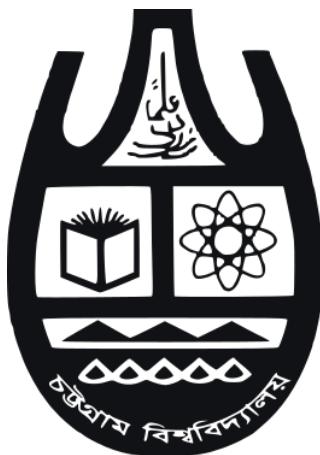


# **Lab Assignment-01**

**Course: Computer Networks Lab**

**Course Code: CSE-614**



**Submitted to:**

Dr. Farah Jahan

Professor

Department of Computer Science and Engineering

University of Chittagong

**Submitted by:**

Shanewaz Aurnob

ID: 20701066

Department of Computer Science and Engineering

University of Chittagong

**Date: September 30, 2024**

# 1 Wireshark Lab: Intro v8.0

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

The three different protocols that appear in the protocol column in the unfiltered packet listing window are

1. UDP
2. TCP
3. QUIC

No.	Time	Source	Destination	Protocol	Length Info
527	21.039262	192.168.56.102	172.253.118.95	UDP	71 56812 → 443 Len=29
528	21.170348	192.168.56.102	18.67.233.8	TCP	55 3667 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1
529	21.192251	172.253.118.95	192.168.56.102	UDP	68 443 → 56812 Len=26
530	21.214838	18.67.233.8	192.168.56.102	TCP	66 443 → 3667 [ACK] Seq=1 Ack=2 Win=145 Len=0 SLE=1 SRE=2
531	21.964075	172.253.118.95	192.168.56.102	UDP	121 443 → 56812 Len=79
532	21.985102	192.168.56.102	172.253.118.95	UDP	75 56812 → 443 Len=33
533	22.310474	172.253.118.95	192.168.56.102	UDP	836 443 → 56812 Len=794
534	22.310474	172.253.118.95	192.168.56.102	UDP	66 443 → 56812 Len=24
535	22.321615	192.168.56.102	74.125.24.95	QUIC	334 Protected Payload (KP0), DCID=e654ebfb8657b7c0
536	22.332821	192.168.56.102	172.253.118.95	UDP	75 56812 → 443 Len=33
537	22.442466	74.125.24.95	192.168.56.102	QUIC	72 Protected Payload (KP0)
538	22.469296	192.168.56.102	74.125.24.95	QUIC	74 Protected Payload (KP0), DCID=e654ebfb8657b7c0

Figure 1: Protocols Identified in the Packet-Listing Window

## 1.2 How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull-down menu, then select Time Display Format, then select Time-of-day.)

It took **0.187677s** from when the HTTP GET message was sent until the HTTP OK reply was received

http					
No.	Time	Source	Destination	Protocol	Length Info
103	20:50:53.078493	192.168.0.179	184.26.54.208	HTTP	165 GET /connecttest.txt HTTP/1.1
119	20:50:53.266170	184.26.54.208	192.168.0.179	HTTP	241 HTTP/1.1 200 OK (text/plain)

Figure 2: Time Duration Between HTTP GET and HTTP OK Messages

### 1.3 What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

- The Internet address of the gaia.cs.umass.edu (also known as www.net.cs.umass.edu) is **184.26.54.208**
- The Internet address of my computer is **192.168.0.179**

http						
No.	Time	Source	Destination	Protocol	Length	Info
103	20:50:53.078493	192.168.0.179	184.26.54.208	HTTP	165	GET /connecttest.txt HTTP/1.1
119	20:50:53.266170	184.26.54.208	192.168.0.179	HTTP	241	HTTP/1.1 200 OK (text/plain)

Figure 3: IP Addresses of the gaia.cs.umass.edu Server and the Client's Computer

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

- The HTTP message GET

```
C:\Users\HP\AppData\Local\Temp\wireshark_Wi-FiVOMU2.pcapng 542 total packets, 1 shown

No. Time Source Destination Protocol Length Info
103 20:50:53.078493 192.168.0.179 184.26.54.208 HTTP 165 GET /connecttest.txt HTTP/1.1
Frame 103: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{4D25AFB4-508C-4E7F-8114-
C230197048D2}, id 0
Ethernet II, Src: AzureWaveTec_ee:59:db (80:91:33:ee:59:db), Dst: TendaTechnol_15:b4:00 (50:0f:f5:15:b4:00)
Internet Protocol Version 4, Src: 192.168.0.179, Dst: 184.26.54.208
Transmission Control Protocol, Src Port: 4862, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol
```

Figure 4: HTTP GET Request Message

- The HTTP message OK

```
No. Time Source Destination Protocol Length Info
119 20:50:53.266170 184.26.54.208 192.168.0.179 HTTP 241 HTTP/1.1 200 OK (text/plain)
Frame 119: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0
Ethernet II, Src: TendaTechnol_15:b4:00 (50:0f:f5:15:b4:00), Dst: AzureWaveTec_ee:59:db (80:91:33:ee:59:db)
Internet Protocol Version 4, Src: 184.26.54.208, Dst: 192.168.0.179
Transmission Control Protocol, Src Port: 80, Dst Port: 4862, Seq: 1, Ack: 112, Len: 187
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
```

Figure 5: HTTP OK Response Message

## 2 Wireshark Lab : HTTP v7.0

### 2.1 The Basic HTTP GET/response interaction

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

My browser is running HTTP version 1.1. The version 4 of the HTTP server is running.

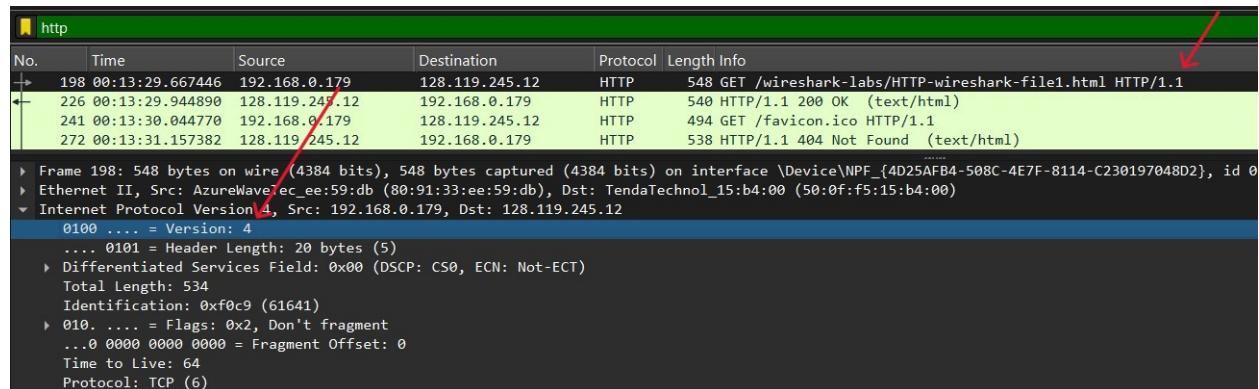


Figure 6: HTTP Versions Used by the Browser and the Server

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

My browser indicates that the language it can accept to the server is English(US).

