دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه های کامپیوتری

(پاییز ۱۴۰۰)

جلسه پنجم

تحلیل **TCP** با استفاده از **Whireshark**

محمد چوپان ۹۸۳۱۱۲۵

۱- تحلیل TCP با استفاده از Wireshark

۱-۱- هدف آزمایش

در این آزمایش قصد داریم آشنایی بیشتری با نرم‌افزار Wireshark و منوی Statistics در آن پیدا کنیم و از امکانات آن برای تحلیل بسته‌های جمع‌آوری‌شده استفاده نماییم.

۱-۲- فعالیت‌های قبل از آزمایش

دستور کار جلسه‌ی آشنایی با wireshark را مرور کنید.

۱-۳- شرح آزمایش

نرم‌افزار wireshark را باز کرده، چند دقیقه به وب گردی بپردازید و بسته‌ها را جمع‌آوری کنید. سپس مطابق جمع‌آوری بسته را متوقف کرده و از منوی بالا بر روی گزینه‌ی Statistics کلیک کنید. در ادامه قصد داریم مواردی که در این زبانه وجود دارند را بررسی کنیم.

۱. بر روی گزینه‌ی Resolved Addresses کلیک کنید.

سوال ۱: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

در این قسمت آدرس ip که به آن متصل شدیم را نشان می دهد که host ها را به چه ip هایی متصل کرده است و علاوه بر آن آدرس فیزیکی کارت شبکه جایی که آن متصل شده ایم را هم برای ما می آورد.

142.250.185.42	cloudsearch.googleapis.com
142.250.180.42	content-autofill.googleapis.com
108.138.7.100	dexeqbeb7giwr.cloudfront.net
108.138.7.13	dexeqbeb7giwr.cloudfront.net
108.138.7.81	dexeqbeb7giwr.cloudfront.net

03:00:00:00:00:10	(OS/2-1.3-EE+Communications-Manager)
03:00:00:00:00:40	(OS/2-1.3-EE+Communications-Manager)
70:02:58	01Db-Metravib
7c:cb:e2:20:00:00	1000eyes
70:b3:d5:7e:60:00	11811347

سوال ۲: آیا می‌توانید ســـه بایت اولی که برای آدرس فیزیکی کارت‌های شـــبکه Cisco می‌باشند را مشخص کنید؟

بله وقتی از منوی بالا Ethernet Well-Known Addresses را انتخاب کنیم برای ما تمامی کارت های شبکه های شناخته شده را می آورد و در نهایت زمانی که cisco را سرچ کنیم :

00:07:0d	Cisco
00:10:79	Cisco
00:60:3e	Cisco
00:90:f2	Cisco
00:60:70	Cisco
00:60:09	Cisco
00:90:2b	Cisco

نتیجه بالا را مشاهده میکنیم.

۲. بر روی گزینه‌ی protocol hierarchy کلیک کنید.

سوال ۳: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

با اســـتفاده از مدل لایه ای پرتکل هایی که وجود دارند با مقدار درصـــد اســـتفاده و یا مقادیر انتقال داده آن ها را به ما نشان می دهد. که مثلا در جستجوی شما ۵۰ % پرتکل IPV4 بوده است .

سوال ۴: چند درصد بسته‌های شما به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند؟

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	42154	100.0	36179147	4046 k	0	0	0
Ethernet	100.0	42154	1.6	590156	66 k	0	0	0
Internet Protocol Version 6	0.1	44	0.0	1760	196	0	0	0
Internet Protocol Version 4	99.9	42106	2.3	842120	94 k	0	0	0
User Datagram Protocol	1.5	647	0.0	5176	578	0	0	0
Transmission Control Protocol	98.3	41456	95.6	34577661	3867 k	35935	31496482	3522 k
Internet Control Message Protocol	0.0	3	0.0	1668	186	3	1668	186
Address Resolution Protocol	0.0	4	0.0	112	12	4	112	12

با توجه به شکل بالا ۹۸/۳ درصد بسته ها این مورد را شامل می شوند.

۳. بر روی گزینه‌ی Conversations کلیک کنید.

سوال ۵: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

می بینیم که نشست ها را با توجه به پروتکل های آن ها دسته بندی کرده است.

Ethernet · 3 | IPv4 · 39 | IPv6 · 2 | TCP · 54 | UDP · 22

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
13.107.21.200	443	192.168.1.35	55287	2	109	1	55	1	54	18.978969	0.0001	—	
52.97.153.178	443	192.168.1.35	54795	10	685	5	415	5	270	8.982128	59.9827	55	
185.5.160.42	80	192.168.1.35	55117	18,026	15 M	11,195	15 M	6,831	466 k	0.048506	71.4752	1732 k	
192.168.1.35	55370	185.5.160.43	80	16,286	14 M	6,128	420 k	10,158	14 M	0.000000	71.5155	47 k	
192.168.1.35	55010	3.142.211.167	443	29	4646	13	2542	16	2104	0.235524	66.5703	305	
192.168.1.35	55637	185.195.79.35	443	2	132	2	132	0	0	0.748063	1.0014	1054	
192.168.1.35	55638	185.195.79.19	443	2	132	2	132	0	0	0.748868	1.0006	1055	
192.168.1.35	55639	218.232.76.179	443	2	132	2	132	0	0	0.749655	1.0099	1045	
192.168.1.35	55250	142.250.180.46	443	23	3799	11	2249	12	1550	1.770738	63.1757	284	
192.168.1.35	55237	35.186.224.47	443	12	846	6	429	6	417	2.505449	62.1790	55	
192.168.1.35	55659	185.195.79.35	443	2	132	2	132	0	0	3.732121	1.0054	1050	
192.168.1.35	55660	185.195.79.19	443	2	132	2	132	0	0	3.732931	1.0046	1051	
192.168.1.35	55661	218.232.76.179	443	2	132	2	132	0	0	3.733763	1.0038	1052	

۴. 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.

