

CNS Lab Experiment 8

AIM: Study of packet sniffer tools Wireshark

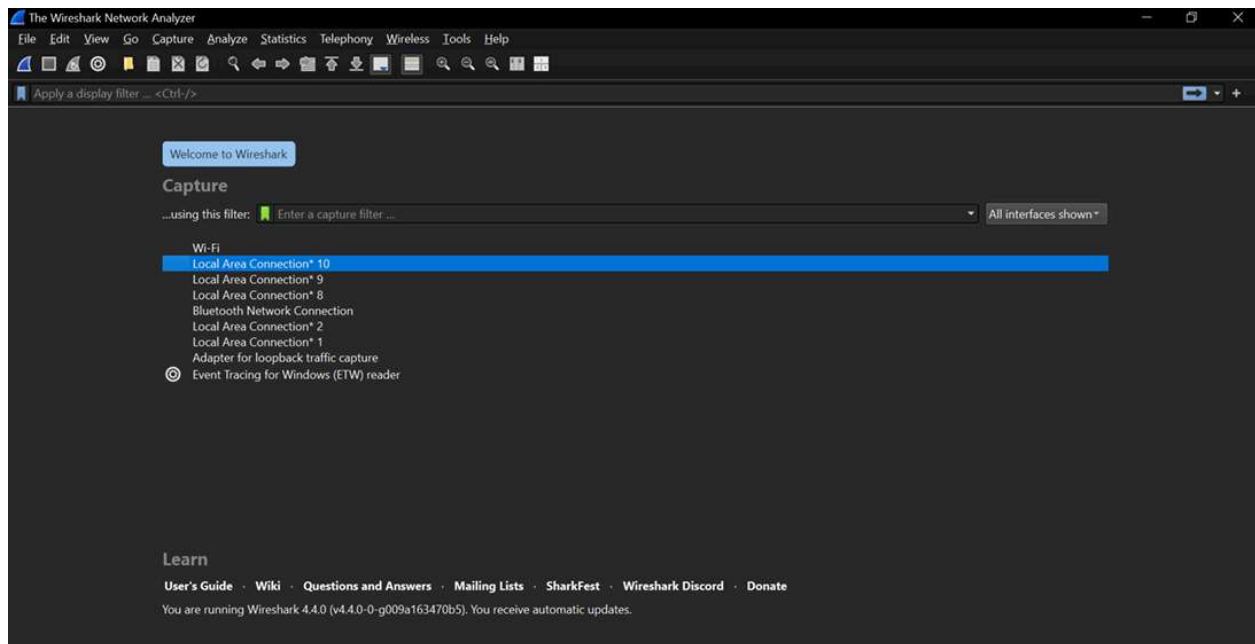
Theory:

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable.

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

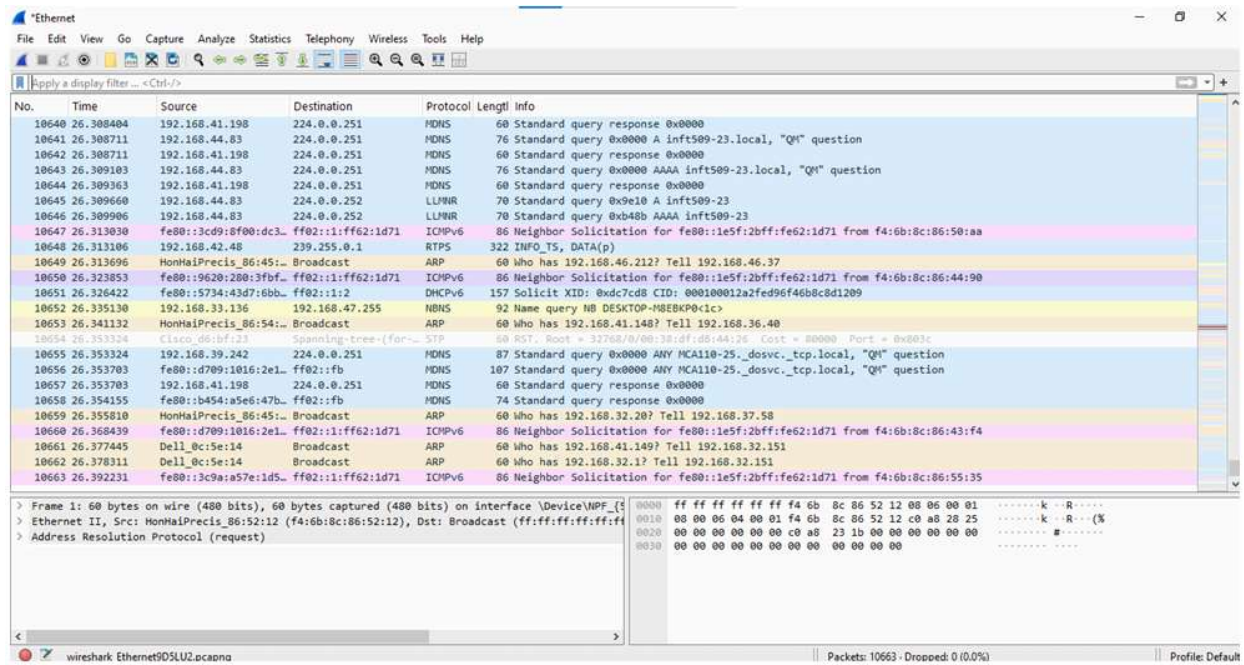
Applications of wireshark :

