به نام ایزد یکتا

آزمایش دوم درس آزمایشگاه شبکه‌های کامپیوتری

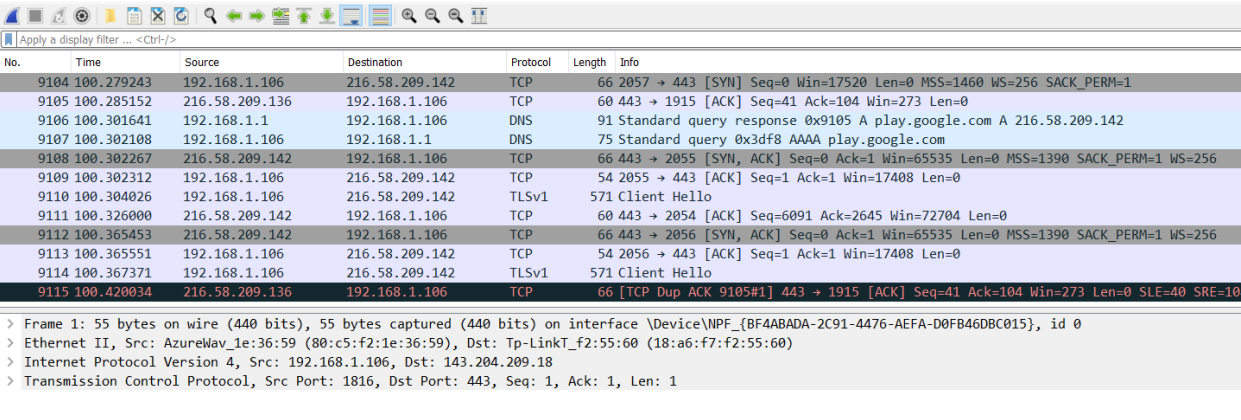
­­

گروه دوم

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲

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

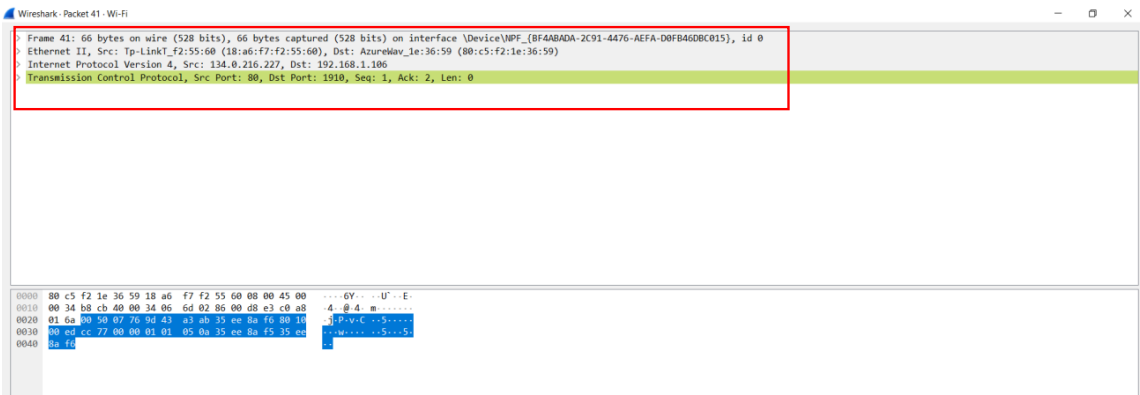


عکس 1-1

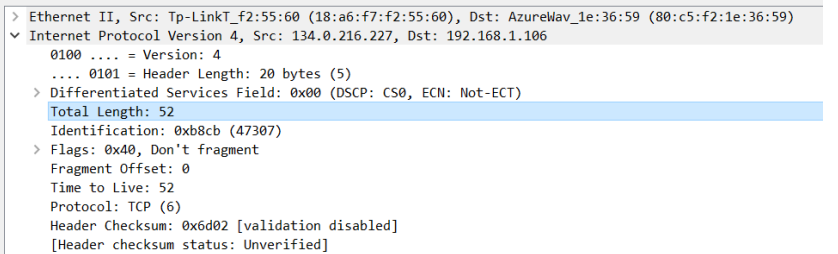
سوال دوم)

