

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

### 1. Objective

To capture live network packets using Wireshark and identify different network protocols and traffic types.

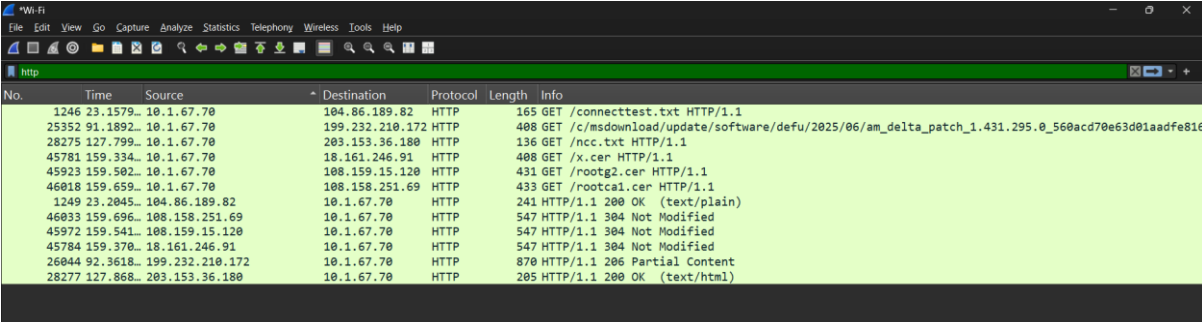
### 2.Tools Used:

- Wireshark(for capturing network packets)
- Chrome browser(for generating https requests)

### 3.Process:

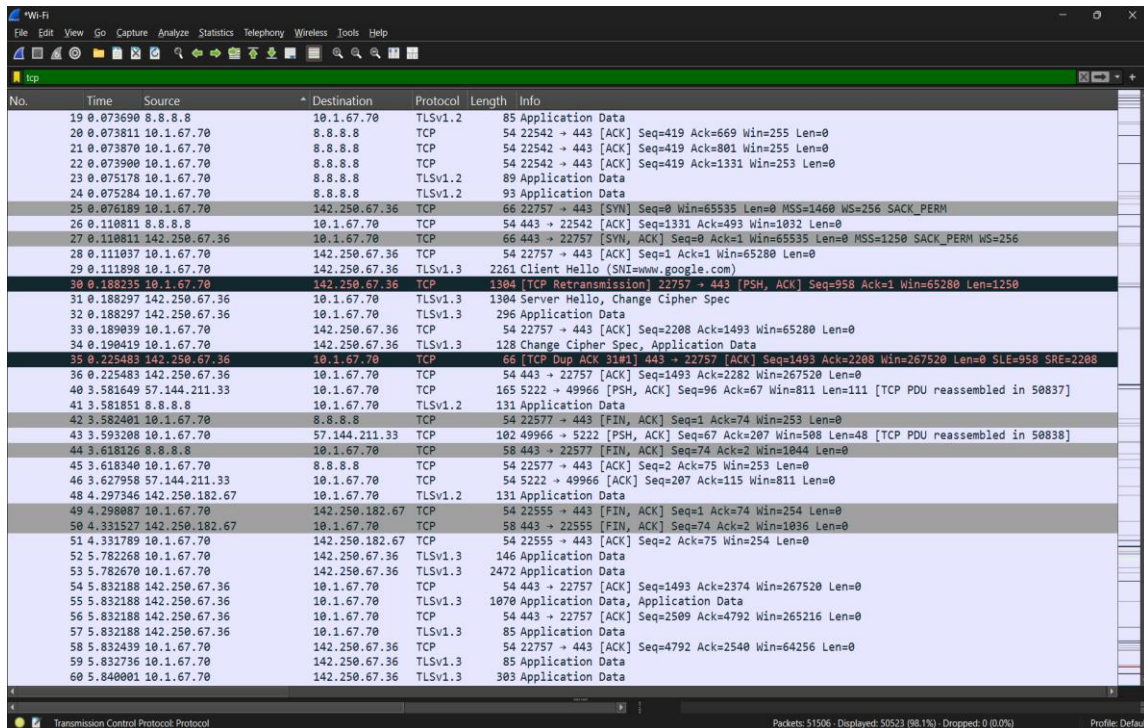
1. Download wireshark
2. Select the active network interface(wifi, ethernet-2,)
3. Start capturing packets
4. Visit any websites for generating traffic.
5. Stop the capture after some period of time.
6. Wireshark has a filter option that helps users focus on specific types of packets, such as HTTP or DNS, for easier analysis.( Note: Filter keywords must be written in lowercase letters (e.g., use http, not HTTP)).
7. Apply filters such as http, dns, tcp.
8. Export the packets and save them using .pcap extension.