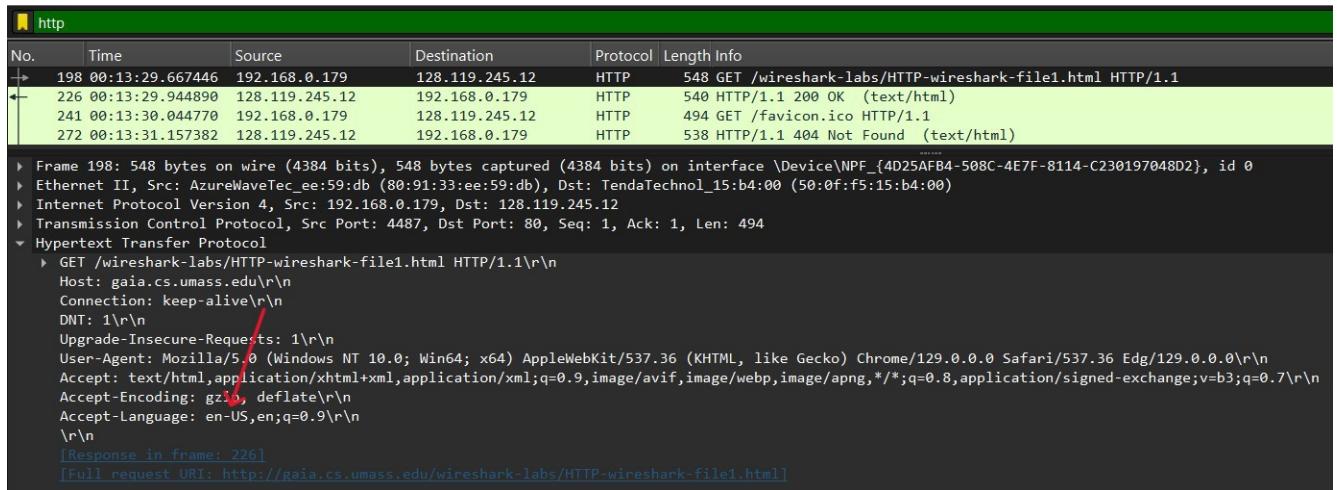


Figure 7: Languages Accepted by the Browser

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

- The IP address of my computer is **192.168.0.179**
- The IP address of the gaia.cs.umass.edu server is **128.119.245.12**

No.	Time	Source	Destination	Protocol	Length Info
198	00:13:29.667446	192.168.0.179	128.119.245.12	HTTP	548 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
226	00:13:29.944890	128.119.245.12	192.168.0.179	HTTP	540 HTTP/1.1 200 OK (text/html)
241	00:13:30.044770	192.168.0.179	128.119.245.12	HTTP	494 GET /favicon.ico HTTP/1.1
272	00:13:31.157382	128.119.245.12	192.168.0.179	HTTP	538 HTTP/1.1 404 Not Found (text/html)

Figure 8: IP Addresses of the Client and the Server

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

The status code returned from the server to my browser is **200**

No.	Time	Source	Destination	Protocol	Length Info
198	00:13:29.667446	192.168.0.179	128.119.245.12	HTTP	548 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
226	00:13:29.944890	128.119.245.12	192.168.0.179	HTTP	540 HTTP/1.1 200 OK (text/html)
241	00:13:30.044770	192.168.0.179	128.119.245.12	HTTP	494 GET /favicon.ico HTTP/1.1
272	00:13:31.157382	128.119.245.12	192.168.0.179	HTTP	538 HTTP/1.1 404 Not Found (text/html)

```

> Frame 226: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0
> Ethernet II, Src: TendaTechnol_15:b4:00 (50:0f:f5:15:b4:00), Dst: AzureWaveTec_ee:59:db (80:91:33:ee:59:db)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 4487, Seq: 1, Ack: 495, Len: 486
    > Hypertext Transfer Protocol
        > HTTP/1.1 200 OK\r\n
            Response Version: HTTP/1.1
            Status Code: 200
                [Status Code Description: OK]
                Response Phrase: OK
            Date: Fri, 27 Sep 2024 18:13:31 GMT\r\n
            Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
            Last-Modified: Fri, 27 Sep 2024 05:59:01 GMT\r\n
            ETag: "80-623138d421ba0"\r\n
            Accept-Ranges: bytes\r\n

```

Figure 9: HTTP Status Code Returned by the Server

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

The HTML file that I retrieved was last modified at the server at **Fri, 27 Sep 2024 05:59:01 GMT**.

No.	Time	Source	Destination	Protocol	Length Info
198	00:13:29.667446	192.168.0.179	128.119.245.12	HTTP	548 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
226	00:13:29.944890	128.119.245.12	192.168.0.179	HTTP	540 HTTP/1.1 200 OK (text/html)
241	00:13:30.044770	192.168.0.179	128.119.245.12	HTTP	494 GET /favicon.ico HTTP/1.1
272	00:13:31.157382	128.119.245.12	192.168.0.179	HTTP	538 HTTP/1.1 404 Not Found (text/html)

```

> Frame 226: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0
> Ethernet II, Src: TendaTechnol_15:b4:00 (50:0f:f5:15:b4:00), Dst: AzureWaveTec_ee:59:db (80:91:33:ee:59:db)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 4487, Seq: 1, Ack: 495, Len: 486
    > Hypertext Transfer Protocol
        > HTTP/1.1 200 OK\r\n
            Response Version: HTTP/1.1
            Status Code: 200
                [Status Code Description: OK]
                Response Phrase: OK
            Date: Fri, 27 Sep 2024 18:13:31 GMT\r\n
            Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
            Last-Modified: Fri, 27 Sep 2024 05:59:01 GMT\r\n
            ETag: "80-623138d421ba0"\r\n
            Accept-Ranges: bytes\r\n

```

Figure 10: Last Modification Date of the Retrieved HTML File

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

128 bytes of content are being returned to my browser.

Figure 11 shows a Wireshark capture of an HTTP request and response. The request (Frame 198) is a GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1. The response (Frame 26) is a 200 OK with a Content-Length of 128. The raw data section shows the response body, which is a single byte '\n'. A red arrow points to the 'Content-Length: 128' header in the response details.

