



## Lab Report

### CSE351, Computer Networks

Name: **Malak Mohamed Helmy Elbakry** ID: **20P2434**  
Lab No: ( 2 ) Experiment Title: Wireshark\_HTTP\_v7.0  
Date: 25 / 10 /2023

#### The Basic HTTP GET/response interaction:

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
164	22:40:29.439680	172.20.10.4	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
502	22:40:35.598501	128.119.245.12	172.20.10.4	HTTP	540	HTTP/1.1 200 OK (text/html)
507	22:40:35.709801	172.20.10.4	128.119.245.12	HTTP	478	GET /favicon.ico HTTP/1.1
694	22:40:40.592219	172.20.10.4	128.119.245.12	HTTP	478	GET /favicon.ico HTTP/1.1
812	22:40:43.705515	128.119.245.12	172.20.10.4	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
164	22:40:29.439680	172.20.10.4	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
502	22:40:35.598501	128.119.245.12	172.20.10.4	HTTP	540	HTTP/1.1 200 OK (text/html)
507	22:40:35.709801	172.20.10.4	128.119.245.12	HTTP	478	GET /favicon.ico HTTP/1.1
694	22:40:40.592219	172.20.10.4	128.119.245.12	HTTP	478	GET /favicon.ico HTTP/1.1
812	22:40:43.705515	128.119.245.12	172.20.10.4	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 502: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_a4:4a:2b (3c:22:fb:a4:4a:2b), Dst: Apple\_a4:4a:2b (3c:22:fb:a4:4a:2b)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.4  
> Transmission Control Protocol, Src Port: 80, Dst Port: 51925, Seq: 1, Ack: 479, Len: 486  
Hypertext Transfer Protocol  
> HTTP/1.1 200 OK\r\nDate: Wed, 25 Oct 2023 19:40:32 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Wed, 25 Oct 2023 05:59:01 GMT\r\nETag: "80-6088426e7faf"\r\nAccept-Ranges: bytes\r\nContent-Length: 128\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/2]  
[Time since request: 6.158821000 seconds]  
[Request in frame: 164]  
[Next request in frame: 507]  
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]  
File Data: 128 bytes  
Line-based text data: text/html (4 lines)

0000 3c 22 fb a4 4a 2b f6 be  
0010 02 0e 7b 69 00 00 25 06  
0020 0a 04 00 50 ca d5 19 5a  
0030 00 ed fe 18 00 00 48 54  
0040 30 30 20 4f 4b 0d 0a 44  
0050 2c 20 32 35 20 4f 63 74  
0060 3a 34 30 3a 33 32 20 47  
0070 65 72 3a 20 41 70 61 63  
0080 20 28 43 65 6e 74 4f 53  
0090 4c 2f 31 2e 30 2e 32 6b  
00a0 50 2f 37 2e 34 2e 33 33  
00b0 6c 2f 32 2e 30 2e 31 31  
00c0 2e 31 36 2e 33 0d 0a 4c  
00d0 66 69 65 64 3a 20 57 65  
00e0 74 20 32 30 32 33 20 30  
00f0 47 4d 54 0d 0a 45 54 61  
0100 30 38 38 34 32 36 65 37  
0110 63 63 65 70 74 2d 52 61  
0120 74 65 73 0d 0a 43 6f 6e  
0130 67 74 68 3a 20 31 32 38  
0140 6c 69 76 65 3a 20 74 69  
0150 20 6d 61 78 3d 31 30 30  
0160 74 69 6f 6e 3a 20 4b 65  
0170 0d 0a 43 6f 6e 74 65 6e  
0180 74 65 78 74 2f 68 74 6d  
0190 65 74 3d 55 54 46 2d 38  
01a0 6c 3e 0a 43 6f 6e 67 72  
01b0 6e 73 2e 20 20 59 6f 75  
01c0 6c 6f 61 64 65 64 20 74  
01d0 0a 68 74 74 70 3a 2f 2f  
01e0 75 6d 61 73 73 2e 65 64  
01f0 61 72 6b 2d 6c 61 62 73  
0200 72 65 73 68 61 72 6b 2d  
0210 6d 6c 21 0a 3c 2f 68 74

## 1. Question 1

Wireshark capture showing network traffic for question 1. The packet list pane shows several frames, with frame 164 selected. The details pane shows the following information:

Frame 164: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface en0, id 0  
Ethernet II, Src: Apple\_a4:a2:b (3c:22:fb:a4:a2:b), Dst: f6:be:ec:8c:1f:64 (f6:be:ec:8c:1f:64)  
Internet Protocol Version 4, Src: 172.20.10.4, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 51925, Dst Port: 80, Seq: 1, Ack: 1, Len: 478

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 HTTP/1.1\r\n[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n[Severity level: Chat]  
[Group: Sequence]  
Request Method: GET  
Request URI: /wireshark-labs/HTTP-wireshark-file1.html  
Request Version: HTTP/1.1

The bytes pane shows the raw hex and ASCII data for the selected frame.

