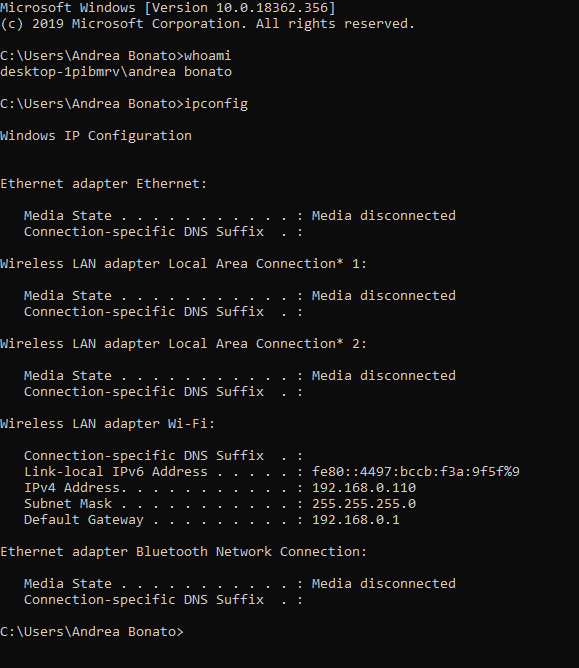
**COMP-3670 FALL 2019 Assignment 1**

**Andrea Bonato**

**104760390**



**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).

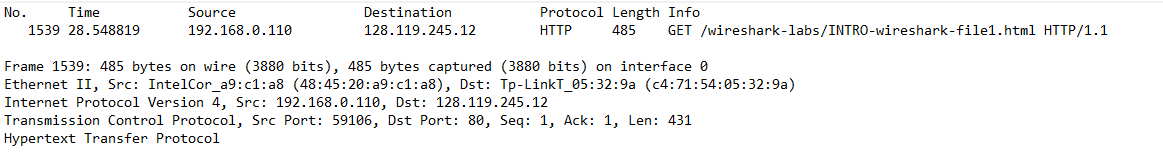
**2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column**

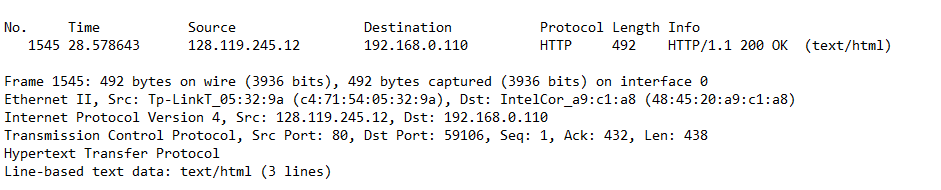
Between the HTTP GET message departure and the HTTP OK arrival, it took 0.029824 seconds. 

**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?**

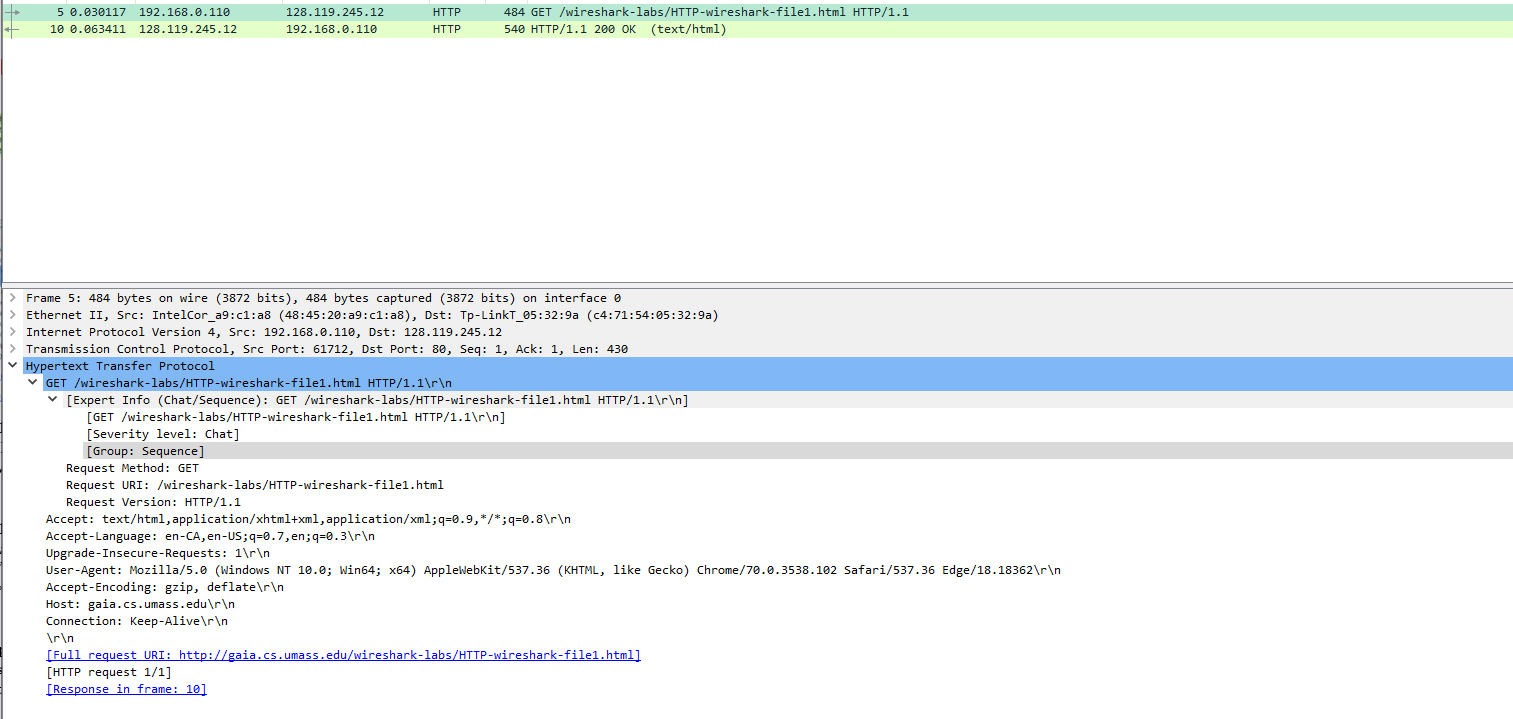
The IP address of my computer is 192.168.0.110 and the gaia.cs.umass.edu server is 128.119.245.12.

