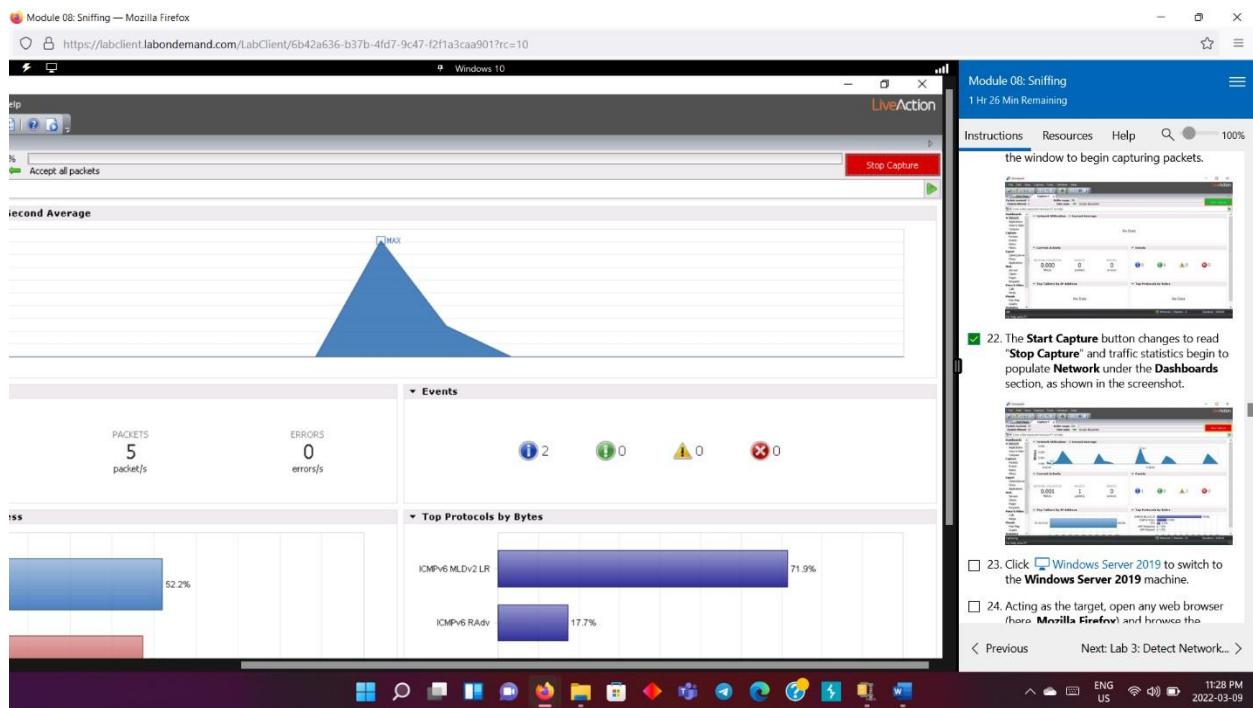
- The Omnipipek window appears.



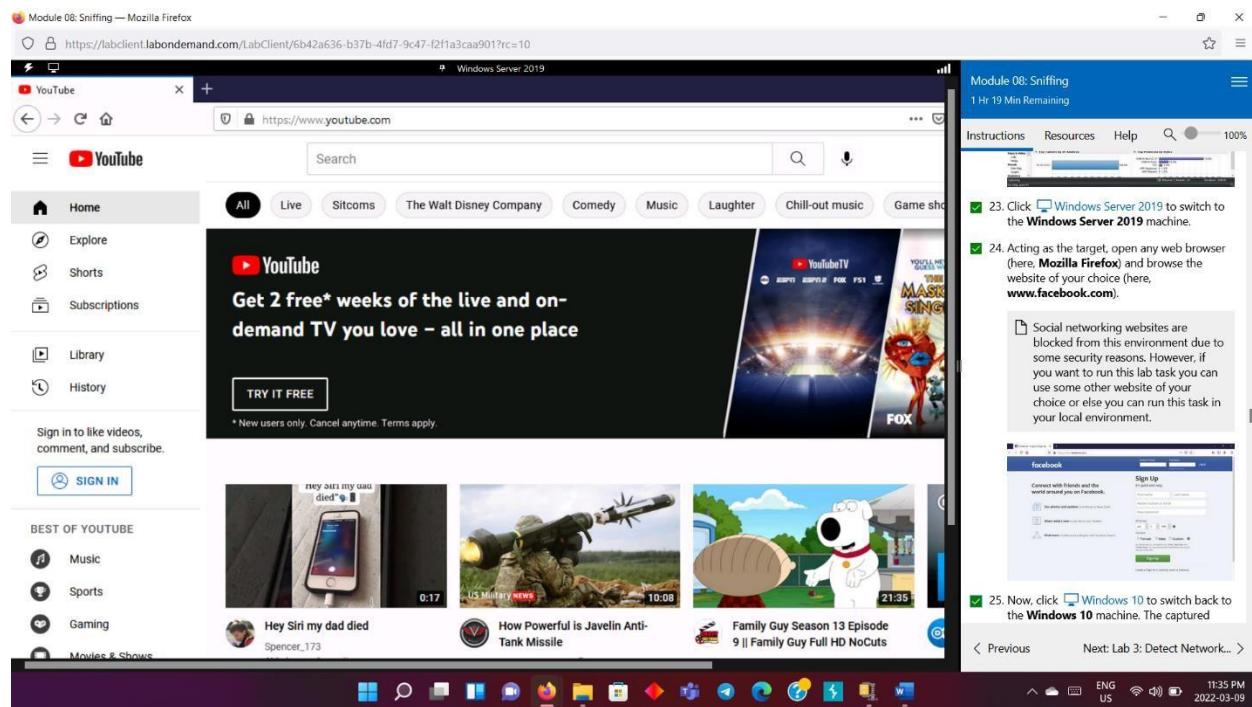
- Now click on the button new capture from the main screen to create a new omnipeek capture window.
 - The adapter option opens. Below the adapter option, expand the local machine: windows 10 node. Then select ethernet 2 and select Ok.



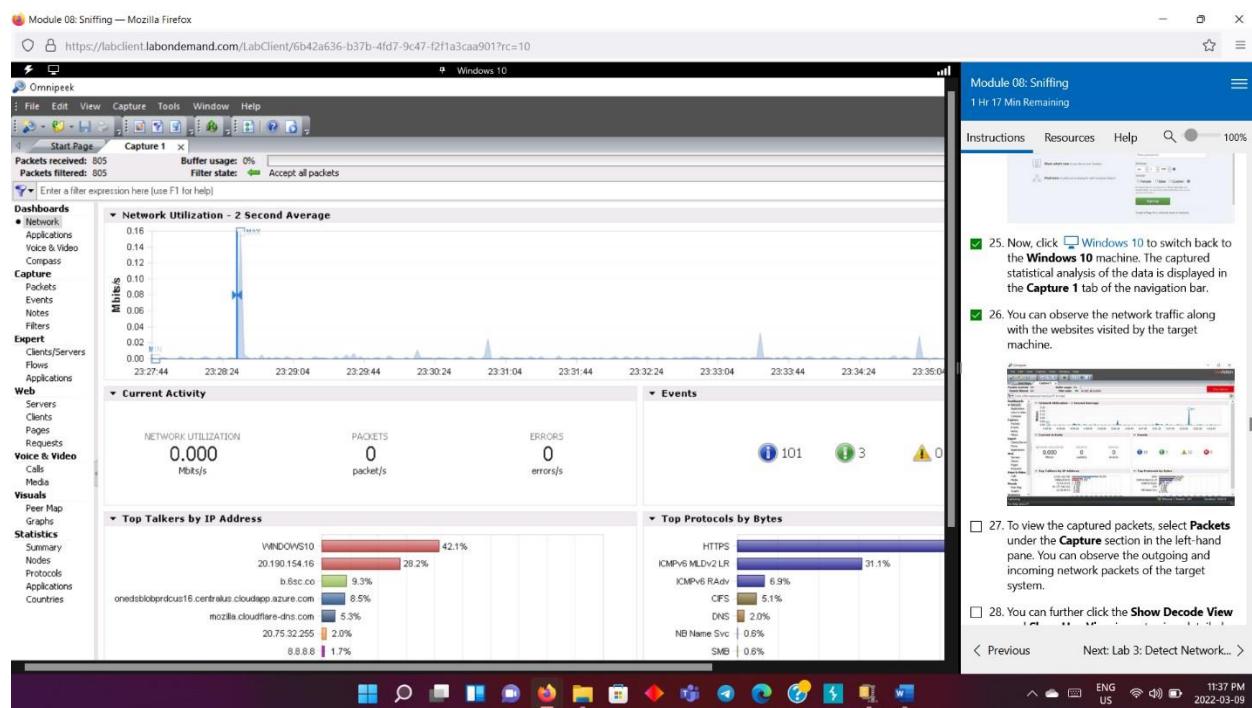
- The capture 1-tab pops up. Now click on the start capture button to start capturing packets.



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.



Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/LabClient/6b42a636-b37b-4fd7-9c47-f2f1a3caa901?rc=10

Windows 10

OmniPeek

Capture 1

Packets received: 1,071 Buffer usage: 0% Filter state: Accept all packets

Enter a filter expression here (use F1 for help)

Dashboards

- Network
- Applications
- Voice & Video
- Compass
- Capture**
 - Packets
 - Events
 - Notes
 - Filters
- Expert
- Clients/Servers
- Flows
- Applications
- Web**
 - Servers
 - Clients
 - Pages
 - Requests
- Voice & Video
- Calls
- Media
- Visuals
- Peer Map
- Graphs
- Statistics**
 - Summary
 - Nodes
 - Protocols
 - Applications
 - Countries

Packet Source Destination Flow ID Flags Size Relative Time Protocol Application Summary

Packet	Source	Destination	Flow ID	Flags	Size	Relative Time	Protocol	Application	Summary
1	fe80::1:1	All ML-Dv2-capabl...			94	0.217614	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
2	fe80::1:1	All Nodes			114	6.897739	ICMPv6 Radv	ICMPv6	Multicast
3	fe80::8567:8114:...	All ML-Dv2-capabl...			94	6.905309	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
4	fe80::cc61:f2c3:...	All ML-Dv2-capabl...			114	6.907074	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
5	fe80::cc61:f2c3:...	All ML-Dv2-capabl...			114	7.075118	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
6	fe80::8567:8114:...	All ML-Dv2-capabl...			94	7.242141	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
7	WINDOWS10	b.6sc.co		1	64	8.346930	HTTPS	SSL	Src=
8	b.6sc.co	WINDOWS10		1	70	8.351037	HTTPS	SSL	Src=
9	fe80::1:1	All Nodes			114	16.509199	ICMPv6 Radv	ICMPv6	Multicast
10	fe80::8567:8114:...	All ML-Dv2-capabl...			94	16.518944	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
11	fe80::cc61:f2c3:...	All ML-Dv2-capabl...			114	16.519152	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
12	fe80::cc61:f2c3:...	All ML-Dv2-capabl...			114	16.571298	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
13	fe80::1:1	All ML-Dv2-capabl...			94	16.617502	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
14	fe80::8567:8114:...	All ML-Dv2-capabl...			94	17.536359	ICMPv6 ML-Dv2 LR	ICMPv6	Multicast
15	WINDOWS10	b.6sc.co		1	64	18.350840	HTTPS	SSL	Src=
16	b.6sc.co	WINDOWS10		1	70	18.351035	HTTPS	SSL	Src=

Module 08: Sniffing
1 Hr 15 Min Remaining

Instructions Resources Help

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

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

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

< Previous Next: Lab 3: Detect Network... >

11:39 PM 2022-03-09

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

Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/LabClient/6b42a636-b37b-4fd7-9c47-f2f1a3caa901?rc=10

Windows 10

OmniPeek

Capture 1

Packets received: 1,145 Buffer usage: 0% Filter state: Accept all packets

Enter a filter expression here (use F1 for help)

Dashboards

- Network
- Applications
- Voice & Video
- Compass
- Capture**
 - Packets
 - Events**
 - Notes
 - Filters
- Expert
- Clients/Servers
- Flows
- Applications
- Web**
 - Servers
 - Clients
 - Pages
 - Requests
- Voice & Video
- Calls
- Media
- Visuals
- Peer Map
- Graphs
- Statistics**
 - Summary
 - Nodes
 - Protocols
 - Applications
 - Countries

Events: 134

Date Time Event

Date	Time	Event
3/9/2022	23:36:38	Expert: TCP Selective ACK (2296109693-2296109694), Packet 765 (184.06.193.166:443 -> 10.10.10.10:50278)
3/9/2022	23:36:48	Expert: TCP Keep-Alive, Packet 778 (10.10.10.10:50278 -> 184.06.193.166:443)
3/9/2022	23:36:50	Expert: TCP Selective ACK, Packet 779 (184.06.193.166:443 -> 10.10.10.10:50278)
3/9/2022	23:37:39	Expert: TCP Keep-Alive, Packet 830 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:37:39	Expert: TCP Keep-Alive ACK, Packet 831 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:38:29	Expert: TCP Selective ACK (1927016998-1927016999), Packet 831 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:38:29	Expert: TCP Selective ACK (1927016998-1927016999), Packet 831 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:38:29	Expert: TCP Selective ACK (1927016998-1927016999), Packet 831 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:38:29	Expert: TCP Port Unreachable, Packet 914 (8.8.8.8:5 -> 10.10.10.10:55001)
3/9/2022	23:38:57	Expert: TCP Keep-Alive ACK, Packet 1,051 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:38:57	Expert: TCP Keep-Alive ACK, Packet 1,051 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:38:57	Expert: TCP Selective ACK (161822258-161822259), Packet 1,051 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:38:57	Expert: TCP Selective ACK (161822258-161822259), Packet 1,051 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:39:11	Expert: TCP Keep-Alive ACK, Packet 1,052 (10.10.10.10:50285 -> 184.06.193.166:443)
3/9/2022	23:39:11	Expert: TCP Keep-Alive ACK, Packet 1,053 (184.06.193.166:443 -> 10.10.10.10:50285)
3/9/2022	23:39:21	Expert: TCP Keep-Alive ACK, Packet 1,054 (10.10.10.10:50285 -> 184.06.193.166:443)
3/9/2022	23:39:21	Expert: TCP Selective ACK (255161516-255161517), Packet 1,054 (184.06.193.166:443 -> 10.10.10.10:50285)
3/9/2022	23:39:21	Expert: TCP Keep-Alive ACK, Packet 1,073 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:39:21	Expert: TCP Keep-Alive ACK, Packet 1,074 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:39:21	Expert: TCP Selective ACK (161822258-161822259), Packet 1,074 (fe80::d59e:e842:b733:20b:445 -> fe80::d59e:e842:b733:20b:445)
3/9/2022	23:39:31	Expert: TCP Keep-Alive ACK, Packet 1,096 (10.10.10.10:50285 -> 184.06.193.166:443)
3/9/2022	23:39:31	Expert: TCP Keep-Alive ACK, Packet 1,097 (184.06.193.166:443 -> 10.10.10.10:50285)
3/9/2022	23:39:31	Expert: TCP Selective ACK (255161516-255161517), Packet 1,097 (184.06.193.166:443 -> 10.10.10.10:50285)
3/9/2022	23:39:37	Expert: TCP Keep-Alive, Packet 1,121 (10.10.10.10:50285 -> 184.06.193.166:443)
3/9/2022	23:39:41	Expert: TCP Keep-Alive ACK, Packet 1,122 (184.06.193.166:443 -> 10.10.10.10:50285)

Module 08: Sniffing
1 Hr 14 Min Remaining

Instructions Resources Help

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

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

< Previous Next: Lab 3: Detect Network... >

11:39 PM 2022-03-09

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

The screenshot shows the NetworkMiner interface. On the left, the 'Expert' section is expanded, showing the 'Clients/Servers' tab. It lists various active systems on the network, such as 'Windows10', 'Windows10.10.10.19', 'Windows10.10.10.255', and 'Windows10.190.154.16'. Below this, the 'Flows and Applications' section is expanded, showing a table of analyzed flows. The table includes columns for Name, Flows, Events, Packets, Bytes, Duration, Avg Response Time, and TCP. The table shows entries for SSL, TCP, and other protocols. At the bottom, there is an 'Event Log' table showing transport layer events like 'TCP Selective ACK' and 'TCP Keep-Alive ACK'.

Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/LabClient/6b42a636-b37b-4fd7-9c47-f2f1a3caa901?rc=10

Packets received: 1,372 Buffer usage: 0% Filter state: Accept all packets

Start Page Capture 1

Dashboards Network Applications Voice & Video Compass Capture Packets Events Notes Filters Expert Clients/Servers Flows Applications Web Services Servers Clients Pages Requests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries

Flows analyzed: 62 Events detected: 151 Packets dropped: 0

Client Addr Server Addr Flows Events Packets Bytes Duration 3-Way Handshake Avg Response Time TCP

Windows10 8.8.8 18 0 40 5,571 0:12:00.038289 0.018714

Windows10 10.10.10.19 1 0 1 108 0.000000

Windows10 10.10.10.255 2 0 4 535 14.707073

Windows10 20.75.32.255 1 0 31 3,466 0:03:47.168532 0.082308

Windows10 onediscordplus4.westus... 1 0 19 9,369 0.119155 0.022243 0.021558

Windows10 20.190.154.16 1 6 33 25,607 0.085978 0.007436 0.019453

Windows10 e15275.q.akamedge.net 1 0 13 5,667 0:01:00.073702 0.002706 0.001627

Windows10 40.83.240.146 2 0 6 851 0:05:55.144537 0.020051

Windows10 g-men-com-rnatec.traffic... 1 3 27 9,199 0.139551 0.007078 0.006543

Windows10 52.11.62.36 1 2 13 1,052 0:10:00.200749 0:03:20.010351

Windows10 wwe2.frontdoor.licensing.c... 1 0 30 14,057 0.095783 0.007053 0.015876

Windows10 104.16.249.249 1 0 95 10,514 0:11:27.704633 0.002713

Windows10 104.96.163.140 2 0 52 27,722 0:01:00.026469 0.002009 0.003074

Windows10 e9659.dspg.akamedge.net 1 0 60 64,639 0.032214 0.002932 0.002277

Windows10 e10603.dsppg.akamedge.net 2 0 20 3,242 0:01:00.064929 0.001067 0.002364

Windows10 1 0 21 12,272 0.292032 0.042810 0.049284

Windows10 onediscordplus16.centra... 1 0 23 9,640 0.025334 0.001407 0.003540

Windows10 safetrowsing.googleapis.c... 1 113 136 19,672 0:12:39.044690 0.003735 0.002752

Windows10 b.6sc.co 4 1 113 136 19,672 0:12:39.044690 0.003735 0.002752

Windows10 cds.ds7q6s2.hwdcn.net 1 3 12 1,245 0:01:00.009063 0.001734 0.004270

mDNS 1 0 2 190 0.001130

SSDP 1 0 3 549 6.001135

Windows10 10.10.10.16 2 0 4 535 0:07:34.754342

Details Event Summary Event Log

Layer Event Count First Time Last Time

Transport TCP Selective ACK 51 3/9/2022 23:27:52 3/9/2022 23:40:31

Transport TCP Keep-Alive ACK 44 3/9/2022 23:28:02 3/9/2022 23:40:32

Transport TCP Keep-Alive 44 3/9/2022 23:28:02 3/9/2022 23:40:32

Module 08: Sniffing

1 Hr 13 Min Remaining

Instructions Resources Help

Enter a filter expression here (use F1 for help)

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

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

31. Similarly, under the **Flows and Applications**

< Previous Next: Lab 3: Detect Network... >

ENG US 2022-03-09 11:40 PM

- Select flows and applications to view the packet flow.

