Name: Shubhan Singh

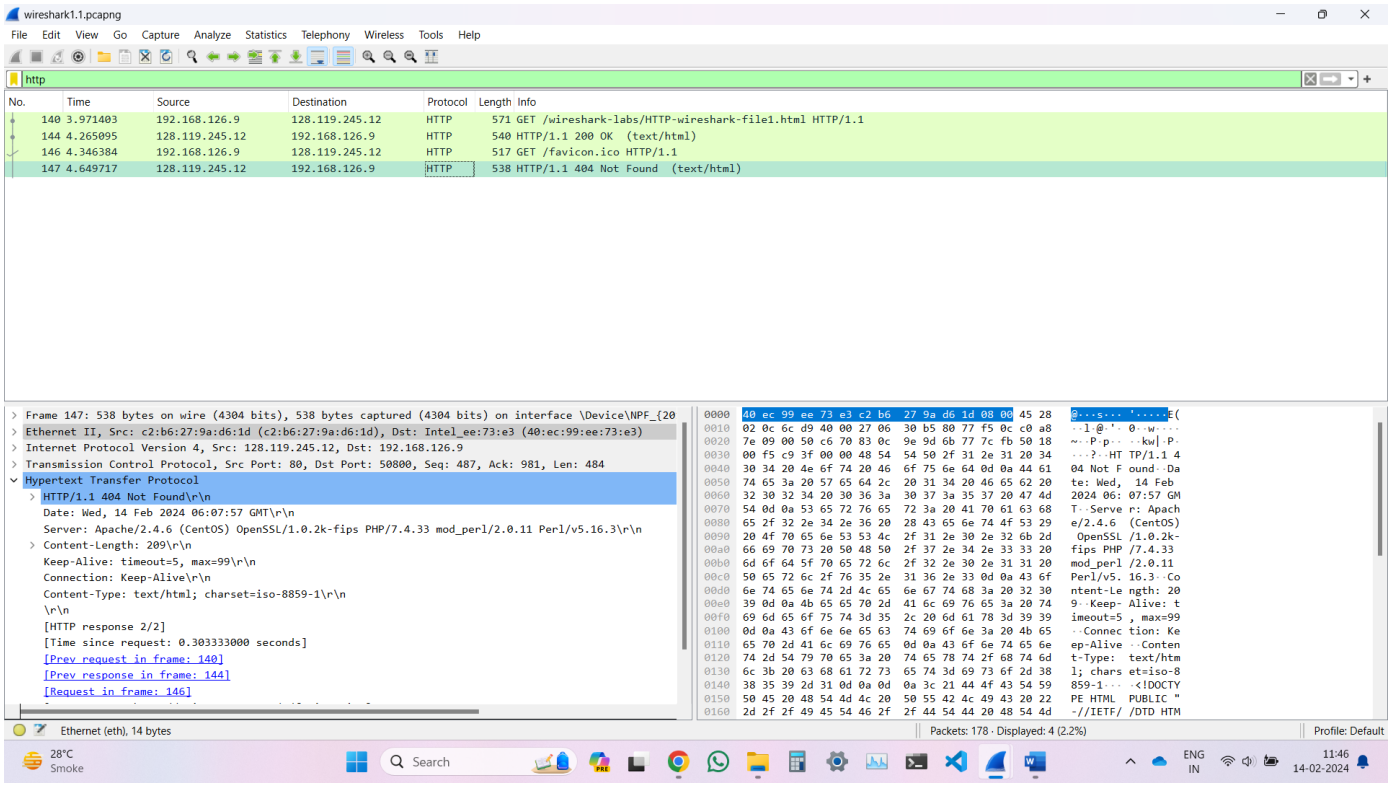
Class: SE Comps B

Roll no.:2022300118

CCN Experiment 4

Wireshark lab: HTTP

Part 1: The Basic HTTP GET/response interaction



1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

    - The browser and server are both running HTTP 1.1 . This is because the browser sends the initial GET message using HTTP 1.1, and the server responds with the same version. The server responds with the highest version of HTTP that it atleast partially supports and which is lower than or equal to the major version that the request was issued in.

