



NETWORK SECURITY FUNDAMENTALS V2

Lab 3: Creating Packet Captures

Document Version: **2023-10-16**

Copyright © 2023 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

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

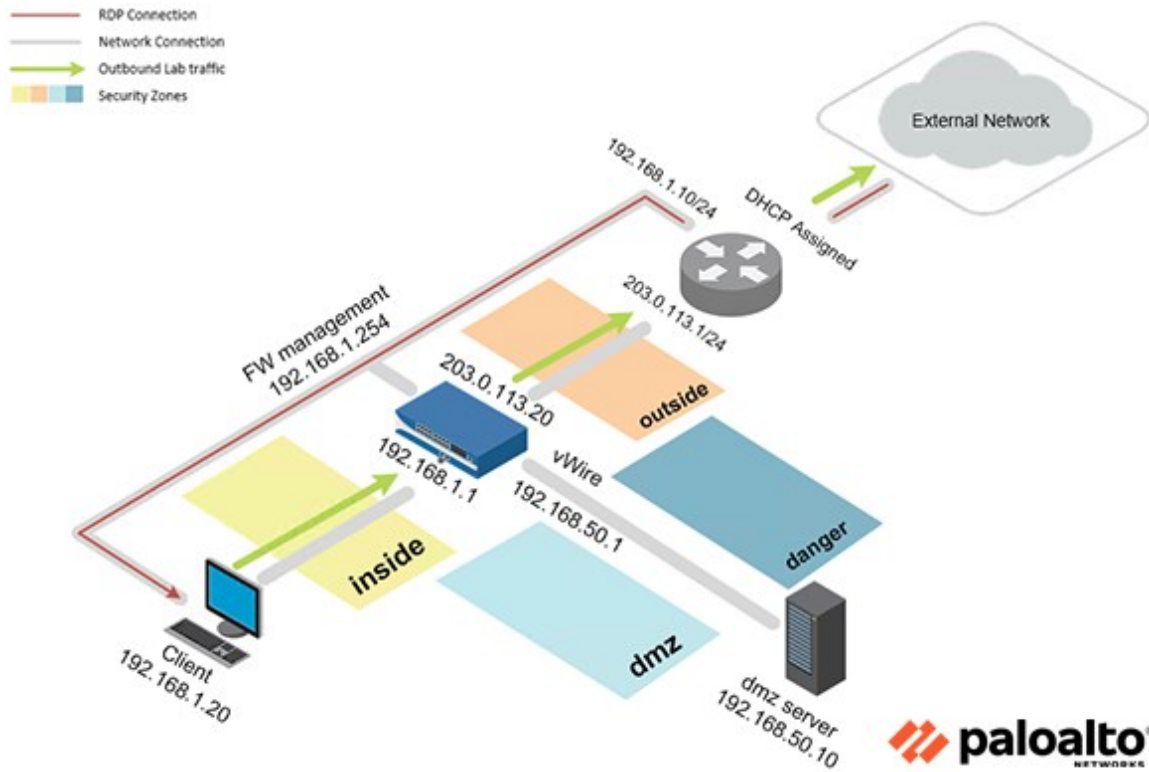
In this lab, you will utilize Wireshark to initiate a packet capture. Wireshark captures packets and allows network administrators to examine the data within the packet.

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.

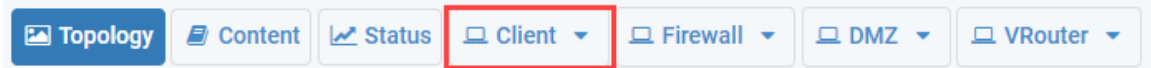
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Creating Packet Captures

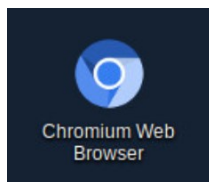
1.0 Load Lab Configuration

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

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



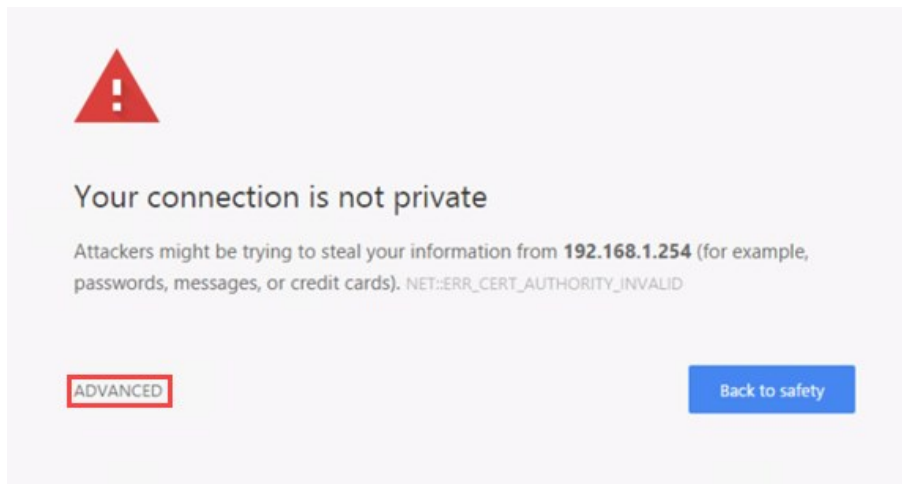
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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

