

## CYBER SECURITY INTERNSHIP

### **Task 5 : Capture and Analyze Network Traffic Using Wireshark.**

**Objective:** Capture live network packets and identify basic protocols and traffic types.

**Tools:** Wireshark (free). Deliverables: A packet capture (.pcap) file and a short report of protocols identified

#### **1.Install Wireshark**



## 2.Start capturing on your active network interface

The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 1298, Time 0.540939, Source 192.168.156.151, Destination 192.168.156.151, Protocol TCP, Length 26). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1279	0.500719	192.168.156.151	118.158.219.40	TCP	54	42025 → 51413 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1280	0.500984	192.168.156.151	118.158.219.40	BitTorrent	122	Handshake
1281	0.506268	194.168.169.26	192.168.156.151	TCP	66	6817 → 42019 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=128
1282	0.506543	192.168.156.151	194.168.169.26	TCP	54	42019 → 6817 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1283	0.512433	192.168.156.151	194.168.169.26	TCP	317	42019 → 6817 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=263
1284	0.515295	107.5.129.107	192.168.156.151	UDP	62	24528 → 55375 Len=20
1285	0.515295	172.185.8.23	192.168.156.151	TCP	54	6944 → 41999 [FIN, ACK] Seq=349 Ack=539 Win=64128 Len=0
1286	0.515295	62.93.178.211	192.168.156.151	TCP	340	23864 → 42006 [PSH, ACK] Seq=286 Ack=327 Win=43808 Len=206
1287	0.515625	192.168.156.151	172.185.8.23	TCP	54	41999 → 6944 [ACK] Seq=539 Ack=350 Win=65024 Len=0
1288	0.516241	192.168.156.151	107.5.129.107	UDP	130	55375 → 24528 Len=88
1289	0.516973	192.168.156.151	62.93.178.211	TCP	54	42006 → 23864 [FIN, ACK] Seq=327 Ack=572 Win=64768 Len=0
1290	0.523045	46.4.112.66	192.168.156.151	BitTorrent	171	Handshake
1291	0.523580	192.168.156.151	46.4.112.66	BitTorrent	523	Extended Bitfield, Len:8x41 Unchoke
1292	0.536200	207.6.204.147	192.168.156.151	UDP	67	43144 → 55375 Len=25
1293	0.547139	116.202.214.217	192.168.156.151	UDP	62	56015 → 55375 Len=20
1294	0.547139	116.202.214.217	192.168.156.151	UDP	346	56015 → 55375 Len=304
1295	0.547139	87.58.176.238	192.168.156.151	BitTorrent	247	Extended Have All Port Extended
1296	0.547591	192.168.156.151	116.202.214.217	UDP	62	55375 → 56015 Len=20
1297	0.548444	192.168.156.151	87.58.176.238	TCP	54	41997 → 62004 [FIN, ACK] Seq=543 Ack=262 Win=65024 Len=0
1298	0.540939	192.168.156.151	116.202.214.217	UDP	68	55375 → 56015 Len=26
1299	0.550095	66.107.22.94	192.168.156.151	TCP	66	57910 → 42017 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=128
1300	0.550400	192.168.156.151	66.107.22.94	TCP	54	42017 → 57910 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1301	0.550384	192.168.156.151	66.107.22.94	TCP	306	42017 → 57910 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=252
1302	0.576512	177.116.159.6	192.168.156.151	UDP	62	51413 → 55375 Len=20
1303	0.576885	192.168.156.151	177.116.159.6	UDP	130	55375 → 51413 Len=88
1304	0.583499	192.168.156.151	188.165.197.21	BT-DHT	146	Get_peers Info_hash=d6f9e9cd140c380f38ca2f2a2a770656383b04d

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF{6F158064-F515-4263-A3F2-24C8E287AE86}, 1  
> Ethernet II, Src: ae:31:31:77:7c:c0 (ae:31:31:77:7c:c0), Dst: AzureWaveTec\_e5:06:d5 (2c:3b:70:e5:06:d5)  
> Internet Protocol Version 4, Src: 77.239.102.59, Dst: 192.168.156.151  
> Transmission Control Protocol, Src Port: 12351, Dst Port: 41931, Seq: 1, Ack: 1, Len: 0

## 3.Browse a website or ping a server to generate traffic.

The image shows the Facebook login page in a Microsoft Edge browser. The address bar displays the URL https://www.facebook.com. A notification banner at the top states "Microsoft Edge isn't your default browser" with "Confirm" and "Not now" buttons. The main content area features the Facebook logo, the tagline "Facebook helps you connect and share with the people in your life.", and a login form with fields for "Email address or phone number" and "Password", a "Log in" button, a link for "Forgotten password?", and a "Create new account" button. At the bottom, there is a link to "Create a Page for a celebrity, brand or business."

