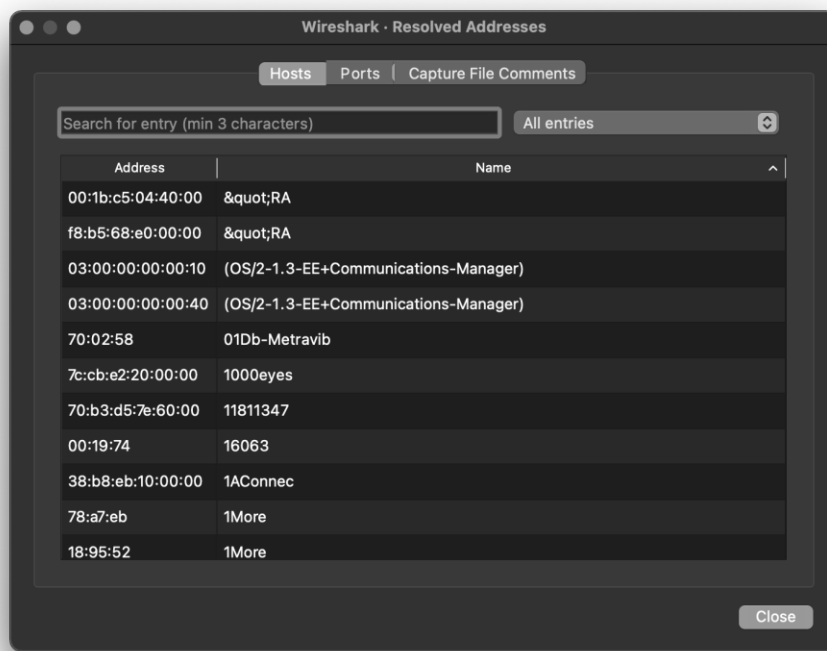
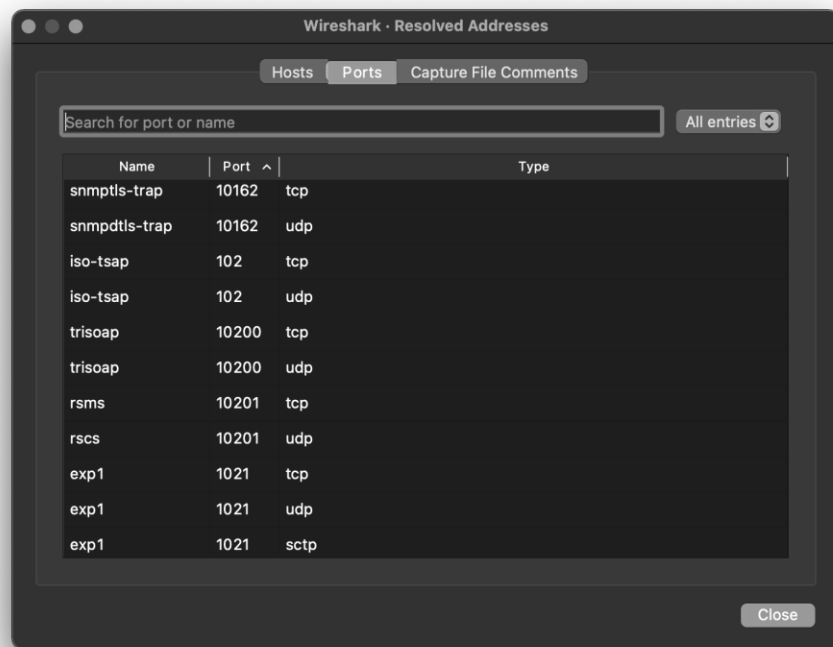


