

بسمه تعالی



گزارش کار دوم آزمایشگاه شبکه

آشنایی با نرم افزار Wireshark

استاد:

دکتر بردیا صفایی

نویسندگان:

امیرمحمد صالح 99101824

امیررضا آذری 99101087

بزرگمهر ضیا 99100422

دانشگاه صنعتی شریف

تابستان 1403

فهرست

3	هدف
3	بخش اول
4	سوالات
9	بخش دوم
12	سوالات
14	بخش سوم
16	سوالات

هدف

هدف از انجام این آزمایش، آشنایی بیشتر با نرم‌افزار Wireshark است و همچنین تلاش شده است تا در کنار این امر، به بررسی تعدادی از پروتکل‌های لایه کاربرد پرداخته شود.

بخش اول

ابتدا نرم‌افزار Wireshark را باز می‌کنیم و سپس آن را در حالت **capture** قرار می‌دهیم. حال باید یک وب سایت که از پروتکل **http** استفاده می‌کند و همچنین دارای عکس نیز است را انتخاب کنیم که برای این کار سایت http://help.websiteos.com/websiteos/example_of_a_simple_html_page.htm را در نظر می‌گیریم. سپس آدرس **url** را در مرورگر خود وارد می‌کنیم و اجازه می‌دهیم تمامی اطلاعات لود شود سپس نرم‌افزار Wireshark را از حالت **Capture** خارج می‌کنیم. سپس با استفاده از امکاناتی که نرم‌افزار در اختیار ما قرار می‌دهد بسته مربوط به **http** را فیلتر می‌کنیم.

No.	Time	Source	Destination	Protocol	Length	Info
598	11.725483	100.127.255...	216.251.32.98	HTTP	530	GET /websiteos/example_of_a_simple_html_page.htm HTTP/1.1
601	11.964615	216.251.32.98	100.127.255...	HTTP	847	HTTP/1.1 200 OK (text/html)
603	11.998751	100.127.255...	216.251.32.98	HTTP	444	GET /websiteos/default_ns.css HTTP/1.1
619	12.000802	100.127.255...	216.251.32.98	HTTP	423	GET /websiteos/whmsg.js HTTP/1.1
621	12.000968	100.127.255...	216.251.32.98	HTTP	423	GET /websiteos/whver.js HTTP/1.1
623	12.001116	100.127.255...	216.251.32.98	HTTP	425	GET /websiteos/whproxy.js HTTP/1.1
626	12.001257	100.127.255...	216.251.32.98	HTTP	425	GET /websiteos/whutils.js HTTP/1.1
628	12.001355	100.127.255...	216.251.32.98	HTTP	425	GET /websiteos/whtopic.js HTTP/1.1
639	12.217060	216.251.32.98	100.127.255...	HTTP	840	HTTP/1.1 200 OK (text/css)
640	12.219023	100.127.255...	216.251.32.98	HTTP	488	GET /websiteos/htmlpage.jpg HTTP/1.1
646	12.237609	216.251.32.98	100.127.255...	HTTP	505	HTTP/1.1 200 OK (application/javascript)
647	12.240011	216.251.32.98	100.127.255...	HTTP	992	HTTP/1.1 200 OK (application/javascript)
648	12.240056	216.251.32.98	100.127.255...	HTTP	465	HTTP/1.1 200 OK (application/javascript)
653	12.242238	216.251.32.98	100.127.255...	HTTP	1237	HTTP/1.1 200 OK (application/javascript)
654	12.242280	216.251.32.98	100.127.255...	HTTP	827	HTTP/1.1 200 OK (application/javascript)
702	12.498429	216.251.32.98	100.127.255...	HTTP	437	HTTP/1.1 200 OK (JPEG JFIF image)
758	13.310085	100.127.255...	66.175.41.113	HTTP	957	GET /track/ctin.php?t=1720253453617&custnum=a57bcd0d5bb4bdac&sr
760	13.602007	66.175.41.113	100.127.255...	HTTP	664	HTTP/1.1 200 OK (GIF89a)
1616	30.542738	100.127.255...	23.204.21.189	HTTP	267	GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB94
1627	30.762667	23.204.21.189	100.127.255...	HTTP/XML	228	HTTP/1.1 200 OK

تصویر 1 بسته های **capture** شده توسط نرم‌افزار

No.	Time	Source	Destination	Protocol	Length	Info
598	11.725483	100.127.255...	216.251.32.98	HTTP	530	GET /websites/example_of_a_simple_html_page.htm HTTP/1.1
601	11.964615	216.251.32.98	100.127.255...	HTTP	847	HTTP/1.1 200 OK (text/html)
▶ Frame 598: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{9D307267-89D0-413C-9311-8EED30C1941D}, id 0 ▶ Ethernet II, Src: 00:ff:9d:30:72:67 (00:ff:9d:30:72:67), Dst: 00:ff:9e:30:72:67 (00:ff:9e:30:72:67) ▶ Internet Protocol Version 4, Src: 100.127.255.249, Dst: 216.251.32.98 ▶ Transmission Control Protocol, Src Port: 57731, Dst Port: 80, Seq: 1, Ack: 1, Len: 476 ▼ Hypertext Transfer Protocol ▶ GET /websites/example_of_a_simple_html_page.htm HTTP/1.1\r\n Host: help.websites.com\r\n Connection: keep-alive\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/126.0.0.0 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,application/signed-exchange;v=b3;q=0.7\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: en-US,en;q=0.9\r\n \r\n [Full request URI: http://help.websites.com/websites/example_of_a_simple_html_page.htm] [HTTP request 1/3] [Response in frame: 601] [Next request in frame: 603]						

تصویر 2 اطلاعات مرتبط به اولین بسته ارسالی

همانطور که در تصویر 2 مشاهده می‌کنید، نخستین درخواست از نوع GET است و اگر بسته مربوطه را باز کنیم مشاهده می‌کنیم که Host آن با url ای که در مرورگر وارد کردیم منطبق است.

سوالات

سوال اول:

برای این کار از بخش statistic گزینه protocol hierarchy را انتخاب می‌کنیم. همانطور که در تصویر 3 مشاهده می‌کنید:

- تمامی بسته‌ها در لایه لینک از پروتکل Ethernet استفاده کرده‌اند.
- همچنین 96.7 درصد از بسته‌ها در لایه network از پروتکل IPv4 استفاده کرده‌اند.
- در لایه transport نیز 91.3 درصد از پروتکل TCP و 5.4 درصد از پروتکل UDP استفاده کرده‌اند.
- در لایه application نیز 0.6 درصد از پروتکل http استفاده کرده‌اند.

