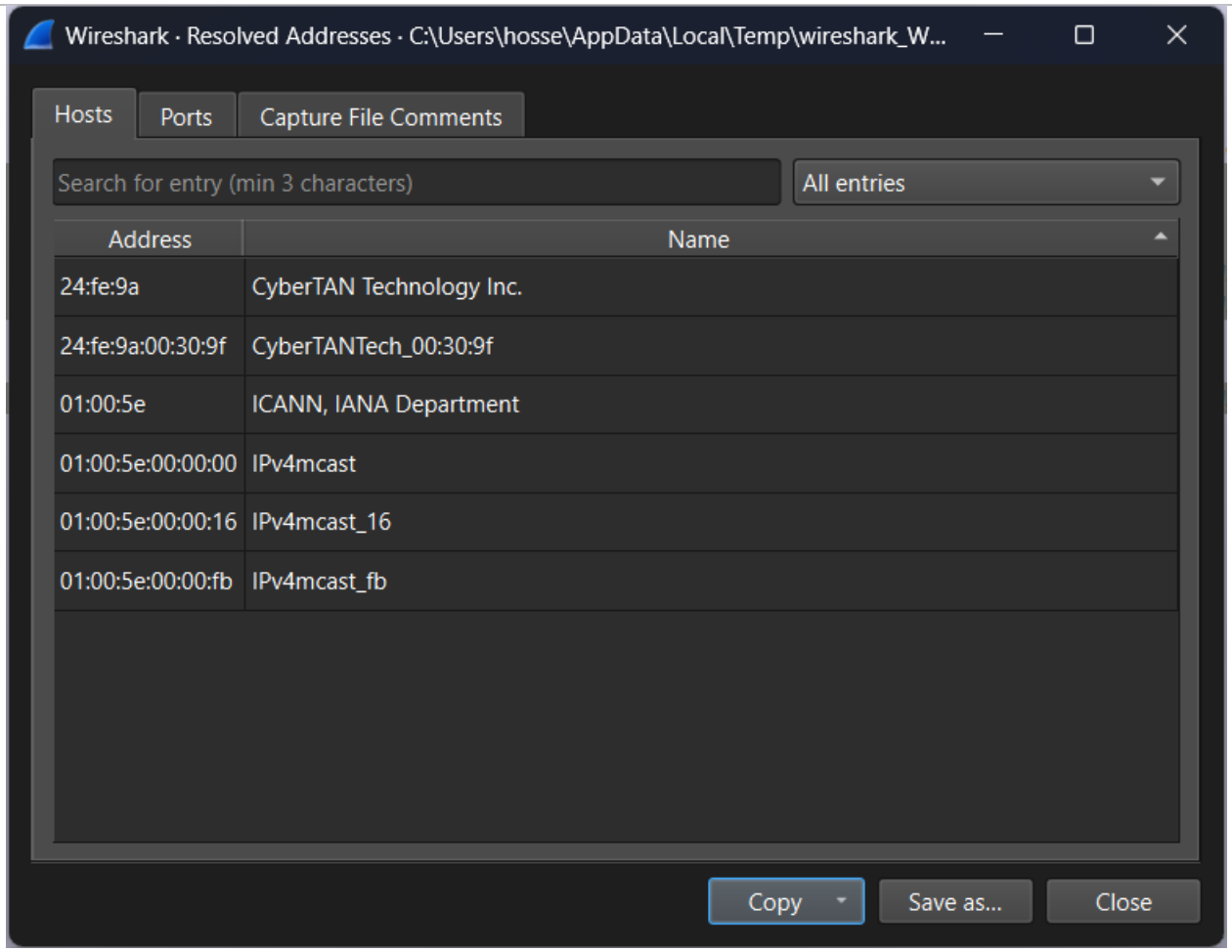
فرم گزارش کار آزمایشگاه شبکه

نام و نام خانوادگی	حسین تاتار	شماره دانشجویی	40133014	نام و شماره آزمایش	8- تحلیل ترافیک TCPو UDPبا استفاده از Wireshark
هدف آزمایش	در این آزمایش قصد داریم آشنایی بیشتری با نرمافزار Wiresharkو منوي Statisticsدر آن پیدا کنیم و از امکانات آن براي تحلیل بستههاي جمع آوري شده استفاده نماییم				
ابزارهای مورد نیاز	دستور کار مربوط به آشنایی Wiresharkرا مرور کنید				
شرح آزمایش	بر روي گزینه ي Resolved Addressesکلیک کنید. **سؤال 1:** در پنجرهاي که باز میشود چه چیزي را مشاهده میکنید؟ **جواب:** در پنجره Resolved Addresses درWireshark ، اطلاعات زیر مشاهده می‌شود: 1. لیست آدرس‌های MAC و نام‌های مرتبط با آن‌ها: ○ این پنجره آدرس‌های فیزیکی (MAC) و نام دستگاه‌ها یا سازنده‌هایی که این آدرس‌ها به آن‌ها اختصاص داده شده‌اند را نمایش می‌دهد. ○ مثال‌های موجود در تصویر: ▪ 24:fe:9a متعلق به شرکت CyberTAN Technology Inc (سازنده تجهیزات شبکه). ▪ 01:00:5e مربوط به ICANN, IANA Department آدرس‌های مالتی‌کست استاندارد.(IPv4) 2. اطلاعات مالتی‌کست(Multicast) : ○ آدرس‌هایی که با 01:00:5e شروع می‌شوند، برای ترافیک‌های مالتی‌کست IPv4 استفاده می‌شوند. ○ مثلاً: ▪ 01:00:5e:00:00:00 با نام IPv4mcast نمایش داده شده است. ▪ 01:00:5e:00:00:fb مربوط به گروه مالتی‌کست خاصی (مثلاً پروتکل‌های مسیریابی). 3. جستجو و فیلتر: ○ امکان جستجو (Search) برای یافتن مدخل‌های خاص وجود دارد (حداقل ۳ کاراکتر نیاز است).				



