Experiment 9

Date of Performance : 17-04-2023 **Date of Submission : 07-05-2023**

SAP Id: 60004200107 **Name :** Kartik Jolapara

Div: B **Batch :** B1

Aim of Experiment

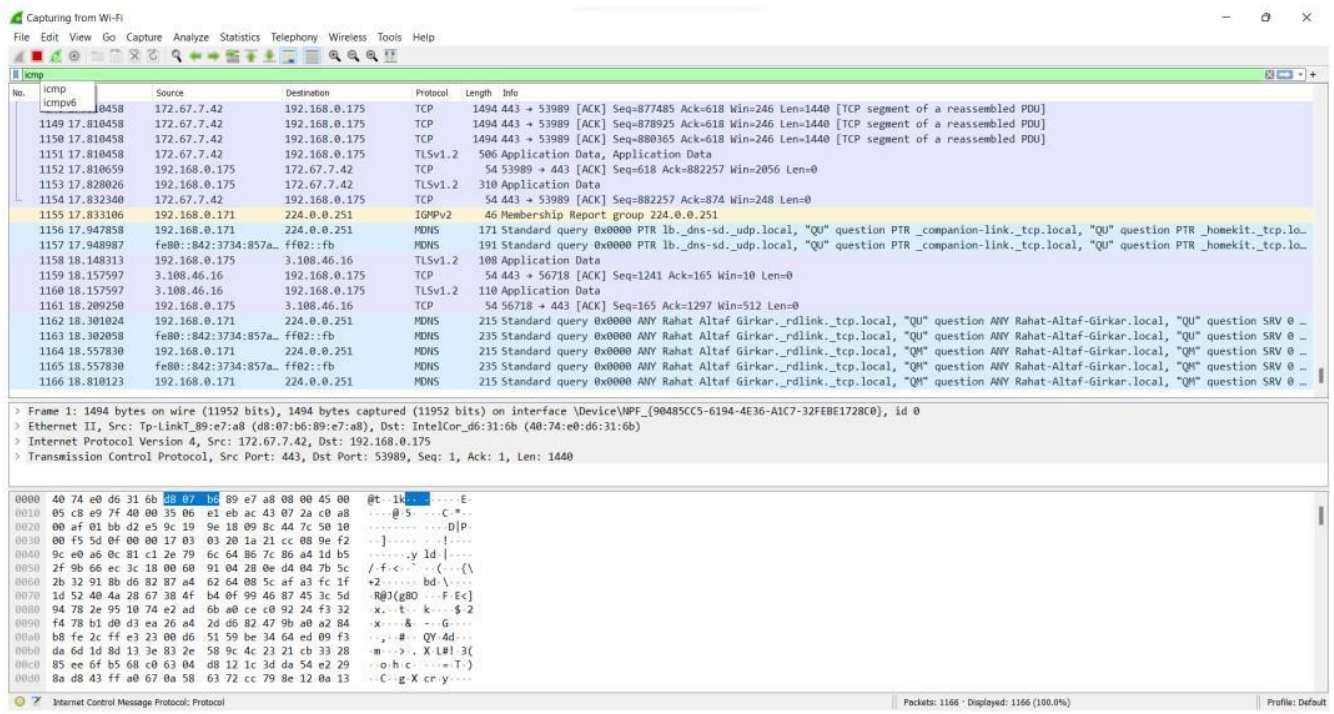
Study of packet sniffer tools: WireShark Download and install wireshark and captue icmp, tcp and http packets in promiscuous mode Explore how the packets can be traced based on different filters.

