

به نام خدا

آشنایی با نرم افزارWireShark

فصل یک، آزمایش سه



محمد جواد زندیه 9831032

3 مهر 1401

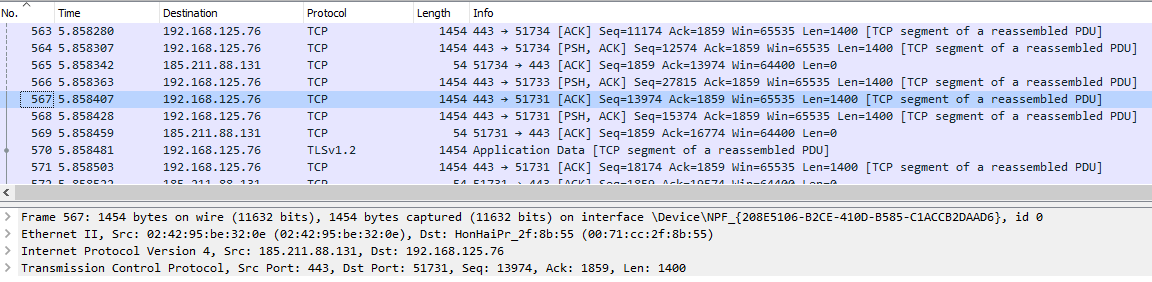
دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر، آزمایشگاه شبکه های کامپیوتری

سوال 1: به یک بخش دلخواه از بسته های شنود شده مراجعه کنید. چه پروتکل هایی را مشاهده می کنید. لیست آن ها را یادداشت کنید.

UDP, TLSv1.3, TLSv1.2, TCP, SSDP, QUIC, MDNS, LLMNR, IGMPv2, ICMPv6, ICMP, HTTP, DNS, DHCPv6, ARP

سوال 2: یک بسته را به دلخواه انتخاب کنید. مشخص کنید که چه پروتکل هایی در لایه های مختلف آن استفاده شده است. ترتیب قرارگیری بیت ها داخل بسته چه ارتباطی با لایه های مختلف دارد؟ اندازه فریم لایه دو این بسته چقدر است؟ اندازه بسته لایه سه چقدر است؟

بسته شماره 567 در این capture را برای پاسخ به این سوال بررسی می کنیم(این بسته از پروتکل TCP که دارای 3 لایه است استفاده می کند).



Transport Layer (layer 3)

Network Layer (layer 2)

Data Link Layer (layer 1)

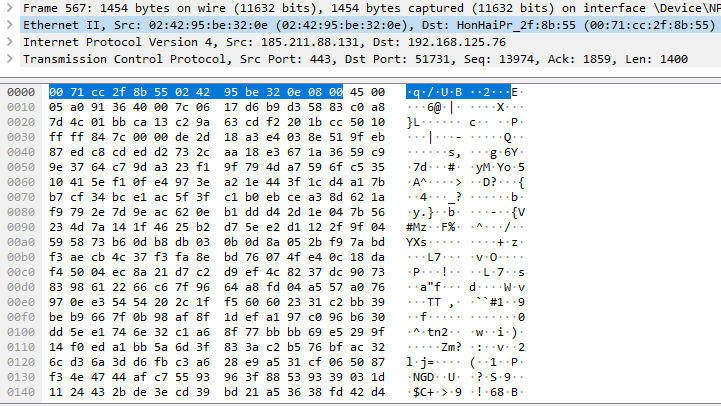
شکل (1) بسته شماره 567 به همراه اسم و شماره لایه ها[[1]](#footnote-1)

پروتکل لایه های مختلف:

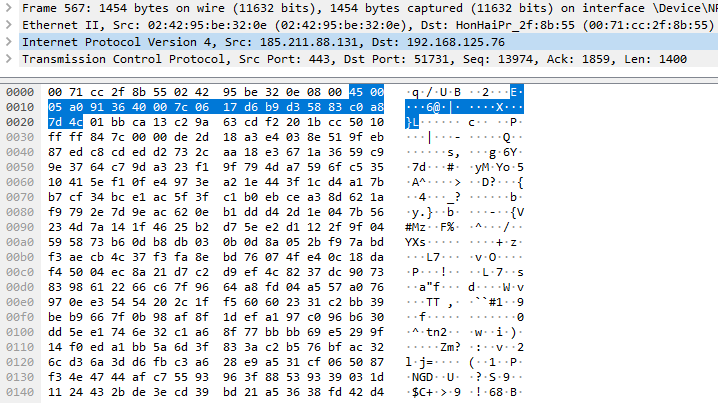
لایه اول(Data Link Layer): Ethernet II لایه دوم(Network Layer): IP version 4 لایه سوم(Transport Layer): TCP

بررسی ارتباط بین ترتیب قرار گیری بیت ها با لایه های مختلف:

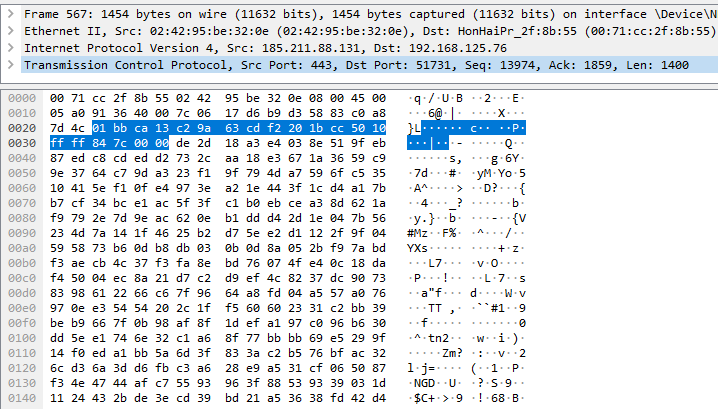
اگر روی هر یک از لایه ها در نرم افزار Wireshark کلیک کنیم، بیت های مربوط به آن لایه در بسته را با رنگ آبی highlight می کند. با انجام این کار متوجه می شویم که ابتدا بیت های مربوط به لایه اول، سپس بیت های مربوط به لایه دوم و در آخر بیت های مربوط به لایه سوم در بسته قرار گرفته اند. یعنی بیت های لایه های بالاتر، در آدرس های پایین تر در بسته قرار دارند(توجه به نمایش Hex بسته). در شکل های زیر این موضوع را نمایش داده ایم:



شکل (2) بیت های مربوط به لایه اول (Ethernet II)

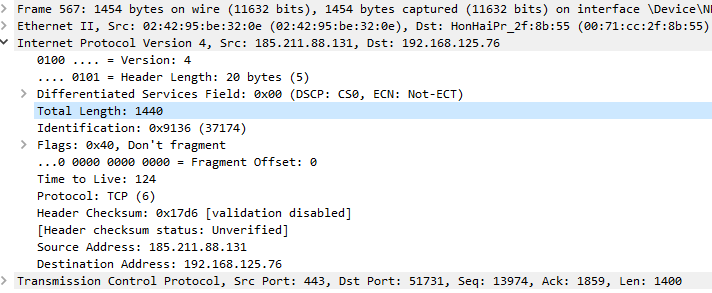


شکل (3) بیت های مربوط به لایه دوم (IP version 4)



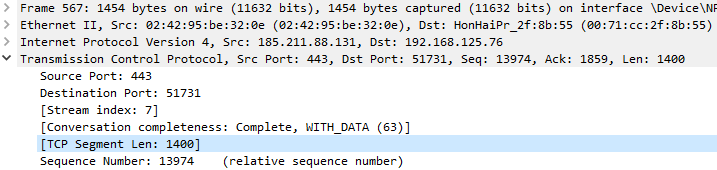
شکل (4) بیت های مربوط به لایه سوم (TCP)

اندازه فریم لایه دوم این بسته: 1440 بایت



شکل (5) اندازه فریم لایه دوم (Total Length)