2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

Frame 140: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{2018CEF0-D239-4896-B0A1-5D1A2638F381}, id 0

Ethernet II, Src: Intel_ee:73:e3 (40:ec:99:ee:73:e3), Dst: c2:b6:27:9a:d6:1d (c2:b6:27:9a:d6:1d)

Internet Protocol Version 4, Src: 192.168.126.9, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50800, Dst Port: 80, Seq: 1, Ack: 1, Len: 517

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-IN,en;q=0.9,hi-IN;q=0.8,hi;q=0.7,en-GB;q=0.6,en-US;q=0.5\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

[HTTP request 1/2]

[Response in frame: 144]

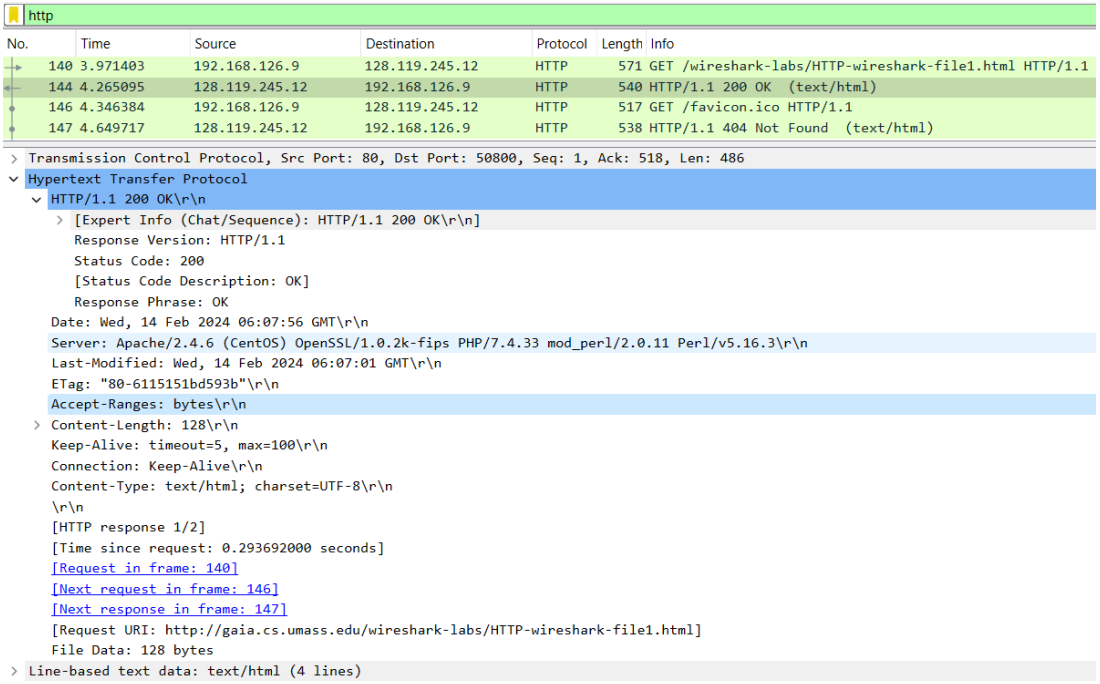
[Next request in frame: 146]

- As can be seen in this GET request, the browser accepts the following languages: en-IN,en;q=0.9,hi-IN;q=0.8,hi;q=0.7,en-GB;q=0.6,en-US;q=0.5
- The browser also relays data about the accepted encoding formats, the accepted data formats like html,xml,etc.

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

- As can be seen in the source and destination columns, the IP address of my computer is 192.168.126.9 and the IP address of the server is 128.119.245.12

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



- The status code returned from the server to my browser was 200 (OK).

