دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دستور کار آزمایشگاه شبکه‌های کامپیوتری

مسئول آزمایشگاه:
دکتر مسعود صبایی

بهار ۱۴۰۴

قوانین آزمایشگاه شبکه‌های کامپیوتری

برای افزایش کارایی درس آزمایشگاه شبکه‌های کامپیوتری، رعایت عدالت بین تمامی گروه‌های آزمایشگاهی و آموزش حداکثری مطالب درس به‌صورت عملی، مدرسین و دانشجویان ملزم به رعایت نکات و قوانین ذیل هستند:

۱. تعداد جلسات در طول نیمسال ۱۰ تا ۱۲ جلسه خواهد بود.
۲. مدرسین و دانشجویان موظف‌اند رأس ساعت مقرر در کلاس حضور یابند.
۳. قبل از انجام هر آزمایش، مبحث تئوری مربوط به آن آزمایش باید به‌طور کامل مطالعه شود، زیرا در حین جلسه وقت کافی برای توضیح و یادگیری مطالب تئوری وجود ندارد.
۴. پس از گذشت پنج دقیقه از شروع کلاس، به ازای هر پنج دقیقه تأخیر ۱۰ درصد نمره آن جلسه کسر می‌شود.
۵. حداکثر میزان تأخیر ۳۰ دقیقه است.
۶. هر آزمایش شامل یک پیش گزارش است که باید پیش از شروع آزمایش‌ها به مدرس تحویل داده شود. پیش گزارش مطلوب هر آزمایش در دستور کار آمده است.
۷. به ازای هر آزمایش، یک گزارش کار تهیه می‌شود که شامل تمامی مواردی است که در حین آزمایش با آن‌ها برخورد شده است. در این گزارش باید تمامی مشکلات پیش‌آمده و نحوه برطرف کردن آن‌ها ذکر گردد. همچنین، چگونگی انجام آزمایش مشتمل بر تحلیل آزمایش، به همراه اسکرین شات از مراحل انجام آزمایش‌ها تهیه شود.
۸. جهت کسب نمره قبولی در آزمایشگاه، کسب حداقل نمره قبولی در درس الزامی است.
۹. به‌منظور حفظ حرمت کلاس و نظافت آزمایشگاه، از خوردن و آشامیدن در طول کلاس خودداری نمایید.

فهرست آزمایش‌ها

۸- تحلیل ترافیک TCP و UDP با استفاده از Wireshark

۸-۱- هدف آزمایش:

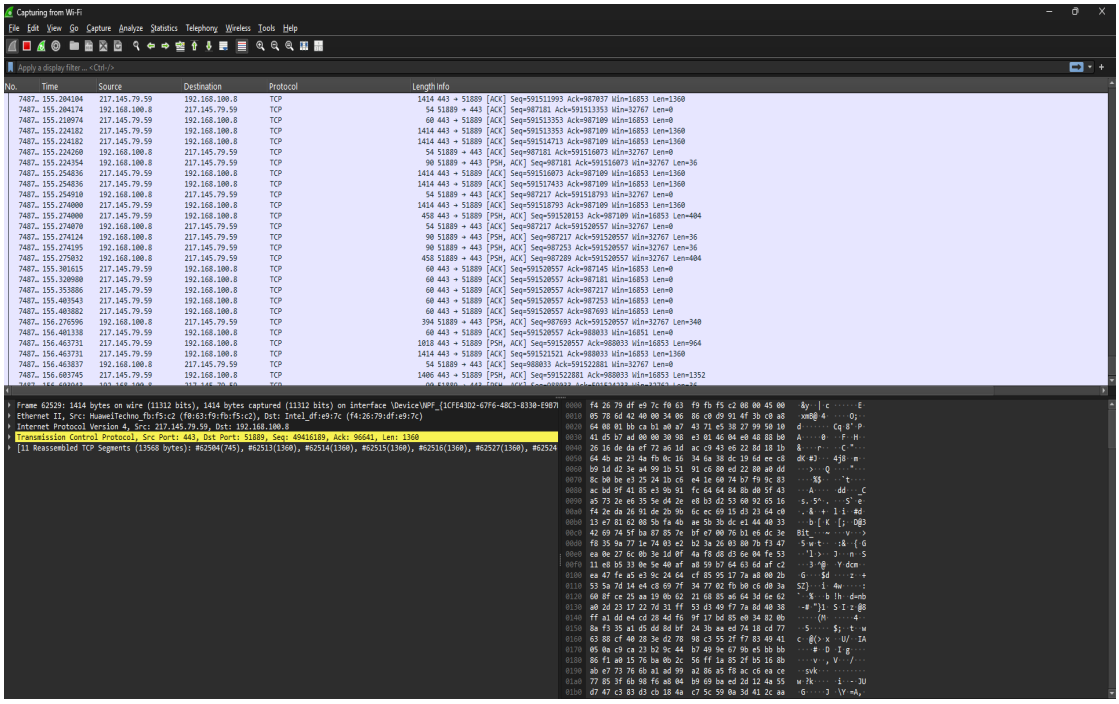
در این آزمایش قصد داریم آشنایی بیشتری با نرم‌افزار Wireshark و منوی Statistics در آن پیدا کنیم و از امکانات آن برای تحلیل بسته‌های جمع‌آوری‌شده استفاده نماییم.

