

# آزمایشگاه شبکه‌های کامپیوتری

نیمسال سوم ۱۴۰۳-۰۴

استاد: دکتر بردیا صفائی



دانشکده مهندسی کامپیوتر

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

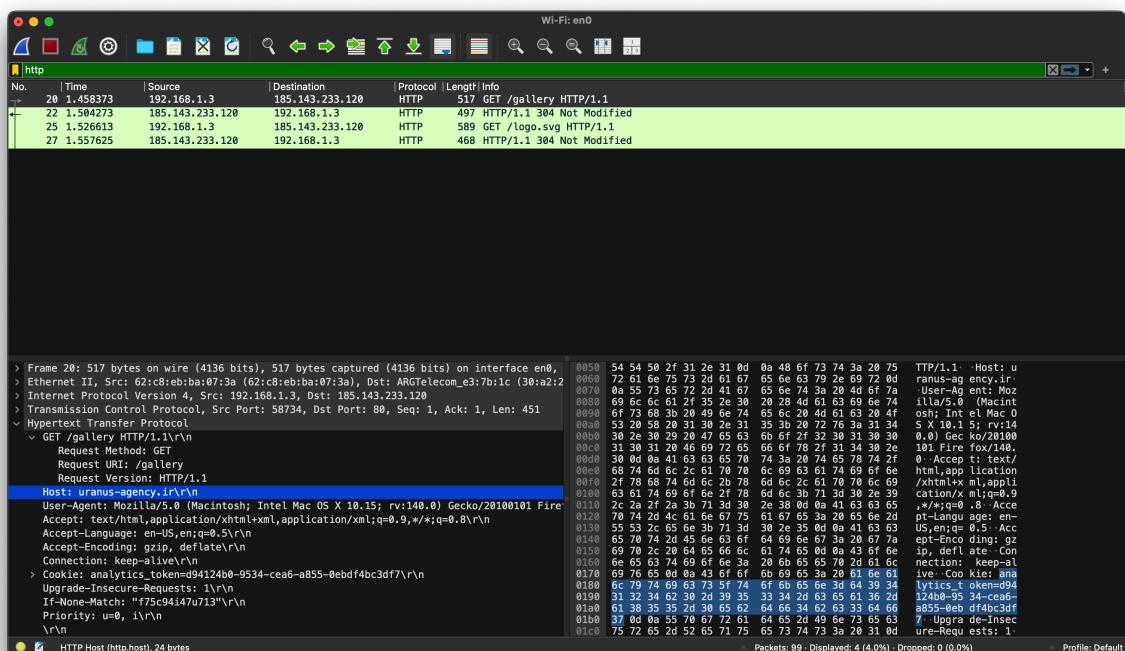
## گزارش آزمایش شماره ۲

### فهرست مطالب

- ۱ فهم اولیه از HTTP
- ۵ بررسی ارتباط از طریق Telnet
- ۸ بررسی درخواست و پاسخ‌های DNS

