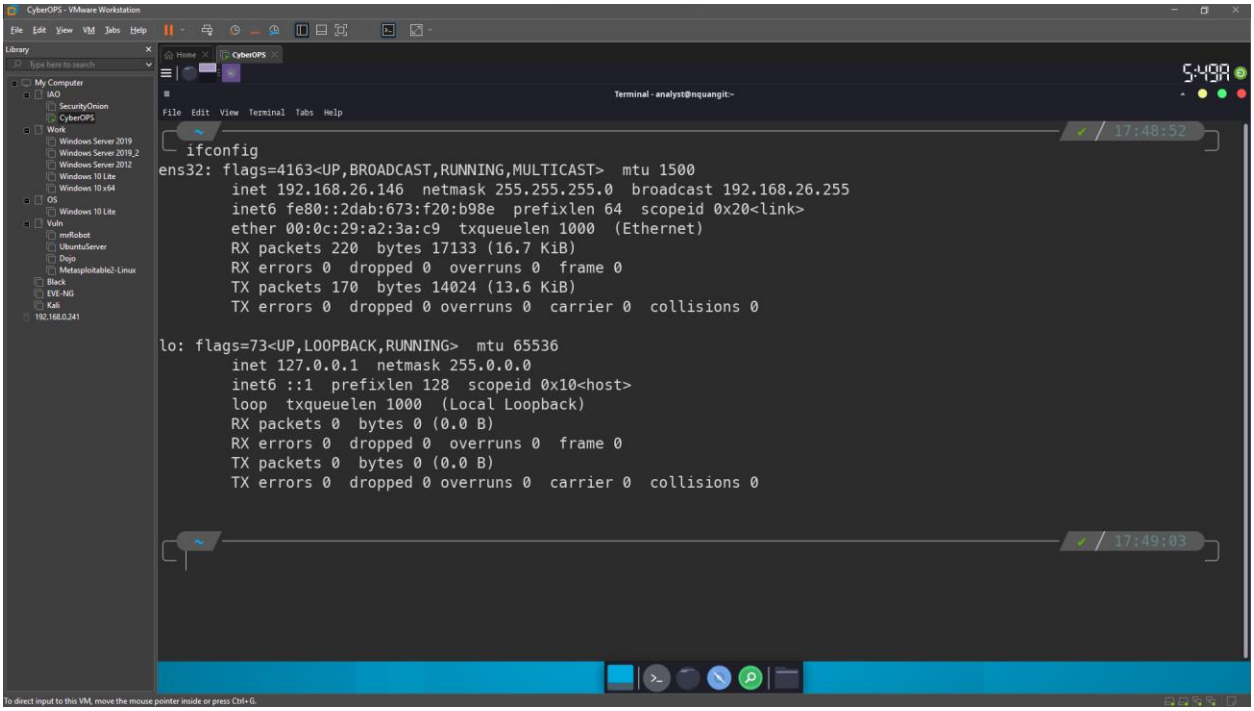
Lab - Introduction to Wireshark

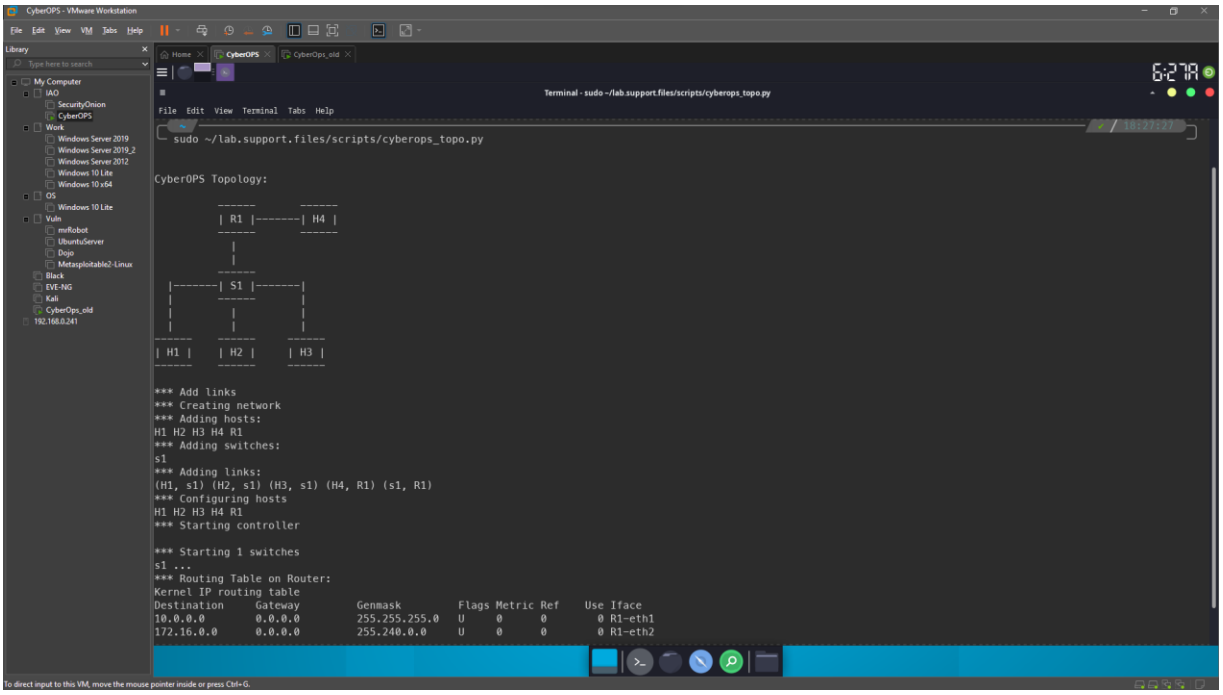
Instructions

Install and Verify the Mininet Topology

Verify your PC's interface addresses.

