Assignment-04

Submitted to :

Prof.Dr.Md Shariful Islam

Institute of Information Technology

University of Dhaka

Submitted by :

Md.Farhan Islam Shuvro

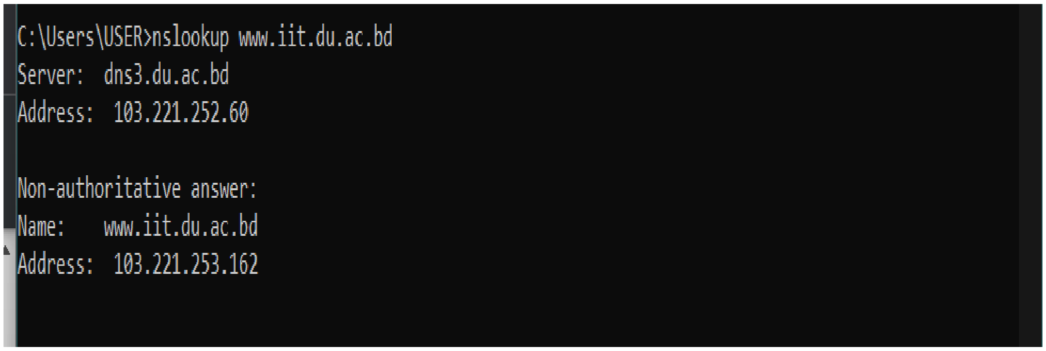
Roll: 1303

Institute of Information Technology

University of Dhaka

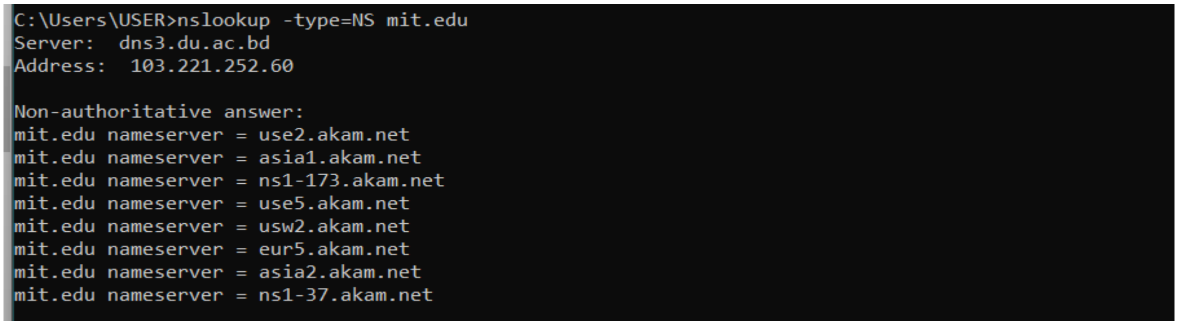
Answer to the question about NSLOOKUP

1. I performed nslookup for www.iit.du.ac.bd It’s Ip address is 103.221.252.60



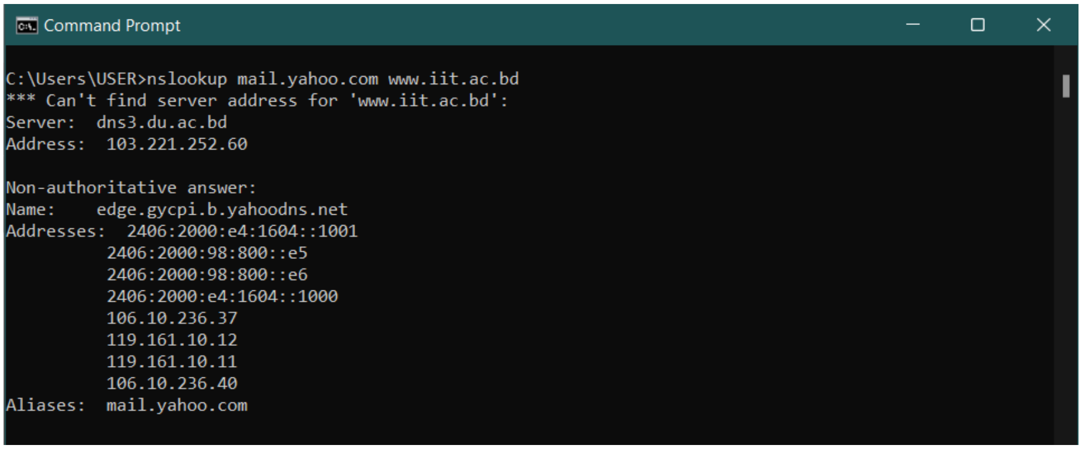
```
C:\Users\USER>nslookup www.iit.du.ac.bd
Server:  dns3.du.ac.bd
Address:  103.221.252.60

Non-authoritative answer:
Name:    www.iit.du.ac.bd
Address:  103.221.253.162
```

