**Assignment 06 – Wireshark- Lab Report**

**Department of Computer Science**

**Adelphi university  
CSC – 380 -001 Computer and Network Security**

**Professor. Sung Kim By – Dikshant Kakadiya**

**Date – April 16th 2024**

# Overview

# This exercise introduces the Wireshark network traffic analysis tool. The student will use Wireshark to view network traffic captured in a “PCAP” file and locate a specific packet. PCAP files contain copies of network traffic stored in a format that can be processed by various network analysis tools, such as Wireshark and TCPdump. PCAP is short for “packet capture.”

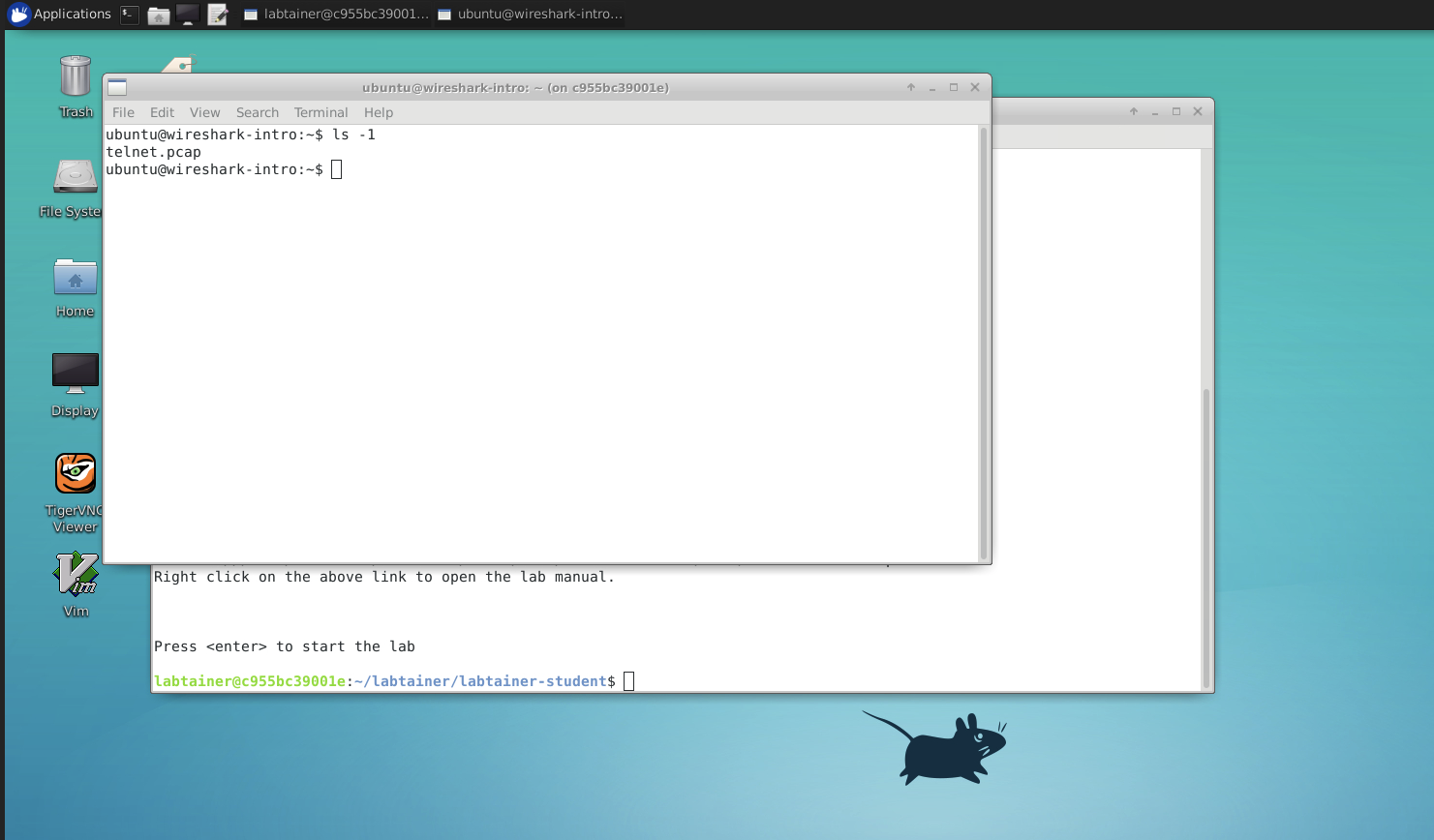
**Set-up for Lab Environment**

To start the lab, we will type: labtainer wireshark-intro

# Tasks

## Explore

Use the ls -l command to view the content of the directory in the terminal that opened when you started the lab.

