

به نام خدا

آزمایش شماره چهار

گروه 4



محمد جواد زندیه 9831032، محمد حسین اسدی 9831005

31 فروردین 1400

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

سوال یک: در پنجره Host نسبت دادن Name به Address IP را مشاهده می کنیم(کارت شبکه Host مورد نظر را نشان میدهد). در این بخش میتوان روی Ethernet Address و Ethernet Well-Known و Ethernet Manufacture فیلتر گذاشت برای Name ها و Address ها.

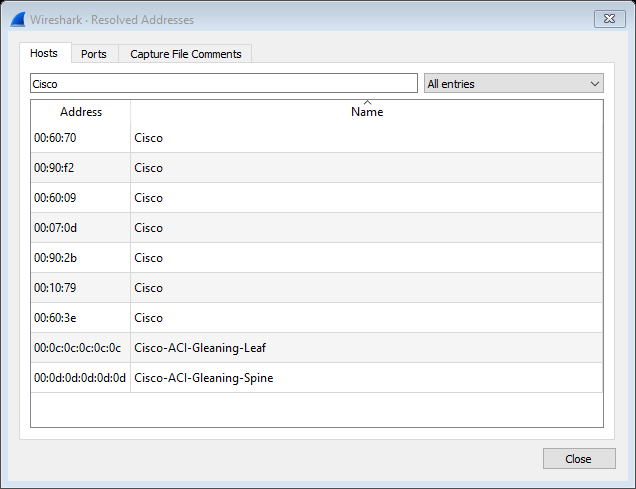
فقط قسمت Host است که از روی پکت های دریافتی بدست می آید و مابقی یک سری موارد از پیش تعریف شده اند.

در پنجره Port، بر اساس انواع پروتکل ها (tcp, udp, sctp, dccp) میتوان Port ها و Name های متناظر را بدست آورد.

سوال دو: کارت شبکه Cisco در شکل زیر قابل مشاهده است.

مثلا 00:60:70 چون نمایش بر اساس هگزا دسیمال است 3 بایت اول به صورت 00 و 60 و 70 می باشد

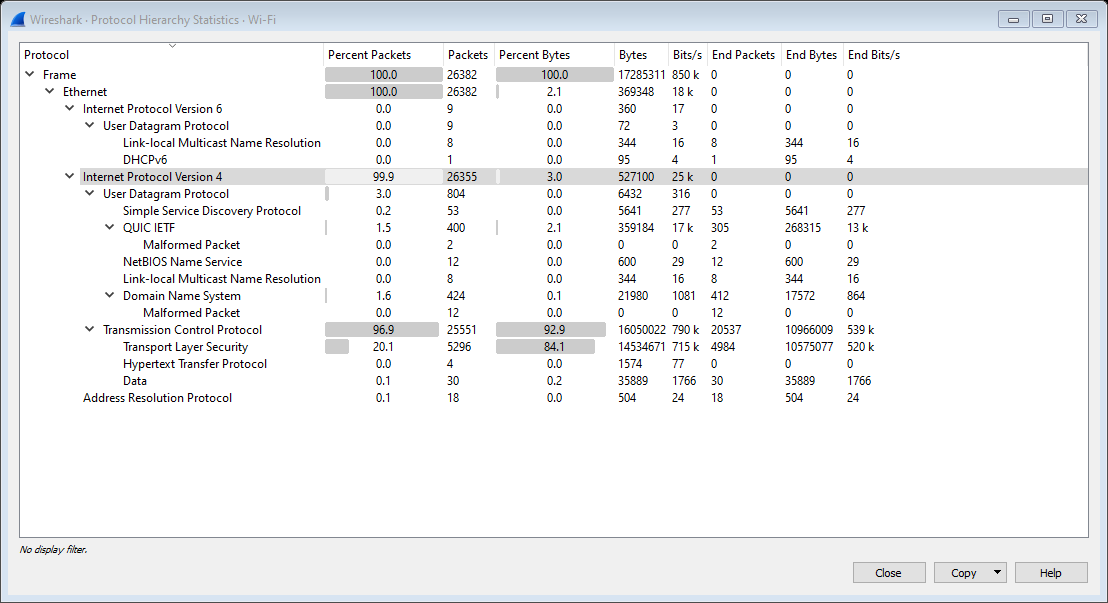
و ...



