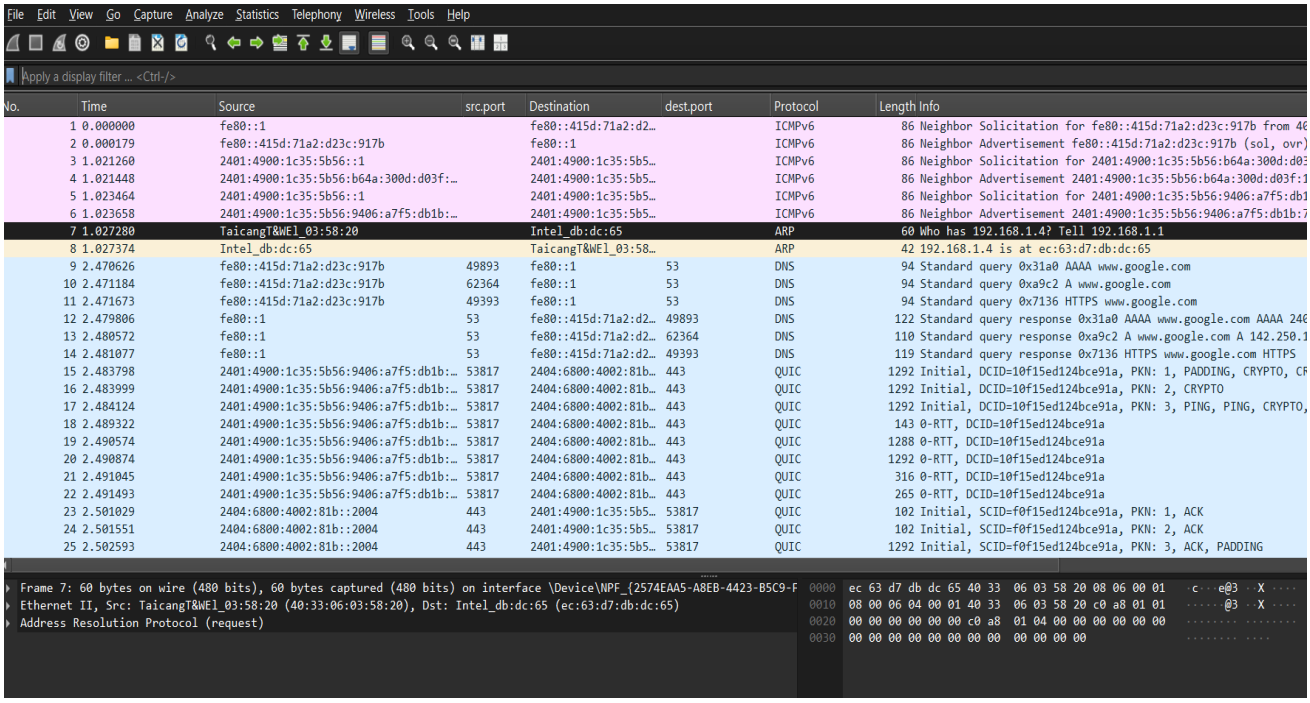
Task 5: Capture and Analyse Network Traffic Using Wireshark.

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

Tools: Wireshark (free).

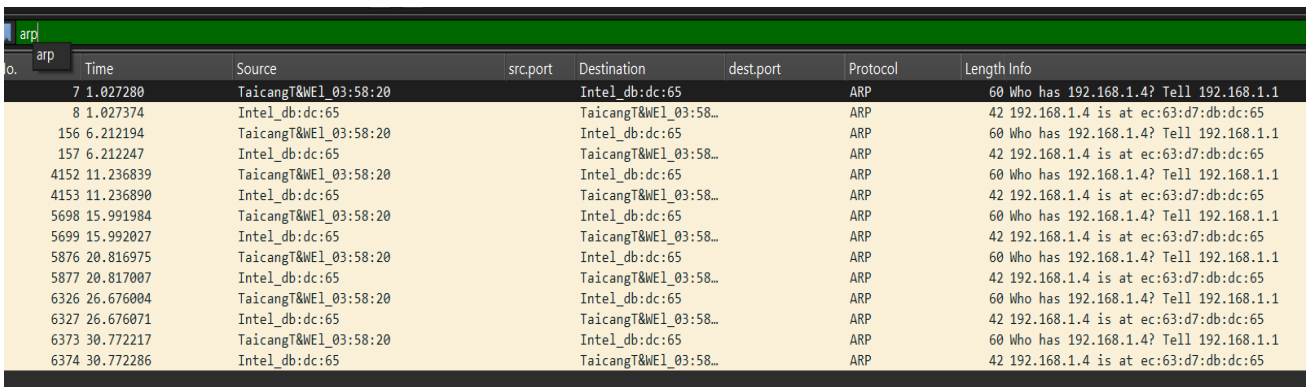
Deliverables: A packet capture (.pcap) file and a short report of protocols identified.