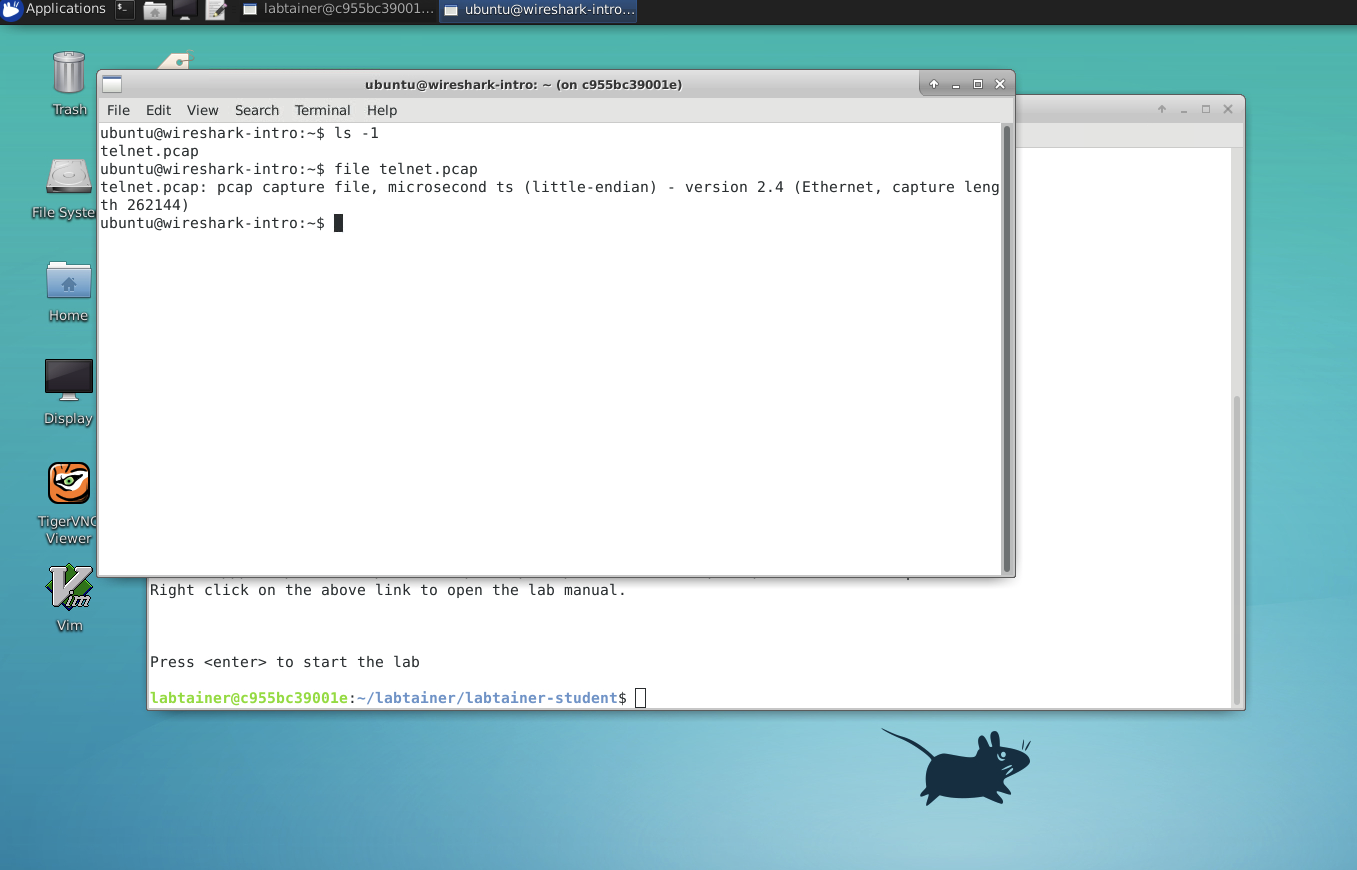


As shown in the image above, we used the 'ls-l' command to display the files in the directory. We observed that there is a single file named 'talent. cap '. This file is crucial as it contains the network traffic data we will be analyzing using Wireshark.

That telnet. pcap file contains the network traffic you will analyze. Use

file telnet.pcap

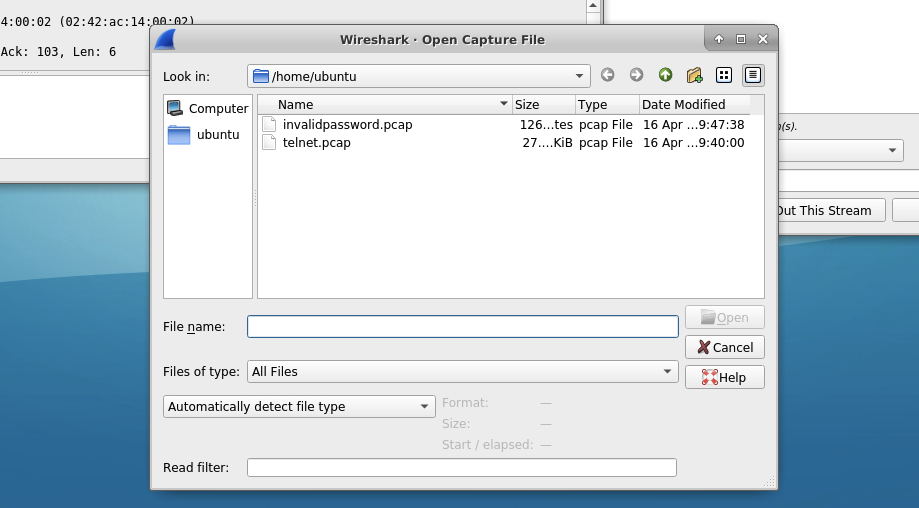
to view information about the file.



As we can see in the above image, we used file commands to see information about the file. I have information about the version and entrant.

## Run wireshark to perform PCAP Analysis

Start Wireshark using the wireshark command. Then use File->Open to open the telnet.pcap file. **NOTE:** If you encounter a black or corrupt window while using Wireshark, try to resize the window a bit. if the window will not resize, try stopping the applicaiton and starting it again.



As we can see in the above image, this is what opening a file menu looks alike.

1.3 Find a specific packet

Locate the single packet which contains the password provided when the user attempted to use Telnet to login as the ”john” user.

Hint: If you type telnet.data into the field that says “Add a display filter” (see Figure 1), the tool will display only Telnet data packets. Press return to apply the filter.