Figure 11: Total Number of Bytes Returned by the Server to the Browser

### 2.1.7 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.

By inspecting the raw data in the packet content window, I don't see any headers within the data that are not displayed in the packet-listing window.

## 2.2 The HTTP CONDITIONAL GET/response interaction

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

NO, I don't see any “IF-MODIFIED-SINCE” line in the first HTTP GET.

Figure 12 shows a Wireshark capture of an HTTP request and response. The request (Frame 3691) is a GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1. The response (Frame 3736) is a 200 OK with a Content-Length of 784. The raw data section shows the request body, which includes the User-Agent and Accept headers. A red arrow points to the 'Request Method: GET' line in the raw data.

Figure 12: Absence of "If-Modified-Since" Header in the First HTTP GET Request

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

**Yes,** The server explicitly return the contents of the file. The text under ‘Line-Based Text Data’ and the text that was sent to my browser from the server is same.

```

http
No. Time Source Destination Protocol Length Info
1 3691 00:27:08.227605 192.168.0.179 128.119.245.12 HTTP 548 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2 3736 00:27:08.518502 128.119.245.12 192.168.0.179 HTTP 784 HTTP/1.1 200 OK (text/html)

Frame 3736: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0
Ethernet II, Src: TendaTechno_15:b4:00 (50:0f:f5:15:b4:00), Dst: AzureWaveTec_ee:59:db (80:91:33:ee:59:db)
Internet Protocol Version 4 Src: 128.119.245.12, Dst: 192.168.0.179
Transmission Control Protocol, Src Port: 80, Dst Port: 5184, Seq: 1, Ack: 495, 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

```

Figure 13: Inspection of the Server’s Response Content

## 2.2.3 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?

**No,** I don’t see any “IF-MODIFIED-SINCE” line in the second HTTP GET.

```

http
No. Time Source Destination Protocol Length Info
1 6960 00:36:10.297310 192.168.0.179 128.119.245.12 HTTP 548 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2 7417 00:36:10.601532 128.119.245.12 192.168.0.179 HTTP 784 HTTP/1.1 200 OK (text/html)
3 7577 00:36:10.731574 192.168.0.179 128.119.245.12 HTTP 494 GET /favicon.ico HTTP/1.1
4 7641 00:36:11.023553 128.119.245.12 192.168.0.179 HTTP 538 HTTP/1.1 404 Not Found (text/html)
5 8735 00:36:18.618930 192.168.0.179 128.119.245.12 HTTP 660 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
6 8743 00:36:18.897757 128.119.245.12 192.168.0.179 HTTP 294 HTTP/1.1 304 Not Modified
7 8751 00:36:20.347222 192.168.0.179 128.119.245.12 HTTP 660 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
8 8758 00:36:20.638785 128.119.245.12 192.168.0.179 HTTP 293 HTTP/1.1 304 Not Modified

Frame 7577: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface \Device\NPF_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0
Ethernet II, Src: AzureWaveTec_ee:59:db (80:91:33:ee:59:db), Dst: TendaTechno_15:b4:00 (50:0f:f5:15:b4:00)
  Destination: TendaTechno_15:b4:00 (50:0f:f5:15:b4:00)
  Source: AzureWaveTec_ee:59:db (80:91:33:ee:59:db)
  Type: IPv4 (0x0800)
  [Stream index: 0]
  Internet Protocol Version 4, Src: 192.168.0.179, Dst: 128.119.245.12
  Transmission Control Protocol, Src Port: 6117, Dst Port: 80, Seq: 495, Ack: 731, Len: 440
  Hypertext Transfer Protocol
    GET /favicon.ico HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36 Edg/129.0.0.0\r\n
    DNT: 1\r\n
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n

```

Figure 14: Absence of ”If-Modified-Since” Header in the Second HTTP GET Request

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

The server responded with an HTTP status code of 404 and the phrase "Not Found" to the second HTTP GET request.

No, the server did not send the file's content again. A 404 'Not Found' response indicates that the file has not changed since the last time the client cached it. As a result, only headers and metadata are included in the response, instructing the client to rely on its cached copy of the file.

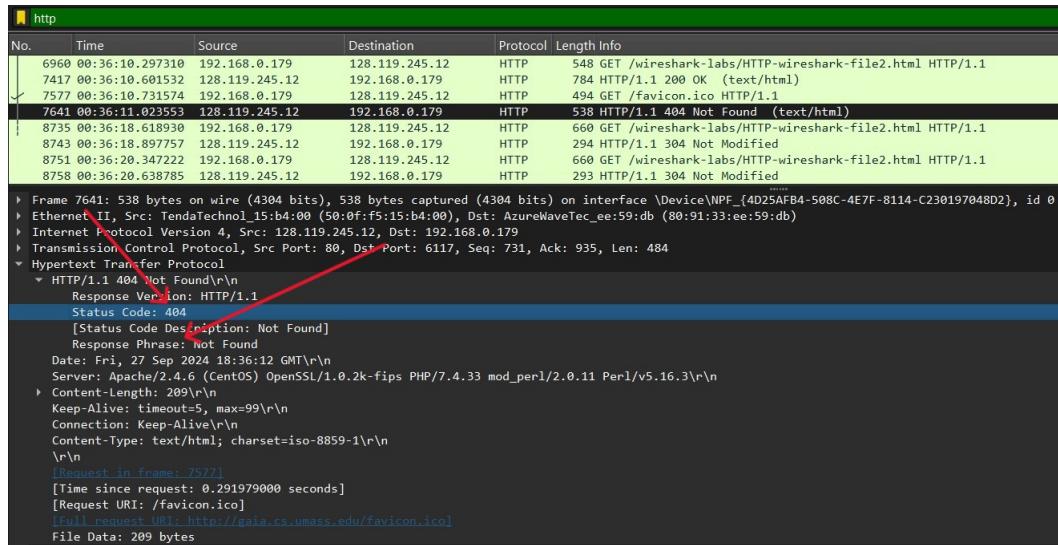


Figure 15: Server Response to the Second HTTP GET Request

## 2.3 Retrieving Long Documents

### 2.3.1 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?

- My browser sent **1** HTTP GET request message.
- The packet number in the trace which contains the GET message for the Bill or Rights is **133**

