دانشکده‌ی مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

نیم‌سال سوم ۰۴-۱۴۰۳

استاد: دکتر بردیا صفائی

گروه شماره ۱ : مهدی محمدی (۴۰۰۱۰۵۲۳۹) - ملیکا علیزاده (۴۰۱۱۰۶۲۵۵) - معین آعلی (۴۰۱۱۰۵۵۶۱)

گزارش آزمایش شماره‌ی ۲

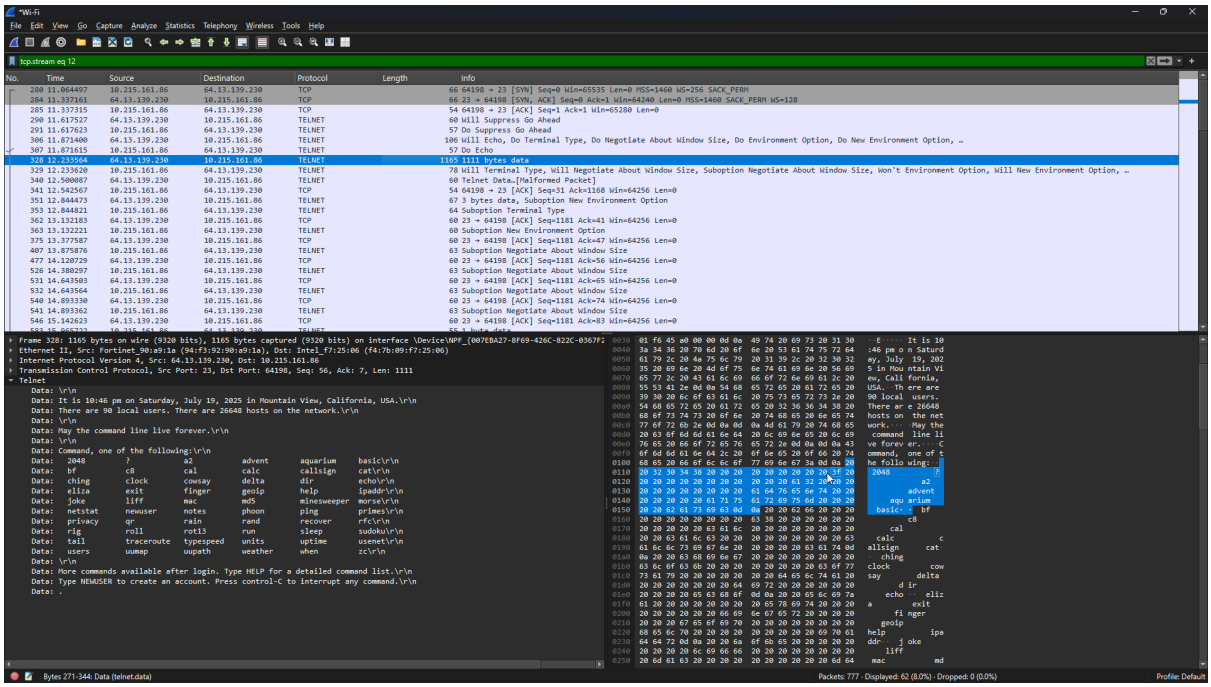
فهرست مطالب

بررسی ارتباط از طریق Telnet

در ابتدا نیاز است تا telnet را روی ویندوز فعال کنیم. وارد control panel می‌شویم و در بخش Programs گزینه‌ی Turn Windows features on or off را انتخاب می‌کنیم. سپس به دنبال telnet client می‌گردیم و آن را فعال می‌کنیم.

