

دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه های کامپیوتری

(پاییز ۱۴۰۰)

**جلسه پنجم**

**تحلیل TCP با استفاده از Whireshark**

**محمد چوپان 9831125**

* 1. تحلیل TCP با استفاده از Wireshark
     1. 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.

* + 1. فعالیت‌های قبل از آزمایش

دستور کار جلسه‌ی آشنایی با wireshark را مرور کنید.

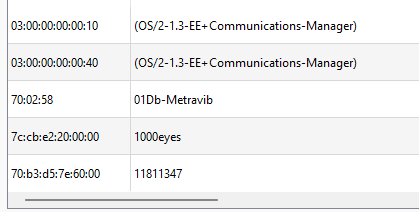
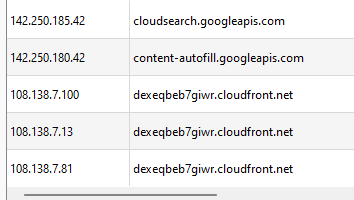
* + 1. شرح آزمایش

نرم‌افزار wireshark را باز کرده، چند دقیقه به وب گردی بپردازید و بسته‌ها را جمع‌آوری کنید. سپس مطابق جمع‌آوری بسته را متوقف کرده و از منوی بالا بر روی گزینه‌ی Statistics کلیک کنید. در ادامه قصد داریم مواردی که در این زبانه وجود دارند را بررسی کنیم.

1. بر روی گزینه‌ی Resolved Addresses کلیک کنید.

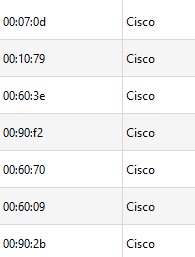
در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

در این قسمت آدرس ip که به آن متصل شدیم را نشان می دهد که host ها را به چه ip هایی متصل کرده است و علاوه بر آن آدرس فیزیکی کارت شبکه جایی که آن متصل شده ایم را هم برای ما می آورد.

آیا می‌توانید سه بایت اولی که برای آدرس فیزیکی کارت‌های شبکه Cisco می‌باشند را مشخص کنید؟

بله وقتی از منوی بالا Ethernet Well-Known Addresses را انتخاب کنیم برای ما تمامی کارت های شبکه های شناخته شده را می آورد و در نهایت زمانی که cisco را سرچ کنیم :

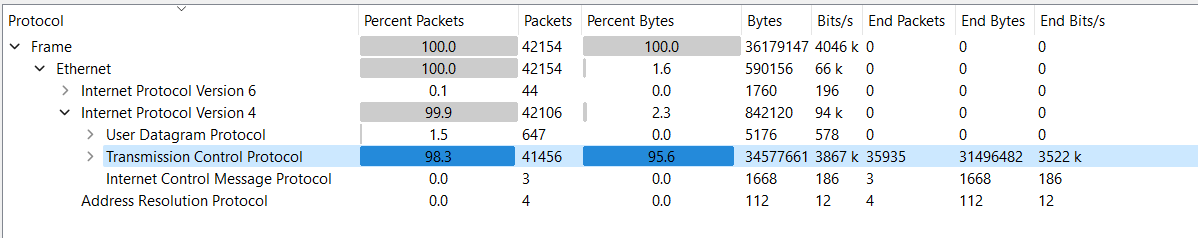
 نتیجه بالا را مشاهده میکنیم.

1. بر روی گزینه‌ی protocol hierarchy کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

با استفاده از مدل لایه ای پرتکل هایی که وجود دارند با مقدار درصد استفاده و یا مقادیر انتقال داده آن ها را به ما نشان می دهد. که مثلا در جستجوی شما 50 % پرتکل IPV4 بوده است .

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

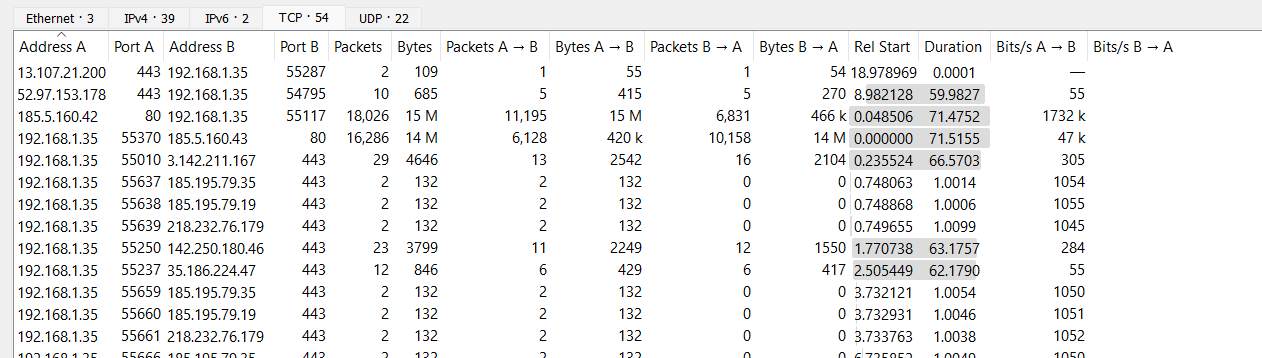


با توجه به شکل بالا 98.3 درصد بسته ها این مورد را شامل می شوند.

1. بر روی گزینه‌ی Conversations کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

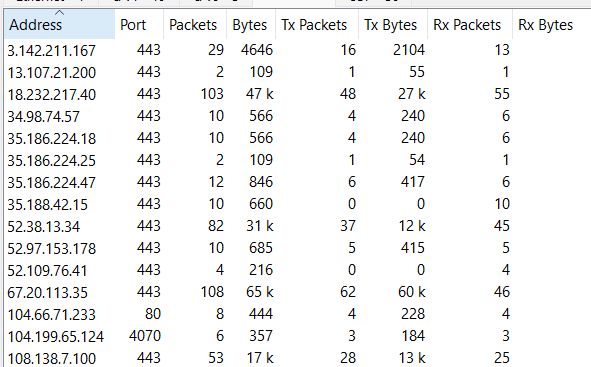
می بینیم که نشست ها را با توجه به پروتکل های آن ها دسته بندی کرده است.



