# 21CY681 - INTERNET PROTOCOL LAB - III

Name: KARTHIKA P Date: 20th October 2022

Assignment Topic: To USE WIRESHARK AND ANALYSE VARIOUS HTTP PACKETS AND PROTOCOL

Register Number: CB. EN. P2CYS22001

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

```
    80 HTTP      479 GET /favicon.ico HTTP/1.1
 56377 HTTP      539 HTTP/1.1 404 Not Found  (text/html)
```

What version of HTTP is the server running?

```
    80 HTTP      479 GET /favicon.ico HTTP/1.1
 56377 HTTP      539 HTTP/1.1 404 Not Found  (text/html)
```

Browser is running on HTTP version 1.1 and the server has version 1.1.

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

It indicates that it can accept en-US.

```
Accept-Language: en-US,en;q=0.9\r\n
<Accept-Language: en-US,en;q=0.9\r\n>
```

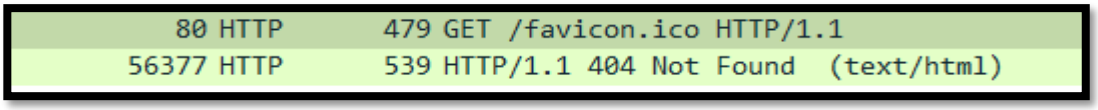
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

My IP address is 192.168.170.120 and the server is 128.119.245.12

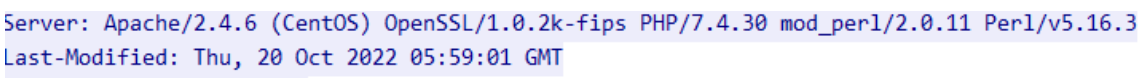
```
192.168.170.120
128.119.245.12
```

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

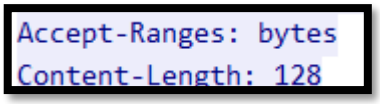
Status code: 404 Not Found




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




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

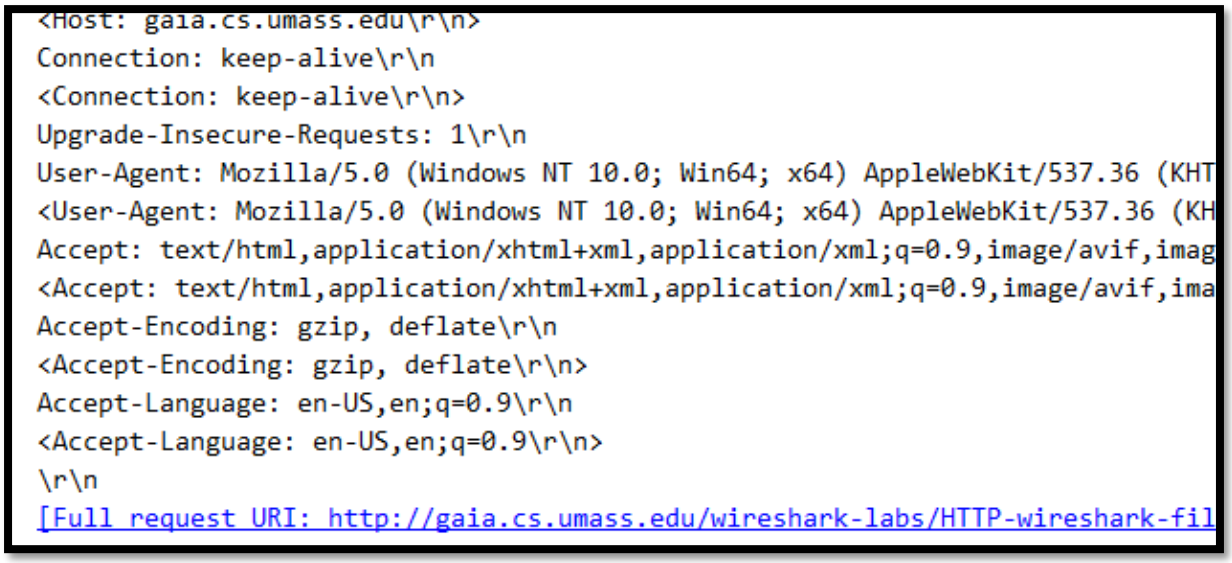



7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, there is no header within data.

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

NO, there is no “ IF MODIFIED –SINCE “ line in the HTTP GET.