سوال سه: سلسله مراتب پروتکل بر اساس TCP/IP (لایه ای) را برای ما مشخص می‌کند. همچنین درصد استفاده از پروتکل ها در لایه های مختلف را به ما میدهد. ارزیابی از بستر هایی که پکت روی آنها می باشد هم میتوان انجام داد.

سوال چهار: 99.9 درصد از بسته ها لایه دوم شان روی بستر IPV4 می باشد.

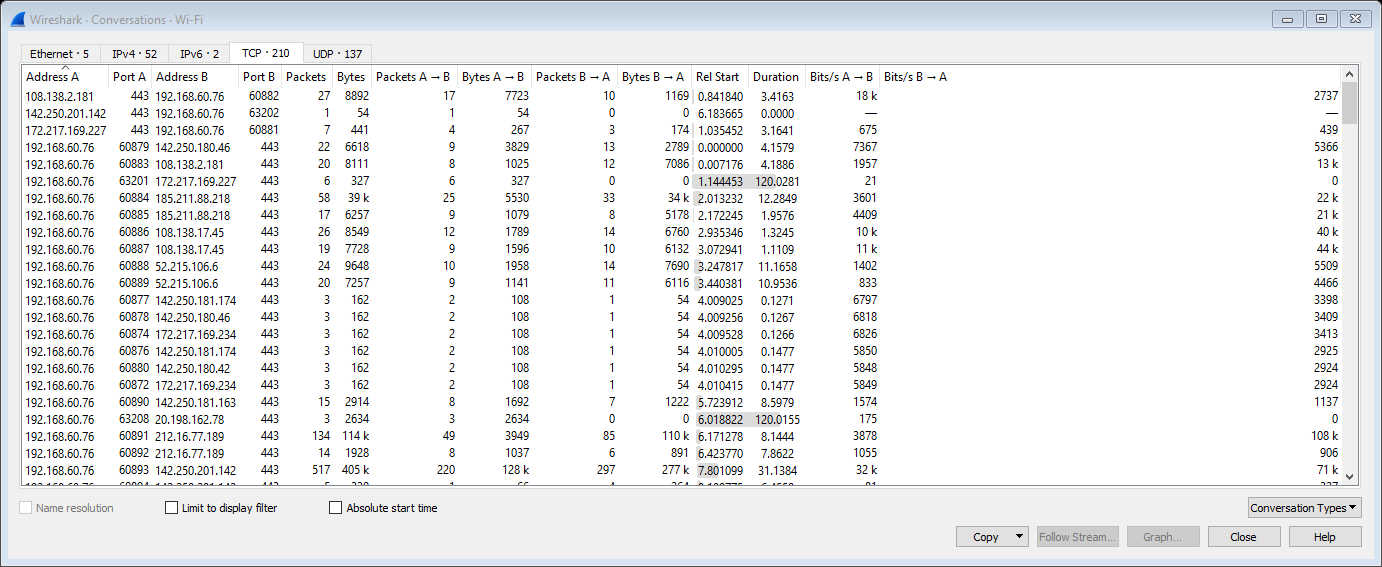
در شکل زیر قابل مشاهده است.



