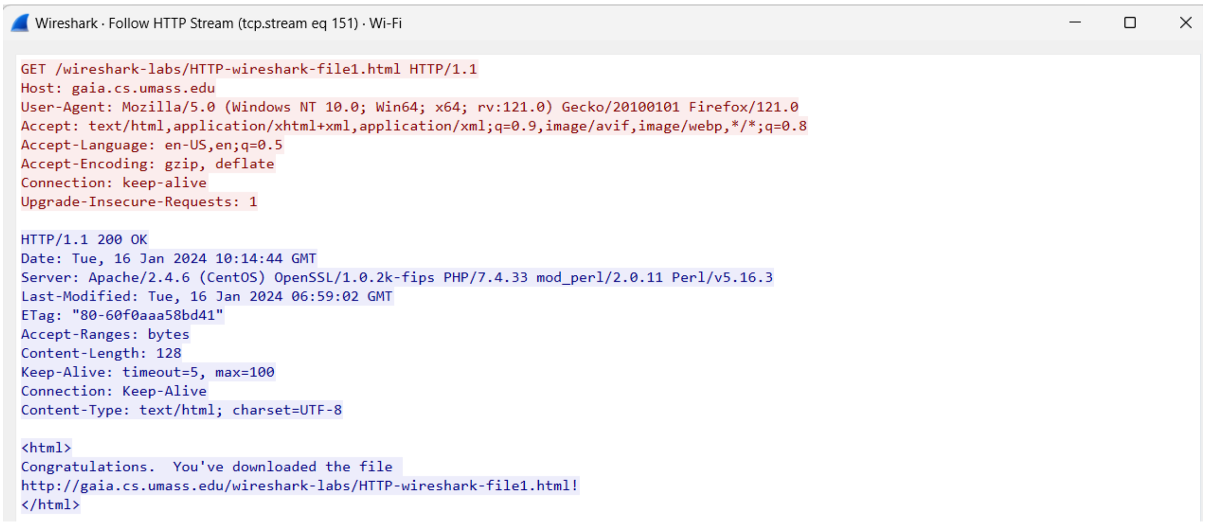
Assignment 3: HTTP

Name: Hrishikesh Ravindra karande

Roll no: 210010020

Part1:

1. Browser is running HTTP version 1.1 and server is also running on version 1.1.
2. Language Accepted en-US,en.
3. IP Address of Computer: 10.196.106.44
   IP Address of server   : 128.119.245.12
4. Status code returned from server to browser is 200.
5. Last Modified: Tue, 16 Jan 2024 06:59:02 GMT
6. The entire packet length is = 540 but the content length = Content-Length: 128.
7. No, all the headers can be found in raw data.



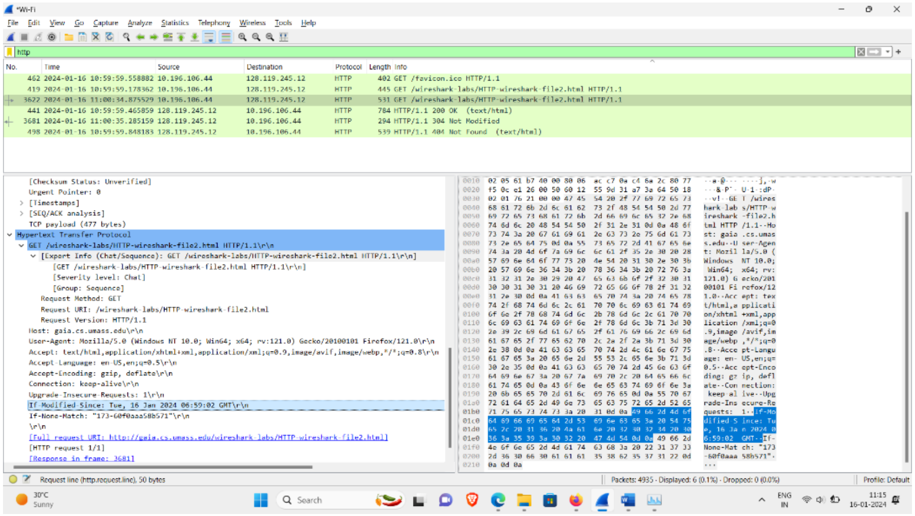
```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Tue, 16 Jan 2024 10:14:44 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Tue, 16 Jan 2024 06:59:02 GMT
ETag: "80-60f0aaa58bd41"
Accept-Ranges: bytes
Content-Length: 128
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations.  You've downloaded the file 
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!
</html>
```

