Lab - Examining Telnet and SSH in Wireshark

Objectives

Part 1: Examine a Telnet Session with Wireshark

Part 2: Examine an SSH Session with Wireshark

Background / Scenario

In this lab, you will configure a router to accept SSH connectivity and use Wireshark to capture and view Telnet and SSH sessions. This will demonstrate the importance of encryption with SSH.

Required Resources

- CyberOps Workstation VM

Part 1: Examining a Telnet Session with Wireshark

You will use Wireshark to capture and view the transmitted data of a Telnet session.

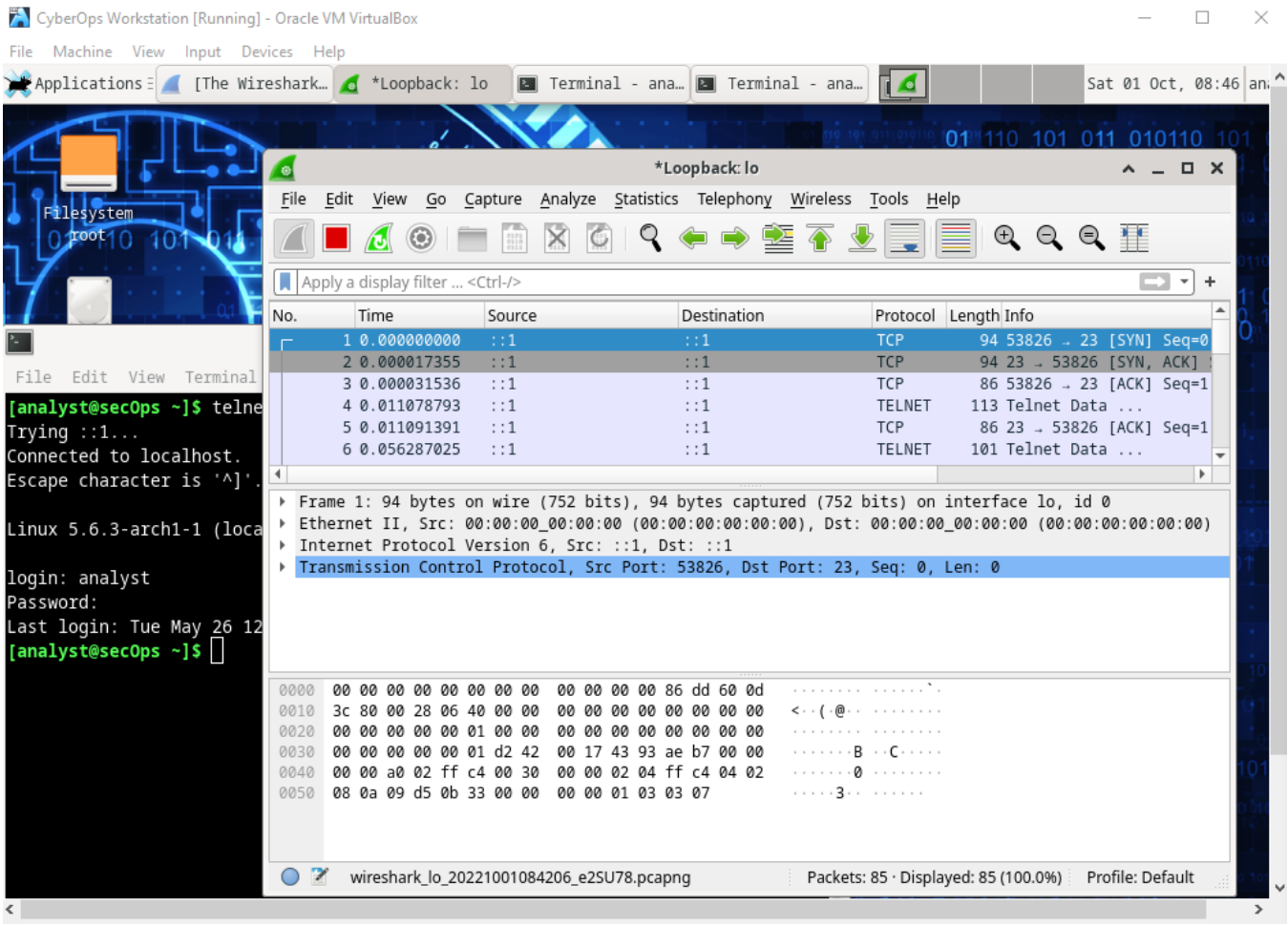
Step 1: Capture data.

