NETWORK SECURITY FUNDAMENTALS V2

Lab 3: Creating Packet Captures

Document Version: 2023-10-16

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Creating Packet Captures 6
1.0 Load Lab Configuration 6
1.1 Create a Wireshark Packet Capture 11

Introduction

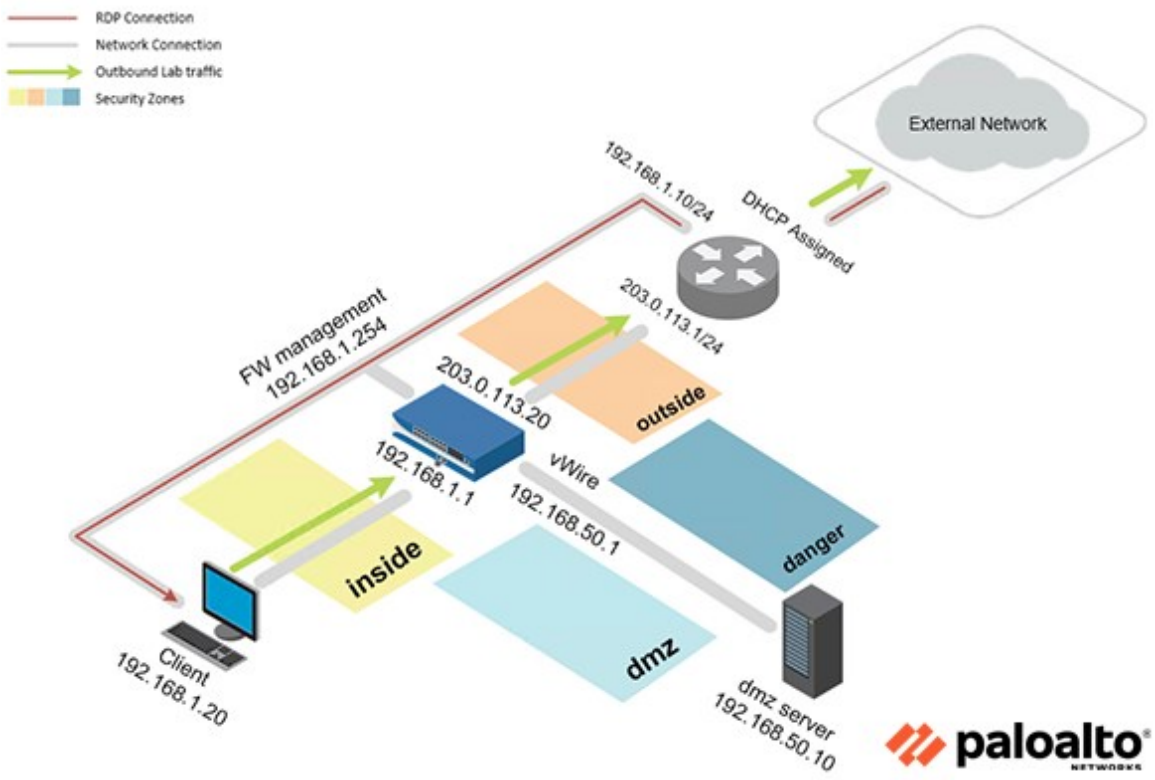
In this lab, you will utilize Wireshark to initiate a packet capture. Wireshark captures packets and allows network administrators to examine the data within the packet.

Objective

In this lab, you will perform the following tasks:

- Create a Packet Capture using Wireshark

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

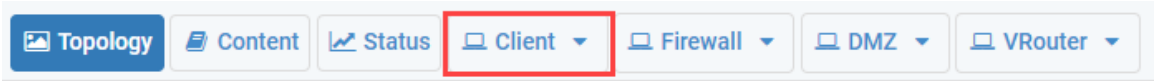
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Creating Packet Captures

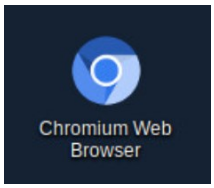
1.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the Client PC.

