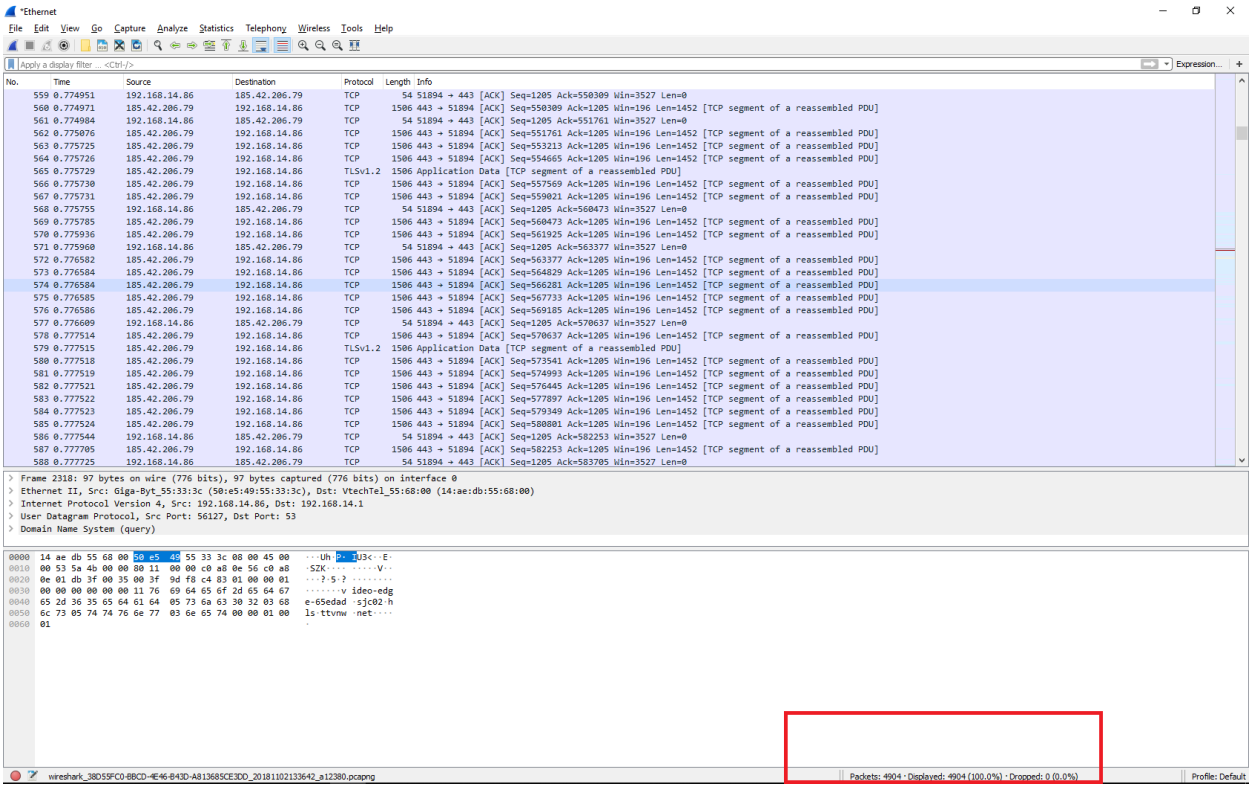
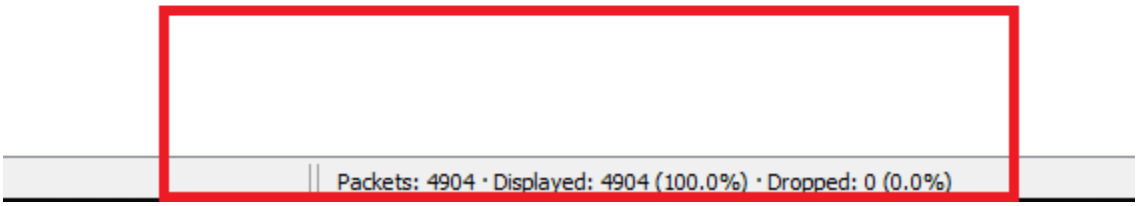
שאלה 2

א.





4909 פקטות הוסנפו

ב.