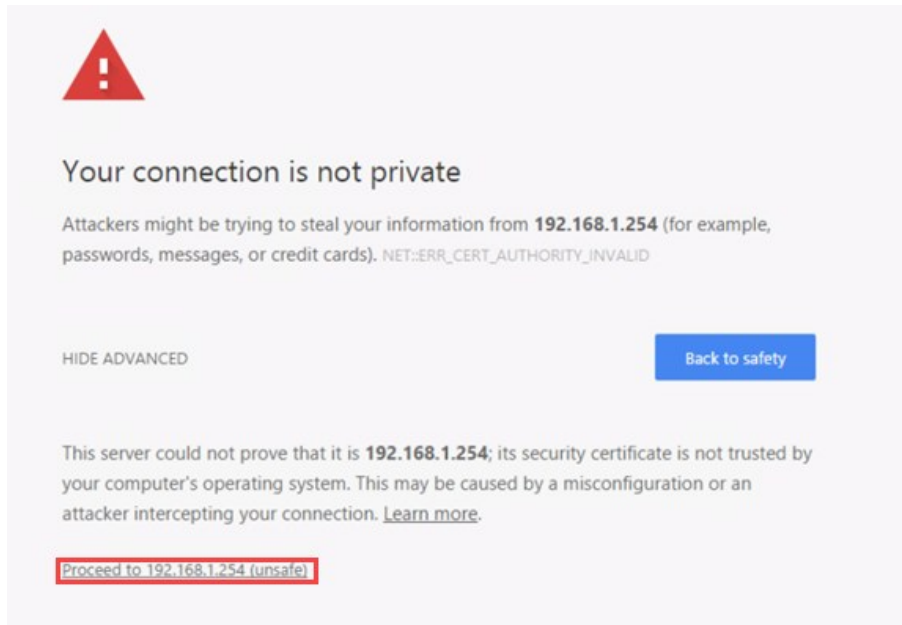


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

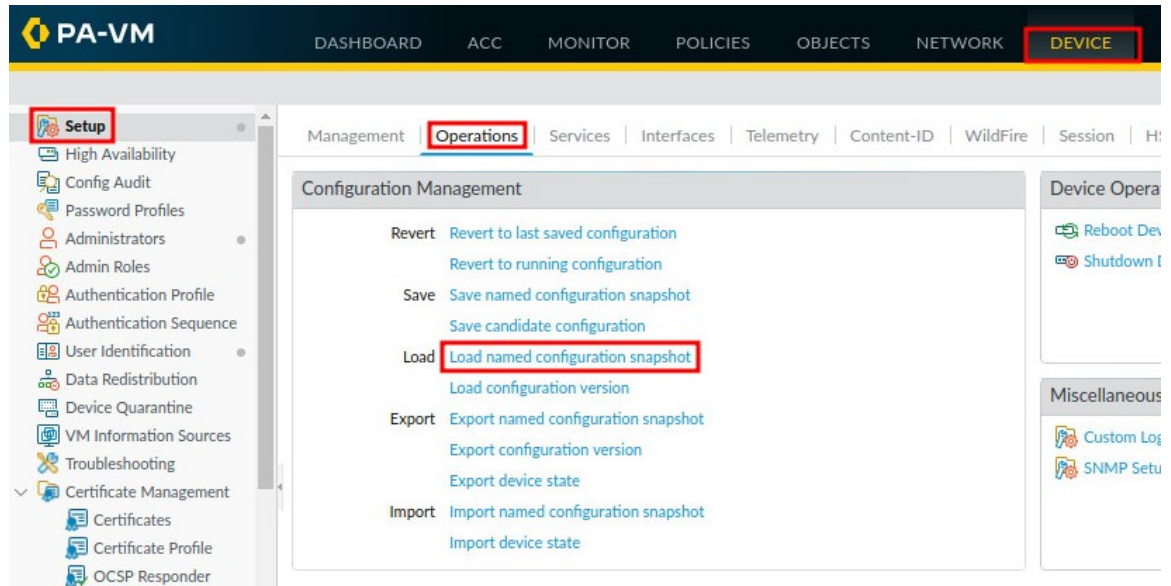
- Click on **Proceed to 192.168.1.254 (unsafe)**.



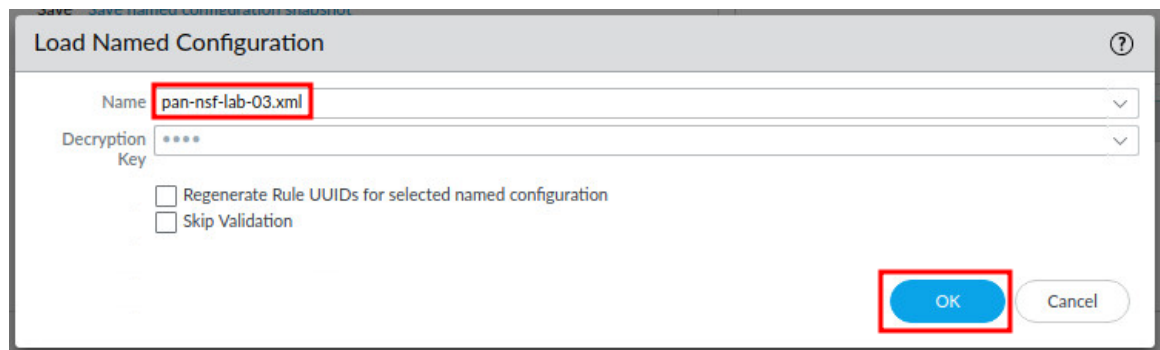
- Log in to the Firewall web interface as username admin, password Pal0Alt0!.



