

# Computer Network (Lab session -11)

## Wireshark with IP & ICMP protocol

### Q-1) Wireshark Software

**A -> Capture analyze IP protocol message being exchanged.**

**B -> Capture analyze ICMP message being exchanged.**

- ✚ Wireshark is the world's foremost and widely-used network protocol analyzer. We also perform practical on TCP, UDP protocol, DNS services and HTTP response.
- ✚ Now working with IP protocol, that give us the full information about IP address. Like Source address, destination address and IPV6 address.
- ✚ IPv4 is a **32-bit address** in which each group represents 8 bits ranging from 0 to 255.
- ✚ IPv6 is a 128-bit address. Ip.addr gives the all the address where no condition.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.201	5.178.65.245	TCP	55	1083 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
2	0.000196	192.168.43.201	74.118.186.210	TCP	55	1092 → 443 [ACK] Seq=1 Ack=1 Win=63178 Len=1 [TCP segment of a reassembled PDU]
3	0.000337	192.168.43.201	34.98.64.218	TCP	55	1090 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
4	0.000442	192.168.43.201	103.231.98.193	TCP	55	1081 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
5	0.035690	192.168.43.201	13.249.220.101	TCP	55	1079 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
6	0.051631	192.168.43.201	49.44.165.201	TCP	55	1088 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
7	0.051737	192.168.43.201	49.44.165.201	TCP	55	1089 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
8	0.067874	34.98.64.218	192.168.43.201	TCP	66	443 → 1090 [ACK] Seq=1 Ack=2 Win=339 Len=0 SLE=1 SRE=2
9	0.083811	49.44.165.201	192.168.43.201	TCP	66	443 → 1089 [ACK] Seq=1 Ack=2 Win=364 Len=0 SLE=1 SRE=2
10	0.096875	13.249.220.101	192.168.43.201	TCP	66	443 → 1079 [ACK] Seq=1 Ack=2 Win=163 Len=0 SLE=1 SRE=2
11	0.109615	103.231.98.193	192.168.43.201	TCP	54	443 → 1081 [ACK] Seq=1 Ack=2 Win=15272 Len=0
12	0.109867	74.118.186.210	192.168.43.201	TCP	54	443 → 1092 [ACK] Seq=1 Ack=2 Win=16267 Len=0
13	0.185363	5.178.65.245	192.168.43.201	TCP	66	443 → 1083 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
14	0.217261	49.44.165.201	192.168.43.201	TCP	66	443 → 1089 [ACK] Seq=1 Ack=2 Win=348 Len=0 SLE=1 SRE=2
15	0.706996	192.168.43.201	69.173.159.63	TCP	55	1144 → 443 [ACK] Seq=1 Ack=1 Win=64390 Len=1 [TCP segment of a reassembled PDU]
16	1.293511	69.173.159.63	192.168.43.201	TCP	54	443 → 1144 [ACK] Seq=1 Ack=2 Win=42840 Len=0
17	1.615212	192.168.43.201	13.94.40.40	TLSv...	112	Application Data
18	0.806808	13.94.40.40	192.168.43.201	TLSv...	101	Application Data
19	1.852595	192.168.43.201	13.94.40.40	TCP	54	1244 → 443 [ACK] Seq=59 Ack=48 Win=513 Len=0
20	2.277008	192.168.43.201	104.85.134.35	TCP	55	1045 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
21	2.323841	192.168.43.201	40.81.31.55	TCP	55	1047 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
22	2.324658	104.85.134.35	192.168.43.201	TCP	66	443 → 1045 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
23	2.522040	40.81.31.55	192.168.43.201	TCP	66	443 → 1047 [ACK] Seq=1 Ack=2 Win=2044 Len=0 SLE=1 SRE=2
24	3.905837	192.168.43.201	20.189.124.38	TCP	55	1273 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
25	4.058447	20.189.124.38	192.168.43.201	TCP	66	443 → 1273 [ACK] Seq=1 Ack=2 Win=1027 Len=0 SLE=1 SRE=2

! Ip.src == 192.168.43.201 gives the source IP address where source is only on 192.168.43.201

