

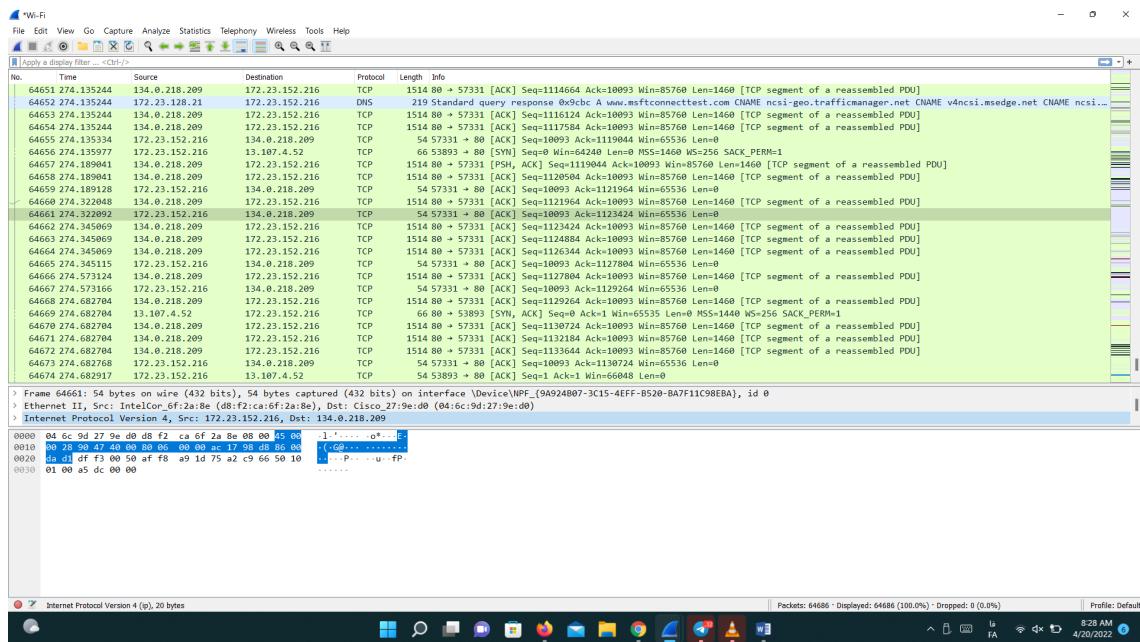
گزارش کار آزمایشگاه ۴ شبکه‌های کامپیووتری

تحلیل TCP با استفاده از Wireshark

شایان بالی ۱۴۰۶-هیلیاسادات هاشمی پور ۹۸۳۱۱

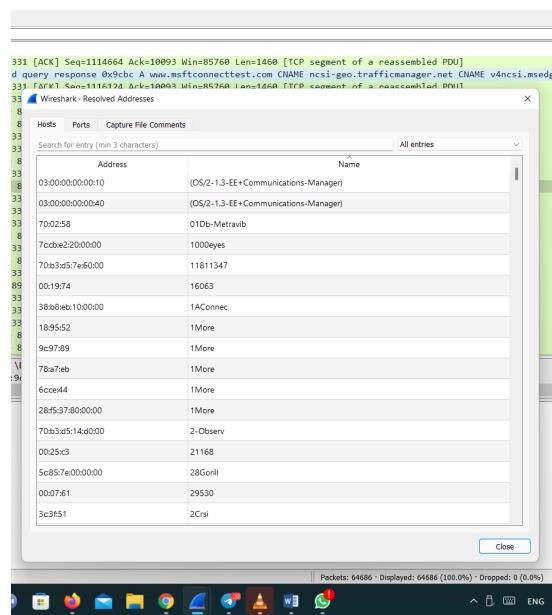
گروه ۴

بخش ۱: بر روی گزینه Resolved Addresses کلیک کنید.



سوال ۱: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

در این پنجره در بخش Hosts مشاهده می‌شود که تعداد آدرس با نام‌هایی لیست شده‌اند. در بخش Ports هم برای پورت‌های مختلف پروتکل‌ها اسم‌هایی نوشته شده است. در سربرگ آخر هم یک سری کامنت وجود دارد.



