

به نام خدا

گزارش آزمایش دوم

دستیار آموزشی

آقای سیامکی

اعضای گروه

نگار باباشه

۹۹۱۰۹۳۲۵

ایمان محمدی

۹۹۱۰۲۲۰۷

محمد مهدی میرزایی

۹۹۱۷۱۰۲۲

نیمسال تابستان ۱۴۰۳

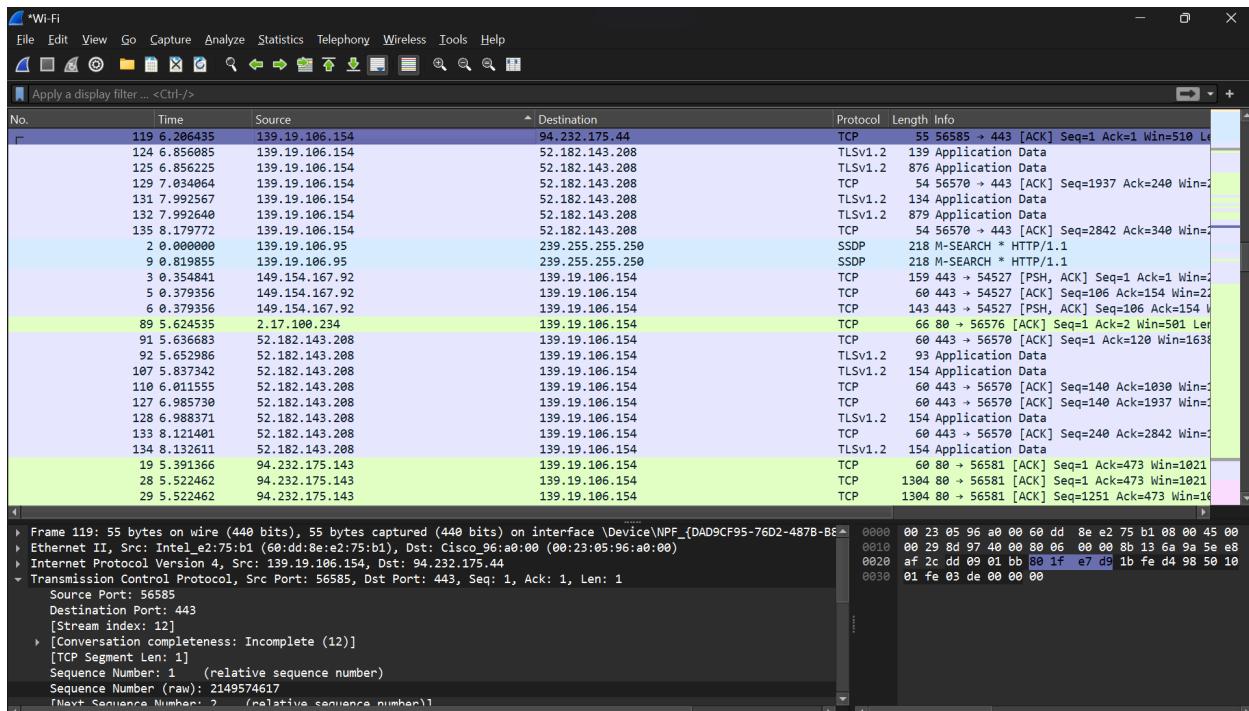
بخش اول. فهم اولیه از HTTP

شرح آزمایش

در این بخش هدف این است که هم با محیط نرم افزار wireshark آشنا شویم و هم یک سری ارتباط را بررسی کنیم و پیام های مربوط به آن را تحلیل کنیم.

مراحل

ابتدا capture را در حالت Wi-Fi قرار می دهیم. سپس مرورگر خود را باز می کنیم و وارد سایت <http://farzanegan2t.ir> می شویم. دلیل انتخاب این سایت این است که ریکوئست های مربوط به آن زده می شوند و این صفحه ای انتخاب شده شامل عکس نیز هست.
حال همان طور که گفته شده است، capture کردن را متوقف می کنیم. در ابتدا چنین تصویری می بینیم:



در ادامه همان طور که در دستور کار گفته شده است، بسته‌های حاوی http را فیلتر می‌کنیم تا به این پیام‌ها برسیم:

No.	Time	Source	Destination	Protocol	Length	Info
15	5.260951	139.19.106.154	94.232.175.143	HTTP	526	/Default.aspx?PageId=72 HTTP/1.1
50	5.544119	139.19.106.154	94.232.175.143	HTTP	494	GET /CaptchaImage.axd?guid=7dcc9e3-f5a2-44ea-944 GET /CaptchaImage.axd?guid=9b6e4ddc-4aef-4d28-88 5.621143
68	5.563205	139.19.106.154	94.232.175.143	HTTP	494	GET /CaptchaImage.axd?guid=9b6e4ddc-4aef-4d28-84 5.567596
88	5.621143	139.19.106.154	94.232.175.143	HTTP/J...	625	POST /Services/VisitorCounterService.asmx/Insert 84 5.567596
84	5.567596	94.232.175.143	139.19.106.154	HTTP	244	HTTP/1.1 200 OK (text/html)
95	5.657917	94.232.175.143	139.19.106.154	HTTP	463	HTTP/1.1 200 OK (JPEG JFIF image)
99	5.668337	94.232.175.143	139.19.106.154	HTTP	909	HTTP/1.1 200 OK (JPEG JFIF image)
102	5.706776	94.232.175.143	139.19.106.154	HTTP/J...	302	HTTP/1.1 200 OK , JSON (application/json)

اولین پیام در لیست بالا، روی آن کلیک می‌کنیم تا در قسمت پایین اطلاعات بیشتر مربوط به آن را ببینیم:

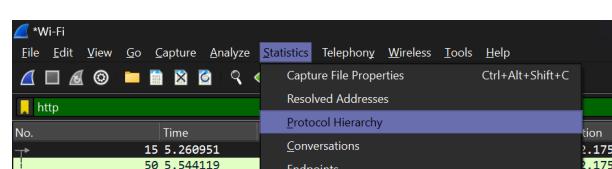
No.	Time	Source	Destination	Protocol	Length	Info
15	5.260951	139.19.106.154	94.232.175.143	HTTP	526	GET /Default.aspx?PageId=72 HTTP/1.1
50	5.544119	139.19.106.154	94.232.175.143	HTTP	494	GET /CaptchaImage.axd?guid=7dcc9e3-f5a2-44ea-944 GET /CaptchaImage.axd?guid=9b6e4ddc-4aef-4d28-88 5.621143
68	5.563205	139.19.106.154	94.232.175.143	HTTP	494	GET /CaptchaImage.axd?guid=9b6e4ddc-4aef-4d28-84 5.567596
88	5.621143	139.19.106.154	94.232.175.143	HTTP/J...	625	POST /Services/VisitorCounterService.asmx/Insert 84 5.567596
84	5.567596	94.232.175.143	139.19.106.154	HTTP	244	HTTP/1.1 200 OK (text/html)
95	5.657917	94.232.175.143	139.19.106.154	HTTP	463	HTTP/1.1 200 OK (JPEG JFIF image)
99	5.668337	94.232.175.143	139.19.106.154	HTTP	909	HTTP/1.1 200 OK (JPEG JFIF image)
102	5.706776	94.232.175.143	139.19.106.154	HTTP/J...	302	HTTP/1.1 200 OK , JSON (application/json)

