

Syahira Azizah Rendra Putri

SIB – 4C / 18 / 2141762059

Lab - Use Wireshark to Compare Telnet and SSH Traffic

Objectives

- Use Wireshark to capture web browser traffic.
- Use Wireshark to capture Telnet traffic.
- Use Wireshark to capture SSH traffic.

Background / Scenario

Wireshark is a network protocol analyzer that lets you see what's happening on your network at a microscopic level. You can capture packets and store them for offline analysis. Wireshark includes many tools for deep inspection of hundreds of network protocols. In this lab, you will use Wireshark to capture and inspect web traffic, Telnet traffic, and SSH traffic.

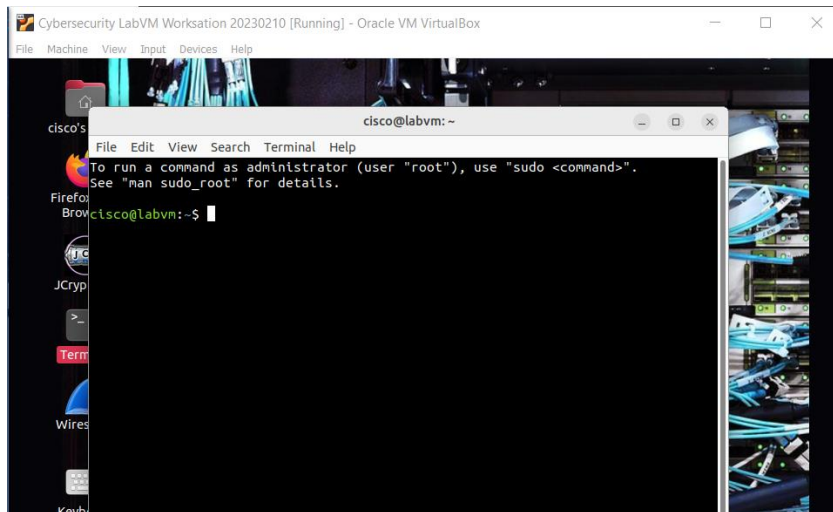
Required Resources

PC with the **CSE-LABVM** installed in VirtualBox

Instructions

Step 1: Open a terminal window in the CSE-LABVM.

- Launch the **CSE-LABVM**.
- Double-click the **Terminal** icon to open a terminal.



Step 2: Explore the Wireshark protocol analyzer.

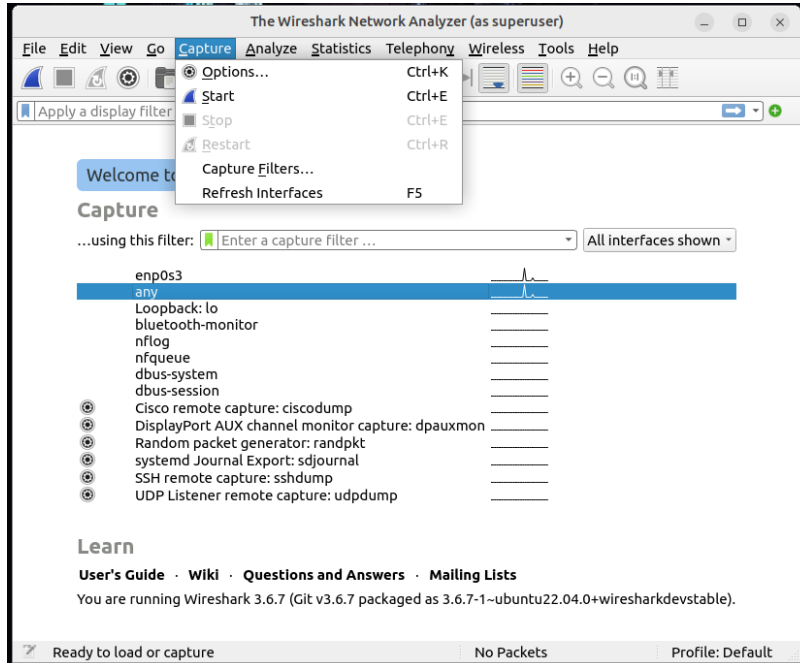
- To capture traffic on your VM, you need to run Wireshark in promiscuous mode, which requires running with escalated privileges using **sudo**. Enter the **sudo wireshark** command, and then enter **password** for the password. The Wireshark graphical user interface (GUI) will open up.

```
cisco@labvm:~$ sudo wireshark
```

