به نام خدا

آزمایشگاه شبکه‌های کامپیوتری

گزارش آزمایش دوم

استاد:

دکتر حمید بیگی

نویسندگان :

محمدهومان کشوری

هیربد بهنام

علی نظری

شماره دانشجویی :

99105667

99171333

99102401

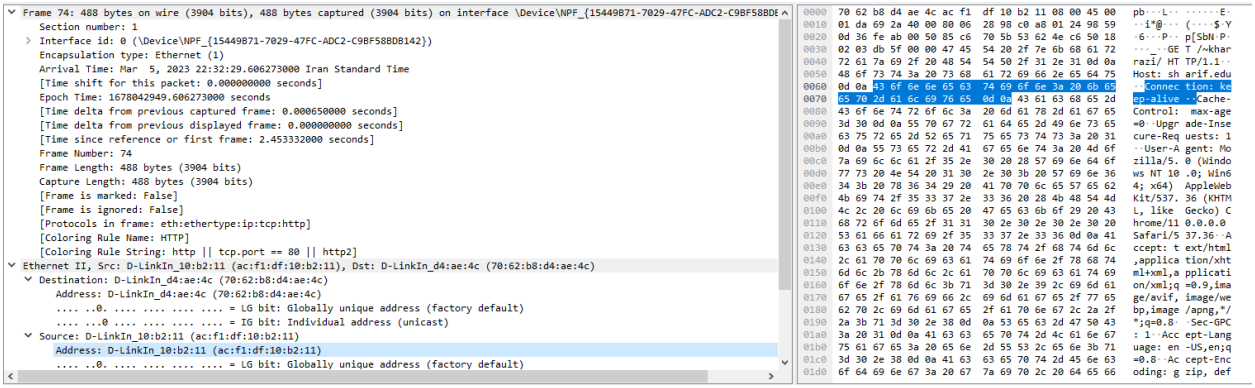
راه حل

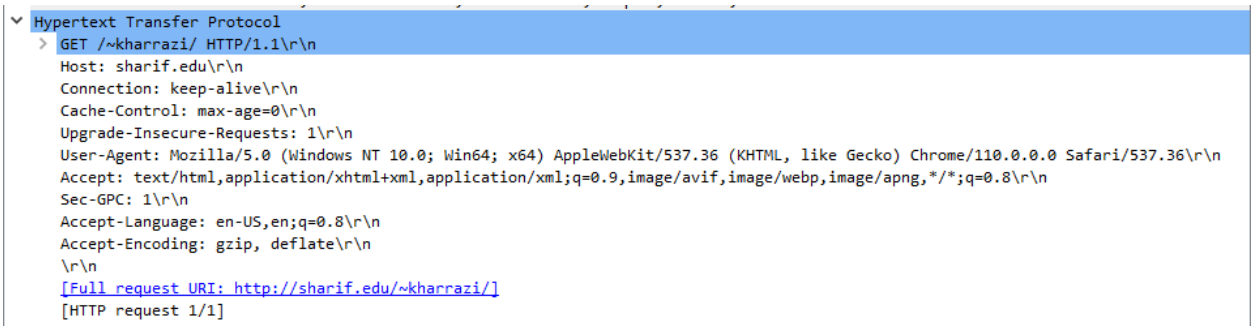
بخش اول

در این بخش، نخست مرورگر دلخواه را باز می‌کنیم. سپس wireshark را در حالت capture قرار می‌دهیم. سپس یک سایت دارای عکس را در نظر می‌گیریم و آن را باز می‌کنیم. ما سایت http://sharif.edu/~kharrazi را برای این موضوع انتخاب کردیم. بعد از باز کردن این سایت، capture کردن wireshark را stop می‌کنیم. سپس در بخش filter کاری می‌کنیم که فقط http ها را ببینیم و نتیجه مانند عکس زیر می‌شود:

No.	Time	Source	Destination	Protocol	Length	Info
74	2.453332	192.168.1.36	152.89.13.54	HTTP	488	GET /~kharrazi/ HTTP/1.1
82	2.511329	152.89.13.54	192.168.1.36	HTTP	677	Continuation
90	2.546737	152.89.13.54	192.168.1.36	HTTP	435	Continuation

همانطور که می‌بینیم، نخستین مورد همان GET است. اطلاعات آن را در بخش زیر می‌توانیم مشاهده کنیم:





همانطور که می‌بینیم، host و URL مدنظر، همان است که ما در مرورگر وارد کردیم.

سوالات:

۱- از گزینه statistics و سپس protocol hierarchy استفاده می‌کنیم.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	152	100.0	29159	45 k	0	0	0	152
Ethernet	100.0	152	7.3	2128	3305	0	0	0	152
Internet Protocol Version 6	0.7	1	0.1	40	62	0	0	0	1
Internet Control Message Protocol v6	0.7	1	0.1	24	37	1	24	37	1
Internet Protocol Version 4	98.0	149	10.2	2980	4628	0	0	0	149
User Datagram Protocol	20.4	31	0.9	248	385	0	0	0	31
Simple Service Discovery Protocol	5.3	8	5.2	1510	2345	8	1510	2345	8
NetBIOS Name Service	5.9	9	1.5	450	698	9	450	698	9
Multicast Domain Name System	2.6	4	0.5	160	248	4	160	248	4
Domain Name System	2.6	4	0.6	188	291	4	188	291	4
Data	3.9	6	9.3	2709	4207	6	2709	4207	6
Transmission Control Protocol	77.0	117	63.6	18542	28 k	113	16962	26 k	117
Hypertext Transfer Protocol	2.0	3	18.9	5518	8570	3	5518	8570	3
Domain Name System	0.7	1	0.2	64	99	1	64	99	1
Internet Control Message Protocol	0.7	1	0.4	124	192	0	0	0	1
Domain Name System	0.7	1	0.3	88	136	1	88	136	1
Address Resolution Protocol	1.3	2	0.2	56	86	2	56	86	2

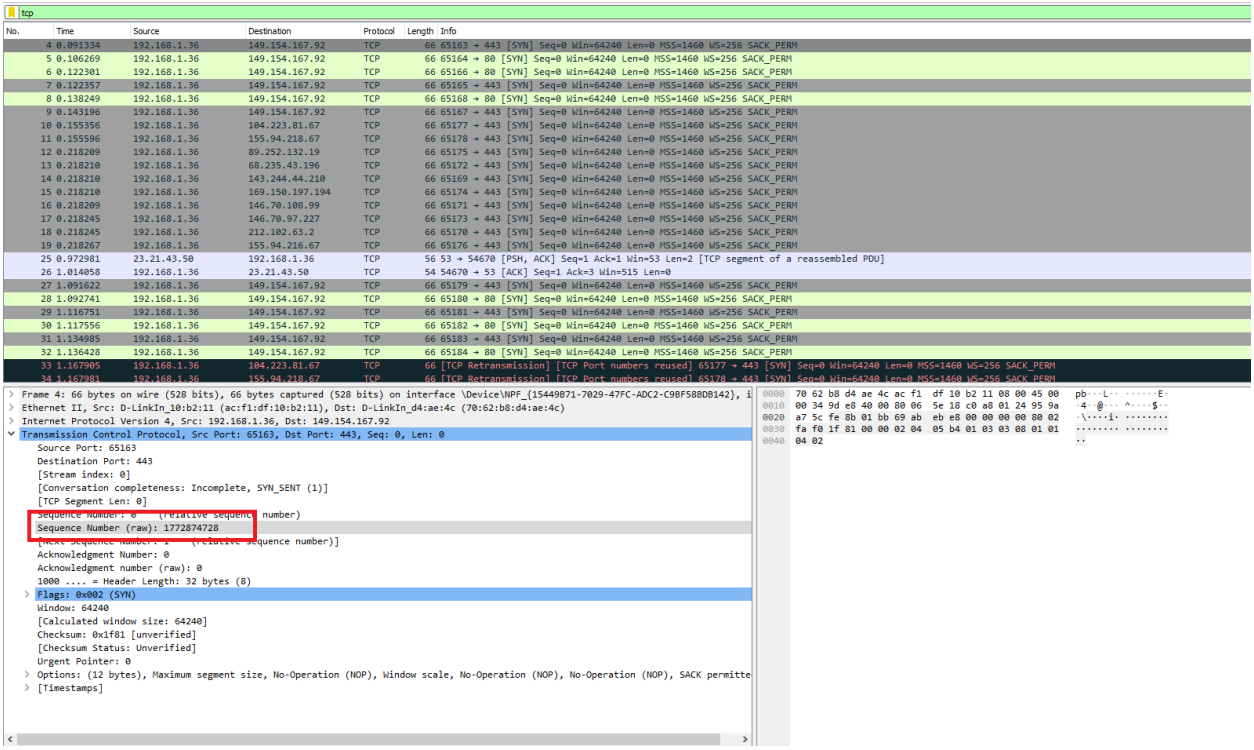
نتیجه به این شکل است. با توجه به عکس بالا:

- تمامی بسته‌ها از لایه لینک و فیزیکی عبور کرده‌اند.
- حدود ۹۸ درصد بسته‌ها از پروتکل IPV4 استفاده کرده‌اند در لایه شبکه.
- حدود ۷۳ درصد بسته‌ها در لایه انتقال از پروتکل TCP استفاده کرده‌اند.
- در رده بهد در لایه انتقال، UDP قرار دارد.
- در لایه کاربرد هم بیشترین سهم برای HTTP است برای بسته‌ها.