The screenshot shows the NetworkMiner interface. The 'Expert' section is expanded, showing the 'Flows and Applications' tab. It lists various application flows, such as 'SSL', 'TCP', 'HTTP', 'Windows Update', and 'Mozilla'. Below this, the 'Web Services' section is expanded, showing a table of analyzed flows. The table includes columns for Name, Flows, Events, Packets, Bytes, Duration, Avg Response Time, and TCP. The table shows entries for various protocols like SSL, TCP, and HTTP. At the bottom, there is an 'Event Log' table showing transport layer events like 'TCP Selective ACK' and 'TCP Keep-Alive ACK'.

Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/LabClient/6b42a636-b37b-4fd7-9c47-f2f1a3caa901?rc=10

Packets received: 2,266 Buffer usage: 0% Filter state: Accept all packets

Start Page Capture 1

Dashboards Network Applications Voice & Video Compass Capture Packets Events Notes Filters Expert Clients/Servers Flows Applications Web Services Servers Clients Pages Requests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries

Flows analyzed: 76 Events detected: 271 Packets dropped: 0

Name Flows Events Packets Bytes Duration Avg Response Time

SSL 12 199 478 63,024 0:23:48.012384 14.529601

TCP 1 45 72 11,915 0:16:58.707774 0.002751

Office 365 2 9 63 34,998 0:13:27.106081 0.012076

HTTP 1 7 7 448 18.915036

Windows Update 1 3 12 1,245 0:01:00.009063 0.004270

Mozilla 1 3 42 10,851 0:02:50.694440 0.004263

Microsoft 5 2 113 55,505 0:19:16.532920 0.020788

SSDP 1 0 3 549 6.001135

NetBIOS NS 4 0 11 1,068 0:07:20.908105

MSN 4 0 72 24,964 0:01:00.060429 0.003497

MDNS 4 0 8 776 0.001562

LMMR 9 0 11 990 0:04:57.023754

Google APIs 1 0 36 10,655 0:02:51.008759 0.003226

DNS 24 0 52 7,041 0:21:16.335995 0.018166

CFPS 3 0 7 1,738 0:12:28.061011

Bonjour 2 0 2 202 0.002107

Details Event Summary Event Log

Layer Event Count First Time Last Time

Transport TCP Selective ACK 90 3/9/2022 23:27:52 3/9/2022 23:51:40

Transport TCP Keep-Alive ACK 79 3/9/2022 23:28:02 3/9/2022 23:51:40

Transport TCP Keep-Alive 79 3/9/2022 23:28:02 3/9/2022 23:51:40

Module 08: Sniffing

1 Hr 2 Min Remaining

Instructions Resources Help

Enter a filter expression here (use F1 for help)

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

32. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.

33. Expand client nodes (here, **WINDOWS10**) and click on any packet to view its detailed information under the **Details** tab in the lower section of the window.

< Previous Next: Lab 3: Detect Network... >

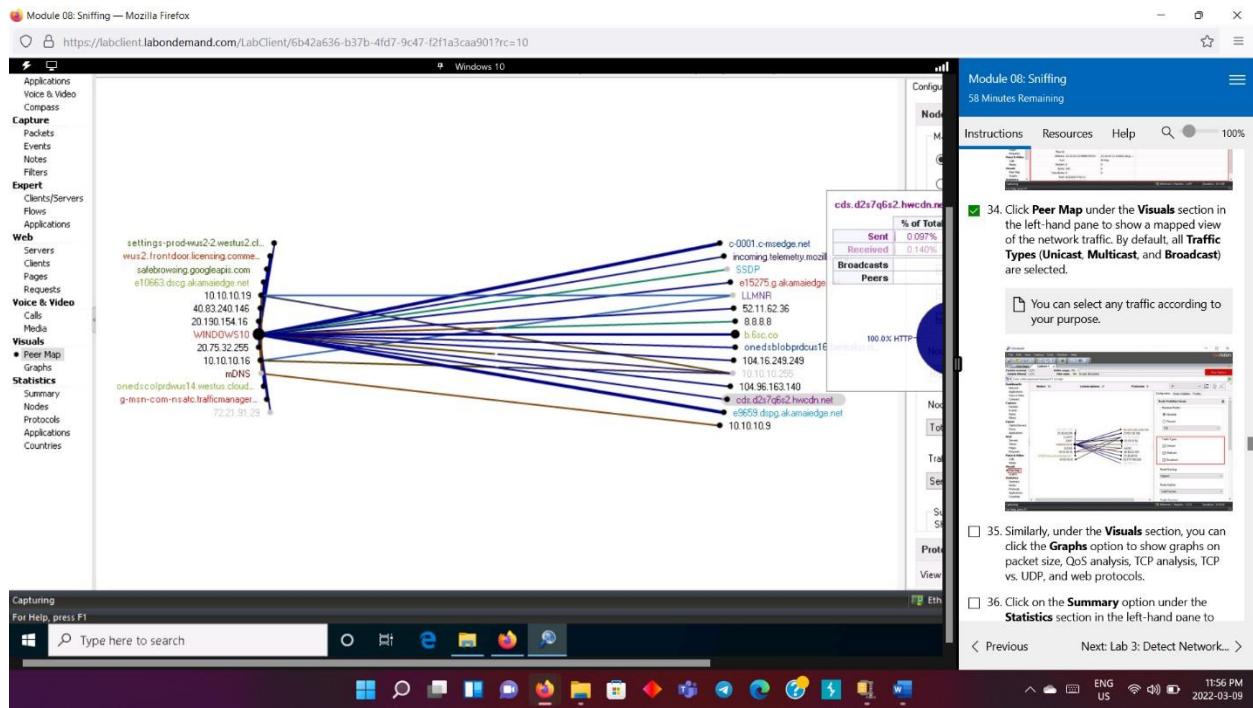
ENG US 2022-03-09 11:51 PM

The screenshot shows the NetworkMiner interface. On the left, the navigation pane includes sections like Dashboards, Applications, Web, and Visuals. The main area displays a table of captured packets with columns for Name, Request ID, Client Addr, Response Code, Response Text, Content-Type, and Host. A specific packet is selected, showing its details in a tabular format with rows for Client and Server, and sub-rows for URI/Host, Response Code, and Referrer. The status bar at the bottom right indicates the date and time as 2022-03-09 11:53 PM.

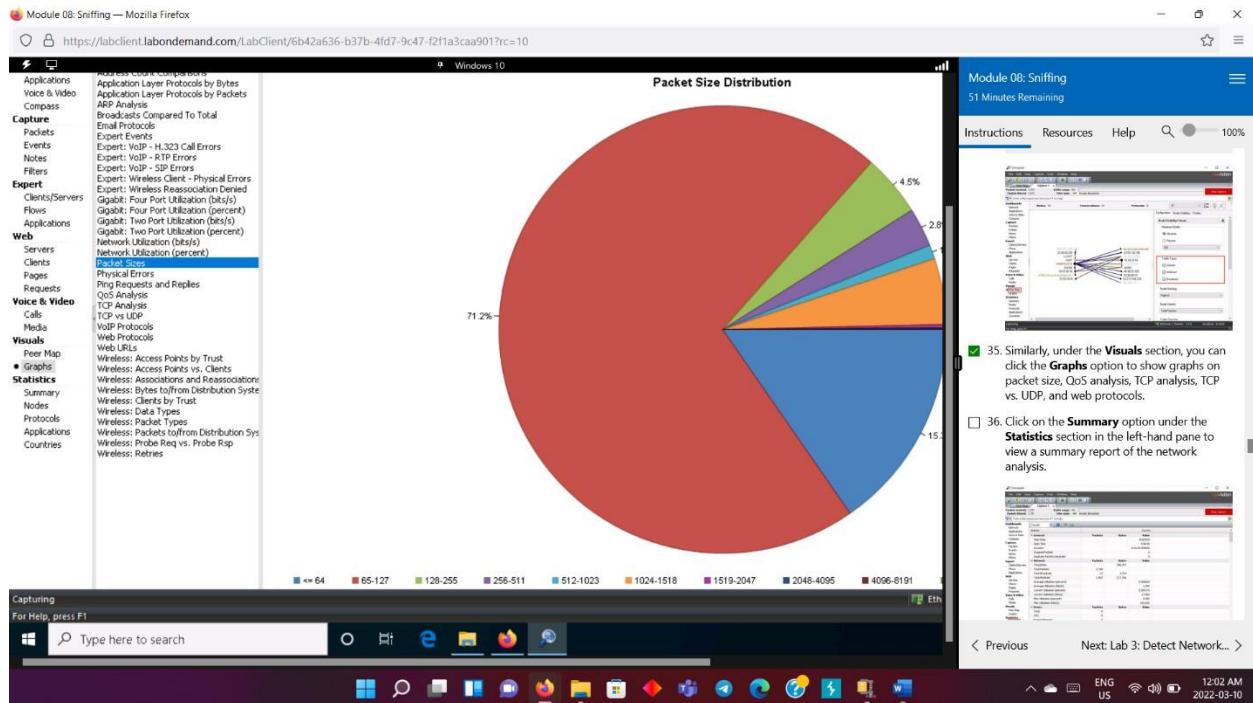
- Choose any packet to get the detailed information.

This screenshot is nearly identical to the first one, showing the NetworkMiner interface with captured traffic. The main difference is that a different packet is selected in the list, specifically a Microsoft Edge update request. The detailed view below shows the client's request for the update file and the server's response. The status bar at the bottom right indicates the date and time as 2022-03-09 11:53 PM.

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.

The screenshot shows a Windows 10 desktop with the NetworkMiner application open. The left pane displays a hierarchical tree of network monitoring categories: Applications, Voice & Video, Capture, Events, Notes, Filters, Export, Web, Servers, Clients, Pages, Requests, Voice & Video, Calls, Media, Visuals, Errors, and Counts. The right pane shows a detailed table of captured packets, bytes, and values. A summary report is visible in the top right corner.