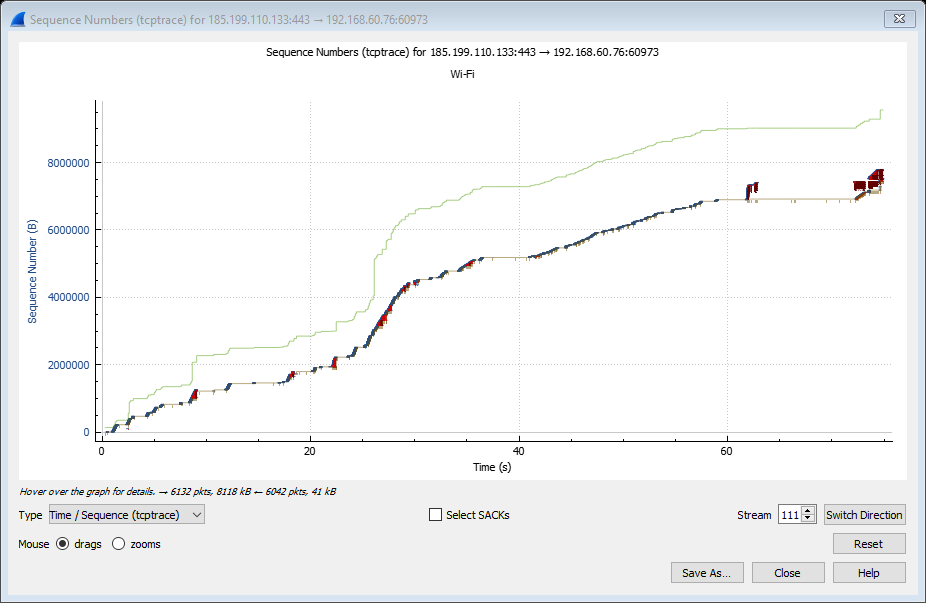
سوال پنج: نگاه Conversation به صورت گره به گره می باشد. بر اساس انواع پروتکل ها مشخصات مبدا و مقصد packet ها را مشخص می کند. مثلا در TCP پورت مبدا و مقصد و آدرس آنها را نشان میدهد. همچنین میتوان تعداد و طول پکت ها را مشاهده کرد.

در این بخش نشست ها را بر اساس Ethernet , Port, IPV6, TCP, UDP نشان میدهد. همچنین تعداد نشست ها نیز نشان داده شده است، مثلا برای TCP تعداد نشست ها 210 تا می باشد.

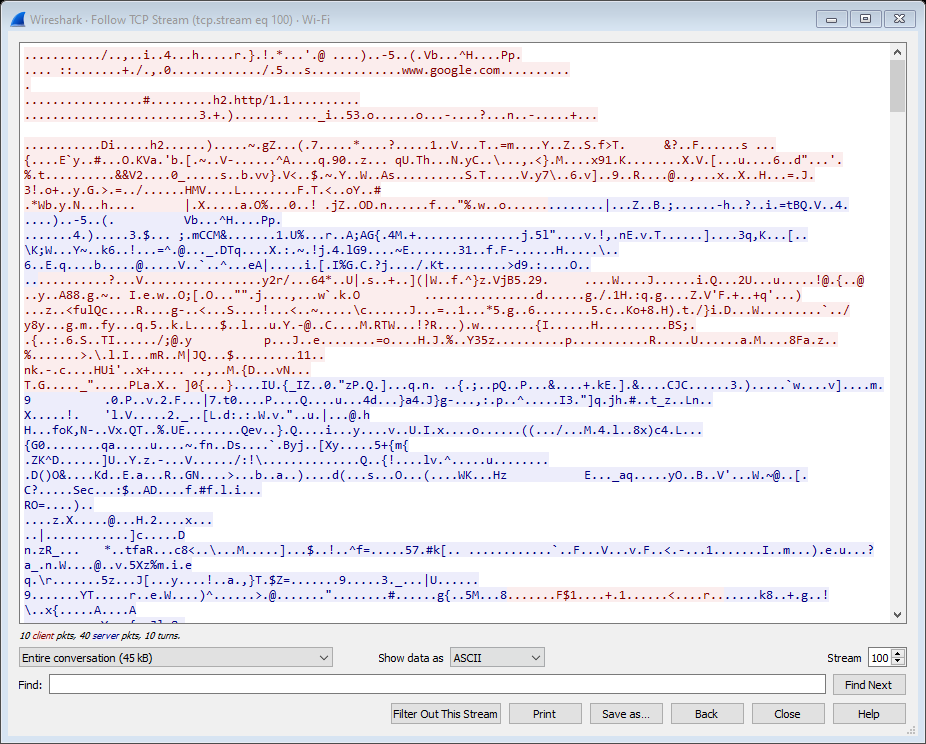
در قسمت TCP که در شکل مشاهده می شود، آدرس و پورت مبدا و مقصد را نشان داده است، به همراه جزئیات دیگر ...



