HAMMAD KHAN MUSAKHEL
21801175

CS472

Wireshark Assignment

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

   MDNS
   ARP
   LLMNR
   UDP
   TCP
   SSDP
   NBNS
   IGMPv2
   TLSv1…
   DNS

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 in the packet- listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

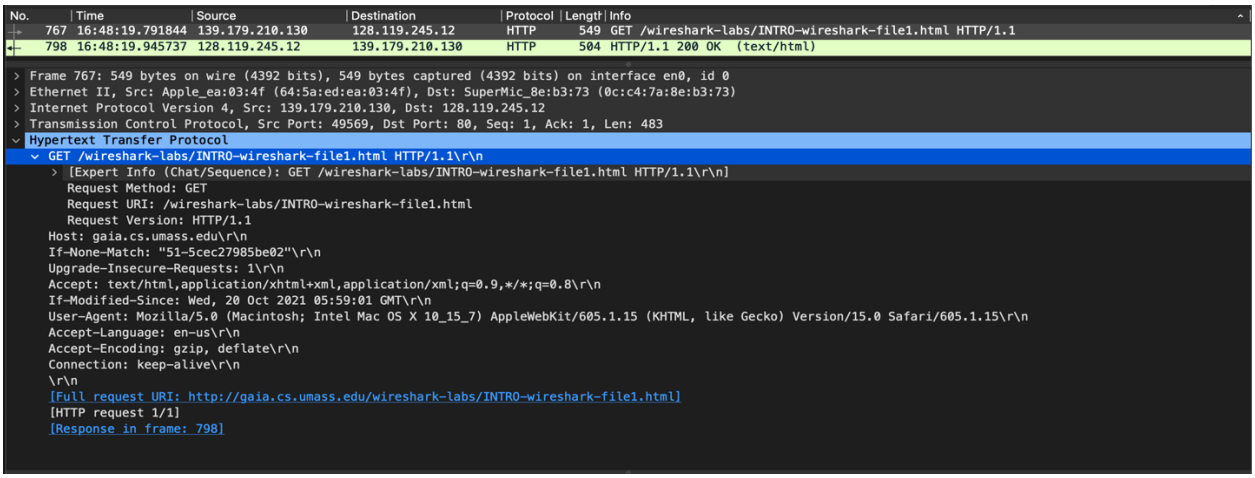
   16:48:19.791844, request sent
   16:48:19.945737, response OK received
   It took 0.153893 seconds to receive the HTTP OK reply.

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?

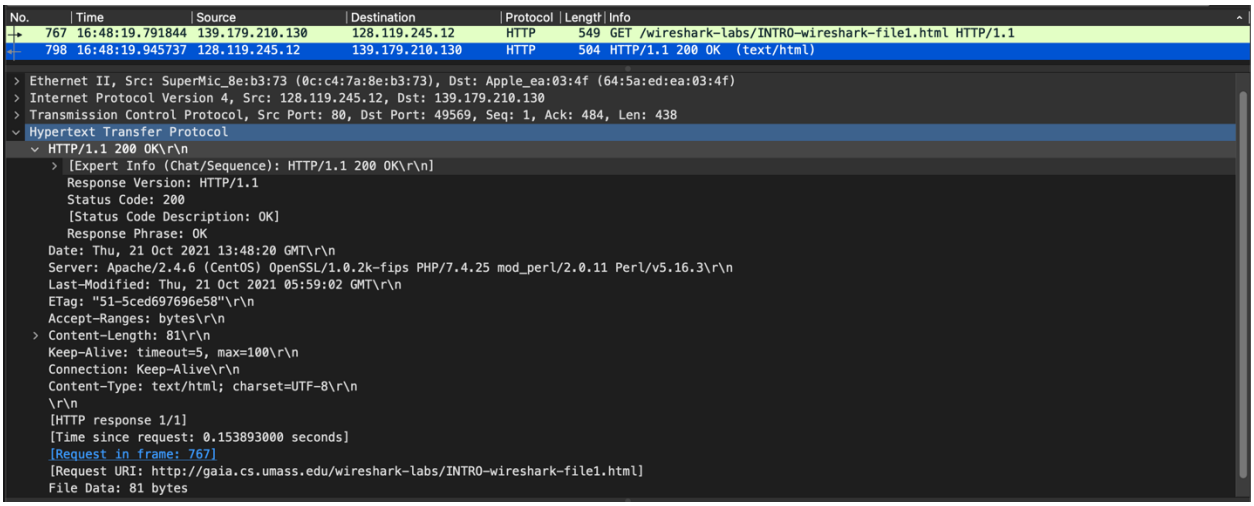
   Internet Address of gaia.cs.umass.edu: 128.119.245.12
   Internet Address of my computer: 139.179.210.130

4. Print the two HTTP messages displayed in step 9 above. To do so, select *Print* from the Wireshark *File* command menu, and select "*Selected Packet Only"* and *"Print as displayed"* and then click OK.

   First HTTP Message (using Screenshot as Print was not working on my PC) below:



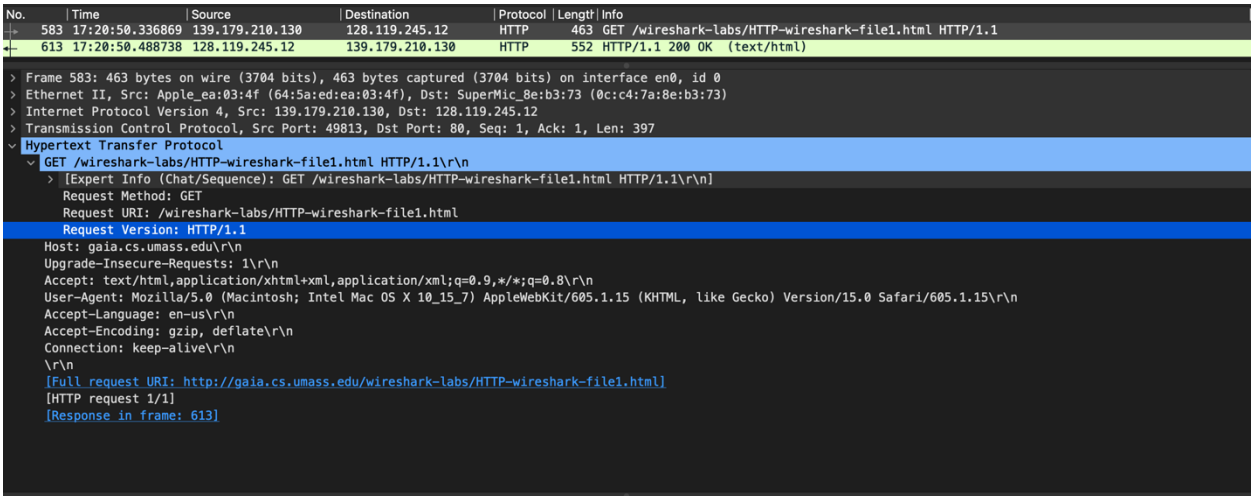
Second HTTP Message (using Screenshot as Print was not working on my PC)



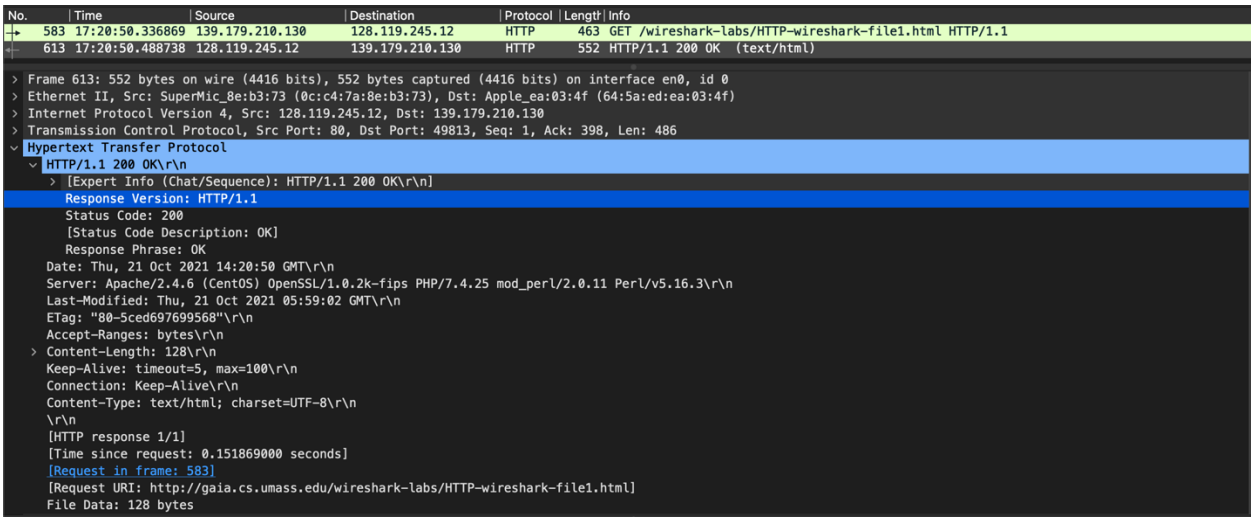
Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction

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

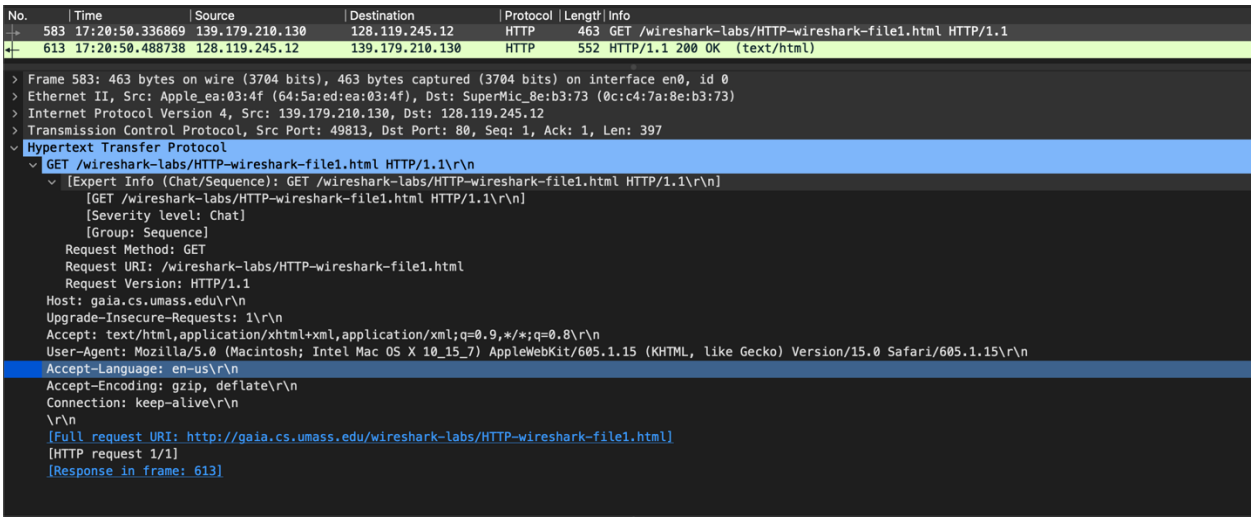


Browser HTTP version

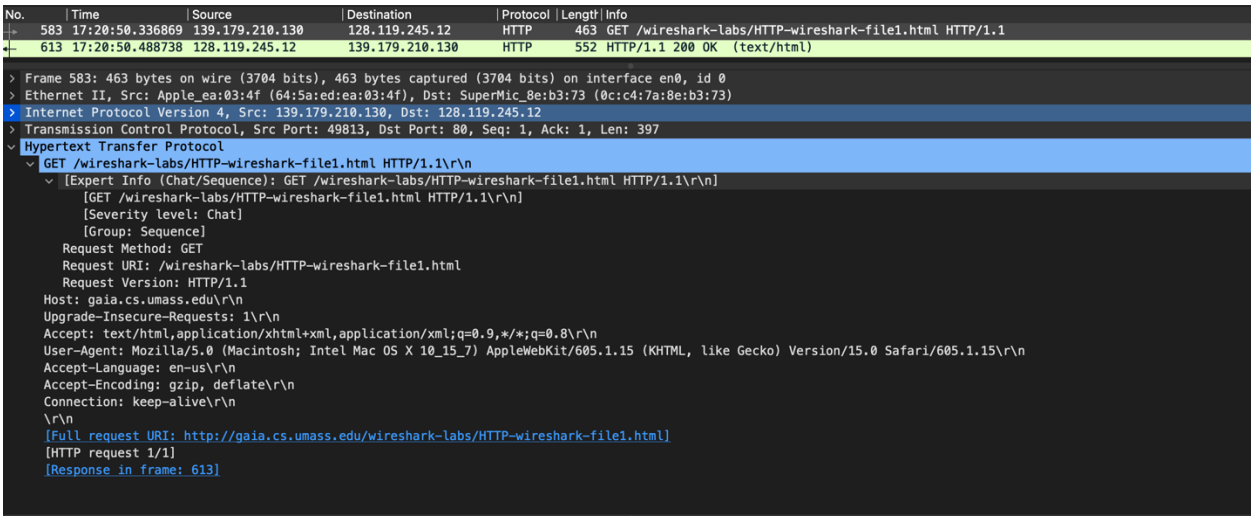


Server HTTP version

2. What languages (if any) does your browser indicate that it can accept to the server?
   My browser indicates it can accept en-us (English – United States):

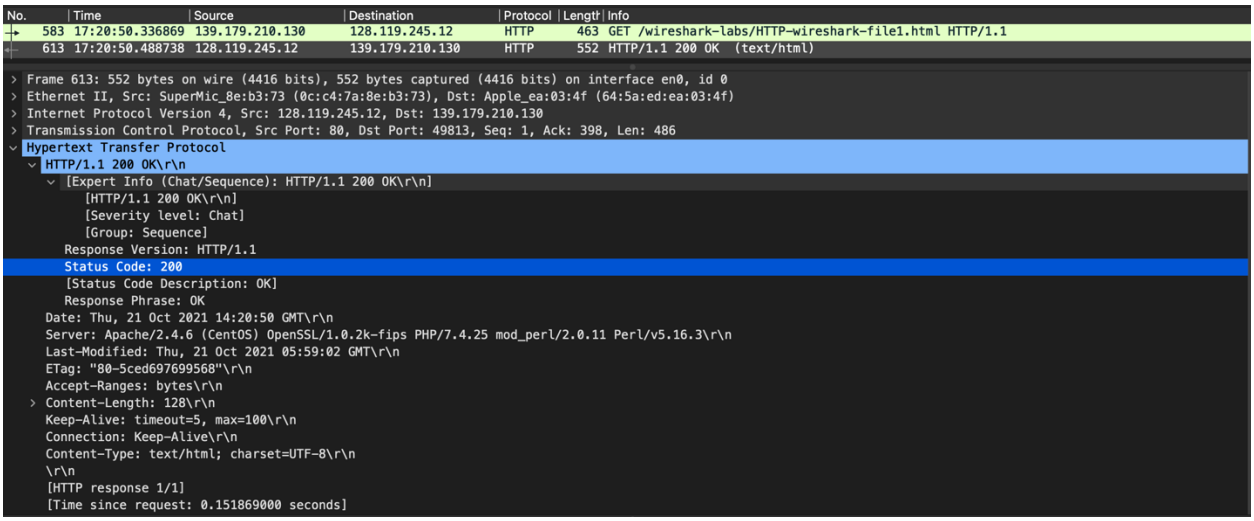


3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   IP Address of gaia.cs.umass.edu: 128.119.245.12
   IP Address of my computer: 139.179.210.130



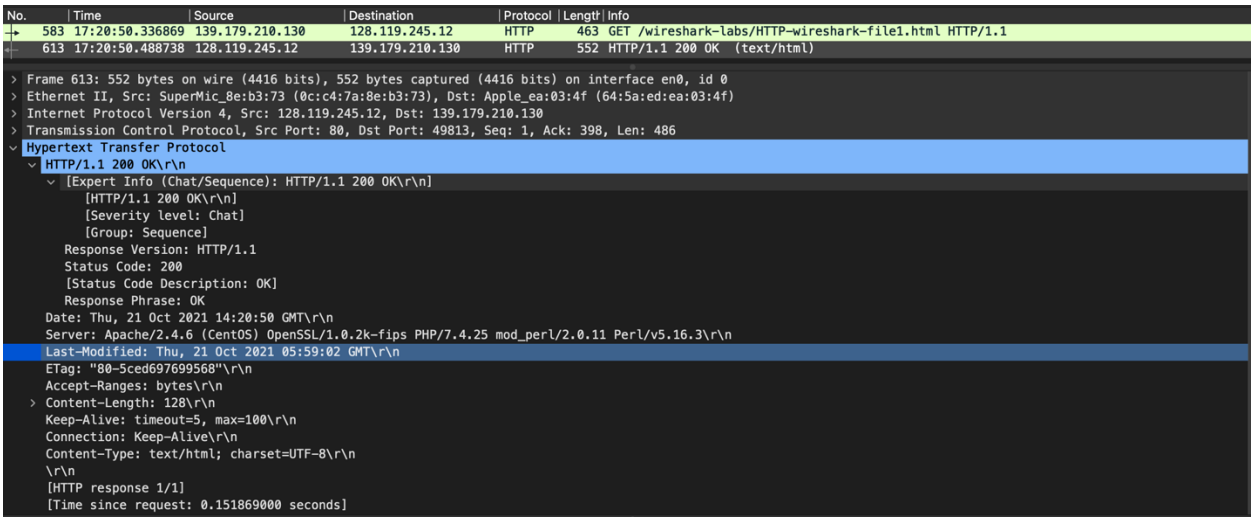
The light blue line indicates from where the information was received.

4. What is the status code returned from the server to your browser?
   Status code return: 200



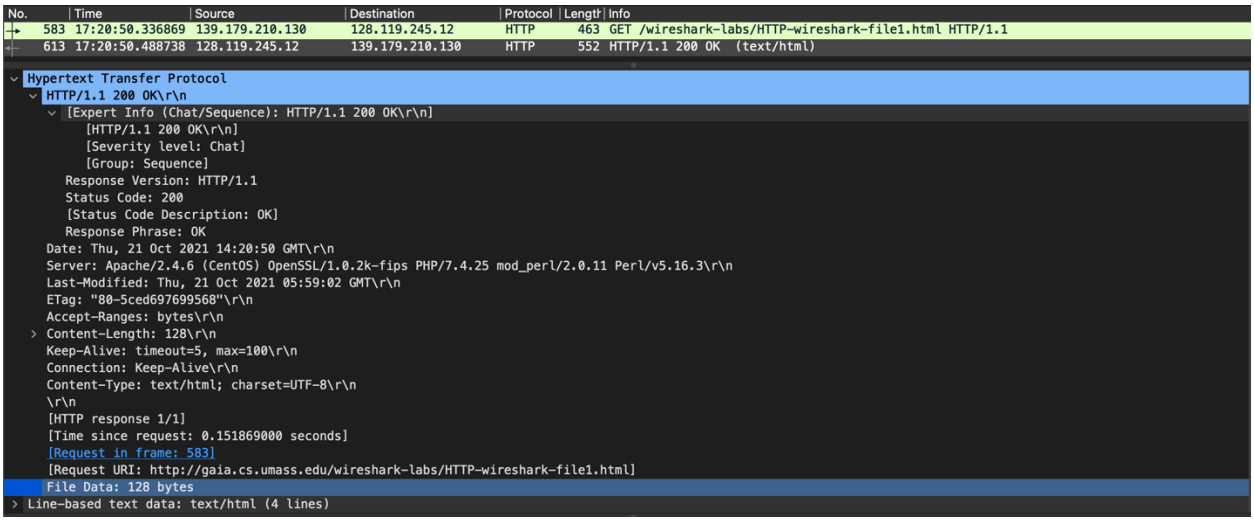
5. When was the HTML file that you are retrieving last modified at the server?

   The HTMP file retrieved was last modified at 21 October 2021, 05:59:02:



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

Bytes received: 128 bytes



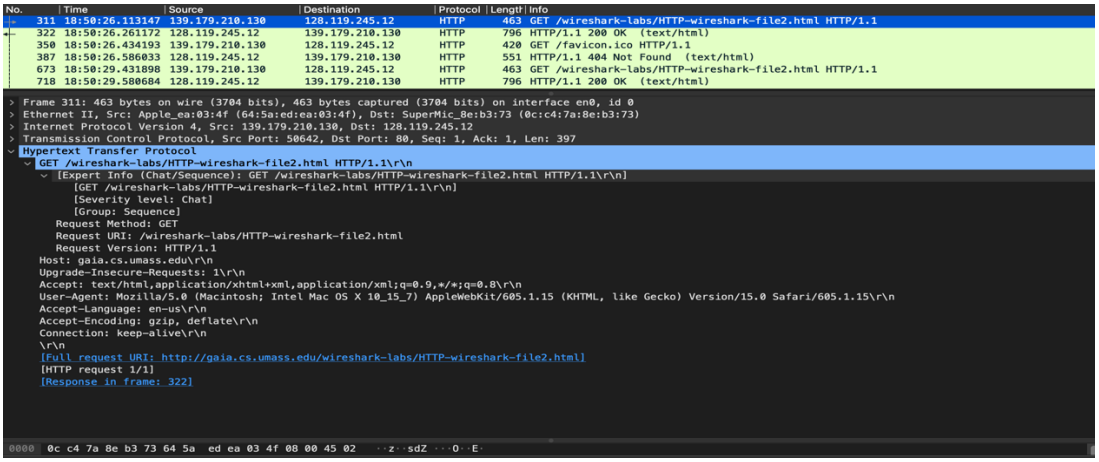
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, all the layers are present in the content window.

