

به نام خدا



آزمایش شماره چهار

گروه ۴



محمد جواد زندیه ۹۸۳۱۰۳۲، محمد حسین اسدی ۹۸۳۱۰۰۵

۳۱ فروردین ۱۴۰۰

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

سوال یک: در پنجره Host نسبت دادن Name به Address IP را مشاهده می کنیم (کارت شبکه Host مورد نظر را نشان میدهد). در این بخش میتوان روی Ethernet Address و Ethernet Well-Known و Ethernet Manufacture فیلتر گذاشت برای Name ها و Address ها.

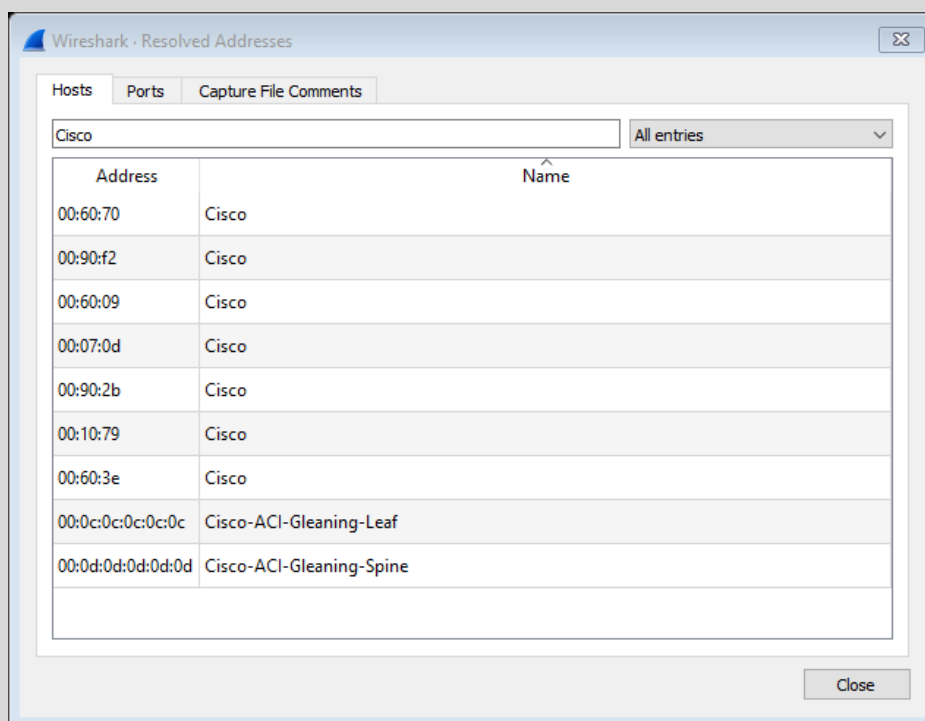
فقط قسمت Host است که از روی پکت های دریافتی بدست می آید و مابقی یک سری موارد از پیش تعریف شده اند.

در پنجره Port، بر اساس انواع پروتکل ها (tcp, udp, sctp, dccp) میتوان Port ها و Name های متناظر را بدست آورد.

سوال دو: کارت شبکه Cisco در شکل زیر قابل مشاهده است.

مثلا 00:60:70 چون نمایش بر اساس هگزا دسیمال است ۳ بایت اول به صورت 00 و 60 و 70 می باشد

و ...



سوال سه: سلسله مراتب پروتکل بر اساس TCP/IP (لایه ای) را برای ما مشخص می کند. همچنین درصد استفاده از پروتکل ها در لایه های مختلف را به ما میدهد. ارزیابی از بستر هایی که پکت روی آنها می باشد هم میتوان انجام داد.

سوال چهار: ۹۹.۹ درصد از بسته ها لایه دوم شان روی بستر IPV4 می باشد.

در شکل زیر قابل مشاهده است.

Wireshark - Protocol Hierarchy Statistics - Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	26382	100.0	17285311	850 k	0	0	0
▼ Ethernet	100.0	26382	2.1	369348	18 k	0	0	0
▼ Internet Protocol Version 6	0.0	9	0.0	360	17	0	0	0
▼ User Datagram Protocol	0.0	9	0.0	72	3	0	0	0
Link-local Multicast Name Resolution	0.0	8	0.0	344	16	8	344	16
DHCPv6	0.0	1	0.0	95	4	1	95	4
▼ Internet Protocol Version 4	99.9	26355	3.0	527100	25 k	0	0	0
▼ User Datagram Protocol	3.0	804	0.0	6432	316	0	0	0
Simple Service Discovery Protocol	0.2	53	0.0	5641	277	53	5641	277
▼ QUIC IETF	1.5	400	2.1	359184	17 k	305	268315	13 k
Malformed Packet	0.0	2	0.0	0	0	2	0	0
NetBIOS Name Service	0.0	12	0.0	600	29	12	600	29
Link-local Multicast Name Resolution	0.0	8	0.0	344	16	8	344	16
▼ Domain Name System	1.6	424	0.1	21980	1081	412	17572	864
Malformed Packet	0.0	12	0.0	0	0	12	0	0
▼ Transmission Control Protocol	96.9	25551	92.9	16050022	790 k	20537	10966009	539 k
Transport Layer Security	20.1	5296	84.1	14534671	715 k	4984	10575077	520 k
Hypertext Transfer Protocol	0.0	4	0.0	1574	77	0	0	0
Data	0.1	30	0.2	35889	1766	30	35889	1766
Address Resolution Protocol	0.1	18	0.0	504	24	18	504	24

No display filter.

