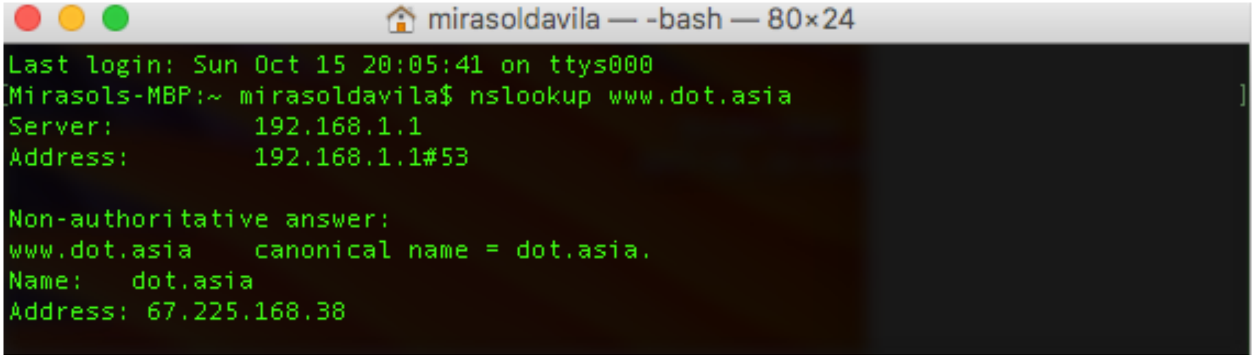
WireShark Lab - Mirasol Davila 303437269

1. nslookup

1. nslookup www.dot.asia

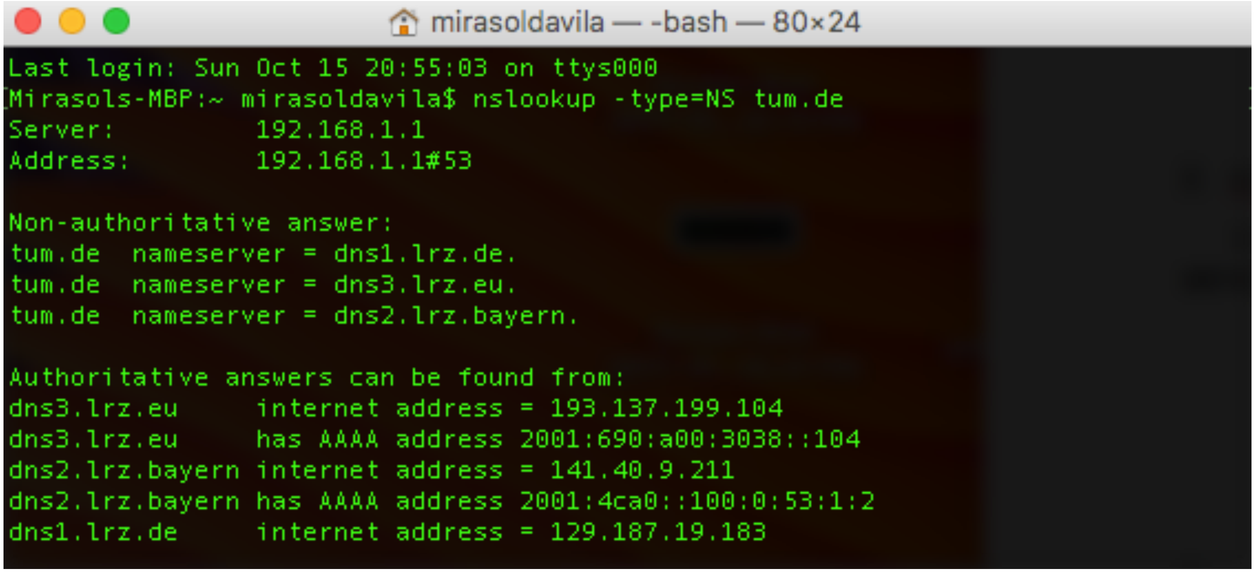
The IP address of the server for www.dot.asia is 67.225.168.38



```
Last login: Sun Oct 15 20:05:41 on ttys000
[Mirasols-MBP:~ mirasoldavila$ nslookup www.dot.asia                          ]
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.dot.asia    canonical name = dot.asia.
Name:   dot.asia
Address: 67.225.168.38
```

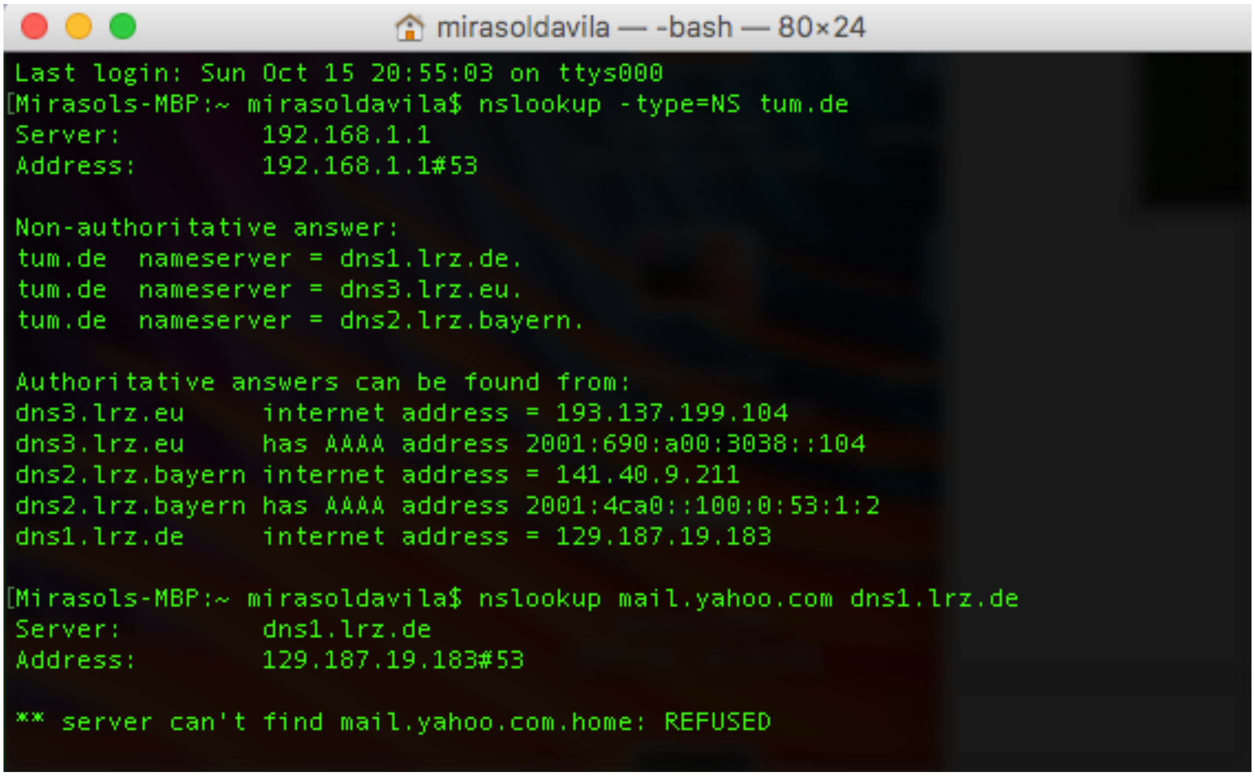
2. nslookup -type=NS tum.de

The authoritative DNS Servers for the Technical University of Munich the authoritative servers are : dns1.lrz,de , dns3.lrz.eu , and dns2.lrz.bayern



