

«باسمه تعالی»



گزارش کار آزمایش

تحلیل TCP با استفاده از Wireshark



طراحی و تدوین:

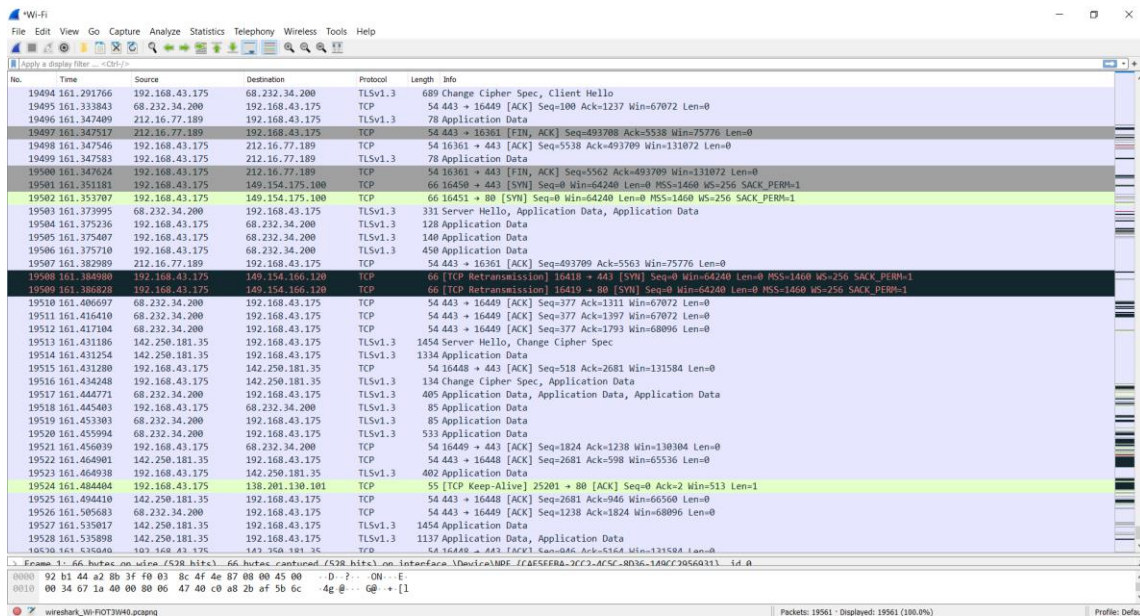
مهدی رحمانی / 9731701

هدف آزمایش

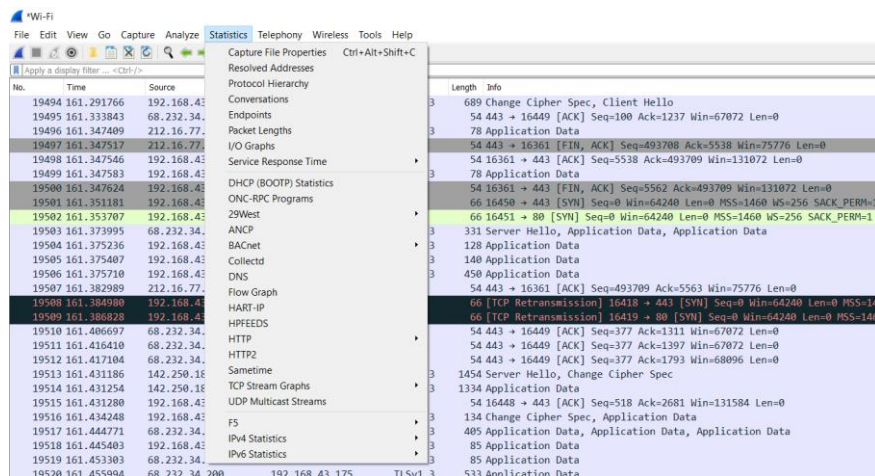
در این آزمایش آشنایی بیشتری با نرم افزار Wireshark و منوی Statistics در آن پیدا میکنیم و از امکانات آن برای تحلیل بسته های جمع آوری شده استفاده می نماییم.

شرح آزمایش

ابتدا نرم افزار wireshark را باز کرده، چند دقیقه به وب گردی میکنیم و بسته ها را جمع آوری میکنیم و سپس آن را متوقف میکنیم:



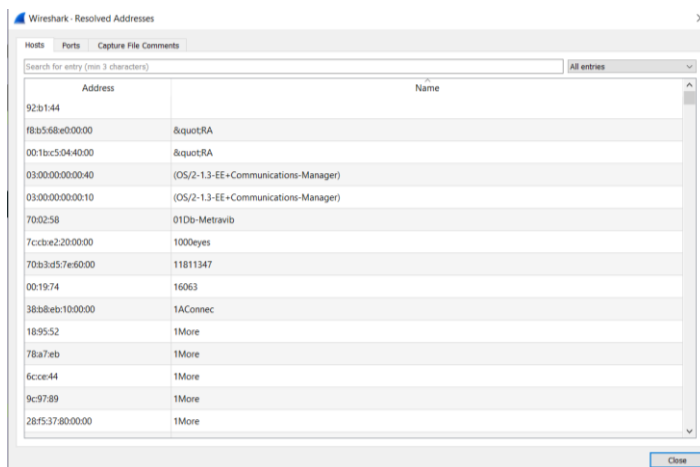
از منوی بالا بر روی گزینه ی Statistics کلیک میکنیم. در ادامه قصد داریم مواردی که در این زبانه وجود دارند را بررسی کنیم.



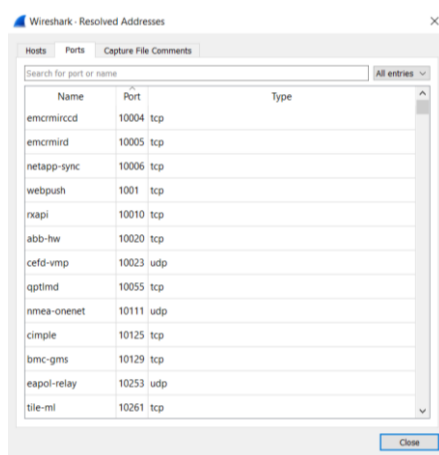
1. بر روی گزینه‌ی Resolved Addresses کلیک کنید.

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

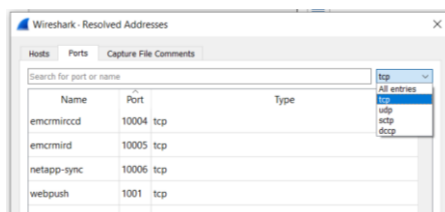
پنجره‌ای که باز می‌شود به صورت زیر می‌باشد:



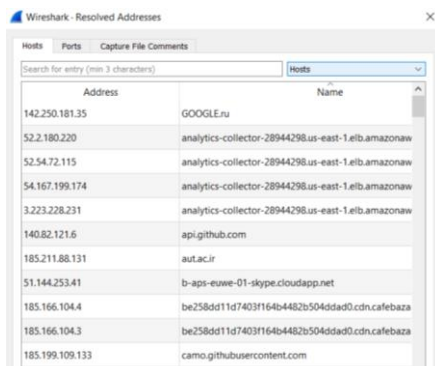
درواقع می‌گویند که یک سری عدد را به یک سری اسم تبدیل می‌کند و به عبارت دیگر برای هر پورت و IP آدرس را به یک اسم map می‌کند. مثلاً در tab مربوط به پورت در عکس زیر می‌گویند وقتی یک سری پورت‌ها را ببیند آن‌ها را به چه اسمی تبدیل می‌کند. و در بسته‌های capture شده این تبدیل را می‌کند.



از گوشه‌ی سمت راست بالا نیز می‌توان type سوکت آن را مشخص کرد.



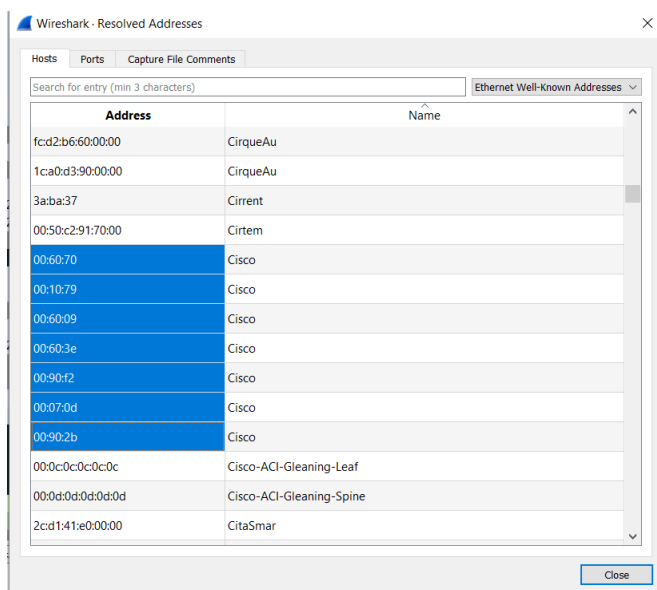
همچنین در همان tab مربوط به Hosts اگر از گوشه سمت راست بالا Hosts را انتخاب کنیم بسته به اینکه در چه صفحاتی گشتیم اسم این host ها را به IP Address آن map میکند که براساس آنچه که capture کردیم میفهمد چون DNS ها را درواقع ندارد.



Address	Name
142.250.181.35	GOOGLE.ru
52.2.180.220	analytics-collector-28944298.us-east-1.elb.amazonaws
52.54.72.115	analytics-collector-28944298.us-east-1.elb.amazonaws
54.167.199.174	analytics-collector-28944298.us-east-1.elb.amazonaws
3.223.228.231	analytics-collector-28944298.us-east-1.elb.amazonaws
140.82.121.6	api.github.com
185.211.88.131	aut.ac.ir
51.144.253.41	b-aps-euwe-01-skype.cloudapp.net
185.166.104.4	be258dd11d7403f164b4482b504ddad0.cdn.cafebaza
185.166.104.3	be258dd11d7403f164b4482b504ddad0.cdn.cafebaza
185.199.109.133	camo.githubusercontent.com

سوال 2: آیا می‌توانید سه بایت اولی که برای آدرس فیزیکی کارت‌های شبکه Cisco می‌باشند را مشخص کنید؟

بله - طبق توضیحات ویودئو ابتدا از گوشه سمت راست بالا Ethernet Well-Known Address را انتخاب میکنیم. سپس با کمی جست و جو کارت های شبکه Cisco را میابیم. 3 بایت اول آن ها به صورت زیر میباشد (سلکت شده اند):



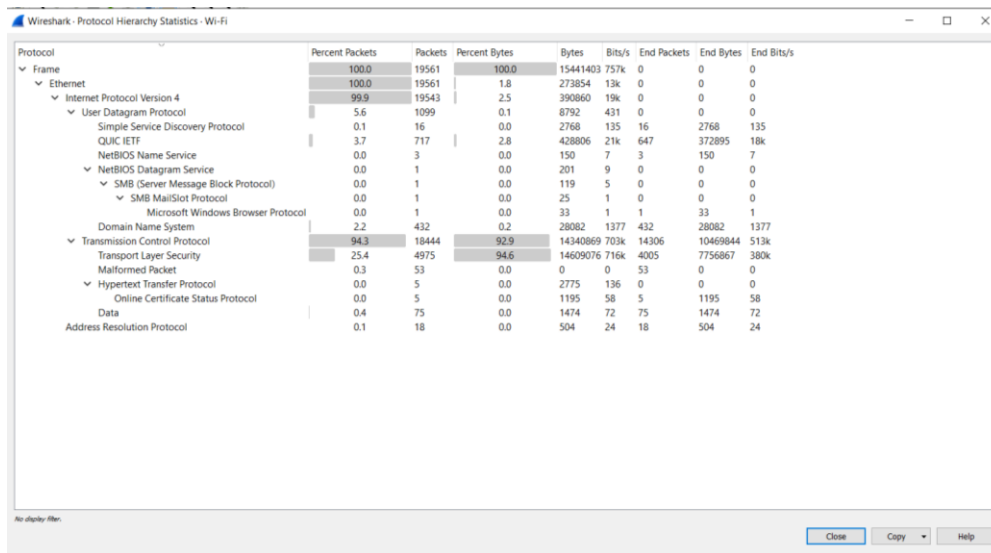
Address	Name
fc02:b6:00:00:00	CirqueAu
1ca0:d3:90:00:00	CirqueAu
3a:ba:37	Cirrent
00:50:c2:91:70:00	Cirtem
00:60:70	Cisco
00:10:79	Cisco
00:60:09	Cisco
00:60:3e	Cisco
00:90:f2	Cisco
00:07:0d	Cisco
00:90:2b	Cisco
00:0c:0c:0c:0c:0c	Cisco-ACI-Gleaning-Leaf
00:0d:0d:0d:0d:0d	Cisco-ACI-Gleaning-Spine
2cd1:41:e0:00:00	CitaSmar

2. بر روی گزینه‌ی protocol hierarchy کلیک کنید.