Part 2

1. Yes **IF-MODIFIED-SINCE** field can be seen.



```
No.   Time                        Source           Destination      Protocol Length Info
  462 2024-01-16 10:59:59.558882 10.196.106.44    128.119.245.12   HTTP     402 GET /favicon.ico HTTP/1.1
  419 2024-01-16 10:59:59.178362 10.196.106.44    128.119.245.12   HTTP     445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 3622 2024-01-16 11:00:34.875529 10.196.106.44    128.119.245.12   HTTP     531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  441 2024-01-16 10:59:59.465859 128.119.245.12   10.196.106.44    HTTP     784 HTTP/1.1 200 OK  (text/html)
 3681 2024-01-16 11:00:35.285159 128.119.245.12   10.196.106.44    HTTP     294 HTTP/1.1 304 Not Modified
  498 2024-01-16 10:59:59.848183 128.119.245.12   10.196.106.44    HTTP     539 HTTP/1.1 404 Not Found  (text/html)
```

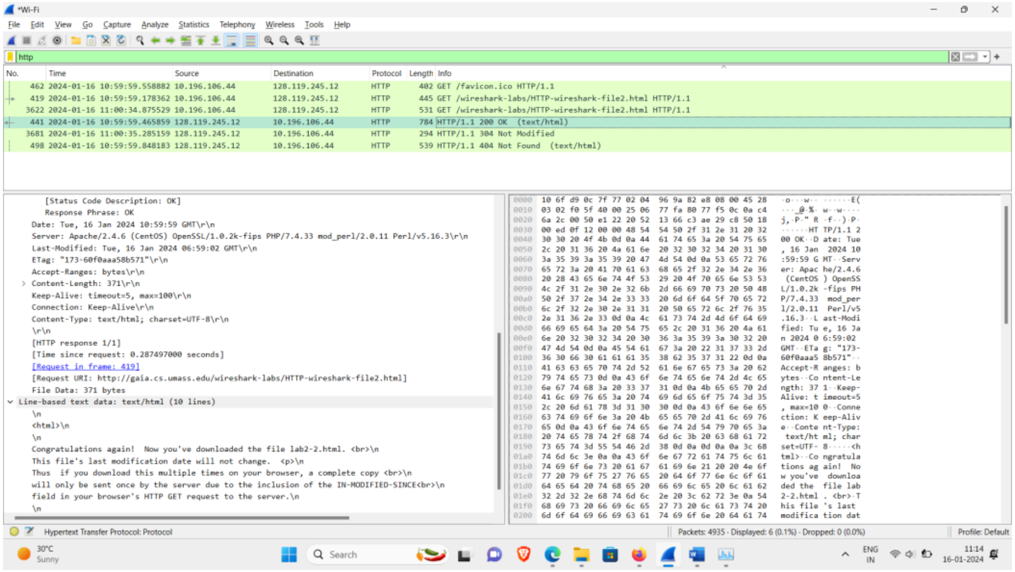
```
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (477 bytes)
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Tue, 16 Jan 2024 06:59:02 GMT\r\n
    If-None-Match: "173-60f0aaa58b571"\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 3681]
```