سوال ۱-



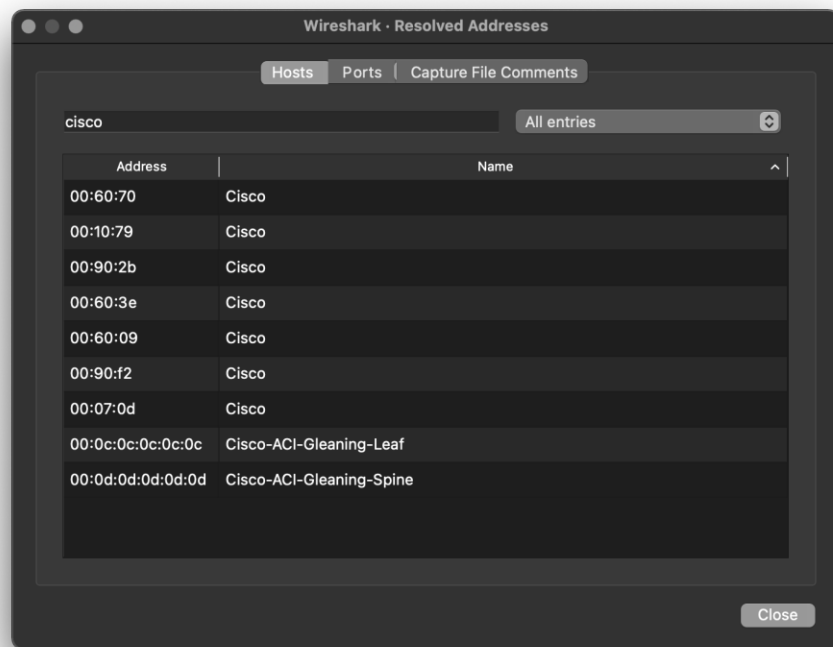
در ستون اول همه آدرس‌هایی که در بسته ما کپی را نمایش می‌دهد و در ستون دوم DNS name متناظر با هر کدام از آنها را به ما می‌دهد .

همچنین در بخش دیگر یعنی port هم به ما نشان می‌دهد که چه port هایی را به چه اسم‌هایی تبدیل می‌کند.



سوال ۲-

Host را انتخاب می‌کنیم و در بخش search cisco را می‌نویسیم و به همین ترتیب ۳ بایت اول را نمایش می‌دهد.



سوال ۳-

The image shows the 'Protocol Hierarchy Statistics' window in Wireshark for the interface 'Wi-Fi: en0'. It displays a tree view of protocols and a corresponding table of statistics.

| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s |
|--------------------------------------|-----------------|---------|---------------|----------|--------|-------------|-----------|------------|
| Frame | 100.0 | 31548 | 100.0 | 14620270 | 320k | 0 | 0 | 0 |
| Ethernet | 100.0 | 31548 | 3.0 | 441672 | 9686 | 0 | 0 | 0 |
| Internet Protocol Version 6 | 0.0 | 13 | 0.0 | 520 | 11 | 0 | 0 | 0 |
| User Datagram Protocol | 0.0 | 12 | 0.0 | 96 | 2 | 0 | 0 | 0 |
| Multicast Domain Name System | 0.0 | 12 | 0.0 | 900 | 19 | 12 | 900 | 19 |
| Internet Control Message Protocol v6 | 0.0 | 1 | 0.0 | 24 | 0 | 1 | 24 | 0 |
| Internet Protocol Version 4 | 99.9 | 31530 | 4.3 | 630648 | 13k | 0 | 0 | 0 |
| User Datagram Protocol | 1.1 | 358 | 0.0 | 2864 | 62 | 0 | 0 | 0 |
| Network Time Protocol | 0.0 | 6 | 0.0 | 288 | 6 | 6 | 288 | 6 |
| Multicast Domain Name System | 0.0 | 12 | 0.0 | 900 | 19 | 12 | 900 | 19 |
| Domain Name System | 1.1 | 340 | 0.2 | 25828 | 566 | 340 | 25828 | 566 |
| Transmission Control Protocol | 98.7 | 31144 | 92.4 | 13515218 | 296k | 21260 | 6028925 | 132k |
| Transport Layer Security | 31.1 | 9801 | 64.1 | 9368721 | 205k | 9712 | 8663443 | 190k |
| Malformed Packet | 0.3 | 105 | 0.0 | 0 | 0 | 105 | 0 | 0 |
| Hypertext Transfer Protocol | 0.0 | 4 | 0.0 | 3627 | 79 | 2 | 691 | 15 |
| Online Certificate Status Protocol | 0.0 | 2 | 0.0 | 2203 | 48 | 2 | 2936 | 64 |
| Data | 0.2 | 63 | 0.5 | 77929 | 1709 | 63 | 77929 | 1709 |
| Internet Group Management Protocol | 0.0 | 12 | 0.0 | 96 | 2 | 12 | 96 | 2 |
| Internet Control Message Protocol | 0.1 | 16 | 0.0 | 576 | 12 | 16 | 576 | 12 |
| Address Resolution Protocol | 0.0 | 5 | 0.0 | 140 | 3 | 5 | 140 | 3 |

