

بخش اول (آشنایی با وایرشارک (HTTP)

(الف)

```

maryan@naryan:~$ sudo tshark -r /home/naryan/Documents/97_4/Network/AHW2_WiresharkPart.pcapng -z io,phs -q | tr -s ' ' | cut -f 2 -d ' ' | tail -n +7 | head -n -1
[sudo] password for maryan:
Running as user "root" and group "root". This could be dangerous.
tshark: lua: Error during loading:
/usr/share/wireshark/init.lua:32: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
arp
ip
udp
nbdgm
smb
mailslot
browser
dns
ssdp
mdns
tcp
ssl
tcp.segments
data
http
_ws.malformed
ipv6
udp
mdns
maryan@naryan:~$

```

به کمک دستور

```
sudo tshark -r "file" -z io,phs -q | tr -s ' ' | cut -f 2 -d ' ' | tail -n +7 | head -n -1
```

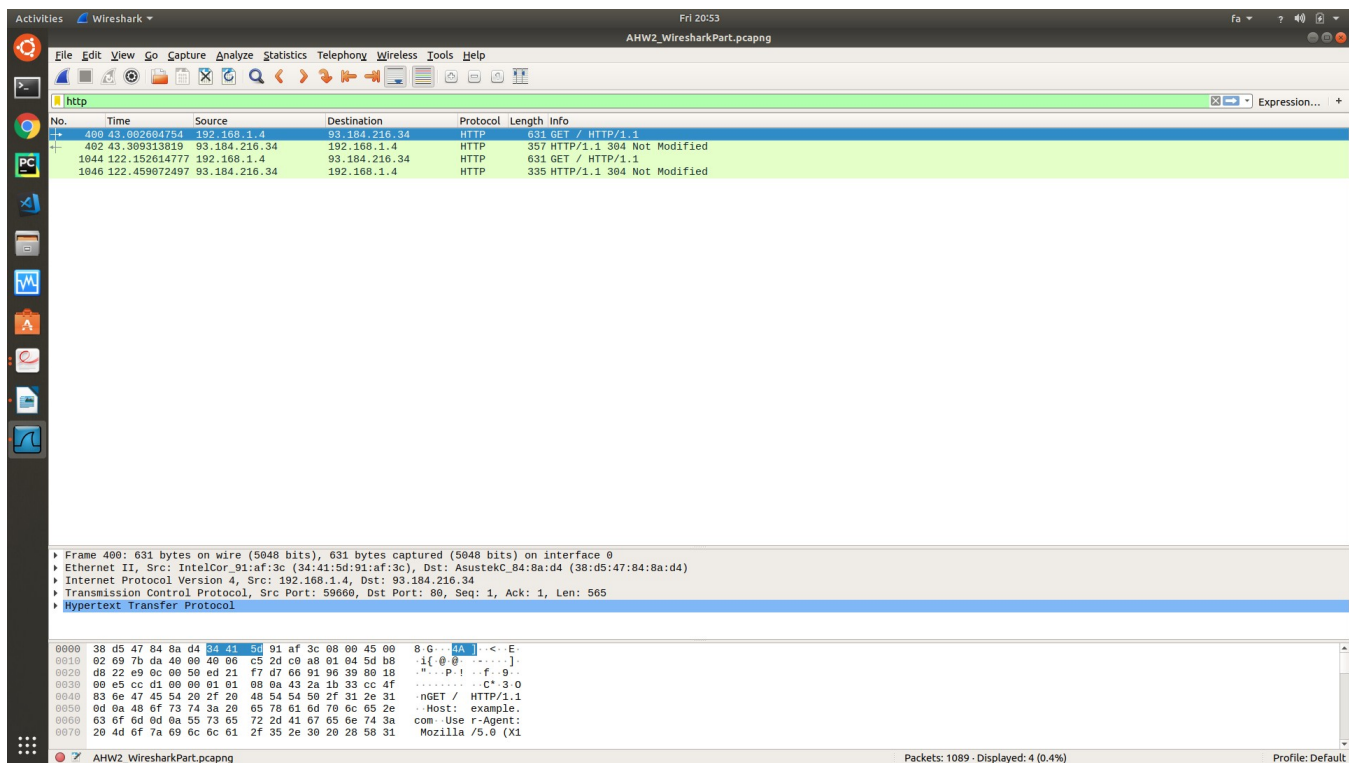
، که به جای "file" باید نام فایل مورد نظر با پسوند .pcapng را بگذاریم ، میتوانیم تمام

انواع پروتکل هایی که در فایل مذکور آمده را استخراج کنیم.