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

پنجره‌ی زیر باز می‌شود. در اینجا سلسله مراتب پروتکل را براساس مدل لایه‌ای TCP/IP که در درس شبکه داشتیم، را لیست میکند مثلاً می‌گوید در این frame ها چه پروتکل هایی دیده شده. مثلاً IPv4 میتواند باشد یا IPv6 که در تصویر زیر بسته ای با پروتکل IPv6 دریافت نشده. درواقع اطلاعاتی آماری در مورد پروتکل های استفاده شده در بسته های capture شده را به صورت سلسله مراتبی نشان میدهد. حال اینجا در زیرمجموعه IPv4 در لایه transport آن UDP و TCP داریم. در زیرمجموعه های خود TCP نگاه کنیم نیز application layer ما را هم نشان میدهد که برای مثال اینجا HTTP داریم که در کل 5 تا packet از آن دریافت شده است.

درواقع یک آماری از کل بسته های دریافتی و شبکه ما میدهد و بعداً در تصمیم گیری ها میتوان به این آمار نگاه کرد. مثلاً بفرض اگر نباید IPv6 داشته باشیم ولی الان اگر بفرض فلان قدر درصد داریم، چرا داریم؟



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	19561	100.0	15441403	757k	0	0	0
Ethernet	100.0	19561	1.8	273854	13k	0	0	0
Internet Protocol Version 4	99.9	19543	2.5	390860	19k	0	0	0
User Datagram Protocol	5.6	1099	0.1	8792	431	0	0	0
Simple Service Discovery Protocol	0.1	16	0.0	2768	135	16	2768	135
QUIC IETF	3.7	717	2.8	428806	21k	647	372895	18k
NetBIOS Name Service	0.0	3	0.0	150	7	3	150	7
NetBIOS Datagram Service	0.0	1	0.0	201	9	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	5	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	1	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	1	1	33	1
Domain Name System	2.2	432	0.2	28082	1377	432	28082	1377
Transmission Control Protocol	94.3	18444	92.9	14340869	703k	14306	10469844	513k
Transport Layer Security	25.4	4975	94.6	14609076	716k	4005	7756867	380k
Malformed Packet	0.3	53	0.0	0	0	53	0	0
Hypertext Transfer Protocol	0.0	5	0.0	2775	136	0	0	0
Online Certificate Status Protocol	0.0	5	0.0	1195	58	5	1195	58
Data	0.4	75	0.0	1474	72	75	1474	72
Address Resolution Protocol	0.1	18	0.0	504	24	18	504	24

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

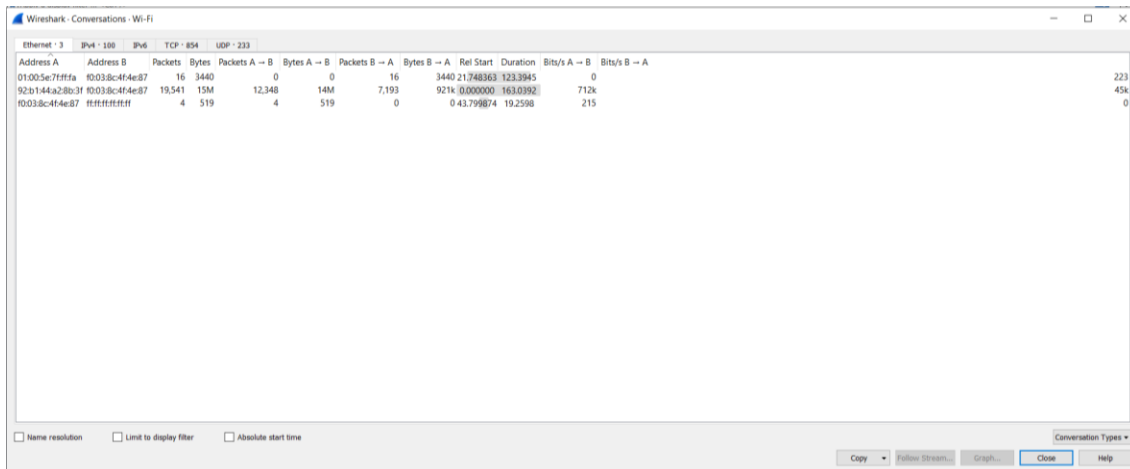
SMB MailSlot Protocol	0.0	1	0.0	25	1	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	1	1	33	1
Domain Name System	2.2	432	0.2	28082	1377	432	28082	1377
Transmission Control Protocol	94.3	18444	92.9	14340869	703k	14306	10469844	513k
Transport Layer Security	25.4	4975	94.6	14609076	716k	4005	7756867	380k
Malformed Packet	0.3	53	0.0	0	0	53	0	0
Hypertext Transfer Protocol	0.0	5	0.0	2775	136	0	0	0
Online Certificate Status Protocol	0.0	5	0.0	1195	58	5	1195	58

همانطور که دیده میشود 94.3 درصد بسته های به یک ارتباط TCP بر روی بستر IPv4 تعلق دارد.

3. بر روی گزینه‌ی Conversations کلیک کنید.

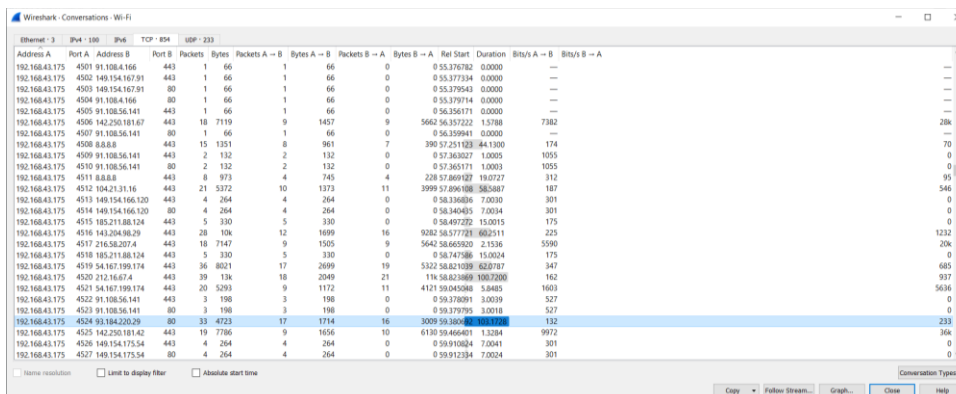
سوال 5: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

وقتی بر روی این گزینه میزیم پنجره زیر باز می‌شود. نشست‌ها را در قالب Ethernet و IPv4 و IPv6 و TCP و UDP برای ما آورده است و به ترتیب layer شان آن‌ها را دسته‌بندی کرده است و البته تعریف نشست در Wireshark کمی با تعریفی که در درس خوانده ایم فرق دارد. درواقع اطلاعات آماری conversation‌ها بین دو نقطه ابتدایی و انتهایی را نشان می‌دهد. حال اگر برای مثال یک نشست را در TCP مشخص کنیم و follow stream را بزنیم، میتوانیم Conversation انجام شده را ببینیم. که حالت‌های مختلفی برای نمایش این مکالمه وجود دارد که مثلاً مکالمه‌ای که فقط در رفت انجام شده را نشان دهد یا فقط برگشت را یا هر دو را باهم.



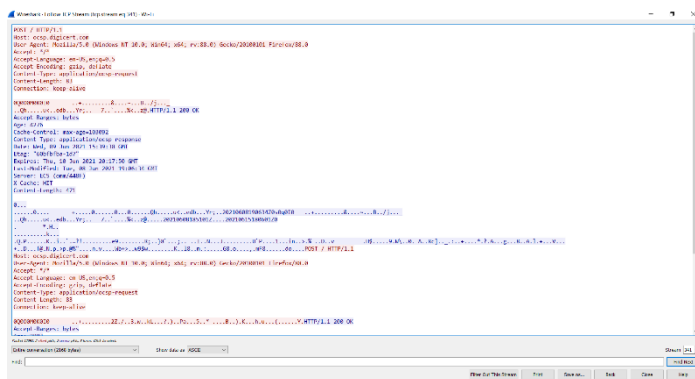
4. یک نشست TCP را مشخص کنید. (برای مشخص کردن یک نشست TCP نیاز است که آدرس و پورت مبدا و مقصد را مشخص کنید.) توجه داشته باشید مفهومی که Wireshark از نشست برداشت می‌کند با مفهومی که در کلاس آموخته‌اید تفاوت دارد.

ابتدا به Tab مربوط به TCP می‌رویم و بعد برای مثال نشست‌ی که در تصویر زیر مشخص شده است را انتخاب می‌کنیم:

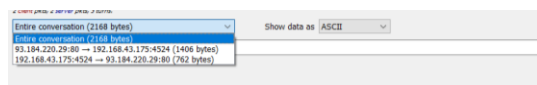


همانطور که مشخص است برای این نشست، آدرس مبدأ 192.168.43.175 و پورت مبدأ نیز 4524 است. همچنین آدرس مقصد 93.184.220.29 میباشد و پورت مقصد نیز 80 میباشد.

