

DATA COMMUNICATION AND COMPUTER NETWORKS LAB

SEMESTER:6TH



LAB REPORT # 3

Submitted By: *Zainab Khalid*
Registration No: *19PWCSE1743*
Section: **A**
Submitted to: *Engr Faiz Ullah*

DEPARTMENT OF COMPUTER SYSTEMS ENGINEERING
UNIVERSITY OF ENGINEERING AND TECHNOLOGY PESHAWAR

Lab 3

INSTALL WIRESHARK

Objectives

Download and Install Wireshark

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC, or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark.

Required Resources

- 1 PC (Windows with internet access)

Instructions

Wireshark has become the industry standard packet-sniffer program used by network engineers. This open-source software is available for many different operating systems, including Windows, Mac, and Linux. In this lab, you will download and install the Wireshark software program on your PC.

Note: Before downloading Wireshark, check with your instructor about the software download policy of your academy.

Step 1: Download Wireshark.

- a. Wireshark can be downloaded from www.wireshark.org.
- b. Choose the software version you need based on your PC's architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.

After making a selection, the download should start. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

Step 2: Install Wireshark.

- a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number if you downloaded the 64bit version. Double-click the file to start the installation process.

Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.

- b. If this is your first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.
- c. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.
- d. Keep the default settings on the Choose Components window and click **Next**.
- e. Choose your desired shortcut options and click **Next**.
- f. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location. Click **Next** to continue.
- g. To capture live network data, Npcap must be installed on your PC. If Npcap is already installed on your PC, the Install check box will be unchecked. If your installed version of Npcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install Npcap x.x.x** (version number) check box. Click **Next** to continue.
- h. **Do NOT** install USBPcap for normal traffic capture. **Do NOT select the checkbox to install USBPcap**. USBPcap is experimental, and it could cause USB problems on your PC. Click **Install** to continue.
- i. Wireshark starts installing its files and displays with the status of the installation.
- j. In a separate window, accept the license agreement in the Npcap Setup Wizard if installing Npcap. Click **I Agree** to continue. Click **Install** to install Npcap. Click **Next** to finish the Npcap installation and click **Finish** to exit the Npcap installation.
- k. Click **Next** when the Wireshark installation is complete.
- l. Click **Finish** to complete the Wireshark install process. Reboot the computer if necessary.

Introduction to Wireshark:

Wireshark is an open-source project whose primary purpose is to develop a standard analysis tool for network protocols. It's a network packet analyzer that captures data on a network then presents it in a human-understandable form.

Lab - Install Wireshark

Operations Performed:

This tool performs various operations such as:

- *Troubleshooting networks.*
- *Performing security operations used to detect security threats such as port scanning on a network.*
- *Learning more about network protocols at the microscopic level.*
- *Performing analysis of voice over the internet (VoIP).*

Working of Wireshark:

Wireshark is, like we said, a packet analyzer or a packet sniffer. Wireshark captures network traffic (the data moving currently on your network) and records the movement of data offline. To analyze the network activities, you can then use this data.

Wireshark Graphical User Interface:

Wireshark contains some commonly used menus:

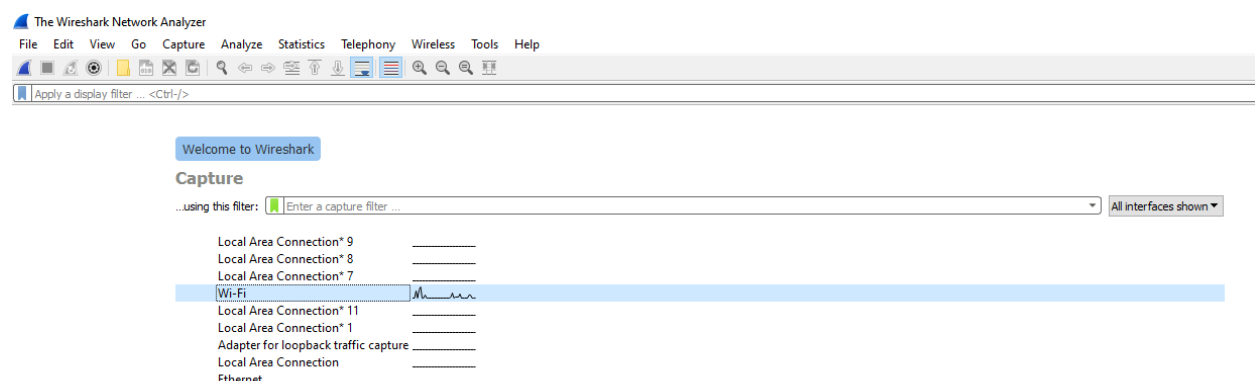
File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help.