ترتیب مراتب protocol را از اولین لایه تا لایه آخر را به ما نشان می‌دهد، همچنین درصد و تعداد بسته‌ها و بایت‌هایی که از این protocol استفاده کرده‌اند را به ما نمایش می‌دهد

سوال ۴-

در اینجا نزدیک به ۸۲٪ به این نوع ارتباط تعلق دارند.

سوال ۵-

Wireshark - Conversations - Wi-Fi: en0

Ethernet II

IPv4 74

IPv6 2

TCP 580

UDP 172

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel. Start | Duration | Blocks A → B | Blocks B → A |
|-------------------|-------------------|---------|-------|---------------|-------------|---------------|-------------|------------|----------|--------------|--------------|
| 01:00:5e:00:00:fb | 3c:22:fb:d3:38:fd | 18 | 1680 | 0 | 0 | 18 | 1680 | 17.161383 | 300.2873 | 0 | 44 |
| 30:a2:20:ef:dd:ae | 3c:22:fb:d3:38:fd | 31,516 | 14M | 15,468 | 12M | 16,048 | 2272k | 0.000000 | 364.7642 | 270k | 49k |
| 30:a2:20:ef:dd:ae | ff:ff:ff:ff:ff:ff | 1 | 42 | 1 | 42 | 0 | 0 | 204.738409 | 0.0000 | — | — |
| 30:a2:20:ef:dd:ae | 33:33:00:00:00:01 | 1 | 78 | 1 | 78 | 0 | 0 | 271.912765 | 0.0000 | — | — |
| 33:33:00:00:00:fb | 3c:22:fb:d3:38:fd | 12 | 1644 | 0 | 0 | 12 | 1644 | 108.786794 | 174.6558 | 0 | 75 |

Name resolution

Limit to display filter

Absolute start time

Conversation Types

Help

Copy

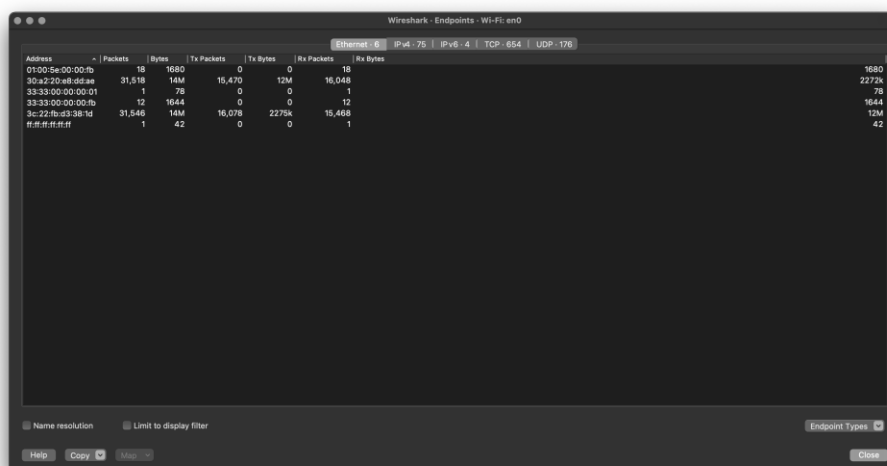
Follow Stream

Analyze

Close

آدرس مبدا و مقصد - بسته‌های مبادله شده بین مبدا و مقصد - نمایش نشست‌ها به ترتیب لایه‌ها - بایت‌های مبادله شده بین مبدا و مقصد - زمان شروع - مدت زمان

