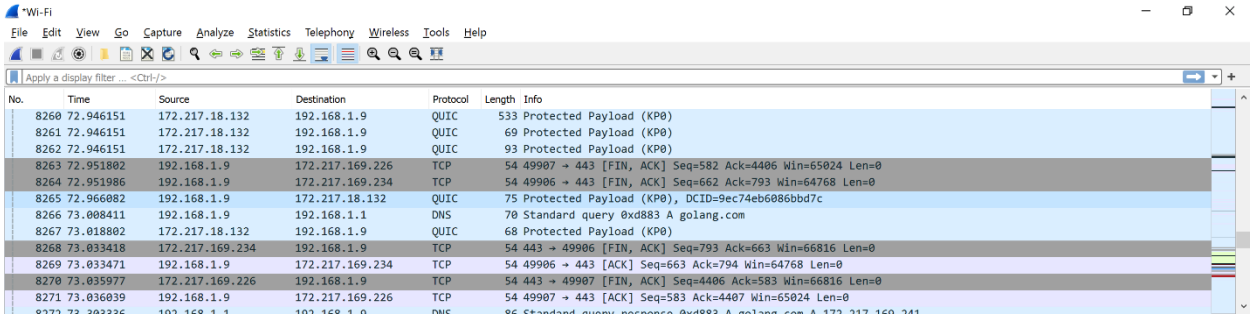
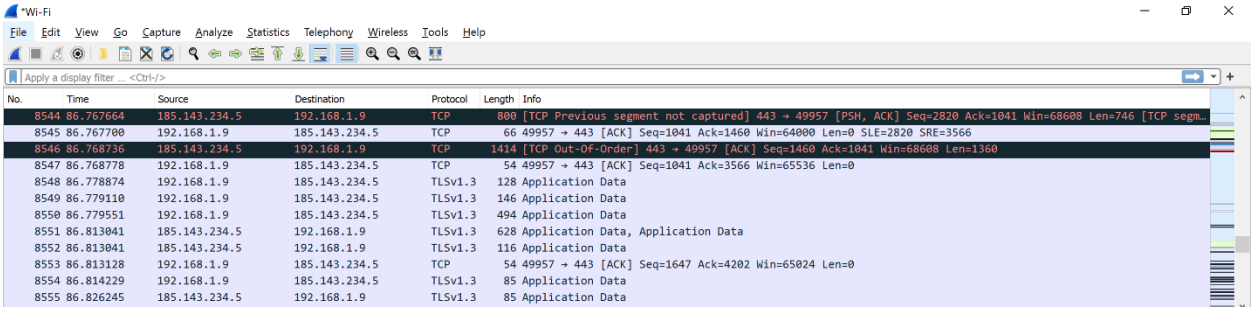
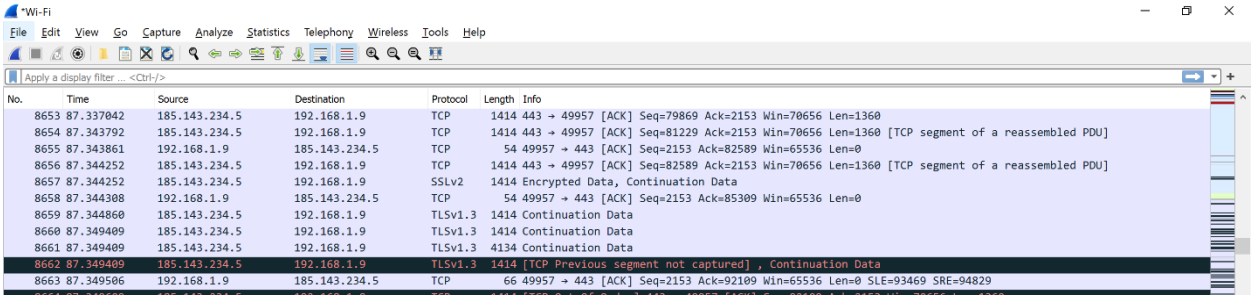
امیرمحمد راعی – ۹۷۳۱۰۸۳

