1- تحلیل TCP با استفاده از Wireshark

1-1- هدف آزمایش

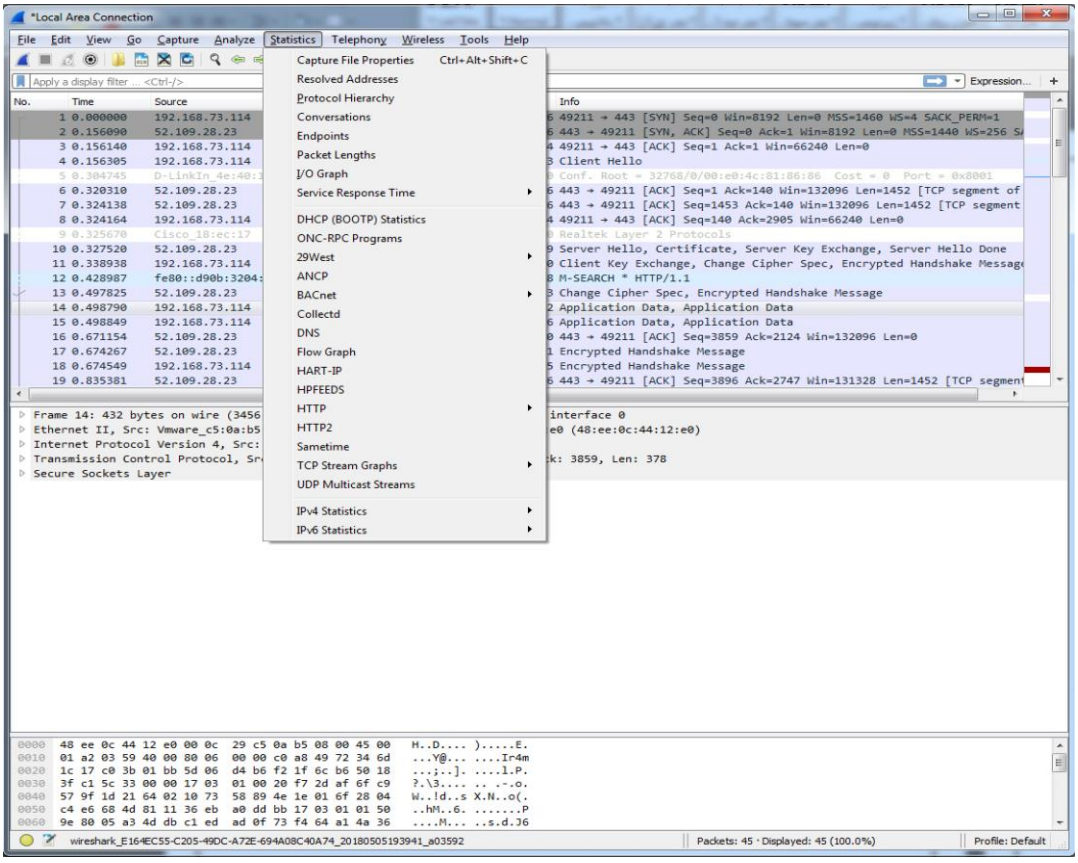
در این آزمایش قصد داریم آشنایی بیشتری با نرم‌افزار Wireshark و منوی Statistics در آن پیدا کنیم و از امکانات آن برای تحلیل بسته‌های جمع‌آوری‌شده استفاده نماییم.

1-2- فعالیت‌های قبل از آزمایش

دستور کار جلسه‌ی آشنایی با wireshark را مرور کنید.

1-3- 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.



شکل (1-1) زبانه Statistics

1. **بر روی گزینه‌ی Resolved Addresses کلیک کنید.**

سوال 1: **در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟**

مجموعه‌ای از mac-address ها و شرکت سازنده آن‌ها

سوال 2: **آیا می‌توانید سه بایت اولی که بـرای آدرس فیزیکـی کارت‌هـای شـبکه Cisco می‌باشند را مشخص کنید؟**

00:6 - 00:9

2. **بر روی گزینه‌ی protocol hierarchy کلیک کنید.**

سوال 3: **در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟**

لیست پروتکل‌ها براساس مدل لایه‌ای و درصد هرکدام

سوال 4: **چند درصد بسته‌های شما به یک ارتباط TCP بر روی بستر IPv4 تعلـق دارند؟**

۸۸ درصد

3. **بر روی گزینه‌ی Conversations کلیک کنید.**

سوال 5: **در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟**

اطلاعات نشست‌ها براساس پروتکل هرکدام(Ethernet, IPv4, IPv6, TCP, UDP)

