

## به نام خدا

(ابتدا قسمت هایی که در آ 3 با توجه به مشکل نرم افزارم، نتوانستم انجام بدهم را گزارش داده ام: )

عوض کردن IP (در فایل قبل به صورتی گرافیکی را انجام دادم) با استفاده از ترمینال:

```
[sudo] password for marzieh:
root@ubuntu:/home/marzieh# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.196.130 netmask 255.255.255.0 broadcast 192.168.196.255
    inet6 fe80::2cb:c94d:91b6:d721 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c6:49:9a txqueuelen 1000 (Ethernet)
    RX packets 2012 bytes 2242229 (2.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 941 bytes 93849 (93.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 312 bytes 27126 (27.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 312 bytes 27126 (27.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:/home/marzieh# ifconfig ens33 192.168.58.2
root@ubuntu:/home/marzieh# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.58.2 netmask 255.255.255.0 broadcast 192.168.58.255
    inet6 fe80::2cb:c94d:91b6:d721 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c6:49:9a txqueuelen 1000 (Ethernet)
    RX packets 2027 bytes 2243472 (2.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 959 bytes 96279 (96.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 318 bytes 27617 (27.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 318 bytes 27617 (27.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

دستور route و دیدن default gateway :

```
root@ubuntu:/home/marzieh# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 100 0 0 ens33
link-local 0.0.0.0 255.255.0.0 U 1000 0 0 ens33
192.168.196.0 0.0.0.0 255.255.255.0 U 100 0 0 ens33
root@ubuntu:/home/marzieh#
```

تغییر آدرس gateway :

```
root@ubuntu:/home/marzieh# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.196.2 0.0.0.0 UG 100 0 0 ens33
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 ens33
192.168.196.0 0.0.0.0 255.255.255.0 U 100 0 0 ens33
root@ubuntu:/home/marzieh# route add default gw 192.168.196.10
root@ubuntu:/home/marzieh# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.196.10 0.0.0.0 UG 0 0 0 ens33
0.0.0.0 192.168.196.2 0.0.0.0 UG 100 0 0 ens33
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 ens33
192.168.196.0 0.0.0.0 255.255.255.0 U 100 0 0 ens33
root@ubuntu:/home/marzieh# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 0 0 0 ens33
default _gateway 0.0.0.0 UG 100 0 0 ens33
link-local 0.0.0.0 255.255.0.0 U 1000 0 0 ens33
192.168.196.0 0.0.0.0 255.255.255.0 U 100 0 0 ens33
root@ubuntu:/home/marzieh#
```

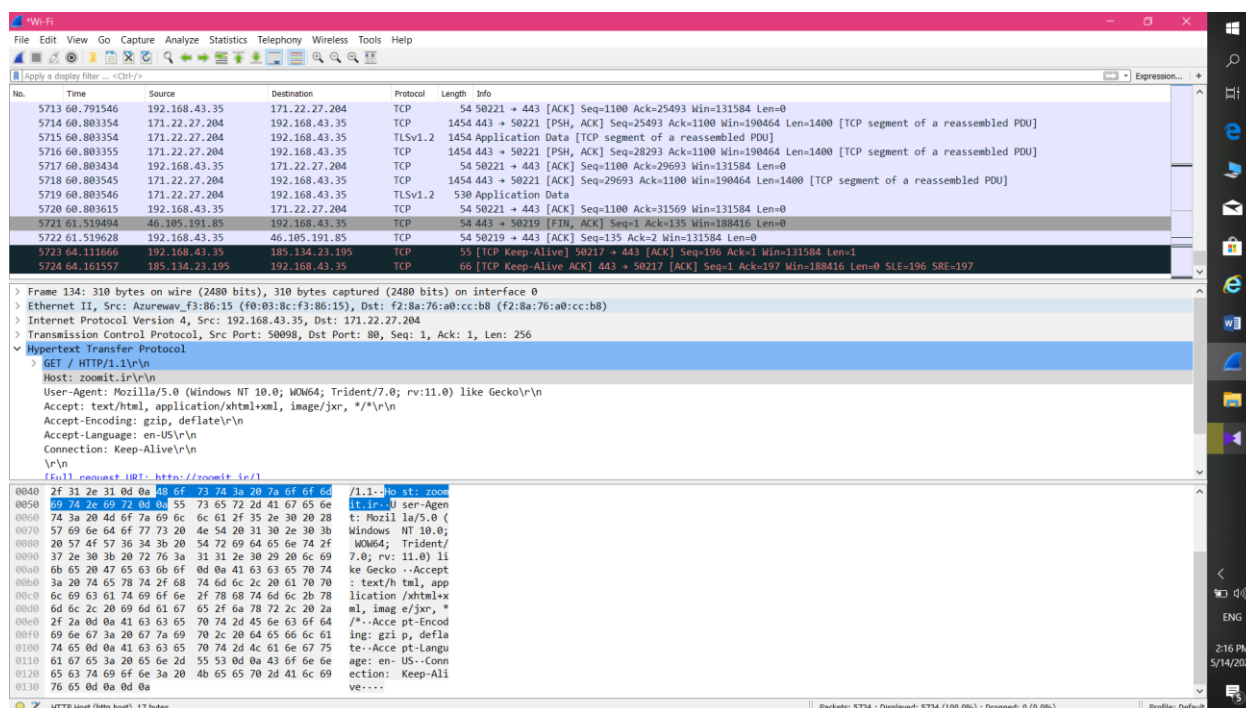
اطلاعات مسیریابی کش شده: (خالی بود)

