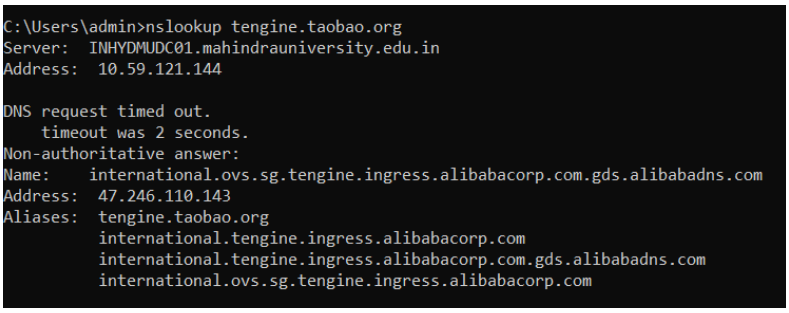
Computer Networks - Lab 3

Bhuvana Kanakam - SE21UCSE035

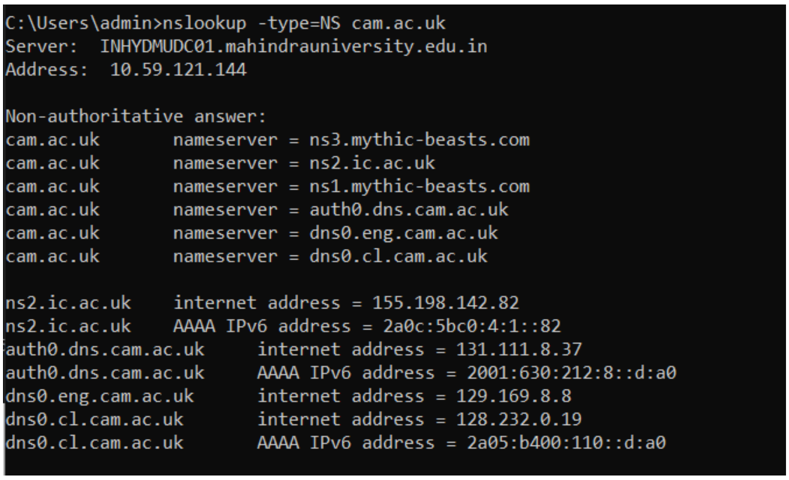
nslookup

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
I performed nslookup for tengine.taobao.org Its IP address is 47.246.110.143



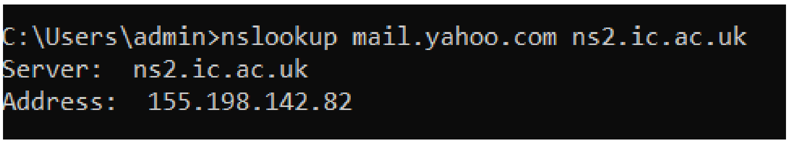
```
C:\Users\admin>nslookup tengine.taobao.org
Server:  INHYDMUDC01.mahindrauniversity.edu.in
Address:  10.59.121.144

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    international.ovs.sg.tengine.ingress.alibabacorp.com.gds.alibabadns.com
Address:  47.246.110.143
Aliases:  tengine.taobao.org
          international.tengine.ingress.alibabacorp.com
          international.tengine.ingress.alibabacorp.com.gds.alibabadns.com
          international.ovs.sg.tengine.ingress.alibabacorp.com
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
I performed nslookup for a European University - Cambridge Universiy. Its IP address is 155.198.142.82



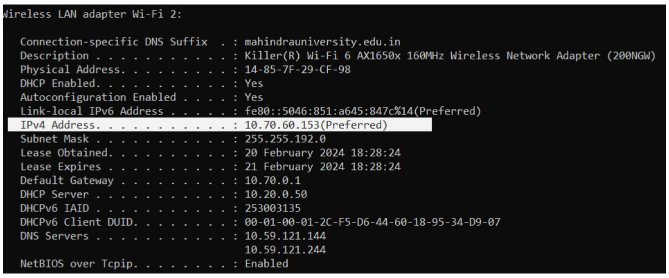
```
C:\Users\admin>nslookup -type=NS cam.ac.uk
Server:  INHYDMUDC01.mahindrauniversity.edu.in
Address:  10.59.121.144