## Example website: "facebook.com" traffic

The screenshot shows a Wireshark packet capture window titled "Capturing from Wi-Fi". The filter bar at the top is set to "dns.qry.name contains 'facebook.com'". The packet list shows 20 packets, all of which are DNS queries or responses to facebook.com. The packet details pane shows the selected packet (No. 6239) is a Standard query response from 192.168.156.26 to 192.168.156.151. The packet bytes pane shows the raw data of the DNS response, including the query ID, flags, and the answer section containing the IP address 163.70.140.35.

No.	Time	Source	Destination	Protocol	Length	Info
6239	00.595811	192.168.156.151	192.168.156.26	DNS	76	Standard query 0xf834 A www.facebook.com
6248	00.616896	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x2769 HTTPS www.facebook.com
6249	00.617457	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x5efa A www.facebook.com
6250	00.627708	192.168.156.151	192.168.156.26	DNS	76	Standard query 0xf08 HTTPS www.facebook.com
6251	00.628978	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x2477 A www.facebook.com
6252	00.689289	192.168.156.26	192.168.156.151	DNS	121	Standard query response 0xf834 A www.facebook.com CNAME star-mini.c10r.facebook.com A 163.70.140.35
6253	00.689289	192.168.156.26	192.168.156.151	DNS	192	Standard query response 0x2769 HTTPS www.facebook.com CNAME star-mini.c10r.facebook.com HTTPS HTTPS
6254	00.689925	192.168.156.26	192.168.156.151	DNS	121	Standard query response 0x5efa A www.facebook.com CNAME star-mini.c10r.facebook.com A 163.70.140.35
6255	00.691061	192.168.156.26	192.168.156.151	DNS	192	Standard query response 0xf08 HTTPS www.facebook.com CNAME star-mini.c10r.facebook.com HTTPS HTTPS
6256	00.692752	192.168.156.26	192.168.156.151	DNS	121	Standard query response 0x2477 A www.facebook.com CNAME star-mini.c10r.facebook.com A 163.70.140.35
6257	00.697716	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x45a7 A www.facebook.com
6260	00.702700	192.168.156.26	192.168.156.151	DNS	133	Standard query response 0x45a7 A www.facebook.com CNAME star-mini.c10r.facebook.com A 163.70.140.35
6564	01.527540	192.168.156.151	192.168.156.26	DNS	72	Standard query 0x5754 HTTPS facebook.com
6565	01.528176	192.168.156.151	192.168.156.26	DNS	72	Standard query 0x0531 A facebook.com
6567	01.547277	192.168.156.26	192.168.156.151	DNS	159	Standard query response 0x5754 HTTPS facebook.com HTTPS HTTPS
6570	01.564217	192.168.156.26	192.168.156.151	DNS	88	Standard query response 0x0531 A facebook.com A 163.70.140.35
12932	183.426812	192.168.156.151	192.168.156.26	DNS	90	Standard query 0xbc81 HTTPS www.facebook.com
12934	183.427294	192.168.156.151	192.168.156.26	DNS	88	Standard query 0x2e64 A www.facebook.com
12909	185.194760	192.168.156.151	192.168.156.26	DNS	90	Standard query 0xc816 HTTPS www.facebook.com
12990	185.195826	192.168.156.151	192.168.156.26	DNS	90	Standard query 0x981d A www.facebook.com
13098	188.753376	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x152c A www.facebook.com
13157	189.762226	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x152c A www.facebook.com
13207	190.775570	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x152c A www.facebook.com
13294	192.785163	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x152c A www.facebook.com
13438	196.788755	192.168.156.151	192.168.156.26	DNS	76	Standard query 0x152c A www.facebook.com

> Frame 6239: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF...  
> Ethernet II, Src: AzurelWaveTec\_e5:06:d5 (2c:3b:70:e5:06:d5), Dst: ae:31:31:77:7c:c0 (ae:31:31:77:7c:c0)  
> Internet Protocol Version 4, Src: 192.168.156.151, Dst: 192.168.156.26  
> User Datagram Protocol, Src Port: 53855, Dst Port: 53  
> Domain Name System (query)