### Applied http protocol:



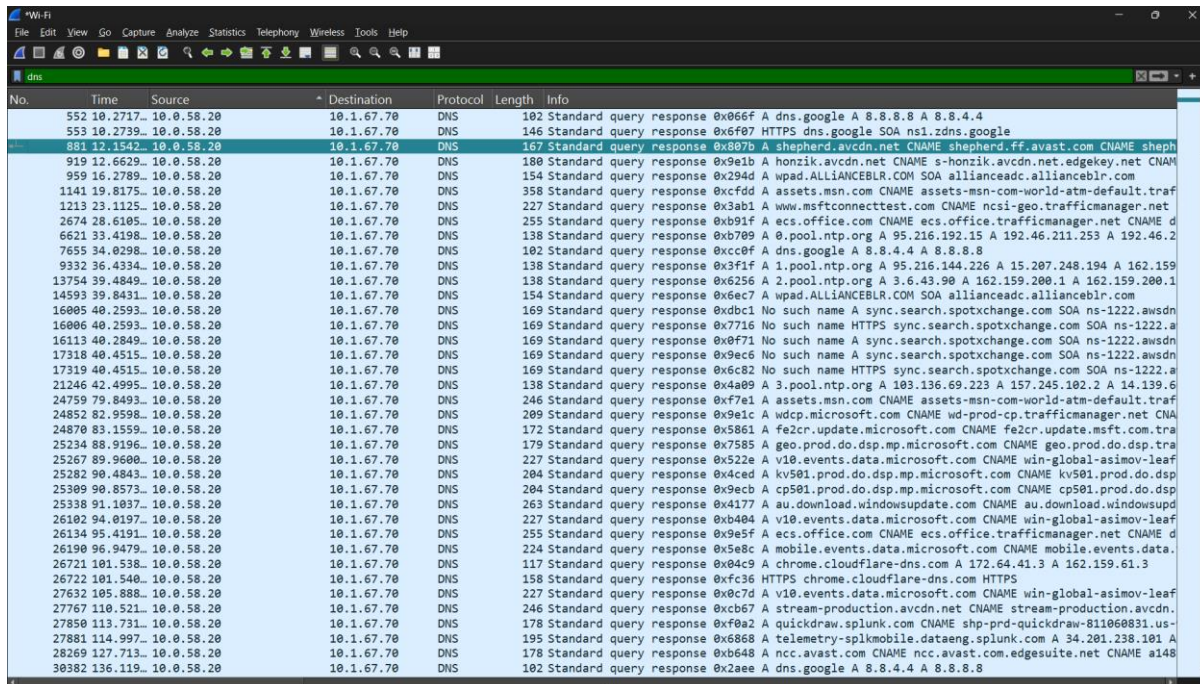
No.	Time	Source	Destination	Protocol	Length	Info
1246	23.1579...	10.1.67.70	104.86.189.82	HTTP	165	GET /connecttest.txt HTTP/1.1
25352	91.1892...	10.1.67.70	199.232.210.172	HTTP	408	GET /c/msdownload/update/software/defu/2025/06/am_delta_patch_1.431.295.0_560acd70e63d01aadfe816
28275	127.799...	10.1.67.70	203.153.36.180	HTTP	136	GET /ncc.txt HTTP/1.1
45781	159.334...	10.1.67.70	18.161.246.91	HTTP	408	GET /x.cer HTTP/1.1
45923	159.502...	10.1.67.70	108.159.15.120	HTTP	431	GET /rootg2.cer HTTP/1.1
46018	159.659...	10.1.67.70	108.158.251.69	HTTP	433	GET /rootca1.cer HTTP/1.1
1249	23.2045...	104.86.189.82	10.1.67.70	HTTP	241	HTTP/1.1 200 OK (text/plain)
46033	159.696...	108.158.251.69	10.1.67.70	HTTP	547	HTTP/1.1 304 Not Modified
45972	159.541...	108.159.15.120	10.1.67.70	HTTP	547	HTTP/1.1 304 Not Modified
45784	159.370...	18.161.246.91	10.1.67.70	HTTP	547	HTTP/1.1 304 Not Modified
26044	92.3618...	199.232.210.172	10.1.67.70	HTTP	870	HTTP/1.1 206 Partial Content
28277	127.068...	203.153.36.180	10.1.67.70	HTTP	205	HTTP/1.1 200 OK (text/html)