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

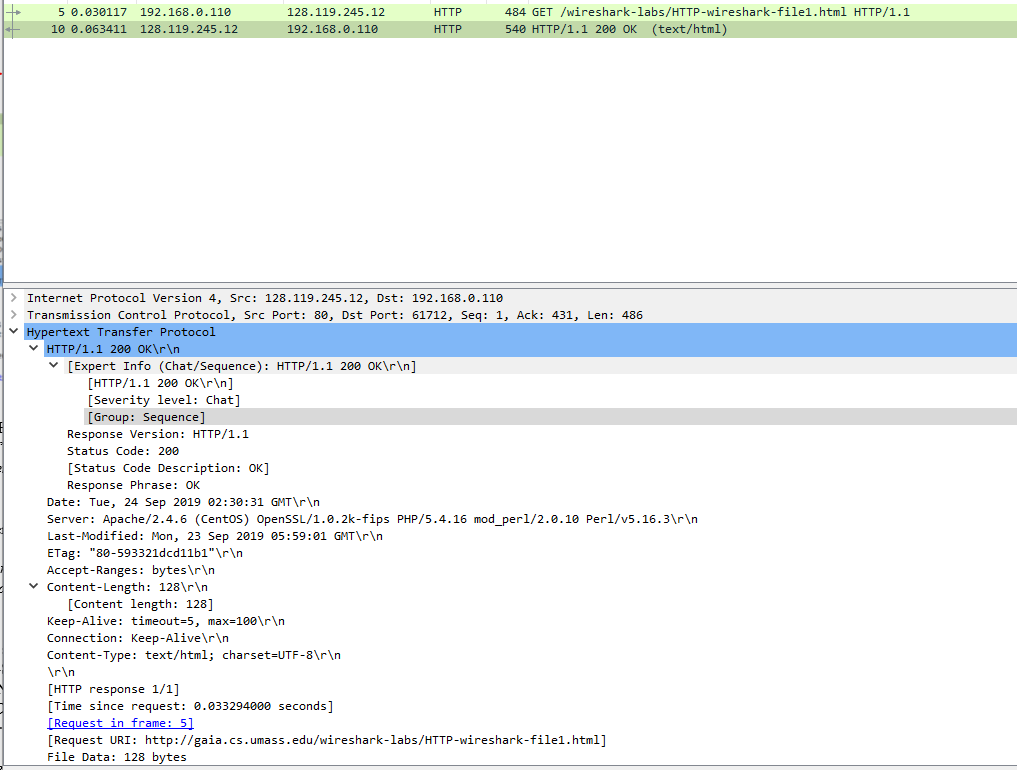
For get: 

For ok: 

**HTTP**



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



**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.

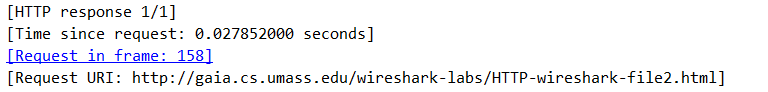
**5. When was the HTML file that you are retrieving last modified at the server?**