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

   - The file was last updated at: Wed, 14 Feb 2024 06:07:56 GMT

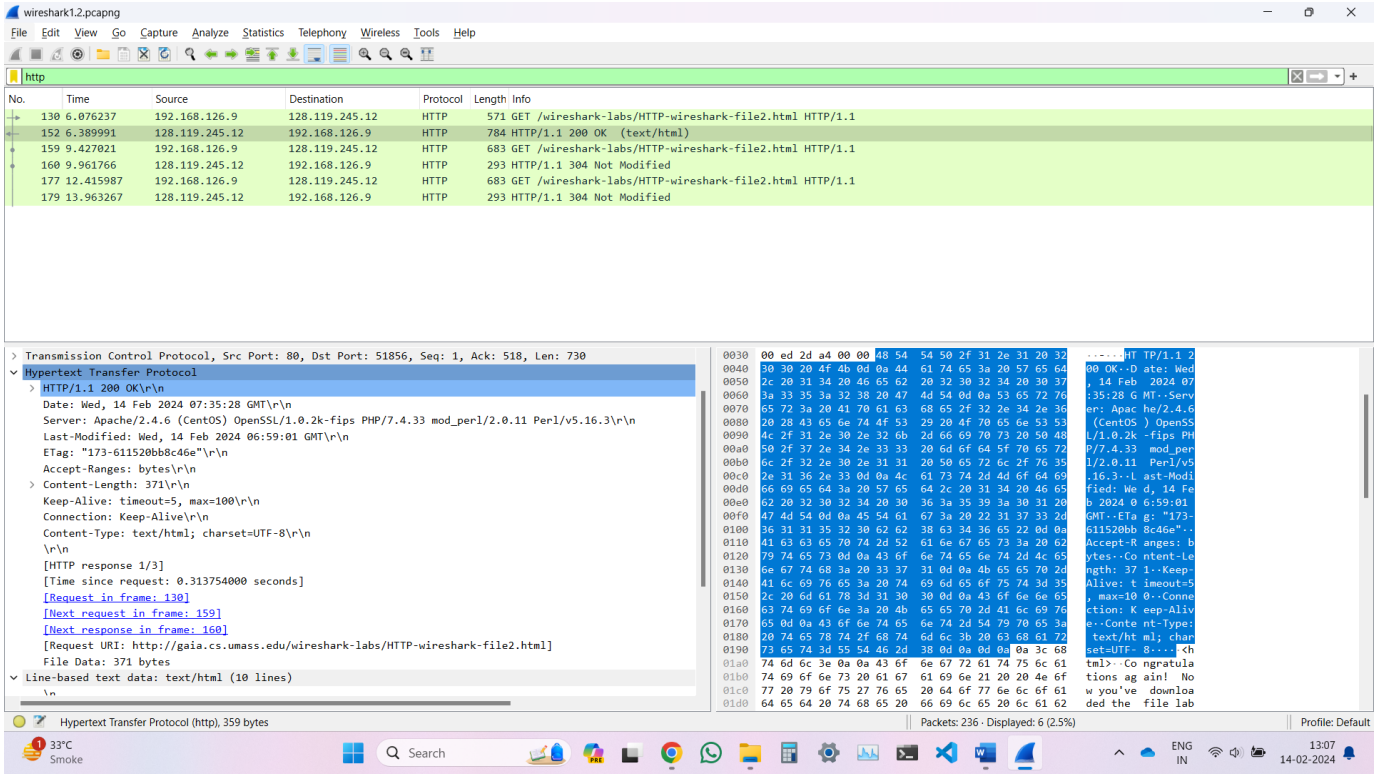
6. How many bytes of content are being returned to your browser?

   - 128 bytes of data

7. By inspecting the raw data in the "packet bytes" pane, do you see any http headers within the data that are not displayed in the "packet details" pane? If so, name one.

   - No such headers were found.

