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

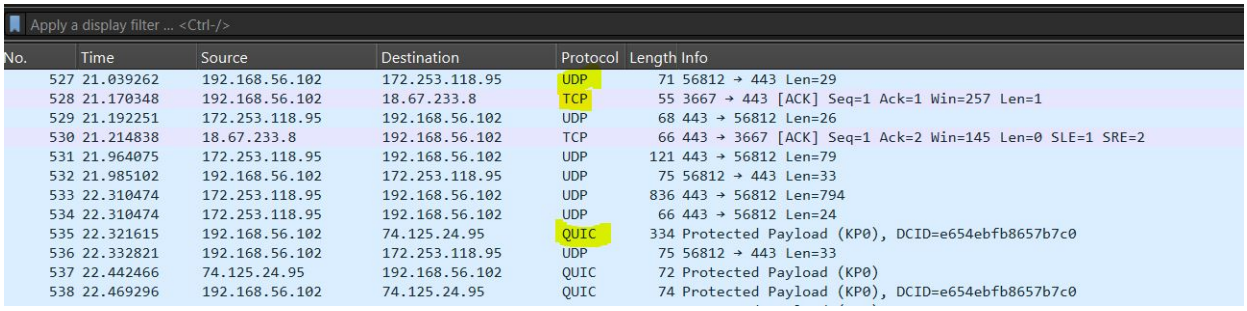

Figure 1: Protocols Identified in the Packet-Listing Window

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

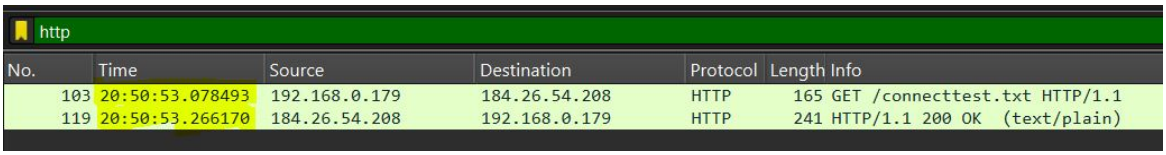

Figure 2: Time Duration Between HTTP GET and HTTP OK Messages

1.3 What is the Internet address of the gaia.cs.umass.edu (also knwon 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**

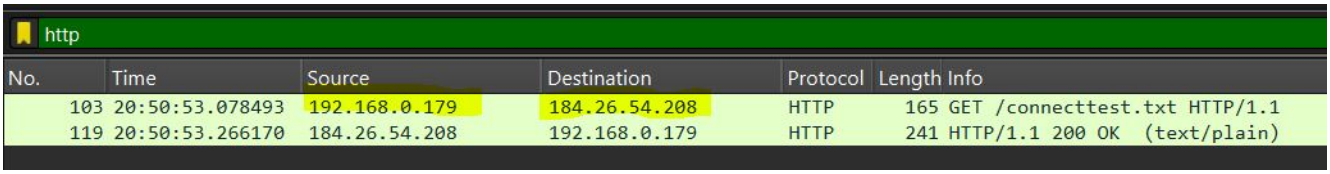

Figure 3: IP Addresses of the gaia.cs.umass.edu Server and the Client's Computer

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

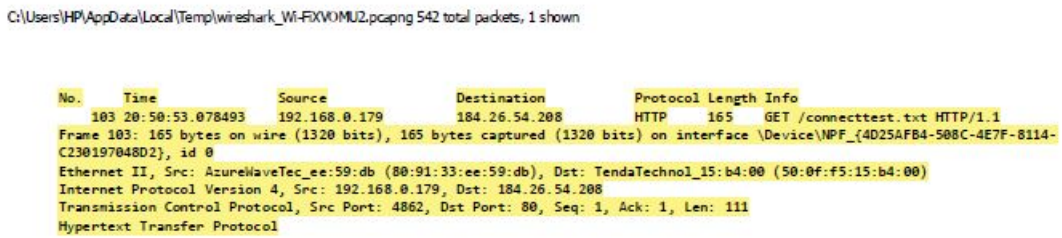

Figure 4: HTTP GET Request Message

- The HTTP message OK

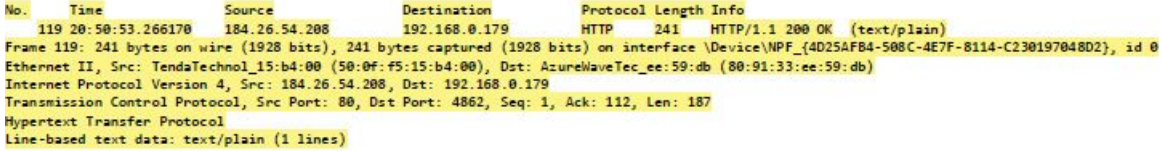

Figure 5: HTTP OK Response Message

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.

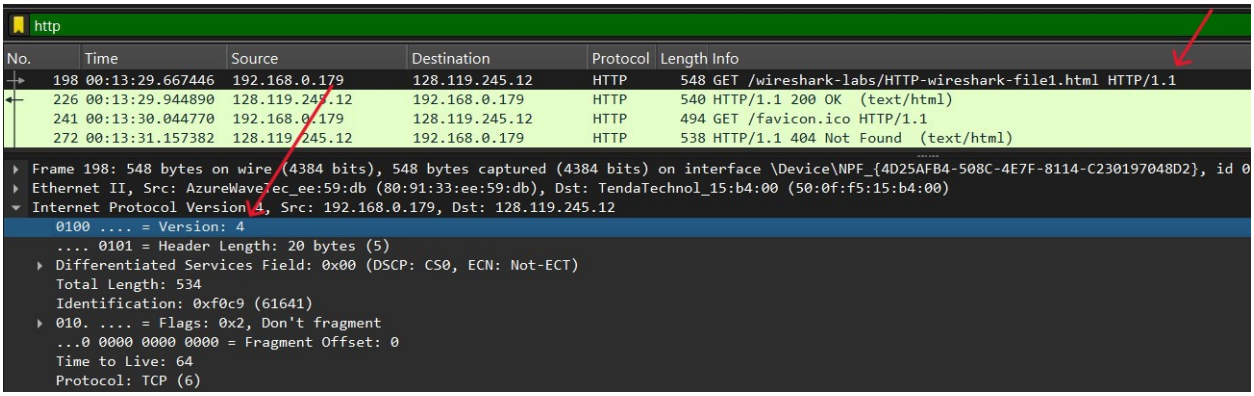

Figure 6: HTTP Versions Used by the Browser and the Server

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).

