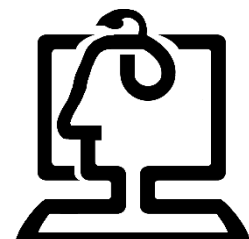


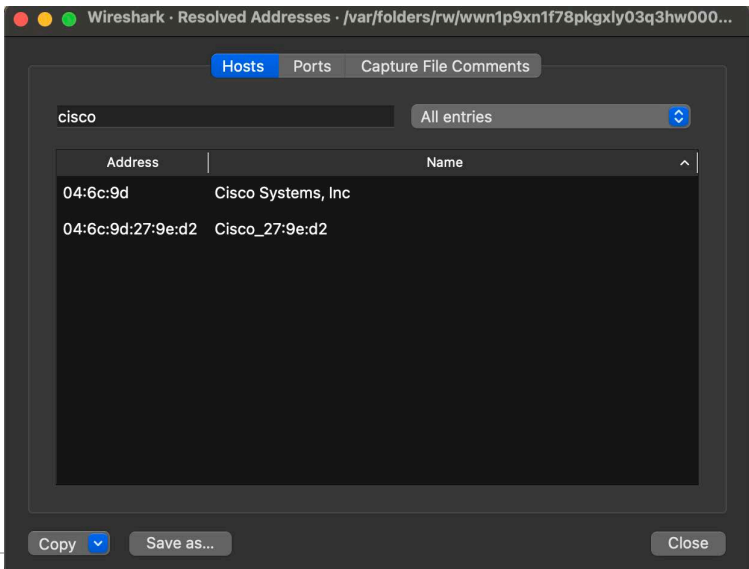


دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

فرم گزارش کار آزمایشگاه شبکه



دانشکده مهندسی کامپیوتر

نام و نام خانوادگی	کیان پورآذر	شماره دانشجویی	۴۰۱۳۱۴۰۳	نام و شماره آزمایش	۶- تحلیل TCP با استفاده از وایرشارک
هدف آزمایش	آشنایی بیشتر با نرم افزار wireshark و منوی statistics آن و تحلیل بسته های جمع آوری شده با استفاده از این ابزار				
ابزارها و مورد نیاز	نرم افزار وایرشارک				
شرح آزمایش	<p>سوال ۱:</p> <p>در بخش host، مک آدرس hostها را میبینیم.</p> <p>در بخش ports نام و پورت و نوع سرویس ها را میبینیم.</p> <p>در بخش capture file comments کامنتها را میبینیم.</p> <p>سوال ۲: سه بایت اول در تصویر میباشد</p> 				

سوال ۳: لایه های مختلف به همراه اطلاعات مختلف مشاهده میشود.

Wireshark - Protocol Hierarchy Statistics - Wi-Fi: en0

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	24224	100.0	14834510	571 k	0	0	0	24224
Ethernet	100.0	24224	2.6	387254	14 k	0	0	0	24224
Logical-Link Control	0.1	29	0.0	106	4	0	0	0	29
Logical-Link Control Basic Format XID	0.0	10	0.0	430	16	10	430	16	10
Data	0.1	19	0.0	418	16	19	418	16	19
Internet Protocol Version 6	3.0	718	0.2	28720	1106	0	0	0	718
User Datagram Protocol	2.8	669	0.0	5352	206	0	0	0	669
Multicast Domain Name System	2.8	669	1.3	191063	7359	669	191063	7359	669
Internet Control Message Protocol v6	0.2	49	0.0	1472	56	49	1472	56	49
Internet Protocol Version 4	85.6	20740	2.8	414808	15 k	0	0	0	20740
User Datagram Protocol	12.5	3033	0.2	24264	934	0	0	0	3033
QUIC IETF	8.7	2102	12.1	1793329	69 k	2101	1788910	68 k	2119
VSS Monitoring Ethernet trailer	0.0	1	0.0	8	0	1	8	0	1
NetBIOS Name Service	0.1	15	0.0	966	37	15	966	37	15
NetBIOS Datagram Service	0.0	1	0.0	82	3	0	0	0	1
SMB (Server Message Block Protocol)	0.0	1	0.0	119	4	0	0	0	1
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0	1
Microsoft Windows Browser Protocol	0.0	1	0.0	33	1	1	33	1	1
Multicast Domain Name System	2.0	486	1.2	175151	6746	486	175151	6746	486
Dynamic Host Configuration Protocol	0.1	15	0.0	4595	177	15	4595	177	15
Domain Name System	1.6	379	0.2	29530	1137	379	29530	1137	379
Data	0.1	35	0.0	6090	234	35	6090	234	35
Transmission Control Protocol	72.9	17664	3.9	577720	22 k	13383	440896	16 k	17664
Transport Layer Security	17.7	4280	65.4	9704143	373 k	4280	8751125	337 k	4461
Data	0.0	1	0.0	1115	42	1	1115	42	1
Internet Group Management Protocol	0.0	3	0.0	24	0	3	24	0	3
Internet Control Message Protocol	0.2	40	0.0	6640	255	40	6640	255	40
Address Resolution Protocol	11.1	2681	0.5	75068	2891	2681	75068	2891	2681
802.1X Authentication	0.2	56	0.0	3136	120	0	0	0	56
Data	0.2	56	0.0	2912	112	56	2912	112	56

Protocol changes have been reverted.

Help Copy Protocols Close

سوال ۴: ۷۲.۹ درصد مربوط به TCP است

سوال ۵: در این پنجره اطلاعات مربوط به ارتباطات بین مبداء و مقصد نشان داده میشود و ما میتوانیم از فیلترهای مختلف استفاده کنیم و اطلاعات مفیدی کسب کنیم.

Wireshark - Conversations - Wi-Fi: en0

Conversation Settings

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

Copy

Follow Stream...

Graph...

