VIET NAM NATIONAL UNIVERSITY HO CHI MINH CITY
HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

ASSIGNMENT REPORT

LAB 3b

COMPUTER NETWORK

Instructor: PROF. NGUYEN MANH THIN

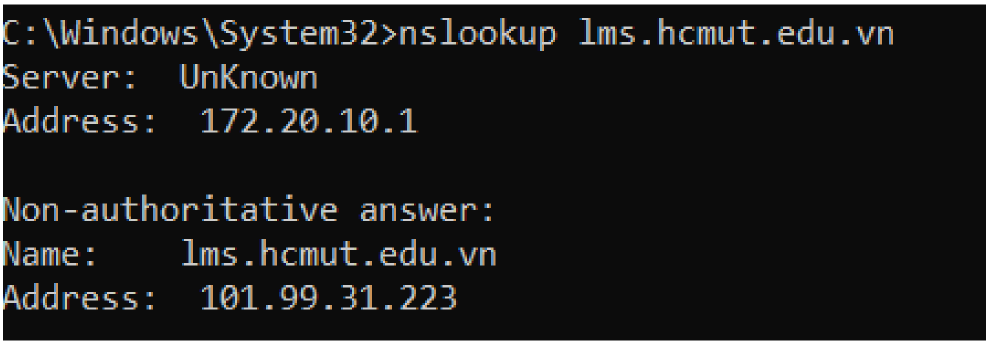
HO CHI MINH CITY, APRIL 2024

Contents

1 nslookup command

1.1 Run nslookup to obtain the IP address of a Web server in Asia

To begin with, I will use the command for the HCMUT-LMS website. The output will be as below:



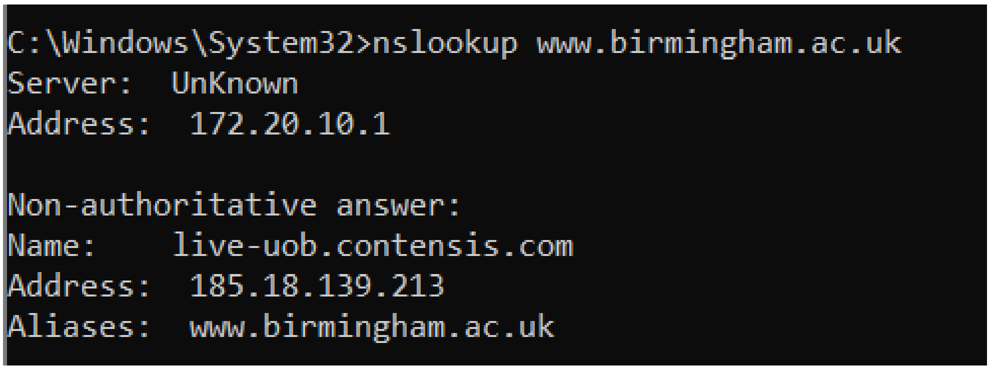
```
C:\Windows\System32>nslookup lms.hcmut.edu.vn
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    lms.hcmut.edu.vn
Address:  101.99.31.223
```

Figure 1: The output of the command.

IP address of the server: **101.99.31.223**

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

In this exercise, I choose Birmingham University in the UK. Here is the answer:



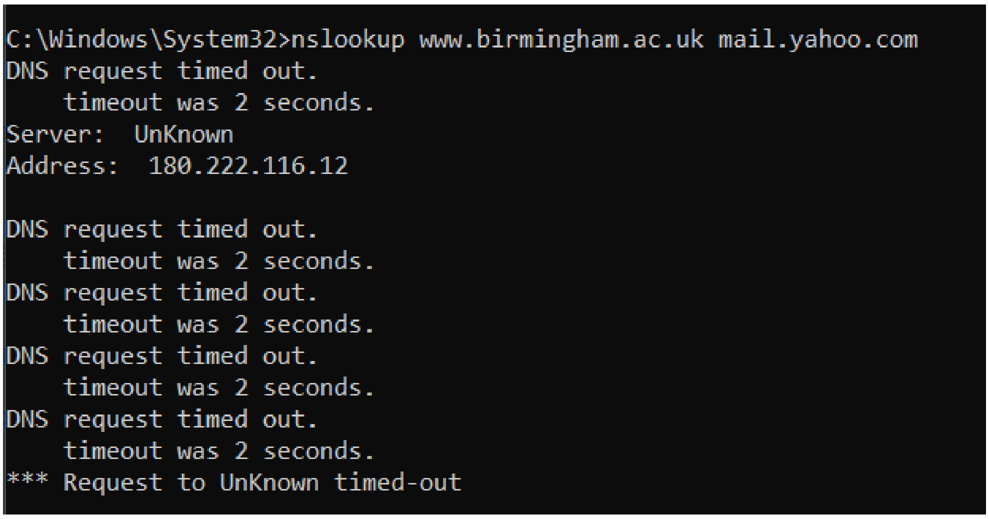
```
C:\Windows\System32>nslookup www.birmingham.ac.uk
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    live-uob.contensis.com
Address:  185.18.139.213
Aliases:  www.birmingham.ac.uk
```

Figure 2: Birmingham University

IP address of the Europe University server: **185.18.139.213**

1.3 Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.

The output will be as below:



```
C:\Windows\System32>nslookup www.birmingham.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  180.222.116.12

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
```

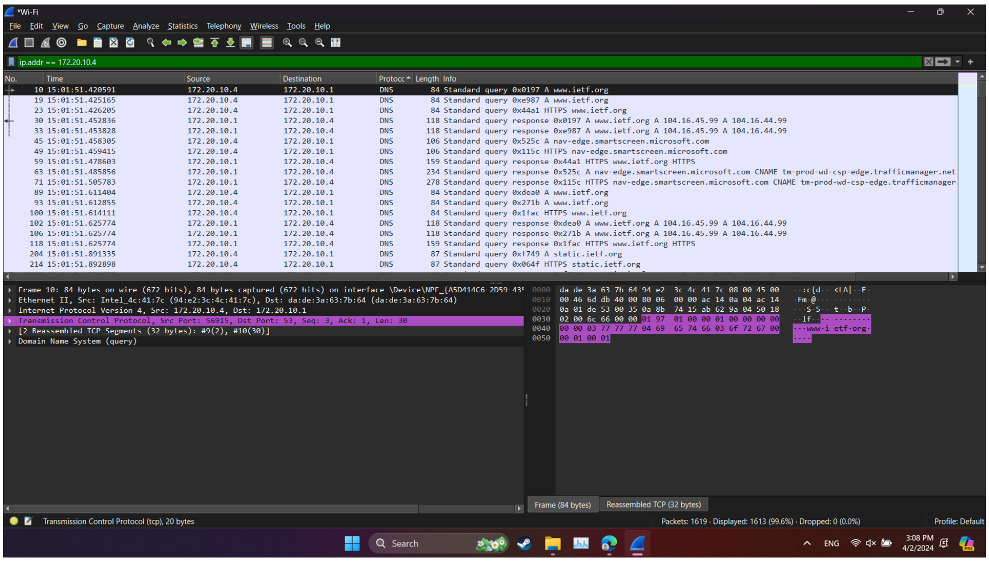
Figure 3: Mail server.

IP address of Yahoo! mail server: **180.222.116.12**

2 Tracing DNS with Wireshark

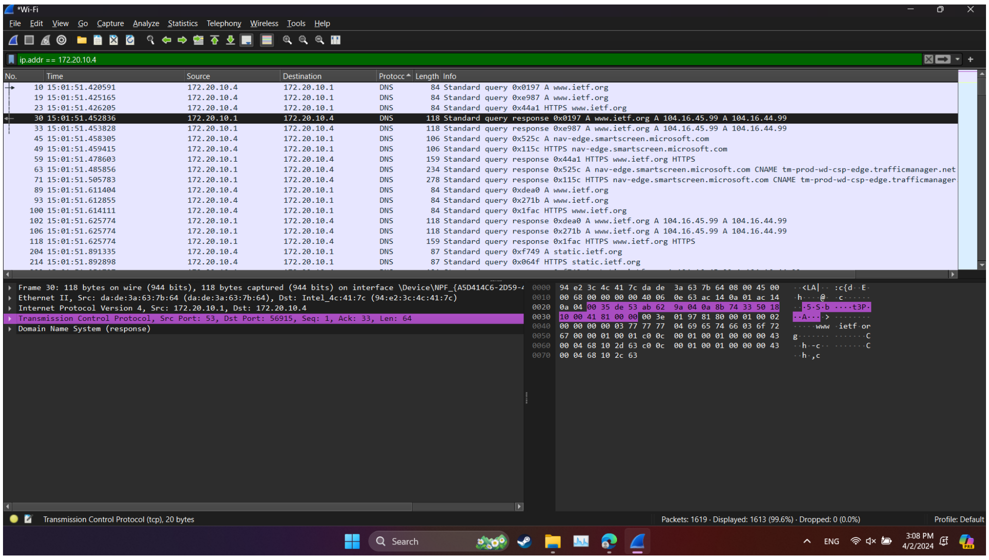
2.1 Locate the DNS query and response messages. Are then sent over UDP or TCP.

