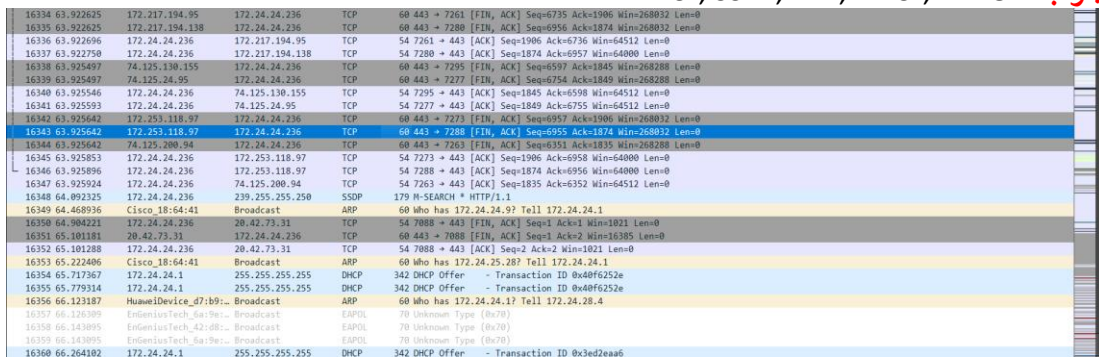




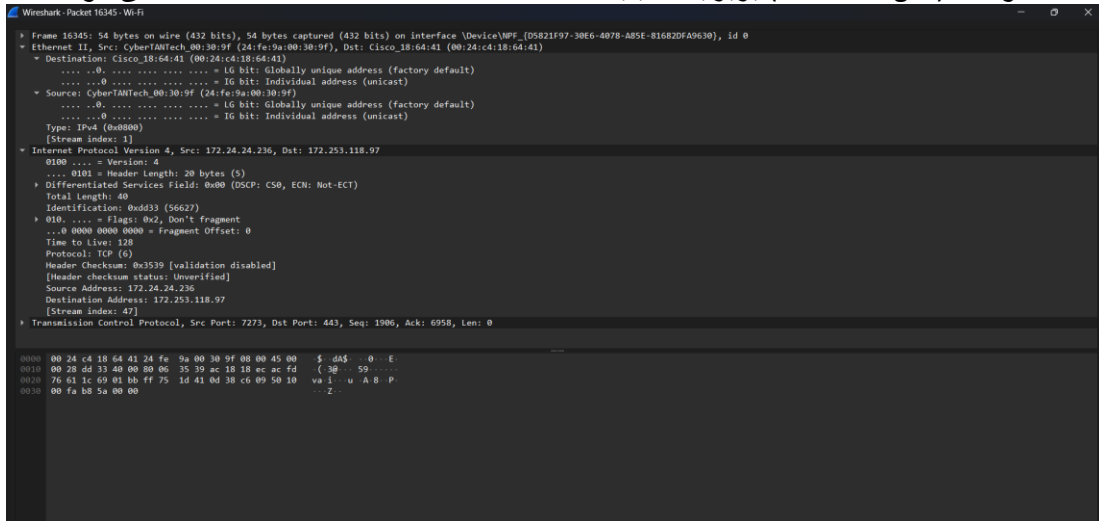
## فرم گزارش کار آزمایشگاه شبکه

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی امیرکبیر  
(پلی تکنیک تهران)