اندازه بسته لایه سوم: 1400 بایت



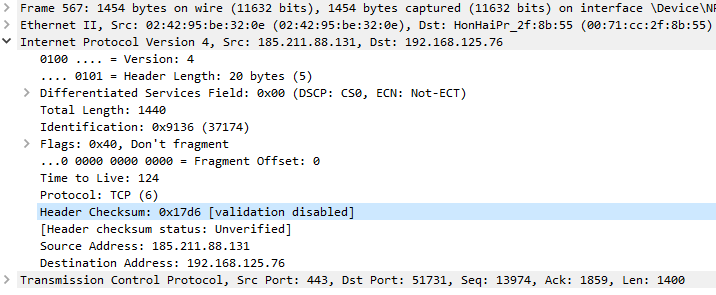
شکل (6) اندازه بسته لایه سوم (TCP Segment Len)

سوال 3: آیا می توانید بسته هایی را پیدا کنید که بدون پروتکل های لایه های Application, Transport, Network باشند؟ این بسته ها از چه پروتکلی استفاده کرده اند؟

بله، از پروتکل ARP استفاده کرده اند.

سوال 4: از یکی از بسته ها بخش مربوط به پروتکل Internet Protocol(IP) را پیدا کنید. Checksum پروتکل IP را پیدا کنید و یادداشت کنید.

Checksum پروتکل IP برای بسته شماره 567: 0x17d6



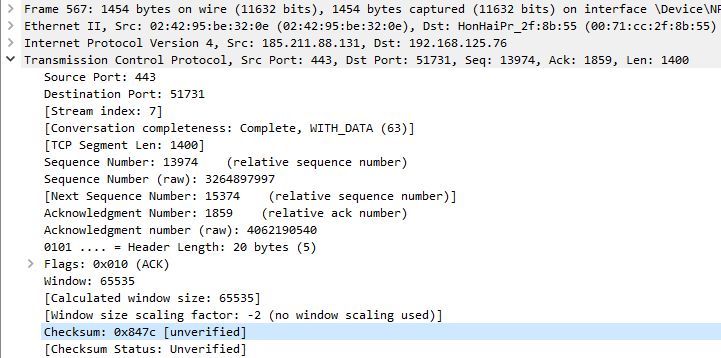
شکل (8) Checksum پروتکل IP بسته شماره 567

سوال 5: از یکی از بسته ها بخش مربوط به پروتکل Transport Control Protocol(TCP) و یا User Datagram Protocol(UDP) را پیدا کنید. عدد مربوط به port مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص می کند؟ Checksum مربوط به پروتکل های TCP و UDP را مشخص کنید.

Checksum پروتکل TCP برای بسته شماره 567: 0x847c

Port مبدا: 443 Port مقصد: 51713

برای آنکه به صورت یکتا بتوانیم ارتباط بین مبدا و مقصد را برقرار کنیم، علاوه بر آدرس IP نیاز به port مبدا و مقصد نیز داریم، زیرا ممکن است یک مبدا بیش از یک ارتباط(connection) با مقصد داشته باشد و این تمایز بین ارتباط ها با شماره های port مختلف در مبدا برطرف می شود و همچنین همین روند در مقصد هم ممکن است اتفاق بیفتد. پس با (Src IP, Src Port, Dst IP, Dst Port) میتوان به صورت یکتا ارتباط ها را مشخص کرد.

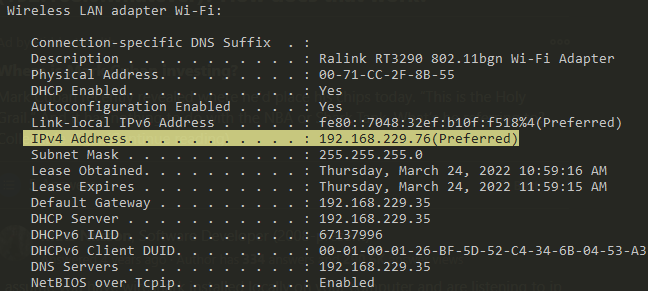


شکل (9) پروتکل TCP برای بسته شماره 567

سوال 6: یکی از بسته ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟ آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

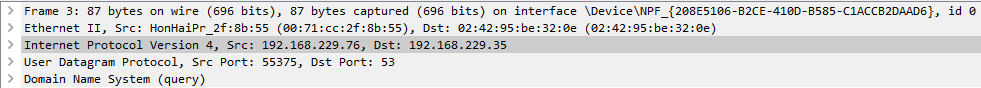
ابتدا ip کامپیوتر خودمان را بدست می آوریم و بسته هایی که ip مبدا آنها برابر با ip کامپیوتر ما باشند، یعنی از سیستم ما ارسال شده اند.