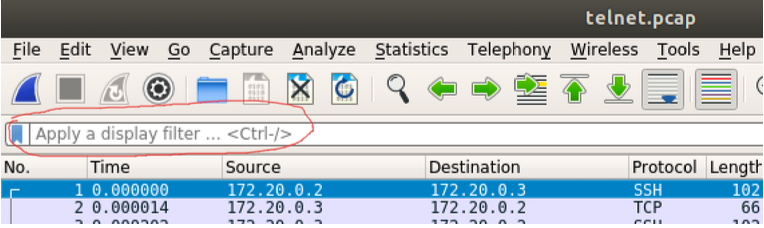
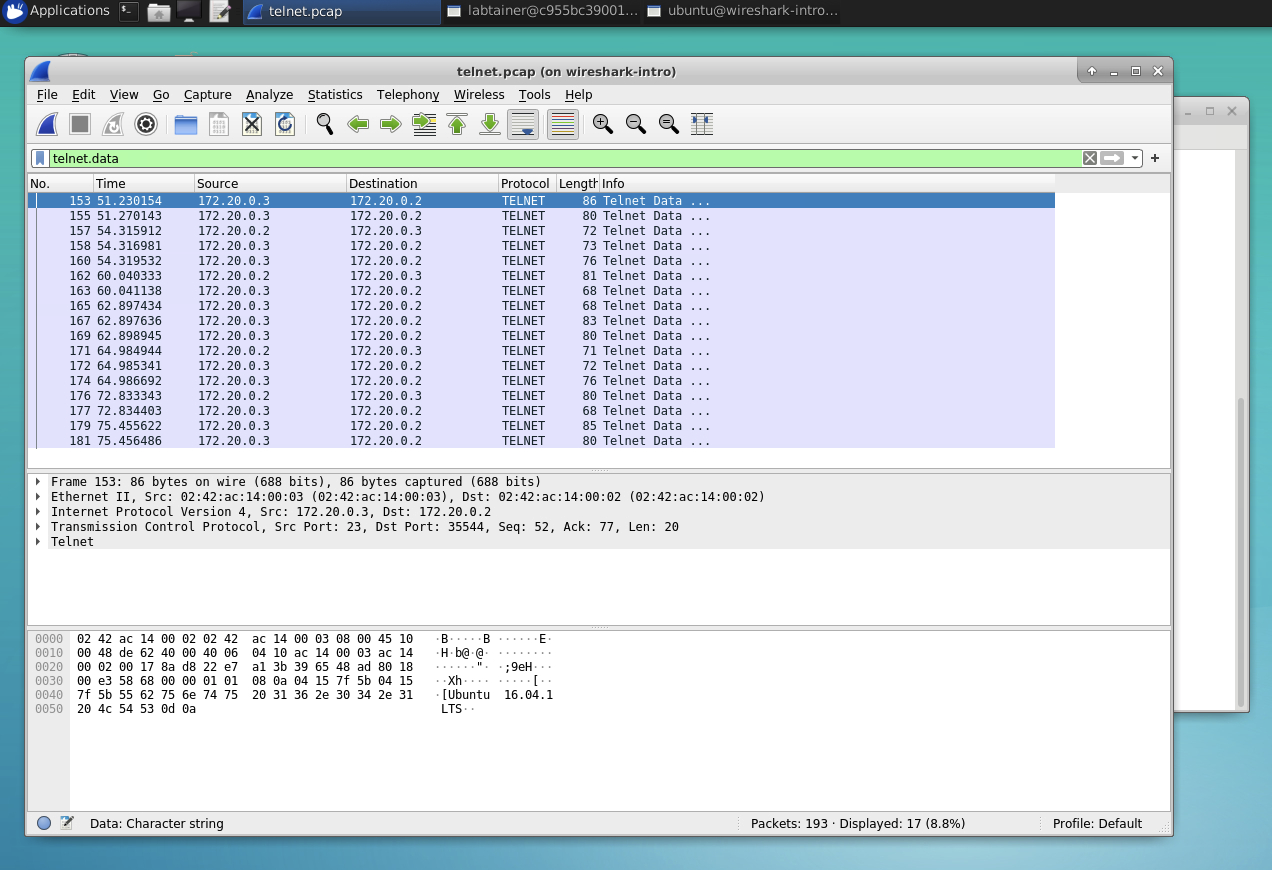


Figure 1: Display filter

Onceyoulocatethesinglepacketcontainingtheinvalidpassword,useFile=>Export specified packets to save the single packet that you located. Save the single packet as *invalidpassword.pcap*. Be suretoselecttheSelected packets onlyradiobuttonintheExportdialogandbesuretogetthefile name exactly right.

After you save the packet, you might then use File=>Open to open your new pcap file to confirm it contains the correct packet.