a. Start the CyberOps Workstation VM and log in with username **analyst** and password **cyberops**.

b. Open a terminal window and start Wireshark. Press **OK** to continue after reading the warning message.

```
[analyst@secOps analyst]$ sudo wireshark-gtk
[sudo] password for analyst: cyberops

** (wireshark-gtk:950): WARNING **: Couldn't connect to accessibility bus:
Failed to connect to socket /tmp/dbus-REDRWOHelr: Connection refused
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
```

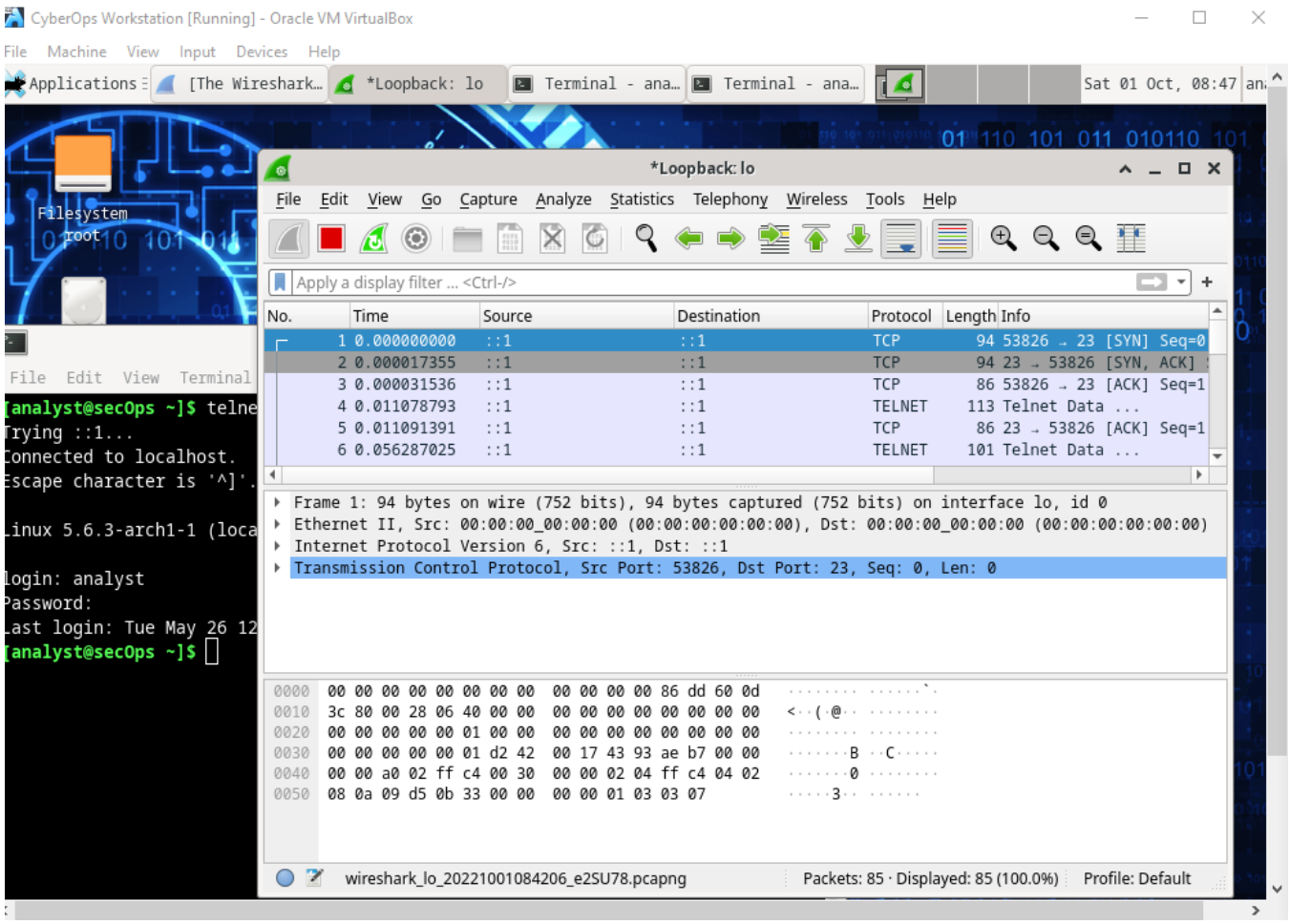
c. Start a Wireshark capture on the **Loopback: lo** interface.



