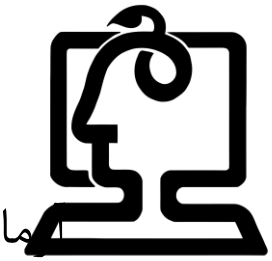
به نام ایزد یکتا



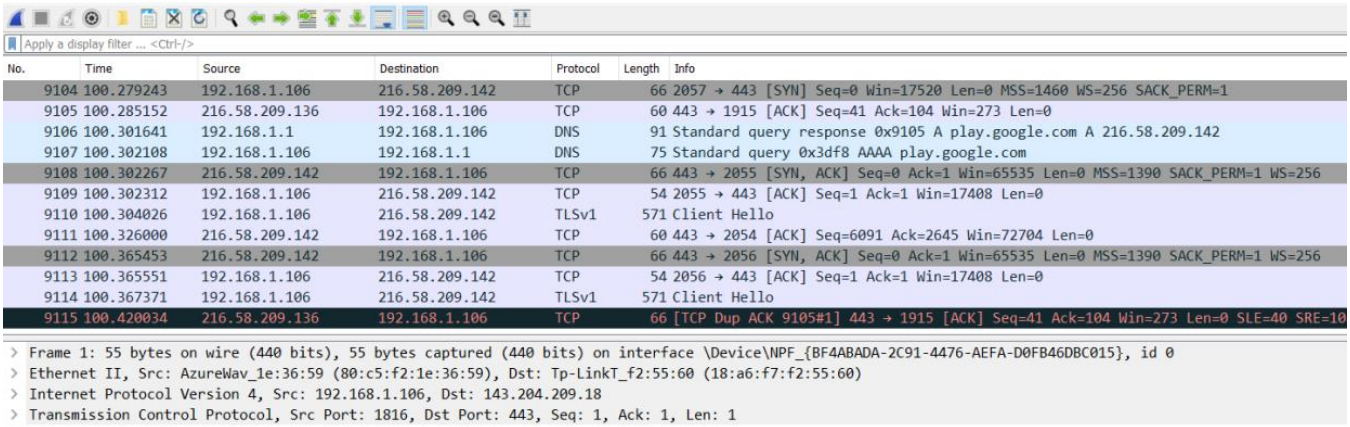
آزمایش دوم درس آزمایشگاه شبکه‌های کامپیوتری

گروه دوم

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲

سوال اول) پروتکل‌هایی من‌جمله TCP, DNS, TLSv1, TLSv1.3, TLSv1.2, MDNS,...

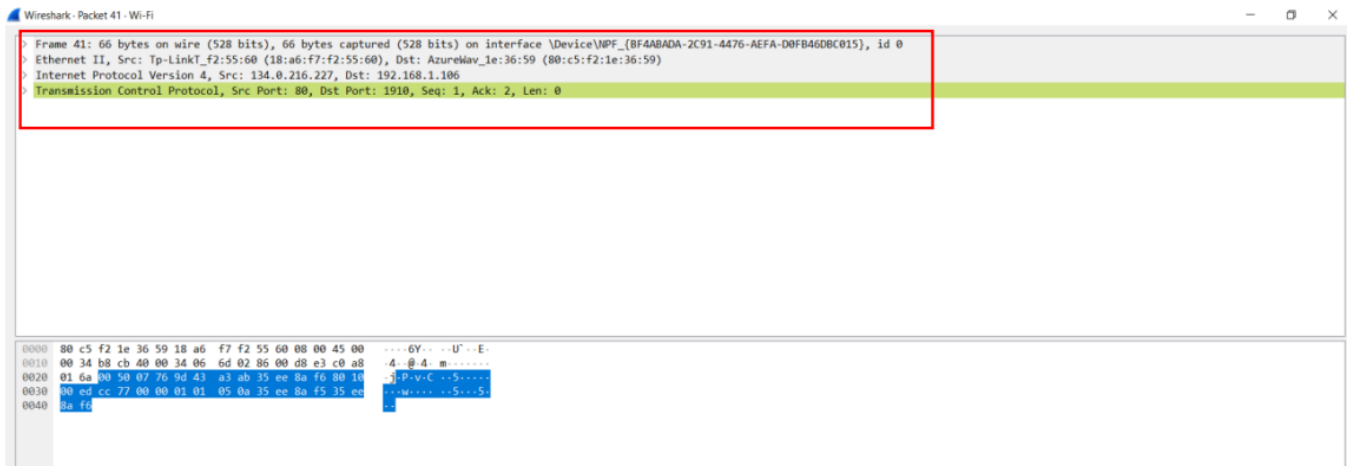


عکس 1-1

سوال دوم)

در اینجا بسته شماره 4 را انتخاب کردیم و اطالعات پروتکل‌های لایه‌های مختلف آن را مشاهده می‌کنیم:

در لایه Transport از TCP ،در لایه Network از پروتکل IPv4، در لایه Link از پروتکلچ Ethernet II استفاده شده است (در این بسته، اطلاعات پروتکل لایه اپلیکیشن را مشاهده نمی‌کنیم). هر لایه اطلاعات دریافتی از لایه بالاتر را می‌گیرد و اطلاعات جدیدی به آن اضافه می‌کند (مثلا لایه انتقال، مسیج را از لایه اپلیکیشن دریافت کرده و به سر آن بیت‌های جدیدی اضافه می‌کند و یک Segment را به لایه شبکه تحویل می‌دهد) همانطوری که در شکل 2-1 مشاهده می‌کنید اندازه فریم در این بسته 66بایت است و اندازه بسته‌ی لایه 3 (Network) در شکل 2-2 مشخص شده است که 52 بایت می‌باشد.



