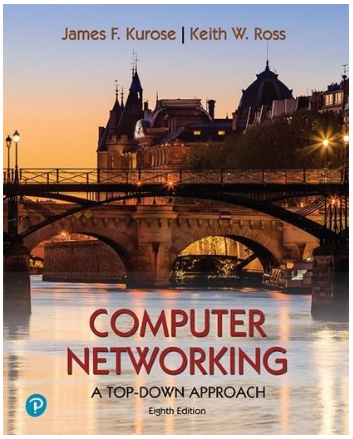
Wireshark Lab: DNS v8.0

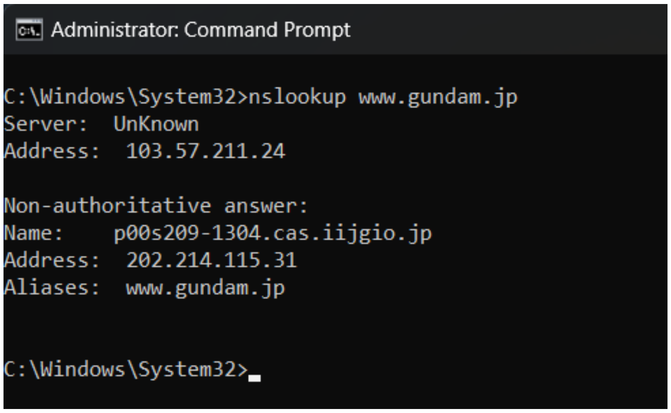
Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



Student Name : Nguyễn Hữu Hiếu
Student ID : 2013149

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



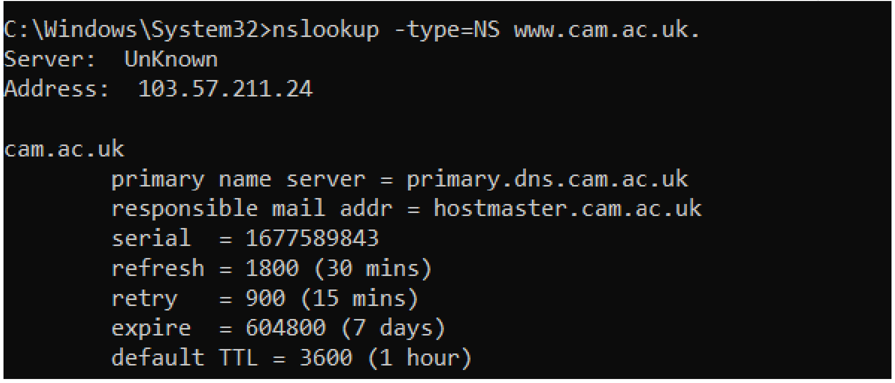
```
C:\Windows\System32>nslookup www.gundam.jp
Server:  UnKnown
Address:  103.57.211.24

Non-authoritative answer:
Name:    p00s209-1304.cas.iijgio.jp
Address:  202.214.115.31
Aliases:  www.gundam.jp


C:\Windows\System32>_
```

Address: 202.214.115.31

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

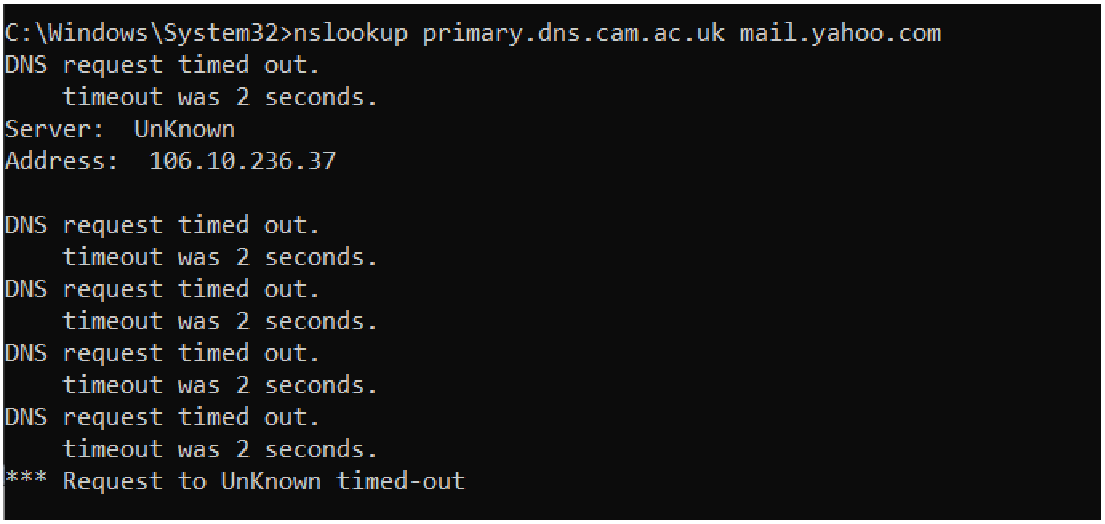


```
C:\Windows\System32>nslookup -type=NS www.cam.ac.uk.
Server:  UnKnown
Address:  103.57.211.24

cam.ac.uk
        primary name server = primary.dns.cam.ac.uk
        responsible mail addr = hostmaster.cam.ac.uk
        serial  = 1677589843
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)
```

The authoritative DNS server for Cambridge is primary.dns.cam.ac.uk

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?

