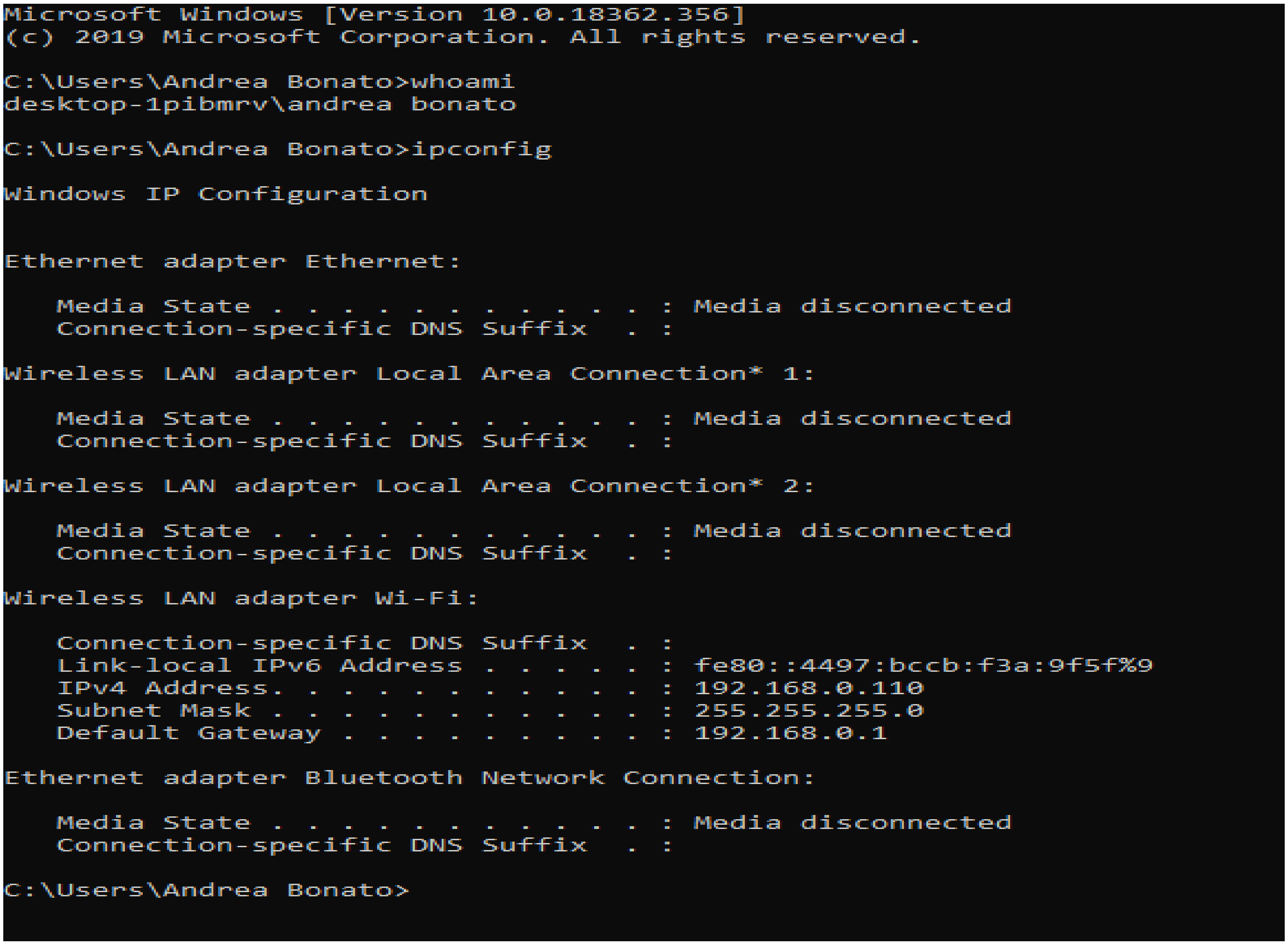
COMP-3670 FALL 2019 Assignment 1

Andrea Bonato

104760390



```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

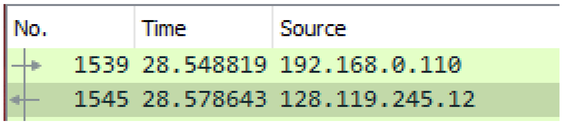
Introduction to Wireshark

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Three different protocols that appear in the protocol column in the unfiltered packet-listing window would be HTTP (Hypertext Transfer Protocol), TCP (Transmission Control Protocol) and ARP (Address Resolution Protocol).

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column

Between the HTTP GET message departure and the HTTP OK arrival, it took 0.029824 seconds.



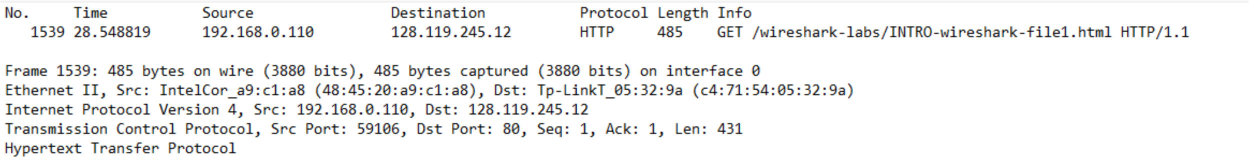
No.	Time	Source
1539	28.548819	192.168.0.110
1545	28.578643	128.119.245.12

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

The IP address of my computer is 192.168.0.110 and the gaia.cs.umass.edu server is 128.119.245.12.

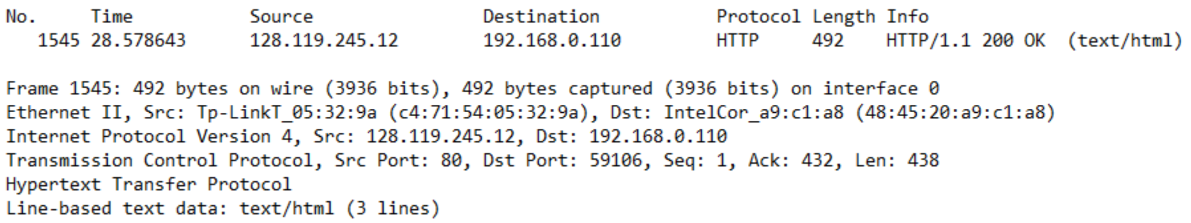
4. Print the two HTTP messages (GET and OK) referred to in question 2 above.

For get:



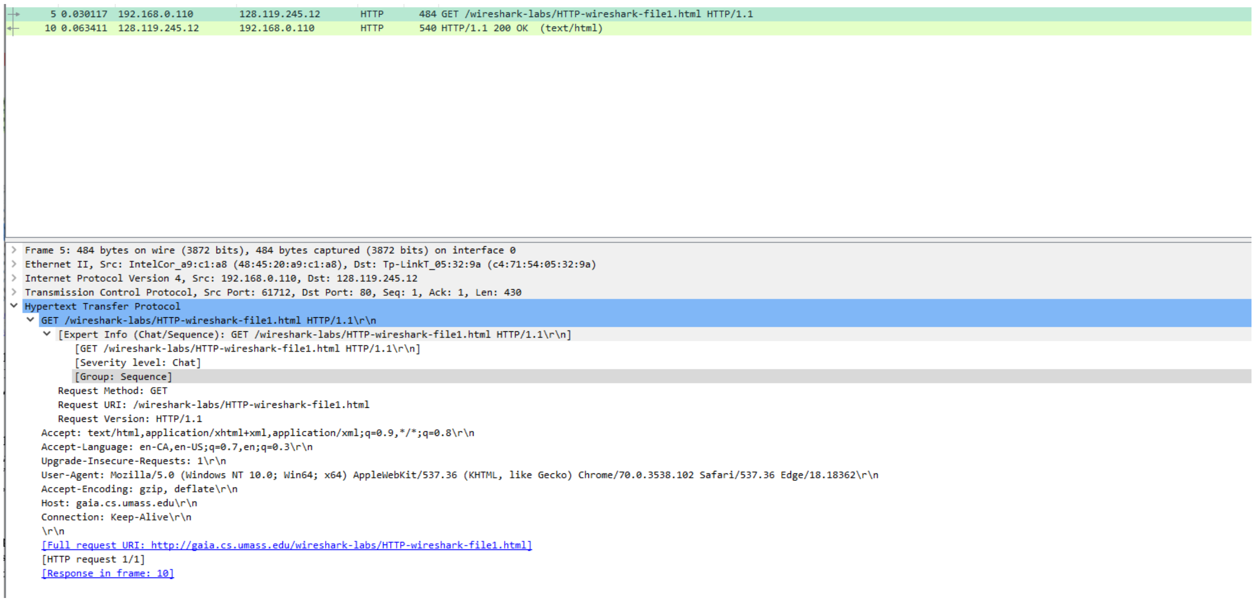
```
No.     Time           Source                Destination           Protocol Length Info
   1539 28.548819      192.168.0.110         128.119.245.12        HTTP     485    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 1539: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface 0
Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
Internet Protocol Version 4, Src: 192.168.0.110, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59106, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
Hypertext Transfer Protocol
```

For ok:



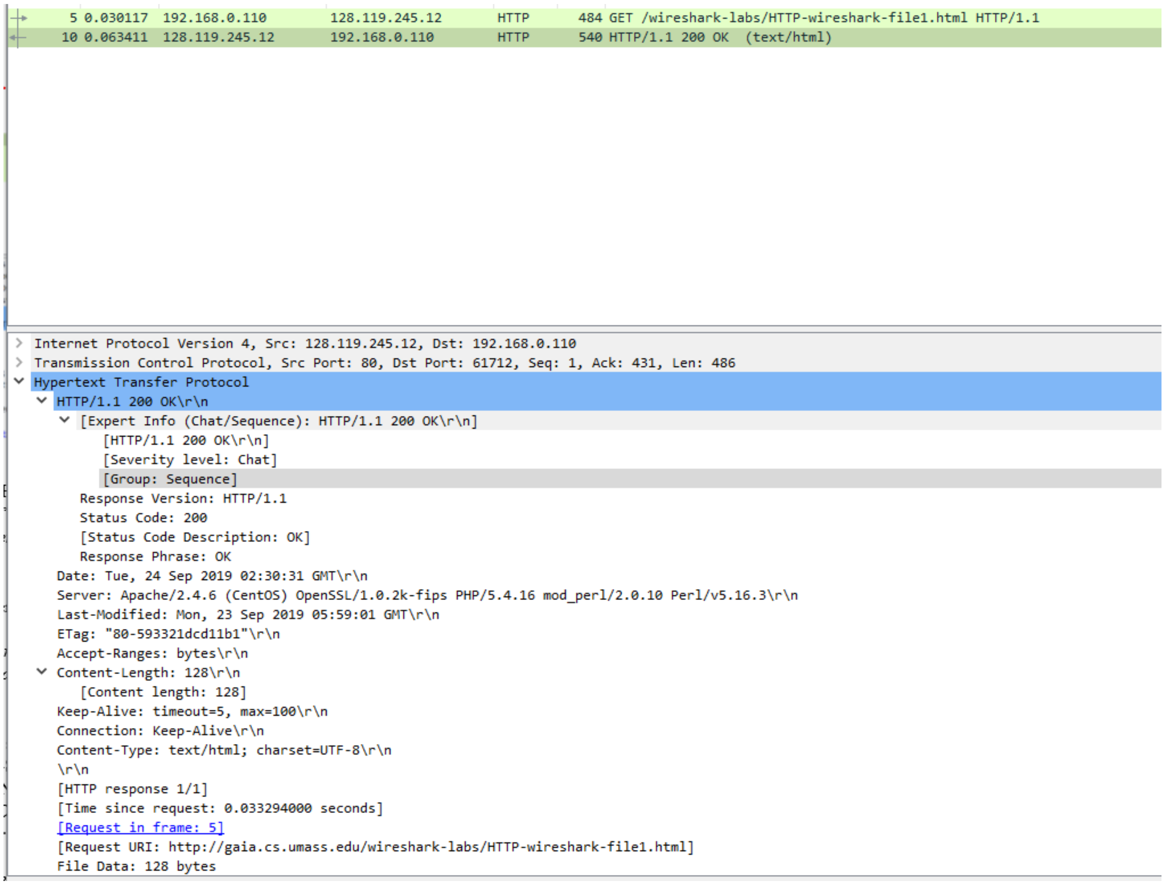
```
No.     Time           Source                Destination           Protocol Length Info
   1545 28.578643      128.119.245.12        192.168.0.110         HTTP     492    HTTP/1.1 200 OK  (text/html)

