

## CS-315: COMPUTER NETWORKS LAB ASSIGNMENT 3

### PART-1:

1. My browser is running http version 1.1 and the server is also running http version 1.1 =>

```

▶ Frame 62: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interf
▶ Ethernet II, Src: IntelCor_1f:79:8a (20:c1:9b:1f:79:8a), Dst: Cisco_0a:9a:e1 (44:
▶ Internet Protocol Version 4, Src: 10.240.16.46, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 57120, Dst Port: 80, Seq: 1, Ack: 1, Len
- Hypertext Transfer Protocol
  - GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) Gecko/20100101 F
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
      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
▶ Frame 66: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interf
▶ Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: IntelCor_1f:79:8a (20:
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.240.16.46
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 57120, Seq: 1, Ack: 390, L
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Mon, 22 Jan 2024 12:34:39 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Pe
      Last-Modified: Mon, 22 Jan 2024 06:59:02 GMT\r\n
      ETag: "80-60f835d62e850"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 128\r\n
      Keep-Alive: timeout=5, max=100\r\n

```

2. Accepted-Languages: en-US, en  
Accept: text/html,application/xhtml+xml  
Accept-Language: en-US,en;q=0.5\r\n

3. My computer IP address: 10.240.16.46  
IP address of gaia.cs.umass.edu server: 128.119.245.12

Source	Destination
10.240.16.46	128.119.245.12
128.119.245.12	10.240.16.46

4. Status code: 200

```

HTTP/1.1 200 OK\r\n
▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK

```

5. The HTML file that I was retrieving was last modified on Mon, 22 Jan 2024 06:59:02 GMT.

```
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
Last-Modified: Mon, 22 Jan 2024 06:59:02 GMT\r\n
ETag: "80-60f835d62e850"\r\n
```

6. Size/Bytes of content = 128 bytes[can be seen below in the screenshot as content length]

```
[Status Code Description: OK]
Response Phrase: OK
Date: Mon, 22 Jan 2024 12:34:39 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Pe
Last-Modified: Mon, 22 Jan 2024 06:59:02 GMT\r\n
ETag: "80-60f835d62e850"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\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: 0.250192856 seconds]
[Request in frame: 62]
Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.htm
File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

7. No, all the headers are displayed in the packet listing window since here we can see all the content that we see on the web page of the given URL.

```
Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

```
65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d et=UTF-8 ....<htm
6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f l>Congr atulatio
6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e ns. You 've down
6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 loaded t he file
0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e .http:// gaia.cs.
75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 umass.ed u/wiresh
61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 ark-labs /HTTP-wi
72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 reshark- file1.ht
6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a ml!.</ht ml>
```

## PART-2:

Current filter: http					
No.	Time	Source	Destination	Protocol	Length Info
129	18:11:54.718467120	10.240.16.46	128.119.245.12	HTTP	443 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
134	18:11:54.968694428	128.119.245.12	10.240.16.46	HTTP	784 HTTP/1.1 200 OK (text/html)
154	18:11:55.066934344	10.240.16.46	128.119.245.12	HTTP	400 GET /favicon.ico HTTP/1.1
180	18:11:55.326264868	128.119.245.12	10.240.16.46	HTTP	539 HTTP/1.1 404 Not Found (text/html)
350	18:12:13.625438988	10.240.16.46	128.119.245.12	HTTP	529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
352	18:12:13.873838345	128.119.245.12	10.240.16.46	HTTP	294 HTTP/1.1 304 Not Modified

  

