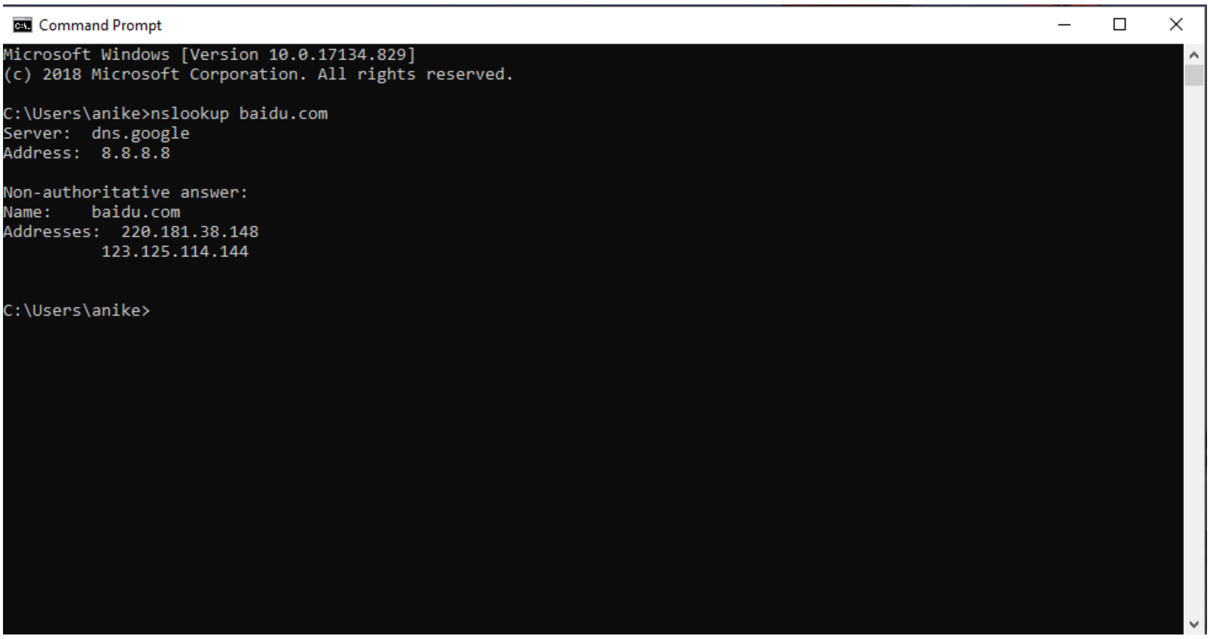
CSE-5344 Lab 1

Submitted by:
Aniket Gade
UTA ID - 1001505046

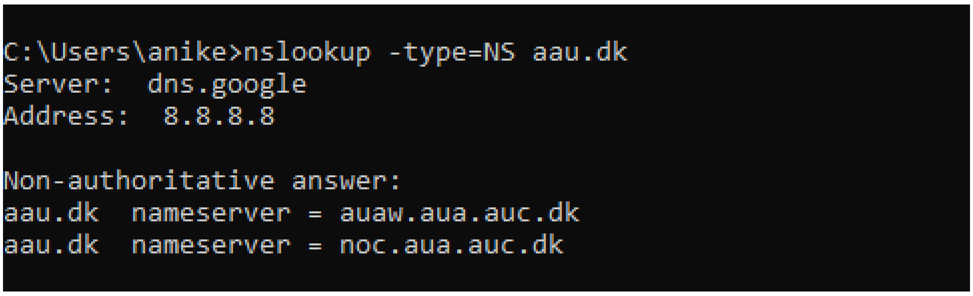
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?



```
Microsoft Windows [Version 10.0.17134.829]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\anike>nslookup baidu.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    baidu.com
Addresses:  220.181.38.148
          123.125.114.144


C:\Users\anike>
```

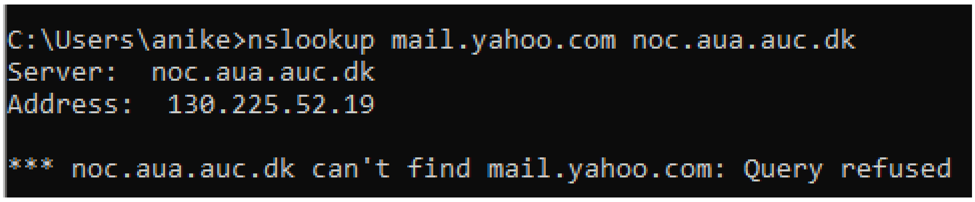
The IP address of baidu.com's server is 220.181.38.148.

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



```
C:\Users\anike>nslookup -type=NS aau.dk
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
aau.dk  nameserver = auaw.aua.auc.dk
aau.dk  nameserver = noc.aua.auc.dk
```

3. 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?