شکل 2-1

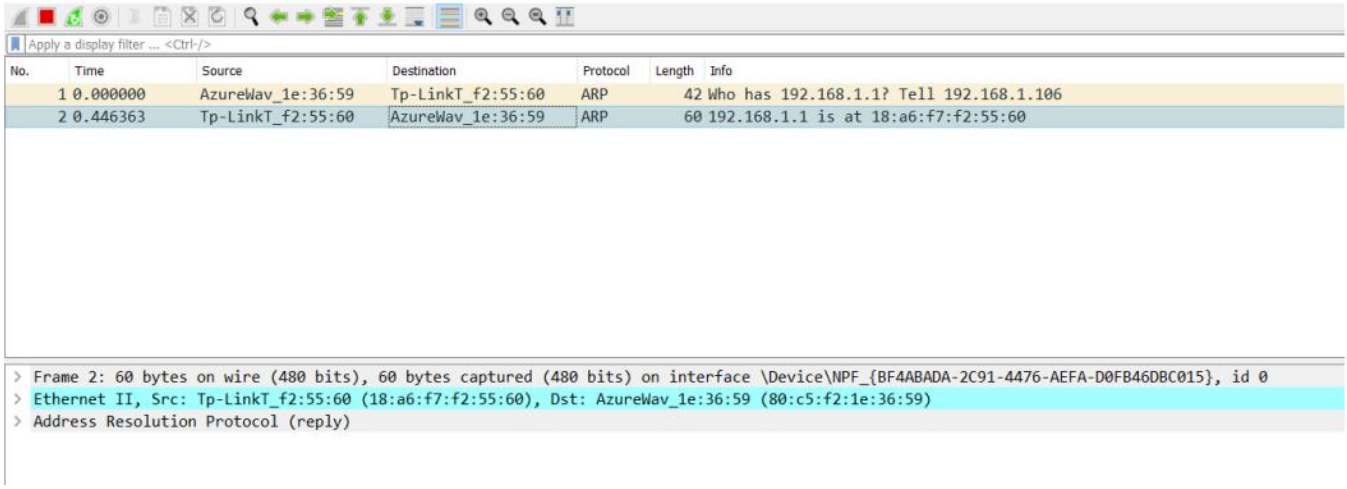
```
> Ethernet II, Src: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60), Dst: AzureWav_1e:36:59 (80:c5:f2:1e:36:59)
v Internet Protocol Version 4, Src: 134.0.216.227, Dst: 192.168.1.106
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xb8cb (47307)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 52
    Protocol: TCP (6)
    Header Checksum: 0x6d02 [validation disabled]
    [Header checksum status: Unverified]
```

شکل 2-2

سوال سوم)

بسته‌ای که در سوال 2 مشاهده کردیم، لایه اپلیکیشن نداشت.

بسته‌ی زیر نیز ARP است و لایه اپلیکیشن و انتقال را ندارد.



شکل 3-1

در هردوی این بسته‌ها لایه فیزیکی و لایه لینک را داریم.

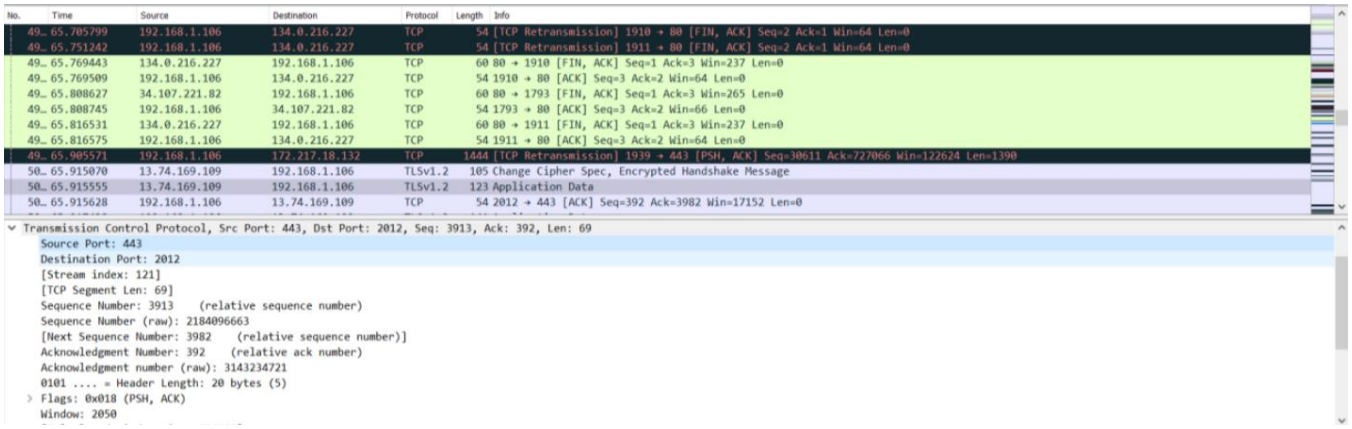
سوال چهارم) 0x1307

```
> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)
v Internet Protocol Version 4, Src: 192.168.1.106, Dst: 23.58.222.26
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0x3061 (12385)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x1307 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.106
    Destination Address: 23.58.222.26
```

شکل 4-1

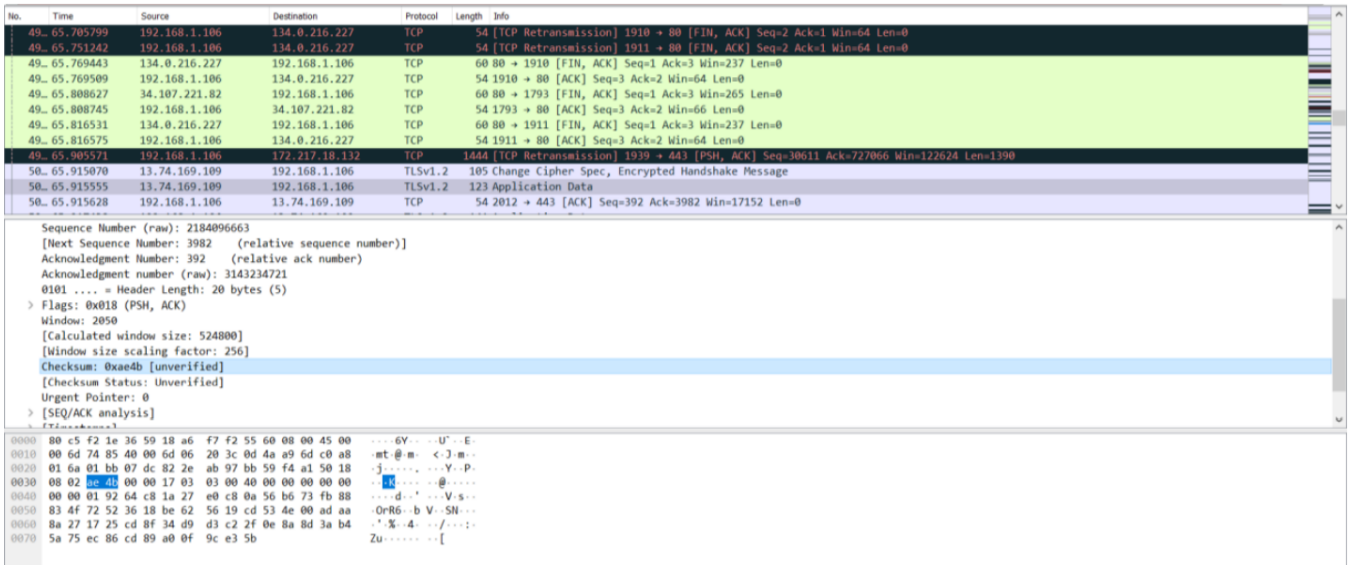
سوال پنجم)