## Applied tcp protocol:



No.	Time	Source	Destination	Protocol	Length	Info
19	0.073690	8.8.8.8	10.1.67.70	TLSv1.2	85	Application Data
20	0.073811	10.1.67.70	8.8.8.8	TCP	54	22542 → 443 [ACK] Seq=419 Ack=669 Win=255 Len=0
21	0.073870	10.1.67.70	8.8.8.8	TCP	54	22542 → 443 [ACK] Seq=419 Ack=801 Win=255 Len=0
22	0.073900	10.1.67.70	8.8.8.8	TCP	54	22542 → 443 [ACK] Seq=419 Ack=1331 Win=253 Len=0
23	0.075178	10.1.67.70	8.8.8.8	TLSv1.2	89	Application Data
24	0.075284	10.1.67.70	8.8.8.8	TLSv1.2	93	Application Data
25	0.076189	10.1.67.70	142.250.67.36	TCP	66	22757 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
26	0.110811	8.8.8.8	10.1.67.70	TCP	54	443 → 22542 [ACK] Seq=1331 Ack=493 Win=1032 Len=0
27	0.110811	142.250.67.36	10.1.67.70	TCP	66	443 → 22757 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM WS=256
28	0.110837	10.1.67.70	142.250.67.36	TCP	54	22757 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
29	0.111898	10.1.67.70	142.250.67.36	TLSv1.3	2261	Client Hello (SNI=www.google.com)
30	0.188235	10.1.67.70	142.250.67.36	TCP	1304	[TCP Retransmission] 22757 → 443 [PSH, ACK] Seq=958 Ack=1 Win=65280 Len=1250
31	0.188297	142.250.67.36	10.1.67.70	TLSv1.3	1304	Server Hello, Change Cipher Spec
32	0.188297	142.250.67.36	10.1.67.70	TLSv1.3	296	Application Data
33	0.189039	10.1.67.70	142.250.67.36	TCP	54	22757 → 443 [ACK] Seq=2208 Ack=1493 Win=65280 Len=0
34	0.190419	10.1.67.70	142.250.67.36	TLSv1.3	128	Change Cipher Spec, Application Data
35	0.225483	142.250.67.36	10.1.67.70	TCP	66	[TCP Dup ACK 31#1] 443 → 22757 [ACK] Seq=1493 Ack=2208 Win=267520 Len=0 SLE=958 SRE=2208
36	0.225483	142.250.67.36	10.1.67.70	TCP	54	443 → 22757 [ACK] Seq=1493 Ack=2282 Win=267520 Len=0
40	3.581649	57.144.211.33	10.1.67.70	TCP	165	5222 → 49966 [PSH, ACK] Seq=96 Ack=67 Win=811 Len=111 [TCP PDU reassembled in 50837]
41	3.581851	8.8.8.8	10.1.67.70	TLSv1.2	131	Application Data
42	3.582481	10.1.67.70	8.8.8.8	TCP	54	22577 → 443 [FIN, ACK] Seq=1 Ack=74 Win=253 Len=0
43	3.593208	10.1.67.70	57.144.211.33	TCP	102	49966 → 5222 [PSH, ACK] Seq=67 Ack=207 Win=508 Len=48 [TCP PDU reassembled in 50838]
44	3.618126	8.8.8.8	10.1.67.70	TCP	58	443 → 22577 [FIN, ACK] Seq=74 Ack=2 Win=1844 Len=0
45	3.618340	10.1.67.70	8.8.8.8	TCP	54	22577 → 443 [ACK] Seq=2 Ack=75 Win=253 Len=0
46	3.627958	57.144.211.33	10.1.67.70	TCP	54	5222 → 49966 [ACK] Seq=207 Ack=115 Win=811 Len=0
48	4.297346	142.250.182.67	10.1.67.70	TLSv1.2	131	Application Data
49	4.298087	10.1.67.70	142.250.182.67	TCP	54	22555 → 443 [FIN, ACK] Seq=1 Ack=74 Win=254 Len=0
50	4.331527	142.250.182.67	10.1.67.70	TCP	58	443 → 22555 [FIN, ACK] Seq=74 Ack=2 Win=1836 Len=0
51	4.331789	10.1.67.70	142.250.182.67	TCP	54	22555 → 443 [ACK] Seq=2 Ack=75 Win=254 Len=0
52	5.782268	10.1.67.70	142.250.67.36	TLSv1.3	146	Application Data
53	5.782670	10.1.67.70	142.250.67.36	TLSv1.3	2472	Application Data
54	5.832188	142.250.67.36	10.1.67.70	TCP	54	443 → 22757 [ACK] Seq=1493 Ack=2374 Win=267520 Len=0
55	5.832188	142.250.67.36	10.1.67.70	TLSv1.3	1070	Application Data, Application Data
56	5.832188	142.250.67.36	10.1.67.70	TCP	54	443 → 22757 [ACK] Seq=2509 Ack=4792 Win=265216 Len=0
57	5.832188	142.250.67.36	10.1.67.70	TLSv1.3	85	Application Data
58	5.832439	10.1.67.70	142.250.67.36	TCP	54	22757 → 443 [ACK] Seq=4792 Ack=2540 Win=64256 Len=0
59	5.832736	10.1.67.70	142.250.67.36	TLSv1.3	85	Application Data
60	5.840001	10.1.67.70	142.250.67.36	TLSv1.3	303	Application Data