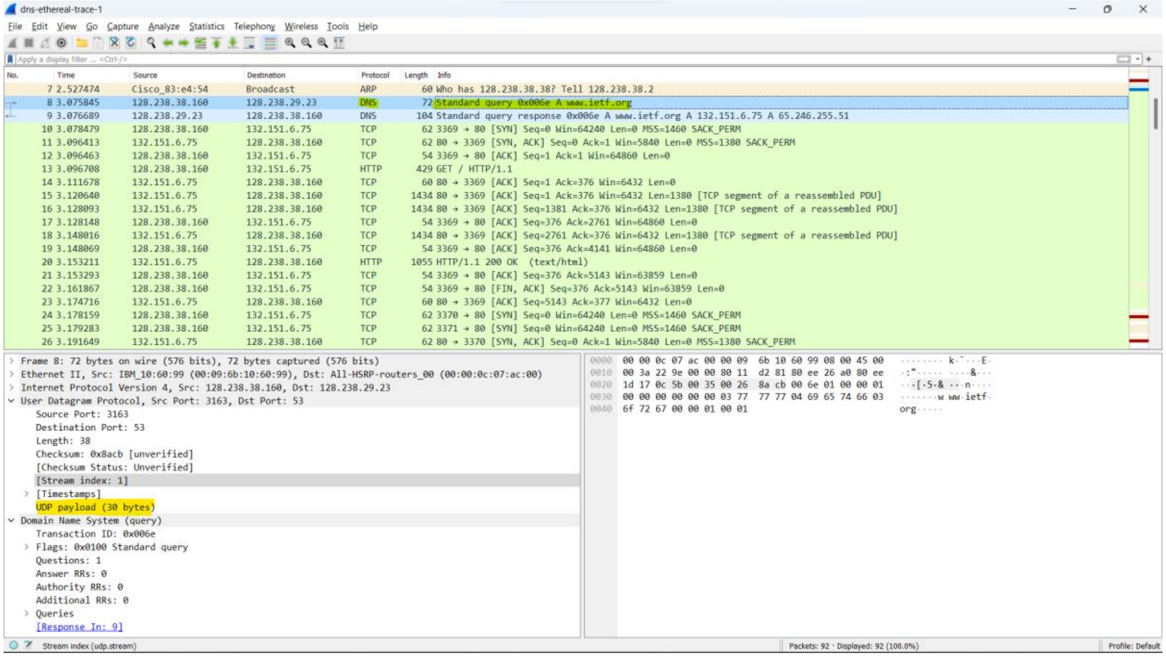


```
C:\Windows\System32>nslookup primary.dns.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  106.10.236.37

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
```

The IP address is 106.10.236.37

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



dns-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source            Destination       Protocol  Length Info
    7 2.527474   Cisco_83:e4:54    Broadcast         ARP         60 Who has 128.238.38.38? Tell 128.238.38.2
    8 3.075845   128.238.38.160    128.238.29.23     DNS         72 Standard query 0x006e A www.ietf.org
    9 3.076689   128.238.29.23     128.238.38.160    DNS        104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
   10 3.078479   128.238.38.160    132.151.6.75      TCP         62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   11 3.096413   132.151.6.75      128.238.38.160    TCP         62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
   12 3.096463   128.238.38.160    132.151.6.75      TCP         54 3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
   13 3.096708   128.238.38.160    132.151.6.75      HTTP       429 GET / HTTP/1.1
   14 3.111678   132.151.6.75      128.238.38.160    TCP         60 80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=0
   15 3.120640   132.151.6.75      128.238.38.160    TCP       1434 80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
   16 3.128093   132.151.6.75      128.238.38.160    TCP       1434 80 → 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
   17 3.128148   128.238.38.160    132.151.6.75      TCP         54 3369 → 80 [ACK] Seq=376 Ack=2761 Win=64860 Len=0
   18 3.148016   132.151.6.75      128.238.38.160    TCP       1434 80 → 3369 [ACK] Seq=2761 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
   19 3.148069   128.238.38.160    132.151.6.75      TCP         54 3369 → 80 [ACK] Seq=376 Ack=4141 Win=64860 Len=0
   20 3.153211   132.151.6.75      128.238.38.160    HTTP      1055 HTTP/1.1 200 OK  (text/html)
   21 3.153293   128.238.38.160    132.151.6.75      TCP         54 3369 → 80 [ACK] Seq=376 Ack=5143 Win=63859 Len=0
   22 3.161867   128.238.38.160    132.151.6.75      TCP         54 3369 → 80 [FIN, ACK] Seq=376 Ack=5143 Win=63859 Len=0
   23 3.174716   132.151.6.75      128.238.38.160    TCP         60 80 → 3369 [ACK] Seq=5143 Ack=377 Win=6432 Len=0
   24 3.178159   128.238.38.160    132.151.6.75      TCP         62 3370 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   25 3.179283   128.238.38.160    132.151.6.75      TCP         62 3371 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   26 3.191649   132.151.6.75      128.238.38.160    TCP         62 80 → 3370 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
```

```
> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
v User Datagram Protocol, Src Port: 3163, Dst Port: 53
    Source Port: 3163
    Destination Port: 53
    Length: 38
    Checksum: 0x8acb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (30 bytes)
v Domain Name System (query)
    Transaction ID: 0x006e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 9]
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3a 22 9e 00 00 80 11  d2 81 80 ee 26 a0 80 ee   ·:"····· ····&···
0020  1d 17 0c 5b 00 35 00 26  8a cb 00 6e 01 00 00 01   ···[·5·& ···n····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····
```

Stream index (udp.stream)
Packets: 92 · Displayed: 92 (100.0%)
Profile: Default

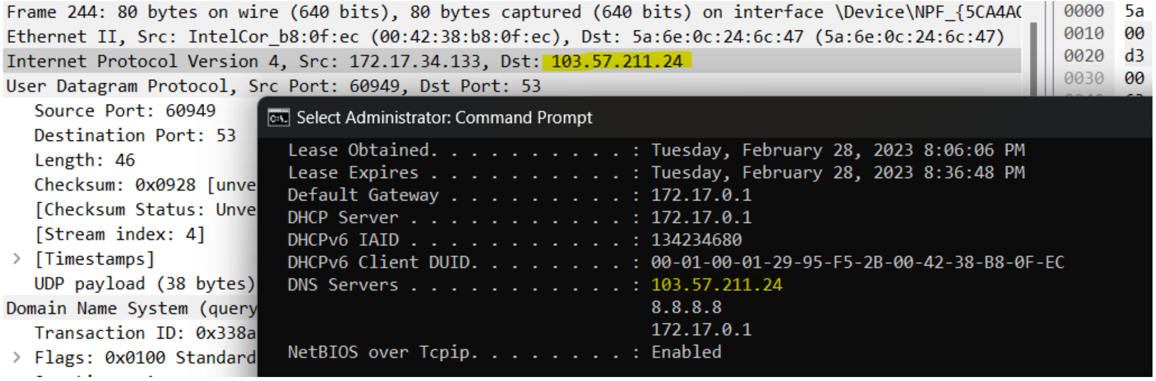
The query and response messages are sent via UDP.

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

Destination Port: 53

Source Port: 3163

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?