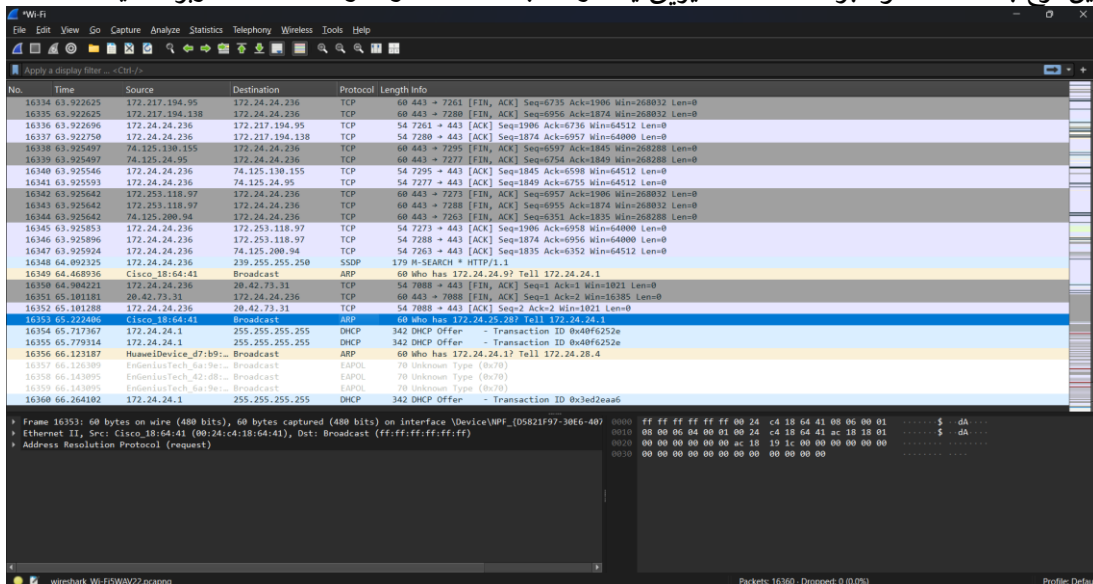
نام و نام خانوادگی	حسین تاتار	شماره دانشجویی	40133014	نام و شماره آزمایش	3 - آشنایی با نرمافزار Wireshark
هدف آزمایش	در این آزمایش با نرمافزار Wireshark آشنا میشویم تا بتوانیم با کمک این ابزار، ترافیک شبکه را ضبط، تحلیل و پروتکل های مختلف را در لایه های گوناگون شناسایی کنیم.				
ابزارهای مورد نیاز	نرمافزار Wireshark دسترسی به اینترنت				
شرح آزمایش	<p><b>سوال 1:</b> به یک بخش دلخواه از بسته های شنود شده مراجعه کنید. چه پروتکلهایی را مشاهده میکنید. لیست آنها را یادداشت کنید.</p> <p><b>جواب:</b> TCP, SSDP, ARP, DHCP, EAPOL</p>  <p><b>سوال 2:</b> یک بسته را به دلخواه انتخاب کنید. مشخص کنید که چه پروتکل هایی در لایه های مختلف آن استفاده شده است. ترتیب قرارگیری بیت ها داخل بسته چه ارتباطی با لایه های مختلف دارد؟ اندازه فریم لایه دو این بسته چقدر است؟ اندازه بسته لایه 3 چقدر است؟</p> <p><b>جواب:</b></p> <p>لایه ۲) لایه پیوند داده (Data Link Layer): پروتکل Ethernet II</p> <p>لایه ۳) لایه شبکه (Network Layer): پروتکل IPv4</p> <p>لایه ۴) لایه انتقال (Transport Layer): پروتکل TCP</p> <p>در هر بسته شبکه، داده ها به صورت لایه ای سازمان دهی می شوند. هر لایه اطلاعات مربوط به خود را به بسته اضافه می کند و این اطلاعات به صورت سریرگ (Header) در ابتدای بسته قرار می گیرد.</p> <p>اندازه فریم لایه دو 54 بایت یا 432 بیت: این اندازه شامل تمام داده های لایه به علاوه داده های لایه های بالاتر است.</p>				

اندازه بسته لایه سه (IPv4) 40 بایت: این اندازه شامل هدر IPv4 و داده‌های لایه‌های بالاتر است. در این بسته، طول کل (Total Length) برابر با 40 بایت است که شامل هدر IPv4 و داده‌های TCP می‌شود.



**سوال 3:** آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Network و Transport باشند؟

**جواب:** بسته‌هایی که بدون پروتکل‌های لایه‌های Network و Transport باشند، معمولاً در لایه‌های پایین‌تر شبکه (لایه‌های فیزیکی و پیوند داده) قرار می‌گیرند. این نوع بسته‌ها معمولاً برای اهداف مدیریتی یا کنترل شبکه استفاده و حاوی داده‌های کاربردی نیستند.