۵. بر روی گزینه‌ی endpoints کلیک کنید.

سوال ۶: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

مقصد هایی که در قالب پروتکل های متفاوت با آن ها در ارتباط بوده ایم .

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
3.142.211.167	443	29	4646	16	2104	13	
13.107.21.200	443	2	109	1	55	1	
18.232.217.40	443	103	47 k	48	27 k	55	
34.98.74.57	443	10	566	4	240	6	
35.186.224.18	443	10	566	4	240	6	
35.186.224.25	443	2	109	1	54	1	
35.186.224.47	443	12	846	6	417	6	
35.188.42.15	443	10	660	0	0	10	
52.38.13.34	443	82	31 k	37	12 k	45	
52.97.153.178	443	10	685	5	415	5	
52.109.76.41	443	4	216	0	0	4	
67.20.113.35	443	108	65 k	62	60 k	46	
104.66.71.233	80	8	444	4	228	4	
104.199.65.124	4070	6	357	3	184	3	
108.138.7.100	443	53	17 k	28	13 k	25	

سوال ۷: چه مقصـــدهایی برای ارتباط‌های TCP در ســیســـتم شـــما اســـتفاده شده‌اند؟

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
3.142.211.167	443	29	4646	16	2104	13	
13.107.21.200	443	2	109	1	55	1	
18.232.217.40	443	103	47 k	48	27 k	55	
34.98.74.57	443	10	566	4	240	6	
35.186.224.18	443	10	566	4	240	6	
35.186.224.25	443	2	109	1	54	1	
35.186.224.47	443	12	846	6	417	6	
35.188.42.15	443	10	660	0	0	10	
52.38.13.34	443	82	31 k	37	12 k	45	
52.97.153.178	443	10	685	5	415	5	
52.109.76.41	443	4	216	0	0	4	
67.20.113.35	443	108	65 k	62	60 k	46	
104.66.71.233	80	8	444	4	228	4	
104.199.65.124	4070	6	357	3	184	3	
108.138.7.100	443	53	17 k	28	13 k	25	
140.82.112.26	443	5	337	3	199	2	
142.250.102.188	5228	2	121	1	66	1	
142.250.180.46	443	23	3799	12	1550	11	
142.250.181.163	443	4	242	2	132	2	
151.101.112.176	443	47	23 k	26	20 k	21	
185.5.160.42	80	18,026	15 M	11,195	15 M	6,831	
185.5.160.43	80	16,286	14 M	10,158	14 M	6,128	
185.140.5.168	443	271	163 k	159	140 k	112	
185.195.79.19	443	8	528	0	0	8	
185.195.79.35	443	8	528	0	0	8	
185.199.110.133	443	2	121	1	66	1	
185.211.88.218	443	4	242	2	132	2	

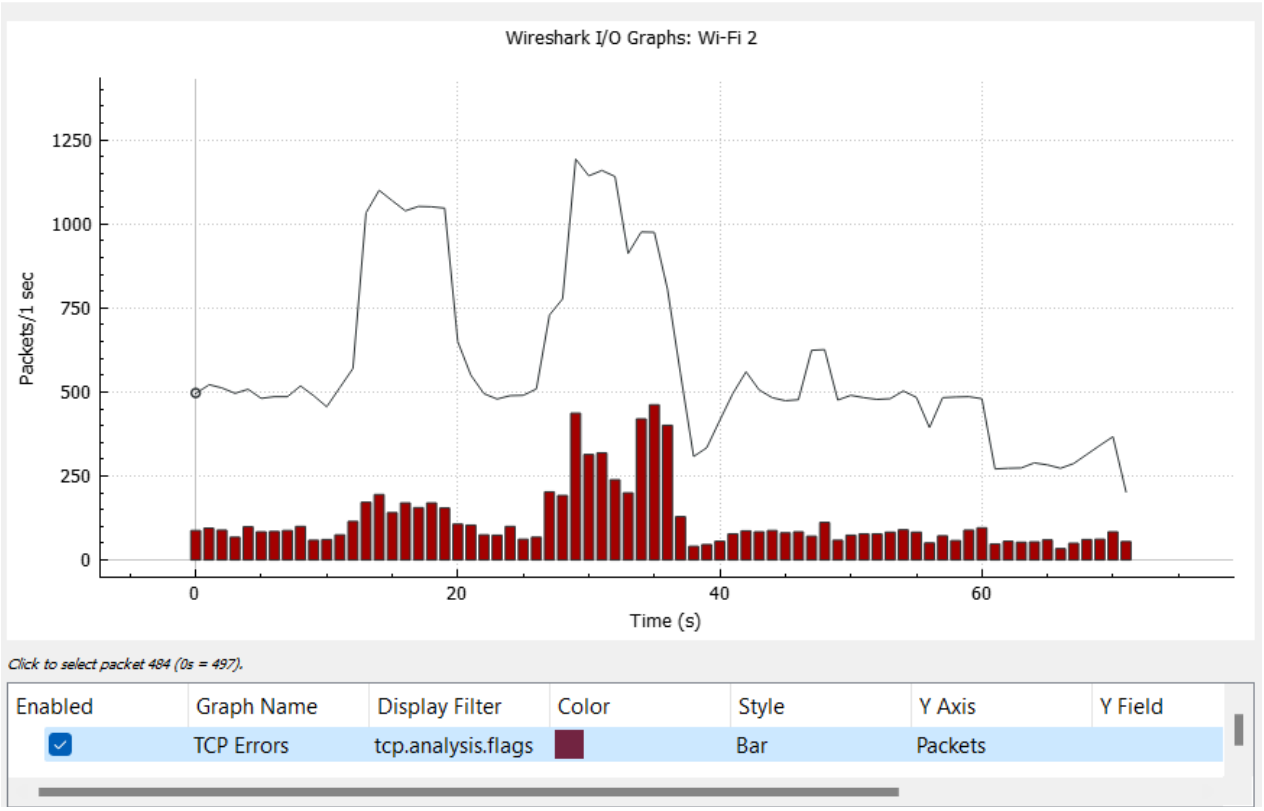
در اینجا همان مقصـد هایی اسـت که در conversation وجود داشـته برای مثال گزینه انتخاب شـده آدرس سرور شخصی برای proxy به گیت لب یک شرکت است. که فایل ها با آن انتقال داده شده است .