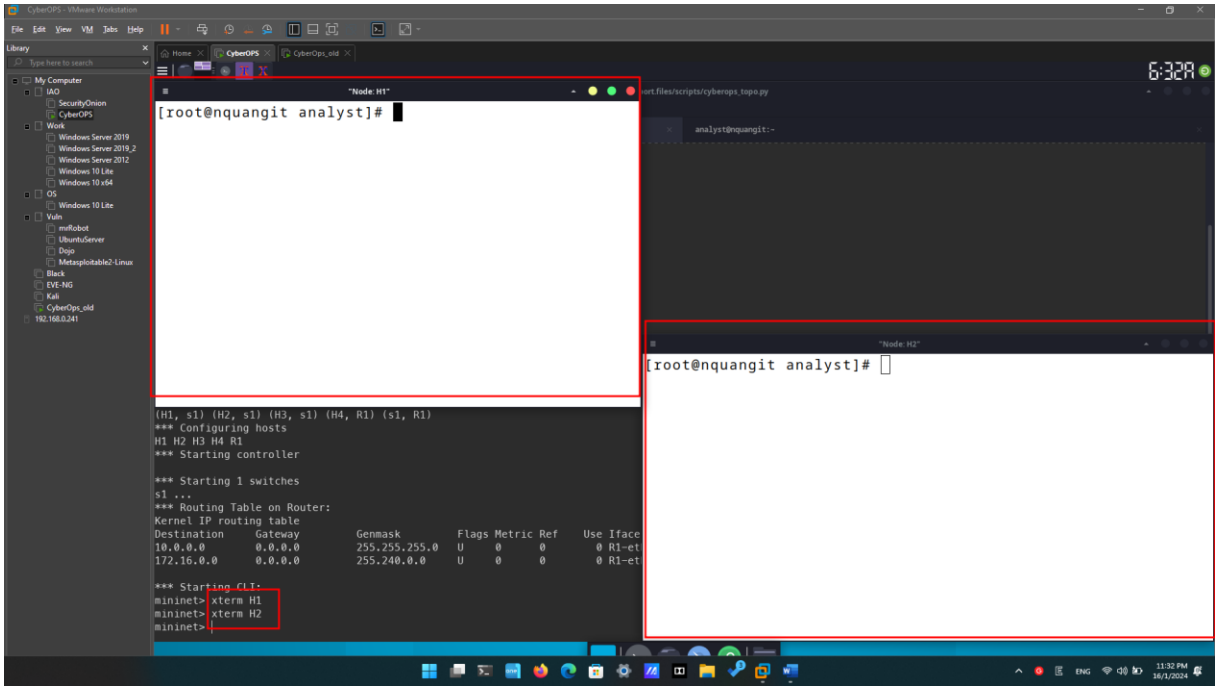


Run the Python script to install the Mininet Topology.

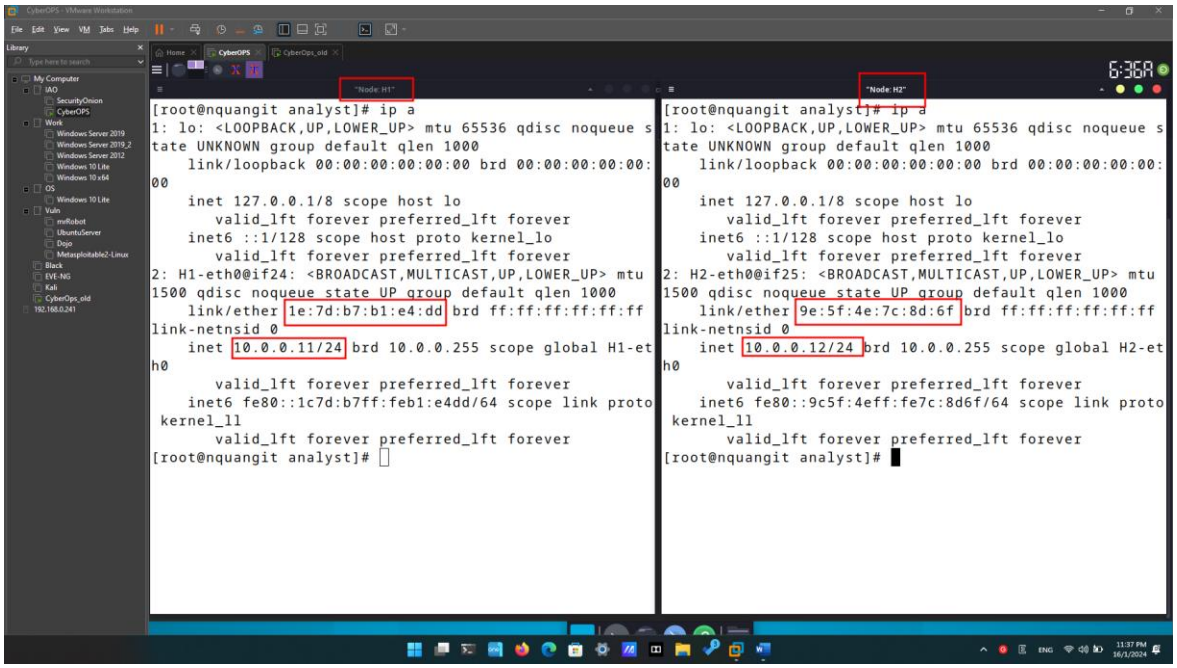


Record IP and MAC addresses for H1 and H2.