سوال ۶-



Wireshark - Endpoints - Wi-Fi: en0

| Ethernet II | | IPv4 75 | | IPv6 4 | | TCP 654 | | UDP 176 | |
|-------------------|---------|---------|------------|----------|------------|----------|--|---------|--|
| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | | | |
| 01:00:5e:00:00:fb | 18 | 1680 | 0 | 0 | 18 | 1680 | | | |
| 30:a2:20:ef:dd:ae | 31,516 | 14M | 15,470 | 12M | 16,048 | 2272k | | | |
| 33:33:00:00:00:01 | 1 | 78 | 0 | 0 | 1 | 78 | | | |
| 33:33:00:00:00:fb | 12 | 1644 | 0 | 0 | 12 | 1644 | | | |
| 3c:22:fb:d3:38:fd | 31,546 | 14M | 16,076 | 2270k | 15,468 | 12M | | | |
| ff:ff:ff:ff:ff:ff | 1 | 42 | 0 | 0 | 1 | 42 | | | |

Buttons: Name resolution, Limit to display filter, Endpoint Types, Help, Copy, Map, Close

نقاط پایانی ترافیک هر پروتکل خاص در یک لایه به خصوص هستند و در اینجا میبینیم که که نقطه‌های پایانی فقط مشخص شده‌اند یعنی مبدا و مقصد را به ما نشان می‌دهند.

