T.C.

MARMARA UNIVERSITY

FACULTY of ENGINEERING

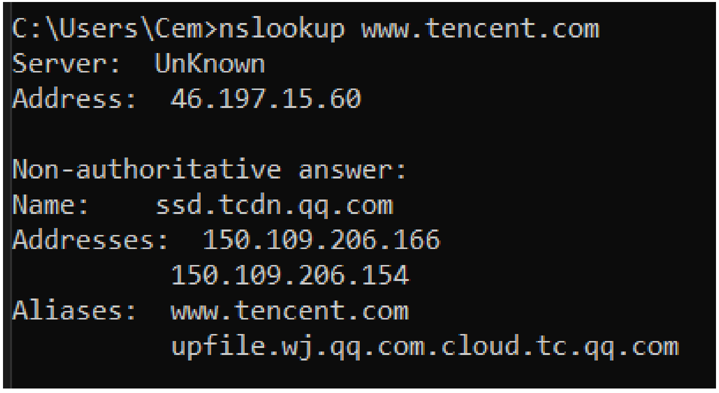
COMPUTER ENGINEERING DEPARTMENT

CSE4074 – Computer Networks Homework II Report

Cem GÜLEÇ - 150117828

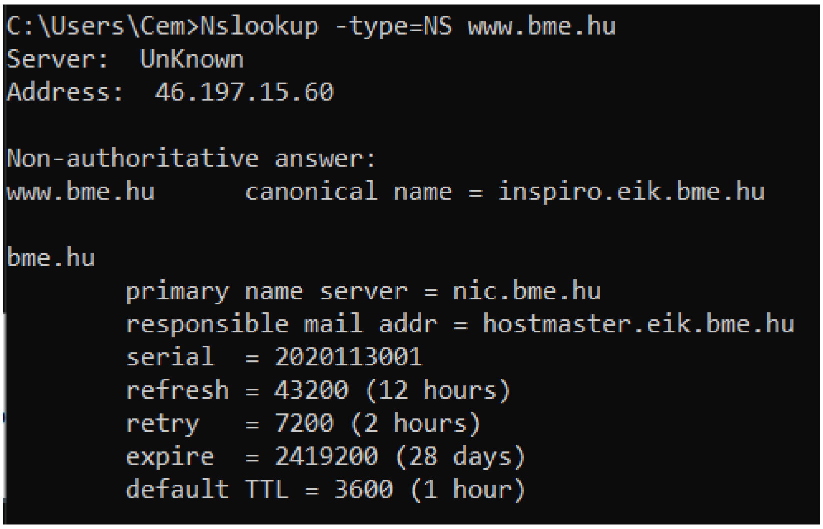
04 December 2020

1. nslookup:



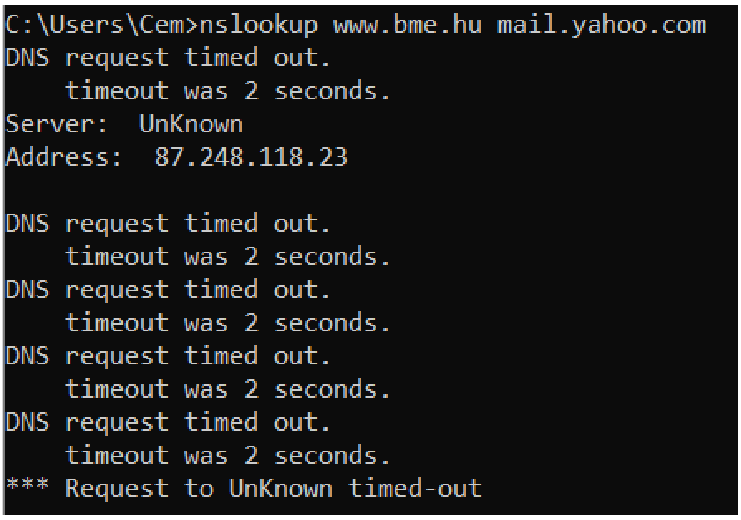
```
C:\Users\Cem>nslookup www.tencent.com
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
Name:    ssd.tcdn.qq.com
Addresses:  150.109.206.166
          150.109.206.154
Aliases:  www.tencent.com
          upfile.wj.qq.com.cloud.tc.qq.com
```

1) As a web server in Asia, I performed the test for Tencent which is a technology company located in China. IP address of the server: 150.109.206.166



```
C:\Users\Cem>Nslookup -type=NS www.bme.hu
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
www.bme.hu      canonical name = inspiro.eik.bme.hu

bme.hu
        primary name server = nic.bme.hu
        responsible mail addr = hostmaster.eik.bme.hu
        serial  = 2020113001
        refresh = 43200 (12 hours)
        retry   = 7200 (2 hours)
        expire  = 2419200 (28 days)
        default TTL = 3600 (1 hour)
```

2) As the European university, I performed the test for Budapest University of Technology located in Hungary in this case. Authoritative DNS server: nic.bme.hu

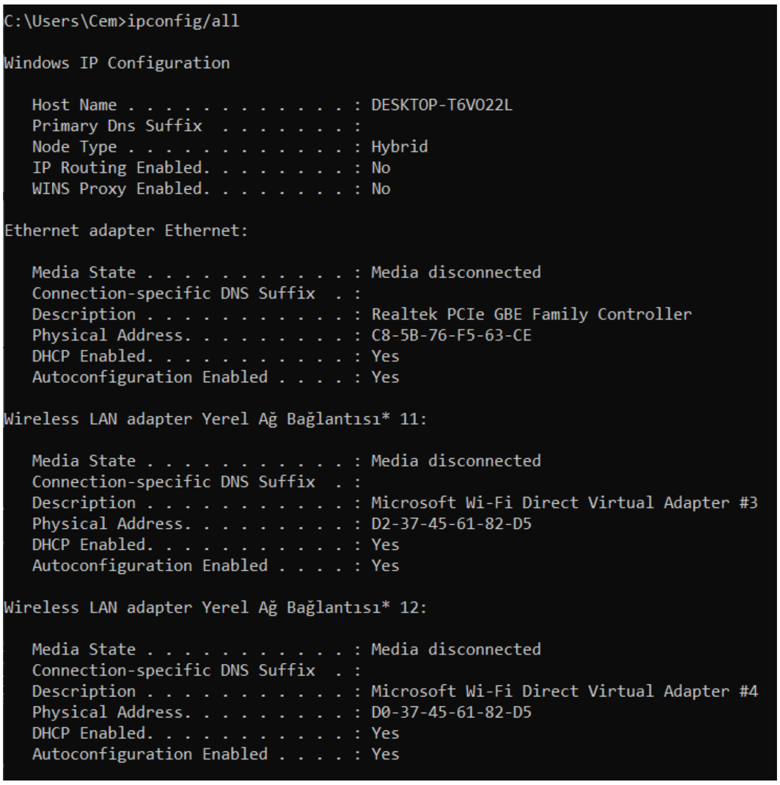


```
C:\Users\Cem>nslookup www.bme.hu mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.118.23

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

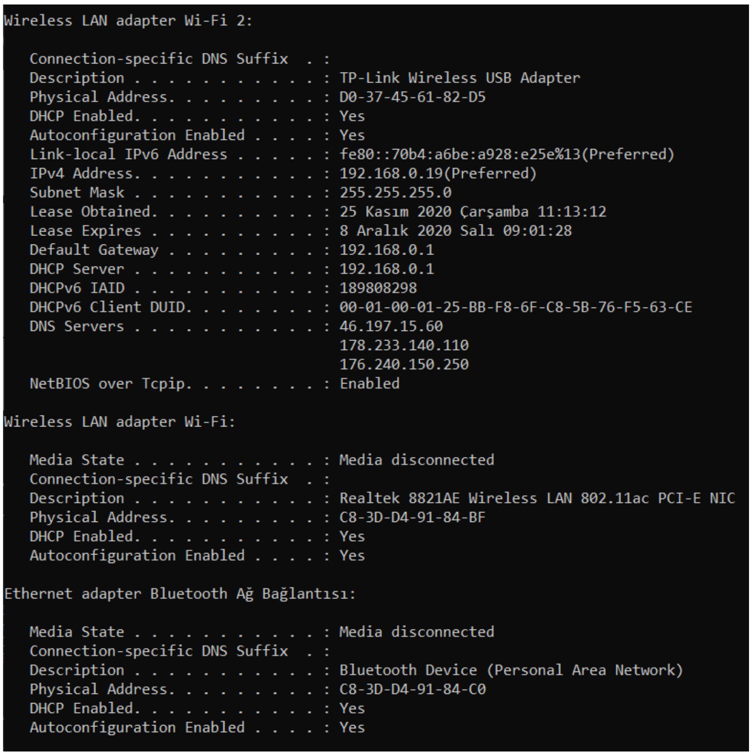
3) I performed the test again for www.bme.hu. I received time out message, assuming that no servers could be reached in via this command.
IP address for the DNS server: 87.248.118.23

2. ipconfig:

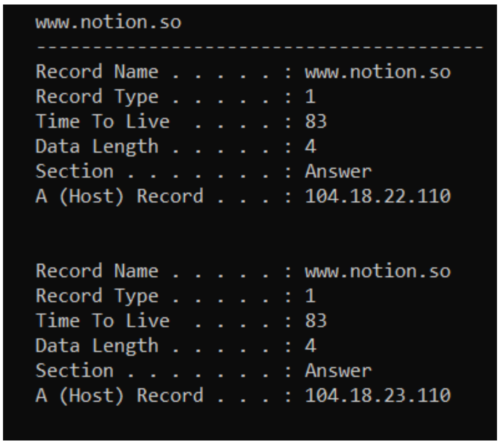
Below screenshots taken for the 2nd part ipconfig commands respectively:
* ipconfig /all
* ipconfig /displaydns
* ipconfig /flushdns



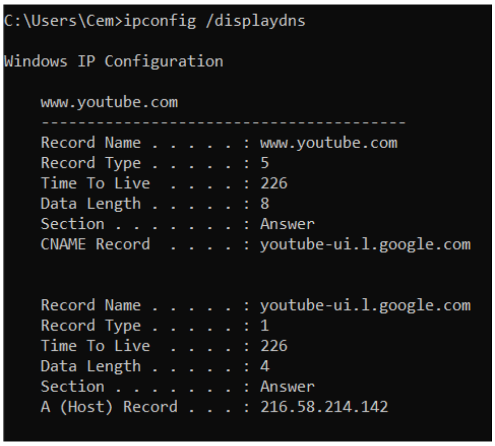
```
C:\Users\Cem>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-T6VO22L
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : C8-5B-76-F5-63-CE
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Yerel Ağ Bağlantısı* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : D2-37-45-61-82-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Yerel Ağ Bağlantısı* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : D0-37-45-61-82-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```



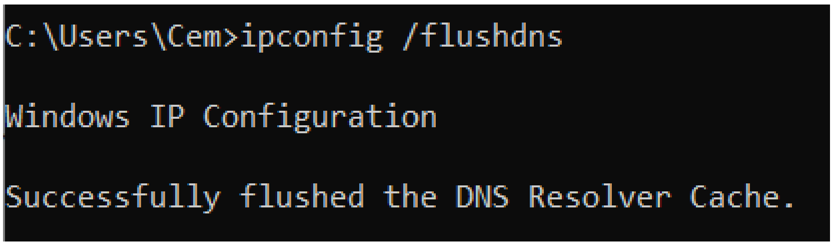
```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TP-Link Wireless USB Adapter
   Physical Address. . . . . . . . . : D0-37-45-61-82-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::70b4:a6be:a928:e25e%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.19(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 25 Kasım 2020 Çarşamba 11:13:12
   Lease Expires . . . . . . . . . . : 8 Aralık 2020 Salı 09:01:28
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 189808298
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-BB-F8-6F-C8-5B-76-F5-63-CE
   DNS Servers . . . . . . . . . . . : 46.197.15.60
                                       178.233.140.110
                                       176.240.150.250
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC
   Physical Address. . . . . . . . . : C8-3D-D4-91-84-BF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Bluetooth Ağ Bağlantısı:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : C8-3D-D4-91-84-C0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```



```
    www.notion.so
    ----------------------------------------
    Record Name . . . . . : www.notion.so
    Record Type . . . . . : 1
    Time To Live  . . . . : 83
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 104.18.22.110