Transmission Control Protocol, Src Port: 56740, Dst Port: 80, Seq: 1, Len: 0	0000	44 b6 be 0a 9a e1 20 c1 2b 1f 79 8a 08 00 45 00	D... ..y...E...
Hypertext Transfer Protocol	0010	01 ad 24 a6 40 00 40 05 84 03 0a f0 10 2e 89 77	... ..w...
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1	0020	f5 0c dd a4 00 50 ac 0c 38 a5 e9 24 88 5d 50 18	... ..P... ..]P...
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html	0030	01 f0 92 41 00 00 47 45 54 20 2f 77 69 72 05 73	... ..GE T /wires...
[GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1]	0040	68 61 72 0b 2d 0c 61 62 73 2f 48 54 54 50 2d 77	... ..ark-lab s/HTTP-w...
[Severity level: Chat]	0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68	... ..reshark -file2.h...
[Group: Sequence]	0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f	... ..tml HTTP /1.1 ..Ho...
Request Method: GET	0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73	... ..st: gaia .cs.umass...
Request URI: /wireshark-labs/HTTP-wireshark-file2.html	0080	73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e	... ..s.edu ..U ser-Agen...
Request Version: HTTP/1.1	0090	74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28	... ..t: Mozil la/5.0 (...
Host: gaia.cs.umass.edu	00a0	58 31 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e	... ..X11; Ubuntu; Lin...
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0	00b0	75 78 20 78 38 36 5f 36 34 3b 20 72 76 3a 31 32	... ..ux x86_64; rv:12...
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	00c0	31 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30	... ..1.0) Gec ko/20100...
Accept-Encoding: gzip, deflate	00d0	31 30 31 20 46 69 72 65 66 6f 78 2f 31 32 31 2e	... ..101 Fire fox/121.0
Accept-Language: en-US,en;q=0.5	00e0	30 0d 0a 41 63 63 05 70 74 3a 20 74 65 78 74 2f	... ..0: Accept: text/...
Connection: keep-alive	00f0	68 74 6d 6c 2c 61 79 70 6c 69 63 61 74 69 6f 6e	... ..html,app lication...
Upgrade-Insecure-Requests: 1	0100	2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69	... .. /xhtml+ x ml,appli...
	0110	63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39	... ..cation/x ml;q=0.9...
	0120	2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67	... ..,image/a vif,imag...

1. No, there is no 'IF-MODIFIED-SINCE' line in the HTTP GET request as we can see above.
2. Yes, the server explicitly returns the contents of the file. As we can see a Line-based text data section which has the same content that we saw on the web page of the given URL.

HTTP response 1/1	0190	73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 0a 3c 06	set=UTF-8...
[Time since request: 0.250227398 seconds]	01a0	74 6d 6c 3e 0a 0a 43 0f 0e 67 72 61 74 75 6c 61	... ..congrat...
[Request in frame: 129]	01b0	74 69 6f 6e 73 20 61 07 61 69 6e 21 20 20 4e 6f	... ..tions ag ain...
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]	01c0	77 29 70 6f 75 27 70 85 29 84 6f 77 6e 6c 6f 61	... ..w you've downl...
File Data: 371 bytes	01d0	84 65 64 20 74 68 65 20 69 69 6c 65 20 6c 61 62	... ..ded the file...
Line-based text data: text/html (10 lines)	01e0	32 2d 32 2e 68 74 6d 6c 2e 20 3c 62 72 3e 0a 54	... ..2-2.html . <br...
	01f0	68 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20	... ..his file 's la...
	0200	6d 6f 64 69 66 69 63 61 74 69 6f 6e 20 64 61 74	... ..modificat ion...
	0210	65 20 77 69 6c 6c 20 6e 6f 74 20 63 68 61 6e 67	... ..e will n ot ch...
	0220	65 2e 20 3c 70 3e 0a 54 68 75 73 20 20 69 6c	... ..e. <p>. Thus...
	0230	20 79 6f 75 20 64 6f 77 6e 6c 6f 61 64 20 74 68	... ..you dow nload...
	0240	69 73 20 6d 75 6c 74 69 79 6c 65 20 74 69 6d 65	... ..is multi ple t...
	0250	73 20 6f 6e 20 79 6f 75 72 20 62 72 6f 77 73 65	... ..s on you r bro...
	0260	72 2c 20 61 29 63 6f 6d 70 6c 65 74 65 20 63 6f	... ..r, a complete...
	0270	70 79 20 3c 62 72 3e 0a 77 69 6c 6c 20 6f 6e 6c	... ..py  . will...
	0280	79 20 62 65 20 73 65 6e 74 20 6f 6e 63 65 20 62	... ..y be sen t onc...
	0290	79 20 74 68 65 20 73 65 72 70 65 72 20 64 75 65	... ..y the se rver...
	02a0	20 74 6f 20 74 68 65 20 69 6e 63 6c 75 73 69 6f	... ..to the inclu...
	02b0	6e 20 6f 66 20 74 68 65 20 49 4e 2d 4d 4f 44 45	... ..n of the IN-W...

