

Nama : Rizqi Hendra Ardiansyah
Kelas : SIB-4C
NIM : 2141762145
No.Absen : 11

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 whatâ€™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.

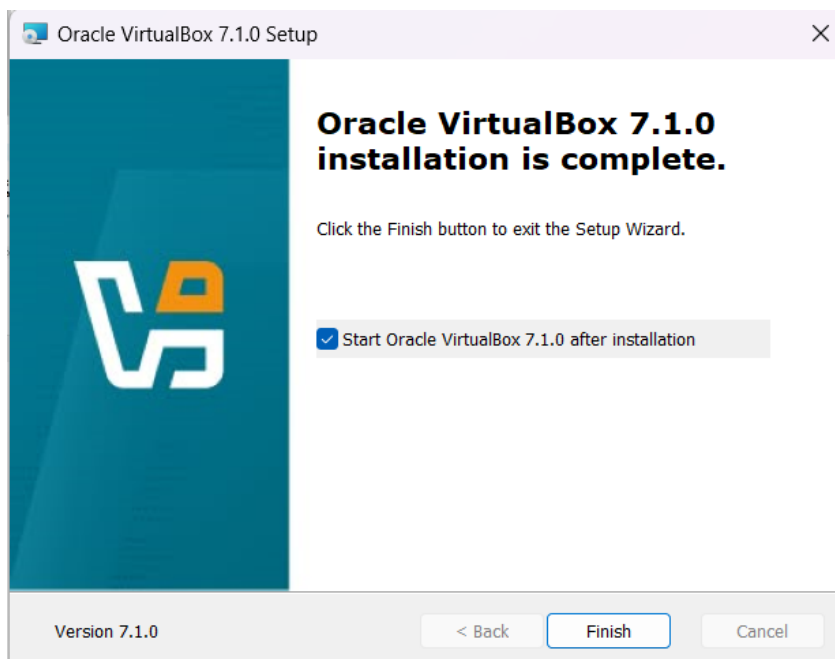
Required Resources

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

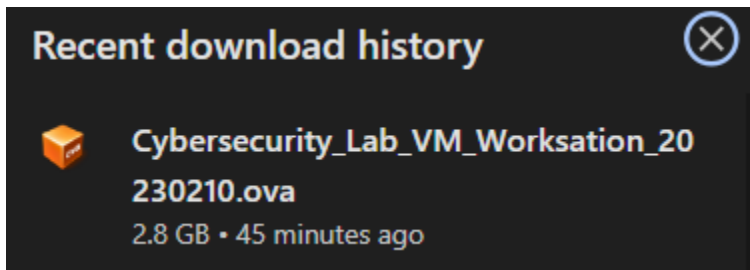
Instructions

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

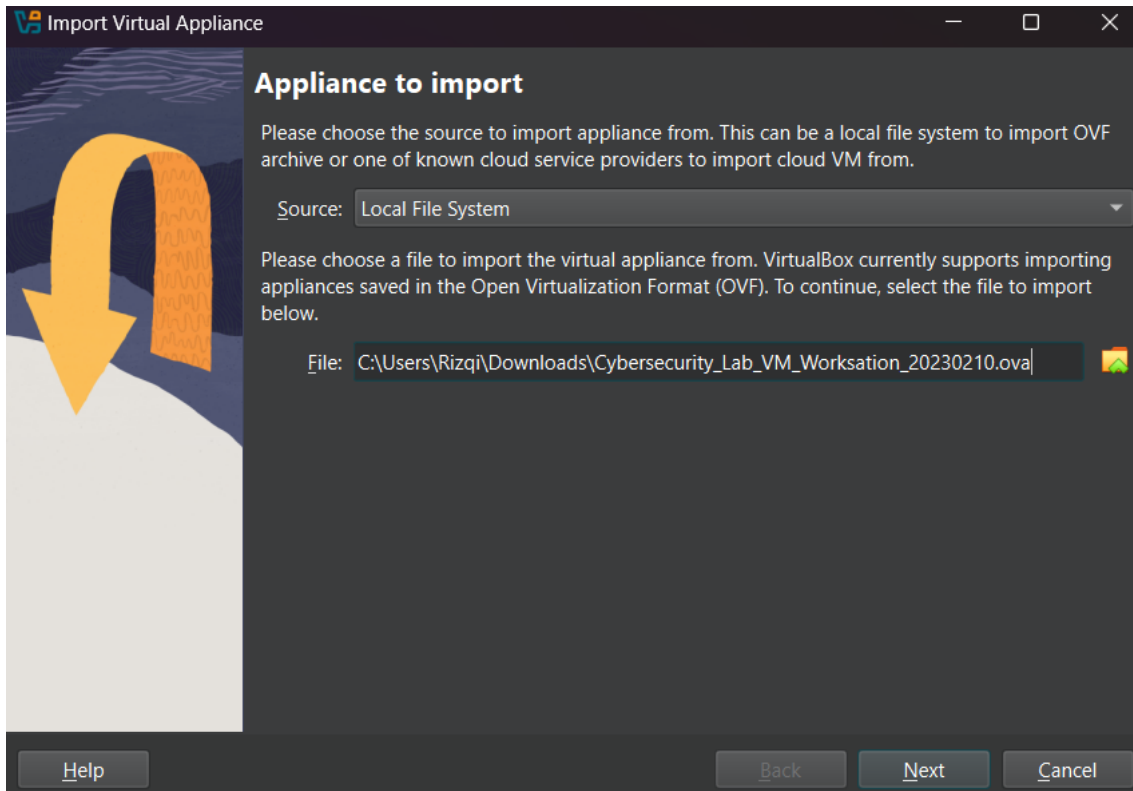
- a. Install VirtualBox



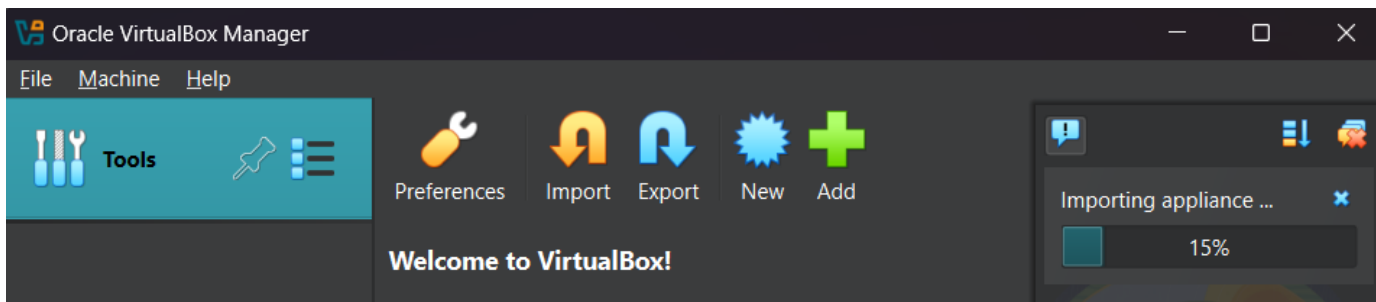
- b. Download CSE-LABVM



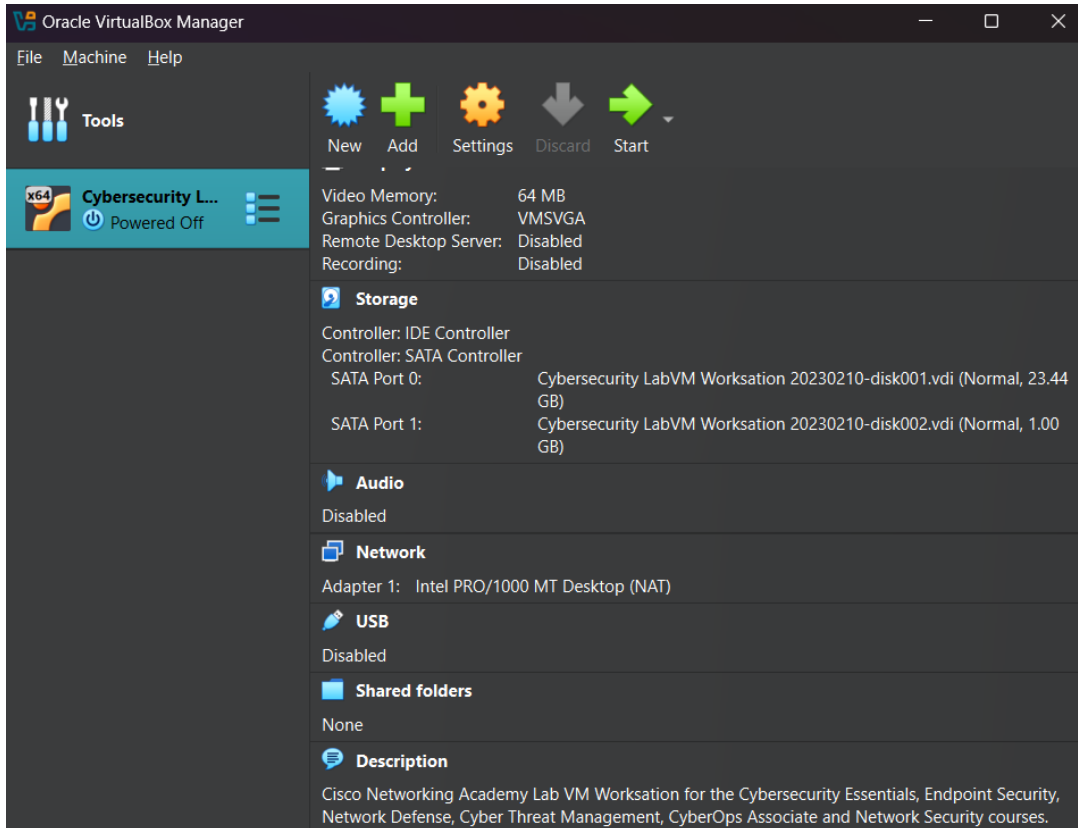
- c. Open VirtualBox that has been installed and select File > Import Appliance



