

Name : P.Damodar.

Roll No : 411964.

Lab-3

Task : Install Wireshark and what can we do with it.

Work :

1.Installed 'Wireshark' from
<https://www.wireshark.org/#download>

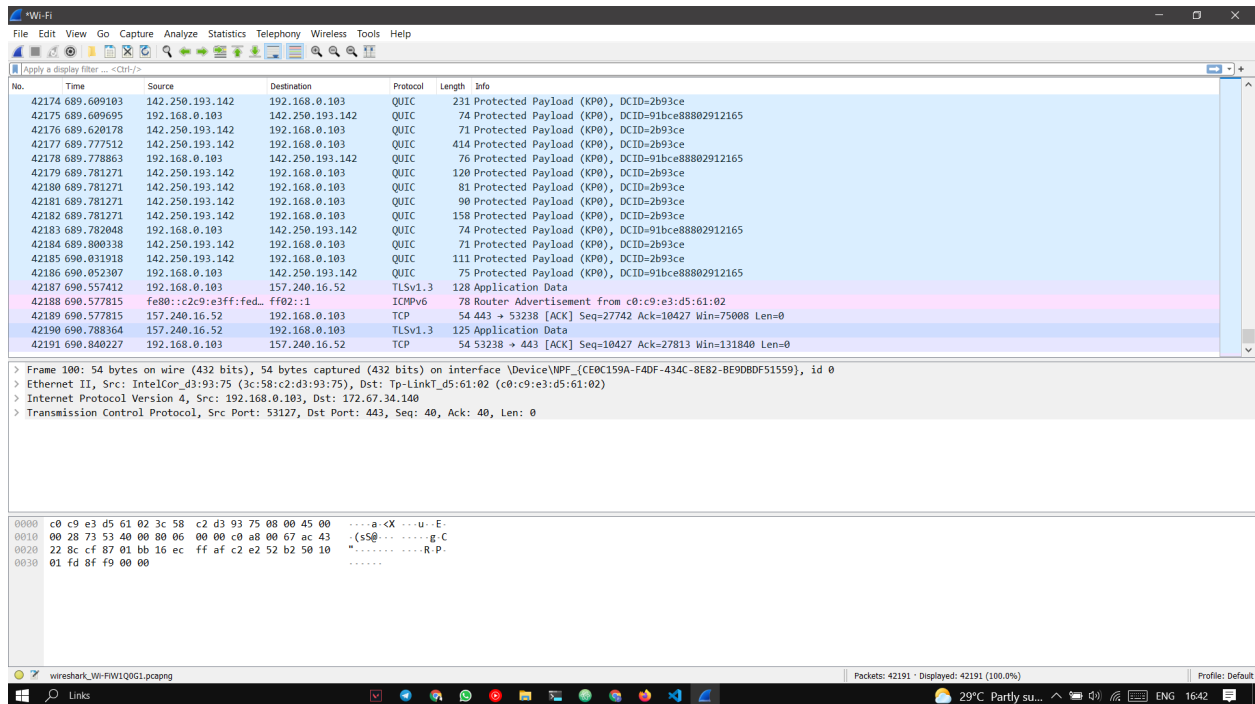
2.

Wireshark is a network packet analyzer, presents what happens inside a network cable.

Wireshark can be used for :-

- Troubleshooting network problems
- Examine security problems
- Debug protocol implementations.
- Learn network protocol internals.

Features of Wireshark :-



- Capture packet data from a network interface.