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

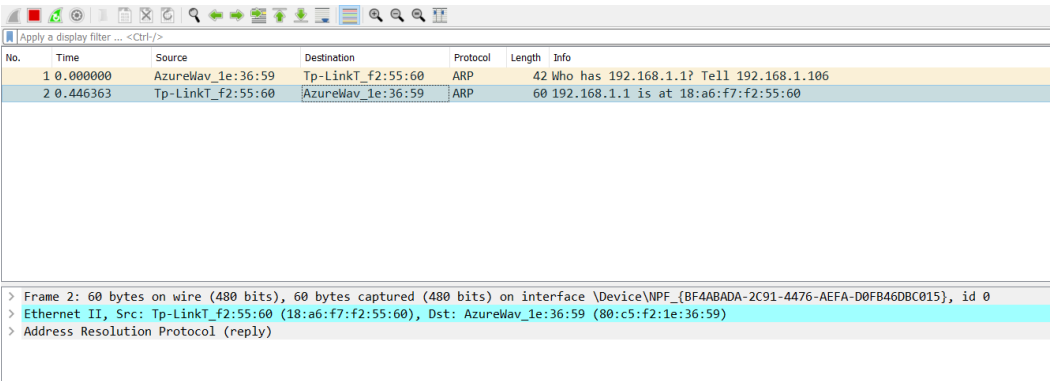


شکل 2-2

سوال سوم)

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

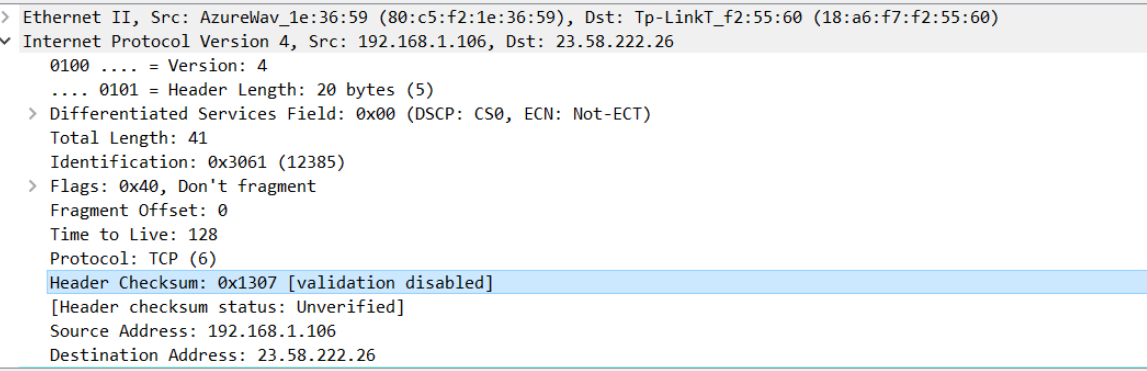
بسته‌ی زیر نیز ARP است و لایه اپلیکیشن و انتقال را ندارد.