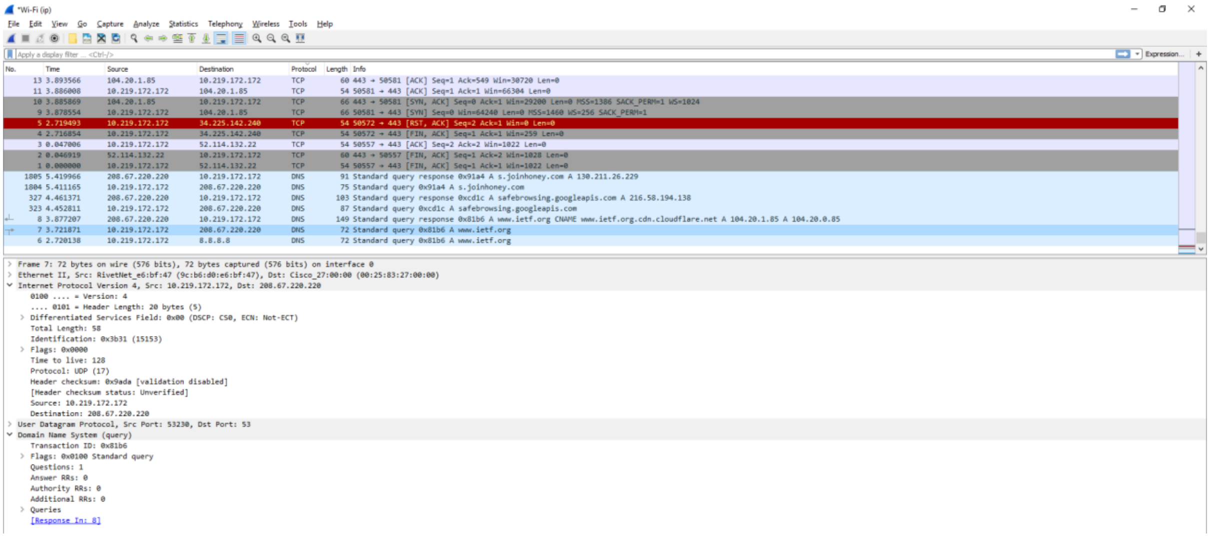
```
C:\Users\anike>nslookup mail.yahoo.com noc.aua.auc.dk
Server:  noc.aua.auc.dk
Address:  130.225.52.19

*** noc.aua.auc.dk can't find mail.yahoo.com: Query refused
```

The IP address is 130.225.52.19

Part 2

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

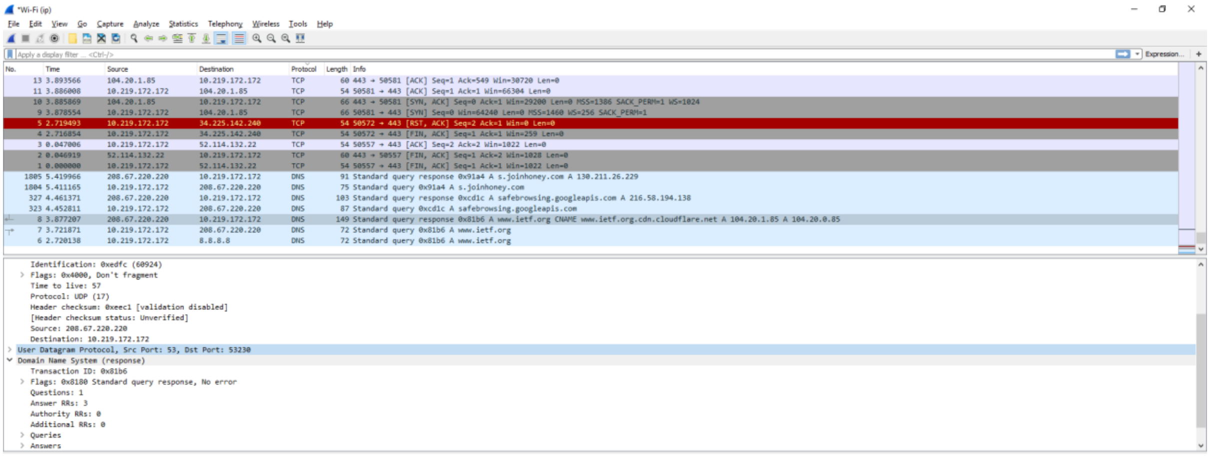
a) Query:



```
No.   Time       Source          Destination     Protocol Length Info
   13 3.893566   104.20.1.85     10.219.172.172  TCP      60 443 → 50581 [ACK] Seq=1 Ack=549 Win=30720 Len=0
   11 3.886008   10.219.172.172  104.20.1.85     TCP      54 50581 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
   10 3.885869   104.20.1.85     10.219.172.172  TCP      66 443 → 50581 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=1024
    9 3.878554   10.219.172.172  104.20.1.85     TCP      66 50581 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    5 2.719493   10.219.172.172  34.225.142.240  TCP      54 50572 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
    4 2.716854   10.219.172.172  34.225.142.240  TCP      54 50572 → 443 [FIN, ACK] Seq=1 Ack=1 Win=259 Len=0
    3 0.047006   10.219.172.172  52.114.132.22   TCP      54 50557 → 443 [ACK] Seq=2 Ack=2 Win=1022 Len=0
    2 0.046919   52.114.132.22   10.219.172.172  TCP      60 443 → 50557 [FIN, ACK] Seq=1 Ack=2 Win=1028 Len=0
    1 0.000000   10.219.172.172  52.114.132.22   TCP      54 50557 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
 1805 5.419966   208.67.220.220  10.219.172.172  DNS      91 Standard query response 0x91a4 A s.joinhoney.com A 130.211.26.229
 1804 5.411165   10.219.172.172  208.67.220.220  DNS      75 Standard query 0x91a4 A s.joinhoney.com
  327 4.461371   208.67.220.220  10.219.172.172  DNS     103 Standard query response 0xcd1c A safebrowsing.googleapis.com A 216.58.194.138
  323 4.452811   10.219.172.172  208.67.220.220  DNS      87 Standard query 0xcd1c A safebrowsing.googleapis.com
    8 3.877207   208.67.220.220  10.219.172.172  DNS     149 Standard query response 0x81b6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
    7 3.721871   10.219.172.172  208.67.220.220  DNS      72 Standard query 0x81b6 A www.ietf.org
    6 2.720138   10.219.172.172  8.8.8.8         DNS      72 Standard query 0x81b6 A www.ietf.org
```

```
> Frame 7: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: RivetNet_e6:bf:47 (9c:b6:d0:e6:bf:47), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
v Internet Protocol Version 4, Src: 10.219.172.172, Dst: 208.67.220.220
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x3b31 (15153)
  > Flags: 0x0000
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x9ada [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.219.172.172
    Destination: 208.67.220.220
> User Datagram Protocol, Src Port: 53230, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x81b6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 8]
```