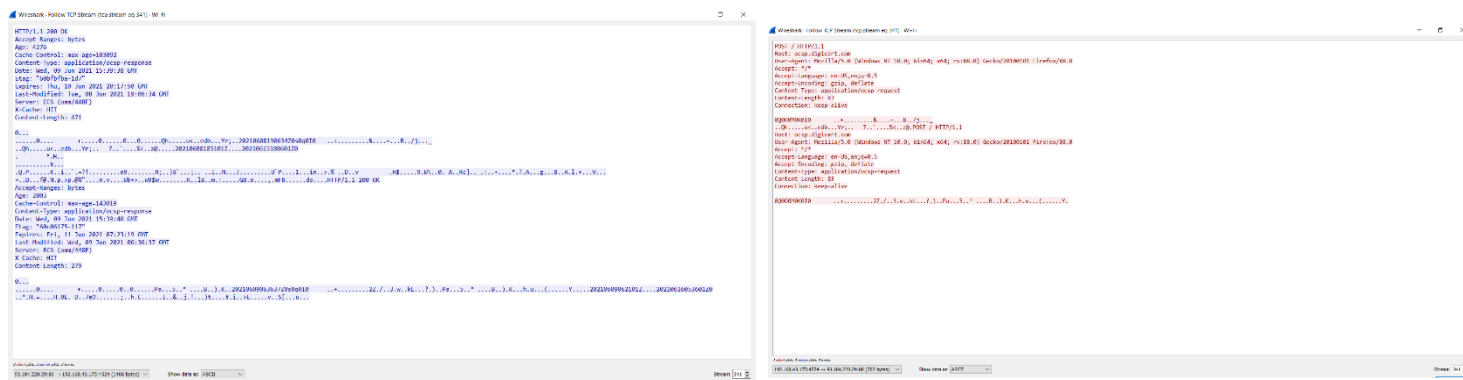
سپس گزینه Follow Stream را میزنیم. و میتوان conversation انجام شده در این نشست را مشاهده کرد:



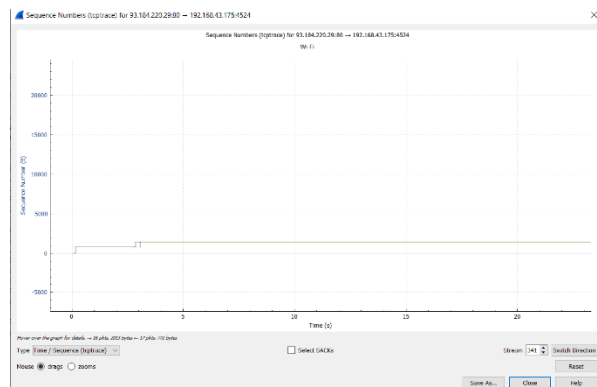
با انتخاب گزینه های زیر میتوان مکالمه را در یک طرف نیز فقط مشاهده کرد.



که نتیجه انتخاب هریک را در زیر میتوانید مشاهده کنید:



همچنین اگر گزینه Graph را برای این نشست انتخاب کنیم تصویر زیر را مشاهده خواهیم کرد:

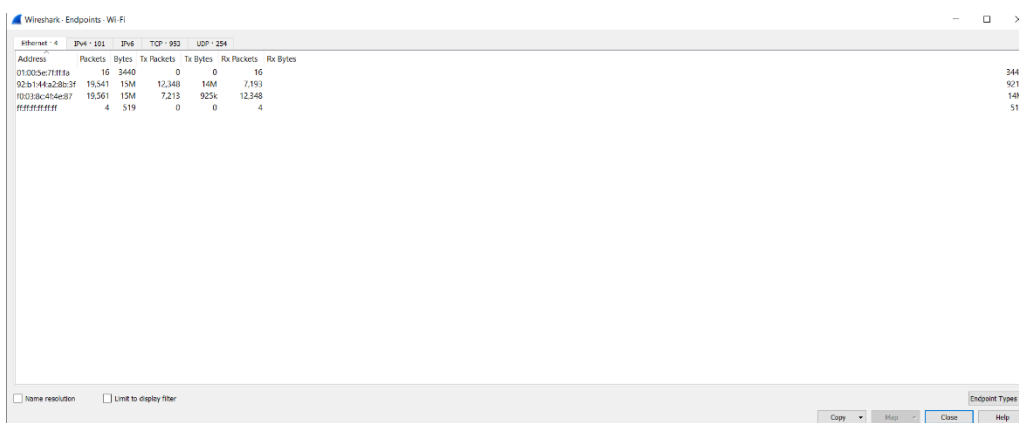


5. بر روی گزینه‌ی endpoints کلیک کنید.

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

وقتی روی این گزینه می‌زنیم با تصویر زیر روبرو می‌شویم. درواقع نشان دهنده endpoint هایی است که ما با آن‌ها در ارتباط بودیم و در قالب های UDP ، TCP ، IPv6 ، IPv4 و Ethernet میتوان لیستشان را مشاهده کرد.البته چون این‌ها را از conversation سلکت میکند ممکن است تکراری هم بینشان باشد. کمکی که به ما میکند این است که به کمک آن می‌فهمیم که چند درصد از اطلاعات ما به یک IP می‌رود یا مثلا دنبال یک IP مشخصی هستید که در آن شبکه و سازمان نباید مشاهده کنید، میتوانید سرچ کنید و مشاهده کنید که ببینید آیا این جزء endpoint ها بوده است یا نه و اگر بوده چرا؟

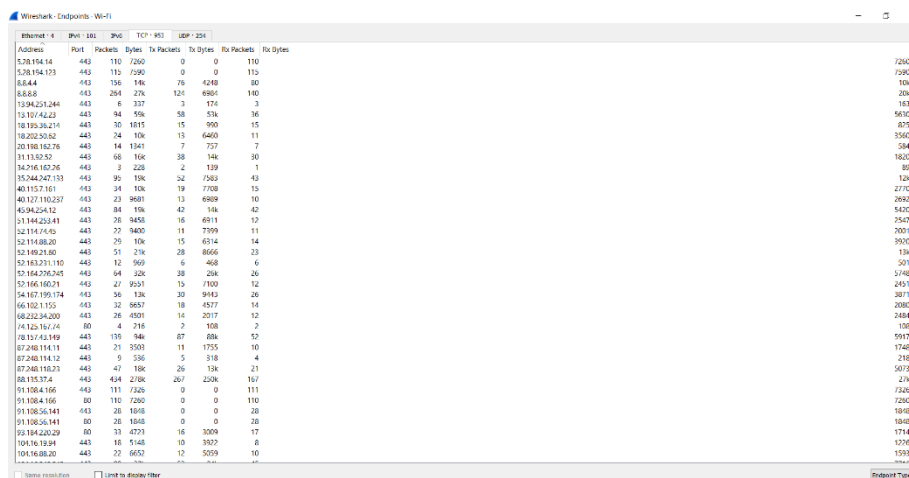
بنابراین endpoint های ارتباطات را میتوان به کمک آن دید.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:7f:ff:fa	6	3440	0	0	16	3440
92:37:44:a2:2b:c5f	19,541	15M	12,348	5488	7,193	5214
10:0:38:c4:04:e87	19,561	15M	7,213	925k	12,348	14M
#####	4	519	0	0	4	519

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

اگر در tab مربوط به TCP برویم به تصاویر زیر می‌رسیم.



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
5.38.154.14	443	110	7260	0	0	110	7260
5.38.154.123	443	115	7280	0	0	115	7280
8.8.8.8	443	156	186	79	4248	80	100
8.8.8.8	443	284	278	121	6861	160	206
13.94.251.244	443	6	337	3	1514	3	163
15.107.42.23	443	94	59k	58	53k	36	5630
18.189.39.214	443	30	1815	15	990	15	875
18.202.50.92	443	24	10k	15	6460	11	3560
20.108.162.76	443	14	1341	7	737	7	584
31.13.82.52	443	68	15k	38	14k	30	1620
34.796.162.26	443	2	228	2	129	1	89
35.242.247.133	443	90	19k	52	7583	43	12k
40.115.7.161	443	34	10k	19	7708	15	2770
40.127.110.237	443	23	8681	13	6869	10	2682
45.94.254.12	443	84	19k	42	14k	42	5430
51.144.23.41	443	28	9458	16	4911	12	2547
52.114.17.63	443	27	9400	11	7799	11	2601
52.114.88.20	443	29	10k	15	6314	14	3930
52.169.21.80	443	51	27k	28	8666	23	13k
52.163.271.110	443	12	960	6	466	6	501
52.164.276.245	443	64	32k	38	29k	26	5748
52.166.160.21	443	27	9531	15	7300	12	2451
54.167.199.174	443	36	13k	20	9443	26	3871
66.102.1.155	443	32	8657	18	4577	14	2080
68.222.34.200	443	26	4591	14	2017	12	2484
74.125.151.14	80	4	765	2	108	2	100
78.157.43.149	443	135	94k	87	88k	52	5917
87.248.114.11	443	21	5593	11	1755	10	1748
87.248.114.12	443	9	595	5	318	4	218
87.248.116.23	443	47	18k	26	13k	21	5073
88.135.374	443	434	270k	267	250k	167	27k
91.108.4.166	443	111	526	9	0	111	7336
91.108.4.166	80	110	7260	0	0	110	7260
91.108.56.141	443	28	1818	0	0	28	1818
91.108.56.141	80	28	1818	0	0	28	1818
99.194.220.29	80	33	4773	16	3009	17	1714
10.16.19.194	443	18	6148	10	3927	8	1276
101.16.88.20	443	27	6552	12	5059	10	1593

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
101.16.18.94	443	18	5148	10	3522	8	1226
104.16.88.20	443	22	8832	12	5059	10	1393
104.16.242.249	443	98	328	59	246	45	7716
104.16.249.249	443	340	1096	187	836	153	266
104.21.31.16	443	21	3372	11	3999	10	1373
101.17.140.219	443	15	4925	8	3753	7	1172
104.26.10.240	443	4	278	2	108	2	108
134.0.218.208	80	3	162	1	54	2	108
138.201.130.101	80	38	2484	19	1074	19	1050
140.82.114.22	443	15	1075	9	599	6	416
140.82.121.4	443	96	776	66	746	30	3247
140.82.121.5	443	6	363	3	201	3	162
140.82.121.6	443	45	198	23	3765	22	146
142.250.11.188	5228	6	363	3	198	3	165
142.250.181.135	443	33	586	17	176	16	2821
142.250.181.136	443	24	6577	13	4566	11	2011
142.250.181.42	443	285	1706	153	876	132	236
142.250.181.67	443	40	586	20	116	20	3048
142.250.181.99	443	19	7225	10	5715	9	1510
142.250.181.104	443	16	5175	9	4003	7	1172
142.250.181.110	80	3	162	2	108	1	54
142.250.181.112	80	3	162	1	54	2	108
142.250.181.112	443	3	162	1	54	2	108
143.204.98.23	443	10	602	5	306	5	296
143.204.98.29	443	28	196	16	9382	12	989
143.204.98.39	443	24	8317	13	6885	11	1427
143.204.98.69	443	38	126	21	106	17	2187
149.154.166.120	443	82	5412	0	0	82	5412
149.154.166.120	80	82	5412	0	0	82	5412
149.154.167.50	443	108	7128	0	0	108	7128
149.154.167.50	80	108	7128	0	0	108	7128
149.154.167.51	443	108	7128	0	0	108	7128
149.154.167.51	80	109	7194	0	0	109	7194
149.154.167.80	443	37	2112	0	0	37	2112
149.154.167.91	443	110	7260	0	0	110	7260
149.154.167.91	80	112	7592	0	0	112	7592
149.154.175.54	443	109	7194	0	0	109	7194
149.154.175.54	80	110	7260	0	0	110	7260

همانطور که مشاهده میشود مقصدهای زیادی برای ارتباط های TCP در سیستم ما استفاده شده است.آدرس این مقصد ها در ستون اول قابل مشاهده میباشد.