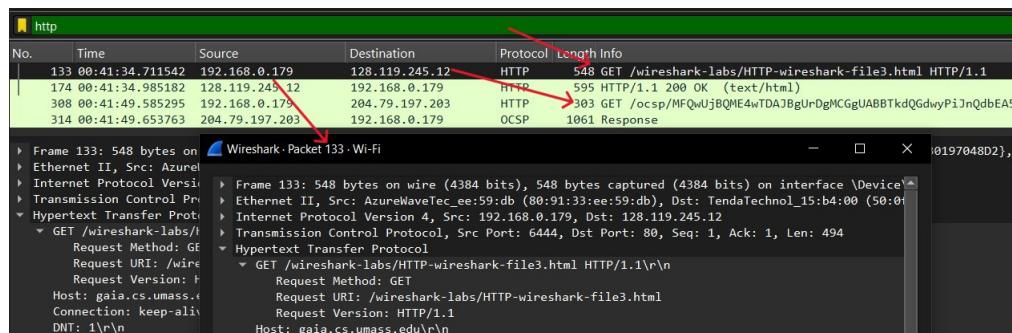


Figure 16: HTTP GET Requests and Corresponding Responses

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

The packet number in the trace which contains the status code and the phrase associated with the response to the HTTP GET request, is **174**

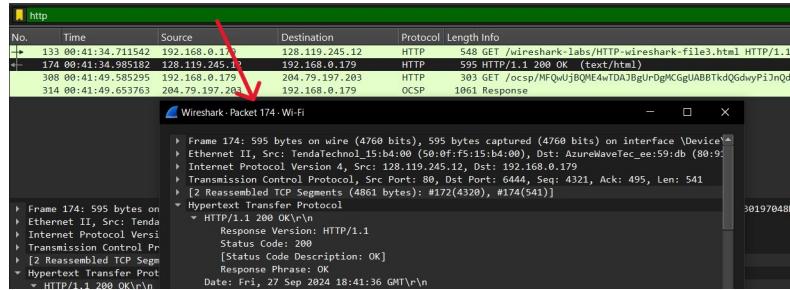


Figure 17: Packet Containing HTTP Status Code and Phrase

### 2.3.3 What is the status code and phrase in the response?

The status code is **"200"** and the response contains the phrase **"OK"**.

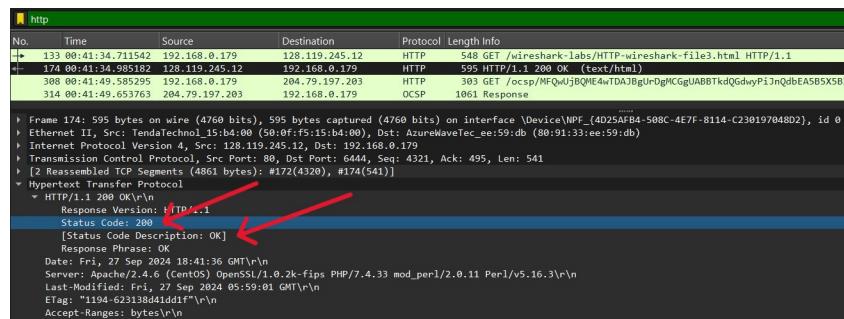


Figure 18: HTTP Status Code and Phrase in Response

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

Two data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

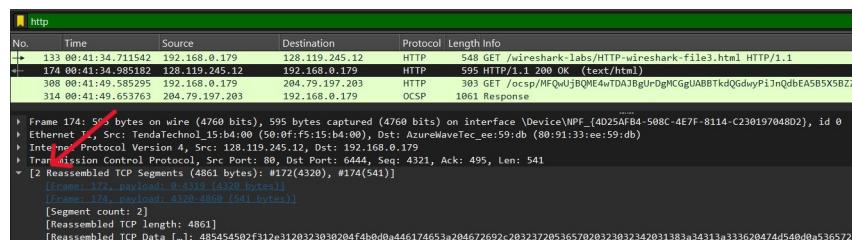


Figure 19: Data-Containing TCP Segments for HTTP Response

## 2.4 HTML Documents with Embedded Objects

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

My Browser sent **3** HTTP GET request messages. The destination address of these GET requests are given below, respectively:

- **128.119.245.12**
- **128.119.245.12**
- **178.70.137.164**

No.	Time	Source	Destination	Protocol	Length Info
153	00:48:01.994164	192.168.0.179	128.119.245.12	HTTP	548 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
193	00:48:02.291833	128.119.245.12	192.168.0.179	HTTP	1355 HTTP/1.1 200 OK (text/html)
195	00:48:02.315617	192.168.0.179	128.119.245.12	HTTP	494 GET /pearson.png HTTP/1.1
245	00:48:02.594826	128.119.245.12	192.168.0.179	HTTP	785 HTTP/1.1 200 OK (PNG)
262	00:48:02.867695	192.168.0.179	178.79.137.164	HTTP	461 GET /8E_cover_small.jpg HTTP/1.1
267	00:48:03.069922	178.79.137.164	192.168.0.179	HTTP	225 HTTP/1.1 301 Moved Permanently

Figure 20: Summary of HTTP GET Requests Sent by the Browser

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

The browser downloaded the two images serially because the request for the first image was sent and completed before the request for the second image was initiated. If the images had been downloaded in parallel, both requests would have been made at the same time and would have returned within the same time frame.

No.	Time	Source	Destination	Protocol	Length Info
153	00:48:01.994164	192.168.0.179	128.119.245.12	HTTP	548 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
193	00:48:02.291833	128.119.245.12	192.168.0.179	HTTP	1355 HTTP/1.1 200 OK (text/html)
195	00:48:02.315617	192.168.0.179	128.119.245.12	HTTP	494 GET /pearson.png HTTP/1.1
245	00:48:02.594826	128.119.245.12	192.168.0.179	HTTP	785 HTTP/1.1 200 OK (PNG)
262	00:48:02.867695	192.168.0.179	178.79.137.164	HTTP	461 GET /8E_cover_small.jpg HTTP/1.1
267	00:48:03.069922	178.79.137.164	192.168.0.179	HTTP	225 HTTP/1.1 301 Moved Permanently

Figure 21: Analysis of Image Download Methodology

## 2.5 HTTP Authentication

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

The server's response status code is **401** and the phrase is “**Unauthorized**” in response to the initial HTTP GET message from my browser.