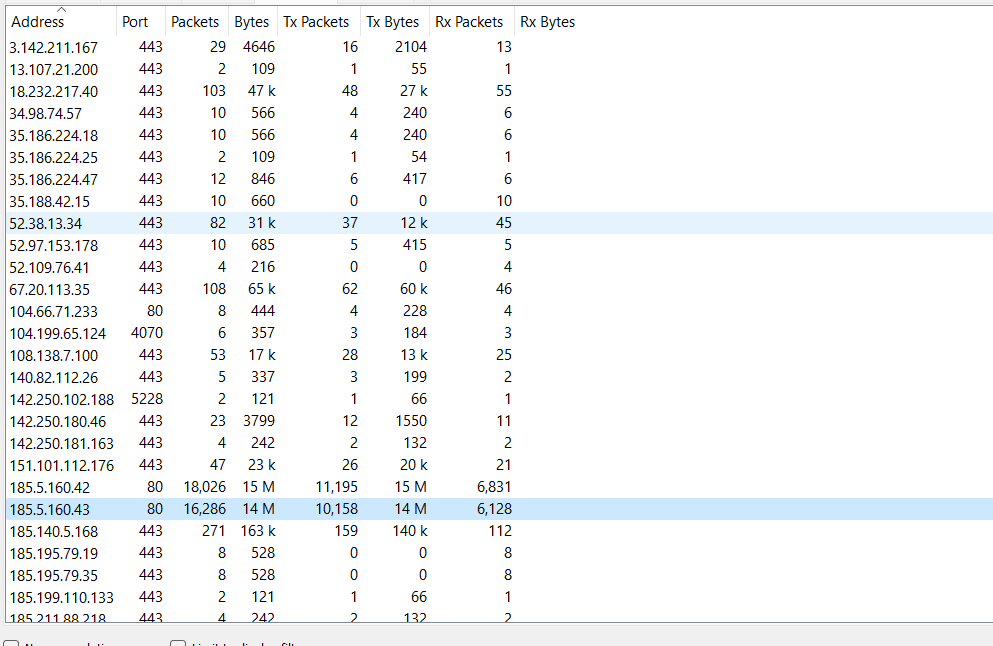
1. یک نشست TCP را مشخص کنید. (برای مشخص کردن یک نشست TCP نیاز است که آدرس و پورت مبدا و مقصد را مشخص کنید.) توجه داشته باشید مفهومی که Wireshark از نشست برداشت می‌کند با مفهومی که در کلاس آموخته‌اید تفاوت دارد.
2. بر روی گزینه‌ی endpoints کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

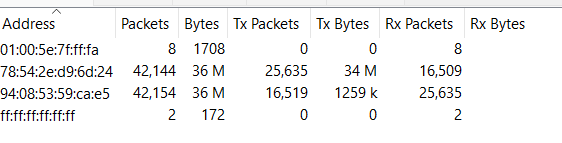
مقصد هایی که در قالب پروتکل های متفاوت با آن ها در ارتباط بوده ایم .



چه مقصدهایی برای ارتباط‌های TCP در سیستم شما استفاده شده‌اند؟

در اینجا همان مقصد هایی است که در conversation وجود داشته برای مثال گزینه انتخاب شده آدرس سرور شخصی برای proxy به گیت لب یک شرکت است. که فایل ها با آن انتقال داده شده است .

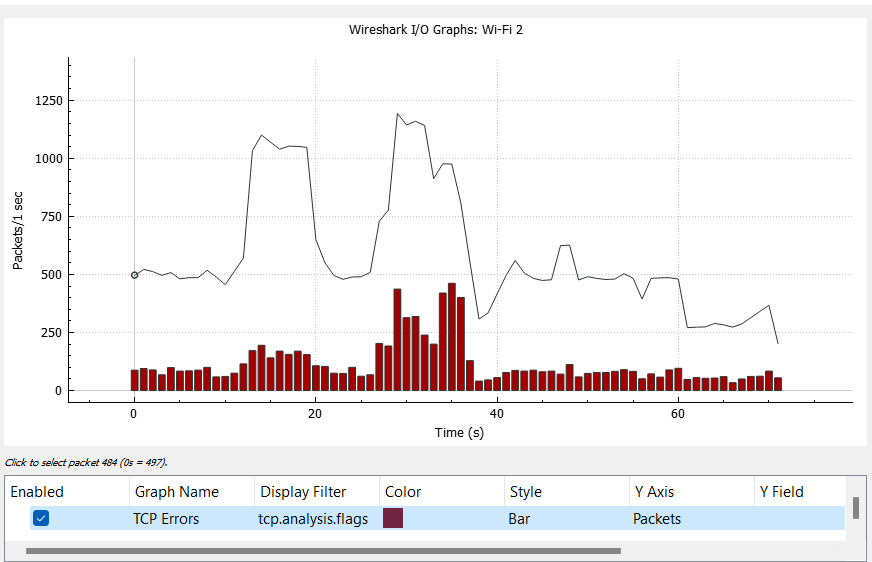
آیا می‌توانید از زبانه Ethernet و از روی تعداد بسته‌های مبادله شده، Default Gateway شبکه خود را تشخیص دهید؟





