به نام خدا

گزارشکار آزمایش دوم (آشنایی با وایرشارک)

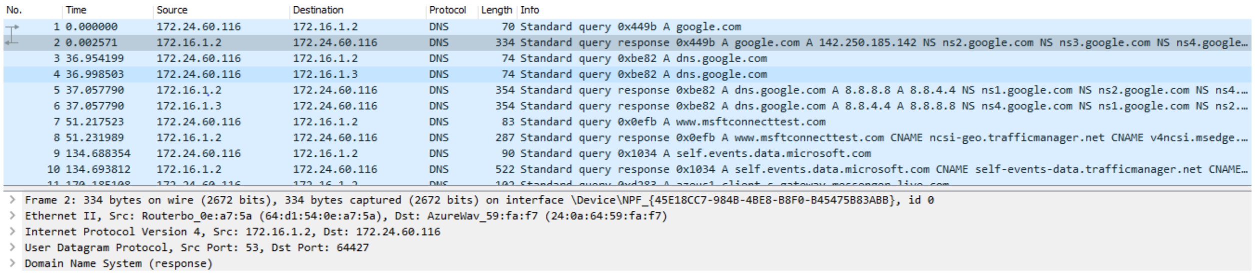
امیرحسین سرآهنگ

9831085

بخش اول ، لایه بندی پروتوکل ها :

سوال 1) ... TCP / UDP /DNS

سوال 2)



```
No.  Time        Source          Destination     Protocol Length Info
   1 0.000000    172.24.60.116   172.16.1.2      DNS        70 Standard query 0x449b A google.com
   2 0.002571    172.16.1.2      172.24.60.116   DNS       334 Standard query response 0x449b A google.com A 142.250.185.142 NS ns2.google.com NS ns3.google.com NS ns4.google…
   3 36.954199   172.24.60.116   172.16.1.2      DNS        74 Standard query 0xbe82 A dns.google.com
   4 36.998503   172.24.60.116   172.16.1.3      DNS        74 Standard query 0xbe82 A dns.google.com
   5 37.057790   172.16.1.2      172.24.60.116   DNS       354 Standard query response 0xbe82 A dns.google.com A 8.8.8.8 A 8.8.4.4 NS ns1.google.com NS ns2.google.com NS ns4.…
   6 37.057790   172.16.1.3      172.24.60.116   DNS       354 Standard query response 0xbe82 A dns.google.com A 8.8.4.4 A 8.8.8.8 NS ns4.google.com NS ns1.google.com NS ns2.…
   7 51.217523   172.24.60.116   172.16.1.2      DNS        83 Standard query 0x0efb A www.msftconnecttest.com
   8 51.231989   172.16.1.2      172.24.60.116   DNS       287 Standard query response 0x0efb A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME v4ncsi.msedge.…
   9 134.688354  172.24.60.116   172.16.1.2      DNS        90 Standard query 0x1034 A self.events.data.microsoft.com
  10 134.693812  172.16.1.2      172.24.60.116   DNS       522 Standard query response 0x1034 A self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net CNAME…

> Frame 2: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits) on interface \Device\NPF_{45E18CC7-984B-4BE8-B8F0-B45475B83ABB}, id 0
> Ethernet II, Src: Routerbo_0e:a7:5a (64:d1:54:0e:a7:5a), Dst: AzureWav_59:fa:f7 (24:0a:64:59:fa:f7)
> Internet Protocol Version 4, Src: 172.16.1.2, Dst: 172.24.60.116
> User Datagram Protocol, Src Port: 53, Dst Port: 64427
> Domain Name System (response)
```

DNS

IPv4

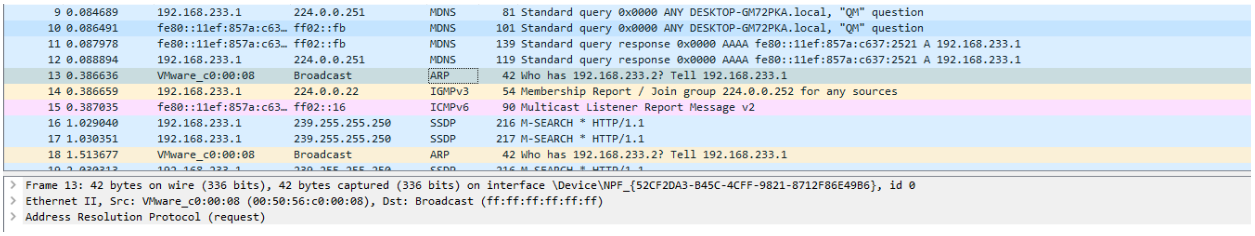
UDP

بیت های اول مربوط به لایه اول، بیت ها ی دوم مربوط به لایه ی دوم و دسته بیت های سوم برای لایه سوم می باشد ! به عبارت دیگر هدر لایه ها به payload های قبل اضافه می شوند .

