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.

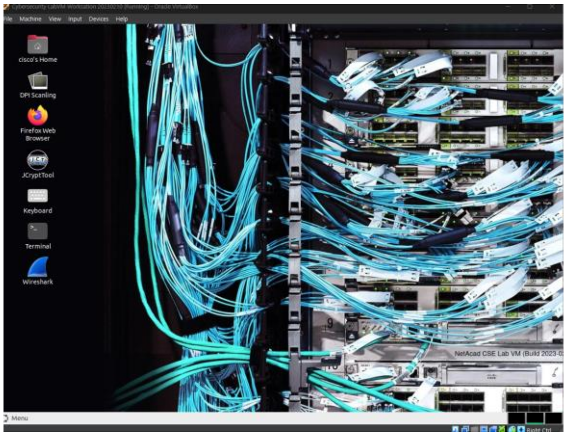
Required Resources

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

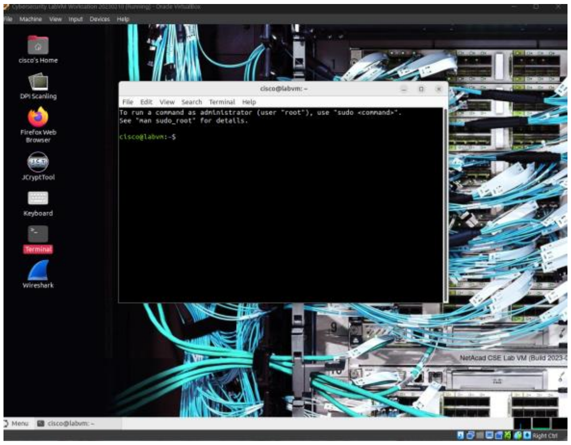
Instructions

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

a. Launch the **CSE-LABVM**.



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

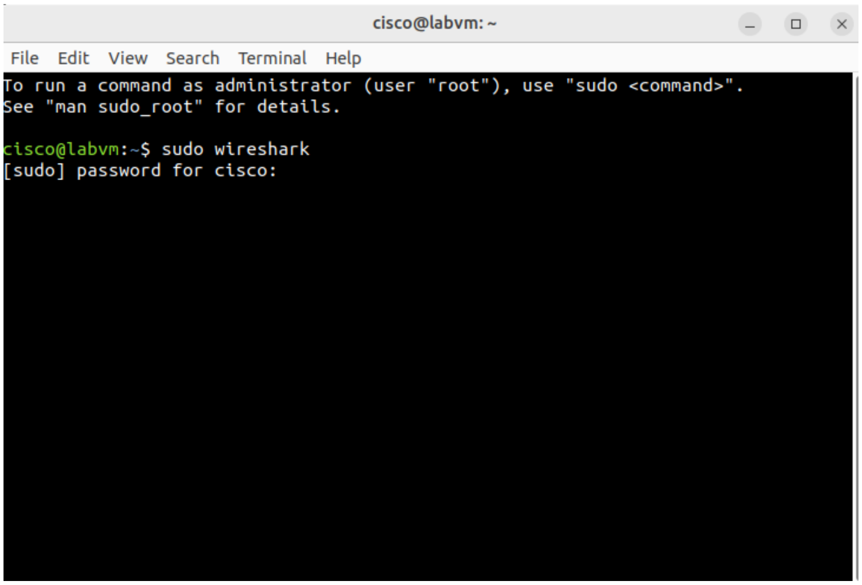


```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

cisco@labvm:~$
```

Step 2: Explore the Wireshark protocol analyzer.

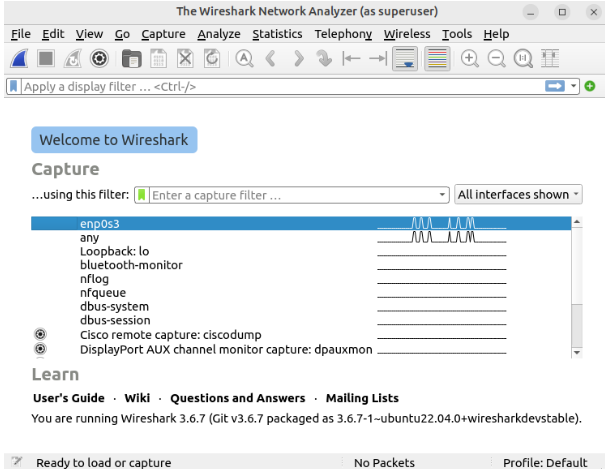
a. To capture traffic on your VM, you need to run Wireshark in promiscuous mode, which requires running with escalated privileges using **sudo**. Enter the **sudo wireshark** command, and then enter **password** for the password. The Wireshark graphical user interface (GUI) will open up.

```
cisco@labvm:~$ sudo wireshark
[sudo] password for cisco: password
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

cisco@labvm:~$ sudo wireshark
[sudo] password for cisco:
```

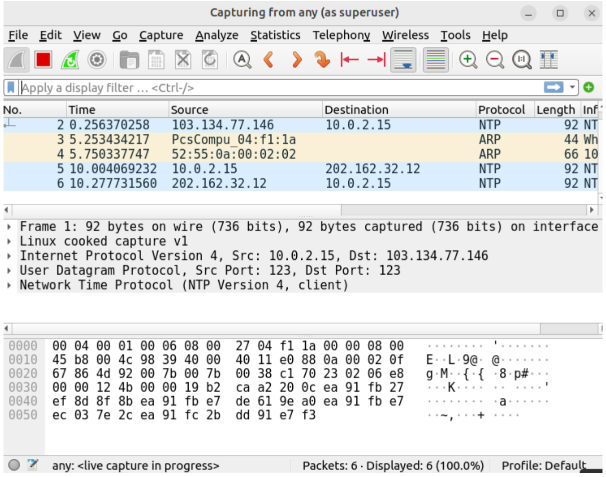
c. Under the listing of interfaces, select **any**, and then click **Capture** > **Start** from the menus. Alternatively, you can click the shark fin icon. Wireshark will begin capturing packets.


The Wireshark Network Analyzer (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

```
enp0s3
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
```

You are running Wireshark 3.6.7 (Git v3.6.7 packaged as 3.6.7-1~ubuntu22.04.0+wiresharkdevstable).

