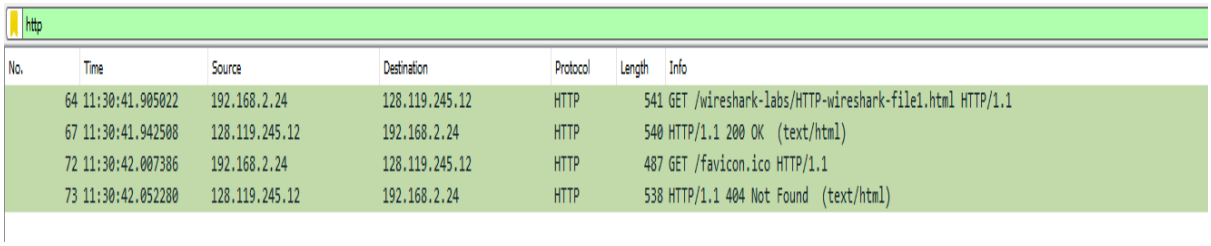
Wireshark lab 2

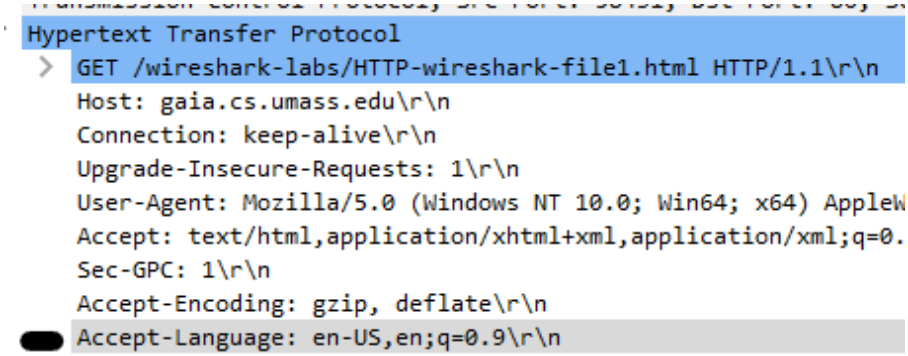
Name: Nirmith Victor D'Almeida
Student Number : 101160124

1. The Basic HTTP GET/response interaction

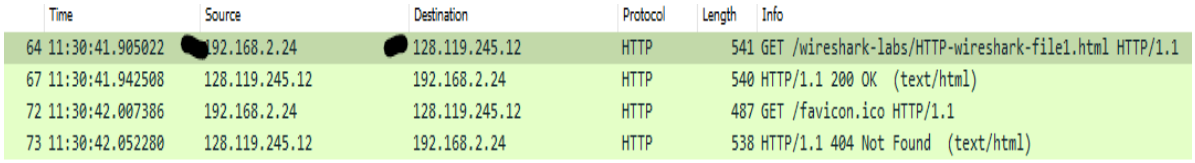
1. My browser is running http version 1.1



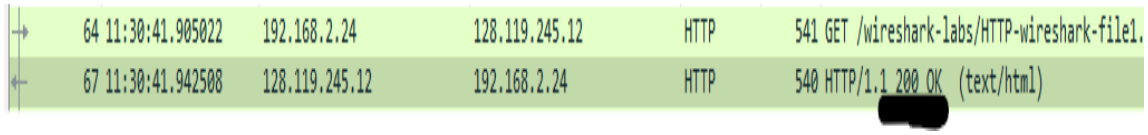
2. Browser indicates that it will accept English language



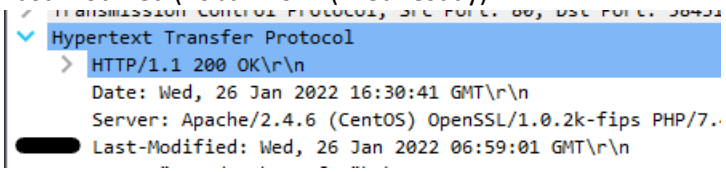
3. IP Address of my computer is 192.168.2.24
   IP address of destination is 128.119.245.12



4. Status Code is 200 OK



5. Last Modified (26 Jan 2022 (Wednesday)



6. Content length is 128 bytes

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
    [Content length: 128]
```

7. I do not see any difference between the packet window and packet listing window.

2. The HTTP CONDITIONAL GET/response interaction

8. No I do not see any If-Modified-Since line in the GET message
9. The server did return the contents of a file. We can view it in the line-based text data.

