



NETWORK SECURITY FUNDAMENTALS

Lab 3: Creating Packet Captures

Document Version: **2021-01-30**

Copyright © 2021 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
3 Creating Packet Captures.....	6
3.0 Load Lab Configuration	6
3.1 Create a Wireshark Packet Capture	10

Introduction

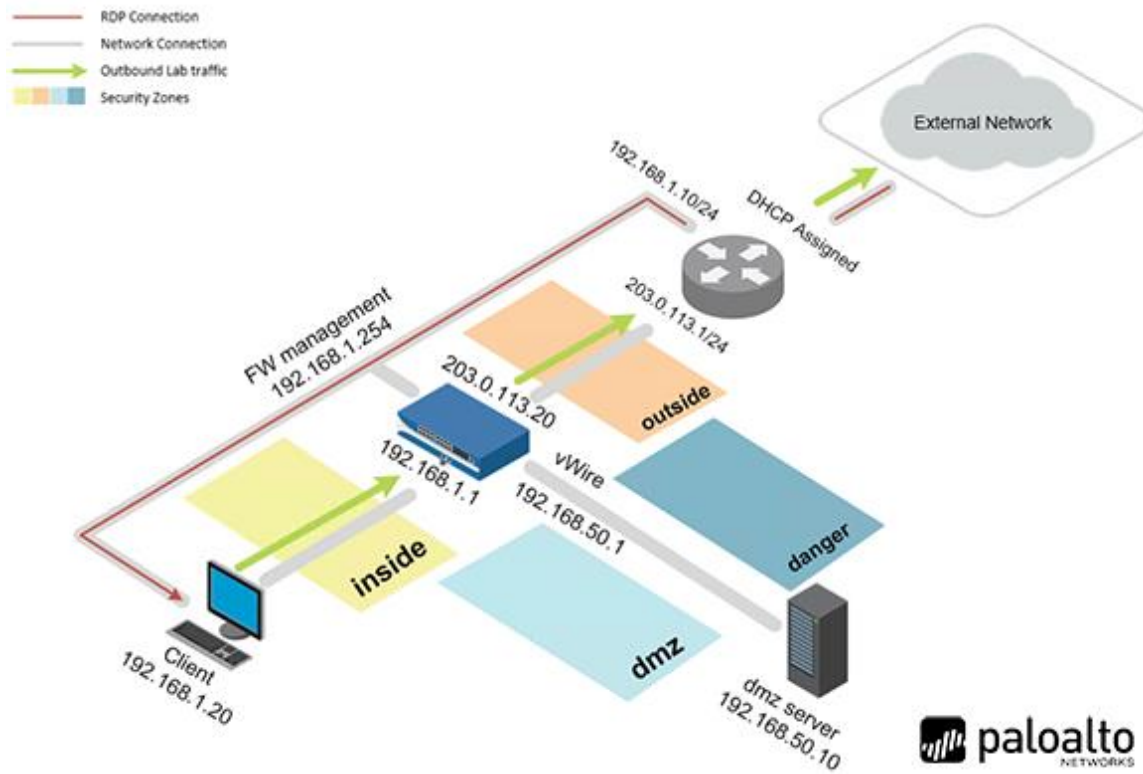
In this lab, you will utilize Wireshark to initiate a packet capture. Wireshark captures packets and allows network administrators to examine the data within the packet.

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.

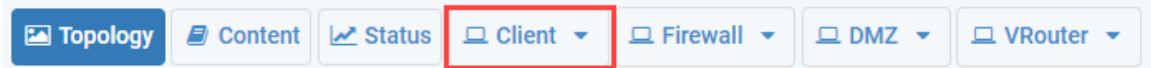
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

3 Creating Packet Captures

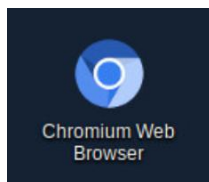
3.0 Load Lab Configuration

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

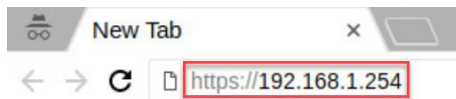
1. Click on the **Client** tab to access the Client PC.



