

# Computer Networks

K. Jaywanth Reddy

UFID : 22719671

## Homework - 2

P1:- I or f :-

- a) A user requests a webpage that consists of some text and 3 images. For this page, the client will send one request message and receive 4 responses message.

Sol:- This has to be 'false', the client has to send 4 messages and will receive 4 response messages in return.

- b). Two distinct web pages can be sent over the same persistent connection?

Sol:- This will be 'true', http persistent connection will be open until the it is explicitly closed by either Client / server.

- c). With non-persistent connections between browser & origin server, it is possible for a single TCP segment to carry 2 distinct http request messages.

Sol:- False. with non-persistent connections it has the capability to carry only one request by each TCP segment.

- d). The date header in the http response message indicates when the object in the response was last modified.

Sol:- False. Date in the header indicates the req. generation time

e). Http response message never have an empty message body.

Sol:- False. Response Message 204: No content indicates an empty message body in the Http response message.

====

P:-

a) find the total average response time.

Sol:-

$$\Rightarrow \text{Average time to transmit} = \left( \frac{L}{R} \right)$$

$\Rightarrow$  Average object size is 8,50,000 bits.

$\Rightarrow$  Average request rate from institution browser  $\rightarrow$  Origin servers  $\Rightarrow$  16 requests/second.

$$\text{Average Access delay} \Rightarrow \left( \frac{\Delta}{1 - \Delta \beta} \right)$$

$$\Delta \Rightarrow \frac{8,50,000}{15,000,000} \frac{\text{bits}}{\text{bits/sec}}$$

$$\Delta \Rightarrow \left( \frac{85}{1500} \right) \Rightarrow 0.0567 \text{ sec}$$

$$\Rightarrow \text{Traffic Intensity } \beta^\Delta \Rightarrow \{16 \text{ req/sec}\} \cdot \{0.0567 \text{ sec/sec}\}$$

$$\beta^\Delta = 0.907$$

$$\text{Average Access delay} \Rightarrow \left\{ \frac{0.0567}{1 - 0.907} \right\} \approx 0.6 \text{ sec.}$$

$$\therefore \text{Total average response time} \Rightarrow 0.6 + 3 \\ \Rightarrow 3.6 \text{ sec.}$$

- b). Suppose, Cache is installed in the institutional LAN  
 Suppose the miss rate is 0.4. find the total response time.

Sol:- we have reduced the traffic intensity on the access link by 60% for requests within institutional network.

$$\text{Average access delay} \Rightarrow \frac{0.0567}{1 - (0.4)(0.907)} \text{ sec} \\ \Rightarrow 0.089 \text{ sec.}$$

$$\text{Average response time} \Rightarrow (0.6) \cdot 0 + (0.4) (3.089) \\ \Rightarrow 1.24 \text{ sec.}$$

P3:- 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?

Sol: for the given Scenario:

→ Application Layer Protocols — DNS, HTTP

→ Transport Layer Protocols — { UDP for DNS  
TCP for HTTP

→ The above mentioned protocols are basically req.  
for making up the scenario we wanted.

## Wireshark Lab: HTTP v7.0

### 1. The basic HTTP GET/response interaction.

#### Questions:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?  
Ans: Both the browser and the server are running on HTTP version 1.1

No.	Time	Source	Destination	Protocol	Length	Info
305	6.065303	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
316	6.120880	128.119.245.12	192.168.1.225	HTTP	552	HTTP/1.1 200 OK (text/html)
625	8.646299	192.168.1.225	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
634	8.700265	128.119.245.12	192.168.1.225	HTTP	550	HTTP/1.1 404 Not Found (text/html)

2. What languages (if any) does your browser indicate that it can accept to the server?  
Ans: Browser indicates that it accepts en-US; English – United States for the server.

No.	Time	Source	Destination	Protocol	Length	Info
305	6.065303	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
316	6.120880	128.119.245.12	192.168.1.225	HTTP	552	HTTP/1.1 200 OK (text/html)
625	8.646299	192.168.1.225	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
634	8.700265	128.119.245.12	192.168.1.225	HTTP	550	HTTP/1.1 404 Not Found (text/html)

```
> Frame 305: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface en0, id 0
> Ethernet II, Src: Apple_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0)
> Internet Protocol Version 4, Src: 192.168.1.225, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 57733, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
< Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
```

3. What is the IP address of your computer? Of the ‘gaia.cs.umass.edu.server’?  
Ans: My computer Address is 192.168.1.225 and the server’s address is 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
305	6.065303	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
316	6.120880	128.119.245.12	192.168.1.225	HTTP	552	HTTP/1.1 200 OK (text/html)
625	8.646299	192.168.1.225	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
634	8.700265	128.119.245.12	192.168.1.225	HTTP	550	HTTP/1.1 404 Not Found (text/html)

4. What is the status code returned from the server to your browser?  
Ans: Status code returned is “200 OK”

No.	Time	Source	Destination	Protocol	Length	Info
305	6.065303	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
316	6.120880	128.119.245.12	192.168.1.225	HTTP	552	HTTP/1.1 200 OK (text/html)
625	8.646299	192.168.1.225	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
634	8.700265	128.119.245.12	192.168.1.225	HTTP	550	HTTP/1.1 404 Not Found (text/html)

5. When was the HTML file that you are retrieving last modified at the server?  
Ans: The last modified date of the HTML file is “Fri, 23 Sep 2022 05:59:01 GMT”

No.	Time	Source	Destination	Protocol	Length	Info
305	6.065303	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
316	6.120880	128.119.245.12	192.168.1.225	HTTP	552	HTTP/1.1 200 OK (text/html)
625	8.646299	192.168.1.225	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
634	8.700265	128.119.245.12	192.168.1.225	HTTP	550	HTTP/1.1 404 Not Found (text/html)

```
> Frame 316: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
> Ethernet II, Src: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple_dd:38:1b (98:01:a7:dd:38:1b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.225
> Transmission Control Protocol, Src Port: 80, Dst Port: 57733, Seq: 1, Ack: 479, Len: 486
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 23 Sep 2022 05:59:01 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 23 Sep 2022 05:59:01 GMT\r\n
    ETag: "80-5e951dfebb45b"\r\n
    Accept-Ranges: bytes\r\n
```

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

Ans: Response from the server is about 128 bytes to the browser.

The Wireshark interface shows a list of network frames. Frame 316 is selected, which is a GET request for 'HTTP-wireshark-file1.html'. Below the list, the raw hex and ASCII data for this frame is displayed. A red box highlights the 'Content-Length: 128\r\n' header in the ASCII dump, indicating the size of the file being served.

No.	Time	Source	Destination	Protocol	Length	Info
305	6.065303	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
316	6.120880	128.119.245.12	192.168.1.225	HTTP	552	HTTP/1.1 200 OK (text/html)
625	8.646299	192.168.1.225	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
634	8.700265	128.119.245.12	192.168.1.225	HTTP	550	HTTP/1.1 404 Not Found (text/html)

```
> Frame 316: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
> Ethernet II, Src: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple_dd:38:1b (98:01:a7:dd:38:1b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.225
> Transmission Control Protocol, Src Port: 80, Dst Port: 57733, Seq: 1, Ack: 479, Len: 486
  Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Fri, 23 Sep 2022 14:46:22 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Fri, 23 Sep 2022 05:59:01 GMT\r\n
      ETag: "80-5e951dfebb45b"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 128\r\n
      [Content length: 128]
```

## 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.

Ans: After the inspection of the raw data packet content window, we cannot find any headers within the data.

## 2. The HTTP CONDITIONAL GET/response interaction

Questions:

## 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?

Ans: For the first HTTP GET request from my browser to the server, there is no “IF-MODIFIED-SINCE”.

The Wireshark interface shows a list of network frames. Frame 1454 is selected, which is a GET request for 'HTTP-wireshark-file2.html'. Below the list, the raw hex and ASCII data for this frame is displayed. A red box highlights the 'If-Modified-Since' header in the ASCII dump, which is present in the request but has no corresponding response in the capture.

