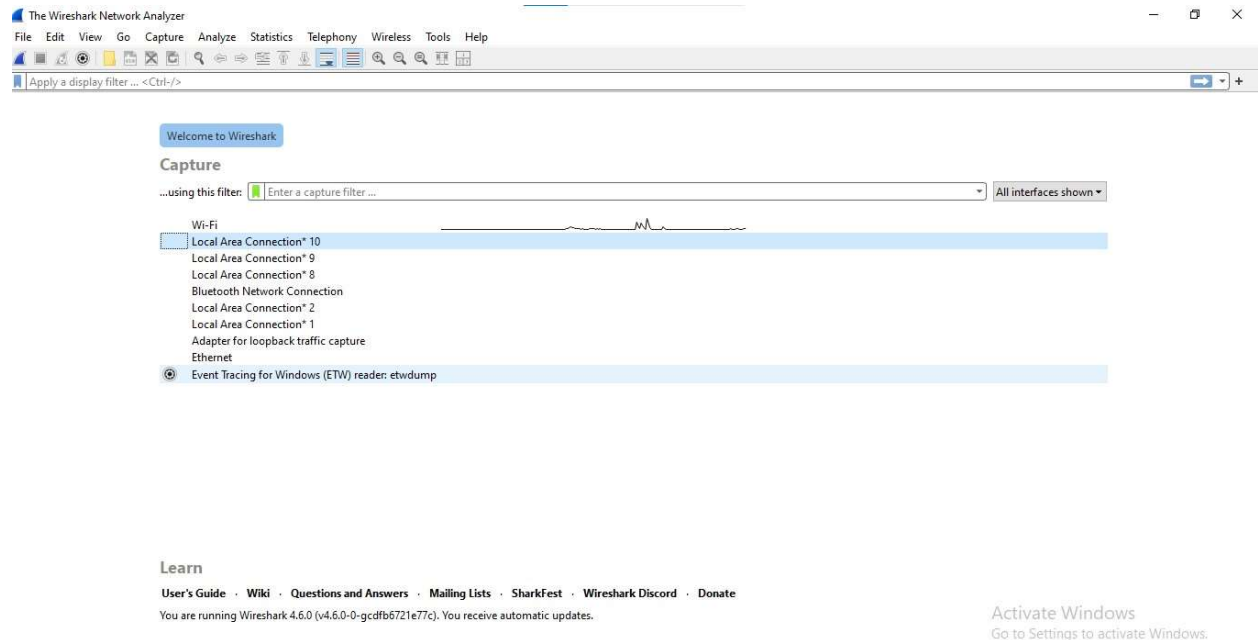
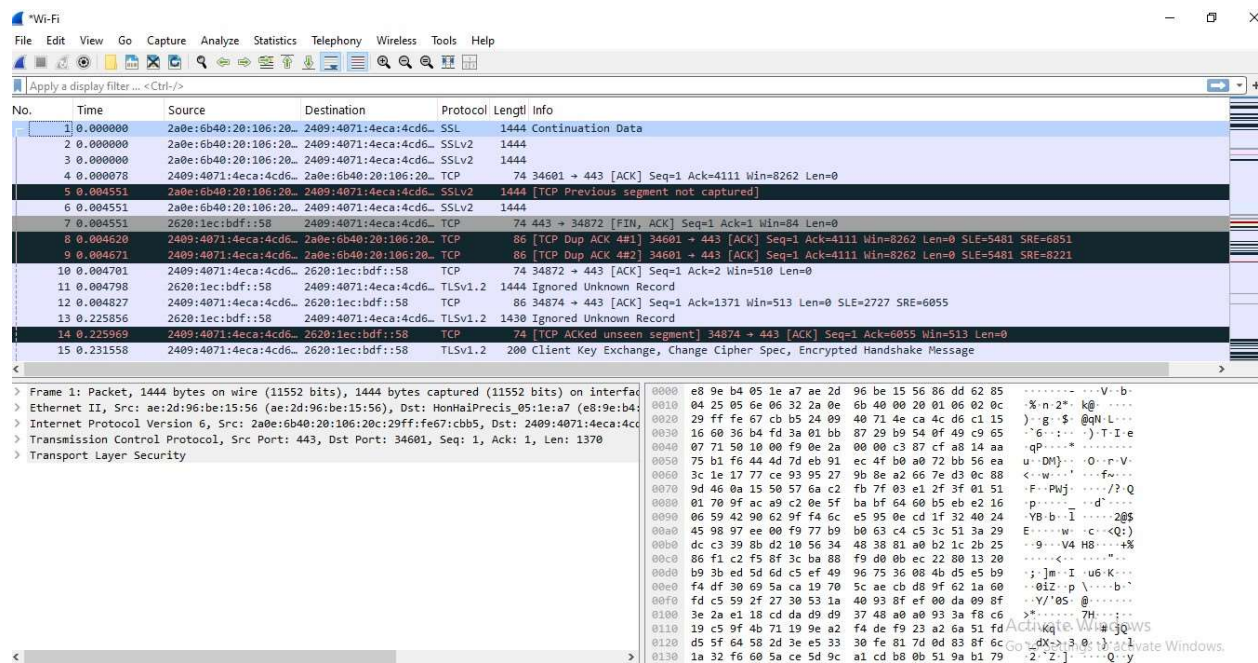


