به نام خدا

گزارش کار آزمایش شماره 4

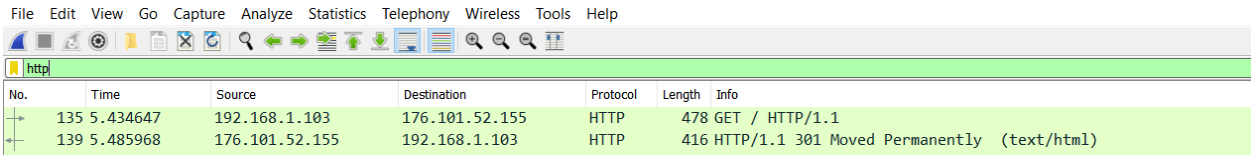
حدیث غفوری (9825413)

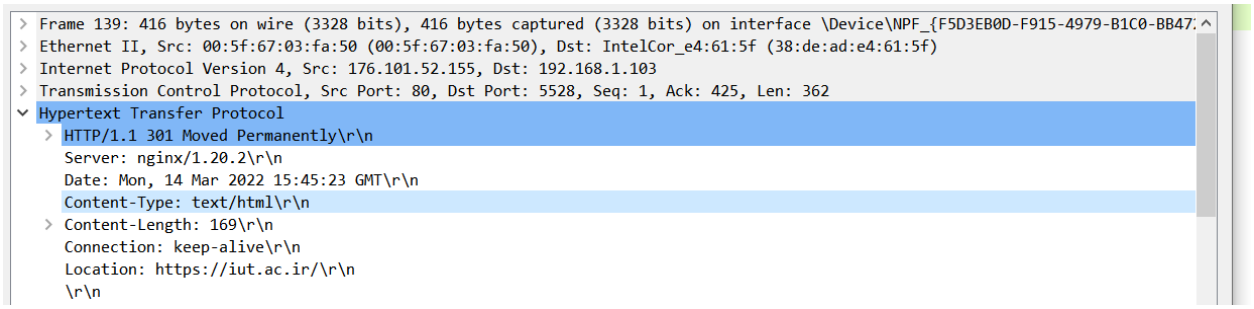
1.1.1

UDP,TCP,DNS,HTTP,TLSv1.2, TLSv1.3,SSDP,ARP

1.1.2

زمان بین http get تا http ok مدت 5.434647-5.485968=0.051321ثانیه طول کشیده است





اولین درخواست خروجی هنگام باز کردن سایت iut.ac.ir بعلت اینکه باید اسم سایت را به ادرس ip تبدیل کند پروتکل DNS را اجرا میکند و به همین علت اولین درخواست به ادرس DNS SERVER محلی میرود یعنی از مقصد سیستم من با ادرس (192.168.1.103) به مقصد dns server محلی با ادرس 192.168.1.1 میرود.

ادرس dns server محلی با دستور ipconfig/all در کامند بصورت زیر است که همان ادرس بالاست