Close Copy Help

سوال پنج: نگاه Conversation به صورت گره به گره می باشد. بر اساس انواع پروتکل ها مشخصات مبدا و مقصد packet ها را مشخص می کند. مثلا در TCP پورت مبدا و مقصد و آدرس آنها را نشان میدهد. همچنین میتوان تعداد و طول پکت ها را مشاهده کرد.

در این بخش نشست ها را بر اساس Ethernet , Port, IPV6, TCP, UDP نشست ها نیز نشان داده شده است، مثلا برای TCP تعداد نشست ها ۲۱۰ تا می باشد.

در قسمت TCP که در شکل مشاهده می شود، آدرس و پورت مبدا و مقصد را نشان داده است، به همراه جزئیات دیگر ...

Wireshark - Conversations - Wi-Fi

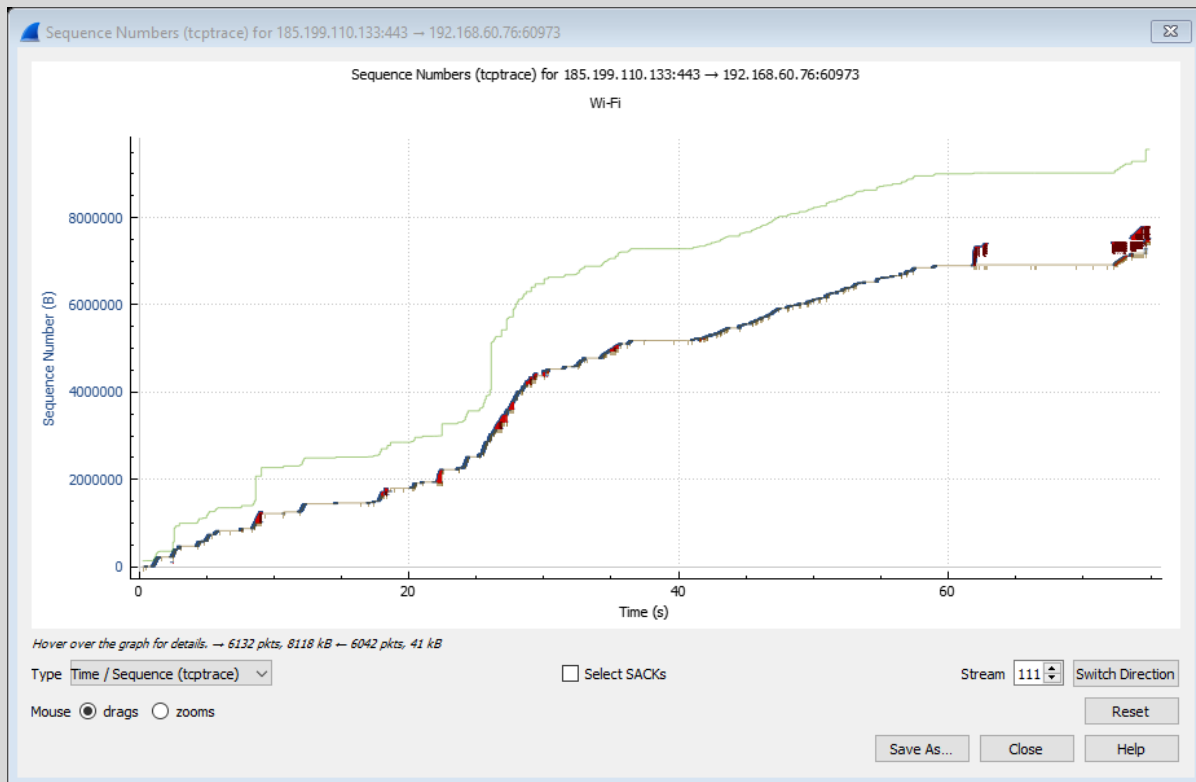
Ethernet · 5		IPv4 · 52		IPv6 · 2		TCP · 210		UDP · 137										
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A					
108.138.2.181	443	192.168.60.76	60882	27	8892	17	7723	10	1169	0.841840	3.4163	18 k		2737				
142.250.201.142	443	192.168.60.76	63202	1	54	1	54	0	0	6.183665	0.0000	—		—				
172.217.169.227	443	192.168.60.76	60881	7	441	4	267	3	174	1.035452	3.1641	675		439				
192.168.60.76	60879	142.250.180.46	443	22	6618	9	3829	13	2789	0.000000	4.1579	7367		5366				
192.168.60.76	60883	108.138.2.181	443	20	8111	8	1025	12	7086	0.007176	4.1886	1957		13 k				
192.168.60.76	63201	172.217.169.227	443	6	327	6	327	0	0	1.144453	120.0281	21		0				
192.168.60.76	60884	185.211.88.218	443	58	39 k	25	5530	33	34 k	2.013232	12.2849	3601		22 k				
192.168.60.76	60885	185.211.88.218	443	17	6257	9	1079	8	5178	2.172245	1.9576	4409		21 k				
192.168.60.76	60886	108.138.17.45	443	26	8549	12	1789	14	6760	2.935346	1.3245	10 k		40 k				
192.168.60.76	60887	108.138.17.45	443	19	7728	9	1596	10	6132	3.072941	1.1109	11 k		44 k				
192.168.60.76	60888	52.215.106.6	443	24	9648	10	1958	14	7690	3.247817	11.1658	1402		5509				
192.168.60.76	60889	52.215.106.6	443	20	7257	9	1141	11	6116	3.440381	10.9536	833		4466				
192.168.60.76	60877	142.250.181.174	443	3	162	2	108	1	54	4.009025	0.1271	6797		3398				
192.168.60.76	60878	142.250.180.46	443	3	162	2	108	1	54	4.009256	0.1267	6818		3409				
192.168.60.76	60874	172.217.169.234	443	3	162	2	108	1	54	4.009528	0.1266	6826		3413				
192.168.60.76	60876	142.250.181.174	443	3	162	2	108	1	54	4.010005	0.1477	5850		2925				
192.168.60.76	60880	142.250.180.42	443	3	162	2	108	1	54	4.010295	0.1477	5848		2924				
192.168.60.76	60872	172.217.169.234	443	3	162	2	108	1	54	4.010415	0.1477	5849		2924				
192.168.60.76	60890	142.250.181.163	443	15	2914	8	1692	7	1222	5.723912	8.5979	1574		1137				
192.168.60.76	63208	20.198.162.78	443	3	2634	3	2634	0	0	6.018822	120.0155	175		0				
192.168.60.76	60891	212.16.77.189	443	134	114 k	49	3949	85	110 k	6.171278	8.1444	3878		108 k				
192.168.60.76	60892	212.16.77.189	443	14	1928	8	1037	6	891	6.423770	7.8622	1055		906				
192.168.60.76	60893	142.250.201.142	443	517	405 k	220	128 k	297	277 k	7.801099	31.1384	32 k		71 k				