2. I performed nslookup for a European University MIT. Its IP address is 103.221.252.60



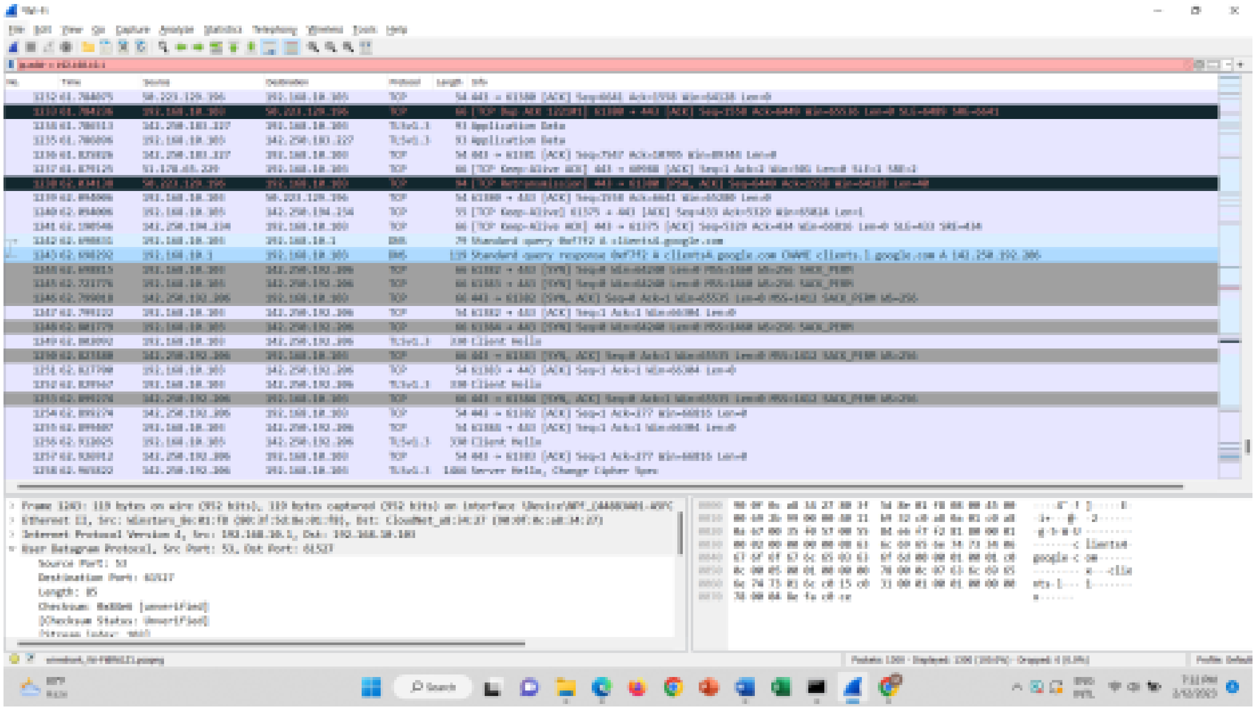
```
C:\Users\USER>nslookup -type=NS mit.edu
Server:  dns3.du.ac.bd
Address:  103.221.252.60

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

3. The Ip address of the mail server is:



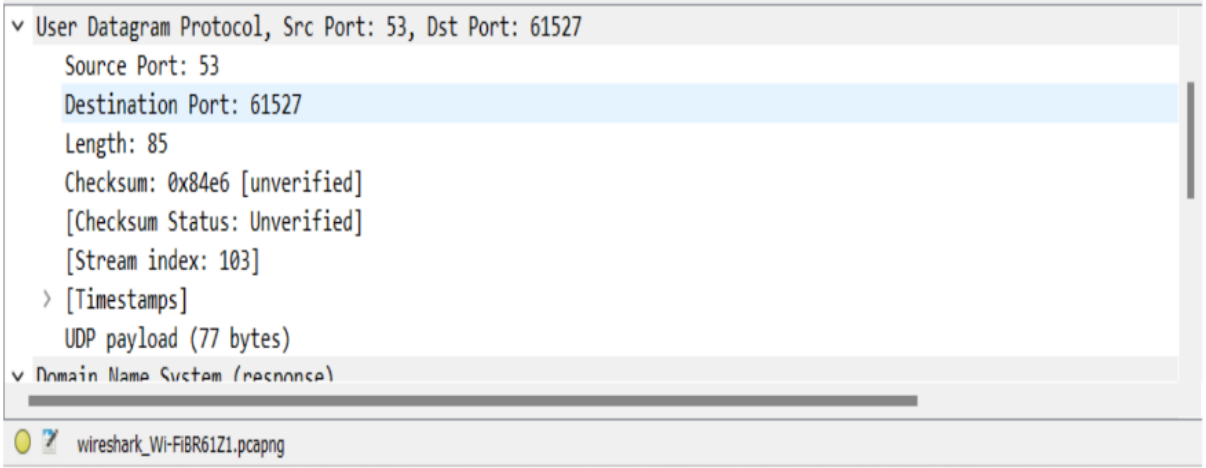
```
C:\Users\USER>nslookup mail.yahoo.com www.iit.ac.bd
*** Can't find server address for 'www.iit.ac.bd':
Server:  dns3.du.ac.bd
Address:  103.221.252.60

Non-authoritative answer:
Name:    edge.gycpi.b.yahoodns.net
Addresses:  2406:2000:e4:1604::1001
          2406:2000:98:800::e5
          2406:2000:98:800::e6
          2406:2000:e4:1604::1000
          106.10.236.37
          119.161.10.12
          119.161.10.11
          106.10.236.40
Aliases:  mail.yahoo.com
```

Answer to question about IPCONFIG



4. They are sent over UDP.

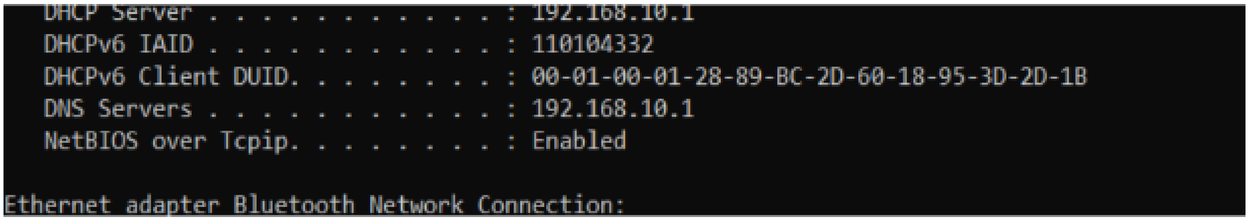
5. The destination port for the DNS quarry is 53 & the source port of the DNS response is 53.