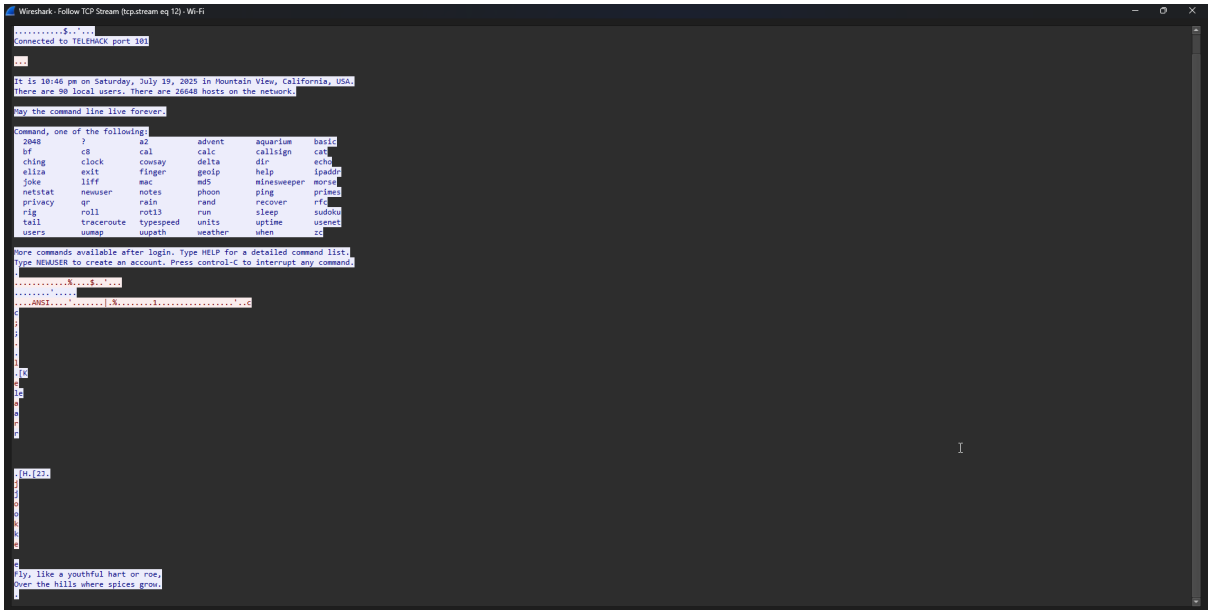
حال وارد cmd شده و با استفاده از دستور telnet telehack.com به آن متصل می‌شویم. البته قبل از آن باید wire-shark را در حالت capture بر روی interface اینترنت خود قرار دهیم. سپس تعدادی از دستورات را امتحان کرده و در نهایت capture را متوقف می‌کنیم.

در Wireshark فیلتر را روی telnet قرار داده و بسته‌ها را مشاهده می‌کنیم:



به عنوان مثال این بسته مربوط به پیام welcome این سیستم است که دستورات خود را به ما معرفی کرده است.

برای این که پیام‌ها را دنبال کنیم، روی این بسته کلیک راست کرده و از منوی follow گزینه‌ی tcp stream را انتخاب می‌کنیم.

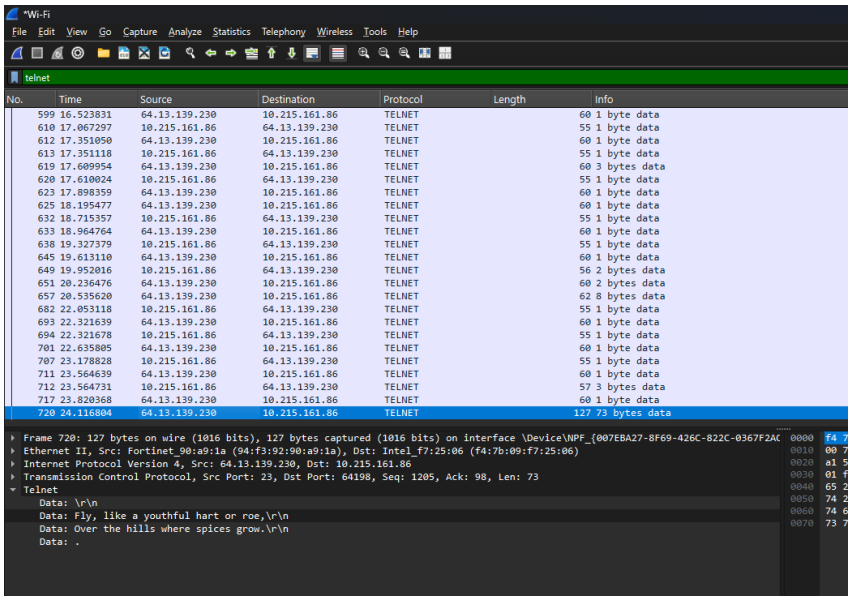


همانطور که در تصویر مشخص است، من با استفاده از کامند joke درخواست یک جوک کردم و در اخرین بسته این جوک به دست من رسیده است.