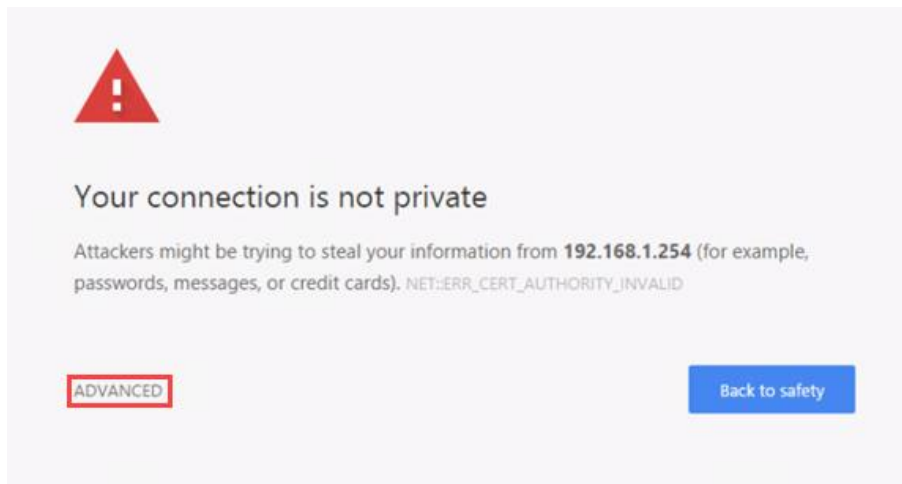
2. Log in to the Client PC as username **lab-user**, password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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