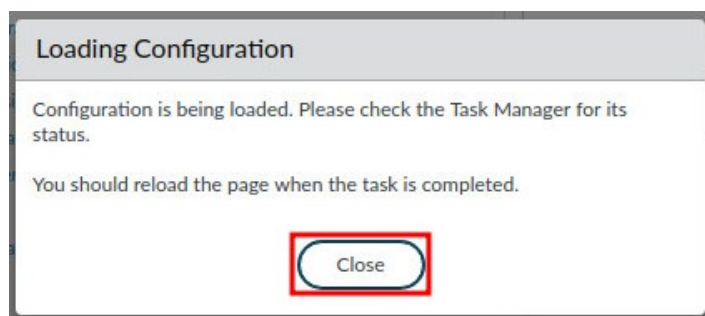
- In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



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



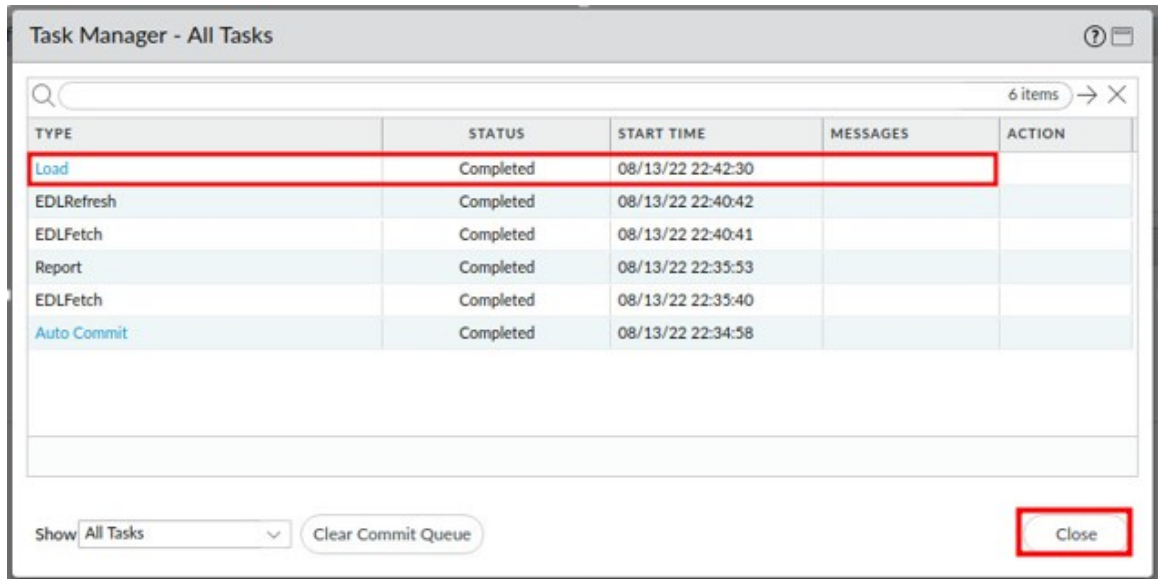
- In the Loading Configuration window, a message will show *Configuration is being loaded*. Please check the Task Manager for its status. You should reload the page when the task is completed. Click **Close** to continue.



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



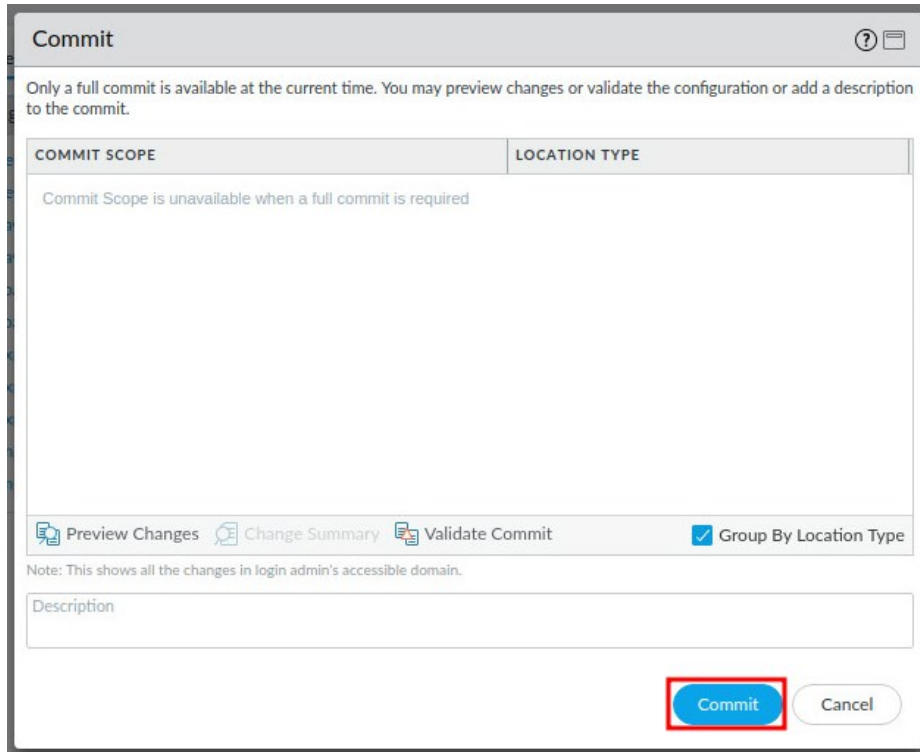
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