## 4. Stop capture after a minute

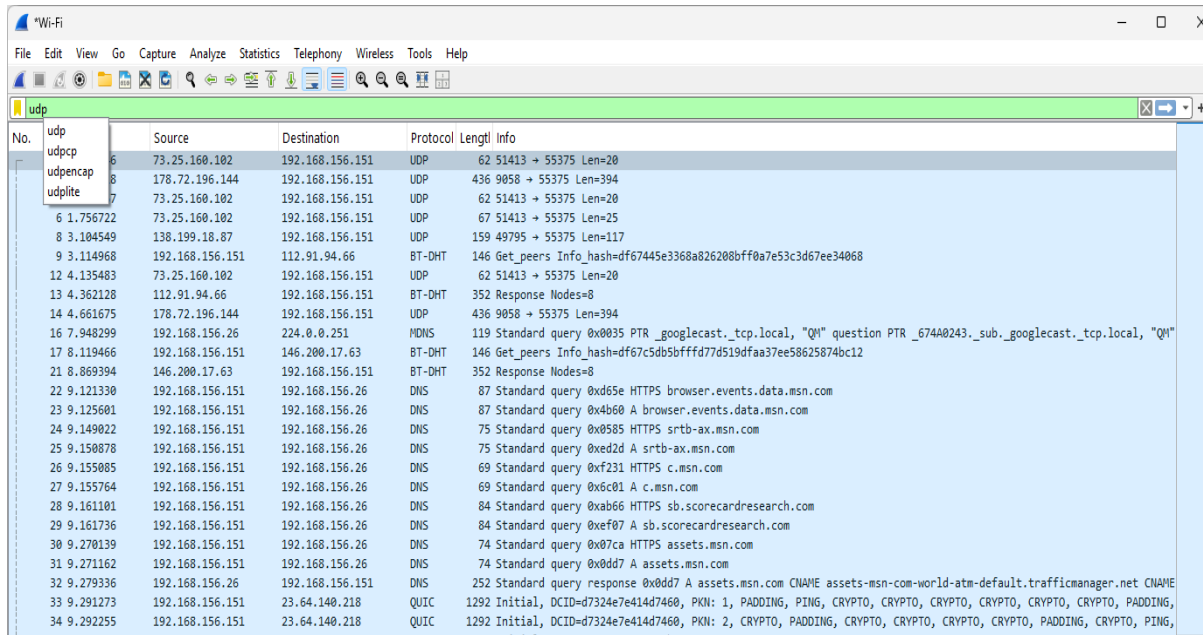
## 5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP)

### a. HTTP

The screenshot shows a Wireshark packet capture window titled "Wi-Fi". The filter bar at the top is set to "http". The packet list shows 2 packets, both of which are HTTP GET requests. The packet details pane shows the selected packet (No. 5454) is a GET request for /captiveportal/generate\_204 from 192.168.156.151 to 150.171.74.11. The packet bytes pane shows the raw data of the HTTP request, including the method, URI, and headers.

No.	Time	Source	Destination	Protocol	Length	Info
5454	70.063593	192.168.156.151	150.171.74.11	HTTP	622	GET /captiveportal/generate_204 HTTP/1.1
5625	78.270832	150.171.74.11	192.168.156.151	HTTP	313	HTTP/1.1 204 No Content