Capture and Analyze Network Traffic Using Wireshark.

1. Installation of wireshark

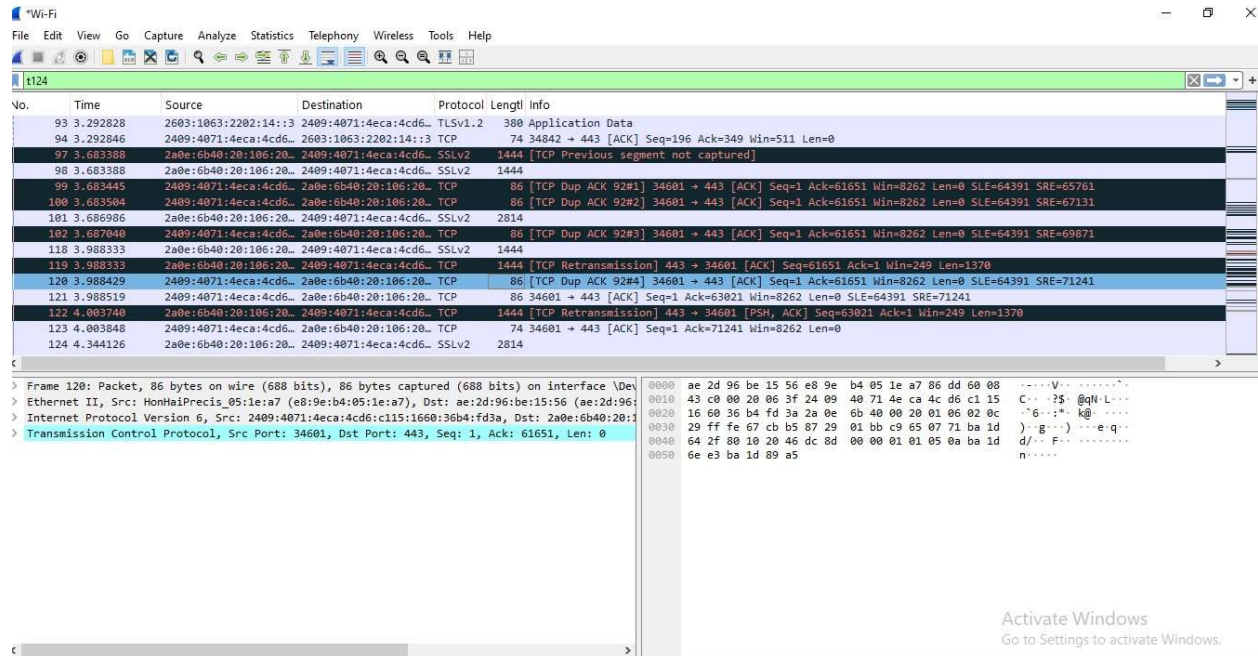


2. Capturing active network interface



3.browsed website to generate traffic and captured the packets

Tcp

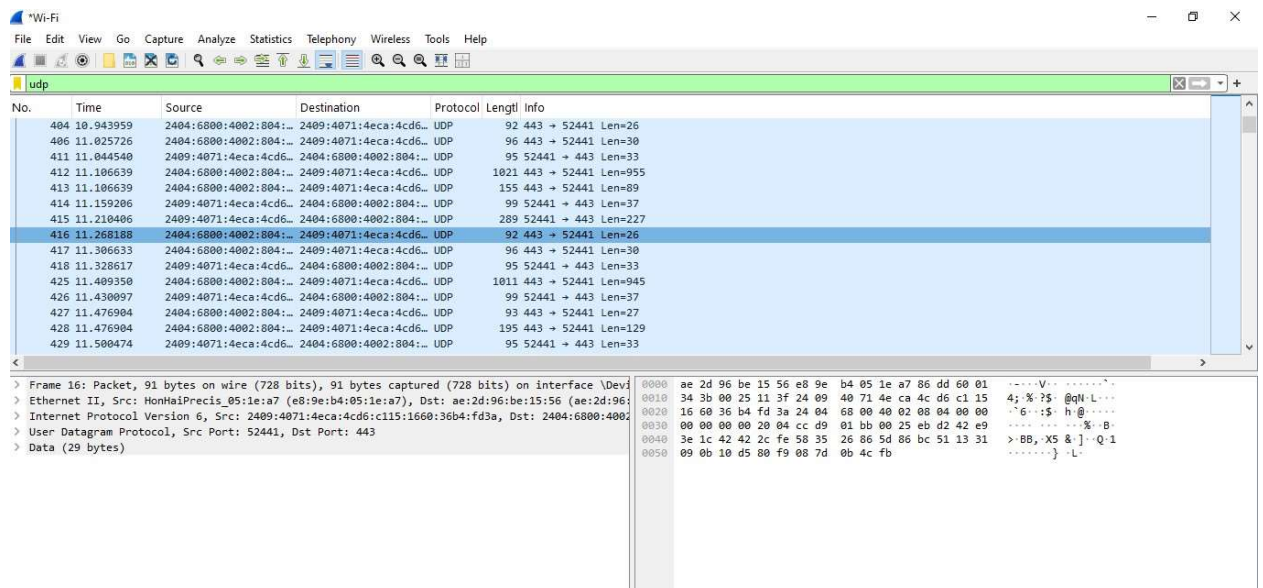


The image shows a Wireshark packet capture window titled "Wi-Fi". The packet list on the left shows several TCP segments. The selected packet is packet 120, which is a TCP segment from source 2409:4071:4eca:4cd6::2a0e:6b40:20:106:20 to destination 2409:4071:4eca:4cd6::2a0e:6b40:20:106:20. The packet details pane shows the following information:

- Frame 120: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Dev
- Ethernet II, Src: HonHaiPrecis_05:1e:a7 (e8:9e:b4:05:1e:a7), Dst: ae:2d:96:be:15:56 (ae:2d:96:be:15:56)
- Internet Protocol Version 6, Src: 2409:4071:4eca:4cd6:c115:1660:36b4:fd3a, Dst: 2a0e:6b40:20:106:20:106:20:106:20
- Transmission Control Protocol, Src Port: 34601, Dst Port: 443, Seq: 1, Ack: 61651, Len: 0