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals



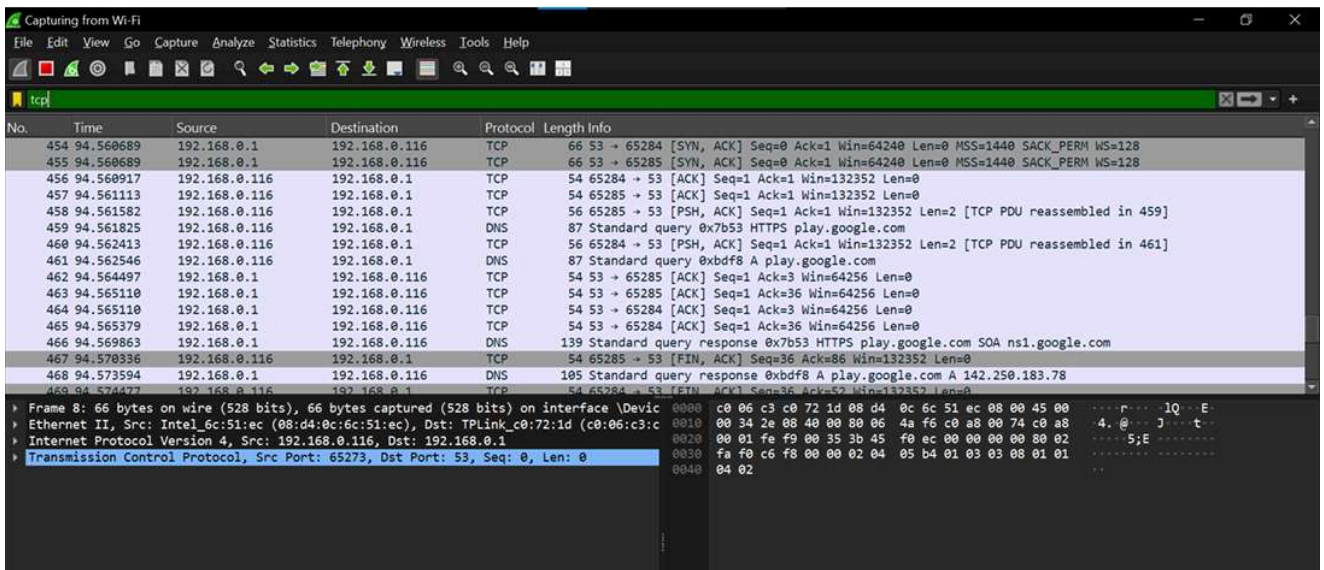
a. Observe performance in promiscuous as well as non-promiscuous mode.

- Promiscuous mode

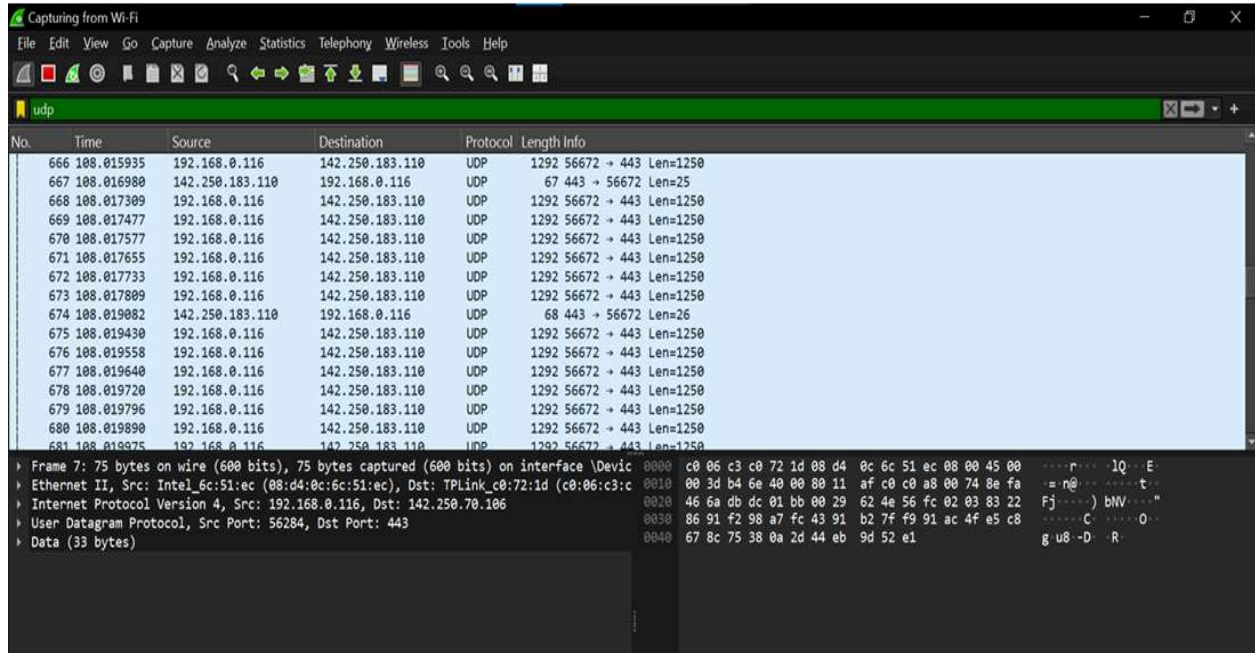


Applying filters in promiscuous mode:

- TCP



• UDP

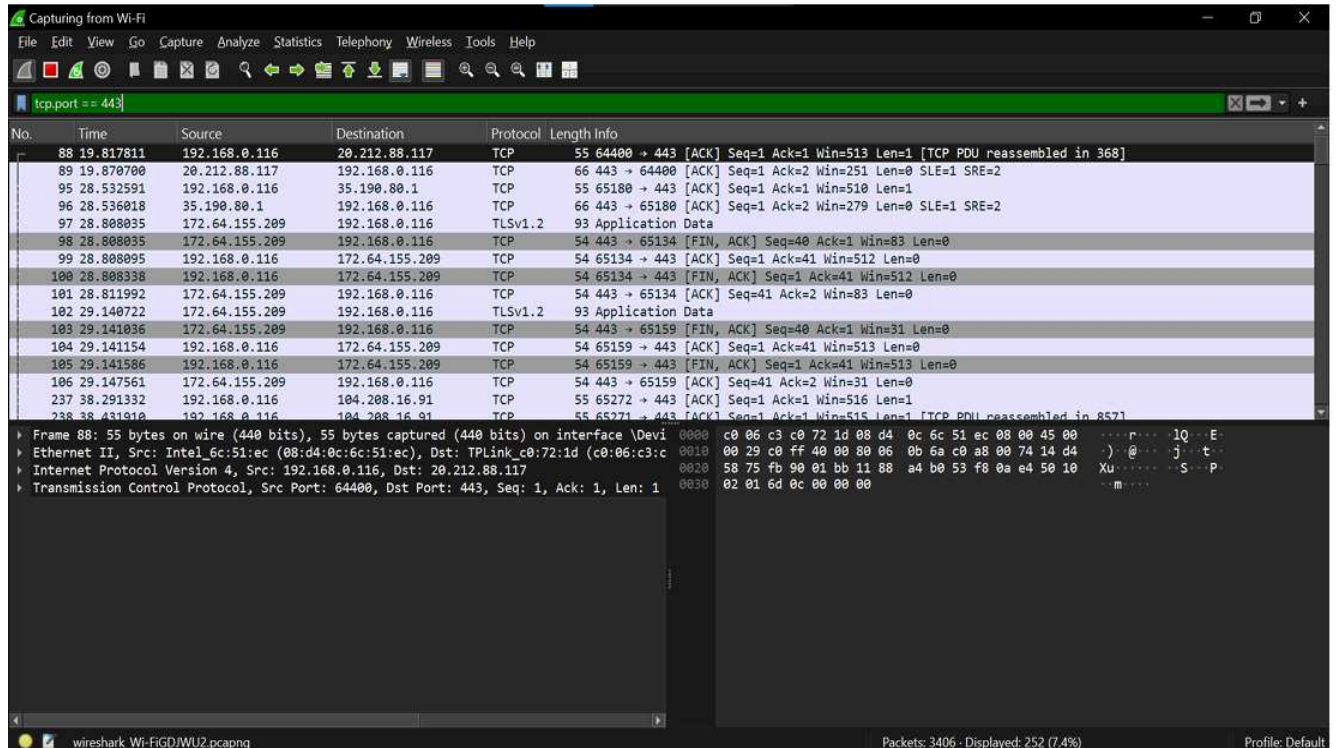


The screenshot shows a Wireshark capture of UDP traffic. The packet list pane displays a series of UDP packets from source 192.168.0.116 to destination 142.250.183.110 on port 443. The packet details pane for packet 666 shows the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
666	108.015935	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
667	108.016980	142.250.183.110	192.168.0.116	UDP	67	443 → 56672 Len=25
668	108.017309	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
669	108.017477	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
670	108.017577	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
671	108.017655	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
672	108.017733	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
673	108.017809	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
674	108.019082	142.250.183.110	192.168.0.116	UDP	68	443 → 56672 Len=26
675	108.019430	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
676	108.019558	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
677	108.019640	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
678	108.019720	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
679	108.019796	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
680	108.019890	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250
681	108.019975	192.168.0.116	142.250.183.110	UDP	1292	56672 → 443 Len=1250

Frame 7: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device...
Ethernet II, Src: Intel_6c:51:ec (08:d4:0c:6c:51:ec), Dst: TPLink_c0:72:1d (c0:06:c3:c0:06:c3:c0:72:1d)
Internet Protocol Version 4, Src: 192.168.0.116, Dst: 142.250.70.106
User Datagram Protocol, Src Port: 56284, Dst Port: 443
Data (33 bytes)