Protocol

- ☐ Bluetooth
- ☐ BPv7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6

Filter list for specific type

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A
00:13:f7:55:24:80	01:00:5e:00:00:01	1	60 bytes	99	1	60 bytes	0
00:13:f7:55:24:80	ff:ff:ff:ff:ff:ff	1	60 bytes	105	1	60 bytes	0
00:28:f8:23:f4:42	33:33:00:00:00:fb	3	306 bytes	39	3	306 bytes	0
04:6c:9d:27:9e:d2	ff:ff:ff:ff:ff:ff	2,570	155 kB	5	2,570	155 kB	0
0a:54:bb:c2:0d:77	01:00:5e:00:00:fb	6	1 kB	54	6	1 kB	0
0a:54:bb:c2:0d:77	33:33:00:00:00:fb	7	1 kB	45	7	1 kB	0
0a:54:bb:c2:0d:77	b2:26:06:67:2f:41	7	2 kB	47	2	172 bytes	5
0a:54:bb:c2:0d:77	ff:ff:ff:ff:ff:ff	10	600 bytes	44	10	600 bytes	0
0c:9a:3c:ab:21:56	33:33:00:00:00:01	1	86 bytes	91	1	86 bytes	0
0c:9a:3c:ab:21:56	33:33:00:00:00:fb	42	4 kB	3	42	4 kB	0
0c:9a:3c:ab:21:56	ff:ff:ff:ff:ff:ff	14	1 kB	70	14	1 kB	0
0c:c6:fd:14:09:47	01:00:5e:00:00:fb	7	3 kB	81	7	3 kB	0
0c:c6:fd:14:09:47	33:33:00:00:00:fb	6	3 kB	82	6	3 kB	0
0c:c6:fd:14:09:47	ff:ff:ff:ff:ff:ff	2	120 bytes	79	2	120 bytes	0
16:23:85:43:4e:7c	33:33:00:00:00:fb	3	683 bytes	108	3	683 bytes	0
16:23:85:43:4e:7c	b2:26:06:67:2f:41	2	506 bytes	111	1	86 bytes	1
16:23:85:43:4e:7c	ff:ff:ff:ff:ff:ff	13	2 kB	107	13	2 kB	0
1e:a2:ca:2d:94:ca	01:00:5e:00:00:fb	6	618 bytes	98	6	618 bytes	0
1e:a2:ca:2d:94:ca	ff:ff:ff:ff:ff:ff	3	180 bytes	64	3	180 bytes	0
2c:33:58:cb:ce:8d	01:00:5e:00:00:fb	2	782 bytes	38	2	782 bytes	0
2c:33:58:cb:ce:8d	ff:ff:ff:ff:ff:ff	4	336 bytes	19	4	336 bytes	0
30:89:4a:d1:85:c1	33:33:00:00:00:fb	3	270 bytes	6	3	270 bytes	0
30:89:4a:d1:85:c1	ff:ff:ff:ff:ff:ff	3	462 bytes	4	3	462 bytes	0
34:02:86:dd:3f:01	ff:ff:ff:ff:ff:ff	1	42 bytes	62	1	42 bytes	0
34:6f:24:e2:c4:27	33:33:00:00:00:fb	2	210 bytes	71	2	210 bytes	0
36:d6:e9:e0:39:10	ff:ff:ff:ff:ff:ff	8	1 kB	90	8	1 kB	0

Help

Close

سوال ۶: میتوانیم همه end point ها را ببینیم.

سوال ۷: TCP را انتخاب میکنیم و مقصدهای TCP را میبینیم.

Wireshark - Endpoints - Wi-Fi: en0

Endpoint Settings

- ☐ Name resolution
- ☐ Limit to display filter

Copy

Map

Protocol

- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP
- ☐ SCTP
- ☐ SLL
- ☒ TCP
- ☐ Token-Ring
- ☐ UDP
- ☐ USB
- ☐ ZigBee

Filter list for specific type

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.10.34.36	443	55	4 kB	0	0 bytes	55	4 kB
13.32.143.59	443	967	903 kB	652	860 kB	315	43 kB
17.36.206.4	443	29	7 kB	12	5 kB	17	2 kB
17.36.206.5	443	18	7 kB	9	5 kB	9	2 kB
18.165.140.120	443	73	21 kB	36	9 kB	37	12 kB
35.241.17.230	443	122	39 kB	64	13 kB	58	25 kB
44.215.128.147	443	72	35 kB	37	22 kB	35	13 kB
44.215.137.64	443	811	636 kB	310	70 kB	501	567 kB
44.215.138.159	443	108	45 kB	51	19 kB	57	26 kB
52.206.58.112	443	200	56 kB	112	23 kB	88	32 kB
64.233.161.84	443	148	55 kB	74	28 kB	74	27 kB
74.125.205.188	5228	37	14 kB	21	10 kB	16	4 kB
79.127.127.35	443	358	313 kB	222	297 kB	136	16 kB
79.127.127.102	443	1,274	1 MB	756	927 kB	518	92 kB
87.248.129.14	443	289	103 kB	144	34 kB	145	69 kB
87.248.129.15	443	147	47 kB	64	24 kB	83	24 kB
87.248.129.18	443	71	25 kB	33	15 kB	38	10 kB
87.248.129.19	443	67	24 kB	31	16 kB	36	8 kB
87.248.129.20	443	125	43 kB	62	15 kB	63	28 kB
98.82.157.231	443	66	31 kB	33	19 kB	33	12 kB
104.16.132.229	443	30	12 kB	15	8 kB	15	4 kB
104.21.10.81	443	59	23 kB	28	15 kB	31	9 kB
108.157.0.98	443	4,759	4 MB	3,144	4 MB	1,615	181 kB
108.157.7.75	443	72	31 kB	36	22 kB	36	9 kB
130.211.29.143	443	151	44 kB	76	24 kB	75	20 kB
140.82.113.26	443	99	35 kB	45	17 kB	54	18 kB
140.82.121.4	443	1,214	996 kB	742	944 kB	472	52 kB

