Wireshark Lab 2 —— DNS

Kangyan XU

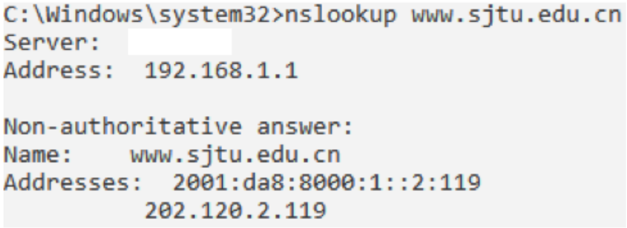
Brief Abstract

This report runs *nslookup* and analyzes the detail of DNS querying and responding.

Questions

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

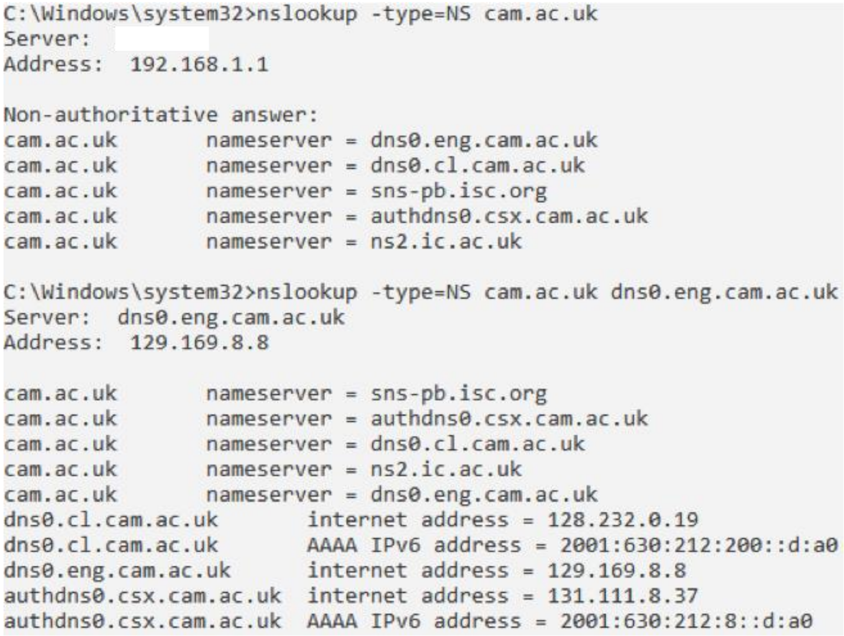
A: The IP address of Shanghai Jiao Tong University obtained is 202.120.2.119



```
C:\Windows\system32>nslookup www.sjtu.edu.cn
Server:  [redacted]
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.sjtu.edu.cn
Addresses:  2001:da8:8000:1::2:119
          202.120.2.119
```

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

A: Get 5 authoritative DNS servers for the University of Cambridge. Besides, when using the server "dns0.eng.cam.ac.uk" to send the query, authoritative records and some IP addresses of the authoritative DNS servers are returned.



```
C:\Windows\system32>nslookup -type=NS cam.ac.uk
Server:  [redacted]
Address:  192.168.1.1

Non-authoritative answer:
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk
cam.ac.uk       nameserver = sns-pb.isc.org
cam.ac.uk       nameserver = authdns0.csx.cam.ac.uk
cam.ac.uk       nameserver = ns2.ic.ac.uk

C:\Windows\system32>nslookup -type=NS cam.ac.uk dns0.eng.cam.ac.uk
Server:  dns0.eng.cam.ac.uk
Address:  129.169.8.8

cam.ac.uk       nameserver = sns-pb.isc.org
cam.ac.uk       nameserver = authdns0.csx.cam.ac.uk
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk
cam.ac.uk       nameserver = ns2.ic.ac.uk
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk
dns0.cl.cam.ac.uk       internet address = 128.232.0.19
dns0.cl.cam.ac.uk       AAAA IPv6 address = 2001:630:212:200::d:a0
dns0.eng.cam.ac.uk      internet address = 129.169.8.8
authdns0.csx.cam.ac.uk  internet address = 131.111.8.37
authdns0.csx.cam.ac.uk  AAAA IPv6 address = 2001:630:212:8::d:a0
```

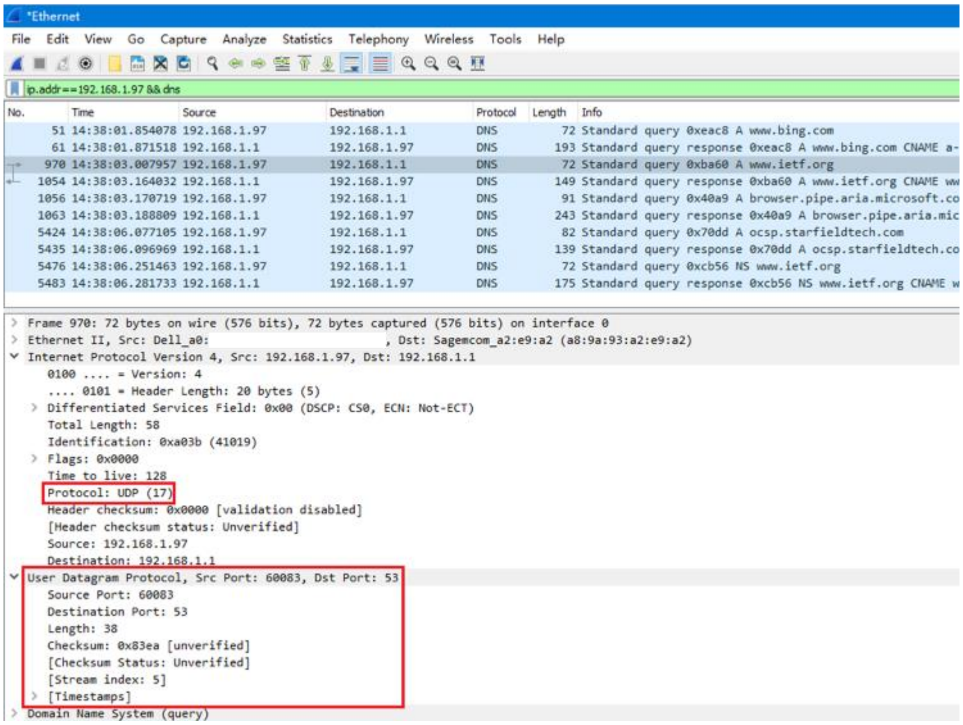
3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

A: When using DNS servers obtained above to query, it is refused, so Google Public DNS Server 8.8.8.8 is used, and two IP addresses are received (69.147.88.7 and 69.147.88.8) given Yahoo has multiple servers distributed geographically.

```
C:\Windows\system32>nslookup mail.yahoo.com dns0.cl.cam.ac.uk
Server:  dns0.cl.cam.ac.uk
Address:  128.232.0.19

*** dns0.cl.cam.ac.uk can't find mail.yahoo.com: Query refused

C:\Windows\system32>nslookup mail.yahoo.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    fd-geoycpi-uno.gycpi.b.yahoodns.net
Addresses:  2001:4998:18:800::4002
          2001:4998:18:800::4003
          69.147.88.7
          69.147.88.8
Aliases:  mail.yahoo.com
```

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

A: They are sent over UDP.



ip.addr==192.168.1.97 && dns

```
No.   Time            Source        Destination   Protocol Length Info
   51 14:38:01.854078 192.168.1.97  192.168.1.1   DNS        72 Standard query 0xeac8 A www.bing.com
   61 14:38:01.871518 192.168.1.1   192.168.1.97  DNS       193 Standard query response 0xeac8 A www.bing.com CNAME a-
  970 14:38:03.007957 192.168.1.97  192.168.1.1   DNS        72 Standard query 0xba60 A www.ietf.org
 1054 14:38:03.164032 192.168.1.1   192.168.1.97  DNS       149 Standard query response 0xba60 A www.ietf.org CNAME ww
 1056 14:38:03.170719 192.168.1.97  192.168.1.1   DNS        91 Standard query 0x40a9 A browser.pipe.aria.microsoft.co
 1063 14:38:03.188809 192.168.1.1   192.168.1.97  DNS       243 Standard query response 0x40a9 A browser.pipe.aria.mic
 5424 14:38:06.077105 192.168.1.97  192.168.1.1   DNS        82 Standard query 0x70dd A ocsp.starfieldtech.com
 5435 14:38:06.096969 192.168.1.1   192.168.1.97  DNS       139 Standard query response 0x70dd A ocsp.starfieldtech.co
 5476 14:38:06.251463 192.168.1.97  192.168.1.1   DNS        72 Standard query 0xcb56 NS www.ietf.org
 5483 14:38:06.281733 192.168.1.1   192.168.1.97  DNS       175 Standard query response 0xcb56 NS www.ietf.org CNAME w
```

