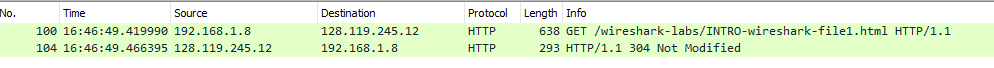
Nicholas Shari - CSE422 - Project#3

1.4

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

TCP, HTTP,TLSv1, UDP

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.)



0.05sec

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

My Computer: 192.168.1.8

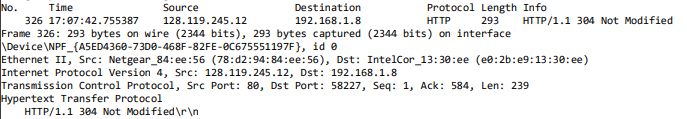
Gaia: 128.119.245.12

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

2.1

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





Both HTTP 1.1

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

Line:19

 English-US

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

Line 2 Source: My Computer: 192.168.1.8

Line 2 Destination: Gaia: 128.119.245.12

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



Line 27: 304 Not Modified

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



Line 35: 22:07:04 GMT

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



Line 28: 293 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.

None.

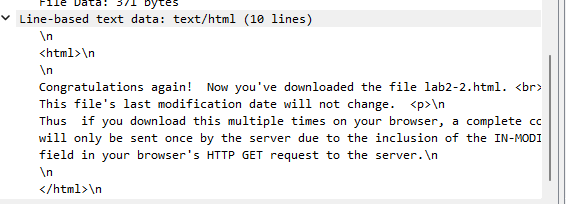
2.2

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.

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

Yes. In the Line-based Text data:

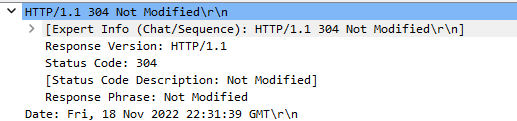


10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Yes. The date and time since I last accessed the page.



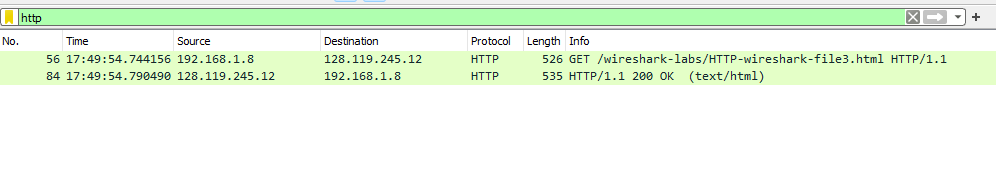
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



Status code: 304 Not Modified

The server has not modified the contents of the file since my last request.

2.3



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

My browser sent 1 GET. With packet number 56

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

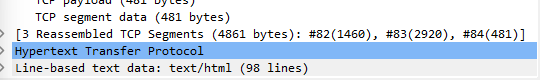
The response packet was 84.

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



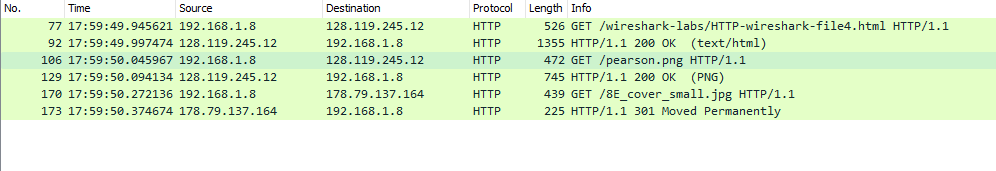
The status code and phrase was 200 OK.

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



3 Segments

2.4



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

3 requests

128.119.245.12 wireshark-labs

128.119.245.12 pearson

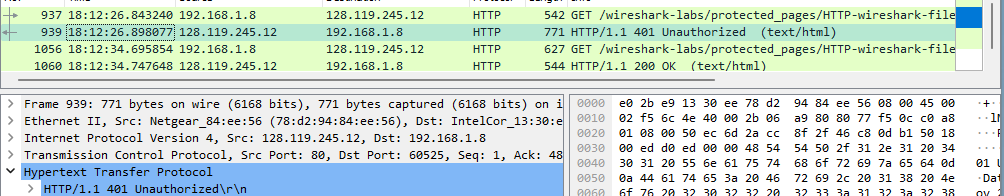
178.79.137.164 8E\_cover

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

Serially. The first image was requested and returned. Then the second image was requested then returned.

