

به نام خدا



# آزمایشگاه شبکه‌های کامپیوتری

گزارش آزمایش دوم

استاد:

دکتر حمید بیگی

نویسندگان :

محمد هومان 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:

▼ Frame 74: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface \Device\NPF\_{15449871-7029-47FC-ADC2-C98F5880E...}

Section number: 1

> Interface id: 0 (\Device\NPF\_{15449871-7029-47FC-ADC2-C98F5880E142})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 5, 2023 22:32:29.606273000 Iran Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1678042949.606273000 seconds

[Time delta from previous captured frame: 0.000650000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 2.453332000 seconds]

Frame Number: 74

Frame Length: 488 bytes (3904 bits)

Capture Length: 488 bytes (3904 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: D-LinkIn\_10:b2:11 (ac:f1:df:10:b2:11), Dst: D-LinkIn\_d4:ae:4c (70:62:b8:d4:ae:4c)

▼ Destination: D-LinkIn\_d4:ae:4c (70:62:b8:d4:ae:4c)

Address: D-LinkIn\_d4:ae:4c (70:62:b8:d4:ae:4c)

... .. = LG bit: Globally unique address (factory default)

... .. = IG bit: Individual address (unicast)

▼ Source: D-LinkIn\_10:b2:11 (ac:f1:df:10:b2:11)

Address: D-LinkIn\_10:b2:11 (ac:f1:df:10:b2:11)

... .. = LG bit: Globally unique address (factory default)

0000 70 62 b8 d4 ae 4c ac f1 df 10 b2 11 00 00 45 00 pb...L.....E

0010 01 da 69 2a 40 00 09 06 28 98 c0 a8 01 24 98 59 ..!g...(...\$Y

0020 0d 3e fe ab 00 00 85 c6 70 5b 53 62 4e c0 50 18 ..6...P...p(SbN-P

0030 02 03 db 5f 00 00 47 45 54 20 2f 7e 6b 68 61 72 ....GE T /~khar

0040 72 61 7a 69 2f 20 48 54 54 50 2f 31 2e 31 0d 0a razif/ HT TP/1.1

0050 48 6f 73 74 3a 20 73 68 61 72 69 66 2e 65 64 75 Host: sh arif.edu

0060 0d 0a 43 6f 6e 6a 65 63 74 69 6f 6e 3a 20 65 65 ..Connect ion: ke

0070 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d ..p- alive ..Cache-

0080 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 Control: max-age

0090 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 => Upgr ade-Inse

00a0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 ..ure-Req uests: 1

00b0 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ..-User-A gent: Mo

00c0 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo

00d0 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 ws NT 10 .0; Win6

00e0 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4; x64) AppleWeb

00f0 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d Kit/537. 36 (KHTM

0100 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 L, like Gecko) C

0110 68 72 6f 6d 65 2f 31 31 30 2e 30 2e 30 2e 30 20 hrome/11 0.0.0.0

0120 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 Safari/5 37.36; A

0130 63 63 65 70 74 3a 20 74 65 70 2f 2f 69 74 6d 6c cept: t ext/html

0140 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 , applica tion/xht

0150 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 m+xml,a pplicati

0160 6f 6e 2f 78 6d 6c 30 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9,ima

0170 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 ge/avif, image/av

0180 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f bp,image /apng,\*

0190 2a 3b 71 3d 30 2e 38 0d 0a 53 65 63 2d 47 50 43 ;q=0.8 -Sec-GPC

01a0 3a 20 31 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 : 1 -Acc ept-Lang

01b0 75 61 67 65 3a 20 65 66 2d 55 53 2c 65 6e 3b 71 uage: en -US,en;q

01c0 3d 30 2e 38 0d 0a 43 63 65 70 74 2d 45 6e 63 =>8.0 -Ac cept-Enc

01d0 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 oding: g zip, def

▼ Hypertext Transfer Protocol

> GET /~kharrazi/ HTTP/1.1\r\n

Host: sharif.edu\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8\r\n

Sec-GPC: 1\r\n

Accept-Language: en-US,en;q=0.8\r\n

Accept-Encoding: gzip, deflate\r\n

\r\n

[Full request URI: http://sharif.edu/~kharrazi/]