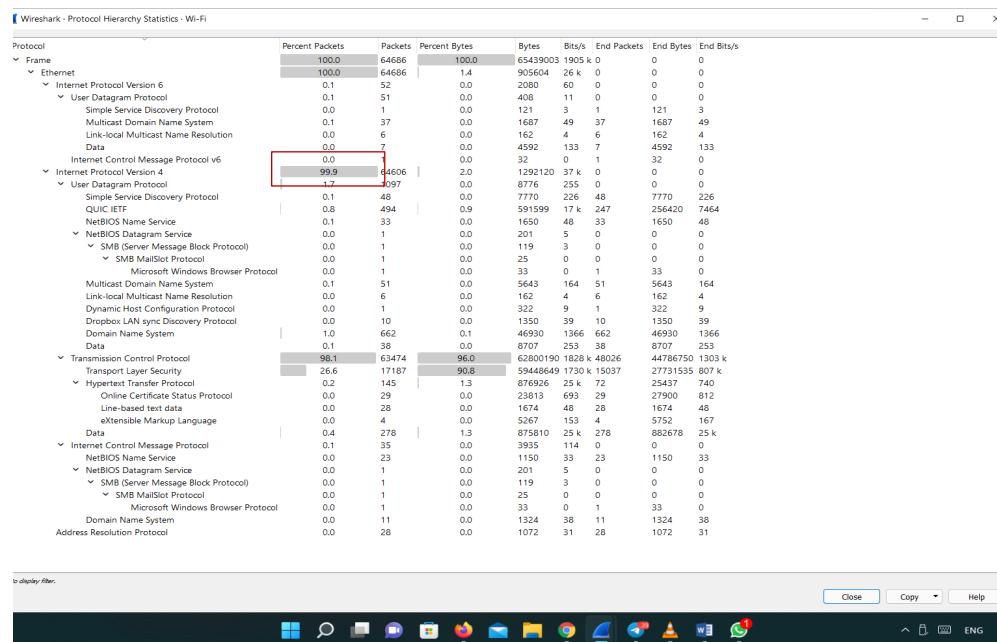
سوال ۲: آیا می توانید سه بایت اولی که برای آدرس فیزیکی کارت های شبکه Cisco می باشد را مشخص کنید؟

بله می شود - طبق اسکرین شات زیر: (سه بایت اول آن به صورت زیر است)

| Resolved Addresses | |
|---|--------------------------|
| Hosts | Ports |
| Search for entry (min 3 characters) | All entries |
| Address | Name |
| fcd2:b6:60:00:00:00 | CirqueAu |
| 3:a:ba:37 | Cirrent |
| 8c:1f:64:8c:20:00 | Cirrus |
| 00:50:c2:91:70:00 | Cirtem |
| 00:60:09 | Cisco |
| 00:10:79 | Cisco |
| 00:90:f2 | Cisco |
| 00:60:70 | Cisco |
| 00:90:2b | Cisco |
| 00:60:3e | Cisco |
| 00:07:0d | Cisco |
| 00:0c:0c:0c:0c:0c | Cisco-ACI-Gleaning-Leaf |
| 00:0d:0d:0d:0d:0d | Cisco-ACI-Gleaning-Spine |
| 04:6c:9d:27:9e:d0 | Cisco_27:9e:d0 |
| 2:cd:1:41:e:0:0:0:0:0 | CitaSmar |
| 00:10:01 | Citel |
| 00:a:0:20 | Citicorp/Tti |

۲- بر روی گزینه‌ی protocol hierarchy کلیک کنید.
سوال ۳: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

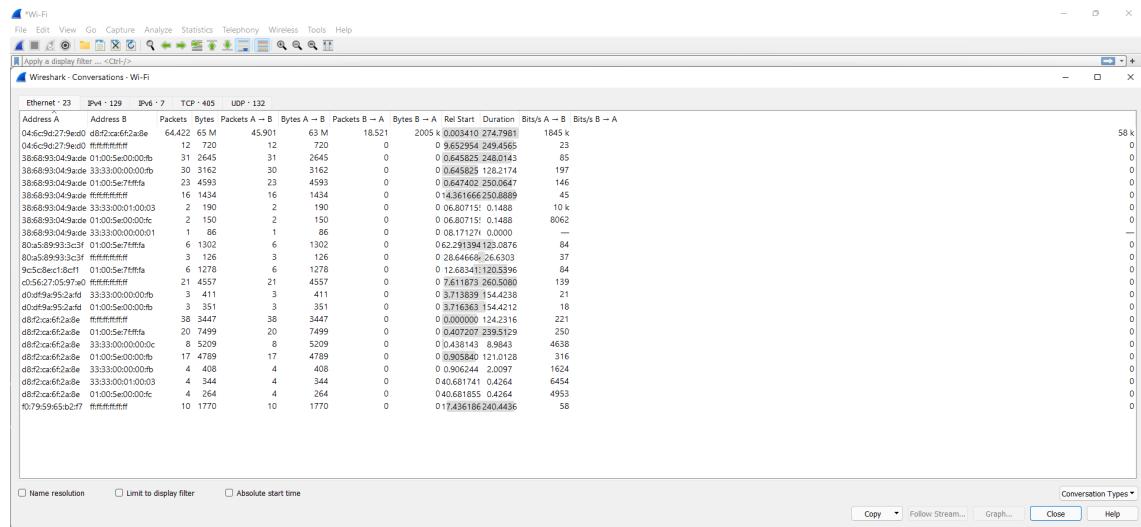
مشاهده می‌شود که تمام اطلاعات مربوط به لایه‌های مختلف طی یک آمارگیری لیست شده‌اند به طوریکه می‌توان متوجه می‌شود که در شنودهایمان چقدر یا چند درصد از هر پروتکلی هست. در اصل یک آماری از کل بسته‌های دریافتی و شبکه به ما می‌دهد و بعدا در تصمیم گیری‌ها می‌توان به این آمار مراجعه کرد.



