MARMARA UNIVERSITY

FACULTY OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING DEPARTMENT

CSE4074
COMPUTER NETWORKS
Homework #2

A. Tunahan Cinsoy
150117062

1.nslookup

Q1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

```
C:\Users\dell>nslookup www.hiroshima-u.ac.jp
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    v.ssl.global.fastly.net
Address:  151.101.113.128
Aliases:  www.hiroshima-u.ac.jp


C:\Users\dell>
```

I've queried the webpage of Hiroshima University located in Japan. The IP address of that server is 151.101.113.128

Q2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

```
C:\Users\dell>nslookup -type=NS www.lazarski.pl
Server:  UnKnown
Address:  192.168.1.1

lazarski.pl
        primary name server = ns1.domena.pl
        responsible mail addr = hosting.agnat.pl
        serial  = 2015066203
        refresh = 43200 (12 hours)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)
```

I've used the webpage of Lazarski University located in Poland. The authoritative DNS server is ns1.domena.pl

Q3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

```
C:\Users\dell>nslookup www.lazarski.pl 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
```

The IP address is 87.248.118.23 if we query ww.lazarski.pl for the mail server of Yahoo! mail

2. ipconfig

ipconfig /all

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : TunaCinsoy
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : home

Wireless LAN adapter Yerel Ağ Bağlantısı* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 34-F6-4B-F1-DE-C1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Yerel Ağ Bağlantısı* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 36-F6-4B-F1-DE-C0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 50-9A-4C-BF-27-89
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::3c09:528e:d646:e8a3%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.33(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 29 Kasım 2020 Pazar 19:53:19
   Lease Expires . . . . . . . . . . : 30 Kasım 2020 Pazartesi 19:53:18
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 206608972
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-53-65-61-50-9A-4C-BF-27-89
   DNS Servers . . . . . . . . . . . : 192.168.1.1
                                       192.168.1.1
```

ipconfig /displaydns

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

Windows IP Configuration

    play.google.com
    ----------------------------------------
    Record Name . . . . . : play.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 110
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 216.58.206.206


    s0.wp.com
    ----------------------------------------
    Record Name . . . . . : s0.wp.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 10803
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.0.77.32


    relay-5c15c79b.net.anydesk.com
    ----------------------------------------
    Record Name . . . . . : relay-5c15c79b.net.anydesk.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 4657
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 51.178.65.230


    roaming.officeapps.live.com
    ----------------------------------------
    Record Name . . . . . : roaming.officeapps.live.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 131
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : prod.roaming1.live.com.akadns.net


    Record Name . . . . . : prod.roaming1.live.com.akadns.net
    Record Type . . . . . : 5
    Time To Live  . . . . : 131
```