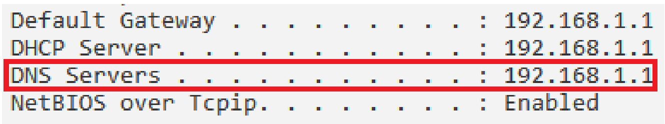
```
> Frame 970: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: Dell_a0:[redacted], Dst: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2)
v Internet Protocol Version 4, Src: 192.168.1.97, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0xa03b (41019)
  > Flags: 0x0000
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.97
    Destination: 192.168.1.1
v User Datagram Protocol, Src Port: 60083, Dst Port: 53
    Source Port: 60083
    Destination Port: 53
    Length: 38
    Checksum: 0x83ea [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  > [Timestamps]
> Domain Name System (query)
```

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

A: All of these ports are 53.

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

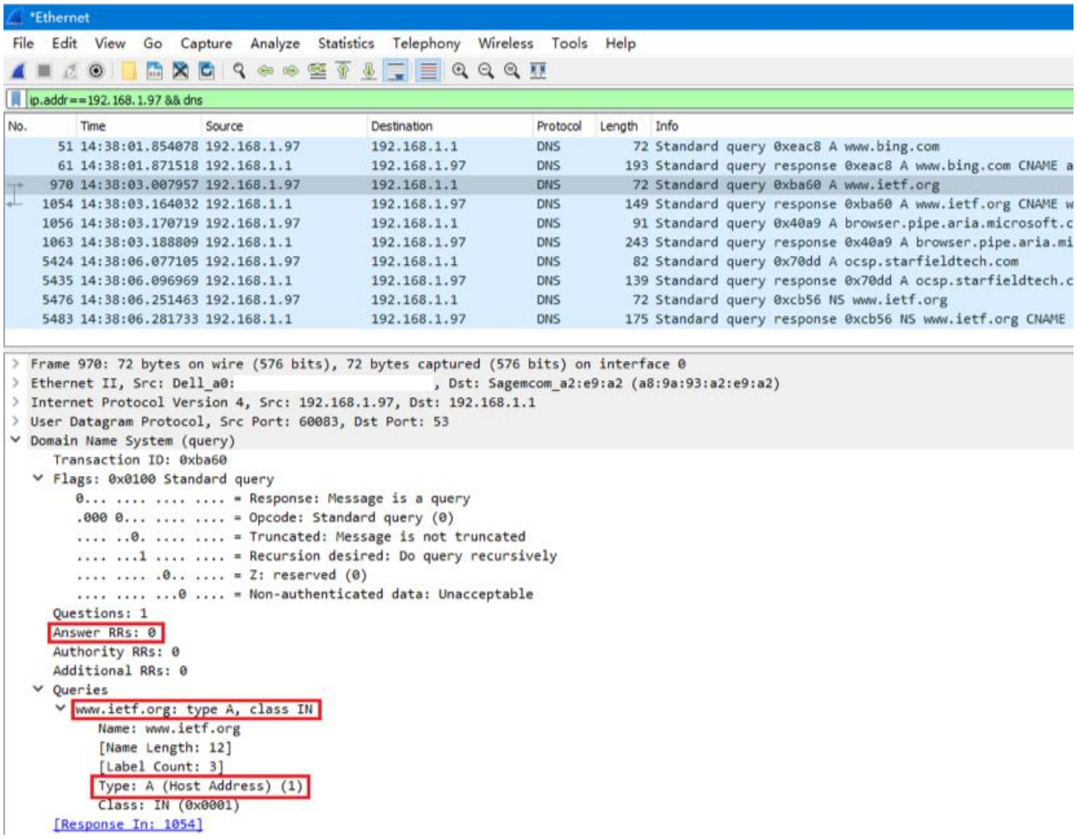
A: It is sent to 192.168.1.1 These two IP addresses are same.



```
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

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

A: The type is “A”. The query message contains no “answers”.



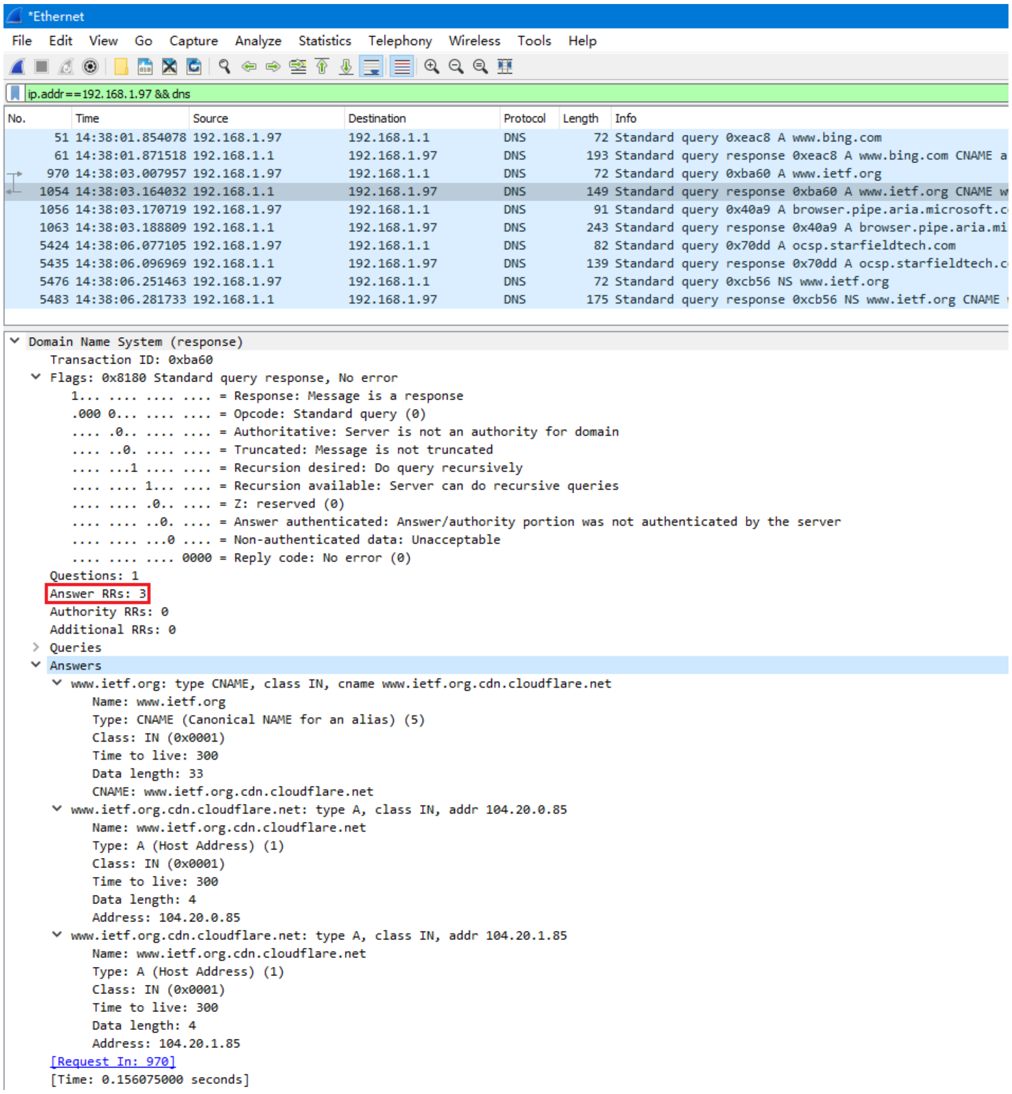
```
ip.addr==192.168.1.97 && dns
```

