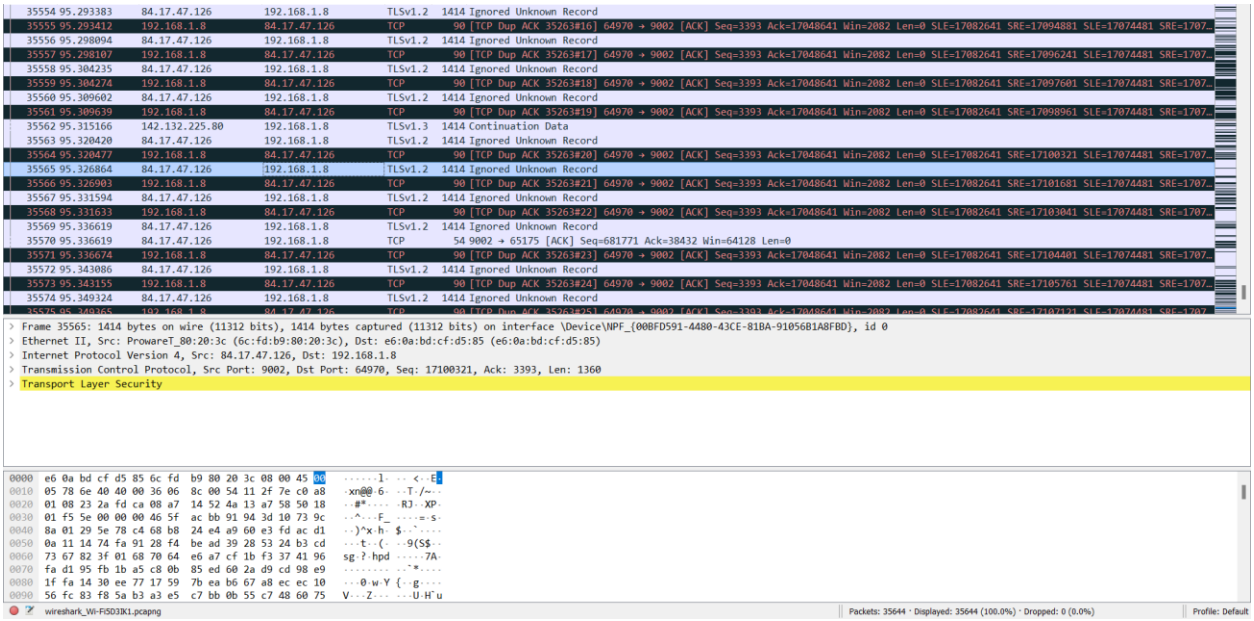
گزارش کار دوم آزمایشگاه شبکه

سوال اول)

سایت های جست و جو شده: YouTube، Reddit، Twitter، GitHub، Gmail

لیست پروتکل های مشاهده شده:

TCP, TLSv1.2, TLSv1.3, HTTP, TLS, HTTPS, DNS

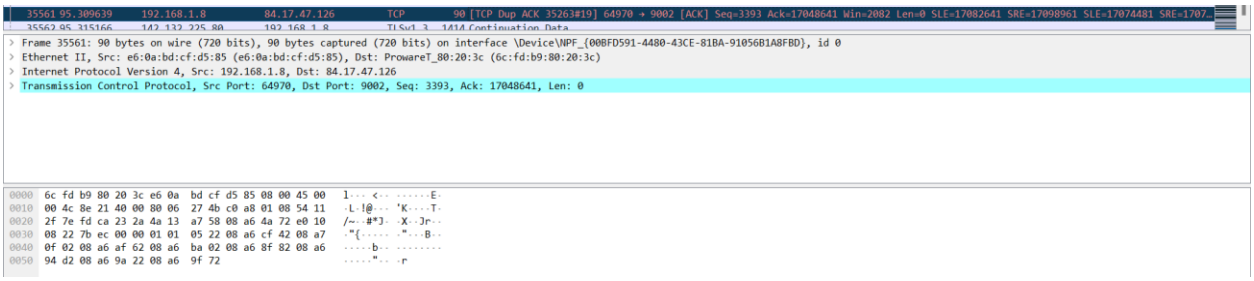


سوال دوم)

در package انتخابی، دو پروتکل استفاده شده: Internet Protocol Version 4 و Transmission Control Protocol.