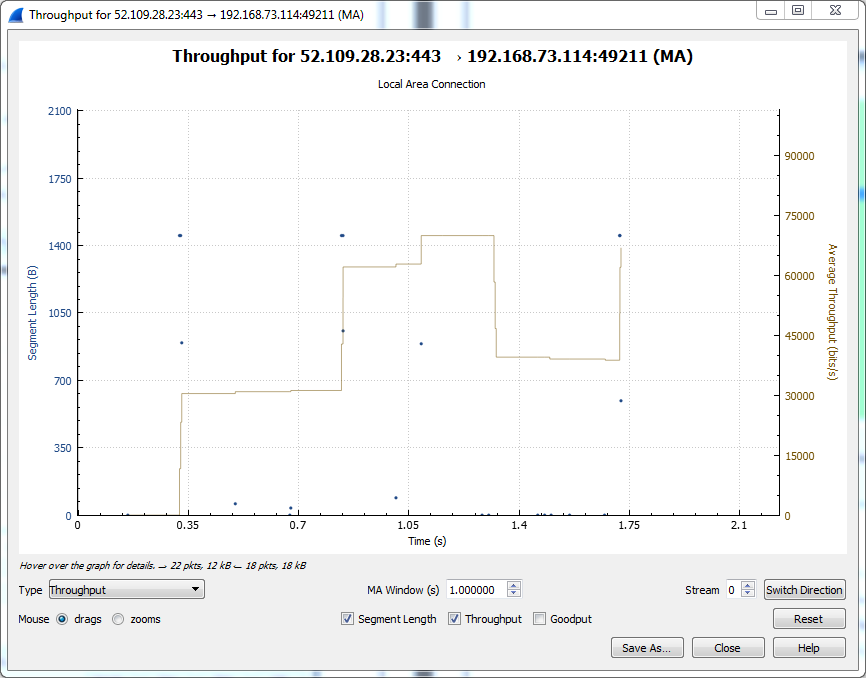
بله آدرسی که بیشترین تعداد بسته با آن انتقال یافته است همان default gateway ما می باشد.

1. بر روی گزینه‌ی I/O Graph 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 خواهند شد.



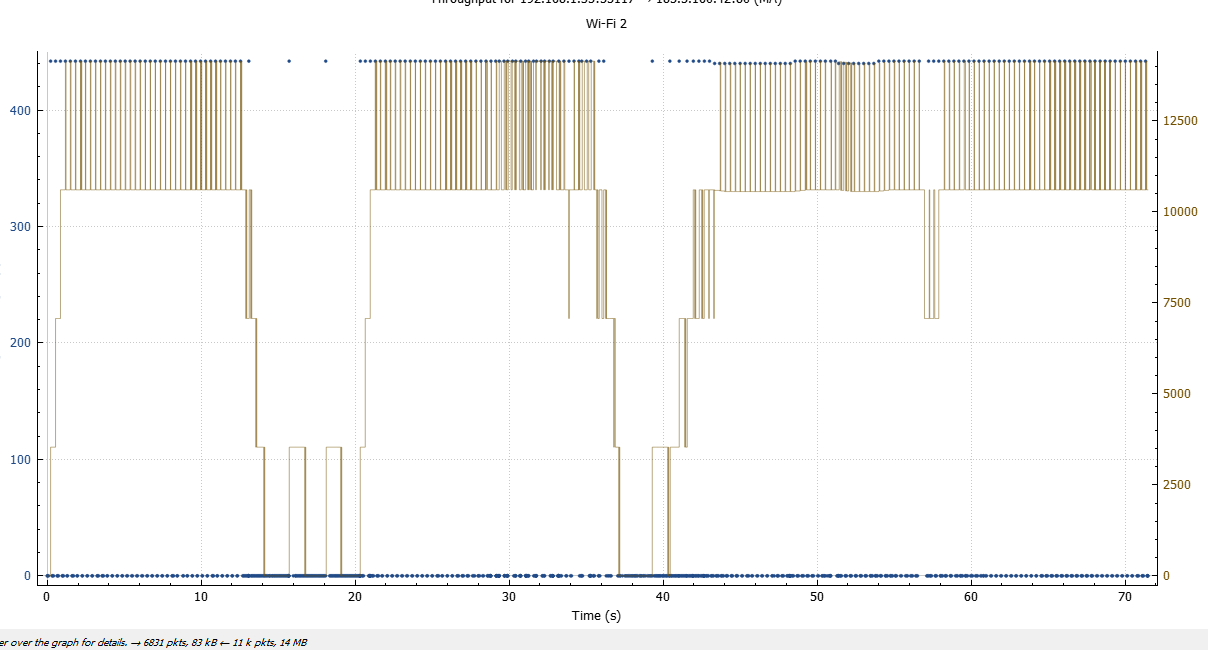
که فیلتر ارور های TCP گذاشته شده است.

1. 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.
2. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Throughput کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید گذردهی میانگین با واحد بیت در ثانیه در طول زمان برای یک ارتباط TCP را مانند ‏شکل (1-1) مشاهده کنید. با گزینه‌ی Switch Direction می‌توانید ارتباط در جهت برعکس را بررسی کنید. بر روی نمودار نقاط آبی رنگی قرار دارند، این نقاط طول segmentهای 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.