Frame 15: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{DAD9CF95-76D2-487B-E0050	32 20 48 54 54 50 2f 31 2e 31 3d 0a 48 6f 73 74
Ethernet II, Src: Intel e2:75:b1 (60:0d:8e:e2:75:b1), Dst: Cisco_96:a0:00 (00:23:05:96:a0:00)	0060 3a 20 66 61 72 7a 61 6e 65 67 61 6e 32 74 2e 69
Internet Protocol Version 4, Src: 139.19.106.154, Dst: 94.232.175.143	0070 72 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
Transmission Control Protocol, Src Port: 56581, Dst Port: 80, Seq: 1, Ack: 1, Len: 472	0080 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64
HTTP/1.1 200 OK (text/html)	0090 6f 77 73 29 4e 28 30 28 31 30 2e 30 3b 28 57 69 6e
HTTP/1.1 200 OK (JPEG JFIF image)	00a0 36 34 3b 28 78 36 34 3b 28 72 76 3a 31 32 37 2e
HTTP/1.1 200 OK (JPEG JFIF image)	00b0 30 29 20 47 65 63 6b ef 2f 32 30 31 38 30 31 36
HTTP/1.1 200 OK , JSON (application/json)	00c0 31 20 46 69 72 65 66 6f 78 2f 31 32 37 2e 30 0d
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0\r\n	00d0 04 41 63 65 78 74 3a 20 74 65 78 74 2f 68 74
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n	00e0 6d 6c 2e 61 78 76 69 63 61 74 69 6f 6e 2f 78
Accept-Language: en-US,en;q=0.5\r\n	00f0 68 74 60 6c 2b 78 6d 62 2c 61 70 78 6d 69 63 61
Accept-Encoding: gzip, deflate\r\n	0100 74 69 6f 6e 2f 78 6d 63 71 3d 38 2e 39 2e 69
Referer: http://farzanegan2t.ir/\r\n	0110 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f
Connection: keep-alive\r\n	0120 77 65 62 70 2c 2a 2f 2a 3b 71 3d 38 2e 38 0d 0a
Cookie: ASP.NET_SessionId=jhuthfwrbxsxyswda5zb2w50\r\n	0130 41 63 65 78 74 2d 4c 61 6e 67 75 61 67 65 3a
Upgrade-Insecure-Requests: 1\r\n	0140 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d
Priority: u1\r\n	0150 0a 41 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67
\r\n	0160 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d
[Full request URI: http://farzanegan2t.ir/Default.aspx?PageId=72]	0170 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f
[HTTP request 1/2]	0180 2f 6d 61 72 7a 6e 65 67 61 6e 32 74 2e 69 72
[Response in frame: 84]	0190 2f 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b
[Next request in frame: 88]	01a0 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6b 69
	01b0 65 3a 20 41 53 50 2e 4e 45 54 5f 53 65 73 73 69

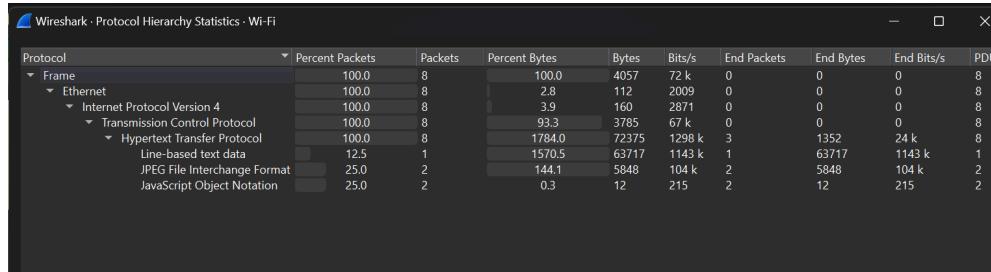
می‌توان دید که مربوطه همان host farzanegan2t.ir است که وارد کردہ‌ایم. حال می‌توان به سوالات پاسخ داد.

پاسخ به سوالات

۱ - مطابق شکل زیر از تب statistics به بخش protocol hierarchy می‌رویم:

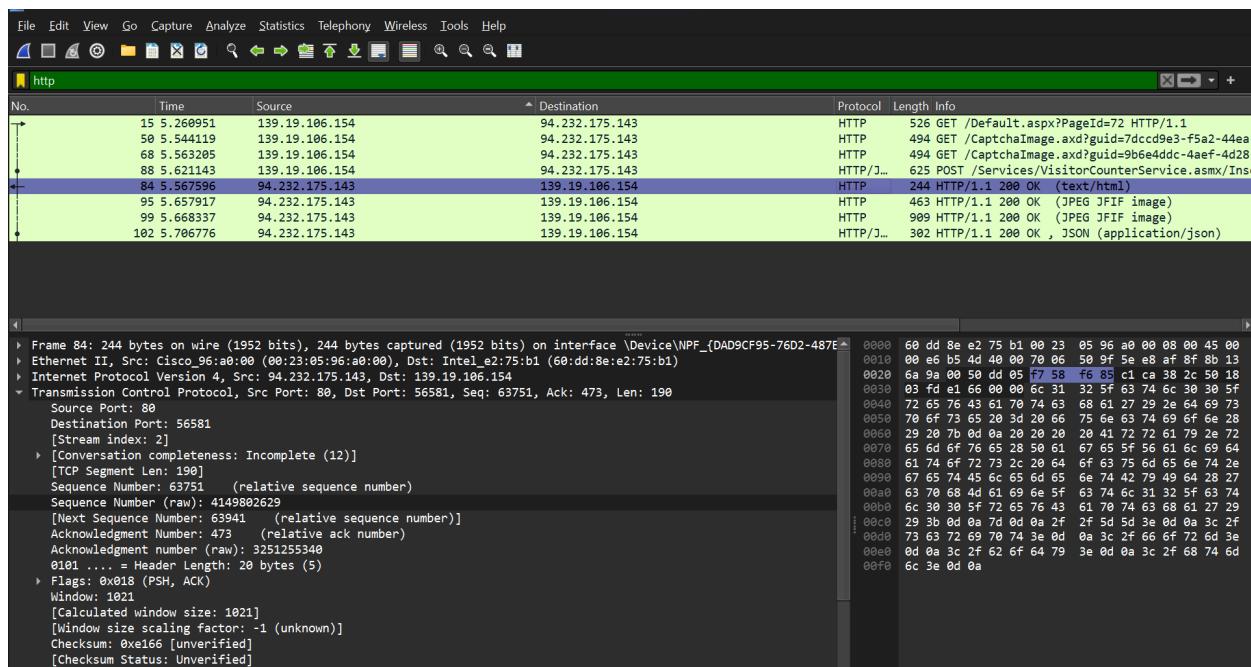


سپس روی آن کلیک می‌کنیم و سلسله مراتب پروتکل‌ها را مشاهده می‌کنیم.



مشاهده می‌شود که تمام بسته‌ها از لایه‌ی لینک frame و فیزیکی Ethernet عبور کرده‌اند. در لایه‌ی network هم همه‌ی بسته‌ها هستند. در لایه‌ی transport هم همگی tcp بوده و در لایه‌ی application هم همه‌ی بسته‌ها http هستند.

۲ - می‌توان دید که پاسخ مربوط به اولین بسته‌ی get که در بالا دیدیم، این پاسخ html است:



اگر چنین باشد، اختلاف زمانی بین درخواست و پاسخ، با استفاده از ستون time محاسبه می‌شود که حدوداً برابر با $0.3 = 5.26 - 5.56$ خواهد بود.