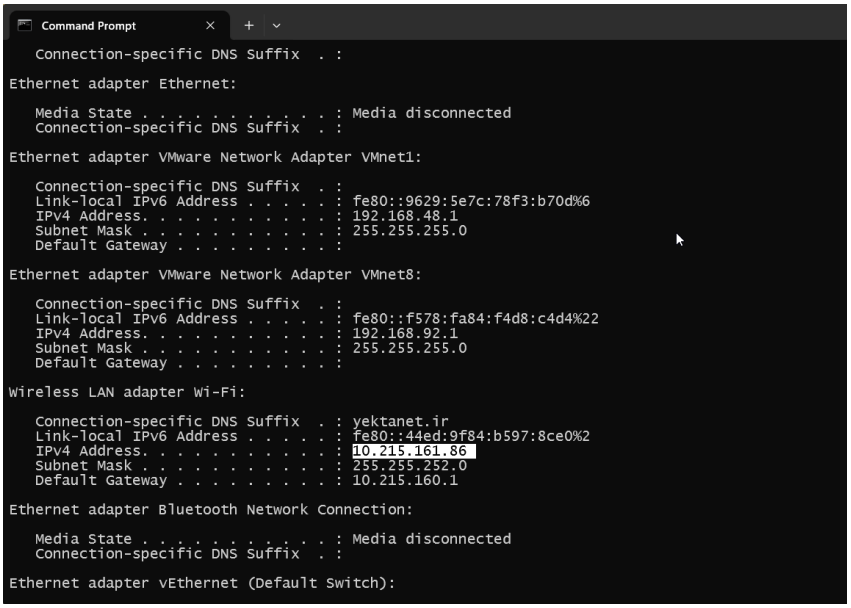
نکته مهمی که در شل گرفتن قابل توجه است، این است که وقتی ما در شل تایپ می‌کنیم. هر کارکتر در یک بسته جدا به سمت سرور فرستاده می‌شود و سپس از سمت سرور اگر به درستی به دستش رسیده باشد همان را برای ما برمی‌گرداند. این موضوع داخل tcp trace فوق قابل مشاهده است.

نکته مهم دیگری که در این پروتوکل مورد توجه قرار می‌گیرد، این است که پیام‌ها و بسته‌ها به صورت رمزنگاری نشده رد و بدل می‌شود که نشان دهنده امنیت پایین‌تر این پروتوکل نسبت به پروتوکل‌های دیگر نظیر SSH است.

سوال ۱.



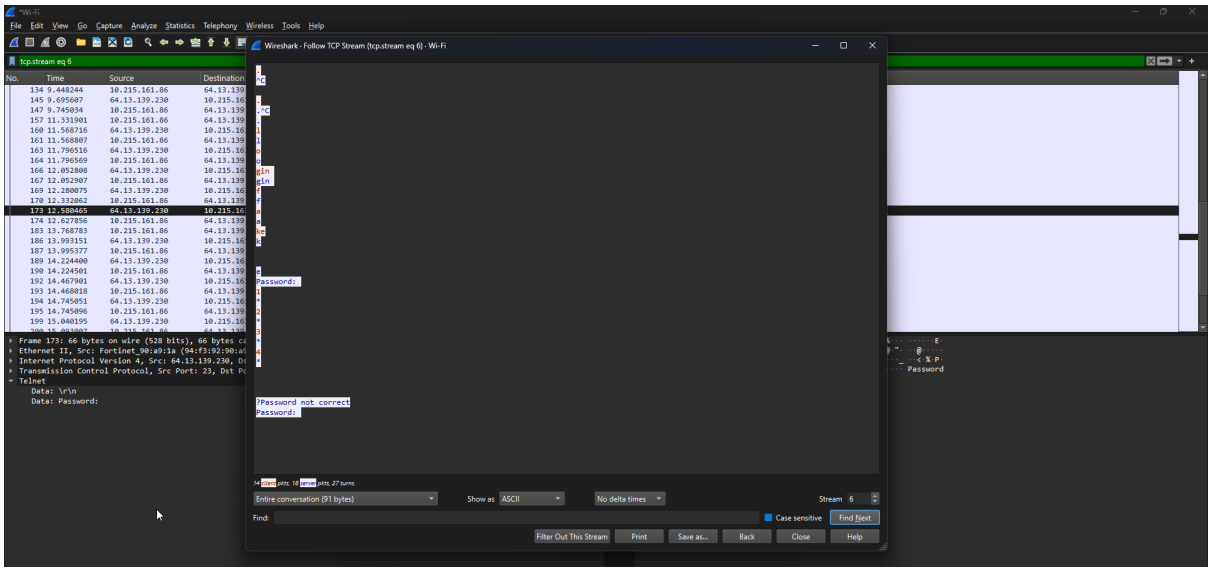
با توجه به شکل فوق واضح است که آیپی سرور Source و ایپی من Destination است.