Non-authoritative answer:
cam.ac.uk       nameserver = ns3.mythic-beasts.com
cam.ac.uk       nameserver = ns2.ic.ac.uk
cam.ac.uk       nameserver = ns1.mythic-beasts.com
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk

ns2.ic.ac.uk    internet address = 155.198.142.82
ns2.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk     internet address = 131.111.8.37
auth0.dns.cam.ac.uk     AAAA IPv6 address = 2001:630:212:8::d:a0
dns0.eng.cam.ac.uk      internet address = 129.169.8.8
dns0.cl.cam.ac.uk       internet address = 128.232.0.19
dns0.cl.cam.ac.uk       AAAA IPv6 address = 2a05:b400:110::d:a0
```

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?
The IP address is 155.198.142.82



```
C:\Users\admin>nslookup mail.yahoo.com ns2.ic.ac.uk
Server:  ns2.ic.ac.uk
Address:  155.198.142.82
```

ipconfig



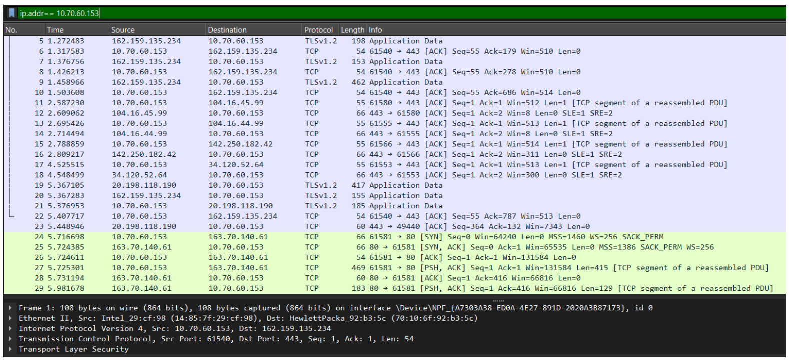
```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . : mahindrauniversity.edu.in
   Description . . . . . . . . . . . : Killer(R) Wi-Fi 6 AX1650x 160MHz Wireless Network Adapter (200NGW)
   Physical Address. . . . . . . . . : 14-85-7F-29-CF-98
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5046:851:a645:847c%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.70.60.153(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.192.0
   Lease Obtained. . . . . . . . . . : 20 February 2024 18:28:24
   Lease Expires . . . . . . . . . . : 21 February 2024 18:28:24
   Default Gateway . . . . . . . . . : 10.70.0.1
   DHCP Server . . . . . . . . . . . : 10.20.0.50
   DHCPv6 IAID . . . . . . . . . . . : 253003135
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-F5-D6-44-60-18-95-34-D9-07
   DNS Servers . . . . . . . . . . . : 10.59.121.144
                                       10.59.121.244
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Tracing DNS with Wireshark