Here is the output picture:



```
ip.addr == 172.20.10.4

No.  Time             Source        Destination   Protocol Length Info
  10 15:01:51.420591  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x0197 A www.ietf.org
  19 15:01:51.425165  172.20.10.4   172.20.10.1   DNS       84 Standard query 0xe987 A www.ietf.org
  23 15:01:51.426205  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x44a1 HTTPS www.ietf.org
  30 15:01:51.452836  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0x0197 A www.ietf.org A 104.16.45.99 A 104.16.44.99
  33 15:01:51.453828  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0xe987 A www.ietf.org A 104.16.45.99 A 104.16.44.99
  45 15:01:51.458305  172.20.10.4   172.20.10.1   DNS      106 Standard query 0x525c A nav-edge.smartscreen.microsoft.com
  49 15:01:51.459415  172.20.10.4   172.20.10.1   DNS      106 Standard query 0x115c HTTPS nav-edge.smartscreen.microsoft.com
  59 15:01:51.478603  172.20.10.1   172.20.10.4   DNS      159 Standard query response 0x44a1 HTTPS www.ietf.org HTTPS
  63 15:01:51.485856  172.20.10.1   172.20.10.4   DNS      234 Standard query response 0x525c A nav-edge.smartscreen.microsoft.com CNAME tm-prod-wd-csp-edge.trafficmanager.net
  71 15:01:51.505783  172.20.10.1   172.20.10.4   DNS      278 Standard query response 0x115c HTTPS nav-edge.smartscreen.microsoft.com CNAME tm-prod-wd-csp-edge.trafficmanager
  89 15:01:51.611404  172.20.10.4   172.20.10.1   DNS       84 Standard query 0xdea0 A www.ietf.org
  93 15:01:51.612855  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x271b A www.ietf.org
 100 15:01:51.614111  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x1fac HTTPS www.ietf.org
 102 15:01:51.625774  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0xdea0 A www.ietf.org A 104.16.45.99 A 104.16.44.99
 106 15:01:51.625774  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0x271b A www.ietf.org A 104.16.45.99 A 104.16.44.99
 118 15:01:51.625774  172.20.10.1   172.20.10.4   DNS      159 Standard query response 0x1fac HTTPS www.ietf.org HTTPS
 204 15:01:51.891335  172.20.10.4   172.20.10.1   DNS       87 Standard query 0xf749 A static.ietf.org
 214 15:01:51.892898  172.20.10.4   172.20.10.1   DNS       87 Standard query 0x064f HTTPS static.ietf.org

> Frame 10: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{A5D414C6-2D59-43
> Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
> Transmission Control Protocol, Src Port: 56915, Dst Port: 53, Seq: 3, Ack: 1, Len: 30
> [2 Reassembled TCP Segments (32 bytes): #9(2), #10(30)]
> Domain Name System (query)

0000  da de 3a 63 7b 64 94 e2  3c 4c 41 7c 08 00 45 00   ··:c{d·· <LA|··E·
0010  00 46 6d db 40 00 80 06  00 00 ac 14 0a 04 ac 14   ·Fm·@··· ········
0020  0a 01 de 53 00 35 0a 8b  74 15 ab 62 9a 04 50 18   ···S·5·· t··b··P·
0030  02 00 6c 66 00 00 01 97  01 00 00 01 00 00 00 00   ··lf···· ········
0040  00 00 03 77 77 77 04 69  65 74 66 03 6f 72 67 00   ···www·i etf·org·
0050  00 01 00 01                                        ····

Frame (84 bytes)   Reassembled TCP (32 bytes)

Transmission Control Protocol (tcp), 20 bytes     Packets: 1619 · Displayed: 1613 (99.6%) · Dropped: 0 (0.0%)     Profile: Default
```

Figure 4: DNS query message.



```
ip.addr == 172.20.10.4

No.  Time             Source        Destination   Protocol Length Info
  10 15:01:51.420591  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x0197 A www.ietf.org
  19 15:01:51.425165  172.20.10.4   172.20.10.1   DNS       84 Standard query 0xe987 A www.ietf.org
  23 15:01:51.426205  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x44a1 HTTPS www.ietf.org
  30 15:01:51.452836  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0x0197 A www.ietf.org A 104.16.45.99 A 104.16.44.99
  33 15:01:51.453828  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0xe987 A www.ietf.org A 104.16.45.99 A 104.16.44.99
  45 15:01:51.458305  172.20.10.4   172.20.10.1   DNS      106 Standard query 0x525c A nav-edge.smartscreen.microsoft.com
  49 15:01:51.459415  172.20.10.4   172.20.10.1   DNS      106 Standard query 0x115c HTTPS nav-edge.smartscreen.microsoft.com
  59 15:01:51.478603  172.20.10.1   172.20.10.4   DNS      159 Standard query response 0x44a1 HTTPS www.ietf.org HTTPS
  63 15:01:51.485856  172.20.10.1   172.20.10.4   DNS      234 Standard query response 0x525c A nav-edge.smartscreen.microsoft.com CNAME tm-prod-wd-csp-edge.trafficmanager.net
  71 15:01:51.505783  172.20.10.1   172.20.10.4   DNS      278 Standard query response 0x115c HTTPS nav-edge.smartscreen.microsoft.com CNAME tm-prod-wd-csp-edge.trafficmanager
  89 15:01:51.611404  172.20.10.4   172.20.10.1   DNS       84 Standard query 0xdea0 A www.ietf.org
  93 15:01:51.612855  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x271b A www.ietf.org
 100 15:01:51.614111  172.20.10.4   172.20.10.1   DNS       84 Standard query 0x1fac HTTPS www.ietf.org
 102 15:01:51.625774  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0xdea0 A www.ietf.org A 104.16.45.99 A 104.16.44.99
 106 15:01:51.625774  172.20.10.1   172.20.10.4   DNS      118 Standard query response 0x271b A www.ietf.org A 104.16.45.99 A 104.16.44.99
 118 15:01:51.625774  172.20.10.1   172.20.10.4   DNS      159 Standard query response 0x1fac HTTPS www.ietf.org HTTPS
 204 15:01:51.891335  172.20.10.4   172.20.10.1   DNS       87 Standard query 0xf749 A static.ietf.org
 214 15:01:51.892898  172.20.10.4   172.20.10.1   DNS       87 Standard query 0x064f HTTPS static.ietf.org

> Frame 30: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{A5D414C6-2D59-4
> Ethernet II, Src: da:de:3a:63:7b:64 (da:de:3a:63:7b:64), Dst: Intel_4c:41:7c (94:e2:3c:4c:41:7c)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.4
> Transmission Control Protocol, Src Port: 53, Dst Port: 56915, Seq: 1, Ack: 33, Len: 64
> Domain Name System (response)

0000  94 e2 3c 4c 41 7c da de  3a 63 7b 64 08 00 45 00   ··<LA|·· :c{d··E·
0010  00 68 00 00 00 00 40 06  0e 63 ac 14 0a 01 ac 14   ·h····@· ·c······
0020  0a 04 00 35 de 53 ab 62  9a 04 0a 8b 74 33 50 18   ···5·S·b ····t3P·
0030  10 00 41 81 00 00 00 3e  01 97 81 80 00 01 00 02   ··A····> ········
0040  00 00 00 00 03 77 77 77  04 69 65 74 66 03 6f 72   ·····www ·ietf·or
0050  67 00 00 01 00 01 c0 0c  00 01 00 01 00 00 00 43   g······· ·······C
0060  00 04 68 10 2d 63 c0 0c  00 01 00 01 00 00 00 43   ··h·-c·· ·······C
0070  00 04 68 10 2c 63                                  ··h·,c

Transmission Control Protocol (tcp), 20 bytes     Packets: 1619 · Displayed: 1613 (99.6%) · Dropped: 0 (0.0%)     Profile: Default
```

Figure 5: DNS response message.

It can be seen that both are used TCP protocol.

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

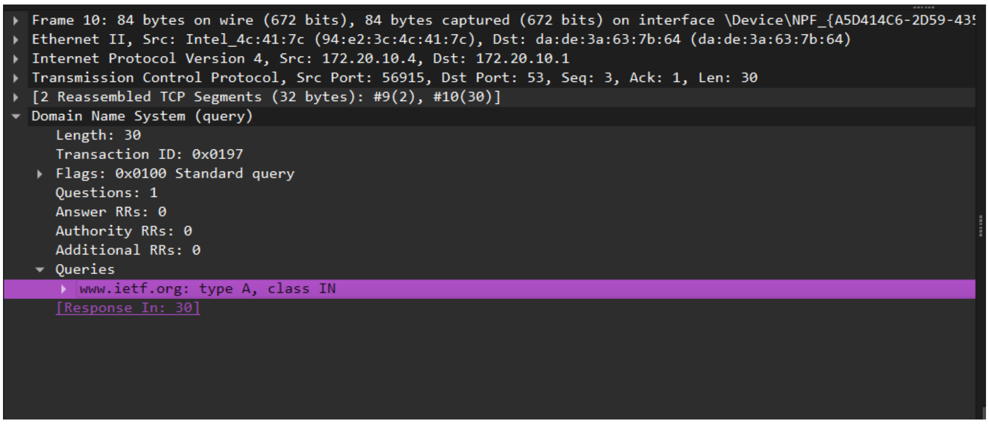
- The destination port of **DNS query message**: 53
- The source port of **DNS response message**: 53

2.3 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 **172.20.10.1**, which is the IP address of one of my local DNS server.

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

It's a **type A** and it doesn't contain any answers.

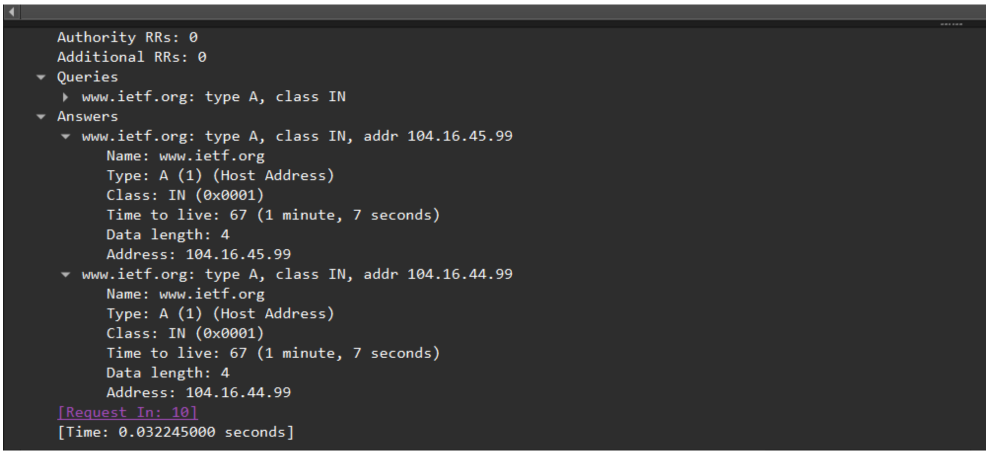


```
Frame 10: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{A5D414C6-2D59-43
Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
Transmission Control Protocol, Src Port: 56915, Dst Port: 53, Seq: 3, Ack: 1, Len: 30
[2 Reassembled TCP Segments (32 bytes): #9(2), #10(30)]
Domain Name System (query)
  Length: 30
  Transaction ID: 0x0197
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.ietf.org: type A, class IN
  [Response In: 30]
```

Figure 6: DNS query information

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

There are two answers and both of them contain the information about the name of the host, the typeof address, class, the TTL, the data length and the IP address.



```
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.ietf.org: type A, class IN
  Answers
    www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 67 (1 minute, 7 seconds)
      Data length: 4
      Address: 104.16.45.99
    www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 67 (1 minute, 7 seconds)
      Data length: 4
      Address: 104.16.44.99
  [Request In: 10]
  [Time: 0.032245000 seconds]
```

Figure 7: DNS response message.