[HTTP request 1/1]

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	PDU's
▼ 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:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.891334	192.168.1.36	149.154.167.92	TCP	66	65163 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5	0.106269	192.168.1.36	149.154.167.92	TCP	66	65164 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6	0.122301	192.168.1.36	149.154.167.92	TCP	66	65166 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7	0.122357	192.168.1.36	149.154.167.92	TCP	66	65165 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8	0.138249	192.168.1.36	149.154.167.92	TCP	66	65168 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9	0.143196	192.168.1.36	149.154.167.92	TCP	66	65167 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	0.155356	192.168.1.36	149.154.167.92	TCP	66	65177 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	0.155596	192.168.1.36	155.94.218.67	TCP	66	65178 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12	0.218209	192.168.1.36	89.252.132.19	TCP	66	65175 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13	0.218210	192.168.1.36	68.235.43.196	TCP	66	65172 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
14	0.218210	192.168.1.36	143.244.44.218	TCP	66	65169 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15	0.218210	192.168.1.36	189.150.197.194	TCP	66	65174 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
16	0.218209	192.168.1.36	146.70.100.99	TCP	66	65171 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17	0.218245	192.168.1.36	146.70.97.227	TCP	66	65173 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
18	0.218245	192.168.1.36	212.102.63.2	TCP	66	65170 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19	0.218267	192.168.1.36	155.94.216.67	TCP	66	65176 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
25	0.972981	23.21.43.50	192.168.1.36	TCP	56	53 → 54670 [PSH, ACK] Seq=1 Ack=1 Win=53 Len=2 [TCP segment of a reassembled PDU]
26	1.014858	192.168.1.36	23.21.43.50	TCP	54	54670 → 53 [ACK] Seq=1 Ack=3 Win=515 Len=0
27	1.091022	192.168.1.36	149.154.167.92	TCP	66	65179 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
28	1.092741	192.168.1.36	149.154.167.92	TCP	66	65180 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
29	1.116751	192.168.1.36	149.154.167.92	TCP	66	65181 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
30	1.117556	192.168.1.36	149.154.167.92	TCP	66	65182 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
31	1.134985	192.168.1.36	149.154.167.92	TCP	66	65183 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32	1.136428	192.168.1.36	149.154.167.92	TCP	66	65184 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
33	1.162905	192.168.1.36	109.8223.218.67	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 65177 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34	1.167381	192.168.1.36	155.94.218.67	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 65178 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

> Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF{15449071-7029-47FC-ADC2-C9BF580B142}, 1	0000	70 62 b8 d4 ae 4c ac f1 df 10 b2 11 00 00 45 00	pb...	.....E:
> Ethernet II, Src: D-LinkIn_10:b2:11 (ac:f1:df:10:b2:11), Dst: D-LinkIn_d4:ae:4c (78:62:b8:d4:ae:4c)	0010	00 34 9d e8 40 00 00 06 5e 18 c0 a8 01 24 95 9a	..4..@..A....\$..	
> Internet Protocol Version 4, Src: 192.168.1.36, Dst: 149.154.167.92	0020	a7 5c fe 8b 01 bb 69 ab eb e8 00 00 00 00 00 02	.....I.....	
> Transmission Control Protocol, Src Port: 65163, Dst Port: 443, Seq: 0, Len: 0	0030	fa f0 1f 01 00 00 02 04 05 b4 01 03 03 08 01 01	.....	
Source Port: 65163	0040	04 02	..	
Destination Port: 443				
[Stream index: 0]				
[Conversation completeness: Incomplete, SYN_SENT (1)]				
[TCP Segment Len: 0]				
Sequence Number: 0 (relative sequence number)				
Sequence Number (raw): 1772874728 (relative sequence number)				
Acknowledgment Number: 0				
Acknowledgment number (raw): 0				
1000 ... = Header Length: 32 bytes (0)				
Flags: 0x002 (SYN)				
Window: 64240				
[Calculated window size: 64240]				
Checksum: 0x1f81 [unverified]				
[Checksum Status: Unverified]				
Urgent Pointer: 0				
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permi				
[Timestamps]				