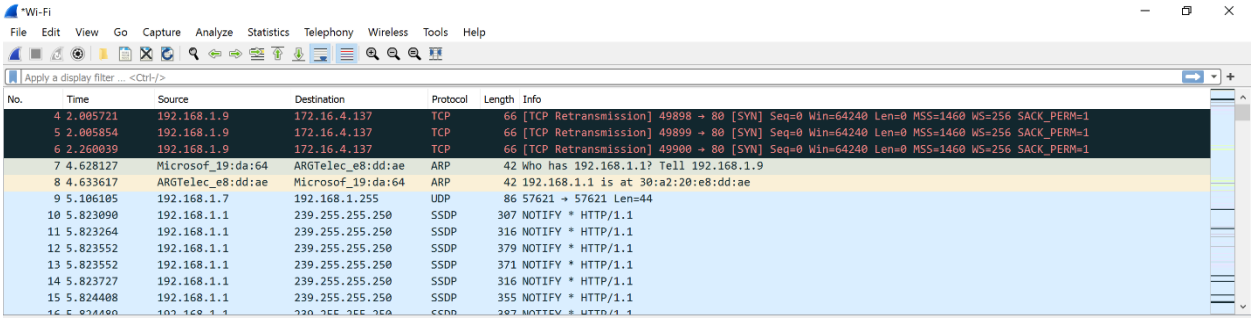
جواب سوال ۱-

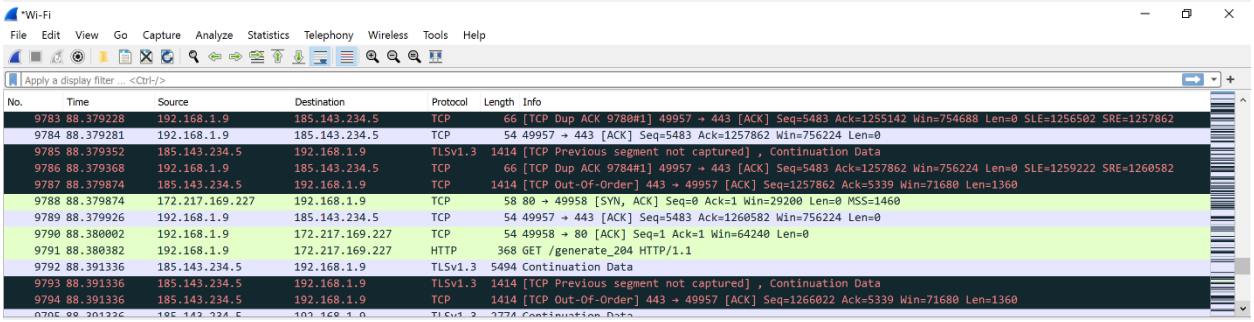
QUIC – TCP – DNS – TLSv1.3 – TLSv1.2 – SSLV2 – SSDP – ARP – UDP – HTTP – NBSN – MDNS – IGMPv2

