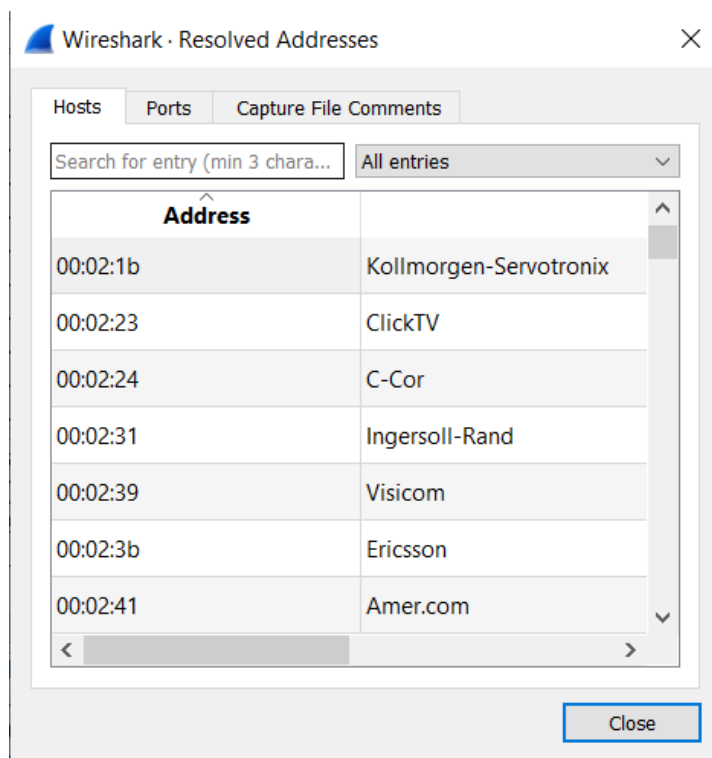


## به نام خدا

۹۷۲۳۱۰۰	محمد مهدی هجرتی
تحلیل TCP با استفاده از Wireshark	آزمایشگاه شبکه - آزمایش هشتم
خرداد ۱۴۰۰	استاد نقی زاده