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

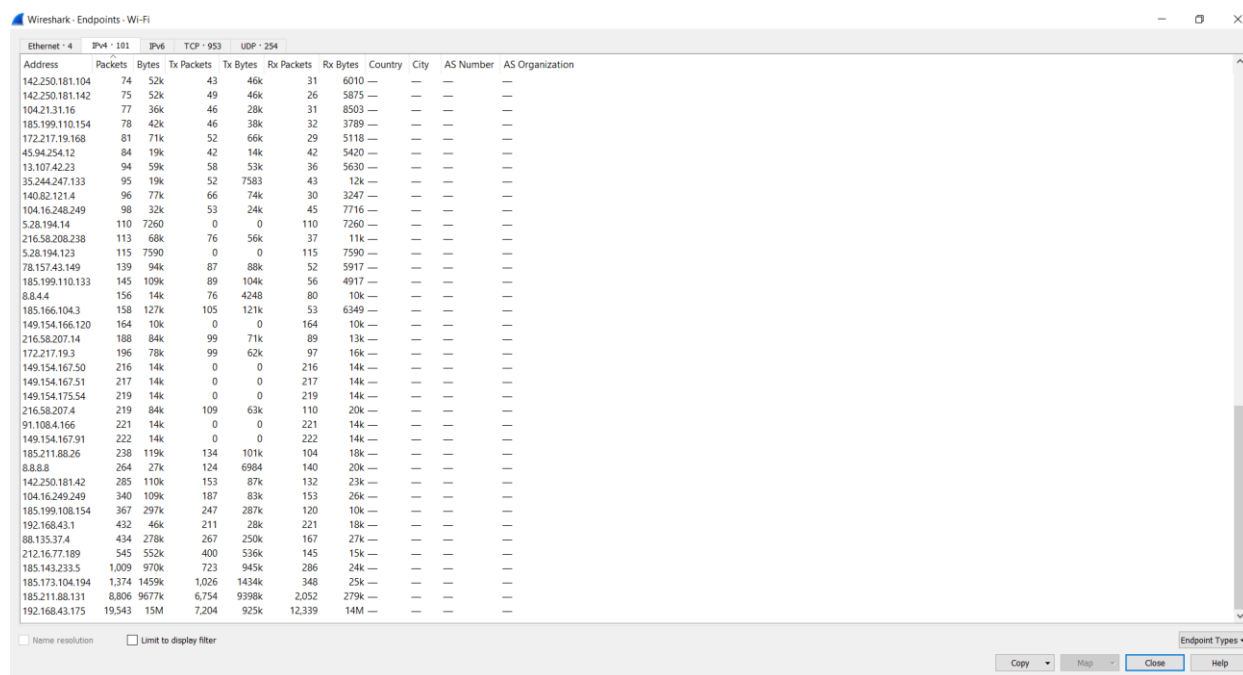
بله-اگر در زبانه Ethernet برویم و اگر Endpoint ها را بر مبنای تعداد بسته ها sortکنیم خروجی به صورت

زیر میشود:

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
ff:ff:ff:ff:ff:ff	4	519	0	0	4	519
01:00:5e:7:fff:fa	16	3440	0	0	16	3440
92:b1:44:a2:8b:3f	19,541	15M	12,348	14M	7,193	921k
f0:03:8c:4f:4e:87	19,561	15M	7,213	925k	12,348	14M

همانطور که مشاهده میشود آخرین سطر که مربوط به بیشترین تعداد بسته‌های مبادله شده میباشد، نشان دهنده آدرس فیزیکی سیستم خودمان میباشد ولی اگر دقت شود بعد از آن(یعنی سطر قبلی) آدرسی که بیشترین تعداد بسته های جابجا شده را دارد، مربوط به آدرس فیزیکی Default Gateway ما میباشد. همچنین اگر به ستون TX packets نگاه کنیم، میتوان گفت با توجه به آن بیشترین بسته‌های جابه جا شده مربوط به همین Default Gateway میباشد.

حال طبق ویدئو خواسته شده که به زبانه IPv4 مراجعه کنیم و ببینیم که آیا در آنجا نیز میشود از روی بسته های مبادله شده ، Default gateway شبکه را تشخیص داد یا خیر. پس ابتدا به این زبانه میرویم و سورت میکنیم خروجی به صورت زیر میباشد:



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
142.250.181.104	74	52k	43	46k	31	6010	---	---	---	---
142.250.181.142	75	52k	49	46k	26	5875	---	---	---	---
104.21.31.16	77	36k	46	28k	31	8503	---	---	---	---
185.199.110.154	78	42k	46	38k	32	3789	---	---	---	---
172.217.19.168	81	71k	52	66k	29	5118	---	---	---	---
45.94.254.12	84	19k	42	14k	42	5420	---	---	---	---
13.107.42.23	94	59k	58	53k	36	5630	---	---	---	---
35.244.247.133	95	19k	52	7583	43	12k	---	---	---	---
140.82.121.4	96	77k	66	74k	30	3247	---	---	---	---
104.16.248.249	98	32k	53	24k	45	7716	---	---	---	---
5.28.194.14	110	7260	0	0	110	7260	---	---	---	---
216.58.208.238	113	68k	76	56k	37	11k	---	---	---	---
5.28.194.123	115	7590	0	0	115	7590	---	---	---	---
78.157.43.149	139	94k	87	88k	52	5917	---	---	---	---
185.199.110.133	145	109k	89	104k	56	4917	---	---	---	---
8.8.4.4	156	14k	76	4248	80	10k	---	---	---	---
185.166.104.3	158	127k	105	121k	53	6349	---	---	---	---
149.154.166.120	164	10k	0	0	164	10k	---	---	---	---
216.58.207.14	188	84k	99	71k	89	13k	---	---	---	---
172.217.19.3	196	78k	99	62k	97	16k	---	---	---	---
149.154.167.50	216	14k	0	0	216	14k	---	---	---	---
149.154.167.51	217	14k	0	0	217	14k	---	---	---	---
149.154.175.54	219	14k	0	0	219	14k	---	---	---	---
216.58.207.4	219	84k	109	63k	110	20k	---	---	---	---
91.108.4.166	221	14k	0	0	221	14k	---	---	---	---
149.154.167.91	222	14k	0	0	222	14k	---	---	---	---
185.211.88.26	238	119k	134	101k	104	18k	---	---	---	---
8.8.8.8	264	27k	124	6984	140	20k	---	---	---	---
142.250.181.42	285	110k	153	87k	132	23k	---	---	---	---
104.16.249.249	340	109k	187	83k	153	26k	---	---	---	---
185.199.108.154	367	297k	247	287k	120	10k	---	---	---	---
192.168.43.1	432	46k	211	28k	221	18k	---	---	---	---
88.135.37.4	434	278k	267	250k	167	27k	---	---	---	---
212.16.77.189	545	552k	400	536k	145	15k	---	---	---	---
185.143.233.5	1,009	970k	723	945k	286	24k	---	---	---	---
185.173.104.194	1,374	1459k	1,026	1434k	348	25k	---	---	---	---
185.211.88.131	8,806	9677k	6,754	9398k	2,052	279k	---	---	---	---
192.168.43.175	19,543	15M	7,204	925k	12,339	14M	---	---	---	---

آدرس IP مربوط به default gateway بنده باتوجه به عکس زیر برابر با 192.168.43.1 میباشد:

```

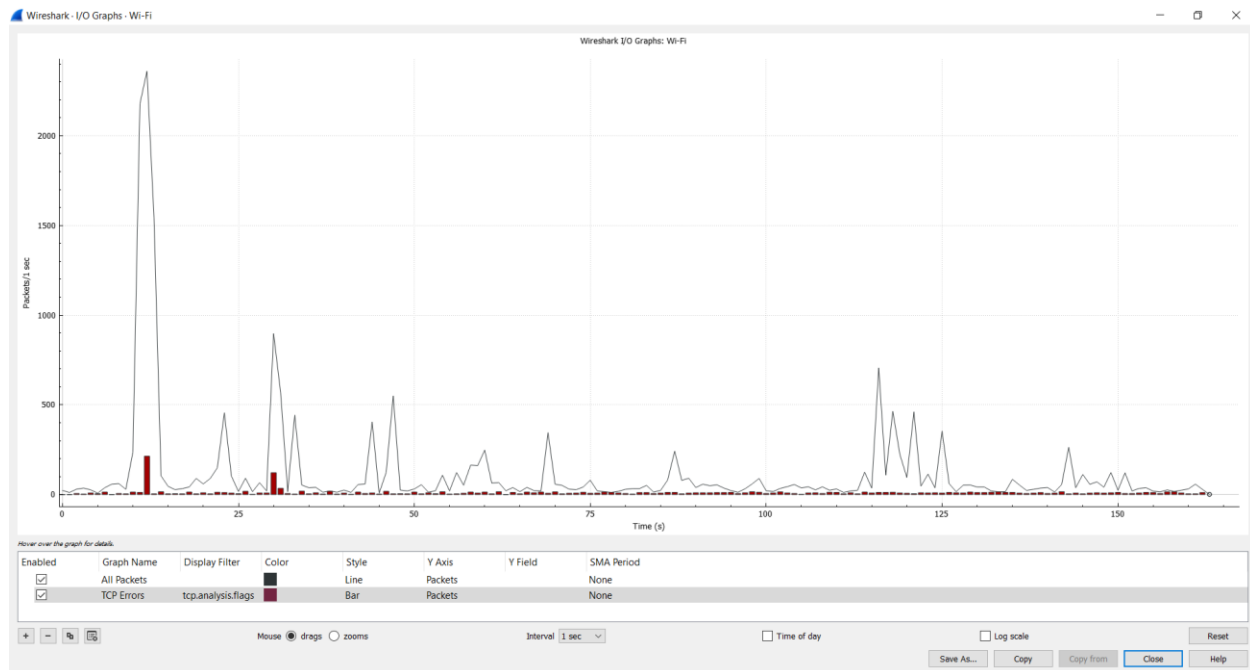
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::2074:9514:ad7e:2987%22
    IPv4 Address. . . . . : 192.168.43.175
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.43.1
  
```

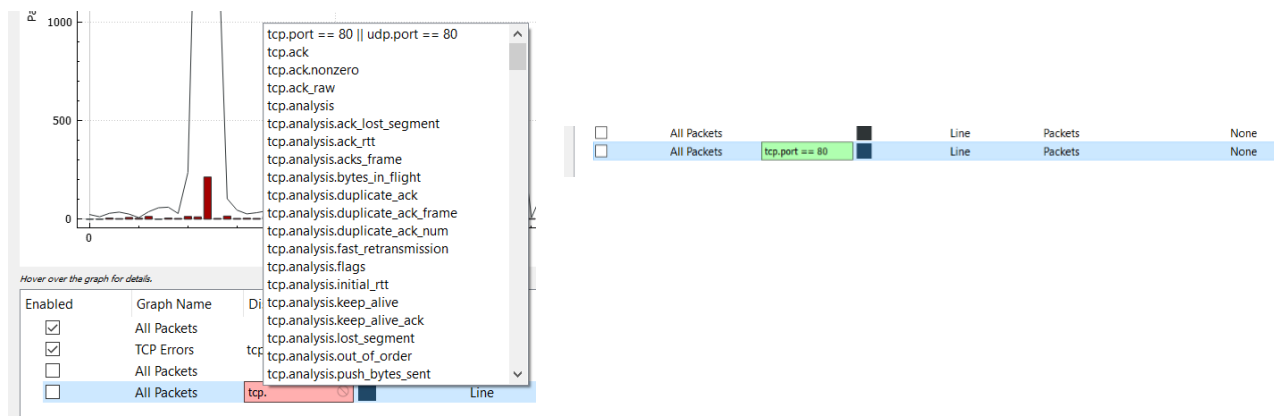
بنابراین

همانطور که مشخص است از روی تعداد بسته ها نمیتوان در زبانه IPv4 ، Default Gateway شبکه را تشخیص داد. در واقع بیشترین تعداد بسته مربوط به IPv4 Address مربوط به سیستم خودمان میباشد نه آدرس Default Gateway .