```
root@ubuntu:/home/marzieh# route -Cn
Kernel IP routing table
Source          Destination    Gateway        Flags Metric Ref    Use Iface
root@ubuntu:/home/marzieh#
```

آز 4:

(تکلیف خواسته شده، در صفحه ی آخر قرار دارد)

در برنامه، capture را شروع کردم. و سایت zoomit.ir را در مرورگر وارد کردم. و تا لود شدن آن صبر کردم. و سپس capture را متوقف کردم. صفحه ی wireshark:



1. پروتکل های مشاهده شده:

TCP, TLS , DNS, HTTP, ARP

2.

## HTTP GET :

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane shows three packets: a SYN packet (No. 134), a SYN-ACK packet (No. 137), and an HTTP GET packet (No. 3601). The packet details pane for packet 3601 shows the following structure:

- Frame 134: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0
- Ethernet II, Src: Azurewav\_f3:86:15 (f0:03:8c:f3:86:15), Dst: f2:8a:76:a0:cc:b8 (f2:8a:76:a0:cc:b8)
- Internet Protocol Version 4, Src: 192.168.43.35, Dst: 171.22.27.204
- Transmission Control Protocol, Src Port: 50098, Dst Port: 80, Seq: 1, Ack: 1, Len: 256
- Hypertext Transfer Protocol
  - GET / HTTP/1.1\r\n
  - Host: zoomit.ir\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  - Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: en-US\r\n
  - Connection: Keep-Alive\r\n
  - \r\n
  - [Full request URI: http://zoomit.ir/]

The packet bytes pane shows the raw data of the request, including the GET method, host, user-agent, and other headers.

## HTTP RESPONSE:

The screenshot shows a Wireshark capture of an HTTP 301 Moved Permanently response. The packet list pane shows three packets: a SYN packet (No. 134), a SYN-ACK packet (No. 137), and an HTTP 301 response packet (No. 3601). The packet details pane for packet 3601 shows the following structure:

- Frame 137: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
- Ethernet II, Src: f2:8a:76:a0:cc:b8 (f2:8a:76:a0:cc:b8), Dst: Azurewav\_f3:86:15 (f0:03:8c:f3:86:15)
- Internet Protocol Version 4, Src: 171.22.27.204, Dst: 192.168.43.35
- Transmission Control Protocol, Src Port: 80, Dst Port: 50098, Seq: 1, Ack: 257, Len: 87
- Hypertext Transfer Protocol
  - HTTP/1.1 301 Moved Permanently\r\n
  - Content-length: 0\r\n
  - Location: https://www.zoomit.ir/\r\n
  - \r\n
  - [HTTP response 1/1]
  - [Time since request: 0.067535000 seconds]
  - [Request in frame: 134]
  - [Request URI: http://zoomit.ir/]

The packet bytes pane shows the raw data of the response, including the 301 status code, content-length, location, and other headers.

مدت زمان برای load سایت: 0.067535 ثانیه

3. ابتدا پروتکل dns اجرا می شود. و اولین درخواست، به مقصد dns server محلی فرستاده میشود. مقایسه IP مربوط به مقصد با IP مربوط به dns server محلی شبکه مان: (178.22.122.100)

The screenshot displays the Wireshark network traffic analysis tool. The main pane shows a list of captured packets, with the DNS protocol selected. The packet list shows several DNS queries and responses. The packet details pane shows the structure of a DNS query, including the question section with the domain name 'api.bing.com'. The packet bytes pane shows the raw data of the packet. A Windows Command Prompt window is open in the foreground, displaying the output of the 'ipconfig /all' command, which shows the network configuration for the wireless LAN adapter 'Wi-Fi'. The output includes the IP address '192.168.43.35', the subnet mask '255.255.255.0', and the default gateway '192.168.43.1'. The DNS servers listed are '178.22.122.100' and '185.51.200.2'.

No.	Time	Source	Destination	Protocol	Length	Info
9	2.232146	192.168.43.35	178.22.122.100	DNS	72	Standard query 0x3ccf A api.bing.com
10	2.279856	178.22.122.100	192.168.43.35	DNS	210	Standard query response 0x3ccf A api.bing.com CNAME uk.shcan.ir A 185.134.23.195 A 5.226.141.206 A 185.134.23.170 A ...
128	8.739659	192.168.43.35	178.22.122.100	DNS	69	Standard query 0x32dd A zoomit.ir
129	8.846231	192.168.43.35	185.51.200.2	DNS	69	Standard query 0x32dd A zoomit.ir
130	9.764075	185.51.200.2	192.168.43.35	DNS	85	Standard query response 0x32dd A zoomit.ir A 171.22.27.204
136	9.869928	178.22.122.100	192.168.43.35	DNS	85	Standard query response 0x32dd A zoomit.ir A 171.22.27.204
147	12.722961	192.168.43.35	178.22.122.100	DNS	82	Standard query 0x67c0 A iecvlist.microsoft.com
148	12.798762	178.22.122.100	192.168.43.35	DNS	164	Standard query response 0x67c0 A iecvlist.microsoft.com CNAME ie9comview.vo.msccnd.net CNAME cs9.wpc.v0cdn.net A 152...
585	22.743403	192.168.43.35	178.22.122.100	DNS	84	Standard query 0x458c A www.googletagmanager.com
598	22.800279	178.22.122.100	192.168.43.35	DNS	192	Standard query response 0x458c A www.googletagmanager.com CNAME bulk.shcan.ir A 176.9.122.183 A 176.9.122.176 A 176...
1147	24.489779	192.168.43.35	178.22.122.100	DNS	75	Standard query 0xbd13 A www.gstatic.com
1188	24.541320	178.22.122.100	192.168.43.35	DNS	91	Standard query response 0xbd13 A www.gstatic.com A 216.58.207.35