a. At the mininet prompt, start terminal windows on hosts H1 and H2. This will open separate windows for these hosts. Each host will have a separate configuration for the network including unique IP and MAC addresses.



b. At the prompt on **Node: H1**, enter **ip address** to verify the IPv4 address and record the MAC address. Do the same for **Node: H2**. The IPv4 address and MAC address are highlighted below for reference.

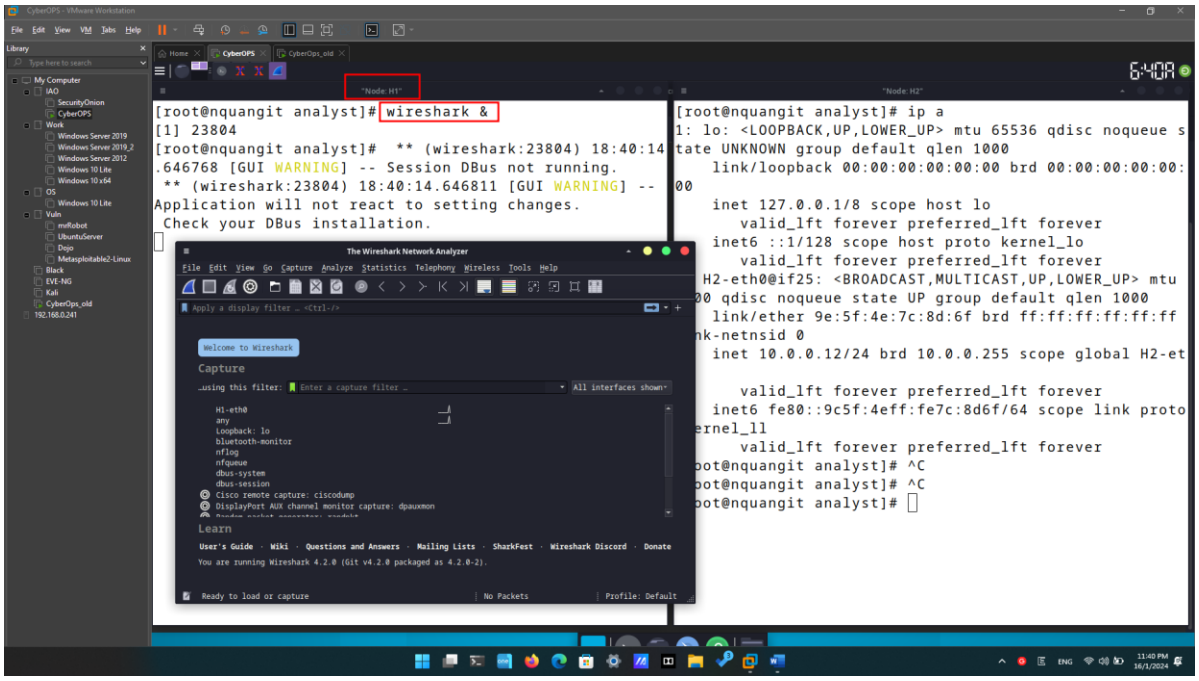


Host-interface	IP Address	MAC Address
H1-eth0	10.0.0.11/24	1e:7d:b7:b1:e4:dd
H2-eth0	10.0.0.12/24	9e:5f:4e:7c:8d:6f

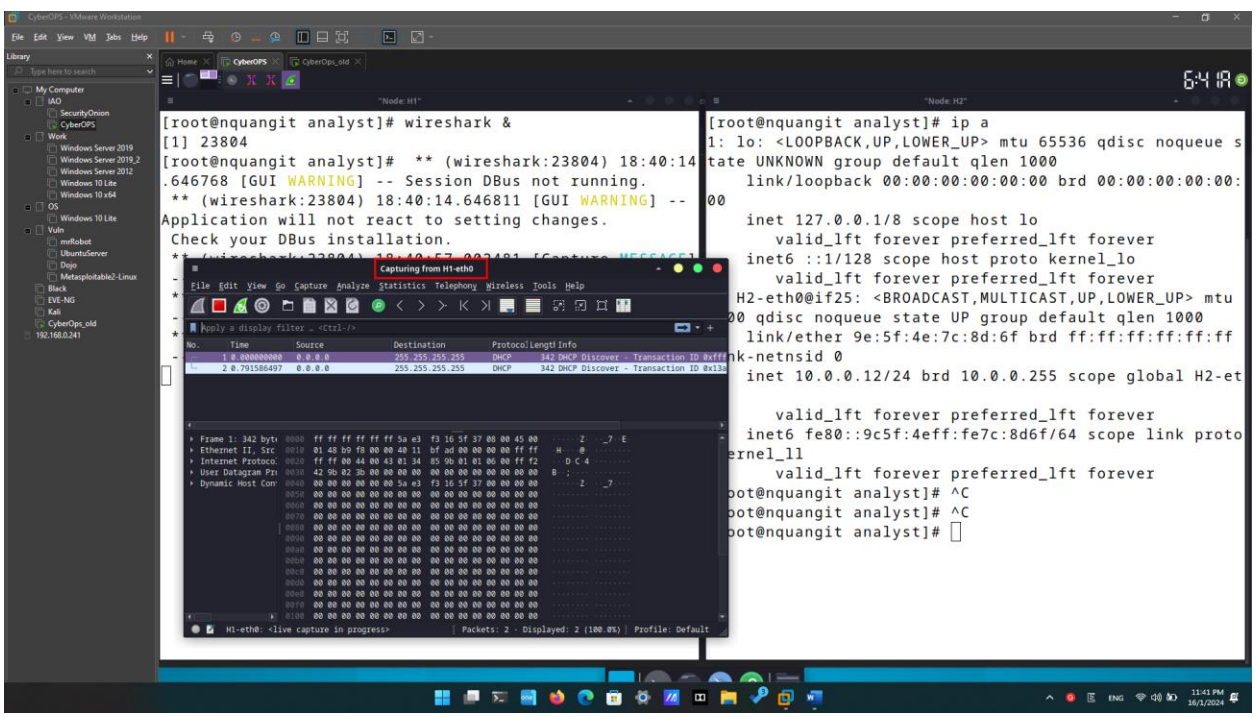
Capture and Analyze ICMP Data in Wireshark

