Computer Networks Assignment - 1

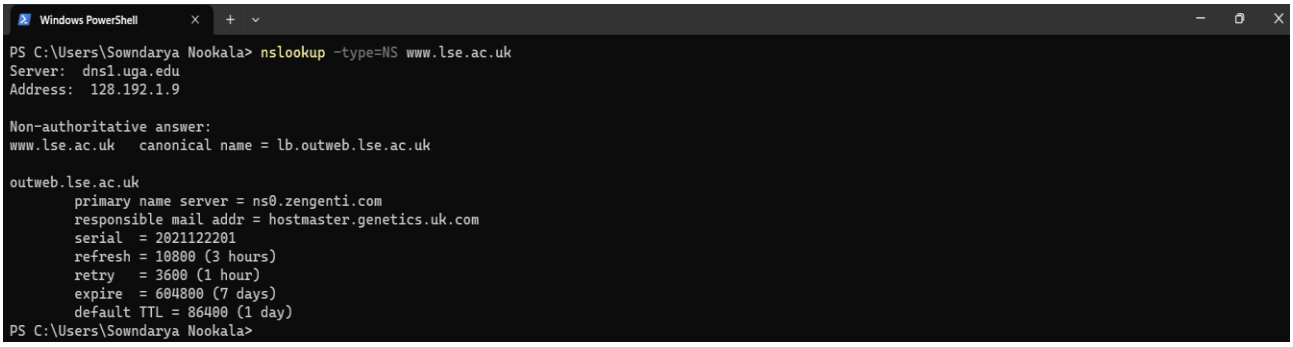
Submitted By: N V H Sowndarya
Email ID: sowndaryanoookala.vh@uga.edu
UGA ID: 811594990
Submission Date: 24th February,23

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 a server in Asia (www.iiit.ac.in) is 196.12.53.50

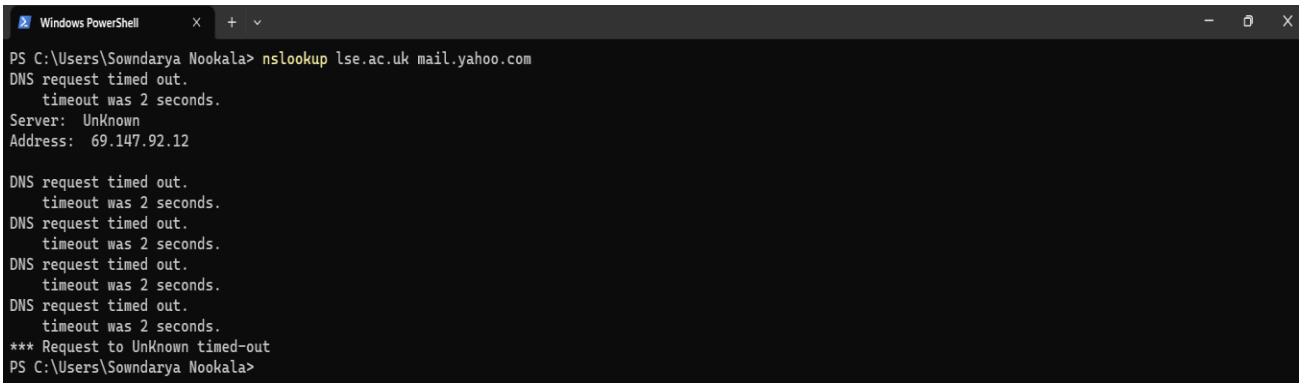
2. **Run *nslookup* to determine the authoritative DNS servers for a university in Europe.**

   The authoritative DNS servers for London School of Economics and Political Science in United Kingdom, Europe with (https://www.lse.ac.uk/) is ns0.zengenti.com



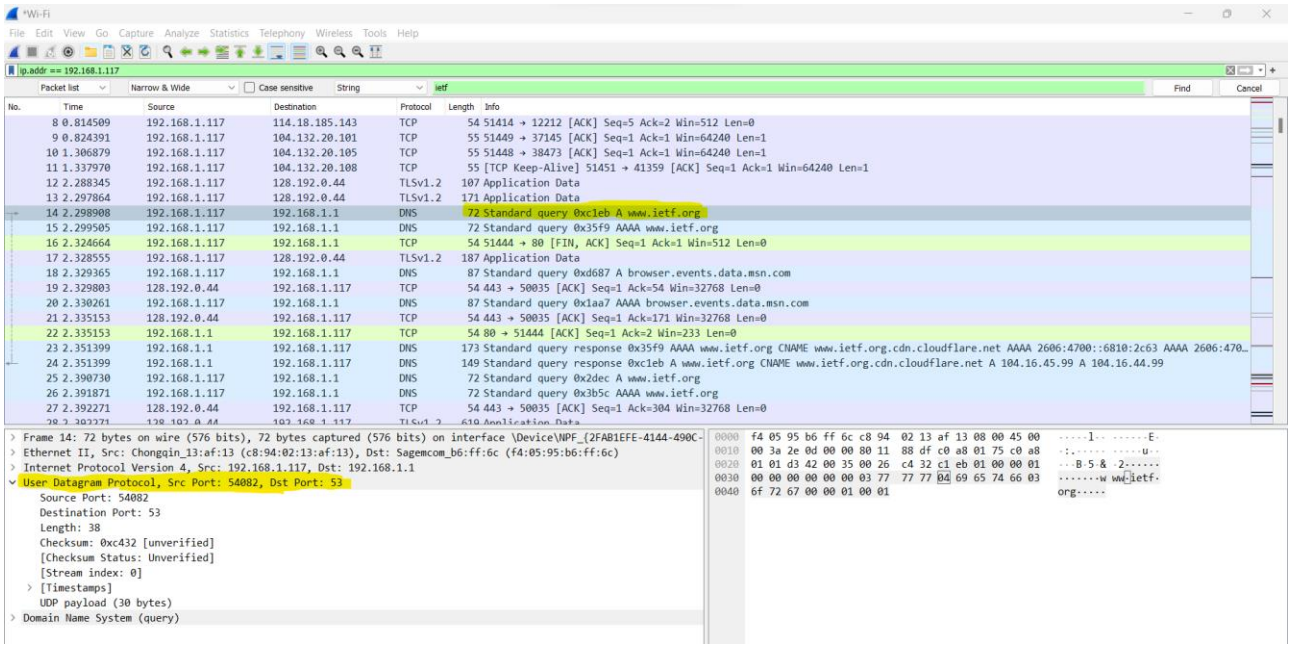
3. **Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?**

   The IP address after querying lse.ac.uk with yahoo mail server using the nslookup is 69.147.92.12



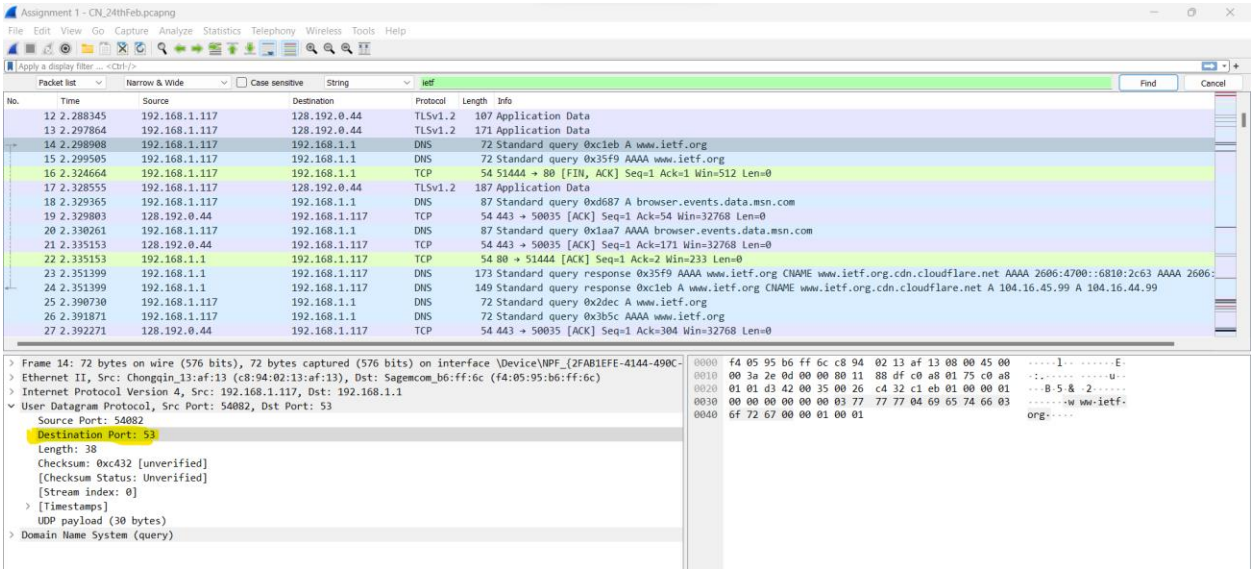
4. **Locate the DNS query and response messages. Are then sent over UDP or TCP?**

The DNS query and response messages are sent over User Datagram Protocol (UDP).

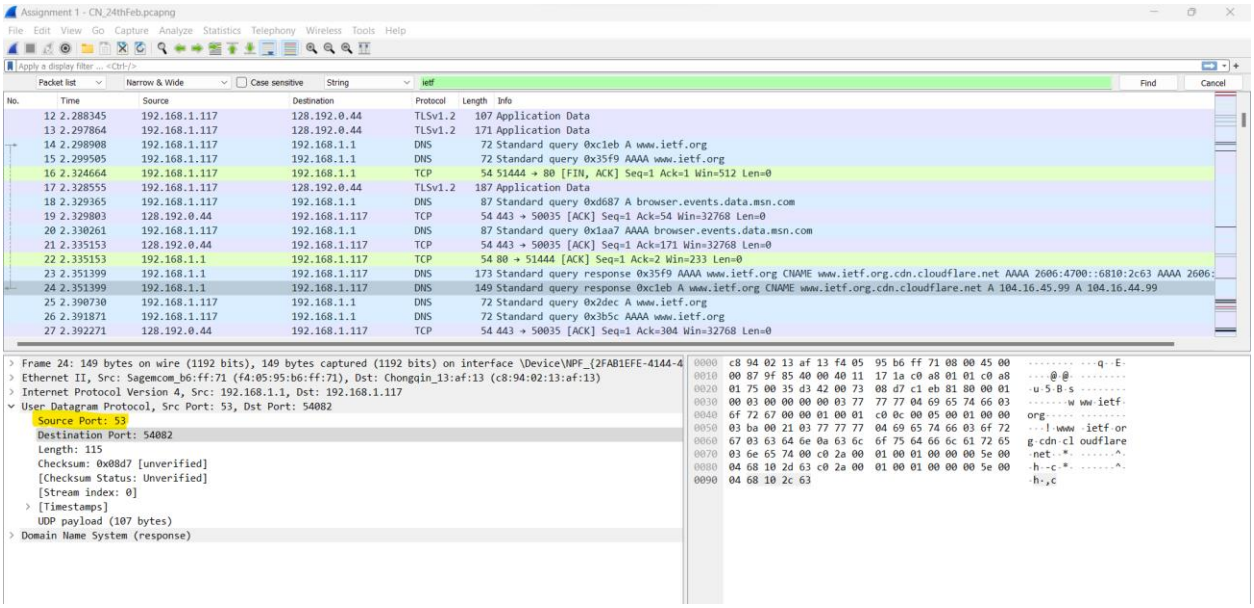


5. **What is the destination port for the DNS query message? What is the source port of DNS response message?**

The Source port is 54082 and the Destination port is 53 for the DNS query message.