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

Udp

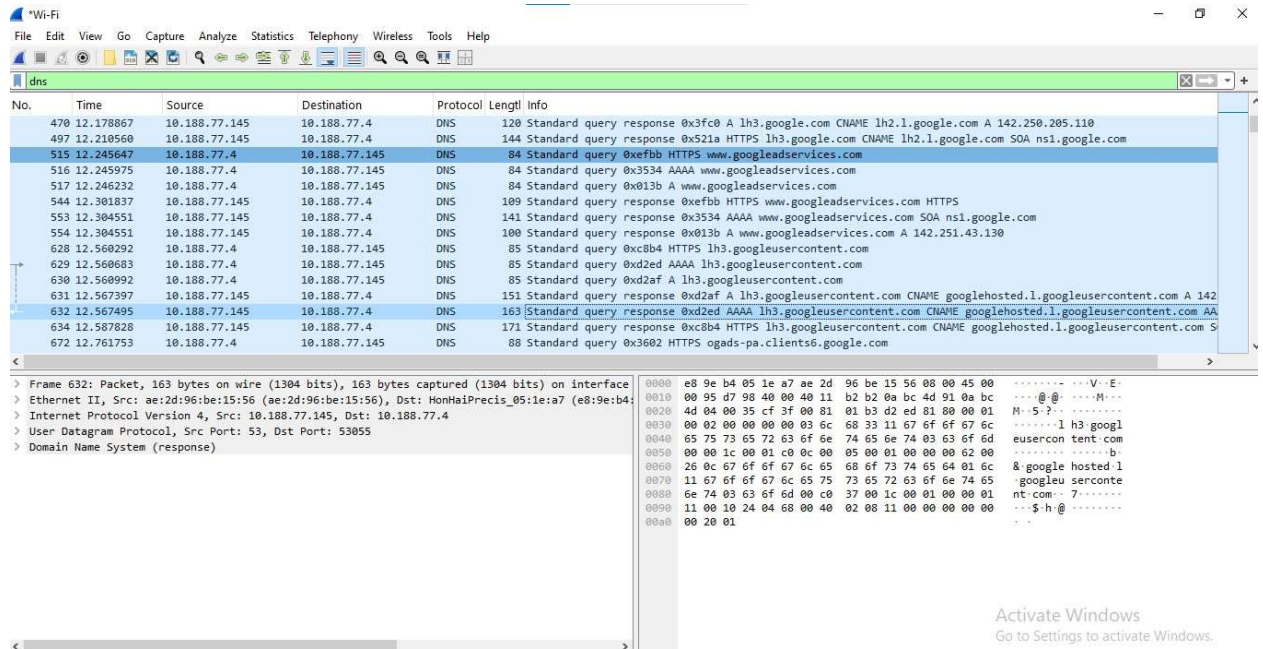


The image shows a Wireshark packet capture window titled "Wi-Fi". The packet list on the left shows several UDP segments. The selected packet is packet 16, which is a UDP segment from source 2409:4071:4eca:4cd6:c115:1660:36b4:fd3a to destination 2409:4071:4eca:4cd6:c115:1660:36b4:fd3a. The packet details pane shows the following information:

- Frame 16: Packet, 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Dev
- Ethernet II, Src: HonHaiPrecis_05:1e:a7 (e8:9e:b4:05:1e:a7), Dst: ae:2d:96:be:15:56 (ae:2d:96:be:15:56)
- Internet Protocol Version 6, Src: 2409:4071:4eca:4cd6:c115:1660:36b4:fd3a, Dst: 2409:4071:4eca:4cd6:c115:1660:36b4:fd3a
- User Datagram Protocol, Src Port: 52441, Dst Port: 443
- Data (29 bytes)