```
Frame 244: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{5CA4A(
Ethernet II, Src: IntelCor_b8:0f:ec (00:42:38:b8:0f:ec), Dst: 5a:6e:0c:24:6c:47 (5a:6e:0c:24:6c:47)
Internet Protocol Version 4, Src: 172.17.34.133, Dst: 103.57.211.24
User Datagram Protocol, Src Port: 60949, Dst Port: 53
    Source Port: 60949
    Destination Port: 53
    Length: 46
    Checksum: 0x0928 [unve
    [Checksum Status: Unve
    [Stream index: 4]
  > [Timestamps]
    UDP payload (38 bytes)
Domain Name System (query
    Transaction ID: 0x338a
  > Flags: 0x0100 Standard
```

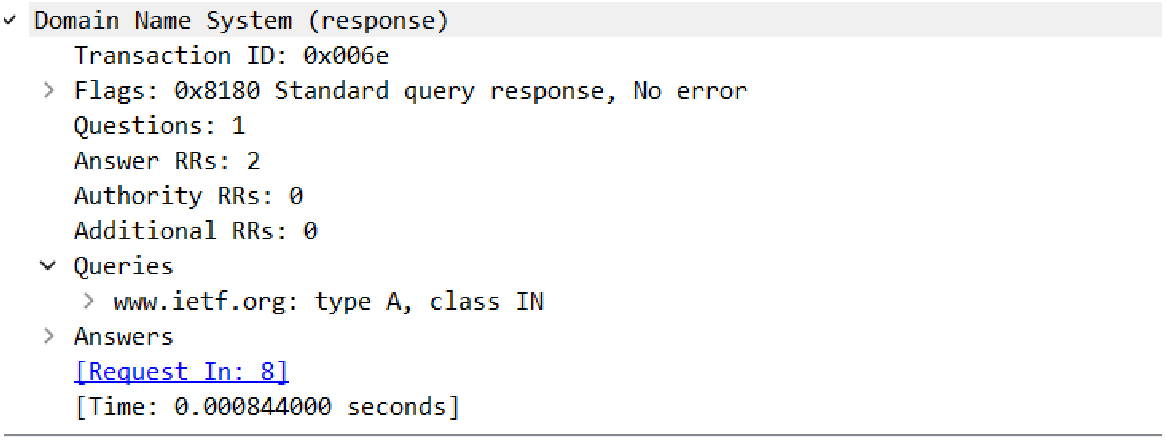
```
0000  5a
0010  00
0020  d3
0030  00
```

Select Administrator: Command Prompt

```
   Lease Obtained. . . . . . . . . . : Tuesday, February 28, 2023 8:06:06 PM
   Lease Expires . . . . . . . . . . : Tuesday, February 28, 2023 8:36:48 PM
   Default Gateway . . . . . . . . . : 172.17.0.1
   DHCP Server . . . . . . . . . . . : 172.17.0.1
   DHCPv6 IAID . . . . . . . . . . . : 134234680
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-95-F5-2B-00-42-38-B8-0F-EC
   DNS Servers . . . . . . . . . . . : 103.57.211.24
                                       8.8.8.8
                                       172.17.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

IP addresses is the same

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

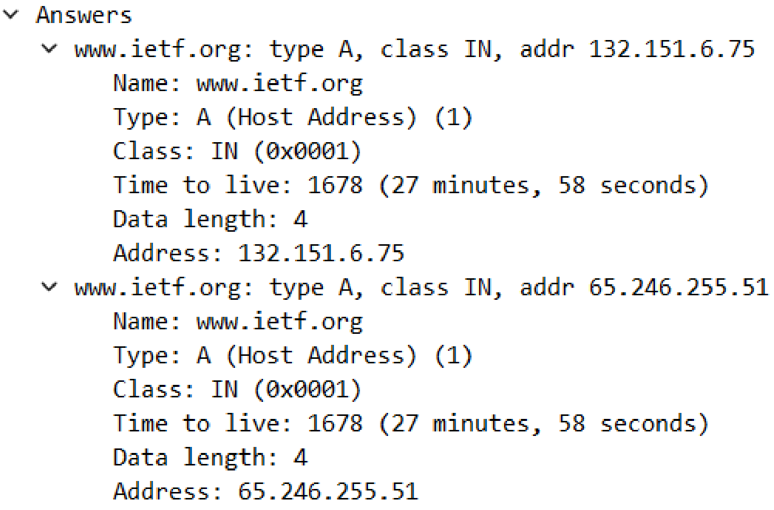


```
v Domain Name System (response)
      Transaction ID: 0x006e
    > Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 2
      Authority RRs: 0
      Additional RRs: 0
    v Queries
        > www.ietf.org: type A, class IN
    > Answers
      [Request In: 8]
      [Time: 0.000844000 seconds]
```

Type A

No answer

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



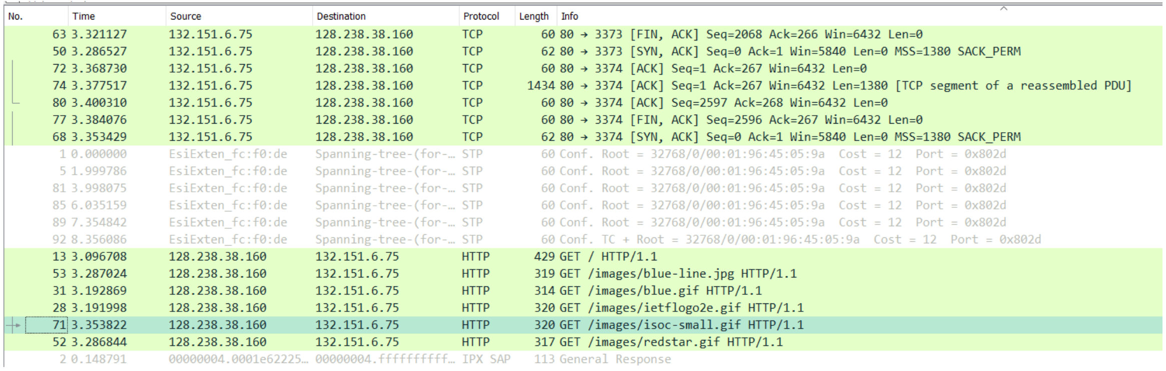
```
v Answers
    v www.ietf.org: type A, class IN, addr 132.151.6.75
          Name: www.ietf.org
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 1678 (27 minutes, 58 seconds)
          Data length: 4
          Address: 132.151.6.75
    v www.ietf.org: type A, class IN, addr 65.246.255.51
          Name: www.ietf.org
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 1678 (27 minutes, 58 seconds)
          Data length: 4
          Address: 65.246.255.51
```

This DNS response message provided two answers. The answers contains the address of the website that it was queried for.

