گزارشکار آزمایش چهارم ، تحلیل TCP با استفاده از Wireshark

گروه 6 چهارشنبه ساعت 30 : 16 تا 19

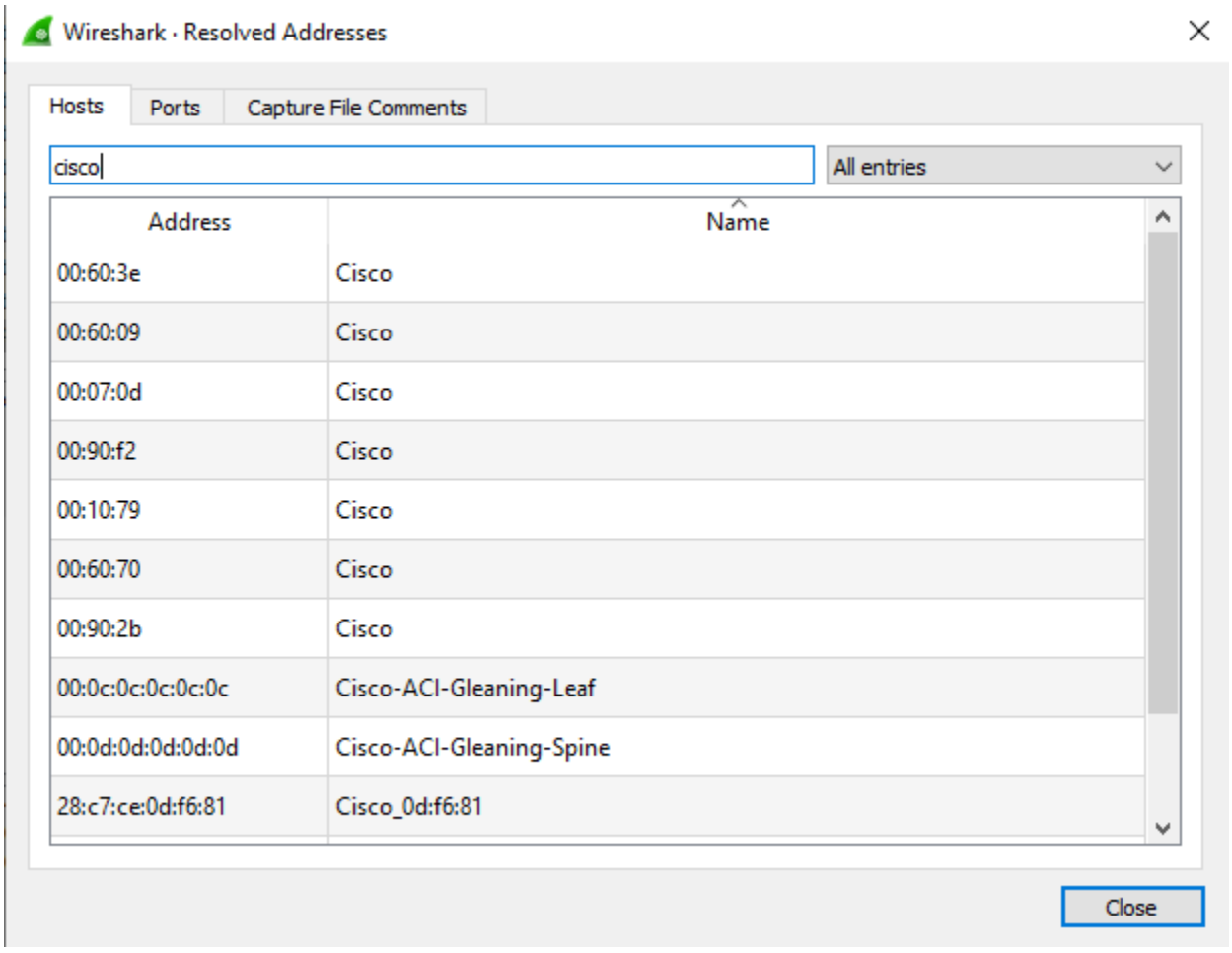
کیوان ایپچی / امیرحسین سرآهنگ

سوال 1 :

پنجره Resolver Addresses شامل 3 قسمت host ، port و ...capture است : که در تب host در بسته هایی که capture کردیم ، آدرس ها به چه اسم هایی map شدند . بعد از آن در تب port ، مشاهده می شود که چه پورت هایی داریم و چه تایپی دارند و به چه اسمی map شدند .