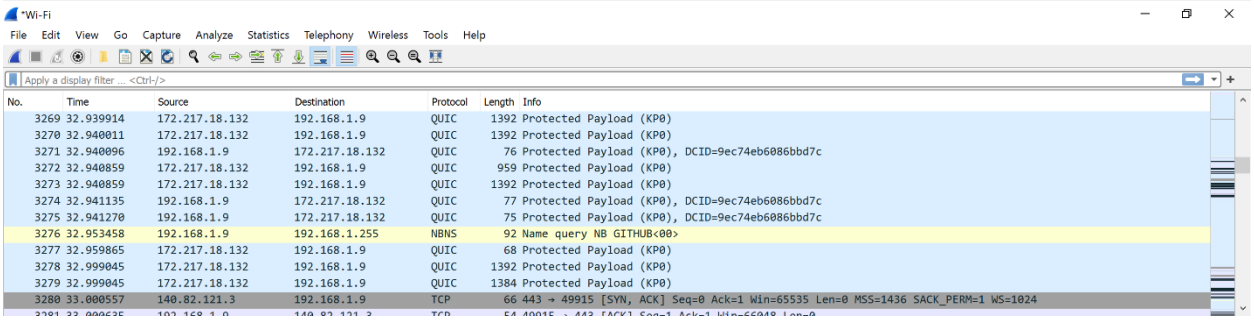


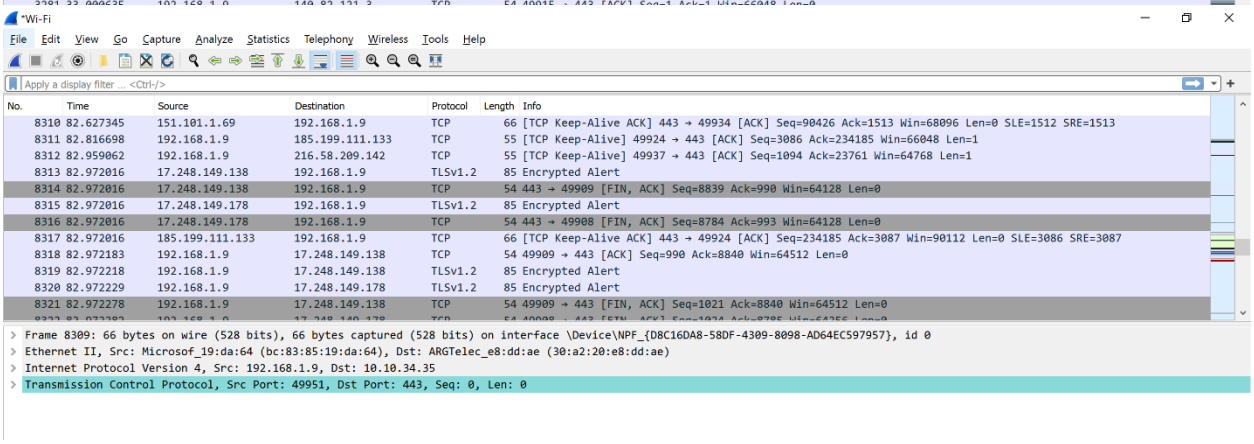





*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
4 2.005721 192.168.1.9 172.16.4.137 TCP 66 [TCP Retransmission] 49898 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5 2.005854 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

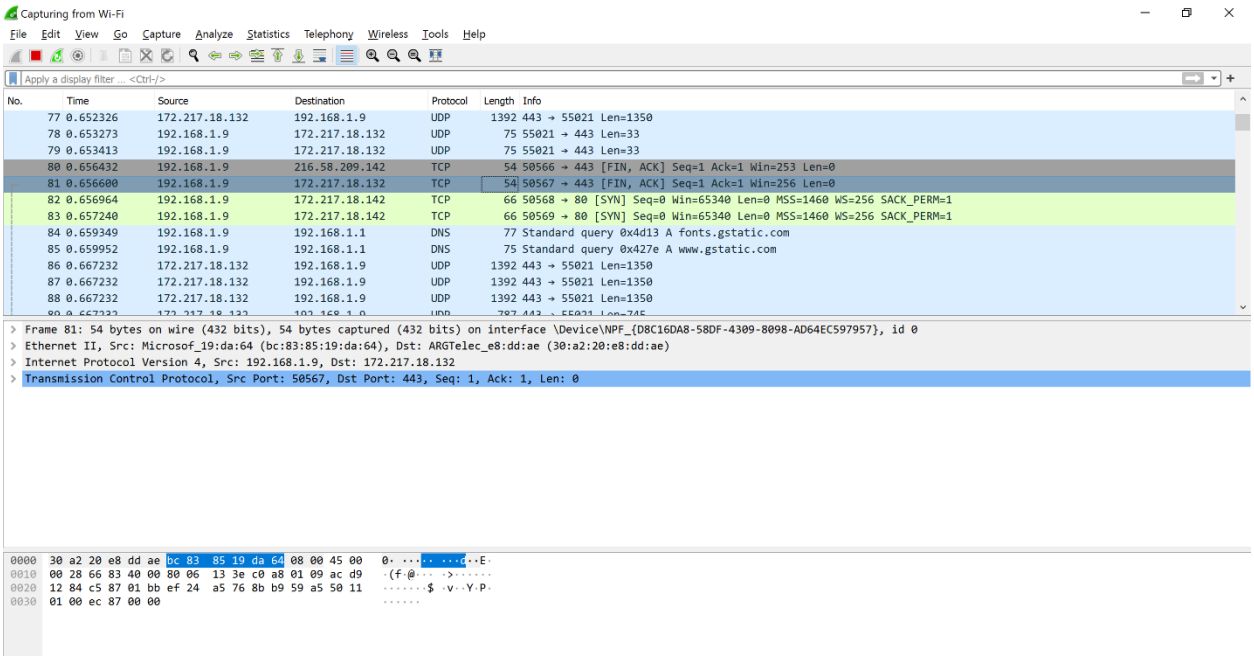

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
9783 88.379228 192.168.1.9 185.143.234.5 TCP 66 [TCP Dup ACK 9780#1] 49957 → 443 [ACK] Seq=5483 Ack=1255142 Win=754688 Len=0 SLE=1256502 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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
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
Frame 8309: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 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.