    Record Name . . . . . : www.notion.so
    Record Type . . . . . : 1
    Time To Live  . . . . : 83
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 104.18.23.110
```

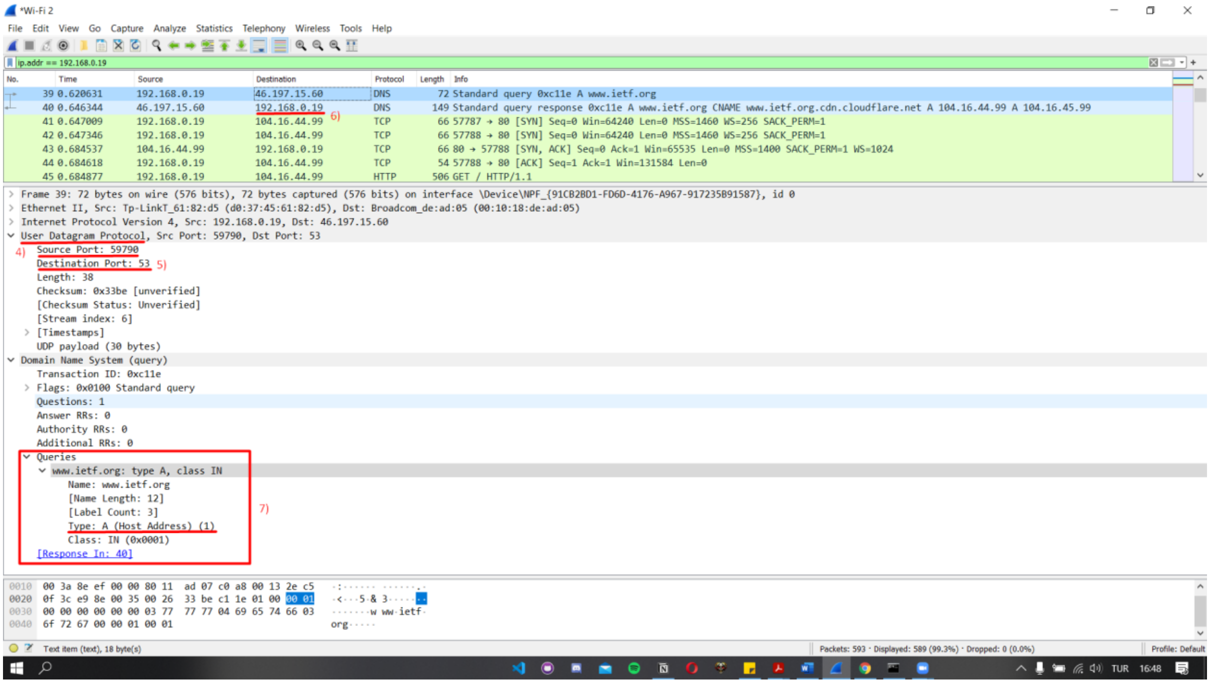


```
C:\Users\Cem>ipconfig /displaydns

Windows IP Configuration

    www.youtube.com
    ----------------------------------------
    Record Name . . . . . : www.youtube.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 226
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : youtube-ui.l.google.com


    Record Name . . . . . : youtube-ui.l.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 226
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 216.58.214.142
```



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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

3. Tracing DNS with Wireshark:


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
4)
5)
6)
7)
TUR
16:48

```
ip.addr == 192.168.0.19

No.  Time      Source         Destination    Protocol Length Info
  39 0.620631  192.168.0.19   46.197.15.60   DNS        72 Standard query 0xc11e A www.ietf.org
  40 0.646344  46.197.15.60   192.168.0.19   DNS       149 Standard query response 0xc11e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
  41 0.647009  192.168.0.19   104.16.44.99   TCP        66 57787 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  42 0.647346  192.168.0.19   104.16.44.99   TCP        66 57788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  43 0.684537  104.16.44.99   192.168.0.19   TCP        66 80 → 57788 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
  44 0.684618  192.168.0.19   104.16.44.99   TCP        54 57788 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
  45 0.684877  192.168.0.19   104.16.44.99   HTTP      506 GET / HTTP/1.1

> Frame 39: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 46.197.15.60
v User Datagram Protocol, Src Port: 59790, Dst Port: 53
    Source Port: 59790
    Destination Port: 53
    Length: 38
    Checksum: 0x33be [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
  > [Timestamps]
    UDP payload (30 bytes)
v Domain Name System (query)
    Transaction ID: 0xc11e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 40]

0010  00 3a 8e ef 00 00 80 11  ad 07 c0 a8 00 13 2e c5   ·:······ ······.·
0020  0f 3c e9 8e 00 35 00 26  33 be c1 1e 01 00 00 01   ·<···5·& 3·······
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····

Text item (text), 18 byte(s)        Packets: 593 · Displayed: 589 (99.3%) · Dropped: 0 (0.0%)        Profile: Default
```

4) As it is indicated in the above image DNS query and response messages sent over User Datagram Protocol (UDP).

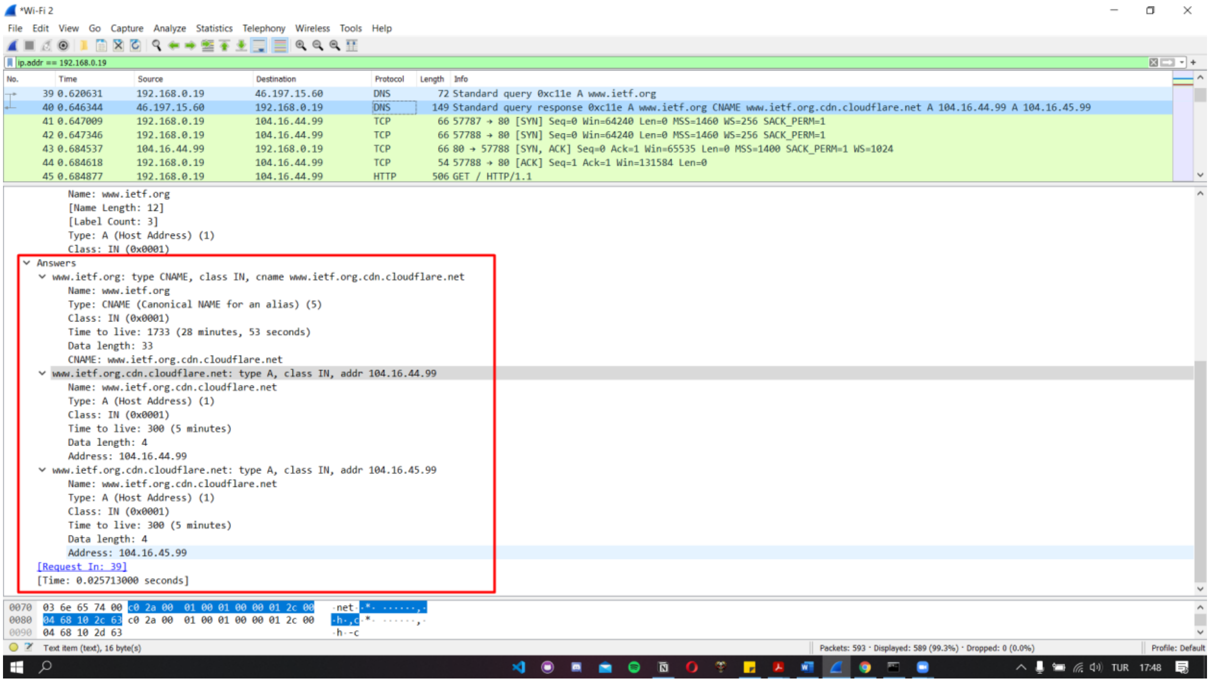
5) Destination port of the DNS query message: 53
   Source port of the DNS response message   : 53

6) Under the section name of “2.ipconfig”, ipconfig /all command has been used to list all information about my network connection. It can be seen there that my IP address of my local DNS service is 192.168.0.19. Also, in wireshark this IP address is used as a filter.

On the other hand, destination of the DNS query message sent is 192.168.0.19 Therefore, both my IP address and destination of DNS query message is the same.

7) As it can be observed in above image, under the “Queries” header, DNS query is indicated as: “Type: A (Host Address)”.

No, it does not contain any “answers”.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Text item (text), 16 byte(s)
Packets: 593 · Displayed: 589 (99.3%) · Dropped: 0 (0.0%)
Profile: Default
TUR
17:48

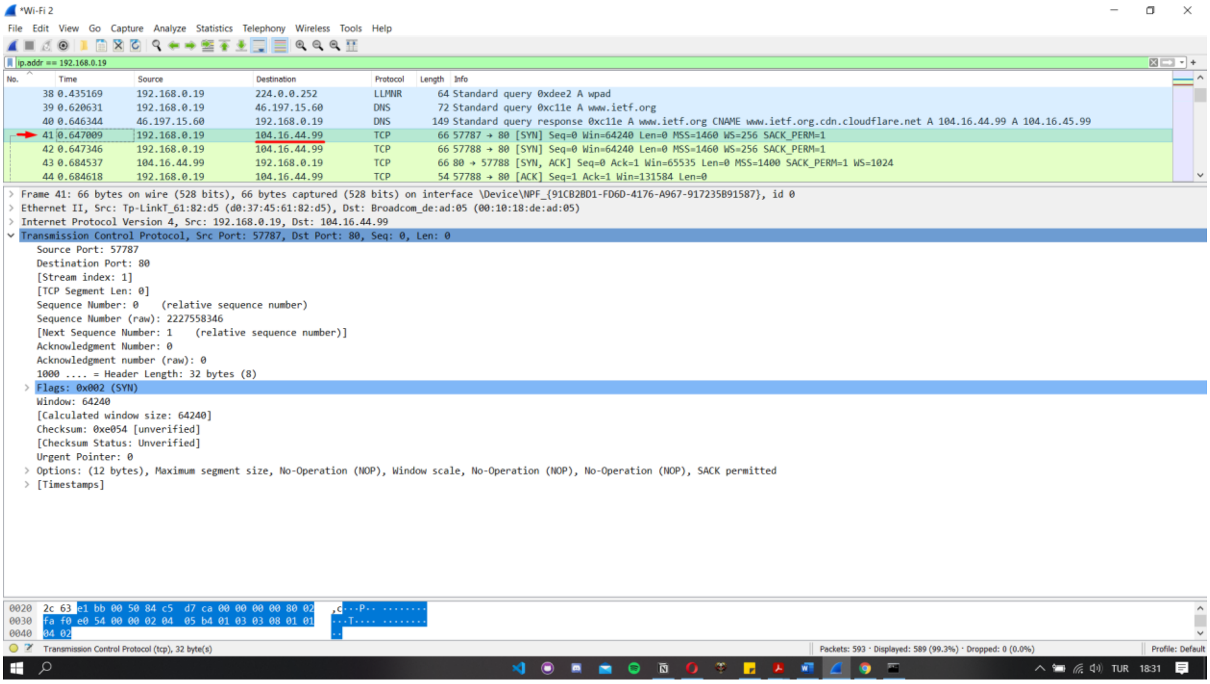
```
ip.addr == 192.168.0.19
```

```
No.   Time        Source          Destination     Protocol  Length  Info
   39 0.620631    192.168.0.19    46.197.15.60    DNS        72 Standard query 0xc11e A www.ietf.org
   40 0.646344    46.197.15.60    192.168.0.19    DNS       149 Standard query response 0xc11e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
   41 0.647009    192.168.0.19    104.16.44.99    TCP        66 57787 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   42 0.647346    192.168.0.19    104.16.44.99    TCP        66 57788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   43 0.684537    104.16.44.99    192.168.0.19    TCP        66 80 → 57788 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
   44 0.684618    192.168.0.19    104.16.44.99    TCP        54 57788 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
   45 0.684877    192.168.0.19    104.16.44.99    HTTP      506 GET / HTTP/1.1
```

```
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        Name: www.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1733 (28 minutes, 53 seconds)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.44.99
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.45.99
  [Request In: 39]
  [Time: 0.025713000 seconds]
```