Capture

	Packets	Bytes	Value
Start Date			3/9/2022
Start Time			23:27:44
Duration			0:35:25.000000
Dropped Packets			0
Duplicate Packets Discarded			0

Network

	Packets	Bytes	Value
Total Bytes		567,023	
Total Packets	3,094		
Total Broadcast	29	4,399	
Total Multicast	1,727	179,171	

Errors

	Packets	Bytes	Value
Total	0		
CRC	0		
Frame Alignment	0		
Runt	0		
Oversize	0		

Counts

	Packets	Bytes	Value
Physical Addresses		17	
IP Addresses		29	
IPv6 Addresses		13	
Protocols		27	
Applications		19	
Countries		5	
Files		0	

Size Distribution

	Packets	Bytes	Value
<= 64	469		
65-127	2,215		

Module 08: Sniffing
51 Minutes Remaining

Instructions Resources Help 100%

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

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

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

Capturing
For Help, press F1

Type here to search

Eth

12:03 AM
ENG US

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

Module 08: Sniffing — Mozilla Firefox

https://fabclient.labondemand.com/LabClient/6b42a636-b37b-4fd7-9c47-f2f1a3caa901?rc=10

Windows 10

OmniPeek

Packets received: 3,125 Buffer usage: 0% Filter state: Accept all packets

Start Page Capture x

Enter a filter expression here (use F1 for help)

Dashboards

- Network
- Applications
- Voice & Video
- Compass
- Capture

 - Packets
 - Events
 - Notes
 - Filters

- Expert

 - Clients/Servers
 - Flows
 - Applications

- Web

 - Servers
 - Clients
 - Pages
 - Requests

- Voice & Video

 - Calls
 - Media

- Visuals

 - Peer Map
 - Graphs

- Statistics

 - Summary
 - Nodes
 - Protocols
 - Applications
 - Countries

Counts

Statistic	Current
General	
Start Date	3/9/2022
Start Time	23:27:44
Duration	0:36:08.000000
Dropped Packets	0
Duplicate Packets Discarded	0
Network	
Total Bytes	570,177
Total Packets	3,125
Total Broadcast	29
Total Multicast	1,756
Average Utilization (percent)	
Current Utilization (bits/s)	
Current Utilization (percent)	
Max Utilization (percent)	
Max Utilization (bits/s)	
Errors	
Total	0
CRC	0
Frame Alignment	0
Runt	0
Oversize	0
Counts	
Physical Addresses	17
IP Addresses	29
IPv6 Addresses	13
Protocols	27
Applications	19

Save Report

Report type: Full PDF Report

Report folder: C:\Users\Admin\Documents\Reports\Capture 1

Report description

For reports on Summary Statistics, Node Statistics, Protocol Statistics, Node/Protocol Detail Statistics, Export Stream and Application Statistics, Voice and Video, Wireless Node and Channels Statistics, and graphs.

Save Cancel Help

Module 08: Sniffing
50 Minutes Remaining

Instructions Resources Help Report... to save the report.

39. The Save Report window appears; under the Report folder field, click the ellipse icon to change the download location.

Save Report

Report type: Full PDF Report

Report folder: C:\Users\Admin\Documents\Reports\Capture 1

Report description

For reports on Summary Statistics, Node Statistics, Protocol Statistics, Node/Protocol Detail Statistics, Export Stream and Application Statistics, Voice and Video, Wireless Node and Channels Statistics, and graphs.

Save Cancel Help

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

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

< Previous Next: Lab 3: Detect Network... >

ENG US 12:04 AM 2022-03-10

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

Module 08: Sniffing — Mozilla Firefox

Report.pdf - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools Report.pdf x

Bookmarks

- Omnipeek Report
- Statistics
- Expert
- Graphs

Omnipeek Report: 3/10/2022 0:05:19

Start: 3/9/2022 23:27:44, Duration: 0:36:08

Total Bytes: 570177, Total Packets: 3125

Packet Size Distribution

Size Range	Percentage
0-128	71.0%
129-256	15.1%
257-512	4.6%
513-1024	0.2%
1025-2048	4.0%
2049-4096	1.2%
4097-8192	0.4%
8193-16384	0.2%
16385-32768	0.2%
32769-65536	0.2%
65537-131072	0.2%
131073-262144	0.2%
262145-512000	4.4%

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

Module 08: Sniffing 48 Minutes Remaining

Instructions Resources Help

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

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

44. This concludes the demonstration of analyzing a network using the Omnipacket Network Protocol Analyzer.

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

Previous Next: Lab 3: Detect Network... >

12:05 AM 2022-03-10

Module 08: Sniffing — Mozilla Firefox

Report.pdf - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools Report.pdf x

Bookmarks

- Omnipeek Report
- Statistics
- Expert
- Graphs

Summary Statistics: Reported 3/10/2022 0:05:19

Name	Bytes	Packets	Pct of Bytes	Pct of Packets
Group: Expert				
ICMP Host Unknown	0	0	0	0
ICMP Net Unreachable TOS	0	0	0	0
ICMP Host Unreachable TOS	0	0	0	0
ICMP Comm Admin Prohibited	0	0	0	0
ICMP Host Precedence Violation	0	0	0	0
ICMP Precedence Cutoff	0	0	0	0
ICMP Host Redirect	0	0	0	0
ICMP Host TOS Redirect	0	0	0	0
ICMP TTL Exceeded	0	0	0	0
ICMP Fragmentation Time Exceeded	0	0	0	0
ICMP Parameter Problem	0	0	0	0
ICMP Obsolete Message	0	0	0	0
802.1X Dictionary Attack	0	0	0	0
ARP Request Storm	0	0	0	0
Broadcast Storm	0	0	0	0
Multicast Storm	0	0	0	0
Severe Broadcast Storm	0	0	0	0
Severe Multicast Storm	0	0	0	0
Spanning Tree Topology Change	0	0	0	0
EAP Authentication Failure	0	0	0	0
Too Many Physical Errors	0	0	0	0

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

Module 08: Sniffing 47 Minutes Remaining

Instructions Resources Help

44. This concludes the demonstration of analyzing a network using the Omnipacket Network Protocol Analyzer.

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

Task 3: Analyze a Network using the SteelCentral Packet Analyzer

SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

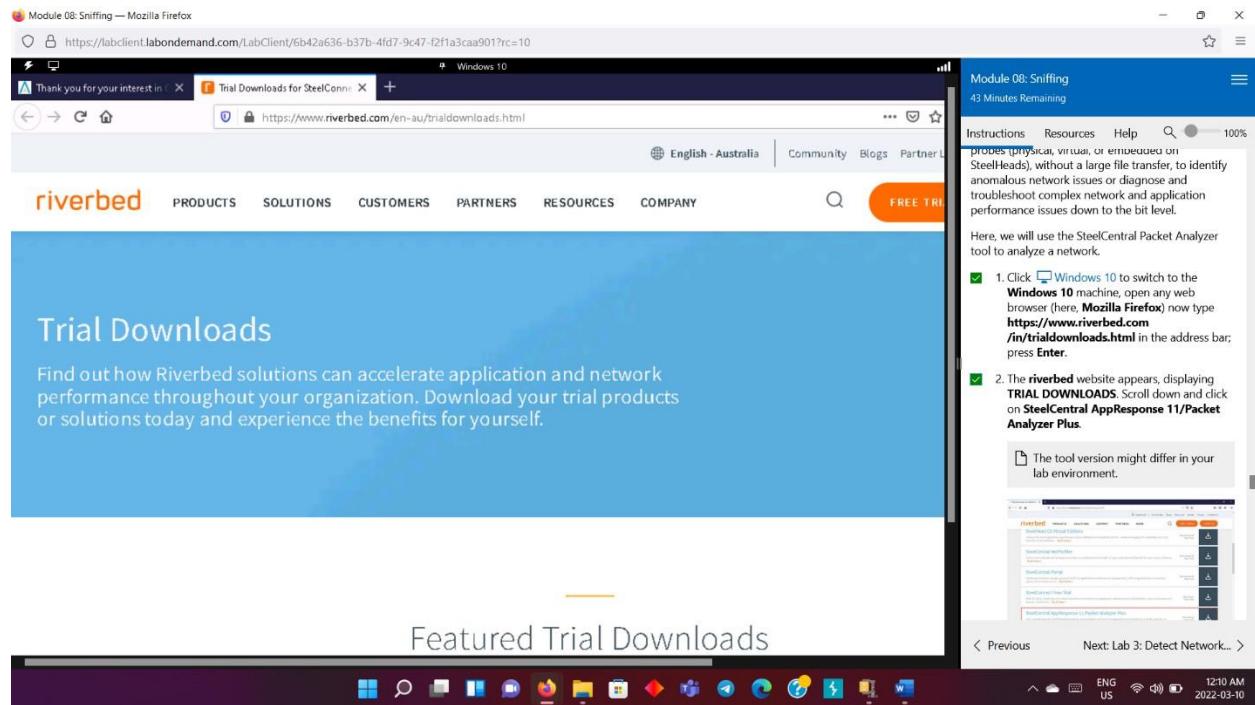
Here, we will use the SteelCentral Packet Analyzer tool to analyze a network.

Previous Next: Lab 3: Detect Network... >

12:07 AM 2022-03-10

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.