ipconfig /flushdns

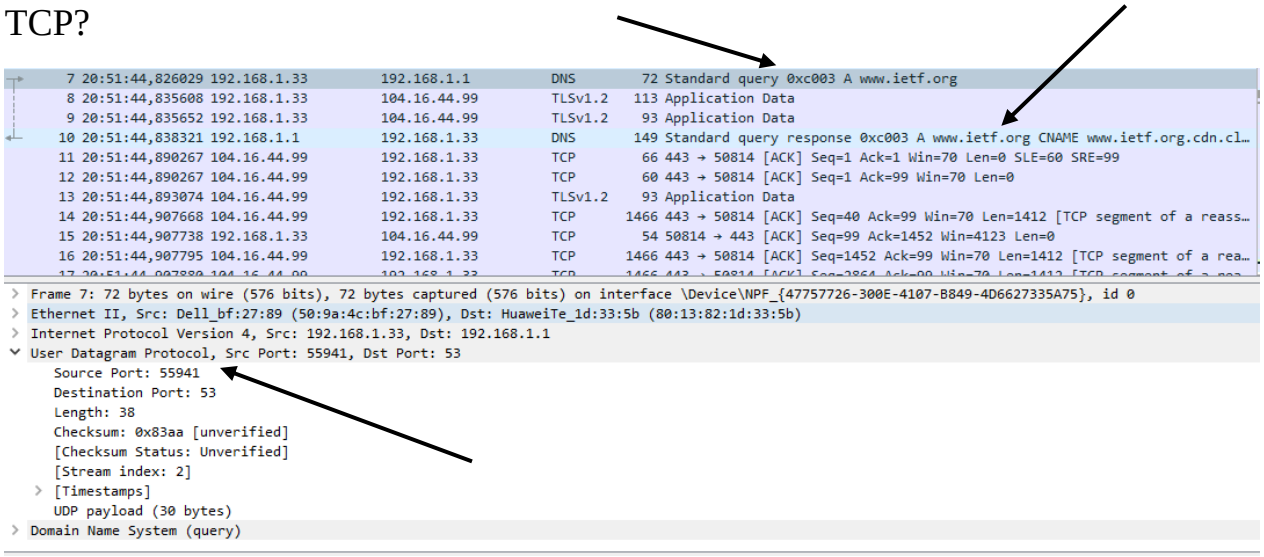
```
C:\Users\dell>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

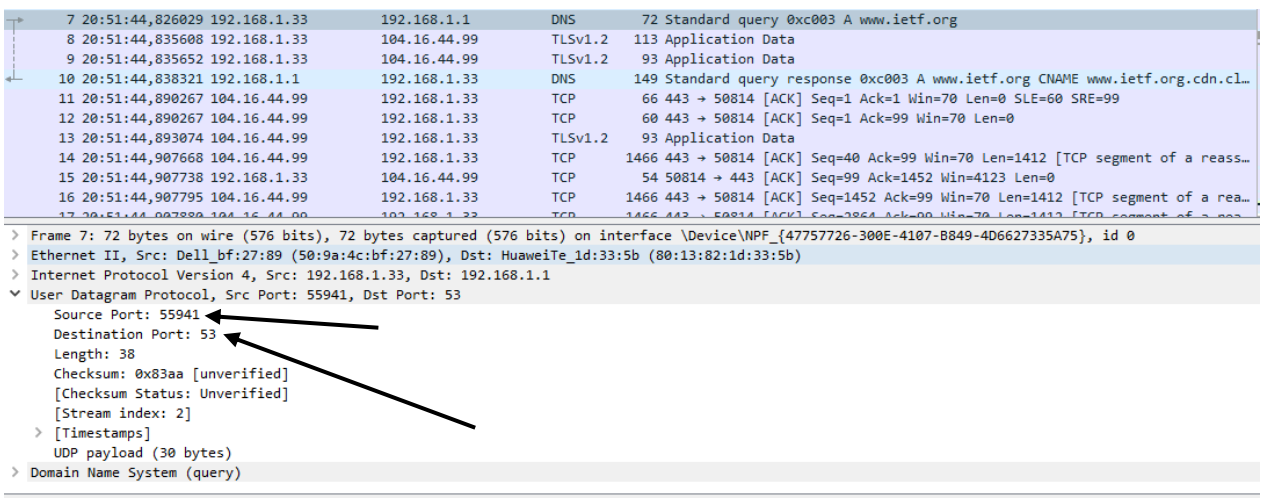
3. Tracing DNS with Wireshark

Q4. Locate the DNS query and response messages. Are then sent over UDP or TCP?



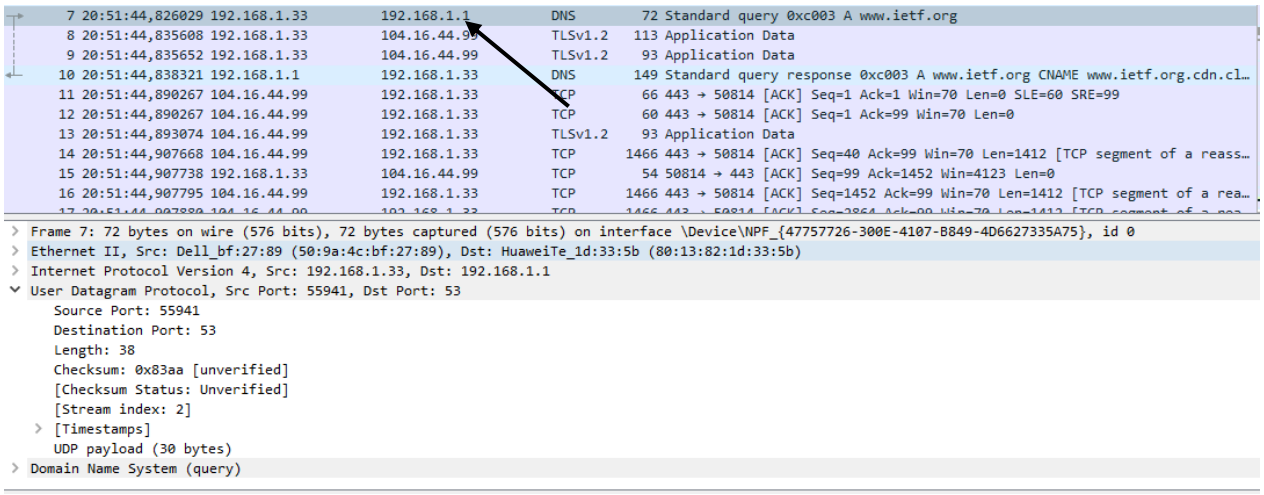
DNS query and response messages are sent over UDP.

Q5. What is the destination port for the DNS query message? What is the source port of DNS response message?



Destination port for the DNS query message is 53. Source port of DNS response message is 55941

Q6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?



7	20:51:44,826029	192.168.1.33	192.168.1.1	DNS	72	Standard query 0xc003 A www.ietf.org
8	20:51:44,835608	192.168.1.33	104.16.44.99	TLSv1.2	113	Application Data
9	20:51:44,835652	192.168.1.33	104.16.44.99	TLSv1.2	93	Application Data
10	20:51:44,838321	192.168.1.1	192.168.1.33	DNS	149	Standard query response 0xc003 A www.ietf.org CNAME www.ietf.org.cdn.cl…
11	20:51:44,890267	104.16.44.99	192.168.1.33	TCP	66	443 → 50814 [ACK] Seq=1 Ack=1 Win=70 Len=0 SLE=60 SRE=99
12	20:51:44,890267	104.16.44.99	192.168.1.33	TCP	60	443 → 50814 [ACK] Seq=1 Ack=99 Win=70 Len=0
13	20:51:44,893074	104.16.44.99	192.168.1.33	TLSv1.2	93	Application Data
14	20:51:44,907668	104.16.44.99	192.168.1.33	TCP	1466	443 → 50814 [ACK] Seq=40 Ack=99 Win=70 Len=1412 [TCP segment of a reass…
15	20:51:44,907738	192.168.1.33	104.16.44.99	TCP	54	50814 → 443 [ACK] Seq=99 Ack=1452 Win=4123 Len=0
16	20:51:44,907795	104.16.44.99	192.168.1.33	TCP	1466	443 → 50814 [ACK] Seq=1452 Ack=99 Win=70 Len=1412 [TCP segment of a rea…

