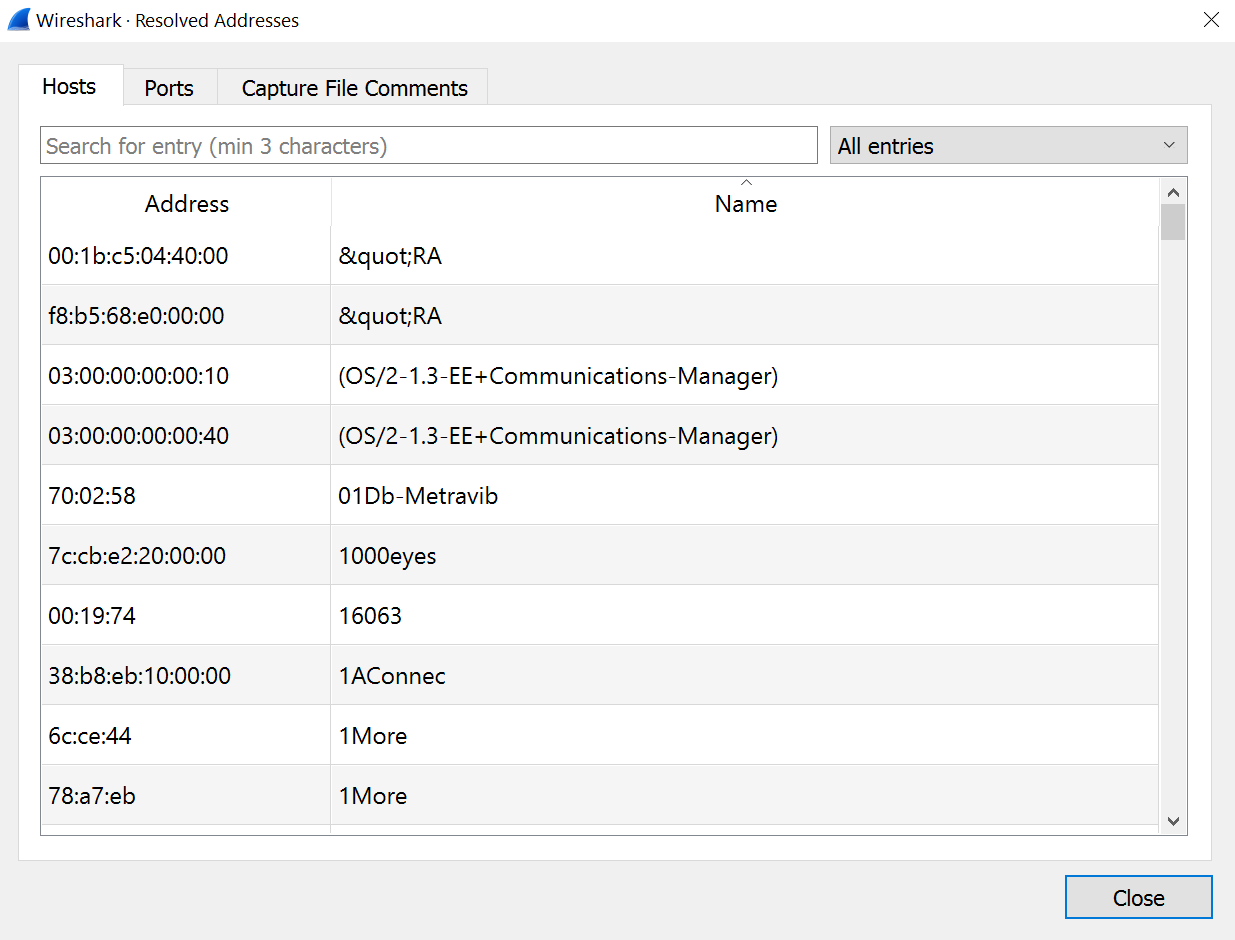
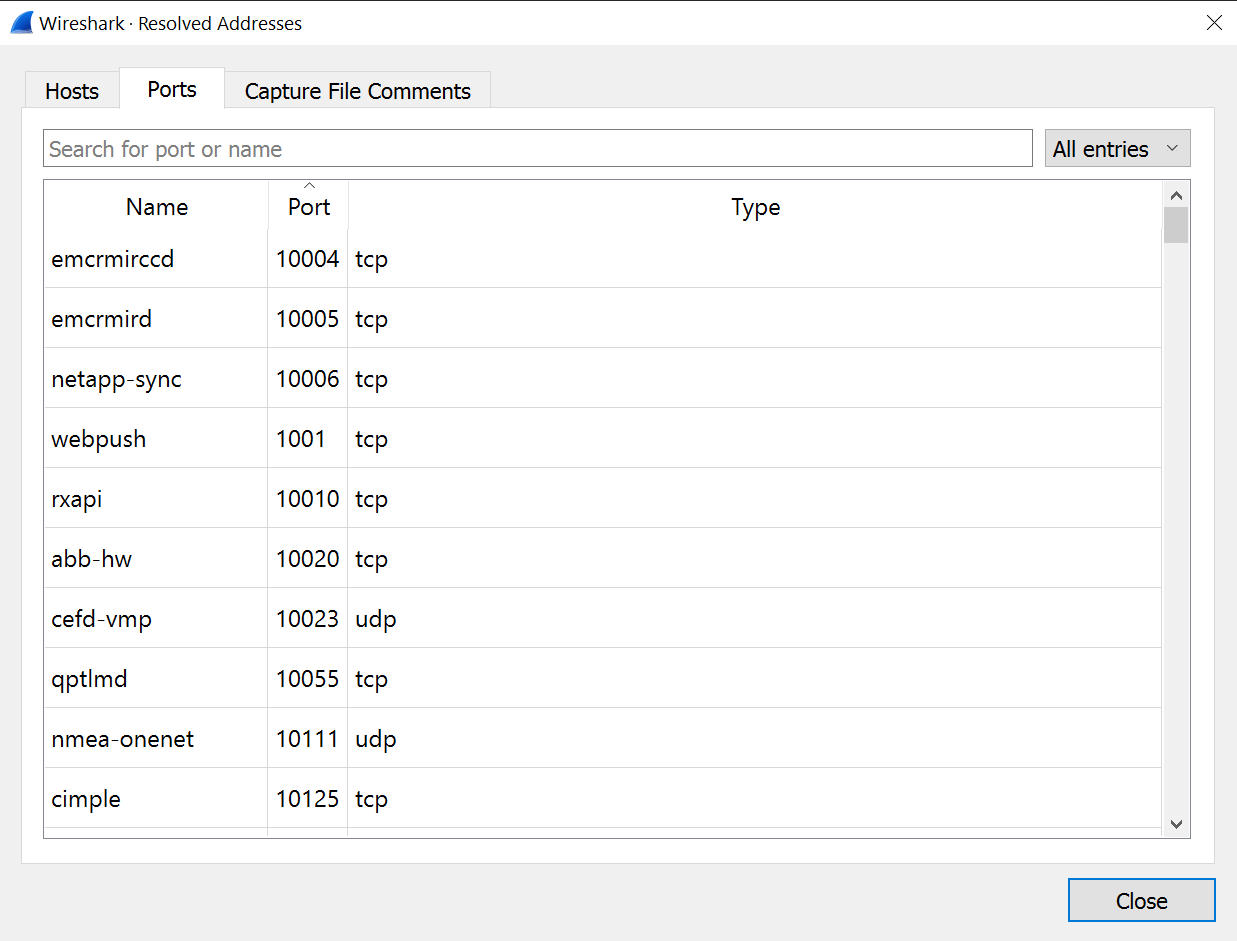
# سوال ۱