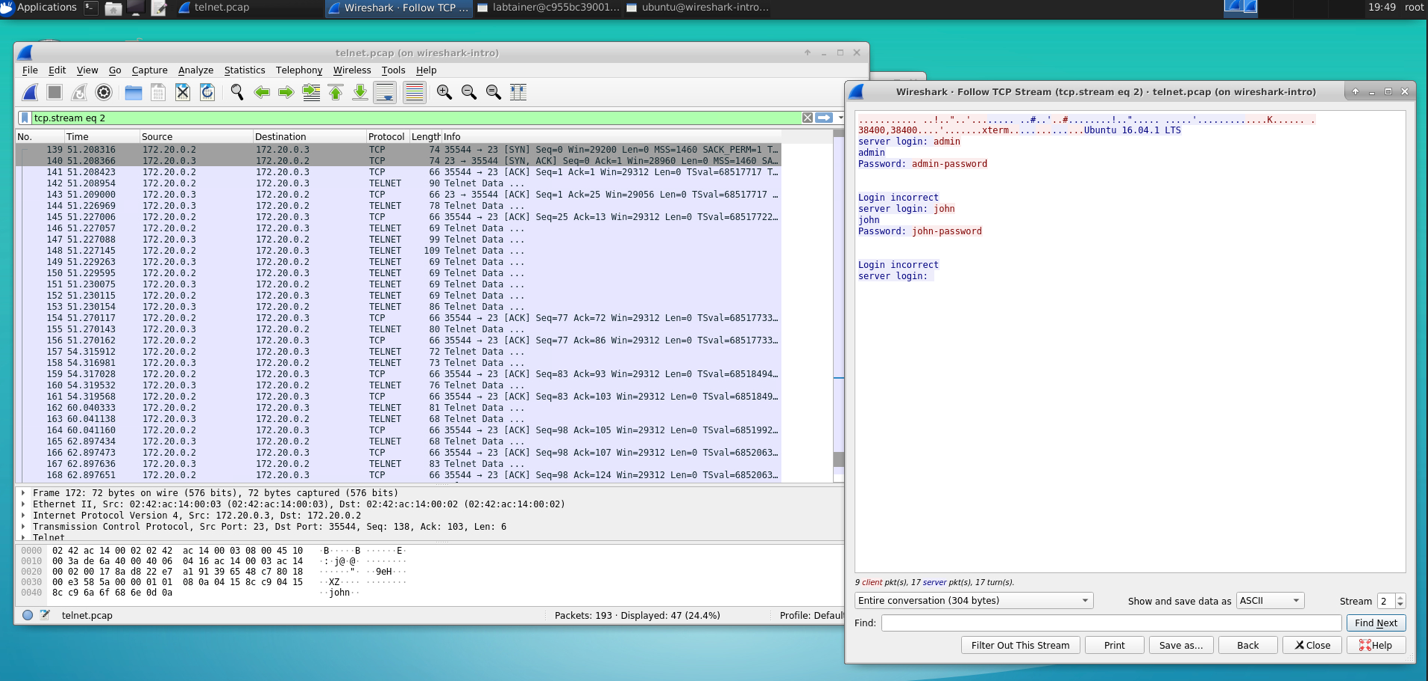


As we can see in the figure above, we used the search box at the top left corner and typed ‘Telenet. data’. so it will find all the files that are related to this particular key work that we tried in the box. Also, we can see there are few results that we were able to find.