No.	Time	Source	Destination	Protocol	Length	Info
1454	6.180266	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1486	6.256603	128.119.245.12	192.168.1.225	HTTP	796	HTTP/1.1 200 OK (text/html)
1552	6.508245	2600:1700:e62..	2607:fb80:400..	HTTP	198	GET /generate_204 HTTP/1.1
1554	6.516480	2607:fb80:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content
148.. 58.9772..	192.168.1.225	128.119.245.12	HTTP	656	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1	
148.. 59.0316..	128.119.245.12	192.168.1.225	HTTP	386	HTTP/1.1 304 Not Modified	
168.. 66.5354..	2600:1700:e62..	2607:fb80:400..	HTTP	198	GET /generate_204 HTTP/1.1	
168.. 66.5397..	2607:fb80:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content	

```
> Frame 1454: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface en0, id 0
> Ethernet II, Src: Apple_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0)
> Internet Protocol Version 4, Src: 192.168.1.225, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58941, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
  Hypertext Transfer Protocol
    > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      [HTTP request 1/1]
      [Response in frame: 1486]
```

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

Ans: “Line-based text data” field is used for returning the contents of the file to the browser.

No.	Time	Source	Destination	Protocol	Length	Info
1454	6.180266	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1486	6.256603	128.119.245.12	192.168.1.225	HTTP	796	HTTP/1.1 200 OK (text/html)
1552	6.508245	2600:1700:e62..	2607:f8b0:400..	HTTP	198	GET /generate_204 HTTP/1.1
1554	6.516480	2607:f8b0:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content
148..	58.9772..	192.168.1.225	128.119.245.12	HTTP	656	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
148..	59.0316..	128.119.245.12	192.168.1.225	HTTP	306	HTTP/1.1 304 Not Modified
168..	66.5354..	2600:1700:e62..	2607:f8b0:400..	HTTP	198	GET /generate_204 HTTP/1.1
168..	66.5397..	2607:f8b0:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content

> Frame 1486: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface en0, id 0  
> Ethernet II, Src: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple\_dd:38:1b (98:01:a7:dd:38:1b)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.225  
> Transmission Control Protocol, Src Port: 80, Dst Port: 58941, Seq: 1, Ack: 479, Len: 730  
> Hypertext Transfer Protocol  
Line-based text data: text/html (10 lines)

```

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

```

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

Ans: We observed to have “IF-MODIFIED-SINCE” header representing the last time at which the file was downloaded from the server.

No.	Time	Source	Destination	Protocol	Length	Info
1454	6.180266	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1486	6.256603	128.119.245.12	192.168.1.225	HTTP	796	HTTP/1.1 200 OK (text/html)
1552	6.508245	2600:1700:e62..	2607:f8b0:400..	HTTP	198	GET /generate_204 HTTP/1.1
1554	6.516480	2607:f8b0:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content
148..	58.9772..	192.168.1.225	128.119.245.12	HTTP	656	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
148..	59.0316..	128.119.245.12	192.168.1.225	HTTP	306	HTTP/1.1 304 Not Modified
168..	66.5354..	2600:1700:e62..	2607:f8b0:400..	HTTP	198	GET /generate_204 HTTP/1.1
168..	66.5397..	2607:f8b0:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content

> Frame 14829: 656 bytes on wire (5248 bits), 656 bytes captured (5248 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0)  
> Internet Protocol Version 4, Src: 192.168.1.225, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 58943, Dst Port: 80, Seq: 1, Ack: 1, Len: 590  
> Hypertext Transfer Protocol

```

> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
Tf_Non-Match: "172-50-51-49-80"\r\n
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 14844]
```

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

Ans: For the second http get request, status code obtained is “304 Not Modified” as the browser is fetching the content which got stored in the cache after the first request being made, as it involves no modification and it results in Not Modified response.

No.	Time	Source	Destination	Protocol	Length	Info
1454	6.180266	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1486	6.256603	128.119.245.12	192.168.1.225	HTTP	796	HTTP/1.1 200 OK (text/html)
1552	6.508245	2600:1700:e62..	2607:f8b0:400..	HTTP	198	GET /generate_204 HTTP/1.1
1554	6.516480	2607:f8b0:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content
148..	58.9772..	192.168.1.225	128.119.245.12	HTTP	656	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
148..	59.0316..	128.119.245.12	192.168.1.225	HTTP	306	HTTP/1.1 304 Not Modified
168..	66.5354..	2600:1700:e62..	2607:f8b0:400..	HTTP	198	GET /generate_204 HTTP/1.1
168..	66.5397..	2607:f8b0:400..	2600:1700:e62..	HTTP	213	HTTP/1.1 204 No Content

### 3. Retrieving Long Documents

#### Questions:

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?

Ans: Browser has sent one HTTP GET request and received GET message for the Bill or Rights at packet number 2188.

No.	Time	Source	Destination	Protocol	Length	Info
2188	9.575470	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2205	9.633531	128.119.245.12	192.168.1.225	HTTP	583	HTTP/1.1 200 OK (text/html)

> Frame 2188: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0)  
> Internet Protocol Version 4, Src: 192.168.1.225, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 58952, Dst Port: 80, Seq: 1, Ack: 1, Len: 478  
> Hypertext Transfer Protocol  
> GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\n

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

Ans: We got status code along with a phrase as “200 OK” associated with the response to the HTTP GET request at packet number 2205.

No.	Time	Source	Destination	Protocol	Length	Info
2188	9.575470	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2205	9.633531	128.119.245.12	192.168.1.225	HTTP	583	HTTP/1.1 200 OK (text/html)

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

Ans: It produces “200 Ok” as the status code and the phrase as a part of the response.

No.	Time	Source	Destination	Protocol	Length	Info
2188	9.575470	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2205	9.633531	128.119.245.12	192.168.1.225	HTTP	583	HTTP/1.1 200 OK (text/html)

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

Ans: 4 data-containing TCP segments to carry HTTP response.

No.	Time	Source	Destination	Protocol	Length	Info
2188	9.575470	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2205	9.633531	128.119.245.12	192.168.1.225	HTTP	583	HTTP/1.1 200 OK (text/html)

> Frame 2205: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0  
> Ethernet II, Src: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple\_dd:38:1b (98:01:a7:dd:38:1b)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.225  
> Transmission Control Protocol, Src Port: 80, Dst Port: 58952, Seq: 4345, Ack: 478, Len: 517  
> [4 Reassembled TCP Segments (4861 bytes): #2201(1448), #2202(1448), #2203(1448), #2205(517)]  
[Frame: 2201, payload: 0-1447 (1448 bytes)]  
[Frame: 2202, payload: 1448-2895 (1448 bytes)]  
[Frame: 2203, payload: 2896-4343 (1448 bytes)]  
[Frame: 2205, payload: 4344-4860 (517 bytes)]  
[Segment count: 4]  
[Reassembled TCP length: 4861]  
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203233205365702032...]  
> Hypertext Transfer Protocol  
> Line-based text data: text/html (98 lines)

## 4. HTML Document with Embedded Objects

### Questions:

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

Ans: There are 3 HTTP GET request messages that are sent by the browser, and they were sent to the 128.119.245.32 and 178.79.137.164 ips.

No.	Time	Source	Destination	Protocol	Length	Info
1153	5.475196	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1166	5.529376	128.119.245.12	192.168.1.225	HTTP	1367	HTTP/1.1 200 OK (text/html)
1177	5.572337	192.168.1.225	128.119.245.12	HTTP	490	GET /pearson.png HTTP/1.1
1201	5.646609	128.119.245.12	192.168.1.225	HTTP	781	HTTP/1.1 200 OK (PNG)
1270	5.822843	192.168.1.225	178.79.137.164	HTTP	457	GET /8E_cover_small.jpg HTTP/1.1
1291	5.939364	178.79.137.164	192.168.1.225	HTTP	237	HTTP/1.1 301 Moved Permanently

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

Ans: The two images were downloaded serially as the GET request for the second image is published after receiving the response for the first GET request for image. The same is said to be downloaded parallelly when we have both the GET requests side by side/ immediately.