4. **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.**

Address A(مبدأ): 192.168.1.33

Port A(مبدأ): 2933

Address B(مقصد): 185.211.88.131

Port B(مقصد): 443

5. **بر روی گزینه‌ی endpoints کلیک کنید.**

سوال 6: **در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟**

لیست آدرس مقصدها به‌همراه پورت آن‌ها، تعداد بسته‌ها و حجم اطلاعات ارسال و دریافت‌شده

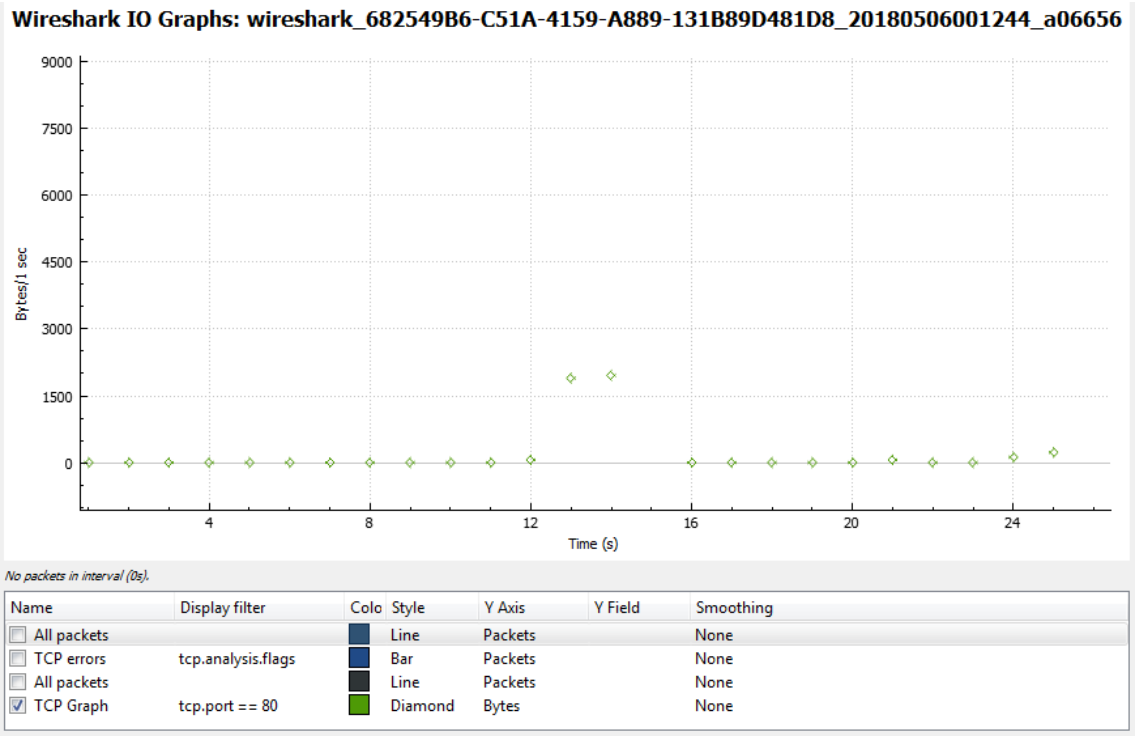
سوال 7: **چه مقصدهایی برای ارتباط‌های TCP در سیستم شما استفاده شده‌اند؟**

آدرس سایت‌های مراجعه‌شده و آدرس IP محلی(local)

سوال 8: **آیا می‌توانید از زبانه Ethernet و از روی تعداد بسته‌های مبادله شده، Default Gateway شبکه خود را تشخیص دهید؟**

بله، از آن‌جایی که تمام اطلاعات از Default Gateway عبور می‌کنند، آدرسی که بیشترین تعداد بسته مبادله‌شده را دارد، Default Gateway شبکه خواهد بود.