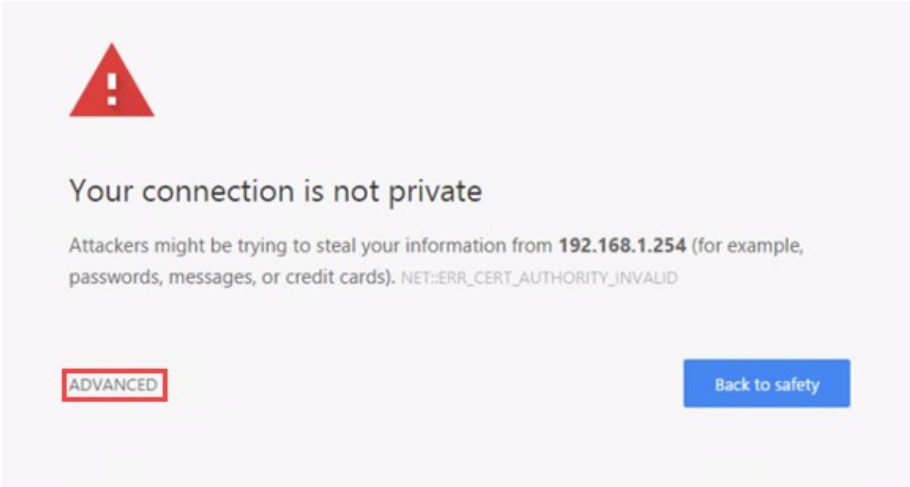


2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



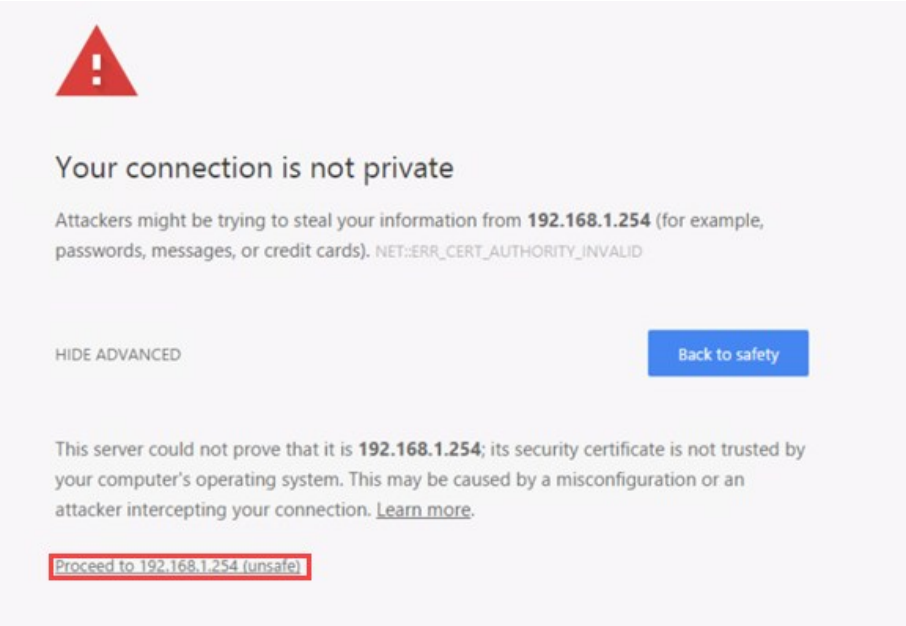
4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.

5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



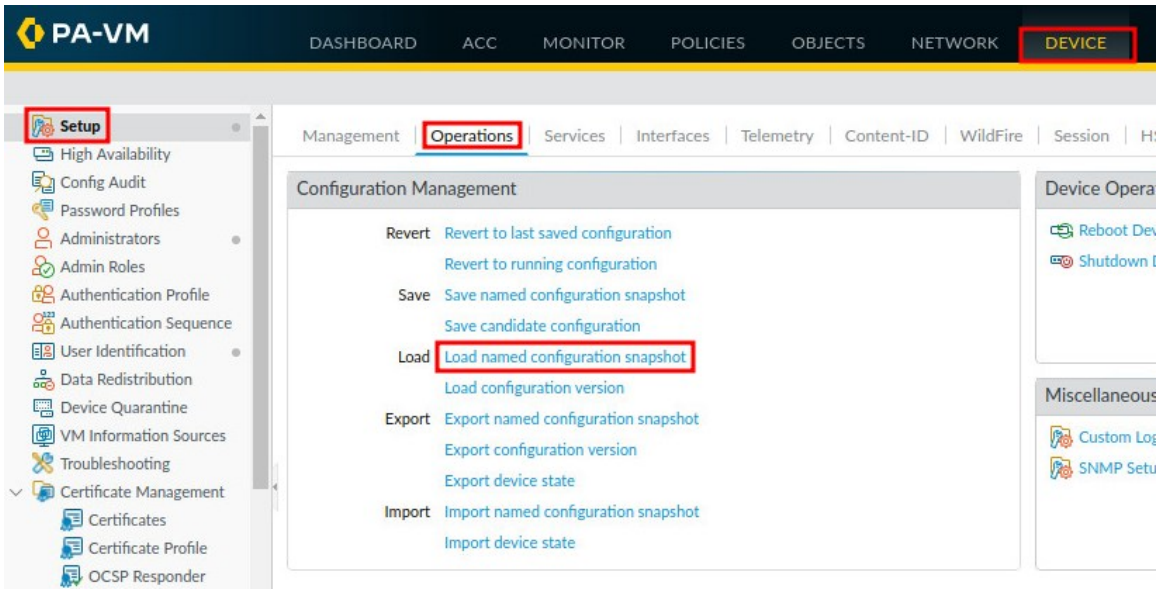
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