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

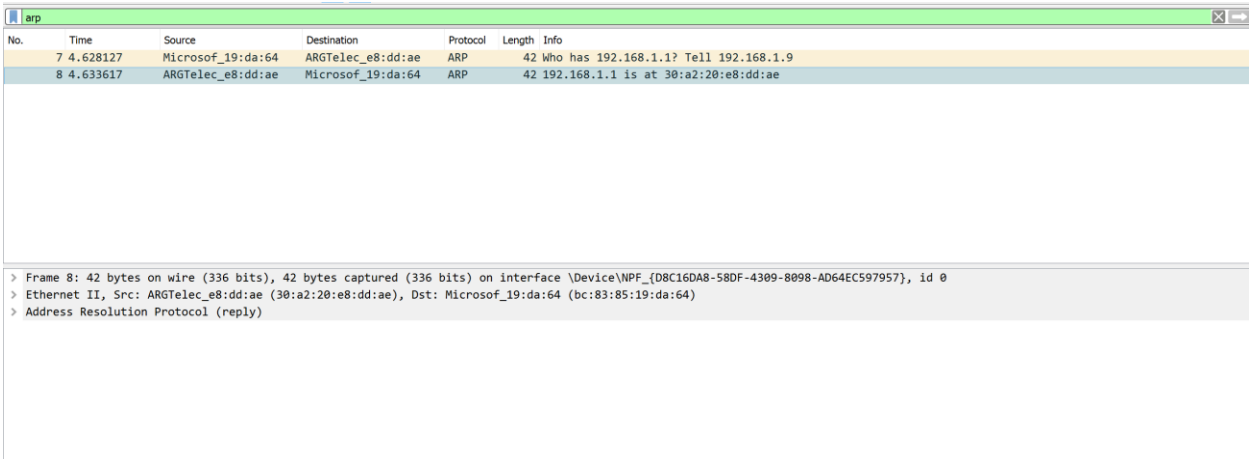
ترتیب قرار گرفتن بیت‌ها در ارتباط با ترتیب لایه‌ها می باشد. اول از همه بیت‌های مربوط به لایه‌های اول و بعد لایه‌های بعدی به ترتیب می‌ایند. به طور مثال در تصویر بالا اول بیت‌های datalink و بعد لایه network و در اخر بیت‌های مربوط به لایه transport آمده‌اند.