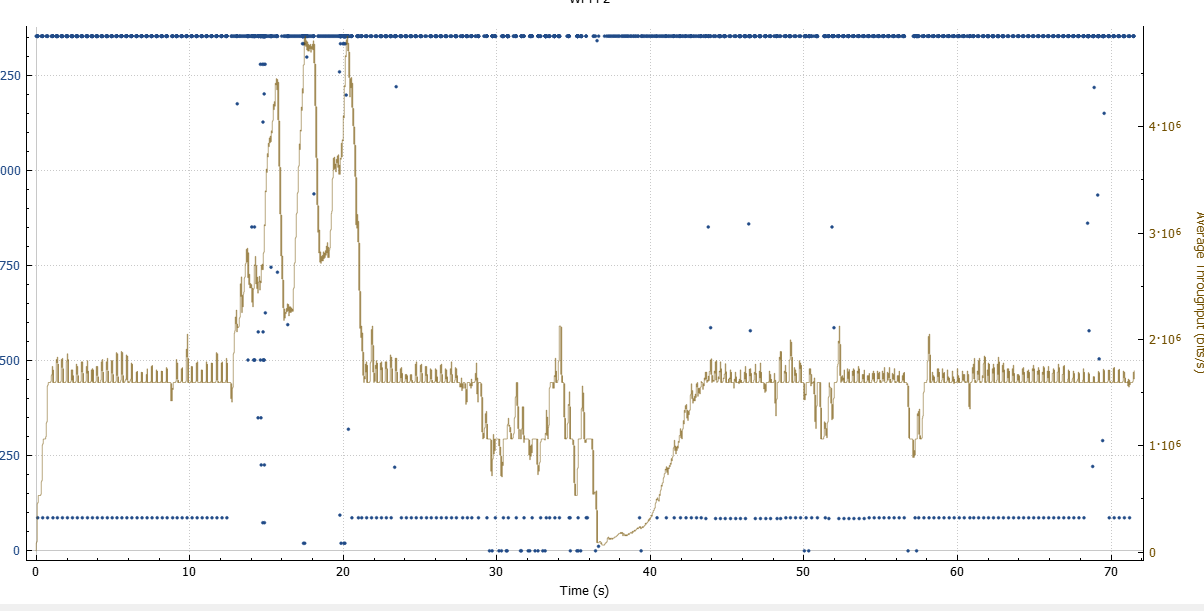


نمودار گذردهی

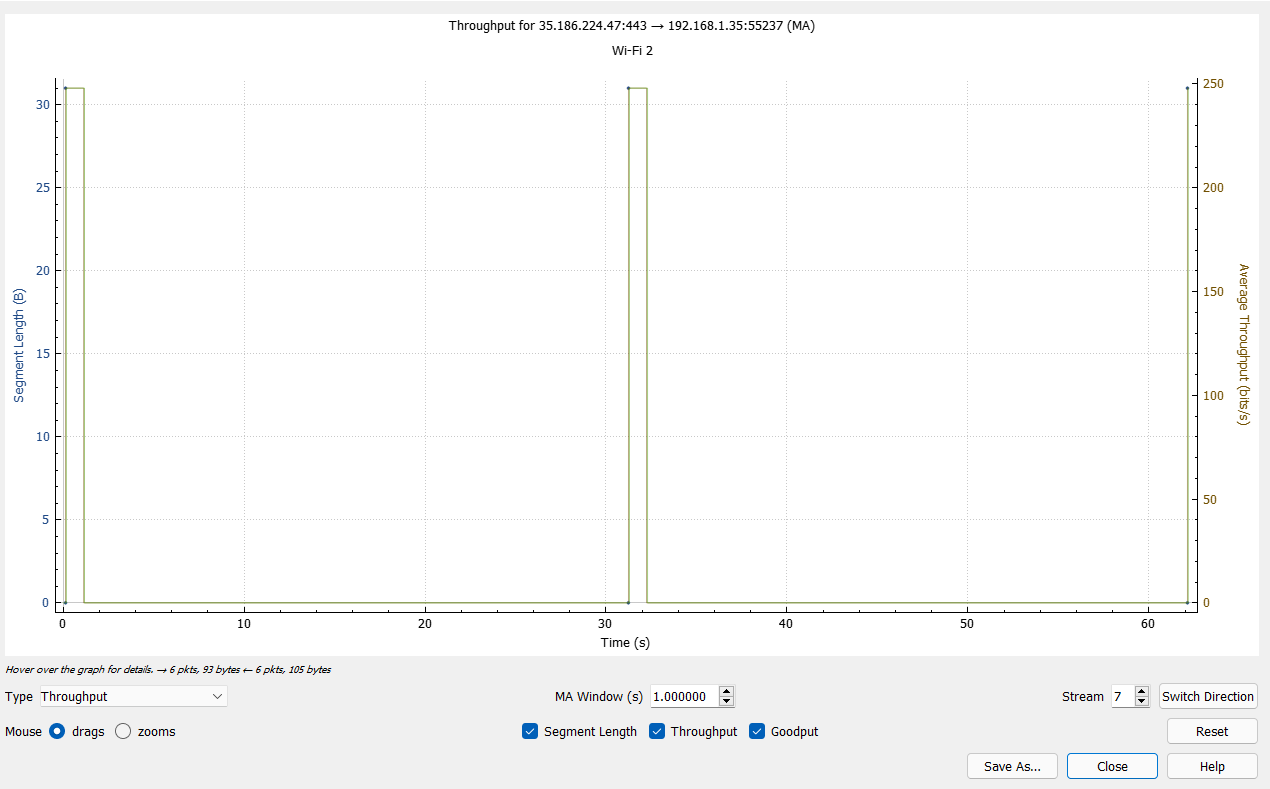
مثال ما :