Frame Length = 334 byte

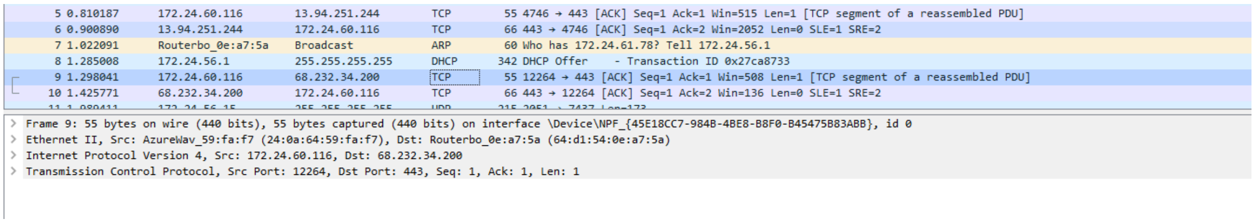
اندازه لایه 3 : 300 byte

سوال 3) اولین تصویر بسته ARP است و فاقد لایه Transport



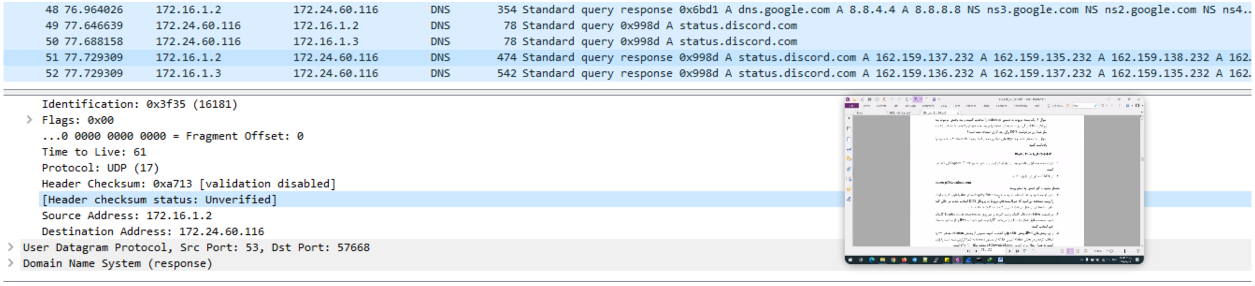
```
   9 0.084689    192.168.233.1        224.0.0.251      MDNS      81 Standard query 0x0000 ANY DESKTOP-GM72PKA.local, "QM" question
  10 0.086491    fe80::11ef:857a:c63… ff02::fb         MDNS     101 Standard query 0x0000 ANY DESKTOP-GM72PKA.local, "QM" question
  11 0.087978    fe80::11ef:857a:c63… ff02::fb         MDNS     139 Standard query response 0x0000 AAAA fe80::11ef:857a:c637:2521 A 192.168.233.1
  12 0.088894    192.168.233.1        224.0.0.251      MDNS     119 Standard query response 0x0000 AAAA fe80::11ef:857a:c637:2521 A 192.168.233.1
  13 0.386636    VMware_c0:00:08      Broadcast        ARP       42 Who has 192.168.233.2? Tell 192.168.233.1
  14 0.386659    192.168.233.1        224.0.0.22       IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
  15 0.387035    fe80::11ef:857a:c63… ff02::16         ICMPv6    90 Multicast Listener Report Message v2
  16 1.029040    192.168.233.1        239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
  17 1.030351    192.168.233.1        239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  18 1.513677    VMware_c0:00:08      Broadcast        ARP       42 Who has 192.168.233.2? Tell 192.168.233.1

> Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{52CF2DA3-B45C-4CFF-9821-8712F86E49B6}, id 0
> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

تصویر زیر، بسته TCP است و فاقد لایه Application