۸-۲- آمادگی پیش از آزمایش:

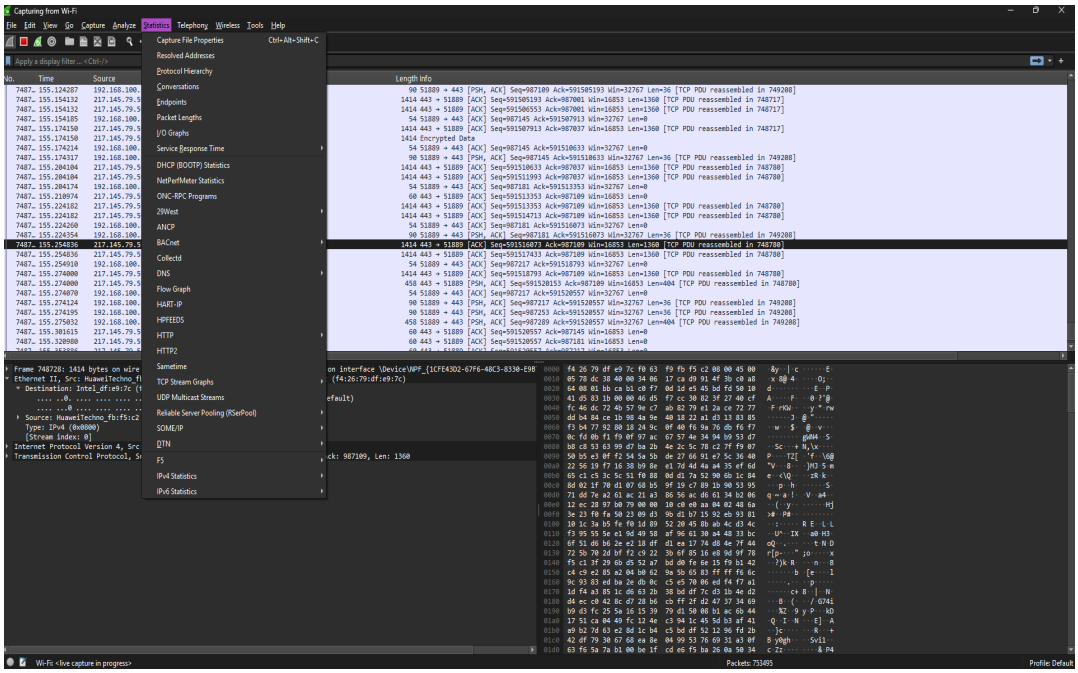
دستور کار مربوط به آشنایی Wireshark را مرور کنید.

۸-۳- شرح آزمایش:

نرم‌افزار Wireshark را بازکرده، چند دقیقه به وب گردی بپردازید و بسته‌ها را جمع‌آوری کنید. سپس مطابق جمع‌آوری بسته را متوقف کرده و از منوی بالا بر روی گزینه Statistics کلیک کنید. در ادامه قصد داریم مواردی که در این Tab وجود دارند و ترافیک‌های موجود را بررسی کنیم.



شکل ۱: جمع‌آوری بسته‌ها



شکل ۲: Statistics Menu

- بر روی گزینه‌ی Resolved Addresses کلیک کنید.

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

سؤال ۲: آیا می‌توانید ۳ بایت اولی که برای آدرس فیزیکی کارت‌های شبکه Cisco می‌باشند را مشخص کنید؟

- بر روی گزینه‌ی Protocol Hierarchy کلیک کنید.

سؤال ۳: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

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

- بر روی گزینه‌ی Conversations کلیک کنید.

سؤال ۵: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

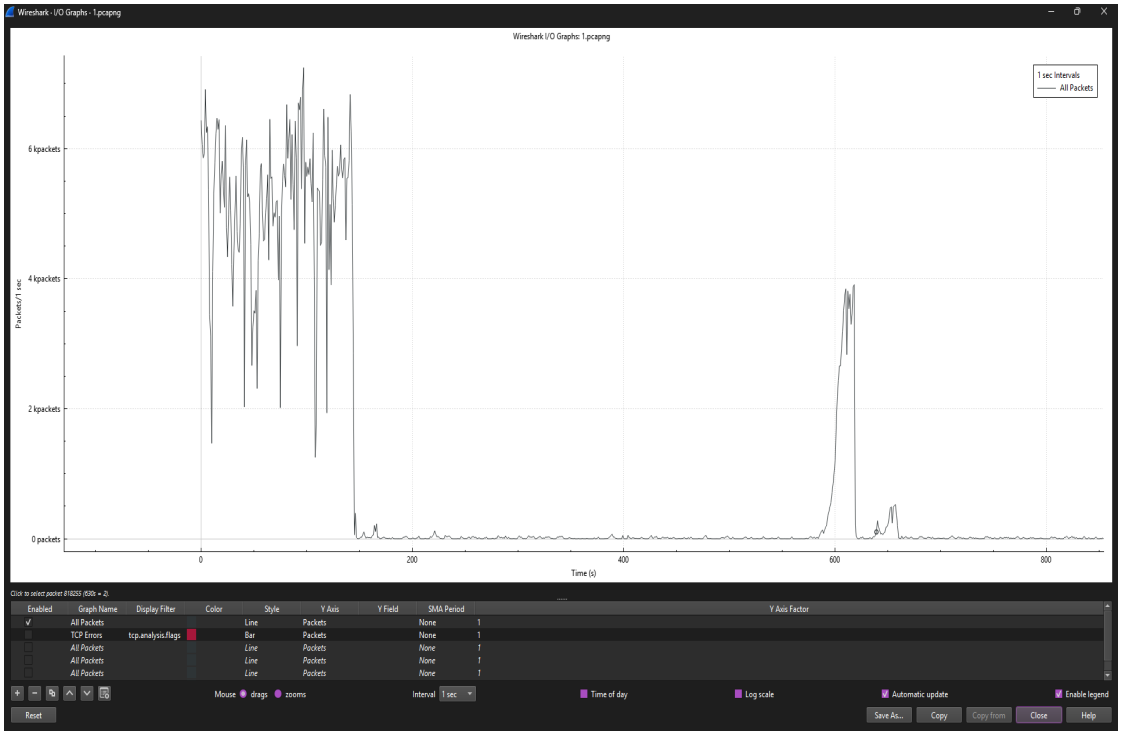
- یک نشست TCP و UDP را مشخص کنید. (برای مشخص کردن یک نشست TCP و UDP نیاز است که آدرس و پورت مبدأ و مقصد را مشخص کنید.)
- بر روی گزینه endpoints کلیک کنید.