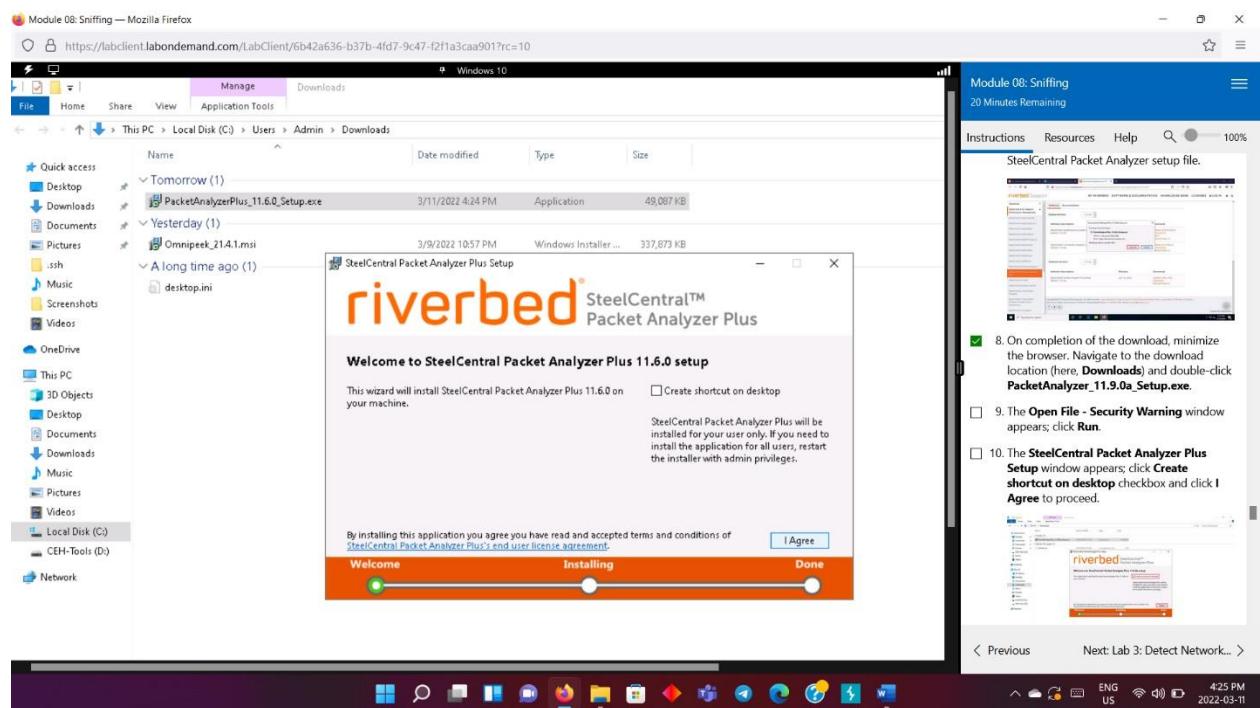
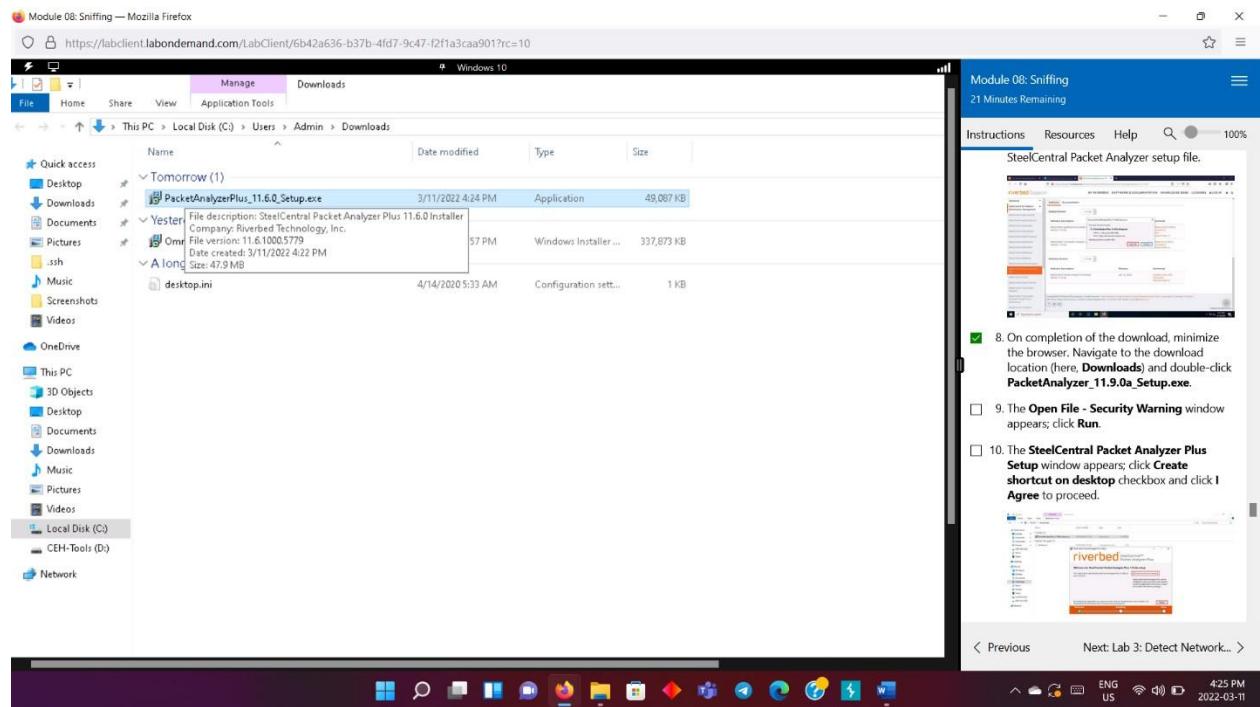
- The website launches, select steel central packet analyzer. Now fill the form and click on submit.

The screenshot shows a Windows 10 desktop with two Firefox browser windows open. The left window displays the Riverbed AppResponse trial download page at <https://www.riverbed.com/en-au/forms/trial-downloads/appresponse11-trial.html>. It features a registration form with fields for First Name, Last Name, Work Email, Company, Job Level, Job Function, Telephone, and Country. The right window shows a 'Module 08: Sniffing' lab guide titled '40 Minutes Remaining'. Step 3 shows a screenshot of the registration form with the instruction: 'A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.' Step 4 shows a screenshot of a 'Please verify your email address' pop-up with the instruction: 'Here, you must give your work email to create an account.' The taskbar at the bottom shows various pinned icons.

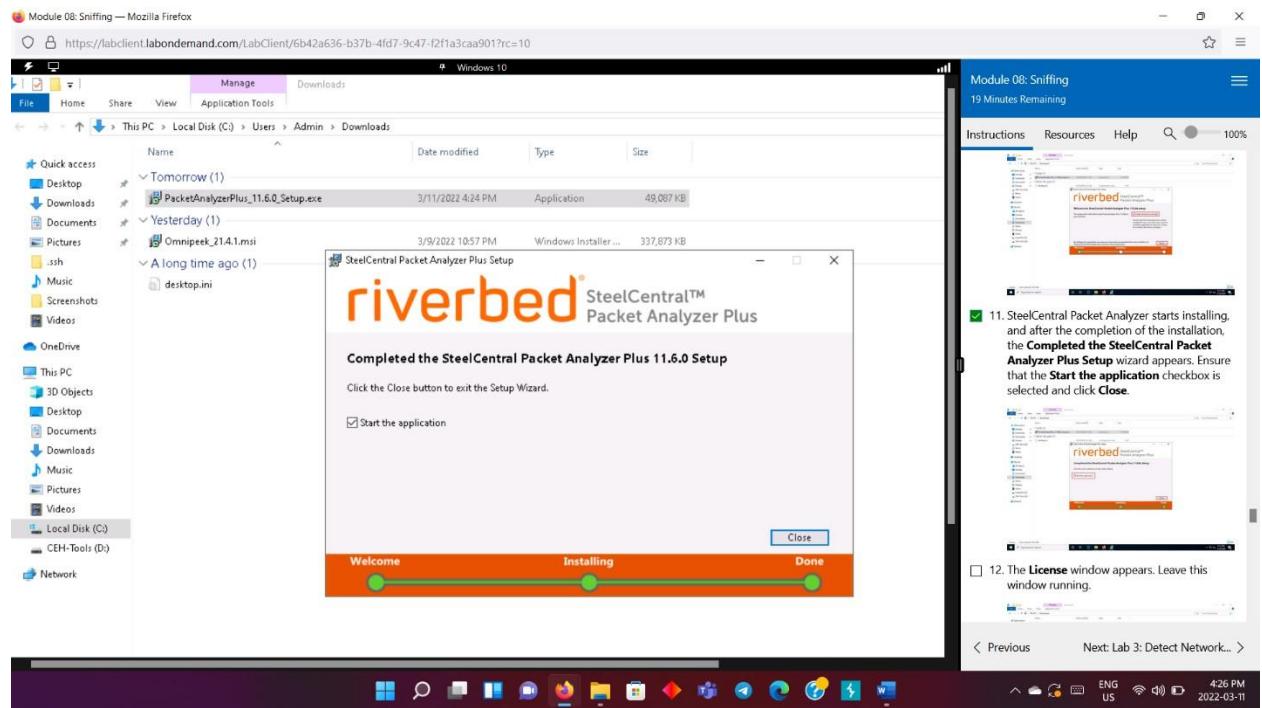
Confirm the email address. Launch the email received and select the link to download the software.

The screenshot shows a Windows 10 desktop with a Firefox browser window and a 'Module 08: Sniffing' lab guide. The browser window shows a 'riverbed Support' page with a 'Did you find what you were looking for?' section and support contact options. A file download dialog is open, prompting to save 'PacketAnalyzerPlus_11.6.0_Setup.exe' from 'https://download.riverbed.com'. The right window shows a 'Module 08: Sniffing' lab guide titled '22 Minutes Remaining'. Step 5 shows a 'Thank You' webpage with the instruction: 'A Thank You webpage appears with information regarding the trial version.' Step 6 shows a screenshot of a 'SteelCentral Application Performance Test' interface with the instruction: 'Open a new tab and log in to the email account you provided during registration. Open the email from **Riverbed Evaluation License Request for SteelCentral AppResponse Virtual**, and click the **Software** link to download SteelCentral Packet Analyzer.' The taskbar at the bottom shows various pinned icons.