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 destination IP address of the SYN packet corresponds to the address provided by the DNS response, 12.22.58.30.

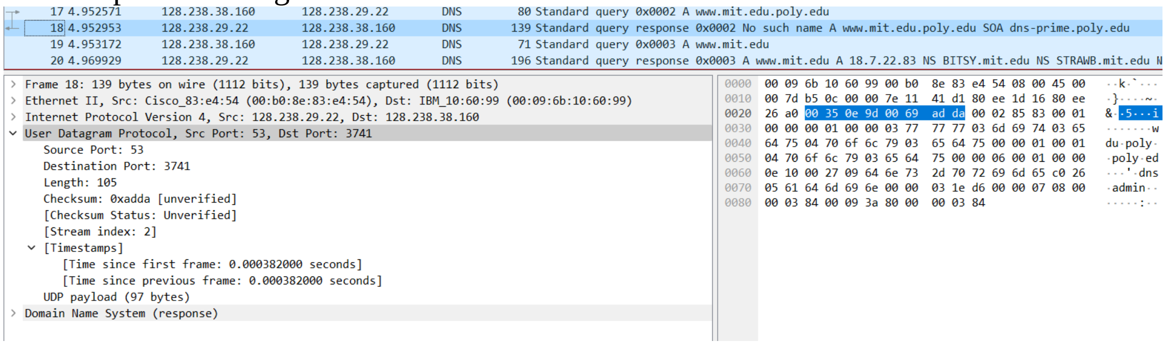
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?



```
No.   Time       Source                  Destination             Protocol  Length  Info
   63 3.321127   132.151.6.75            128.238.38.160          TCP        60 80 → 3373 [FIN, ACK] Seq=2068 Ack=266 Win=6432 Len=0
   50 3.286527   132.151.6.75            128.238.38.160          TCP        62 80 → 3373 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
   72 3.368730   132.151.6.75            128.238.38.160          TCP        60 80 → 3374 [ACK] Seq=1 Ack=267 Win=6432 Len=0
   74 3.377517   132.151.6.75            128.238.38.160          TCP      1434 80 → 3374 [ACK] Seq=1 Ack=267 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
   80 3.400310   132.151.6.75            128.238.38.160          TCP        60 80 → 3374 [ACK] Seq=2597 Ack=268 Win=6432 Len=0
   77 3.384076   132.151.6.75            128.238.38.160          TCP        60 80 → 3374 [FIN, ACK] Seq=2596 Ack=267 Win=6432 Len=0
   68 3.353429   132.151.6.75            128.238.38.160          TCP        62 80 → 3374 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
    1 0.000000   EsiExten_fc:f0:de       Spanning-tree-(for-…    STP        60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
    5 1.999786   EsiExten_fc:f0:de       Spanning-tree-(for-…    STP        60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
   81 3.998075   EsiExten_fc:f0:de       Spanning-tree-(for-…    STP        60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
   85 6.035159   EsiExten_fc:f0:de       Spanning-tree-(for-…    STP        60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
   89 7.354842   EsiExten_fc:f0:de       Spanning-tree-(for-…    STP        60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
   92 8.356086   EsiExten_fc:f0:de       Spanning-tree-(for-…    STP        60 Conf. TC + Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
   13 3.096708   128.238.38.160          132.151.6.75            HTTP      429 GET / HTTP/1.1
   53 3.287024   128.238.38.160          132.151.6.75            HTTP      319 GET /images/blue-line.jpg HTTP/1.1
   31 3.192869   128.238.38.160          132.151.6.75            HTTP      314 GET /images/blue.gif HTTP/1.1
   28 3.191998   128.238.38.160          132.151.6.75            HTTP      320 GET /images/ietflogo2e.gif HTTP/1.1
   71 3.353822   128.238.38.160          132.151.6.75            HTTP      320 GET /images/isoc-small.gif HTTP/1.1
   52 3.286844   128.238.38.160          132.151.6.75            HTTP      317 GET /images/redstar.gif HTTP/1.1
    2 0.148791   00000004.0001e62225…    00000004.ffffffffff…    IPX SAP   113 General Response
```

Yes, the host issues new DNS queries for each image

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



```
   17 4.952571   128.238.38.160   128.238.29.22    DNS    80 Standard query 0x0002 A www.mit.edu.poly.edu
   18 4.952953   128.238.29.22    128.238.38.160   DNS   139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
   19 4.953172   128.238.38.160   128.238.29.22    DNS    71 Standard query 0x0003 A www.mit.edu
   20 4.969929   128.238.29.22    128.238.38.160   DNS   196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu N
```

```
> Frame 18: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
v User Datagram Protocol, Src Port: 53, Dst Port: 3741
    Source Port: 53
    Destination Port: 3741
    Length: 105
    Checksum: 0xadda [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  v [Timestamps]
      [Time since first frame: 0.000382000 seconds]
      [Time since previous frame: 0.000382000 seconds]
    UDP payload (97 bytes)
> Domain Name System (response)
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`···
0010  00 7d b5 0c 00 00 7e 11  41 d1 80 ee 1d 16 80 ee   ·}····~·
0020  26 a0 00 35 0e 9d 00 69  ad da 00 02 85 83 00 01   &··5···i
0030  00 00 00 01 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w
0040  64 75 04 70 6f 6c 79 03  65 64 75 00 00 01 00 01   du·poly·
0050  04 70 6f 6c 79 03 65 64  75 00 00 06 00 01 00 00   ·poly·ed
0060  0e 10 00 27 09 64 6e 73  2d 70 72 69 6d 65 c0 26   ···'·dns
0070  05 61 64 6d 69 6e 00 00  03 1e d6 00 00 07 08 00   ·admin··
0080  00 03 84 00 09 3a 80 00  00 03 84                  ·····:··
```