Ready to load or capture   No Packets   Profile: Default


Capturing from any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

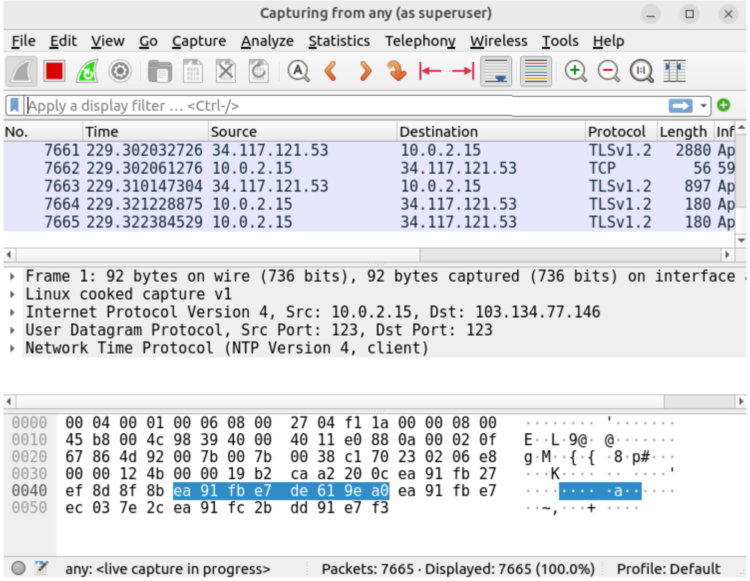
```
No.   Time          Source              Destination     Protocol  Length Inf
    2 0.256370258   103.134.77.146      10.0.2.15       NTP           92 NT
    3 5.253434217   PcsCompu_04:f1:1a                   ARP           44 Wh
    4 5.750337747   52:55:0a:00:02:02                   ARP           66 10
    5 10.004069232  10.0.2.15           202.162.32.12   NTP           92 NT
    6 10.277731560  202.162.32.12       10.0.2.15       NTP           92 NT
```

```
› Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 103.134.77.146
› User Datagram Protocol, Src Port: 123, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)
```

```
0000  00 04 00 01 00 06 08 00  27 04 f1 1a 00 00 08 00   ········ '·······
0010  45 b8 00 4c 98 39 40 00  40 11 e0 88 0a 00 02 0f   E··L·9@· @·······
0020  67 86 4d 92 00 7b 00 7b  00 38 c1 70 23 02 06 e8   g·M··{·{ ·8·p#···
0030  00 00 12 4b 00 00 19 b2  ca a2 20 0c ea 91 fb 27   ···K···· ·· ····'
0040  ef 8d 8f 8b ea 91 fb e7  de 61 9e a0 ea 91 fb e7   ········ ·a······
0050  ec 03 7e 2c ea 91 fc 2b  dd 91 e7 f3               ··~,···+ ····
```

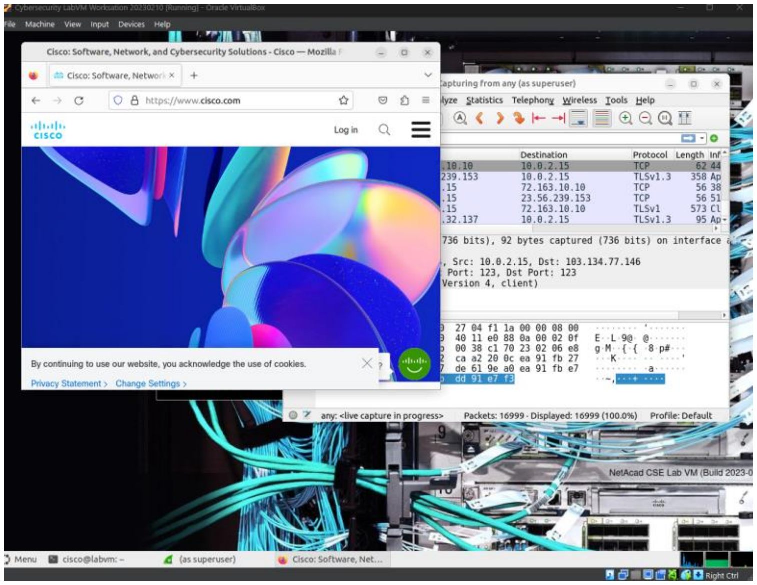
any: <live capture in progress>   Packets: 6 · Displayed: 6 (100.0%)   Profile: Default

d. 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.


Capturing from any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time            Source          Destination     Protocol  Length Inf
 7661 229.302032726  34.117.121.53   10.0.2.15       TLSv1.2    2880 Ap
 7662 229.302061276  10.0.2.15       34.117.121.53   TCP          56 59
 7663 229.310147304  34.117.121.53   10.0.2.15       TLSv1.2     897 Ap
 7664 229.321228875  10.0.2.15       34.117.121.53   TLSv1.2     180 Ap
 7665 229.322384529  10.0.2.15       34.117.121.53   TLSv1.2     180 Ap

› Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 103.134.77.146
› User Datagram Protocol, Src Port: 123, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)

0000  00 04 00 01 00 06 08 00  27 04 f1 1a 00 00 08 00   ········ '·······
0010  45 b8 00 4c 98 39 40 00  40 11 e0 88 0a 00 02 0f   E··L·9@· @·······
0020  67 86 4d 92 00 7b 00 7b  00 38 c1 70 23 02 06 e8   g·M··{·{ ·8·p#···
0030  00 00 12 4b 00 00 19 b2  ca a2 20 0c ea 91 fb 27   ···K···· ·· ····'
0040  ef 8d 8f 8b ea 91 fb e7  de 61 9e a0 ea 91 fb e7   ········ ·a······
0050  ec 03 7e 2c ea 91 fc 2b  dd 91 e7 f3               ··~,···+ ····

any: <live capture in progress>    Packets: 7665 · Displayed: 7665 (100.0%)    Profile: Default
```

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

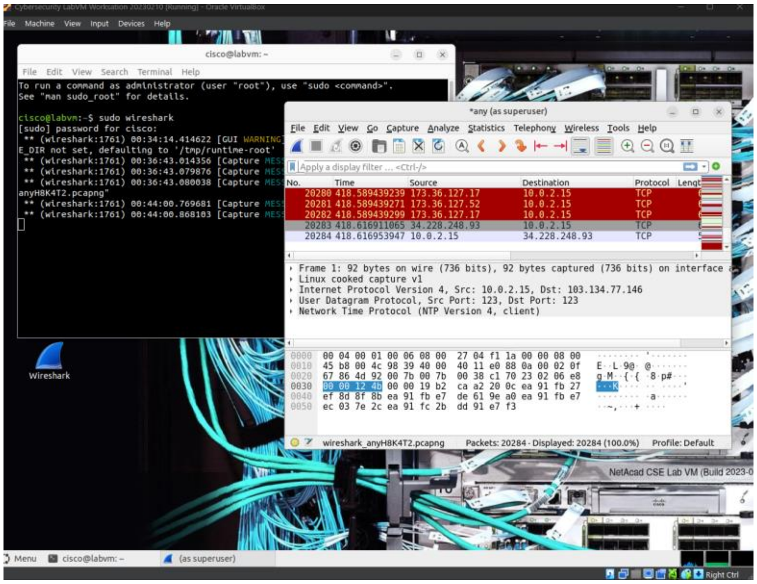

File Machine View Input Devices Help
Cisco: Software, Network, and Cybersecurity Solutions - Cisco — Mozilla F
Cisco: Software, Network
https://www.cisco.com
cisco
Log in
Capturing from any (as superuser)
lyze Statistics Telephony Wireless Tools Help
NetAcad CSE Lab VM (Build 2023-0
Menu
cisco@labvm: ~
(as superuser)
Cisco: Software, Net...
Right Ctrl

By continuing to use our website, you acknowledge the use of cookies.

Privacy Statement › Change Settings ›

```
        Destination     Protocol  Length Inf
.10.10  10.0.2.15       TCP          62 44
239.153 10.0.2.15       TLSv1.3     358 Ap
.15     72.163.10.10    TCP          56 38
.15     23.56.239.153   TCP          56 51
.15     72.163.10.10    TLSv1       573 Cl
.32.137 10.0.2.15       TLSv1.3      95 Ap

