

به نام یزدان پاک

آزمایشگاه شبکه های کامپیوتری
آزمایش پنجم

تهیه کننده:
سارا تاجرنیا

استاد مربوطه:
استاد صادقیان

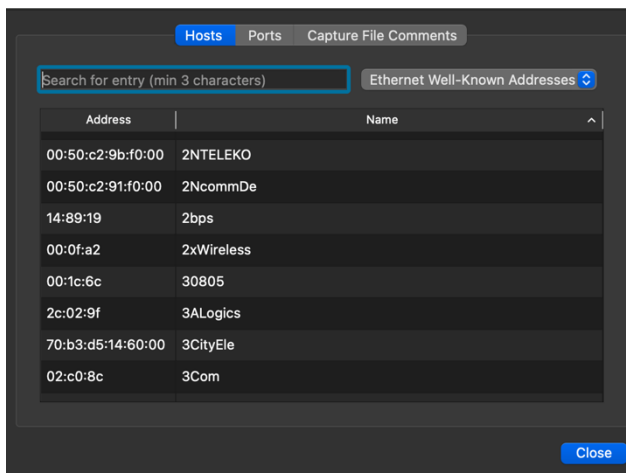
۱۴۰۱/۲/۱۵

۱-۱- هدف آزمایش

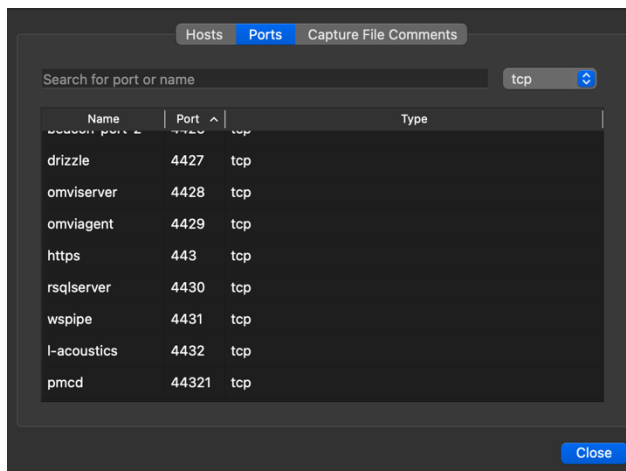
در این آزمایش قصد داریم آشنایی بیشتری با نرم افزار Wireshark و منوی Statistics در آن پیدا کنیم و از امکانات آن برای تحلیل بسته های جمع آوری شده استفاده نماییم.
۱. بر روی گزینه ی Resolved Addresses کلیک کنید.

سوال ۱: در پنجره ای که باز می شود چه چیزی را مشاهده می کنید؟

برای Resolve Address در قسمت Hosts، Name ها با IP Address های مربوطه مشخص میشود. در این قسمت به صورت default همه ی Host ها را نشان میدهد و میتوان کارت شبکه Host را تشخیص داد. برای مثال در قسمت well known موارد زیر را داریم:

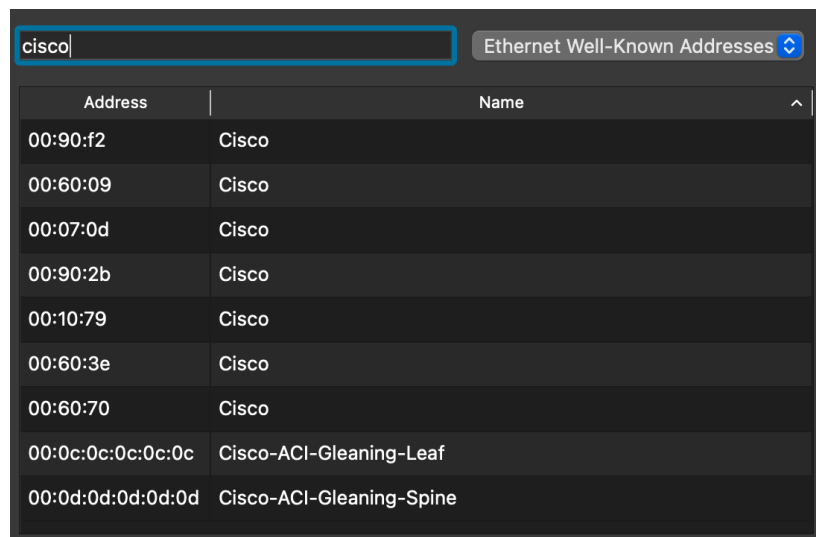


همچنین در قسمت Ports مشخص میشود که چگونه عدد را به اسم تبدیل کنیم. در این قسمت به صورت default همه ی type های ورودی را نشان میدهد اما اگر بخواهیم میتوانیم یک type دلخواه برای مثال tcp را در نظر بگیریم و name را بر اساس port داشته باشیم. البته میتوانیم port یا اسم مورد نظر را سرچ کنیم. برای مثال در شکل زیر port 443 برای https است:



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

حاصل سرچ ما به صورت زیر است:



The screenshot shows a search interface with 'cisco' entered in the search bar. Below the search bar is a table titled 'Ethernet Well-Known Addresses'. The table has two columns: 'Address' and 'Name'. It lists several MAC addresses and their corresponding names, all of which are Cisco-related.

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

۲. بر روی گزینه‌ی protocol hierarchy کلیک کنید.

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

پروتکل را براساس مدل لایه ای TCIP نشان میدهد به این صورت که در هر کدام از لایه ها چه درصدی چه packet وجود دارد. برای مثال در شکل زیر نشان میدهد که:

100% لایه اول frame

100% لایه دوم Ethernet

99.9% لایه سوم 4 Internet Version Protocol است که 11% آن برای User Datagram

Protocol و 88.8% آن Transmission Control Protocol که این دو هر کدام خود شامل زیر لایه هایی هستند.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
▼ Frame	100.0	6978	100.0	3363575	146 k	0	0
▼ Ethernet	100.0	6978	2.9	97692	4258	0	0
▼ Internet Protocol Version 6	0.0	3	0.0	120	5	0	0
▼ User Datagram Protocol	0.0	2	0.0	16	0	0	0
Multicast Domain Name System	0.0	1	0.0	45	1	1	45
DHCPv6	0.0	1	0.0	38	1	1	38
Internet Control Message Protocol v6	0.0	1	0.0	24	1	1	24
▼ Internet Protocol Version 4	99.9	6973	4.1	139500	6080	0	0
▼ User Datagram Protocol	11.0	767	0.2	6136	267	0	0
Simple Service Discovery Protocol	6.6	460	3.9	130047	5668	460	130047
QUIC IETF	1.7	117	1.3	42688	1860	114	40883
Multicast Domain Name System	0.2	11	0.0	655	28	11	655
Domain Name System	2.1	150	0.3	10085	439	150	10085
Data	0.5	32	0.0	1248	54	32	1248
▼ Transmission Control Protocol	88.8	6196	87.3	2935209	127 k	4212	150824
Transport Layer Security	28.0	1957	54.2	1823825	79 k	1947	177528
▼ Hypertext Transfer Protocol	0.7	47	2.5	84327	3675	17	6719
Line-based text data	0.1	10	0.1	3094	134	10	3094
Data	0.0	3	1.9	63778	2780	3	65077
Data	0.1	7	0.3	9768	425	7	9768
Internet Group Management Protocol	0.1	10	0.0	80	3	10	80
Address Resolution Protocol	0.0	2	0.0	56	2	2	56

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

▼ Transmission Control Protocol	88.8	6196	87.3	2935209	127 k	4212
---------------------------------	------	------	------	---------	-------	------

88.8% روی TCP قرار دارد.

۳. بر روی گزینه‌ی Conversations کلیک کنید.