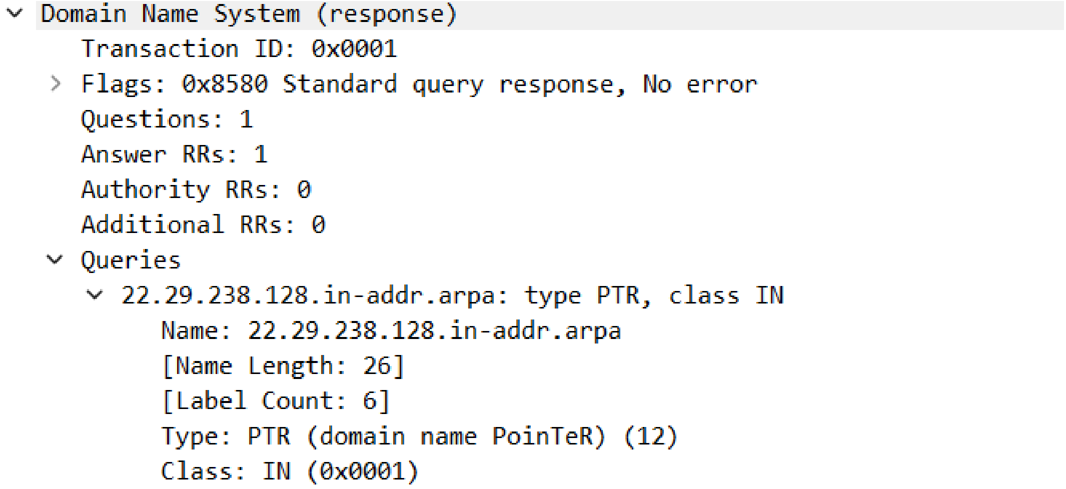
The destination port for the DNS query message is port 53. The source port of the DNS response message is also port 53

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

    I can’t answer this question because my WireShark is not work.

    But I guess Ip address that The DNS query message is the same IP address of local DNS server.

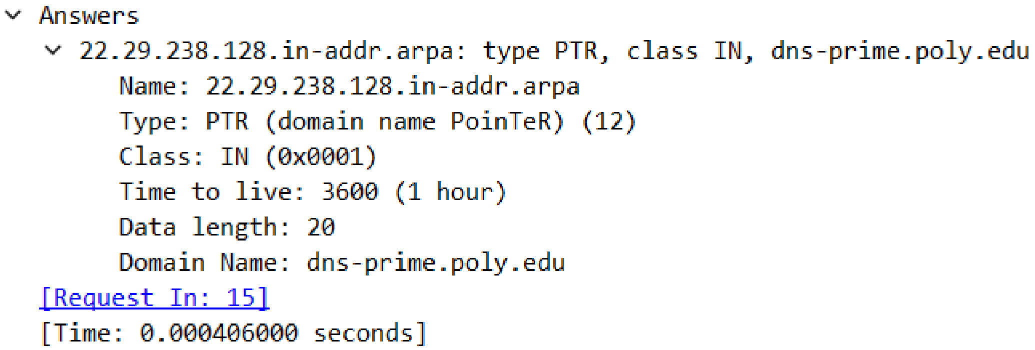
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
Domain Name System (response)
    Transaction ID: 0x0001
  Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    22.29.238.128.in-addr.arpa: type PTR, class IN
        Name: 22.29.238.128.in-addr.arpa
        [Name Length: 26]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
```

This message is of type PTR and contains no answers.

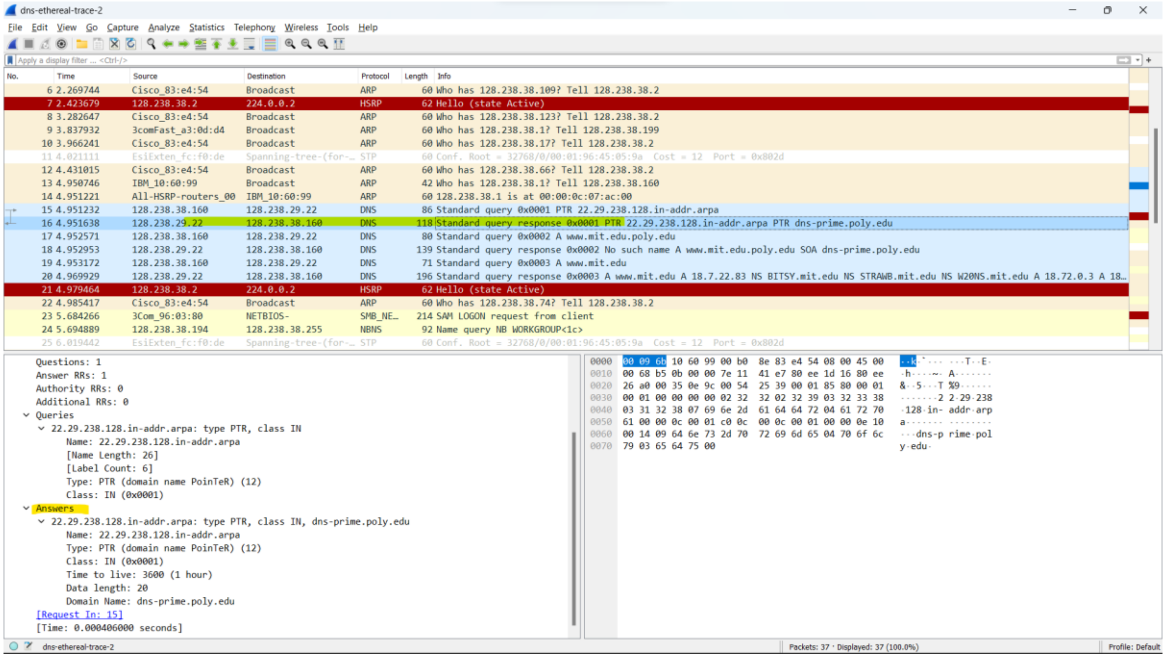
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