```
Frame 128: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
> Ethernet II, Src: Azureway, F3:86:15 (F8:03:8C:F3:86:15), Dst: f2:8a:76:a0:cc:b8 (f2:8a:76:a0:cc:b8)
> Internet Protocol Version 4, Src: 192.168.43.35, Dst: 178.22.122.100
> User Datagram Protocol, Src Port: 58197, Dst Port: 53
> Domain Name System (query)

0000 f2 8a 76 a0 cc b8 03 8c f3 86 15 00 00 45 00  --v...
0010 00 37 a1 32 00 00 80 11 81 3d c0 a8 2b 23 b2 16  -7-2...
0020 7a 64 e3 55 00 35 00 23 0d 31 32 dd 01 00 00 01  -zd-U...
0030 00 00 00 00 00 06 7a 6f 6f 6d 69 74 02 69 72  -.....
0040 00 00 01 00 01  -.....
```

```
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
Physical Address. . . . . : F0-03-8C-F3-86-15
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::192:c59:ddab:cbd4%13(Prefered)
IPv4 Address. . . . . : 192.168.43.35(Prefered)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, May 14, 2020 1:51:57 PM
Lease Expires . . . . . : Thursday, May 14, 2020 3:21:56 PM
Default Gateway . . . . . : 192.168.43.1
DHCP Server . . . . . : 192.168.43.1
DHCPv6 IAID . . . . . : 116392844
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-CC-4B-BC-10-7B-44-1F-CA-0C
DNS Servers . . . . . : 178.22.122.100
                        185.51.200.2
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

## ورژن مربوط به مرورگر: 1.1

Wireshark packet capture showing an HTTP GET request. The packet list shows three packets: a GET request (No. 134), a 301 Moved Permanently response (No. 137), and a GET request for a proxy file (No. 3601). The packet details pane shows the structure of the GET request, including the request line, headers, and body. The packet bytes pane shows the raw data of the request.

