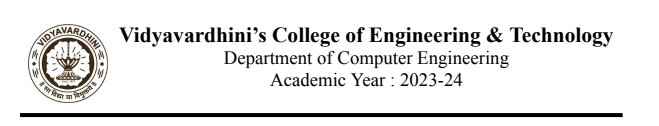
****

**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

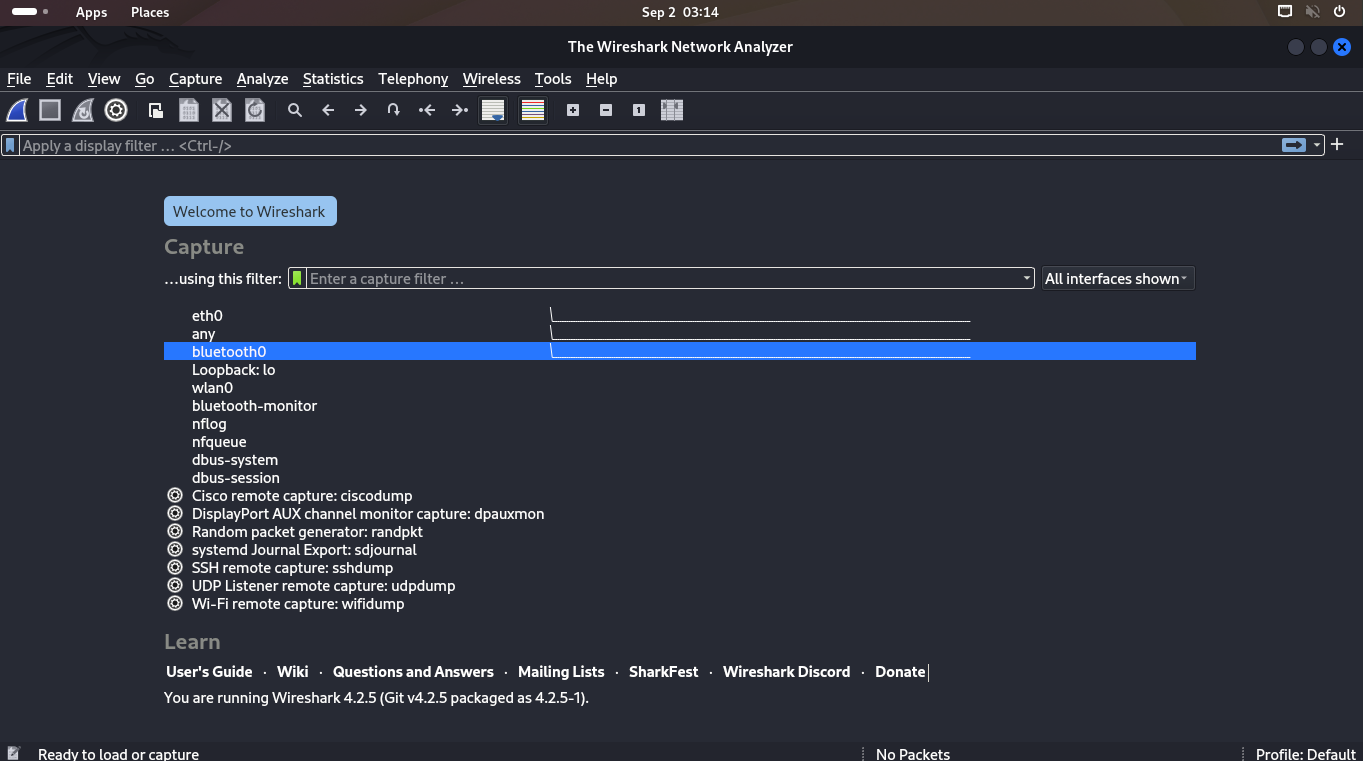