6. Click on **Proceed to 192.168.1.254 (unsafe)**.

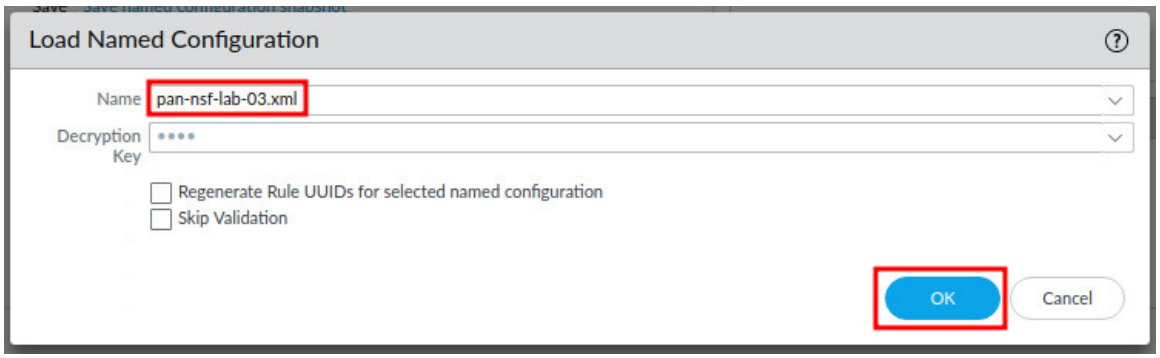


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

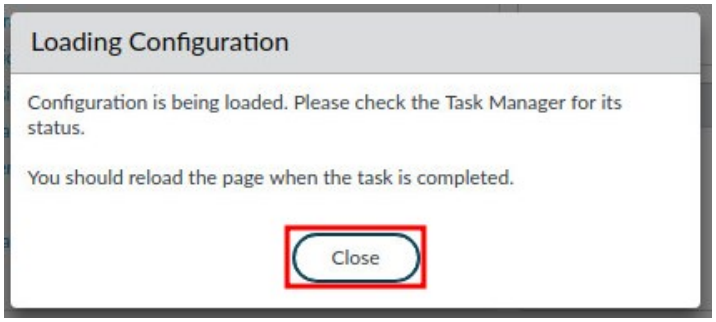
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-nsf-lab-03.xml** from the *Name* dropdown box and click **OK**.