برای اطمینان از صحت عملکرد، دستور ipconfig را در cmd وارد کرده و آیپی خود را مشاهده می‌کنیم.

سوال ۲.

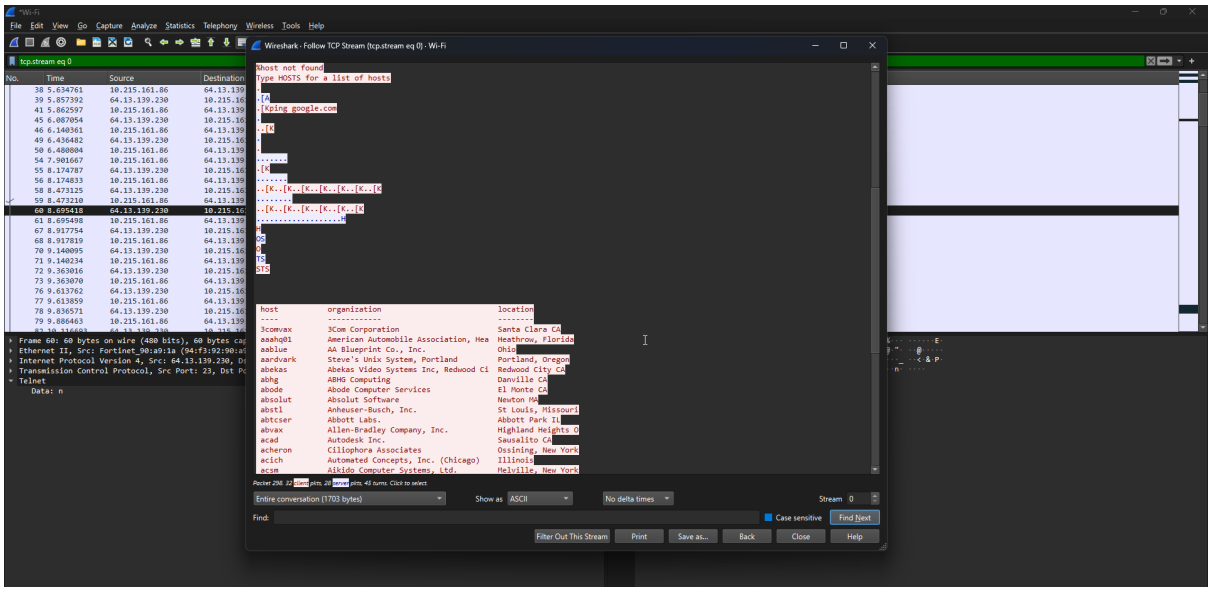
در این بخش هم با استفاده از tcp stream می‌توانیم بسته‌های مبادله شده را مشاهده کنیم. من به عنوان تست از یوزرنیم fake و پسورد 1234 استفاده می‌کنم.



همانطور که مشخص است پسورد و یوزرنیم به صورت raw بین کلاینت و سرور مبادله شده است و به راحتی قابل دسترسی است.

سوال ۳.

واضح است که بسته‌های آبی مربوط به من و بسته‌های قرمز مربوط به سرور است.



