Name/Surname of Members: Ayça Akyol - Gamze Ergin

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

We looked up United Nation’s web server and its IP address is: 18.244.87.103

2. Run nslookup to determine the authoritative DNS servers for a university in United States.

```
Server:  ns01.hacettepe.edu.tr
Address:  193.140.216.203

Non-authoritative answer:
www.nyu.edu     canonical name = d1q5ku5vnwkd2k.cloudfront.net
d1q5ku5vnwkd2k.cloudfront.net   nameserver = ns-744.awsdns-29.net
d1q5ku5vnwkd2k.cloudfront.net   nameserver = ns-1782.awsdns-30.co.uk
d1q5ku5vnwkd2k.cloudfront.net   nameserver = ns-1040.awsdns-02.org
d1q5ku5vnwkd2k.cloudfront.net   nameserver = ns-45.awsdns-05.com

ns-1040.awsdns-02.org   internet address = 205.251.196.16
ns-744.awsdns-29.net    internet address = 205.251.194.232
ns-1040.awsdns-02.org   AAAA IPv6 address = 2600:9000:5304:1000::1
ns-744.awsdns-29.net    AAAA IPv6 address = 2600:9000:5302:e800::1
```

3. Run nslookup so that one of the DNS servers of Google is queried for the mail servers for Yahoo! mail. What is its IP address?

```
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    src.g03.yahoodns.net
Addresses:  13.50.184.192
          13.49.212.207
Aliases:  www.mail.yahoo.com
          rc.yahoo.com
```

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

UDP

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

source: 10.225.125.101 destination: 193.140.216.203

6. 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?

yes they are the same

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

It has Type: A (Host Address) so it has type A query. But it does not have any answers as we can see from this line: Answer RRs: 0

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

There are 2 answers. Answers are ietf analytics like:
analytics.ietf.org: type A, class IN, addr 104.16.45.99

9. 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?

Yes. the destination IP address is 104.16.44.99. And one of the answers from the DNS had the same IP address as address.

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

we think no but answer might be yes?????

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

destination port: 53 and source: 65369

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

Message is sent to 193.140.216.203 which is also the IP address of the local DNS server.

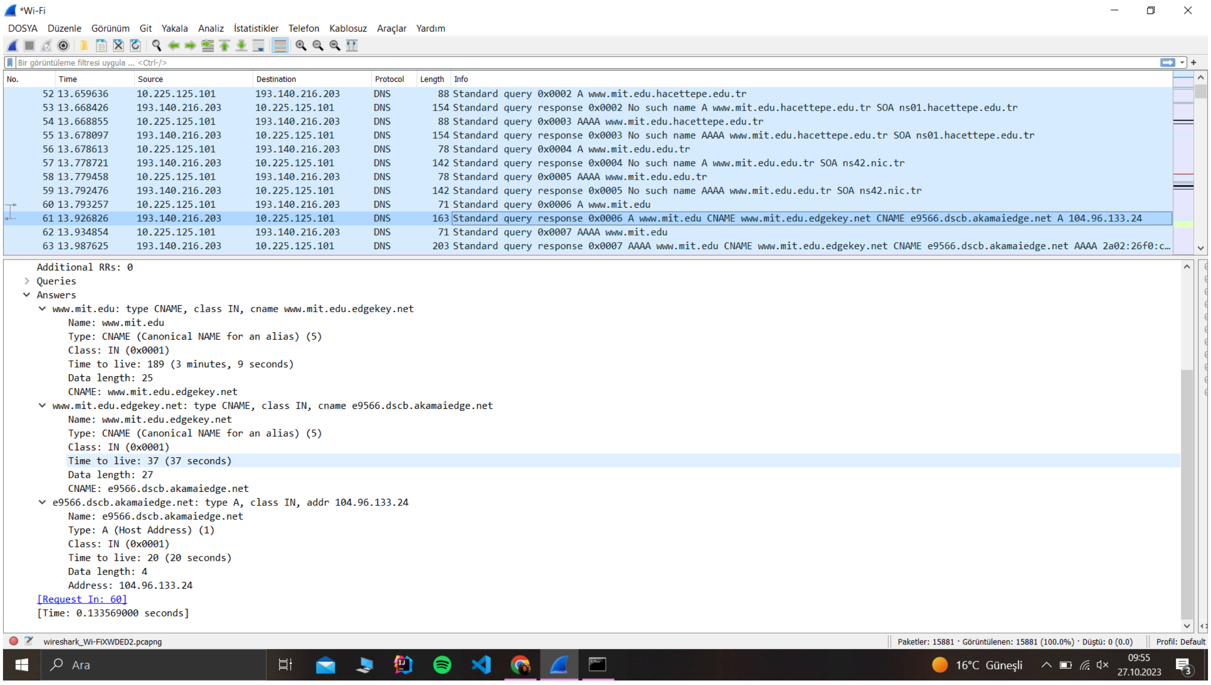
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Type A. No answers.