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.201	5.178.65.245	TCP	55	1083 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
2	0.000196	192.168.43.201	74.118.186.210	TCP	55	1092 → 443 [ACK] Seq=1 Ack=1 Win=6178 Len=1 [TCP segment of a reassembled PDU]
3	0.008037	192.168.43.201	34.98.64.218	TCP	55	1090 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
4	0.008042	192.168.43.201	103.231.98.193	TCP	55	1081 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
5	0.035690	192.168.43.201	13.249.220.101	TCP	55	1079 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
6	0.051631	192.168.43.201	49.44.165.201	TCP	55	1088 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
7	0.051737	192.168.43.201	49.44.165.201	TCP	55	1089 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
17	0.706996	192.168.43.201	69.173.159.63	TCP	55	1144 → 443 [ACK] Seq=1 Ack=1 Win=64390 Len=1 [TCP segment of a reassembled PDU]
19	1.615212	192.168.43.201	13.94.40.40	TLSv...	112	Application Data
21	1.852595	192.168.43.201	13.94.40.40	TCP	54	1244 → 443 [ACK] Seq=59 Ack=48 Win=513 Len=0
22	2.277008	192.168.43.201	104.85.134.35	TCP	55	1045 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
23	2.323841	192.168.43.201	40.81.31.55	TCP	55	1047 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
26	3.905837	192.168.43.201	20.189.124.38	TCP	55	1273 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
28	4.518020	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=1 (no response found!)
30	4.980271	192.168.43.201	5.178.65.245	TCP	54	1083 → 443 [FIN, ACK] Seq=2 Ack=47 Win=513 Len=0
32	4.982060	192.168.43.201	5.178.65.245	TCP	54	1083 → 443 [RST, ACK] Seq=3 Ack=78 Win=0 Len=0
36	5.247363	192.168.43.201	204.79.197.203	TCP	55	1039 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
38	5.443822	192.168.43.201	52.139.250.253	TCP	55	1037 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
42	8.348025	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=1 (no response found!)
43	8.51719	192.168.43.1	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
44	8.357543	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=1 (no response found!)
45	8.360660	192.168.43.1	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
46	8.620337	192.168.43.201	52.33.219.121	TCP	55	1077 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
48	9.368888	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=2 (no response found!)
55	11.6313	192.168.43.201	13.249.214.81	TCP	55	1168 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
59	13.3526	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=2 (no response found!)

! (Ip.src == 192.168.43.201) gives the source IP address where source is not 192.168.43.201