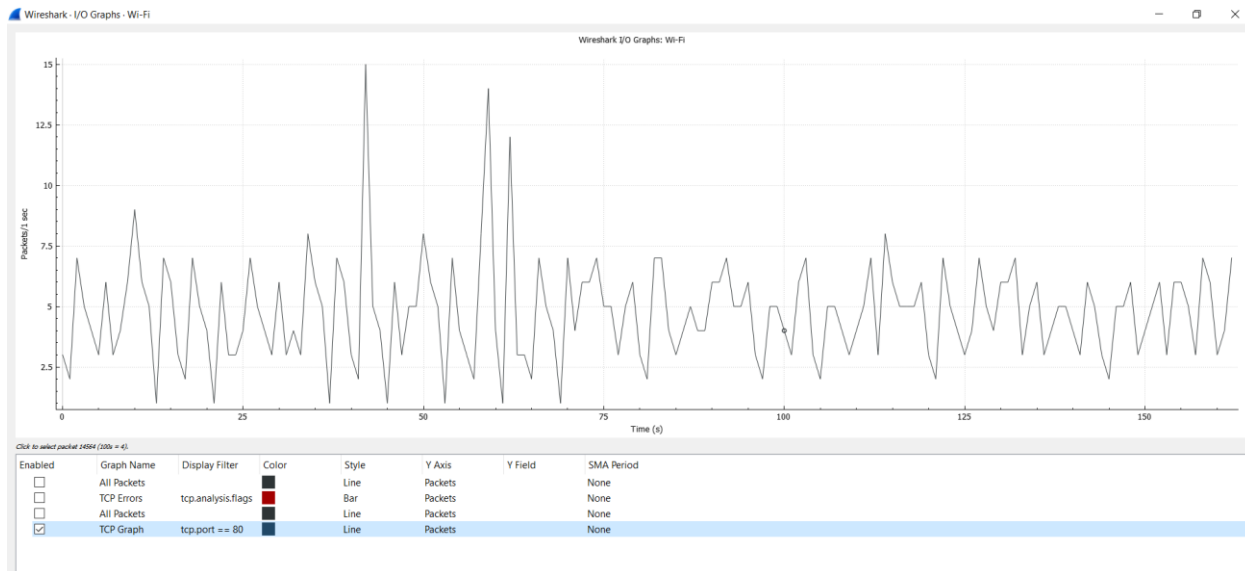
6. بر روی گزینه‌ی I/O Graph کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید نرخ I/O را مشاهده کنید. شما می‌توانید در این صفحه نمودارهای مختلفی بسازید. بر روی دکمه + در پایین پنجره باز شده کلیک کنید، سپس یک فیلتر به آن اضافه کنید تا نمودار تعداد بسته‌ها در ثانیه را مشاهده کنید. مشاهده می‌کنید که با کلیک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



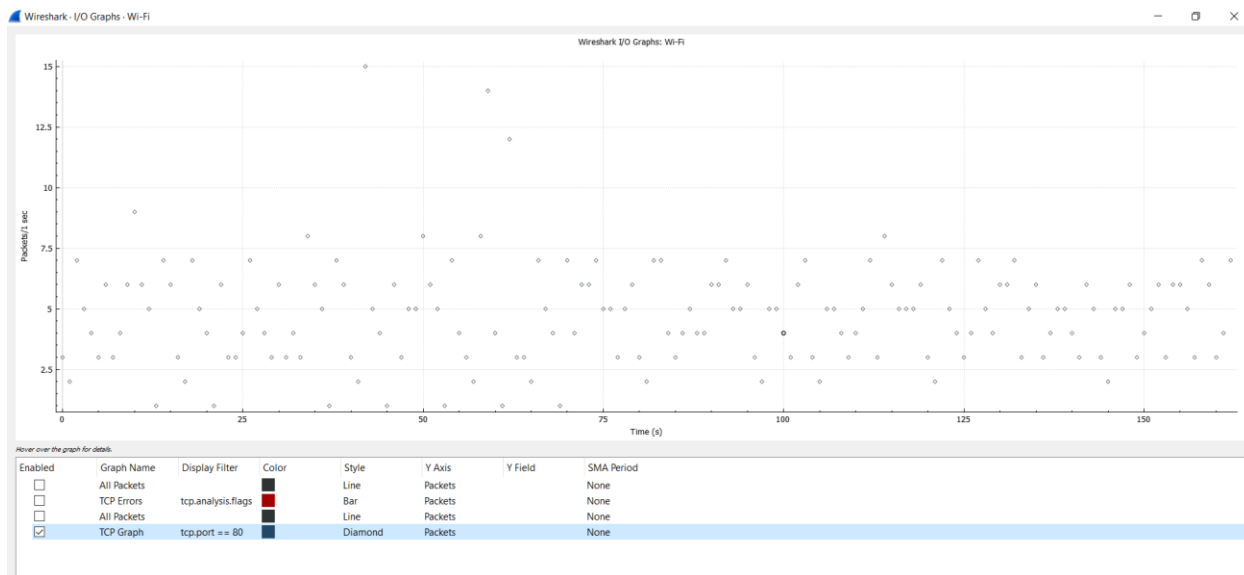
حال اگر بر روی + کلیک کنیم و بعد یک فیلتر اضافه کنیم، برای مثال فیلتر `tcp.port == 80` را اضافه کنیم:



و بعد این نمودار را نام گذاری و نمایش دهیم به صورت زیر میباشد:



همچنین میتوان استایل آن را نیز تغییر داد و به صورت Diamond قرار داد:



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 Displayed packets، Show را انتخاب کنید. به‌صورت کامل جزئیات مربوط به SeqNum و Ack و شماره پنجره را دنبال کنید.

ابتدا به منوی conversation مراجعه می‌کنیم و در آنجا یکی از ارتباطات TCP را سلکت می‌کنیم و بعد بر روی گزینه Graph در پایین صفحه می‌زنیم. برای مثال ارتباط TCP زیر را انتخاب کرده:

Wireshark - Conversations - Wi-Fi

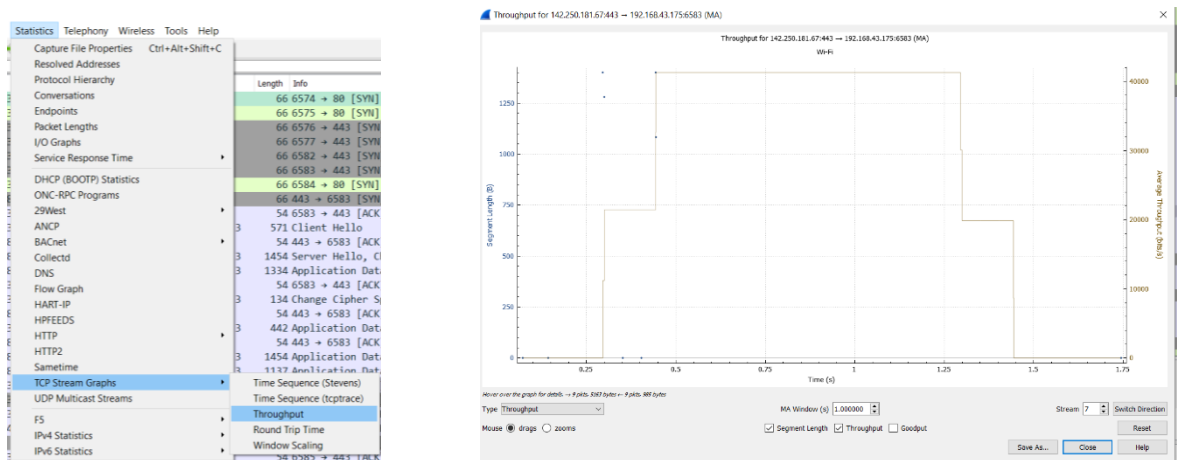
Ethernet - 3		IPv4 - 100		IPv6		TCP - 854		UDP - 233	
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.43.175	6622	8.8.4.4	443	8	973	4	745	4	228
192.168.43.175	11470	52.149.21.60	443	14	7045	6	5868	8	1177
192.168.43.175	6428	185.211.88.218	443	13	813	6	351	7	462
192.168.43.175	6623	91.108.4.166	443	2	132	2	132	0	0
192.168.43.175	6624	149.154.167.91	443	2	132	2	132	0	0
192.168.43.175	6625	91.108.4.166	80	2	132	2	132	0	0
192.168.43.175	6626	149.154.167.91	80	2	132	2	132	0	0
192.168.43.175	6627	142.250.181.42	443	12	4223	5	799	7	3424
192.168.43.175	30543	74.125.167.74	80	4	216	2	108	2	108
192.168.43.175	6628	185.211.88.131	443	3,582	4032k	789	85k	2,793	3946k
192.168.43.175	6629	185.211.88.131	443	846	946k	183	31k	663	914k
192.168.43.175	6630	216.58.207.4	443	18	7186	9	1544	9	5642
192.168.43.175	6631	185.211.88.131	443	1,377	1527k	325	42k	1,052	1484k
192.168.43.175	6632	185.211.88.131	443	1,222	1296k	322	40k	900	1256k
192.168.43.175	6633	185.211.88.131	443	750	836k	163	30k	587	805k
192.168.43.175	6634	149.154.166.120	443	4	264	4	264	0	0
192.168.43.175	6635	149.154.166.120	80	4	264	4	264	0	0
192.168.43.175	6636	8.8.4.4	443	17	1459	9	1015	8	444
192.168.43.175	11403	13.94.251.244	443	6	337	3	163	3	174
192.168.43.175	6637	91.108.4.166	443	3	198	3	198	0	0
192.168.43.175	6638	149.154.167.91	443	3	198	3	198	0	0
192.168.43.175	6639	149.154.167.91	80	3	198	3	198	0	0
192.168.43.175	6640	91.108.4.166	80	3	198	3	198	0	0
192.168.43.175	6542	8.8.4.4	443	1	54	0	0	1	54
192.168.43.175	11405	68.232.34.200	443	5	283	3	163	2	120
192.168.43.175	6641	142.250.181.42	443	19	7787	9	1656	10	6131
192.168.43.175	6642	149.154.175.54	443	4	264	4	264	0	0
192.168.43.175	6643	149.154.167.80	443	4	264	4	264	0	0
192.168.43.175	6644	149.154.175.54	80	4	264	4	264	0	0
192.168.43.175	6645	149.154.167.50	443	4	264	4	264	0	0
192.168.43.175	6646	149.154.167.51	443	4	264	4	264	0	0
192.168.43.175	6647	149.154.167.51	80	4	264	4	264	0	0
192.168.43.175	6648	149.154.167.50	80	4	264	4	264	0	0
192.168.43.175	25097	140.82.121.5	443	6	363	3	162	3	201
192.168.43.175	1024	18.195.36.214	443	8	484	4	220	4	264
192.168.43.175	6649	104.16.248.249	443	20	6448	9	1519	11	4929
192.168.43.175	6650	5.28.194.14	443	1	66	1	66	0	0
192.168.43.175	6651	5.28.194.123	443	2	132	2	132	0	0

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time

Copy Follow Stream... Graph... Close Help

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 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 بر حسب بایت در ارتباط TCP را در آن زمان نمایش می‌دهد. با افزایش شماره‌های که در پایین پنجره با نام Stream قرار دارد می‌توانید ارتباط TCP خود را عوض کنید. منظور از Goodput نرخ است که کاربرد داده خود را دریافت می‌کند و در آن Retransmission ها در نظر گرفته نمی‌شوند.