• Port



The screenshot shows a Wireshark capture of TCP traffic. The packet list pane displays a series of TCP packets from source 192.168.0.116 to destination 20.212.88.117 on port 443. The packet details pane for packet 88 shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
88	19.817811	192.168.0.116	20.212.88.117	TCP	55	64400 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP PDU reassembled in 368]
89	19.870700	20.212.88.117	192.168.0.116	TCP	66	443 → 64400 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2
95	28.532591	192.168.0.116	35.190.80.1	TCP	55	65180 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
96	28.536818	35.190.80.1	192.168.0.116	TCP	66	443 → 65180 [ACK] Seq=1 Ack=2 Win=279 Len=0 SLE=1 SRE=2
97	28.808035	172.64.155.209	192.168.0.116	TLSv1.2	93	Application Data
98	28.808035	172.64.155.209	192.168.0.116	TCP	54	443 → 65134 [FIN, ACK] Seq=40 Ack=1 Win=83 Len=0
99	28.808095	192.168.0.116	172.64.155.209	TCP	54	65134 → 443 [ACK] Seq=1 Ack=41 Win=512 Len=0
100	28.808338	192.168.0.116	172.64.155.209	TCP	54	65134 → 443 [FIN, ACK] Seq=1 Ack=41 Win=512 Len=0
101	28.811992	172.64.155.209	192.168.0.116	TCP	54	443 → 65134 [ACK] Seq=41 Ack=2 Win=83 Len=0
102	29.140722	172.64.155.209	192.168.0.116	TLSv1.2	93	Application Data
103	29.141036	172.64.155.209	192.168.0.116	TCP	54	443 → 65159 [FIN, ACK] Seq=40 Ack=1 Win=31 Len=0
104	29.141154	192.168.0.116	172.64.155.209	TCP	54	65159 → 443 [ACK] Seq=1 Ack=41 Win=513 Len=0
105	29.141586	192.168.0.116	172.64.155.209	TCP	54	65159 → 443 [FIN, ACK] Seq=1 Ack=41 Win=513 Len=0
106	29.147561	172.64.155.209	192.168.0.116	TCP	54	443 → 65159 [ACK] Seq=41 Ack=2 Win=31 Len=0
237	38.291332	192.168.0.116	104.208.16.91	TCP	55	65272 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1
238	38.476100	192.168.0.116	104.208.16.91	TCP	55	65272 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP PDU reassembled in 857]

Frame 88: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device...
Ethernet II, Src: Intel_6c:51:ec (08:d4:0c:6c:51:ec), Dst: TPLink_c0:72:1d (c0:06:c3:c0:06:c3:c0:72:1d)
Internet Protocol Version 4, Src: 192.168.0.116, Dst: 20.212.88.117
Transmission Control Protocol, Src Port: 64400, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

● Frame Matches

Frame matches: 01

No.	Time	Source	Destination	Protocol	Length	Info
186	28.565709	192.168.0.1	239.255.255.250	SSDP	428	NOTIFY * HTTP/1.1
187	28.565709	192.168.0.1	239.255.255.250	SSDP	437	NOTIFY * HTTP/1.1
188	28.565709	192.168.0.1	239.255.255.250	SSDP	500	NOTIFY * HTTP/1.1
189	28.565709	192.168.0.1	239.255.255.250	SSDP	496	NOTIFY * HTTP/1.1
190	28.565709	192.168.0.1	239.255.255.250	SSDP	476	NOTIFY * HTTP/1.1
191	28.565709	192.168.0.1	239.255.255.250	SSDP	508	NOTIFY * HTTP/1.1
192	28.565709	192.168.0.1	239.255.255.250	SSDP	490	NOTIFY * HTTP/1.1
193	28.565709	192.168.0.1	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1
194	28.565709	192.168.0.1	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1

Frame 194: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface
Ethernet II, Src: TPLink_c0:72:1d (c0:06:c3:c0:72:1d), Dst: IPv4mcast_7f:ff:fa (01:00:
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 36660, Dst Port: 1900
Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa c0 06 c3 c0 72 1d 08 00 45 00 ...
0010 01 0e 0a 75 40 00 02 11 bb f6 c0 a8 00 01 ef ff ...
0020 ff fa 8f 34 07 6c 01 ca c7 bf 4e 4f 54 49 46 59 ...
0030 20 2a 20 48 54 50 2f 31 2e 31 0d 0a 48 4f 53 ...
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 ...
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 ...
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d ...
0070 36 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68 74 ...
0080 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 30 2e 31 ...
0090 3a 31 39 30 30 2f 71 79 79 6a 6e 2f 72 6f 6f 74 ...
00a0 44 65 73 63 2e 78 6d 6c 0d 0a 53 45 52 56 45 52 ...
00b0 3a 20 54 50 2d 4c 69 6e 60 2f 54 50 2d 4c 69 6e ...
00c0 6b 20 55 50 6e 50 2f 31 2e 31 20 4d 69 6e 69 55 ...
00d0 50 6e 50 64 2f 31 2e 38 0d 0a 4e 54 3a 20 75 72 ...
00e0 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f ...
00f0 72 67 3a 73 65 72 76 69 63 65 3a 4c 61 79 65 72 ...
0100 33 46 6f 72 77 61 72 64 69 6e 67 3a 31 0d 0a 55 ...
0110 53 4e 3a 20 75 75 69 64 3a 65 34 63 37 39 37 65 ...