No.	Time	Source	Destination	Protocol	Length	Info
1153	5.475196	192.168.1.225	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1166	5.529376	128.119.245.12	192.168.1.225	HTTP	1367	HTTP/1.1 200 OK (text/html)
1177	5.572337	192.168.1.225	128.119.245.12	HTTP	490	GET /pearson.png HTTP/1.1
1201	5.646609	128.119.245.12	192.168.1.225	HTTP	781	HTTP/1.1 200 OK (PNG)
1270	5.822843	192.168.1.225	178.79.137.164	HTTP	457	GET /8E_cover_small.jpg HTTP/1.1
1291	5.939364	178.79.137.164	192.168.1.225	HTTP	237	HTTP/1.1 301 Moved Permanently

## 5. HTTP Authentication

### Questions:

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

Ans: Server response is "401 Unauthorized" as the status code and phrase in the initial HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
2721	7.912937	192.168.1.225	128.119.245.12	HTTP	560	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
2736	7.968083	128.119.245.12	192.168.1.225	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
9007	33.404945	192.168.1.225	128.119.245.12	HTTP	645	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
9029	33.459757	128.119.245.12	192.168.1.225	HTTP	556	HTTP/1.1 200 OK (text/html)
13544	50.770354	2600:1700:e62..	2607:f8b0:4000:810::200e	HTTP	198	[TCP Previous segment not captured] GET /generate_204 HTTP/1.1
13546	50.774718	2607:f8b0:400..	2600:1700:e62:6580:a9b9:ca5:1d..	HTTP	213	[TCP ACKed unseen segment] HTTP/1.1 204 No Content
27933	110.843531	2600:1700:e62..	2607:f8b0:4000:810::200e	HTTP	198	GET /generate_204 HTTP/1.1
27936	110.849486	2607:f8b0:400..	2600:1700:e62:6580:a9b9:ca5:1d..	HTTP	213	HTTP/1.1 204 No Content

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

Ans: Field called as "Authorization" was added to the GET message during the second time, representing username and password (credentials) used to authorize for the site.

No.	Time	Source	Destination	Protocol	Length	Info
2721	7.912937	192.168.1.225	128.119.245.12	HTTP	560	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
2736	7.968083	128.119.245.12	192.168.1.225	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
9007	33.404945	192.168.1.225	128.119.245.12	HTTP	645	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
9029	33.459757	128.119.245.12	192.168.1.225	HTTP	556	HTTP/1.1 200 OK (text/html)
13544	50.770354	2600:1700:e62..	2607:f8b0:4000:810::200e	HTTP	198	[TCP Previous segment not captured] GET /generate_204 HTTP/1.1
13546	50.774718	2607:f8b0:400..	2600:1700:e62:6580:a9b9:ca5:1d..	HTTP	213	[TCP ACKed unseen segment] HTTP/1.1 204 No Content
27933	110.843531	2600:1700:e62..	2607:f8b0:4000:810::200e	HTTP	198	GET /generate_204 HTTP/1.1
27936	110.849486	2607:f8b0:400..	2600:1700:e62:6580:a9b9:ca5:1d..	HTTP	213	HTTP/1.1 204 No Content

> Frame 9007: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_dd38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro\_58:63:f0 (6:c6:9c:58:63:f0)  
> Internet Protocol Version 4, Src: 192.168.1.225, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 58986, Dst Port: 80, Seq: 1, Ack: 1, Len: 579  
> Hypertext Transfer Protocol  
> > GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\nHost: galia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nAuthorization: Basic d2lyZXNoYXJrLXN0dWlbnRz0m5ldHdvcms=\r\nCredentials: wireshark-students:network

## Wireshark Lab: DNS v7.0 1. Nslookup

### Questions:

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

Ans: The nslookup for “www.modak.com” resulted in the IP address 172.67.153.76

```
(base) jaswanth@jaswanths-Air ~ % nslookup modak.com
Server: 2600:1700:e62:6580::1
Address: 2600:1700:e62:6580::1#53

Non-authoritative answer:
Name: modak.com
Address: 104.21.80.192
Name: modak.com
Address: 172.67.153.76
```

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

Ans: The nslookup for authoritative DNS servers is “nslookup -type=NS gla.ac.uk” and the authoritative dns server is “dns.gla.ac.uk”

```
(base) jaswanth@jaswanths-Air ~ % nslookup -type=NS gla.ac.uk
Server: 2600:1700:e62:6580::1
Address: 2600:1700:e62:6580::1#53

Non-authoritative answer:
gla.ac.uk      nameserver = dns0.gla.ac.uk.
gla.ac.uk      nameserver = dns1.gla.ac.uk.
gla.ac.uk      nameserver = dns2.gla.ac.uk.

Authoritative answers can be found from:
dns0.gla.ac.uk  internet address = 130.209.16.6
dns2.gla.ac.uk  internet address = 130.209.4.18
dns1.gla.ac.uk  internet address = 130.209.4.16
```

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

Ans: The IP address of the DNS server “dns.gla.ac.uk” obtained from the query to mail.yahoo.com is “130.209.16.6#53”

```
(base) jaswanth@jaswanths-Air ~ % nslookup mail.yahoo.com dns0.gla.ac.uk
Server: dns0.gla.ac.uk
Address: 130.209.16.6#53

** server can't find mail.yahoo.com: REFUSED
```

## 2. Ipconfig

```
ipconfig /all
```

```
C:\Users\MANISH>ipconfig /all
Windows IP Configuration

Host Name . . . . . : DESKTOP-3T0PPCI
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek PCIe FE Family Controller
Physical Address . . . . . : 18-60-24-16-C3-95
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
Physical Address . . . . . : F8-28-19-88-DE-67
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address . . . . . : FA-28-19-88-DE-67
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address . . . . . : F8-28-19-88-DE-67
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address . . . . . : F8-28-19-88-DE-68
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

C:\Users\MANISH>
```

```
ipconfig /displaydns
```

```
C:\Users\MANISH>ipconfig /displaydns
Windows IP Configuration

mssplus.mcafee.com
-----
Record data for type AAAA could not be displayed.

mssplus.mcafee.com
-----
Record Name . . . . . : mssplus.mcafee.com
Record Type . . . . . : 1
Time To Live . . . . . : 604363
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . . : 0.0.0.1

1.0.0.0.in-addr.arpa
-----
Record Name . . . . . : 1.0.0.0.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 604363
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : mssplus.mcafee.com
```

```
ipconfig /flushdns
```

```
C:\Users\MANISH>ipconfig /flushdns
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\MANISH>
```

### 3. Tracing DNS with Wireshark

Questions:

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

Ans: Both Query and the response messages for the DNS are sent over User Datagram Protocol (UDP).

