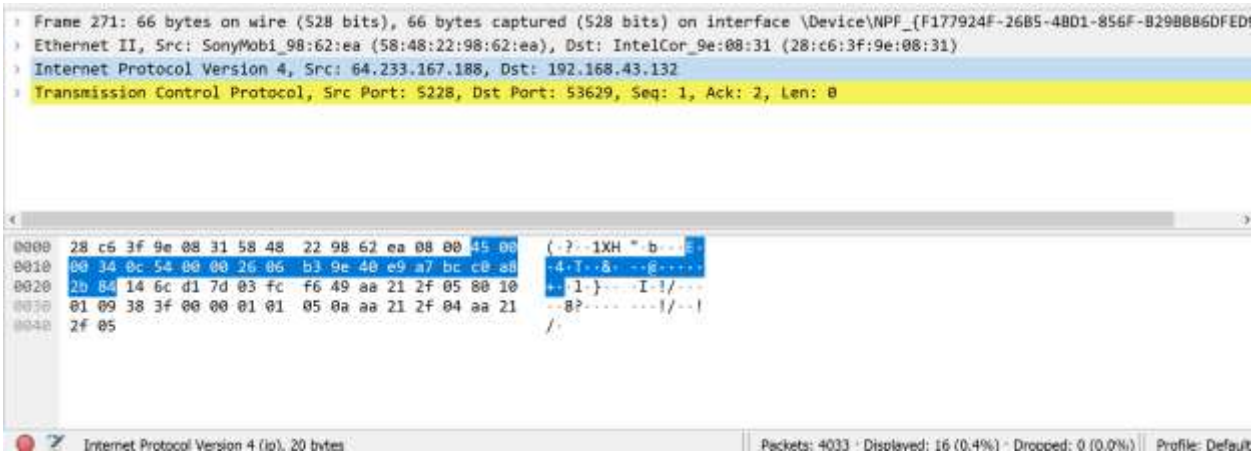
لایه‌بندی پروتکل‌ها

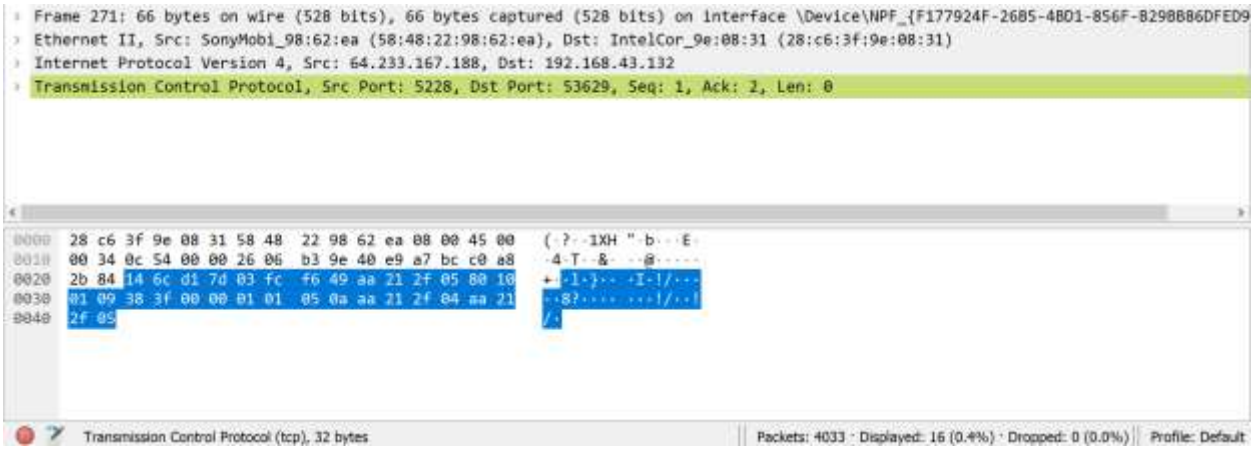
۱.به یک بخش دلخواه از بسته‌های شنودشده مراجعه کنید. چه پروتکل‌هایی را مشاهده می‌کنید؟ لیست آنها را یادداشت کنید.