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: 

**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. 

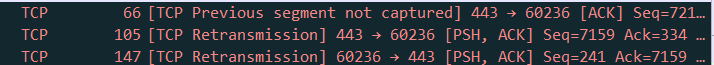
**13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**

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

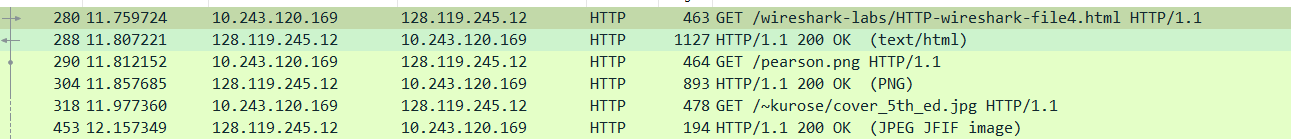
**14. What is the status code and phrase in the response?**

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.

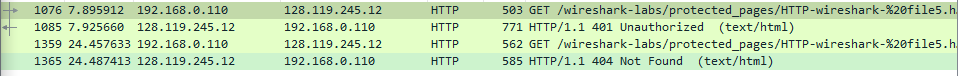
**16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?**

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.

**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.

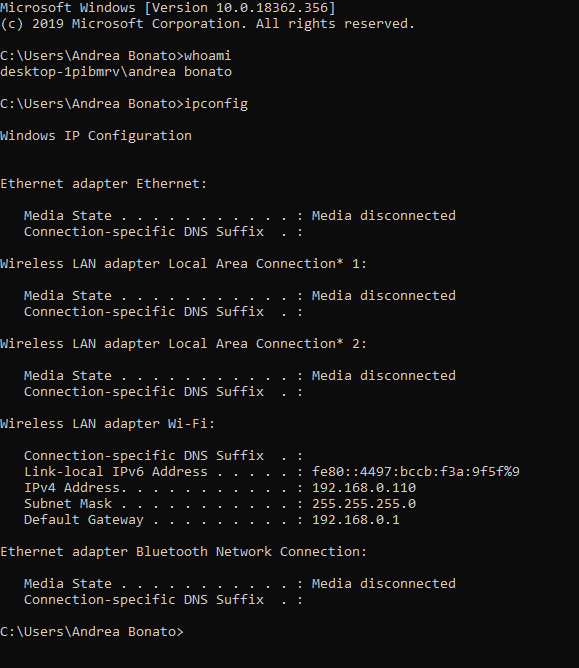
**18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?**

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. 

**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.

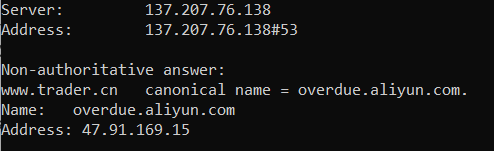
**\*\*NOTE: I did change to my home internet and thus my IP address changed\*\***



**DNS**

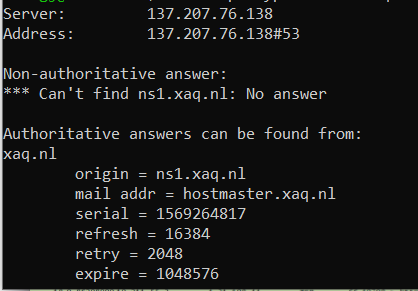
**1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**

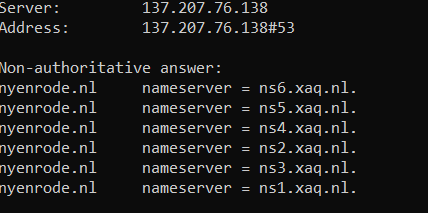
The ip address of the asian web server www.trader.cn is 47.91.169.15. As shown in the following photo.