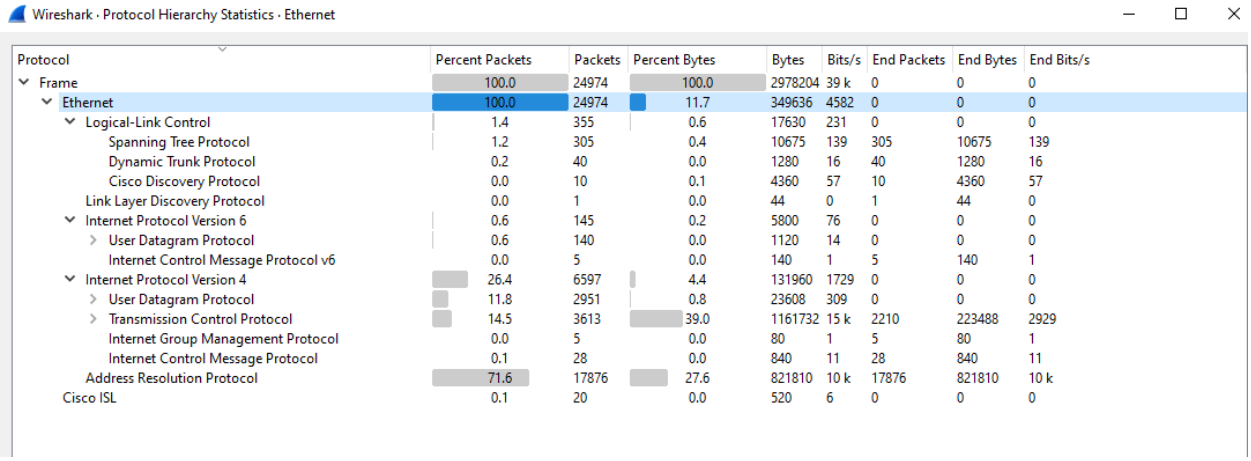
سوال 2 :

در بخش host ، cisco رو سرچ می کنیم و آدرس های فیزیکی مد نظر قابل رویت هستند .



سوال 3 :

در واقع درگاه ها و پروتوکل های مختلف مشاهده می شود و نیز 7 لایه شبکه رو هم به وضوح دیده می شود از جمله internet و transmission و ... برای مثال : 100 ٪ پکت ها از نوع Ethernet هستند .



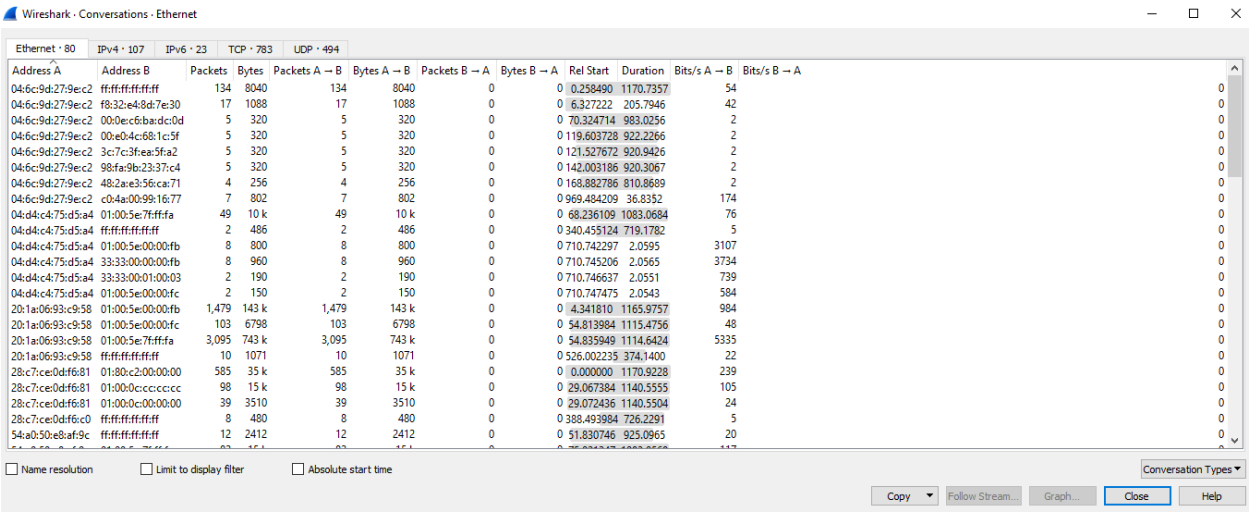
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	24974	100.0	2978204	39 k	0	0	0
Ethernet	100.0	24974	11.7	349636	4582	0	0	0
Logical-Link Control	1.4	355	0.6	17630	231	0	0	0
Spanning Tree Protocol	1.2	305	0.4	10675	139	305	10675	139
Dynamic Trunk Protocol	0.2	40	0.0	1280	16	40	1280	16
Cisco Discovery Protocol	0.0	10	0.1	4360	57	10	4360	57
Link Layer Discovery Protocol	0.0	1	0.0	44	0	1	44	0
Internet Protocol Version 6	0.6	145	0.2	5800	76	0	0	0
User Datagram Protocol	0.6	140	0.0	1120	14	0	0	0
Internet Control Message Protocol v6	0.0	5	0.0	140	1	5	140	1
Internet Protocol Version 4	26.4	6597	4.4	131960	1729	0	0	0
User Datagram Protocol	11.8	2951	0.8	23608	309	0	0	0
Transmission Control Protocol	14.5	3613	39.0	1161732	15 k	2210	223488	2929
Internet Group Management Protocol	0.0	5	0.0	80	1	5	80	1
Internet Control Message Protocol	0.1	28	0.0	840	11	28	840	11
Address Resolution Protocol	71.6	17876	27.6	821810	10 k	17876	821810	10 k
Cisco ISL	0.1	20	0.0	520	6	0	0	0