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

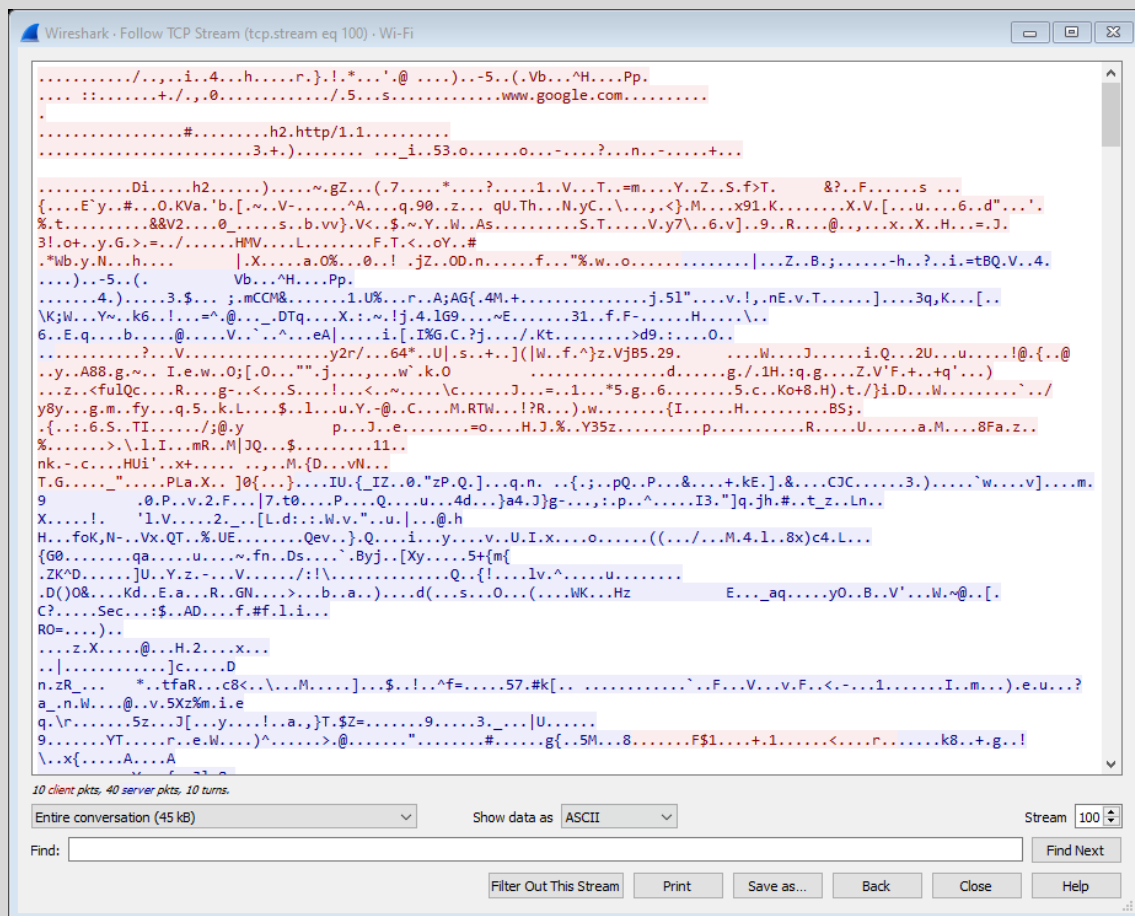
Copy Follow Stream... Graph... Close Help