IPv4 Address = 192.168.229.76



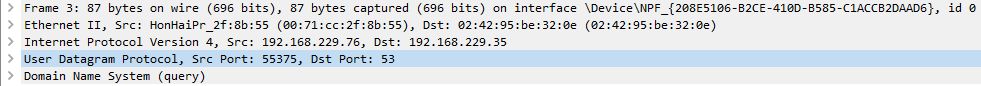
شکل (10) بدست آوردن ip سیستم با دستور ipconfig /all

بسته شماره 3 را که ip مبدا آن 192.168.229.76 است انتخاب می کنیم.



شکل (11) بسته شماره 3 با ip مبدا 192.168.229.76

پروتکل لایه Transport: UDP



Transport Layer (layer 3)

Network Layer (layer 2)

Data Link Layer (layer 1)

شکل (12) پروتکل لایه های مختلف بسته ای با پروتکل DNS

آدرس ip مقصد: 192.168.229.35 (در شکل (11) قابل مشاهده است)

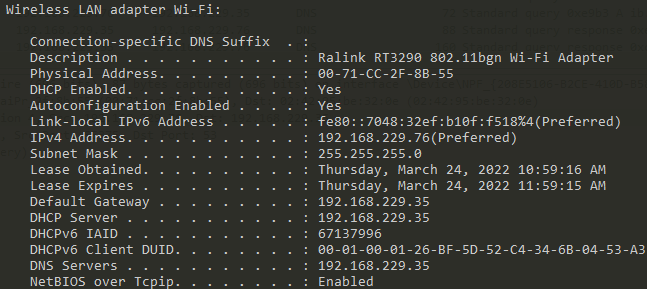
سوال 7: کدام یک از آدرس های پیدا کرده در بخش قبل را می توانید در خروجی دستور ipconfig /all مشاهده کنید؟

آی پی 192.168.229.76 مربوط به سیستم ما می باشد.

آی پی 192.168.229.35 مربوط به مودم ما می باشد.

در واقع بسته های ارسالی از طرف سیستم ما برای مودم ارسال می شوند و مودم مابقی کار ها را می کند....

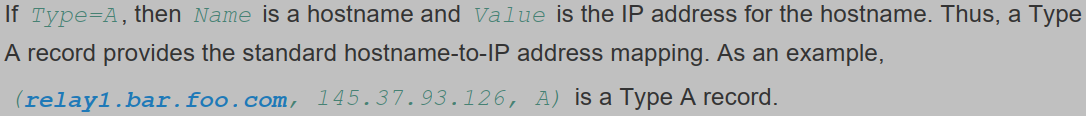
به شکل های (11) و (13) دقت شود.

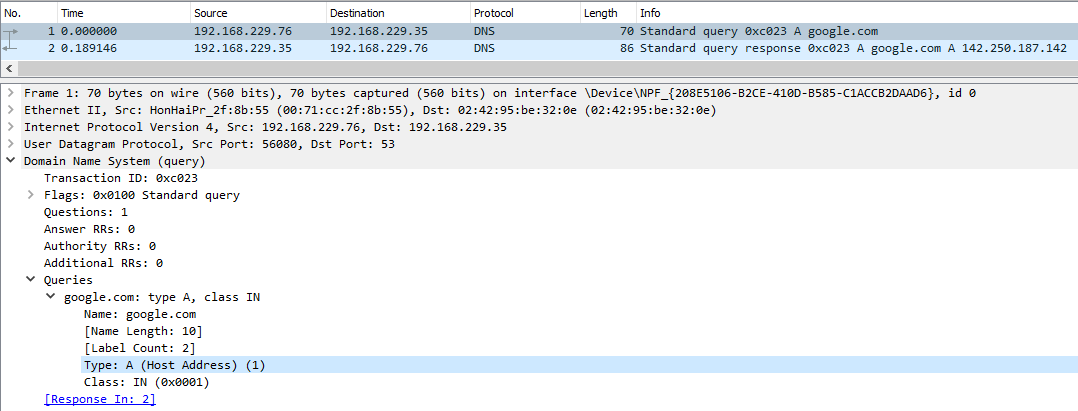


شکل (13) خروجی ipconfig /all

سوال 8: یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

تایپ A انتخاب شده است. تایپ A به منظور نگاشت hostname به ip address استفاده می شود.