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



~kharrazi.png

## 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.

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 (78:66:55: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
▼ 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 call\r\n
  Data: calc cat ching clear clock ddate\r\n
  Data: delta diff dir echo exit factor\r\n
  Data: file finger fnord geoup head ipaddr\r\n
  Data: joke liiff 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 call
calc cat ching clear clock ddate
delta diff dir echo exit factor
file finger fnord geoup head ipaddr
joke liiff 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 عملاً اولین پیام را tcp trace می‌کنیم تا رد و بدل شدن پیام‌ها را ببینیم.

```
.....$..'.
Connected to TELEHACK port 143
.....P.....$.....'.
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.
More commands become available after login.
...$.....XTERM.....$.....2020....[K..[Kcaccalc..l....[K..[K....[K..[Kkoklo1.....[K..[K..[Kjojkeoke

Eye for eye, tooth for tooth, hand for hand, foot for foot.
.calccalc

Type HELP for calculator help.
calc> 2 2+ 2+ 2

4
.[0m.[?25h.[?1000lcalc> 2 2 ****22

4
.[0m.[?25h.[?1000lcalc> 2 2* ** 88

256
.[0m.[?25h.[?1000lcalc> 2 2^ ^8

8
.ccc

Packet 11612, 179 client pkts, 162 server pkts, 231 turns. Click to select.
```

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.

No.	Time	Source	Destination	Protocol	Length	Info
13165	176.809580	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13186	177.106515	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13196	177.387757	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
13215	177.634066	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13239	177.931685	64.13.139.230	172.27.170.167	TELNET	92	Telnet Data ...
13366	179.854590	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
13377	180.014837	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
13387	180.099971	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13413	180.329555	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
13414	180.394280	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13416	180.443092	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
13431	180.615419	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
13433	180.685884	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13458	180.974167	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13480	181.393116	172.27.170.167	64.13.139.230	TELNET	55	Telnet Data ...
13495	181.637856	64.13.139.230	172.27.170.167	TELNET	60	Telnet Data ...
13505	181.934653	64.13.139.230	172.27.170.167	TELNET	83	Telnet Data ...
13566	183.275214	172.27.170.167	64.13.139.230	TFINFT	55	Telnet Data ...

> Frame 13431: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{9F1245B9-FE4A-408D-8000-000000000000} on interface 10/10/100 Ethernet II, Src: AzureWav_ce:41:43 (70:66:55:ce:41:43), Dst: Cisco_b4:bb:ec (10:b3:c6:b4:bb:ec)
> Internet Protocol Version 4, Src: 172.27.170.167, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 9556, Dst Port: 23, Seq: 101, Ack: 1366, Len: 1
▼ Telnet
Data: 2

0000	10 b3 c6 b4 bb ec 70 66 55 ce 41 43 08 00 45 00	.....pf U-AC...E-
0010	00 29 6b 1c 40 00 80 06 6c fc ac 1b aa a7 40 0d	...)k:@...l....@-
0020	8b e6 25 54 00 17 47 dd 56 1f d7 50 a4 89 50 18	..%T...G...V...P..P-
0030	01 fb 19 d8 00 00 32	.....2

## سوالات 3.3 :

- 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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=10233636 TSecr=0 WS=1
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=2467372 TSecr=10233636
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=2467372
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...

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

```
Wireshark - Follow TCP Stream (tcp.stream eq 0) - telnet.pcap
.....#.%..P:.....b....B
.....#.&.&.&.&.&..#.#.bam.zing.org:0.0....DISPLAY.bam.zing.org:0.0.....xterm-color.....!.....
OpenBSD/i386 (oof) (ttyp2)

login: fake
.....Password:user

.....Last login: Sat Nov 27 20:11:43 on ttty2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ /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
```

همان گونه که از شکل پیدا است:

```
....."
OpenBSD/i386 (oof) (ttyp2)

login: fake
.....Password:user
```

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 ارسالی از سرور به کلاینت هستند.