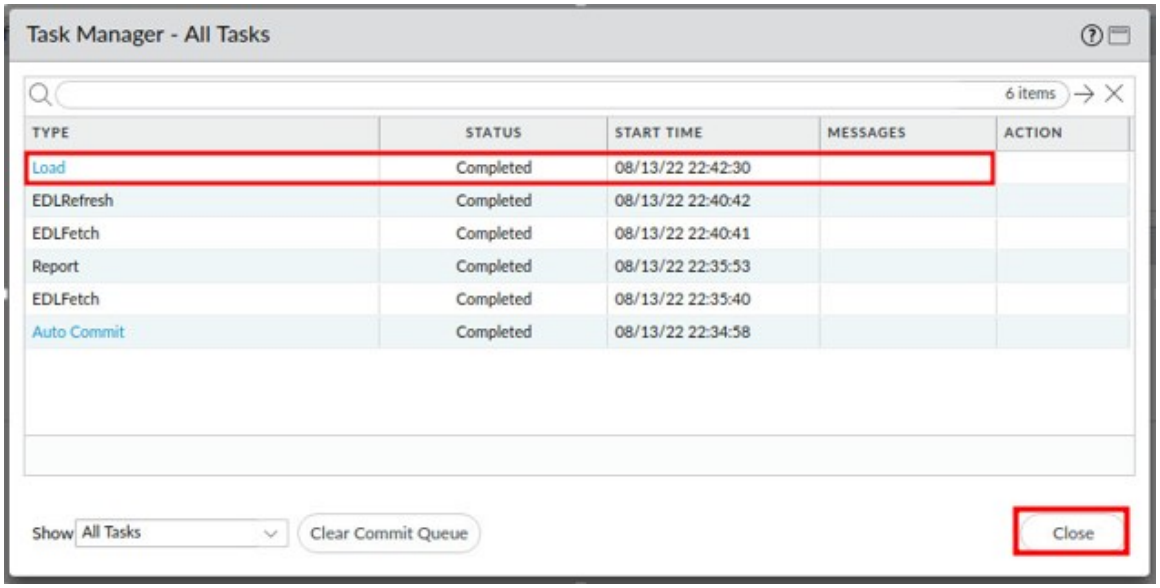


10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

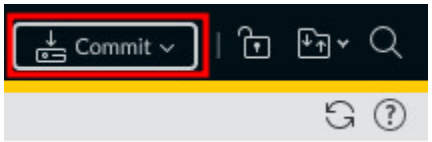


11. Click the **Tasks** icon located at the bottom-right of the web interface.

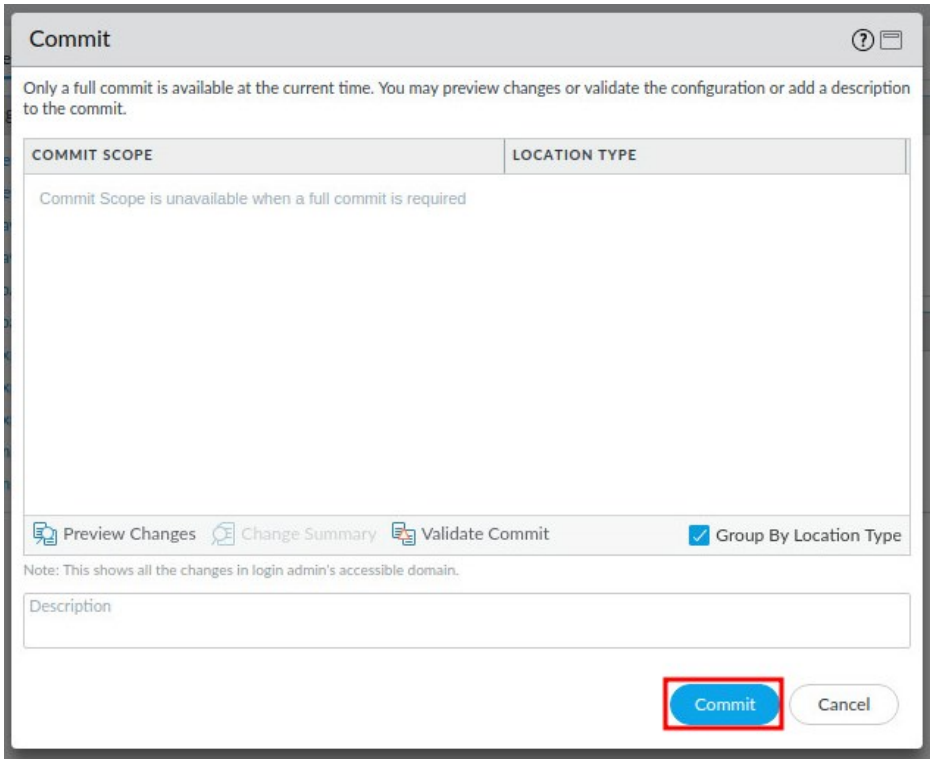
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



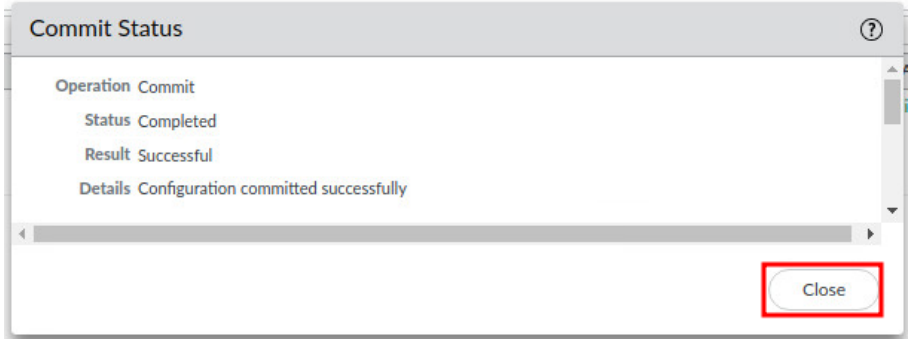
13. Click the **Commit** link located at the top-right of the web interface.