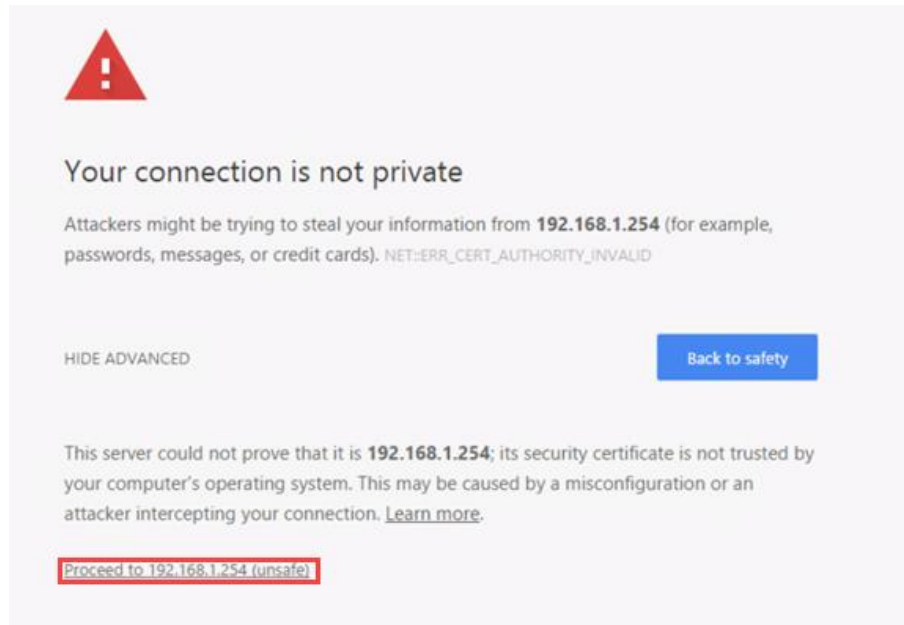


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

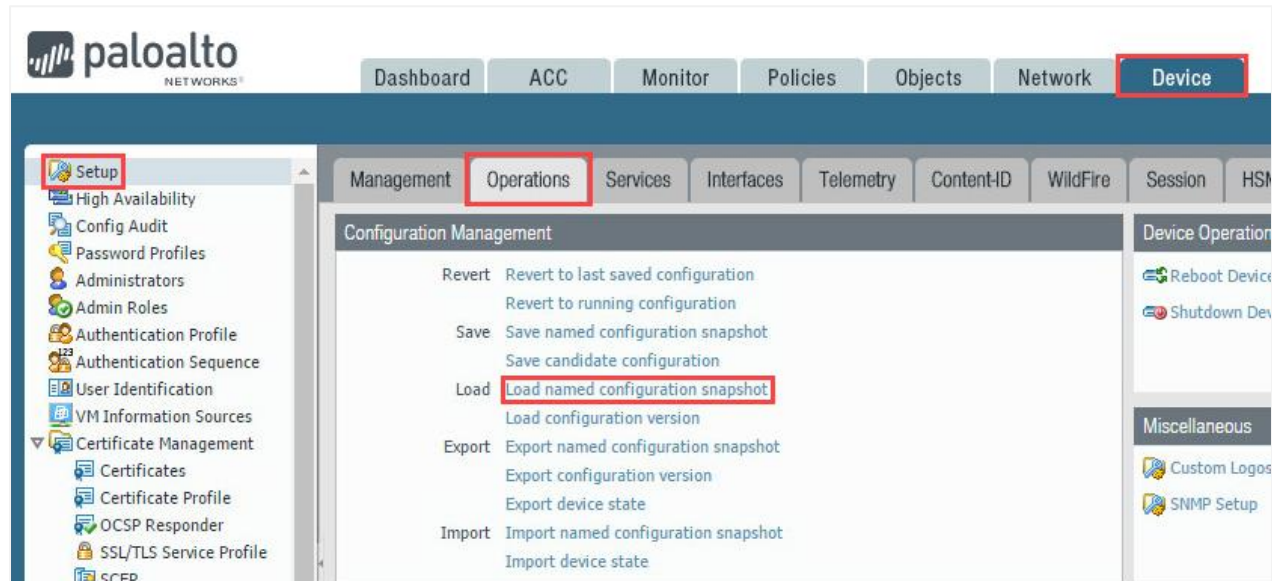
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



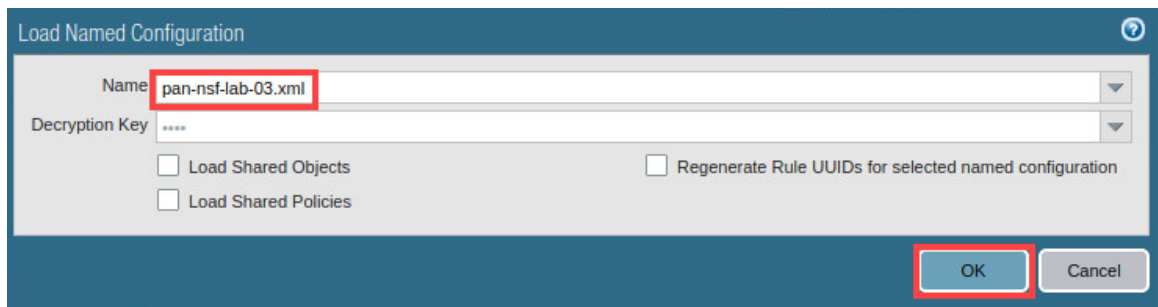
7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



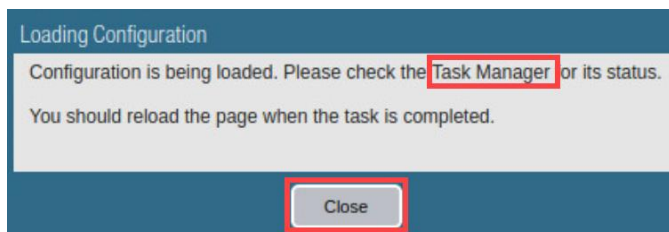
- In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



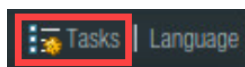
- In the *Load Named Configuration* window, select **pan-nsf-lab-03.xml** from the *Name* dropdown box and click **OK**.