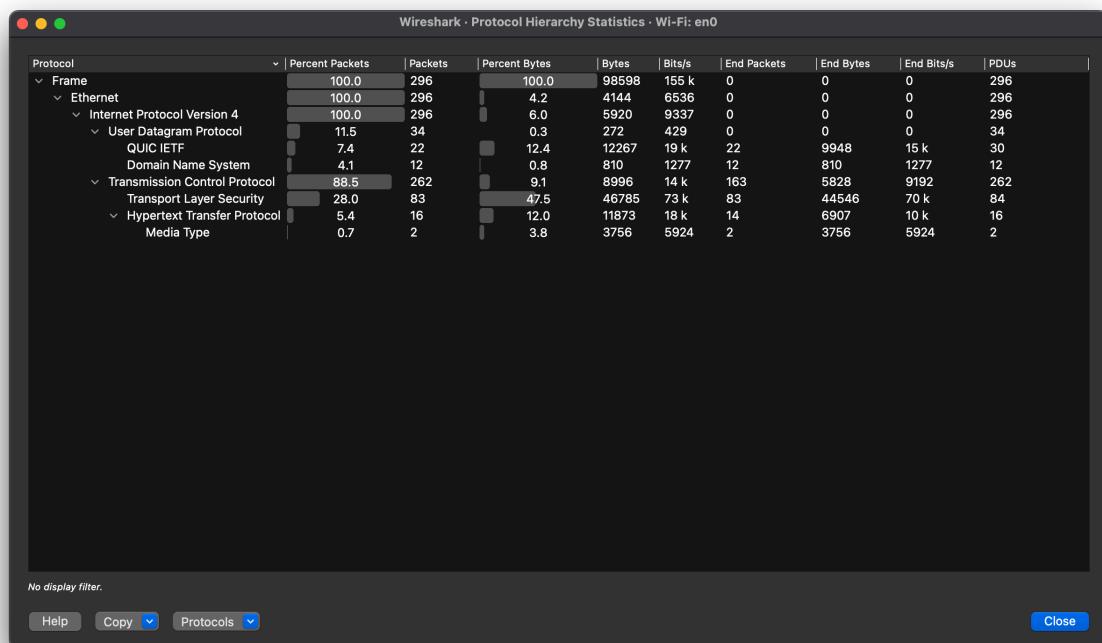
### فهم اولیه از HTTP

ابتدا نرم‌افزار Wireshark را باز کرده و روی حالت capture قرار می‌دهیم، سپس وب‌سایت <https://uranus-agency.ir/gallery/> را باز می‌کنیم. در نهایت capture را متوقف می‌کنیم و پکت‌ها را مشاهده می‌کنیم:



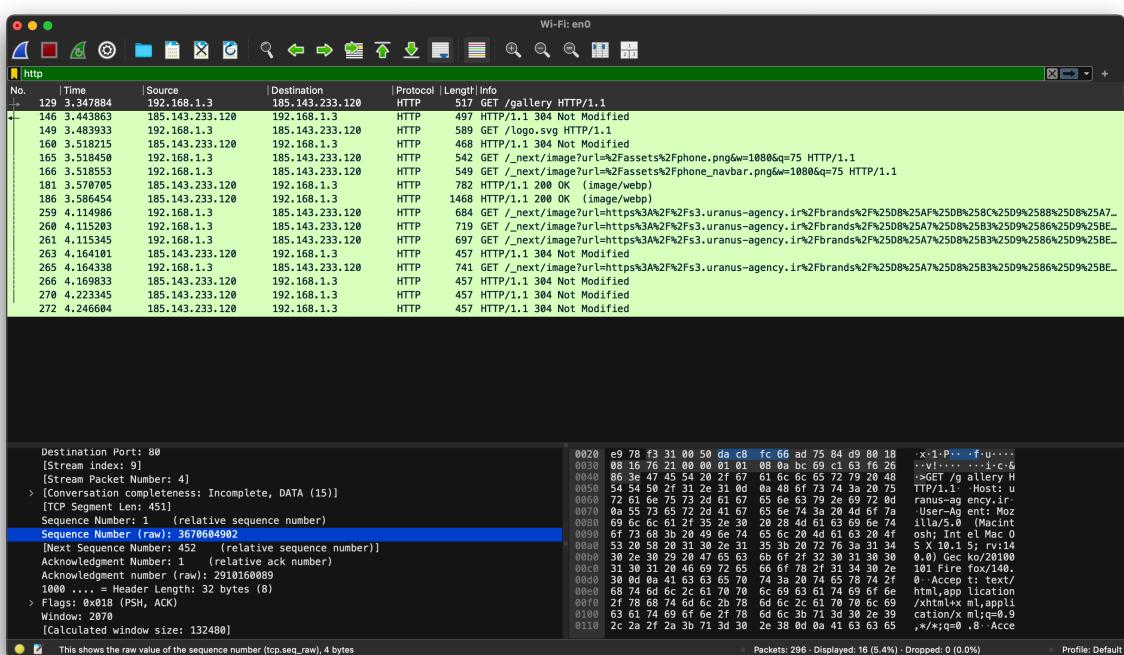
سوال ۱.

از گزینه protocol-hierarchy statistics کلیک می‌کنیم.