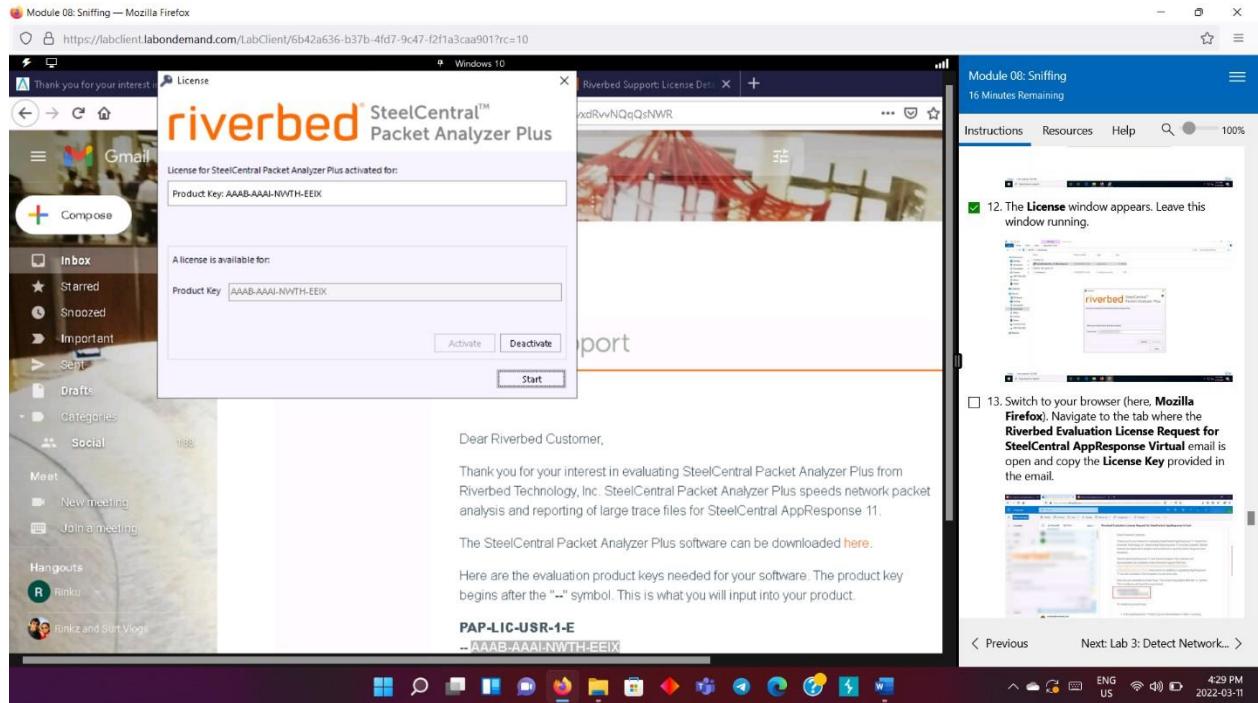
- The exe file pops up, save the file in the folder.



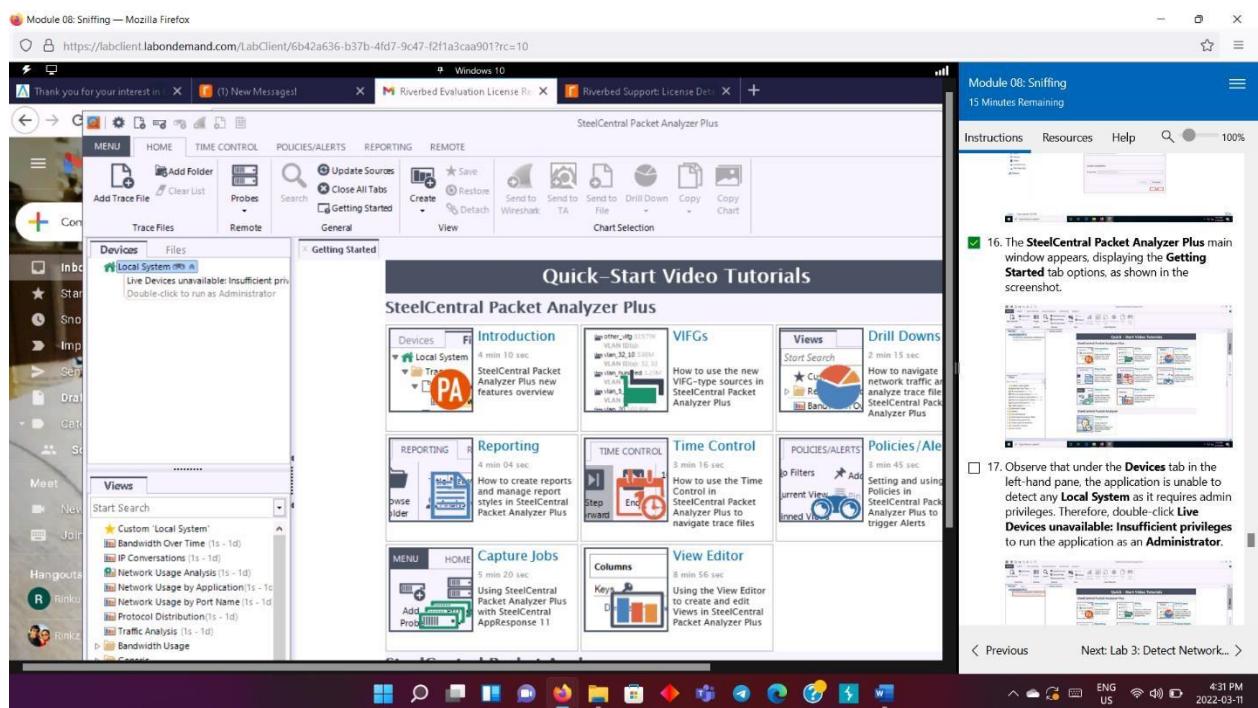
- Once the installation is complete, check the start the application option and click on close button.



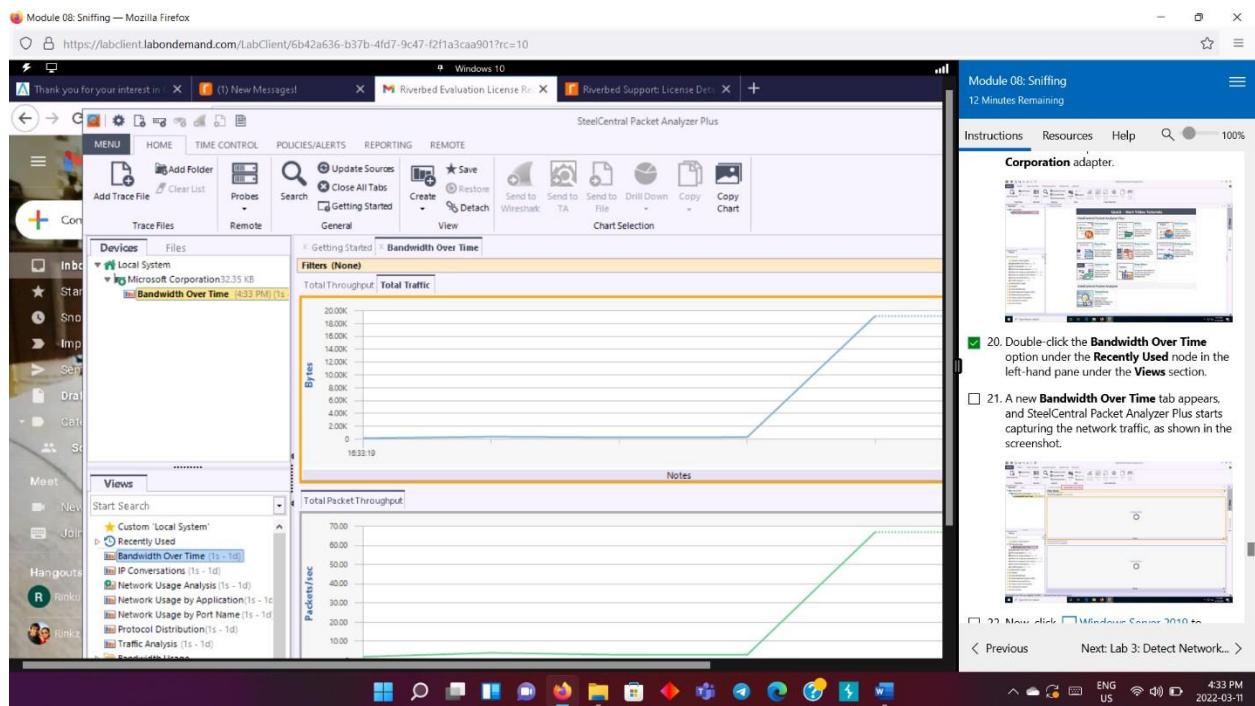
Copy & paste the license key from the email received and then click on the activate button.



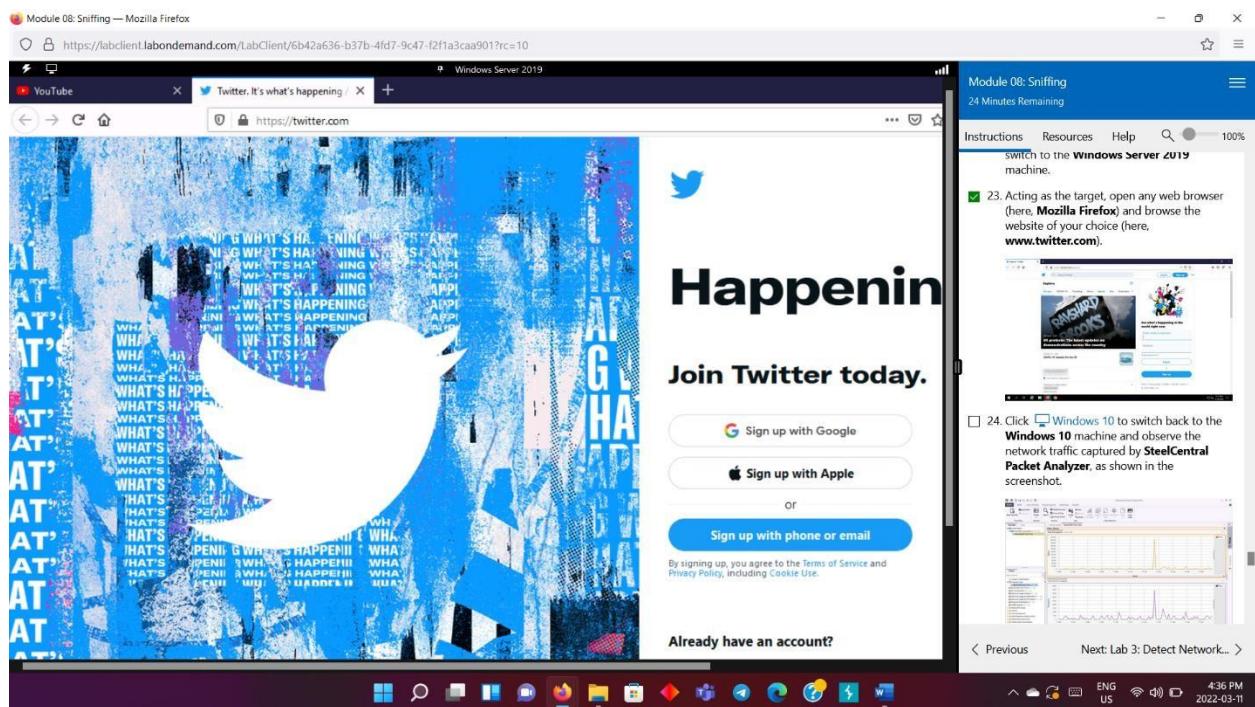
- Click on start button to start the application.