```
    5 0.810187     172.24.60.116      13.94.251.244      TCP      55 4746 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
    6 0.900890     13.94.251.244      172.24.60.116      TCP      66 443 → 4746 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2
    7 1.022091     Routerbo_0e:a7:5a  Broadcast          ARP      60 Who has 172.24.61.78? Tell 172.24.56.1
    8 1.285008     172.24.56.1        255.255.255.255    DHCP    342 DHCP Offer    - Transaction ID 0x27ca8733
    9 1.298041     172.24.60.116      68.232.34.200      TCP      55 12264 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]
   10 1.425771     68.232.34.200      172.24.60.116      TCP      66 443 → 12264 [ACK] Seq=1 Ack=2 Win=136 Len=0 SLE=1 SRE=2
   11 1.080411     172.24.56.15       255.255.255.255    UDP     215 2051 → 7437 Len=173

> Frame 9: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{45E18CC7-984B-4BE8-B8F0-B45475B83ABB}, id 0
> Ethernet II, Src: AzureWav_59:fa:f7 (24:0a:64:59:fa:f7), Dst: Routerbo_0e:a7:5a (64:d1:54:0e:a7:5a)
> Internet Protocol Version 4, Src: 172.24.60.116, Dst: 68.232.34.200
> Transmission Control Protocol, Src Port: 12264, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

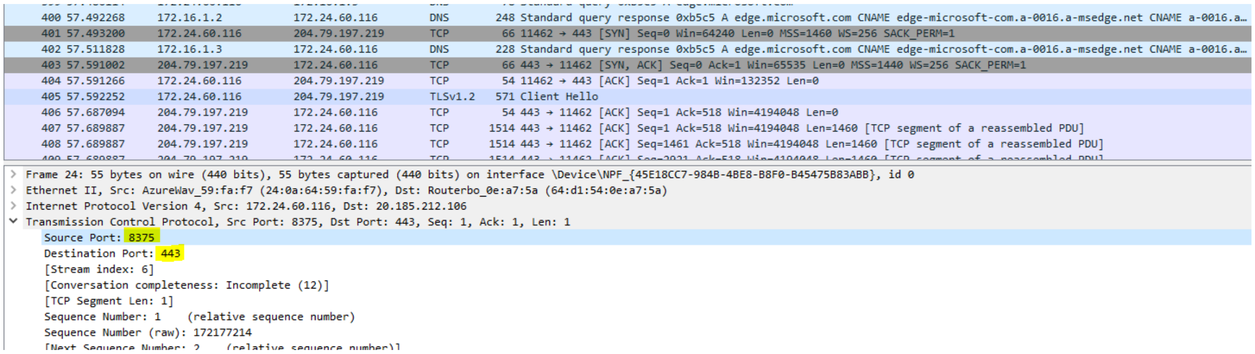
سوال 4)



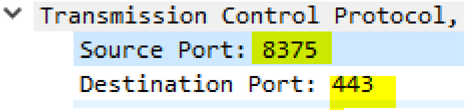
```
   48 76.964026    172.16.1.2         172.24.60.116      DNS     354 Standard query response 0x6bd1 A dns.google.com A 8.8.4.4 A 8.8.8.8 NS ns3.google.com NS ns2.google.com NS ns4..
   49 77.646639    172.24.60.116      172.16.1.2         DNS      78 Standard query 0x998d A status.discord.com
   50 77.688158    172.24.60.116      172.16.1.3         DNS      78 Standard query 0x998d A status.discord.com
   51 77.729309    172.16.1.2         172.24.60.116      DNS     474 Standard query response 0x998d A status.discord.com A 162.159.137.232 A 162.159.135.232 A 162.159.138.232 A 162.
   52 77.729309    172.16.1.3         172.24.60.116      DNS     542 Standard query response 0x998d A status.discord.com A 162.159.136.232 A 162.159.137.232 A 162.159.135.232 A 162.

    Identification: 0x3f35 (16181)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 61
    Protocol: UDP (17)
    Header Checksum: 0xa713 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.1.2
    Destination Address: 172.24.60.116
> User Datagram Protocol, Src Port: 53, Dst Port: 57668
> Domain Name System (response)
```

سوال 5)

TCP :