Examine the captured data on the same LAN.

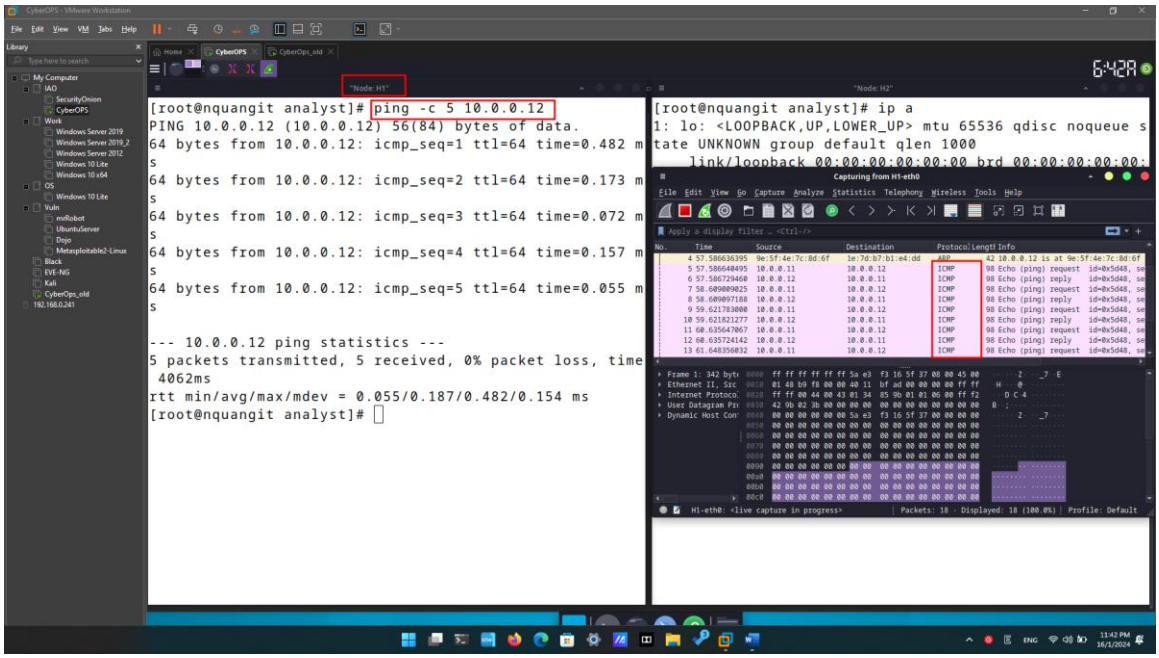
a. On **Node: H1**, enter **wireshark &** to start Wireshark (The pop-up warning is not important for this lab.). Click **OK** to continue.