udp

No.	Time	Source	Destination	Protocol	Length	Info
2283	6.235760	185.212.200.74	192.168.14.86	UDP	211	51766 → 64499 Len=169
2284	6.260100	185.212.200.74	192.168.14.86	UDP	141	51766 → 64499 Len=99
2285	6.277847	185.212.200.74	192.168.14.86	UDP	143	51766 → 64499 Len=101
2289	6.295755	185.212.200.74	192.168.14.86	UDP	144	51766 → 64499 Len=102
2290	6.319276	185.212.200.74	192.168.14.86	UDP	167	51766 → 64499 Len=125
2291	6.336302	185.212.200.74	192.168.14.86	UDP	140	51766 → 64499 Len=98
2292	6.360255	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2293	6.383447	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2294	6.402818	185.212.200.74	192.168.14.86	UDP	186	51766 → 64499 Len=144
2295	6.423275	185.212.200.74	192.168.14.86	UDP	181	51766 → 64499 Len=139
2296	6.437846	185.212.200.74	192.168.14.86	UDP	188	51766 → 64499 Len=146
2298	6.455875	185.212.200.74	192.168.14.86	UDP	144	51766 → 64499 Len=102
2299	6.478576	185.212.200.74	192.168.14.86	UDP	164	51766 → 64499 Len=122
2300	6.496562	185.212.200.74	192.168.14.86	UDP	141	51766 → 64499 Len=99
2302	6.520441	185.212.200.74	192.168.14.86	UDP	145	51766 → 64499 Len=103
2303	6.537925	185.212.200.74	192.168.14.86	UDP	155	51766 → 64499 Len=113
2304	6.562308	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2305	6.579374	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2306	6.598262	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2307	6.619669	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2308	6.636690	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2309	6.661308	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2310	6.678784	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2311	6.697761	185.212.200.74	192.168.14.86	UDP	185	51766 → 64499 Len=143
2313	6.719766	185.212.200.74	192.168.14.86	UDP	154	51766 → 64499 Len=112
2314	6.737979	185.212.200.74	192.168.14.86	UDP	197	51766 → 64499 Len=155
2316	6.756233	185.212.200.74	192.168.14.86	UDP	196	51766 → 64499 Len=154
2317	6.777557	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121

Packets: 4904 · Displayed: 1203 (24.5%) · Dropped: 0 (0.0%)

1203 פקטות מוצגות

ג.

```
C:\Users\ranra>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : Home
   IPv6 Address. . . . . . . . . . . : fd26:ae94:5fc:0:57c:9893:5a36:7dae
   Temporary IPv6 Address. . . . . . : fd26:ae94:5fc:0:d5c9:8ea8:b782:5fdd
   Link-local IPv6 Address . . . . . : fe80::57c:9893:5a36:7dae%6
   IPv4 Address. . . . . . . . . . . : 192.168.14.86
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.14.1
```

הIP הוא 192.168.14.86

ד.

```
0.262975    192.168.14.86    192.168.14.1    DNS    77 Standard query 0x586f A ekg.riotgames.com
> Frame 33: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
> Ethernet II, Src: Giga-Byt_55:33:3c (50:e5:49:55:33:3c), Dst: VtechTel_55:68:00 (14:ae:db:55:68:00)
> Internet Protocol Version 4, Src: 192.168.14.86, Dst: 192.168.14.1
> User Datagram Protocol, Src Port: 60478, Dst Port: 53
> Domain Name System (query)
```

החבילה נשלחה מהמחשב שלי (כי הIP של השולח הוא הIP שלי)
החבילה נשלחה מפורט 60478 לפורט 53
תוכן החבילה הוא:

```
0000  14 ae db 55 68 00 50 e5  49 55 33 3c 08 00 45 00   ···Uh·P· IU3<··E·
0010  00 3f 5a 49 00 00 80 11  00 00 c0 a8 0e 56 c0 a8   ·?ZI···· ·····V··
0020  0e 01 ec 3e 00 35 00 2b  9d e4 58 6f 01 00 00 01   ···>·5·+ ··Xo····
0030  00 00 00 00 00 00 03 65  6b 67 09 72 69 6f 74 67   ·******e kg·riotg
0040  61 6d 65 73 03 63 6f 6d  00 00 01 00 01            ames·com *****
```

הIP של שולח היא 192.168.14.86 ושל המקבל 192.168.14.1

באדום, כתובת הIP של השולח. בירוק כתובת הIP של המקבל
כתובת הMAC של השולח: 50:e5:49:55:33:3c, של המקבל 14:ae:db:55:68:00

ה.

```
> Frame 36: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits) on interface 0
v Ethernet II, Src: VtechTel_55:68:00 (14:ae:db:55:68:00), Dst: Giga-Byt_55:33:3c (50:e5:49:55:33:3c)
  > Destination: Giga-Byt_55:33:3c (50:e5:49:55:33:3c)
  > Source: VtechTel_55:68:00 (14:ae:db:55:68:00)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.14.1, Dst: 192.168.14.86
> User Datagram Protocol, Src Port: 53, Dst Port: 60478
> Domain Name System (response)

0000  50 e5 49 55 33 3c 14 ae  db 55 68 00 08 00 45 00   P·IU3<·· ·Uh···E·
0010  00 fa 00 00 40 00 40 11  9c 4b c0 a8 0e 01 c0 a8   ····@·@· ·K******
0020  0e 56 00 35 ec 3e 00 e6  15 c2 58 6f 81 80 00 01   ·V·5·>·· ··Xo····
0030  00 09 00 00 00 00 03 65  6b 67 09 72 69 6f 74 67   *******e kg·riotg
0040  61 6d 65 73 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ames·com ********
0050  05 00 01 00 00 00 5c 00  2f 11 70 72 6f 64 2d 6c   ******\· /·prod-l
0060  62 2d 34 30 33 36 39 38  36 39 36 09 75 73 2d 77   b-403698 696·us-w
0070  65 73 74 2d 32 03 65 6c  62 09 61 6d 61 7a 6f 6e   est-2·el b·amazon
0080  61 77 73 03 63 6f 6d 00  c0 2f 00 01 00 01 00 00   aws·com· ·/******
0090  00 1e 00 04 36 45 70 45  c0 2f 00 01 00 01 00 00   ····6EpE ·/******
00a0  00 1e 00 04 36 ba bf 79  c0 2f 00 01 00 01 00 00   ····6··y ·/******
00b0  00 1e 00 04 36 da 21 27  c0 2f 00 01 00 01 00 00   ····6·!' ·/******
00c0  00 1e 00 04 23 a5 3c 1a  c0 2f 00 01 00 01 00 00   ····#·<· ·/******
00d0  00 1e 00 04 36 c9 74 12  c0 2f 00 01 00 01 00 00   ····6·t· ·/******
00e0  00 1e 00 04 22 d6 46 fc  c0 2f 00 01 00 01 00 00   ····"·F· ·/******
00f0  00 1e 00 04 36 bb 4c 89  c0 2f 00 01 00 01 00 00   ····6·L· ·/******
0100  00 1e 00 04 36 44 65 c7                            ····6De·
```