No.	Time	Source	Destination	Protocol	Length	Info
24	00:54:14.591650	192.168.0.179	128.119.245.12	HTTP	564	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
68	00:54:14.866096	128.119.245.12	192.168.0.179	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
141	00:54:25.481106	192.168.0.179	128.119.245.12	HTTP	629	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
147	00:54:25.759553	128.119.245.12	192.168.0.179	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
165	00:54:26.933536	192.168.0.179	128.119.245.12	HTTP	590	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
168	00:54:27.212012	128.119.245.12	192.168.0.179	HTTP	770	HTTP/1.1 401 Unauthorized (text/html)

Frame 68: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF\_{4D25AFB4-508C-4E7F-8114-C23019704BD2}, id 0  
Ethernet II, Src: TendaTechnol\_15:b4:00 (50:0f:f5:15:b4:00), Dst: AzureWaveTec\_ee:59:db (80:91:33:ee:59:db)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.179  
Transmission Control Protocol, Src Port: 80, Dst Port: 6940, Seq: 1, Ack: 511, Len: 717  
Hypertext Transfer Protocol  
  HTTP/1.1 401 Unauthorized\r\n    Response Version: HTTP/1.1

Figure 22: Server Response to Initial HTTP GET Request

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

When my browser sends the HTTP GET message for the second time, a new field named “**Authorization**” is included in the HTTP GET message.

No.	Time	Source	Destination	Protocol	Length	Info
24	00:54:14.591650	192.168.0.179	128.119.245.12	HTTP	564	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
68	00:54:14.866096	128.119.245.12	192.168.0.179	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
141	00:54:25.481106	192.168.0.179	128.119.245.12	HTTP	629	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
147	00:54:25.759553	128.119.245.12	192.168.0.179	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
165	00:54:26.933536	192.168.0.179	128.119.245.12	HTTP	590	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
168	00:54:27.212012	128.119.245.12	192.168.0.179	HTTP	770	HTTP/1.1 401 Unauthorized (text/html)

Frame 141: 629 bytes on wire (5032 bits), 629 bytes captured (5032 bits) on interface \Device\NPF\_{4D25AFB4-508C-4E7F-8114-C23019704BD2}, id 0  
Ethernet II, Src: AzureWaveTec\_ee:59:db (80:91:33:ee:59:db), Dst: TendaTechnol\_15:b4:00 (50:0f:f5:15:b4:00)  
Internet Protocol Version 4, Src: 192.168.0.179, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 6939, Dst Port: 80, Seq: 2, Ack: 1, Len: 575  
Hypertext Transfer Protocol  
  GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.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    Authorization: Basic YXVybmsiOjEyMzQ=\r\n    DNT: 1\r\n    Upgrade-Insecure-Requests: 1\r\n    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36 Edg/129.0.0.0\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=0.7\r\n    Accept-Encoding: gzip, deflate\r\n    Accept-Language: en-US,en;q=0.9

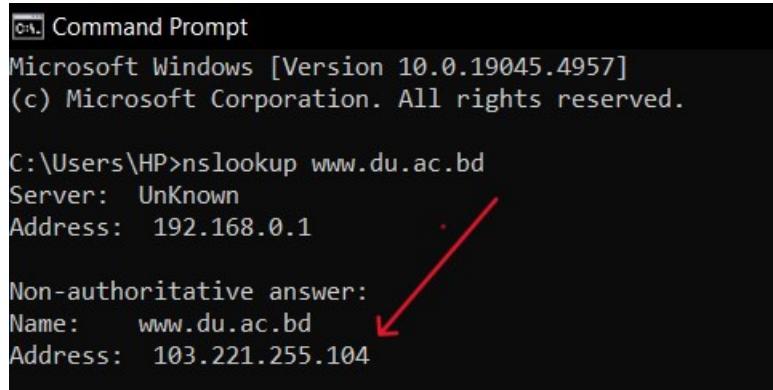
Figure 23: New Header Field in Second HTTP GET Request

### 3 Wireshark Lab : DNS v8.0

#### 3.1 nslookup

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

The IP address of an asian web server (www.du.ac.bd) is **103.221.255.104**



```
Windows [Version 10.0.19045.4957]
(c) Microsoft Corporation. All rights reserved.

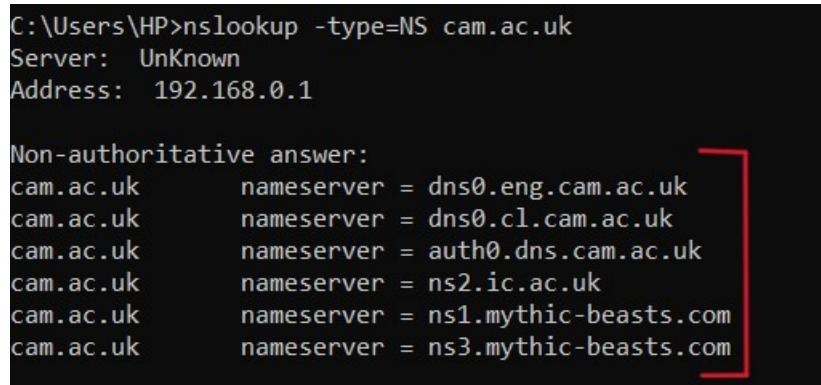
C:\Users\HP>nslookup www.du.ac.bd
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: www.du.ac.bd
Address: 103.221.255.104
```

Figure 24: nslookup Command Output for Asian Web Server

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

Determining the authoritative DNS servers for a university (**cam.ac.uk**) in Europe:



```
C:\Users\HP>nslookup -type=NS cam.ac.uk
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk
cam.ac.uk      nameserver = auth0.dns.cam.ac.uk
cam.ac.uk      nameserver = ns2.ic.ac.uk
cam.ac.uk      nameserver = ns1.mythic-beasts.com
cam.ac.uk      nameserver = ns3.mythic-beasts.com
```