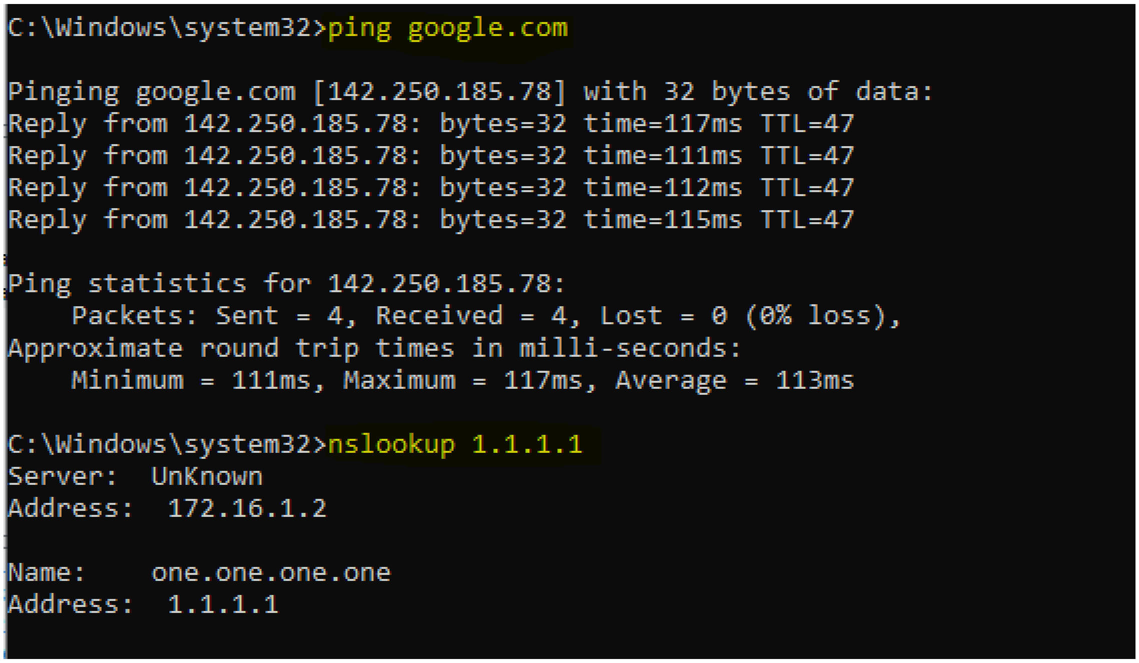
```
  400 57.492268    172.16.1.2         172.24.60.116      DNS     248 Standard query response 0xb5c5 A edge.microsoft.com CNAME edge-microsoft-com.a-0016.a-msedge.net CNAME a-0016.a…
  401 57.493200    172.24.60.116      204.79.197.219     TCP      66 11462 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  402 57.511828    172.16.1.3         172.24.60.116      DNS     228 Standard query response 0xb5c5 A edge.microsoft.com CNAME edge-microsoft-com.a-0016.a-msedge.net CNAME a-0016.a…
  403 57.591002    204.79.197.219     172.24.60.116      TCP      66 443 → 11462 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
  404 57.591266    172.24.60.116      204.79.197.219     TCP      54 11462 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  405 57.592252    172.24.60.116      204.79.197.219     TLSv1.2 571 Client Hello
  406 57.687094    204.79.197.219     172.24.60.116      TCP      54 443 → 11462 [ACK] Seq=1 Ack=518 Win=4194048 Len=0
  407 57.689887    204.79.197.219     172.24.60.116      TCP    1514 443 → 11462 [ACK] Seq=1 Ack=518 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
  408 57.689887    204.79.197.219     172.24.60.116      TCP    1514 443 → 11462 [ACK] Seq=1461 Ack=518 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
  409 57.689887    204.79.197.219     172.24.60.116      TCP    1514 443 → 11462 [ACK] Seq=2921 Ack=518 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]

> Frame 24: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{45E18CC7-984B-4BE8-B8F0-B45475B83ABB}, id 0
> Ethernet II, Src: AzureWav_59:fa:f7 (24:0a:64:59:fa:f7), Dst: Routerbo_0e:a7:5a (64:d1:54:0e:a7:5a)
> Internet Protocol Version 4, Src: 172.24.60.116, Dst: 20.185.212.106
v Transmission Control Protocol, Src Port: 8375, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
    Source Port: 8375
    Destination Port: 443
    [Stream index: 6]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 1]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 172177214
    [Next Sequence Number: 2    (relative sequence number)]
```



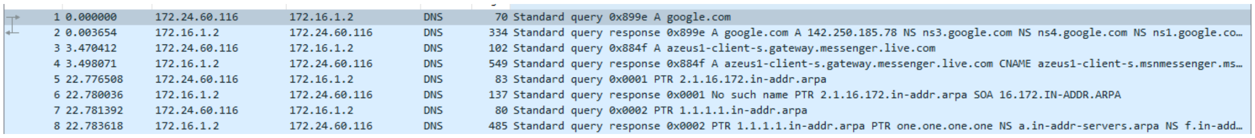
```
v Transmission Control Protocol,
    Source Port: 8375
    Destination Port: 443
```