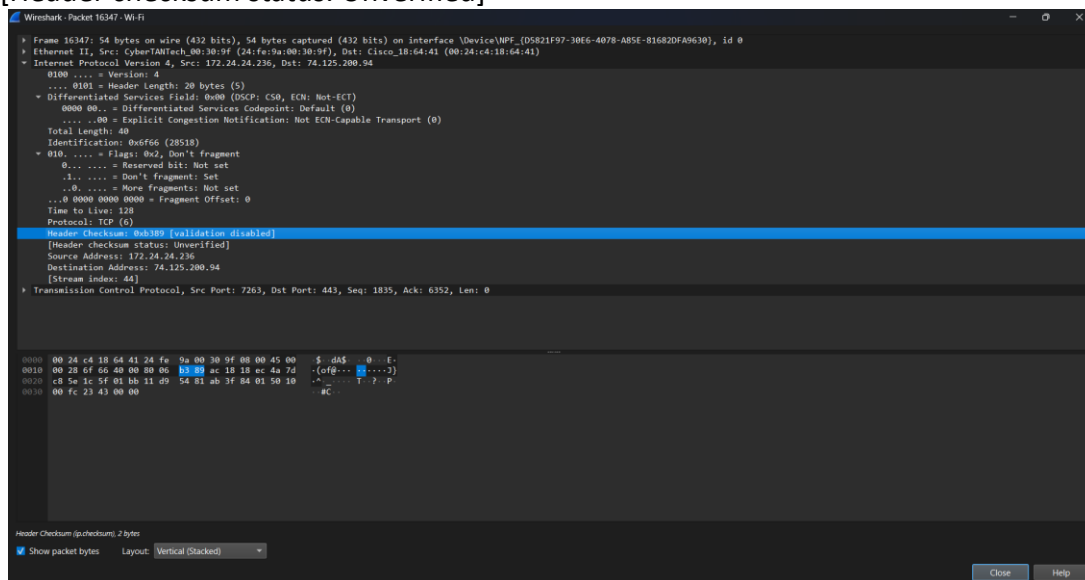
**سوال 4:** این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

**جواب:**  
ARP (Address Resolution Protocol)  
STP (Spanning Tree Protocol)  
LLDP (Link Layer Discovery Protocol)

**سوال 5:** از یکی از بسته ها بخش مربوط به پروتکل Internet Protocol(IP) را پیدا کنید .  
Checksum پروتکل IP را پیدا کنید و آن را یادداشت کنید.

**جواب:** Checksum در پروتکل IP برای بررسی صحت هدر IP استفاده می شود. در این بسته، وضعیت Checksum به عنوان Unverified (تایید نشده) مشخص شده است، یعنی Wireshark نتوانسته صحت Checksum را تأیید کند.

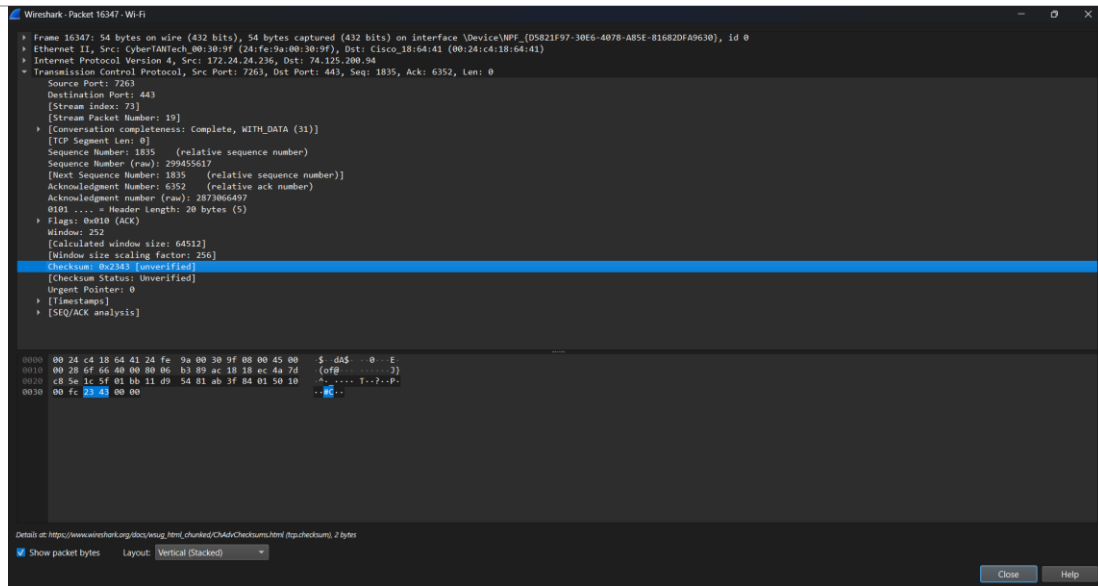
Header Checksum: 0xb389 [validation disabled]  
[Header checksum status: Unverified]