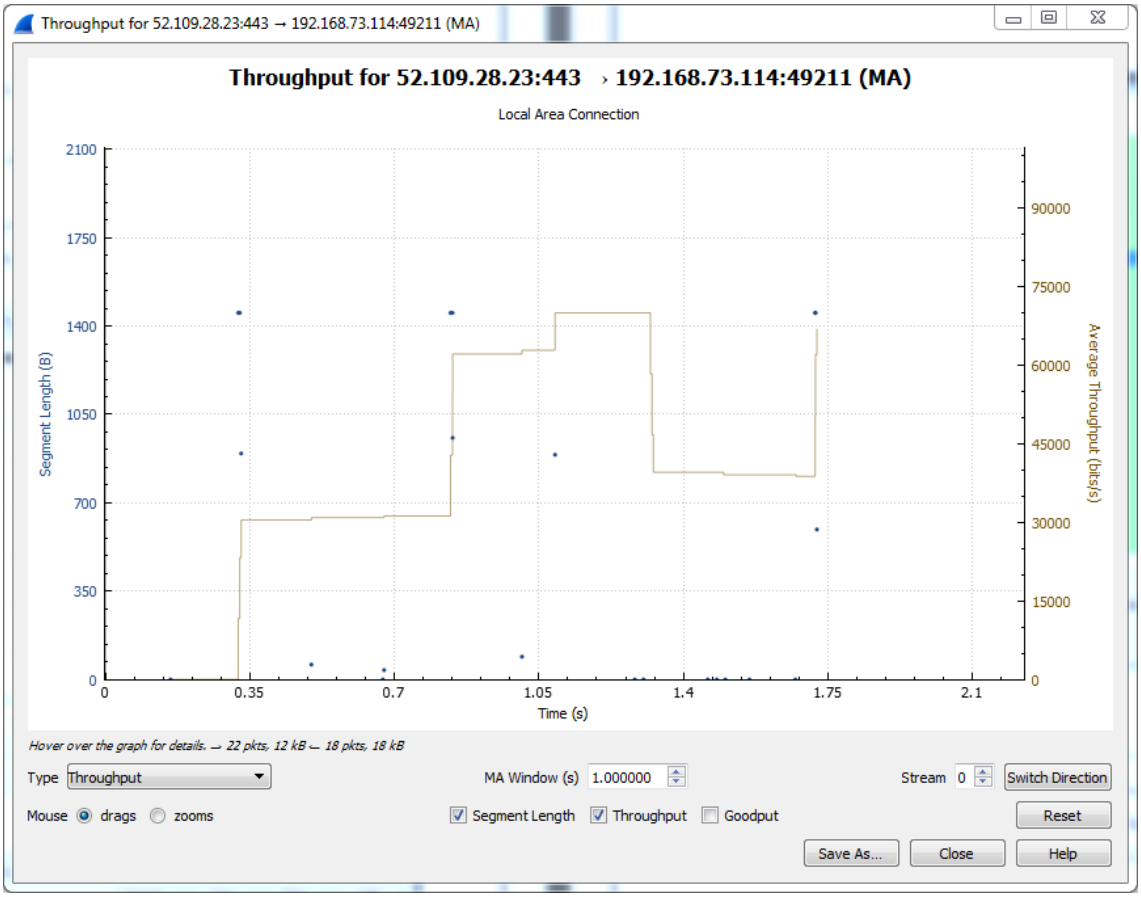
6. **بر روی گزینه‌ی I/O Graph کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید نرخ I/O را مشاهده کنید. شما می‌توانید در این صفحه نمودارهای مختلفی بسازید. بر روی دکمه +در پایین پنجره باز شده کلیک کنید، سپس یک فیلتر به آن اضافه کنید تا نمودار تعداد بسته‌ها در ثانیه را مشاهده کنید. مشاهده می‌کنید که با کلیک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



شکل IO Graphs (1-2)

