Manish Yadav
3836-6483
m.yadav@ufl.edu

Homework 1

CNT5106C : Fall 2020 : Dr. Ye Xia
Due Tue, Sept 15, 2020

Contents

Problem 1

(a)

A user requests a Web page that consists of some text and three images. For this page, the client will send one request message and receive four response messages

Answer

False. Only Single response would be received.

(b)

Two distinct Web pages (for example, www.mit.edu/research.html and www.mit.edu/students.html) can be sent over the same persistent connection.

Answer

True. With persistent connections, the server leaves the TCP connection open after sending responses and hence the subsequent requests and responses between the same client and server can be sent.

(c)

With nonpersistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages.

Answer

False. A single TCP segment can carry only single request/response.

(d)

The `Date: header` in the HTTP response message indicates when the object in the response was last modified.

Answer

False. The date and time at which the message was originated (in "HTTP-date" format as defined by RFC 7231 Date/Time Formats).

(e)

HTTP response messages never have an empty message body.

Answer

False. Not all responses have one: responses with a status code that sufficiently answers the request without the need for corresponding payload (like 201 Created or 204 No Content) usually don't.

Problem 2

Consider an HTTP client that wants to retrieve a Web document at a given URL. The IP address of the HTTP server is initially unknown. What transport and application-layer protocols besides HTTP are needed in this scenario

Answer

In order to receive a web document from a given URL, its IP address needs to be resolved. This is done using DNS. Once the URL is resolved a subsequent request is made to fetch Web document.
Transport Layer Protocol Used: UDP(DNS) and TCP (HTTP)
Application Layer Protocol Used: DNS and HTTP

Problem 3

Consider Figure 2.12 , for which there is an institutional network connected to the Internet. Suppose that the average object size is 850,000 bits and that the average request rate from the institution's browsers to the origin servers is 16 requests per second. Also suppose that the amount of time it takes from when the router on the Internet side of the access link forwards an HTTP request until it receives the response is three seconds on average (see Section 2.2.5). Model the total average response time as the sum of the average access delay (that is, the delay from Internet router to institution router) and the average Internet delay. For the average access delay, use $\Delta/(1-\Delta\beta)$, where Δ is the average time required to send an object over the access link and b is the arrival rate of objects to the access link.

(a)

Find the total average response time.

Answer

Time required = L/R = $\frac{850000}{15{,}000{,}000} = 0.0567s$
Traffic Intensity = $16 * 0.0567 = 0.907$
Therefore, average access delay = $\frac{0.0567}{1-0.907} = 0.6s$
The total average response time = $0.6 + 3 = 3.6s$

(b)

Now suppose a cache is installed in the institutional LAN. Suppose the miss rate is 0.4. Find the total response time.

Answer

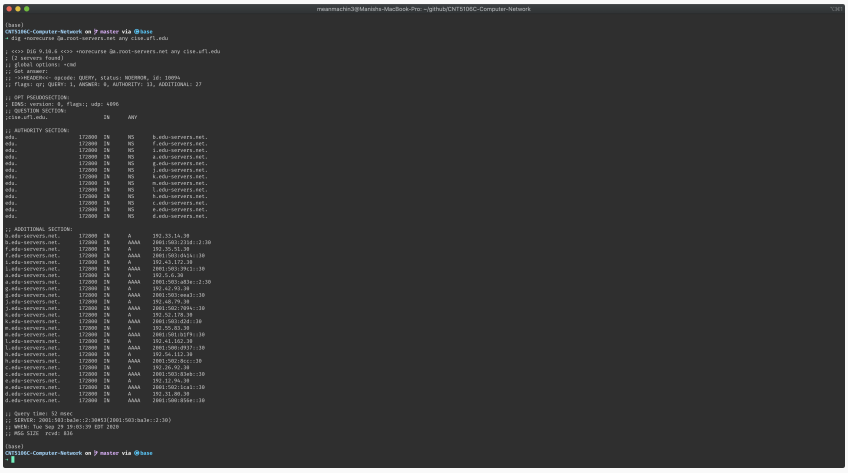
Average access delay = $\frac{\Delta}{1-\beta\Delta} = \frac{0.0567}{1-0.4*16*0.0567} = 0.089$
Average response time from cache misses = 3 + 0.089 = 3.089s
Total average response time is 0.6 * 0 + 0.4 * 3.089 = 1.24s
Due to cache hit, response time is 0 and average response time is reduced from 3.6s to 1.24s.

