

Name : Jawad Ahmed

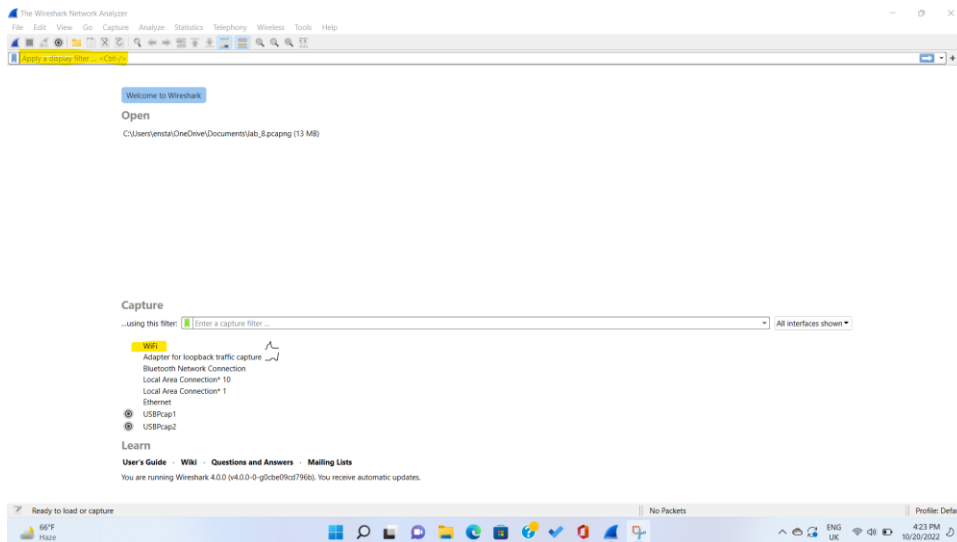
Roll No : 20P-0165

Section : BCS-5A

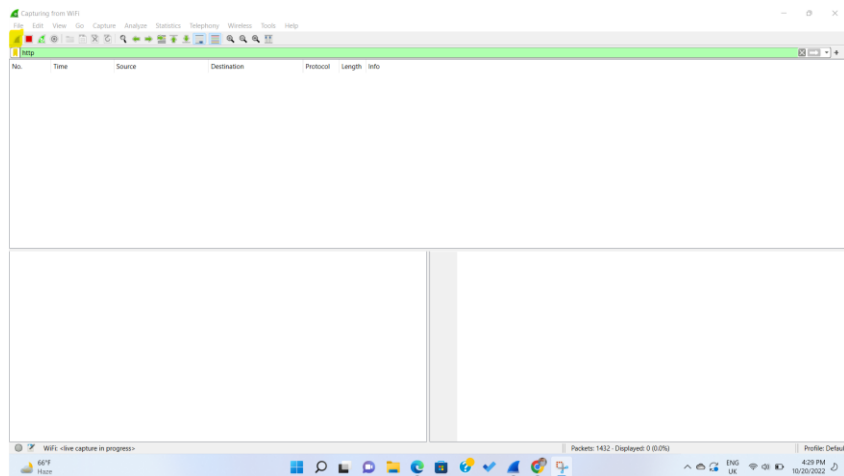
Computer Networks Lab

Task: Running the Wireshark

When Wireshark is successfully installed in your system. First time you will see this screen.



In the search bar type **http** and from the below options double click on **wifi**.
After that you will see this screen.



To capture the packets begin the Wireshark packet capture.

Task: The Basic HTTP GET/response interaction

Let's begin our exploration of HTTP by downloading a very simple HTML file .