Conversation Types ▼

با کلیک روی هر یک از نشست ها میتوان گراف انتقال پکت ها را مشاهده کرد. به عنوان مثال شکل زیر را مشاهده کنید.



همچنین میتوان در قسمت Fellow Stream محتوای پکت های ارسالی را به صورت ASCII و YAML و ... مشاهده کرد.



تعداد بسته های بیشتر دیفالت .. را نشان میدهد

هر چقدر شبکه بزرگ تر شود تعداد دیفالت .. بیشتر می شود

سوال شش: نگاه End point ارتباط به ارتباط است (تشخیص مبدا و مقصد)

در این قسمت مقصد هایی که با آنها در ارتباط بودیم مشاهده می شود.

مثلا برای قسمت TCP به صورت زیر می باشد:

Address: آدرسی که پکت باید به آن ارسال شود

Port: شماره پورت مقصد

Packets: تعداد پکت های رد و بدل شده

Bytes: مجموع بایت ها (طول) پکت رد و بدل شده

Tx packets: تعداد پکت های ارسالی از مبدا به مقصد

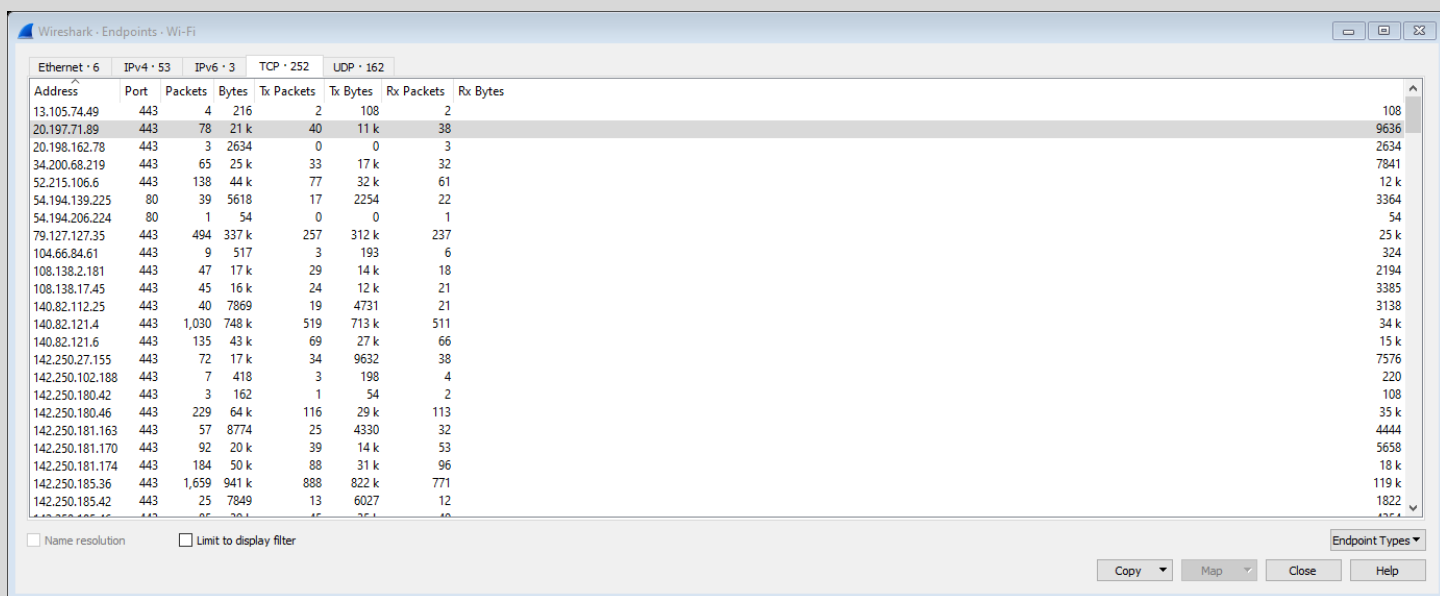
Tx Bytes: مجموع بایت های پکت های ارسالی

Rx packets: تعداد پکت های دریافتی در مقصد

Rx Bytes: تعداد بایت دریافتی در مقصد

$Tx\ Bytes + Rx\ Bytes = Bytes$

$Tx\ packets + Rx\ packets = packets$



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
13.105.74.49	443	4	216	2	108	2	108
20.197.71.89	443	78	21 k	40	11 k	38	9636
20.198.162.78	443	3	2634	0	0	3	2634
34.200.68.219	443	65	25 k	33	17 k	32	7841
52.215.106.6	443	138	44 k	77	32 k	61	12 k
54.194.139.225	80	39	5618	17	2254	22	3364
54.194.206.224	80	1	54	0	0	1	54
79.127.127.35	443	494	337 k	257	312 k	237	25 k
104.66.84.61	443	9	517	3	193	6	324
108.138.2.181	443	47	17 k	29	14 k	18	2194
108.138.17.45	443	45	16 k	24	12 k	21	3385
140.82.112.25	443	40	7869	19	4731	21	3138
140.82.121.4	443	1,030	748 k	519	713 k	511	34 k
140.82.121.6	443	135	43 k	69	27 k	66	15 k
142.250.27.155	443	72	17 k	34	9632	38	7576
142.250.102.188	443	7	418	3	198	4	220
142.250.180.42	443	3	162	1	54	2	108
142.250.180.46	443	229	64 k	116	29 k	113	35 k
142.250.181.163	443	57	8774	25	4330	32	4444
142.250.181.170	443	92	20 k	39	14 k	53	5658
142.250.181.174	443	184	50 k	88	31 k	96	18 k
142.250.185.36	443	1,659	941 k	888	822 k	771	119 k
142.250.185.42	443	25	7849	13	6027	12	1822

سوال هفت: مقصد های با پورت ۴۴۳ و ۸۰ و ۶۰۹۴۵ و ... مشاهده میشوند.

سوال هشت: برای خارج کردن بسته از شبکه از Default Gateway استفاده می شود. همچنین تعداد بسته های رد و بدل شده در Default Gateway بیشتر است. پس در منوی Ethernet آدرس های مقصدی که تعداد پکت های بیشتری به سمت آنها رفته است Default Gateway هستند. در شکل زیر میتوان دید که آدرس های 00:71;cc:2f:8b:55 و 02:42:95:be:32:0e دیفالت گیت وی هستند.

Ethernet • 6							IPv4 • 53	IPv6 • 3	TCP • 252	UDP • 162
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes				
00:71;cc:2f:8b:55	26,382	17 M	12,903	1610 k	13,479					15 M
01:00:5e:00:00:fc	8	680	0	0	8					680
01:00:5e:7f:ff:fa	53	7867	0	0	53					7867
02:42:95:be:32:0e	26,312	17 M	13,479	15 M	12,833					1600 k
33:33:00:01:00:02	1	157	0	0	1					157
33:33:00:01:00:03	8	840	0	0	8					840

☐ Name resolution
 ☐ Limit to display filter
 Endpoint Types ▼
 Copy ▼ Map ▼ Close Help

سوال نه:

IP Address of AUT = 172.16.1.82

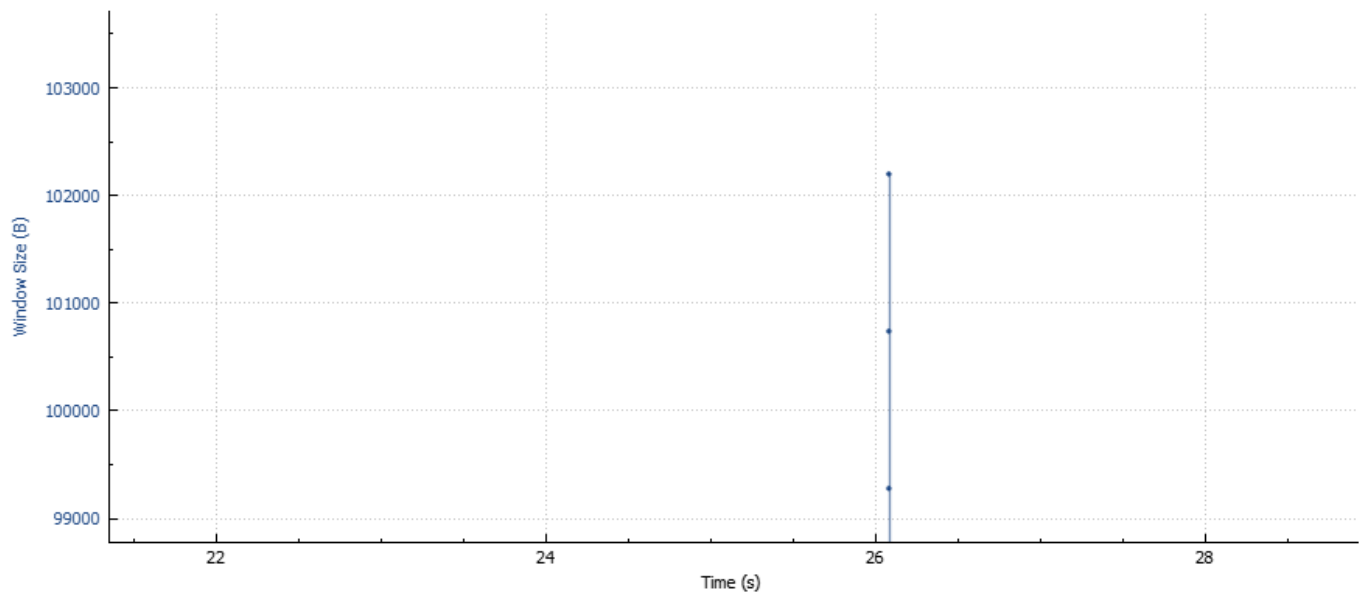
Wireshark - Conversations - Ethernet

Ethernet • 25														IPv4 • 43	IPv6 • 5	TCP • 92	UDP • 42
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				
172.16.1.82	80	172.23.143.215	61928	101,685	108 M	70,839	107 M	30,846	1744 k	0.000000	120.0702	7140 k	116 k				
172.16.1.82	80	172.23.143.215	61929	106,205	112 M	73,412	111 M	32,793	1869 k	0.000949	119.2454	7450 k	125 k				
172.23.143.215	62422	142.250.185.170	443	18	1134	9	594	9	540	74.100180	2.0719	2293	2085				
172.23.143.215	62360	142.250.186.42	443	2	126	1	66	1	60	4.006318	0.0072	73 k	66 k				
172.23.143.215	62417	172.217.18.99	443	10	636	6	396	4	240	64.973168	10.0666	314	190				
172.23.143.215	62361	172.217.18.106	443	10	630	5	330	5	300	5.455131	2.0652	1278	1162				
172.23.143.215	62362	172.217.18.106	443	10	630	5	330	5	300	5.705629	2.0925	1261	1146				
172.23.143.215	62363	142.250.185.202	443	10	630	5	330	5	300	7.521120	2.0650	1278	1162				
172.23.143.215	62364	142.250.185.202	443	10	630	5	330	5	300	7.798695	2.0838	1266	1151				
172.23.143.215	62420	142.250.186.170	443	13	822	7	462	6	360	70.856976	5.5670	663	517				
172.23.143.215	62423	142.250.181.234	443	18	1140	10	660	8	480	76.172852	2.5645	2058	1497				
172.23.143.215	62365	142.250.185.138	443	10	630	5	330	5	300	9.586657	2.0807	1268	1153				
172.23.143.215	62366	142.250.185.138	443	10	630	5	330	5	300	9.882909	2.0934	1261	1146				
172.23.143.215	62367	142.250.185.74	443	10	630	5	330	5	300	11.667843	2.0650	1278	1162				
172.23.143.215	62368	142.250.185.74	443	10	630	5	330	5	300	11.977289	2.0692	1275	1159				
172.23.143.215	62424	142.250.185.234	443	18	1140	10	660	8	480	76.424563	2.5648	2058	1497				