```
No.   Time            Source        Destination   Protocol Length Info
   51 14:38:01.854078 192.168.1.97  192.168.1.1   DNS       72 Standard query 0xeac8 A www.bing.com
   61 14:38:01.871518 192.168.1.1   192.168.1.97  DNS      193 Standard query response 0xeac8 A www.bing.com CNAME a
  970 14:38:03.007957 192.168.1.97  192.168.1.1   DNS       72 Standard query 0xba60 A www.ietf.org
 1054 14:38:03.164032 192.168.1.1   192.168.1.97  DNS      149 Standard query response 0xba60 A www.ietf.org CNAME w
 1056 14:38:03.170719 192.168.1.97  192.168.1.1   DNS       91 Standard query 0x40a9 A browser.pipe.aria.microsoft.c
 1063 14:38:03.188809 192.168.1.1   192.168.1.97  DNS      243 Standard query response 0x40a9 A browser.pipe.aria.mi
 5424 14:38:06.077105 192.168.1.97  192.168.1.1   DNS       82 Standard query 0x70dd A ocsp.starfieldtech.com
 5435 14:38:06.096969 192.168.1.1   192.168.1.97  DNS      139 Standard query response 0x70dd A ocsp.starfieldtech.c
 5476 14:38:06.251463 192.168.1.97  192.168.1.1   DNS       72 Standard query 0xcb56 NS www.ietf.org
 5483 14:38:06.281733 192.168.1.1   192.168.1.97  DNS      175 Standard query response 0xcb56 NS www.ietf.org CNAME
```

```
> Frame 970: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: Dell_a0: [redacted] , Dst: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2)
> Internet Protocol Version 4, Src: 192.168.1.97, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 60083, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xba60
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 1054]
```

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

A: 3 answers are provided. The first contains cname www.ietf.org.cdn.cloudflare.net, the latter two contains its IP address (104.20.0.85 and 104.20.1.85).


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

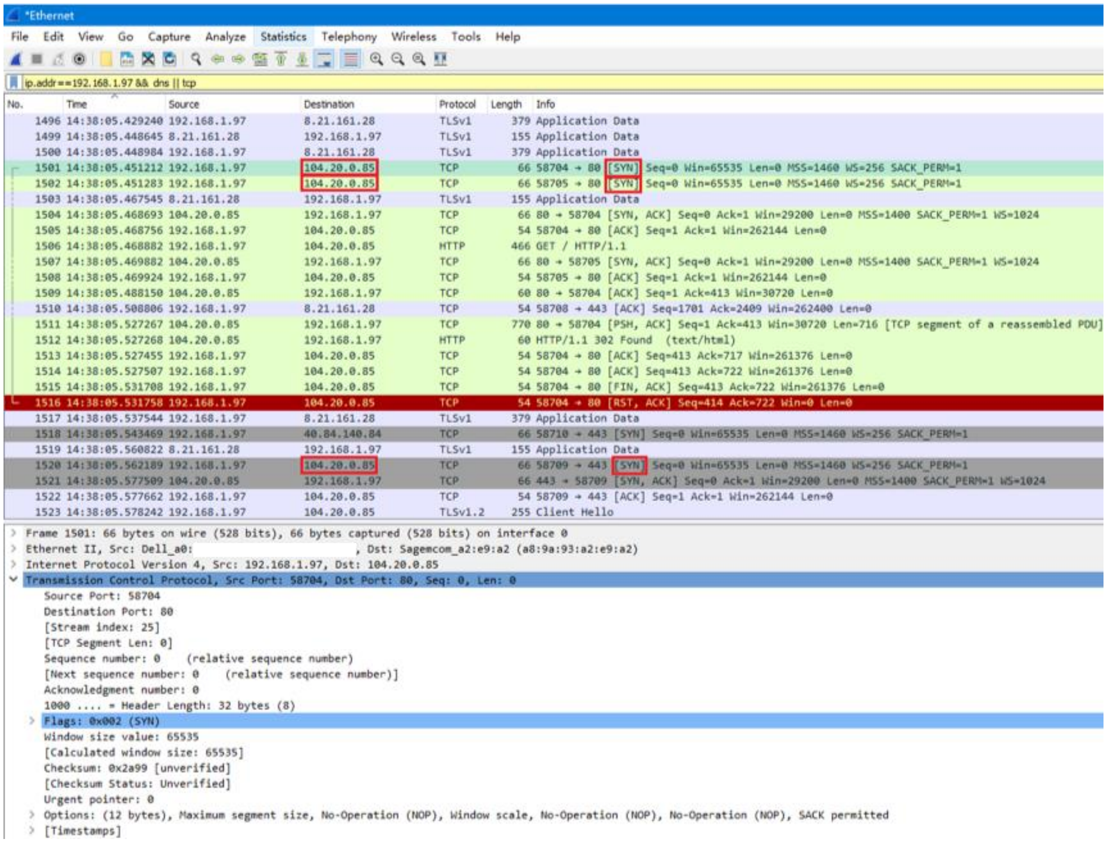
ip.addr==192.168.1.97 && dns

```
No.    Time            Source        Destination   Protocol Length Info
    51 14:38:01.854078 192.168.1.97  192.168.1.1   DNS       72 Standard query 0xeac8 A www.bing.com
    61 14:38:01.871518 192.168.1.1   192.168.1.97  DNS      193 Standard query response 0xeac8 A www.bing.com CNAME a
   970 14:38:03.007957 192.168.1.97  192.168.1.1   DNS       72 Standard query 0xba60 A www.ietf.org
  1054 14:38:03.164032 192.168.1.1   192.168.1.97  DNS      149 Standard query response 0xba60 A www.ietf.org CNAME w
  1056 14:38:03.170719 192.168.1.97  192.168.1.1   DNS       91 Standard query 0x40a9 A browser.pipe.aria.microsoft.c
  1063 14:38:03.188809 192.168.1.1   192.168.1.97  DNS      243 Standard query response 0x40a9 A browser.pipe.aria.mi
  5424 14:38:06.077105 192.168.1.97  192.168.1.1   DNS       82 Standard query 0x70dd A ocsp.starfieldtech.com
  5435 14:38:06.096969 192.168.1.1   192.168.1.97  DNS      139 Standard query response 0x70dd A ocsp.starfieldtech.c
  5476 14:38:06.251463 192.168.1.97  192.168.1.1   DNS       72 Standard query 0xcb56 NS www.ietf.org
  5483 14:38:06.281733 192.168.1.1   192.168.1.97  DNS      175 Standard query response 0xcb56 NS www.ietf.org CNAME
```