Frame 1545: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a), Dst: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.110
Transmission Control Protocol, Src Port: 80, Dst Port: 59106, Seq: 1, Ack: 432, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

HTTP



```
   5 0.030117  192.168.0.110     128.119.245.12    HTTP     484 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  10 0.063411  128.119.245.12    192.168.0.110     HTTP     540 HTTP/1.1 200 OK  (text/html)

> Frame 5: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface 0
> Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61712, Dst Port: 80, Seq: 1, Ack: 1, Len: 430
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-CA,en-US;q=0.7,en;q=0.3\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 10]
```

Figure 1: This is the image that will be used to answer the following questions about the HTTP GET



```
   5 0.030117  192.168.0.110     128.119.245.12    HTTP     484 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  10 0.063411  128.119.245.12    192.168.0.110     HTTP     540 HTTP/1.1 200 OK  (text/html)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.110
> Transmission Control Protocol, Src Port: 80, Dst Port: 61712, Seq: 1, Ack: 431, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 24 Sep 2019 02:30:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Mon, 23 Sep 2019 05:59:01 GMT\r\n
    ETag: "80-593321dcd11b1"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 128\r\n
      [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.033294000 seconds]
    [Request in frame: 5]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
```

Figure 2: This is the image that will be used to answer the following questions about the HTTP OK

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

The browser is running HTTP version 1.1, as found where it is highlighted in red. The server is running HTTP version 1.1 as well.

2. What languages (if any) does your browser indicate that it can accept to the server?

The browser indicates that it can accepts only English, but both the US and Canadian spelling.

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

The IP address of my computer is 192.168.0.110 and the IP address of the gaia.cs.umass.edu server is 128.119.245.12.

4. What is the status code returned from the server to your browser?

The status code returned from the server is 200 OK. This means that the request has succeeded.

5. When was the HTML file that you are retrieving last modified at the server?

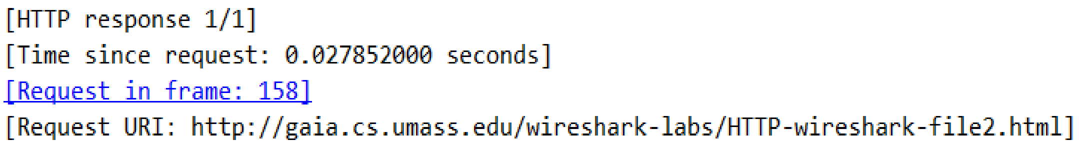
The HTML file that I am receiving was last modified Sun, 22 Sep 2019 05:59:01 GMT.

6. How many bytes of content are being returned to your browser?

The contents that are being returned to the browser is 128 bytes.

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

The only information that is not shown in the packet listing window is:



```
[HTTP response 1/1]
[Time since request: 0.027852000 seconds]
[Request in frame: 158]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

In the contents of the first HTTP GET request, there is no "IF-MODIFED_SINCE" statement.

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Since the status code for the returned contents of the file is 200, this means that the information was returned successfully.

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

There is an IF-MODIFIED-SINCE line, and following it, it says "IF-MODIFIED-SINCE: Sun, 22 Sep 2019 05:59:01 gmt\r\n" Under this, there is a URI request

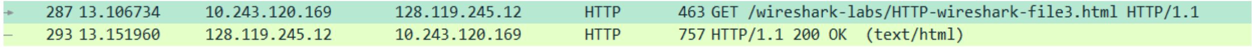
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The status code is 304 Not Modified, which means that the browser already had the latest update. This the server did not return the contents of the file.

****NOTE: I did change to the university wifi and thus my IP address changed****

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

The browser sent only one HTTP GET request messages. The packet number that the browser sent was 287 as shown below.



```
→  287 13.106734   10.243.120.169   128.119.245.12   HTTP   463 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
←  293 13.151960   128.119.245.12   10.243.120.169   HTTP   757 HTTP/1.1 200 OK  (text/html)
```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

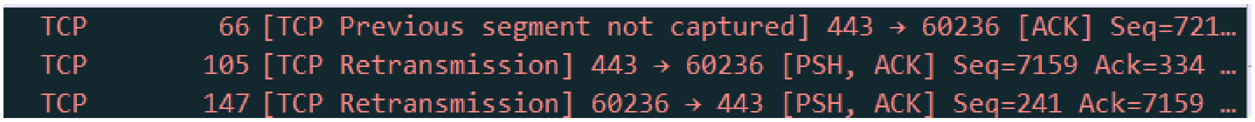
The packet, as shown above, that contains the status code and phrase is packet 293. This status code is 200.

14. What is the status code and phrase in the response?

The status code that was received was 200, which means that the information was received successfully. The response was OK.

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

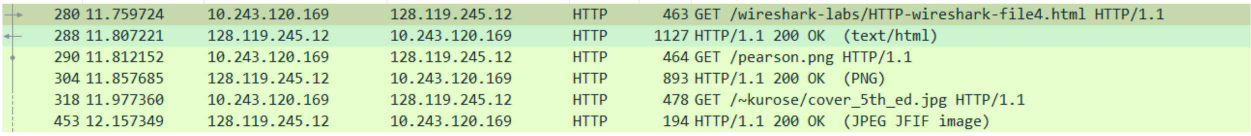
According to the screenshot below, it took a total of 3 data-containing TCP segments to carry the HTTP response.



```
TCP        66 [TCP Previous segment not captured] 443 → 60236 [ACK] Seq=721…
TCP       105 [TCP Retransmission] 443 → 60236 [PSH, ACK] Seq=7159 Ack=334 …
TCP       147 [TCP Retransmission] 60236 → 443 [PSH, ACK] Seq=241 Ack=7159 …
```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

The browser sent three HTTP GET messages as shown below in the screenshot. The destination that these requests were sent to was 128.119.245.12.



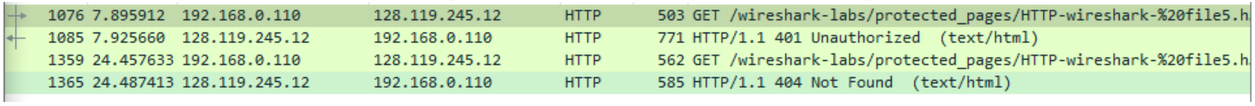
```
280 11.759724   10.243.120.169   128.119.245.12   HTTP    463 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
288 11.807221   128.119.245.12   10.243.120.169   HTTP   1127 HTTP/1.1 200 OK  (text/html)
290 11.812152   10.243.120.169   128.119.245.12   HTTP    464 GET /pearson.png HTTP/1.1
304 11.857685   128.119.245.12   10.243.120.169   HTTP    893 HTTP/1.1 200 OK  (PNG)
318 11.977360   10.243.120.169   128.119.245.12   HTTP    478 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
453 12.157349   128.119.245.12   10.243.120.169   HTTP    194 HTTP/1.1 200 OK  (JPEG JFIF image)
```

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

I would assume that each message was downloaded serially because of the fact that each GET message is followed by an OK message. In addition to that, since they are broken up into 3 different sections, it is assumed each one is an HTTP GET request.

18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

The status code in the servers response is 401 and the response is Unauthorized. This means that the credientials lack the authority to access the information on this part of the server.

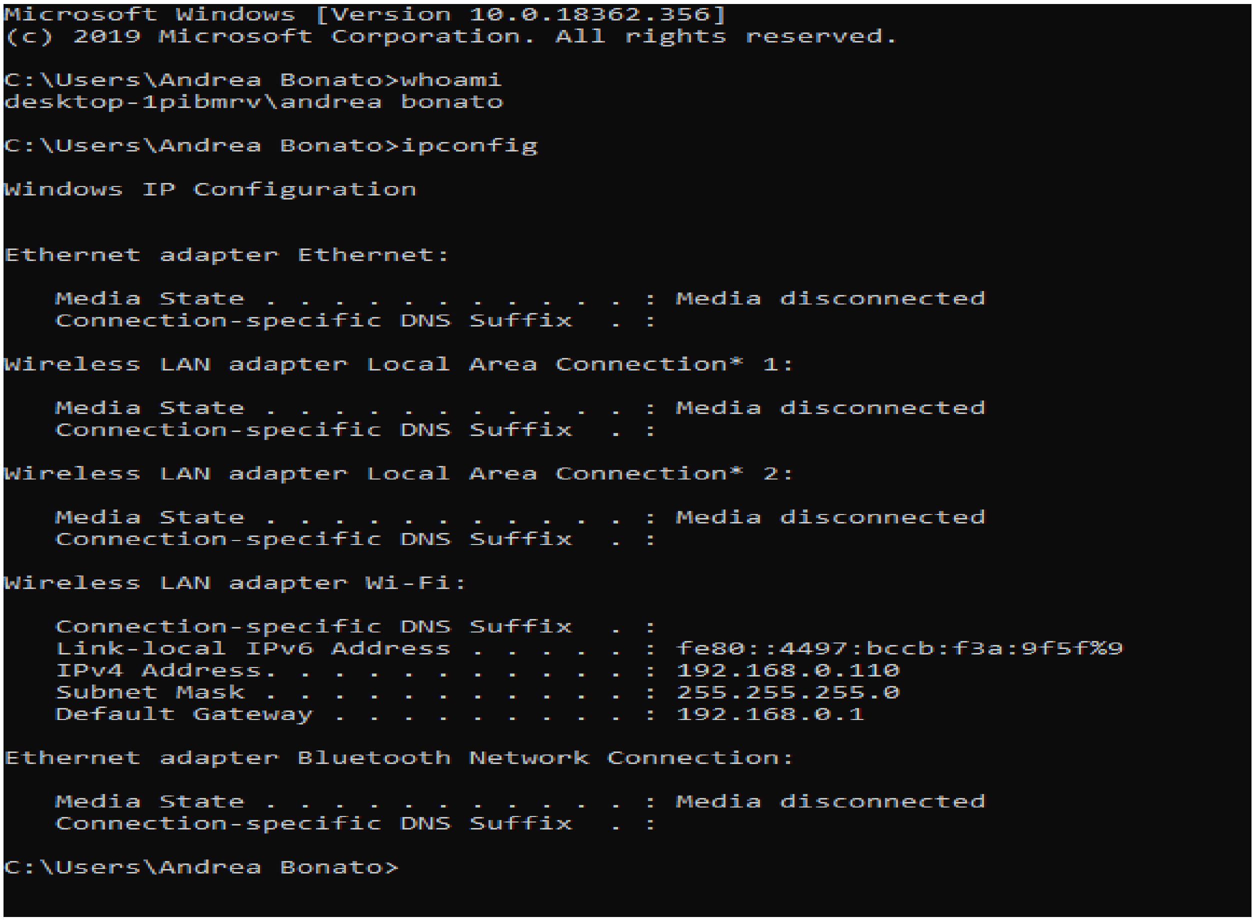