انواع پروتکل ها به شرح زیر است :

ARP , IP , UDP , nbdgm , SMB , Mailslot , BROWSER , DNS , SSDP , mDNS , TCP ,
SSL , TCP.segments , SSL , data , TCP.segments , HTTP , _ws.malformed , IPv6 ,
UDP , MDNS

(ب)



طبق این عکس ، GET از طرف IP:192.168.1.4 در زمان 43.002604754 ارسال شده و پیام "304 not Modified" از طرف IP:93.184.216.34 در زمان 43.309313819 دریافت شده ، پس فاصله این دو 0.306709062 ثانیه شده است! /:

چ) درخواست فروجی از سیستم من به ادرس IP:93.184.216.34 که همان IP Address مربوط به سرور سایت مورد نظر بوده یعنی همان example.com ، ارسال شده است! واضح است که دلیل این امر یک ارتباط سرور-کلاینت است که سیستم من کلاینت بوده و درخواستش را به سرور مبنی بر دریافت یه URL ارسال کرده و سرور هم پاسخی داده که اینجا این پاسخ 304notModified بوده
}* کد 304 ، بدون تغییر (Not Modified):

کد 304 مربوط به مواقعی است که مرورگر همراه درخواست خود، تقاضای اطلاعات مربوط به آخرین تغییرات فایل یا منبع را نیز از سرور می نماید، اگر در فایل مورد نظر، از آخرین درخواست تا لحظه

فعلی، تغییری صورت نگرفته باشد) با هر تغییر در فایل ها، تاریخ آخرین تغییر در قسمت اطلاعات فایل، ذخیره می شود)، سرور در پاسخ، کد 304 را ارسال می کند، این کار علاوه بر اینکه باعث صرفه جویی در منابع سرور می شود، در افزایش سرعت پردازش در سمت کاربر نیز نقش بسیار موثری دارد.}

همچنین این اطلاعات جزیی این ادرس IP به شرح زیر است (برگرفته از سایت <https://ipinfo.io>):

```
city: "Norwel"
region: "Massachusetts"
country: "US"
loc: "42.1596,-70.8217"
postal: "02061"
asn: Object
asn: "AS15133"
name: "MCI Communications Services, Inc. d/b/a Verizon Business"
domain: "verizondigitalmedia.com"
route: "93.184.216.0/24"
type: "business"
company: Object
name: "NETBLK-03-EU-93-184-216-0-24"
domain: "verizondigitalmedia.com"
type: "business"
```

د) هم مرورگر من و هم سرور ، 1.1 HTTP را اجرا میکنند.

تفاوت نسخه 1.0 و 1.0 HTTP :

- ** تفاوت عمده بین HTTP 1.0 و HTTP 1.1 در این است که HTTP 1.0 برای هر یک از پروسه

های درخواست و پاسخ (Request/Response) یک ارتباط جدید ایجاد می کند، در صورتی که در

HTTP 1.1 برای مبادلات یک یا چندین درخواست و پاسخ از یک ارتباط استفاده می کند و ارتباط

جدیدی ایجاد نمی کند.