```
Domain Name System (response)
    Transaction ID: 0xba60
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  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: 300
        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: 300
        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: 300
        Data length: 4
        Address: 104.20.1.85
    [Request In: 970]
    [Time: 0.156075000 seconds]
```

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

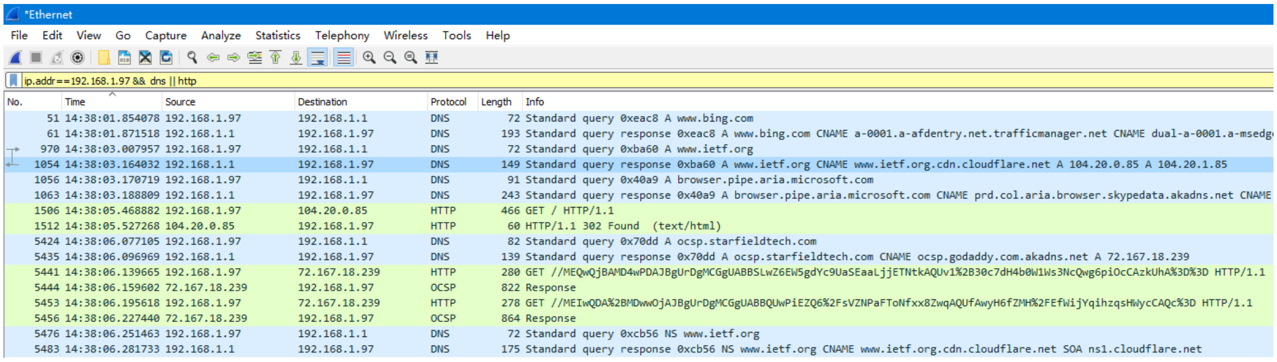
A: Several correspond to the IP address 104.20.0.85


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==192.168.1.97 && dns || tcp

No.  Time            Source        Destination   Protocol Length Info
1496 14:38:05.429240 192.168.1.97  8.21.161.28   TLSv1    379 Application Data
1499 14:38:05.448645 8.21.161.28   192.168.1.97  TLSv1    155 Application Data
1500 14:38:05.448984 192.168.1.97  8.21.161.28   TLSv1    379 Application Data
1501 14:38:05.451212 192.168.1.97  104.20.0.85   TCP       66 58704 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1502 14:38:05.451283 192.168.1.97  104.20.0.85   TCP       66 58705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1503 14:38:05.467545 8.21.161.28   192.168.1.97  TLSv1    155 Application Data
1504 14:38:05.468693 104.20.0.85   192.168.1.97  TCP       66 80 → 58704 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=1024
1505 14:38:05.468756 192.168.1.97  104.20.0.85   TCP       54 58704 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1506 14:38:05.468882 192.168.1.97  104.20.0.85   HTTP     466 GET / HTTP/1.1
1507 14:38:05.469882 104.20.0.85   192.168.1.97  TCP       66 80 → 58705 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=1024
1508 14:38:05.469924 192.168.1.97  104.20.0.85   TCP       54 58705 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1509 14:38:05.488150 104.20.0.85   192.168.1.97  TCP       60 80 → 58704 [ACK] Seq=1 Ack=413 Win=30720 Len=0
1510 14:38:05.508806 192.168.1.97  8.21.161.28   TCP       54 58708 → 443 [ACK] Seq=1701 Ack=2409 Win=262400 Len=0
1511 14:38:05.527267 104.20.0.85   192.168.1.97  TCP      770 80 → 58704 [PSH, ACK] Seq=1 Ack=413 Win=30720 Len=716 [TCP segment of a reassembled PDU]
1512 14:38:05.527268 104.20.0.85   192.168.1.97  HTTP      60 HTTP/1.1 302 Found  (text/html)
1513 14:38:05.527455 192.168.1.97  104.20.0.85   TCP       54 58704 → 80 [ACK] Seq=413 Ack=717 Win=261376 Len=0
1514 14:38:05.527507 192.168.1.97  104.20.0.85   TCP       54 58704 → 80 [ACK] Seq=413 Ack=722 Win=261376 Len=0
1515 14:38:05.531708 192.168.1.97  104.20.0.85   TCP       54 58704 → 80 [FIN, ACK] Seq=413 Ack=722 Win=261376 Len=0
1516 14:38:05.531758 192.168.1.97  104.20.0.85   TCP       54 58704 → 80 [RST, ACK] Seq=414 Ack=722 Win=0 Len=0
1517 14:38:05.537544 192.168.1.97  8.21.161.28   TLSv1    379 Application Data
1518 14:38:05.543469 192.168.1.97  40.84.140.84  TCP       66 58710 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1519 14:38:05.560822 8.21.161.28   192.168.1.97  TLSv1    155 Application Data
1520 14:38:05.562189 192.168.1.97  104.20.0.85   TCP       66 58709 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1521 14:38:05.577509 104.20.0.85   192.168.1.97  TCP       66 443 → 58709 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=1024
1522 14:38:05.577662 192.168.1.97  104.20.0.85   TCP       54 58709 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1523 14:38:05.578242 192.168.1.97  104.20.0.85   TLSv1.2  255 Client Hello

> Frame 1501: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Dell_a0:                    , Dst: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2)
> Internet Protocol Version 4, Src: 192.168.1.97, Dst: 104.20.0.85
v Transmission Control Protocol, Src Port: 58704, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 58704
    Destination Port: 80
    [Stream index: 25]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0x2a99 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

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

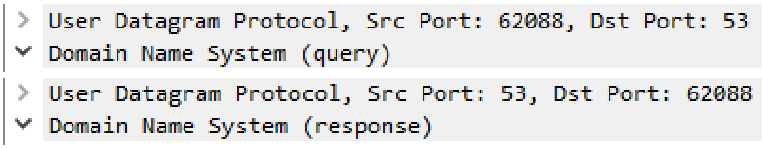
A: No. There is a similar process (retriving) relating to IP address 72.167.18.239


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==192.168.1.97 && dns || http

No.  Time            Source         Destination    Protocol Length Info
  51 14:38:01.854078 192.168.1.97   192.168.1.1    DNS       72 Standard query 0xeac8 A www.bing.com
  61 14:38:01.871518 192.168.1.1    192.168.1.97   DNS      193 Standard query response 0xeac8 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME dual-a-0001.a-msedg
 970 14:38:03.007957 192.168.1.97   192.168.1.1    DNS       72 Standard query 0xba60 A www.ietf.org
1054 14:38:03.164032 192.168.1.1    192.168.1.97   DNS      149 Standard query response 0xba60 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85
1056 14:38:03.170719 192.168.1.97   192.168.1.1    DNS       91 Standard query 0x40a9 A browser.pipe.aria.microsoft.com
1063 14:38:03.188809 192.168.1.1    192.168.1.97   DNS      243 Standard query response 0x40a9 A browser.pipe.aria.microsoft.com CNAME prd.col.aria.browser.skypedata.akadns.net CNAME
1506 14:38:05.468882 192.168.1.97   104.20.0.85    HTTP     466 GET / HTTP/1.1
1512 14:38:05.527268 104.20.0.85    192.168.1.97   HTTP      60 HTTP/1.1 302 Found  (text/html)
5424 14:38:06.077105 192.168.1.97   192.168.1.1    DNS       82 Standard query 0x70dd A ocsp.starfieldtech.com
5435 14:38:06.096969 192.168.1.1    192.168.1.97   DNS      139 Standard query response 0x70dd A ocsp.starfieldtech.com CNAME ocsp.godaddy.com.akadns.net A 72.167.18.239
5441 14:38:06.139665 192.168.1.97   72.167.18.239  HTTP     280 GET //MEQwQjBAMD4wPDAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCAzkUhA%3D%3D HTTP/1.1
5444 14:38:06.159602 72.167.18.239  192.168.1.97   OCSP     822 Response
5453 14:38:06.195618 192.168.1.97   72.167.18.239  HTTP     278 GET //MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBQUwPiEZQ6%2FsVZNPaFToNfxx8ZwqAQUfAwyH6fZMH%2FEfWijYqihzqsHWycCAQc%3D HTTP/1.1
5456 14:38:06.227440 72.167.18.239  192.168.1.97   OCSP     864 Response
5476 14:38:06.251463 192.168.1.97   192.168.1.1    DNS       72 Standard query 0xcb56 NS www.ietf.org
5483 14:38:06.281733 192.168.1.1    192.168.1.97   DNS      175 Standard query response 0xcb56 NS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net SOA ns1.cloudflare.net
```

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

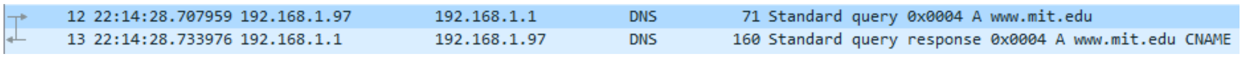
A: They are both 53.



```
> User Datagram Protocol, Src Port: 62088, Dst Port: 53
v Domain Name System (query)
> User Datagram Protocol, Src Port: 53, Dst Port: 62088
v Domain Name System (response)
```