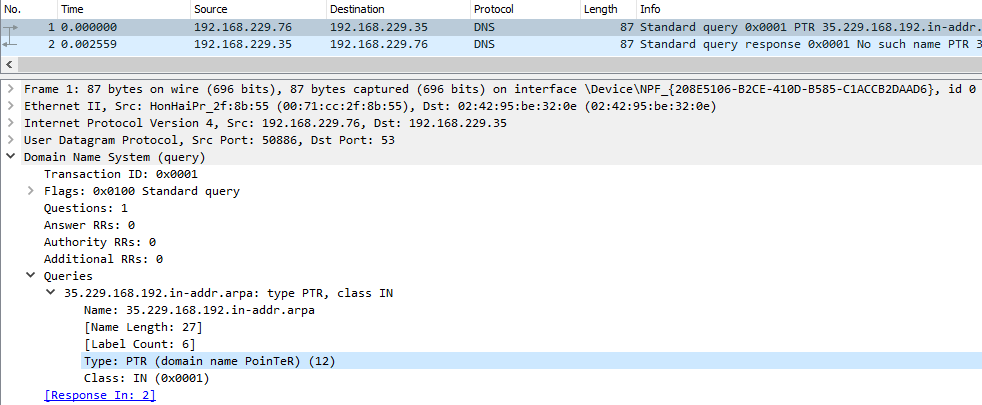


hostname

شکل (14) type بخش Queries برای دستور ping

سوال 9: یک بسته مربوط به دستور nslookup را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

تایپ PTR است. دقیقا بر خلاف تایپ A است و hostname متناسب با ip address را بر میگرداند یعنی در واقع نگاشت ip address به hostname را انجام میدهد.



ip address

شکل (15) type بخش Queries برای دستور nslookup

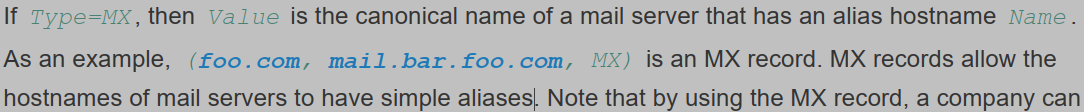
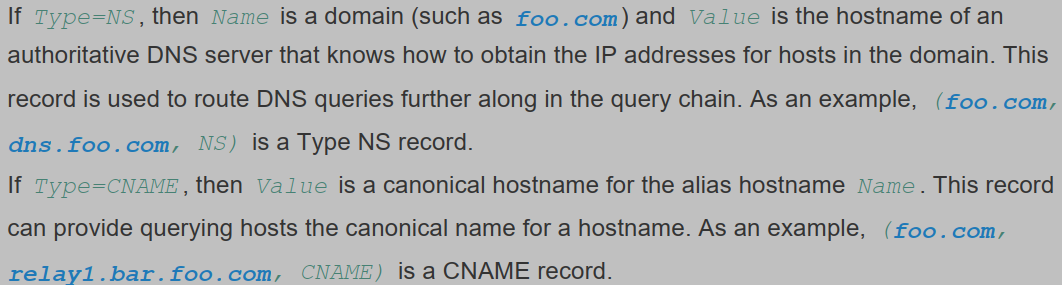
سوال 10: به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

NS: فیلد Name در آن یک domain است و فیلد Value در آن hostname مربوط به یک DNS server است که میداند چگونه ip address مربوط به host را در domain بدست آورد. این تایپ به منظور مسیر یابی DNS query ها در زنجیره query ها استفاده می شود.

CNAME: فیلد Name در آن یک نام مستعار (alias hostname) است و فیلد Value در آن یک نام رسمی (canonical hostname) است. این تایپ میتواند نام رسمی یک نام مستعار را بدست آورد.