سوال ۸: آیا می‌توانید از زبانه Ethernet و از روی تعداد بسـته‌های مبادله شـده، Default Gateway شبکه خود را تشخیص دهید؟

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:7f:ff:fa	8	1708	0	0	8	
78:54:2e:d9:6d:24	42,144	36 M	25,635	34 M	16,509	
94:08:53:59:ca:e5	42,154	36 M	16,519	1259 k	25,635	
ff:ff:ff:ff:ff:ff	2	172	0	0	2	

بله آدرسی که بیشترین تعداد بسته با آن انتقال یافته است همان default gateway ما می باشد.

۶. 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.

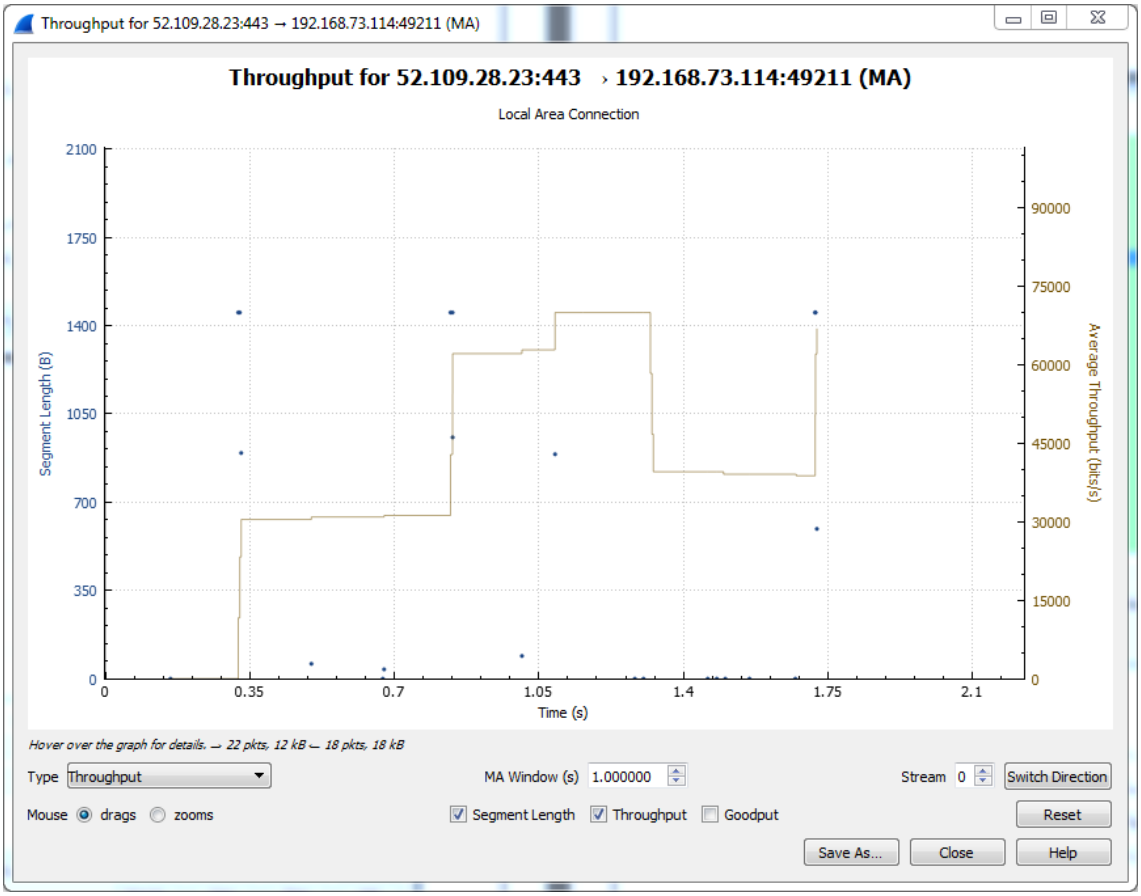


که فیلتر ارور های TCP گذاشته شده است.