اندازه فریم لایه ۲ برابر ۵۴

و اندازه بسته لایه ۳ برابر ۴۰

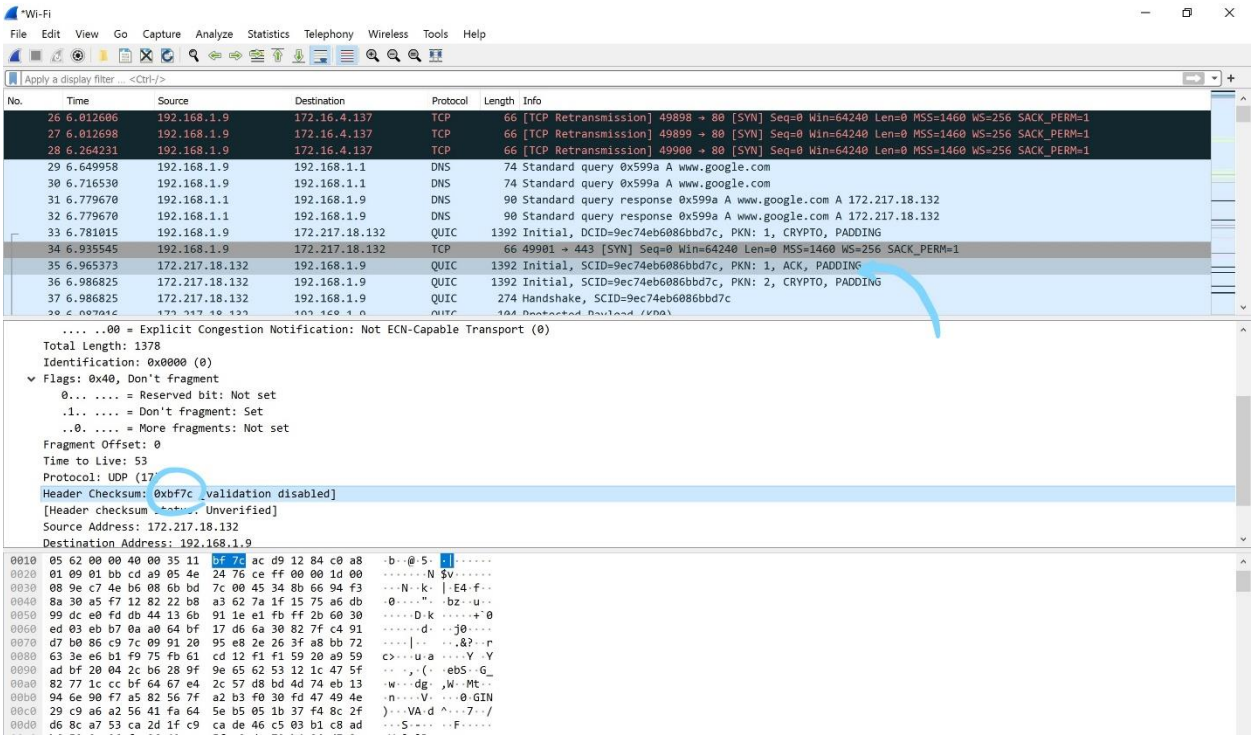
جواب سوال ۳ –

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



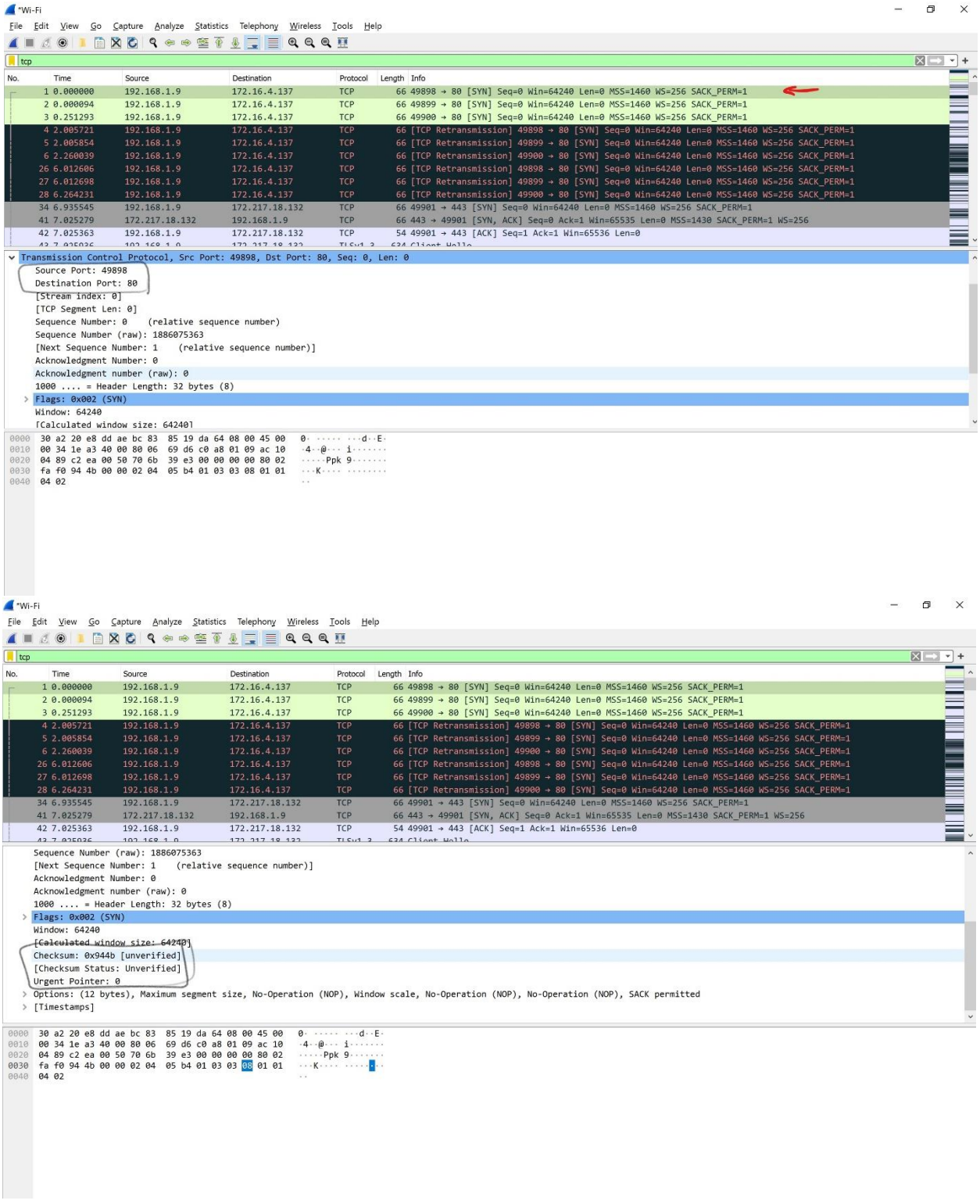
جواب سوال ۴ –

برای بسته انتخاب شده مقدار 0xbf7c نشان داده می‌شود.