سؤال ۶: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

سؤال ۷: چه مقصدهایی برای ارتباط‌های TCP در سیستم شما استفاده‌شده است؟

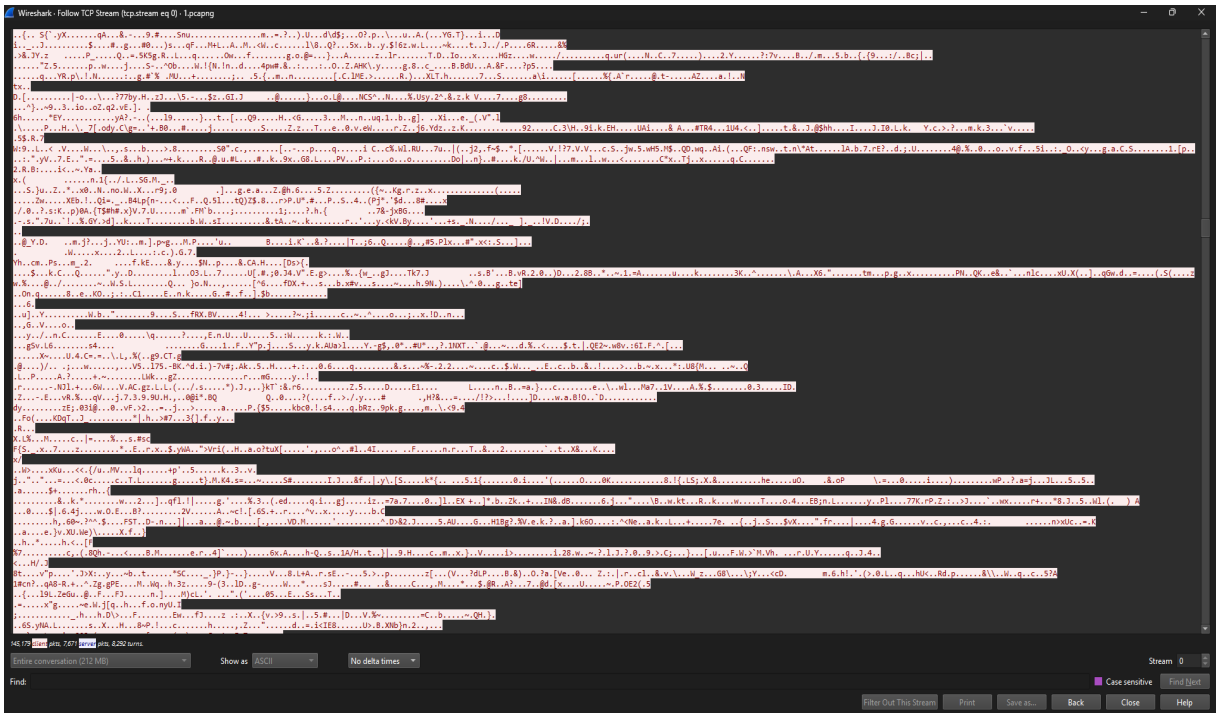
سؤال ۸: از قسمت Ethernet و از روی تعداد بسته‌های مبادله شده، Default Gateway شبکه خود را تشخیص دهید.

- بر روی گزینه‌ی I/O Graph کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید نرخ I/O را مشاهده کنید. شما قادر هستید در این صفحه نمودارهای مختلفی بسازید. بر روی دکمه + در پایین سپس یک فیلتر به آن اضافه کنید تا نمودار تعداد بسته‌ها در ثانیه را مشاهده کنید. با کلیک روی نمودار، بسته‌ها در پنجره اصلی مشخص خواهند شد.