2. The HTTP CONDITIONAL GET/response interaction

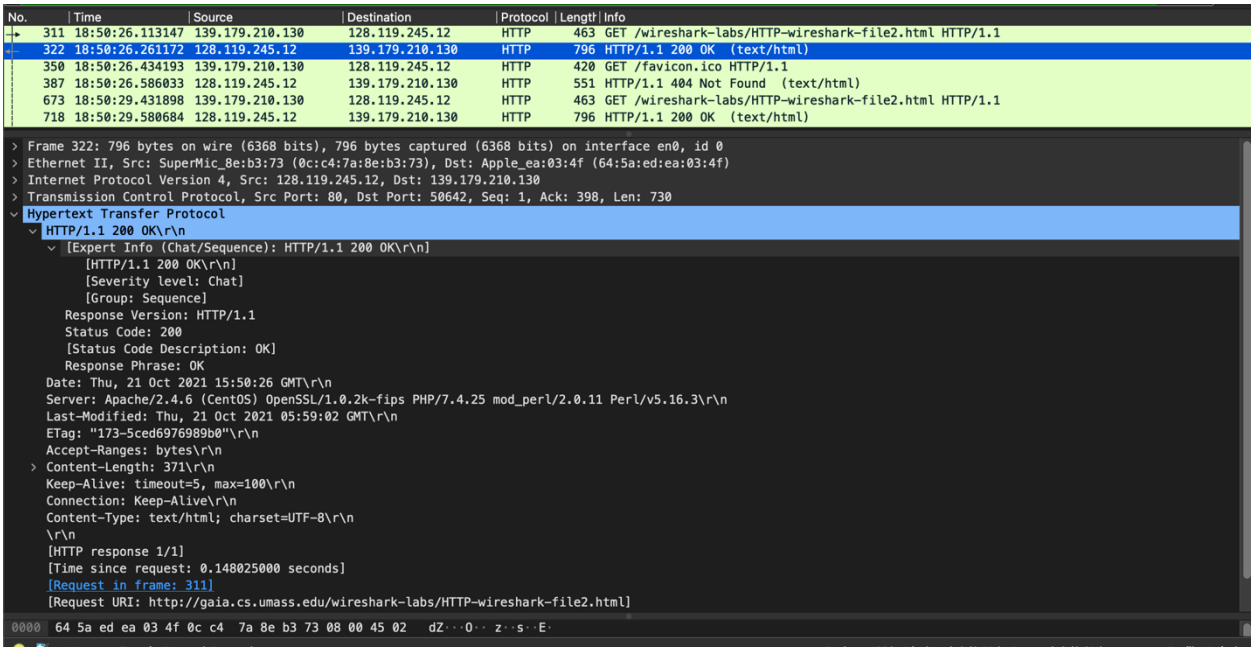
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

   No, I don’t. I can’t figure out where it is. I have assessed the entire content of the request sent from my browser and there’s no “IF-MODIFIED-SINCE.”



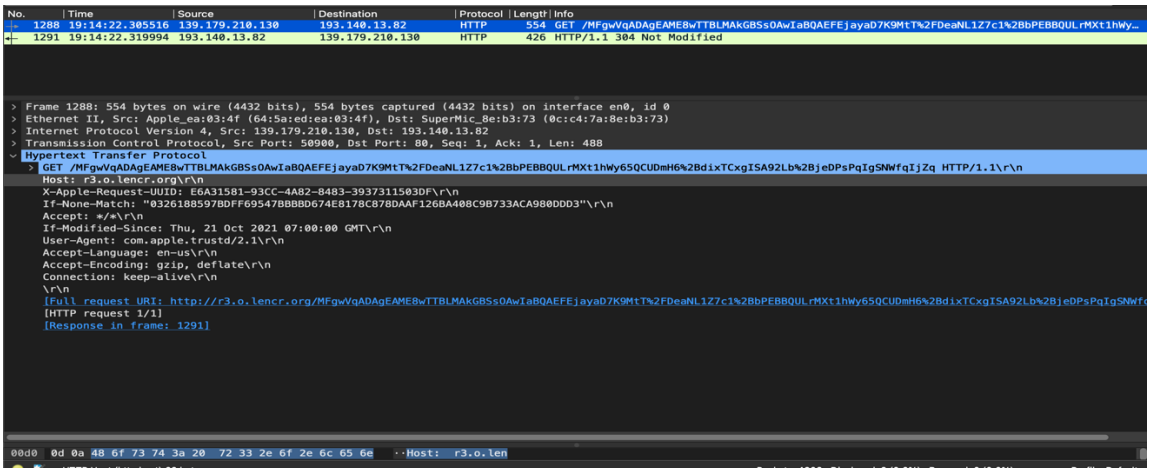
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

   Yes, the status is 200 OK from the server and there was no significant delay:



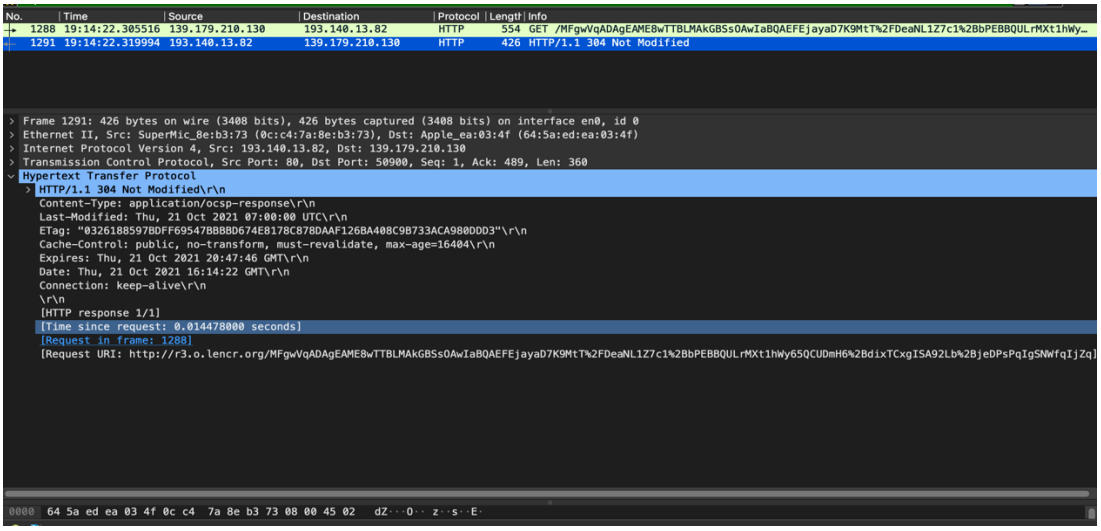
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

    Yes, I can seem to have the “IF-MODIFIED-SINCE:” header in my second GET request. This is to make sure we don’t fetch the same contents already downloaded if not modified:

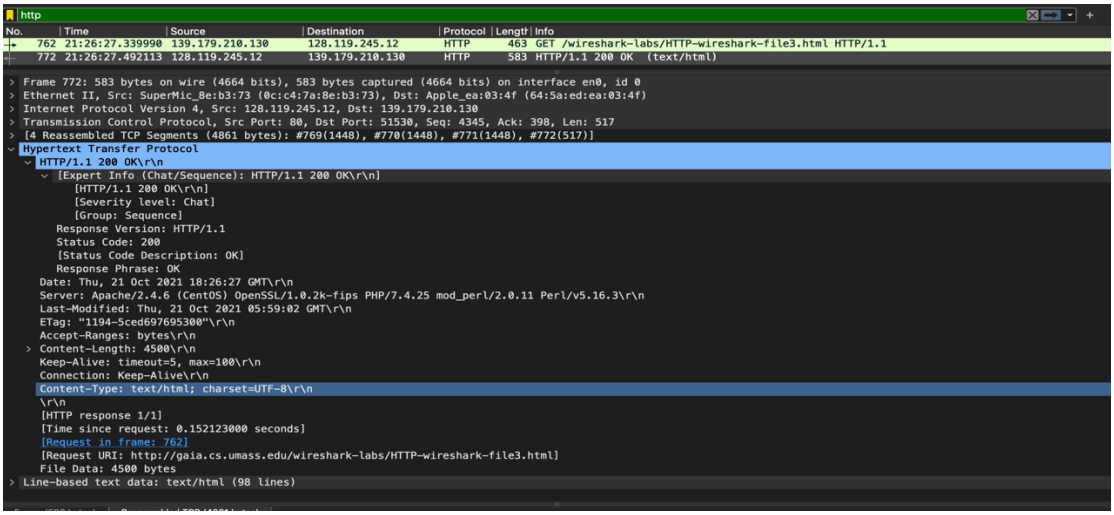


11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file?

    No, we have the content in the cache thus we receive the 304 Not Modified status code; the server didn't return files explicitly:



3. Retrieving Long Documents



4. How many HTTP GET request messages were sent by your browser?

There is only one GET message request sent from my browser to the server

5. How many data-containing TCP segments were needed to carry the single HTTP response?

   Only one data segment needed to carry out the HTTP response with 4500 bytes carried in file data. Ironically, I expected there to be more as suggested in the problem set, but I received only one response from the HTTP server. The attached screenshot above shows that only one data containing TCP segment is received.