736 bits), 92 bytes captured (736 bits) on interface
, Src: 10.0.2.15, Dst: 103.134.77.146
 Port: 123, Dst Port: 123
Version 4, client)

 27 04 f1 1a 00 00 08 00   ········ '·······
 40 11 e0 88 0a 00 02 0f   E··L·9@· @·······
 00 38 c1 70 23 02 06 e8   g·M··{·{ ·8·p#···
 ca a2 20 0c ea 91 fb 27   ···K···· ·· ····'
 de 61 9e a0 ea 91 fb e7   ········ ·a······
 dd 91 e7 f3               ··~,···+ ····

any: <live capture in progress>    Packets: 16999 · Displayed: 16999 (100.0%)    Profile: Default
```

e. Return to Wireshark and click **Capture** > **Stop** from the menus. Alternatively, you can click the red square button next to the shark fin.


Cybersecurity LabVM Workstation 20230210 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
cisco@labvm: ~
File Edit View Search Terminal Help
*any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark
NetAcad CSE Lab VM (Build 2023-0
Menu
cisco@labvm: ~
(as superuser)
Right Ctrl

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

cisco@labvm:~$ sudo wireshark
[sudo] password for cisco:
 ** (wireshark:1761) 00:34:14.414622 [GUI WARNING]
E_DIR not set, defaulting to '/tmp/runtime-root'
 ** (wireshark:1761) 00:36:43.014356 [Capture MES
 ** (wireshark:1761) 00:36:43.079876 [Capture MES
 ** (wireshark:1761) 00:36:43.080038 [Capture MES
anyH8K4T2.pcapng"
 ** (wireshark:1761) 00:44:00.769681 [Capture MES
 ** (wireshark:1761) 00:44:00.868103 [Capture MES
```

```
No.    Time          Source          Destination     Protocol  Lengt
 20280 418.589439239 173.36.127.17   10.0.2.15       TCP
 20281 418.589439271 173.36.127.52   10.0.2.15       TCP
 20282 418.589439299 173.36.127.17   10.0.2.15       TCP
 20283 418.616911065 34.228.248.93   10.0.2.15       TCP
 20284 418.616953947 10.0.2.15       34.228.248.93   TCP

› Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 103.134.77.146
› User Datagram Protocol, Src Port: 123, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)

0000  00 04 00 01 00 06 08 00  27 04 f1 1a 00 00 08 00   ········'·······
0010  45 b8 00 4c 98 39 40 00  40 11 e0 88 0a 00 02 0f   E··L·9@·@·······
0020  67 86 4d 92 00 7b 00 7b  00 38 c1 70 23 02 06 e8   g·M··{·{·8·p#···
0030  00 00 12 4b 00 00 19 b2  ca a2 20 0c ea 91 fb 27   ···K···········'
0040  ef 8d 8f 8b ea 91 fb e7  de 61 9e a0 ea 91 fb e7   ·········a······
0050  ec 03 7e 2c ea 91 fc 2b  dd 91 e7 f3               ··~,···+····

wireshark_anyH8K4T2.pcapng    Packets: 20284 · Displayed: 20284 (100.0%)    Profile: Default
```

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.

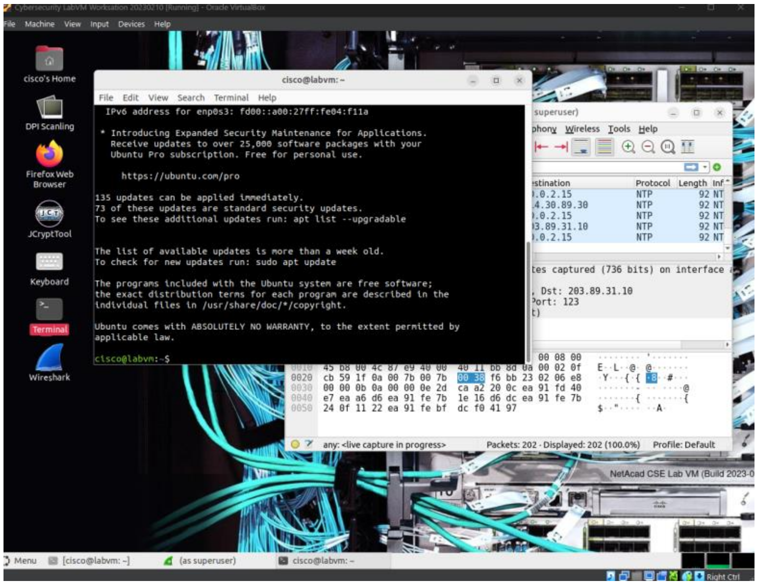
a. Start a new capture. In the **Unsaved packets…** dialog box, click **Continue without Saving**. This will clear out the packets from your last capture and start a new capture.

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:~$
```

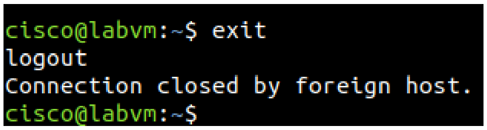

Cybersecurity LabVM Workstation 20230210 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
cisco's Home
DPI Scanling
Firefox Web Browser
JCryptTool
Keyboard
Terminal
Wireshark
cisco@labvm: ~
File Edit View Search Terminal Help
superuser)
phony Wireless Tools Help
NetAcad CSE Lab VM (Build 2023-0
Menu
[cisco@labvm: ~]
(as superuser)
cisco@labvm: ~
Right Ctrl

```
 IPv6 address for enp0s3: fd00::a00:27ff:fe04:f11a

 * 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


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

cisco@labvm:~$
```

```
estination     Protocol Length Inf
).0.2.15       NTP         92 NT
.4.30.89.30    NTP         92 NT
).0.2.15       NTP         92 NT
)3.89.31.10    NTP         92 NT
).0.2.15       NTP         92 NT

tes captured (736 bits) on interface a

, Dst: 203.89.31.10
Port: 123
t)

                                     00 08 00
0010  45 b8 00 4c 87 e9 40 00  40 11 bb 8d 0a 00 02 0f   E··L··@· @·······
0020  cb 59 1f 0a 00 7b 00 7b  00 38 f6 bb 23 02 06 e8   ·Y···{·{ ·8··#···
0030  00 00 0b 0a 00 00 0e 2d  ca a2 20 0c ea 91 fd 40   ·······- ·······@
0040  e7 ea a6 d6 ea 91 fe 7b  1e 16 d6 dc ea 91 fe 7b   ·······{ ·······{
0050  24 0f 11 22 ea 91 fe bf  dc f0 41 97               $··"···· ··A·