سؤال 2: آیا میتوانید 3بایت اولی که براي آدرس فیزیکی کارتهاي شبکه Cisco میباشند را مشخص کنید؟

جواب:

در تصویر ارسال‌شده، آدرس‌های مربوط به CyberTAN و مالتی‌کست (01:00:5e) نمایش داده شده‌اند.

بر روي گزینه ي Protocol Hierarchyکلیک کنید.

سؤال 3: در پنجرهاي که باز میشود چه چیزي را مشاهده میکنید؟

جواب:

در پنجره Protocol Hierarchy Statistics درWireshark ، اطلاعات زیر مشاهده می‌شود:

ساختار سلسله‌مراتبی پروتکل‌ها

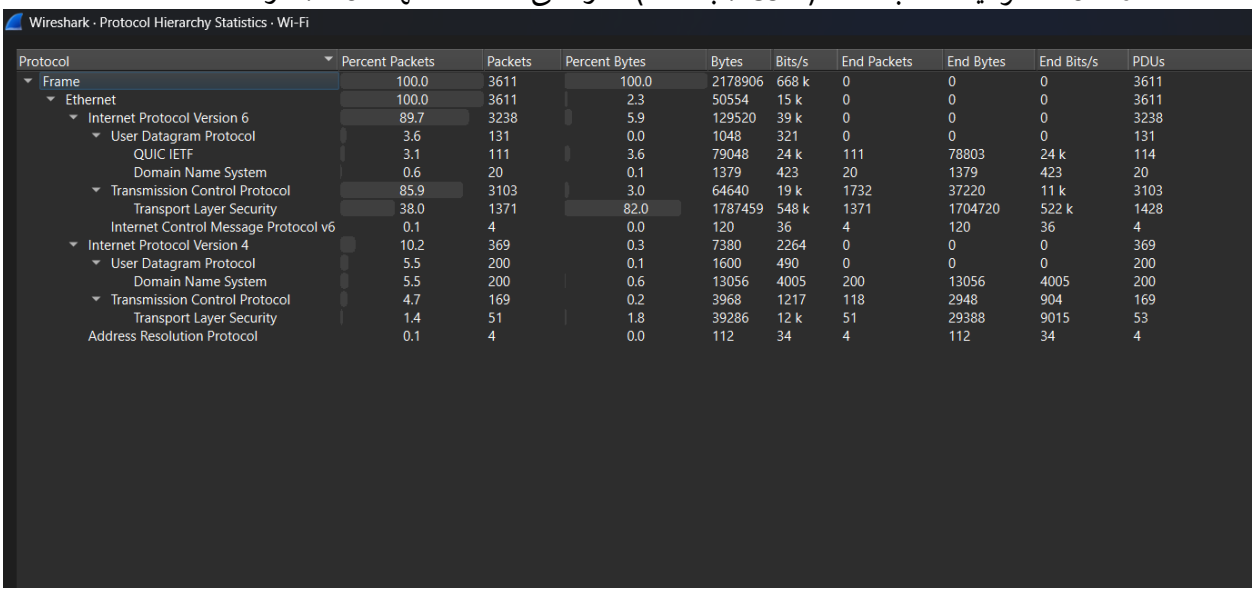
این پنجره ترافیک شبکه را بر اساس پروتکل‌های لایه‌های مختلف (از لایه فیزیکی تا لایه کاربردی) دسته‌بندی می‌کند. هر پروتکل با درصد و حجم ترافیک مرتبط نمایش داده می‌شود.

داده‌های کلیدی در جدول:

- Protocol نام پروتکل: مانندTCP ، UDP، IPv6، DNSو غیره.
- Percent Packets: درصد بسته‌های متعلق به آن پروتکل از کل ترافیک.
- Packets: تعداد مطلق بسته‌های مشاهده‌شده.
- Percent Bytes: درصد حجم داده (بر حسب بایت) متعلق به آن پروتکل.
- Bytes: حجم مطلق داده (بایت).

یافته‌های مهم از تصویر:

- پروتکل‌های غالب:
  - IPv6(89.7% بسته‌ها): نشان‌دهنده استفاده گسترده از این پروتکل در شبکه.
  - TCP(85.9% بسته‌ها): ترافیک اصلی لایه انتقال، عمدتاً برای ارتباطات پایدار (مثل وب‌گردی).
  - TLS(38% بسته‌ها، 82% حجم داده): نشان‌دهنده رمزگذاری ترافیک مثلHTTPS
- پروتکل‌های فرعی:
  - UDP(3.6% بسته‌ها): برای پروتکل‌های سبک‌وزن مانند QUIC مورد استفاده در Google وDNS
  - DNS 0.6%در IPv6 و 5.5% در IPv4: برای تبدیل نام دامنه به آدرسIP
  - ICMPv6 (0.1%): برای مدیریت شبکه IPv6 مثلPing
- مقایسهIPv6 vs IPv4 :
  - IPv6 ترافیک غالب است (89.7% بسته‌ها) ، در حالی که IPv4 تنها 10.2% دارد.