172.23.143.215	62369	216.58.212.138	443	10	630	5	330	5	300	13.733598	2.0573	1283	1166				
172.23.143.215	62370	216.58.212.138	443	9	570	5	330	4	240	14.047077	3.5779	737	536				
172.23.143.215	62371	142.250.185.170	443	10	630	5	330	5	300	15.791497	2.0947	1260	1145				
172.23.143.215	62372	142.250.185.170	443	10	630	5	330	5	300	17.625387	2.0788	1269	1154				
172.23.143.215	62373	142.250.181.234	443	10	630	5	330	5	300	17.886677	2.0932	1261	1146				
172.23.143.215	62374	142.250.181.234	443	10	630	5	330	5	300	19.704669	2.0738	1273	1157				
172.23.143.215	62375	142.250.184.234	443	10	630	5	330	5	300	19.980395	2.0749	1272	1156				
172.23.143.215	62376	142.250.184.234	443	10	630	5	330	5	300	21.778870	2.0941	1260	1146				
172.23.143.215	62377	142.250.186.170	443	10	630	5	330	5	300	22.055854	2.0732	1273	1157				
172.23.143.215	62378	142.250.186.170	443	10	630	5	330	5	300	23.873404	2.0820	1268	1152				
172.23.143.215	62379	142.250.185.234	443	10	630	5	330	5	300	24.129419	2.0626	1279	1163				
172.23.143.215	62380	142.250.185.234	443	10	630	5	330	5	300	25.955951	2.0935	1261	1146				
172.23.143.215	62381	142.250.186.74	443	10	630	5	330	5	300	26.192565	2.0873	1264	1149				
172.23.143.215	62382	142.250.186.74	443	10	630	5	330	5	300	28.049937	2.0516	1286	1169				
172.23.143.215	62383	172.217.16.138	443	10	630	5	330	5	300	28.280271	2.0706	1275	1159				
172.23.143.215	62384	74.125.206.188	443	10	630	5	330	5	300	28.953947	2.0643	1278	1162				
172.23.143.215	62385	172.217.16.138	443	10	630	5	330	5	300	30.101862	2.0653	1278	1162				
172.23.143.215	62386	142.250.185.106	443	9	570	5	330	4	240	30.351280	2.5727	1026	746				