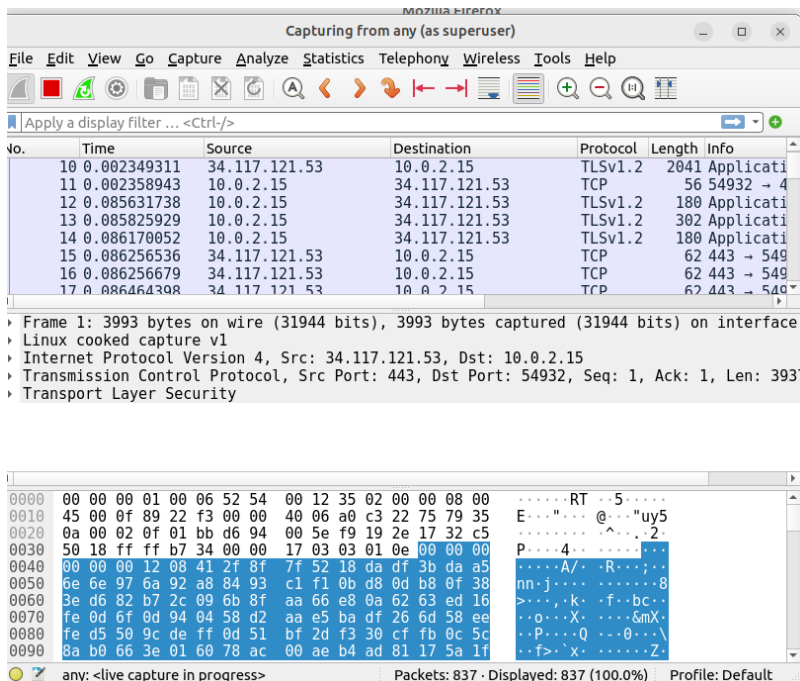
```
[sudo] password for cisco: password
```

```
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

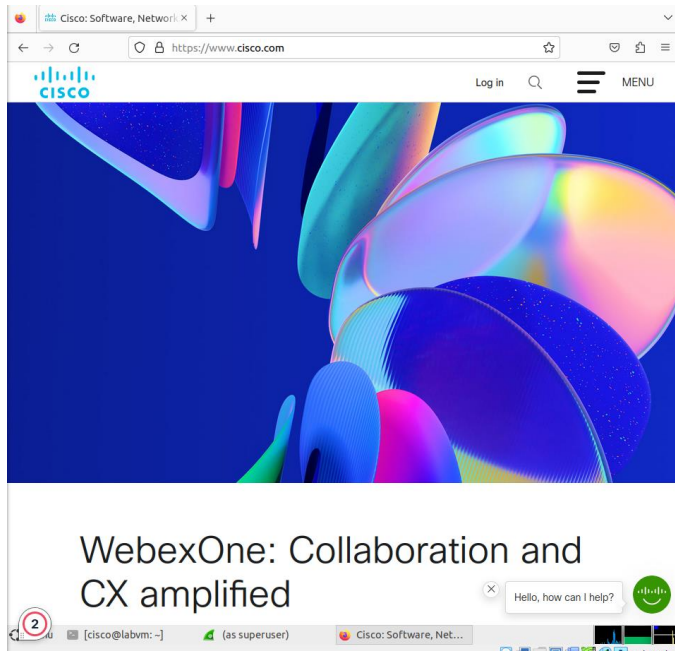
- b. Under the listing of interfaces, select **any**, and then click **Capture > Start** from the menus. Alternatively, you can click the shark fin icon. Wireshark will begin capturing packets.



- c. If you already have Firefox open, you may see traffic captured in the Wireshark interface. If Firefox is not open, go ahead and open it now. In Wireshark, you should now see captured TCP traffic in the top third of the window.



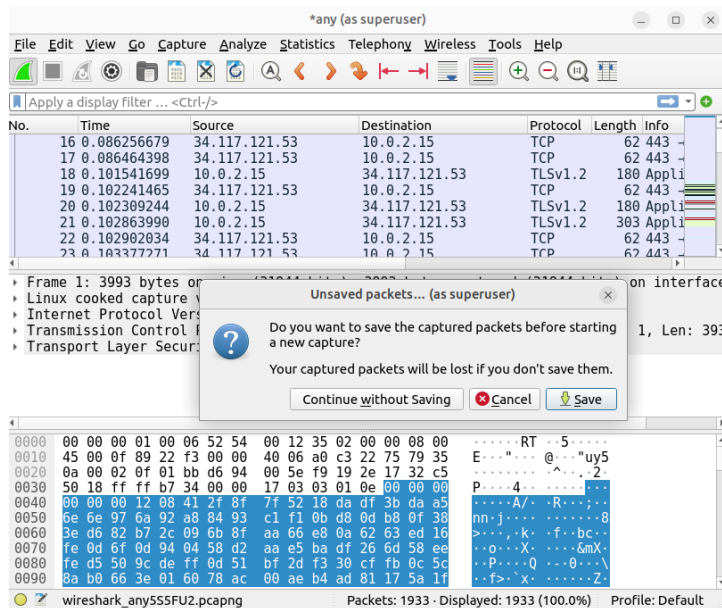
- d. In Firefox, enter www.cisco.com to visit the Cisco website. After the website loads, you can close Firefox.



- e. Return to Wireshark and click **Capture > Stop** from the menus. Alternatively, you can click the red square button next to the shark fin.
- f. In Wireshark, you will see the filter field and three key panes or work areas:
 - The **Apply a display filter** field is directly below the toolbar.
 - The **Packet List** pane includes the following columns for each captured packet:
 - **No** - the number of the packet (in numerical order).
 - **Time** - the timestamp of the packet
 - **Source** - the source IP address of the packet
 - **Destination** - the destination IP address of the packet
 - **Protocol** - the protocol of the packet
 - **Length** - the number of bytes captured for this packet
 - **Info** - additional information about the packet's content
 - The **Packet Details** pane shows the protocols and protocol fields of the selected packet. Notice that the fields can be expanded or collapsed by clicking the arrow next to the field.
 - The **Packet Bytes** pane shows the byte details of the selected packet. As you select parts of the packet in the Packet Details pane, the corresponding bytes will be highlighted in the Packet Bytes pane. The left side shows the hexadecimal representation of the bytes, and the right side shows the ASCII representation.

Step 3: Capture and analyze unencrypted Telnet traffic.

- Start a new capture. In the **Unsaved packets...** dialog box, click **Continue without Saving**. This will clear out the packets from your last capture and start a new capture.



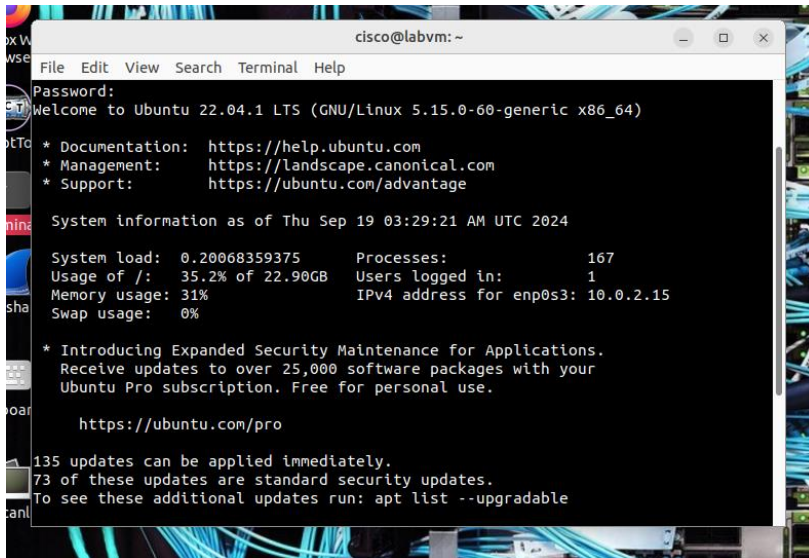
- Double-click the **Terminal** icon to open a new terminal window.
- You can simulate a remote login to your VM by entering the **telnet localhost** command, and then logging in as **cisco** with **password** as the password.