3. Yes, there is an 'IF-MODIFIED-SINCE' line in the HTTP GET. The information that follows the header is the time and date[can be seen below] of the last modification of the file from the previous get request.



```

Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [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 (X11; Ubuntu; Linux x86_64; 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: Mon, 22 Jan 2024 06:59:02 GMT\r\n
    If-None-Match: "173-60f835d62e080"\r\n

```

- The status code and phrase returned from the server is 'HTTP/1.1 304 Not Modified'. No, the server didn't return the contents of the file as the browser loaded it from its cache.

### PART-3:

- My browser sent one HTTP GET request message(ignoring the request for favicon). Packet number 232 in the trace contains the GET message for the Bill or Rights.

No.	Time	Source	Destination	Protocol	Length	Info
232	18:19:28.911876369	10.240.16.46	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
240	18:19:29.163075284	128.119.245.12	10.240.16.46	HTTP	4915	HTTP/1.1 200 OK (text/html)
259	18:19:29.247172482	10.240.16.46	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
288	18:19:29.498899140	128.119.245.12	10.240.16.46	HTTP	539	HTTP/1.1 404 Not Found (text/html)

  

Frame 232: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface wlp0s201 Ethernet II, Src: IntelCor_1f:79:8a (28:c1:9b:1f:79:8a), Dst: Cisco_0a:9a:e1 (44:b6:be:0a:9a:e1) Internet Protocol Version 4, Src: 10.240.16.46, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 33580, Dst Port: 80, Seq: 1, Ack: 1, Len: 389 Hypertext Transfer Protocol GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n         [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]         [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]         [Severity level: Chat]         [Group: Sequence]         Request Method: GET         Request URI: /wireshark-labs/HTTP-wireshark-file3.html         Request Version: HTTP/1.1         Host: gaia.cs.umass.edu\r\n         User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; 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         \r\n         [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]         [HTTP request 1/1]         [Response in frame: 240]	0000 44 b0 be 0a 9a e1 20 c1 9b 1f 79 8a 08 00 45 00 D.....y... 0010 01 ad 05 c8 40 00 40 06 a2 e1 0a f0 10 2e 80 77 ...@... 0020 f5 0c 83 2c 00 50 8d 6e 2c e4 33 e6 ac d6 50 18 ...P.n.,3.. 0030 01 f6 92 41 00 00 47 45 54 20 2f 77 69 72 65 73 ...A.GE T /wi 0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTT 0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 33 2e 68 ireshark -file 0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1 0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.u 0080 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e s.edu - U ser-A 0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5. 00a0 58 31 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e X11; Ubu ntui; 00b0 75 78 20 78 38 36 5f 36 34 3b 20 72 76 3a 31 32 ux x86.6 4; rv 00c0 31 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 1.0) Gec ko/20 00d0 31 30 31 20 46 69 72 65 66 6f 78 2f 31 32 31 2e 101 Fire fox/1 00e0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 0 .Accep t: te 00f0 68 74 6d 6c 2c 61 70 78 6c 69 63 61 74 69 6f 6e HTML,app licat 0100 2f 78 0d 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 65 /xhtml-x ml,ap 0110 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 cation/x ml;q 0120 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 ,image/a vif,i 0130 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 e/webp,* /*;q= 0140 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 .Accep t-Lang 0150 65 3a 20 65 6e 2d 55 53 2c 65 0e 3b 71 3d 30 2e e: en-US ,en;q 0160 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 5 -Accep t-Enc 0170 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 ng: gzip , def 0180 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b e-Connec tion 0190 6e 67 7a 74 61 6a 69 76 65 6d 0a 65 70 67 75 61 ean-ali v e .lha
--	--