MX: فیلد Name در آن یک نام مستعار (alias hostname) است و فیلد Value در آن یک نام رسمی (canonical name) مربوط به mail server است. این تایپ به hostname یک mail server اجازه میدهد تا یک نام مستعار برای خود داشته باشد.

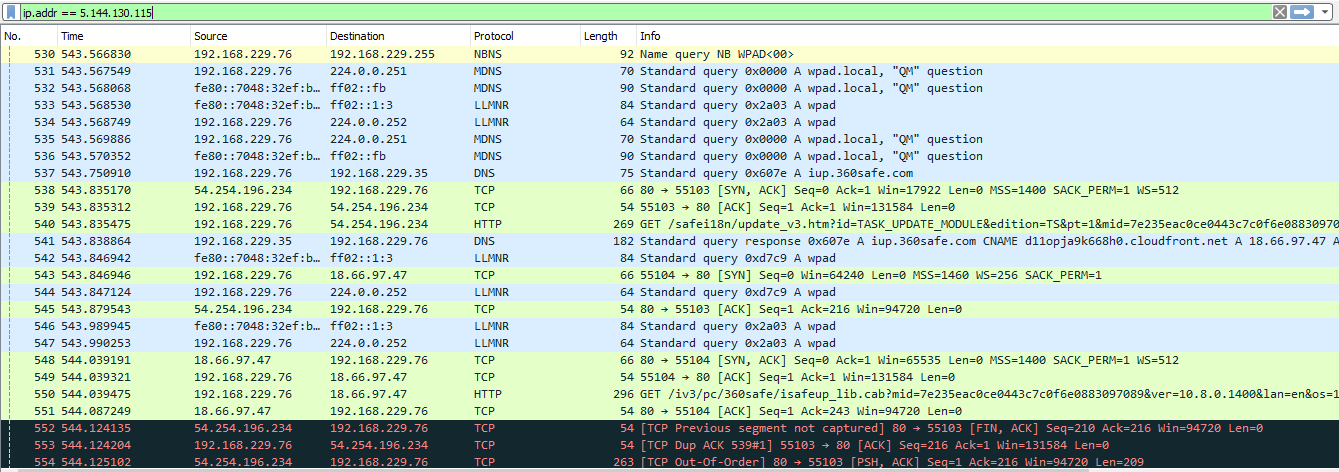
اطلاعات تکمیلی:



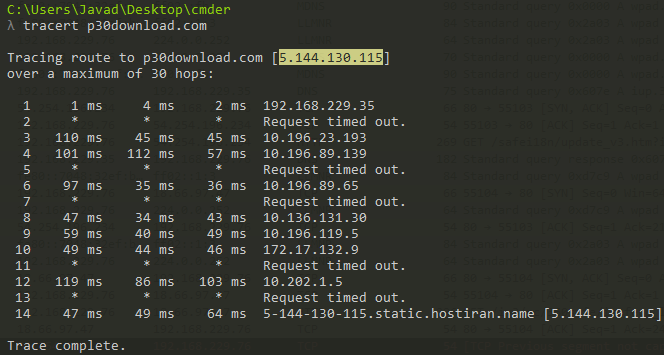
سوال 11: بعد از کلیک کردن بر روی OK چه اتفاقی می افتد؟ در بسته هایی که مشخص شده اند چه پروتکل هایی را مشاهده می کنید؟

تمامی بسته هایی که مبدا یا مقصد آنها ip مربوط به p30download.com (یعنی 5.144.130.115) باشد را نشان می دهد، زیرا فیلتر ip.addr همانطور که در توضیحات جلوی آن نوشته است ip های با مبدا و مقصد را بررسی میکند طبق عملگری که روی آن میگذاریم.