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

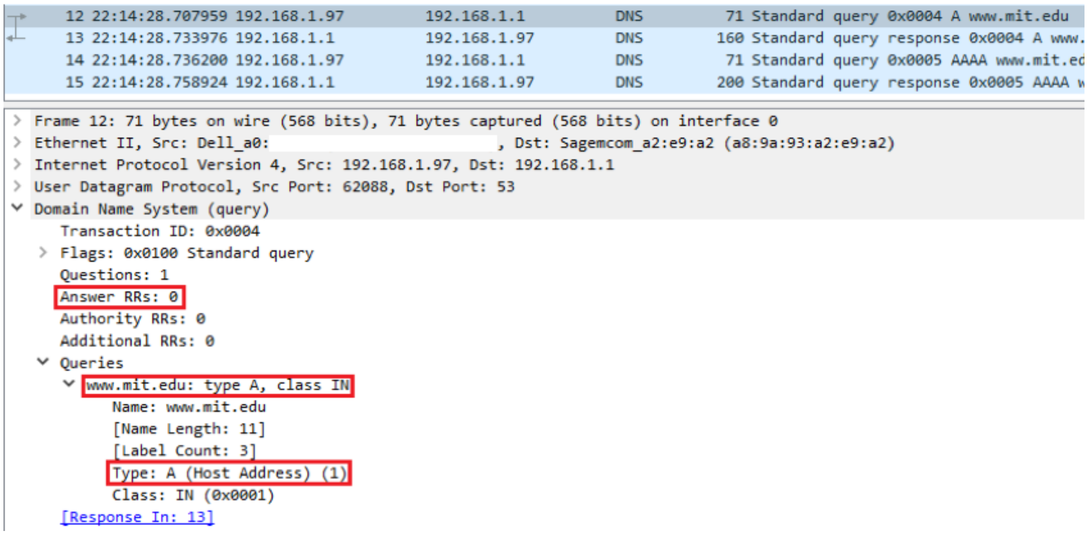
A: To 192.168.1.1 This is the IP address of my default local DNS server.



```
12 22:14:28.707959 192.168.1.97      192.168.1.1        DNS       71 Standard query 0x0004 A www.mit.edu
13 22:14:28.733976 192.168.1.1       192.168.1.97       DNS      160 Standard query response 0x0004 A www.mit.edu CNAME
```

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

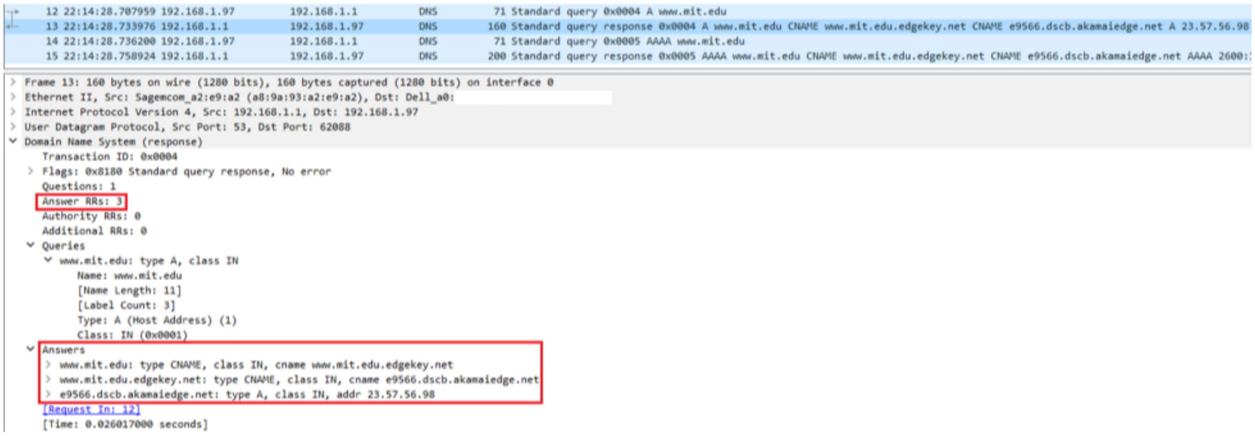
A: It is type “A”. It contains no answers.



```
12 22:14:28.707959 192.168.1.97      192.168.1.1       DNS       71 Standard query 0x0004 A www.mit.edu
13 22:14:28.733976 192.168.1.1       192.168.1.97      DNS      160 Standard query response 0x0004 A www.
14 22:14:28.736200 192.168.1.97      192.168.1.1       DNS       71 Standard query 0x0005 AAAA www.mit.ed
15 22:14:28.758924 192.168.1.1       192.168.1.97      DNS      200 Standard query response 0x0005 AAAA w

> Frame 12: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: Dell_a0: [redacted], Dst: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2)
> Internet Protocol Version 4, Src: 192.168.1.97, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 62088, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 13]
```

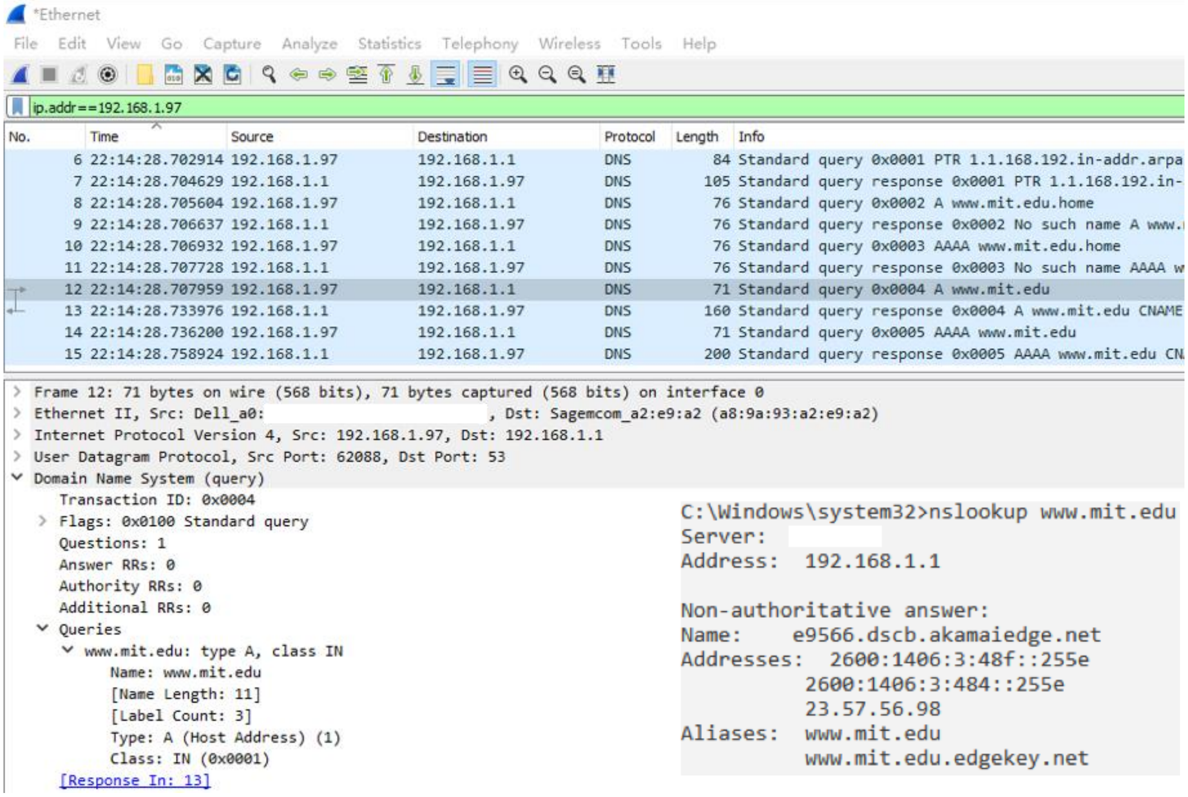
14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