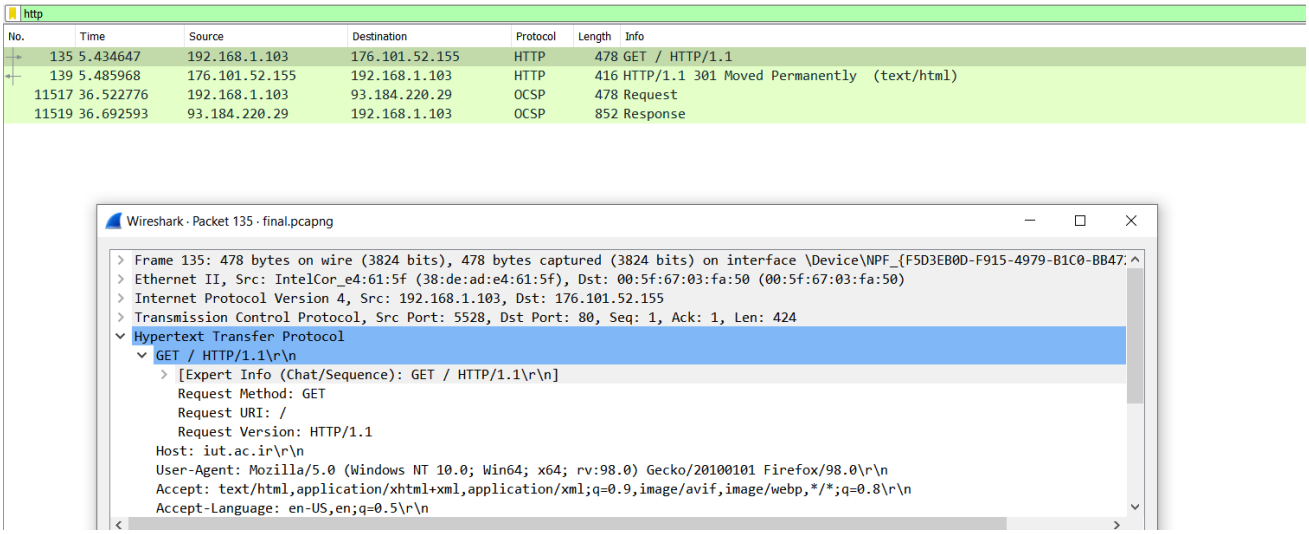
Source	Destination	Protocol	Length	Info
192.168.1.103	192.168.1.1	DNS	86	Standard query 0xb932 A cloudsearch.googleapis.com
192.168.1.1	192.168.1.103	DNS	102	Standard query response 0xb932 A cloudsearch.google
192.168.1.103	192.168.1.1	DNS	86	Standard query 0x98ff A encrypted-tbn0.gstatic.com
192.168.1.103	192.168.1.1	DNS	85	Standard query 0x33cf A lh5.googleusercontent.com
192.168.1.1	192.168.1.103	DNS	102	Standard query response 0x98ff A encrypted-tbn0.gst
192.168.1.1	192.168.1.103	DNS	130	Standard query response 0x33cf A lh5.googleusercont
192.168.1.103	192.168.1.1	DNS	74	Standard query 0x6472 A www.aparat.com
192.168.1.103	192.168.1.1	DNS	79	Standard query 0x22d7 A analytics.iut.ac.ir
192.168.1.1	192.168.1.103	DNS	138	Standard query response 0x6472 A www.aparat.com A 1
192.168.1.1	192.168.1.103	DNS	95	Standard query response 0x22d7 A analytics.iut.ac.i

```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz #2
   Physical Address. . . . . . . . . : 38-DE-AD-E4-61-5F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.103(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, March 13, 2022 4:23:51 PM
   Lease Expires . . . . . . . . . . : Tuesday, March 15, 2022 5:35:54 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Win 10>
```

آزمایش 2-1-1

Client:

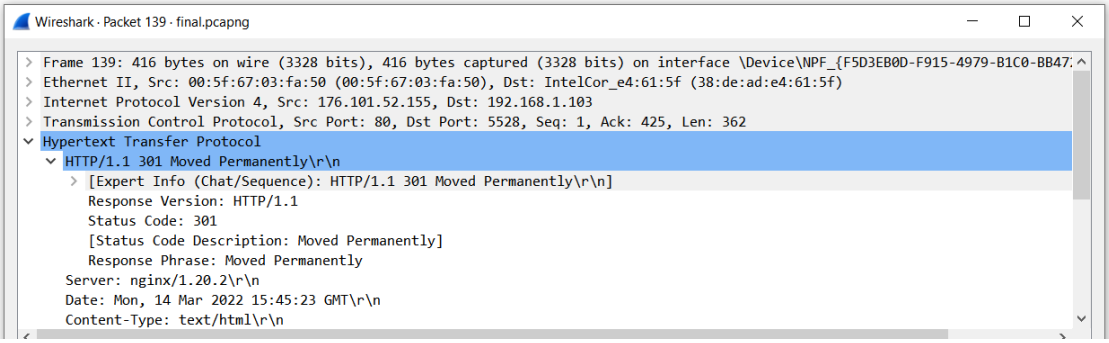
در اینجا مرورگر همان کلاینت است که درخواست http get را ارسال میکند بنابراین در بسته درخواست به دنبال ورژن http مرورگر میگردیم که ورژن 1.1 است



Server:

اما برای سرور باید در بسته response به دنبال ورژن ان بگردیم که ورژن 1.1 است

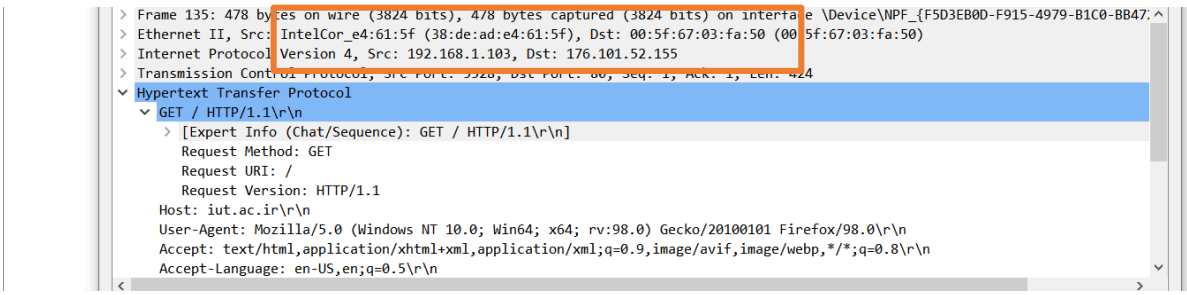
135	5.434647	192.168.1.103	176.101.52.155	HTTP	478 GET / HTTP/1.1
139	5.485968	176.101.52.155	192.168.1.103	HTTP	416 HTTP/1.1 301 Moved Permanently (text/html)
11517	36.522776	192.168.1.103	93.184.220.29	OCSP	478 Request
11519	36.692593	93.184.220.29	192.168.1.103	OCSP	852 Response



تفاوت http1.1,http1.0 : در ورژن 1.1 امکان برقراری ارتباط پایا وجود دارد به این معنی که میتوان در یک ارتباط http بیش از یک درخواست و پاسخ داشت اما در ورژن 1.0 به ازای هر درخواست و پاسخ باید یک ارتباط http جداگانه برقرار شود چون بعد از هر درخواست و پاسخ ان ارتباط بسته میشود و شروع ارتباط جدید با tcp بعلت هندشیک سه مرحله ای ان زمان زیادی را مصرف میکند بنابراین در ورژن 1.1 هم ارتباط پایا (باز ماندن ارتباط تا هنگامی که در ان ارتباط درخواست از سمت کلاینت هست) و هم پایپ لاین وجود دارد تا بتوان همزمان چندین درخواست و پاسخ داشت.

در ورژن 1.1 کد 100 continue وجود دارد و به کلاینت این اجازه را میدهد که بفهمد سرور میتواند درخواستش را پردازش کند یا خیر بنابراین کلاینت تنها هدر میفرستد و سرور با کد 100 continue به کلاینت میگوید که درخواستش را میتواند پردازش کند و بدنه ی پیام را ارسال کند

زبان هایی که مرورگر (کلاینت و بسته ی http get) میتواند قبول کند English امریکایی است (en-US)



در http get در قسمت detail ادرس src همان ادرس کامپیوتر ما یعنی 192.168.1.103 است و ادرس dst همان ادرس مقصد یا سرور (سایت iut.ac.ir) یعنی 176.101.52.155است

چون http یک انتقال امن ایجاد میکند از پروتکل tcp استفاده میکند که از تصویر زیر در لایه انتقال میتوان transmission control protocol را مشاهده کرد

```
> Frame 135: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface \Device\NPF_{F5D3EB
> Ethernet II, Src: IntelCor_e4:61:5f (38:de:ad:e4:61:5f), Dst: 00:5f:67:03:fa:50 (00:5f:67:03:fa:50)
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 176.101.52.155
v Transmission Control Protocol, Src Port: 5528, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
    Source Port: 5528
    Destination Port: 80
    [Stream index: 5]
    [TCP Segment Len: 424]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 2110056816
    [Next sequence number: 425    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 410088334
    0101 .... = Header Length: 20 bytes (5)
```

در http get شماره پورت مبدا، شماره پورت کامپیوتر من و شماره پورت مقصد، شماره پورت سرور است پس پورت مبدا5528 (هنگام برقراری ارتباط باید پورت ازاد استفاده شود پس از هزار شماره پورت بالاتر است) و پورت مقصد 80 است که پورت رزور شده است.

