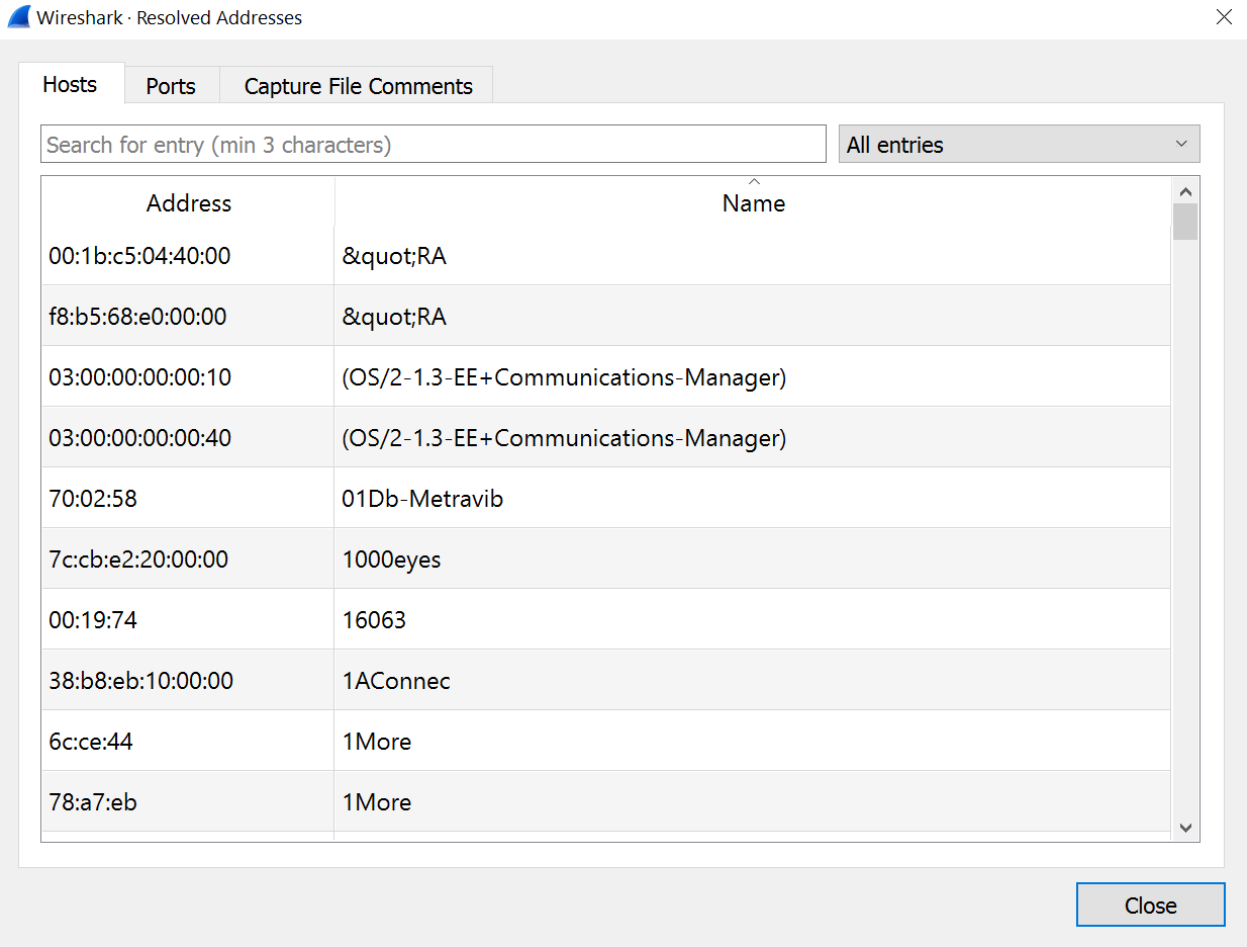
نام و نام خانوادگی: **امیرحسین علی‌بخشی**
شماره‌ی دانشجویی: **۹۷۳۱۰۹۶**