Filter: ip.addr == 192.168.0.116

Capturing from Wi-Fi

ip.addr == 192.168.0.116

No.	Time	Source	Destination	Protocol	Length	Info
9175	86.025153	192.168.0.116	142.250.192.78	QUIC	1292	Initial, DCID=ef47f7ffdf91c681, PKN: 13, PADDING, PING, PADDING
9176	86.029193	142.250.67.228	192.168.0.116	QUIC	162	Protected Payload (KP0)
9177	86.030608	142.250.192.78	192.168.0.116	QUIC	1292	Initial, SCID=ef47f7ffdf91c681, PKN: 7, CRYPTO, PADDING
9178	86.030857	142.250.192.78	192.168.0.116	QUIC	344	Protected Payload (KP0)
9179	86.031511	142.250.192.78	192.168.0.116	QUIC	986	Protected Payload (KP0)
9180	86.031511	142.250.192.78	192.168.0.116	QUIC	67	Protected Payload (KP0)
9181	86.031662	192.168.0.116	142.250.192.78	QUIC	120	Handshake, DCID=ef47f7ffdf91c681
9182	86.031862	192.168.0.116	142.250.192.78	QUIC	73	Protected Payload (KP0), DCID=ef47f7ffdf91c681
9183	86.033753	142.250.192.78	192.168.0.116	QUIC	1292	Initial, SCID=ef47f7ffdf91c681, PKN: 12, ACK, CRYPTO, PADDING
9184	86.035530	142.250.192.78	192.168.0.116	QUIC	162	Protected Payload (KP0)
9185	86.035922	192.168.0.116	142.250.192.78	QUIC	75	Protected Payload (KP0), DCID=ef47f7ffdf91c681
9186	86.064528	192.168.0.116	142.250.67.228	QUIC	74	Protected Payload (KP0), DCID=e00a31777ec062f1
9187	86.065642	142.250.67.228	192.168.0.116	QUIC	162	Protected Payload (KP0)
9188	86.066032	192.168.0.116	142.250.67.228	QUIC	75	Protected Payload (KP0), DCID=e00a31777ec062f1
9189	86.099086	192.168.0.116	142.250.183.110	QUIC	71	Protected Payload (KP0), DCID=f02a698e261492c2

Frame 9020: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \DeviceNPF...
Ethernet II, Src: Intel_6c:51:ec (08:d4:0c:6c:51:ec), Dst: TPLink_c0:72:1d (c0:06:c3:c0:72:1d)
Internet Protocol Version 4, Src: 192.168.0.116, Dst: 142.250.183.110
User Datagram Protocol, Src Port: 59091, Dst Port: 443
QUIC IETF

0000 c0 06 c3 c0 72 1d 08 d4 0c 6c 51 ec 08 00 45 00 ...
0010 00 39 9c 86 40 00 80 11 56 a8 c0 a8 00 74 8e fa ...
0020 b7 6e e6 d3 01 bb 00 25 32 fe 4d f0 2a 69 8e 26 ...
0030 14 92 c2 41 02 47 64 78 49 98 cf 0e 0a 9d f9 3d ...
0040 72 9a 70 22 76 3f 23

• Non-Promiscuous mode

Wireshark capture of network traffic in non-promiscuous mode. The packet list shows various protocols including LLNMR, ARP, SSDP, MDNS, and NBNS. The packet details pane shows the selected packet (Frame 1) as an ARP request from HonHaiPrecis_86:4d:d8 to the broadcast address ff:ff:ff:ff:ff:ff.