دستورات ارسالی مطابق با شکل بالا:

/sbin/ping [www.yahoo.com](http://www.yahoo.com)

ls

ls -a

exit

## بخش سوم

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

```
PowerShell
PS C:\Windows\System32> ipconfig /all

Windows IP Configuration

Host Name . . . . . : Hirbod-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter cfw-tap:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : TAP-Windows Adapter V9
Physical Address. . . . . : 00-FF-78-39-71-55
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-16
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8abc:e8e:eb0c:9113%22(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

حال به دنبال interface 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:

```
PowerShell

DHCPv6 IAID . . . . . : 604000342
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-D5-97-CF-78-24-AF-89-E3-59
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       : fec0:0:0:ffff::2%1
                       : fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter dlink:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Ethernet Connection (2) I218-V
Physical Address. . . . . : 78-24-AF-89-E3-59
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, March 9, 2023 9:00:25 AM
Lease Expires . . . . . : Thursday, March 9, 2023 9:00:24 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-82-20-FC
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

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

```
PowerShell
PS C:\Users\Hirbod> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Users\Hirbod> |
```

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.

```
PowerShell
PS C:\Users\Hirbod> nslookup sharif.edu 1.1.1.1
Server:   one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:     sharif.edu
Address:  152.89.13.54

PS C:\Users\Hirbod> |
```

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.

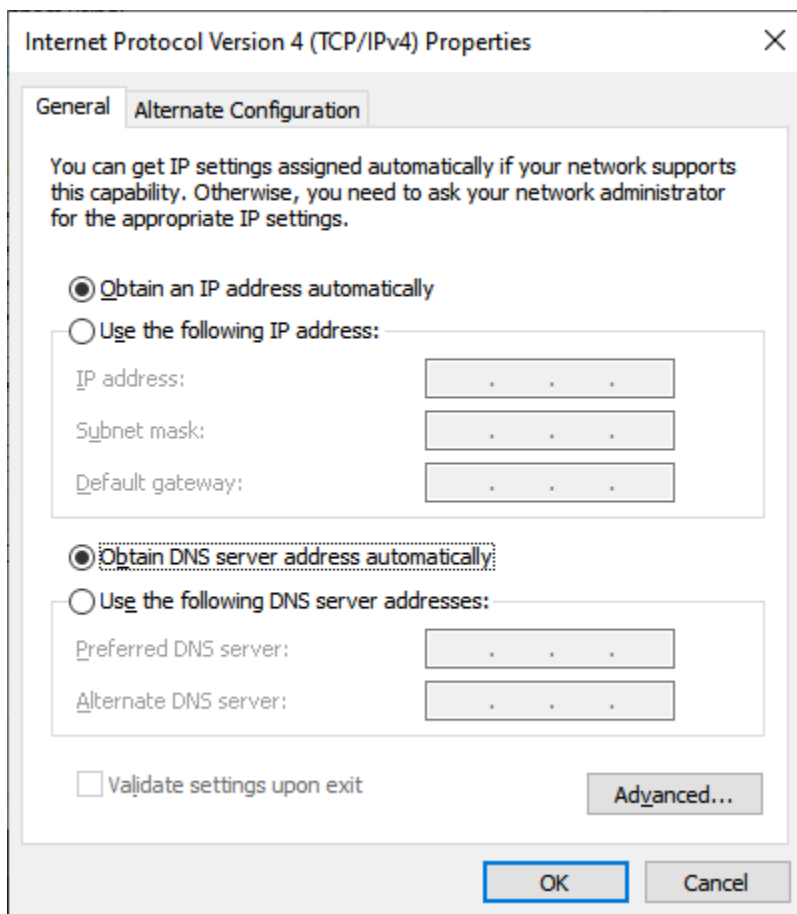
No.	Time	Source	Destination	Protocol	Length	Identification	Info
26	2.304638	192.168.1.100	1.1.1.1	DNS	80	0xeb98 (60312)	Standard query 0x0001 PTR 1.1.1.1.in-addr.arpa
27	2.416989	1.1.1.1	192.168.1.100	DNS	109	0x1c11 (7185)	Standard query response 0x0001 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one
28	2.418395	192.168.1.100	1.1.1.1	DNS	70	0xeb99 (60313)	Standard query 0x0002 A sharif.edu
29	2.627798	1.1.1.1	192.168.1.100	DNS	86	0x40bf (16575)	Standard query response 0x0002 A sharif.edu A 152.89.13.54
30	2.630782	192.168.1.100	1.1.1.1	DNS	70	0xeb9a (60314)	Standard query 0x0003 AAAA sharif.edu
31	2.842001	1.1.1.1	192.168.1.100	DNS	130	0x727a (29306)	Standard query response 0x0003 AAAA sharif.edu SOA ns1.sharif.ir