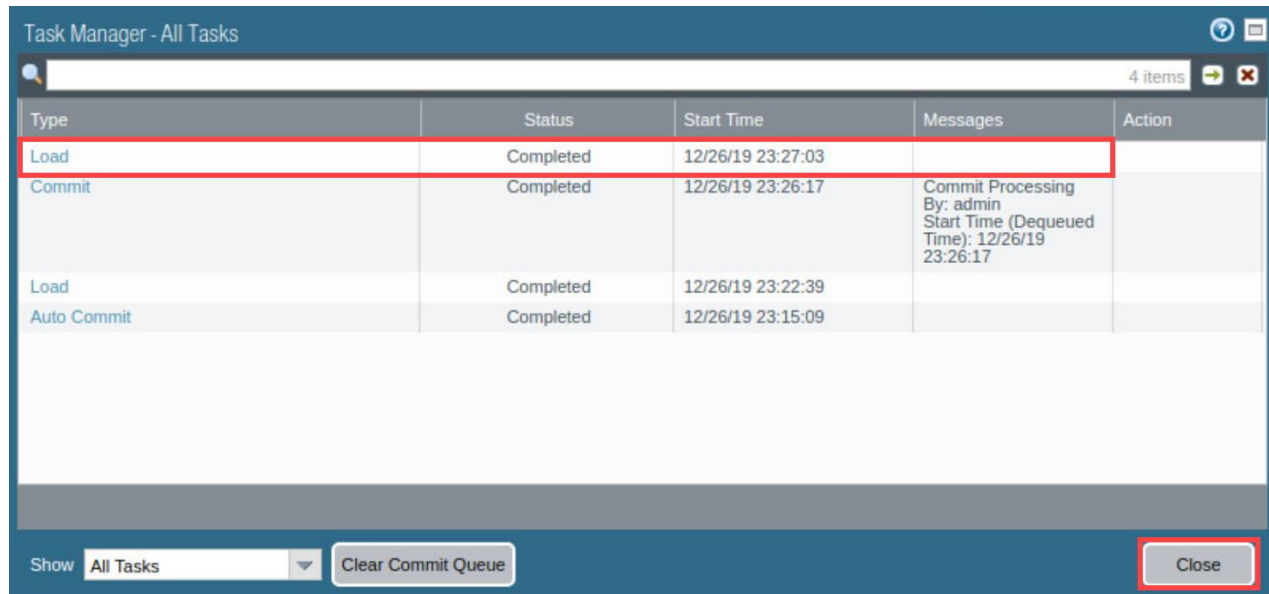
- In the Loading Configuration window, a message will show *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.



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



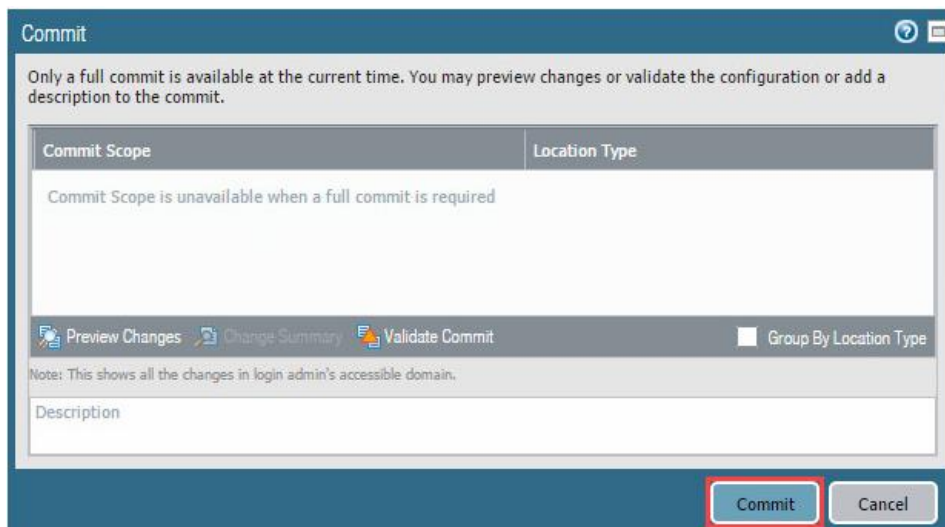
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



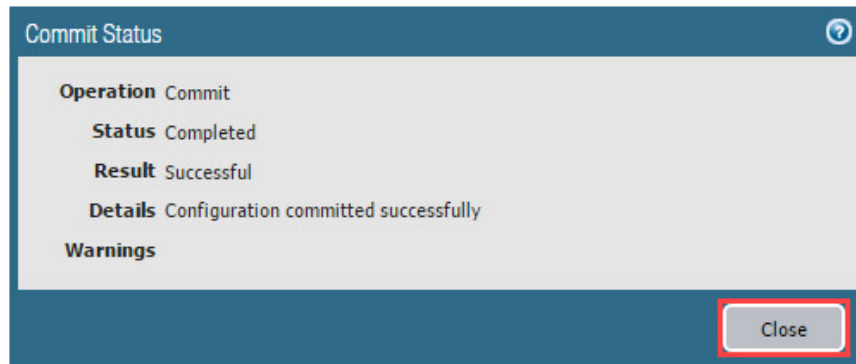
13. Click the **Commit** link located at the top-right of the web interface.



