Experiment No 5

Aim: Use Wire shark to understand the operation of TCP/IP layers

Theory:

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems. Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

The following are some of the many features Wireshark provides:

▪Available for UNIX and Windows.

▪Capture live packet data from a network interface.

▪Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.

▪Import packets from text files containing hex dumps of packet data.

▪Display packets with very detailed protocol information.

▪Save packet data captured.

▪Export some or all packets in a number of capture file formats.

▪Filter packets on many criteria.

▪Search for packets on many criteria.

▪Colorize packet display based on filters.

▪Create various statistics.

Procedure:

1.Download Wireshark tool
sudo apt install wireshark

2.Install with default settings

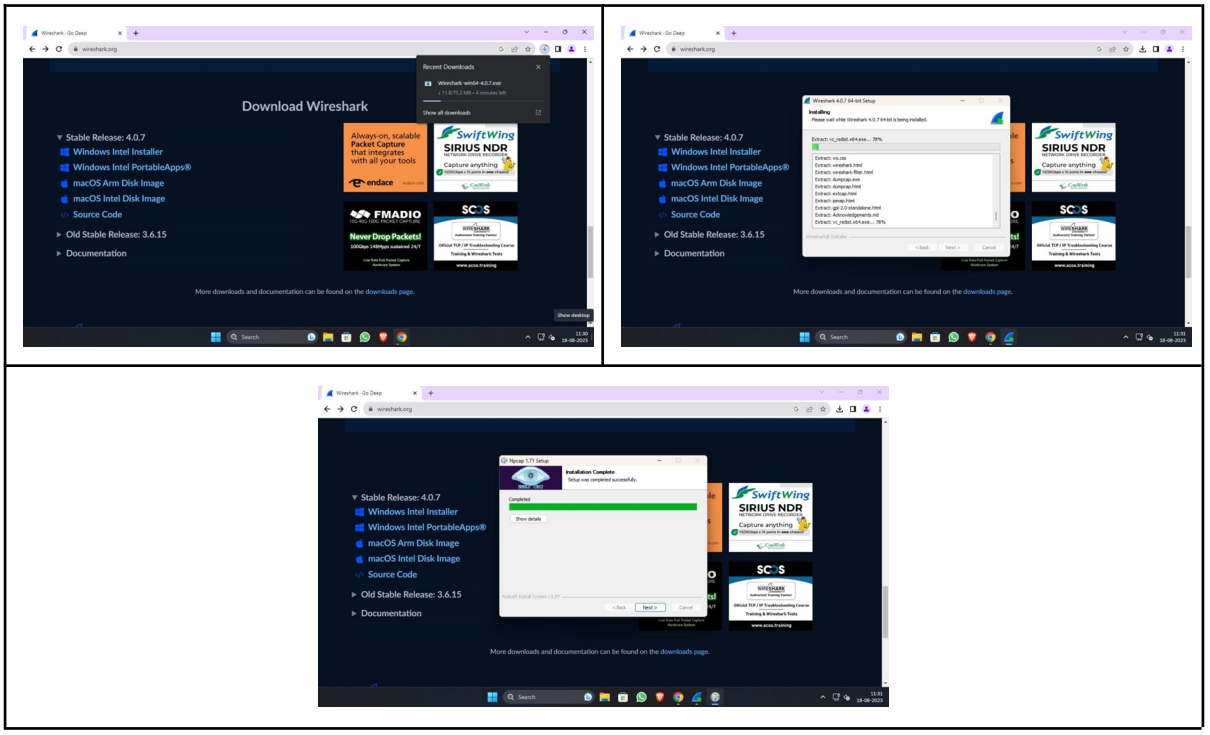
3.After opening wireshark select either wifi or ethernet based on your connect