```
v User Datagram Protocol, Src Port: 53, Dst Port: 61527
    Source Port: 53
    Destination Port: 61527
    Length: 85
    Checksum: 0x84e6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 103]
  > [Timestamps]
    UDP payload (77 bytes)
v Domain Name System (response)
```

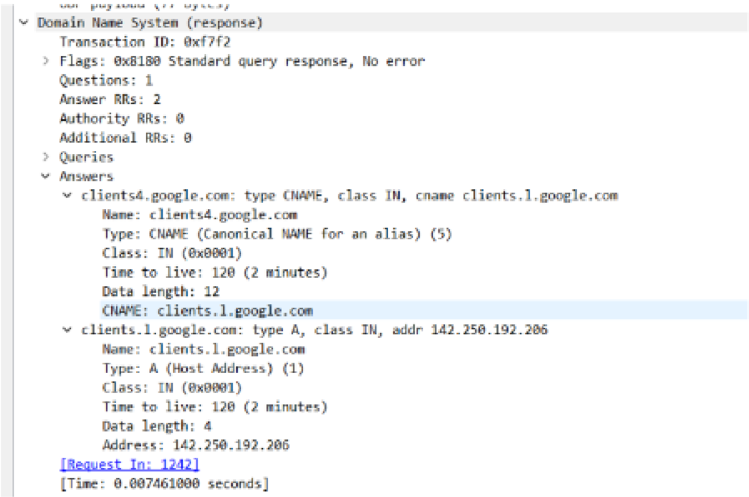
wireshark_Wi-FiBR61Z1.pcapng

6. It’s sent to 192.168.10.1, which is the Ip address of one of my local DNS servers.



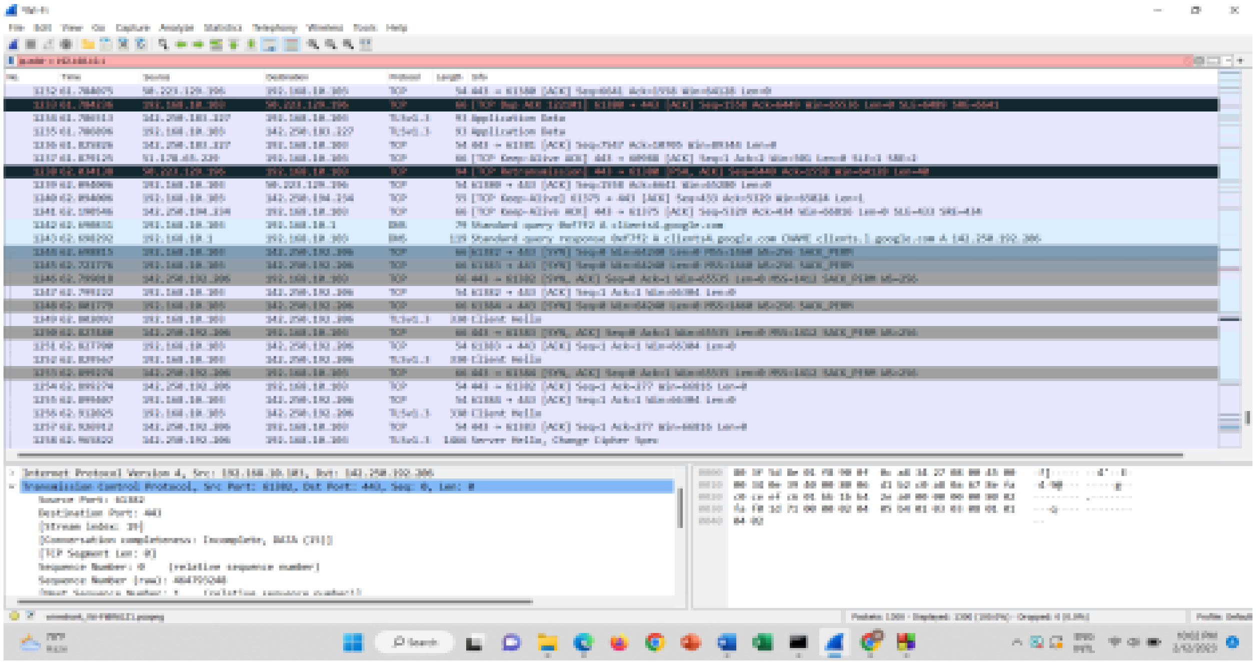
```
    DHCP Server . . . . . . . . . . . . . : 192.168.10.1
    DHCPv6 IAID . . . . . . . . . . . . . : 110104332
    DHCPv6 Client DUID. . . . . . . . . . : 00-01-00-01-28-89-BC-2D-60-18-95-3D-2D-1B
    DNS Servers . . . . . . . . . . . . . : 192.168.10.1
    NetBIOS over Tcpip. . . . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
```

7. It’s a type A standard query & does not contain any answers. 8. There are two answers containing various information.

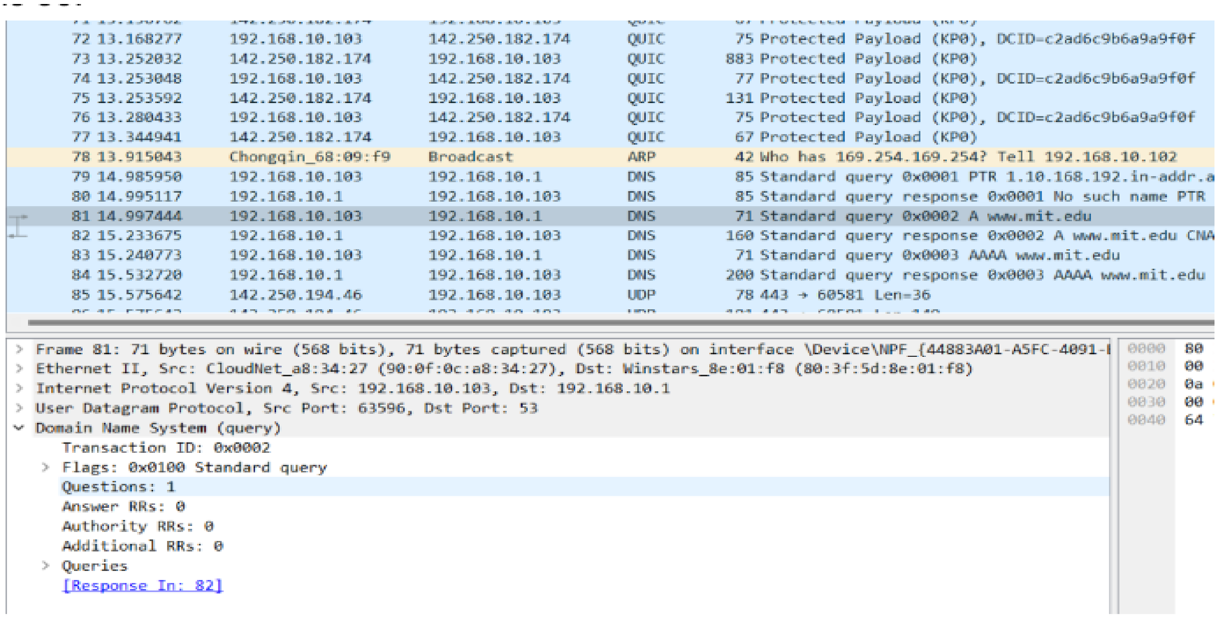