9. 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.

```
<html>

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

</html>
```

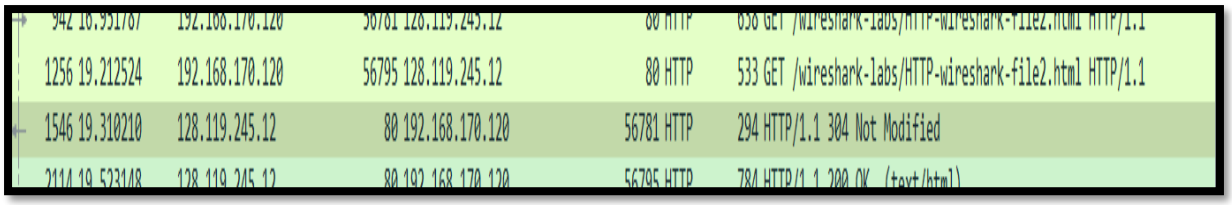
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? What information follows the “IF-MODIFIED SINCE:” header?

Yes, “if modified since” is visible.

```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTI
<User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
<Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
Accept-Encoding: gzip, deflate\r\n
<Accept-Encoding: gzip, deflate\r\n>
Accept-Language: en-US,en;q=0.9\r\n
<Accept-Language: en-US,en;q=0.9\r\n>
If-None-Match: "173-5eb71059bd74a"\r\n
If-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-fil
<Request: True>
```

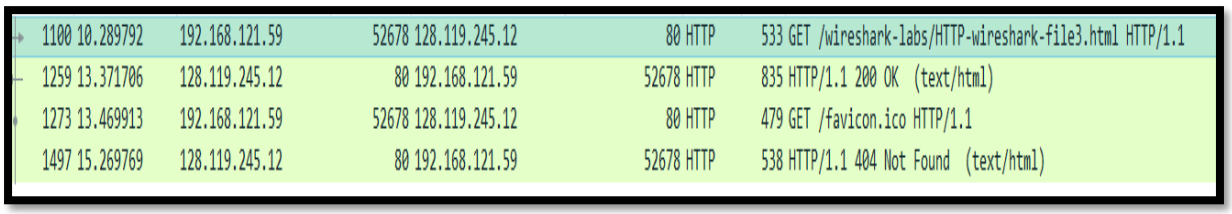
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the file’s contents? Explain.

No, the server did not explicitly return the file contents.



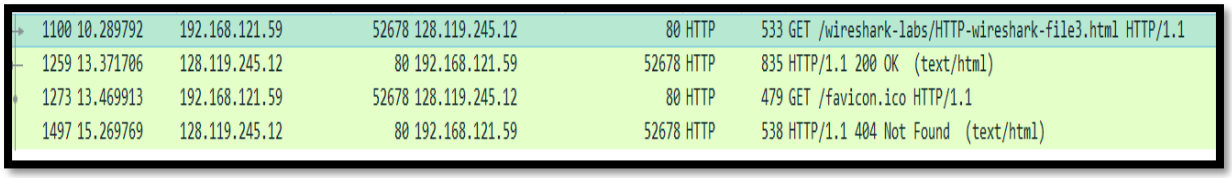

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

We got 2 get request by using this file. The packet number 1100 in the trace contains the GET message for the bill or rights.




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

The packet number 1259 in the trace contains the status code and phrase associated with response to the HTTP GET request.

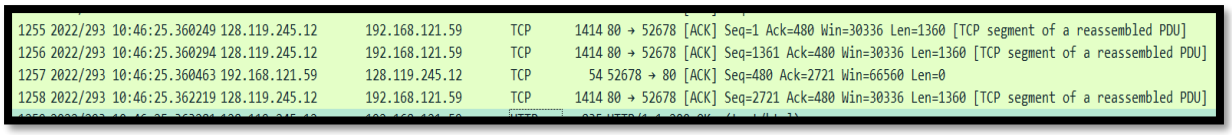



14. What is the status code and phrase in the response?

Status code -200

Phrase -ok

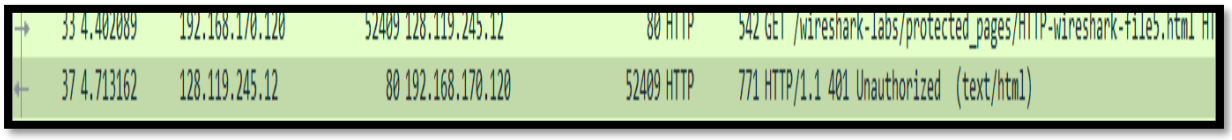
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?




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

STATUS CODE:401

PHRASE: unauthorized




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

Authorization is the new header included in HTTP GET message.

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=
```