لایه Transmission Control Protocol بعد از Internet Protocol Version 4 و آن هم بعد از Ethernet II و آن هم بعد از Frame آمده است. به عبارتی ترتیب قرارگیری به خارجی ترین است.

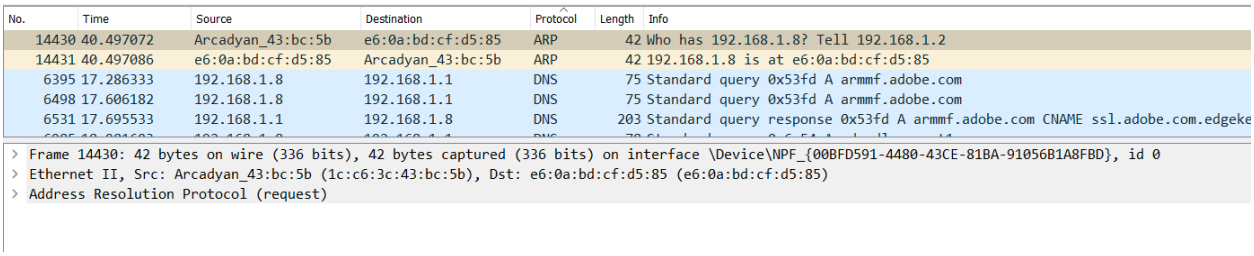
اندازه Frame لایه دو این بسته برابر ۹۰ بایت است. جزئیات این package را مشاهده میکنید:



گزارش کار دوم آزمایشگاه شبکه

سوال سوم)

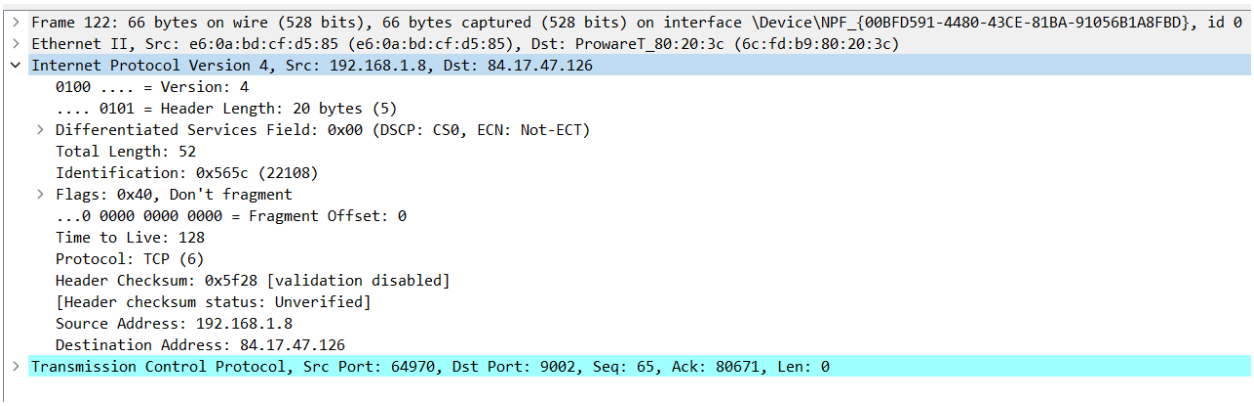
بله. همانطور که در عکس پایین مشاهده میشود Package های ARP دارای لایه های Network، Application و Transport نیستند. پروتکل استفاده شده در این package ها برای Data Link هستند:



سوال چهارم)