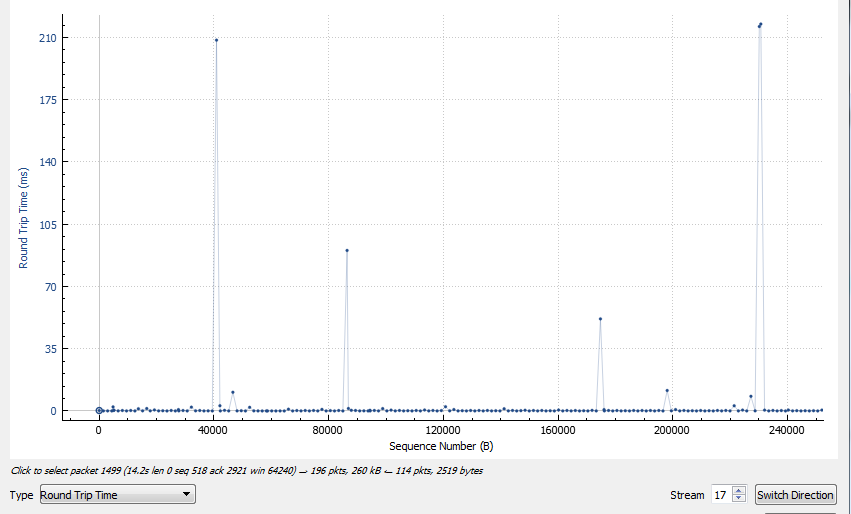
نمودار برعکس شده :



برای استریم دیگر:

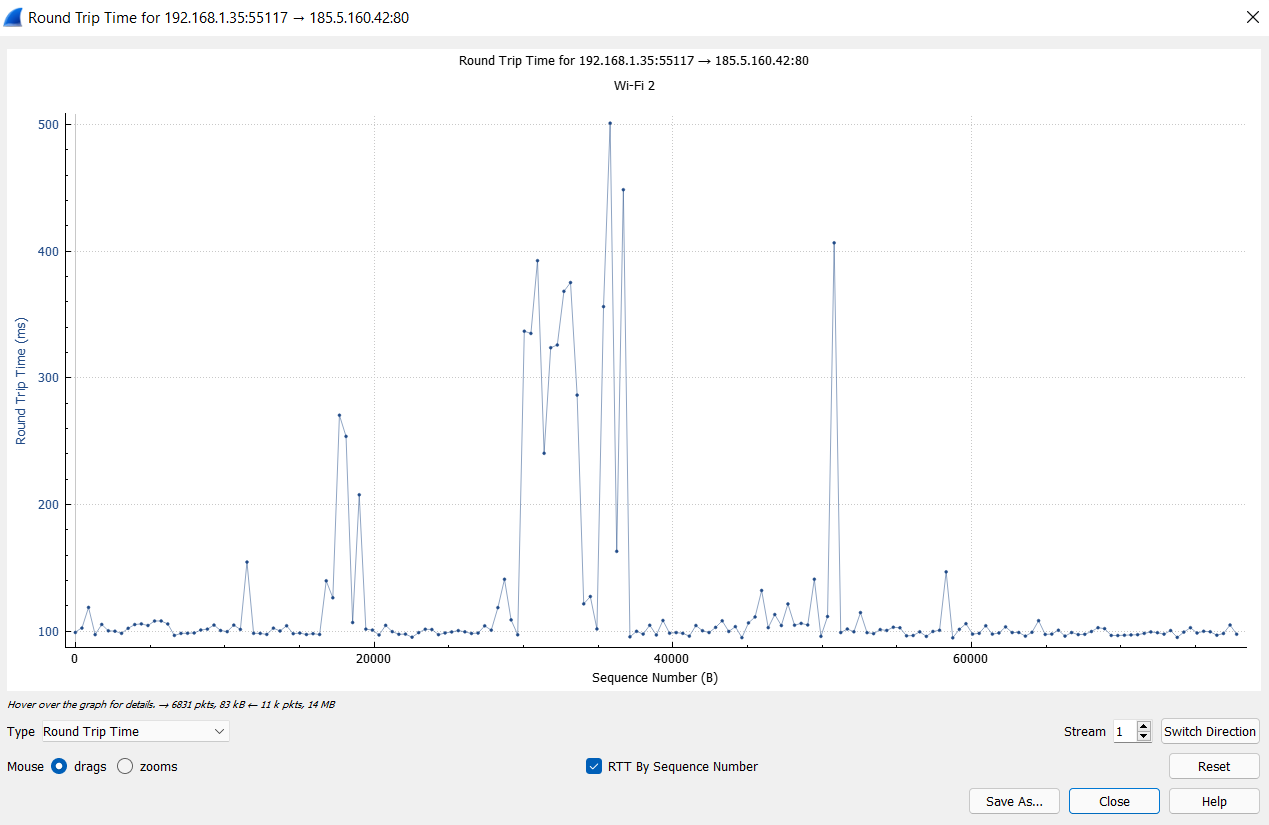


1. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Round Trip Time کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید زمان یک رفت و برگشت را برای یک ارتباط TCP مشاهده کنید (‏شکل (1-2)). گزینه‌های این پنجره نیز مانند قسمت 8 است. می‌توانید با انتخاب گزینه‌ی RTT By Sequence Number این نمودار را برحسب شماره‌ی بسته‌ها داشته باشید. شمارنده Stream در گوشه پایین سمت راست را به شماره Stream مربوط به اتصال TCP با یکی از سایت‌هایی که داشتید تنظیم کنید.