Wireshark · Protocol Hierarchy Statistics · Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	3611	100.0	2178906	668 k	0	0	0	3611
Ethernet	100.0	3611	2.3	50554	15 k	0	0	0	3611
Internet Protocol Version 6	89.7	3238	5.9	129520	39 k	0	0	0	3238
User Datagram Protocol	3.6	131	0.0	1048	321	0	0	0	131
QUIC IETF	3.1	111	3.6	79048	24 k	111	78803	24 k	114
Domain Name System	0.6	20	0.1	1379	423	20	1379	423	20
Transmission Control Protocol	85.9	3103	3.0	64640	19 k	1732	37220	11 k	3103
Transport Layer Security	38.0	1371	82.0	1787459	548 k	1371	1704720	522 k	1428
Internet Control Message Protocol v6	0.1	4	0.0	120	36	4	120	36	4
Internet Protocol Version 4	10.2	369	0.3	7380	2264	0	0	0	369
User Datagram Protocol	5.5	200	0.1	1600	490	0	0	0	200
Domain Name System	5.5	200	0.6	13056	4005	200	13056	4005	200
Transmission Control Protocol	4.7	169	0.2	3968	1217	118	2948	904	169
Transport Layer Security	1.4	51	1.8	39286	12 k	51	29388	9015	53
Address Resolution Protocol	0.1	4	0.0	112	34	4	112	34	4

سؤال 4: چند درصد بسته هاي شما به يک ارتباط TCPبر روي بستر IPv4 تعلق دارند؟

جواب:

این مقدار با عدد ۴.۷٪ در ستون "Percent Packets"مقابل پروتکل TCPزیر IPv4 در جدول مشاهده میشود.
در مقابل، TCPروی IPv6 سهم بسیار بالاتری دارد (۸۵.۹٪)، که نشان‌دهنده اولویت شبکه شما برای استفاده از IPv6 است.

بر روي گزينه ي Conversationsکليک کنيد.

سؤال 5: در پنجرهاي که باز ميشود چه چيزي را مشاهده ميکنيد؟

جواب:

تعریف پنجره Conversations :

این پنجره مکالمات شبکه (ترافیک بین جفت دستگاه‌ها) را بر اساس پروتکل‌های مختلف مانندEthernet ، IPv4، IPv6، TCP، UDP و غیره دسته‌بندی و تحلیل می‌کند. هر ردیف نشان‌دهنده یک ارتباط مجزا بین دو آدرس (مثلاً دو دستگاه یا یک دستگاه و یک سرویس) است .

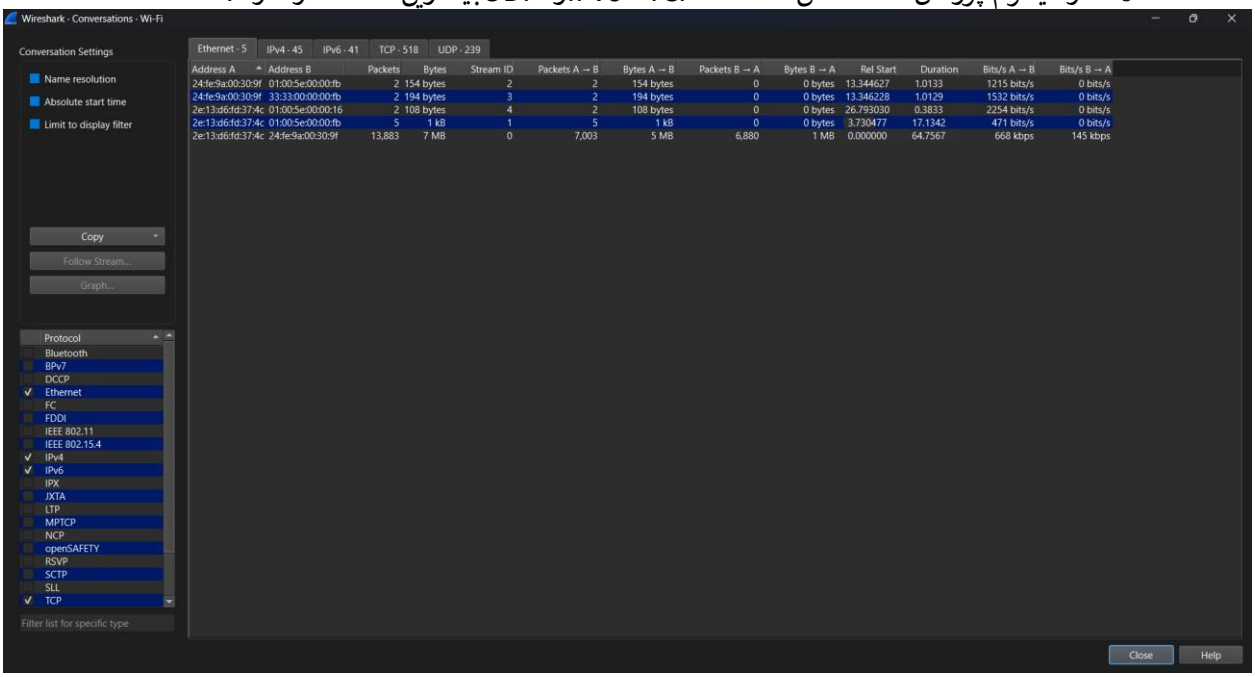
داده‌های کلیدی در جدول:

- Address A وAddress B : آدرس‌های مبدأ و مقصدMAC ، IPیا پورت.
- Packets: تعداد کل بسته‌های مبادله‌شده بین دو آدرس.
- Bytes: حجم کل داده (بر حسب بایت).
- Stream ID: شناسه جریان برای پروتکل‌های مانندTCP .