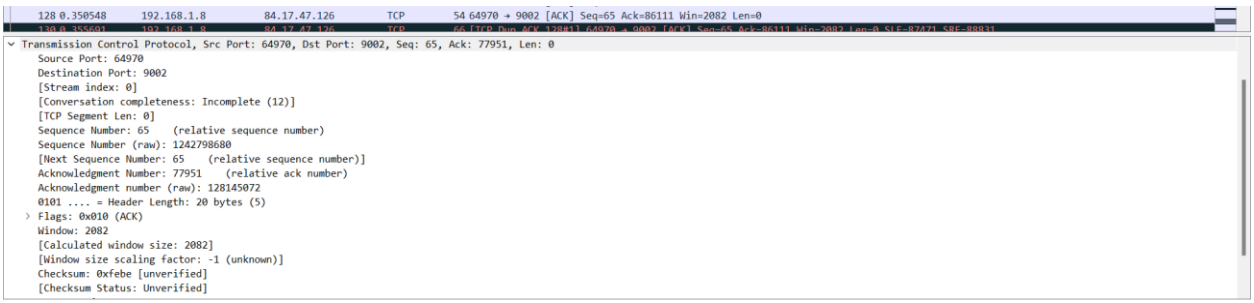
در برنامه Wireshark یک package انتخاب شده و سپس مشخصات لایه Internet Protocol Version 4 باز شد.

همانطور که مشاهده میشود Header Checksum برابر 0x5f28 است. در شکل زیر درستی این حرف اثبات میشود:



سوال پنجم)

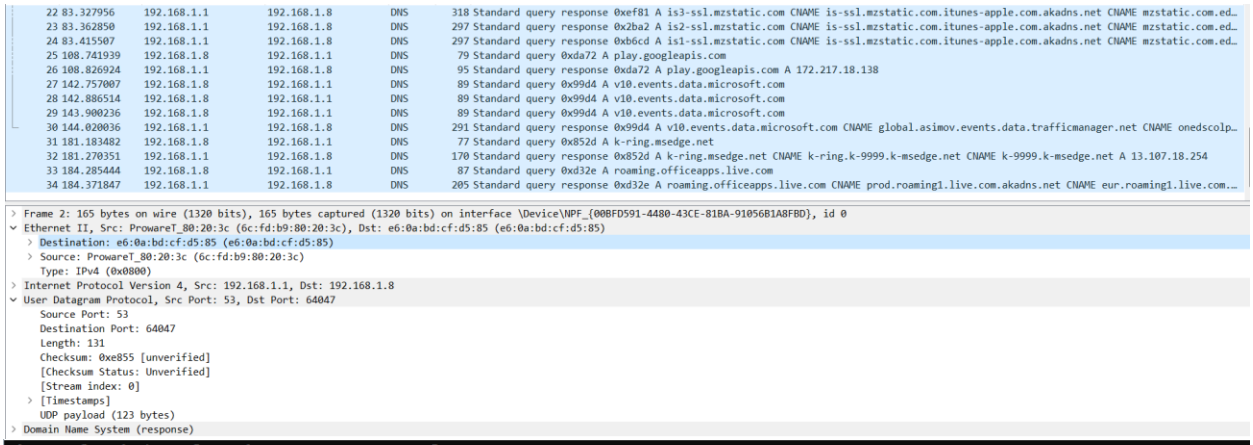
پورت ها برای انتقال دیتا حیاتی هستند. دو پورت Source برابر 64970 و Destination برابر 9002 است. بین این پورت ها میتوان دیتا فرستاد یا دریافت کرد. Checksum پروتکل TCP برابر 0xfebe و پروتکل UDP برابر 0x35c5 است.



گزارش کار دوم آزمایشگاه شبکه

سوال ششم)