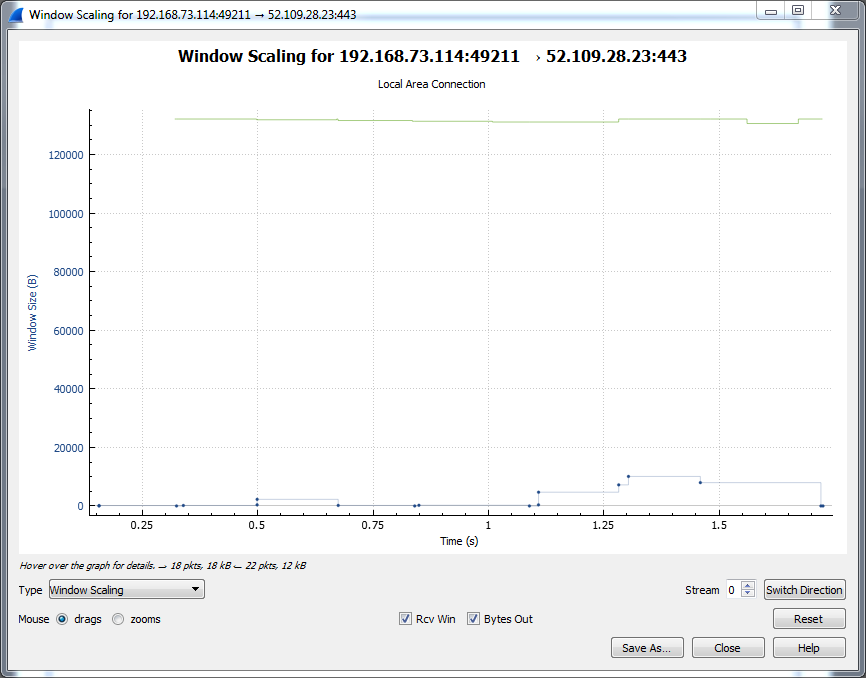


نمودار RTT

اتصال ما :



1. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Window Scaling کلیک کنید. پنجره‌ای مانند ‏شکل (1-3) باز می‌شود که می‌توانید اندازه‌ی پنجره‌ی دریافت (با خط سبز رنگ) و بایت‌های ارسالی (با خط آبی رنگ) را برای یک ارتباط TCP مشاهده نمایید. تمامی تنظیمات این پنجره مانند قسمت ۸ است.

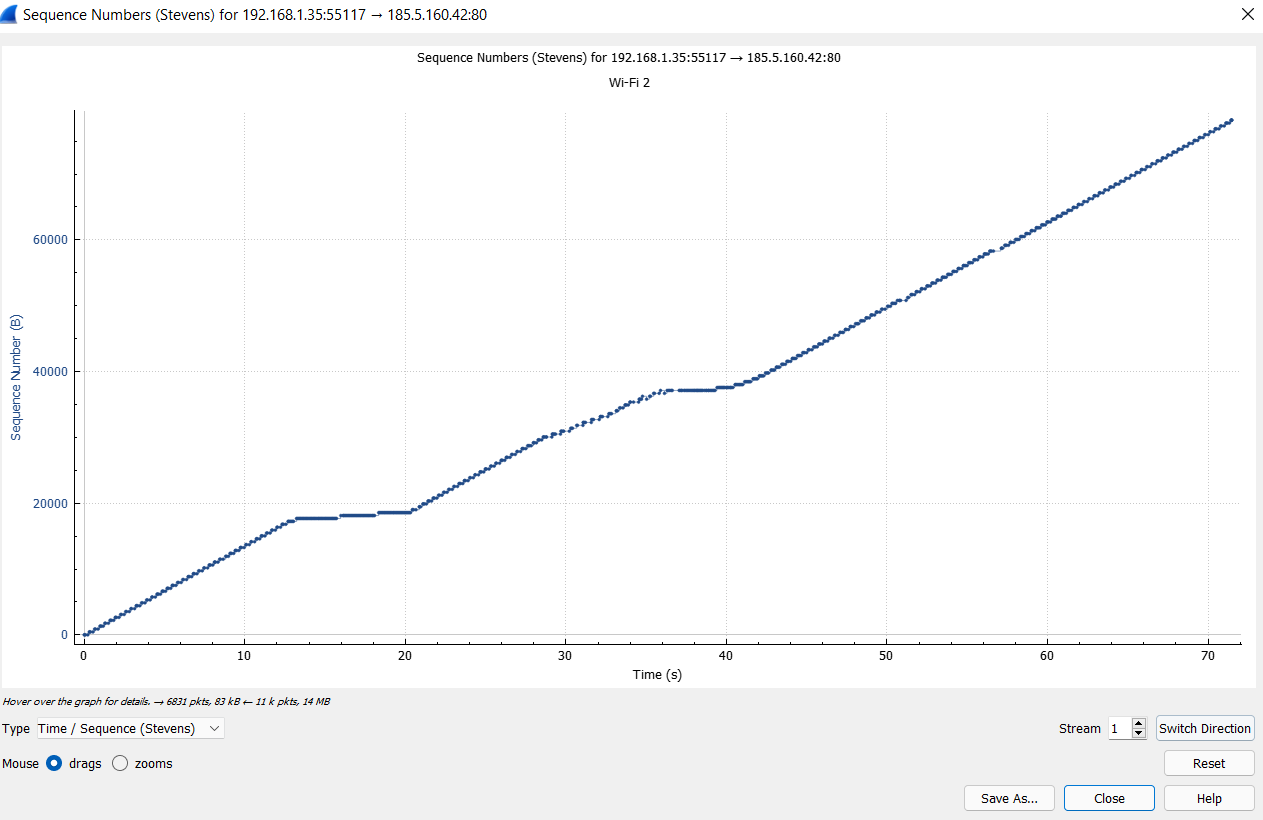


نمودار Window Scaling

مثال ما :



1. 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. تمامی تنظیمات این پنجره مانند قسمت ۸ است. با استفاده از این نمودار می‌توانید تاخیر، از دست رفتن و تداخلات در ارتباط را پیدا کنید. این نمودار توسط W. Richard Stevens پیشنهاد شده است. دقت کنید که نمودار مربوط به اندازه پنجره دریافتی است.



به سایت دانلود دانشگاه مراجعه کنید

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

به‌صورت هم‌زمان دو فایل با اندازه 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 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 بیان شده رخ می‌دهد. تغییرات را برای ده بسته قبل و بعد یک بسته دلخواه به‌صورت دقیق بررسی کنید.