۲-

No.	Time	Source	Destination	Protocol	Length	Info
74	2.453332	192.168.1.36	152.89.13.54	HTTP	488	GET /~kharrazi/ HTTP/1.1
82	2.511329	152.89.13.54	192.168.1.36	HTTP	677	Continuation
90	2.546737	152.89.13.54	192.168.1.36	HTTP	435	Continuation

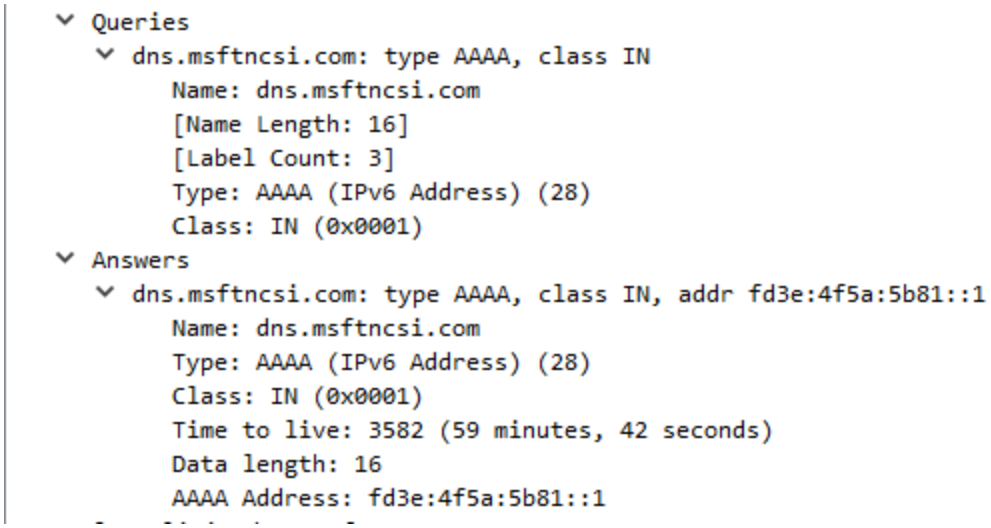
زمان‌ها در ستون دوم قابل مشاهده است و سطر اول ارسال درخواست است و سطر نهایی هم بخش acknowledgement که پایان درخواست است و اختلاف آنها حدود ۰.۰۹ ثانیه است. شماره ترتیب مطلق اولین ارتباط TCP هم به شکل زیر است:

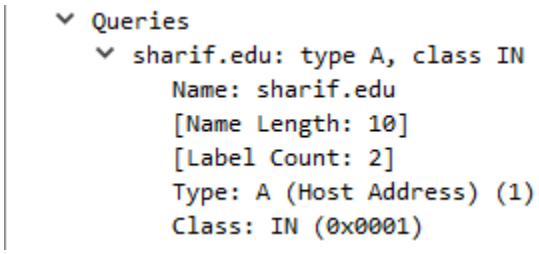


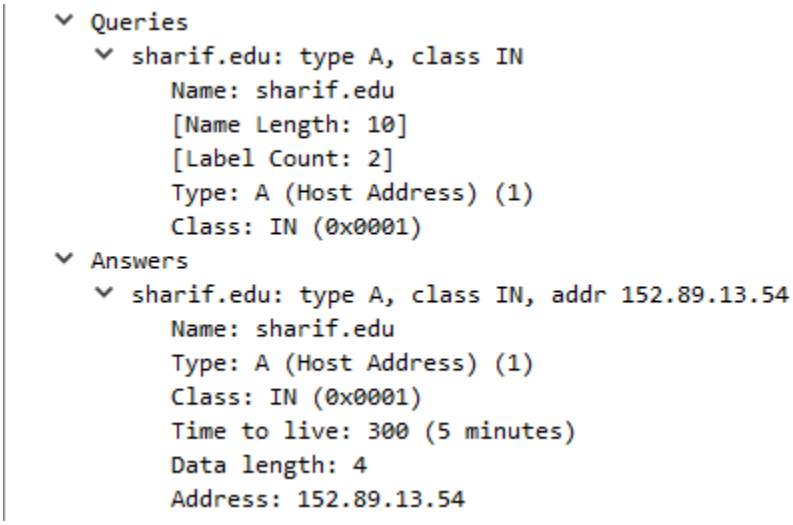
و می‌بینیم که این عدد برابر با ۲۵۱۹۰۵۰۹۲۹ است. دقت کنید که فیلتر را بر روی TCP قرار دادیم.

۳- درخواست های DNS و پاسخ آن هر دو در قالب درخواست استاندارد DNS ارسال و دریافت می شوند. تفاوت یک بسته ی پاسخ با بسته ی پرسش آن است که در بسته ی پاسخ، بیت پاسخ بودن بسته یک است و در بسته های پرسش صفر. همچنین بسته های پرسش تنها شامل پرسش مورد نظر هستند ولی بسته های پاسخ تکمیل شده ی بسته ی پرسش با اضافه شدن پاسخ آن هستند.

کوئری‌های DNS موجود در این فایل از دو نوع A و AAAA هستند. پاسخ کوئری‌های با نوع A از نوع A و پاسخ کوئری‌های از نوع AAAA باید از نوع همان AAAA باشند اما چون شریف IPV6 ندارد پاسخ آمده از نوع SOA هست.


Queries
dns.msftncsi.com: type AAAA, class IN
Name: dns.msftncsi.com
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers
dns.msftncsi.com: type AAAA, class IN, addr fd3e:4f5a:5b81::1
Name: dns.msftncsi.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 3582 (59 minutes, 42 seconds)
Data length: 16
AAAA Address: fd3e:4f5a:5b81::1


Queries
sharif.edu: type A, class IN
Name: sharif.edu
[Name Length: 10]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)


Queries
sharif.edu: type A, class IN
Name: sharif.edu
[Name Length: 10]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
sharif.edu: type A, class IN, addr 152.89.13.54
Name: sharif.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 152.89.13.54

```
Domain Name System (response)
    Length: 62
    Transaction ID: 0x0001
  ▾ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ dns.msftncsi.com: type AAAA, class IN
        Name: dns.msftncsi.com
        [Name Length: 16]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  ▾ Answers
    ▾ dns.msftncsi.com: type AAAA, class IN, addr fd3e:4f5a:5b81::1
        Name: dns.msftncsi.com
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 3582 (59 minutes, 42 seconds)
        Data length: 16
        AAAA Address: fd3e:4f5a:5b81::1
    [Unsolicited: True]
```

```
▾ Domain Name System (query)
    Transaction ID: 0xdcf5
  ▾ 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
    ▾ sharif.edu: type A, class IN
        Name: sharif.edu
        [Name Length: 10]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 70]
```

۴- با استفاده از نرم افزار Wireshark و از طریق گزینه ی File سپس Export Objects سپس HTTP و در نهایت Save می توان تصاویر مورد نظر را انتخاب کرده و در مکانی دلخواه ذخیره کرد. تصاویر ذخیره شده از وبسایت به پیوست این گزارش ارسال شده اند.

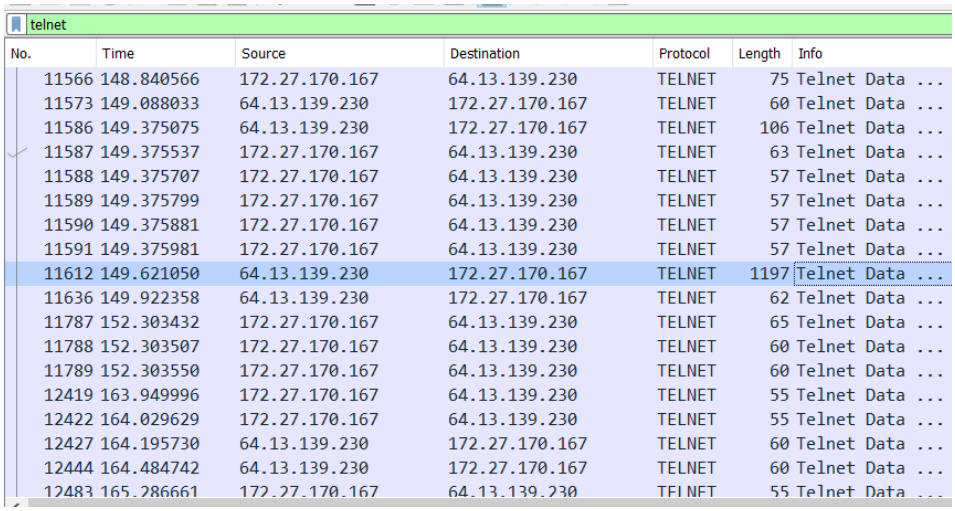
Packet	Hostname	Content Type	Size	Filename
90	sharif.edu		5 bytes	~kharrazi

بخش دوم

برای اتصال از putty استفاده می‌کنیم و پس از وصل شدن به telehack.com، چندین دستور را به صورت تصادفی انتخاب می‌کنیم.

دستورات انتخاب شده : joke, calc, help

حال خروجی دستورات را بررسی می‌کنیم.