شکل 3-1

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

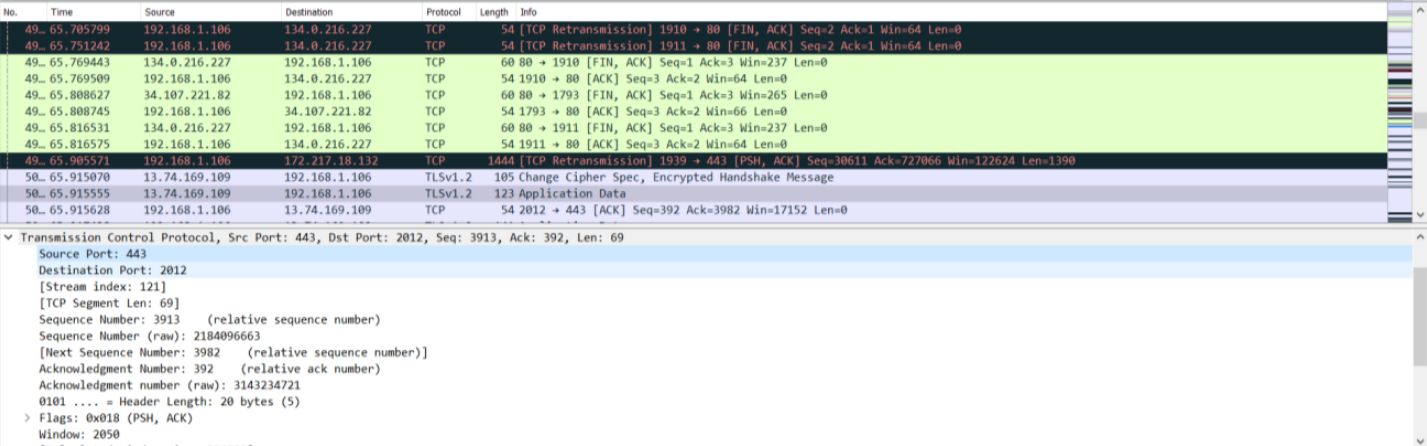
سوال چهارم) 0x1307



شکل 4-1

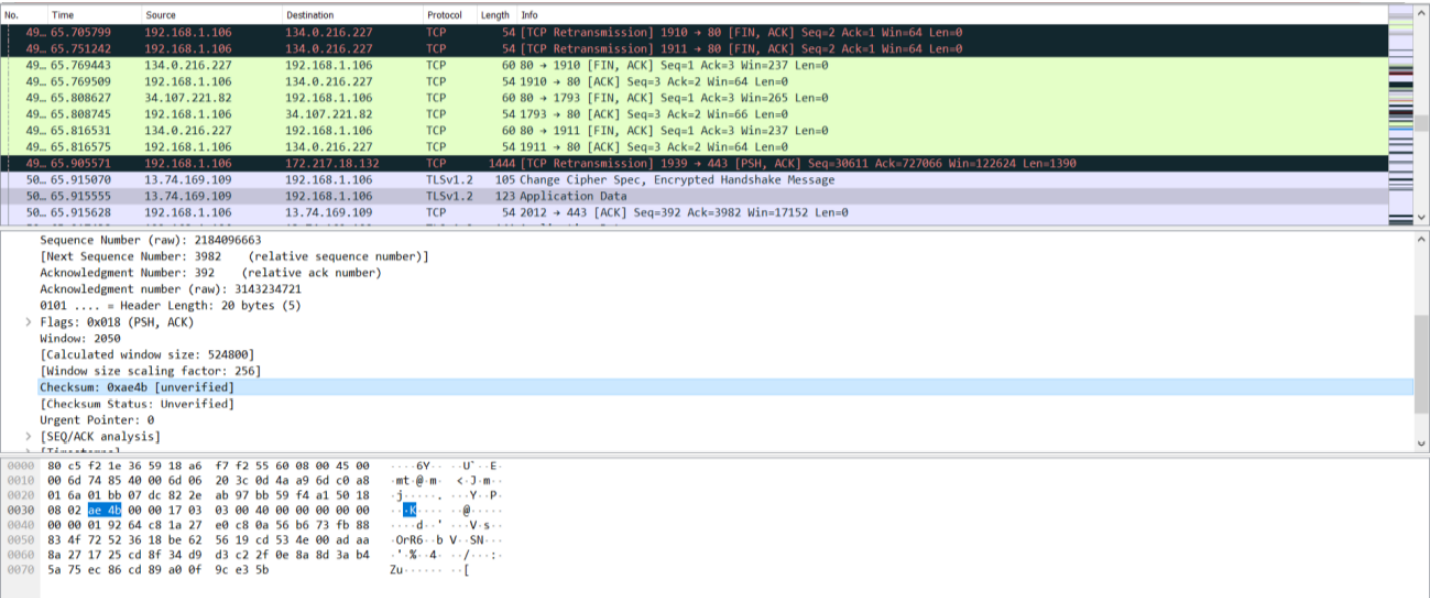
سوال پنجم)

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.