```
Answers
  22.29.238.128.in-addr.arpa: type PTR, class IN, dns-prime.poly.edu
      Name: 22.29.238.128.in-addr.arpa
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
      Time to live: 3600 (1 hour)
      Data length: 20
      Domain Name: dns-prime.poly.edu
[Request In: 15]
[Time: 0.000406000 seconds]
```

The first DNS response message contains one answer. This answer contains the next DNS server to query en route to http://www.mit.edu

15. Provide a screenshot.

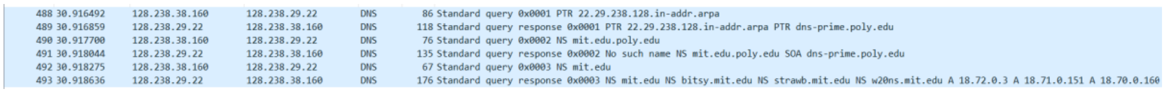

dns-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time        Source               Destination           Protocol  Length Info
  6 2.269744    Cisco_83:e4:54       Broadcast             ARP          60 Who has 128.238.38.109? Tell 128.238.38.2
  7 2.423679    128.238.38.2         224.0.0.2             HSRP         62 Hello (state Active)
  8 3.282647    Cisco_83:e4:54       Broadcast             ARP          60 Who has 128.238.38.123? Tell 128.238.38.2
  9 3.837932    3comFast_a3:0d:d4    Broadcast             ARP          60 Who has 128.238.38.1? Tell 128.238.38.199
 10 3.966241    Cisco_83:e4:54       Broadcast             ARP          60 Who has 128.238.38.17? Tell 128.238.38.2
 11 4.021111    EsiExten_fc:f0:de    Spanning-tree-(for-…  STP          60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
 12 4.431015    Cisco_83:e4:54       Broadcast             ARP          60 Who has 128.238.38.66? Tell 128.238.38.2
 13 4.950746    IBM_10:60:99         Broadcast             ARP          42 Who has 128.238.38.1? Tell 128.238.38.160
 14 4.951221    All-HSRP-routers_00  IBM_10:60:99          ARP          60 128.238.38.1 is at 00:00:0c:07:ac:00
 15 4.951232    128.238.38.160       128.238.29.22         DNS          86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
 16 4.951638    128.238.29.22        128.238.38.160        DNS         118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
 17 4.952571    128.238.38.160       128.238.29.22         DNS          80 Standard query 0x0002 A www.mit.edu.poly.edu
 18 4.952953    128.238.29.22        128.238.38.160        DNS         139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
 19 4.953172    128.238.38.160       128.238.29.22         DNS          71 Standard query 0x0003 A www.mit.edu
 20 4.969929    128.238.29.22        128.238.38.160        DNS         196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 18.72.0.3 A 18…
 21 4.979464    128.238.38.2         224.0.0.2             HSRP         62 Hello (state Active)
 22 4.985417    Cisco_83:e4:54       Broadcast             ARP          60 Who has 128.238.38.74? Tell 128.238.38.2
 23 5.684266    3Com_96:03:80        NETBIOS-              SMB_NE…     214 SAM LOGON request from client
 24 5.694889    128.238.38.194       128.238.38.255        NBNS         92 Name query NB WORKGROUP<1c>
 25 6.019442    EsiExten_fc:f0:de    Spanning-tree-(for-…  STP          60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
```

```
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    ˅ 22.29.238.128.in-addr.arpa: type PTR, class IN
        Name: 22.29.238.128.in-addr.arpa
        [Name Length: 26]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
  ˅ Answers
    ˅ 22.29.238.128.in-addr.arpa: type PTR, class IN, dns-prime.poly.edu
        Name: 22.29.238.128.in-addr.arpa
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 20
        Domain Name: dns-prime.poly.edu
    [Request In: 15]
    [Time: 0.000406000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 68 b5 0b 00 00 7e 11  41 e7 80 ee 1d 16 80 ee   ·h····~· A·······
0020  26 a0 00 35 0e 9c 00 54  25 39 00 01 85 80 00 01   &··5···T %9······
0030  00 01 00 00 00 00 02 32  32 02 32 39 03 32 33 38   ·······2 2·29·238
0040  03 31 32 38 07 69 6e 2d  61 64 64 72 04 61 72 70   ·128·in- addr·arp
0050  61 00 00 0c 00 01 c0 0c  00 0c 00 01 00 00 0e 10   a······· ········
0060  00 14 09 64 6e 73 2d 70  72 69 6d 65 04 70 6f 6c   ···dns-p rime·pol
0070  79 03 65 64 75 00                                  y·edu·
```

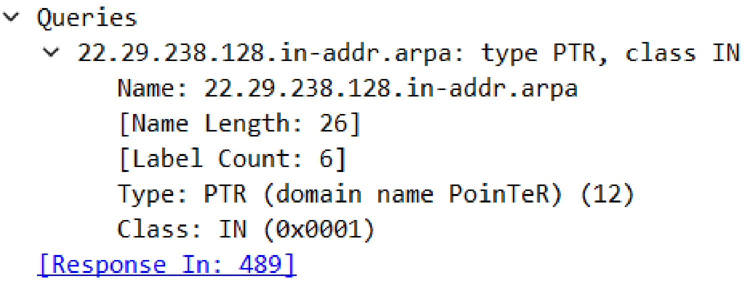
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



```
488 30.916492   128.238.38.160   128.238.29.22    DNS    86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489 30.916859   128.238.29.22    128.238.38.160   DNS   118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490 30.917700   128.238.38.160   128.238.29.22    DNS    76 Standard query 0x0002 NS mit.edu.poly.edu
491 30.918044   128.238.29.22    128.238.38.160   DNS   135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492 30.918275   128.238.38.160   128.238.29.22    DNS    67 Standard query 0x0003 NS mit.edu
493 30.918636   128.238.29.22    128.238.38.160   DNS   176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160
```

IP address of DNS query message sent is 128.238.38.160

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



```
˅ Queries
  ˅ 22.29.238.128.in-addr.arpa: type PTR, class IN
      Name: 22.29.238.128.in-addr.arpa
      [Name Length: 26]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
  [Response In: 489]
```