Problem 4

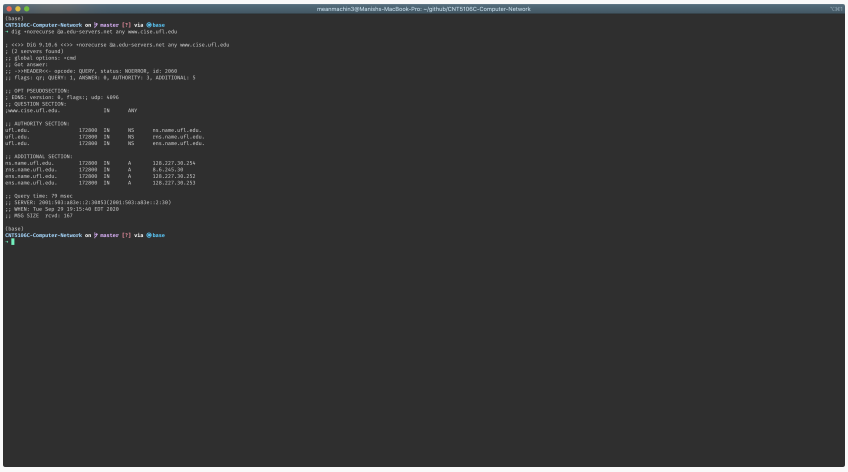
a

Answer

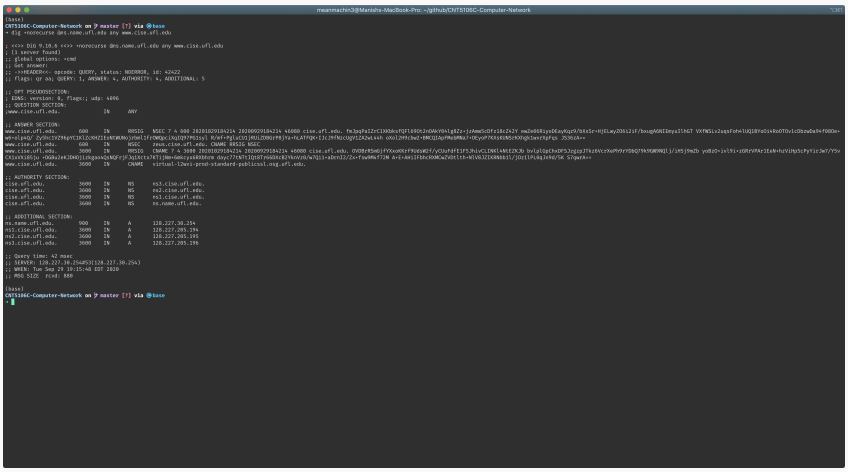
```
dig +norecurse @a.root-servers.net any cise.ufl.edu
```



```
dig +norecurse @a.edu-servers.net any www.cise.ufl.edu
```



```
dig +norecurse @ns.name.ufl.edu any www.cise.ufl.edu
```

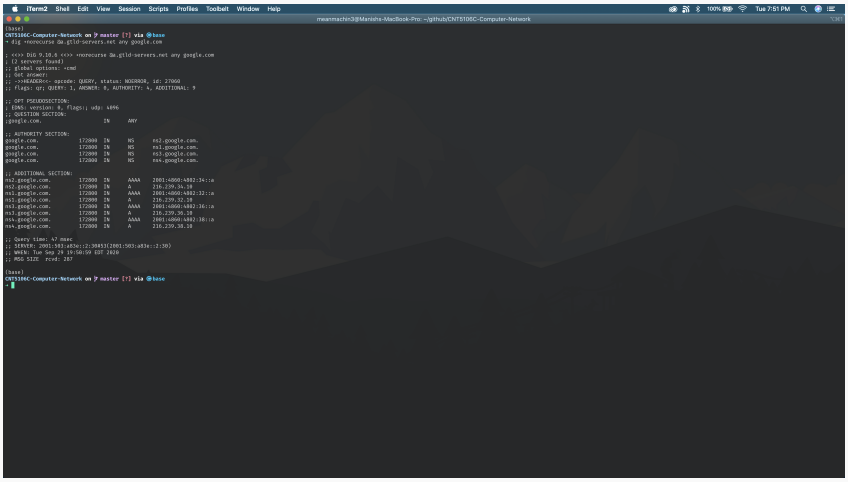


Problem 4 continued on next page. . .