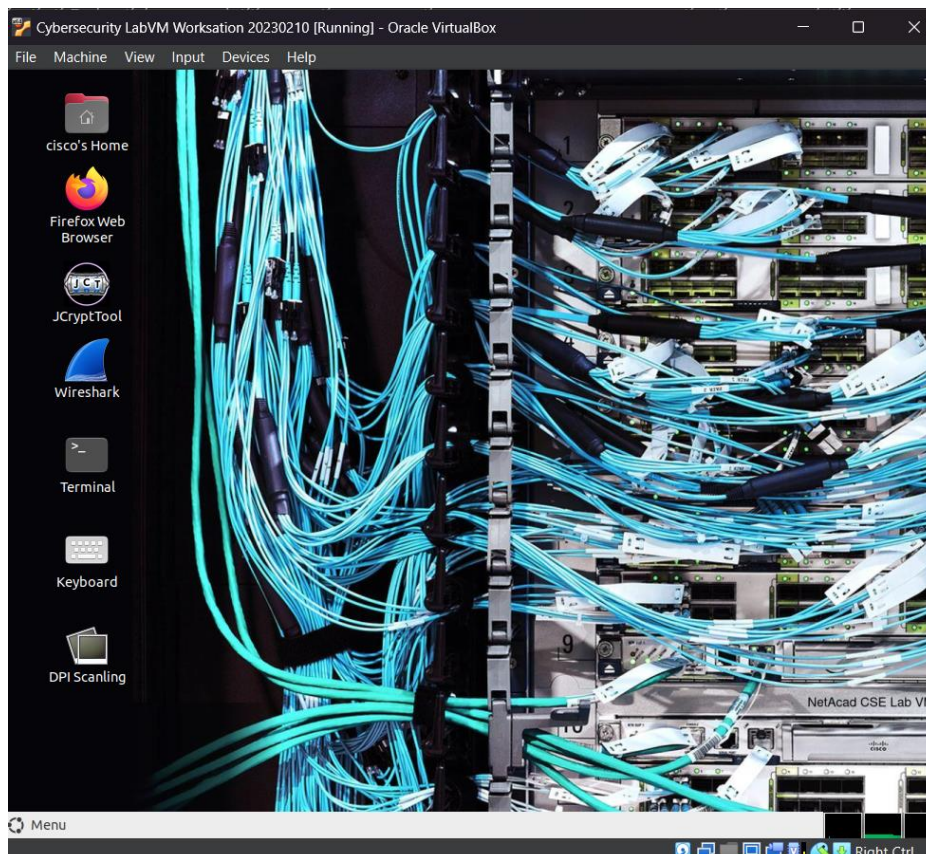
- d. Wait until it's finished



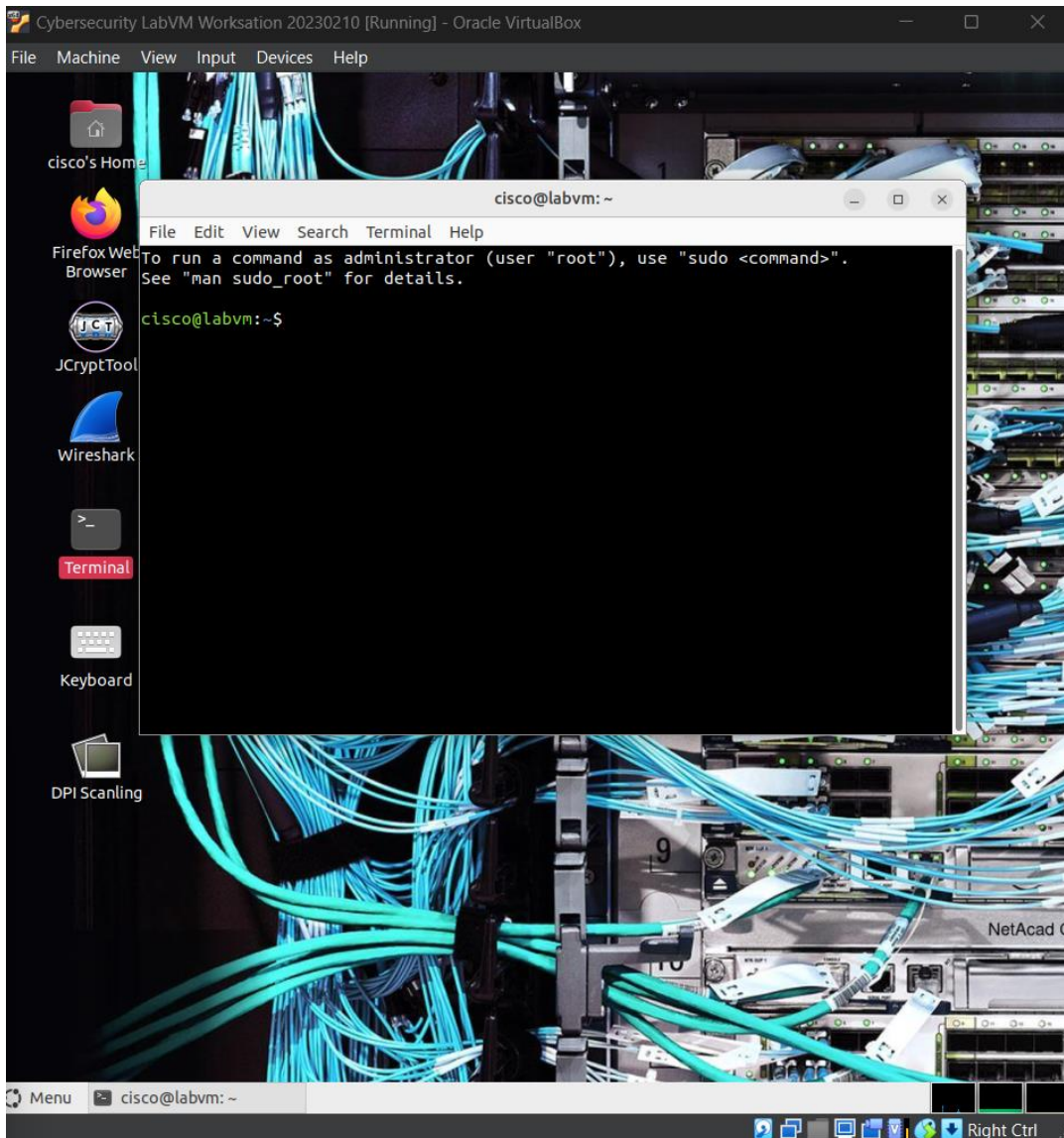
- e. LabVm has been installed



- f. Click start and wait for the running process to complete
- g. Launch the **CSE-LABVM**.

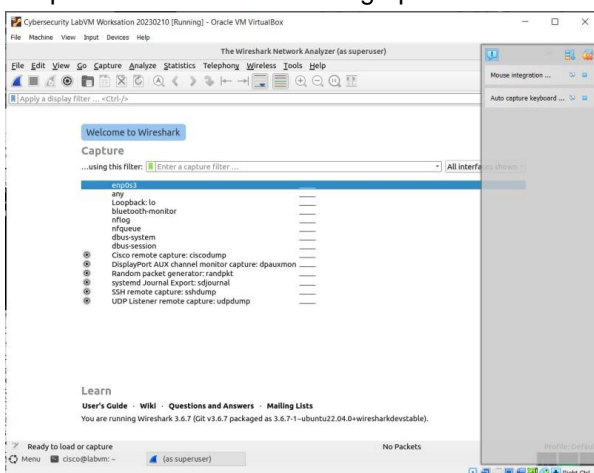


- h. Double-click the **Terminal** icon to open a terminal.



Step 2: Explore the Wireshark protocol analyzer.

- a. 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.