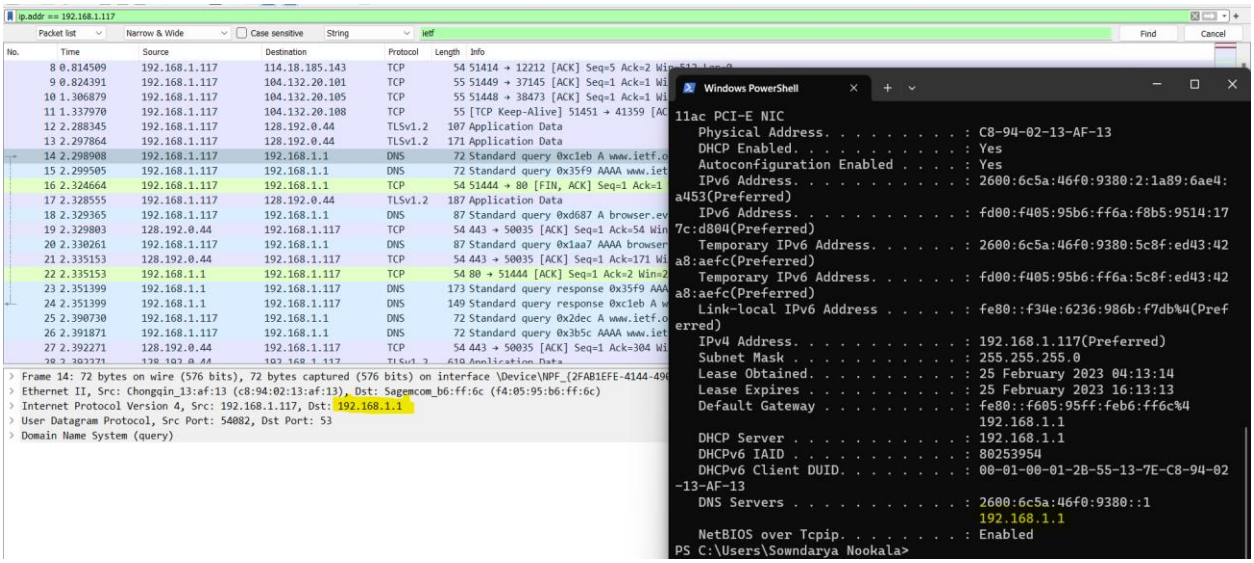


The Source port is 53 and the Destination port is 54082 for the DNS response message.



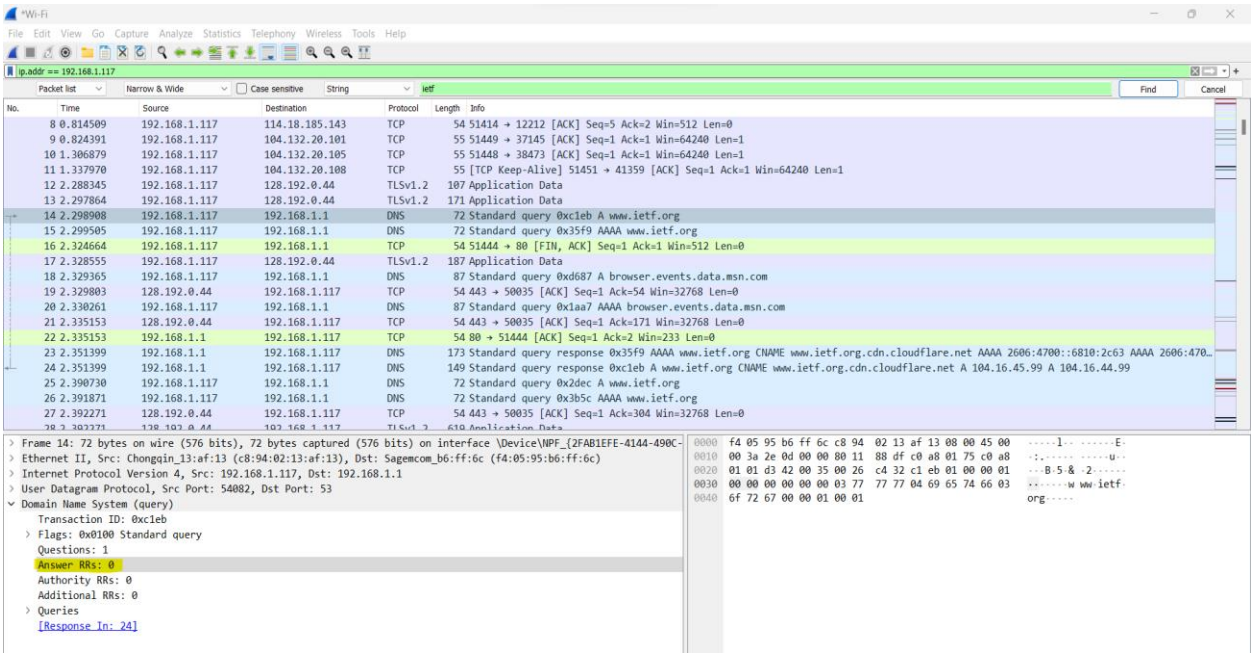
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The DNS query messages are sent to 192.168.1.1 which is same as local address.



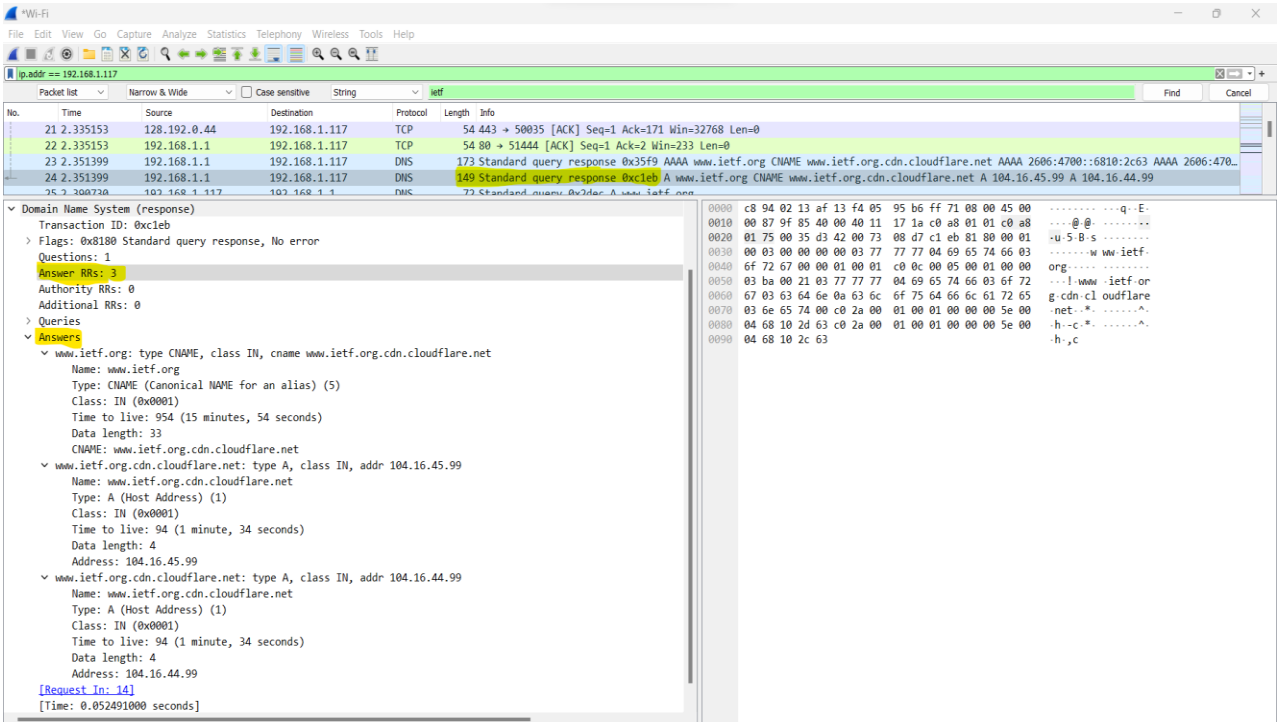
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The Type of DNS query is of Type A. The query does not contain any answers.



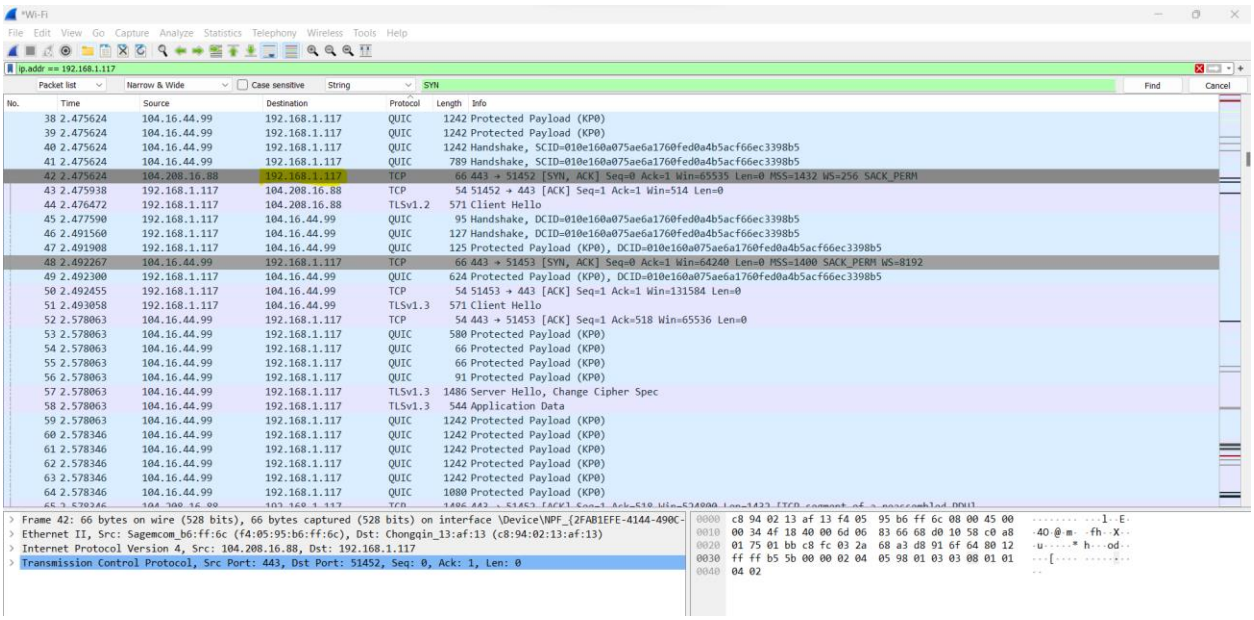
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

For DNS response messages, three answers are retrieved. The answer contains namespace, type, class and address of that web address.



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's destination IP address matches the IP addresses provided in the DNS response message that is 192.168.1.117



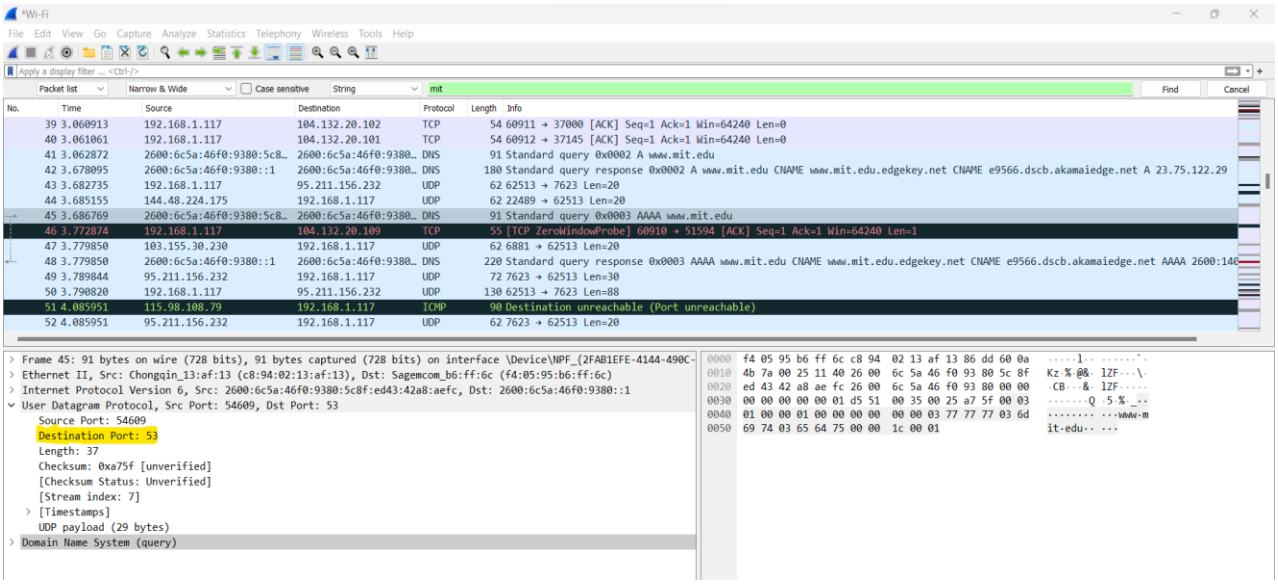
10. **This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

    No, the host is not issuing new DNS queries before retrieving images.