```
> Frame 7: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{47757726-300E-4107-B849-4D6627335A75}, id 0
> Ethernet II, Src: Dell_bf:27:89 (50:9a:4c:bf:27:89), Dst: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b)
> Internet Protocol Version 4, Src: 192.168.1.33, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 55941, Dst Port: 53
    Source Port: 55941
    Destination Port: 53
    Length: 38
    Checksum: 0x83aa [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

```
C:\Users\dell>ipconfig

Windows IP Configuration


Wireless LAN adapter Yerel Ağ Bağlantısı* 1:

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

Wireless LAN adapter Yerel Ağ Bağlantısı* 2:

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

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::3c09:528e:d646:e8a3%7
   IPv4 Address. . . . . . . . . . . : 192.168.1.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Wireless LAN adapter Wi-Fi:

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

The IP address of the DNS query message sent is 192.168.1.1

Yes, they are same.

Q7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
    Destination Port: 53
    Length: 38
    Checksum: 0x83aa [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (30 bytes)
v Domain Name System (query)
    Transaction ID: 0xc003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 10]
```

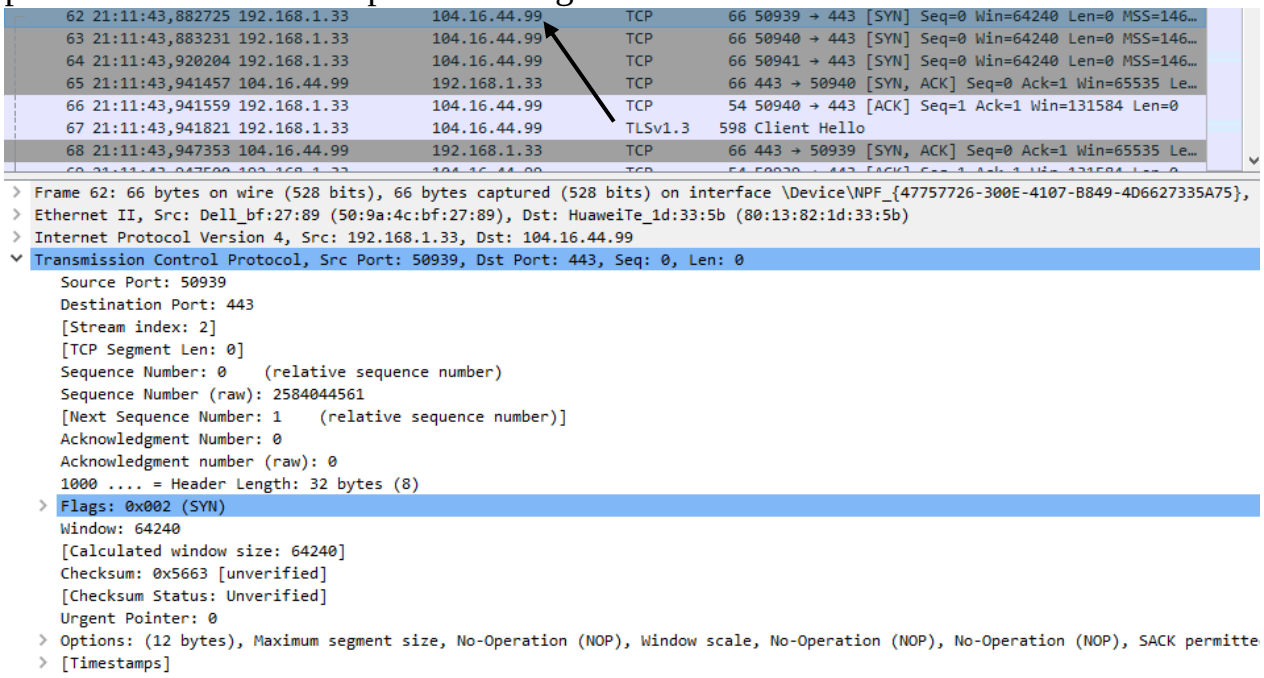
DNS query is type A. Query message does not contain any answer.

Q8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

```
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v 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: 1800 (30 minutes)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    v 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
    v 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: 30]
    [Time: 0.484808000 seconds]
```

3 answers are provided. Each of them contain canonical name, host address and host address respectively.