جواب سوال ۵ –

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



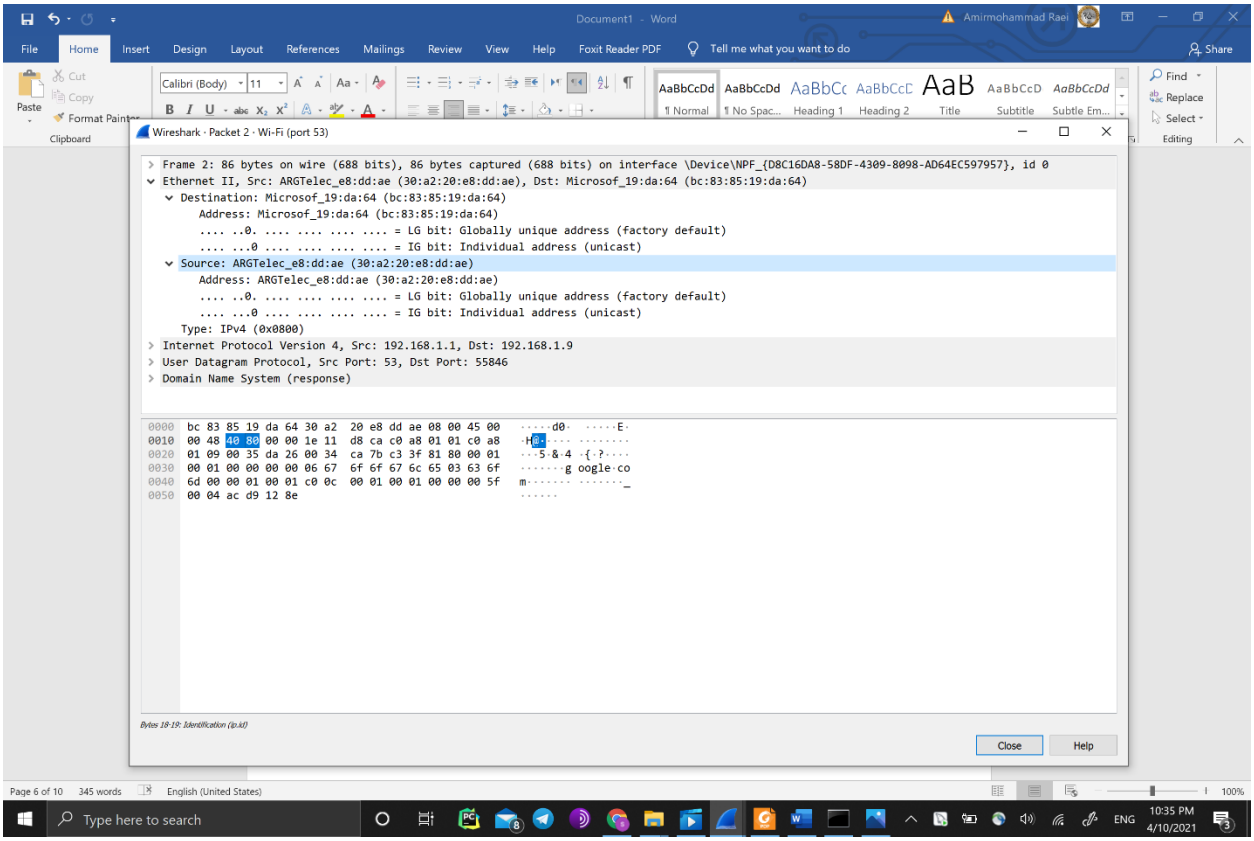
checksum مربوطه هم در عکس بالا نشان داده شده است.

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.