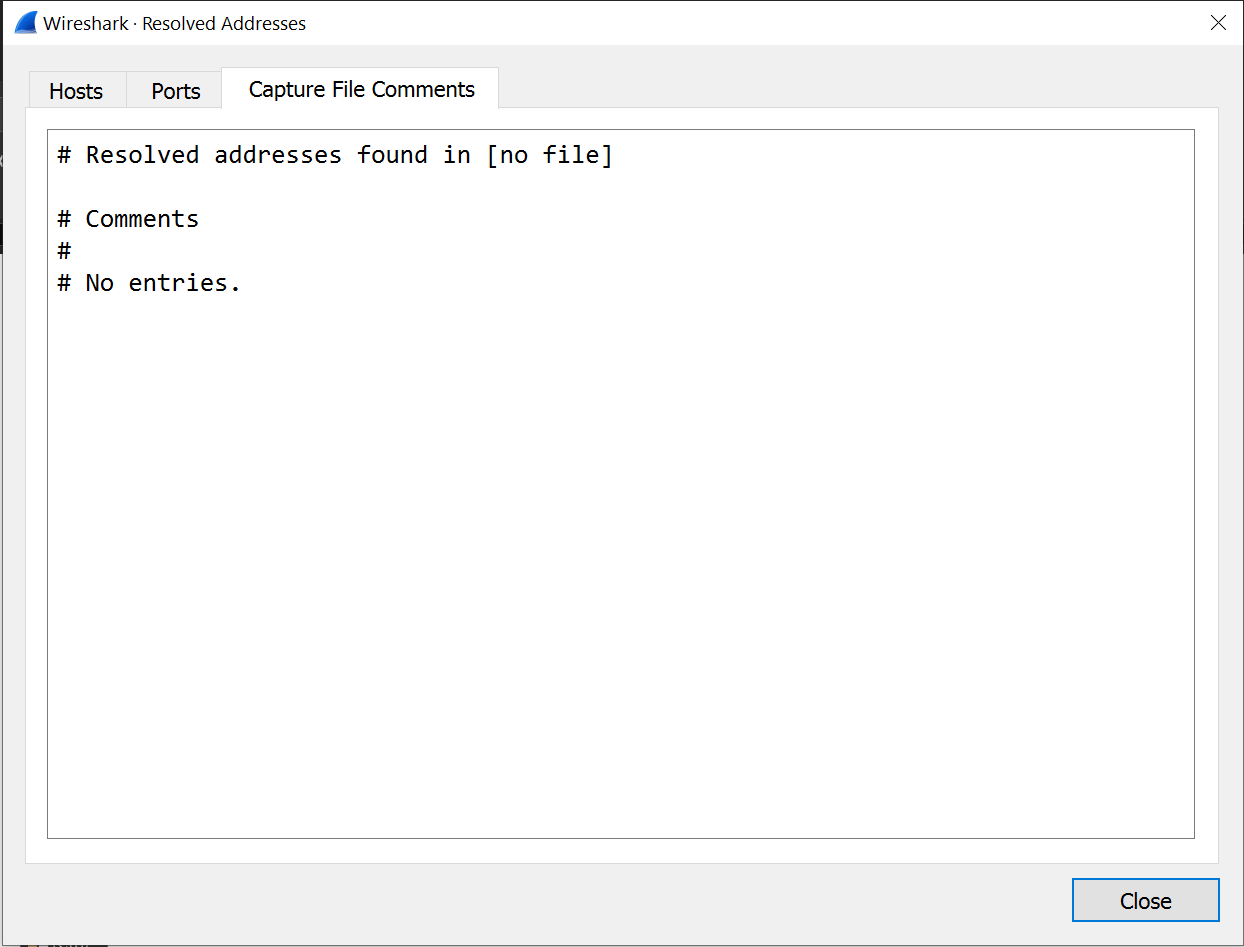
در قسمت hosts مشاهده میکنیم که در بسته هایی که capture کرده ایم ، ادرس ها ip یا آدرس های فیزیکی شبکه(انواع مختلف Ethernet addresses ) ها به چه اسم هایی map شده اند .( البته در بخش آدرس های فیزیکی Ethernet ، ۳ بایت اول آدرس قابل مشاهده است (.



در قسمت ports مشاهده میکنیم که پورت ها به چه اسم هایی map شده اند .در این قسمت قابلیت سرچ بر اساس DCCP,SCTP,UDP,TCP نیز وجود دارد ، اطلاعات این قسمت از قبل تعیین شده است و مانند اطلاعات مشاهده شده در بخش hosts به بسته های capture شده بستگی ندارد .