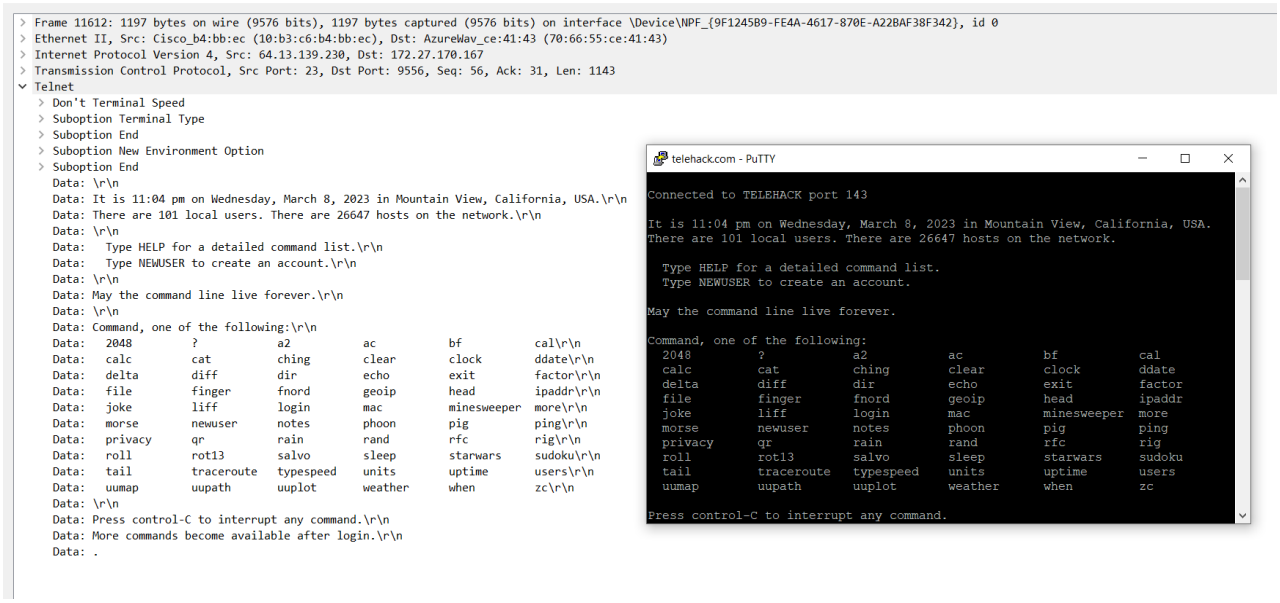
telnet

No.	Time	Source	Destination	Protocol	Length	Info
11566	148.840566	172.27.170.167	64.13.139.230	TELNET	75	Telnet Data ...
11573	149.088033	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
11586	149.375075	64.13.139.230	172.27.170.167	TELNET	106	Telnet Data ...
11587	149.375537	172.27.170.167	64.13.139.230	TELNET	63	Telnet Data ...
11588	149.375707	172.27.170.167	64.13.139.230	TELNET	57	Telnet Data ...
11589	149.375799	172.27.170.167	64.13.139.230	TELNET	57	Telnet Data ...
11590	149.375881	172.27.170.167	64.13.139.230	TELNET	57	Telnet Data ...
11591	149.375981	172.27.170.167	64.13.139.230	TELNET	57	Telnet Data ...
11612	149.621050	64.13.139.230	172.27.170.167	TELNET	1197	Telnet Data ...
11636	149.922358	64.13.139.230	172.27.170.167	TELNET	62	Telnet Data ...
11787	152.303432	172.27.170.167	64.13.139.230	TELNET	65	Telnet Data ...
11788	152.303507	172.27.170.167	64.13.139.230	TELNET	60	Telnet Data ...
11789	152.303550	172.27.170.167	64.13.139.230	TELNET	60	Telnet Data ...
12419	163.949996	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
12422	164.029629	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
12427	164.195730	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
12444	164.484742	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
12483	165.286661	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...

همانطور که واضح است برای ردیابی پیام‌ها از فیلتر telnet استفاده می‌کنیم.

مشاهده می‌کنیم که **مبدا ما 172.27.170.167** است و **مقصد نیز 64.13.139.230**.

حال پیامی که طول آن از بقیه بیشتر از بقیه است را بررسی می‌کنیم.



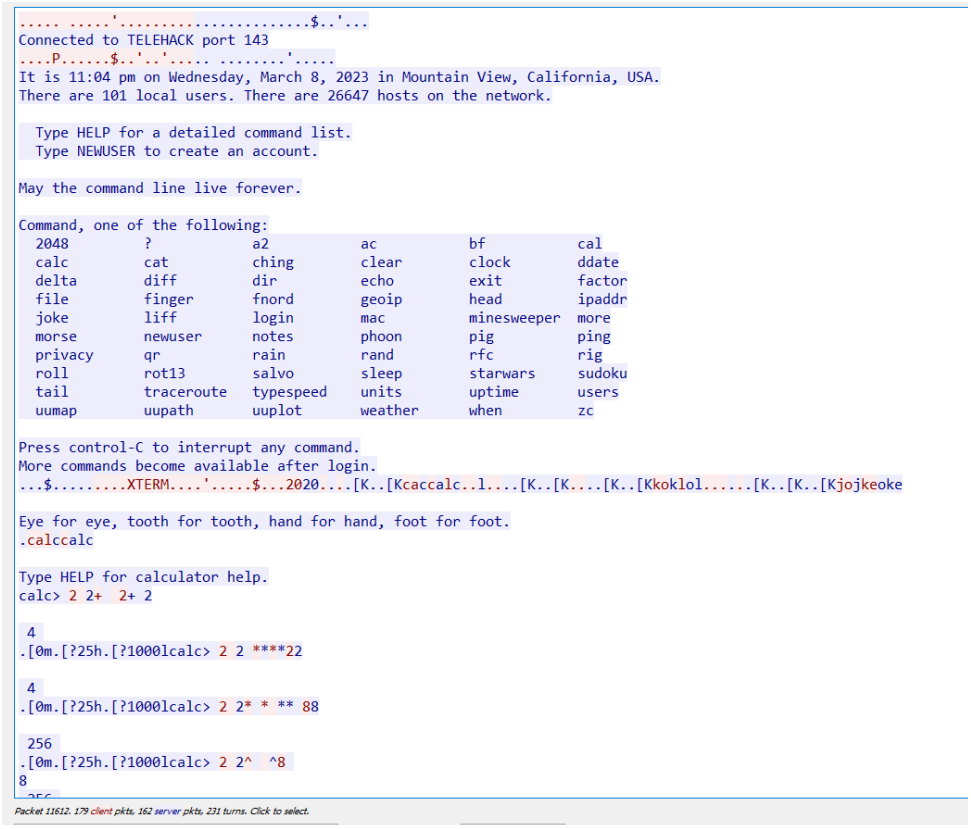
```
> Frame 11612: 1197 bytes on wire (9576 bits), 1197 bytes captured (9576 bits) on interface \Device\NPF_{9F1245B9-FE4A-4617-870E-A22BAF38F342}, id 0
> Ethernet II, Src: Cisco_b4:bb:ec (10:b3:c6:b4:bb:ec), Dst: AzureWav_ce:41:43 (70:66:55:ce:41:43)
> Internet Protocol Version 4, Src: 64.13.139.230, Dst: 172.27.170.167
> Transmission Control Protocol, Src Port: 23, Dst Port: 9556, Seq: 56, Ack: 31, Len: 1143
v Telnet
  > Don't Terminal Speed
  > Suboption Terminal Type
  > Suboption End
  > Suboption New Environment Option
  > Suboption End
    Data: \r\n
    Data: It is 11:04 pm on Wednesday, March 8, 2023 in Mountain View, California, USA.\r\n
    Data: There are 101 local users. There are 26647 hosts on the network.\r\n
    Data: \r\n
    Data:   Type HELP for a detailed command list.\r\n
    Data:   Type NEWUSER to create an account.\r\n
    Data: \r\n
    Data: May the command line live forever.\r\n
    Data: \r\n
    Data: Command, one of the following:\r\n
    Data:   2048        ?           a2          ac          bf          cal\r\n
    Data:   calc        cat         ching       clear       clock       ddate\r\n
    Data:   delta       diff        dir         echo        exit        factor\r\n
    Data:   file        finger      fnord       geoip       head        ipaddr\r\n
    Data:   joke        liff        login       mac         minesweeper more\r\n
    Data:   morse       newuser     notes       phoon       pig         ping\r\n
    Data:   privacy     qr          rain        rand        rfc         rig\r\n
    Data:   roll        rot13       salvo       sleep       starwars    sudoku\r\n
    Data:   tail        traceroute  typespeed   units       uptime      users\r\n
    Data:   uumap       uupath      uuplot      weather     when        zc\r\n
    Data: \r\n
    Data: Press control-C to interrupt any command.\r\n
    Data: More commands become available after login.\r\n
    Data: .
```

telehack.com - PuTTY

```
Connected to TELEHACK port 143

It is 11:04 pm on Wednesday, March 8, 2023 in Mountain View, California, USA.
There are 101 local users. There are 26647 hosts on the network.

  Type HELP for a detailed command list.
  Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
  2048        ?           a2          ac          bf          cal
  calc        cat         ching       clear       clock       ddate
  delta       diff        dir         echo        exit        factor
  file        finger      fnord       geoip       head        ipaddr
  joke        liff        login       mac         minesweeper more
  morse       newuser     notes       phoon       pig         ping
  privacy     qr          rain        rand        rfc         rig
  roll        rot13       salvo       sleep       starwars    sudoku
  tail        traceroute  typespeed   units       uptime      users
  uumap       uupath      uuplot      weather     when        zc

Press control-C to interrupt any command.
```

مشاهده می‌کنیم که این پیام اولین پیامی است که سرور سمت ما فرستاده است و نیز داده‌های درون آنرا نیز بررسی می‌کنیم.