2.Install with default settings

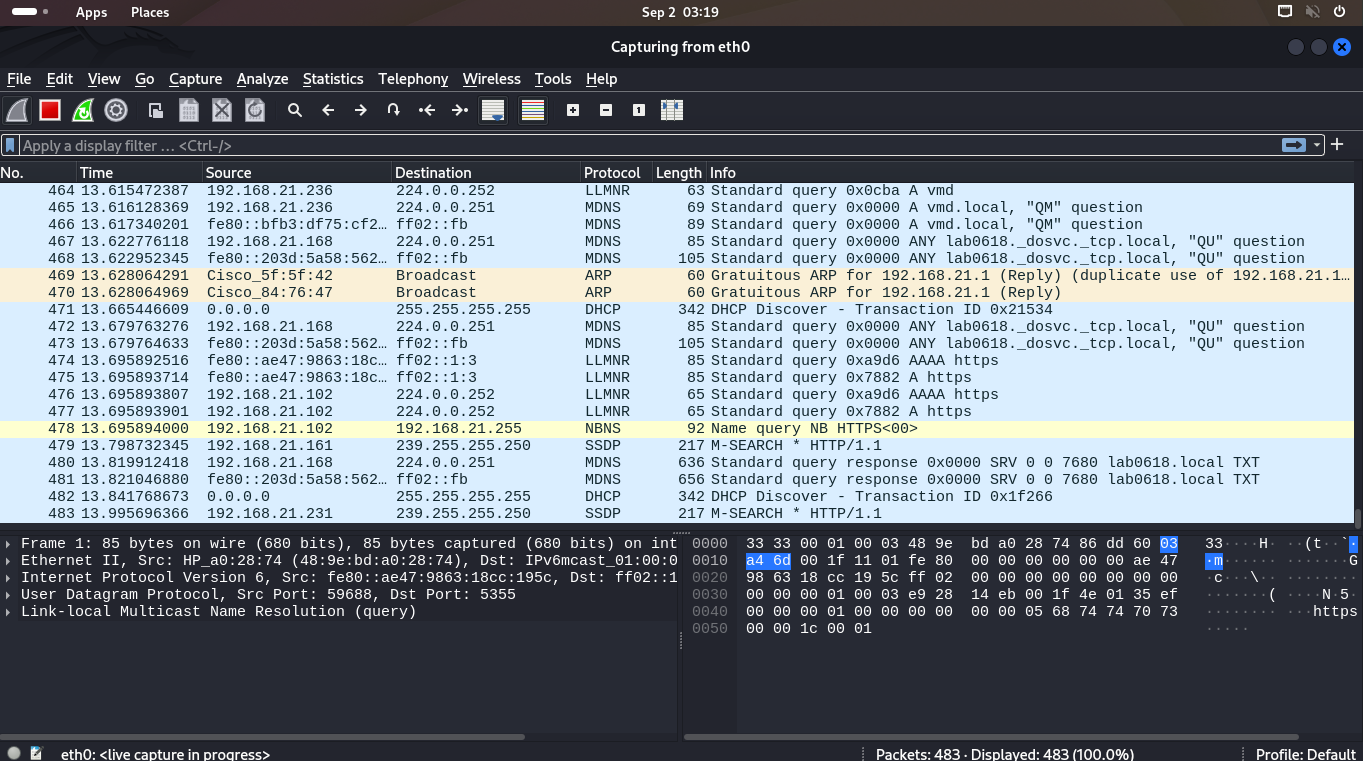
3.After opening wireshark select either wifi or ethernet based on your connect