پروتکل‌هایی همانند `TCP, TLSv1, TLSv1.2, TLSv1.3, SSL, QUIC, ARP, DNS`

۲.یک بسته را به دلخواه انتخاب کنید. مشخص کنید که چه پروتکل‌هایی در لایه‌های مختلف آن استفاده شده است. ترتیب قرارگیری بیت‌های داخل بسته چه ارتباطی با لایه-های مختلف دارد؟ اندازه‌ی فریم لایه‌ی دو این بسته چقدر است؟ اندازه بسته لایه سه چقدر است؟

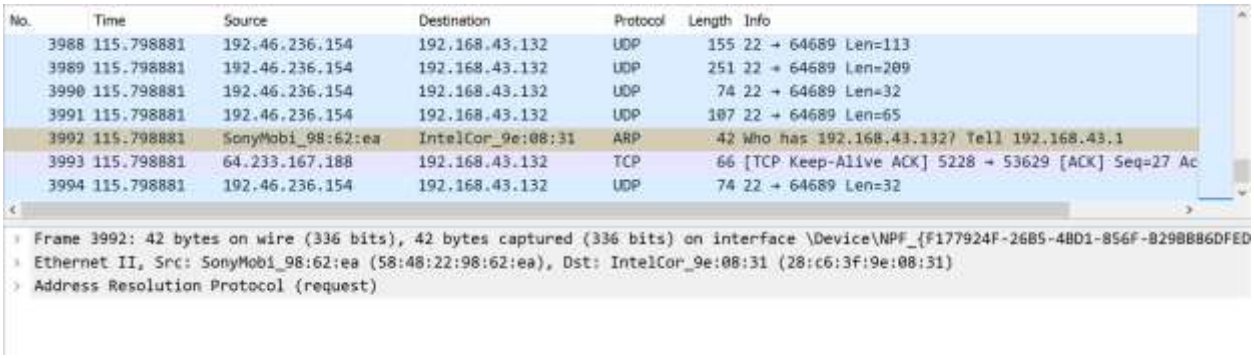
یک بسته‌ی با پروتکل `TCP` انتخاب می‌شود.
بسته‌ی انتخاب شده دارای سه لایه‌ی `Data link Layer, Network Layer` و `Transport Layer` است. بیت‌های بسته به ترتیب گفته شده در بالا از زیری‌ترین لایه به بالا اطلاعات مربوط به هر لایه را مشخص می‌کند (به ترتیب : اول لایه‌ی لینک، دوم لایه‌ی نت‌ورک و در نهایت لایه‌ی `Transport`). لایه‌ی دوم همان لایه‌ی `Network` است. اندازه‌ی این لایه طبق پیام ارسال‌شده، برابر با 20 بایت است(از بایت 14 تا 33). اندازه‌ی بسته‌ی لایه‌ی سوم برابر با 32 بایت است (از بایت 34 تا 65).





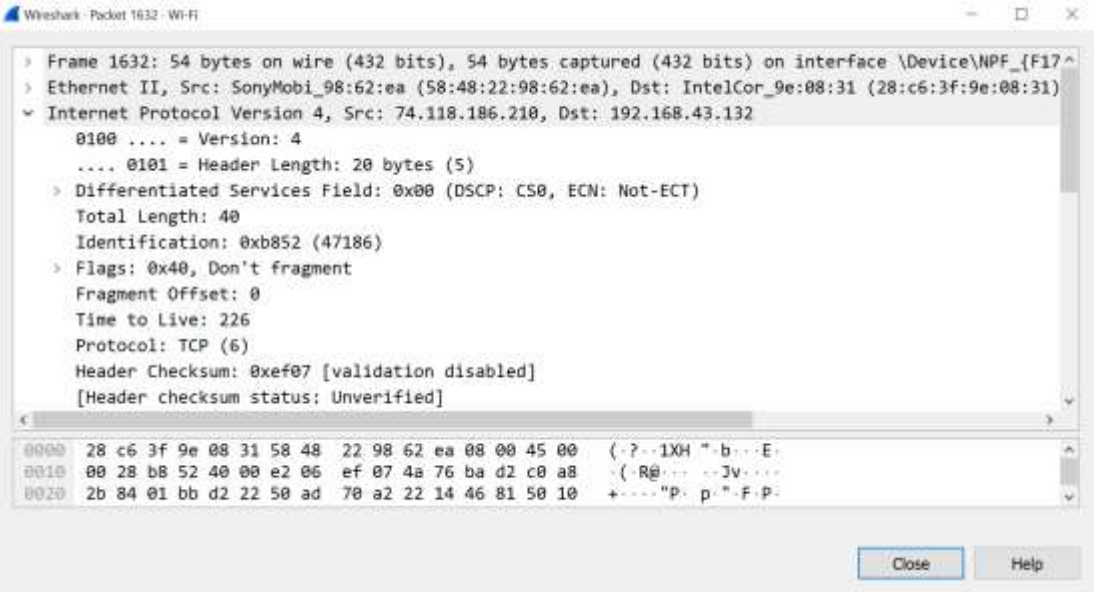
۳.آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Application, Transport, Network باشند؟ این بسته‌ها از چه پروتوکلی استفاده کرده‌اند؟