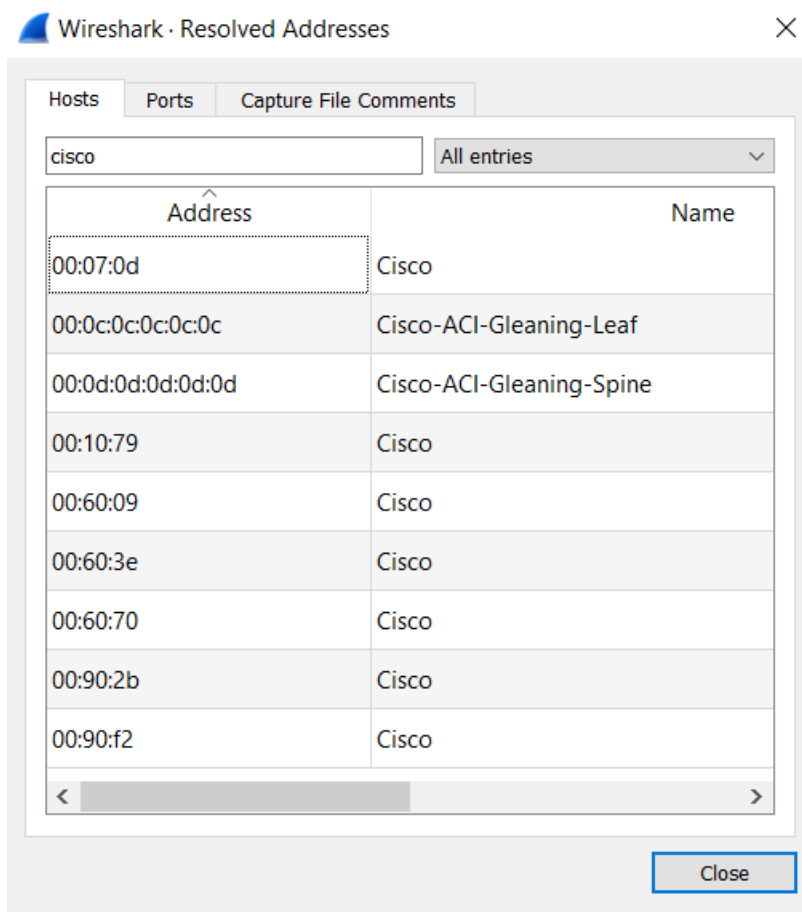
### سوال ۱

این پنجره دو بخش دارد. یک بخش که برای تبدیل اسم هاست به آدرس از آن استفاده می شود. و بخش دیگر برای تبدیل پورت ها به اسم هاست.



## سوال ۲

آدرس فیزیکی کارت شبکه های cisco همگی با ۰۰ شروع می شوند اما بایت سوم ا، ۶ یا ۹ می باشد.



### سوال ۳

در این پنجره آمار مربوط به بسته های کپچر شده را مشاهده می کنیم که به صورت سطح بندی شده آماری شامل تعداد پکت ها و حجم و ... هر کدام از پروتکل ها را نشان می دهد.

Wireshark · Protocol Hierarchy Statistics · Wi-Fi 3

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	22992	100.0	13114517	1116k	0	0	0
▼ Ethernet	100.0	22992	2.5	321888	27k	0	0	0
▼ Internet Protocol Version 6	3.2	730	0.2	29200	2485	0	0	0
▼ User Datagram Protocol	3.0	682	0.0	5456	464	0	0	0
QUIC IETF	2.6	608	1.3	166263	14k	588	155116	13k
Domain Name System	0.4	94	0.1	7108	604	94	7108	604
▼ Transmission Control Protocol	0.1	24	0.0	2037	173	19	478	40
Transport Layer Security	0.0	4	0.0	1458	124	4	1458	124
Data	0.0	1	0.0	1	0	1	1	0
Internet Control Message Protocol v6	0.1	24	0.0	728	61	24	728	61
▼ Internet Protocol Version 4	96.8	22250	3.4	445000	37k	0	0	0
▼ User Datagram Protocol	21.5	4950	0.3	39600	3370	0	0	0
Simple Service Discovery Protocol	0.0	4	0.0	692	58	4	692	58
Session Traversal Utilities for NAT	0.4	96	0.1	7924	674	96	7924	674
QUIC IETF	0.2	37	0.1	19202	1634	35	17418	1482
Domain Name System	0.4	100	0.1	7574	644	100	7574	644
Data	20.5	4715	5.1	665606	56k	4715	665606	56k
▼ Transmission Control Protocol	75.2	17300	86.9	11399796	970k	11744	6262104	532k
▼ X11	0.7	160	0.0	5100	434	11	639	54
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Transport Layer Security	23.9	5491	55.3	7247855	616k	5437	6930842	589k
▼ Hypertext Transfer Protocol	0.0	6	0.0	6518	554	5	1963	167
eXtensible Markup Language	0.0	1	0.0	4214	358	1	4555	387
Data	0.4	101	0.8	105823	9006	101	105823	9006
Address Resolution Protocol	0.1	12	0.0	336	28	12	336	28

No display filter.

Close Copy Help

### سوال ۴

همان طور که در تصویر بالا مشاهده می شود، ۷۵٫۲ درصد از بسته ها مربوط به TCP با IPV4 می باشد.

## سوال ۵

در این پنجره، اطلاعات و آمار مربوط به نشست های برقرار شده و تعداد و حجم بسته های رد و بدل شده در هر جهت و ... را نشان می دهد.