- مقادیر A→B وB→A : جهت ترافیک (ارسال/دریافت) و حجم آن.
- Duration: مدت زمان ارتباط.
- Bitrate: نرخ انتقال داده بر حسبbps

یافته‌های مهم از تصویر :

- ترافیک غالب:
  - یک ارتباط با حجم بالا بین آدرس‌های 26F35dK0E32Ac و 24Fx9dK0D3f8f وجود دارد:
    - ۱۳۸۸۳ بسته با حجم ۷ مگابایت.
    - نرخ انتقال :۶۶۴ کیلوبیت بر ثانیه (A→B) و ۱۴۵ کیلوبیت بر ثانیه.(B→A)
- ترافیک‌های کوچک:
  - چندین ارتباط کوتاه با حجم کم (مثلاً ۱۵۴ بایت، ۱۹۴ بایت) که ممکن است مربوط به پروتکل‌های مدیریتی مثلARP ، ICMP یا درخواست‌های DNS باشند.
- پروتکل‌های شناسایی‌شده:
  - از دیاگرام پروتکل‌ها مشخص است که TCP، IPv6وUDP بیشترین استفاده را دارند.



یک نشست TCPو UDPرا مشخص کنید. (براي مشخص کردن یک نشست TCPو UDPنیاز است که آدرس و پورت مبدأ و مقصد را مشخص کنید).

بر روي گزينه endpointsکليک کنيد.

سؤال 6: در پنجرهاي که باز ميشود چه چيزي را مشاهده ميکنيد؟

جواب:

تعریف پنجره Endpoints

این پنجره لیست تمام نقاط پایانی (Endpoints) فعال در شبکه را نمایش می‌دهد. هر Endpoint می‌تواند شامل:

- آدرس MAC مثل 24h9d8a0d0d0fa
- آدرس IP مثل IPv4 یا IPv6
- پورت‌های TCP/UDP باشد.

داده‌های کلیدی در جدول:

- **Address**: آدرس فیزیکی (MAC) یاIP.
- Packets: تعداد کل بسته‌های ارسال/دریافت شده.

- Bytes: حجم کل داده مبادله شده
- To Packets/Bytes: ترافیک ارسالی از اینEndpoint
- From Packets/Bytes: ترافیک دریافتی توسط اینEndpoint

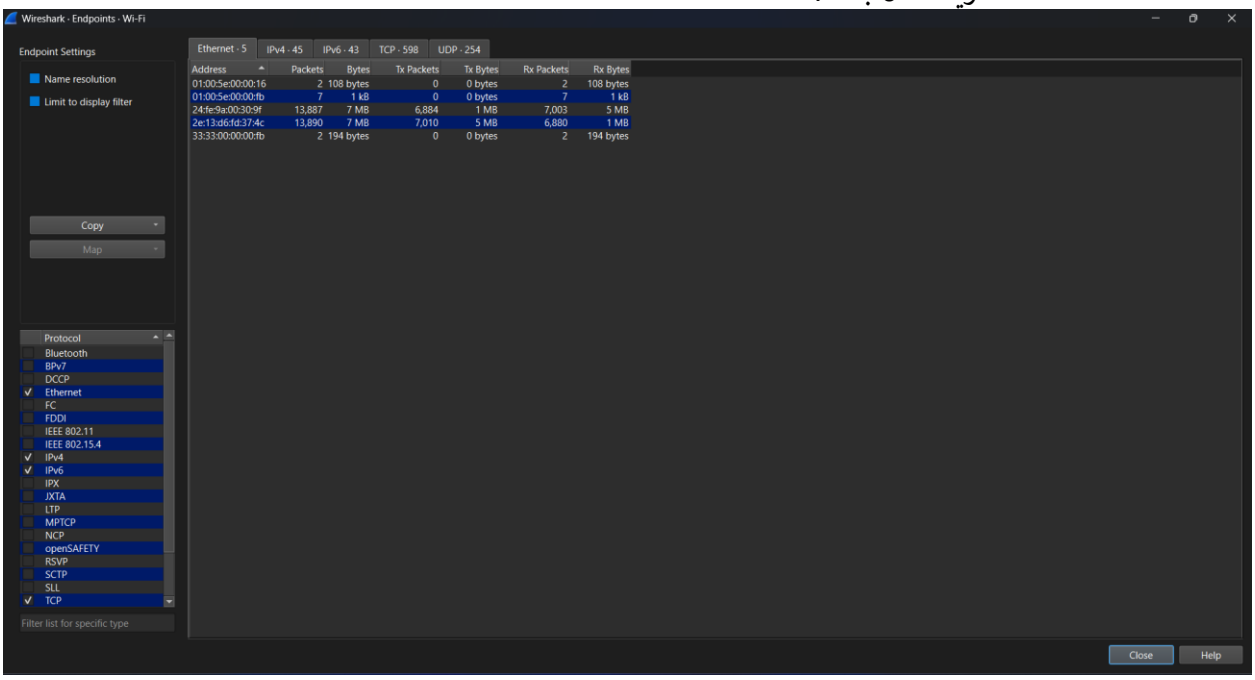
نمونه‌های مشخص از نشست‌های TCP وUDP

الف) نشست TCP پروتکل اتصال‌گرا:

- Endpoint نمونه:
  - آدرس 2e12d6fd4274c : احتمالاً یک دستگاه یا سرور
  - ترافیک:
    - ارسال: 7010 بسته به حجم5 MB
    - دریافت: 6880 بسته به حجم1 MB

ب) نشست UDP پروتکل بی‌اتصال:

- Endpoint نمونه:
  - آدرس 0100-3e20b00fb : مالتی‌کستIPv4
  - ترافیک:
    - ارسال: 7بسته به حجم1 MB
    - دریافت: 0 بسته.