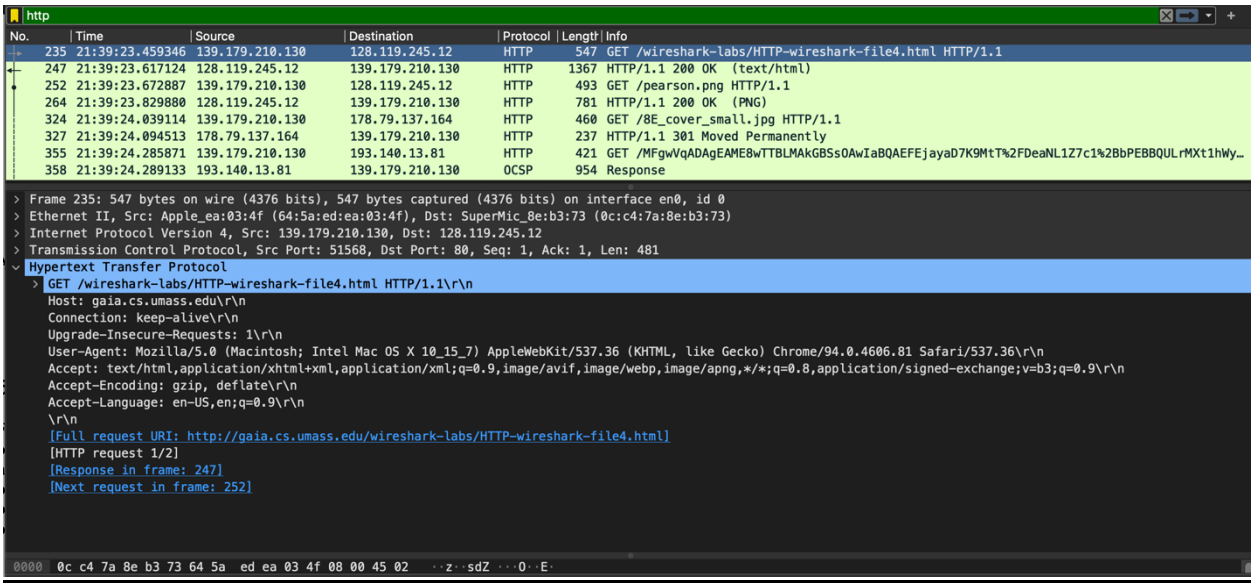
6. What is the status code and phrase associated with the response to the HTTP GET request?

   status code: 200, status response: OK

7. Are there any HTTP status lines in the transmitted data associated with a TCP- induced "Continuation"?

   No.

4. HTML Documents with Embedded Objects



5. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

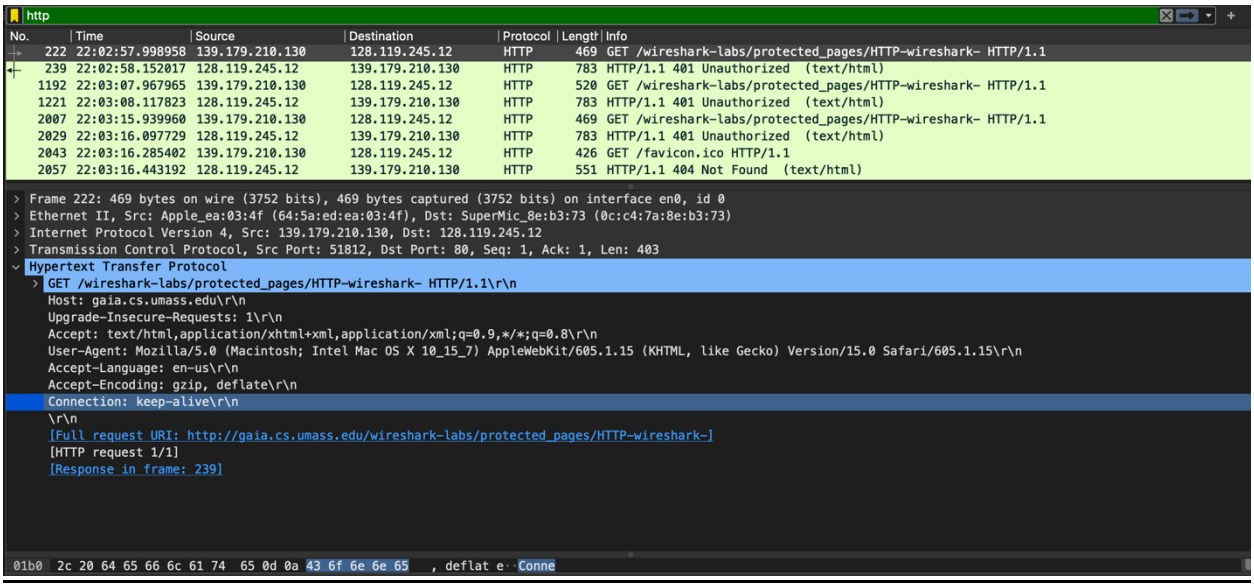
   As one can see from the above screenshot attached, there are in total GET requests sent to the following Internet Addresses:
   128.119.245.12 (2 requests sent to this addresses)

178.79.137.164
193.140.13.81

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

By checking the TCP ports, we can see if the files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections as depicted in the screenshot above, therefore, they were downloaded serially. Two separate connections were made to retrieve these images separately. We can also see that a status code of 301 is received when a GET is requested for cover_small.jpg; this results in a redirection to retrieve the resource. Thus, more than 2 TCP connections to retrieve the images, hence, serially.

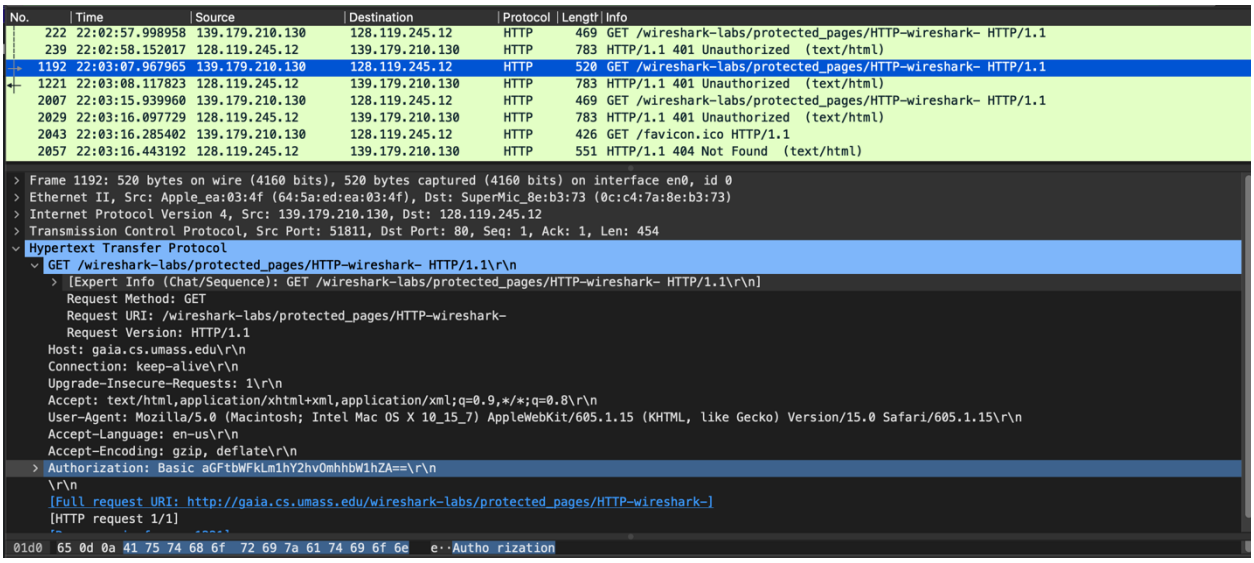
5. HTTP Authentication



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

As we can see above, the status code in response to the initial GET request is 401 with phrase 'Unauthorized.'

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

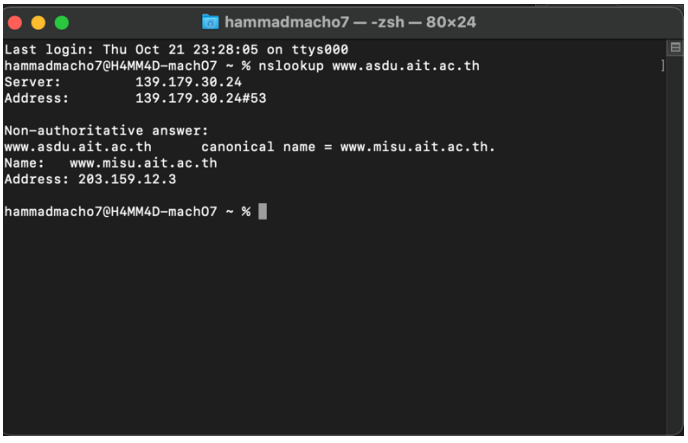


The new field included is Authorization as seen in the screenshot above. I have highlighted the new field. It contains the encoded form of the username and password.

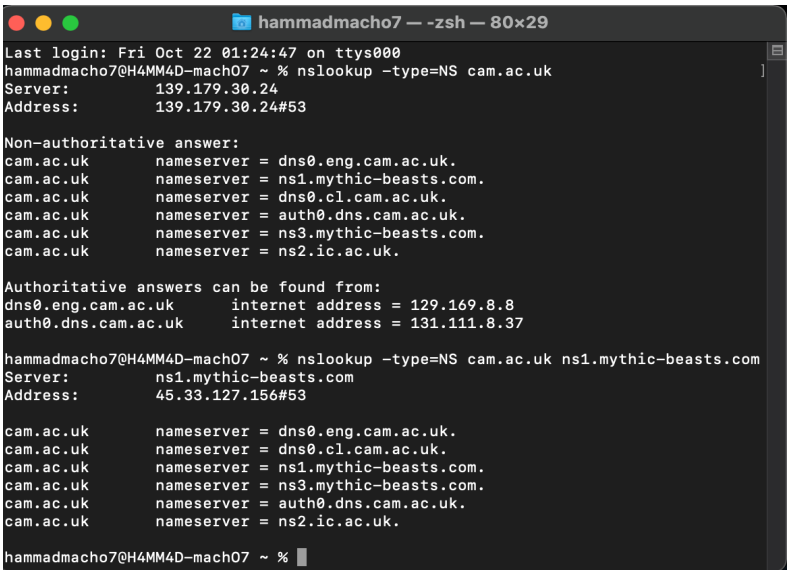
DNS

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

   For this part, I queried the webpage of AIT based in Thailand. The IP address for that server was 203.159.12.3



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

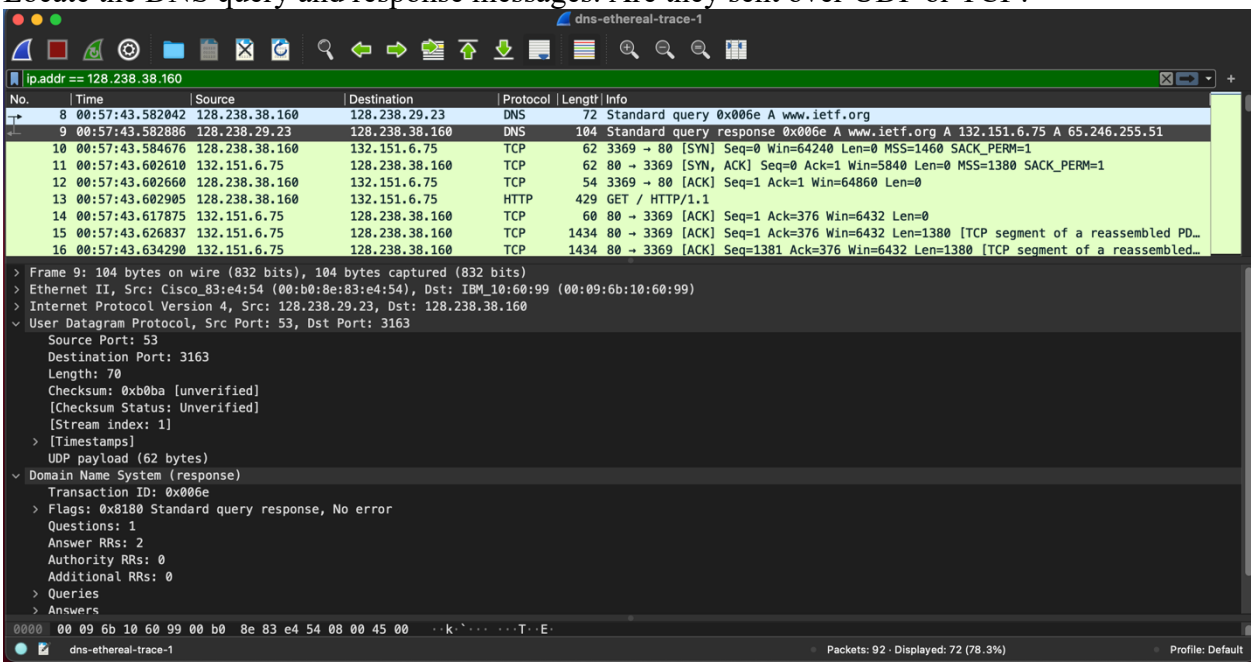


The query I sent for this part was for www.cam.ac.uk (Cambridge University) in England. One of the primary/authoritative servers is: `ns1.mythic-beasts.com`.