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

DNS



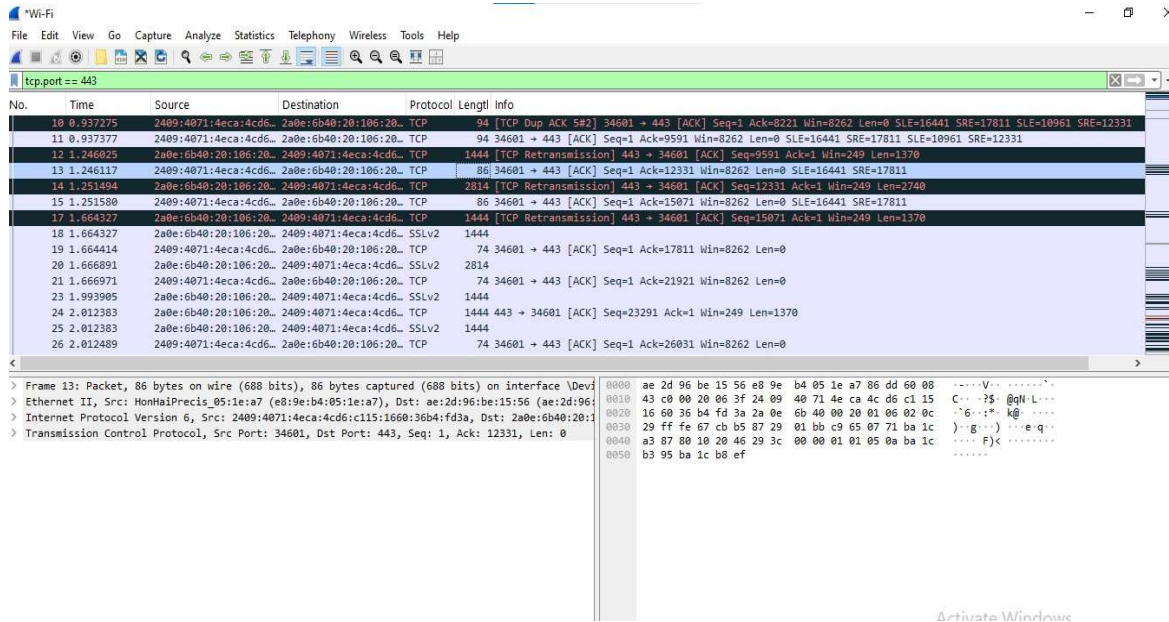
The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of packets, with packet 632 selected. The middle pane shows the details of packet 632, which is a Standard query response from 10.188.77.145 to 10.188.77.4. The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII view shows the response for the query for googlehosted.l.googleusercontent.com.

No.	Time	Source	Destination	Protocol	Length	Info
470	12.178867	10.188.77.145	10.188.77.4	DNS	120	Standard query response 0x3fc0 A lh3.google.com CNAME lh2.l.google.com A 142.250.205.110
497	12.210560	10.188.77.145	10.188.77.4	DNS	144	Standard query response 0x521a HTTPS lh3.google.com CNAME lh2.l.google.com SOA ns1.google.com
515	12.245647	10.188.77.4	10.188.77.145	DNS	84	Standard query 0xefbb HTTPS www.googleadservices.com
516	12.245975	10.188.77.4	10.188.77.145	DNS	84	Standard query 0x3534 AAAA www.googleadservices.com
517	12.246232	10.188.77.4	10.188.77.145	DNS	84	Standard query 0x013b A www.googleadservices.com
544	12.301837	10.188.77.145	10.188.77.4	DNS	109	Standard query response 0xefbb HTTPS www.googleadservices.com HTTPS
553	12.304551	10.188.77.145	10.188.77.4	DNS	141	Standard query response 0x3534 AAAA www.googleadservices.com SOA ns1.google.com
554	12.304551	10.188.77.145	10.188.77.4	DNS	100	Standard query response 0x013b A www.googleadservices.com A 142.251.43.130
628	12.560292	10.188.77.4	10.188.77.145	DNS	85	Standard query 0xc8b4 HTTPS lh3.googleusercontent.com
629	12.560683	10.188.77.4	10.188.77.145	DNS	85	Standard query 0xd2ed AAAA lh3.googleusercontent.com
630	12.560992	10.188.77.4	10.188.77.145	DNS	85	Standard query 0xd2af A lh3.googleusercontent.com
631	12.567397	10.188.77.145	10.188.77.4	DNS	151	Standard query response 0xd2af A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142
632	12.567495	10.188.77.145	10.188.77.4	DNS	163	Standard query response 0xd2ed AAAA lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com AA
634	12.587828	10.188.77.145	10.188.77.4	DNS	171	Standard query response 0xc8b4 HTTPS lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com S
672	12.761753	10.188.77.4	10.188.77.145	DNS	88	Standard query 0x3602 HTTPS ogads-pa.clients6.google.com