Request line (http.request.line), 50 bytes

Packets: 4935 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

2. Yes, the server explicitly returns the contents of the file.



```
No.   Time                        Source           Destination      Protocol Length Info
  462 2024-01-16 10:59:59.558882 10.196.106.44    128.119.245.12   HTTP     402 GET /favicon.ico HTTP/1.1
  419 2024-01-16 10:59:59.178362 10.196.106.44    128.119.245.12   HTTP     445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 3622 2024-01-16 11:00:34.875529 10.196.106.44    128.119.245.12   HTTP     531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  441 2024-01-16 10:59:59.465859 128.119.245.12   10.196.106.44    HTTP     784 HTTP/1.1 200 OK  (text/html)
 3681 2024-01-16 11:00:35.285159 128.119.245.12   10.196.106.44    HTTP     294 HTTP/1.1 304 Not Modified
  498 2024-01-16 10:59:59.848183 128.119.245.12   10.196.106.44    HTTP     539 HTTP/1.1 404 Not Found  (text/html)
```

```
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 16 Jan 2024 10:59:59 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 16 Jan 2024 06:59:02 GMT\r\n
    ETag: "173-60f0aaa58b571"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.287497000 seconds]
    [Request in frame: 419]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
v 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
```

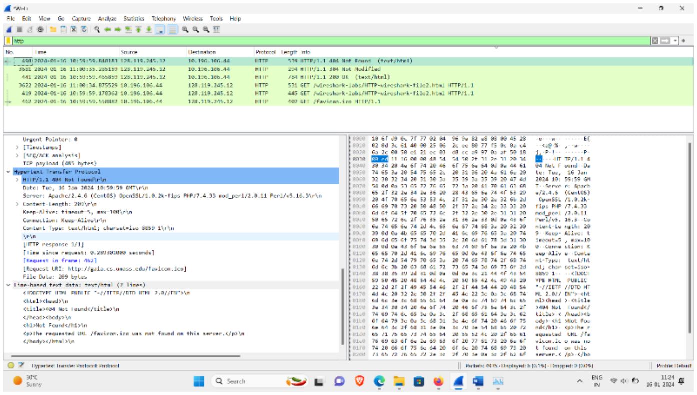
Hypertext Transfer Protocol: Protocol

Packets: 4935 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

3. Yes we get a **IF-MODIFIED-SINCE** after accessing it for second time**.** This is header field which represents whether the source is modified by the server after the last time it was accessed by our machine. Since we are accessing the same resource twice (by refreshing) and in that interval there was no change in the the website the IF-MODIFIED-SINCE header is not displayed.
4. The status code returned was 304 by the server and this time the content was not explicitly returned. The **HTTP status code 304** means **Not Modified** – the web page you requested hasn't changed since the last time you accessed it**.**

   The file has not been modified! So the text of the file is NOT returned in the HTTP message.