```
v Domain Name System (response)
    Transaction ID: 0xf7f2
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v clients4.google.com: type CNAME, class IN, cname clients.l.google.com
          Name: clients4.google.com
          Type: CNAME (Canonical NAME for an alias) (5)
          Class: IN (0x0001)
          Time to live: 120 (2 minutes)
          Data length: 12
          CNAME: clients.l.google.com
    v clients.l.google.com: type A, class IN, addr 142.250.192.206
          Name: clients.l.google.com
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 120 (2 minutes)
          Data length: 4
          Address: 142.250.192.206
    [Request In: 1242]
    [Time: 0.007461000 seconds]
```

9. The first TCP SYN packet was sent to 142.250.192.206 which corresponds to the first IP address provided in the DNS response message.



10. NO.
11. The destination port of the DNS query is 53 & the source port of the DNS response is 53.



```
72 13.168277   192.168.10.103      142.250.182.174   QUIC    75 Protected Payload (KP0), DCID=c2ad6c9b6a9a9f0f
73 13.252032   142.250.182.174     192.168.10.103    QUIC   883 Protected Payload (KP0)
74 13.253048   192.168.10.103      142.250.182.174   QUIC    77 Protected Payload (KP0), DCID=c2ad6c9b6a9a9f0f
75 13.253592   142.250.182.174     192.168.10.103    QUIC   131 Protected Payload (KP0)
76 13.280433   192.168.10.103      142.250.182.174   QUIC    75 Protected Payload (KP0), DCID=c2ad6c9b6a9a9f0f
77 13.344941   142.250.182.174     192.168.10.103    QUIC    67 Protected Payload (KP0)
78 13.915043   Chongqin_68:09:f9   Broadcast         ARP     42 Who has 169.254.169.254? Tell 192.168.10.102
79 14.985950   192.168.10.103      192.168.10.1      DNS     85 Standard query 0x0001 PTR 1.10.168.192.in-addr.a
80 14.995117   192.168.10.1        192.168.10.103    DNS     85 Standard query response 0x0001 No such name PTR
81 14.997444   192.168.10.103      192.168.10.1      DNS     71 Standard query 0x0002 A www.mit.edu
82 15.233675   192.168.10.1        192.168.10.103    DNS    160 Standard query response 0x0002 A www.mit.edu CNA
83 15.240773   192.168.10.103      192.168.10.1      DNS     71 Standard query 0x0003 AAAA www.mit.edu
84 15.532720   192.168.10.1        192.168.10.103    DNS    200 Standard query response 0x0003 AAAA www.mit.edu
85 15.575642   142.250.194.46      192.168.10.103    UDP     78 443 → 60581 Len=36
```

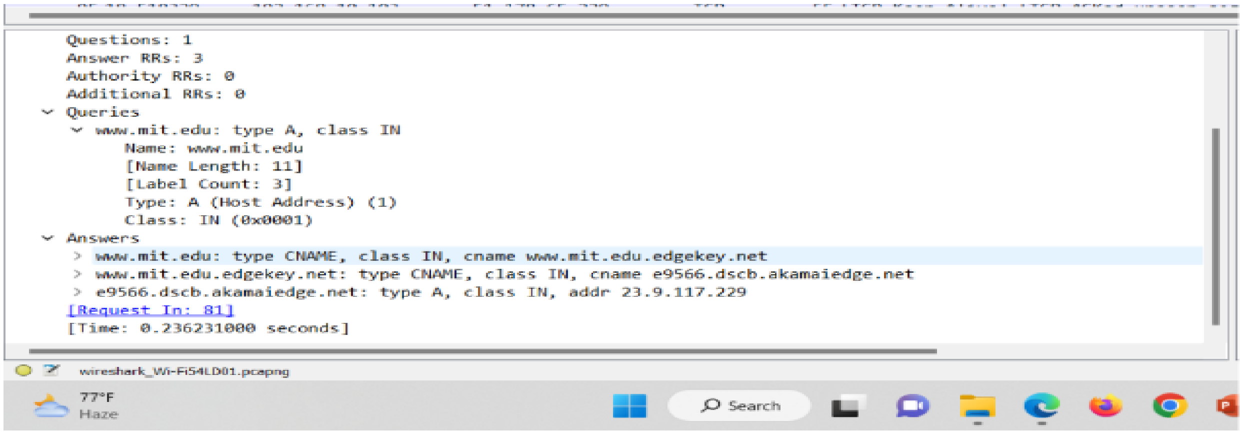
```
> Frame 81: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{44883A01-A5FC-4091-
> Ethernet II, Src: CloudNet_a8:34:27 (90:0f:0c:a8:34:27), Dst: Winstars_8e:01:f8 (80:3f:5d:8e:01:f8)
> Internet Protocol Version 4, Src: 192.168.10.103, Dst: 192.168.10.1
> User Datagram Protocol, Src Port: 63596, 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
  > Queries
    [Response In: 82]
```