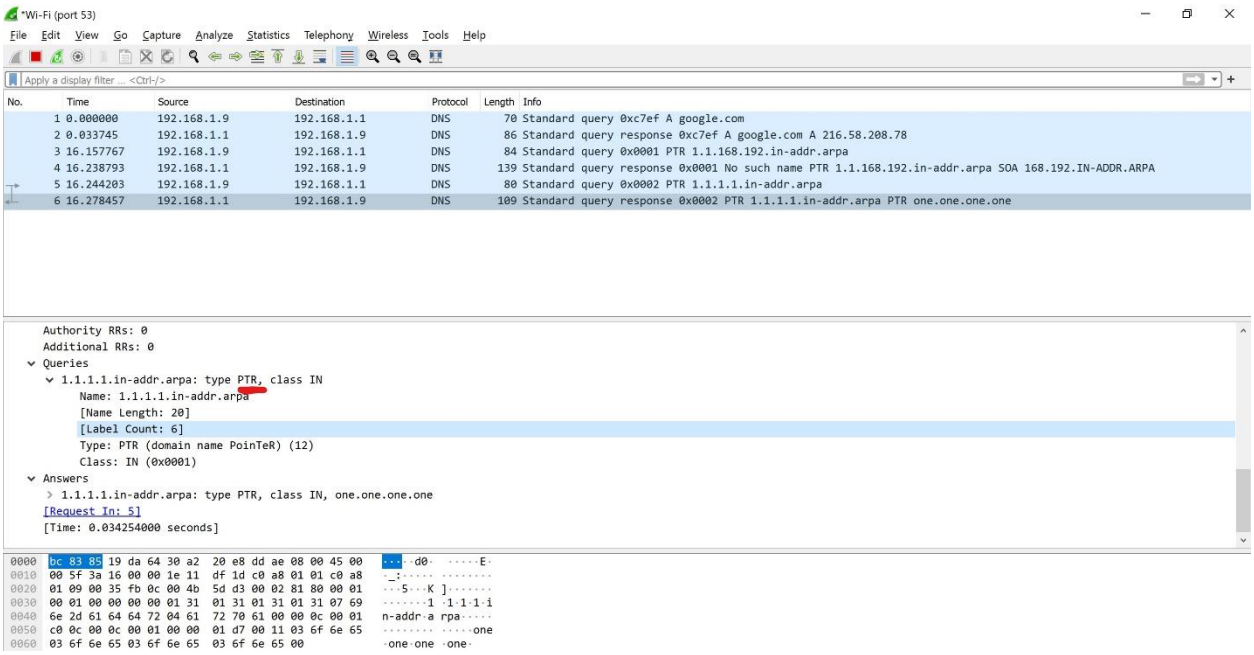
جواب سوال ۸ –

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.