Wireshark · Conversations · Wi-Fi 3

Ethernet · 2		IPv4 · 19		IPv6 · 14		TCP · 130		UDP · 111			
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
5.144.130.115	192.168.43.107	38	13k	19	9966	19	3510	52.348026	6.4399	12k	4360
5.144.130.116	192.168.43.107	1,243	939k	815	843k	428	95k	47.594528	37.6457	179k	20k
20.198.162.76	192.168.43.107	8	1125	0	0	8	1125	18.654699	22.5584	0	398
23.61.94.150	192.168.43.107	15	5602	8	4999	7	603	18.874778	21.6217	1849	223
34.252.217.79	192.168.43.107	39	16k	21	13k	18	3044	46.296889	45.6678	2414	533
51.103.5.159	192.168.43.107	29	8814	17	5604	12	3210	44.907225	0.8498	52k	30k
52.114.158.91	192.168.43.107	31	13k	15	8019	16	5159	2.595703	5.9685	10k	6914
52.218.112.72	192.168.43.107	39	13k	22	10k	17	2818	80.753100	8.6791	9931	2597
82.178.158.114	192.168.43.107	67	11k	35	3961	32	7557	45.910824	33.0868	957	1827
88.135.37.4	192.168.43.107	500	331k	320	300k	180	31k	56.937508	23.6875	101k	10k
92.114.19.28	192.168.43.107	115	54k	63	43k	52	10k	45.907192	30.2692	11k	2833
93.113.225.8	192.168.43.107	44	37k	29	35k	15	2845	81.428370	0.3096	907k	73k
104.21.31.16	192.168.43.107	35	19k	19	15k	16	3247	55.439397	0.4848	261k	53k
151.101.2.219	192.168.43.107	21	8370	12	6536	9	1834	48.470036	0.7321	71k	20k
154.13.1.221	192.168.43.107	15,007	10M	8,215	9781k	6,792	662k	0.340175	93.5627	836k	56k
192.168.43.1	192.168.43.107	100	11k	50	7713	50	4061	2.410068	79.0174	780	411
192.168.43.107	212.16.77.237	4,897	961k	91	12k	4,806	948k	0.000000	94.0003	1100	80k
192.168.43.107	212.16.77.235	18	1908	9	558	9	1350	5.422605	80.4358	55	134
192.168.43.107	239.255.255.250	4	860	4	860	0	0	83.800344	3.0098	2285	0

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾

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

## سوال ۶

در این پنجره لیست endpoint هایی که با آن ها ارتباط برقرار شده و آمار و ارقام مربوط به آن آورده شده است.

Wireshark · Endpoints · Wi-Fi 3

Ethernet · 3IPv4 · 20IPv6 · 15TCP · 112UDP · 126

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
5.144.130.115	443	38	13k	19	9966	19	3510
5.144.130.116	80	27	3304	12	1338	15	1966
5.144.130.116	443	1,216	936k	803	842k	413	94k
20.198.162.76	443	8	1125	0	0	8	1125
23.61.94.150	80	15	5602	8	4999	7	603
34.252.217.79	443	39	16k	21	13k	18	3044
51.103.5.159	443	29	8814	17	5604	12	3210
52.114.158.91	443	31	13k	15	8019	16	5159
52.218.112.72	443	39	13k	22	10k	17	2818
82.178.158.114	443	67	11k	35	3961	32	7557
88.135.37.4	443	500	331k	320	300k	180	31k
92.114.19.28	443	115	54k	63	43k	52	10k
93.113.225.8	443	44	37k	29	35k	15	2845
151.101.2.219	443	21	8370	12	6536	9	1834
154.13.1.221	9002	15,007	10M	8,215	9781k	6,792	662k
192.168.43.107	1035	265	118k	140	82k	125	35k
192.168.43.107	1041	60	9871	29	6700	31	3171