از آنجایی که محیط گرافیکی ممکن است قادر به نمایش همه بسته‌ها نباشد، Wireshark را در محیط خط فرمان از طریق دستور زیر اجرا کنید. ابتدا به محل نصب Wireshark بروید و برنامه tshark که مخصوص خط فرمان است را اجرا کنید:

tshark –D

با اجرای این دستور مشاهده می‌کنید که اینترفیس‌های شما لیست می‌شوند. عدد اینترفیسی که می‌خواهید بر روی آن شنود کنید را یادداشت کنید. به فرض اینترفریس شماره 4 را انتخاب کرده‌اید. دستور زیر را اجرا کنید:

tshark –i 4 –p –w output.pcap

پس از آن بسته‌ها شنود می‌شوند. درنهایت Ctrl + C را فشار دهید و فایل output.pcap را با Wireshark باز کنید.

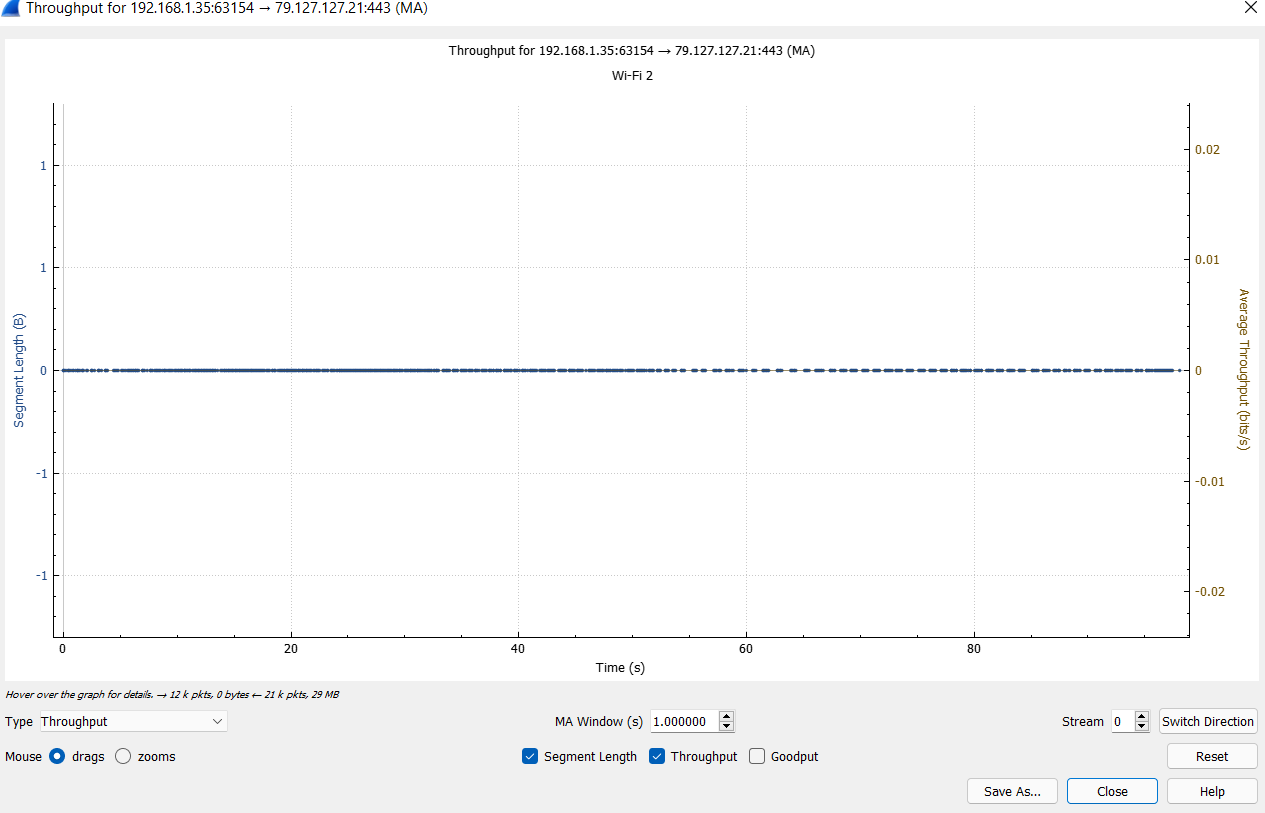
به علت در دسترس نبودن سایت دانشگاه از سایت soft98.ir استفاده شده است .

[لینک1](https://soft98.ir/os/windows/17807-%D8%AF%D8%A7%D9%86%D9%84%D9%88%D8%AF-%D9%88%DB%8C%D9%86%D9%80%D8%AF%D9%88%D8%B2-10-%D8%A2%DB%8C%D9%80%D9%88.html) و [لینک2](https://soft98.ir/os/windows-11/886-%D8%AF%D8%A7%D9%86%D9%84%D9%80%D9%88%D8%AF-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-11.html) برای دانلود در نظر گرفته شده است .