- در حقیقت HTTP 1.1 نسخه ارتقا یافته ی 1.0 HTTP است

- HTTP 1.0 از 14 status codes استفاده میکند

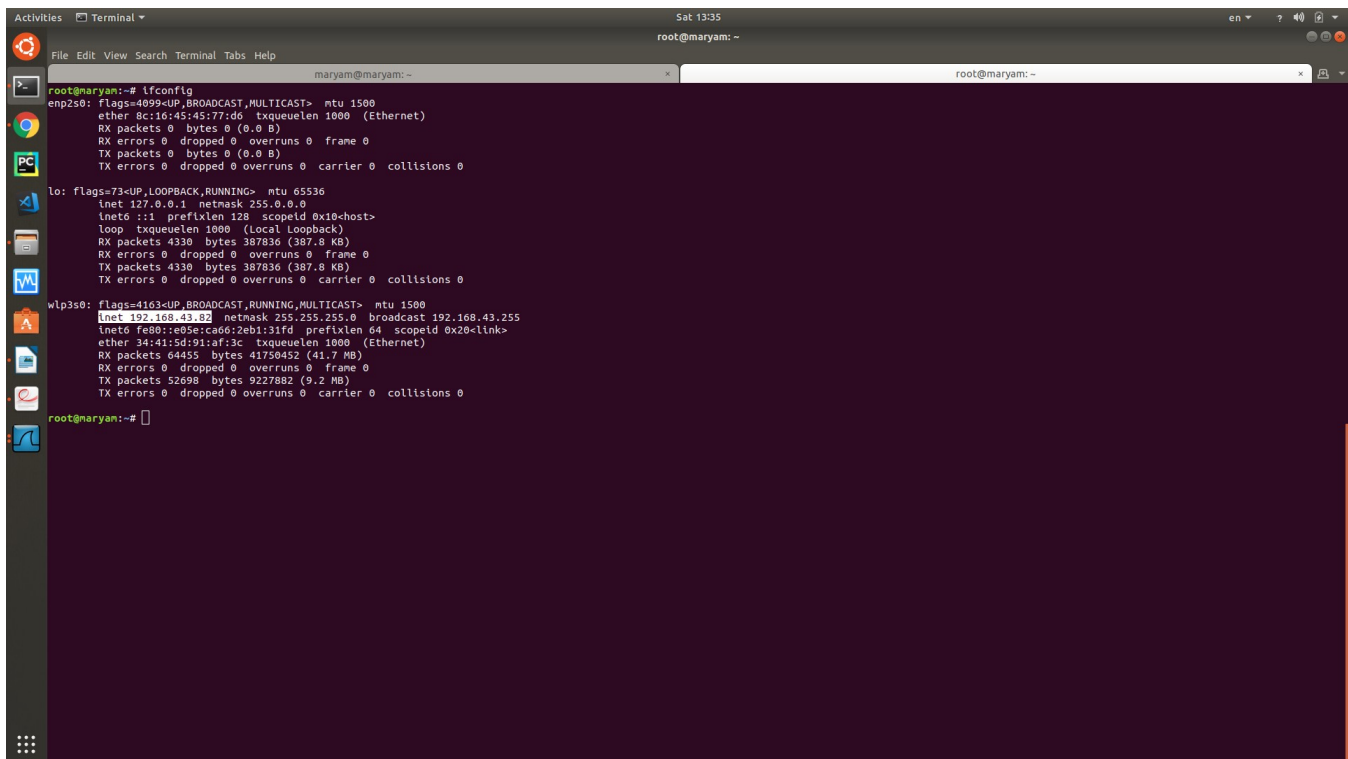
- HTTP 1.1 از 24 status codes استفاده میکند

- 1.1 HTTP از یک هدر تحت عنوان warning استفاده میکند تا بتواند هشدارهای وضعیت ثانویه بدهد.

- امروز هویت در HTTP 1.0 ناامن است زیرا کدگذاری نشده است

- 1.1 HTTP امن است زیرا از username, password و one time value استفاده میکند

هـ) My IP Address : 192.168.43.82



```
root@maryam:~# ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 8c:16:45:45:77:d6 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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 4330 bytes 387836 (387.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4330 bytes 387836 (387.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.82 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::e058:ca60:2eb1:31fd prefixlen 64 scopeid 0x20<link>
    ether 34:41:5d:91:af:3c txqueuelen 1000 (Ethernet)
    RX packets 64455 bytes 41750452 (41.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 52698 bytes 9227882 (9.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@maryam:~#
```

و) از پروتکل های TCP , UDP استفاده شده است.

ز) همان طور که در عکس هم پیداس ، دوبار ارتباط با IP:93.184.216.34 (example.com) داشتیم:

دفعه دوم :

پورت مبدا : 59744

پورت مقصد : 80

دفعه اول :

پورت مبدا : 59660

پورت مقصد : 80

Activities Wireshark Sat 02:14 en ? 40 AHW2_WiresharkPart.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark - Conversations - AHW2_WiresharkPart.pcapng