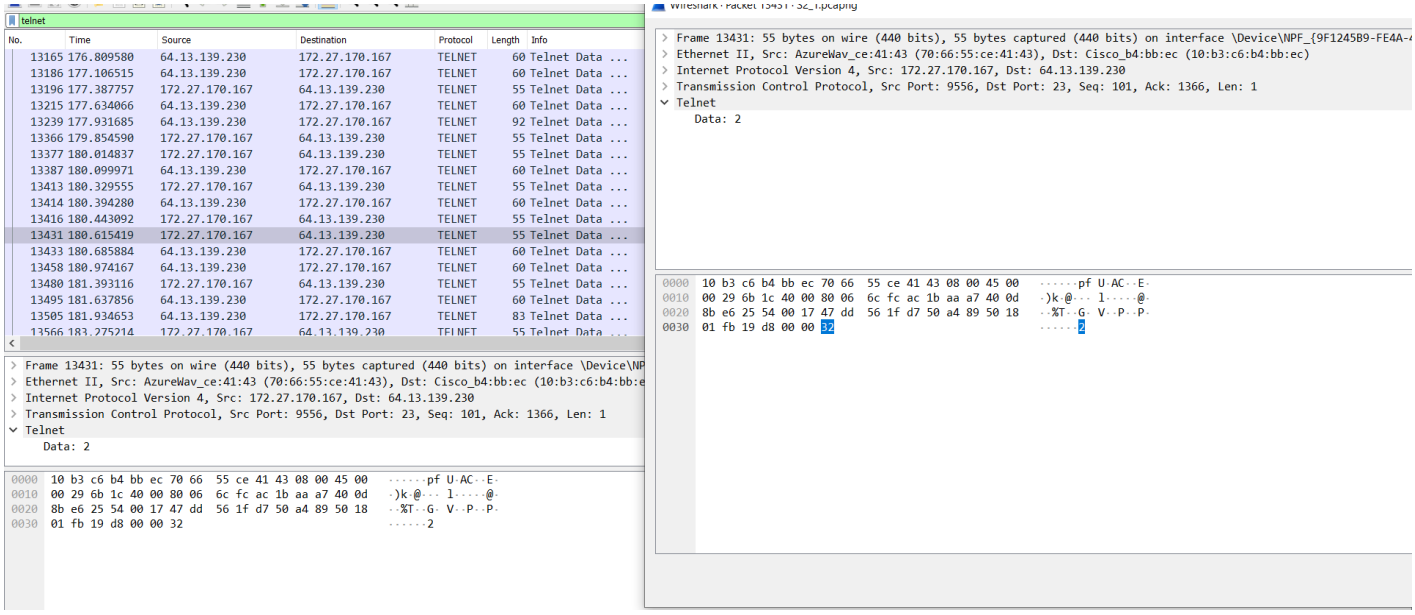
حال پیام‌های بعدی را بررسی می‌کنیم و عملا اولین پیام را tcp trace می‌کنیم تا رد و بدل شدن پیام‌ها را ببینیم.



حال یکی از پیام‌ها را جداگانه بررسی می‌کنیم.

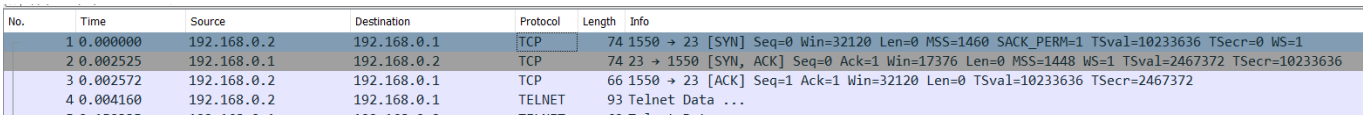
در عکس صفحه بعد متوجه می‌شویم که این پروتکل، پیام‌ها را به صورت کاراکتر به کاراکتر برای سرور ارسال می‌کند، همان گونه که مشخص است در زدن عبارت 2 + 2 هر کدام از کاراکترها را جداگانه برای سرور ارسال کرده است.

تفاوت این پروتکل با ssh این است که ssh پیام‌ها را **رمزگذاری** نیز می‌کند.

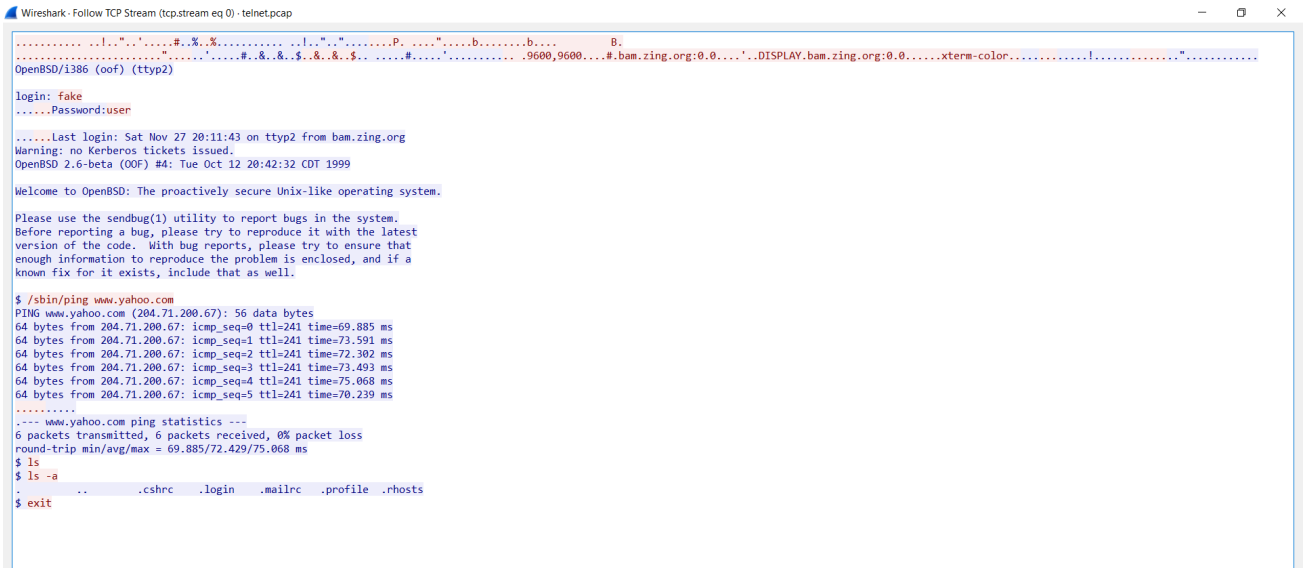


سوالات 3.3 :

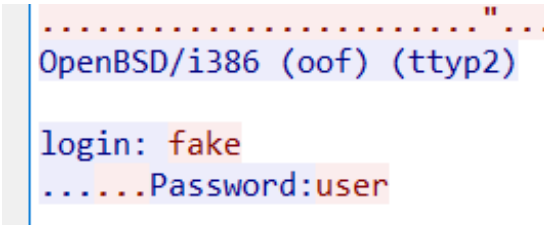
1. همان گونه که در شکل زیر مشخص است، ابتدا از **کلاینت یعنی 192.168.0.2** پیامی به عنوان handshake برای **192.168.0.1** (**سرور**) ارسال شده و SYN ACK آن نیز برگردانده شده است.



2. برای پیدا کردن ارتباط سرور و کلاینت، **استریم tcp** را دنبال می‌کنیم.



همان گونه که از شکل پیدا است:



که یعنی یوزر fake و پسورد user است.

3. برای پیدا کردن دستورات از همان استریم tcp استفاده می‌کنیم.

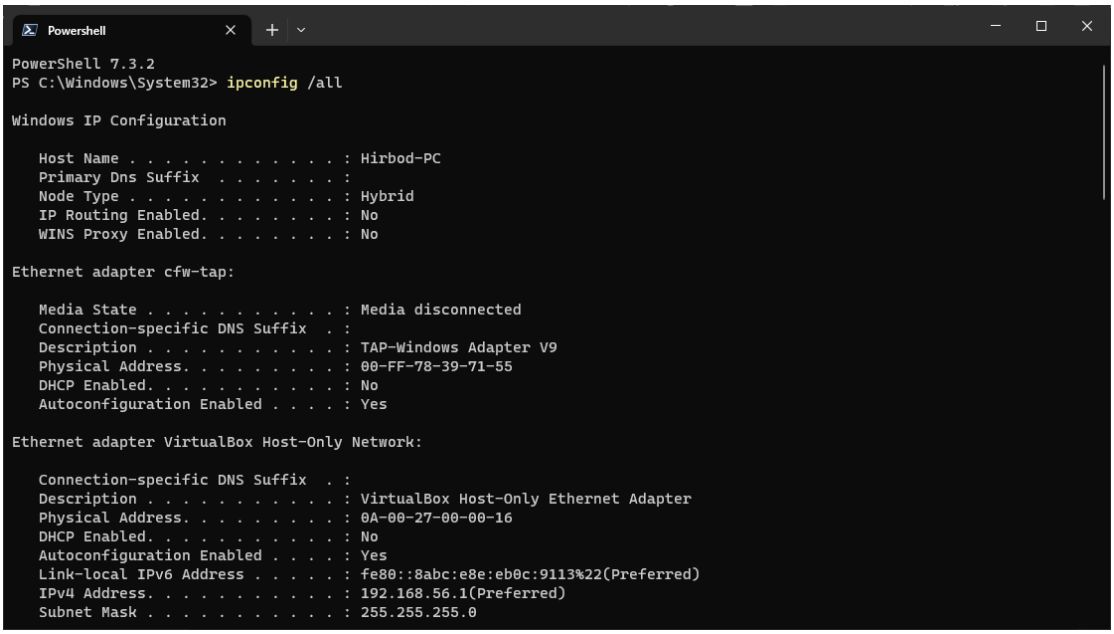
قسمت‌های قرمز، ارسالی از کلاینت به سرور و متون آبی ارسال از سرور به کلاینت هستند.