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

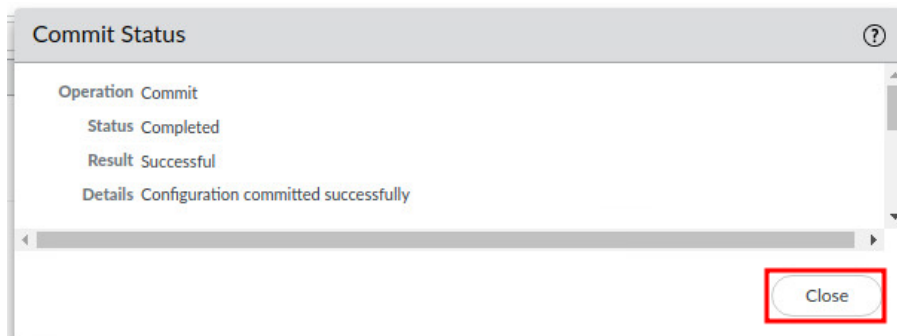


14. In the *Commit* window, click **Commit** to proceed with committing the changes.



The screenshot shows the 'Commit' window. At the top, a message states: 'Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.' Below this is a table with two columns: 'COMMIT SCOPE' and 'LOCATION TYPE'. The 'COMMIT SCOPE' column contains the text 'Commit Scope is unavailable when a full commit is required'. Below the table is a row of buttons: 'Preview Changes', 'Change Summary', 'Validate Commit', and a checked checkbox for 'Group By Location Type'. A note below the buttons reads: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom is a text input field labeled 'Description'. In the bottom right corner, the 'Commit' button is highlighted with a red rectangle, next to a 'Cancel' button.

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



The screenshot shows the 'Commit Status' window. It displays the following information: 'Operation: Commit', 'Status: Completed', 'Result: Successful', and 'Details: Configuration committed successfully'. At the bottom right, the 'Close' button is highlighted with a red rectangle.

