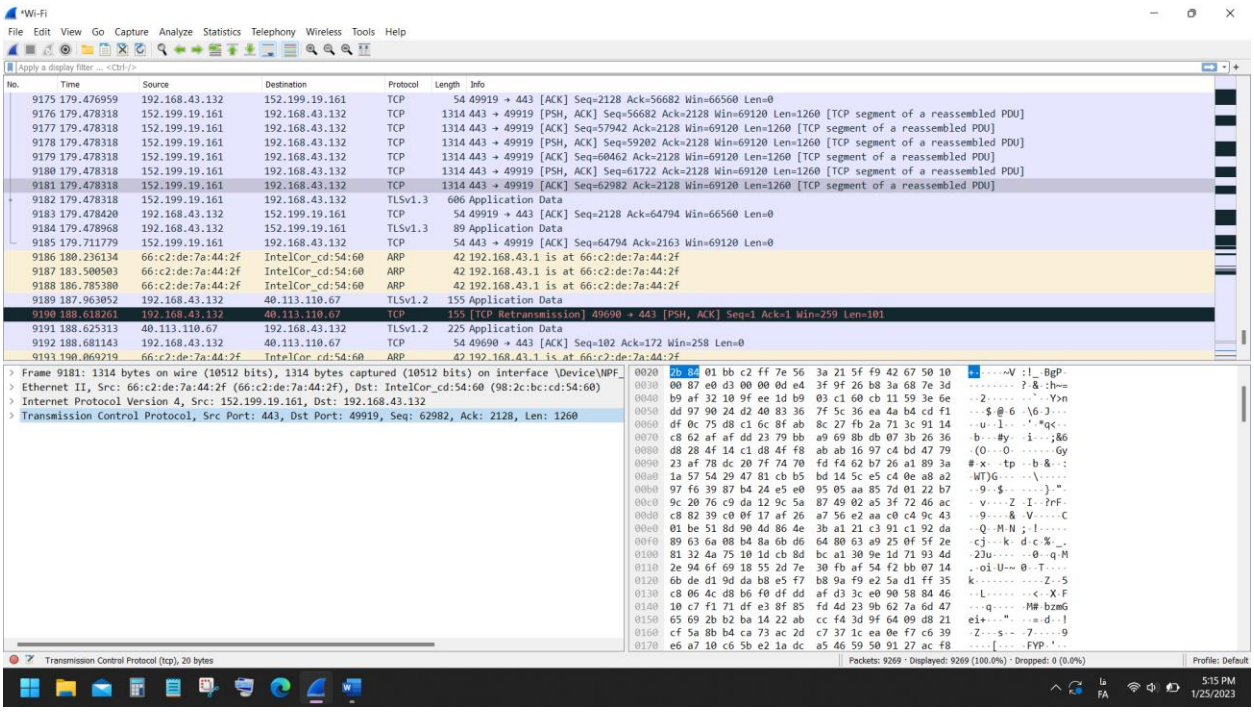
سوال 1)



پروتکل‌های TCP، ARP، TLSv1.3 و TLSv1.2 قابل مشاهده اند.

سوال 2) طبق عکس بالا پروتکل های لایه Transport، Network و Network Interface به ترتیب TCP، IPV4 و Ethernet II است. ترتیب قرارگیری بیت‌ها به ترتیب هدر هر لایه است. اندازه frame 1314 بایت است.

```
Internet Protocol Version 4, Src: 152.199.19.161, Dst: 192.168.43.132
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1300
    Identification: 0x9a0a (39434)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 47
    Protocol: TCP (6)
    Header Checksum: 0x5445 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 152.199.19.161
    Destination Address: 192.168.43.132
```

اندازه بسته لایه سوم با توجه به عکس بالا 1300 بایت است.

سوال 3) در بسته‌های من وجود نداشت چنین بسته‌ای ولی بسته‌های با پروتکل LOOP این ویژگی را دارند.

سوال 4)

```
Internet Protocol Version 4, Src: 152.199.19.161, Dst: 192.168.43.132
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1300
    Identification: 0x9a0a (39434)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 47
    Protocol: TCP (6)
    Header Checksum: 0x5445 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 152.199.19.161
    Destination Address: 192.168.43.132
```

طبق عکس مقدار 0x5445 است.