Part 3a. http://www.ietf.org

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

The DNS query and response messages are sent over TCP



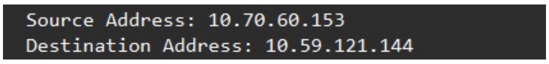
```
ip.addr== 10.70.60.153

No.  Time      Source           Destination      Protocol Length Info
   5 1.272483  162.159.135.234  10.70.60.153     TLSv1.2   198 Application Data
   6 1.317583  10.70.60.153     162.159.135.234  TCP        54 61540 → 443 [ACK] Seq=55 Ack=179 Win=510 Len=0
   7 1.376756  162.159.135.234  10.70.60.153     TLSv1.2   153 Application Data
   8 1.426213  10.70.60.153     162.159.135.234  TCP        54 61540 → 443 [ACK] Seq=55 Ack=278 Win=510 Len=0
   9 1.458966  162.159.135.234  10.70.60.153     TLSv1.2   462 Application Data
  10 1.503608  10.70.60.153     162.159.135.234  TCP        54 61540 → 443 [ACK] Seq=55 Ack=686 Win=514 Len=0
  11 2.587230  10.70.60.153     104.16.45.99     TCP        55 61580 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
  12 2.609062  104.16.45.99     10.70.60.153     TCP        66 443 → 61580 [ACK] Seq=1 Ack=2 Win=8 Len=0 SLE=1 SRE=2
  13 2.695426  10.70.60.153     104.16.44.99     TCP        55 61555 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
  14 2.714494  104.16.44.99     10.70.60.153     TCP        66 443 → 61555 [ACK] Seq=1 Ack=2 Win=8 Len=0 SLE=1 SRE=2
  15 2.788859  10.70.60.153     142.250.182.42   TCP        55 61566 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
  16 2.809217  142.250.182.42   10.70.60.153     TCP        66 443 → 61566 [ACK] Seq=1 Ack=2 Win=311 Len=0 SLE=1 SRE=2
  17 4.525515  10.70.60.153     34.120.52.64     TCP        55 61553 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
  18 4.548499  34.120.52.64     10.70.60.153     TCP        66 443 → 61553 [ACK] Seq=1 Ack=2 Win=300 Len=0 SLE=1 SRE=2
  19 5.367105  20.198.118.190   10.70.60.153     TLSv1.2   417 Application Data
  20 5.367283  162.159.135.234  10.70.60.153     TLSv1.2   155 Application Data
  21 5.376953  10.70.60.153     20.198.118.190   TLSv1.2   185 Application Data
  22 5.407717  10.70.60.153     162.159.135.234  TCP        54 61540 → 443 [ACK] Seq=55 Ack=787 Win=513 Len=0
  23 5.448946  20.198.118.190   10.70.60.153     TCP        60 443 → 49440 [ACK] Seq=364 Ack=132 Win=7343 Len=0
  24 5.716698  10.70.60.153     163.70.140.61    TCP        66 61581 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  25 5.724385  163.70.140.61    10.70.60.153     TCP        66 80 → 61581 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 SACK_PERM WS=256
  26 5.724611  10.70.60.153     163.70.140.61    TCP        54 61581 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
  27 5.725301  10.70.60.153     163.70.140.61    TCP       469 61581 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=415 [TCP segment of a reassembled PDU]
  28 5.731194  163.70.140.61    10.70.60.153     TCP        60 80 → 61581 [ACK] Seq=1 Ack=416 Win=66816 Len=0
  29 5.981678  163.70.140.61    10.70.60.153     TCP       183 80 → 61581 [PSH, ACK] Seq=1 Ack=416 Win=66816 Len=129 [TCP segment of a reassembled PDU]

▸ Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface \Device\NPF_{A7303A38-ED0A-4E27-891D-2020A3B87173}, id 0
▸ Ethernet II, Src: Intel_29:cf:98 (14:85:7f:29:cf:98), Dst: HewlettPacka_92:b3:5c (70:10:6f:92:b3:5c)
▸ Internet Protocol Version 4, Src: 10.70.60.153, Dst: 162.159.135.234
▸ Transmission Control Protocol, Src Port: 61540, Dst Port: 443, Seq: 1, Ack: 1, Len: 54
▸ Transport Layer Security
```