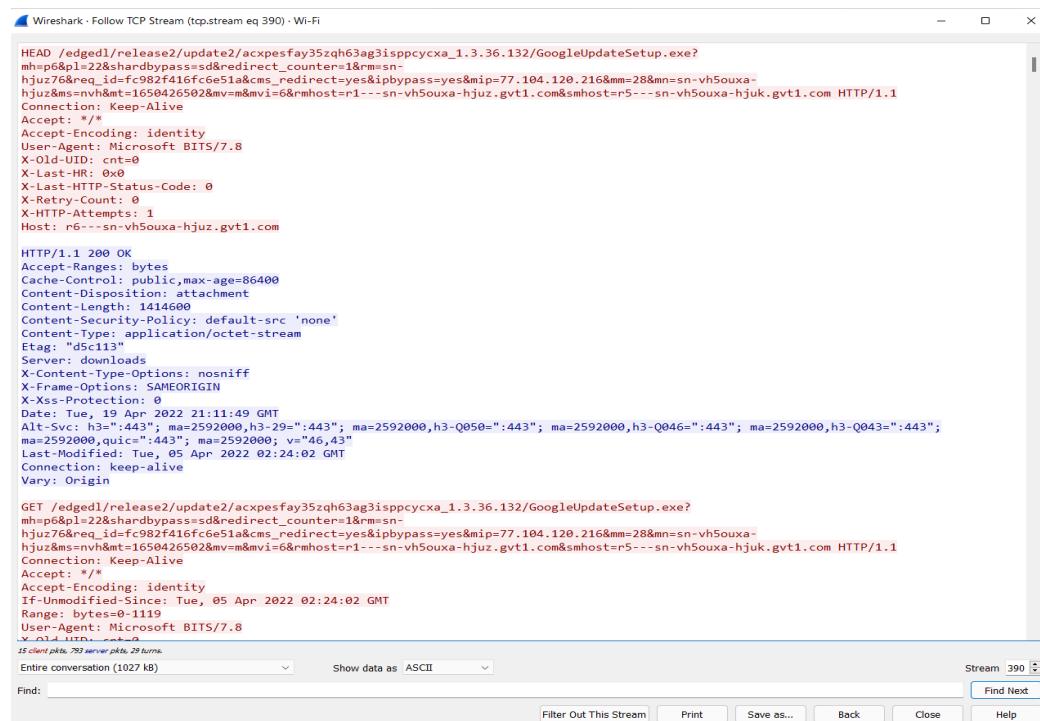
سوال ۴: چند درصد بسته‌های شما به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند؟
درصد ۹۹.۹

بخش ۳: بر روی گزینه Conversations کلیک کنید.
سوال ۵: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

مشاهده می‌شود که conversations های مختلفی در سربرگ‌های لیست شده‌اند و به ترتیب layer آن‌ها را دسته بندی کرده است. در اصل اطلاعات آماری conversations دو نقطه مبدأ و مقصد را به ما نشان می‌دهد. در واقع حالت‌های مختلفی برای نمایش مکالمه وجود دارد که در رفت انجام شده است یا برگشت را یا هر دو را با هم نشان می‌دهد.

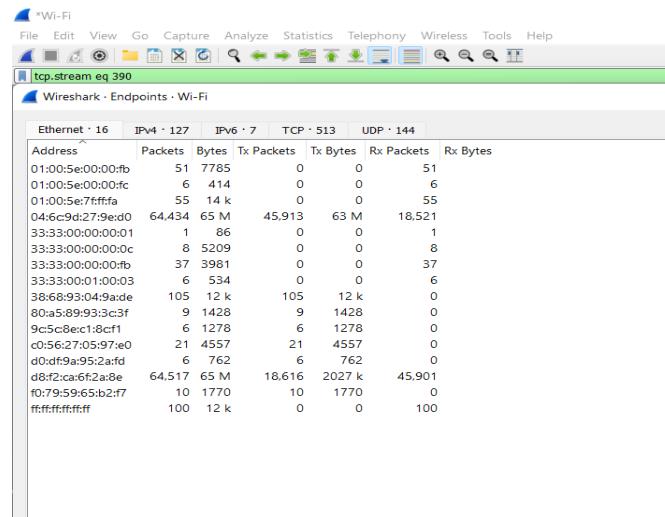


یک نشست TCP را مشخص کنید. (برای مشخص کردن یک نشست TCP نیاز است که آدرس و پورت مبدأ و مقصد را مشخص کنید). توجه داشته باشید مفهومی که از نشست برداشت می‌کند با مفهومی که در کلاس آموخته‌اید تفاوت دارد.