- Packet number 240 in the trace contains the status code and phrase associated with the response to the HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
232	18:19:28.911876369	10.240.16.46	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
240	18:19:29.163075284	128.119.245.12	10.240.16.46	HTTP	4915	HTTP/1.1 200 OK (text/html)
259	18:19:29.247172482	10.240.16.46	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
288	18:19:29.498899140	128.119.245.12	10.240.16.46	HTTP	539	HTTP/1.1 404 Not Found (text/html)

  

Transmission Control Protocol, Src Port: 80, Dst Port: 33580, Seq: 1, Ack: 390, Len: 4861				0000	20 c1 9b 1f 79 8a f8 7a 41 13 2a c2 08 00 45 28	...y..z A..*
Hypertext Transfer Protocol				0010	13 25 e6 44 48 00 23 06 cd c4 80 77 f5 9c 0a f0	%D#...w.
HTTP/1.1 200 OK\r\n				0020	10 2e 00 50 83 2c 33 e6 ac d0 8d 6e 2e 09 50 18	.P..3...n.
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]				0030	00 ed a3 b9 00 00 48 54 54 50 2f 31 2e 31 20 32	...HT TP/1.
[HTTP/1.1 200 OK\r\n]				0040	30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e	00 OK..D ate:
[Severity level: Chat]				0050	2c 20 32 32 20 4a 61 6e 20 32 30 32 20 31 32	, 22 Jan 2024
[Group: Sequence]				0060	3a 34 39 3a 32 30 20 47 4d 54 0d 0a 53 65 72 76	:49:28 G MT..S
Response Version: HTTP/1.1				0070	65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36	er: Apac he/2.
Status Code: 200				0080	20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53	(CentOS ) Ope
[Status Code Description: OK]				0090	4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48	L/1.0.2k -flips
Response Phrase: OK				00a0	50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72	P/7.4.33 mod
Date: Mon, 22 Jan 2024 12:49:28 GMT\r\n				00b0	6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35	l/2.0.11 Perl
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				00c0	2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69	.16.3..L ast-M
Last-Modified: Mon, 22 Jan 2024 06:59:02 GMT\r\n				00d0	66 69 65 64 3a 20 4d 6f 6e 2c 20 32 32 20 4a 61	fied: Mo n, 22
ETag: "1194-60f835d62a9c"\r\n				00e0	6e 20 32 30 32 34 20 30 36 3a 35 39 3a 30 32 20	n 2024 0 6:59:
Accept-Ranges: bytes\r\n				00f0	47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 31 39 34	GMT..ETA g: "1
Content-Length: 4500\r\n				0100	2d 30 39 66 38 33 35 64 30 32 61 39 63 60 22 0d	-60f835d 62a9c
Keep-Alive: timeout=5, max=100\r\n				0110	0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20	Accept- Range
Connection: Keep-Alive\r\n				0120	62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c	bytes..C onten
Content-Type: text/html; charset=UTF-8\r\n				0130	65 6e 67 74 68 3a 20 34 35 30 30 0d 0a 4b 65 65	length: 4 500 ..
\r\n				0140	70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74	p-Alive: time
[HTTP response 1/1]				0150	3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e	=5, max= 100 ..
[Time since request: 0.251198915 seconds]				0160	6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c	nection: Keep
[Request in frame: 232]				0170	69 70 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70	ive..Con tent-
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]				0180	65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68	e: text/ html;
File Data: 4500 bytes				0190	61 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c	arset=UTF F-8 ..
Line-based text data: text/html (98 lines)				01a0	68 74 6d 6c 3e 3c 68 65 61 64 3e 20 0a 3c 74 69	html>che ad> ..
				01b0	74 6c 65 3e 48 69 73 74 6f 72 69 63 61 6c 20 44	tle>Hist orica