No.	Time	Source	Destination	Protocol	Length	Info
8	0.067874	34.98.64.218	192.168.43.201	TCP	66	443 → 1090 [ACK] Seq=1 Ack=2 Win=339 Len=0 SLE=1 SRE=2
9	0.083811	49.44.165.201	192.168.43.201	TCP	66	443 → 1088 [ACK] Seq=1 Ack=2 Win=364 Len=0 SLE=1 SRE=2
10	0.096875	13.249.220.101	192.168.43.201	TCP	66	443 → 1079 [ACK] Seq=1 Ack=2 Win=163 Len=0 SLE=1 SRE=2
11	0.109615	103.231.98.193	192.168.43.201	TCP	54	443 → 1081 [ACK] Seq=1 Ack=2 Win=15272 Len=0
12	0.109867	74.118.186.210	192.168.43.201	TCP	54	443 → 1092 [ACK] Seq=1 Ack=2 Win=16267 Len=0
13	0.185363	5.178.65.245	192.168.43.201	TCP	66	443 → 1083 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
14	0.190889	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:ae80:1411:13::1780	TCP	75	1094 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]
15	0.217261	49.44.165.201	192.168.43.201	TCP	66	443 → 1089 [ACK] Seq=1 Ack=2 Win=348 Len=0 SLE=1 SRE=2
16	0.678653	2606:ae80:1411:13::1780	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	74	443 → 1094 [ACK] Seq=1 Ack=2 Win=89 Len=0
18	1.293531	69.173.159.63	192.168.43.201	TCP	54	443 → 1144 [ACK] Seq=1 Ack=2 Win=42840 Len=0
20	1.806080	13.94.40.40	192.168.43.201	TLSv...	101	Application Data
24	2.324658	104.85.134.35	192.168.43.201	TCP	66	443 → 1045 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
25	2.522040	40.81.31.55	192.168.43.201	TCP	66	443 → 1047 [ACK] Seq=1 Ack=2 Win=2044 Len=0 SLE=1 SRE=2
27	4.058447	20.189.124.38	192.168.43.201	TCP	66	443 → 1273 [ACK] Seq=1 Ack=2 Win=1027 Len=0 SLE=1 SRE=2
29	4.979894	5.178.65.245	192.168.43.201	TLSv...	100	Application Data
31	4.982000	5.178.65.245	192.168.43.201	TLSv...	85	Encrypted Alert
33	5.185036	5.178.65.245	192.168.43.201	TCP	54	443 → 1083 [ACK] Seq=79 Ack=3 Win=501 Len=0
34	5.185713	d2:b6:ba:f8:e1:0d	IntelCor: 0a:df:8e	ARP	42	Who has 192.168.43.201? Tell 192.168.43.1
35	5.185747	IntelCor: 0a:df:8e	d2:b6:ba:f8:e1:0d	ARP	42	192.168.43.201 is at 0a:fd:d1:0a:df:8e
37	5.304309	204.79.197.203	192.168.43.201	TCP	66	443 → 1039 [ACK] Seq=1 Ack=2 Win=1022 Len=0 SLE=1 SRE=2
39	5.541668	52.139.250.253	192.168.43.201	TCP	66	443 → 1037 [ACK] Seq=1 Ack=2 Win=7971 Len=0 SLE=1 SRE=2
40	7.381521	2409:4041:e88:40b:1ce7:70de:d31a:...	2600:140f:4:78c::11a6	TCP	75	1097 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
41	7.442885	2600:140f:4:78c::11a6	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	86	443 → 1097 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
47	9.077101	52.33.219.121	192.168.43.201	TCP	66	443 → 1077 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
49	9.382478	2606:2800:147:ff8:129b:22eb:20b:1...	2409:4041:e88:40b:1ce7:70de:d31a:...	TLSv...	131	Application Data
50	9.382898	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:2800:147:ff8:129b:22eb:20b:1...	TCP	74	1161 → 443 [FIN, ACK] Seq=1 Ack=58 Win=514 Len=0

! Ip.dst == 192.168.43.201 gives the destination IP address where destination is only on 192.168.43.201

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ip.dst == 192.168.43.201

No.	Time	Source	Destination	Protocol	Length	Info
8	0.067874	34.98.64.218	192.168.43.201	TCP	66	443 → 1090 [ACK] Seq=1 Ack=2 Win=339 Len=0 SLE=1 SRE=2
9	0.083811	49.44.165.201	192.168.43.201	TCP	66	443 → 1088 [ACK] Seq=1 Ack=2 Win=364 Len=0 SLE=1 SRE=2
10	0.096875	13.249.220.101	192.168.43.201	TCP	66	443 → 1079 [ACK] Seq=1 Ack=2 Win=163 Len=0 SLE=1 SRE=2
11	0.109615	103.231.98.193	192.168.43.201	TCP	54	443 → 1081 [ACK] Seq=1 Ack=2 Win=15272 Len=0
12	0.109867	74.118.186.210	192.168.43.201	TCP	54	443 → 1092 [ACK] Seq=1 Ack=2 Win=16267 Len=0
13	0.185363	5.178.65.245	192.168.43.201	TCP	66	443 → 1083 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
15	0.217261	49.44.165.201	192.168.43.201	TCP	66	443 → 1089 [ACK] Seq=1 Ack=2 Win=348 Len=0 SLE=1 SRE=2
18	1.293531	69.173.159.63	192.168.43.201	TCP	54	443 → 1144 [ACK] Seq=1 Ack=2 Win=42840 Len=0
20	1.806080	13.94.40.40	192.168.43.201	TLV...	101	Application Data
24	2.324658	104.85.134.35	192.168.43.201	TCP	66	443 → 1045 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
25	2.522040	40.81.31.55	192.168.43.201	TCP	66	443 → 1047 [ACK] Seq=1 Ack=2 Win=2044 Len=0 SLE=1 SRE=2
27	4.058447	20.189.124.38	192.168.43.201	TCP	66	443 → 1273 [ACK] Seq=1 Ack=2 Win=1027 Len=0 SLE=1 SRE=2
29	4.979894	5.178.65.245	192.168.43.201	TLV...	100	Application Data
31	4.982000	5.178.65.245	192.168.43.201	TLV...	85	Encrypted Alert
33	5.185036	5.178.65.245	192.168.43.201	TCP	54	443 → 1083 [ACK] Seq=79 Ack=3 Win=501 Len=0
37	5.304309	204.79.197.203	192.168.43.201	TCP	66	443 → 1039 [ACK] Seq=1 Ack=2 Win=1022 Len=0 SLE=1 SRE=2
39	5.541668	52.139.250.253	192.168.43.201	TCP	66	443 → 1037 [ACK] Seq=1 Ack=2 Win=7971 Len=0 SLE=1 SRE=2
43	8.351719	192.168.43.1	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
45	8.360060	192.168.43.1	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
47	9.077101	52.33.219.121	192.168.43.201	TCP	66	443 → 1077 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
56	11.6962	13.249.214.81	192.168.43.201	TCP	66	443 → 1168 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
63	14.4772	193.122.128.135	192.168.43.201	TLV...	100	Application Data
64	14.4774	193.122.128.135	192.168.43.201	TLV...	85	Encrypted Alert
65	14.4774	193.122.128.135	192.168.43.201	TCP	54	443 → 1194 [FIN, ACK] Seq=78 Ack=1 Win=68 Len=0
68	14.5180	185.29.135.42	192.168.43.201	TCP	66	443 → 1188 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 SRE=2
70	14.6218	49.44.165.201	192.168.43.201	TCP	66	443 → 1180 [ACK] Seq=1 Ack=2 Win=259 Len=0 SLE=1 SRE=2

#!(Ip.dst == 192.168.43.201) gives the destination IP address where destination is not 192.168.43.201

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ip.dst == 192.168.43.201

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.201	5.178.65.245	TCP	55	1083 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
2	0.000196	192.168.43.201	74.118.186.210	TCP	55	1092 → 443 [ACK] Seq=1 Ack=1 Win=63178 Len=1 [TCP segment of a reassembled PDU]
3	0.000807	192.168.43.201	34.98.64.218	TCP	55	1090 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
4	0.008042	192.168.43.201	103.231.98.193	TCP	55	1081 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
5	0.035690	192.168.43.201	13.249.220.101	TCP	55	1079 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
6	0.051631	192.168.43.201	49.44.165.201	TCP	55	1088 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
7	0.051737	192.168.43.201	49.44.165.201	TCP	55	1089 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
14	0.190889	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:ae80:1411:13:1780	TCP	75	1094 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]
16	0.678653	2606:ae80:1411:13:1780	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	74	443 → 1094 [ACK] Seq=1 Ack=2 Win=89 Len=0
17	0.706996	192.168.43.201	69.173.159.63	TCP	55	1144 → 443 [ACK] Seq=1 Ack=1 Win=64390 Len=1 [TCP segment of a reassembled PDU]
19	1.615212	192.168.43.201	13.94.40.40	TLV...	112	Application Data
21	1.852595	192.168.43.201	13.94.40.40	TCP	54	1244 → 443 [ACK] Seq=59 Ack=48 Win=513 Len=0
22	2.277008	192.168.43.201	104.85.134.35	TCP	55	1045 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
23	2.323841	192.168.43.201	40.81.31.55	TCP	55	1047 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
26	3.905837	192.168.43.201	20.189.124.38	TCP	55	1273 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
28	4.518024	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=1 (no response found!)
30	4.980271	192.168.43.201	5.178.65.245	TCP	54	1083 → 443 [FIN, ACK] Seq=2 Ack=47 Win=513 Len=0
32	4.982060	192.168.43.201	5.178.65.245	TCP	54	1083 → 443 [RST, ACK] Seq=3 Ack=78 Win=0 Len=0
34	5.185713	d2:b8:ba:f8:e1:0d	IntelCor_0a:df:8e	ARP	42	Who has 192.168.43.201? Tell 192.168.43.1
35	5.185747	IntelCor_0a:df:8e	d2:b8:ba:f8:e1:0d	ARP	42	192.168.43.201 is at 84:fd:d1:0a:df:8e
36	5.247363	192.168.43.201	204.79.197.203	TCP	55	1039 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
38	5.443822	192.168.43.201	52.139.250.253	TCP	55	1037 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
40	7.381521	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:140f:4:78c:11a6	TCP	75	1097 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
41	7.442885	2606:140f:4:78c:11a6	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	86	443 → 1097 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
42	8.348025	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=1 (no response found!)
44	8.357543	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=1 (no response found!)