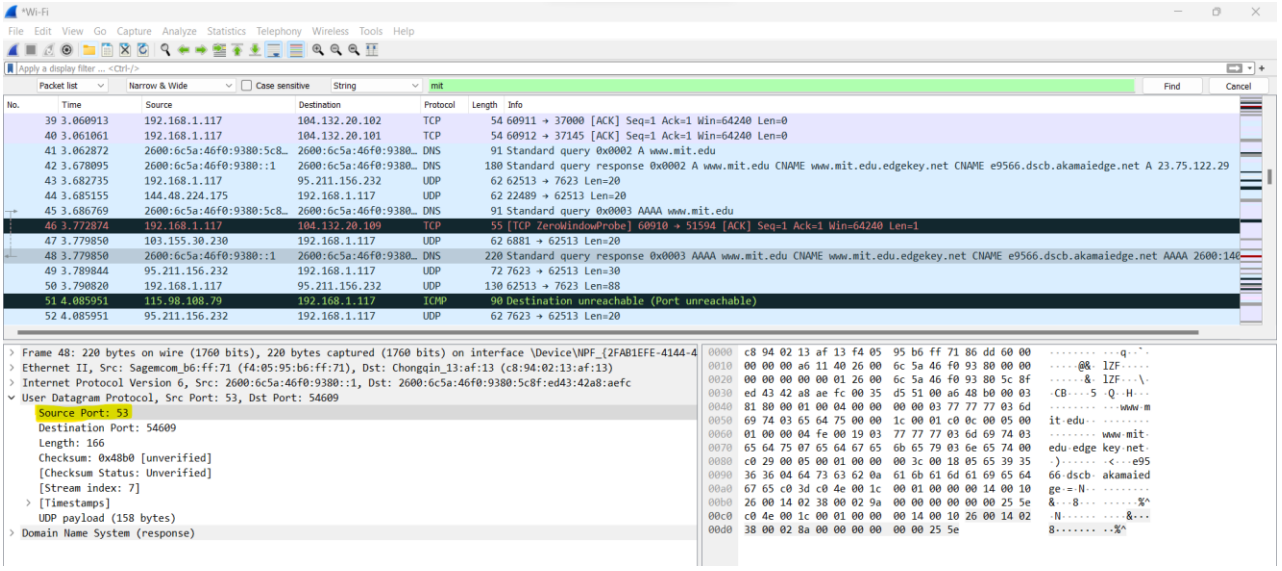
11. **What is the destination port for the DNS query message? What is the source port of DNS response message?**

    The destination port of the DNS query message and the source port of DNS response message is 53.

    For Query Message - Source Port: 54609 Destination Port: 53

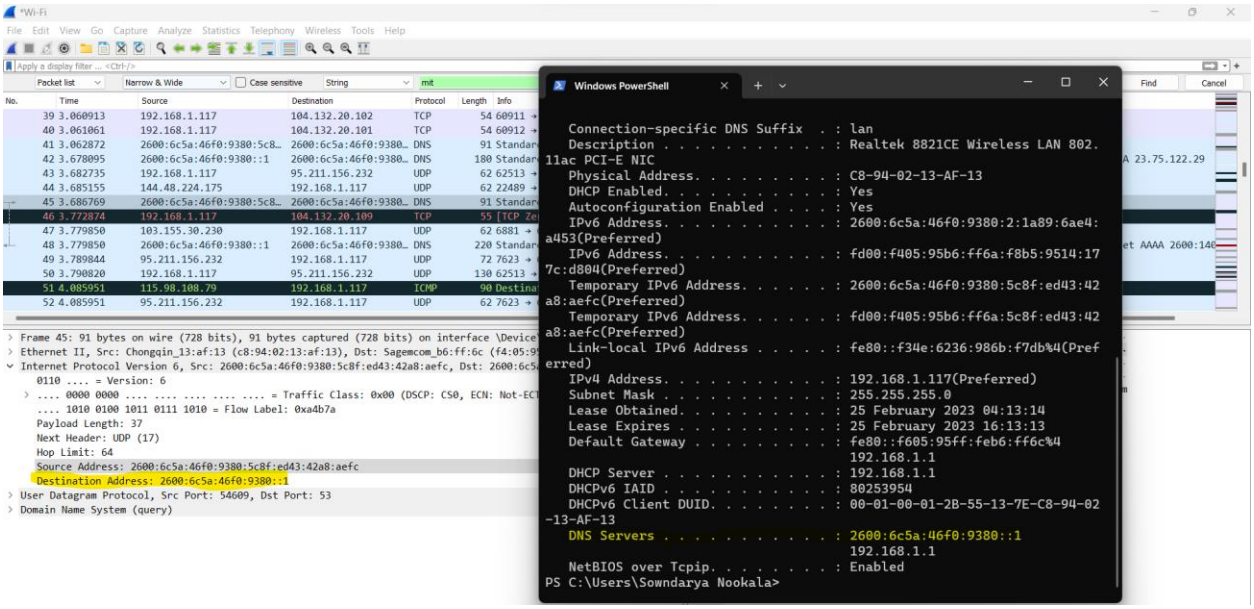


For Response Message - Source Port: 53 Destination Port: 54609



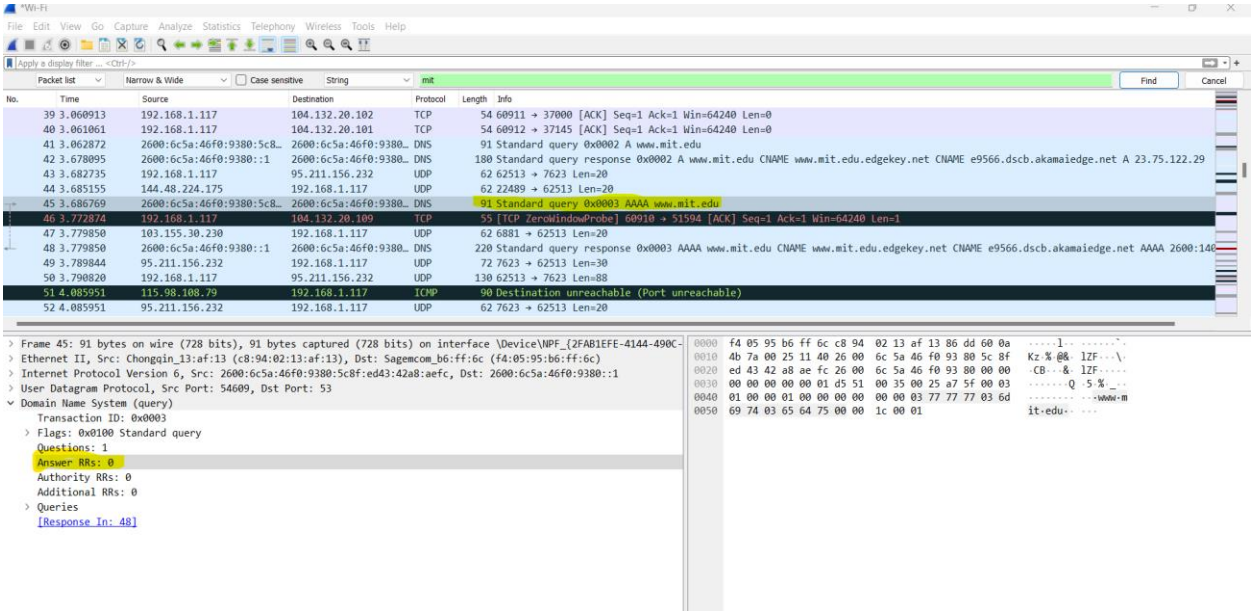
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS query message is sent to the IP address(v6) 2600:6c5a:46f0:9380::1
Yes, this is same as my local DNS server.



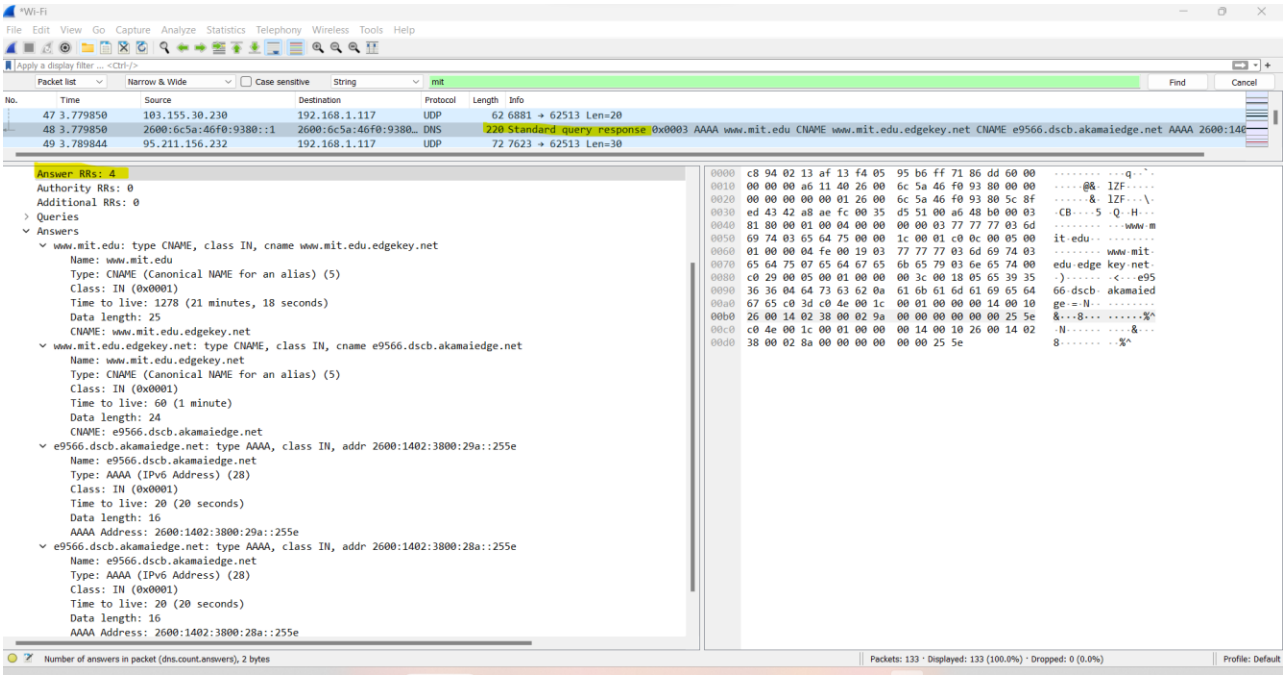
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

This is DNS query is of TYPE AAAA and it doesn't contain any answers.

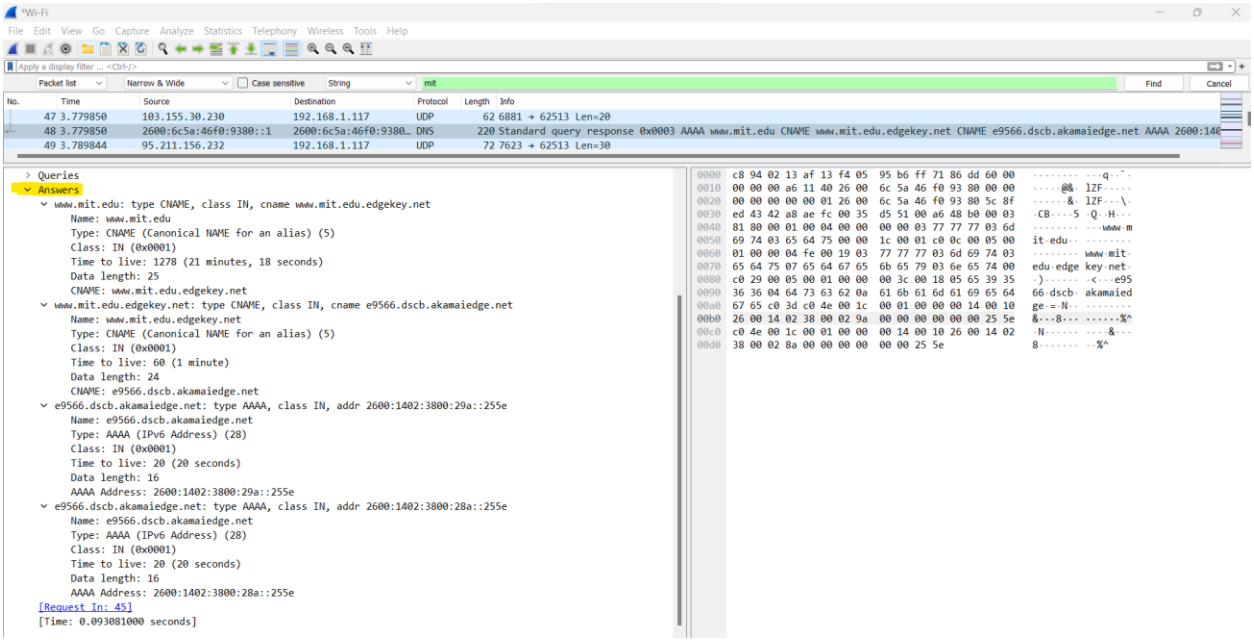


14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Four answers are provided in the DNS response message.