تحلیل TCP با وایرشارک

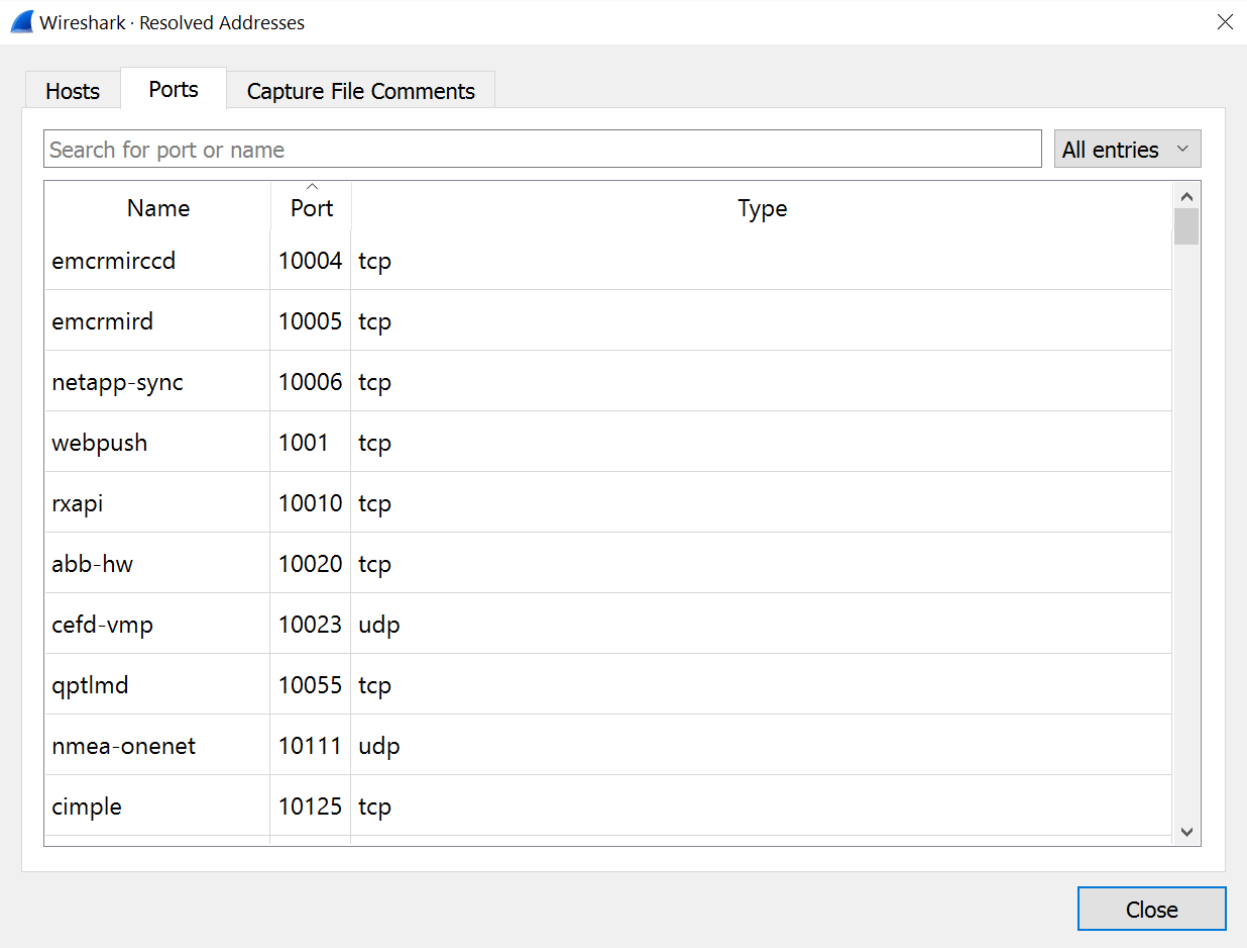
استاد: **خانم نقی پور**
درس: **آز شبکه**

سوال ۱

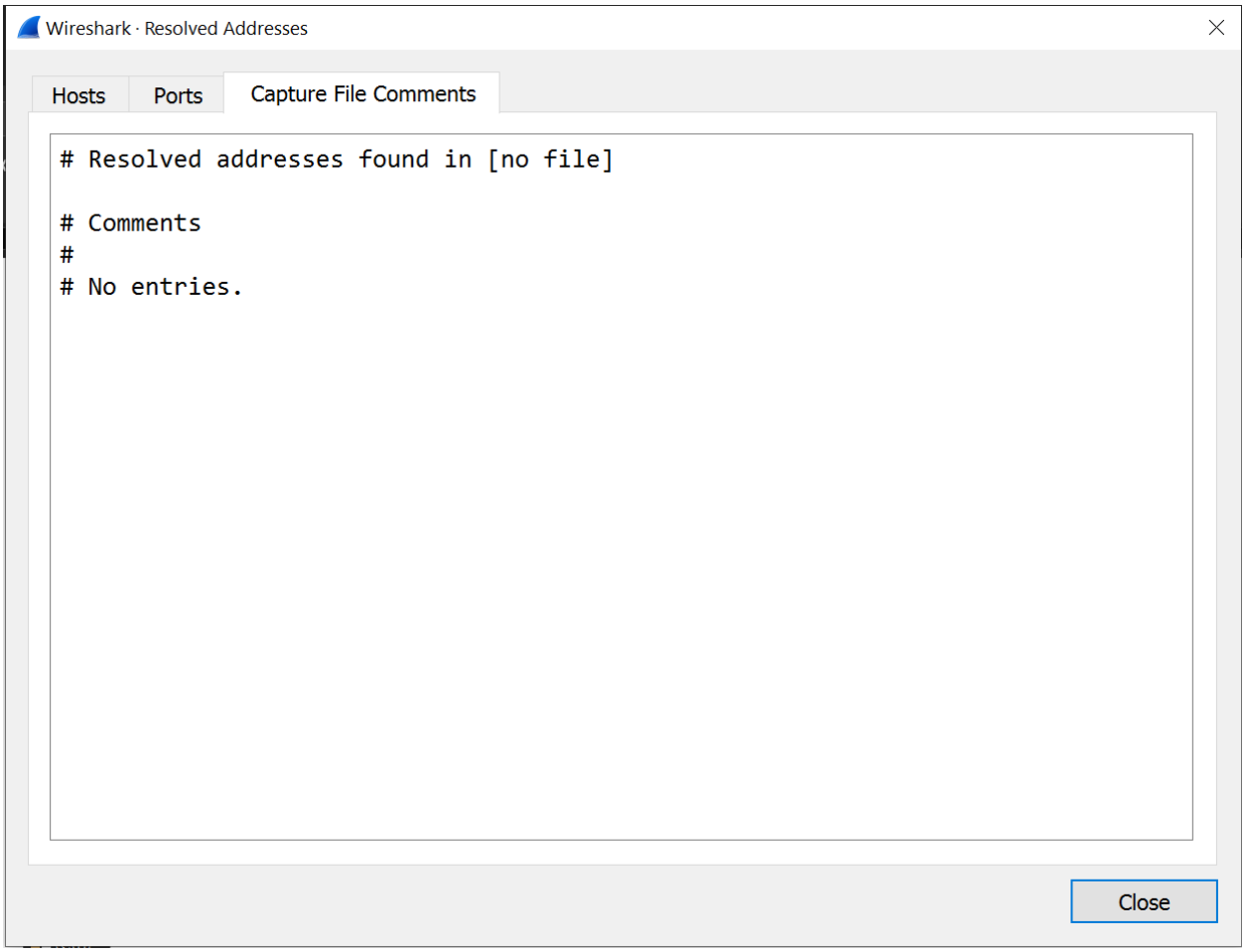
در قسمت hosts مشاهده میکنیم که در بسته هایی که capture کرده ایم ، ادرس ها ip یا آدرس های فیزیکی شبکه(انواع مختلف Ethernet addresses) ها به چه اسم هایی map شده اند .(البته در بخش آدرس های فیزیکی Ethernet ، ۳ بایت اول آدرس قابل مشاهده است .)