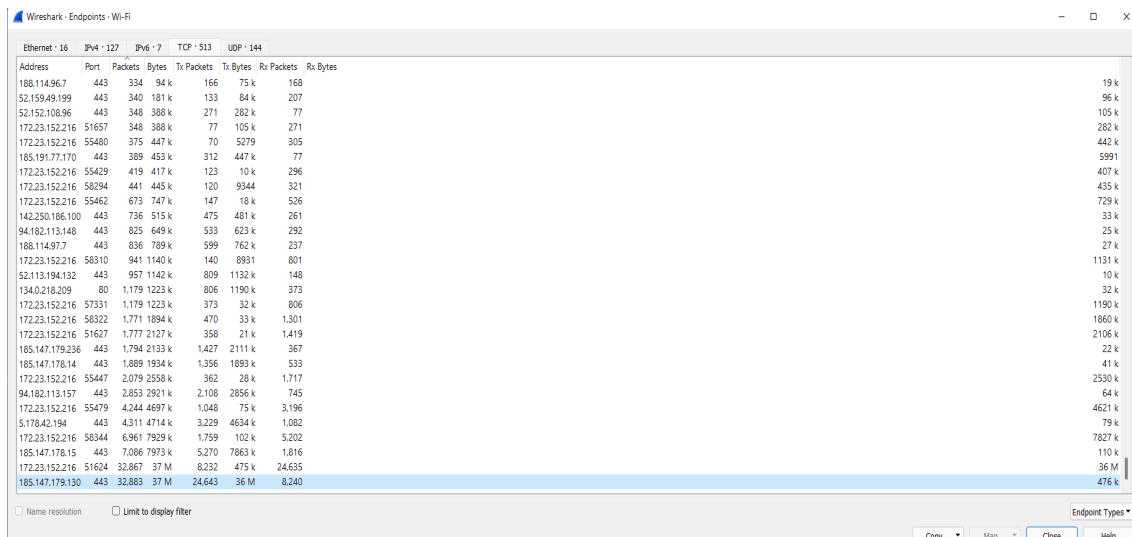
بخش ۴: بر روی گزینه endpoints کلیک کنید.
سوال ۶: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

لیستی از end point‌ها یعنی مبدأ و مقصد ارتباطات مختلف با توجه به پروتکل‌های انتخاب شده لیست شده‌اند.



سوال ۷: چه مقصد هایی برای ارتباط های TCP در سیستم شما استفاده شده اند؟

در تب طبق شکل زیر حاصل می شود. همانطور که می بینیم مقصد های زیادی برای ارتباط های TCP استفاده شده است.



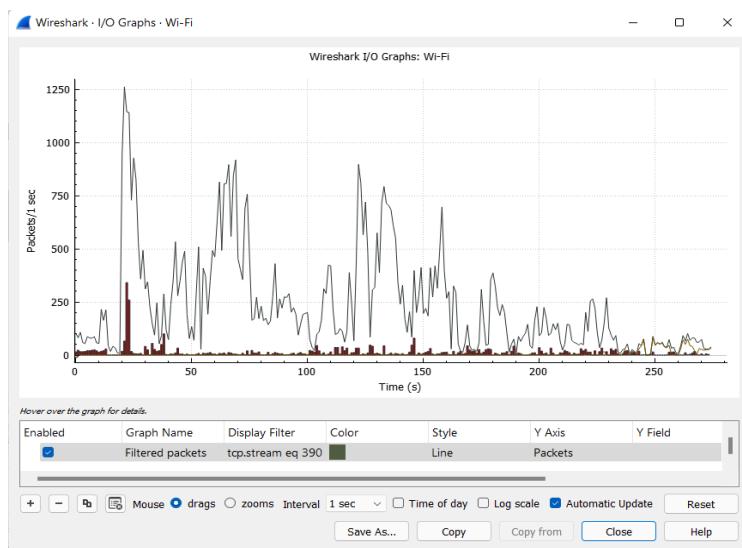
سوال ۸: آیا می توانید از زبانه Default و از روی تعداد بسته های مبادله شده، Gateway شبکه خود را تشخیص دهید؟