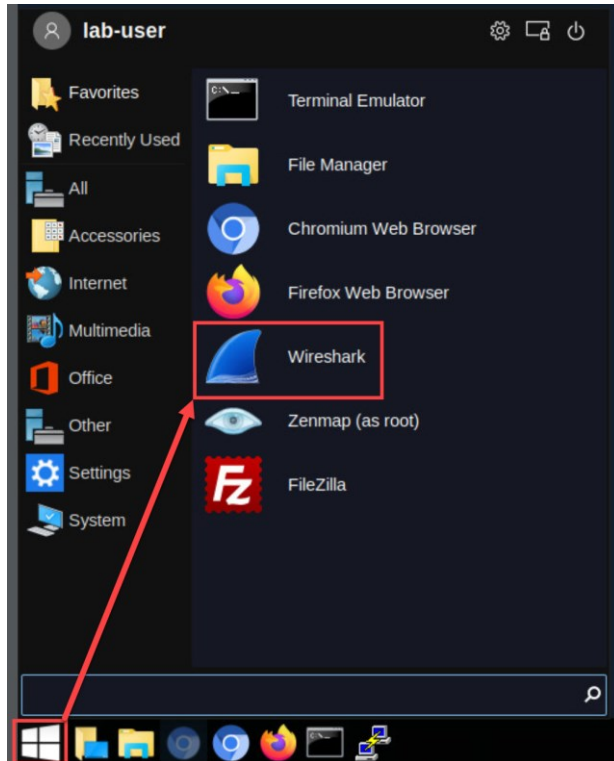


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

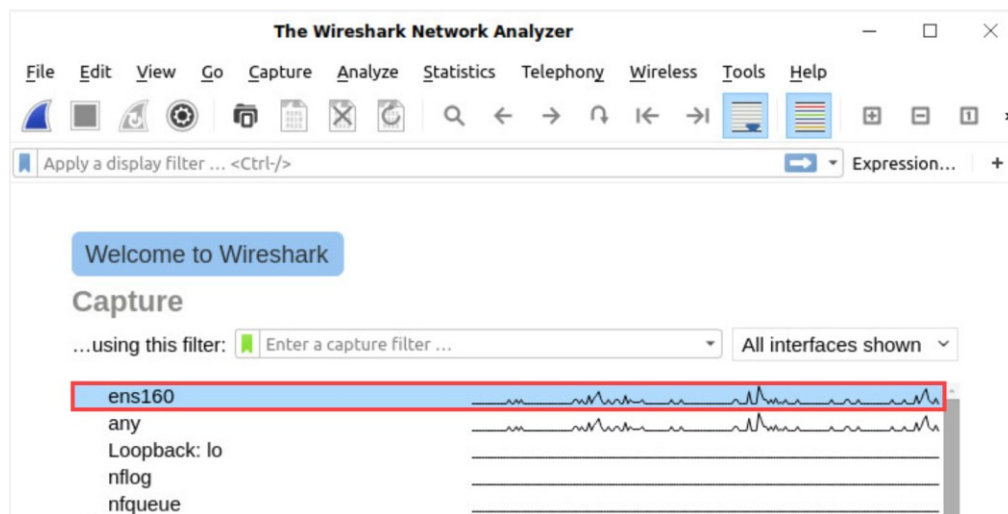
1.1 Create a Wireshark Packet Capture

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.

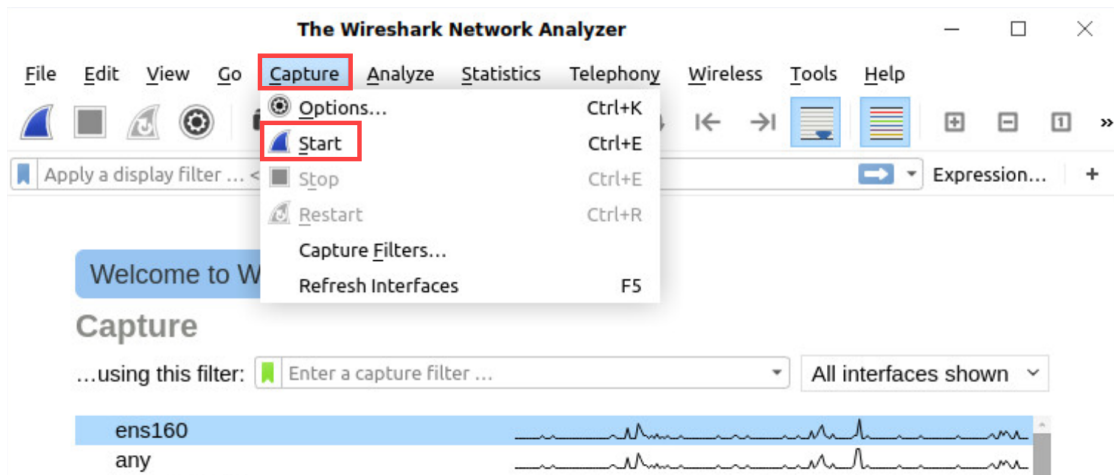
1. Click on the **Start Menu** icon, located at the bottom-left and select **Wireshark**.



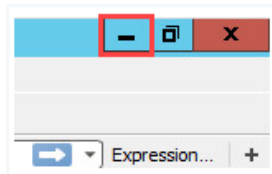
2. Click on the **ens160** interface from the list.



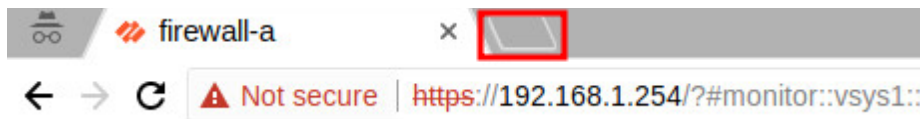
- From the menu bar, click on **Capture > Start**.



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



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



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



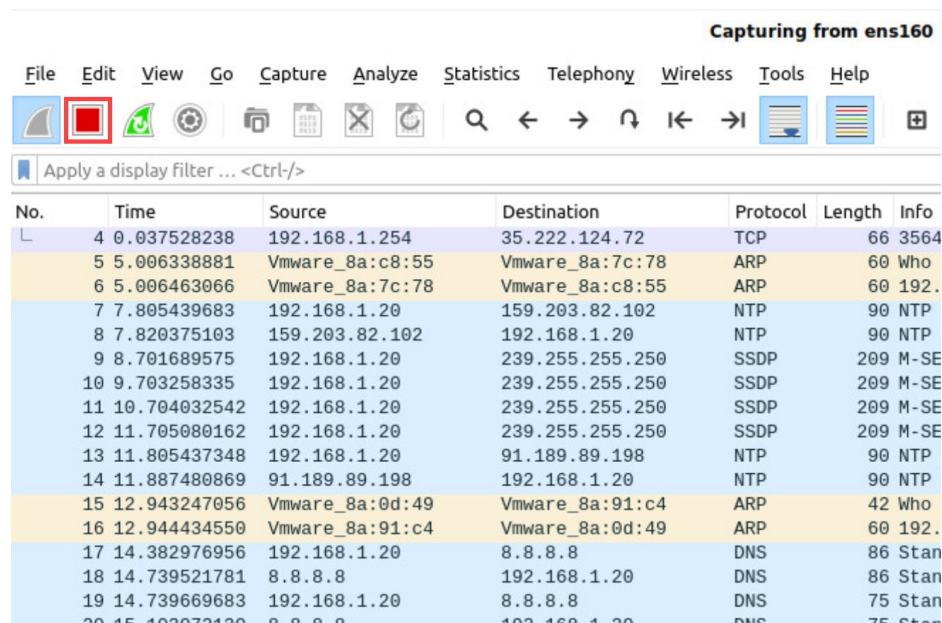
- Once the page loads, minimize the *Palo Alto Networks Education Files – Chromium* window.