پروتکل ها: SSDP, TCP, ARP, TLSv1.2, MDNS, LLMNR, NBNS



شکل (16) بخشی از بسته های فیلتر شده ip.addr == 5.144.130.115

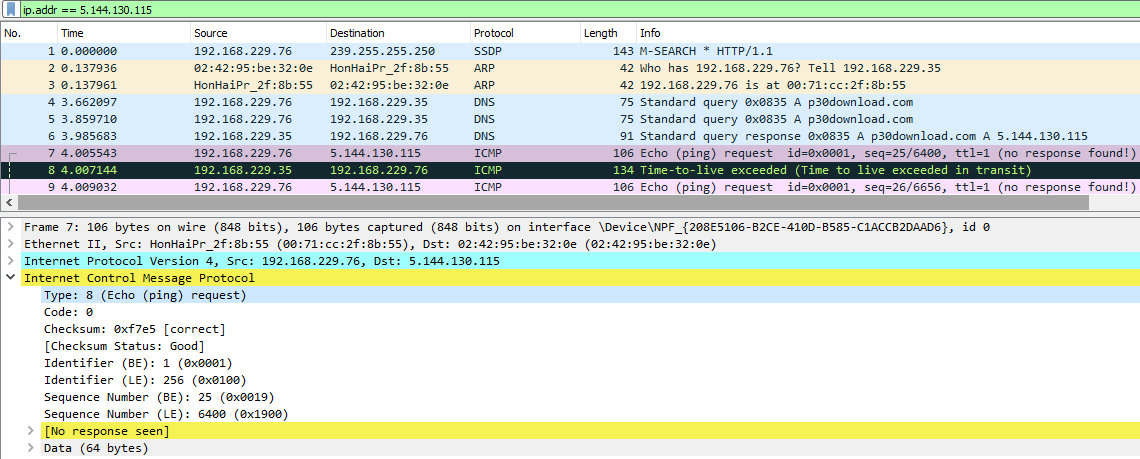


شکل (17) tracert p30download.com و بدست آوردن ip آن

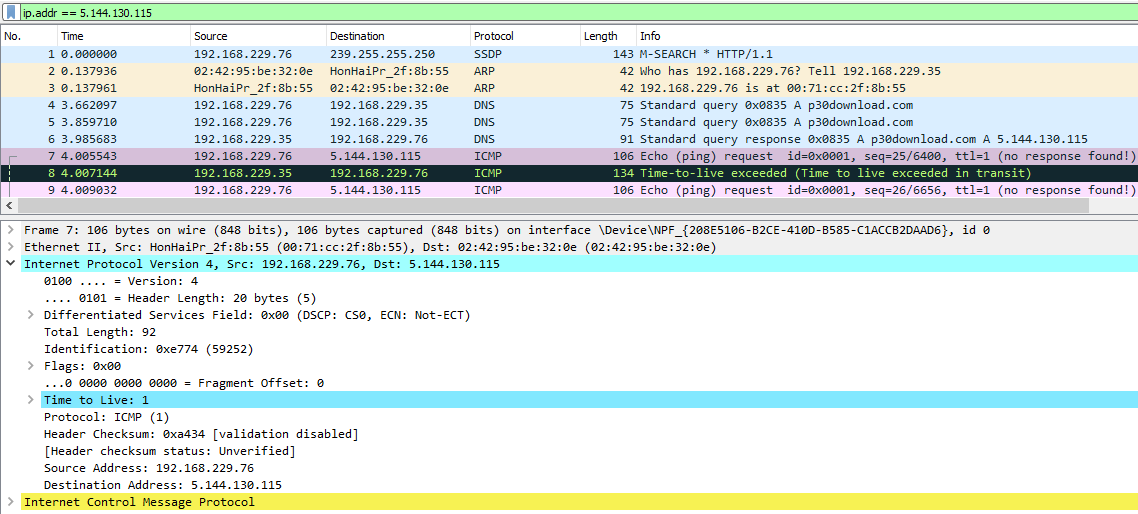
سوال 12: اولین بسته را انتخاب کنید. به بخش پروتکل Internet Control Message Protocol بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