Theory / Algorithm / Conceptual Description

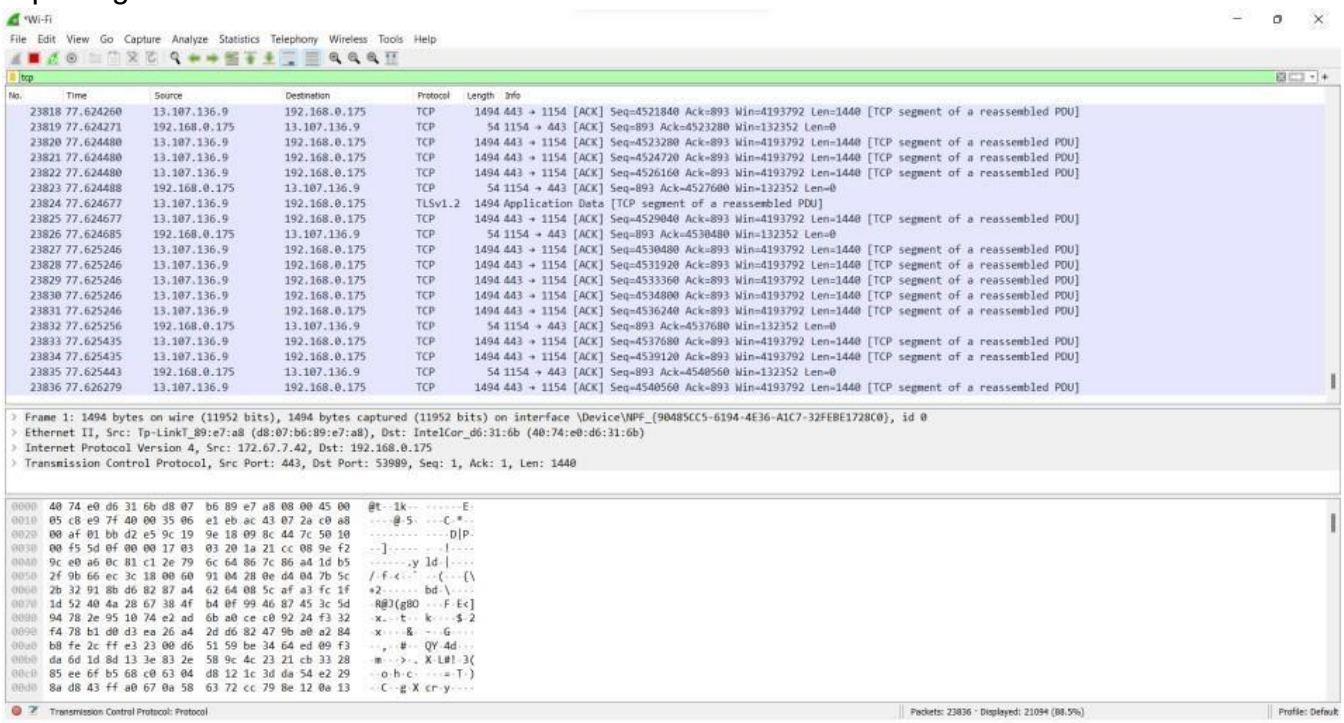
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

Capturing ICMP Packets:

C:\Users\Marwin Shroff>ping 8.8.8.8 Pinging
8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
Reply from 8.8.8.8: bytes=32 time=6ms TTL=119
Reply from 8.8.8.8: bytes=32 time=2ms TTL=119
Reply from 8.8.8.8: bytes=32 time=3ms TTL=119 Ping
statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 6ms, Average = 4ms



Capturing TCP Packets:



Capturing FTP Packets:

C:\Users\Marwin Shroff>ftp ftp.cdc.gov Connected to ftp.cdc.gov.

