

به نام خدا

گروه ۳

اعضاي گروه:

فرشيد نوشی ۹۸۳۱۰۶۸

اميرحسين نجفي زاده ۹۸۳۱۰۶۵

تاریخ:

۷ اردیبهشت ۱۴۰۱ ساعت ۳۰:۳۰ تا

سوال ۱:

در این قسمت برای تمام بسته هایی که دریافت کردیم، مشخص شده است ادرس ها ip یا آدرس های فیزیکی شبکه (انواع مختلف Ethernet addresses) ها به چه اسم هایی map شده اند.

همچنین 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.

یک سری اطلاعات هم راجب فایل هایی که دریافت کردیم قابل مشاهده است.

سوال ۲:

سه بایت اول در قسمت آدرس ها مشخص شده اند. برای CISCO، پنج مورد اول عبارت اند از:

00:17:5a

00:03:32

00:d0:bb

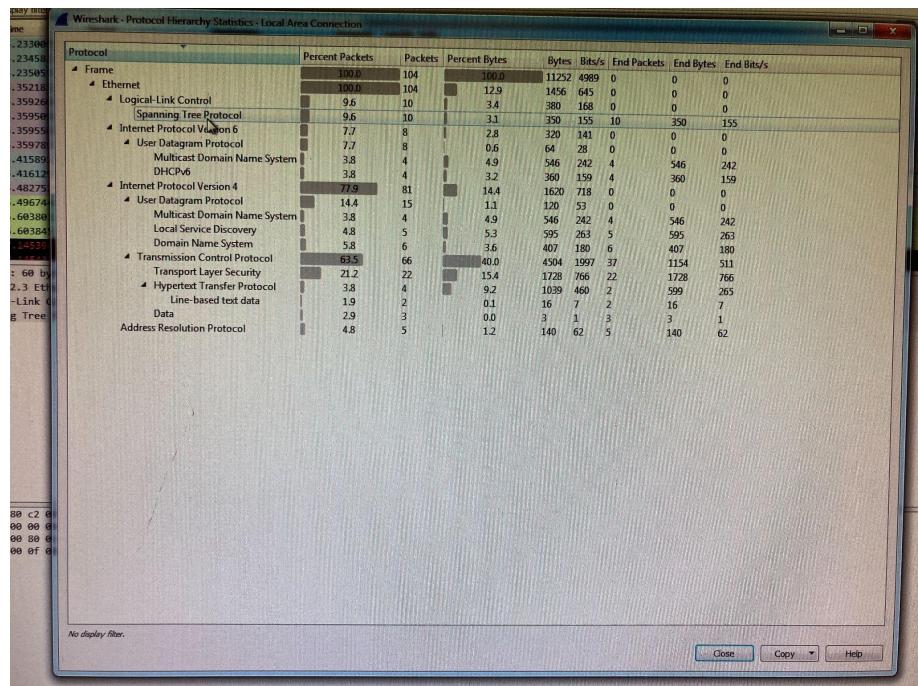
04:2a:e2

fc:fb:fb

سوال ۳:

در این بخش آماری از سلسله مراتب protocol های لایه های مختلف بسته های دریافت شده مشاهده میکنیم.