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

There are 3 answers.

15. Provide a screenshot.


*Wi-Fi
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
Bir görüntüleme filtresi uygula ... <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
   52 13.659636  10.225.125.101   193.140.216.203  DNS       88 Standard query 0x0002 A www.mit.edu.hacettepe.edu.tr
   53 13.668426  193.140.216.203  10.225.125.101   DNS      154 Standard query response 0x0002 No such name A www.mit.edu.hacettepe.edu.tr SOA ns01.hacettepe.edu.tr
   54 13.668855  10.225.125.101   193.140.216.203  DNS       88 Standard query 0x0003 AAAA www.mit.edu.hacettepe.edu.tr
   55 13.678097  193.140.216.203  10.225.125.101   DNS      154 Standard query response 0x0003 No such name AAAA www.mit.edu.hacettepe.edu.tr SOA ns01.hacettepe.edu.tr
   56 13.678613  10.225.125.101   193.140.216.203  DNS       78 Standard query 0x0004 A www.mit.edu.edu.tr
   57 13.778721  193.140.216.203  10.225.125.101   DNS      142 Standard query response 0x0004 No such name A www.mit.edu.edu.tr SOA ns42.nic.tr
   58 13.779458  10.225.125.101   193.140.216.203  DNS       78 Standard query 0x0005 AAAA www.mit.edu.edu.tr
   59 13.792476  193.140.216.203  10.225.125.101   DNS      142 Standard query response 0x0005 No such name AAAA www.mit.edu.edu.tr SOA ns42.nic.tr
   60 13.793257  10.225.125.101   193.140.216.203  DNS       71 Standard query 0x0006 A www.mit.edu
   61 13.926826  193.140.216.203  10.225.125.101   DNS      163 Standard query response 0x0006 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.96.133.24
   62 13.934854  10.225.125.101   193.140.216.203  DNS       71 Standard query 0x0007 AAAA www.mit.edu
   63 13.987625  193.140.216.203  10.225.125.101   DNS      203 Standard query response 0x0007 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:c…
```

```
    Additional RRs: 0
  > Queries
  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: 189 (3 minutes, 9 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: 37 (37 seconds)
          Data length: 27
          CNAME: e9566.dscb.akamaiedge.net
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.133.24
          Name: e9566.dscb.akamaiedge.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 20 (20 seconds)
          Data length: 4
          Address: 104.96.133.24
    [Request In: 60]
    [Time: 0.133569000 seconds]
```

wireshark_Wi-FiXWDED2.pcapng
Paketler: 15881 · Görüntülenen: 15881 (100.0%) · Düştü: 0 (0.0)
Profil: Default
Ara
16°C Güneşli
09:55
27.10.2023

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

Message is sent to 193.140.216.203 which is also the IP address of the local DNS server.

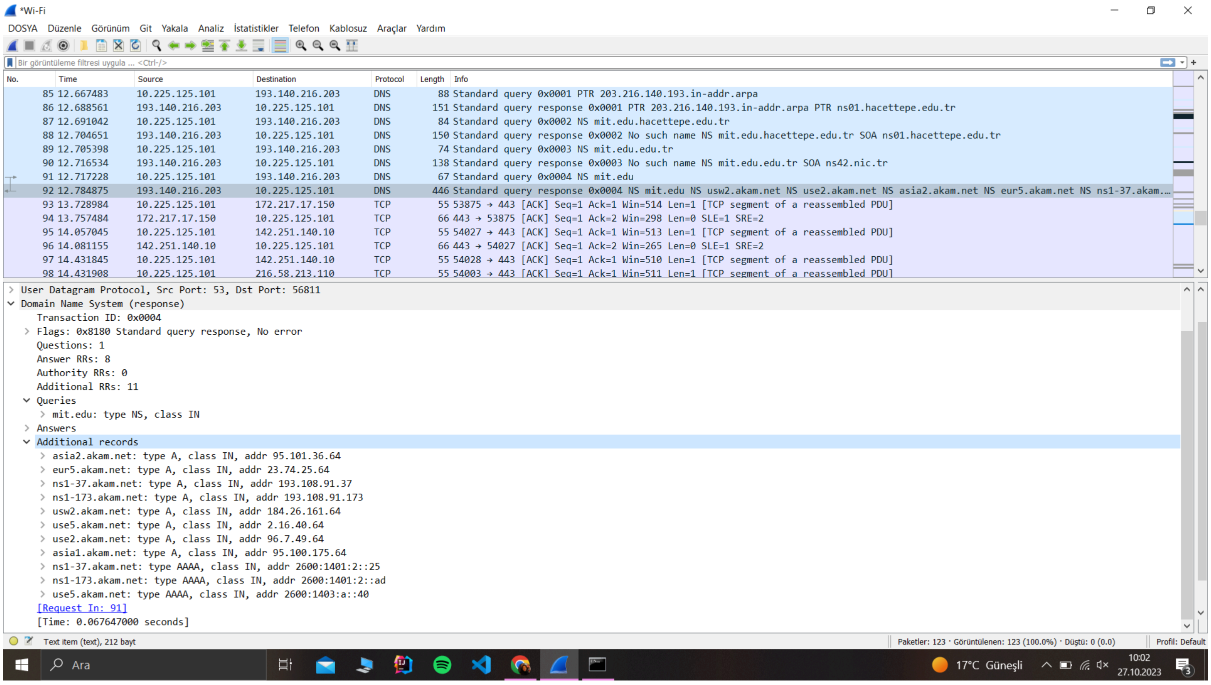
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type is NS (authoritative Name Server) but it does not have any answers.

18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

Response message provides 11 additional records with name servers and their IP addresses. You can see all of them in the screenshot below.

19. Provide a screenshot.


*Wi-Fi
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
Bir görüntüleme filtresi uygula ... <Ctrl-/>
Ara
17°C Güneşli
10:02
27.10.2023