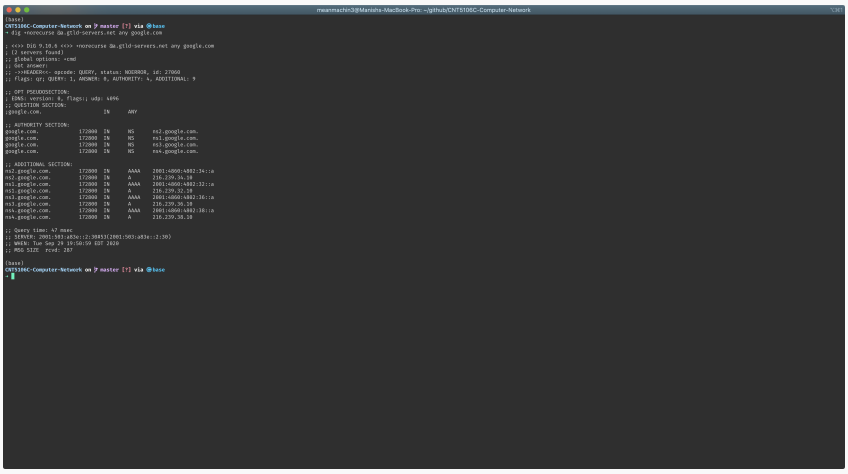
b

Answer

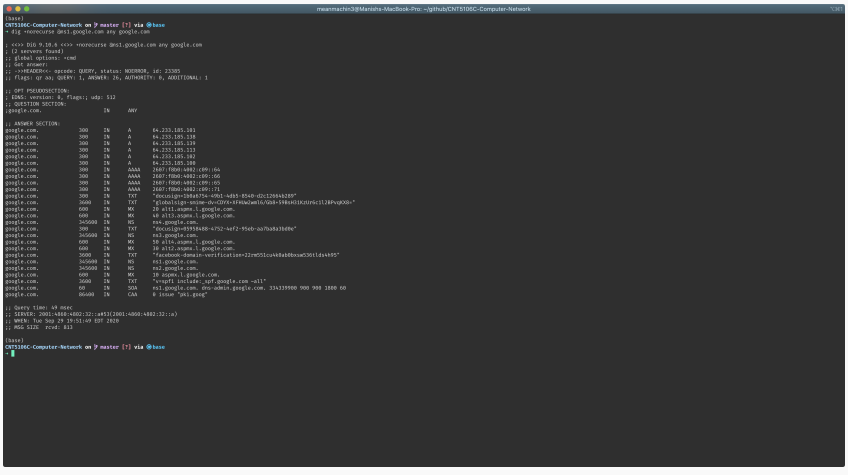
`dig +norecurse @a.root-servers.net any google.com`



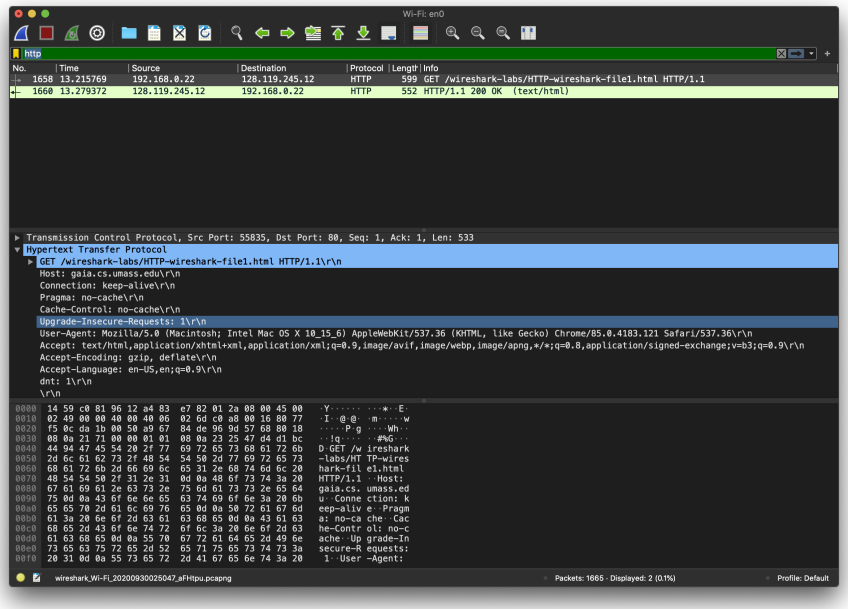
`dig +norecurse @a.edu-servers.net any google.com`



`dig +norecurse @ns1.google.com any google.com`



Problem 5



1

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

Answer

Both run 1.1.