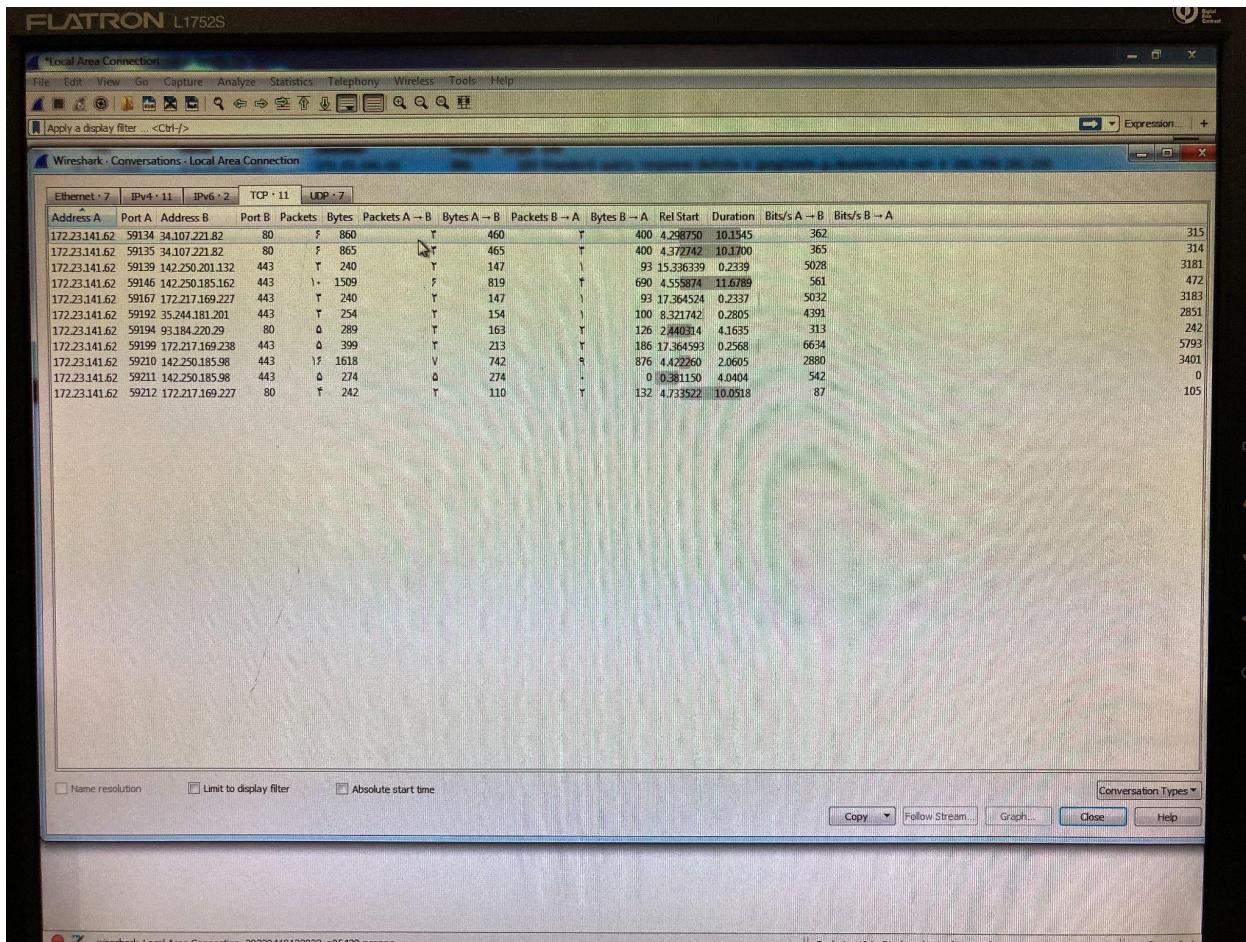
در بسته های دریافت شده ۱۰۰٪ بسته ها در لایه‌ی Ethernet از نوع link data هستند و ۷۷.۹٪ بسته ها در لایه‌ی شبکه دارای پروتکل IPv4 هستند و همچنین از بین این بسته ها ۱۴.۴٪ آن ها در لایه‌ی انتقال دارای پروتکل TCP هستند و ... سایر اطلاعات آماری که همگی در این پنجره قابل مشاهده هستند.



سوال ۴:

تقریبا 100% بسته ها در لایه ی شبکه دارای پرتوکل IPv4 هستند. همچنین ازین این بسته ها 62.1% آنها در لایه ی انتقال دارای پرتوکل TCP هستند. بنابراین حدودا 62.1% بسته ها به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند.

سوال ۵:



در این بخش آدرس مبدأ و مقصد (دو طرف ارتباط)، port و تعداد بسته های منتقل شده (هم از a به b و هم از b به a)، بات های انتقال داده شده (مجموع از a به b و از b به a) و مجموع کل بایت های انتقال یافته. زمان شروع ارتباط و همچنین مدت زمان ارتباط نیز قابل مشاهده است.