- Status Code: 200; Phrase in the Response: OK [Can be seen above from the screenshot]

Hypertext Transfer Protocol	
HTTP/1.1 200 OK\r\n	
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]	
[HTTP/1.1 200 OK\r\n]	
[Severity level: Chat]	
[Group: Sequence]	
Response Version: HTTP/1.1	
Status Code: 200	
[Status Code Description: OK]	
Response Phrase: OK	

  

Transmission Control Protocol, Src Port: 80, Dst Port: 63037, Seq: 3751, Ack: 473, Len: 1111	
[4 Reassembled TCP Segments (4861 bytes): #232(1250), #233(1250), #234(1250), #235(1111)]	

## PART-4:

No.	Time	Source	Destination	Protocol	Length	Info
240	18:41:16.086242871	10.240.16.46	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
244	18:41:16.426723125	128.119.245.12	10.240.16.46	HTTP	1355	HTTP/1.1 200 OK (text/html)
259	18:41:16.505981801	10.240.16.46	128.119.245.12	HTTP	400	GET /pearson.png HTTP/1.1
263	18:41:16.706084195	10.240.16.46	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
280	18:41:16.840127093	128.119.245.12	10.240.16.46	HTTP	3660	HTTP/1.1 200 OK (PNG)
283	18:41:17.082193957	128.119.245.12	10.240.16.46	HTTP	539	HTTP/1.1 404 Not Found (text/html)
308	18:41:19.894054962	10.240.16.46	178.79.137.164	HTTP	379	GET /8E_cover_small.jpg HTTP/1.1
323	18:41:20.086078361	178.79.137.164	10.240.16.46	HTTP	237	HTTP/1.1 301 Moved Permanently

- My browser sent 3 HTTP GET request messages(ignore the one for favicon). The internet addresses to which the GET requests were sent:
  - 128.119.245.12 (1<sup>st</sup> GET – Page Address)
  - 128.119.245.12 (2<sup>nd</sup> GET – pearson.png)
  - 178.79.137.164 (3<sup>rd</sup> GET – 8E\_cover\_small.jpg)

2. The browser downloaded the images serially because we can see from the screenshot above that the request for the second image was sent only after a response for the first image was received after sending the request for the first image, i.e., the second image was only requested after the first image came back. Also, the images were transmitted over two TCP connections, so we can say that they were downloaded serially.

## PART-5:

### 1. Status code: 401; Phrase: Unauthorized

+	1065	19:03:00.066873550	10.240.16.46	128.119.245.12	HTTP	459	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
+	1083	19:03:00.340344594	128.119.245.12	10.240.16.46	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
	1537	19:04:06.207886005	10.240.16.46	128.119.245.12	HTTP	518	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
	1540	19:04:06.537856194	128.119.245.12	10.240.16.46	HTTP	544	HTTP/1.1 200 OK (text/html)

▼	Hypertext Transfer Protocol
▼	HTTP/1.1 401 Unauthorized\r\n
▶	[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
	Response Version: HTTP/1.1
	Status Code: 401
	[Status Code Description: Unauthorized]
	Response Phrase: Unauthorized

2. As we can see in the screenshot below, a new field (Authorization) is included in the HTTP GET message=> Authorization: Basic

▼	Hypertext Transfer Protocol
▼	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
▶	[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
	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 (X11; Ubuntu; Linux x86_64; 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\r\n
	Accept-Encoding: gzip, deflate\r\n
	Connection: keep-alive\r\n
	Upgrade-Insecure-Requests: 1\r\n
▶	Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
	\r\n
	[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
	[HTTP request 1/2]
	[Response in frame: 1540]
	[Next request in frame: 1564]