Q9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?



The subsequent destination IP address of the SYN packet is 104.16.44.99 which is the same address of Type A DNS response message.

Q10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

192.168.1.33	192.168.1.1	DNS	72	Standard query 0xc785 A www.ietf.org
192.168.1.33	192.168.1.255	UDP	305	54915 → 54915 Len=263
192.168.1.33	172.217.169.174	QUIC	1392	Initial, DCID=5acf252f2a09e937, PKN: 1, CRYPTO, PADDING
172.217.169.174	192.168.1.33	QUIC	1392	Initial, SCID=5acf252f2a09e937, PKN: 1, ACK, PADDING
192.168.1.33	172.217.169.174	TCP	66	50996 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.33	192.168.1.1	DNS	72	Standard query 0xc785 A www.ietf.org
172.217.169.174	192.168.1.33	TCP	66	443 → 50996 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 WS=256
192.168.1.33	172.217.169.174	TCP	54	50996 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
192.168.1.33	172.217.169.174	TLSv1.3	643	Client Hello
172.217.169.174	192.168.1.33	QUIC	1392	Initial, SCID=5acf252f2a09e937, PKN: 2, CRYPTO, PADDING
172.217.169.174	192.168.1.33	QUIC	280	Handshake, SCID=5acf252f2a09e937
172.217.169.174	192.168.1.33	QUIC	103	Protected Payload (KP0)
192.168.1.33	172.217.169.174	QUIC	1392	Protected Payload (KP0), DCID=5acf252f2a09e937
192.168.1.33	172.217.169.174	QUIC	736	Protected Payload (KP0), DCID=5acf252f2a09e937
172.217.169.174	192.168.1.33	TCP	60	443 → 50996 [ACK] Seq=1 Ack=590 Win=66816 Len=0
172.217.169.174	192.168.1.33	QUIC	71	Protected Payload (KP0)
192.168.1.33	172.217.169.174	QUIC	76	Protected Payload (KP0), DCID=5acf252f2a09e937
172.217.169.174	192.168.1.33	QUIC	654	Protected Payload (KP0)
172.217.169.174	192.168.1.33	QUIC	67	Protected Payload (KP0)
192.168.1.33	172.217.169.174	QUIC	76	Protected Payload (KP0), DCID=5acf252f2a09e937
192.168.1.33	172.217.169.174	QUIC	75	Protected Payload (KP0), DCID=5acf252f2a09e937
172.217.169.174	192.168.1.33	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
192.168.1.33	172.217.169.174	TLSv1.3	118	Change Cipher Spec, Application Data
172.217.169.174	192.168.1.33	TCP	60	443 → 50996 [ACK] Seq=213 Ack=654 Win=66816 Len=0
172.217.169.174	192.168.1.33	TLSv1.3	634	Application Data, Application Data
172.217.169.174	192.168.1.33	QUIC	344	Protected Payload (KP0)
172.217.169.174	192.168.1.33	QUIC	67	Protected Payload (KP0)
192.168.1.33	172.217.169.174	QUIC	77	Protected Payload (KP0), DCID=5acf252f2a09e937
192.168.1.33	172.217.169.174	QUIC	75	Protected Payload (KP0), DCID=5acf252f2a09e937
192.168.1.33	172.217.169.174	TCP	54	50996 → 443 [ACK] Seq=654 Ack=793 Win=130304 Len=0
172.217.169.174	192.168.1.33	QUIC	67	Protected Payload (KP0)
192.168.1.1	192.168.1.33	DNS	149	Standard query response 0xc785 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
192.168.1.1	192.168.1.33	DNS	149	Standard query response 0xc785 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99

Yes, my host issues new DNS queries but my host does not explicitly retrieve images.

Q11. What is the destination port for the DNS query message? What is the source port of DNS response message?