سرعت انتقال بیت بر ثانیه برای هر دو طرف به طرف دیگر مشخص شده است. برای هر کدام از پرتوکل های ethernet و IPV4 و TCP و UDP این اطلاعات موجود هستند.

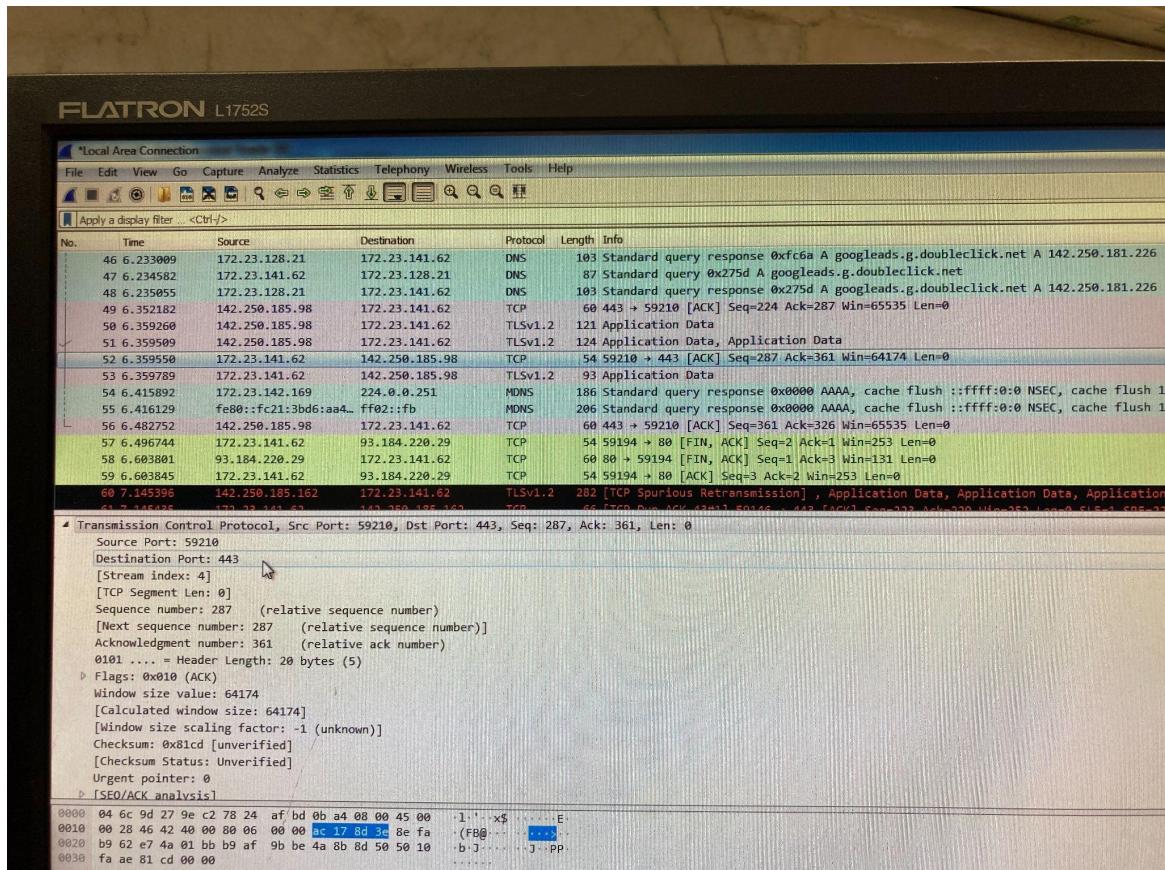
٤ بخش

Source: 172.23.141.62

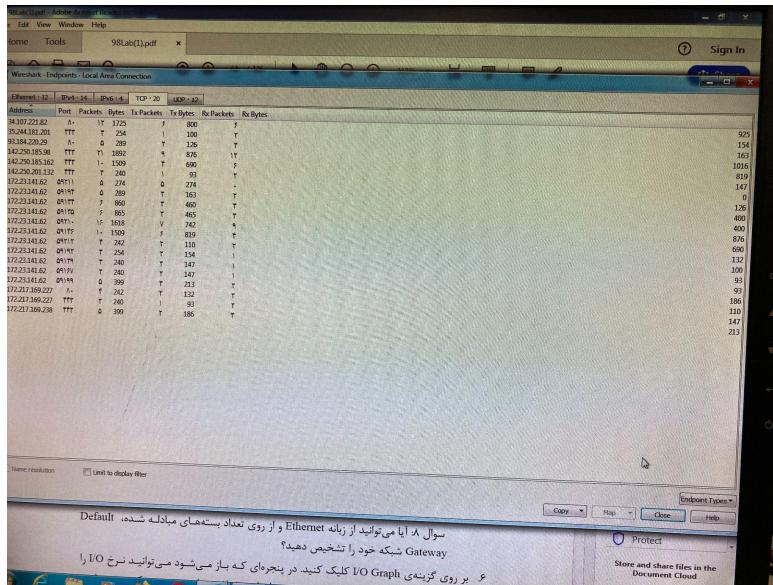
Destination: 142.250.185.98

Source port: 59210

Destination port: 443



سوال ۶:



هایی که از طریق آن ها بسته هایی دریافت شده اند به تفکیک پروتکل های لایه های مختلف آن endpoint ها مشاهده میشود.

اطلاعاتی نظری تعداد بسته ها و تعداد بایت های منتقل شده و همچنین شهر یا کشوری که آن endpoint در آن قرار دارد قابل مشاهده است. 