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



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

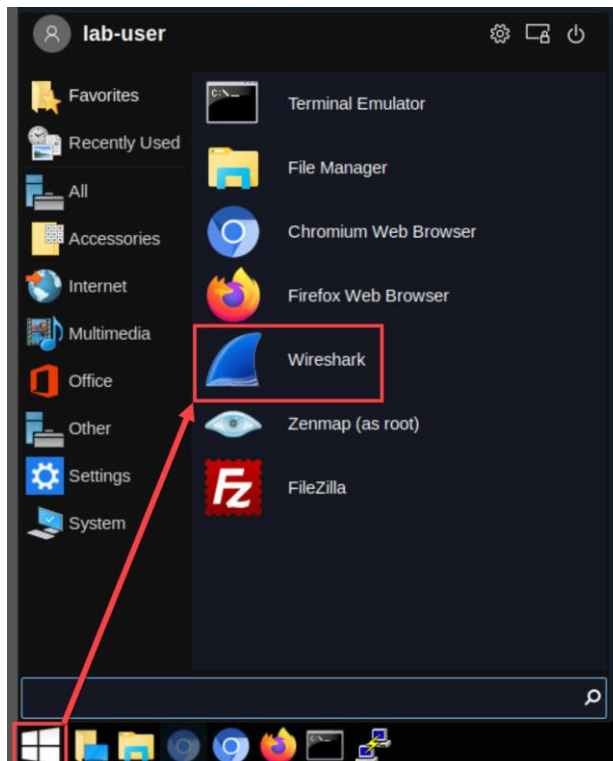


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

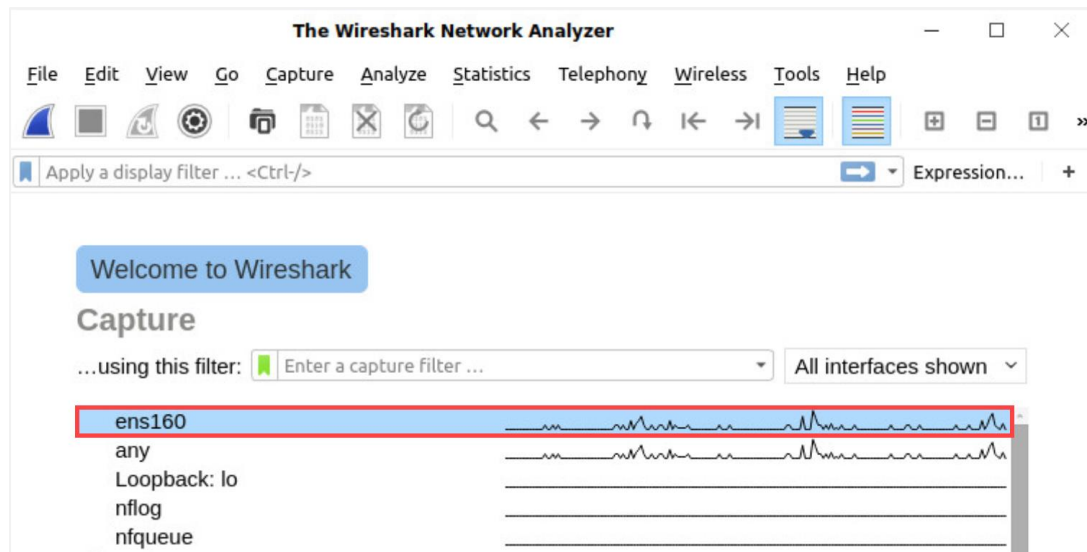
3.1 Create a Wireshark Packet Capture

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.