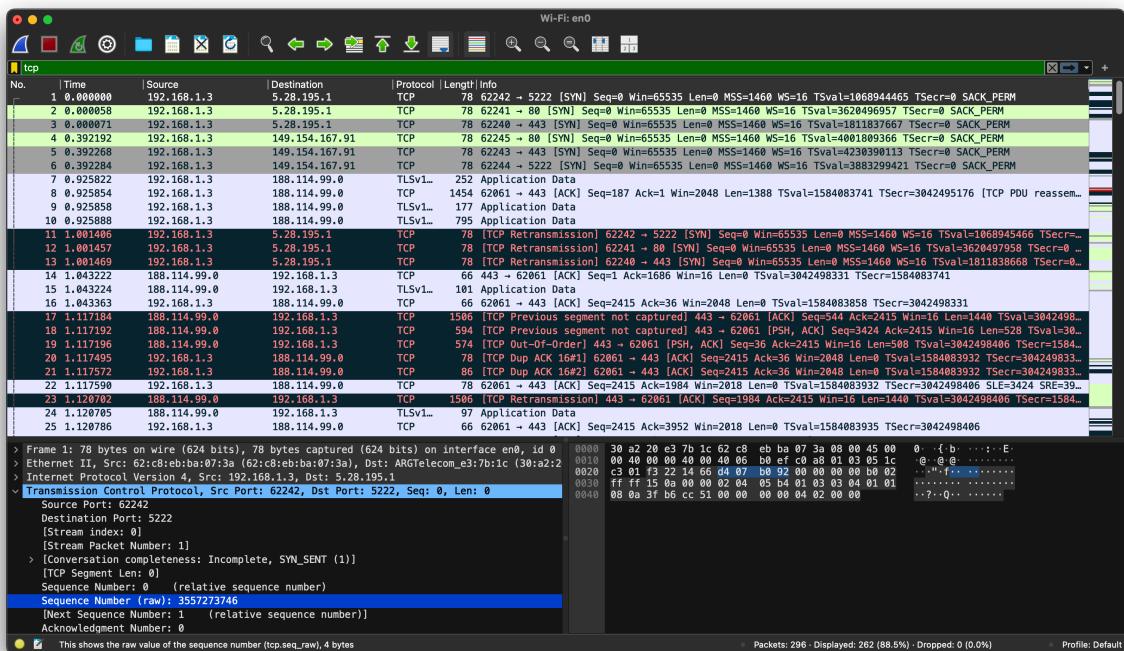


- تمامی پکت‌ها از لایه لینک عبور کرده‌اند.
- ۱۰۰ درصد بسته‌ها از پروتوكول IPv4 استفاده کرده‌اند.
- حدوداً ۸۸ درصد از بسته‌ها از پروتوكول TCP بر بستر IPv4 استفاده کرده‌اند.
- ۱۲ درصد بسته‌ها از پروتوكول UDP بر بستر IPv4 استفاده کرده‌اند.

## سوال ۲.

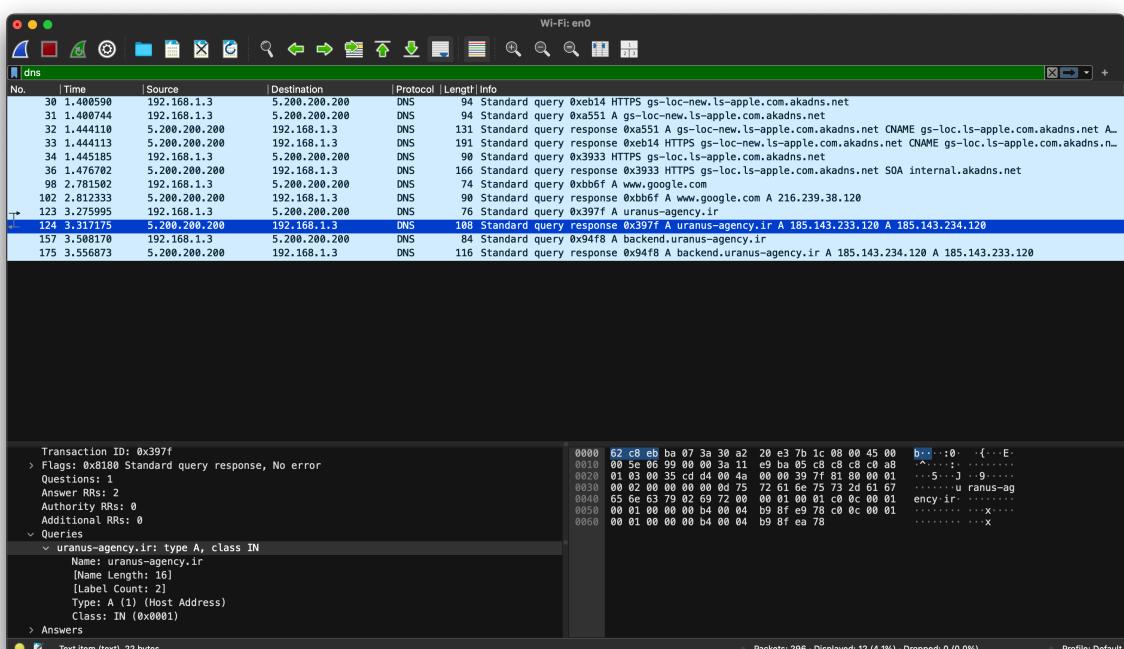


بسته شماره ۱۲۹ به مقصد رسیده و میزبان در بسته ۱۴۶ پاسخ با کد ۳۰۰ داده است یعنی این عکس تغییر نکرده و باید از کش خوانده شود. اختلاف زمانی این دو بسته در ستون دوم مشخص است. می‌توان بسته ۱۶۵ و ۱۸۱ را هم مشاهده کرد که درخواست عکس را دارد و پاسخ http ok را دریافت کرده است.