```
1076 7.895912  192.168.0.110    128.119.245.12   HTTP   503 GET /wireshark-labs/protected_pages/HTTP-wireshark-%20file5.h
1085 7.925660  128.119.245.12   192.168.0.110    HTTP   771 HTTP/1.1 401 Unauthorized  (text/html)
1359 24.457633 192.168.0.110    128.119.245.12   HTTP   562 GET /wireshark-labs/protected_pages/HTTP-wireshark-%20file5.h
1365 24.487413 128.119.245.12   192.168.0.110    HTTP   585 HTTP/1.1 404 Not Found  (text/html)
```

19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

As shown above, the new HTTP get message for the second time is a 404 Not Found text.

****NOTE: I did change to my home internet and thus my IP address changed****

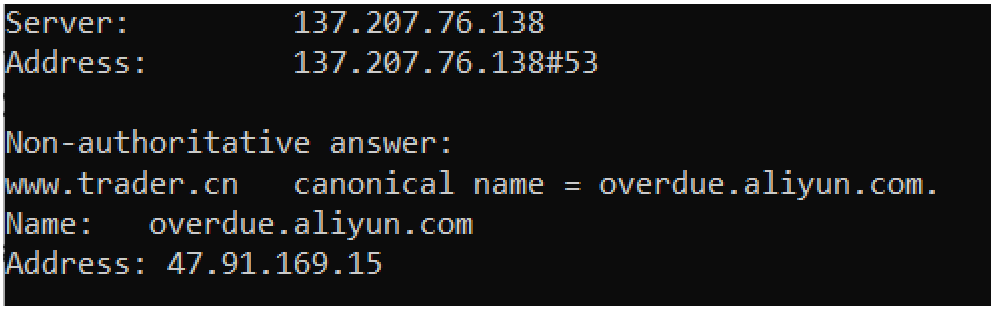


```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

DNS

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

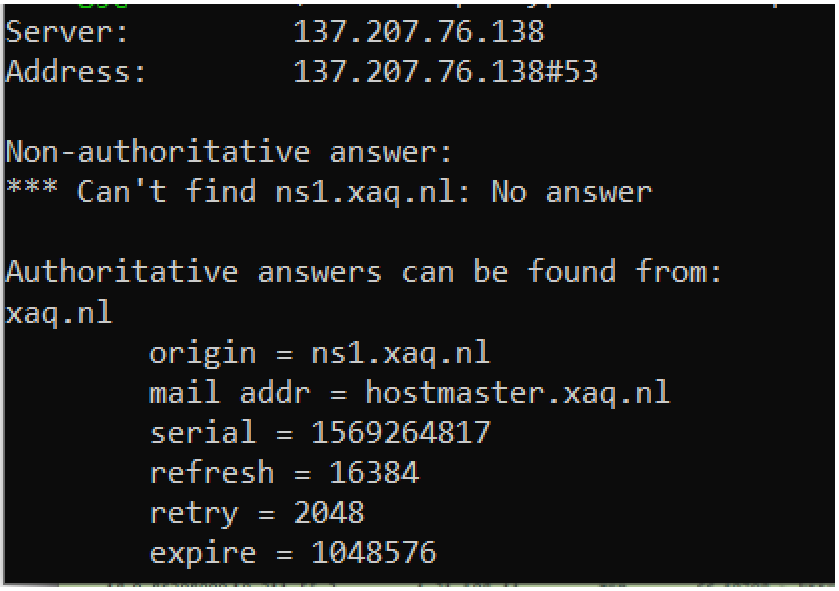
The ip address of the asian web server www.trader.cn is 47.91.169.15. As shown in the following photo.



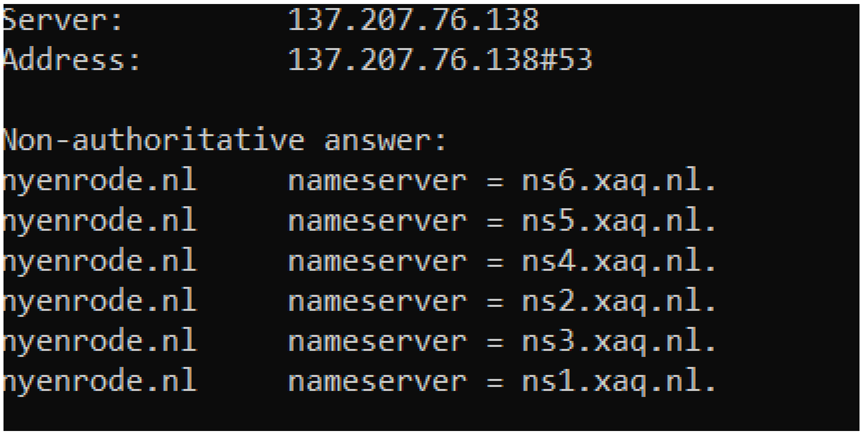
```
Server:         137.207.76.138
Address:        137.207.76.138#53

Non-authoritative answer:
www.trader.cn   canonical name = overdue.aliyun.com.
Name:   overdue.aliyun.com
Address: 47.91.169.15
```

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

The authorative DNS servers (nyenrode.nl) for Nyenrode Business University in Europe are as followed:



```
Server:         137.207.76.138
Address:        137.207.76.138#53

Non-authoritative answer:
*** Can't find ns1.xaq.nl: No answer

Authoritative answers can be found from:
xaq.nl
        origin = ns1.xaq.nl
        mail addr = hostmaster.xaq.nl
        serial = 1569264817
        refresh = 16384
        retry = 2048
        expire = 1048576
```



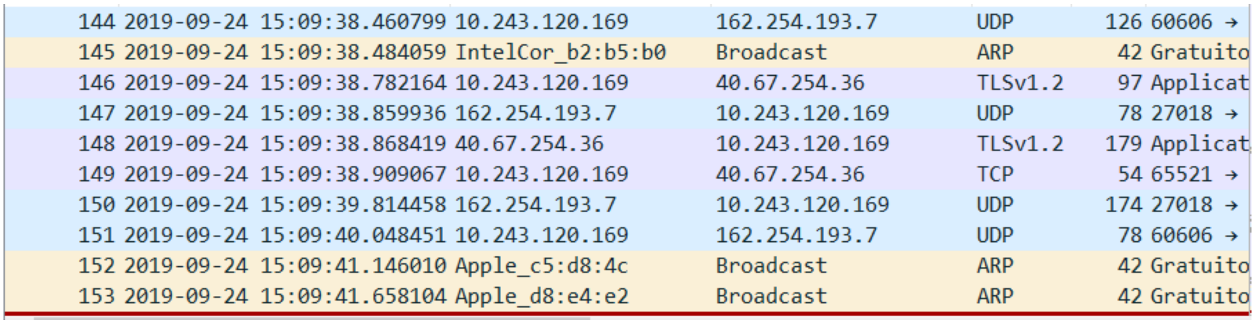
```
Server:         137.207.76.138
Address:        137.207.76.138#53

Non-authoritative answer:
nyenrode.nl     nameserver = ns6.xaq.nl.
nyenrode.nl     nameserver = ns5.xaq.nl.
nyenrode.nl     nameserver = ns4.xaq.nl.
nyenrode.nl     nameserver = ns2.xaq.nl.
nyenrode.nl     nameserver = ns3.xaq.nl.
nyenrode.nl     nameserver = ns1.xaq.nl.
```

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

The IP appress for the DNS server when queries for the Yahoo! Mail server is 209.191.122.42.

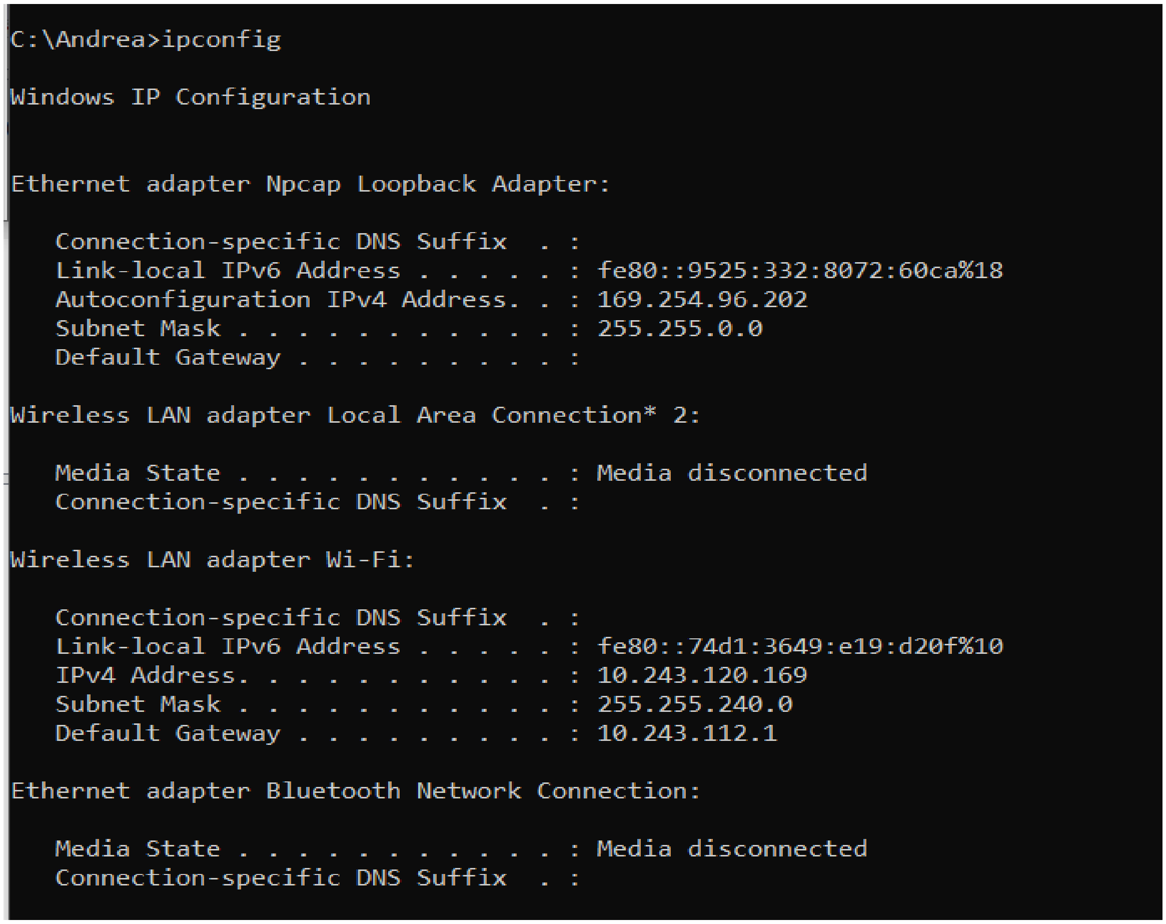
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