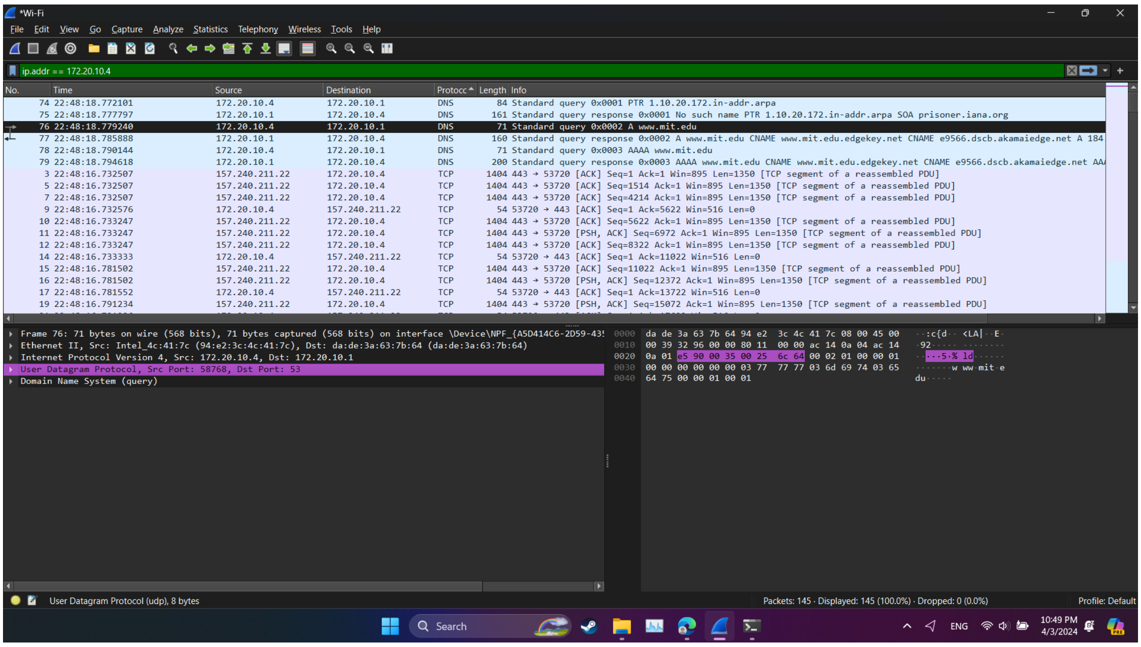
2.6 Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The first SYN packet was sent to 104.16.44.99 which corresponds to the first IP address provided in the DNS response message.

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

No, we don't need any DNS queries more due to the fact that the images have been loaded in ietf.org

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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Search
ENG
10:49 PM
4/3/2024

ip.addr == 172.20.10.4

```
No.  Time             Source          Destination     Protocol Length Info
  74 22:48:18.772101  172.20.10.4     172.20.10.1     DNS        84 Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
  75 22:48:18.777797  172.20.10.1     172.20.10.4     DNS       161 Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA prisoner.iana.org
  76 22:48:18.779240  172.20.10.4     172.20.10.1     DNS        71 Standard query 0x0002 A www.mit.edu
  77 22:48:18.785888  172.20.10.1     172.20.10.4     DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184
  78 22:48:18.790144  172.20.10.4     172.20.10.1     DNS        71 Standard query 0x0003 AAAA www.mit.edu
  79 22:48:18.794618  172.20.10.1     172.20.10.4     DNS       200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AA
   3 22:48:16.732507  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=1 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   5 22:48:16.732507  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=1514 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   7 22:48:16.732507  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=4214 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   9 22:48:16.732576  172.20.10.4     157.240.211.22  TCP        54 53720 → 443 [ACK] Seq=1 Ack=5622 Win=516 Len=0
  10 22:48:16.733247  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=5622 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  11 22:48:16.733247  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [PSH, ACK] Seq=6972 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  12 22:48:16.733247  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=8322 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  14 22:48:16.733333  172.20.10.4     157.240.211.22  TCP        54 53720 → 443 [ACK] Seq=1 Ack=11022 Win=516 Len=0
  15 22:48:16.781502  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=11022 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  16 22:48:16.781502  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [PSH, ACK] Seq=12372 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  17 22:48:16.781552  172.20.10.4     157.240.211.22  TCP        54 53720 → 443 [ACK] Seq=1 Ack=13722 Win=516 Len=0
  19 22:48:16.791234  157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [PSH, ACK] Seq=15072 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
```

```
> Frame 76: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{A5D414C6-2D59-43
> Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 58768, Dst Port: 53
> Domain Name System (query)
```

```
0000  da de 3a 63 7b 64 94 e2  3c 4c 41 7c 08 00 45 00   ··:c{d·· <LA|··E·
0010  00 39 32 96 00 00 80 11  00 00 ac 14 0a 04 ac 14   ·92····· ········
0020  0a 01 e5 90 00 35 00 25  6c 64 00 02 01 00 00 01   ·····5·% ld······
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

User Datagram Protocol (udp), 8 bytes

Packets: 145 · Displayed: 145 (100.0%) · Dropped: 0 (0.0%)

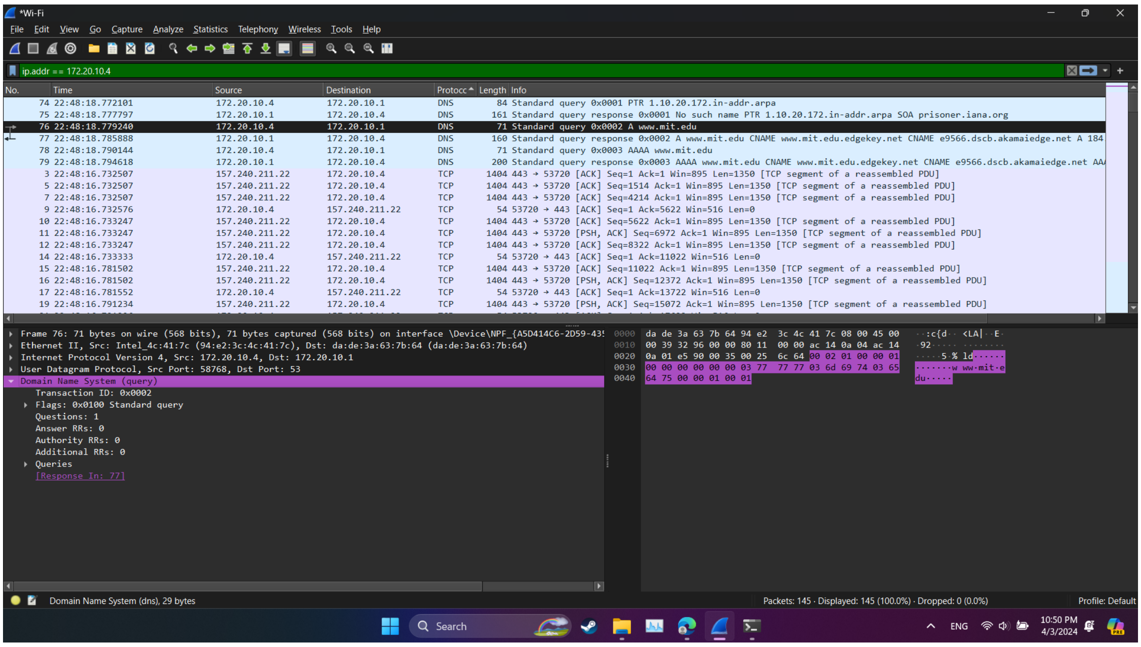
Profile: Default

Destination Port: 53. Source Port: 58768.

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

It's sent to 172.20.10.1, which is the IP address of one of my local DNS servers.

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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 172.20.10.4
Domain Name System (dns), 29 bytes
Packets: 145 · Displayed: 145 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Search
ENG
10:50 PM
4/3/2024