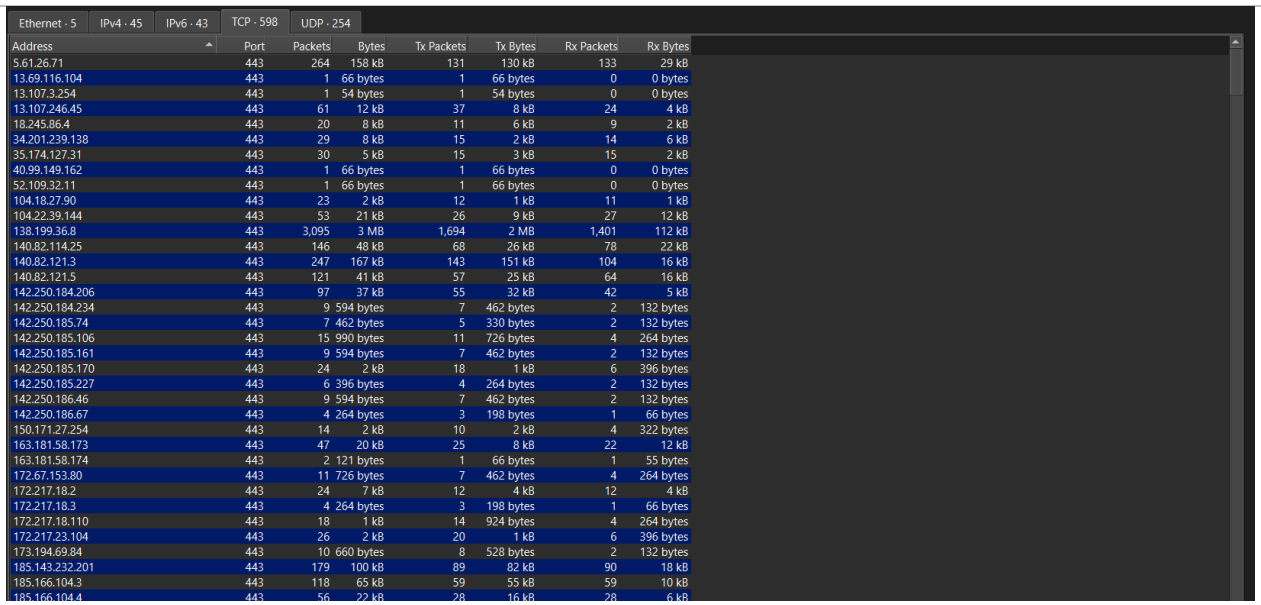


سؤال 7: چه مقصدهایی برای ارتباطهای TCPدر سیستم شما استفادهشده است؟

جواب:

لیست مهم‌ترین مقصدهای TCP بر اساس IP و حجم ترافیک:

توضیحات	حجم کل داده(BYTES)	پورت	آدرس IP مقصد
Microsoftیا GitHub	167 MB	443	140.82.121.3
GitHub	48 MB	443	140.82.114.25
سرویس‌های ابری مثل AWS یا Azure	100 MB	443	165.143.232.201
Google مثلاً YouTube یا Gmail	37 MB	443	142.250.184.206
سرویس‌های رسانه‌ای یا دانلود	21 MB	443	104.232.91.44
سرورهای اروپایی مثلاً هاستینگ یا CDN	158 MB	443	5.61.26.71


Ethernet · 5 | IPv4 · 45 | IPv6 · 43 | TCP · 598 | UDP · 254

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
5.61.26.71	443	264	158 kB	131	130 kB	133	29 kB
13.69.116.104	443	1	66 bytes	1	66 bytes	0	0 bytes
13.107.3.254	443	1	54 bytes	1	54 bytes	0	0 bytes
13.107.246.45	443	61	12 kB	37	8 kB	24	4 kB
18.245.86.4	443	20	8 kB	11	6 kB	9	2 kB
34.201.239.138	443	29	8 kB	15	2 kB	14	6 kB
35.174.127.31	443	30	5 kB	15	3 kB	15	2 kB
40.99.149.162	443	1	66 bytes	1	66 bytes	0	0 bytes
52.109.32.11	443	1	66 bytes	1	66 bytes	0	0 bytes
104.18.27.90	443	23	2 kB	12	1 kB	11	1 kB
104.22.39.144	443	53	21 kB	26	9 kB	27	12 kB
138.199.36.8	443	3,095	3 MB	1,694	2 MB	1,401	112 kB
140.82.114.25	443	146	48 kB	68	26 kB	78	22 kB
140.82.121.3	443	247	167 kB	143	151 kB	104	16 kB
140.82.121.5	443	121	41 kB	57	25 kB	64	16 kB
142.250.184.206	443	97	37 kB	55	32 kB	42	5 kB
142.250.184.234	443	9	594 bytes	7	462 bytes	2	132 bytes
142.250.185.74	443	7	462 bytes	5	330 bytes	2	132 bytes
142.250.185.106	443	15	990 bytes	11	726 bytes	4	264 bytes
142.250.185.161	443	9	594 bytes	7	462 bytes	2	132 bytes
142.250.185.170	443	24	2 kB	18	1 kB	6	396 bytes
142.250.185.227	443	6	396 bytes	4	264 bytes	2	132 bytes
142.250.186.46	443	9	594 bytes	7	462 bytes	2	132 bytes
142.250.186.67	443	4	264 bytes	3	198 bytes	1	66 bytes
150.171.27.254	443	14	2 kB	10	2 kB	4	322 bytes
163.181.58.173	443	47	20 kB	25	8 kB	22	12 kB
163.181.58.174	443	2	121 bytes	1	66 bytes	1	55 bytes
172.67.153.80	443	11	726 bytes	7	462 bytes	4	264 bytes
172.217.18.2	443	24	7 kB	12	4 kB	12	4 kB
172.217.18.3	443	4	264 bytes	3	198 bytes	1	66 bytes
172.217.18.110	443	18	1 kB	14	924 bytes	4	264 bytes
172.217.23.104	443	26	2 kB	20	1 kB	6	396 bytes
173.194.69.84	443	10	660 bytes	8	528 bytes	2	132 bytes
185.143.232.201	443	179	100 kB	89	82 kB	90	18 kB
185.166.104.3	443	118	65 kB	59	55 kB	59	10 kB
185.166.104.4	443	56	22 kB	28	16 kB	28	6 kB