پروتکل لایه Transport برابر UDP بوده و پورت مقصد برابر 192.168.1.8 است. لایه دوم Ethernet II است که آدرس مبدا c:fd:b9:80:20:3c۶ و آدرس مقصد e6:0a:bd:cf:d5:85 است.



```
22 83.327956    192.168.1.1     192.168.1.8     DNS     318 Standard query response 0xef81 A is3-ssl.mzstatic.com CNAME is-ssl.mzstatic.com.itunes-apple.com.akadns.net CNAME mzstatic.com.ed…
23 83.362850    192.168.1.1     192.168.1.8     DNS     297 Standard query response 0x2ba2 A is2-ssl.mzstatic.com CNAME is-ssl.mzstatic.com.itunes-apple.com.akadns.net CNAME mzstatic.com.ed…
24 83.415507    192.168.1.1     192.168.1.8     DNS     297 Standard query response 0xb6cd A is1-ssl.mzstatic.com CNAME is-ssl.mzstatic.com.itunes-apple.com.akadns.net CNAME mzstatic.com.ed…
25 108.741939   192.168.1.8     192.168.1.1     DNS      79 Standard query 0xda72 A play.googleapis.com
26 108.826924   192.168.1.1     192.168.1.8     DNS      95 Standard query response 0xda72 A play.googleapis.com A 172.217.18.138
27 142.757007   192.168.1.8     192.168.1.1     DNS      89 Standard query 0x99d4 A v10.events.data.microsoft.com
28 142.886514   192.168.1.8     192.168.1.1     DNS      89 Standard query 0x99d4 A v10.events.data.microsoft.com
29 143.900236   192.168.1.8     192.168.1.1     DNS      89 Standard query 0x99d4 A v10.events.data.microsoft.com
30 144.020036   192.168.1.1     192.168.1.8     DNS     291 Standard query response 0x99d4 A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedscolp…
31 181.183482   192.168.1.8     192.168.1.1     DNS      77 Standard query 0x852d A k-ring.msedge.net
32 181.270351   192.168.1.1     192.168.1.8     DNS     170 Standard query response 0x852d A k-ring.msedge.net CNAME k-ring.k-9999.k-msedge.net CNAME k-9999.k-msedge.net A 13.107.18.254
33 184.285444   192.168.1.8     192.168.1.1     DNS      87 Standard query 0xd32e A roaming.officeapps.live.com
34 184.371847   192.168.1.1     192.168.1.8     DNS     205 Standard query response 0xd32e A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net CNAME eur.roaming1.live.com…

> Frame 2: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-91056B1A8FBD}, id 0
v Ethernet II, Src: ProwareT_80:20:3c (6c:fd:b9:80:20:3c), Dst: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85)
  > Destination: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85)
  > Source: ProwareT_80:20:3c (6c:fd:b9:80:20:3c)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.8
v User Datagram Protocol, Src Port: 53, Dst Port: 64047
    Source Port: 53
    Destination Port: 64047
    Length: 131
    Checksum: 0xe855 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (123 bytes)
> Domain Name System (response)
```

```
Microsoft Windows [Version 10.0.22000.556]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Keivan>ping google.com

Pinging google.com [142.250.180.46] with 32 bytes of data:
Reply from 142.250.180.46: bytes=32 time=122ms TTL=111
Reply from 142.250.180.46: bytes=32 time=118ms TTL=111
Reply from 142.250.180.46: bytes=32 time=117ms TTL=111
Reply from 142.250.180.46: bytes=32 time=118ms TTL=111

Ping statistics for 142.250.180.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 117ms, Maximum = 122ms, Average = 118ms

C:\Users\Keivan>nslookup 1.1.1.1
Server:  UnKnown
Address:  192.168.1.1

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

سوال هفتم)

از آن جایی که interface انتخابی WIFI بوده، آدرس آن را در ipconfig/all مشاهده میکنیم.

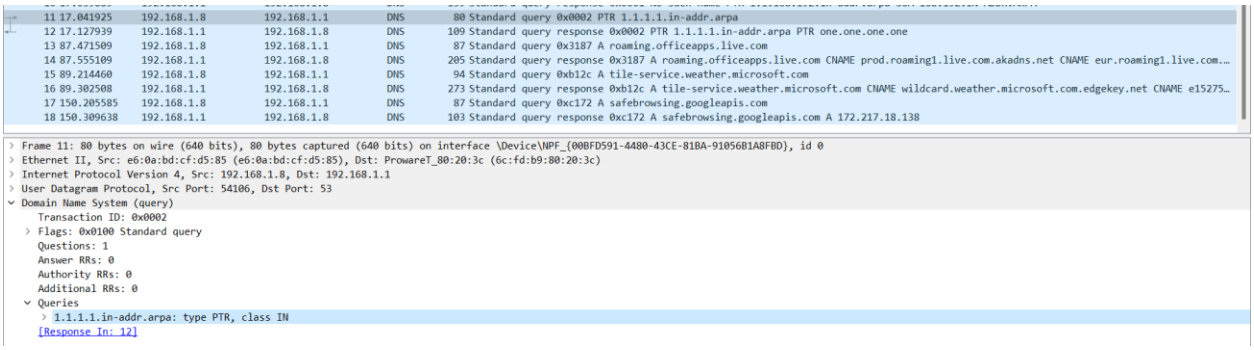
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : domain.name
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : E6-0A-BD-CF-D5-85
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::641c:74d1:67d:33c9%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, April 11, 2022 11:20:15 PM
   Lease Expires . . . . . . . . . . : Wednesday, April 13, 2022 7:26:02 AM
   Default Gateway . . . . . . . . . : fe80::6efd:b9ff:fe80:203c%2
```