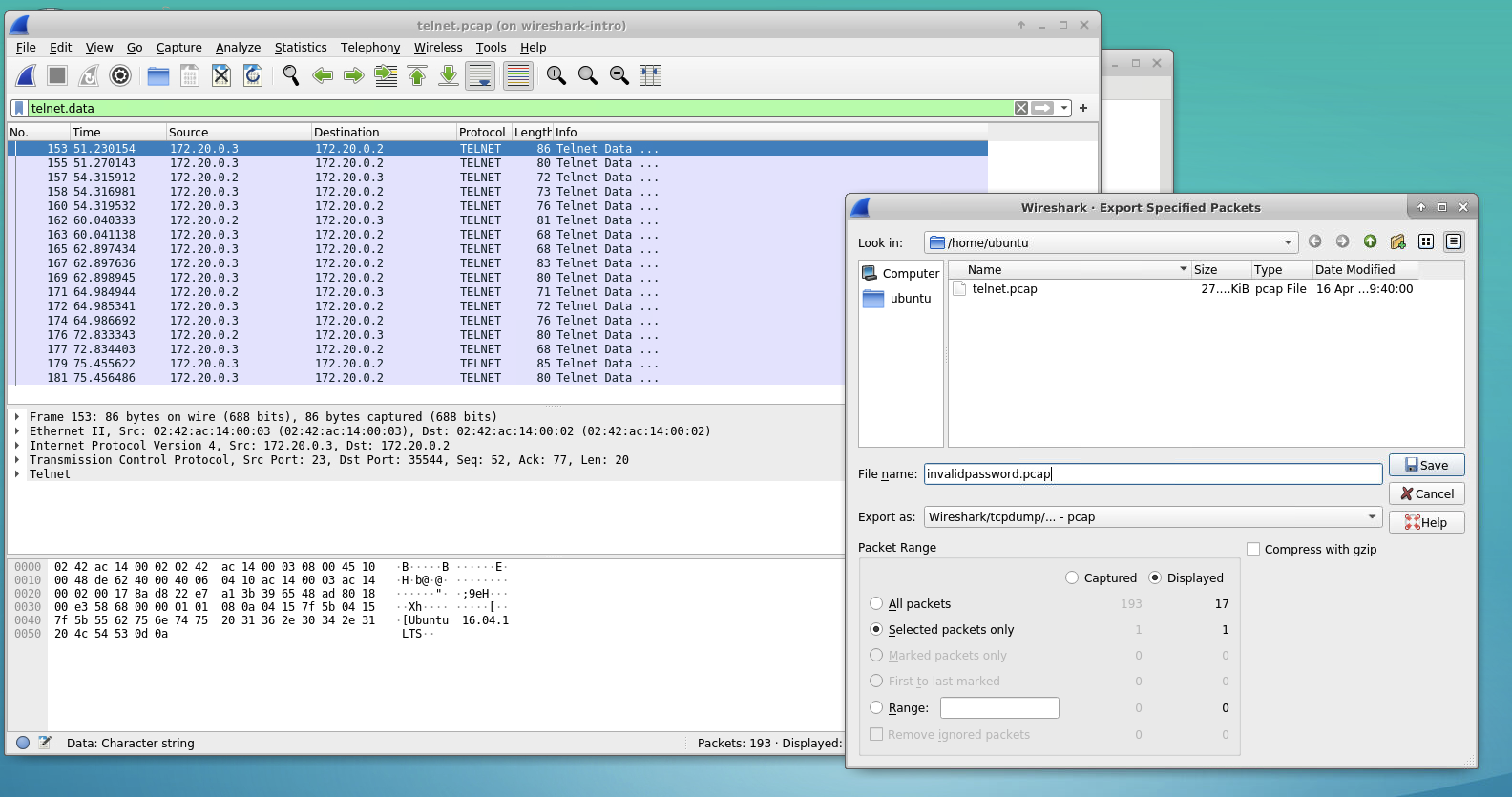
1.4 Explore some more

Look through other packets and experiment with filters. Try selecting one of the TELNET packets and use theAnalyze=>Follow=>TCP streamfunctiontoviewtheentireTELNETconversation.

After you complete this lab, consider performing the *packet-introspection* lab to delve deeper into traffic analysis with Wireshark.



As we can see in the above image, it is of a TCP stream. How do you open this stream? First, click on a file, then go to analyze, then click on follow, then click on TCP stream. A new window will pop up displaying all the information.



We also saved the information of the TCP stream in a field called invalidpassword.pcap. as we can see in the above image how it is done.

**Background**

This exercise assumes you have received instruction TCP/IP networking. In this lab you will be asked to analyze packets from a Telnet session. Telnet is a communications protocol that allows a user to issue shell commands to a remote host. Telnet network traffic is not encrypted, which simplifies traffic analysis. Refer to the *telnetlab* for further background.

This lab exercise only touches on some of the most basic features of Wireshark. Details on using the tool  
can be found at https://www.wireshark.org/docs/wsug\_html\_chunked/ChapterIntroduction. html