سوال 4 :

طبق تصویر بالا 26.4 ٪ بسته ها بر روی بستر IPv4 هستند .

سوال 5 :

در واقع مشخصات جفت آدرس هارو مشاهده می کنیم که آدرسA و B و پکت های مبادله شده و حجم آن ها چقدر بوده و همچنین پکت هایی که بهم فرستاده اند بر اساس مبدا و مقصد تفکیک شده به علاوه جفت آدرس ها بر اساس پروتوکل های مختلف نیز تفکیک شده .



Address A	Address 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
04:6c:9d:27:9e:c2	ff:ff:ff:ff:ff:ff	134	8040	134	8040	0	0	0.258490	1170.7357	54	0
04:6c:9d:27:9e:c2	f8:32:e4:8d:7e:30	17	1088	17	1088	0	0	6.327222	205.7946	42	0
04:6c:9d:27:9e:c2	00:0e:c6:ba:dc:0d	5	320	5	320	0	0	70.324714	983.0256	2	0
04:6c:9d:27:9e:c2	00:e0:4c:68:1c:5f	5	320	5	320	0	0	119.603728	922.2266	2	0
04:6c:9d:27:9e:c2	3c:7c:3f:ea:5f:a2	5	320	5	320	0	0	121.527672	920.9426	2	0
04:6c:9d:27:9e:c2	98:fa:9b:23:37:c4	5	320	5	320	0	0	142.003186	920.3067	2	0
04:6c:9d:27:9e:c2	48:2a:e3:56:ca:71	4	256	4	256	0	0	168.882786	810.8689	2	0
04:6c:9d:27:9e:c2	c0:4a:00:99:16:77	7	802	7	802	0	0	969.484209	36.8352	174	0
04:d4:c4:75:d5:a4	01:00:5e:7f:ff:fa	49	10 k	49	10 k	0	0	68.236109	1083.0684	76	0
04:d4:c4:75:d5:a4	ff:ff:ff:ff:ff:ff	2	486	2	486	0	0	340.455124	719.1782	5	0
04:d4:c4:75:d5:a4	01:00:5e:00:00:fb	8	800	8	800	0	0	710.742297	2.0595	3107	0
04:d4:c4:75:d5:a4	33:33:00:00:00:fb	8	960	8	960	0	0	710.745206	2.0565	3734	0
04:d4:c4:75:d5:a4	33:33:00:01:00:03	2	190	2	190	0	0	710.746637	2.0551	739	0
04:d4:c4:75:d5:a4	01:00:5e:00:00:fc	2	150	2	150	0	0	710.747475	2.0543	584	0
20:1a:06:93:c9:58	01:00:5e:00:00:fb	1,479	143 k	1,479	143 k	0	0	4.341810	1165.9757	984	0
20:1a:06:93:c9:58	01:00:5e:00:00:fc	103	6798	103	6798	0	0	54.813984	1115.4756	48	0
20:1a:06:93:c9:58	01:00:5e:7f:ff:fa	3,095	743 k	3,095	743 k	0	0	54.835949	1114.6424	5335	0
20:1a:06:93:c9:58	ff:ff:ff:ff:ff:ff	10	1071	10	1071	0	0	526.002235	374.1400	22	0
28:c7:ce:0d:f6:81	01:80:c2:00:00:00	585	35 k	585	35 k	0	0	0.000000	1170.9228	239	0
28:c7:ce:0d:f6:81	01:00:0c:cc:cc:cc	98	15 k	98	15 k	0	0	29.067384	1140.5555	105	0
28:c7:ce:0d:f6:81	01:00:0c:00:00:00	39	3510	39	3510	0	0	29.072436	1140.5504	24	0
28:c7:ce:0d:f6:c0	ff:ff:ff:ff:ff:ff	8	480	8	480	0	0	388.493984	726.2291	5	0
54:a0:50:e8:af:9c	ff:ff:ff:ff:ff:ff	12	2412	12	2412	0	0	51.830746	925.0965	20	0