طبق توضیحات بالا هم می‌توان از گزینه TCP Stream Graph کمک گرفت و به قسمت throughput رفت و سپس نمودار مربوطه را در پنجره باز شده مشاهده کرد. مانند زیر :



حال براساس توضیحات ویدئو پیش می‌رویم. و این قسمت را تکرار میکنیم. ابتدا به زبانه statistics می‌رویم و گزینه conversation را انتخاب میکنیم. سپس یکی از ارتباطات TCP را سلکت میکنیم . برای مثال نشست سلکت شده زیر را انتخاب میکنیم که تعداد بسته های تقریباً زیادی دارد:

Edit

View

Go

Capture

Analyze

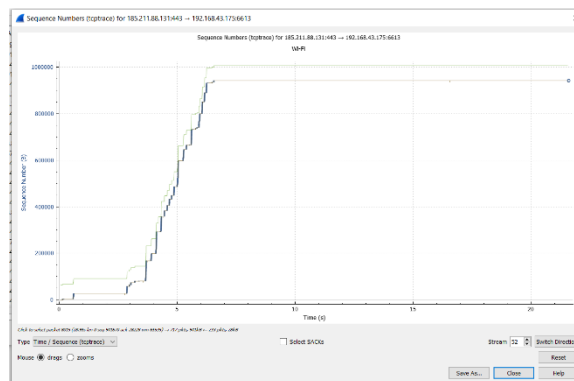
Statistics

Telephony

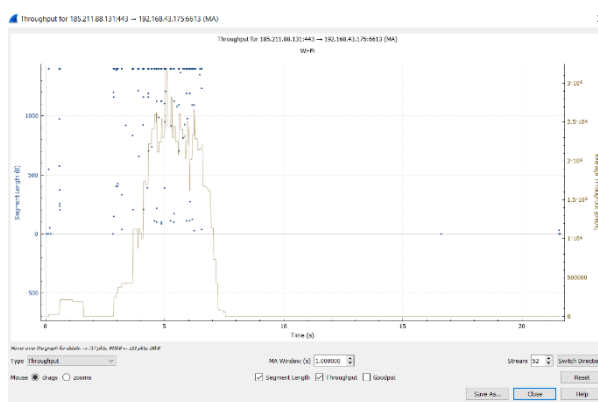
Tools

Help

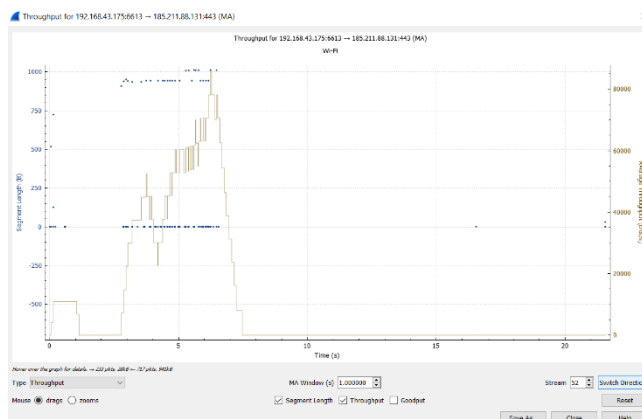
سپس روی گزینه Graph در پایین صفحه میزینیم و صفحه‌ی زیر را نشان میدهد.



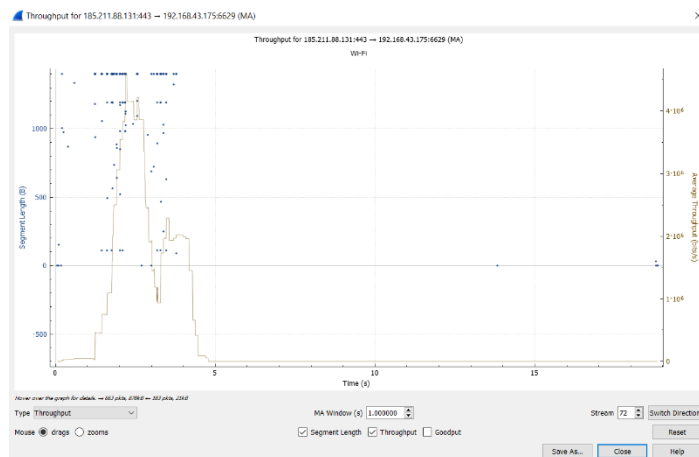
حال در قسمت type میتوان گزینه throughput را انتخاب کرد:



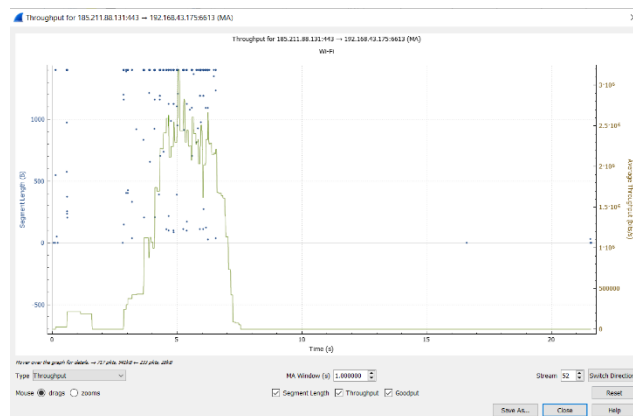
در این پنجره می‌توان throughput کانکشن مربوطه را مشاهده کرد و برحسب segment length بر ثانیه میباشد و میگوید در هر ثانیه طول سگمنت چی بوده است. این segment length نیز برحسب بایت میباشد. میتوان average throughput را برحسب بیت بر ثانیه نیز مشاهده کرد و میتوان متوجه شد که کجاها segment length را کاهش دادیم و کجاها روی ماکسیمم segment length بودیم اگر گزینه‌ی Switch Direction را انتخاب کنیم، ارتباط در جهت برعکس را میتوان بررسی کرد:



میتوان با افزایش شمارنده‌ای که در پایین پنجره با نام Stream قرار دارد ، ارتباط TCP خود را عوض کرد. برای مثال همانطور که در اسکرین های قبلی مشاهده شد مقدارش 52 بود که میتوان آن را تغییر داد و 72 گذاشت که با پنجره زیر مواجه میشویم که در واقع ارتباط TCP خود را عوض کردیم:

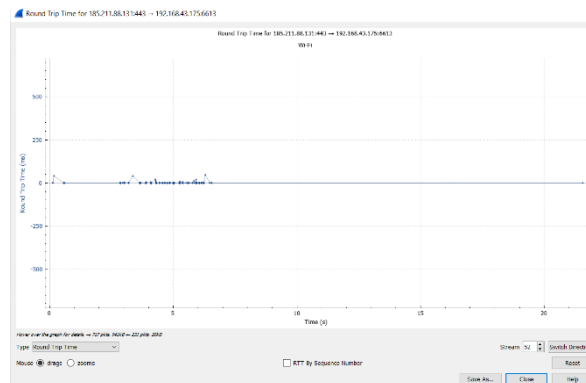


همچنین میتوان گزینه Goodput را انتخاب کرد که در آن Retransmission ها در نظر گرفته نمی‌شوند.

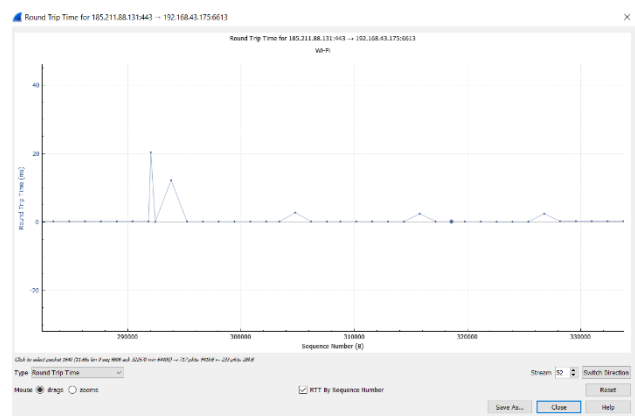
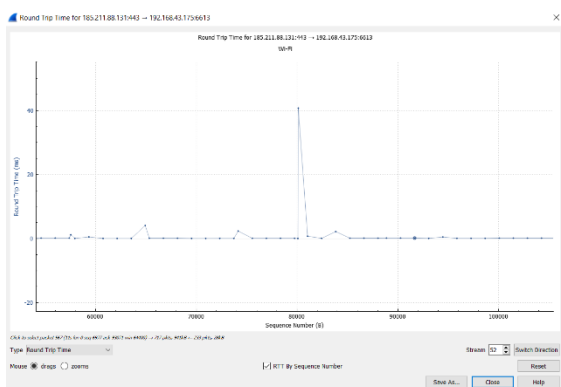


البته لازم است تا ارتباط کمی نویزی باشد یا در آن congestion رخ دهد که در آن retransmission معنی ندهد.

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. 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. حال اگر در این Graph از قسمت type گزینه Round Trip Time را انتخاب کنیم:



اگر گزینه RTT By Sequence Number را فعال کنیم تا نمودار را برحسب شماره بسته‌ها داشته باشیم به جای اینکه برحسب زمان داشته باشیم و بعد کمی زوم کنیم، خواهیم داشت:



همانطور که مشاهده میشود مقدار RTT غالباً برای بسته‌ها کم و در حد چند میلی ثانیه و حتی کم‌تر بوده و برای بسته‌های خیلی کمی تا حدود 20 یا 40 میلی ثانیه نیز این مقدار زیاد شده است. یکی از علل کم بودن این مقدار میتواند این باشد که ما ارتباط اینترنتی خوبی داشتیم.

10. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Window Scaling کلیک کنید. پنجره‌ای 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.

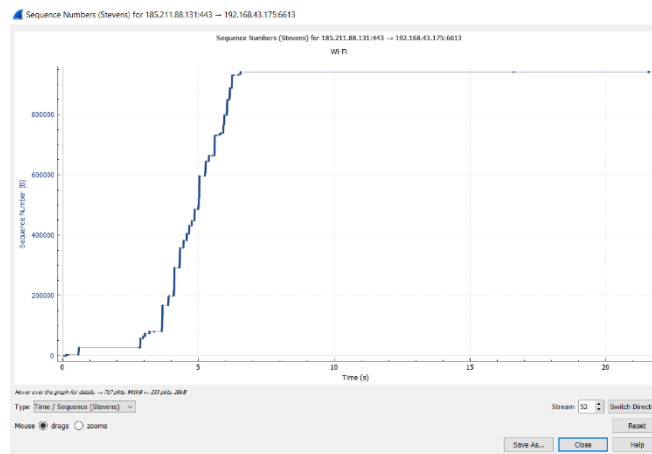
حال اگر در این Graph از قسمت type گزینه Window Scaling را انتخاب کنیم پنجره زیر باز می‌شود:



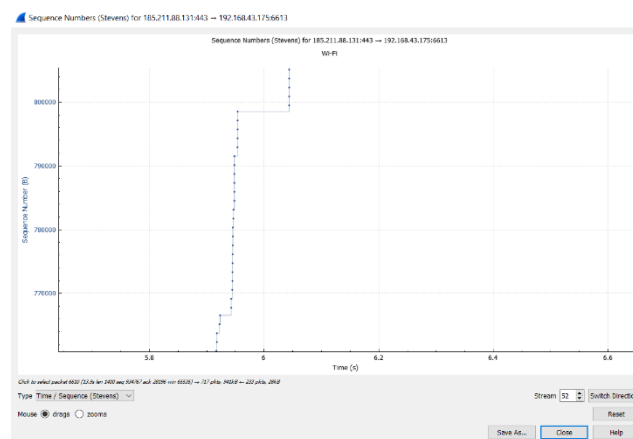
مشخصاً راجع به window size صحبت میکند، قبل تر segment size بود این Window size میباشد. از این نمودار که Window size را نشان میدهد میتوان استفاده کرد برای اینکه فهمید که چه اتفاقاتی برای ارتباطمان داشته میفتاده است و مثلاً حجم داده ارسالی و دریافتی چه قدر بودند و کجاها مجبور شدیم که Window size را کم کنیم و ... همچنین براساس زمان نشان میدهد که در گذر زمان Window size ما چه تغییراتی داشته است.