حال در این زبانه براساس تعداد بسته ها سورت می کنیم.

| Ethernet - 16 | IPv4 - 127 | IPv6 - 7 | TCP - 513 | UDP - 144 | | |
|--------------------|------------|----------|------------|-----------|------------|----------|
| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
| 33:33:00:00:00:01 | 1 | 86 | 0 | 0 | 1 | |
| 0:0:0:5e:0:0:00:08 | 6 | 414 | 0 | 0 | 6 | |
| 33:33:00:01:00:03 | 6 | 534 | 0 | 0 | 6 | |
| 9:c5:8e:c1:8cf1 | 6 | 1278 | 6 | 1278 | 0 | |
| d:0:d9:94:95:2a:fd | 6 | 762 | 6 | 762 | 0 | |
| 33:33:00:00:00:0c | 8 | 5209 | 0 | 0 | 8 | |
| 80:a5:89:93:c3:f3 | 9 | 1428 | 9 | 1428 | 0 | |
| f:7:95:95:65:2c:f7 | 10 | 1770 | 10 | 1770 | 0 | |
| c:0:56:27:05:97:a0 | 21 | 4557 | 21 | 4557 | 0 | |
| 33:33:00:00:00:04 | 37 | 3981 | 0 | 0 | 37 | |
| 0:1:0:0:5e:0:0:fb | 51 | 7785 | 0 | 0 | 51 | |
| 0:1:0:0:5e:7:ff:ff | 55 | 14 k | 0 | 0 | 55 | |
| #ffff#ffff#ffff# | 100 | 12 k | 0 | 0 | 100 | |
| 3:6:6:9:04:9:a0e | 105 | 12 k | 105 | 12 k | 0 | |
| 0:4:6:c9:27:9e:d0 | 64,434 | 65 M | 45,913 | 63 M | 18,521 | |
| d:8:2:a:f6:2:a:ea | 64,517 | 65 M | 18,616 | 2027 k | 45,901 | |
| d:8:2:a:f6:2:a:ea | 64,517 | 65 M | | | | 63 M |

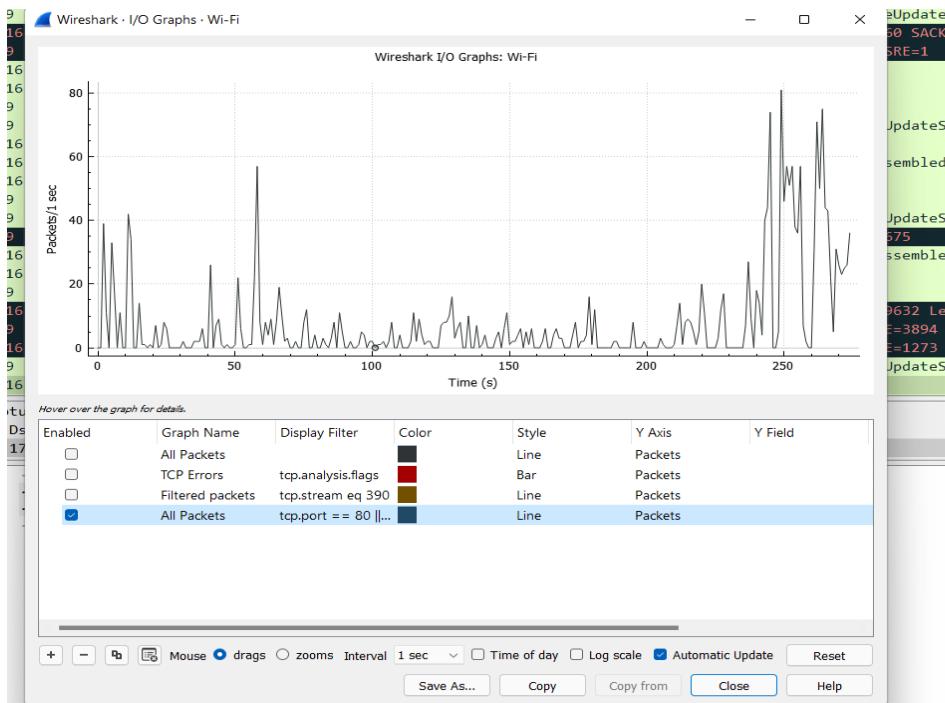
همانطور که می بینیم آخرین سطر مربوط به بیشترین تعداد بسته های مبادله شده می باشد. (که نشان دهنده آدرس فیزیکی سیستم ما است زیرا بیشترین تعداد بسته ها از این طریق مبادله شده است) (البته به شکل دقیق درست نیست)

بخش ۵: بر روی گزینه‌ی Graph I/O کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید نرخ I/O را مشاهده کنید.