220 Microsoft FTP Service

200 OPTS UTF8 command successful - UTF8 encoding now ON.

User (ftp.cdc.gov:(none)): anonymous

331 Anonymous access allowed, send identity (e-mail name) as password.

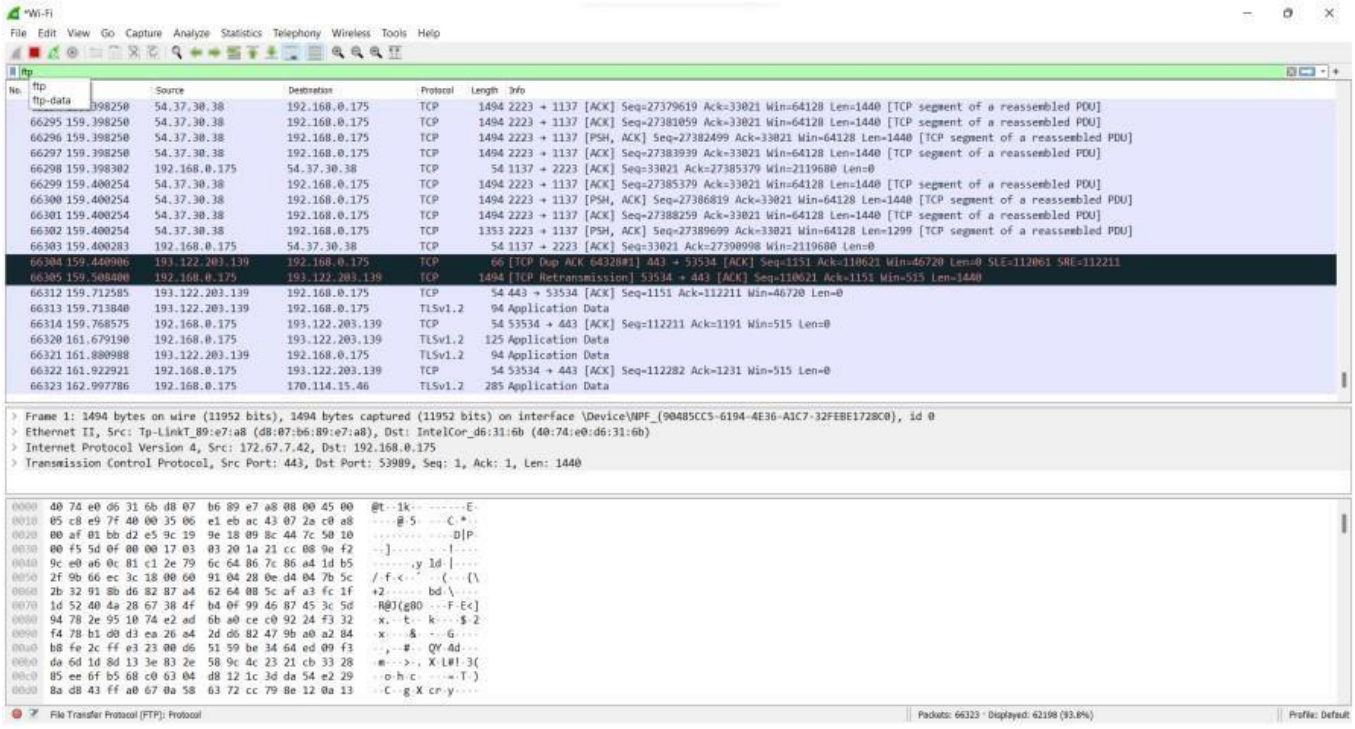
Password: 230 User
logged in.