As shown below, these are all standard queries through DNS. The messages themselves were sent over UDP.



```
144 2019-09-24 15:09:38.460799 10.243.120.169     162.254.193.7      UDP       126 60606 →
145 2019-09-24 15:09:38.484059 IntelCor_b2:b5:b0  Broadcast          ARP        42 Gratuito
146 2019-09-24 15:09:38.782164 10.243.120.169     40.67.254.36       TLSv1.2    97 Applicat
147 2019-09-24 15:09:38.859936 162.254.193.7      10.243.120.169     UDP        78 27018 →
148 2019-09-24 15:09:38.868419 40.67.254.36       10.243.120.169     TLSv1.2   179 Applicat
149 2019-09-24 15:09:38.909067 10.243.120.169     40.67.254.36       TCP        54 65521 →
150 2019-09-24 15:09:39.814458 162.254.193.7      10.243.120.169     UDP       174 27018 →
151 2019-09-24 15:09:40.048451 10.243.120.169     162.254.193.7      UDP        78 60606 →
152 2019-09-24 15:09:41.146010 Apple_c5:d8:4c     Broadcast          ARP        42 Gratuito
153 2019-09-24 15:09:41.658104 Apple_d8:e4:e2     Broadcast          ARP        42 Gratuito
```

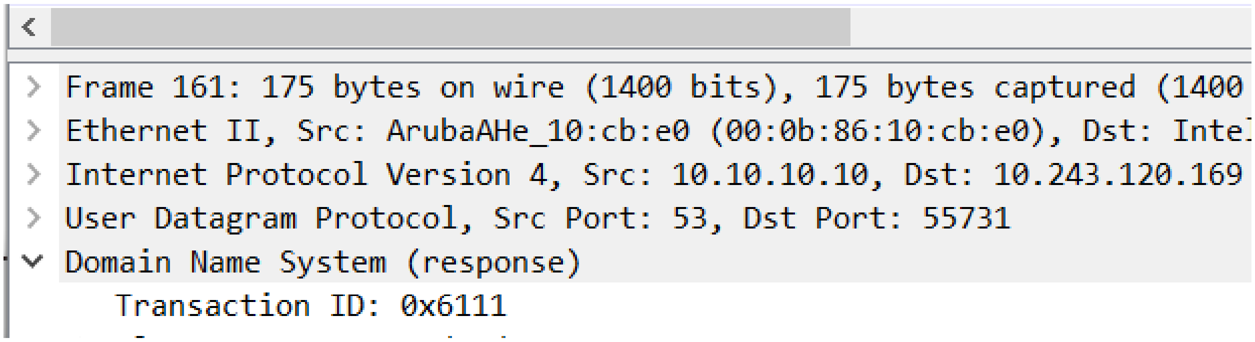
****NOTE: I did change to the university wifi and thus my IP address changed****



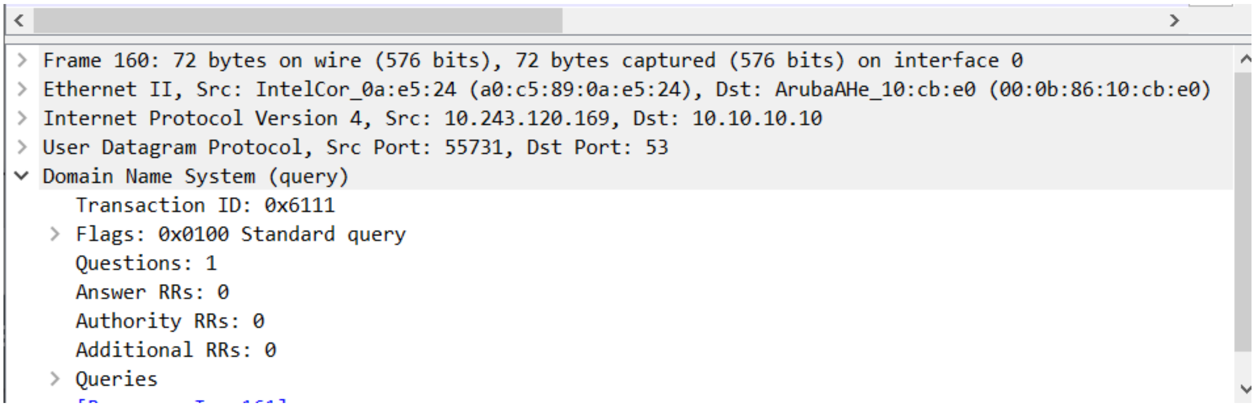
```
C:\Andrea>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.243.120.169
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.243.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

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

The destination port for the DNS query message is port 53 in packet 160. The source port of DNS response message is also port 53 in packet 161.

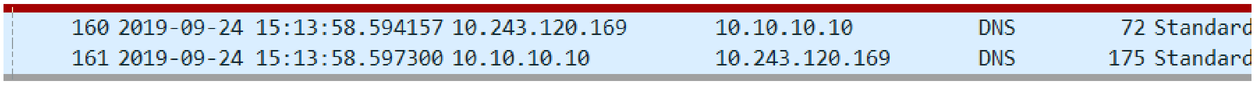


```
> Frame 161: 175 bytes on wire (1400 bits), 175 bytes captured (1400
> Ethernet II, Src: ArubaAHe_10:cb:e0 (00:0b:86:10:cb:e0), Dst: Inte
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.243.120.169
> User Datagram Protocol, Src Port: 53, Dst Port: 55731
v Domain Name System (response)
     Transaction ID: 0x6111
```



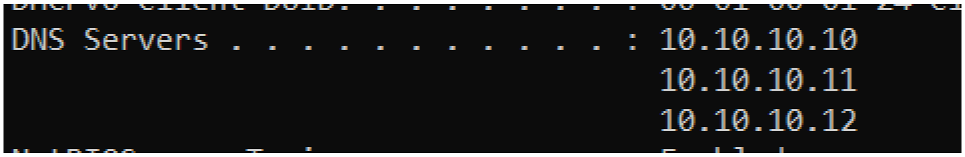
```
> Frame 160: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_10:cb:e0 (00:0b:86:10:cb:e0)
> Internet Protocol Version 4, Src: 10.243.120.169, Dst: 10.10.10.10
> User Datagram Protocol, Src Port: 55731, Dst Port: 53
v Domain Name System (query)
     Transaction ID: 0x6111
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   > Queries
```

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?



```
160 2019-09-24 15:13:58.594157 10.243.120.169    10.10.10.10       DNS       72 Standard
161 2019-09-24 15:13:58.597300 10.10.10.10       10.243.120.169    DNS      175 Standard
```

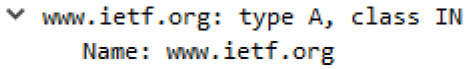
The IP address that the DNS query message sent to was 10.10.10.10. The IP address of your local DNS server is also 10.10.10.10. Thus, they are both the same.



```
DNS Servers . . . . . . . . . . . : 10.10.10.10
                                    10.10.10.11
                                    10.10.10.12
```

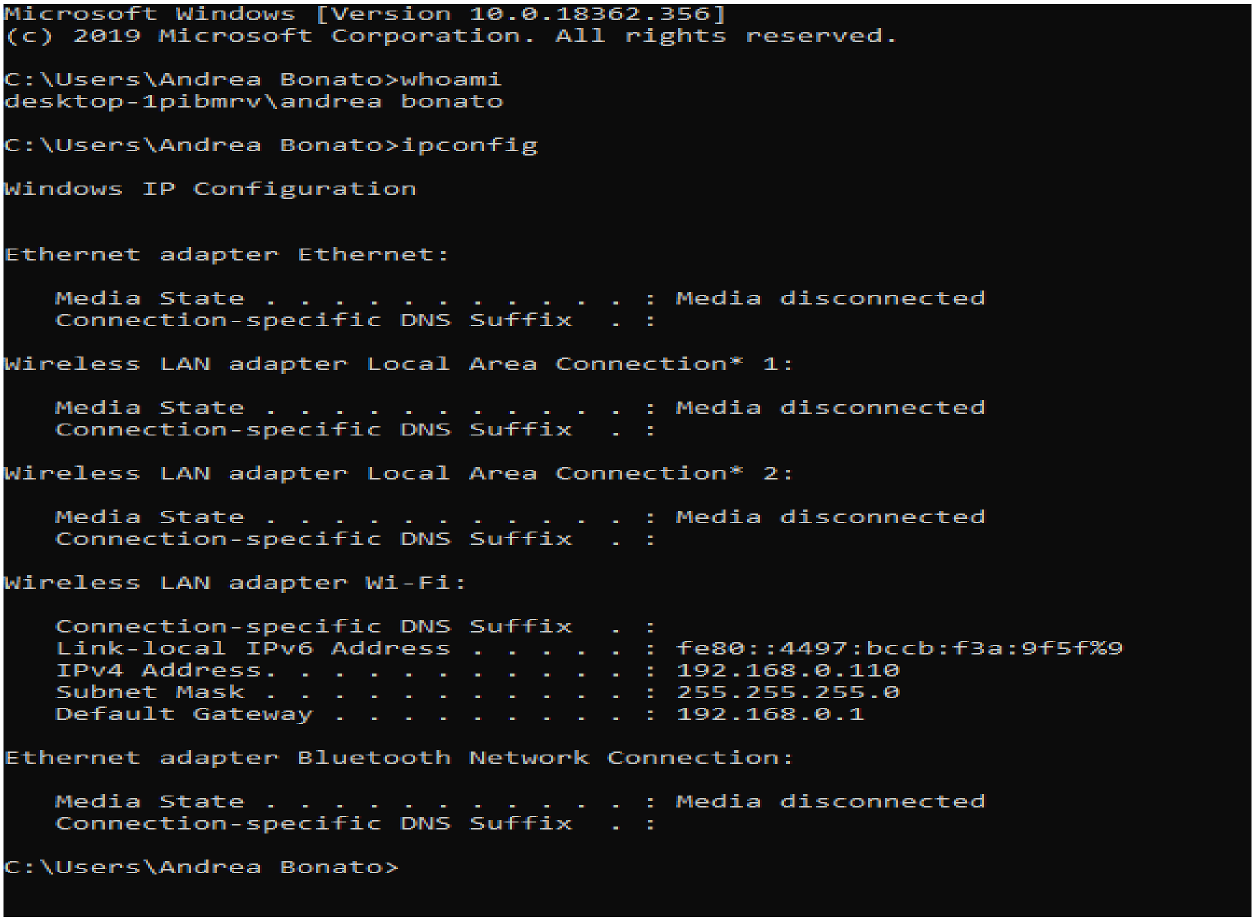
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The type of the query message is A and the DNS query did not contain any answers.