```
0070  03 6e 65 74 00 c0 2a 00  01 00 01 00 00 01 2c 00   ·net··*· ······,·
0080  04 68 10 2c 63 c0 2a 00  01 00 01 00 00 01 2c 00   ·h·,c·*· ······,·
0090  04 68 10 2d 63                                     ·h·-c
```

8) At above image DNS response message is shown. There are 3 answers listed with 2 different types. First answer has type of “CNAME” and the remaining two has type of “A”. Each of them contains: Name, Type, Class, Time to live, Data length, Address (only for the type A) and CNAME (only for the type CNAME).


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Transmission Control Protocol (tcp), 32 byte(s)
Packets: 593 · Displayed: 589 (99.3%) · Dropped: 0 (0.0%)
Profile: Default
TUR
18:31

```
ip.addr == 192.168.0.19
```

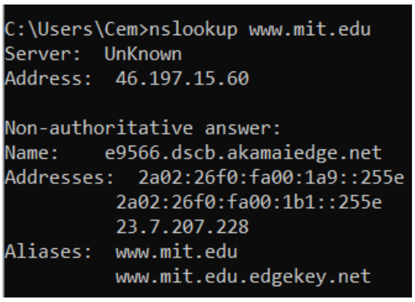
```
No.   Time        Source          Destination     Protocol  Length  Info
   38 0.435169    192.168.0.19    224.0.0.252     LLMNR      64 Standard query 0xdee2 A wpad
   39 0.620631    192.168.0.19    46.197.15.60    DNS        72 Standard query 0xc11e A www.ietf.org
   40 0.646344    46.197.15.60    192.168.0.19    DNS       149 Standard query response 0xc11e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
   41 0.647009    192.168.0.19    104.16.44.99    TCP        66 57787 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   42 0.647346    192.168.0.19    104.16.44.99    TCP        66 57788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   43 0.684537    104.16.44.99    192.168.0.19    TCP        66 80 → 57788 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
   44 0.684618    192.168.0.19    104.16.44.99    TCP        54 57788 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
```

```
> Frame 41: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 104.16.44.99
v Transmission Control Protocol, Src Port: 57787, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 57787
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2227558346
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0xe054 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

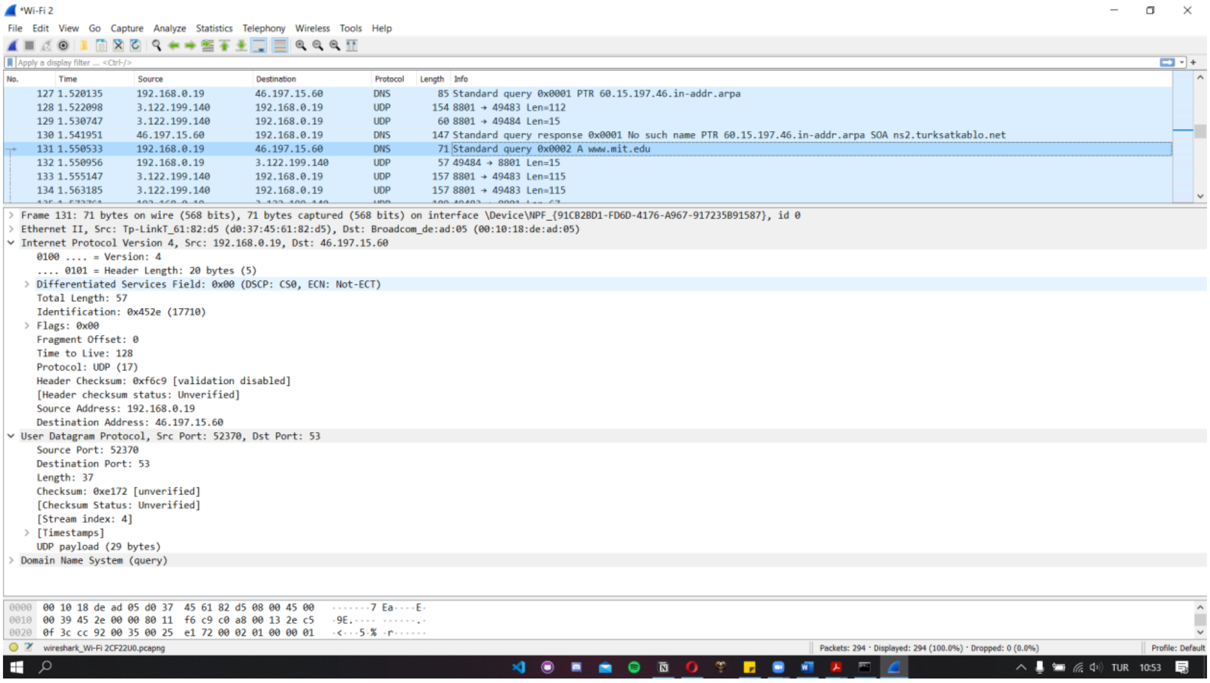
```
0020  2c 63 e1 bb 00 50 84 c5  d7 ca 00 00 00 00 80 02   ,c···P·· ········
0030  fa f0 e0 54 00 00 02 04  05 b4 01 03 03 08 01 01   ···T···· ········
0040  04 02                                              ··
```

9) As in the above image shown, considering the subsequent TCP SYN packets sent, the first SYN packet’s destination is 104.16.44.99 which is the same address with the 2nd answer listed in one previous image. There is only one corresponding matching.

10) Since all of the images contained by the web page, no additional DNS queries required.



```
C:\Users\Cem>nslookup www.mit.edu
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:fa00:1a9::255e
          2a02:26f0:fa00:1b1::255e
          23.7.207.228
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```



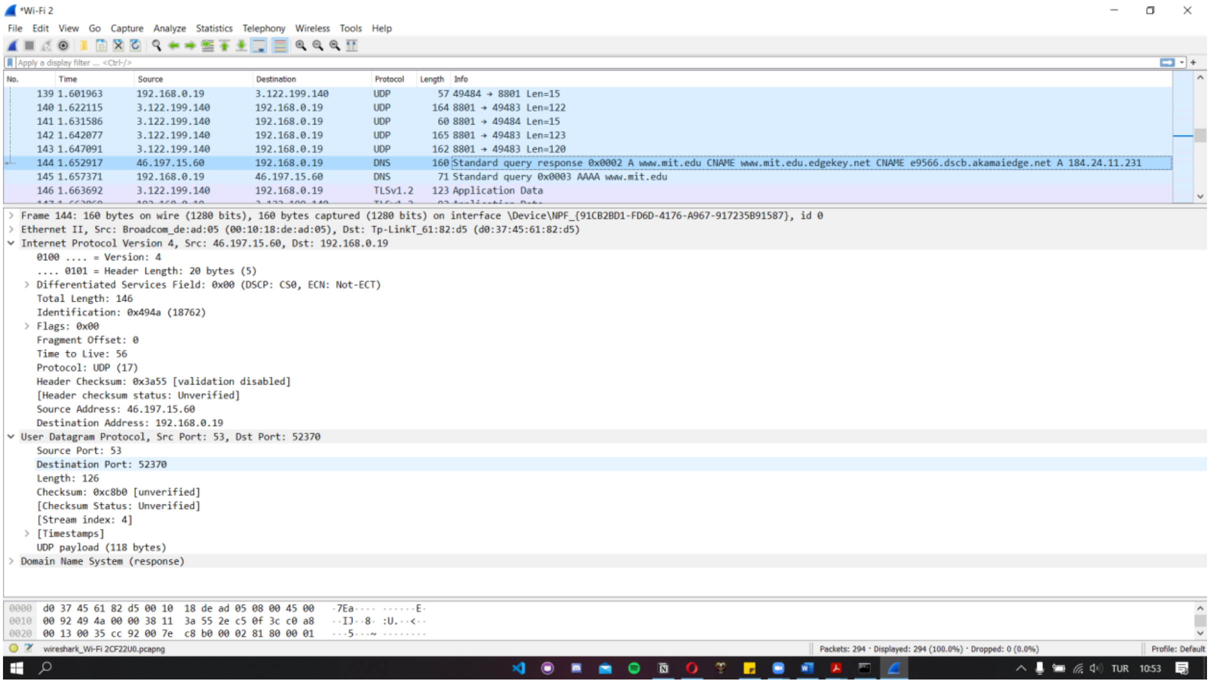
*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination     Protocol  Length  Info
 127 1.520135   192.168.0.19    46.197.15.60    DNS        85 Standard query 0x0001 PTR 60.15.197.46.in-addr.arpa
 128 1.522098   3.122.199.140   192.168.0.19    UDP       154 8801 → 49483 Len=112
 129 1.530747   3.122.199.140   192.168.0.19    UDP        60 8801 → 49484 Len=15
 130 1.541951   46.197.15.60    192.168.0.19    DNS       147 Standard query response 0x0001 No such name PTR 60.15.197.46.in-addr.arpa SOA ns2.turksatkablo.net
 131 1.550533   192.168.0.19    46.197.15.60    DNS        71 Standard query 0x0002 A www.mit.edu
 132 1.550956   192.168.0.19    3.122.199.140   UDP        57 49484 → 8801 Len=15
 133 1.555147   3.122.199.140   192.168.0.19    UDP       157 8801 → 49483 Len=115
 134 1.563185   3.122.199.140   192.168.0.19    UDP       157 8801 → 49483 Len=115
```

```
> Frame 131: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
v Internet Protocol Version 4, Src: 192.168.0.19, Dst: 46.197.15.60
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 57
    Identification: 0x452e (17710)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xf6c9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.19
    Destination Address: 46.197.15.60
v User Datagram Protocol, Src Port: 52370, Dst Port: 53
    Source Port: 52370
    Destination Port: 53
    Length: 37
    Checksum: 0xe172 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

```
0000  00 10 18 de ad 05 d0 37  45 61 82 d5 08 00 45 00   ·······7 Ea····E·
0010  00 39 45 2e 00 00 80 11  f6 c9 c0 a8 00 13 2e c5   ·9E.···· ·······.·
0020  0f 3c cc 92 00 35 00 25  e1 72 00 02 01 00 00 01   ·<···5·% ·r······
```

wireshark_Wi-Fi 2CF22U0.pcapng
Packets: 294 · Displayed: 294 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
TUR
10:53



*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

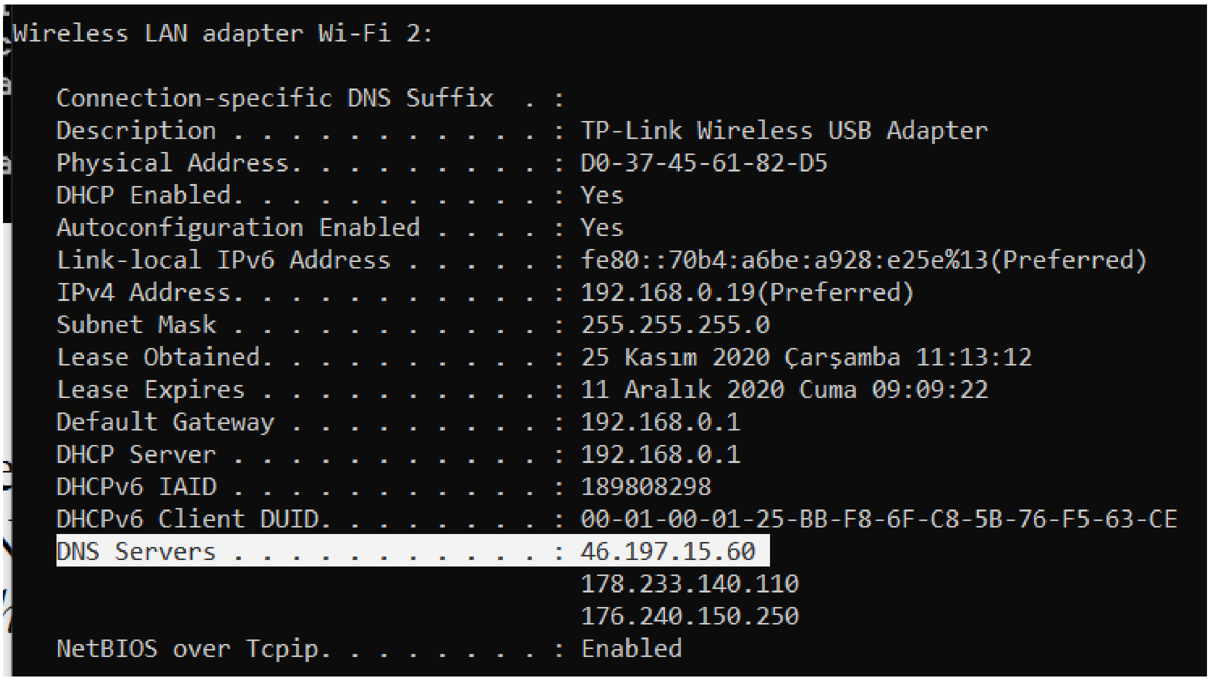
```
No.  Time       Source          Destination     Protocol  Length  Info
 139 1.601963   192.168.0.19    3.122.199.140   UDP        57 49484 → 8801 Len=15
 140 1.622115   3.122.199.140   192.168.0.19    UDP       164 8801 → 49483 Len=122
 141 1.631586   3.122.199.140   192.168.0.19    UDP        60 8801 → 49484 Len=15
 142 1.642077   3.122.199.140   192.168.0.19    UDP       165 8801 → 49483 Len=123
 143 1.647091   3.122.199.140   192.168.0.19    UDP       162 8801 → 49483 Len=120
 144 1.652917   46.197.15.60    192.168.0.19    DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.24.11.231
 145 1.657371   192.168.0.19    46.197.15.60    DNS        71 Standard query 0x0003 AAAA www.mit.edu
 146 1.663692   3.122.199.140   192.168.0.19    TLSv1.2   123 Application Data
```