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

در این قسمت همان طور در تصویر مشخص است نشست ها را به ترتیب لایه هایشان در قالب های Ethernet, IPv4, Ipv6, TCP, UDP نشان میدهد. برای مثال در قسمت TCP به صورت زیر است:

Ethernet · 7 IPv4 · 50 IPv6 · 3 TCP · 58 UDP · 109												
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
59482	185.211.88.218	443	6	420	3	222	3	198	2.279935	0.0397	44 k	39 k
49693	157.240.227.60	443	40	4090	20	2060	20	2030	5.340426	175.0007	94	92
59485	212.16.77.189	443	316	156 k	164	15 k	152	140 k	25.472928	131.3701	963	8548
49732	104.199.240.237	443	2	131	1	77	1	54	45.768880	0.4672	1318	924
59486	104.66.87.191	443	35	10 k	19	2278	16	8543	52.912120	61.2579	297	1115
59487	142.250.201.142	443	70	18 k	33	7229	37	11 k	56.361154	116.6970	495	788
59488	142.250.201.142	443	188	54 k	89	23 k	99	30 k	56.814338	117.1193	1620	2110
49733	172.217.169.227	443	89	48 k	47	4217	42	44 k	58.943725	90.7217	371	3944

۵. بر روی گزینه‌ی endpoints کلیک کنید.

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

گزینه endpoint نشان دهنده endpoint های مبدا و مقصد است که با آنها در ارتباط بوده ایم. مانند گزینه conversations نشست ها را به ترتیب لایه هایشان در قالب های Ethernet, IPv4, Ipv6, TCP, UDP نشان میدهد. که در قسمت بعد مثالی از TCP آن هم داده شده.

سوال ۷: چه مقصدهایی برای ارتباطهای TCP در سیستم شما استفاده شده‌اند؟

انواع مقصد های تکراری و غیر تکراری از جمله IP لپ تاپ ما میتواند وجود داشته باشد برای مثال مقصدهای زیر در قسمت TCP قرار داشتند.

Ethernet · 8 IPv4 · 50 IPv6 · 5 TCP · 98 UDP · 119							
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
172.217.169.227	443	89	48 k	42	44 k	47	4217
172.217.169.238	443	39	11 k	20	6788	19	4782
185.211.88.80	443	98	51 k	44	43 k	54	8080
185.211.88.218	443	148	69 k	71	43 k	77	26 k
192.168.1.7	59482	6	420	3	222	3	198
192.168.1.7	49693	40	4090	20	2060	20	2030
192.168.1.7	59485	316	156 k	164	15 k	152	140 k

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

در قسمت Ethernet با sort کردن قسمت Packets و چندیدن بار امتحان کردیم فهمیدیم که بیشترین Address برای IP خودمان است پس میتوان Default Gateway را تشخیص داده به طوری که بیشترین تعداد بسته را جا به جا کرده است. برای مثال در حالت زیر مشخص است که Default Gateway چیست:

Ethernet · 7 IPv4 · 39 IPv6 · 8 TCP · 77 UDP · 60							
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	
33:33:00:00:00:fb	5	949	0	0	5		949
01:00:5e:00:00:fb	9	1033	0	0	9		1033
c2:e8:d1:1b:be:fb	9	1218	9	1218	0		0
ff:ff:ff:ff:ff:ff	13	942	0	0	13		942
01:00:5e:7f:ff:fa	22	3950	0	0	22		3950
ec:22:80:c8:b9:2c	4,241	1809 k	2,294	1528 k	1,947		281 k
a4:83:e7:5f:ff:f3	4,291	1817 k	1,992	288 k	2,299		1529 k

Ethernet · 7 IPv4 · 39 IPv6 · 8 TCP · 77 UDP · 60							
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	
IPv6mcast_fb	5	949	0	0	5		949
IPv4mcast_fb	9	1033	0	0	9		1033
c2:e8:d1:1b:be:fb	9	1218	9	1218	0		0
Broadcast	13	942	0	0	13		942
IPv4mcast_7f:ff:fa	22	3950	0	0	22		3950
D-Linkln_c8:b9:2c	4,241	1809 k	2,294	1528 k	1,947		281 k
Apple_5f:ff:f3	4,291	1817 k	1,992	288 k	2,299		1529 k

سوال ۹: 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.