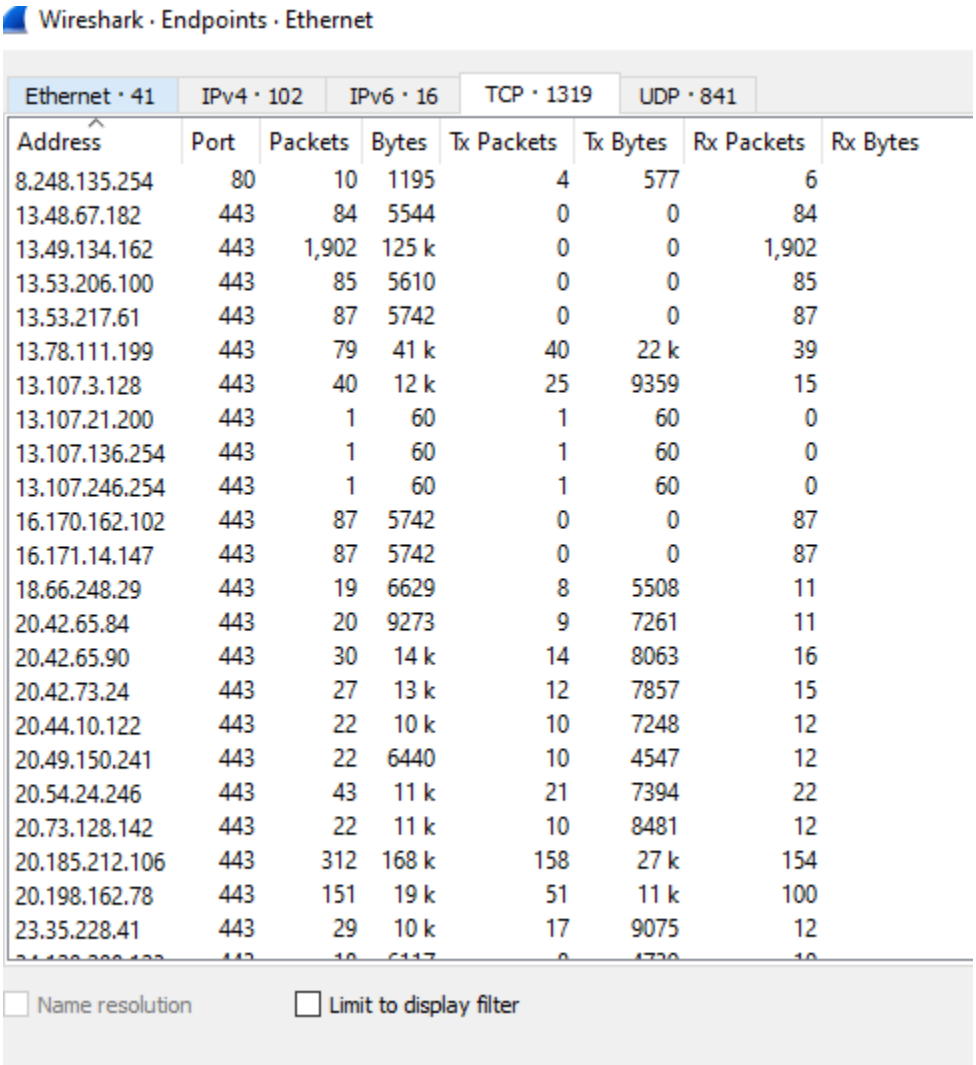
سوال 6 :

رو پروتکل TCP، right click کردیم و از قسمت follow ، tcp stream رو انتخاب کردیم و مشاهده کردیم که دیتا به علت https بودن رمزنگاری شده است و قادر به مشاهده دیتای خام آن نیستیم .