در این بسته که از پروتکل tcp استفاده کرده است شماره پورت مبدا 443 و پورت مقصد 2012 می‌باشد. شماره پورت در مبدا نشان‌دهنده پردازه است که داده را ارسال کرده است و در مقصد نشان دهنده پردازه‌ایست که میبایست داده را دریافت کند و در اولین هدرهای tcp و udp گنجانده می‌شود.



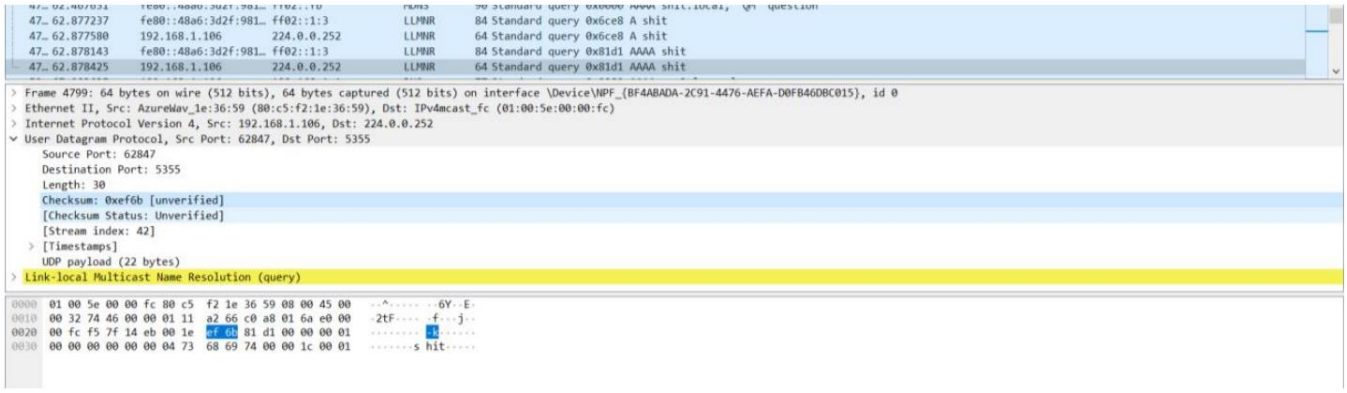
عکس 5-1

TCP Checksum: 0x0000ae4b



عکس 5-2

UDP checksum: 0x0000ef6b



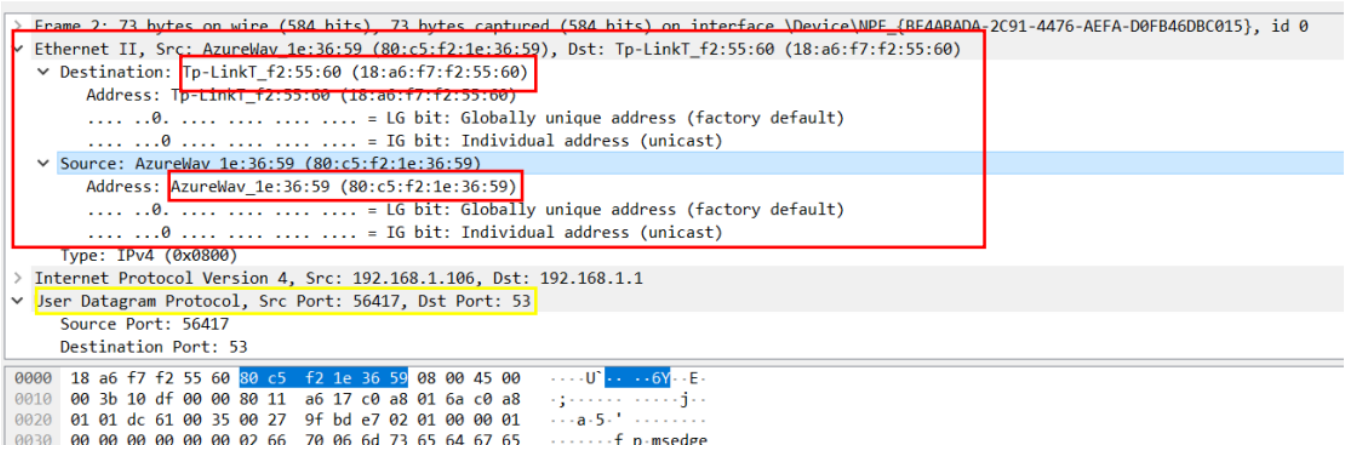
عکس 5-3

بخش دوم

```
Pinging google.com [216.58.210.78] with 32 bytes of data:
Reply from 216.58.210.78: bytes=32 time=183ms TTL=111
Reply from 216.58.210.78: bytes=32 time=170ms TTL=111
Reply from 216.58.210.78: bytes=32 time=150ms TTL=111
Reply from 216.58.210.78: bytes=32 time=171ms TTL=111

Ping statistics for 216.58.210.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 150ms, Maximum = 183ms, Average = 168ms

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

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

عکس 5-4

سوال ششم) یکی از بسته‌های ارسال شده را انتخاب کردیم. مبدا آن 192.168.1.106 می‌باشد. پروتکل لایه UDP می‌باشد که با کادر زرد مشخص شده است. آدرس IP مقصد نیز برابر 192.168.1.1 می‌باشد و از سرآیند لایه دوم، آدرس فیزیکی مبدا و مقصد را مشاهده می‌کنیم که در شکل با کادر قرمز مشخص شده است.



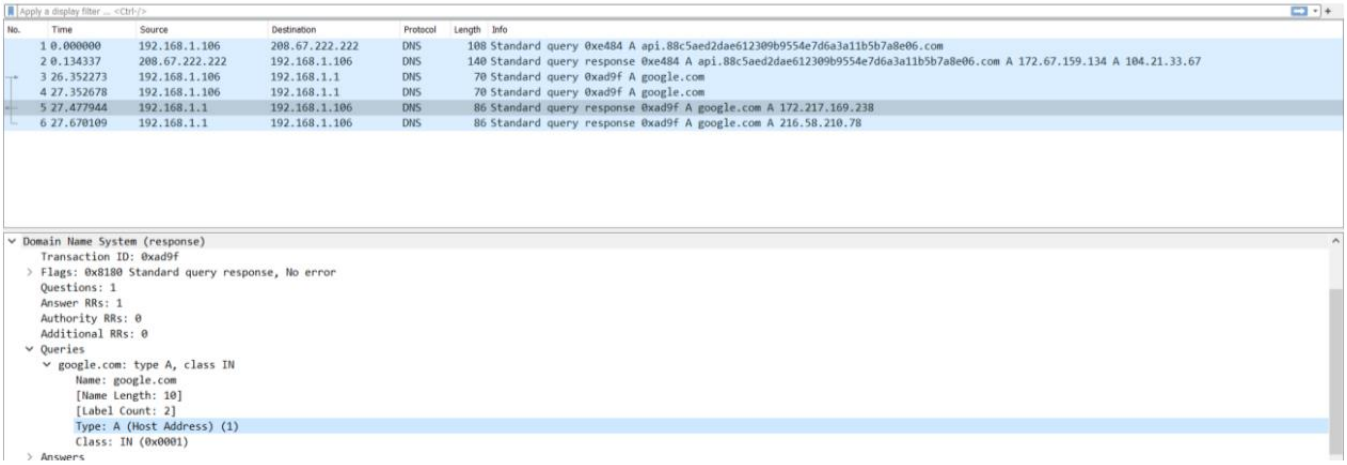
شکل 6-1