2.5

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



401 Unauthorized

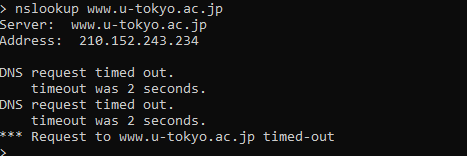
19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?



Authorization

3.1

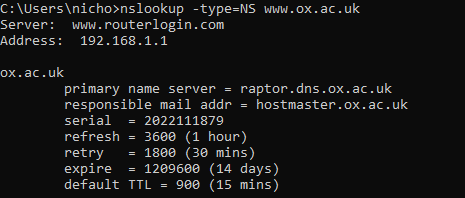
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the hostname and IP address of that server?



Hostname: [www.u-tokyo.ac.jp](http://www.u-tokyo.ac.jp)

IP: 210.152.243.234

2. Run nslookup to determine the authoritative DNS servers for a university in Europe. What University did you query for and what was the domain name you used? List two of the hostnames and IP addresses of the servers indicated in the response.

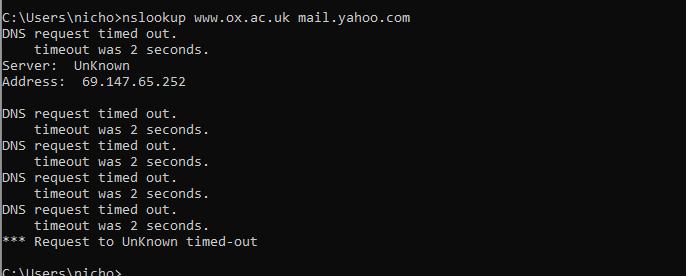


University of Oxford domain: [www.ox.ac.uk](http://www.ox.ac.uk)

Primary name server = raptor.dns.ox.ac.uk

Responsible mail addr = hostmaster.ox.ac.uk

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What kind of response do you get?

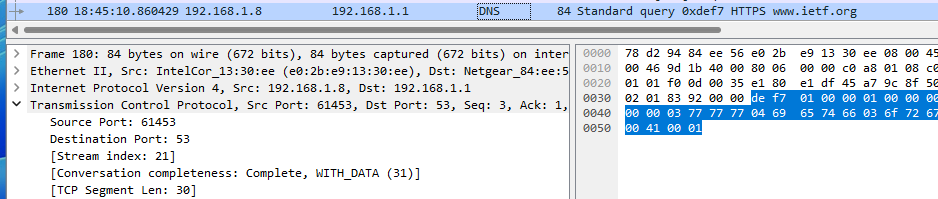


Server unknown, multiple timeouts

3.3

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

TCP

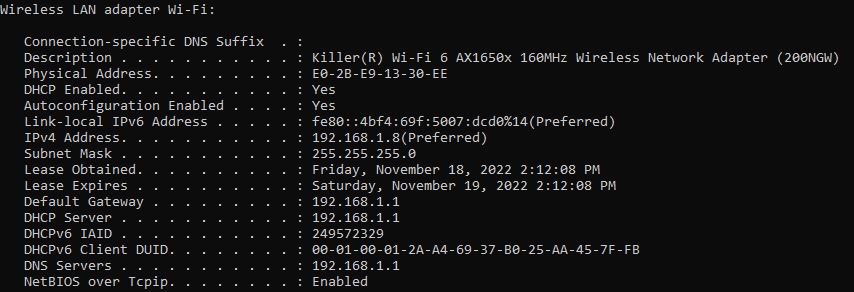


5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Destination of dns query: 53

Source port of dns response: 61453

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?



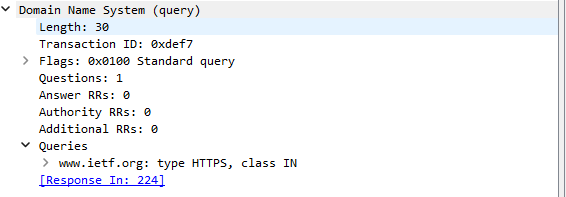
Local dns : 192.168.1.1



DNS query sent to: 192.168.1.1

My local dns and the query IP address were the same.