دستورات ارسالی مطابق با شکل بالا:

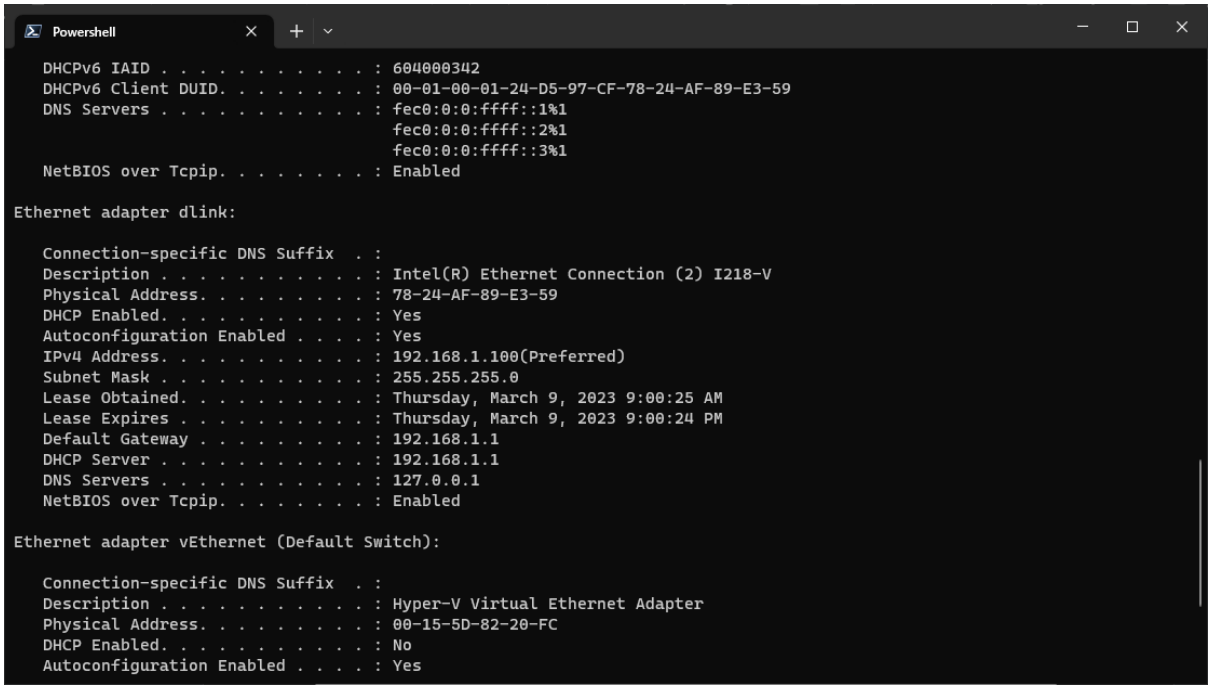
```
/sbin/ping www.yahoo.com
ls
ls -a
exit
```

بخش سوم

در ابتدا از دستور ipconfig /all استفاده می‌کنیم تا تمامی interfaceهای شبکه موجود در سیستم را مشاهده کنیم.

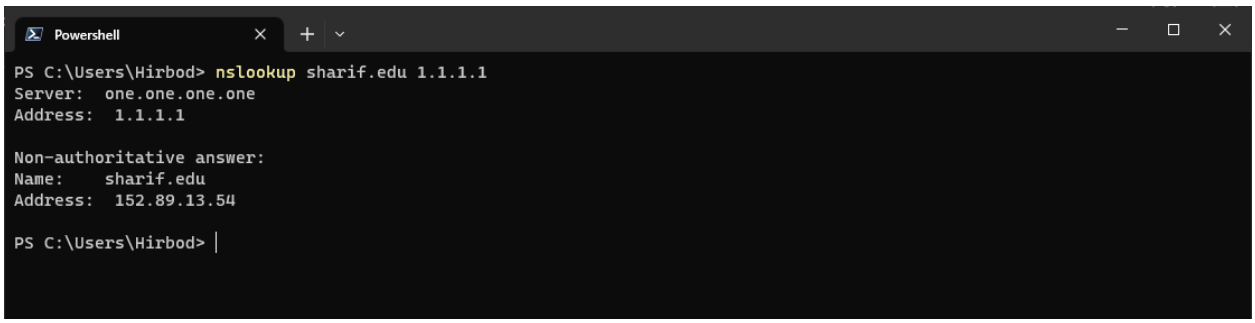


حال به دنبال interfaceی می‌گردیم که کامپیوتر ما را به اینترنت وصل می‌کند. اسم این interface در کامپیوتر من dlink است و دیتای آن را می‌توانید در زیر مشاهده کنید:

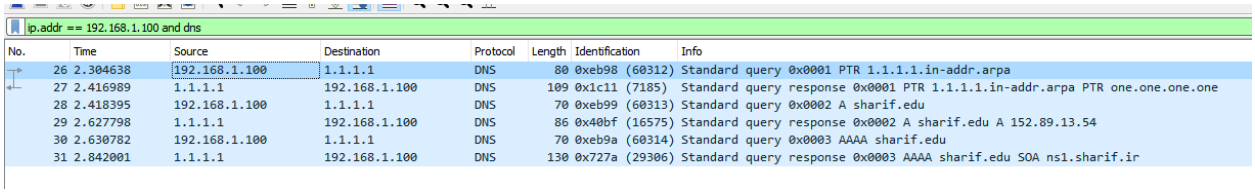


حال آزمایش را انجام می‌دهیم. در ابتدا طبق دستور کار dns cache خود را flush می‌کنیم.

سپس به کمک دستور زیر سعی می‌کنیم که دامنه‌ی sharif.edu را به کمک DNS serverهای Cloudflare تبدیل به IP کنیم. در حین این کار wireshark را نیز باز می‌گذاریم که بتوانیم پکت‌ها را تحلیل کنیم.



حال در wireshark به کمک فیلتر ip.addr == 192.168.1.100 and dns تمامی پکت‌هایی را انتخاب می‌کنیم که از نوع DNS هستند و IP مبدا یا مقصد آنها 192.168.1.100 است که همان طور که در خروجی ipconfig نیز دیدید، private IP کامپیوتر من است.

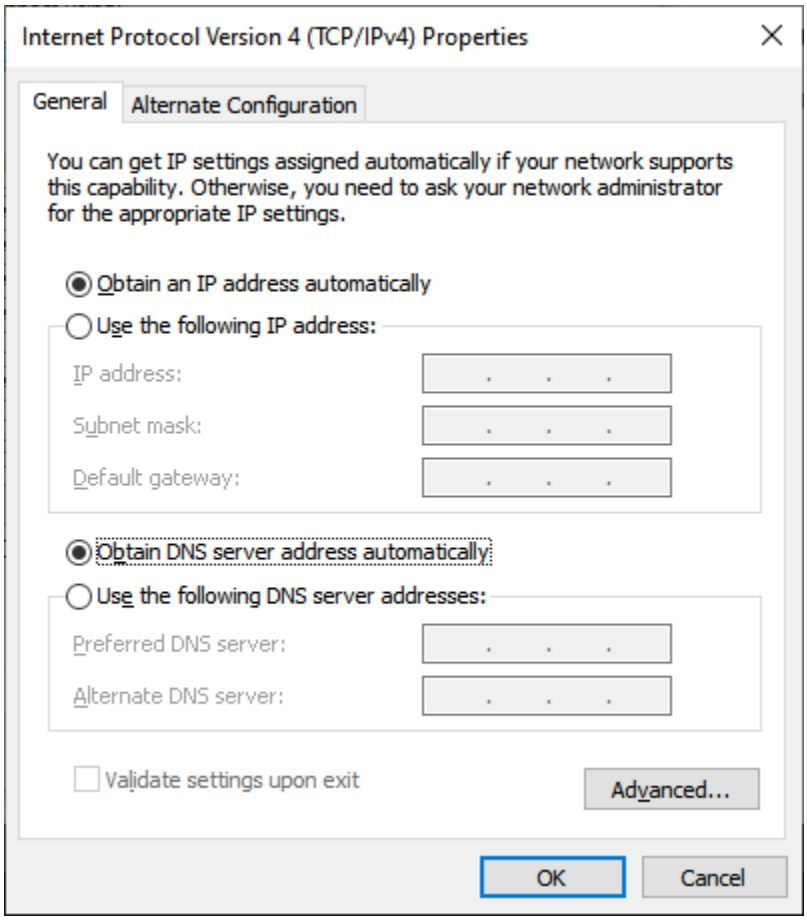


حال به جواب دادن سوالات پرسیده شده می‌پردازیم.