b) Response:



```
No.   Time       Source          Destination     Protocol Length Info
   13 3.893566   104.20.1.85     10.219.172.172  TCP      60 443 → 50581 [ACK] Seq=1 Ack=549 Win=30720 Len=0
   11 3.886008   10.219.172.172  104.20.1.85     TCP      54 50581 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
   10 3.885869   104.20.1.85     10.219.172.172  TCP      66 443 → 50581 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=1024
    9 3.878554   10.219.172.172  104.20.1.85     TCP      66 50581 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    5 2.719493   10.219.172.172  34.225.142.240  TCP      54 50572 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
    4 2.716854   10.219.172.172  34.225.142.240  TCP      54 50572 → 443 [FIN, ACK] Seq=1 Ack=1 Win=259 Len=0
    3 0.047006   10.219.172.172  52.114.132.22   TCP      54 50557 → 443 [ACK] Seq=2 Ack=2 Win=1022 Len=0
    2 0.046919   52.114.132.22   10.219.172.172  TCP      60 443 → 50557 [FIN, ACK] Seq=1 Ack=2 Win=1028 Len=0
    1 0.000000   10.219.172.172  52.114.132.22   TCP      54 50557 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
 1805 5.419966   208.67.220.220  10.219.172.172  DNS      91 Standard query response 0x91a4 A s.joinhoney.com A 130.211.26.229
 1804 5.411165   10.219.172.172  208.67.220.220  DNS      75 Standard query 0x91a4 A s.joinhoney.com
  327 4.461371   208.67.220.220  10.219.172.172  DNS     103 Standard query response 0xcd1c A safebrowsing.googleapis.com A 216.58.194.138
  323 4.452811   10.219.172.172  208.67.220.220  DNS      87 Standard query 0xcd1c A safebrowsing.googleapis.com
    8 3.877207   208.67.220.220  10.219.172.172  DNS     149 Standard query response 0x81b6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
    7 3.721871   10.219.172.172  208.67.220.220  DNS      72 Standard query 0x81b6 A www.ietf.org
    6 2.720138   10.219.172.172  8.8.8.8         DNS      72 Standard query 0x81b6 A www.ietf.org
```

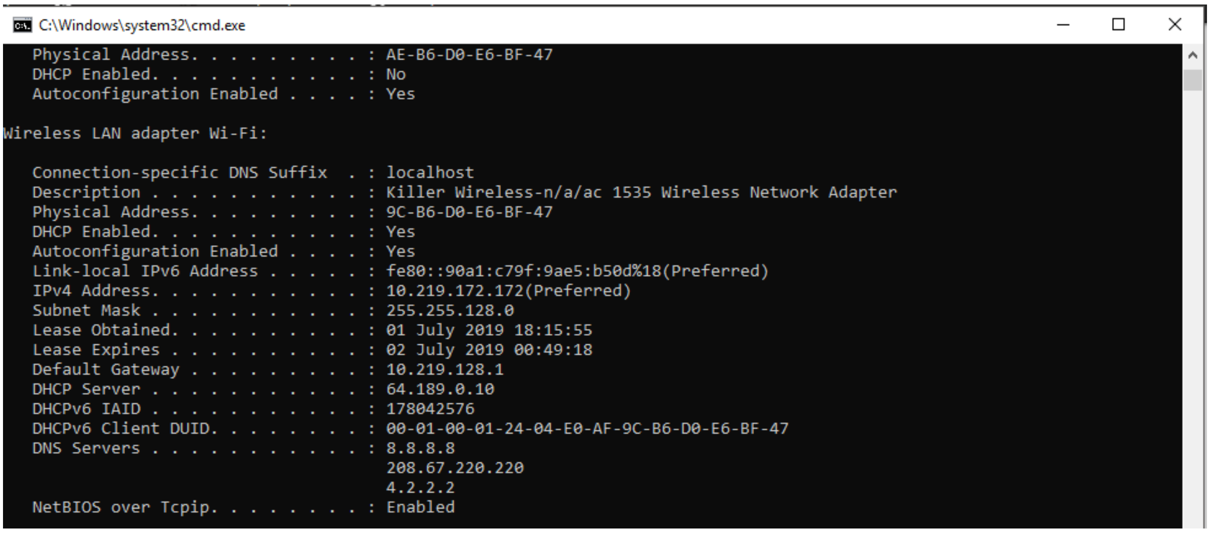
```
    Identification: 0xedfc (60924)
  > Flags: 0x4000, Don't fragment
    Time to live: 57
    Protocol: UDP (17)
    Header checksum: 0xeec1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 208.67.220.220
    Destination: 10.219.172.172
> User Datagram Protocol, Src Port: 53, Dst Port: 53230
v Domain Name System (response)
    Transaction ID: 0x81b6
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
```

They are sent over UDP.

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

The destination port for DNS query is 53 and the source port of DNS response is 53.

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?