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.

Wireshark · Resolved Addresses

Hosts | Ports | Capture File Comments

cisco

All entries

Address	Name
00:60:3e	Cisco
00:90:f2	Cisco
00:07:0d	Cisco
00:90:2b	Cisco
00:10:79	Cisco
00:60:70	Cisco
00:60:09	Cisco
00:0c:0c:0c:0c:0c	Cisco-ACI-Gleaning-Leaf
00:0d:0d:0d:0d:0d	Cisco-ACI-Gleaning-Spine

Close

سوال ۳

Wireshark · Protocol Hierarchy Statistics · Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	En
Frame	100.0	48368	100.0	19626738	424k	0	0	0
Ethernet	100.0	48368	3.5	677152	14k	0	0	0
Internet Protocol Version 6	0.6	302	0.1	12080	261	0	0	0
Internet Protocol Version 4	99.3	48030	4.9	960624	20k	0	0	0
User Datagram Protocol	37.2	17989	0.7	143912	3111	0	0	0
Simple Service Discovery Protocol	0.2	95	0.1	15131	327	95	15131	32
QUIC IETF	1.5	716	1.4	282558	6109	666	252045	54
NetBIOS Name Service	0.5	253	0.1	12974	280	253	12974	28
NetBIOS Datagram Service	0.0	1	0.0	201	4	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	2	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	0	1	33	0
Multicast Domain Name System	0.3	158	0.0	5215	112	158	5215	11
Link-local Multicast Name Resolution	0.3	125	0.0	3121	67	125	3121	67
Domain Name System	0.4	201	0.1	13789	298	201	13789	29
Data	34.1	16490	44.4	8708685	188k	16490	8708685	18
Transmission Control Protocol	62.1	30035	44.7	8771813	189k	21983	5588767	12
Transport Layer Security	16.7	8073	30.0	5895385	127k	7891	4839131	10
Malformed Packet	0.0	18	0.0	0	0	18	0	0
Hypertext Transfer Protocol	0.1	32	0.1	22459	485	18	7255	15
Online Certificate Status Protocol	0.0	7	0.0	3425	74	7	3425	74

No display filter.