Figure 25: Authoritative DNS Servers for a European University

### 3.1.3 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?

After running the nslookup, one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. Its IP address is **128.232.132.8**

```
C:\Users\HP>nslookup mail.yahoo.com cam.ac.uk
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address: 128.232.132.8 ↗

DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Figure 26: IP address of mail server

## 3.2 Tracing DNS with Wireshark

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

The DNS query and response messages are located in the below picture. They are sent over **UDP**.

No.	Time	Source	Destination	Protocol	Length Info
2192	01:09:15.720800	192.168.0.179	52.182.143.208	TLSv1.2	1060 Application Data
2193	01:09:15.758865	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x295a A www.ietf.org A 104.16.45.99 A 104.16.44.99
2194	01:09:15.761002	192.168.0.1	192.168.0.179	DNS	145 Standard query response 0xa259 HTTPS www.ietf.org HTTPS
2195	01:09:15.766136	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x223f A www.ietf.org ↗
2196	01:09:15.766708	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x502e HTTPS www.ietf.org
2197	01:09:15.768913	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x85bf A www.ietf.org A 104.16.45.99 A 104.16.44.99
2198	01:09:15.770259	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x5e0a A www.ietf.org
2199	01:09:15.770518	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x223f A www.ietf.org A 104.16.45.99 A 104.16.44.99
2200	01:09:15.770518	192.168.0.1	192.168.0.179	DNS	145 Standard query response 0x502e HTTPS www.ietf.org HTTPS
2201	01:09:15.770787	192.168.0.179	192.168.0.1	DNS	94 Standard query 0x34d3 A nav-edge.smartscreen.microsoft.com

Figure 27: DNS Query and Response Protocols

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

The destination port for the DNS query message is **53**. The source port of the DNS response message is also **53**.

No.	Time	Source	Destination	Protocol	Length Info
2192	01:09:15.720800	192.168.0.179	52.182.143.208	TLSv1.2	1060 Application Data
2193	01:09:15.758865	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x295a A www.ietf.org A 104.16.45.99 A 104.16.44.99
2194	01:09:15.761082	192.168.0.1	192.168.0.179	DNS	145 Standard query response 0xa259 HTTPS www.ietf.org HTTPS
2195	01:09:15.766136	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x223f A www.ietf.org
2196	01:09:15.766708	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x502e HTTPS www.ietf.org
2197	01:09:15.768913	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x85bf A www.ietf.org A 104.16.45.99 A 104.16.44.99
2198	01:09:15.770259	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x5e0a A www.ietf.org
2199	01:09:15.770518	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x223f A www.ietf.org A 104.16.45.99 A 104.16.44.99
2200	01:09:15.770518	192.168.0.1	192.168.0.179	DNS	145 Standard query response 0x502e HTTPS www.ietf.org HTTPS
2201	01:09:15.770787	192.168.0.179	192.168.0.1	DNS	94 Standard query 0x34d3 A nav-edge.smartscreen.microsoft.com
Fragment 1195: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0					
> Ethernet II, Src: AzureWaveTec_ee:59:db (80:91:33:ee:59:db), Dst: TendaTechnol_15:b4:00 (50:0f:f5:15:b4:00)					
> Internet Protocol Version 4, Src: 192.168.0.179, Dst: 192.168.0.1					
> User Datagram Protocol, Src Port: 49552, Dst Port: 53					
> Domain Name System (query)					

Figure 28: Source and Destination Ports in DNS Query and Response Messages

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

The DNS query message is sent to the IP address 192.168.0.1. Using ipconfig, I determined the IP address of my local DNS server and that is **192.168.0.1**

Yes, these two IP addresses are the same.

No.	Time	Source	Destination	Protocol	Length Info
2192	01:09:15.720800	192.168.0.179	52.182.143.208	TLSv1.2	1060 Application Data
2193	01:09:15.758865	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x295a A www.ietf.org A 104.16.45.99 A 104.16.44.99
2194	01:09:15.761082	192.168.0.1	192.168.0.179	DNS	145 Standard query response 0xa259 HTTPS www.ietf.org HTTPS
2195	01:09:15.766136	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x223f A www.ietf.org
2196	01:09:15.766708	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x502e HTTPS www.ietf.org
2197	01:09:15.768913	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x85bf A www.ietf.org A 104.16.45.99 A 104.16.44.99
2198	01:09:15.770259	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x5e0a A www.ietf.org
2199	01:09:15.770518	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x223f A www.ietf.org A 104.16.45.99 A 104.16.44.99
2200	01:09:15.770518	192.168.0.1	192.168.0.179	DNS	145 Standard query response 0x502e HTTPS www.ietf.org HTTPS

Figure 29: DNS query message IP address