החבילה נשלחה מהשרת למחשב שלי
נשלחה מפורט 60478 לפורט 53
כתובת הIP של השולח היא 192.168.14.1 ושל המקבל היא 192.168.86 והן מצויות כאן:

```
0000  50 e5 49 55 33 3c 14 ae  db 55 68 00 08 00 45 00   P·IU3<·· ·Uh···E·
0010  00 fa 00 00 40 00 40 11  9c 4b c0 a8 0e 01 c0 a8   ····@·@· ·K******
0020  0e 56 00 35 ec 3e 00 e6  15 c2 58 6f 81 80 00 01   ·V·5·>·· ··Xo····
0030  00 09 00 00 00 00 03 65  6b 67 09 72 69 6f 74 67   *******e kg·riotg
0040  61 6d 65 73 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ames·com ********
0050  05 00 01 00 00 00 5c 00  2f 11 70 72 6f 64 2d 6c   ******\· /·prod-l
0060  62 2d 34 30 33 36 39 38  36 39 36 09 75 73 2d 77   b-403698 696·us-w
0070  65 73 74 2d 32 03 65 6c  62 09 61 6d 61 7a 6f 6e   est-2·el b·amazon
0080  61 77 73 03 63 6f 6d 00  c0 2f 00 01 00 01 00 00   aws·com· ·/******
0090  00 1e 00 04 36 45 70 45  c0 2f 00 01 00 01 00 00   ····6EpE ·/******
00a0  00 1e 00 04 36 ba bf 79  c0 2f 00 01 00 01 00 00   ····6··y ·/******
00b0  00 1e 00 04 36 da 21 27  c0 2f 00 01 00 01 00 00   ····6·!' ·/******
00c0  00 1e 00 04 23 a5 3c 1a  c0 2f 00 01 00 01 00 00   ····#·<· ·/******
00d0  00 1e 00 04 36 c9 74 12  c0 2f 00 01 00 01 00 00   ····6·t· ·/******
00e0  00 1e 00 04 22 d6 46 fc  c0 2f 00 01 00 01 00 00   ····"·F· ·/******
00f0  00 1e 00 04 36 bb 4c 89  c0 2f 00 01 00 01 00 00   ····6·L· ·/******
0100  00 1e 00 04 36 44 65 c7                            ····6De·
```

כתובת הMAC של השולח: 14:ae:db:55:68:00 של המקבל 50:e5:49:55:33:3

ו. הפורט 53 תמיד מעורב בבקשות הDNS. המשמעות של זה היא שיש פורט מיוחד במחשב שמיועד ספציפית לבקשות בקליינט של שרת DNS.
ז. נוכל לסנן ע"י כך שנחפש פקטות שמעורב בהן פורט 53 בפרוטוקול UDP.

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
2	0.017430	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
3	0.040763	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
4	0.058793	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
6	0.076530	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
7	0.100432	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
9	0.119445	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
10	0.135477	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
12	0.160067	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
13	0.177653	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
14	0.195515	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
30	0.219135	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
31	0.237438	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
32	0.259883	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
33	0.262975	192.168.14.86	192.168.14.1	DNS	77	Standard query 0x586f A ekg.riotgames.com
34	0.263444	192.168.14.86	192.168.14.1	DNS	77	Standard query 0xd12f AAAA ekg.riotgames.com
35	0.277468	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
36	0.277567	192.168.14.1	192.168.14.86	DNS	264	Standard query response 0x586f A ekg.riotgames.com CNAME prod-
37	0.279197	192.168.14.1	192.168.14.86	DNS	220	Standard query response 0xd12f AAAA ekg.riotgames.com CNAME pr
42	0.297232	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
44	0.319807	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121
45	0.336637	185.212.200.74	192.168.14.86	UDP	163	51766 → 64499 Len=121