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

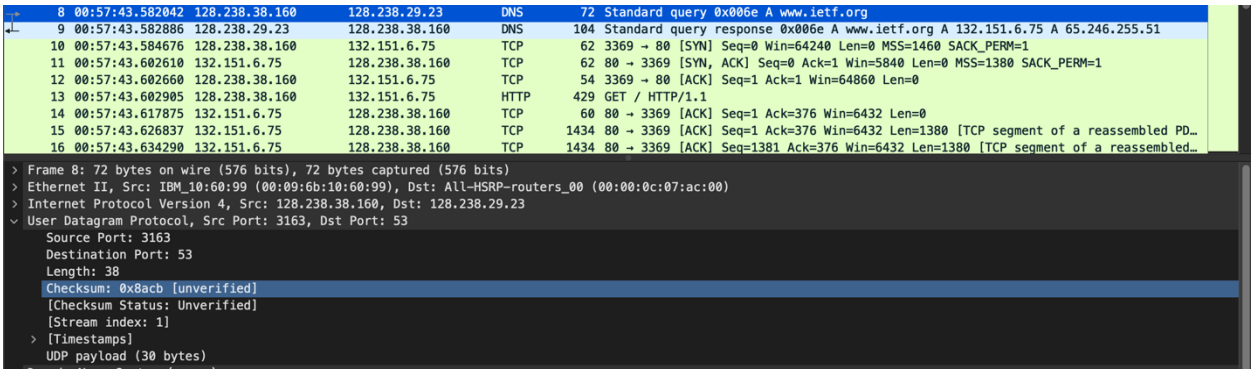
I couldn't find the servers for yahoo mail thus I queried another British university Oxford university using `ns1.mythic-beasts.com`.

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



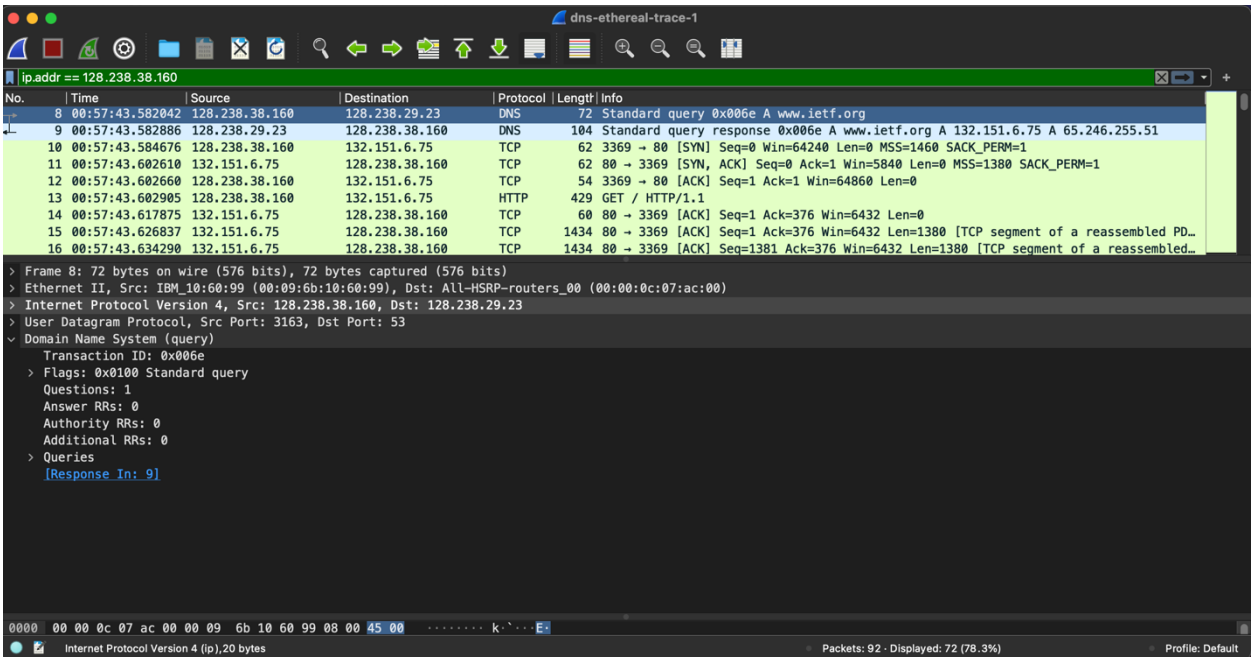
As seen in the Screenshot, it is sent over UDP (User Datagram Protocol).

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



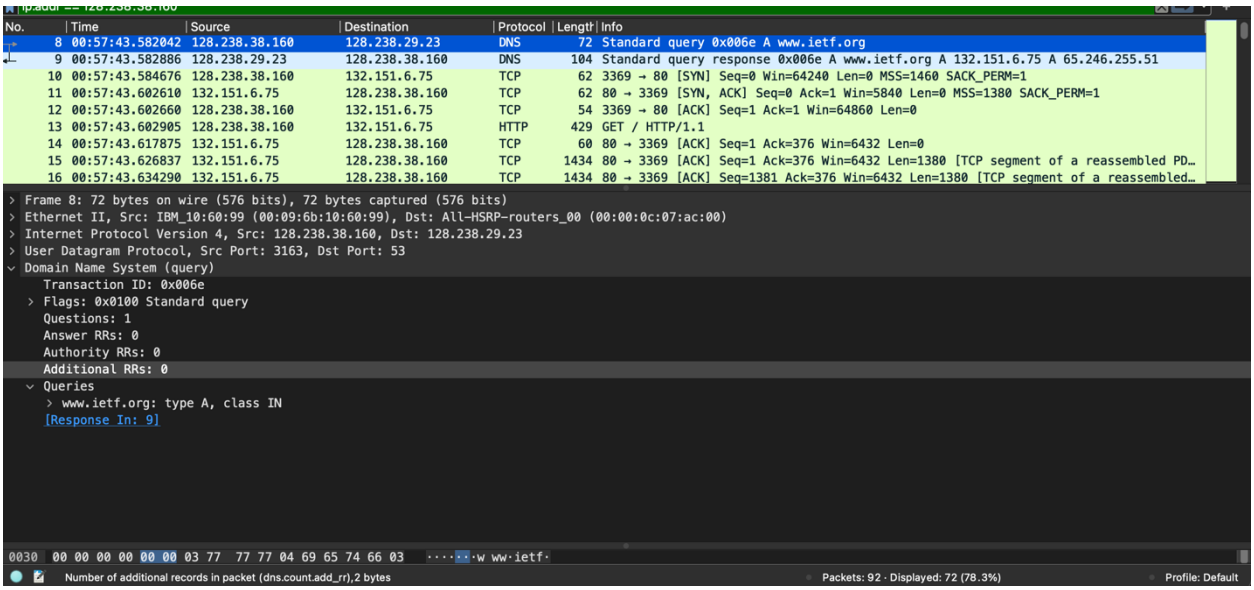
Source port: 3163
Destination Port: 53

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?



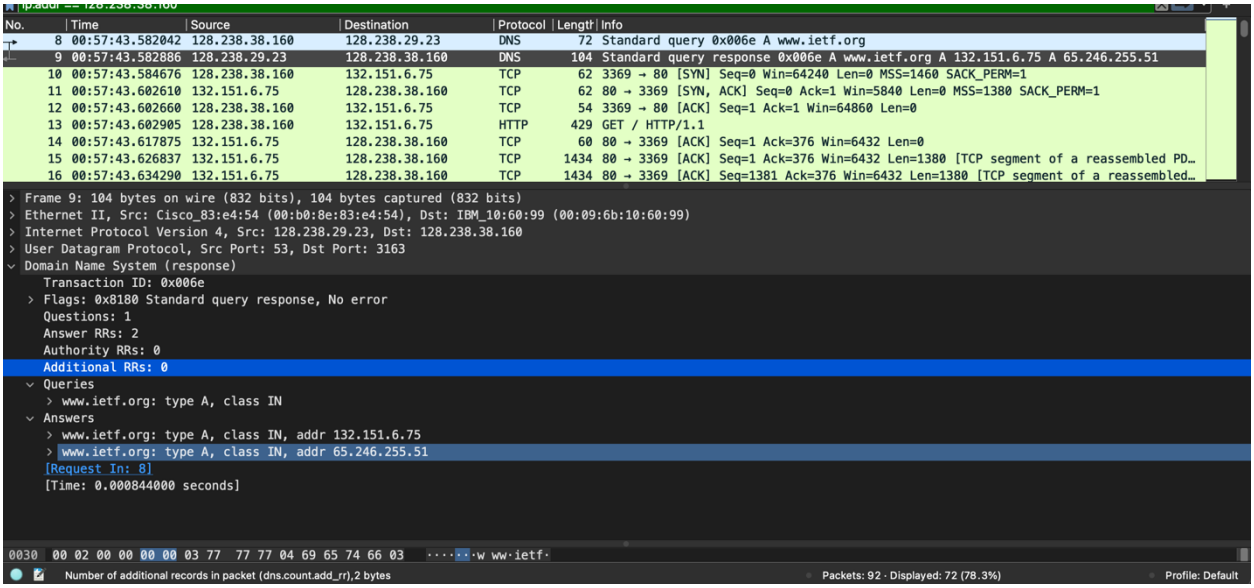
DNS message sent to IP Address: 128.238.29.23
Yes, it must be the local DNS server and be same. I have used the packet lists provided in the assignment PDF. I have resorted to using the packets provided as I have a MacOS which uses Unix CLI. The commands are very different from the ones provided, thus, for uniformity purposes, I am using packets.