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 IPv4 و Ethernet نمایش داده شده اند.

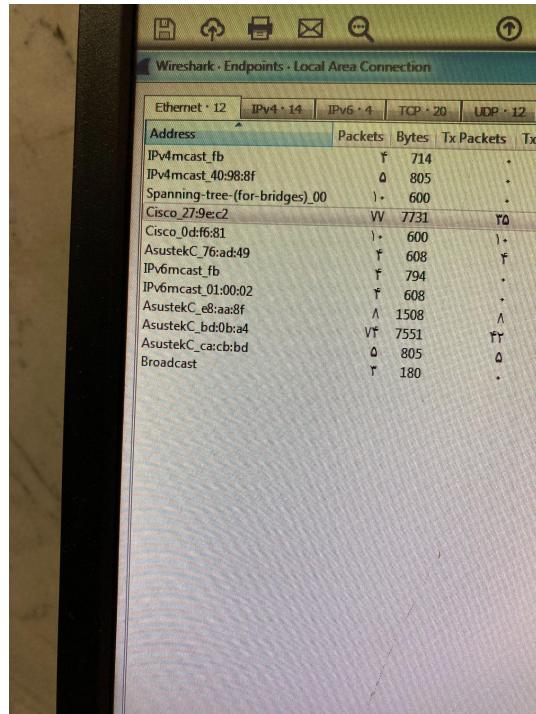
سوال ۷:

Address
34.107.221.82
35.244.181.201
93.184.220.29
142.250.185.98
142.250.185.162
142.250.201.132
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.23.141.62
172.217.169.227
172.217.169.227
172.217.169.238

همانطور که مشاهده میکنید، این آدرس ها مقصد هایی هستند که برای ارتباط های TCP در سیستم ما استفاده شده اند.

سوال ۸:

با توجه به اینکه دو آدرس Cisco_27 و AsustekC_bd بیشترین تعداد پکت ها را داشتند، این دو آدرس،
ما هستند.