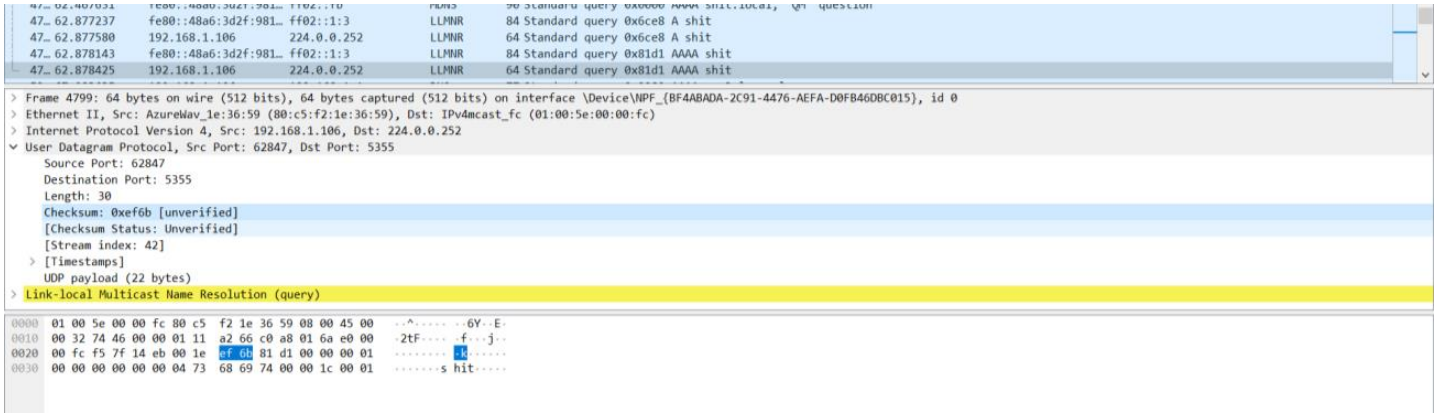
عکس 5-1

TCP Checksum: 0x0000ae4b



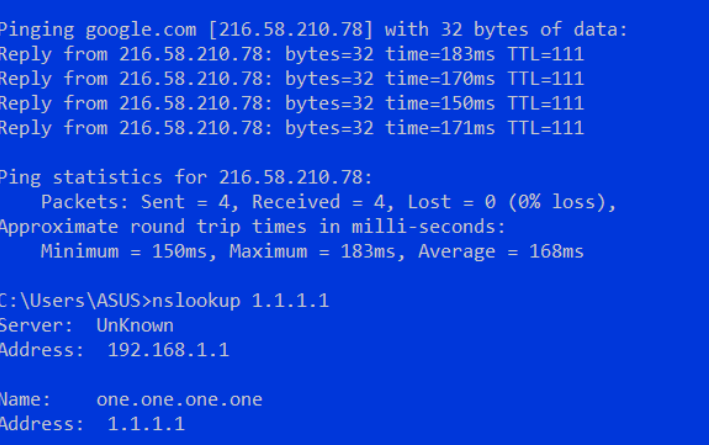
عکس 5-2

UDP checksum: 0x0000ef6b



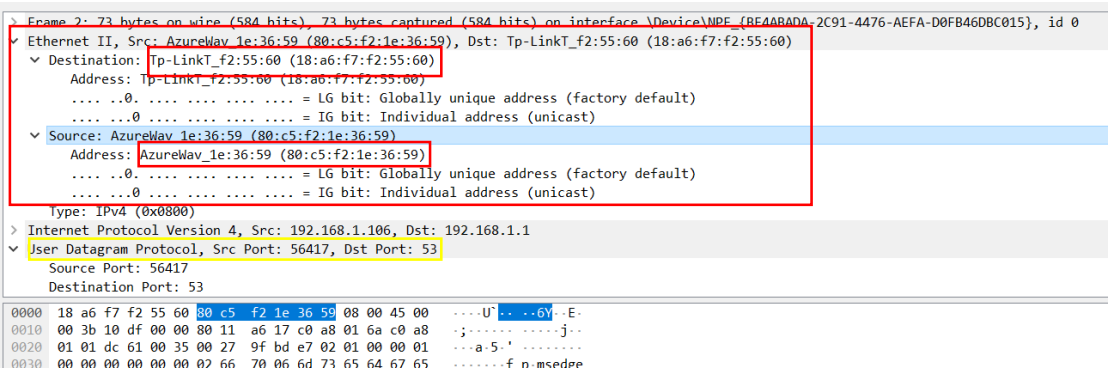
عکس 5-3

بخش دوم

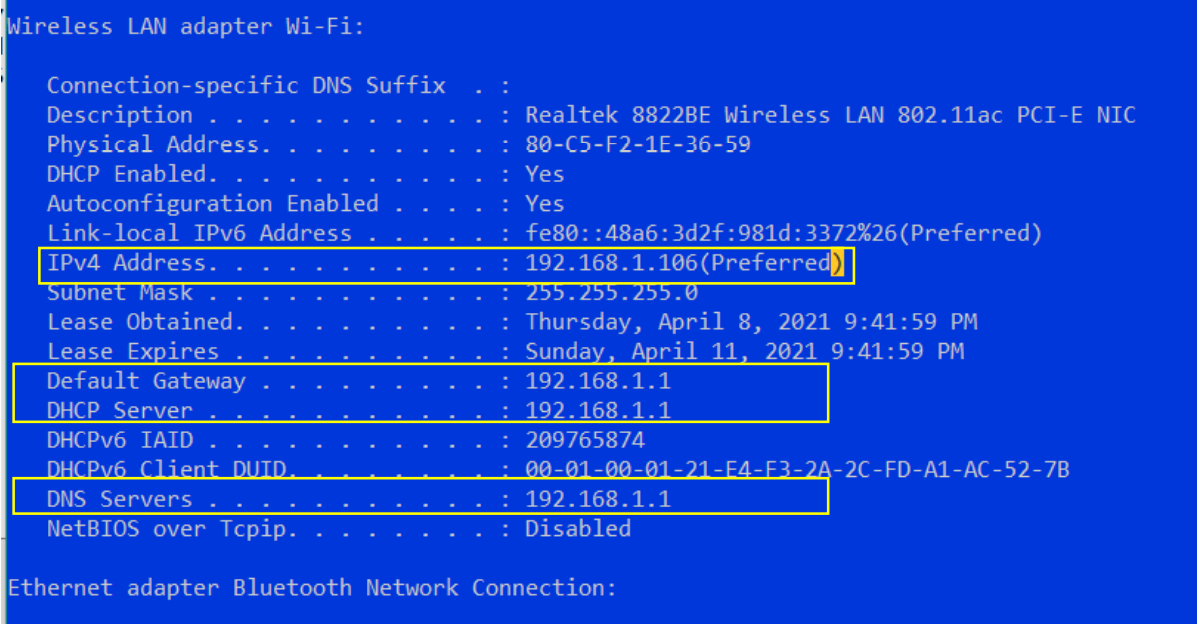


عکس 5-4

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.