**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:

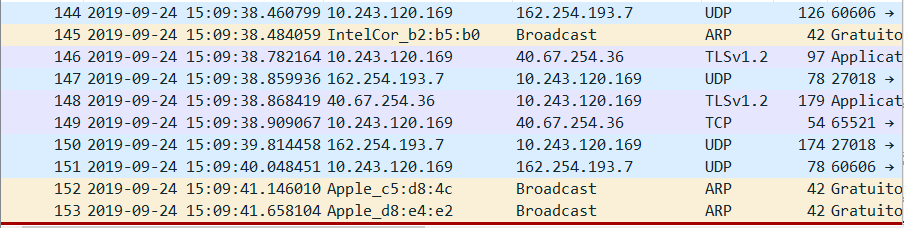




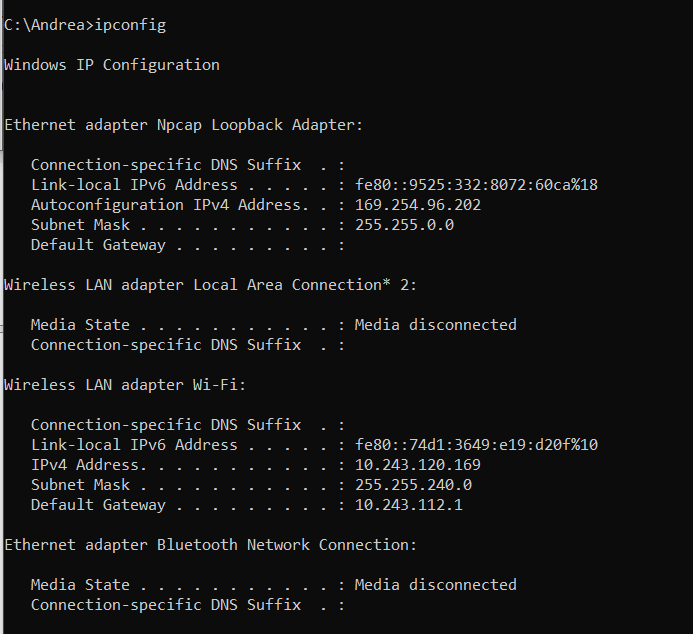
**3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address**

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?**

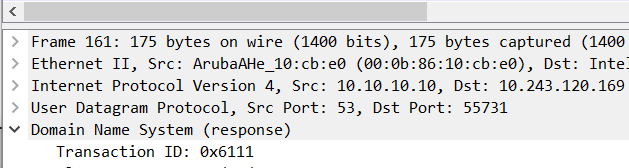
As shown below, these are all standard queries through DNS. The messages themselves were sent over UDP. 

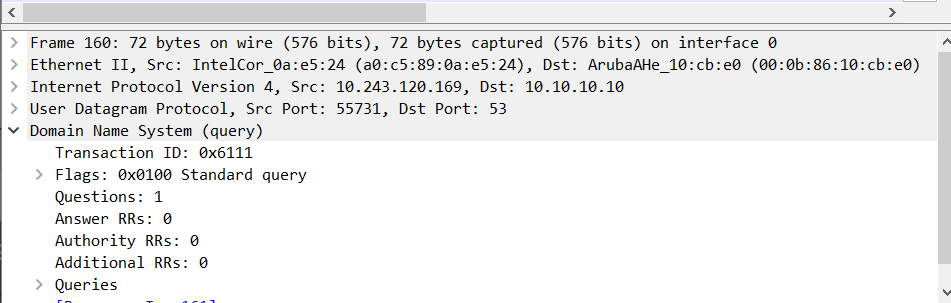
**\*\*NOTE: I did change to the university wifi and thus my IP address changed\*\***



**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.

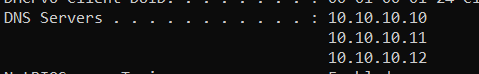




**6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**



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.

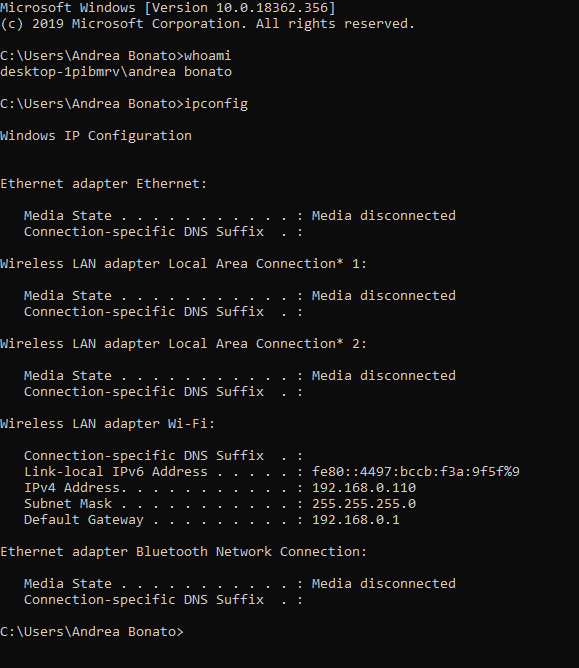


**7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

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

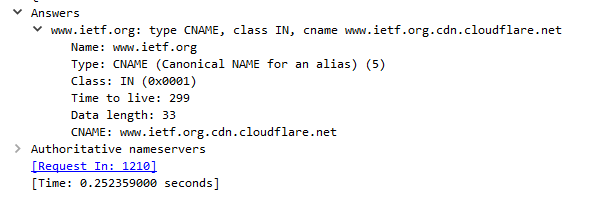


**\*\*NOTE: I did change to my home internet and thus my IP address changed\*\***



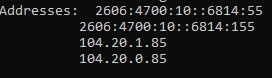
**8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

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.