Help

Close

Wireshark · Endpoints · Wi-Fi: en0

Endpoint Settings

☐ Name resolution

☒ Limit to display filter

Copy

Map

Protocol

☐ Bluetooth

☐ BPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☐ IPv4

☐ IPv6

☐ IPX

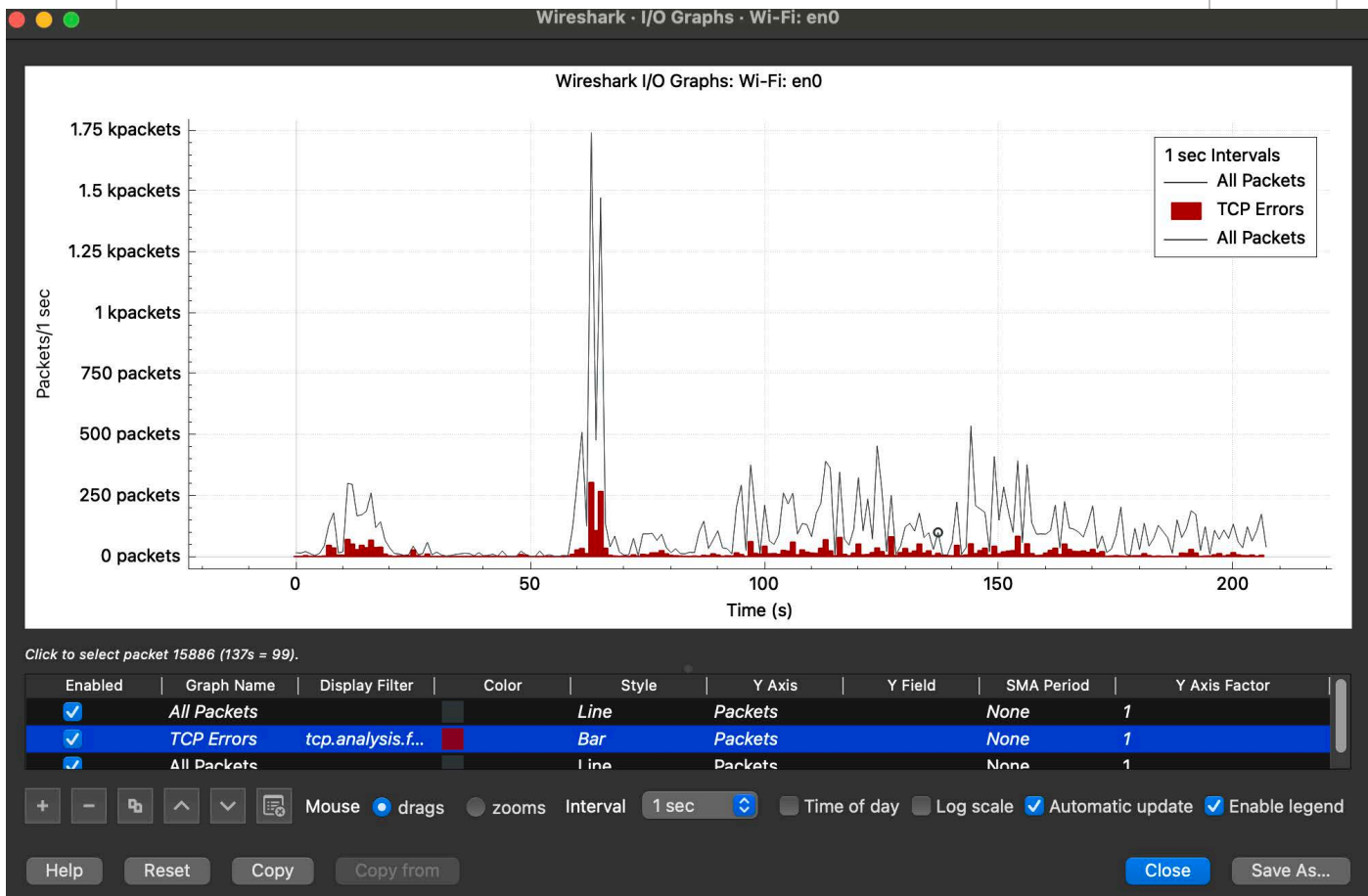
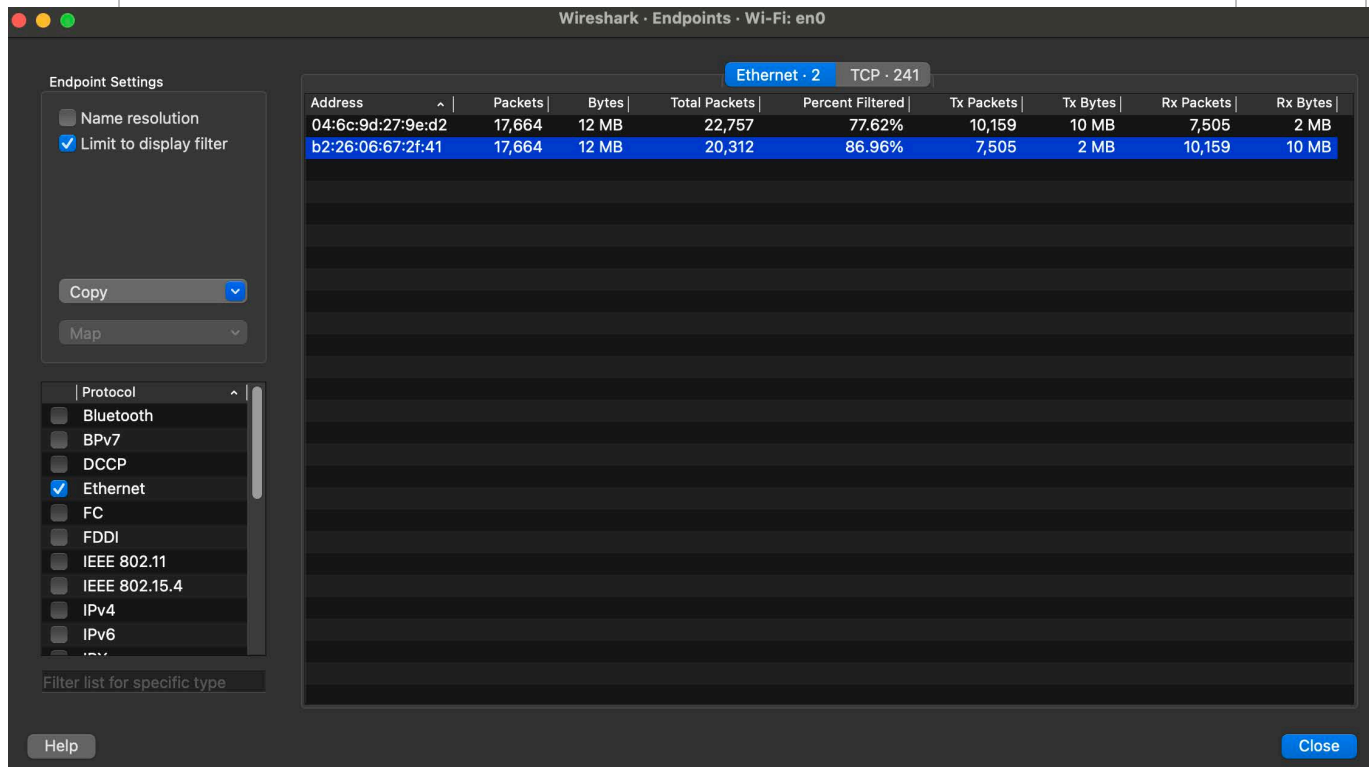
Filter list for specific type