Do the following steps:

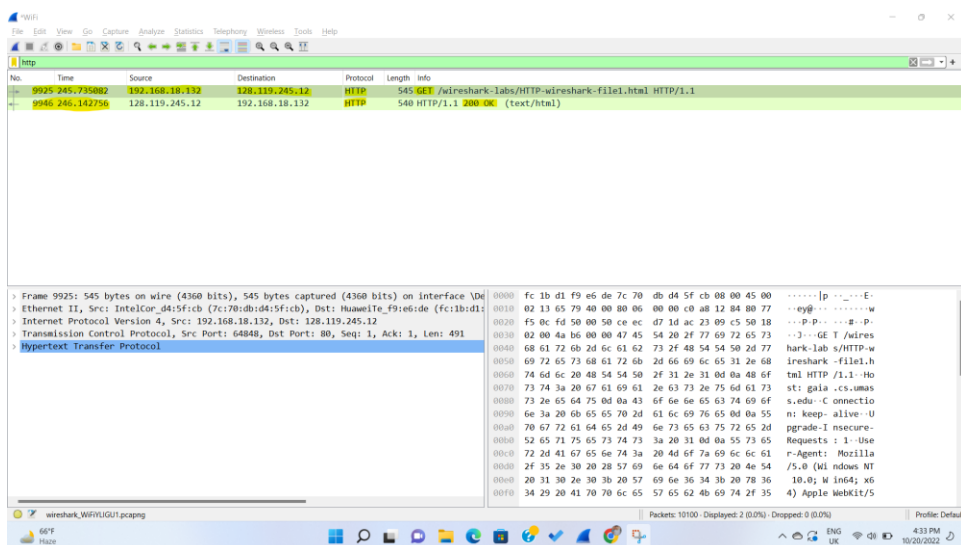
1. Start up your web browser.
4. Enter the following to your browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

Your browser should display the very simple, one-line HTML file.

5. Stop Wireshark packet capture.

You will see this screen.



1. First line means that it is the **GET** request which is used to get the contents of page.
2. Second Line means that response is **200** that mean **OK**. Page downloaded in to the cache successfully.

Task: By looking at the information in the HTTP GET and response messages, answer the following questions

- 1. Is your browser running HTTP version 1.0, 1.1, or 2?**
- 2. What version of HTTP is the server running?**
- 3. What languages (if any) does your browser indicate that it can accept to the server?**
- 4. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?**
- 5. What is the status code returned from the server to your browser?**
- 6. When was the HTML file that you are retrieving last modified at the server?**
- 7. How many bytes of content are being returned to your browser?**
- 8. 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.**

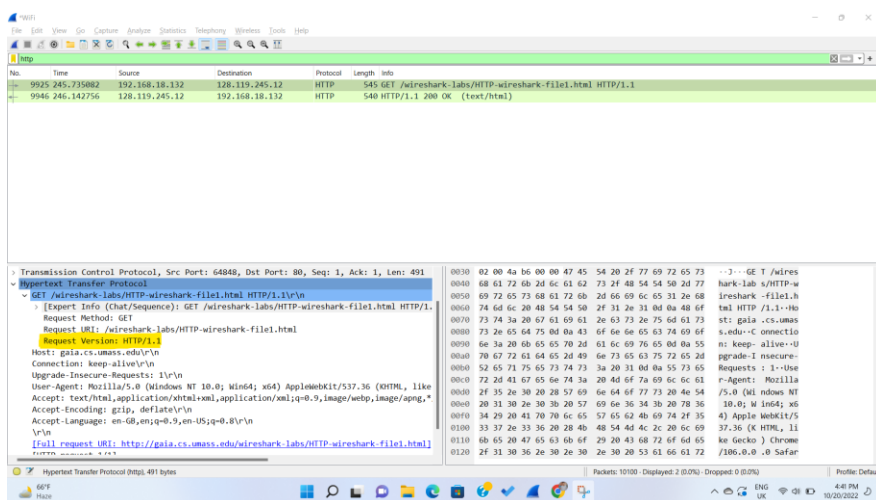
Answers

1. Is your browser running HTTP version 1.0, 1.1, or 2?

To see that what version your browser is running select line one in which **GET** request is made.