☐ Name resolution

☐ Limit to display filter

Endpoint Types ▼

Copy ▼

Map ▼

Close

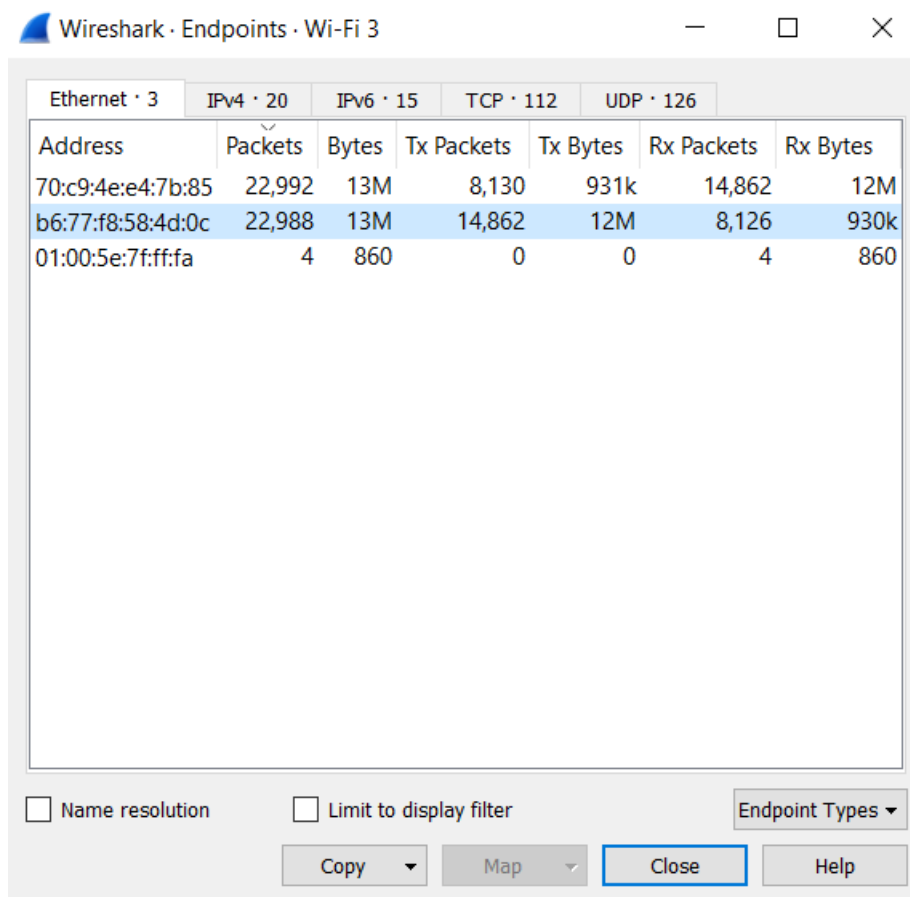
Help

## سوال ۷

در تصویر بالا، از ردیف address می توان لیست مقاصد ارتباط TCP را مشاهده کرد.

## سوال ۸

با توجه به تعداد بالای پکت های ارسال شده از آدرس bf:77:f8:58:4d:0c به نظر می رسد، default gateway ما همین آدرس باشد.



Wireshark · Endpoints · Wi-Fi 3

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
70:c9:4e:e4:7b:85	22,992	13M	8,130	931k	14,862	12M
bf:77:f8:58:4d:0c	22,988	13M	14,862	12M	8,126	930k
01:00:5e:7f:ff:fa	4	860	0	0	4	860

☐ Name resolution ☐ Limit to display filter Endpoint Types ▾

Copy ▾ Map ▾ Close Help

## سوال ۹

به کمک tshark بسته ها را کپچر می کنیم و سپس در وایرشارک آن ها را مشاهده می کنیم.

```
C:\Windows\System32\cmd.exe

D:\Program Files (x86)\Wireshark>tshark -D
1. \Device\NPF_{41F11FF3-C5DD-4830-BE4B-C02D9EDF23CE} (Local Area Connection* 10)
2. \Device\NPF_{A49AFCBB-5AAD-48EF-8AF6-795C0C16951A} (Local Area Connection* 9)
3. \Device\NPF_{19C08828-F853-49CF-A976-C78EAAE4FB4A} (Wi-Fi 3)
4. \Device\NPF_{D7A1C799-2D7C-470B-BCFC-C1B06DC5A4F6} (Local Area Connection* 1)
5. \Device\NPF_{FD1B0CB1-5E5A-4267-B853-E8DDF531D3B9} (Local Area Connection* 8)
6. \Device\NPF_{A43C4B56-90E5-4E42-ABB0-321DAFAE8F34} (VMware Network Adapter VMnet1)
7. \Device\NPF_{F009144C-EE2B-408B-8E0E-B9849FEFA695} (VMware Network Adapter VMnet8)
8. \Device\NPF_{DD137C41-9E69-48C6-BAB7-391471FB8314} (Local Area Connection* 2)
9. \Device\NPF_Loopback (Adapter for loopback traffic capture)
10. \Device\NPF_{71E58854-7B0A-4A39-8D9A-9D4723E635DE} (Ethernet 2)

D:\Program Files (x86)\Wireshark>tshark -i 3 -p -w output.pcap
Capturing on 'Wi-Fi 3'
23588

D:\Program Files (x86)\Wireshark>
```