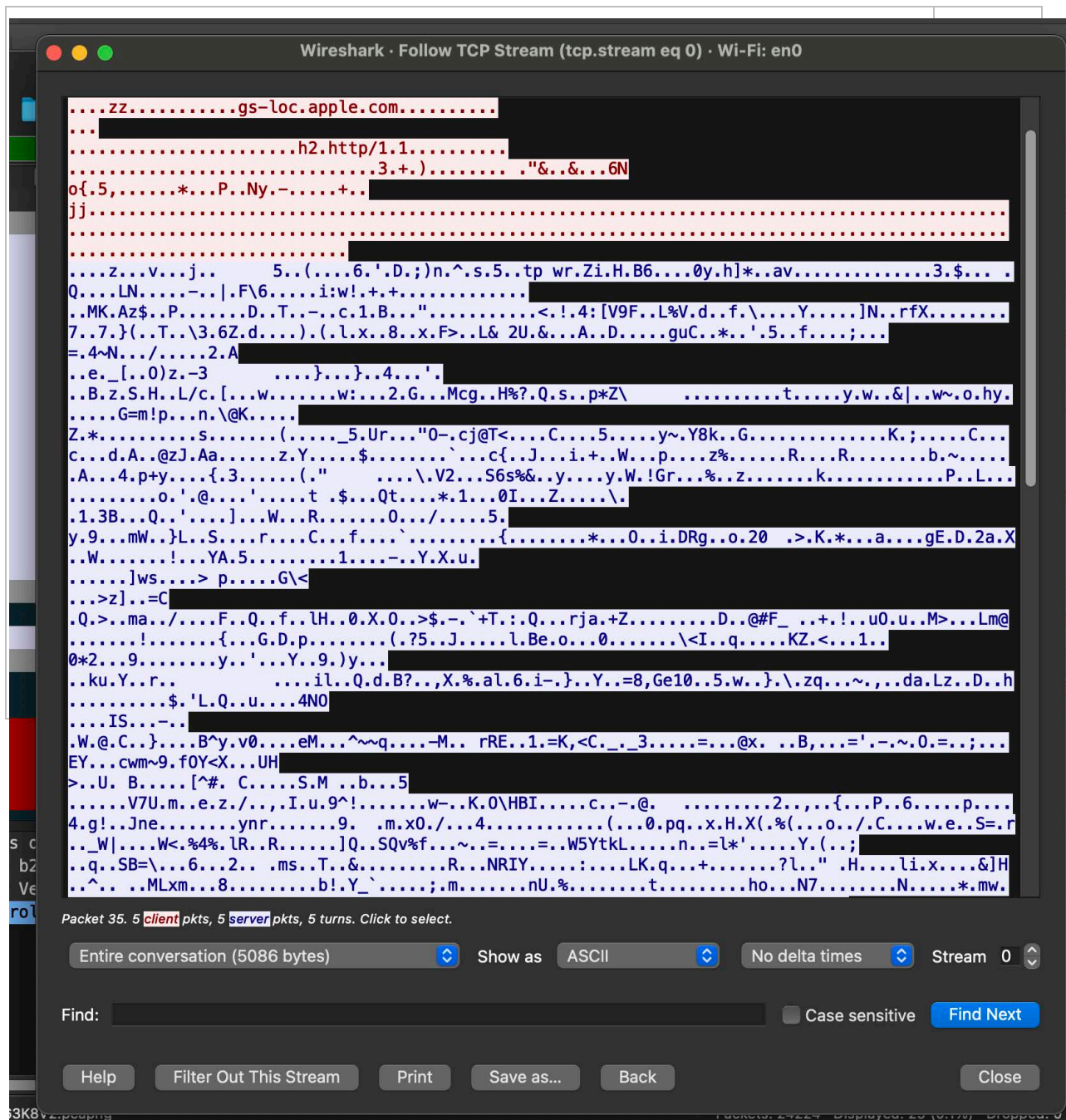
Ethernet · 2TCP · 241

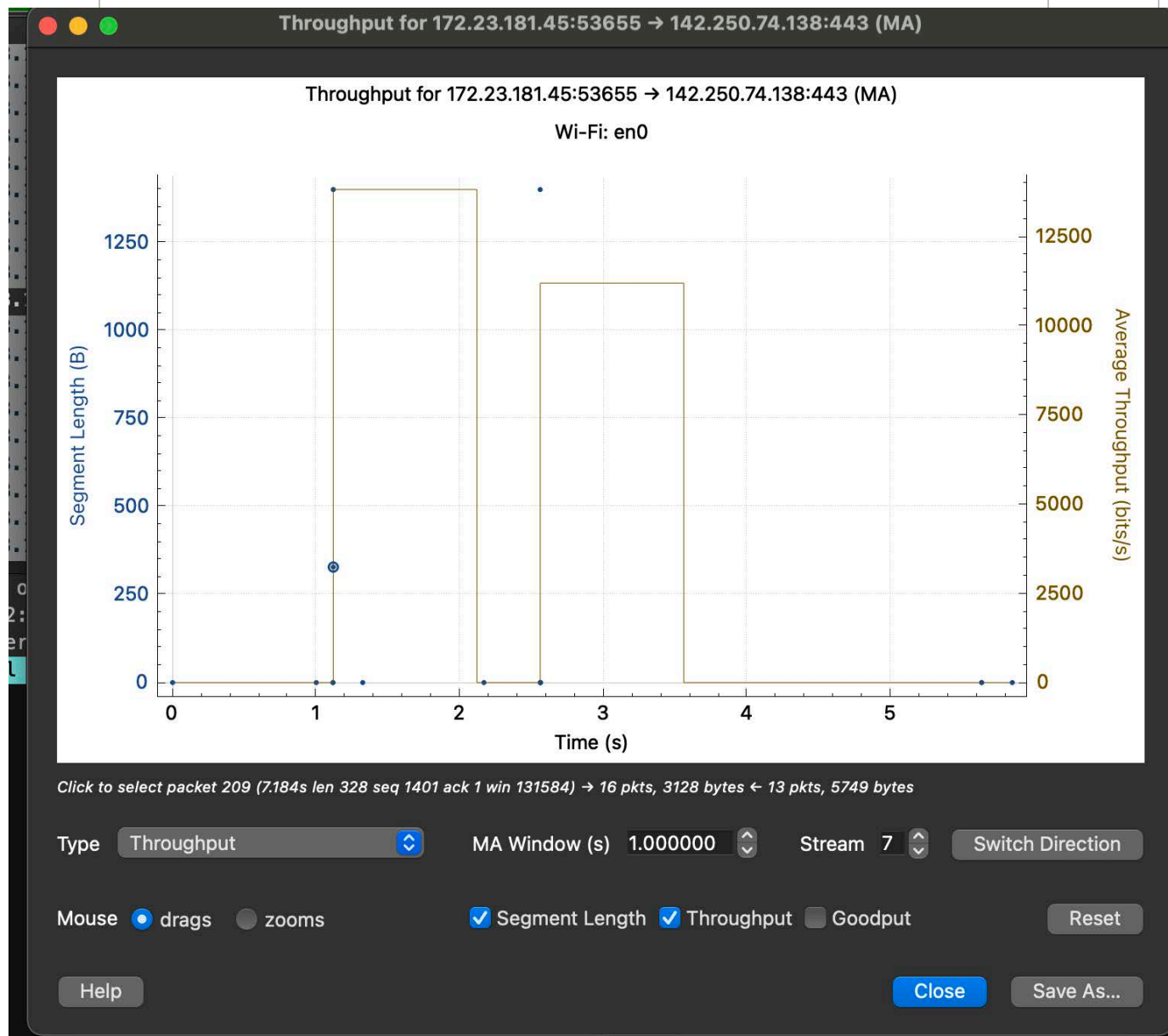
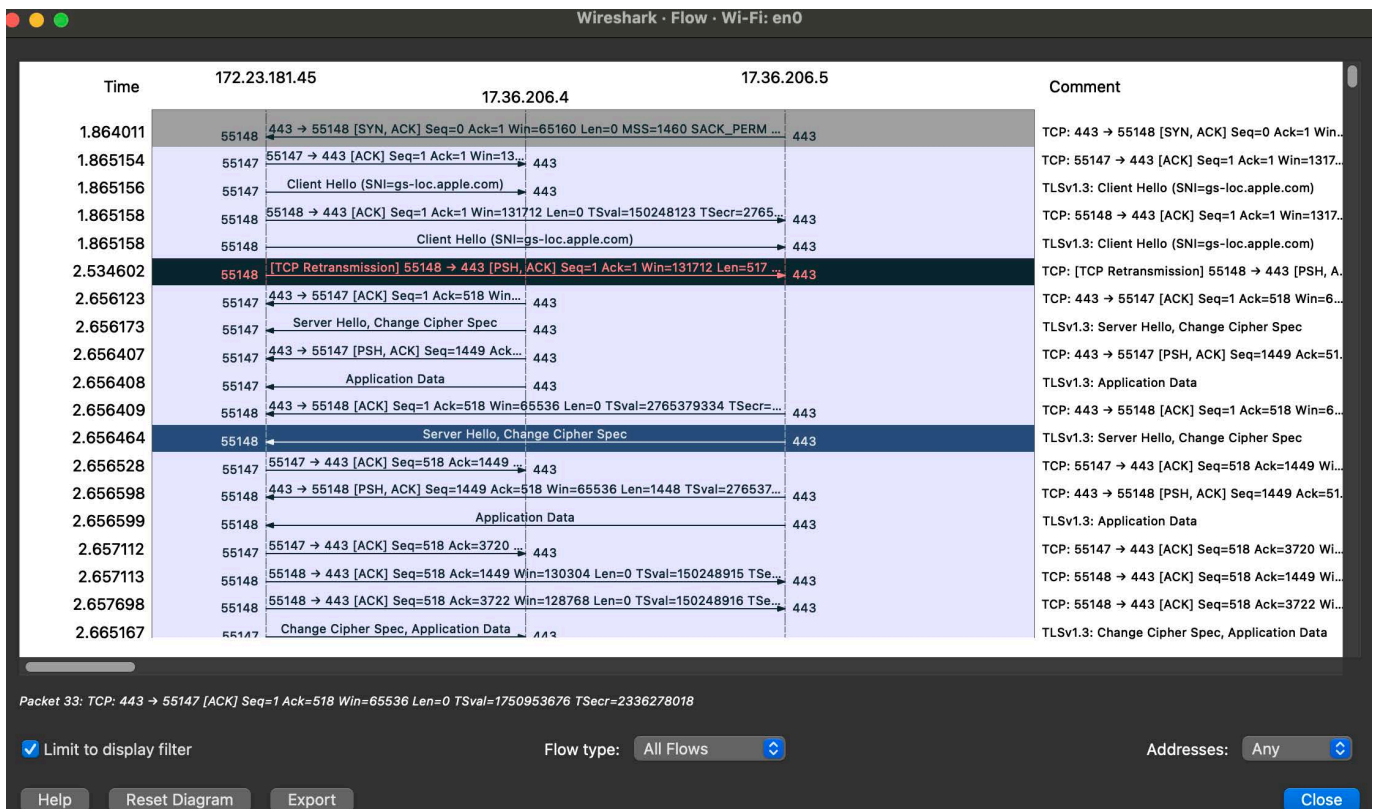
Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
04:6c:9d:27:9e:d2	17,664	12 MB	22,757	77.62%	10,159	10 MB	7,505	2 MB
b2:26:06:67:2f:41	17,664	12 MB	20,312	86.96%	7,505	2 MB	10,159	10 MB

