

جواب سوال ۱-

QUIC – TCP – DNS – TLSv1.3 – TLSv1.2 – SSLV2 – SSDP – ARP – UDP – HTTP – NBSN – MDNS – IGMPv2

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
8260	72.946151	172.217.18.132	192.168.1.9	QUIC	533	Protected Payload (KP0)
8261	72.946151	172.217.18.132	192.168.1.9	QUIC	69	Protected Payload (KP0)
8262	72.946151	172.217.18.132	192.168.1.9	QUIC	93	Protected Payload (KP0)
8263	72.951882	192.168.1.9	172.217.169.226	TCP	54	49907 → 443 [FIN, ACK] Seq=582 Ack=4406 Win=65024 Len=0
8264	72.951986	192.168.1.9	172.217.169.234	TCP	54	49906 → 443 [FIN, ACK] Seq=662 Ack=793 Win=64768 Len=0
8265	72.966082	192.168.1.9	172.217.18.132	QUIC	75	Protected Payload (KP0), DCID=9ec74eb6086bbd7c
8266	73.008411	192.168.1.9	192.168.1.1	DNS	70	Standard query 0xd883 A golang.com
8267	73.018802	172.217.18.132	192.168.1.9	QUIC	68	Protected Payload (KP0)
8268	73.033418	172.217.169.234	192.168.1.9	TCP	54	443 → 49906 [FIN, ACK] Seq=793 Ack=663 Win=66816 Len=0
8269	73.033471	192.168.1.9	172.217.169.234	TCP	54	49906 → 443 [ACK] Seq=663 Ack=794 Win=64768 Len=0
8270	73.035977	172.217.169.226	192.168.1.9	TCP	54	443 → 49907 [FIN, ACK] Seq=4406 Ack=583 Win=66816 Len=0
8271	73.036039	192.168.1.9	172.217.169.226	TCP	54	49907 → 443 [ACK] Seq=583 Ack=4407 Win=65024 Len=0

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
8544	86.767664	185.143.234.5	192.168.1.9	TCP	880	[TCP Previous segment not captured] 443 → 49957 [PSH, ACK] Seq=2820 Ack=1041 Win=68608 Len=746 [TCP segment of a reassembled PDU]
8545	86.767700	192.168.1.9	185.143.234.5	TCP	66	49957 → 443 [ACK] Seq=1041 Ack=1460 Win=64080 Len=0 SLE=2820 SRE=3566
8546	86.767736	185.143.234.5	192.168.1.9	TCP	1414	[TCP Out-Of-Order] 443 → 49957 [ACK] Seq=1460 Ack=1041 Win=68608 Len=1360
8547	86.768778	192.168.1.9	185.143.234.5	TCP	54	49957 → 443 [ACK] Seq=1041 Ack=3566 Win=65536 Len=0
8548	86.778874	192.168.1.9	185.143.234.5	TLSv1.3	128	Application Data
8549	86.779110	192.168.1.9	185.143.234.5	TLSv1.3	146	Application Data
8550	86.779551	192.168.1.9	185.143.234.5	TLSv1.3	494	Application Data
8551	86.813041	185.143.234.5	192.168.1.9	TLSv1.3	628	Application Data, Application Data
8552	86.813041	185.143.234.5	192.168.1.9	TLSv1.3	116	Application Data
8553	86.813128	192.168.1.9	185.143.234.5	TCP	54	49957 → 443 [ACK] Seq=1647 Ack=4202 Win=65024 Len=0
8554	86.814229	192.168.1.9	185.143.234.5	TLSv1.3	85	Application Data
8555	86.826245	185.143.234.5	192.168.1.9	TLSv1.3	85	Application Data

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
8653	87.337042	185.143.234.5	192.168.1.9	TCP	1414	443 → 49957 [ACK] Seq=79869 Ack=2153 Win=70656 Len=1360
8654	87.343792	185.143.234.5	192.168.1.9	TCP	1414	443 → 49957 [ACK] Seq=81229 Ack=2153 Win=70656 Len=1360 [TCP segment of a reassembled PDU]
8655	87.343861	192.168.1.9	185.143.234.5	TCP	54	49957 → 443 [ACK] Seq=2153 Ack=82589 Win=65536 Len=0
8656	87.344252	185.143.234.5	192.168.1.9	TCP	1414	443 → 49957 [ACK] Seq=82589 Ack=2153 Win=70656 Len=1360 [TCP segment of a reassembled PDU]
8657	87.344252	185.143.234.5	192.168.1.9	SSLV2	1414	Encrypted Data, Continuation Data
8658	87.344308	192.168.1.9	185.143.234.5	TCP	54	49957 → 443 [ACK] Seq=2153 Ack=85309 Win=65536 Len=0
8659	87.344860	185.143.234.5	192.168.1.9	TLSv1.3	1414	Continuation Data
8660	87.349409	185.143.234.5	192.168.1.9	TLSv1.3	1414	Continuation Data
8661	87.349409	185.143.234.5	192.168.1.9	TLSv1.3	4134	Continuation Data
8662	87.349409	185.143.234.5	192.168.1.9	TLSv1.3	1414	[TCP Previous segment not captured], Continuation Data
8663	87.349506	192.168.1.9	185.143.234.5	TCP	66	49957 → 443 [ACK] Seq=2153 Ack=92109 Win=65536 Len=0 SLE=93469 SRE=94829

No.	Time	Source	Destination	Protocol	Length	Info
4	2.005721	192.168.1.9	172.16.4.137	TCP	66	[TCP Retransmission] 49898 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	2.005854	192.168.1.9	172.16.4.137	TCP	66	[TCP Retransmission] 49899 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	2.260039	192.168.1.9	172.16.4.137	TCP	66	[TCP Retransmission] 49900 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	4.628127	Microsof_19:da:64	ARGTelec_e8:dd:ae	ARP	42	Who has 192.168.1.1? Tell 192.168.1.9
8	4.633617	ARGTelec_e8:dd:ae	Microsof_19:da:64	ARP	42	192.168.1.1 is at 30:a2:20:e8:dd:ae
9	5.106105	192.168.1.7	192.168.1.255	UDP	86	57621 → 57621 Len=44
10	5.823090	192.168.1.1	239.255.255.250	SSDP	307	NOTIFY * HTTP/1.1
11	5.823264	192.168.1.1	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
12	5.823552	192.168.1.1	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1
13	5.823552	192.168.1.1	239.255.255.250	SSDP	371	NOTIFY * HTTP/1.1
14	5.823727	192.168.1.1	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
15	5.824408	192.168.1.1	239.255.255.250	SSDP	355	NOTIFY * HTTP/1.1
16	6.034480	192.168.1.1	239.255.255.250	SSDP	387	NOTIFY * HTTP/1.1

No.	Time	Source	Destination	Protocol	Length	Info
9783	88.379228	192.168.1.9	185.143.234.5	TCP	66	[TCP Dup ACK 9780#1] 49957 → 443 [ACK] Seq=5483 Ack=1255142 Win=754688 Len=0 SLE=1256502 SRE=1257862
9784	88.379281	192.168.1.9	185.143.234.5	TCP	54	49957 → 443 [ACK] Seq=5483 Ack=1257862 Win=756224 Len=0
9785	88.379352	185.143.234.5	192.168.1.9	TLSv1.3	1414	[TCP Previous segment not captured], Continuation Data
9786	88.379368	192.168.1.9	185.143.234.5	TCP	66	[TCP Dup ACK 9784#1] 49957 → 443 [ACK] Seq=5483 Ack=1257862 Win=756224 Len=0 SLE=1259222 SRE=1260582
9787	88.379874	185.143.234.5	192.168.1.9	TCP	1414	[TCP Out-Of-Order] 443 → 49957 [ACK] Seq=1257862 Ack=5339 Win=71680 Len=1360
9788	88.379874	172.217.169.227	192.168.1.9	TCP	58	80 → 49958 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9789	88.379926	192.168.1.9	185.143.234.5	TCP	54	49957 → 443 [ACK] Seq=5483 Ack=1260582 Win=756224 Len=0
9790	88.380002	192.168.1.9	172.217.169.227	TCP	54	49958 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9791	88.380382	192.168.1.9	172.217.169.227	HTTP	368	GET /generate_204 HTTP/1.1
9792	88.391336	185.143.234.5	192.168.1.9	TLSv1.3	5494	Continuation Data
9793	88.391336	185.143.234.5	192.168.1.9	TLSv1.3	1414	[TCP Previous segment not captured], Continuation Data
9794	88.391336	185.143.234.5	192.168.1.9	TCP	1414	[TCP Out-Of-Order] 443 → 49957 [ACK] Seq=1266022 Ack=5339 Win=71680 Len=1360
9795	88.391336	185.143.234.5	192.168.1.9	TLSv1.3	2774	Continuation Data

No.	Time	Source	Destination	Protocol	Length	Info
3269	32.939914	172.217.18.132	192.168.1.9	QUIC	1392	Protected Payload (KP0)
3270	32.940011	172.217.18.132	192.168.1.9	QUIC	1392	Protected Payload (KP0)
3271	32.940096	192.168.1.9	172.217.18.132	QUIC	76	Protected Payload (KP0), DCID=9ec74eb6086bbd7c
3272	32.940859	172.217.18.132	192.168.1.9	QUIC	959	Protected Payload (KP0)
3273	32.940859	172.217.18.132	192.168.1.9	QUIC	1392	Protected Payload (KP0)
3274	32.941135	192.168.1.9	172.217.18.132	QUIC	77	Protected Payload (KP0), DCID=9ec74eb6086bbd7c
3275	32.941270	192.168.1.9	172.217.18.132	QUIC	75	Protected Payload (KP0), DCID=9ec74eb6086bbd7c
3276	32.953458	192.168.1.9	192.168.1.255	NBNS	92	Name query NB GITHUB:00
3277	32.959865	172.217.18.132	192.168.1.9	QUIC	68	Protected Payload (KP0)
3278	32.999045	172.217.18.132	192.168.1.9	QUIC	1392	Protected Payload (KP0)
3279	32.999045	172.217.18.132	192.168.1.9	QUIC	1384	Protected Payload (KP0)
3280	33.000557	140.82.121.3	192.168.1.9	TCP	66	443 → 49915 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 SACK_PERM=1 WS=1024
3281	33.000635	192.168.1.9	140.82.121.3	TCP	64	49915 → 443 [ACK] Seq=1 Ack=1 Win=66040 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
8310	82.627345	151.101.1.69	192.168.1.9	TCP	66	[TCP Keep-Alive ACK] 443 → 49934 [ACK] Seq=90426 Ack=1513 Win=68096 Len=0 SLE=1512 SRE=1513
8311	82.816698	192.168.1.9	185.199.111.133	TCP	55	[TCP Keep-Alive] 49924 → 443 [ACK] Seq=3086 Ack=234185 Win=66048 Len=1
8312	82.959062	192.168.1.9	216.58.209.142	TCP	55	[TCP Keep-Alive] 49937 → 443 [ACK] Seq=1094 Ack=23761 Win=64768 Len=1
8313	82.972016	17.248.149.138	192.168.1.9	TLSv1.2	85	Encrypted Alert
8314	82.972016	17.248.149.138	192.168.1.9	TCP	54	443 → 49909 [FIN, ACK] Seq=8839 Ack=990 Win=64128 Len=0
8315	82.972016	17.248.149.178	192.168.1.9	TLSv1.2	85	Encrypted Alert
8316	82.972016	17.248.149.178	192.168.1.9	TCP	54	443 → 49908 [FIN, ACK] Seq=8784 Ack=993 Win=64128 Len=0
8317	82.972016	185.199.111.133	192.168.1.9	TCP	66	[TCP Keep-Alive ACK] 443 → 49924 [ACK] Seq=234185 Ack=3087 Win=90112 Len=0 SLE=3086 SRE=3087
8318	82.972183	192.168.1.9	17.248.149.138	TCP	54	49909 → 443 [ACK] Seq=990 Ack=8840 Win=64512 Len=0
8319	82.972218	192.168.1.9	17.248.149.138	TLSv1.2	85	Encrypted Alert
8320	82.972229	192.168.1.9	17.248.149.178	TLSv1.2	85	Encrypted Alert
8321	82.972278	192.168.1.9	17.248.149.138	TCP	54	49909 → 443 [FIN, ACK] Seq=1021 Ack=8840 Win=64512 Len=0
8322	82.973203	192.168.1.9	17.248.149.178	TCP	54	49909 → 443 [FIN, ACK] Seq=1021 Ack=8784 Win=64768 Len=0

> Frame 8309: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D8C16DAB-58DF-4309-8098-AD64EC597957}, id 0

> Ethernet II, Src: Microsof_19:da:64 (bc:83:85:19:da:64), Dst: ARGTelec_e8:dd:ae (30:a2:20:e8:dd:ae)

> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 10.10.34.35

> Transmission Control Protocol, Src Port: 49951, Dst Port: 443, Seq: 0, Len: 0

جواب سوال ۲ –

به طور مثال بسته زیر با protocol ای به نام TCP انتخاب شده است.

Wireshark packet capture showing a TCP segment. The packet list shows a TCP segment from 192.168.1.9 to 192.217.18.132. The packet details show the Ethernet II header, Internet Protocol Version 4 header, and the Transmission Control Protocol header. The packet bytes show the raw data of the TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
77	0.652326	172.217.18.132	192.168.1.9	UDP	1392	443 → 55021 Len=1350
78	0.653273	192.168.1.9	172.217.18.132	UDP	75	55021 → 443 Len=33
79	0.653413	192.168.1.9	172.217.18.132	UDP	75	55021 → 443 Len=33
80	0.656432	192.168.1.9	216.58.209.142	TCP	54	50566 → 443 [FIN, ACK] Seq=1 Ack=1 Win=253 Len=0
81	0.656600	192.168.1.9	172.217.18.132	TCP	54	50567 → 443 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
82	0.656964	192.168.1.9	172.217.18.142	TCP	66	50568 → 80 [SVN] Seq=0 Win=65340 Len=0 MSS=1460 WS=256 SACK_PERM=1
83	0.657240	192.168.1.9	172.217.18.142	TCP	66	50569 → 80 [SVN] Seq=0 Win=65340 Len=0 MSS=1460 WS=256 SACK_PERM=1
84	0.659349	192.168.1.9	192.168.1.1	DNS	77	Standard query 0x4d13 A fonts.gstatic.com
85	0.659952	192.168.1.9	192.168.1.1	DNS	75	Standard query 0x427e A www.gstatic.com
86	0.667232	172.217.18.132	192.168.1.9	UDP	1392	443 → 55021 Len=1350
87	0.667232	172.217.18.132	192.168.1.9	UDP	1392	443 → 55021 Len=1350
88	0.667232	172.217.18.132	192.168.1.9	UDP	1392	443 → 55021 Len=1350
89	0.667232	172.217.18.132	192.168.1.9	UDP	1392	443 → 55021 Len=1350

Frame 81: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{D8C16DA8-58DF-4309-8098-AD64EC597957}, id 0
 > Ethernet II, Src: Microsof_19:da:64 (bc:83:85:19:da:64), Dst: ARGTelec_e8:dd:ae (30:a2:20:e8:dd:ae)
 > Internet Protocol Version 4, Src: 192.168.1.9, Dst: 172.217.18.132
 > Transmission Control Protocol, Src Port: 50567, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000 30 a2 20 e8 dd ae 0c 82 85 19 da 64 00 00 45 00 00 ...E
 0010 00 28 66 83 40 00 00 06 13 3e c0 a8 01 09 ac d9 ..(f@>.....
 0020 12 84 c5 87 01 bb ef 24 a5 76 8b b9 59 a5 50 11\$~v~Y.p
 0030 01 00 ec 87 00 00

خط ۲ ethernet لایه data link -- خط ۳ IP لایه Network -- خط ۴ TCP لایه Transport می‌باشد

ترتیب قرار گرفتن بیت‌ها در ارتباط با ترتیب لایه‌ها می‌باشد. اول از همه بیت‌های مربوط به لایه‌های اول و بعد لایه‌های بعدی به ترتیب می‌آیند. به طور مثال در تصویر بالا اول بیت‌های datalink و بعد لایه network و در آخر بیت‌های مربوط به لایه transport آمده‌اند.

اندازه فریم لایه ۲ برابر ۵۴

و اندازه بسته لایه ۳ برابر ۴۰

جواب سوال ۳ -

آن دسته از بسته‌ها که protocol آن‌ها از نوع ARP می‌باشد.

No.	Time	Source	Destination	Protocol	Length	Info
7	4.628127	Microsof_19:da:64	ARGTelec_e8:dd:ae	ARP	42	Who has 192.168.1.1? Tell 192.168.1.9
8	4.633617	ARGTelec_e8:dd:ae	Microsof_19:da:64	ARP	42	192.168.1.1 is at 30:a2:20:e8:dd:ae

> Frame 8: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D8C16DA8-58DF-4309-8098-AD64EC597957}, id 0
 > Ethernet II, Src: ARGTelec_e8:dd:ae (30:a2:20:e8:dd:ae), Dst: Microsof_19:da:64 (bc:83:85:19:da:64)
 > Address Resolution Protocol (reply)

جواب سوال ۴ -

برای بسته انتخاب شده مقدار 0xbf7c نشان داده می‌شود.

No.	Time	Source	Destination	Protocol	Length	Info
26	6.812606	192.168.1.9	172.16.4.137	TCP	66	[TCP Retransmission] 49898 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
27	6.812698	192.168.1.9	172.16.4.137	TCP	66	[TCP Retransmission] 49899 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	6.264231	192.168.1.9	172.16.4.137	TCP	66	[TCP Retransmission] 49900 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
29	6.649958	192.168.1.9	192.168.1.1	DNS	74	Standard query 0x599a A www.google.com
30	6.716530	192.168.1.9	192.168.1.1	DNS	74	Standard query 0x599a A www.google.com
31	6.779670	192.168.1.1	192.168.1.9	DNS	90	Standard query response 0x599a A www.google.com A 172.217.18.132
32	6.779670	192.168.1.1	192.168.1.9	DNS	90	Standard query response 0x599a A www.google.com A 172.217.18.132
33	6.781015	192.168.1.9	172.217.18.132	QUIC	1392	Initial, DCID=9ec74eb6086bbd7c, PKN: 1, CRYPTO, PADDING
34	6.935545	192.168.1.9	172.217.18.132	TCP	66	49901 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35	6.965373	172.217.18.132	192.168.1.9	QUIC	1392	Initial, SCID=9ec74eb6086bbd7c, PKN: 1, ACK, PADDING
36	6.986825	172.217.18.132	192.168.1.9	QUIC	1392	Initial, SCID=9ec74eb6086bbd7c, PKN: 2, CRYPTO, PADDING
37	6.986825	172.217.18.132	192.168.1.9	QUIC	274	Handshake, SCID=9ec74eb6086bbd7c
38	6.987046	172.217.18.132	192.168.1.9	QUIC	184	Protected Payload (V00)

....00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 1378
 Identification: 0x0000 (0)
 Flags: 0x40, Don't fragment
 0... .. = Reserved bit: Not set
 1... .. = Don't fragment: Set
 ..0... .. = More fragments: Not set
 Fragment Offset: 0
 Time to Live: 53
 Protocol: UDP (17)
 Header Checksum: 0xbf7c [validation disabled]
 [Header checksum status, Unverified]
 Source Address: 172.217.18.132
 Destination Address: 192.168.1.9

0010 05 62 00 00 40 00 35 11 bf 7d ac d9 12 84 c0 a8 -b-@5.....
 0020 01 09 01 bb cd a9 05 4e 24 76 ce ff 00 00 1d 00N\$.....
 0030 08 9e c7 4e b6 08 6b db 7c 00 45 34 8b 66 94 f3 ...N-k-|-E4-f-
 0040 8a 30 a5 f7 12 82 22 b8 a3 62 7a 1f 15 75 a6 db -0-...-bz-u-
 0050 99 dc e0 f7 db 44 13 6b 91 1e e1 fb ff 2b 60 30D.k.....+0
 0060 ed 03 eb b7 8a a0 64 bf 17 d6 6a 30 82 7f c4 91d.....j0.....
 0070 d7 b0 86 c9 7c 09 91 20 95 e8 2e 26 3f a8 bb 72|.....&?-p
 0080 63 3e e6 b1 f9 75 fb 61 cd 12 f1 f1 59 20 a9 59 >...u-a...Y.Y
 0090 ad bf 20 04 2c b6 28 9f 9e 65 62 53 12 1c 47 5f ...-(-eb5-G-
 00a0 82 77 1c cc bf 64 67 e4 2c 57 d8 bd 4d 74 eb 13 -w-dg-,W-Mt-
 00b0 94 6e 90 f7 a5 82 56 7f a2 b3 f0 30 fd 47 49 4e -n...V...0.GIN
 00c0 29 c9 a6 a2 56 41 fa 64 5e b5 05 1b 37 f4 8c 2f)...VA-d...7-/
 00d0 d6 8c a7 53 ca 2d 1f c9 ca de 46 c5 03 b1 c8 ad ...S...-F-...

جواب سوال ۵ -

همانطور که در تصویر پیداست port مبدا نمایانگر آن پرتالهای است که دیتا را ارسال می کند و port مقصد هم که بیانگر آن پرتالز ای است که اطلاعات را دریافت می کند و مقدار آن ها به ترتیب برابر ۴۹۸۹۸ برای مبدا و ۸۰ برای مقصد است.

The image displays two screenshots of the Wireshark network protocol analyzer, specifically focusing on the details of a TCP packet.

Top Screenshot: Shows the packet list and the details pane for a TCP packet. The packet list shows a SYN packet from 192.168.1.9 to 172.16.4.137. The details pane shows the following information:

- Source Port: 49898
- Destination Port: 80
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 1886075363
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x002 (SYN)
- Window: 64240
- [Calculated window size: 64240]

Bottom Screenshot: Shows the same packet list and details pane, but with the checksum field highlighted. The details pane shows the following information:

- Sequence Number (raw): 1886075363
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x002 (SYN)
- Window: 64240
- [Calculated window size: 64240]
- Checksum: 0x944b [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
- [Timestamps]

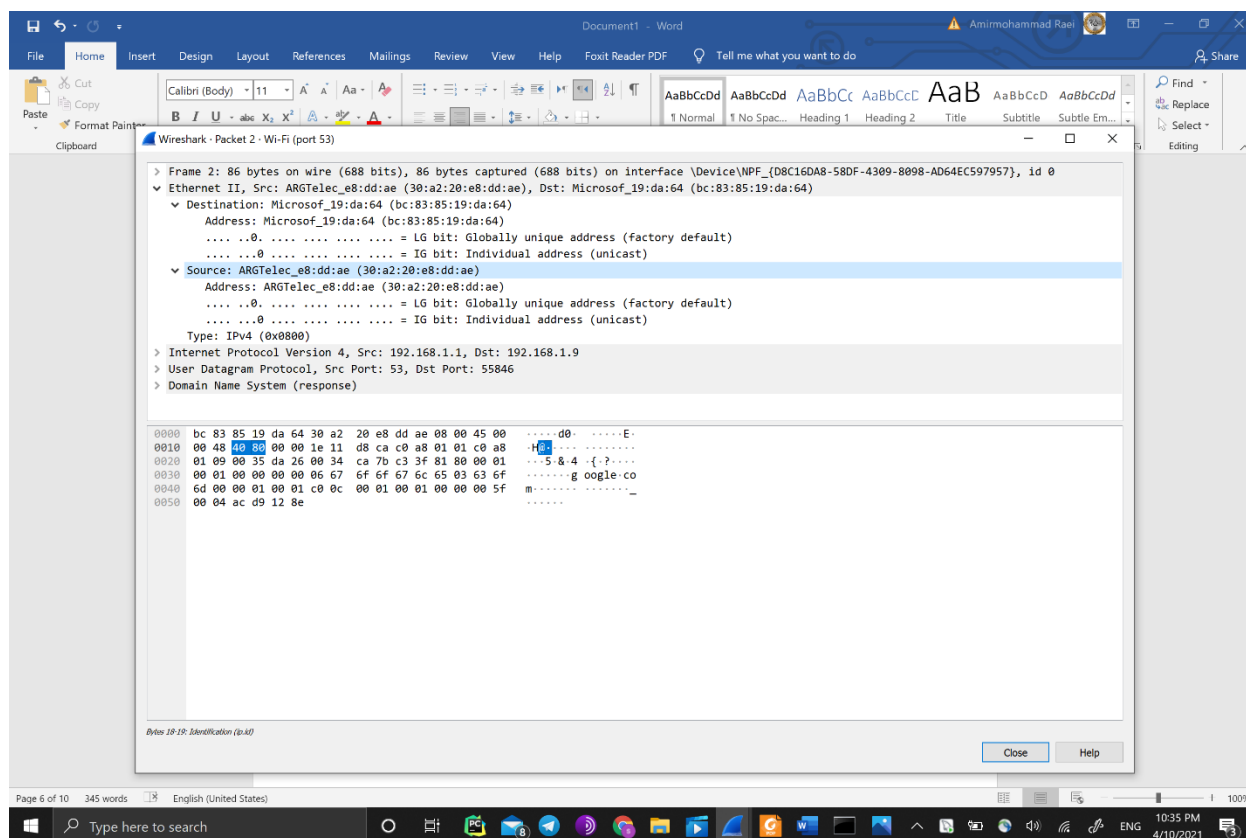
checksum مربوطه هم در عکس بالا نشان داده شده است.

جواب سوال ۶ –

Protocol مربوط به این لایه برابر UDP است. IP مقصد برابر 192.168.1.9 می‌باشد.

مقدار آدرس مبدا 30:a2:20:e8:dd:ae

و برای مقصد bc:83:85:19:da:64



جواب سوال ۷ –

آدرس مبدا در مقابل IPv4 address نشان داده میشود. و نیز آدرس مقصد هم در مقابل DNS Server و یا Default Gateway قابل مشاهده است.

جواب سوال ۸ –

Type انتخابی A است و این برای ذخیره IPv4 و پینگ و یا برای ساختن host name به ip آدرس آن‌ها به کار برده شده است.

▼ Queries

▼ adservice.google.com: type A, class IN

Name: adservice.google.com

[Name Length: 20]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

جواب سوال ۹ –

PTR تایپی است که دیده می‌شود و برای این استفاده شده است که ip address برای dns فراهم شود به host دسترسی پیدا کند.

The image shows a Wireshark capture of DNS traffic on port 53. The packet list shows a series of queries and responses. The selected packet is a PTR query response from 192.168.1.1 to 192.168.1.9. The packet details pane shows the query for 1.1.1.1.in-addr.arpa, type PTR, class IN. The packet bytes pane shows the raw data of the DNS message.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.9	192.168.1.1	DNS	70	Standard query 0xc7ef A google.com
2	0.033745	192.168.1.1	192.168.1.9	DNS	86	Standard query response 0xc7ef A google.com A 216.58.208.78
3	16.157767	192.168.1.9	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
4	16.238793	192.168.1.1	192.168.1.9	DNS	139	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA 168.192.IN-ADDR.ARPA
5	16.244203	192.168.1.9	192.168.1.1	DNS	80	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
6	16.278457	192.168.1.1	192.168.1.9	DNS	109	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one

Authority RRs: 0
Additional RRs: 0

▼ Queries

- ▼ 1.1.1.1.in-addr.arpa: type PTR, class IN
 - Name: 1.1.1.1.in-addr.arpa
 - [Name Length: 20]
 - [Label Count: 6]
 - Type: PTR (domain name Pointer) (12)
 - Class: IN (0x0001)

▼ Answers

- > 1.1.1.1.in-addr.arpa: type PTR, class IN, one.one.one.one
 - [Request in: 5]
 - [Time: 0.034254000 seconds]

0000 bc 83 85 19 da 64 30 a2 20 e8 dd ae 08 00 45 00 ...d0:E:
0010 00 5f 3a 16 00 00 1e 11 df 1d c0 a8 01 01 c0 a8 ...:.....K]
0020 01 09 00 35 fb 0c 00 4b 5d d3 00 02 81 80 00 011 1.1.1.i
0030 00 01 00 00 00 01 31 01 31 01 31 07 69n-addr-a rpa.....
0040 6e 2d 61 64 64 72 04 61 72 70 61 00 00 0c 00 01oneone
0050 c0 0c 00 0c 00 01 00 00 01 d7 00 11 03 6f 6e 65oneone
0060 03 6f 6e 65 03 6f 6e 65 03 6f 6e 65 00

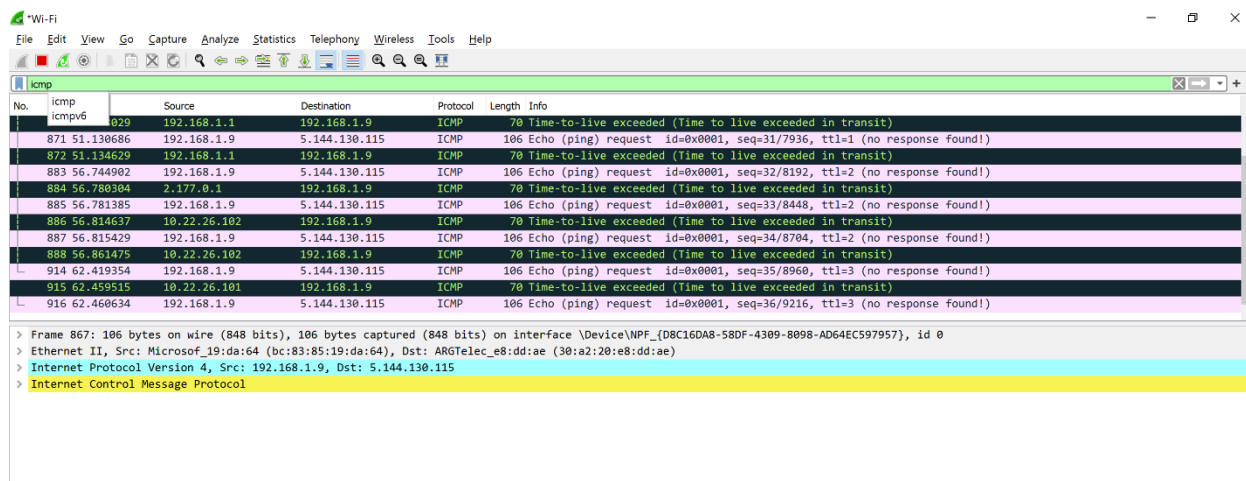
جواب سوال ۱۰ –

NS – CDS – AAAA – MX

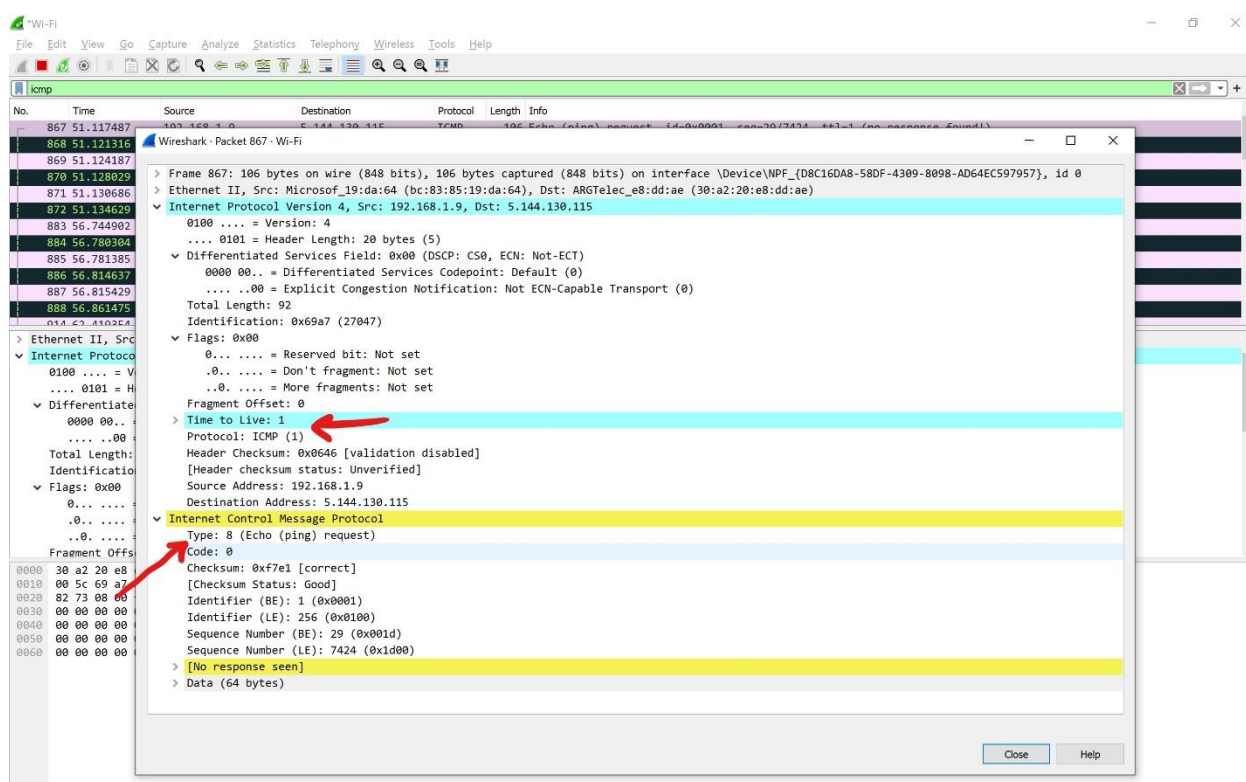
جواب سوال ۱۱ -

آن دسته از بسته‌هایی که Ip آنها مقداری برابر با سایت داده شده دارند که در اینجا 5.144.130.115 هستند نشان داده می‌شوند.

Protocol icmp مشاهده می‌شود.

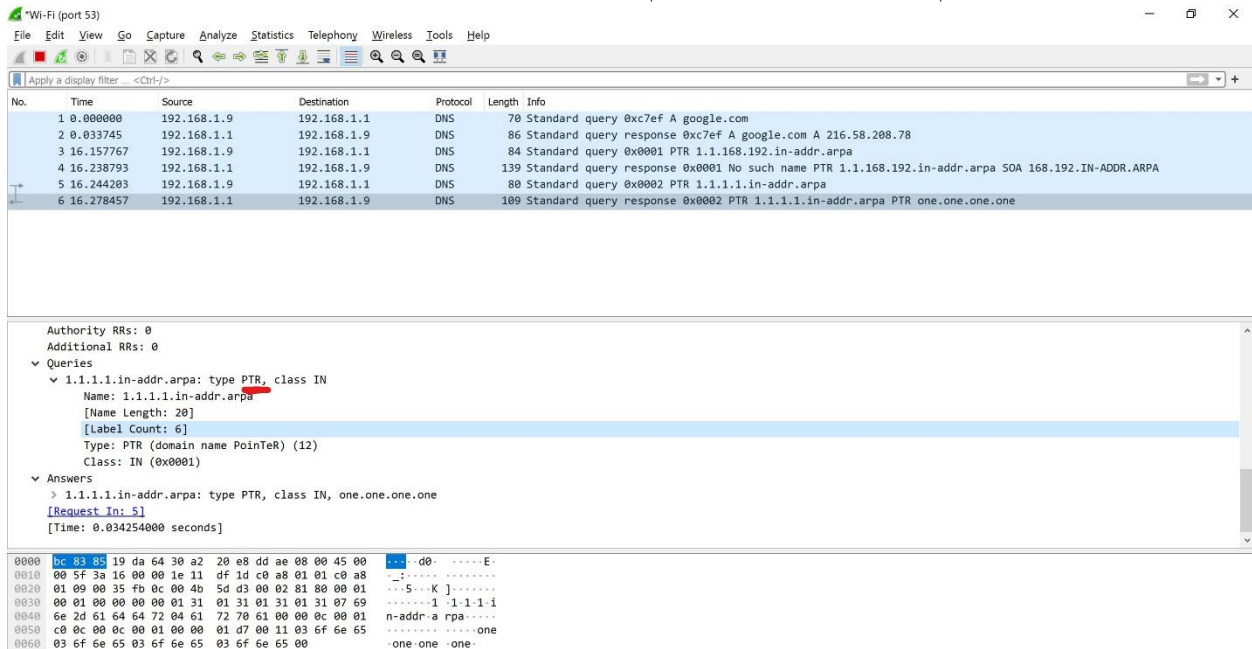


جواب سوال ۱۲ - مقدار type = 8 و TTL = 1 می‌باشد.



جواب سوال ۱۳ -

بیانگر تعداد گام‌ها تا زمانی که بسته از بین می‌رود می‌باشد و هرگامی که جلو می‌رود ۱ واحد کم می‌شود. همچنین با اضافه کردن و یا مقداردهی آن می‌توان تعداد گام‌های ممکن برای بسته را تنظیم کرد.



جواب سوال ۱۴ -

بسته‌هایی که protocol آنها TCP و یا TLSV1.2-3 است را فیلتر می‌کند.