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.

حال اگر در این Graph از قسمت type گزینه Time / Sequence (Stevens) را انتخاب کنیم پنجره زیر باز می‌شود:



همچنین در این نمودار میتوان بازه هایی را مشاهده کرد که در آن ها مقدار sequence number تغییر نکرده است. یک دلیلش میتواند این باشد که اپلیکشن wait کرده یا اینکه خطایی رخ داده است.



همچنین Sequence number در TCP نیز بر حسب بایت میباشد.

سوال 9: به سایت دانلود دانشگاه مراجعه کنید

<http://download.aut.ac.ir/>

به صورت 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 به عنوان 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 به صورت دقیق بررسی کنید.

ابتدا به محل نصب wireshark می‌رویم و سپس دستور D -tshark را وارد می‌کنیم:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files\Wireshark

C:\Program Files\Wireshark>tshark -D
1. \Device\NPF_{50BF86FC-A643-44AB-9109-B17DFE87514C} (VirtualBox Host-Only Network)
2. \Device\NPF_{3A0E6F81-04EF-4BC9-9838-23468A28A90A} (Local Area Connection* 7)
3. \Device\NPF_{C6C42AE3-E178-4F00-830E-82E4C87AF868} (Bluetooth Network Connection)
4. \Device\NPF_{3E32F455-B79D-4428-BDE7-6E807EB6423E} (Local Area Connection* 2)
5. \Device\NPF_{7E6A5258-6A9A-438C-AE4C-5EA299631802} (Local Area Connection* 8)
6. \Device\NPF_{57E0E952-C242-494C-AA2D-118061015E99} (Local Area Connection* 12)
7. \Device\NPF_{6BFD3001-3139-4BDE-8576-A6F31517C553} (Local Area Connection* 9)
8. \Device\NPF_{CAE5FEBA-2CC2-4C5C-8D36-149CC2956931} (Wi-Fi)
9. \Device\NPF_{Loopback (Adapter for loopback traffic capture)}
10. \Device\NPF_{60F1AF36-C3EB-4A96-9C63-87B0036AF1BD} (Local Area Connection)
11. \Device\NPF_{94CC4AF3-EDCB-4866-8509-D27CC2EF2FE0} (Ethernet)
12. \Device\NPF_{84A18F8F-07EC-4080-876F-6B5CC4724DC2} (Ethernet 2)
```

با توجه به عکس فوق عدد اینترفیسی که می‌خواهیم روی آن شنود کنیم 8 می‌باشد که همان Wi-Fi من می‌باشد. حال دو فایل حجیم را شروع به دانلود می‌کنیم و با دستوری که در عکس زیر آمده است عملیات شنود را به مدت یک دقیقه آغاز می‌کنیم:

```
C:\Program Files\Wireshark>tshark -i 8 -p -w output.pcap
Capturing on 'Wi-Fi'
290255