```
No.  Time       Source           Destination      Protocol Length Info
  85 12.667483  10.225.125.101   193.140.216.203  DNS       88 Standard query 0x0001 PTR 203.216.140.193.in-addr.arpa
  86 12.688561  193.140.216.203  10.225.125.101   DNS      151 Standard query response 0x0001 PTR 203.216.140.193.in-addr.arpa PTR ns01.hacettepe.edu.tr
  87 12.691042  10.225.125.101   193.140.216.203  DNS       84 Standard query 0x0002 NS mit.edu.hacettepe.edu.tr
  88 12.704651  193.140.216.203  10.225.125.101   DNS      150 Standard query response 0x0002 No such name NS mit.edu.hacettepe.edu.tr SOA ns01.hacettepe.edu.tr
  89 12.705398  10.225.125.101   193.140.216.203  DNS       74 Standard query 0x0003 NS mit.edu.edu.tr
  90 12.716534  193.140.216.203  10.225.125.101   DNS      138 Standard query response 0x0003 No such name NS mit.edu.edu.tr SOA ns42.nic.tr
  91 12.717228  10.225.125.101   193.140.216.203  DNS       67 Standard query 0x0004 NS mit.edu
  92 12.784875  193.140.216.203  10.225.125.101   DNS      446 Standard query response 0x0004 NS mit.edu NS usw2.akam.net NS use2.akam.net NS asia2.akam.net NS eur5.akam.net NS ns1-37.akam...
  93 13.728984  10.225.125.101   172.217.17.150   TCP       55 53875 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
  94 13.757484  172.217.17.150   10.225.125.101   TCP       66 443 → 53875 [ACK] Seq=1 Ack=2 Win=298 Len=0 SLE=1 SRE=2
  95 14.057045  10.225.125.101   142.251.140.10   TCP       55 54027 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
  96 14.081155  142.251.140.10   10.225.125.101   TCP       66 443 → 54027 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
  97 14.431845  10.225.125.101   142.251.140.10   TCP       55 54028 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
  98 14.431908  10.225.125.101   216.58.213.110   TCP       55 54003 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
```

```
> User Datagram Protocol, Src Port: 53, Dst Port: 56811
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 11
  v Queries
    > mit.edu: type NS, class IN
  > Answers
  v Additional records
    > asia2.akam.net: type A, class IN, addr 95.101.36.64
    > eur5.akam.net: type A, class IN, addr 23.74.25.64
    > ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    > ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    > usw2.akam.net: type A, class IN, addr 184.26.161.64
    > use5.akam.net: type A, class IN, addr 2.16.40.64
    > use2.akam.net: type A, class IN, addr 96.7.49.64
    > asia1.akam.net: type A, class IN, addr 95.100.175.64
    > ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
    > ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    > use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    [Request In: 91]
    [Time: 0.067647000 seconds]
```