Wireshark - Protocol Hierarchy Statistics - Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	4855	100.0	1720469	9818	0	0	0	4855
Ethernet	100.0	4855	4.0	67970	387	0	0	0	4855
Internet Protocol Version 4	96.7	4694	5.5	93880	535	0	0	0	4694
User Datagram Protocol	5.4	260	0.1	2080	11	0	0	0	260
Simple Service Discovery Protocol	2.3	114	1.4	23750	135	114	23750	135	114
QUIC IETF	0.7	34	2.6	44696	255	34	42296	241	36
Domain Name System	2.3	111	0.5	8607	49	111	8607	49	111
Data	0.0	1	0.0	51	0	1	51	0	1
Transmission Control Protocol	91.3	4432	85.8	1476111	8424	3328	932791	5323	4432
Transport Layer Security	19.6	953	62.4	1073924	6128	953	1000089	5707	961
Hypertext Transfer Protocol	0.6	27	4.2	72966	416	22	20449	116	27
Portable Network Graphics	0.0	1	0.4	7439	42	1	7439	42	1
Media Type	0.0	1	0.4	7335	41	1	7335	41	1
Line-based text data	0.0	1	0.7	11378	64	1	11378	64	1
JPEG File Interchange Format	0.0	1	1.3	21969	125	1	21969	125	1
Data	2.6	125	0.7	12436	70	125	12436	70	125
Internet Control Message Protocol	0.0	2	0.1	1112	6	2	1112	6	2
Address Resolution Protocol	3.3	161	0.3	4508	25	161	4508	25	161

تصویر 3 آمار مرتبط به بسته ها

سوال دوم:

No.	Time	Source	Destination	Protocol	Length	Info
598	11.725483	100.127.255...	216.251.32.98	HTTP		530 GET /websites/example_of_a_simple_html_page.htm HTTP/1.1
601	11.964615	216.251.32.98	100.127.255...	HTTP		847 HTTP/1.1 200 OK (text/html)

تصویر 4 ارسال درخواست GET و دریافت جواب آن

همانطور که در تصویر 4 مشاهده می کنید اطلاعات موجود در ستون دوم مرتبط به زمان ارسال و دریافت بسته ها است و اختلاف بین ارسال و دریافت جواب برای اولین بسته ها برابر است با 0.239132 ثانیه.

برای پیدا کردن absolute sequence number در اولین بسته TCP اینگونه عمل می کنیم که ابتدا فیلتر را روی TCP قرار می دهیم سپس در اطلاعات موجود برای اولین بسته، عبارت مقابل sequence number (raw) را مشاهده می کنیم. همانطور که در تصویر 5 مشاهده می کنید این عدد برابر با 3019439640 است.

سوال سوم:

595	11.724071	100.127.255...	216.251.32.98	TCP	66	57731 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
Frame 595: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{9D307267-89D0-413C-9311-8EED30C1941D}, id 0 Ethernet II, Src: 00:ff:9d:30:72:67 (00:ff:9d:30:72:67), Dst: 00:ff:9e:30:72:67 (00:ff:9e:30:72:67) Internet Protocol Version 4, Src: 100.127.255.249, Dst: 216.251.32.98 Transmission Control Protocol, Src Port: 57731, Dst Port: 80, Seq: 0, Len: 0 Source Port: 57731 Destination Port: 80 [Stream index: 9] [Conversation completeness: Complete, WITH_DATA (31)] [TCP Segment Len: 0] Sequence Number: 0 (relative sequence number) Sequence Number (raw): 3019439640 Next Sequence Number: 1 (relative sequence number) Acknowledgment Number: 0						

تصویر 5 اطلاعات مربوط به اولین بسته TCP

همه درخواست‌ها و پاسخ‌های DNS از پروتکل standard DNS استفاده می‌کنند. درخواست‌های DNS در دو نوع A و AAAA موجود هستند که A زمانی استفاده می‌شود که در حال استفاده از IPv4 باشیم و همچنین AAAA زمانی استفاده می‌شود که در حال استفاده از IPv6 باشیم. نکته دیگری که وجود دارد این است که درخواست و پاسخ، هر دو باید از یک نوع باشند. برای مثال نمی‌شود که درخواست از نوع A و پاسخ از نوع AAAA باشد. تفاوت بسته پاسخ با بسته پرسش در این است که در بسته پاسخ، بیت مربوط به پاسخ بودن این بسته 1 است که این مورد را می‌توان در تصویر 6 مشاهده کرد.

No.	Time	Source	Destination	Protocol	Length	Info
593	11.515107	100.127.255...	8.8.8.8	DNS	78	Standard query 0x3663 A help.websiteos.com
594	11.722430	8.8.8.8	100.127.255...	DNS	94	Standard query response 0x3663 A help.websiteos.com A 216.251.32.98
630	12.001993	100.127.255...	8.8.8.8	DNS	81	Standard query 0x7493 A count.carrierzone.com
631	12.200302	8.8.8.8	100.127.255...	DNS	97	Standard query response 0x7493 A count.carrierzone.com A 66.175.41.113
752	13.108519	100.127.255...	8.8.8.8	DNS	81	Standard query 0x4d8c A count.carrierzone.com
754	13.308953	8.8.8.8	100.127.255...	DNS	97	Standard query response 0x4d8c A count.carrierzone.com A 66.175.41.113
1607	30.318164	100.127.255...	8.8.8.8	DNS	94	Standard query 0x46fe A tile-service.weather.microsoft.com
1612	30.532592	8.8.8.8	100.127.255...	DNS	110	Standard query response 0x46fe A tile-service.weather.microsoft.com A 23.204.21
1955	33.226974	100.127.255...	8.8.8.8	DNS	78	Standard query 0xc9a3 A e2c38.gcp.gvt2.com
1956	33.432733	8.8.8.8	100.127.255...	DNS	94	Standard query response 0xc9a3 A e2c38.gcp.gvt2.com A 35.213.232.93
2017	35.399828	100.127.255...	8.8.8.8	DNS	78	Standard query 0xbd97 A e2c21.gcp.gvt2.com
2018	35.617597	8.8.8.8	100.127.255...	DNS	94	Standard query response 0xbd97 A e2c21.gcp.gvt2.com A 34.130.135.16


```

Frame 594: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{9D307267-89D0-413C-9311-8EED30C1941D}, id 0
Ethernet II, Src: 00:ff:9e:30:72:67 (00:ff:9e:30:72:67), Dst: 00:ff:9d:30:72:67 (00:ff:9d:30:72:67)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 100.127.255.249
User Datagram Protocol, Src Port: 53, Dst Port: 59905
Domain Name System (response)
  Transaction ID: 0x3663
  Flags: 0x8080 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
  ....0... .. = Recursion desired: Don't 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)
  
```

تصویر 6 فلگ‌هایی که در پاسخ DNS وجود دارد

نکته دیگری که باید در نظر گرفت این است که بسته‌ها پرسش صرفاً شامل درخواست هستند ولی می‌توان گفت که بسته‌های پاسخ کامل شده بسته‌ی درخواست است که در خود هم درخواست و پاسخ را دارد. برای درک بهتر می‌توان تصویر 8 را مشاهده کرد.

```

dns
No.    Time           Source            Destination      Protocol  Length  Info
-----
593  11.515107      100.127.255...  8.8.8.8         DNS       78      Standard query 0x3663 A help.websiteos.com

> Frame 593: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{9D307267-89D0-413C-9311-8EED30C1941D}, id 0
> Ethernet II, Src: 00:ff:9d:30:72:67 (00:ff:9d:30:72:67), Dst: 00:ff:9e:30:72:67 (00:ff:9e:30:72:67)
> Internet Protocol Version 4, Src: 100.127.255.249, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 59905, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x3663
  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
    > help.websiteos.com: type A, class IN
      Name: help.websiteos.com
      [Name Length: 18]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Response in: 594]