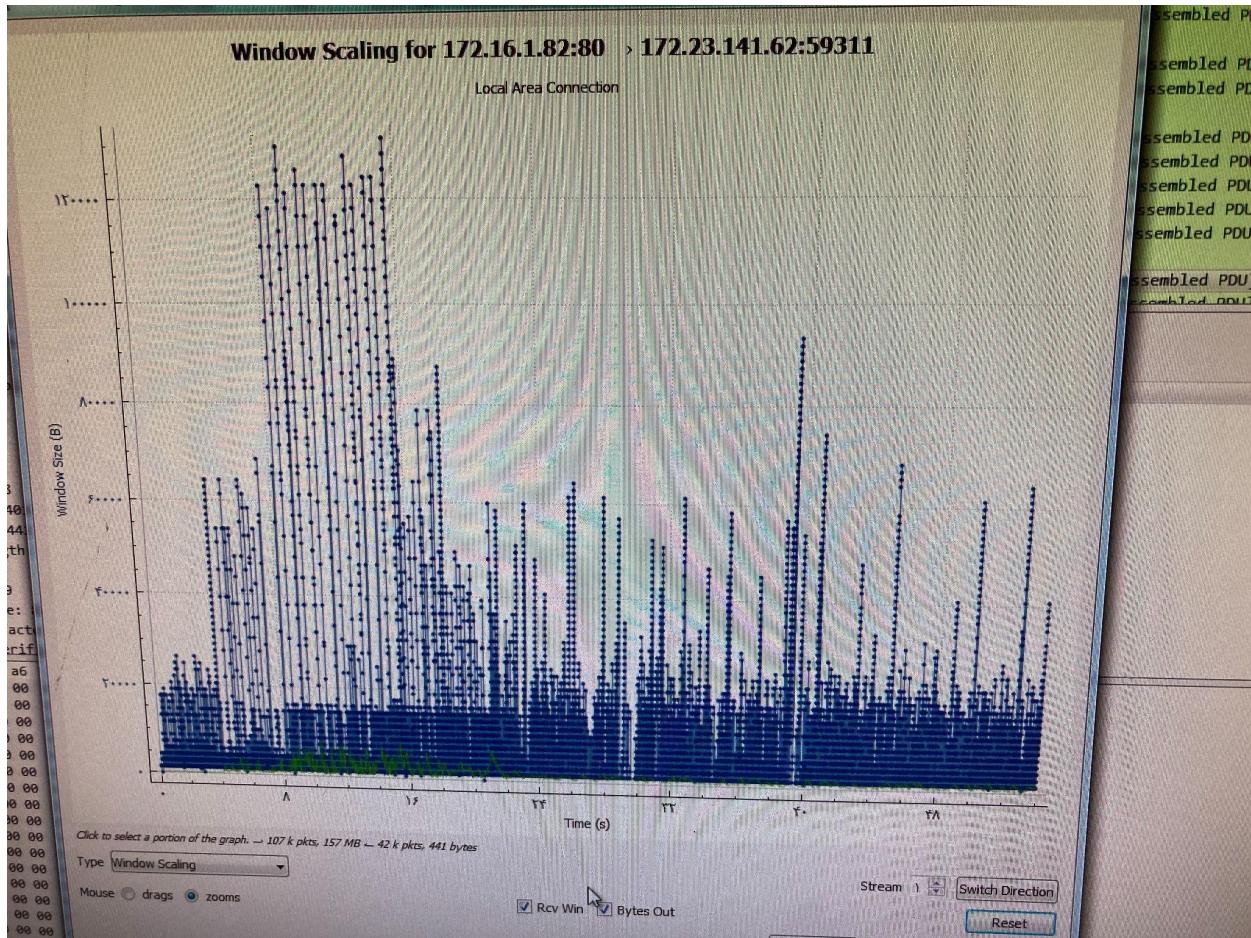


سوال ۹

172.16.1.82

این ip آدرس سایت دانلود دانشکده است

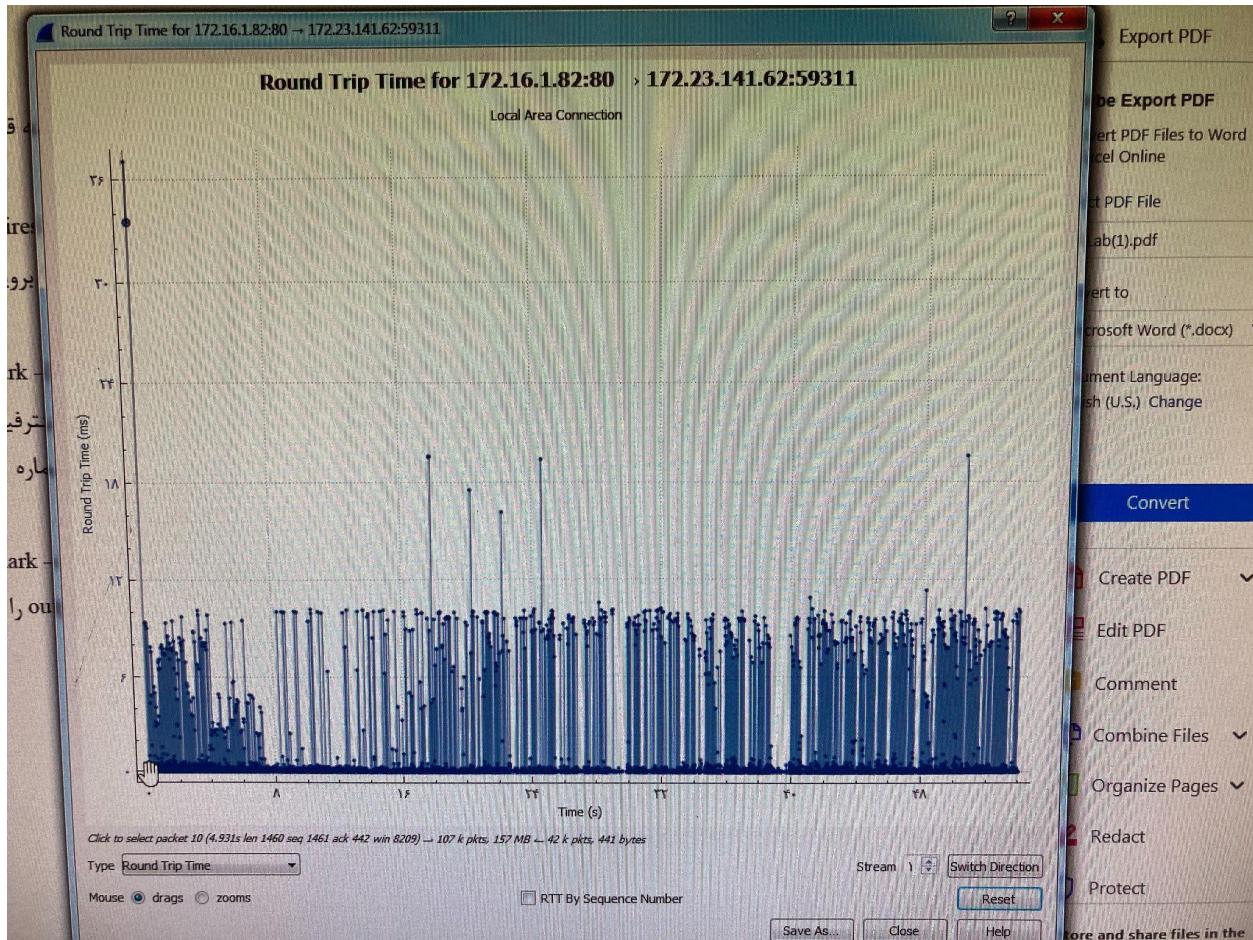
نمودار window scaling



همانطور که مشاهده میکنید پکت 96163 در زمان تقریبی ۱۶ ثانیه گم شده است و conjection در همین لحظه