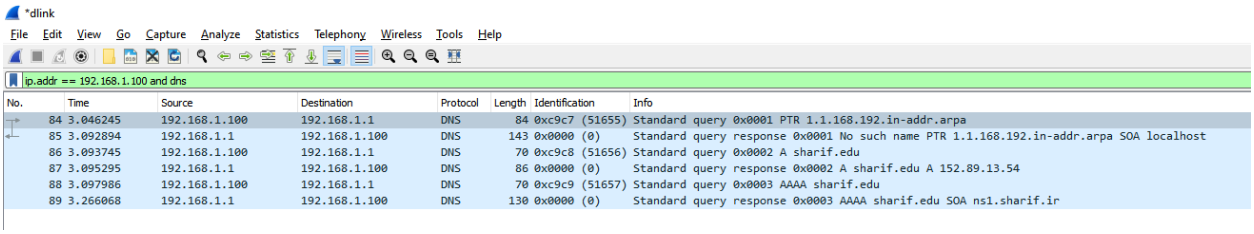
۱. همان طور که در دستور nslookup مشخص کردیم، درخواست‌ها برای 1.1.1.1 که DNS Server شرکت Cloudflare هست ارسال می‌شوند. در صورتی که 1.1.1.1 را در دستور dig تعیین نمی‌کردیم، درخواست‌ها به DNS Serverای که در تنظیمات

interface تعیین کردیم ارسال می‌شد. من از DNSCrypt استفاده می‌کنیم. به همین دلیل در خروجی interface هم می‌توانید مشاهده کنید که DNS Server من بر روی 127.0.0.1 تنظیم شده است.

اما برای این قسمت از آزمایش من تنظیمات DNS خود را عوض کردم که از DNS Serverهایی که بر روی مودم خانه تنظیم شده است استفاده کنم. برای این کار صرفا در تنظیمات آداپتور شبکه تیک Obtain DNS server address automatically را می‌زنیم.



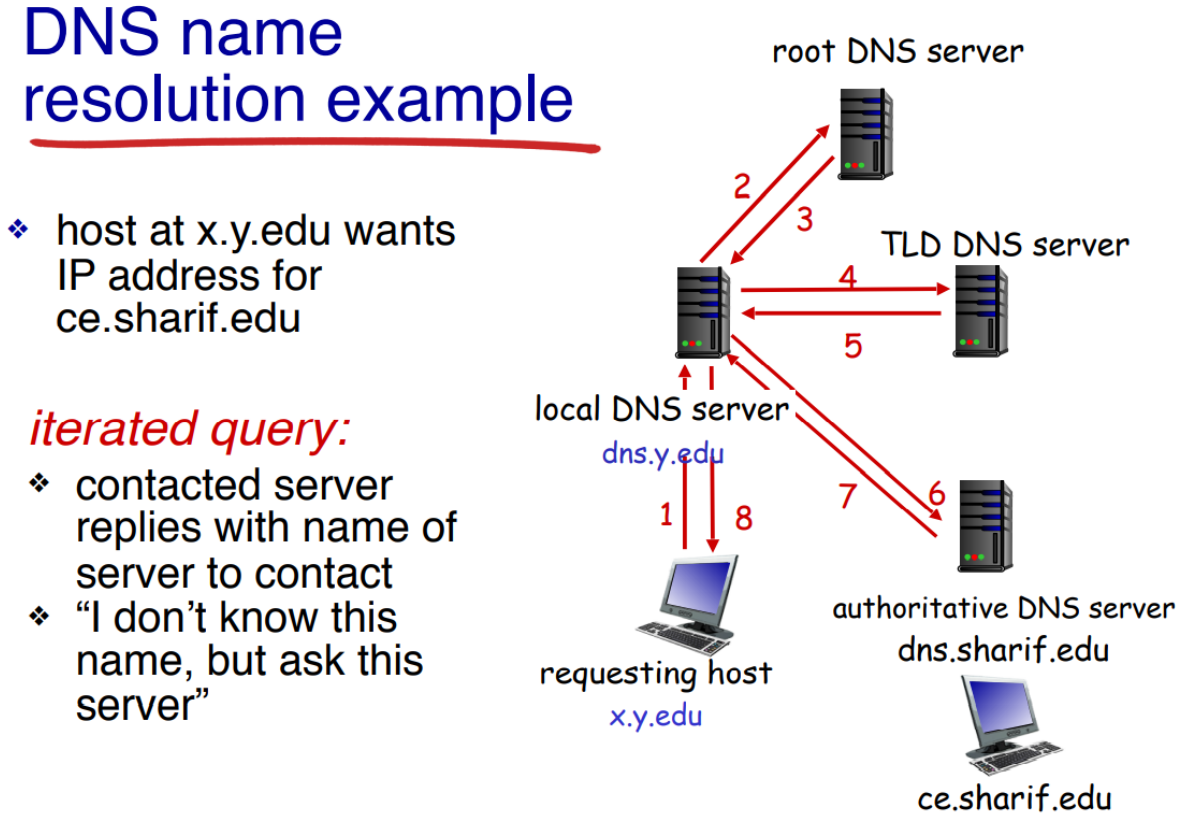
با این کار دوباره اگر آزمایش را انجام دهیم متوجه می‌شویم که مقصد پکت‌های DNS عملا default gateway مودم خانه می‌شود. این بدین معنا است که یک DNS server بر روی مودم خانه در حال اجرا است و می‌تواند با توجه به تنظیمات خود، درخواست‌های DNS را از سروری که در تنظیمات خودش تنظیم شده است بگیرد.



۲. همان طور که در wireshark مشخص است، سه درخواست متفاوت برای DNS Server فرستاده می‌شود. در ابتدا به تحلیل اولین پکت DNS می‌پردازیم.

```
> Frame 26: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface
> Ethernet II, Src: ASUSTekC_89:e3:59 (78:24:af:89:e3:59), Dst: D-LinkIn_25:20:f4 (
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 1.1.1.1
> User Datagram Protocol, Src Port: 60678, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  v 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
  v Queries
    v 1.1.1.1.in-addr.arpa: type PTR, class IN
        Name: 1.1.1.1.in-addr.arpa
        [Name Length: 20]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
    [Response In: 27]
```

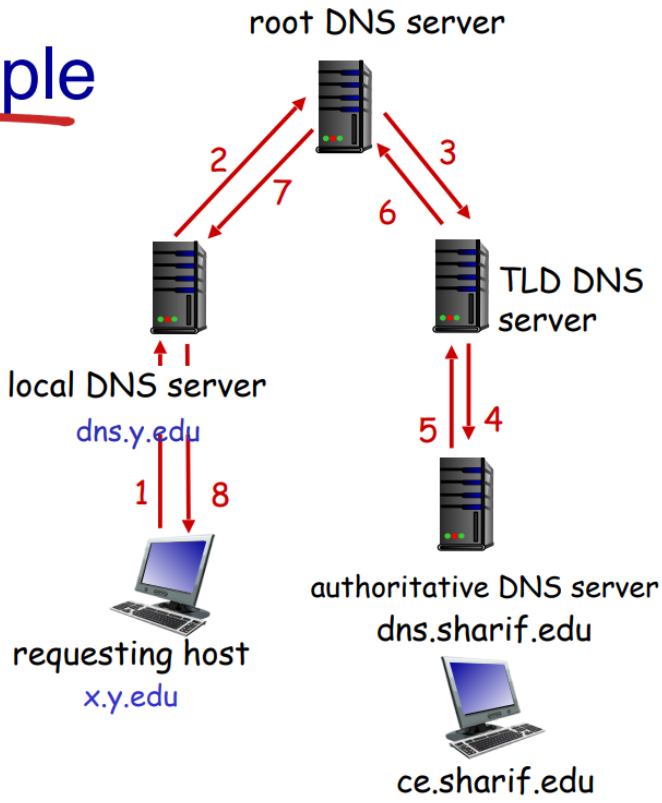
در ابتدا یک سری پرچم برای درخواست تعریف شده است که یکی از آنها فعال است که آن هم Recursion desired هست. فرض کنید که سروری که از آن درخواست می‌کنیم، آن دامنه را در دیتابیس خود نداشته باشد. در این صورت به عنوان مثال باید درخواست را از Root nameserver دامنه بکند. این کار می‌تواند به صورت recursive یا iterated باشد. در حالت recursive در صورتی که سرور خودش آن رکورد را نداشت، خودش می‌رود و از سرورهای دیگر می‌پرسد که آیا شما این دامنه را در دیتابیس خود دارید یا خیر. در عوض در حالت iterated سرور به ما جواب می‌دهد که من این دامنه را ندارم و می‌توانی خودت از این سرور دوباره بپرسی. برای فهم بهتر به عکس زیر که از اسلایدهای دکتر جعفری برداشته شده است توجه کنید:



DNS name resolution example

recursive query:

- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?