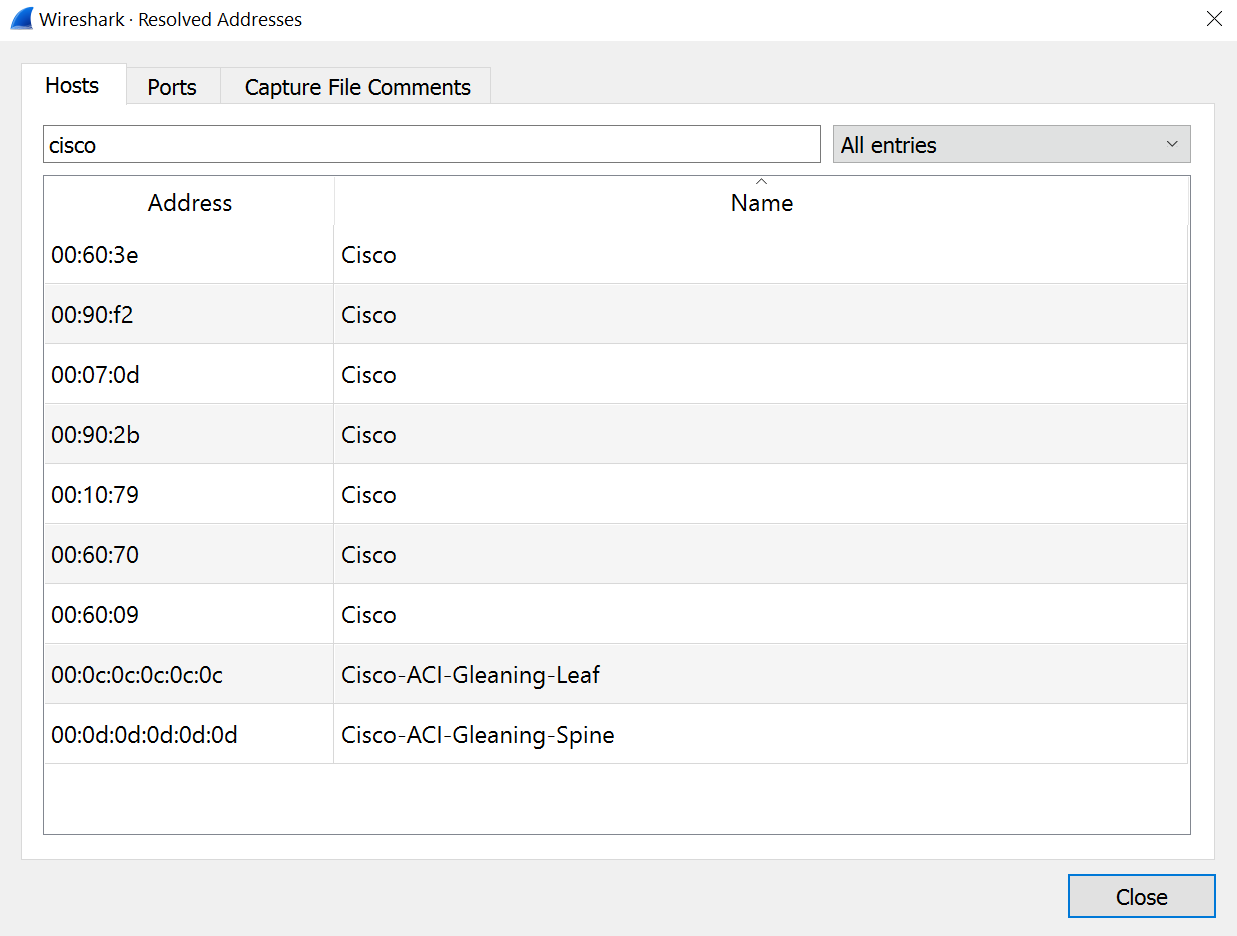


در قسمت capture file comments قادر به مشاهده اطلاعات و کامنت هایی درباره ی فایل هایی که آدرس های resolved شده در آن قرار دارند ، در اختیار ما قرار داده میشود .

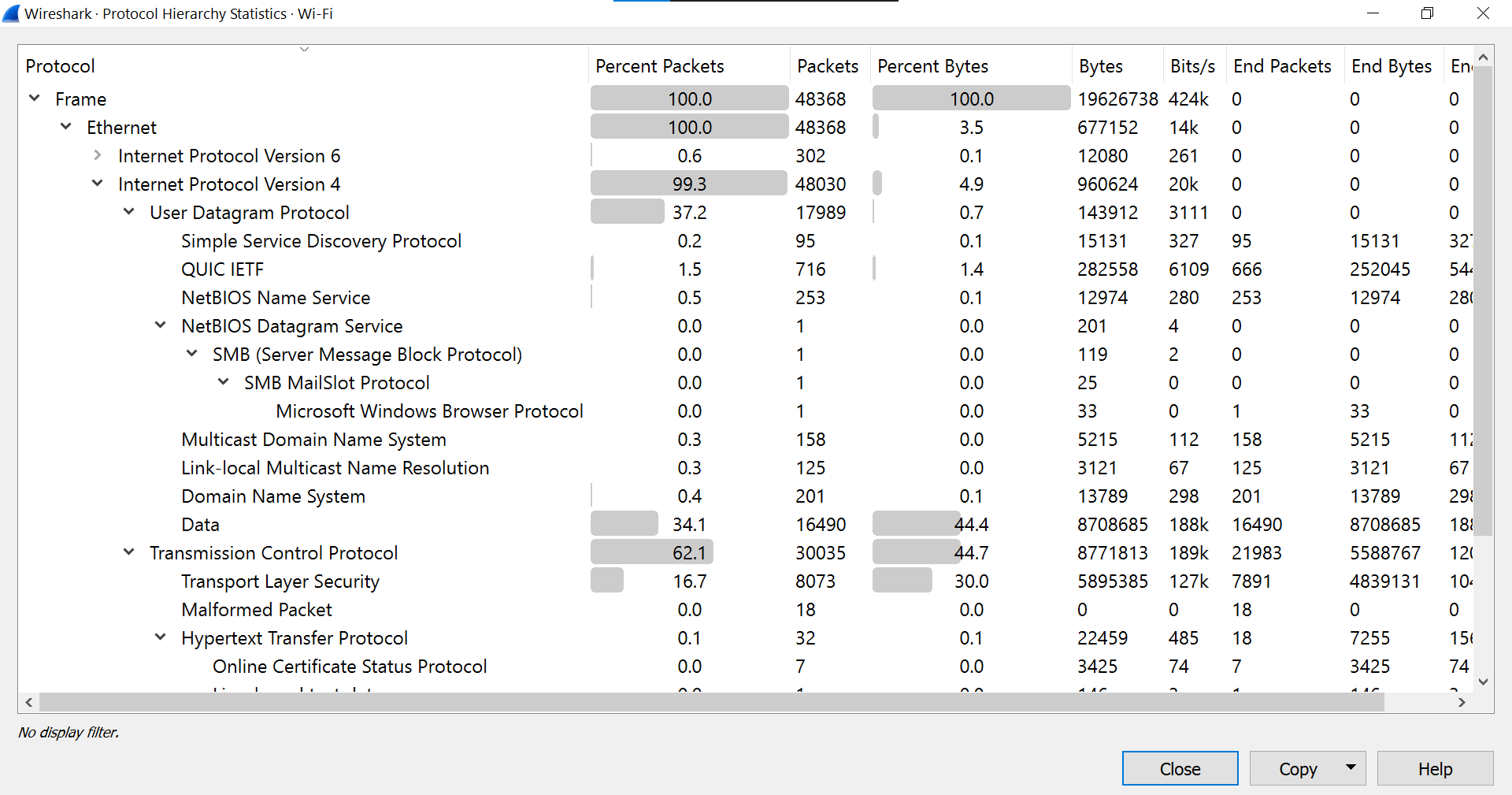


# سوال ۲

اطلاعات زیر مربوط به ۳ بایت اول کارت های شبکه ی cisco هستند . در تمام این موارد ، ۳ بایت اول در قسمت Address نمایش داده شده است .