```

تصویر 7 بسته درخواست DNS

```

dns
No.    Time           Source            Destination      Protocol  Length  Info
-----
593  11.515107      100.127.255...  8.8.8.8         DNS       78      Standard query 0x3663 A help.websiteos.com
594  11.722430      8.8.8.8         100.127.255... DNS       94      Standard query response 0x3663 A help.websiteos.com A 216.251.32.98

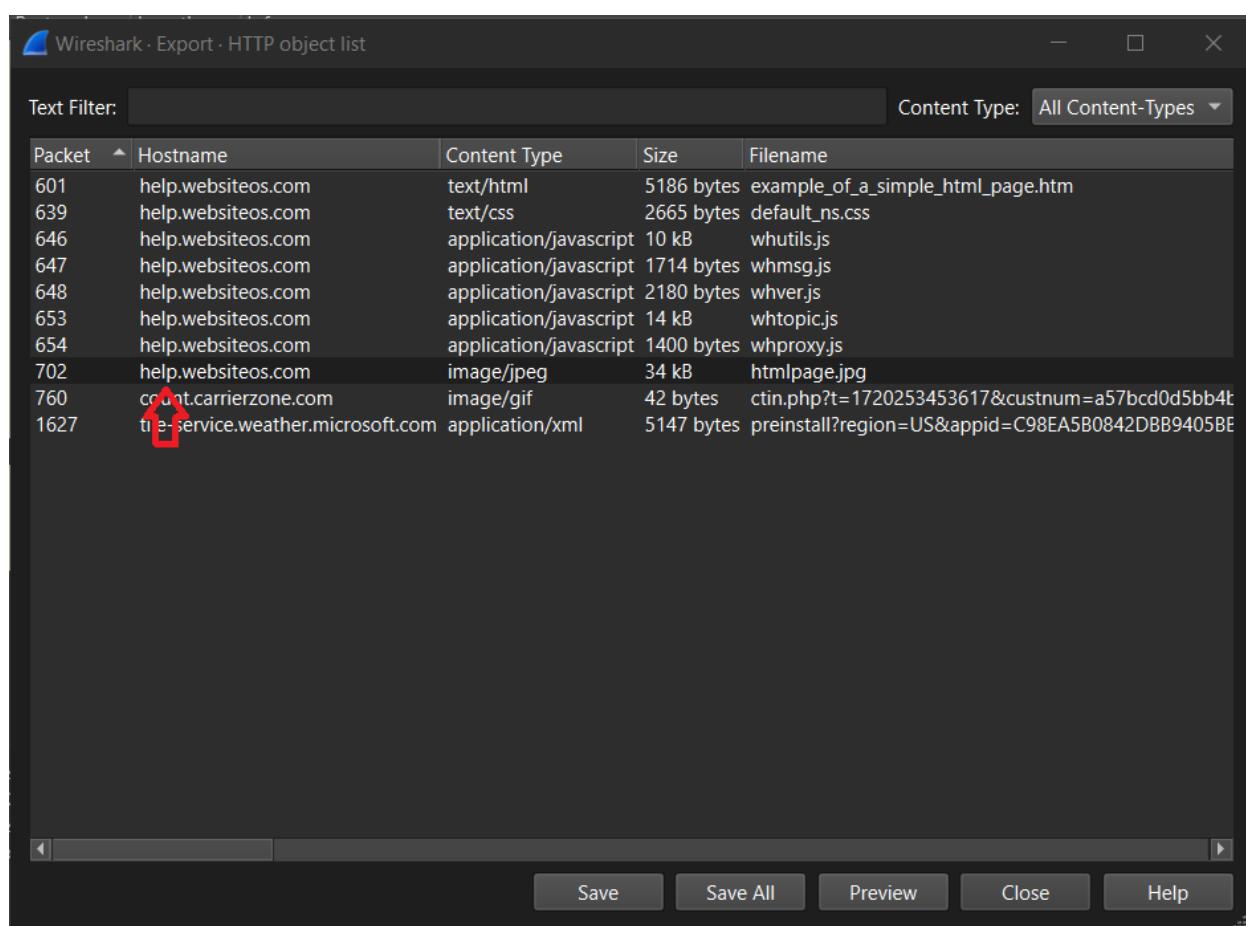
> Frame 594: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{9D307267-89D0-413C-9311-8EED30C1941D}, id 0
> Ethernet II, Src: 00:ff:9e:30:72:67 (00:ff:9e:30:72:67), Dst: 00:ff:9d:30:72:67 (00:ff:9d:30:72:67)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 100.127.255.249
> User Datagram Protocol, Src Port: 53, Dst Port: 59905
> Domain Name System (response)
  Transaction ID: 0x3663
  Flags: 0x8080 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
  .... ..0... .. = Recursion desired: Don't 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
    > help.websiteos.com: type A, class IN
      Name: help.websiteos.com
      [Name Length: 18]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  Answers
    > help.websiteos.com: type A, class IN, addr 216.251.32.98
      Name: help.websiteos.com
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 1 (1 second)
      Data length: 4
      Address: 216.251.32.98
      [Request in: 593]
      [Time: 0.207323000 seconds]

```

تصویر 8 بسته پاسخ DNS

سوال چهارم:

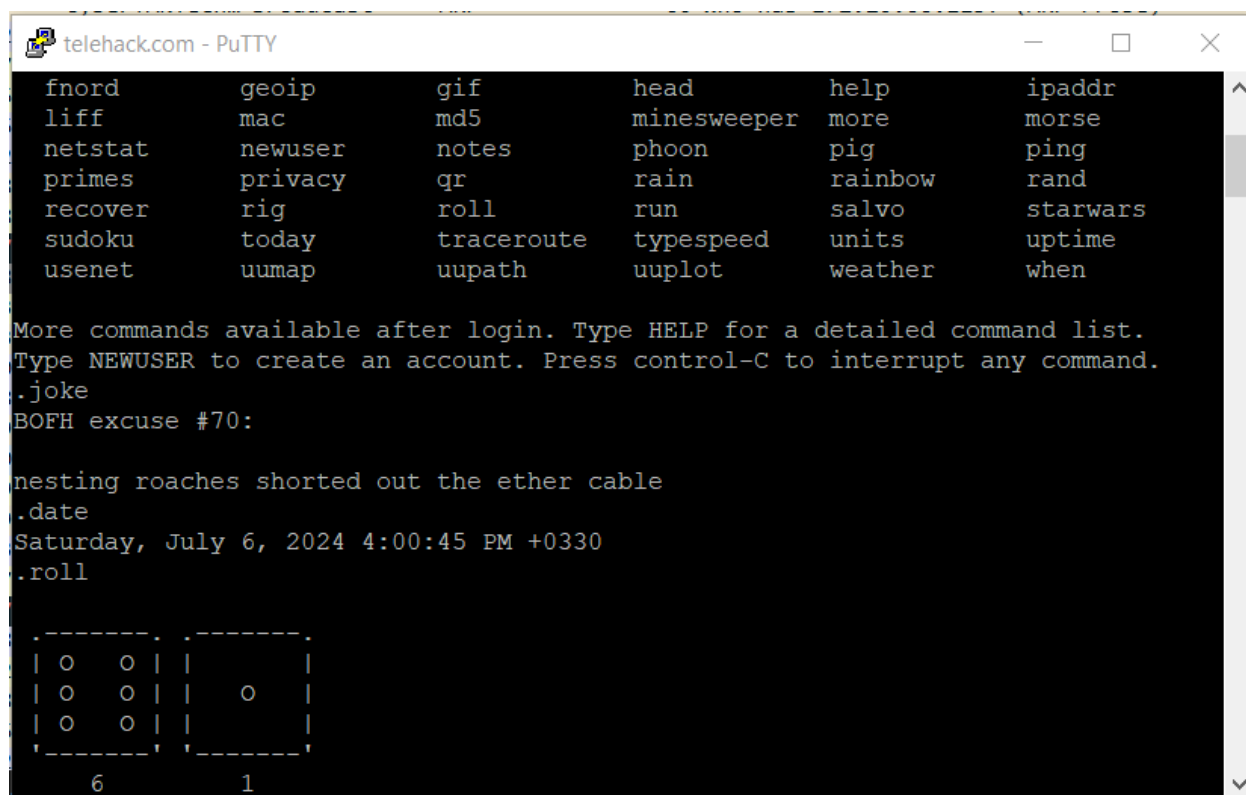
برای این کار به قسمت Http -> Export Object -> File می‌رویم سپس مطابق تصویر فایل مورد نظر را انتخاب می‌کنیم و گزینه save را می‌زنیم.



تصویر 9 انتخاب object مورد نظر

بخش دوم

ابتدا Wireshark را در حالت capture قرار می‌دهیم. سپس برای متصل به telehack.com از putty استفاده می‌کنیم. سپس چندین دستور از قبیل roll , date , joke را انتخاب می‌کنیم و آنها را اجرا می‌کنیم. سپس Wireshark را از حالت capture خارج می‌کنیم. سپس برای مشاهده بسته‌های مربوطه از فیلتر telnet استفاده می‌کنیم.



```
telehack.com - PuTTY
fnord    geoip    gif      head     help     ipaddr
liff     mac      md5      minesweeper more     morse
netstat  newuser  notes    phoon    pig      ping
primes   privacy  qr       rain     rainbow  rand
recover  rig      roll     run      salvo    starwars
sudoku   today    traceroute typespeed units     uptime
usetnet  uumap    uupath   uuplot   weather  when

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.
.joke
BOFH excuse #70:

nesting roaches shorted out the ether cable
.date
Saturday, July 6, 2024 4:00:45 PM +0330
.roll

  .-.-.-.  .-.-.-.
  |  o  o  |  |      |
  |  o  o  |  |      |
  |  o  o  |  |      |
  .-.-.-.  .-.-.-.
      6      1
```

تصویر 10 استفاده از دستورات joke , date , roll

همان‌گونه که در تصویر 11 مشخص است می‌توان دریافت که ip ما 172.20.66.190 است و ip مختص به telehack.com برابر با 64.13.139.230 است. همچنین اولین پیامی که از طرف سرور به برای ما ارسال شده است را می‌توانیم در تصویر 12 مشاهده کنیم که در آن انواع commandهایی که می‌توانیم استفاده کنیم را معرفی کرده است. همچنین می‌توان دید که طول این بسته نسبت به بسته‌های دیگر کمی بیش‌تر است.

telnet						
No.	Time	Source	Destination	Protocol	Length	Info
180	13.817863	172.20.66.190	64.13.139.230	TELNET	75	Telnet Data ...
192	14.076320	64.13.139.230	172.20.66.190	TELNET	57	Telnet Data ...
196	14.457718	64.13.139.230	172.20.66.190	TELNET	1235	Telnet Data ...
197	14.458723	172.20.66.190	64.13.139.230	TELNET	63	Telnet Data ...
198	14.458883	172.20.66.190	64.13.139.230	TELNET	57	Telnet Data ...
199	14.458961	172.20.66.190	64.13.139.230	TELNET	57	Telnet Data ...
200	14.459047	172.20.66.190	64.13.139.230	TELNET	57	Telnet Data ...

تصویر 11 بسته های رد و بدل شده بین سرور و دستگاه ما

```

Data: \r\n
Data: It is 5:30 am on Saturday, July 6, 2024 in Mountain View, California, USA.\r\n
Data: There are 92 local users. There are 26648 hosts on the network.\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      ?      ac      advent      basic      bf\r\n
Data: calc      ching    clear     clock       delta      diff\r\n
Data: dir        echo     factor   figlet      file       finger\r\n
Data: fnord      geoip    gif       head        help       ipaddr\r\n
Data: liff       mac      md5       minesweeper more       morse\r\n
Data: netstat    newuser  notes     phoon       pig        ping\r\n
Data: primes     privacy  qr        rain        rainbow    rand\r\n
Data: recover    rig      roll      run         salvo      starwars\r\n
Data: sudoku     today    traceroute typespeed   units      uptime\r\n
Data: usenet     uumap    uupath    uuplot      weather    when\r\n
Data: \r\n
Data: More commands available after login. Type HELP for a detailed command list.\r\n
Data: Type NEWUSER to create an account. Press control-C to interrupt any command.\r\n
Data: .

```

تصویر 12 بسته ارسالی از سوی سرور که حاوی دستورات قابل اجرا توسط سرور است

یکی از قابلیت‌هایی که Wireshark در اختیار ما قرار می‌دهد tcp stream است که با استفاده از این قابلیت می‌توانیم استریمی از پیام های رد و بدل شده را مشاهده کنیم. برای این کار روی یکی از بسته‌های Telnet کلیک راست می‌کنیم سپس Follow -> TCP stream را انتخاب می‌کنیم. این استریم را می‌توانید در تصویر مشاهده کنید.

Wireshark · Follow TCP Stream (tcp.stream eq 13) · Wi-Fi

```

.....'.....$..'...
Connected to TELEHACK port 130
.....'.....
It is 5:30 am on Saturday, July 6, 2024 in Mountain View, California, USA.
There are 92 local users. There are 26648 hosts on the network.

May the command line live forever.

Command, one of the following:
2048      ?      ac      advent      basic      bf
calc      ching   clear    clock      delta      diff
dir       echo     factor   figlet     file       finger
fnord     geoip    gif      head       help       ipaddr
liff      mac      md5      minesweeper more       morse
netstat   newuser  notes    phoon      pig        ping
primes    privacy  qr       rain       rainbow    rand
recover   rig      roll     run        salvo      starwars
sudo      today    traceroute typespeed  units      uptime
usenet    uumap    uupath   uuplot     weather    when

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.
.....P.....$..'...XTERM.....$.....$...tt...[Kjojokeke

BOFH excuse #70:

nesting roaches shorted out the ether cable
.ddaatete

Saturday, July 6, 2024 4:00:45 PM +0330
.riri..o.[Kollll

.[?251.[H.[2]
| 0 0 | |
| 0 0 | | 0
| 0 0 | |
|-----|
| 6 1 |
|-----|
.[H.[2]
|-----|

28 client pkts, 41 server pkts, 31 turns.
Entire conversation (5655 bytes) Show data as ASCII Stream 13
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

```

TCP stream 13 تصوير

نکته‌ای که در استریم تصویر 13 وجود دارد این است که اطلاعاتی که سرور برای ما ارسال می‌کند با رنگ آبی مشخص شده است و اطلاعاتی که از طرف ما برای سرور ارسال شده است با رنگ قرمز مشخص شده است.