No.	Time	Source	Destination	Protocol	Length	Info
2604	11.433230	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x7afe
2605	11.438180	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x2fa
2607	11.443577	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	169	Standard query response 0x7afe A www.ietf.org
2608	11.445710	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x4b81
2621	11.489403	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	207	Standard query response 0x4b81
2626	11.512656	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	193	Standard query response 0x4b81
2628	11.512791	2600:1700:e62...	2600:1700:e62:6580::1	ICMPv6	241	Destination Unreachable (Port unreachable)
2629	11.515525	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x28a
2630	11.515717	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x511a
2631	11.516949	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x5579
2632	11.519283	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	193	Standard query response 0x5579
2633	11.519286	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	169	Standard query response 0x5579
2654	11.561907	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	207	Standard query response 0x5579
2655	11.562006	2600:1700:e62...	2600:1700:e62:6580::1	ICMPv6	255	Destination Unreachable (Port unreachable)
3722	12.828130	2600:1700:e62...	2600:1700:e62:6580::1	DNS	98	Standard query 0x5c9f
3723	12.828204	2600:1700:e62...	2600:1700:e62:6580::1	DNS	98	Standard query 0x129a

No.	Time	Source	Destination	Protocol	Length	Info
2604	11.433230	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x7afe
2605	11.438180	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x2fa
2607	11.443577	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	169	Standard query response 0x7afe A www.ietf.org
2608	11.445710	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x4b81
2621	11.489403	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	207	Standard query response 0x4b81
2626	11.512656	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	193	Standard query response 0x4b81
2628	11.512791	2600:1700:e62...	2600:1700:e62:6580::1	ICMPv6	241	Destination Unreachable (Port unreachable)
2629	11.515525	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x28a
2630	11.515717	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x511a
2631	11.516949	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x5579
2632	11.519283	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	193	Standard query response 0x5579
2633	11.519286	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	169	Standard query response 0x5579
2654	11.561907	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	207	Standard query response 0x5579
2655	11.562006	2600:1700:e62...	2600:1700:e62:6580::1	ICMPv6	255	Destination Unreachable (Port unreachable)
3722	12.828130	2600:1700:e62...	2600:1700:e62:6580::1	DNS	98	Standard query 0x5c9f
3723	12.828204	2600:1700:e62...	2600:1700:e62:6580::1	DNS	98	Standard query 0x129a

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

Ans: Destination port DNS and response message DNS port is "53".

No.	Time	Source	Destination	Protocol	Length	Info
2604	11.433230	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x7afe A www.ietf.org
2605	11.438180	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x2fa
2607	11.443577	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	169	Standard query response 0x7afe A www.ietf.org
2608	11.445710	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x4b81 HTTPS www.ietf.org
2621	11.489403	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	207	Standard query response 0x4b81 HTTPS www.ietf.org
2626	11.512656	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	193	Standard query response 0x2fad AAAA www.ietf.org
2628	11.512791	2600:1700:e62...	2600:1700:e62:6580::1	ICMPv6	241	Destination Unreachable (Port unreachable)
2629	11.515525	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x28a AAAA www.ietf.org
2630	11.515717	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x511a AAAA www.ietf.org
2631	11.516949	2600:1700:e62...	2600:1700:e62:6580::1	DNS	92	Standard query 0x5579 AAAA www.ietf.org
2632	11.519283	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	193	Standard query response 0x28a AAAA www.ietf.org
2633	11.519286	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	169	Standard query response 0x511a AAAA www.ietf.org
2654	11.561907	2600:1700:e62...	2600:1700:e62:6580:a9b9:ca5:1d...	DNS	207	Standard query response 0x5579 HTTPS www.ietf.org
2655	11.562006	2600:1700:e62...	2600:1700:e62:6580::1	ICMPv6	255	Destination Unreachable (Port unreachable)
3722	12.828130	2600:1700:e62...	2600:1700:e62:6580::1	DNS	98	Standard query 0x5c9f AAAA analytics.ietf.org
3723	12.828204	2600:1700:e62...	2600:1700:e62:6580::1	DNS	98	Standard query 0x129a AAAA analytics.ietf.org

> Frame 2604: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface en0, id 0

> Ethernet II, Src: Apple\_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0)

> Internet Protocol Version 6, Src: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f, Dst: 2600:1700:e62:6580::1

> User Datagram Protocol, Src Port: 63702, Dst Port: 53

Source Port: 63702  
Destination Port: 53

Length: 92

CHECKSUM: 0x4c8e [unverified]

[Checksum Status: Unverified]

[Stream index: 10]

> [Timestamps]

  UDP payload (38 bytes)

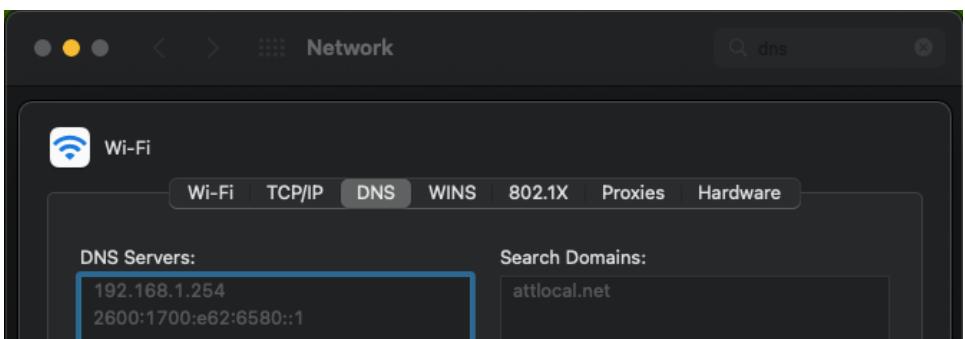
  Domain Name System (query)

No.	Time	Source	Destination	Protocol	Length	Info
2684	11.433230	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x7afe A www.ietf.org
2685	11.438180	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x2faf AAAA www.ietf.org
2687	11.443577	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	169	Standard query response 0x7afe A www.ietf.org
2688	11.445710	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	92	Standard query 0xbab1 HTTPS www.ietf.org
2621	11.489403	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	207	Standard query response 0x4b81 HTTPS www.ietf.org
2626	11.512656	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	138	Standard query response 0x2fad AAAA www.ietf.org
2628	11.512694	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	241	Destination Unreachable (Port unreachable)
2629	11.515525	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x28ae AAAA www.ietf.org
2630	11.515717	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x511a A www.ietf.org
2631	11.516949	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	92	Standard query 0x5579 HTTPS www.ietf.org
2632	11.519283	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	193	Standard query response 0x28ae AAAA www.ietf.org
2633	11.519286	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	169	Standard query response 0x511a A www.ietf.org
2654	11.561907	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	207	Standard query response 0x5579 HTTPS www.ietf.org
2655	11.562006	2600:1700:e62..	2600:1700:e62:6580::1	ICMPv6	255	Destination Unreachable (Port unreachable)
3722	12.828130	2600:1700:e62..	2600:1700:e62:6580::1	DNS	98	Standard query 0x5c9f A analytics.ietf.org
3723	12.828204	2600:1700:e62..	2600:1700:e62:6580::1	DNS	98	Standard query 0x129a AAAA analytics.ietf.org

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?

Ans: DNS query message is sent to the same IPv6 address as my local DNS server i.e. "2600:1700:62:6580::1"

No.	Time	Source	Destination	Protocol	Length	Info
2684	11.433230	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x7afe A www.ietf.org
2685	11.438180	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x2faf AAAA www.ietf.org
2687	11.443577	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	169	Standard query response 0x7afe A www.ietf.org
2688	11.445710	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	92	Standard query 0xbab1 HTTPS www.ietf.org
2621	11.489403	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	207	Standard query response 0x4b81 HTTPS www.ietf.org
2626	11.512656	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	193	Standard query response 0x2fad AAAA www.ietf.org
2628	11.512791	2600:1700:e62..	2600:1700:e62:6580::1	ICMPv6	241	Destination Unreachable (Port unreachable)
2629	11.515525	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x28ae AAAA www.ietf.org
2630	11.515717	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x511a A www.ietf.org
2631	11.516949	2600:1700:e62..	2600:1700:e62:6580::1	DNS	92	Standard query 0x5579 HTTPS www.ietf.org
2632	11.519283	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	193	Standard query response 0x28ae AAAA www.ietf.org
2633	11.519286	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	169	Standard query response 0x511a A www.ietf.org
2654	11.561907	2600:1700:e62..	2600:1700:e62:6580:a9b9:ca5:1d..	DNS	207	Standard query response 0x5579 HTTPS www.ietf.org
2655	11.562006	2600:1700:e62..	2600:1700:e62:6580::1	ICMPv6	255	Destination Unreachable (Port unreachable)
3722	12.828130	2600:1700:e62..	2600:1700:e62:6580::1	DNS	98	Standard query 0x5c9f A analytics.ietf.org
3723	12.828204	2600:1700:e62..	2600:1700:e62:6580::1	DNS	98	Standard query 0x129a AAAA analytics.ietf.org



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

Ans: DNS query message is of Type ‘A’ DNS Query and does not contain any answers.