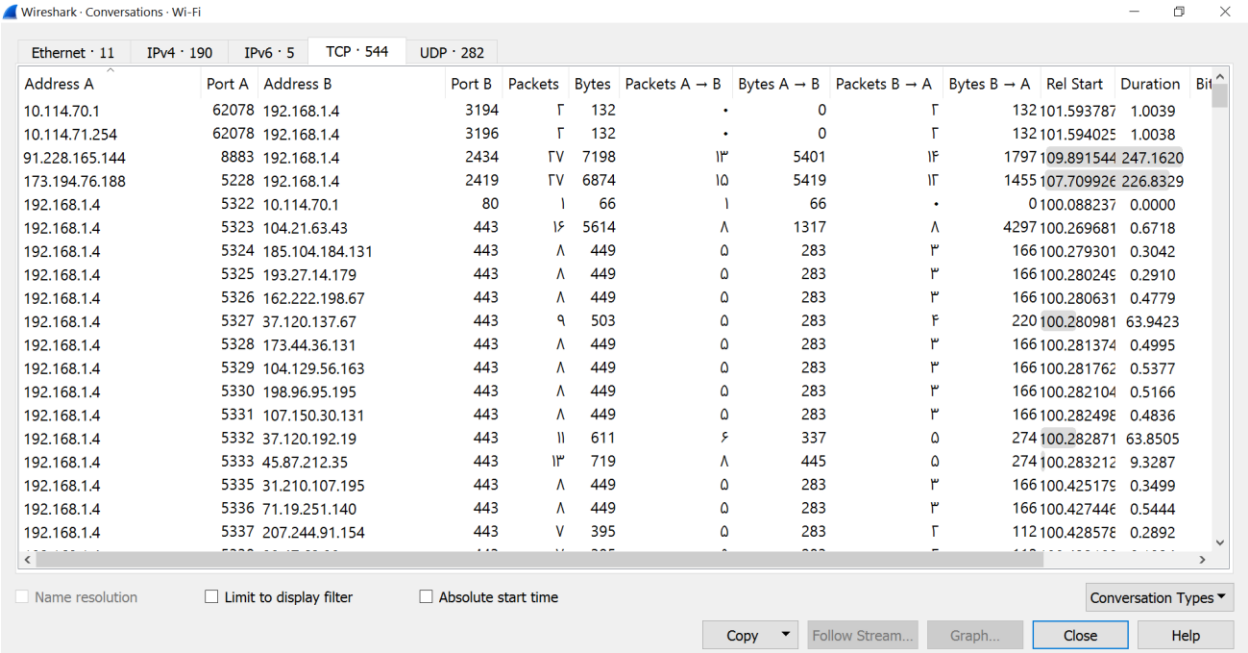
Close | Copy | Help

در این بخش آماری از سلسله مراتب protocol های لایه های مختلف بسته های capture شده مشاهده میکنیم . مثال در بسته های capture شده ۱۰۰ ٪ بسته ها در الیه ی link data از نوع Ethernet هستند و ۹۹.۳٪ 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 ۶۲.۱ ٪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 ۱۰۰ ٪آن ها در لایه ی data link دارای پرتکل Ethernet هستند و تقریبا ۱۰۰ ٪آن ها در لایه ی شبکه دارای پرتکل IPv4هستند . همچنین از بین این بسته ها ۶۲.۱٪ آن ها در لایه ی انتقال دارای پروتکل TCP هستند . بنابراین حدودا (به این علت میگوییم حدودا که تقریبا ۱۰۰ ٪بسته ها در لایه ی شبکه دارای پرتکل IPv4بودند) ، ۶۲.۱ ٪بسته ها به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند.

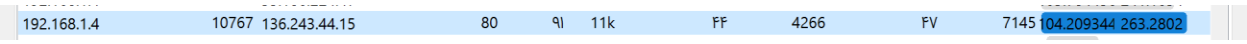
سوال ۵



اطلاعات 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 ۲ 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 ۱۰۷۶۷ با آدرس 192.168.1.4 و مقصد دارای پورت ۸۰ با آدرس مقصد 136.243.44.15 است . تعداد بسته های منتقل شده ۹۱ و تعداد بایت های منتقل شده ، 11k است . سایر موارد ذکر شده در سوال ۵ نیز در این عکس قابل مشاهده هستند.

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

```
GET /
MFMwUTBPME0wSzAJBgUrDgMCGgUABBRI2smg%2ByvTLU%2Fw3mjS9We3NfmzxAQUFC6zF7dYVsuuUAlA5h%
2BvnYsUwsYCEgOY3hiRlwqJgpfPG3sZxDaPrQ%3D%3D HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: r3.o.lencr.org

HTTP/1.1 200 OK
Server: nginx
Content-Type: application/ocsp-response
Content-Length: 503
ETag: "16FF84D281D0F909368D3CCE2D40D3EDE47F3E4BCC8BA093A5BD36862C1F17F6"
Last-Modified: Tue, 01 Jun 2021 23:00:00 UTC
Cache-Control: public, no-transform, must-revalidate, max-age=13989
Expires: Fri, 04 Jun 2021 13:42:31 GMT
Date: Fri, 04 Jun 2021 09:49:22 GMT
Connection: keep-alive
```

سوال ۶

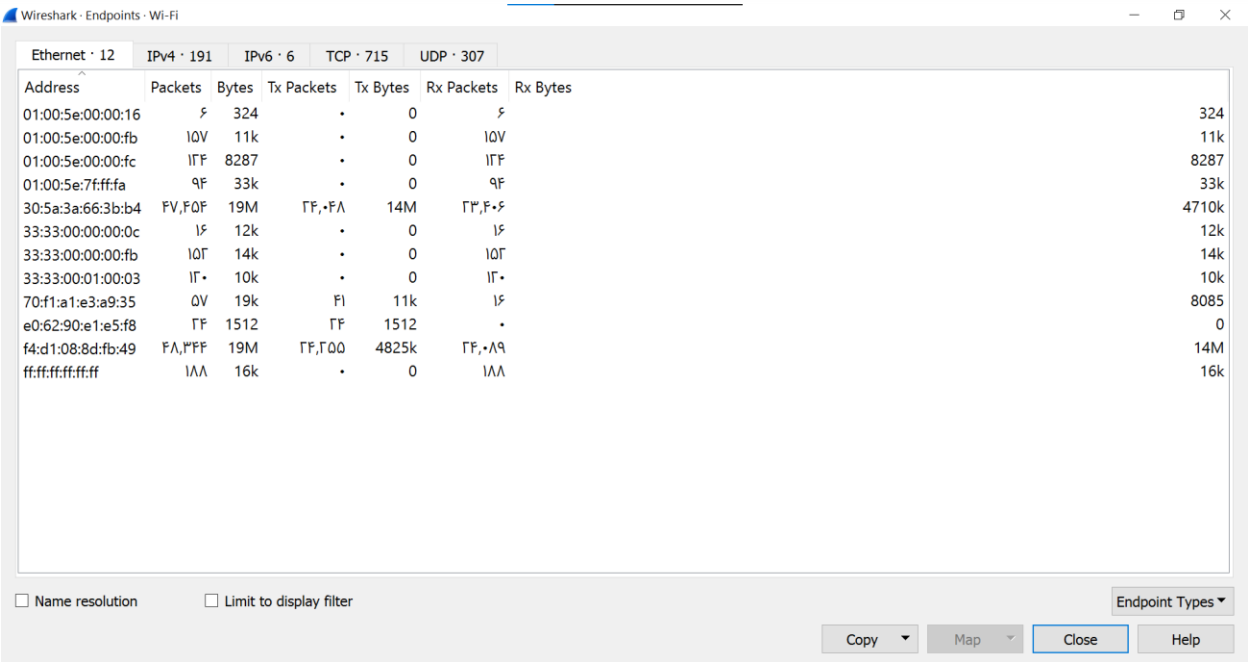
در صفحه ی باز شده که بخشی از آن در صفحه ی بعد قابل مشاهده است ، endpointهایی که از طریق آن ها بسته هایی capture شده اند به تفکیک پروتکل های الیه های مختلف آن ها مشاهده میشود.