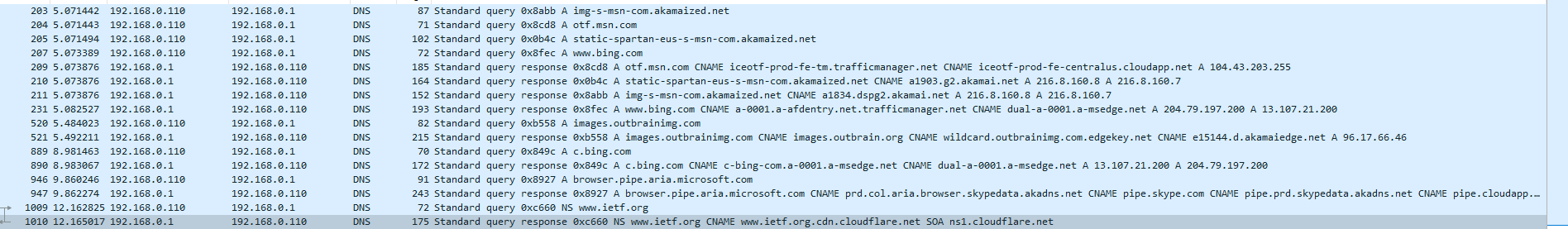
**9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

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

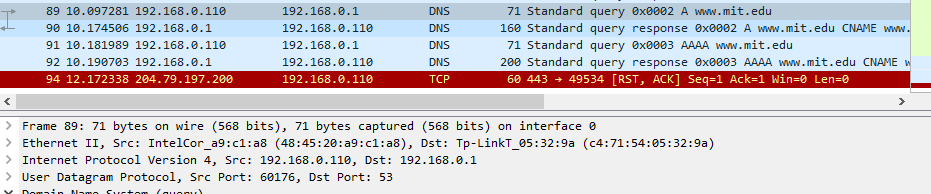


**10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

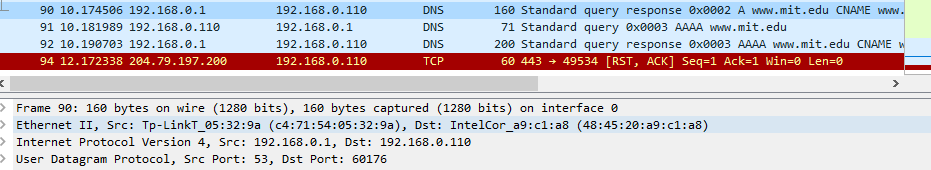
Before the images were retrieved, the host did issue new DNS queries. For each query that related to the image, for example, the image is from another site, it queried that site first.



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



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



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

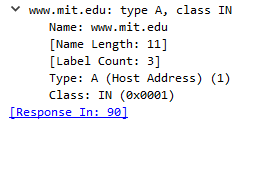
**12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

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.



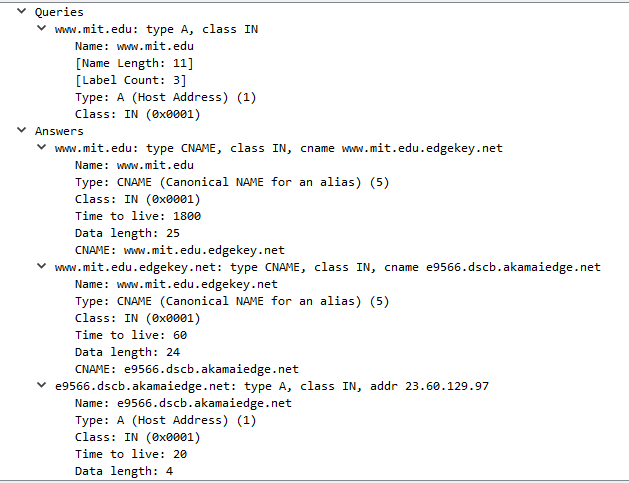
**13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