سوال 7 :

چون در conversation داریم مبادله اطلاعات می کنیم دو طرفه هست چون هم از A به B هست و بل عکس

اما در endpoint از دیدگاه گره ای به موضوع نگاه می شود و آدرس ip هایی که در ارتباط tcp با سیستم ما استفاده شده اند قابل رویت هست .


Wireshark · Endpoints · Ethernet

Ethernet · 41 | IPv4 · 102 | IPv6 · 16 | TCP · 1319 | UDP · 841

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
8.248.135.254	80	10	1195	4	577	6	
13.48.67.182	443	84	5544	0	0	84	
13.49.134.162	443	1,902	125 k	0	0	1,902	
13.53.206.100	443	85	5610	0	0	85	
13.53.217.61	443	87	5742	0	0	87	
13.78.111.199	443	79	41 k	40	22 k	39	
13.107.3.128	443	40	12 k	25	9359	15	
13.107.21.200	443	1	60	1	60	0	
13.107.136.254	443	1	60	1	60	0	
13.107.246.254	443	1	60	1	60	0	
16.170.162.102	443	87	5742	0	0	87	
16.171.14.147	443	87	5742	0	0	87	
18.66.248.29	443	19	6629	8	5508	11	
20.42.65.84	443	20	9273	9	7261	11	
20.42.65.90	443	30	14 k	14	8063	16	
20.42.73.24	443	27	13 k	12	7857	15	
20.44.10.122	443	22	10 k	10	7248	12	
20.49.150.241	443	22	6440	10	4547	12	
20.54.24.246	443	43	11 k	21	7394	22	
20.73.128.142	443	22	11 k	10	8481	12	
20.185.212.106	443	312	168 k	158	27 k	154	
20.198.162.78	443	151	19 k	51	11 k	100	
23.35.228.41	443	29	10 k	17	9075	12	

Name resolution Limit to display filter

Wireshark · Conversations · Ethernet

Ethernet · 82 | IPv4 · 128 | IPv6 · 24 | TCP · 1342 | UDP · 849

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
13.107.21.200	443	172.23.141.169	12723	1	60	1	60	0	0	122.970642	0.0000	—	
13.107.136.254	443	172.23.141.169	12730	1	60	1	60	0	0	122.311599	0.0000	—	
13.107.246.254	443	172.23.141.169	12727	1	60	1	60	0	0	121.471020	0.0000	—	
52.98.163.34	443	172.23.141.169	10341	1	60	1	60	0	0	698.579951	0.0000	—	
52.113.196.254	443	172.23.141.169	12728	1	60	1	60	0	0	125.787472	0.0000	—	
172.23.141.169	12736	13.49.134.162	443	3	198	3	198	0	0	0.319353	3.0244	523	
172.23.141.169	12733	13.53.206.100	443	1	66	1	66	0	0	0.332821	0.0000	—	
172.23.141.169	6617	152.199.19.161	443	2	108	2	108	0	0	1.017345	11.1413	77	
172.23.141.169	12737	16.170.162.102	443	3	198	3	198	0	0	1.315857	3.0218	524	
172.23.141.169	12738	13.49.134.162	443	1	66	1	66	0	0	4.316615	0.0000	—	
172.23.141.169	12739	142.250.181.68	443	1,057	642 k	452	44 k	605	598 k	4.473078	321.9151	1098	
172.23.141.169	12740	142.250.181.68	443	4	264	1	66	3	198	4.859473	2.5851	204	
172.23.141.169	12741	142.250.181.68	443	4	264	1	66	3	198	4.890822	2.5357	208	
172.23.141.169	12716	142.250.186.46	443	29	2378	14	1163	15	1215	5.279683	240.2691	38	
172.23.141.169	12742	142.250.186.131	443	14	2283	8	1103	6	1180	5.286372	68.5588	128	
172.23.141.169	12743	142.250.186.42	443	15	2340	9	1160	6	1180	5.286888	68.5583	135	
172.23.141.169	12744	172.16.1.137	443	68	31 k	28	3816	40	27 k	5.287704	76.8736	397	
172.23.141.169	12745	16.171.14.147	443	3	198	3	198	0	0	5.315220	3.0131	525	
172.23.141.169	12746	13.49.134.162	443	2	132	2	132	0	0	5.315534	1.0010	1054	
172.23.141.169	12747	142.250.184.195	443	109	58 k	50	4801	59	53 k	6.059230	249.8995	153	
172.23.141.169	12748	13.49.134.162	443	2	132	2	132	0	0	6.318388	1.0114	1044	
172.23.141.169	12863	20.185.212.106	443	131	90 k	53	75 k	78	15 k	8.265706	2071.6027	292	
172.23.141.169	12749	13.49.134.162	443	3	198	3	198	0	0	8.322985	3.0271	523	

Name resolution | Limit to display filter | Absolute start time

سوال 8 :

لزوما بیشتر پکت رو داشتن دلیل بر defualt gateway بودن نیست اما با میشه با تخمین خوبی گفت که آدرسی که بیشترین تعداد پکت رو داره میتونه defualt gateway باشه !