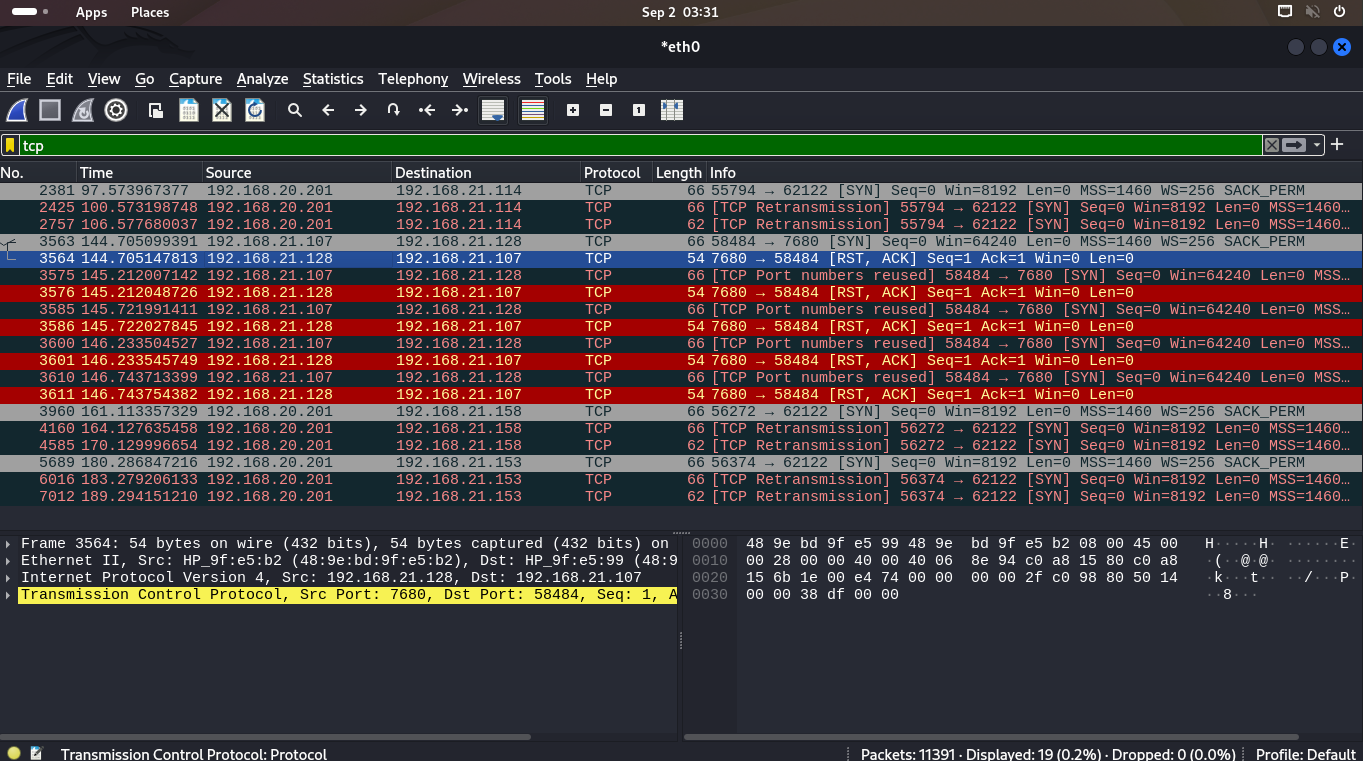
4.Check dns

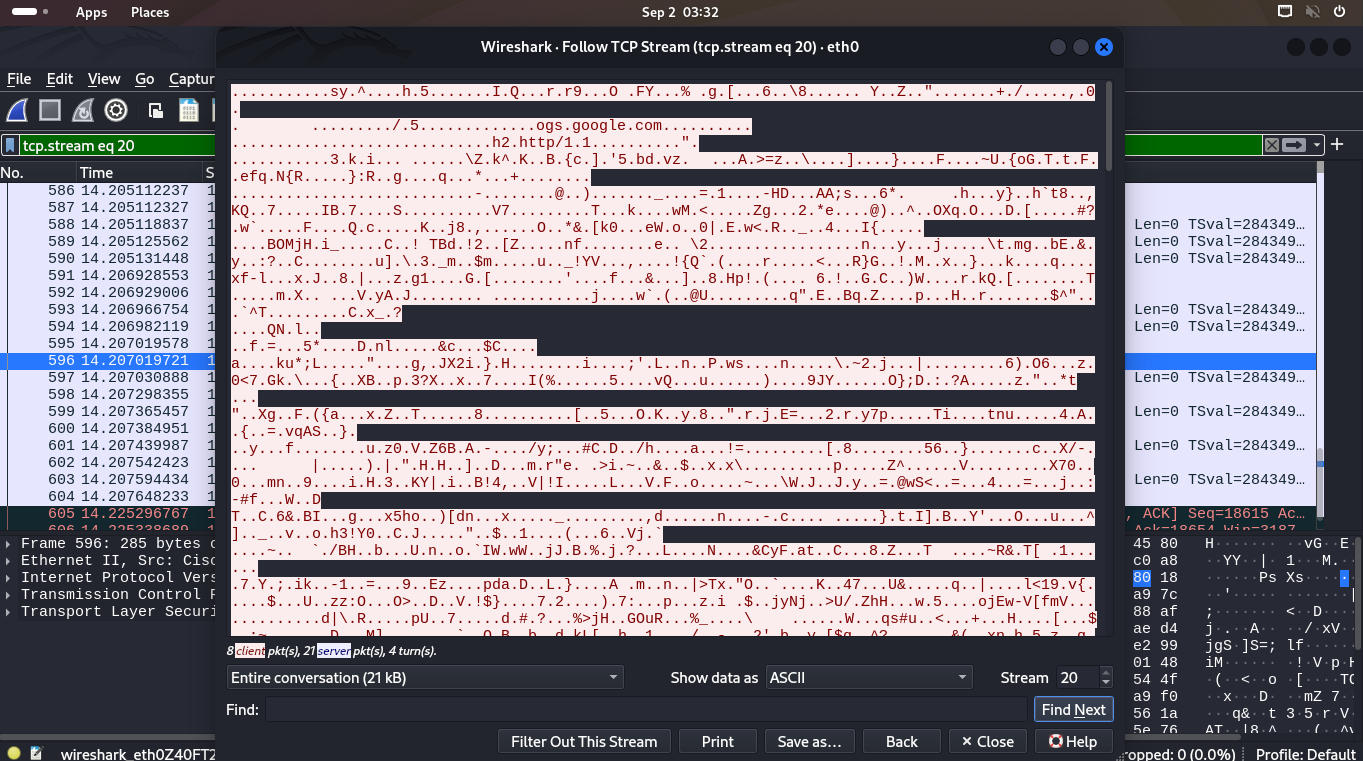
5.Apply udp/ tdp filter also