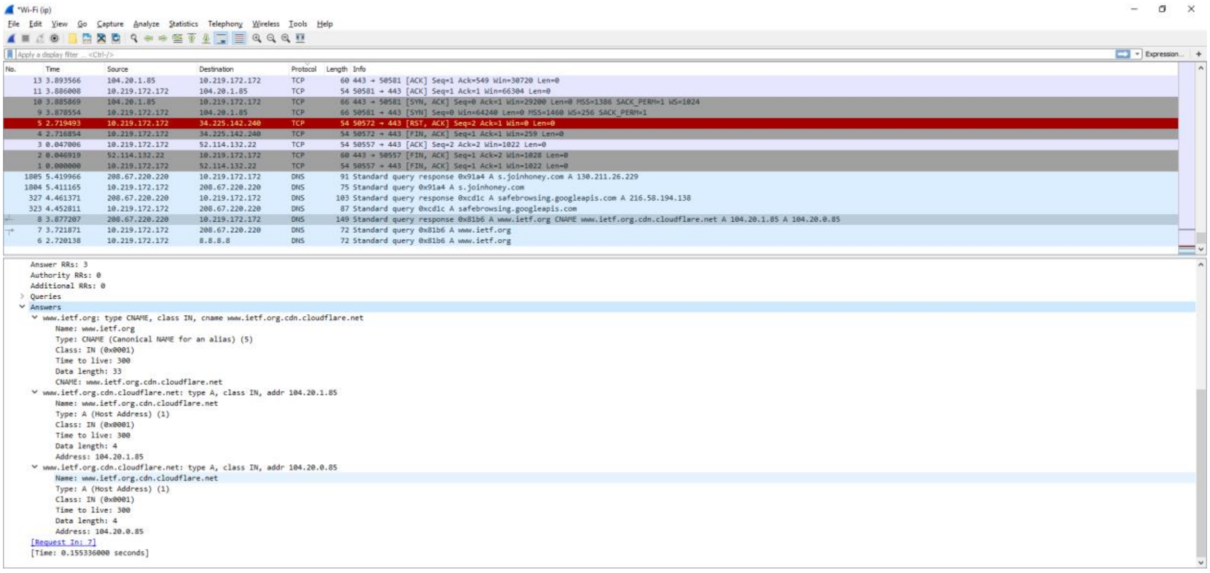


```
   Physical Address. . . . . . . . . : AE-B6-D0-E6-BF-47
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : localhost
   Description . . . . . . . . . . . : Killer Wireless-n/a/ac 1535 Wireless Network Adapter
   Physical Address. . . . . . . . . : 9C-B6-D0-E6-BF-47
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::90a1:c79f:9ae5:b50d%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.219.172.172(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.128.0
   Lease Obtained. . . . . . . . . . : 01 July 2019 18:15:55
   Lease Expires . . . . . . . . . . : 02 July 2019 00:49:18
   Default Gateway . . . . . . . . . : 10.219.128.1
   DHCP Server . . . . . . . . . . . : 64.189.0.10
   DHCPv6 IAID . . . . . . . . . . . : 178042576
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-04-E0-AF-9C-B6-D0-E6-BF-47
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       208.67.220.220
                                       4.2.2.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

It’s sent to 208.67.220.220, which is same as one of my DNS servers.

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
   It is a type A Standard Query and it does not contain any answers.

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



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

```
No.    Time      Source          Destination     Protocol Length Info
  13 3.893566    104.20.1.85     10.219.172.172  TCP       60 443 → 50581 [ACK] Seq=1 Ack=549 Win=30720 Len=0
  11 3.886008    10.219.172.172  104.20.1.85     TCP       54 50581 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
  10 3.885869    104.20.1.85     10.219.172.172  TCP       66 443 → 50581 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=1024
   9 3.878554    10.219.172.172  104.20.1.85     TCP       66 50581 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   5 2.719493    10.219.172.172  34.225.142.240  TCP       54 50572 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
   4 2.716854    10.219.172.172  34.225.142.240  TCP       54 50572 → 443 [FIN, ACK] Seq=1 Ack=1 Win=259 Len=0
   3 0.047006    10.219.172.172  52.114.132.22   TCP       54 50557 → 443 [ACK] Seq=2 Ack=2 Win=1022 Len=0
   2 0.046919    52.114.132.22   10.219.172.172  TCP       60 443 → 50557 [FIN, ACK] Seq=1 Ack=2 Win=1028 Len=0
   1 0.000000    10.219.172.172  52.114.132.22   TCP       54 50557 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
1805 5.419966    208.67.220.220  10.219.172.172  DNS       91 Standard query response 0x91a4 A s.joinhoney.com A 130.211.26.229
1804 5.411165    10.219.172.172  208.67.220.220  DNS       75 Standard query 0x91a4 A s.joinhoney.com
 327 4.461371    208.67.220.220  10.219.172.172  DNS      103 Standard query response 0xcd1c A safebrowsing.googleapis.com A 216.58.194.138
 323 4.452811    10.219.172.172  208.67.220.220  DNS       87 Standard query 0xcd1c A safebrowsing.googleapis.com
   8 3.877207    208.67.220.220  10.219.172.172  DNS      149 Standard query response 0x81b6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
   7 3.721871    10.219.172.172  208.67.220.220  DNS       72 Standard query 0x81b6 A www.ietf.org
   6 2.720138    10.219.172.172  8.8.8.8         DNS       72 Standard query 0x81b6 A www.ietf.org
```