Frame 632: Packet, 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface
Ethernet II, Src: HonHaiPrecis_05:1e:a7 (e8:9e:b4:05:1e:a7), Dst: ae:2d:96:be:15:56 (ae:2d:96:be:15:56)
Internet Protocol Version 4, Src: 10.188.77.145, Dst: 10.188.77.4
User Datagram Protocol, Src Port: 53, Dst Port: 53055
Domain Name System (response)

0000 e8 9e b4 05 1e a7 ae 2d 96 be 15 56 08 00 45 00V...E..
0010 00 95 d7 98 40 00 40 11 b2 b2 0a bc 4d 91 0a bc@...M..
0020 4d 04 00 35 cf 3f 00 81 01 b3 d2 ed 81 80 00 01 M..S?...
0030 00 02 00 00 00 03 6c 68 33 11 67 6f 6f 6f 6cl h3 googl
0040 65 75 73 65 72 63 6f 6e 74 65 6e 74 03 63 6f 6d eusercon tent.com
0050 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 62 00b..
0060 26 0c 67 6f 6f 6f 6c 65 68 6f 73 74 65 64 01 6c & google hosted l
0070 11 67 6f 6f 6f 6c 65 73 65 72 63 6f 6e 74 65 googleu serconte
0080 6e 74 03 63 6f 6d 0c 37 00 1c 00 01 00 00 01 nt.com: 7.....
0090 11 00 10 24 04 68 00 02 08 11 00 00 00 00 00 ..\$.h@.....
00a0 00 20 01

https(port 443)



The image shows a Wireshark packet capture of HTTPS traffic. The top pane displays a list of packets, with packet 13 selected. The middle pane shows the details of packet 13, which is a TCP Retransmission from 2409:4071:4eca:4cd6::2a0e:6b40:20:106:20 to 2409:4071:4eca:4cd6::2a0e:6b40:20:106:20. The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII view shows the response for the query for googlehosted.l.googleusercontent.com.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.937275	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	94	[TCP Dup ACK 582] 34601 → 443 [ACK] Seq=1 Ack=8221 Win=8262 Len=0 SLE=16441 SRE=17811 SLE=10961 SRE=12331
11	0.937377	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	94	34601 → 443 [ACK] Seq=1 Ack=9591 Win=8262 Len=0 SLE=16441 SRE=17811 SLE=10961 SRE=12331
12	1.246025	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	1444	[TCP Retransmission] 443 → 34601 [ACK] Seq=9591 Ack=1 Win=249 Len=1370
13	1.246117	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	86	34601 → 443 [ACK] Seq=1 Ack=12331 Win=8262 Len=0 SLE=16441 SRE=17811
14	1.251494	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	2814	[TCP Retransmission] 443 → 34601 [ACK] Seq=12331 Ack=1 Win=249 Len=2740
15	1.251580	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	86	34601 → 443 [ACK] Seq=1 Ack=15071 Win=8262 Len=0 SLE=16441 SRE=17811
17	1.664327	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	1444	[TCP Retransmission] 443 → 34601 [ACK] Seq=15071 Ack=1 Win=249 Len=1370
18	1.664327	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	SSLV2	1444	
19	1.664414	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	74	34601 → 443 [ACK] Seq=1 Ack=17811 Win=8262 Len=0
20	1.666891	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	SSLV2	2814	
21	1.666971	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	74	34601 → 443 [ACK] Seq=1 Ack=21921 Win=8262 Len=0
23	1.993905	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	SSLV2	1444	
24	2.012383	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	1444	443 → 34601 [ACK] Seq=23291 Ack=1 Win=249 Len=1370
25	2.012383	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	SSLV2	1444	
26	2.012489	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	2409:4071:4eca:4cd6::2a0e:6b40:20:106:20	TCP	74	34601 → 443 [ACK] Seq=1 Ack=26031 Win=8262 Len=0

Frame 13: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Dev
Ethernet II, Src: HonHaiPrecis_05:1e:a7 (e8:9e:b4:05:1e:a7), Dst: ae:2d:96:be:15:56 (ae:2d:96:be:15:56)
Internet Protocol Version 6, Src: 2409:4071:4eca:4cd6::2a0e:6b40:20:106:20, Dst: 2409:4071:4eca:4cd6::2a0e:6b40:20:106:20
Transmission Control Protocol, Src Port: 34601, Dst Port: 443, Seq: 1, Ack: 12331, Len: 0