21	22:52:47,849285	192.168.1.33	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
22	22:52:47,850369	192.168.1.1	192.168.1.33	DNS	84	Standard query response 0x0001 Server failure PTR 1.1.168.192.in-addr.a…
23	22:52:47,851094	192.168.1.33	192.168.1.1	DNS	76	Standard query 0x0002 A www.mit.edu.home
24	22:52:47,999806	192.168.1.1	192.168.1.33	DNS	151	Standard query response 0x0002 No such name A www.mit.edu.home SOA a.ro…
25	22:52:48,000011	192.168.1.33	192.168.1.1	DNS	76	Standard query 0x0003 AAAA www.mit.edu.home
26	22:52:48,055674	192.168.1.1	192.168.1.33	DNS	151	Standard query response 0x0003 No such name AAAA www.mit.edu.home SOA a…
27	22:52:48,055819	192.168.1.33	192.168.1.1	DNS	71	Standard query 0x0004 A www.mit.edu
28	22:52:48,072274	192.168.1.1	192.168.1.33	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.…
29	22:52:48,075709	192.168.1.33	192.168.1.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
30	22:52:48,085311	192.168.1.1	192.168.1.33	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgek…
36	22:52:49,788530	192.168.1.33	192.168.1.1	DNS	75	Standard query 0x81cd A www.youtube.com
37	22:52:49,804261	192.168.1.1	192.168.1.33	DNS	253	Standard query response 0x81cd A www.youtube.com CNAME youtube-ui.l.goo…
38	22:52:49,805090	192.168.1.33	216.58.212.46	QUIC	1392	Initial, DCID=67da265d1abb0d14, PKN: 1, CRYPTO, PADDING
39	22:52:49,830262	216.58.212.46	192.168.1.33	QUIC	1392	Initial, SCID=67da265d1abb0d14, PKN: 1, ACK, PADDING
41	22:52:49,860108	216.58.212.46	192.168.1.33	QUIC	1392	Initial, SCID=67da265d1abb0d14, PKN: 2, CRYPTO, PADDING
42	22:52:49,860108	216.58.212.46	192.168.1.33	QUIC	279	Handshake, SCID=67da265d1abb0d14
43	22:52:49,860206	216.58.212.46	192.168.1.33	QUIC	104	Protected Payload (KP0)
44	22:52:49,861172	192.168.1.33	216.58.212.46	QUIC	193	Protected Payload (KP0), DCID=67da265d1abb0d14
45	22:52:49,861524	192.168.1.33	216.58.212.46	QUIC	1388	Protected Payload (KP0), DCID=67da265d1abb0d14
46	22:52:49,861547	192.168.1.33	216.58.212.46	QUIC	409	Protected Payload (KP0), DCID=67da265d1abb0d14
50	22:52:49,882281	216.58.212.46	192.168.1.33	QUIC	654	Protected Payload (KP0)

```
> Frame 27: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{47757726-300E-4107-B849-4D6627335A75}, id 0
> Ethernet II, Src: Dell_bf:27:89 (50:9a:4c:bf:27:89), Dst: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b)
> Internet Protocol Version 4, Src: 192.168.1.33, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 65353, Dst Port: 53
    Source Port: 65353
    Destination Port: 53
    Length: 37
    Checksum: 0x83a9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

Destination port is 53. Source Port is 65353.

Q12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

21	22:52:47,849285	192.168.1.33	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
22	22:52:47,850369	192.168.1.1	192.168.1.33	DNS	84	Standard query response 0x0001 Server failure PTR 1.1.168.192.in-addr.a…
23	22:52:47,851094	192.168.1.33	192.168.1.1	DNS	76	Standard query 0x0002 A www.mit.edu.home
24	22:52:47,999806	192.168.1.1	192.168.1.33	DNS	151	Standard query response 0x0002 No such name A www.mit.edu.home SOA a.ro…
25	22:52:48,000011	192.168.1.33	192.168.1.1	DNS	76	Standard query 0x0003 AAAA www.mit.edu.home
26	22:52:48,055674	192.168.1.1	192.168.1.33	DNS	151	Standard query response 0x0003 No such name AAAA www.mit.edu.home SOA a…
27	22:52:48,055819	192.168.1.33	192.168.1.1	DNS	71	Standard query 0x0004 A www.mit.edu
28	22:52:48,072274	192.168.1.1	192.168.1.33	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.…
29	22:52:48,075709	192.168.1.33	192.168.1.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
30	22:52:48,085311	192.168.1.1	192.168.1.33	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgek…
36	22:52:49,788530	192.168.1.33	192.168.1.1	DNS	75	Standard query 0x81cd A www.youtube.com
37	22:52:49,804261	192.168.1.1	192.168.1.33	DNS	253	Standard query response 0x81cd A www.youtube.com CNAME youtube-ui.l.goo…
38	22:52:49,805090	192.168.1.33	216.58.212.46	QUIC	1392	Initial, DCID=67da265d1abb0d14, PKN: 1, CRYPTO, PADDING
39	22:52:49,830262	216.58.212.46	192.168.1.33	QUIC	1392	Initial, SCID=67da265d1abb0d14, PKN: 1, ACK, PADDING
41	22:52:49,860108	216.58.212.46	192.168.1.33	QUIC	1392	Initial, SCID=67da265d1abb0d14, PKN: 2, CRYPTO, PADDING
42	22:52:49,860108	216.58.212.46	192.168.1.33	QUIC	279	Handshake, SCID=67da265d1abb0d14
43	22:52:49,860206	216.58.212.46	192.168.1.33	QUIC	104	Protected Payload (KP0)
44	22:52:49,861172	192.168.1.33	216.58.212.46	QUIC	193	Protected Payload (KP0), DCID=67da265d1abb0d14
45	22:52:49,861524	192.168.1.33	216.58.212.46	QUIC	1388	Protected Payload (KP0), DCID=67da265d1abb0d14
46	22:52:49,861547	192.168.1.33	216.58.212.46	QUIC	409	Protected Payload (KP0), DCID=67da265d1abb0d14
50	22:52:49,882281	216.58.212.46	192.168.1.33	QUIC	654	Protected Payload (KP0)

```
> Frame 27: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{47757726-300E-4107-B849-4D6627335A75}, id 0
> Ethernet II, Src: Dell_bf:27:89 (50:9a:4c:bf:27:89), Dst: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b)
> Internet Protocol Version 4, Src: 192.168.1.33, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 65353, Dst Port: 53
    Source Port: 65353
    Destination Port: 53
    Length: 37
    Checksum: 0x83a9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

IP address is 192.168.1.1

Yes, the address is my default local DNS server.