```
    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: 300
          Data length: 33
          CNAME: www.ietf.org.cdn.cloudflare.net
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
          Name: www.ietf.org.cdn.cloudflare.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 300
          Data length: 4
          Address: 104.20.1.85
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
          Name: www.ietf.org.cdn.cloudflare.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 300
          Data length: 4
          Address: 104.20.0.85
    [Request In: 7]
    [Time: 0.155336000 seconds]
```

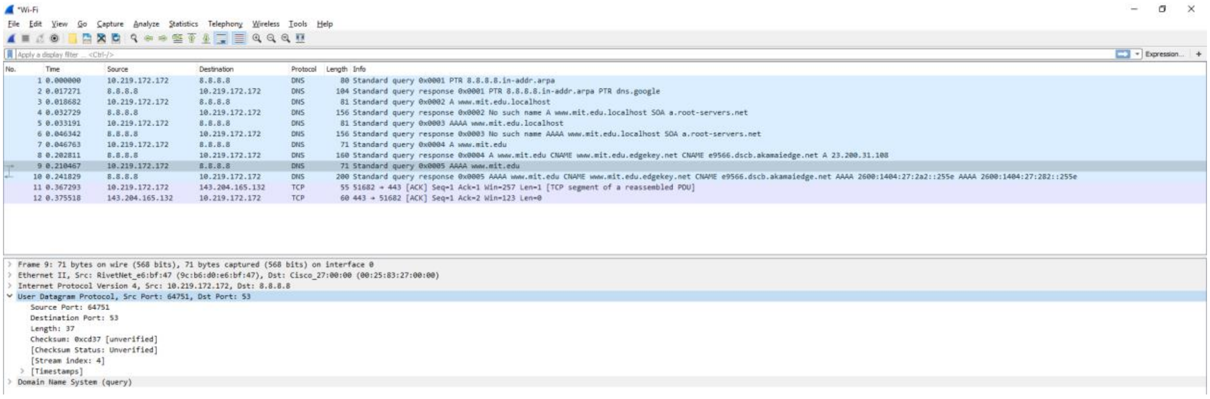
There were 3 answers containing information about the name of the host, type of address, class, the Time To Live (TTL), the data length and the IP.

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?
   The TCP SYN packet was sent to 104.20.1.85 which corresponds to the IP address provided in the DNS response message.

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    No.

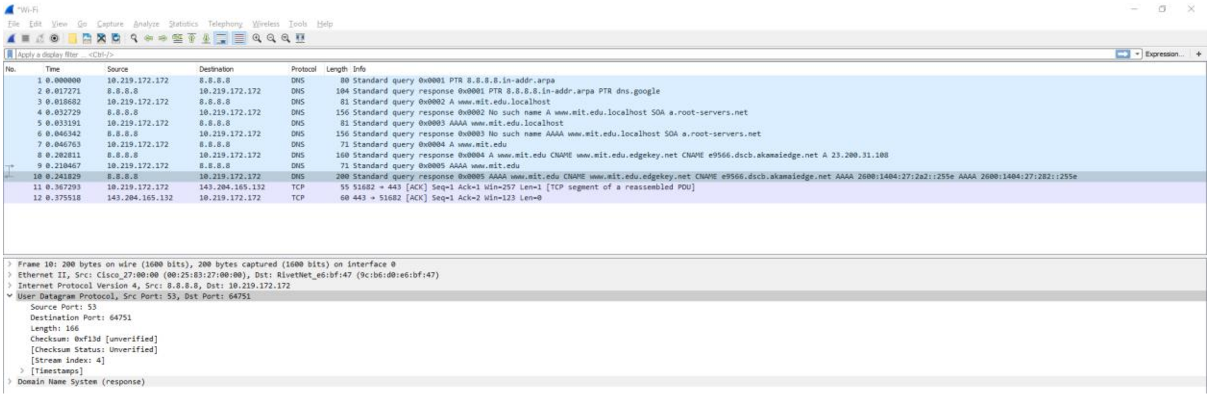
Part 3

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


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

```
No.  Time       Source            Destination       Protocol Length Info
   1 0.000000   10.219.172.172    8.8.8.8           DNS       80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
   2 0.017271   8.8.8.8           10.219.172.172    DNS      104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
   3 0.018682   10.219.172.172    8.8.8.8           DNS       81 Standard query 0x0002 A www.mit.edu.localhost
   4 0.032729   8.8.8.8           10.219.172.172    DNS      156 Standard query response 0x0002 No such name A www.mit.edu.localhost SOA a.root-servers.net
   5 0.033191   10.219.172.172    8.8.8.8           DNS       81 Standard query 0x0003 AAAA www.mit.edu.localhost
   6 0.046342   8.8.8.8           10.219.172.172    DNS      156 Standard query response 0x0003 No such name AAAA www.mit.edu.localhost SOA a.root-servers.net
   7 0.046763   10.219.172.172    8.8.8.8           DNS       71 Standard query 0x0004 A www.mit.edu
   8 0.202811   8.8.8.8           10.219.172.172    DNS      160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.200.31.108
   9 0.210467   10.219.172.172    8.8.8.8           DNS       71 Standard query 0x0005 AAAA www.mit.edu
  10 0.241829   8.8.8.8           10.219.172.172    DNS      200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1404:27:2a2::255e AAAA 2600:1404:27:282::255e
  11 0.367293   10.219.172.172    143.204.165.132   TCP       55 51682 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU]
  12 0.375518   143.204.165.132   10.219.172.172    TCP       60 443 → 51682 [ACK] Seq=1 Ack=2 Win=123 Len=0

> Frame 9: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: RivetNet_e6:bf:47 (9c:b6:d0:e6:bf:47), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
> Internet Protocol Version 4, Src: 10.219.172.172, Dst: 8.8.8.8
v User Datagram Protocol, Src Port: 64751, Dst Port: 53
    Source Port: 64751
    Destination Port: 53
    Length: 37
    Checksum: 0xcd37 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
> Domain Name System (query)
```

b) Response


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

```
No.  Time       Source            Destination       Protocol Length Info
   1 0.000000   10.219.172.172    8.8.8.8           DNS       80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
   2 0.017271   8.8.8.8           10.219.172.172    DNS      104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
   3 0.018682   10.219.172.172    8.8.8.8           DNS       81 Standard query 0x0002 A www.mit.edu.localhost
   4 0.032729   8.8.8.8           10.219.172.172    DNS      156 Standard query response 0x0002 No such name A www.mit.edu.localhost SOA a.root-servers.net
   5 0.033191   10.219.172.172    8.8.8.8           DNS       81 Standard query 0x0003 AAAA www.mit.edu.localhost
   6 0.046342   8.8.8.8           10.219.172.172    DNS      156 Standard query response 0x0003 No such name AAAA www.mit.edu.localhost SOA a.root-servers.net
   7 0.046763   10.219.172.172    8.8.8.8           DNS       71 Standard query 0x0004 A www.mit.edu
   8 0.202811   8.8.8.8           10.219.172.172    DNS      160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.200.31.108
   9 0.210467   10.219.172.172    8.8.8.8           DNS       71 Standard query 0x0005 AAAA www.mit.edu
  10 0.241829   8.8.8.8           10.219.172.172    DNS      200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1404:27:2a2::255e AAAA 2600:1404:27:282::255e
  11 0.367293   10.219.172.172    143.204.165.132   TCP       55 51682 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU]
  12 0.375518   143.204.165.132   10.219.172.172    TCP       60 443 → 51682 [ACK] Seq=1 Ack=2 Win=123 Len=0