Some useful icons are:

- **Start Capturing Packets icon**
- **Stop Capturing Packets icon**
- **Restart Current Capture Icon**

The Capturing of Traffic:

Wireshark lists the available interfaces with which it can capture network packets. I'm using my wireless interface (a.k.a WiFi) to contact the outside world.



Select the interface (in this case, wireless), click the shark tail icon to start to capture packets.



Lab - Install Wireshark

Once we have captured some packets, we can analyze the results. Let's get into the information we captured. The logs captured can be very large, but there is an option to filter out useful information.

Some of the most widely-used filters are:

ip.addr == x.x.x.x

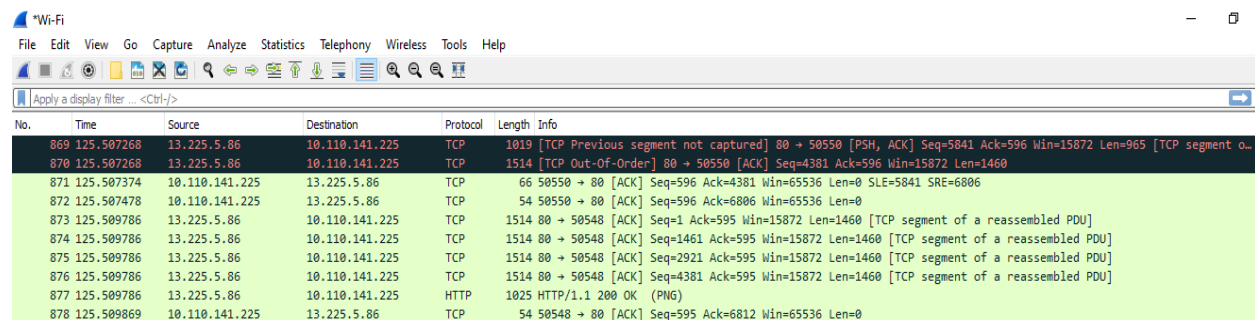
To know what information is getting requested from your system, this filter can be used.

http or dns/dhcp

Now, in this case, a request is issued to Youtube.com.

Panels in Wireshark:

1. Packet List Panel:



The screenshot shows the Wireshark interface with the Packet List Panel. The panel displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are listed in sequential order, with each line representing a captured packet. The first packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 869, length 1019. The second packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 870, length 1514. The third packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 871, length 66. The fourth packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 872, length 54. The fifth packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 873, length 1514. The sixth packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 874, length 1514. The seventh packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 875, length 1514. The eighth packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 876, length 1514. The ninth packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 877, length 1025. The tenth packet is a TCP segment from 10.110.141.225 to 10.110.141.225, sequence number 878, length 54.

No.	Time	Source	Destination	Protocol	Length	Info
869	125.507268	13.225.5.86	10.110.141.225	TCP	1019	[TCP Previous segment not captured] 80 → 50550 [PSH, ACK] Seq=5841 Ack=596 Win=15872 Len=965 [TCP segment o...
870	125.507268	13.225.5.86	10.110.141.225	TCP	1514	[TCP Out-Of-Order] 80 → 50550 [ACK] Seq=4381 Ack=596 Win=15872 Len=1460
871	125.507374	10.110.141.225	13.225.5.86	TCP	66	50550 → 80 [ACK] Seq=596 Ack=4381 Win=65536 Len=0 SLE=5841 SRE=6806
872	125.507478	10.110.141.225	13.225.5.86	TCP	54	50550 → 80 [ACK] Seq=596 Ack=6806 Win=65536 Len=0
873	125.509786	13.225.5.86	10.110.141.225	TCP	1514	80 → 50548 [ACK] Seq=1 Ack=595 Win=15872 Len=1460 [TCP segment of a reassembled PDU]
874	125.509786	13.225.5.86	10.110.141.225	TCP	1514	80 → 50548 [ACK] Seq=1461 Ack=595 Win=15872 Len=1460 [TCP segment of a reassembled PDU]
875	125.509786	13.225.5.86	10.110.141.225	TCP	1514	80 → 50548 [ACK] Seq=2921 Ack=595 Win=15872 Len=1460 [TCP segment of a reassembled PDU]
876	125.509786	13.225.5.86	10.110.141.225	TCP	1514	80 → 50548 [ACK] Seq=4381 Ack=595 Win=15872 Len=1460 [TCP segment of a reassembled PDU]
877	125.509786	13.225.5.86	10.110.141.225	HTTP	1025	HTTP/1.1 200 OK (PNG)
878	125.509869	10.110.141.225	13.225.5.86	TCP	54	50548 → 80 [ACK] Seq=595 Ack=6812 Win=65536 Len=0

In the capture panel above, the network packet capturing is in sequential order, with each line representing each packet captured.