Part-2: The HTTP CONDITIONAL GET/response interaction

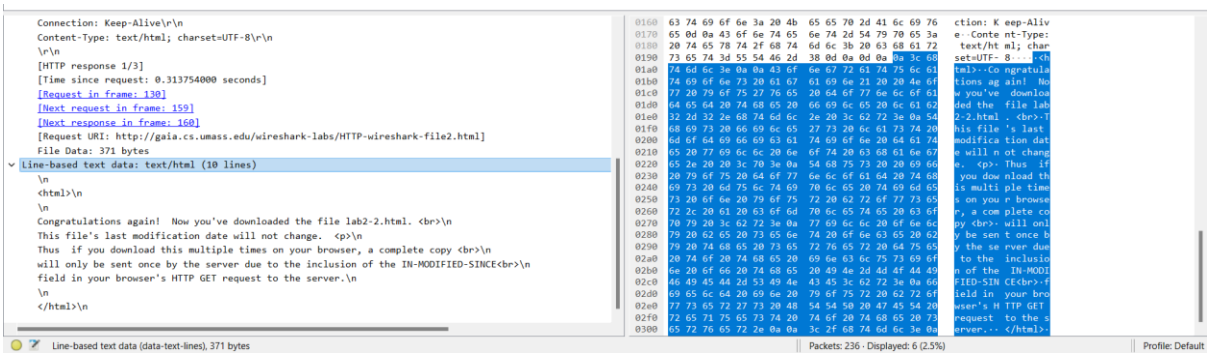


8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

    - No, but it can be seen in the second GET request.

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 returned the contents of the file, this can be seen in both wireshark’s output and the raw data



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? If so, what information follows the “IF-MODIFIED-SINCE:” header?

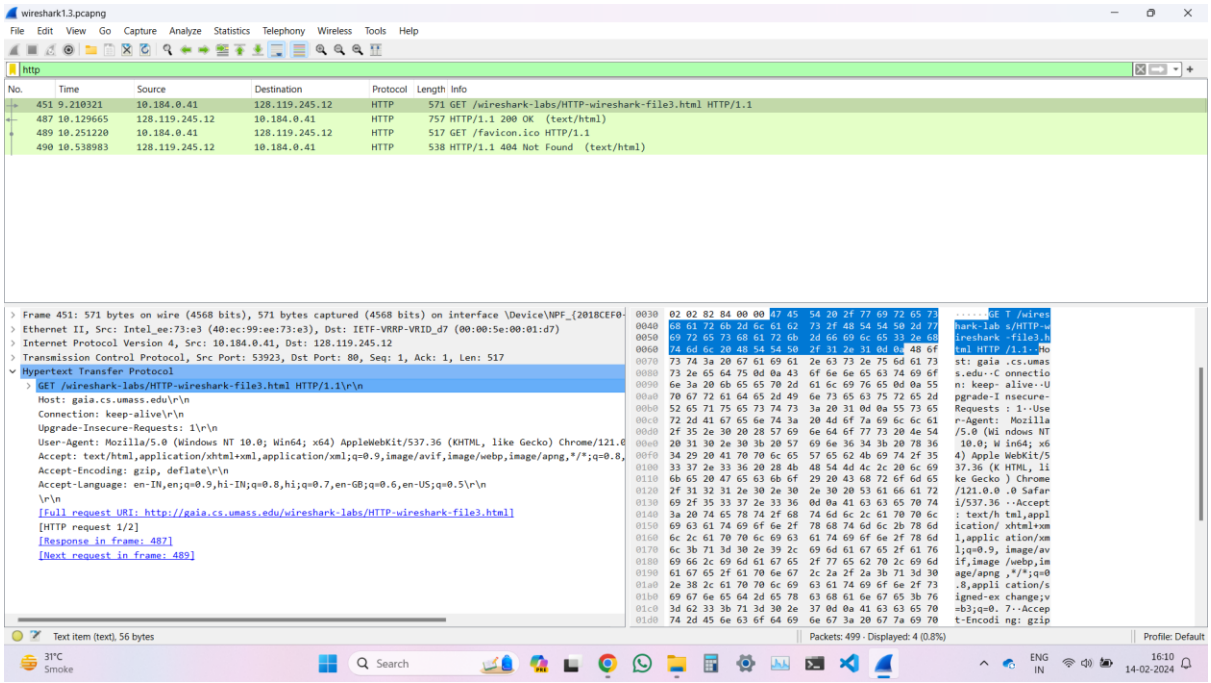
- Yes, an IF-MODIFIED-SINCE: can be seen in the second get request,

```
If-Modified-Since: Wed, 14 Feb 2024 06:59:01 GMT\r\n
```

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

    - For the second request, the server returns code 304, with the description "Not Modified".
    - The second time, the server does not explicitly return the contents of the file.