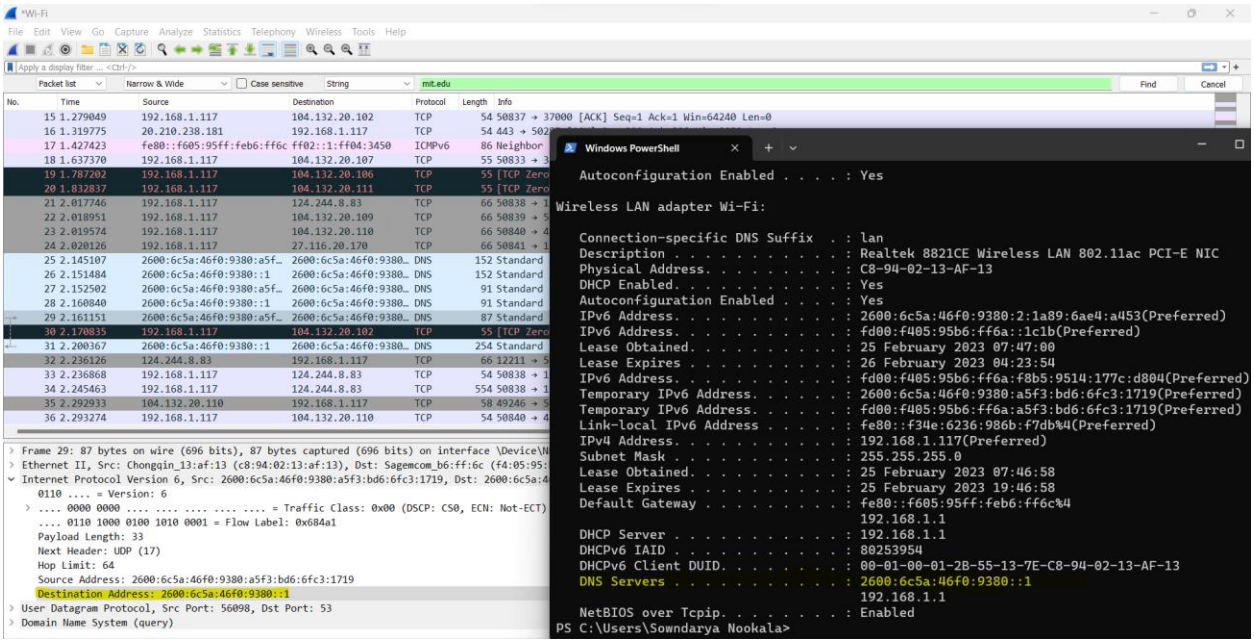


15. Provide a screenshot.



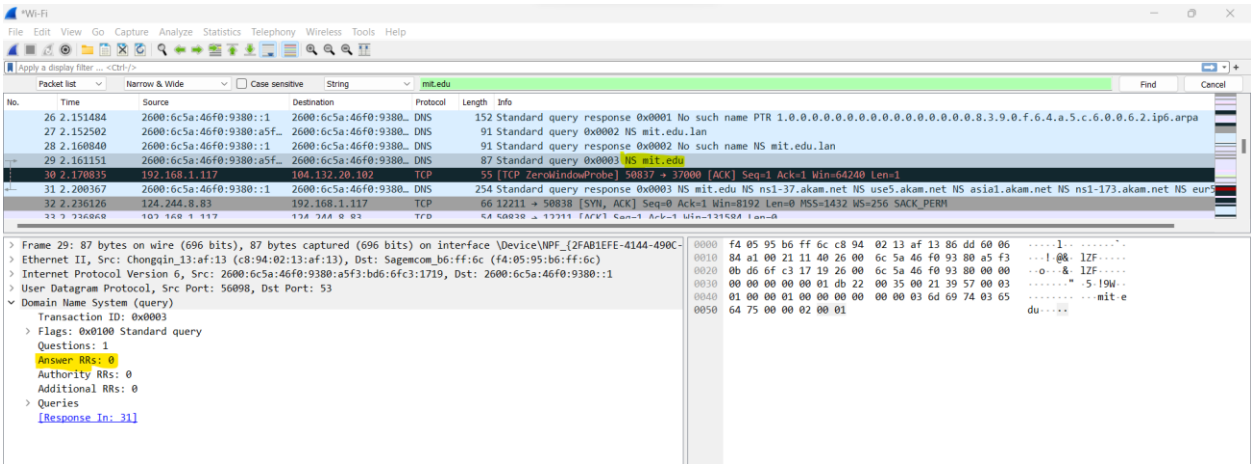
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS query message is sent to the IP address 2600:6c5a:46f0:9380::1
Yes, this is same as my local DNS server.



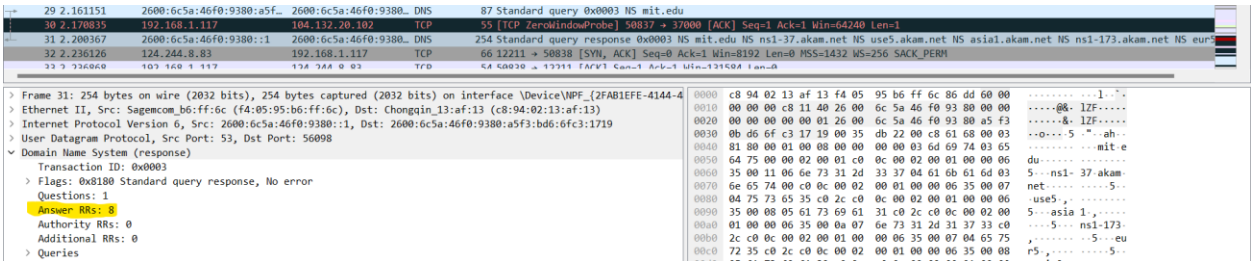
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The DNS query message is of Type: NS, this doesn't contain any 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?

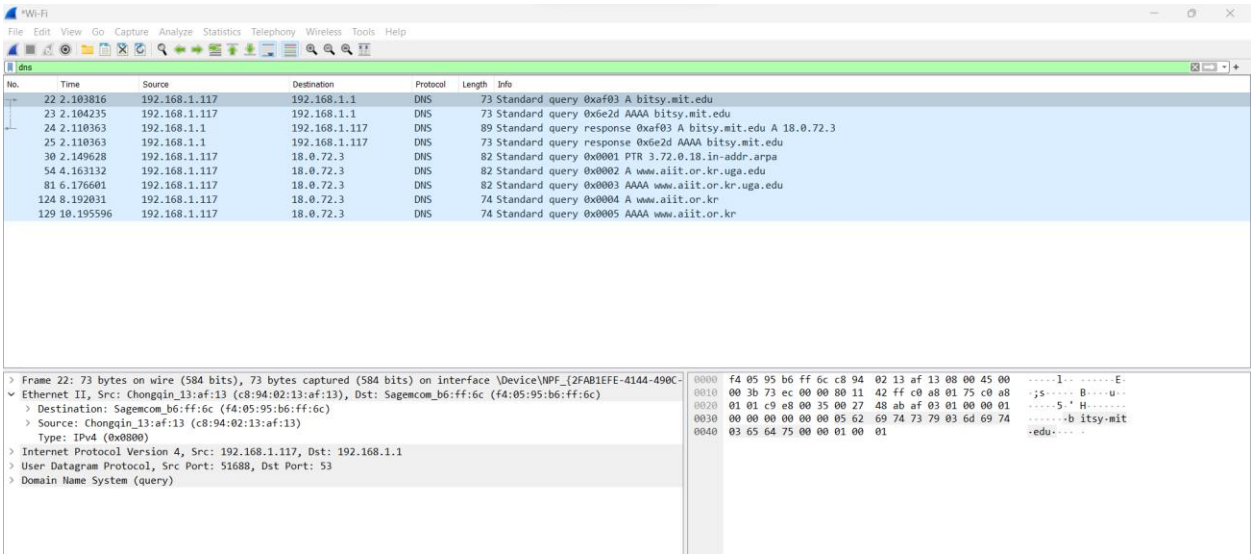
There are 8 nameservers in the DNS response message. No, the response message does not include IP addresses of the nameservers.



19. Provide a screenshot.

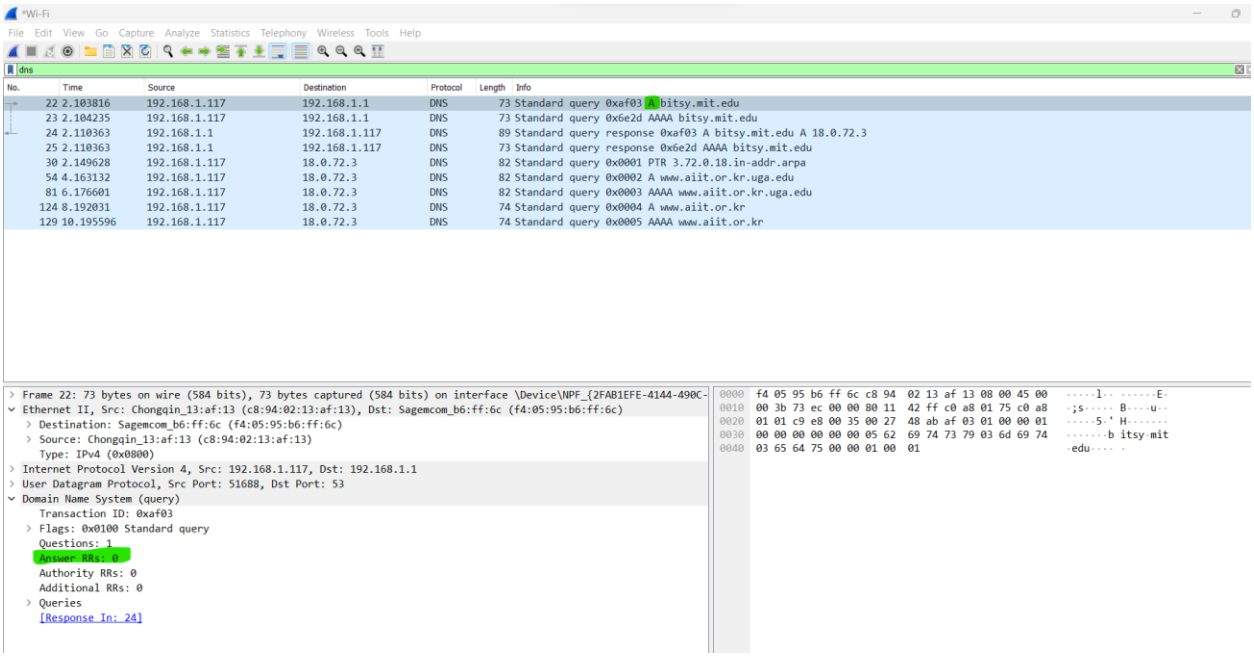
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The query was sent to a two different IP addresses which are 192.168.1.1 and 18.0.72.3 and one of the IP addresses is same as my local.