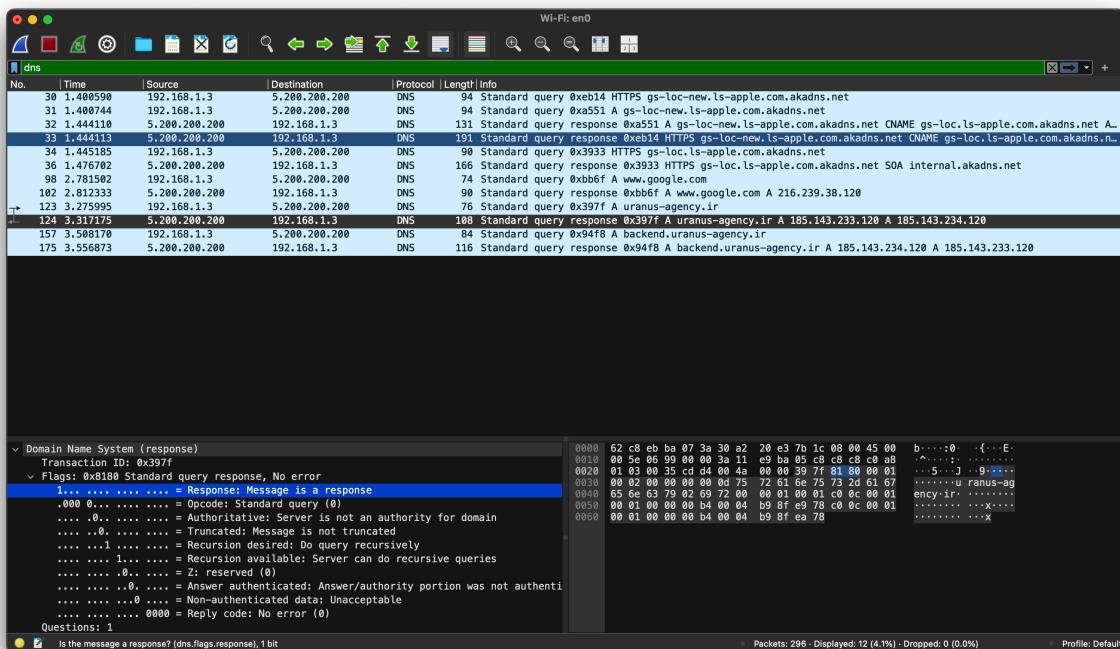
همچنین شماره ترتیب مطلق اولین ارتباط TCP برابر است با ۳۵۵۷۲۷۳۷۴۶.

### سوال ۳



کوئری‌های درخواست DNS از نوع Standard DNS Query هستند.

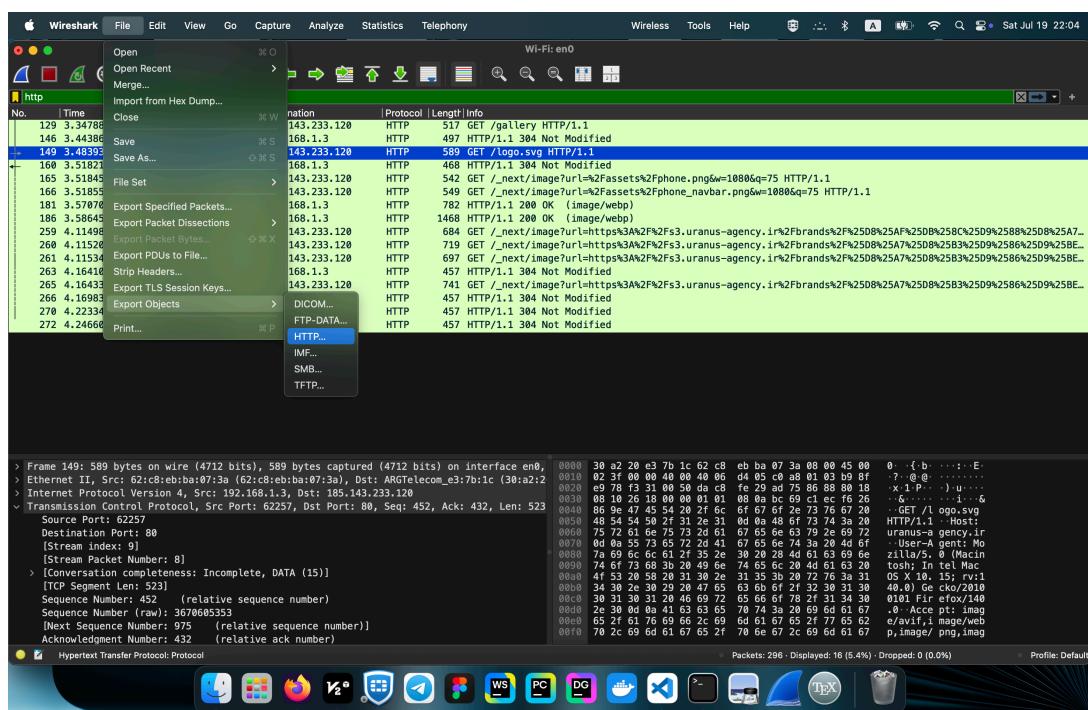
کوئری و پاسخ DNS هر دو از یک نوع هستند با این تفاوت که در پاسخ، فلگ پاسخ فعال است و پاسخ را هم به همراه دارد.  
همچنین نوع رکورد درخواست شده از نوع A است.