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

Conversation Types▼

CopyFollow Stream...Graph...CloseHelp

Window Scaling for 172.16.1.82:80 → 172.23.143.215:49961
Ethernet

Hover over the graph for details. → 501 k pkts, 731 MB ← 216 k pkts, 0 bytes

Type Window Scaling

Stream 0 Switch Direction

Mouse ☒ drags ☐ zooms

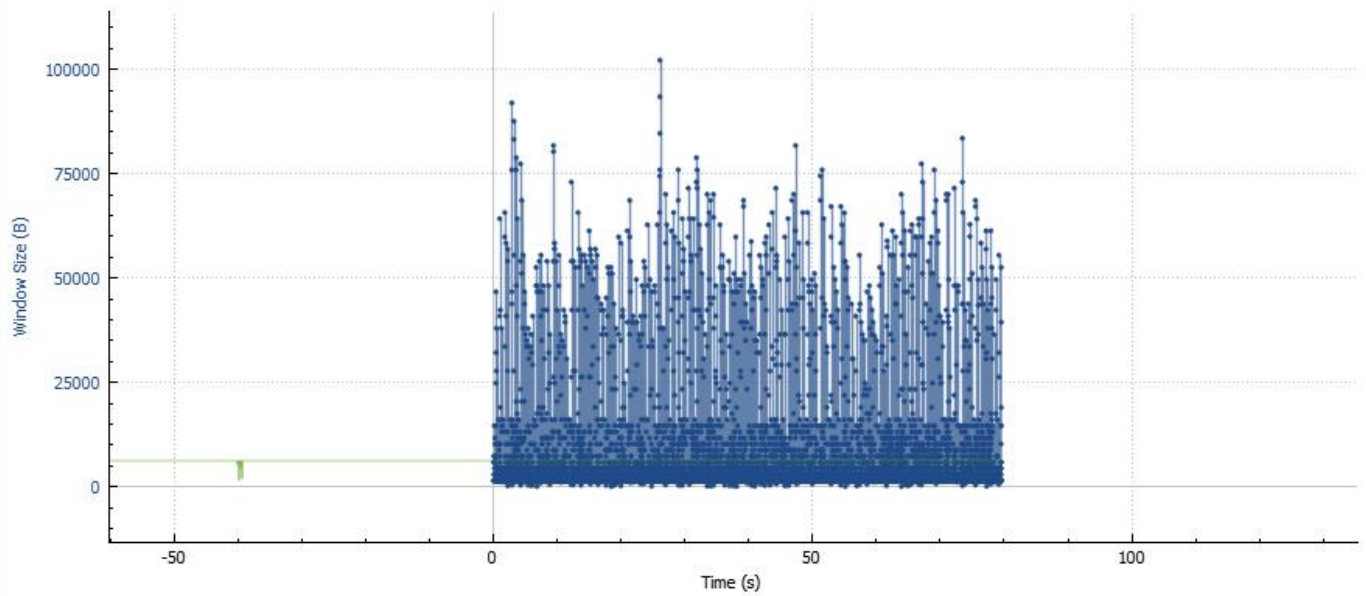
☒ Rcv Win ☒ Bytes Out

Reset

Save As...