بخش دوم ،کار با فیلتر کننده بسته ها :

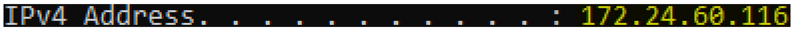
سوال 6)



```
C:\Windows\system32>ping google.com

Pinging google.com [142.250.185.78] with 32 bytes of data:
Reply from 142.250.185.78: bytes=32 time=117ms TTL=47
Reply from 142.250.185.78: bytes=32 time=111ms TTL=47
Reply from 142.250.185.78: bytes=32 time=112ms TTL=47
Reply from 142.250.185.78: bytes=32 time=115ms TTL=47

Ping statistics for 142.250.185.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 111ms, Maximum = 117ms, Average = 113ms

C:\Windows\system32>nslookup 1.1.1.1
Server:  UnKnown
Address:  172.16.1.2

Name:    one.one.one.one
Address:  1.1.1.1
```



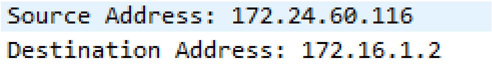
```
1 0.000000   172.24.60.116  172.16.1.2     DNS   70 Standard query 0x899e A google.com
2 0.003654   172.16.1.2     172.24.60.116  DNS  334 Standard query response 0x899e A google.com A 142.250.185.78 NS ns3.google.com NS ns4.google.com NS ns1.google.co…
3 3.470412   172.24.60.116  172.16.1.2     DNS  102 Standard query 0x884f A azeus1-client-s.gateway.messenger.live.com
4 3.498071   172.16.1.2     172.24.60.116  DNS  549 Standard query response 0x884f A azeus1-client-s.gateway.messenger.live.com CNAME azeus1-client-s.msnmessenger.ms…
5 22.776508  172.24.60.116  172.16.1.2     DNS   83 Standard query 0x0001 PTR 2.1.16.172.in-addr.arpa
6 22.780036  172.16.1.2     172.24.60.116  DNS  137 Standard query response 0x0001 No such name PTR 2.1.16.172.in-addr.arpa SOA 16.172.IN-ADDR.ARPA
7 22.781392  172.24.60.116  172.16.1.2     DNS   80 Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
8 22.783618  172.16.1.2     172.24.60.116  DNS  485 Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one NS a.in-addr-servers.arpa NS f.in-add…
```

آی پی سیستم ما : 

```
IPv4 Address. . . . . . . . . . . : 172.24.60.116
```

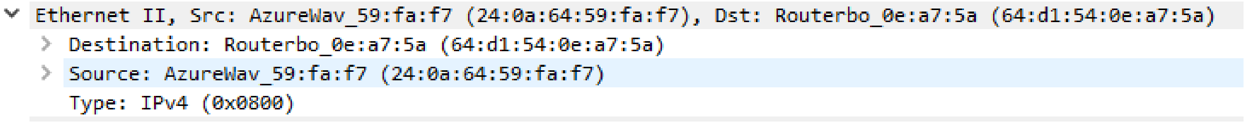
ip مبدا : 172.24.60.116 سیستم خودمون!

Ip مقصد : 172.16.1.2



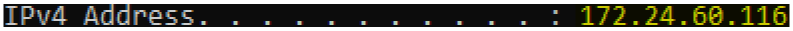
```
Source Address: 172.24.60.116
Destination Address: 172.16.1.2
```

آدرس مبدا و مقصد در سرآیند لایه دوم :

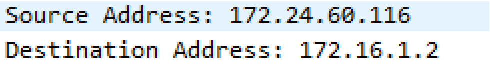


```
Ethernet II, Src: AzureWav_59:fa:f7 (24:0a:64:59:fa:f7), Dst: Routerbo_0e:a7:5a (64:d1:54:0e:a7:5a)
  > Destination: Routerbo_0e:a7:5a (64:d1:54:0e:a7:5a)
  > Source: AzureWav_59:fa:f7 (24:0a:64:59:fa:f7)
    Type: IPv4 (0x0800)
```

سوال 7) آدرس سیستم خودمون :



```
IPv4 Address. . . . . . . . . . . : 172.24.60.116
```



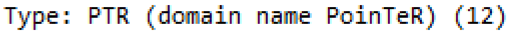
```
Source Address: 172.24.60.116
Destination Address: 172.16.1.2
```

سوال 8)

تایپ A است که از آن برا ی گرفتن آدرس IPV4 مقصد که 32 بیتی است استفاده می شود .