The details, with rows and columns, are displayed in tabular form. Each row represents the collected packet, while additional information such as time, protocols, duration, et cetera is given in columns.

Columns and Information:

No - Represents a specific sequence number of the network packet. To classify a given packet, one can use this.

Time - This is the time that a specific packet has been recorded.

Source - This represents where we are getting the packets from. This is denoted as Internet Protocols (IP Addresses).

Destination - This is used to represent the Internet Protocol (IP Address) where the packet is going.

Protocol - This refers to the protocol of the data you have captured. This could be TCP, ARP et cetera

Length - This is used to represent the size of the packet captured.

Lab - Install Wireshark

Info - This gives you additional information about the packet you have captured.

Each protocol is represented with its color scheme. For example, the TCP protocol has a #cccccc background. This helps the user to differentiate between these protocols easily.

2. Packet Details Panel:

After capturing some data, click on a single row, some data will be displayed on the immediate window.

```
> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{3C888F26-0CA1-42B7-946F-FD204CFD232C}, id 0
> Ethernet II, Src: IntelCor_12:6a:a1 (cc:2f:71:12:6a:a1), Dst: Cisco_e4:f6:d0 (7c:ad:74:e4:f6:d0)
> Internet Protocol Version 4, Src: 10.110.141.225, Dst: 192.168.100.247
> User Datagram Protocol, Src Port: 56284, Dst Port: 53
> Domain Name System (query)
```

3. Packet Byte Panel:

Remember when you clicked a given row from the packet details above, you could get details on the window.

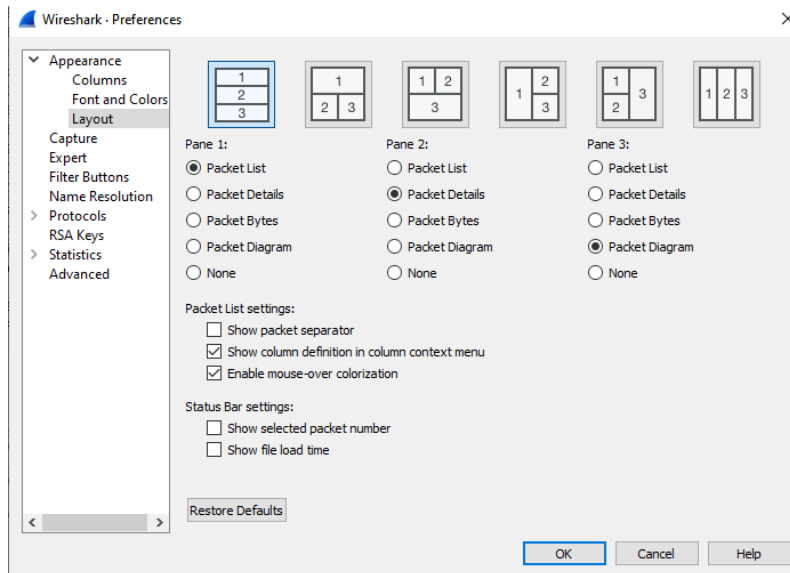
0000	7c ad 74 e4 f6 d0 cc 2f 71 12 6a a1 08 00 45 00	.t.... / q.j...E.
0010	00 44 17 2e 00 00 40 11 a5 8c 0a 6e 8d e1 c0 a8	.D...@. ...n....
0020	64 f7 db dc 00 35 00 30 5b 2e 00 12 01 00 00 01	d....5.0 [.
0030	00 00 00 00 00 00 04 73 70 65 63 05 63 6c 6f 75s pec·clou
0040	64 07 33 36 30 73 61 66 65 03 63 6f 6d 00 00 01	d·360saf e·com·..
0050	00 01	..

This is the exact format of the data dump when the packet is captured.

In this panel, we can also display packet diagram.

- In the men bar, go to **edit=> preferences =>appearance=>layout=>pane 3**.
- Click on the **Packet Diagram** option.

Lab - Install Wireshark



Packet Diagram:

