به نام خدا

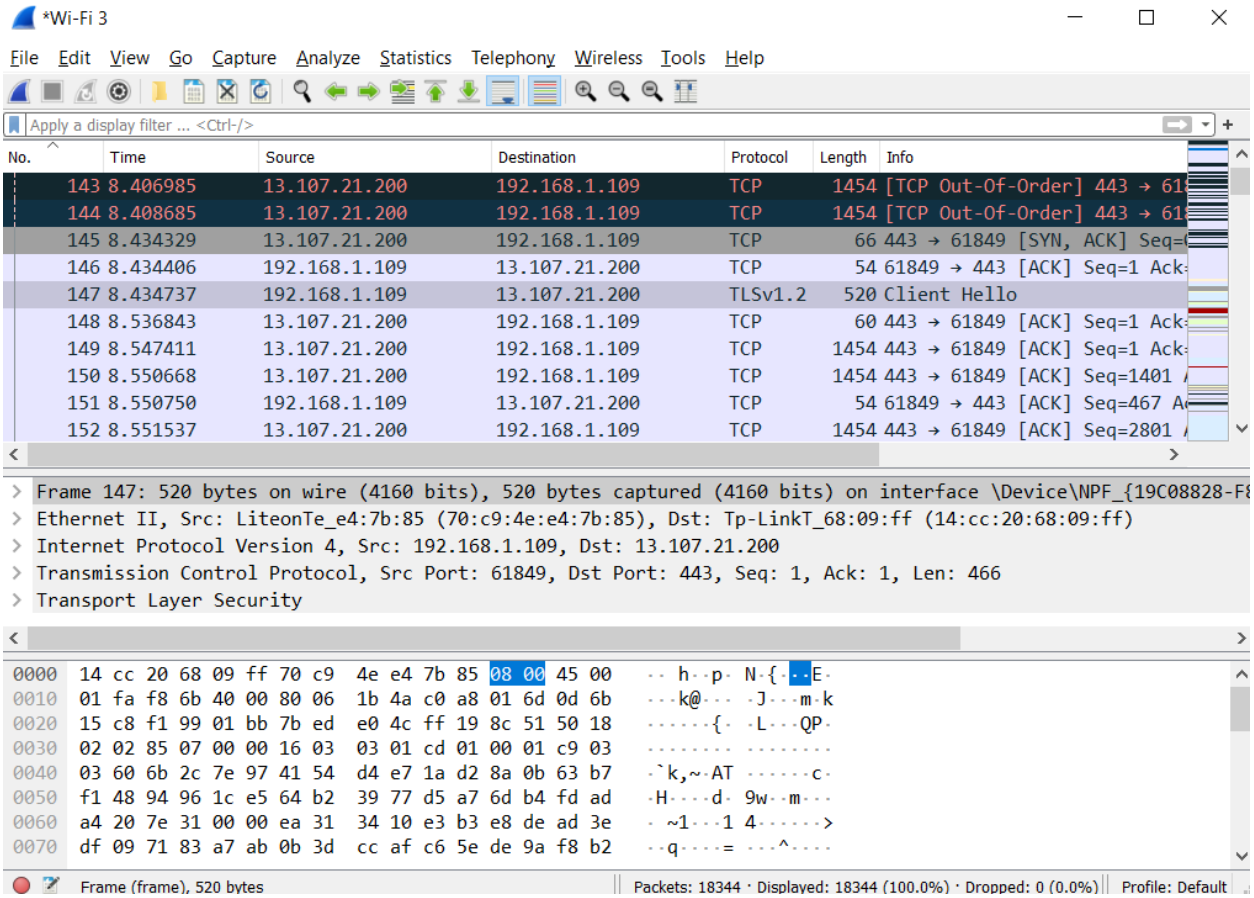
محمدمهدی هجرتی	۹۷۲۳۱۰۰
آزمایشگاه شبکه - آزمایش سوم	آشنایی با وایرشارک
استاد نقی زاده	۱۶ فروردین ۱۴۰۰

سوال ۱

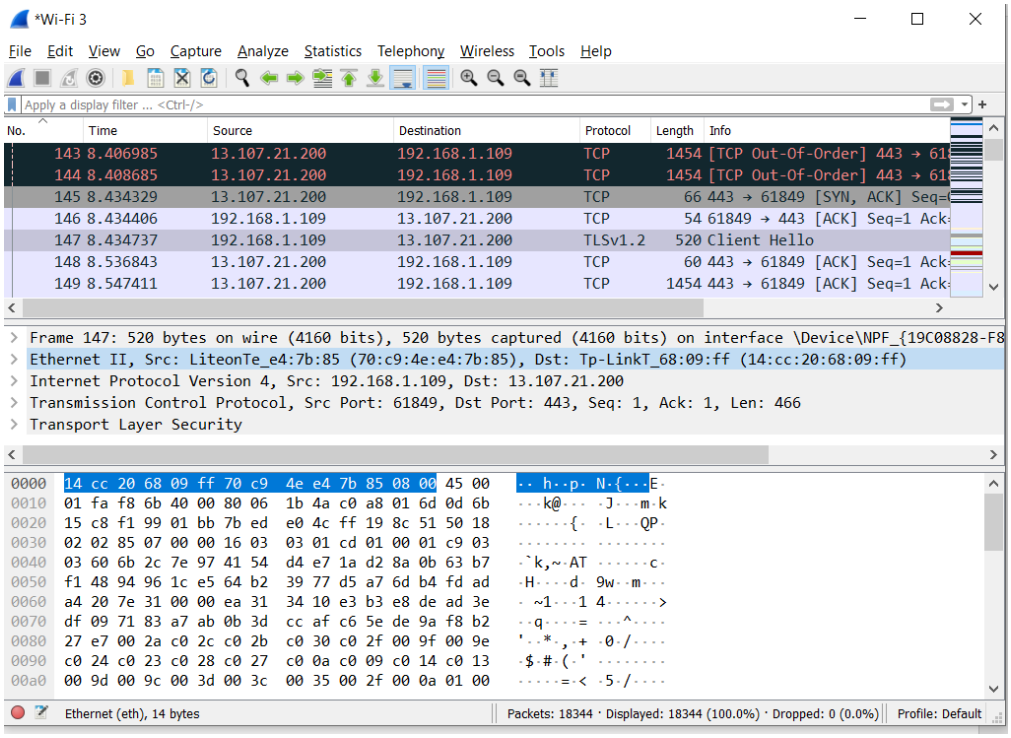
پروتکل های TCP, TLS, DNS, SSL, ARP, QUIC, IGMP, SSDP, RIP دیده می‌شود.

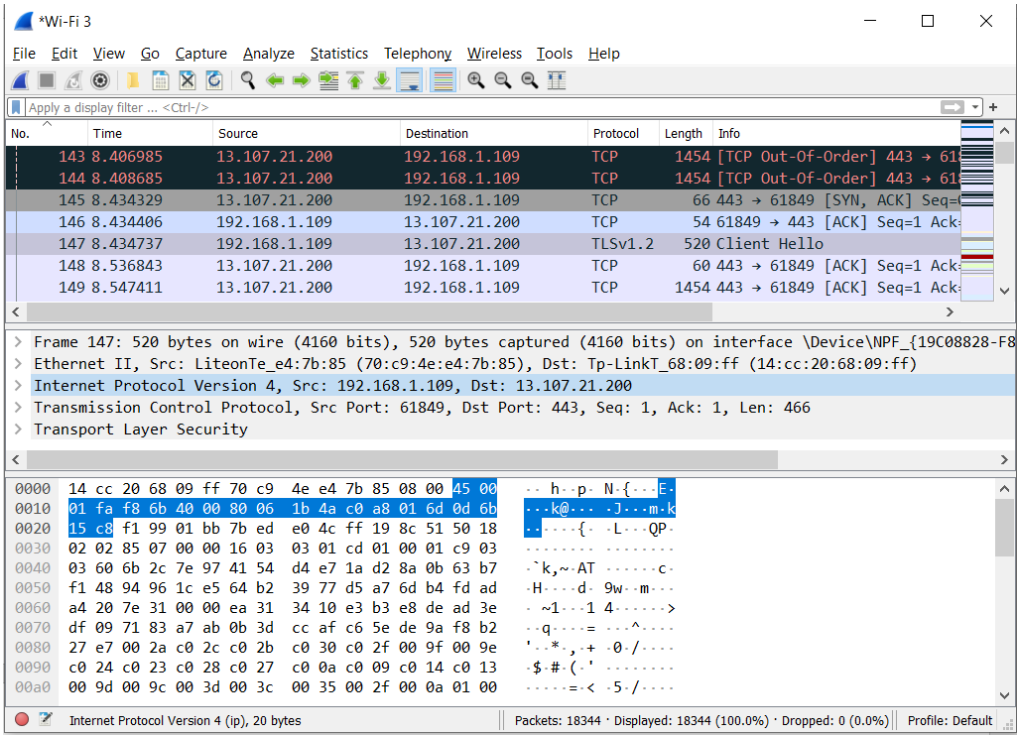
سوال ۲

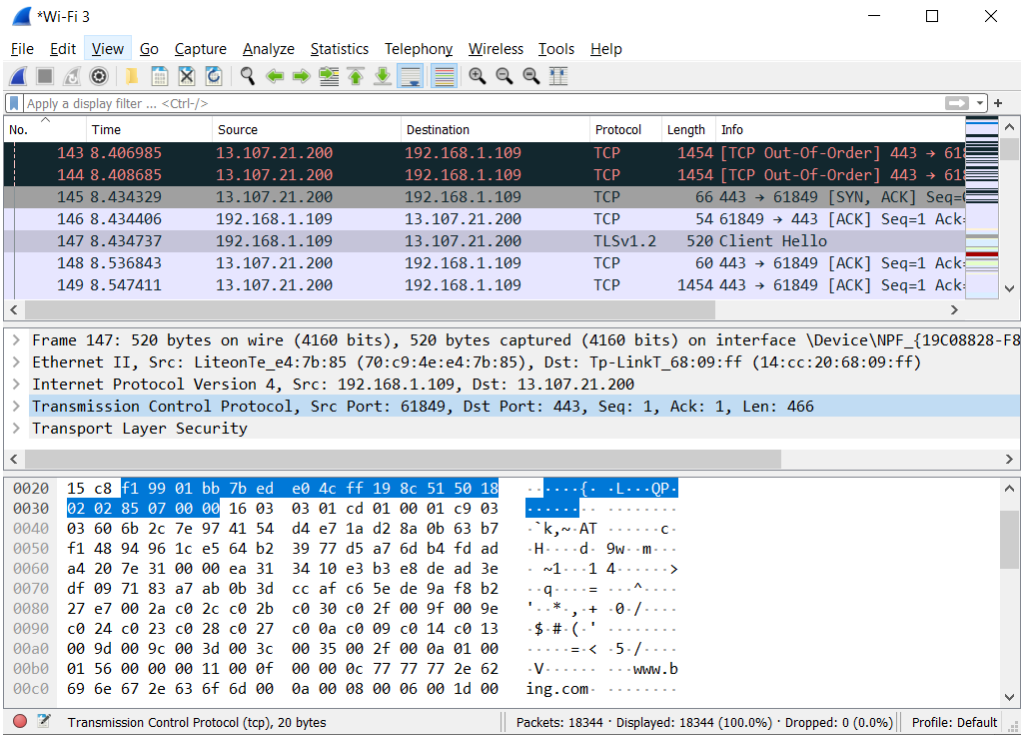
به ترتیب پروتکل Ethernet II در لایه ی data link، IPv4 در لایه ی internet، TCP در لایه ی transport، TLS در لایه ی application استفاده شده است.

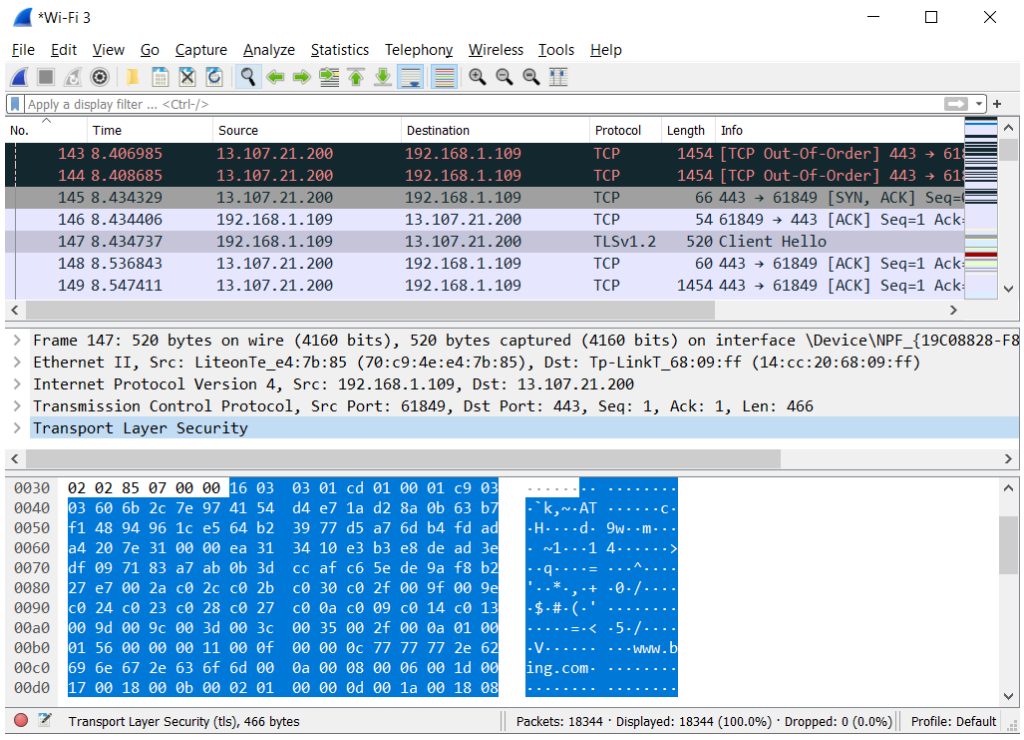


ترتیب قرارگیری بیت ها، به ترتیب شماره لایه ها می باشد. یعنی ابتدا بیت های مربوط به لایه ی data link قرار گرفته است و پس از آن لایه ی internet، transport و در آخر application قرار گرفته است.

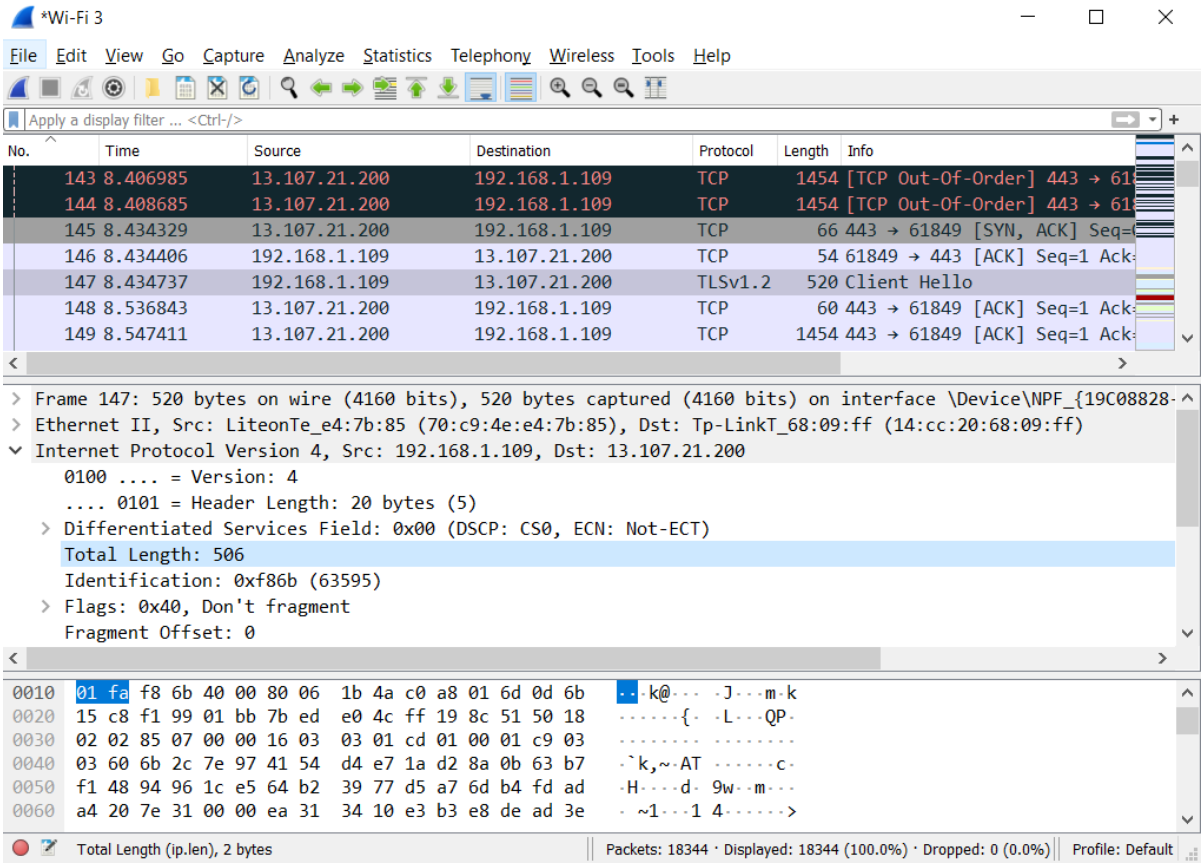





*Wi-Fi 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
143 8.406985 13.107.21.200 192.168.1.109 TCP 1454 [TCP Out-Of-Order] 443 → 61
144 8.408685 13.107.21.200 192.168.1.109 TCP 1454 [TCP Out-Of-Order] 443 → 61
145 8.434329 13.107.21.200 192.168.1.109 TCP 66 443 → 61849 [SYN, ACK] Seq=
146 8.434406 192.168.1.109 13.107.21.200 TCP 54 61849 → 443 [ACK] Seq=1 Ack
147 8.434737 192.168.1.109 13.107.21.200 TLSv1.2 520 Client Hello
148 8.536843 13.107.21.200 192.168.1.109 TCP 60 443 → 61849 [ACK] Seq=1 Ack
149 8.547411 13.107.21.200 192.168.1.109 TCP 1454 443 → 61849 [ACK] Seq=1 Ack
Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-F8
Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200
Transmission Control Protocol, Src Port: 61849, Dst Port: 443, Seq: 1, Ack: 1, Len: 466
Transport Layer Security
0020 15 c8 f1 99 01 bb 7b ed e0 4c ff 19 8c 51 50 18
0030 02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03
0040 03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7
0050 f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad
0060 a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e
0070 df 09 71 83 a7 ab 0b 3d cc af c6 5e de 9a f8 b2
0080 27 e7 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e
0090 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13
00a0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00
00b0 01 56 00 00 00 11 00 0f 00 00 0c 77 77 77 2e 62
00c0 69 6e 67 2e 63 6f 6d 00 0a 00 08 00 06 00 1d 00
Transmission Control Protocol (tcp), 20 bytes
Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

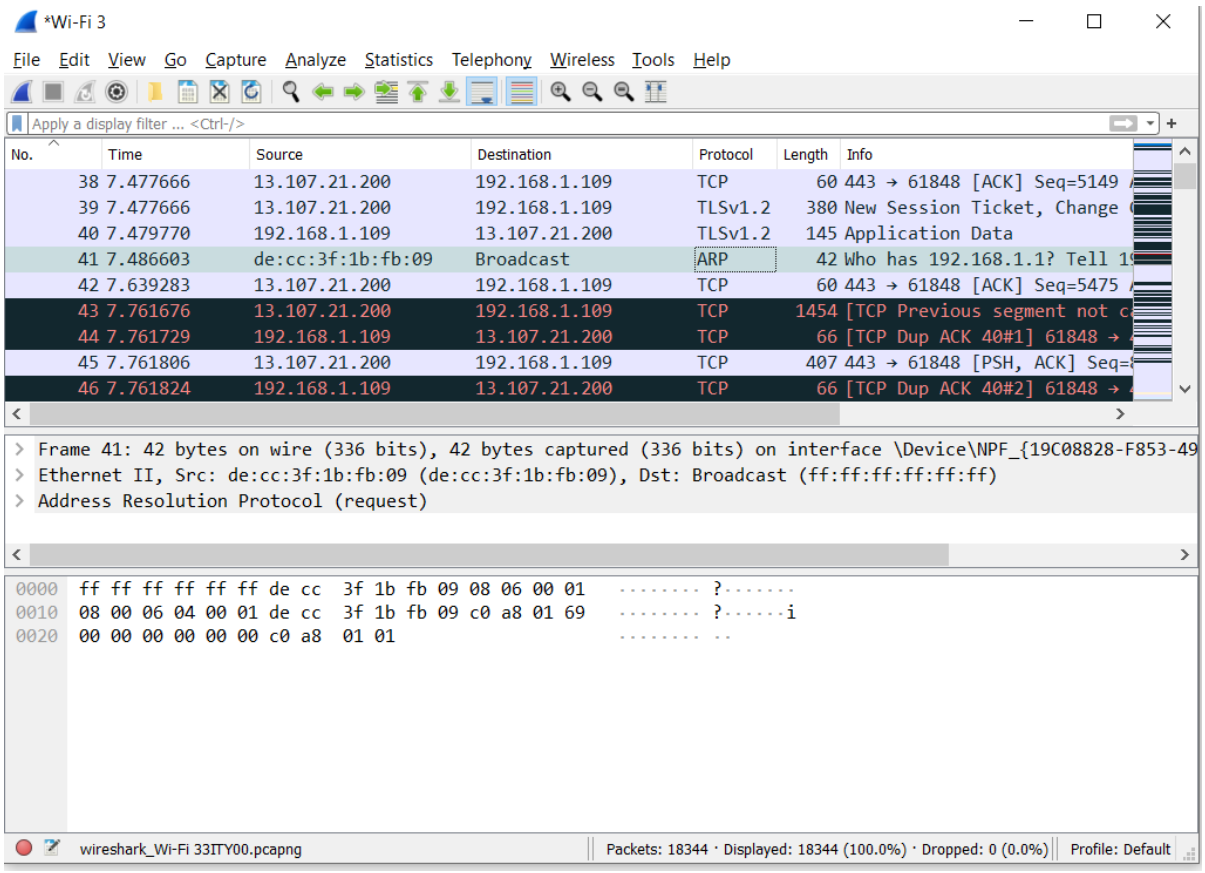

*Wi-Fi 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
143 8.406985 13.107.21.200 192.168.1.109 TCP 1454 [TCP Out-Of-Order] 443 → 61
144 8.408685 13.107.21.200 192.168.1.109 TCP 1454 [TCP Out-Of-Order] 443 → 61
145 8.434329 13.107.21.200 192.168.1.109 TCP 66 443 → 61849 [SYN, ACK] Seq=
146 8.434406 192.168.1.109 13.107.21.200 TCP 54 61849 → 443 [ACK] Seq=1 Ack
147 8.434737 192.168.1.109 13.107.21.200 TLSv1.2 520 Client Hello
148 8.536843 13.107.21.200 192.168.1.109 TCP 60 443 → 61849 [ACK] Seq=1 Ack
149 8.547411 13.107.21.200 192.168.1.109 TCP 1454 443 → 61849 [ACK] Seq=1 Ack
Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-F8
Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200
Transmission Control Protocol, Src Port: 61849, Dst Port: 443, Seq: 1, Ack: 1, Len: 466
Transport Layer Security
0030 02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03
0040 03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7
0050 f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad
0060 a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e
0070 df 09 71 83 a7 ab 0b 3d cc af c6 5e de 9a f8 b2
0080 27 e7 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e
0090 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13
00a0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00
00b0 01 56 00 00 00 11 00 0f 00 00 0c 77 77 77 2e 62
00c0 69 6e 67 2e 63 6f 6d 00 0a 00 08 00 06 00 1d 00
00d0 17 00 18 00 0b 00 02 01 00 00 0d 00 1a 00 18 08
Transport Layer Security (tls), 466 bytes
Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

اندازه ی فریم ۵۲۰ بایت و اندازه ی پکت ۵۰۶ بایت است.



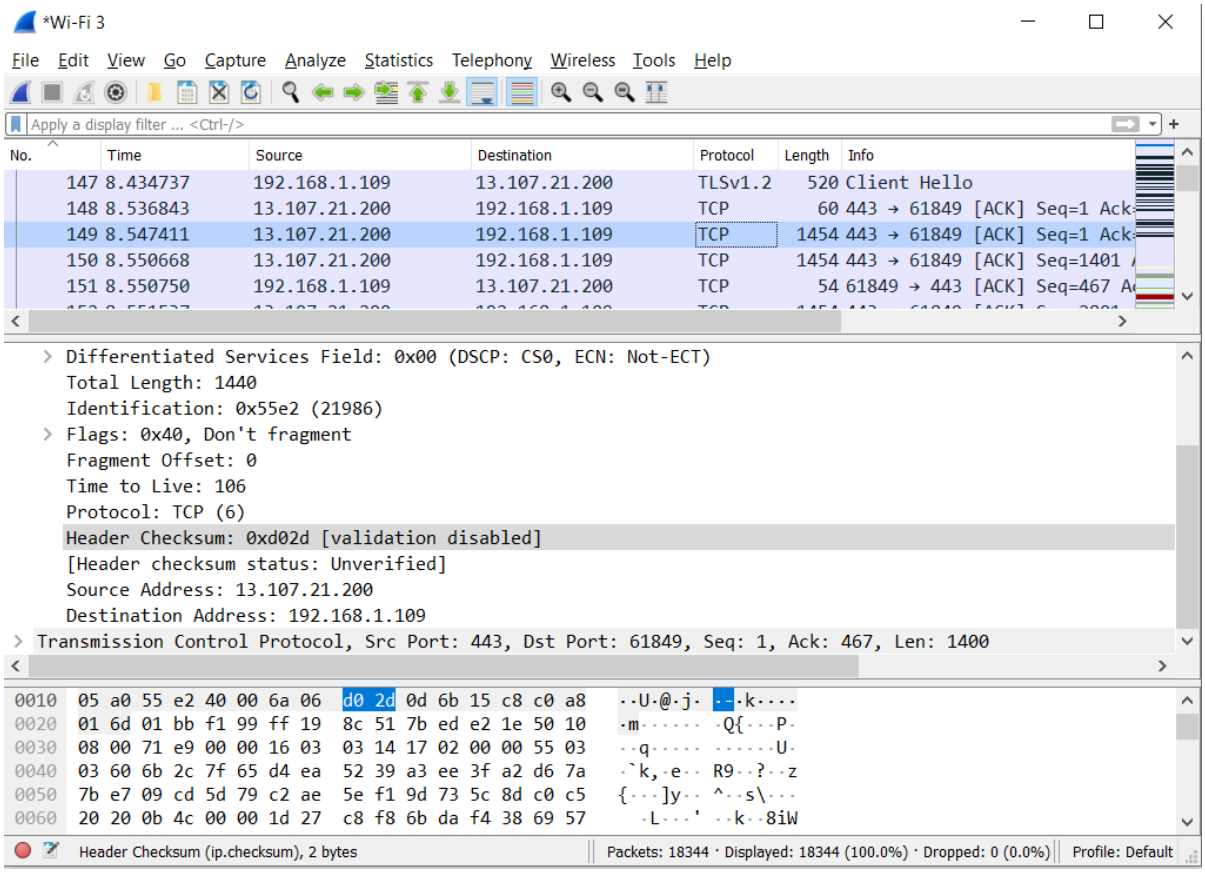
سوال ۳

این بسته از پروتکل ARP استفاده می کند.



سوال ۴

نمایش هگز checksum این پکت به صورت d02d می باشد که به معنای validation disabled است.



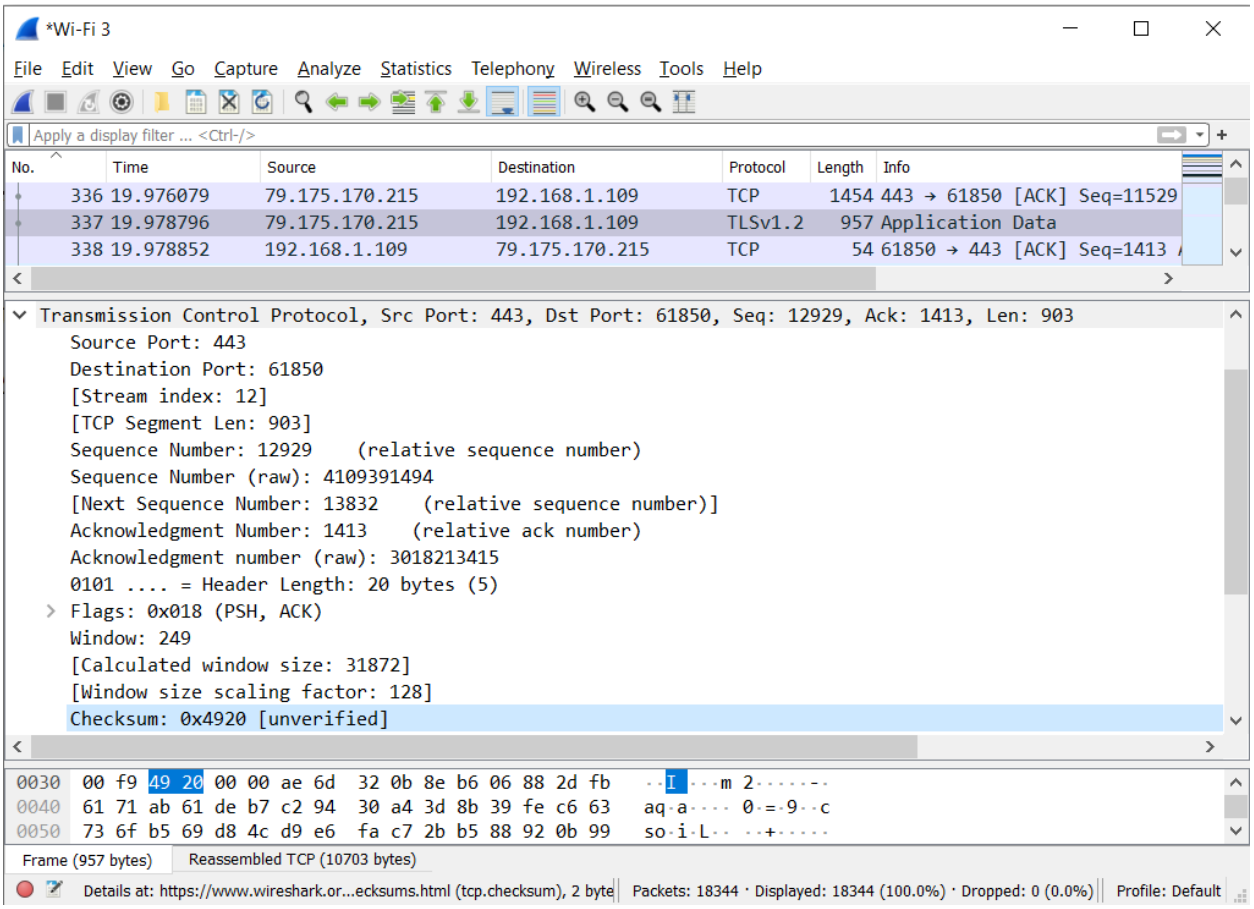
سوال ۵

این بسته از پروتکل TCP استفاده می کند.

پورت مبدا آن ۴۴۳ و مقصد ۶۱۸۵۰ می باشد.

عدد پورت، اپلیکیشنی را در سیستم مبدا یا مقصد مشخص می کند که قرار است با آن ارتباط برقرار شود و پکت ها مربوط به آن هستند.

نمایش هگز checksum پروتکل TCP این پک به صورت 4920 می باشد که unverified است.



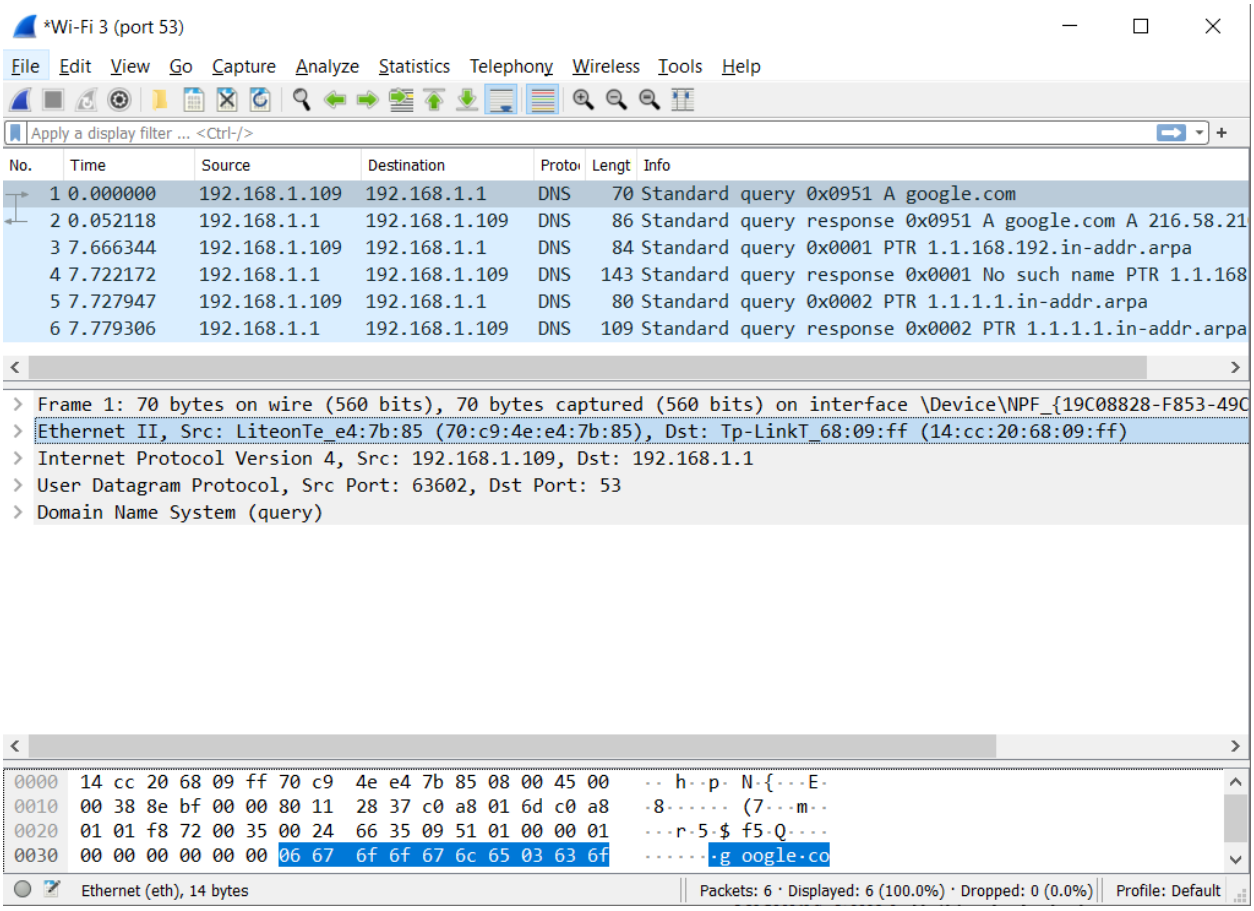
سوال ۶

پروتکل لایه ی Transport در این پکت، UDP می باشد.

آدرس آی پی مبدا 192.168.1.109 است.

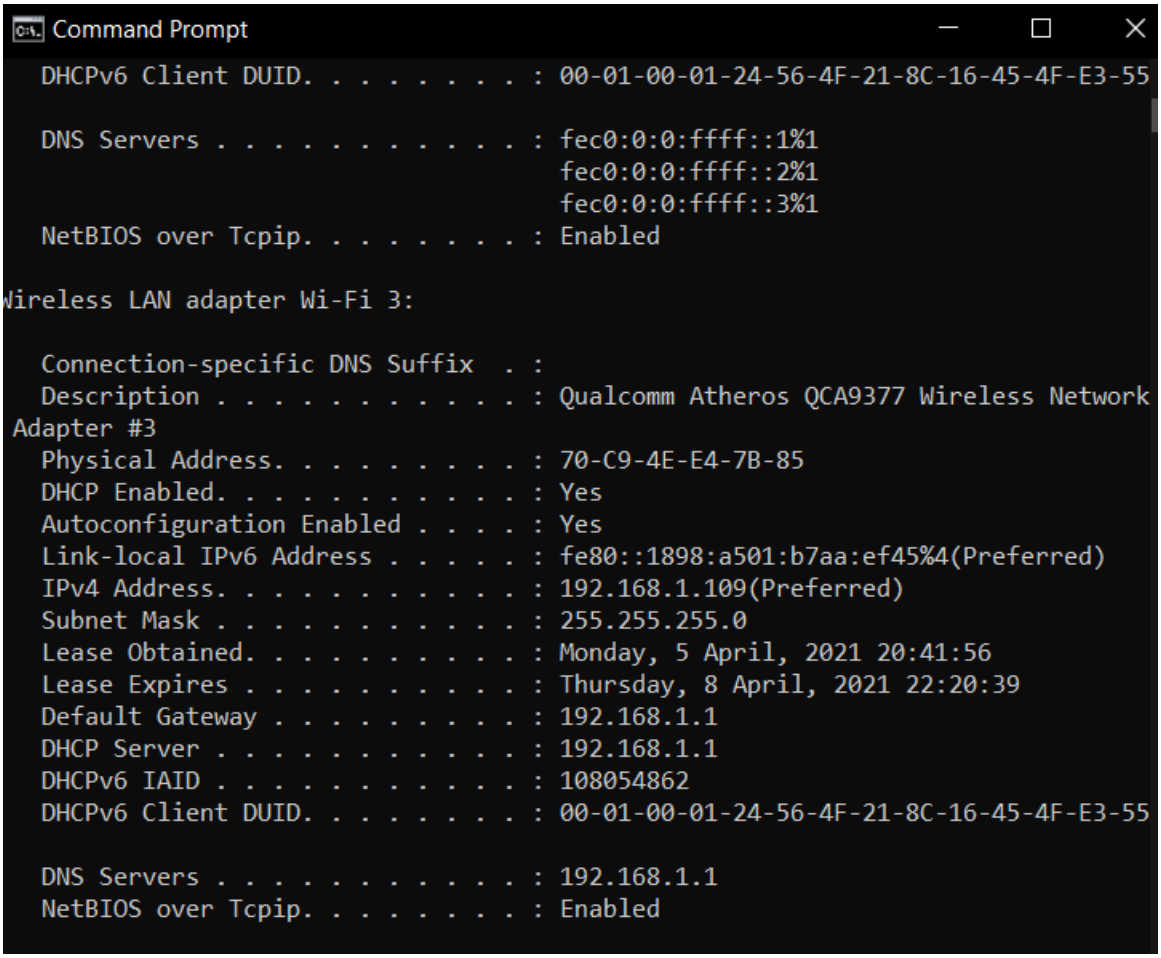
آدرس آی پی مقصد 192.168.1.1 است.

آدرس آی پی ورژن۶ مبدا 70:c9:4e:7b:85 و مقصد 14:cc:68:09:ff است.



سوال ۷

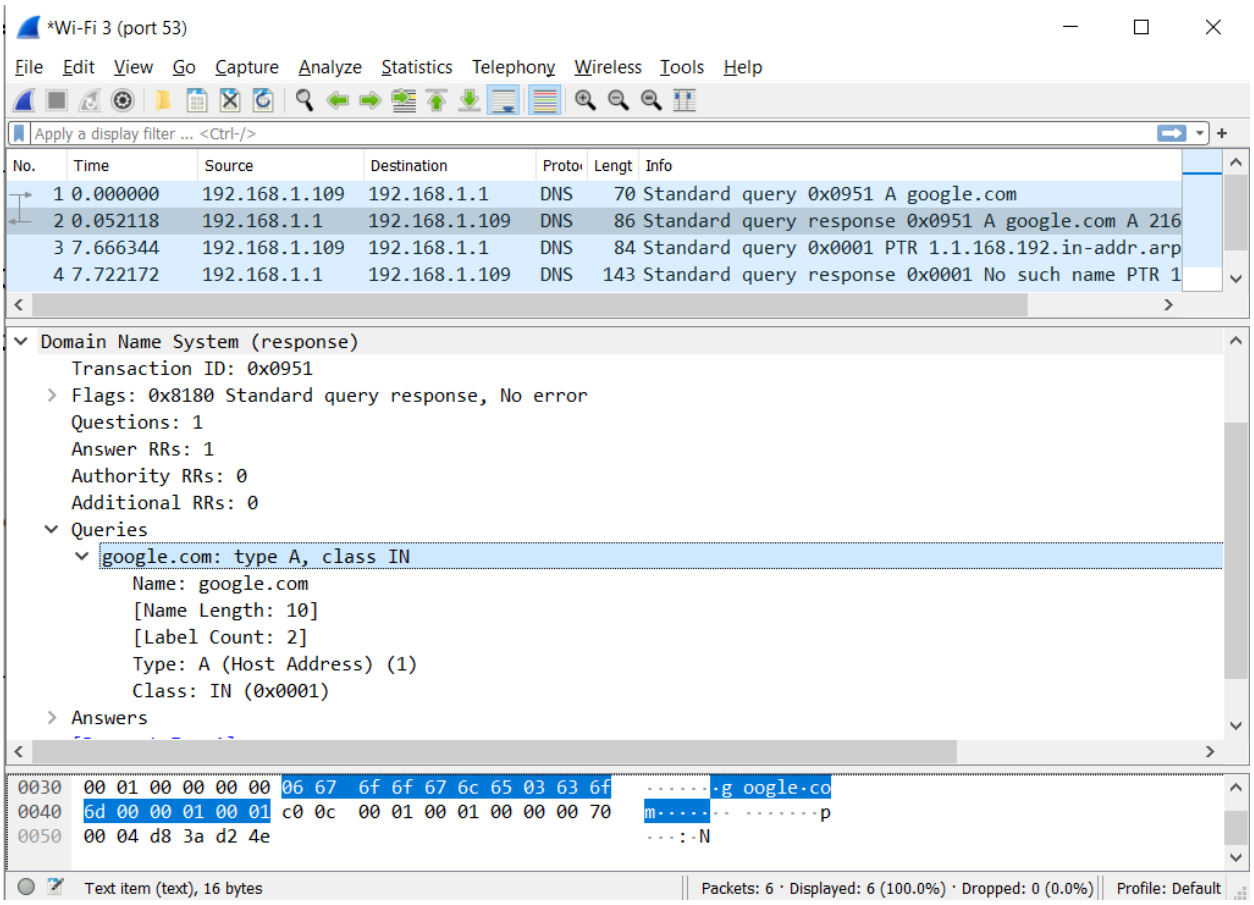
آدرس آی پی اینترفیس انتخاب شده برای کپچر کردن پکت (وای فای۳) همان آدرس مبدا در سوال قبل می باشد.



سوال ۸

رکورد از نوع A زده شده است.

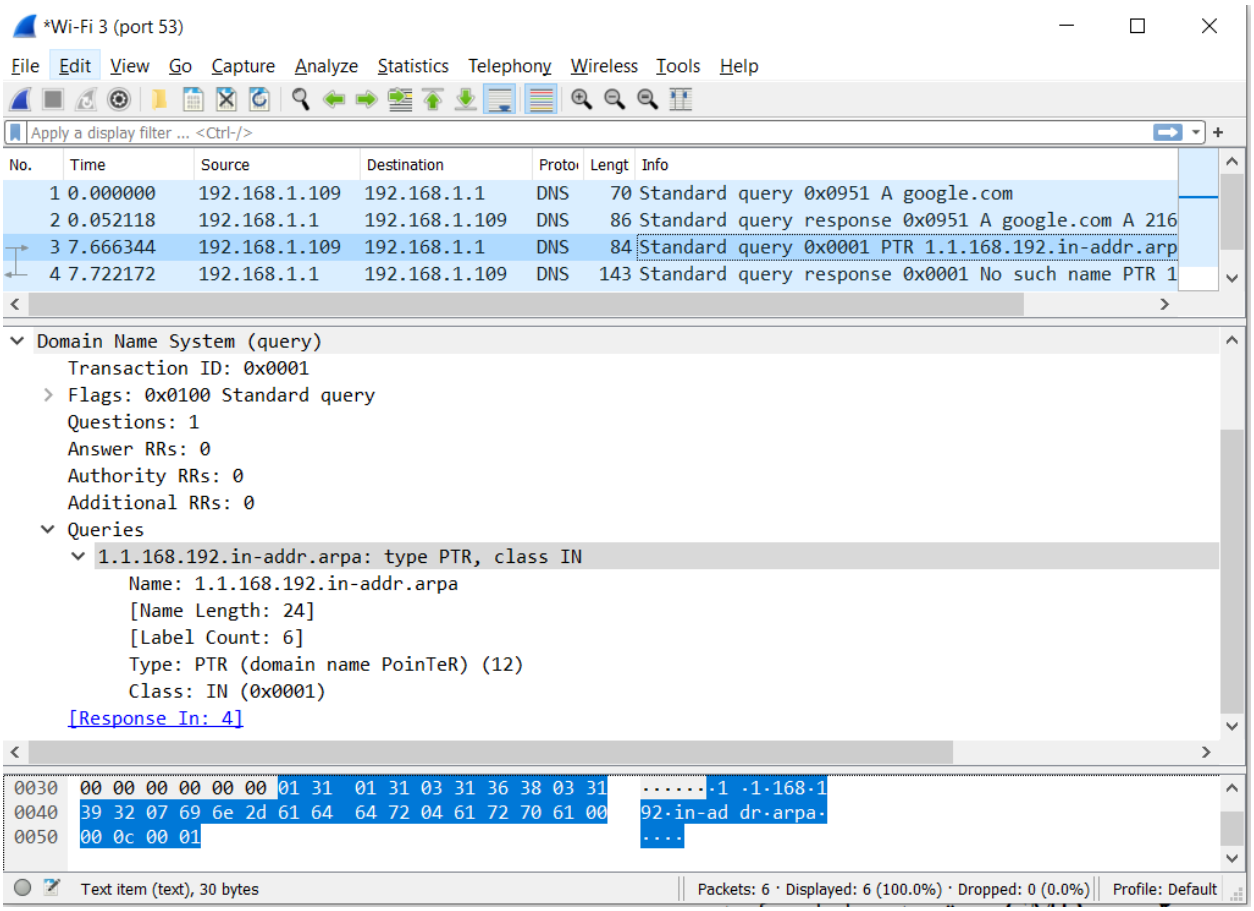
بدین معنا که آدرس آی پی ورژن۴ سایت گوگل با DNS خواسته شده است.



سوال ۹

رکورد از نوع PTR یا pointer زده شده است.

بدین معنا که با وارد کردن آدرس آی پی، میخواهیم اسم دامنه ی سایت مورد نظر را بدست بیاوریم.