A: 3 answers are provided. They contain first cname www.mit.edu.edgekey.net, second cname e9566.dscb.akamaiedge.net and the IP address 23.57.56.98



```
12 22:14:28.707959 192.168.1.97   192.168.1.1    DNS   71 Standard query 0x0004 A www.mit.edu
13 22:14:28.733976 192.168.1.1    192.168.1.97   DNS  160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.57.56.98
14 22:14:28.736200 192.168.1.97   192.168.1.1    DNS   71 Standard query 0x0005 AAAA www.mit.edu
15 22:14:28.758924 192.168.1.1    192.168.1.97   DNS  200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:

> Frame 13: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
> Ethernet II, Src: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2), Dst: Dell_a0: [redacted]
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.97
> User Datagram Protocol, Src Port: 53, Dst Port: 62088
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.57.56.98
    [Request In: 12]
    [Time: 0.026017000 seconds]
```

15. Provide a screenshot.

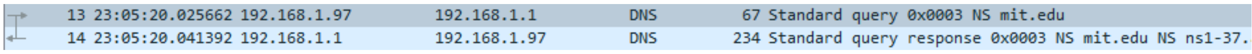


```
ip.addr==192.168.1.97

No.  Time            Source         Destination    Protocol Length Info
   6 22:14:28.702914 192.168.1.97   192.168.1.1    DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   7 22:14:28.704629 192.168.1.1    192.168.1.97   DNS      105 Standard query response 0x0001 PTR 1.1.168.192.in-
   8 22:14:28.705604 192.168.1.97   192.168.1.1    DNS       76 Standard query 0x0002 A www.mit.edu.home
   9 22:14:28.706637 192.168.1.1    192.168.1.97   DNS       76 Standard query response 0x0002 No such name A www.
  10 22:14:28.706932 192.168.1.97   192.168.1.1    DNS       76 Standard query 0x0003 AAAA www.mit.edu.home
  11 22:14:28.707728 192.168.1.1    192.168.1.97   DNS       76 Standard query response 0x0003 No such name AAAA w
  12 22:14:28.707959 192.168.1.97   192.168.1.1    DNS       71 Standard query 0x0004 A www.mit.edu
  13 22:14:28.733976 192.168.1.1    192.168.1.97   DNS      160 Standard query response 0x0004 A www.mit.edu CNAME
  14 22:14:28.736200 192.168.1.97   192.168.1.1    DNS       71 Standard query 0x0005 AAAA www.mit.edu
  15 22:14:28.758924 192.168.1.1    192.168.1.97   DNS      200 Standard query response 0x0005 AAAA www.mit.edu CN

> Frame 12: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: Dell_a0: [redacted], Dst: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2)
> Internet Protocol Version 4, Src: 192.168.1.97, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 62088, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 13]
```

```
C:\Windows\system32>nslookup www.mit.edu
Server:  [redacted]
Address:  192.168.1.1

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2600:1406:3:48f::255e
          2600:1406:3:484::255e
          23.57.56.98
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

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

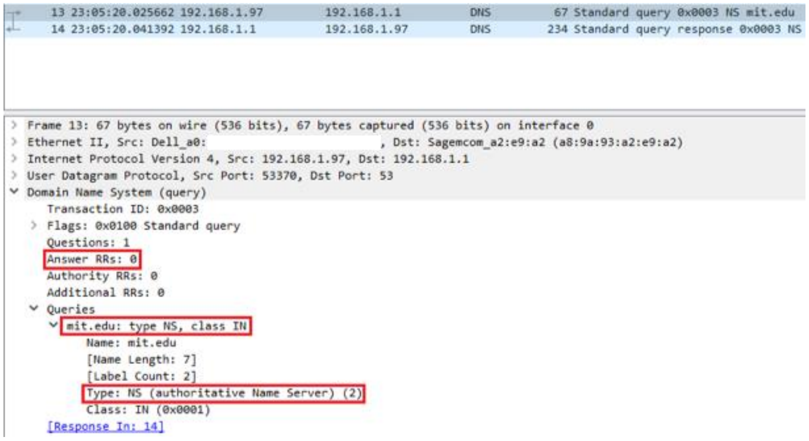
A: To 192.168.1.1 This is the IP address of my default local DNS server.



```
13 23:05:20.025662 192.168.1.97      192.168.1.1       DNS       67 Standard query 0x0003 NS mit.edu
14 23:05:20.041392 192.168.1.1       192.168.1.97      DNS      234 Standard query response 0x0003 NS mit.edu NS ns1-37.
```

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

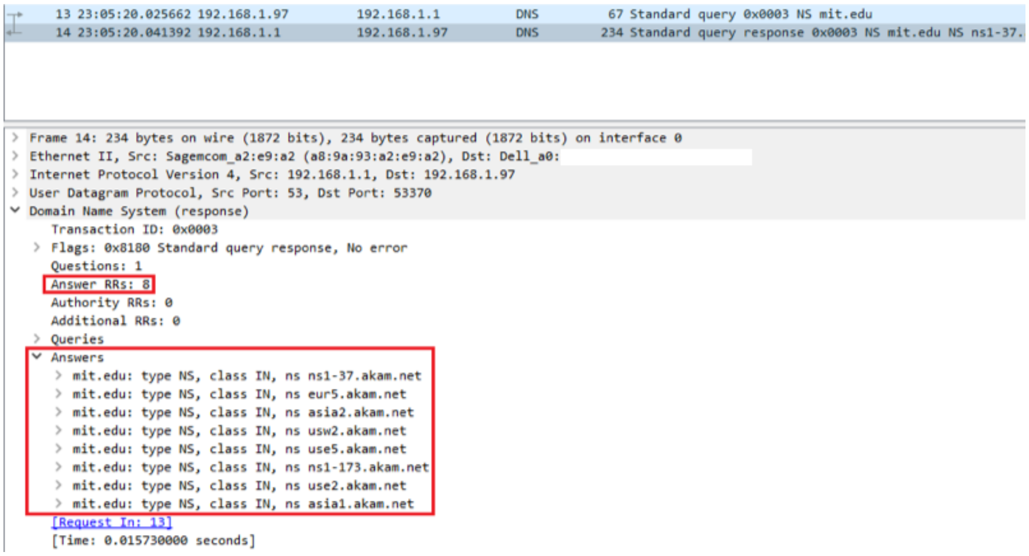
A: It is type “NS”. It contains no answers.



```
13 23:05:20.025662 192.168.1.97      192.168.1.1       DNS       67 Standard query 0x0003 NS mit.edu
14 23:05:20.041392 192.168.1.1       192.168.1.97      DNS      234 Standard query response 0x0003 NS

> Frame 13: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: Dell_a0: [redacted], Dst: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2)
> Internet Protocol Version 4, Src: 192.168.1.97, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 53370, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 14]
```

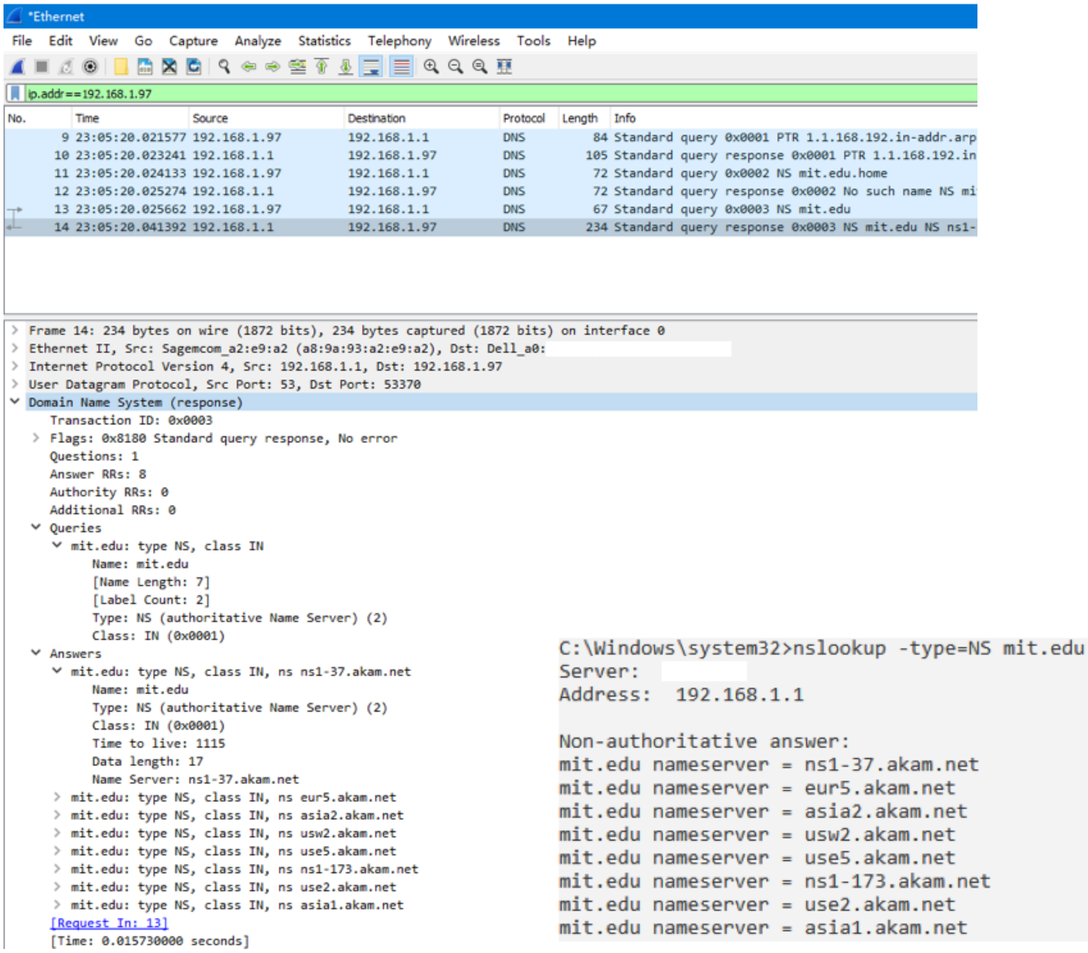
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

A: 8 nameservers are provided with no IP addresses.