any: <live capture in progress>    Packets: 202 · Displayed: 202 (100.0%)    Profile: Default
```

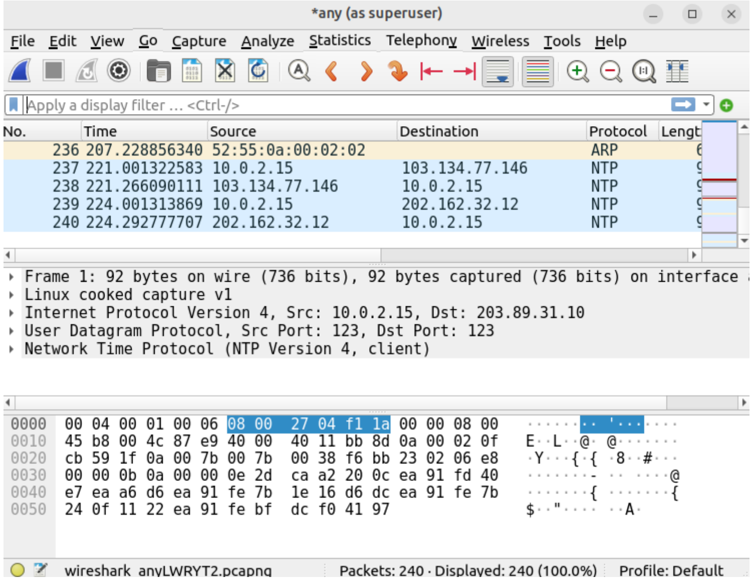
d. Enter the **exit** command to end the Telnet session:

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



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

f. Return to Wireshark and stop the capture.


*any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

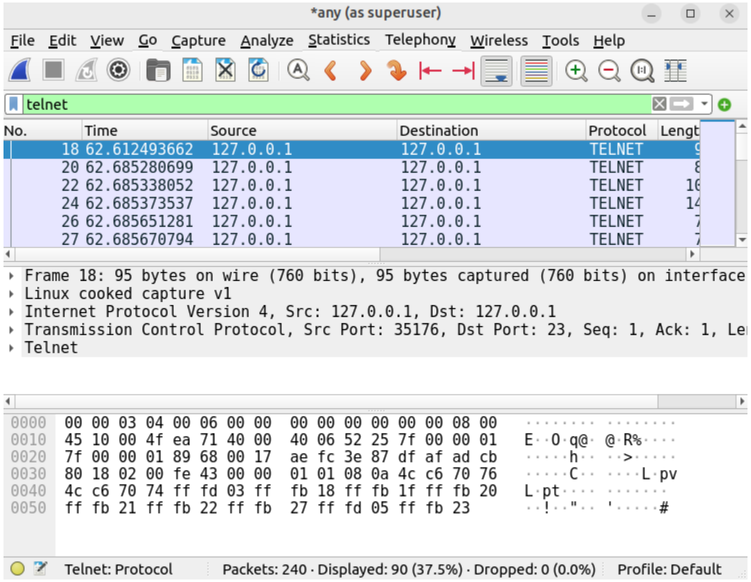
```
No.   Time          Source              Destination       Protocol  Lengt
  236 207.228856340 52:55:0a:00:02:02                     ARP       6
  237 221.001322583 10.0.2.15           103.134.77.146    NTP       9
  238 221.266090111 103.134.77.146      10.0.2.15         NTP       9
  239 224.001313869 10.0.2.15           202.162.32.12     NTP       9
  240 224.292777707 202.162.32.12       10.0.2.15         NTP       9
```

```
› Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 203.89.31.10
› User Datagram Protocol, Src Port: 123, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)
```

```
0000  00 04 00 01 00 06 08 00  27 04 f1 1a 00 00 08 00   ······· '·······
0010  45 b8 00 4c 87 e9 40 00  40 11 bb 8d 0a 00 02 0f   E··L··@· @·······
0020  cb 59 1f 0a 00 7b 00 7b  00 38 f6 bb 23 02 06 e8   ·Y···{·{ ·8··#···
0030  00 00 0b 0a 00 00 0e 2d  ca a2 20 0c ea 91 fd 40   ·······- ·· ····@
0040  e7 ea a6 d6 ea 91 fe 7b  1e 16 d6 dc ea 91 fe 7b   ·······{ ·······{
0050  24 0f 11 22 ea 91 fe bf  dc f0 41 97               $··"···· ··A·
```

```
wireshark_anyLWRYT2.pcapng     Packets: 240 · Displayed: 240 (100.0%)     Profile: Default
```

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


*any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
telnet
```

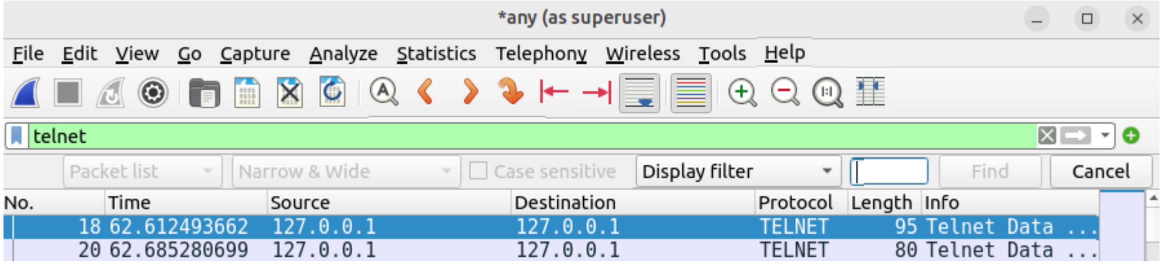
```
No.   Time          Source       Destination   Protocol  Lengt
   18 62.612493662  127.0.0.1    127.0.0.1     TELNET    9
   20 62.685280699  127.0.0.1    127.0.0.1     TELNET    8
   22 62.685338052  127.0.0.1    127.0.0.1     TELNET    10
   24 62.685373537  127.0.0.1    127.0.0.1     TELNET    14
   26 62.685651281  127.0.0.1    127.0.0.1     TELNET    7
   27 62.685670794  127.0.0.1    127.0.0.1     TELNET    7
```

```
› Frame 18: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 35176, Dst Port: 23, Seq: 1, Ack: 1, Le
› Telnet
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 10 00 4f ea 71 40 00  40 06 52 25 7f 00 00 01   E··O·q@· @·R%····
0020  7f 00 00 01 89 68 00 17  ae fc 3e 87 df af ad cb   ·····h·· ··>·····
0030  80 18 02 00 fe 43 00 00  01 01 08 0a 4c c6 70 76   ·····C·· ····L·pv
0040  4c c6 70 74 ff fd 03 ff  fb 18 ff fb 1f ff fb 20   L·pt···· ·······
0050  ff fb 21 ff fb 22 ff fb  27 ff fd 05 ff fb 23      ··!··"·· '·····#
```

```
Telnet: Protocol     Packets: 240 · Displayed: 90 (37.5%) · Dropped: 0 (0.0%)     Profile: Default
```

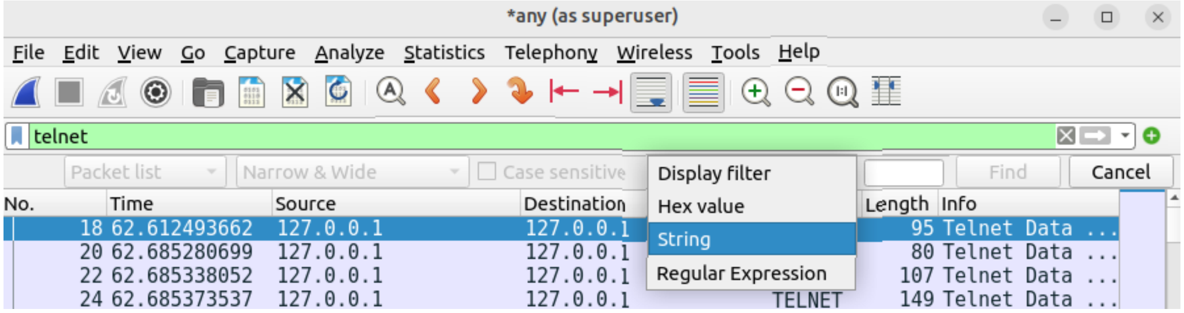
h. On the toolbar, click the magnifying glass icon to **Find a packet**. Additional search features are now shown below the **Apply a display filter** field.