برای بخش بعد که درمورد شماره‌ی sequence number اولین ارتباط tcp پرسیده شده است، ابتدا فیلتر را روی tcp می‌گذاریم. اولین درخواست که فلگ syn هم دارد به این صورت است:

No.	Time	Source	Destination	Protocol	Length	Info
14	5.259679	139.19.106.154	94.232.175.44	TCP	66	56588 → 443 [SYN] Seq=0 Win=64240 Len=0
15	5.260951	139.19.106.154	94.232.175.44	HTTP	526	GET /Default.aspx?PageId=72 HTTP/1.1
16	5.361183	94.232.175.44	139.19.106.154	TCP	66	443 → 56588 [SYN, ACK] Seq=0 Ack=1 Win=131072
17	5.361277	139.19.106.154	94.232.175.44	TCP	54	56588 → 443 [ACK] Seq=1 Ack=1 Win=131072
18	5.362267	139.19.106.154	94.232.175.44	TLSv1.2	722	Client Hello (SNI=theme.behsamanco.com)
19	5.391366	94.232.175.44	139.19.106.154	TCP	60	80 → 56581 [ACK] Seq=1 Ack=473 Win=1024
20	5.470856	94.232.175.44	139.19.106.154	TCP	1304	443 → 56588 [ACK] Seq=1 Ack=669 Win=131072
21	5.470856	94.232.175.44	139.19.106.154	TCP	1304	443 → 56588 [ACK] Seq=1251 Ack=669 Win=131072
22	5.470856	94.232.175.44	139.19.106.154	TLSv1.2	886	Server Hello, Certificate, Server Key Exchange
23	5.470197	139.19.106.154	94.232.175.44	TCP	54	56588 → 443 [ACK] Seq=669 Ack=3333 Win=131072
24	5.473167	139.19.106.154	94.232.175.44	TLSv1.2	204	Client Key Exchange, Change Cipher Spec
25	5.502025	139.19.106.154	52.182.143.208	TLSv1.2	134	Application Data

Frame 14: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 'Device\NPF_{DAD9CF95-76D2-487B-B8ED}' at 00:23:05:96:a0:00 (00:23:05:96:a0:00)
Ethernet II, Src: Intel_e2:75:b1 (60:dd:8e:e2:75:b1), Dst: Cisco_96:a0:00 (00:23:05:96:a0:00)
Internet Protocol Version 4, Src: 139.19.106.154, Dst: 94.232.175.44
Transmission Control Protocol, Src Port: 56588, Dst Port: 443, Seq: 0, Len: 0

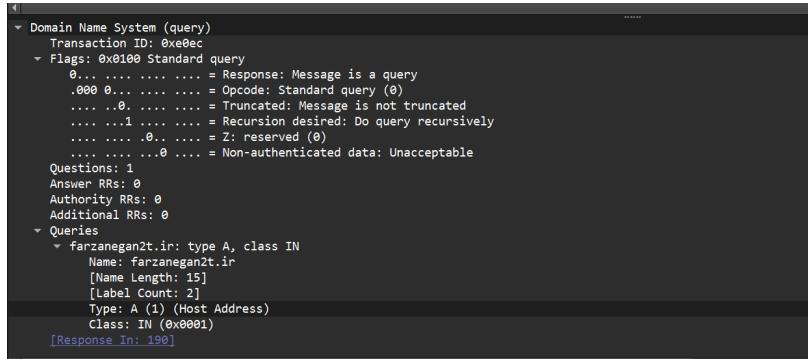
Source Port: 56588
Destination Port: 443
[Stream index: 1]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2856827015
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 ... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x03e9 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP)
[Timestamps]

میتوان دید که مقدار dns raw sequence number در این بسته برابر با 2856827015 است.

۳ - در واپرشارک فیلتر dns را اعمال میکنیم تا بسته‌های نوع dns را ببینیم:

No.	Time	Source	Destination	Protocol	Length	Info
13	4.053797	139.19.106.154	139.19.66.1	DNS	73	Standard query 0x904d A www.adidas.de
14	4.053950	139.19.106.154	139.19.66.1	DNS	73	Standard query 0xf2b8 A www.amazon.de
15	4.054098	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x827e A mail.google.com
16	4.054187	139.19.106.154	139.19.66.1	DNS	69	Standard query 0xa442 A quera.org
17	4.054187	139.19.106.154	139.19.66.1	DNS	76	Standard query 0xe8d6 A www.overleaf.com
18	4.054209	139.19.106.154	139.19.66.1	DNS	73	Standard query 0xc8af A cw.sharif.edu
19	4.060298	139.19.66.1	139.19.106.154	DNS	89	Standard query response 0xc8af A cw.sharif.edu A 81.31.170.68
20	4.060298	139.19.66.1	139.19.106.154	DNS	110	Standard query response 0xe8d6 A www.overleaf.com CNAME lb2.ov
21	4.060298	139.19.66.1	139.19.106.154	DNS	91	Standard query response 0x827e A mail.google.com A 142.250.186
22	4.060810	139.19.106.154	139.19.66.1	DNS	73	Standard query 0x85bf A cw.sharif.edu
23	4.060810	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x3546 A mail.google.com
24	4.060814	139.19.106.154	139.19.66.1	DNS	76	Standard query 0xcee2 A lb2.overleaf.com
25	4.064475	139.19.66.1	139.19.106.154	DNS	92	Standard query response 0xcee2 A lb2.overleaf.com A 34.120.52.0
26	4.064475	139.19.66.1	139.19.106.154	DNS	89	Standard query response 0x85bf A cw.sharif.edu A 81.31.170.68
27	4.064475	139.19.66.1	139.19.106.154	DNS	91	Standard query response 0x3546 A mail.google.com A 142.250.186
28	4.064864	139.19.106.154	139.19.66.1	DNS	76	Standard query 0x139f AAAA lb2.overleaf.com
29	4.064871	139.19.106.154	139.19.66.1	DNS	75	Standard query 0xb789 AAAA mail.google.com
30	4.064871	139.19.106.154	139.19.66.1	DNS	73	Standard query 0x30c1 AAAA cw.sharif.edu
31	4.069235	139.19.66.1	139.19.106.154	DNS	185	Standard query response 0x904d A www.adidas.de CNAME www.adida
32	4.069774	139.19.106.154	139.19.66.1	DNS	83	Standard query 0x3d83 A e46636.a.akamaiedge.net
33	4.070740	139.19.66.1	139.19.106.154	DNS	103	Standard query response 0xb789 AAAA mail.google.com AAAA 2a00:0
34	4.070740	139.19.66.1	139.19.106.154	DNS	151	Standard query response 0x139f AAAA lb2.overleaf.com SOA bob.n
35	4.072226	139.19.66.1	139.19.106.154	DNS	101	Standard query response 0xa442 A quera.org A 185.143.233.61 A :
36	4.072995	139.19.106.154	139.19.66.1	DNS	69	Standard query 0xa745 A quera.org

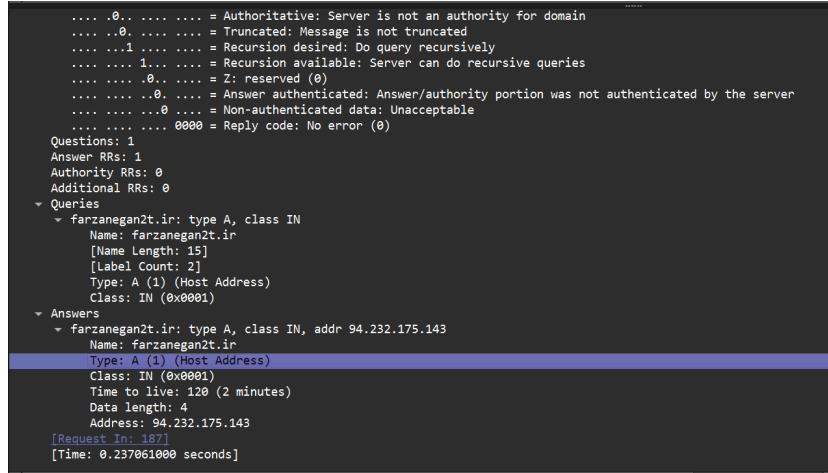
اگر فیلتر dns query را اعمال کنیم، بسته‌های dns && ip.src==139.19.106.154 را می‌بینیم:



```
Domain Name System (query)
  Transaction ID: 0xe0ec
  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
    farzanehan2t.ir: type A, class IN
      Name: farzanehan2t.ir
      [Name Length: 15]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Response In: 190]
```

می‌توان مشاهده کرد که تایپ این کوئری A است.