14. In the *Commit* window, click **Commit** to proceed with committing the changes.



15. When the commit operation successfully completes, click **Close** to continue.

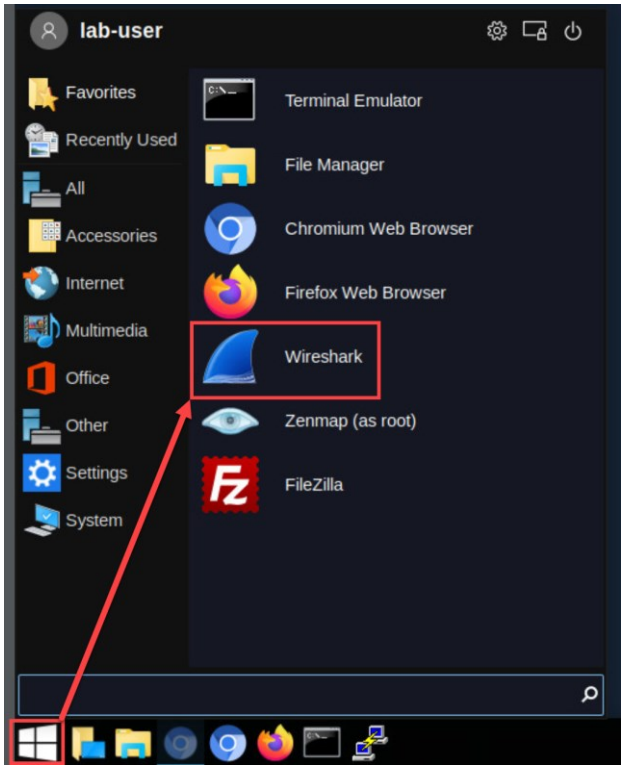


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

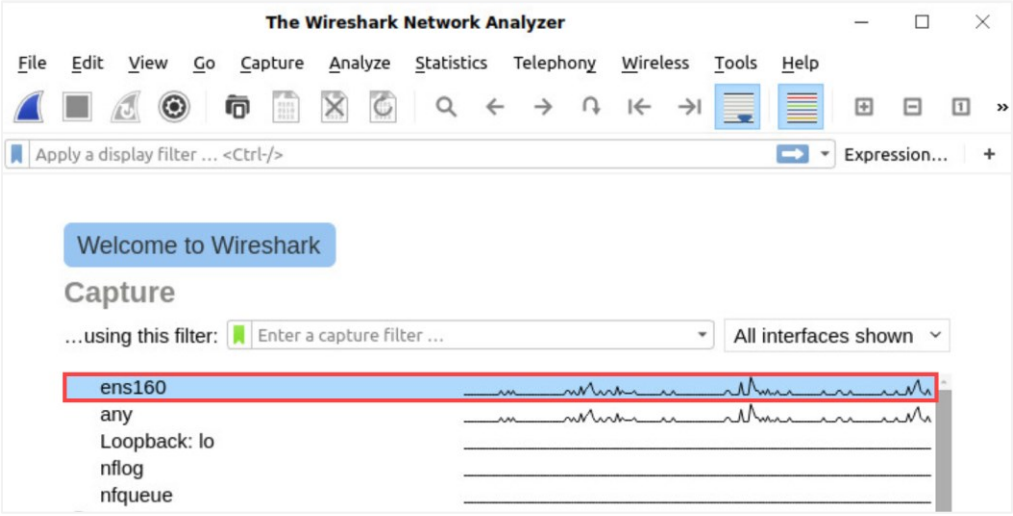
1.1 Create a Wireshark Packet Capture

In this section, you will create a packet capture using Wireshark on the Client. Wireshark is a program used to capture packets from a computers' network adapter. All traffic going from and coming to the Client, in this case, will be recorded.

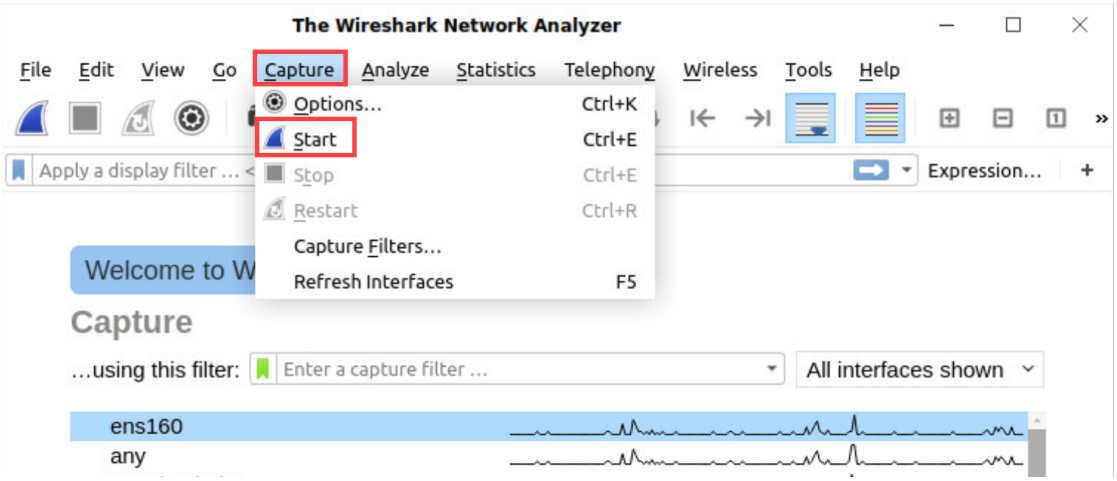
1. Click on the **Start Menu** icon, located at the bottom-left and select **Wireshark**.



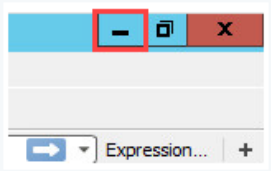
2. Click on the **ens160** interface from the list.



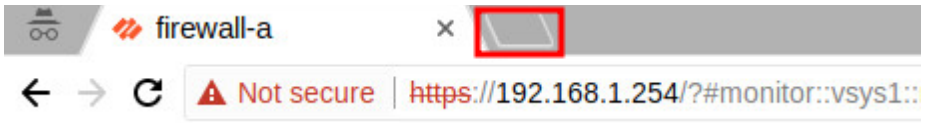
3. From the menu bar, click on **Capture > Start**.