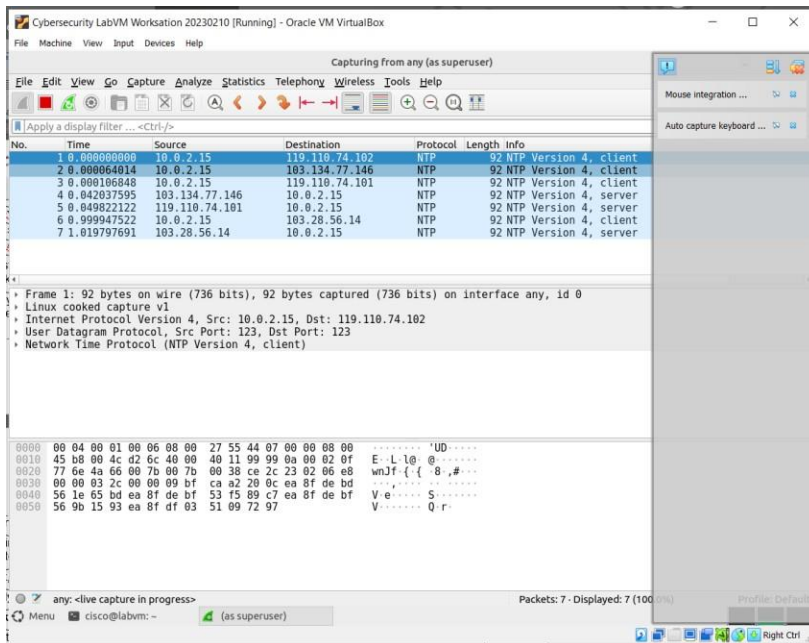
```
cisco@labvm:~$ sudo wireshark
```

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

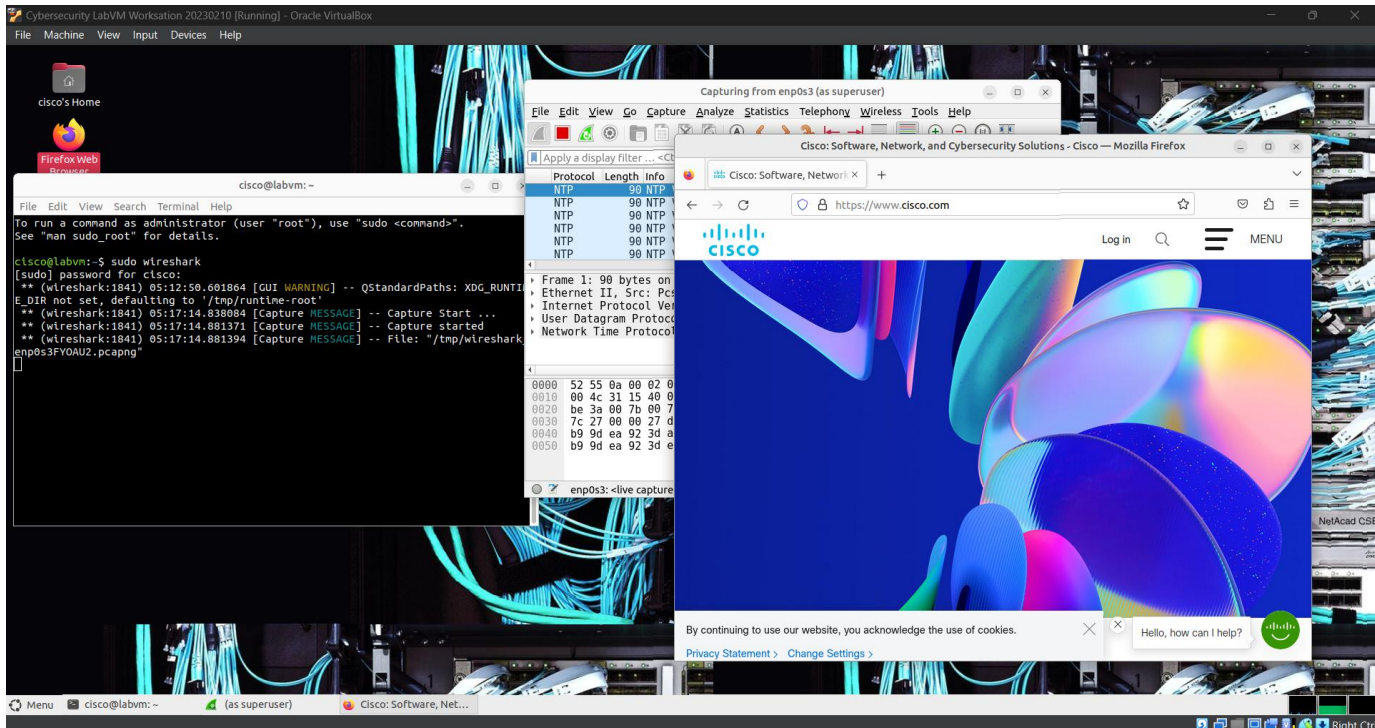
```
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

- 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.

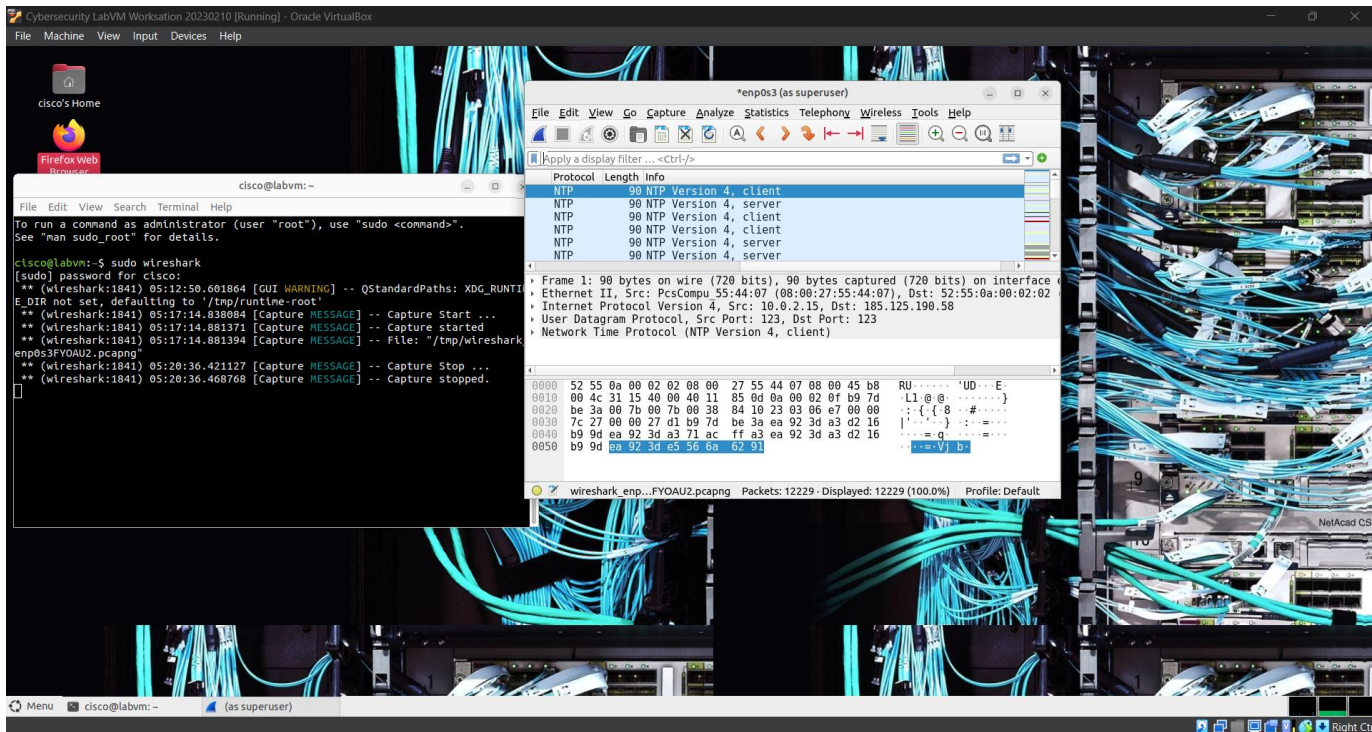
- c. If you already have Firefox open, you may see traffic captured in the Wireshark interface. If Firefox is not open, go ahead and open it now. In Wireshark, you should now see captured TCP traffic in the top third of the window.



- 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.



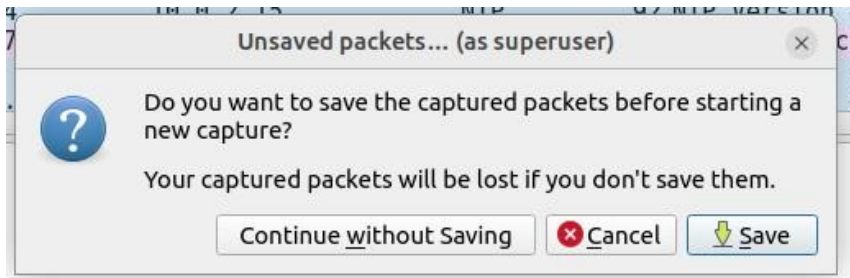
- The **Packet List** pane includes the following columns for each captured packet:
 - **No** - the number of the packet (in numerical order).
 - **Time** - the timestamp of the packet
 - **Source** - the source IP address of the packet
 - **Destination** - the destination IP address of the packet
 - **Protocol** - the protocol of the packet
 - **Length** - the number of bytes captured for this packet
 - **Info** - additional information about the packet's content