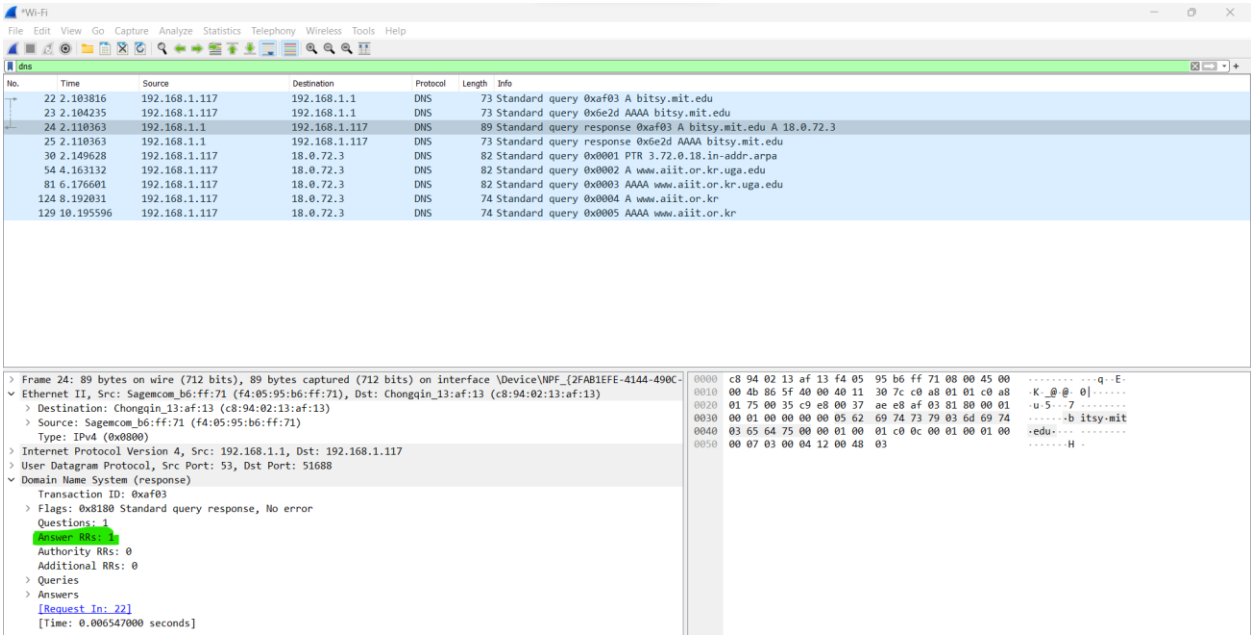
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The DNS query message of my request is of Type: A and the message this doesn't contain any answers.

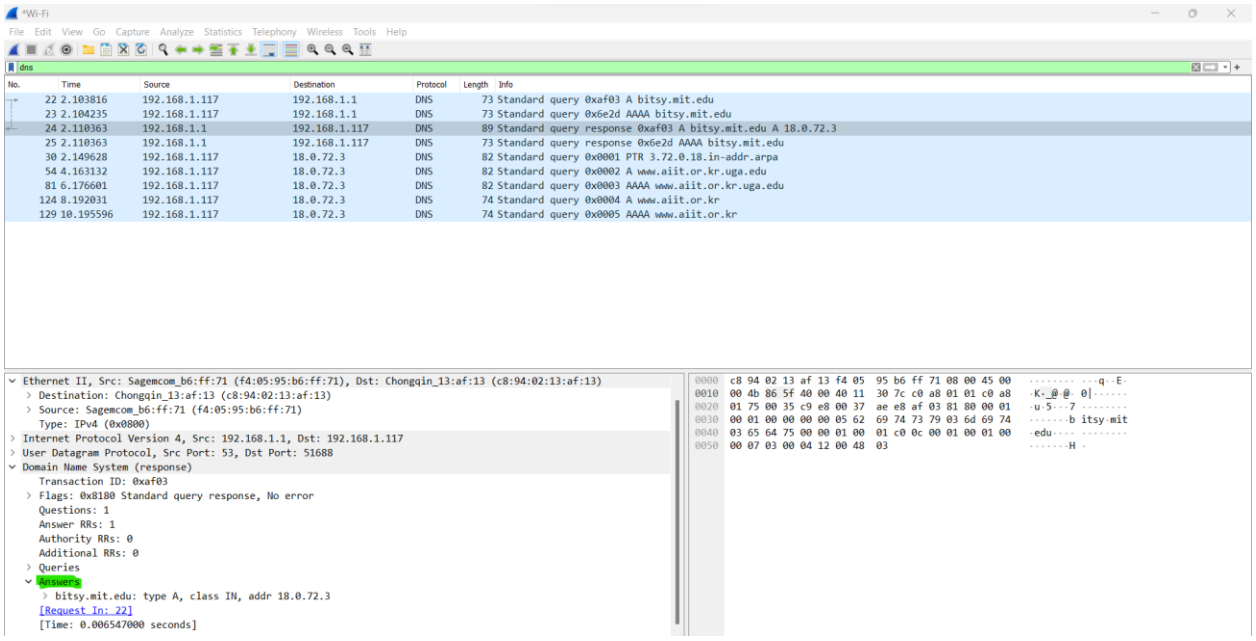


22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

For my DNS response message, one answer is provided. The answer contains type class and the address of the answer received.

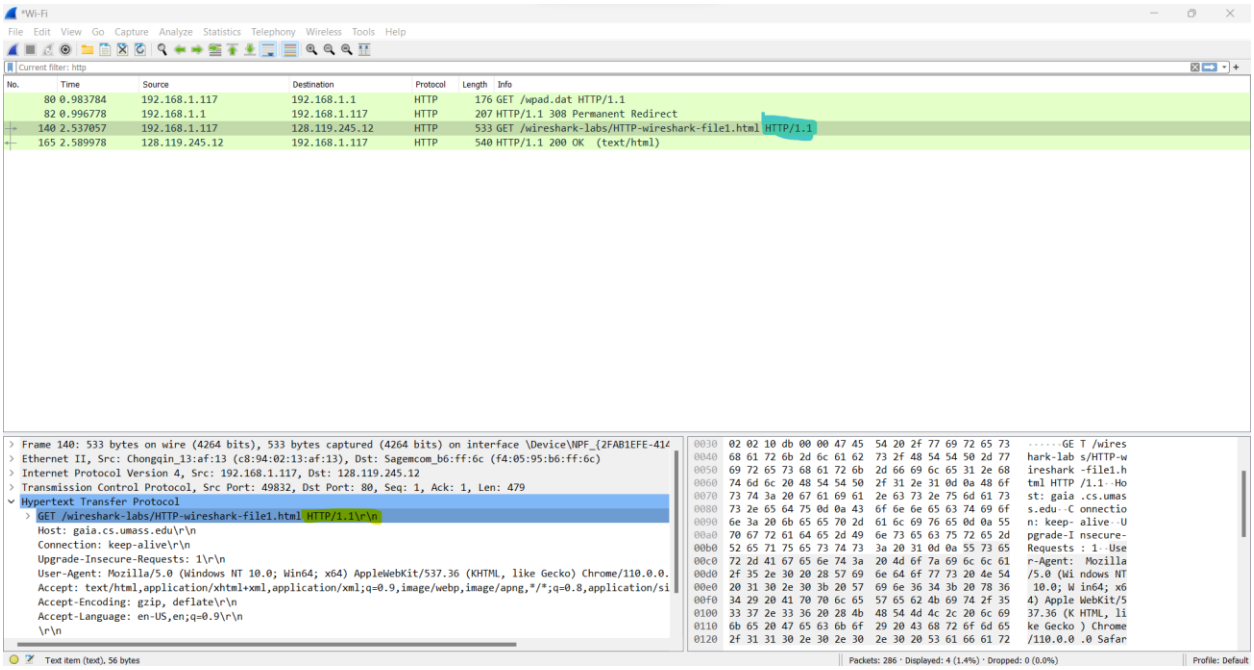


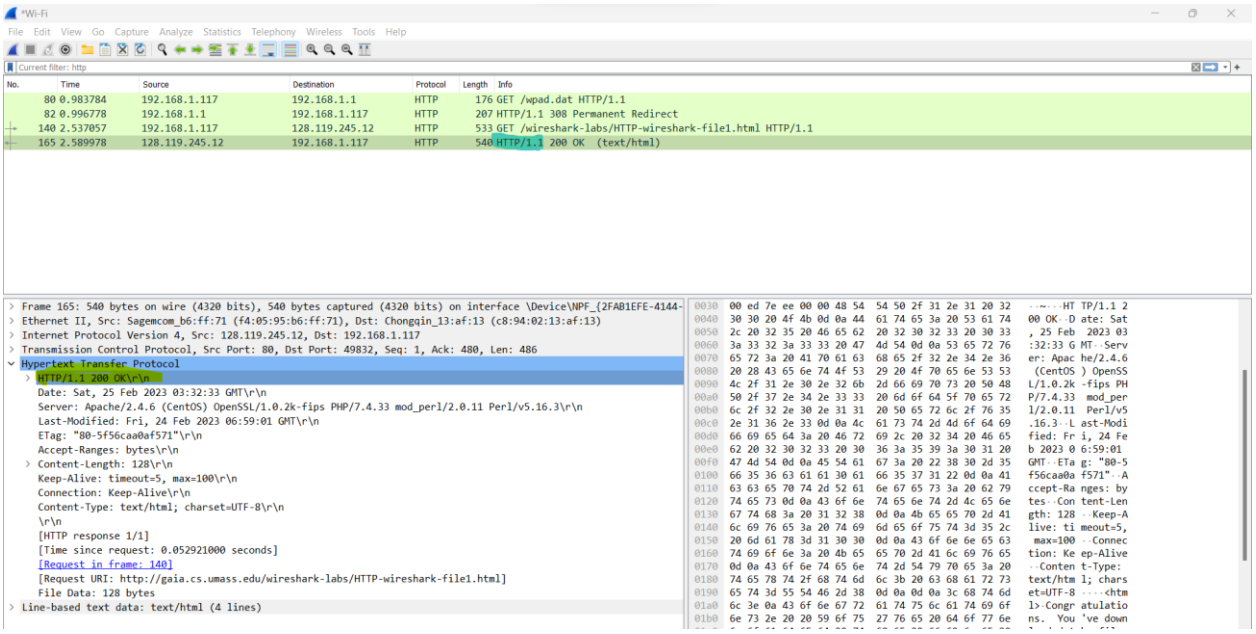
23. Provide a screenshot.



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

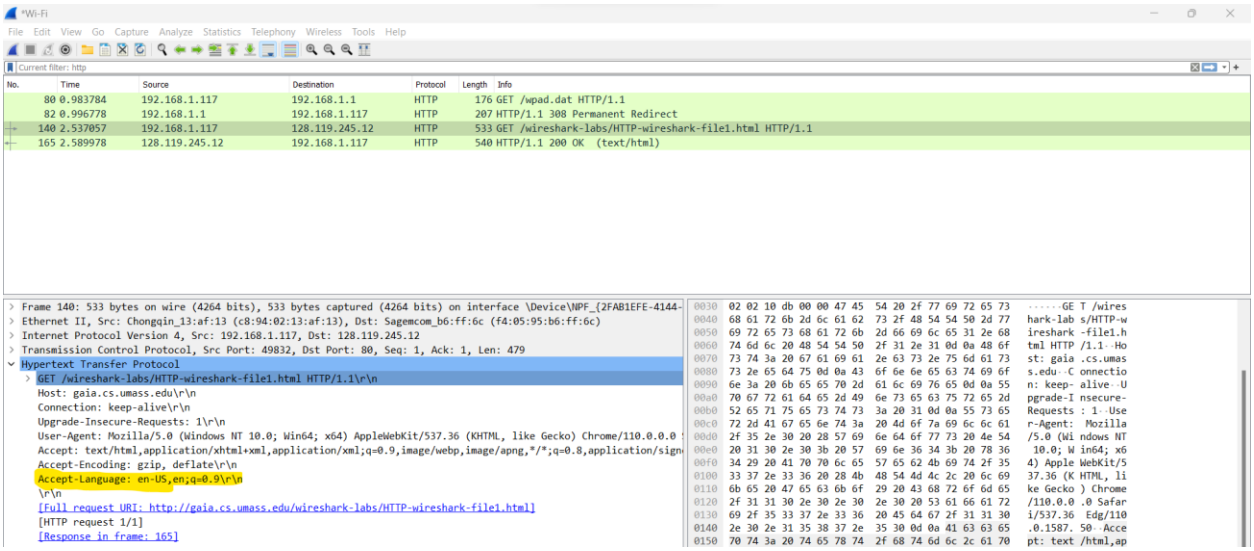
   The browser is running HTTP version 1.1. The HTTP version of the server is also 1.1.