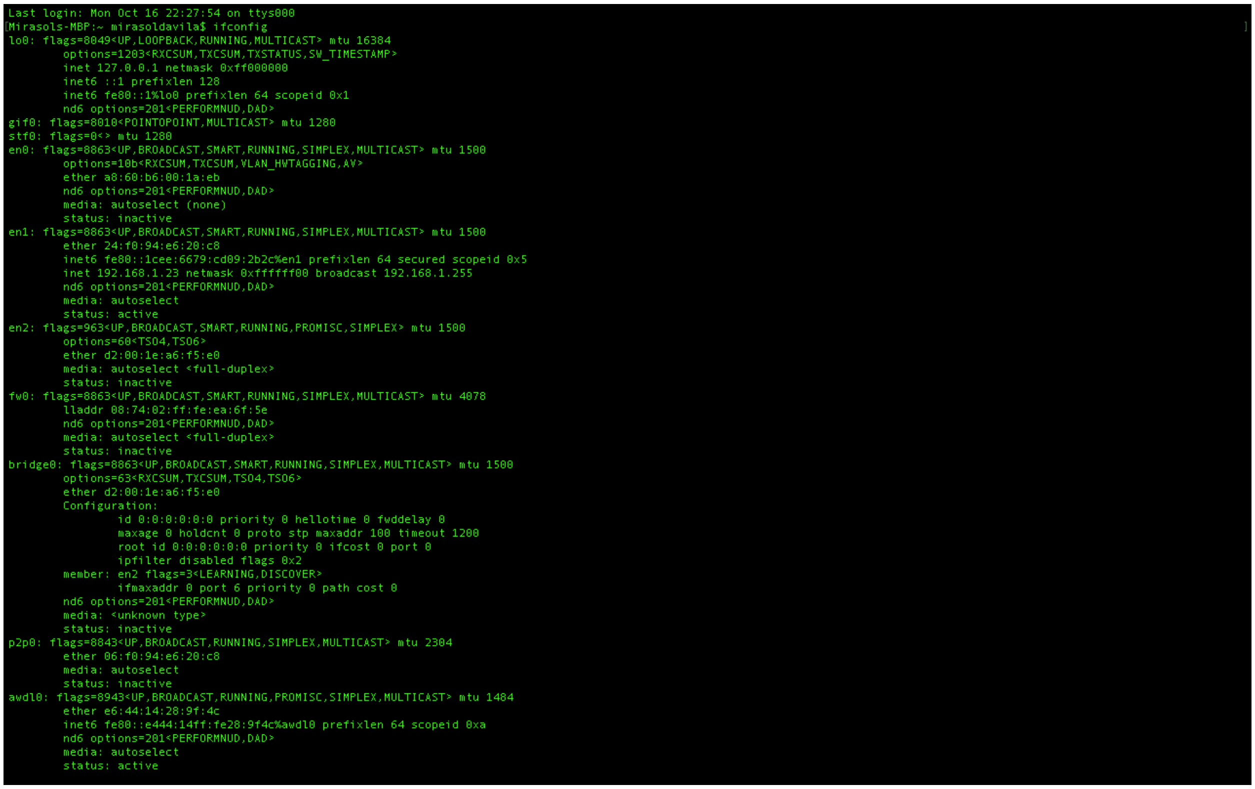
```
Last login: Sun Oct 15 20:55:03 on ttys000
[Mirasols-MBP:~ mirasoldavila$ nslookup -type=NS tum.de
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
tum.de  nameserver = dns1.lrz.de.
tum.de  nameserver = dns3.lrz.eu.
tum.de  nameserver = dns2.lrz.bayern.

Authoritative answers can be found from:
dns3.lrz.eu     internet address = 193.137.199.104
dns3.lrz.eu     has AAAA address 2001:690:a00:3038::104
dns2.lrz.bayern internet address = 141.40.9.211
dns2.lrz.bayern has AAAA address 2001:4ca0::100:0:53:1:2
dns1.lrz.de     internet address = 129.187.19.183
```

3. I'm unable to retrieve the Ip address since the remote firewall blocked my connection.

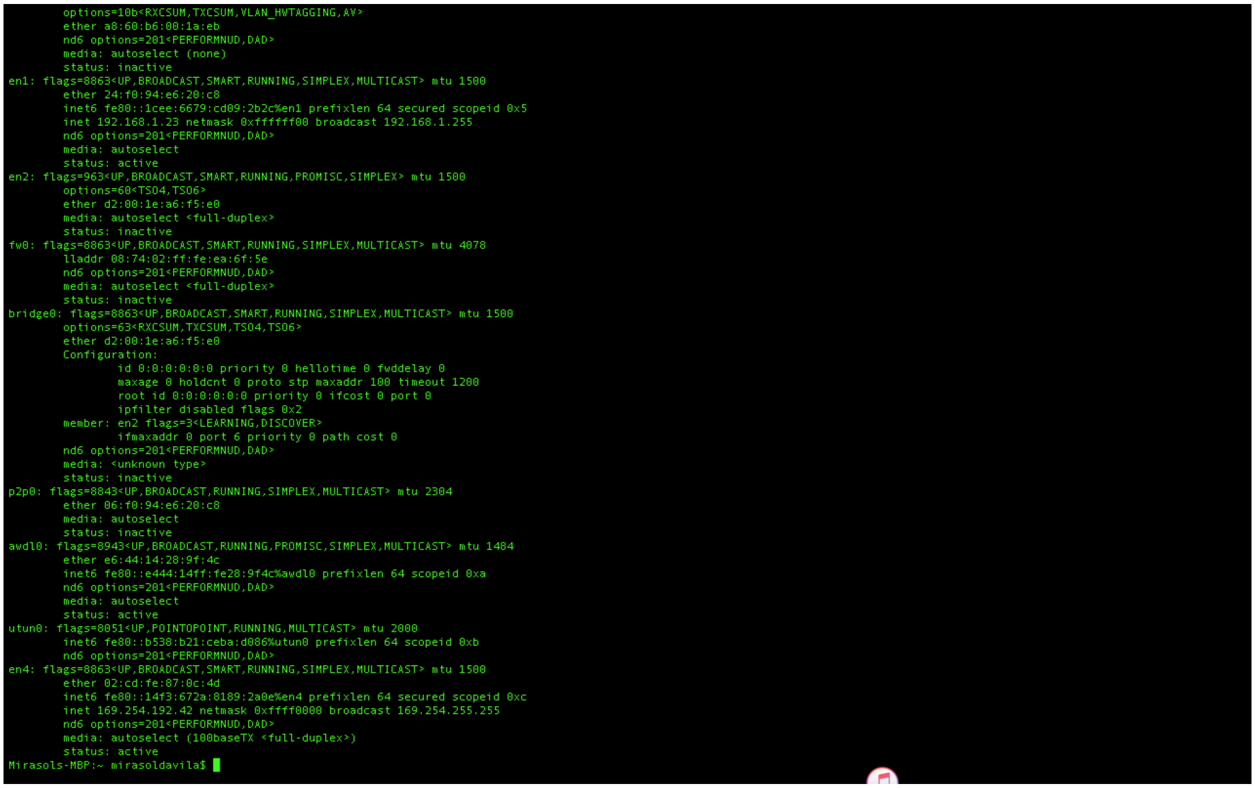


```
Last login: Sun Oct 15 20:55:03 on ttys000
[Mirasols-MBP:~ mirasoldavila$ nslookup -type=NS tum.de
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
tum.de  nameserver = dns1.lrz.de.
tum.de  nameserver = dns3.lrz.eu.
tum.de  nameserver = dns2.lrz.bayern.

Authoritative answers can be found from:
dns3.lrz.eu     internet address = 193.137.199.104
dns3.lrz.eu     has AAAA address 2001:690:a00:3038::104
dns2.lrz.bayern internet address = 141.40.9.211
dns2.lrz.bayern has AAAA address 2001:4ca0::100:0:53:1:2
dns1.lrz.de     internet address = 129.187.19.183

[Mirasols-MBP:~ mirasoldavila$ nslookup mail.yahoo.com dns1.lrz.de
Server:         dns1.lrz.de
Address:        129.187.19.183#53

** server can't find mail.yahoo.com.home: REFUSED
```