ftp> ls

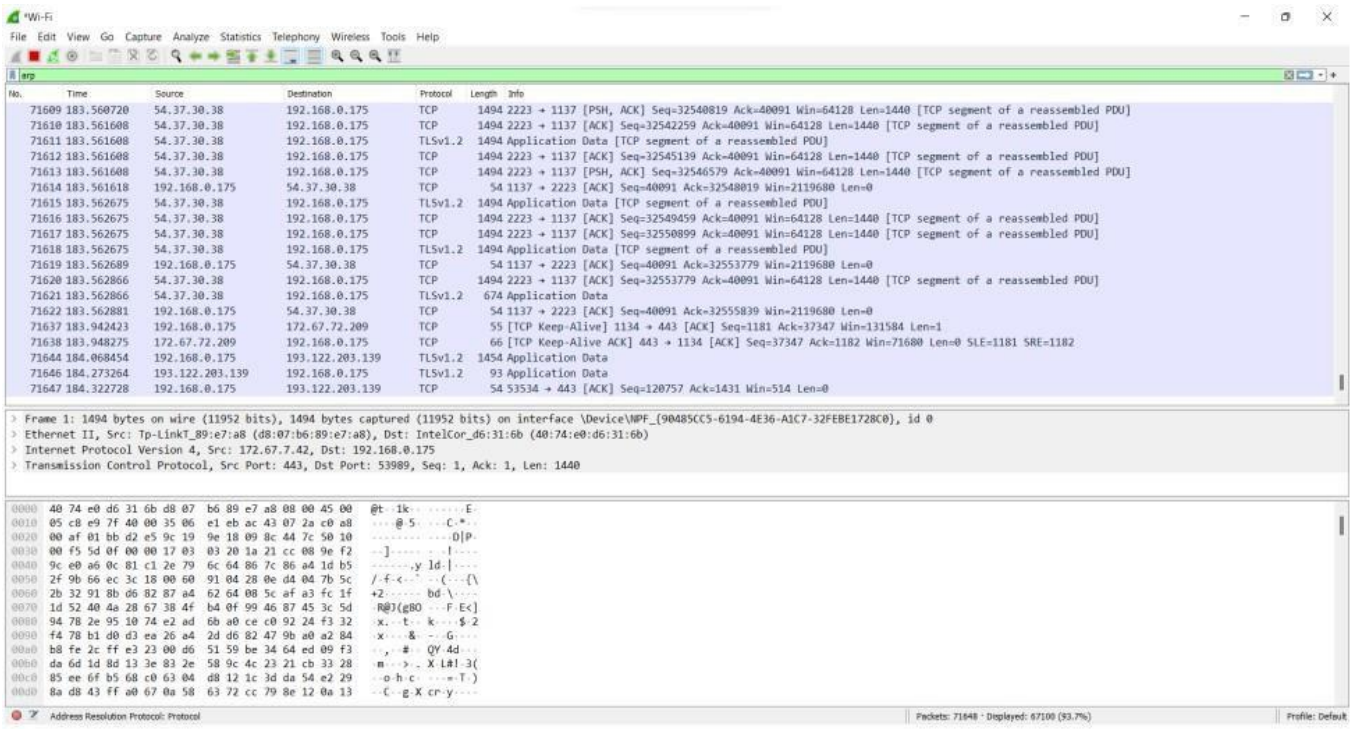
200 PORT command successful.

150 Opening ASCII mode data connection.

.change.dir
.message
pub Readme
Siteinfo w3c welcome.msg 226 Transfer
complete. ftp: 67
bytes received in 0.03Seconds 2.03Kbytes/sec.