سوال 9)

تایپ PTR است



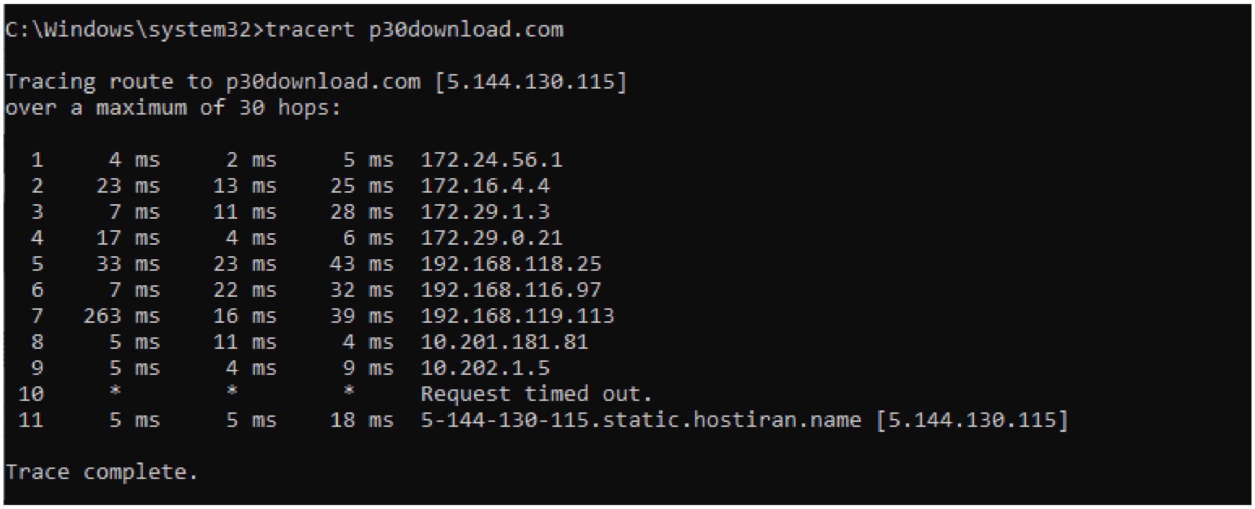
```
Type: PTR (domain name PoinTeR) (12)
```

این تایپ اشارع گری به name canonical می باشد.

سوال 10)

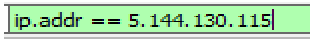
LOC / RP / HINFO

سوال 11)

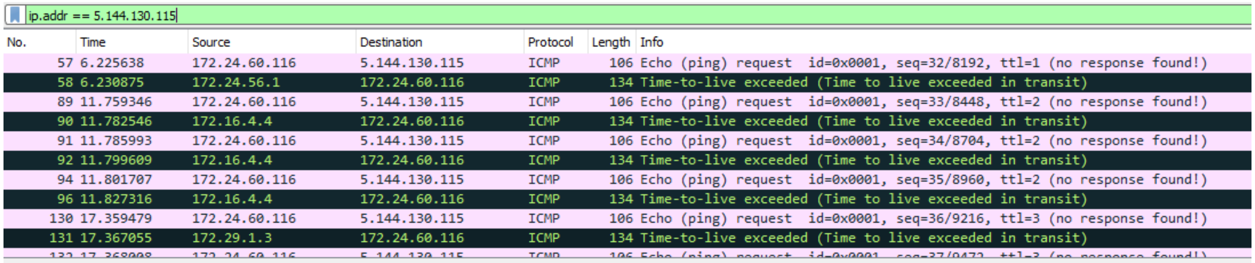


```
C:\Windows\system32>tracert p30download.com

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

  1     4 ms     2 ms     5 ms  172.24.56.1
  2    23 ms    13 ms    25 ms  172.16.4.4
  3     7 ms    11 ms    28 ms  172.29.1.3
  4    17 ms     4 ms     6 ms  172.29.0.21
  5    33 ms    23 ms    43 ms  192.168.118.25
  6     7 ms    22 ms    32 ms  192.168.116.97
  7   263 ms    16 ms    39 ms  192.168.119.113
  8     5 ms    11 ms     4 ms  10.201.181.81
  9     5 ms     4 ms     9 ms  10.202.1.5
 10     *        *        *     Request timed out.
 11     5 ms     5 ms    18 ms  5-144-130-115.static.hostiran.name [5.144.130.115]

Trace complete.
```