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

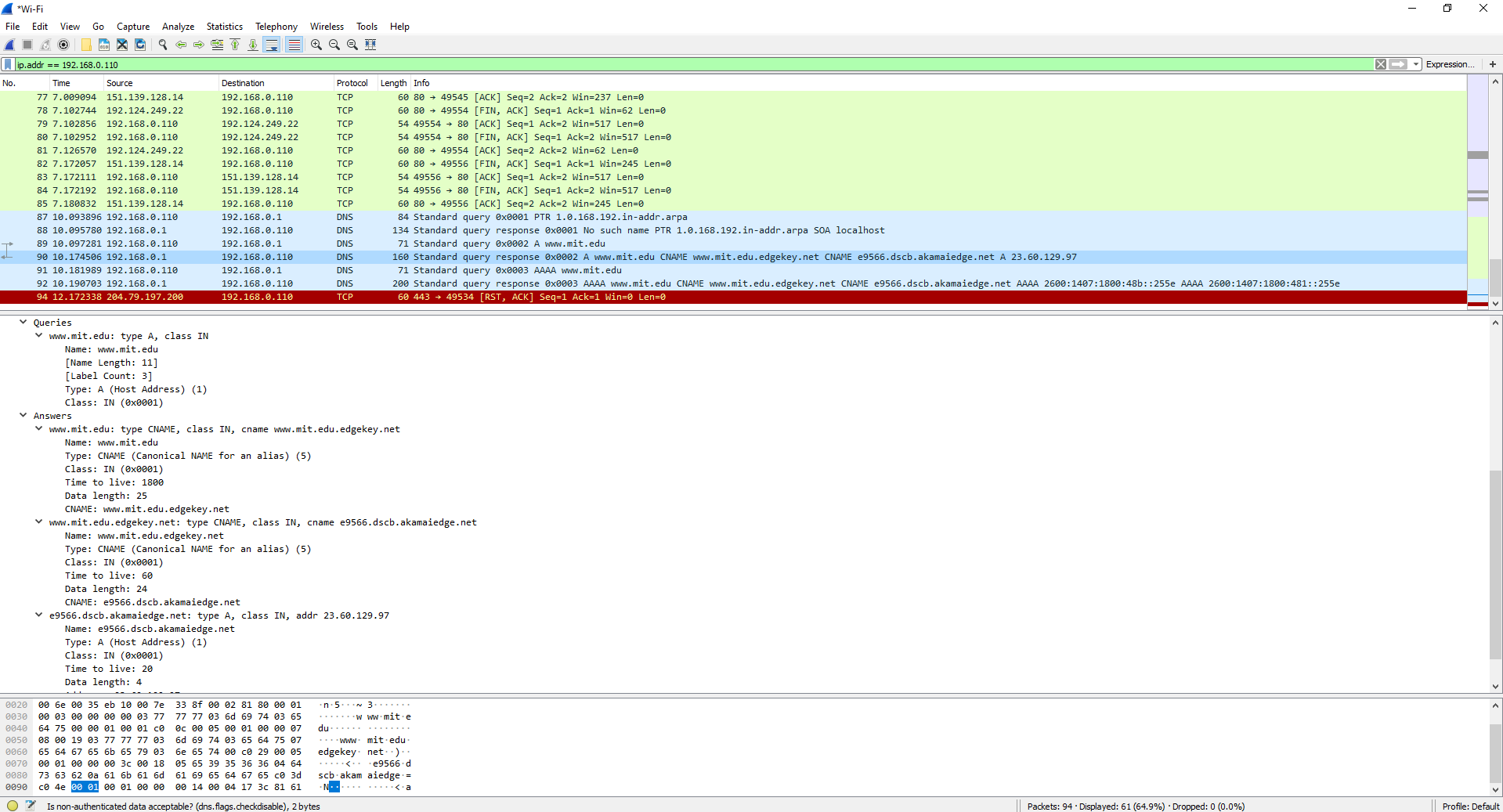


**14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

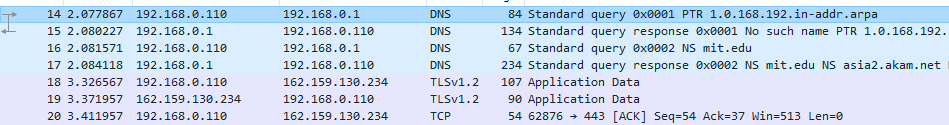
In the response query message sent by [www.mit.edu](http://www.mit.edu), there were 3 answers provided. In these answers, we see information on 3 different servers and records associated with them. It included the IP address of the server, type, name, class etc.



**15. Provide a screenshot**



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

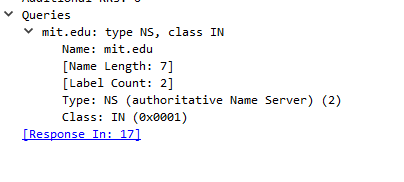


The IP address that the DNS query message is sent to is 192.168.0.1. This is the IP address of my local DNS server.