خروجی آن هم به این شکل است:



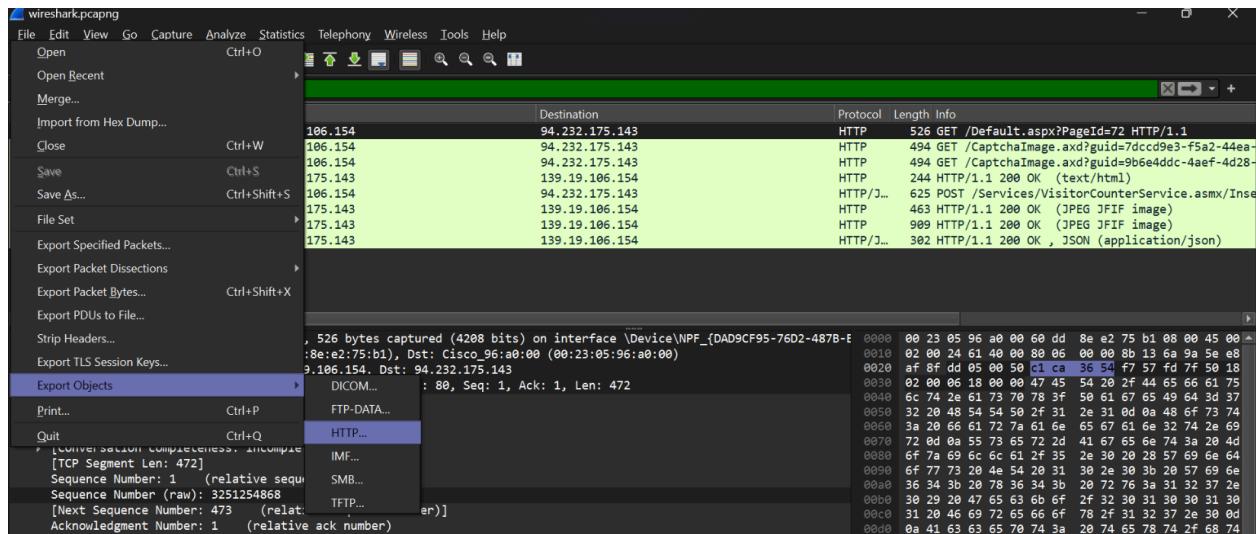
```
.... .0. .... .... = Authoritative: Server is not an authority for domain
.... .0. .... .... = Truncated: Message is not truncated
.... ..1 .... .... = Recursion desired: Do query recursively
.... ..1. .... .... = Recursion available: Server can do recursive queries
.... ..0. .... .... = Z: reserved (0)
.... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... .... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  farzanehan2t.ir: type A, class IN
    Name: farzanehan2t.ir
    [Name Length: 15]
    [Label Count: 2]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
  Answers
    farzanehan2t.ir: type A, class IN, addr 94.232.175.143
      Name: farzanehan2t.ir
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 120 (2 minutes)
      Data length: 4
      Address: 94.232.175.143
      [Request In: 187]
      [Time: 0.237061000 seconds]
```

می‌توان دید که تایپ آن هم A است. A مخفف address است و رایج ترین تایپ dns query است.

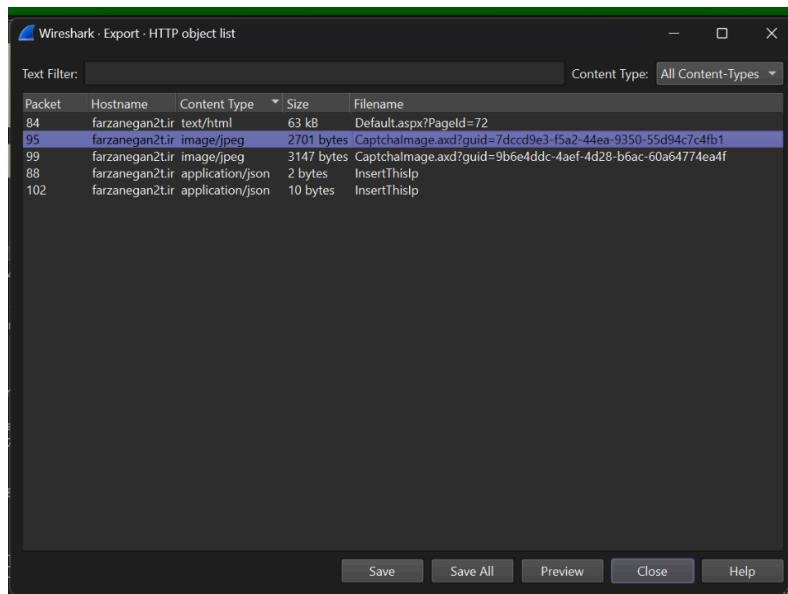
معنی آن هم این است که به دنبال آدرس ip هستیم. تایپ دیگری که ممکن بود، AAAA است و مربوط

به ipv6 می‌شود.

۴ - برای بازیابی عکس‌ها، طبق تصاویر زیر به منوی file > export objects > http می‌رویم. سپس از



منوی باز شده، تصویر مورد نظر (و یا همهٔ تصاویر) را انتخاب کرده و save را می‌زنیم تا ذخیره شوند.



به این صورت تصاویر بازیابی می‌شوند. یکی از این تصاویر به این صورت است:

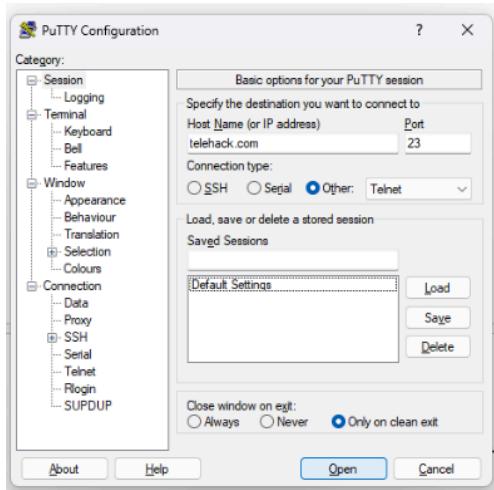


بخش دوم. بررسی ارتباط از طریق Telnet

شرح آزمایش

در این آزمایش هدف این است که از پروتکل تلننت استفاده کنیم و پیام‌های ضبط شده را از طریق wireshark بررسی کنیم.

مراحل



همانند دستور کار، ابتدا wireshark را در حالت capture قرار می‌دهیم تا ارتباطات را ضبط کند. سپس putty را باز می‌کنیم و گزینه‌ی telnet را به عنوان connection type می‌گذاریم. سپس هم آدرس telehack.com/ و پورت ۲۳ را وارد می‌کنیم.