حال با نگاه دقیق‌تر به یکی از بسته‌ها که در تصویر مشخص شده است درمی‌یابیم اطلاعاتی که از سمت ما برای سرور ارسال شده است به صورت کاراکتر به کاراکتر است.

```

> Frame 222: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{1AFEFFFF-147A-498D-8B80-33E42EAA3212}, id 0
> Ethernet II, Src: Cisco_c7:05:40 (00:c1:64:c7:05:40), Dst: Intel_99:ce:bf (8c:55:4a:99:ce:bf)
> Internet Protocol Version 4, Src: 64.13.139.230, Dst: 172.20.66.190
> Transmission Control Protocol, Src Port: 23, Dst Port: 55507, Seq: 1193, Ack: 67, Len: 1
telnet
Data: t

```

تصویر 14 یکی از بسته های ارسالی از طرف ما برای سرور که نشان میدهد اطلاعات به صورت کاراکتر به کاراکتر به سرور انتقال پیدا میکند

همچنین نکته دیگری که در مورد telnet می‌توان گفت این است که این پروتکل بسته‌ها را رمزنگاری نمی‌کند و آن را به صورت ساده ارسال می‌کند ولی در پروتکل ssh اطلاعات به صورت رمزنگاری شده انتقال پیدا می‌کنند.

سوالات

سوال اول

همانطور که در تصویر 15 مشاهده می‌کنید با توجه به دو بسته اول که بین Client و server به عنوان handshake جابه جا شده است می‌توان دریافت که بسته اول از client ارسال شده است زیرا صرفاً دارای syn است و بسته دوم از طرف server ارسال شده است زیرا دارای syn ack است. حال با توجه به موارد بالا می‌توان دریافت که:

Server ip : 192.168.0.1

Client ip :192.168.0.2

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 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	0.004150	192.168.0.2	192.168.0.1	TELNET	83	Telnet Data

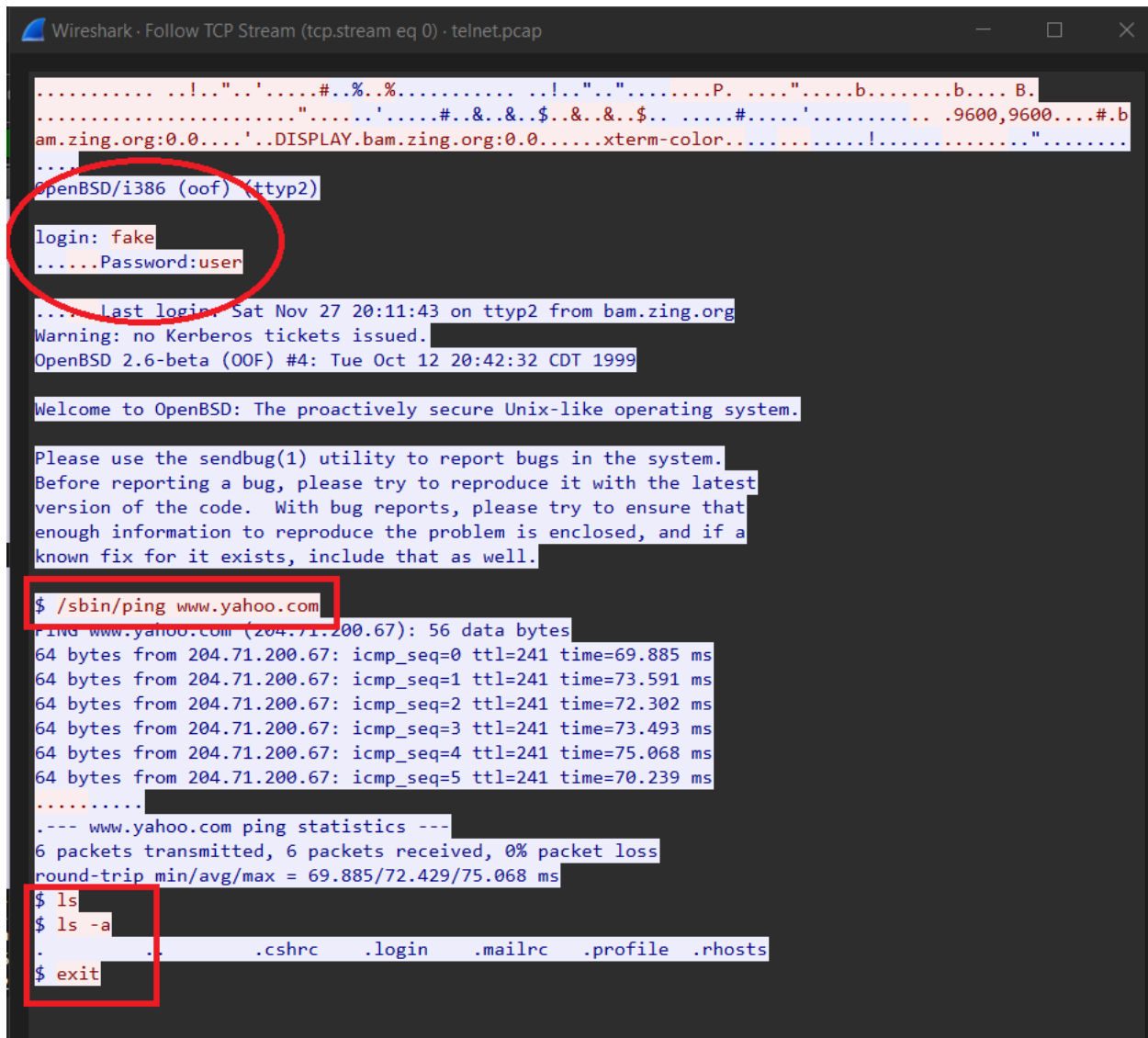
تصویر 15 handshake بین server و client

سوال دوم

برای جواب دادن به این سوال از tcp stream استفاده می‌کنیم. همانطور که در تصویر 16 مشاهده می‌کنید:

Username : fake

Password : user



```
.....!.."'.#.%..%.....!.."'.P.....".....b.....b....B.
.....'.....#..&..&..$..&..$..#.....'.....'.....9600,9600....#.b
am.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 ttyp2 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
```

تصویر 16 tcp stream

سوال سوم:

همانطور که قبل تر هم به آن اشاره کردم، مواردی که در tcp stream با رنگ قرمز مشخص شده اند ، مواردی هستند که کاربر آن ها را وارد کرده است. پس با توجه به این موضوع می توان گفت مواردی که در تصویر 16 با مستطیل مشخص شده اند، دستوراتی هستند که از طرف کاربر اجرا شده اند.

```
/sbin/ping www.yahoo.com
```

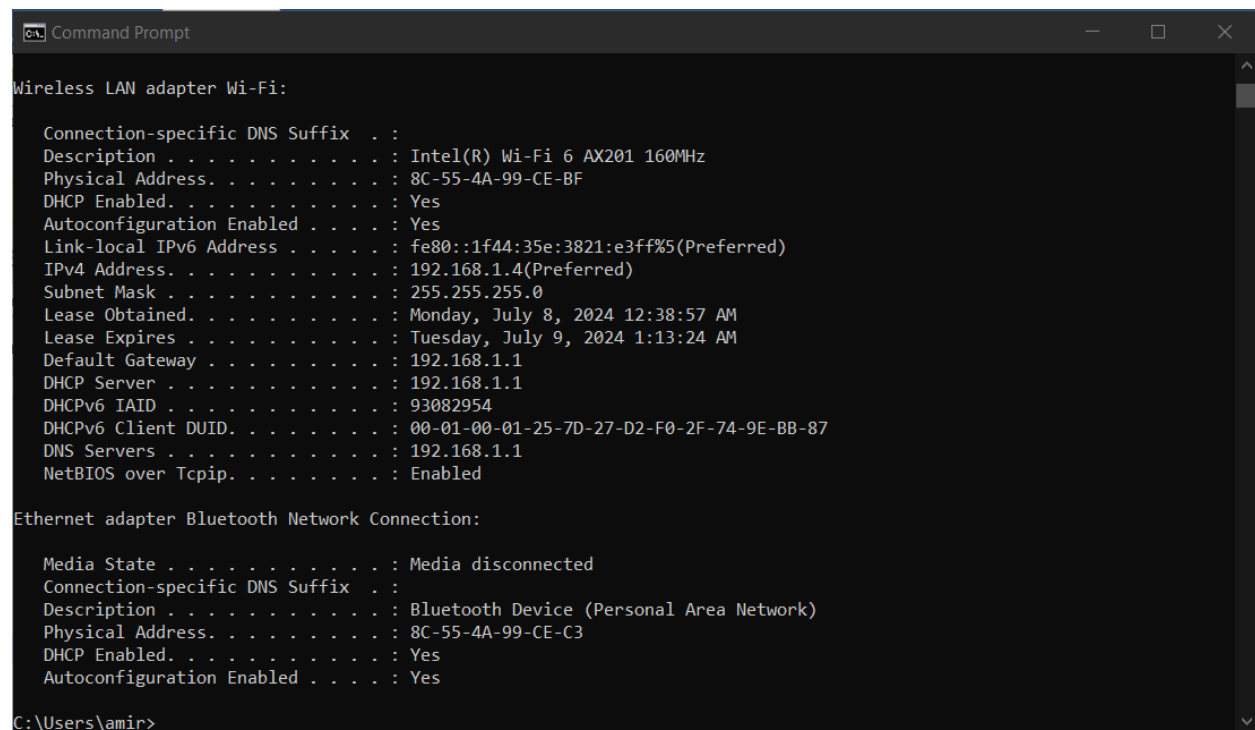
```
ls
```

```
ls -a
```

```
exit
```

بخش سوم

ابتدا با استفاده از دستور `ipconfig /all` تمامی interface های موجود را بررسی می کنیم.



```
Command Prompt

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . . : 
    Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
    Physical Address. . . . . : 8C-55-4A-99-CE-BF
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::1f44:35e:3821:e3ff%5(Preferred)
    IPv4 Address. . . . . : 192.168.1.4(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Monday, July 8, 2024 12:38:57 AM
    Lease Expires . . . . . : Tuesday, July 9, 2024 1:13:24 AM
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 93082954
    DHCPv6 Client DUID. . . . . : 00-01-00-01-25-7D-27-D2-F0-2F-74-9E-BB-87
    DNS Servers . . . . . : 192.168.1.1
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address. . . . . : 8C-55-4A-99-CE-C3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

C:\Users\amir>
```

تصویر 17 interface های موجود در سیستم

حال با استفاده از دستور ipconfig /flushdns می‌توانیم dns cache خود را خالی کنیم.

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\amir>
```

تصویر 18 خالی کردن dns cache

حال سعی می‌کنیم تا به کمک دستور nslookup sharif.edu دامنه sharif.edu را تبدیل به ip آدرس بکنیم.

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

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

C:\Users\amir>
```

تصویر 19 استفاده از nslookup

سپس به کمک فیلتر dns && ip.addr == 192.168.1.4 بسته‌های dns که از سیستم ما ارسال و یا دریافت شده است را فیلتر می‌کنیم. باید توجه داشت که آدرس 192.168.1.4 همان آدرسی است که در تصویر 17 می‌توان مشاهده کرد و متعلق به سیستم ما در زیر شبکه خانگی است. تصویر 20 بسته‌های فیلتر شده را نشان می‌دهد.

ip.addr == 192.168.1.4 && dns						
No.	Time	Source	Destination	Protocol	Length	Info
61	17.130592	192.168.1.4	192.168.1.1	DNS	89	Standard query 0x18b4 A d3sdlzpx54za7n.cloudfront.net
62	17.149464	192.168.1.1	192.168.1.4	DNS	153	Standard query response 0x18b4 A d3sdlzpx54za7n.cloudfront.net A 13.33.158.144 A 13.33.158.225 A 13.33.158.95 A 13.33.158.178
115	38.456399	192.168.1.4	192.168.1.1	DNS	89	Standard query 0x1c37 A d3s0v810qvkt1m.cloudfront.net
116	38.472477	192.168.1.1	192.168.1.4	DNS	153	Standard query response 0x1c37 A d3s0v810qvkt1m.cloudfront.net A 18.172.111.147 A 18.172.111.225 A 18.172.111.17 A 18.172.111.157
142	42.034729	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
143	42.043834	192.168.1.1	192.168.1.4	DNS	153	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
144	42.047374	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0002 A sharif.edu
145	42.250842	192.168.1.1	192.168.1.4	DNS	86	Standard query response 0x0002 A sharif.edu A 152.89.13.54
146	42.253007	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0003 AAAA sharif.edu
147	42.448692	192.168.1.1	192.168.1.4	DNS	130	Standard query response 0x0003 AAAA sharif.edu SOA ns1.sharif.ir