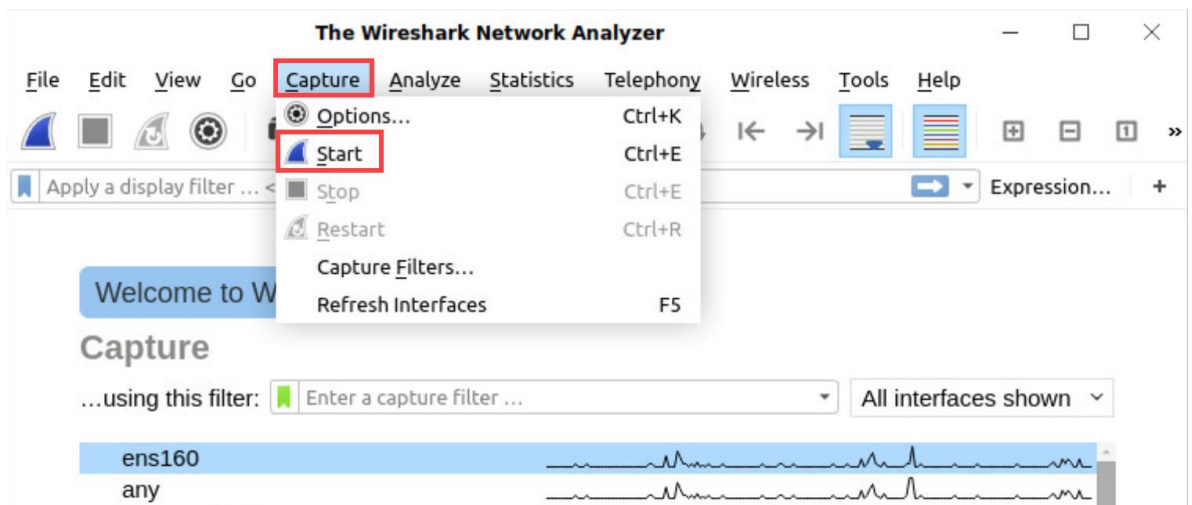
1. Click on the **Start Menu** icon, located at the bottom-left and select **Wireshark**.



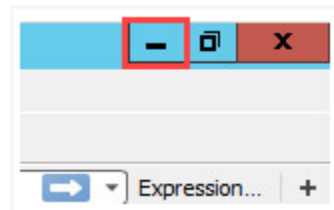
- Click on the **ens160** interface from the list.



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



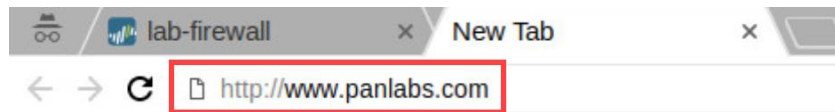
- Minimize *Wireshark* by clicking in the upper-right.



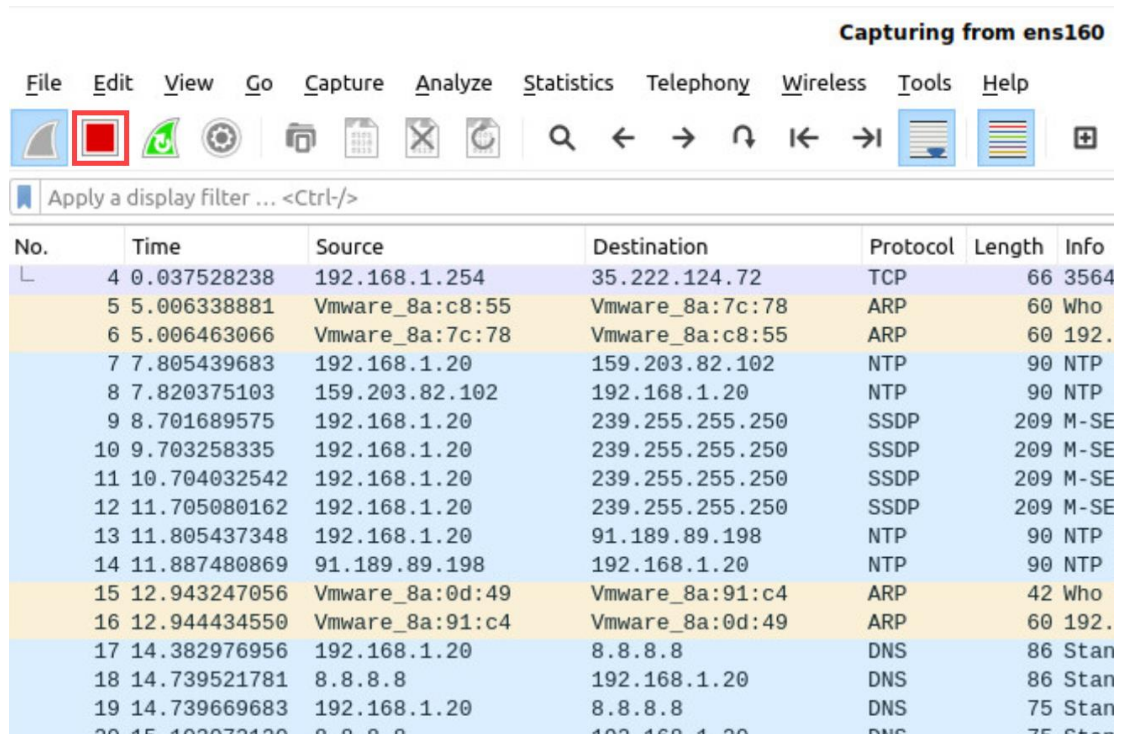
- In *Chromium*, click on the **New tab** button.