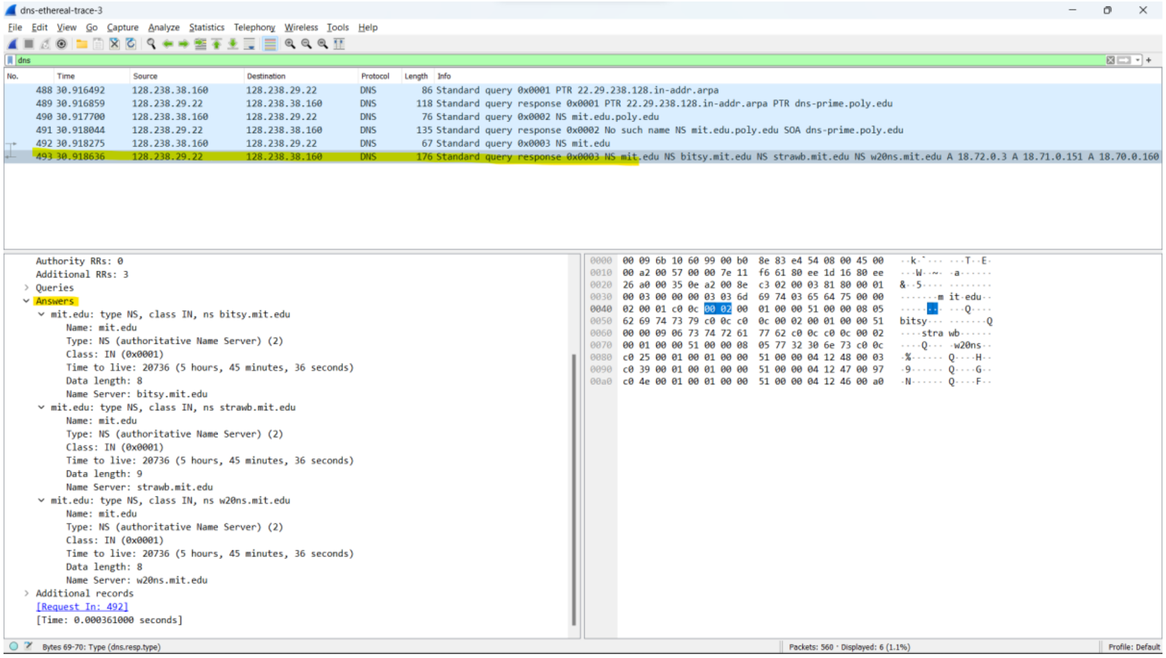
It is a type PTR DNS query that contains no answers.

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?

It provides http://www.mit.edu

This response message does not include IP addresses

19. Provide a screenshot.


dns-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

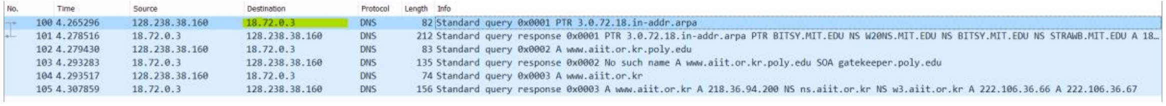
```
No.   Time       Source          Destination     Protocol Length Info
  488 30.916492  128.238.38.160  128.238.29.22   DNS       86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
  489 30.916859  128.238.29.22   128.238.38.160  DNS      118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
  490 30.917700  128.238.38.160  128.238.29.22   DNS       76 Standard query 0x0002 NS mit.edu.poly.edu
  491 30.918044  128.238.29.22   128.238.38.160  DNS      135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
  492 30.918275  128.238.38.160  128.238.29.22   DNS       67 Standard query 0x0003 NS mit.edu
  493 30.918636  128.238.29.22   128.238.38.160  DNS      176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160
```

```
    Authority RRs: 0
    Additional RRs: 3
  > Queries
  v Answers
    v mit.edu: type NS, class IN, ns bitsy.mit.edu
          Name: mit.edu
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
          Time to live: 20736 (5 hours, 45 minutes, 36 seconds)
          Data length: 8
          Name Server: bitsy.mit.edu
    v mit.edu: type NS, class IN, ns strawb.mit.edu
          Name: mit.edu
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
          Time to live: 20736 (5 hours, 45 minutes, 36 seconds)
          Data length: 9
          Name Server: strawb.mit.edu
    v mit.edu: type NS, class IN, ns w20ns.mit.edu
          Name: mit.edu
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
          Time to live: 20736 (5 hours, 45 minutes, 36 seconds)
          Data length: 8
          Name Server: w20ns.mit.edu
  > Additional records
    [Request In: 492]
    [Time: 0.000361000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 a2 00 57 00 00 7e 11  f6 61 80 ee 1d 16 80 ee   ···W··~· ·a······
0020  26 a0 00 35 0e a2 00 8e  c3 02 00 03 81 80 00 01   &··5···· ········
0030  00 03 00 00 00 03 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01 c0 0c 00 02 00  01 00 00 51 00 00 08 05   ········ ···Q····
0050  62 69 74 73 79 c0 0c c0  0c 00 02 00 01 00 00 51   bitsy··· ·······Q
0060  00 00 09 06 73 74 72 61  77 62 c0 0c c0 0c 00 02   ····stra wb······
0070  00 01 00 00 51 00 00 08  05 77 32 30 6e 73 c0 0c   ····Q··· ·w20ns··
0080  c0 25 00 01 00 01 00 00  51 00 00 04 12 48 00 03   ·%······ Q····H··
0090  c0 39 00 01 00 01 00 00  51 00 00 04 12 47 00 97   ·9······ Q····G··
00a0  c0 4e 00 01 00 01 00 00  51 00 00 04 12 46 00 a0   ·N······ Q····F··
```

Bytes 69-70: Type (dns.resp.type)
Packets: 560 · Displayed: 6 (1.1%)
Profile: Default

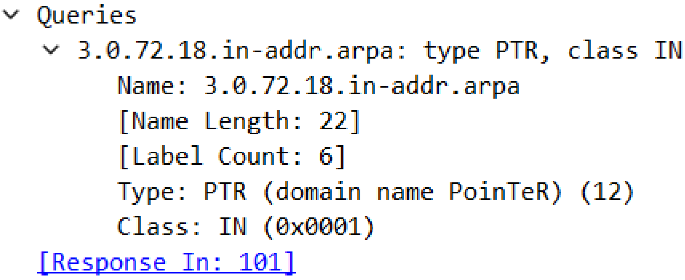
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?



```
No.   Time      Source          Destination     Protocol Length Info
  100 4.265296  128.238.38.160  18.72.0.3       DNS       82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
  101 4.278516  18.72.0.3       128.238.38.160  DNS      212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18…
  102 4.279430  128.238.38.160  18.72.0.3       DNS       83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
  103 4.293283  18.72.0.3       128.238.38.160  DNS      135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
  104 4.293517  128.238.38.160  18.72.0.3       DNS       74 Standard query 0x0003 A www.aiit.or.kr
  105 4.307859  18.72.0.3       128.238.38.160  DNS      156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A 222.106.36.67
```

The DNS query message is sent to 18.72.0.3 which is not the same as my local DNS server. This IP address corresponds to www.aiit.or.kr.