```
v www.ietf.org: type A, class IN
      Name: www.ietf.org
```

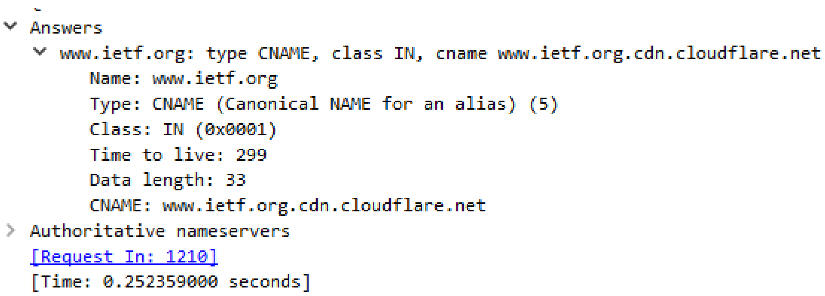
****NOTE: I did change to my home internet and thus my IP address changed****



```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

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

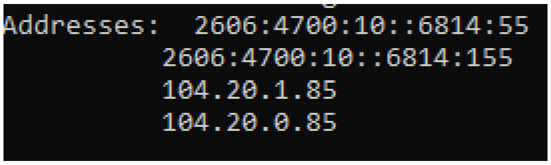
In the repsonse message, there are only 1 answer provided. In this answer, we see the website, type, name, class and the data length of the response.



```
˅ 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: 299
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
> Authoritative nameservers
  [Request In: 1210]
  [Time: 0.252359000 seconds]
```

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

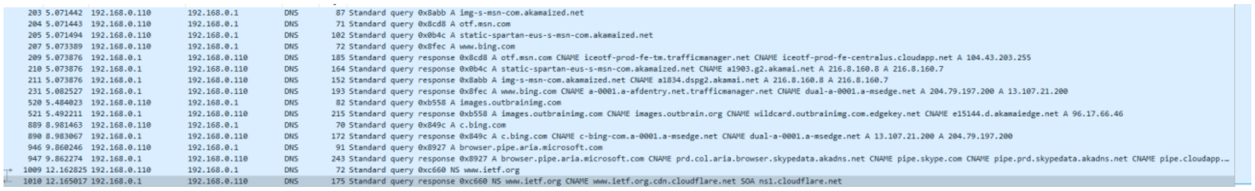
The SYN packet is 104.20.1.85, which is the same address that was associated with the address of the webpage.



```
Addresses:  2606:4700:10::6814:55
          2606:4700:10::6814:155
          104.20.1.85
          104.20.0.85
```

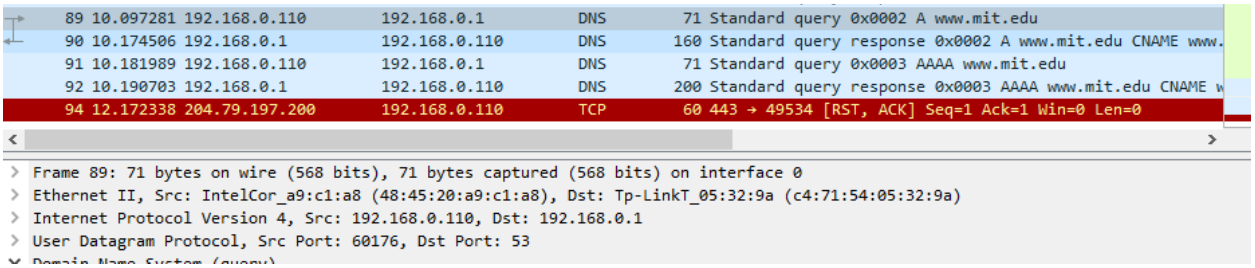
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Before the images were retrieved, the host did issue new DNS queries. For each query that related to the image, for example, the image is from another site, it queried that site first.



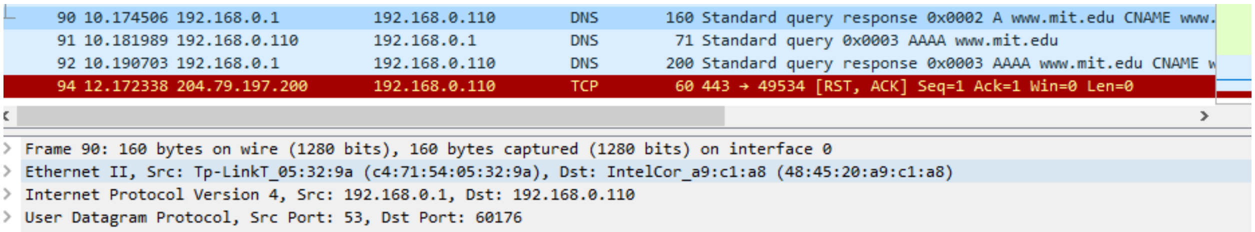
```
 203 5.071442  192.168.0.110  192.168.0.1    DNS   87 Standard query 0x8abb A img-s-msn-com.akamaized.net
 204 5.071443  192.168.0.110  192.168.0.1    DNS   71 Standard query 0x8cd8 A otf.msn.com
 205 5.071494  192.168.0.110  192.168.0.1    DNS  102 Standard query 0x0b4c A static-spartan-eus-s-msn-com.akamaized.net
 207 5.073389  192.168.0.110  192.168.0.1    DNS   72 Standard query 0x8fec A www.bing.com
 209 5.073876  192.168.0.1    192.168.0.110  DNS  185 Standard query response 0x8cd8 A otf.msn.com CNAME iceotf-prod-fe-tm.trafficmanager.net CNAME iceotf-prod-fe-centralus.cloudapp.net A 104.43.203.255
 210 5.073876  192.168.0.1    192.168.0.110  DNS  164 Standard query response 0x0b4c A static-spartan-eus-s-msn-com.akamaized.net CNAME a1903.g2.akamai.net A 216.8.160.8 A 216.8.160.7
 211 5.073876  192.168.0.1    192.168.0.110  DNS  152 Standard query response 0x8abb A img-s-msn-com.akamaized.net CNAME a1834.dspg2.akamai.net A 216.8.160.8 A 216.8.160.7
 231 5.082527  192.168.0.1    192.168.0.110  DNS  193 Standard query response 0x8fec A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME dual-a-0001.a-msedge.net A 204.79.197.200 A 13.107.21.200
 520 5.484023  192.168.0.110  192.168.0.1    DNS   82 Standard query 0xb558 A images.outbrainimg.com
 521 5.492211  192.168.0.1    192.168.0.110  DNS  215 Standard query response 0xb558 A images.outbrainimg.com CNAME images.outbrain.org CNAME wildcard.outbrainimg.com.edgekey.net CNAME e15144.d.akamaiedge.net A 96.17.66.46
 889 8.981463  192.168.0.110  192.168.0.1    DNS   70 Standard query 0x849c A c.bing.com
 890 8.983067  192.168.0.1    192.168.0.110  DNS  172 Standard query response 0x849c A c.bing.com CNAME c-bing-com.a-0001.a-msedge.net CNAME dual-a-0001.a-msedge.net A 13.107.21.200 A 204.79.197.200
 946 9.860246  192.168.0.110  192.168.0.1    DNS   91 Standard query 0x8927 A browser.pipe.aria.microsoft.com
 947 9.862274  192.168.0.1    192.168.0.110  DNS  243 Standard query response 0x8927 A browser.pipe.aria.microsoft.com CNAME prd.col.aria.browser.skypedata.akadns.net CNAME pipe.skype.com CNAME pipe.prd.skypedata.akadns.net CNAME pipe.cloudapp.…
1009 12.162825 192.168.0.110  192.168.0.1    DNS   72 Standard query 0xc660 NS www.ietf.org
1010 12.165017 192.168.0.1    192.168.0.110  DNS  175 Standard query response 0xc660 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?



```
89 10.097281 192.168.0.110      192.168.0.1       DNS      71 Standard query 0x0002 A www.mit.edu
90 10.174506 192.168.0.1        192.168.0.110     DNS     160 Standard query response 0x0002 A www.mit.edu CNAME www.
91 10.181989 192.168.0.110      192.168.0.1       DNS      71 Standard query 0x0003 AAAA www.mit.edu
92 10.190703 192.168.0.1        192.168.0.110     DNS     200 Standard query response 0x0003 AAAA www.mit.edu CNAME w
94 12.172338 204.79.197.200     192.168.0.110     TCP      60 443 → 49534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 89: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 60176, Dst Port: 53
v Domain Name System (query)
```

The source port 607176 and the destination port is 53 in the query message.

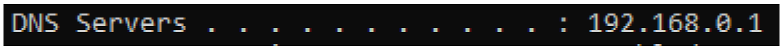


```
90 10.174506 192.168.0.1        192.168.0.110     DNS     160 Standard query response 0x0002 A www.mit.edu CNAME www.
91 10.181989 192.168.0.110      192.168.0.1       DNS      71 Standard query 0x0003 AAAA www.mit.edu
92 10.190703 192.168.0.1        192.168.0.110     DNS     200 Standard query response 0x0003 AAAA www.mit.edu CNAME w
94 12.172338 204.79.197.200     192.168.0.110     TCP      60 443 → 49534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 90: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a), Dst: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.110
> User Datagram Protocol, Src Port: 53, Dst Port: 60176
```

In the response message, the source port and the destination ports are opposite than in the query message.

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

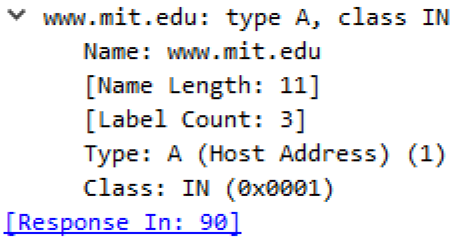
The DNS query message was sent to the IP address 192.168.0.1. which just so happens to be the IP address of my local DNS server.