در شکل فوق مشخص است که فلگ پاسخ برابر ۱ شده است و نوع رکود هم نوشته شده است و برابر A است.

#### سوال ۴.

برای ذخیره کردن عکس‌ها، پکت درخواست آن عکس را سلکت کرده و سپه و سپس مشابه تصویر زیر عمل می‌کنیم:

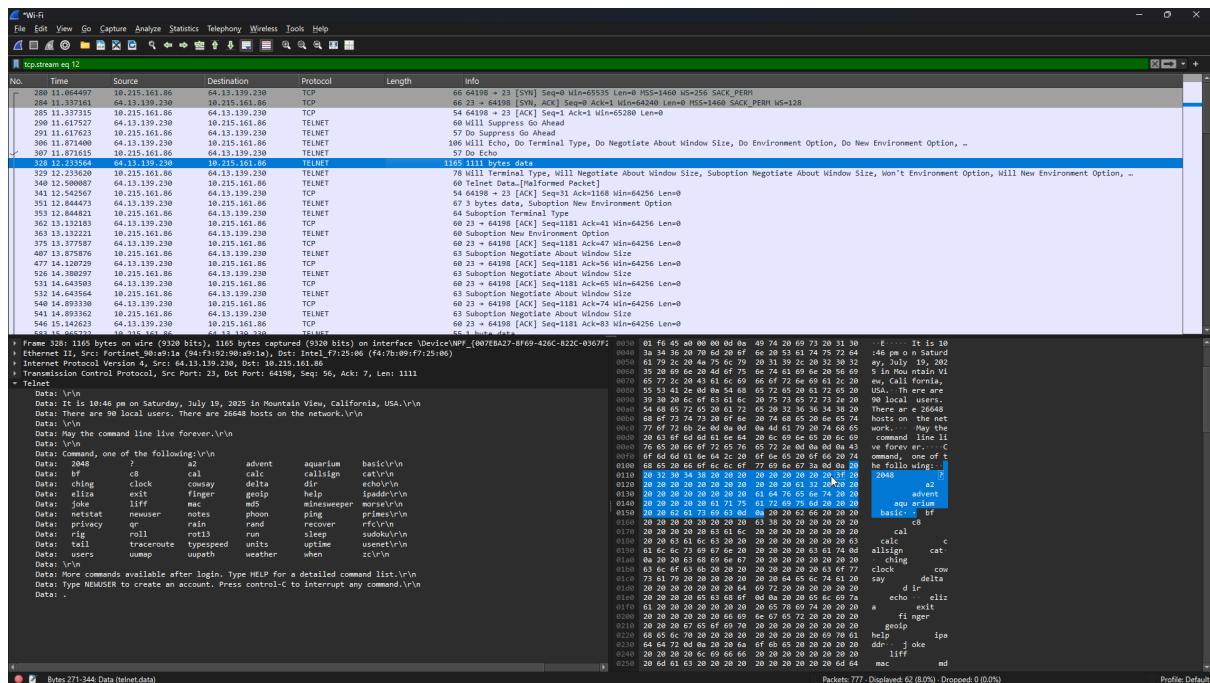


## بررسی ارتباط از طریق Telnet

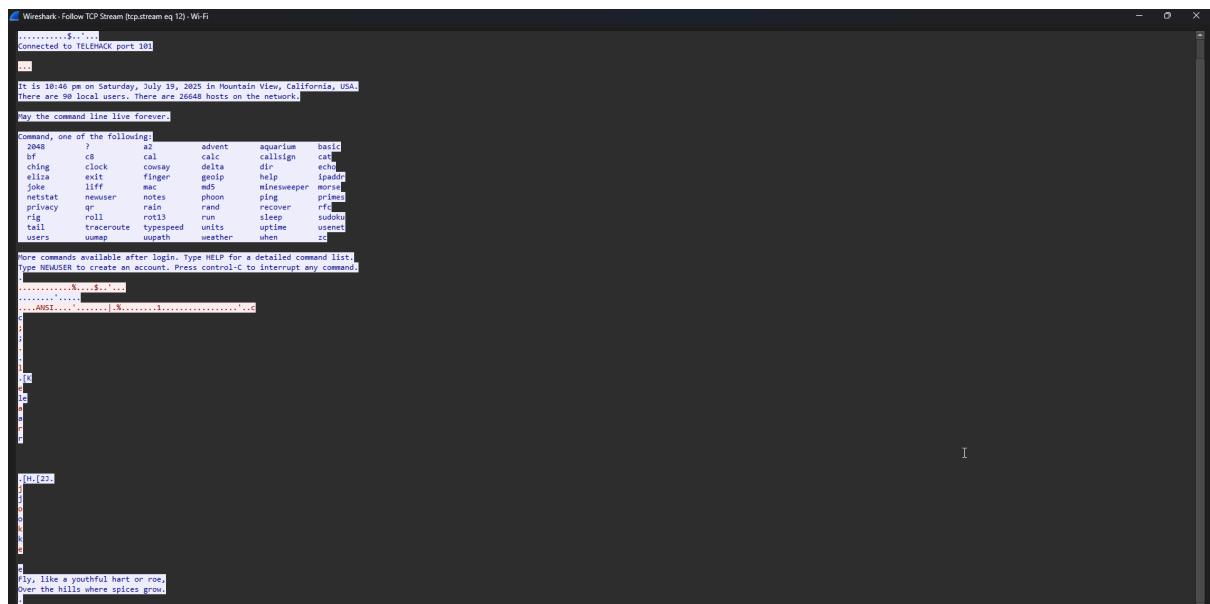
در ابتدای نیاز است تا telnet را روی ویندوز فعال کنیم. وارد control panel می‌شویم و در بخش گزینه‌ی Programs را انتخاب می‌کنیم. سپس به دنبال telnet client می‌گردیم و آن را فعال می‌کنیم. Turn Windows features on or off