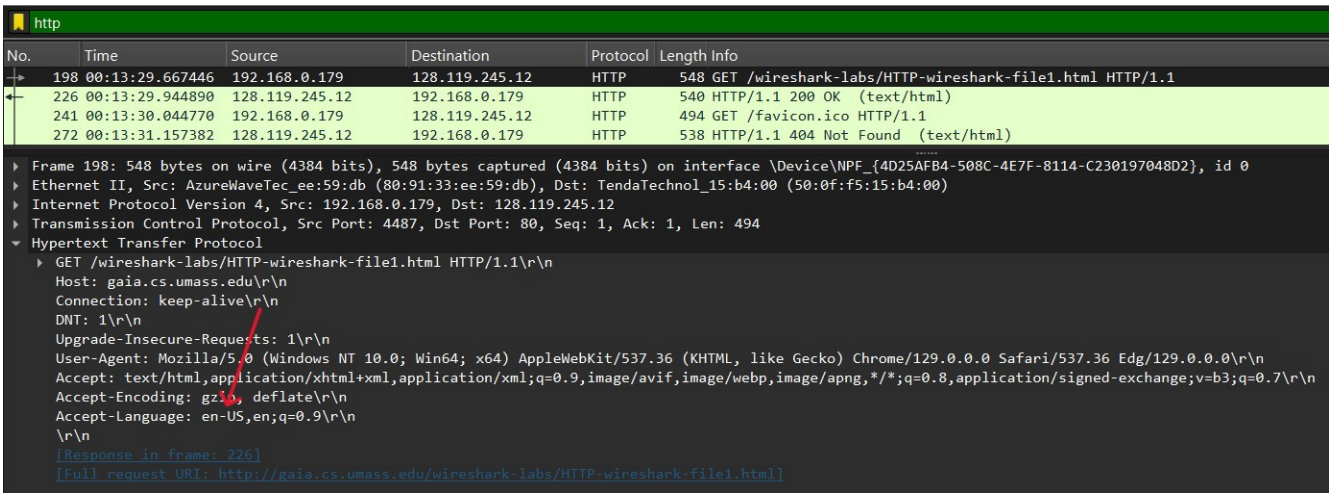

Figure 7: Languages Accepted by the Browser

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**

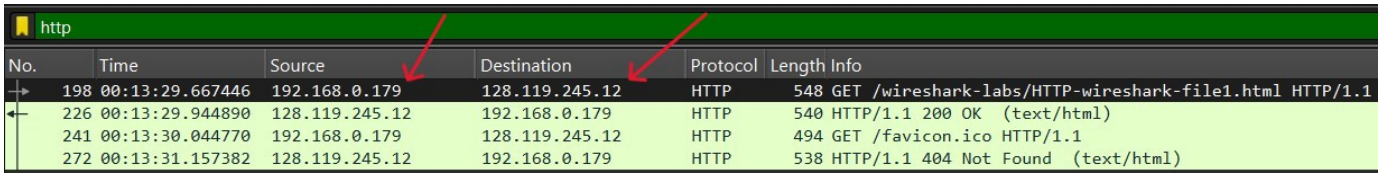

Figure 8: IP Addresses of the Client and the Server

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**

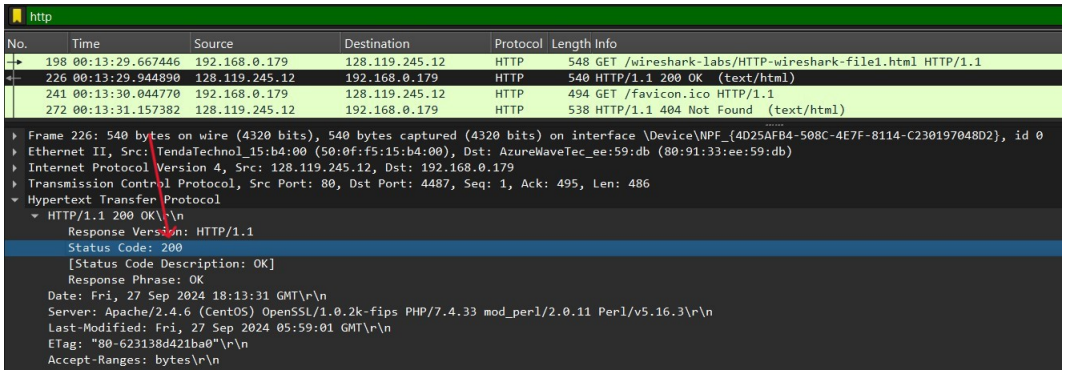

Figure 9: HTTP Status Code Returned by the Server

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.**

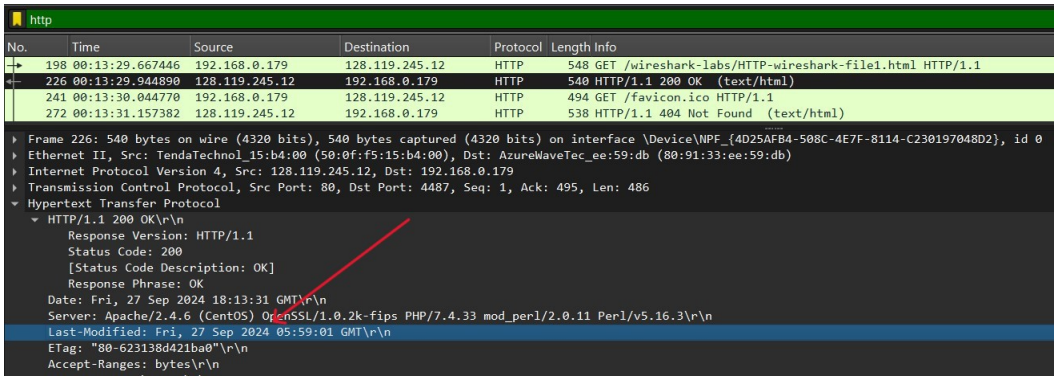

Figure 10: Last Modification Date of the Retrieved HTML File

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

128 bytes of content are being returned to my browser.

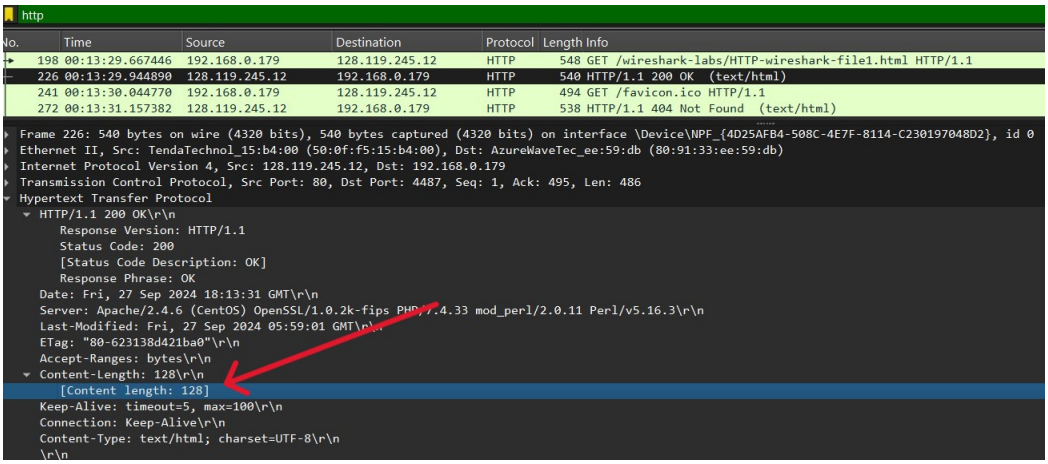

Figure 11: Total Number of Bytes Returned by the Server to the Browser

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.

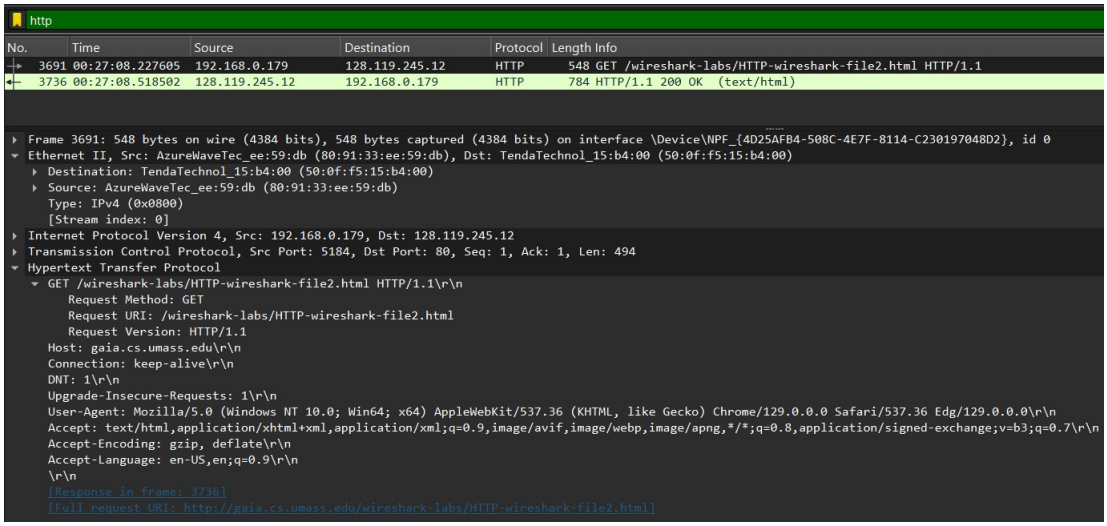

Figure 12: Absence of "If-Modified-Since" Header in the First HTTP GET Request

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.