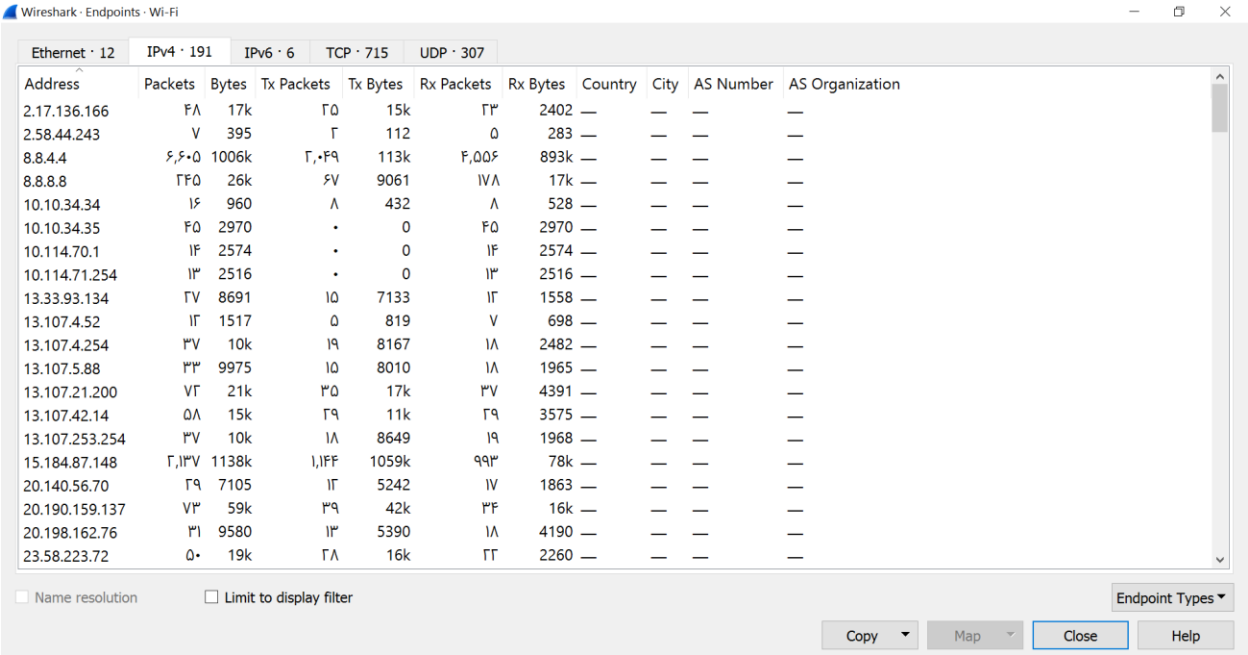
یا مثلا در بخش IPv4 که شکل آن نیز آمده است اطلاعاتی نظیر تعداد بسته ها و تعداد بایت های منتقل شده و همچنین شهر یا کشوری که آن endpoint در آن قرار دارد قابل مشاهده است

(که البته در موارد captureشده اطلاعات این ۲ 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.