1. All Captured packets:

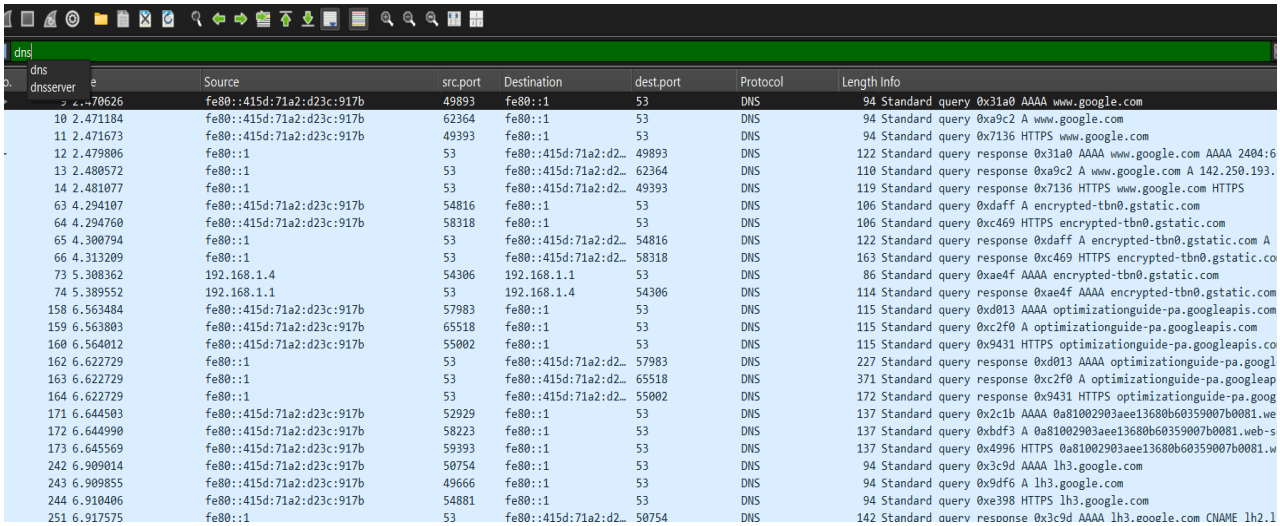


2. Filtering captured packets based on protocols:

a. ARP: Address Resolution Protocol:



b. DNS: Domain Name System

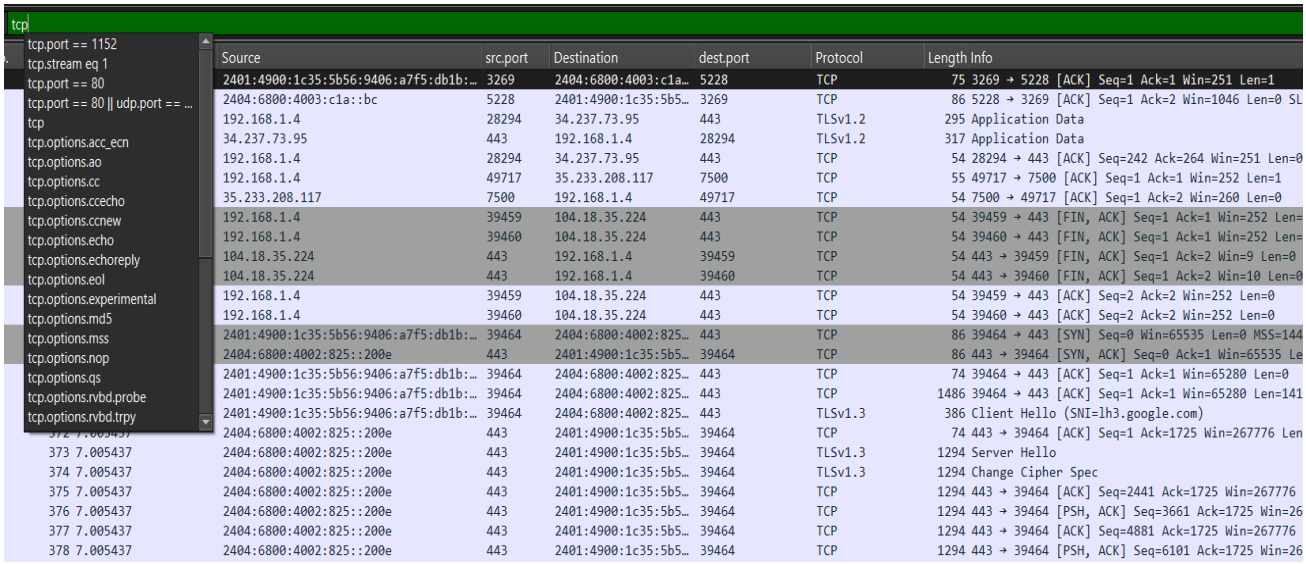


dns

dns
dnsserver

	Source	src.port	Destination	dest.port	Protocol	Length Info
9 2.470626	fe80::415d:71a2:d23c:917b	49893	fe80::1	53	DNS	94 Standard query 0x31a0 AAAA www.google.com
10 2.471184	fe80::415d:71a2:d23c:917b	62364	fe80::1	53	DNS	94 Standard query 0xa9c2 A www.google.com
11 2.471673	fe80::415d:71a2:d23c:917b	49393	fe80::1	53	DNS	94 Standard query 0x7136 HTTPS www.google.com
12 2.479806	fe80::1	53	fe80::415d:71a2:d2…	49893	DNS	122 Standard query response 0x31a0 AAAA www.google.com AAAA 2404:6
13 2.480572	fe80::1	53	fe80::415d:71a2:d2…	62364	DNS	110 Standard query response 0xa9c2 A www.google.com A 142.250.193.
14 2.481077	fe80::1	53	fe80::415d:71a2:d2…	49393	DNS	119 Standard query response 0x7136 HTTPS www.google.com HTTPS
63 4.294107	fe80::415d:71a2:d23c:917b	54816	fe80::1	53	DNS	106 Standard query 0xdaff A encrypted-tbn0.gstatic.com
64 4.294760	fe80::415d:71a2:d23c:917b	58318	fe80::1	53	DNS	106 Standard query 0xc469 HTTPS encrypted-tbn0.gstatic.com
65 4.300794	fe80::1	53	fe80::415d:71a2:d2…	54816	DNS	122 Standard query response 0xdaff A encrypted-tbn0.gstatic.com A
66 4.313209	fe80::1	53	fe80::415d:71a2:d2…	58318	DNS	163 Standard query response 0xc469 HTTPS encrypted-tbn0.gstatic.co
73 5.308362	192.168.1.4	54306	192.168.1.1	53	DNS	86 Standard query 0xae4f AAAA encrypted-tbn0.gstatic.com
74 5.389552	192.168.1.1	53	192.168.1.4	54306	DNS	114 Standard query response 0xae4f AAAA encrypted-tbn0.gstatic.com
158 6.563484	fe80::415d:71a2:d23c:917b	57983	fe80::1	53	DNS	115 Standard query 0xd013 AAAA optimizationguide-pa.googleapis.com
159 6.563803	fe80::415d:71a2:d23c:917b	65518	fe80::1	53	DNS	115 Standard query 0xc2f0 A optimizationguide-pa.googleapis.com
160 6.564012	fe80::415d:71a2:d23c:917b	55002	fe80::1	53	DNS	115 Standard query 0x9431 HTTPS optimizationguide-pa.googleapis.co
162 6.622729	fe80::1	53	fe80::415d:71a2:d2…	57983	DNS	227 Standard query response 0xd013 AAAA optimizationguide-pa.googl
163 6.622729	fe80::1	53	fe80::415d:71a2:d2…	65518	DNS	371 Standard query response 0xc2f0 A optimizationguide-pa.googleap
164 6.622729	fe80::1	53	fe80::415d:71a2:d2…	55002	DNS	172 Standard query response 0x9431 HTTPS optimizationguide-pa.goog
171 6.644503	fe80::415d:71a2:d23c:917b	52929	fe80::1	53	DNS	137 Standard query 0x2c1b AAAA 0a81002903aee13680b60359007b0081.we
172 6.644990	fe80::415d:71a2:d23c:917b	58223	fe80::1	53	DNS	137 Standard query 0xbdf3 A 0a81002903aee13680b60359007b0081.web-s
173 6.645569	fe80::415d:71a2:d23c:917b	59393	fe80::1	53	DNS	137 Standard query 0x4996 HTTPS 0a81002903aee13680b60359007b0081.w
242 6.909014	fe80::415d:71a2:d23c:917b	50754	fe80::1	53	DNS	94 Standard query 0x3c9d AAAA lh3.google.com
243 6.909855	fe80::415d:71a2:d23c:917b	49666	fe80::1	53	DNS	94 Standard query 0x9df6 A lh3.google.com
244 6.910406	fe80::415d:71a2:d23c:917b	54881	fe80::1	53	DNS	94 Standard query 0xe398 HTTPS lh3.google.com
251 6.917575	fe80::1	53	fe80::415d:71a2:d2…	50754	DNS	142 Standard query response 0x3c9d AAAA lh3.google.com CNAME lh2.l