حال وارد cmd شده و با استفاده از دستور telehack.com بر روی interface اینترنت خود قرار دهیم. البته قبل از آن باید wireShark را در حالت capture شروع کنیم. سپس تعدادی از دستورات را امتحان کرده و در نهایت capture را متوقف می‌کنیم.

در این قسمت 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 follow را انتخاب می‌کنیم.

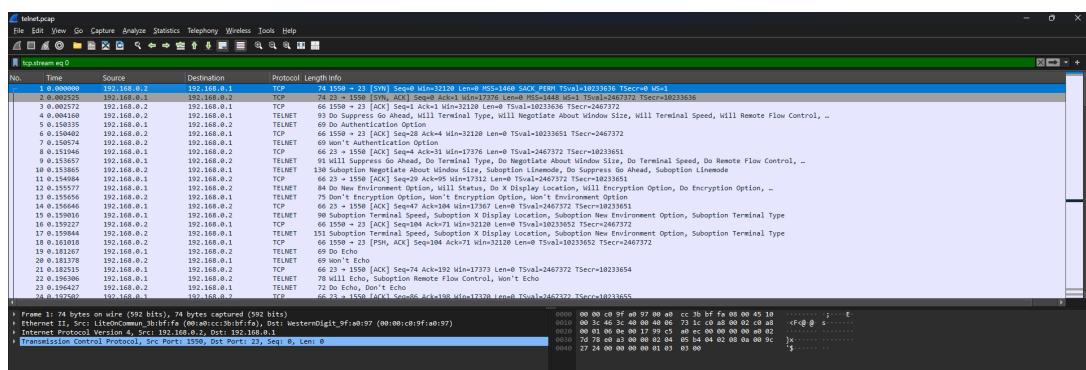


همانطور که در تصویر مشخص است، من با استفاده از کامند joke درخواست یک جوک کردم و در اخیرین بسته این جوک به دست من رسیده است.

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 پروتوكول مورد توجه قرار می‌گیرد، این است که پیام‌ها و بسته‌ها به صورت رمزگاری نشده رد و بدل می‌شود که نشان دهنده امنیت پایین‌تر این پروتوكول نسبت به پروتوكول‌های دیگر نظیر SSH است.