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

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

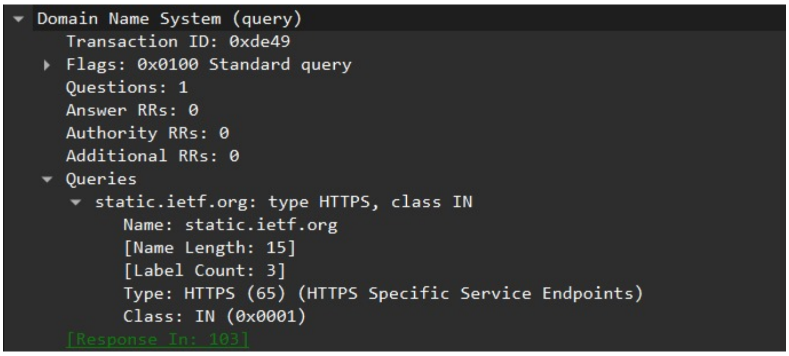
It's sent to 10.59.121.144, which is the IP address of one of my local DNS servers.



```
Source Address: 10.70.60.153
Destination Address: 10.59.121.144
```

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

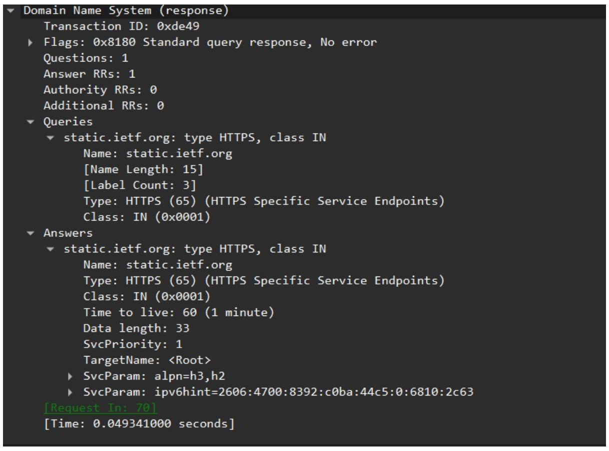
DNS query message is of the type HTTPS and there are not answers



```
▾ Domain Name System (query)
    Transaction ID: 0xde49
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ static.ietf.org: type HTTPS, class IN
        Name: static.ietf.org
        [Name Length: 15]
        [Label Count: 3]
        Type: HTTPS (65) (HTTPS Specific Service Endpoints)
        Class: IN (0x0001)
    [Response In: 103]
```

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

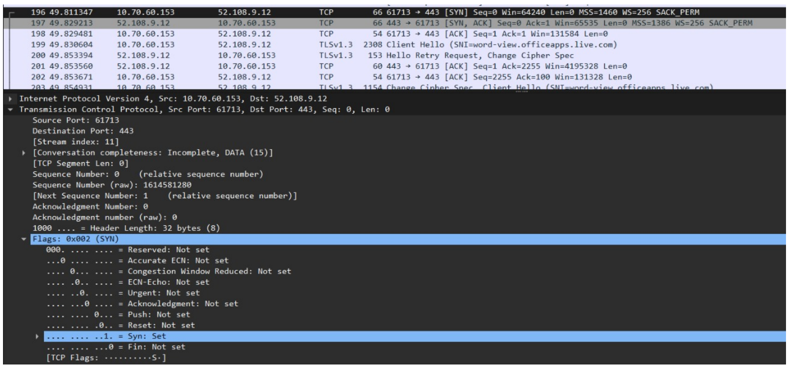
DNS response message is of the type HTTPS and contains one answer containing the name of the host, the type of address and the class.



```
▾ Domain Name System (response)
    Transaction ID: 0xde49
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ static.ietf.org: type HTTPS, class IN
        Name: static.ietf.org
        [Name Length: 15]
        [Label Count: 3]
        Type: HTTPS (65) (HTTPS Specific Service Endpoints)
        Class: IN (0x0001)
  ▾ Answers
    ▾ static.ietf.org: type HTTPS, class IN
        Name: static.ietf.org
        Type: HTTPS (65) (HTTPS Specific Service Endpoints)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 33
        SvcPriority: 1
        TargetName: <Root>
      ▸ SvcParam: alpn=h3,h2
      ▸ SvcParam: ipv6hint=2606:4700:8392:c0ba:44c5:0:6810:2c63
    [Request In: 70]
    [Time: 0.049341000 seconds]
```