```
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
```

10. Yes we can view the If Modified since statement

```
Transmission Control Protocol, Src Port: 63451, Dst Port: 80, Seq: 1, Ack:
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.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
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  Sec-GPC: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "173-5d676bc93581c"\r\n
  If-Modified-Since: Wed, 26 Jan 2022 06:59:01 GMT\r\n
```

11.

a. The HTTP status code is 304 NOT MODIFIED
b. It didn't return the Line-Based Text data. Since we refreshed the page it simply returned data from it's cache and. If the file was modified then the Line-Based Text Data would be visible.

3. Retrieving Long Documents

12. Only one GET HTTP request to the browser and the packet number is 21

No.	Time	Source	Destination	Protocol	Length	Info
21	18:49:51.252389	192.168.2.24	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
28	18:49:51.294298	128.119.245.12	192.168.2.24	HTTP	559	HTTP/1.1 200 OK (text/html)

13. Packet number 28

No.	Time	Source	Destination	Protocol	Length	Info
21	18:49:51.252389	192.168.2.24	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
28	18:49:51.294298	128.119.245.12	192.168.2.24	HTTP	559	HTTP/1.1 200 OK (text/html)

14. The status code is 200 OK as can be seen in the above packet snippet.
15. 4 TCP segments and then reassembled.

```
Checksum: 0x8da2 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (505 bytes)
TCP segment data (505 bytes)
> [4 Reassembled TCP Segments (4861 bytes): #24(1452), #25(1452), #26(1452), #28(505)]
```

4. HTML Documents with embedded objects

16. My browser sent 3 http get requests.
    Three internet addresses
    1. Initial (128.110.245.12)
    2. The pearson.png (128.119.245.12)
    3. The 8E_cover_small.jpg (178.79.137.164)

	Time	Source	Destination	Protocol	Length	Info
11	19:52:27.479223	192.168.2.24	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wiresh…
13	19:52:27.523009	128.119.245.12	192.168.2.24	HTTP	1355	HTTP/1.1 200 OK (text/html)
17	19:52:27.554423	192.168.2.24	128.119.245.12	HTTP	487	GET /pearson.png HTTP/1.1
21	19:52:27.594912	128.119.245.12	192.168.2.24	HTTP	761	HTTP/1.1 200 OK (PNG)
33	19:52:27.773853	192.168.2.24	178.79.137.164	HTTP	454	GET /8E_cover_small.jpg HTTP/1..
35	19:52:27.872264	178.79.137.164	192.168.2.24	HTTP	225	HTTP/1.1 301 Moved Permanently

17. In my opinion, I think the images where downloaded serially since the second image was requested only after the first image was downloaded

	Time	Source	Destination	Protocol	Length	Info
11	19:52:27.479223	192.168.2.24	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wiresh…
13	19:52:27.523009	128.119.245.12	192.168.2.24	HTTP	1355	HTTP/1.1 200 OK (text/html)
[redacted]	19:52:27.554423	192.168.2.24	128.119.245.12	HTTP	487	GET /pearson.png HTTP/1.1
21	19:52:27.594912	128.119.245.12	192.168.2.24	HTTP	761	HTTP/1.1 200 OK (PNG)
[redacted]	19:52:27.773853	192.168.2.24	178.79.137.164	HTTP	454	GET /8E_cover_small.jpg HTTP/1..
35	19:52:27.872264	178.79.137.164	192.168.2.24	HTTP	225	HTTP/1.1 301 Moved Permanently

5. HTTP Authentication

18. The initial Get request returned a 401 Unauthorized

14	20:04:25.530012	192.168.2.24	128.119.245.12	HTTP	557 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
16	20:04:25.571790	128.119.245.12	192.168.2.24	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
170	20:04:52.353510	192.168.2.24	128.119.245.12	HTTP	642 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
172	20:04:52.394165	128.119.245.12	192.168.2.24	HTTP	544 HTTP/1.1 200 OK (text/html)

19. Authorization field is added into the HTTP GET request message

```
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
> Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
```