Q13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
    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)
```

DNS query is type A. Query message does not contain any answers. It contains a single question.

Q14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

```
Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
  v Answers
    v 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: 1644 (27 minutes, 24 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    v 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: 38 (38 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 104.66.82.6
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 19 (19 seconds)
        Data length: 4
        Address: 104.66.82.6
    [Request In: 27]
    [Time: 0.016455000 seconds]
```

3 answers are provided. Answers contain two "type CNAME" and one "type A" information.

Q15. Provide a screenshot.

21	22:52:47,849285	192.168.1.33	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
22	22:52:47,850369	192.168.1.1	192.168.1.33	DNS	84	Standard query response 0x0001 Server failure PTR 1.1.168.192.in-addr.a…
23	22:52:47,851094	192.168.1.33	192.168.1.1	DNS	76	Standard query 0x0002 A www.mit.edu.home
24	22:52:47,999806	192.168.1.1	192.168.1.33	DNS	151	Standard query response 0x0002 No such name A www.mit.edu.home SOA a.ro…
25	22:52:48,000011	192.168.1.33	192.168.1.1	DNS	76	Standard query 0x0003 AAAA www.mit.edu.home
26	22:52:48,055674	192.168.1.1	192.168.1.33	DNS	151	Standard query response 0x0003 No such name AAAA www.mit.edu.home SOA a…
27	22:52:48,055819	192.168.1.33	192.168.1.1	DNS	71	Standard query 0x0004 A www.mit.edu
28	22:52:48,072274	192.168.1.1	192.168.1.33	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.…
29	22:52:48,075709	192.168.1.33	192.168.1.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
30	22:52:48,085311	192.168.1.1	192.168.1.33	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgek…

Q16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

13	23:10:50,669753	192.168.1.33	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
14	23:10:50,670801	192.168.1.1	192.168.1.33	DNS	84	Standard query response 0x0001 Server failure PTR 1.1.168.192.in-addr.arpa
15	23:10:50,671629	192.168.1.33	192.168.1.1	DNS	72	Standard query 0x0002 NS mit.edu.home
16	23:10:50,737906	192.168.1.1	192.168.1.33	DNS	147	Standard query response 0x0002 No such name NS mit.edu.home SOA a.root-servers.net
17	23:10:50,738106	192.168.1.33	192.168.1.1	DNS	67	Standard query 0x0003 NS mit.edu
18	23:10:50,780087	192.168.1.1	192.168.1.33	DNS	234	Standard query response 0x0003 NS mit.edu NS ns1-173.akam.net NS usw2.akam.net NS ns1-37.akam.net N…

The query message is sent to 192.168.1.1, same IP address of my local DNS server.

Q17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type NS, class IN
    [Response In: 18]
```

DNS query is "NS" type. It includes only one question. It does not include any answers.

Q18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

```
v Answers
  > mit.edu: type NS, class IN, ns ns1-173.akam.net
  > mit.edu: type NS, class IN, ns usw2.akam.net
  > mit.edu: type NS, class IN, ns ns1-37.akam.net
  > mit.edu: type NS, class IN, ns asia2.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 use5.akam.net
  > mit.edu: type NS, class IN, ns asia1.akam.net
```

The message provides 8 MIT nameservers. Response message does not provide the IP addresses of them.

Q19. Provide a screenshot.

13	23:10:50,669753	192.168.1.33	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
14	23:10:50,670801	192.168.1.1	192.168.1.33	DNS	84	Standard query response 0x0001 Server failure PTR 1.1.168.192.in-addr.arpa
15	23:10:50,671629	192.168.1.33	192.168.1.1	DNS	72	Standard query 0x0002 NS mit.edu.home
16	23:10:50,737906	192.168.1.1	192.168.1.33	DNS	147	Standard query response 0x0002 No such name NS mit.edu.home SOA a.root-servers.net
17	23:10:50,738106	192.168.1.33	192.168.1.1	DNS	67	Standard query 0x0003 NS mit.edu
18	23:10:50,780087	192.168.1.1	192.168.1.33	DNS	234	Standard query response 0x0003 NS mit.edu NS ns1-173.akam.net NS usw2.akam.net NS ns1-37.aka…