2. ipconfig



```
Last login: Mon Oct 16 22:27:54 on ttys000
[Mirasols-MBP:~ mirasoldavila$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
        ether a8:60:b6:00:1a:eb
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (none)
        status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 24:f0:94:e6:20:c8
        inet6 fe80::1cee:6679:cd09:2b2c%en1 prefixlen 64 secured scopeid 0x5
        inet 192.168.1.23 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en2: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
        options=60<TSO4,TSO6>
        ether d2:00:1e:a6:f5:e0
        media: autoselect <full-duplex>
        status: inactive
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
        lladdr 08:74:02:ff:fe:ea:6f:5e
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether d2:00:1e:a6:f5:e0
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x2
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 6 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 06:f0:94:e6:20:c8
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        ether e6:44:14:28:9f:4c
        inet6 fe80::e444:14ff:fe28:9f4c%awdl0 prefixlen 64 scopeid 0xa
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

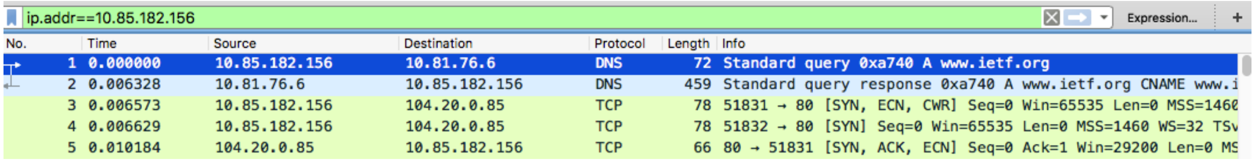


```
        options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
        ether a8:60:b6:00:1a:eb
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (none)
        status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 24:f0:94:e6:20:c8
        inet6 fe80::1cee:6679:cd09:2b2c%en1 prefixlen 64 secured scopeid 0x5
        inet 192.168.1.23 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en2: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
        options=60<TSO4,TSO6>
        ether d2:00:1e:a6:f5:e0
        media: autoselect <full-duplex>
        status: inactive
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
        lladdr 08:74:02:ff:fe:ea:6f:5e
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether d2:00:1e:a6:f5:e0
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x2
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 6 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 06:f0:94:e6:20:c8
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        ether e6:44:14:28:9f:4c
        inet6 fe80::e444:14ff:fe28:9f4c%awdl0 prefixlen 64 scopeid 0xa
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::b538:b21:ceba:d086%utun0 prefixlen 64 scopeid 0xb
        nd6 options=201<PERFORMNUD,DAD>
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 02:cd:fe:87:0c:4d
        inet6 fe80::14f3:672a:8189:2a0e%en4 prefixlen 64 secured scopeid 0xc
        inet 169.254.192.42 netmask 0xffff0000 broadcast 169.254.255.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
Mirasols-MBP:~ mirasoldavila$ 
```

3. Tracing DNS with WireShark

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

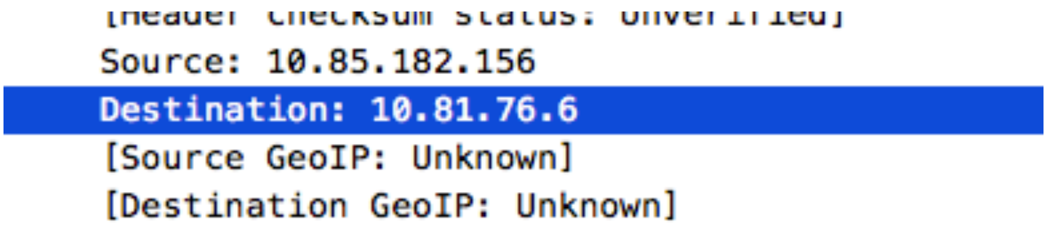
The query and response messages are sent over UDP



```
No.  Time      Source          Destination     Protocol  Length  Info
   1 0.000000  10.85.182.156   10.81.76.6      DNS           72  Standard query 0xa740 A www.ietf.org
   2 0.006328  10.81.76.6      10.85.182.156   DNS          459  Standard query response 0xa740 A www.ietf.org CNAME www.i
   3 0.006573  10.85.182.156   104.20.0.85     TCP           78  51831 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460
   4 0.006629  10.85.182.156   104.20.0.85     TCP           78  51832 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSv
   5 0.010184  104.20.0.85     10.85.182.156   TCP           66  80 → 51831 [SYN, ACK, ECN] Seq=0 Ack=1 Win=29200 Len=0 MS
```

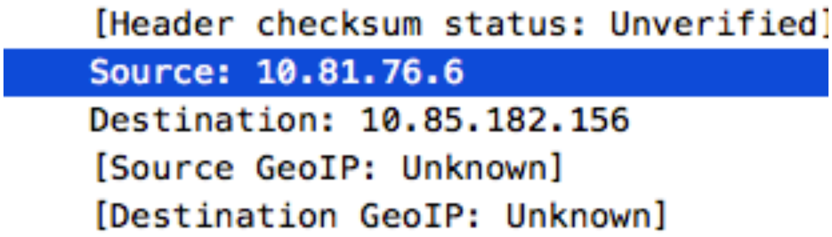
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

The destination port for the DNS query message is



```
[Header checksum status: Unverified]
Source: 10.85.182.156
Destination: 10.81.76.6
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
```

The source port of the DNS response message is



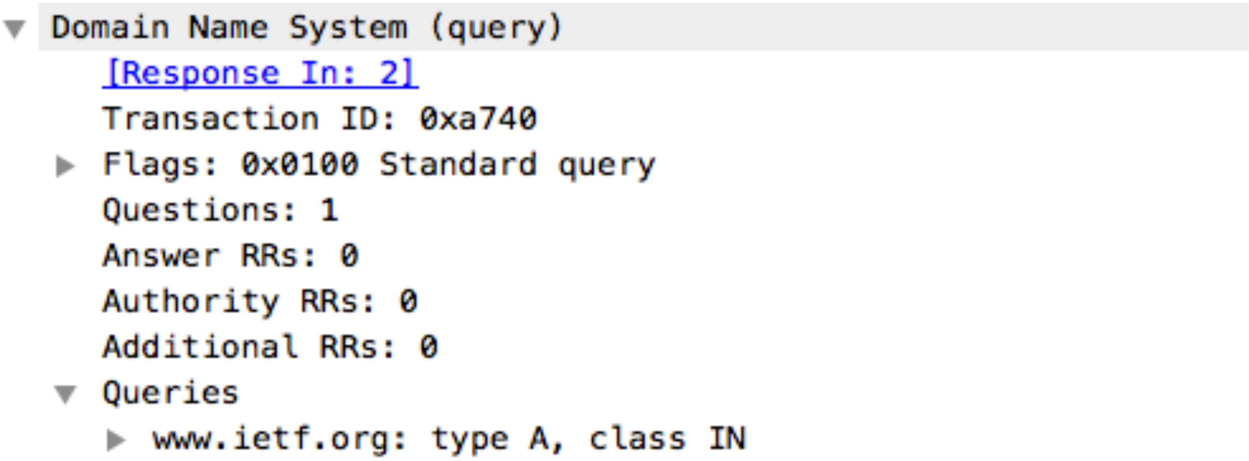
```
    [Header checksum status: Unverified]
    Source: 10.81.76.6
    Destination: 10.85.182.156
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

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 address the same?