## سوال ۱.

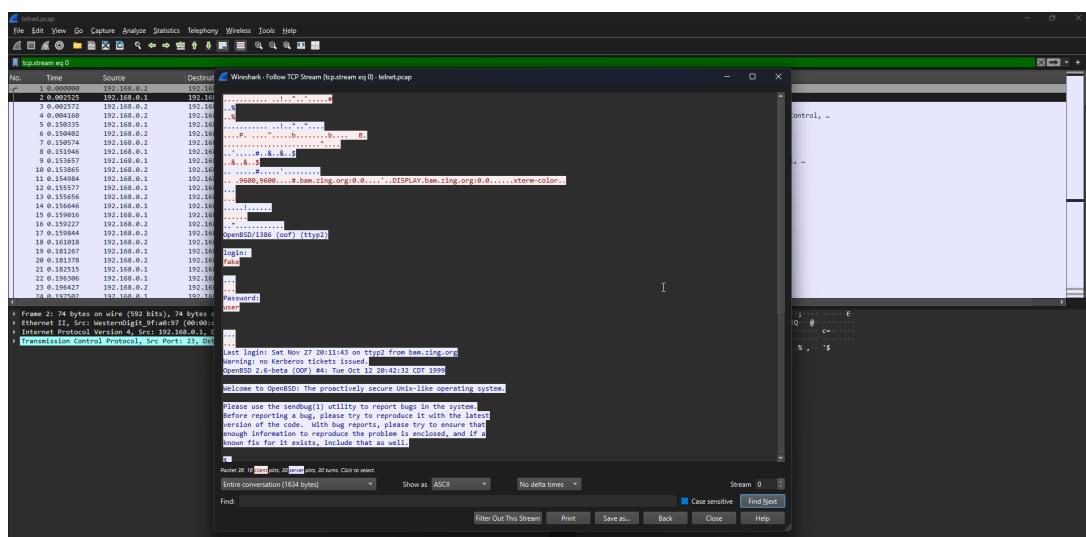


همانطور که در شکل فوق مشخص است، آیپی Source در اولین پکت ۱۹۲.۱۶۸.۰.۲ است که مربوط به کلاینت است و آیپی ۱۹۲.۱۶۸.۰.۱ مربوط به سرور است.

در سه بسته اول که از نوع TCP است فرایند TCP-Handshaking در حال انجام است و منظقاً اولین پکت از سمت کلاینت ارسال شده است.

## سوال ۲.

بر روی اولین پکت مربوط به این گفت‌و‌گو کلیک راست کرده و از منو گزینه‌ی follow TCP Stream را انتخاب می‌کنیم.



داخل تصویر فوق مشخص است که یوزرنیم و پسورد چه مقداری دارند. چون telnet پیام‌ها را رمزگاری نمی‌کند، یوزرنیم و پسورد کلاینت به صورت raw داخل بسته‌های ارسالی قابل مشاهده است.

## سوال ۳

نیاز نیست کار سختی انجام دهیم، کافیست مجدد روی TCP Stream کلیک کنیم. پیام‌های قرمز از سمت کلاینت و پیام‌های آبی از سمت سرور هستند.

کاربر پس از لاگین، این دستورات را اجرا کرده است:

```
$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
.....
.....
--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
. .. .cshrc .login .mailrc .profile .rhosts
$ exit
```

## بررسی درخواست و پاسخ‌های DNS

ابتدا cmd را باز کرده و با استفاده از دستور ipconfig /flushdns 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

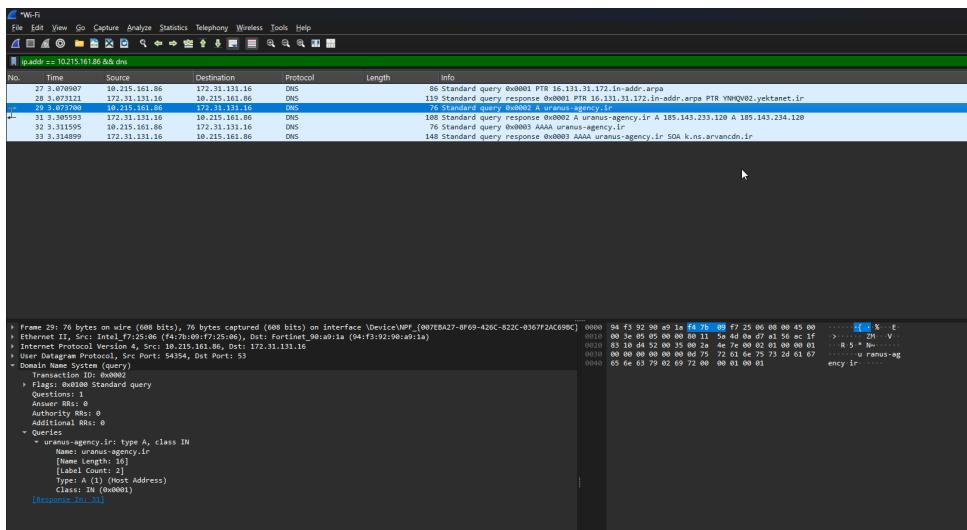
Non-authoritative answer:
Name: uranus-agency.ir
Addresses: 185.143.233.120
185.143.234.120

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 uranus-agency.ir که آدرس آیپی آن هم در تصویر موجود است.