```
DNS Servers . . . . . . . . . . . : 192.168.0.1
```

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

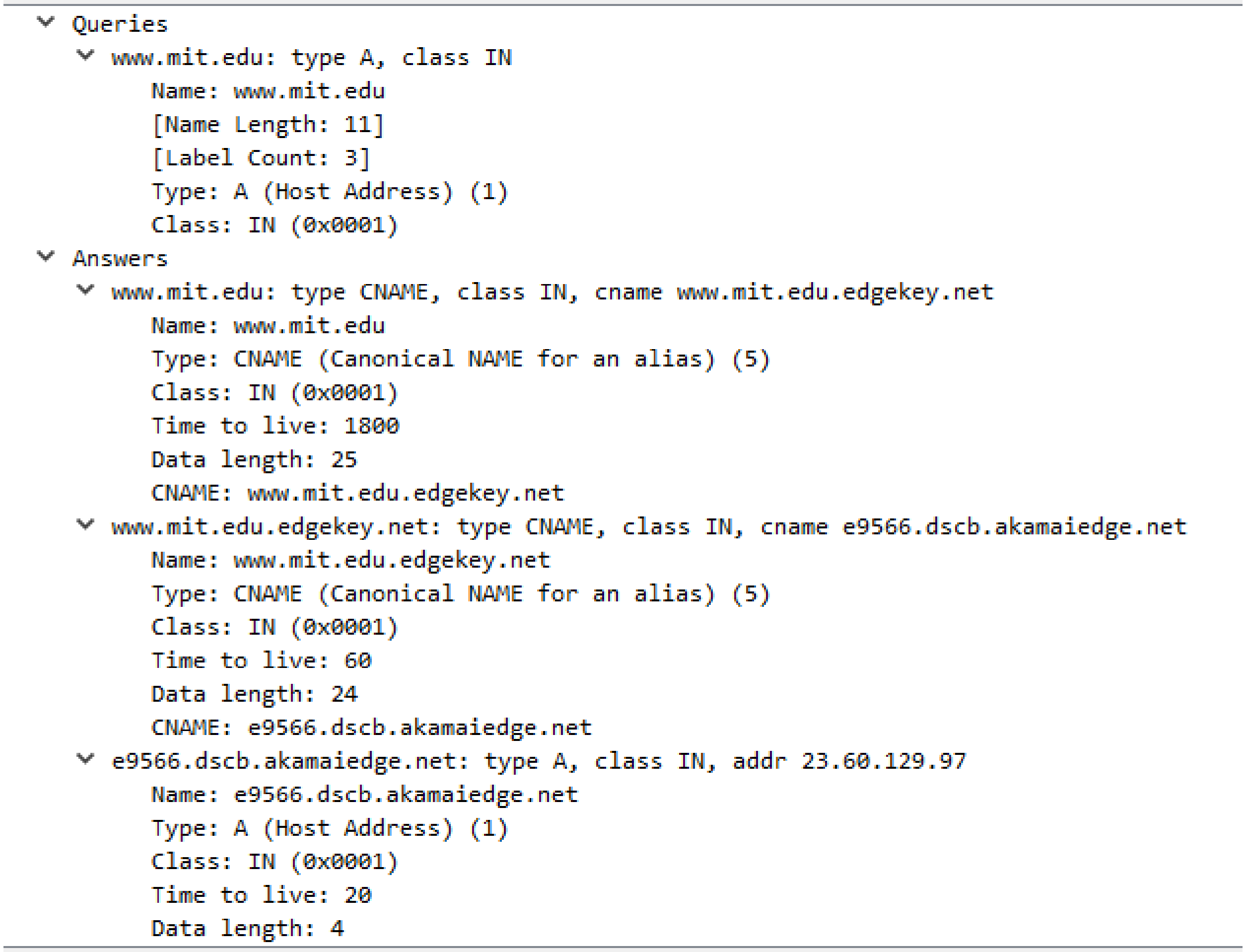
The query message was of type A, and did not contain any answers.



```
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: 90]
```

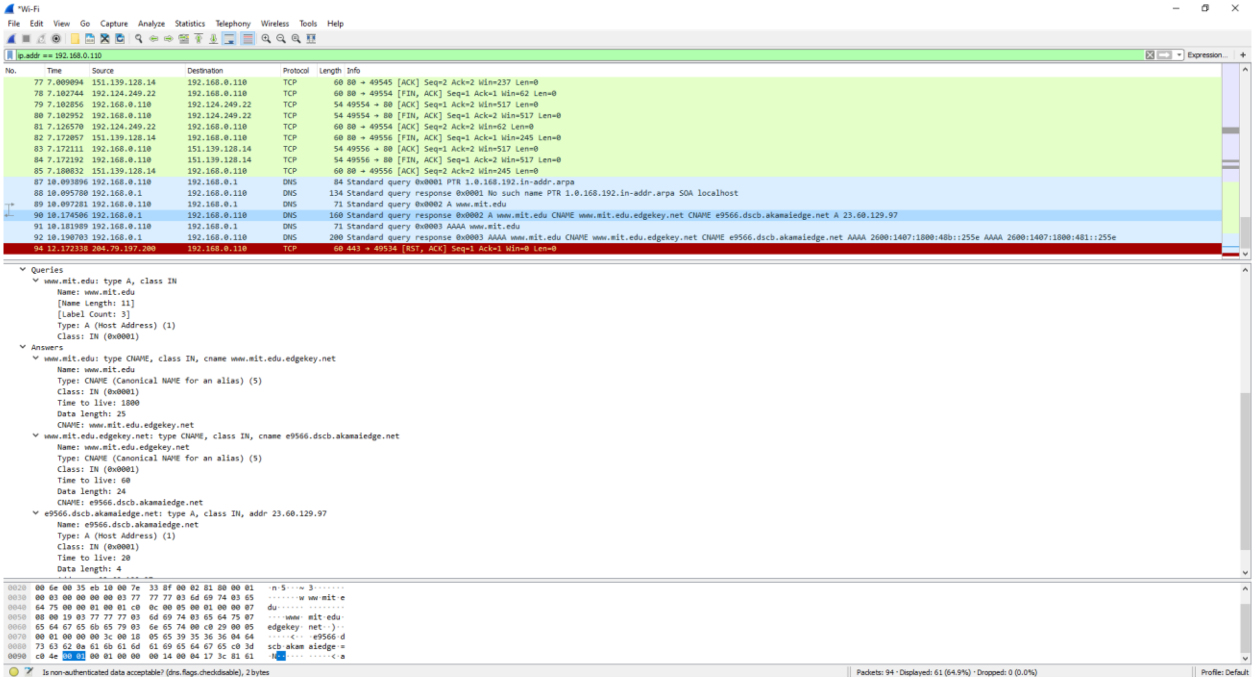
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

In the response query message sent by www.mit.edu, there were 3 answers provided. In these answers, we see information on 3 different servers and records associated with them. It included the IP address of the server, type, name, class etc.



```
⌄ Queries
  ⌄ 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)
⌄ Answers
  ⌄ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ⌄ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ⌄ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.60.129.97
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
```

15. Provide a screenshot


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

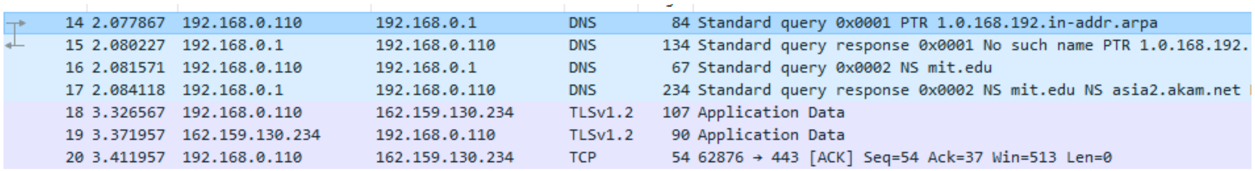
```
ip.addr == 192.168.0.110

No.  Time      Source          Destination     Protocol Length Info
  77 7.009094  151.139.128.14  192.168.0.110   TCP       60 80 → 49545 [ACK] Seq=2 Ack=2 Win=237 Len=0
  78 7.102744  192.124.249.22  192.168.0.110   TCP       60 80 → 49554 [FIN, ACK] Seq=1 Ack=1 Win=62 Len=0
  79 7.102856  192.168.0.110   192.124.249.22  TCP       54 49554 → 80 [ACK] Seq=1 Ack=2 Win=517 Len=0
  80 7.102952  192.168.0.110   192.124.249.22  TCP       54 49554 → 80 [FIN, ACK] Seq=1 Ack=2 Win=517 Len=0
  81 7.126570  192.124.249.22  192.168.0.110   TCP       60 80 → 49554 [ACK] Seq=2 Ack=2 Win=62 Len=0
  82 7.172057  151.139.128.14  192.168.0.110   TCP       60 80 → 49556 [FIN, ACK] Seq=1 Ack=1 Win=245 Len=0
  83 7.172111  192.168.0.110   151.139.128.14  TCP       54 49556 → 80 [ACK] Seq=1 Ack=2 Win=517 Len=0
  84 7.172192  192.168.0.110   151.139.128.14  TCP       54 49556 → 80 [FIN, ACK] Seq=1 Ack=2 Win=517 Len=0
  85 7.180832  151.139.128.14  192.168.0.110   TCP       60 80 → 49556 [ACK] Seq=2 Ack=2 Win=245 Len=0
  87 10.093896 192.168.0.110   192.168.0.1     DNS       84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
  88 10.095780 192.168.0.1     192.168.0.110   DNS      134 Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost
  89 10.097281 192.168.0.110   192.168.0.1     DNS       71 Standard query 0x0002 A www.mit.edu
  90 10.174506 192.168.0.1     192.168.0.110   DNS      160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.60.129.97
  91 10.181989 192.168.0.110   192.168.0.1     DNS       71 Standard query 0x0003 AAAA www.mit.edu
  92 10.190703 192.168.0.1     192.168.0.110   DNS      200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1407:1800:48b::255e AAAA 2600:1407:1800:481::255e
  94 12.172338 204.79.197.200  192.168.0.110   TCP       60 443 → 49534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
  ˅ Queries
    ˅ 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)
  ˅ Answers
    ˅ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1800
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    ˅ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    ˅ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.60.129.97
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20
        Data length: 4
```

```
0020  00 6e 00 35 eb 10 00 7e  33 8f 00 02 81 80 00 01   ·n·5···~ 3·······
0030  00 03 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 c0  0c 00 05 00 01 00 00 07   du······ ········
0050  08 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ····www· mit·edu·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey· net··)··
0070  00 01 00 00 00 3c 00 18  05 65 39 35 36 36 04 64   ·····<·· ·e9566·d
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 c0 3d   scb·akam aiedge·=
0090  c0 4e 00 01 00 01 00 00  00 14 00 04 17 3c 81 61   ·N······ ·····<·a
```

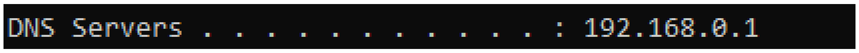
```
Is non-authenticated data acceptable? (dns.flags.checkdisable), 2 bytes     Packets: 94 · Displayed: 61 (64.9%) · Dropped: 0 (0.0%)     Profile: Default
```

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



```
14 2.077867  192.168.0.110   192.168.0.1      DNS       84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
15 2.080227  192.168.0.1     192.168.0.110    DNS      134 Standard query response 0x0001 No such name PTR 1.0.168.192.
16 2.081571  192.168.0.110   192.168.0.1      DNS       67 Standard query 0x0002 NS mit.edu
17 2.084118  192.168.0.1     192.168.0.110    DNS      234 Standard query response 0x0002 NS mit.edu NS asia2.akam.net
18 3.326567  192.168.0.110   162.159.130.234  TLSv1.2  107 Application Data
19 3.371957  162.159.130.234 192.168.0.110    TLSv1.2   90 Application Data
20 3.411957  192.168.0.110   162.159.130.234  TCP       54 62876 → 443 [ACK] Seq=54 Ack=37 Win=513 Len=0
```

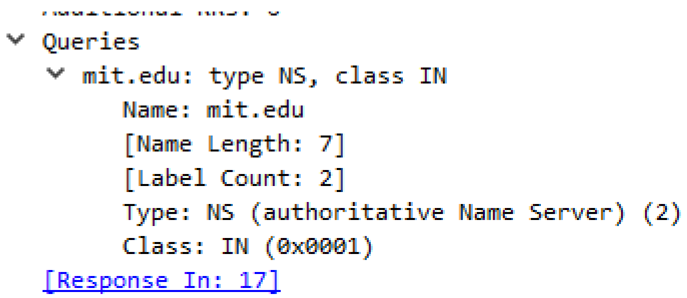
The IP address that the DNS query message is sent to is 192.168.0.1. This is the IP address of my local DNS server.