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

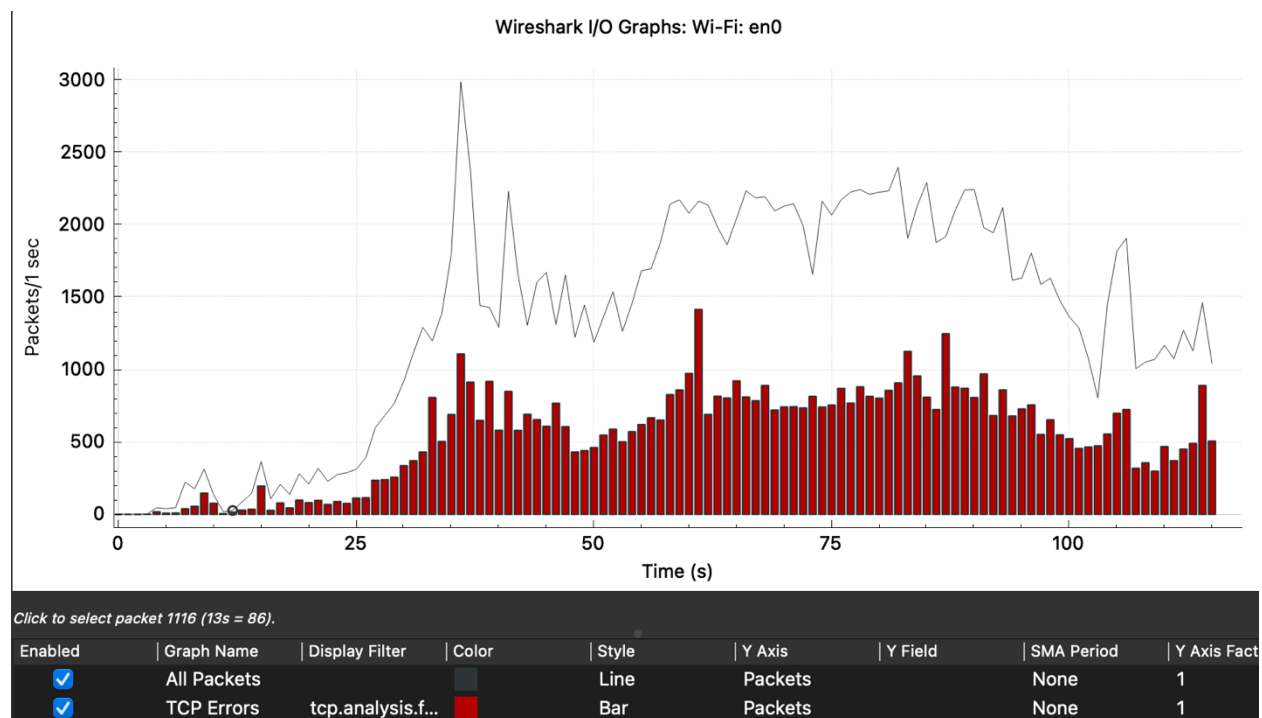
با اجرای این دستور مشاهده می‌کنید که اینترفیس‌های شما لیست می‌شوند. عدد اینترفیسی که می‌خواهید بر روی آن شنود کنید را یادداشت کنید. به فرض اینترفیس شماره ۴ را انتخاب کرده‌اید. دستور زیر را اجرا کنید:

tshark -i 4 -p -w output.pcap

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

این سایت چه با فیلتر شکن چه بدون آن برای من باز نشد زیرا فقط در دانشگاه میتوان به آن متصل شد در ادامه با توجه به ویدیو که قرار داده شد و سایت soft98 دو فایل با حجم بالا را در نظر گرفتم و روی آنها امتحان کردم اما به دلیل وصل نبودن بیشتر از چندین نفر معمول به نتیجه کاملاً مطلوب که قرار بود سر کلاس برسیم، نرسیدم.