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 first SYN packet was sent to 209.173.57.180 which corresponds to the first IP address provided in the DNS response message.



```
  196 49.811347    10.70.60.153    52.108.9.12     TCP        66 61713 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  197 49.829213    52.108.9.12     10.70.60.153    TCP        66 443 → 61713 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 WS=256 SACK_PERM
  198 49.829481    10.70.60.153    52.108.9.12     TCP        54 61713 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
  199 49.830604    10.70.60.153    52.108.9.12     TLSv1.3  2308 Client Hello (SNI=word-view.officeapps.live.com)
  200 49.853394    52.108.9.12     10.70.60.153    TLSv1.3   153 Hello Retry Request, Change Cipher Spec
  201 49.853560    52.108.9.12     10.70.60.153    TCP        60 443 → 61713 [ACK] Seq=1 Ack=2255 Win=4195328 Len=0
  202 49.853671    10.70.60.153    52.108.9.12     TCP        54 61713 → 443 [ACK] Seq=2255 Ack=100 Win=131328 Len=0
  203 49.854931    10.70.60.153    52.108.9.12     TLSv1.3  1154 Change Cipher Spec, Client Hello (SNI=word-view.officeapps.live.com)
▸ Internet Protocol Version 4, Src: 10.70.60.153, Dst: 52.108.9.12
▾ Transmission Control Protocol, Src Port: 61713, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 61713
    Destination Port: 443
    [Stream index: 11]
  ▸ [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1614581280
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▸ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
```

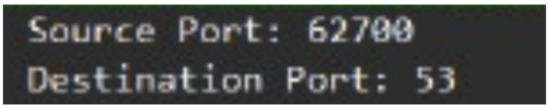
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No

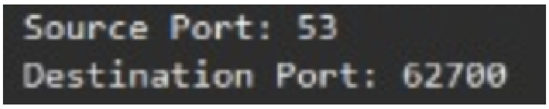
Part 3b. nslookup www.mit.edu

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

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



```
Source Port: 62700
Destination Port: 53
```



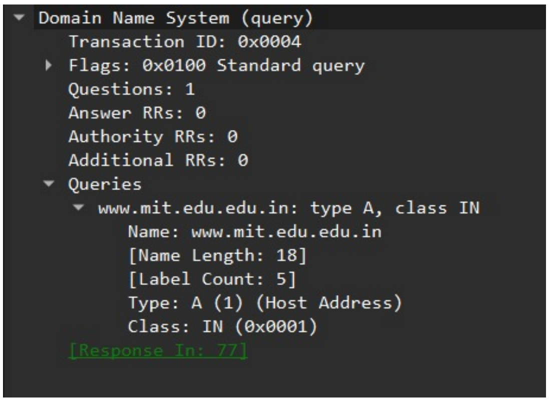
```
Source Port: 53
Destination Port: 62700
```

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

It is 10.70.60.153, and yes it is local DNS server.

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

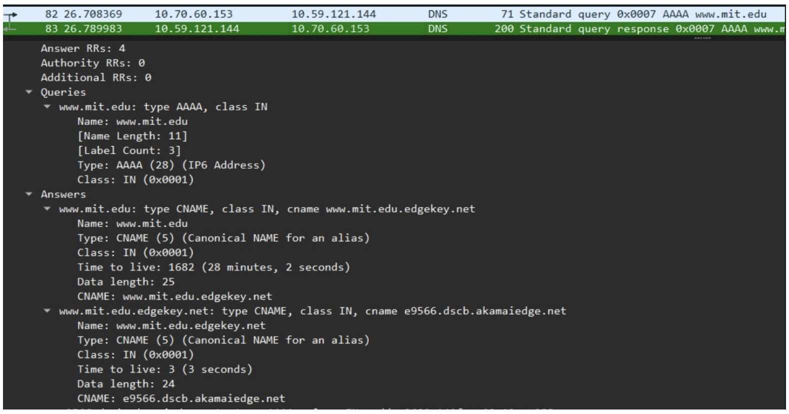
DNS query is of the type 0x0100 Standard query and have no answers.



```
▾ Domain Name System (query)
    Transaction ID: 0x0004
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.mit.edu.edu.in: type A, class IN
        Name: www.mit.edu.edu.in
        [Name Length: 18]
        [Label Count: 5]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 77]
```

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

DNS response mesage is of the type AAAA and has 4 answers.