سؤال 8: از قسمت Ethernet و از روي تعداد بسته هاي مبادله شده، Default Gateway شبکه خود را تشخیص دهید.

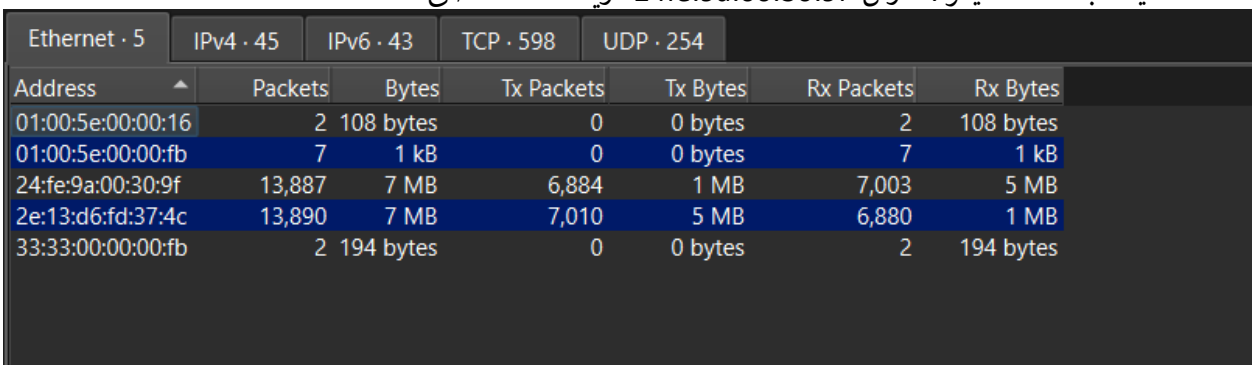
جواب:

برای تشخیص Default Gatewayشبکه از طریق داده‌های Ethernet درWireshark ، باید به دنبال دستگاهی باشید که:

1. بیشترین ترافیک دوطرفه (ارسال و دریافت) را دارد.
2. الگوی آن نشان‌دهنده نقش روتر/گیت‌وی باشد (یعنی هم با دستگاه‌های محلی و هم با اینترنت ارتباط برقرار کند).

2e:13:d6:fd:37:4c گیت‌وی ما است. به دلیل:

- حجم بالای ترافیک ارسالی (5 MB) : نشان‌دهنده نقش مسیریابی ارسال داده به اینترنت یا شبکه‌های دیگر.
- توازن ترافیک : معمولاً گیت‌وی‌ها هم ترافیک ورودی و هم خروجی قابل‌توجهی دارند، اما در اینجا ارسال غالب است.
- مقایسه با دستگاه دیگر : آدرس 24fe:9a:00:30:9f دریافت‌کننده اصلی است .


Ethernet · 5 | IPv4 · 45 | IPv6 · 43 | TCP · 598 | UDP · 254

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:16	2	108 bytes	0	0 bytes	2	108 bytes
01:00:5e:00:00:fb	7	1 kB	0	0 bytes	7	1 kB
24:fe:9a:00:30:9f	13,887	7 MB	6,884	1 MB	7,003	5 MB
2e:13:d6:fd:37:4c	13,890	7 MB	7,010	5 MB	6,880	1 MB
33:33:00:00:00:fb	2	194 bytes	0	0 bytes	2	194 bytes