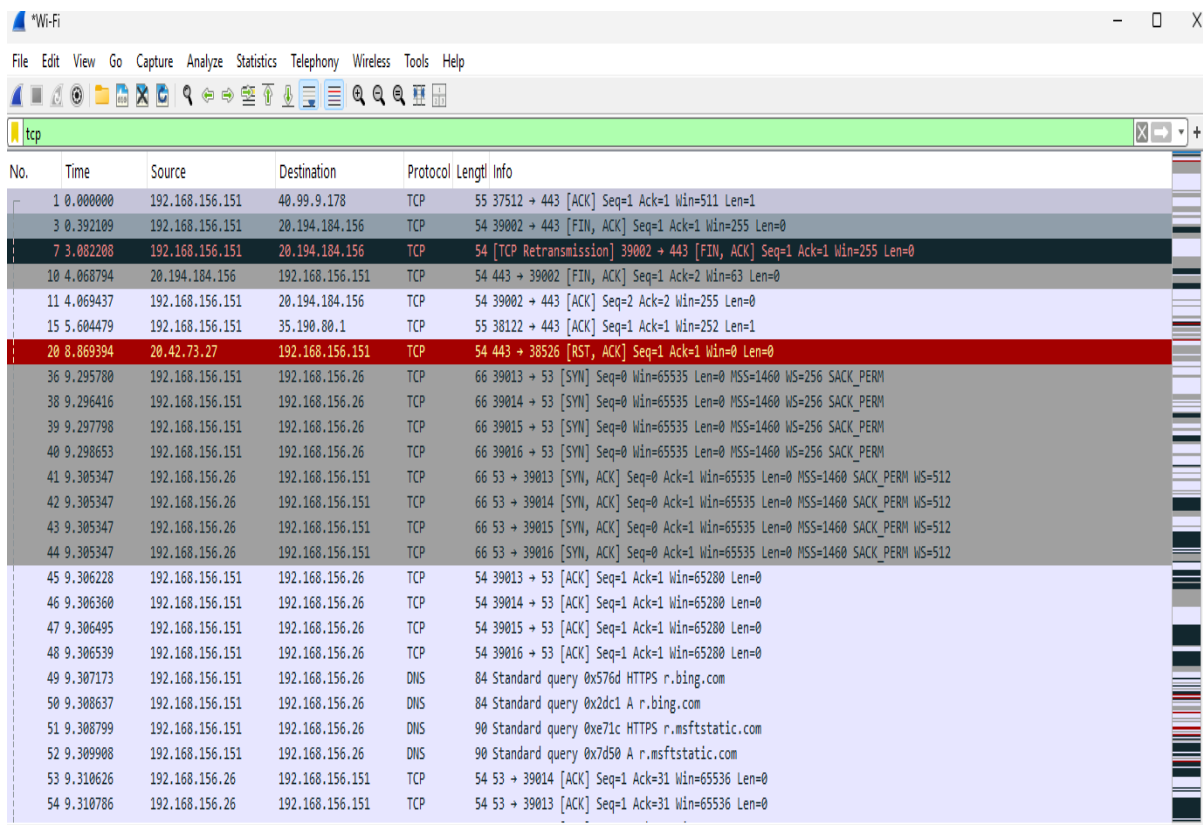
## b.UDP



A screenshot of the Wireshark network protocol analyzer showing a capture of UDP traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a packet list pane on the left. The main packet details pane shows the selected packet (No. 34) with its source (192.168.156.151) and destination (23.64.140.218) IP addresses, and the protocol (QUIC). The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.156.151	40.99.9.178	TCP	55	37512 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1
3	0.392109	192.168.156.151	20.194.184.156	TCP	54	39002 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
7	3.082208	192.168.156.151	20.194.184.156	TCP	54	[TCP Retransmission] 39002 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
10	4.068794	20.194.184.156	192.168.156.151	TCP	54	443 → 39002 [FIN, ACK] Seq=1 Ack=2 Win=63 Len=0
11	4.069437	192.168.156.151	20.194.184.156	TCP	54	39002 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
15	5.604479	192.168.156.151	35.190.80.1	TCP	55	38122 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
20	8.069394	20.42.73.27	192.168.156.151	TCP	54	443 → 38526 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	9.295780	192.168.156.151	192.168.156.26	TCP	66	39013 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
38	9.296416	192.168.156.151	192.168.156.26	TCP	66	39014 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
39	9.297798	192.168.156.151	192.168.156.26	TCP	66	39015 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
40	9.298653	192.168.156.151	192.168.156.26	TCP	66	39016 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
41	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39013 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
42	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39014 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
43	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39015 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
44	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39016 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
45	9.306228	192.168.156.151	192.168.156.26	TCP	54	39013 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
46	9.306360	192.168.156.151	192.168.156.26	TCP	54	39014 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
47	9.306495	192.168.156.151	192.168.156.26	TCP	54	39015 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
48	9.306539	192.168.156.151	192.168.156.26	TCP	54	39016 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
49	9.307173	192.168.156.151	192.168.156.26	DNS	84	Standard query 0x576d HTTPS r.bing.com
50	9.308637	192.168.156.151	192.168.156.26	DNS	84	Standard query 0x2dc1 A r.bing.com
51	9.308799	192.168.156.151	192.168.156.26	DNS	90	Standard query 0xe71c HTTPS r.msftstatic.com
52	9.308908	192.168.156.151	192.168.156.26	DNS	90	Standard query 0x7d50 A r.msftstatic.com
53	9.310626	192.168.156.26	192.168.156.151	TCP	54	53 → 39014 [ACK] Seq=1 Ack=31 Win=65536 Len=0
54	9.310786	192.168.156.26	192.168.156.151	TCP	54	53 → 39013 [ACK] Seq=1 Ack=31 Win=65536 Len=0

