BITS Pilani - Hyderabad Campus
CS F303 (Computer Networks)
Second Semester 2023-24, Lab Sheet 2
Introduction to Wireshark

1. Overview

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. It is a data capturing program that "understands" the encapsulation of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses “pcap” to capture packets, so it can only capture packets on the types of networks that pcap supports.

Note: Wireshark is already installed (on Lab Machine), if want to install on PC, link for Installation of Wireshark: Wireshark User’s Guide.

2. Install Wireshark (if already installed, then please go to Section 3)

Please follow these steps for the installation.

- Using the following command: *sudo apt-get update*
- Then please use: *sudo apt-get install wireshark*
- To see the version use: *wireshark -v*
- To open wireshark use: *sudo wireshark &*
- Finally, you will see the screen shown in Figure 1.

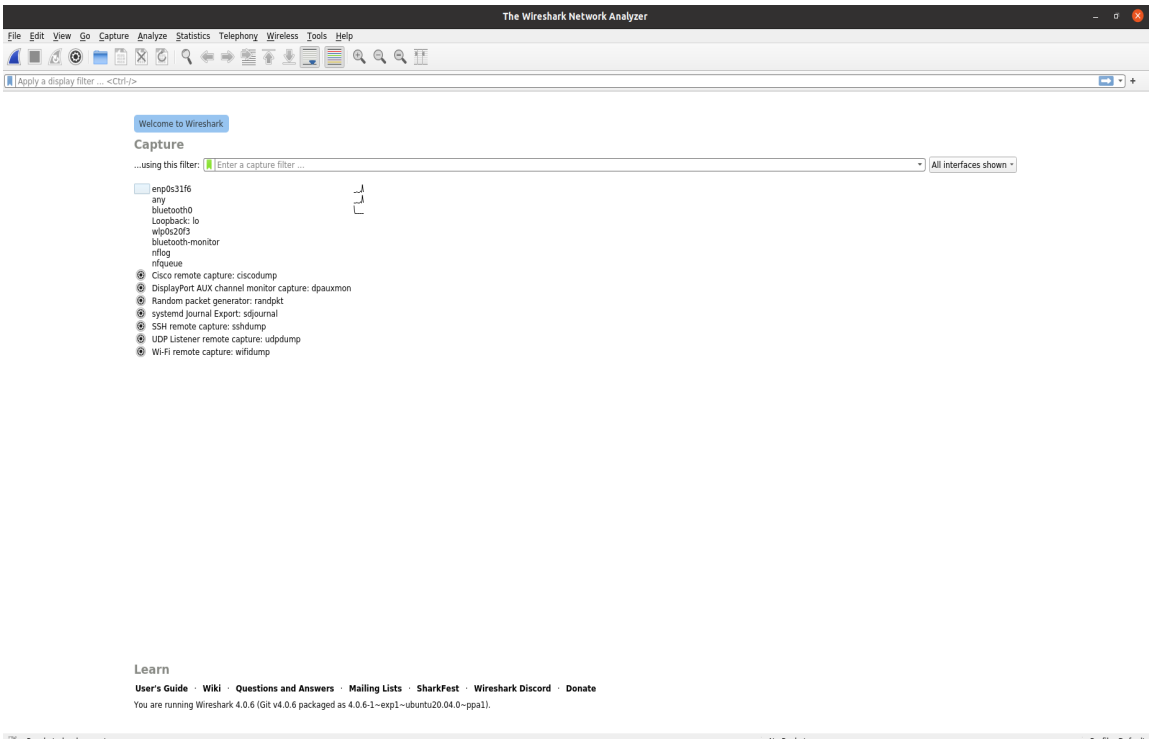

Figure 1 Wireshark main screen after installation and running

Note: One needs administrator privileges to work with Wireshark. Run Wireshark with sudo privileges (type “sudo wireshark” in the Terminal). Ignore any error message.