در پنجره‌ی باز شده، دستوراتی از قبیل help, date, echo را امتحان می‌کنیم.

```

Connected to TELEHACK port 133
It is 7:08 am on Friday, July 12, 2024 in Mountain View, California, USA.
There are 99 local users. There are 26648 hosts on the network.

May the command line live forever.

Command, one of the following:
  2048 ? a2 advent aquarium bf
  c8 cal calc callsign ching clear
  cowsay delta dir echo eliza file
  finger fnord geopol gif ipaddr joke
  mac md5 minesweeper more netstat newuser
  octopus phoon pig primes qr rain
  rainbow rand recover rig roll rot13
  run salvo sleep starwars sudoku tail
  today traceroute typespeed units uptime usenet
  users uumap uuplot weather when zork

More commands available after login. Type HELP for a detailed command list.
Type NEWUSER to create an account. Press control-C to interrupt any command.
.
```

پس از آن به وایرشارک می‌رویم تا بسته‌ها را بررسی کنیم. فیلتر را هم telnet قرار می‌دهیم. می‌توان مشاهده کرد که وقتی ما مثلا دستور help را وارد کرده‌ایم، حروف آن به صورت جدا جدا فرستاده شده‌اند. پس از آن هم یک \n\ فرستاده شده است. ریسپانس آن ولی همزمان فرستاده شده و به شکل زیر است:

No.	Time	Source	Destination	Protocol	Length	Info
1033	35.412548	64.13.139.230	139.19.106.154	TELNET	60	Telnet Data ...
1034	35.442482	139.19.106.154	64.13.139.230	TELNET	55	Telnet Data ...
1042	35.601434	64.13.139.230	139.19.106.154	TELNET	60	Telnet Data ...
1045	35.803106	64.13.139.230	139.19.106.154	TELNET	60	Telnet Data ...
1048	36.424651	139.19.106.154	64.13.139.230	TELNET	55	Telnet Data ...
1049	36.660415	64.13.139.230	139.19.106.154	TELNET	60	Telnet Data ...
1071	38.668732	139.19.106.154	64.13.139.230	TELNET	55	Telnet Data ...
1083	38.829178	64.13.139.230	139.19.106.154	TELNET	60	Telnet Data ...
1084	38.832112	64.13.139.230	139.19.106.154	TELNET	1304	Telnet Data ...
1088	39.016753	64.13.139.230	139.19.106.154	TELNET	180	Telnet Data ...
1228	44.014403	139.19.106.154	64.13.139.230	TELNET	55	Telnet Data ...
1232	44.175997	64.13.139.230	139.19.106.154	TELNET	60	Telnet Data ...
1234	44.176077	64.13.139.230	139.19.106.154	TELNET	60	Telnet Data ...
Telnet						
Data: 2048		sliding tile puzzle game\r\n			0020	6a 9a 00 17 d8 44 6e 00 9d ff 68 a0 7e 65 50 10
Data: ?		show command list\r\n			0030	01 f6 ab 31 00 00 32 30 34 38 20 20 20 20 20 20
Data: a2 <disk> file>		apple] emulator\r\n			0040	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data: advent		play adventure\r\n			0050	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data: aquarium		an aquarium/sea animation in ASCII art\r\n			0060	65 20 75 75 75 75 75 75 75 75 75 75 75 75 75 75
Data: areacode <areacode> location>		look up an areacode or location\r\n			0070	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data: basic		start the basic interpreter\r\n			0080	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data: bf [code]<file>		brainf*ck interpreter\r\n			0090	6f 77 20 63 6f 6d 6d 61 6e 64 20 6c 69 73 74 0d
Data: c8 [rom]		launch CHIP-8 emulator\r\n			00a0	00 61 32 20 3c 64 69 73 6b 7c 66 69 6c 65 3e 20
Data: cal [year]		print a calendar\r\n			00b0	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data: calc [expr]		calculator\r\n			00c0	61 70 70 6c 65 20 5d 5b 20 65 6d 75 6c 61 74 6f
Data: callsign <text>		lookup information for an amateur radio callsign\r\n			00d0	72 0d 0a 61 64 76 65 6e 74 20 20 20 20 20 20 20
Data: cat <file>		dump contents of file\r\n			00e0	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data: ching		The Book of Changes\r\n			00f0	20 20 70 6c 61 79 20 61 64 76 65 6e 74 75 72 65
Data: clear		clear screen\r\n			0100	0d 0a 61 71 75 61 72 69 75 6d 20 20 20 20 20 20
Data: clock [/font=font]		figlet time display. type figlet for a font list\r\n			0110	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Data: cowsay [/cow] <message>		configurable speaking cow\r\n			0120	20 61 66 20 61 71 75 61 72 69 75 6d 2f 73 65 61
Data: date		print day and time\r\n			0130	20 61 6e 69 6d 61 74 69 6f 6e 20 69 6e 20 41 53
Data: ddate		convert Gregorian dates to Discordian dates\r\n			0140	43 49 49 20 61 72 74 6d 0a 61 72 65 61 63 6f 64
Data: delta		convert timestamp to delta time string\r\n			0150	65 20 3c 61 72 65 61 63 6f 64 65 7c 6c 6f 63 61
Data: diff <filea> <fileb>		show the difference between two files\r\n			0160	74 69 6f 6e 3a 20 20 20 6c 6f 6f 6b 20 75 70 20
Data: dir					0170	61 6e 20 61 72 65 61 63 6f 64 65 28 6f 72 20 6c
					0180	6f 63 61 74 69 6f 6e 0d 0a 62 61 73 69 63 20 20
					0190	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
					01a0	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
					01b0	75 74 61 77 74 20 74 65 68 74

پاسخ به سوالات

۱ - فایل wireshark را در telnet.pcap باز می‌کنیم:

No.	Time	Source	Destination	Protocol	Length	Info
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 TSeq=10233652
16	0.159227	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=194 Ack=73 Win=32120 Len=0 TSval=10233652
26	0.209216	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=198 Ack=101 Win=32120 Len=0 TSval=10233657
28	0.229239	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=198 Ack=133 Win=32120 Len=0 TSval=10233659
30	1.329229	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=198 Ack=140 Win=32120 Len=0 TSval=10233769
37	2.589229	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=207 Ack=152 Win=32120 Len=0 TSval=10233895
41	3.859250	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=213 Ack=154 Win=32120 Len=0 TSval=10234022
46	5.159238	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=216 Ack=217 Win=32120 Len=0 TSval=10234152
48	5.179239	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=216 Ack=705 Win=32120 Len=0 TSval=10234154
56	5.209229	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=216 Ack=707 Win=32120 Len=0 TSval=10234157
64	23.399242	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=242 Ack=1014 Win=32120 Len=0 TSval=1023597

برای این که ببینیم کلاینت کدام یک است، می‌توان فیلتر `tcp.flags.syn == 1` را اعمال کرد:

tcp.flags.syn == 1						
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 TStamp=102336
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1448 WS=1 TStamp=102336

بنابراین می‌توان نتیجه گرفت که اولین ریکوئست از کلاینت به سرور زده شده است (`syn` فعال است) و دومی از سرور به کلاینت است (`syn ack`). پس آیپی کلاینت برابر با 192.168.0.2 بوده و آیپی سرور برابر با 192.168.0.1 است.