Then Go to the Hypertext Transfer Protocol -> Select Get -> Request Version

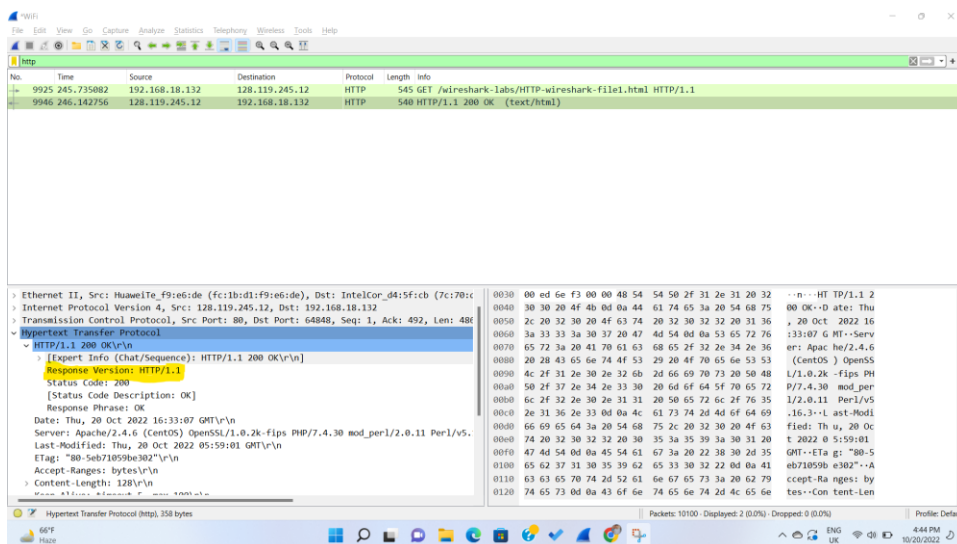
My browser is running on HTTP version 1.1.



2. What version of HTTP is the server running?

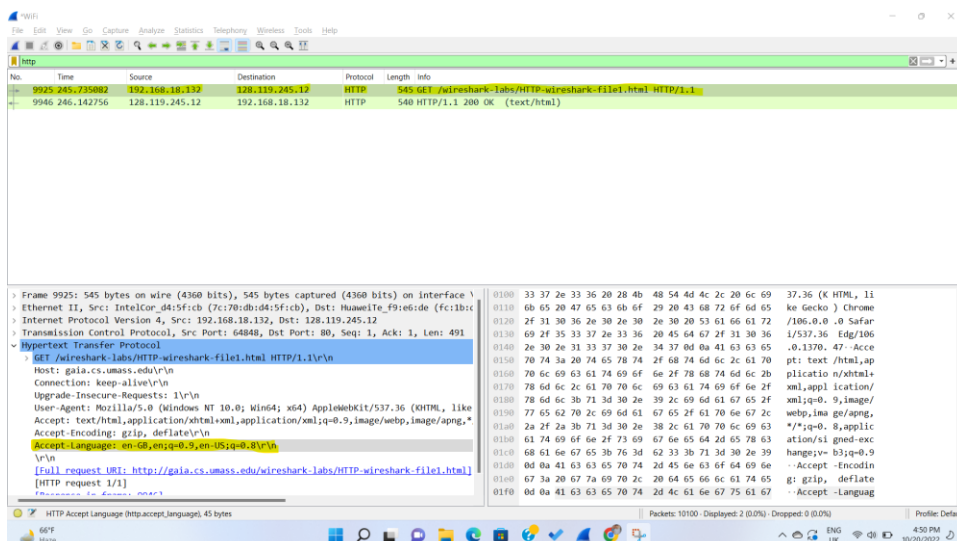
To see that what version of HTTP server is running select second line in which **200** response is coming.

Then Go to the Hypertext Transfer Protocol -> Select HTTP/1.1 200 OK /r/n -> Response Version
Server has a HTTP Version 1.1.