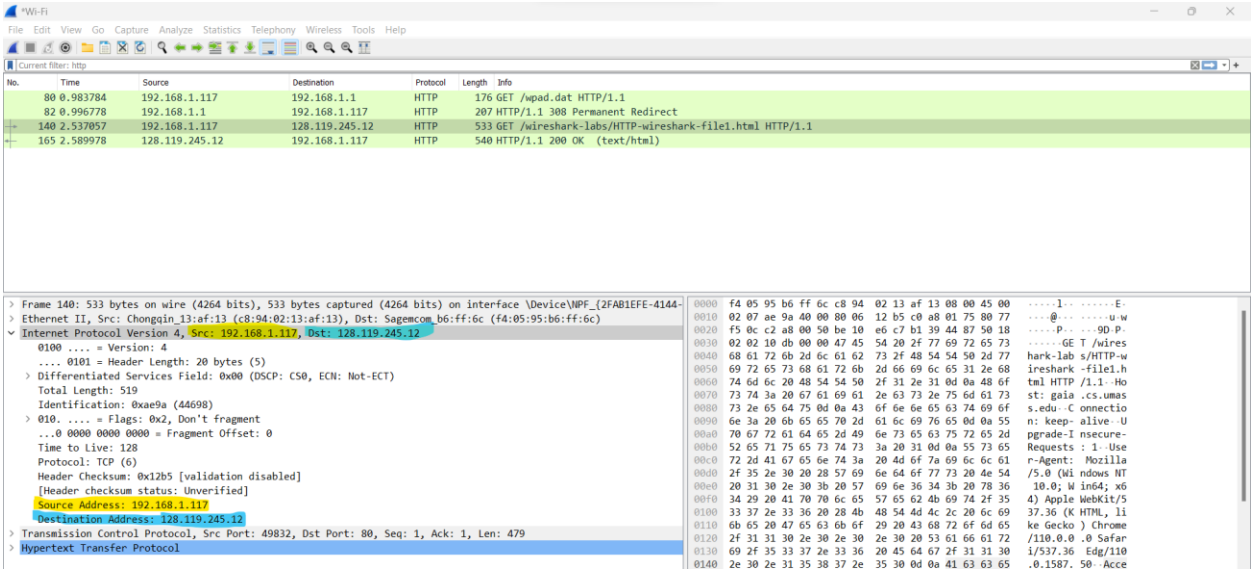
2. **What languages (if any) does your browser indicate that it can accept to the server?**

   The accepted language that is listed by browser is US English.



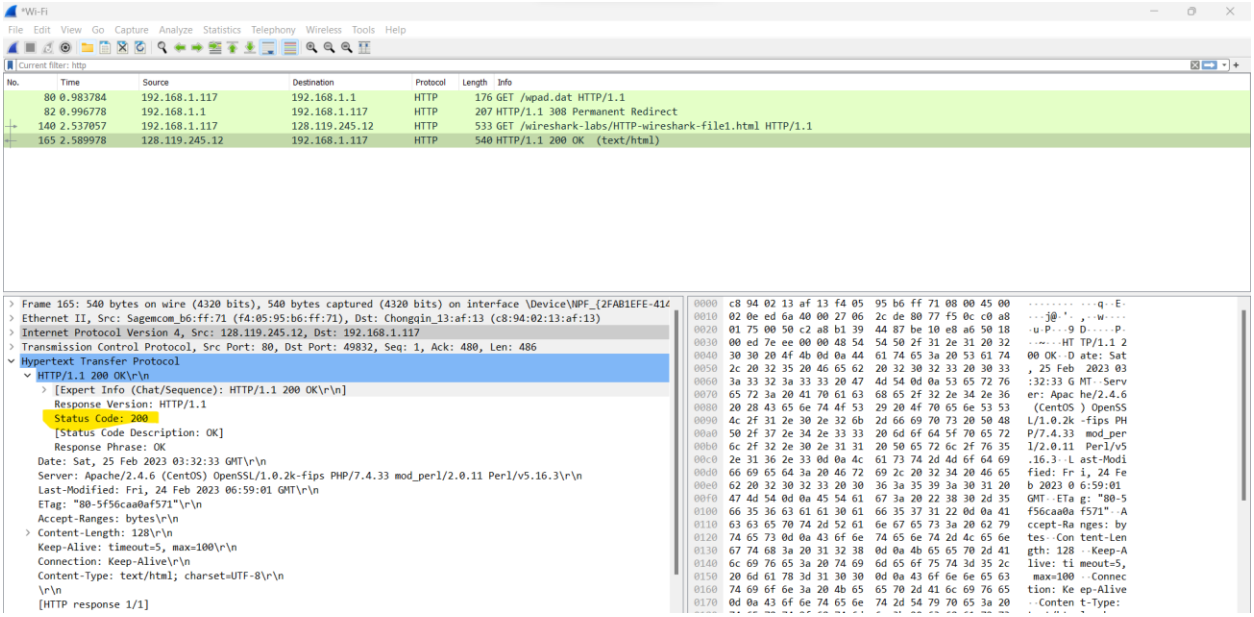
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

The IP address of my computer is 192.168.1.117 and the IP address of gaia.cs.umass.edu server is 128.119.245.12



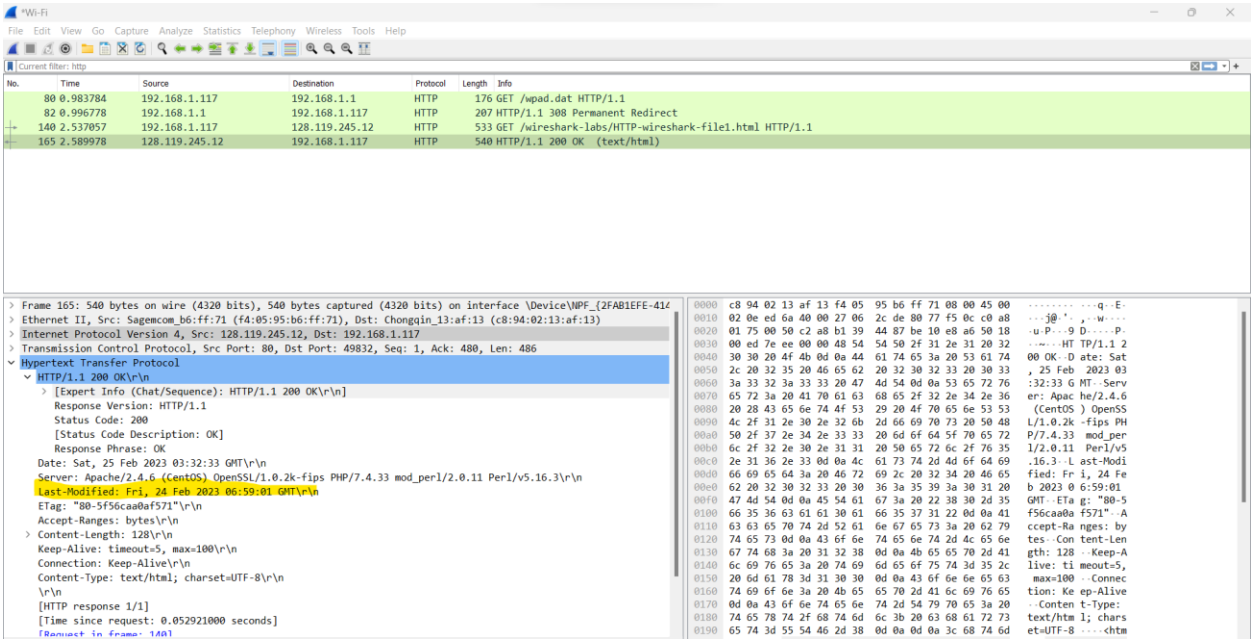
4. What is the status code returned from the server to your browser?

The status code returned from the server is 200 OK.



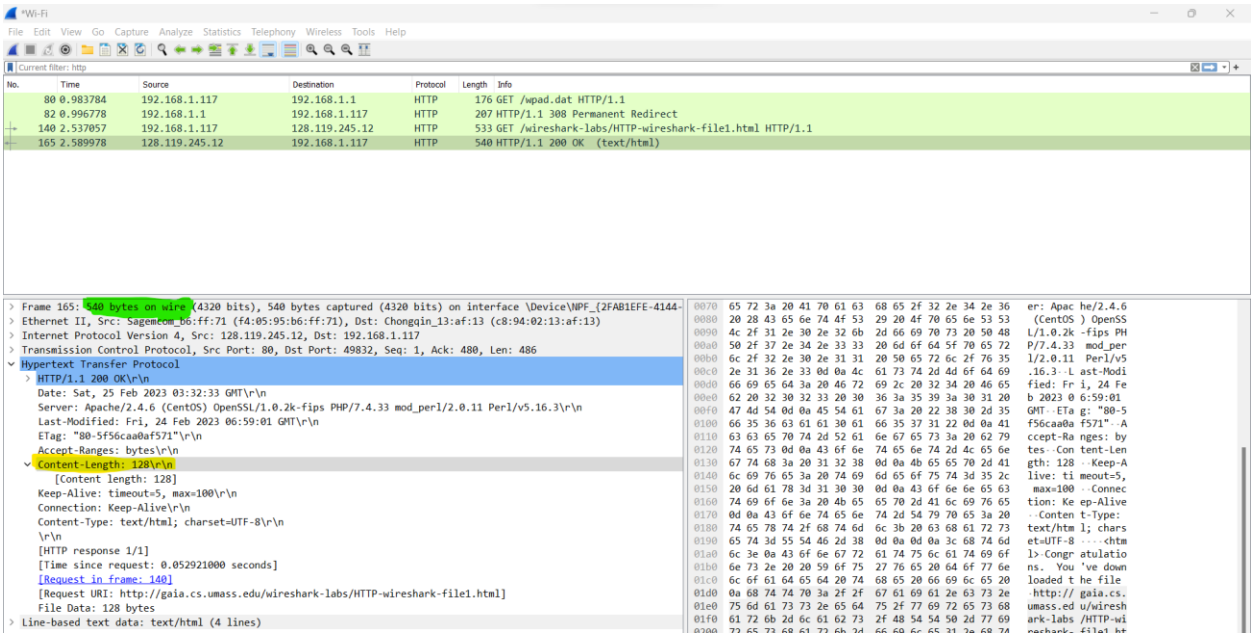
5. When was the HTML file that you are retrieving last modified at the server?

The last modified date of the HTML file is 24th February,2023 at 06:59:01 GMT\r\n



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

The frame is returning 540 bytes of data out of which the HTTP request to the server is returning 128 bytes to my browser.

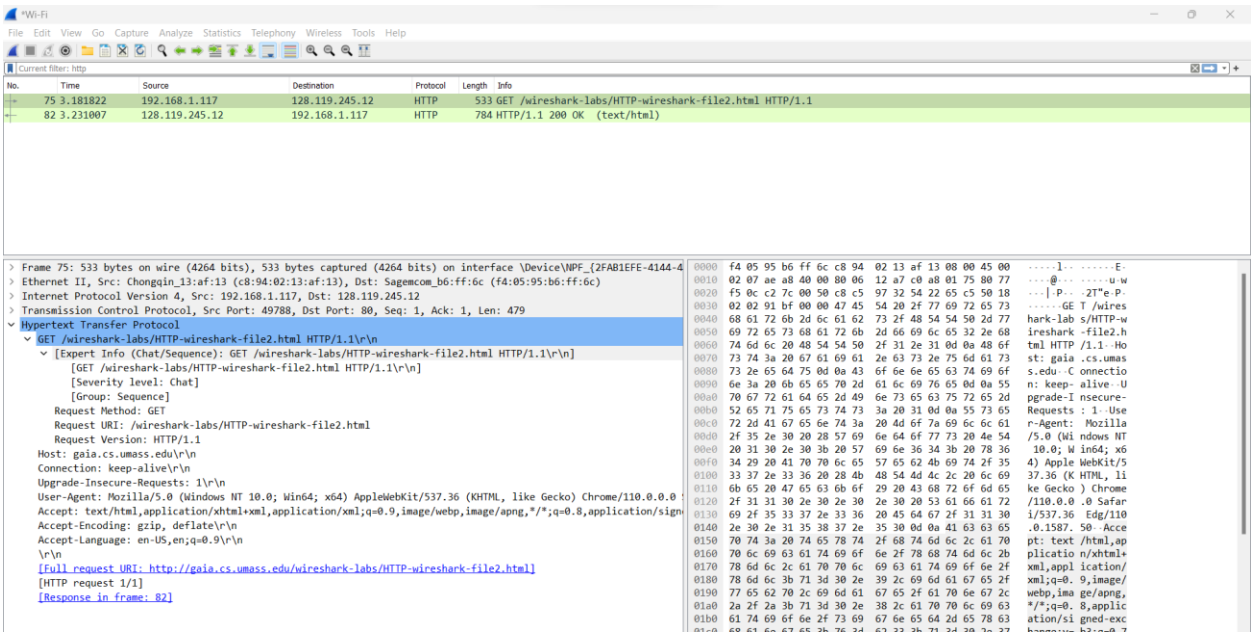


7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

There aren't any headers that are not displayed in the packet window.