حال داخل wireshark فیلتر آیپی خودمان و فیلتر بسته‌های DNS را اعمال می‌کنیم تا 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

```

> Frame 29: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{007EBA27-8F69-426C-822C-0367F2AC69BC}
> Ethernet II, Src: Intel_f7:25:06 (f4:7b:09:f7:25:06), Dst: Fortinet_90:a9:1a (94:f3:92:90:a9:1a)
> Internet Protocol Version 4, Src: 10.215.161.86, Dst: 172.31.131.16
> User Datagram Protocol, Src Port: 54354, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0002
  Flags: 0x0100 Standard query
    0... .... .... = Response: Message is a query
    .000 0.... .... = Opcode: Standard query (0)
    .... 0.... .... = Truncated: Message is not truncated
    .... 1.... .... = Recursion desired: Do query recursively
    .... 0.... .... = Z: reserved (0)
    .... 0.... .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > uranus-agency.ir: type A, class IN
      Name: uranus-agency.ir
      [Name Length: 16]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Response In: 31]

```

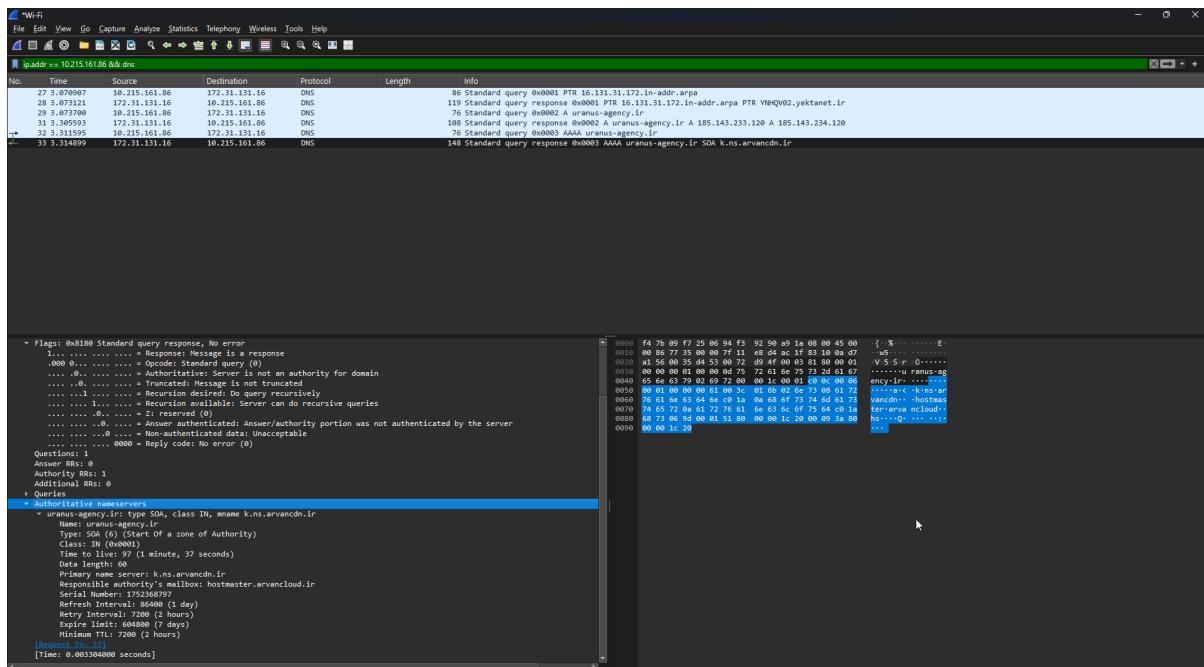
یک نمونه بسته کوئری استاندارد به این صورت است. در اولین فلگ مشخص شده که این کوئری از نوع جواب است یا نه. که در این بسته مقدار ۰ درج شده به این معنی که این بسته از نوع کوئری است. اما در پاسخ، مقدار این فلگ برابر ۱ شده است. همچنین داخل اطلاعات مربوط به کوئری نوشته شده که تایپ درخواست ما A است. پس رکورد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

```

Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
  > Queries
    > uranus-agency.ir: type A, class IN
      Name: uranus-agency.ir
      [Name Length: 16]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  > Answers
    > uranus-agency.ir: type A, class IN, addr 185.143.233.120
      Name: uranus-agency.ir
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 179 (2 minutes, 59 seconds)
      Data length: 4
      Address: 185.143.233.120
    > uranus-agency.ir: type A, class IN, addr 185.143.234.120
      Name: uranus-agency.ir
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 179 (2 minutes, 59 seconds)
      Data length: 4
      Address: 185.143.234.120
      [Request In: 29]
      [Time: 0.231893000 seconds]

```

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 لوكال 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 دارم که مریبوط 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.