تصویر 20 بسته های dns

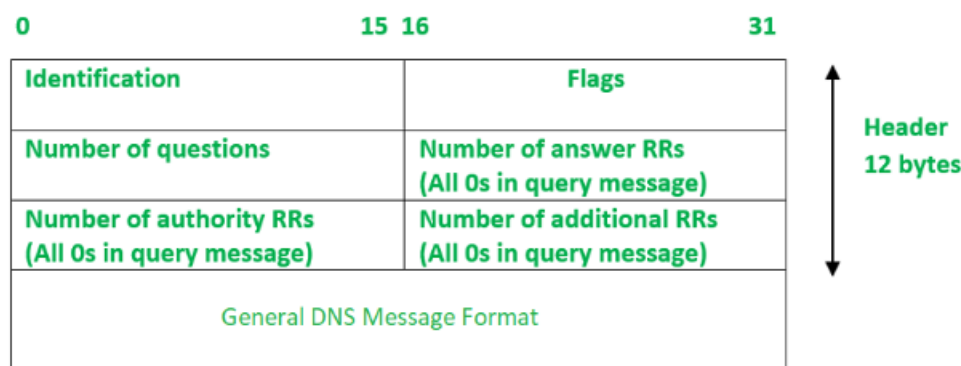
سوالات

سوال اول:

با توجه به آدرس‌های مقصد بسته‌های DNS، متوجه می‌شویم که این بسته‌ها به آدرس 192.168.1.1 ارسال شده‌اند و اگر آدرس default gateway که برای واسطه wifi در تصویر 17 مشخص شده است را در نظر بگیریم، متوجه می‌شویم که مودمی که به آن متصل هستیم دارای یک DNS server است که بسته‌های DNS برای آن ارسال می‌شود.

سوال دوم:

در روند پاسخ‌دهی به این سوال ابتدا به صورت کلی header یک DNS message را بررسی می‌کنیم سپس header یک بسته DNS request و پس از آن یک بسته DNS response را بررسی می‌کنیم.



تصویر 21 header بسته های dns

با توجه به تصویر 21 هر یک از بخش‌های header توضیح داده شده است.

- Identification: این بخش از header از 16 بیت یا 2 byte تشکیل شده است که صرفاً یک شناسه است تا client بتواند جوابی که از سرور گرفته است را با درخواست خود تطبیق بدهد و متوجه شود که این پاسخ متعلق به کدام درخواست است. در طرف سرور هم این 2 byte به صورت مستقیم از header درخواست، در header پاسخ کپی می‌شود.

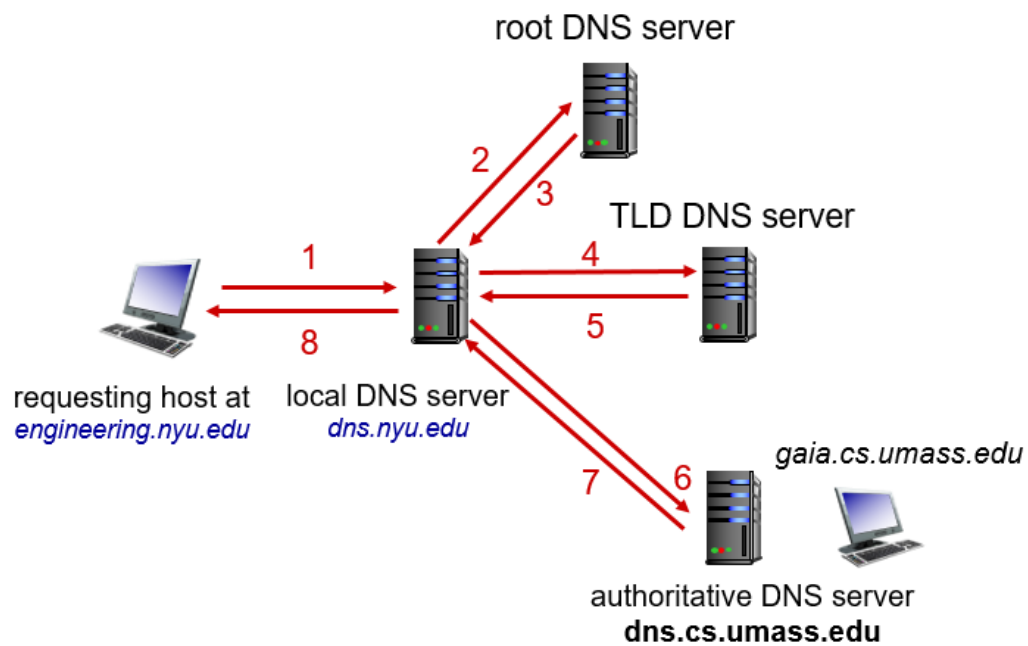
- Flags: این بخش هم از 16 بیت تشکیل شده است که هر کدام از بخش‌های آن را توضیح می‌دهم.