۲ - بسته‌های telnet را فیلتر می‌کنیم. می‌توان در لیست دید که شماره ۲۹ از سمت سرور فرستاده شده و دیتای آن عبارت "login" است.

telnet						
No.	Time	Source	Destination	Protocol	Length	Info
17	0.159844	192.168.0.2	192.168.0.1	TELNET	151	Telnet Data ...
19	0.181267	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
20	0.181378	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
22	0.196306	192.168.0.1	192.168.0.2	TELNET	78	Telnet Data ...
23	0.196427	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
25	0.198286	192.168.0.1	192.168.0.2	TELNET	81	Telnet Data ...
27	0.210527	192.168.0.1	192.168.0.2	TELNET	98	Telnet Data ...
29	1.317863	192.168.0.1	192.168.0.2	TELNET	73	Telnet Data ...
31	2.561993	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
33	2.575446	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
34	2.575598	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
36	2.577672	192.168.0.1	192.168.0.2	TELNET	75	Telnet Data ...
38	3.581505	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
40	3.847152	192.168.0.1	192.168.0.2	TELNET	68	Telnet Data ...
42	3.860413	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
43	3.860571	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...

```

> Frame 29: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: WesternDigit_9f:a0:97 (00:00:c0:9f:a0:97), Dst: LiteOnCommun_3b:bf:fa (00:a0:cc:3b:bf:fa)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
> Transmission Control Protocol, Src Port: 23, Dst Port: 1550, Seq: 133, Ack: 198, Len: 7
    Telnet
        Data: login:

```

در پاسخ به آن، کلاینت fake را فرستاده است. یعنی این یوزرنیم است.

telnet						
No.	Time	Source	Destination	Protocol	Length	Info
27	0.210527	192.168.0.1	192.168.0.2	TELNET	98	Telnet Data ...
29	1.317863	192.168.0.1	192.168.0.2	TELNET	73	Telnet Data ...
31	2.561993	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
33	2.575446	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
34	2.575598	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
36	2.577672	192.168.0.1	192.168.0.2	TELNET	75	Telnet Data ...
38	3.581505	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
40	3.847152	192.168.0.1	192.168.0.2	TELNET	68	Telnet Data ...
42	3.860413	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
43	3.860571	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...

```

> Frame 31: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: LiteOnCommun_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternDigit_9f:a0:97 (00:00:c0:9f:a0:97)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 1550, Dst Port: 23, Seq: 198, Ack: 140, Len: 6
    Telnet
        Data: fake\r\n

```

پس از آن، سرور درخواست پسورد کرده است:

33 2.575446	192.168.0.1	192.168.0.1	TELNET	72 Telnet Data ...
34 2.575598	192.168.0.2	192.168.0.1	TELNET	69 Telnet Data ...
36 2.577672	192.168.0.1	192.168.0.2	TELNET	75 Telnet Data ...
38 3.581505	192.168.0.2	192.168.0.1	TELNET	72 Telnet Data ...
40 3.847152	192.168.0.1	192.168.0.2	TELNET	68 Telnet Data ...
42 3.860413	192.168.0.1	192.168.0.2	TELNET	69 Telnet Data ...
43 3.860571	192.168.0.2	192.168.0.1	TELNET	69 Telnet Data ...

```

> Frame 36: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
> Ethernet II, Src: WesternDigit_9f:a0:97 (00:00:c0:9f:a0:97), Dst: LiteOnCommun_3b:bf:fa (00:a0:cc:3b:bf:fa)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
> Transmission Control Protocol, Src Port: 23, Dst Port: 1550, Seq: 143, Ack: 207, Len: 9
    Telnet
        Data: Password:

```

در پیام بعدی، کلاینت user را فرستاده است که یعنی پسورد است.

33 2.575446	192.168.0.1	192.168.0.2	TELNET	69 Telnet Data ...
34 2.575598	192.168.0.2	192.168.0.1	TELNET	75 Telnet Data ...
36 2.577672	192.168.0.1	192.168.0.2	TELNET	72 Telnet Data ...
38 3.581505	192.168.0.2	192.168.0.1	TELNET	68 Telnet Data ...
40 3.847152	192.168.0.1	192.168.0.2	TELNET	69 Telnet Data ...
42 3.860413	192.168.0.1	192.168.0.2	TELNET	69 Telnet Data ...
43 3.860571	192.168.0.2	192.168.0.1	TELNET	69 Telnet Data ...

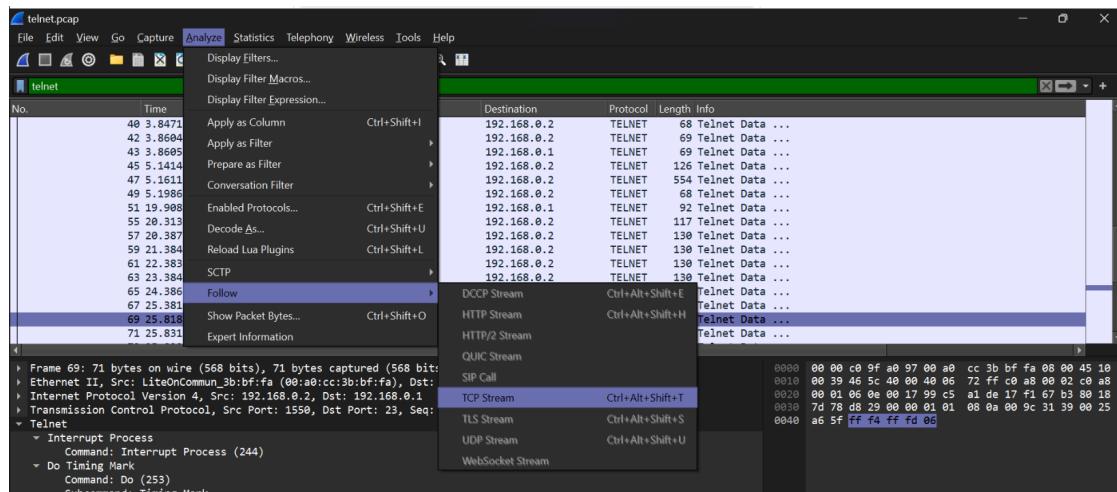
```

> Frame 38: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: LiteOnCommun_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternDigit_9f:a0:97 (00:00:c0:9f:a0:97)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 1550, Dst Port: 23, Seq: 207, Ack: 152, Len: 6
    Telnet
        Data: user\r\n

```

پس در نهایت یوزرنیم برابر با fake و پسورد برابر با user خواهد بود.

۳ - برای بررسی این مورد، هم می‌توان بسته‌ها را جدا جدا چک کرد، هم این که از امکانات وایرشارک کمک بگیریم. مانند شکل زیر، به قسمت analyze > follow > tcp stream می‌رویم:



در خروجی (تصویر بالا) می‌توان مشاهده کرد که کلاینت پس از لگین، دستورهای زیر (قسمت‌های قرمز تصویر) را استفاده کرده است:

/sbin/ping www.yahoo.com

ls

ls -a

exit

The screenshot shows a terminal window on an OpenBSD system. The session starts with a root login:

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

Following the login, the system displays its welcome message and information about reporting bugs:

```
.....
OpenBSD/1386 (oof) (tty2)

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

.....
Last login: Sat Nov 27 20:11:43 on ttym2 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.
```

The user then runs the /sbin/ping command to test connectivity to www.yahoo.com:

```
$ /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=75.868 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
```

Finally, the user exits the terminal session:

```
$ ls
$ ls -a
. .. .cshrc .login .mailrc .profile .rhosts
$ exit
```

At the bottom of the terminal window, there is a status bar with the text: "Packet 67. 16 client ppts, 30 server ppts, 30 turns. Click to select."

بخش سوم. بررسی و درخواست پاسخهای DNS

شرح آزمایش

در این آزمایش هدف این است با خروجی‌های دستور ipconfig و nslookup یا همچنین dig یا آشنا شویم.