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

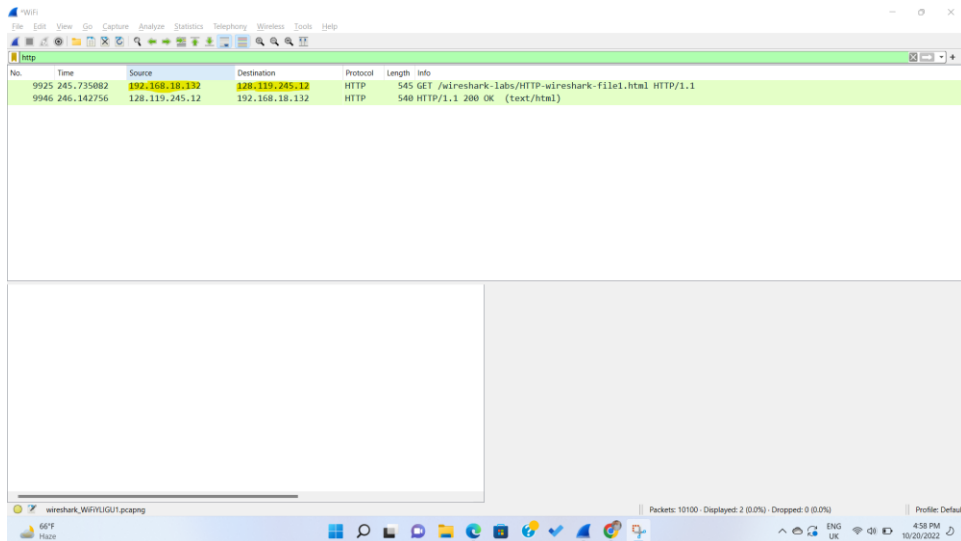
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8\r\n. American English language is accepted language to the server.



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

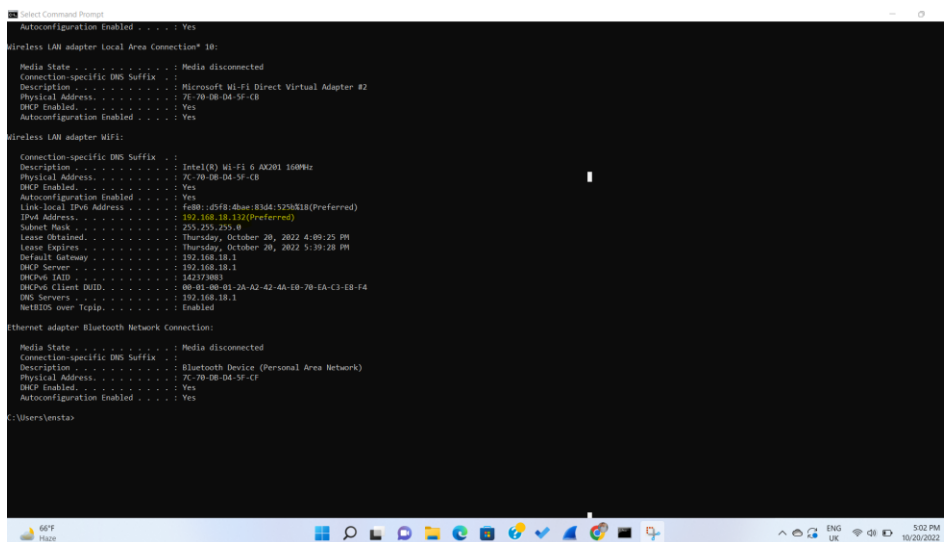
IP address of my computer: 192.168.18.132

IP address of the gaia.cs.umass.edu server = 128.119.245.12



Verification:

My PC IP:



Server IP:

```
C:\Users\ensta>ping gaia.cs.umass.edu

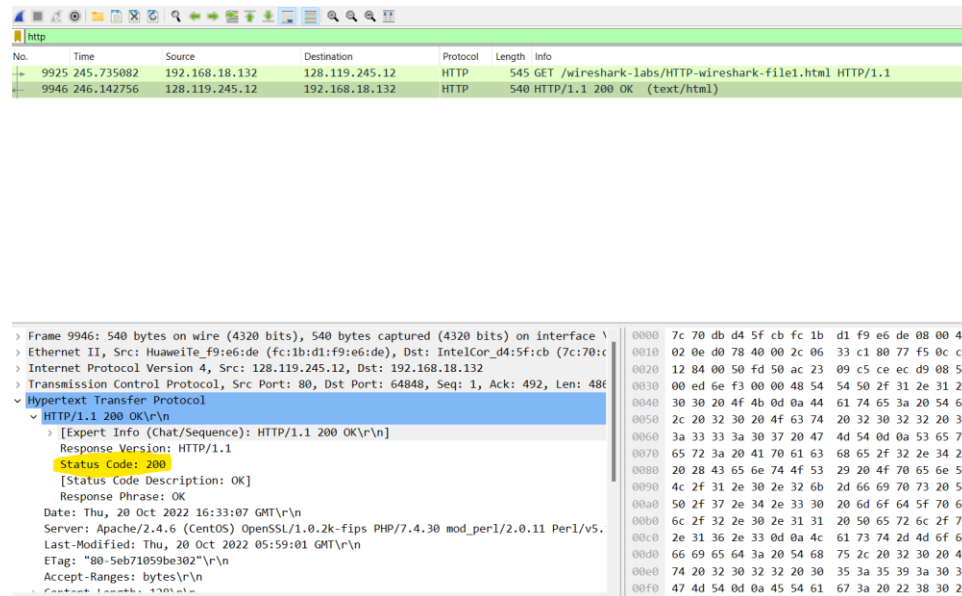
Pinging gaia.cs.umass.edu [128.119.245.12] with 32 bytes of data:
Reply from 128.119.245.12: bytes=32 time=346ms TTL=44
Reply from 128.119.245.12: bytes=32 time=362ms TTL=44
Reply from 128.119.245.12: bytes=32 time=312ms TTL=44
Reply from 128.119.245.12: bytes=32 time=325ms TTL=44

Ping statistics for 128.119.245.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 312ms, Maximum = 362ms, Average = 336ms

C:\Users\ensta>
```

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

The status code returned from the server is **200** that mean **OK**. That means the page is successfully retrieved without any error.



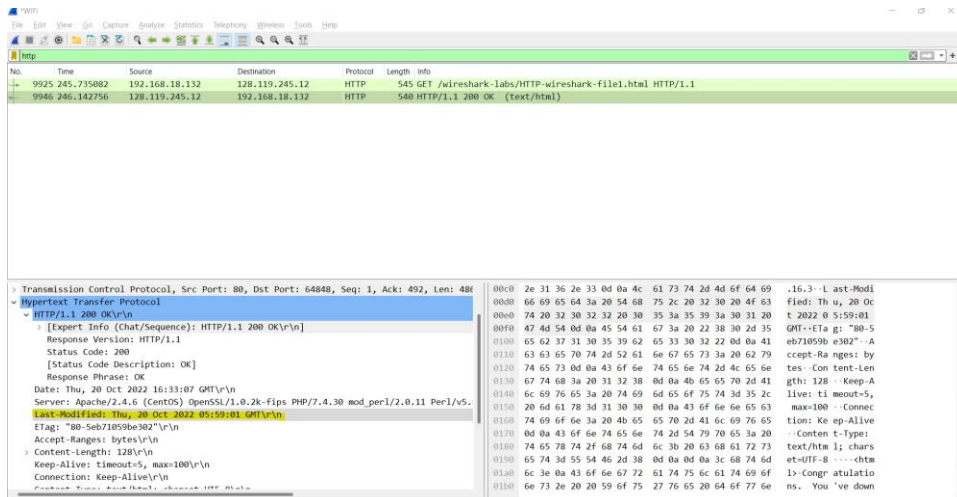
The image shows a Wireshark packet capture of an HTTP GET request and its response. The packet list on the left shows packet 9946 as the selected item, which is an HTTP 200 OK response. The packet details pane on the right shows the structure of the HTTP response, including the status code 200 and the response phrase 'OK'.