Wireshark · Endpoints · Ethernet

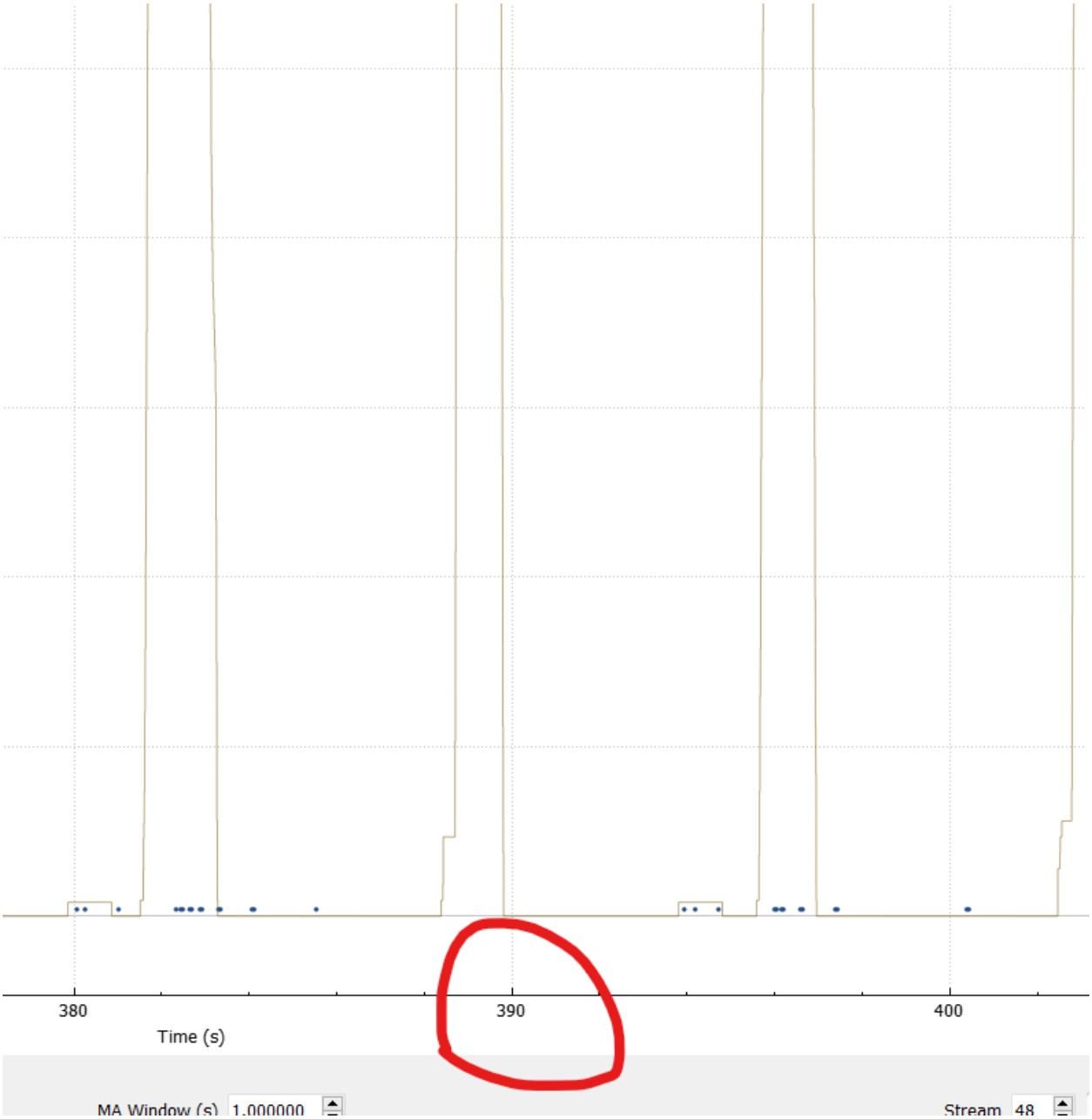
Ethernet · 44 | IPv4 · 111 | IPv6 · 16 | TCP · 1758 | UDP · 1131