# سوال ۳

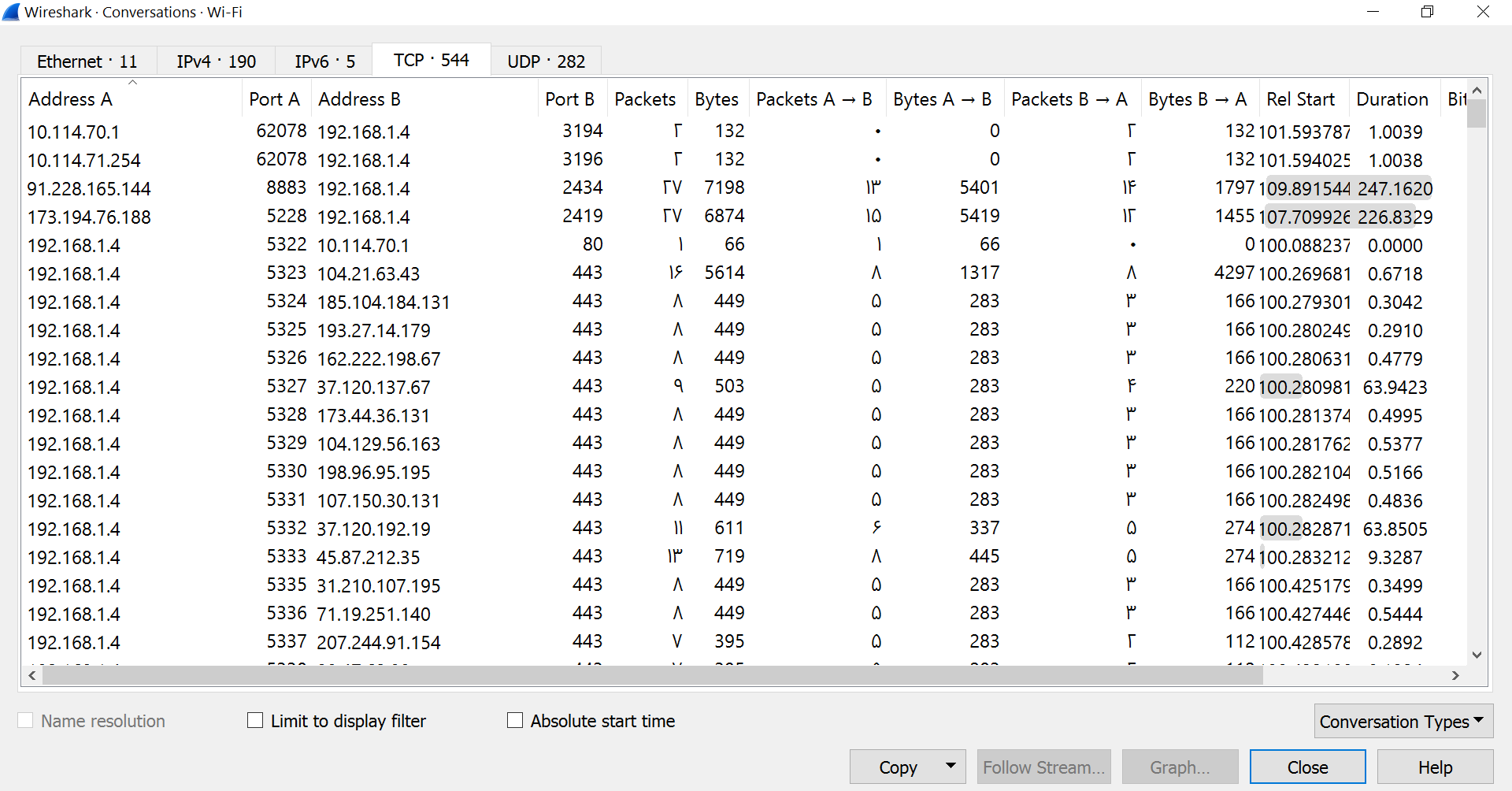


در این بخش آماری از سلسله مراتب protocol های لایه های مختلف بسته های capture شده مشاهده میکنیم . مثال در بسته های capture شده 100 % بسته ها در الیه ی link data از نوع Ethernet هستند و %99.3 بسته ها در لایه ی شبکه دارای پروتکل IPv4 هستند و همچنین از بین این بسته ها 37.2% آن ها در لایه ی انتقال دارای پروتکل UDP هستند و 62.1 %بسته ها در لایه ی انتقال دارای پروتکل TCP هستن و ... سایر اطلاعات آماری که همگی در این پنجره قابل مشاهده هستند .

# سوال۴

همانطور که در سوال بالا نیز توضیح داده شده ، در میان بسته های capture شده 100 %آن ها در لایه ی data link دارای پرتکل Ethernet هستند و تقریبا 100 %آن ها در لایه ی شبکه دارای پرتکل IPv4 هستند . همچنین از بین این بسته ها %62.1 آن ها در لایه ی انتقال دارای پروتکل TCP هستند . بنابراین حدودا (به این علت میگوییم حدودا که تقریبا 100 %بسته ها در لایه ی شبکه دارای پرتکل IPv4 بودند) ، 62.1 %بسته ها به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند .

# سوال ۵



اطالعات آماری مرتبط با اطالعات و نشست هایی که در زمان capture کردن بسته ها ایجاد شده اند به تفکیک پروتکل های الیه های مختلف و اطالعات مرتبط با هر پروتکل مشاهده میشود . برای مثال در قسمت TCP شماره پورت و آدرس های مبدا و مقصد ، تعداد بایت ها و بسته های جابجا شده زمان شروع و مدت زمان جابجایی بسته ها و نرخ جابجایی مشاهده میشود . در سایز tab های این صفحه نیز به همین ترتیب اطالعات مربوط به پروتکل های الیه های مختلف مشاهده میشود .

برای مثال در بخش Ethernet که در واقع مربوط به الیه ی 2 یعنی link data است اطالعاتی نظیر mac address ها و اطالعاتی مانند تعداد بایت ها و بسته های منتقل شده ، نرخ انتقال و ... قابل مشاهده است .

حال بنا به دستور کار یک نشست TCP را دنبال میکنیم :



در مورد انتخاب شده ، پورت مبدا 10767 با آدرس 192.168.1.4 و مقصد دارای پورت 80 با آدرس مقصد 136.243.44.15 است . تعداد بسته های منتقل شده 91 و تعداد بایت های منتقل شده ، 11k است . سایر موارد ذکر شده در سوال 5 نیز در این عکس قابل مشاهده هستند .

سپس stream follow را میزنیم و صفحه ی زیر نمایش داده میشود . (از نمایش ASCII استفاده میکنیم)