با کلیک روی هر یک از نشست ها میتوان گراف انتقال پکت ها را مشاهده کرد. به عنوان مثال شکل زیر را مشاهده کنید.



همچنین میتوان در قسمت Fellow Stream محتوای پکت های ارسالی را به صورت ASCII و YAML و ... مشاهده کرد.



تعداد بسته های بیشتر دیفالت .. را نشان میدهد

هر چقدر شبکه بزرگ تر شود تعداد دیفالت .. بیشتر می شود

سوال شش: نگاهEnd point ارتباط به ارتباط است (تشخیص مبدا و مقصد)

در این قسمت مقصد هایی که با آنها در ارتباط بودیم مشاهده می شود.

مثلا برای قسمت TCP به صورت زیر می باشد:

Address: آدرسی که پکت باید به آن ارسال شود

Port: شماره پورت مقصد

Packets: تعداد پکت های رد و بدل شده

Bytes: مجموع بایت ها (طول) پکت رد و بدل شده

Tx packets: تعداد پکت های ارسالی از مبدا به مقصد

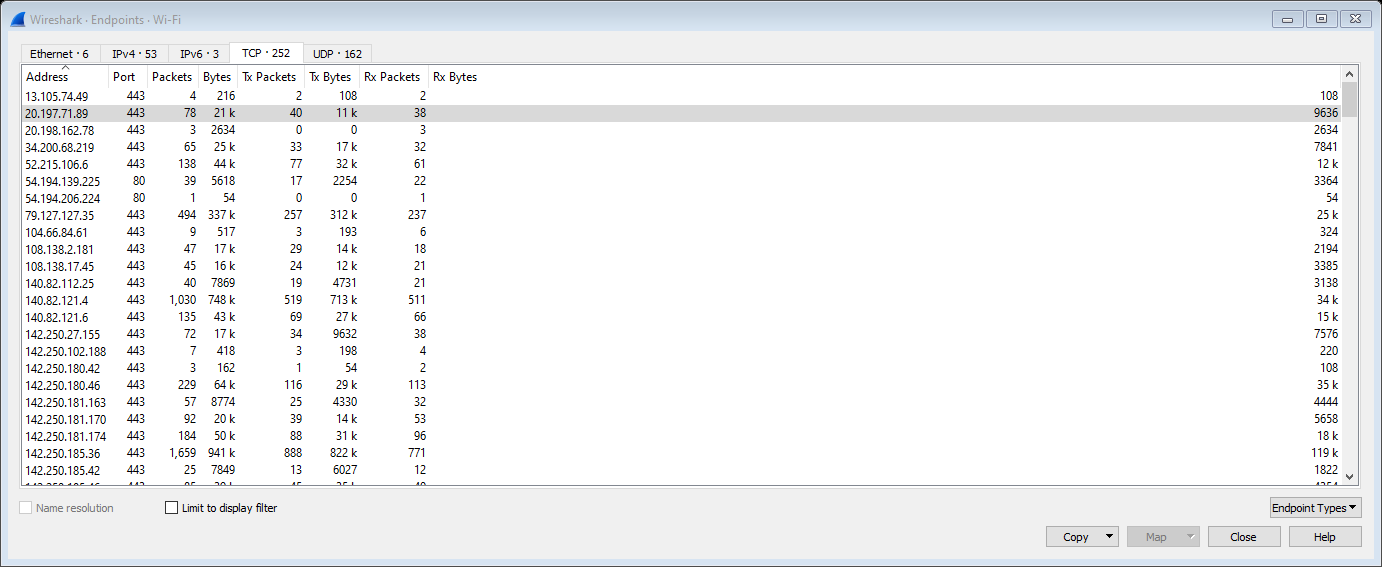
Tx Bytes: مجموع بایت های پکت های ارسالی

Rx packets: تعداد پکت های دریافی در مقصد

Rx Bytes: تعداد بایت دریافتی در مقصد

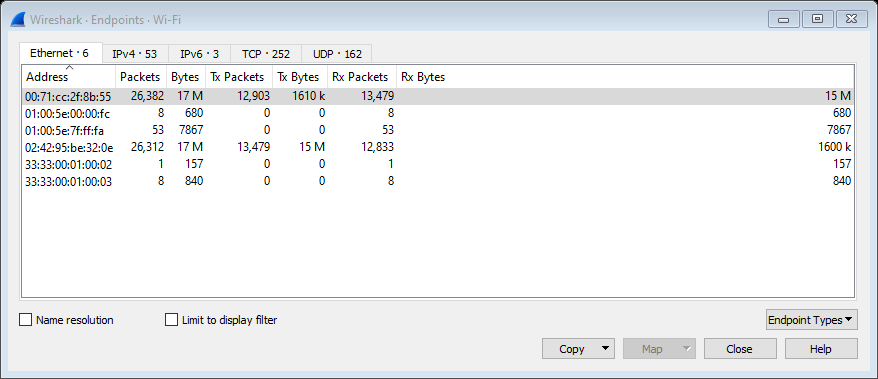
Tx Bytes + Rx Bytes = Bytes

Tx packets + Rx packets = packets



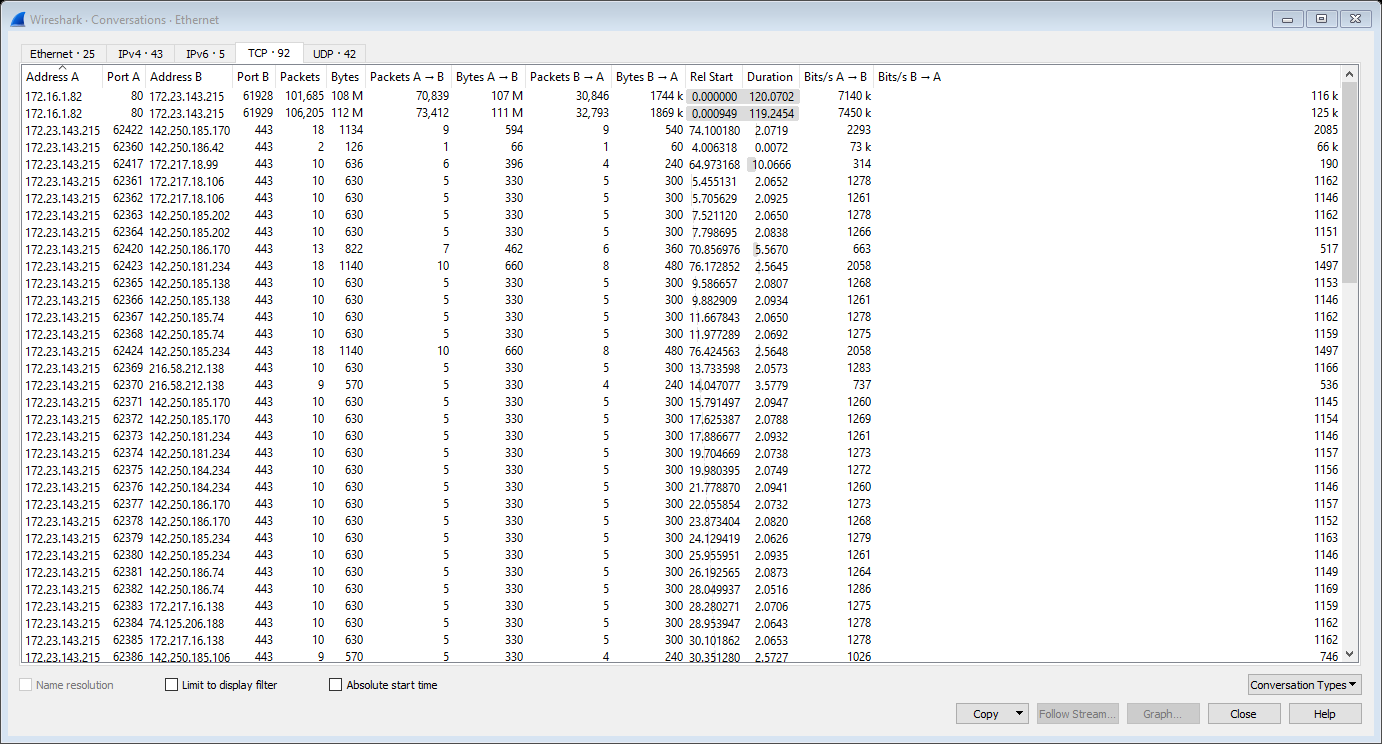
سوال هفت: مقصد های با پورت 443 و 80 و 60945 و ... مشاهده میشوند.