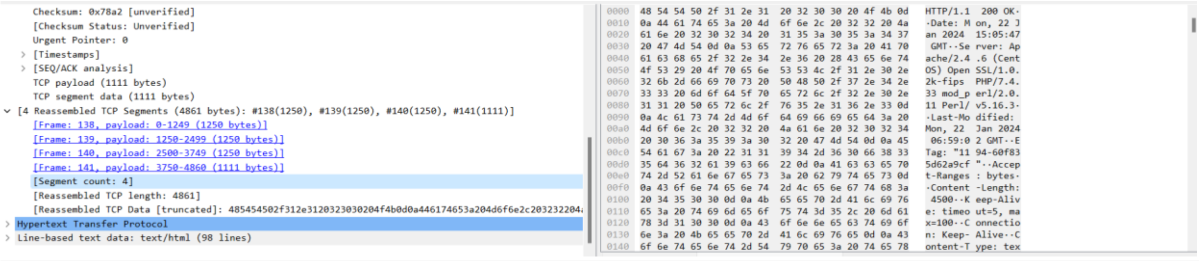
```
No.   Time                        Source           Destination      Protocol Length Info
  490 2024-01-16 10:59:59.840183 128.119.245.12   10.196.106.44    HTTP     519 HTTP/1.1 404 Not Found  (text/html)
 3581 2024-01-16 11:00:35.285159 128.119.245.12   10.196.106.44    HTTP     294 HTTP/1.1 304 Not Modified
  441 2024-01-16 10:59:59.465859 128.119.245.12   10.196.106.44    HTTP     784 HTTP/1.1 200 OK  (text/html)
 3622 2024-01-16 11:00:34.875529 10.196.106.44    128.119.245.12   HTTP     531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  419 2024-01-16 10:59:59.178362 10.196.106.44    128.119.245.12   HTTP     445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  462 2024-01-16 10:59:59.558882 10.196.106.44    128.119.245.12   HTTP     402 GET /favicon.ico HTTP/1.1
```

```
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (465 bytes)
v Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Tue, 16 Jan 2024 10:59:59 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  > Content-Length: 209\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.281301000 seconds]
    [Request in frame: 462]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 209 bytes
v Line-based text data: text/html (7 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>404 Not Found</title>\n
    </head><body>\n
    <h1>Not Found</h1>\n
    <p>The requested URL /favicon.ico was not found on this server.</p>\n
    </body></html>\n
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol Protocol
30°C
Sunny
Search

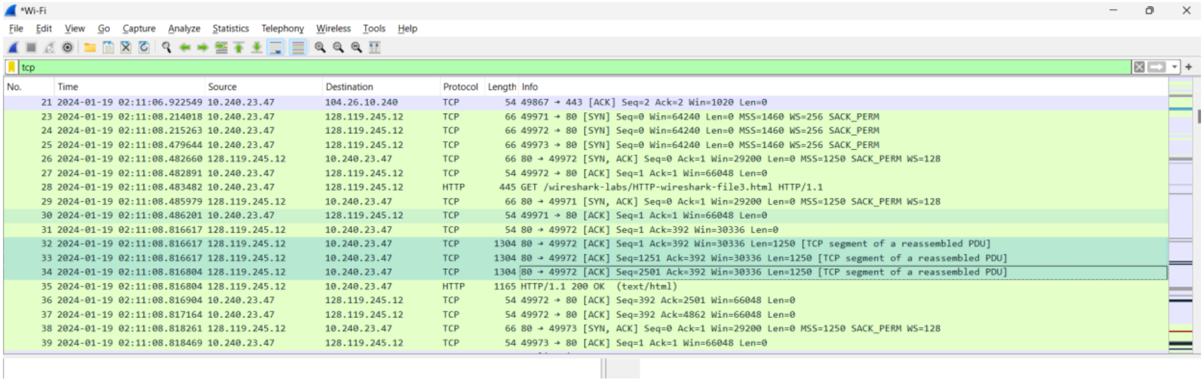
Part 3:

1. There is 1 GET Message in the packet listing window. Packet No. with the GET request 214.
2. Response code is 200 and Packet No. is 217.
3. In Response Status code is 200 and phrase is OK.
4. Total 4 TCP segments were required to carry the HTTPS request. The segment count is displayed here.