No.	Time	Source	Destination	Protocol	Length	Info
42174	689.609183	142.250.193.142	192.168.0.103	QUIC	231	Protected Payload (KP0), DCID=2b93ce
42175	689.609695	192.168.0.103	142.250.193.142	QUIC	74	Protected Payload (KP0), DCID=91bce88802912165
42176	689.620178	142.250.193.142	192.168.0.103	QUIC	71	Protected Payload (KP0), DCID=2b93ce
42177	689.777512	142.250.193.142	192.168.0.103	QUIC	414	Protected Payload (KP0), DCID=2b93ce
42178	689.778863	192.168.0.103	142.250.193.142	QUIC	76	Protected Payload (KP0), DCID=91bce88802912165
42179	689.781271	142.250.193.142	192.168.0.103	QUIC	120	Protected Payload (KP0), DCID=2b93ce
42180	689.781271	142.250.193.142	192.168.0.103	QUIC	81	Protected Payload (KP0), DCID=2b93ce
42181	689.781271	142.250.193.142	192.168.0.103	QUIC	90	Protected Payload (KP0), DCID=2b93ce
42182	689.781271	142.250.193.142	192.168.0.103	QUIC	158	Protected Payload (KP0), DCID=2b93ce
42183	689.782048	192.168.0.103	142.250.193.142	QUIC	74	Protected Payload (KP0), DCID=91bce88802912165
42184	689.800338	142.250.193.142	192.168.0.103	QUIC	71	Protected Payload (KP0), DCID=2b93ce
42185	690.031918	142.250.193.142	192.168.0.103	QUIC	111	Protected Payload (KP0), DCID=2b93ce
42186	690.052307	192.168.0.103	142.250.193.142	QUIC	75	Protected Payload (KP0), DCID=91bce88802912165
42187	690.557412	192.168.0.103	157.240.16.52	TLSv1.3	128	Application Data
42188	690.577815	fe80::c2c9:e3ff:fed::1	ff02::1	ICMPv6	78	Router Advertisement from c0:c9:e3:d5:61:02
42189	690.577815	157.240.16.52	192.168.0.103	TCP	54	443 → 53238 [ACK] Seq=27742 Ack=10427 Win=75008 Len=0
42190	690.788364	157.240.16.52	192.168.0.103	TLSv1.3	125	Application Data
42191	690.840227	192.168.0.103	157.240.16.52	TCP	54	53238 → 443 [ACK] Seq=10427 Ack=27813 Win=131840 Len=0

- See the hex dumps of packet data.

0000	c0 c9 e3 d5 61 02 3c 58 c2 d3 93 75 08 00 45 00a<X...u..E.
0010	00 28 73 53 40 00 80 06 00 00 c0 a8 00 67 ac 43	-(sS@-...-g.C
0020	22 8c cf 87 01 bb 16 ec ff af c2 e2 52 b2 50 10	".....R.P.
0030	01 fd 8f f9 00 00

- Display detailed protocol information

▸ Flags: 0x40, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: TCP (6)
 Header Checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.0.103
 Destination Address: 172.67.34.140

- Search for packets using filter
(Using a protocol is done)

The image 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 packet capture and analysis. The main window is divided into three panes:

- Packet List Pane:** Displays a list of captured packets. The first three packets are highlighted in green. A filter box on the left shows 'http', 'http2', and 'http3'.
- Packet Details Pane:** Shows the hierarchical structure of the selected packet (No. 14328). It includes Ethernet II, Internet Protocol Version 4, and TCP.
- Packet Bytes Pane:** Displays the raw data of the selected packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.119775	192.168.0.103	142.250.71.3	OCSP	481	Request
2	0.167785	142.250.71.3	192.168.0.103	OCSP	756	Response
21633	312.696557	192.168.0.103	117.18.237.29	OCSP	478	Request
21647	312.714150	117.18.237.29	192.168.0.103	OCSP	660	Response
40605	666.484965	192.168.0.103	184.31.215.15	HTTP	267	GET /en-GB/livetile/prein...
40611	666.524762	184.31.215.15	192.168.0.103	HTTP/X...	240	HTTP/1.1 200 OK

Packet Details:

- > Frame 14328: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface \Device\NPF_{...}
- > Ethernet II, Src: IntelCor_d3:93:75 (3c:58:c2:d3:93:75), Dst: Tp-LinkT_d5:61:02 (c0:c9:e3:d5:61:02)
- ✓ Internet Protocol Version 4, Src: 192.168.0.103, Dst: 142.250.71.3
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 467
 - Identification: 0x7a57 (31319)
 - > Flags: 0x40, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 128
 - Protocol: TCP (6)
 - Header Checksum: 0x0000 [validation disabled]

Packet Bytes:

```

0000  c0 c9 e3 d5 61 02 3c 58  c2 d3 93 75 08 00 45 00  ...a-<X ...u--E-
  
```