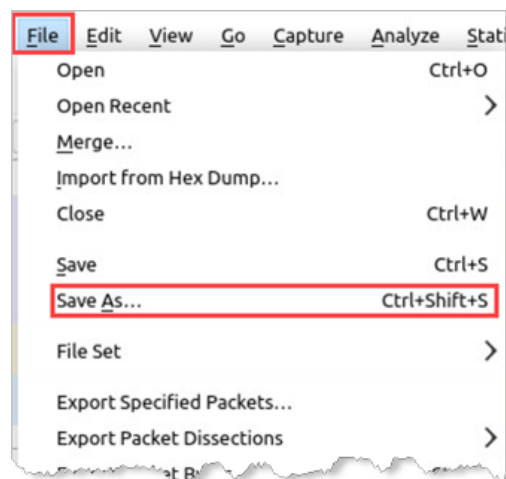
8. Wait for 5 to 10 seconds, then reopen **Wireshark** by clicking on the icon in the bottom taskbar.



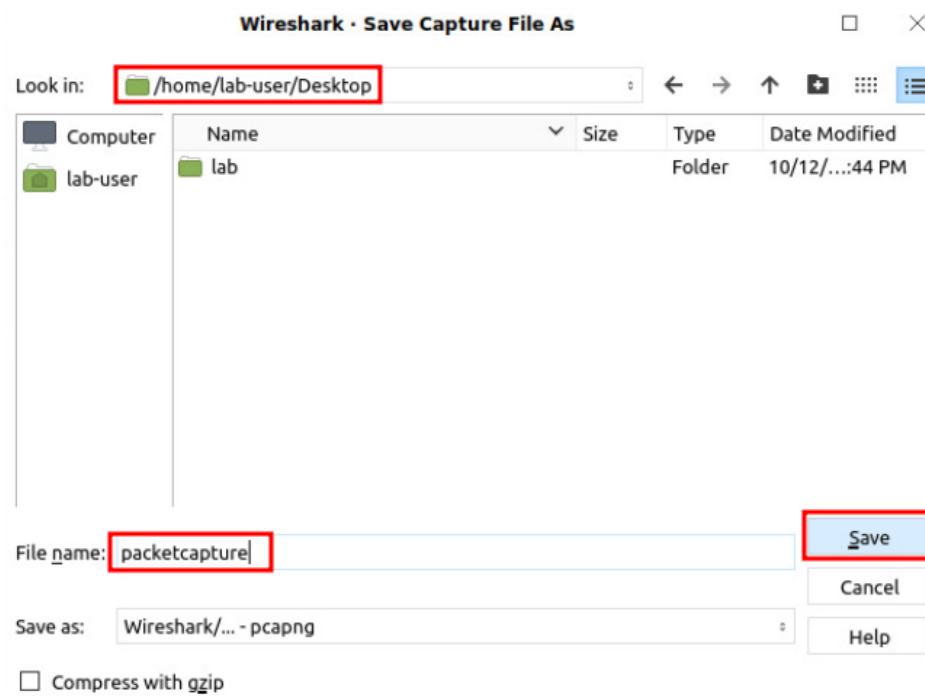
9. Click the **Stop capturing packets** button.



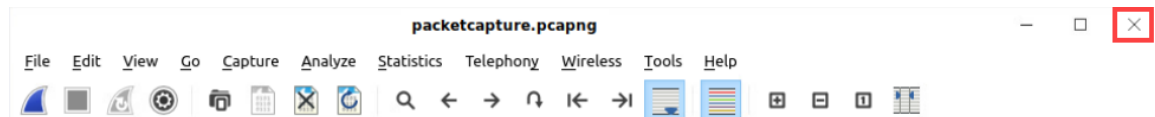
10. To save the Wireshark packet capture, click on **File > Save As....**



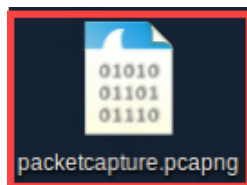
11. In the *Save file as* window, make sure to select **/home/lab-user/Desktop** as the *Look in* selection. Type packetcapture in the *File name* field. Finally, click **Save**.