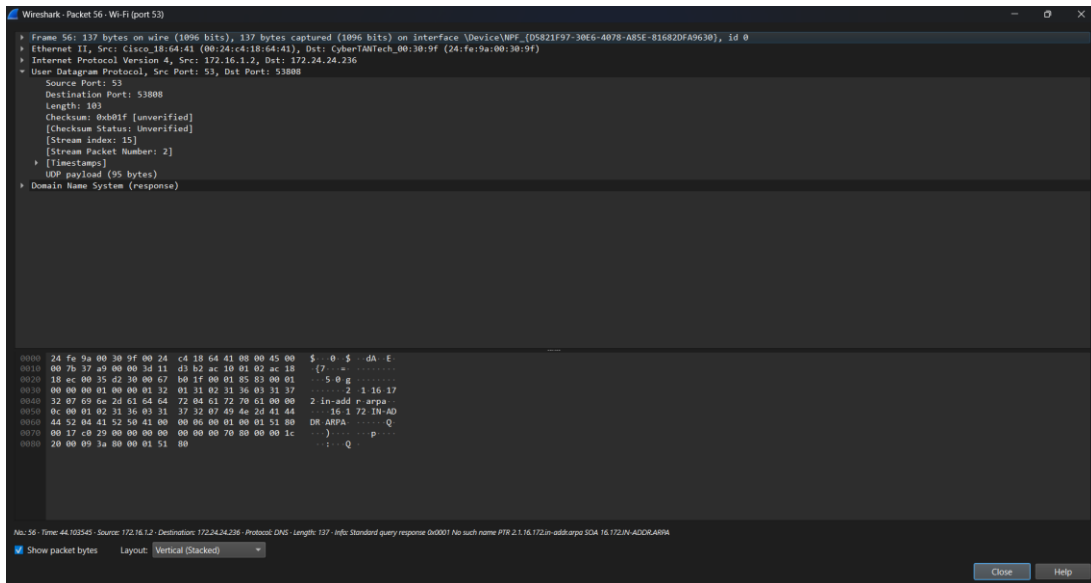
**سوال 6:** از یکی از بسته ها بخش مربوط به پروتکل TCP, UDP را پیدا کنید. عدد مربوط به Port مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص میکند؟ Checksum مربوط به پروتکل های TCP و UDP را مشخص کنید.

**جواب:** بخش مربوط به پروتکل TCP: ۴۳  
-پورت مبدا (Source Port): 7263  
-پورت مقصد (Destination Port): 443  
-Checksum پروتکل TCP: 0x2343

پورت ها برای شناسایی سرویس های خاص در شبکه استفاده می شوند. پورت مقصد (443) نشان دهنده ی این است که این بسته به یک سرویس HTTPS ارسال شده است، در حالی که پورت مبدا (7263) به صورت موقت توسط کلاینت انتخاب شده است تا پاسخ ها به درستی به این ارتباط اختصاص داده شوند.



**سوال 7:** یکی از بسته ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟  
 آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.  
**جواب:** پروتکل لایه Transport: UDP (User Datagram Protocol)  
 آدرس IP مقصد: 172.24.24.236  
 سرایند (Header) لایه دوم (Ethernet II) : آدرس MAC مبدا 00:24:c4:18:64:41 و آدرس MAC مقصد 24:fe:9a:00:30:9f است.