> Frame 10: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface 0
> Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: RivetNet_e6:bf:47 (9c:b6:d0:e6:bf:47)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.219.172.172
v User Datagram Protocol, Src Port: 53, Dst Port: 64751
    Source Port: 53
    Destination Port: 64751
    Length: 166
    Checksum: 0xf13d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
> Domain Name System (response)
```

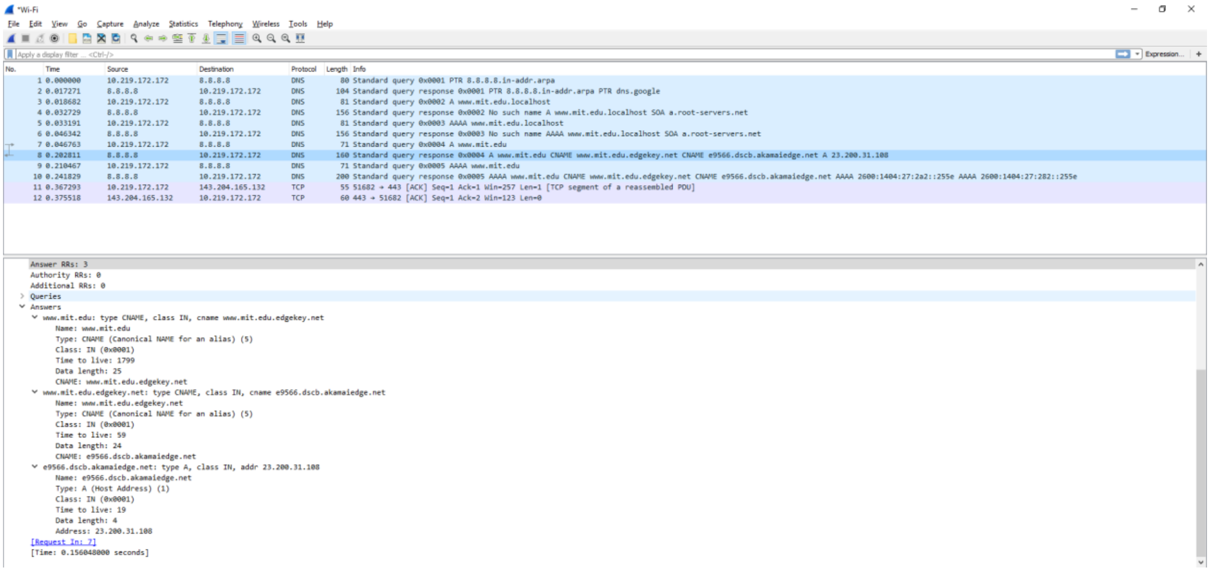
The destination port for DNS query is 53 and the source port of DNS response is 53.

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    It's sent to 8.8.8.8, which is same as one of my DNS servers.

13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    The query is of type A and it does not contain any answers.

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
    There were 3 answers containing information about the name of the host, type of address, class, the Time To Live (TTL), the data length and the IP.

15. Provide a Screenshot


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

```
No.   Time       Source            Destination       Protocol  Length  Info
    1 0.000000   10.219.172.172    8.8.8.8           DNS        80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
    2 0.017271   8.8.8.8           10.219.172.172    DNS       104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
    3 0.018682   10.219.172.172    8.8.8.8           DNS        81 Standard query 0x0002 A www.mit.edu.localhost
    4 0.032729   8.8.8.8           10.219.172.172    DNS       156 Standard query response 0x0002 No such name A www.mit.edu.localhost SOA a.root-servers.net
    5 0.033191   10.219.172.172    8.8.8.8           DNS        81 Standard query 0x0003 AAAA www.mit.edu.localhost
    6 0.046342   8.8.8.8           10.219.172.172    DNS       156 Standard query response 0x0003 No such name AAAA www.mit.edu.localhost SOA a.root-servers.net
    7 0.046763   10.219.172.172    8.8.8.8           DNS        71 Standard query 0x0004 A www.mit.edu
    8 0.202811   8.8.8.8           10.219.172.172    DNS       160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.200.31.108
    9 0.210467   10.219.172.172    8.8.8.8           DNS        71 Standard query 0x0005 AAAA www.mit.edu
   10 0.241829   8.8.8.8           10.219.172.172    DNS       200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1404:27:2a2::255e AAAA 2600:1404:27:282::255e
   11 0.367293   10.219.172.172    143.204.165.132   TCP        55 51682 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU]
   12 0.375518   143.204.165.132   10.219.172.172    TCP        60 443 → 51682 [ACK] Seq=1 Ack=2 Win=123 Len=0
```