No.	Time	Source	Destination	Protocol	Length	Info
6893	22.023199	2600:1700:e62..	2600:1700:e62:6580::1	DNS	91	Standard query 0x819b A www.mit.edu
6896	22.035163	2600:1700:e62..	2600:1700:e62:6580:a..	DNS	216	Standard query response 0x819b A www.mit.edu
7102	23.029564	192.168.1.225	192.168.1.254	DNS	71	Standard query 0x819b A www.mit.edu
7116	23.057955	192.168.1.254	192.168.1.225	DNS	196	Standard query response 0x819b A www.mit.edu

Frame 6893: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0

Ethernet II, Src: Apple\_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRIISGro\_58:63:f0 (ec:63:9c:58:63:f0)

Internet Protocol Version 6, Src: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f, Dst: 2600:1700:e62:6580::1

User Datagram Protocol, Src Port: 56727, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x819b

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

> www.mit.edu: type A, class IN

[Response\_In: 6896]

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

Ans: DNS response message has 3 answers each of which contains the Name, Type, TTL, Data Length and Server IP Address.

```

dns
No. | Time | Source | Destination | Protocol | Length | Info
6893 22.023199 2600:1700:e62.. 2600:1700:e62:6580::1 DNS 91 Standard query 0x819b A www.mit.edu
6896 22.035163 2600:1700:e62.. 2600:1700:e62:6580:a.. DNS 216 Standard query response 0x819b A www.
7102 23.029564 192.168.1.225 192.168.1.254 DNS 71 Standard query 0x819b A www.mit.edu
7116 23.057955 192.168.1.254 192.168.1.225 DNS 196 Standard query response 0x819b A www.

> Frame 6896: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface en0, id 0
> Ethernet II, Src: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple_dd:38:1b (98:01:a7:dd:38:1b)
> Internet Protocol Version 6, Src: 2600:1700:e62:6580::1, Dst: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f
> User Datagram Protocol, Src Port: 53, Dst Port: 56727
> Domain Name System (response)
  Transaction ID: 0x819b
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.mit.edu: type A, class IN
  > Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type CNAME, class IN, cname user-att-108-211-88-0.e9566.dscb.akamaiedge.net
    > user-att-108-211-88-0.e9566.dscb.akamaiedge.net: type A, class IN, addr 23.5.71.191
[Request In: 6893]
[Time: 0.011964000 seconds]

```

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?

Ans: IP address of the destination of TCP SYN packet corresponds to the IP address in the type A response received i.e., “104.16.44.99”

```

> Answers
  > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
[Request In: 2604]
[Time: 0.010347000 seconds]

```

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

Ans: Host does not issue any new DNS queries for retrieval of every image.

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

Ans: Destination port of the DNS query message and the source port of DNS response message are the same and the port number is 53.

```

dns
No. | Time | Source | Destination | Protocol | Length | Info
6893 22.023199 2600:1700:e62.. 2600:1700:e62:6580::1 DNS 91 Standard query 0x819b A www.mit.edu
6896 22.035163 2600:1700:e62.. 2600:1700:e62:6580:a.. DNS 216 Standard query response 0x819b A www.
7102 23.029564 192.168.1.225 192.168.1.254 DNS 71 Standard query 0x819b A www.mit.edu
7116 23.057955 192.168.1.254 192.168.1.225 DNS 196 Standard query response 0x819b A www.

> Frame 6893: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0
> Ethernet II, Src: Apple_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0)
> Internet Protocol Version 6, Src: 2600:1700:e62:6580::1, Dst: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f
> User Datagram Protocol, Src Port: 56727, Dst Port: 53
> Domain Name System (query)

```

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

Ans: DNS query message is sent to the same IP address as my local DNS server which is “2600:1700:e62:6580:a9b9:ca5:1de0:e73f”

No.	Time	Source	Destination	Protocol	Length	Info
6893	22.023199	2600:1700:e62...	2600:1700:e62:6580::1	DNS	91	Standard query 0x819b A www.mit.edu
6896	22.035163	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	216	Standard query response 0x819b A www.m...
7102	23.029564	192.168.1.225	192.168.1.254	DNS	71	Standard query 0x819b A www.mit.edu
7116	23.057955	192.168.1.254	192.168.1.225	DNS	196	Standard query response 0x819b A www.m...

> Frame 6896: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface en0, id 0  
> Ethernet II, Src: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple\_dd:38:1b (98:01:a7:dd:38:1b)  
> Internet Protocol Version 6, Src: 2600:1700:e62:6580::1, Dst: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f  
> User Datagram Protocol, Src Port: 53, Dst Port: 56727  
> Domain Name System (response)

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

Ans: DNS query is a type NS DNS query and does not have any answers.

No.	Time	Source	Destination	Protocol	Length	Info
7594	31.268485	2600:1700:e62...	2600:1700:e62:6580::1	DNS	91	Standard query 0x3203 NS www.mit.edu
7615	31.341400	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	264	Standard query response 0x3203 NS www.m...

> Frame 7594: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0)  
> Internet Protocol Version 6, Src: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f, Dst: 2600:1700:e62:6580::1  
> User Datagram Protocol, Src Port: 65323, Dst Port: 53  
  Domain Name System (query)  
    Transaction ID: 0x3203  
    Flags: 0x0100 Standard query  
    Questions: 1  
      Answer RRs: 0  
      Authority RRs: 0  
      Additional RRs: 0  
    Queries  
      > www.mit.edu: type NS, class IN  
      [Response In: 7615]

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

Ans: DNS response message has three answers and each of them has Name, Type, TTL, Data Length and Server IP Address as fields.

No.	Time	Source	Destination	Protocol	Length	Info
7594	31.268485	2600:1700:e62...	2600:1700:e62:6580::1	DNS	91	Standard query 0x3203 NS www.mit.edu
7615	31.341400	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	264	Standard query response 0x3203 NS www.m...

> Frame 7615: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits) on interface en0, id 0  
> Ethernet II, Src: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple\_dd:38:1b (98:01:a7:dd:38:1b)  
> Internet Protocol Version 6, Src: 2600:1700:e62:6580::1, Dst: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f  
> User Datagram Protocol, Src Port: 53, Dst Port: 65323  
  Domain Name System (response)  
    Transaction ID: 0x3203  
    Flags: 0x8180 Standard query response, No error  
    Questions: 1  
    Answer RRs: 3  
    Authority RRs: 1  
    Additional RRs: 0  
    Queries  
      > www.mit.edu: type NS, class IN  
    Answers  
      > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net  
      > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net  
      > e9566.dscb.akamaiedge.net: type CNAME, class IN, cname user-att-108-211-88-0.e9566.dscb.akamaiedge.net

15. Provide a screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
1824	8.714332	2600:1700:e62...	2600:1700:e62:6580::1	DNS	91	Standard query 0xb287 NS www.mit.edu
1848	8.778639	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	264	Standard query response 0xb287 NS www.