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	119.110.74.102	NTP	92	NTP Version 4, client
2	0.000064014	10.0.2.15	103.134.77.146	NTP	92	NTP Version 4, client
3	0.000106848	10.0.2.15	119.110.74.101	NTP	92	NTP Version 4, client
4	0.042037595	103.134.77.146	10.0.2.15	NTP	92	NTP Version 4, server
5	0.049022122	119.110.74.101	10.0.2.15	NTP	92	NTP Version 4, server
6	0.999947522	10.0.2.15	103.28.56.14	NTP	92	NTP Version 4, client
7	1.019797691	103.28.56.14	10.0.2.15	NTP	92	NTP Version 4, server
8	42.652892672	fe80::a00:27ff:fe55::ff02::2		ICMPv6	72	Router Solicitation from 08:00:27:55:44:07
9	60.047123894	10.0.2.15	103.169.192.229	NTP	92	NTP Version 4, client
10	60.068191931	103.169.192.229	10.0.2.15	NTP	92	NTP Version 4, server

- 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.

- a. 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.



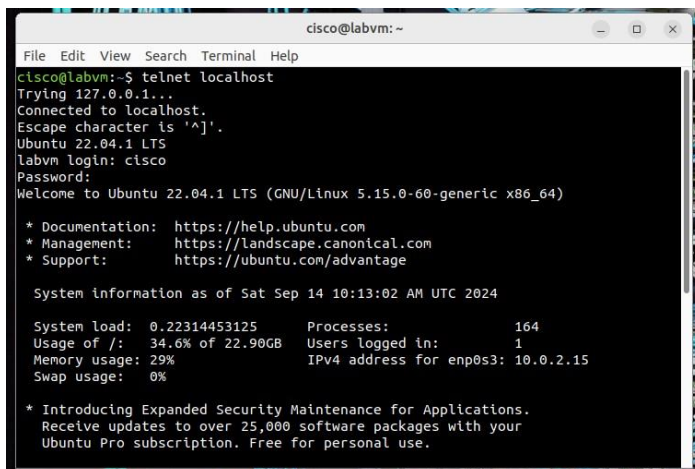
- b. Double-click the **Terminal** icon to open a new terminal window.
- c. You can simulate a remote login to your VM by entering the **telnet localhost** command, and then logging in as **cisco** with **password** as the password.