```

Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 109089075
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-18-B7-41-04-0E-3C-51-06-96
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled

```

Figure 30: DNS server IP address

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

The “Type” of DNS query is “**Type A**”.

**No**, the query message doesn’t contain any “**answers**”.

No.	Time	Source	Destination	Protocol	Length Info
2192	01:09:15.720800	192.168.0.179	52.182.143.208	TLSv1.2	1060 Application Data
2193	01:09:15.758865	192.168.0.1	192.168.0.179	DNS	104 Standard query response 0x295a A www.ietf.org A 104.16.45.99 A 104.16.44.99
2194	01:09:15.761002	192.168.0.1	192.168.0.179	DNS	145 Standard query response 0xa259 HTTPS www.ietf.org HTTPS
2195	01:09:15.766136	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x223f A www.ietf.org
2196	01:09:15.766708	192.168.0.179	192.168.0.1	DNS	72 Standard query 0x502e HTTPS www.ietf.org

Frame 2195: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0  
Ethernet II, Src: AzureWaveTec\_ee:59:db (80:91:33:ee:59:db), Dst: TendaTechnol\_15:b4:00 (50:0f:f5:15:b4:00)  
Internet Protocol Version 4, Src: 192.168.0.179, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 49552, Dst Port: 53  
Domain Name System (query)  
Transaction ID: 0x223f  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
www.ietf.org: type A, class IN  
[Response In: 2195]

Figure 31: DNS Query Type and Contents

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

Two “answers” are provided. Each of these answers contains **Name**, **Type**, **Class**, **Time to live**, **Data Length**, and **Address**.

▼ Domain Name System (response)
Transaction ID: 0x223f
► Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
▼ Queries
► www.ietf.org: type A, class IN
▼ Answers
▼ www.ietf.org: type A, class IN, addr 104.16.45.99
Name: www.ietf.org
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.16.45.99
► www.ietf.org: type A, class IN, addr 104.16.44.99
[Request In: 2195]
[Time: 0.004382000 seconds]

Figure 32: DNS Response Message and Answer Details

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

The IP addresses in the DNS response message are **104.16.44.99**.

The destination IP address of the SYN packet is **104.16.44.99**. So, the destination IP address of the SYN packet corresponds to any of the IP addresses provided in the DNS response message.

ip.addr == 192.168.0.179						
No.	Time	Source	Destination	Protoc	Length	Info
2465	01:09:16.322000	192.168.0.179	20.194.184.156	TCP	54	7450 → 443 [ACK] Seq=5807 Ack=9034 Win=131328 Len=0
2536	01:09:16.357849	20.194.184.156	192.168.0.179	TCP	60	443 → 7450 [ACK] Seq=9034 Ack=5807 Win=64512 Len=0
2617	01:09:16.482722	192.168.0.179	128.119.245.12	TCP	54	[TCP Retransmission] 7393 → 88 [FIN, ACK] Seq=2 Ack=2 Win=517 Len=0
2622	01:09:16.499310	192.168.0.179	128.119.245.12	TCP	54	[TCP Retransmission] 7392 → 88 [FIN, ACK] Seq=2 Ack=2 Win=517 Len=0
2623	01:09:16.501208	192.168.0.179	104.16.44.99	TCP	66	7454 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2697	01:09:16.533161	104.16.44.99	192.168.0.179	TCP	66	443 → 7454 [SYN, ACK] Seq=1 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
2698	01:09:16.533346	192.168.0.179	104.16.44.99	TCP	54	7454 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0

Frame 2623: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0  
Ethernet II, Src: AzureWaveTec\_ee:59:db (80:91:33:ee:59:db), Dst: TendaTechnol\_15:b4:00 (50:0f:f5:15:b4:00)  
Internet Protocol Version 4, Src: 192.168.0.179, Dst: 104.16.44.99  
 0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 52  
 Identification: 0x130b (4875)  
 010. .... = Flags: 0x2, Don't fragment  
...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 64  
 Protocol: TCP (6)  
 Header Checksum: 0xdleaa [validation disabled]  
[Header checksum status: Unverified]  
 Source Address: 192.168.0.179  
 Destination Address: 104.16.44.99  
[Stream index: 31]

Figure 33: TCP SYN Packet and DNS Response IP Address Match

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

No, my host does not issue new DNS queries before retrieving each image. Because these images are from same domain. If multiple images are hosted on the same domain, the host only needs to perform the DNS query **once**. After that, the cached IP address is used for all subsequent requests to the same domain, eliminating the need for new DNS queries.

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

The destination port for the DNS query message is **53**. The source port of DNS response message is also **53**.

ip.addr == 192.168.0.179						
No.	Time	Source	Destination	Protoc	Length	Info
131	01:34:38.655000	192.168.0.179	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
132	01:34:38.706010	192.168.0.1	192.168.0.179	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.
133	01:34:38.707466	192.168.0.179	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
136	01:34:38.813400	192.168.0.1	192.168.0.179	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
137	01:34:38.817650	192.168.0.179	192.168.0.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu

Frame 133: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0  
Ethernet II, Src: AzureWaveTec\_ee:59:db (80:91:33:ee:59:db), Dst: TendaTechnol\_15:b4:00 (50:0f:f5:15:b4:00)  
Internet Protocol Version 4, Src: 192.168.0.179, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 63291, Dst Port: 53  
Domain Name System (query)

Figure 34: Source and Destination Ports of DNS Query and Response Messages

ip.addr == 192.168.0.179						
No.	Time	Source	Destination	Protoc	Length	Info
131	01:34:38.655000	192.168.0.179	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
132	01:34:38.706010	192.168.0.1	192.168.0.179	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
133	01:34:38.707466	192.168.0.179	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
136	01:34:38.813400	192.168.0.1	192.168.0.179	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dsrb.akamaiedge.net A 23.36.28.220
137	01:34:38.817650	192.168.0.179	192.168.0.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu

Frame 136: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF\_{4D25AFB4-508C-4E7F-8114-C230197048D2}, id 0  
Ethernet II, Src: TendaTechnol\_15:b4:00 (50:0f:f5:15:b4:00), Dst: AzureWaveTec\_ee:59:db (80:91:33:ee:59:db)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.179  
User Datagram Protocol, Src Port: 53, Dst Port: 63291  
Domain Name System (response)

Figure 35: Source and Destination Ports of DNS Query and Response Messages

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

The IP address to which the DNS query message was sent is **192.168.0.1**. Yes, This is the same IP address of my default local DNS server.

No.	Time	Source	Destination	Protocol	Length Info
75	01:34:28.930220	192.168.0.179	192.168.0.1	DNS	87 Standard query 0x2f1b A safebrowsing.googleapis.com
76	01:34:28.930389	192.168.0.179	192.168.0.1	DNS	87 Standard query 0x9f63 HTTPS safebrowsing.googleapis.com
77	01:34:28.934022	192.168.0.1	192.168.0.179	DNS	103 Standard query response 0x2f1b A safebrowsing.googleapis.com
78	01:34:28.934022	192.168.0.1	192.168.0.179	DNS	144 Standard query response 0x9f63 HTTPS safebrowsing.googleapis.com
131	01:34:38.655000	192.168.0.179	192.168.0.1	DNS	84 Standard query 0x0001 PTR 1.0.168.192.in-addr.a
132	01:34:38.706010	192.168.0.1	192.168.0.179	DNS	84 Standard query response 0x0001 No such name PTR
133	01:34:38.707466	192.168.0.179	192.168.0.1	DNS	71 Standard query 0x0002 A www.mit.edu
136	01:34:38.813400	192.168.0.1	192.168.0.179	DNS	160 Standard query response 0x0002 A www.mit.edu CN
137	01:34:38.817650	192.168.0.179	192.168.0.1	DNS	71 Standard query 0x0003 AAAA www.mit.edu
139	01:34:38.910020	192.168.0.1	192.168.0.179	DNS	200 Standard query response 0x0003 AAAA www.mit.edu

Figure 36: Destination IP Address of DNS Query Message

```
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 109089075
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-18-B7-41-04-0E-3C-51-06-96
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

Figure 37: DNS Query Destination IP with Local DNS Server

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

The “Type” of DNS query is “Type A”. No, the query message does not contain any “answers”.

```
► User Datagram Protocol, Src Port: 63291, Dst Port: 53
  ▶ Domain Name System (query)
    Transaction ID: 0x0002
    ► 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: 136]
```

Figure 38: DNS Query Type and Contents

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

Three “answers” are provided. Each of these answers contains the Name, Type, Class, Time to live, Data length, and CNAME.

```

User Datagram Protocol, Src Port: 53, Dst Port: 63291
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0xB180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  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
      Name: www.mit.edu
      Type: CNAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 468 (7 minutes, 48 seconds)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
    www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dsrb.akamaiedge.net
    e9566.dsrb.akamaiedge.net: type A, class IN, addr 23.36.28.220
  Request Id: 133
  [Time: 0.105934000 seconds]