2

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

Answer

US English (en-US) and other types of English (en)

3

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

Answer

Internal IP address of my computer: 192.168.0.22
External IP address of my computer: 70.171.35.146
IP address of Server: 128.119.245.12

4

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

Answer

200 (OK).

5

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

Answer

Last-Modified: Wed, 30 Sep 2020 05:59:02 GMT (As per HTTP Response)

6

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

Answer

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.

Answer

No.

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?

Answer

No

9

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

Answer

Yes. Server returned the content of webpage in html format.

```
 <html> Congratulations again!  Now you've downloaded the file lab2-2.html.
<br> This file's last modification date will not change.  <p> Thus if you
download this multiple times on your browser, a complete copy <br> will only
be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
```

```
field in your browser's HTTP GET request to the server.</html>
```

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?

Answer

Yes. If-Modified-Since: Wed, 30 Sep 2020 05:59:02 GMT (Request date time)

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.

Answer

HTTP/1.1 304 Not Modified. No the server didn't explicitly returned the content of the file. The contents of the file were picked up from the browser cache.

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?

Answer

My Browser sent 1 `HTTP` Request. Packet No 3605 contains `GET` request.

13

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

Answer

Packet No 3610

14

What is the status code and phrase in the response?

Answer

HTTP/1.1 200 OK

15

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

Answer

4

16

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

Answer

3. All request were made to 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.

Answer

As per timestamp images appear to be downloaded serially. Since image 2 requested only after the response of image 1 was completed.

18

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

Answer

HTTP/1.1 401 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?