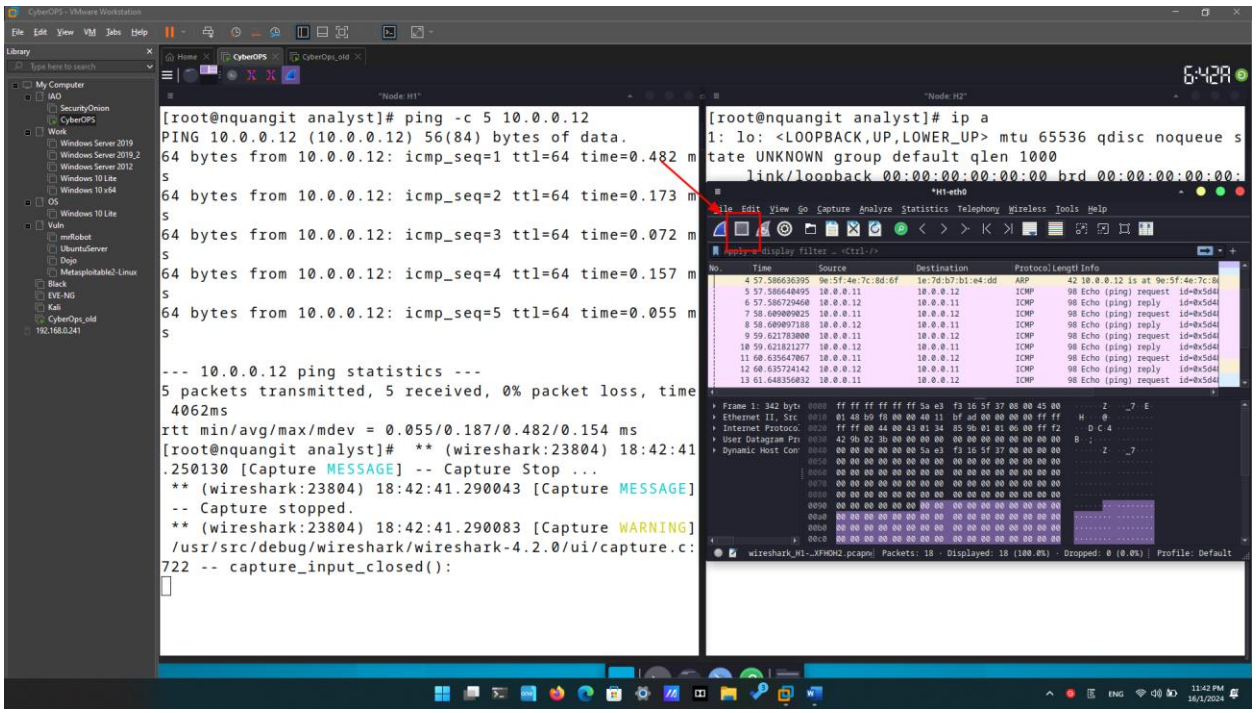
b. In the Wireshark window, under the **Capture** heading, select the **H1-eth0** interface. Click **Start** to capture the data traffic.



c. On **Node: H1**, press the Enter key, if necessary, to get a prompt. Then type **ping -c 5 10.0.0.12** to ping H2 five times. The command option **-c** specifies the count or number of pings. The **5** specifies that five pings should be sent. The pings will all be successful.



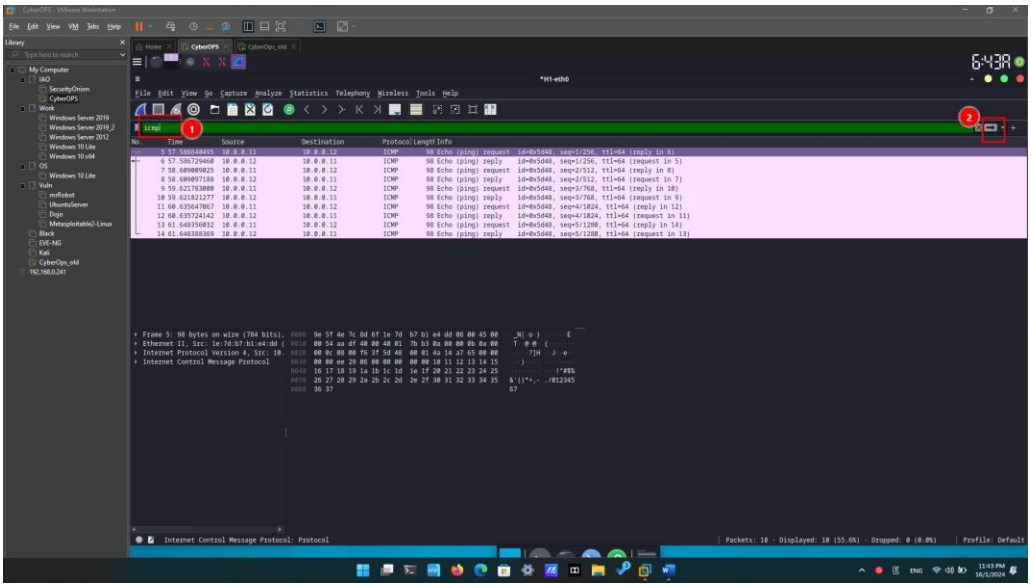
d. Navigate to the Wireshark window, click **Stop** to stop the packet capture.



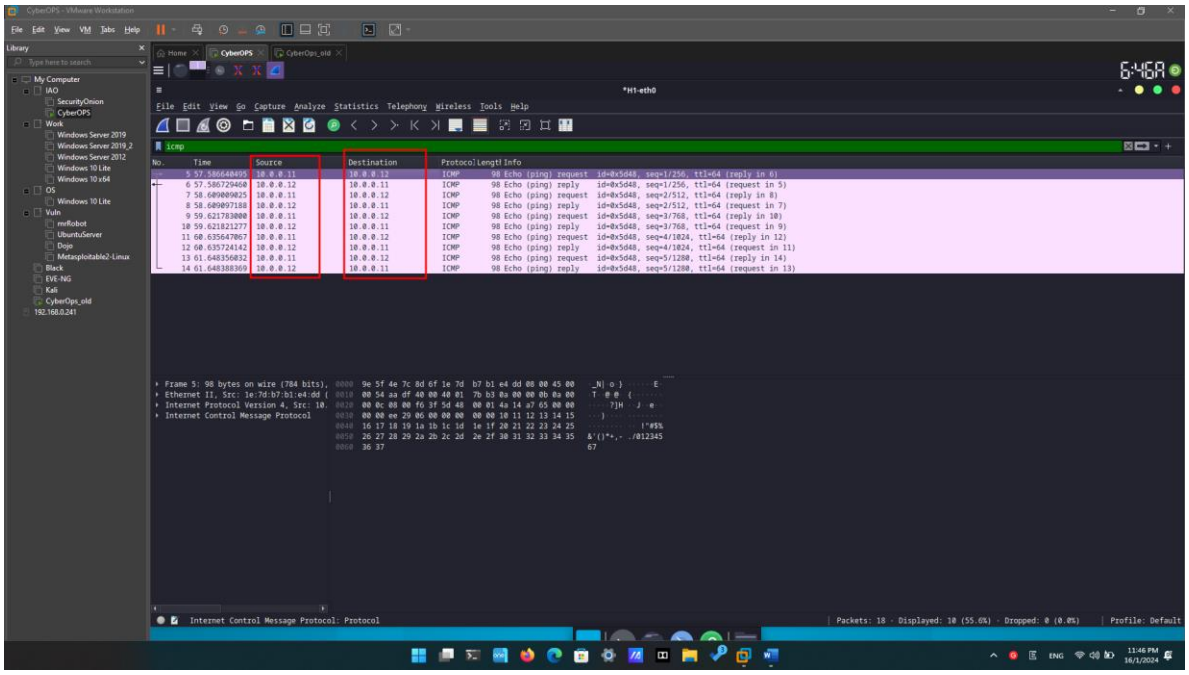
e. A filter can be applied to display only the interested traffic.