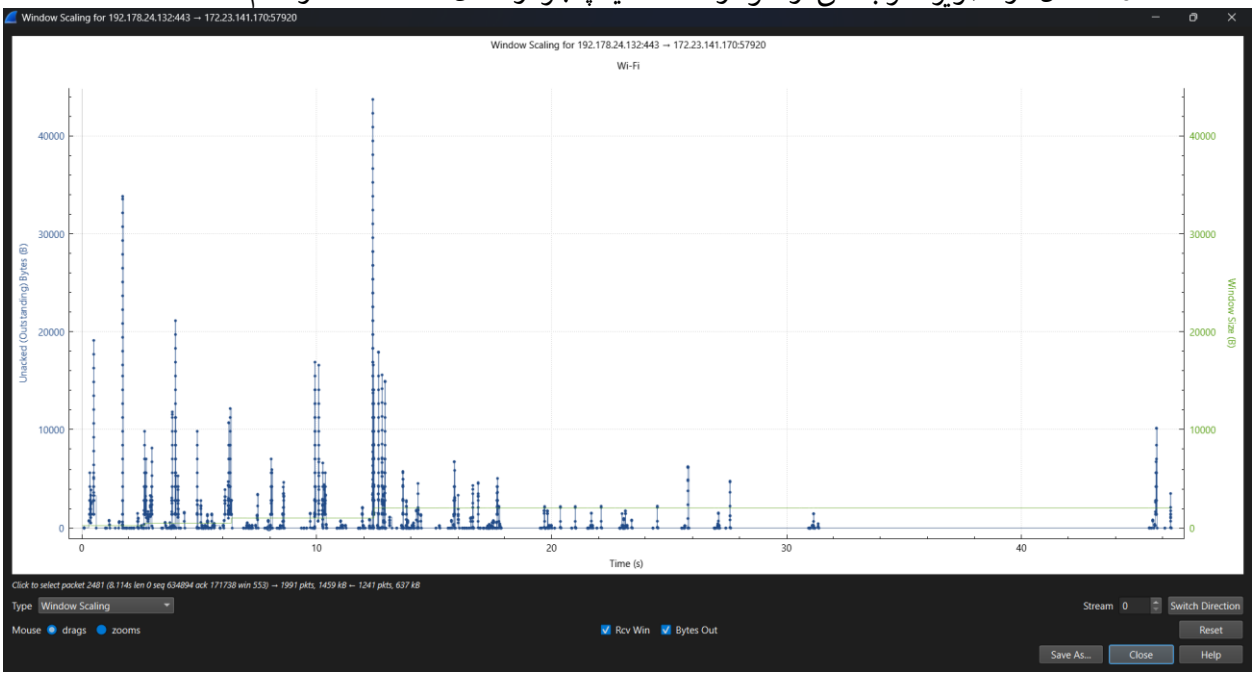
سوال 9: نمودارهاي Windows scaling،Throughputو RTTرا بررسی کنید و مشخص کنید در شرایط ازدحام چه اتفاق براي موارد بیان شده رخ میدهد.

جواب:

نمودارWindow Scaling :

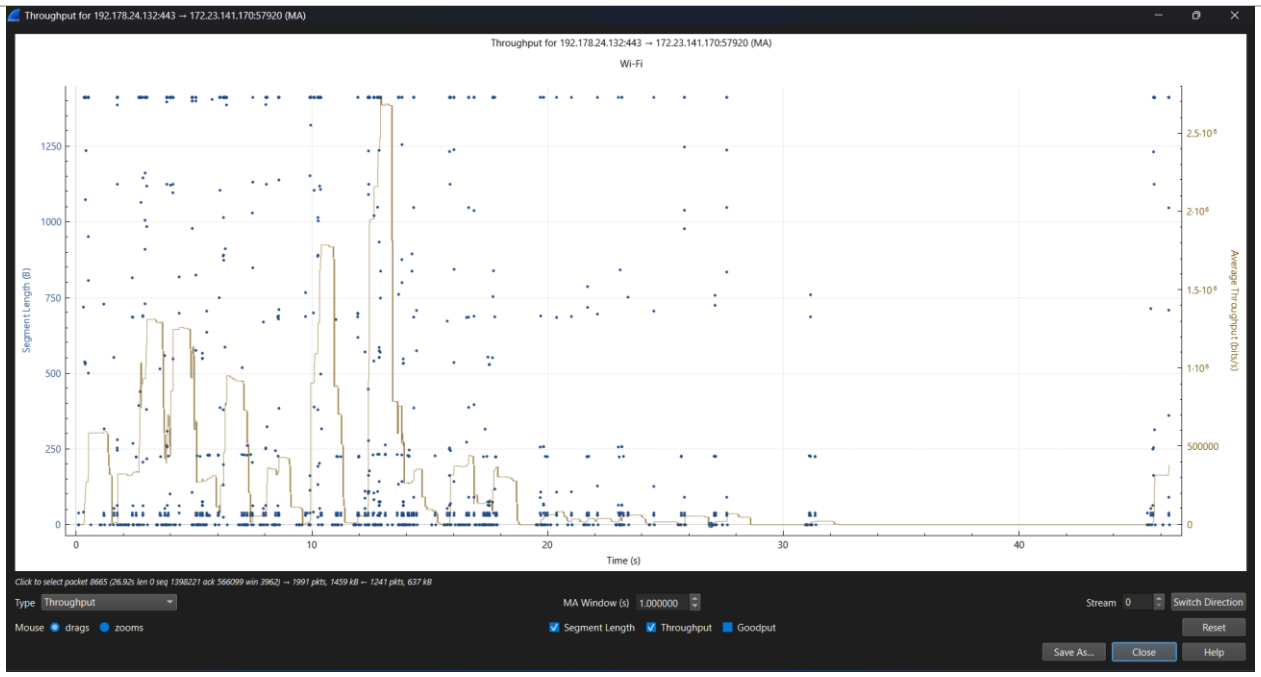
- رفتار عادی:
  - خط سبز (اندازه پنجره دریافت) و خط آبی (داده ارسالی) با شیب ملایم و پایدار افزایش/کاهش می‌یابند.
  - پنجره دریافت بهینه است و تطابق خوبی با نرخ ارسال دارد.
- در شرایط ازدحام:

- کاهش ناگهانی اندازه پنجره (خط سبز) :گیت‌وی یا گیرنده به دلیل پر شدن بافر، پنجره را کوچک می‌کند.
- نوسانات شدید در داده ارسالی (خط آبی) : ارسال داده متوقف یا با نرخ کمتری ادامه می‌یابد.
- مثال در تصویر: اگر بخشی از نمودار افت شدید پنجره را نشان دهد، نشانه ازدحام است.