```
> Frame 144: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Broadcom_de:ad:05 (00:10:18:de:ad:05), Dst: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5)
v Internet Protocol Version 4, Src: 46.197.15.60, Dst: 192.168.0.19
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 146
    Identification: 0x494a (18762)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 56
    Protocol: UDP (17)
    Header Checksum: 0x3a55 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 46.197.15.60
    Destination Address: 192.168.0.19
v User Datagram Protocol, Src Port: 53, Dst Port: 52370
    Source Port: 53
    Destination Port: 52370
    Length: 126
    Checksum: 0xc8b0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (118 bytes)
> Domain Name System (response)
```

```
0000  d0 37 45 61 82 d5 00 10  18 de ad 05 08 00 45 00   ·7Ea···· ······E·
0010  00 92 49 4a 00 00 38 11  3a 55 2e c5 0f 3c c0 a8   ··IJ··8· :U.··<··
0020  00 13 00 35 cc 92 00 7e  c8 b0 00 02 81 80 00 01   ···5···~ ········
```

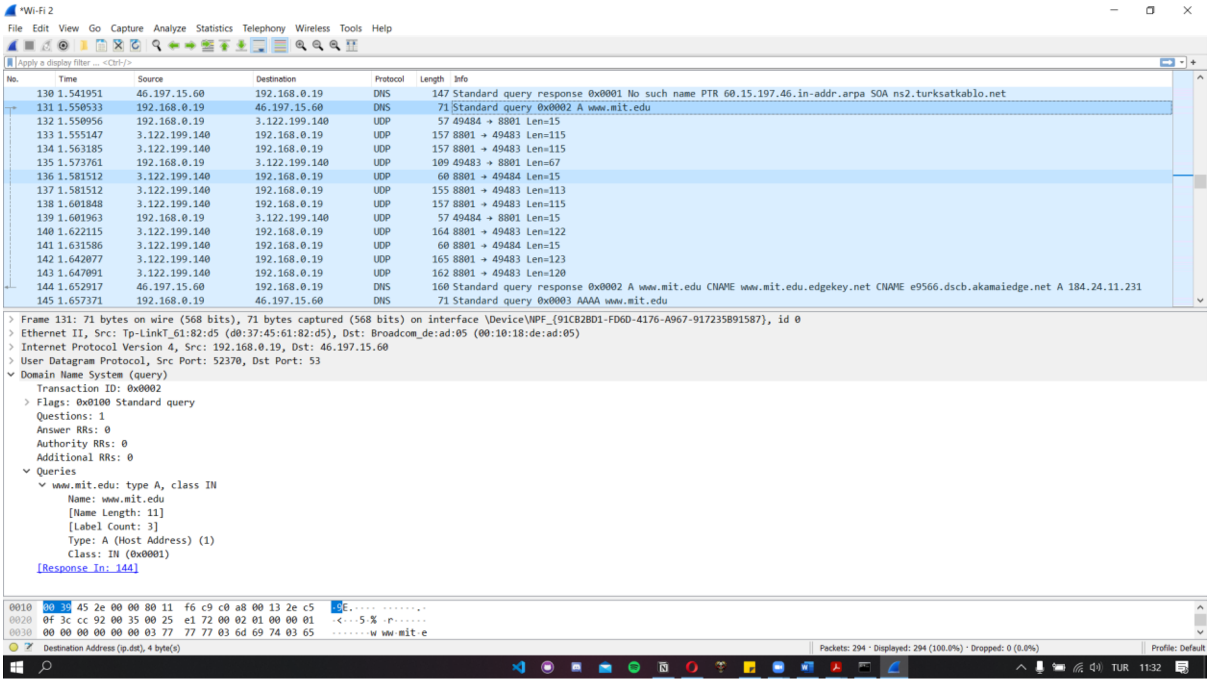
wireshark_Wi-Fi 2CF22U0.pcapng
Packets: 294 · Displayed: 294 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
TUR
10:53

11) At above two screenshots taken to show DNS query message and DNS response message respectively. Destination port of the DNS query message: 53
Source port of the DNS response message: 53



```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TP-Link Wireless USB Adapter
   Physical Address. . . . . . . . . : D0-37-45-61-82-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::70b4:a6be:a928:e25e%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.19(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 25 Kasım 2020 Çarşamba 11:13:12
   Lease Expires . . . . . . . . . . : 11 Aralık 2020 Cuma 09:09:22
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 189808298
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-BB-F8-6F-C8-5B-76-F5-63-CE
   DNS Servers . . . . . . . . . . . : 46.197.15.60
                                       178.233.140.110
                                       176.240.150.250
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

12) It was sent to IP address: 46.197.15.60. Yes, it matches with IP address of my local DNS server which is shown at above screenshot.

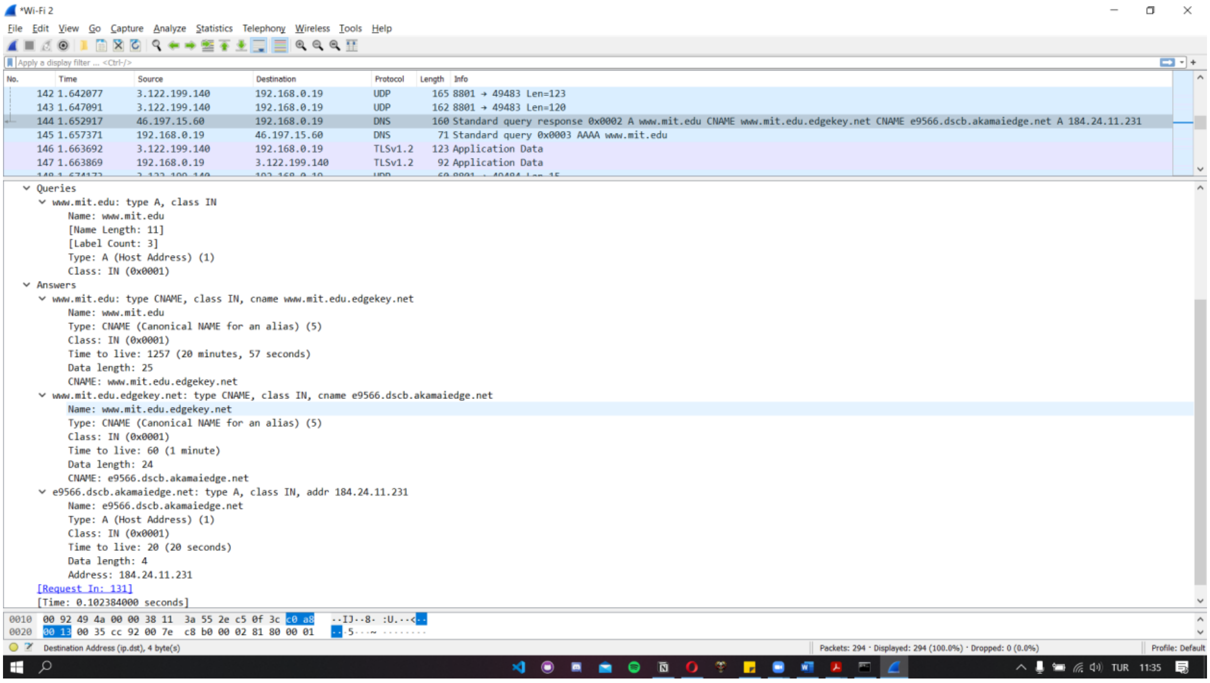


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source          Destination     Protocol Length Info
 130 1.541951  46.197.15.60    192.168.0.19    DNS       147 Standard query response 0x0001 No such name PTR 60.15.197.46.in-addr.arpa SOA ns2.turksatkablo.net
 131 1.550533  192.168.0.19    46.197.15.60    DNS        71 Standard query 0x0002 A www.mit.edu
 132 1.550956  192.168.0.19    3.122.199.140   UDP        57 49484 → 8801 Len=15
 133 1.555147  3.122.199.140   192.168.0.19    UDP       157 8801 → 49483 Len=115
 134 1.563185  3.122.199.140   192.168.0.19    UDP       157 8801 → 49483 Len=115
 135 1.573761  192.168.0.19    3.122.199.140   UDP       109 49483 → 8801 Len=67
 136 1.581512  3.122.199.140   192.168.0.19    UDP        60 8801 → 49484 Len=15
 137 1.581512  3.122.199.140   192.168.0.19    UDP       155 8801 → 49483 Len=113
 138 1.601848  3.122.199.140   192.168.0.19    UDP       157 8801 → 49483 Len=115
 139 1.601963  192.168.0.19    3.122.199.140   UDP        57 49484 → 8801 Len=15
 140 1.622115  3.122.199.140   192.168.0.19    UDP       164 8801 → 49483 Len=122
 141 1.631586  3.122.199.140   192.168.0.19    UDP        60 8801 → 49484 Len=15
 142 1.642077  3.122.199.140   192.168.0.19    UDP       165 8801 → 49483 Len=123
 143 1.647091  3.122.199.140   192.168.0.19    UDP       162 8801 → 49483 Len=120
 144 1.652917  46.197.15.60    192.168.0.19    DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.24.11.231
 145 1.657371  192.168.0.19    46.197.15.60    DNS        71 Standard query 0x0003 AAAA www.mit.edu

> Frame 131: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 46.197.15.60
> User Datagram Protocol, Src Port: 52370, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 144]

0010  00 39 45 2e 00 00 80 11  f6 c9 c0 a8 00 13 2e c5   ·9E.···· ·······.
0020  0f 3c cc 92 00 35 00 25  e1 72 00 02 01 00 00 01   ·<···5·% ·r······
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
```

Destination Address (ip.dst), 4 byte(s)
Packets: 294 · Displayed: 294 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
TUR
11:32

13) DNS query messages type is A. No, it does not contain any answers.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time      Source          Destination     Protocol Length Info
  142 1.642077   3.122.199.140   192.168.0.19    UDP       165 8801 → 49483 Len=123
  143 1.647091   3.122.199.140   192.168.0.19    UDP       162 8801 → 49483 Len=120
  144 1.652917   46.197.15.60    192.168.0.19    DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.24.11.231
  145 1.657371   192.168.0.19    46.197.15.60    DNS        71 Standard query 0x0003 AAAA www.mit.edu
  146 1.663692   3.122.199.140   192.168.0.19    TLSv1.2   123 Application Data
  147 1.663869   192.168.0.19    3.122.199.140   TLSv1.2    92 Application Data
```