```
cisco@labvm:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
labvm login: cisco
Password: password
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
```

```
0 updates can be installed immediately.
0 of these updates are security updates.
```

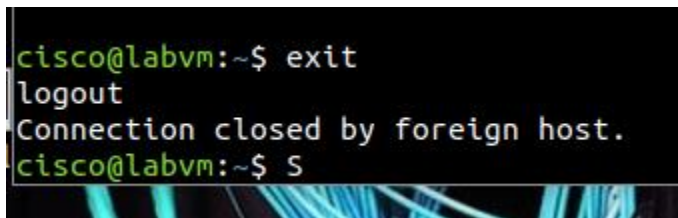
```
Last login: Thu Mar 18 21:47:23 UTC 2021 on tty2
cisco@labvm:~$
```



```
cisco@labvm: ~  
File Edit View Search Terminal Help  
Password:  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Thu Sep 19 03:29:21 AM UTC 2024  
  
System load:  0.20068359375    Processes:            167  
Usage of /:   35.2% of 22.9GB   Users logged in:      1  
Memory usage: 31%             IPv4 address for enp0s3: 10.0.2.15  
Swap usage:   0%  
  
* Introducing Expanded Security Maintenance for Applications.  
  Receive updates to over 25,000 software packages with your  
  Ubuntu Pro subscription. Free for personal use.  
  
  https://ubuntu.com/pro  
  
135 updates can be applied immediately.  
73 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable
```

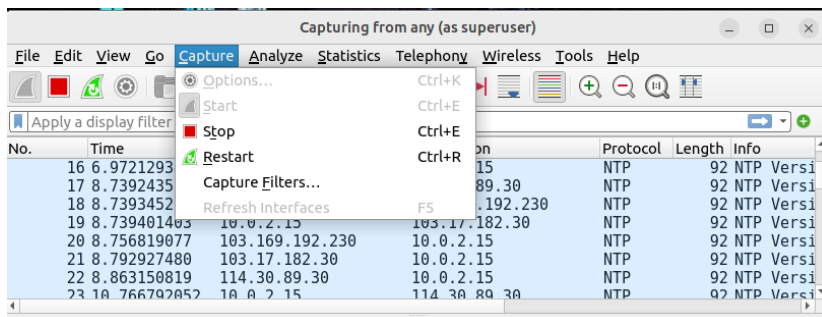
- d. Enter the **exit** command to end the Telnet session:

```
cisco@labvm:~$ exit  
logout  
Connection closed by foreign host.  
cisco@labvm:~$
```

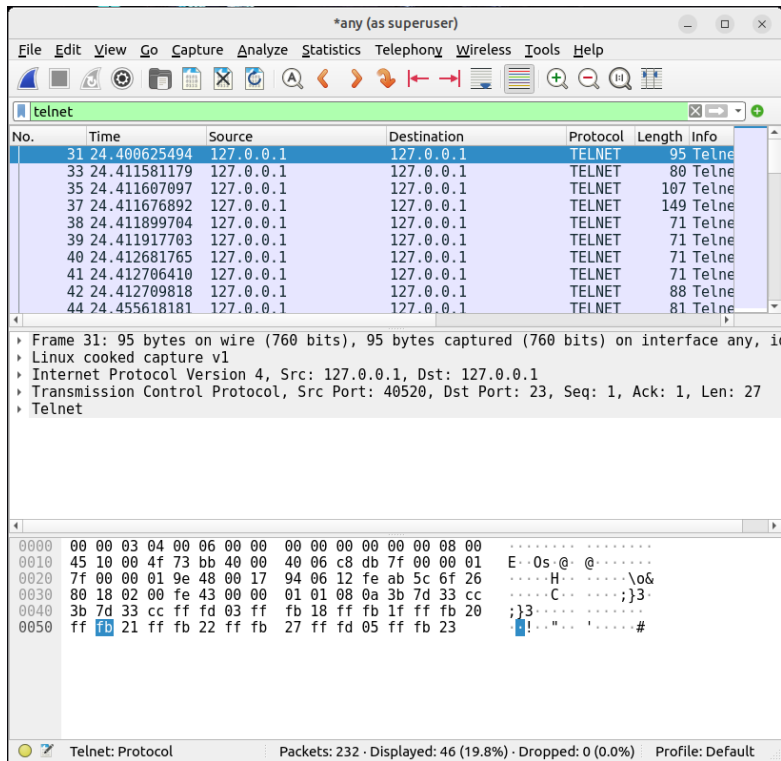