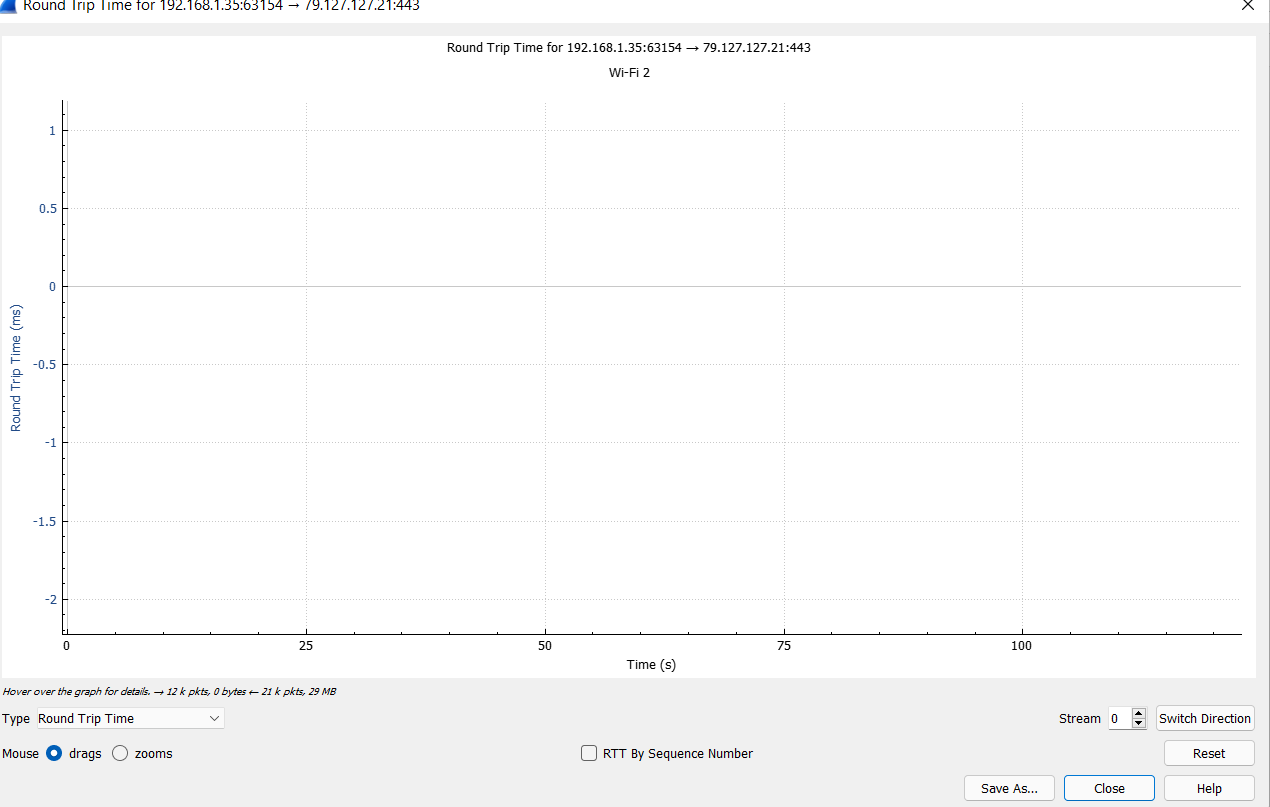


آدرس های ip سایت soft98

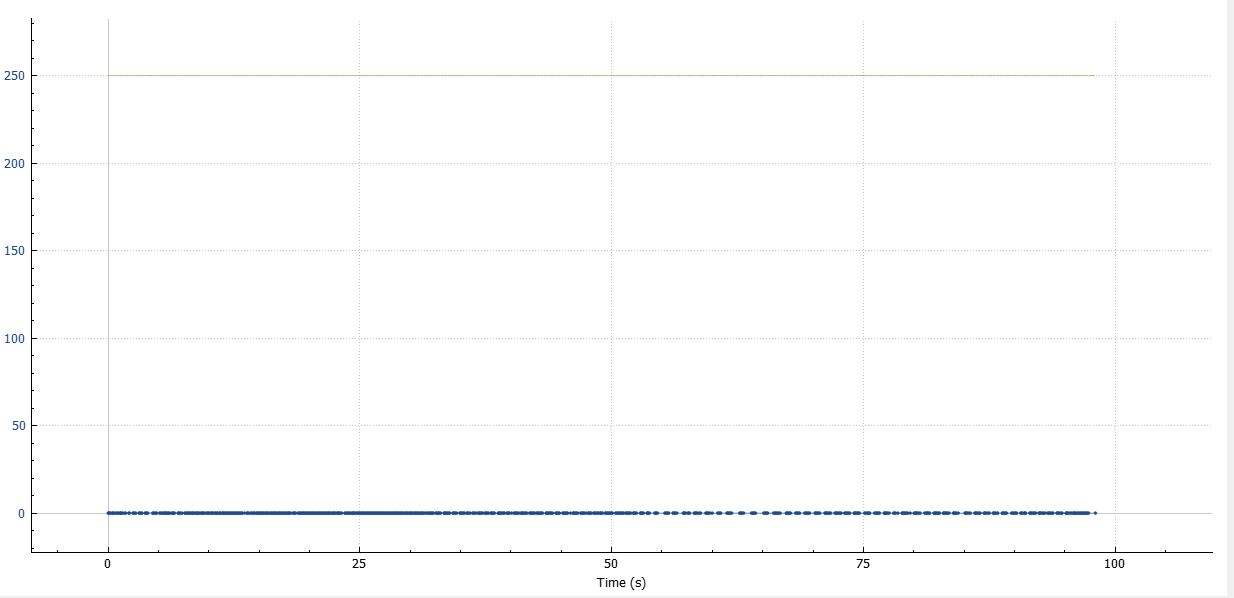
**نمودار throughput :**



**نمودار RTT :**



**نمودار Window scaling :**



با توجه به توضیحات ویدیو در صورتی که به صورت گروهی این آزمایش انجام می شد و شرایط به وجود آمده شرایط ازدحام می بود . نمودار اندازه پنجره نمودار دندان کوسه ای باید می شد . یعنی این که که همه با هم اندازه پنجره زیاد می شد برای تمامی کاربر ها سپس بعد از این که همه دچار شرایط ازدحام شدند اندازه پنجره به صورت ناگهانی کاهش پیدا میکرد. اما به این دلیل که از سایت خارجی استفاده شده است این شرایط رخ نداده است .