```
0000  80
0010  00
0020  0a
0030  00
0040  64
```

12. It is sent to 192.168.10.1. As we can see from the ipconfig -all screenshots are the default local DNS server.

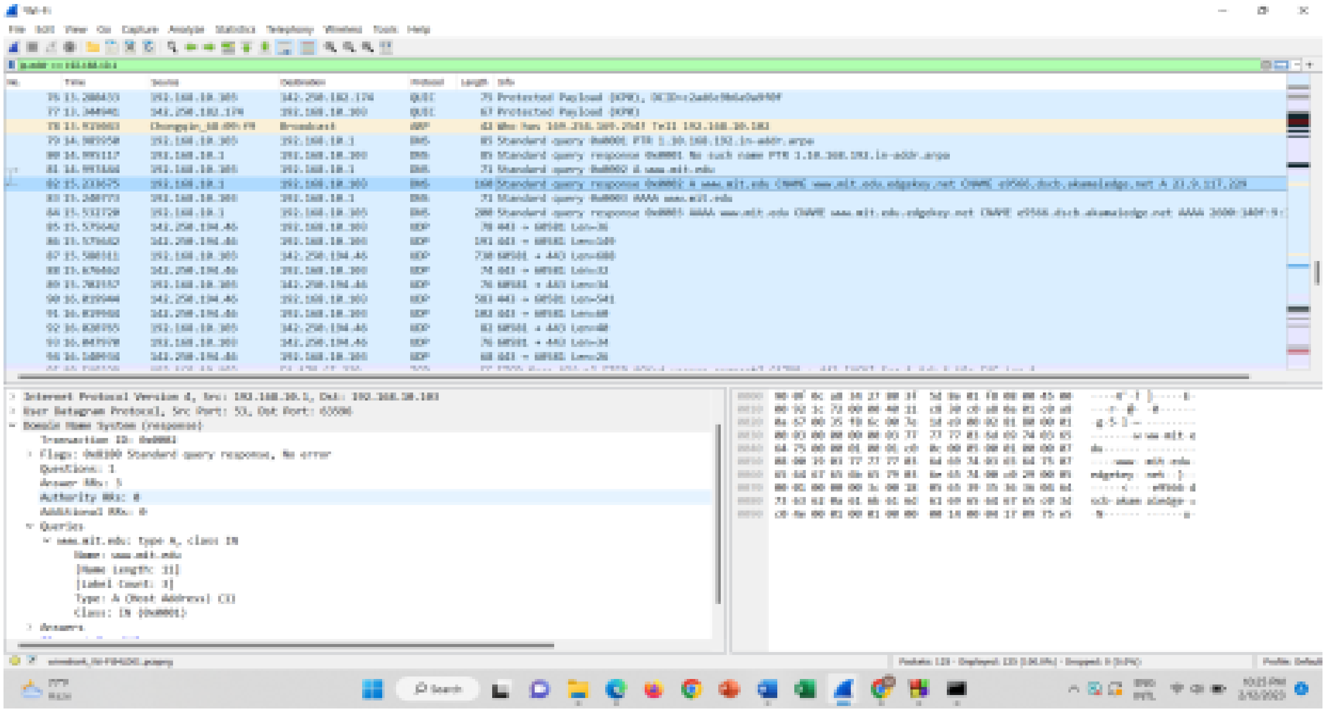
13. The query is of type A & it does not contain any answers.

14. The response DNS message contains three answers containing such information.