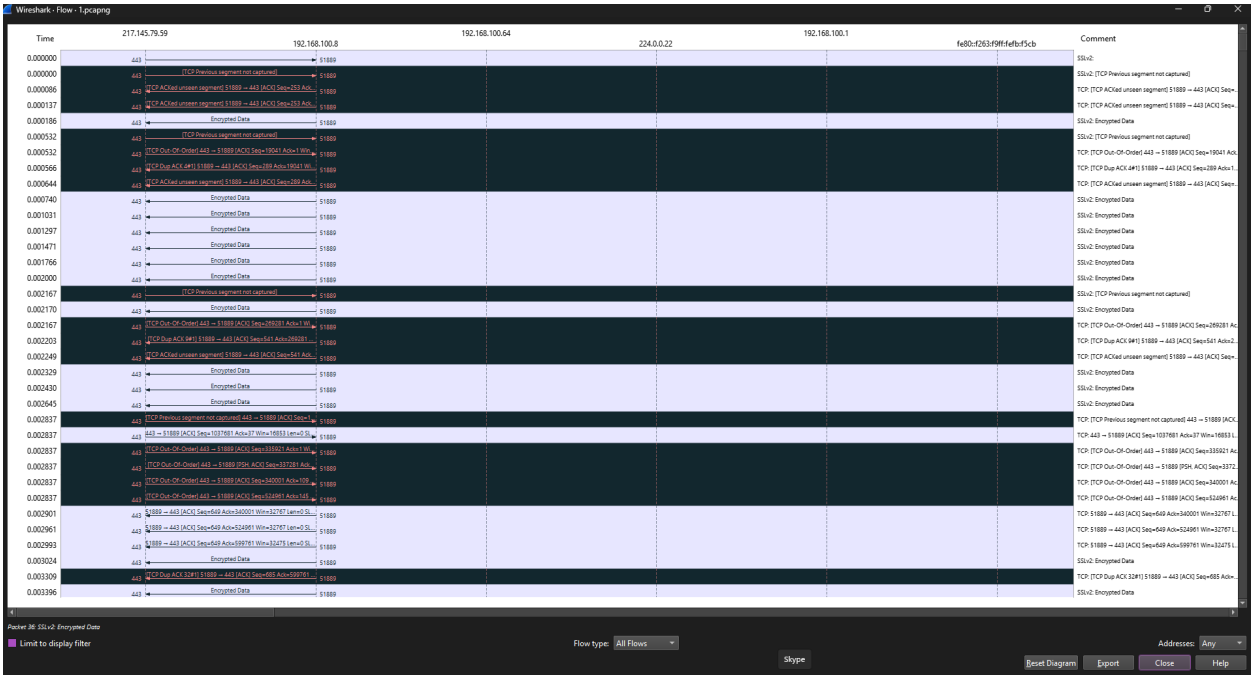


شکل ۳: I/O Graphs

- بسته‌های مربوط به ارتباط با یک سایت را فیلتر کنید (با استفاده از Follow TCP Stream). سپس بر روی گزینه‌ی Flow Graph کلیک کنید. از منوی پایین، در بخش Show، Displayed packets را انتخاب کنید. به‌صورت کامل جزئیات مربوط به SeqNum و Ack و شماره پنجره را دنبال کنید.

