Experiments 10:

Aim: - to capture and analyze packets in Wire shark

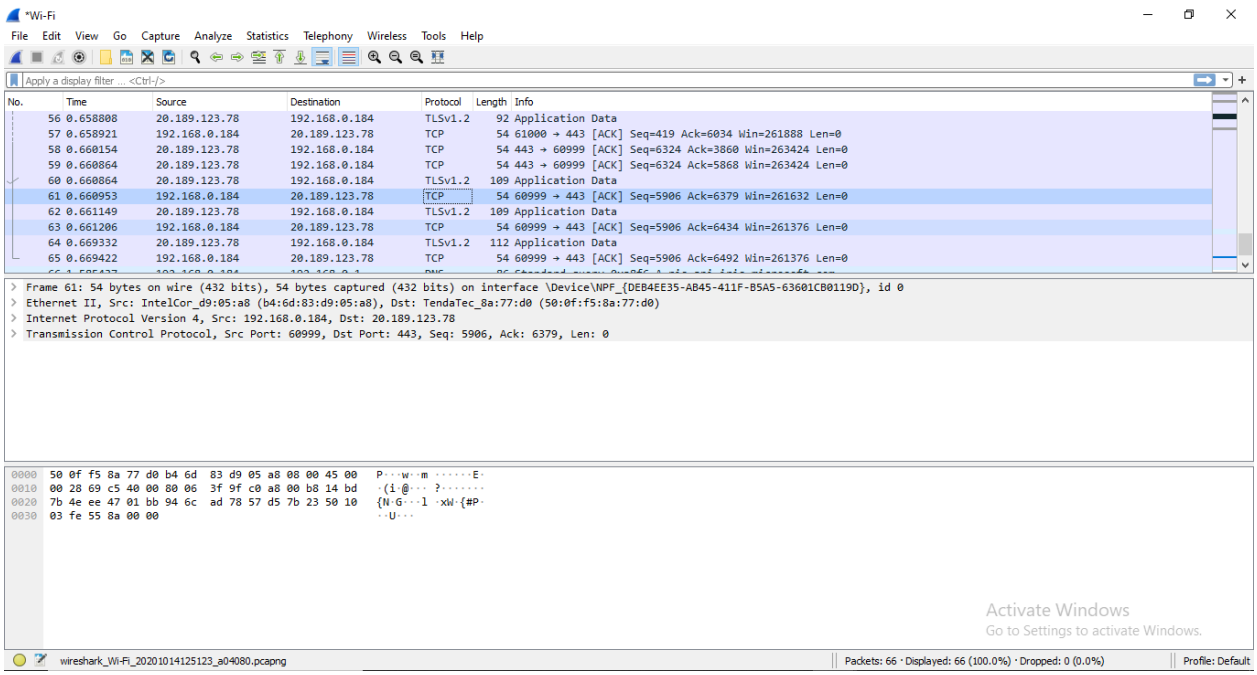
Theory: -

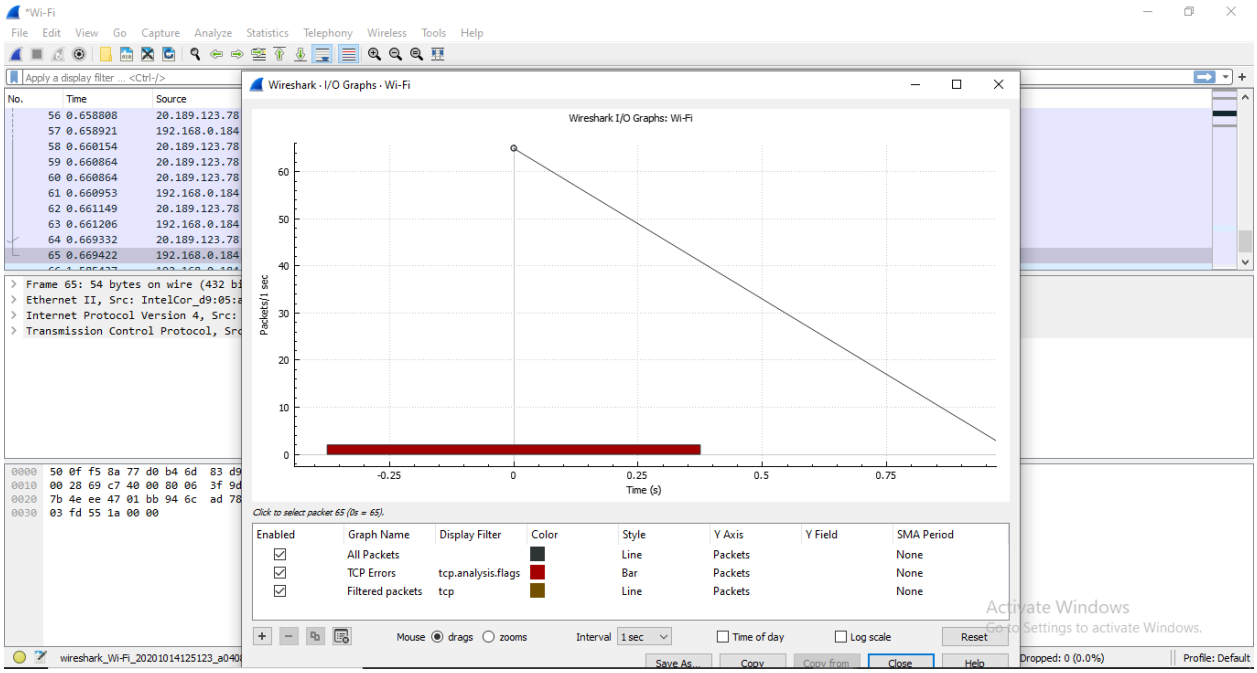
Wire shark is an open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Steps: -

1.> Select the interface for which you want to capture packets from the list shown on starting window in wire shark.
2.> Either double click on the interface or go to capture tab and select start to start capturing packets.
3.> When you are done capturing packets go to capture tab and select stop to stop capturing packets.
4.> Then you can apply filter if you want to see some specific protocol packets.
5.> You can plot graph between protocols.
6.> And by double clicking on the packet you will get detailed information about the packet.

Result: -




*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source
56 0.658808 20.189.123.78
57 0.658921 192.168.0.184
58 0.660154 20.189.123.78
59 0.660864 20.189.123.78
60 0.660864 20.189.123.78
61 0.660953 192.168.0.184
62 0.661149 20.189.123.78
63 0.661206 192.168.0.184
64 0.669332 20.189.123.78
65 0.669422 192.168.0.184
Frame 65: 54 bytes on wire (432 bi
Ethernet II, Src: IntelCor_d9:05:a
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src
0000 50 0f f5 8a 77 d0 b4 6d 83 d9
0010 00 28 69 c7 40 00 80 06 3f 9d
0020 7b 4e ee 47 01 bb 94 6c ad 78
0030 03 fd 55 1a 00 00
wireshark_Wi-Fi_20201014125123_a040
Dropped: 0 (0.0%)
Profile: Default
Wireshark · I/O Graphs · Wi-Fi
Wireshark I/O Graphs: Wi-Fi
Packets/1 sec
Time (s)
Click to select packet 65 (0s = 65).
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period
All Packets Line Packets None
TCP Errors tcp.analysis.flags Bar Packets None
Filtered packets tcp Line Packets None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Save As...
Copy
Copy from ...
Close
Help
Activate Windows
Go to Settings to activate Windows.