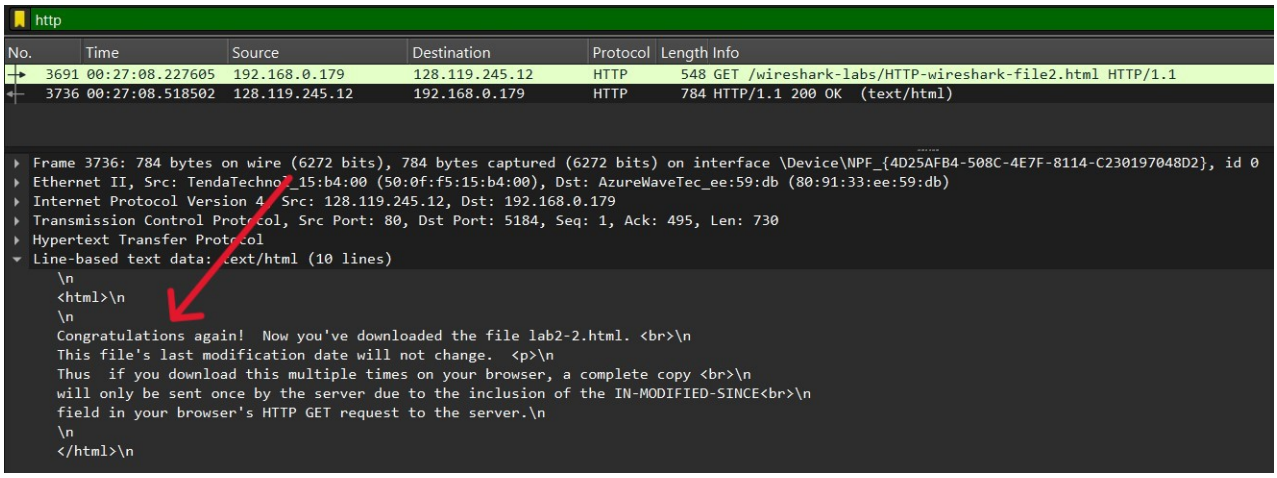

Figure 13: Inspection of the Server's Response Content

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.

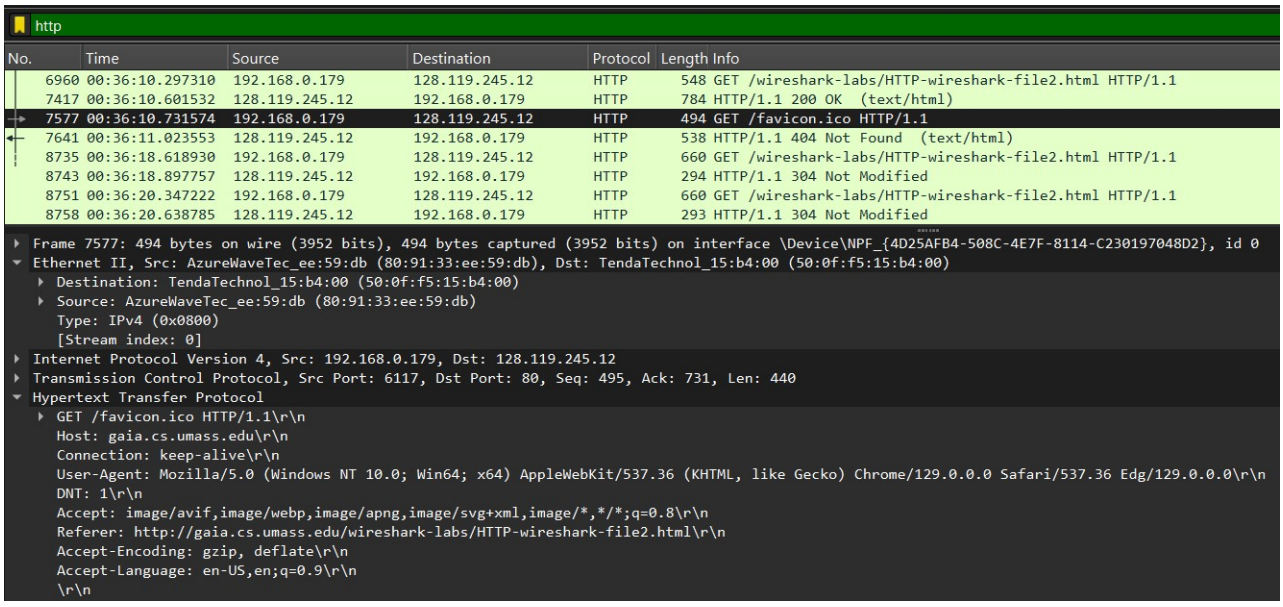

Figure 14: Absence of "If-Modified-Since" Header in the Second HTTP GET Request

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.