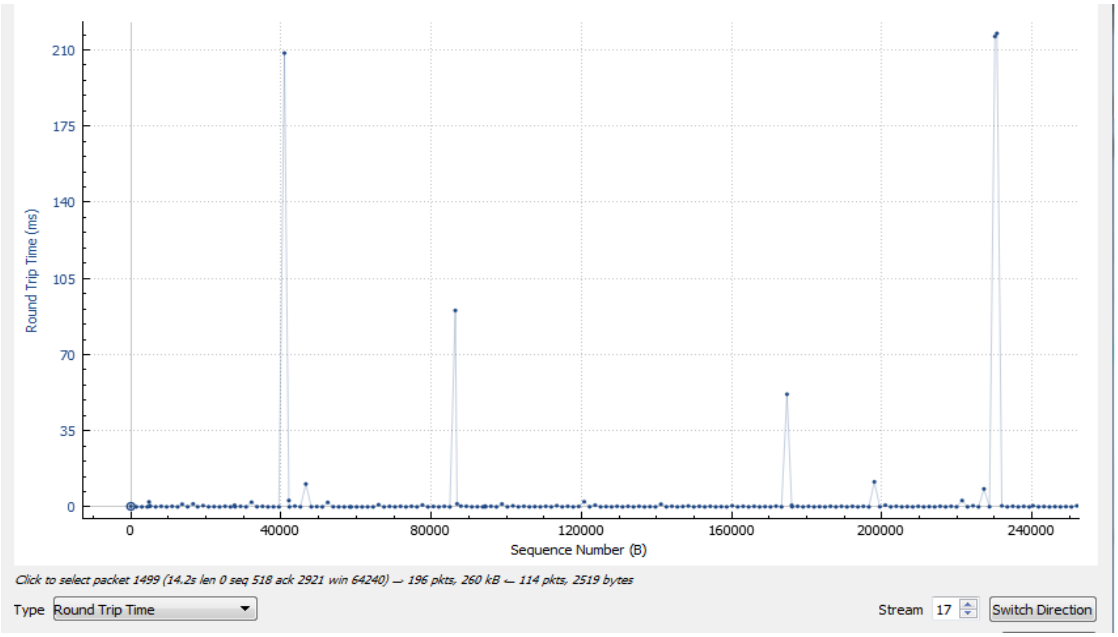
7. **بسته‌های مربوط به ارتباط با یک سایت را فیلتر کنید (با استفاده از Follow TCP Stream). سپس بر روی گزینه‌ی Flow Graph کلیک کنید. از منوی پایین، در بخش Show، Displayed packets را انتخاب کنید. به‌صورت کامل جزئیات مربوط به SeqNum و Ack و شماره پنجره را دنبال کنید.**

8. **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 (1-3) 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 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.**



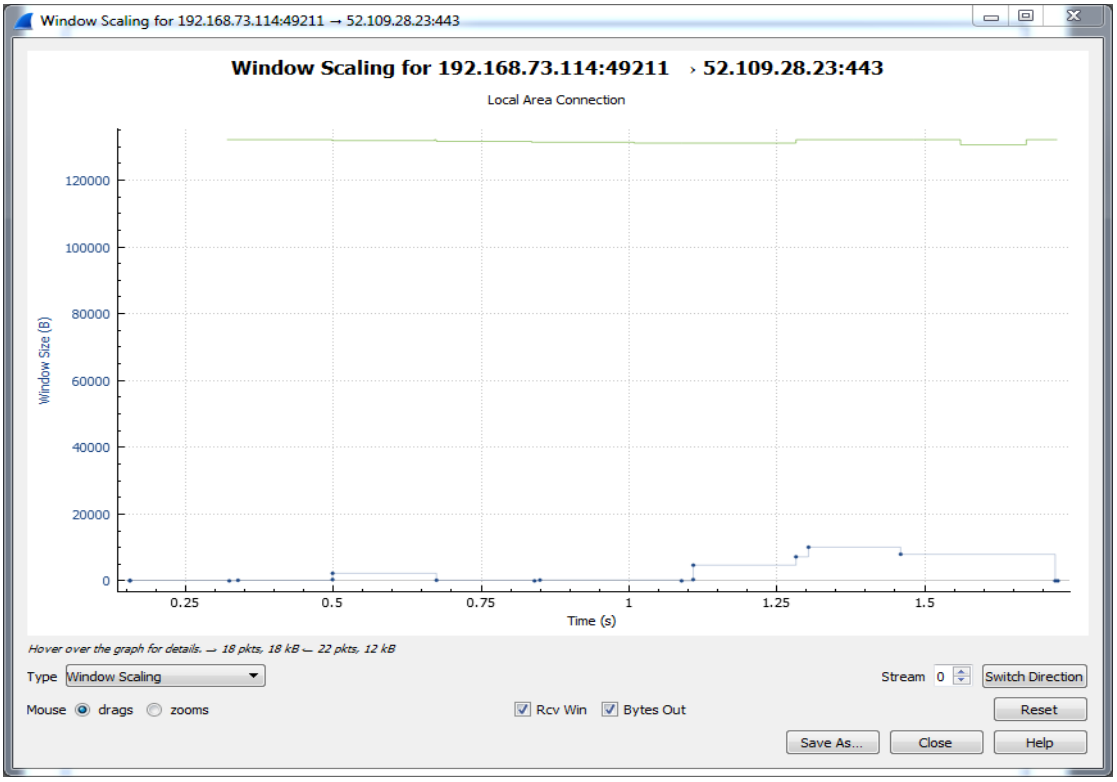
شکل (3-1) نمودار گذردهی

9. 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 (1-4)). 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.