## 2. Question 2

Wireshark capture showing network traffic for question 2. The packet list pane shows several frames, with frame 164 selected. The details pane shows the following information:

Frame 164: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface en0, id 0  
Ethernet II, Src: Apple\_a4:a2:b (3c:22:fb:a4:a2:b), Dst: f6:be:ec:8c:1f:64 (f6:be:ec:8c:1f:64)  
Internet Protocol Version 4, Src: 172.20.10.4, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 51925, Dst Port: 80, Seq: 1, Ack: 1, Len: 478

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 HTTP/1.1\r\n[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n[Severity level: Chat]  
[Group: Sequence]  
Request Method: GET  
Request URI: /wireshark-labs/HTTP-wireshark-file1.html  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\nAccept: 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\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n

## 3. Question 3

Wireshark capture showing network traffic for question 3. The packet list pane shows several frames, with frame 164 selected. The details pane shows the following information:

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\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n

## 4. Question 4

My IP address : 172.20.10.4      IP of the gaia.cs.umass.edu server:      128.119.245.12

Status Code:200

```

http
No. | Time           | Source          | Destination      | Protocol | Length| Info
+-- 164 22:40:29.439680 172.20.10.4    128.119.245.12   HTTP     532 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
+-- 502 22:40:35.598501 128.119.245.12  172.20.10.4    HTTP     540 HTTP/1.1 200 OK (text/html)
+-- 507 22:40:35.709801 172.20.10.4    128.119.245.12   HTTP     478 GET /favicon.ico HTTP/1.1
+-- 694 22:40:40.592219 172.20.10.4    128.119.245.12   HTTP     478 GET /favicon.ico HTTP/1.1
+-- 812 22:40:43.705515 128.119.245.12  172.20.10.4    HTTP     539 HTTP/1.1 404 Not Found (text/html)

> Frame 502: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en0, id 0
> Ethernet II, Src: f6:be:ec:8c:1f:64 (f6:be:ec:8c:1f:64), Dst: Apple_a4:a4:2b (3c:22:fb:a4:a4:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 51925, Seq: 1, Ack: 479, Len: 486
< 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
    Date: Wed, 25 Oct 2023 19:40:32 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: Wed, 25 Oct 2023 05:59:01 GMT\r\n
    ETag: "80-6088426e74faf"\r\n
    Accept-Ranges: bytes\r\n

```

## 5. Question 5

```

http
No. | Time           | Source          | Destination      | Protocol | Length| Info
+-- 164 22:40:29.439680 172.20.10.4    128.119.245.12   HTTP     532 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
+-- 502 22:40:35.598501 128.119.245.12  172.20.10.4    HTTP     540 HTTP/1.1 200 OK (text/html)

> Frame 502: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en0, id 0
> Ethernet II, Src: f6:be:ec:8c:1f:64 (f6:be:ec:8c:1f:64), Dst: Apple_a4:a4:2b (3c:22:fb:a4:a4:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 51925, Seq: 1, Ack: 479, Len: 486
< 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
    Date: Wed, 25 Oct 2023 19:40:32 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: Wed, 25 Oct 2023 05:59:01 GMT\r\n
    ETag: "80-6088426e74faf"\r\n
    Accept-Ranges: bytes\r\n

```

## 6. Question 6

```

Accept-Ranges: bytes\r\n
> Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n

```

## 7. Question 7

No there is no any headers within the data that are not displayed in the packet-listing window.