No.	Time	Source	Destination	Protocol	Length	Info
9925	245.735082	192.168.18.132	128.119.245.12	HTTP	545	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
9946	246.142756	128.119.245.12	192.168.18.132	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 9946: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \	0000	7c 70 db d4 5f cb fc 1b d1 f9 e6 de 08 00 45
> Ethernet II, Src: HuaweiTe_f9:e6:de (fc:1b:d1:f9:e6:de), Dst: IntelCor_d4:5f:cb (7c:70:c	0010	02 0e d0 78 40 00 2c 06 33 c1 80 77 f5 0c c0
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.18.132	0020	12 84 00 50 fd 50 ac 23 09 c5 ce ec d9 08 50
> Transmission Control Protocol, Src Port: 80, Dst Port: 64848, Seq: 1, Ack: 492, Len: 486	0030	00 ed 6e f3 00 00 48 54 54 50 2f 31 2e 31 20
> Hypertext Transfer Protocol	0040	30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68
> HTTP/1.1 200 OK\r\n	0050	2c 20 32 30 20 4f 63 74 20 32 30 32 32 20 31
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]	0060	3a 33 33 3a 30 37 20 47 4d 54 0d 0a 53 65 72
> Response Version: HTTP/1.1	0070	65 72 3a 20 41 70 61 63 68 65 2f 32 2e 3a 2e
> Status Code: 200	0080	20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53
> [Status Code Description: OK]	0090	4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50
> Response Phrase: OK	00a0	50 2f 37 2e 34 2e 33 30 20 6d 6f 64 5f 70 65
> Date: Thu, 20 Oct 2022 16:33:07 GMT\r\n	00b0	6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76
> Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.	00c0	2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64
> Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT\r\n	00d0	66 69 65 64 3a 20 54 68 75 2c 20 32 30 20 4f
> ETag: "80-5eb71059be302"\r\n	00e0	74 20 32 30 32 32 20 30 35 3a 35 39 3a 30 31
> Accept-Ranges: bytes\r\n	00f0	47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d

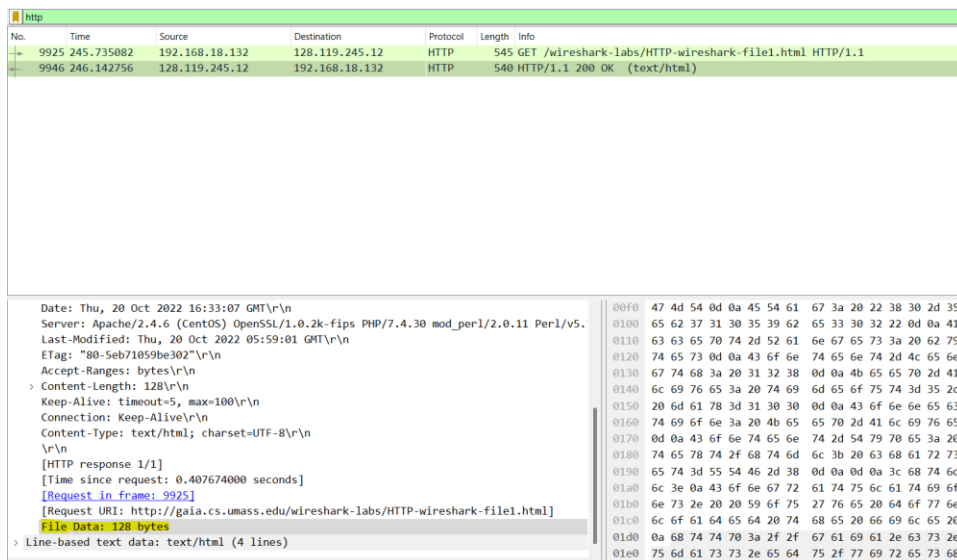
6. When was the HTML file that you are retrieving last modified at the server?

The page is last modified: Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT\r\n



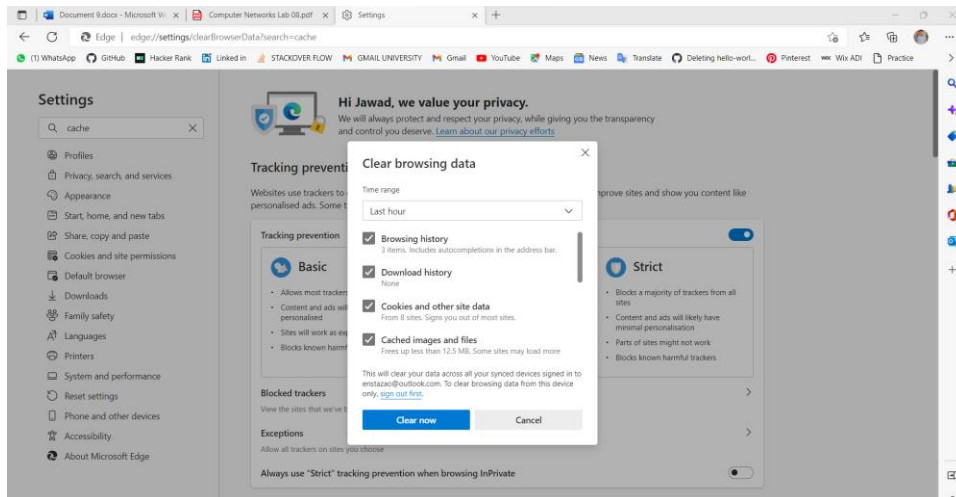
7. How many bytes of content are being returned to your browser?