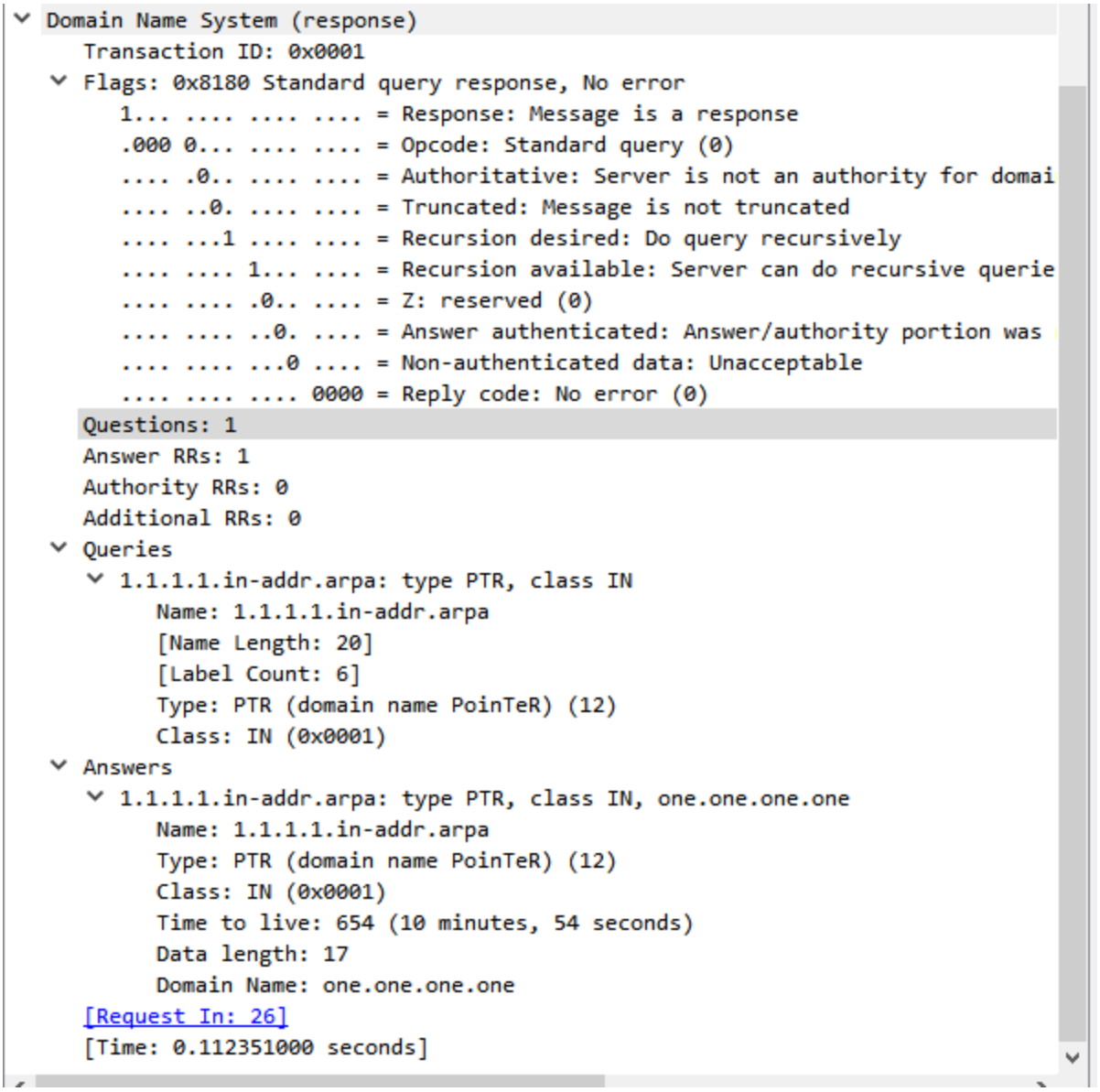
در ادامه مشخص شده است که از سرور تنها یک سوال داریم. آن سوال نیز از نوع PTR query است. این کوئری برای تبدیل یک IP address به دامنه استفاده می‌شود. به طور خلاصه IP که می‌خواهد reverse lookup شود، به صورت برعکس به in-addr.arpa چسبانده می‌شود و ارسال می‌شود. به عنوان مثال در صورتی که می‌خواستیم 1.2.3.4 را reverse lookup کنیم، باید دامنه‌ی زیر را می‌فرستادیم:

4.3.2.1.in-addr.arpa

برای اطلاعات بیشتر می‌توانید اینجا را مطالعه کنید.

همچنین مشخص است که می‌خواهیم دامنه‌ی DNS Server را پیدا کنیم.

حال جواب این درخواست را بررسی می‌کنیم:

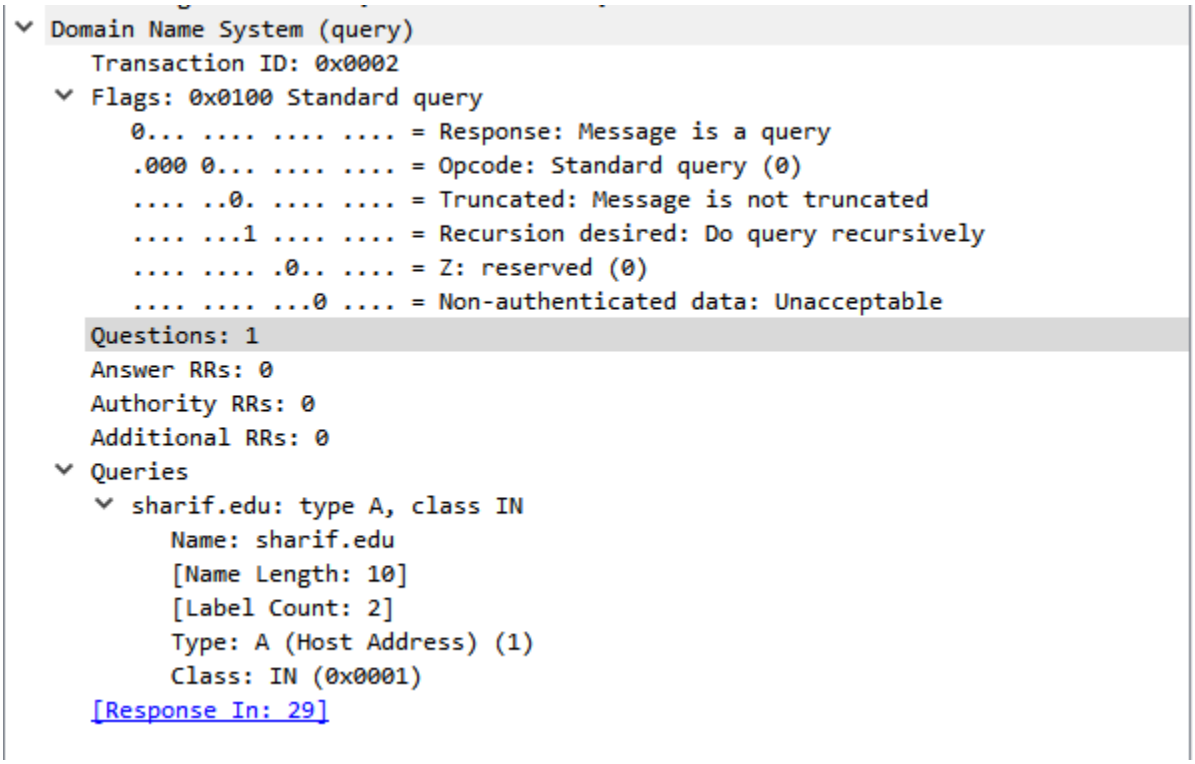


در اینجا نیز همان طور که مشخص است یک سری پرچم داریم. اولین پرچم مشخص می‌کند که این یک جواب برای درخواست‌های قبلی است. یکی دیگر از فلگ‌ها این است که سرور مشخص کرده است که می‌تواند به صورت recursive درخواست‌ها را بررسی کند.