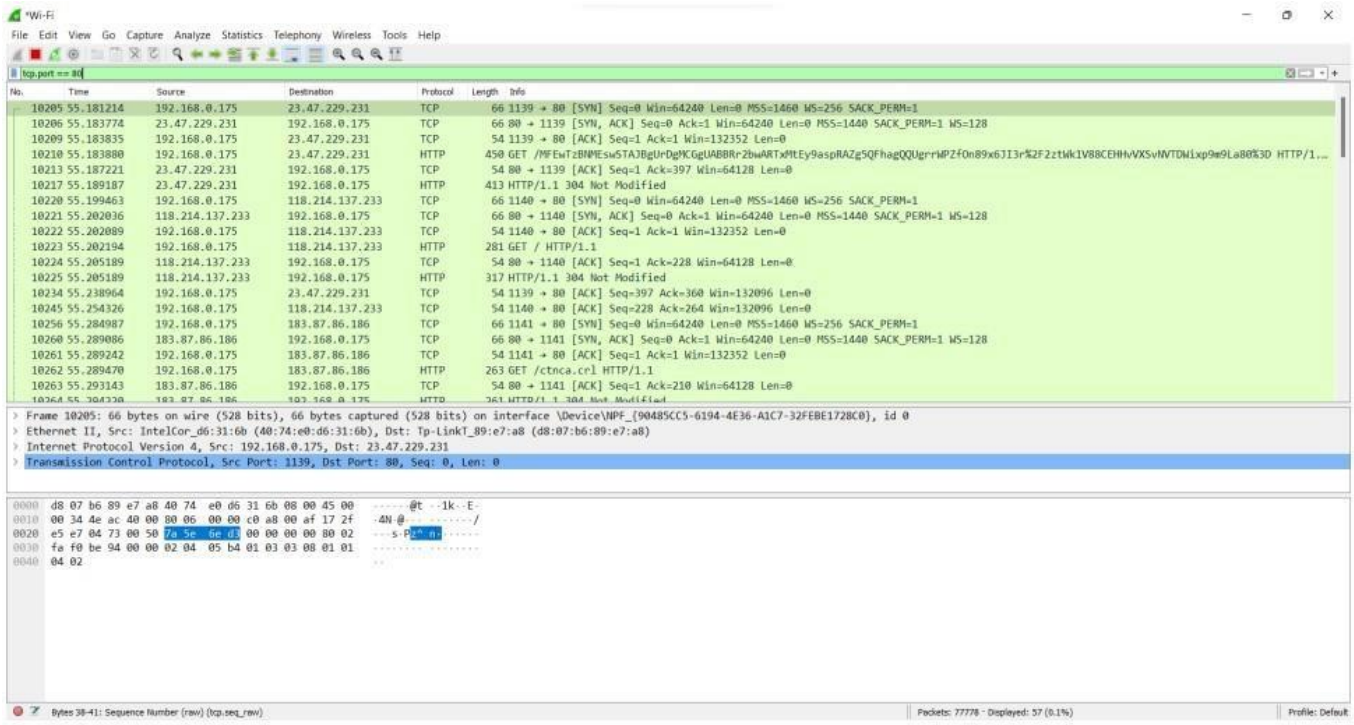
Capturing ARP Packets:



B] Tracing Packets based on filters:

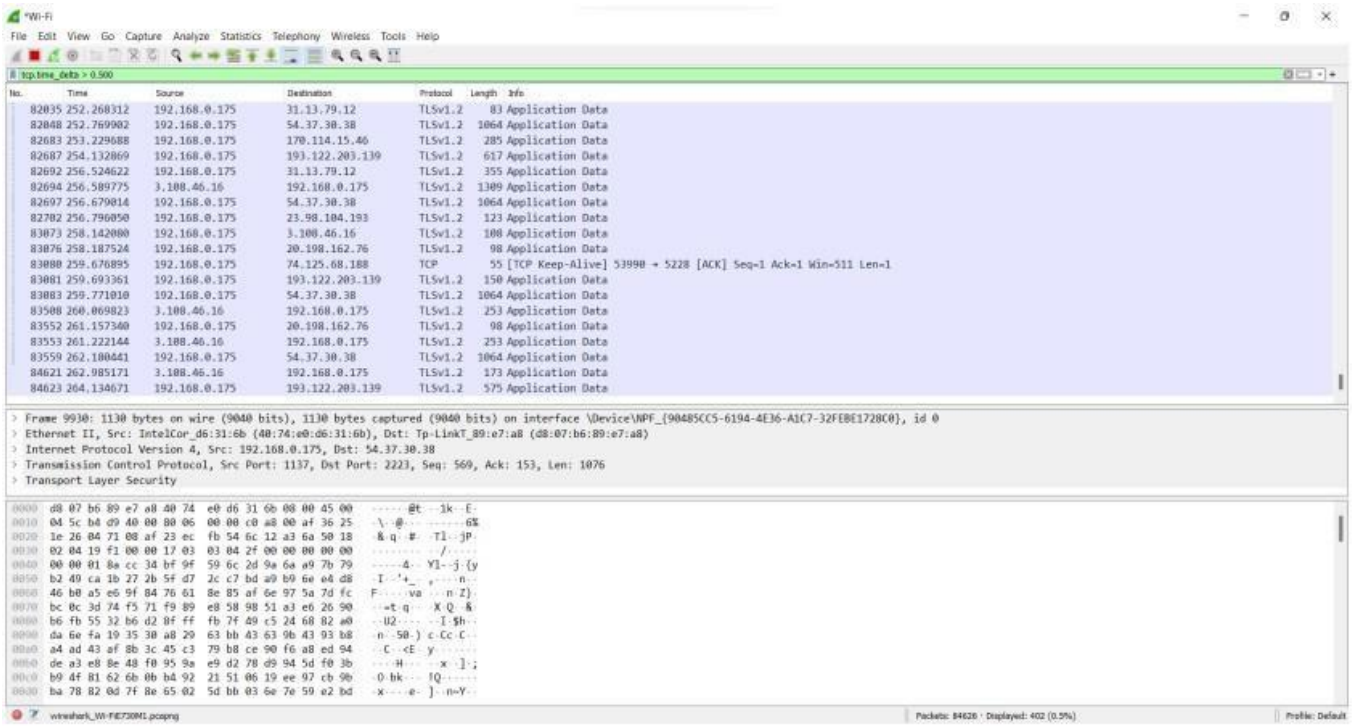
1] Filter Results by Port:

Traces all packets related to Port 80.



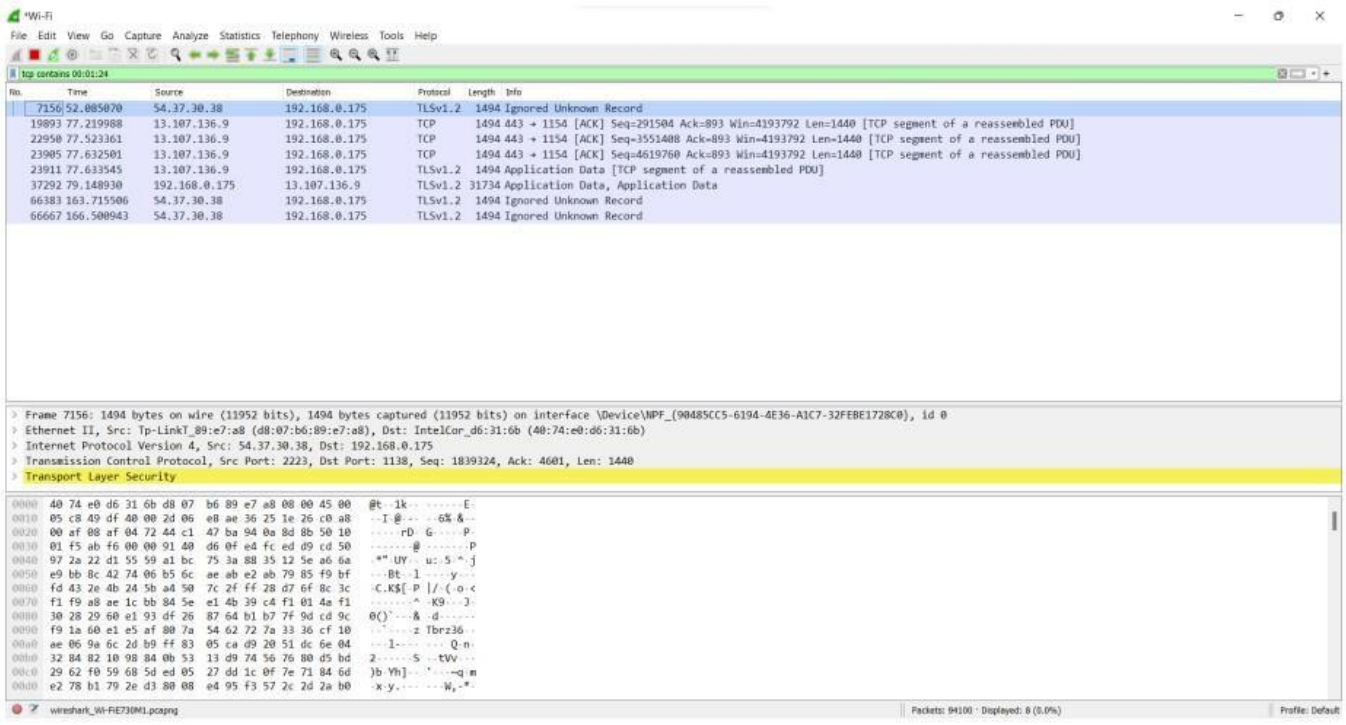
2] Filter by Delta Time :