```
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
```

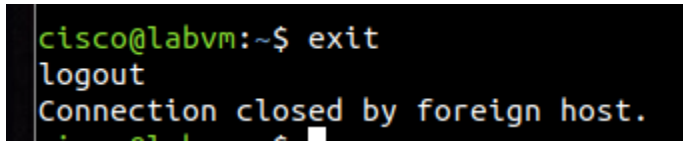
```
0 updates can be installed immediately.
0 of these updates are security updates.
```

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



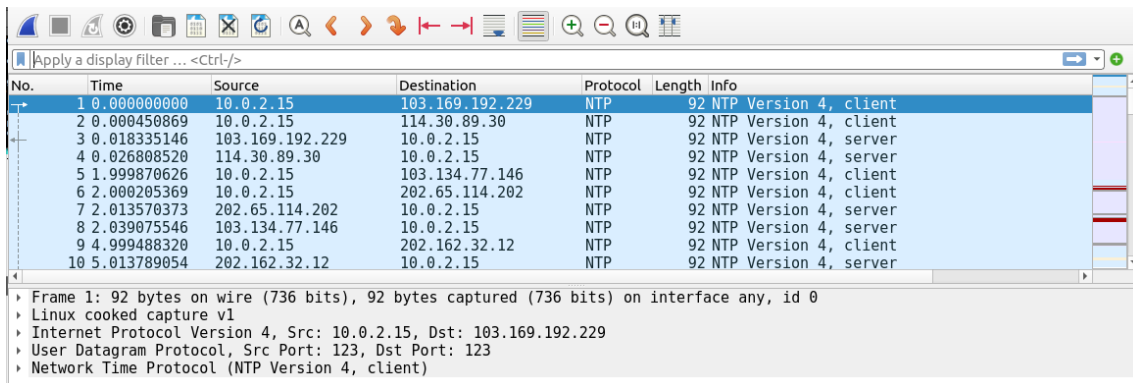
- d. Enter the **exit** command to end the Telnet session:

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

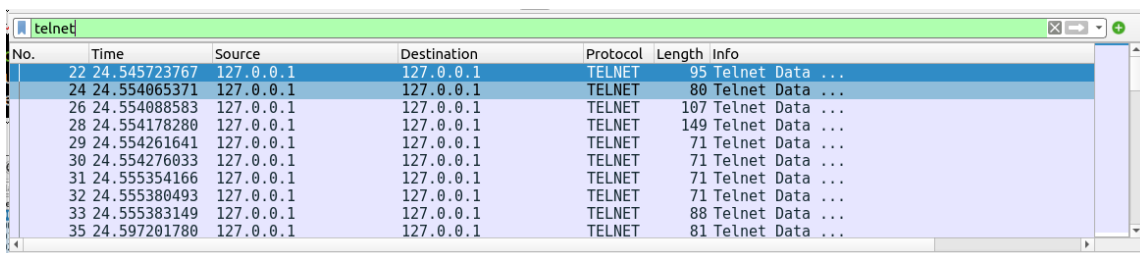