با توجه به نشست های زیر می توان حدس زد که آی پی سایت دانشگاه ۱۸۵/۲۱۱/۸۸/۱۳۱ می باشد.

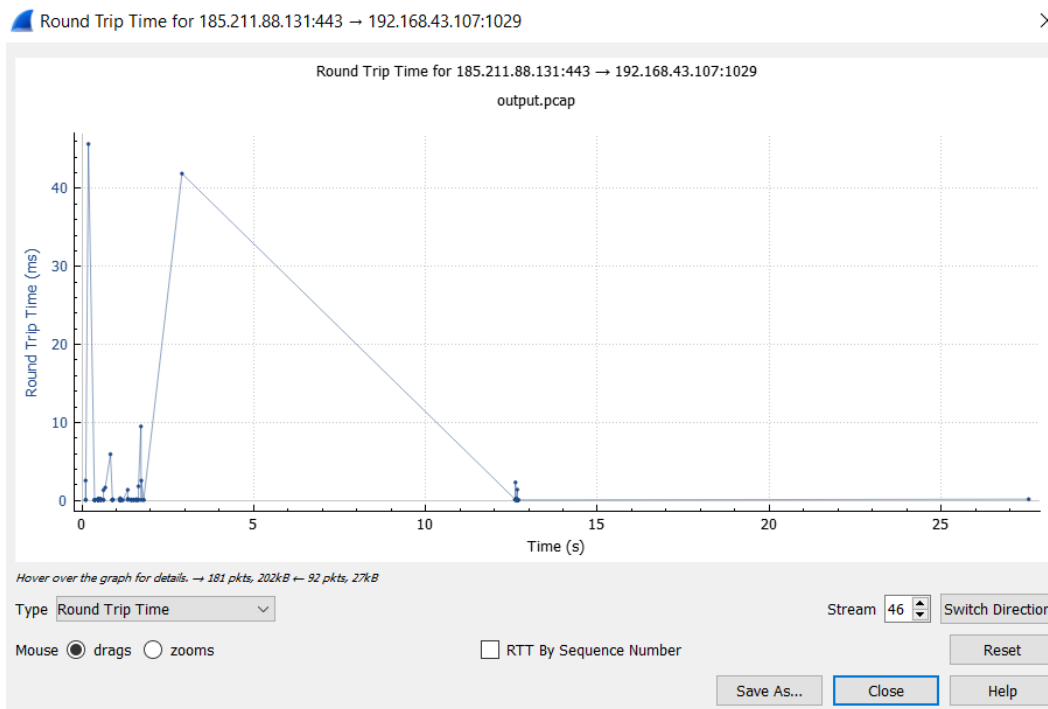
Wireshark · Conversations · output.pcap

Ethernet · 8		IPv4 · 17		IPv6 · 20		TCP · 83		UDP · 98						
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		
192.168.43.107	24288	46.4.74.56	443	15,311	16M	4,185	255k	11,126	16M	132.158230	65.4293			
192.168.43.107	13265	109.94.166.16	443	1,911	1573k	423	24k	1,488	1548k	14.626395	1.4234			
192.168.43.107	32483	185.211.88.131	443	757	838k	178	23k	579	814k	50.288735	37.9205			
192.168.43.107	1031	185.211.88.131	443	350	343k	104	27k	246	315k	49.878470	38.2607			
192.168.43.107	31906	185.211.88.131	443	323	314k	93	28k	230	285k	50.290647	37.9190			
192.168.43.107	8520	185.211.88.131	443	297	275k	96	29k	201	246k	50.286870	37.9226			
192.168.43.107	1029	185.211.88.131	443	273	244k	92	32k	181	211k	49.878061	38.2604			
192.168.43.107	28430	185.211.88.131	443	223	182k	79	31k	144	151k	50.291847	37.9176			
192.168.43.107	29419	109.94.166.16	443	192	149k	50	5429	142	144k	14.352768	126.6993			