Part-3: Retrieving Long Documents

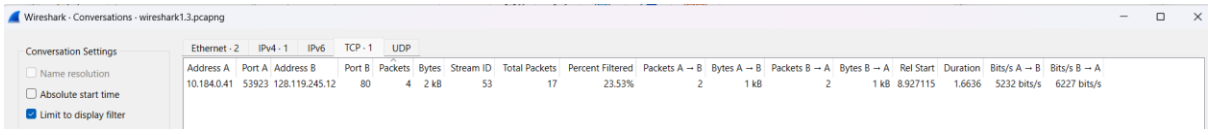


12. How many HTTP GET request messages were sent by your browser?

    - The browser sent only 1 GET request (the other one was for the favicon).

13. How many data-containing TCP segments were needed to carry the single HTTP response?

    - 4 TCP segments were needed.




```
> Transmission Control Protocol, Src Port: 80, Dst Port: 53923, Seq: 4159, Ack: 518, Len: 703
> [3 Reassembled TCP Segments (4861 bytes): #484(1386), #485(2772), #487(703)]
```

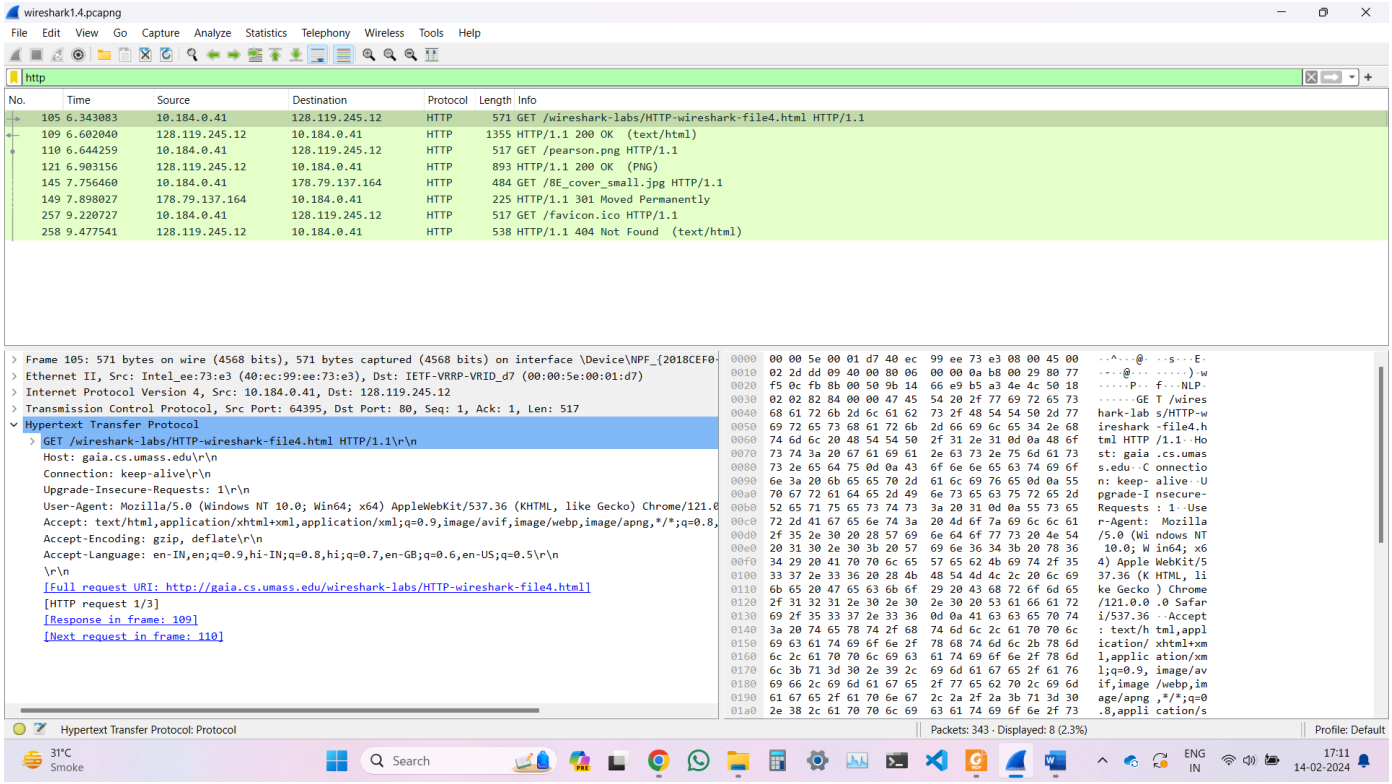
14. What is the status code and phrase associated with the response to the HTTP GET request?