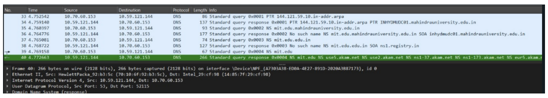


```
82 26.708369    10.70.60.153     10.59.121.144    DNS     71 Standard query 0x0007 AAAA www.mit.edu
83 26.789983    10.59.121.144    10.70.60.153     DNS    200 Standard query response 0x0007 AAAA www.m
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.mit.edu: type AAAA, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  ▾ Answers
    ▾ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 1682 (28 minutes, 2 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    ▾ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 3 (3 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
```

15. Provide a screenshot

Have attached screenshots above.

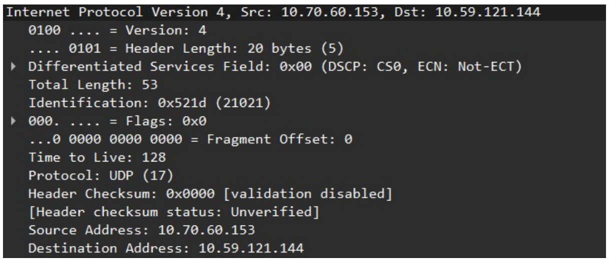
Part 3c. nslookup –type=NS mit.edu



```
No. Time        Source          Destination     Protocol Length Info
 33 4.752542    10.70.60.153    10.59.121.144   DNS     86 Standard query 0x0001 PTR 144.121.59.10.in-addr.arpa
 34 4.759140    10.59.121.144   10.70.60.153    DNS    137 Standard query response 0x0001 PTR 144.121.59.10.in-addr.arpa PTR INHYDMUDC01.mahindrauniversity.edu.in
 35 4.760397    10.70.60.153    10.59.121.144   DNS     93 Standard query 0x0002 NS mit.edu.mahindrauniversity.edu.in
 36 4.764776    10.59.121.144   10.70.60.153    DNS    177 Standard query response 0x0002 No such name NS mit.edu.mahindrauniversity.edu.in SOA inhydmudc01.mahindrauniversity.edu.in
 37 4.765081    10.70.60.153    10.59.121.144   DNS     74 Standard query 0x0003 NS mit.edu.edu.in
 38 4.768722    10.59.121.144   10.70.60.153    DNS    127 Standard query response 0x0003 No such name NS mit.edu.edu.in SOA ns1.registry.in
 39 4.769158    10.70.60.153    10.59.121.144   DNS     67 Standard query 0x0004 NS mit.edu
 40 4.772663    10.59.121.144   10.70.60.153    DNS    266 Standard query response 0x0004 NS mit.edu NS use5.akam.net NS use2.akam.net NS ns1-37.akam.net NS ns1-173.akam.net NS eur5.akam.

▸ Frame 40: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) on interface \Device\NPF_{A7303A38-ED0A-4E27-891D-2020A3B87173}, id 0
▸ Ethernet II, Src: HewlettPacka_92:b3:5c (70:10:6f:92:b3:5c), Dst: Intel_29:cf:98 (14:85:7f:29:cf:98)
▸ Internet Protocol Version 4, Src: 10.59.121.144, Dst: 10.70.60.153
▸ User Datagram Protocol, Src Port: 53, Dst Port: 52115
▸ Domain Name System (response)
```