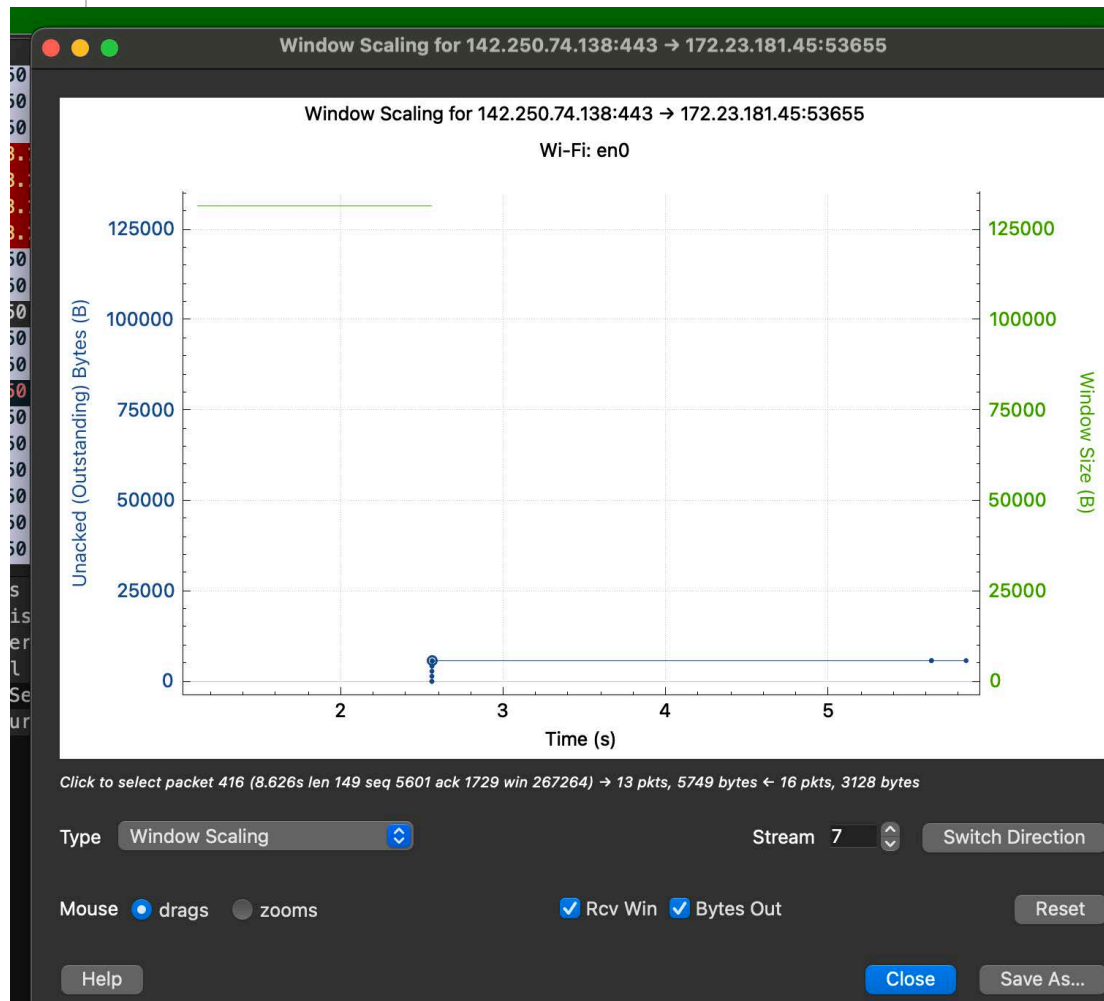
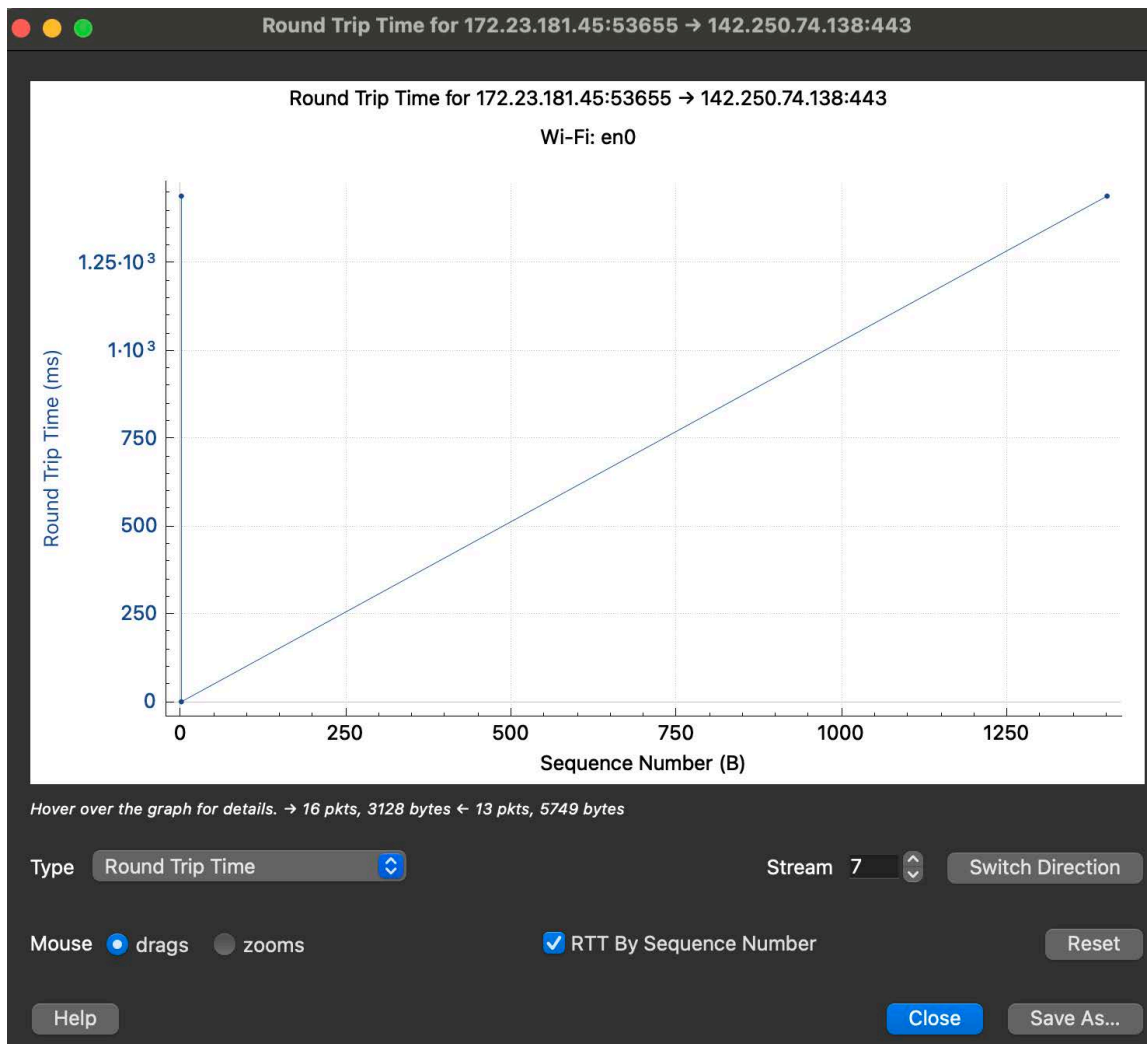
Help