```
Text item (text), 212 bayt        Paketler: 123 · Görüntülenen: 123 (100.0%) · Düştü: 0 (0.0)        Profil: Default
```

20. 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?

Query message is sent to 193.140.216.203 and this is the local DNS server's IP address.

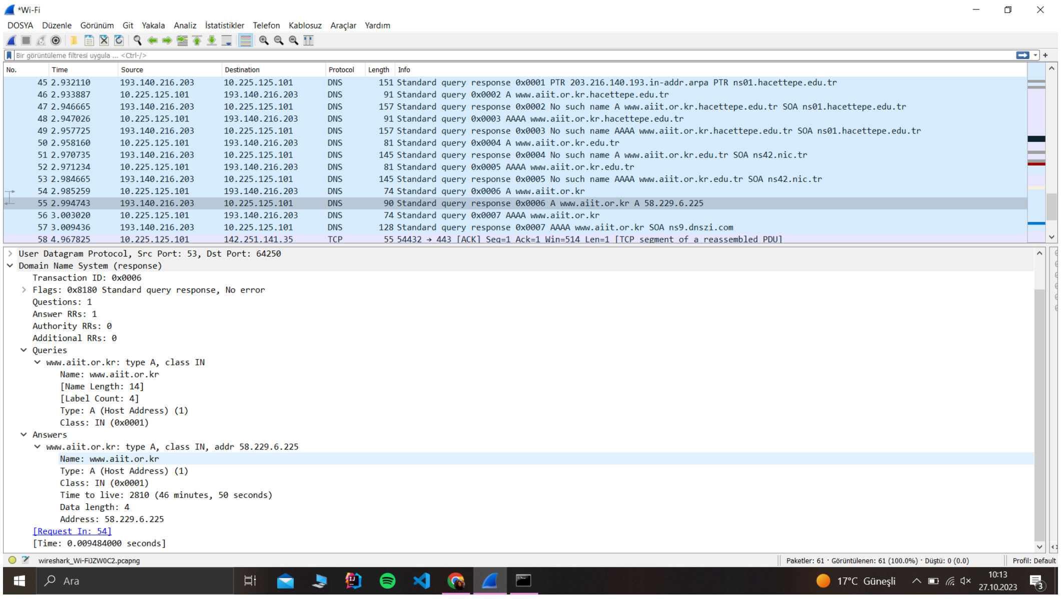
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

It's type A and does not have any answers.

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

It has 1 answer and it contains information like IP address, name, type etc. You can see the full answer from the screenshot.

23. Provide a screenshot.


*Wi-Fi
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
Bir görüntüleme filtresi uygula ... <Ctrl-/>
Ara
17°C Güneşli
10:13
27.10.2023

```
No.  Time      Source           Destination      Protocol Length Info
  45 2.932110  193.140.216.203  10.225.125.101   DNS      151 Standard query response 0x0001 PTR 203.216.140.193.in-addr.arpa PTR ns01.hacettepe.edu.tr
  46 2.933887  10.225.125.101   193.140.216.203  DNS       91 Standard query 0x0002 A www.aiit.or.kr.hacettepe.edu.tr
  47 2.946665  193.140.216.203  10.225.125.101   DNS      157 Standard query response 0x0002 No such name A www.aiit.or.kr.hacettepe.edu.tr SOA ns01.hacettepe.edu.tr
  48 2.947026  10.225.125.101   193.140.216.203  DNS       91 Standard query 0x0003 AAAA www.aiit.or.kr.hacettepe.edu.tr
  49 2.957725  193.140.216.203  10.225.125.101   DNS      157 Standard query response 0x0003 No such name AAAA www.aiit.or.kr.hacettepe.edu.tr SOA ns01.hacettepe.edu.tr
  50 2.958160  10.225.125.101   193.140.216.203  DNS       81 Standard query 0x0004 A www.aiit.or.kr.edu.tr
  51 2.970735  193.140.216.203  10.225.125.101   DNS      145 Standard query response 0x0004 No such name A www.aiit.or.kr.edu.tr SOA ns42.nic.tr
  52 2.971234  10.225.125.101   193.140.216.203  DNS       81 Standard query 0x0005 AAAA www.aiit.or.kr.edu.tr
  53 2.984665  193.140.216.203  10.225.125.101   DNS      145 Standard query response 0x0005 No such name AAAA www.aiit.or.kr.edu.tr SOA ns42.nic.tr
  54 2.985259  10.225.125.101   193.140.216.203  DNS       74 Standard query 0x0006 A www.aiit.or.kr
  55 2.994743  193.140.216.203  10.225.125.101   DNS       90 Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
  56 3.003020  10.225.125.101   193.140.216.203  DNS       74 Standard query 0x0007 AAAA www.aiit.or.kr
  57 3.009436  193.140.216.203  10.225.125.101   DNS      128 Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com
  58 4.967825  10.225.125.101   142.251.141.35   TCP       55 54432 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
```

```
> User Datagram Protocol, Src Port: 53, Dst Port: 64250
v Domain Name System (response)
    Transaction ID: 0x0006
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v www.aiit.or.kr: type A, class IN, addr 58.229.6.225
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 2810 (46 minutes, 50 seconds)
        Data length: 4
        Address: 58.229.6.225
    [Request In: 54]
    [Time: 0.009484000 seconds]
```

```
wireshark_Wi-FiJZW0C2.pcapng        Paketler: 61 · Görüntülenen: 61 (100.0%) · Düştü: 0 (0.0)        Profil: Default
```