```
    Questions: 1
    Answer RRs: 3
    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)
  v 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
    > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.9.117.229
    [Request In: 81]
    [Time: 0.236231000 seconds]
```

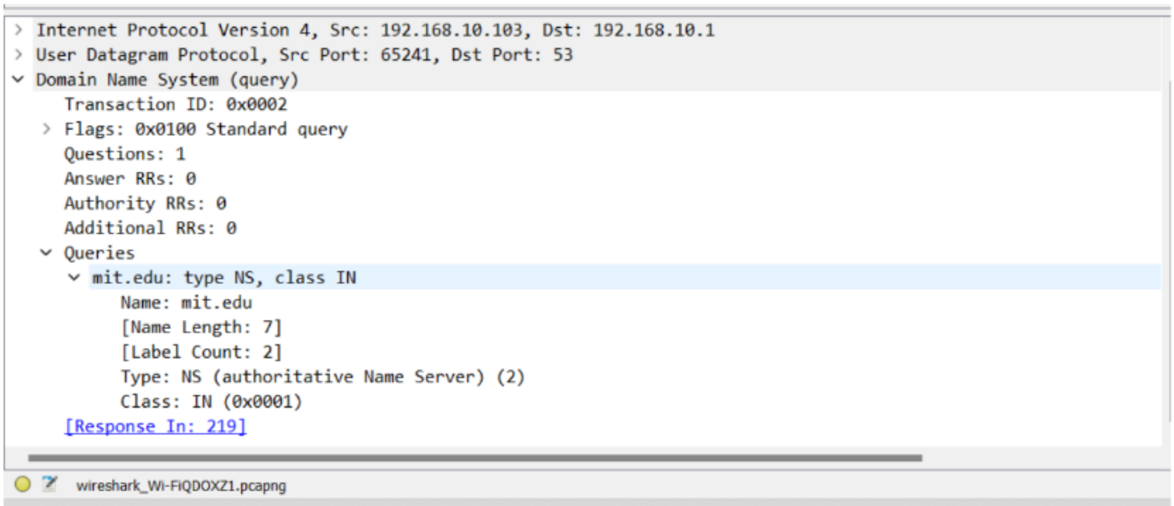
15.



```
> Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.103
> User Datagram Protocol, Src Port: 53, Dst Port: 63508
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    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)
  > Answers
```

16. It was sent to 192.168.10.1 which is my default DNS server.

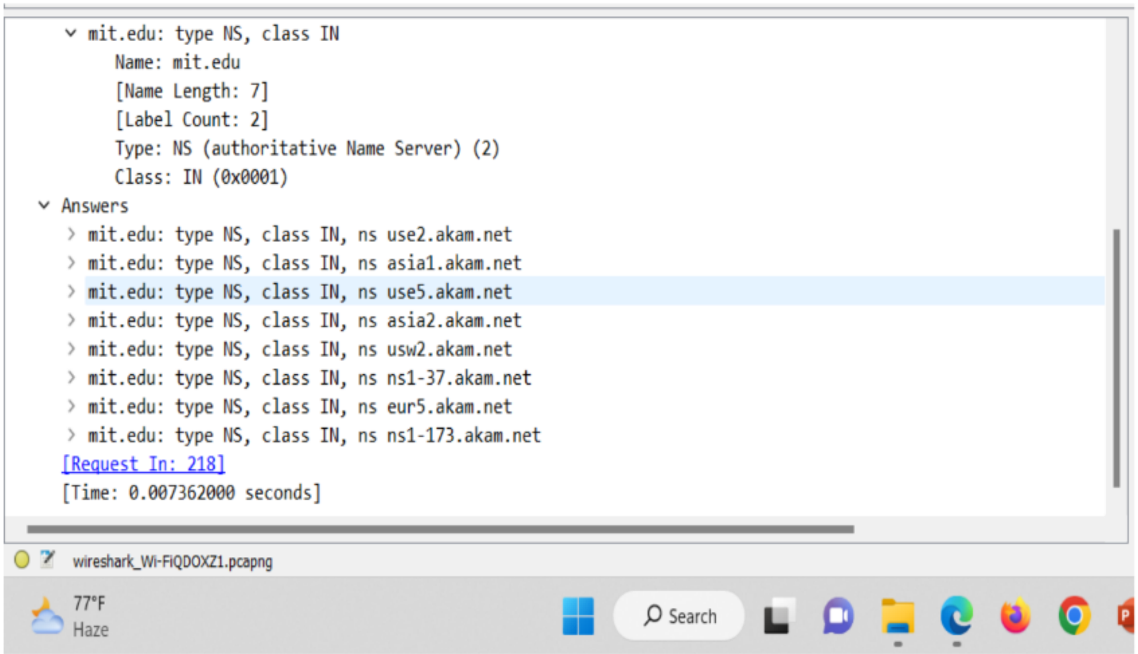
17. It’s a type of NS DNS query containing no answers.