# سوال ۶

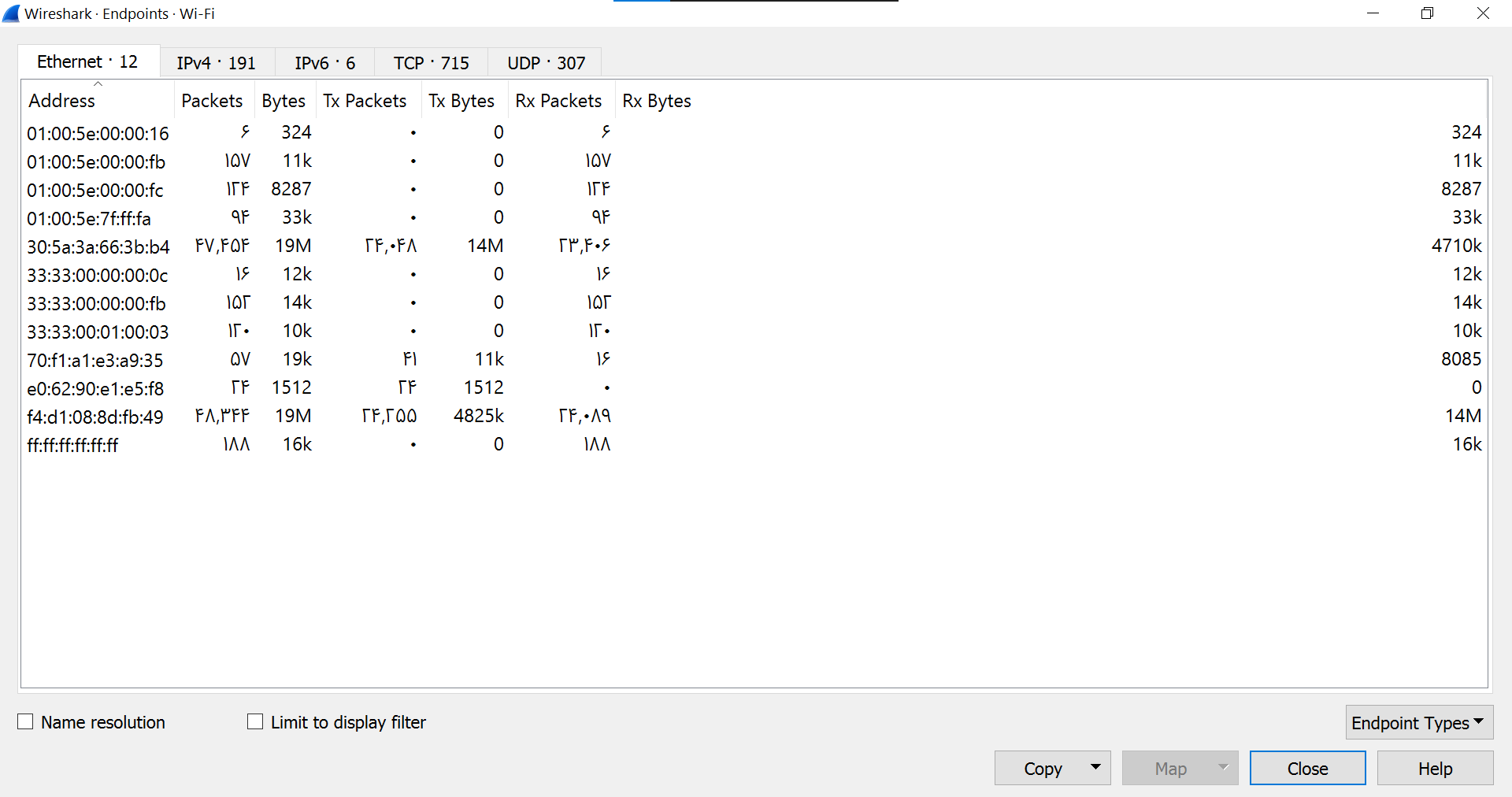
در صفحه ی باز شده که بخشی از آن در صفحه ی بعد قابل مشاهده است ، endpoint هایی که از طریق آن ها بسته هایی capture شده اند به تفکیک پروتکل های الیه های مختلف آن ها مشاهده میشود.

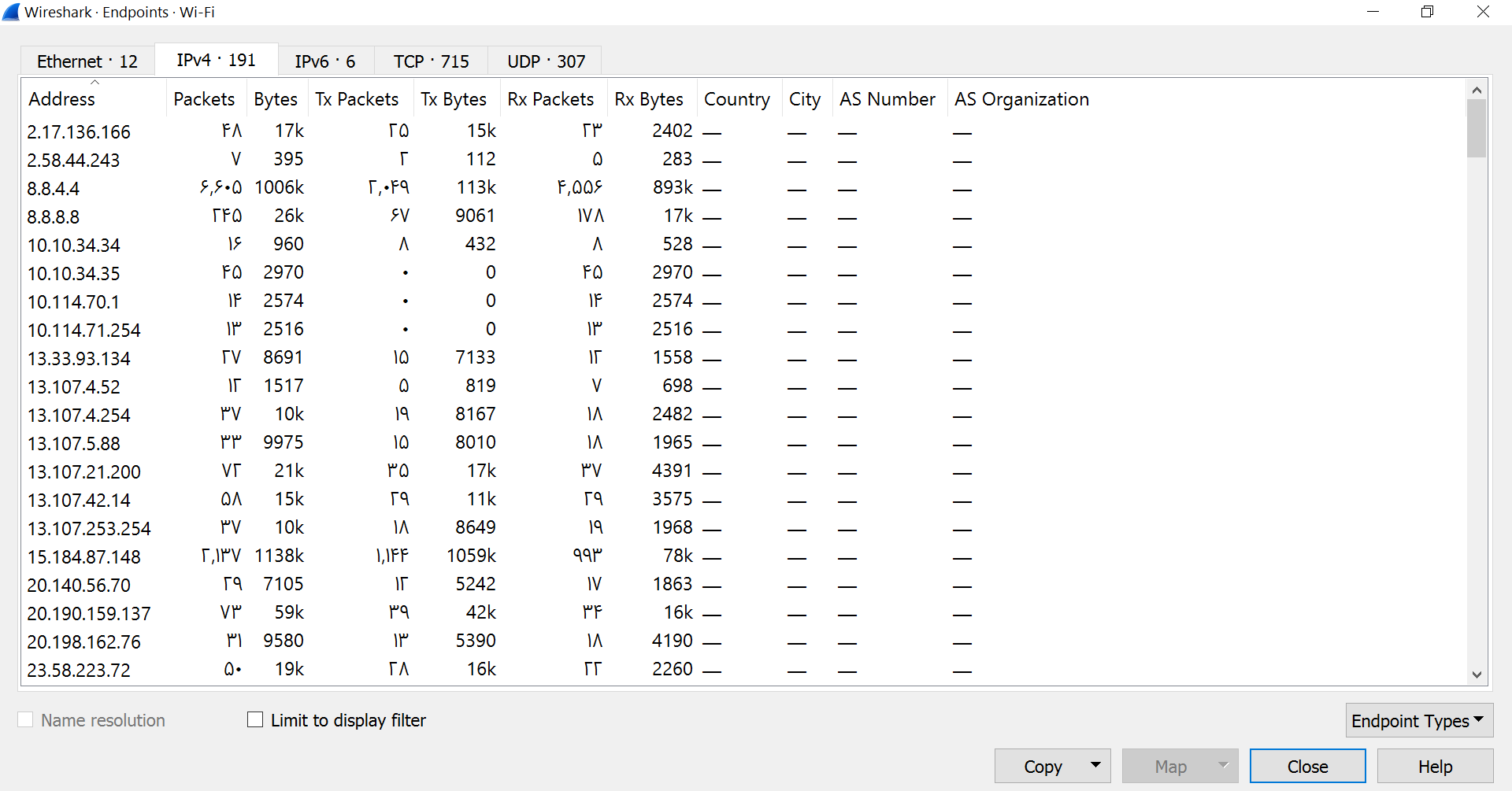
یا مثلا در بخش IPv4 که شکل آن نیز آمده است اطالعاتی نظیر تعداد بسته ها و تعداد بایت های منتقل شده و همچنین شهر یا کشوری که آن endpoint در آن قرار دارد قابل مشاهده است

(که البته در موارد capture شده اطالعات این 2 مورد موجود نبود (

یا مثال در بخش های TCP و UDP ، پورت و آدرس مقصد ، تعداد بایت های و بسته ها منتقل شده و... قابل مشاهده هستند .