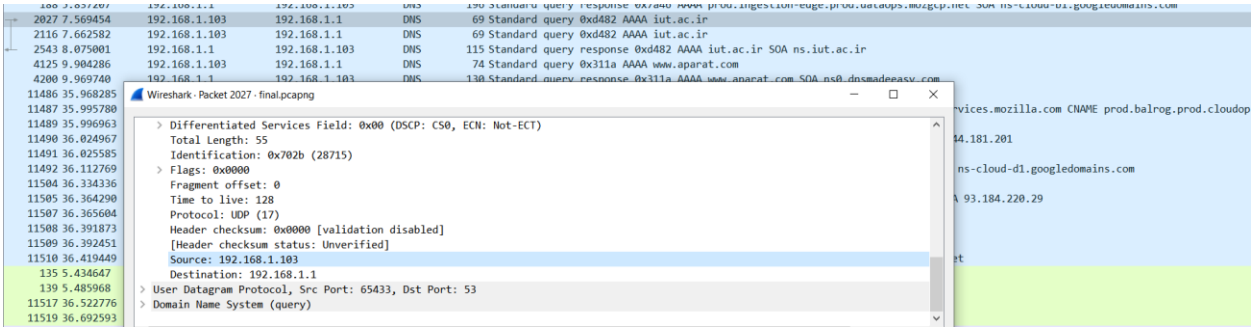
چون اطلاعاتی را میخواهد که از سرور به کامپیوتر من برگشته است باید در http response به دنبال اطلاعات بگردیم که در اینجا کد وضعیت 301 است که یعنی بصورت دائمی جابجا شده است

```
    TCP payload (362 bytes)
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
    Server: nginx/1.20.2\r\n
    Date: Mon, 14 Mar 2022 15:45:23 GMT\r\n
```

آزمایش 3-1

فرستنده dns queries کامپیوتر من با ادرس 192.168.1.103 است

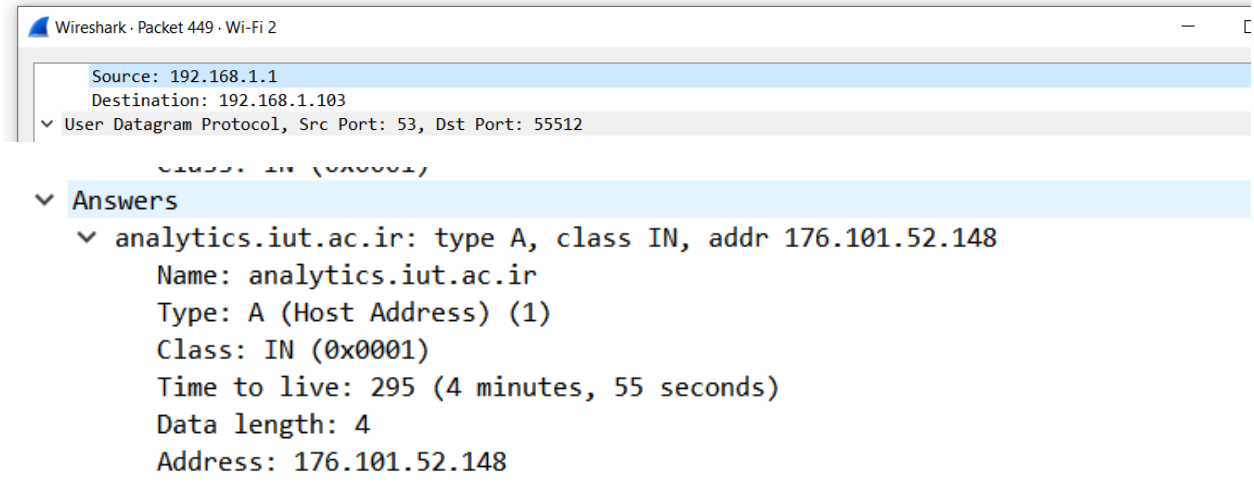
412	2.800384	192.168.1.103	192.168.1.1	DNS	79 Standard query 0x22d7 A analytics.iut.ac.ir
441	2.820514	192.168.1.1	192.168.1.103	DNS	138 Standard query response 0x6472 A www.aparat.com A 185.147.178.14 A 185.
449	2.829081	192.168.1.1	192.168.1.103	DNS	95 Standard query response 0x22d7 A analytics.iut.ac.ir A 176.101.52.148



ادرس پیام پاسخ:

176.101.52.148

192.168.1.103	192.168.1.1	DNS	79	Standard query 0x22d7 A analytics.iut.ac.ir
192.168.1.1	192.168.1.103	DNS	138	Standard query response 0x6472 A www.aparat.com A 185.
192.168.1.1	192.168.1.103	DNS	95	Standard query response 0x22d7 A analytics.iut.ac.ir A 176.101.52.148



چون dns احتیاج به پروتکل امنی ندارد پس از UDP استفاده میکند که طبق تصویر زیر همان user datagram protocol است

```
    [Header checksum status: Unverified]
    Source: 192.168.1.103
    Destination: 192.168.1.1
User Datagram Protocol, Src Port: 65433, Dst Port: 53
    Source Port: 65433
    Destination Port: 53
    Length: 35
```

```
    Source: 192.168.1.1
    Destination: 192.168.1.103
User Datagram Protocol, Src Port: 53, Dst Port: 65433
    Source Port: 53
    Destination Port: 65433
    Length: 81
```

مقصد پیام dns query همان dns server محلی است که پورت ان 53 است و مبدا پیام پاسخ dns query response هم همان dns server محلی است پس هر دو یکی هستند و پورت 53 دارند که رزور شده برای dns است

پیام dns query به dns server محلی میرود که بالاتر با دستور ipconfig/all دیدیم ادرس ان 192.168.1.1 است و هر دو یکسان هستند

412	2.800384	192.168.1.103	192.168.1.1	DNS	79 Standard query 0x22d7 A analytics.iut.ac.ir
441	2.820514	192.168.1.1	192.168.1.103	DNS	138 Standard query response 0x6472 A www.aparat.com A 185.147.178.14 A 185.
449	2.829081	192.168.1.1	192.168.1.103	DNS	95 Standard query response 0x22d7 A analytics.iut.ac.ir A 176.101.52.148

```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz #2
   Physical Address. . . . . . . . . : 38-DE-AD-E4-61-5F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.103(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, March 13, 2022 4:23:51 PM
   Lease Expires . . . . . . . . . . : Tuesday, March 15, 2022 5:35:54 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Win 10>
```

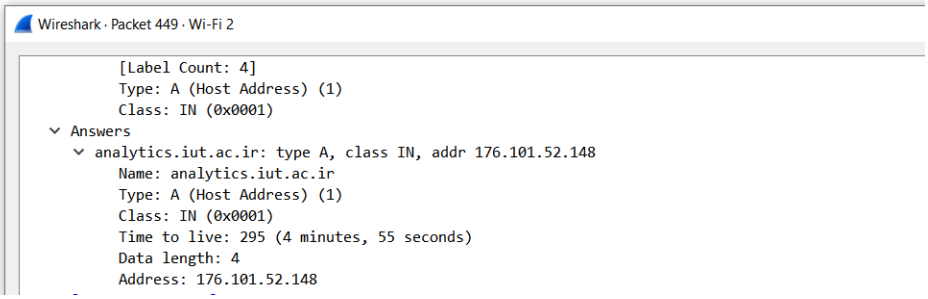
پیام dns query نوعش A که در این نوع اسم سایت مورد نظر را میگیرد و ادرس IP ان سایت را پیدا میکند و حاوی جواب نیست چون QUERY است

```
192.168.1.103   192.168.1.1     DNS    74 Standard query 0x6472 A www.aparat.com
192.168.1.103   192.168.1.1     DNS    79 Standard query 0x22d7 A analytics.iut.ac.ir
192.168.1.1     192.168.1.103   DNS   138 Standard query response 0x6472 A www.aparat.com A 185.147.178.14 A 185
192.168.1.1     192.168.1.103   DNS    95 Standard query response 0x22d7 A analytics.iut.ac.ir A 176.101.52.148
```

Dns response

سایت مورد نظر تنها دارای یک ادرس IP بود بنابراین یک عدد جواب داریم که محتوای ان ادرس IP سایت iut.ac.ir است

```
192.168.1.1     192.168.1.103   DNS    95 Standard query response 0x22d7 A analytics.iut.ac.ir A 176.101.52.148
```