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

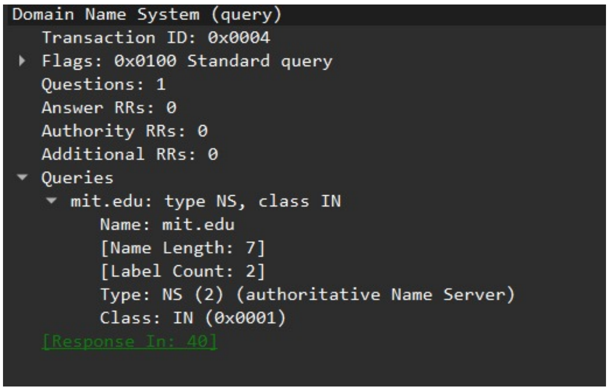
It is 10.70.60.153, and yes it is local DNS server.



```
Internet Protocol Version 4, Src: 10.70.60.153, Dst: 10.59.121.144
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x521d (21021)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.70.60.153
    Destination Address: 10.59.121.144
```

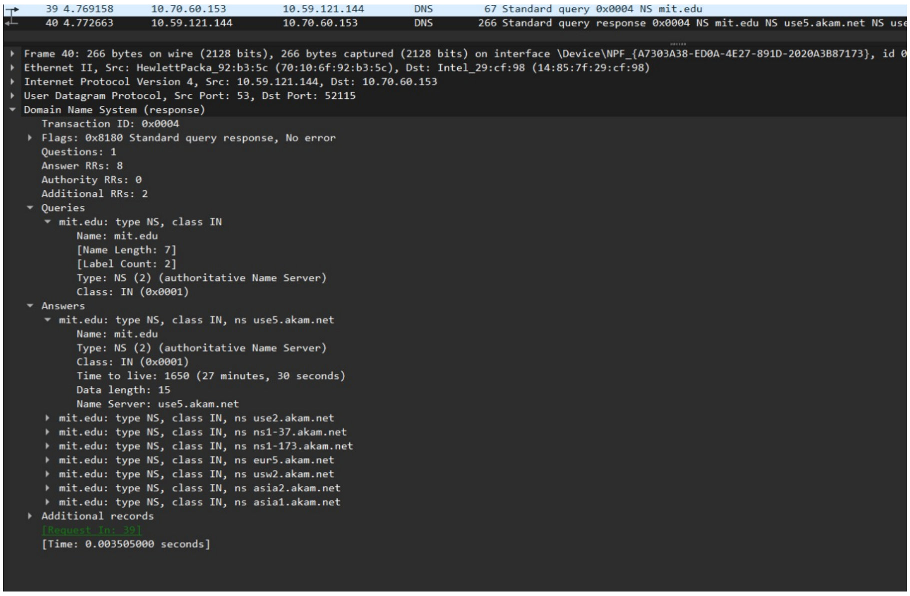
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

It's a type NS DNS query that doesn't 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
  ▾ Queries
    ▾ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
    [Response In: 40]
```

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?



```
  39 4.769158    10.70.60.153    10.59.121.144   DNS    67 Standard query 0x0004 NS mit.edu
  40 4.772663    10.59.121.144   10.70.60.153    DNS   266 Standard query response 0x0004 NS mit.edu NS use5.akam.net NS use