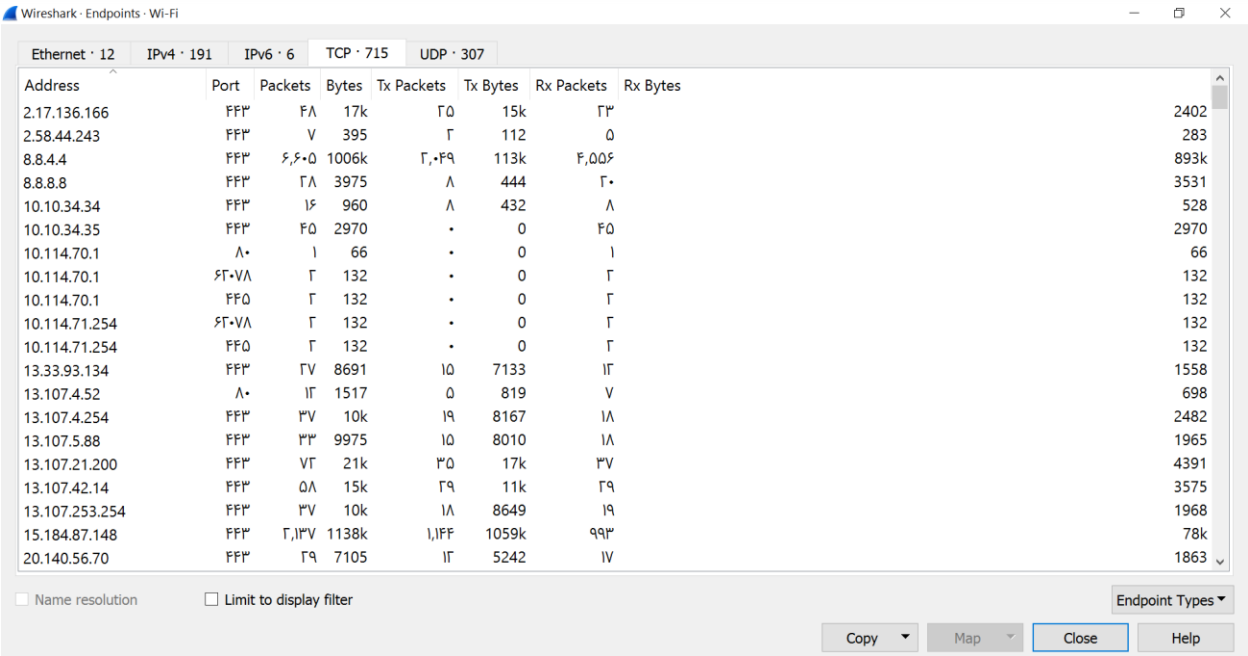
همچنین در تمام بخش ها بسته ها و بایت های Rx و Tx منتقل شده نیز قابل مشاهده هستند . دو بخش Ethernet و IPv4 نمایش داده شده اند.





سوال ۷

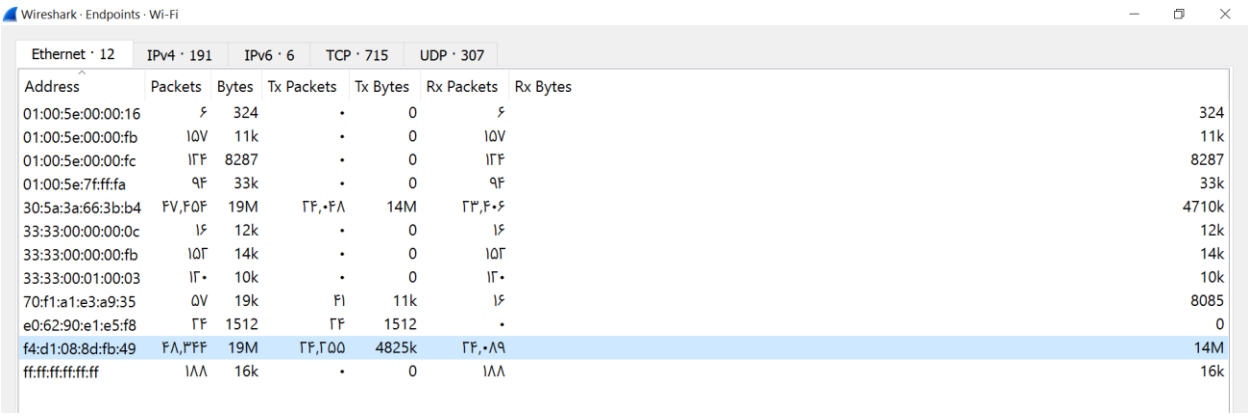
در قسمت TCP در پنجره ی endpoints آدرس IP مقصد هایی که در ارتباط TCP با سیستم من استفاده شده اند مشاهده میشود . که همانطور که در شکل صفحه ی بعد نیز مشاهده میشود ، تعداد مقصد های انتخابی ۷۱۵ تا است.



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
2.17.136.166	۴۴۳	۴۸	17k	۲۵	15k	۲۳	2402
2.58.44.243	۴۴۳	۷	395	۲	112	۵	283
8.8.4.4	۴۴۳	۶,۶۰۵	1006k	۲,۰۴۹	113k	۴,۵۵۶	893k
8.8.8.8	۴۴۳	۲۸	3975	۸	444	۲۰	3531
10.10.34.34	۴۴۳	۱۶	960	۸	432	۸	528
10.10.34.35	۴۴۳	۴۵	2970	۰	0	۴۵	2970
10.114.70.1	۸۰	۱	66	۰	0	۱	66
10.114.70.1	۶۲۰۷۸	۲	132	۰	0	۲	132
10.114.70.1	۴۴۵	۲	132	۰	0	۲	132
10.114.71.254	۶۲۰۷۸	۲	132	۰	0	۲	132
10.114.71.254	۴۴۵	۲	132	۰	0	۲	132
13.33.93.134	۴۴۳	۲۷	8691	۱۵	7133	۱۲	1558
13.107.4.52	۸۰	۱۲	1517	۵	819	۷	698
13.107.4.254	۴۴۳	۳۷	10k	۱۹	8167	۱۸	2482
13.107.5.88	۴۴۳	۳۳	9975	۱۵	8010	۱۸	1965
13.107.21.200	۴۴۳	۷۲	21k	۳۵	17k	۳۷	4391
13.107.42.14	۴۴۳	۵۸	15k	۲۹	11k	۲۹	3575
13.107.253.254	۴۴۳	۳۷	10k	۱۸	8649	۱۹	1968
15.184.87.148	۴۴۳	۲,۱۳۷	1138k	۱,۱۴۴	1059k	۹۹۳	78k
20.140.56.70	۴۴۳	۲۹	7105	۱۲	5242	۱۷	1863