مراحل

ابتدا طبق دستور کار دستور ipconfig /all را در ترمینال ویندوز وارد می‌کنیم تا خروجی‌های زیر را مشاهده کنیم:

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

Windows IP Configuration

Host Name . . . . . : DESKTOP-MUJ2RFM
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : mpi-klsb.mpg.de
                                         mpi-inf.mpg.de
                                         mpi-sws.org
                                         mpi-sb.mpg.de

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Intel(R) Ethernet Connection (13) I219-V
    Physical Address. . . . . : 50-EB-F6-8D-36-96
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 60-DD-8E-E2-75-B2
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : 62-DD-8E-E2-75-B1
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::b5ec:8941:6196:f8d5%6(Preferred)
    IPv4 Address. . . . . : 192.168.137.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
```

```

Physical Address . . . . . : 60-DD-8E-E2-75-B2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 62-DD-8E-E2-75-B1
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b5ec:8941:6196:f8d5%6(PREFERRED)
IPv4 Address. . . . . : 192.168.137.1(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : mpi-klslb.mpg.de
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : 60-DD-8E-E2-75-B1
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ca51:4913:9b7a:9643%29(PREFERRED)
IPv4 Address. . . . . : 139.19.106.154(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, July 12, 2024 2:28:03 PM
Lease Expires . . . . . : Friday, July 12, 2024 5:59:54 PM
Default Gateway . . . . . : 139.19.106.254
DHCP Server . . . . . : 139.19.68.233
DHCPv6 IID . . . . . : 341892494
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-93-8D-C6-50-EB-F6-8D-36-96
DNS Servers . . . . . : 139.19.66.1
                               139.19.68.1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                               mpi-klslb.mpg.de
                               mpi-inf.mpg.de
                               mpi-sws.org
                               mpi-sb.mpg.de

```

اطلاعات در عکس‌های بالا مشاهده می‌شوند. حال دستور flushdns را می‌زنیم تا کش مربوط به dns را در host خود پاک کنیم. خروجی به این صورت است:

```
C:\Windows\System32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

حال wireshark را در حالت capture قرار می‌دهیم. سپس دستور nslookup را برای سایت sharif.edu وارد می‌کنیم.

```
C:\Windows\System32>nslookup sharif.edu
server:  nsintern2.mpi-klslb.mpg.de
Address: 139.19.66.1

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

می‌توان دید که درخواست به سرور nsintern2.mpi-klslb.mpg.de ارسال شده است که در خروجی دستور ipconfig هم دیدیم DNS Suffix Search List در لیست mpi-klslb.mpg.de هم بود. آدرس آن را هم می‌توان مشاهده کرد.

آیپی ما برابر با 139.19.106.154 است. در وایرشارک در بین پیامهای capture شده، باید فیلتر اعمال کنیم تا بتوانیم پیامهای نوع dns برای ip.addr == 139.19.106.154 && dns گیرنده یا فرستنده‌ی آنها را ببینیم:

No.	Time	Source	Destination	Protocol	Length	Info
33	1.422256	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x0820 A ssl.gstatic.com
35	1.425784	139.19.66.1	139.19.106.154	DNS	91	Standard query response 0x0820 A ssl.gstatic.com A 142.250.185
36	1.426740	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x77fe A ssl.gstatic.com
43	1.435207	139.19.66.1	139.19.106.154	DNS	91	Standard query response 0x77fe A ssl.gstatic.com A 142.250.185
44	1.435576	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x8d54 AAAA ssl.gstatic.com
46	1.440214	139.19.66.1	139.19.106.154	DNS	103	Standard query response 0x8d54 AAAA ssl.gstatic.com AAAA 2a00::
48	47.706247	139.19.106.154	139.19.66.1	DNS	72	Standard query 0x116b A www.bing.com
49	47.706546	139.19.106.154	139.19.66.1	DNS	72	Standard query 0x0088 HTTPS www.bing.com
432	47.731667	139.19.66.1	139.19.106.154	DNS	277	Standard query response 0x0088 HTTPS www.bing.com CNAME www-ww
433	47.744637	139.19.66.1	139.19.106.154	DNS	343	Standard query response 0x116b A www.bing.com CNAME www-www.bi
459	49.556301	139.19.106.154	139.19.66.1	DNS	84	Standard query 0x0001 PTR 1.66.19.139.in-addr.arpa
460	49.569326	139.19.66.1	139.19.106.154	DNS	123	Standard query response 0x0001 PTR 1.66.19.139.in-addr.arpa PTR
461	49.570801	139.19.106.154	139.19.66.1	DNS	70	Standard query 0x0002 A sharif.edu
462	49.698819	139.19.66.1	139.19.106.154	DNS	86	Standard query response 0x0002 A sharif.edu A 152.89.13.54
463	49.695723	139.19.106.154	139.19.66.1	DNS	70	Standard query response 0x0003 AAAA sharif.edu
464	49.798133	139.19.106.154	139.19.66.1	DNS	96	Standard query 0x37bd A functional.events.data.microsoft.com
465	49.798525	139.19.106.154	139.19.66.1	DNS	96	Standard query 0xc5e4 HTTPS functional.events.data.microsoft.co
468	49.859193	139.19.66.1	139.19.106.154	DNS	286	Standard query response 0xc5e4 HTTPS functional.events.data.mi
469	49.859193	139.19.66.1	139.19.106.154	DNS	229	Standard query response 0x37bd A functional.events.data.microsoft
481	50.612285	139.19.66.1	139.19.106.154	DNS	130	Standard query response 0x0003 AAAA sharif.edu SOA ns1.sharif.edu
500	54.579478	139.19.106.154	139.19.66.1	DNS	91	Standard query 0x353f A signaler-pa.clients6.google.com
501	54.591701	139.19.66.1	139.19.106.154	DNS	107	Standard query response 0x353f A signaler-pa.clients6.google.com
502	54.592287	139.19.106.154	139.19.66.1	DNS	91	Standard query 0xddcc A signaler-pa.clients6.google.com
503	54.594520	139.19.66.1	139.19.106.154	DNS	107	Standard query response 0xddcc A signaler-pa.clients6.google.com
504	54.594699	139.19.106.154	139.19.66.1	DNS	91	Standard query 0x7717 AAAA signaler-pa.clients6.google.com
505	54.597045	139.19.66.1	139.19.106.154	DNS	119	Standard query response 0x7717 AAAA signaler-pa.clients6.google.com
799	91.535376	139.19.106.154	139.19.66.1	DNS	92	Standard query 0x8f17 A mobile.events.data.microsoft.com

```

> Frame 33: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{DAD9CF95-76D2-487B-B8E
> Ethernet II, Src: Intel_e2:75:b1 (00:0d:8e:e2:75:b1), Dst: Cisco_96:a0:00 (00:23:05:96:a0:00)
> Internet Protocol Version 4, Src: 139.19.106.154, Dst: 139.19.66.1
> User Datagram Protocol, Src Port: 64726, Dst Port: 53
- Domain Name System (query)
  Transaction ID: 0x0820
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0

```

پاسخ به سوالات

۱ - همان طور که در شرح آزمایش گفتیم، درخواست برای سرور nsintern2.mpi-klslb.mpg.de آدرس 139.19.66.1 ارسال می‌شود و در اینجا از همان سرور هم دریافت شده است. این موضوع را می‌توان با اعمال کوئری ip.addr!=139.19.66.1 && dns متوجه شد.

در این مثال این دستور خروجی خالی برمی‌گرداند که به این معنی است که هر بسته‌ای یا به این سرور فرستاده شده است یا از آن دریافت شده است.

No.	Time	Source	Destination	Protocol	Length	Info

خود اولین بسته مربوط به dns هم به این صورت است (فیلتر nslookup را اعمال کرده‌ایم):