```

Figure 39: DNS Response Message with Answers

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

The DNS query message is sent to the IP address **192.168.0.1**

**Yes**, this is the same IP address of my default local DNS server.

No.	Time	Source	Destination	Protocol	Length	Info
33	01:39:58.838769	192.168.0.179	192.168.0.1	DNS	77	Standard query 0xb3be A beacon4.gvt2.com
34	01:39:58.838843	192.168.0.179	192.168.0.1	DNS	77	Standard query 0x36af HTTPS beacon4.gvt2.com
35	01:39:58.842298	192.168.0.1	192.168.0.179	DNS	93	Standard query response 0xb3be A beacon4.gvt2.com A 216.239.32.116
39	01:39:58.886967	192.168.0.1	192.168.0.179	DNS	148	Standard query response 0x36af HTTPS beacon4.gvt2.com SOA ns1.google.com
49	01:39:58.886998	192.168.0.179	192.168.0.1	ICMP	162	Destination unreachable (Port unreachable)
41	01:39:58.894117	192.168.0.179	192.168.0.1	DNS	79	Standard query 0x484e A aefd.nelreports.net
42	01:39:58.894595	192.168.0.179	192.168.0.1	DNS	79	Standard query 0x01ce HTTPS aefd.nelreports.net
43	01:39:58.898329	192.168.0.1	192.168.0.179	DNS	188	Standard query 0x48de A aefd.nelreports.net CNAME aefd.nelreports.net.a
44	01:39:58.898329	192.168.0.1	192.168.0.179	DNS	221	Standard query response 0x01ce HTTPS aefd.nelreports.net CNAME aefd.nelreports.net
111	01:39:59.256887	192.168.0.179	192.168.0.1	DNS	75	Standard query 0x114c A docs.google.com
112	01:39:59.257075	192.168.0.179	192.168.0.1	DNS	75	Standard query 0xbee7 HTTPS docs.google.com
113	01:39:59.269708	192.168.0.1	192.168.0.179	DNS	91	Standard query response 0x114c A docs.google.com A 142.250.195.14
114	01:39:59.270006	192.168.0.179	192.168.0.1	DNS	125	Standard query 0x484e A www.bing.com HTTPS docs.google.com SOA ns1.google.com
138	01:39:59.625096	192.168.0.179	192.168.0.1	DNS	72	Standard query 0x7e73 A www.bing.com
139	01:39:59.625278	192.168.0.179	192.168.0.1	DNS	72	Standard query 0x5f92 HTTPS www.bing.com
140	01:39:59.628842	192.168.0.1	192.168.0.179	DNS	257	Standard query response 0x7e73 A www.bing.com CNAME www.www.bing.com.trafficmanagement
141	01:39:59.628842	192.168.0.1	192.168.0.179	DNS	254	Standard query response 0x5f92 HTTPS www.bing.com CNAME www.www.bing.com.trafficmanagement
167	01:39:59.953927	192.168.0.179	192.168.0.1	DNS	75	Standard query 0x234d A ssl.gstatic.com
168	01:39:59.954166	192.168.0.179	192.168.0.1	DNS	75	Standard query 0x28ad HTTPS ssl.gstatic.com
169	01:39:59.958029	192.168.0.1	192.168.0.179	DNS	91	Standard query response 0x234d A ssl.gstatic.com A 142.250.193.227
170	01:39:59.958029	192.168.0.1	192.168.0.179	DNS	132	Standard query response 0x28ad HTTPS ssl.gstatic.com SOA ns1.google.com
229	01:40:12.977467	192.168.0.179	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
230	01:40:13.026352	192.168.0.1	192.168.0.179	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
231	01:40:13.028628	192.168.0.179	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
232	01:40:13.092020	192.168.0.1	192.168.0.179	DNS	234	Standard query response 0x0002 NS mit.edu NS ns.eur5.akam.net NS asia2.akam.net NS

Figure 40: Destination IP Address of DNS Query Message

Default Gateway . . . . .	: 192.168.0.1
DHCP Server . . . . .	: 192.168.0.1
DHCPv6 IAID . . . . .	: 109089075
DHCPv6 Client DUID. . . . .	: 00-01-00-01-2A-18-B7-41-04-0E-3C-51-06-96
DNS Servers . . . . .	: 192.168.0.1
NetBIOS over Tcpip. . . . .	: Enabled

Figure 41: DNS Query Destination IP with Local DNS Server

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

The ”Type” of DNS query is ”**NS**”. **No**, the query message does not contain any ”**answers**”.

```
▼ Domain Name System (query)
  Transaction ID: 0x0002
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
    ▶ mit.edu: type NS, class IN
      [Response In: 232]
```

Figure 42: Examination of DNS Query Message

**3.2.14 Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?**

The MIT nameservers that are provided by the response messages are given in the below picture. **No**, This response message does not provide the IP addresses of the MIT namesers.

```
▼ Domain Name System (response)
  Transaction ID: 0x0002
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
    ▶ mit.edu: type NS, class IN
  ▶ Answers
    ▶ mit.edu: type NS, class IN, ns eur5.akam.net
    ▶ mit.edu: type NS, class IN, ns asia2.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▶ mit.edu: type NS, class IN, ns asia1.akam.net
    ▶ mit.edu: type NS, class IN, ns usw2.akam.net
    ▶ mit.edu: type NS, class IN, ns use5.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▶ mit.edu: type NS, class IN, ns use2.akam.net
  [Request In: 231]
  [Time: 0.063400000 seconds]
```

Figure 43: DNS Response Message with MIT Nameservers

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

The DNS query message is sent to the IP address **192.168.0.1**. Yes, this is the same IP address of my default local DNS server.

No.	Time	Source	Destination	Protocol	Length	Info
64	01:44:35.767791	192.168.0.179	192.168.0.1	DNS	73	Standard query 0xb5d5 A bitsy.mit.edu
65	01:44:35.810383	192.168.0.179	192.168.0.1	DNS	73	Standard query 0xb5d5 A bitsy.mit.edu
66	01:44:35.832119	192.168.0.1	192.168.0.179	DNS	89	Standard query response 0xb5d5 A bitsy.mit.edu A 18.0.72.3
67	01:44:35.839324	192.168.0.179	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
68	01:44:35.860237	192.168.0.1	192.168.0.179	DNS	89	Standard query response 0xb5d5 A bitsy.mit.edu A 18.0.72.3
69	01:44:35.860306	192.168.0.179	192.168.0.1	ICMP	117	Destination unreachable (Port unreachable)
77	01:44:37.847502	192.168.0.179	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
82	01:44:39.858612	192.168.0.179	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
83	01:44:41.865369	192.168.0.179	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
97	01:44:43.872550	192.168.0.179	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Figure 44: Destination IP Address of DNS Query Message

```

Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 109089075
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-18-B7-41-04-0E-3C-51-06-96
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled

```

Figure 45: Verification of Local DNS Server IP Address

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

The “Type” of DNS query is “A”. No, the query message does not contain any “answers”.

```

▼ Domain Name System (query)
  Transaction ID: 0xb5d5
  ▶ 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: 66] ↓

```

Figure 46: Examination of DNS Query Message

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

One “answer” is provided. The answer contains the Name, Type, Class, Time to live, Data length, and Address.

```
Domain Name System (response)
  Transaction ID: 0xb5d5
  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
      Name: bitsy.mit.edu
      [Name Length: 13]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  Answers
    bitsy.mit.edu: type A, class IN, addr 18.0.72.3
      Name: bitsy.mit.edu
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 388 (6 minutes, 28 seconds)
      Data length: 4
      Address: 18.0.72.3
      [Request In: 64]
      [Time: 0.064328000 seconds]
```

Figure 47: Examination of DNS Response Message

.....THE END.....