d. Open another terminal window. Start a Telnet session to the localhost. Enter username **analyst** and password **cyberops** when prompted. Note that it may take several minutes for the "connected to localhost" and login prompt to appear.

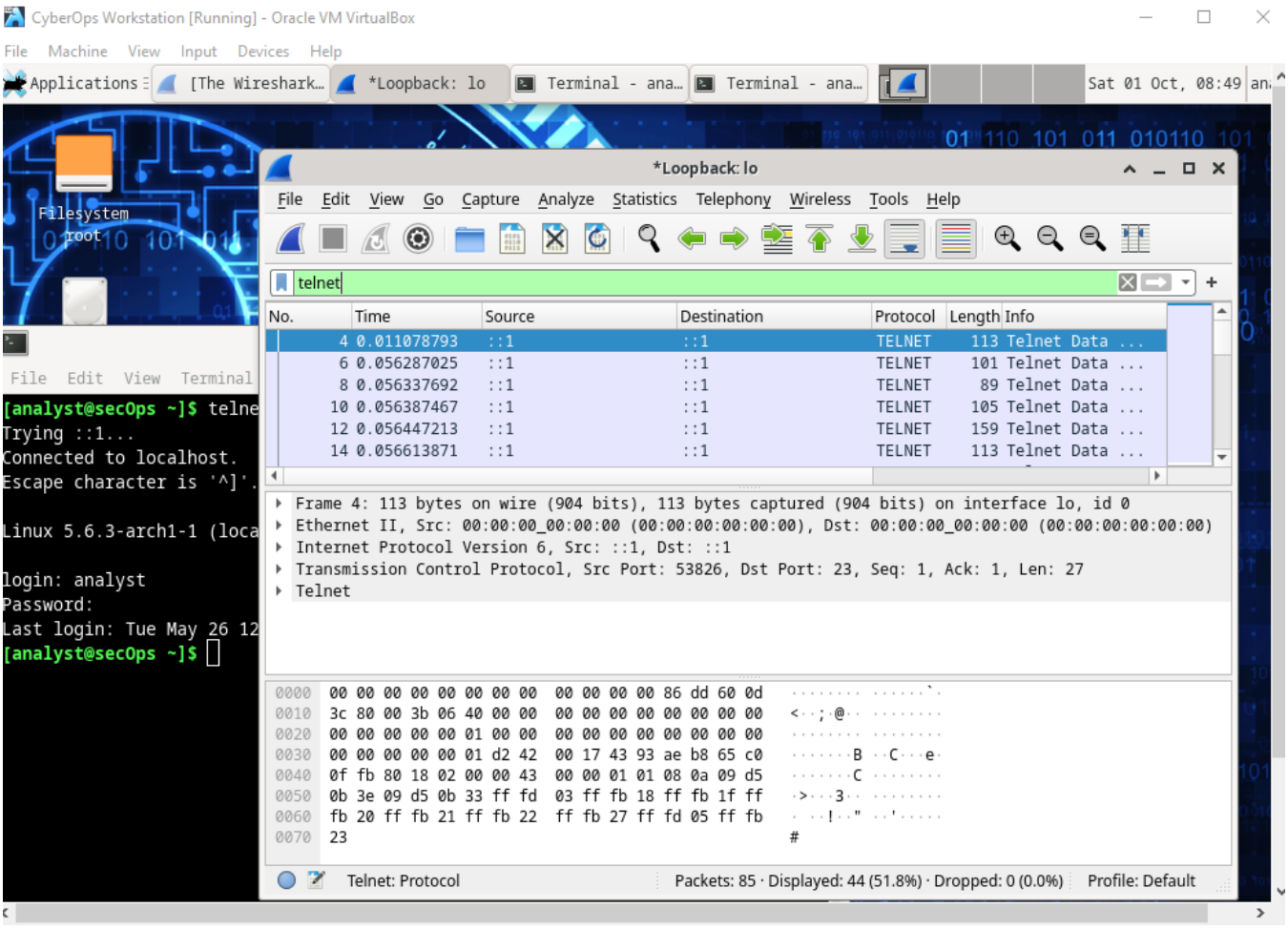
```
[analyst@secOps ~]$ telnet localhost
Trying ::1...
Connected to localhost.
Escape character is '^]'.

Linux 4.10.10-1-ARCH (unallocated.barefruit.co.uk) (pts/12)

secOps login: analyst
Password:
Last login: Fri Apr 28 10:50:52 from localhost.localdomain
[analyst@secOps ~]$
```