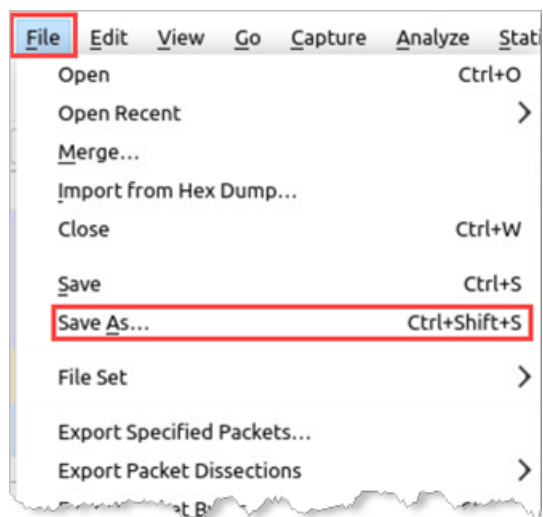
6. In the *address bar*, type `http://www.panlabs.com` and press **Enter**.



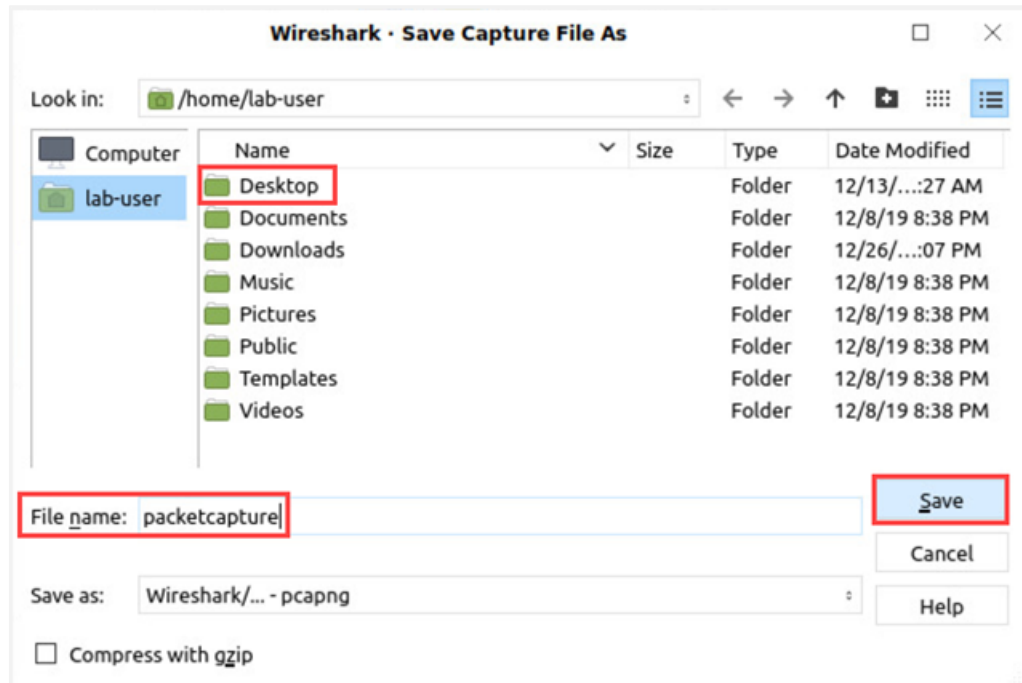
7. Wait for 5 to 10 seconds, reopen **Wireshark**, and then click the **Stop capturing packets** button.