The IP addres the DNS query message is 10.85.182.156 . The IP address of my local DNS server and IP address of the DNS query message are the same

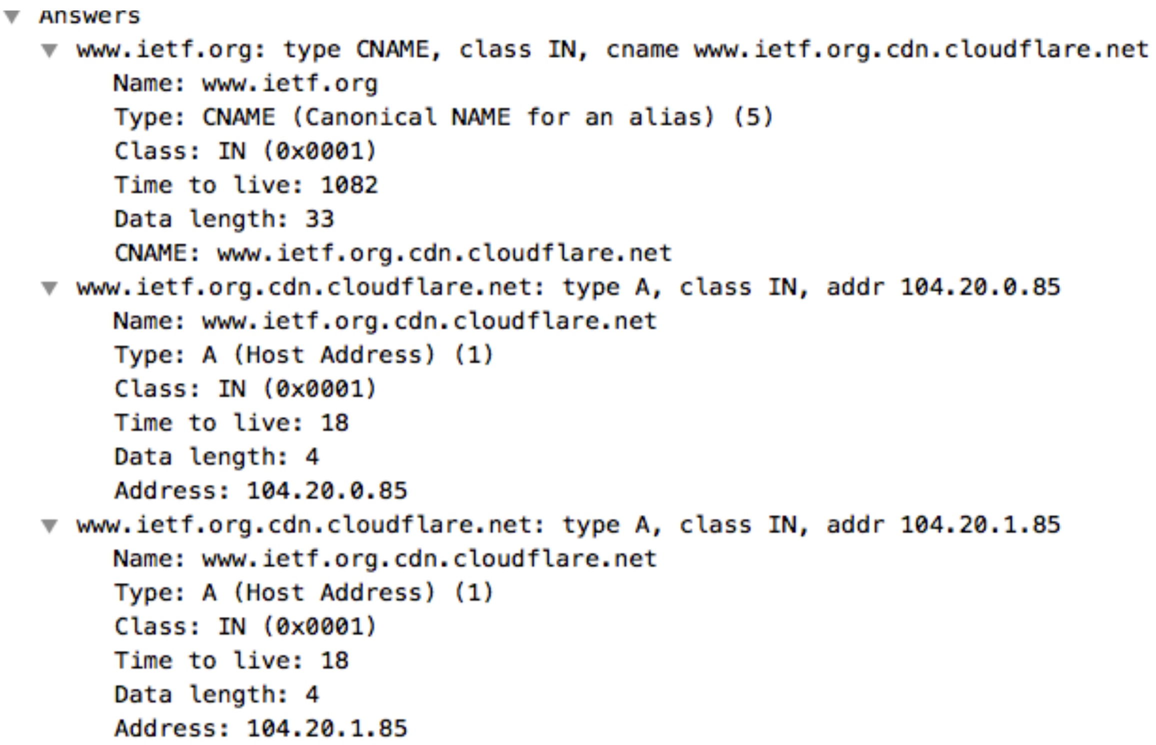
7. Examine the DNS query message. What “Type” of DNS query is it?  Does the query message contain any “answers”?

The DNS query message is type A. The query message doesn’t contain any answers.



```
▼ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0xa740
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.ietf.org: type A, class IN
```

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
The DNS response message contains 3 answers, with the name of the host, the type of address, class, the TTL, data length and the IP address.



```
▼ Answers
  ▼ 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: 1082
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  ▼ 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: 18
      Data length: 4
      Address: 104.20.0.85
  ▼ 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: 18
      Data length: 4
      Address: 104.20.1.85
```

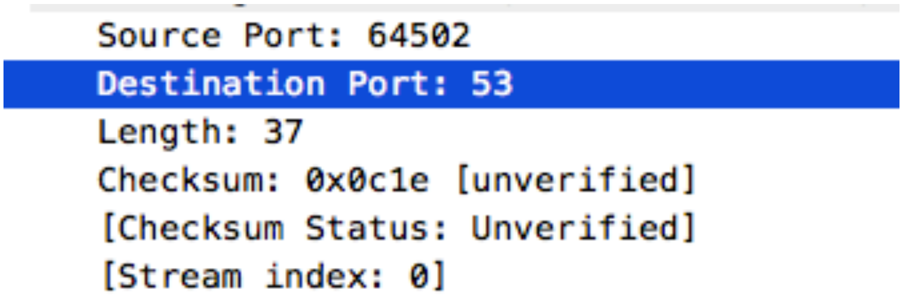
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

No the destination IP address of the SYN packet doesn’t correspond to any of the IP addresses that were provided in the DNS response message

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

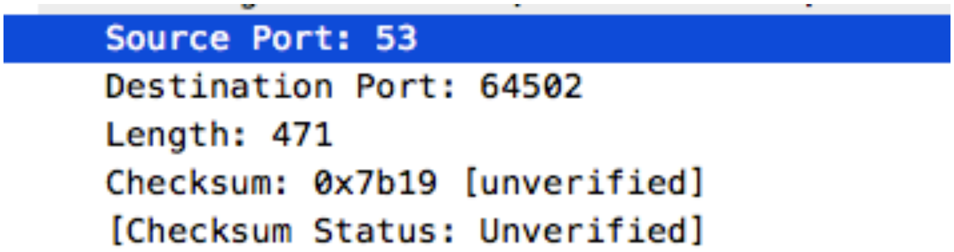
11. What is the destination port for the DNS query message? What is the source port of DNS response message?

The destionation port for the DNS query message is:



```
Source Port: 64502
Destination Port: 53
Length: 37
Checksum: 0x0c1e [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
```

The source port of DNS response message is:



```
Source Port: 53
Destination Port: 64502
Length: 471
Checksum: 0x7b19 [unverified]
[Checksum Status: Unverified]
```

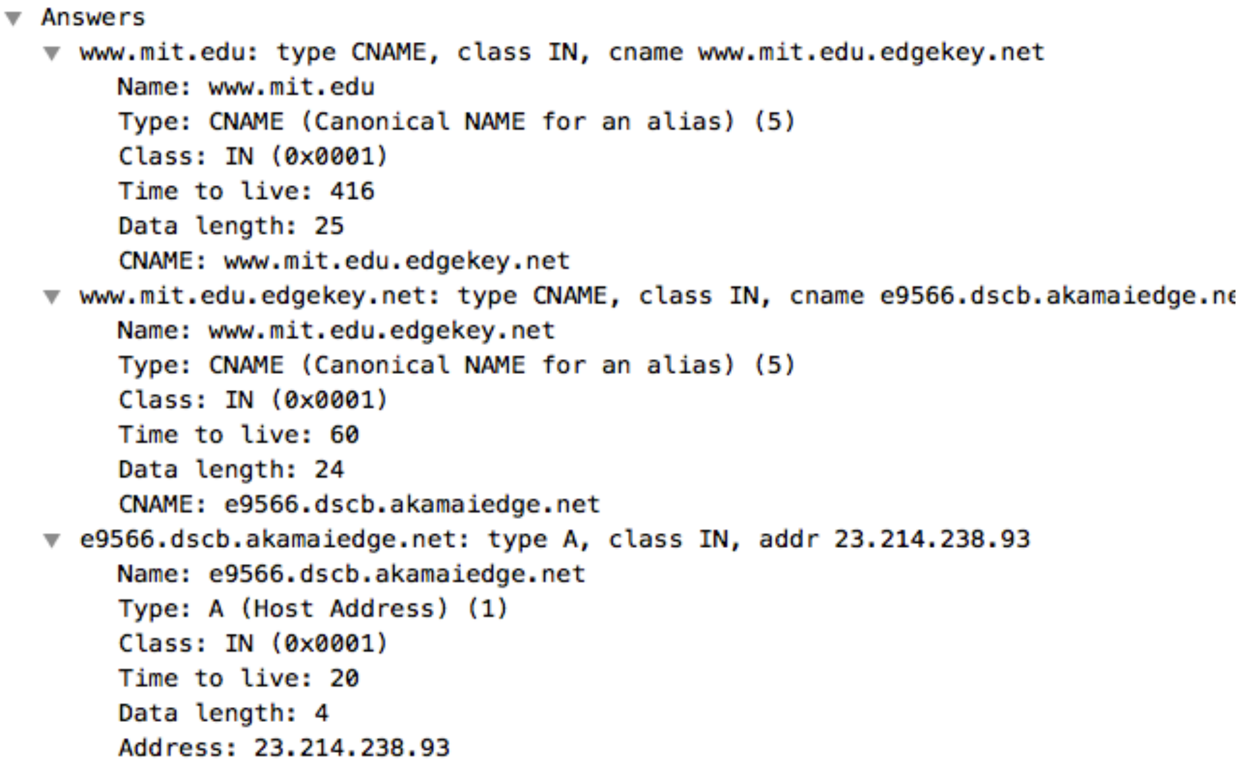
12.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
The IP address the DNS query message is being sent to is,10.81.28.5 , which is my default locak DNS server.