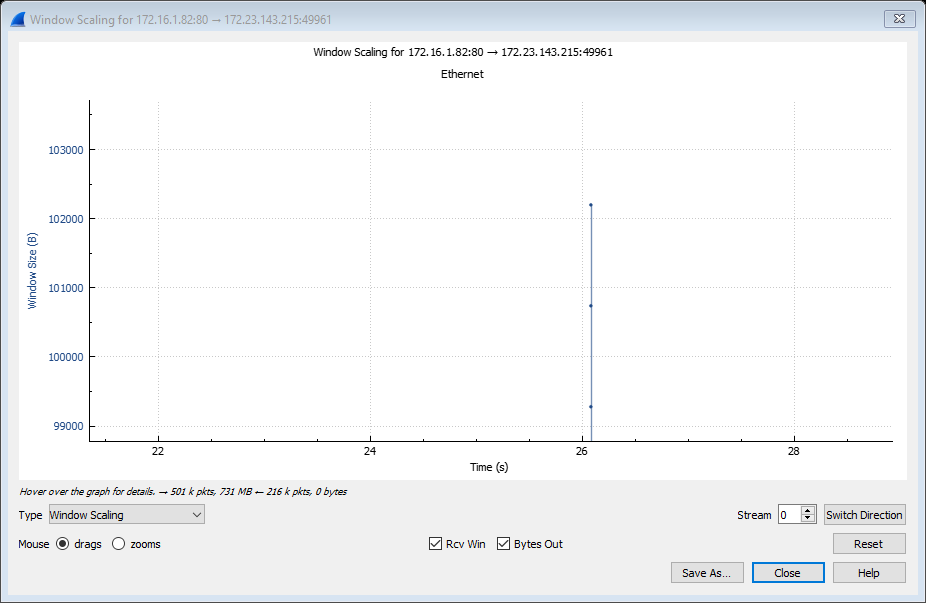
سوال هشت: برای خارج کردن بسته از شبکه از Default Gateway استفاده می شود. همچنین تعداد بسته های رد و بدل شده در Default Gateway بیشتر است. پس در منوی Ethernet آدرس های مقصدی که تعداد پکت های بیشتری به سمت آنها رفته است Default Gateway هستند. در شکل زیر میتوان دید که آدرس های 00:71;cc:2f:8b:55 و 02:42:95:be:32:0e دیفالت گیت وی هستند.