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

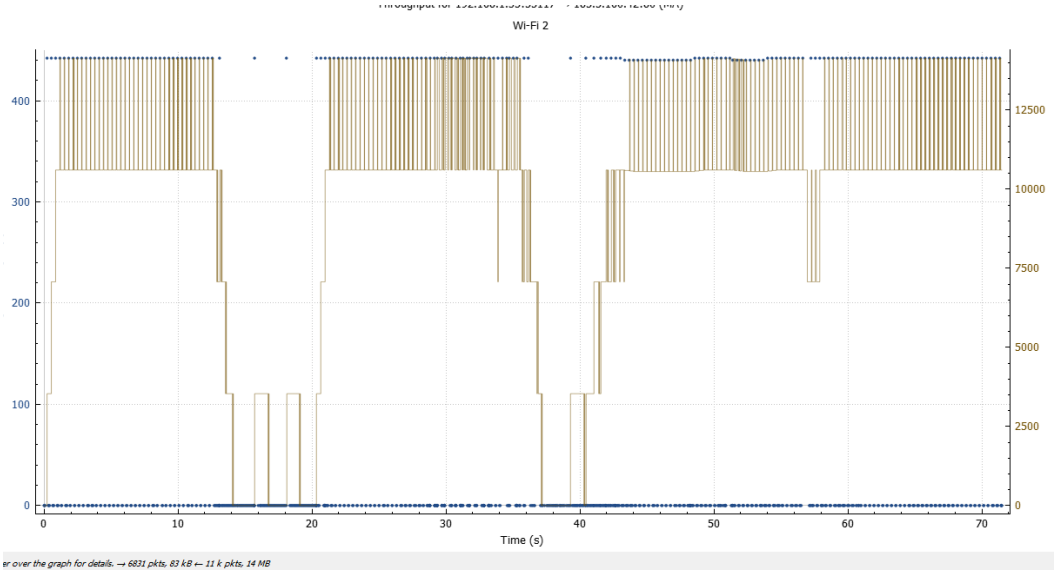
۸. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Throughput کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید گذردهی میانگین با واحد بیت در ثانیه در طول زمان برای یک ارتباط TCP را مانند شکل (۱-۱) مشاهده کنید. با گزینه‌ی Switch Direction می‌توانید ارتباط در جهت برعکس را بررسی کنید. بر روی نمودار نقاط آبی رنگی قرار دارند، این نقاط طول segment های

ارسال شده برحسب بایت در ارتباط TCP را در آن زمان نمایش می‌دهد. با افزایش شـــمارنده‌ای که در پایین پنجره با نام Stream قرار دارد می‌توانید ارتباط TCP خود را عوض کنید. منظور از Goodput نرخی اســـت که کاربرد داده خود را دریافت می‌کند و در آن Retransmission ها در نظر گرفته نمی‌شوند.