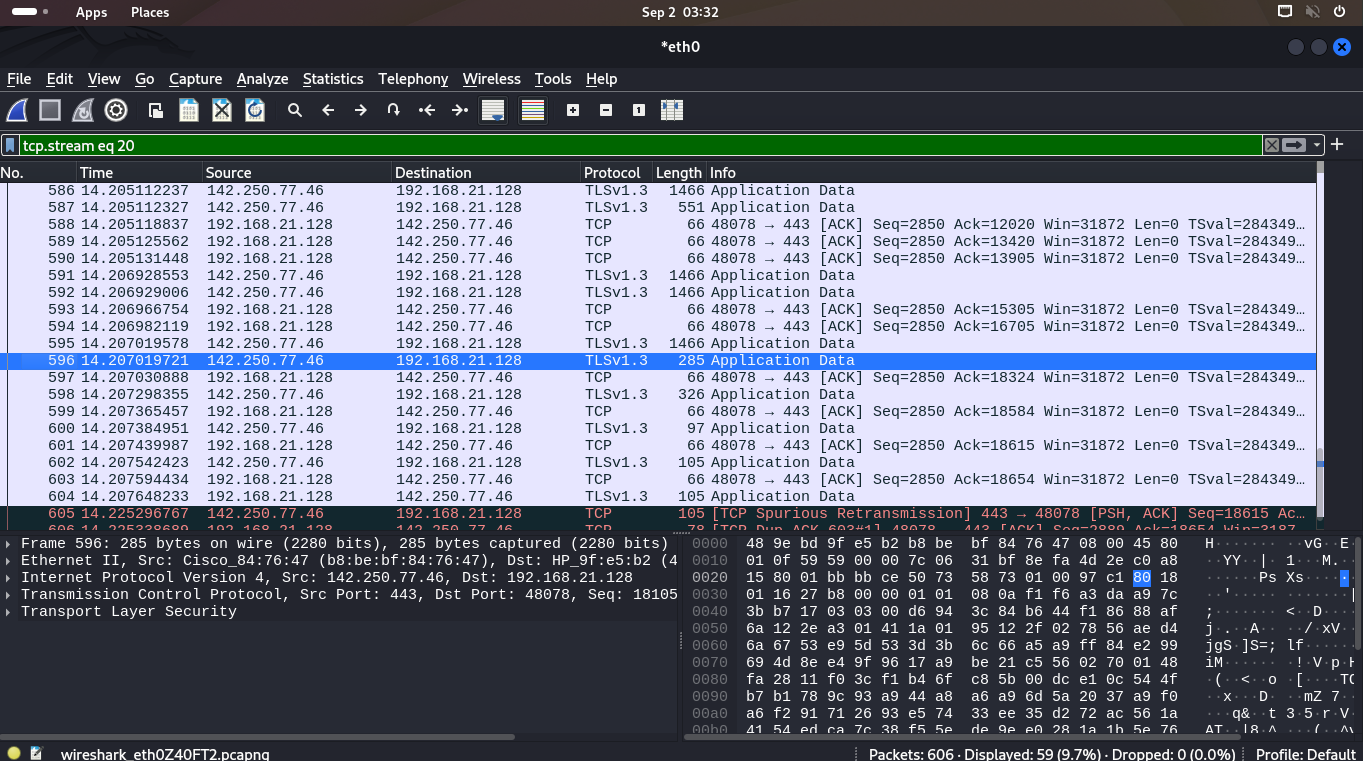
**Output:**











**Conclusion:** We have successfullyuse Wire shark to understand the operation of TCP/IP layers