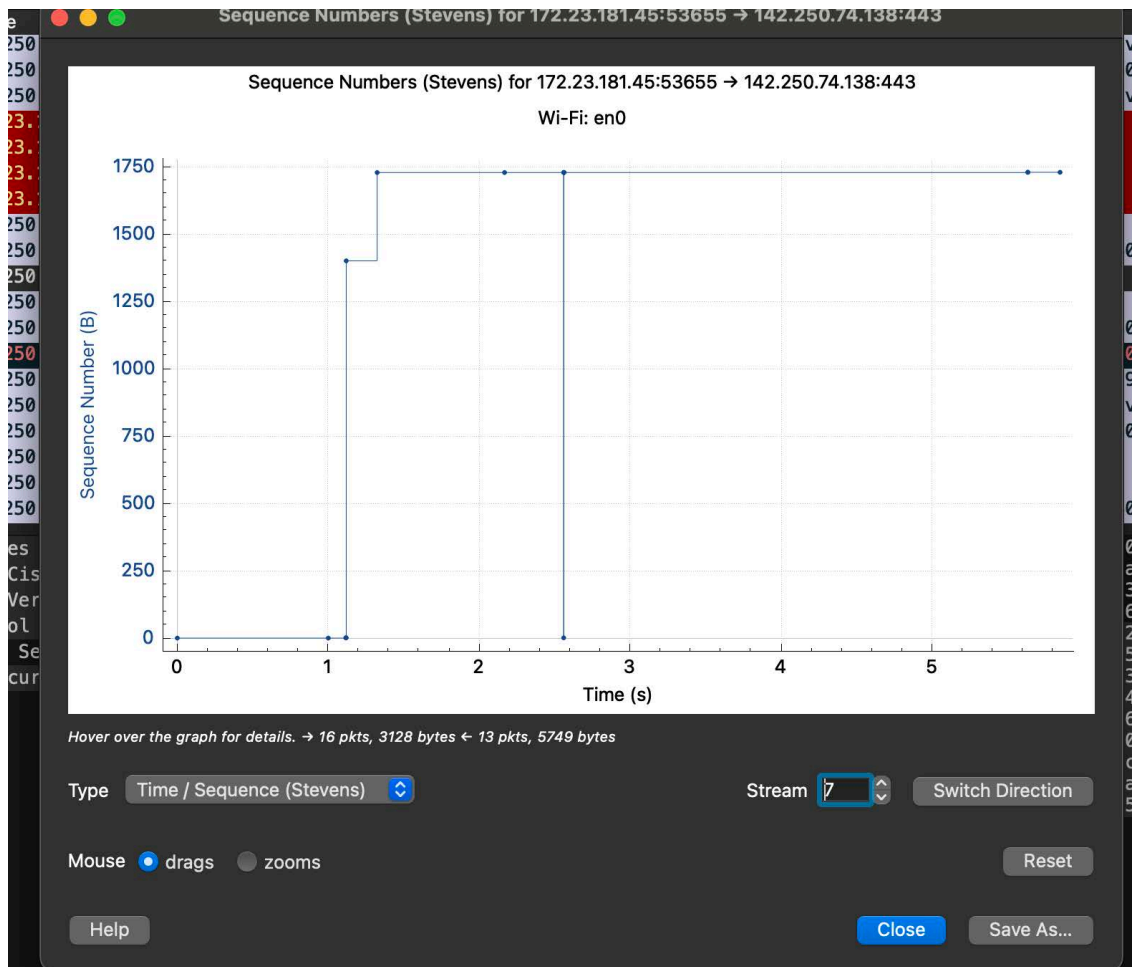
Close











Wireshark - Conversations - Wi-Fi: en0

Conversation Settings

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

Copy

Follow Stream...

Graph...