Type **icmp** in the **Filter** field and click **Apply**.

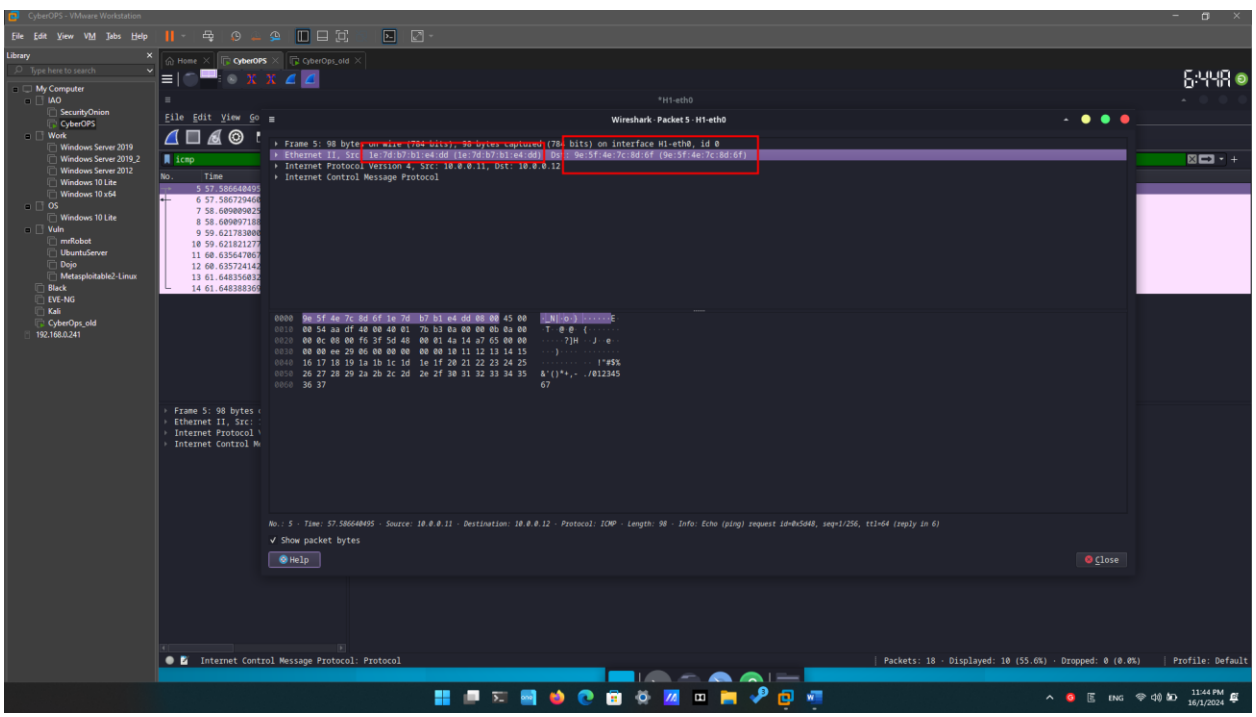
Networking Academy



f. If necessary, click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has H1's IP address, and the Destination column has H2's IP address.



g. With this PDU frame still selected in the top section, navigate to the middle section. Click the arrow to the left of the Ethernet II row to view the Destination and Source MAC addresses.



Does the Source MAC address match H1's interface?