*any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
telnet
Packet list ▾   Narrow & Wide ▾   □ Case sensitive   Display filter ▾   [ ]   Find   Cancel
```

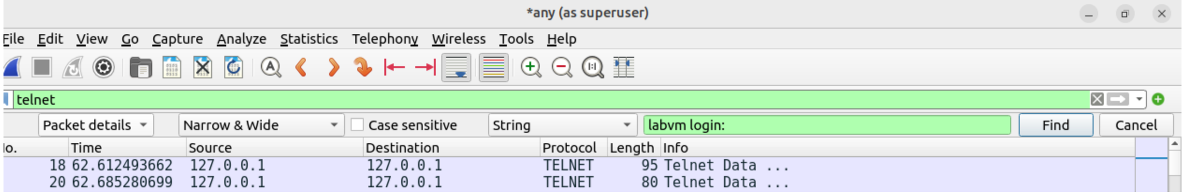
```
No.   Time          Source       Destination   Protocol  Length Info
   18 62.612493662  127.0.0.1    127.0.0.1     TELNET        95 Telnet Data ...
   20 62.685280699  127.0.0.1    127.0.0.1     TELNET        80 Telnet Data ...
```

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**.



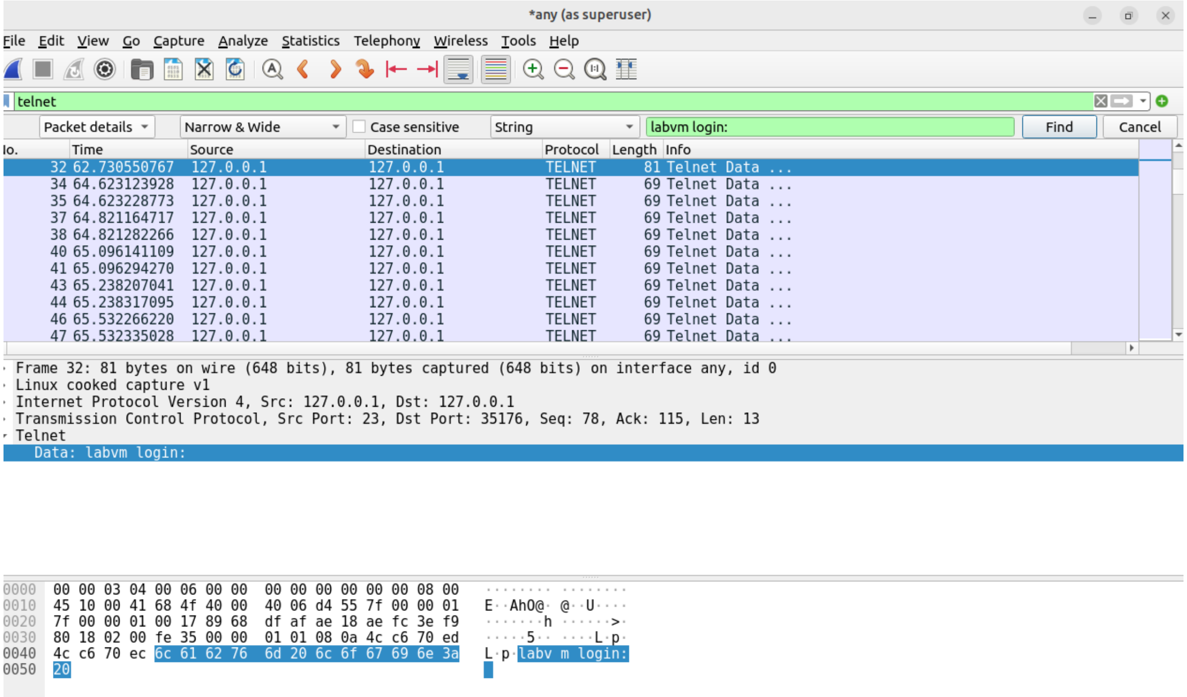
```
No.  Time          Source      Destination              Length Info
  18 62.612493662  127.0.0.1   127.0.0.1                    95 Telnet Data ...
  20 62.685280699  127.0.0.1   127.0.0.1                    80 Telnet Data ...
  22 62.685338052  127.0.0.1   127.0.0.1                   107 Telnet Data ...
  24 62.685373537  127.0.0.1   127.0.0.1        TELNET     149 Telnet Data ...
```

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.



```
lo.  Time          Source      Destination   Protocol  Length Info
  18 62.612493662  127.0.0.1   127.0.0.1     TELNET        95 Telnet Data ...
  20 62.685280699  127.0.0.1   127.0.0.1     TELNET        80 Telnet Data ...
```

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.

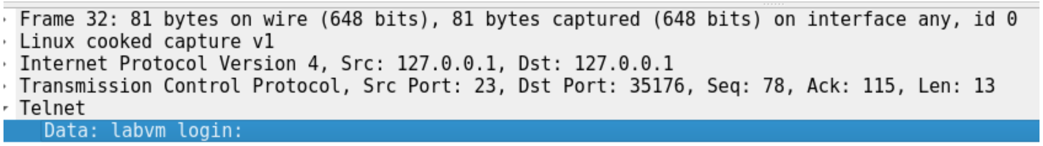


```
lo.  Time          Source      Destination   Protocol  Length Info
  32 62.730550767  127.0.0.1   127.0.0.1     TELNET        81 Telnet Data ...
  34 64.623123928  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  35 64.623228773  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  37 64.821164717  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  38 64.821282266  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  40 65.096141109  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  41 65.096294270  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  43 65.238207041  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  44 65.238317095  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  46 65.532266220  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
  47 65.532335028  127.0.0.1   127.0.0.1     TELNET        69 Telnet Data ...
```

```
› Frame 32: 81 bytes on wire (648 bits), 81 bytes captured (648 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: 23, Dst Port: 35176, Seq: 78, Ack: 115, Len: 13
▾ Telnet
    Data: labvm login:
```

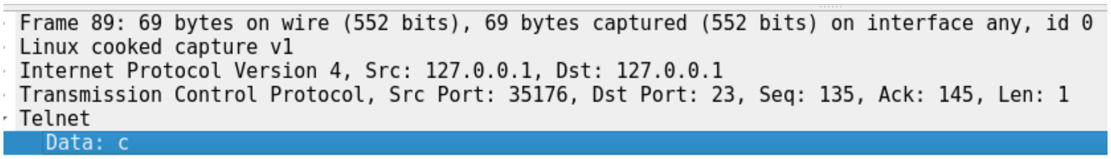
```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 10 00 41 68 4f 40 00  40 06 d4 55 7f 00 00 01   E··AhO@· @··U····
0020  7f 00 00 01 00 17 89 68  df af ae 18 ae fc 3e f9   ·······h ······>·
0030  80 18 02 00 fe 35 00 00  01 01 08 0a 4c c6 70 ed   ·····5·· ····L·p·
0040  4c c6 70 ec 6c 61 62 76  6d 20 6c 6f 67 69 6e 3a   L·p·labv m login:
0050  20
```

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

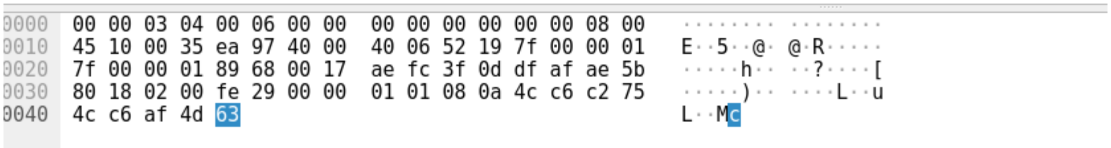