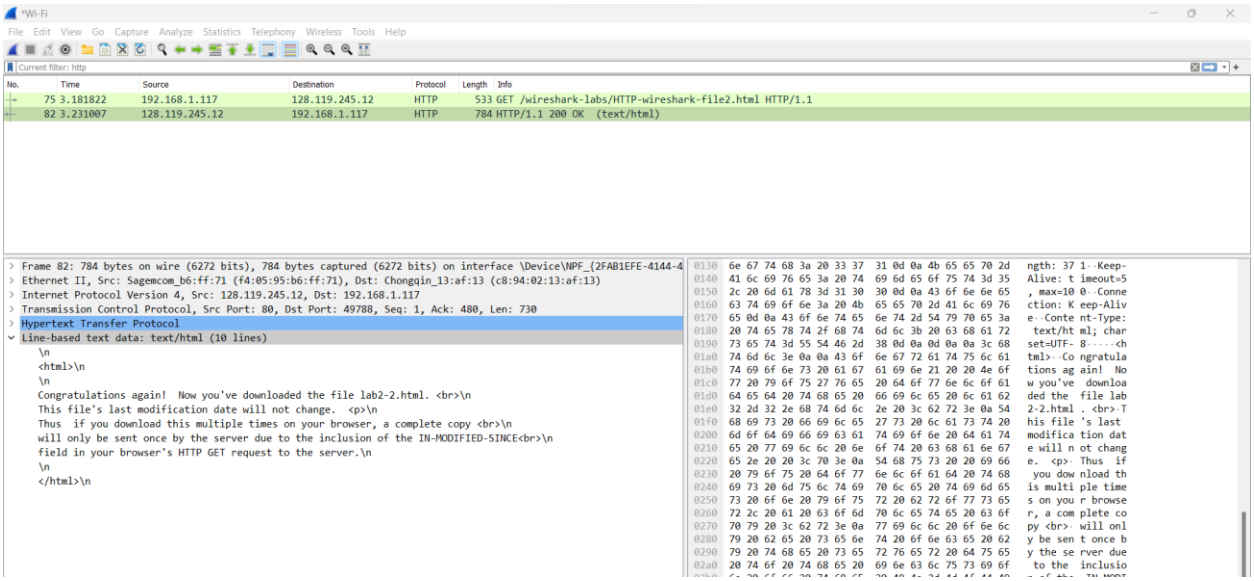
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

In the HTTP GET request there is no "IF-MODIFIED-SINCE".



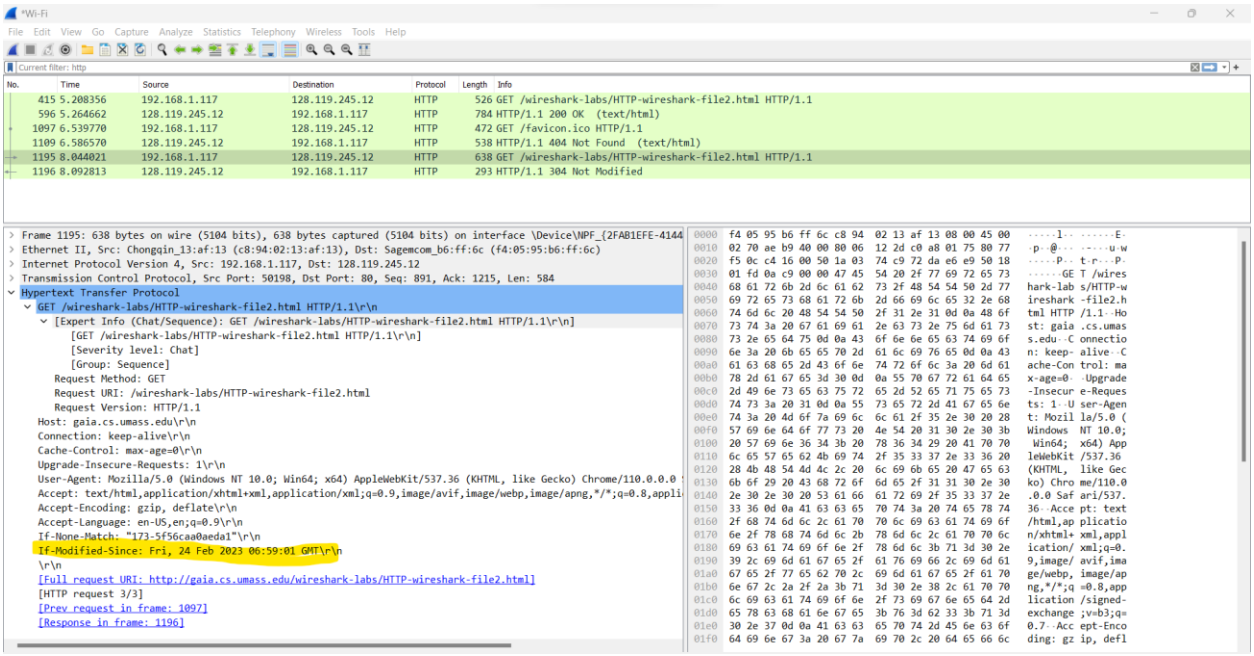
9. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**

The browser returned the contents of the file which are displayed under Line-based text data.



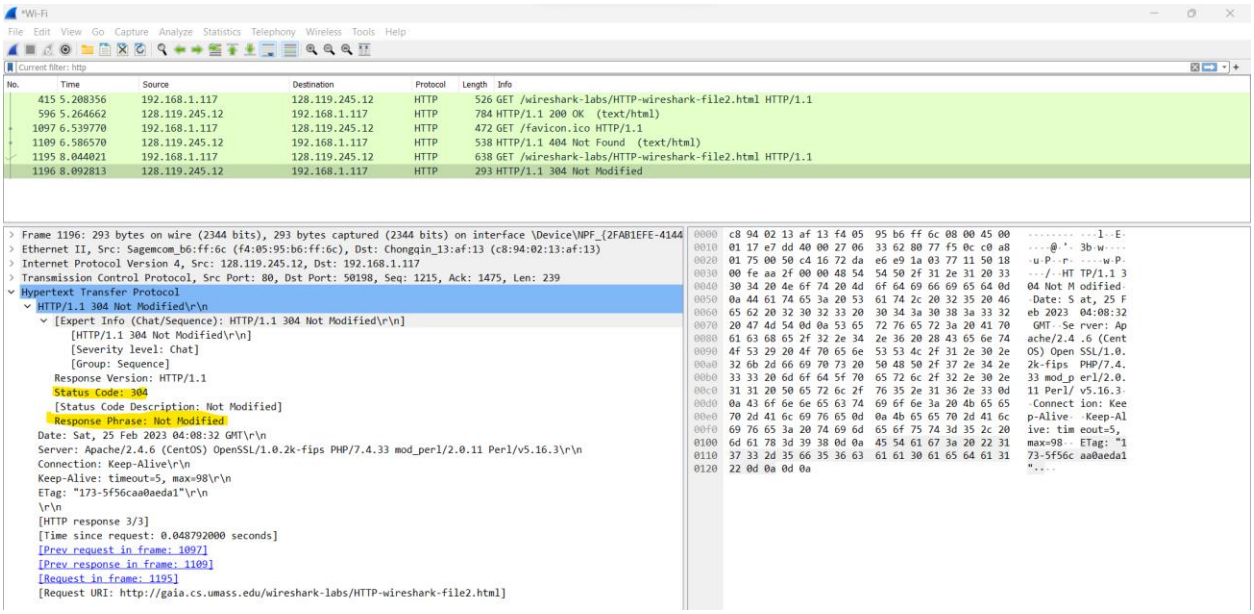
10. **Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?**

The second HTTP Get request contains the if-modified since line and it has the information about the date it was modified.



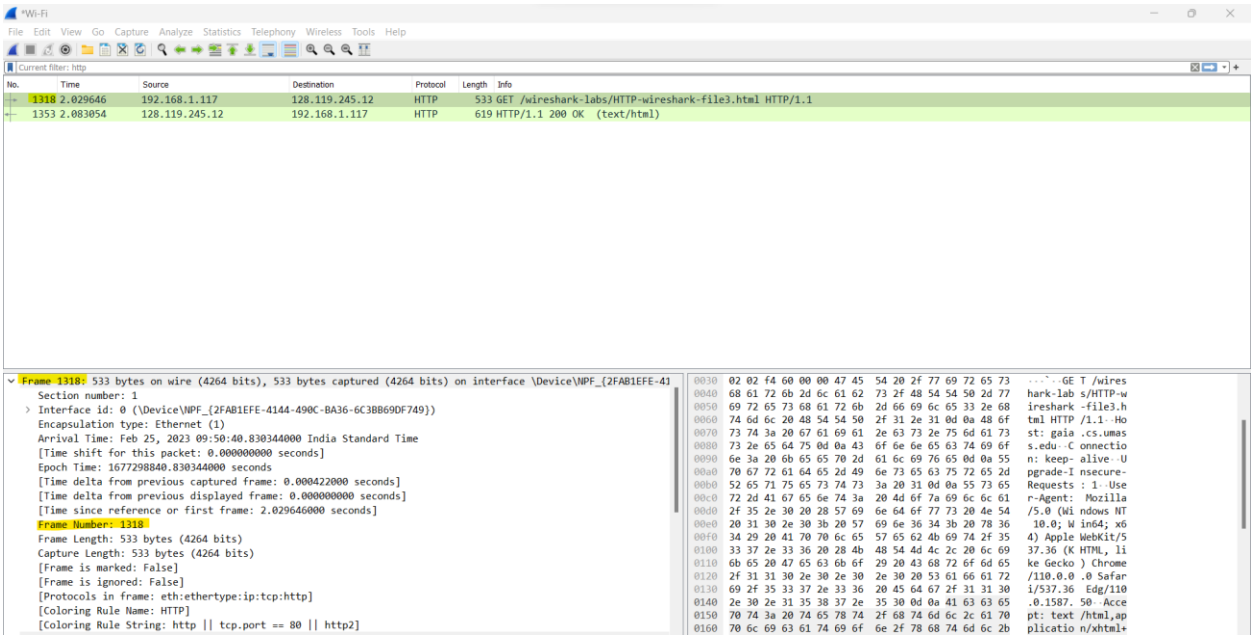
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The HTTP status code that the server responded with was a 304 Not Modified. This means that the server explicitly returned the contents of the file with no modifications made to the file that was returned.



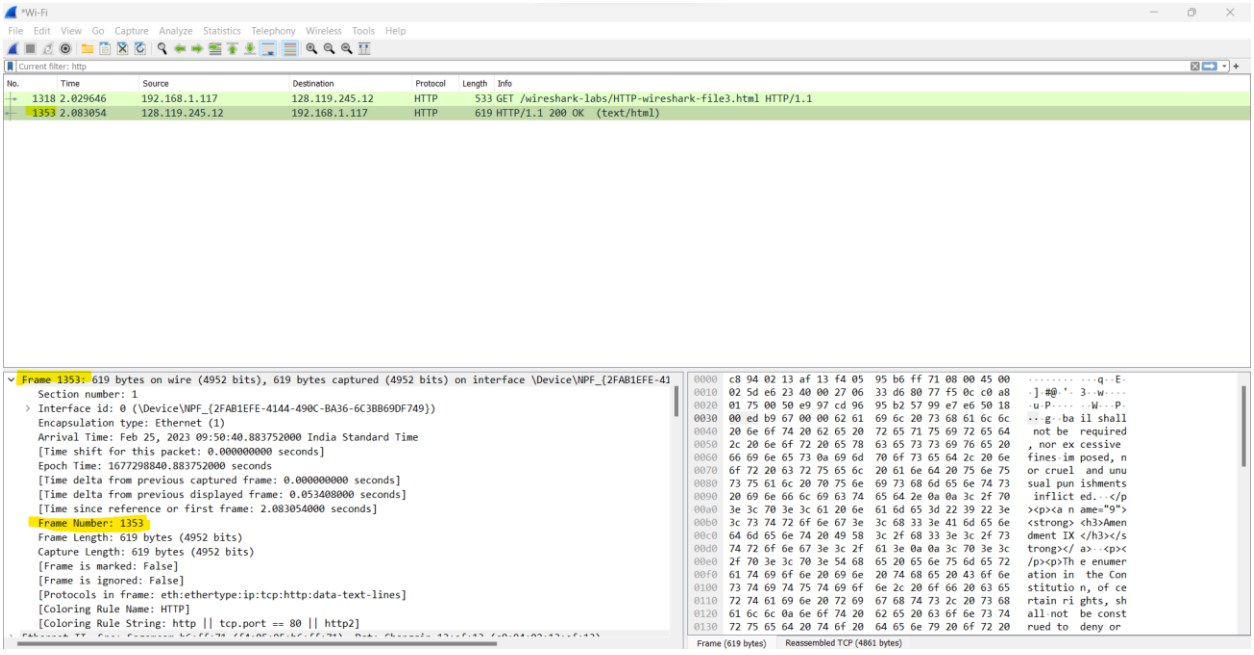
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

The browser sent only one HTTP GET request to the server. The packet number of the GET message in the trace is at 1318.