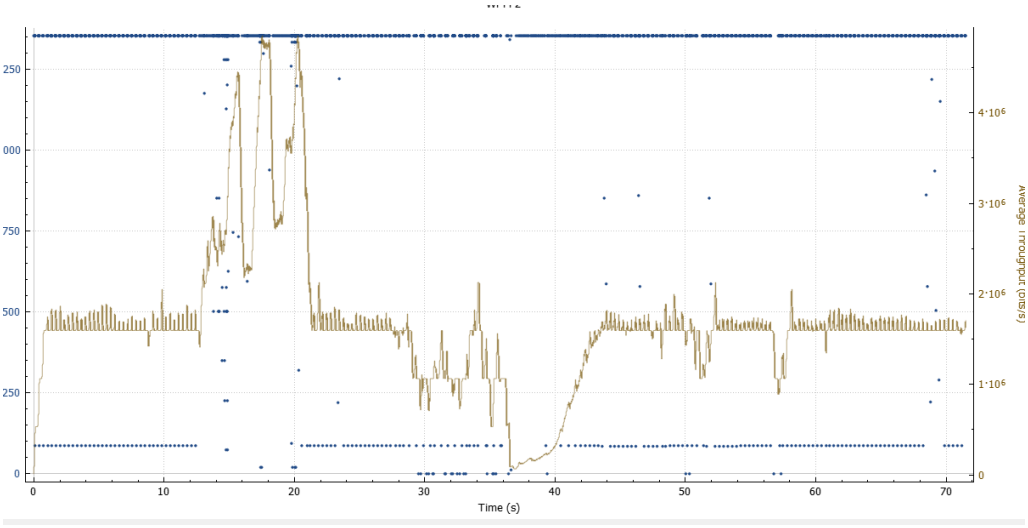


شکل (۱-۱) نمودار گذردهی

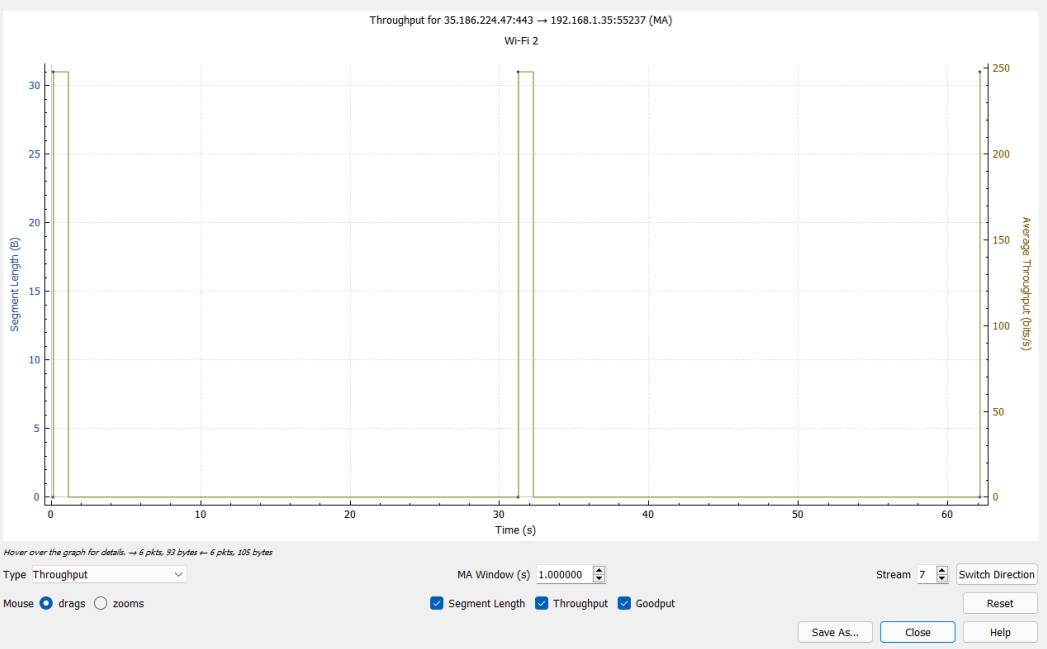
مثال ما :



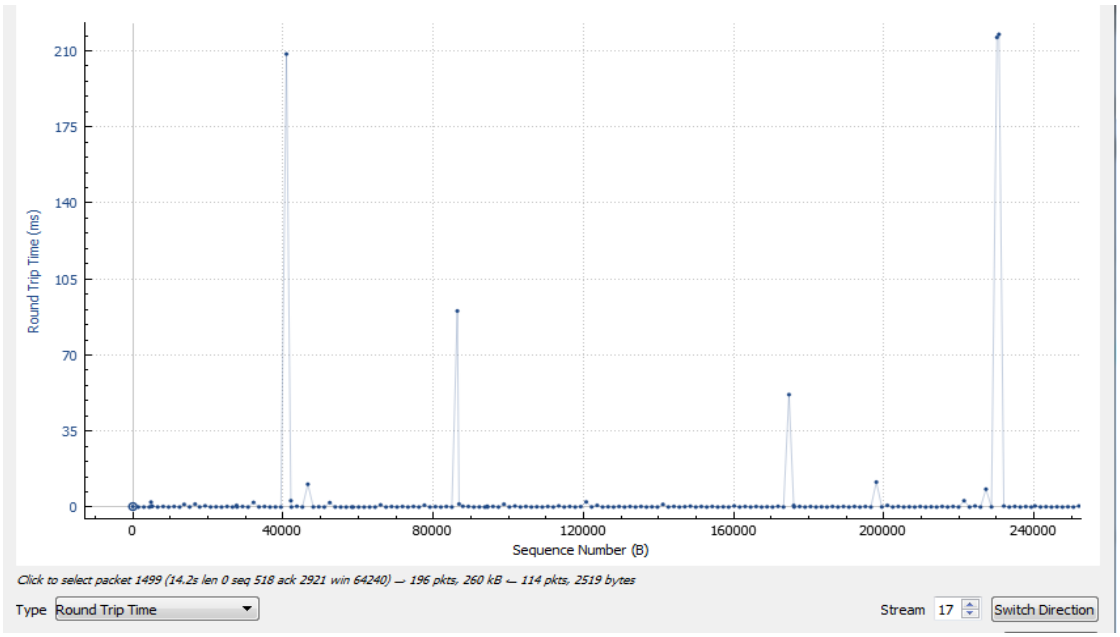
نمودار برعکس شده :



برای استریم دیگر:

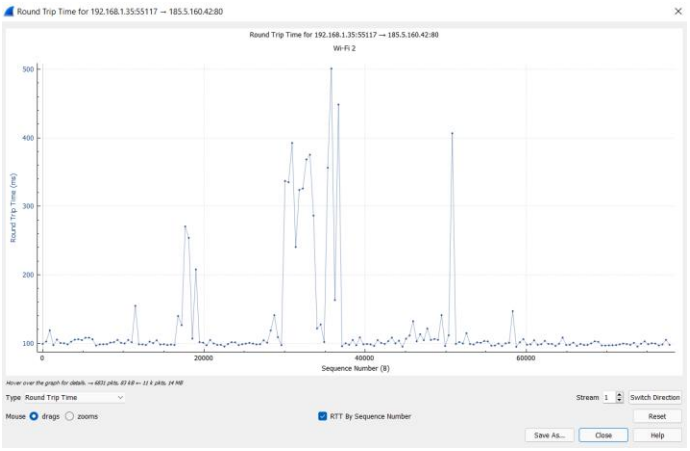


۹. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شـــود بر روی Round Trip Time کلیک کنید. در پنجره‌ای که باز می‌شـــود می‌توانید زمان یک رفت و برگشـت را برای یک ارتباط TCP مشـاهده کنید (شـکل (۱-۲)). گزینه‌های این پنجره نیز مانند قســمت ۸ اســت. می‌توانید با انتخاب گزینه‌ی RTT By Sequence Number این نمودار را برحسب شماره‌ی بسته‌ها داشته باشید. شمارنده Stream در گوشــه پایین ســمت راســت را به شــماره Stream مربوط به اتصــال TCP با یکی از سایت‌هایی که داشتید تنظیم کنید.

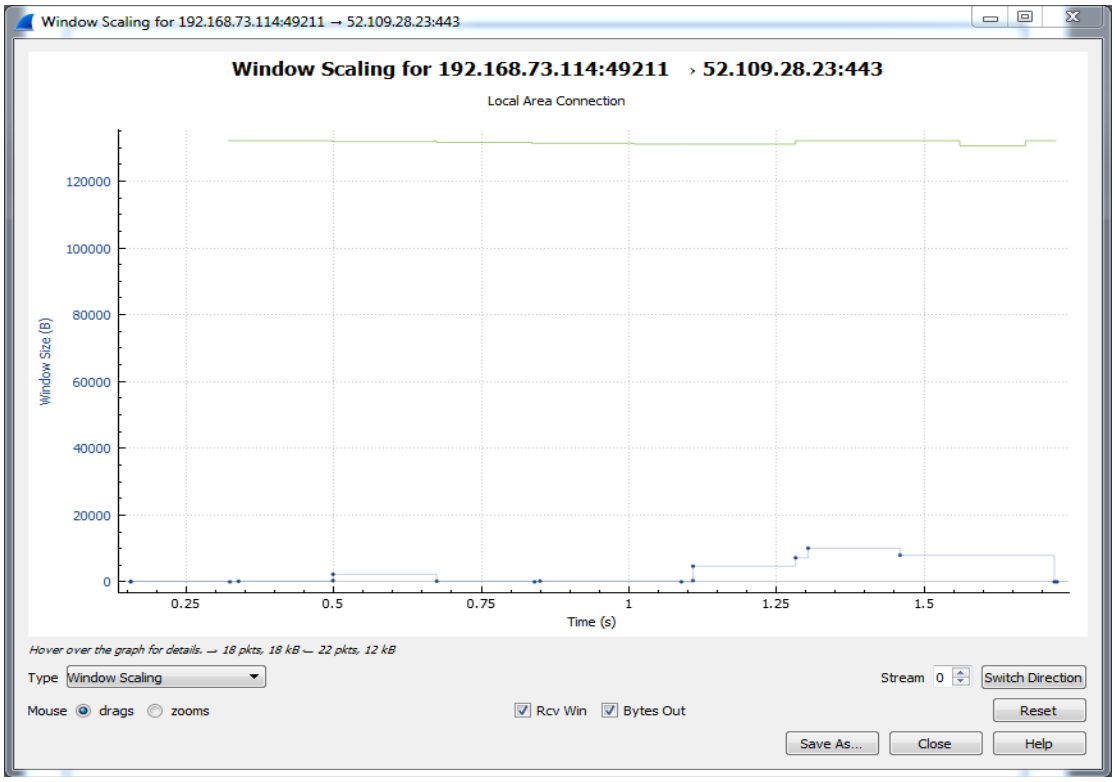


شکل (۲-۱) نمودار RTT

اتصال ما :



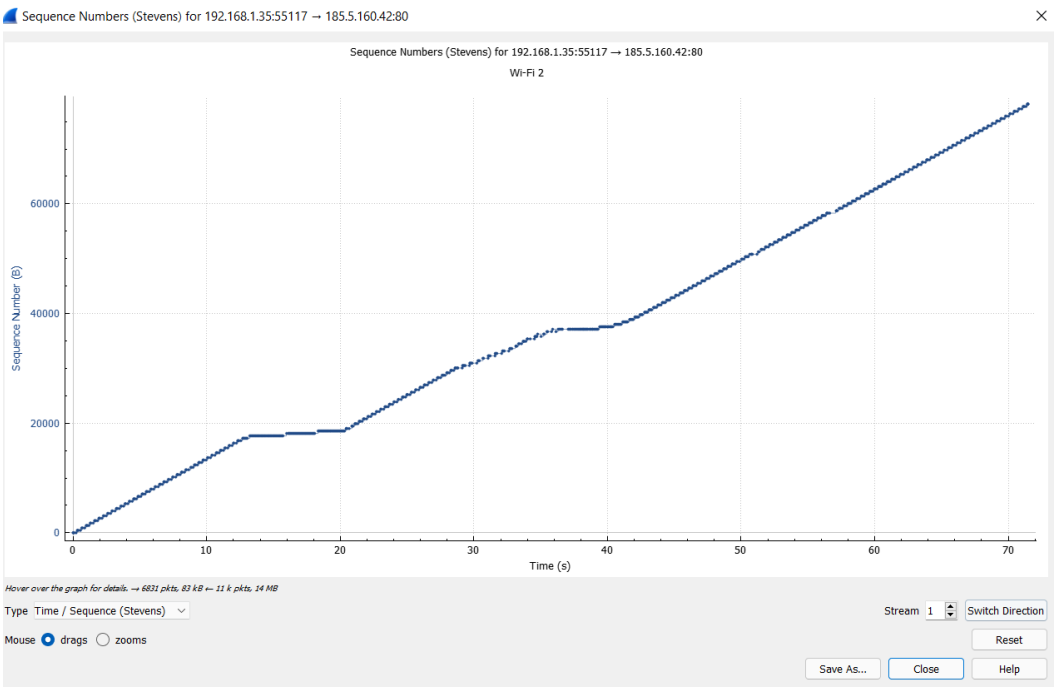
۱۰. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شـود بر روی Window Scaling کلیک کنید. پنجره‌ای مانند شکل (۱-۳) باز می‌شود که می‌توانید اندازه‌ی پنجره‌ی دریافت (با خط سـبز رنگ) و بایت‌های ارسـالی (با خط آبی رنگ) را برای یک ارتباط TCP مشـاهده نمایید. تمامی تنظیمات این پنجره مانند قسـمت ۸ است.