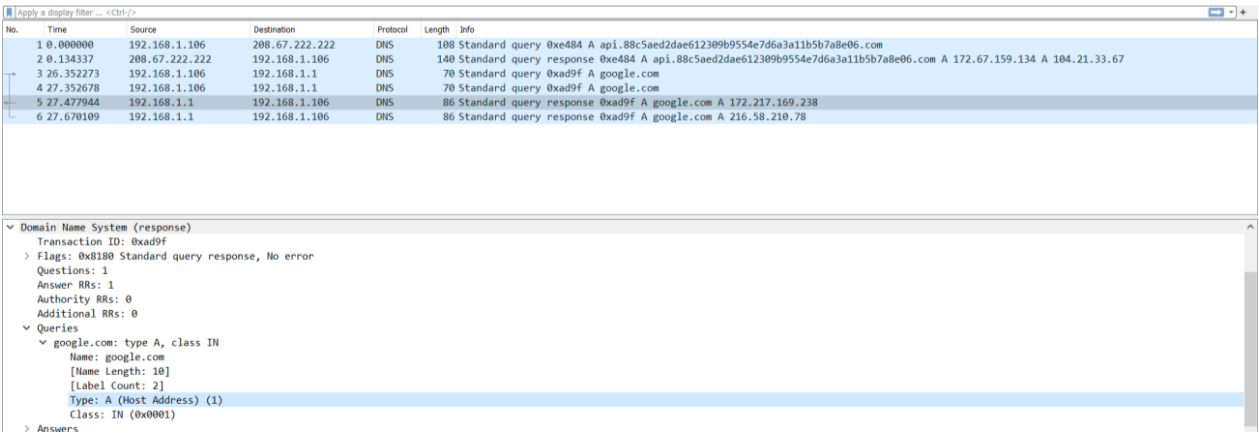


شکل 6-1

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

عکس 7-1

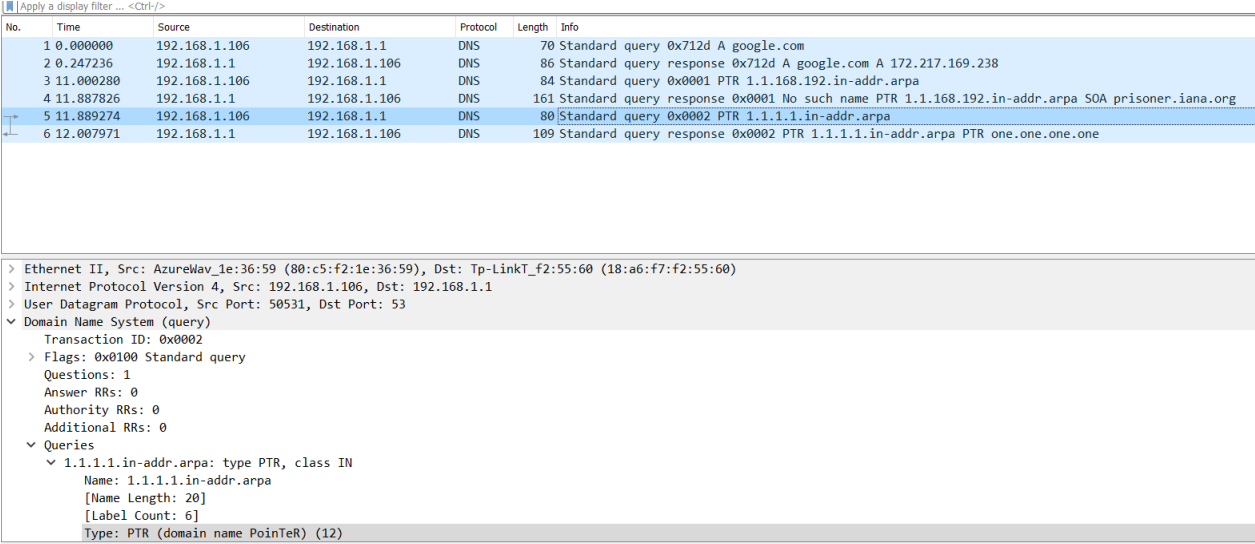
سوال هشتم) محددا ران می‌کنیم و پینگ می‌پیریم تا فقط بستههای مربوط به پینگ را capture کنیم.