3. Installing Npcap

The Wireshark installer contains the latest Npcap installer. If you don’t have Npcap installed, you won’t be able to capture live network traffic but you will still be able to open saved capture files. By default, the latest version of Npcap will be installed. If you don’t wish to do this or if you wish to reinstall Npcap you can check the Install Npcap box as needed. For more information about Npcap see https://nmap.org/npcap/ and https://wiki.wireshark.org/Npcap.

4. Working with Wireshark

Capture with Wireshark: Start the Wireshark and Go to Capture->interfaces. This will show all the interfaces available in the system (See Figure 2). **Observe the number of interfaces in your system.**

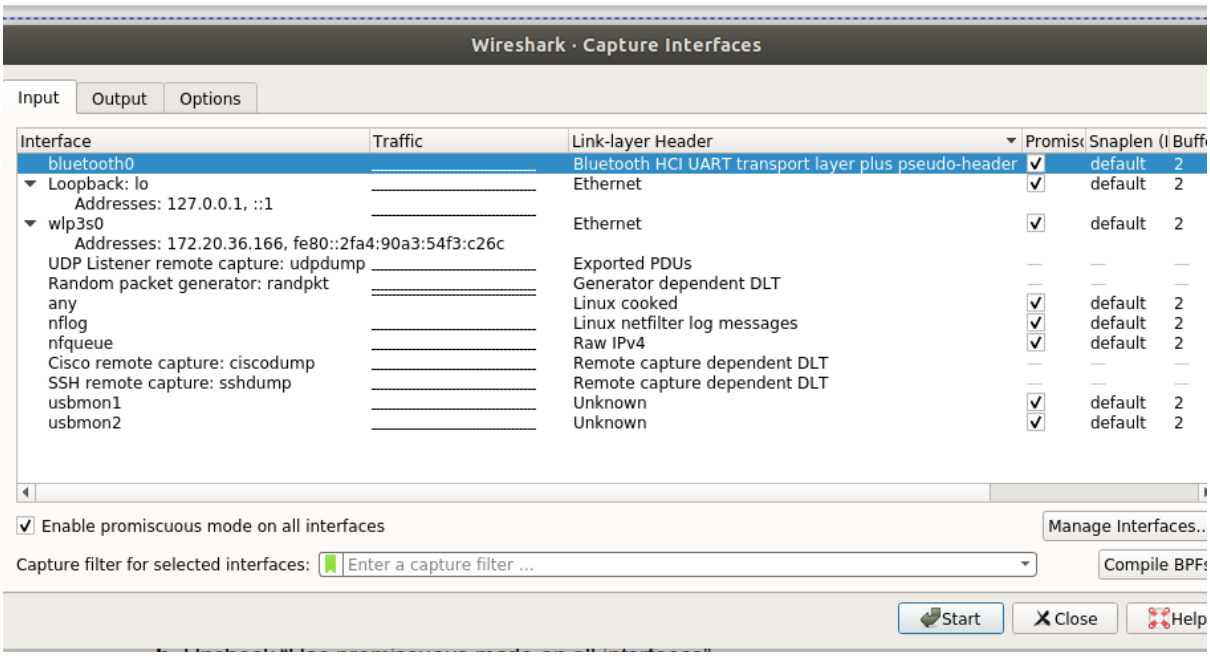

Figure 2 Available interfaces captured via Wireshark

Now Go to Capture->Options menu and:

- Check the “eth0” interface and uncheck all other interfaces.
- Uncheck “Use promiscuous mode on all interfaces”.

Do packet capturing by clicking Capture->Start button. Now, the captured packets are shown in the center window. Browse one or more websites. After a while (15 to 20 seconds), stop the capturing (Capture->Stop button). Find out what is promiscuous mode of operation. Also, there are several protocol packets captured by your system. You can write down the names of 3-4 of them.

Filters with Wireshark: There are display filters and capture filters. Display filters can be used on already captured packets. Specify any one of the following items (HTTP and ICMP) in the display filter and press “Apply”. The sample output is shown in Figure 3. Observe the difference.