سوال 5)

```
Transmission Control Protocol, Src Port: 49904, Dst Port: 443, Seq: 9761, Ack: 41692, Len: 1260
    Source Port: 49904
    Destination Port: 443
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 1260]
    Sequence Number: 9761    (relative sequence number)
    Sequence Number (raw): 4012613760
    [Next Sequence Number: 11021    (relative sequence number)]
    Acknowledgment Number: 41692    (relative ack number)
    Acknowledgment number (raw): 2390460808
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
```

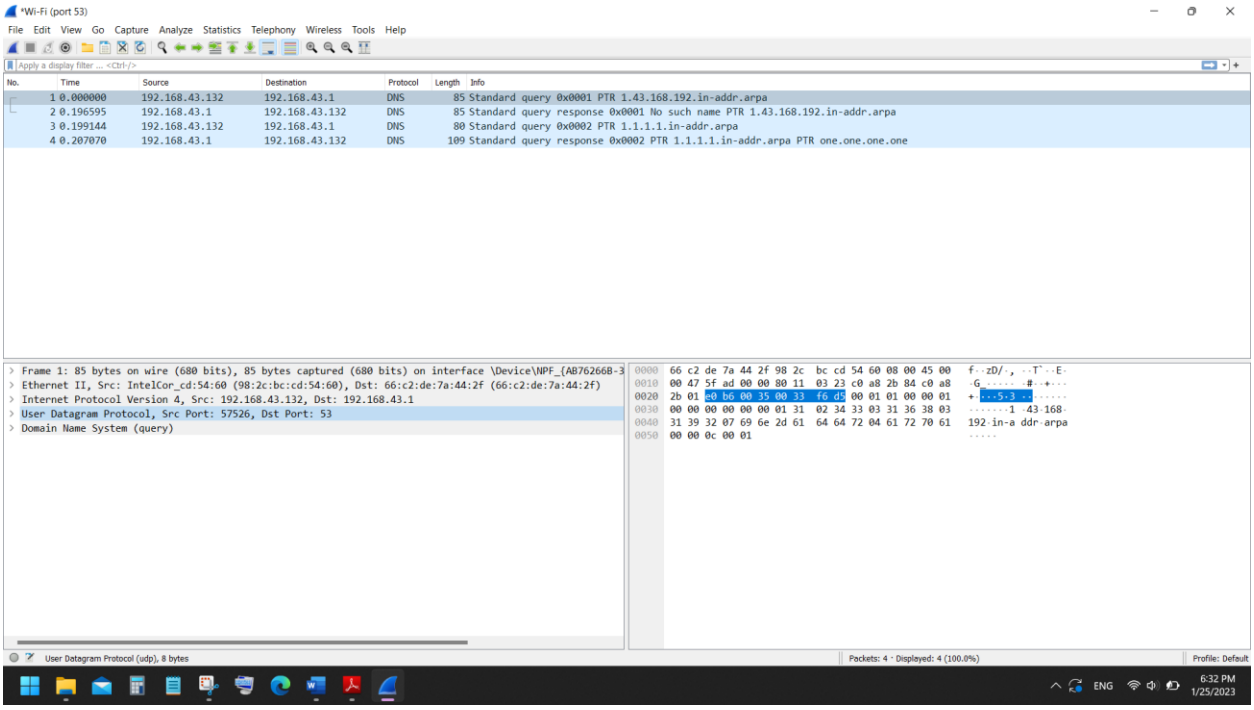
مقدار port مبدا 49904 و port مقصد 443 است. این اعداد آدرس port در مبدا و مقصد اند.

```
Transmission Control Protocol, Src Port: 49904, Dst Port: 443, Seq: 9761, Ack: 41692, Len: 1260
    Source Port: 49904
    Destination Port: 443
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 1260]
    Sequence Number: 9761    (relative sequence number)
    Sequence Number (raw): 4012613760
    [Next Sequence Number: 11021    (relative sequence number)]
    Acknowledgment Number: 41692    (relative ack number)
    Acknowledgment number (raw): 2390460808
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0x02e1 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

```
User Datagram Protocol, Src Port: 443, Dst Port: 57840
    Source Port: 443
    Destination Port: 57840
    Length: 37
    Checksum: 0xc157 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 22]
  > [Timestamps]
    UDP payload (29 bytes)
```

مقادیر checksum برای TCP و UDP بالا مشخص شده اند.

سوال 6)



پروتکلش UDP است. آدرس IP مقصد 192.168.43.1 است.