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

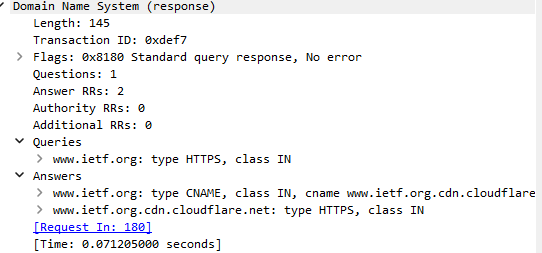


Type: HTTPS

Answers: 0

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

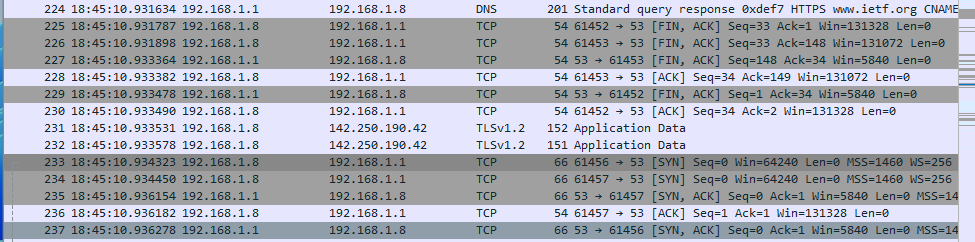




Answers: Two answers

The names of the sites.

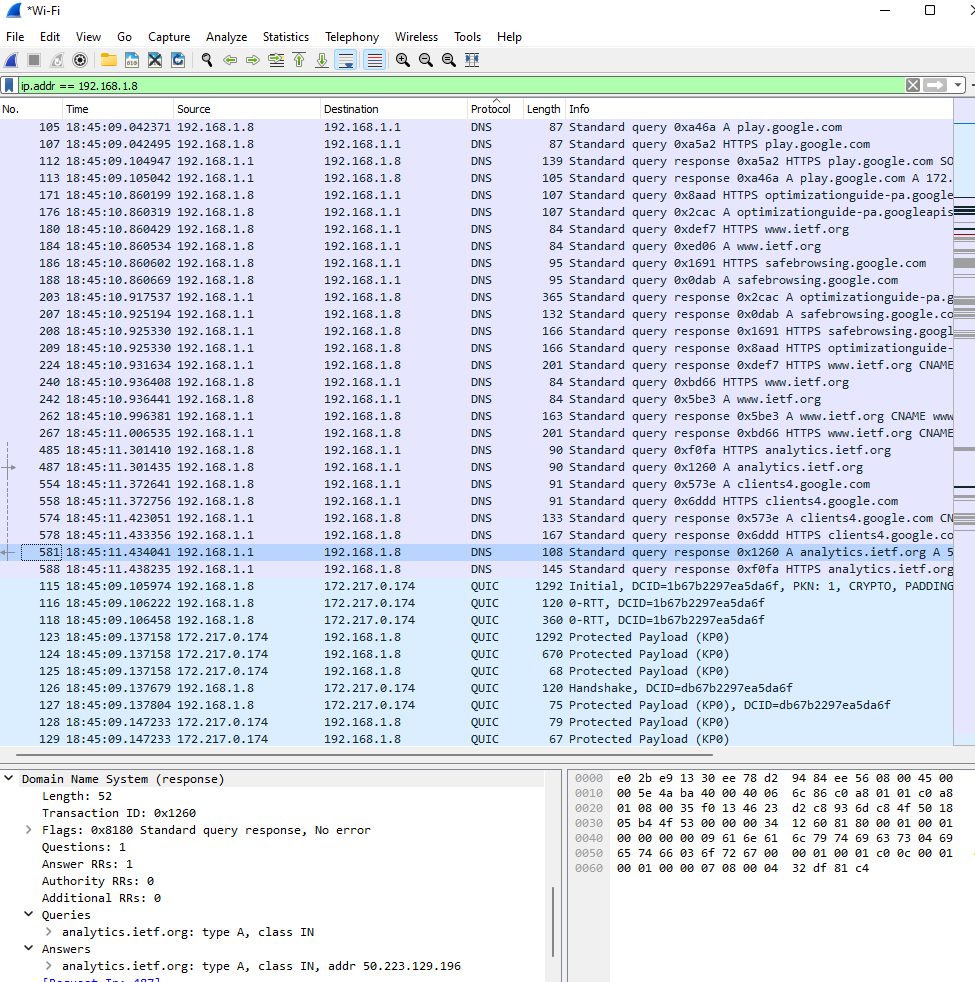
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