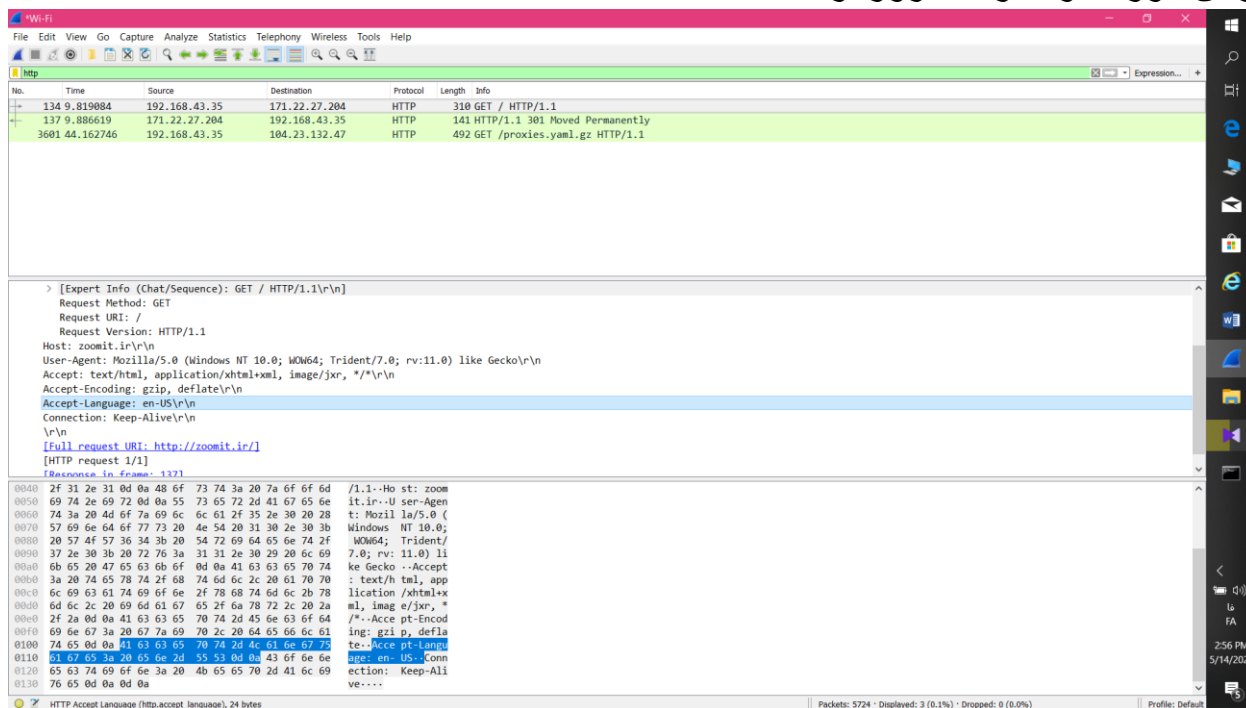
Frame 134: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0  
 Ethernet II, Src: Azurewav\_f3:86:15 (f0:03:8c:f3:86:15), Dst: f2:8a:76:a0:cc:b8 (f2:8a:76:a0:cc:b8)  
 Internet Protocol Version 4, Src: 192.168.43.35, Dst: 171.22.27.204  
 Transmission Control Protocol, Src Port: 50098, Dst Port: 80, Seq: 1, Ack: 1, Len: 256  
 Hypertext Transfer Protocol  
 GET / HTTP/1.1  
 [Expert Info (Chat/Sequence): GET / HTTP/1.1  
 Request Method: GET  
 Request URI: /  
 Request Version: HTTP/1.1  
 Host: zoomit.ir  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko  
 Accept: text/html,application/xhtml+xml,image/jxr,\*/\*  
 Accept-Encoding: gzip, deflate

## ورژن برای سرور: 1.1

Wireshark packet capture showing an HTTP 301 Moved Permanently response. The packet list shows three packets: a GET request (No. 134), a 301 Moved Permanently response (No. 137), and a GET request for a proxy file (No. 3601). The packet details pane shows the structure of the 301 response, including the status line, headers, and body. The packet bytes pane shows the raw data of the response.