```
› Frame 32: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 23, Dst Port: 35176, Seq: 78, Ack: 115, Len: 13
▾ Telnet
    Data: labvm login:
```

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.

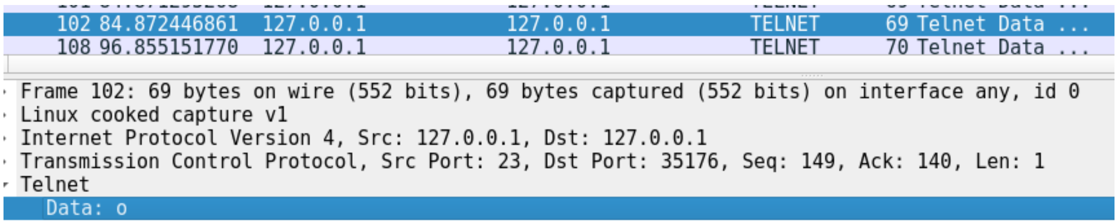


```
› Frame 89: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 35176, Dst Port: 23, Seq: 135, Ack: 145, Len: 1
⌄ Telnet
    Data: c
```

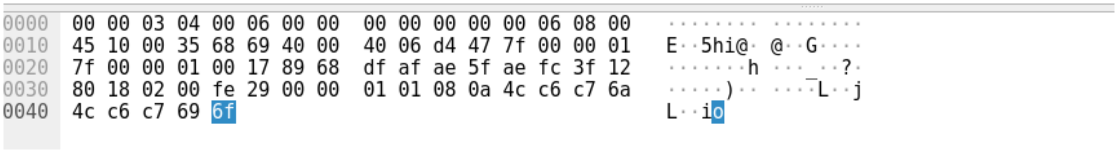


```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 10 00 35 ea 97 40 00  40 06 52 19 7f 00 00 01   E··5··@· @·R·····
0020  7f 00 00 01 89 68 00 17  ae fc 3f 0d df af ae 5b   ·····h·· ··?····[
0030  80 18 02 00 fe 29 00 00  01 01 08 0a 4c c6 c2 75   ·····)·· ····L··u
0040  4c c6 af 4d 63                                     L··Mc
```

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

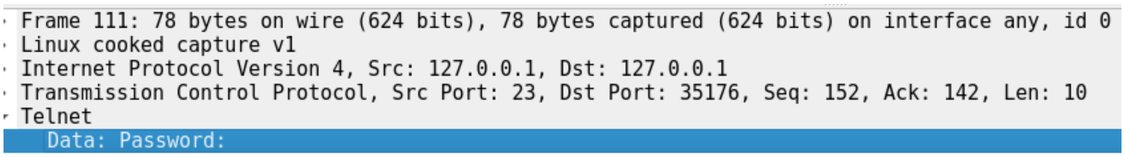


```
  102 84.872446861  127.0.0.1            127.0.0.1            TELNET      69 Telnet Data ...
  108 96.855151770  127.0.0.1            127.0.0.1            TELNET      70 Telnet Data ...

› Frame 102: 69 bytes on wire (552 bits), 69 bytes captured (552 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: 23, Dst Port: 35176, Seq: 149, Ack: 140, Len: 1
⌄ Telnet
    Data: o
```



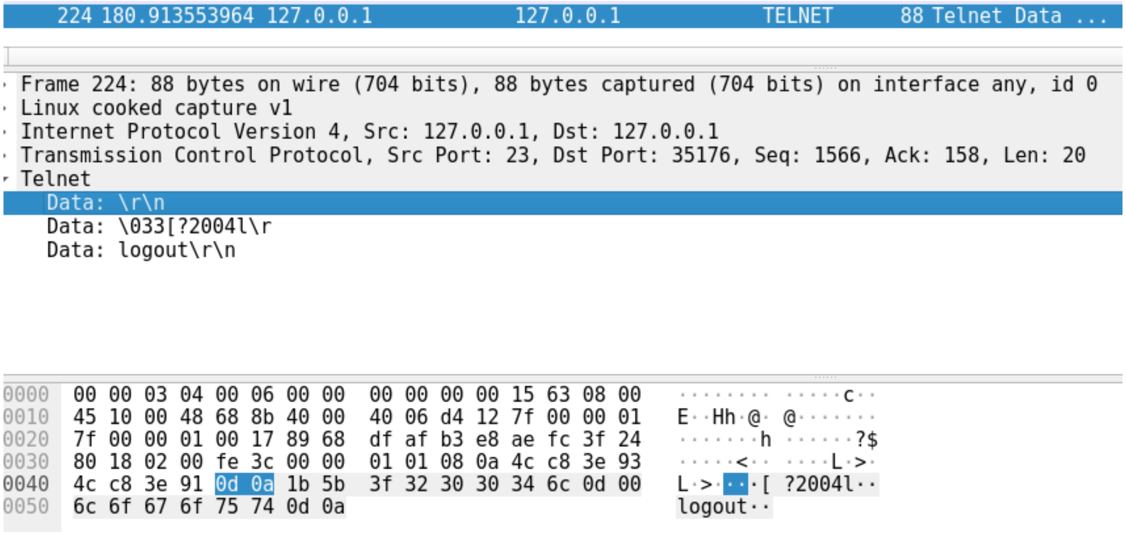
```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 06 08 00   ········ ········
0010  45 10 00 35 68 69 40 00  40 06 d4 47 7f 00 00 01   E··5hi@· @··G····
0020  7f 00 00 01 00 17 89 68  df af ae 5f ae fc 3f 12   ·······h ···_··?·
0030  80 18 02 00 fe 29 00 00  01 01 08 0a 4c c6 c7 6a   ·····)·· ····L··j
0040  4c c6 c7 69 6f                                     L··io
```

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**.



```
› Frame 111: 78 bytes on wire (624 bits), 78 bytes captured (624 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: 23, Dst Port: 35176, Seq: 152, Ack: 142, Len: 10
⌄ Telnet
    Data: Password:
```

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.



```
  224 180.913553964 127.0.0.1          127.0.0.1          TELNET     88 Telnet Data ...