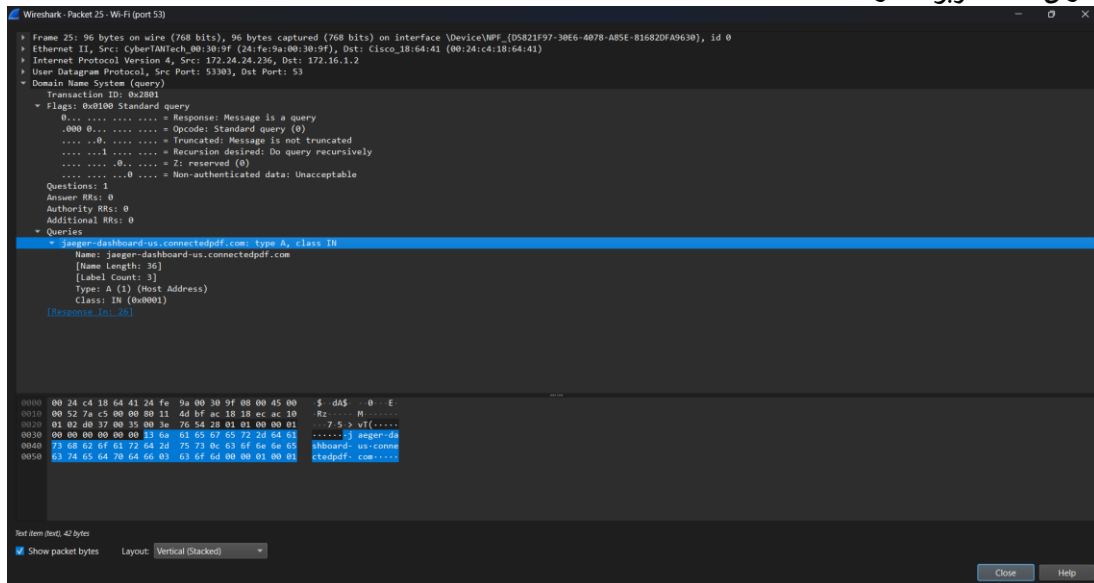
**سوال 8:** کدامیک از آدرسهای پیدا کرده در قبل را میتوانید در خروجی دستور all ipconfig /all مشاهده کنید؟  
**جواب:** آدرس IP مقصد 172.24.24.236 و آدرس MAC مقصد 24:fe:9a:00:30:9f در سرایند لایه 2.

#### Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : Bastami
Description . . . . . : Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
Physical Address. . . . . : 24-FE-9A-00-30-9F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-Local IPv6 Address . . . . : fe80::44cf:b3fd:ea05:e47c%21(Preferred)
IPv4 Address. . . . . : 172.24.24.236(Preferred)
Subnet Mask . . . . . : 255.255.248.0
Lease Obtained. . . . . : Wednesday, March 5, 2025 3:46:36 PM
Lease Expires . . . . . : Monday, March 10, 2025 7:07:18 PM
Default Gateway . . . . . : 172.24.24.1
DHCP Server . . . . . : 172.24.24.1
DHCPv6 IAID . . . . . : 136642202
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-FA-93-23-24-FE-9A-00-30-9F
DNS Servers . . . . . : 172.16.1.2
                        172.16.1.3
NetBIOS over Tcpip. . . . . : Enabled
```

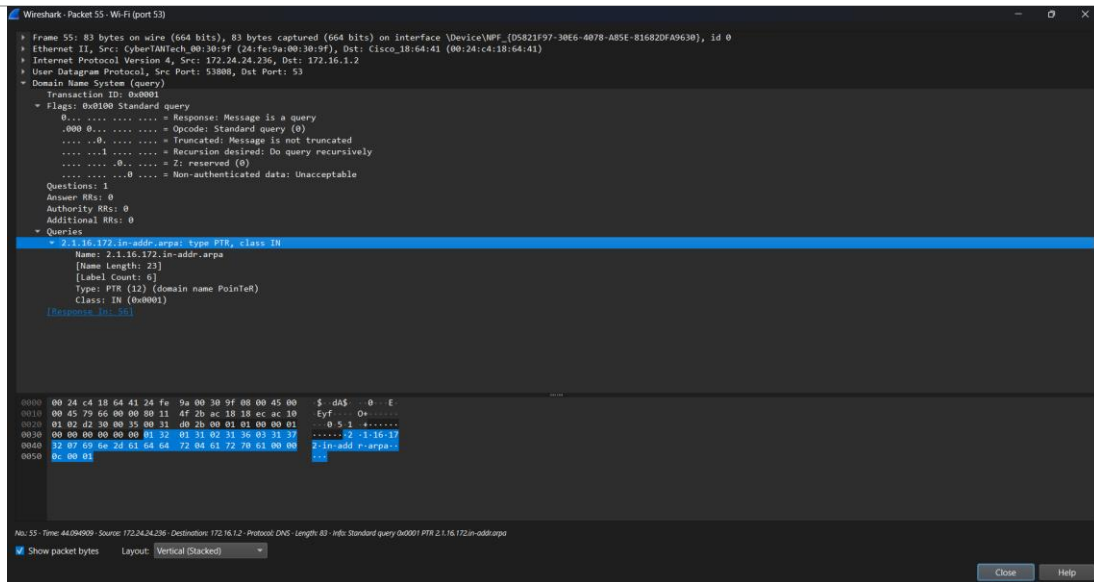
**سوال 9:** یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

**جواب:** نوع درخواست (Type) A Record :A برای تبدیل نام دامنه به آدرس IPv4 استفاده می‌شود. این کار معمولاً برای دسترسی به سرورها یا سرویس‌های مبتنی بر IP انجام می‌شود. در این بسته، درخواست برای تبدیل نام دامنه `jaeger-dashboard-us.connectedpdf.com` به آدرس IPv4 مربوطه ارسال شده است.



**سوال 10:** یک بسته مربوط به دستور nslookup را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ بده نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

**جواب:** نوع درخواست (Type) PTR (Pointer Record) (Type) (Reverse DNS Lookup) : این نوع درخواست برای تبدیل آدرس IP به نام دامنه در این بسته، درخواست برای تبدیل آدرس IP 172.16.1.2 به نام دامنه‌ی مربوطه ارسال شده است.



**سوال 11:** به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.  
**جواب:**

AAAA (IPv6 Address Record): تبدیل نام دامنه به آدرس IPv6  
 CNAME (Canonical Name Record): ایجاد یک نام مستعار (Alias) برای یک نام دامنه ی دیگر  
 MX (Mail Exchange Record): مشخص کردن سرورهای ایمیل مرتبط با یک دامنه

**سوال 12:** بعد از کلیک کردن بر روی OK چه اتفاقی می افتد؟ در بسته هایی که مشخص شده اند چه پروتکل هایی را مشاهده میکنید؟

**جواب:** بعد از کلیک کردن بر روی OK، Wireshark فقط بسته هایی را نمایش می دهد که با فیلتر اعمال شده مطابقت داشته باشند. در این حالت، بسته هایی که آدرس IP مبدا یا مقصد آنها برابر با آدرس IP وارد شده است، نمایش داده می شوند. (5.144.130.115)

پروتکل های مشاهده شده عبارتند از:

Ethernet II: لایه ۲ (Data Link Layer)

IPv4: لایه ۳ (Network Layer)

ICMP: لایه ۴ (Transport Layer)

- IPv4: درون (ICMP): آدرس IP مقصد: 5.144.130.115

- ICMP: درون (ICMP)

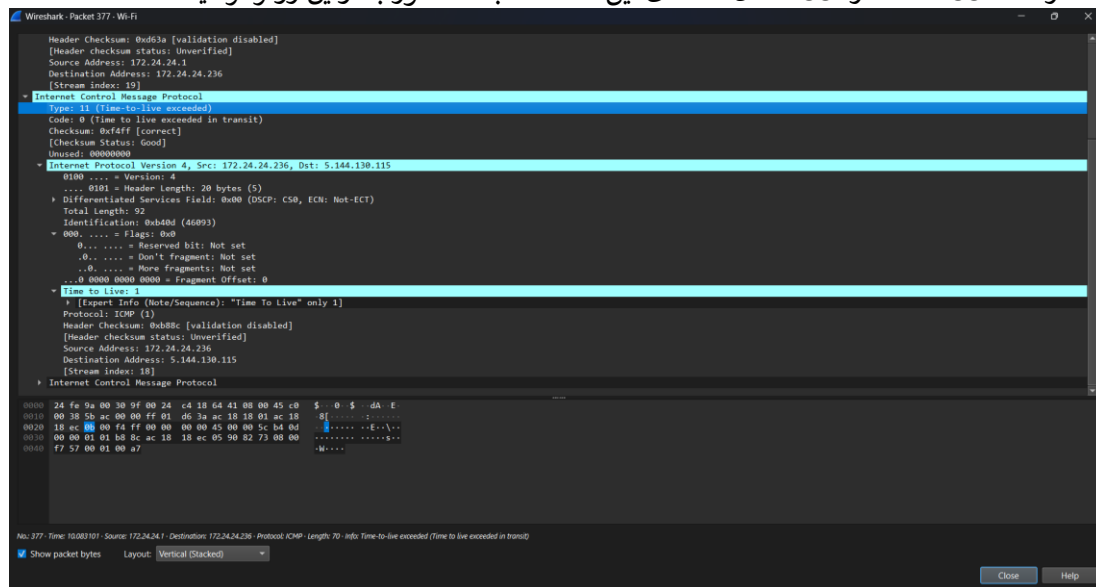