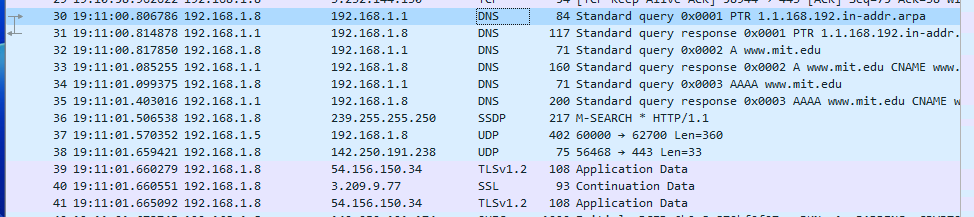


The designation of the SYN is the same as the DNS response. 192.168.1.8

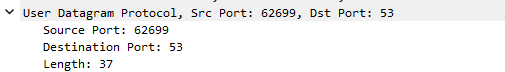
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No. My computer didn’t make any have any HTTP or GET requests

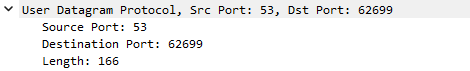




11. What is the destination port for the DNS query message? What is the source port of DNS response message?

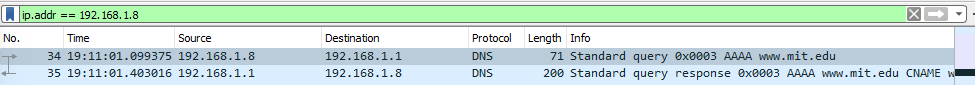


Query Destination port: 53



DNs response source port: 53

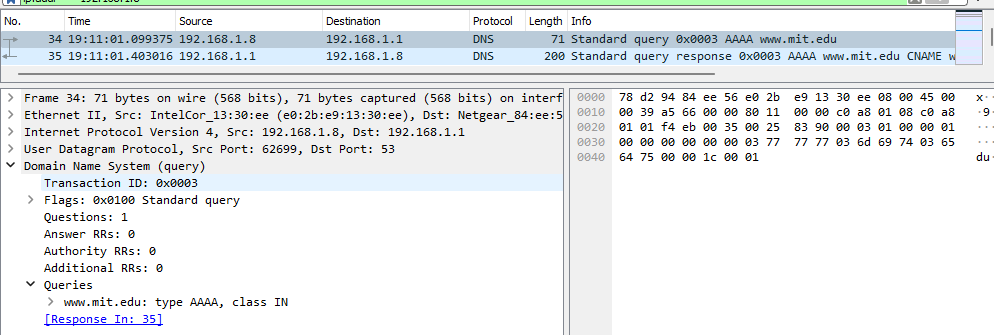
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



Query destination: 192.168.1.1

Yes. My local dns is the same.

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



Type: AAAA

No answers

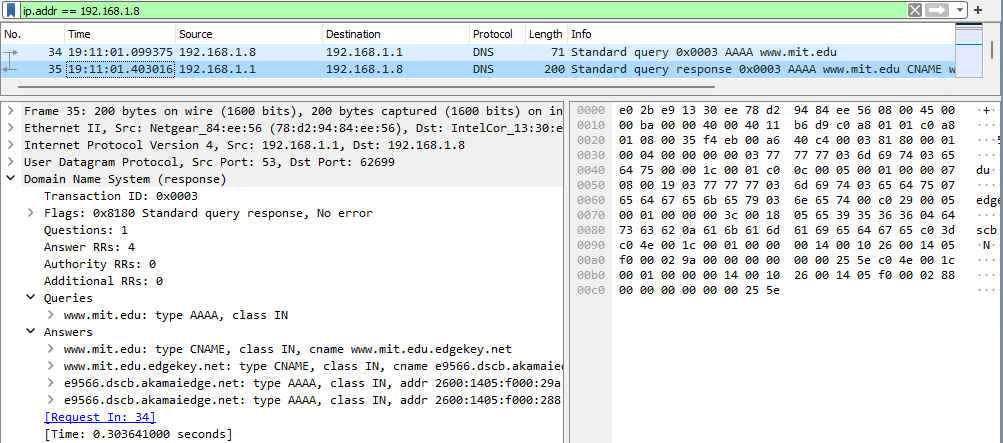
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answers: 4

The answers are the address of the query “[www.mit.edu](http://www.mit.edu)”

And 3 authoritative name servers.