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



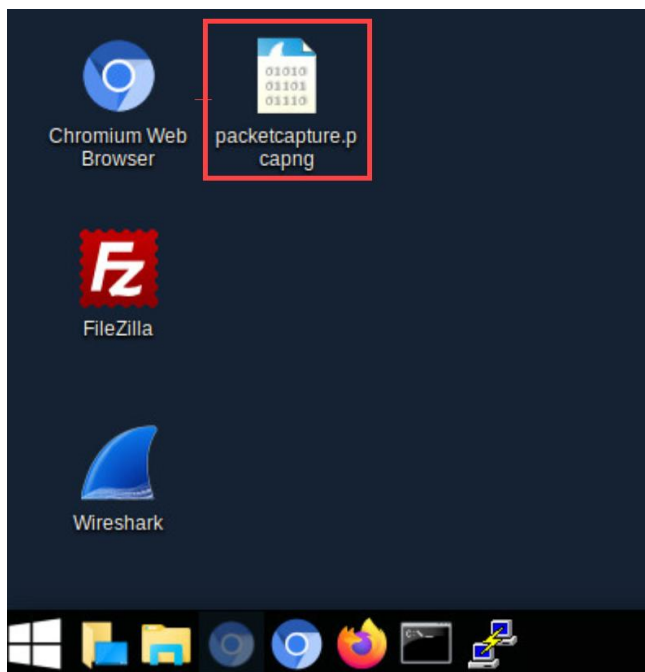
9. In the *Save file as* window, double-click on **Desktop** in the *Name* pane. Verify the path `/home/lab-user/Desktop` is shown, type **packetcapture** in the *File name* field. Finally, click **Save**.



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



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



12. While examining the Wireshark Packet Capture, notice the **ARP**, **DNS**, **TCP**, and **HTTP** Protocols.

packetcapture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
5	6.201794126	Vmware_8a:0d:49	Vmware_8a:91:c4	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20
6	6.202687709	Vmware_8a:91:c4	Vmware_8a:0d:49	ARP	60	192.168.1.1 is at 00:50:56:8a:91:c4
33	19.540129840	35.222.124.72	192.168.1.254	TCP	60	443 → 48910 [RST] Seq=1 Win=0 Len=0
51	24.515475554	Vmware_8a:c8:55	Vmware_8a:7c:78	ARP	60	Who has 192.168.1.254? Tell 192.168.1.10
52	24.516009077	Vmware_8a:7c:78	Vmware_8a:c8:55	ARP	60	192.168.1.254 is at 00:50:56:8a:7c:78
27	19.506029379	192.168.1.254	35.222.124.72	TCP	66	48910 → 443 [RST, ACK] Seq=32 Ack=1 Win=296
35	19.552385184	192.168.1.254	35.222.124.72	TCP	66	60910 → 443 [ACK] Seq=1 Ack=1 Win=14720 Len=
37	19.593217837	35.222.124.72	192.168.1.254	TCP	66	443 → 60910 [ACK] Seq=1 Ack=274 Win=29312 Le
40	19.596507097	192.168.1.254	35.222.124.72	TCP	66	60910 → 443 [ACK] Seq=274 Ack=5809 Win=26240
45	19.633291741	35.222.124.72	192.168.1.254	TCP	66	443 → 60910 [ACK] Seq=5809 Ack=4811 Win=3840
48	19.715623037	35.222.124.72	192.168.1.254	TCP	66	443 → 60910 [ACK] Seq=5860 Ack=5461 Win=4403
50	19.769411307	192.168.1.254	35.222.124.72	TCP	66	60910 → 443 [ACK] Seq=5461 Ack=6171 Win=3788
32	19.518235506	192.168.1.254	35.222.124.72	TCP	74	60910 → 443 [SYN] Seq=0 Win=14600 Len=0 MSS=
34	19.551933060	35.222.124.72	192.168.1.254	TCP	74	443 → 60910 [SYN, ACK] Seq=0 Ack=1 Win=28160
24	17.652171591	192.168.1.20	8.8.8.8	DNS	75	Standard query 0x8df3 A www.panlabs.com
25	18.014309102	8.8.8.8	192.168.1.20	DNS	75	Standard query response 0x8df3 Server failure
22	17.185906534	192.168.1.20	8.8.8.8	DNS	86	Standard query 0x8df3 A www.panlabs.com OPT
23	17.652011302	8.8.8.8	192.168.1.20	DNS	86	Standard query response 0x8df3 Server failure



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 address to IP addresses.

DNS, Domain Name System, resolves fully qualified domain names to an IP address. For example, if you type www.google.com in a web browser, DNS resolves www.google.com to the associated IP address.

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.

HTTP, Hypertext Transfer Protocol, is a TCP application protocol for distributed, collaborative, and hypermedia information systems. Web servers use HTTP to show information to web browsers.

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