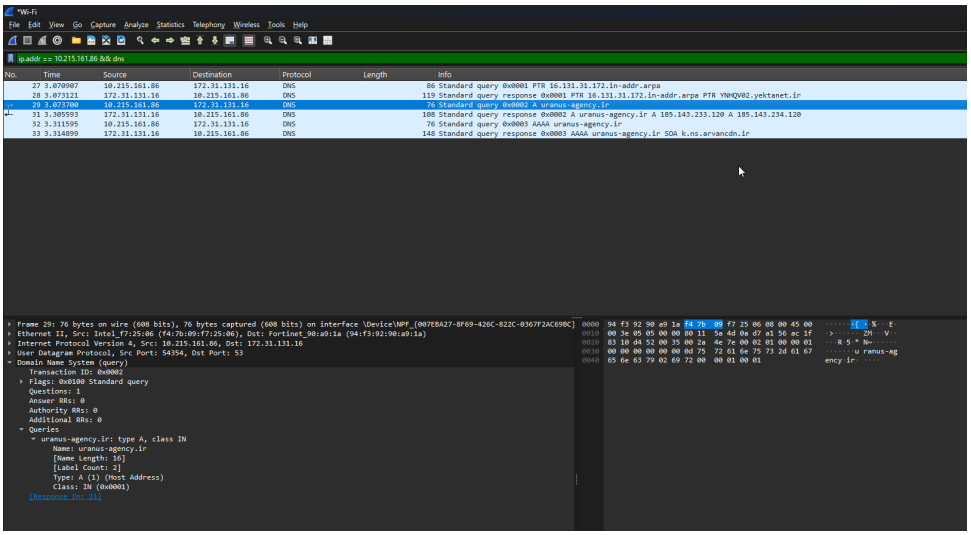
بررسی درخواست و پاسخ‌های DNS

ابتدا cmd را باز کرده و با استفاده از دستور ipconfig /flushdns کش DNS خود را پاک می‌کنیم. سپس با استفاده از دستور nslookup یک کوئری استاندارد برای این دامنه ارسال می‌کنیم.

```
C:\Users\moeei>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\moeei>nslookup uranus-agency.ir
Server:  YNHQV02.yektanet.ir
Address:  172.31.131.16

Non-authoritative answer:
Name:    uranus-agency.ir
Addresses:  185.143.233.120
          185.143.234.120


C:\Users\moeei>nslookup uranus-agency.ir
Server:  YNHQV02.yektanet.ir
Address:  172.31.131.16

Non-authoritative answer:
Name:    uranus-agency.ir
Addresses:  185.143.233.120
          185.143.234.120
```

همانطور که در تصویر مشخص است، از یک سرور DNS لوکال استفاده شده به نام YNHQV02.yektanet.ir که آدرس آیپی آن هم در تصویر موجود است.

حال داخل wireshark فیلتر آیپی خودمان و فیلتر بسته‌های DNS را اعمال می‌کنیم تا بسته‌ها را مشاهده کنیم:

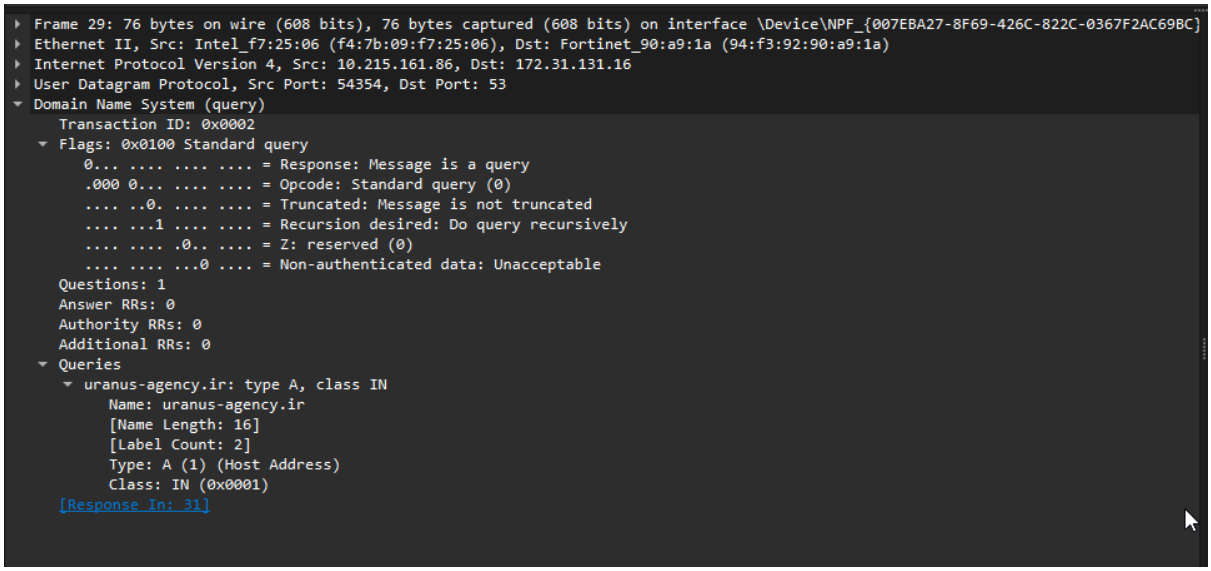


سوال ۱.

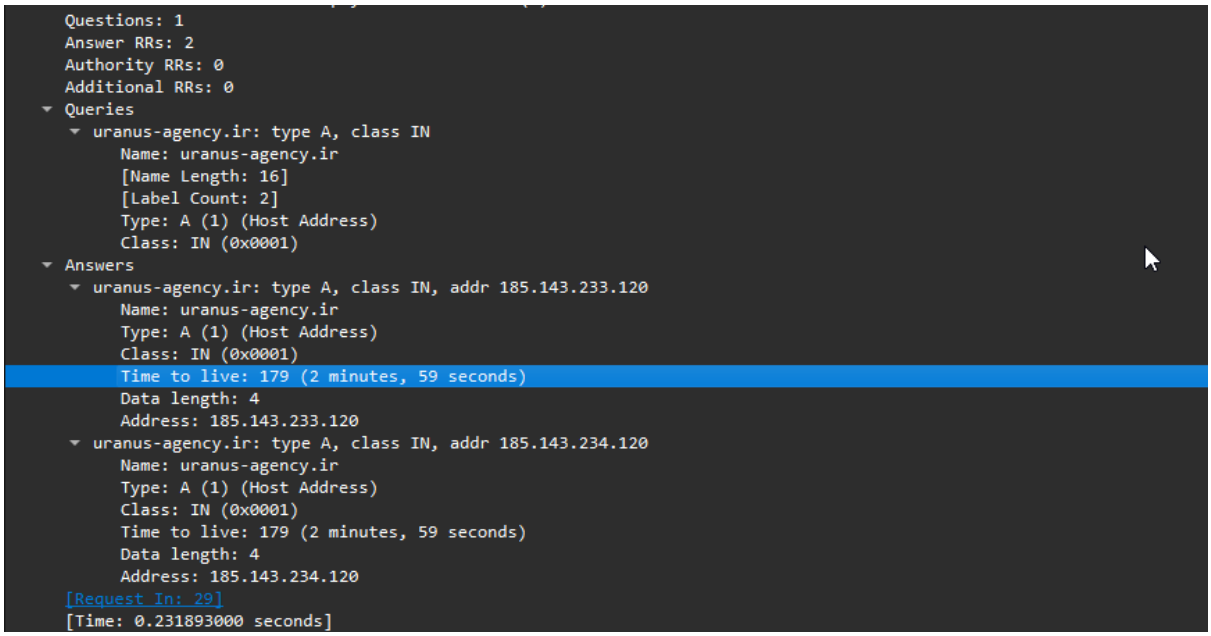
داخل بسته‌های فوق برای destination همان آدرس سرور DNS محلی که در تصاویر گذشته مشاهده کردیم نوشته شده است. پس بسته‌های کوئری استاندارد DNS برای آن ارسال شده و پاسخ استاندارد هم از همان آدرس برای ما برمی‌گردد.

الته ما می‌توانیم سرور DNS را خودمان در دستور nslookup مشخص کنیم و آدرس آن را دستی وارد کنیم. اما اگر وارد نکنیم سلسه‌مراتب کوئری DNS اجرا می‌شود.