4. Minimize *Wireshark* by clicking in the upper-right.

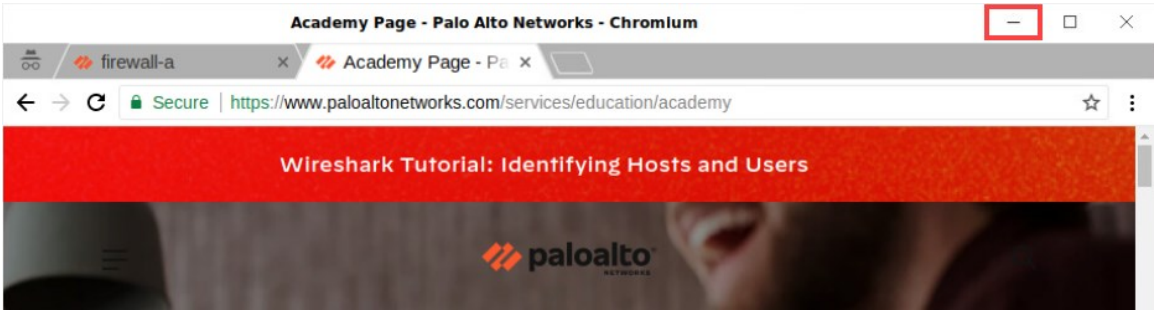


5. In *Chromium*, click on the **New tab** button.



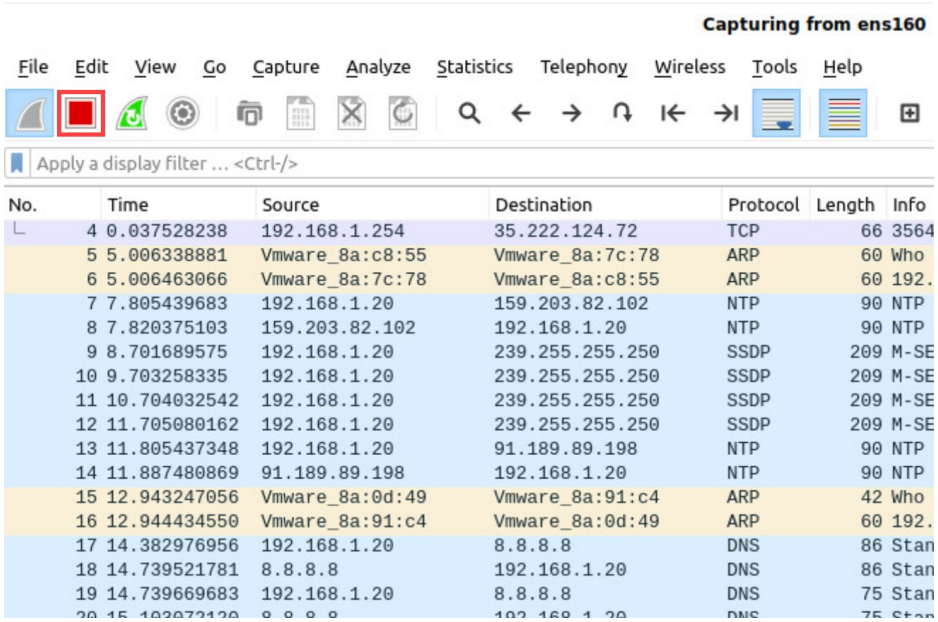
6. In the *address bar*, type `https://www.paloaltonetworks.com/academy` and press **Enter**.

7. Once the page loads, minimize the *Palo Alto Networks Education Files – Chromium* window.



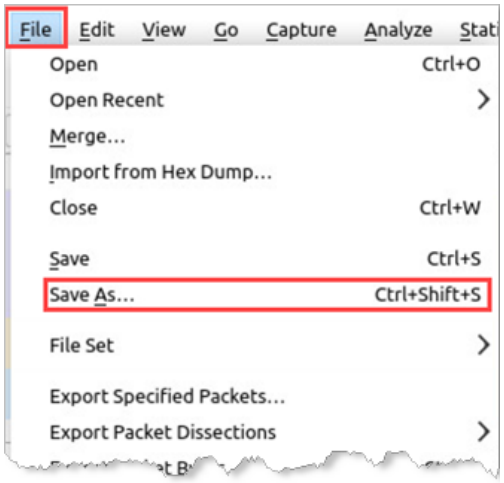
8. Wait for 5 to 10 seconds, then reopen **Wireshark** by clicking on the icon in the bottom taskbar.