Displays tcp packets with delta time of greater than 0.500 sec



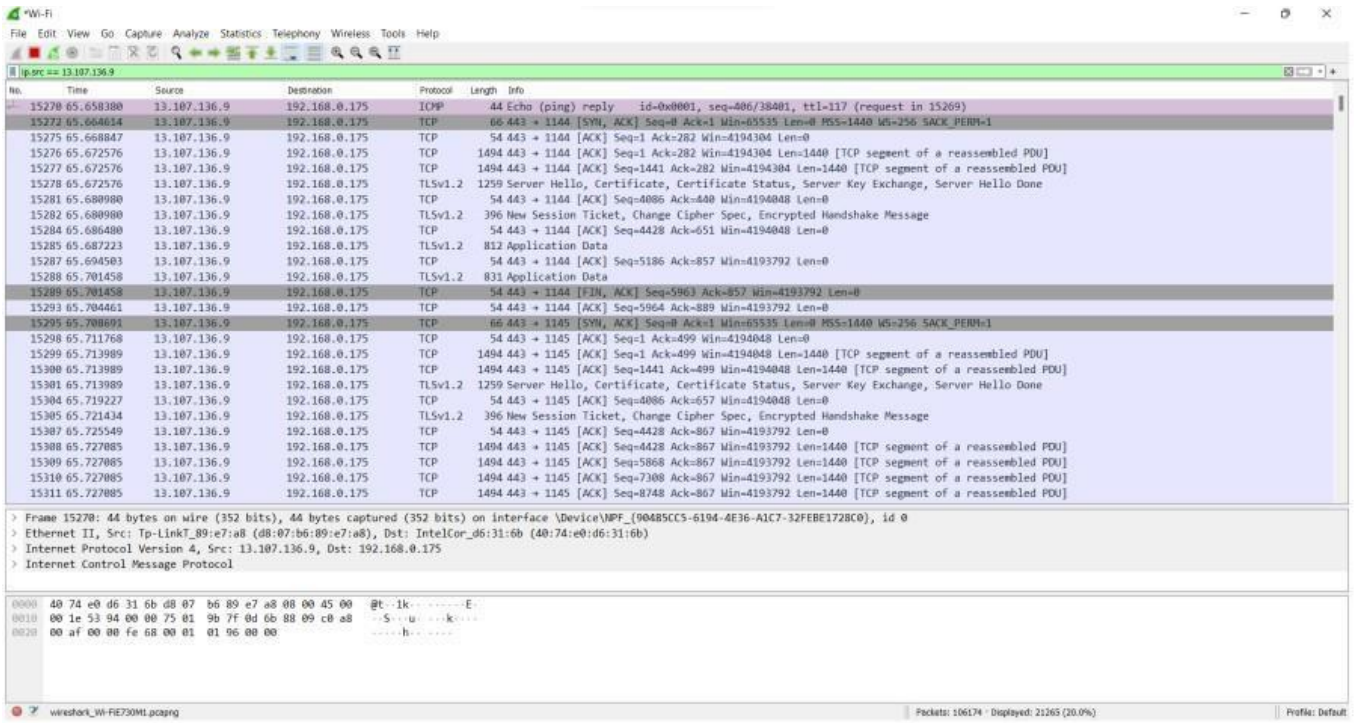
3] Filter by Byte Sequence:

Displays packets which contain a particular byte sequence.



4] Filter by Source IP Address:

Displays packets which have source IP address same as the one provided in the argument.



CONCLUSION

Thus, we have successfully studied packet sniffing tools (wireshark) and explored how packets can be traced on the basis of different filters.