سوال ۷-

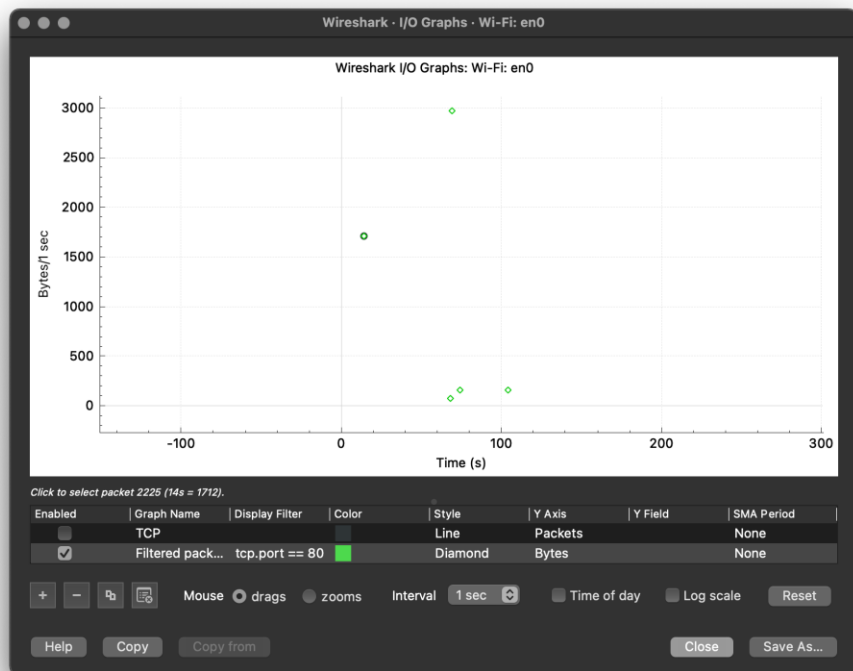
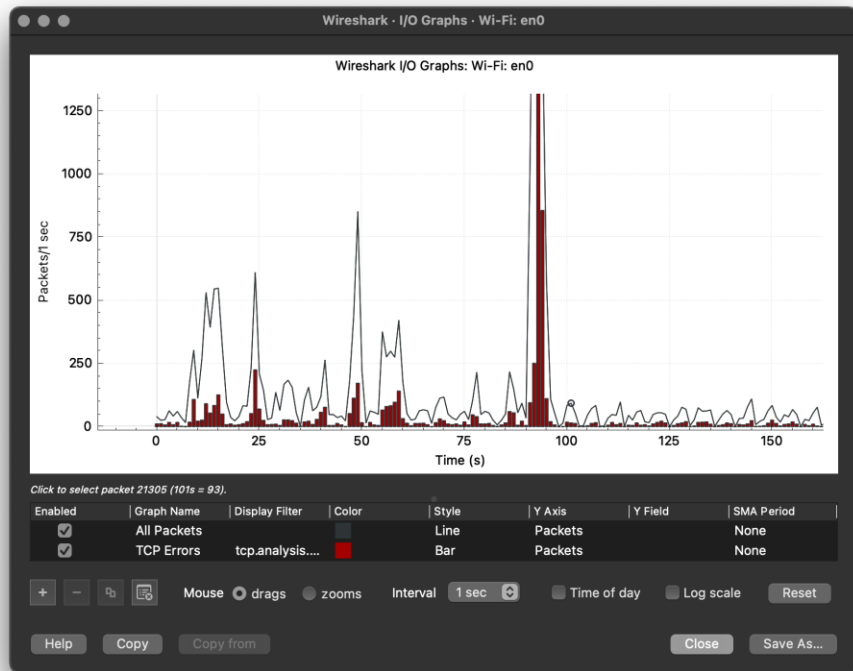
| Address | Port | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|----------------|------|---------|-------|------------|----------|------------|----------|
| 3.223.228.231 | 443 | 59 | 18k | 24 | 8051 | 35 | 10k |
| 13.107.43.14 | 443 | 1,227 | 568k | 584 | 262k | 643 | 309k |
| 1757.12.11 | 443 | 24 | 6573 | 10 | 4307 | 14 | 2266 |
| 1757.146.116 | 5223 | 6 | 2802 | 2 | 156 | 4 | 2646 |
| 17.186.138.30 | 443 | 3 | 206 | 1 | 74 | 2 | 122 |
| 17.188.140.50 | 443 | 30 | 10k | 14 | 8660 | 16 | 1900 |
| 17.248.180.38 | 443 | 238 | 75k | 110 | 43k | 128 | 31k |
| 17.253.38.243 | 443 | 8 | 671 | 3 | 268 | 5 | 405 |
| 17.253.55.201 | 443 | 8 | 552 | 4 | 264 | 4 | 288 |
| 17.253.55.203 | 443 | 8 | 552 | 4 | 264 | 4 | 288 |
| 17.253.55.211 | 443 | 32 | 9606 | 14 | 6746 | 18 | 3099 |
| 17.253.57.209 | 443 | 39 | 9693 | 13 | 6690 | 16 | 2903 |
| 17.253.57.211 | 443 | 61 | 17k | 27 | 12k | 34 | 5165 |
| 17.253.144.10 | 443 | 16 | 1092 | 7 | 486 | 9 | 606 |
| 23.45.74.46 | 443 | 12 | 830 | 5 | 373 | 7 | 457 |
| 23.209.125.20 | 443 | 34 | 11k | 15 | 8548 | 19 | 2458 |
| 23.209.125.22 | 443 | 29 | 10k | 12 | 8162 | 17 | 2290 |
| 35.190.80.1 | 443 | 11,813 | 3679k | 5,684 | 2581k | 6,119 | 793k |
| 45.54.49.1 | 443 | 146 | 41k | 65 | 29k | 81 | 12k |
| 45.54.49.5 | 443 | 69 | 35k | 31 | 31k | 38 | 4243 |
| 52.211.113.33 | 443 | 46 | 17k | 19 | 7462 | 27 | 4392 |
| 54.171.219.200 | 443 | 31 | 10k | 13 | 7365 | 18 | 2834 |
| 54.204.180.26 | 443 | 58 | 15k | 24 | 10k | 34 | 5333 |
| 92.122.249.35 | 443 | 36 | 10k | 17 | 8633 | 19 | 2353 |
| 92.122.252.160 | 443 | 44 | 10k | 21 | 7840 | 23 | 2489 |
| 92.122.253.104 | 443 | 54 | 15k | 26 | 12k | 34 | 3109 |
| 94.162.163.21 | 443 | 26 | 9412 | 11 | 7410 | 15 | 1732 |
| 104.19.98.194 | 443 | 39 | 7023 | 19 | 4716 | 20 | 2308 |
| 104.21.33.132 | 443 | 40 | 6266 | 19 | 3942 | 21 | 2324 |
| 104.226.98.129 | 443 | 32 | 10k | 14 | 7712 | 18 | 2383 |
| 108.174.11.85 | 443 | 47 | 12k | 21 | 9717 | 26 | 7025 |