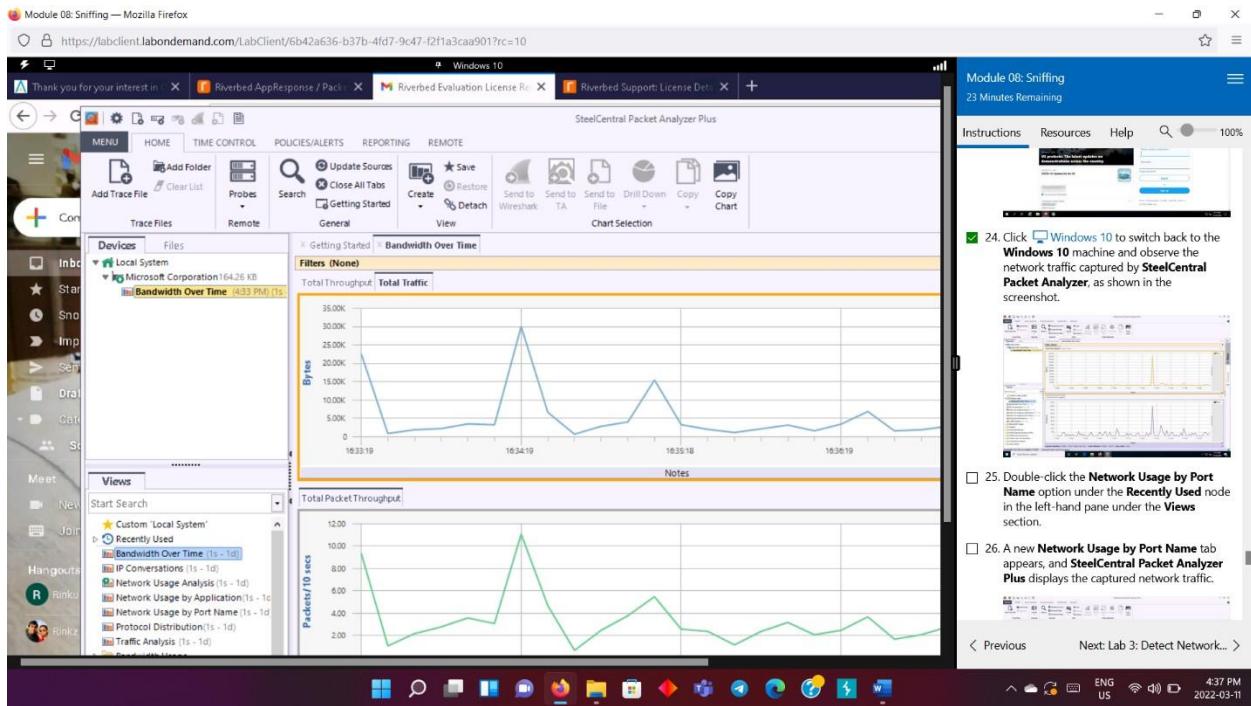
Run the application as administrator by double clicking the live devices unavailable: insufficient privileges. Select Microsoft corporation under ethernet. The bandwidth over time tab appears, now it starts capturing network traffic.



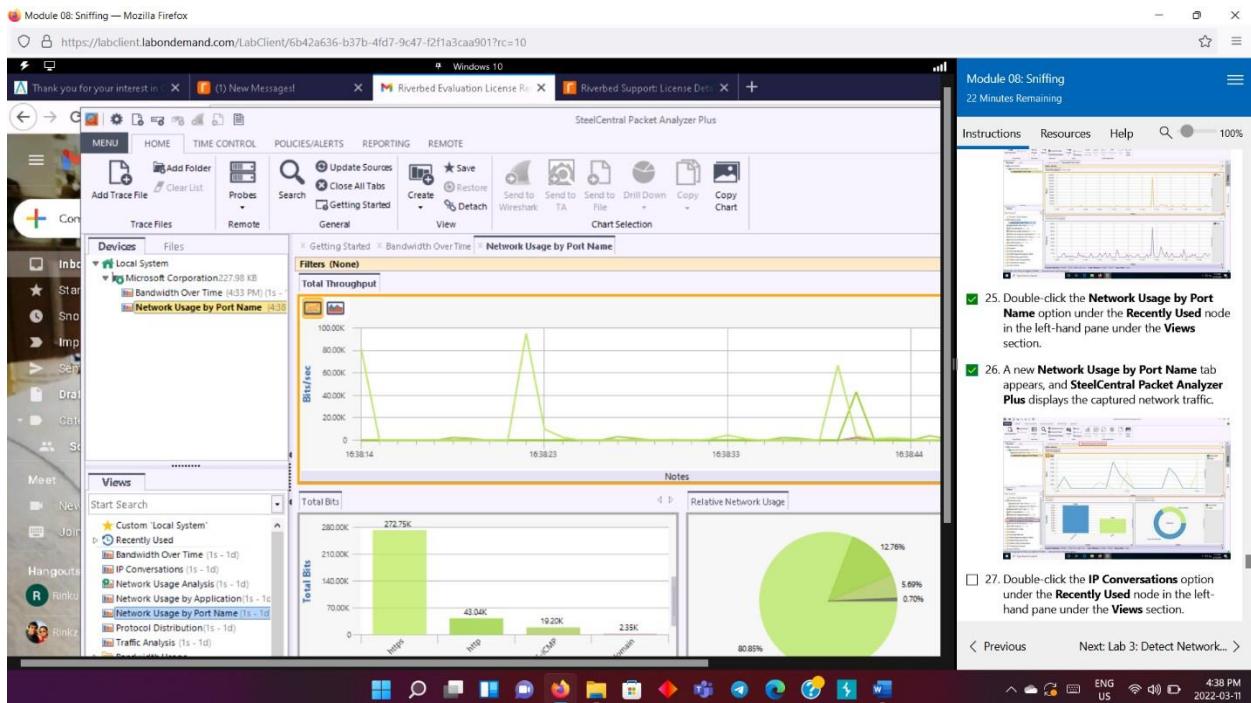
- Switch back to windows server 2019, since the machine acts as the target, launch any web browser and search for twitter.



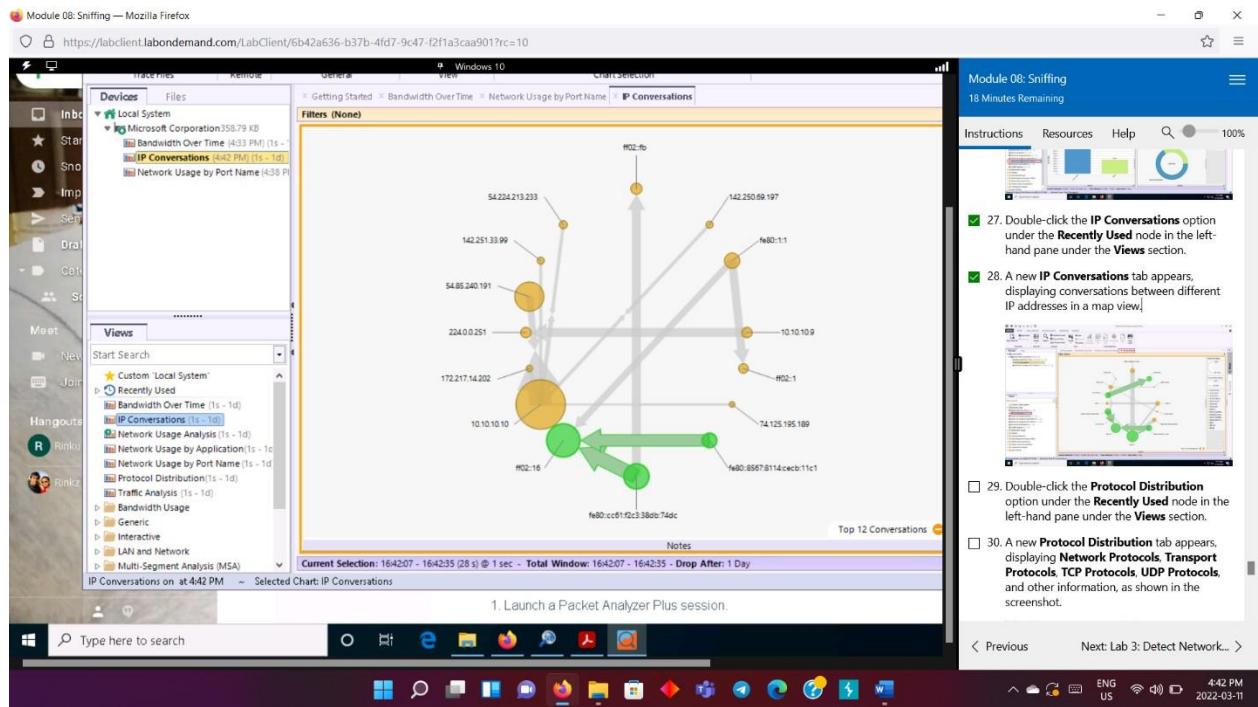
Go back to windows 10 OS and observe the packets captured.



- 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.

Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/labClient/6b42a636-b37b-4fd7-9c47-f2f1a3caa901?rc=10

Protocol Distribution

Network Protocols - Bits

Protocol	Value
64.19K	
5.52K	
0.072	

Transport Protocols - Bits

Protocol	Value
64.19K	
0.072	

TCP Protocols - Bits

Protocol	Value
63.62K	
52B	

UDP Protocols - Bits

Protocol	Value
52B	

Protocol Distribution on at 4:43 PM ~ Selected Chart: Network Protocols - Bits

1. Launch a Packet Analyzer Plus session.

Module 08: Sniffing
17 Minutes Remaining

Instructions Resources Help

29. Double-click the **Protocol Distribution** option under the **Recently Used** node in the left-hand pane under the **Views** section.

30. A new **Protocol Distribution** tab appears, displaying **Network Protocols**, **Transport Protocols**, **TCP Protocols**, **UDP Protocols**, and other information, as shown in the screenshot.

31. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.

32. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.

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

< Previous Next: Lab 3: Detect Network... >

4:43 PM 2022-03-11

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.

Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/labClient/6b42a636-b37b-4fd7-9c47-f2f1a3caa901?rc=10

Capture Summary

Statistic Name	Value
Total Number of Bytes	631
Total Number of Packets	7
Number IP Bytes	631
Number TCP Bytes	121
Number UDP Bytes	0

Capture Summary on at 4:44 PM ~ Selected Chart: Capture Summary

1. Launch a Packet Analyzer Plus session.

Module 08: Sniffing
16 Minutes Remaining

Instructions Resources Help

31. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.

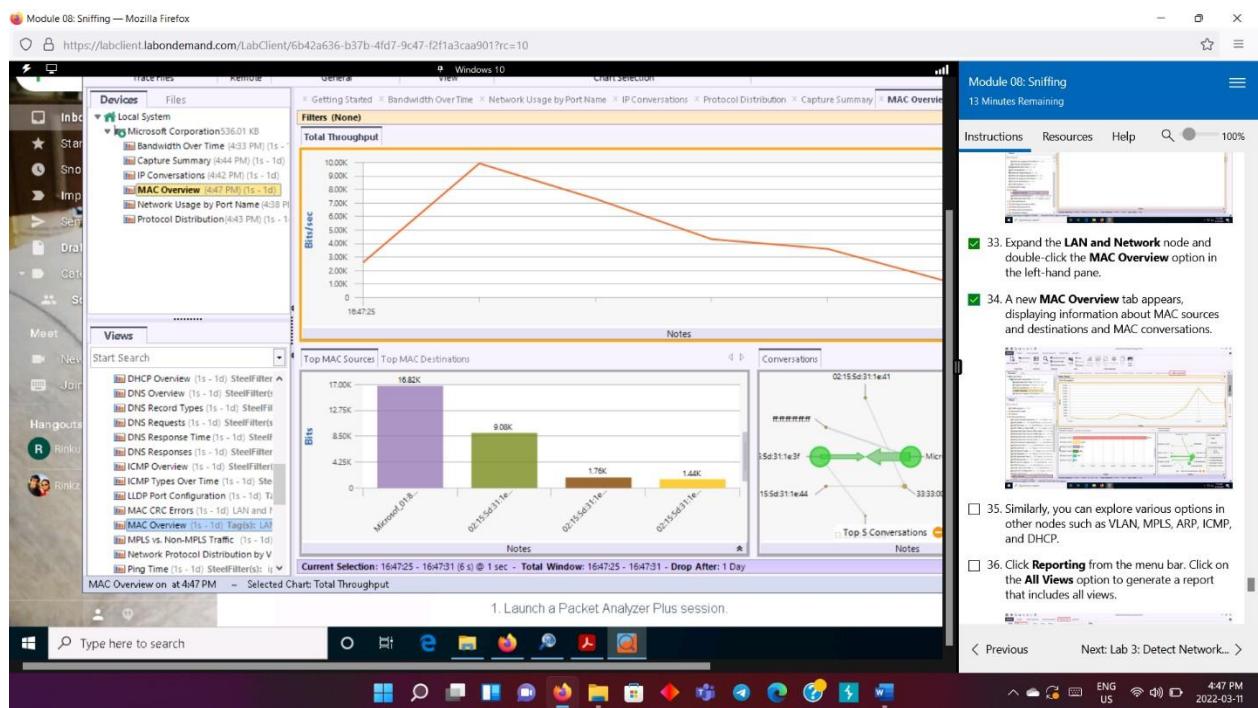
32. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.

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

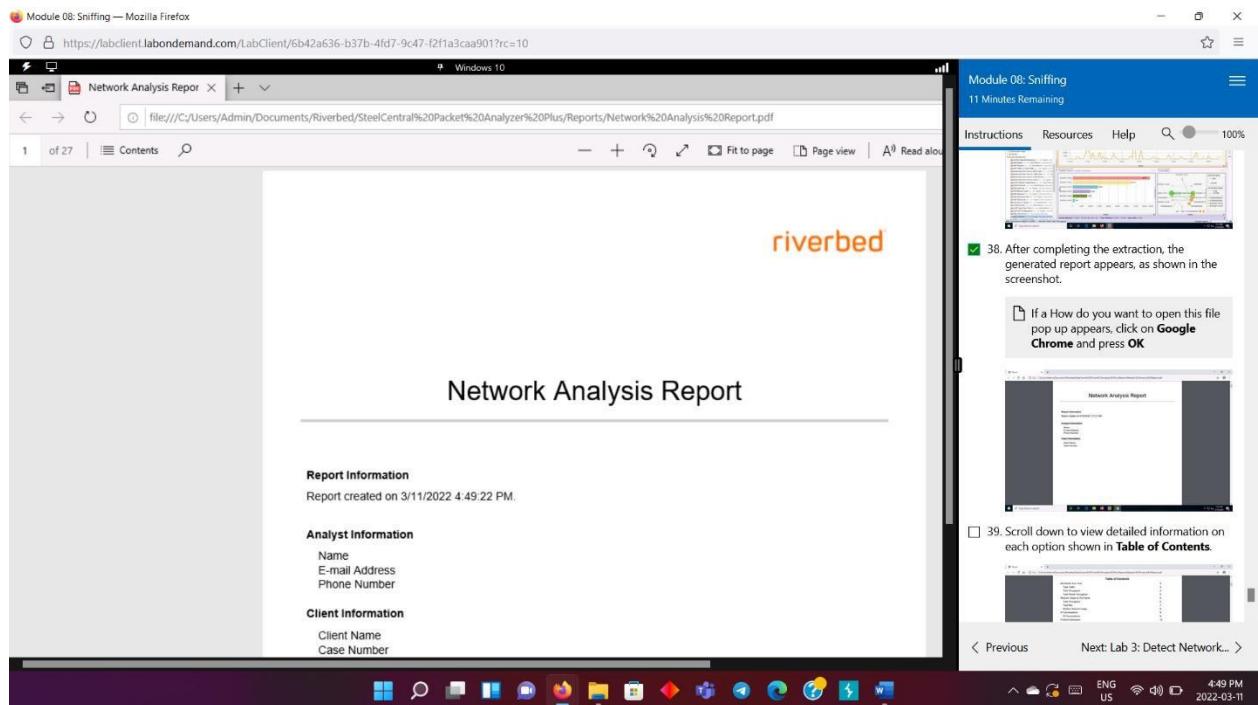
< Previous Next: Lab 3: Detect Network... >

4:44 PM 2022-03-11

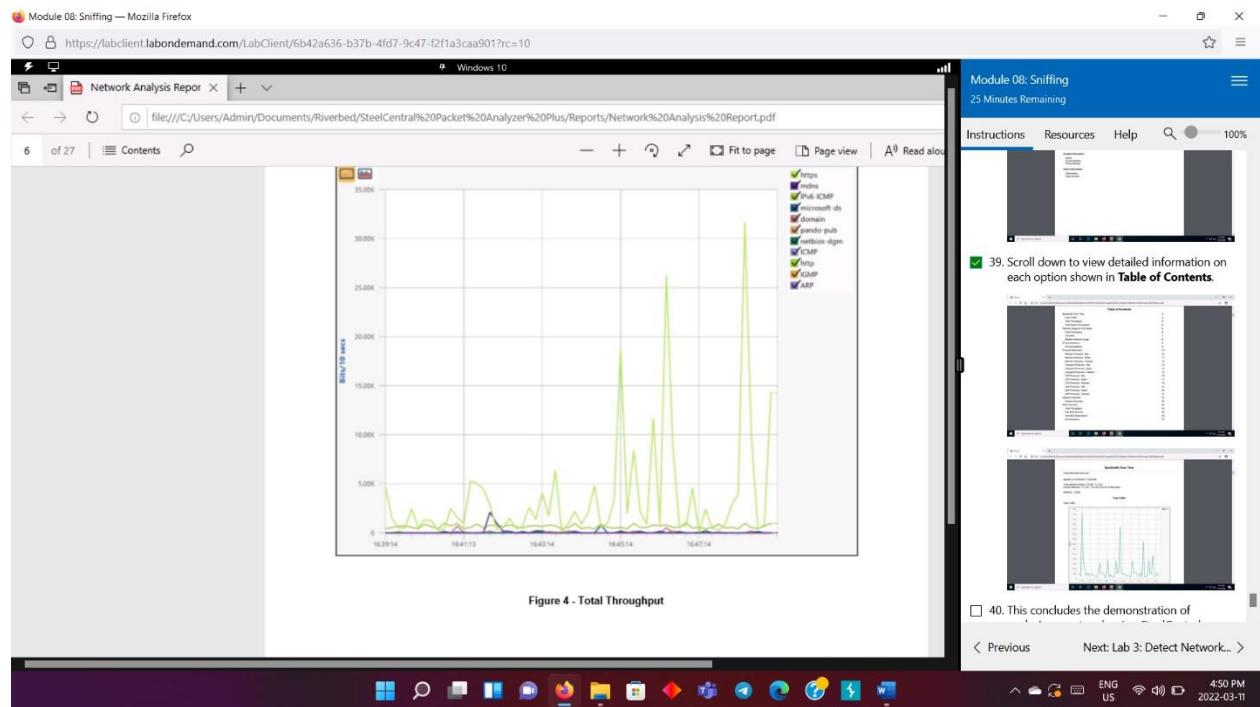
- Select MAC overview, it provides the MAC source and MAC conversations.



- 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.