**سوال 13:** اولین بسته را انتخاب کنید. به بخش پروتکل Internet Message Protocol بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

**جواب:**

نوع ICMP: 11 (Time-to-live exceeded) - این نوع پیام ICMP نشان دهنده این است که بسته‌ی ارسالی به دلیل پایان یافتن زمان حیات (TTL) دور انداخته شده است.

مقدار TTL: 255 - مقدار 255 نشان دهنده این است که بسته هنوز به اولین روتر نرسیده است.



برای بسته هایی که مبدا آنها ماشین شماست مقدار TTL را یادداشت کنید. این مقدار در حال تغییر است.

**سوال 14:** به نظر شما هدف از تغییر این مقدار چیست؟ میتوانید با مراجعه به هدف دستور tracer آن را شرح دهید.

**جواب:** هدف اصلی TTL جلوگیری از چرخش بی پایان بسته‌ها در شبکه است. هر بار که بسته از یک روتر عبور می‌کند، مقدار TTL آن کاهش می‌یابد. اگر TTL به صفر برسد، بسته دور انداخته می‌شود و یک پیام ICMP با نوع Time-to-live exceeded به مبدا ارسال می‌شود.



هدف در دستور `tracert` از تغییر مقدار TTL برای تشخیص مسیر بسته‌ها در شبکه است. این دستور به صورت زیر کار می‌کند:

1. ابتدا یک بسته با TTL برابر 1 ارسال می‌کند. این بسته به اولین روتر می‌رسد و TTL آن به صفر می‌رسد. روتر یک پیام ICMP با نوع `Time-to-live exceeded` به مبدا ارسال می‌کند.
2. سپس یک بسته با TTL برابر 2 ارسال می‌کند. این بسته به دومین روتر می‌رسد و TTL آن به صفر می‌رسد. روتر یک پیام ICMP با نوع `Time-to-live exceeded` به مبدا ارسال می‌کند.
3. این روند ادامه می‌یابد تا بسته به مقصد نهایی برسد. با این روش، مسیر کامل بسته‌ها از مبدا به مقصد مشخص می‌شود.

از بخش فیلتر، مقدار فیلتر را به دستور `ip.proto == 6` تغییر دهید .

**سوال 15:** این فیلتر چه کاری انجام می‌دهد؟

**جواب:** این فیلتر فقط بسته‌هایی را نمایش می‌دهد که پروتکل لایه شبکه (IP) آن‌ها برابر با 6 باشد. مقدار 6 در پروتکل IP نشان‌دهنده‌ی (Transmission Control Protocol) TCP است. بنابراین، فقط بسته‌های TCP را نمایش می‌دهد.

The screenshot shows the Wireshark interface with a packet capture from a Wi-Fi interface. The packet list on the left shows various protocols including TCP, SYN, ACK, and TLS. The selected packet (No. 1891) is a TCP packet from 172.24.24.236 to 172.24.24.236, Seq=1514, Ack=443, Len=1460. The packet details pane on the right shows the TCP header and application data. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1884	305.582631	172.24.24.236	172.24.24.236	TCP	60	53 → 3007 [FIN, ACK] Seq=192 Ack=38 Win=29312 Len=0
1885	305.582741	172.24.24.236	172.16.1.2	TCP	54	3007 → 53 [ACK] Seq=38 Ack=193 Win=65280 Len=0
1886	305.852168	172.24.24.236	47.246.50.183	TCP	66	3009 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1887	305.839877	47.246.50.183	172.24.24.236	TCP	66	443 → 3009 [SYN, ACK] Seq=0 Ack=1 Min=42340 Len=0 MSS=1460 SACK_PERM WS=512