## Applied dns filter:



No.	Time	Source	Destination	Protocol	Length	Info
552	10.2717.	10.0.58.20	10.1.67.70	DNS	102	Standard query response 0x066f A dns.google A 8.8.8.8 A 8.8.4.4
553	10.2739.	10.0.58.20	10.1.67.70	DNS	146	Standard query response 0x6f07 HTTPS dns.google SOA ns1.zdns.google
881	12.1542.	10.0.58.20	10.1.67.70	DNS	167	Standard query response 0x807b A shepherd.avcdn.net CNAME shepherd.ff.avast.com CNAME sheph
919	12.6629.	10.0.58.20	10.1.67.70	DNS	188	Standard query response 0x9e1b A honzik.avcdn.net CNAME s-honzik.avcdn.net.edgekey.net CNAM
959	16.2789.	10.0.58.20	10.1.67.70	DNS	154	Standard query response 0x294d A wpad.ALLIANCEBLR.COM SOA allianceadc.allianceblr.com
1141	19.8175.	10.0.58.20	10.1.67.70	DNS	358	Standard query response 0xcfd5 A assets.msn.com CNAME assets-msn-com-world-atm-default-traf
1213	23.1125.	10.0.58.20	10.1.67.70	DNS	227	Standard query response 0x3ab1 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net
2674	28.6105.	10.0.58.20	10.1.67.70	DNS	255	Standard query response 0xb91f A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME d
6621	33.4198.	10.0.58.20	10.1.67.70	DNS	138	Standard query response 0xb709 A 0.pool.ntp.org A 95.216.192.15 A 192.46.211.253 A 192.46.2
7655	34.0298.	10.0.58.20	10.1.67.70	DNS	102	Standard query response 0xcc0f A dns.google A 8.8.4.4 A 8.8.8.8
9332	36.4334.	10.0.58.20	10.1.67.70	DNS	138	Standard query response 0x3f1f A 1.pool.ntp.org A 95.216.144.226 A 15.207.248.194 A 162.159
13754	39.4849.	10.0.58.20	10.1.67.70	DNS	138	Standard query response 0x6256 A 2.pool.ntp.org A 3.6.43.90 A 162.159.200.1 A 162.159.200.1
14593	39.8431.	10.0.58.20	10.1.67.70	DNS	154	Standard query response 0x6ec7 A wpad.ALLIANCEBLR.COM SOA allianceadc.allianceblr.com
16005	40.2593.	10.0.58.20	10.1.67.70	DNS	169	Standard query response 0x0bc1 No such name A sync.search.spotxchange.com SOA ns-1222.avs
16006	40.2593.	10.0.58.20	10.1.67.70	DNS	169	Standard query response 0x7716 No such name HTTPS sync.search.spotxchange.com SOA ns-1222.a
16113	40.2849.	10.0.58.20	10.1.67.70	DNS	169	Standard query response 0x8f71 No such name A sync.search.spotxchange.com SOA ns-1222.avs
17318	40.4515.	10.0.58.20	10.1.67.70	DNS	169	Standard query response 0x9ec6 No such name A sync.search.spotxchange.com SOA ns-1222.avs
17319	40.4515.	10.0.58.20	10.1.67.70	DNS	169	Standard query response 0x6c82 No such name HTTPS sync.search.spotxchange.com SOA ns-1222.a
21246	42.4995.	10.0.58.20	10.1.67.70	DNS	138	Standard query response 0x4a09 A 3.pool.ntp.org A 103.136.69.223 A 157.245.102.2 A 14.139.6