```
No.  Time             Source          Destination     Protocol Length Info
 74 22:48:18.772101   172.20.10.4     172.20.10.1     DNS      84 Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
 75 22:48:18.777797   172.20.10.1     172.20.10.4     DNS     161 Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA prisoner.iana.org
 76 22:48:18.779240   172.20.10.4     172.20.10.1     DNS      71 Standard query 0x0002 A www.mit.edu
 77 22:48:18.785888   172.20.10.1     172.20.10.4     DNS     160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184
 78 22:48:18.790144   172.20.10.4     172.20.10.1     DNS      71 Standard query 0x0003 AAAA www.mit.edu
 79 22:48:18.794618   172.20.10.1     172.20.10.4     DNS     200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AA
  3 22:48:16.732507   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [ACK] Seq=1 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  5 22:48:16.732507   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [ACK] Seq=1514 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  7 22:48:16.732507   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [ACK] Seq=4214 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
  9 22:48:16.732576   172.20.10.4     157.240.211.22  TCP      54 53720 → 443 [ACK] Seq=1 Ack=5622 Win=516 Len=0
 10 22:48:16.733247   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [ACK] Seq=5622 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
 11 22:48:16.733247   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [PSH, ACK] Seq=6972 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
 12 22:48:16.733247   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [ACK] Seq=8322 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
 14 22:48:16.733333   172.20.10.4     157.240.211.22  TCP      54 53720 → 443 [ACK] Seq=1 Ack=11022 Win=516 Len=0
 15 22:48:16.781502   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [ACK] Seq=11022 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
 16 22:48:16.781502   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [PSH, ACK] Seq=12372 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
 17 22:48:16.781552   172.20.10.4     157.240.211.22  TCP      54 53720 → 443 [ACK] Seq=1 Ack=13722 Win=516 Len=0
 19 22:48:16.791234   157.240.211.22  172.20.10.4     TCP    1404 443 → 53720 [PSH, ACK] Seq=15072 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
```

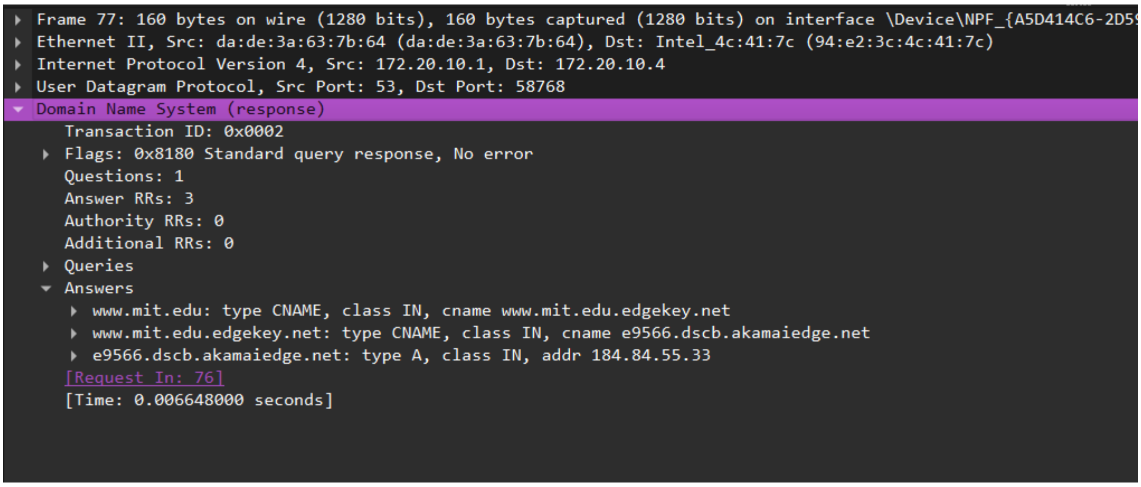
```
▸ Frame 76: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{A5D414C6-2D59-43
▸ Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
▸ Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
▸ User Datagram Protocol, Src Port: 58768, Dst Port: 53
▾ 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: 77]
```

```
0000  da de 3a 63 7b 64 94 e2  3c 4c 41 7c 08 00 45 00   ··:c{d·· <LA|··E·
0010  00 39 32 96 00 00 80 11  00 00 ac 14 0a 04 ac 14   ·92····· ········
0020  0a 01 e5 90 00 35 00 25  6c 64 00 02 01 00 00 01   ·····5·% ld······
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

The query is of type A and it doesn't contain any answers.

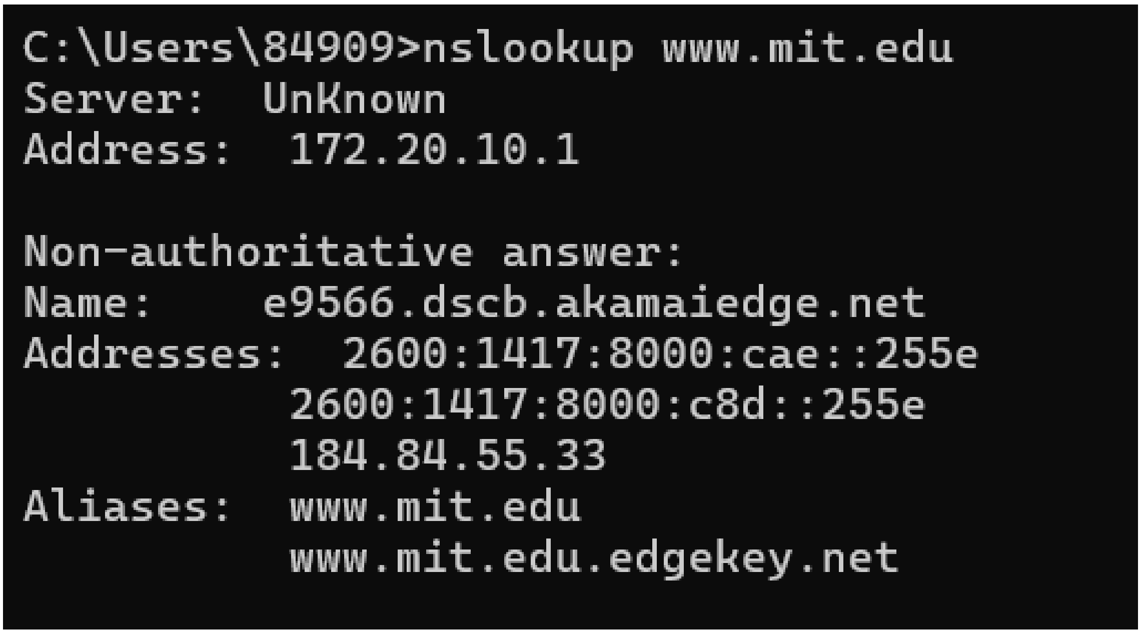
2.11 Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

The response DNS message contains 3 answers containing the name of the host, the type of address, the class, and the IP address.

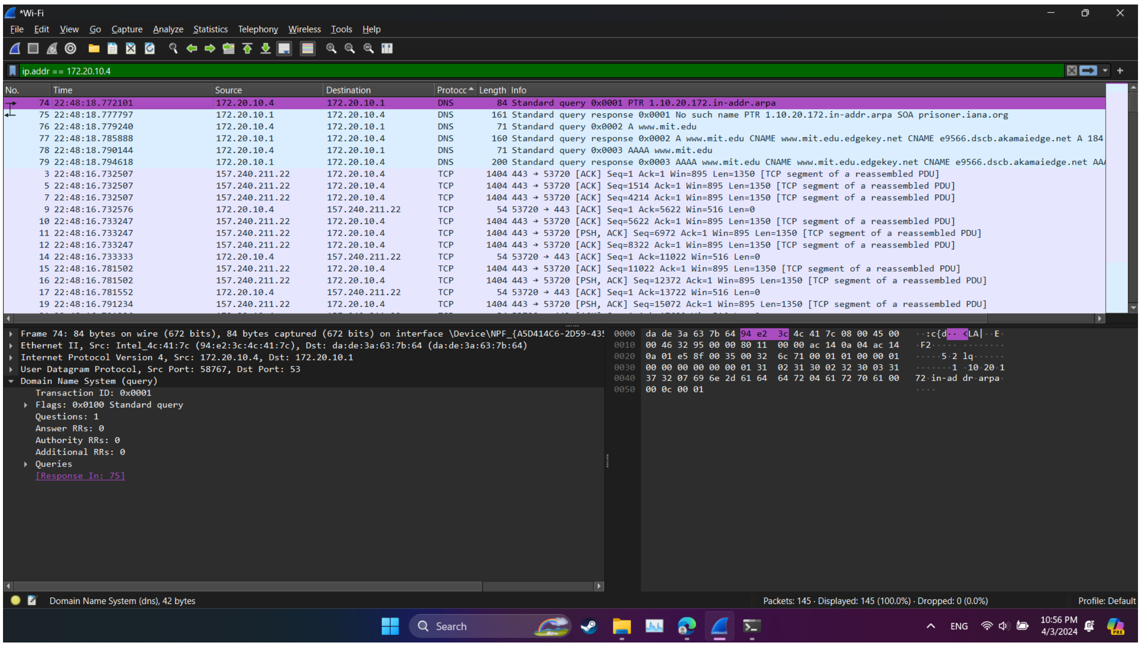


```
▸ Frame 77: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{A5D414C6-2D5
▸ Ethernet II, Src: da:de:3a:63:7b:64 (da:de:3a:63:7b:64), Dst: Intel_4c:41:7c (94:e2:3c:4c:41:7c)
▸ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.4
▸ User Datagram Protocol, Src Port: 53, Dst Port: 58768
▾ 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
  ▸ Queries
  ▾ 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 184.84.55.33
    [Request In: 76]
    [Time: 0.006648000 seconds]
```

2.12 Provide a screenshot.



```
C:\Users\84909>nslookup www.mit.edu
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2600:1417:8000:cae::255e
          2600:1417:8000:c8d::255e
          184.84.55.33
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 172.20.10.4