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



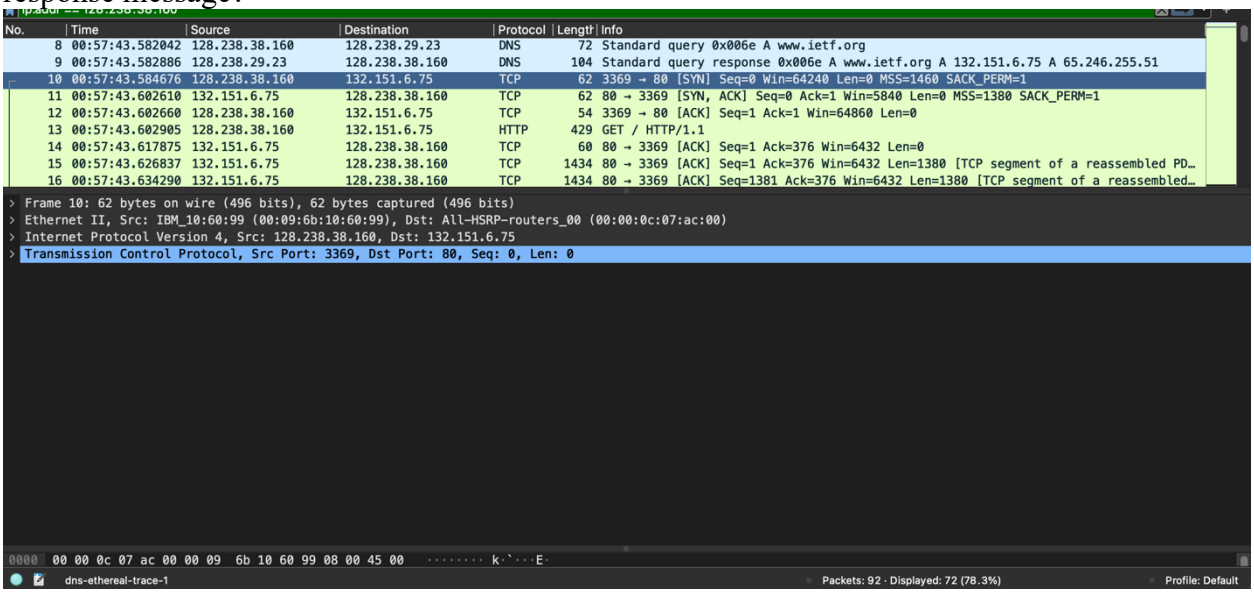
The query type is A, and as the screenshot above displays, it doesn't contain any answers.

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



Two answers are provided;
each answer contains name, type, class, time to live, data length, and address of the queried webpage.

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?

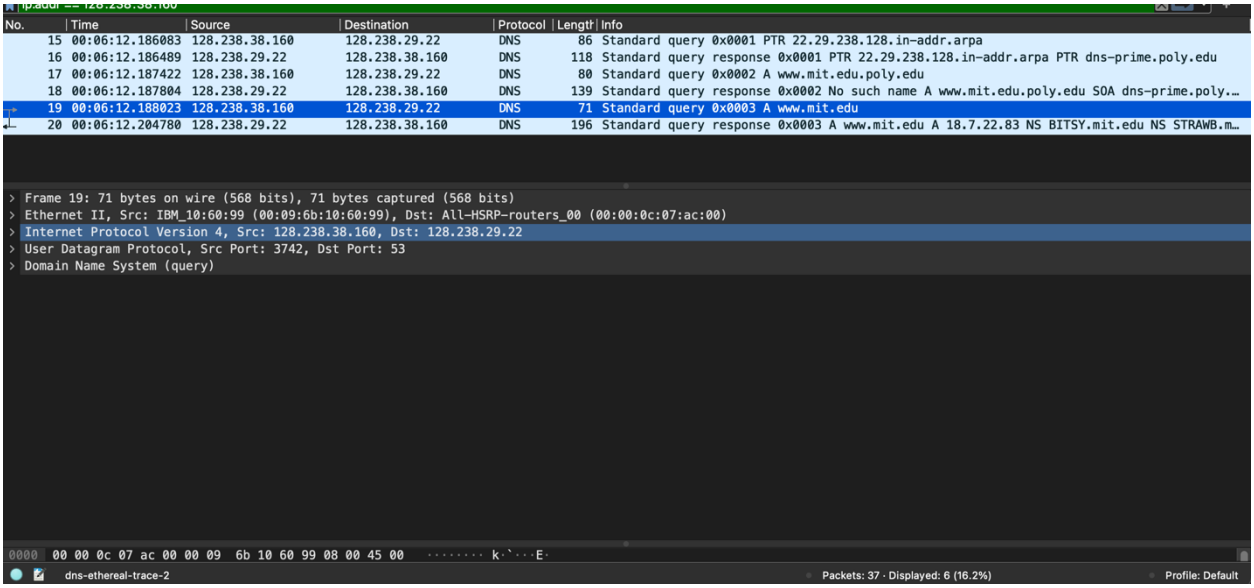


Yes, it corresponds to the IP address 132.151.6.75

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

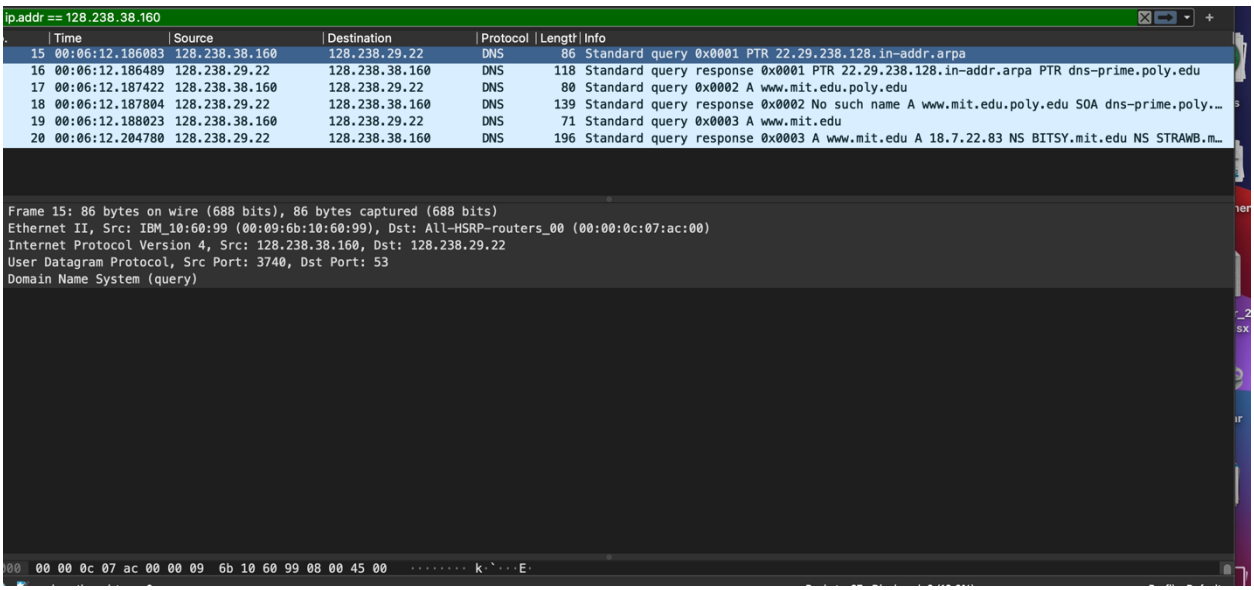
No, there are no further DNS requests sent. The images are loaded from www.ietf.org.
We can also see from the screenshots provided above that only one DNS request is sent.

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



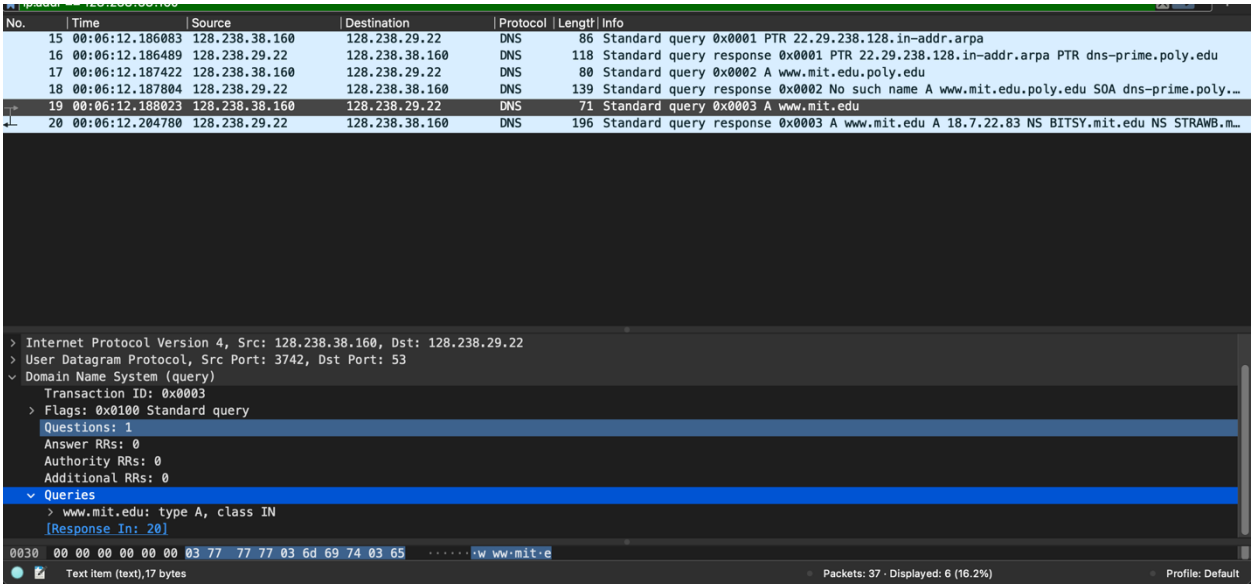
Source Port for query: 3742
Source Port for response: 53