```
Ethernet II, Src: IntelCor_cd:54:60 (98:2c:bc:cd:54:60), Dst: 66:c2:de:7a:44:2f (66:c2:de:7a:44:2f)
  > Destination: 66:c2:de:7a:44:2f (66:c2:de:7a:44:2f)
  > Source: IntelCor_cd:54:60 (98:2c:bc:cd:54:60)
    Type: IPv4 (0x0800)
```

آدرس مبدا و مقصد بالا مشخص اند.

سوال 7)

```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 9A-2C-BC-CD-54-60
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

آدرس فیزیکی ماشین خودمان قابل مشاهده است.

سوال 8)

```
Domain Name System (query)
    Transaction ID: 0x5f7b
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v google.com: type A, class IN
        Name: google.com
        [Name Length: 10]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Type آن A است. این درخواست برای گرفتن آدرس IP دامنه google.com است.

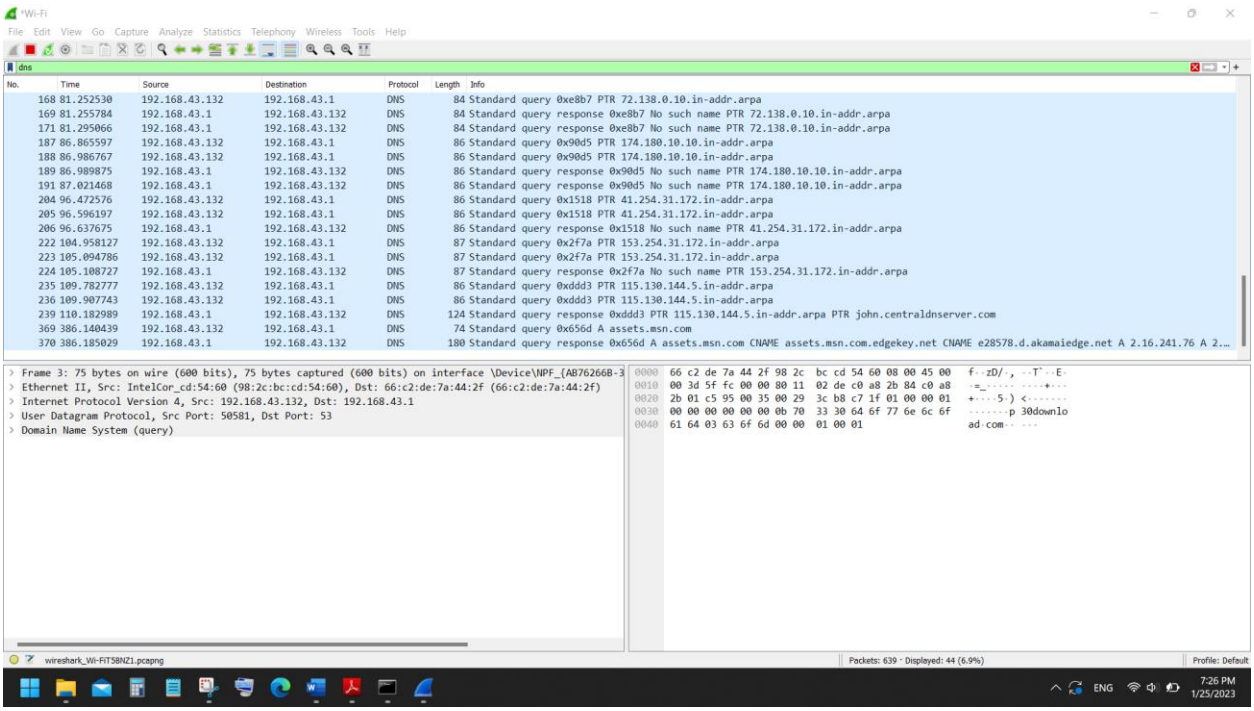
سوال 9)