c. TCP: Transmission Control Protocol



tcp

tcp.port == 1152
tcp.stream eq 1
tcp.port == 80
tcp.port == 80 || udp.port == ...
tcp
tcp.options.acc_ecn
tcp.options.ao
tcp.options.cc
tcp.options.ccecho
tcp.options.ccnew
tcp.options.echo
tcp.options.echoreply
tcp.options.eol
tcp.options.experimental
tcp.options.md5
tcp.options.mss
tcp.options.nop
tcp.options.qs
tcp.options.rvbd.probe
tcp.options.rvbd.trpy

	Source	src.port	Destination	dest.port	Protocol	Length Info
	2401:4900:1c35:5b56:9406:a7f5:db1b:…	3269	2404:6800:4003:c1a…	5228	TCP	75 3269 → 5228 [ACK] Seq=1 Ack=1 Win=251 Len=1
	2404:6800:4003:c1a::bc	5228	2401:4900:1c35:5b5…	3269	TCP	86 5228 → 3269 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SL
	192.168.1.4	28294	34.237.73.95	443	TLSv1.2	295 Application Data
	34.237.73.95	443	192.168.1.4	28294	TLSv1.2	317 Application Data
	192.168.1.4	28294	34.237.73.95	443	TCP	54 28294 → 443 [ACK] Seq=242 Ack=264 Win=251 Len=0
	192.168.1.4	49717	35.233.208.117	7500	TCP	55 49717 → 7500 [ACK] Seq=1 Ack=1 Win=252 Len=1
	35.233.208.117	7500	192.168.1.4	49717	TCP	54 7500 → 49717 [ACK] Seq=1 Ack=2 Win=260 Len=0
	192.168.1.4	39459	104.18.35.224	443	TCP	54 39459 → 443 [FIN, ACK] Seq=1 Ack=1 Win=252 Len=
	192.168.1.4	39460	104.18.35.224	443	TCP	54 39460 → 443 [FIN, ACK] Seq=1 Ack=1 Win=252 Len=
	104.18.35.224	443	192.168.1.4	39459	TCP	54 443 → 39459 [FIN, ACK] Seq=1 Ack=2 Win=9 Len=0
	104.18.35.224	443	192.168.1.4	39460	TCP	54 443 → 39460 [FIN, ACK] Seq=1 Ack=2 Win=10 Len=0
	192.168.1.4	39459	104.18.35.224	443	TCP	54 39459 → 443 [ACK] Seq=2 Ack=2 Win=252 Len=0
	192.168.1.4	39460	104.18.35.224	443	TCP	54 39460 → 443 [ACK] Seq=2 Ack=2 Win=252 Len=0
	2401:4900:1c35:5b56:9406:a7f5:db1b:…	39464	2404:6800:4002:825…	443	TCP	86 39464 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=144
	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TCP	86 443 → 39464 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
	2401:4900:1c35:5b56:9406:a7f5:db1b:…	39464	2404:6800:4002:825…	443	TCP	74 39464 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
	2401:4900:1c35:5b56:9406:a7f5:db1b:…	39464	2404:6800:4002:825…	443	TCP	1486 39464 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=141
	2401:4900:1c35:5b56:9406:a7f5:db1b:…	39464	2404:6800:4002:825…	443	TLSv1.3	386 Client Hello (SNI=lh3.google.com)
	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TCP	74 443 → 39464 [ACK] Seq=1 Ack=1725 Win=267776 Len
373 7.005437	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TLSv1.3	1294 Server Hello
374 7.005437	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TLSv1.3	1294 Change Cipher Spec
375 7.005437	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TCP	1294 443 → 39464 [ACK] Seq=2441 Ack=1725 Win=267776
376 7.005437	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TCP	1294 443 → 39464 [PSH, ACK] Seq=3661 Ack=1725 Win=26
377 7.005437	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TCP	1294 443 → 39464 [ACK] Seq=4881 Ack=1725 Win=267776
378 7.005437	2404:6800:4002:825::200e	443	2401:4900:1c35:5b5…	39464	TCP	1294 443 → 39464 [PSH, ACK] Seq=6101 Ack=1725 Win=26

Findings:

a. Arp was used to resolve find mac address related to ip address.
b. DNS was used to resolve the ip address related to the domain.
c. TCP was used to establish a connection between client and server.