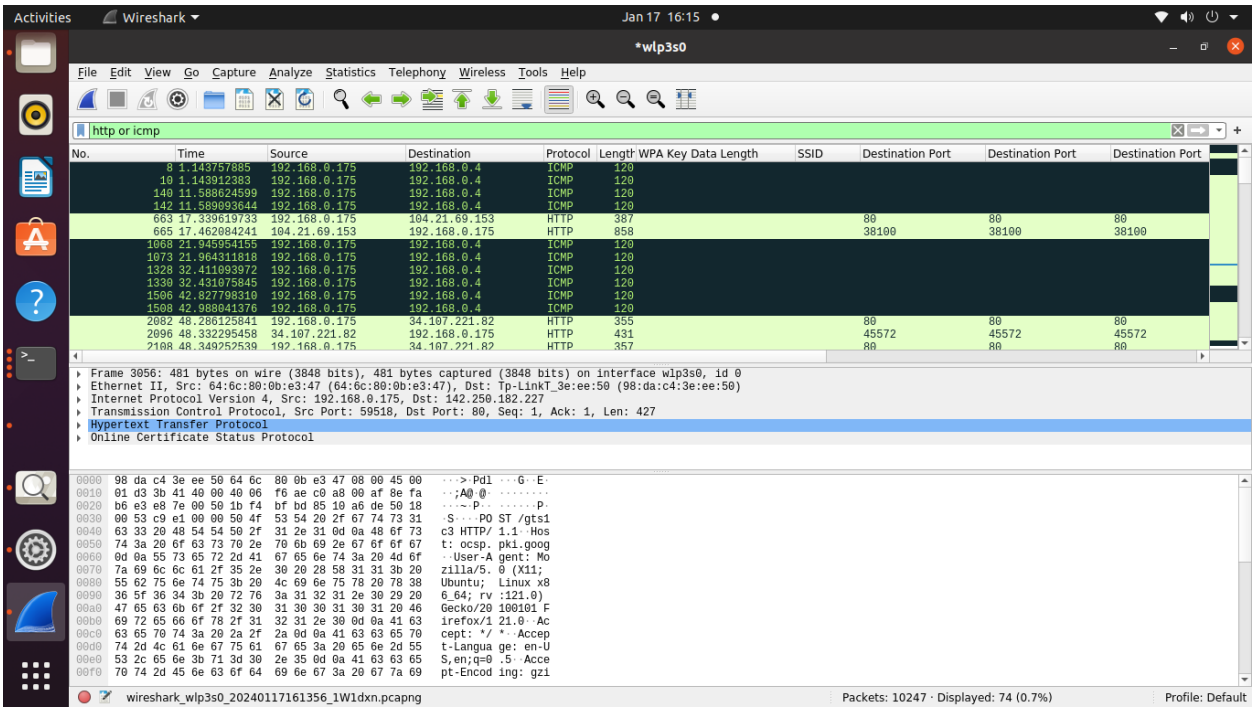

Figure 3 Filtering and capturing via Wireshark

Coloring rules with Wireshark – Depending on the protocol (HTTP, ICMP, etc.) the color of a packet is different as shown in Figure 4. These rules can be changed accordingly (View->Coloring Rules).