```
> Internet Protocol Version 4, Src: 192.168.10.103, Dst: 192.168.10.1
> User Datagram Protocol, Src Port: 65241, 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: 219]
```

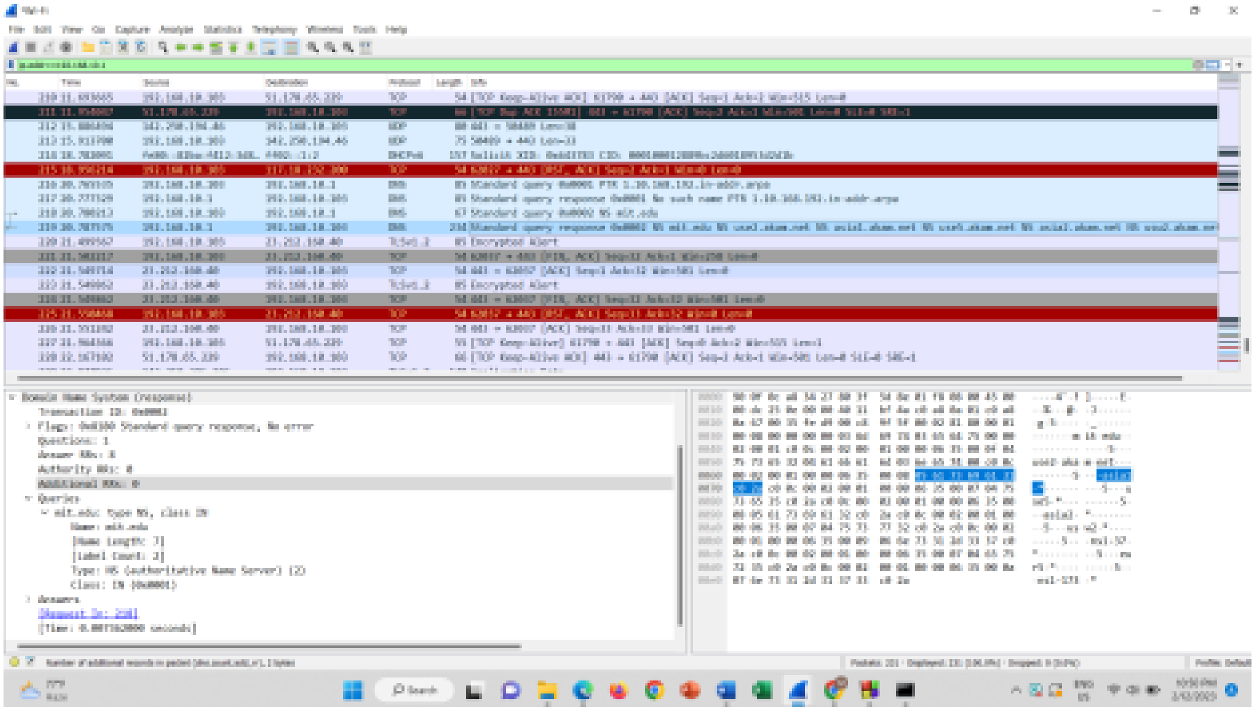
wireshark_Wi-FiQDOXZ1.pcapng

18. The nameservers are use2, asia1, use5, asia2, usw2, ns1-37, eur5, ns1-173. There are no additional records, so we cannot find their IP address.



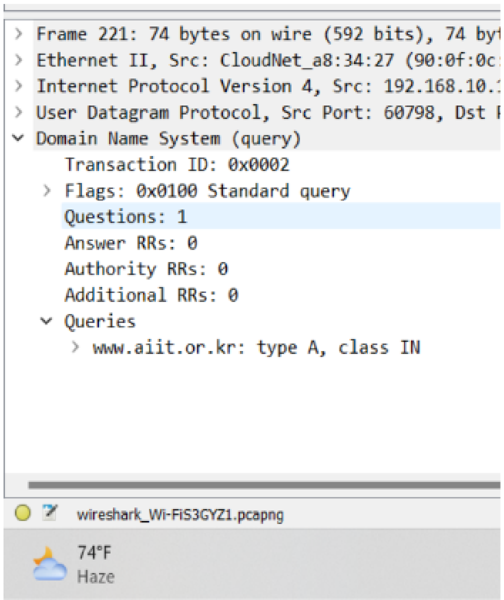
```
    ˅ mit.edu: type NS, class IN
          Name: mit.edu
          [Name Length: 7]
          [Label Count: 2]
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
  ˅ Answers
    › mit.edu: type NS, class IN, ns use2.akam.net
    › mit.edu: type NS, class IN, ns asia1.akam.net
    › mit.edu: type NS, class IN, ns use5.akam.net
    › mit.edu: type NS, class IN, ns asia2.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 eur5.akam.net
    › mit.edu: type NS, class IN, ns ns1-173.akam.net
  [Request In: 218]
  [Time: 0.007362000 seconds]
```

19.