No.	Time	Source	Destination	Protocol	Length	Info
1653	5.993250	fe80::673c:bdea:13c...	ff02::1:3	LLNMR	90	Standard query 0x693e AAAA CHPN301-11
1654	5.993502	192.168.36.26	224.0.0.252	LLNMR	70	Standard query 0x693e AAAA CHPN301-11
1655	5.994715	Dell_2a:9c:2b	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.41.216
1656	5.995973	192.168.36.78	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1657	6.000036	HonHaiPrecis_86:54:...	Broadcast	ARP	60	Who has 192.168.45.19? Tell 192.168.36.40
1658	6.002931	Dell_a6:09:97	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.36.201
1659	6.009614	HonHaiPrecis_86:4d:...	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.46.172
1660	6.009975	192.168.43.152	224.0.0.251	MDNS	76	Standard query 0x0000 PTR _ipps_tcp.local, "QU" question
1661	6.009975	fe80::5150:a8c4:555...	ff02::fb	MDNS	96	Standard query 0x0000 PTR _ipps_tcp.local, "QU" question
1662	6.010181	192.168.43.152	224.0.0.251	MDNS	75	Standard query 0x0000 PTR _ipp_tcp.local, "QU" question
1663	6.010181	fe80::5150:a8c4:555...	ff02::fb	MDNS	95	Standard query 0x0000 PTR _ipp_tcp.local, "QU" question
1664	6.010181	192.168.41.198	224.0.0.251	MDNS	60	Standard query response 0x0000
1665	6.010317	fe80::b454:a5e6:47b...	ff02::fb	MDNS	74	Standard query response 0x0000
1666	6.010596	192.168.41.198	224.0.0.251	MDNS	60	Standard query response 0x0000
1667	6.010596	fe80::b454:a5e6:47b...	ff02::fb	MDNS	74	Standard query response 0x0000
1668	6.013234	192.168.46.80	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1669	6.018337	HonHaiPrecis_86:46:...	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.34.141
1670	6.035055	HonHaiPrecis_86:4d:...	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.36.29
1671	6.035341	Dell_ad:41:6a	Broadcast	ARP	60	Who has 192.168.32.19? Tell 192.168.38.110
1672	6.042781	192.168.43.53	192.168.47.255	NBNS	92	Name query NB CA-3<20>
1673	6.043279	HonHaiPrecis_86:4b:...	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.45.129
1674	6.043681	HonHaiPrecis_8d:11:...	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.40.62
1675	6.045551	HonHaiPrecis_86:4a:...	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.44.160
1676	6.069915	MicroStarINT_ee:93:...	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.40.4

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF...
 Ethernet II, Src: HonHaiPrecis_86:4d:d8 (f4:6b:8c:86:4d:d8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

Applying filters in non promiscuous mode:

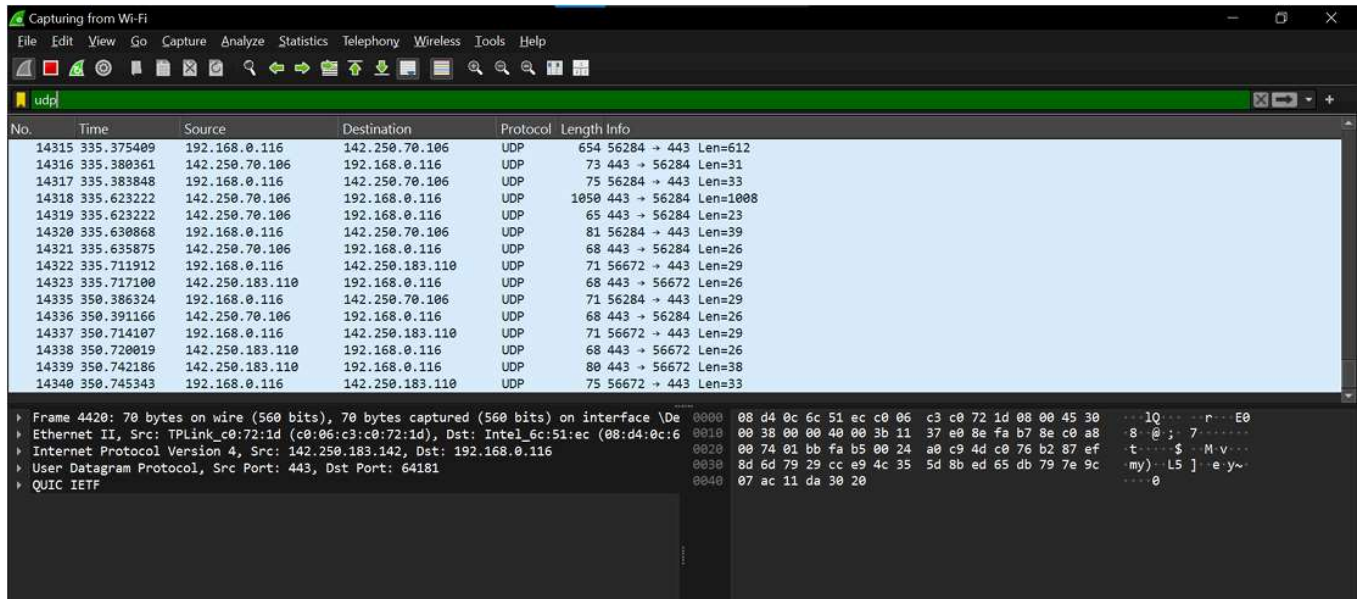
• TCP

Wireshark capture of network traffic in non-promiscuous mode with a TCP filter applied. The packet list shows various protocols including TCP, TLSv1.2, and Internet Protocol Version 4. The packet details pane shows the selected packet (Frame 4) as a TCP Keep-Alive message from 192.168.0.116 to 23.206.173.25.