```
No.   Time              Source          Destination     Protocol Length Info
   74 22:48:18.772101   172.20.10.4     172.20.10.1     DNS        84 Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
   75 22:48:18.777797   172.20.10.1     172.20.10.4     DNS       161 Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA prisoner.iana.org
   76 22:48:18.779240   172.20.10.4     172.20.10.1     DNS        71 Standard query 0x0002 A www.mit.edu
   77 22:48:18.785888   172.20.10.1     172.20.10.4     DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184
   78 22:48:18.790144   172.20.10.4     172.20.10.1     DNS        71 Standard query 0x0003 AAAA www.mit.edu
   79 22:48:18.794618   172.20.10.1     172.20.10.4     DNS       200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AA
    3 22:48:16.732507   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=1 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
    5 22:48:16.732507   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=1514 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
    7 22:48:16.732507   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=4214 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
    9 22:48:16.732576   172.20.10.4     157.240.211.22  TCP        54 53720 → 443 [ACK] Seq=1 Ack=5622 Win=516 Len=0
   10 22:48:16.733247   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=5622 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   11 22:48:16.733247   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [PSH, ACK] Seq=6972 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   12 22:48:16.733247   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=8322 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   14 22:48:16.733333   172.20.10.4     157.240.211.22  TCP        54 53720 → 443 [ACK] Seq=1 Ack=11022 Win=516 Len=0
   15 22:48:16.781502   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [ACK] Seq=11022 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   16 22:48:16.781502   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [PSH, ACK] Seq=12372 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
   17 22:48:16.781552   172.20.10.4     157.240.211.22  TCP        54 53720 → 443 [ACK] Seq=1 Ack=13722 Win=516 Len=0
   19 22:48:16.791234   157.240.211.22  172.20.10.4     TCP      1404 443 → 53720 [PSH, ACK] Seq=15072 Ack=1 Win=895 Len=1350 [TCP segment of a reassembled PDU]
```

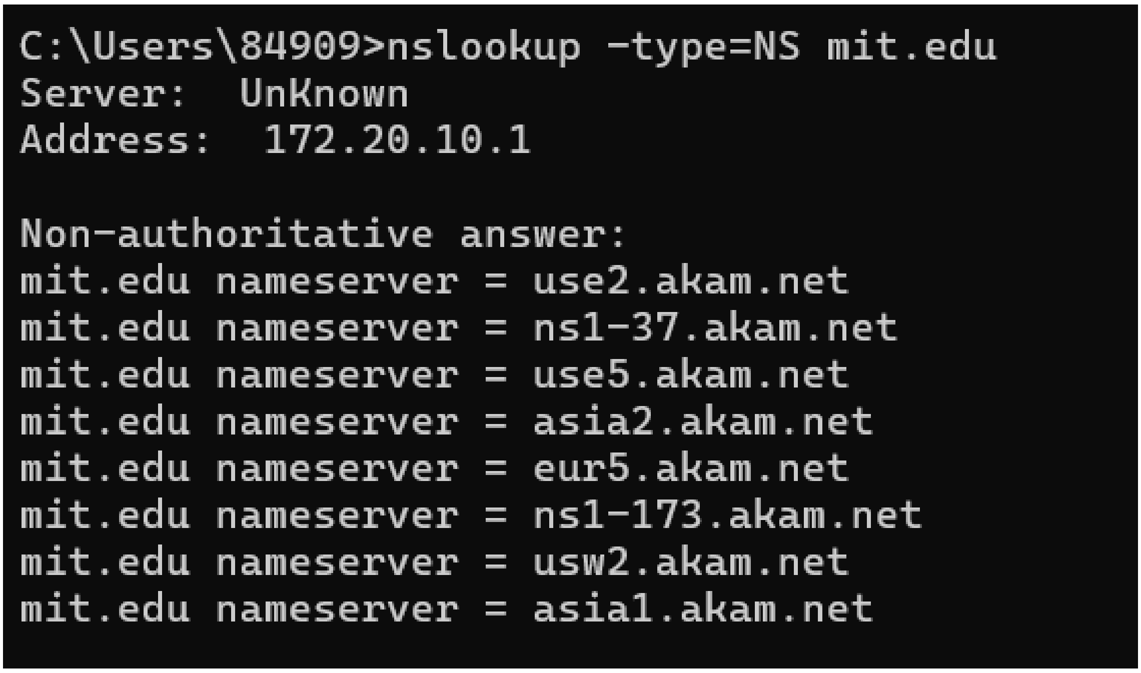
```
> Frame 74: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{A5D414C6-2D59-43!
> Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 58767, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 75]
```

```
0000  da de 3a 63 7b 64 94 e2  3c 4c 41 7c 08 00 45 00   ··:c{d·· <LA|··E·
0010  00 46 32 95 00 00 80 11  00 00 ac 14 0a 04 ac 14   ·F2····· ········
0020  0a 01 e5 8f 00 35 00 32  6c 71 00 01 01 00 00 01   ·····5·2 lq······
0030  00 00 00 00 00 00 01 31  02 31 30 02 32 30 03 31   ·······1 ·10·20·1
0040  37 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   72·in-ad dr·arpa·
0050  00 0c 00 01                                        ····
```

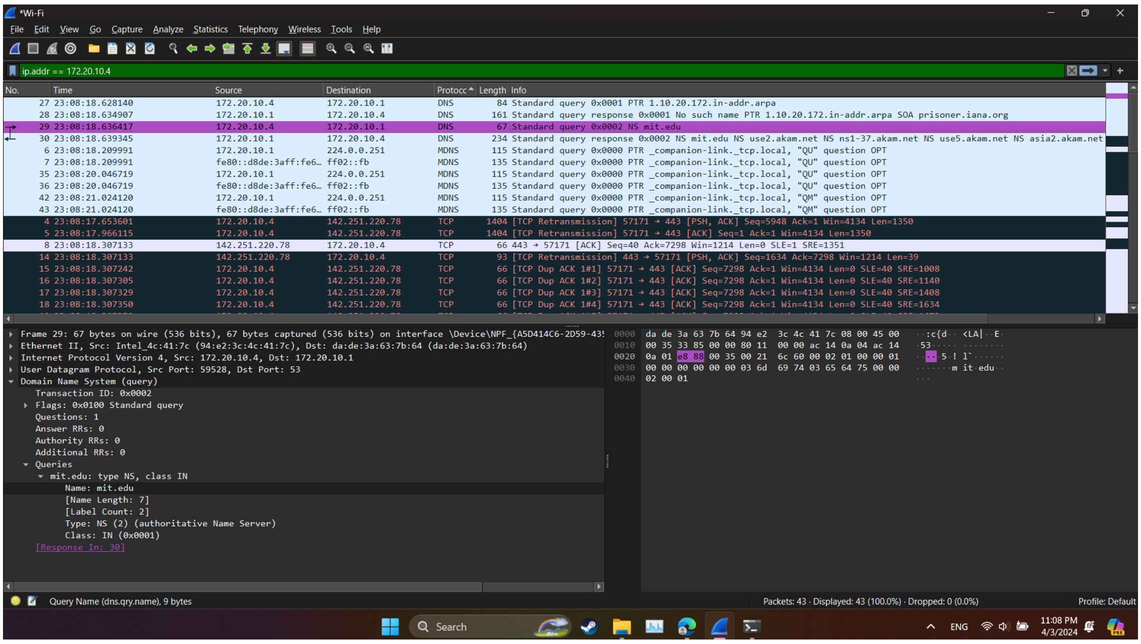
Domain Name System (dns), 42 bytes

Packets: 145 · Displayed: 145 (100.0%) · Dropped: 0 (0.0%)

Profile: Default



```
C:\Users\84909>nslookup -type=NS mit.edu
Server:  UnKnown
Address:  172.20.10.1

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



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.20.10.4

```
No.  Time             Source              Destination      Protocol Length Info
  27 23:08:18.628140  172.20.10.4         172.20.10.1      DNS        84 Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
  28 23:08:18.634907  172.20.10.1         172.20.10.4      DNS       161 Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA prisoner.iana.org
  29 23:08:18.636417  172.20.10.4         172.20.10.1      DNS        67 Standard query 0x0002 NS mit.edu
  30 23:08:18.639345  172.20.10.1         172.20.10.4      DNS       234 Standard query response 0x0002 NS mit.edu NS use2.akam.net NS ns1-37.akam.net NS use5.akam.net NS asia2.akam.net
   6 23:08:18.209991  172.20.10.1         224.0.0.251      MDNS      115 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question OPT
   7 23:08:18.209991  fe80::d8de:3aff:fe6… ff02::fb        MDNS      135 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question OPT
  35 23:08:20.046719  172.20.10.1         224.0.0.251      MDNS      115 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question OPT
  36 23:08:20.046719  fe80::d8de:3aff:fe6… ff02::fb        MDNS      135 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question OPT
  42 23:08:21.024120  172.20.10.1         224.0.0.251      MDNS      115 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question OPT
  43 23:08:21.024120  fe80::d8de:3aff:fe6… ff02::fb        MDNS      135 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question OPT
   4 23:08:17.653601  172.20.10.4         142.251.220.78   TCP      1404 [TCP Retransmission] 57171 → 443 [PSH, ACK] Seq=5948 Ack=1 Win=4134 Len=1350
   5 23:08:17.966115  172.20.10.4         142.251.220.78   TCP      1404 [TCP Retransmission] 57171 → 443 [ACK] Seq=1 Ack=1 Win=4134 Len=1350
   8 23:08:18.307133  142.251.220.78      172.20.10.4      TCP        66 443 → 57171 [ACK] Seq=40 Ack=7298 Win=1214 Len=0 SLE=1 SRE=1351
  14 23:08:18.307133  142.251.220.78      172.20.10.4      TCP        93 [TCP Retransmission] 443 → 57171 [PSH, ACK] Seq=1634 Ack=7298 Win=1214 Len=39
  15 23:08:18.307242  172.20.10.4         142.251.220.78   TCP        66 [TCP Dup ACK 1#1] 57171 → 443 [ACK] Seq=7298 Ack=1 Win=4134 Len=0 SLE=40 SRE=1008
  16 23:08:18.307305  172.20.10.4         142.251.220.78   TCP        66 [TCP Dup ACK 1#2] 57171 → 443 [ACK] Seq=7298 Ack=1 Win=4134 Len=0 SLE=40 SRE=1140
  17 23:08:18.307329  172.20.10.4         142.251.220.78   TCP        66 [TCP Dup ACK 1#3] 57171 → 443 [ACK] Seq=7298 Ack=1 Win=4134 Len=0 SLE=40 SRE=1408
  18 23:08:18.307350  172.20.10.4         142.251.220.78   TCP        66 [TCP Dup ACK 1#4] 57171 → 443 [ACK] Seq=7298 Ack=1 Win=4134 Len=0 SLE=40 SRE=1634
```

```
Frame 29: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{A5D414C6-2D59-43!
Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
User Datagram Protocol, Src Port: 59528, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0002
    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: 30]
```

```
0000  da de 3a 63 7b 64 94 e2  3c 4c 41 7c 08 00 45 00   ··:c{d··<LA|··E·
0010  00 35 33 85 00 00 80 11  00 00 ac 14 0a 04 ac 14   ·53·····  ········
0020  0a 01 e8 88 00 35 00 21  6c 60 00 02 01 00 00 01   ······5·!l`······
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01                                           ···
```

Query Name (dns.qry.name), 9 bytes

Packets: 43 · Displayed: 43 (100.0%) · Dropped: 0 (0.0%)

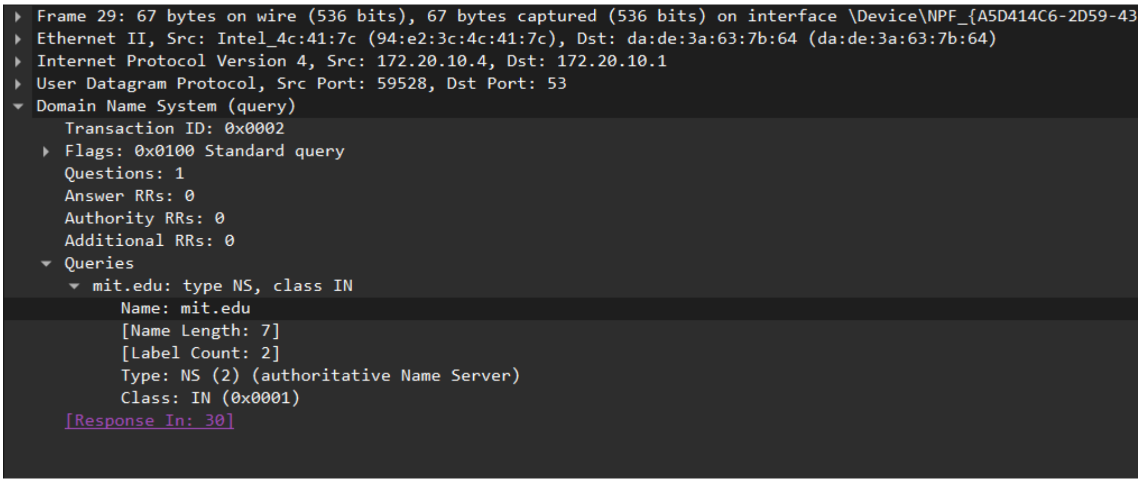
Profile: Default

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

It's sent to 172.20.10.1, which is the IP address of one of my local DNS servers.