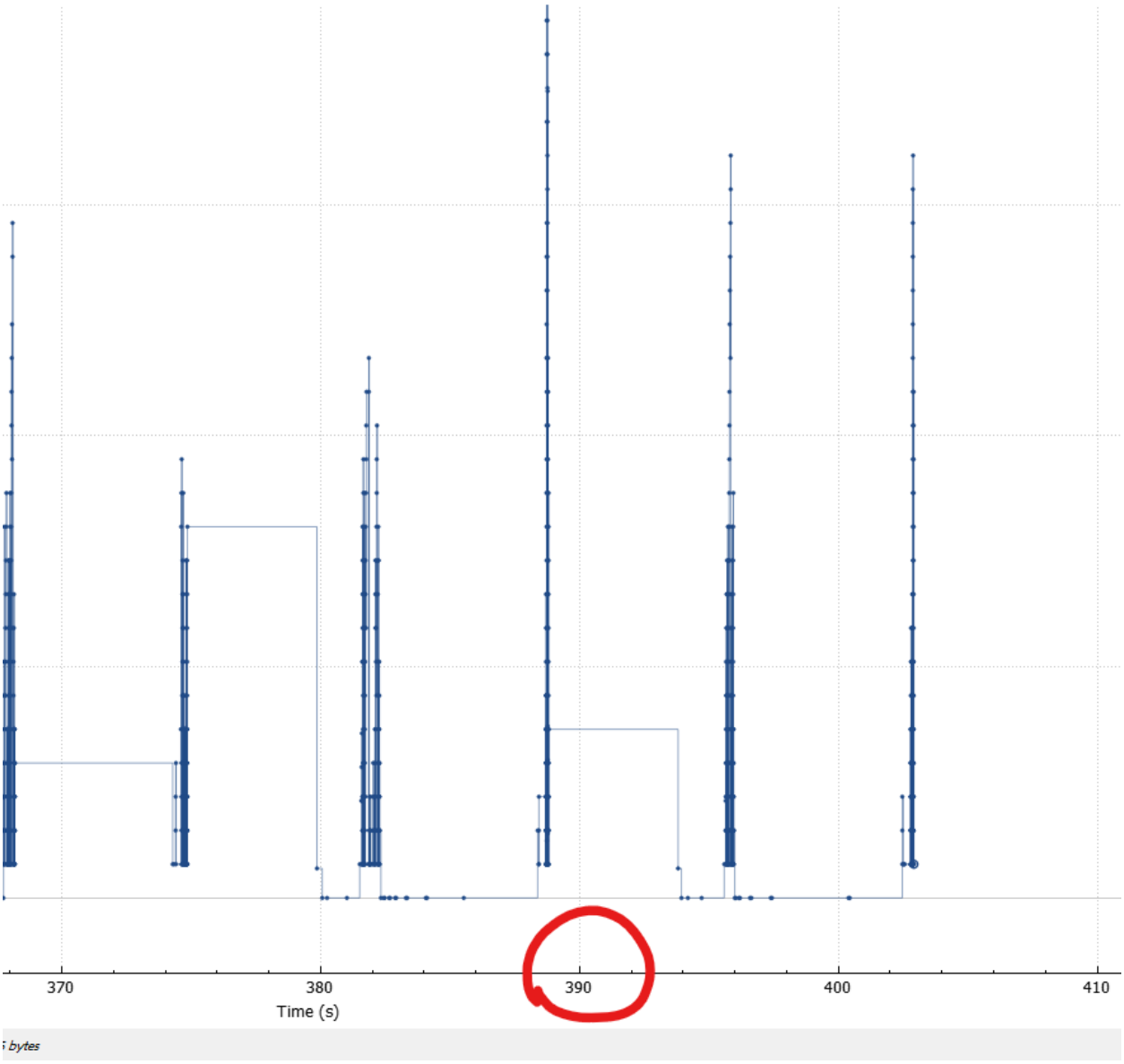
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
ff:ff:ff:ff:ff:ff	34,631	2102 k	0	0	34,631	
98:29:a6:4a:0d:04	33,956	2060 k	33,956	2060 k	0	
20:1a:06:93:c9:58	11,584	2157 k	11,584	2157 k	0	
04:6c:9d:27:9e:c2	11,429	3122 k	4,691	2002 k	6,738	
ac:22:0b:0f:38:d1	10,970	3126 k	6,996	1167 k	3,974	
01:00:5e:7f:ff:fa	9,125	2101 k	0	0	9,125	
01:00:5e:00:00:fb	3,969	391 k	0	0	3,969	