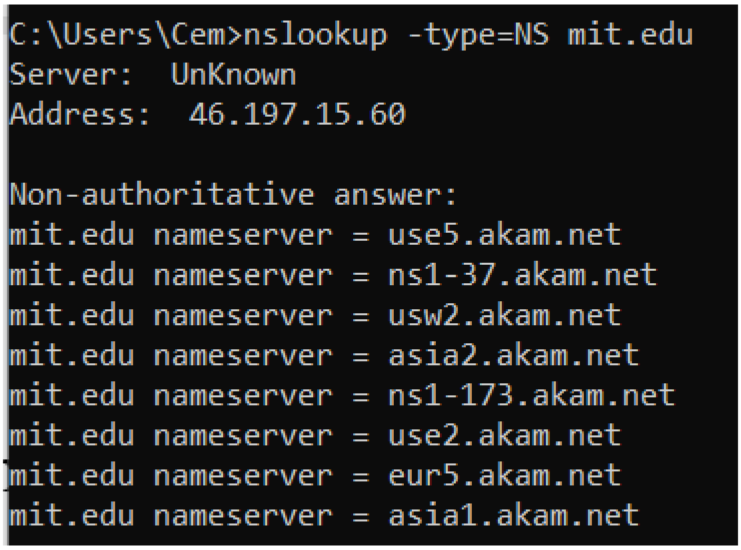
```
  Queries
    www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1257 (20 minutes, 57 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    e9566.dscb.akamaiedge.net: type A, class IN, addr 184.24.11.231
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 184.24.11.231
  [Request In: 131]
  [Time: 0.102384000 seconds]
```

```
0010  00 92 49 4a 00 00 38 11  3a 55 2e c5 0f 3c c0 a8   ··IJ··8· :U.··<··
0020  00 13 00 35 cc 92 00 7e  c8 b0 00 02 81 80 00 01   ··5···~ ········
```

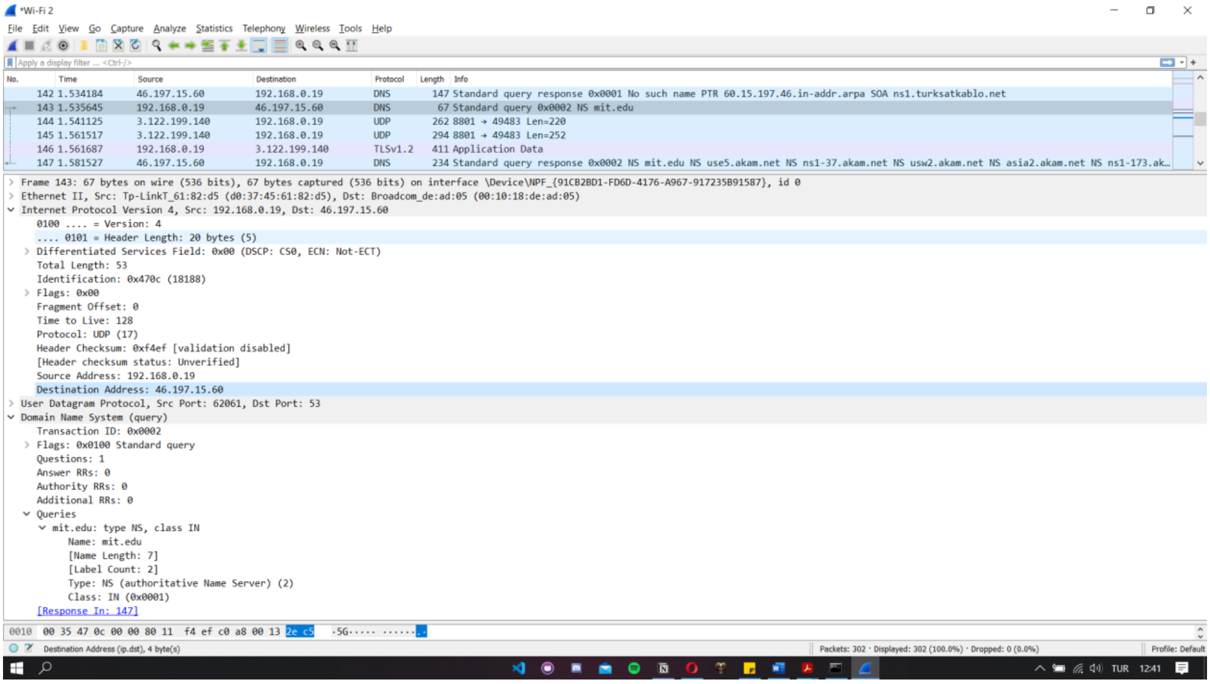
Destination Address (ip.dst), 4 byte(s)
Packets: 294 · Displayed: 294 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
TUR
11:35

14) At above image DNS response message is shown. There are 3 answers listed with 2 different types. First two answers has type of “CNAME” and the last one has type of “A”. Each of them contains: Name, Type, Class, Time to live, Data length, Address (only for the type A) and CNAME (only for the type CNAME).

15) Screenshots provided at above respectively in every question.



```
C:\Users\Cem>nslookup -type=NS mit.edu
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net
```



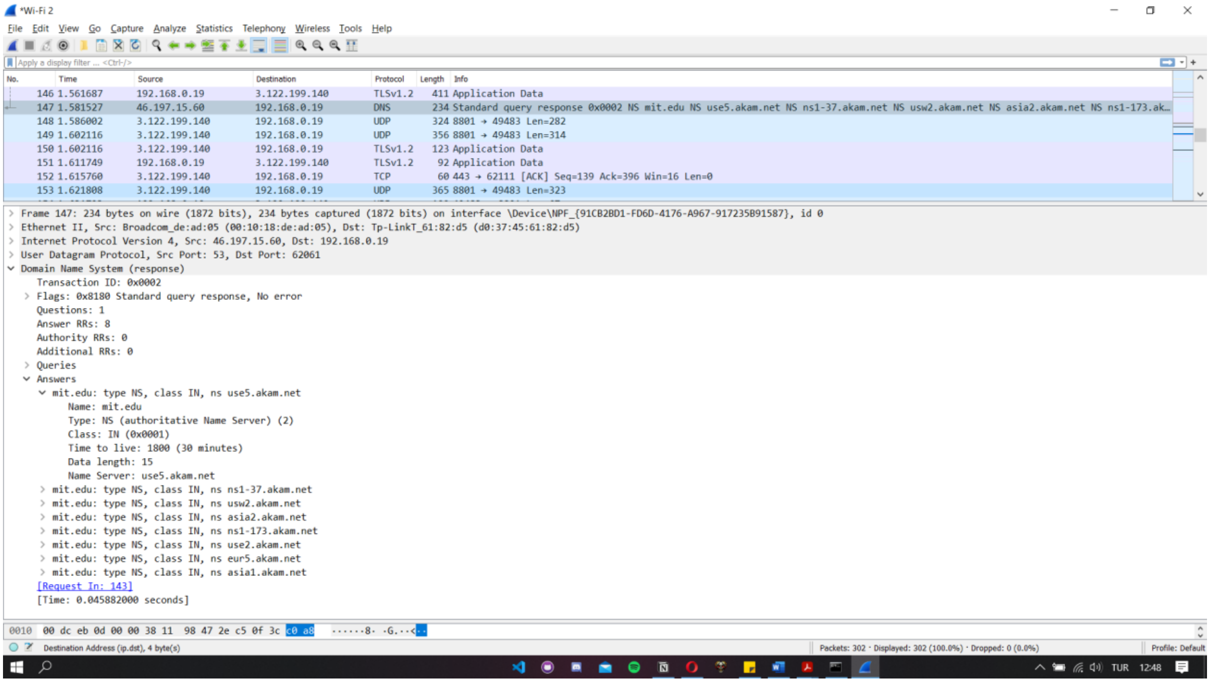
*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source          Destination     Protocol  Length Info
  142 1.534184   46.197.15.60    192.168.0.19    DNS        147 Standard query response 0x0001 No such name PTR 60.15.197.46.in-addr.arpa SOA ns1.turksatkablo.net
  143 1.535645   192.168.0.19    46.197.15.60    DNS         67 Standard query 0x0002 NS mit.edu
  144 1.541125   3.122.199.140   192.168.0.19    UDP        262 8801 → 49483 Len=220
  145 1.561517   3.122.199.140   192.168.0.19    UDP        294 8801 → 49483 Len=252
  146 1.561687   192.168.0.19    3.122.199.140   TLSv1.2    411 Application Data
  147 1.581527   46.197.15.60    192.168.0.19    DNS        234 Standard query response 0x0002 NS mit.edu NS use5.akam.net NS ns1-37.akam.net NS usw2.akam.net NS asia2.akam.net NS ns1-173.ak…

> Frame 143: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
v Internet Protocol Version 4, Src: 192.168.0.19, Dst: 46.197.15.60
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x470c (18188)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xf4ef [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.19
    Destination Address: 46.197.15.60
> User Datagram Protocol, Src Port: 62061, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 147]

0010  00 35 47 0c 00 00 80 11  f4 ef c0 a8 00 13 2e c5   ·5G····· ········
```

Destination Address (ip.dst), 4 byte(s)
Packets: 302 · Displayed: 302 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
TUR
12:41

16) It was sent to IP address: 46.197.15.60. Yes, again it is the same IP address of my default local DNS server.

17) As it is can be observed in above image, type of the DNS query message is NS.
No, it does not contain any answers.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time          Source            Destination       Protocol  Length Info
    146 1.561687      192.168.0.19      3.122.199.140     TLSv1.2   411 Application Data
    147 1.581527      46.197.15.60      192.168.0.19      DNS       234 Standard query response 0x0002 NS mit.edu NS use5.akam.net NS ns1-37.akam.net NS usw2.akam.net NS asia2.akam.net NS ns1-173.ak…
    148 1.586002      3.122.199.140     192.168.0.19      UDP       324 8801 → 49483 Len=282
    149 1.602116      3.122.199.140     192.168.0.19      UDP       356 8801 → 49483 Len=314
    150 1.602116      3.122.199.140     192.168.0.19      TLSv1.2   123 Application Data
    151 1.611749      192.168.0.19      3.122.199.140     TLSv1.2    92 Application Data
    152 1.615760      3.122.199.140     192.168.0.19      TCP        60 443 → 62111 [ACK] Seq=139 Ack=396 Win=16 Len=0
    153 1.621808      3.122.199.140     192.168.0.19      UDP       365 8801 → 49483 Len=323
```

```
> Frame 147: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Broadcom_de:ad:05 (00:10:18:de:ad:05), Dst: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5)
> Internet Protocol Version 4, Src: 46.197.15.60, Dst: 192.168.0.19
> User Datagram Protocol, Src Port: 53, Dst Port: 62061
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v mit.edu: type NS, class IN, ns use5.akam.net
          Name: mit.edu
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
          Time to live: 1800 (30 minutes)
          Data length: 15
          Name Server: use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    [Request In: 143]
    [Time: 0.045882000 seconds]

0010  00 dc eb 0d 00 00 38 11  98 47 2e c5 0f 3c c0 a8   ······8· ·G.··<··
```

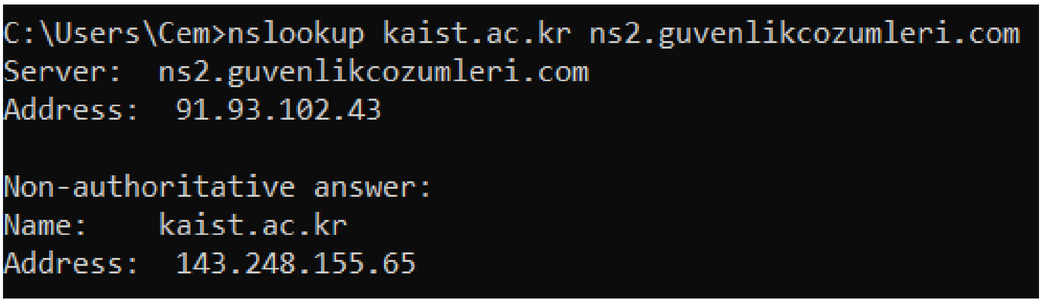
Destination Address (ip.dst), 4 byte(s)

Packets: 302 · Displayed: 302 (100.0%) · Dropped: 0 (0.0%)