سوال هفتم) آدرس آیپی مبدا و مقصد را می‌توانیم در بخش ipconfig /all مشاهده کنیم.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek 8822BE Wireless LAN 802.11ac PCI-E NIC
   Physical Address. . . . . . . . . : 80-C5-F2-1E-36-59
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::48a6:3d2f:981d:3372%26(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, April 8, 2021 9:41:59 PM
   Lease Expires . . . . . . . . . . : Sunday, April 11, 2021 9:41:59 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 209765874
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F4-F3-2A-2C-FD-A1-AC-52-7B
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Disabled

Ethernet adapter Bluetooth Network Connection:
```

عکس 7-1

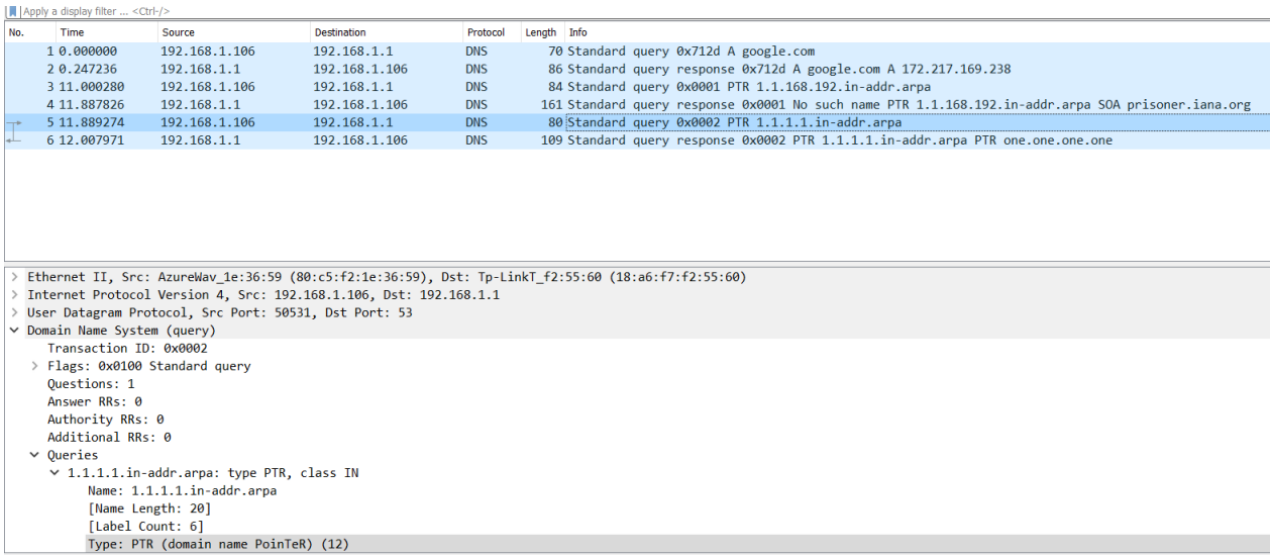
سوال هشتم) محددا ران می‌کنیم و پینگ می‌پیریم تا فقط بسته‌های مربوط به پینگ را capture کنیم.



عکس 8-1

همانطور که می‌بینیم تایپ A یا 1 است. دکوردهای این تایپ ساده ترین دکوردهای DNS هستند و از آن‌ها برای اشاره یک دامنه با زیردامنه به یک آدرس IP استفاده می‌شود. به عبارتی این تایپ از دکورد برای ترجمه آدرس دامنه google.com به آدرس IP آن استفاده شده است.

سوال نهم) این بار تایپ query ما PTR است یا پوینتر است که برعکس دکوردهای تایپ 1، مشخص می‌کند که یک آدرس IP به چه دامنه‌ای اشاده می‌کند و بیشتر در DNS lookup از آن استفاده می‌شود.