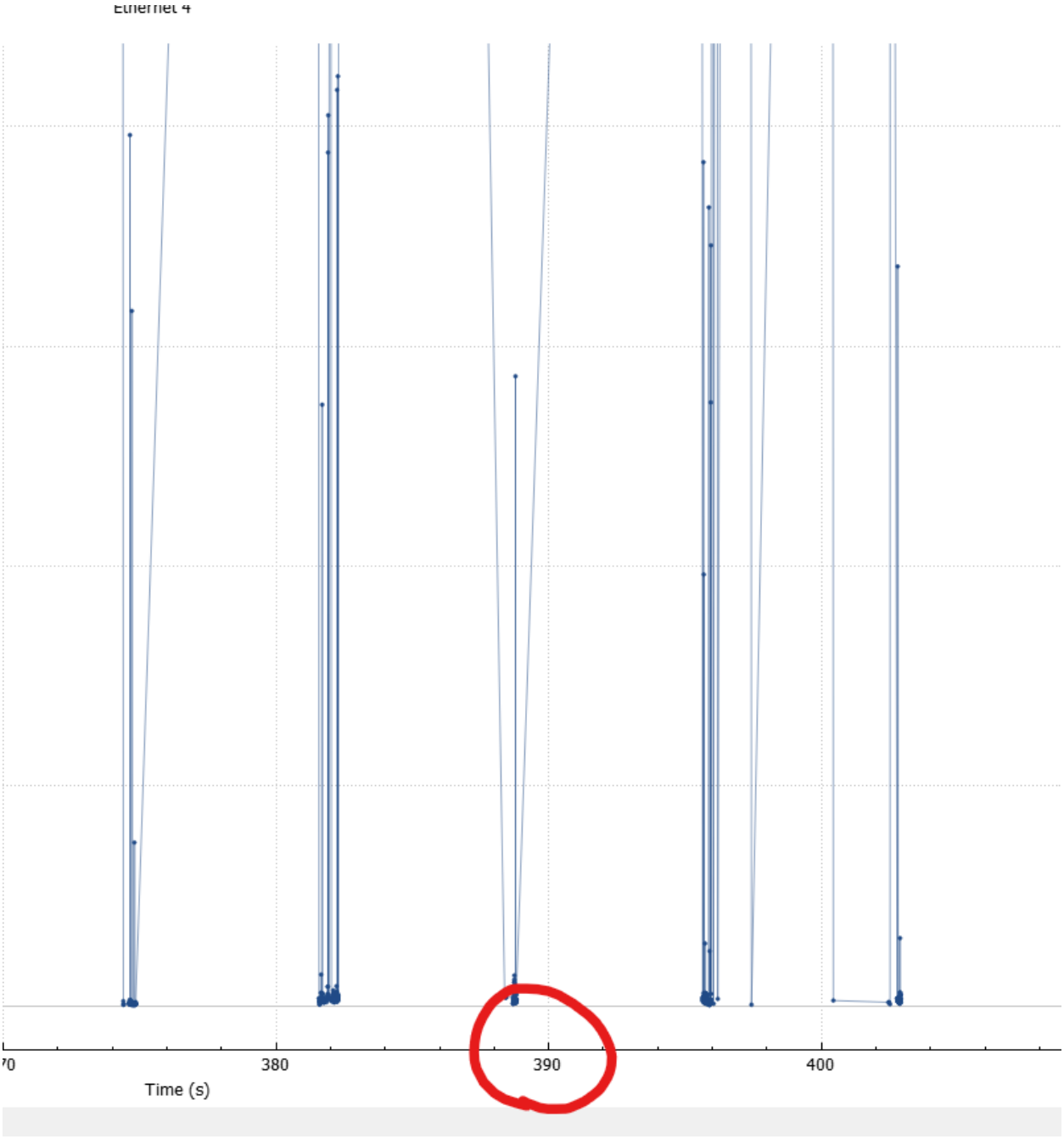
سوال 9)

در شرایط ازدحام throughput کاهش پیدا می کنه و RTT افزایش پیدا میکند اما در نقاطی که اردحام کم میشود شرایط عکس اتفاق می افتد !

در Windows scaling نیز زمانی که نشانه ای از ازدحام ظاهر می شود فرستنده مجبود به ارسال مجدد بسته ها می شود و به همین علت به طور ناگهانی کاهش پیدا می کند !


380
390
400
Time (s)
MA Window (s) 1.000000
Stream 48


370
380
390
400
410
Time (s)
bytes


Ethernet 4
70
380
390
400
Time (s)