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

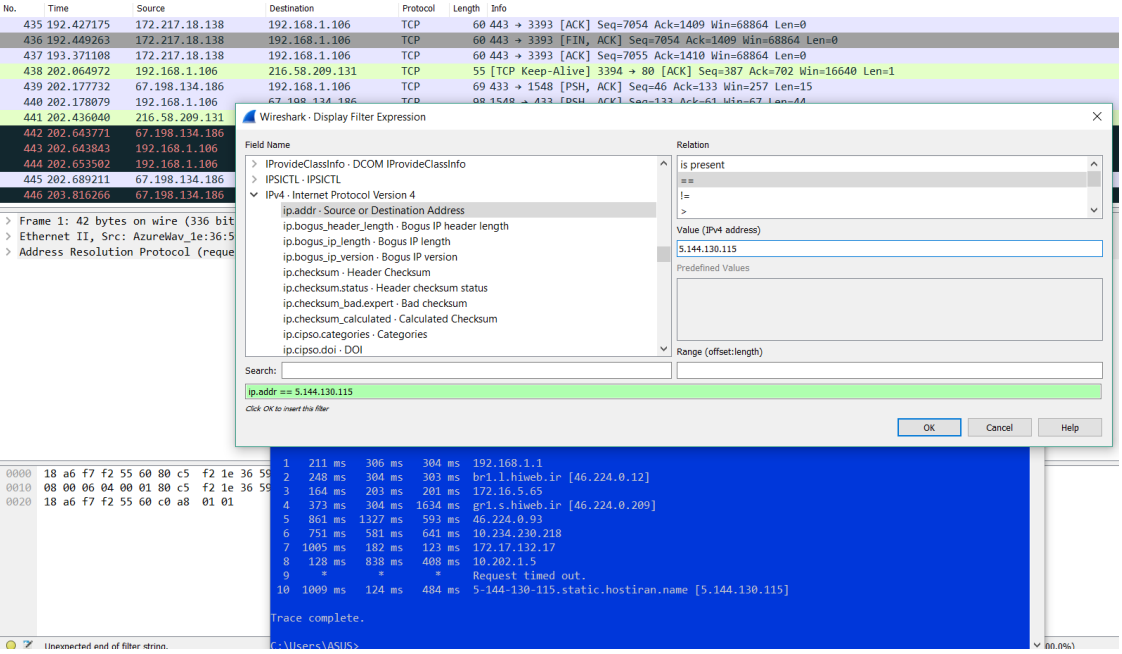
سوال دهم)

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

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

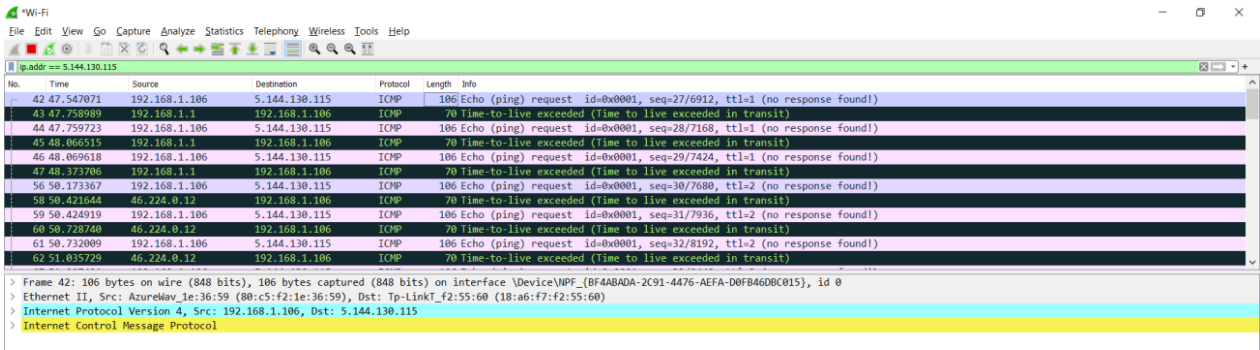
دکورد تایپ APL که لیستی از رنج‌های آدرسی را مشخص می‌کند.