0000	f6	be	ec	8c	1f	64	3c	22	fb	a4	4a	2b	08	00	45	02	.....d<" ..J+..E..
0010	02	06	00	00	40	00	40	06	0d	54	ac	14	0a	04	80	77	.....@..@.. T.....w
0020	f5	0c	ca	d5	00	50	8f	a8	e4	b1	19	5a	9f	a7	50	18	.....P.. ..Z..P..
0030	10	00	cb	e9	00	00	47	45	54	20	2f	77	69	72	65	73	.....GE T /wires
0040	68	61	72	6b	2d	6c	61	62	73	2f	48	54	54	50	2d	77	hark-lab s/HTTP-w
0050	69	72	65	73	68	61	72	6b	2d	66	69	6c	65	31	2e	68	ireshark -file1.h
0060	74	6d	6c	20	48	54	54	50	2f	31	2e	31	0d	0a	48	6f	tml HTTP /1.1..Ho
0070	73	74	3a	20	67	61	69	61	2e	63	73	2e	75	6d	61	73	st: gaia .cs.umass
0080	73	2e	65	64	75	0d	0a	43	6f	6e	6e	65	63	74	69	6f	s.edu..C onnectio
0090	6e	3a	20	6b	65	65	70	2d	61	6c	69	76	65	0d	0a	55	n: keep- alive..U
00a0	70	67	72	61	64	65	2d	49	6e	73	65	63	75	72	65	2d	pgrade-I nsecure-
00b0	52	65	71	75	65	73	74	73	3a	20	31	0d	0a	55	73	65	Requests : 1..Use
00c0	72	2d	41	67	65	6e	74	3a	20	4d	6f	7a	69	6c	6c	61	r-Agent: Mozilla
00d0	2f	35	2e	30	20	28	4d	61	63	69	6e	74	6f	73	68	3b	/5.0 (Macintosh; Intel Mac OS X
00e0	20	49	6e	74	65	6c	20	4d	61	63	20	4f	53	20	58	20	10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
00f0	31	30	5f	31	35	5f	37	29	20	41	70	70	6c	65	57	65	Chrome/18.0.0.0
0100	62	4b	69	74	2f	35	33	37	2e	33	36	20	28	4b	48	54	Safari/537.36..
0110	4d	4c	2c	20	6c	69	6b	65	20	47	65	63	6b	6f	29	20	Accept: text/html,application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp,image/apng,*/*;q=0.8 ,application/signature;v=b3;q=0.7.
0120	43	68	72	6f	6d	65	2f	31	31	38	2e	30	2e	30	2e	30	Accept-Encoding: gzip, deflate..Accept-Language: en-US, en;q=0.9
0130	20	53	61	66	61	72	69	2f	35	33	37	2e	33	36	0d	0a	....
0140	41	63	63	65	70	74	3a	20	74	65	78	74	2f	68	74	6d	....
0150	6c	2c	61	70	70	6c	69	63	61	74	69	6f	6e	2f	78	68	....
0160	74	6d	6c	2b	78	6d	6c	2c	61	70	70	6c	69	63	61	74	....
0170	69	6f	6e	2f	78	6d	6c	3b	71	3d	30	2e	39	2c	69	6d	....
0180	61	67	65	2f	61	76	69	66	2c	69	6d	61	67	65	2f	77	....
0190	65	62	70	2c	69	6d	61	67	65	2f	61	70	6e	67	2c	2a	....
01a0	2f	2a	3b	71	3d	30	2e	38	2c	61	70	70	6c	69	63	61	....
01b0	74	69	6f	6e	2f	73	69	67	6e	65	64	2d	65	78	63	68	....
01c0	61	6e	67	65	3b	76	3d	62	33	3b	71	3d	30	2e	37	0d	....
01d0	0a	41	63	63	65	70	74	2d	45	6e	63	6f	64	69	6e	67	....
01e0	3a	20	67	7a	69	70	2c	20	64	65	66	6c	61	74	65	0d	....
01f0	0a	41	63	63	65	70	74	2d	4c	61	6e	67	75	61	67	65	....
0200	3a	20	65	6e	2d	55	53	2c	65	6e	3b	71	3d	30	2e	39	....
0210	0d	0a	0d	0a													....

# The HTTP CONDITIONAL GET/response interaction

## 8. Question 8

There is no IF-MODIFIED-SINCE as it was not cached before

```
No. | Time | Source | Destination | Protocol | Length| Info
+-- 747 08:03:05.859843 192.168.1.6 128.119.245.12 HTTP 532 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+-- 776 08:03:06.016937 128.119.245.12 192.168.1.6 HTTP 784 HTTP/1.1 200 OK (text/html)
856 08:03:21.030700 192.168.1.6 128.119.245.12 HTTP 644 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
858 08:03:21.201126 128.119.245.12 192.168.1.6 HTTP 294 HTTP/1.1 304 Not Modified

> Frame 747: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b), Dst: zte_c8:26:a3 (c0:fd:84:c8:26:a3)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52597, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
+ 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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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-US,en;q=0.9\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: 776]
```