Frame 137: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0  
 Ethernet II, Src: f2:8a:76:a0:cc:b8 (f2:8a:76:a0:cc:b8), Dst: Azurewav\_f3:86:15 (f0:03:8c:f3:86:15)  
 Internet Protocol Version 4, Src: 192.168.43.35, Dst: 134.9.819084  
 Transmission Control Protocol, Src Port: 80, Dst Port: 50098, Seq: 1, Ack: 257, Len: 87  
 Hypertext Transfer Protocol  
 HTTP/1.1 301 Moved Permanently  
 [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently  
 Response Version: HTTP/1.1  
 Status Code: 301  
 [Status Code Description: Moved Permanently]  
 Response Phrase: Moved Permanently  
 Content-length: 0  
 Location: https://www.zoomit.ir/

## 2. زبان مورد قبول برای مرورگر: en-US



## 3. آدرس IP کامپیوتر من: 192.168.43.35 آدرس IP سرور (سایت): 171.22.27.204

## 4.

Transmission Control Protocol, Src Port: 50098, Dst Port: 80, Seq: 1, Ack: 1, Len: 256

از TCP استفاده میکند.

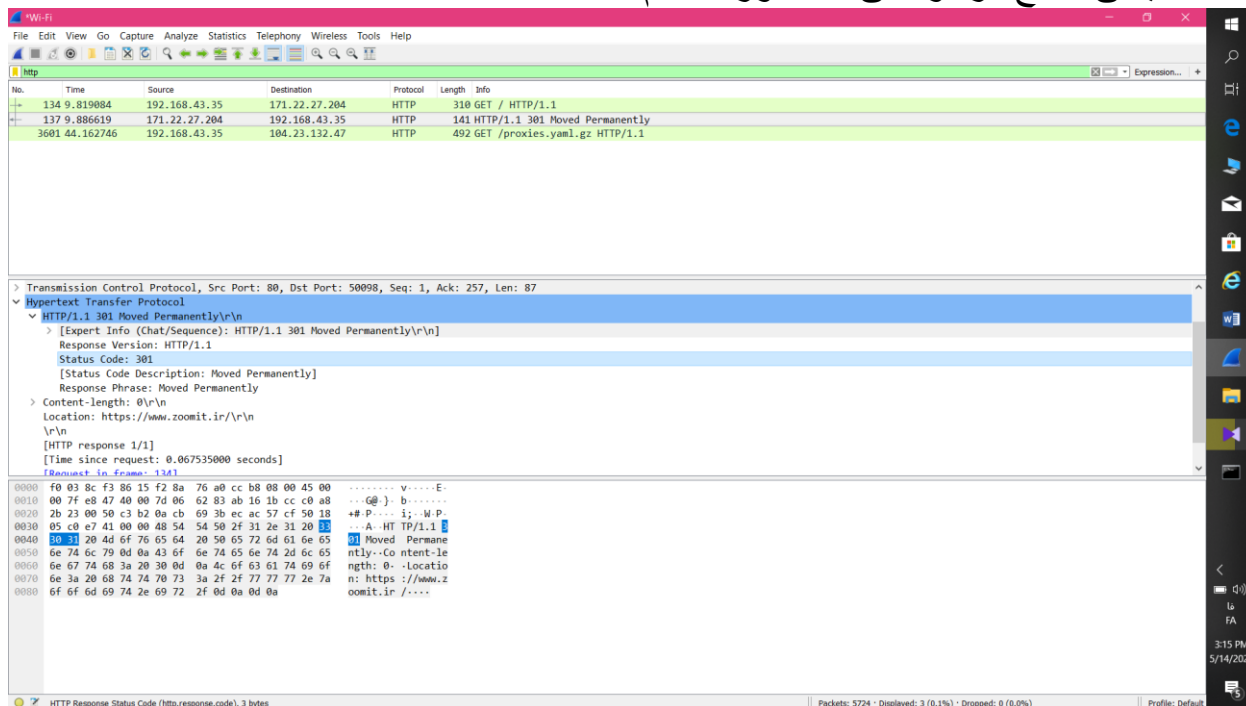
## 5. در مورد HTTP GET :

Transmission Control Protocol, Src Port: 50098, Dst Port: 80, Seq: 1, Ack: 1, Len: 256

