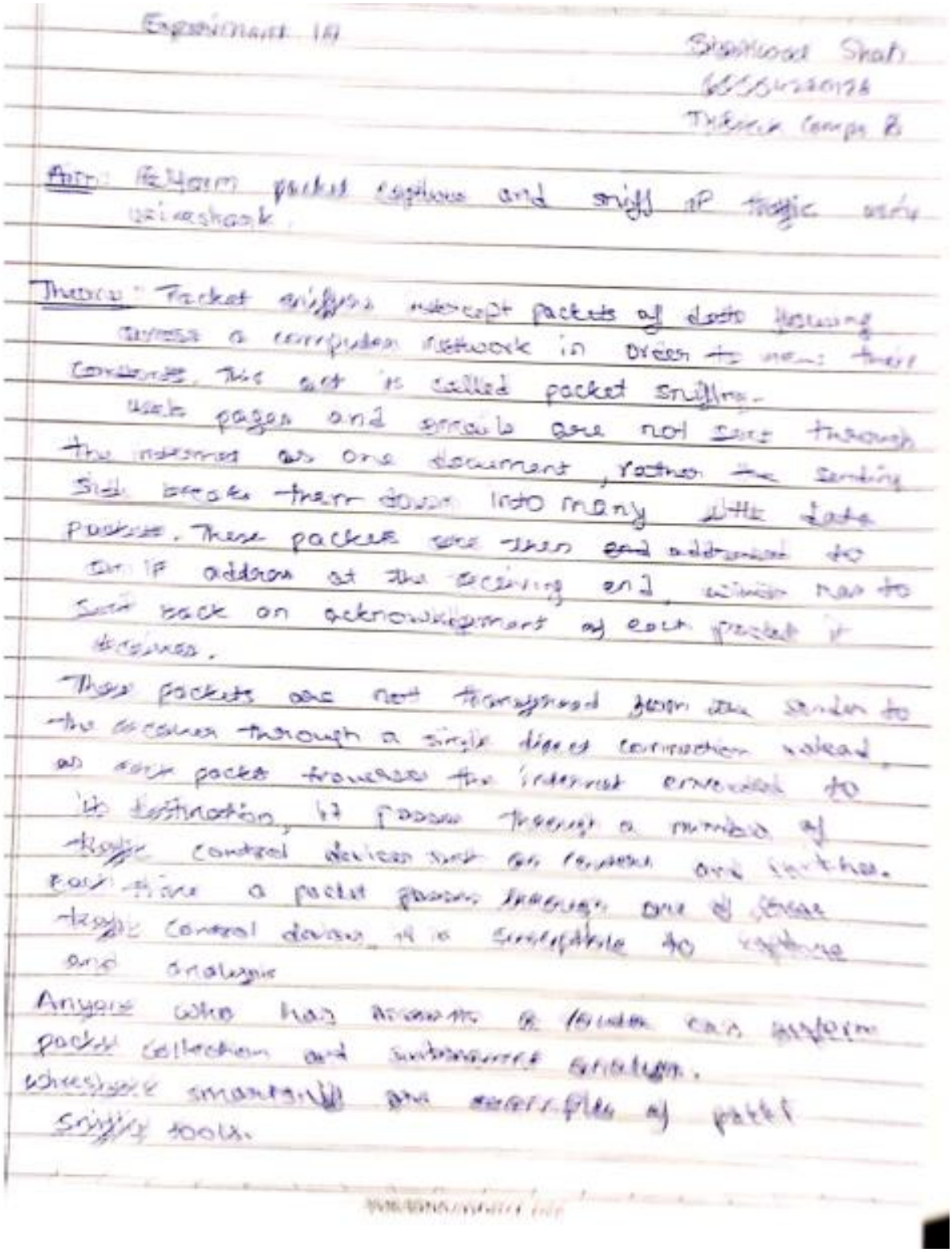
AIM:Perform Packet Capture and Sniff IP traffic using Wireshark.