QR	Opcode	AA	TC	RD	RA	zero	rCode
1	4	1	1	1	1	3	4

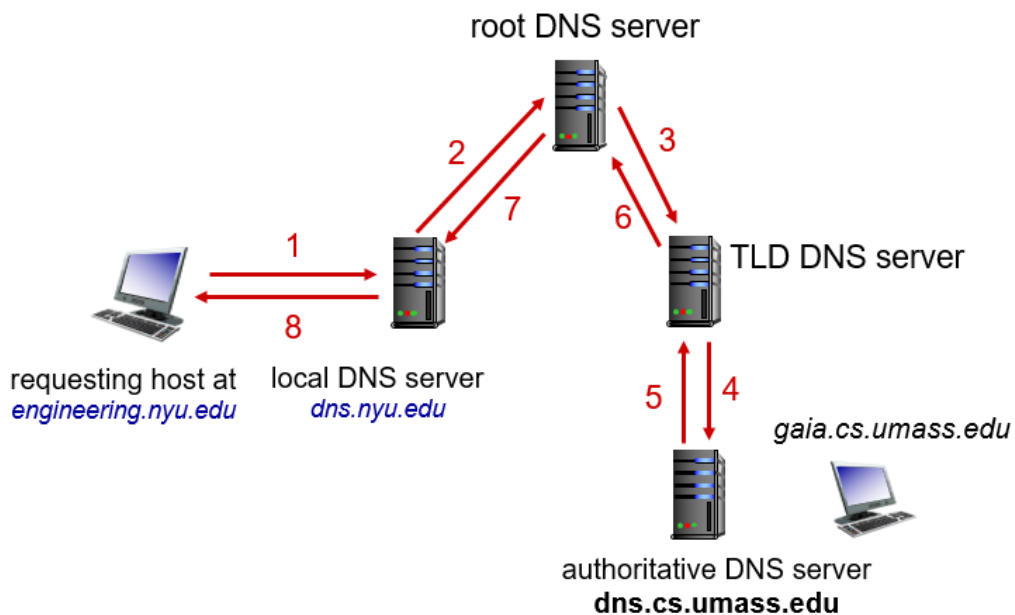
تصویر 22 بخش‌های مختلف flags

- QR: این بخش از یک بیت تشکیل شده است که نوع بسته را مشخص می‌کند در واقع اگر 0 باشد به این معنی است که بسته از نوع request است و اگر 1 باشد به این معنی است که بسته از نوع response است.
- Opcode: این 4 بیت مشخص می‌کنند که نوع کوئری که در message استفاده شده است، چیست. برای مثال اگر مقدار آن برابر با 0 باشد به این معنی است که کوئری از نوع standard query است.
- AA (Authoritative Answer): این بخش از یک بیت تشکیل شده است که مشخص می‌کند که سروری که پاسخ را برای ما ارسال کرده است یک Authoritative Server است یا نه. مقدار 1 برای بودن و 0 برای نبودن مقداردهی می‌شود.
- TC (Truncated): زمانی که از پروتکل UDP در لایه transport استفاده می‌کنیم، باعث می‌شود که برای message که در لایه کاربرد قرار می‌گیرد، محدودیت حجم داشته باشیم که این محدودیت 512 byte است. حال زمانی که این بیت در بسته‌های DNS برابر با یک است به این معنی است که طول پیام از 512 byte بیش‌تر بوده است که باعث می‌شود پیام قرار گرفته کوتاه شده باشد. به همین منظور می‌توان فهمید که بسته DNS کامل نیست.
- RD (Recursion Desired): زمانی که ما از DNS server برای پیدا کردن یک آدرس IP در خواست می‌کنیم، اگر جواب را در Cache داشته باشد جواب را برای ما برمی‌گرداند. در غیر این صورت برای پیدا کردن جواب دو راه حل وجود دارد، یا باید به صورت iterated و یا به صورت recursive باید عمل کند. همانطور که در تصویر 23 مشاهده می‌کنید، اگر به صورت iterated عمل کند، ابتدا از root DNS server درخواست می‌کند، سپس از TLD DNS server درخواست می‌کند و در نهایت به authoritative DNS server درخواست ارسال می‌کند. سپس پاسخ دریافت کرده را برای client ارسال می‌کند و لی همانطور که در تصویر 24 مشاهده می‌کنید اگر به صورت Recursive عمل کند باعث می‌شود، که ابتدا درخواست را برای root DNS server ارسال کند. سپس root DNS server این درخواست را برای TLD مربوطه ارسال می‌کند و TLD نیز درخواست را برای authoritative DNS server

ارسال می‌کند و سپس جواب از این مسیر باز می‌گردد و در نهایت به دست Client می‌رسد.



تصویر 24 استفاده از راهبرد *iterated*



تصویر 23 استفاده از راهبرد *recursive*

- RA (Recursion Available) : این بیت در بسته‌های پاسخ نشان می‌دهد که سرور قابلیت انجام کوئری‌های recursive را دارد یا خیر.
- Z (reserved bit) : یک بیت رزرو قرار دارد که مقدار آن همواره برابر با صفر است.
- DA (Data Authenticated) : این بیت در بسته‌های پاسخ نشان می‌دهد که اطلاعات ارسال شده از طرف سرور صحت‌سنجی شده است یا خیر و در صورت صحت‌سنجی، این بیت برابر با یک در نظر گرفته می‌شود.
- CD (Checking Disabled) : این بیت در بسته‌های درخواست مشخص می‌کند که آیا Client از server این درخواست را دارد تا داده‌ها را صحت‌سنجی کند. اگر این بیت 1 باشد نشان می‌دهد که این درخواست را ندارد و اگر این بیت 0 باشد نشان می‌دهد که این درخواست را دارد.
- RC (Response Code) : این بخش چهار بیت به خود اختصاص می‌دهد و مشخص می‌کند که آیا درخواست با موفقیت پاسخ داده شده است یا خیر.
- Number of questions : این بخش 16 بیتی است و تعداد پرسش‌هایی که در بدنه پیام آمده است را مشخص می‌کند.
- Answer RRs : این بخش نیز 16 بیت دارد که نشان‌دهنده تعداد پاسخ‌هایی است که در بخش پاسخ، در یک DNS message آمده است که این 16 بیت همگی، در بسته‌های پرسش (query)، 0 هستند.
- Authority RRs : این بخش نیز 16 بیت دارد که تعداد record هایی را نشان می‌دهد که در بخش Authority در بدنه پیام وجود دارد. البته باید ذکر کرد که این 16 بیت همگی در بسته‌های پرسش برابر با 0 هستند.
- Additional RRs : این بخش نیز 16 بیت دارد که تعداد record هایی را نشان می‌دهد که حاوی اطلاعات اضافی هستند و در بدنه پیام وجود دارند.

حال یک بسته حاوی query را تحلیل می‌کنیم.

```
▶ Frame 15: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on inte
▶ Ethernet II, Src: Intel_99:ce:bf (8c:55:4a:99:ce:bf), Dst: DLinkInterna_78:
▶ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
▶ User Datagram Protocol, Src Port: 50752, 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: 16]
```

تصویر 25 بسته حاوی query

- همانطور که مشاهده می‌کنید شناسه پیام برابر است با 0x0002.
- این message، از نوع query است زیرا بیت Response آن برابر با 0 است.
- Opcode نیز برابر با صفر است که نشان می‌دهد، پیام از نوع standard query است.
- بیت truncated برابر با صفر است که نشان می‌دهد پیام کوتاه نشده است.
- بیت RD برابر با 1 است که نشان می‌دهد عملیات باید به صورت recursive انجام شود.
- بیت checking disabled نیز برابر با 0 است که نشان می‌دهد اطلاعات حتما باید در سرور صحت‌سنجی بشوند.
- تعداد پرسش‌ها نیز برابر با 1 است.
- تعداد answer record ها برابر با صفر است.

- تعداد authoritative server record ها نیز برابر با صفر است.

- همچنین هیچ record اضافه‌ای وجود ندارد.

حال یک بسته حاوی response را بررسی می‌کنیم.

```
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 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
    Name: sharif.edu
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 40 (40 seconds)
    Data length: 4
    Address: 152.89.13.54
[Request In: 15]
[Time: 0.007437000 seconds]
```

تصویر 26 بسته حاوی response

- همانطور که مشاهده می‌کنید شناسه پیام برابر است با 0x0002.
- این message، از نوع response است زیرا بیت Response آن برابر با 1 است.
- Opcode نیز برابر با صفر است که نشان می‌دهد، پیام از نوع standard query است.
- بیت AA برابر با صفر است که مشخص می‌کند که این بسته از طرف authoritative server مرتبط با دامنه درخواست شده برای ما ارسال نشده است.
- بیت truncated برابر با صفر است که نشان می‌دهد پیام کوتاه نشده است.
- بیت RD برابر با 1 است که نشان می‌دهد عملیات به صورت recursive انجام شده است.
- بیت RA نیز برابر با 1 است که نشان می‌دهد سرور قابلیت انجام درخواست‌ها به صورت recursive را دارد.
- بیت DA برابر با صفر است که نشان می‌دهد داده‌هایی که در پاسخ آمده‌اند صحت‌سنجی نشده‌اند.

- بیت checking disabled نیز برابر با 0 است که نشان می‌دهد اطلاعات حتما باید در سرور صحت‌سنجی بشوند.
- تعداد پرسش‌ها نیز برابر با 1 است.
- تعداد answer record ها برابر با 1 است.
- تعداد authoritative server record ها نیز برابر با صفر است.
- همچنین هیچ record اضافه‌ای وجود ندارد.