```
    Checksum: 0x78a2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (1111 bytes)
    TCP segment data (1111 bytes)
v [4 Reassembled TCP Segments (4861 bytes): #138(1250), #139(1250), #140(1250), #141(1111)]
    [Frame: 138, payload: 0-1249 (1250 bytes)]
    [Frame: 139, payload: 1250-2499 (1250 bytes)]
    [Frame: 140, payload: 2500-3749 (1250 bytes)]
    [Frame: 141, payload: 3750-4860 (1111 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203232204
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 32 32 20 4a   ·Date: M on, 22 J
0020  61 6e 20 32 30 32 34 20  31 35 3a 30 35 3a 34 37   an 2024  15:05:47
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified: 
00a0  4d 6f 6e 2c 20 32 32 20  4a 61 6e 20 32 30 32 34   Mon, 22  Jan 2024
00b0  20 30 36 3a 35 39 3a 30  32 20 47 4d 54 0d 0a 45    06:59:0 2 GMT··E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 36 30 66 38 33   Tag: "11 94-60f83
00d0  35 64 36 32 61 39 63 66  22 0d 0a 41 63 63 65 70   5d62a9cf "··Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
00f0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0100  20 34 35 30 30 0d 0a 4b  65 65 70 2d 41 6c 69 76    4500··K eep-Aliv
0110  65 3a 20 74 69 6d 65 6f  75 74 3d 35 2c 20 6d 61   e: timeo ut=5, ma
0120  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=100··C onnectio
0130  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive··C
0140  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
```



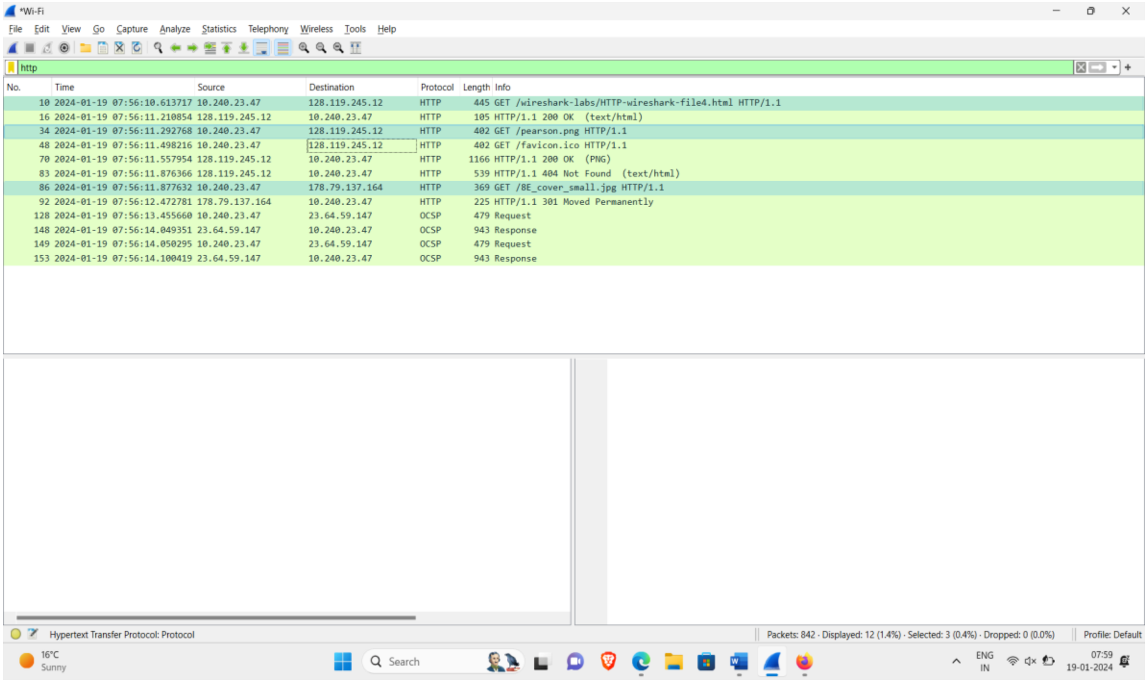
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time                        Source           Destination      Protocol Length Info
  21 2024-01-19 02:11:06.922549 10.240.23.47     104.26.10.240    TCP        54 49867 → 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0
  23 2024-01-19 02:11:08.214018 10.240.23.47     128.119.245.12   TCP        66 49971 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  24 2024-01-19 02:11:08.215263 10.240.23.47     128.119.245.12   TCP        66 49972 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  25 2024-01-19 02:11:08.479644 10.240.23.47     128.119.245.12   TCP        66 49973 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  26 2024-01-19 02:11:08.482660 128.119.245.12   10.240.23.47     TCP        66 80 → 49972 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
  27 2024-01-19 02:11:08.482891 10.240.23.47     128.119.245.12   TCP        54 49972 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
  28 2024-01-19 02:11:08.483482 10.240.23.47     128.119.245.12   HTTP      445 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  29 2024-01-19 02:11:08.485979 128.119.245.12   10.240.23.47     TCP        66 80 → 49971 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
  30 2024-01-19 02:11:08.486201 10.240.23.47     128.119.245.12   TCP        54 49971 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
  31 2024-01-19 02:11:08.816617 128.119.245.12   10.240.23.47     TCP        54 80 → 49972 [ACK] Seq=1 Ack=392 Win=30336 Len=0
  32 2024-01-19 02:11:08.816617 128.119.245.12   10.240.23.47     TCP      1304 80 → 49972 [ACK] Seq=1 Ack=392 Win=30336 Len=1250 [TCP segment of a reassembled PDU]
  33 2024-01-19 02:11:08.816617 128.119.245.12   10.240.23.47     TCP      1304 80 → 49972 [ACK] Seq=1251 Ack=392 Win=30336 Len=1250 [TCP segment of a reassembled PDU]
  34 2024-01-19 02:11:08.816804 128.119.245.12   10.240.23.47     TCP      1304 80 → 49972 [ACK] Seq=2501 Ack=392 Win=30336 Len=1250 [TCP segment of a reassembled PDU]
  35 2024-01-19 02:11:08.816804 128.119.245.12   10.240.23.47     HTTP     1165 HTTP/1.1 200 OK  (text/html)
  36 2024-01-19 02:11:08.816904 10.240.23.47     128.119.245.12   TCP        54 49972 → 80 [ACK] Seq=392 Ack=2501 Win=66048 Len=0
  37 2024-01-19 02:11:08.817164 10.240.23.47     128.119.245.12   TCP        54 49972 → 80 [ACK] Seq=392 Ack=4862 Win=66048 Len=0
  38 2024-01-19 02:11:08.818261 128.119.245.12   10.240.23.47     TCP        66 80 → 49973 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
  39 2024-01-19 02:11:08.818469 10.240.23.47     128.119.245.12   TCP        54 49973 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
```