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



```
v Queries
  v 3.0.72.18.in-addr.arpa: type PTR, class IN
        Name: 3.0.72.18.in-addr.arpa
        [Name Length: 22]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
  [Response In: 101]
```

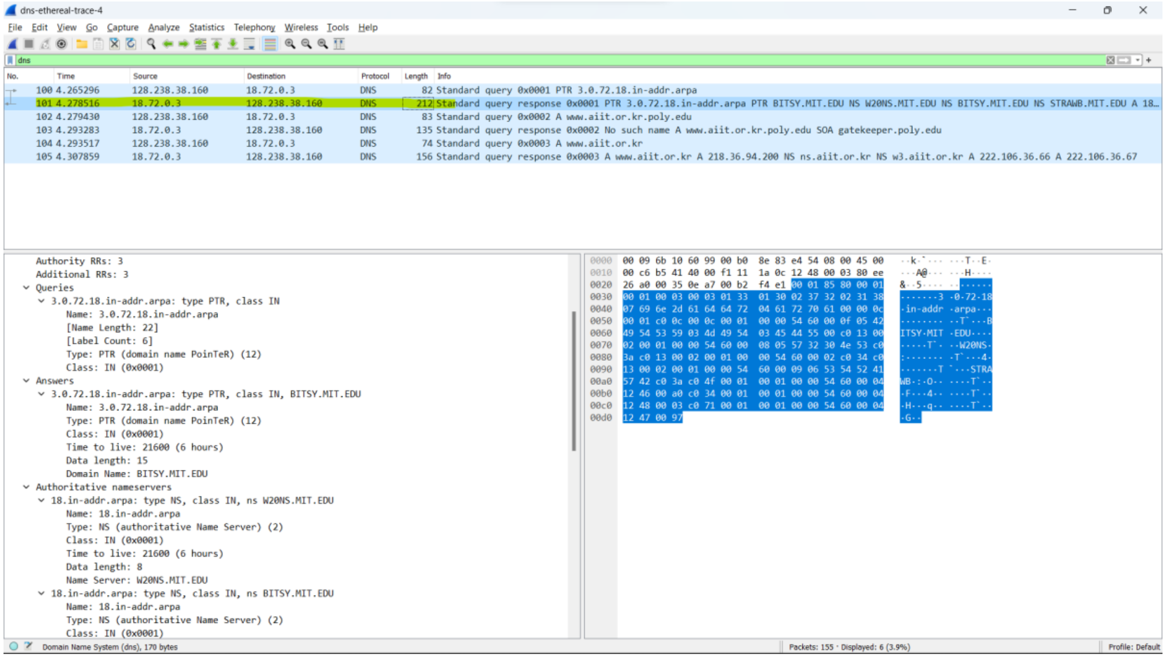
The DNS query message is a Domain name pointer, type PTR, and does not contain any answers.

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

It contain the ip address of each of them

23. Provide a screenshot.

24.



dns-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.      Time      Source          Destination     Protocol Length Info
     100 4.265296  128.238.38.160  18.72.0.3       DNS       82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
     101 4.278516  18.72.0.3       128.238.38.160  DNS      212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18…
     102 4.279430  128.238.38.160  18.72.0.3       DNS       83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
     103 4.293283  18.72.0.3       128.238.38.160  DNS      135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
     104 4.293517  128.238.38.160  18.72.0.3       DNS       74 Standard query 0x0003 A www.aiit.or.kr
     105 4.307859  18.72.0.3       128.238.38.160  DNS      156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A 222.106.36.67
```

```
    Authority RRs: 3
    Additional RRs: 3
  ˅ Queries
    ˅ 3.0.72.18.in-addr.arpa: type PTR, class IN
        Name: 3.0.72.18.in-addr.arpa
        [Name Length: 22]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
  ˅ Answers
    ˅ 3.0.72.18.in-addr.arpa: type PTR, class IN, BITSY.MIT.EDU
        Name: 3.0.72.18.in-addr.arpa
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
        Time to live: 21600 (6 hours)
        Data length: 15
        Domain Name: BITSY.MIT.EDU
  ˅ Authoritative nameservers
    ˅ 18.in-addr.arpa: type NS, class IN, ns W20NS.MIT.EDU
        Name: 18.in-addr.arpa
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 21600 (6 hours)
        Data length: 8
        Name Server: W20NS.MIT.EDU
    ˅ 18.in-addr.arpa: type NS, class IN, ns BITSY.MIT.EDU
        Name: 18.in-addr.arpa
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 c6 b5 41 40 00 f1 11  1a 0c 12 48 00 03 80 ee   ···A@··· ···H····
0020  26 a0 00 35 0e a7 00 b2  f4 e1 00 01 85 80 00 01   &··5···· ········
0030  00 01 00 03 00 03 01 33  01 30 02 37 32 02 31 38   ·······3 ·0·72·18
0040  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00 0c   ·in-addr ·arpa···
0050  00 01 c0 0c 00 0c 00 01  00 00 54 60 00 0f 05 42   ········ ··T`···B
0060  49 54 53 59 03 4d 49 54  03 45 44 55 00 c0 13 00   ITSY·MIT ·EDU····
0070  02 00 01 00 00 54 60 00  08 05 57 32 30 4e 53 c0   ·····T`· ··W20NS·
0080  3a c0 13 00 02 00 01 00  00 54 60 00 02 c0 34 c0   :······· ·T`···4·
0090  13 00 02 00 01 00 00 54  60 00 09 06 53 54 52 41   ·······T `···STRA
00a0  57 42 c0 3a c0 4f 00 01  00 01 00 00 54 60 00 04   WB·:·O·· ····T`··
00b0  12 46 00 a0 c0 34 00 01  00 01 00 00 54 60 00 04   ·F···4·· ····T`··
00c0  12 48 00 03 c0 71 00 01  00 01 00 00 54 60 00 04   ·H···q·· ····T`··
00d0  12 47 00 97                                        ·G··
```

Domain Name System (dns), 170 bytes

Packets: 155 · Displayed: 6 (3.9%)

Profile: Default