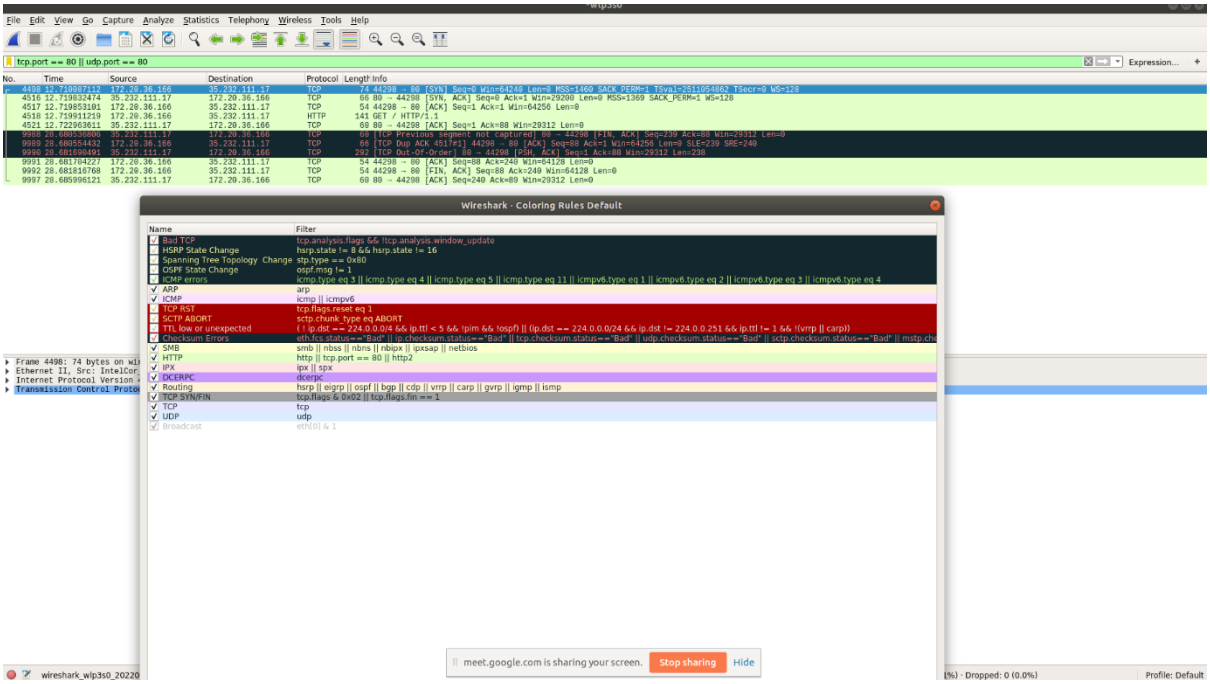

Figure 4 Coloring rules with Wireshark

Saving the output with Wireshark: After stopping the capture, do it from File->Save As. After that you can close the file and try to open the pcap file in Wireshark.

Statistics in Wireshark:

To understand the tools used in Wireshark to measure network statistics, do the following:

- Start a new capture in Wireshark.
- Browse a couple of websites.
- Stop the capture after a while (30 to 40 seconds).
- Go to the Protocol hierarchy.
- Give the major protocol hierarchies which you see for any two of the websites surfed by you?
- Do you observe any differences in protocol hierarchies? If yes, mention.
- How many ethernet endpoints are visible? Is your PC's MAC address part of the Ethernet ?
- Goto Explore Statistics -> Endpoints to identify entities involved in capture (Figure 5)