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

The query message is Type A and doesn’t contain any answers.

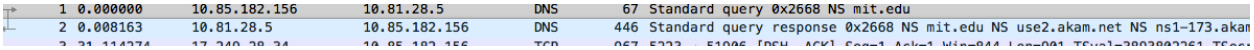
14. Examine the DNs response message. How many “answers” are provided? What do each of these answers contain?

The DNS response message contains 3 answer.

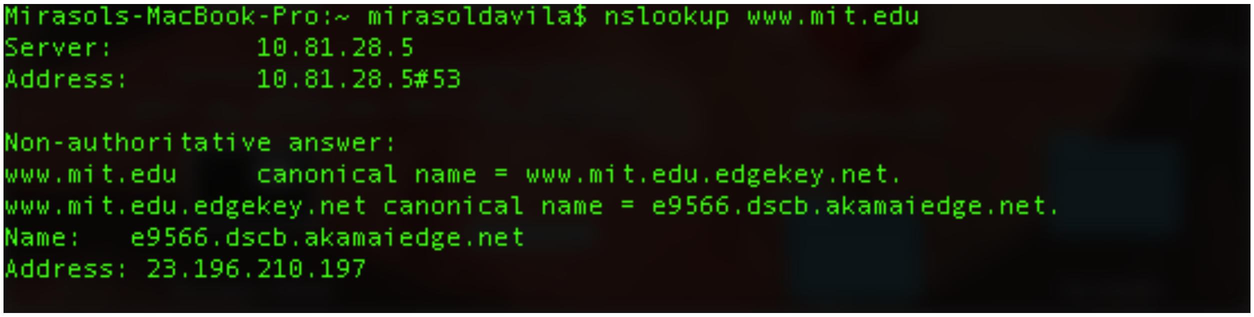


```
▼ Answers
  ▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 416
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.ne
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.214.238.93
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
      Address: 23.214.238.93
```

15.



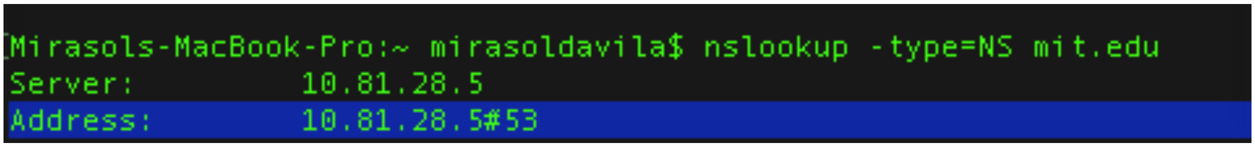
```
1 0.000000    10.85.182.156   10.81.28.5      DNS    67 Standard query 0x2668 NS mit.edu
2 0.008163    10.81.28.5      10.85.182.156   DNS   446 Standard query response 0x2668 NS mit.edu NS use2.akam.net NS ns1-173.akam
3 31.114274   17.249.28.34    10.85.182.156   TCP   967 5223 → 51906 [PSH, ACK] Seq=1 Ack=1 Win=844 Len=901 TSval=3893802261 TSec
```



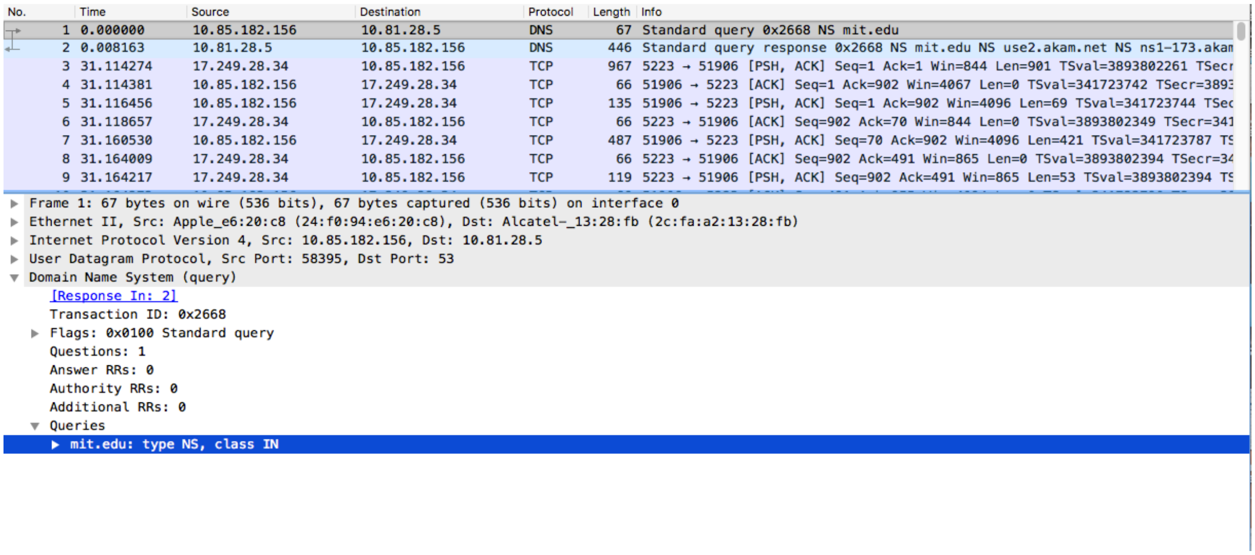
```
Mirasols-MacBook-Pro:~ mirasoldavila$ nslookup www.mit.edu
Server:         10.81.28.5
Address:        10.81.28.5#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 23.196.210.197
```

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

The IP address the DNS query message sent is 10.81.28.5, which is my default local DNS server.