Ethernet II	IP v4	Port A	Port B	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.4	49254	172.217.23.131	443	18	5,823	10	1,278	8	4,545	20.936772	61.3918	166
192.168.1.4	60168	172.217.22.99	443	18	5,822	10	1,278	8	4,544	20.936902	61.3842	166
192.168.1.4	33574	172.217.22.100	443	24	3,902	12	2,022	12	1,880	20.939454	66.7058	242
192.168.1.4	48710	172.217.21.193	443	20	6,554	11	1,344	9	5,210	20.970343	61.3453	175
192.168.1.4	49700	172.217.23.163	443	18	5,834	10	1,290	8	4,544	20.972403	61.3458	168
192.168.1.4	33596	172.217.22.100	443	13	1,598	7	1,050	6	548	21.044797	33.5281	250
192.168.1.4	48720	172.217.21.193	443	48	16 k	24	3,189	24	13 k	21.056082	89.2156	285
192.168.1.4	38446	172.217.16.142	443	135	34 k	55	18 k	80	16 k	25.651418	108.5831	1,329
192.168.1.4	39934	66.102.1.188	5228	20	6,001	10	1,468	10	5,133	28.524197	98.5429	119
192.168.1.4	49162	35.224.99.156	80	5	370	5	370	0	0	29.869192	15.3167	193
192.168.1.4	39888	66.102.1.188	5228	2	120	1	66	1	54	30.520993	0.1943	2,718
192.168.1.4	59660	93.184.216.34	80	10	1,532	6	969	4	503	42.679131	60.9401	127
192.168.1.4	33616	107.191.46.11	443	38	15 k	20	11 k	18	3,979	51.166129	2.6969	33 k
192.168.1.4	33618	107.191.46.11	443	10	2,381	6	643	4	1,738	51.810027	0.5119	10 k
192.168.1.4	33622	107.191.46.11	443	20	5,289	10	1,830	10	3,459	52.118810	0.9176	15 k
192.168.1.4	33624	107.191.46.11	443	10	2,381	6	643	4	1,738	52.508113	0.5698	9,028
192.168.1.4	33564	107.191.46.11	443	5	337	3	174	2	163	65.288975	0.1379	10 k
192.168.1.4	33554	107.191.46.11	443	3	198	2	132	1	66	65.289002	0.1379	7,659
192.168.1.4	32982	192.0.32.8	443	25	5,160	13	3,005	12	2,155	80.478511	24.5737	978
192.168.1.4	32984	192.0.32.8	443	20	2,165	10	1,260	10	905	80.478547	25.9049	389
192.168.1.4	43570	172.217.18.163	443	19	4,084	10	2,217	9	1,867	81.942741	0.6852	25 k
192.168.1.4	38486	172.217.16.142	443	21	4,647	11	1,856	10	2,791	82.460272	0.7819	18 k
192.168.1.4	32996	192.0.32.8	443	41	15 k	20	3,514	21	12 k	103.775187	7.1542	3,929
192.168.1.4	33642	172.217.22.100	443	144	78 k	67	7,944	77	70 k	109.856256	2.0560	30 k
192.168.1.4	49334	172.217.23.131	443	15	5,624	8	1,146	7	4,478	109.866818	0.4572	20 k
192.168.1.4	60248	172.217.22.99	443	15	5,625	8	1,146	7	4,479	109.866865	0.4934	18 k
192.168.1.4	33658	172.217.22.100	443	22	3,770	11	1,956	11	1,814	109.871192	0.6748	23 k
192.168.1.4	48790	172.217.21.193	443	17	6,368	9	1,224	8	5,144	109.872177	0.4888	20 k
192.168.1.4	49780	172.217.23.163	443	15	5,624	8	1,146	7	4,478	109.872372	0.4856	18 k
192.168.1.4	33666	172.217.22.100	443	11	1,478	6	984	5	494	109.976087	10.3738	758
192.168.1.4	48804	172.217.21.193	443	34	14 k	16	2,565	18	11 k	109.988990	0.6737	30 k
192.168.1.4	48806	172.217.21.193	443	10	1,491	6	994	4	497	109.989008	0.4924	16 k
192.168.1.4	48808	172.217.21.193	443	11	1,557	7	1,060	4	497	109.989010	0.5004	16 k
192.168.1.4	33692	107.191.46.11	443	19	5,223	10	1,830	9	3,393	112.836622	1.0341	14 k
192.168.1.4	33694	107.191.46.11	443	10	2,381	6	643	4	1,738	113.449123	0.4923	10 k
192.168.1.4	59744	93.184.216.34	80	7	1,312	4	837	3	475	121.880493	0.5786	11 k
192.168.1.4	46206	74.125.133.188	5228	14	6,204	7	1,258	7	4,946	124.898520	0.6327	15 k