Experiment 10

Siddhesh Shah
60553220026
TY Comps B

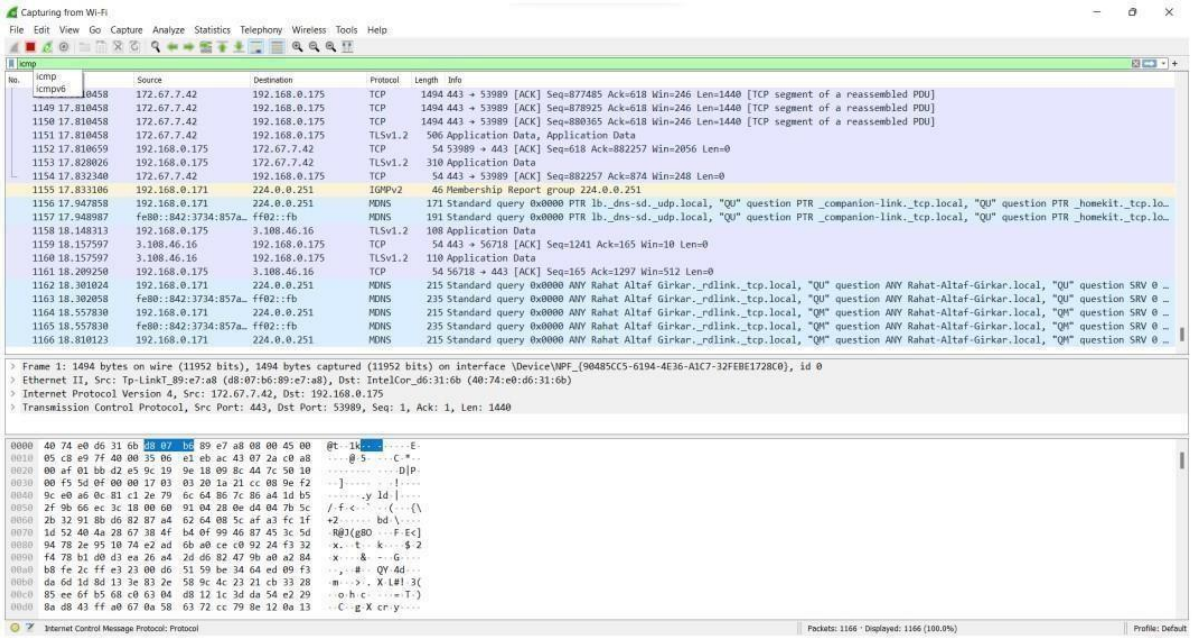
Aim: To perform packet capture and sniff IP traffic using Wireshark

Theory: Packet sniffers intercept packets of data flowing across a computer network in order to read their contents. This act is called packet sniffing.
Web pages and emails are not sent through the internet as one document, rather the sending side breaks them down into many little data packets. These packets are then addressed to an IP address at the receiving end, which has to send back an acknowledgement of each packet it receives.
These packets are not transmitted from the sender to the receiver through a single direct connection instead, as each packet traverses the internet enroute to its destination, it passes through a number of network control devices such as routers and switches. Each time a packet passes through one of these network control devices, it is susceptible to capture and analysis.
Anyone who has access to a network can perform packet collection and subsequent analysis. Wireshark, among other packet sniffing tools.