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



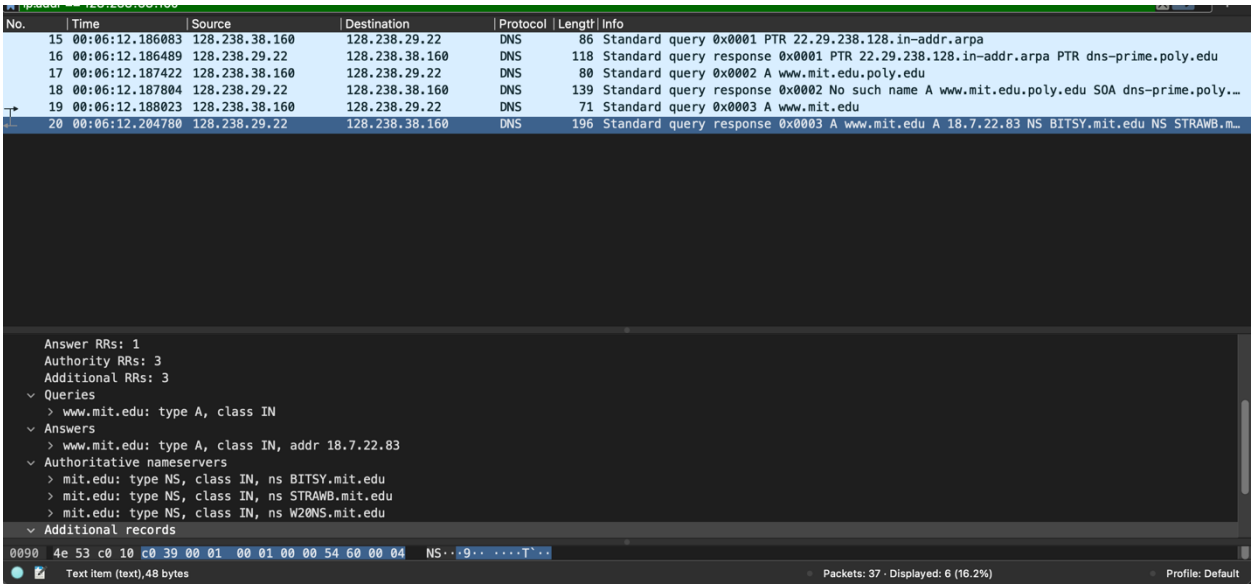
IP address query message sent: 128.238.29.22, and yes, it is the default local DNS server.

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



The type of query sent is A, and no this query doesn’t contain any answers.

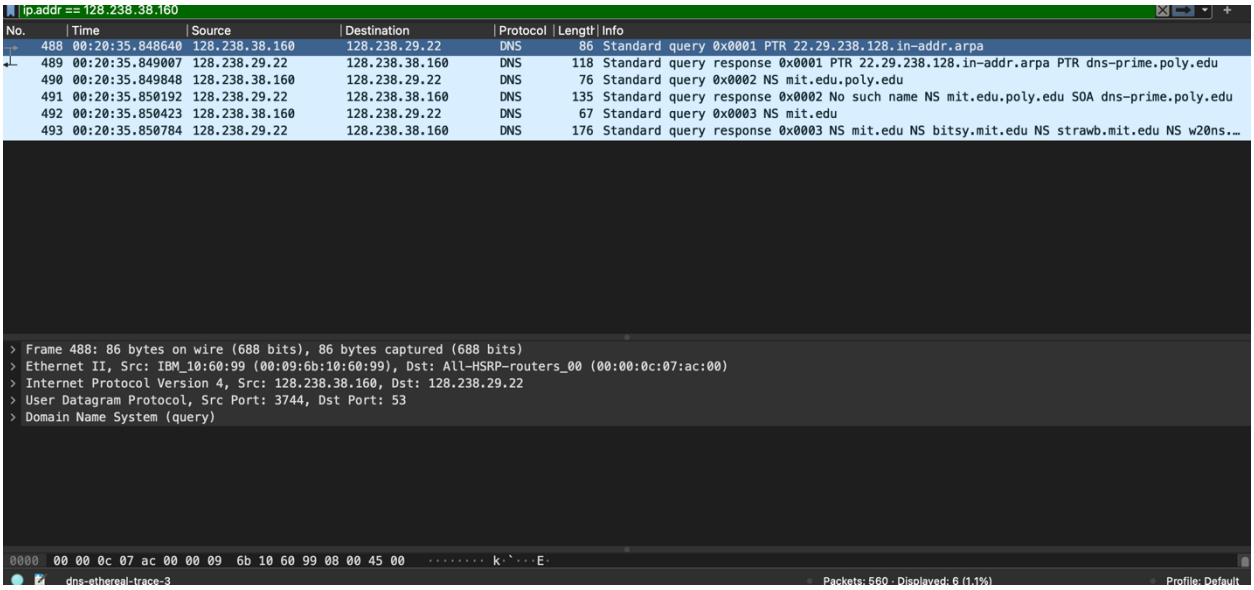
14. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?



One answer provided and three authority RR’s.

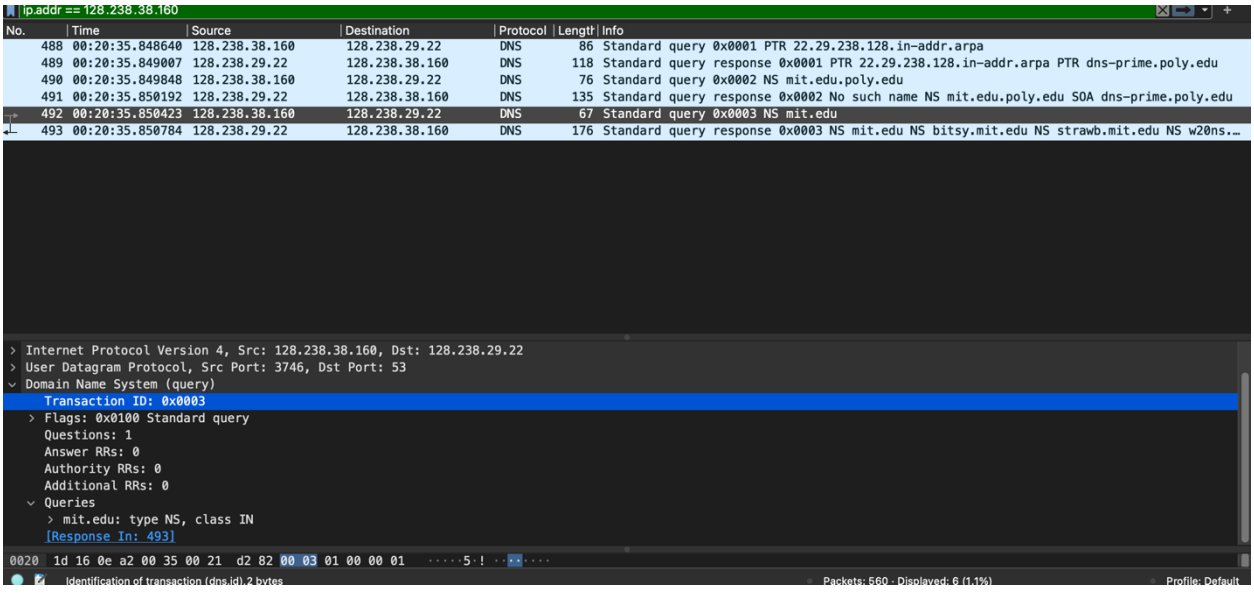
15. Provide a screenshot. (Provided above)

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



The local DNS server query sent to is IP address 128.238.29.22, and yes, this is the local DNS server. We can see that in the above screenshots tat it is the same local server queries are sent to.

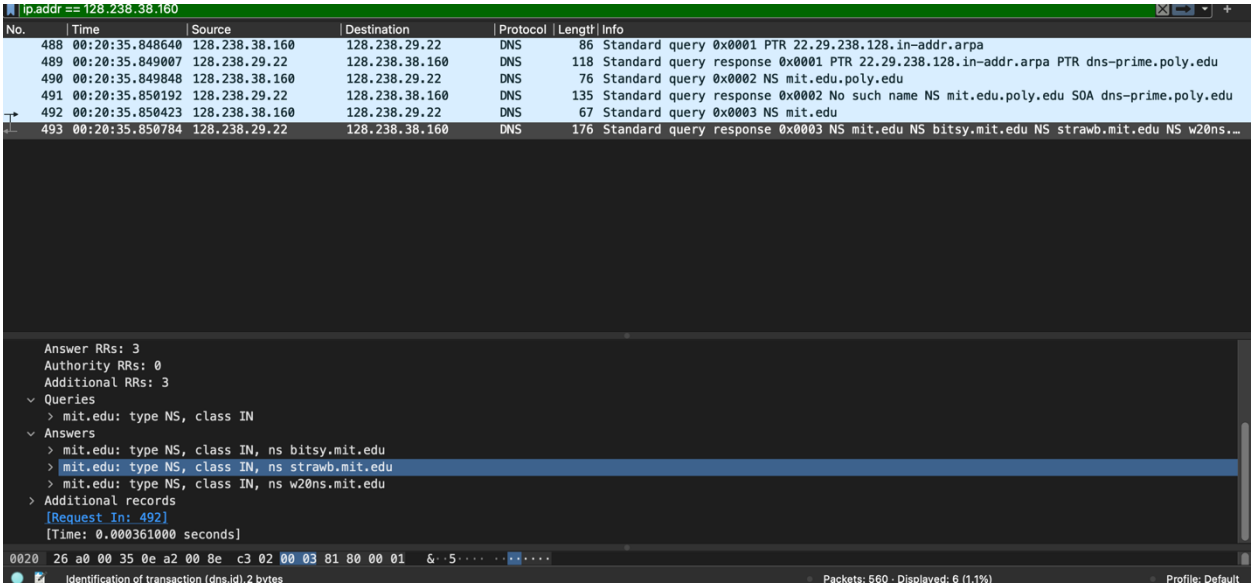
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

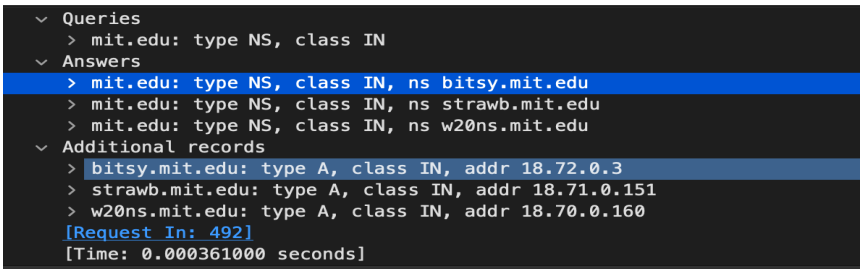


Examining the second last and last queries; the last query request sent is of type NS as seen in the above screenshot.