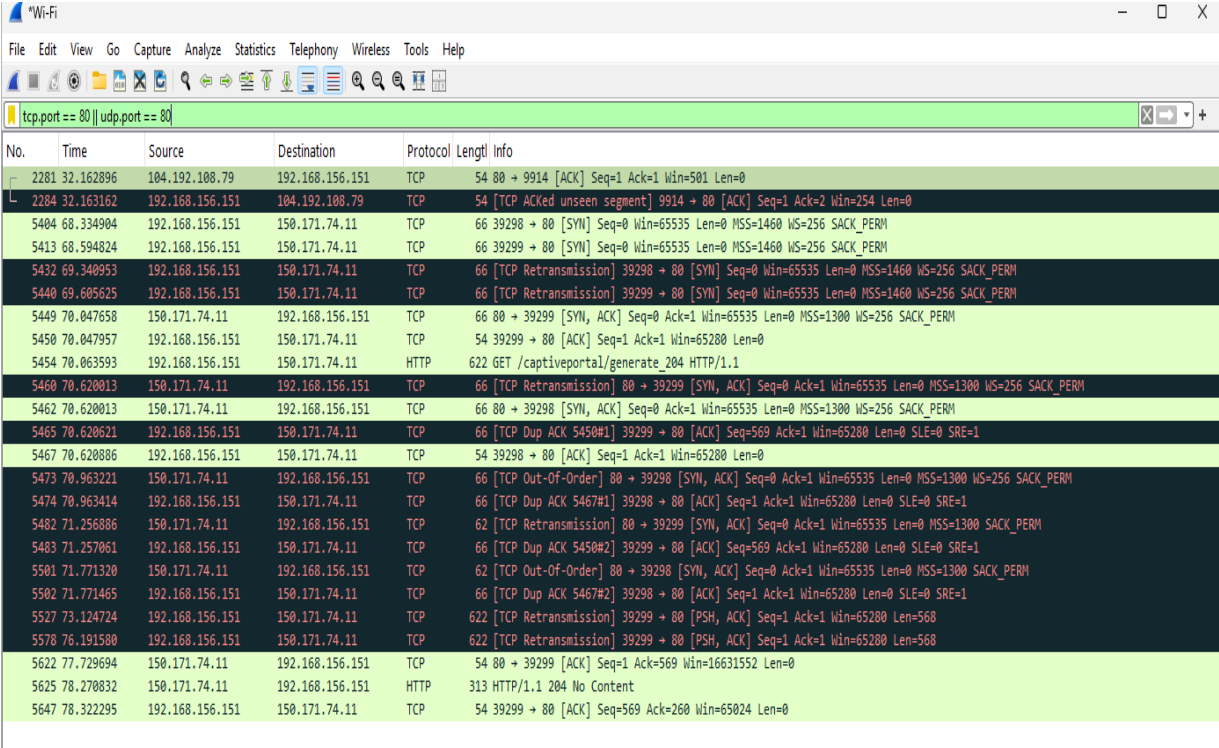
## c.TCP



A screenshot of the Wireshark network protocol analyzer showing a capture of TCP traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a packet list pane on the left. The main packet details pane shows the selected packet (No. 20) with its source (20.42.73.27) and destination (192.168.156.151) IP addresses, and the protocol (TCP). The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.156.151	40.99.9.178	TCP	55	37512 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1
3	0.392109	192.168.156.151	20.194.184.156	TCP	54	39002 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
7	3.082208	192.168.156.151	20.194.184.156	TCP	54	[TCP Retransmission] 39002 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
10	4.068794	20.194.184.156	192.168.156.151	TCP	54	443 → 39002 [FIN, ACK] Seq=1 Ack=2 Win=63 Len=0
11	4.069437	192.168.156.151	20.194.184.156	TCP	54	39002 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
15	5.604479	192.168.156.151	35.190.80.1	TCP	55	38122 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
20	8.069394	20.42.73.27	192.168.156.151	TCP	54	443 → 38526 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	9.295780	192.168.156.151	192.168.156.26	TCP	66	39013 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
38	9.296416	192.168.156.151	192.168.156.26	TCP	66	39014 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
39	9.297798	192.168.156.151	192.168.156.26	TCP	66	39015 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
40	9.298653	192.168.156.151	192.168.156.26	TCP	66	39016 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
41	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39013 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
42	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39014 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
43	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39015 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
44	9.305347	192.168.156.26	192.168.156.151	TCP	66	53 → 39016 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
45	9.306228	192.168.156.151	192.168.156.26	TCP	54	39013 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
46	9.306360	192.168.156.151	192.168.156.26	TCP	54	39014 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
47	9.306495	192.168.156.151	192.168.156.26	TCP	54	39015 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
48	9.306539	192.168.156.151	192.168.156.26	TCP	54	39016 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
49	9.307173	192.168.156.151	192.168.156.26	DNS	84	Standard query 0x576d HTTPS r.bing.com
50	9.308637	192.168.156.151	192.168.156.26	DNS	84	Standard query 0x2dc1 A r.bing.com
51	9.308799	192.168.156.151	192.168.156.26	DNS	90	Standard query 0xe71c HTTPS r.msftstatic.com
52	9.308908	192.168.156.151	192.168.156.26	DNS	90	Standard query 0x7d50 A r.msftstatic.com
53	9.310626	192.168.156.26	192.168.156.151	TCP	54	53 → 39014 [ACK] Seq=1 Ack=31 Win=65536 Len=0
54	9.310786	192.168.156.26	192.168.156.151	TCP	54	53 → 39013 [ACK] Seq=1 Ack=31 Win=65536 Len=0