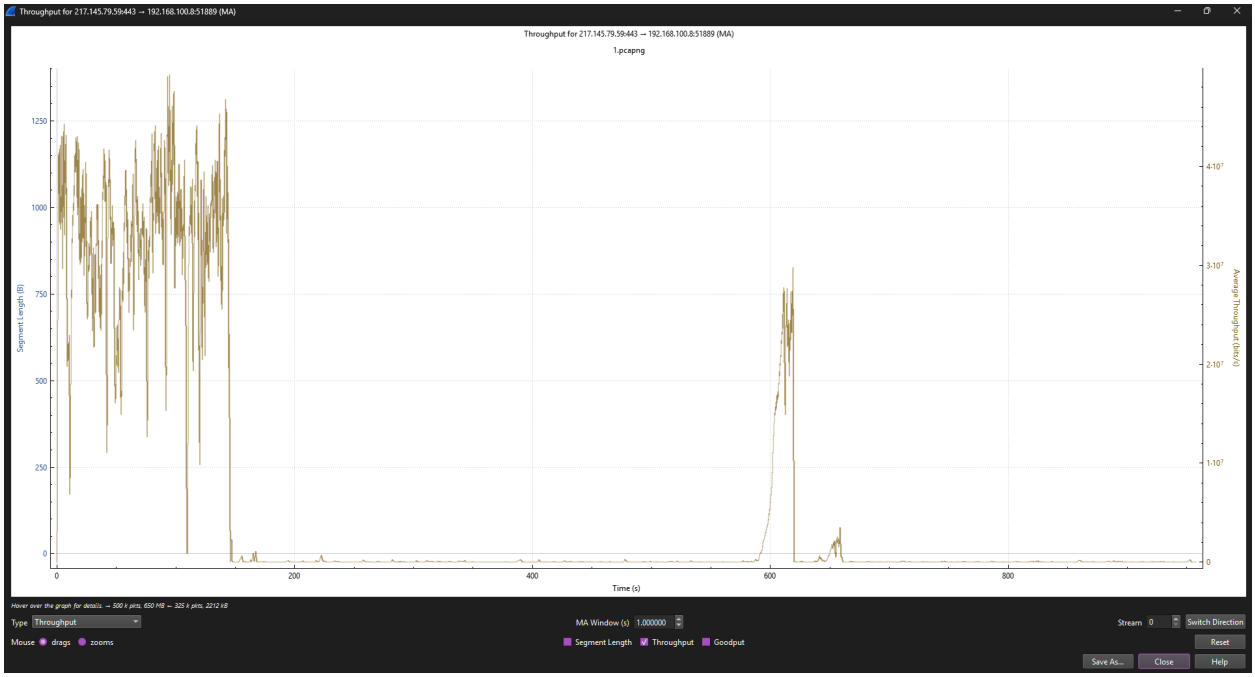


شکل ۴: Follow TCP Stream

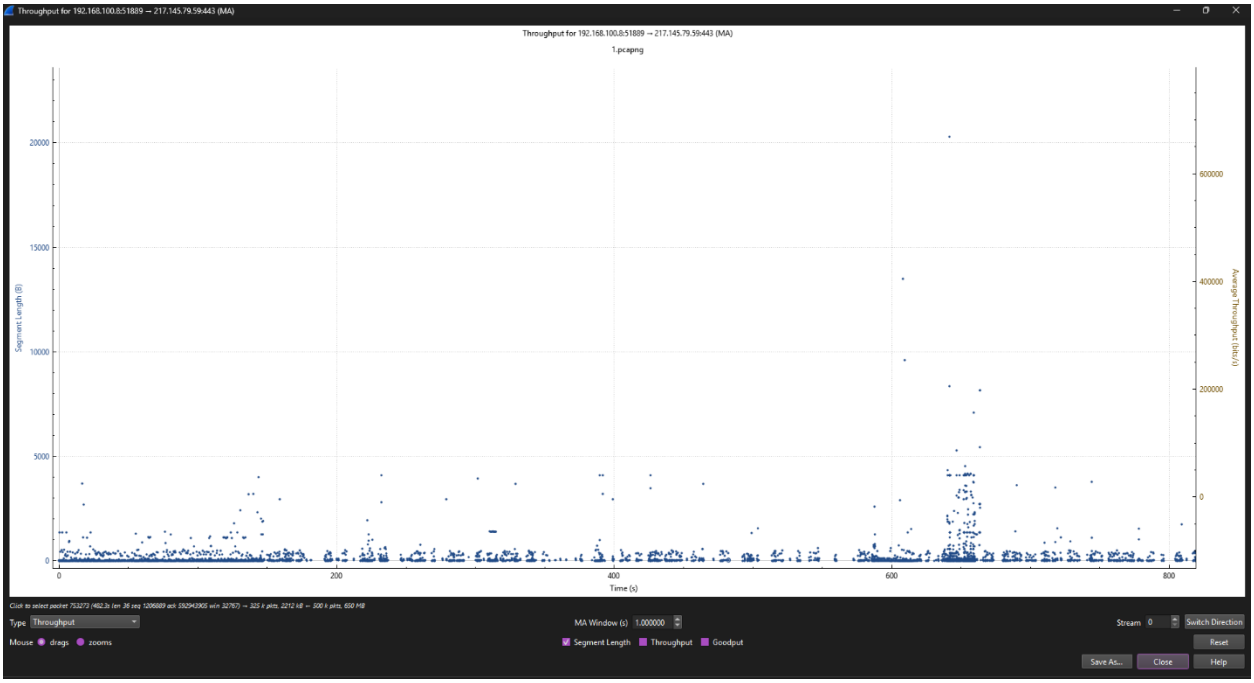


شکل ۵: Flow Graph

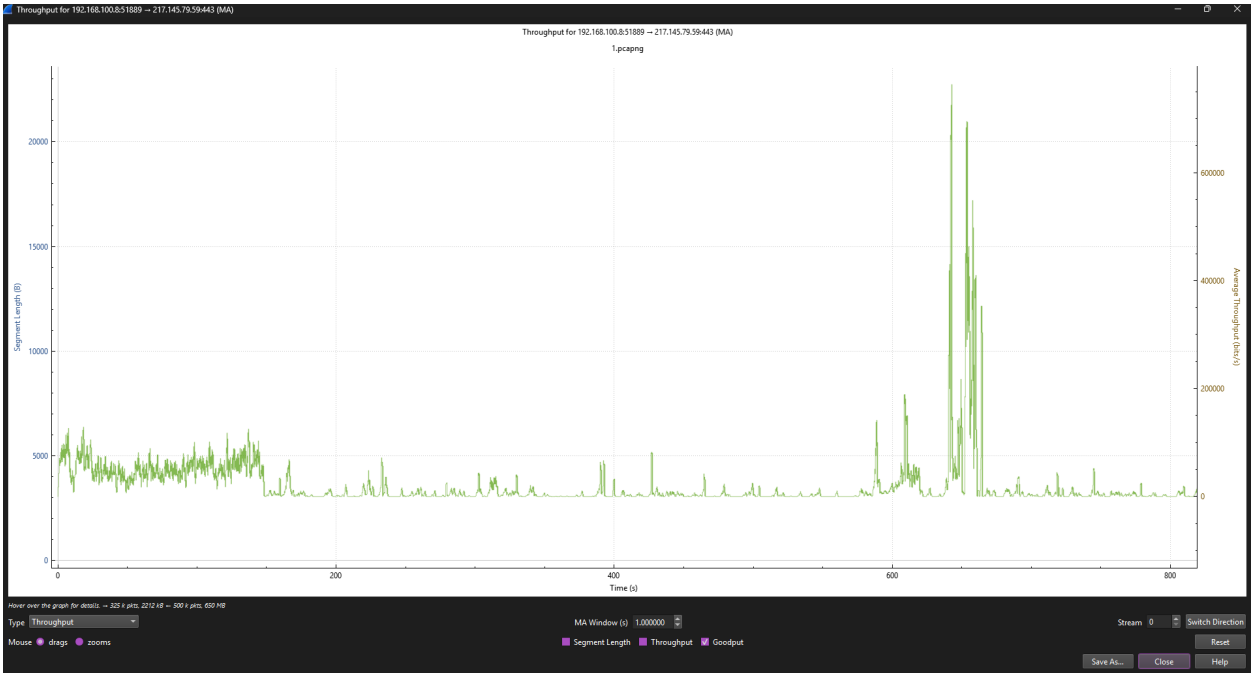
- بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Throughput کلیک کنید. در این پنجره می‌توانید گذردهی میانگین با واحد بیت در ثانیه در طول زمان برای یک ارتباط TCP را مشاهده کنید. با گزینه‌ی Switch Direction می‌توانید ارتباط در جهت برعکس را بررسی کنید. بر روی نمودار نقاط آبی‌رنگی قرار دارند، این نقاط طول segmentهای ارسال‌شده 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 کاربر داده خود را دریافت می‌کند و در آن Retransmissionها را در نظر گرفته نمی‌شوند.