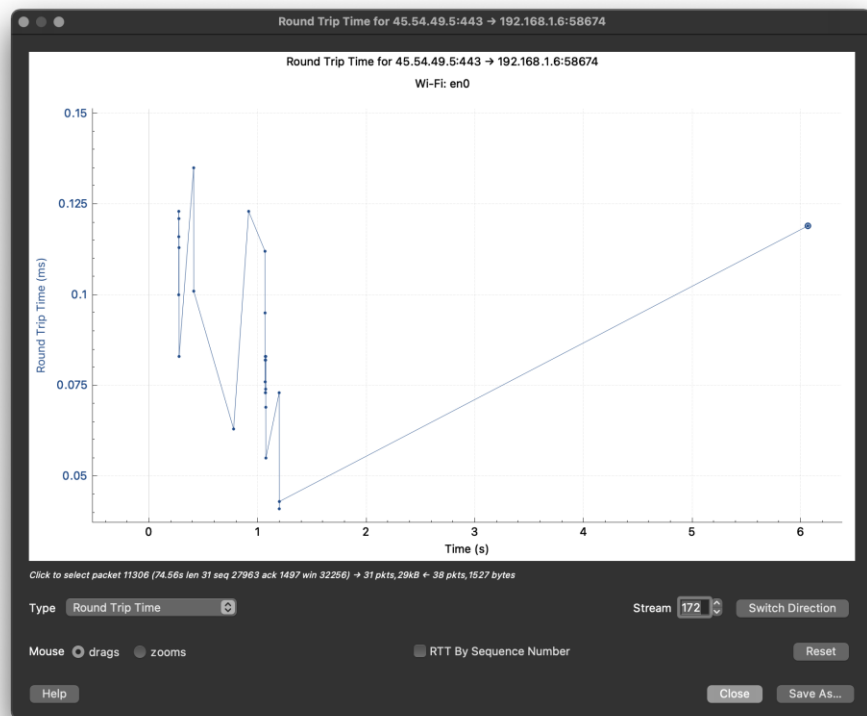
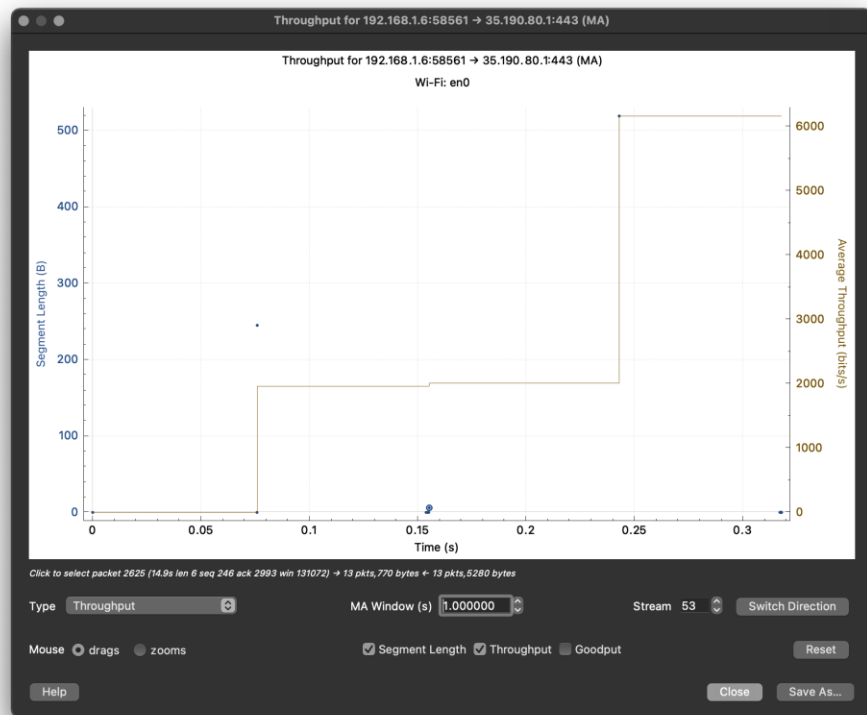
سوال ۸-