سوال ۱۰

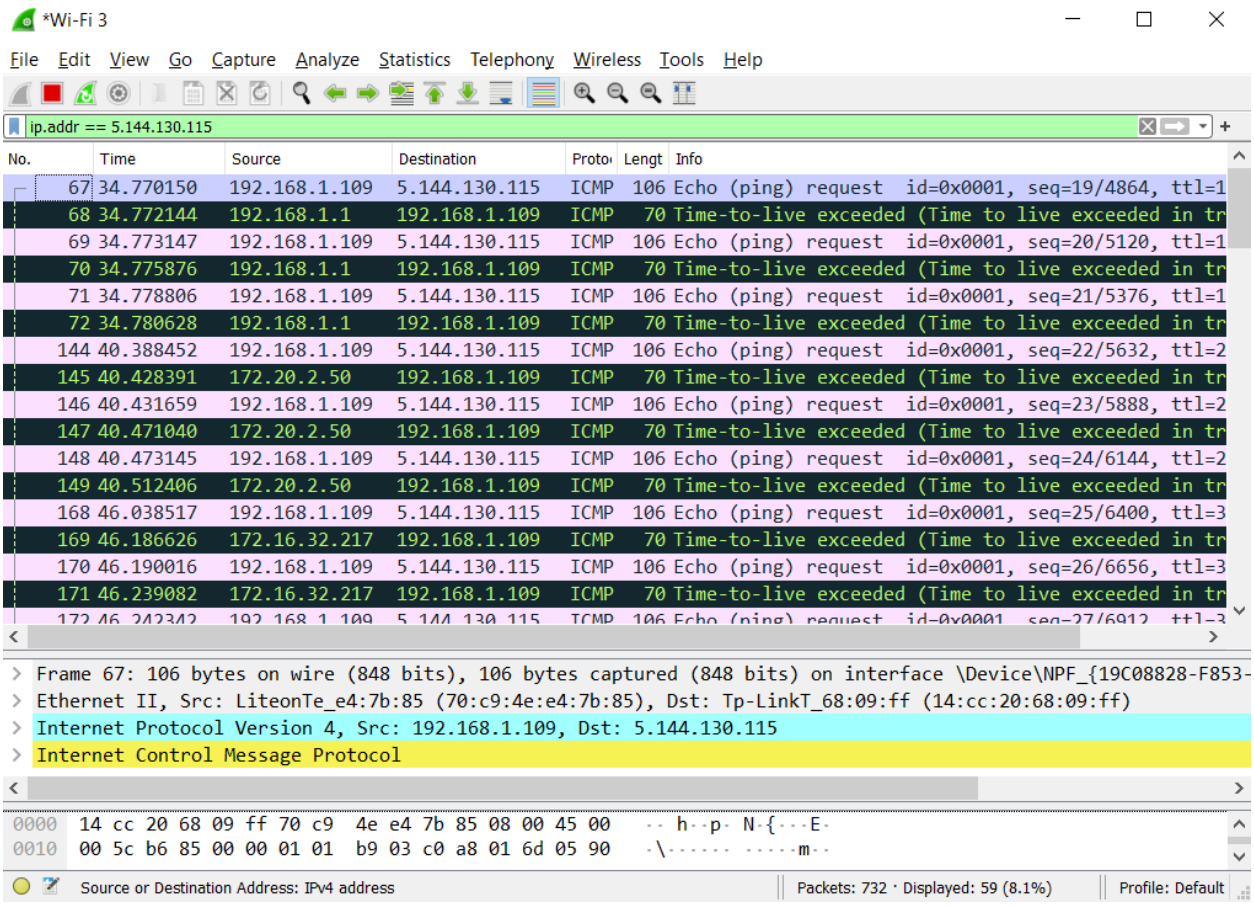
AAAA: مشابه رکورد A می باشد با این تفاوت که آی پی ورژن ۶ درخواست شده است.

NS: آدرس DNS server معتبر برای این دامنه را ثبت می کند.

MX: برای هدایت ایمیل ها به سمت سرور ایمیل استفاده می شود.

سوال ۱۱

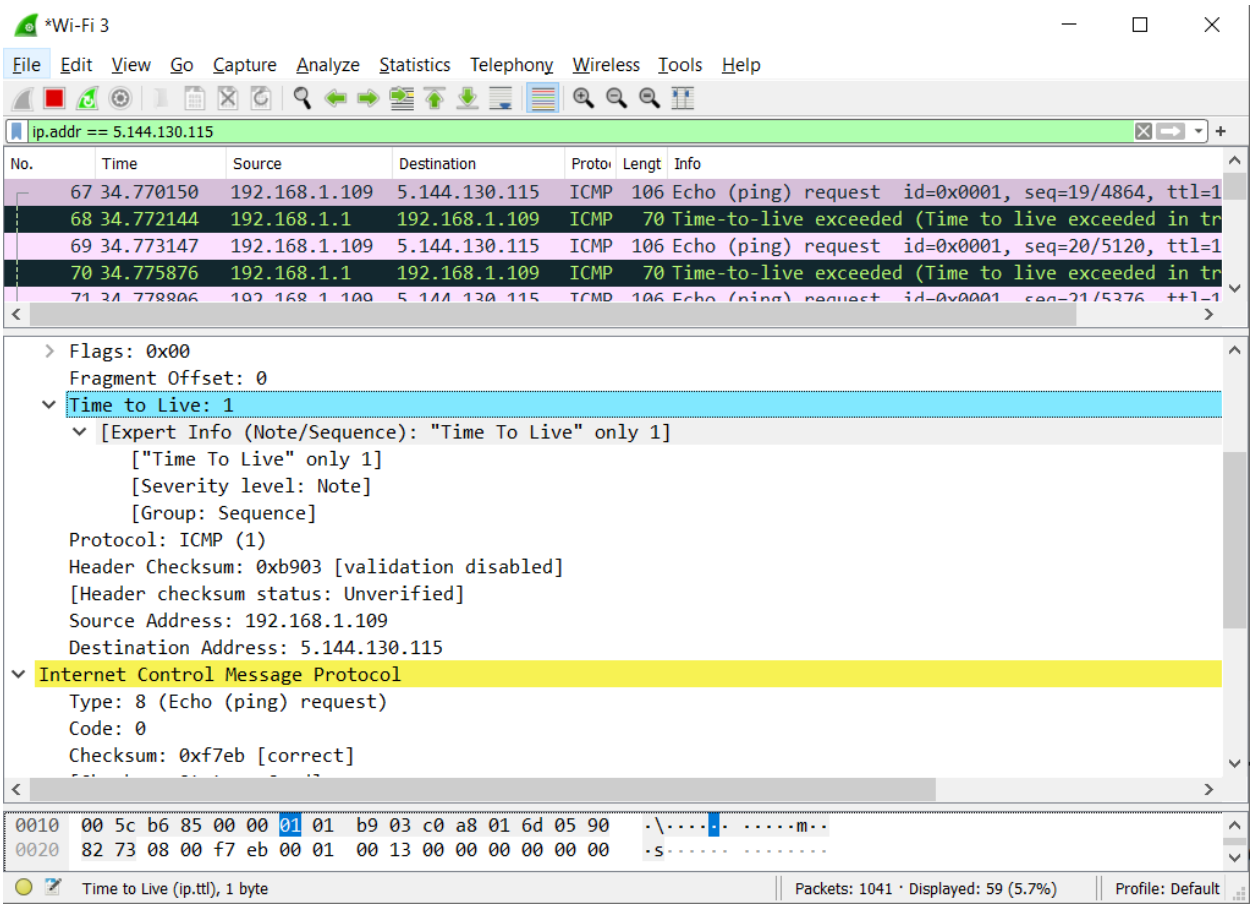
بسته های نمایش داده شده تماما از پروتکل ICMP می باشد.



سوال ۱۲

عدد type برابر ۸ می باشد به معنای ping request

مقدار عدد time to live برابر ۱ می باشد.



سوال ۱۳

مقدار عدد ttl برای بسته های ارسالی از ۱ تا ۱۱ افزایش یافته است.

از طرفی با توجه به بررسی tracert میبینیم که ۱۱ گره در مسیر تا مقصد وجود دارد.

به نظر می رسد فرستنده ی پکت ها با توجه به فاصله ی مبدا تا گره ها، ttl را تنظیم می کند تا هر چه دروتر می شود، پکت برای زمان بیشتری زنده بماند.

سوال ۱۴

ip.proto == 6 پکت های با پروتکل tcp را فیلتر می کند.