شکل ۶: Throughput

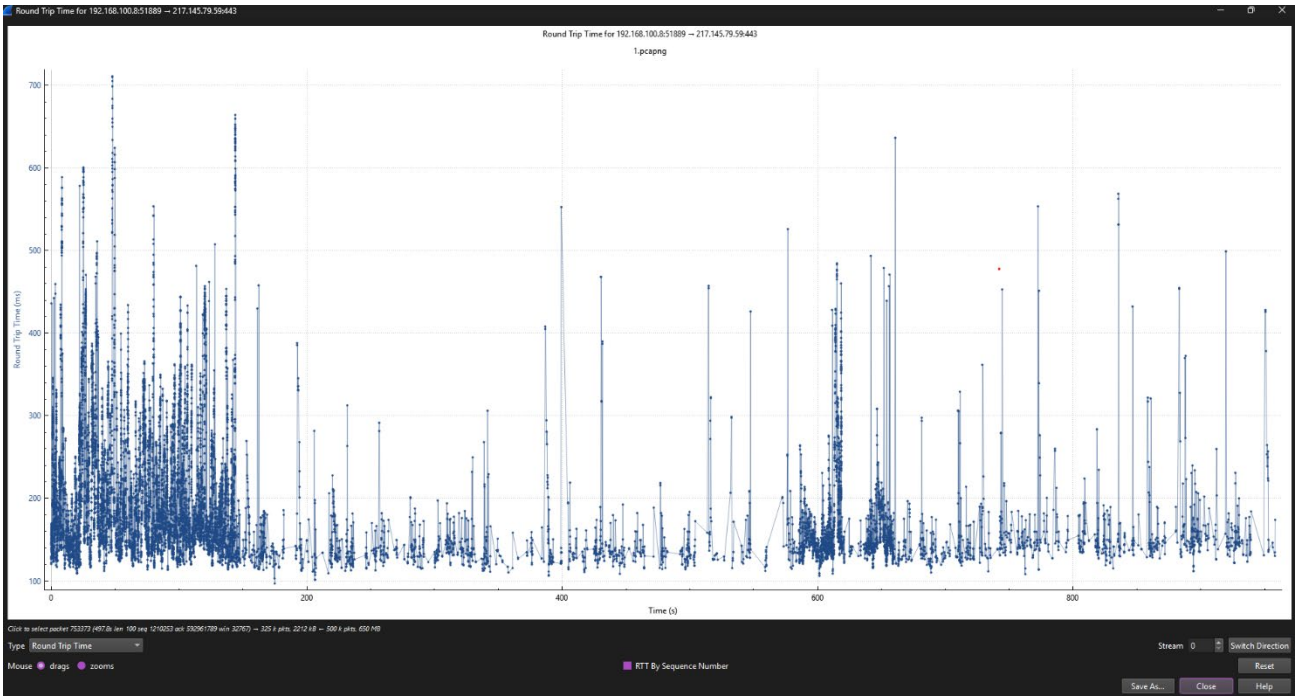


شکل ۷: Segment Length



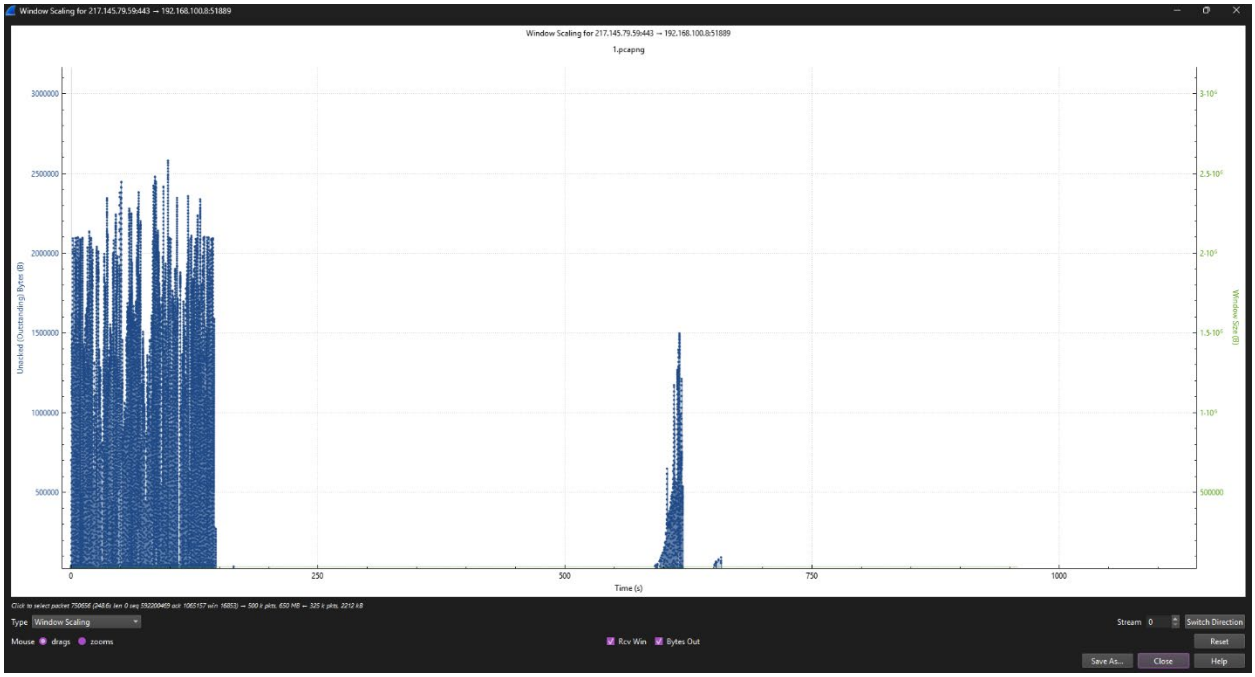
شکل ۸: Goodput

- بر روی گزینه TCP Stream Graph کلیک کنید. در منوی جدیدی که باز می‌شود بر روی Round Trip Time کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید زمان رفت‌وبرگشت را برای یک ارتباط TCP مشاهده کنید. گزینه‌های این پنجره مانند قسمت قبل