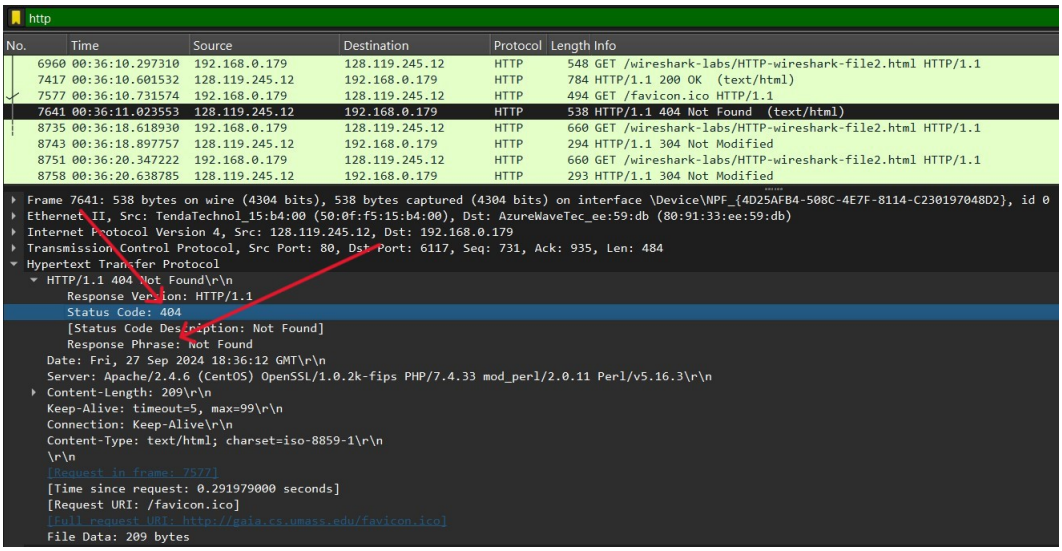

Figure 15: Server Response to the Second HTTP GET Request

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**

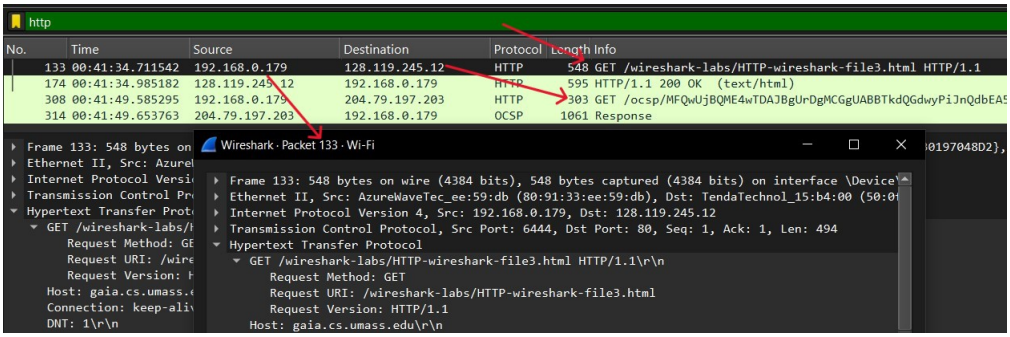

Figure 16: HTTP GET Requests and Corresponding Responses

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**

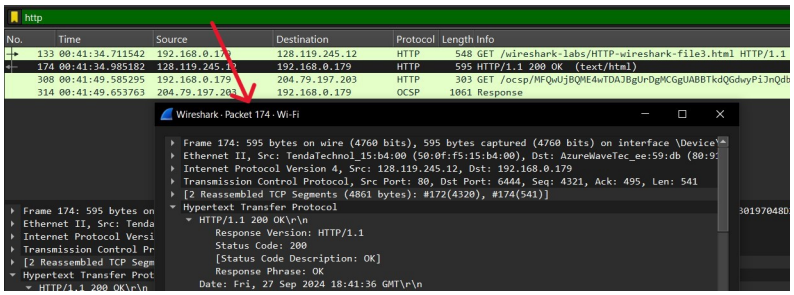

Figure 17: Packet Containing HTTP Status Code and Phrase

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"**.

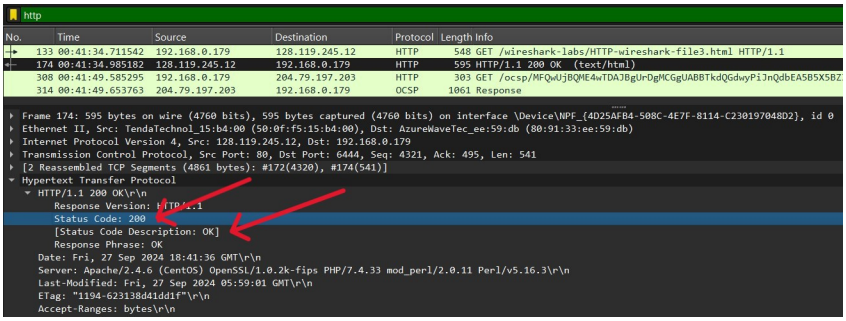

Figure 18: HTTP Status Code and Phrase in Response

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.

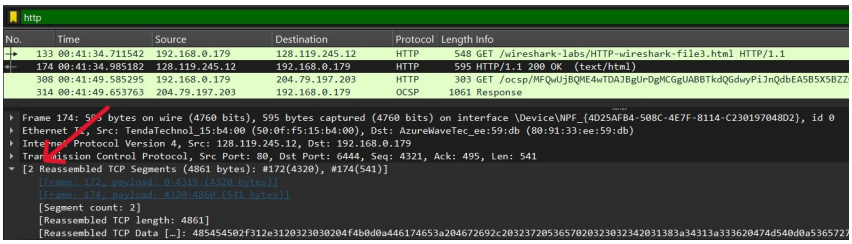

Figure 19: Data-Containing TCP Segments for HTTP Response

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**

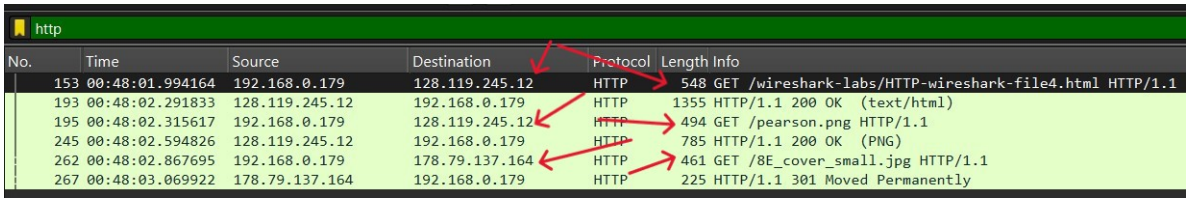

Figure 20: Summary of HTTP GET Requests Sent by the Browser

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.

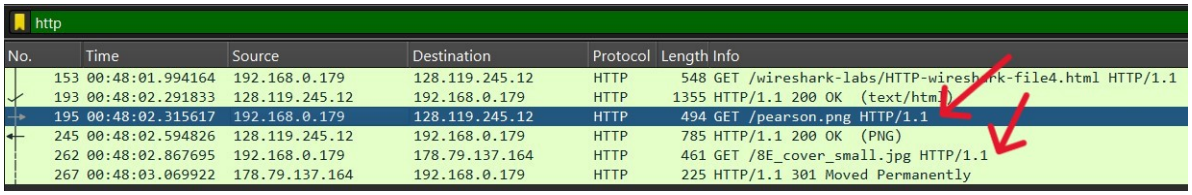

Figure 21: Analysis of Image Download Methodology

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.

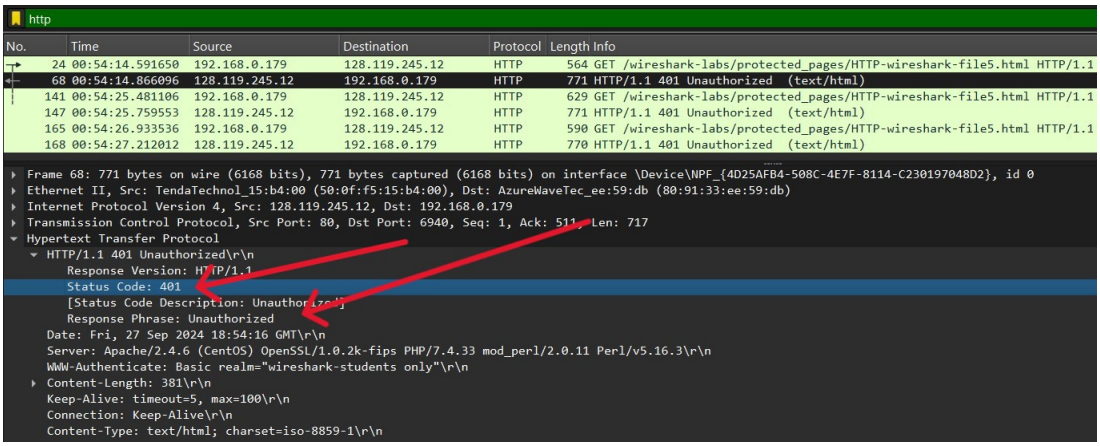

Figure 22: Server Response to Initial HTTP GET Request

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.