عکس 9-1

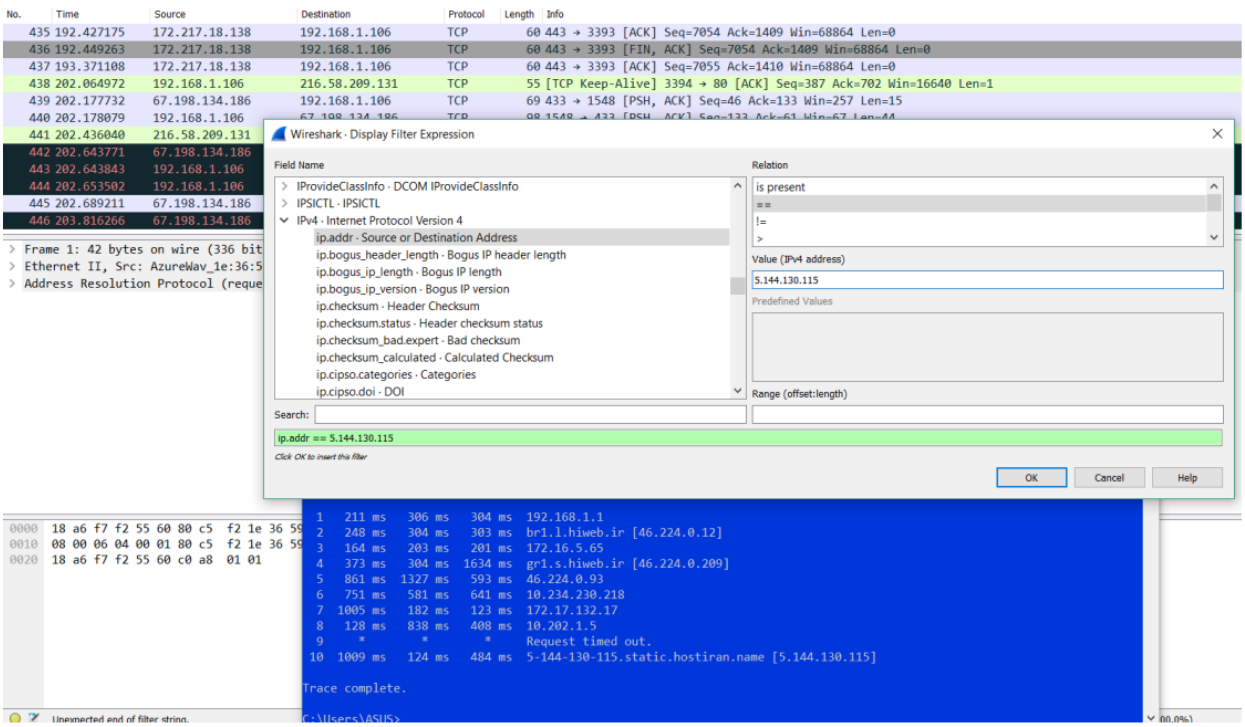
سوال دهم)

دکورد تایپ MX که در ارسال ایمیل از آن استفاده می‌شود.

دکورد تایپ LOC که نقطه جغرافیایی منسوب به یک دامنه را مشخص می‌کند.

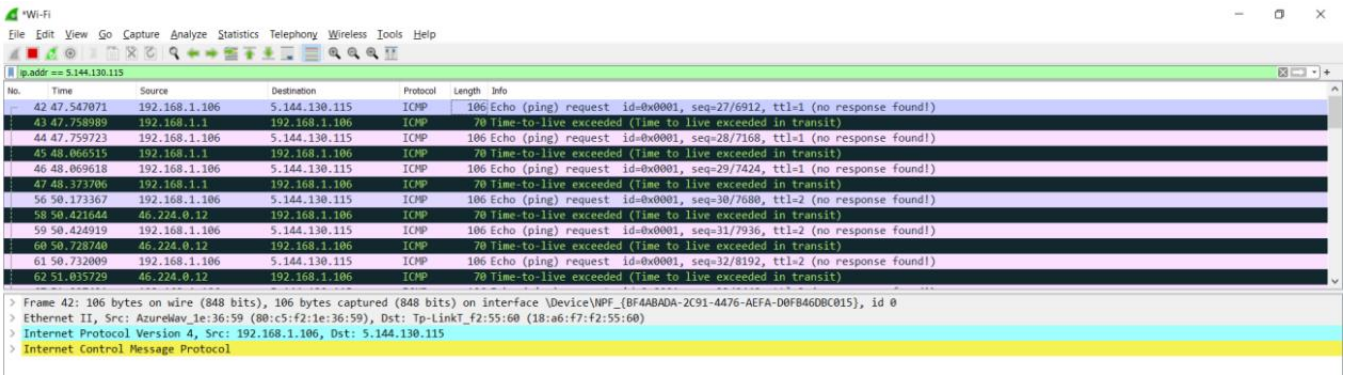
دکورد تایپ APL که لیستی از رنج‌های آدرسی را مشخص می‌کند.