```
Domain Name System (response)
    Transaction ID: 0x0001
  > Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 1.43.168.192.in-addr.arpa: type PTR, class IN
        Name: 1.43.168.192.in-addr.arpa
        [Name Length: 25]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
    [Request In: 8]
    [Time: 5.330835000 seconds]
```

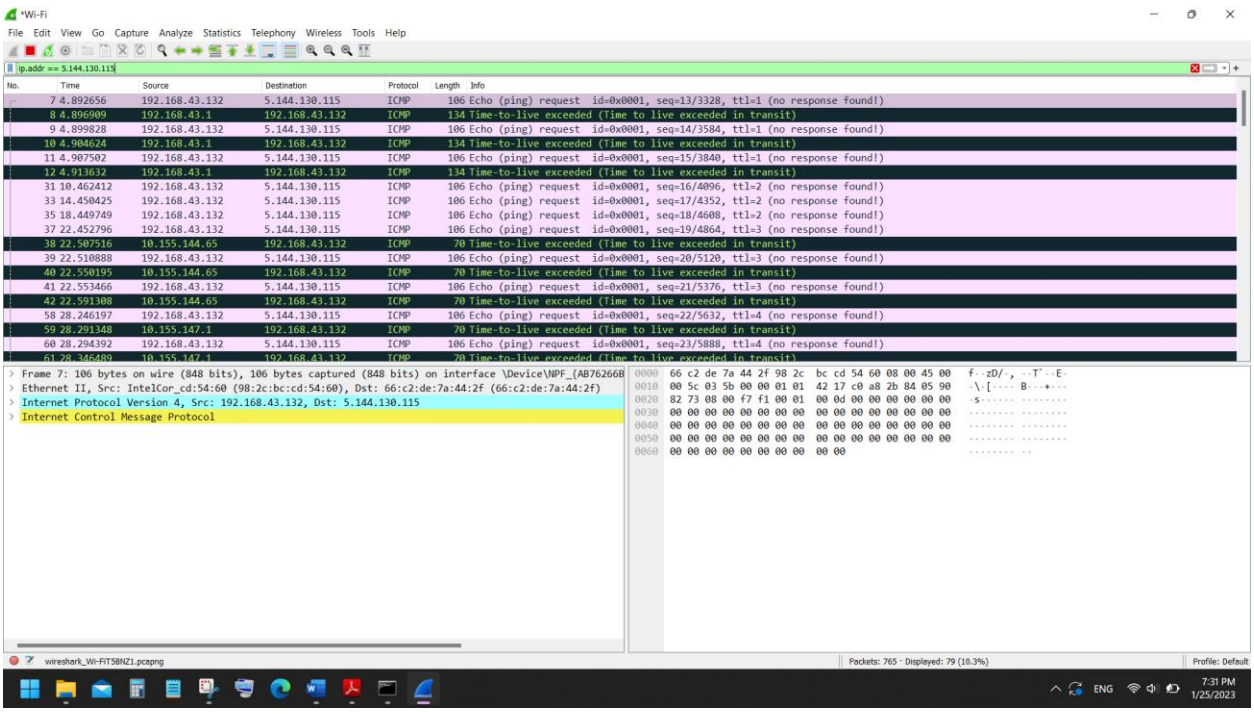
Type آن PTR است. این درخواست برای گرفتن FQDN است.

سوال 10) CNAME، AAAA و NS.

سوال 11)



```
C:\Users\Amir47>tracert p30download.com

Tracing route to p30download.com [5.144.130.115]
over a maximum of 30 hops:

  1     4 ms     4 ms     6 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    54 ms    39 ms    38 ms  10.155.144.65
  4    45 ms    52 ms    28 ms  10.155.147.1
  5    72 ms    41 ms    35 ms  10.0.250.70
  6    56 ms    33 ms    52 ms  10.0.136.14
  7    48 ms    36 ms    55 ms  10.185.68.38
  8    50 ms    64 ms    37 ms  10.185.68.17
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    49 ms    37 ms    42 ms  10.0.138.72
 12    51 ms    28 ms    36 ms  10.10.180.174
 13    48 ms    68 ms     *     172.31.254.41
 14    53 ms    47 ms     *     172.31.254.153
 15    59 ms    48 ms    46 ms  john.centraldnserver.com [5.144.130.115]

Trace complete.