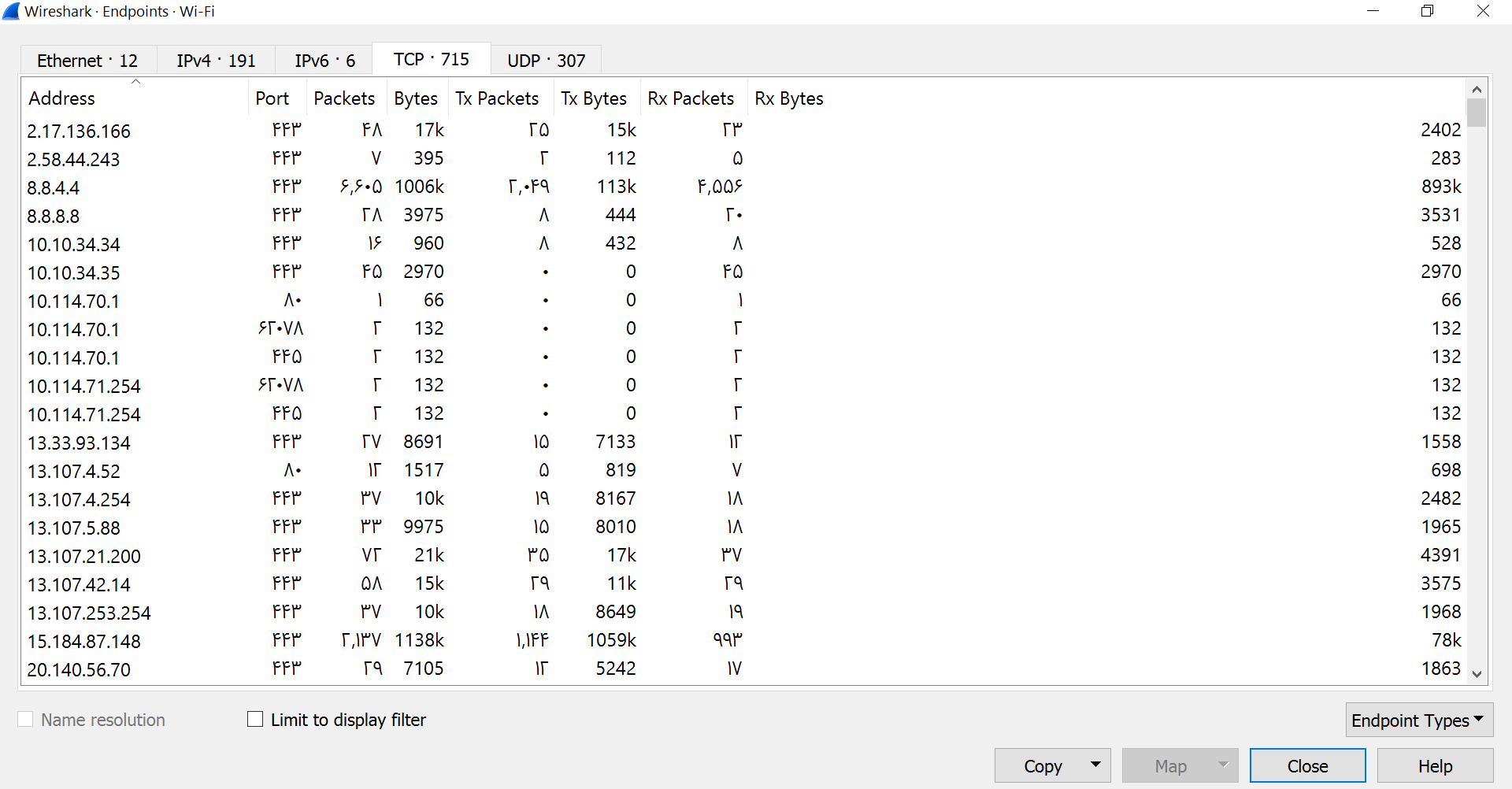
همچنین در تمام بخش ها بسته ها و بایت های Rx و Tx منتقل شده نیز قابل مشاهده هستند . دو بخش Ethernet و IPv4 نمایش داده شده اند .





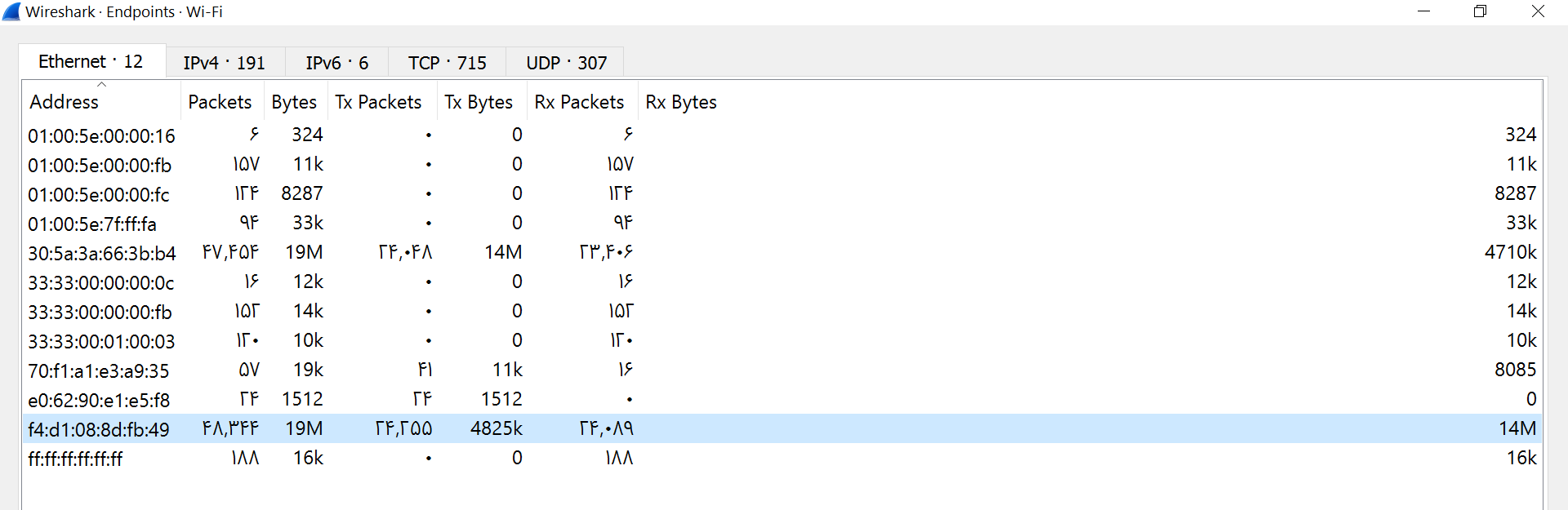
# سوال ۷

در قسمت TCP در پنجره ی endpoints آدرس IP مقصد هایی که در ارتباط TCP با سیستم من استفاده شده اند مشاهده میشود . که همانطور که در شکل صفحه ی بعد نیز مشاهده میشود ، تعداد مقصد های انتخابی 715 تا است .