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

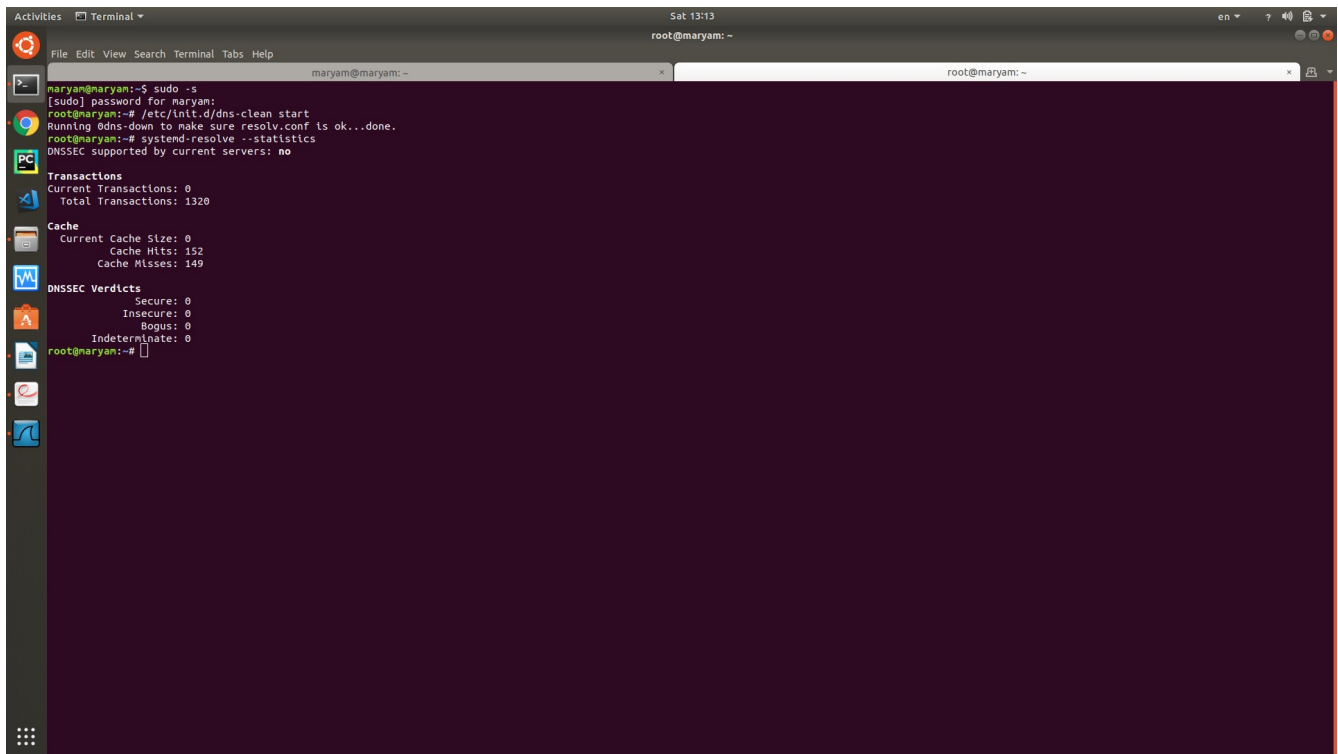
Help Copy Follow Stream... Graph... Close

0000 38 d5 47 84 8a d4 34 41 5d 91 af 3c 08 00 45 00 8 G...4A]< E
0010 02 09 7b da 48 08 48 06 c5 2d c0 a8 01 04 5d b8 i { @ @]
0020 d8 22 e9 0c 08 50 ed 21 f7 d7 06 01 06 39 80 18 . . P i . . f . 9 .
0030 00 e5 cc d1 09 00 01 01 08 0a 43 2a 1b 33 cc 4f C* 3 0
0040 83 6e 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 nGET / HTTP/1.1
0050 0d 6a 48 6f 73 74 3a 20 65 78 61 6d 70 6c 65 2e . Host: example.
0060 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 74 3a com Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1

AWH2_WiresharkPart.pcapng Packets: 1089 - Displayed: 4 (0.4%) Profile: Default

بخش دوم (دیباغی DNS توسط وایرشارک)

طبق عکس زیر کش میزبان خود را پاک کردیم.




```
maryam@maryam:~$ sudo -s
[sudo] password for maryam:
root@maryam:~# /etc/init.d/dns-clean start
Running dnsmasq to make sure resolv.conf is ok...done.
root@maryam:~# systemd-resolve --statistics
DNSSEC supported by current servers: no
Transactions
Current Transactions: 0
Total Transactions: 1320
Cache
Current Cache Sizes: 0
Cache Hits: 152
Cache Misses: 149
DNSSEC Verdicts
Secure: 0
Insecure: 0
Bogus: 0
Indeterminate: 0
root@maryam:~#
```

flush the DNS Resolver Cache in ubuntu

و در ادامه ، طبق مراحل زیر کش مرورگر را هم پاک کردیم:

In Chrome

- 1.On your computer, open Chrome.
- 2.At the top right, click More .
- 3.Click **More tools>Clear browsing data**.
- 4.At the top, choose a time range. To delete everything, select **All time**.
- 5.Next to "Cookies and other site data" and "Cached images and files," check the boxes.
- 6.Click **Clear data**.