```
cisco@labvm:~$ exit
logout
Connection closed by foreign host.
```

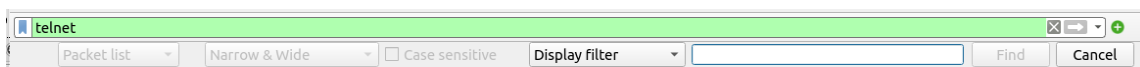
- f. Return to Wireshark and stop the capture.



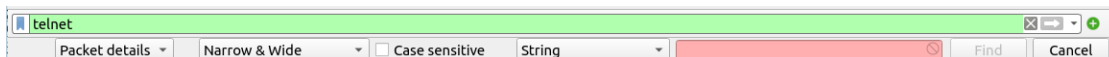
- g. In the **Apply a display filter** field, type **telnet** and press **Enter** to filter for only Telnet packets.



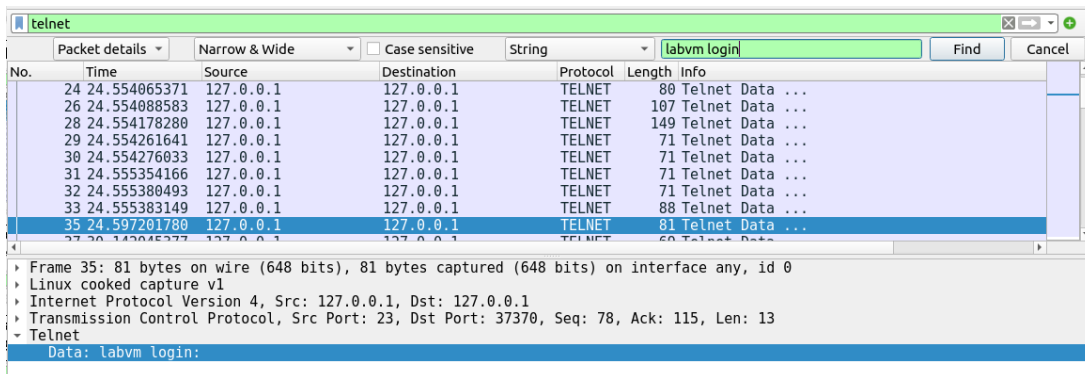
- h. On the toolbar, click the magnifying glass icon to **Find a packet**. Additional search features are now shown below the **Apply a display filter** field.



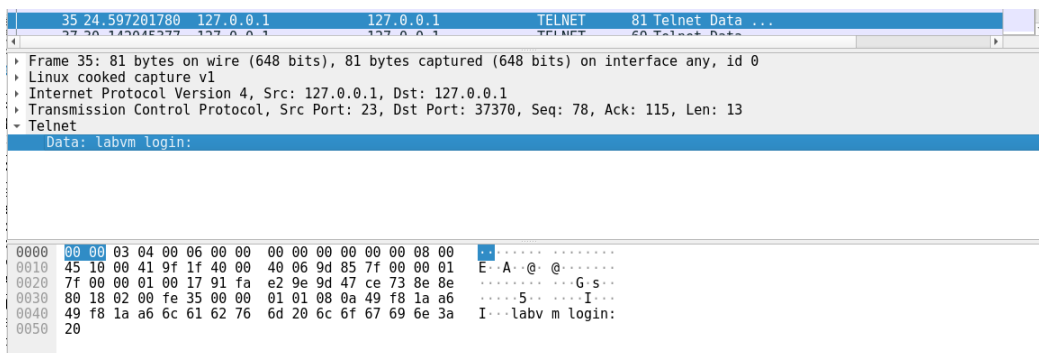
- i. Click the arrows next to **Display filter** and change it to **String**. Then click the arrows next to **Packet list** and change it to **Packet details**.



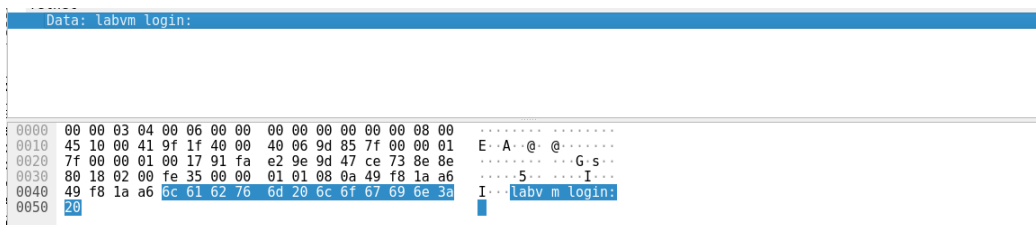
- j. To find the packet requesting login information, type **labvm login:** in the field next to **String**, and then press **Enter** or click **Find**. Wireshark will highlight the packet that contains the "labvm login:" text string.



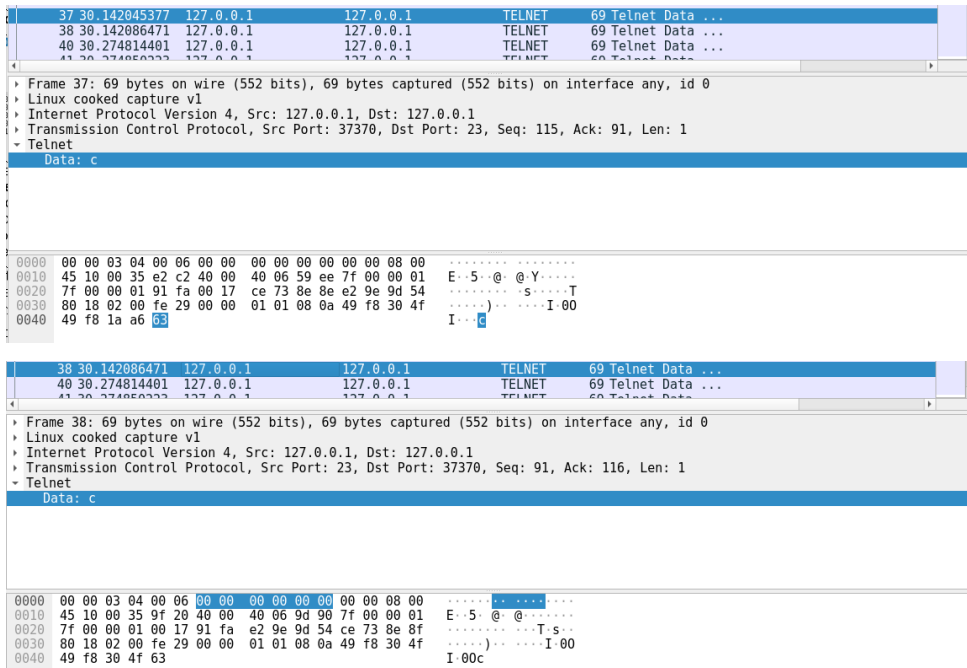
- k. In the **Packet Details** pane, click the arrow next to **Telnet** to expand its content. You should see that **labvm login:** is the data for this packet. The data for the packet is also shown in **Packet Bytes** pane. You can tell that the text was sent unencrypted because you can read it.



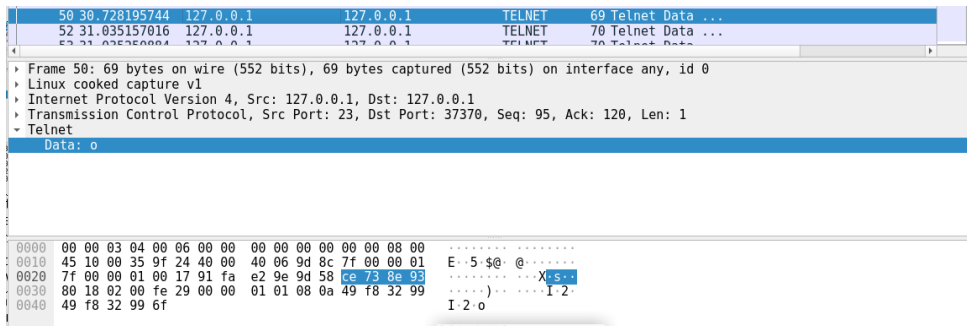
- l. In the **Packet List** pane, click the highlighted packet with **labvm login** as the data to select it.



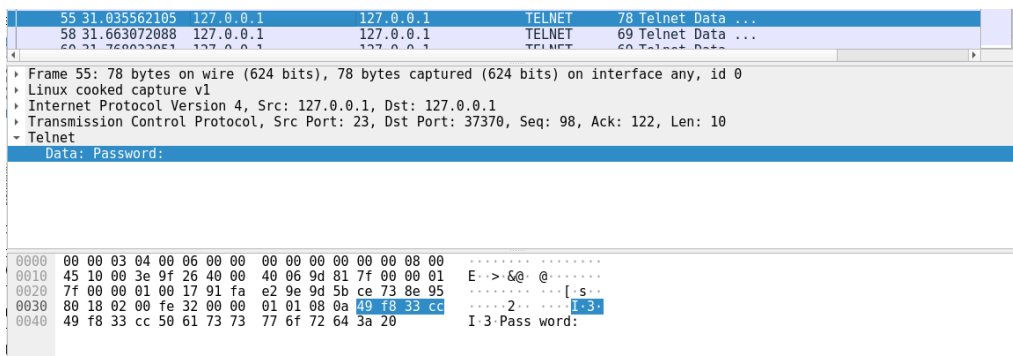
- m. To find the username and password, use your down arrow on the keyboard to select the next packet. In the **Packet Details** pane, you should see the value for **Data** under **Telnet** is the first letter you typed in the field for "labvm login:" prompt, which was **c** for **cisco**. If you click 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.



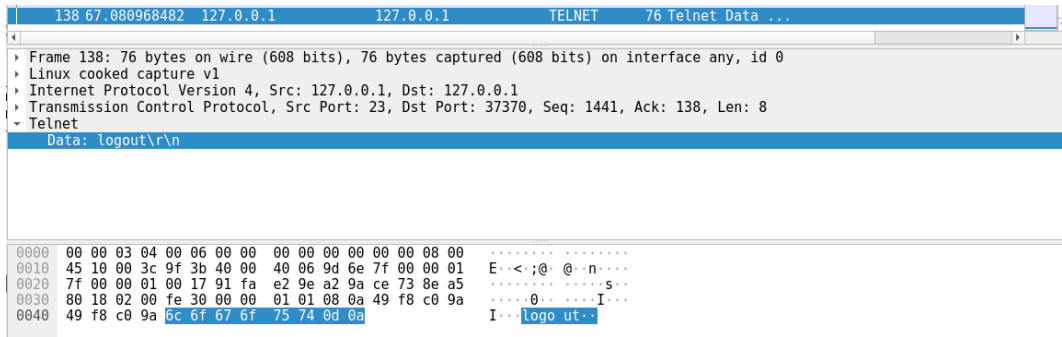
- n. Continue to press the down arrow key until you reach the last packet with a data value of **o** for the username **cisco**.



- o. 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**.

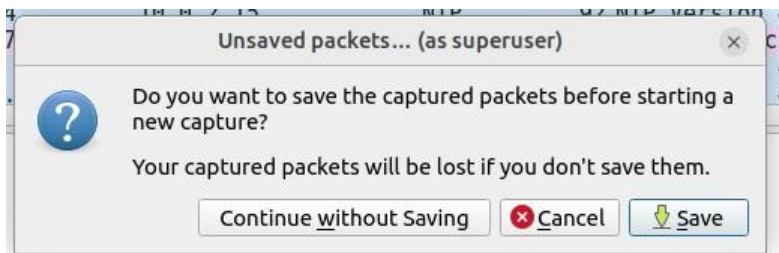


- p. If you continue to press the down arrow through the rest of the captured packets, you will see all the text sent and received during the Telnet session, including your **exit** command and the **logout** message.



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:lEvtfM55v9O8L88uvZ4Em/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:~$
```