No.	Time	Source	Destination	Protocol	Length	Info
6934	78.377166	13.107.246.68	192.168.0.116	TCP	54	443 → 64880 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0
6935	78.377312	192.168.0.116	13.107.246.68	TCP	66	64880 → 443 [ACK] Seq=1 Ack=4294967251 Win=1018 Len=0 SLE=1 SRE=32
6936	78.377537	192.168.0.116	13.107.246.68	TCP	54	64880 → 443 [ACK] Seq=1 Ack=32 Win=1024 Len=0
6937	78.377634	192.168.0.116	13.107.246.68	TCP	54	64880 → 443 [ACK] Seq=1 Ack=33 Win=1024 Len=0
6938	78.901216	192.168.0.116	20.189.173.11	TLSv1.2	139	Application Data
6939	78.901574	192.168.0.116	20.189.173.11	TLSv1.2	894	Application Data
6942	79.119903	20.189.173.11	192.168.0.116	TCP	54	443 → 64879 [ACK] Seq=1387 Ack=77807 Win=16385 Len=0
6943	79.135050	20.189.173.11	192.168.0.116	TLSv1.2	153	Application Data
6944	79.137958	192.168.0.116	20.189.173.11	TLSv1.2	89	Application Data
6945	79.400475	20.189.173.11	192.168.0.116	TCP	54	443 → 64879 [ACK] Seq=1486 Ack=77842 Win=16385 Len=0
6979	94.511481	20.212.88.117	192.168.0.116	TLSv1.2	113	Application Data
6980	94.513654	192.168.0.116	20.212.88.117	TLSv1.2	120	Ignored Unknown Record
6981	94.565113	20.212.88.117	192.168.0.116	TCP	54	443 → 64400 [ACK] Seq=60 Ack=68 Win=251 Len=0
6983	96.875643	192.168.0.116	204.79.197.239	TCP	55	[TCP Keep-Alive] 64898 → 443 [ACK] Seq=8390 Ack=1517 Win=132352 Len=1
6984	96.879573	204.79.197.239	192.168.0.116	TCP	66	[TCP Keep-Alive ACK] 443 → 64898 [ACK] Seq=1517 Ack=8391 Win=4193792 Len=0 SLE=8390 SRE=8391

Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF...
 Ethernet II, Src: Intel_6c:51:ec (08:d4:0c:6c:51:ec), Dst: TPLink_c0:72:1d (c0:06:c3:c0:72:1d)
 Internet Protocol Version 4, Src: 192.168.0.116, Dst: 23.206.173.25
 Transmission Control Protocol, Src Port: 64850, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

• UDP

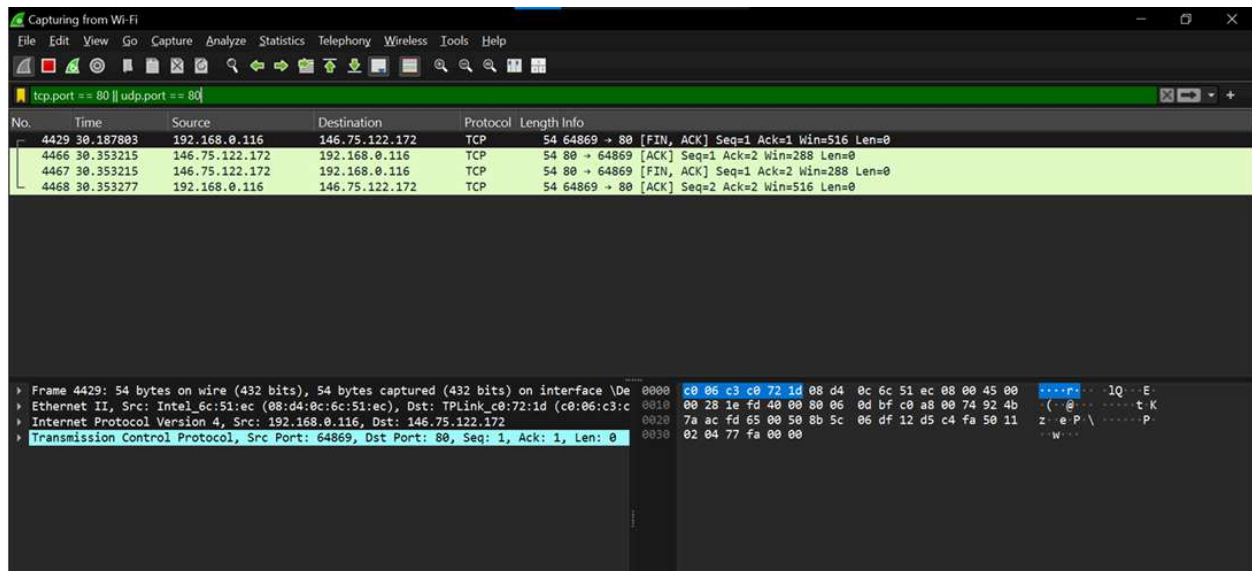


The screenshot shows a Wireshark capture of network traffic on a Wi-Fi interface. The filter bar at the top is set to 'udp'. The packet list pane displays a series of UDP packets, with packet 4420 selected. The packet details pane for packet 4420 shows the following structure:

- Frame 4420: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF{...}
- Ethernet II, Src: TPLink_c0:72:1d (c0:06:c3:c0:72:1d), Dst: Intel_6c:51:ec (08:d4:0c:6c:51:ec)
- Internet Protocol Version 4, Src: 142.250.183.142, Dst: 192.168.0.116
- User Datagram Protocol, Src Port: 443, Dst Port: 64181
- QUIC IETF

The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header, IP header, and QUIC data.