## 9. Question 9

Knew from:

- 1- In the line 776 it is visible the (text/html)
- 2- In the details of the packet there is content length
- 3- Line-based text data is visible

```
No. | Time | Source | Destination | Protocol | Length| Info
+-- 747 08:03:05.859843 192.168.1.6 128.119.245.12 HTTP 532 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+-- 776 08:03:06.016937 128.119.245.12 192.168.1.6 HTTP 784 HTTP/1.1 200 OK (text/html)
856 08:03:21.030700 192.168.1.6 128.119.245.12 HTTP 644 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
858 08:03:21.201126 128.119.245.12 192.168.1.6 HTTP 294 HTTP/1.1 304 Not Modified

Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Thu, 26 Oct 2023 05:03:06 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: Thu, 26 Oct 2023 05:03:01 GMT\r\n
ETag: "173-608977c7aaa56"\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: 0.157094000 seconds]
[Request in frame: 747]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
+ Line-based text data: text/html (10 lines)

\b
<html>\n\b
  Congratulations again! Now you've downloaded the file lab2.html. <br>\n
  This file's last modification date will not change. <br>\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
</html>\n\b
```

## 10. Question 10

No.	Time	Source	Destination	Protocol	Length	Info
747	08:03:05.859843	192.168.1.6	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
776	08:03:06.016937	128.119.245.12	192.168.1.6	HTTP	784	HTTP/1.1 200 OK (text/html)
→ 856	08:03:21.030700	192.168.1.6	128.119.245.12	HTTP	644	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
→ 858	08:03:21.201126	128.119.245.12	192.168.1.6	HTTP	294	HTTP/1.1 304 Not Modified

```

> Frame 856: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b), Dst: zte_c8:26:a3 (c0:fd:84:c8:26:a3)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52596, Dst Port: 80, Seq: 1, Ack: 1, Len: 590
└ 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
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-608977c7aaa56"\r\n
    If-Modified-Since: Thu, 26 Oct 2023 05:03:01 GMT\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: 858]

```

## 11. Question 11

No.	Time	Source	Destination	Protocol	Length	Info
747	08:03:05.859843	192.168.1.6	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
776	08:03:06.016937	128.119.245.12	192.168.1.6	HTTP	784	HTTP/1.1 200 OK (text/html)
→ 856	08:03:21.030700	192.168.1.6	128.119.245.12	HTTP	644	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
→ 858	08:03:21.201126	128.119.245.12	192.168.1.6	HTTP	294	HTTP/1.1 304 Not Modified

```

> Frame 858: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface en0, id 0
> Ethernet II, Src: zte_c8:26:a3 (c0:fd:84:c8:26:a3), Dst: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6
> Transmission Control Protocol, Src Port: 80, Dst Port: 52596, Seq: 1, Ack: 591, Len: 240
└ Hypertext Transfer Protocol
  └ HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      [HTTP/1.1 304 Not Modified\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
    Date: Thu, 26 Oct 2023 05:03:21 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-608977c7aaa56"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.170426000 seconds]
  [Request in frame: 856]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

Status Code 304 -> Not Modified

```

> Frame 858: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface en0, id 0
> Ethernet II, Src: zte_c8:26:a3 (c0:fd:84:c8:26:a3), Dst: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6
> Transmission Control Protocol, Src Port: 80, Dst Port: 52596, Seq: 1, Ack: 591, Len: 240
  Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
      [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
          [Severity level: Chat]
          [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
      Date: Thu, 26 Oct 2023 05:03:21 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
      Connection: Keep-Alive\r\n
      Keep-Alive: timeout=5, max=100\r\n
      ETag: "173-608977c7aaa56"\r\n
    \r\n
      [HTTP response 1/1]
      [Time since request: 0.170426000 seconds]
      [Request in frame: 856]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