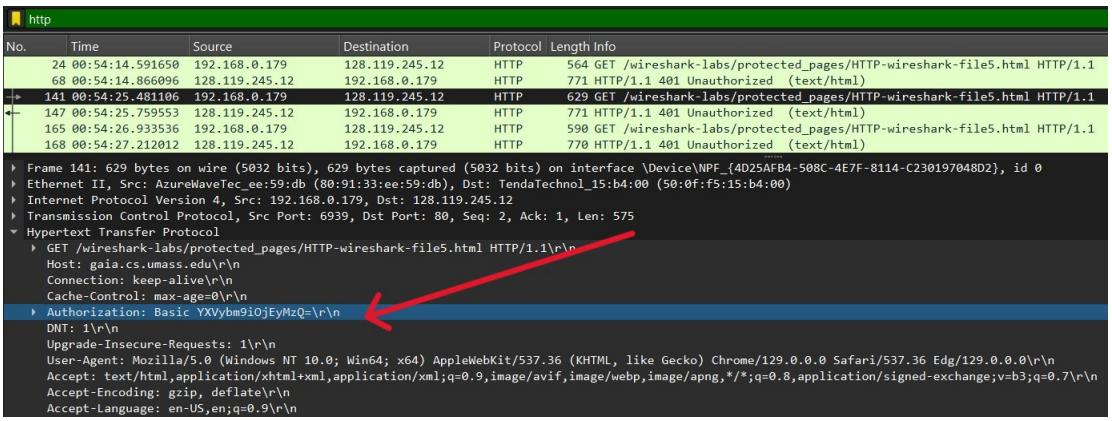

Figure 23: New Header Field in Second HTTP GET Request

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**

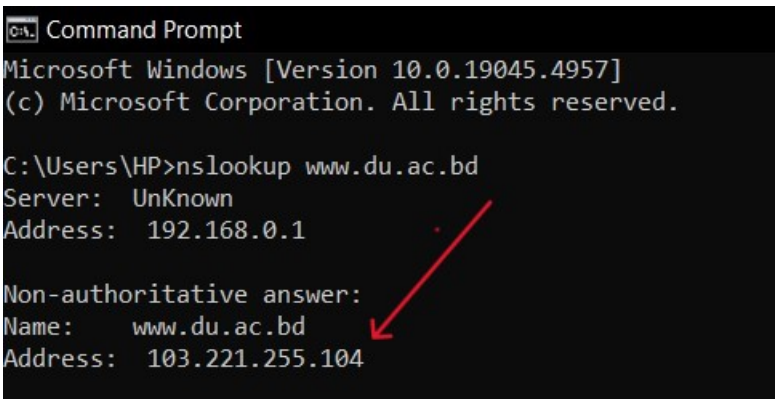

Figure 24: nslookup Command Output for Asian Web Server

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:

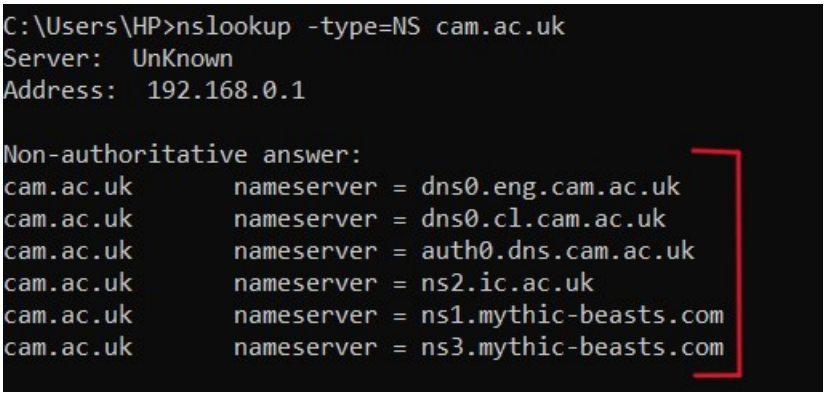

Figure 25: Authoritative DNS Servers for a European University

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**

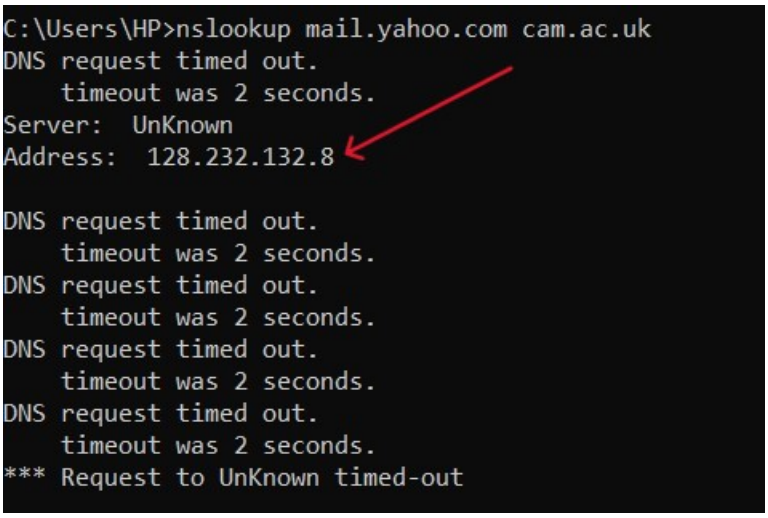

Figure 26: IP address of mail server

3.2 Tracing DNS with Wireshark

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

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

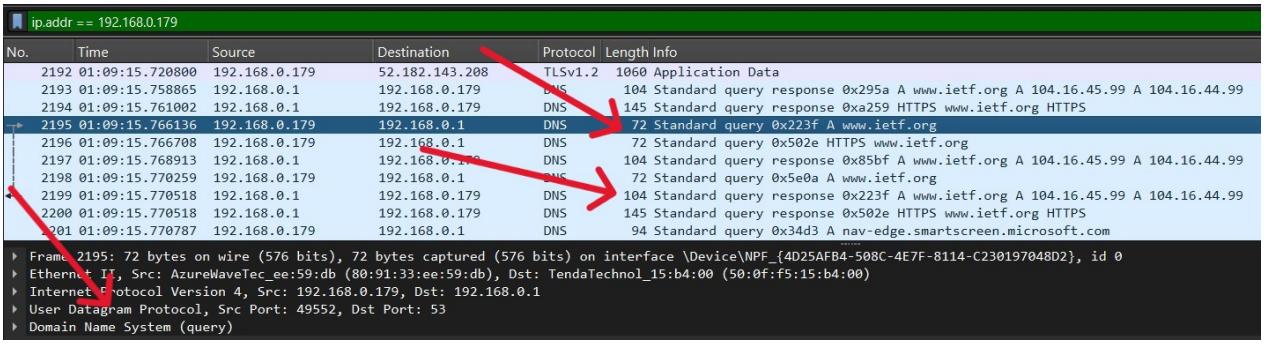

Figure 27: DNS Query and Response Protocols

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**.

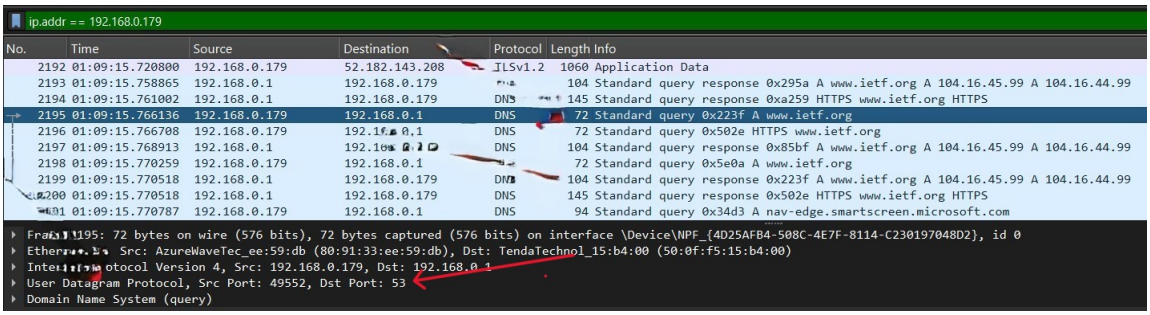

Figure 28: Source and Destination Ports in DNS Query and Response Messages

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.