```
13 23:05:20.025662 192.168.1.97      192.168.1.1       DNS       67 Standard query 0x0003 NS mit.edu
14 23:05:20.041392 192.168.1.1       192.168.1.97      DNS      234 Standard query response 0x0003 NS mit.edu NS ns1-37.

> Frame 14: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
> Ethernet II, Src: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2), Dst: Dell_a0: [redacted]
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.97
> User Datagram Protocol, Src Port: 53, Dst Port: 53370
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    [Request In: 13]
    [Time: 0.015730000 seconds]
```

19. Provide a screenshot.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==192.168.1.97
```

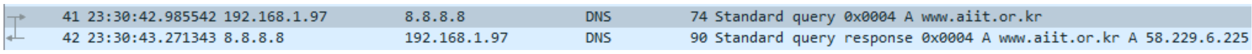
```
No.   Time               Source         Destination    Protocol Length Info
    9 23:05:20.021577 192.168.1.97   192.168.1.1    DNS          84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arp
   10 23:05:20.023241 192.168.1.1    192.168.1.97   DNS         105 Standard query response 0x0001 PTR 1.1.168.192.in
   11 23:05:20.024133 192.168.1.97   192.168.1.1    DNS          72 Standard query 0x0002 NS mit.edu.home
   12 23:05:20.025274 192.168.1.1    192.168.1.97   DNS          72 Standard query response 0x0002 No such name NS mi
   13 23:05:20.025662 192.168.1.97   192.168.1.1    DNS          67 Standard query 0x0003 NS mit.edu
   14 23:05:20.041392 192.168.1.1    192.168.1.97   DNS         234 Standard query response 0x0003 NS mit.edu NS ns1-
```

```
> Frame 14: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
> Ethernet II, Src: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2), Dst: Dell_a0: [redacted]
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.97
> User Datagram Protocol, Src Port: 53, Dst Port: 53370
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  v Answers
    v mit.edu: type NS, class IN, ns ns1-37.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1115
        Data length: 17
        Name Server: ns1-37.akam.net
    > mit.edu: type NS, class IN, ns eur5.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 use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    [Request In: 13]
    [Time: 0.015730000 seconds]
```

```
C:\Windows\system32>nslookup -type=NS mit.edu
Server:  [redacted]
Address:  192.168.1.1

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

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?

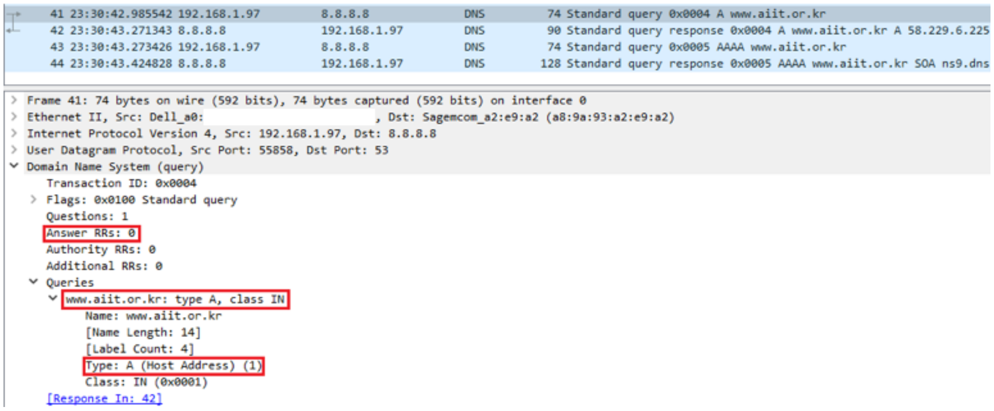
A: To 8.8.8.8 This is not the IP address of my default local DNS server. It is Google public DNS server.



```
   41 23:30:42.985542 192.168.1.97   8.8.8.8        DNS     74 Standard query 0x0004 A www.aiit.or.kr
   42 23:30:43.271343 8.8.8.8        192.168.1.97   DNS     90 Standard query response 0x0004 A www.aiit.or.kr A 58.229.6.225
```

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

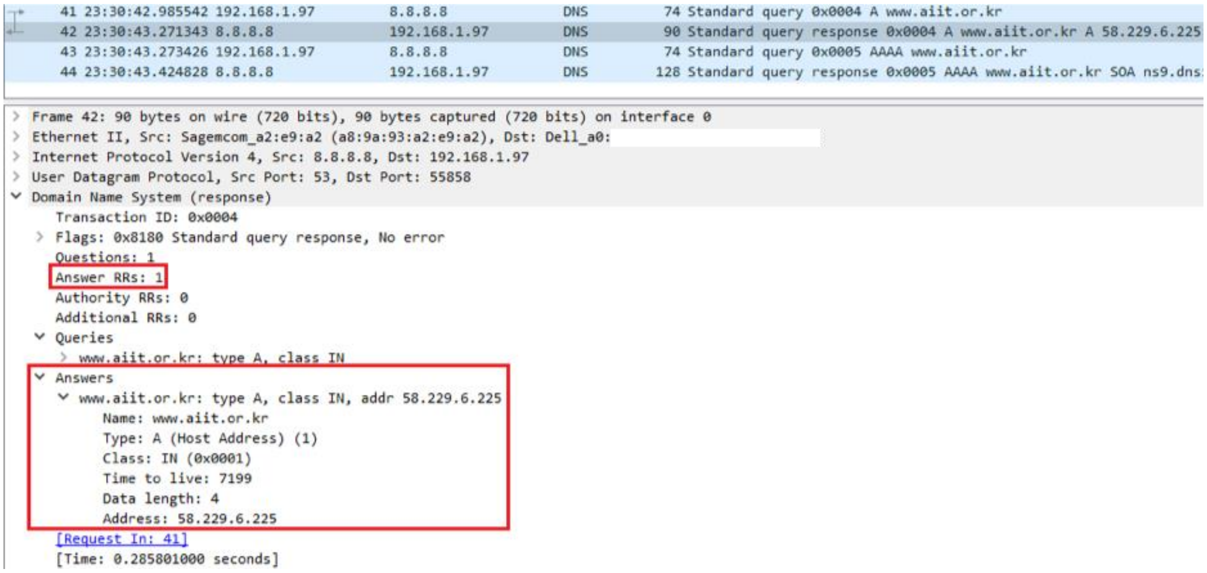
A: It is type "A". It contains no answers.