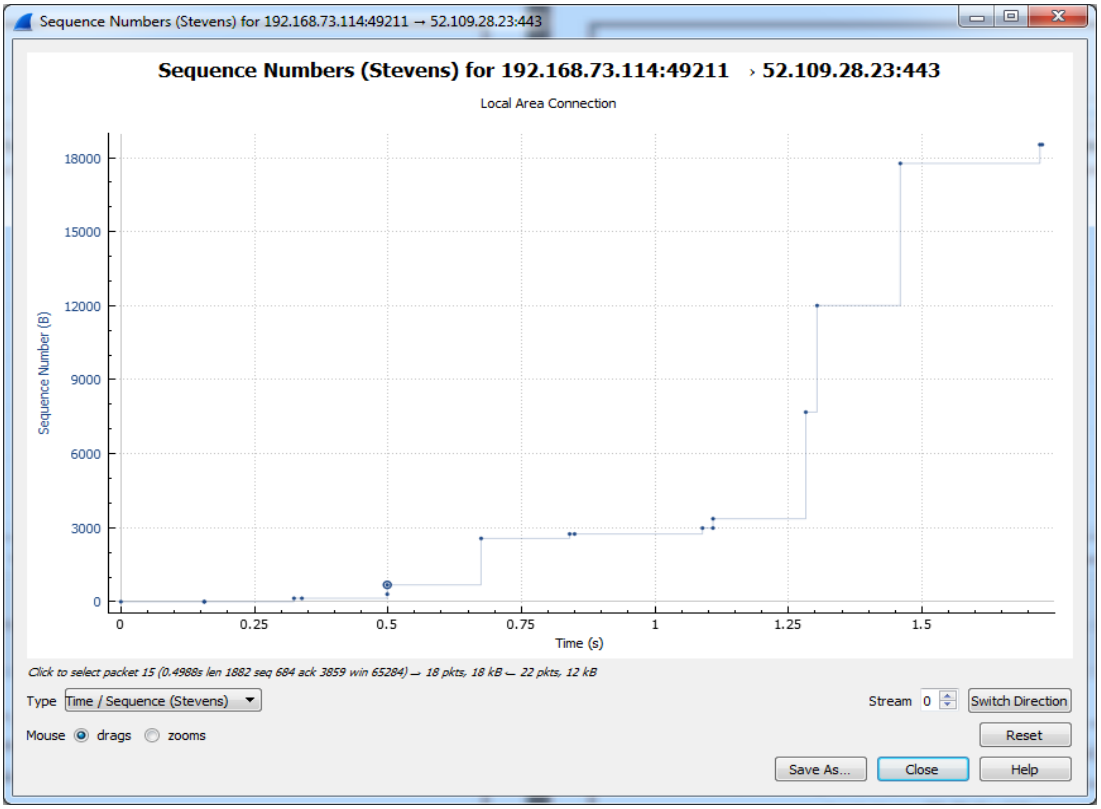
شکل (4-1) نمودار RTT

10. **بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Window Scaling کلیک کنید. پنجره‌ای مانند شکل (1-5) 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.**



شکل (5-1) نمودار Window Scaling

11. **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.**



شکل (6-1) نمودار Sequence Numbers

سوال 9: **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.

هر سه به‌صورت سینوسی کم و زیاد می‌شوند.

از آنجایی که محیط گرافیکی ممکن است قادر بـه نمـایش همـه بسـته‌ها نباشـد، Wireshark را در محیط خط فرمان از طریق دستور زیر اجرا کنید. ابتـدا بـه محـل 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. عـدد اینترفیسی که می‌خواهید بر روی آن شـنود کنیـد را یادداشـت کنیـد. بـه فـرض اینترفریس شماره 4 را انتخاب کرده‌اید. دستور زیر را اجرا کنید:

```
tshark –i 4 –p –w output.pcap
```

پس از آن بسـته‌ها شـنود می‌شـوند. درنهایـت Ctrl + C را فشـار دهیـد و فایـل output.pcap را با Wireshark باز کنید.