e. Stop the Wireshark capture after you have provided the user credentials.

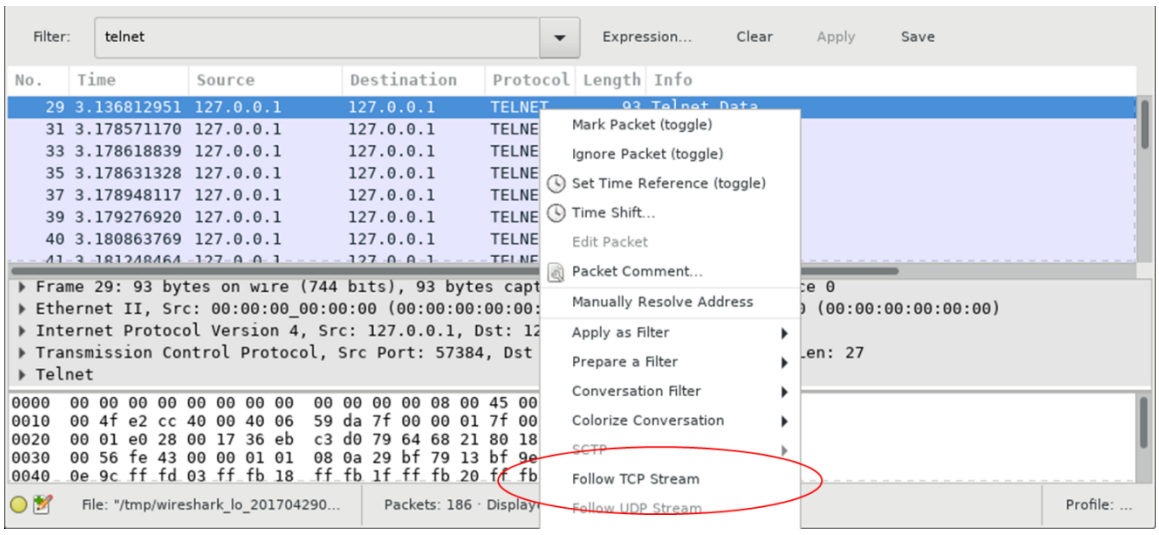


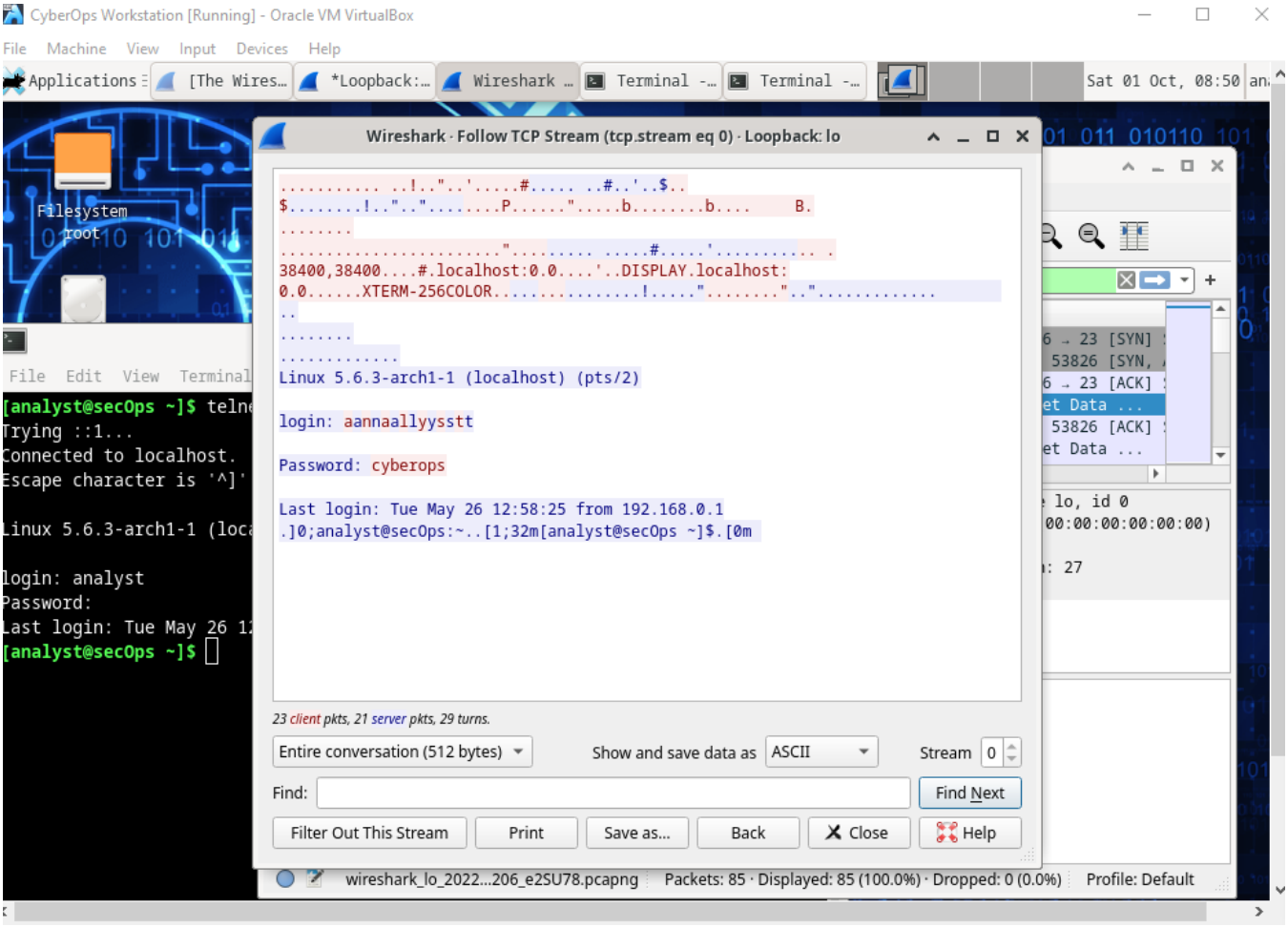
Step 2: **Examine the Telnet session.**

a. Apply a filter that only displays Telnet-related traffic. Enter **Telnet** in the filter field and click **Apply**.