همانطور که مشاهده میشود Physical Address چاپ شده با سوال ششم همخوانی دارد.

گزارش کار دوم آزمایشگاه شبکه

سوال هشتم)

در لایه Query و بخش Query تایپ PTR انتخاب شده. این تایپ برای تبدیل یک IP Address به Host Name استفاده میشود. (برعکس این تایپ یعنی تایپ A، عکس این عملیات را انجام میدهد.)



در عکس، سطر تایپ انتخاب شده.

سوال نهم)

برای دستور nslookup تایپ A استفاده شده است. این تایپ برای تبدیل یک Host Name به IP Address استفاده میشود. (برعکس لایه سوال قبل، PTR)

سوال دهم)

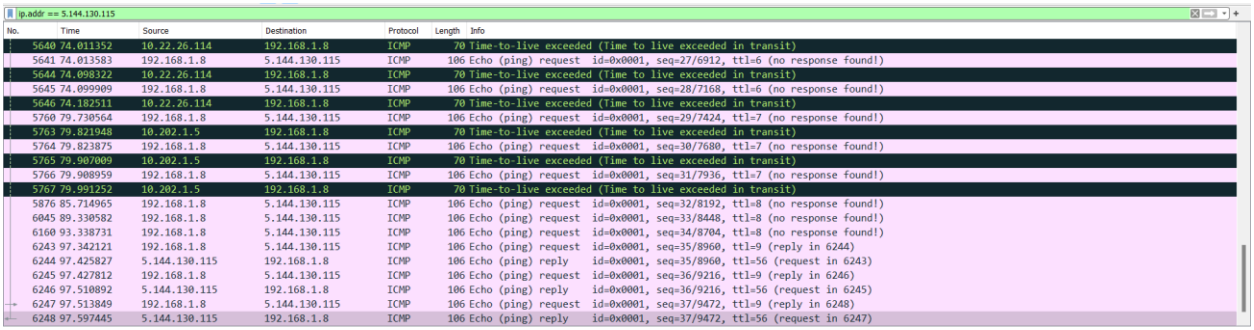
سه نوع کوئری دیگر:

- کوئری تایپ MD مربوط به Mail Destination
- کوئری تایپ TXT مربوط به Text Strings
- کوئری تایپ HINF0 مربوط به Host Information

سوال یازدهم)

درصورت انتخاب این فیلتر فقط package هایی که IP مقصد یا مبدا آنها برابر IP که دادیم بود نمایش داده میشوند. از طرفی تمام پروتکل های مشاهده شده برابر ICMP میشود. همانطور که در شکل مشاهده میشود فیلتر اعمال شده:

گزارش کار دوم آزمایشگاه شبکه



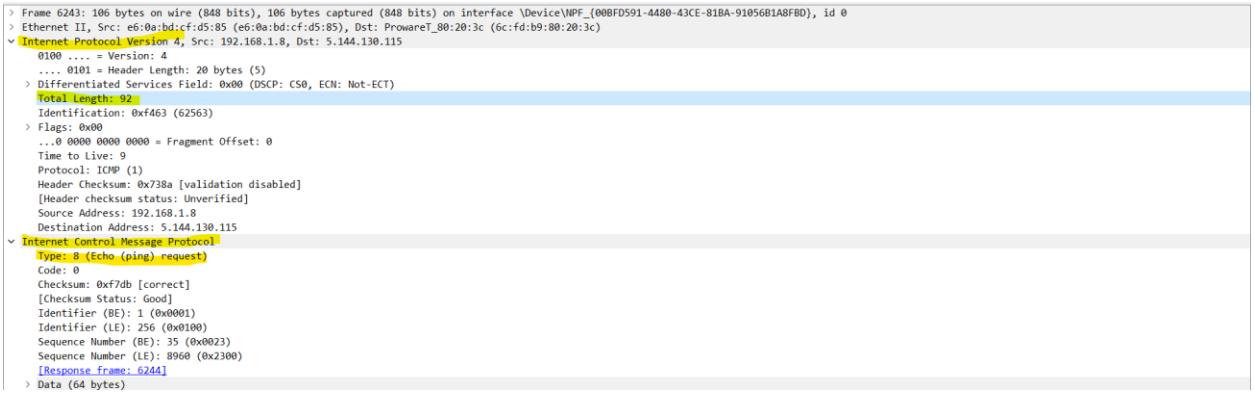
No.	Time	Source	Destination	Protocol	Length	Info
5640	74.011352	10.22.26.114	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5641	74.013583	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=6 (no response found!)
5644	74.098322	10.22.26.114	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5645	74.099909	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=6 (no response found!)
5646	74.182511	10.22.26.114	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5760	79.730564	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=7 (no response found!)
5763	79.821948	10.202.1.5	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5764	79.823875	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=7 (no response found!)
5765	79.907009	10.202.1.5	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5766	79.908959	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=7 (no response found!)
5767	79.991252	10.202.1.5	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5876	85.714965	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=8 (no response found!)
6045	89.330582	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=8 (no response found!)
6160	93.338731	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=8 (no response found!)
6243	97.342121	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=9 (reply in 6244)
6244	97.425827	5.144.130.115	192.168.1.8	ICMP	106	Echo (ping) reply id=0x0001, seq=35/8960, ttl=56 (request in 6243)
6245	97.427812	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=9 (reply in 6246)
6246	97.510892	5.144.130.115	192.168.1.8	ICMP	106	Echo (ping) reply id=0x0001, seq=36/9216, ttl=56 (request in 6245)
6247	97.513849	192.168.1.8	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=9 (reply in 6248)
6248	97.597445	5.144.130.115	192.168.1.8	ICMP	106	Echo (ping) reply id=0x0001, seq=37/9472, ttl=56 (request in 6247)

از آنجایی که IP Address سایت p30download.com برابر ۵.۱۴۴.۱۳۰.۱۱۵ است، فیلتر اعمال شده:

ip.addr == 5.144.130.115

سوال دوازدهم)

در قسمت Internet Control Message Protocol، تایپ برابر Echo (ping) Request است. از طرفی TTL یا Time To Live برابر ۹ بوده است. در شکل مشاهده میشود:



```
Frame 6243: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{00BFD591-4480-43CE-81BA-91056B1A8FBD}, id 0
Ethernet II, Src: e6:0a:bd:cf:d5:85 (e6:0a:bd:cf:d5:85), Dst: ProwareT_80:20:3c (6c:fd:b9:80:20:3c)
Internet Protocol Version 4, Src: 192.168.1.8, 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: 0xf463 (62563)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 9
    Protocol: ICMP (1)
    Header Checksum: 0x738a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.8
    Destination Address: 5.144.130.115
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7db [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 35 (0x0023)
    Sequence Number (LE): 8960 (0x2300)
    [Response frame: 6244]
  > Data (64 bytes)
```

سوال سیزدهم)

بله، مقادیر در حال تغییر هستند زیرا در صورت بروز هر خطایی در دریافت/ارسال بسته ها TTLیا Time To Live از گیر کردن در حلقه بینهایت جلوگیری میکند.

سوال چهاردهم)

این فیلتر برا نمایش پروتکل های TCP است. سایت Wikipedia این مشاهده را تایید میکند.