```
cisco@labvm:~$ exit  
logout  
Connection closed by foreign host.  
cisco@labvm:~$
```

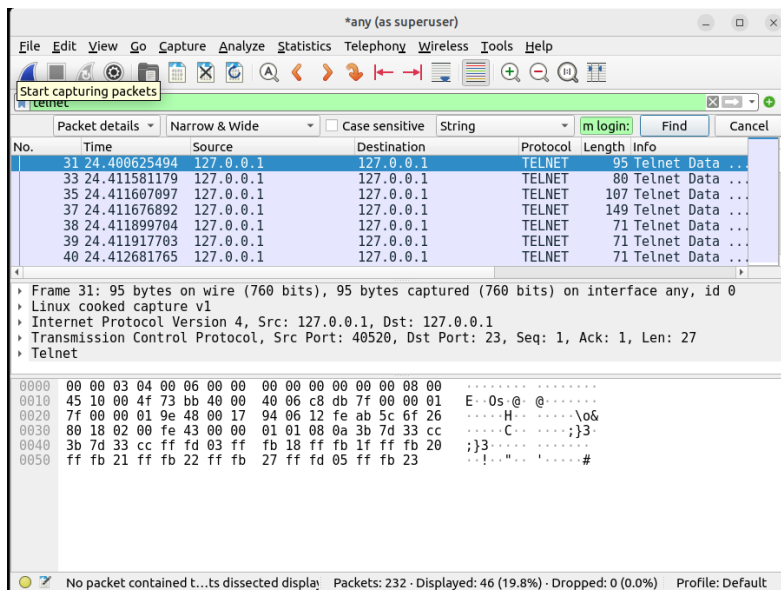
- e. Return to Wireshark and stop the capture.



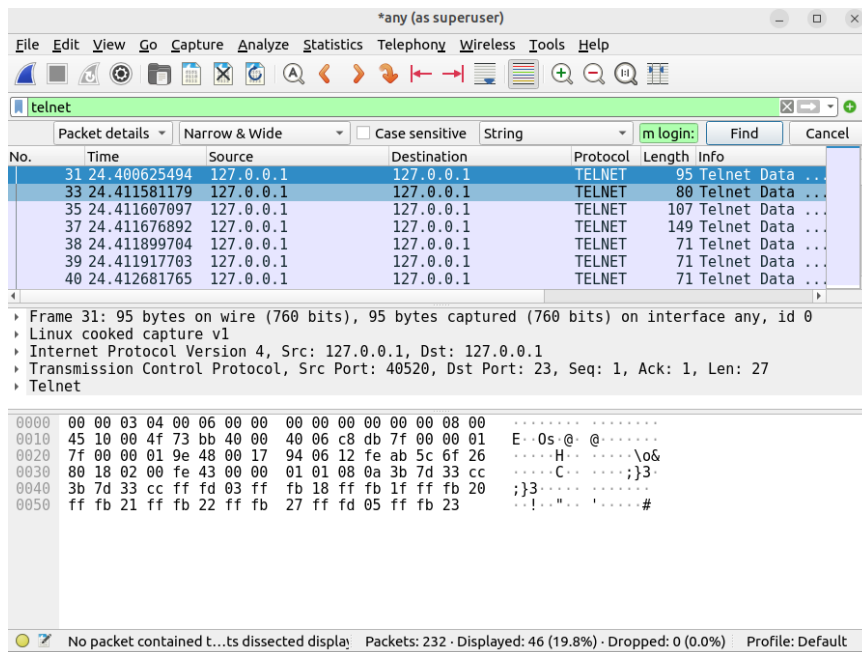
- f. In the **Apply a display filter** field, type **telnet** and press **Enter** to filter for only Telnet packets.



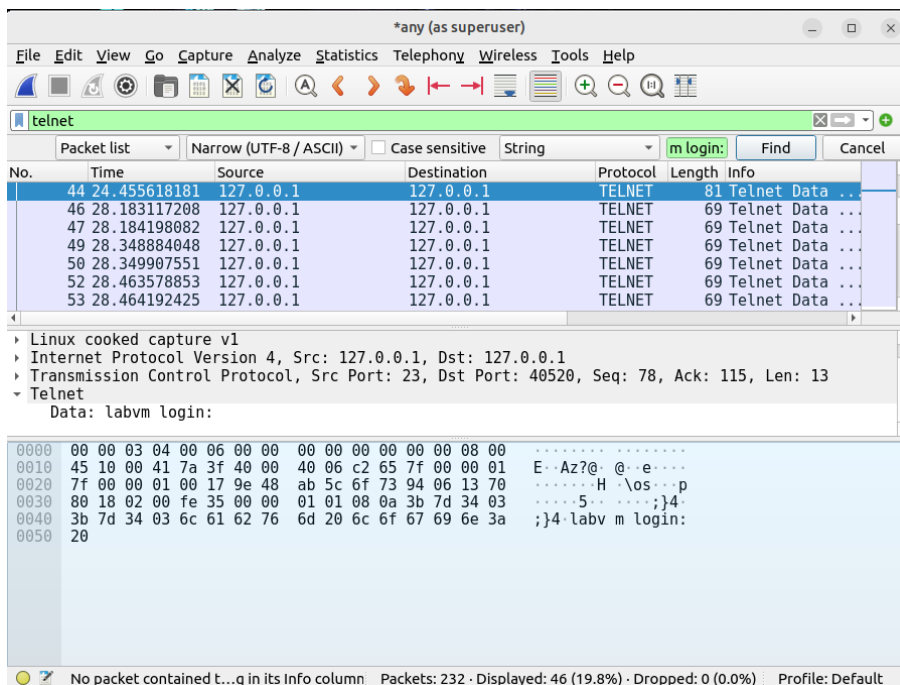
- g. On the toolbar, click the magnifying glass icon to **Find a packet**. Additional search features are now shown below the **Apply a display filter** field.
- h. Click the arrows next to **Display filter** and change it to **String**. Then click the arrows next to Packet list and change it to **Packet details**.



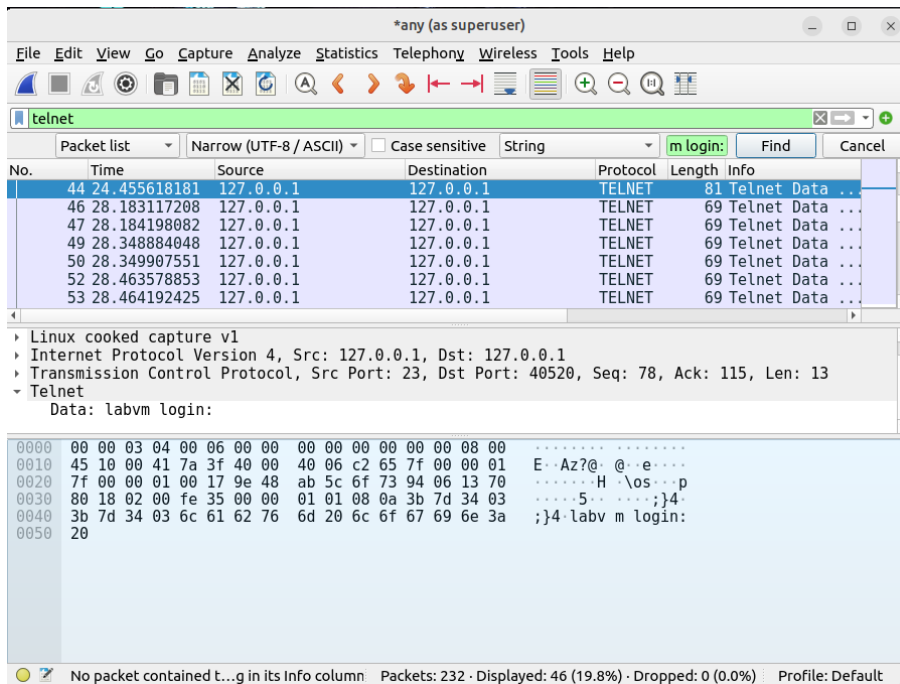
- i. To find the packet requesting login information, type **labvm login:** in the field next to **String**, and then press **Enter** or click **Find**. Wireshark will highlight the packet that contains the "labvm login:" text string.



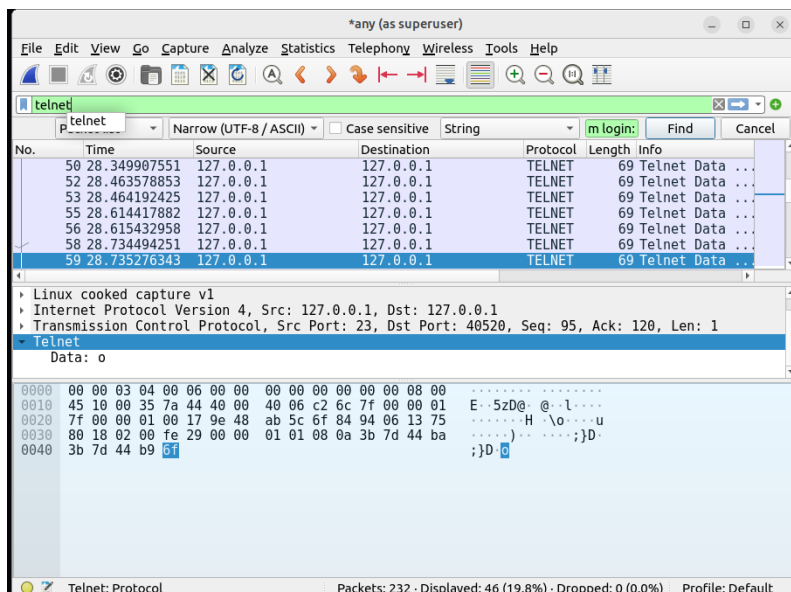
- j. In the **Packet Details** pane, click the arrow next to **Telnet** to expand its content. You should see that **labvm login:** is the data for this packet. The data for the packet is also shown in **Packet Bytes** pane. You can tell that the text was sent unencrypted because you can read it.
- k. In the **Packet List** pane, click the highlighted packet with **labvm login** as the data to select it.



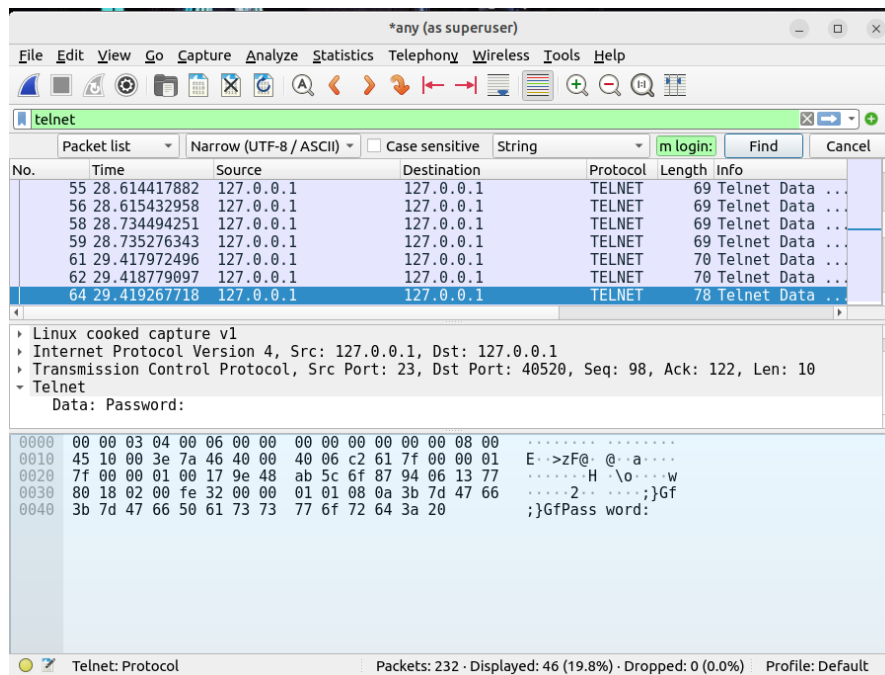