128 bytes of content are being returned to the browser.



Task2: The HTTP CONDITIONAL GET/response interaction

Before doing this ask I successfully clear the cache.



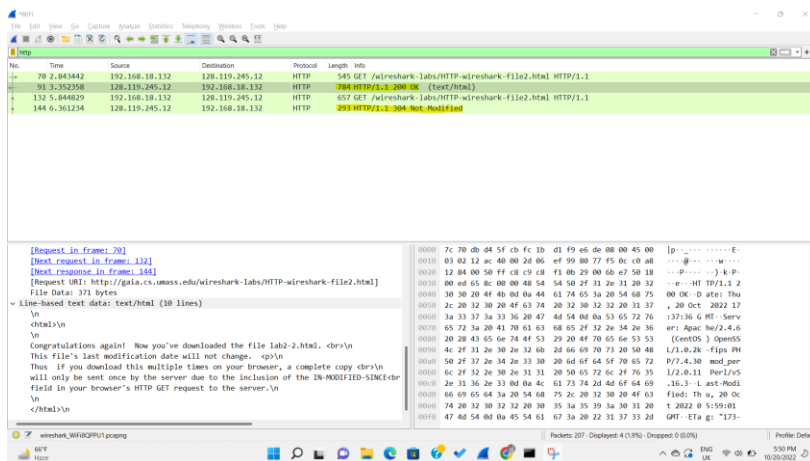
Now do the following:

- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser:

`http://gaia.cs.umass.edu/wireshark-labs/HTTPwireshark-file2.html`

- Your browser should display a very simple five-line HTML file.
- Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)

First time page is fetched successfully and **200** response came. But when I refreshed **304** response came. That mean page is not modified and page is already present in the cache.



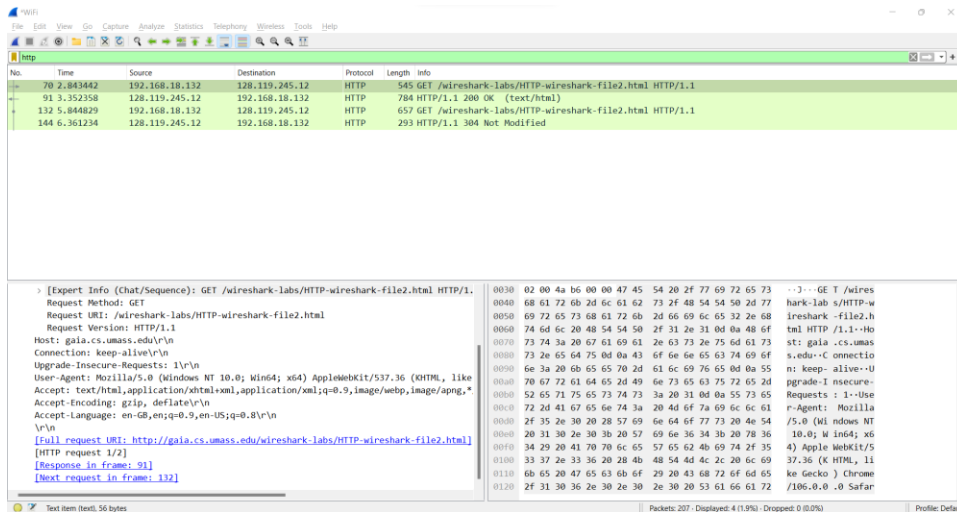
Task2: Answer the following questions:

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

Answers

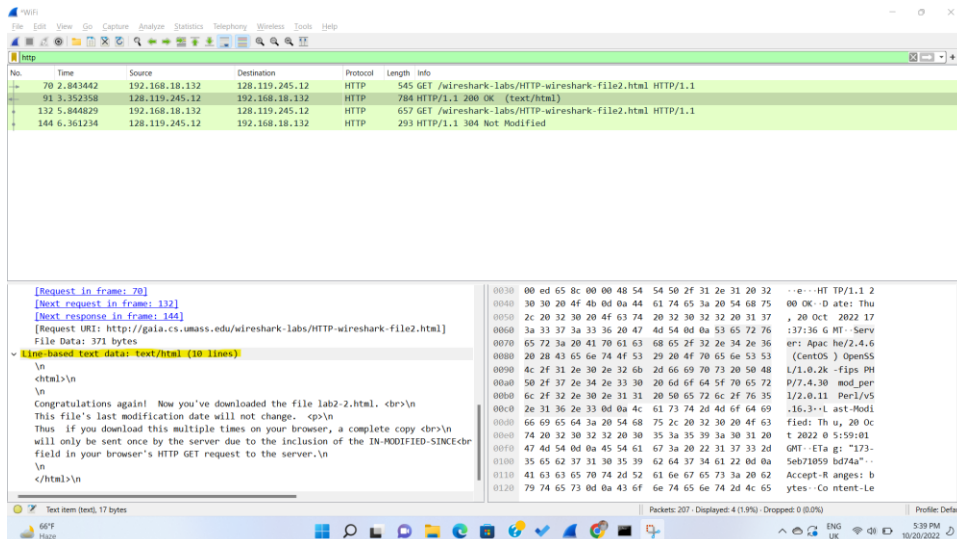
1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Ans: I inspected the first HTTP GET request from the browser but IF-MODIFIED-SINCE is not found. This is due to this because that is our first time, we are fetching the page so IF-MODIFIED-SINCE is not checked.



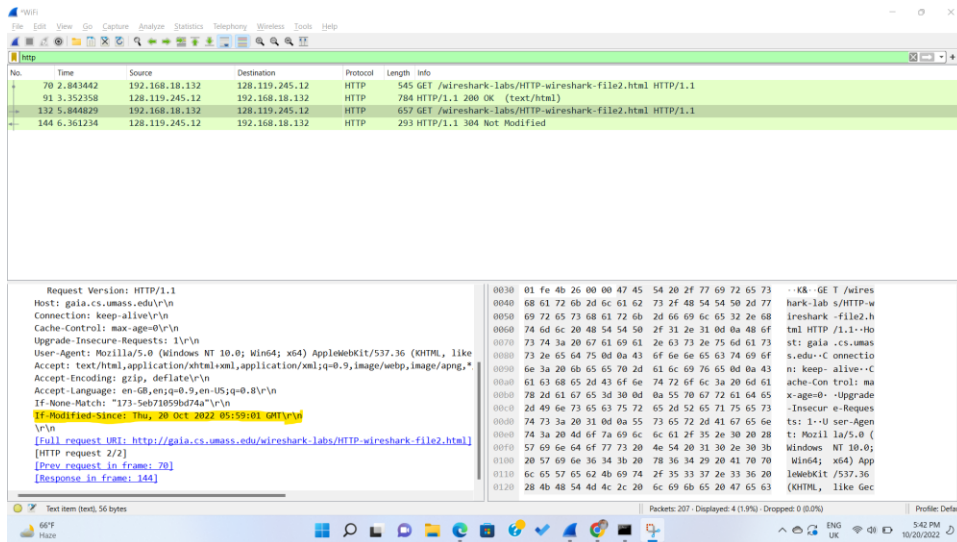
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

I inspected the contents of the server response. Server is explicitly returning the contents of the file in the option **Line-based text data: text/html (10 lines)**.



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?

Ans: I inspected the second HTTP GET request. This time **IF-MODIFIED-SINCE** found. Reason for this is that because we are fetching the page second time page is already present in cache and if page is not modified then it will not fetch complete page from server rather it will pick page from cache and show to the user.



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.

Ans: 304 status code returned from the server in response to this second HTTP Get. No, Server did not explicitly return the contents of the file.