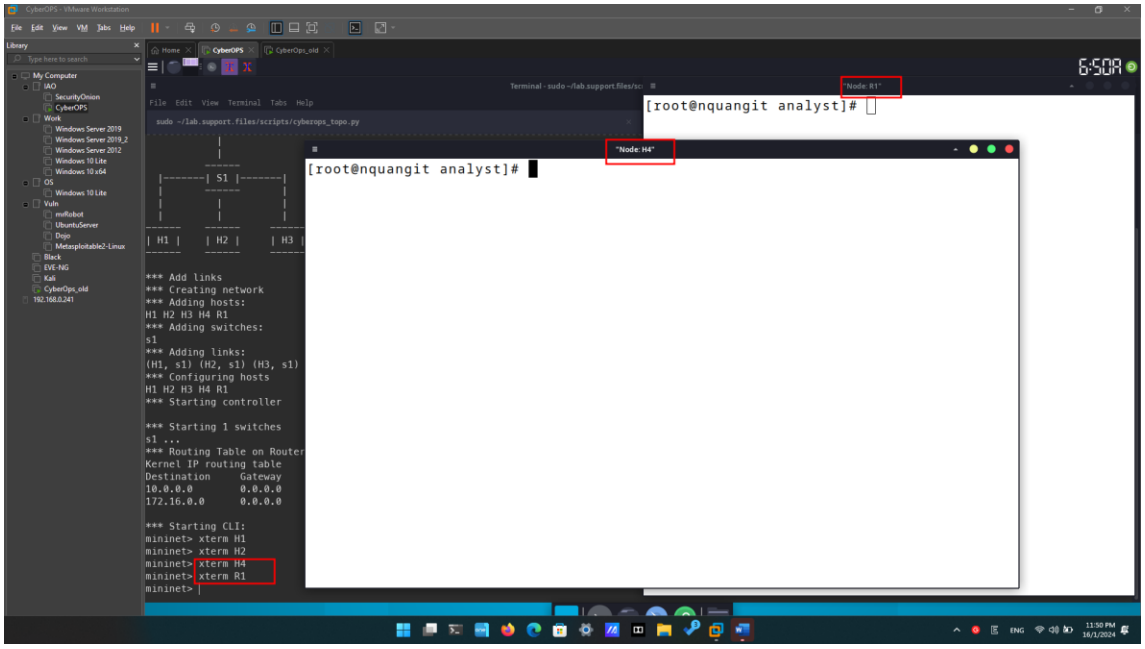
Yes

Does the Destination MAC address in Wireshark match H2's MAC address?

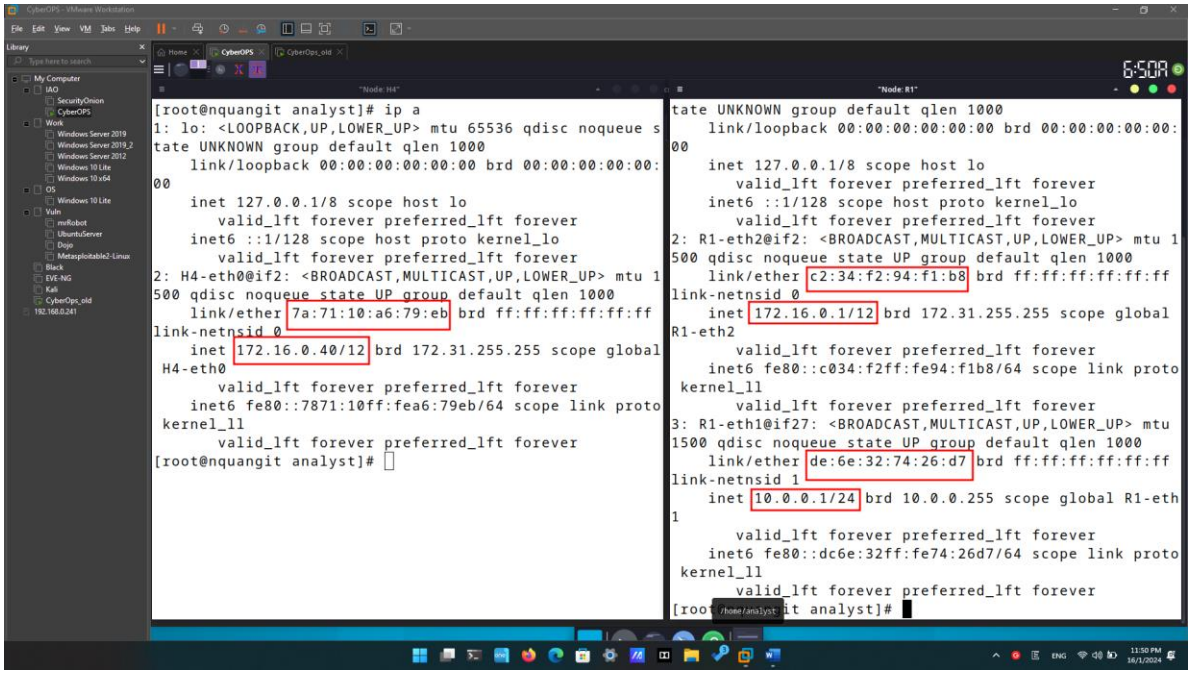
Yes

Examine the captured data on the remote LAN.

a. At the mininet prompt, start terminal windows on hosts H4 and R1.