Answer RRs: 3  
 Authority RRs: 1  
 Additional RRs: 0  
 Queries  
 > www.mit.edu: type NS, class IN  
**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 CNAME, class IN, cname user-att-108-211-88-0.e9566.dscb.akamaiedge.net
  - Name: e9566.dscb.akamaiedge.net
  - Type: CNAME (Canonical NAME for an alias) (5)
  - Class: IN (0x0001)
  - Time to live: 1 (1 second)
  - Data length: 24
  - CNAME: user-att-108-211-88-0.e9566.dscb.akamaiedge.net

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

Ans: DNS query message was sent to same IP address that of the local DNS server which is “2600:1700:62:6580::1”

No.	Time	Source	Destination	Protocol	Length	Info
1520	6.304137	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0xbd38 A bitsy.mit.edu
1521	6.304191	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0x0530 AAAA bitsy.mit.edu
1528	6.327398	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	158	Standard query response 0x0530 AAAA bitsy.mi...
1533	6.348487	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	109	Standard query response 0xbd38 A bitsy.mit.e...
1536	6.353794	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
2684	11.356432	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
3945	16.360460	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
4436	19.098117	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x48ed A play.google.com
4438	19.098502	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x9f9e AAAA play.google.com
4439	19.101868	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0xbeeb HTTPS play.google.com
4440	19.105419	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	111	Standard query response 0x48ed A play.google...

```
> Frame 1520: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0
> Ethernet II, Src: Apple_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0)
✓ Internet Protocol Version 6, Src: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f, Dst: 2600:1700:e62:6580::1
  0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0100 0000 0100 0000 0000 = Flow Label: 0x40400
  Payload Length: 39
  Next Header: UDP (17)
  Hop Limit: 64
  Source Address: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f
Destination Address: 2600:1700:e62:6580::1
> User Datagram Protocol, Src Port: 62998, Dst Port: 53
> Domain Name System (query)
```

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

Ans: DNS query is of type A and the query message does not have any answers.

No.	Time	Source	Destination	Protocol	Length	Info
1520	6.304137	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0xbd38 A bitsy.mit.edu
1521	6.304191	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0x0530 AAAA bitsy.mit.edu
1528	6.327398	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	158	Standard query response 0x0530 AAAA bitsy.mit.edu
1533	6.348487	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	109	Standard query response 0xbd38 A bitsy.mit.edu
1536	6.353794	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
2684	11.356432	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
3945	16.360460	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
4436	19.098117	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x48ed A play.google.com
4438	19.098502	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x9f9e AAAA play.google.com
4439	19.101868	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0xbeeb HTTPS play.google.com
4440	19.105419	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	111	Standard query response 0x48ed A play.google.com

> Frame 1520: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0)  
> Internet Protocol Version 6, Src: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f, Dst: 2600:1700:e62:6580::1  
> User Datagram Protocol, Src Port: 62998, Dst Port: 53  
  `- Domain Name System (query)  
    Transaction ID: 0xbd38  
    Flags: 0x0100 Standard query  
    Questions: 1  
      Answer RRs: 0  
      Authority RRs: 0  
      Additional RRs: 0  
    `- Queries  
      > bitsy.mit.edu: type A, class IN  
      [Response In: 1533]

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?

Ans: DNS response message contains 8 MIT nameservers along with the IP addresses which are highlighted in the screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
1520	6.304137	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0xbd38 A bitsy.mit.edu
1521	6.304191	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0x0530 AAAA bitsy.mit.edu
1528	6.327398	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	158	Standard query response 0x0530 AAAA bitsy.mit.edu
1533	6.348487	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	109	Standard query response 0xbd38 A bitsy.mit.edu
1536	6.353794	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
2684	11.356432	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
3945	16.360460	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
4436	19.098117	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x48ed A play.google.com
4438	19.098502	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x9f9e AAAA play.google.com
4439	19.101868	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0xbeeb HTTPS play.google.com
4440	19.105419	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	111	Standard query response 0x48ed A play.google.com

> Frame 1533: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface en0, id 0  
> Ethernet II, Src: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple\_dd:38:1b (98:01:a7:dd:38:1b)  
> Internet Protocol Version 6, Src: 2600:1700:e62:6580::1, Dst: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f  
> User Datagram Protocol, Src Port: 53, Dst Port: 62998  
  `- Domain Name System (response)  
    Transaction ID: 0xbd38  
    Flags: 0x8100 Standard query response, No error  
    Questions: 1  
      Answer RRs: 1  
      Authority RRs: 0  
      Additional RRs: 0  
    `- Queries  
      > bitsy.mit.edu: type A, class IN  
  `- Answers  
    `- bitsy.mit.edu: type A, class IN, addr 18.0.72.3  
      Name: bitsy.mit.edu  
      Type: A (Host Address) (1)  
      Class: IN (0x0001)  
      Time to live: 1800 (30 minutes)  
      Data length: 4  
      Address: 18.0.72.3  
      [Request In: 1520]  
      [Time: 0.044350000 seconds]

19. Please provide screenshots.

No.	Time	Source	Destination	Protocol	Length	Info
1824	8.714332	2600:1700:e62..	2600:1700:e62:6580::1	DNS	91	Standard query 0xb287 NS www.mit.edu
1848	8.778639	2600:1700:e62..	2600:1700:e62:6580:a...	DNS	264	Standard query response 0xb287 NS www.

```

Answer RRs: 3
Authority RRs: 1
Additional RRs: 0
`- Queries
  > www.mit.edu: type NS, class IN
`- 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.dsrb.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.dsrb.akamaiedge.net
  > e9566.dsrb.akamaiedge.net: type CNAME, class IN, cname user-att-108-211-88-0.e9566.dsrb.akamaiedge.net
    Name: e9566.dsrb.akamaiedge.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1 (1 second)
    Data length: 24
    CNAME: user-att-108-211-88-0.e9566.dsrb.akamaiedge.net

```

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?

Ans: DNS query message is sent to the IP address “2600:1700:62:6580:a9b9:ca5:1de0:e73f” which is the IP address of bitsy.mit DNS response server.

No.	Time	Source	Destination	Protocol	Length	Info
1520	6.304137	2600:1700:e62..	2600:1700:e62:6580::1	DNS	93	Standard query 0xbd38 A bitsy.mit.edu
1521	6.304191	2600:1700:e62..	2600:1700:e62:6580::1	DNS	93	Standard query 0x0530 AAAA bitsy.mit.edu
1528	6.327398	2600:1700:e62..	2600:1700:e62:6580:a...	DNS	158	Standard query response 0x0530 AAAA bitsy.mit.edu
1533	6.348487	2600:1700:e62..	2600:1700:e62:6580:a...	DNS	109	Standard query response 0xbd38 A bitsy.mit.edu
1536	6.353794	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
2684	11.356432	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
3945	16.360460	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.aiit.or.kr
4436	19.098117	2600:1700:e62..	2600:1700:e62:6580::1	DNS	95	Standard query 0x48ed A play.google.com
4438	19.098502	2600:1700:e62..	2600:1700:e62:6580::1	DNS	95	Standard query 0x9f9e AAAA play.google.com
4439	19.101868	2600:1700:e62..	2600:1700:e62:6580::1	DNS	95	Standard query 0xbeeb HTTPS play.google.com
4440	19.105419	2600:1700:e62..	2600:1700:e62:6580:a...	DNS	111	Standard query response 0x48ed A play.google.com

```

> Frame 1520: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0
> Ethernet II, Src: Apple_dd:38:1b (98:01:a7:dd:38:1b), Dst: ARRISGro_58:63:f0 (6c:63:9c:58:63:f0)
> Internet Protocol Version 6, Src: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f, Dst: 2600:1700:e62:6580::1
> User Datagram Protocol, Src Port: 62998, Dst Port: 53
`- Domain Name System (query)
  Transaction ID: 0xbd38
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  `-' Queries
    > bitsy.mit.edu: type A, class IN
      [Response In: 1533]

```

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

Ans: DNS query message is type A and does not contain any “answers.”