!Ipv6 gives all IP address

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ipv6

No.	Time	Source	Destination	Protocol	Length	Info
14	0.190889	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:ae80:1411:13:1780	TCP	75	1094 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]
16	0.678653	2606:ae80:1411:13:1780	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	74	443 → 1094 [ACK] Seq=1 Ack=2 Win=89 Len=0
40	7.381521	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:140f:4:78c:11a6	TCP	75	1097 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
41	7.442885	2606:140f:4:78c:11a6	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	86	443 → 1097 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
49	9.382478	2606:2800:147:ff8:129b:22eb:20b:1...	2409:4041:e88:40b:1ce7:70de:d31a:...	TLV...	131	Application Data
50	9.382898	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:2800:147:ff8:129b:22eb:20b:1...	TCP	74	1161 → 443 [FIN, ACK] Seq=1 Ack=58 Win=514 Len=0
51	9.388805	2606:2800:147:ff8:129b:22eb:20b:1...	2409:4041:e88:40b:1ce7:70de:d31a:...	TLV...	98	Application Data
52	9.388806	2606:2800:147:ff8:129b:22eb:20b:1...	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	74	443 → 1161 [FIN, ACK] Seq=82 Ack=1 Win=136 Len=0
53	9.388876	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:2800:147:ff8:129b:22eb:20b:1...	TCP	74	1161 → 443 [RST, ACK] Seq=2 Ack=82 Win=0 Len=0
54	9.444266	2606:2800:147:ff8:129b:22eb:20b:1...	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	74	443 → 1161 [ACK] Seq=83 Ack=2 Win=136 Len=0
57	12.0707	2409:4041:e88:40b:1ce7:70de:d31a:...	2404:6800:4009:801:12001	TCP	75	1162 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
58	12.1117	2404:6800:4009:801:12001	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	86	443 → 1162 [ACK] Seq=1 Ack=2 Win=271 Len=0 SLE=1 SRE=2
61	14.4143	fe80:d0b8:baff:fe8:e10d	2409:4041:e88:40b:1ce7:70de:d31a:...	ICMP...	86	Neighbor Solicitation for 2409:4041:e88:40b:1ce7:70de:d31a:537e from d2:b8:ba:f8:e1:0d
62	14.4145	2409:4041:e88:40b:1ce7:70de:d31a:...	fe80:d0b8:baff:fe8:e10d	ICMP...	86	Neighbor Advertisement 2409:4041:e88:40b:1ce7:70de:d31a:537e (sol, ovr) is at 84:fd:d1:0a:df:8e
88	17.6231	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:140f:1c00:b854:e8e9	TCP	75	1250 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
91	17.7115	2606:140f:1c00:b854:e8e9	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	86	443 → 1250 [ACK] Seq=1 Ack=2 Win=498 Len=0 SLE=1 SRE=2
168	30.6014	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:9000:2149:9e00:1a3fa:7c0:9...	TCP	75	1064 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
169	30.6656	2606:9000:2149:9e00:1a3fa:7c0:9...	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	86	443 → 1064 [ACK] Seq=1 Ack=2 Win=104 Len=0 SLE=1 SRE=2
177	31.8258	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:140f:1c00:b854:e8e9	TLV...	526	Ignored Unknown Record
179	31.8708	2606:140f:1c00:b854:e8e9	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	74	443 → 1250 [ACK] Seq=1 Ack=454 Win=519 Len=0
180	32.2185	2606:140f:1c00:b854:e8e9	2409:4041:e88:40b:1ce7:70de:d31a:...	TLV...	395	Application Data
181	32.2192	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:140f:1c00:b854:e8e9	TLV...	1019	Application Data
182	32.2603	2606:140f:1c00:b854:e8e9	2409:4041:e88:40b:1ce7:70de:d31a:...	TCP	74	443 → 1250 [ACK] Seq=322 Ack=1399 Win=541 Len=0
184	32.5381	2606:140f:1c00:b854:e8e9	2409:4041:e88:40b:1ce7:70de:d31a:...	TLV...	419	Application Data
186	32.5871	2409:4041:e88:40b:1ce7:70de:d31a:...	2606:140f:1c00:b854:e8e9	TCP	74	1250 → 443 [ACK] Seq=1399 Ack=667 Win=513 Len=0
193	32.7944	2409:4041:e88:40b:1ce7:70de:d31a:...	2620:1ec:c11:1200	TCP	75	1051 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]



- ICMP protocol is Internet Control Message Protocol.
- Where we first run the command `tracert -d 8.8.8.8` for google DNS public services.

```

C:\WINDOWS\system32\cmd.exe

1      6 ms      2 ms      2 ms  192.168.43.1
2      *        *        ^C
C:\Users\ARJUN VANKANI>

C:\Users\ARJUN VANKANI>

C:\Users\ARJUN VANKANI>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  0  *          3 ms      2 ms  192.168.43.1
  1  *          *        *      Request timed out.
  2  35 ms     41 ms     36 ms  10.72.234.145
  3  36 ms     50 ms     41 ms  192.168.38.4
  4  38 ms     34 ms     34 ms  192.168.38.5
  5  37 ms     36 ms     35 ms  172.26.101.8
  6  78 ms     32 ms     43 ms  172.26.100.246
  7  35 ms     65 ms     37 ms  192.168.38.23
  8  37 ms     36 ms    134 ms  192.168.38.24
  9  154 ms    49 ms    142 ms  172.16.92.145
 10  51 ms     32 ms     47 ms  172.16.25.2
 11  42 ms     37 ms     49 ms  172.16.1.218
 12  54 ms     36 ms     45 ms  108.170.248.193
 13  47 ms     35 ms     36 ms  209.85.244.157
 14  78 ms     70 ms     76 ms  8.8.8.8

Trace complete.