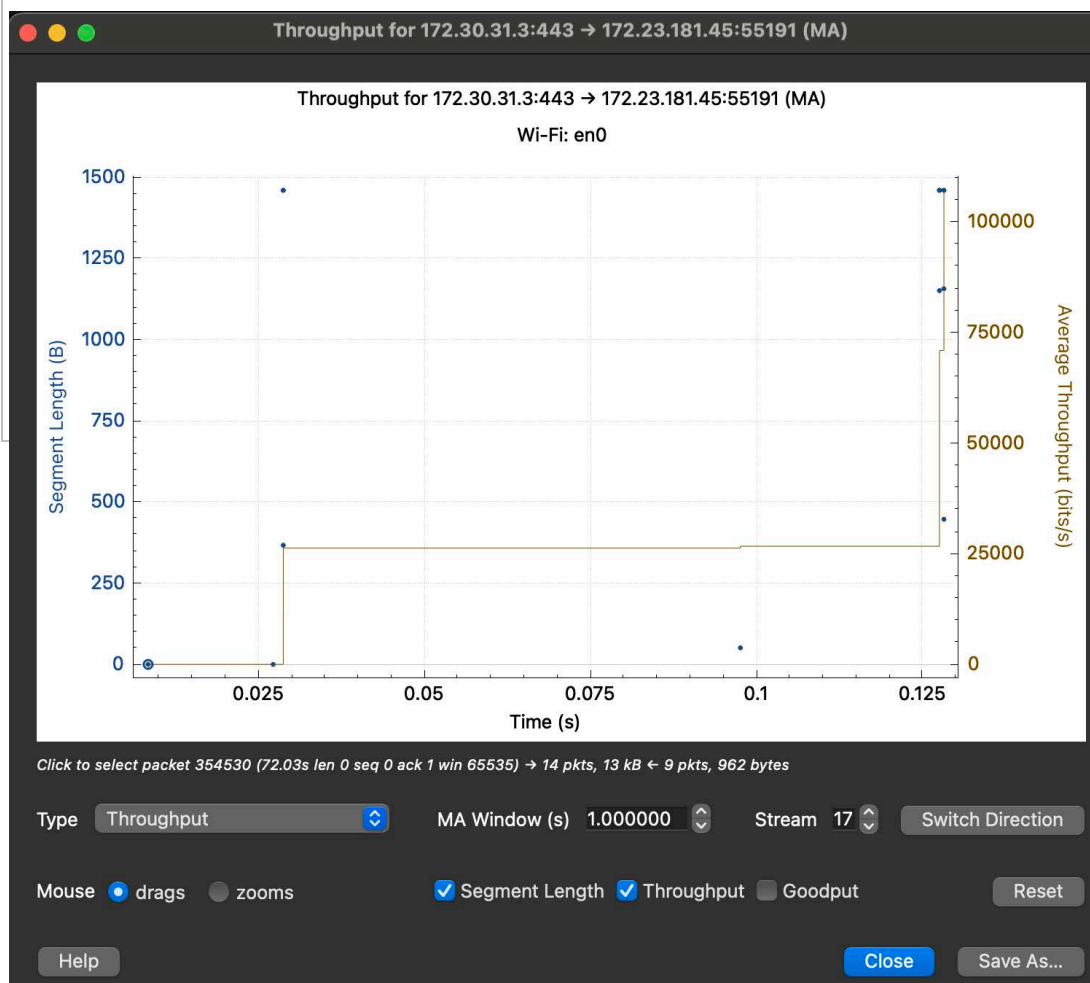
Protocol

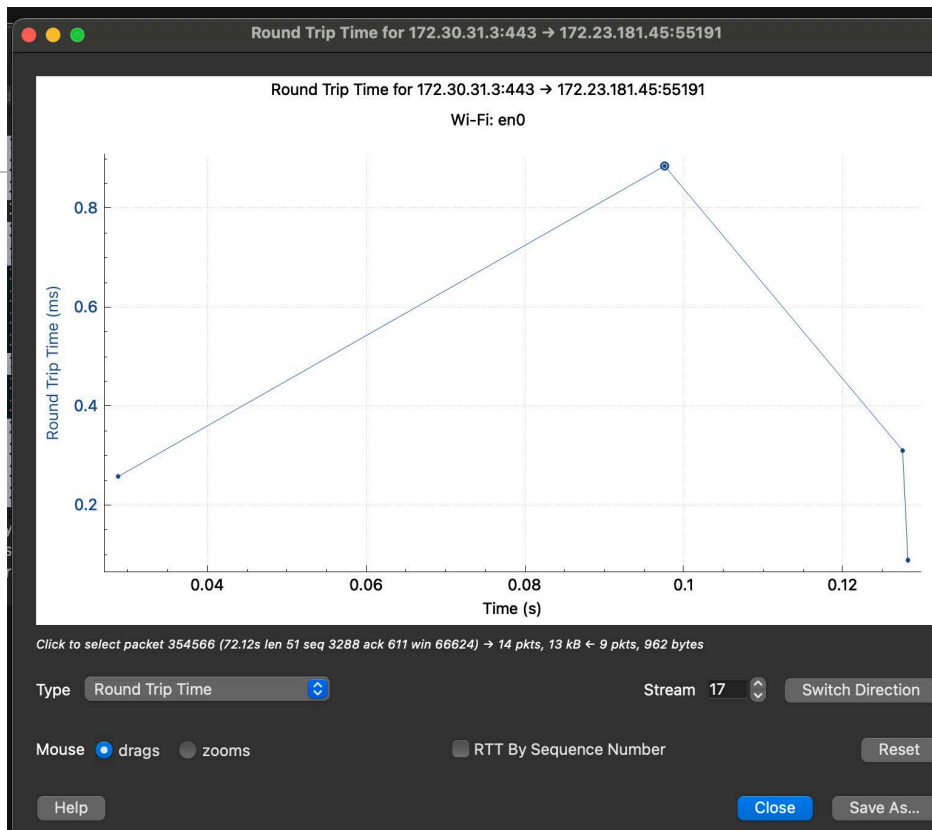
- ☐ Bluetooth
- ☐ BPv7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6

Filter list for specific type

Help Close

Ethernet · 1		IPv4 · 7		IPv6		TCP · 19		UDP	
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packet
172.23.181.45	55177	10.10.34.36	853	10	780 bytes	3	10	100.00%	
172.23.181.45	55178	10.10.34.36	853	10	780 bytes	4	10	100.00%	
172.23.181.45	55179	10.10.34.36	443	10	780 bytes	5	10	100.00%	
172.23.181.45	55180	10.10.34.36	443	10	780 bytes	6	10	100.00%	
172.23.181.45	55186	17.248.209.69	443	1	78 bytes	12	1	100.00%	
172.23.181.45	55187	17.248.209.71	443	33	14 kB	13	33	100.00%	
172.23.181.45	55188	17.248.209.72	443	14	7 kB	14	14	100.00%	
172.23.181.45	55181	17.248.209.73	443	1	78 bytes	7	1	100.00%	
172.23.181.45	55183	17.248.209.73	443	26	10 kB	9	26	100.00%	
172.23.181.45	55184	17.248.209.73	443	27	11 kB	10	27	100.00%	
172.23.181.45	55182	17.248.209.74	443	25	10 kB	8	25	100.00%	
172.23.181.45	55185	17.248.209.74	443	23	10 kB	11	23	100.00%	
172.23.181.45	55172	172.30.31.3	80	2	108 bytes	2	2	100.00%	
172.23.181.45	55189	172.30.31.3	443	20	10 kB	15	20	100.00%	
172.23.181.45	55190	172.30.31.3	443	18	10 kB	16	18	100.00%	
172.23.181.45	55191	172.30.31.3	443	23	16 kB	17	23	100.00%	
172.23.181.45	55192	172.30.31.3	443	26	16 kB	18	26	100.00%	
172.30.31.3	443	172.23.181.45	55176	152,664	176 MB	0	152,664	100.00%	1
172.30.31.3	443	172.23.181.45	55174	197,108	232 MB	1	197,108	100.00%	1





```
Last login: Sun Oct 27 15:48:14 on ttys000
kiyanpourazar@Kiyans-MacBook-Pro ~ % /Applications/Wireshark.app/Contents/MacOS/tshark -D
1. en0 (Wi-Fi)
2. awdl0
3. llw0
4. utun0
5. utun1
6. utun2
7. utun3
8. utun4
9. utun5
10. utun6
11. utun7
12. lo0 (Loopback)
13. ap1
14. en1 (Thunderbolt 1)
15. en2 (Thunderbolt 2)
16. en4 (Thunderbolt 4)
17. en3 (Thunderbolt 3)
18. bridge0 (Thunderbolt Bridge)
19. gif0
20. stf0
21. ciscodump (Cisco remote capture)
22. randpkt (Random packet generator)
23. sshdump (SSH remote capture)
24. udpdump (UDP Listener remote capture)
25. wifidump (Wi-Fi remote capture)
kiyanpourazar@Kiyans-MacBook-Pro ~ %
```

cap

```
> Frame 1: 970 bytes on wire (7760 bits), 970 bytes captured (7760 bits) on 0:00:00.000000
```

نتیجہ گیری