4.Check dns

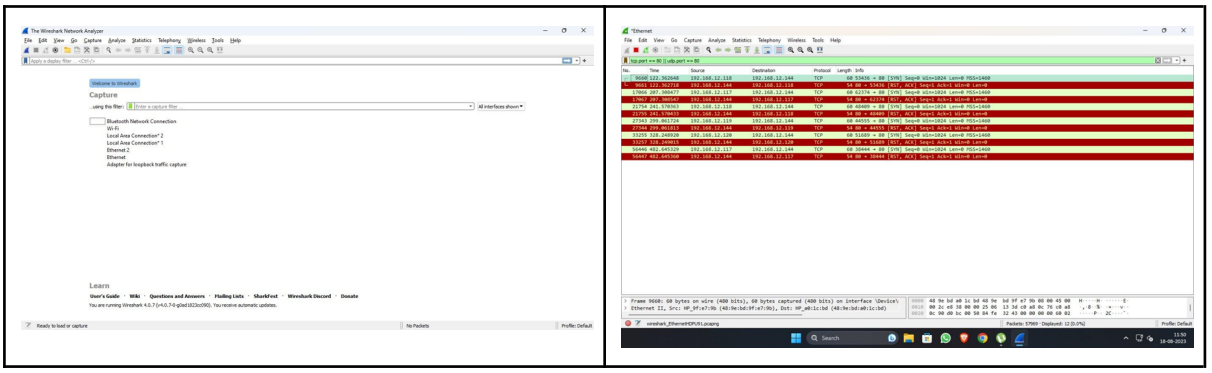
5.Apply udp/ tdp filter also

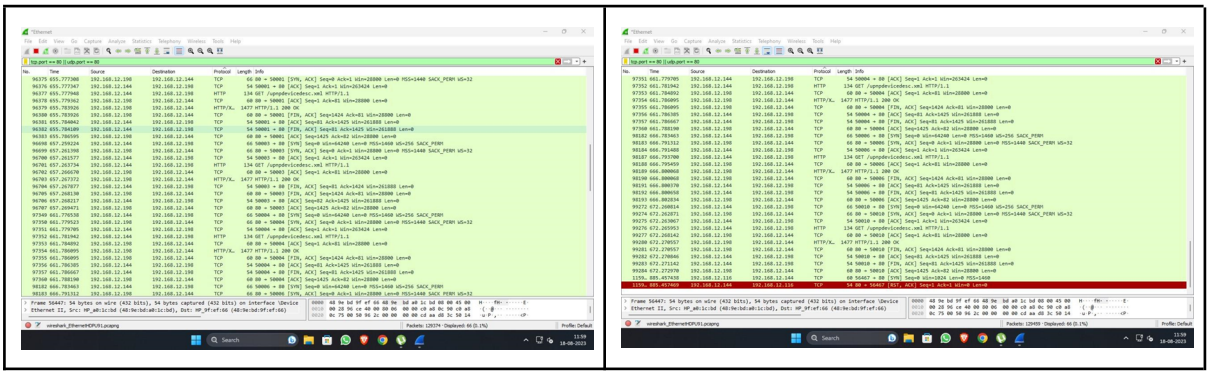
Output:

Wire shark installation:



Implementation:





Conclusion:

In this experiment, we utilized Wireshark to gain insights into the functioning of the TCP/IP protocol suite. By capturing and analyzing network traffic, we observed the establishment of a TCP connection, data transfer, and the role of the TCP header in controlling data flow.

Key conclusions include Wireshark's ability to analyze traffic across all TCP/IP layers, its usefulness in understanding various protocols (TCP, UDP, ICMP), and its applications in network monitoring, troubleshooting, and security investigation.

Advantages of using Wireshark:

1. Free software
2. Available for multiple platforms – Windows & UNIX
3. Can see detailed information about packets within a network
4. Not proprietary can be used on multiple vendors unlike Cisco Prime

Applications of Wireshark:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch,

routers, etc., communicate in a local network or the rest of the world.

- Similar tools like Wireshark:

1. Tcpdump
2. EtherApe
3. Capsa
4. Paessler PRTG
5. Effectech