بخش سوم



عکس 10-1

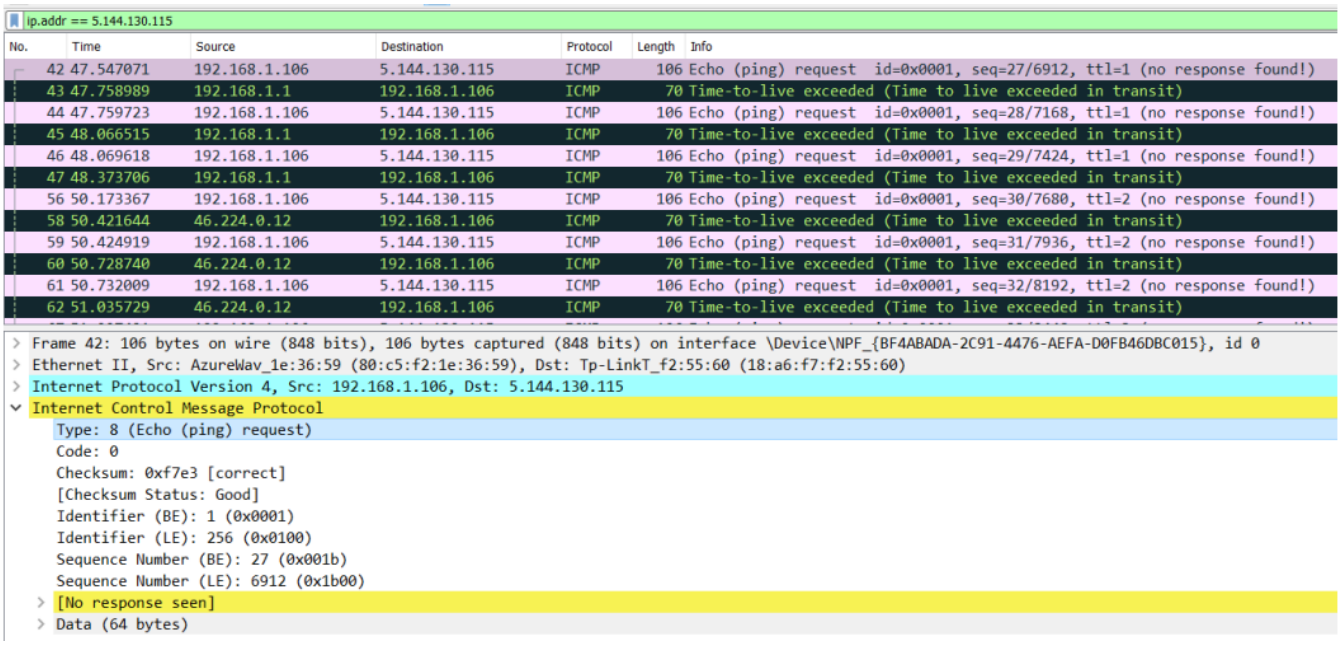
سوال یازدهم) ICMP



عکس 11-1

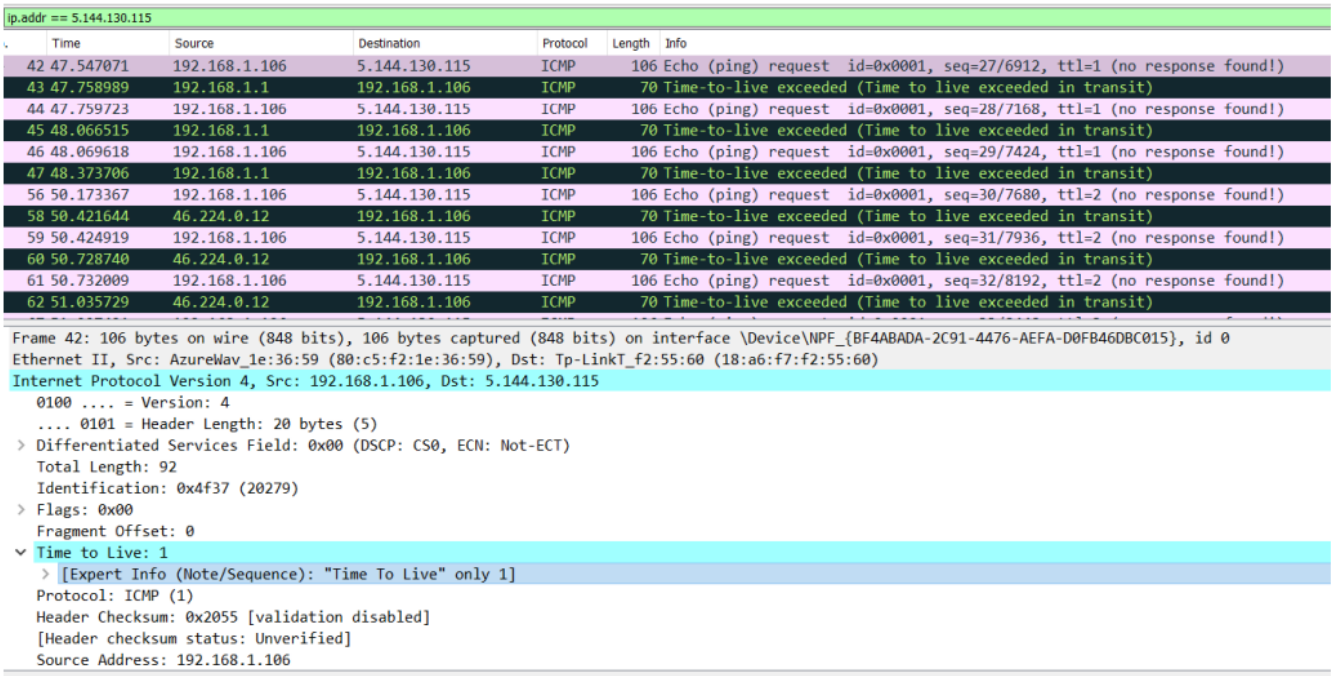
تایپ B

سوال دوازدهم)