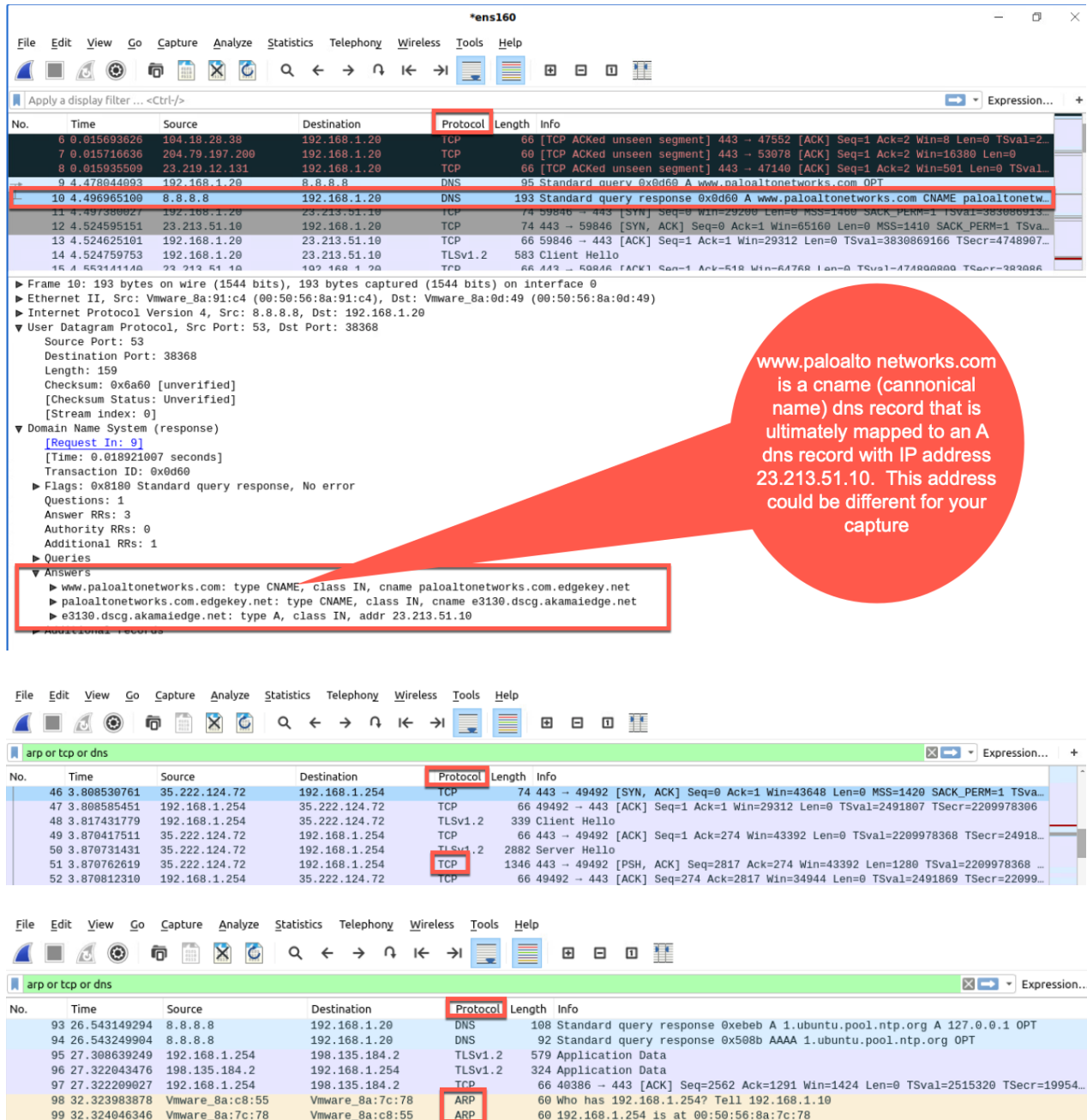
12. Close Wireshark by clicking on the **close** icon.



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.



The screenshot shows a Wireshark packet capture on interface *ens160. The display filter is set to "arp or tcp or dns". The packet list shows several packets, with packet 10 (DNS) highlighted. The packet details pane shows the DNS response for "www.paloaltonetworks.com" with the CNAME "paloaltonetworks.com" and the IP address "23.213.51.10". A red circle highlights this information, with a callout stating: "www.paloaltonetworks.com is a cname (canonical name) dns record that is ultimately mapped to an A dns record with IP address 23.213.51.10. This address could be different for your capture".

The packet list shows the following protocols:

No.	Time	Source	Destination	Protocol	Length	Info
6	0.015693626	192.168.1.20	192.168.1.20	TCP	66	[TCP ACKed unseen segment] 443 → 47552 [ACK] Seq=1 Ack=2 Win=8 Len=0 TSval=2...
7	0.015716636	204.79.197.200	192.168.1.20	TCP	60	[TCP ACKed unseen segment] 443 → 53078 [ACK] Seq=1 Ack=2 Win=16380 Len=0
8	0.015935509	23.219.12.131	192.168.1.20	TCP	66	[TCP ACKed unseen segment] 443 → 47140 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=1...
9	4.478044093	192.168.1.20	8.8.8.8	DNS	95	Standard query request 0x0d60 A www.paloaltonetworks.com OPT
10	4.496965100	8.8.8.8	192.168.1.20	DNS	193	Standard query response 0x0d60 A www.paloaltonetworks.com CNAME paloaltonetw...
11	4.497380027	192.168.1.20	23.213.51.10	TCP	74	59846 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=383080913...
12	4.524595151	23.213.51.10	192.168.1.20	TCP	74	443 → 59846 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1410 SACK_PERM=1 TSva...
13	4.524625101	192.168.1.20	23.213.51.10	TCP	66	59846 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=383080916 TSecr=4748907...
14	4.524759753	192.168.1.20	23.213.51.10	TLSv1.2	583	Client Hello
15	4.524814110	23.213.51.10	192.168.1.20	TCP	66	443 → 59846 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=474800000 TSecr=383080...