• Port



The screenshot shows a Wireshark capture of network traffic on a Wi-Fi interface. The filter bar at the top is set to 'tcp.port == 80 || udp.port == 80'. The packet list pane displays a series of TCP packets, with packet 4429 selected. The packet details pane for packet 4429 shows the following structure:

- Frame 4429: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF{...}
- Ethernet II, Src: Intel_6c:51:ec (08:d4:0c:6c:51:ec), Dst: TPLink_c0:72:1d (c0:06:c3:c0:72:1d)
- Internet Protocol Version 4, Src: 192.168.0.116, Dst: 146.75.122.172
- Transmission Control Protocol, Src Port: 64869, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header, IP header, and TCP header.

• Frame Matches

Current filter: frame matches "01"

No.	Time	Source	Destination	Protocol	Length	Info
6	0.000000	192.168.0.1	239.255.255.250	SSDP	508	NOTIFY * HTTP/1.1
7	0.000000	192.168.0.1	239.255.255.250	SSDP	490	NOTIFY * HTTP/1.1
8	0.000000	192.168.0.1	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1
9	0.000000	192.168.0.1	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1
35	3.967582	192.168.0.116	142.250.76.174	QUIC	1292	Protected Payload (KP0), DCID=fa8338ddaeabc3d4
78	6.903751	192.168.0.116	142.250.76.174	QUIC	1292	Protected Payload (KP0), DCID=fa8338ddaeabc3d4
203	30.007043	192.168.0.1	239.255.255.250	SSDP	428	NOTIFY * HTTP/1.1
204	30.007043	192.168.0.1	239.255.255.250	SSDP	437	NOTIFY * HTTP/1.1
205	30.007043	192.168.0.1	239.255.255.250	SSDP	500	NOTIFY * HTTP/1.1
206	30.007043	192.168.0.1	239.255.255.250	SSDP	496	NOTIFY * HTTP/1.1
207	30.007043	192.168.0.1	239.255.255.250	SSDP	476	NOTIFY * HTTP/1.1
208	30.007043	192.168.0.1	239.255.255.250	SSDP	508	NOTIFY * HTTP/1.1
209	30.007043	192.168.0.1	239.255.255.250	SSDP	490	NOTIFY * HTTP/1.1
210	30.007043	192.168.0.1	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1
211	30.007043	192.168.0.1	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1

Frame 1: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface VD
 Ethernet II, Src: TPLink_c0:72:1d (c0:06:c3:c0:72:1d), Dst: IPv4mcast_7f:ff:fa (01:00:
 Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
 User Datagram Protocol, Src Port: 36660, Dst Port: 1900
 Simple Service Discovery Protocol

Filter: ip.addr == 192.168.0.4

Capturing from Wi-Fi

Filter: ip.addr == 192.168.0.116

No.	Time	Source	Destination	Protocol	Length	Info
16	6.330961	23.212.254.51	192.168.0.116	QUIC	329	Protected Payload (KP0)
17	6.330961	23.212.254.51	192.168.0.116	QUIC	103	Protected Payload (KP0)
18	6.330961	23.212.254.51	192.168.0.116	QUIC	63	Protected Payload (KP0)
19	6.332200	192.168.0.116	23.212.254.51	QUIC	73	Protected Payload (KP0), DCID=0b40a0bbd7019c24
20	6.361698	192.168.0.116	23.212.254.51	QUIC	74	Protected Payload (KP0), DCID=0b40a0bbd7019c24
21	6.362019	192.168.0.116	23.212.254.51	QUIC	116	Protected Payload (KP0), DCID=0b40a0bbd7019c24
22	6.368248	192.168.0.116	192.168.0.116	QUIC	66	Protected Payload (KP0)
23	6.368400	23.212.254.51	192.168.0.116	QUIC	68	Protected Payload (KP0)
24	6.642524	192.168.0.116	35.174.127.31	TLSv1.2	294	Application Data
25	6.838518	35.174.127.31	192.168.0.116	TLSv1.2	316	Application Data
26	6.878850	192.168.0.116	35.174.127.31	TCP	54	4176 → 443 [ACK] Seq=241 Ack=263 Win=256 Len=0
27	8.150824	192.168.0.116	192.168.1.50	TCP	66	4206 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
28	8.819796	192.168.0.116	13.107.21.239	TCP	55	4142 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
29	8.822689	13.107.21.239	192.168.0.116	TCP	66	443 → 4142 [ACK] Seq=1 Ack=2 Win=16385 Len=0 SLE=1 SRE=2
30	9.166166	192.168.0.116	192.168.1.50	TCP	66	[TCP Retransmission] 4206 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device
 Ethernet II, Src: Intel_6c:51:ec (08:d4:0c:6c:51:ec), Dst: TPLink_c0:72:1d (c0:06:c3:c0:
 Internet Protocol Version 4, Src: 192.168.0.116, Dst: 140.82.114.26
 Transmission Control Protocol, Src Port: 4128, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

Conclusion: Thus, by performing this experiment, we have studied and implemented packet sniffing tool Wireshark