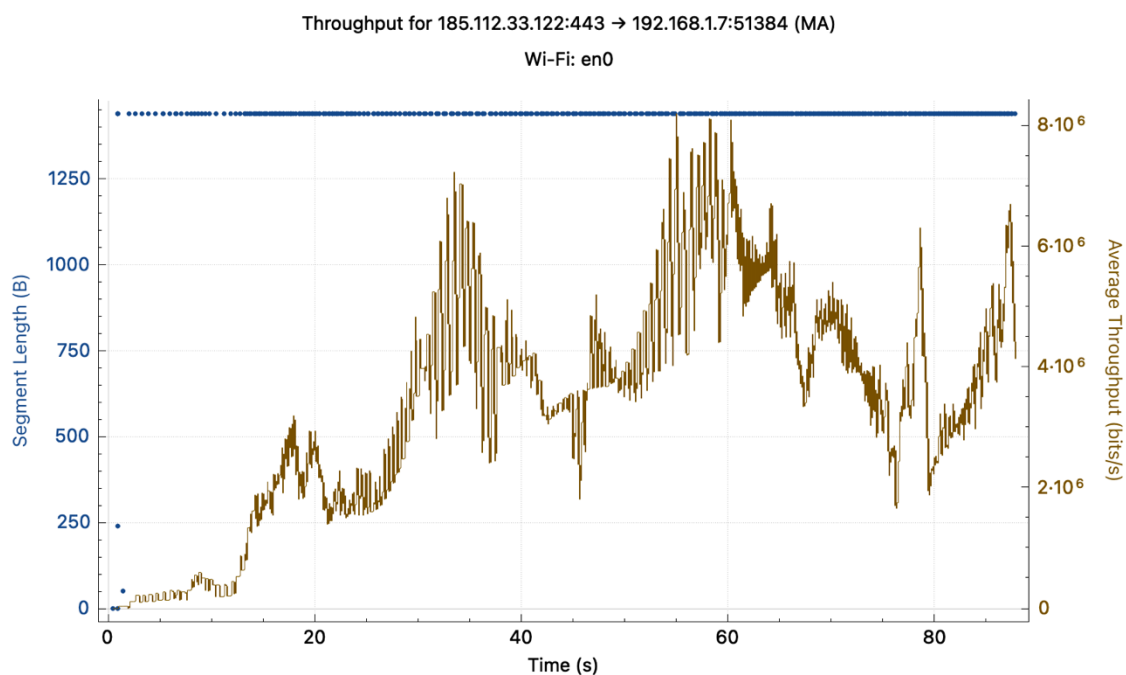
I/O graph نشان دهنده این که چند package در هر ثانیه جا به جا شده. که البته میتوان برای آن فیلتر در نظر گرفت.



ابتدا در conversations آدرس مورد نظر را انتخاب میکنیم.

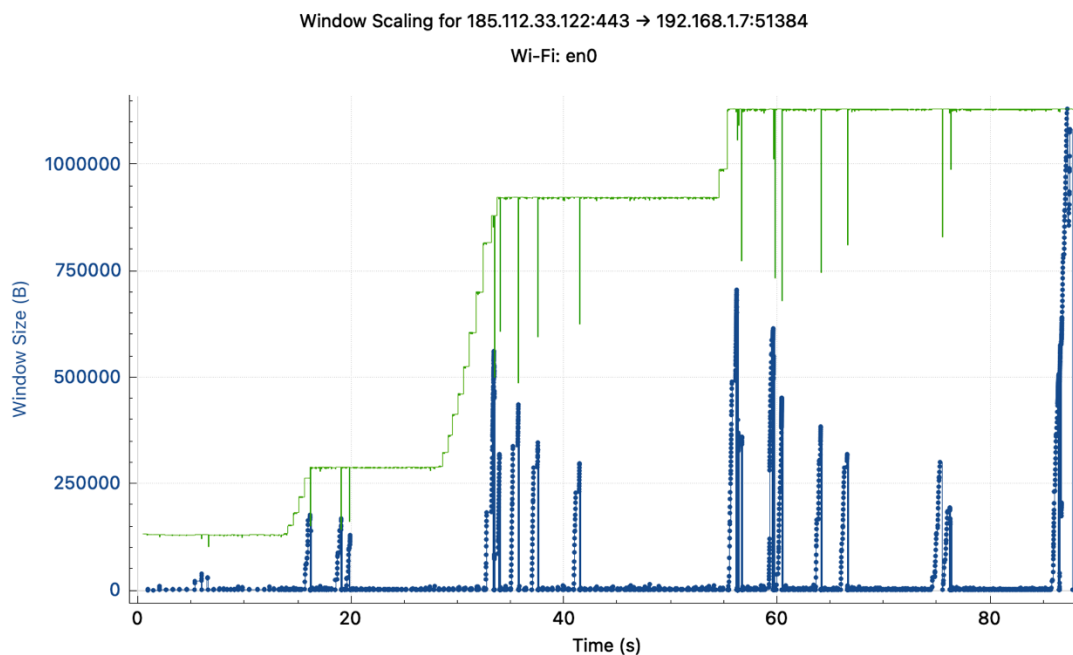
Ethernet · 8 IPv4 · 27 IPv6 · 2 TCP · 34 UDP · 38												
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
192.168.1.7	51383	185.112.33.122	443	98,276	72 M	52,632	3717 k	45,644	68 M	11.043212	104.7705	283 k
192.168.1.7	51384	185.112.33.122	443	55,261	40 M	29,461	2111 k	25,800	38 M	28.006895	87.7362	192 k
192.168.1.7	51376	185.18.212.82	443	205	126 k	116	11 k	89	114 k	7.147730	19.0834	5004
192.168.1.7	51375	185.18.212.82	443	194	125 k	108	10 k	86	114 k	7.147268	18.7324	4524
192.168.1.7	51379	185.18.212.82	443	190	122 k	104	9681	86	112 k	7.149175	18.4273	4202

