

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: -

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A display filter bar shows "<Ctrl-/>". The packet list pane displays a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 61 is selected, showing a TCP ACK from 192.168.0.184 to 20.189.123.78. The packet details pane shows the hierarchy: Frame 61 (54 bytes captured on interface \Device\NPF_{DEB4EE35-AB45-411F-B5A5-63601CB01190}, id 0), Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 66 packets displayed (100.0%) and 0 dropped (0.0%).

No.	Time	Source	Destination	Protocol	Length	Info
56	0.658808	20.189.123.78	192.168.0.184	TLSv1.2	92	Application Data
57	0.658921	192.168.0.184	20.189.123.78	TCP	54	61000 → 443 [ACK] Seq=419 Ack=6034 Win=261888 Len=0
58	0.660154	20.189.123.78	192.168.0.184	TCP	54	443 → 60999 [ACK] Seq=6324 Ack=3860 Win=263424 Len=0
59	0.660864	20.189.123.78	192.168.0.184	TCP	54	443 → 60999 [ACK] Seq=6324 Ack=5868 Win=263424 Len=0
60	0.660864	20.189.123.78	192.168.0.184	TLSv1.2	109	Application Data
61	0.660953	192.168.0.184	20.189.123.78	TCP	54	60999 → 443 [ACK] Seq=5906 Ack=6379 Win=261632 Len=0
62	0.661149	20.189.123.78	192.168.0.184	TLSv1.2	109	Application Data
63	0.661206	192.168.0.184	20.189.123.78	TCP	54	60999 → 443 [ACK] Seq=5906 Ack=6434 Win=261376 Len=0
64	0.669332	20.189.123.78	192.168.0.184	TLSv1.2	112	Application Data
65	0.669422	192.168.0.184	20.189.123.78	TCP	54	60999 → 443 [ACK] Seq=5906 Ack=6492 Win=261376 Len=0

Frame 61: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{DEB4EE35-AB45-411F-B5A5-63601CB01190}, id 0
> Ethernet II, Src: IntelCor_d9:05:a8 (b4:6d:83:d9:05:a8), Dst: TendaTec_8a:77:d0 (50:0f:f5:8a:77:d0)
> Internet Protocol Version 4, Src: 192.168.0.184, Dst: 20.189.123.78
> Transmission Control Protocol, Src Port: 60999, Dst Port: 443, Seq: 5906, Ack: 6379, Len: 0

0000 50 0f f5 8a 77 d0 b4 6d 83 d9 05 a8 08 00 45 00 P...w...m.....E..
0010 00 28 69 c5 40 00 08 06 3f 9f c0 a8 08 b8 14 bd .(i@...?.....
0020 7b 4e ee 47 01 bb 94 6c ad 78 57 d5 7b 23 50 10 {N.G...l..xN..{#P..
0030 03 fe 55 8a 00 00 ..U...

Activate Windows
Go to Settings to activate Windows.

wireshark_Wi-Fi_20201014125123_a04080.pcapng | Packets: 66 · Displayed: 66 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