است. می‌توانید با انتخاب گزینه‌ی RTT by Sequence Number این نمودار را برحسب شماره‌ی بسته‌ها داشته باشید.



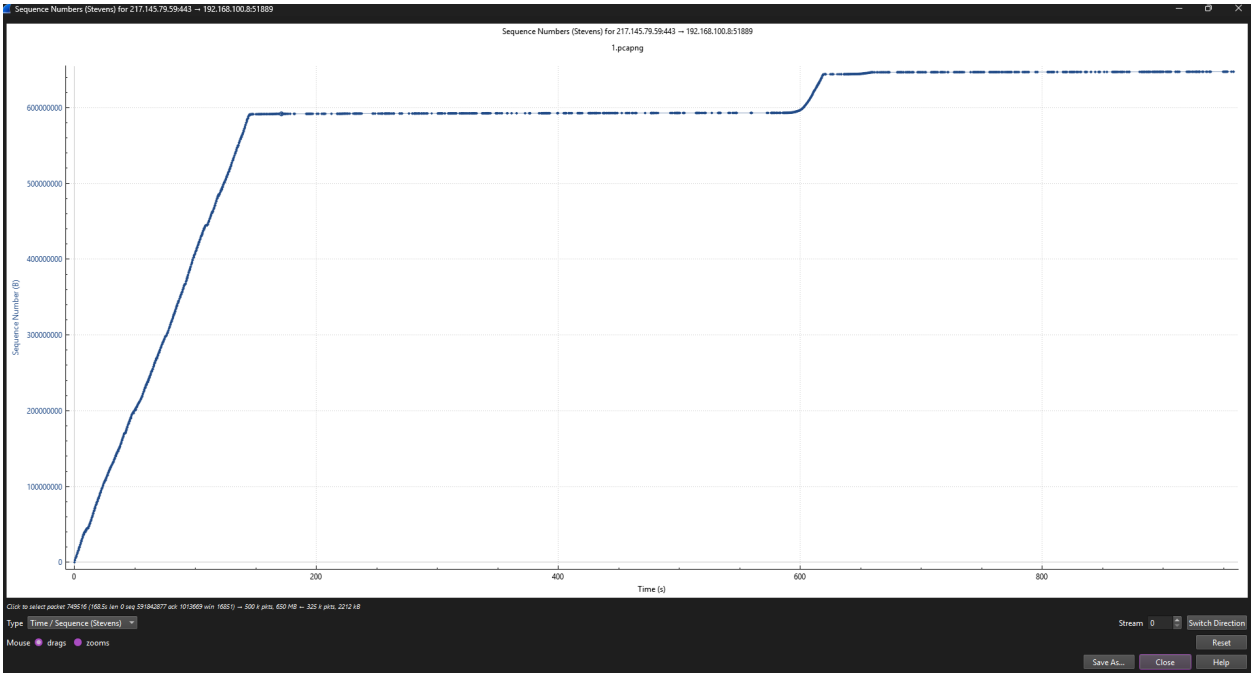
شکل ۹: نمودار RTT

- بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Window Scaling کلیک کنید. در این قسمت می‌توانید اندازه‌ی پنجره‌ی دریافت (با خط سبزرنگ) و بایت ارسالی (با خط آبی‌رنگ) را برای یک ارتباط TCP مشاهده نمایید.