9. Click the **Stop capturing packets** button.

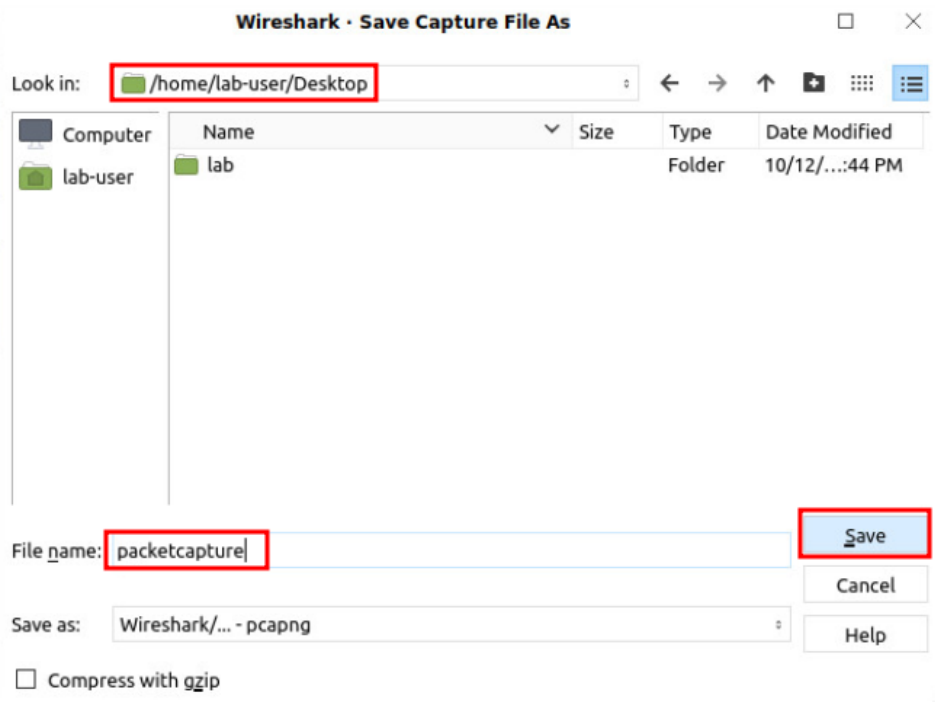


No.	Time	Source	Destination	Protocol	Length	Info
4	0.037528238	192.168.1.254	35.222.124.72	TCP	66	3564
5	5.006338881	Vmware_8a:c8:55	Vmware_8a:7c:78	ARP	60	Who
6	5.006463066	Vmware_8a:7c:78	Vmware_8a:c8:55	ARP	60	192.
7	7.805439683	192.168.1.20	159.203.82.102	NTP	90	NTP
8	7.820375103	159.203.82.102	192.168.1.20	NTP	90	NTP
9	8.701689575	192.168.1.20	239.255.255.250	SSDP	209	M-SE
10	9.703258335	192.168.1.20	239.255.255.250	SSDP	209	M-SE
11	10.704032542	192.168.1.20	239.255.255.250	SSDP	209	M-SE
12	11.705080162	192.168.1.20	239.255.255.250	SSDP	209	M-SE
13	11.805437348	192.168.1.20	91.189.89.198	NTP	90	NTP
14	11.887480869	91.189.89.198	192.168.1.20	NTP	90	NTP
15	12.943247056	Vmware_8a:0d:49	Vmware_8a:91:c4	ARP	42	Who
16	12.944434550	Vmware_8a:91:c4	Vmware_8a:0d:49	ARP	60	192.
17	14.382976956	192.168.1.20	8.8.8.8	DNS	86	Stan
18	14.739521781	8.8.8.8	192.168.1.20	DNS	86	Stan
19	14.739669683	192.168.1.20	8.8.8.8	DNS	75	Stan

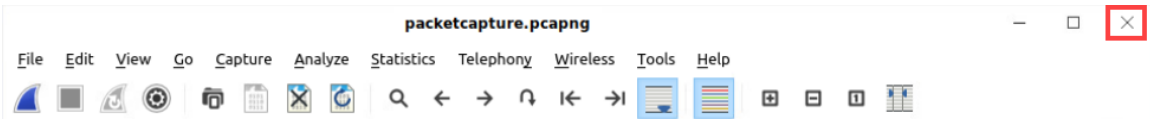
10. To save the Wireshark packet capture, click on **File > Save As…**.



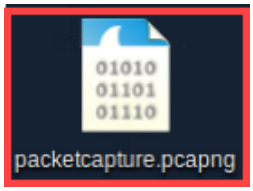
11. In the *Save file as* window, make sure to select **/home/lab-user/Desktop** as the *Look in* selection. Type `packetcapture` in the *File name* field. Finally, click **Save**.



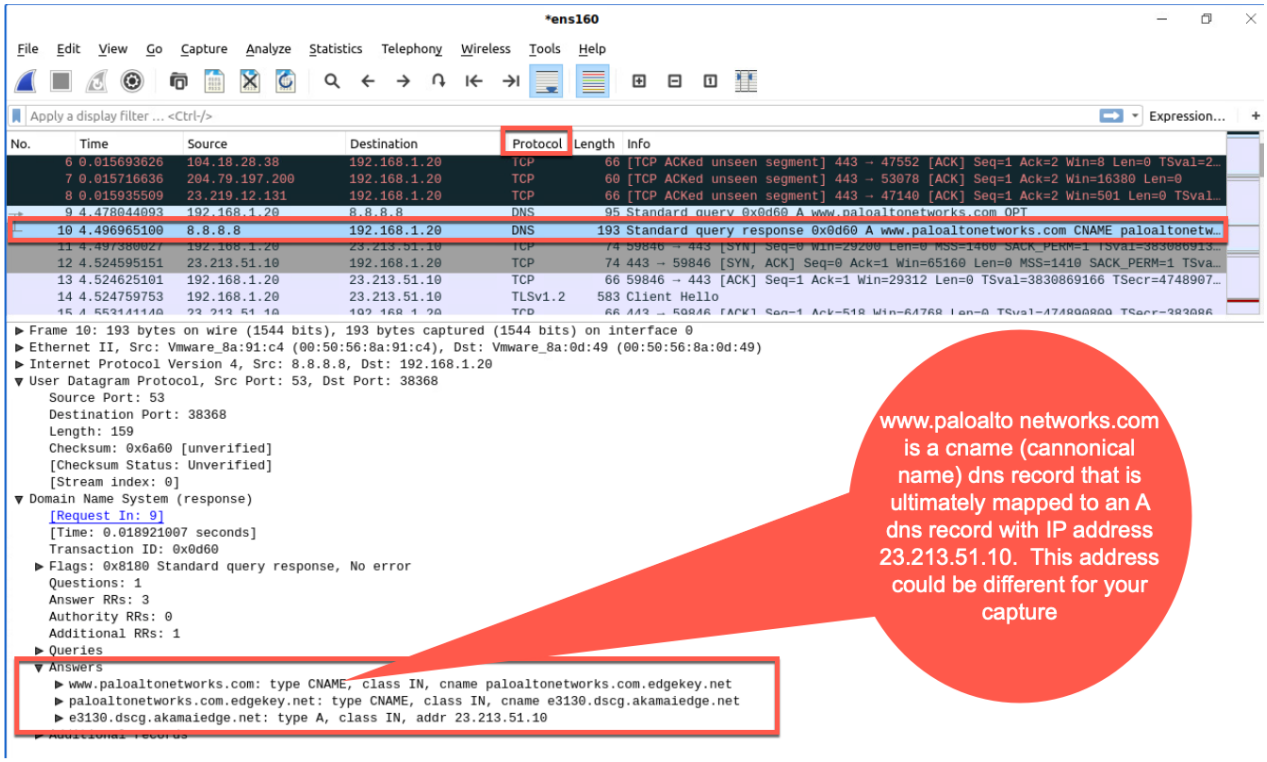
12. Close Wireshark by clicking on the **close** icon.