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

- The DNS query is a type “NS” message and including one question.
- The query message did not contain any answers.



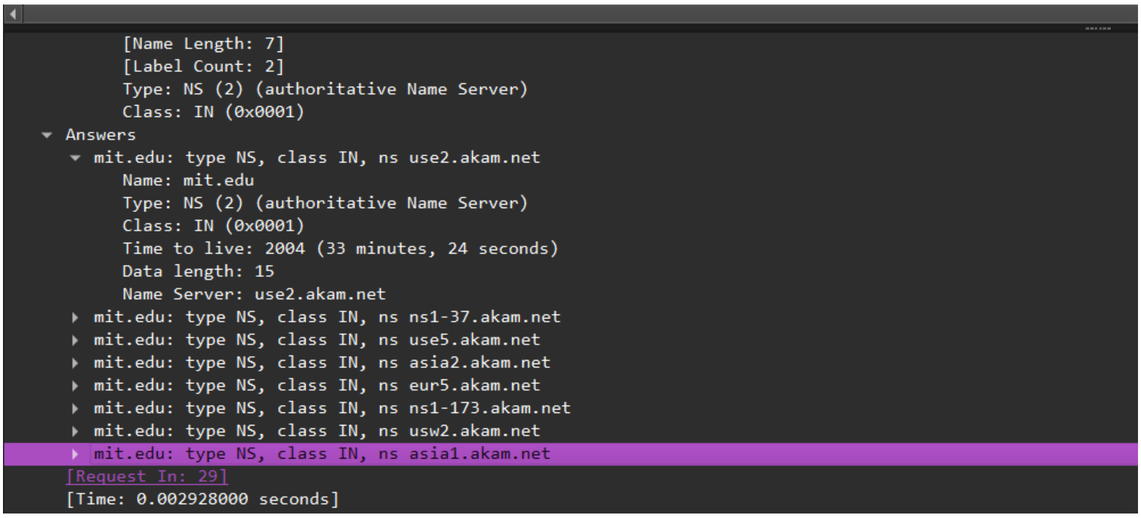
```
▸ Frame 29: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{A5D414C6-2D59-43
▸ Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
▸ Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
▸ User Datagram Protocol, Src Port: 59528, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x0002
  ▸ 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: 30]
```

2.15 Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

The **MIT nameservers** are:

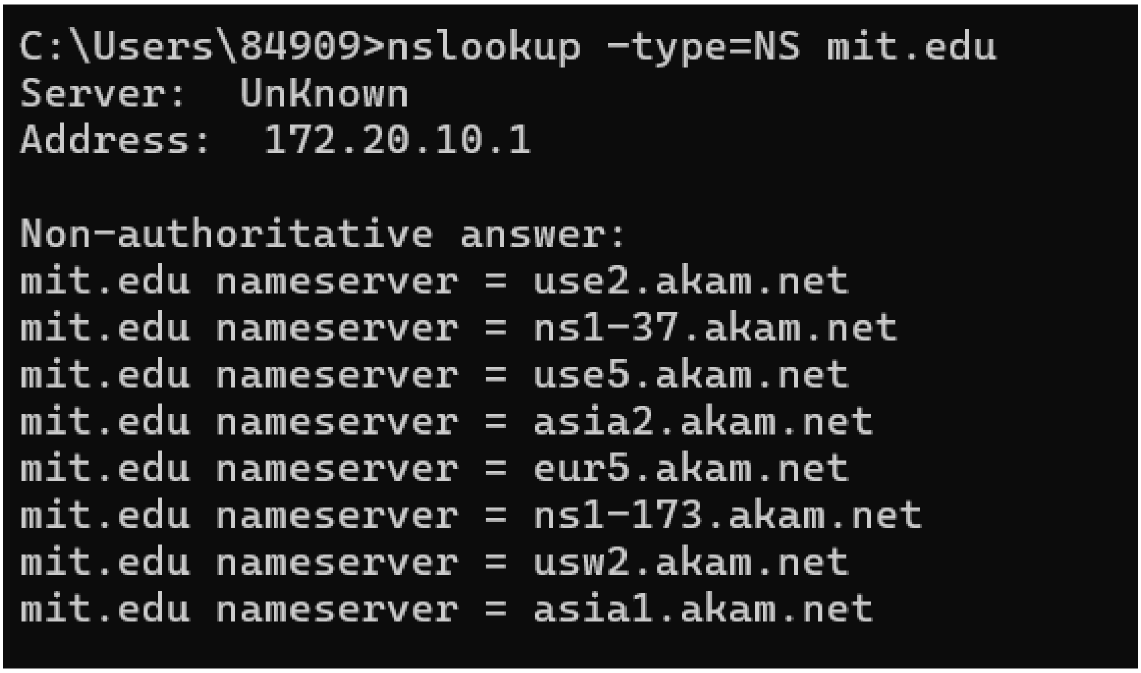
- use2.akam.net
- ns1-37.akam.net
- use5.akam.net
- asia2.akam.net
- eur5.akam.net
- ns1-173.akam.net
- usw2.akam.net
- asia1.akam.net

The answer just contained the server names but did not contain the IP of those MIT servers.

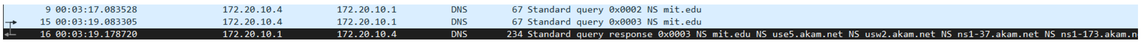


```
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
  Answers
    mit.edu: type NS, class IN, ns use2.akam.net
        Name: mit.edu
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
        Time to live: 2004 (33 minutes, 24 seconds)
        Data length: 15
        Name Server: use2.akam.net
    mit.edu: type NS, class IN, ns ns1-37.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 eur5.akam.net
    mit.edu: type NS, class IN, ns ns1-173.akam.net
    mit.edu: type NS, class IN, ns usw2.akam.net
    mit.edu: type NS, class IN, ns asia1.akam.net
  [Request In: 29]
  [Time: 0.002928000 seconds]
```

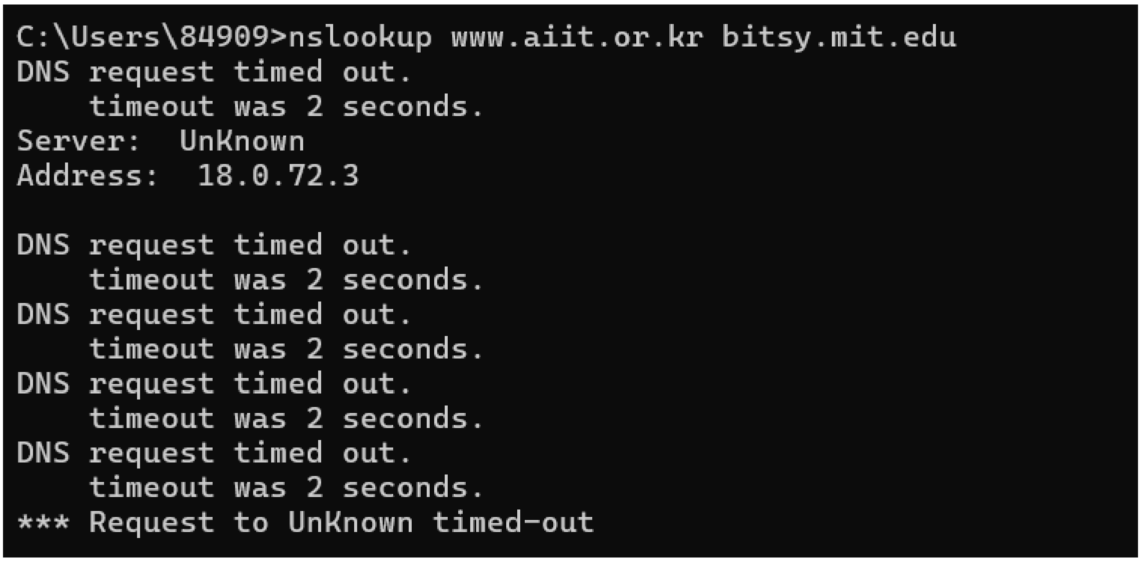
2.16 Provide a screenshot.



```
C:\Users\84909>nslookup -type=NS mit.edu
Server:  UnKnown
Address:  172.20.10.1

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