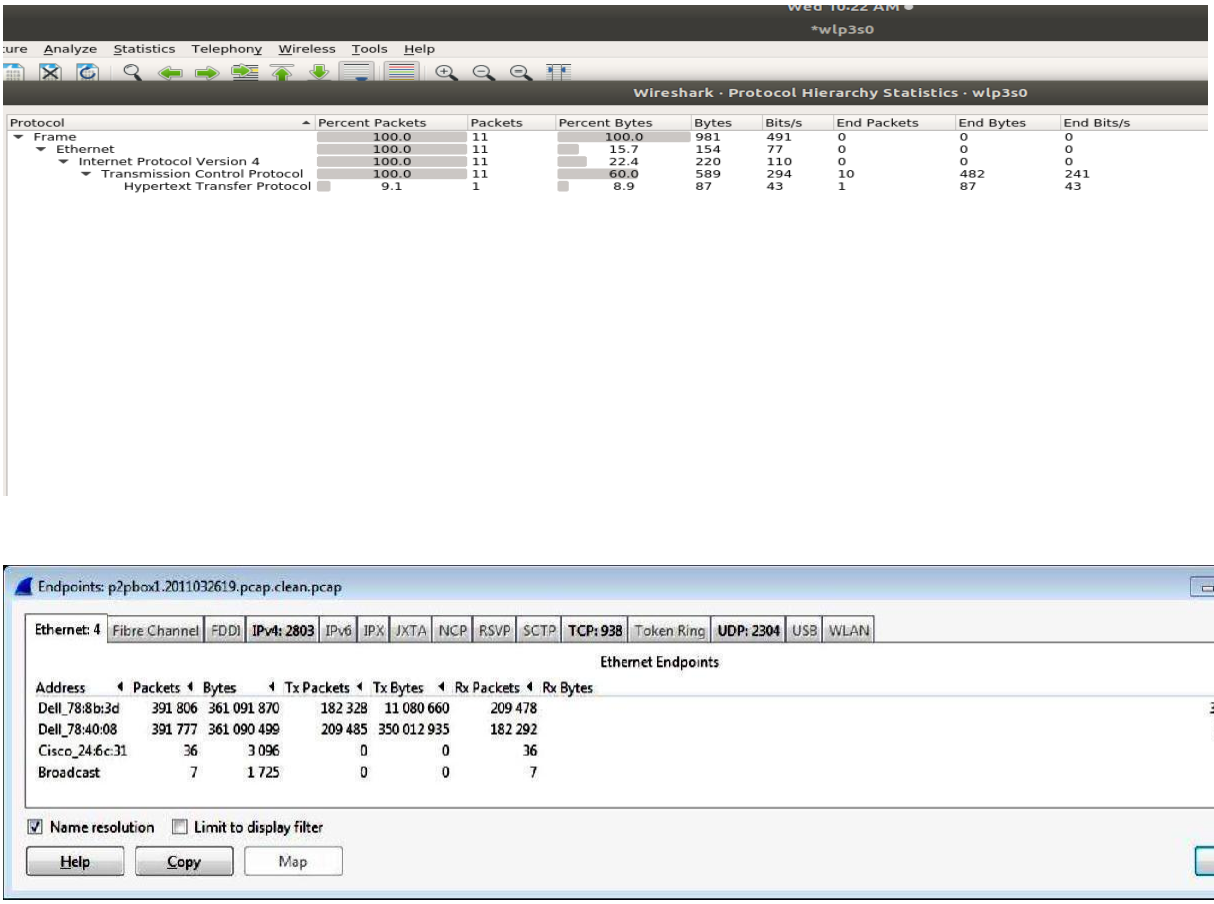

Figure 5 Statistics display in Wireshark

5. Use Wireshark with Mininet

To be able to use Wireshark with Mininet, you can do the following:

- From mininet prompt: mininet> h1 wireshark & #Run the wireshark on host
- From the system terminal: $sudo wireshark &

Now, consider a default Mininet topology with two hosts and a switch and create the following HTTP Traffic:

- To create a http server on the host machine
- mininet> h1 python3 -m http.server 80 &
- To send the http request from the other host machine (client)
- mininet > h2 wget -o - h1
- To shutdown the server
- mininet > h1 kill

6. Lab Exercises

Q1) Create a Mininet topology with 4 hosts (ip range from 10.0.0.1-4) connected to each other with a single switch and filter the ICMP packets transferring from h2 to h4?
Note: Open the terminal (xterm) for each host and ping the machines.

Q2) After filtering the traffic in Q1, add more parameters to the display, and save only those packets in wireshark which you have filtered, in file1.pcap and file1.csv format? Finally, open the file1.pcap and check, what packets are visible?

Q3) Create a mininet topology with 3 hosts machines (one HTTP client H1 and two HTTP server H2 and H3) and three switches in parallel to which all the 3 hosts are connected. Run http servers on H2 and H3, assume H2 and H3 server contains file h1.txt (content: this is h1) and file h2.txt (content: this is h2) and send an http request from H1 to both H2 and H3 to get the files on H1, and analyze the HTTP traffic through Wireshark?

Q4) After filtering the HTTP packets in Q3), filter all the HTTP get request packets, count the request packets, similarly filter the HTTP response packet with status code 200 or 204, identify the difference between request and response packets?