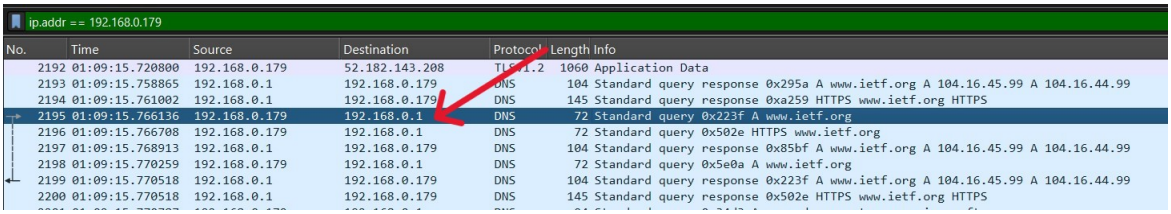

Figure 29: DNS query message IP address

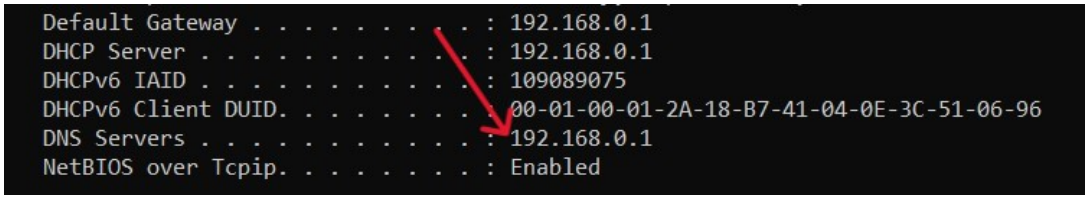

Figure 30: DNS server IP address

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"**.

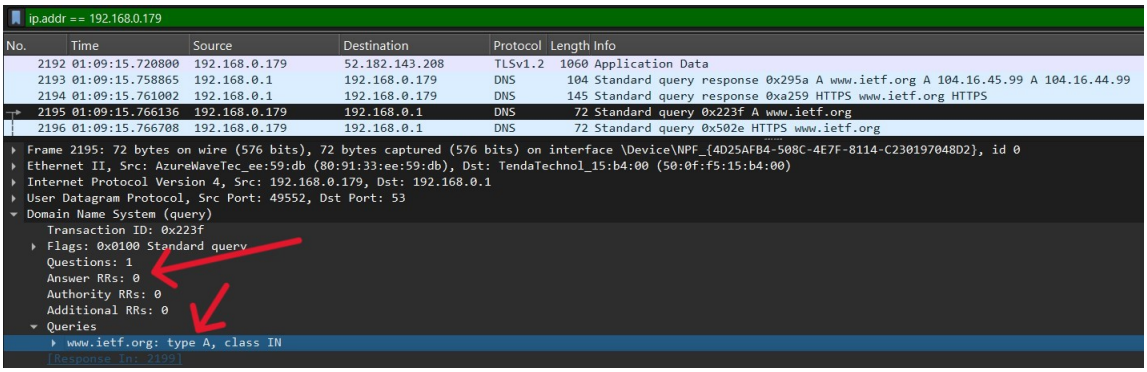

Figure 31: DNS Query Type and Contents

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**.

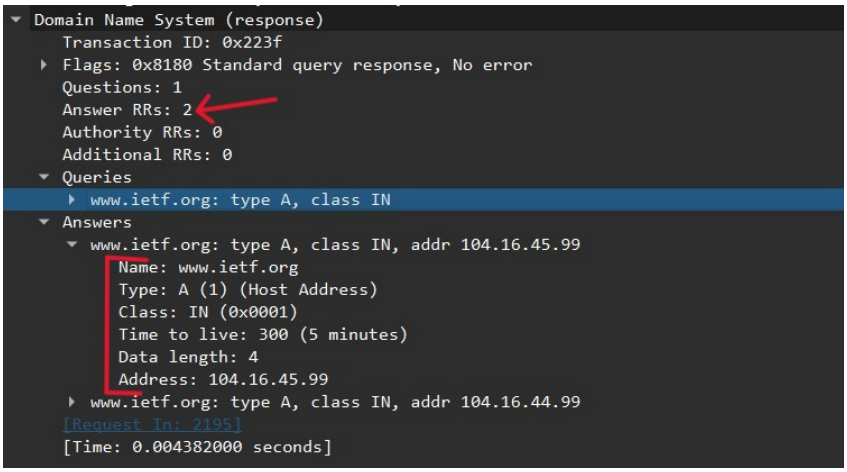

Figure 32: DNS Response Message and Answer Details

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.

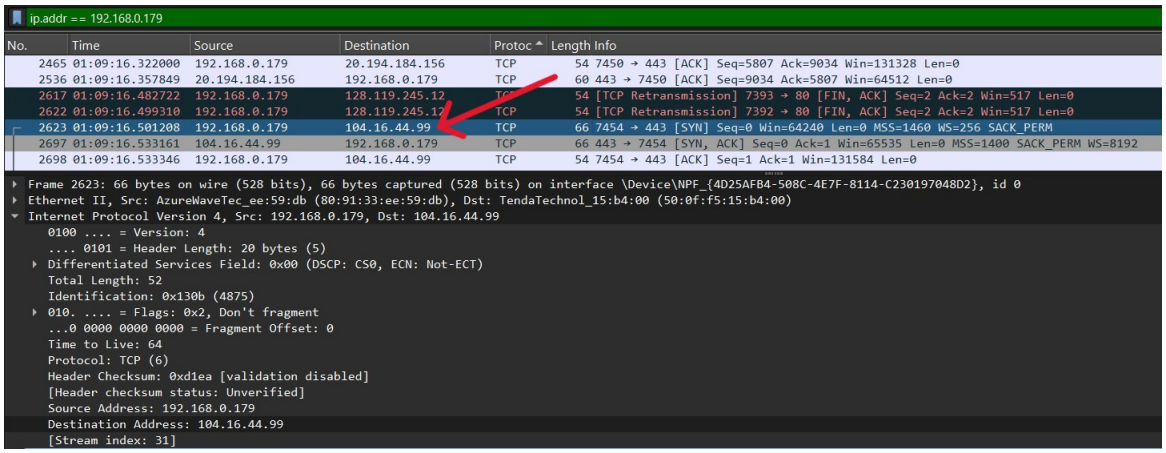

Figure 33: TCP SYN Packet and DNS Response IP Address Match

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**.

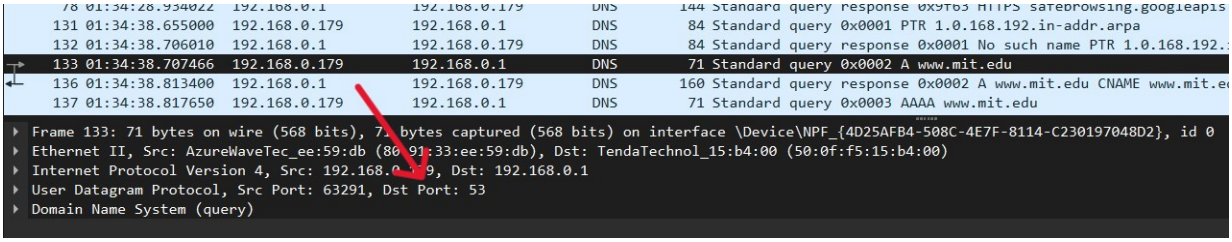

Figure 34: Source and Destination Ports of DNS Query and Response Messages

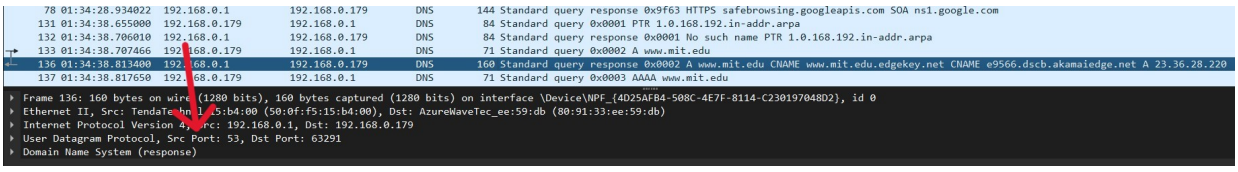

Figure 35: Source and Destination Ports of DNS Query and Response Messages

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.