15. Provide a screenshot.





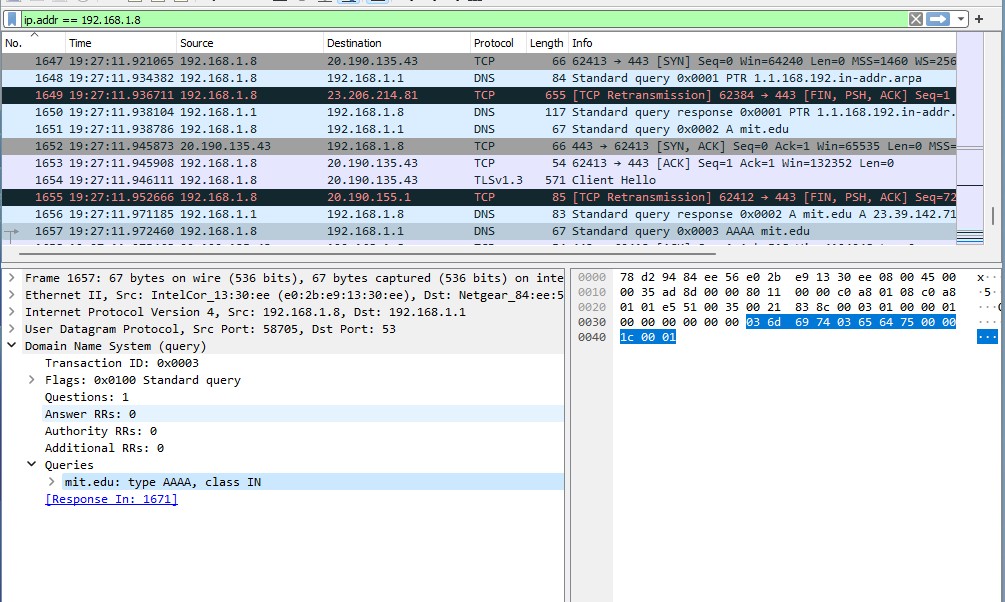


16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

DNS Query: 192.168.1.1

My local default dns: 192.168.1.1

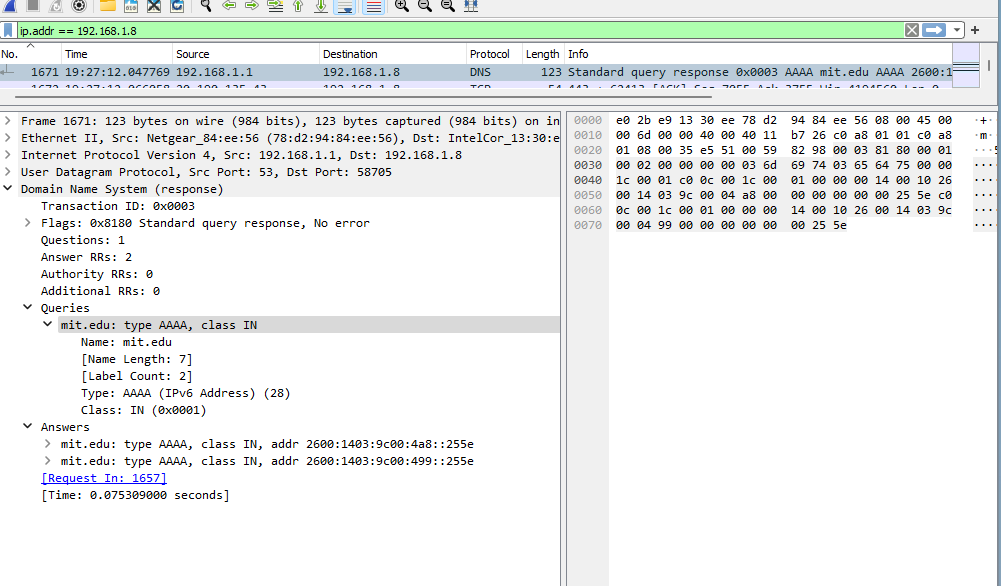
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



Type: AAAA

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 namesers?



MIT Nameservers:

It provides two “mit.edu” names

Along with their IPv6 address: 2600:1403:9c00:499::255e

19. Provide a screenshot.