No, the sever did not send the content in the second response, as there was

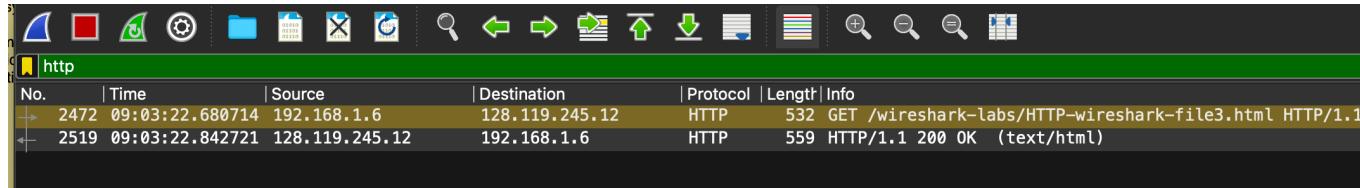
- 1- no line-based text
- 2- no text/html message with the packet received
- 3- no content length

## Retrieving Long Documents

### 12. Question 12

Only one GET request

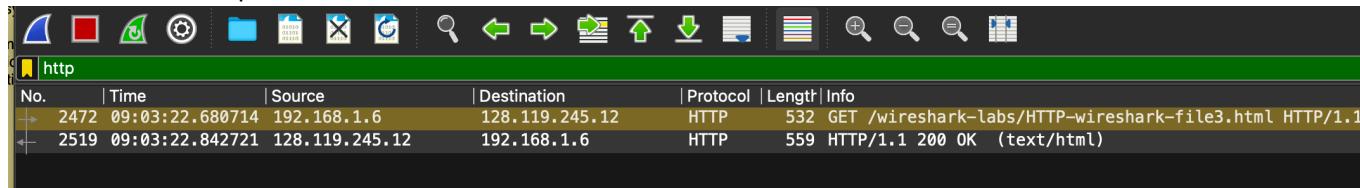
Packet number is 2472



No.	Time	Source	Destination	Protocol	Length	Info
2472	09:03:22.680714	192.168.1.6	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2519	09:03:22.842721	128.119.245.12	192.168.1.6	HTTP	559	HTTP/1.1 200 OK (text/html)

### 13. Question 13

The number of the packet is 2519



No.	Time	Source	Destination	Protocol	Length	Info
2472	09:03:22.680714	192.168.1.6	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2519	09:03:22.842721	128.119.245.12	192.168.1.6	HTTP	559	HTTP/1.1 200 OK (text/html)

### 14. Question 14

Status Code is 200

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

## 15. Question 15

4 TCP segments

→ 2472 09:03:22.680714 192.168.1.6	128.119.245.12	HTTP	532 GET /wireshark-labs/HTTP-wireshark-
2519 09:03:22.842721 128.119.245.12	192.168.1.6	HTTP	559 HTTP/1.1 200 OK (text/html)
> Frame 2519: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface en0, id 0			
> Ethernet II, Src: zte_c8:26:a3 (c0:fd:84:c8:26:a3), Dst: Apple_a4:4a:2b (3c:22:fb:a4:4a:2b)			
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6			
> Transmission Control Protocol, Src Port: 80, Dst Port: 53064, Seq: 4357, Ack: 479, Len: 505			
└ [4 Reassembled TCP Segments (4861 bytes): #2515(1452), #2517(1452), #2518(1452), #2519(505)]			
[Frame: 2515, payload: 0-1451 (1452 bytes)]			
[Frame: 2517, payload: 1452-2903 (1452 bytes)]			
[Frame: 2518, payload: 2904-4355 (1452 bytes)]			
[Frame: 2519, payload: 4356-4860 (505 bytes)]			
[Segment count: 4]			
[Reassembled TCP length: 4861]			
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205468752c203236204f63742032...]			

## HTML Documents with Embedded Objects

### 16. Question 16

3 GET requests, 1 for the html and the other 2 for the images

The IP address : 128.119.245.12 and 178.79.137.164 (for the other photo)

645	16:28:34.088989	192.168.1.6	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file4.html	HTTP/1.1
668	16:28:34.248706	128.119.245.12	192.168.1.6	HTTP	1355	HTTP/1.1 200 OK (text/html)	
671	16:28:34.267874	192.168.1.6	128.119.245.12	HTTP	478	GET /pearson.png	HTTP/1.1
680	16:28:34.353594	192.168.1.6	178.79.137.164	HTTP	457	GET /8E_cover_small.jpg	HTTP/1.1
682	16:28:34.426493	178.79.137.164	192.168.1.6	HTTP	237	HTTP/1.1 301 Moved Permanently	
685	16:28:34.426528	128.119.245.12	192.168.1.6	HTTP	761	HTTP/1.1 200 OK (PNG)	