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 Serverی 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 Server هایی که بر روی مودم خانه تنظیم شده است استفاده کنم. برای این کار صرفاً 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 عملاً 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.

```
PS C:\Users\Hirbod> nslookup sharif.edu
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name:     sharif.edu
Address:  152.89.13.54

PS C:\Users\Hirbod> |
```

\*dlink

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.100 and dns

No.	Time	Source	Destination	Protocol	Length	Identification	Info
84	3.046245	192.168.1.100	192.168.1.1	DNS	84	0xc9c7 (51655)	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
85	3.092894	192.168.1.1	192.168.1.100	DNS	143	0x0000 (0)	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
86	3.093745	192.168.1.100	192.168.1.1	DNS	70	0xc9c8 (51656)	Standard query 0x0002 A sharif.edu
87	3.095295	192.168.1.1	192.168.1.100	DNS	86	0x0000 (0)	Standard query response 0x0002 A sharif.edu A 152.89.13.54
88	3.097986	192.168.1.100	192.168.1.1	DNS	70	0xc9c9 (51657)	Standard query 0x0003 AAAA sharif.edu
89	3.266068	192.168.1.1	192.168.1.100	DNS	130	0x0000 (0)	Standard query response 0x0003 AAAA sharif.edu SOA ns1.sharif.ir