Answer

Cache-Control: max-age=0
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

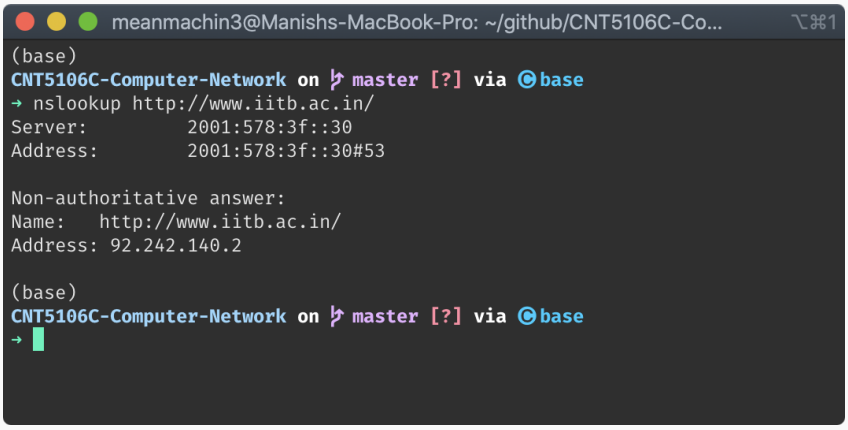
Problem 6

1

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

Answer

IP address of the server is `92.242.140.2`



2

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

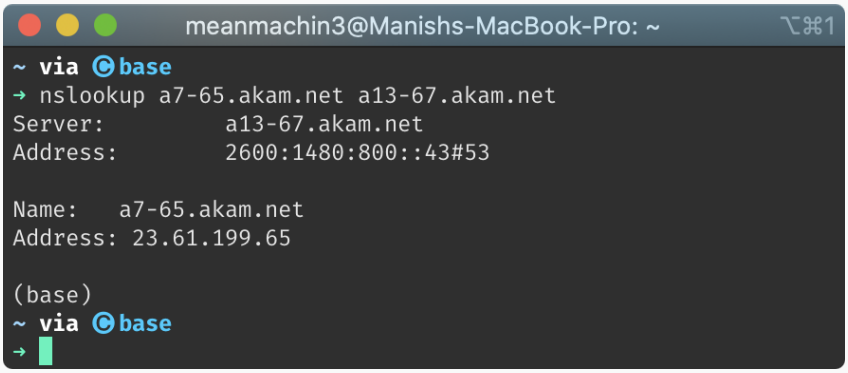
Answer

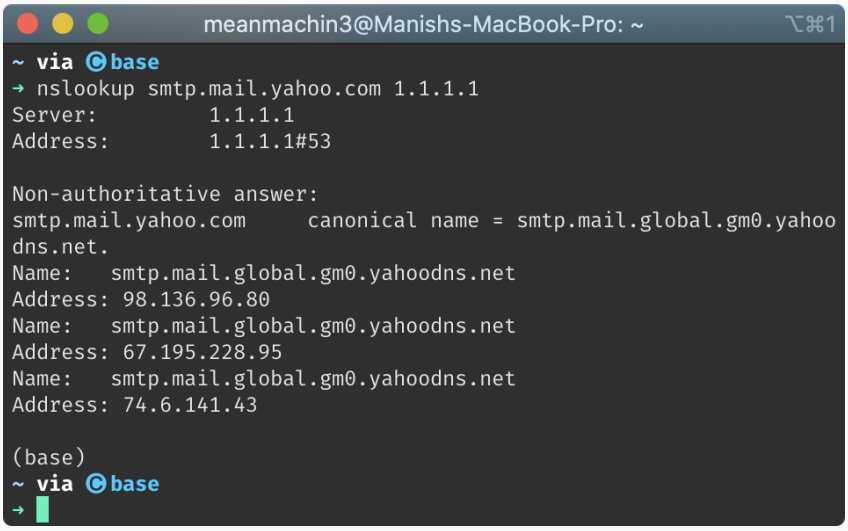
3

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?

Answer

I was unable to get response for `smtp.mail.yahoo.com/imap.mail.yahoo.com/mail.yahoo.com` and `yahoo.com` so I queried another DNS server with their DNS server. Apart from this, I also queried `smtp.mail.yahoo.com` with a public DNS and got a response. It is clear that Private DNS by European University are unable to query sites like `yahoo.com`.



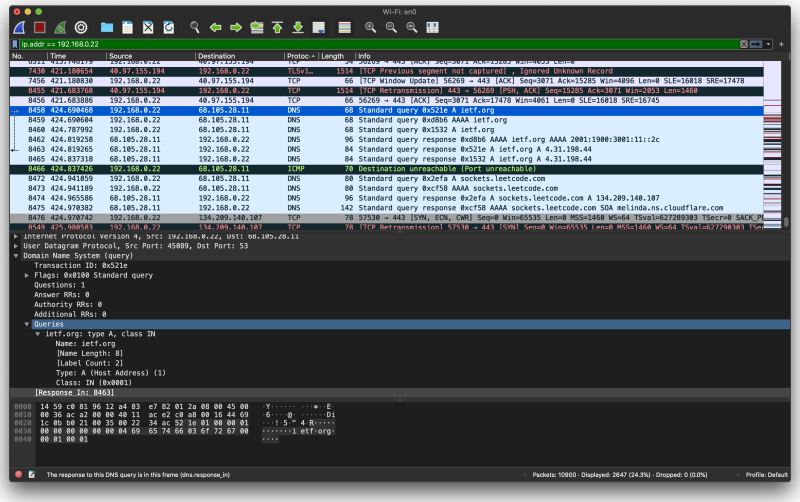


4

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

Answer

They are sent over UDP.



5

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

Answer

Port 53 for both query and 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?

Answer

`68.105.28.11`. It's the DNS address of my ISP (Cox Communication). Yes, it matches one of the Local DNS Server.

7

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

Answer

It's type A (IPv4) and type AAAA (IPv6). Nope both do not contains any "answers".

8

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

Answer

There are 3 responses. One for type AAAA and 2 for type A. Following is the response for each type:

Type AAAA Response:

```
Answers
ietf.org:  type AAAA, class IN, addr 2001:1900:3001:11::2c
Name:  ietf.org
Type:  AAAA (IPv6 Address) (28)
Class:  IN (0x0001)
Time to live:  1773 (29 minutes, 33 seconds)
Data length:  16
AAAA Address:  2001:1900:3001:11::2c
```

Type A Response:

```
Answers
ietf.org:  type A, class IN, addr 4.31.198.44
Name:  ietf.org
Type:  A (Host Address) (1)
Class:  IN (0x0001)
Time to live:  1800 (30 minutes)
Data length:  4
Address:  4.31.198.44
```

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?

Answer

Yes. The IPv6 address corresponding to AAAA response address.

10

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

Answer

No.

11

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

Answer

Port 53. Both for source and destination port

12

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

Answer

`2001:578:3f::30`. This IP refers to my ISP's DNS Server.