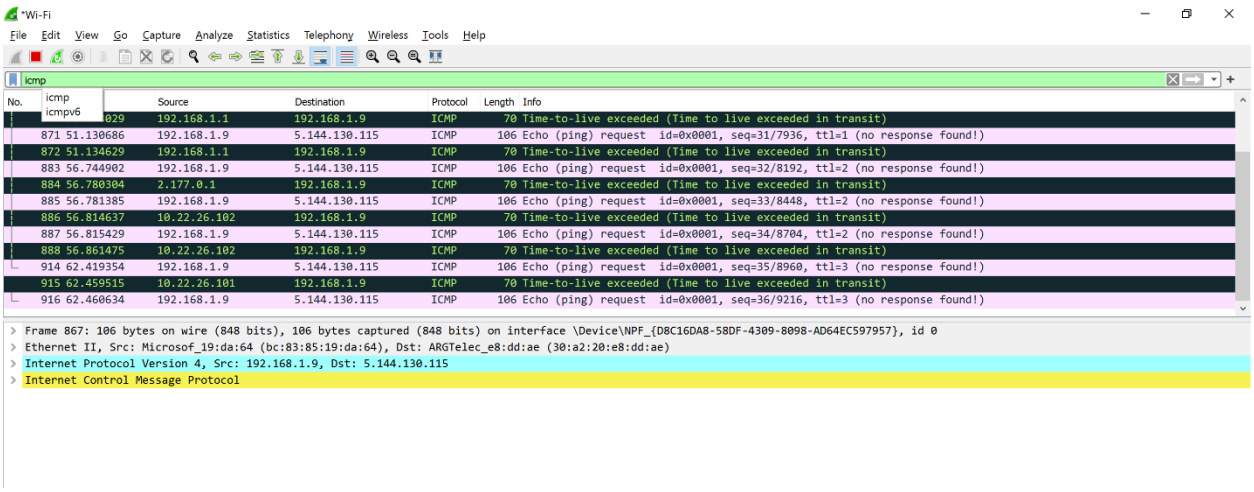
جواب سوال ۱۰ –

NS – CDS – AAAA – MX

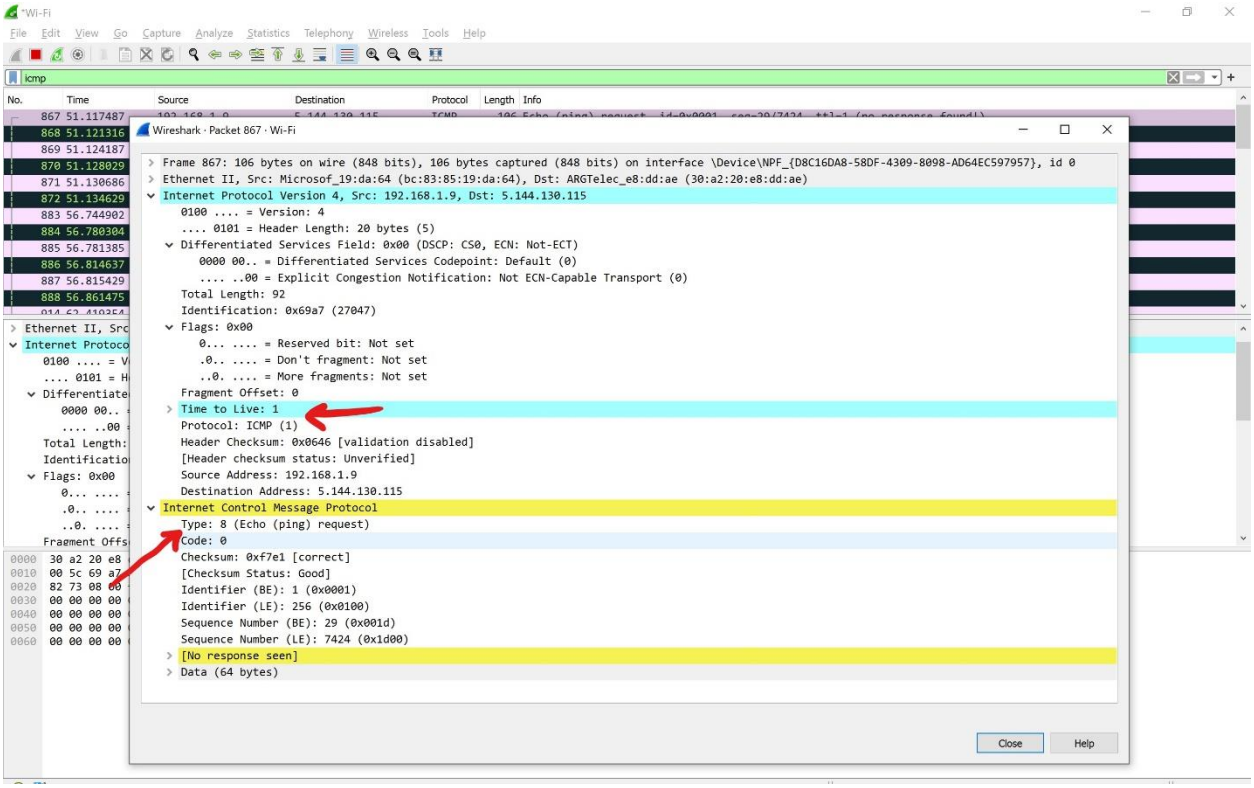
جواب سوال ۱۱ –

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

Protocol icmp مشاهده می‌شود.

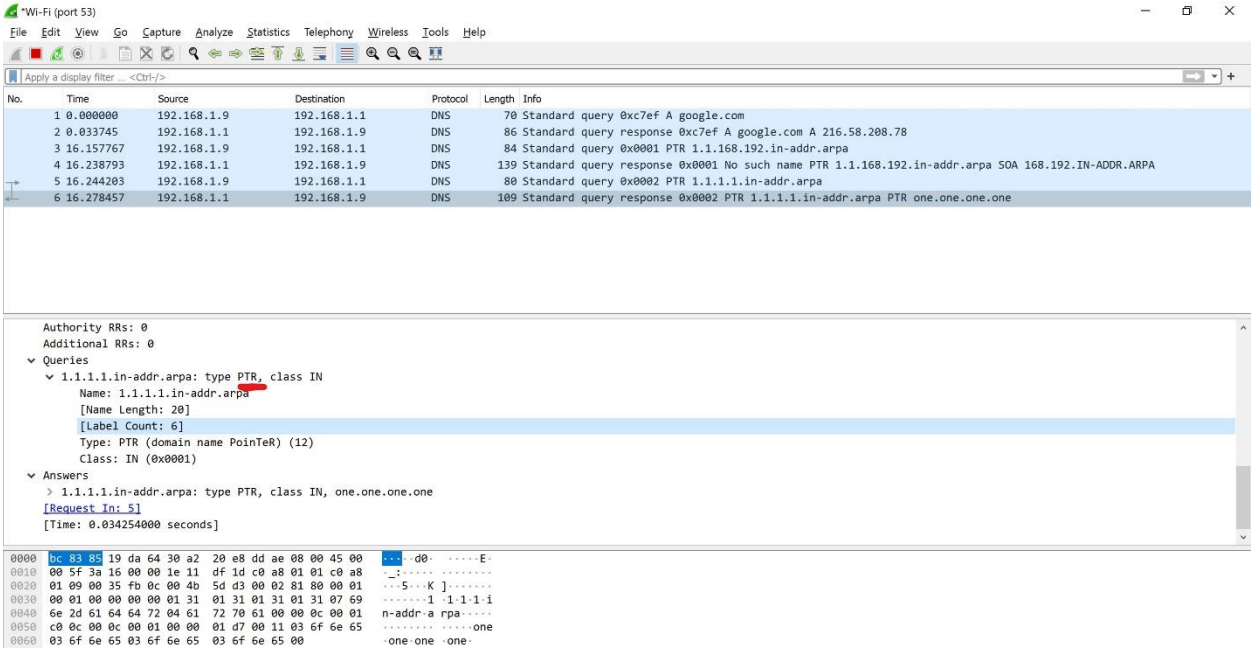


جواب سوال ۱۲ – مقدار type = 8 و TTL = 1 می‌باشد.



جواب سوال ۱۳ –

بیانگر تعداد گام‌ها تا زمانی که بسته از بین می‌رود می‌باشد و هرگامی که جلو می‌رود ۱ واحد کم می‌شود.ه 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 می کند.