Part4:

1. There were 3 HTTP Get messages sent two at the same IP address and 1 at different by packet numbered 10,34,86 respectively. Packet 10,34 was sent at Destination IP of 128.119.245.12(Address of Page & pearson.png) whereas packet 86 was sent at

178.79.137.164(8E_cover_small.png).



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	2024-01-19 07:56:10.613717	10.240.23.47	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
16	2024-01-19 07:56:11.210854	128.119.245.12	10.240.23.47	HTTP	105	HTTP/1.1 200 OK (text/html)
34	2024-01-19 07:56:11.292768	10.240.23.47	128.119.245.12	HTTP	402	GET /pearson.png HTTP/1.1
48	2024-01-19 07:56:11.498216	10.240.23.47	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
70	2024-01-19 07:56:11.557954	128.119.245.12	10.240.23.47	HTTP	1166	HTTP/1.1 200 OK (PNG)
83	2024-01-19 07:56:11.876366	128.119.245.12	10.240.23.47	HTTP	539	HTTP/1.1 404 Not Found (text/html)
86	2024-01-19 07:56:11.877632	10.240.23.47	178.79.137.164	HTTP	369	GET /8E_cover_small.jpg HTTP/1.1
92	2024-01-19 07:56:12.472781	178.79.137.164	10.240.23.47	HTTP	225	HTTP/1.1 301 Moved Permanently
128	2024-01-19 07:56:13.455660	10.240.23.47	23.64.59.147	OCSP	479	Request
148	2024-01-19 07:56:14.049351	23.64.59.147	10.240.23.47	OCSP	943	Response
149	2024-01-19 07:56:14.050295	10.240.23.47	23.64.59.147	OCSP	479	Request
153	2024-01-19 07:56:14.100419	23.64.59.147	10.240.23.47	OCSP	943	Response

Hypertext Transfer Protocol: Protocol

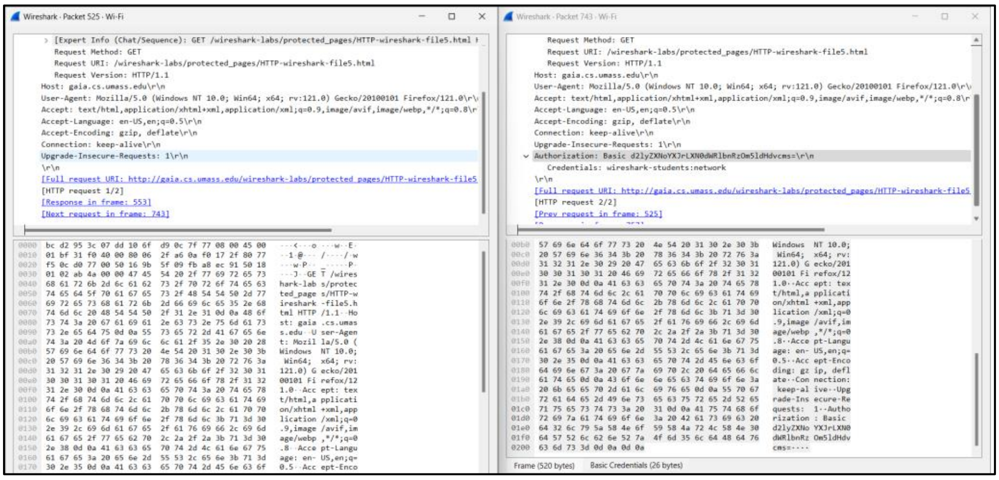
Packets: 842 · Displayed: 12 (1.4%) · Selected: 3 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