13

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

Answer

Type A. No, doesn't contain any "answers".

14

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

Answer

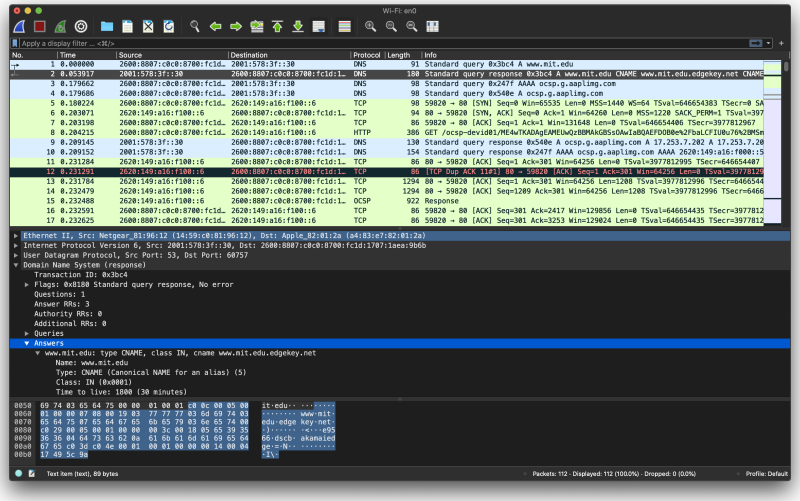
3 answers are provided and following are the content

```
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 (30 minutes)
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 (1 minute)
Data length:  24
CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net:  type A, class IN, addr 23.73.92.154
Name:  e9566.dscb.akamaiedge.net
Type:  A (Host Address) (1)
Class:  IN (0x0001)
Time to live:  20 (20 seconds)
Data length:  4
Address:  23.73.92.154
```

15

Provide a screenshot.

Answer



16

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

Answer

`2001:578:3f::30`. This IP refers to my ISP's DNS Server.

17

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

Answer

Type NS. No, 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?

Answer

Following are the list of nameservers and yes it does provide IP address

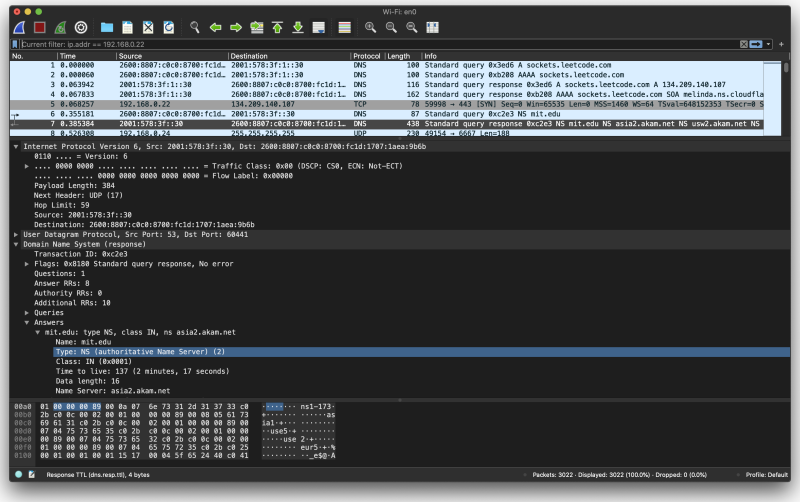
- asia2.akam.net
- usw2.akam.net

- ns1-37.akam.net
- ns1-173.akam.net
- asia1.akam.net
- use5.akam.net
- use2.akam.net
- eur5.akam.net

19

Provide a screenshot.

Answer



Note: For the below experiment (20-23), I was unable to use `bitsy.mit.edu`. Old DNS server is moved and hence I am using `1.1.1.1` as DNS server to answer these messages

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?

Answer

My DNS query is being sent to `1.1.1.1` and this IP is different from local DNS IP that I have.

21

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

Answer

Type A. Not, doesn't contain any "answers".

22

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

Answer

Only 1 answer is provided and contains the following

```
Answers
aiit.or.kr:  type A, class IN, addr 58.229.6.225
Name:  aiit.or.kr
Type:  A (Host Address) (1)
Class:  IN (0x0001)
Time to live:  3600 (1 hour)
Data length:  4
Address:  58.229.6.225
```

23

Provide a screenshot.

Answer