مقدار type بخش ICMP برابر با 8 (Echo (ping) request) است ]شکل (18)[

مقدار TTL هم در بخش پروتکل IP برابر با 1 می باشد]شکل (19)[



شکل (18) مقدار type بخش پروتکل ICMP



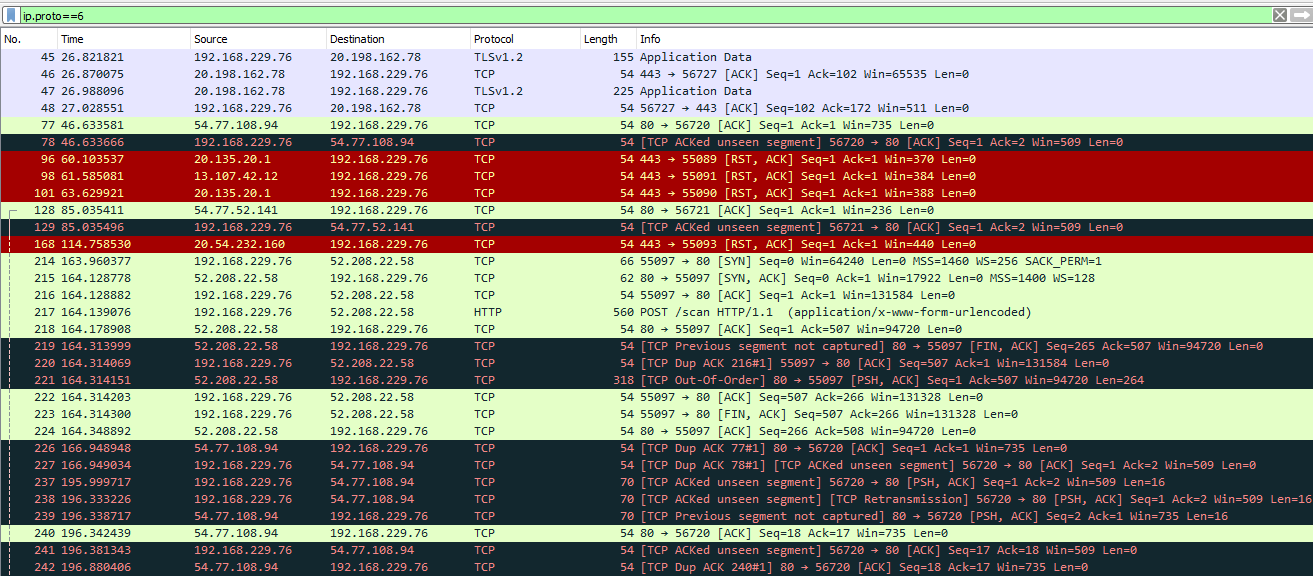
شکل (19) مقدار Time to live بخش پروتکل IP

سوال 13: به نظر شما هدف از تغییر این مقدار(TTL) چیست؟ می توانید با مراجعه به هدف دستور tracert آن را شرح دهید.

هر بسته در مسیری از مبدا به مقصد از میان دستگاه‌ های مختلفی عبور می کند که هر یک از آنها یک hop هستند. TTL ارتباط مستقیمی با تعداد گام‌ های مسیری که بسته از آن عبور می کند دارد. با عبور از هر hop، یک واحد از TTL بسته کاسته می ‌شود. هنگامی که یک بسته با مقدار hop صفر به دستگاهی می‌ رسد که مقصدش نیست، توسط آن دستگاه دور ریخته می ‌شود و یک پیغام خطای ICMP را برای میزبانی ارسال می‌ کند که اقدام به ارسال بسته کرده است. هنگامی که مقدار به صفر یا یک برسد و بسته به دستگاه مقصد رسیده باشد، پیغام Accept را برای میزبان ارسال می‌ کند. پس TTL مقدار زمانی است که بسته در شبکه اعتبار دارد. TTL همچنین به ارسال کننده بسته اجازه می دهد از تعداد گام ها در طول مسیر اطلاع پیدا کند، پس میتوان از TTL برای ارزیابی عملکرد شبکه استفاده کرد.

سوال 14: این فیلتر(ip.proto==6) چه کاری انجام می دهد؟

پروتکل شماره 6 همان TCP است و این فیلتر میگوید که بسته های با پروتکل TCP نمایش داده شود ]شکل (30)[.



شکل (20) فیلتر ip.proto==6

1. [Wireshark packet layers](https://linuxhint.com/wp-content/uploads/2020/08/e-fiverr-work-linuxhint_mail74838-book-linux-f-15.png) [↑](#footnote-ref-1)