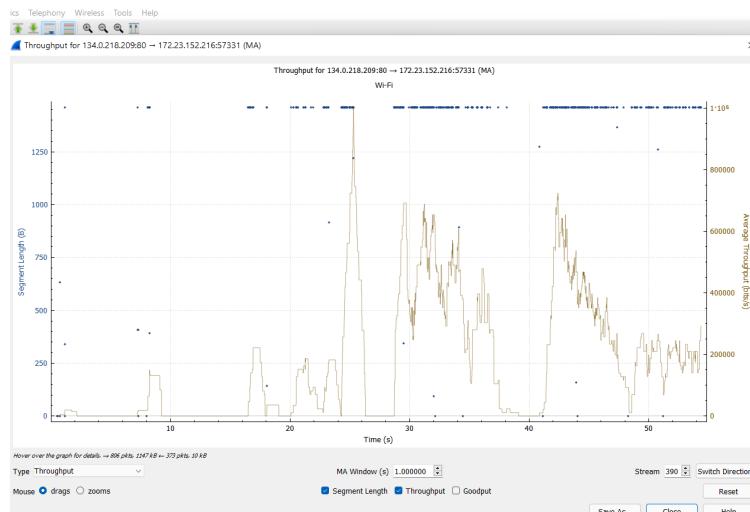


شما می‌توانید در این صفحه نمودارهای مختلفی بسازید. بر روی دکمه + در پایین پنجره باز شده کلیک کنید، سپس یک فیلتر به آن اضافه کنید تا نمودار تعداد بسته‌ها در ثانیه را مشاهده کنید. مشاهده می‌کنید که با کلیک بر روی نمودار، بسته‌ها در پنجره اصلی مشخص خواهد شد:

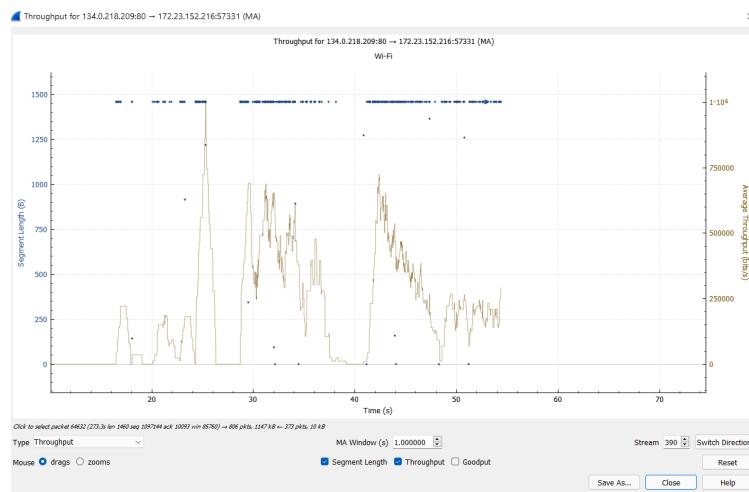
برای مثال `tcp.port==80` را اضافه می کنیم.



بر روی گزینه TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Throughput کلیک کنید.

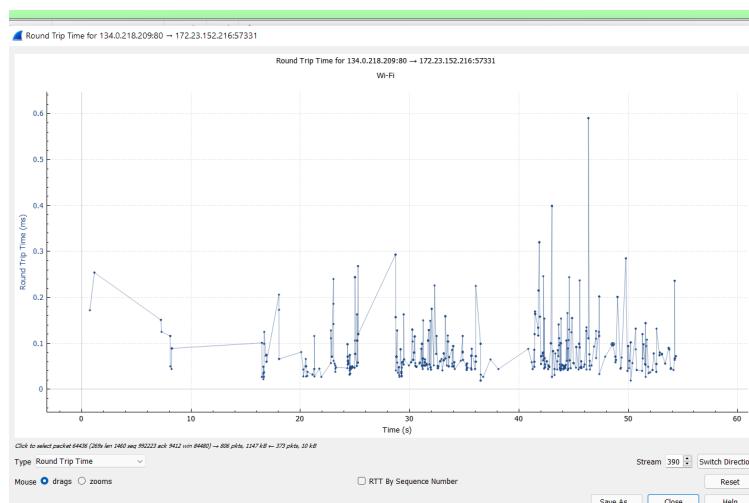


با گزینه Switch Direction می‌توانید ارتباط در جهت برعکس را بررسی کنید.