18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?
    MIT name servers responded with addresses:
    bitsy.mit.edu 18.72.0.3
    strawb.mit.edu 18.71.0.151
    w20ns.mit.edu 18.70.0.160

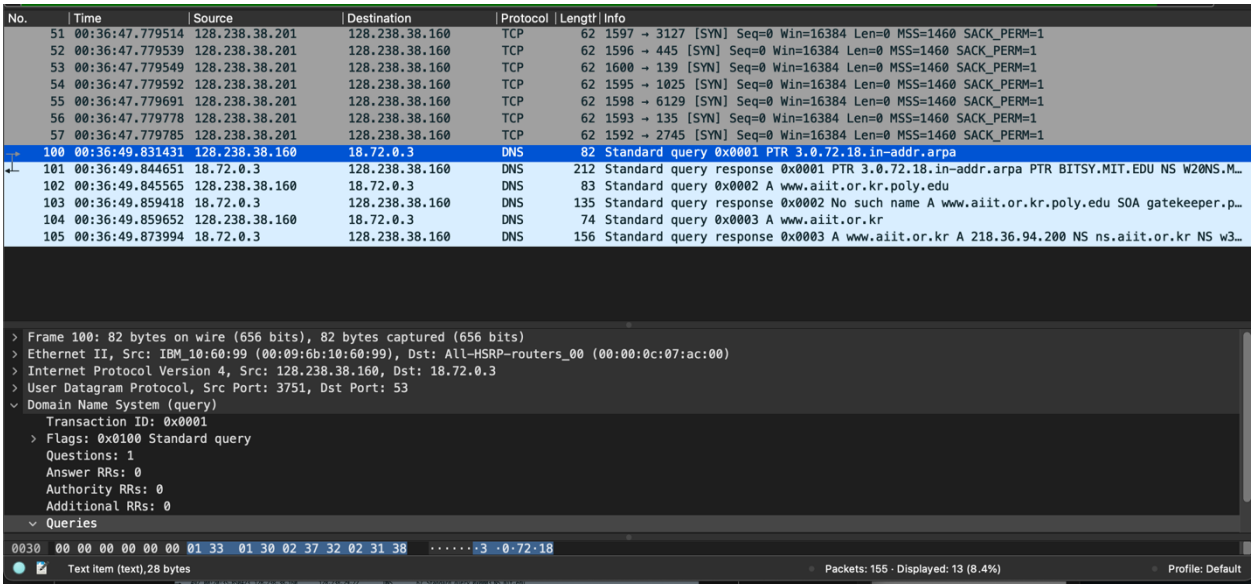
    And no authority RRs.





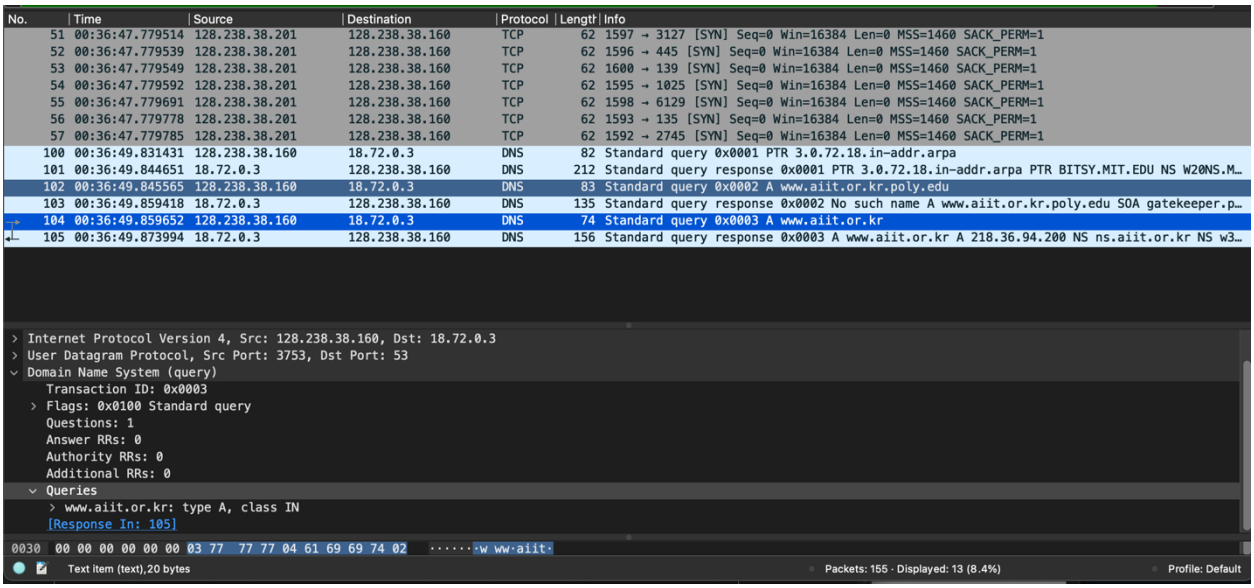
19. Provide a screenshot. (Provided above)

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?



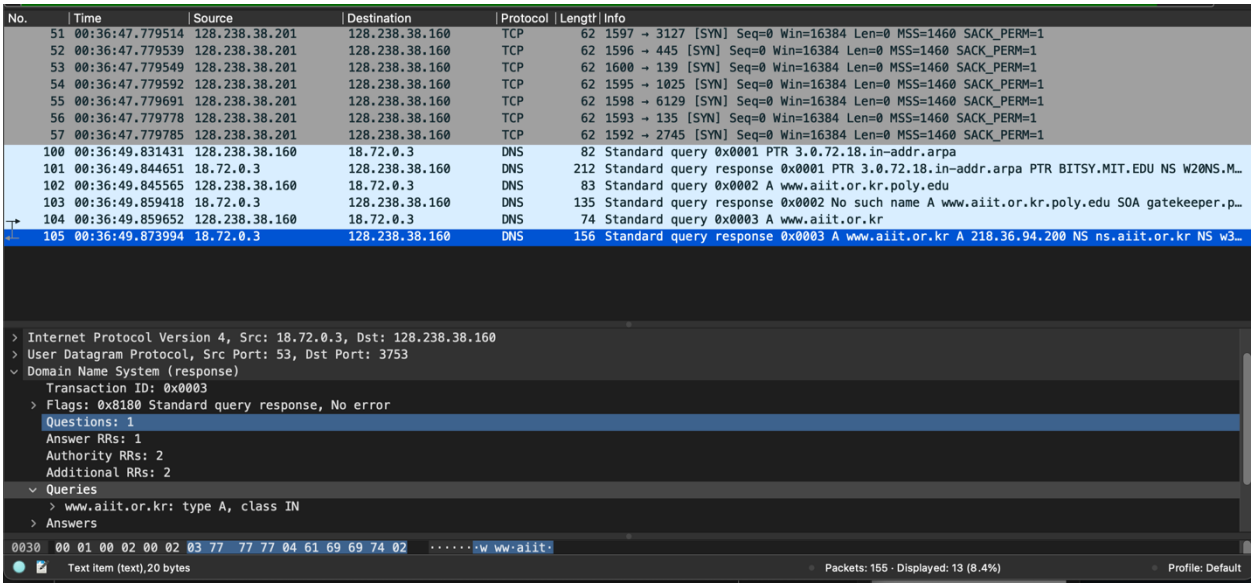
The query is sent to IP address 18.72.0.3, which is the IP address of bitsy.mit.edu (the server queried for the query instead of the default local server).

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

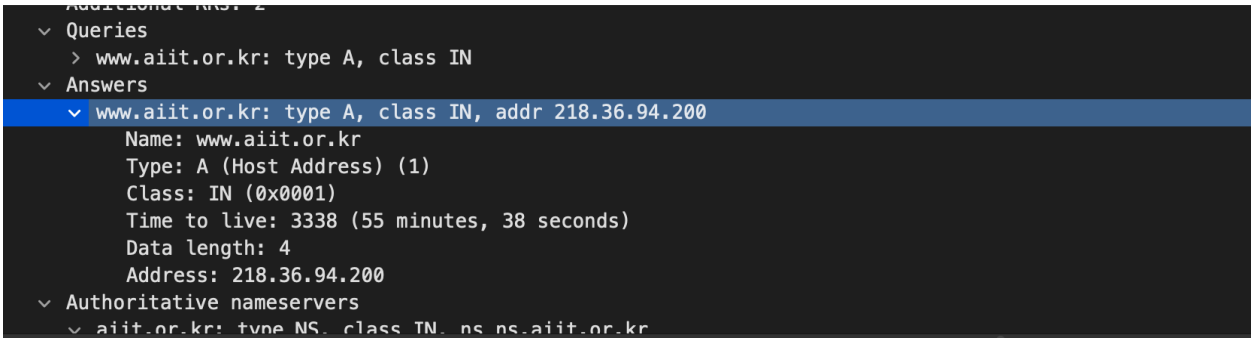


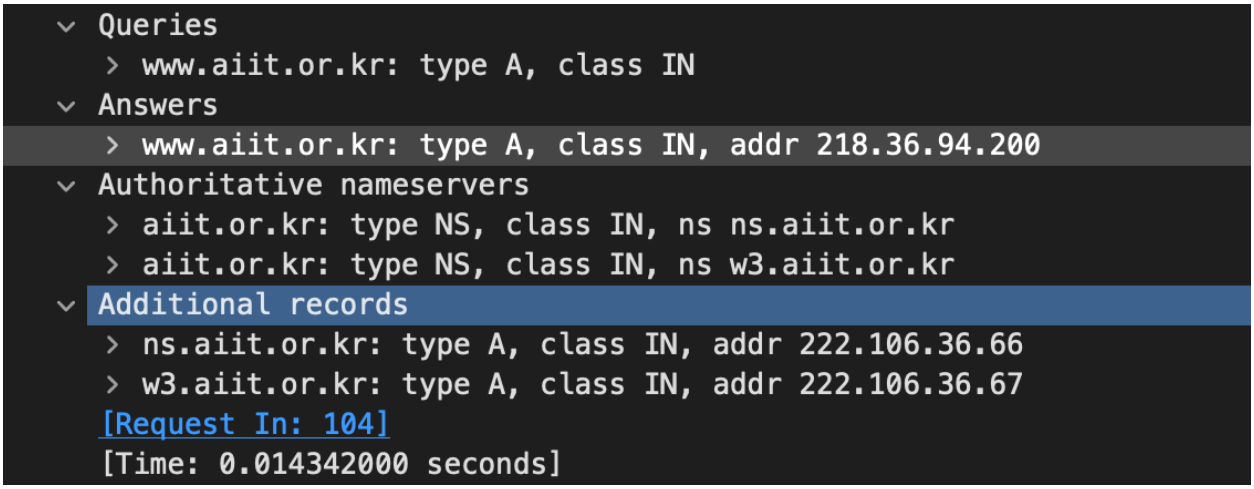
Type of query: A
and the query message doesn't contain any answers.

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



There is One answer RRs and Two authority RRs. The answer contains type of query, address of the queried webpage, class, time to live, data length, and address. The below screenshot provides further details of the answer and authority RRs.





23. Provide a screenshot.