Q20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

21	23:22:46,000963	192.168.1.33	91.93.102.43	DNS	76	Standard query 0x0002 A kaist.ac.kr.home
22	23:22:46,051353	91.93.102.43	192.168.1.33	DNS	151	Standard query response 0x0002 No such name A kaist.ac.kr.home SOA a.root-servers.net
23	23:22:46,051558	192.168.1.33	91.93.102.43	DNS	76	Standard query 0x0003 AAAA kaist.ac.kr.home
24	23:22:46,061091	91.93.102.43	192.168.1.33	DNS	151	Standard query response 0x0003 No such name AAAA kaist.ac.kr.home SOA a.root-servers.net
25	23:22:46,061234	192.168.1.33	91.93.102.43	DNS	71	Standard query 0x0004 A kaist.ac.kr
26	23:22:46,101719	192.168.1.33	159.89.100.215	TLSv1	571	Client Hello
28	23:22:46,420857	91.93.102.43	192.168.1.33	DNS	87	Standard query response 0x0004 A kaist.ac.kr A 143.248.155.65
29	23:22:46,424099	192.168.1.33	91.93.102.43	DNS	71	Standard query 0x0005 AAAA kaist.ac.kr
30	23:22:46,505506	192.168.1.33	192.168.1.255	UDP	305	54915 → 54915 Len=263
31	23:22:46,760423	91.93.102.43	192.168.1.33	DNS	120	Standard query response 0x0005 AAAA kaist.ac.kr SOA dns181.kaist.ac.kr

DNS query message is sent to 91.93.102.43

It is not my default local DNS server. That IP address corresponds to KAIST's DNS response sender.

Q21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > kaist.ac.kr: type A, class IN
    [Response In: 28]
```

DNS query is type A query. It does not contain any answers.

Q22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

```
Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > kaist.ac.kr: type A, class IN
  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: 25]
    [Time: 0.359623000 seconds]
```

Response message provided a single answer which contains server's IP address.

Q23. Provide a screenshot.

15	23:22:45,871397	192.168.1.33	192.168.1.1	DNS	85	Standard query 0x75ce A ns2.guvenlikcozumleri.com
16	23:22:45,911336	192.168.1.33	192.168.1.1	DNS	85	Standard query 0x75ce A ns2.guvenlikcozumleri.com
17	23:22:45,989095	192.168.1.1	192.168.1.33	DNS	101	Standard query response 0x75ce A ns2.guvenlikcozumleri.com A 91.93.102.43
18	23:22:45,989173	192.168.1.1	192.168.1.33	DNS	101	Standard query response 0x75ce A ns2.guvenlikcozumleri.com A 91.93.102.43
19	23:22:45,991552	192.168.1.33	91.93.102.43	DNS	85	Standard query 0x0001 PTR 43.102.93.91.in-addr.arpa
20	23:22:46,000017	91.93.102.43	192.168.1.33	DNS	124	Standard query response 0x0001 PTR 43.102.93.91.in-addr.arpa PTR ns2.guvenlikcozumleri.com
21	23:22:46,000963	192.168.1.33	91.93.102.43	DNS	76	Standard query 0x0002 A kaist.ac.kr.home
22	23:22:46,051353	91.93.102.43	192.168.1.33	DNS	151	Standard query response 0x0002 No such name A kaist.ac.kr.home SOA a.root-servers.net
23	23:22:46,051558	192.168.1.33	91.93.102.43	DNS	76	Standard query 0x0003 AAAA kaist.ac.kr.home
24	23:22:46,061091	91.93.102.43	192.168.1.33	DNS	151	Standard query response 0x0003 No such name AAAA kaist.ac.kr.home SOA a.root-servers.net
25	23:22:46,061234	192.168.1.33	91.93.102.43	DNS	71	Standard query 0x0004 A kaist.ac.kr
26	23:22:46,101719	192.168.1.33	159.89.100.215	TLSv1	571	Client Hello
28	23:22:46,420857	91.93.102.43	192.168.1.33	DNS	87	Standard query response 0x0004 A kaist.ac.kr A 143.248.155.65
29	23:22:46,424099	192.168.1.33	91.93.102.43	DNS	71	Standard query 0x0005 AAAA kaist.ac.kr
30	23:22:46,505506	192.168.1.33	192.168.1.255	UDP	305	54915 → 54915 Len=263
31	23:22:46,760423	91.93.102.43	192.168.1.33	DNS	120	Standard query response 0x0005 AAAA kaist.ac.kr SOA dns181.kaist.ac.kr

3. Extras

Exercise 1: You may send queries to root DNS servers and see what you get. You may try the following root server: a.root-servers.net

- Please try the following: "nslookup www.marmara.edu.tr a.root-servers.net"

```
C:\Users\dell>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
```

- You will get a list of TLD servers

- Then please send the same query to one of the TLD servers.

```
C:\Users\dell>nslookup www.marmara.edu.tr ns21.nic.tr
Server:  UnKnown
Address:  213.14.246.2

Name:    www.marmara.edu.tr
Served by:
- ns1.marmara.edu.tr
          193.140.143.2
          2001:a98:a070:8c8f::2
          marmara.edu.tr
- ns2.marmara.edu.tr
          193.140.143.3
          2001:a98:a070:8c8f::3
          marmara.edu.tr
```

- You will get a list of authoritative DNS servers of marmara.edu.tr

- Then please send the same query to authoritative DNS server of marmara.edu.tr

```
C:\Users\dell>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
```

- You will get the IP address of www.marmara.edu.tr

- Repeat the above steps for any address in Asia.