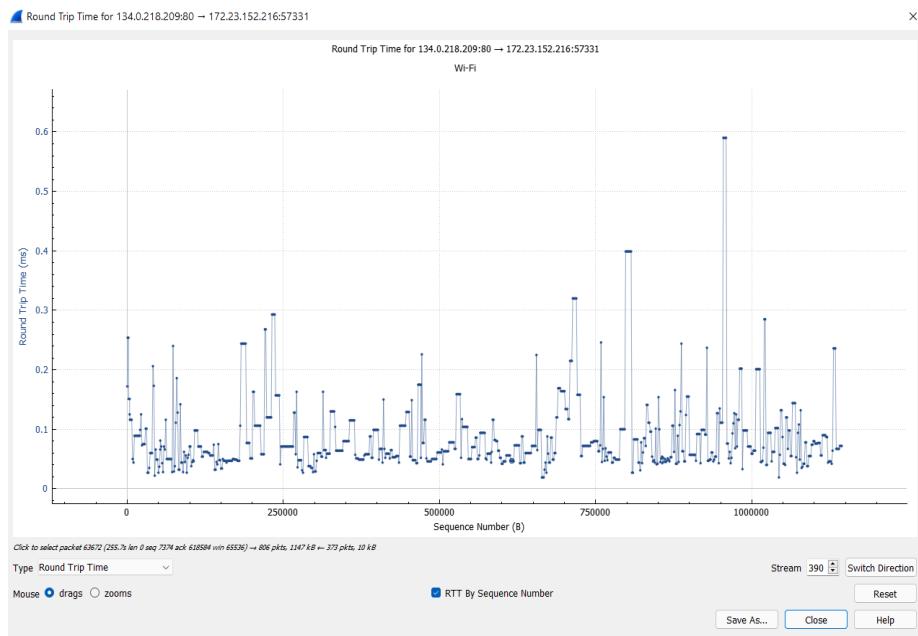


بر روی نمودار نقاط آبی رنگی قرار دارد، این نقاط طول segment های ارسال شده برحسب بایت در ارتباط TCP را در آن زمان نمایش می‌دهد. با افزایش شمارندهای که در پایین پنجره با نام Stream قرار دارد می‌توانید ارتباط TCP خود را عوض کنید. منظور از Goodput نرخی است که کاربرد داده خود را دریافت می‌کند و در آن Retransmission ها در نظر گرفته نمی‌شوند.

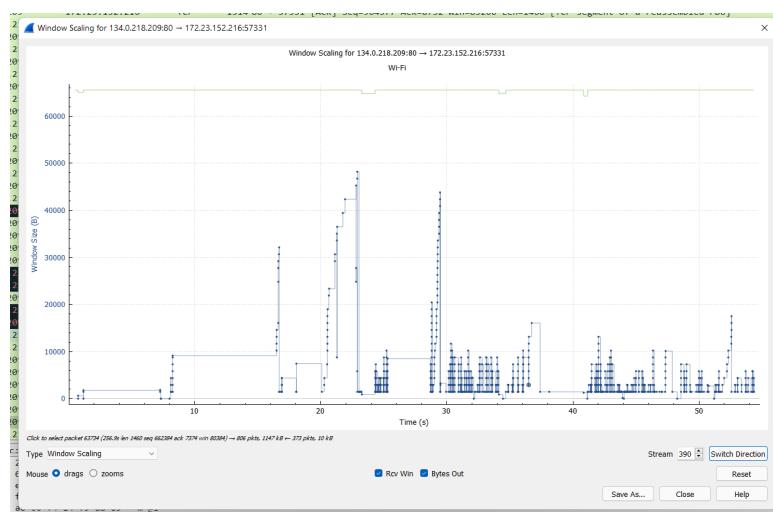
بر روی گزینه TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Round Trip Time کلیک کنید.



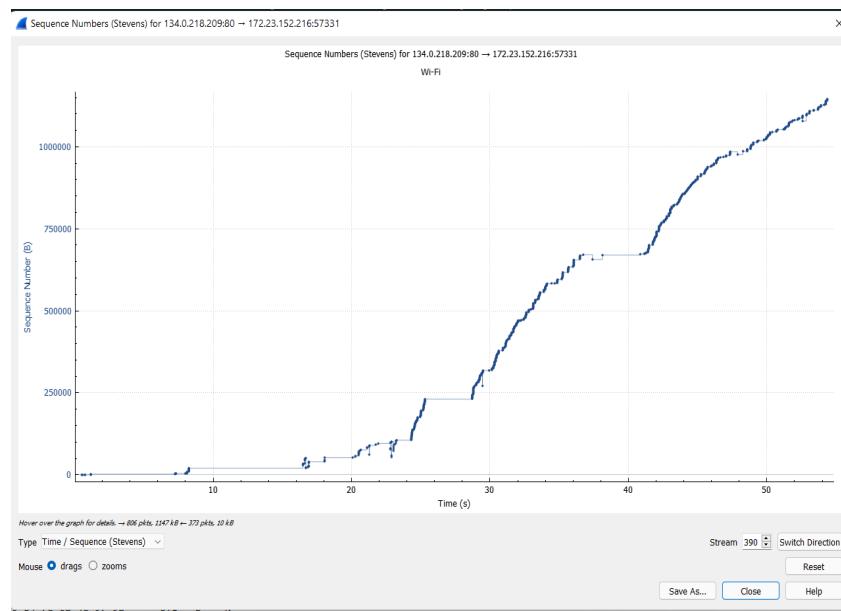
می‌توانید با انتخاب گزینه RTT By Sequence Number این نمودار را برحسب شماره‌ی بسته‌ها داشته باشید.