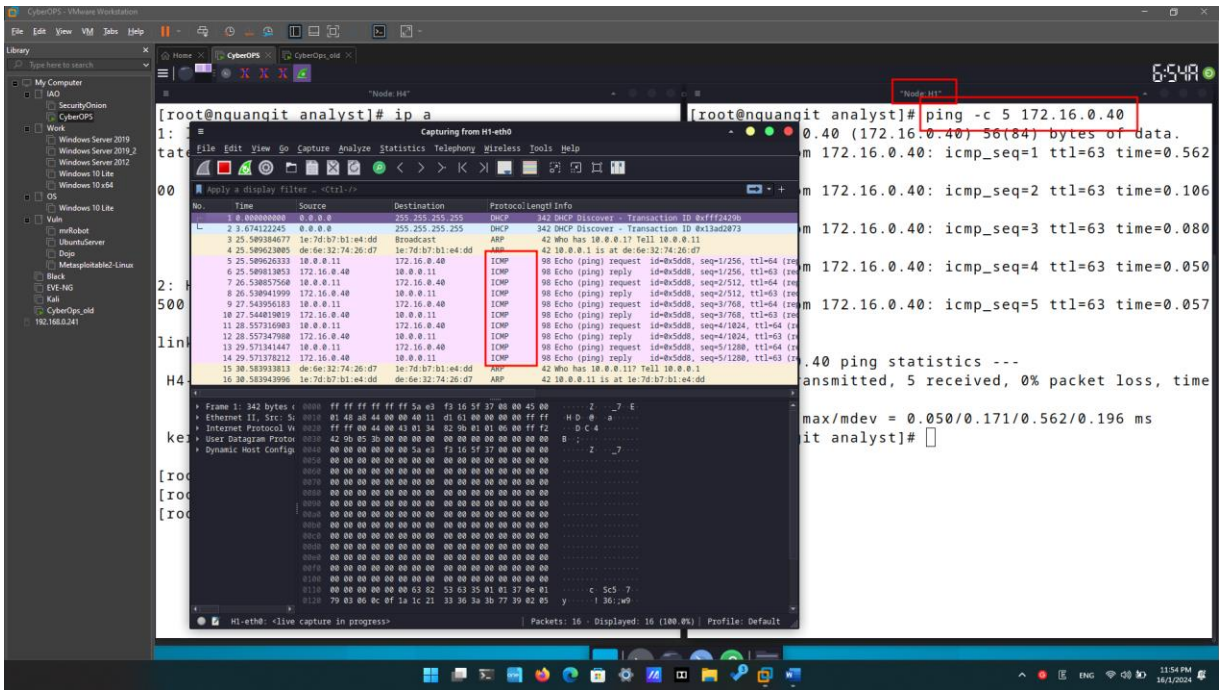
b. At the prompt on **Node: H4**, enter **ip address** to verify the IPv4 address and record the MAC address. Do the same for the **Node: R1**.



Host-interface	IP Address	MAC Address
H4-eth0	172.16.0.40/12	7a:71:10:a6:79:eb
R1-eth1	10.0.0.1/24	de:6e:32:74:26:d7
R1-eth2	172.16.0.1/12	c2:34:f2:94:f1:b8

c. Start a new Wireshark capture on H1 by selecting **Capture > Start**. You can also click the **Start** button or type **Ctrl-E** Click **Continue without Saving** to start a new capture.

d. H4 is a simulated remote server. Ping H4 from H1. The ping should be successful.

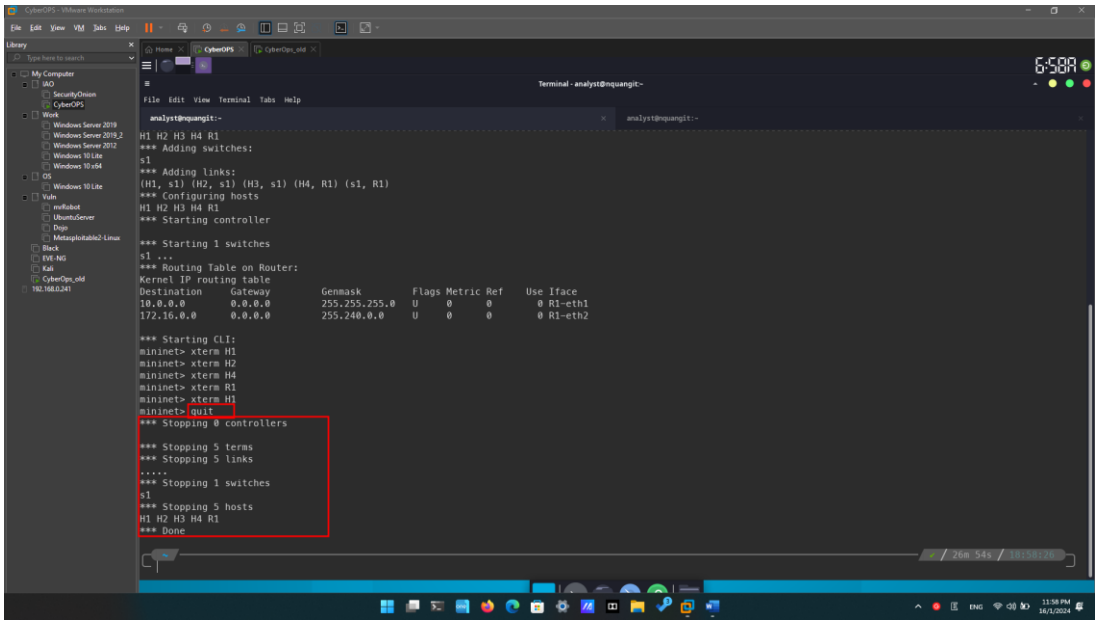


e. Review the captured data in Wireshark. Examine the IP and MAC addresses that you pinged. Notice that the MAC address is for the R1-eth1 interface. List the destination IP and MAC addresses.

IP address: 172.16.0.40, 10.0.0.11

MAC address: de:6e:32:74:26:d7, 1e:7d:b7:b1:e4:dd

f. In the main CyberOps VM window, enter **quit** to stop Mininet.



g. To clean up all the processes that were used by Mininet, enter the **sudo mn -c** command at the prompt.