شکل ۱۰: نمودار Window Scaling

- بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Time / Sequence (Stevens) کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید Sequence number در طی زمان را برای یک ارتباط TCP مشاهده نمایید. با استفاده از این نمودار می‌توانید تأخیر، از دست رفتن و تداخلات در ارتباط را پیدا کنید. دقت کنید که این نمودار مربوط به‌اندازه پنجره دریافتی است.



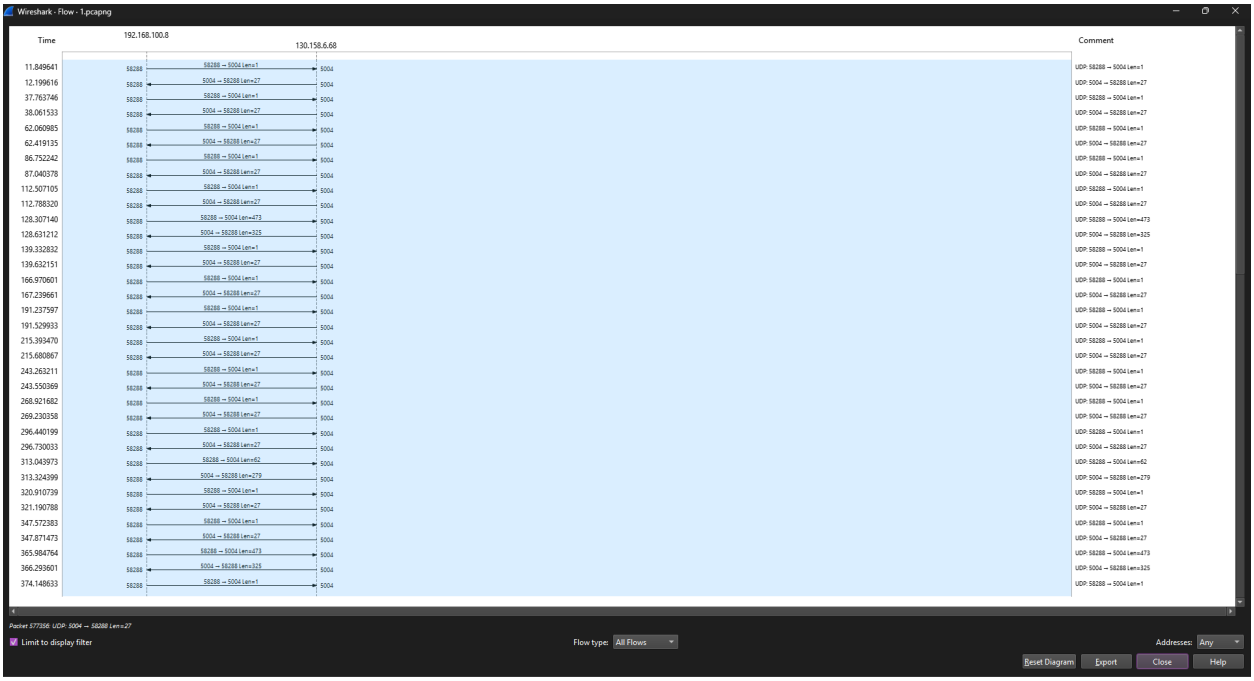
شکل ۱۱: نمودار Sequence Numbers

سؤال ۹: به‌صورت هم‌زمان ۲ فایل نسبتا حجیم را دانلود کنید و در Wireshark بسته‌ها را به مدت یک دقیقه شنود کنید. ممکن است که ازدحامی رخ دهد، برای بررسی این اتفاق ابتدا از طریق Conversation آدرس IP آن سایت را مشخص کنید. سپس می‌توانید آن را به‌عنوان یک فیلتر اعمال کنید و نمودارهای Throughput، Windows scaling و RTT را بررسی کنید و مشخص کنید در شرایط ازدحام چه اتفاقی برای موارد بیان‌شده رخ می‌دهد.

سؤال ۱۰: ترافیک‌های UDP موجود در Wireshark را فیلتر کرده (در صورت لزوم توسط iperf ترافیکی بین یک سیستم کلاینت و سرور ایجاد کنید.)

Server: iperf -s -u
Client: iperf -c <IP-server> -u -b 10M -t 30

در قسمت Flow graph، مشاهده کنید که UDP بدون ACK و شماره تأیید کار می‌کند. چرا UDP در مقایسه با TCP، Flow control ندارد؟



شکل ۱۲: Flow Graph برای UDP