(الف)

ActivitiesWireshark

Sat 16:08

en ?

AHW2_WiresharkPart(B).pcapng

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Expression...

dns

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000540873	192.168.43.82	192.168.43.1	DNS	89	Standard query 0x7e9b A clientservices.googleapis.com
3	0.000611373	192.168.43.82	192.168.43.1	DNS	79	Standard query 0xe96a A accounts.google.com
4	0.000819137	192.168.43.82	192.168.43.1	DNS	78	Standard query 0xc76c A www.googleapis.com
5	0.002981856	192.168.43.82	192.168.43.1	DNS	76	Standard query 0xb192 A mtalk.google.com
6	0.031413355	192.168.43.82	192.168.43.1	DNS	74	Standard query 0xf5e9 A www.google.com
8	0.171734597	192.168.43.82	192.168.43.1	DNS	75	Standard query 0x9d58 A ssl.gstatic.com
9	0.222823496	192.168.43.1	192.168.43.82	DNS	121	Standard query response 0xb192 A mtalk.google.com CNAME mobile-gtalk.l.google.com A 198.177.15.188
10	0.222953094	192.168.43.1	192.168.43.82	DNS	98	Standard query response 0xf5e9 A www.google.com A 172.217.16.164
11	0.223074613	192.168.43.1	192.168.43.82	DNS	105	Standard query response 0x7e9b A clientservices.googleapis.com A 216.58.208.35
12	0.223172127	192.168.43.1	192.168.43.82	DNS	95	Standard query response 0xe96a A accounts.google.com A 172.217.16.173
13	0.223322210	192.168.43.1	192.168.43.82	DNS	352	Standard query response 0xc76c A www.googleapis.com CNAME googleapis.l.google.com A 172.217.18.10 A 172.217.18.106 A 172.217...
14	0.242341327	192.168.43.82	192.168.43.1	DNS	91	Standard query response 0x9d58 A ssl.gstatic.com A 172.217.16.131
200	1.138466225	192.168.43.82	192.168.43.1	DNS	94	Standard query 0xc593 A oauthaccountmanager.googleapis.com
240	1.162932935	192.168.43.1	192.168.43.82	DNS	368	Standard query response 0xc593 A oauthaccountmanager.googleapis.com CNAME googleapis.l.google.com A 172.217.22.42 A 172.217.1...
350	1.666096244	192.168.43.82	192.168.43.1	DNS	75	Standard query 0xc34b A www.gstatic.com
355	1.697785962	192.168.43.1	192.168.43.82	DNS	91	Standard query response 0xc34b A www.gstatic.com A 172.217.18.99
480	2.105642379	192.168.43.82	192.168.43.1	DNS	84	Standard query 0xfef5 A accounts.doubleclick.net
481	2.105726565	192.168.43.82	192.168.43.1	DNS	80	Standard query 0xcd64 A accounts.youtube.com
507	2.146640521	192.168.43.1	192.168.43.82	DNS	131	Standard query response 0xfef5 A accounts.doubleclick.net CNAME www3.l.google.com A 172.217.21.206
511	2.147818956	192.168.43.1	192.168.43.82	DNS	96	Standard query response 0xcd64 A accounts.youtube.com A 10.10.34.35
563	2.490618746	192.168.43.82	192.168.43.1	DNS	79	Standard query 0x86af A clients4.google.com
574	2.534568652	192.168.43.1	192.168.43.82	DNS	119	Standard query response 0x86af A clients4.google.com CNAME clients.l.google.com A 172.217.22.14
622	2.690614081	192.168.43.82	192.168.43.1	DNS	75	Standard query 0xdac6 A apis.google.com
628	2.734470319	192.168.43.1	192.168.43.82	DNS	112	Standard query response 0xdac6 A apis.google.com CNAME plus.l.google.com A 172.217.22.118
781	3.446127399	192.168.43.82	192.168.43.1	DNS	69	Standard query 0x142b A nooli.org
833	4.052591599	192.168.43.82	192.168.43.1	DNS	84	Standard query 0x52c9 A fonts.googleapis.com
839	4.052591599	192.168.43.82	192.168.43.1	DNS	84	Standard query 0xe357 A www.googletagmanager.com
841	9.512893084	192.168.43.1	192.168.43.82	DNS	132	Standard query response 0x52c9 A fonts.googleapis.com CNAME googleadapis.l.google.com A 172.217.18.106
845	9.516983929	192.168.43.1	192.168.43.82	DNS	144	Standard query response 0xe357 A www.googletagmanager.com CNAME www-googletagmanager.l.google.com A 172.217.22.8
1105	10.378929619	192.168.43.82	192.168.43.1	DNS	77	Standard query 0xeb6e A fonts.gstatic.com
1191	10.219371768	192.168.43.1	192.168.43.82	DNS	129	Standard query response 0xeb6e A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 216.58.208.35
1267	10.348561338	192.168.43.82	192.168.43.1	DNS	79	Standard query 0x4533 A clients1.google.com
1301	10.379802481	192.168.43.82	192.168.43.1	DNS	84	Standard query 0x3f51 A www.google-analytics.com
1314	10.379437249	192.168.43.1	192.168.43.82	DNS	119	Standard query response 0x4533 A clients1.google.com CNAME clients.l.google.com A 172.217.22.14
1461	10.404535186	192.168.43.82	192.168.43.1	DNS	144	Standard query response 0x3f51 A www.google-analytics.com CNAME www-google-analytics.l.google.com A 172.217.18.174
1848	11.134977177	192.168.43.82	192.168.43.1	DNS	79	Standard query 0x3864 A client2.google.com
1860	11.157335487	192.168.43.1	192.168.43.82	DNS	119	Standard query response 0x3864 A client2.google.com CNAME clients.l.google.com A 172.217.21.206