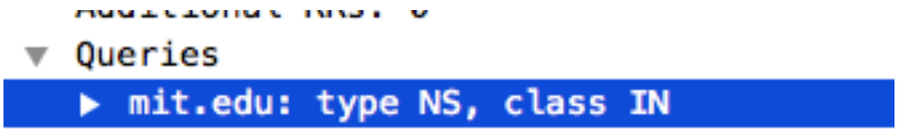


```
Mirasols-MacBook-Pro:~ mirasoldavila$ nslookup -type=NS mit.edu
Server:         10.81.28.5
Address:        10.81.28.5#53
```



```
No.  Time       Source         Destination    Protocol Length Info
  1 0.000000    10.85.182.156  10.81.28.5     DNS         67 Standard query 0x2668 NS mit.edu
  2 0.008163    10.81.28.5     10.85.182.156  DNS        446 Standard query response 0x2668 NS mit.edu NS use2.akam.net NS ns1-173.akam
  3 31.114274   17.249.28.34   10.85.182.156  TCP        967 5223 → 51906 [PSH, ACK] Seq=1 Ack=1 Win=844 Len=901 TSval=3893802261 TSecr
  4 31.114381   10.85.182.156  17.249.28.34   TCP         66 51906 → 5223 [ACK] Seq=1 Ack=902 Win=4067 Len=0 TSval=341723742 TSecr=3893
  5 31.116456   10.85.182.156  17.249.28.34   TCP        135 51906 → 5223 [PSH, ACK] Seq=1 Ack=902 Win=4096 Len=69 TSval=341723744 TSec
  6 31.118657   17.249.28.34   10.85.182.156  TCP         66 5223 → 51906 [ACK] Seq=902 Ack=70 Win=844 Len=0 TSval=3893802349 TSecr=341
  7 31.160530   10.85.182.156  17.249.28.34   TCP        487 51906 → 5223 [PSH, ACK] Seq=70 Ack=902 Win=4096 Len=421 TSval=341723787 TS
  8 31.164009   17.249.28.34   10.85.182.156  TCP         66 5223 → 51906 [ACK] Seq=902 Ack=491 Win=865 Len=0 TSval=3893802394 TSecr=34
  9 31.164217   17.249.28.34   10.85.182.156  TCP        119 5223 → 51906 [PSH, ACK] Seq=902 Ack=491 Win=865 Len=53 TSval=3893802394 TS

▶ Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▶ Ethernet II, Src: Apple_e6:20:c8 (24:f0:94:e6:20:c8), Dst: Alcatel-_13:28:fb (2c:fa:a2:13:28:fb)
▶ Internet Protocol Version 4, Src: 10.85.182.156, Dst: 10.81.28.5
▶ User Datagram Protocol, Src Port: 58395, Dst Port: 53
▼ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x2668
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ mit.edu: type NS, class IN
```

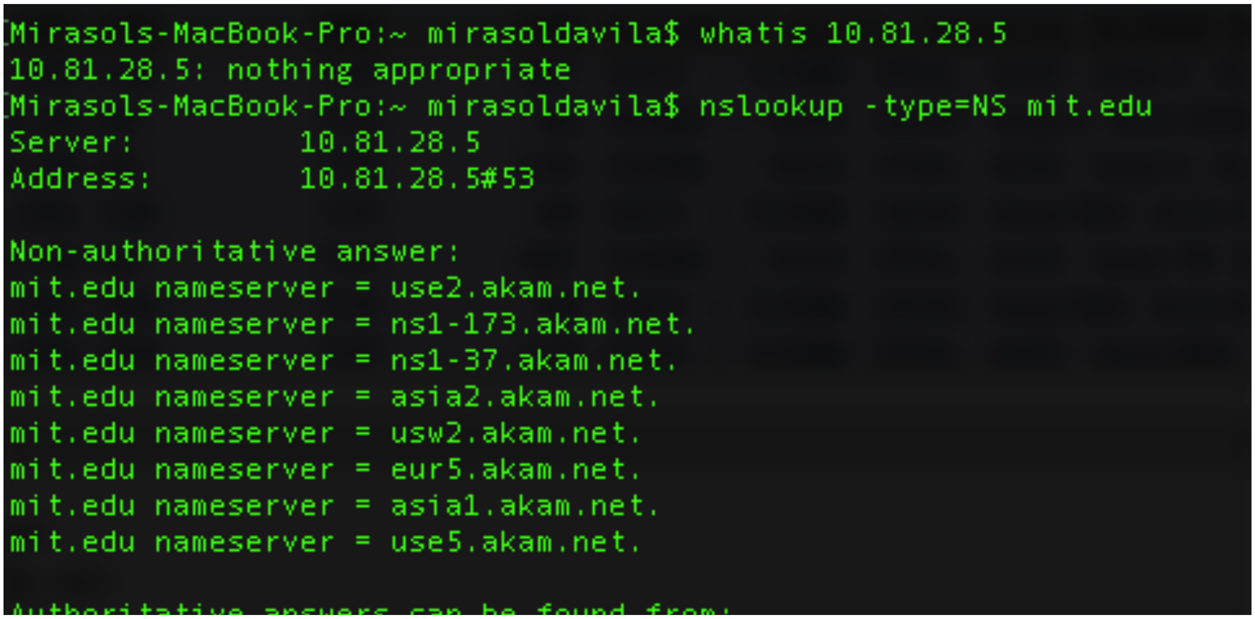
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
The DNS query message is type A and doesn’t contain any answers.



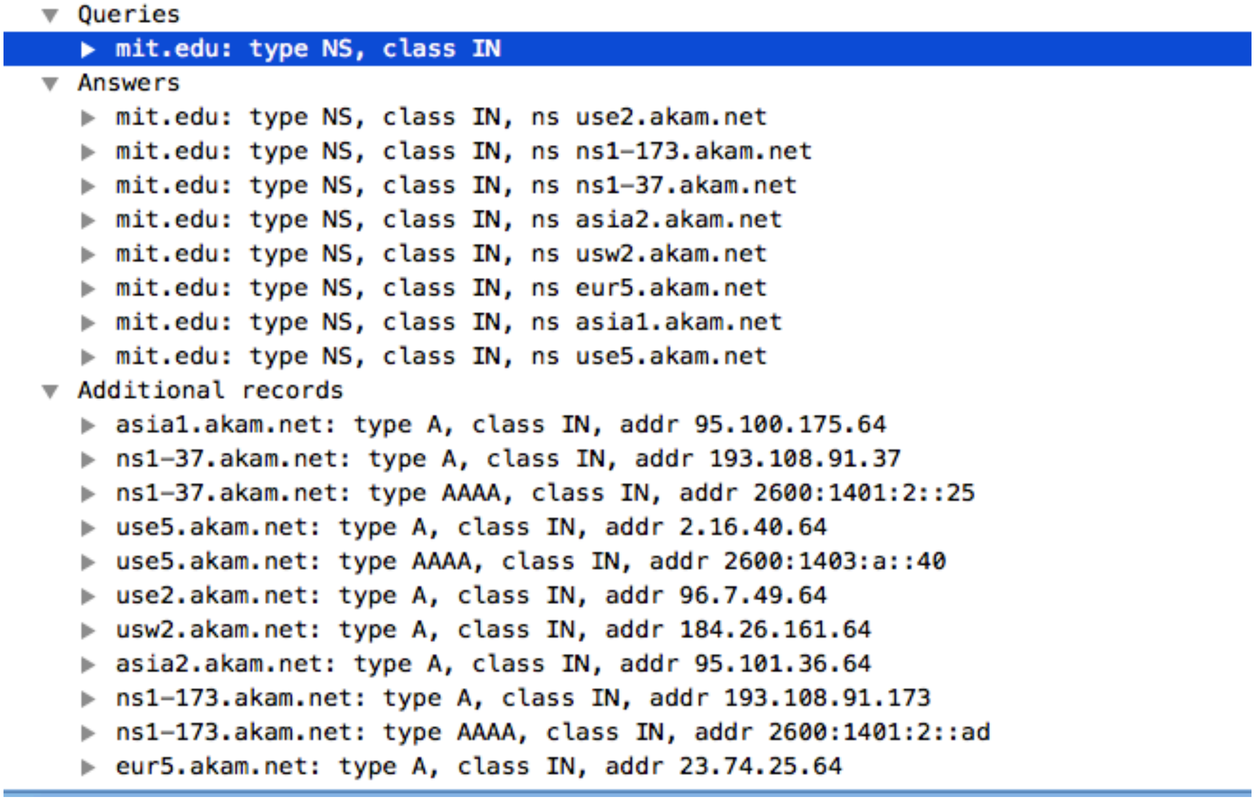
```
    Additional RRs: 0
  ▼ Queries
    ▶ mit.edu: type NS, class IN
```