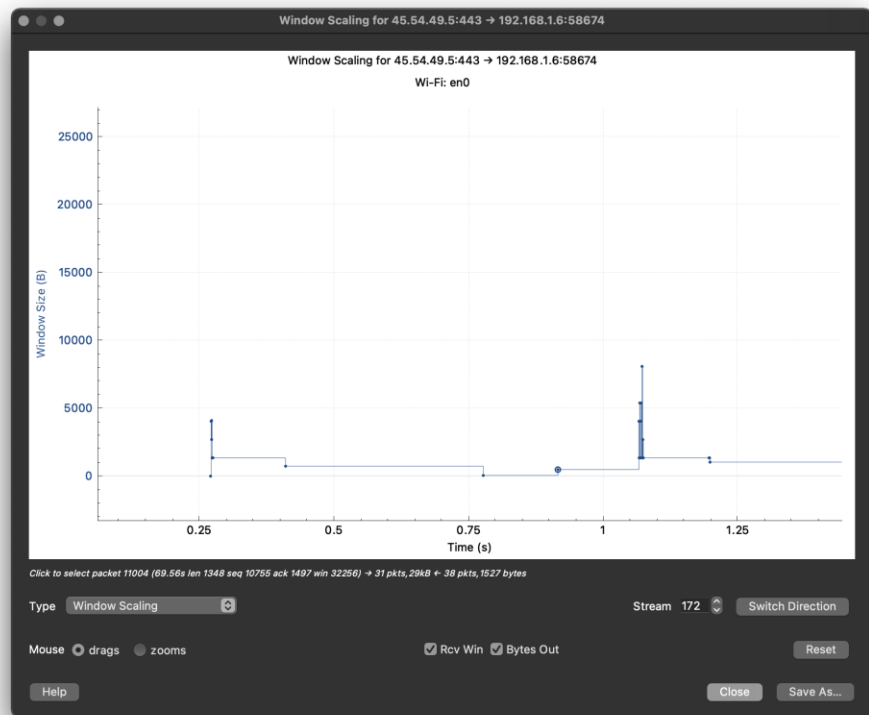
آن که با فلش مشخص شده است.

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|-------------------|---------|-------|------------|----------|------------|----------|
| 0100:5e:00:00:7b | 18 | 1680 | 0 | 0 | 18 | 1680 |
| 30a2:20:eb:dd:ae | 31,518 | 14M | 15,470 | 12M | 16,048 | 2272k |
| 33:33:00:00:00:01 | 1 | 78 | 0 | 0 | 1 | 78 |
| 33:33:00:00:00:7b | 12 | 1644 | 0 | 0 | 12 | 1644 |
| 3c:22:9e:a3:98:1d | 31,846 | 14M | 16,078 | 2275k | 15,468 | 12M |
| ff:ff:ff:ff:ff:ff | 1 | 42 | 0 | 0 | 1 | 42 |

سوال ۹-







به دلیل ازدحام بیش از حد در برخی از نقاط میزان سرعت دانلود بسیار بالا می‌رود و می‌توان آنها را به دست آورد اما در برخی از نقاط سرعت بسیار کاهش پیدا می‌کند و می‌توان گفت در برخی از موارد به صفر میل می‌کند و به همین دلیل می‌توان گفت رفتار آنها به مانند یکدیگر است به این معنا که در فرایند دانلود و توقف همزمانی داریم.