C:\Users\Amir47>
```



بسته‌های شامل آدرس IP مشخص شده فیلتر می‌شوند که دارای پروتکل ICMP اند.

سوال 12)

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7f1 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 13 (0x000d)
    Sequence Number (LE): 3328 (0x0d00)
  > [No response seen]
  > Data (64 bytes)
```

```
Internet Protocol Version 4, Src: 192.168.43.132, Dst: 5.144.130.115
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x035b (859)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x4217 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.132
    Destination Address: 5.144.130.115
```

Type 8 و TTL 1 می‌باشد.

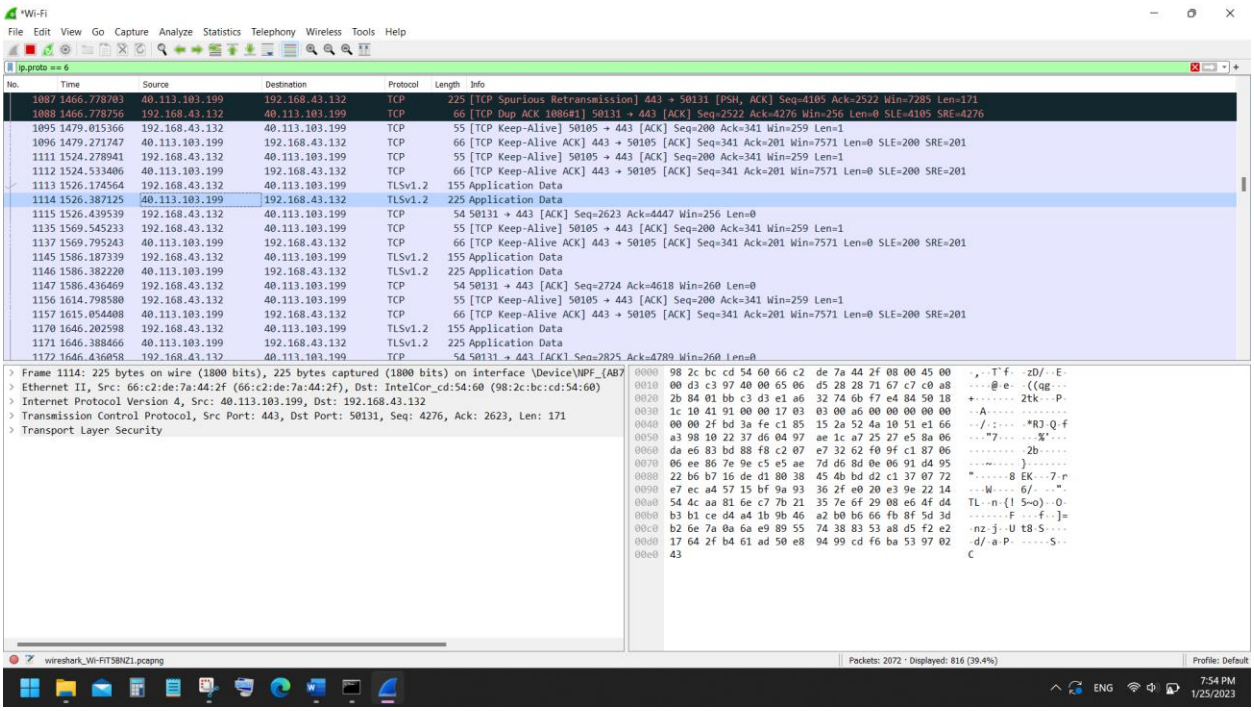
سوال 13)

```
> Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x4217 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.43.132
  Destination Address: 5.144.130.115

> Time to Live: 2
  Protocol: ICMP (1)
  Header Checksum: 0x4114 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.43.132
  Destination Address: 5.144.130.115
```

```
> Time to Live: 3
  Protocol: ICMP (1)
  Header Checksum: 0x4010 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.43.132
  Destination Address: 5.144.130.115

Time to Live: 49
Protocol: ICMP (1)
Header Checksum: 0x6bba [validation disabled]
[Header checksum status: Unverified]
Source Address: 5.144.130.115
Destination Address: 192.168.43.132
```

علت این امر این است که هر چه در طول گره‌ها جلو می‌رویم، به مقدار TTL بیشتری نیاز داریم.

سوال 14)



با این کار فقط بسته‌هایی که پروتکل لایه دوم آنها TCP است نمایش داده می‌شوند.