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
▼ Domain Name System (query)
  Transaction ID: 0x0001
  ▼ 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
    ▼ 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]
```

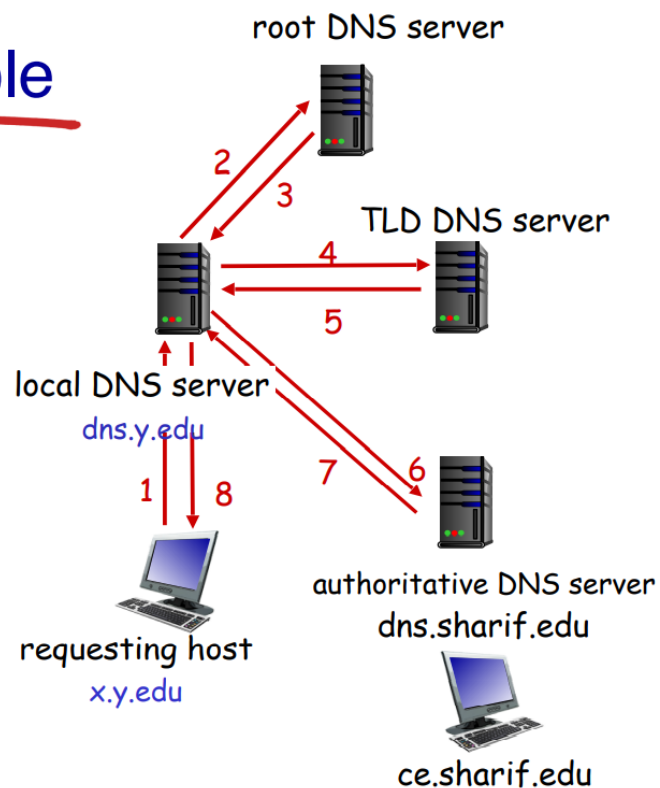
در ابتدا یک سری پرچم برای درخواست تعریف شده است که یکی از آنها فعال است که آن هم Recursion desired هست. فرض کنید که سروری که از آن درخواست می‌کنیم، آن دامنه را در دیتابیس خود نداشته باشد. در این صورت به عنوان مثال باید درخواست را از Root nameserver دامنه بکند. این کار می‌تواند به صورت recursive یا iterated 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

- ❖ host at x.y.edu wants IP address for ce.sharif.edu

### *iterated query:*

- ❖ contacted server replies with name of server to contact
- ❖ "I don't know this name, but ask this server"

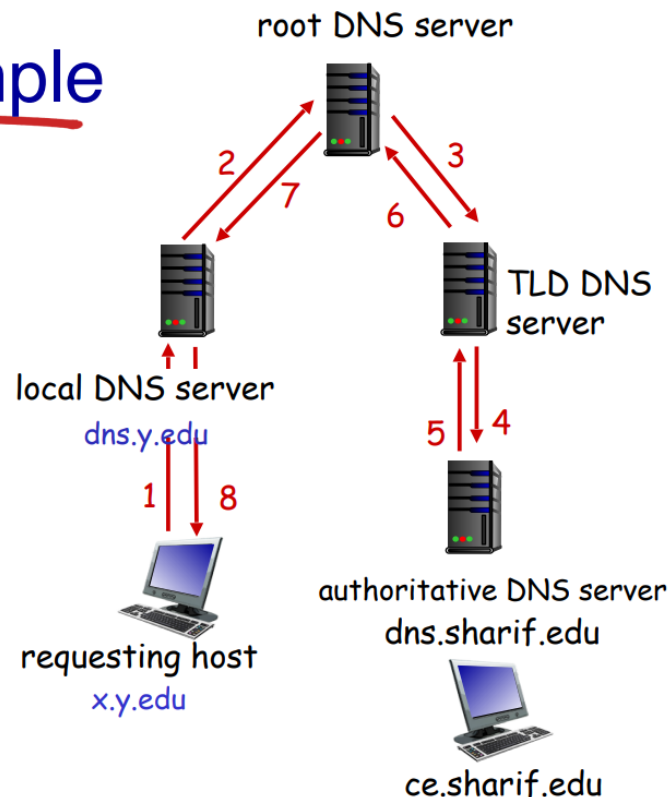




# DNS name resolution example

## 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:

```

Domain Name System (response)
  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
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)

  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    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)
  Answers
    1.1.1.1.in-addr.arpa: type PTR, class IN, one.one.one.one
      Name: 1.1.1.1.in-addr.arpa
      Type: PTR (domain name Pointer) (12)
      Class: IN (0x0001)
      Time to live: 654 (10 minutes, 54 seconds)
      Data length: 17
      Domain Name: one.one.one.one
      [Request In: 26]
      [Time: 0.112351000 seconds]

```

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 درخواست‌ها 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.

```
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
  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: 29]
```

این یک درخواست از نوع A است. درخواست‌های نوع A صرفاً 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.

```

User Datagram Protocol, Src Port: 55, Dst Port: 60079
Domain Name System (response)
  Transaction ID: 0x0002
  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
    .... 0... .. = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  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)
  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: 60 (1 minute)
      Data length: 4
      Address: 152.89.13.54
    [Request In: 28]
    [Time: 0.209403000 seconds]

```

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.

```

Domain Name System (query)
  Transaction ID: 0x0003
  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 AAAA, class IN
      Name: sharif.edu
      [Name Length: 10]
      [Label Count: 2]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
\[Response In: 31\]

```

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 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
.....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 اصلاً هیچ IPv6 ای به این دامنه وصل نشده است!

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

اطلاعاتی نظیر nameserver ها 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 صرفاً 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>
```