```
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  ˅ 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: 1799
          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: 59
          Data length: 24
          CNAME: e9566.dscb.akamaiedge.net
    ˅ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.200.31.108
          Name: e9566.dscb.akamaiedge.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 19
          Data length: 4
          Address: 23.200.31.108
    [Request In: 7]
    [Time: 0.156048000 seconds]
```

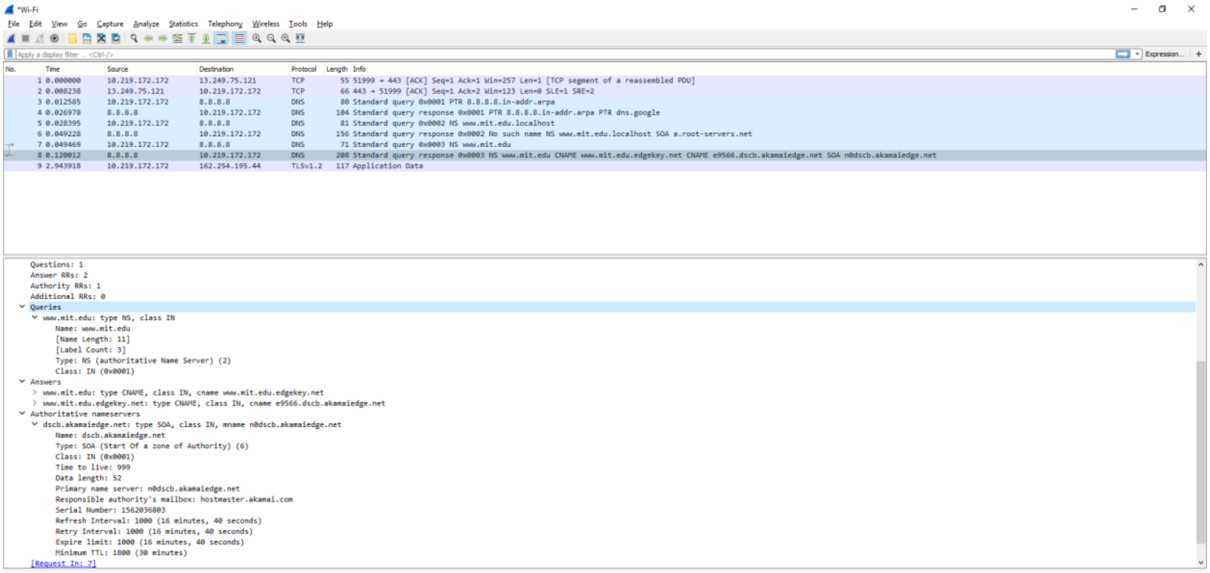
Part 4

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    It’s sent to 8.8.8.8, which is same as one of my DNS servers.

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    The query is of type NS and it does not contain any answers.

18. 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 namesers?
    The primary name server is n0dscb.akamaiedge.net. The response does not provide the IP address of the nameserver.

19. Provide a screenshot.


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

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  10.219.172.172  13.249.75.121   TCP       55 51999 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU]
   2 0.008238  13.249.75.121   10.219.172.172  TCP       66 443 → 51999 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
   3 0.012585  10.219.172.172  8.8.8.8         DNS       80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
   4 0.026978  8.8.8.8         10.219.172.172  DNS      104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
   5 0.028395  10.219.172.172  8.8.8.8         DNS       81 Standard query 0x0002 NS www.mit.edu.localhost
   6 0.049228  8.8.8.8         10.219.172.172  DNS      156 Standard query response 0x0002 No such name NS www.mit.edu.localhost SOA a.root-servers.net
   7 0.049469  10.219.172.172  8.8.8.8         DNS       71 Standard query 0x0003 NS www.mit.edu
   8 0.120012  8.8.8.8         10.219.172.172  DNS      208 Standard query response 0x0003 NS www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net SOA n0dscb.akamaiedge.net
   9 2.943918  10.219.172.172  162.254.195.44  TLSv1.2  117 Application Data
```

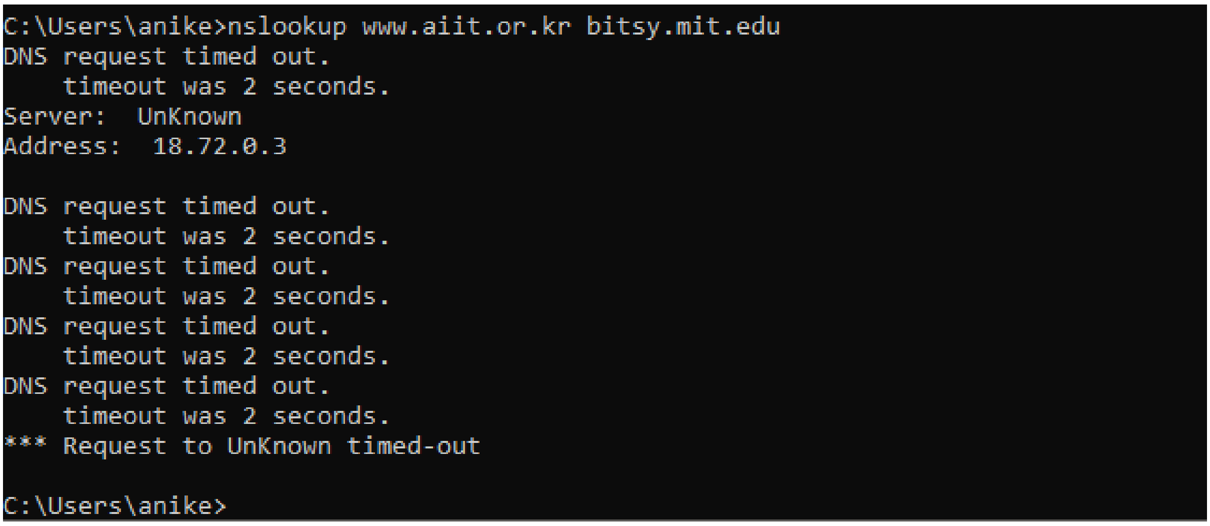
```
    Questions: 1
    Answer RRs: 2
    Authority RRs: 1
    Additional RRs: 0
  ˅ Queries
    ˅ www.mit.edu: type NS, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ˅ Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  ˅ Authoritative nameservers
    ˅ dscb.akamaiedge.net: type SOA, class IN, mname n0dscb.akamaiedge.net
        Name: dscb.akamaiedge.net
        Type: SOA (Start Of a zone of Authority) (6)
        Class: IN (0x0001)
        Time to live: 999
        Data length: 52
        Primary name server: n0dscb.akamaiedge.net
        Responsible authority's mailbox: hostmaster.akamai.com
        Serial Number: 1562036803
        Refresh Interval: 1000 (16 minutes, 40 seconds)
        Retry Interval: 1000 (16 minutes, 40 seconds)
        Expire limit: 1000 (16 minutes, 40 seconds)
        Minimum TTL: 1800 (30 minutes)
    [Request In: 7]
```

Part 5

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?
The query is initially sent to 8.8.8.8 then sent to 18.72.0.3 which corresponds to bitsy.mit.edu.