- l. To find the username and password, use your down arrow on the keyboard to select the next packet. In the **Packet Details** pane, you should see the value for **Data** under **Telnet** is the first letter you typed in the field for "labvm login:" prompt, which was **c** for **cisco**. If you click the down arrow again, you will see the next packet's data is also **c**. This is because the packet is listed twice: one time for source sending to destination and again for destination receiving the packet. Because the source and destination are the same interface (loopback 127.0.0.1), the packet is listed twice by Wireshark.



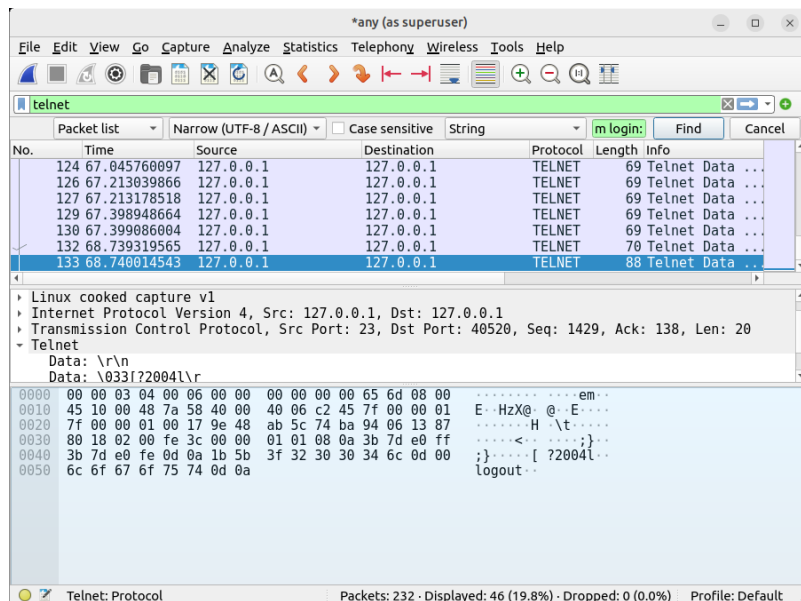
- m. Continue to press the down arrow key until you reach the last packet with a data value of **o** for the username **cisco**.



- n. Continue to click the down arrow until you will see **Password:** in the **Data** field. Continue pressing the down arrow to read the data of the next eight packets which reveal, one letter at a time, that **password** is the password for user **cisco**.



- o. If you continue to press the down arrow through the rest of the captured packets, you will see all the text sent and received during the Telnet session, including your **exit** command and the **logout** message.



Step 4: Capture and analyze encrypted SSH traffic.

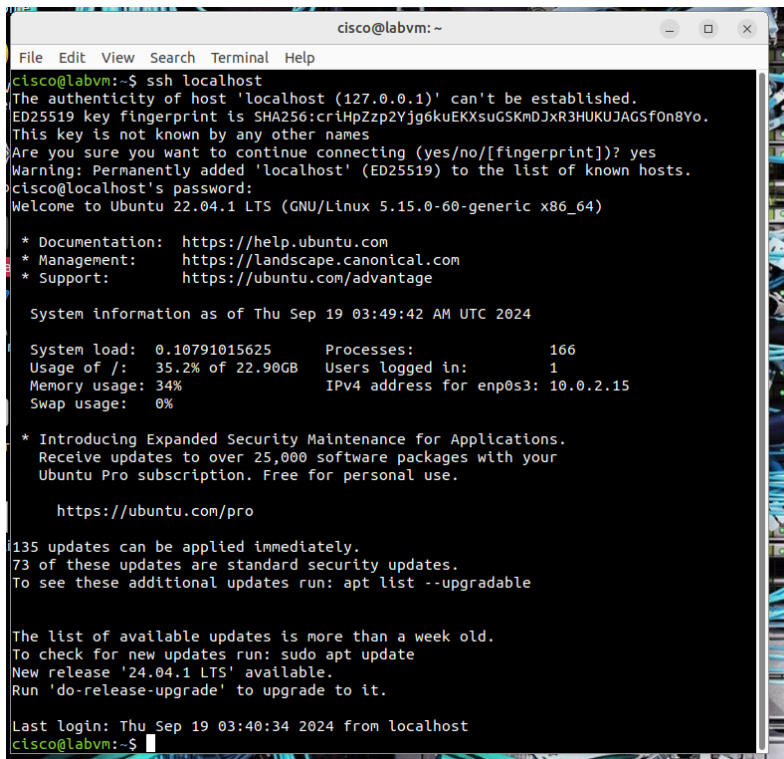
- Start a new capture. In the **Unsaved packets...** dialog box, click **Continue without Saving**. This will clear out the packets from your last capture and start a new capture.
- Return to your open terminal window or start a new terminal session.
- To simulate an SSH login, enter the command **ssh localhost**. If this is your first time to use the command, the system warns you about the authenticity of localhost and asks you if you want to continue. Enter **yes**, and then **password** as the password to log in.