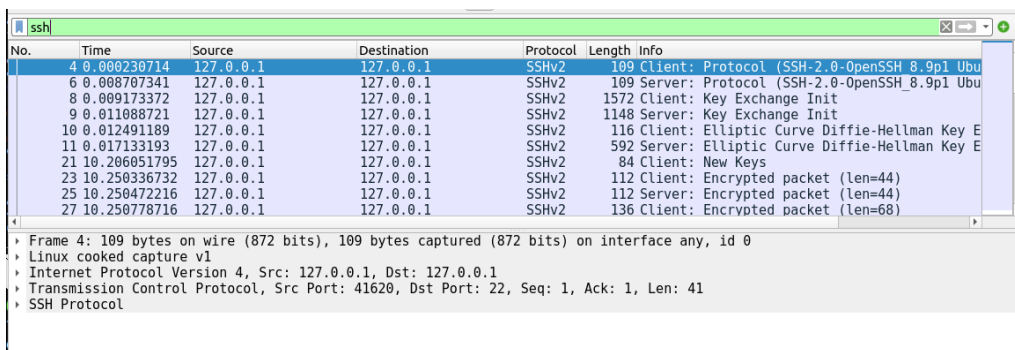


```
cisco@labvm: ~  
File Edit View Search Terminal Help  
cisco@labvm:~$ ssh localhost  
The authenticity of host 'localhost (127.0.0.1)' can't be established.  
ED25519 key fingerprint is SHA256:criHpZzp2Yjg6kuEKXsuGSKmDJxR3HUKUJAGSf0n8Yo.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.  
cisco@localhost's 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 Mon Sep 16 05:30:02 AM UTC 2024  
  
System load:          0.14794921875  
Usage of /:           35.0% of 22.90GB  
Memory usage:         22%  
Swap usage:           0%  
Processes:            159  
Users logged in:      1  
IPv4 address for enp0s3: 10.0.2.15  
IPv6 address for enp0s3: fd00::a00:27ff:fe55:4407
```