```

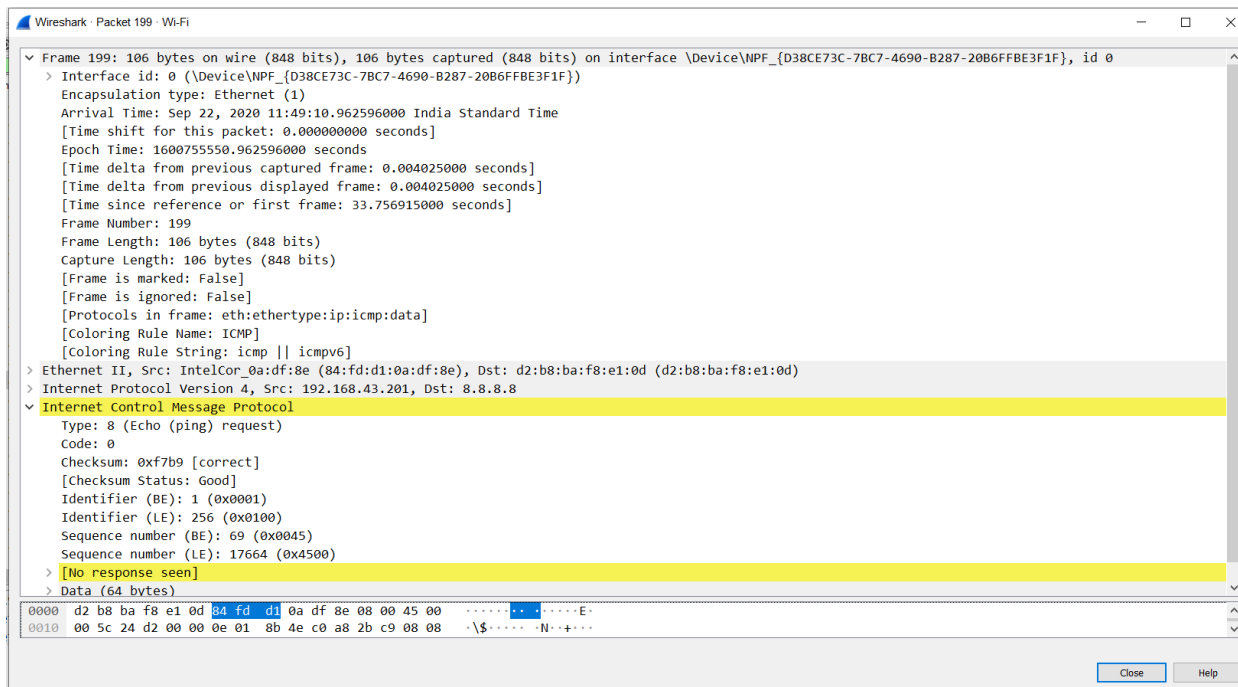
- At the time we analysis the Wireshark software ICMP protocol.

No.	Time	Source	Destination	Protocol	Length	Info
167	30.5115..	172.16.25.2	192.168.43.201	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
170	31.4806..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=12 (no response found!)
171	31.5222..	172.16.1.218	192.168.43.201	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
172	31.5265..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=12 (no response found!)
173	31.5633..	172.16.1.218	192.168.43.201	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
174	31.5680..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=12 (no response found!)
175	31.6171..	172.16.1.218	192.168.43.201	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
187	32.5887..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=13 (no response found!)
188	32.6427..	108.170.248.193	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
189	32.6465..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=13 (no response found!)
190	32.6824..	108.170.248.193	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
191	32.6866..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=13 (no response found!)
192	32.7322..	108.170.248.193	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
197	33.7057..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=14 (no response found!)
198	33.7528..	209.85.244.157	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
199	33.7569..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=14 (no response found!)
200	33.7916..	209.85.244.157	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
201	33.7958..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=14 (no response found!)
202	33.8317..	209.85.244.157	192.168.43.201	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
203	34.8125..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=15 (reply in 206)
206	34.8905..	8.8.8.8	192.168.43.201	ICMP	106	Echo (ping) reply id=0x0001, seq=71/18176, ttl=111 (request in 203)
207	34.8979..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=72/18432, ttl=15 (reply in 208)
208	34.9083..	8.8.8.8	192.168.43.201	ICMP	106	Echo (ping) reply id=0x0001, seq=72/18432, ttl=111 (request in 207)
209	34.9730..	192.168.43.201	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=73/18688, ttl=15 (reply in 210)
210	35.0497..	8.8.8.8	192.168.43.201	ICMP	106	Echo (ping) reply id=0x0001, seq=73/18688, ttl=111 (request in 209)

Frame 28: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF\_{D38CE73C-7BC7-4690-B287-20B6FFB3F1F}, id 0  
 Ethernet II, Src: IntelCor 0a:df:8e (84:fd:d1:0a:df:8e), Dst: d2:b8:ba:f8:e1:0d (d2:b8:ba:f8:e1:0d)  
 Internet Protocol Version 4, Src: 192.168.43.201, Dst: 8.8.8.8  
 Internet Control Message Protocol

0000 d2 b8 ba f8 e1 0d 84 fd d1 0a df 8e 08 00 45 00 .....E..  
 0010 00 5c 24 aa 00 00 01 01 98 76 c0 a8 2b c9 08 08 ..\\$. ....  
 0020 08 08 00 00 f7 e1 00 01 00 1d 00 00 00 00 00 .....

## This is for message request to DNS



## This is for message reply to DNS