› Frame 224: 88 bytes on wire (704 bits), 88 bytes captured (704 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: 23, Dst Port: 35176, Seq: 1566, Ack: 158, Len: 20
▾ Telnet
    Data: \r\n
    Data: \033[?2004l\r
    Data: logout\r\n

0000  00 00 03 04 00 06 00 00  00 00 00 00 15 63 08 00   ········ ·····c··
0010  45 10 00 48 68 8b 40 00  40 06 d4 12 7f 00 00 01   E··Hh·@· @·······
0020  7f 00 00 01 00 17 89 68  df af b3 e8 ae fc 3f 24   ·······h ······?$
0030  80 18 02 00 fe 3c 00 00  01 01 08 0a 4c c8 3e 93   ·····<·· ····L·>·
0040  4c c8 3e 91 0d 0a 1b 5b  3f 32 30 30 34 6c 0d 00   L·>····[ ?2004l··
0050  6c 6f 67 6f 75 74 0d 0a                            logout··
```

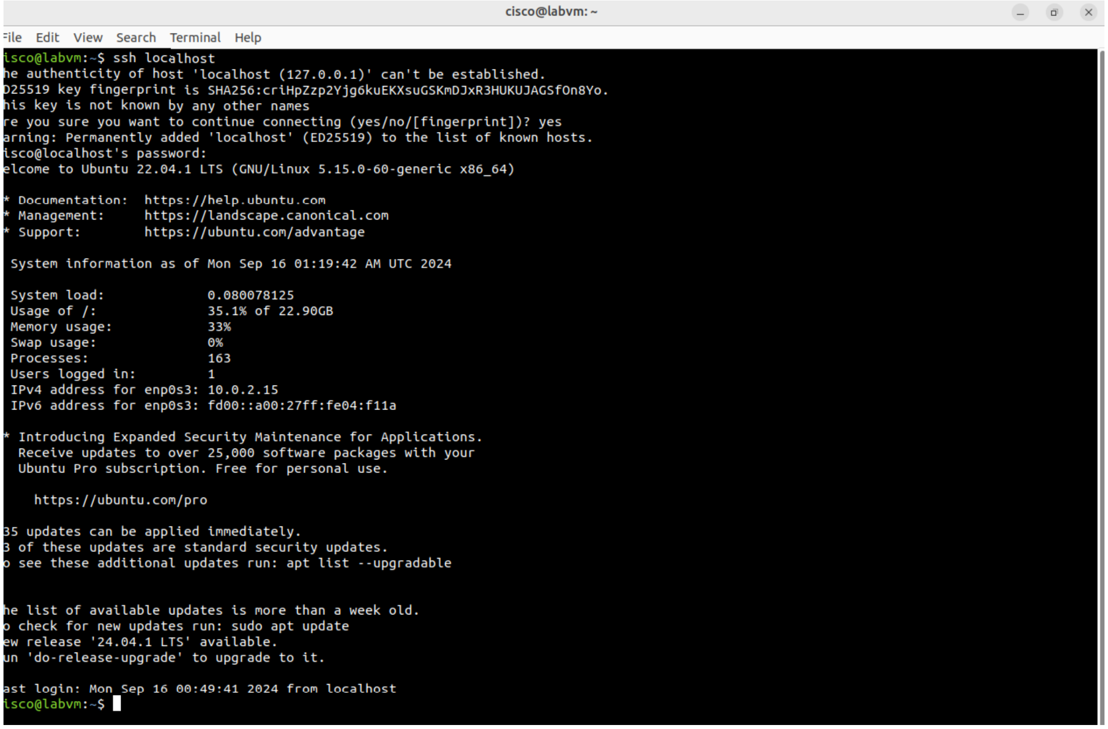
Step 4: Capture and analyze encrypted SSH traffic.

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. Return to your open terminal window or start a new terminal session.

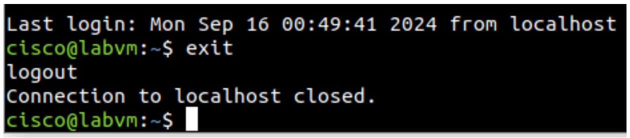
c. To simulate an SSH login, enter the command **ssh localhost**. If this is your first time to use the command, the system warns you about the authenticity of localhost and asks you if you want to continue. Enter **yes**, and then **password** as the password to log in.

```
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:~$
```



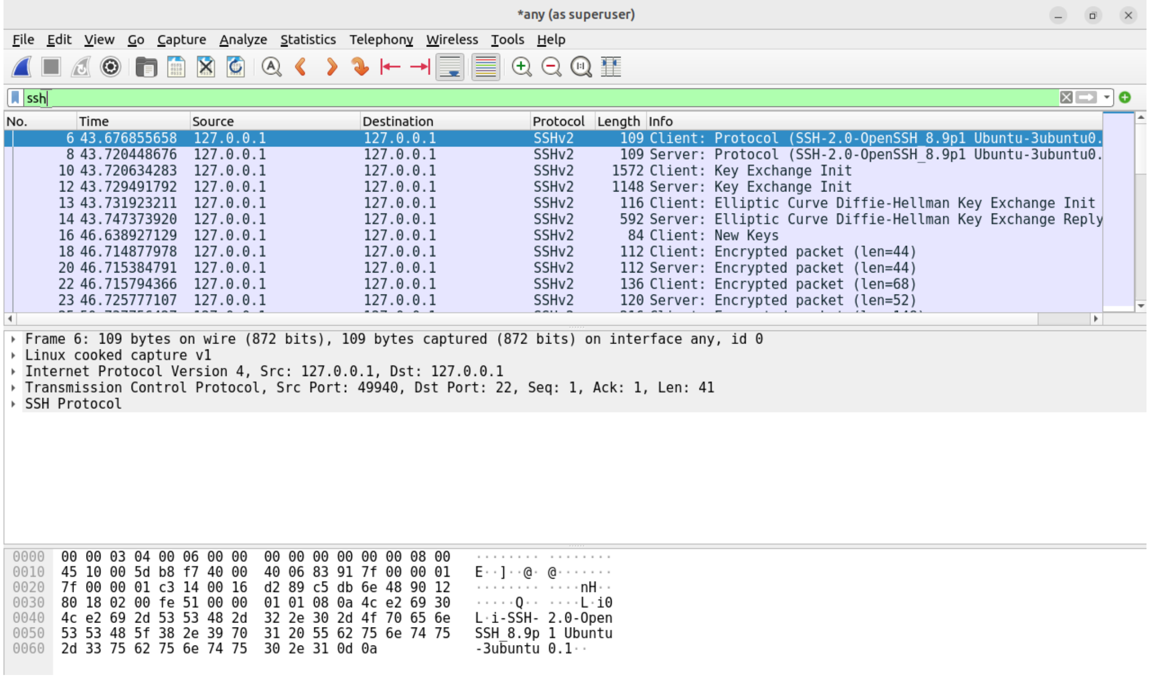
```
isco@labvm:~$ ssh localhost
he authenticity of host 'localhost (127.0.0.1)' can't be established.
D25519 key fingerprint is SHA256:criHpZzp2Yjg6kuEKXsuGSKmDJxR3HUKUJAGSfOn8Yo.
his key is not known by any other names
re you sure you want to continue connecting (yes/no/[fingerprint])? yes
arning: Permanently added 'localhost' (ED25519) to the list of known hosts.
isco@localhost's password:
elcome 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 01:19:42 AM UTC 2024

 System load:             0.080078125
 Usage of /:              35.1% of 22.90GB
 Memory usage:            33%
 Swap usage:              0%
 Processes:               163
 Users logged in:         1
 IPv4 address for enp0s3: 10.0.2.15
 IPv6 address for enp0s3: fd00::a00:27ff:fe04:f11a

* 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

35 updates can be applied immediately.
3 of these updates are standard security updates.
o see these additional updates run: apt list --upgradable


he list of available updates is more than a week old.
o check for new updates run: sudo apt update
ew release '24.04.1 LTS' available.
un 'do-release-upgrade' to upgrade to it.

ast login: Mon Sep 16 00:49:41 2024 from localhost
isco@labvm:~$ 
```

d. Enter the **exit** command to end the SSH session.