عکس 12-1

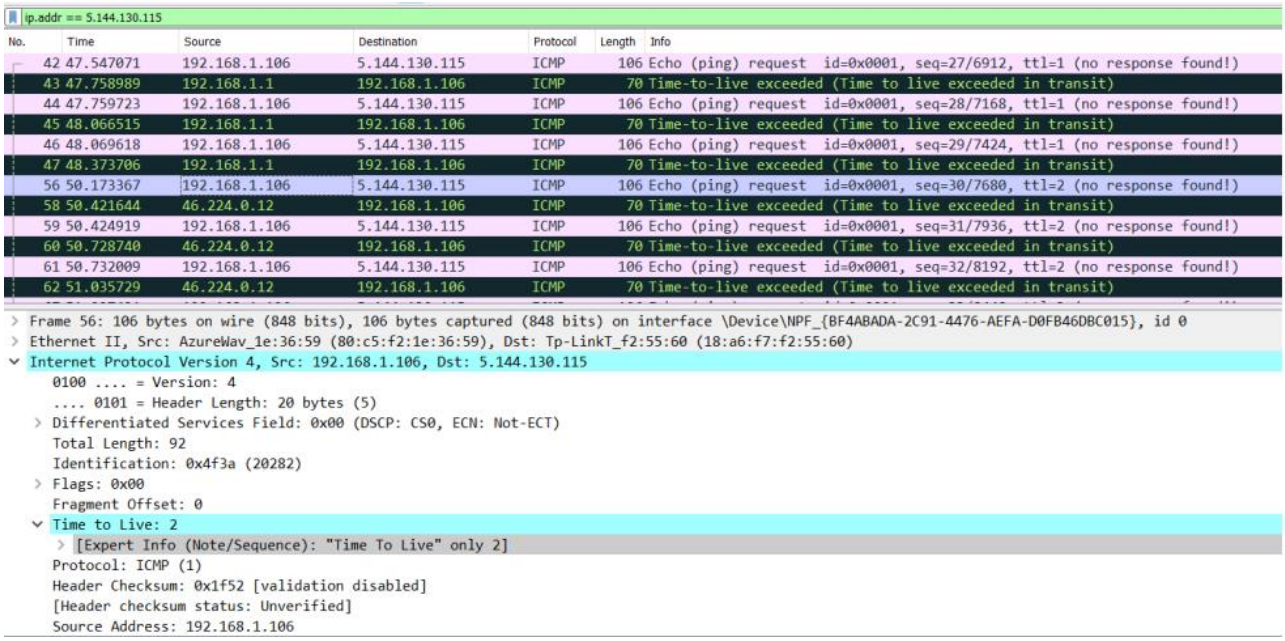
TTL=1



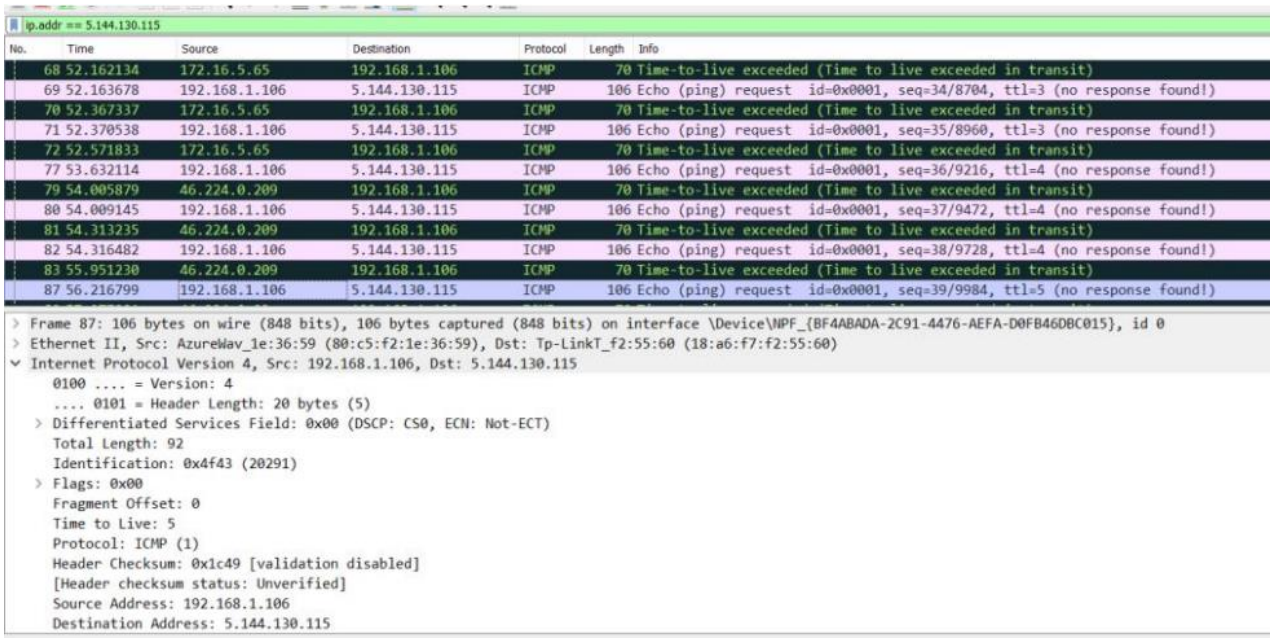
عکس 12-2

سوال سیزدهم) همانطور که مشاهده می‌کنید هرچه در بسته‌هایی که از آدرس 192.168.1.106 ارسال شده‌اند پیش می‌رویم؛ TTL افزایش می‌یابد. باید از دستور tracert برای بررسی مسیری که یک بسته برای رسیدن به IP مقصد آن را طی می‌کند استفاده می‌کنیم.

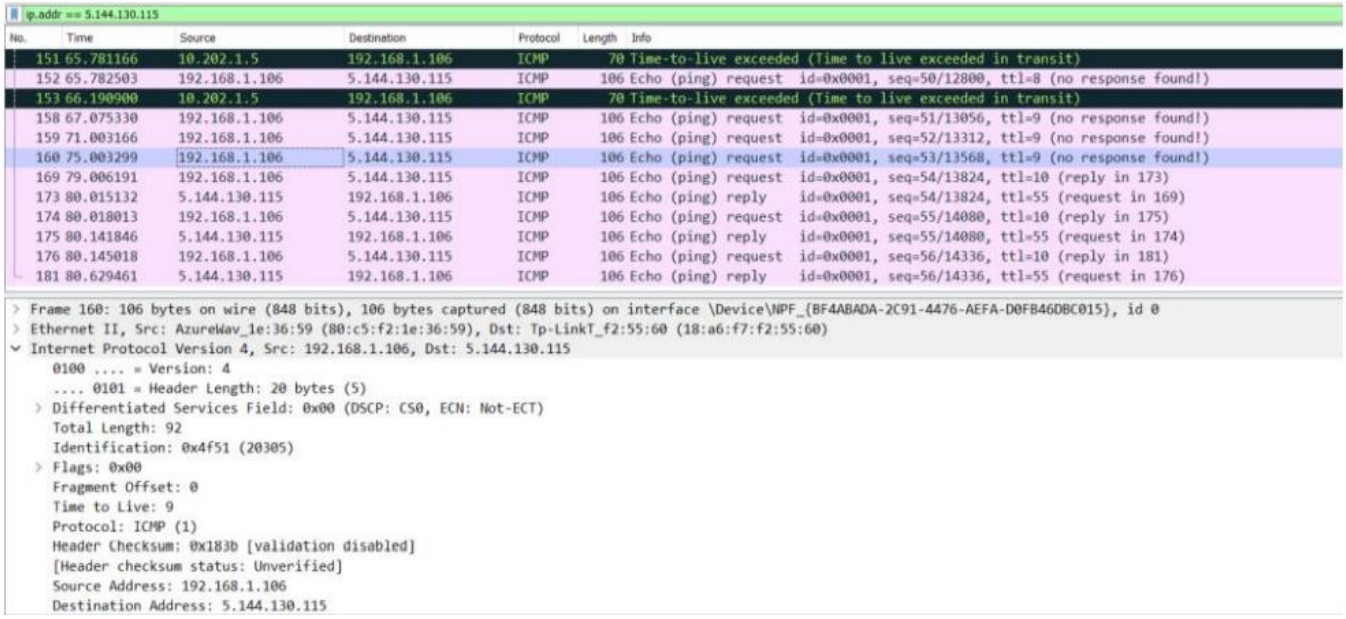
این عدد از 1 تا 10 تغییر می‌کند چون tracert نیز در ده گام انجام شد.