```
˅ 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
    ˅ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  › Answers
    [Request In: 218]
    [Time: 0.007362000 seconds]
```

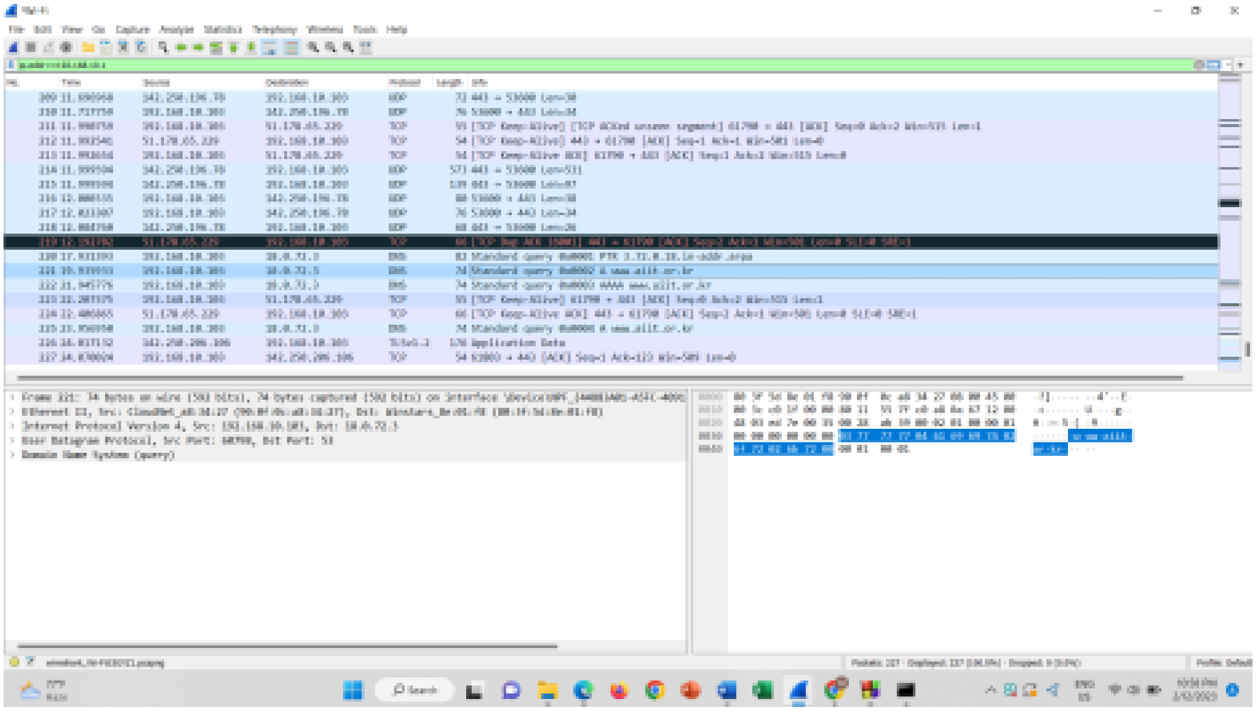
20. The query is sent to 18.0.72.3.
21. It is a standard type A query that does not contain any answer.



```
> Frame 221: 74 bytes on wire (592 bits), 74 byt
> Ethernet II, Src: CloudNet_a8:34:27 (90:0f:0c
> Internet Protocol Version 4, Src: 192.168.10.
> User Datagram Protocol, Src Port: 60798, Dst P
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: type A, class IN
```

22. There are two answers provided in the DNS response message

23.



```
No.  Time          Source           Destination      Protocol  Length  Info
209  11.690968     142.250.196.78   192.168.10.103   UDP        72  443 → 53600 Len=30
210  11.717750     192.168.10.103   142.250.196.78   UDP        76  53600 → 443 Len=34
211  11.990759     192.168.10.103   51.178.65.220    TCP        55  [TCP Keep-Alive] [TCP ACKed unseen segment] 61790 → 443 [ACK] Seq=0 Ack=2 Win=515 Len=1
212  11.992540     51.178.65.220    192.168.10.103   TCP        54  [TCP Keep-Alive] 443 → 61790 [ACK] Seq=1 Ack=1 Win=501 Len=0
213  11.992658     192.168.10.103   51.178.65.220    TCP        54  [TCP Keep-Alive ACK] 61790 → 443 [ACK] Seq=1 Ack=2 Win=515 Len=0
214  11.999504     142.250.196.78   192.168.10.103   UDP       573  443 → 53600 Len=531
215  11.999990     142.250.196.78   192.168.10.103   UDP       139  443 → 53600 Len=97
216  12.000135     192.168.10.103   142.250.196.78   UDP        80  53600 → 443 Len=38
217  12.023307     192.168.10.103   142.250.196.78   UDP        76  53600 → 443 Len=34
218  12.068760     142.250.196.78   192.168.10.103   UDP        68  443 → 53600 Len=26
219  12.[illegible] 51.178.65.220   192.168.10.103   TCP        66  [TCP Dup ACK 150#1] 443 → 61790 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
220  17.931393     192.168.10.103   10.0.72.3        DNS        83  Standard query 0x0001 PTR 3.72.0.10.in-addr.arpa
221  19.939933     192.168.10.103   10.0.72.3        DNS        74  Standard query 0x0002 A www.aiit.or.kr
222  21.945776     192.168.10.103   10.0.72.3        DNS        74  Standard query 0x0003 AAAA www.aiit.or.kr
223  22.207375     192.168.10.103   51.178.65.220    TCP        55  [TCP Keep-Alive] 61790 → 443 [ACK] Seq=0 Ack=2 Win=515 Len=1
224  22.400865     51.178.65.220    192.168.10.103   TCP        66  [TCP Keep-Alive ACK] 443 → 61790 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
225  23.950950     192.168.10.103   10.0.72.3        DNS        74  Standard query 0x0004 A www.aiit.or.kr
226  24.037132     142.250.206.106  192.168.10.103   TLSv1.2   176  Application Data
227  34.070024     192.168.10.103   142.250.206.106  TCP        54  63003 → 443 [ACK] Seq=1 Ack=123 Win=509 Len=0
```

```
> Frame 221: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{[illegible]}
> Ethernet II, Src: CloudNet_a8:34:27 ([illegible]), Dst: Winstars_8e:01:f8 ([illegible])
> Internet Protocol Version 4, Src: 192.168.10.103, Dst: 10.0.72.3
> User Datagram Protocol, Src Port: 60790, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 1f 5d 8e 01 f8 90 0f  8c a8 34 27 08 00 45 00   ..].......4'..E.
0010  00 3c c0 1f 00 00 80 11  55 7f c0 a8 0a 67 12 00   .<......U....g..
0020  48 03 ed 7e 00 35 00 28  ab 39 00 02 01 00 00 01   H..~.5.(.9......
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   .......www.aiit.
0040  6f 72 02 6b 72 00 00 01  00 01                     or.kr.....
```

Packets: 227 · Displayed: 227 (100.0%) · Dropped: 0 (0.0%)

Profile: Default