بسته ها با فیلتری که در filter مشخص کردیم نمایش داده میشوند



```
ip.addr == 5.144.130.115
```

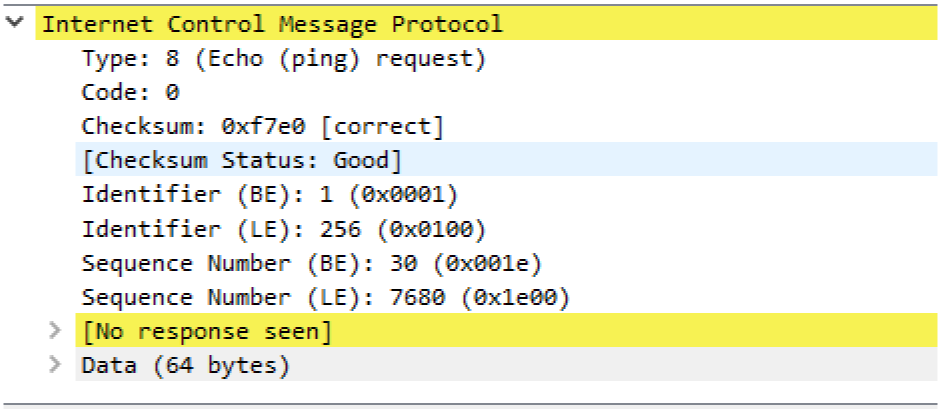


```
ip.addr == 5.144.130.115
No.   Time       Source         Destination    Protocol Length Info
 57 6.225638     172.24.60.116  5.144.130.115  ICMP     106 Echo (ping) request  id=0x0001, seq=32/8192, ttl=1 (no response found!)
 58 6.230875     172.24.56.1    172.24.60.116  ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 89 11.759346    172.24.60.116  5.144.130.115  ICMP     106 Echo (ping) request  id=0x0001, seq=33/8448, ttl=2 (no response found!)
 90 11.782546    172.16.4.4     172.24.60.116  ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 91 11.785993    172.24.60.116  5.144.130.115  ICMP     106 Echo (ping) request  id=0x0001, seq=34/8704, ttl=2 (no response found!)
 92 11.799609    172.16.4.4     172.24.60.116  ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 94 11.801707    172.24.60.116  5.144.130.115  ICMP     106 Echo (ping) request  id=0x0001, seq=35/8960, ttl=2 (no response found!)
 96 11.827316    172.16.4.4     172.24.60.116  ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
130 17.359479    172.24.60.116  5.144.130.115  ICMP     106 Echo (ping) request  id=0x0001, seq=36/9216, ttl=3 (no response found!)
131 17.367055    172.29.1.3     172.24.60.116  ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
132 17.368008    172.24.60.116  5.144.130.115  ICMP     106 Echo (ping) request  id=0x0001, seq=37/9472, ttl=3 (no response found!)
```

و از پروتکل ICMP بهره میبرند !

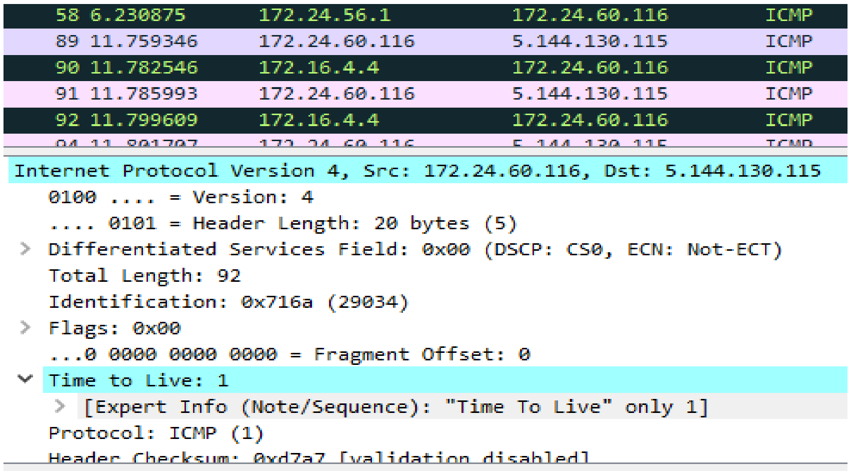
سوال 12)