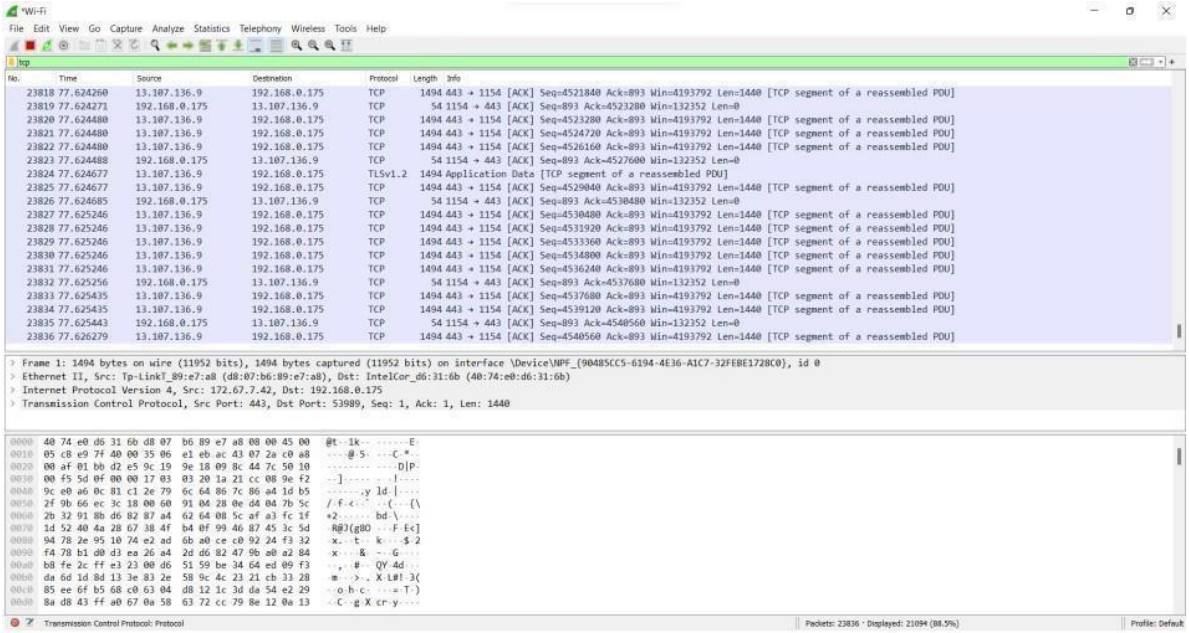
Conclusion: Thus, we have performed packet capture and sniffed IP traffic using wireshark.

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

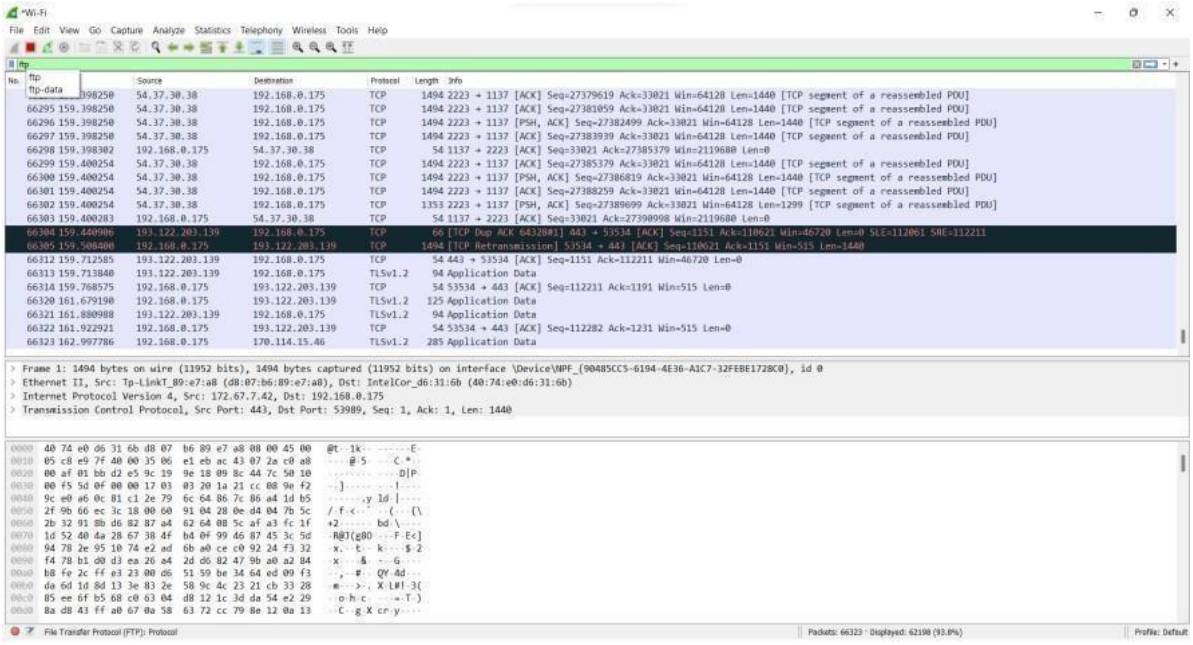


Capturing TCP Packets:

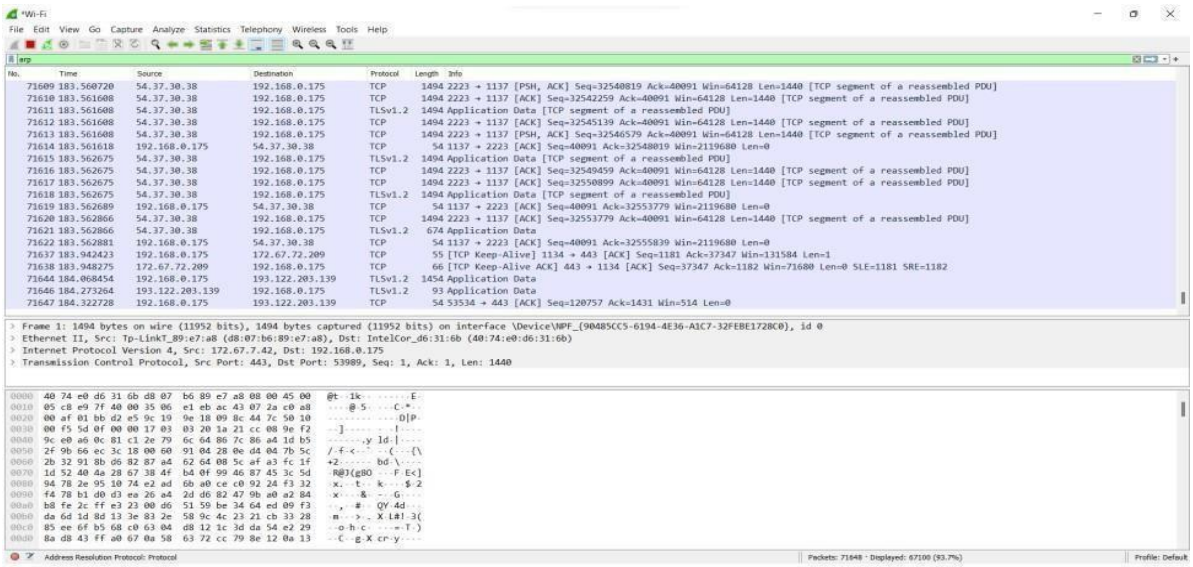


Capturing FTP Packets:

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.



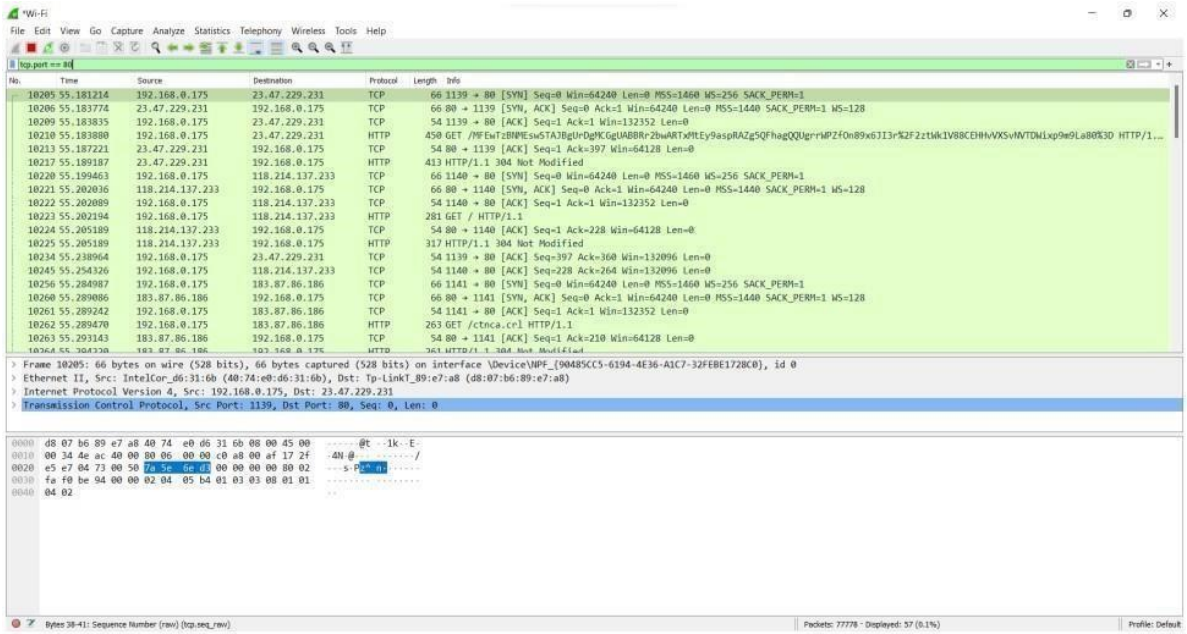
Capturing ARP Packets:



B] Tracing Packets based on filters:

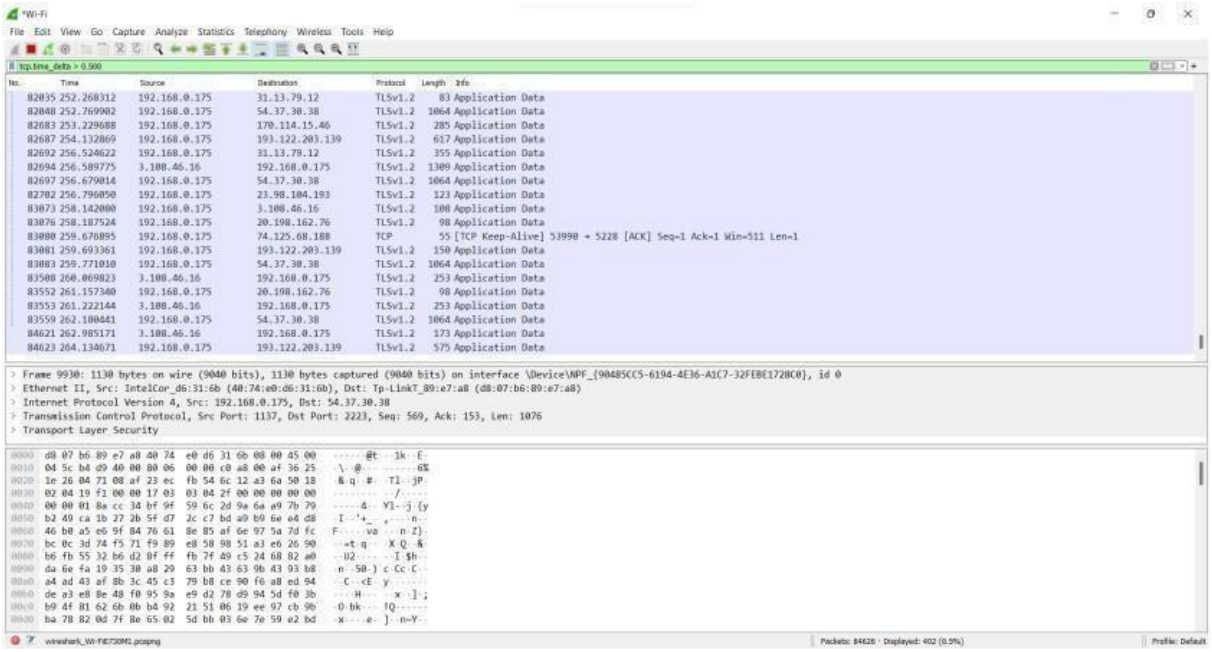
1] Filter Results by Port:

Traces all packets related to Port 80.