بسته‌ی مربوط به پروتکل ARP فاقد لایه‌های Network, Transport و Application است. این پروتکل برای یافتن آدرس لایه‌ی لینک (همانند Mac address) استفاده می‌شود.



۴.از یکی از بسته‌ها، بخش مربوط به پروتوکل Internet Protocol (IP) را پیدا کنید. Checksum پروتکل IP را پیدا کنید و آن را یادداشت کنید.

مقدار Checksum هدر پروتکل IP یکی از بسته‌ها برابر با 0xef07 است.



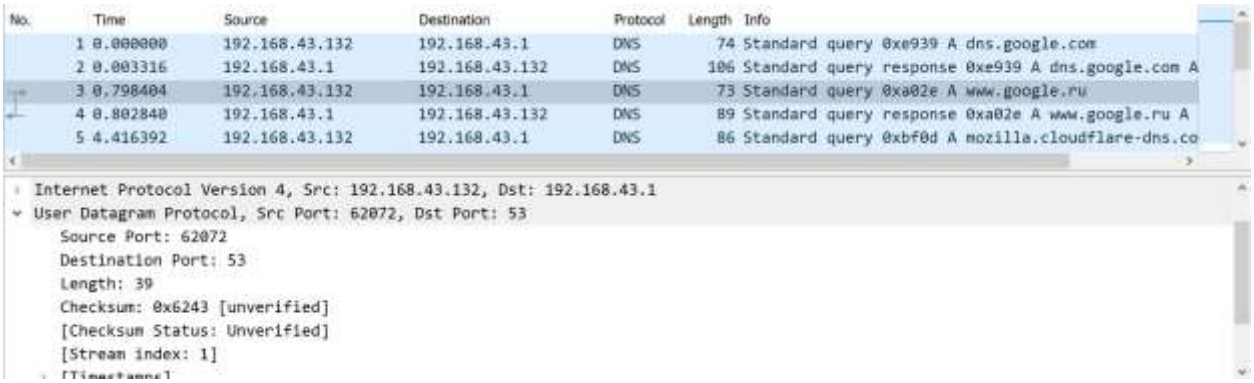
۵.از یکی از بسته‌ها بخش مربوط به پروتکل TCP یا UDP را پیدا کنید. عدد مربوط به پورت مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص می‌کند؟ Checksum مربوط به پروتکل‌های TCP و UDP را مشخص کنید.

پروتکل بسته‌ی مورد بحث UDP است.عدد پورت مبدا 64689 و عدد پورت مقصد 22 است. مقدار پورت در شبکه‌های کامپیوتری، نوع سرویس را نشان می‌دهند. برای مثال پورت 53 و پورت 80 به ترتیب برای سرویس‌های مربوط به DNS و HTTP مورد استفاده قرار می‌گیرند. مقدار Checksum مربوط به یکی از بسته‌های دارای پروتکل UDP برابر با 0xcbc5 و یکی از بسته‌های دارای پروتکل TCP برابر با 0xc53e است.