بخش سوم



عکس 10-1

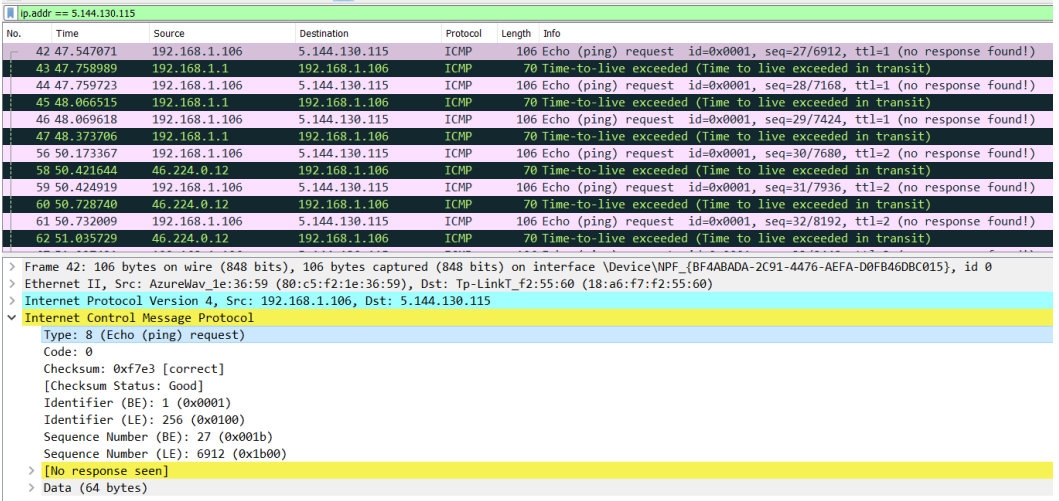
سوال یازدهم) ICMP



عکس 11-1

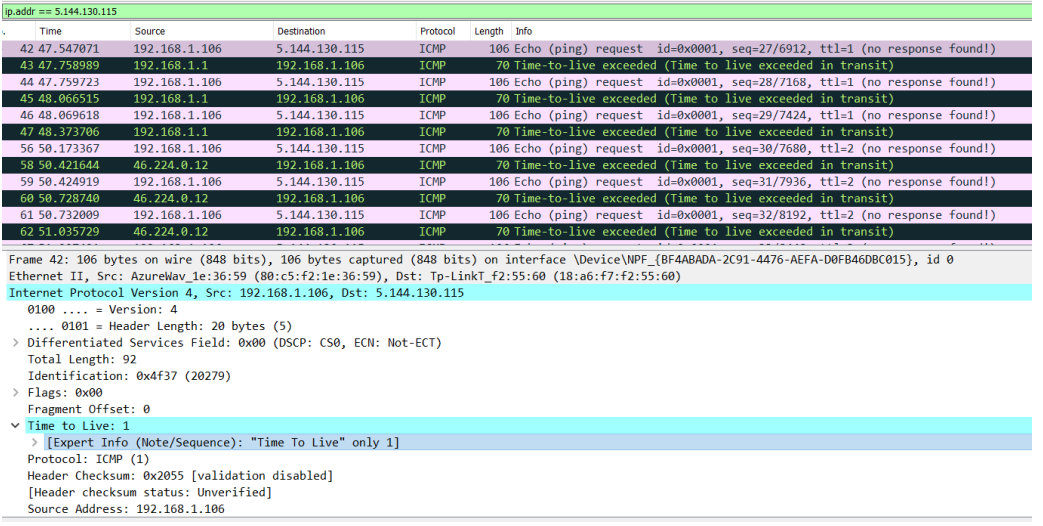
تایپ B

سوال دوازدهم)