سوال ۸

برای تشخیص default gateway باید به این نکته توجه داشته باشیم که در بخش Ethernet ، end pointای 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 ۴۸۳۴۴ عدد و با حجمی برابر 19MB است.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:16	۶	324	۰	0	۶	324
01:00:5e:00:00:fb	۱۵۷	11k	۰	0	۱۵۷	11k
01:00:5e:00:00:fc	۱۲۴	8287	۰	0	۱۲۴	8287
01:00:5e:7f:ff:fa	۹۴	33k	۰	0	۹۴	33k
30:5a:3a:66:3b:b4	۴۷,۴۵۴	19M	۲۴,۰۴۸	14M	۲۳,۴۰۶	4710k
33:33:00:00:00:0c	۱۶	12k	۰	0	۱۶	12k
33:33:00:00:00:fb	۱۵۲	14k	۰	0	۱۵۲	14k
33:33:00:01:00:03	۱۲۰	10k	۰	0	۱۲۰	10k
70:f1:a1:e3:a9:35	۵۷	19k	۴۱	11k	۱۶	8085
e0:62:90:e1:e5:f8	۲۴	1512	۲۴	1512	۰	0
f4:d1:08:8d:fb:49	۴۸,۳۴۴	19M	۲۴,۲۵۵	4825k	۲۴,۰۸۹	14M
ff:ff:ff:ff:ff:ff	۱۸۸	16k	۰	0	۱۸۸	16k

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.

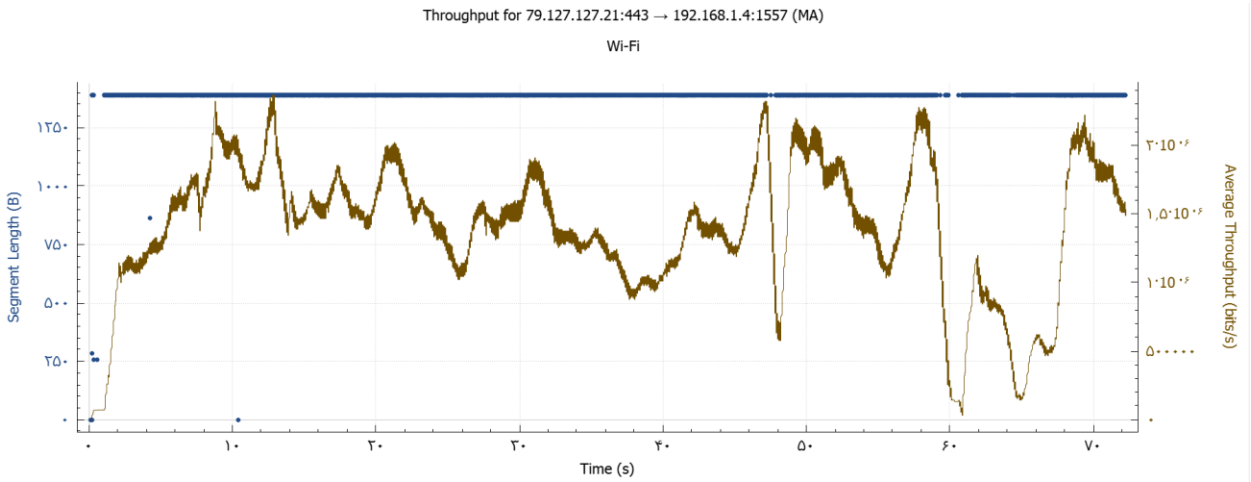
Wireshark · Conversations · Wi-Fi

Ethernet · 4 | IPv4 · 50 | IPv6 | TCP · 78 | UDP · 36

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B
192.168.1.4	2417	79.127.127.21	443	۲۱,۷۸۱	19M	۸,۴۰۹	507k	۱۳,۳۷۲	19M	8.371961	85.1801	47k	1
192.168.1.4	3515	79.127.127.21	443	۲۰,۹۸۸	19M	۸,۱۳۱	489k	۱۲,۸۵۷	18M	8.372348	85.1441	45k	1
192.168.1.4	2727	79.127.127.21	443	۲۰,۹۴۸	19M	۸,۰۶۹	486k	۱۲,۸۷۹	18M	10.111795	83.4430	46k	1
192.168.1.4	1557	79.127.127.21	443	۱۴,۸۸۱	13M	۵,۷۳۷	346k	۹,۱۴۴	13M	21.354017	72.2039	38k	1
192.168.1.4	12652	79.127.127.21	443	۱۴,۸۸۰	13M	۵,۷۵۴	345k	۹,۱۲۶	13M	23.053921	70.4886	39k	1
192.168.1.4	5081	79.127.127.21	443	۱۴,۶۸۳	13M	۵,۶۲۲	334k	۹,۰۶۱	13M	20.129283	73.3491	36k	1
192.168.1.4	2348	13.227.173.128	443	۸,۷۴۲	7006k	۴,۱۲۳	346k	۴,۶۱۹	6659k	77.164030	13.2555	209k	4
192.168.1.4	12658	65.9.82.11	443	۵۵	33k	۲۴	3250	۳۱	30k	72.829589	2.6364	9861	
192.168.1.4	6996	213.239.221.102	88	۵۲	19k	۲۴	4983	۲۸	14k	7.455904	62.0354	642	
192.168.1.4	12655	213.239.221.102	88	۴۵	28k	۲۲	21k	۲۳	6979	64.582732	3.1358	54k	
192.168.1.4	12654	213.239.221.102	88	۳۹	26k	۱۹	19k	۲۰	6733	34.267984	2.4908	63k	
192.168.1.4	12660	13.227.173.46	443	۳۷	12k	۱۷	1754	۲۰	10k	74.410897	1.1821	11k	
192.168.1.4	11984	213.239.221.102	88	۳۵	25k	۱۸	18k	۱۷	6662	0.031594	0.8336	176k	
192.168.1.4	2350	35.244.247.133	443	۳۳	11k	۱۷	6371	۱۶	4801	89.521283	1.8825	27k	
192.168.1.4	3519	23.58.222.25	443	۲۷	10k	۱۴	1702	۱۳	8344	9.891276	61.7156	220	
192.168.1.4	3520	23.58.222.25	443	۲۶	9753	۱۲	1365	۱۴	8388	9.891276	61.7207	176	
192.168.1.4	13691	142.250.185.46	443	۲۶	7548	۱۲	1636	۱۴	5912	76.572473	1.6405	7978	
192.168.1.4	3518	72.247.161.167	443	۲۴	8970	۱۱	1162	۱۳	7808	9.151907	62.4513	148	
192.168.1.4	2347	162.159.136.232	443	۲۴	3276	۱۲	1846	۱۲	1430	13.407440	75.5525	195	