```
cisco@labvm:~$ ssh localhost
The authenticity of host 'localhost (:::1)' can't be established.
ECDSA key fingerprint is SHA256:1EvtfM55v908I88uvZ4Em/UL4ARo8jWGE1hV8mVnDhQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
cisco@localhost's password: password
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

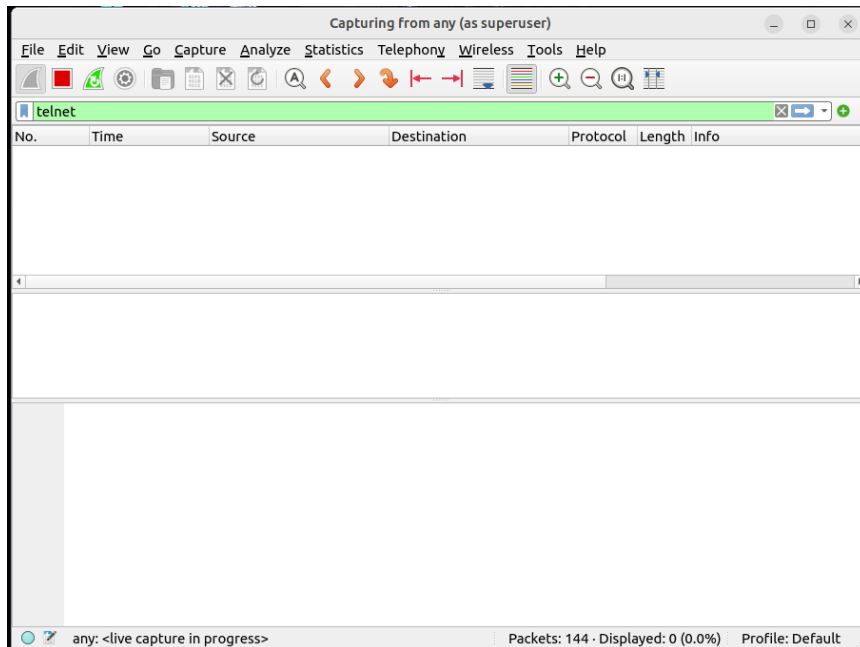
0 updates can be installed immediately.
0 of these updates are security updates.