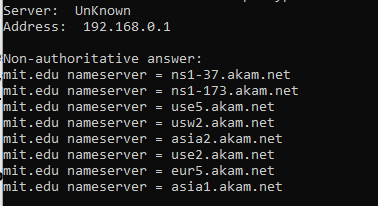


**17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

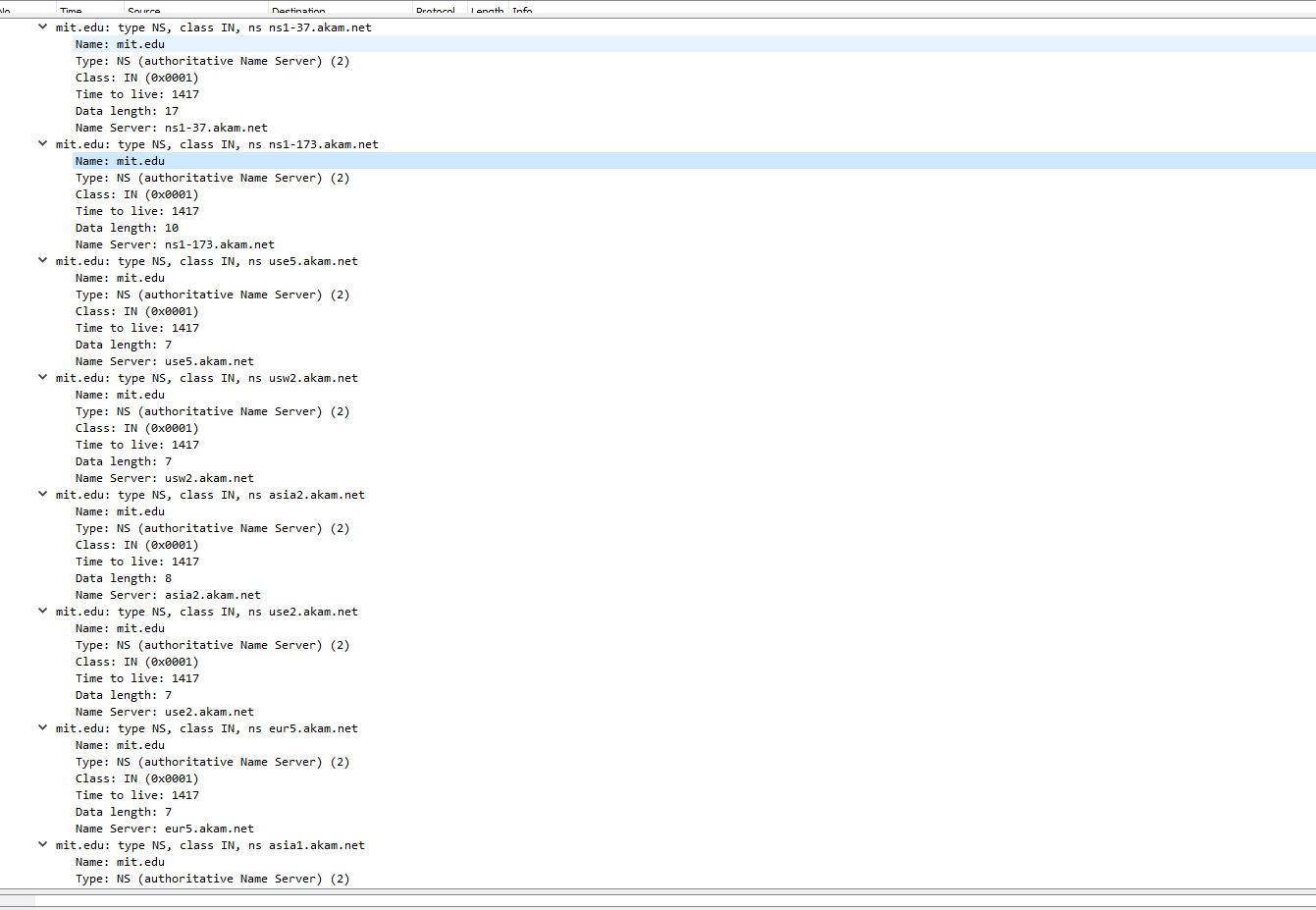
The DNS query message is of type NS. It contains only 1 question, but no answers.