No.	Time	Source	Destination	Protocol	Length	Info
1520	6.304137	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0xbd38 A bitsy.mit.edu
1521	6.304191	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0x0530 AAAA bitsy.mit.edu
1528	6.327398	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	158	Standard query response 0x0530 AAAA bitsy
1533	6.348487	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	109	Standard query response 0xbd38 A bitsy.mi
1536	6.353794	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.ait.or.kr
2684	11.356432	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.ait.or.kr
3945	16.360460	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.ait.or.kr
4436	19.098117	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x48ed A play.google.com
4438	19.098502	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x9f9e AAAA play.google.co
4439	19.101868	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0xbeeb HTTPS play.google.c
4440	19.105419	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	111	Standard query response 0x48ed A play.goo

> Frame 1533: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface en0, id 0  
> Ethernet II, Src: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple\_dd:38:1b (98:01:a7:dd:38:1b)  
> Internet Protocol Version 6, Src: 2600:1700:e62:6580::1, Dst: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f  
> User Datagram Protocol, Src Port: 53, Dst Port: 62998  
 Domain Name System (response)  
 Transaction ID: 0xbd38  
 Flags: 0x8180 Standard query response, No error  
 Questions: 1  
 Answer RRs: 1  
 Authority RRs: 0  
 Additional RRs: 0  
 Queries  
 > bitsy.mit.edu: type A, class IN  
 Answers  
 > bitsy.mit.edu: type A, class IN, addr 18.0.72.3  
 Name: bitsy.mit.edu  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 Time to live: 1800 (30 minutes)  
 Data length: 4  
 Address: 18.0.72.3  
 [Request In: 1520]  
 [Time: 0.044350000 seconds]

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

Ans: Only one answer provided in the DNS response message and the answer contains fields like Name, Type, TTL, Data Length and Servers IP addresses.

23. Provide Screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
1520	6.304137	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0xbd38 A bitsy.mit.edu
1521	6.304191	2600:1700:e62...	2600:1700:e62:6580::1	DNS	93	Standard query 0x0530 AAAA bitsy.mit.edu
1528	6.327398	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	158	Standard query response 0x0530 AAAA bitsy
1533	6.348487	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	109	Standard query response 0xbd38 A bitsy.mi
1536	6.353794	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.ait.or.kr
2684	11.356432	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.ait.or.kr
3945	16.360460	192.168.1.225	18.0.72.3	DNS	74	Standard query 0xdfcf A www.ait.or.kr
4436	19.098117	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x48ed A play.google.com
4438	19.098502	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0x9f9e AAAA play.google.co
4439	19.101868	2600:1700:e62...	2600:1700:e62:6580::1	DNS	95	Standard query 0xbeeb HTTPS play.google.c
4440	19.105419	2600:1700:e62...	2600:1700:e62:6580:a...	DNS	111	Standard query response 0x48ed A play.goo

> Frame 1533: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface en0, id 0  
> Ethernet II, Src: ARRISGro\_58:63:f0 (6c:63:9c:58:63:f0), Dst: Apple\_dd:38:1b (98:01:a7:dd:38:1b)  
> Internet Protocol Version 6, Src: 2600:1700:e62:6580::1, Dst: 2600:1700:e62:6580:a9b9:ca5:1de0:e73f  
> User Datagram Protocol, Src Port: 53, Dst Port: 62998  
 Domain Name System (response)  
 Transaction ID: 0xbd38  
 Flags: 0x8180 Standard query response, No error  
 Questions: 1  
 Answer RRs: 1  
 Authority RRs: 0  
 Additional RRs: 0  
 Queries  
 > bitsy.mit.edu: type A, class IN  
 Answers  
 > bitsy.mit.edu: type A, class IN, addr 18.0.72.3  
 Name: bitsy.mit.edu  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 Time to live: 1800 (30 minutes)  
 Data length: 4  
 Address: 18.0.72.3  
 [Request In: 1520]  
 [Time: 0.044350000 seconds]

**Problem 19:**

- a. Starting with a root DNS Server (for one of the root-servers[a-m].root-servers.net), initiate a sequence of queries for the IP Address for your department's web server by using dig. Show the list of the names of DNS servers in the delegation chain in answering your query.

Solution: I have initiated a sequence of queries using dig on the department's website (cise.ufl.edu)

```
(base) jaswanth@jaswanths-Air ~ % dig @j.root-servers.net cise.ufl.edu

; <>> DiG 9.10.6 <>> @j.root-servers.net cise.ufl.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 6839
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cise.ufl.edu.           IN      A

;; AUTHORITY SECTION:
edu.          172800  IN      NS      b.edu-servers.net.
edu.          172800  IN      NS      f.edu-servers.net.
edu.          172800  IN      NS      i.edu-servers.net.
edu.          172800  IN      NS      a.edu-servers.net.
edu.          172800  IN      NS      g.edu-servers.net.
edu.          172800  IN      NS      j.edu-servers.net.
edu.          172800  IN      NS      k.edu-servers.net.
edu.          172800  IN      NS      m.edu-servers.net.
edu.          172800  IN      NS      l.edu-servers.net.
edu.          172800  IN      NS      h.edu-servers.net.
edu.          172800  IN      NS      c.edu-servers.net.
edu.          172800  IN      NS      e.edu-servers.net.
edu.          172800  IN      NS      d.edu-servers.net.

;; ADDITIONAL SECTION:
b.edu-servers.net.    172800  IN      A      192.33.14.30
b.edu-servers.net.    172800  IN      AAAA     2001:503:231d::2:30
f.edu-servers.net.    172800  IN      A      192.35.51.30
f.edu-servers.net.    172800  IN      AAAA     2001:503:d414::30
i.edu-servers.net.    172800  IN      A      192.43.172.30
i.edu-servers.net.    172800  IN      AAAA     2001:503:39c1::30
a.edu-servers.net.    172800  IN      A      192.5.6.30
a.edu-servers.net.    172800  IN      AAAA     2001:503:a83e::2:30
g.edu-servers.net.    172800  IN      A      192.42.93.30
g.edu-servers.net.    172800  IN      AAAA     2001:503:eea3::30
j.edu-servers.net.    172800  IN      A      192.48.79.30
j.edu-servers.net.    172800  IN      AAAA     2001:502:7094::30
k.edu-servers.net.    172800  IN      A      192.52.178.30
k.edu-servers.net.    172800  IN      AAAA     2001:503:d2d::30
m.edu-servers.net.    172800  IN      A      192.55.83.30
m.edu-servers.net.    172800  IN      AAAA     2001:501:b1f9::30
l.edu-servers.net.    172800  IN      A      192.41.162.30
l.edu-servers.net.    172800  IN      AAAA     2001:500:d937::30
h.edu-servers.net.    172800  IN      A      192.54.112.30
h.edu-servers.net.    172800  IN      AAAA     2001:502:8cc::30
c.edu-servers.net.    172800  IN      A      192.26.92.30
c.edu-servers.net.    172800  IN      AAAA     2001:503:83eb::30
e.edu-servers.net.    172800  IN      A      192.12.94.30
e.edu-servers.net.    172800  IN      AAAA     2001:502:1ca1::30
d.edu-servers.net.    172800  IN      A      192.31.80.30
d.edu-servers.net.    172800  IN      AAAA     2001:500:856e::30

;; Query time: 11 msec
;; SERVER: 2001:503:c27::2:30#53(2001:503:c27::2:30)
;; WHEN: Fri Sep 23 14:48:14 CDT 2022
;; MSG SIZE rcvd: 836
```

```
(base) jaswanth@jaswanths-Air ~ % dig @j.edu-servers.net cise.ufl.edu

; <>> DiG 9.10.6 <>> @j.edu-servers.net cise.ufl.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 15665
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cise.ufl.edu.           IN      A

;; AUTHORITY SECTION:
ufl.edu.        172800  IN      NS      ns.name.ufl.edu.
ufl.edu.        172800  IN      NS      rns.name.ufl.edu.
ufl.edu.        172800  IN      NS      ens.name.ufl.edu.

;; ADDITIONAL SECTION:
ns.name.ufl.edu. 172800  IN      A      128.227.30.254
rns.name.ufl.edu. 172800  IN      A      128.6.224.66
ens.name.ufl.edu. 172800  IN      A      128.227.30.252
ens.name.ufl.edu. 172800  IN      A      128.227.30.253

;; Query time: 77 msec
;; SERVER: 2001:502:7094::30#53(2001:502:7094::30)
;; WHEN: Fri Sep 23 14:49:22 CDT 2022
;; MSG SIZE rcvd: 163
```