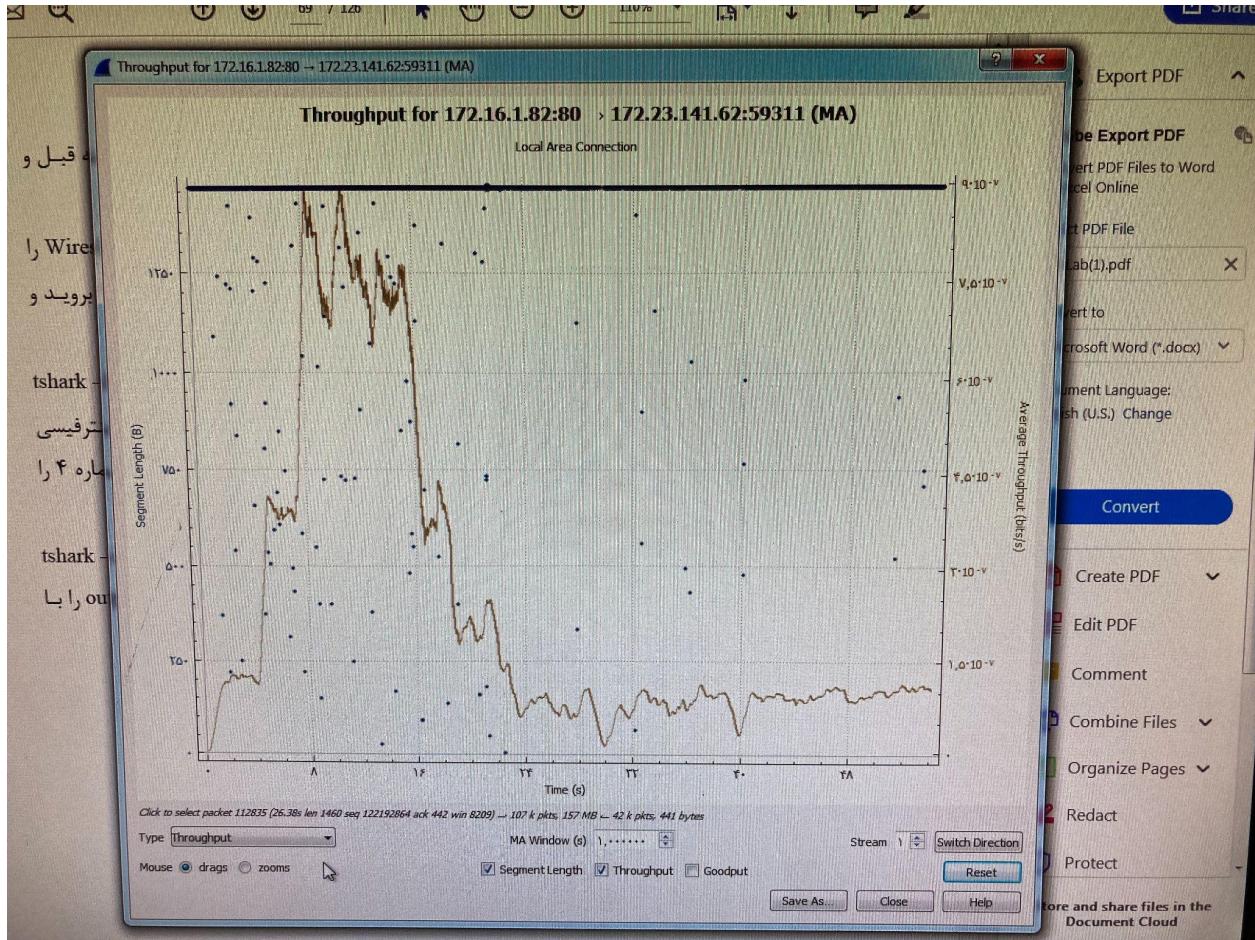
رخ داده است.

نمودار RTT



در همان لحظه ای که گفته شد، مشاهده میکنید که زمان RTT افزایش یافته است و می توان فهمید که در این لحظه رخداده است.

نحوه دار Throughput



همچنین در نمودار گذره‌ی، در این لحظه یک کاهش شدید داشته ایم که به دلیل رخ دادن *conjecture* این اتفاق افتاده است و سپس در مرحله recovery یک افزایش اندک داشته است.