شکل (۳-۱) نمودار Window Scaling

مثال ما :

۱۱. 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.



سوال ۹: به سایت دانلود دانشگاه مراجعه کنید

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

به‌صورت 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 به‌عنوان 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 به‌صورت دقیق بررسی کنید.

از آنجایی که محیط گرافیکی ممکن است قادر به نمایش همه بسته‌ها نباشد، Wireshark را در محیط خط فرمان از طریق دستور زیر اجرا کنید. ابتدا به محل نصب Wireshark بروید و برنامه tshark که مخصوص خط فرمان است را اجرا کنید:

tshark –D

با اجرای این دستور مشاهده می‌کنید که اینترفیس‌های شما لیست می‌شوند. عدد اینترفیسی که می‌خواهید بر روی آن شنود کنید را یادداشت کنید. به فرض اینترفریس شماره ۴ را انتخاب کرده‌اید. دستور زیر را اجرا کنید:

tshark –i 4 –p –w output.pcap

پس از آن بسته‌ها شنود می‌شوند. درنهایت Ctrl + C را فشار دهید و فایل output.pcap را با Wireshark باز کنید.

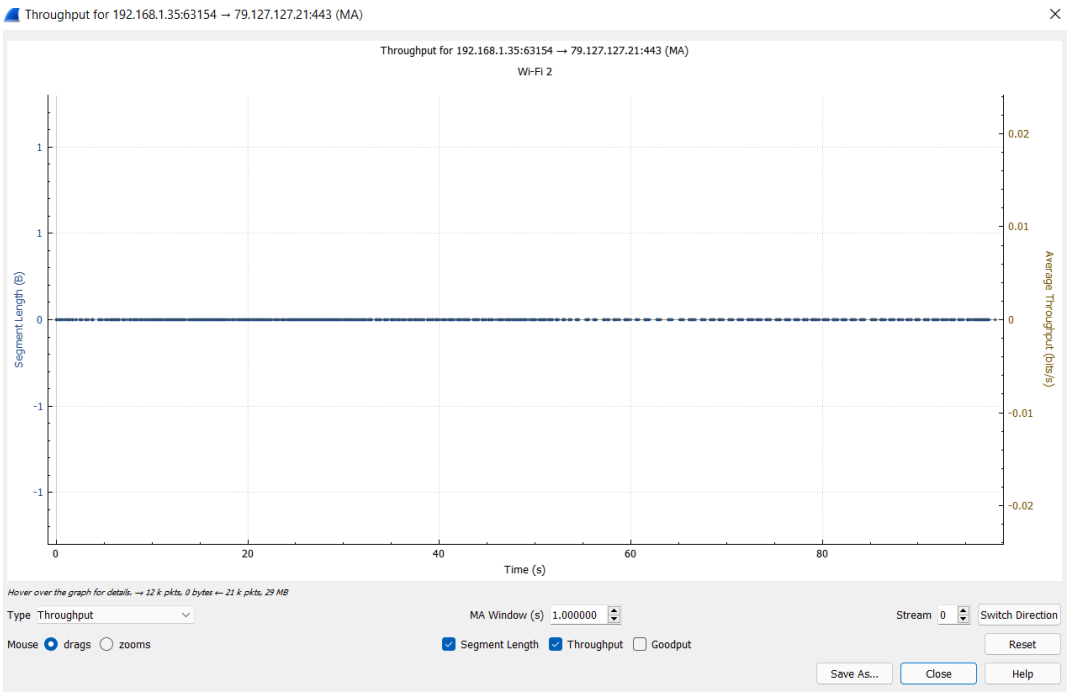
به علت در دسترس نبودن سایت دانشگاه از سایت soft98.ir استفاده شده است .

لینک۱ و لینک۲ برای دانلود در نظر گرفته شده است .