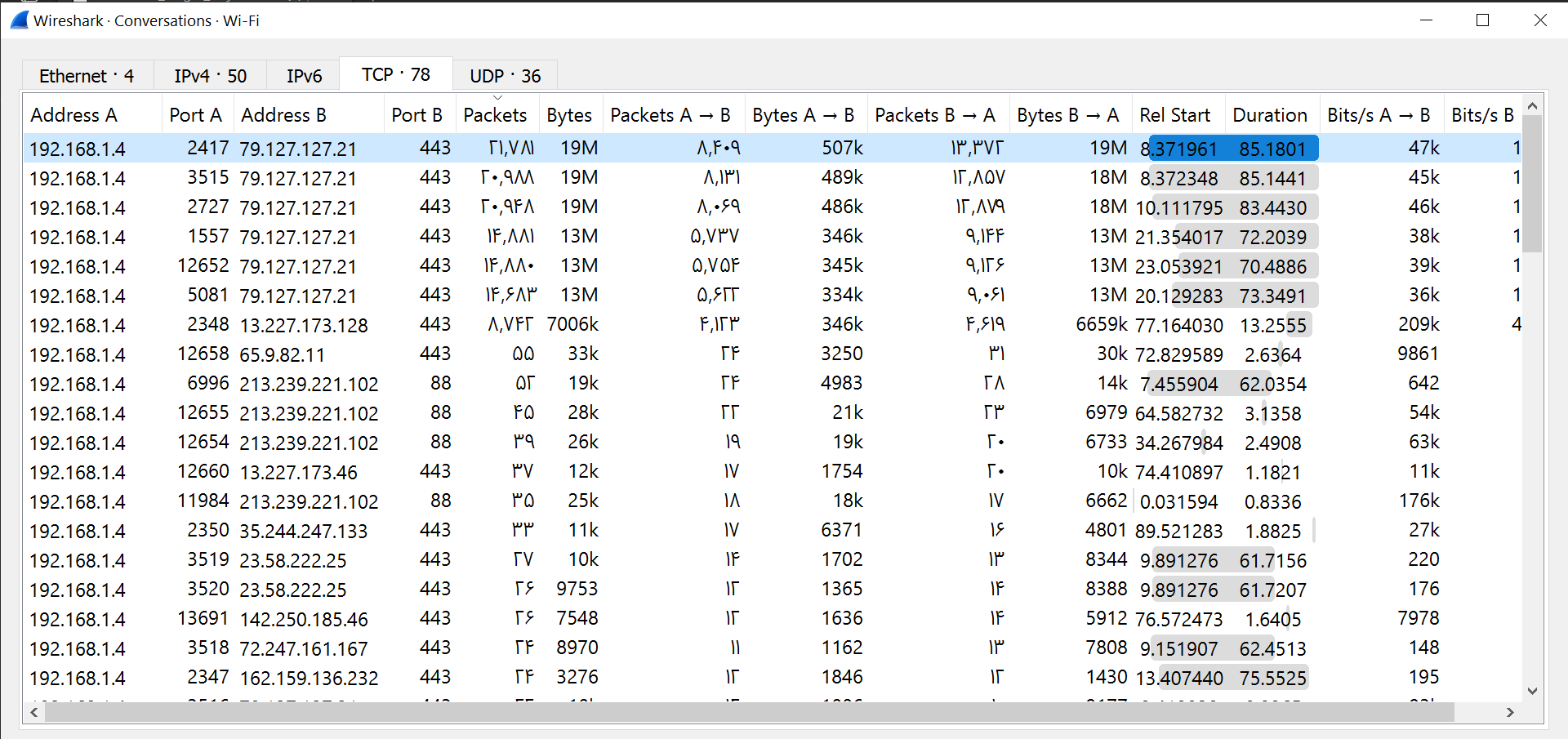
# سوال ۸

برای تشخیص default gateway باید به این نکته توجه داشته باشیم که در بخش Ethernet ، end point ای که بیشترین تبادل بسته با سیستم ما را داشته باشد به عنوان gateway default شناخته میشود )در این بخش MAC Address آن قابل مشاهده است(. که با توجه به شکل پایین این آدرس f4:d1:08:8d:fb:49 است و تعداد بسته های مبادله شده 48344 عدد و با حجمی برابر 19MB است .



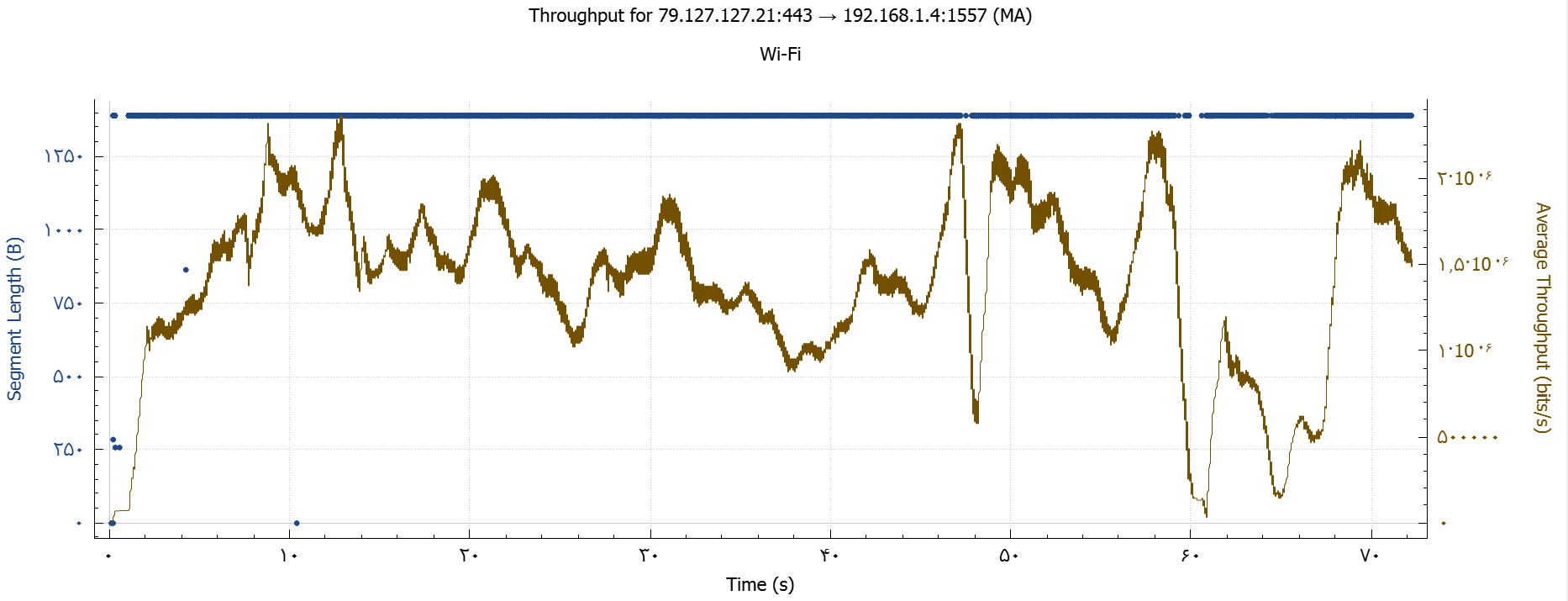
# سوال ۹

چون لینک داده شده را نتوانستیم استفاده کنیم از سایت soft98.ir استفاده کردیم. در conversation در بخش TCP تعیین میکنیم بیشترین پکت با کدام آدرس مبادله شده است.