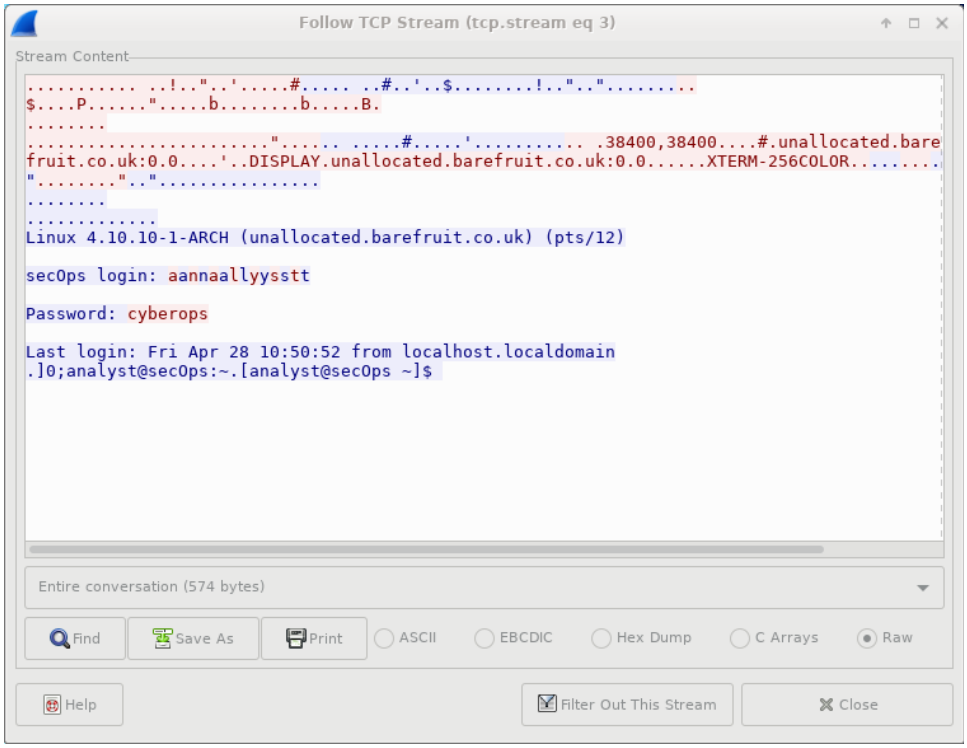


b. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow TCP Stream**.





c. The Follow TCP Stream window displays the data for your Telnet session with the CyberOps Workstation VM. The entire session is displayed in plaintext, including your password. Notice that the username that you entered is displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.



d. After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**.

e. Type **exit** at the terminal to exit the **Telnet** session.

```
[analyst@secOps ~]$ exit
```

Part 2: Examine an SSH Session with Wireshark

In Part 2, you will establish an SSH session with the localhost. Wireshark will be used to capture and view the data of this SSH session.

a. Start another Wireshark capture.

b. You will establish an SSH session with the localhost. At the terminal prompt, enter **ssh localhost**. Enter **yes** to continue connecting. Enter the **cyberops** when prompted.