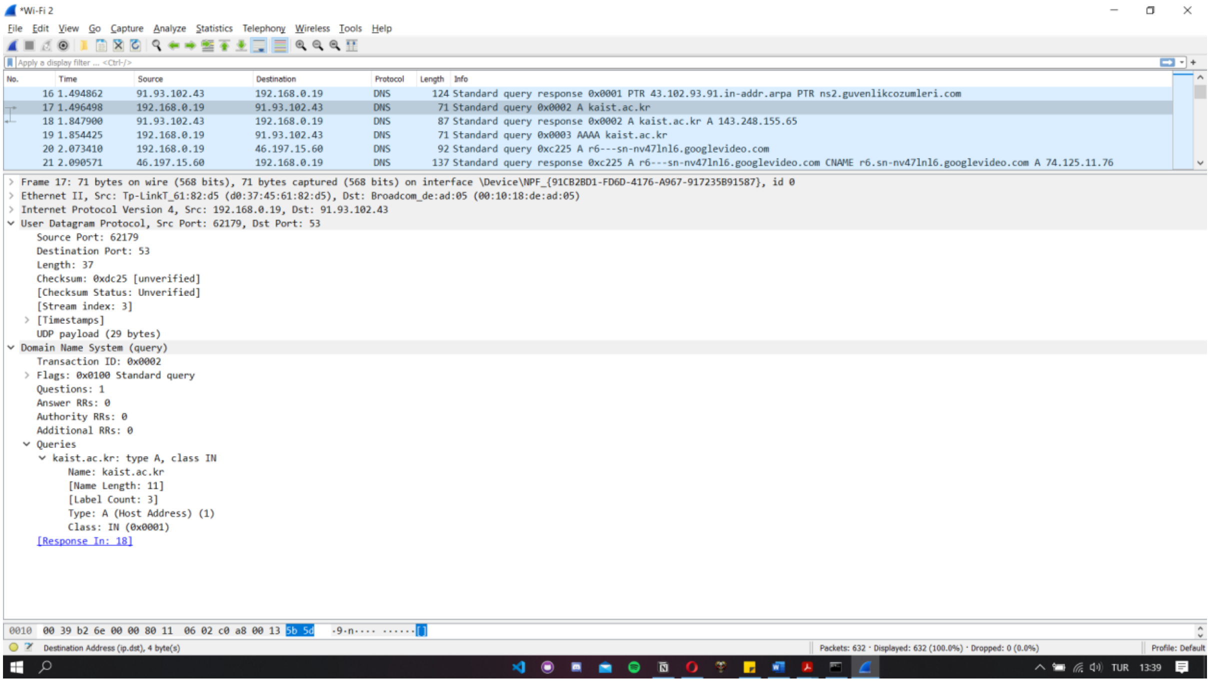
Profile: Default

18) Response message provides use5, ns1-37, usw2, asia2, ns1-173, use2, eur5 and asia1 MIT nameservers. No, response message does not provide the IP addresses of the MIT nameservers (in above image what nameservers contain is listed).

19) Screenshots provided at above respectively in every question.



```
C:\Users\Cem>nslookup kaist.ac.kr ns2.guvenlikcozumleri.com
Server:  ns2.guvenlikcozumleri.com
Address:  91.93.102.43

Non-authoritative answer:
Name:    kaist.ac.kr
Address:  143.248.155.65
```


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

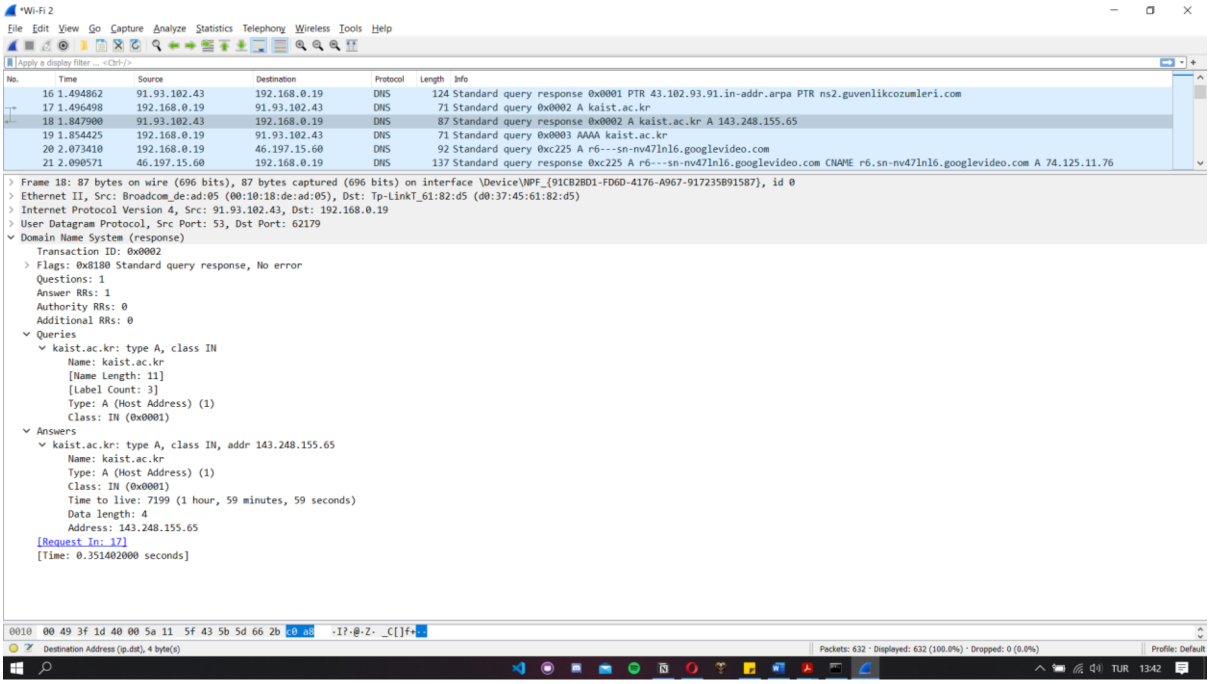
```
No.  Time       Source          Destination     Protocol Length Info
  16 1.494862   91.93.102.43    192.168.0.19    DNS       124 Standard query response 0x0001 PTR 43.102.93.91.in-addr.arpa PTR ns2.guvenlikcozumleri.com
  17 1.496498   192.168.0.19    91.93.102.43    DNS        71 Standard query 0x0002 A kaist.ac.kr
  18 1.847900   91.93.102.43    192.168.0.19    DNS        87 Standard query response 0x0002 A kaist.ac.kr A 143.248.155.65
  19 1.854425   192.168.0.19    91.93.102.43    DNS        71 Standard query 0x0003 AAAA kaist.ac.kr
  20 2.073410   192.168.0.19    46.197.15.60    DNS        92 Standard query 0xc225 A r6---sn-nv47ln16.googlevideo.com
  21 2.090571   46.197.15.60    192.168.0.19    DNS       137 Standard query response 0xc225 A r6---sn-nv47ln16.googlevideo.com CNAME r6.sn-nv47ln16.googlevideo.com A 74.125.11.76
```

```
> Frame 17: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 91.93.102.43
v User Datagram Protocol, Src Port: 62179, Dst Port: 53
    Source Port: 62179
    Destination Port: 53
    Length: 37
    Checksum: 0xdc25 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (29 bytes)
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v kaist.ac.kr: type A, class IN
        Name: kaist.ac.kr
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 18]

0010  00 39 b2 6e 00 00 80 11  06 02 c0 a8 00 13 5b 5d   ·9·n···· ······[]
```

Destination Address (ip.dst), 4 byte(s)
Packets: 632 · Displayed: 632 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
TUR
13:39

20) It was sent to IP address of 91.93.102.43. No, it is not my IP address of default local DNS server but the corresponding IP address of ns2.guvenlikcozumleri.com

21) Type of the DNS query message is type A as in the screenshot above.
No, it does not contain any answers.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination     Protocol Length Info
  16 1.494862   91.93.102.43    192.168.0.19    DNS       124 Standard query response 0x0001 PTR 43.102.93.91.in-addr.arpa PTR ns2.guvenlikcozumleri.com
  17 1.496498   192.168.0.19    91.93.102.43    DNS        71 Standard query 0x0002 A kaist.ac.kr
  18 1.847900   91.93.102.43    192.168.0.19    DNS        87 Standard query response 0x0002 A kaist.ac.kr A 143.248.155.65
  19 1.854425   192.168.0.19    91.93.102.43    DNS        71 Standard query 0x0003 AAAA kaist.ac.kr
  20 2.073410   192.168.0.19    46.197.15.60    DNS        92 Standard query 0xc225 A r6---sn-nv47ln16.googlevideo.com
  21 2.090571   46.197.15.60    192.168.0.19    DNS       137 Standard query response 0xc225 A r6---sn-nv47ln16.googlevideo.com CNAME r6.sn-nv47ln16.googlevideo.com A 74.125.11.76
```

```
> Frame 18: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{91CB2BD1-FD6D-4176-A967-917235B91587}, id 0
> Ethernet II, Src: Broadcom_de:ad:05 (00:10:18:de:ad:05), Dst: Tp-LinkT_61:82:d5 (d0:37:45:61:82:d5)
> Internet Protocol Version 4, Src: 91.93.102.43, Dst: 192.168.0.19
> User Datagram Protocol, Src Port: 53, Dst Port: 62179
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v kaist.ac.kr: type A, class IN
        Name: kaist.ac.kr
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v kaist.ac.kr: type A, class IN, addr 143.248.155.65
        Name: kaist.ac.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 7199 (1 hour, 59 minutes, 59 seconds)
        Data length: 4
        Address: 143.248.155.65
    [Request In: 17]
    [Time: 0.351402000 seconds]