192.168.43.107	1046	109.94.166.16	443	160	120k	38	4171	122	116k	14.352363	126.6997			
192.168.43.107	1039	185.211.88.131	443	95	80k	30	8396	65	72k	89.211027	31.8964			
192.168.43.107	1043	185.211.88.131	443	83	63k	31	8469	52	55k	9.127285	29.1251			
192.168.43.107	24022	154.28.188.213	9002	108	63k	49	5529	59	57k	1.454643	182.1719			
192.168.43.107	26182	185.211.88.131	443	84	57k	40	24k	44	33k	152.019591	41.8469			
192.168.43.107	13608	185.211.88.131	443	84	54k	37	16k	47	37k	80.220075	31.8775			

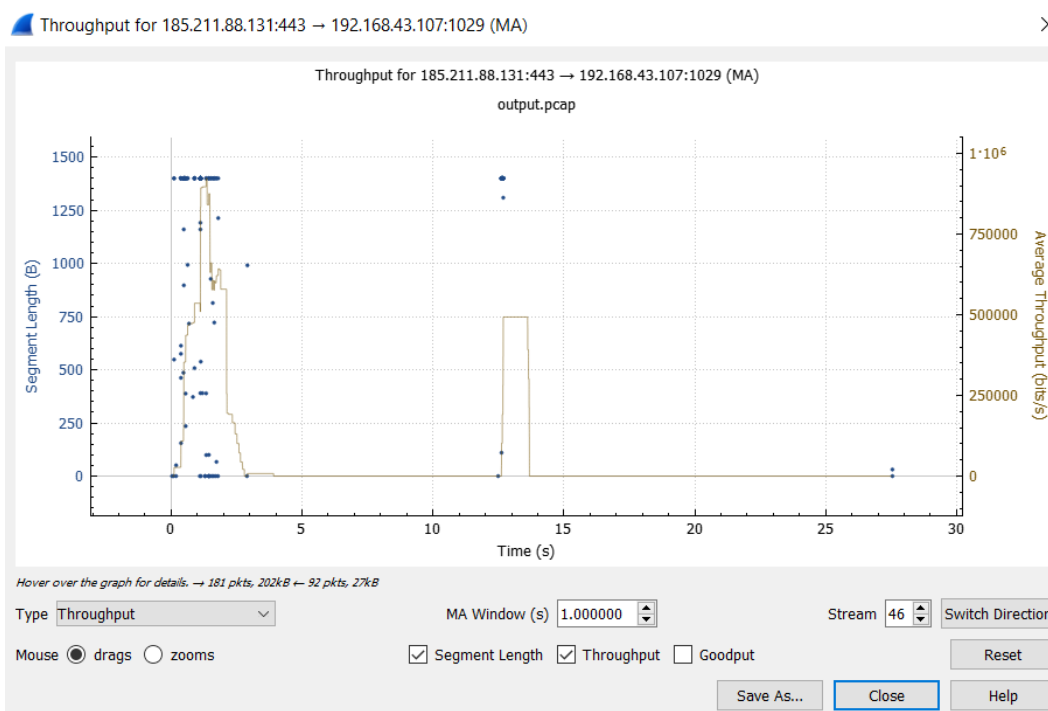
☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾
 Copy ▾ Follow Stream... Graph... Close Help

در تصویر زیر نمودار زمان رفت و برگشت در زمان های مختلف را برای یکی از ارتباط های بین سرور دانشگاه و سیستم خودمان را می بینیم.

به نظر می رسد در زمان شروع ارتباط و نیز حدود ثانیه ی سوم اختلالی بوجود آمده است.



این نمودار میزان گذردهی بر حسب زمان را نشان می دهد. که در ثانیه سوم کاهش یافته است.





نمودار بعدی اندازه پنجره ی ارسال را در زمان های مختلف نشان می دهد.