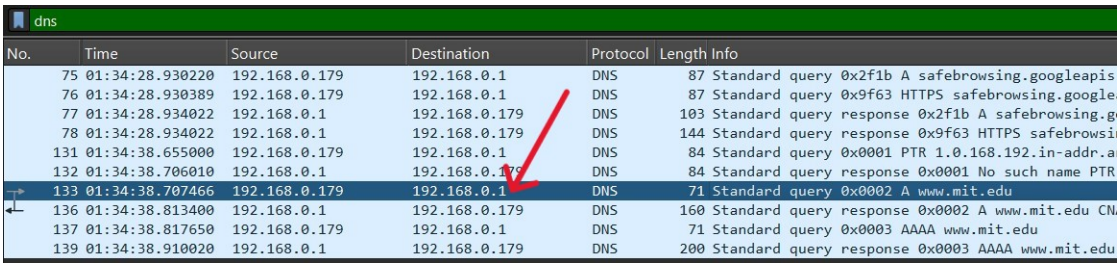

Figure 36: Destination IP Address of DNS Query Message

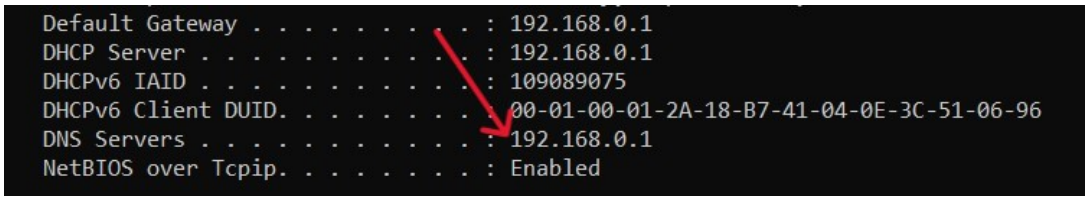

Figure 37: DNS Query Destination IP with Local DNS Server

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".

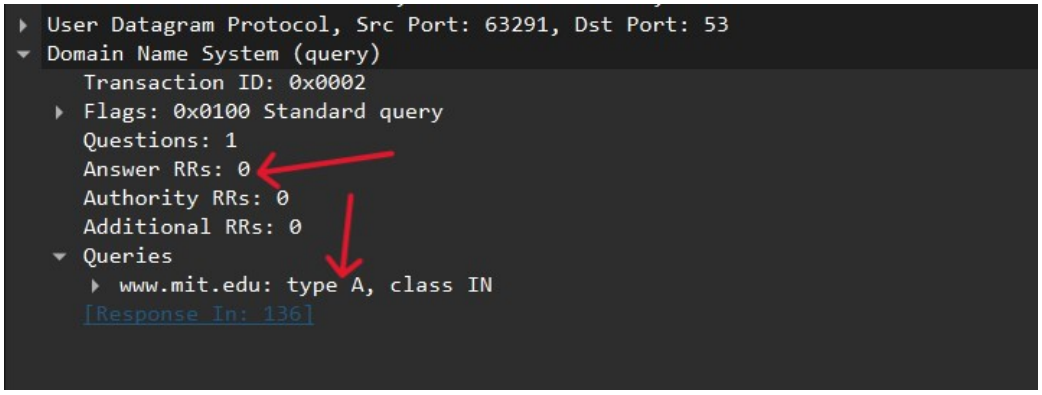

Figure 38: DNS Query Type and Contents

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**.

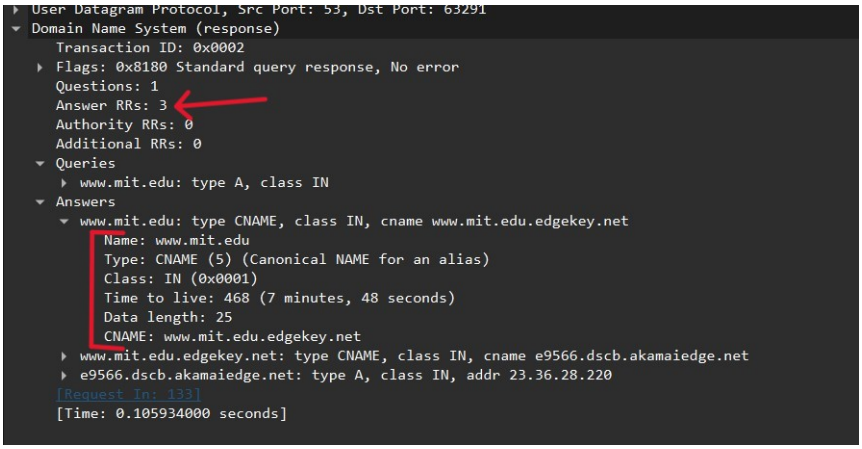

Figure 39: DNS Response Message with Answers

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.

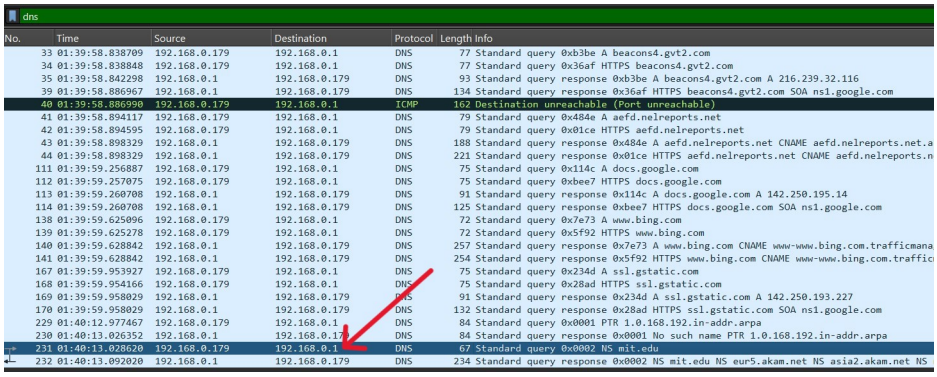

Figure 40: Destination IP Address of DNS Query Message

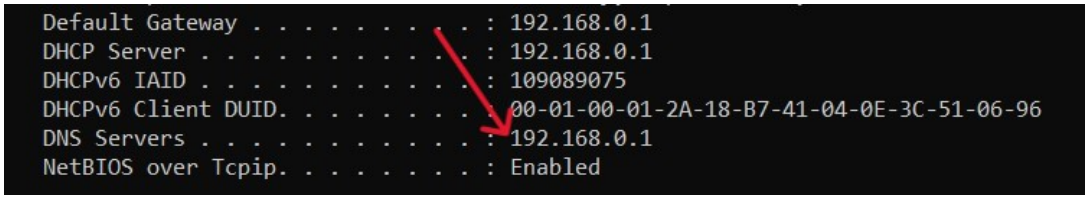

Figure 41: DNS Query Destination IP with Local DNS Server

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"**.