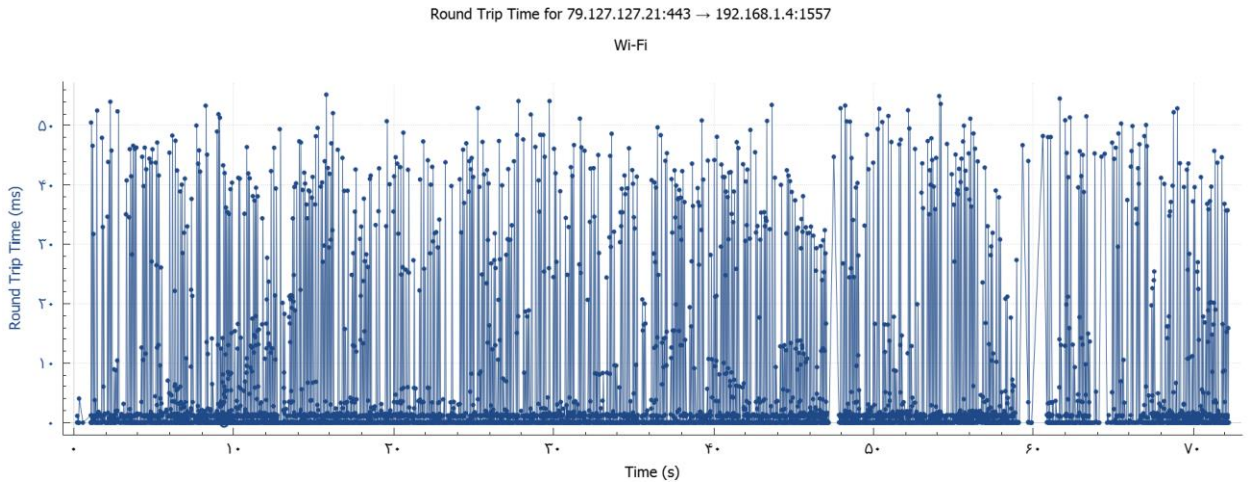
این آدرس برابر 79.127.127.21 بوده که مربوط به سایت soft98.ir میباشد.

نمودار Troughout



مقدار آن میتواند متغیر باشد ولی همیشه از ۱۵۰۰ کمتر خواهد بود.

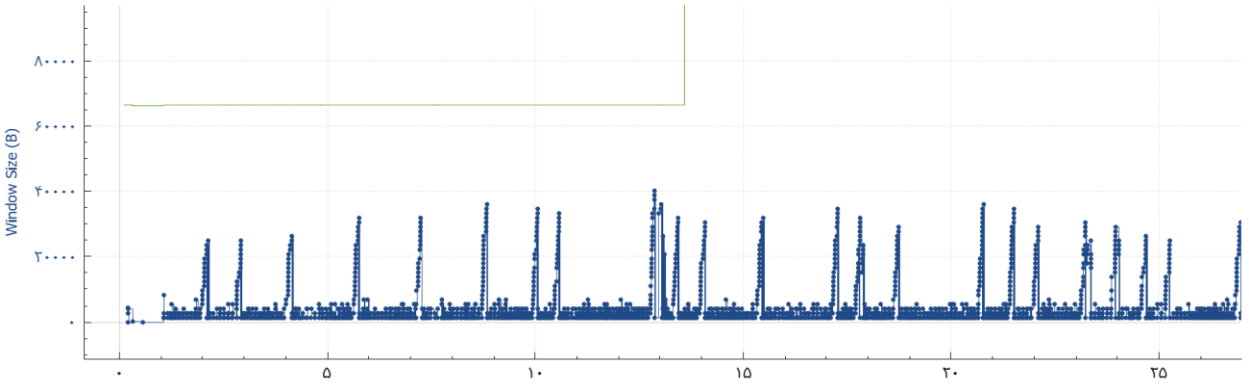
نمودار RTT



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 ، RTTافزایش می یابد ، اما در نقاطی که ازدحام تا حدی کم میشود مجددا RTTنیز 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.