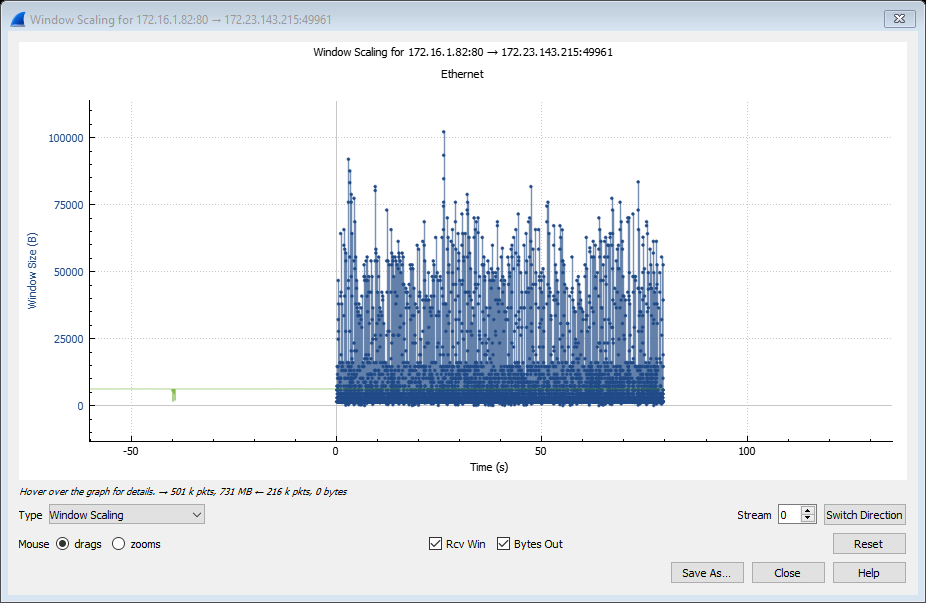


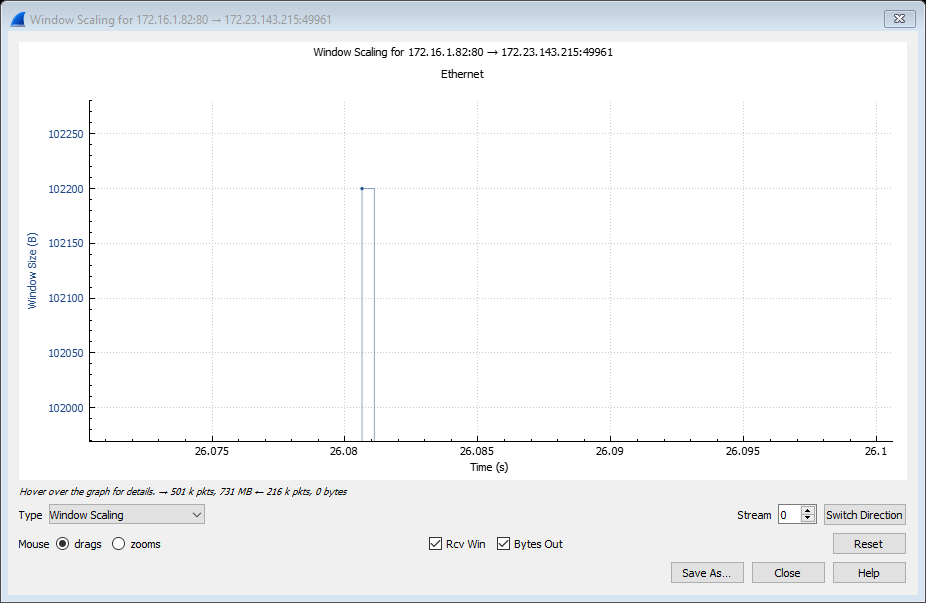
سوال نه:

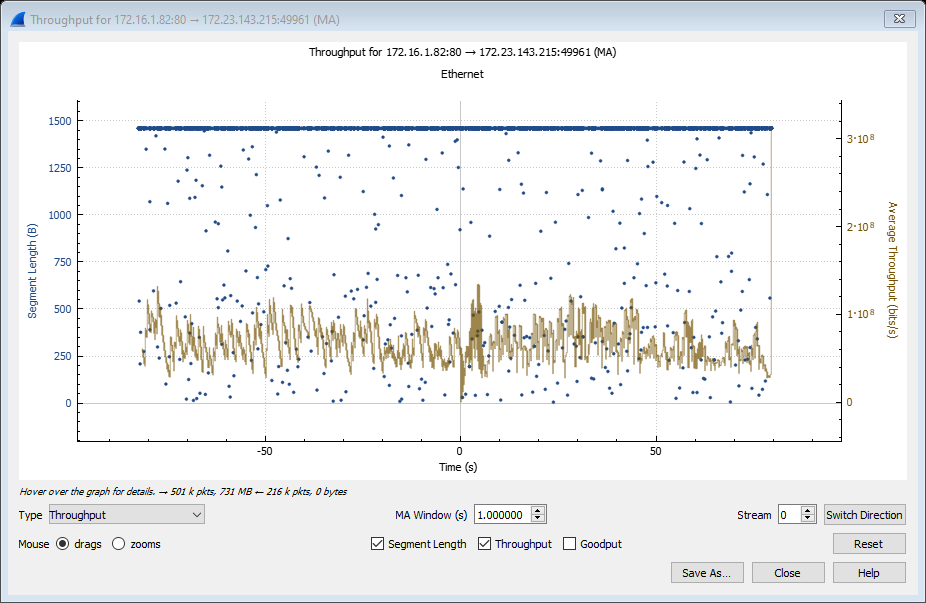
IP Address of AUT = 172.16.1.82

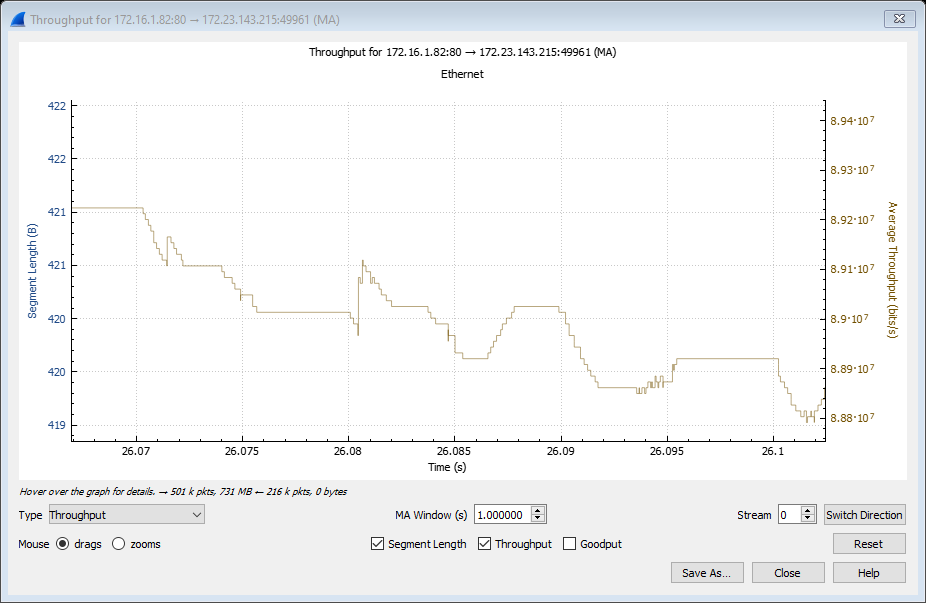




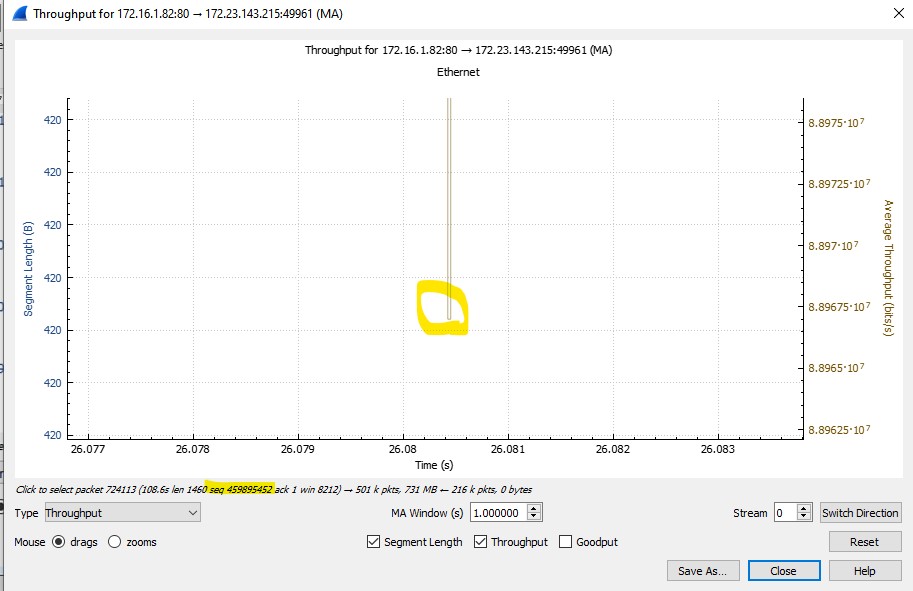








در نقاطی که مشخص کردیم، زمانی که RTT حداکثر باشد، یعنی ازدحام زیاد است پس Throuput کم شده است.



Seq number = 459895452