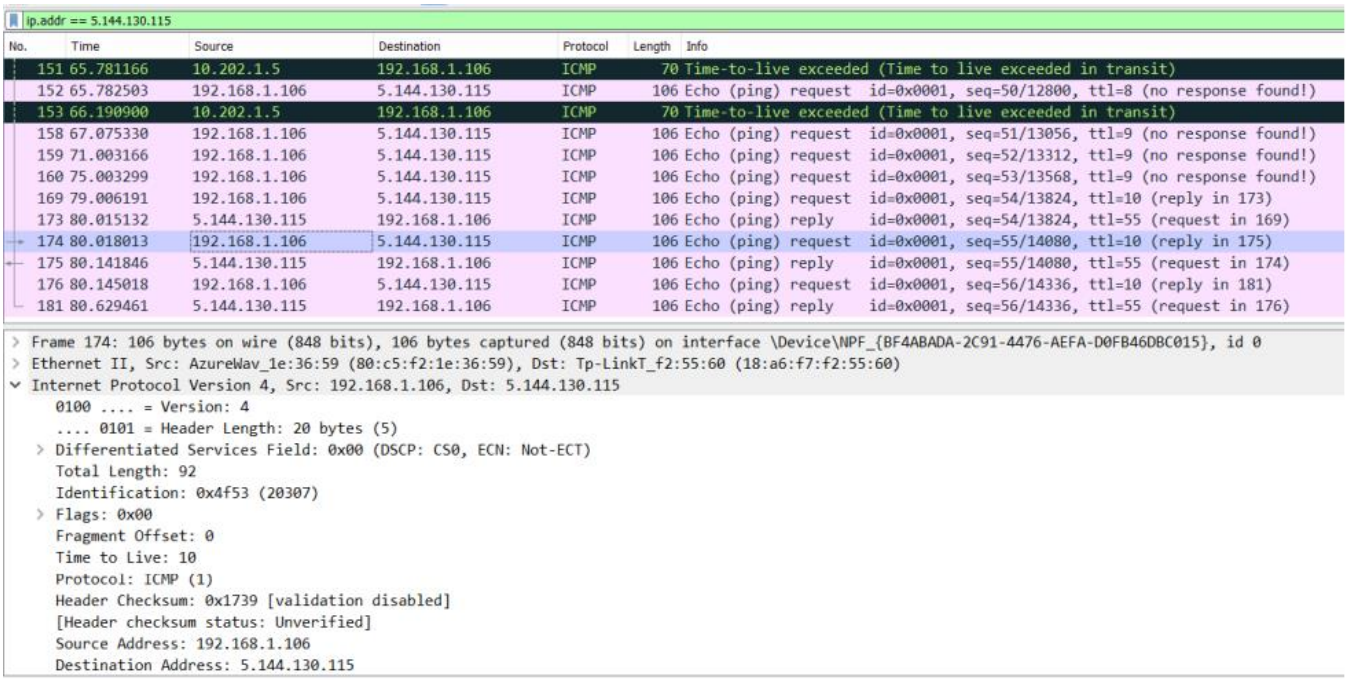
عکس 13-1



عکس 13-2



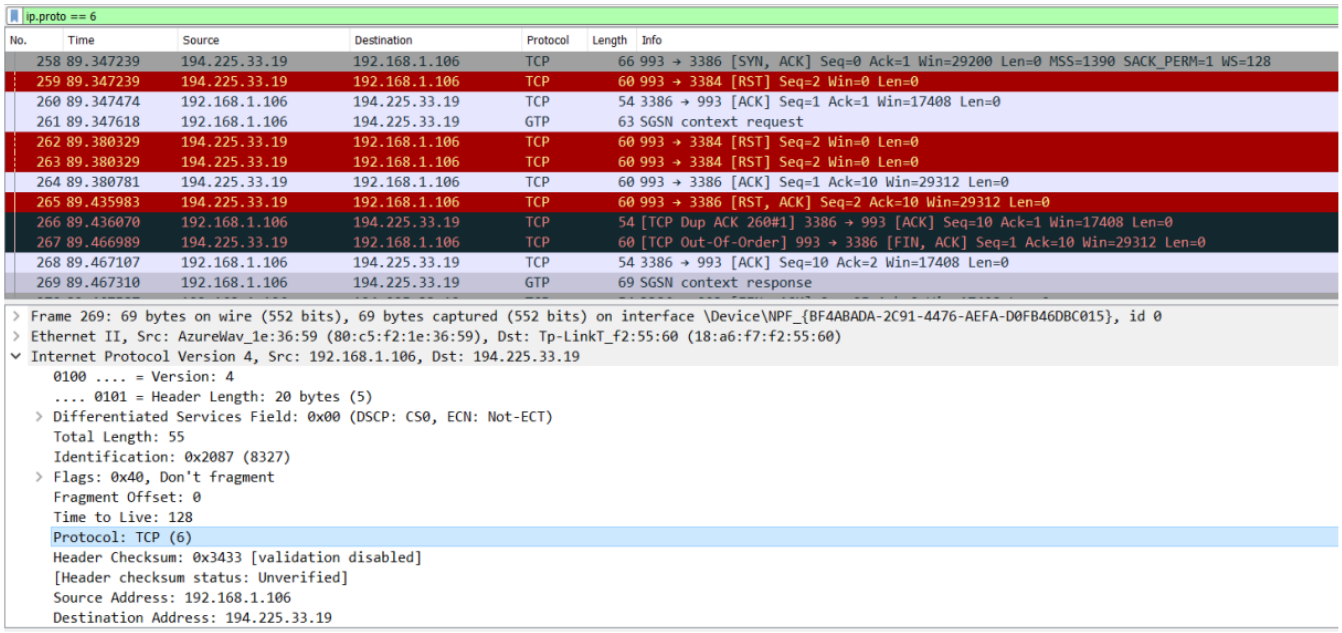
عکس 13-3



عکس 13-4

سوال چهاردهم)

این فیلتر بسته‌ها را بر اساس ورژن پروتکل IP آنها جداسازی می‌کند و بخش مشترک تمامی آنها، قسمت پروتکل در لایه سوم می‌باشد که برابر 6 است.



عکس 14-1