1888	305.839877	47.246.50.183	172.24.24.236	TCP	66	[TCP Out-Of-Order] 443 → 3009 [SYN, ACK] Seq=0 Ack=1 Min=42340 Len=0 MSS=1460 SACK_PERM WS=512
1889	305.648114	172.24.24.236	47.246.50.183	TCP	54	3009 → 443 [ACK] Seq=1 Ack=1 Min=65280 Len=0
1890	305.841327	172.24.24.236	47.246.50.183	TCP	1514	3009 → 443 [ACK] Seq=1 Ack=1 Min=65280 Len=1460 [TCP PDU reassembled in 1891]
1891	305.841327	172.24.24.236	47.246.50.183	TLSv1.3	793	Client Hello (SHA-gator.volces.com)
1892	305.976204	104.18.27.90	172.24.24.236	TLSv1.3	221	Application Data
1893	305.976204	104.18.27.90	172.24.24.236	TLSv1.3	379	Application Data
1894	305.976351	172.24.24.236	104.18.27.90	TCP	54	3004 → 443 [ACK] Seq=4384 Ack=3241 Win=64800 Len=0
1895	305.977322	104.18.27.90	172.24.24.236	TLSv1.3	85	Application Data
1896	305.977322	47.246.50.183	172.24.24.236	TCP	66	[TCP Out-Of-Order] 443 → 3009 [SYN, ACK] Seq=0 Ack=1 Min=42340 Len=0 MSS=1460 SACK_PERM WS=512
1897	305.977322	47.246.50.183	172.24.24.236	TCP	66	443 → 3009 [SYN, ACK] Seq=0 Ack=1 Min=42340 Len=0 MSS=1460 SACK_PERM WS=512
1898	305.977322	47.246.50.183	172.24.24.236	TCP	66	[TCP Dup ACK 1897] 443 → 3009 [ACK] Seq=1 Ack=1 Min=42496 Len=0 SLE=1461 SRE=2110
1899	305.977322	47.246.50.183	172.24.24.236	TCP	60	443 → 3009 [ACK] Seq=1 Ack=2110 Win=4496 Len=0
1900	305.977322	47.246.50.183	172.24.24.236	TLSv1.3	298	Server Hello, Change Cipher Spec, Application Data, Application Data
1901	305.977430	172.24.24.236	47.246.50.183	TCP	66	[TCP Dup ACK 1899] 3009 → 443 [ACK] Seq=2110 Ack=1 Min=65280 Len=0 SLE=0 SRE=1
1902	305.977652	172.24.24.236	47.246.50.183	TCP	54	3009 → 443 [ACK] Seq=1 Ack=1 Min=65280 Len=0
1903	305.978521	172.24.24.236	47.246.50.183	TLSv1.3	118	Change Cipher Spec, Application Data
1904	305.979439	172.24.24.236	47.246.50.183	TCP	1514	3009 → 443 [ACK] Seq=1 Ack=1 Min=65280 Len=1460 [TCP PDU reassembled in 1905]
1905	305.979439	172.24.24.236	47.246.50.183	TLSv1.3	607	Client Hello (SHA-gator.volces.com)
1906	305.981654	172.24.24.236	47.246.50.183	TLSv1.3	600	Application Data

Packet Details (No. 1891):

- Ethernet II, Src: Intel(R) Dual Band Wireless-AC 8265, Dst: Intel(R) Dual Band Wireless-AC 8265
- Internet Protocol Version 4, Src: 172.24.24.236, Dst: 172.24.24.236
- Transmission Control Protocol, Src Port: 3009, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
- Stream index: 59

Packet Bytes:

0000 24 fe 9a 00 30 9f 00 24 c4 18 64 41 88 00 45 00 5 0 5 da E  
0010 00 34 00 3c 40 00 20 86 57 46 2f f6 32 57 ac 18 -4-0- W / 2...  
0020 15 4c 01 b0 00 c0 1f 02 88 ba 45 05 80 20 00 00 - - - - E - -  
0030 00 53 1d 7f 00 00 01 01 05 0a 45 05 90 d4 45 05 5 - - - - E - E  
0040 93 5d ]