بر روی گزینه TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Window Scaling کلیک کنید.



بر روی گزینه TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Time / Sequence (Stevens) کلیک کنید.



سوال ۹: به سایت دانلود دانشگاه مراجعه کنید

<http://download.aut.ac.ir/>

به صورت همزمان دو فایل با لندازه بزرگ را دانلود کنید و در Wireshark بسته‌ها را به مدت یک دقیقه شنود کنید. به عنوان مثال می‌توانید دو نسخه ویندوز

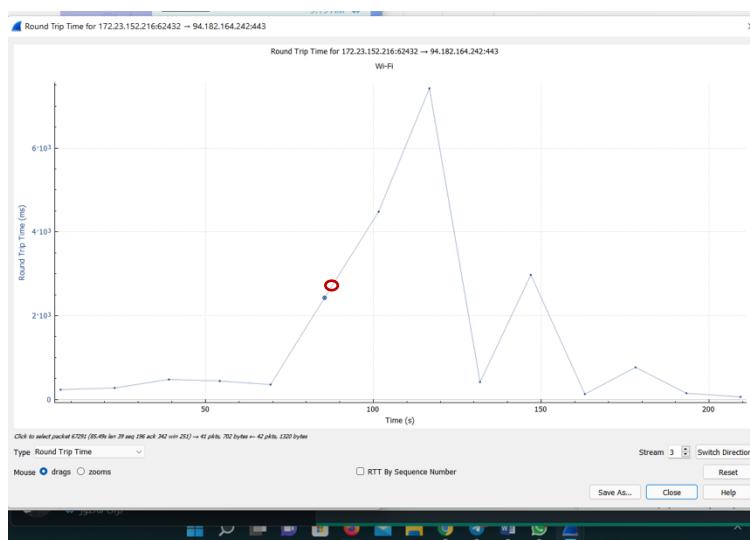
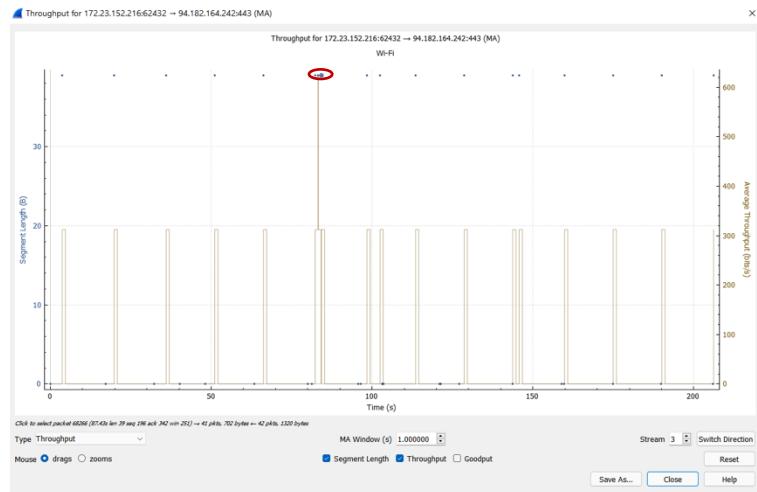
<http://download.aut.ac.ir/prg/Utility/7.iso>

<http://download.aut.ac.ir/prg/Utility/Windows.8.Enterprise.x64.iso>

را دانلود کنید. شرایط ازدحام در شبکه رخ می‌دهد. ابتدا از طریق Conversation آدرس IP سایت دانشگاه را مشخص کنید. سپس می‌توانید آن را به عنوان یک فیلتر اعمال کنید و نمودارهای Throughput و Windows scaling، RTT را بررسی کنید و مشخص کنید در شرایط ازدحام چه اتفاقی برای موارد بیان شده رخ می‌دهد. تغییرات را برای ده بسته قبل و بعد یک بسته دلخواه به صورت دقیق بررسی کنید.



در اینجا گذرهی به مaks رسیده است.



در اینجا RTT عدد کوچکی دارد که با حداکثر گذردگی مان
تناسب دارد. (اگر RTT پایین بیاید گذردگی باید افزایش
باید)