عکس 12-1

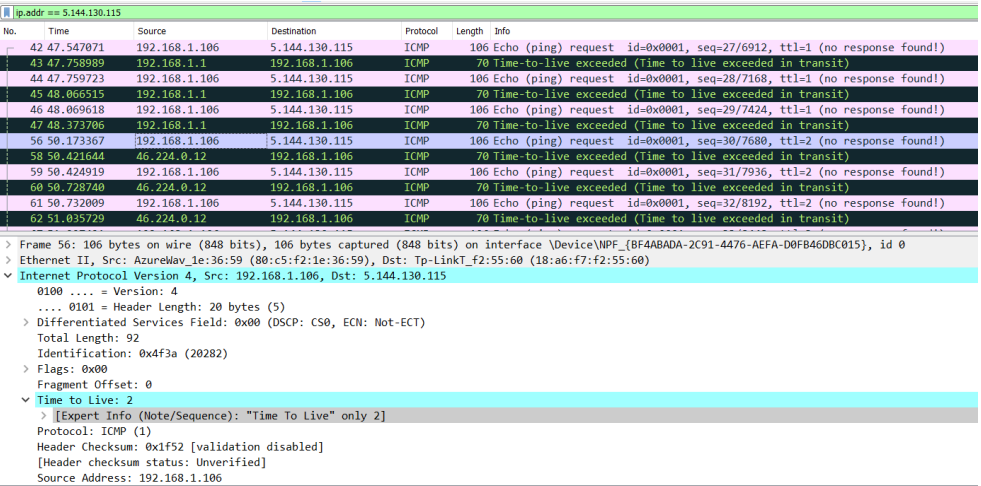
TTL=1



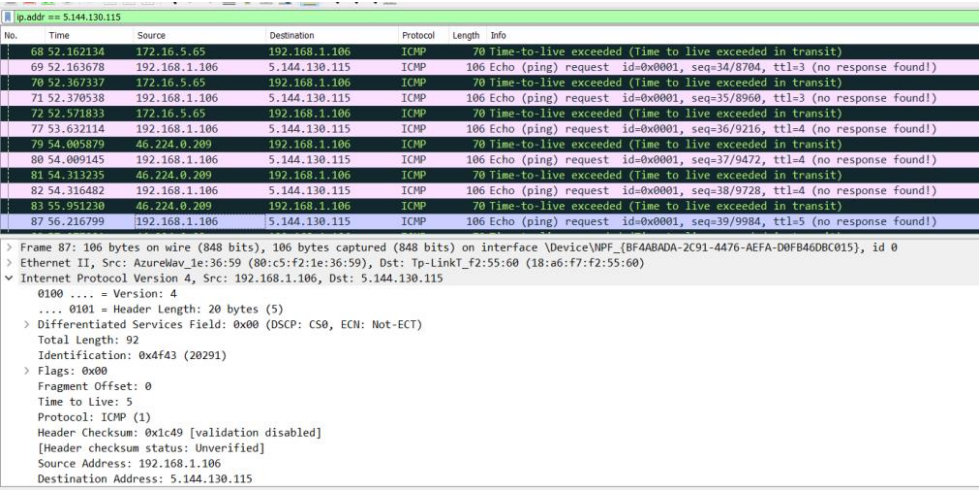
عکس 12-2

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.

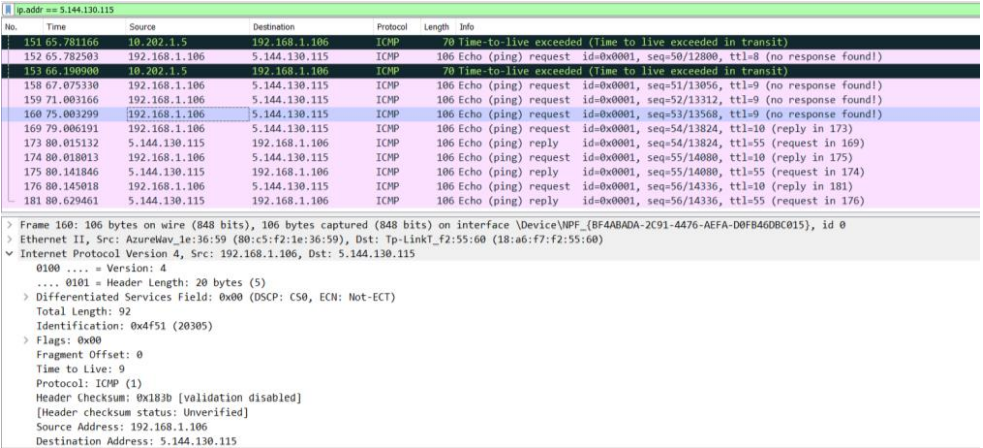
این عدد از 1 تا 10 تغییر می‌کند چون tracert نیز در ده گام انجام شد.



عکس 13-1



عکس 13-2



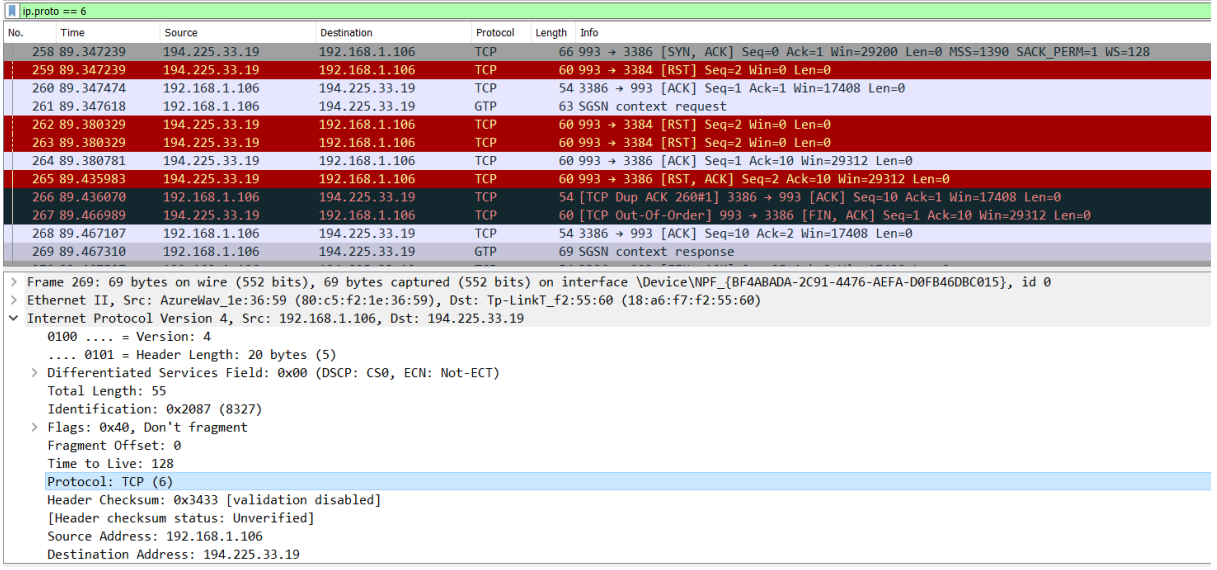
عکس 13-3



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