```
41 23:30:42.985542 192.168.1.97     8.8.8.8          DNS      74 Standard query 0x0004 A www.aiit.or.kr
42 23:30:43.271343 8.8.8.8          192.168.1.97     DNS      90 Standard query response 0x0004 A www.aiit.or.kr A 58.229.6.225
43 23:30:43.273426 192.168.1.97     8.8.8.8          DNS      74 Standard query 0x0005 AAAA www.aiit.or.kr
44 23:30:43.424828 8.8.8.8          192.168.1.97     DNS     128 Standard query response 0x0005 AAAA www.aiit.or.kr SOA ns9.dns

> Frame 41: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_a0:                    , Dst: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2)
> Internet Protocol Version 4, Src: 192.168.1.97, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 55858, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 42]
```

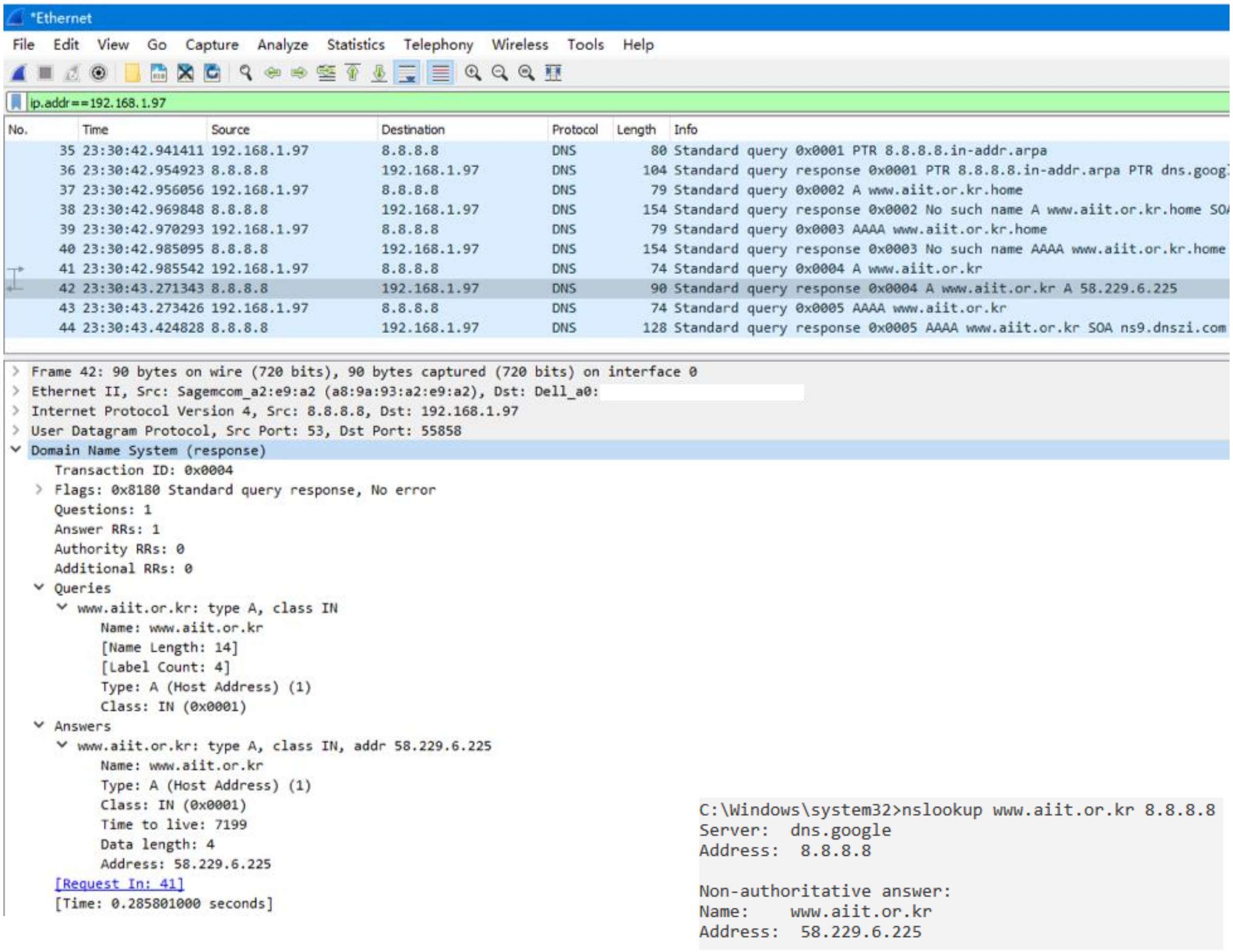
22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

A: 1 answer is provided. It contains the IP address 58.229.6.225



```
41 23:30:42.985542 192.168.1.97     8.8.8.8          DNS      74 Standard query 0x0004 A www.aiit.or.kr
42 23:30:43.271343 8.8.8.8          192.168.1.97     DNS      90 Standard query response 0x0004 A www.aiit.or.kr A 58.229.6.225
43 23:30:43.273426 192.168.1.97     8.8.8.8          DNS      74 Standard query 0x0005 AAAA www.aiit.or.kr
44 23:30:43.424828 8.8.8.8          192.168.1.97     DNS     128 Standard query response 0x0005 AAAA www.aiit.or.kr SOA ns9.dns:

> Frame 42: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2), Dst: Dell_a0:
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.97
> User Datagram Protocol, Src Port: 53, Dst Port: 55858
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.aiit.or.kr: type A, class IN
  v Answers
    v www.aiit.or.kr: type A, class IN, addr 58.229.6.225
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 7199
        Data length: 4
        Address: 58.229.6.225
    [Request In: 41]
    [Time: 0.285801000 seconds]
```

23. Provide a screenshot.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==192.168.1.97
```

```
No.  Time            Source          Destination   Protocol Length Info
  35 23:30:42.941411 192.168.1.97    8.8.8.8       DNS        80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
  36 23:30:42.954923 8.8.8.8         192.168.1.97  DNS       104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.googl
  37 23:30:42.956056 192.168.1.97    8.8.8.8       DNS        79 Standard query 0x0002 A www.aiit.or.kr.home
  38 23:30:42.969848 8.8.8.8         192.168.1.97  DNS       154 Standard query response 0x0002 No such name A www.aiit.or.kr.home SO
  39 23:30:42.970293 192.168.1.97    8.8.8.8       DNS        79 Standard query 0x0003 AAAA www.aiit.or.kr.home
  40 23:30:42.985095 8.8.8.8         192.168.1.97  DNS       154 Standard query response 0x0003 No such name AAAA www.aiit.or.kr.home
  41 23:30:42.985542 192.168.1.97    8.8.8.8       DNS        74 Standard query 0x0004 A www.aiit.or.kr
  42 23:30:43.271343 8.8.8.8         192.168.1.97  DNS        90 Standard query response 0x0004 A www.aiit.or.kr A 58.229.6.225
  43 23:30:43.273426 192.168.1.97    8.8.8.8       DNS        74 Standard query 0x0005 AAAA www.aiit.or.kr
  44 23:30:43.424828 8.8.8.8         192.168.1.97  DNS       128 Standard query response 0x0005 AAAA www.aiit.or.kr SOA ns9.dnszi.com
```

```
> Frame 42: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: Sagemcom_a2:e9:a2 (a8:9a:93:a2:e9:a2), Dst: Dell_a0: [redacted]
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.97
> User Datagram Protocol, Src Port: 53, Dst Port: 55858
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v www.aiit.or.kr: type A, class IN, addr 58.229.6.225
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 7199
        Data length: 4
        Address: 58.229.6.225
    [Request In: 41]
    [Time: 0.285801000 seconds]
```

```
C:\Windows\system32>nslookup www.aiit.or.kr 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  58.229.6.225
```

Conclusion

The *nslookup* can be used to obtain IP address or nameserver. In the lab, three types of DNS records are met, which are type “A” (stores hostname and IP address), type “NS” (returns the authoritative nameserver to the DNS zone) and type “CNAME” (alias a host name to another host name).

The Wireshark is good for analyzing DNS query and request message, it labels the detail of Queries and Answers.

Sept.29 2019