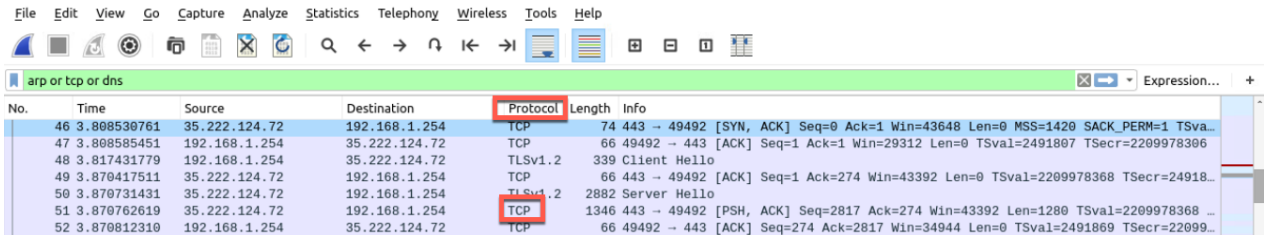


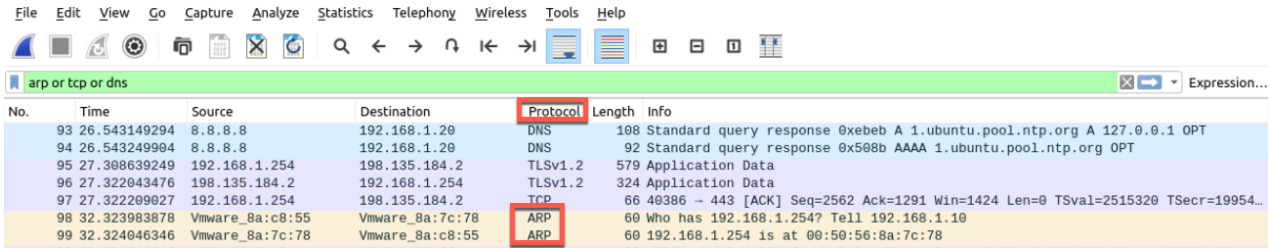
13. On the client desktop, double-click on the **packetcapture.pcapng** file to examine the Wireshark capture.

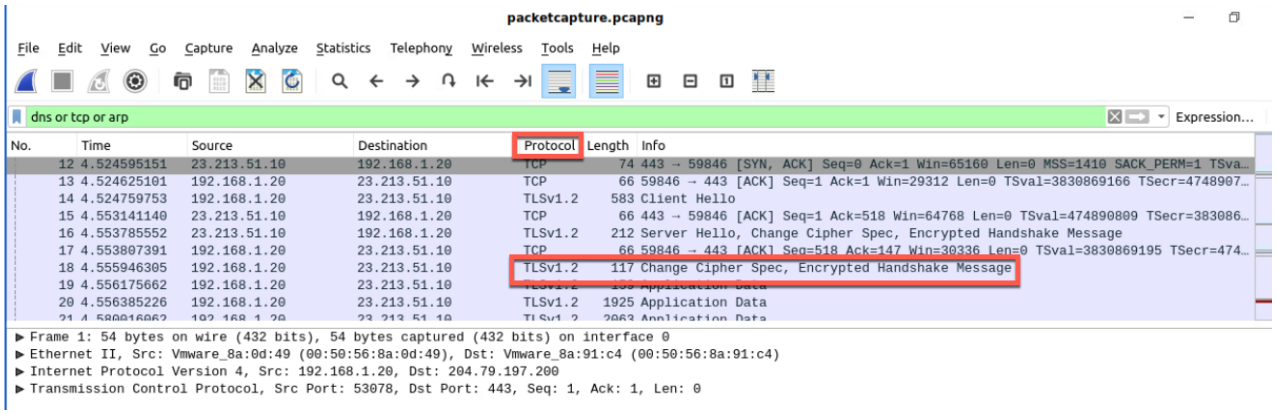


14. While examining the Wireshark packet capture, notice the **ARP**, **DNS**, **TCP, TLSv1.2** protocols. You can search for these protocols by entering the following expression in the display filter bar: “arp or dns or tcp” and clicking the arrow button. Then, scroll down until you observe each protocol.









Due to the nature of the lab environment, your packet capture may differ from the results above.

ARP, Address Resolution Protocol, will find the IP addresses of devices on the same network by resolving MAC addresses to IP addresses.

DNS, Domain Name System, resolves fully qualified domain names to an IP address. In the above example, it eventually resolves www.paloaltonetworks.com to 23.213.51.10.

TCP, Transmission Control Protocol, is a connection-oriented protocol. When a program using TCP establishes a connection, the connection is maintained until the application has finished exchanging messages with the other end.

TLSv1.2, Transport Layer Security v1.2 is the successor to Secure Socket Layer (SSL). It encrypts traffic between endpoints and application servers over a network providing data confidentiality.

15. The lab is now complete; you may end the reservation.