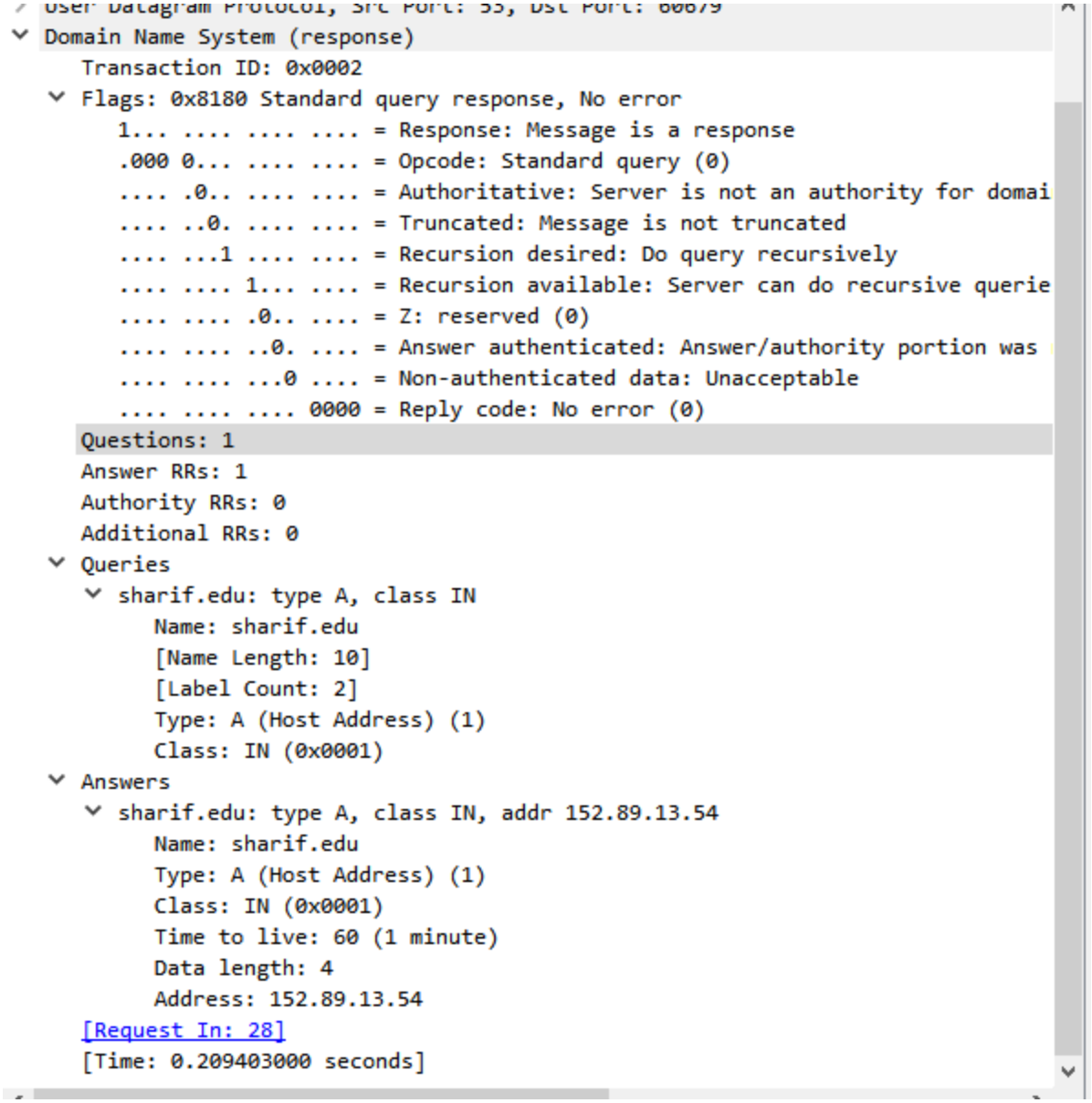
سپس درخواست‌هایی که فرستاده شده را دوباره در جواب نیز قرار می‌دهیم و بعد از آن جواب‌های درخواست ها را قرار می‌دهیم. همان طور که مشخص است جواب درخواست

reverse lookup برابر one.one.one.one است. نتیجه‌ی این درخواست را می‌توان جلوی خط Server در برنامه‌ی nslookup مشاهده کرد.

حال درخواست بعدی را بررسی می‌کنیم.

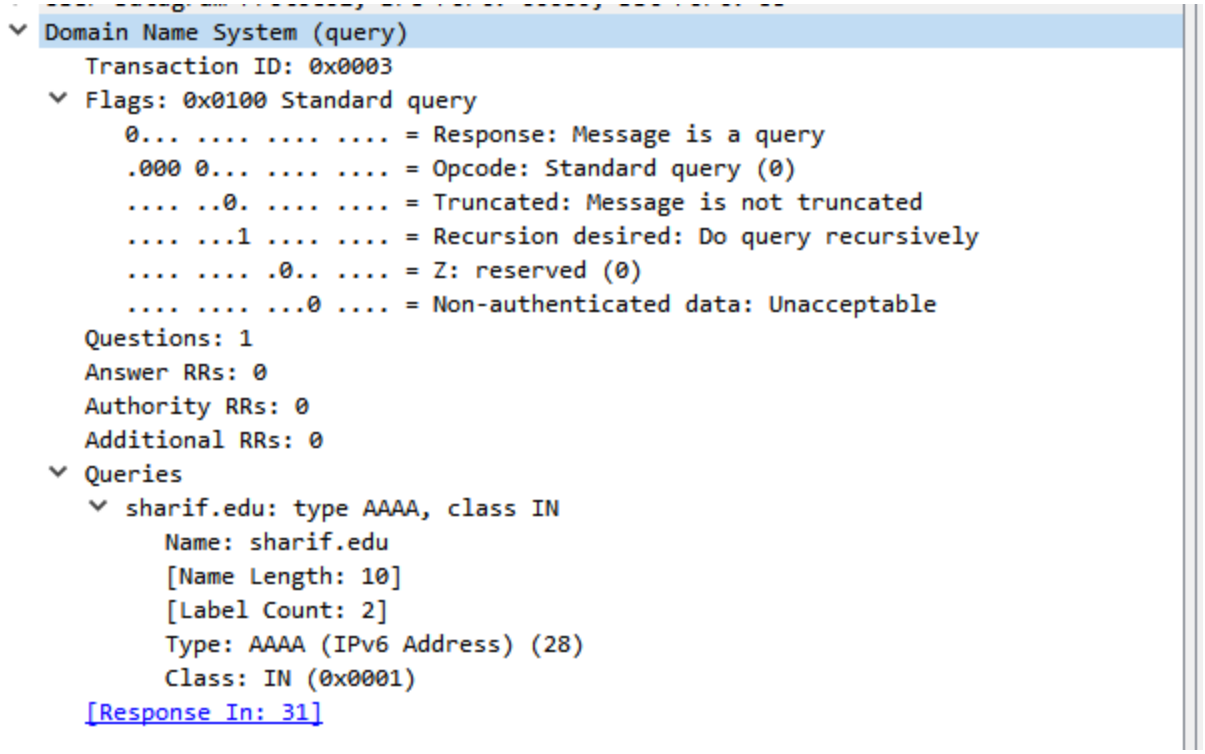


این یک درخواست از نوع A است. درخواست‌های نوع A صرفا دامنه را تبدیل به IPv4 می‌کنند. همان طور که مشخص است از سرور درخواست کرده‌ایم که sharif.edu را تبدیل به IPv4 بکند. حال جواب این درخواست را بررسی می‌کنیم.



همان طور که مشخص است IP برگردانده شده برابر 152.89.13.54 است. همچنین با توجه به TTL متوجه می‌شویم که می‌توانیم این IP را به مدت یک دقیقه در سیستم cache کنیم.

سپس درخواست آخر را بررسی می‌کنیم.



درخواست AAAA برای تبدیل کردن دامنه به IPv6 است. حال جواب این درخواست را نیز بررسی می‌کنیم.

```
    .... .0.. .... .... = Authoritative: Server is not an authority for domai
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... 1... .... = Recursion available: Server can do recursive querie
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
▾ Queries
  ▾ sharif.edu: type AAAA, class IN
      Name: sharif.edu
      [Name Length: 10]
      [Label Count: 2]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
▾ Authoritative nameservers
  ▾ sharif.edu: type SOA, class IN, mname ns1.sharif.ir
      Name: sharif.edu
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 48
      Primary name server: ns1.sharif.ir
      Responsible authority's mailbox: ksouratgar.sharif.ir
      Serial Number: 2023030501
      Refresh Interval: 60 (1 minute)
      Retry Interval: 120 (2 minutes)
      Expire limit: 1209600 (14 days)
      Minimum TTL: 60 (1 minute)
  [Request In: 30]
  [Time: 0.211219000 seconds]
```

همان طور که مشخص است این بار جواب واضحی به ما برنگشت که فلان IPv6 برای این سرور است. دلیل این موضوع این است که اصلا هیچ IPv6ای به این دامنه وصل نشده است!

به صورت کلی جواب SOA نشان می‌دهد که سرورهای cloudflare به authoritative serverهای سایت شریف رفته‌اند و باز هم جوابی برای درخواست نوع AAAA پیدا نکرده‌اند. برای همین صرفا اطلاعات این authority record را بر می‌گرداند. در این جواب

اطلاعاتی نظیر nameserverها و شماره سریال و اسم و آدرس ایمیل کسی که مسئول این سرویس هست برگردانده می‌شود. [منبع]
برای نمونه نیز من جواب یک درخواست را آوردم که IPv6 به دامنه assign شده باشد. این دامنه cloudflare.com است.

```
▼ Queries
  ▼ cloudflare.com: type AAAA, class IN
      Name: cloudflare.com
      [Name Length: 14]
      [Label Count: 2]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
▼ Answers
  ▼ cloudflare.com: type AAAA, class IN, addr 2606:4700::6810:84e5
      Name: cloudflare.com
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 190 (3 minutes, 10 seconds)
      Data length: 16
      AAAA Address: 2606:4700::6810:84e5
  ▼ cloudflare.com: type AAAA, class IN, addr 2606:4700::6810:85e5
      Name: cloudflare.com
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 190 (3 minutes, 10 seconds)
      Data length: 16
      AAAA Address: 2606:4700::6810:85e5
  [Request In: 181]
  [Time: 0.111934000 seconds]
```

همان طور که مشخص است، مانند درخواست‌های A، جواب این نوع درخواست نیز حاوی یک IPv6 و یک TTL است. نکته‌ای که در این جواب توجه را جلب می‌کند این است که دو IP برای این درخواست برگشته است! این موضوع صرفا به load balance کمک می‌کند.
همچنین نتیجه‌ی این درخواست در nslookup در زیر آمده است:

```
PS C:\Users\Hirbod> nslookup cloudflare.com 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    cloudflare.com
Addresses:  2606:4700::6810:84e5
          2606:4700::6810:85e5
          104.16.133.229
          104.16.132.229

PS C:\Users\Hirbod>
```