2. The two images were serially downloaded this can be seen from the screenshot attached above where unless the first one returned an OK the request for the next image was not sent. We can cross verify this by the time stamps also.

Part 5:

1. There are two http get messages one at 488 and other at 1517. The first (488) is entered without authorization whereas the second is after entering the given username and passwords. The response code for first request is in packet 518 with status code 401 and phrase as Unauthorized.
2. When two packets were compared there was an authorization field in the second packet to which we had entered the username and password, whereas it wasn’t present for the first one. This can be seen in the screenshot attached below the right side is second packet and left side is of first packet.



```
> [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html H
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
    Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0\r\
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5
[HTTP request 1/2]
[Response in frame: 553]
[Next request in frame: 743]
```

```
0000  bc d2 95 3c 07 dd 10 6f  d9 0c 7f 77 08 00 45 00   ···<···o ···w··E·
0010  01 bf 31 f0 40 00 80 06  2f a6 0a f0 17 2f 80 77   ··1·@··· /····/·w
0020  f5 0c d0 77 00 50 16 9b  5f 09 fb a8 ec 91 50 18   ···w·P·· _·····P·
0030  01 02 ab 4a 00 00 47 45  54 20 2f 77 69 72 65 73   ···J··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 35 2e 68   ireshark -file5.h
0070  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0080  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0090  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
00a0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00b0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00c0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
00d0  31 32 31 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   121.0) G ecko/201
00e0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 32   00101 Fi refox/12
00f0  31 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   1.0··Acc ept: tex
0100  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
0110  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
0120  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
0130  2e 39 2c 69 6d 61 67 65  2f 61 76 69 66 2c 69 6d   .9,image /avif,im
0140  61 67 65 2f 77 65 62 70  2c 2a 2f 2a 3b 71 3d 30   age/webp ,*/*;q=0
0150  2e 38 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   .8··Acce pt-Langu
0160  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
0170  30 2e 35 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.5··Acc ept-Enco
```

```
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
    Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0\r\
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5
[HTTP request 2/2]
[Prev request in frame: 525]
```

```
00b0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00c0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
00d0  31 32 31 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   121.0) G ecko/201
00e0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 32   00101 Fi refox/12
00f0  31 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   1.0··Acc ept: tex
0100  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
0110  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
0120  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
0130  2e 39 2c 69 6d 61 67 65  2f 61 76 69 66 2c 69 6d   .9,image /avif,im
0140  61 67 65 2f 77 65 62 70  2c 2a 2f 2a 3b 71 3d 30   age/webp ,*/*;q=0
0150  2e 38 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   .8··Acce pt-Langu
0160  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
0170  30 2e 35 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.5··Acc ept-Enco
0180  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
0190  61 74 65 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   ate··Con nection:
01a0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 55 70 67    keep-al ive··Upg
01b0  72 61 64 65 2d 49 6e 73  65 63 75 72 65 2d 52 65   rade-Ins ecure-Re
01c0  71 75 65 73 74 73 3a 20  31 0d 0a 41 75 74 68 6f   quests:  1··Autho
01d0  72 69 7a 61 74 69 6f 6e  3a 20 42 61 73 69 63 20   rization : Basic 
01e0  64 32 6c 79 5a 58 4e 6f  59 58 4a 72 4c 58 4e 30   d2lyZXNo YXJrLXN0
01f0  64 57 52 6c 62 6e 52 7a  4f 6d 35 6c 64 48 64 76   dWRlbnRz Om5ldHdv
0200  63 6d 73 3d 0d 0a 0d 0a                            cms=····
```