0010  00 49 3f 1d 40 00 5a 11  5f 43 5b 5d 66 2b c0 a8   ·I?·@·Z· _C[]f+··
```

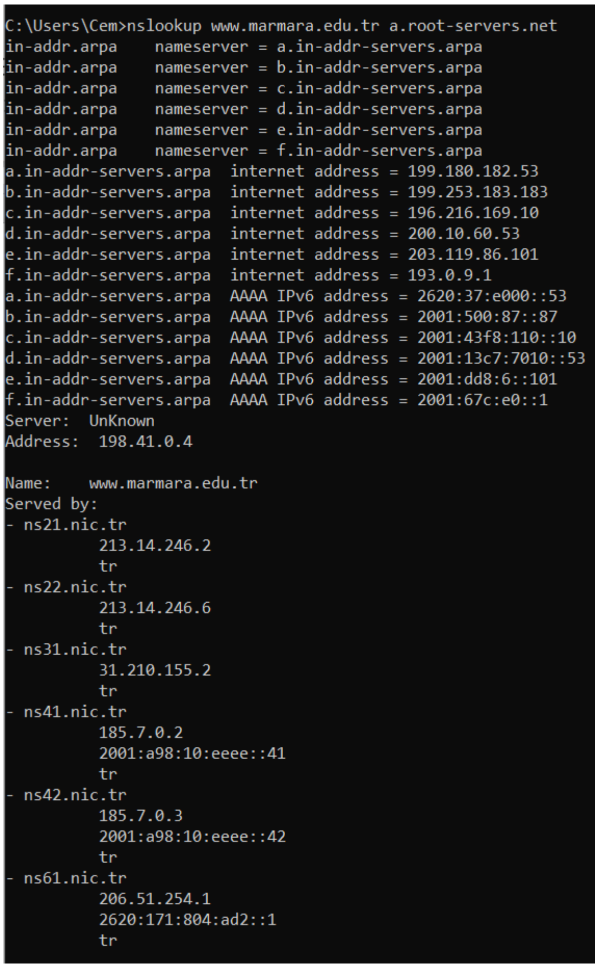
Destination Address (ip.dst), 4 byte(s)
Packets: 632 · Displayed: 632 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
TUR
13:42

22) Within the DNS response message only one answer is provided. As in the screenshot above its type is A and contains name, type, class, time to live, data length and address information within it.

23) Screenshots provided at above respectively in every question.

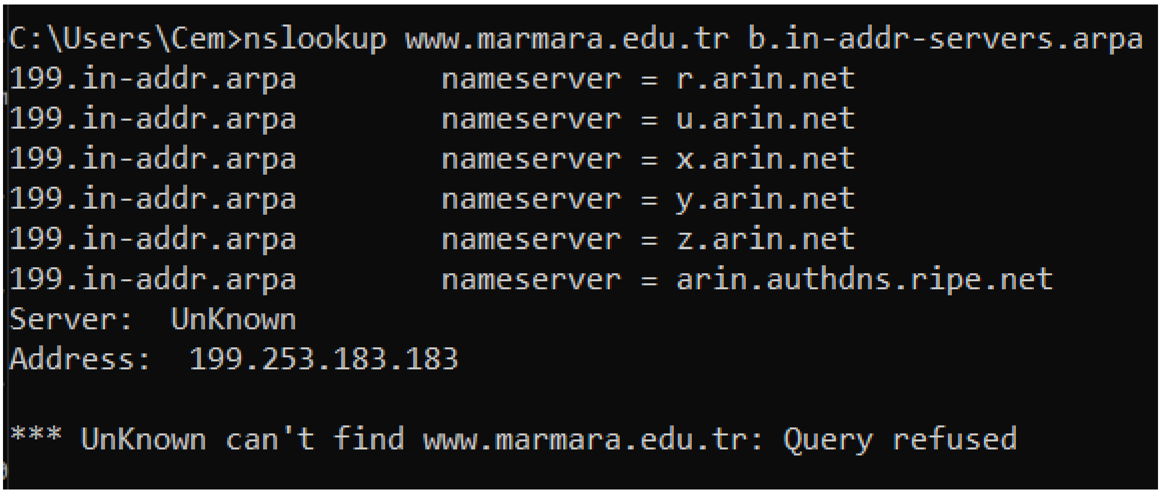
Extras - Exercise 1:

- As in the screenshot below, applying the first command TLD servers are listed.



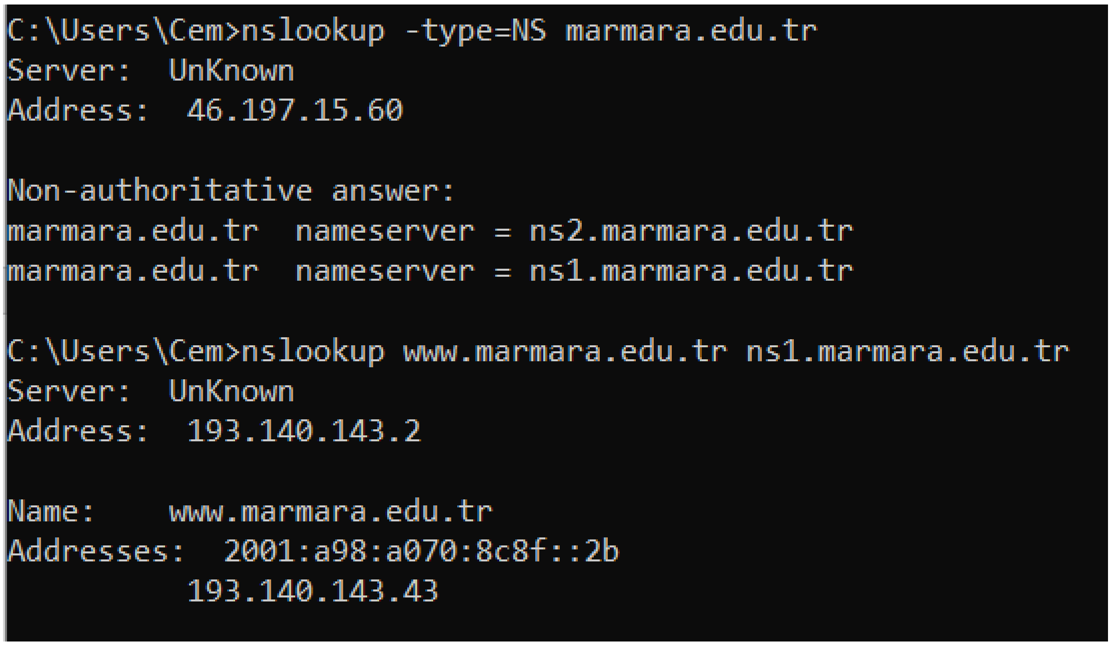
```
C:\Users\Cem>nslookup www.marmara.edu.tr a.root-servers.net
in-addr.arpa    nameserver = a.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = c.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = e.in-addr-servers.arpa
in-addr.arpa    nameserver = f.in-addr-servers.arpa
a.in-addr-servers.arpa  internet address = 199.180.182.53
b.in-addr-servers.arpa  internet address = 199.253.183.183
c.in-addr-servers.arpa  internet address = 196.216.169.10
d.in-addr-servers.arpa  internet address = 200.10.60.53
e.in-addr-servers.arpa  internet address = 203.119.86.101
f.in-addr-servers.arpa  internet address = 193.0.9.1
a.in-addr-servers.arpa  AAAA IPv6 address = 2620:37:e000::53
b.in-addr-servers.arpa  AAAA IPv6 address = 2001:500:87::87
c.in-addr-servers.arpa  AAAA IPv6 address = 2001:43f8:110::10
d.in-addr-servers.arpa  AAAA IPv6 address = 2001:13c7:7010::53
e.in-addr-servers.arpa  AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa  AAAA IPv6 address = 2001:67c:e0::1
Server:  UnKnown
Address:  198.41.0.4

Name:    www.marmara.edu.tr
Served by:
- ns21.nic.tr
          213.14.246.2
          tr
- ns22.nic.tr
          213.14.246.6
          tr
- ns31.nic.tr
          31.210.155.2
          tr
- ns41.nic.tr
          185.7.0.2
          2001:a98:10:eeee::41
          tr
- ns42.nic.tr
          185.7.0.3
          2001:a98:10:eeee::42
          tr
- ns61.nic.tr
          206.51.254.1
          2620:171:804:ad2::1
          tr
```

- Then same query is sent to one of the TLD servers. As in screenshot below, a list of authoritative DNS servers marmara.edu.tr are listed.



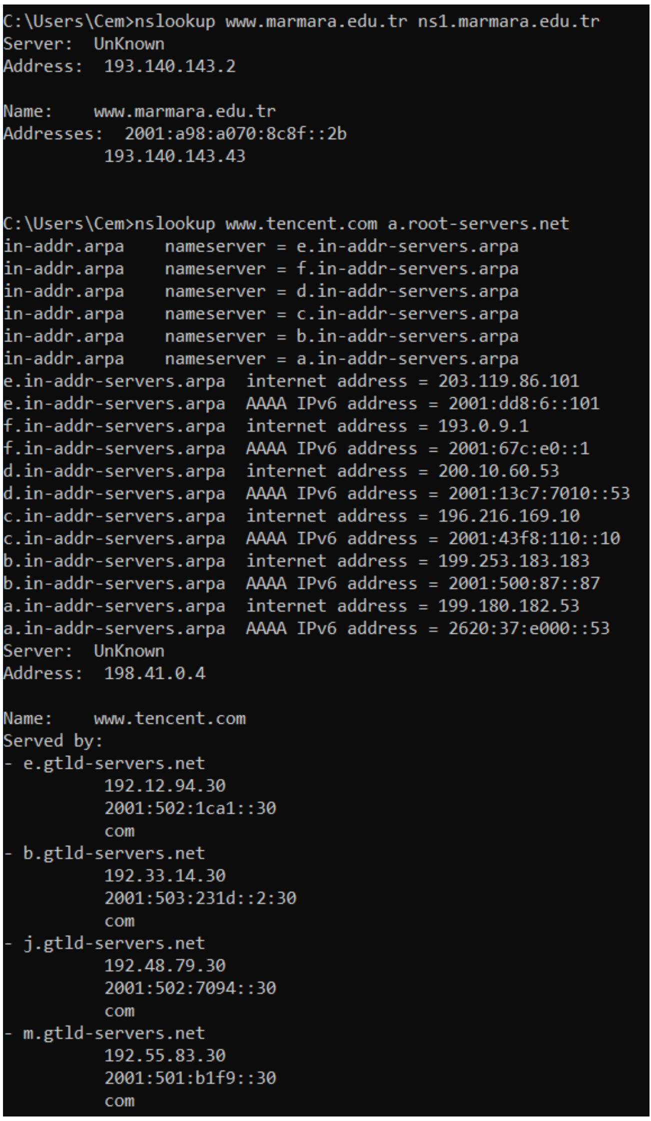
```
C:\Users\Cem>nslookup www.marmara.edu.tr b.in-addr-servers.arpa
199.in-addr.arpa        nameserver = r.arin.net
199.in-addr.arpa        nameserver = u.arin.net
199.in-addr.arpa        nameserver = x.arin.net
199.in-addr.arpa        nameserver = y.arin.net
199.in-addr.arpa        nameserver = z.arin.net
199.in-addr.arpa        nameserver = arin.authdns.ripe.net
Server:  UnKnown
Address:  199.253.183.183

*** UnKnown can't find www.marmara.edu.tr: Query refused
```

- Then same query is sent to an authoritative DNS server of marmara.edu.tr. As a result, IP address of www.marmara.edu.tr is received.

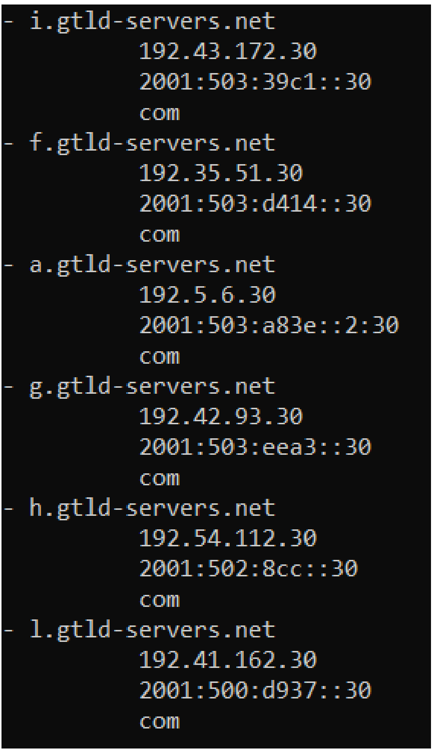


```
C:\Users\Cem>nslookup -type=NS marmara.edu.tr
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
marmara.edu.tr  nameserver = ns2.marmara.edu.tr
marmara.edu.tr  nameserver = ns1.marmara.edu.tr

C:\Users\Cem>nslookup www.marmara.edu.tr ns1.marmara.edu.tr
Server:  UnKnown
Address:  193.140.143.2