▸ Frame 40: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) on interface \Device\NPF_{A7303A38-ED0A-4E27-891D-2020A3B87173}, id 0
▸ Ethernet II, Src: HewlettPacka_92:b3:5c (70:10:6f:92:b3:5c), Dst: Intel_29:cf:98 (14:85:7f:29:cf:98)
▸ Internet Protocol Version 4, Src: 10.59.121.144, Dst: 10.70.60.153
▸ User Datagram Protocol, Src Port: 53, Dst Port: 52115
▾ Domain Name System (response)
    Transaction ID: 0x0004
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 2
  ▾ Queries
    ▾ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
  ▾ Answers
    ▾ mit.edu: type NS, class IN, ns use5.akam.net
        Name: mit.edu
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
        Time to live: 1650 (27 minutes, 30 seconds)
        Data length: 15
        Name Server: use5.akam.net
    ▸ mit.edu: type NS, class IN, ns use2.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▸ mit.edu: type NS, class IN, ns eur5.akam.net
    ▸ mit.edu: type NS, class IN, ns usw2.akam.net
    ▸ mit.edu: type NS, class IN, ns asia2.akam.net
    ▸ mit.edu: type NS, class IN, ns asia1.akam.net
  ▸ Additional records
    [Request In: 39]
    [Time: 0.003505000 seconds]
```

19. Provide a screenshot.

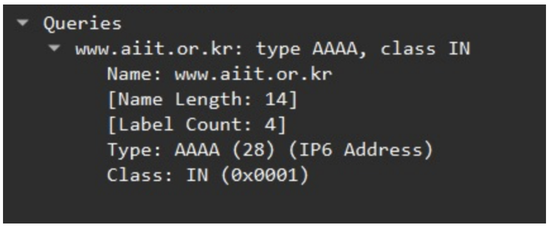
Attached in the above questions.

Part 3d. nslookup www.aiit.or.kr bitsy.mit.edu

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?

It is 10.70.60.153, and yes it is local DNS server.

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

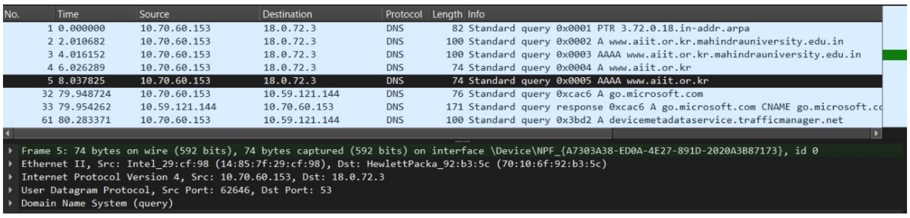


```
▾ Queries
  ▾ www.aiit.or.kr: type AAAA, class IN
      Name: www.aiit.or.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
```

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

I was unable to get a response to this query on my server.

23. Provide a screenshot.



```
No.  Time         Source          Destination     Protocol  Length Info
   1 0.000000     10.70.60.153    18.0.72.3       DNS         82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
   2 2.010682     10.70.60.153    18.0.72.3       DNS        100 Standard query 0x0002 A www.aiit.or.kr.mahindrauniversity.edu.in
   3 4.016152     10.70.60.153    18.0.72.3       DNS        100 Standard query 0x0003 AAAA www.aiit.or.kr.mahindrauniversity.edu.in
   4 6.026289     10.70.60.153    18.0.72.3       DNS         74 Standard query 0x0004 A www.aiit.or.kr
   5 8.037825     10.70.60.153    18.0.72.3       DNS         74 Standard query 0x0005 AAAA www.aiit.or.kr
  32 79.948724    10.70.60.153    10.59.121.144   DNS         76 Standard query 0xcac6 A go.microsoft.com
  33 79.954262    10.59.121.144   10.70.60.153    DNS        171 Standard query response 0xcac6 A go.microsoft.com CNAME go.microsoft.cc
  61 80.283371    10.70.60.153    10.59.121.144   DNS        100 Standard query 0x3bd2 A devicemetadataservice.trafficmanager.net

▸ Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A7303A38-ED0A-4E27-891D-2020A3B87173}, id 0
▸ Ethernet II, Src: Intel_29:cf:98 (14:85:7f:29:cf:98), Dst: HewlettPacka_92:b3:5c (70:10:6f:92:b3:5c)
▸ Internet Protocol Version 4, Src: 10.70.60.153, Dst: 18.0.72.3
▸ User Datagram Protocol, Src Port: 62646, Dst Port: 53
▸ Domain Name System (query)
```