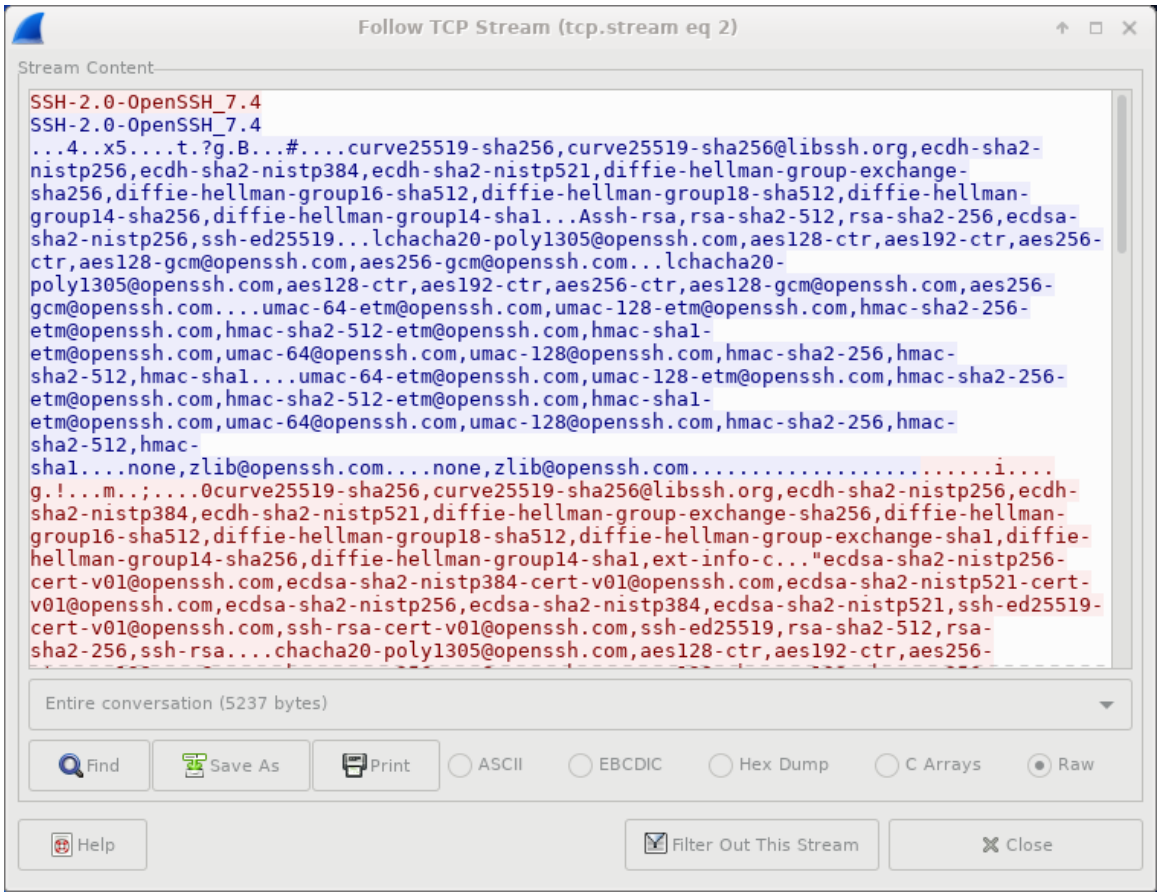
```
[analyst@secOps ~]$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:uLDhKZflmvsR8Et8jer1NuD91cGDS1mUl/p7VI3u6kI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
analyst@localhost's password:
Last login: Sat Apr 29 00:04:21 2017 from localhost.localdomain
```

c. Stop the Wireshark capture.