Name:    www.marmara.edu.tr
Addresses:  2001:a98:a070:8c8f::2b
          193.140.143.43
```

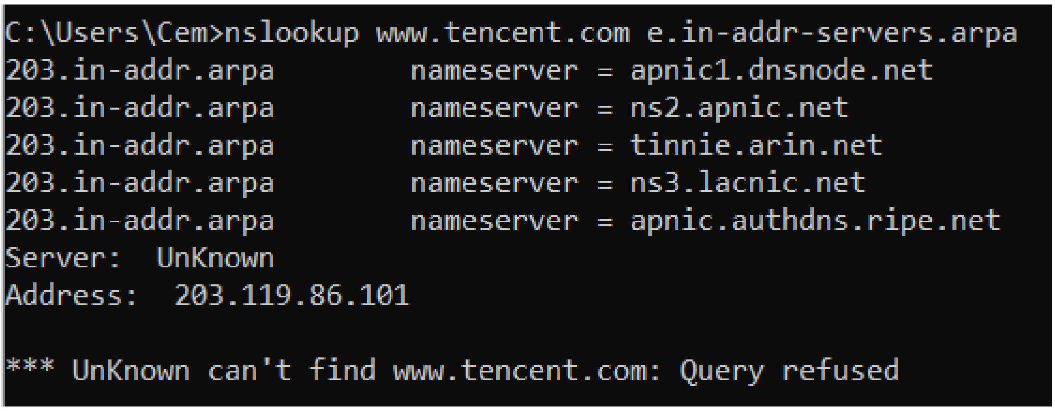
- Same procedure is repeated for an address in Asia region.
First of all, by the first command applied TLD servers are listed.
Secondly, sending the same query to one of the TLD servers, list of authoritative DNS servers of tencent.com is received.
Then finally, sending the same query to an authoritative DNS server of tencent.com, IP addresses of www.tencent.com are received.



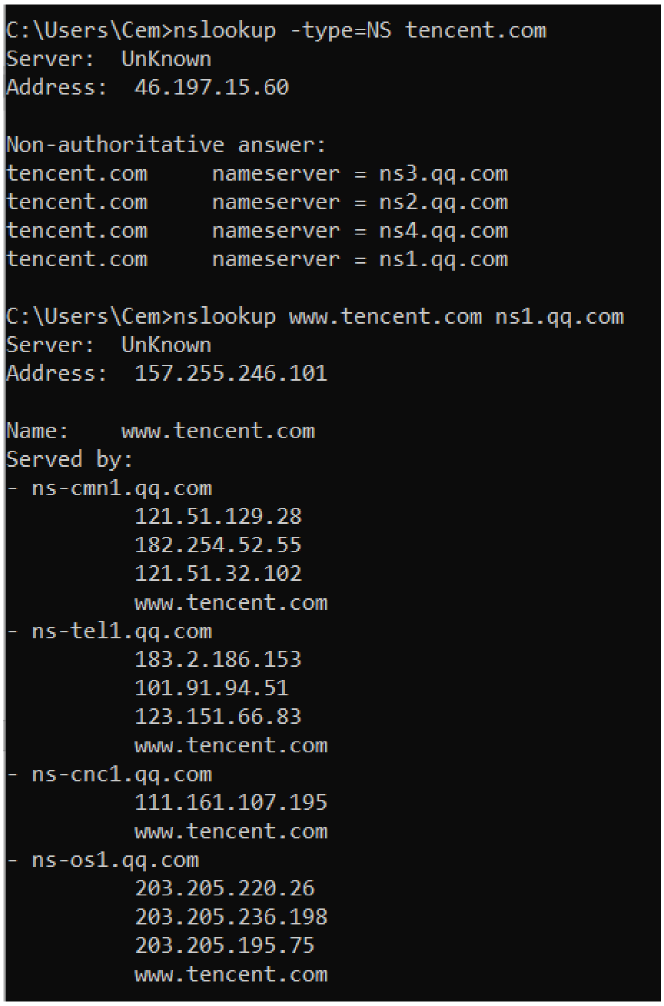
```
C:\Users\Cem>nslookup www.marmara.edu.tr ns1.marmara.edu.tr
Server:  UnKnown
Address:  193.140.143.2

Name:    www.marmara.edu.tr
Addresses:  2001:a98:a070:8c8f::2b
          193.140.143.43


C:\Users\Cem>nslookup www.tencent.com a.root-servers.net
in-addr.arpa    nameserver = e.in-addr-servers.arpa
in-addr.arpa    nameserver = f.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = c.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = a.in-addr-servers.arpa
e.in-addr-servers.arpa  internet address = 203.119.86.101
e.in-addr-servers.arpa  AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa  internet address = 193.0.9.1
f.in-addr-servers.arpa  AAAA IPv6 address = 2001:67c:e0::1
d.in-addr-servers.arpa  internet address = 200.10.60.53
d.in-addr-servers.arpa  AAAA IPv6 address = 2001:13c7:7010::53
c.in-addr-servers.arpa  internet address = 196.216.169.10
c.in-addr-servers.arpa  AAAA IPv6 address = 2001:43f8:110::10
b.in-addr-servers.arpa  internet address = 199.253.183.183
b.in-addr-servers.arpa  AAAA IPv6 address = 2001:500:87::87
a.in-addr-servers.arpa  internet address = 199.180.182.53
a.in-addr-servers.arpa  AAAA IPv6 address = 2620:37:e000::53
Server:  UnKnown
Address:  198.41.0.4

Name:    www.tencent.com
Served by:
- e.gtld-servers.net
          192.12.94.30
          2001:502:1ca1::30
          com
- b.gtld-servers.net
          192.33.14.30
          2001:503:231d::2:30
          com
- j.gtld-servers.net
          192.48.79.30
          2001:502:7094::30
          com
- m.gtld-servers.net
          192.55.83.30
          2001:501:b1f9::30
          com
```



```
- i.gtld-servers.net
          192.43.172.30
          2001:503:39c1::30
          com
- f.gtld-servers.net
          192.35.51.30
          2001:503:d414::30
          com
- a.gtld-servers.net
          192.5.6.30
          2001:503:a83e::2:30
          com
- g.gtld-servers.net
          192.42.93.30
          2001:503:eea3::30
          com
- h.gtld-servers.net
          192.54.112.30
          2001:502:8cc::30
          com
- l.gtld-servers.net
          192.41.162.30
          2001:500:d937::30
          com
```



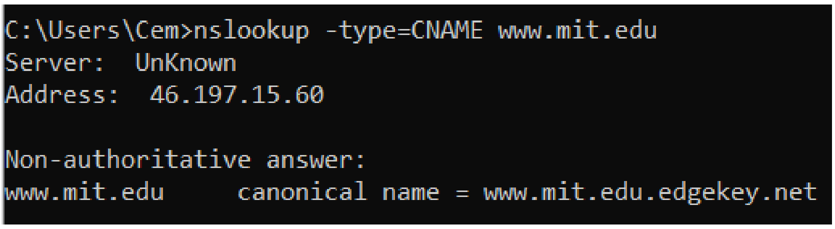
```
C:\Users\Cem>nslookup www.tencent.com e.in-addr-servers.arpa
203.in-addr.arpa        nameserver = apnic1.dnsnode.net
203.in-addr.arpa        nameserver = ns2.apnic.net
203.in-addr.arpa        nameserver = tinnie.arin.net
203.in-addr.arpa        nameserver = ns3.lacnic.net
203.in-addr.arpa        nameserver = apnic.authdns.ripe.net
Server:  UnKnown
Address:  203.119.86.101

*** UnKnown can't find www.tencent.com: Query refused
```



```
C:\Users\Cem>nslookup -type=NS tencent.com
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
tencent.com     nameserver = ns3.qq.com
tencent.com     nameserver = ns2.qq.com
tencent.com     nameserver = ns4.qq.com
tencent.com     nameserver = ns1.qq.com

C:\Users\Cem>nslookup www.tencent.com ns1.qq.com
Server:  UnKnown
Address:  157.255.246.101

Name:    www.tencent.com
Served by:
- ns-cmn1.qq.com
          121.51.129.28
          182.254.52.55
          121.51.32.102
          www.tencent.com
- ns-tel1.qq.com
          183.2.186.153
          101.91.94.51
          123.151.66.83
          www.tencent.com
- ns-cnc1.qq.com
          111.161.107.195
          www.tencent.com
- ns-os1.qq.com
          203.205.220.26
          203.205.236.198
          203.205.195.75
          www.tencent.com
```

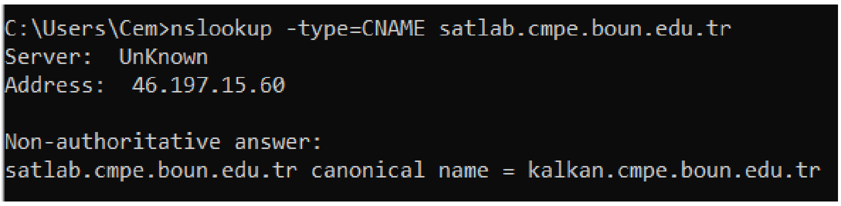
Extras - Exercise 2:

- By sending query to type “CNAME” in the screenshot below, canonical name of www.mit.edu is received.



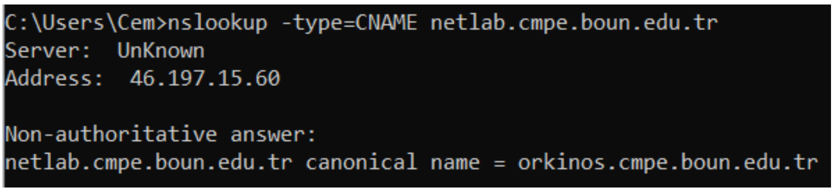
```
C:\Users\Cem>nslookup -type=CNAME www.mit.edu
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net
```

- Same procedure is applied for the type “CNAME”, for the satlab.cmpe.boun.edu.tr



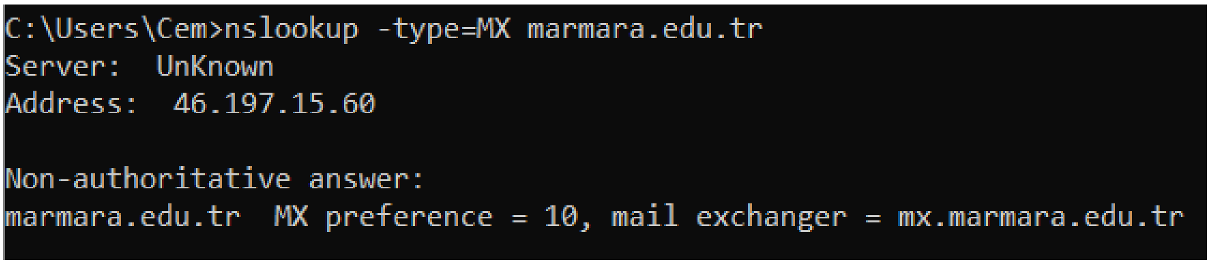
```
C:\Users\Cem>nslookup -type=CNAME satlab.cmpe.boun.edu.tr
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
satlab.cmpe.boun.edu.tr canonical name = kalkan.cmpe.boun.edu.tr
```

- Same procedure is applied for the type “CNAME”, for the netlab.cmpe.boun.edu.tr

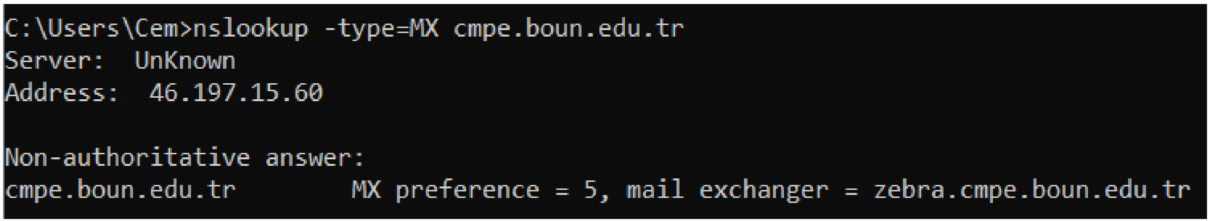


```
C:\Users\Cem>nslookup -type=CNAME netlab.cmpe.boun.edu.tr
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
netlab.cmpe.boun.edu.tr canonical name = orkinos.cmpe.boun.edu.tr
```

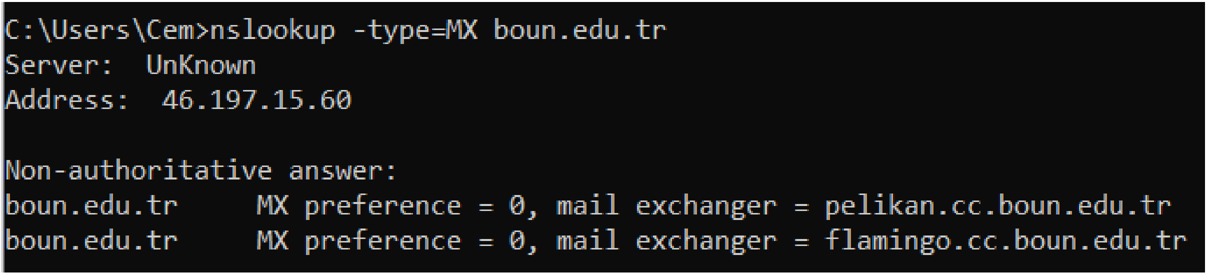
- Below, queries sent to 3 different addresses in order to receive their name of the mail server (mail exchanger).



```
C:\Users\Cem>nslookup -type=MX marmara.edu.tr
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
marmara.edu.tr  MX preference = 10, mail exchanger = mx.marmara.edu.tr
```



```
C:\Users\Cem>nslookup -type=MX cmpe.boun.edu.tr
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
cmpe.boun.edu.tr        MX preference = 5, mail exchanger = zebra.cmpe.boun.edu.tr
```



```
C:\Users\Cem>nslookup -type=MX boun.edu.tr
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
boun.edu.tr     MX preference = 0, mail exchanger = pelikan.cc.boun.edu.tr
boun.edu.tr     MX preference = 0, mail exchanger = flamingo.cc.boun.edu.tr
```