```
Last login: Mon Sep 16 00:49:41 2024 from localhost
cisco@labvm:~$ exit
logout
Connection to localhost closed.
cisco@labvm:~$ 
```

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.


*any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

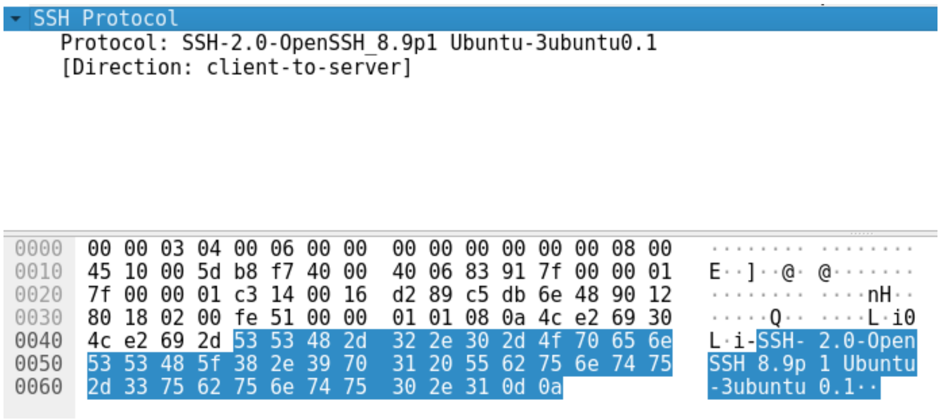
ssh

```
No.   Time          Source      Destination   Protocol  Length Info
    6 43.676855658  127.0.0.1   127.0.0.1     SSHv2        109 Client: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.
    8 43.720448676  127.0.0.1   127.0.0.1     SSHv2        109 Server: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.
   10 43.720634283  127.0.0.1   127.0.0.1     SSHv2       1572 Client: Key Exchange Init
   12 43.729491792  127.0.0.1   127.0.0.1     SSHv2       1148 Server: Key Exchange Init
   13 43.731923211  127.0.0.1   127.0.0.1     SSHv2        116 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
   14 43.747373920  127.0.0.1   127.0.0.1     SSHv2        592 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply
   16 46.638927129  127.0.0.1   127.0.0.1     SSHv2         84 Client: New Keys
   18 46.714877978  127.0.0.1   127.0.0.1     SSHv2        112 Client: Encrypted packet (len=44)
   20 46.715384791  127.0.0.1   127.0.0.1     SSHv2        112 Server: Encrypted packet (len=44)
   22 46.715794366  127.0.0.1   127.0.0.1     SSHv2        136 Client: Encrypted packet (len=68)
   23 46.725777107  127.0.0.1   127.0.0.1     SSHv2        120 Server: Encrypted packet (len=52)
```

```
› Frame 6: 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: 49940, Dst Port: 22, Seq: 1, Ack: 1, Len: 41
› SSH Protocol
```

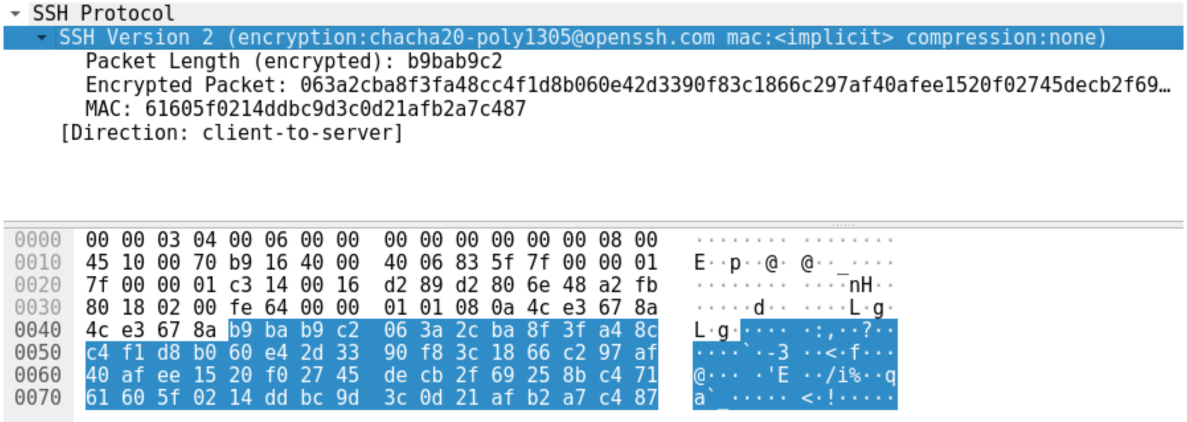
```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 10 00 5d b8 f7 40 00  40 06 83 91 7f 00 00 01   E··]··@· @·······
0020  7f 00 00 01 c3 14 00 16  d2 89 c5 db 6e 48 90 12   ········ ····nH··
0030  80 18 02 00 fe 51 00 00  01 01 08 0a 4c e2 69 30   ·····Q·· ····L·i0
0040  4c e2 69 2d 53 53 48 2d  32 2e 30 2d 4f 70 65 6e   L·i-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··
```

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.



```
▾ 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 00 08 00   ········ ········
0010  45 10 00 5d b8 f7 40 00  40 06 83 91 7f 00 00 01   E··]··@· @·······
0020  7f 00 00 01 c3 14 00 16  d2 89 c5 db 6e 48 90 12   ········ ····nH··
0030  80 18 02 00 fe 51 00 00  01 01 08 0a 4c e2 69 30   ·····Q·· ····L·i0
0040  4c e2 69 2d 53 53 48 2d  32 2e 30 2d 4f 70 65 6e   L·i-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··
```



```
▾ SSH Protocol
  ▾ SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)
      Packet Length (encrypted): b9bab9c2
      Encrypted Packet: 063a2cba8f3fa48cc4f1d8b060e42d3390f83c1866c297af40afee1520f02745decb2f69…
      MAC: 61605f0214ddbc9d3c0d21afb2a7c487
    [Direction: client-to-server]
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 10 00 70 b9 16 40 00  40 06 83 5f 7f 00 00 01   E··p··@· @··_····
0020  7f 00 00 01 c3 14 00 16  d2 89 d2 80 6e 48 a2 fb   ········ ····nH··
0030  80 18 02 00 fe 64 00 00  01 01 08 0a 4c e3 67 8a   ·····d·· ····L·g·
0040  4c e3 67 8a b9 ba b9 c2  06 3a 2c ba 8f 3f a4 8c   L·g····· ·:,··?··
0050  c4 f1 d8 b0 60 e4 2d 33  90 f8 3c 18 66 c2 97 af   ····`·-3 ··<·f···
0060  40 af ee 15 20 f0 27 45  de cb 2f 69 25 8b c4 71   @··· ·'E ··/i%··q
0070  61 60 5f 02 14 dd bc 9d  3c 0d 21 af b2 a7 c4 87   a`_····· <·!·····
```