```
DNS Servers . . . . . . . . . . . : 192.168.0.1
```

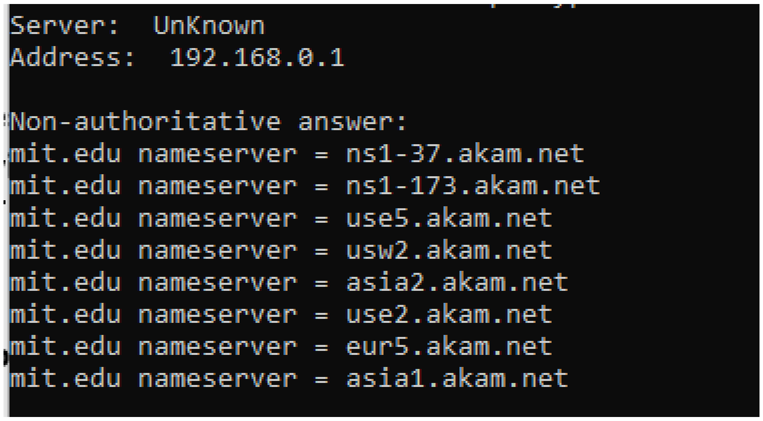
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The DNS query message is of type NS. It contains only 1 question, but no answers.



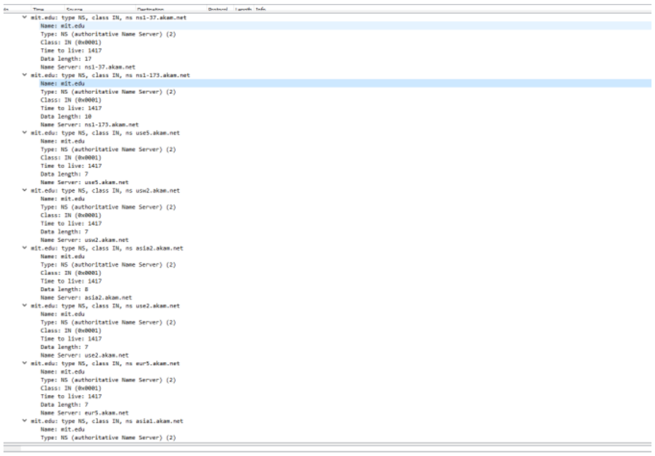
```
v Queries
  v mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
  [Response In: 17]
```

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?



```
Server:  UnKnown
Address:  192.168.0.1

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

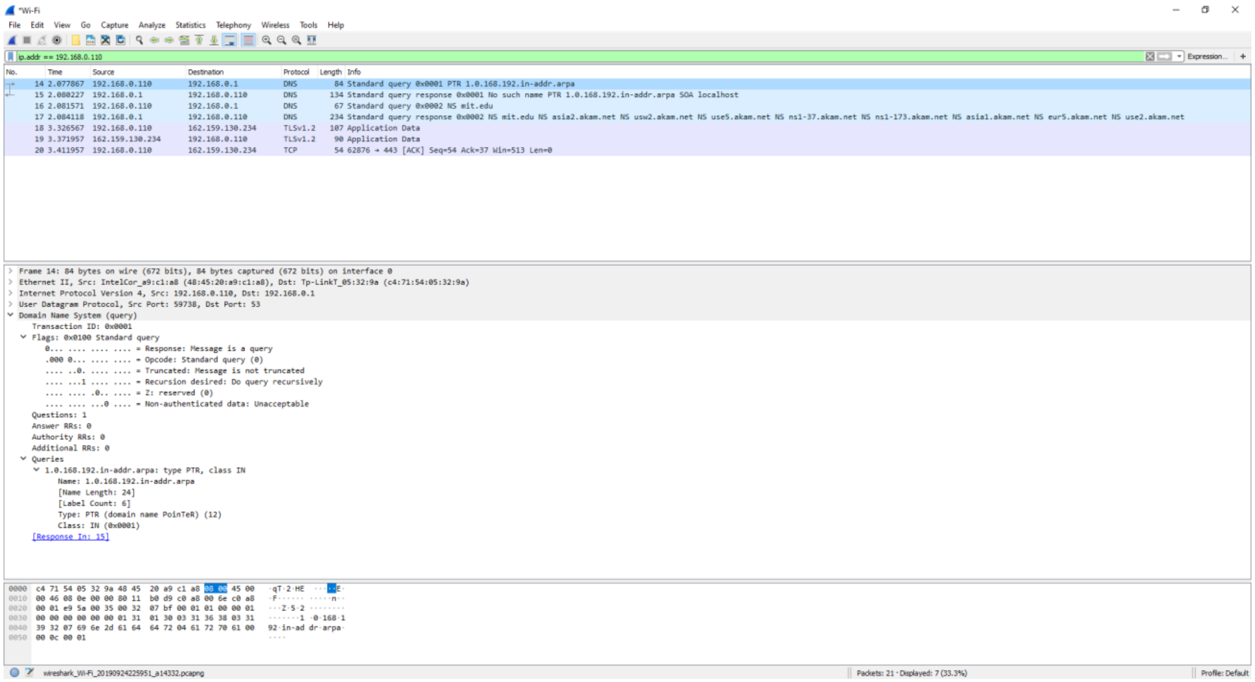
In the answer, there are 8 nameservers.



```
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: 1417
    Data length: 17
    Name Server: ns1-37.akam.net
v mit.edu: type NS, class IN, ns ns1-173.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1417
    Data length: 10
    Name Server: ns1-173.akam.net
v mit.edu: type NS, class IN, ns use5.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1417
    Data length: 7
    Name Server: use5.akam.net
v mit.edu: type NS, class IN, ns usw2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1417
    Data length: 7
    Name Server: usw2.akam.net
v mit.edu: type NS, class IN, ns asia2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1417
    Data length: 8
    Name Server: asia2.akam.net
v mit.edu: type NS, class IN, ns use2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1417
    Data length: 7
    Name Server: use2.akam.net
v mit.edu: type NS, class IN, ns eur5.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1417
    Data length: 7
    Name Server: eur5.akam.net
v mit.edu: type NS, class IN, ns asia1.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
```

As shown above, these messages did not provide the IP addresses of the servers.

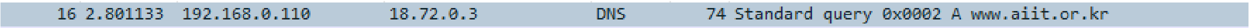
19. Provide a screenshot.


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

```
ip.addr == 192.168.0.110

No.   Time      Source           Destination      Protocol Length Info
   14 2.077867  192.168.0.110    192.168.0.1      DNS        84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
   15 2.080227  192.168.0.1      192.168.0.110    DNS       134 Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost
   16 2.081571  192.168.0.110    192.168.0.1      DNS        67 Standard query 0x0002 NS mit.edu
   17 2.084118  192.168.0.1      192.168.0.110    DNS       234 Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS usw2.akam.net NS use5.akam.net NS ns1-37.akam.net NS ns1-173.akam.net NS asia1.akam.net NS eur5.akam.net NS use2.akam.net
   18 3.326567  192.168.0.110    162.159.130.234  TLSv1.2   107 Application Data
   19 3.371957  162.159.130.234  192.168.0.110    TLSv1.2    90 Application Data
   20 3.411957  192.168.0.110    162.159.130.234  TCP        54 62876 → 443 [ACK] Seq=54 Ack=37 Win=513 Len=0

> Frame 14: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 59738, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  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 1.0.168.192.in-addr.arpa: type PTR, class IN
        Name: 1.0.168.192.in-addr.arpa
        [Name Length: 24]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
    [Response In: 15]

0000  c4 71 54 05 32 9a 48 45  20 a9 c1 a8 08 00 45 00   ·qT·2·HE ······E·
0010  00 46 08 0e 00 00 80 11  b0 d9 c0 a8 00 6e c0 a8   ·F······ ·····n··
0020  00 01 e9 5a 00 35 00 32  07 bf 00 01 01 00 00 01   ···Z·5·2 ········
0030  00 00 00 00 00 00 01 31  01 30 03 31 36 38 03 31   ·······1 ·0·168·1
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   92·in-ad dr·arpa·
0050  00 0c 00 01                                        ····

wireshark_Wi-Fi_20190924225951_a14332.pcapng    Packets: 21 · Displayed: 7 (33.3%)    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?

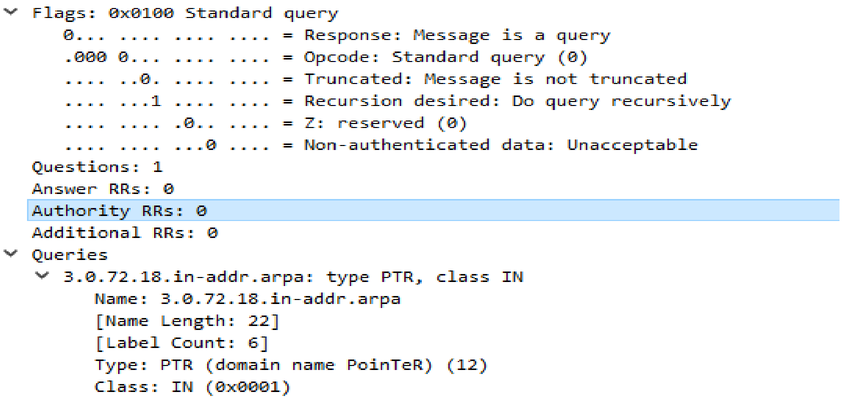
The IP address that the DNS query message sent to was 18.72.0.3, which is the destination IP for www.aiit.or.kr. This is not the IP address of the default local DNS server, it is the DNS server for the website states above.



```
   16 2.801133  192.168.0.110       18.72.0.3          DNS        74 Standard query 0x0002 A www.aiit.or.kr
```

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

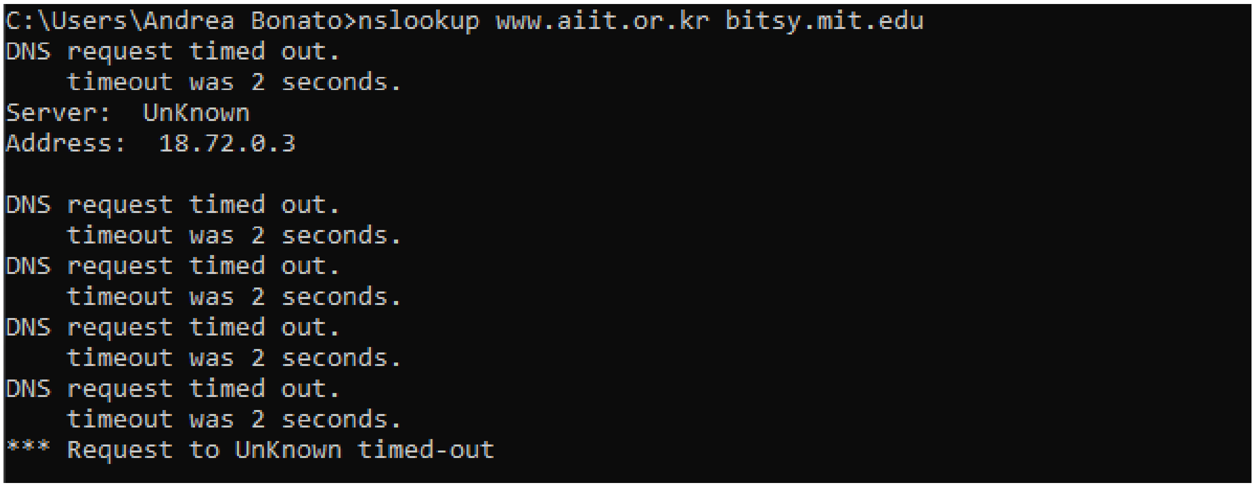
The DNS query message is of type PTR. It contains 1 question and 0 answers.