بخش Internet Control Message :



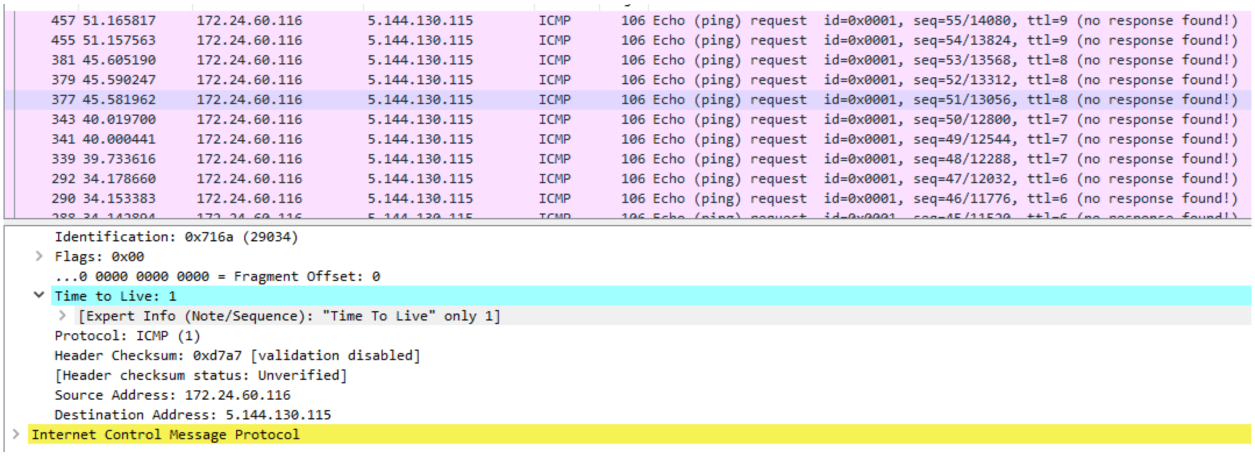
```
∨ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7e0 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 30 (0x001e)
    Sequence Number (LE): 7680 (0x1e00)
  > [No response seen]
  > Data (64 bytes)
```

بخش ip :



```
 58 6.230875    172.24.56.1     172.24.60.116   ICMP
 89 11.759346   172.24.60.116   5.144.130.115   ICMP
 90 11.782546   172.16.4.4      172.24.60.116   ICMP
 91 11.785993   172.24.60.116   5.144.130.115   ICMP
 92 11.799609   172.16.4.4      172.24.60.116   ICMP
 94 11.801707   172.24.60.116   5.144.130.115   ICMP

Internet Protocol Version 4, Src: 172.24.60.116, 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: 0x716a (29034)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  ∨ Time to Live: 1
      > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header Checksum: 0xd7a7 [validation disabled]
```

بسته هارا به صورت source مرتب می کنیم :



```
    457 51.165817    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=55/14080, ttl=9 (no response found!)
    455 51.157563    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=54/13824, ttl=9 (no response found!)
    381 45.605190    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=53/13568, ttl=8 (no response found!)
    379 45.590247    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=52/13312, ttl=8 (no response found!)
    377 45.581962    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=51/13056, ttl=8 (no response found!)
    343 40.019700    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=50/12800, ttl=7 (no response found!)
    341 40.000441    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=49/12544, ttl=7 (no response found!)
    339 39.733616    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=48/12288, ttl=7 (no response found!)
    292 34.178660    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=47/12032, ttl=6 (no response found!)
    290 34.153383    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=46/11776, ttl=6 (no response found!)
    288 34.142804    172.24.60.116    5.144.130.115    ICMP    106 Echo (ping) request  id=0x0001, seq=45/11520, ttl=6 (no response found!)

    Identification: 0x716a (29034)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  v Time to Live: 1
     > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header Checksum: 0xd7a7 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.24.60.116
    Destination Address: 5.144.130.115
> Internet Control Message Protocol
```

سوال 13)

مقدار TTL از 10 تا 1 هست یعنی همان 10 گام tracert ! که در هر گام 3 بسته داریم و در هر گامی که بسته طی می کند یکی از TTL آن کاسته می شود و زمانی کع به صفر برسد باید مجدد ارسال بشه !

سوال 14)

بسته ها بر اساس پروتکل IPv6 انتخاب می شوند