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 71

Identification: 0xb0be (36286)

Flags: 0x0000, Don't fragment

Time to live: 64

Protocol: UDP (17)

Header checksum: 0xd543 [validation disabled]

0010 00 47 8b de 40 00 40 15 d5 43 c0 8b 2b 01 c0 a8 -G-@-@-C-+...

Protocol (ip.addr) 1 byte

Packets: 1984 - Displayed: 38 (1.9%)

Profile: Default

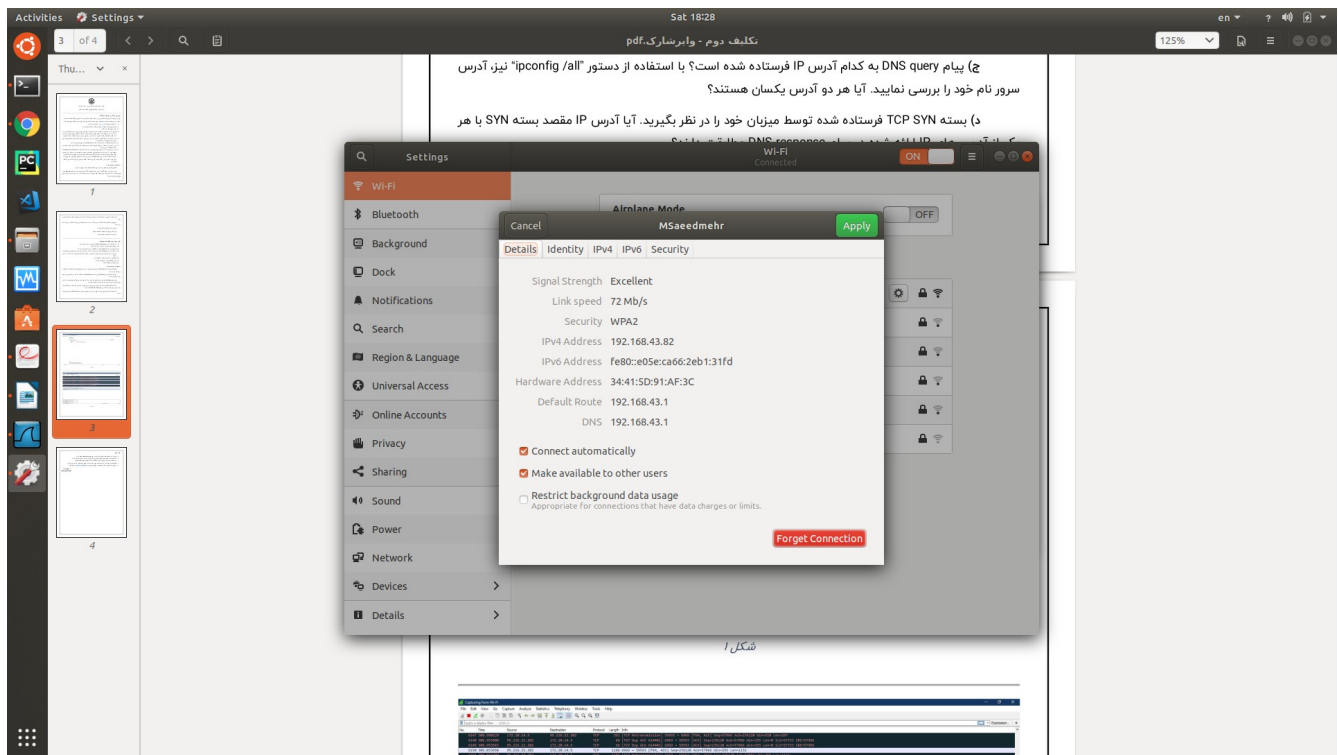
طبق عکس فوق ، IP Addr:192.168.43.82 آدرس فرستنده ی DNS query است و گیرنده IP Addr:192.168.43.1 است. همچنین از پروتکل UDP استفاده شده است.