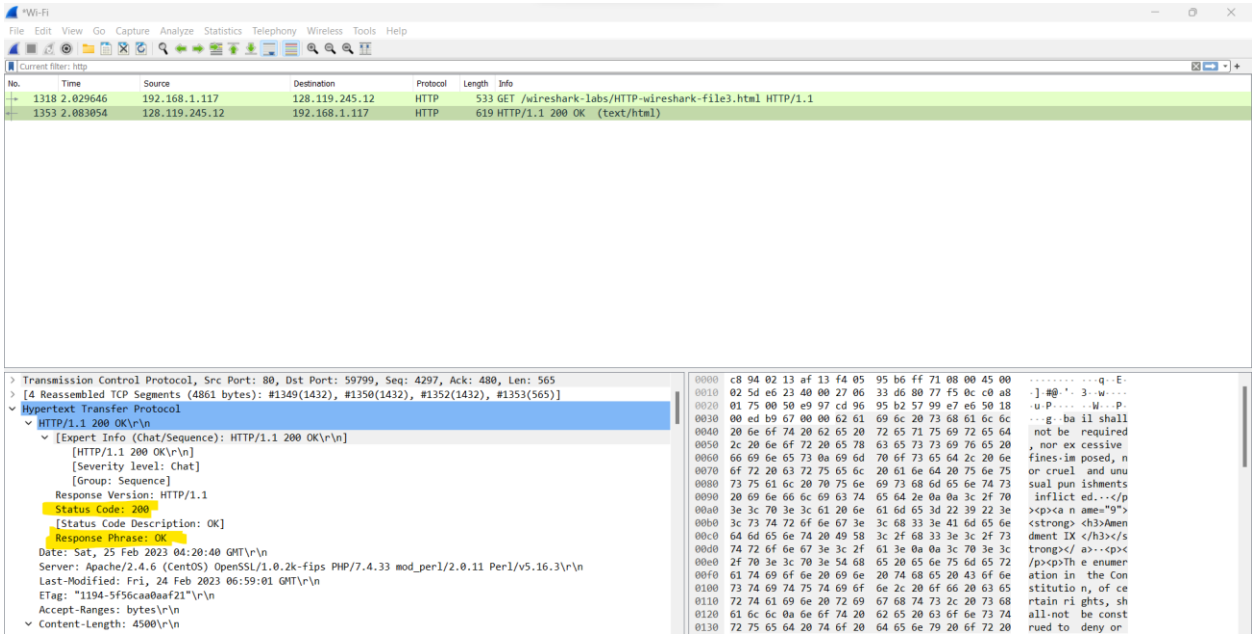
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

The packet number which contains the status code and phrase associated with the HTTP GET response is 1353.



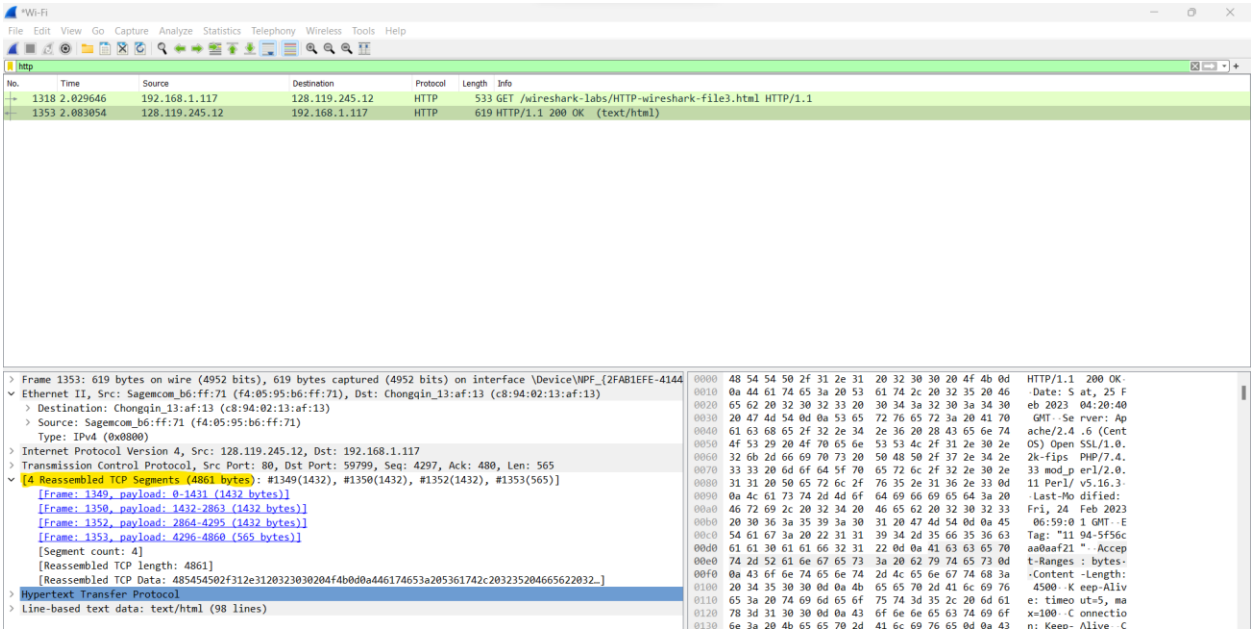
14. What is the status code and phrase in the response?

The status code of the response packet is 200, and the response phrase was “OK”.



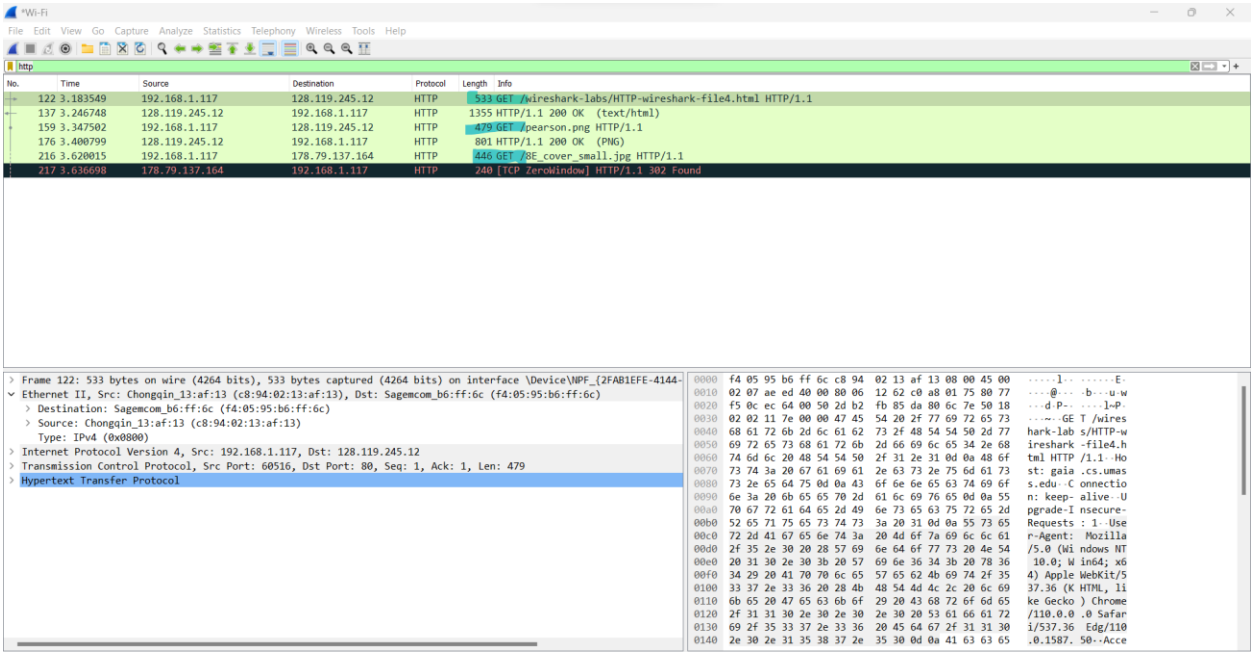
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

The HTTP response and the text of the Bill of Rights takes 4 data-containing TCP segments.



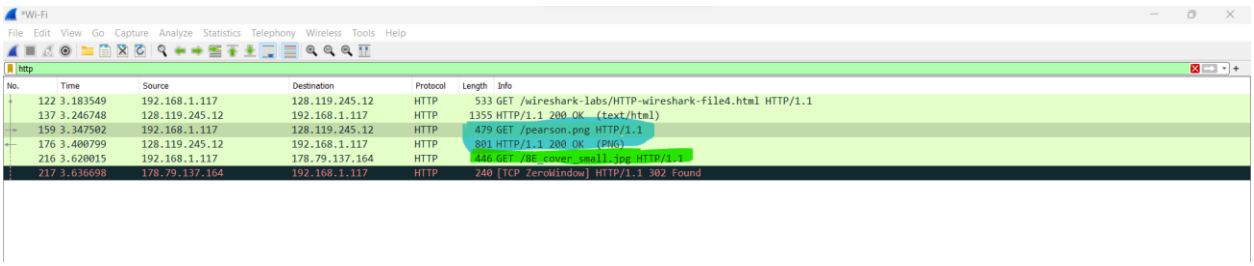
16. **How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent.**

    The browser sent 3 HTTP GET request messages to the server. The address to which the first two GET requests were sent are 128.119.245.12. The last GET request was sent 178.79.137.164



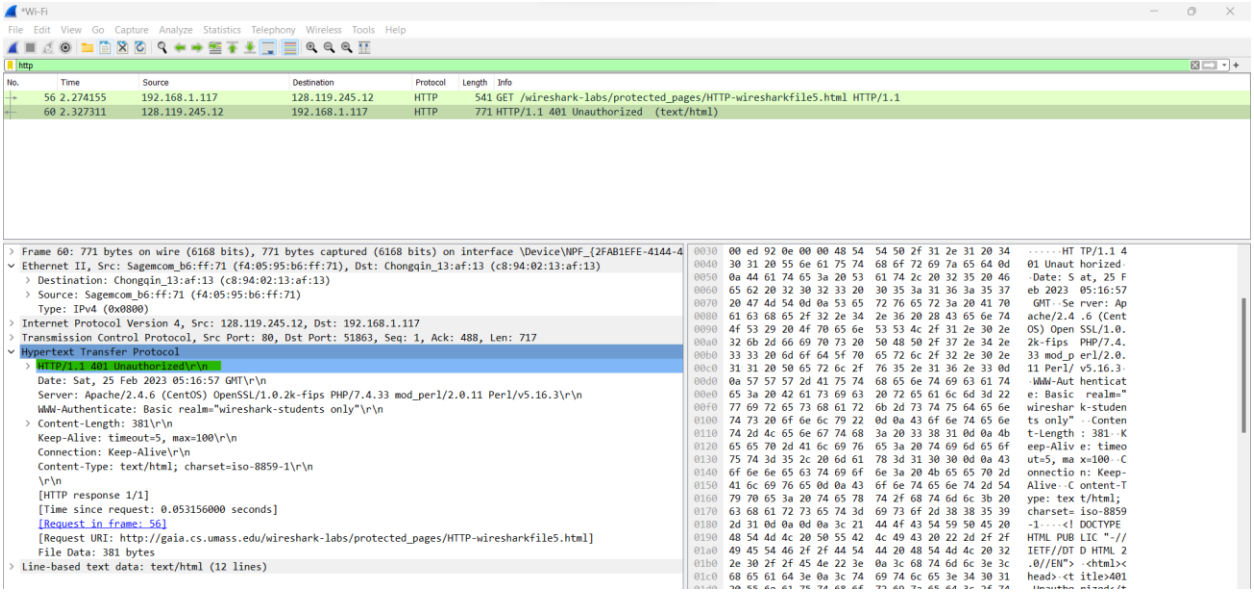
17. **Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**

    The browser downloaded the two images ***serially*** which is evident from the request and response messages received in the trace. For the first image a http get and response was done after which the next request for second image was sent.



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

The server's response to my HTTP GET message is a 401 with "Unauthorized phrase".



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 that is included in the HTTP GET message is the Authorization field as Authorization: Basic ZHE6YWZzYWE