کار با فیلترکننده بسته

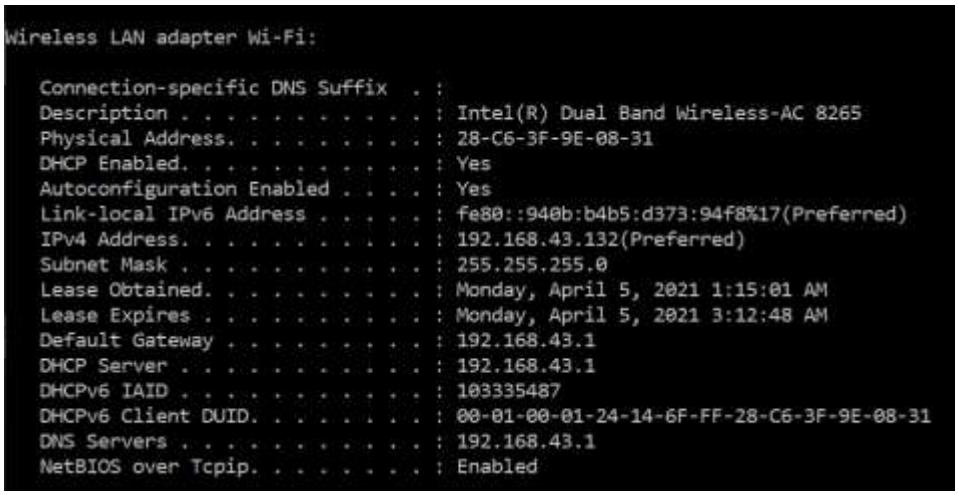
۶.یکی از بسته‌ها که از سیستم شما ارسال‌شده است را انتخاب کنید. پروتکل لایه‌ی Transport چیست؟ آدرس IP مقصد چیست؟ سرآیند لایه‌ی دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

پروتکل استفاده‌شده در لایه‌ی Transport، User Datagram Protocol (UDP) است. آدرس مقصد برابر با 192.168.43.1 است. (از هات‌اسپات برای اتصال به شبکه استفاده شده است.)



۷.کدام یک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستور ipconfig /all مشاهده کنید.

هر دوی مبدا و مقصد را می‌توان در خروجی مشاهده کرد.
آدرس مقصد به عنوان DNS Servers و آدرس مبدا به عنوان IPv4 Address آمده‌اند.



۸.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. از این تایپ برای پیدا کردن آدرس IP یک URL استفاده می‌شود. (طبق پروتکل DNS)

۹.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 انتخاب شده است. این تایپ دقیقا برعکس تایپ A عمل می‌کند و برای پیدا کردن Domain Name یک آدرس IP بکار برده می‌شود.

۱۰.به نظر شما چه `type` های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

طبق RFC 1035 تایپ‌هایی همانند NS, MD, MF, CNAME, SOA, MB, MG, MR, NULL, WKS, HINFO, MINFO, MX و TXT بغیر از دو مورد ذکرشده وجود دارند.

۱۱.بعد از کلیک کردن برروی OK چه اتفاقی می‌افتد؟ در بسته‌هایی که مشخص شده‌اند، چه پروتکل‌هایی را مشاهده می‌کنید؟

با کلیلک کردن، تنها بسته‌هایی که مبدا یا مقصد آنها برابر با آدرس p30download.com هستند، نشان داده می‌شوند. (آدرس p30download.com توسط tracert برابر با 5.144.130.115 بدست آمد.) پروتکل بسته‌ها ICMP است.

۱۲.اولین بسته را انتخاب کنید. به بخش پروتکل ICMP بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکلIP بروید و مقدار TTL را یادداشت کنید.

مقدار type برابر با (echo (ping) request 8 است. مقدار TTL در اولین بسته برابر با 1 است.

۱۳.به نظر شما هدف از تغییر مقدار TTL چیست؟ می‌توانید با مراجعه به هدف tracert آن را شرح دهید.

بدلیل اینکه از تجهیزات Packet Switch برای ارسال بسته‌ها استفاده می‌شود و مسیر هر بسته تا مقصد با بسته‌های دیگر متفاوت است، مقدار TTL متغیر است.

۱۴.فیلتر ip.proto == 6 چه کاری انجام می‌دهد؟

با استفاده از این فیلتر، تمامی بسته‌هایی که IP protocol آنها TCP است نمایش داده می‌شود.