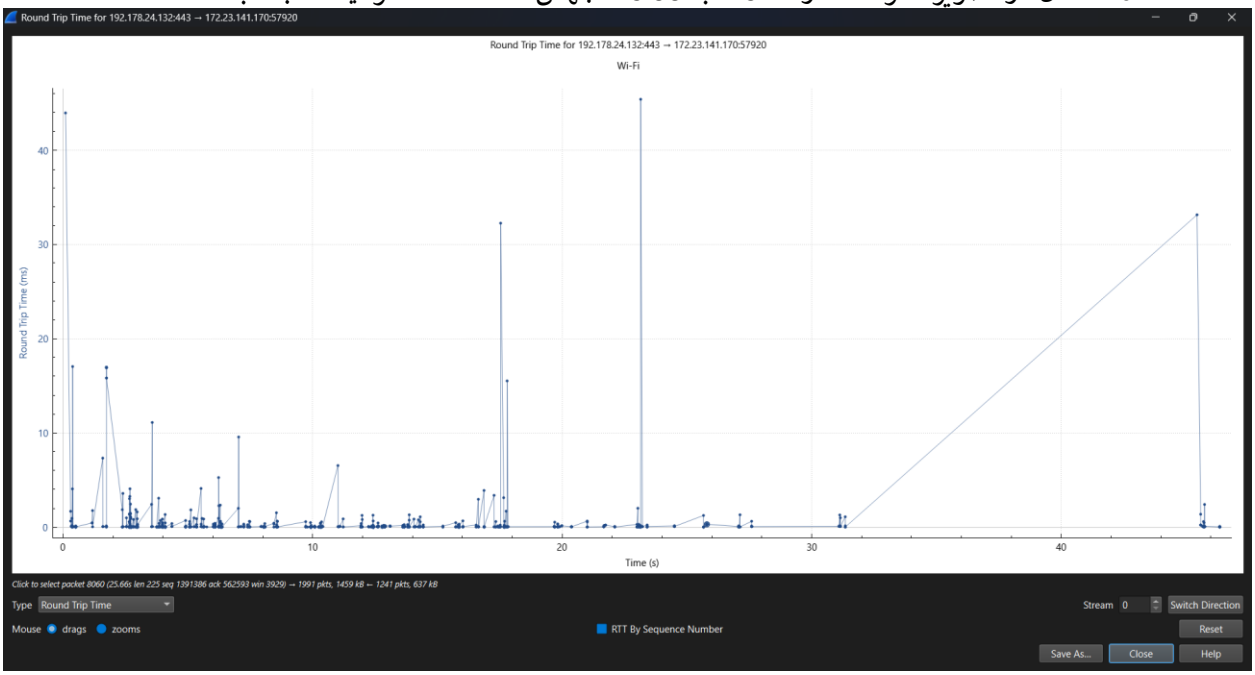
نمودار Throughput یا گذردهی:

- رفتار عادی:
  - گذردهی ثابت یا با افزایش تدریجی (مثلاً در دانلود فایل).
  - Goodput (داده مفید کاربر) نزدیک به Throughput کل است.
- در شرایط ازدحام:
  - افت ناگهانی گذردهی : به دلیل تاخیر در ACK یا از دست رفتن بسته‌ها.
  - اختلاف زیاد بین Throughput و Goodput نشانه Retransmission های مکرر است.
  - مثال در تصویر: اگر نمودار Throughput به جای الگوی صاف، دندانه‌های شدید مشاهده شود، احتمالاً شبکه اشباع شده است.



نمودار Round-Trip Time (RTT) :

- رفتار عادی:
  - RTT پایدار با تغییرات کم مثلاً 50-100 ms برای شبکه‌های محلی.
- در شرایط ازدحام:
  - افزایش ناگهانیRTT : بسته‌ها در صف‌های روتر معطل می‌شوند.
  - ناپایداری در نمودار : تغییرات سریع RTT نشانه ازدحام یا مسیریابی ضعیف است.
  - مثال در تصویر: اگر RTT از 22 ms به 60 ms جهش کند، احتمالاً ترافیک شبکه بالا است.



سؤال 10: چرا UDPدر مقایسه با TCP،Flow controlندارد؟

جواب:

ماهیت طراحی پروتکل‌ها:

- TCP (Transmission Control Protocol):
  - اتصال‌گرا (Connection-Oriented) یعنی قبل از انتقال داده، یک ارتباط سه‌مرحله‌ای برقرار می‌کند.
  - قابلیت اطمینان :تضمین می‌کند تمام داده‌ها بدون خطا و به ترتیب صحیح به مقصد برسند.
  - کنترل جریان (Flow Control) : با استفاده از مکانیسم پنجره لغزان(Sliding Window) ، نرخ ارسال داده را با توجه به ظرفیت گیرنده تنظیم می‌کند تا از اشباع گیرنده جلوگیری شود.
- UDP (User Datagram Protocol):
  - بی‌اتصال (Connectionless) یعنی هیچ تاییدیه‌ای قبل از ارسال داده وجود ندارد.
  - غیرقابل اعتماد :هیچ تضمینی برای تحویل داده یا ترتیب صحیح آن ندارد.
  - سادگی و سرعت :به دلیل عدم وجود مکانیسم‌های کنترل، سربار (Overhead) کمتری دارد و سریع‌تر است.