```
C:\Users\dell>nslookup www.english.pku.edu.cn 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.english.pku.edu.cn
Served by:
- c.dns.cn
          203.119.27.1
          cn
- g.dns.cn
          66.198.183.65
          cn
- b.dns.cn
          203.119.26.1
          cn
- ns.cernet.net
          202.112.0.44
          cn
- e.dns.cn
          203.119.29.1
          cn
- f.dns.cn
          195.219.8.90
          cn
- a.dns.cn
          203.119.25.1
          2001:dc7::1
          cn
```

```
C:\Users\dell>nslookup www.english.pku.edu.cn c.dns.cn
Server:  c.dns.cn
Address:  203.119.27.1

Name:    www.english.pku.edu.cn
Served by:
- ns2.cuhk.hk

          edu.cn
- ns2.cernet.net

          edu.cn
- deneb.dfn.de

          edu.cn
- dns.edu.cn
          202.38.109.35
          2001:250:c006::35
          edu.cn
- dns2.edu.cn
          202.112.0.13
          2001:da8:1:100::13
          edu.cn
```

```
C:\Users\dell>nslookup www.english.pku.edu.cn dns2.edu.cn
Server:  dns2.edu.cn
Address:  202.112.0.13

Name:    www.english.pku.edu.cn
Served by:
- dns.pku.edu.cn
          162.105.129.26
          pku.edu.cn
- dns2.pku.edu.cn
          162.105.129.122
          pku.edu.cn
- ns.pku.edu.cn
          202.112.7.13
          pku.edu.cn
```

```
C:\Users\dell>nslookup www.english.pku.edu.cn ns.pku.edu.cn
Server:  UnKnown
Address:  162.105.129.130

Name:    www.english.pku.edu.cn
Addresses:  2001:da8:201:1920::731b:f097
          115.27.240.151
```

Exercise 2: You may also try other types, such as CNAME and MX.

- What is the canonical name of www.mit.edu? What about "satlab.cmpe.boun.edu.tr" (my previous lab)? Or "netlab.cmpe.boun.edu.tr" (another lab that I worked in)?

```
Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
  v Answers
    v 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: 1644 (27 minutes, 24 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    v 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: 38 (38 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 104.66.82.6
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 19 (19 seconds)
        Data length: 4
        Address: 104.66.82.6
    [Request In: 27]
    [Time: 0.016455000 seconds]
```

Canonical name of www.mit.edu is www.mit.edu.edgekey.net

```
v Answers
  v satlab.cmpe.boun.edu.tr: type CNAME, class IN, cname kalkan.cmpe.boun.edu.tr
      Name: satlab.cmpe.boun.edu.tr
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 9
      CNAME: kalkan.cmpe.boun.edu.tr
  v kalkan.cmpe.boun.edu.tr: type A, class IN, addr 79.123.177.146
      Name: kalkan.cmpe.boun.edu.tr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 4
      Address: 79.123.177.146
```

Canonical name of satlab.cmpe.boun.edu.tr is kalkan.cmpe.boun.edu.tr

```
Answers
  netlab.cmpe.boun.edu.tr: type CNAME, class IN, cname orkinos.cmpe.boun.edu.tr
      Name: netlab.cmpe.boun.edu.tr
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 10
      CNAME: orkinos.cmpe.boun.edu.tr
  orkinos.cmpe.boun.edu.tr: type A, class IN, addr 79.123.177.242
      Name: orkinos.cmpe.boun.edu.tr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 4
      Address: 79.123.177.242
```

Canonical name of netlab.cmpe.boun.edu.tr is orkinos.cmpe.boun.edu.tr

- What is the name of the mail server (mail exchanger) of marmara.edu.tr? What about "cmpe.boun.edu.tr"? or "boun.edu.tr"?

```
C:\Users\dell>nslookup -type=NS www.marmara.edu.tr
Server:  UnKnown
Address:  192.168.1.1

marmara.edu.tr
        primary name server = ns1.marmara.edu.tr
        responsible mail addr = sysadmin.marmara.edu.tr
        serial  = 2020120101
        refresh = 10800 (3 hours)
        retry   = 900 (15 mins)
        expire  = 2419200 (28 days)
        default TTL = 900 (15 mins)
```

Name of the mail server of marmara.edu.tr is sysadmin.marmara.edu.tr

```
C:\Users\dell>nslookup -type=MX cmpe.boun.edu.tr
Server:  UnKnown
Address:  192.168.1.1

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

C:\Users\dell>nslookup -type=NS zebra.cmpe.boun.edu.tr
Server:  UnKnown
Address:  192.168.1.1

cmpe.boun.edu.tr
        primary name server = ns1.cmpe.boun.edu.tr
        responsible mail addr = admin.cmpe.boun.edu.tr
        serial  = 2020102801
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

Name of the mail server of cmpe.boun.edu.tr is admin.cmpe.boun.edu.tr

- Please repeat the above for any web server and mail domain, respectively.

```
C:\Users\dell>nslookup -type=NS www.lazarski.pl
Server:  UnKnown
Address:  192.168.1.1

lazarski.pl
        primary name server = ns1.domena.pl
        responsible mail addr = hosting.agnat.pl
        serial  = 2015066206
        refresh = 43200 (12 hours)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)
```

Name of the mail server of lazarski.pl is hosting.agnat.pl