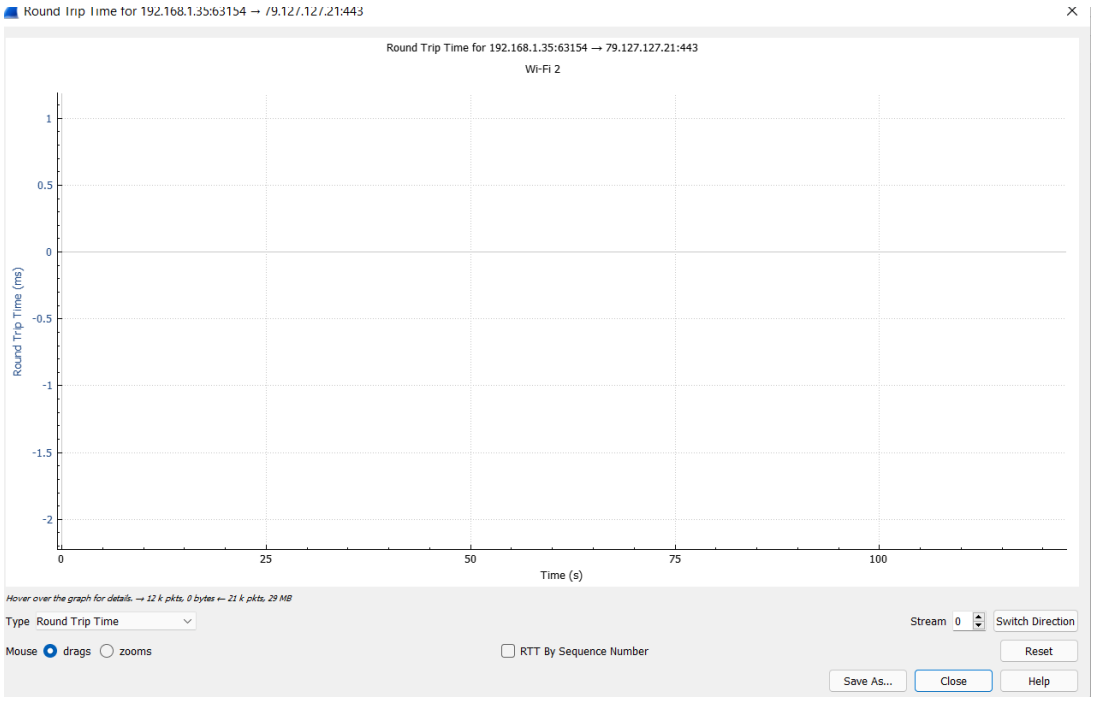
79.127.127.21	443	192.168.1.35	63154	34,240	31 M	21,628	30 M	12,612	709 k	0.000000	98.0519	2490 k
79.127.127.21	443	192.168.1.35	63173	47,795	43 M	30,149	42 M	17,646	1000 k	0.035909	98.4406	3461 k

آدرس های ip سایت soft98

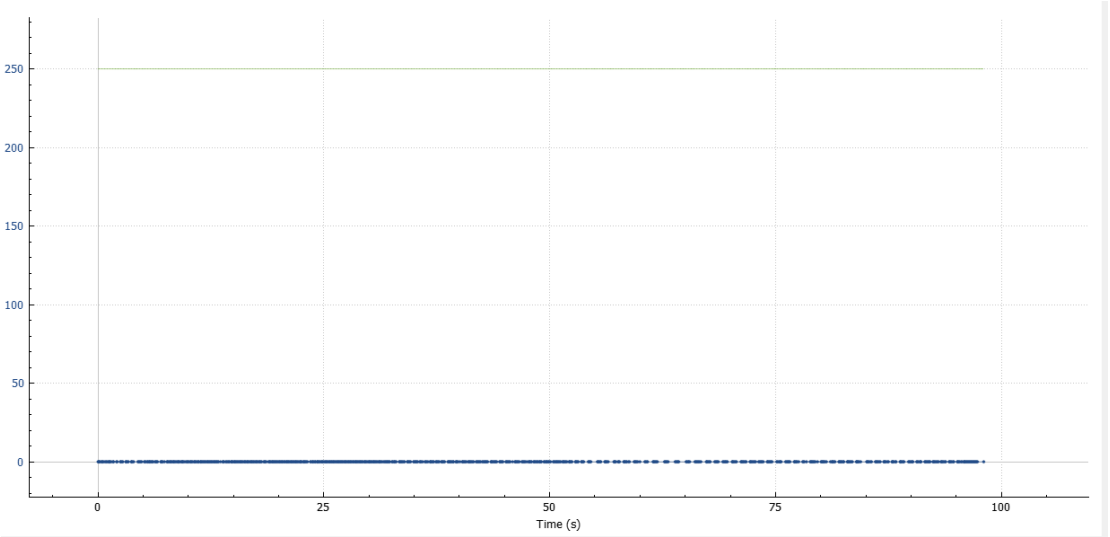
نمودار **throughput** :



نمودار **RTT** :



نمودار **Window scaling** :



با توجه به توضیحات ویدیو در صورتی که به صورت گروهی این آزمایش انجام می شد و شرایط به وجود آمده شرایط ازدحام می بود . نمودار اندازه پنجره نمودار دندان کوسه ای باید می شد . یعنی این که که همه با هم اندازه پنجره زیاد می شد برای تمامی کاربر ها سپس بعد از این که همه دچار شرایط ازدحام شدند اندازه پنجره به صورت ناگهانی کاهش پیدا میکرد. اما به این دلیل که از سایت خارجی استفاده شده است این شرایط رخ نداده است .