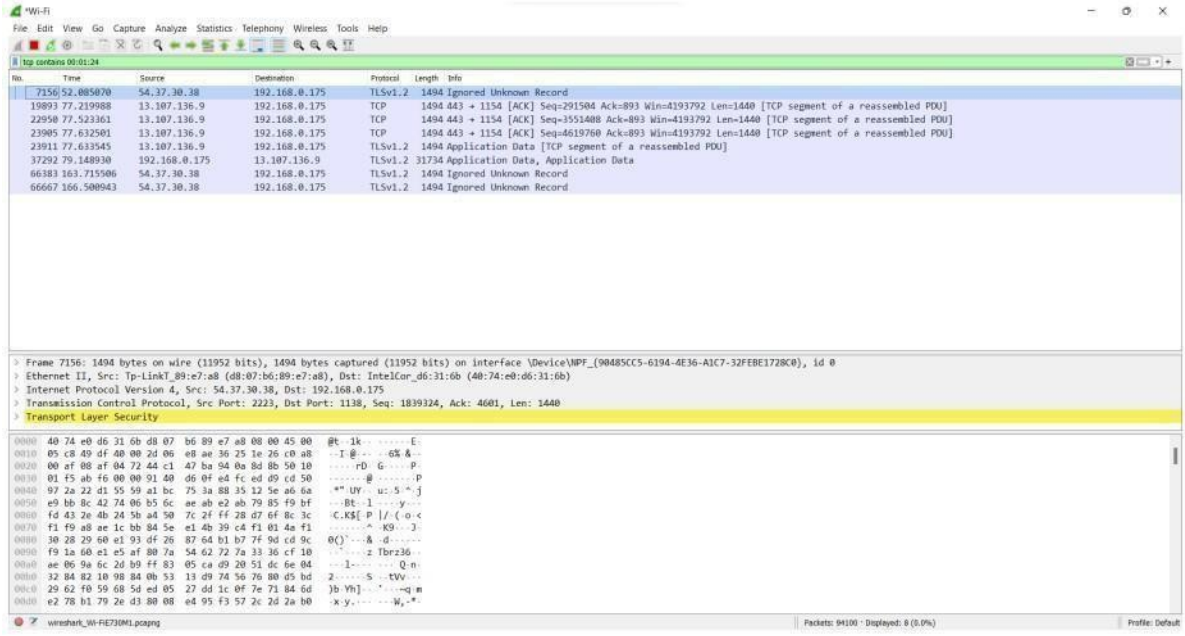
2] `Filter by Delta Time :`

Displays tcp packets with delta time of greater than 0.500 sec



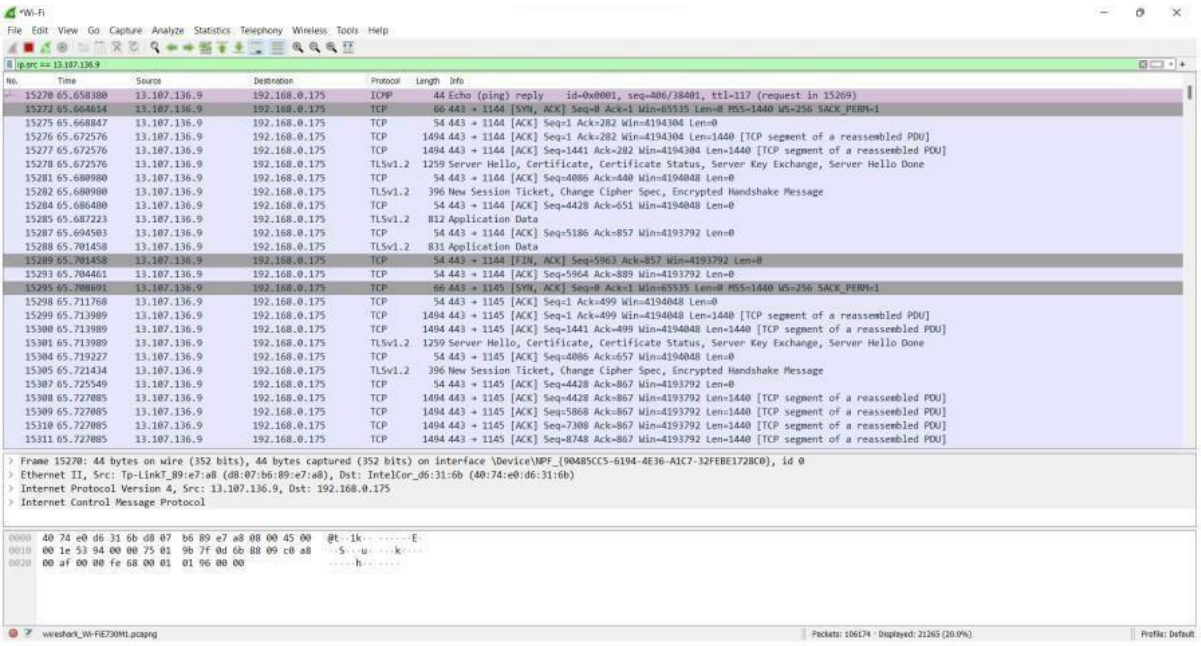
3]`Filter by Byte Sequence:`

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 exploredhow packets can be traced based on different filters