Last login: Thu Mar 25 14:01:58 2021 from localhost
cisco@labvm:~$
```

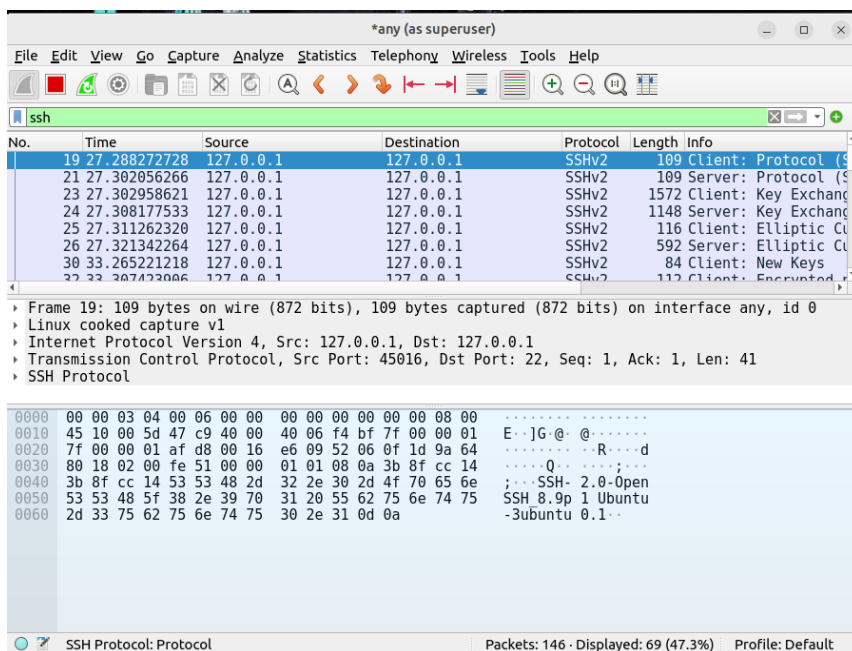


- d. Enter the **exit** command to end the SSH session.
- e. Return to Wireshark and stop the capture. If you left **telnet** as the search term in the **Apply a display filter** field, no packets will be listed. Change the search term from **telnet** to **ssh**. All the packets from your SSH session should now be shown in the **Packet List** pane.

- Telnet



- SSH



- f. In the **Packet Details** pane, expand the **SSH Protocol** fields to view the content. In the **Packet List** pane, click the first packet, and then use the down arrow to view a variety of the SSH packets. Notice that the **Data** for the **SSH Protocol** field shows that all the data is encrypted.

The image shows a Wireshark capture of SSH traffic. The top pane displays a list of packets, all of which are SSHv2 packets. The middle pane shows the details of the selected packet (SSH Version 2), indicating that the data is encrypted. The bottom pane shows the raw packet data in hexadecimal and ASCII, which is mostly illegible due to encryption.

Time	Source	Destination	Protocol	Length	Info
49.38.577244696	127.0.0.1	127.0.0.1	SSHv2	608	Server: Encrypted packet
50.38.579661721	127.0.0.1	127.0.0.1	SSHv2	176	Server: Encrypted packet
52.38.579976782	127.0.0.1	127.0.0.1	SSHv2	1216	Server: Encrypted packet
54.38.623052120	127.0.0.1	127.0.0.1	SSHv2	176	Server: Encrypted packet
56.43.741369031	127.0.0.1	127.0.0.1	SSHv2	136	Client: Encrypted packet
57.43.742676727	127.0.0.1	127.0.0.1	SSHv2	168	Server: Encrypted packet
59.43.766676663	127.0.0.1	127.0.0.1	SSHv2	136	Client: Encrypted packet

SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)
 Packet Length (encrypted): bcfaafee
 Encrypted Packet: 679842ce66493ad42c7c836db739ed4c68eab15d2a692779a971fa3567db8a532b9eee8...
 MAC: 843641ec60fff4af324f657ea633cb8e
 [Direction: client-to-server]

0040 3b 8f f8 27 bc fa af ee 67 98 42 ce 66 49 3a d4 ;... g·B·fI:·
 0050 2c 7c 83 6d b7 39 ed 4c 68 ea b1 5d 2a 69 27 79 ,|·m·9·L h·]·i'y
 0060 a9 71 fa 35 67 db 8a 53 2b 9e ee 8e eb 14 18 ce ·q·5g·S +·.....
 0070 2b d3 3b 71 ce 92 8f 7b 28 80 24 2f 8e 28 8e 11 +;q·{ (·\$/·(·
 0080 d6 da ac 2f 0b aa 92 ef c0 de b6 95 1a 4c b3 e4 ···/···· ····L·
 0090 9b ff 55 e5 ff 7a d6 46 84 8c 81 c7 50 7a 58 72 ··U·z·F ···PzXr
 00a0 bb 45 3c 4e 74 60 34 b9 c0 f6 d9 ce 4e b8 25 af ·E<Nt`4· ···N·%·
 00b0 8f 2b f8 c6 c8 8d 20 ed 8a 91 b5 94 82 fc 98 a0 +·.....
 00c0 4b 99 71 a0 4e de ec d4 07 e4 19 10 31 19 8f b8 K·q·N· ···1·
 00d0 b4 69 30 b8 6b 21 e5 82 b7 90 55 d9 92 76 5a cd ·i0·k!· ··U·vZ·
 00e0 85 02 c9 89 67 01 a3 6c d7 5e 9c 29 9f 18 9b 12 ···g·l ^·)·
 00f0 75 81 d9 02 32 d1 89 73 87 c8 9d 9f 95 02 c4 d6 u··2·s ···
 0100 c5 35 35 8a b7 52 39 76 60 9b aa 03 c7 6f 0f 57 ·55·R9v `···o·W

Encrypted Packet (ssh.encrypted_packet), 560 bytes Packets: 201 · Displayed: 69 (34.3%) Profile: Default