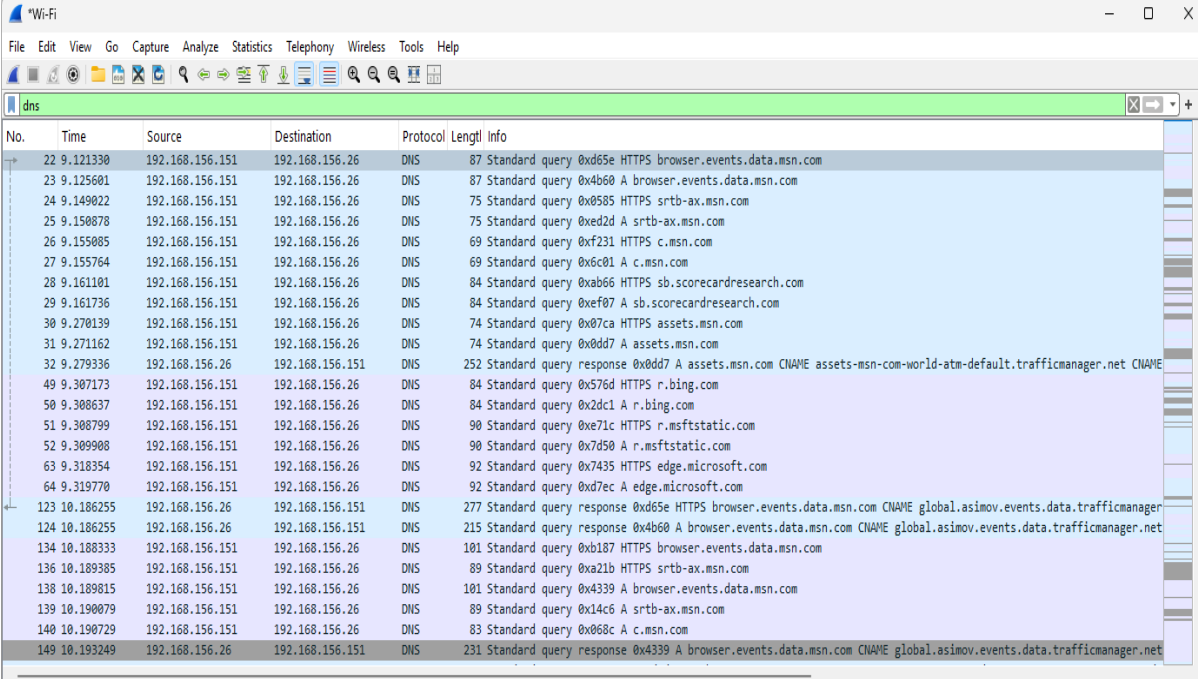
## d.tcp.port == 80 || udp.port == 80



Wi-Fi network traffic capture window showing a list of packets filtered by 'tcp.port == 80 || udp.port == 80'. The table displays packet details including No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
2281	32.162896	104.192.108.79	192.168.156.151	TCP	54	80 → 9914 [ACK] Seq=1 Ack=1 Win=501 Len=0
2284	32.163162	192.168.156.151	104.192.108.79	TCP	54	[TCP ACKed unseen segment] 9914 → 80 [ACK] Seq=1 Ack=2 Win=254 Len=0
5404	68.334984	192.168.156.151	150.171.74.11	TCP	66	39298 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
5413	68.594824	192.168.156.151	150.171.74.11	TCP	66	39299 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
5432	69.340953	192.168.156.151	150.171.74.11	TCP	66	[TCP Retransmission] 39298 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
5440	69.605625	192.168.156.151	150.171.74.11	TCP	66	[TCP Retransmission] 39299 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
5449	70.047658	150.171.74.11	192.168.156.151	TCP	66	80 → 39299 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
5450	70.047957	192.168.156.151	150.171.74.11	TCP	54	39299 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
5454	70.063593	192.168.156.151	150.171.74.11	HTTP	622	GET /captiveportal/generate_204 HTTP/1.1
5460	70.620013	150.171.74.11	192.168.156.151	TCP	66	[TCP Retransmission] 80 → 39299 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
5462	70.620013	150.171.74.11	192.168.156.151	TCP	66	80 → 39298 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
5465	70.620621	192.168.156.151	150.171.74.11	TCP	66	[TCP Dup ACK 5450#1] 39299 → 80 [ACK] Seq=569 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
5467	70.620886	192.168.156.151	150.171.74.11	TCP	54	39298 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
5473	70.963221	150.171.74.11	192.168.156.151	TCP	66	[TCP Out-Of-Order] 80 → 39298 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
5474	70.963414	192.168.156.151	150.171.74.11	TCP	66	[TCP Dup ACK 5467#1] 39298 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
5482	71.256886	150.171.74.11	192.168.156.151	TCP	62	[TCP Retransmission] 80 → 39299 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM
5483	71.257061	192.168.156.151	150.171.74.11	TCP	66	[TCP Dup ACK 5450#2] 39299 → 80 [ACK] Seq=569 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
5501	71.771320	150.171.74.11	192.168.156.151	TCP	62	[TCP Out-Of-Order] 80 → 39298 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM
5502	71.771465	192.168.156.151	150.171.74.11	TCP	66	[TCP Dup ACK 5467#2] 39298 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
5527	73.124724	192.168.156.151	150.171.74.11	TCP	622	[TCP Retransmission] 39299 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=568
5578	76.191580	192.168.156.151	150.171.74.11	TCP	622	[TCP Retransmission] 39299 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=568
5622	77.729694	150.171.74.11	192.168.156.151	TCP	54	80 → 39299 [ACK] Seq=1 Ack=569 Win=16631552 Len=0
5625	78.270832	150.171.74.11	192.168.156.151	HTTP	313	HTTP/1.1 204 No Content
5647	78.322295	192.168.156.151	150.171.74.11	TCP	54	39299 → 80 [ACK] Seq=569 Ack=260 Win=65024 Len=0