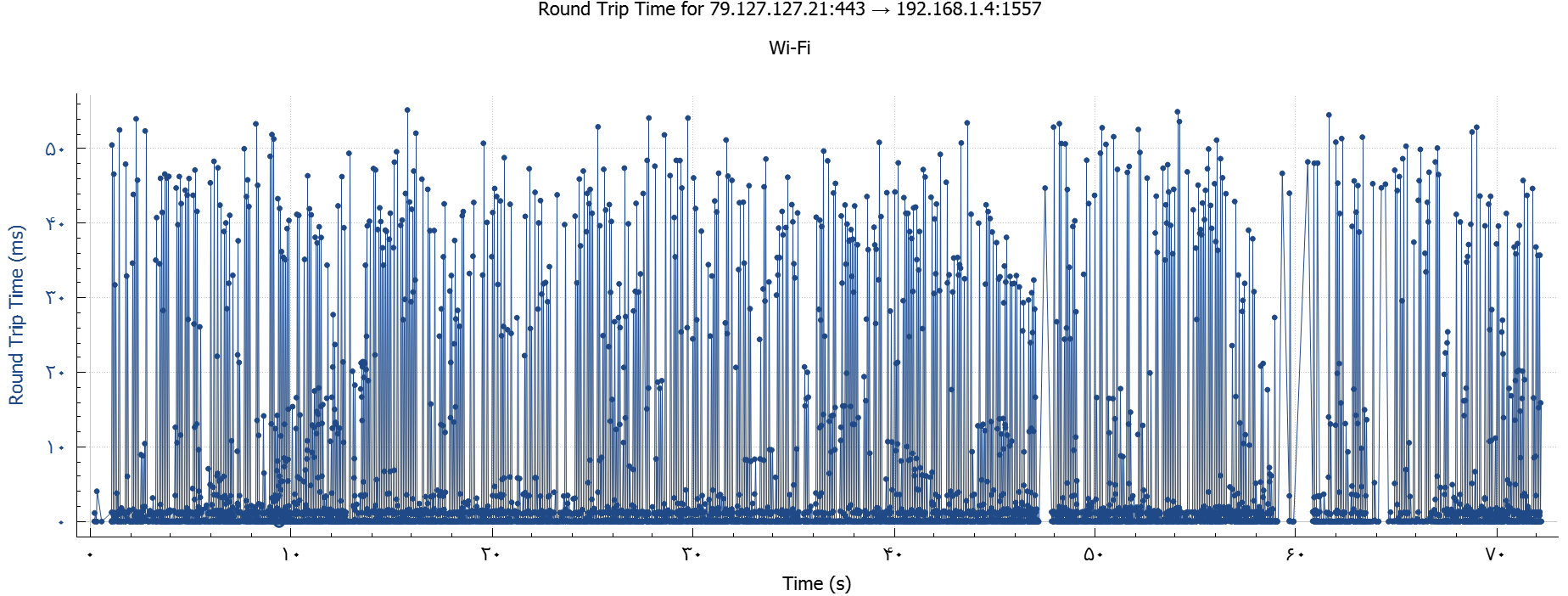
این آدرس برابر 79.127.127.21 بوده که مربوط به سایت soft98.ir میباشد.

## نمودار Troughout



مقدار آن میتواند متغیر باشد ولی همیشه از 1500 کمتر خواهد بود.

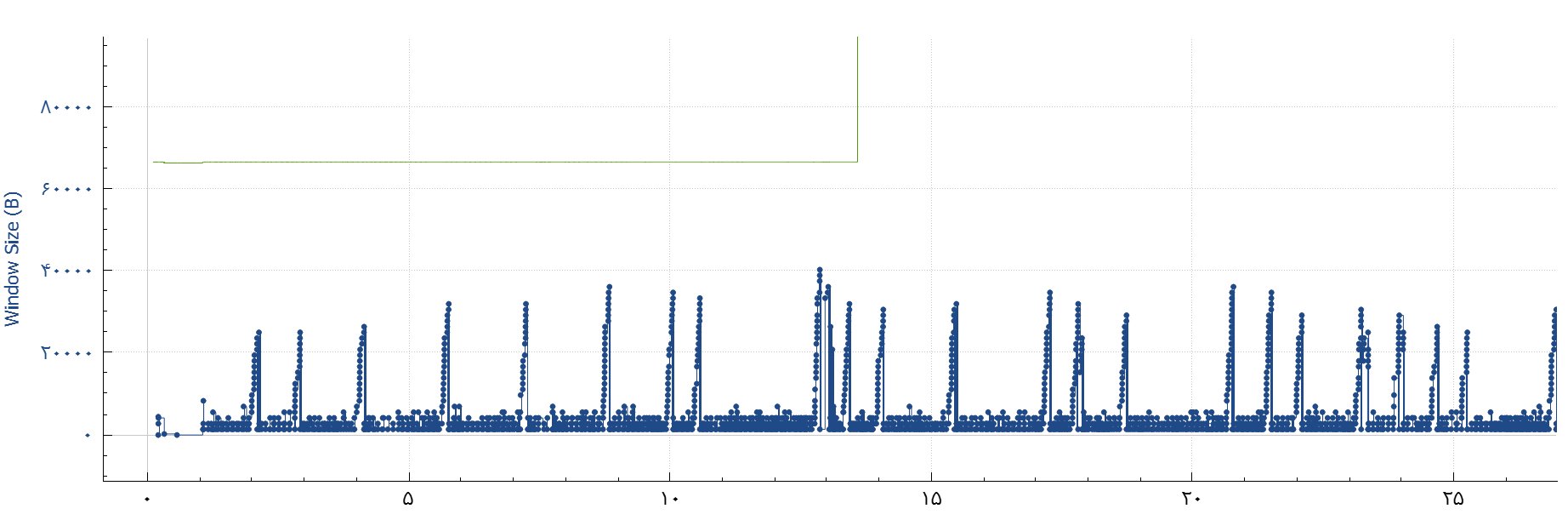
## نمودار RTT



در شرایط بدون ازدحام : اگر در شرایط عادی شبکه را شنود میکردیم نمودار خطی تقریبا ثابت بود به گونه ای که نمودار RTT تقریبا ثابت و نزدیک به صفر است که این موضوع بیانگر ارتباط مناسب اینترنت و با سرعت مناسب است و بنابراین در شبکه ازدحامی نداریم .

اما در شرایط ازدحام نمودار مانند نمودار شکل بالا است میبینیم که RTT در بازه های مختلف در حال تغییر است در نقاطی که ازدحام شبکه بالا است و بسته ها مجبور به طی کردن نود های میانی بیشتری برای رسیدن به مقصد هستند ، RTT افزایش می یابد ، اما در نقاطی که ازدحام تا حدی کم میشود مجددا RTT نیز کاهش می یابد اما به طور کلی مانند حالت بدون ازدحام ، روند ثابتی را دنبال نمیکند

## نمودار Window Scaling



در این نمودار مشاهده میکنیم که اندازه ی window رفته رفته زیاد شده(ابتدا در مودر slow start بوده ایم( تا به جایی میرسد که در شبکه نشانه هایی از ازدحام مشاهده میشود و حاالتی پیش می آید که فرستنده مجبور به ارسال مجدد بسته ها است . بدین ترتیب در این حالت که در شبکه ازدحام تشخیص داده شد ، اندازه ی window ناگهان کاهش داده میشود و همانطور که در شکل مشاهده میشود برای مدتی ثابت مانده و سپس کم کم افزایش داده میشود .