(ب)

يُورَت مَبْدَا : 52671 يُورَت مَقْصَد : 53

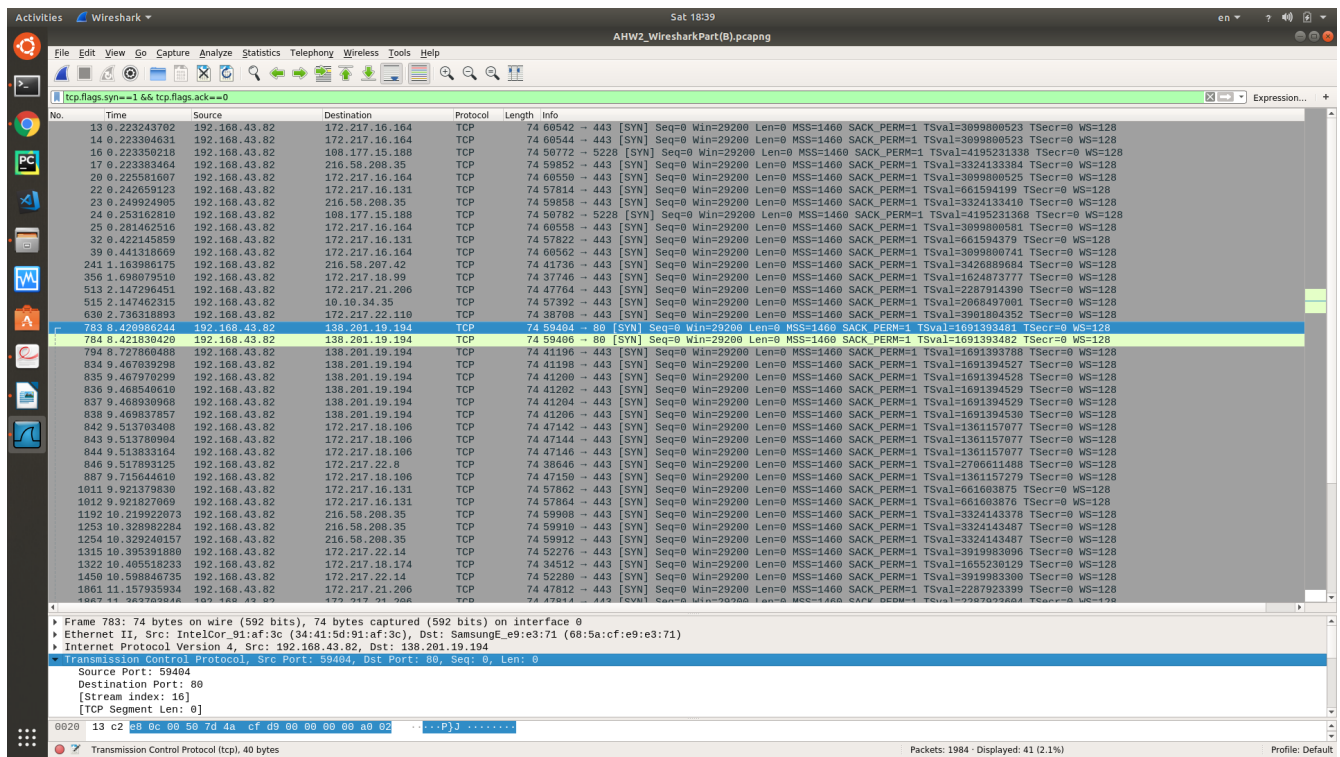
این شماره پورت (۵۳) سرویس دهنده ی DNS است.

ج) به ادرس 192.168.43.1 ارسال میشود.



طبق عکس فوق ادرس server name من همان 192.168.43.1 است

(د)



بله ، طبق عکس فوق ، ادرس IP مقصد بسته ی SYN با ادرس IP:138.201.19.194 که در پیام DNS response هم بود مطابقت دارد.

ه (خیر