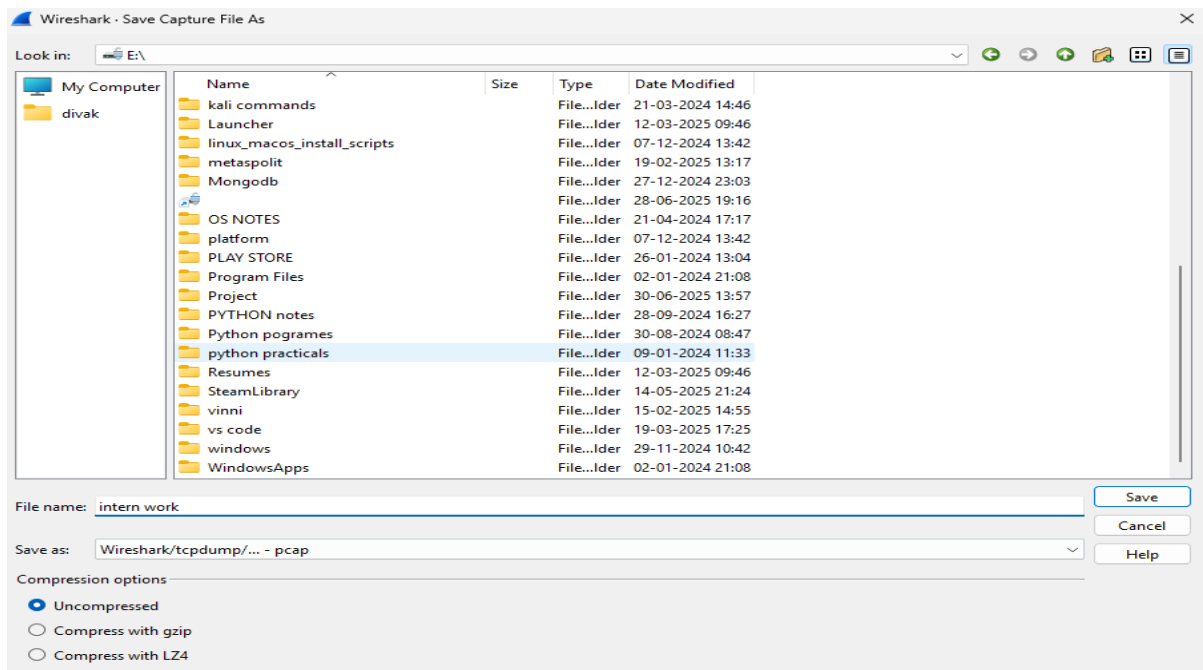
## e.DNS



Wi-Fi network traffic capture window showing a list of DNS packets. The table displays packet details including No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
22	9.121330	192.168.156.151	192.168.156.26	DNS	87	Standard query 0xd65e HTTPS browser.events.data.msn.com
23	9.125601	192.168.156.151	192.168.156.26	DNS	87	Standard query 0x4b60 A browser.events.data.msn.com
24	9.149022	192.168.156.151	192.168.156.26	DNS	75	Standard query 0x0585 HTTPS srtb-ax.msn.com
25	9.150878	192.168.156.151	192.168.156.26	DNS	75	Standard query 0xed2d A srtb-ax.msn.com
26	9.155085	192.168.156.151	192.168.156.26	DNS	69	Standard query 0xf231 HTTPS c.msn.com
27	9.155764	192.168.156.151	192.168.156.26	DNS	69	Standard query 0xc081 A c.msn.com
28	9.161101	192.168.156.151	192.168.156.26	DNS	84	Standard query 0xab66 HTTPS sb.scorecardresearch.com
29	9.161736	192.168.156.151	192.168.156.26	DNS	84	Standard query 0xef07 A sb.scorecardresearch.com
30	9.270139	192.168.156.151	192.168.156.26	DNS	74	Standard query 0x07ca HTTPS assets.msn.com
31	9.271162	192.168.156.151	192.168.156.26	DNS	74	Standard query 0x0dd7 A assets.msn.com
32	9.279336	192.168.156.26	192.168.156.151	DNS	252	Standard query response 0x0dd7 A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME
49	9.307173	192.168.156.151	192.168.156.26	DNS	84	Standard query 0x576d HTTPS r.bing.com
50	9.308637	192.168.156.151	192.168.156.26	DNS	84	Standard query 0x2dc1 A r.bing.com
51	9.308799	192.168.156.151	192.168.156.26	DNS	90	Standard query 0xe71c HTTPS r.msftstatic.com
52	9.309908	192.168.156.151	192.168.156.26	DNS	90	Standard query 0x7d50 A r.msftstatic.com
63	9.318354	192.168.156.151	192.168.156.26	DNS	92	Standard query 0x7435 HTTPS edge.microsoft.com
64	9.319770	192.168.156.151	192.168.156.26	DNS	92	Standard query 0xd7ec A edge.microsoft.com
123	10.186255	192.168.156.26	192.168.156.151	DNS	277	Standard query response 0xd65e HTTPS browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager
124	10.186255	192.168.156.26	192.168.156.151	DNS	215	Standard query response 0x4b60 A browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net
134	10.188333	192.168.156.151	192.168.156.26	DNS	101	Standard query 0xb187 HTTPS browser.events.data.msn.com
136	10.189385	192.168.156.151	192.168.156.26	DNS	89	Standard query 0xa21b HTTPS srtb-ax.msn.com
138	10.189815	192.168.156.151	192.168.156.26	DNS	101	Standard query 0x4339 A browser.events.data.msn.com
139	10.190079	192.168.156.151	192.168.156.26	DNS	89	Standard query 0x14c6 A srtb-ax.msn.com
140	10.190729	192.168.156.151	192.168.156.26	DNS	83	Standard query 0x068c A c.msn.com
149	10.193249	192.168.156.26	192.168.156.151	DNS	231	Standard query response 0x4339 A browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net

## 7.Export the capture as a .pcap file.



## 8. findings and packet details.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
▼ Frame	100.0	8080	100.0	3080196	273 k	0	0	0	8080
▼ Ethernet	100.0	8080	3.7	113120	10 k	0	0	0	8080
▼ Internet Protocol Version 4	100.0	8078	5.2	161560	14 k	0	0	0	8078
▼ User Datagram Protocol	20.1	1627	0.4	13016	1157	0	0	0	1627
QUIC IETF	15.4	1244	25.9	797354	70 k	1244	781921	69 k	1296
Multicast Domain Name System	0.1	5	0.0	385	34	5	385	34	5
Domain Name System	1.7	141	0.3	8952	795	141	8952	795	141
Data	2.6	207	0.8	25304	2249	207	25304	2249	207
BitTorrent DHT Protocol	0.4	30	0.1	4251	377	30	4251	377	30
▼ Transmission Control Protocol	79.8	6451	4.6	142792	12 k	5099	115668	10 k	6451
XMPP Protocol	0.0	1	0.1	1995	177	1	1995	177	1
X11	0.0	3	0.0	1280	113	3	96	8	40
Transport Layer Security	8.2	663	34.3	1056272	93 k	663	766380	68 k	709
Hypertext Transfer Protocol	0.0	2	0.0	827	73	2	827	73	2
Domain Name System	3.1	252	0.8	24763	2201	252	24763	2201	252
Data	2.9	235	2.1	63428	5639	235	63428	5639	235
BitTorrent	2.4	196	1.1	34188	3039	196	12050	1071	446
Address Resolution Protocol	0.0	2	0.0	56	4	2	56	4	2