The packet details pane for packet 10 shows the following information:

- Frame 10: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface 0
- Ethernet II, Src: Vmware_8a:91:c4 (00:50:56:8a:91:c4), Dst: Vmware_8a:0d:49 (00:50:56:8a:0d:49)
- Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.20
- User Datagram Protocol, Src Port: 53, Dst Port: 38368
- Source Port: 53
- Destination Port: 38368
- Length: 159
- Checksum: 0x6a60 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 0]
- Domain Name System (response)
 - [Request In: 9]
 - [Time: 0.018921007 seconds]
 - Transaction ID: 0x0d60
 - Flags: 0x1800 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - Answers
 - www.paloaltonetworks.com: type CNAME, class IN, cname paloaltonetworks.com.edgekey.net
 - paloaltonetworks.com.edgekey.net: type CNAME, class IN, cname e3130.dscg.akamaiedge.net
 - e3130.dscg.akamaiedge.net: type A, class IN, addr 23.213.51.10

The display filter is set to "arp or tcp or dns". The packet list shows the following protocols:

No.	Time	Source	Destination	Protocol	Length	Info
46	3.808530761	35.222.124.72	192.168.1.254	TCP	74	443 → 49492 [SYN, ACK] Seq=0 Ack=1 Win=43648 Len=0 MSS=1420 SACK_PERM=1 TSva...
47	3.808585451	192.168.1.254	35.222.124.72	TCP	66	49492 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2491807 TSecr=2209978306
48	3.817431779	192.168.1.254	35.222.124.72	TLSv1.2	339	Client Hello
49	3.870417511	35.222.124.72	192.168.1.254	TCP	66	443 → 49492 [ACK] Seq=1 Ack=274 Win=43392 Len=0 TSval=2209978368 TSecr=24918...
50	3.870731431	35.222.124.72	192.168.1.254	TLSv1.2	2882	Server Hello
51	3.870762619	35.222.124.72	192.168.1.254	TCP	1346	443 → 49492 [PSH, ACK] Seq=2817 Ack=274 Win=43392 Len=1280 TSval=2209978368 ...
52	3.870812310	192.168.1.254	35.222.124.72	TCP	66	49492 → 443 [ACK] Seq=274 Ack=2817 Win=34944 Len=0 TSval=2491869 TSecr=22099...

The display filter is set to "arp or tcp or dns". The packet list shows the following protocols:

No.	Time	Source	Destination	Protocol	Length	Info
93	26.543149294	8.8.8.8	192.168.1.20	DNS	108	Standard query response 0xebeb A 1.ubuntu.pool.ntp.org A 127.0.0.1 OPT
94	26.543249904	8.8.8.8	192.168.1.20	DNS	92	Standard query response 0x508b AAAA 1.ubuntu.pool.ntp.org OPT
95	27.308639249	192.168.1.254	198.135.184.2	TLSv1.2	579	Application Data
96	27.322043476	198.135.184.2	192.168.1.254	TLSv1.2	324	Application Data
97	27.322209027	192.168.1.254	198.135.184.2	TCP	66	40386 → 443 [ACK] Seq=2562 Ack=1291 Win=1424 Len=0 TSval=2515320 TSecr=19954...
98	32.323983878	Vmware_8a:c8:55	Vmware_8a:7c:78	ARP	60	Who has 192.168.1.254? Tell 192.168.1.10
99	32.324046346	Vmware_8a:7c:78	Vmware_8a:c8:55	ARP	60	192.168.1.254 is at 00:50:56:8a:7c:78

packetcapture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns or tcp or arp

No.	Time	Source	Destination	Protocol	Length	Info
12	4.524595151	23.213.51.10	192.168.1.20	TCP	74	443 → 59846 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1410 SACK_PERM=1 TSval=...
13	4.524625101	192.168.1.20	23.213.51.10	TCP	66	59846 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3830869166 TSecr=4748907...
14	4.524759753	192.168.1.20	23.213.51.10	TLSv1.2	583	Client Hello
15	4.553141149	23.213.51.10	192.168.1.20	TCP	66	443 → 59846 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=474890809 TSecr=383086...
16	4.553785552	23.213.51.10	192.168.1.20	TLSv1.2	212	Server Hello, Change Cipher Spec, Encrypted Handshake Message
17	4.553807391	192.168.1.20	23.213.51.10	TCP	66	59846 → 443 [ACK] Seq=518 Ack=147 Win=30336 Len=0 TSval=3830869195 TSecr=474...
18	4.555946305	192.168.1.20	23.213.51.10	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
19	4.556175662	192.168.1.20	23.213.51.10	TLSv1.2	1925	Application Data
20	4.556385226	192.168.1.20	23.213.51.10	TLSv1.2	1925	Application Data
21	4.556516062	192.168.1.20	23.213.51.10	TLSv1.2	2063	Application Data

▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_8a:0d:49 (00:50:56:8a:0d:49), Dst: Vmware_8a:91:c4 (00:50:56:8a:91:c4)
 ▶ Internet Protocol Version 4, Src: 192.168.1.20, Dst: 204.79.197.200
 ▶ Transmission Control Protocol, Src Port: 53078, Dst Port: 443, Seq: 1, Ack: 1, Len: 0



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.