    - The status code associated with the response is 200 and the phrase was “OK”.

15. Is there any HTTP header information in the transmitted data associated with TCP segmentation?

    - No, only the raw data is present in the TCP segments.

4. HTML Documents with Embedded Objects



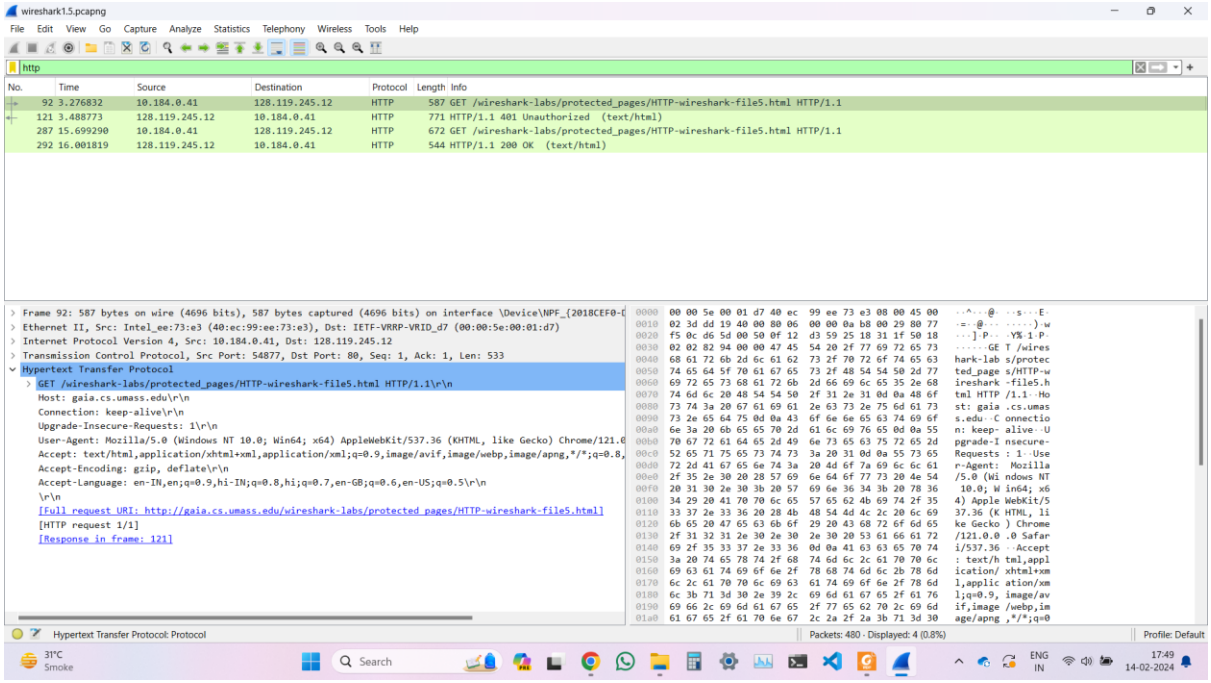
16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

    - 4 GET requests were sent (including the one for the favicon). The GET request for the HTML was sent to the ip address 128.119.245.12, the request for the pearson.png image file was also sent to this server. The request for the 8E_cover_small.jpg was sent to 178.79.137.164. The request for the favicon was also sent to 128.119.245.12.

17. 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 images were downloaded serially, this can be seen as the packet numbers are not close (they are 35 apart) and the timestamps are also not close.

5. HTTP Authentication



18. 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 to the initial GET request from the browser is 401 and the phrase is "Unauthorised".

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

    - When the browser sends the second GET request, a new field Authorisation is included.

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
```