C:\Program Files\Wireshark>
```

حال باید فایل زیر را در wireshark باز کنیم:

output.pcap 6/20/2021 11:59 PM Wireshark capture ... 329,068 KB

اگر این فایل را باز کنیم به صورت زیر خواهد بود که تعداد بسیار زیادی بسته capture شده است:

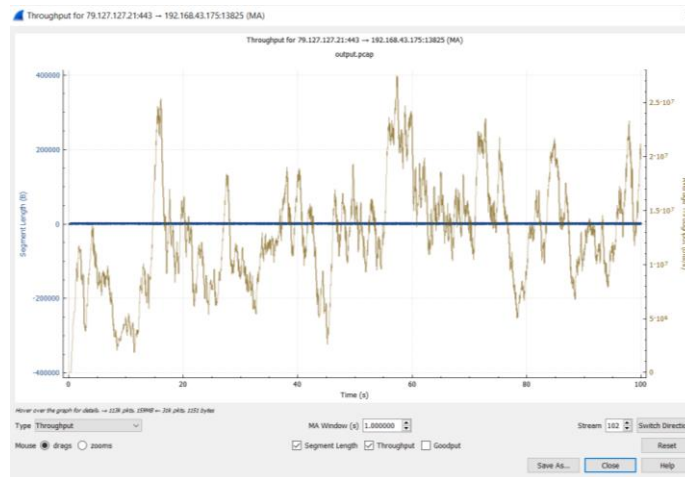
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.175	149.154.175.100	TCP	66	13739 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.009521	192.168.43.175	91.108.4.166	TCP	66	13742 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.010472	192.168.43.175	149.154.167.91	TCP	66	13743 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.010803	192.168.43.175	142.250.181.100	TCP	66	13744 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.013614	192.168.43.175	91.108.4.166	TCP	66	13745 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	0.013876	192.168.43.175	149.154.167.91	TCP	66	13746 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	0.056800	192.168.43.175	8.248.95.254	ICMP	186	Echo (ping) request id=0x0001, seq=682/43522, ttl=28 (no response found!)
8	0.091893	142.250.181.100	192.168.43.175	TCP	66	443 → 13744 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=256
9	0.092131	192.168.43.175	142.250.181.100	TCP	54	13744 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
10	0.092681	192.168.43.175	5.28.154.123	TCP	66	13741 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	0.092781	192.168.43.175	5.28.154.14	TCP	66	13740 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	0.122420	192.168.43.175	142.250.181.100	TLSv1.3	571	Client Hello
13	0.163913	142.250.181.100	192.168.43.175	TCP	54	443 → 13744 [ACK] Seq=1 Ack=518 Win=94720 Len=0
14	0.315717	192.168.43.175	149.154.167.50	TCP	66	13747 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	0.316745	192.168.43.175	149.154.167.51	TCP	66	13748 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	0.322962	192.168.43.175	149.154.167.51	TCP	66	13749 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	0.323943	192.168.43.175	149.154.167.50	TCP	66	13750 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	0.331005	142.250.181.100	192.168.43.175	TLSv1.3	1454	Server Hello, Change Cipher Spec
19	0.332142	142.250.181.100	192.168.43.175	TLSv1.3	1297	Application Data
20	0.332191	192.168.43.175	142.250.181.100	TCP	54	13744 → 443 [ACK] Seq=518 Ack=2644 Win=131584 Len=0
21	0.335264	192.168.43.175	142.250.181.100	TLSv1.3	134	Change Cipher Spec, Application Data
22	0.376754	142.250.181.100	192.168.43.175	TCP	54	443 → 13744 [ACK] Seq=2644 Ack=598 Win=94720 Len=0
23	0.376832	192.168.43.175	142.250.181.100	TLSv1.3	455	Application Data
24	0.408058	142.250.181.100	192.168.43.175	TCP	54	443 → 13744 [ACK] Seq=2644 Ack=999 Win=95744 Len=0
25	0.456209	142.250.181.100	192.168.43.175	TLSv1.3	1454	Application Data
26	0.456328	142.250.181.100	192.168.43.175	TLSv1.3	1187	Application Data, Application Data
27	0.456366	192.168.43.175	142.250.181.100	TCP	54	13744 → 443 [ACK] Seq=999 Ack=5177 Win=131584 Len=0
28	0.504989	192.168.43.175	149.154.167.91	TCP	66	13718 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
29	0.507997	192.168.43.175	91.108.4.166	TCP	66	13717 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	0.513041	192.168.43.175	149.154.167.91	TCP	66	13719 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

لازم به ذکر است چون دوسایت پیشنهادی باز نمیشدند من دو فایل حجیم گرفته شده را از soft98.ir دانلود کردم.

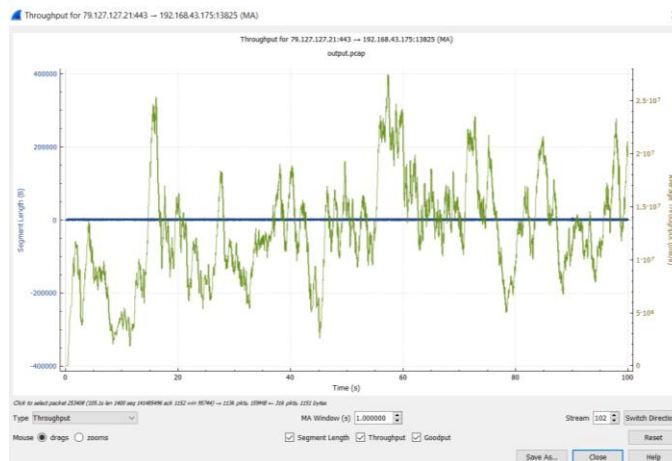
اگر به قسمت conversation برویم و بعد به قسمت زبانه TCP برویم و سپس براساس تعداد بسته های تبادل شده مرتب کنیم، آن آدرس IP که بیشترین تبادل را با آن داشتیم متعلق به IP همان سروری است که از آن دانلود کرده ایم. که در اینجا IP موردنظر ما برابر با 79.127.127.21 میباشد که سایت soft98.ir میباشد:

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 → A
192.168.43.175	10866	142.250.181.138	443	21	9356	10	1722	11	7634	57.602196	3.0090	4578	20k
192.168.43.175	10960	216.58.208.234	443	21	9357	10	1722	11	7635	76.878021	2.3371	5894	26k
192.168.43.175	11111	216.58.208.234	443	21	9357	10	1722	11	7635	107.787446	1.8876	7298	32k
192.168.43.175	13046	104.16.249.240	443	22	7981	10	1599	12	6382	10.401019	1.6857	7588	30k
192.168.43.175	10745	104.16.249.240	443	22	7960	10	1577	12	6383	33.778499	1.7029	7408	29k
192.168.43.175	10838	104.16.249.240	443	22	8019	10	1639	12	6380	53.370122	1.2205	10k	41k
192.168.43.175	10878	104.16.249.240	443	22	7944	10	1562	12	6382	61.994476	1.6740	7464	30k
192.168.43.175	10908	104.16.249.240	443	22	7993	10	1610	12	6383	65.598186	1.4139	9109	36k
192.168.43.175	10961	104.16.249.240	443	22	7928	10	1546	12	6382	77.680606	1.6645	7430	30k
192.168.43.175	10992	104.16.249.240	443	22	7929	10	1546	12	6383	81.598094	1.5938	7760	32k
192.168.43.175	11027	104.16.249.240	443	22	7934	10	1551	12	6383	89.598219	0.9921	12k	51k
192.168.43.175	11112	104.16.249.240	443	22	7951	10	1569	12	6382	108.585961	1.1072	11k	46k
192.168.43.175	13807	142.250.181.14	443	22	9489	10	1504	12	7985	10.343697	3.6235	3320	17k
192.168.43.175	10850	142.250.181.14	443	22	10k	10	1503	12	9385	56.006789	4.6103	2608	16k
192.168.43.175	10956	142.250.181.14	443	22	10k	10	2066	12	7997	75.278642	4.0458	4085	15k
192.168.43.175	11082	142.250.181.14	443	22	9472	10	1487	12	7985	103.998768	2.3409	5064	27k
192.168.43.175	13834	172.217.19.163	443	22	9414	11	2180	11	7234	16.505800	3.5330	4936	16k
192.168.43.175	10683	172.217.19.163	443	22	10k	11	1575	11	8623	24.001426	2.5058	5028	27k
192.168.43.175	10794	104.16.249.240	443	23	6625	10	1591	13	5034	43.882733	1.8641	6827	21k
192.168.43.175	10932	142.250.181.14	443	23	10k	11	1570	12	9386	71.997602	3.3888	3706	22k
192.168.43.175	11007	142.250.181.14	443	23	11k	11	1652	12	9386	87.998375	2.5890	5104	29k
192.168.43.175	8056	46.46.40.45	80	26	1443	13	705	13	738	7.522243	102.1988	55	57
192.168.43.175	13096	13.224.195.52	443	28	1691	14	791	14	900	3.779840	105.7799	59	68
192.168.43.175	10785	52.109.88.174	443	66	40k	30	28k	36	12k	42.567047	2.3030	97k	44k
192.168.43.175	13772	79.127.127.21	443	142	181	159M	33,822	190k	108,359	157M	6,045,494	108,7813	140k
192.168.43.175	13825	79.127.127.21	443	144,866	166M	31,278	1757k	113,588	165M	14,933,358	99,8979	140k	11M

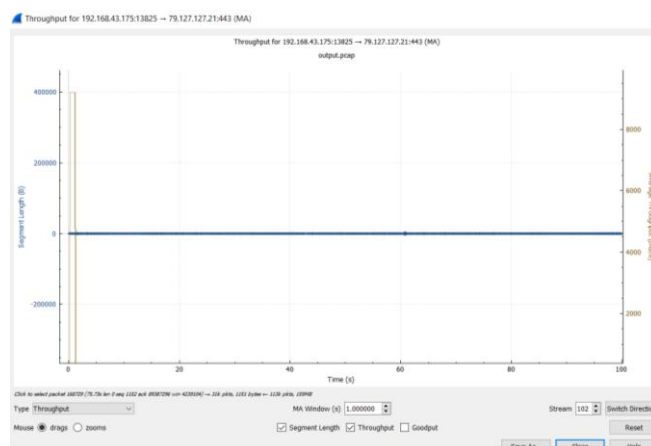
سپس اگر آن را به عنوان یک فیلتر اعمال کنیم و نمودارهای خواسته شده را به دست آوریم:
نمودار Throughput به صورت زیر است:



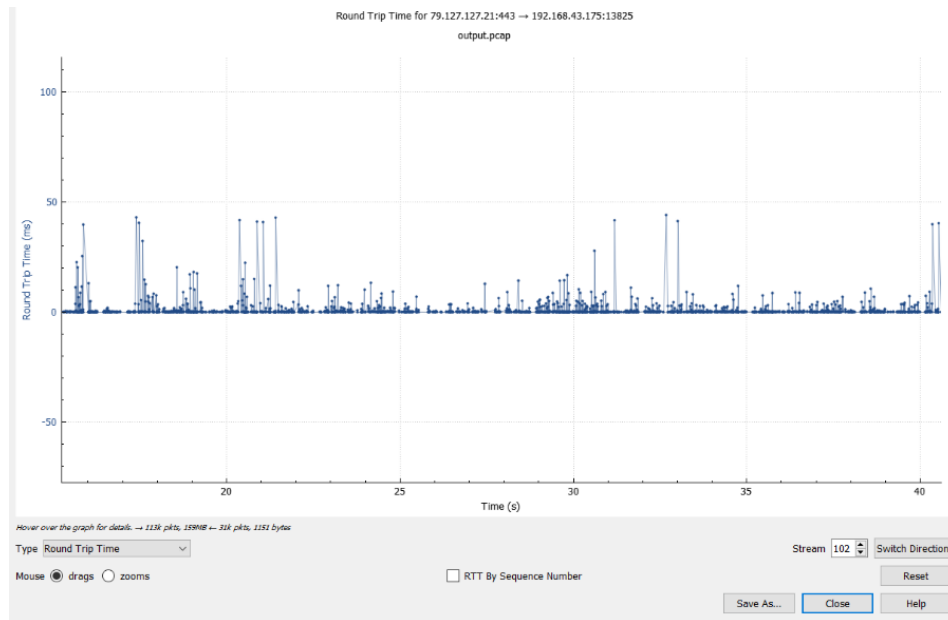
حال اگر Goodput را هم فعال کنیم:



و اگر بر روی switch direction بزنیم:

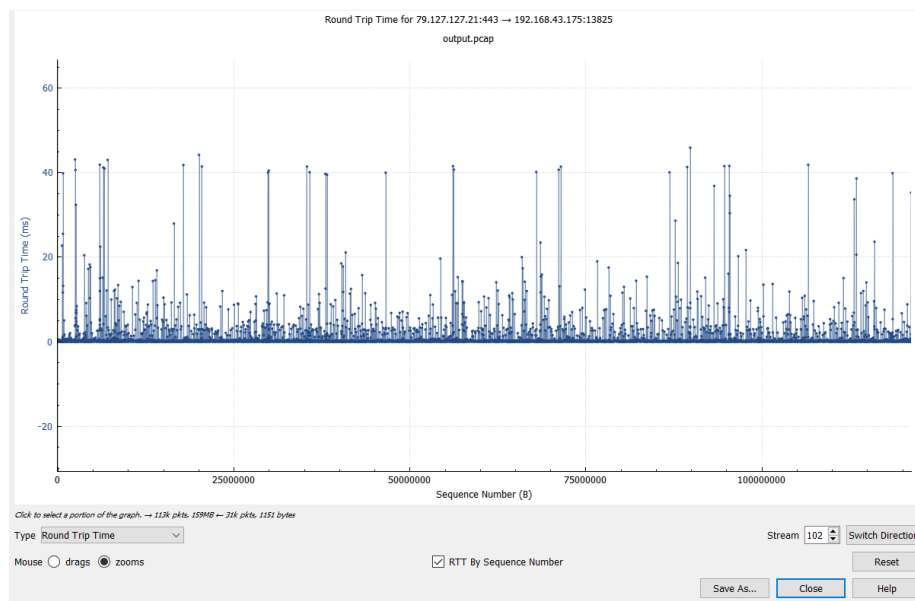


نمودار Round Trip Time به صورت زیر است:

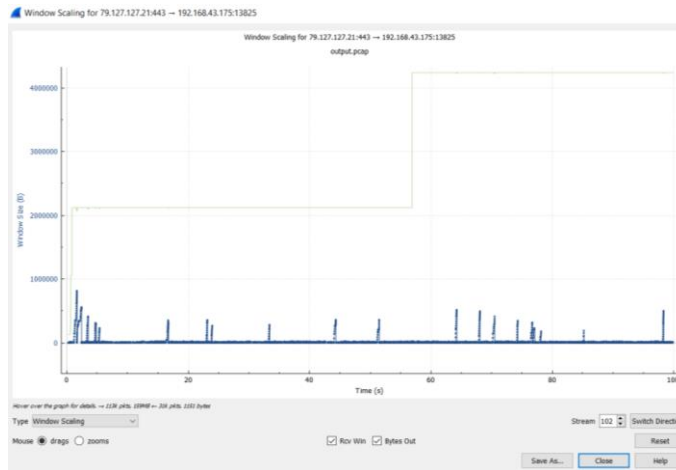


همانطور که مشاهده میشود غالباً زیر 45 میلی ثانیه میباشد.

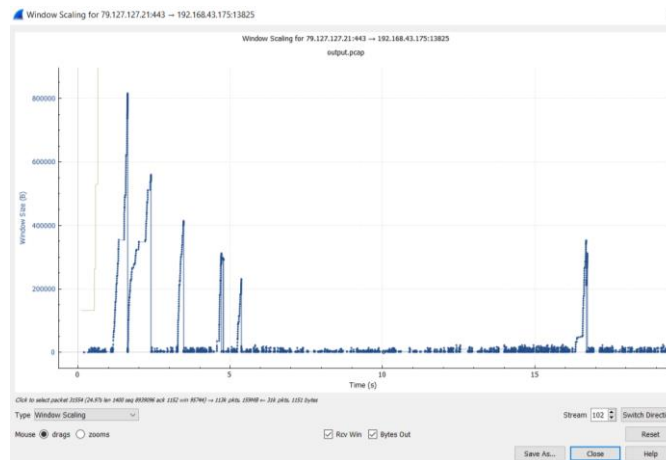
اگر نمودار RTT By Sequence Number به صورت زیر میشود:



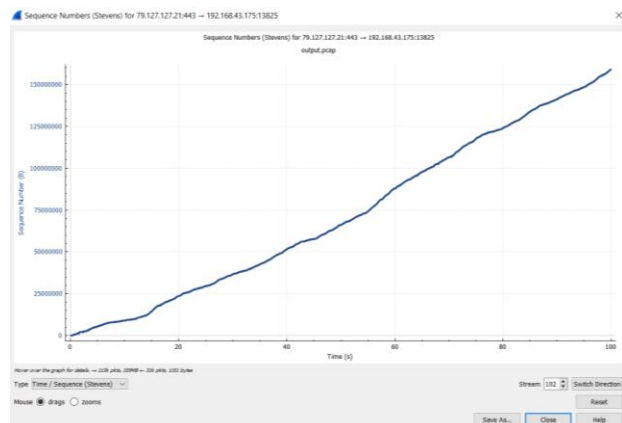
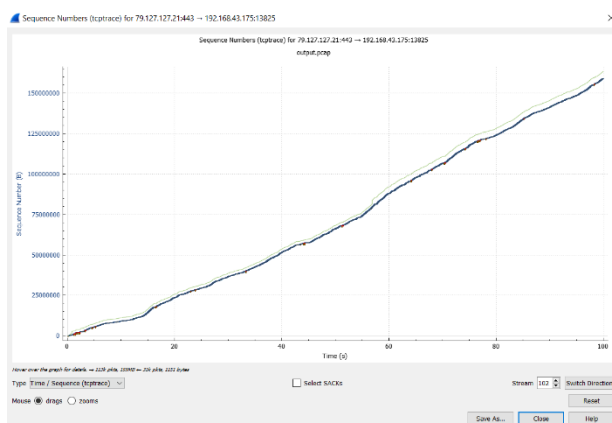
نمودار Window Scaling به صورت زیر است:



و با کم کردن به صورت زیر میباشد:



همچنین نمودارهای Time/Sequence(Stevens) در راست و Time/Sequence(tcptrace) در چپ میباشند:



در صورت وقوع ازدحام طبق آنچیزی که در ویدیو گفته شد نموداری که میگیریم نمودار دندان کوسه ای میباشد و وقتی window size بزرگ میشود congestion رخ میدهد و خب مجبور به کم کردن window size میشیم و به این شکل همانطور که گفته شد یک نمودار دندان کوسه ای خواهیم داشت.