18. Examine the DNs response message. What MIT nameservers does the response message provide? Does this response message also provide the IP address of the MIT nameserts?

the nameservers are use2.akam.net , ns1-173.akam.net , ns1-37.akam.net , asia2.akam.net , usw2.akam.net , eur5.akam.net , asia1.akam.net , use5.akam.net. I've attached screenshots with each servers IP address.



```
Mirasols-MacBook-Pro:~ mirasoldavila$ whatis 10.81.28.5
10.81.28.5: nothing appropriate
Mirasols-MacBook-Pro:~ mirasoldavila$ nslookup -type=NS mit.edu
Server:         10.81.28.5
Address:        10.81.28.5#53

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

Authoritative answers can be found from:
```

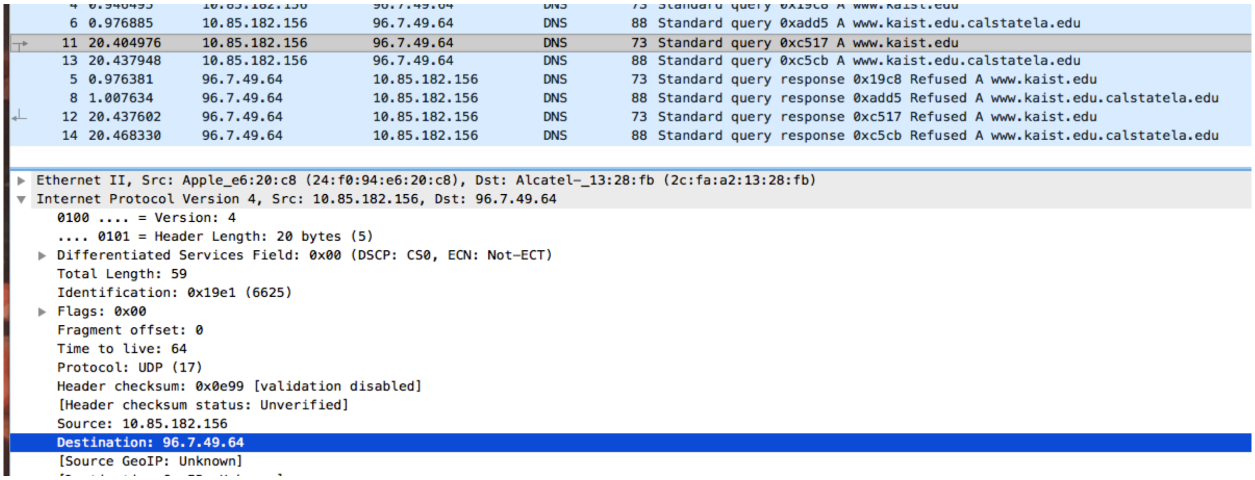


```
  ▼ Queries
    ▶ mit.edu: type NS, class IN
  ▼ Answers
    ▶ mit.edu: type NS, class IN, ns use2.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▶ mit.edu: type NS, class IN, ns asia2.akam.net
    ▶ mit.edu: type NS, class IN, ns usw2.akam.net
    ▶ mit.edu: type NS, class IN, ns eur5.akam.net
    ▶ mit.edu: type NS, class IN, ns asia1.akam.net
    ▶ mit.edu: type NS, class IN, ns use5.akam.net
  ▼ Additional records
    ▶ asia1.akam.net: type A, class IN, addr 95.100.175.64
    ▶ ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    ▶ ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
    ▶ use5.akam.net: type A, class IN, addr 2.16.40.64
    ▶ use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    ▶ use2.akam.net: type A, class IN, addr 96.7.49.64
    ▶ usw2.akam.net: type A, class IN, addr 184.26.161.64
    ▶ asia2.akam.net: type A, class IN, addr 95.101.36.64
    ▶ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    ▶ ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    ▶ eur5.akam.net: type A, class IN, addr 23.74.25.64
```

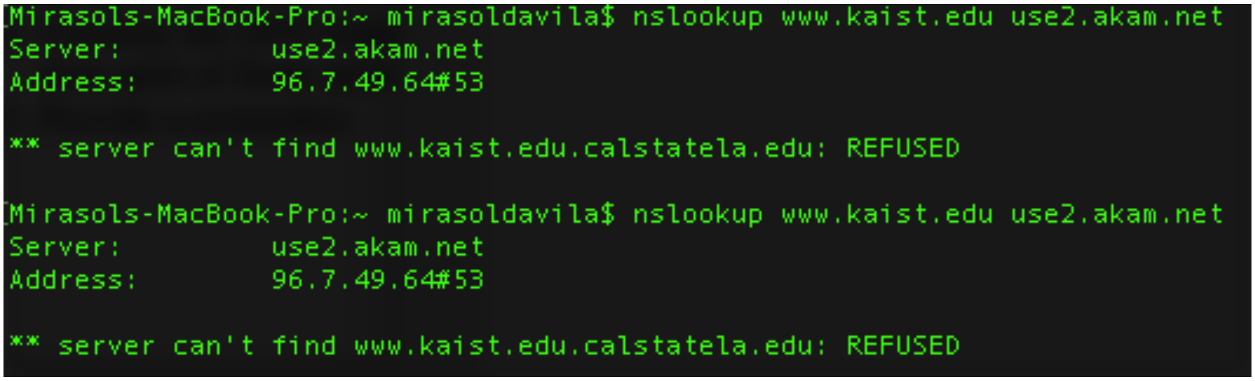
19. You can look at number 18 for the screenshots.

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 I{ address coresspind to?

The Ip address of the DNS query message sent to 96.7.49.64 , which is not my local DNS server, remote firewall blocked my  connection.

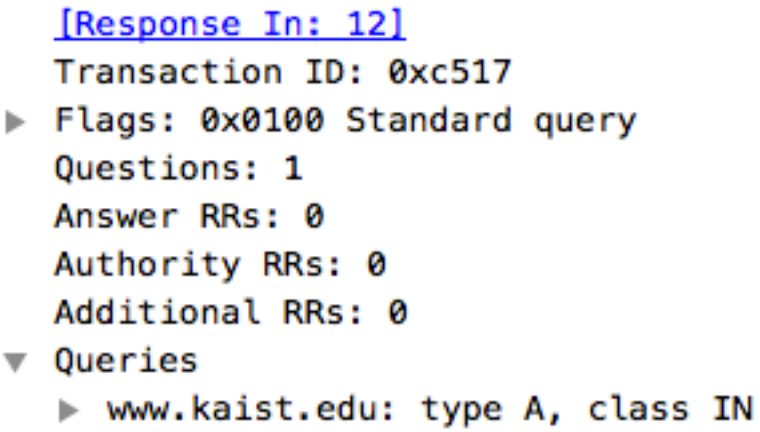


```
   4 0.946493    10.85.182.156    96.7.49.64       DNS      73 Standard query 0x19c8 A www.kaist.edu
   6 0.976885    10.85.182.156    96.7.49.64       DNS      88 Standard query 0xadd5 A www.kaist.edu.calstatela.edu
  11 20.404976   10.85.182.156    96.7.49.64       DNS      73 Standard query 0xc517 A www.kaist.edu
  13 20.437948   10.85.182.156    96.7.49.64       DNS      88 Standard query 0xc5cb A www.kaist.edu.calstatela.edu
   5 0.976381    96.7.49.64       10.85.182.156    DNS      73 Standard query response 0x19c8 Refused A www.kaist.edu
   8 1.007634    96.7.49.64       10.85.182.156    DNS      88 Standard query response 0xadd5 Refused A www.kaist.edu.calstatela.edu
  12 20.437602   96.7.49.64       10.85.182.156    DNS      73 Standard query response 0xc517 Refused A www.kaist.edu
  14 20.468330   96.7.49.64       10.85.182.156    DNS      88 Standard query response 0xc5cb Refused A www.kaist.edu.calstatela.edu

▶ Ethernet II, Src: Apple_e6:20:c8 (24:f0:94:e6:20:c8), Dst: Alcatel-_13:28:fb (2c:fa:a2:13:28:fb)
▼ Internet Protocol Version 4, Src: 10.85.182.156, Dst: 96.7.49.64
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x19e1 (6625)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x0e99 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.85.182.156
    Destination: 96.7.49.64
    [Source GeoIP: Unknown]
```