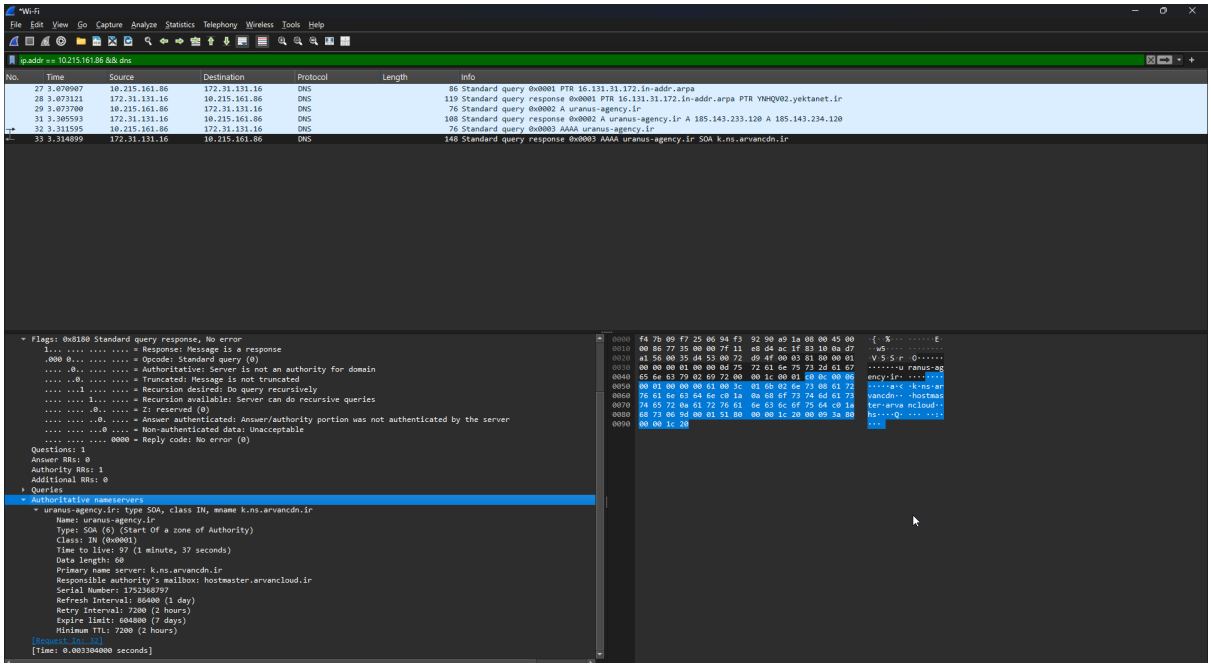
سوال ۲.



یک نمونه بسته کوئری استاندارد به این صورت است. در اولین فلگ مشخص شده که این کوئری از نوع جواب است یا نه. که در این بسته مقدار ۰ درج شده به این معنی که این بسته از نوع کوئری است. اما در پاسخ، مقدار این فلگ برابر ۱ شده است. همچنین داخل اطلاعات مربوط به کوئری نوشته شده که تایپ درخواست ما A است. پس رکورد A مربوط به دامنه‌ی درخواست داده شده را برای ما برمی‌گرداند.



داخل بسته پاسخ هم برای این درخواست ۲ جواب برگردانده شده است. پس این دامنه ۲ آیپی ادرس دارد که بین آن‌ها load balancing انجام می‌شود . همچنین داخل جواب‌ها به ازای هر کدام از آیپی‌ها یک TTL برگردانده شده است که نشان می‌دهد ما می‌توانیم این مقدار را به مدت ۳ دقیقه در سرور DNS لوکال خود کش کنیم و پس از آن دوباره به سرور DNS اصلی کوئری ارسال کنیم.



پس از آن مشاهده می‌کنیم که یک کوئری از نوع AAAA هم برای به دست آوردن IPv6 این دامنه ارسال شده است. اما چون برای این دامنه من آیپی ورژن ۶ تنظیم نکردم، در ریسپانس فقط اطلاعات Authoritative nameserver برگردانده شده است که مربوط به ابرآروان است.

همچنین باقی فلگ‌های موجود در هدر داخل بخش flags تصویر فوق قابل مشاهده است. جلوی هر کدام توضیحاتی نوشته شده که مشخص می‌کند هر کدام چه کاربردی دارند و مقدارشان در حال حاضر چند است.