```

> Frame 461: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{DAD9CF95-76D2-487B-B8E1
> Ethernet II, Src: Intel_e2:75:b1 (60:dd:8e:e2:75:b1), Dst: Cisco_96:a0:00 (00:23:05:96:a0:00)
> Internet Protocol Version 4, Src: 139.19.106.154, Dst: 139.19.66.1
> User Datagram Protocol, Src Port: 63083, 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
        > sharif.edu: type A, class IN
            Name: sharif.edu
            [Name Length: 10]
            [Label Count: 2]
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            [Response In: 462]

```

۲ - ابتدا پیام‌های request را بررسی می‌کنیم. با اعمال فیلتر dns && ip.dst==139.19.66.1 این بسته‌ها به دست می‌آیند:

No.	Time	Source	Destination	Protocol	Length	Info
33	1.422256	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x0820 A ssl.gstatic.com
36	1.426740	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x77fe A ssl.gstatic.com
44	1.435576	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x8d54 AAAA ssl.gstatic.com
438	47.706247	139.19.106.154	139.19.66.1	DNS	72	Standard query 0x116b A www.bing.com
431	47.706546	139.19.106.154	139.19.66.1	DNS	72	Standard query 0x0008 HTTPS www.bing.com
459	49.556301	139.19.106.154	139.19.66.1	DNS	84	Standard query 0x0001 PTR 1.66.19.139.in-addr.arpa
461	49.570801	139.19.106.154	139.19.66.1	DNS	70	Standard query 0x0002 A sharif.edu
463	49.695723	139.19.106.154	139.19.66.1	DNS	70	Standard query 0x0003 AAAA sharif.edu
464	49.798133	139.19.106.154	139.19.66.1	DNS	96	Standard query 0x37bd A functional.events.data.microsoft.com
465	49.798525	139.19.106.154	139.19.66.1	DNS	96	Standard query 0xc5e4 HTTPS functional.events.data.microsoft.com
506	54.579478	139.19.106.154	139.19.66.1	DNS	91	Standard query 0x353f A signaler-pa.clients6.google.com
502	54.592287	139.19.106.154	139.19.66.1	DNS	91	Standard query 0xddcc A signaler-pa.clients6.google.com
504	54.594699	139.19.106.154	139.19.66.1	DNS	91	Standard query 0x7717 AAAA signaler-pa.clients6.google.com
799	91.535376	139.19.106.154	139.19.66.1	DNS	92	Standard query 0x8f17 A mobile.events.data.microsoft.com
842	96.067609	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x111d A docs.google.com
847	96.071707	139.19.106.154	139.19.66.1	DNS	75	Standard query 0x1004 A docs.google.com

```

> Frame 463: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{DAD9CF95-76D2-487B-B8E1
> Ethernet II, Src: Intel_e2:75:b1 (60:dd:8e:e2:75:b1), Dst: Cisco_96:a0:00 (00:23:05:96:a0:00)
> Internet Protocol Version 4, Src: 139.19.106.154, Dst: 139.19.66.1
> User Datagram Protocol, Src Port: 63084, Dst Port: 53
> Domain Name System (query)
    Transaction ID: 0x0003
    Flags: 0x0100 Standard query
    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 (28) (IP6 Address)
            Class: IN (0x0001)
            [Response In: 481]

```

می‌توان دید که همه‌ی این پیام‌ها از یک نوع هستند. بسته‌ای که مربوط به ریکوئستی که ما زدیم flag (sharif.edu) می‌شد را در تصویر بالا مشاهده می‌کنید. هدرهای آن را هم می‌توان دید. یک سری flag یا پرچم هم می‌توانند سمت شوند که به شرح زیراند:

```

> 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

```

فلگ response صفر شده است که به این منظور است که این یک ریکوئست است (کوئری).
 فلگ opcode هم صفر است که یک آپکد برای نوع کوئری است (اینجا کوئری استاندارد است).
 فلگ truncated هم صفر است شده است که منظورش این است که این پیام کوتاه بوده و نیازی نبود
 که شود و بنابراین یکپارچه است.

فلگ recursion desired در این جا برابر ۱ است شده است. این فلگ در واقع این که کوئری به صورت recursive یا iterative باشد را مشخص می‌کند. منظور هم این است که اگر dns server رکورد گفته شده را نداشت، خودش می‌رود و از یک dns server بعدی می‌پرسد و جواب آن را برمی‌گرداند (recursive) یا این که خروجی می‌دهد که آدرس را ندارد و باید از چه سروری خودمان بپرسیم .(iterative)

فلگ reserved در حقیقت کاربردی (فعلا) ندارد و برای استفاده‌های آینده گذاشته شده است. فلگ non authenticaded هم ۰ شده است که به این منظور است که دیتابی که non authenticaed نشده باشد قابل قبول نیست.

علاوه بر هدر فلگ‌ها، یک هدر query هم می‌بینیم که در حقیقت همان آدرس مورد کوئری است . یک تایپ AAAA هم دارد که مربوط به ip6 sharif.edu (). حال رسپانس را هم می‌آوریم:

No.	Time	Source	Destination	Protocol	Length	Info
35	1.425784	139.19.66.1	139.19.106.154	DNS	91	Standard query response 0x0820 A ssl.gstatic.com A 142.250.185
43	1.435287	139.19.66.1	139.19.106.154	DNS	91	Standard query response 0x77fe A ssl.gstatic.com A 142.250.185
46	1.448214	139.19.66.1	139.19.106.154	DNS	103	Standard query response 0x8d5f AAAA ssl.gstatic.com AAAA 2a09:2400:cc00::142.250.185
432	47.731667	139.19.66.1	139.19.106.154	DNS	277	Standard query response 0x0000 HTTPS www.bing.com CNAME www-www.bing.com
433	47.744637	139.19.66.1	139.19.106.154	DNS	343	Standard query response 0x1161 A www.bing.com CNAME www-www.bing.com
468	49.569326	139.19.66.1	139.19.106.154	DNS	123	Standard query response 0x0001 PTR 1.66.19.139.in-addr.arpa PTR www.bing.com
462	49.698819	139.19.66.1	139.19.106.154	DNS	86	Standard query response 0x0002 A sharif.edu A 152.89.13.54
468	49.859193	139.19.66.1	139.19.106.154	DNS	286	Standard query response 0xc5e4 HTTPS functional.events.data.microsoft.com
469	49.859193	139.19.66.1	139.19.106.154	DNS	229	Standard query response 0x37bd A functional.events.data.microsoft.com

Flags: 0x8100 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
 sharif.edu: type A, class IN
 Name: sharif.edu
 [Name Length: 10]
 [Label Count: 2]
 Type: A (1) (Host Address)
 Class: IN (0x0001)
 Answers
 sharif.edu: type A, class IN, addr 152.89.13.54
 [Request_Id: 461]
 [Time: 0.120018000 seconds]

در اینجا هم هدراها مشابه هستند. فلگ authoritative response این بار ۱ شده است. فلگ recursive required هست یا خیر. علاوه بر فلگ recursion available هم داریم که نشان می‌دهد سرور می‌تواند کوئری recursive بزند یا خیر (که این جا ۰ است). یک فلگ authenticated answer نشده است. یک reply code هم داریم که در این جا ۰ (به معنی no error است).

یک answers هم داریم که این اطلاعات مربوط به کوئری داخلش هستند:

```

▼ Answers
  ▼ sharif.edu: type A, class IN, addr 152.89.13.54
    Name: sharif.edu
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 4
    Address: 152.89.13.54
    [Request In: 461]
    [Time: 0.120018000 seconds]

```

البته می‌توان دید که در request , response هر یک پسته‌ی دیگر هم مربوط به هست که تنها فرق آن در type است.