```
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 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)
```

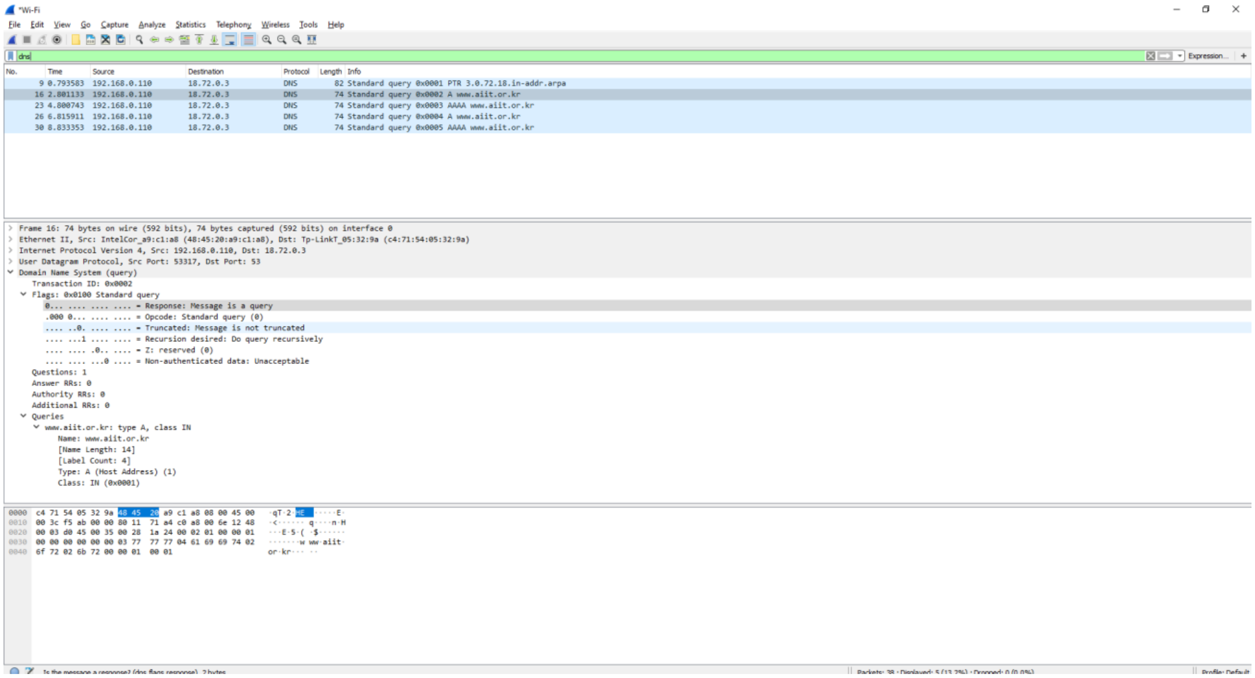
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

There were no response messages that were sent out, thus there were no answers.



```
C:\Users\Andrea Bonato>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.72.0.3

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
```

23. Provide a screenshot.



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

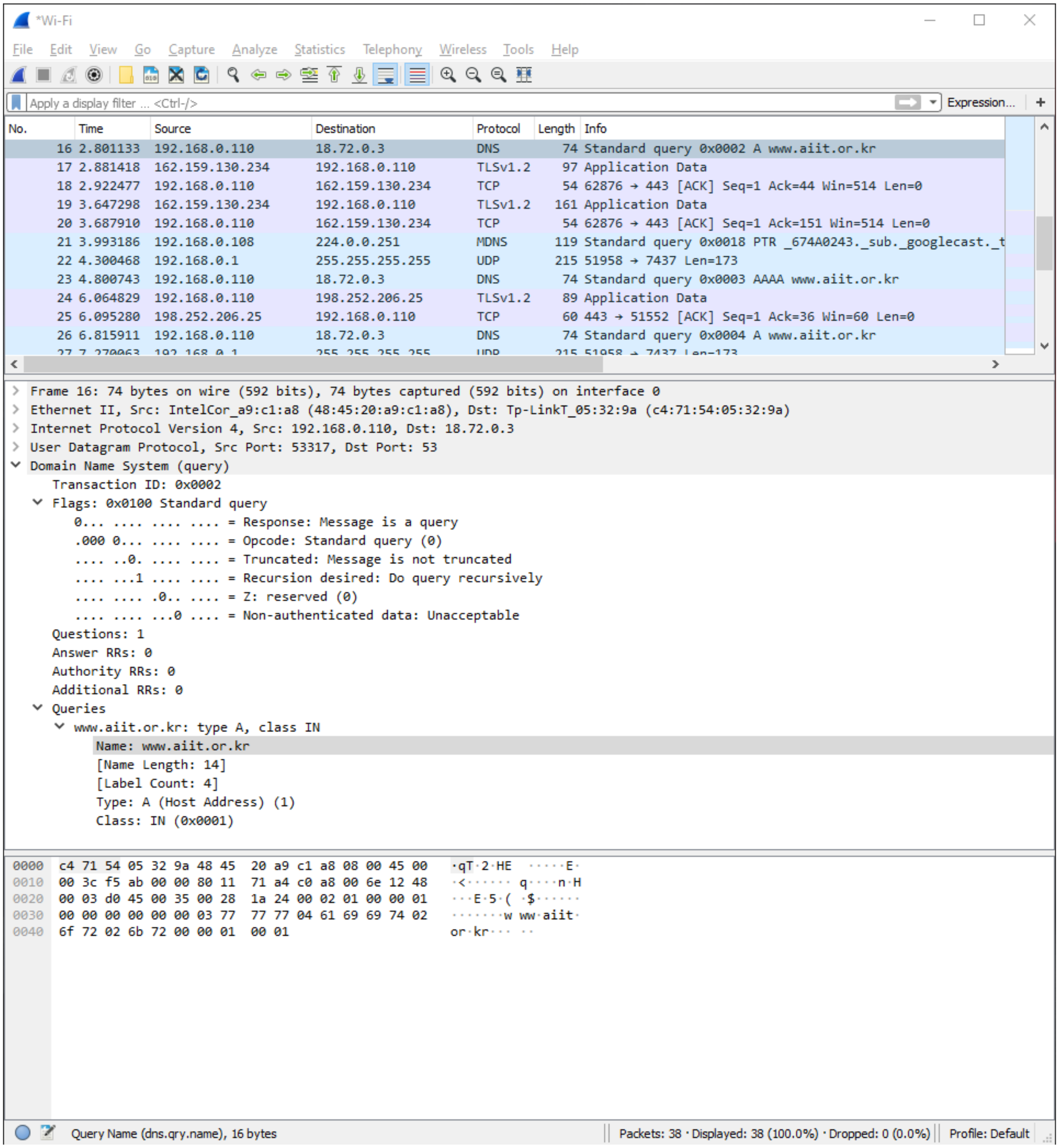
dns

```
No.  Time       Source          Destination  Protocol Length Info
   9 0.793583   192.168.0.110   18.72.0.3    DNS      82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
  16 2.801133   192.168.0.110   18.72.0.3    DNS      74 Standard query 0x0002 A www.aiit.or.kr
  23 4.800743   192.168.0.110   18.72.0.3    DNS      74 Standard query 0x0003 AAAA www.aiit.or.kr
  26 6.815911   192.168.0.110   18.72.0.3    DNS      74 Standard query 0x0004 A www.aiit.or.kr
  30 8.833353   192.168.0.110   18.72.0.3    DNS      74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
> Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 53317, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  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.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)
```

```
0000  c4 71 54 05 32 9a 48 45  20 a9 c1 a8 08 00 45 00   ·qT·2·HE ·····E·
0010  00 3c f5 ab 00 00 80 11  71 a4 c0 a8 00 6e 12 48   ·<······ q····n·H
0020  00 03 d0 45 00 35 00 28  1a 24 00 02 01 00 00 01   ···E·5·( ·$······
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   ·······w ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01                     or·kr··· ··
```

Is the message a response? (dns.flags.response), 2 bytes   Packets: 38 · Displayed: 5 (13.2%) · Dropped: 0 (0.0%)   Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.    Time      Source           Destination      Protocol Length Info
    16 2.801133  192.168.0.110    18.72.0.3        DNS       74 Standard query 0x0002 A www.aiit.or.kr
    17 2.881418  162.159.130.234  192.168.0.110    TLSv1.2   97 Application Data
    18 2.922477  192.168.0.110    162.159.130.234  TCP       54 62876 → 443 [ACK] Seq=1 Ack=44 Win=514 Len=0
    19 3.647298  162.159.130.234  192.168.0.110    TLSv1.2  161 Application Data
    20 3.687910  192.168.0.110    162.159.130.234  TCP       54 62876 → 443 [ACK] Seq=1 Ack=151 Win=514 Len=0
    21 3.993186  192.168.0.108    224.0.0.251      MDNS     119 Standard query 0x0018 PTR _674A0243._sub._googlecast._t
    22 4.300468  192.168.0.1      255.255.255.255  UDP      215 51958 → 7437 Len=173
    23 4.800743  192.168.0.110    18.72.0.3        DNS       74 Standard query 0x0003 AAAA www.aiit.or.kr
    24 6.064829  192.168.0.110    198.252.206.25   TLSv1.2   89 Application Data
    25 6.095280  198.252.206.25   192.168.0.110    TCP       60 443 → 51552 [ACK] Seq=1 Ack=36 Win=60 Len=0
    26 6.815911  192.168.0.110    18.72.0.3        DNS       74 Standard query 0x0004 A www.aiit.or.kr
    27 7.270063  192.168.0.1      255.255.255.255  UDP      215 51958 → 7437 Len=173
```

```
> Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 53317, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  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.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)
```

```
0000  c4 71 54 05 32 9a 48 45  20 a9 c1 a8 08 00 45 00   ·qT·2·HE  ·····E·
0010  00 3c f5 ab 00 00 80 11  71 a4 c0 a8 00 6e 12 48   ·<······  q····n·H
0020  00 03 d0 45 00 35 00 28  1a 24 00 02 01 00 00 01   ···E·5·(  ·$······
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   ·······w  ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01                     or·kr···  ··
```

Query Name (dns.qry.name), 16 bytes | Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%) | Profile: Default