24759	79.8493.	10.0.58.20	10.1.67.70	DNS	246	Standard query response 0xf7e1 A assets.msn.com CNAME assets-msn-com-world-atm-default-traf
24852	82.9598.	10.0.58.20	10.1.67.70	DNS	209	Standard query response 0x9e1c A wdcprod.microsoft.com CNAME wdcprod-cp.trafficmanager.net CNA
24870	83.1559.	10.0.58.20	10.1.67.70	DNS	172	Standard query response 0x5861 A fe2cr.update.microsoft.com CNAME fe2cr.update.msft.com.tra
25234	88.9196.	10.0.58.20	10.1.67.70	DNS	179	Standard query response 0x7585 A geo.prod.do.dsp.mp.microsoft.com CNAME geo.prod.do.dsp.tra
25267	89.9600.	10.0.58.20	10.1.67.70	DNS	227	Standard query response 0x522e A v10.events.data.microsoft.com CNAME win-global-asimov-leaf
25282	90.4843.	10.0.58.20	10.1.67.70	DNS	204	Standard query response 0x4ced A kv501.prod.do.dsp.mp.microsoft.com CNAME kv501.prod.do.dsp
25309	90.8573.	10.0.58.20	10.1.67.70	DNS	204	Standard query response 0x9ecb A cp501.prod.do.dsp.mp.microsoft.com CNAME cp501.prod.do.dsp
25338	91.1037.	10.0.58.20	10.1.67.70	DNS	263	Standard query response 0x4177 A au.download.windowsupdate.com CNAME au.download.windowsup
26102	94.0157.	10.0.58.20	10.1.67.70	DNS	227	Standard query response 0xb404 A v10.events.data.microsoft.com CNAME win-global-asimov-leaf
26134	95.4191.	10.0.58.20	10.1.67.70	DNS	255	Standard query response 0x9e5f A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME d
26190	96.9479.	10.0.58.20	10.1.67.70	DNS	224	Standard query response 0x5e8c A mobile.events.data.microsoft.com CNAME mobile.events.data.
26721	101.538.	10.0.58.20	10.1.67.70	DNS	117	Standard query response 0x04c9 A chrome.cloudflare-dns.com A 172.64.41.3 A 162.159.61.3
26722	101.540.	10.0.58.20	10.1.67.70	DNS	158	Standard query response 0xfc36 HTTPS chrome.cloudflare-dns.com HTTPS
27632	105.888.	10.0.58.20	10.1.67.70	DNS	227	Standard query response 0x0c7d A v10.events.data.microsoft.com CNAME win-global-asimov-leaf
27767	110.521.	10.0.58.20	10.1.67.70	DNS	246	Standard query response 0xc6b7 A stream-production.avcdn.net CNAME stream-production.avcdn.
27850	113.731.	10.0.58.20	10.1.67.70	DNS	178	Standard query response 0xf0a2 A quickdraw.splunk.com CNAME shp-prd-quickdraw-811060831.us-
27881	114.997.	10.0.58.20	10.1.67.70	DNS	195	Standard query response 0x6868 A telemetry-splkmobile.dataeng.splunk.com A 34.201.238.101 A
28269	127.713.	10.0.58.20	10.1.67.70	DNS	178	Standard query response 0xb648 A ncc.avast.com CNAME ncc.avast.com.edgesuite.net CNAME a148
38382	136.119.	10.0.58.20	10.1.67.70	DNS	102	Standard query response 0x2aee A dns.google A 8.8.4.4 A 8.8.8.8