Close

Help

Window Scaling for 172.16.1.82:80 → 172.23.143.215:49961
Ethernet

Type Window Scaling

Stream 0 Switch Direction

Mouse ● drags ○ zooms

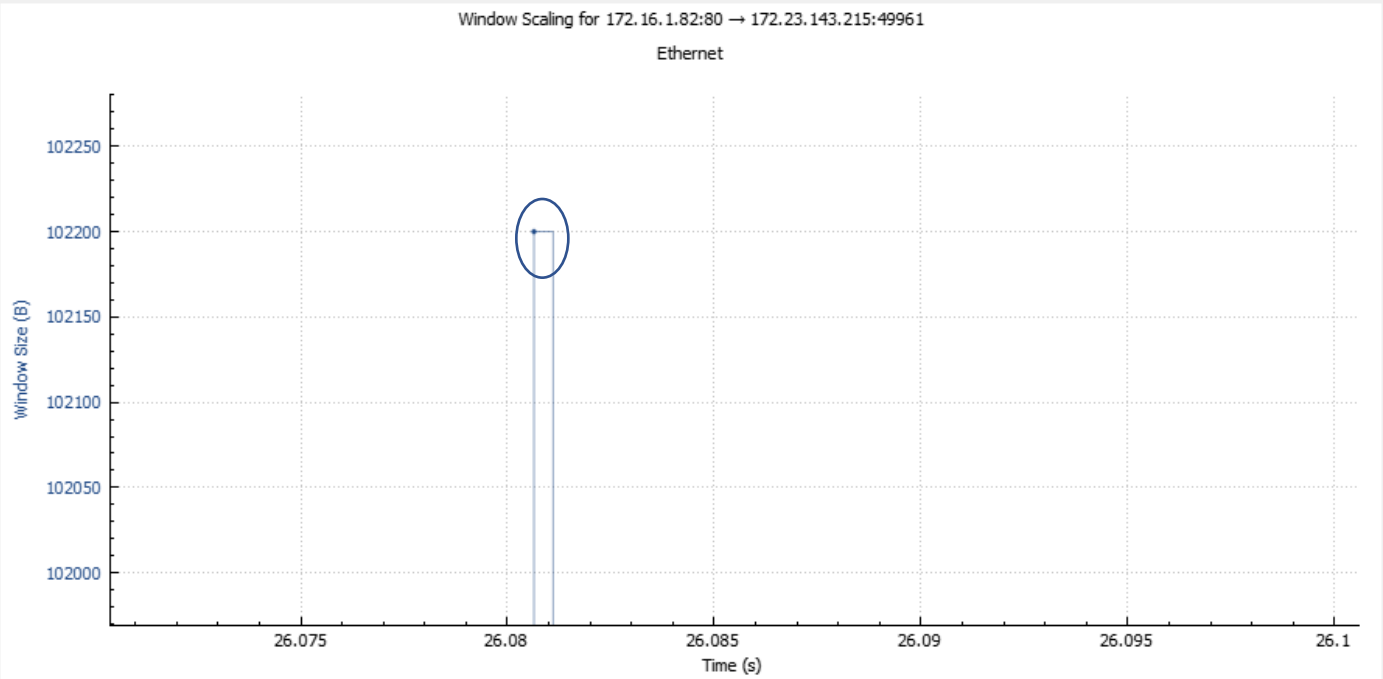
☒ Rcv Win ☒ Bytes Out

Reset

Save As...

Close

Help



Type Window Scaling

Stream 0

Switch Direction

Mouse ● drags ○ zooms

☒ Rcv Win ☒ Bytes Out

Reset

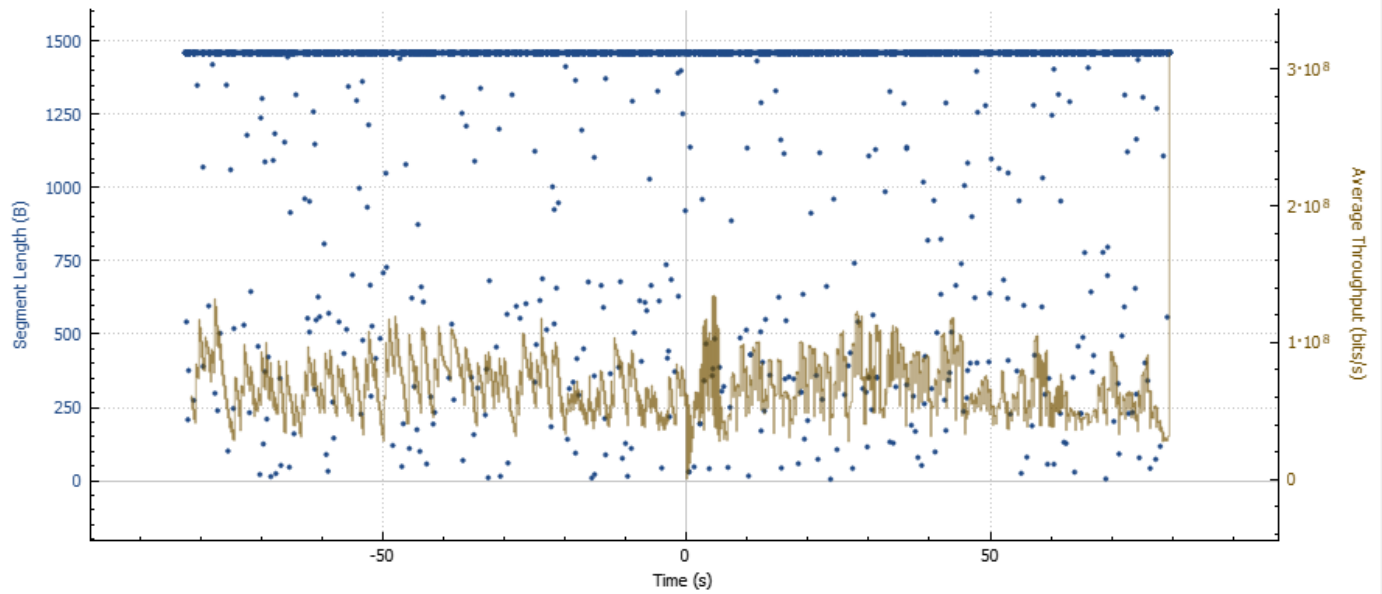
Save As...

Close

Help

Throughput for 172.16.1.82:80 → 172.23.143.215:49961 (MA)

Ethernet



Hover over the graph for details. → 501 k pkts, 731 MB ← 216 k pkts, 0 bytes

Type Throughput

MA Window (s) 1.000000

Stream 0 Switch Direction

Mouse ☒ drags ☐ zooms

☒ Segment Length ☒ Throughput ☐ Goodput

Reset

Save As...

Close

Help



در نقاطی که مشخص کردیم، زمانی که RTT حداکثر باشد، یعنی ازدحام زیاد است پس Throuput کم شده است.



Seq number = 459895452