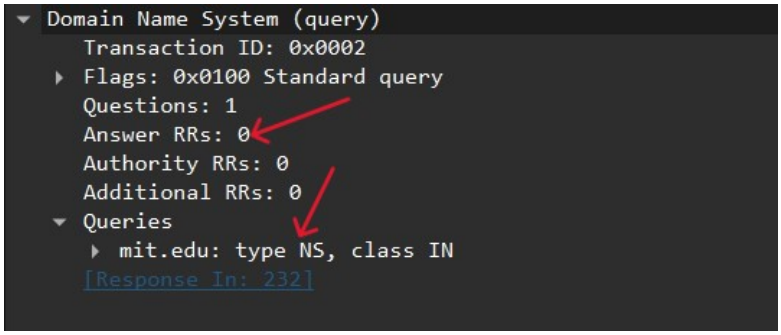

Figure 42: Examination of DNS Query Message

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.

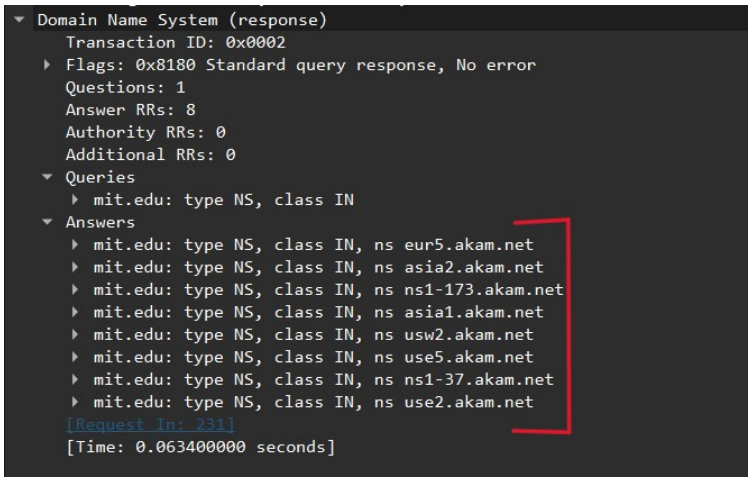

Figure 43: DNS Response Message with MIT Nameservers

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.

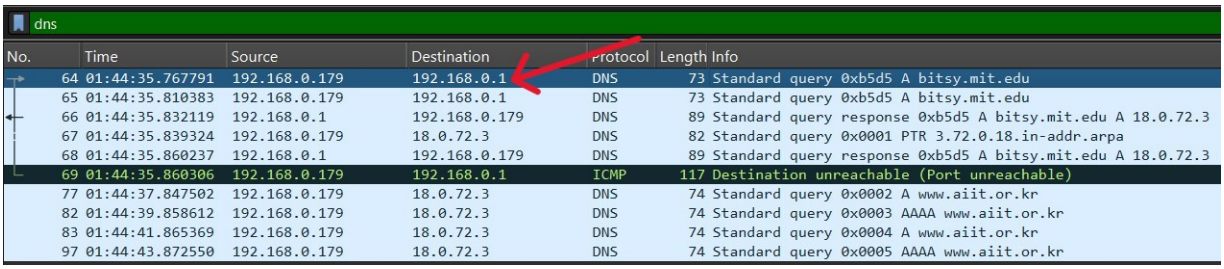

Figure 44: Destination IP Address of DNS Query Message

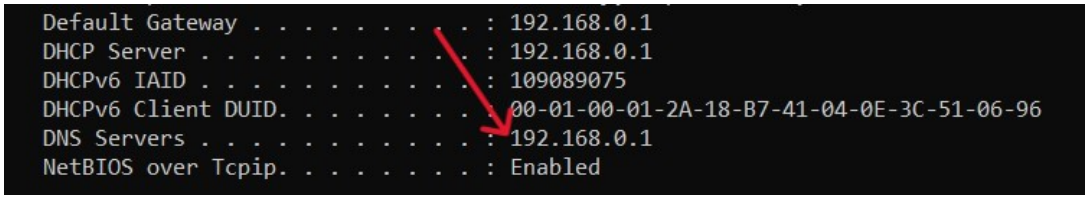

Figure 45: Verification of Local DNS Server IP Address

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"**.

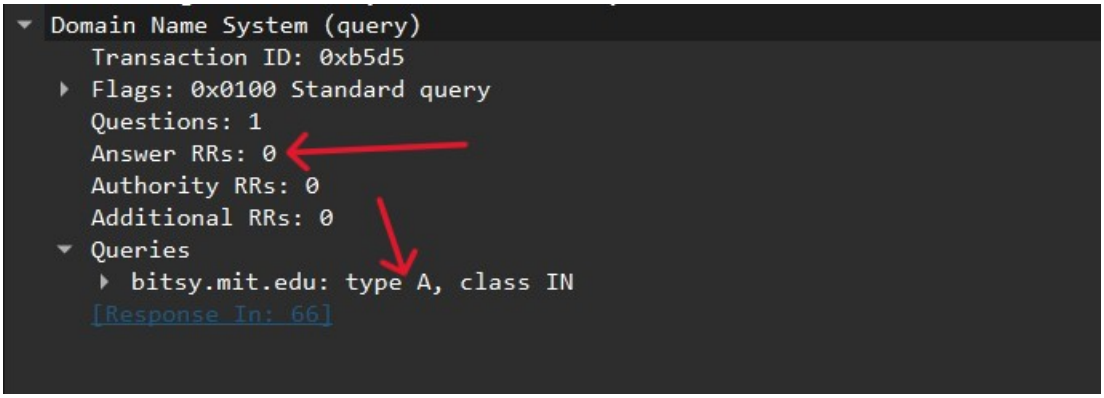

Figure 46: Examination of DNS Query Message

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**.

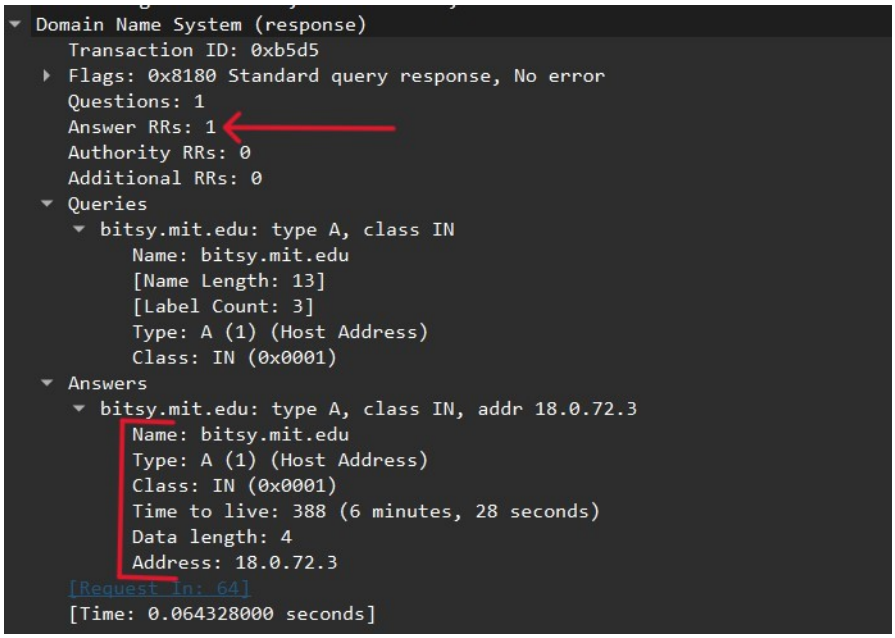

Figure 47: Examination of DNS Response Message

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