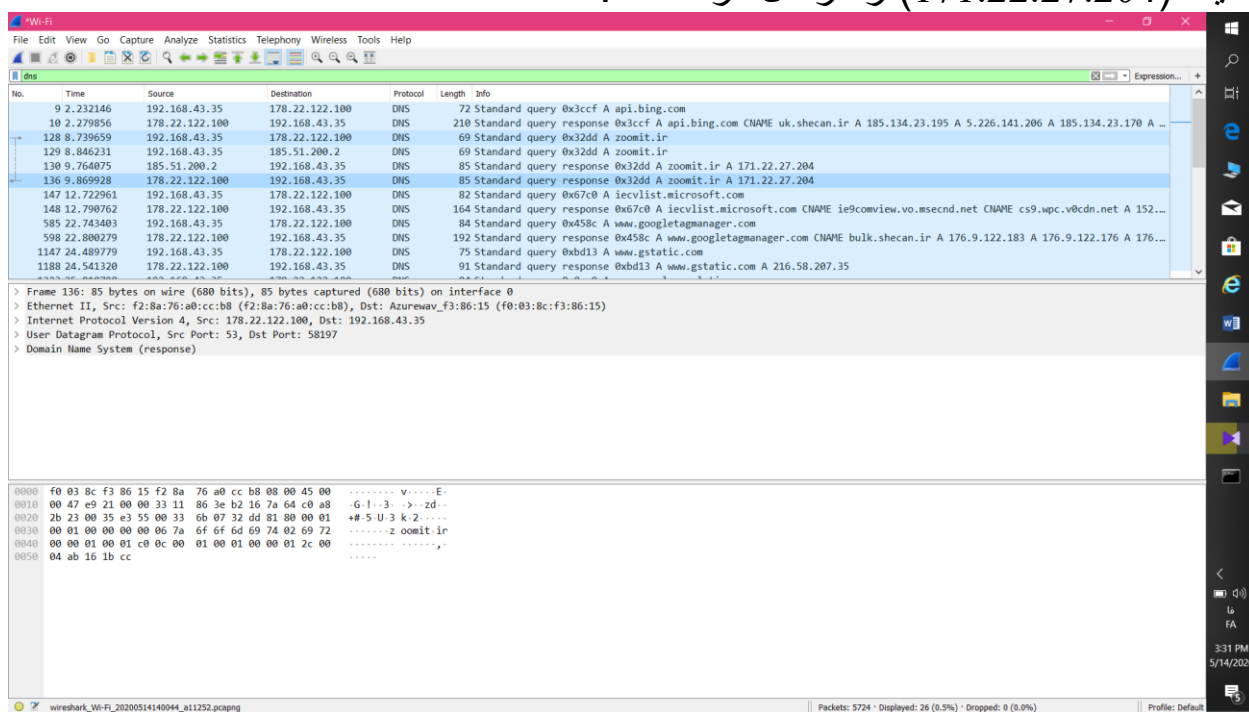
پس پورت مبدا: 50098 و پورت مقصد: 80 است.



## 6. کد وضعیت=301 [Status Code Description: Moved Permanently] یعنی: منبع درخواستی به صورت دائم منتقل شده است.



## 1. در dns query آدرس فرستنده 192.168.43.35 است. در dns response آدرس فرستنده که dns server محلی است، 178.22.122.100 است که آدرس سایت (171.22.27.204) را ارسال کرده است.





و از UDP استفاده میکنند:

User Datagram Protocol, Src Port: 58197, Dst Port: 53

2. در dns query : Destination Port: 53  
و در dns response : Source Port: 53  
که برای هردو برابر 53 است که مربوط به dns است.

3. به مقصد dns server محلی فرستاده میشود: 178.22.122.100

The image shows a Wireshark packet capture of a DNS query. The packet list shows a query for 'api.bing.com' from source 192.168.43.35 to destination 178.22.122.100. The packet details show the query structure. A Windows Command Prompt window is overlaid, displaying the output of the 'ipconfig /all' command for the 'Wi-Fi' adapter, showing the IP address 192.168.43.35 and the DNS server 178.22.122.100.

4. zoomit.ir: type A, class IN  
نوع A است. جواب ندارد.

5. یک جواب دارد: zoomit.ir: type A, class IN, addr 171.22.27.204  
با محتوای IP سایت

## 6. در TCP SYN رساله سده توسط ميزبان:

The image shows a Wireshark capture of a network packet. The packet list pane shows a packet of type TCP from source 192.168.43.35 to destination 171.22.27.204. The packet details pane shows the TCP header with Seq=0, Win=0, and the SYN flag set. The packet bytes pane shows the raw TCP segment.