**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?**

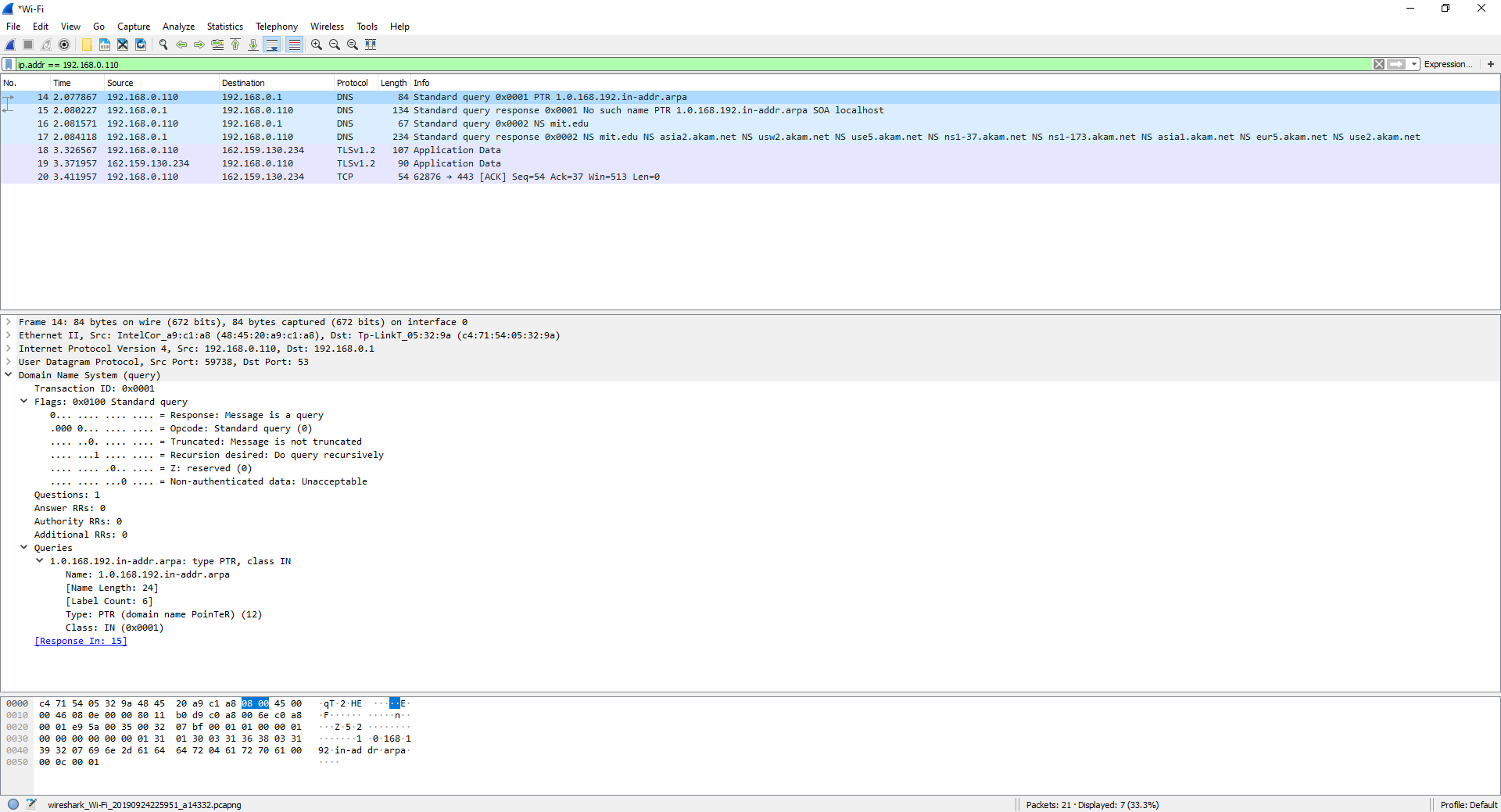


In the answer, there are 8 nameservers.



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

**19. Provide a screenshot.**



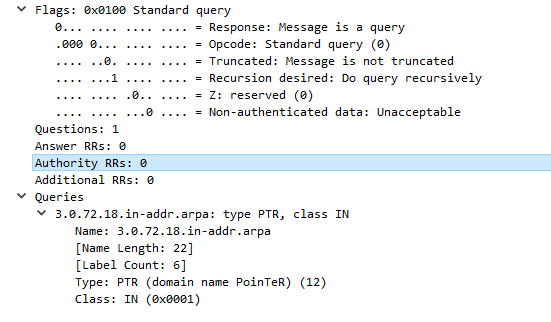
**20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?**

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](http://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.



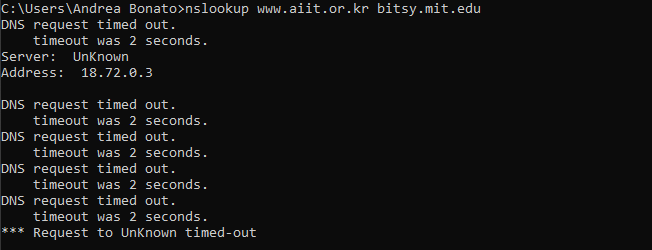
**21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

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



**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.



**23. Provide a screenshot.**