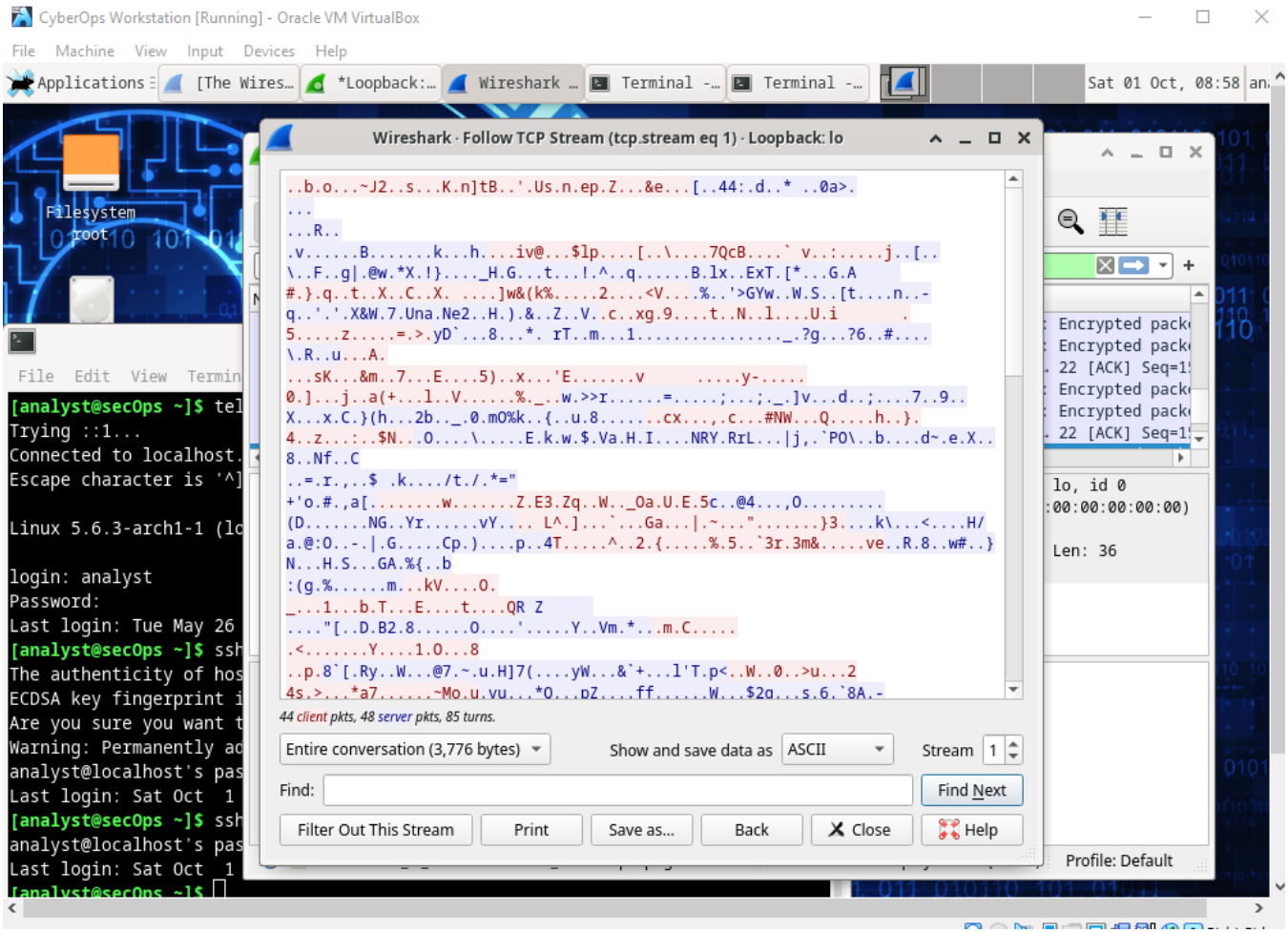
d. Apply an SSH filter on the Wireshark capture data. Enter **ssh** in the filter field and click **Apply**.

e. Right-click one of the **SSHv2** lines in the **Packet list** section of Wireshark, and in the drop-down list, select the **Follow TCP Stream** option.

f. Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.



Screenshot



g. After examining your SSH session, click **Close**.

h. Close Wireshark.

Reflection

Why is SSH preferred over Telnet for remote connections?

SSH performs the same primary function as Telnet, but in a more secure manner. This protocol ensures secure access even on unsecured networks, removing many of Telnet's flaws. Administrators can use SSH to log into remote devices, execute commands, transfer files between devices, and more. This prevents sensitive information from being captured during transmission, such as usernames and passwords.