گراف Throughput آن به صورت زیر است:



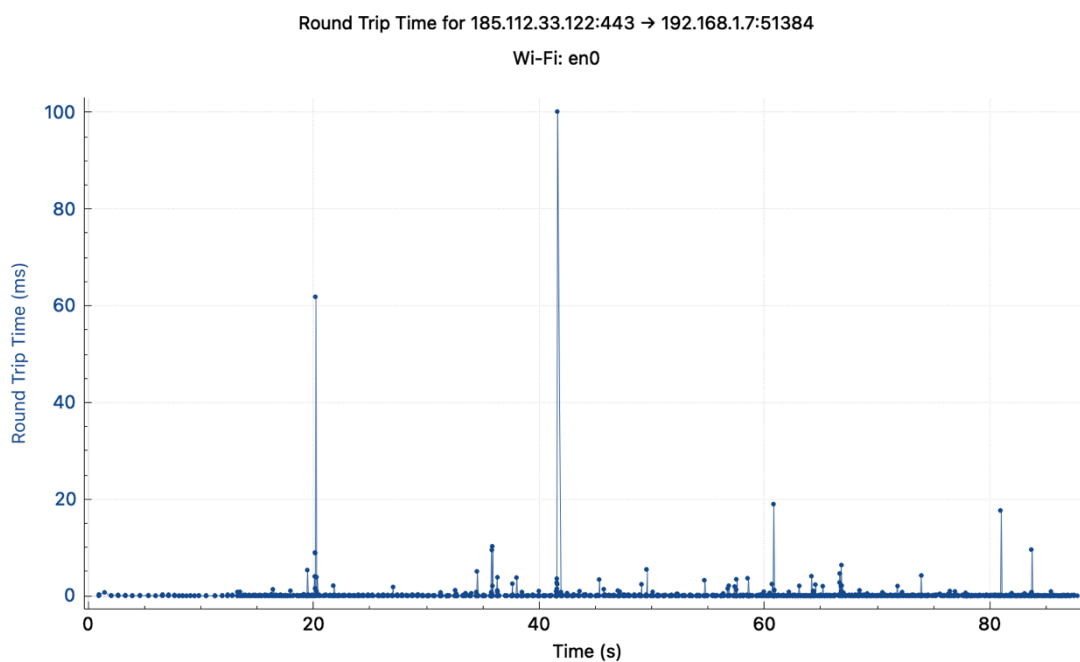
این گراف بر اساس segment length/sec است به این صورت که نشان میدهد در هر ثانیه (نقطه های آبی بالاتر از نمودار) طول Segment چقدر بوده است. در بازه هایی که Segment length در یک زمان معین یکسان تغییر ممکن از به دلیل بالا بودن weight باشد با خطای از دست دادن اطلاعات که برای ما بیشتر گزینه دوم است.

گراف Windows Scaling به صورت زیر است:



این گراف بر اساس Window Size/sec است به این صورت که نشان میدهد در هر ثانیه اندازه Window ها چقدر بوده است.

گراف Roundtrip time به صورت زیر است:



این گراف که بر اساس Round Trip Tme(ms)/s است نشان دهنده این است که در هر ثانیه چند Round Trip داشته ایم.