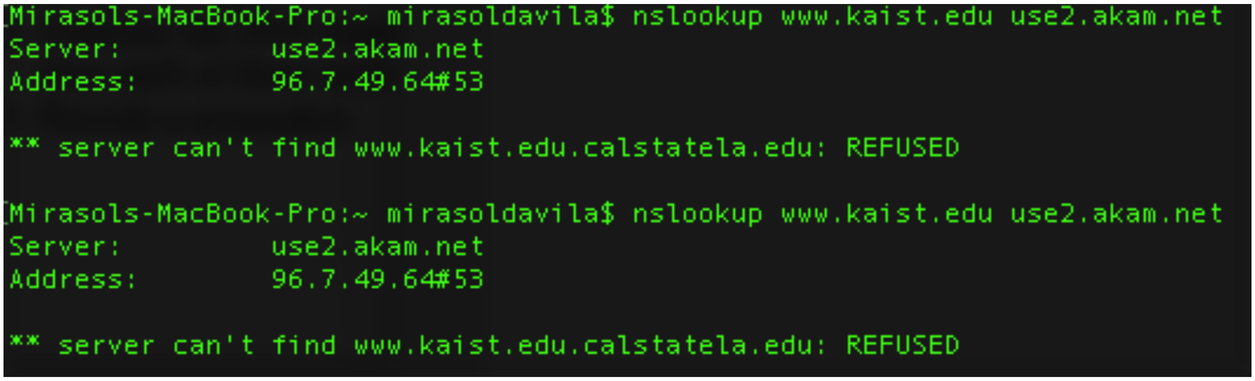
```
Mirasols-MacBook-Pro:~ mirasoldavila$ nslookup www.kaist.edu use2.akam.net
Server:         use2.akam.net
Address:        96.7.49.64#53

** server can't find www.kaist.edu.calstatela.edu: REFUSED

Mirasols-MacBook-Pro:~ mirasoldavila$ nslookup www.kaist.edu use2.akam.net
Server:         use2.akam.net
Address:        96.7.49.64#53

** server can't find www.kaist.edu.calstatela.edu: REFUSED
```

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”
The DNS query message is Type A and doesn’t contain any answers.

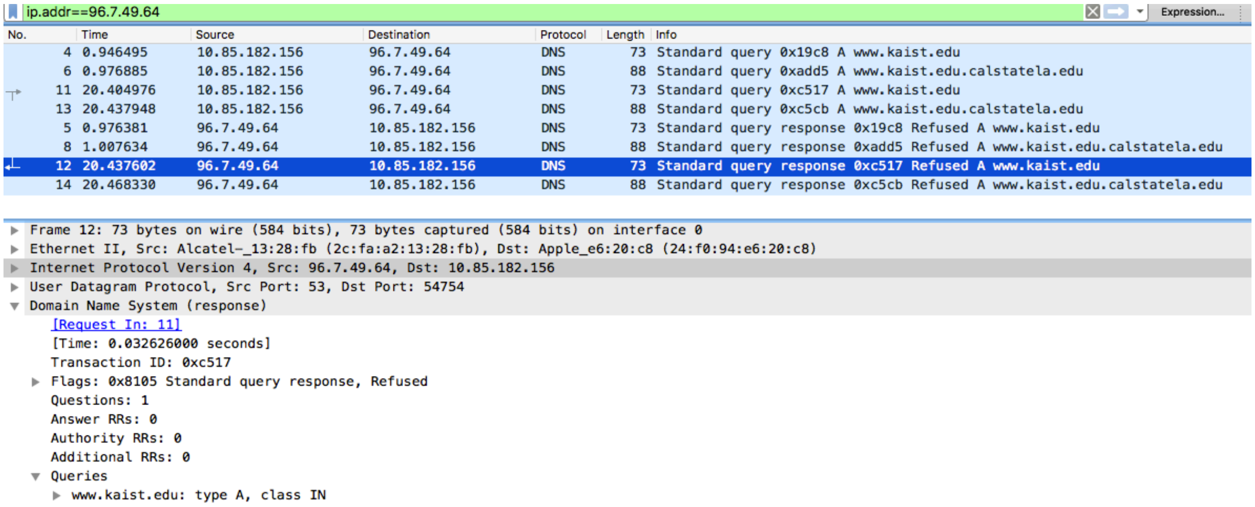


```
  [Response In: 12]
  Transaction ID: 0xc517
▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
▼ Queries
  ▶ www.kaist.edu: type A, class IN
```

22.Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
The DNS response message doesn’t contain any answers since it was refused.



```
Mirasols-MacBook-Pro:~ mirasoldavila$ nslookup www.kaist.edu use2.akam.net
Server:         use2.akam.net
Address:        96.7.49.64#53

** server can't find www.kaist.edu.calstatela.edu: REFUSED

Mirasols-MacBook-Pro:~ mirasoldavila$ nslookup www.kaist.edu use2.akam.net
Server:         use2.akam.net
Address:        96.7.49.64#53

** server can't find www.kaist.edu.calstatela.edu: REFUSED
```



```
ip.addr==96.7.49.64

No.     Time        Source          Destination     Protocol  Length  Info
   4    0.946495    10.85.182.156   96.7.49.64      DNS          73   Standard query 0x19c8 A www.kaist.edu
   6    0.976885    10.85.182.156   96.7.49.64      DNS          88   Standard query 0xadd5 A www.kaist.edu.calstatela.edu
  11   20.404976    10.85.182.156   96.7.49.64      DNS          73   Standard query 0xc517 A www.kaist.edu
  13   20.437948    10.85.182.156   96.7.49.64      DNS          88   Standard query 0xc5cb A www.kaist.edu.calstatela.edu
   5    0.976381    96.7.49.64      10.85.182.156   DNS          73   Standard query response 0x19c8 Refused A www.kaist.edu
   8    1.007634    96.7.49.64      10.85.182.156   DNS          88   Standard query response 0xadd5 Refused A www.kaist.edu.calstatela.edu
  12   20.437602    96.7.49.64      10.85.182.156   DNS          73   Standard query response 0xc517 Refused A www.kaist.edu
  14   20.468330    96.7.49.64      10.85.182.156   DNS          88   Standard query response 0xc5cb Refused A www.kaist.edu.calstatela.edu
```

```
▶ Frame 12: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▶ Ethernet II, Src: Alcatel-_13:28:fb (2c:fa:a2:13:28:fb), Dst: Apple_e6:20:c8 (24:f0:94:e6:20:c8)
▶ Internet Protocol Version 4, Src: 96.7.49.64, Dst: 10.85.182.156
▶ User Datagram Protocol, Src Port: 53, Dst Port: 54754
▼ Domain Name System (response)
    [Request In: 11]
    [Time: 0.032626000 seconds]
    Transaction ID: 0xc517
  ▶ Flags: 0x8105 Standard query response, Refused
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.kaist.edu: type A, class IN
```

23. Look at number 22 for the screenshot