0000 ae 2d 96 be 15 56 e8 9e b4 05 1e a7 86 dd 60 08V...
0010 43 c0 00 20 06 3f 24 09 40 71 4e ca 4c d6 c1 15 C...?S...
0020 16 60 36 b4 fd 3a 2a 0e 65 40 00 20 01 06 02 0c '6...:..@...
0030 29 ff fe 67 cb b5 87 29 01 bb c9 65 07 71 ba 1c):g...:...e...
0040 a3 87 80 10 20 46 29 3c 00 00 01 01 05 0a ba 1cF)<.....
0050 b3 95 ba 1c b8 ef

summary

The packet capture indicates normal browsing behavior with one suspicious outbound connections to unknown IP addresses over port 35579. Multiple DNS queries were responded, some SYN packets and repeated TCP ACK packets suggest a potential port scan or successful connection attempt. No data exfiltration was observed.

The image shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane displays several packets, with packet 12640 selected. The packet details pane shows the structure of packet 12640, which is a TCP RST, ACK packet.

No.	Time	Source	Destination	Protocol	Length	Info
12640	48.088152	10.188.77.4	104.17.209.240	TCP	66	35579 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12697	48.133686	104.17.209.240	10.188.77.4	TCP	66	443 → 35579 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM WS=8192
12698	48.133758	10.188.77.4	104.17.209.240	TCP	54	35579 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
12703	48.134531	10.188.77.4	104.17.209.240	TCP	1424	35579 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1370 [TCP PDU reassembled in 12704]
12704	48.134531	10.188.77.4	104.17.209.240	TLV1.3	453	Client Hello (SNI=siteintercept.qualtrics.com)
12725	48.182399	10.188.77.4	104.17.209.240	TCP	54	35579 → 443 [FIN, ACK] Seq=1770 Ack=1 Win=131328 Len=0
12743	48.223578	104.17.209.240	10.188.77.4	TCP	54	443 → 35579 [ACK] Seq=1 Ack=1371 Win=139264 Len=0
12744	48.235034	104.17.209.240	10.188.77.4	TCP	54	443 → 35579 [ACK] Seq=1 Ack=1770 Win=139264 Len=0
12745	48.235034	104.17.209.240	10.188.77.4	TLV1.3	2794	Server Hello, Change Cipher Spec
12746	48.235086	10.188.77.4	104.17.209.240	TCP	54	35579 → 443 [RST, ACK] Seq=1771 Ack=2741 Win=0 Len=0
12752	48.243397	104.17.209.240	10.188.77.4	TCP	1424	443 → 35579 [ACK] Seq=2741 Ack=1770 Win=139264 Len=1370 [TCP PDU reassembled in 12753]
12753	48.243397	104.17.209.240	10.188.77.4	TLV1.3	417	Application Data
12791	48.275194	104.17.209.240	10.188.77.4	TCP	54	443 → 35579 [FIN, ACK] Seq=4474 Ack=1771 Win=139264 Len=0

Frame 12640: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF{...} Ethernet II, Src: HonHaiPrecis_05:1e:a7 (e8:9e:b4:05:1e:a7), Dst: ae:2d:96:be:15:56 (ae:2d:96:d1:f0:8a:fb:01:bb:45:bf) Internet Protocol Version 4, Src: 10.188.77.4, Dst: 104.17.209.240 Transmission Control Protocol, Src Port: 35579, Dst Port: 443, Seq: 0, Len: 0

0000 ae 2d 96 be 15 56 e8 9e b4 05 1e a7 08 00 45 00V.....E
0010 00 34 31 2d 40 00 00 06 37 d5 0a bc 4d 04 68 11 -41-@...Z...M-h
0020 d1 f0 8a fb 01 bb 45 bf 6a b8 00 00 00 00 80 02E.....
0030 fa f0 a5 2f 00 00 02 04 05 b4 01 03 08 01 01 .../.....
0040 04 02 ..

Attivata Windows