- c. Enter the **exit** command to end the SSH session.

```
cisco@labvm:~$ exit  
logout  
Connection to localhost closed.
```

- d. 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.



- e. 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.

ssh						
Filter details		Narrow & Wide		Case sensitive		String
						labvm login
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000230714	127.0.0.1	127.0.0.1	SSHv2	109	Client: Protocol (SSH-2.0-OpenSSH 8.9p1 Ubu
6	0.008707341	127.0.0.1	127.0.0.1	SSHv2	109	Server: Protocol (SSH-2.0-OpenSSH 8.9p1 Ubu
8	0.009173372	127.0.0.1	127.0.0.1	SSHv2	1572	Client: Key Exchange Init
9	0.011088721	127.0.0.1	127.0.0.1	SSHv2	1148	Server: Key Exchange Init
10	0.012491189	127.0.0.1	127.0.0.1	SSHv2	116	Client: Elliptic Curve Diffie-Hellman Key E
11	0.017133193	127.0.0.1	127.0.0.1	SSHv2	592	Server: Elliptic Curve Diffie-Hellman Key E
21	10.206051795	127.0.0.1	127.0.0.1	SSHv2	84	Client: New Keys
23	10.250336732	127.0.0.1	127.0.0.1	SSHv2	112	Client: Encrypted packet (len=44)
25	10.250472216	127.0.0.1	127.0.0.1	SSHv2	112	Server: Encrypted packet (len=44)
27	10.250730716	127.0.0.1	127.0.0.1	SSHv2	136	Client: Encrypted packet (len=60)
Frame 4: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface any, id 0 Linux cooked capture v1 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1 Transmission Control Protocol, Src Port: 41620, Dst Port: 22, Seq: 1, Ack: 1, Len: 41 SSH Protocol Protocol: SSH-2.0-OpenSSH 8.9p1 Ubuntu-3ubuntu0.1 [Direction: client-to-server]						
0000	00 00 03 04 00 06 00 00	00 00 00 00 00 08 00			
0010	45 10 00 5d 37 d9 40 00	40 06 04 b0 7f 00 00 01	E...]7@.@.....			
0020	7f 00 00 01 a2 94 00 16	ac 5b 71 18 16 81 16 94[q.....			
0030	80 18 02 00 fe 51 00 00	01 01 08 0a 4a 00 e7 ccQ...J....			
0040	4a 00 e7 cc 53 53 48 2d	32 2e 30 2d 4f 70 65 6e	J...SSH- 2.0-Open			
0050	53 53 48 5f 38 2e 39 70	31 20 55 62 75 6e 74 75	SSH 8.9p 1 Ubuntu			
0060	2d 33 75 62 75 6e 74 75	30 2e 31 0d 0a	-3ubuntu 0.1..			
76	50.191737444	127.0.0.1	127.0.0.1	SSHv2	104	Client: Encrypted packet (len=50)
73	50.191764271	127.0.0.1	127.0.0.1	SSHv2	128	Client: Encrypted packet (len=60)
Frame 73: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface any, id 0 Linux cooked capture v1 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1 Transmission Control Protocol, Src Port: 41620, Dst Port: 22, Seq: 3238, Ack: 4762, Len: 60 SSH Protocol SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none) Packet Length (encrypted): d20cdfcd Encrypted Packet: ed548f73e06b30d0c17a9a49084abcea951511f5da129cec9430ae4210ca8146807e61... MAC: 919429c5b5c00408fec78af869524a36 [Direction: client-to-server]						
0000	00 00 03 04 00 06 00 00	00 00 00 00 6c 6d 08 00lm..			
0010	45 10 00 70 37 f7 40 00	40 06 04 7f 7f 00 00 01	E..p7@.@.....			
0020	7f 00 00 01 a2 94 00 16	ac 5b 7d bd 16 81 29 2d[}....)-			
0030	80 18 02 00 fe 64 00 00	01 01 08 0a 4a 01 ab dcd...J....			
0040	4a 01 ab dc d2 0c df cd	ed 54 8f 73 e0 6b 30 0d	J.....T.s.k0..			
0050	0c e1 7a 9a 49 08 4a bc	ea 95 15 11 f5 da 12 9c	..z.I.J.....			
0060	ec 94 30 ae 42 10 ca 81	46 80 7e 61 9a 71 13 7c	..0.B...F~a.q.			
0070	91 94 29 c5 b5 c0 04 08	fe c7 8a f8 69 52 4a 36	..).1RJ6			