```
 9 00:03:17.083528    172.20.10.4    172.20.10.1    DNS     67 Standard query 0x0002 NS mit.edu
15 00:03:19.083305    172.20.10.4    172.20.10.1    DNS     67 Standard query 0x0003 NS mit.edu
16 00:03:19.178720    172.20.10.1    172.20.10.4    DNS    234 Standard query response 0x0003 NS mit.edu NS use5.akam.net NS usw2.akam.net NS ns1-37.akam.net NS ns1-173.akam.n
```

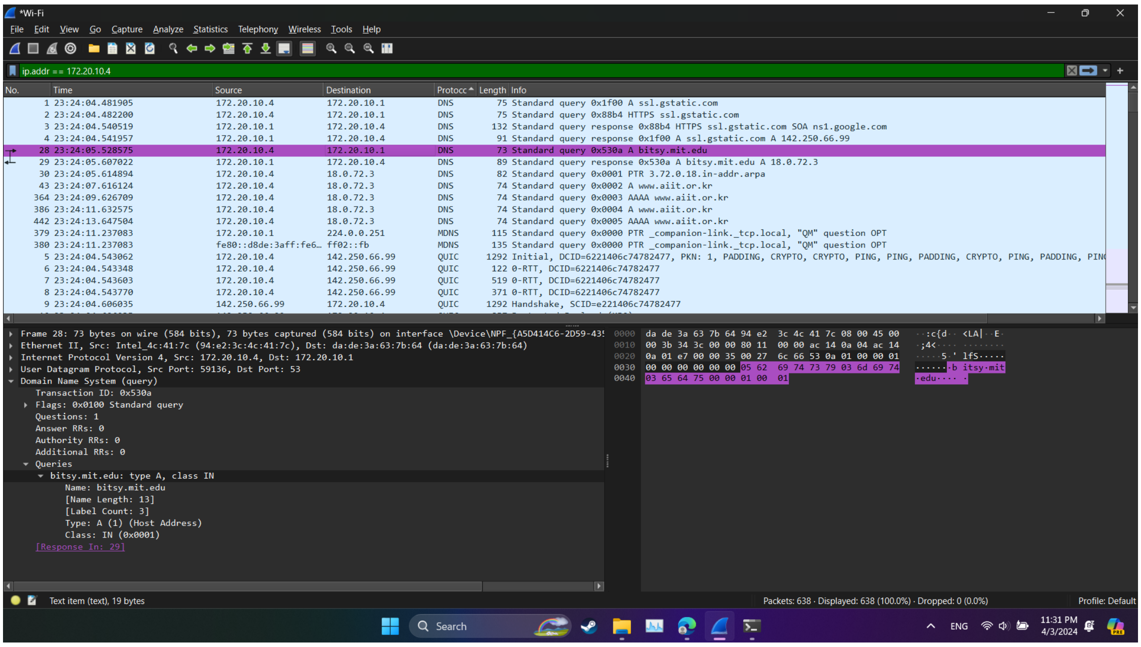


```
C:\Users\84909>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

]

2.17 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?

- At the beginning, it was sent to the IP 172.20.10.1 which is my default local DNS server.
- After finishing query the **bitsy.mit.edu**, the IP address of the DNS query was changed to the IP of the **bitsy.mit.edu** as *18.0.72.3*



ip.addr == 172.20.10.4

```
No.  Time             Source                Destination     Protocc Length Info
  1 23:24:04.481905  172.20.10.4           172.20.10.1     DNS       75 Standard query 0x1f00 A ssl.gstatic.com
  2 23:24:04.482200  172.20.10.4           172.20.10.1     DNS       75 Standard query 0x88b4 HTTPS ssl.gstatic.com
  3 23:24:04.540519  172.20.10.1           172.20.10.4     DNS      132 Standard query response 0x88b4 HTTPS ssl.gstatic.com SOA ns1.google.com
  4 23:24:04.541957  172.20.10.1           172.20.10.4     DNS       91 Standard query response 0x1f00 A ssl.gstatic.com A 142.250.66.99
 28 23:24:05.528575  172.20.10.4           172.20.10.1     DNS       73 Standard query 0x530a A bitsy.mit.edu
 29 23:24:05.607022  172.20.10.1           172.20.10.4     DNS       89 Standard query response 0x530a A bitsy.mit.edu A 18.0.72.3
 30 23:24:05.614894  172.20.10.4           18.0.72.3       DNS       82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
 43 23:24:07.616124  172.20.10.4           18.0.72.3       DNS       74 Standard query 0x0002 A www.aiit.or.kr
364 23:24:09.626709  172.20.10.4           18.0.72.3       DNS       74 Standard query 0x0003 AAAA www.aiit.or.kr
386 23:24:11.632575  172.20.10.4           18.0.72.3       DNS       74 Standard query 0x0004 A www.aiit.or.kr
442 23:24:13.647504  172.20.10.4           18.0.72.3       DNS       74 Standard query 0x0005 AAAA www.aiit.or.kr
379 23:24:11.237083  172.20.10.1           224.0.0.251     MDNS     115 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question OPT
380 23:24:11.237083  fe80::d8de:3aff:fe6… ff02::fb        MDNS     135 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question OPT
  5 23:24:04.543062  172.20.10.4           142.250.66.99   QUIC    1292 Initial, DCID=6221406c74782477, PKN: 1, PADDING, CRYPTO, CRYPTO, PING, PING, PADDING, CRYPTO, PING, PADDING, PIN
  6 23:24:04.543348  172.20.10.4           142.250.66.99   QUIC     122 0-RTT, DCID=6221406c74782477
  7 23:24:04.543603  172.20.10.4           142.250.66.99   QUIC     519 0-RTT, DCID=6221406c74782477
  8 23:24:04.543770  172.20.10.4           142.250.66.99   QUIC     371 0-RTT, DCID=6221406c74782477
  9 23:24:04.606035  142.250.66.99         172.20.10.4     QUIC    1292 Handshake, SCID=e221406c74782477
```

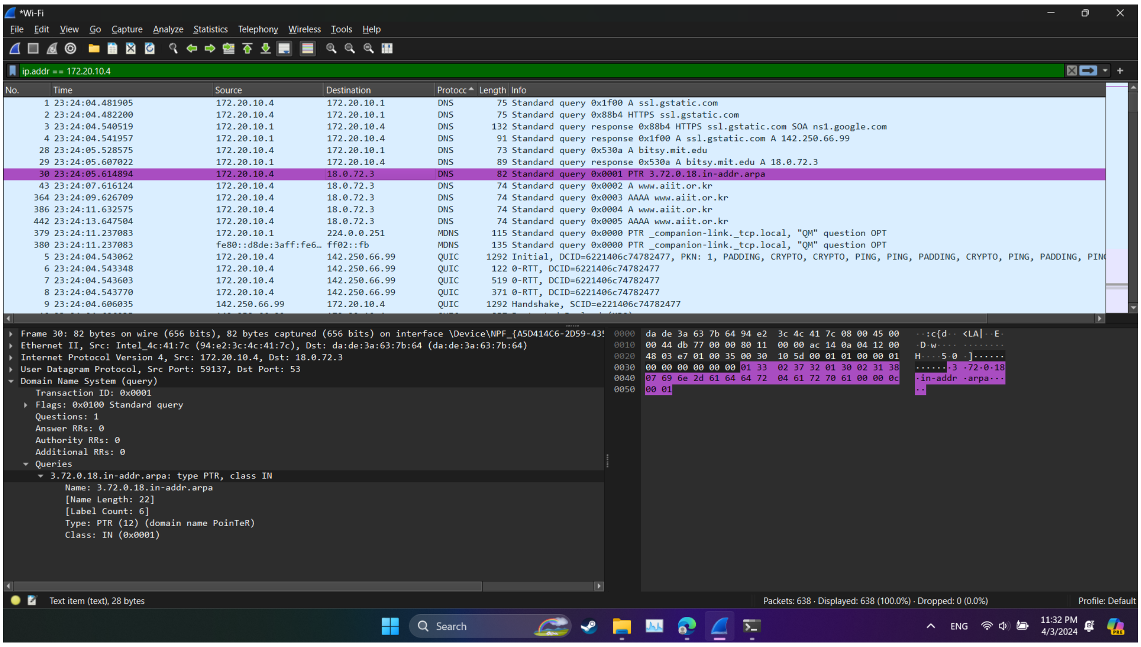
```
> Frame 28: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{A5D414C6-2D59-43!
> Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 59136, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x530a
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 29]
```

```
0000  da de 3a 63 7b 64 94 e2  3c 4c 41 7c 08 00 45 00   ··:c{d··<LA|··E·
0010  00 3b 34 3c 00 00 80 11  00 00 ac 14 0a 04 ac 14   ·;4<···· ········
0020  0a 01 e7 00 00 35 00 27  6c 66 53 0a 01 00 00 01   ·····5·' lfS·····
0030  00 00 00 00 00 00 05 62  69 74 73 79 03 6d 69 74   ·······b itsy·mit
0040  03 65 64 75 00 00 01 00  01                        ·edu···· ·
```

Text item (text), 19 bytes

Packets: 638 · Displayed: 638 (100.0%) · Dropped: 0 (0.0%)

Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Search
ENG
11:32 PM
4/3/2024

```
ip.addr == 172.20.10.4

No.  Time             Source                 Destination     Protocc Length Info
   1 23:24:04.481905  172.20.10.4            172.20.10.1     DNS       75 Standard query 0x1f00 A ssl.gstatic.com
   2 23:24:04.482200  172.20.10.4            172.20.10.1     DNS       75 Standard query 0x88b4 HTTPS ssl.gstatic.com
   3 23:24:04.540519  172.20.10.1            172.20.10.4     DNS      132 Standard query response 0x88b4 HTTPS ssl.gstatic.com SOA ns1.google.com
   4 23:24:04.541957  172.20.10.1            172.20.10.4     DNS       91 Standard query response 0x1f00 A ssl.gstatic.com A 142.250.66.99
  28 23:24:05.528575  172.20.10.4            172.20.10.1     DNS       73 Standard query 0x530a A bitsy.mit.edu
  29 23:24:05.607022  172.20.10.1            172.20.10.4     DNS       89 Standard query response 0x530a A bitsy.mit.edu A 18.0.72.3
  30 23:24:05.614894  172.20.10.4            18.0.72.3       DNS       82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  43 23:24:07.616124  172.20.10.4            18.0.72.3       DNS       74 Standard query 0x0002 A www.aiit.or.kr
 364 23:24:09.626709  172.20.10.4            18.0.72.3       DNS       74 Standard query 0x0003 AAAA www.aiit.or.kr
 386 23:24:11.632575  172.20.10.4            18.0.72.3       DNS       74 Standard query 0x0004 A www.aiit.or.kr
 442 23:24:13.647504  172.20.10.4            18.0.72.3       DNS       74 Standard query 0x0005 AAAA www.aiit.or.kr
 379 23:24:11.237083  172.20.10.1            224.0.0.251     MDNS     115 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question OPT
 380 23:24:11.237083  fe80::d8de:3aff:fe6…   ff02::fb        MDNS     135 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question OPT
   5 23:24:04.543062  172.20.10.4            142.250.66.99   QUIC    1292 Initial, DCID=6221406c74782477, PKN: 1, PADDING, CRYPTO, CRYPTO, PING, PING, PADDING, CRYPTO, PING, PADDING, PIN
   6 23:24:04.543348  172.20.10.4            142.250.66.99   QUIC     122 0-RTT, DCID=6221406c74782477
   7 23:24:04.543603  172.20.10.4            142.250.66.99   QUIC     519 0-RTT, DCID=6221406c74782477
   8 23:24:04.543770  172.20.10.4            142.250.66.99   QUIC     371 0-RTT, DCID=6221406c74782477
   9 23:24:04.606035  142.250.66.99          172.20.10.4     QUIC    1292 Handshake, SCID=e221406c74782477
```

```
› Frame 30: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{A5D414C6-2D59-43!
› Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
› Internet Protocol Version 4, Src: 172.20.10.4, Dst: 18.0.72.3
› User Datagram Protocol, Src Port: 59137, Dst Port: 53
⌄ Domain Name System (query)
    Transaction ID: 0x0001
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ 3.72.0.18.in-addr.arpa: type PTR, class IN
        Name: 3.72.0.18.in-addr.arpa
        [Name Length: 22]
        [Label Count: 6]
        Type: PTR (12) (domain name PointeR)
        Class: IN (0x0001)
```

```
0000  da de 3a 63 7b 64 94 e2  3c 4c 41 7c 08 00 45 00   ··:c{d·· <LA|··E·
0010  00 44 db 77 00 00 80 11  00 00 ac 14 0a 04 12 00   ·D·w···· ········
0020  48 03 e7 01 00 35 00 30  10 5d 00 01 01 00 00 01   H····5·0 ·]······
0030  00 00 00 00 00 00 01 33  02 37 32 01 30 02 31 38   ·······3 ·72·0·18
0040  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00 0c   ·in-addr ·arpa···
0050  00 01                                              ··
```

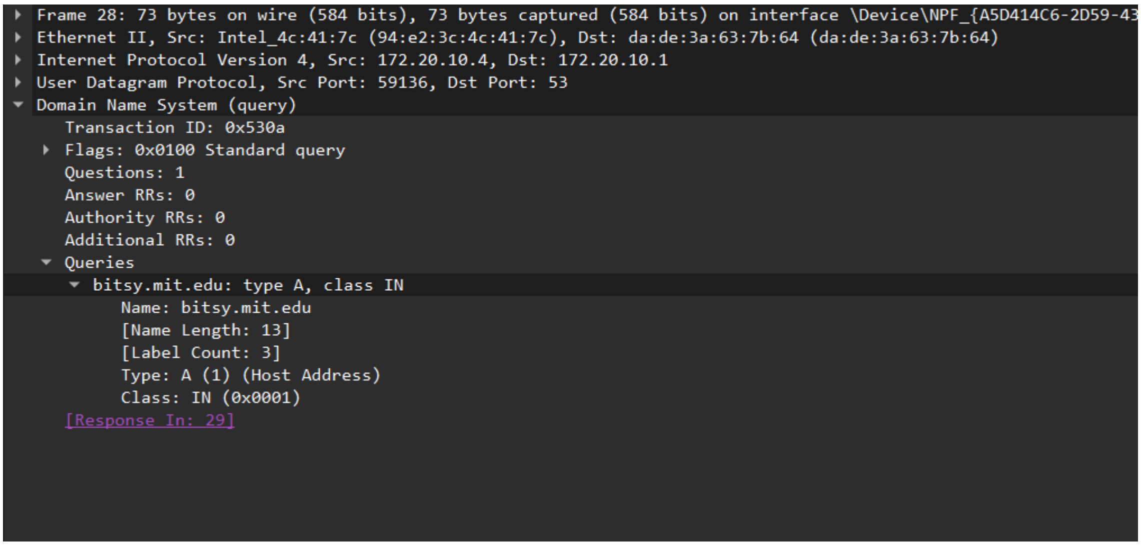
Text item (text), 28 bytes

Packets: 638 · Displayed: 638 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

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

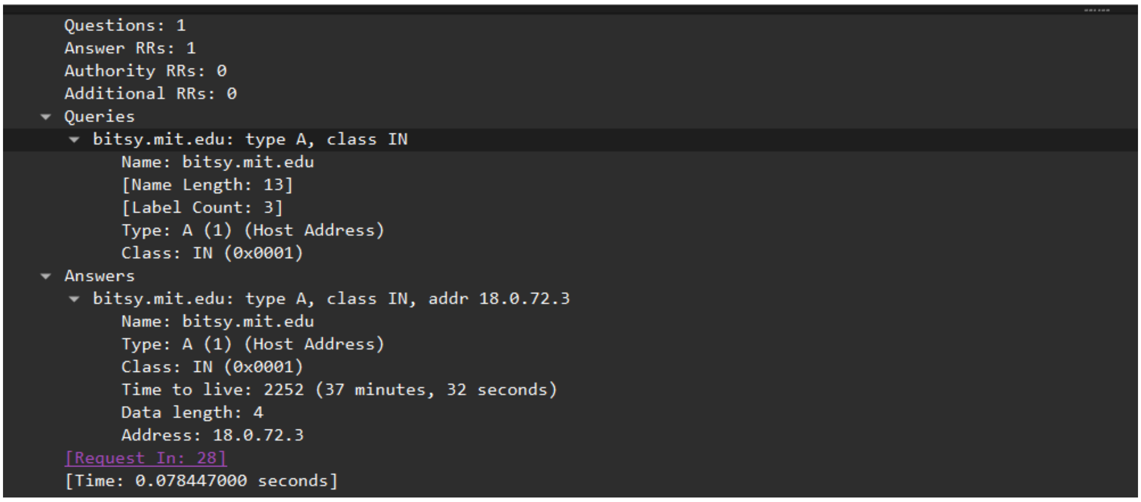
It is type A and contains no answer.



```
› Frame 28: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{A5D414C6-2D59-43
› Ethernet II, Src: Intel_4c:41:7c (94:e2:3c:4c:41:7c), Dst: da:de:3a:63:7b:64 (da:de:3a:63:7b:64)
› Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.1
› User Datagram Protocol, Src Port: 59136, Dst Port: 53
⌄ Domain Name System (query)
    Transaction ID: 0x530a
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 29]
```

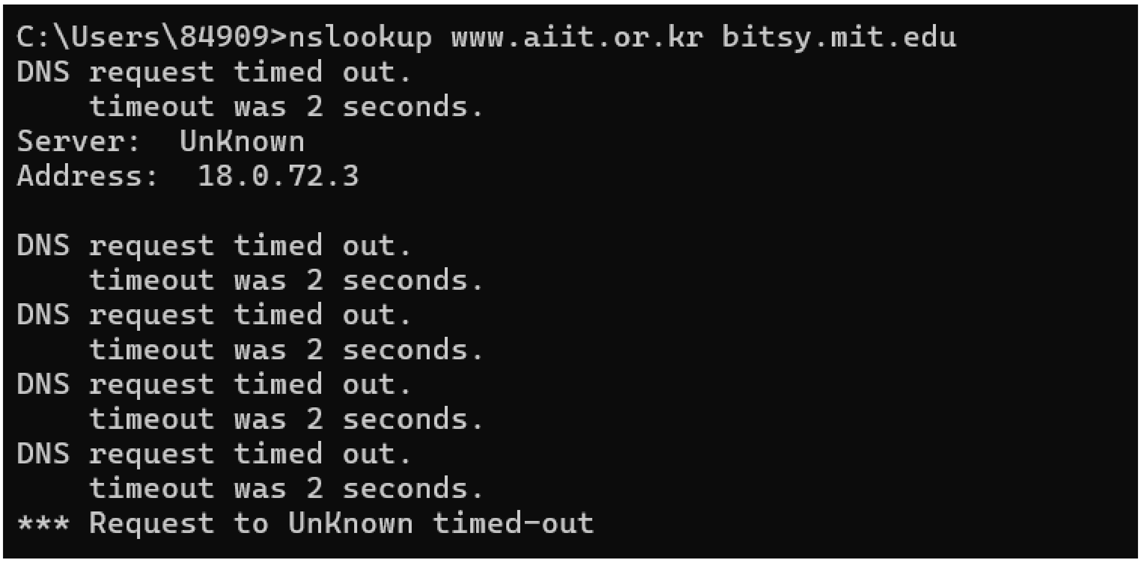
2.19 Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

One answer is provided in the DNS response message

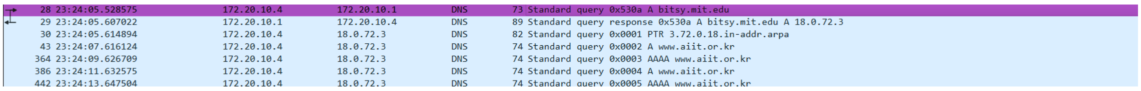


```
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Answers
    ▾ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
        Name: bitsy.mit.edu
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 2252 (37 minutes, 32 seconds)
        Data length: 4
        Address: 18.0.72.3
    [Request In: 28]
    [Time: 0.078447000 seconds]
```

2.20 Provide a screenshot.



```
C:\Users\84909>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```



```
 28 23:24:05.528575   172.20.10.4   172.20.10.1   DNS   73 Standard query 0x530a A bitsy.mit.edu
 29 23:24:05.607022   172.20.10.1   172.20.10.4   DNS   89 Standard query response 0x530a A bitsy.mit.edu A 18.0.72.3
 30 23:24:05.614894   172.20.10.4   18.0.72.3     DNS   82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
 43 23:24:07.616124   172.20.10.4   18.0.72.3     DNS   74 Standard query 0x0002 A www.aiit.or.kr
364 23:24:09.626709   172.20.10.4   18.0.72.3     DNS   74 Standard query 0x0003 AAAA www.aiit.or.kr
386 23:24:11.632575   172.20.10.4   18.0.72.3     DNS   74 Standard query 0x0004 A www.aiit.or.kr
442 23:24:13.647504   172.20.10.4   18.0.72.3     DNS   74 Standard query 0x0005 AAAA www.aiit.or.kr
```