Now we fetch the list of names of name servers / DNS servers in the chain

```
(base) jaswanth@jaswanths-Air ~ % dig @ns.name.ufl.edu cise.ufl.edu
; <>> DiG 9.10.6 <>> @ns.name.ufl.edu cise.ufl.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58773
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
;; QUESTION SECTION:
;cise.ufl.edu.           IN      A

;; ANSWER SECTION:
cise.ufl.edu.      3600    IN      A      128.227.36.46

;; AUTHORITY SECTION:
cise.ufl.edu.      3600    IN      NS     ns.name.ufl.edu.
cise.ufl.edu.      3600    IN      NS     ns1.cise.ufl.edu.
cise.ufl.edu.      3600    IN      NS     ns2.cise.ufl.edu.
cise.ufl.edu.      3600    IN      NS     ns3.cise.ufl.edu.

;; ADDITIONAL SECTION:
ns.name.ufl.edu.   900     IN      A      8.6.245.30
ns.name.ufl.edu.   900     IN      A      128.227.30.254
ns1.cise.ufl.edu. 3600    IN      A      128.227.205.194
ns2.cise.ufl.edu. 3600    IN      A      128.227.205.195
ns3.cise.ufl.edu. 3600    IN      A      128.227.205.196

;; Query time: 215 msec
;; SERVER: 8.6.245.30#53(8.6.245.30)
;; WHEN: Fri Sep 23 14:50:34 CDT 2022
;; MSG SIZE  rcvd: 213
```

b. Repeat part (a) for a popular website

Solution: I have initiated a sequence of queries using dig on popular website – Apple (apple.com)

```
(base) jaswanth@jaswanths-Air ~ % dig @j.gtld-servers.net apple.com
; <>> DiG 9.10.6 <>> @j.gtld-servers.net apple.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15679
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;apple.com.           IN      A

;; AUTHORITY SECTION:
apple.com.        172800  IN      NS     a.ns.apple.com.
apple.com.        172800  IN      NS     b.ns.apple.com.
apple.com.        172800  IN      NS     c.ns.apple.com.
apple.com.        172800  IN      NS     d.ns.apple.com.

;; ADDITIONAL SECTION:
a.ns.apple.com.   172800  IN      A      17.253.200.1
a.ns.apple.com.   172800  IN      AAAA   2620:149:ae0::53
b.ns.apple.com.   172800  IN      A      17.253.207.1
b.ns.apple.com.   172800  IN      AAAA   2620:149:ae7::53
c.ns.apple.com.   172800  IN      A      204.19.119.1
c.ns.apple.com.   172800  IN      AAAA   2620:171:800:714::1
d.ns.apple.com.   172800  IN      A      204.26.57.1
d.ns.apple.com.   172800  IN      AAAA   2620:171:801:714::1

;; Query time: 75 msec
;; SERVER: 2001:502:7094::30#53(2001:502:7094::30)
;; WHEN: Fri Sep 23 14:52:23 CDT 2022
;; MSG SIZE  rcvd: 281
```

```
(base) jaswanth@jaswanths-Air ~ % dig @j.root-servers.net apple.com
; <>> DiG 9.10.6 <>> @j.root-servers.net apple.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17427
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;apple.com.           IN      A

;; AUTHORITY SECTION:
com.                  172800  IN      NS      e.gtld-servers.net.
com.                  172800  IN      NS      b.gtld-servers.net.
com.                  172800  IN      NS      j.gtld-servers.net.
com.                  172800  IN      NS      m.gtld-servers.net.
com.                  172800  IN      NS      i.gtld-servers.net.
com.                  172800  IN      NS      f.gtld-servers.net.
com.                  172800  IN      NS      a.gtld-servers.net.
com.                  172800  IN      NS      g.gtld-servers.net.
com.                  172800  IN      NS      h.gtld-servers.net.
com.                  172800  IN      NS      l.gtld-servers.net.
com.                  172800  IN      NS      k.gtld-servers.net.
com.                  172800  IN      NS      c.gtld-servers.net.
com.                  172800  IN      NS      d.gtld-servers.net.

;; ADDITIONAL SECTION:
e.gtld-servers.net.  172800  IN      A      192.12.94.30
e.gtld-servers.net.  172800  IN      AAAA   2001:502:1ca1::30
b.gtld-servers.net.  172800  IN      A      192.33.14.30
b.gtld-servers.net.  172800  IN      AAAA   2001:503:231d::2:30
j.gtld-servers.net.  172800  IN      A      192.48.79.30
j.gtld-servers.net.  172800  IN      AAAA   2001:502:7094::30
m.gtld-servers.net.  172800  IN      A      192.55.83.30
m.gtld-servers.net.  172800  IN      AAAA   2001:501:b1f9::30
i.gtld-servers.net.  172800  IN      A      192.43.172.30
i.gtld-servers.net.  172800  IN      AAAA   2001:503:39c1::30
f.gtld-servers.net.  172800  IN      A      192.35.51.30
f.gtld-servers.net.  172800  IN      AAAA   2001:503:d414::30
a.gtld-servers.net.  172800  IN      A      192.5.6.30
a.gtld-servers.net.  172800  IN      AAAA   2001:503:a83e::2:30
g.gtld-servers.net.  172800  IN      A      192.42.93.30
g.gtld-servers.net.  172800  IN      AAAA   2001:503:eea3::30
h.gtld-servers.net.  172800  IN      A      192.54.112.30
h.gtld-servers.net.  172800  IN      AAAA   2001:502:8cc::30
l.gtld-servers.net.  172800  IN      A      192.41.162.30
l.gtld-servers.net.  172800  IN      AAAA   2001:500:d937::30
k.gtld-servers.net.  172800  IN      A      192.52.178.30
k.gtld-servers.net.  172800  IN      AAAA   2001:503:d2d::30
c.gtld-servers.net.  172800  IN      A      192.26.92.30
c.gtld-servers.net.  172800  IN      AAAA   2001:503:83eb::30
d.gtld-servers.net.  172800  IN      A      192.31.80.30
d.gtld-servers.net.  172800  IN      AAAA   2001:500:856e::30

;; Query time: 17 msec
;; SERVER: 192.58.128.30#53(192.58.128.30)
;; WHEN: Fri Sep 23 14:51:30 CDT 2022
;; MSG SIZE  rcvd: 834
```

```
(base) jaswanth@jaswanths-Air ~ % dig @a.ns.apple.com apple.com
; <>> DiG 9.10.6 <>> @a.ns.apple.com apple.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35132
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;apple.com.           IN      A

;; ANSWER SECTION:
apple.com.          900    IN      A      17.253.144.10

;; AUTHORITY SECTION:
apple.com.          43200   IN      NS      b.ns.apple.com.
apple.com.          43200   IN      NS      a.ns.apple.com.
apple.com.          43200   IN      NS      c.ns.apple.com.
apple.com.          43200   IN      NS      d.ns.apple.com.

;; ADDITIONAL SECTION:
b.ns.apple.com.    43200   IN      AAAA   2620:149:ae7::53
a.ns.apple.com.    43200   IN      AAAA   2620:149:ae0::53
c.ns.apple.com.    43200   IN      AAAA   2620:171:800:714::1
d.ns.apple.com.    43200   IN      AAAA   2620:171:801:714::1
b.ns.apple.com.    43200   IN      A      17.253.207.1
a.ns.apple.com.    43200   IN      A      17.253.200.1
c.ns.apple.com.    43200   IN      A      204.19.119.1
d.ns.apple.com.    43200   IN      A      204.26.57.1

;; Query time: 132 msec
;; SERVER: 2620:149:ae0::53#53(2620:149:ae0::53)
;; WHEN: Fri Sep 23 14:52:53 CDT 2022
;; MSG SIZE  rcvd: 297
```