اينجا IP مقصد برابر IP كامپيوتر من (192.168.43.35) است، كه در dns Response هم، مقصد بود.

7. بله سايتي كه من باز كردم شامل چند تصوير بود كه براي لود كردن آنها چند درخواست dns براي سايت هاي مختلف زده شد:

The image shows a Wireshark capture of network traffic. The packet list pane shows several DNS packets. The packet details pane shows the DNS header and the query name. The packet bytes pane shows the raw DNS segment.

دستور ping با پروتکل ICMP کار میکند.  
ابتدا از سمت کامپیوتر من به مقصد، یک ICMP REQUEST ارسال میشود.  
اگر مشکلی پیش نیاید، سیستم مقصد، یک ICMP REPLY به کامپیوتر من میفرستد.

که در صورت دریافت reply از مقصد، ما در دستور ping میتوانیم جواب آن را مشاهده کنیم. ولی اگر دریافت نشد، خطا مشاهده خواهیم کرد.

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 1, an ICMP Echo (ping) request). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.35	178.22.122.100	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 2)
2	0.355859	178.22.122.100	192.168.43.35	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=52 (request in 1)
3	1.016769	192.168.43.35	178.22.122.100	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 4)
4	1.089234	178.22.122.100	192.168.43.35	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=52 (request in 3)
5	2.029032	192.168.43.35	178.22.122.100	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 6)
6	2.080473	178.22.122.100	192.168.43.35	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=52 (request in 5)
7	3.041031	192.168.43.35	178.22.122.100	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 8)
8	3.090594	178.22.122.100	192.168.43.35	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=52 (request in 7)
9	3.621542	192.168.43.35	54.182.5.89	TCP	66	51861 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	3.627960	192.168.43.35	178.22.122.100	DNS	80	Standard query 0x1d15 A config.getiantem.org
11	3.779914	178.22.122.100	192.168.43.35	DNS	112	Standard query response 0x1d15 A config.getiantem.org A 104.23.131.47 A 104.23.132.47
12	3.781680	192.168.43.35	104.23.131.47	TCP	66	51863 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	3.908390	104.23.131.47	192.168.43.35	TCP	66	80 → 51863 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
14	3.908639	192.168.43.35	104.23.131.47	TCP	54	51863 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
15	3.911596	192.168.43.35	104.23.131.47	HTTP	492	GET /proxies.yaml.gz HTTP/1.1
16	3.948153	54.182.5.89	192.168.43.35	TCP	66	443 → 51861 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=256
17	3.948360	192.168.43.35	54.182.5.89	TCP	54	51861 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
18	3.952853	192.168.43.35	54.182.5.89	TLSv1.2	295	Client Hello
19	3.954167	104.23.131.47	192.168.43.35	TCP	54	80 → 51863 [ACK] Seq=1 Ack=439 Win=188416 Len=0

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
 Ethernet II, Src: Azurewaf-f3:86:15 (f0:03:8c:f3:86:15), Dst: f2:8a:76:a0:cc:b8 (f2:8a:76:a0:cc:b8)  
 Internet Protocol Version 4, Src: 192.168.43.35, Dst: 178.22.122.100  
 Internet Control Message Protocol

0000 f2 8a 76 a0 cc b8 f0 03 8c f3 86 15 00 00 45 00 . . . . . E  
 0010 00 3c a2 38 00 00 80 01 80 42 c0 a8 2b 23 b2 16 . < 8 . . . B + #  
 0020 7a 64 08 00 4d 56 00 01 00 05 61 62 63 64 65 66 zd - MV . . . abcdef  
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklm opqrstuv  
 0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

\*دو فایل MyOwnICMP و MyOwnCapture ضمیمه شده است.

### **\*\*تکلیف: تفاوت بین ورژن HTTP/1 و HTTP/1.1 :**

در پروتکل HTTP 1.1 ، داشتن یک header برای host، بر اساس مشخصات، ضروری است. اما در HTTP 1.0 ، به طور رسمی، داشتن header برای host ضرورتی ندارد؛ اگرچه اضافه کردن آن ضروری ندارد. و البته بسیاری از برنامه ها، صرف نظر از نسخه پروتکلی که از آن استفاده میکنند، انتظار مشاهده ی header مربوط به host را دارند. webServer می تواند از قسمت مربوط به host برای تشخیص اینکه client کدام سایت را می خواهد، استفاده کند.