بعد از دریافت ادرس ip سایت مورد نظر از پروتکلdns برای برقراری ارتباط http باید هندشیک سه مرحله ای tcp انجام شود که در قدم اول کامپیوتر من بسته ای که SYN ان یک باشد را به سرور سایت مورد نظر ارسال میکند پس مقصد این بسته iut.ac.ir است که در زیر میبینیم ادرس ان همان 176.101.52.148 بود که توسط پروتکل dns بدست امده بود

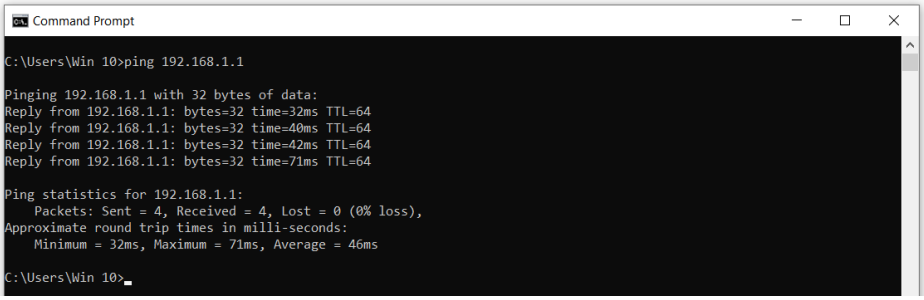
```
132 5.395151    192.168.1.103   176.101.52.155  TCP    66 5529 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
133 5.434334    176.101.52.155  192.168.1.103   TCP    66 80 → 5528 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1410 SACK_PERM=1 WS=128
134 5.434408    192.168.1.103   176.101.52.155  TCP    54 5528 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0

137 5.435791    192.168.1.103   176.101.52.155  TCP    54 5529 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
138 5.485313    176.101.52.155  192.168.1.103   TCP    54 80 → 5528 [ACK] Seq=1 Ack=425 Win=64128 Len=0
140 5.493738    192.168.1.103   176.101.52.155  TCP    66 5530 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
141 5.531947    192.168.1.103   176.101.52.155  TCP    54 5528 → 80 [ACK] Seq=425 Ack=363 Win=65792 Len=0
```

بله برای دریافت هر عکسی که در سایت iut.ac.ir موجود است و از سایت های دیگر لینک شده است برای مشاهده عکس ها باید ادرس ان سایت ها هم بدست ایند که پروتکل dns برای هر کدام از انها باید یک dns query ارسال کند تا ادرس ip هر کدام از سایتها را دریافت کند

آزمایش 3-1-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.103	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=640/32770, ttl=128 (reply in 2)
2	0.032710	192.168.1.1	192.168.1.103	ICMP	74	Echo (ping) reply id=0x0001, seq=640/32770, ttl=64 (request in 1)
3	1.013706	192.168.1.103	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=641/33026, ttl=128 (reply in 4)
4	1.053643	192.168.1.1	192.168.1.103	ICMP	74	Echo (ping) reply id=0x0001, seq=641/33026, ttl=64 (request in 3)
5	2.035904	192.168.1.103	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=642/33282, ttl=128 (reply in 6)
6	2.078021	192.168.1.1	192.168.1.103	ICMP	74	Echo (ping) reply id=0x0001, seq=642/33282, ttl=64 (request in 5)
7	3.046559	192.168.1.103	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=643/33538, ttl=128 (reply in 8)
8	3.118212	192.168.1.1	192.168.1.103	ICMP	74	Echo (ping) reply id=0x0001, seq=643/33538, ttl=64 (request in 7)
9	5.141316	00:5f:67:03:fa:50	IntelCor_e4:61:5f	ARP	42	Who has 192.168.1.103? Tell 192.168.1.1
10	5.141367	IntelCor_e4:61:5f	00:5f:67:03:fa:50	ARP	42	192.168.1.103 is at 38:de:ad:e4:61:5f
11	5.371548	192.168.1.103	20.54.232.160	TCP	54	5722 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
12	5.372503	192.168.1.103	20.54.232.160	TCP	66	5725 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	5.524225	20.54.232.160	192.168.1.103	TCP	54	443 → 5722 [FIN, ACK] Seq=1 Ack=2 Win=2048 Len=0



ادرس 192.168.1.1 را ping میکنیم و میدانیم ping با پروتکل ICMP کار میکند که با ارسال یک request منتظر پاسخ میشود که اگر reply دریافت شد یعنی هاست مورد نظر پاسخ داده است.