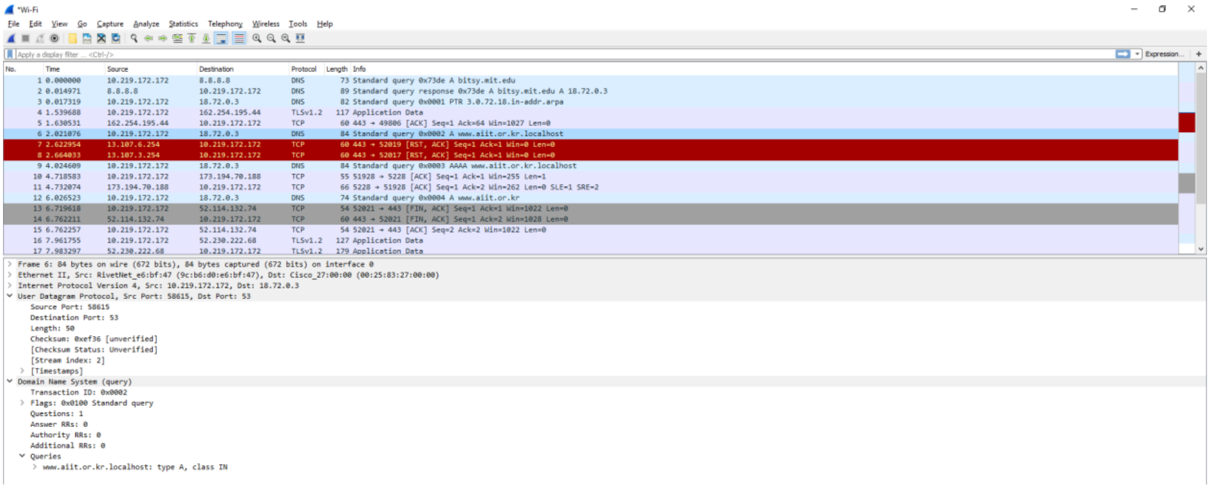
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
It's a standard type A query that doesn't contain any answers.

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
The DNS request was timed out and no response was received. (As shown in the screenshot below)



```
C:\Users\anike>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.72.0.3

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

C:\Users\anike>
```

23. Provide a Screenshot.



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

```
No.     Time        Source            Destination       Protocol  Length Info
      1 0.000000    10.219.172.172    8.8.8.8           DNS           73 Standard query 0x73de A bitsy.mit.edu
      2 0.014971    8.8.8.8           10.219.172.172    DNS           89 Standard query response 0x73de A bitsy.mit.edu A 18.72.0.3
      3 0.017319    10.219.172.172    18.72.0.3         DNS           82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
      4 1.539688    10.219.172.172    162.254.195.44    TLSv1.2      117 Application Data
      5 1.630531    162.254.195.44    10.219.172.172    TCP           60 443 → 49806 [ACK] Seq=1 Ack=64 Win=1027 Len=0
      6 2.021076    10.219.172.172    18.72.0.3         DNS           84 Standard query 0x0002 A www.aiit.or.kr.localhost
      7 2.622954    13.107.6.254      10.219.172.172    TCP           60 443 → 52019 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
      8 2.664033    13.107.3.254      10.219.172.172    TCP           60 443 → 52017 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
      9 4.024609    10.219.172.172    18.72.0.3         DNS           84 Standard query 0x0003 AAAA www.aiit.or.kr.localhost
     10 4.718583    10.219.172.172    173.194.70.188    TCP           55 51928 → 5228 [ACK] Seq=1 Ack=1 Win=255 Len=1
     11 4.732074    173.194.70.188    10.219.172.172    TCP           66 5228 → 51928 [ACK] Seq=1 Ack=2 Win=262 Len=0 SLE=1 SRE=2
     12 6.026523    10.219.172.172    18.72.0.3         DNS           74 Standard query 0x0004 A www.aiit.or.kr
     13 6.719618    10.219.172.172    52.114.132.74     TCP           54 52021 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
     14 6.762211    52.114.132.74     10.219.172.172    TCP           60 443 → 52021 [FIN, ACK] Seq=1 Ack=2 Win=1028 Len=0
     15 6.762257    10.219.172.172    52.114.132.74     TCP           54 52021 → 443 [ACK] Seq=2 Ack=2 Win=1022 Len=0
     16 7.961755    10.219.172.172    52.230.222.68     TLSv1.2      127 Application Data
     17 7.983297    52.230.222.68     10.219.172.172    TLSv1.2      179 Application Data
```

```
> Frame 6: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: RivetNet_e6:bf:47 (9c:b6:d0:e6:bf:47), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
> Internet Protocol Version 4, Src: 10.219.172.172, Dst: 18.72.0.3
v User Datagram Protocol, Src Port: 58615, Dst Port: 53
    Source Port: 58615
    Destination Port: 53
    Length: 50
    Checksum: 0xef36 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
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
    > www.aiit.or.kr.localhost: type A, class IN
```