### 17. Question 17

```
Line wrap □
1 <html>
2 <head>
3 <title>Lab2-4 file: Embedded URLs</title>
4 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
5 </head>
6
7 <body bgcolor="#FFFFFF" text="#000000">
8
9 <p>
10  </p>
11 <p>This little HTML file is being served by gaia.cs.umass.edu.
12 It contains two embedded images. The image above, also served from the
13 gaia.cs.umass.edu web site, is the logo of our publisher, Pearson.
14 The image of our 8th edition book cover below is stored at, and served from,
15 a WWW server kurose.cslash.net in France:</p>
16 <p align="left"></p>
18 And while we have your attention, you might want to take time to check out the
19 available open resources for this book at
20 <a href="http://gaia.cs.umass.edu/kurose_ross"> http://gaia.cs.umass.edu/kurose_ross</a>.
21
22 </body>
23 </html>
24
```

One of the photos were from the same source as the text and the other one from another source (src from img tag)  
So, they were downloaded from 2 different sources in parallel

## HTTP Authentication

### 18. Question 18

The Wireshark interface shows a list of network frames. Frame 167 is highlighted in green, indicating it is selected. The details pane displays the following information:

No. | Time | Source | Destination | Protocol | Length | Info

167	16:57:01.309488	192.168.1.6	128.119.245.12	HTTP	538	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
192	16:57:01.468281	128.119.245.12	192.168.1.6	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
428	16:57:29.381225	192.168.1.6	128.119.245.12	HTTP	623	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
433	16:57:29.546304	128.119.245.12	192.168.1.6	HTTP	574	HTTP/1.1 404 Not Found (text/html)
660	16:58:05.022309	192.168.1.6	128.119.245.12	HTTP	623	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
664	16:58:05.181603	128.119.245.12	192.168.1.6	HTTP	574	HTTP/1.1 404 Not Found (text/html)
726	16:58:09.803842	192.168.1.6	128.119.245.12	HTTP	597	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
754	16:58:09.952514	128.119.245.12	192.168.1.6	HTTP	573	HTTP/1.1 404 Not Found (text/html)

> Frame 192: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface en0, id 0  
> Ethernet II, Src: zte\_c8:26:a3 (c0:fd:84:c8:26:a3), Dst: Apple\_a4:4a:2b (3c:22:fb:a4:4a:2b)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6  
> Transmission Control Protocol, Src Port: 80, Dst Port: 54227, Seq: 1, Ack: 485, Len: 717  
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  
    Date: Thu, 26 Oct 2023 13:57:01 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    WWW-Authenticate: Basic realm="wireshark-students only"\r\n    Content-Length: 381\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: 0.158793000 seconds]  
    [Request in frame: 167]  
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-]  
    File Data: 381 bytes  
Line-based text data: text/html (12 lines)

Status Code: 401 Unauthorized

### 19. Question 19

The Wireshark interface shows a list of network frames. Frame 660 is highlighted in green, indicating it is selected. The details pane displays the following information:

No. | Time | Source | Destination | Protocol | Length | Info

167	16:57:01.309488	192.168.1.6	128.119.245.12	HTTP	538	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
192	16:57:01.468281	128.119.245.12	192.168.1.6	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
428	16:57:29.381225	192.168.1.6	128.119.245.12	HTTP	623	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
433	16:57:29.546304	128.119.245.12	192.168.1.6	HTTP	574	HTTP/1.1 404 Not Found (text/html)
660	16:58:05.022309	192.168.1.6	128.119.245.12	HTTP	623	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
664	16:58:05.181603	128.119.245.12	192.168.1.6	HTTP	574	HTTP/1.1 404 Not Found (text/html)
726	16:58:09.803842	192.168.1.6	128.119.245.12	HTTP	597	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
754	16:58:09.952514	128.119.245.12	192.168.1.6	HTTP	573	HTTP/1.1 404 Not Found (text/html)

> Frame 660: 623 bytes on wire (4984 bits), 623 bytes captured (4984 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_a4:4a:2b (3c:22:fb:a4:4a:2b), Dst: zte\_c8:26:a3 (c0:fd:84:c8:26:a3)  
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 54234, Dst Port: 80, Seq: 1, Ack: 1, Len: 569  
HyperText Transfer Protocol  
  GET /wireshark-labs/protected\_pages/HTTP-wireshark- HTTP/1.1\r\n    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected\_pages/HTTP-wireshark- HTTP/1.1\r\n    [GET /wireshark-labs/protected\_pages/HTTP-wireshark- HTTP/1.1\r\n    [Severity level: Chat]  
    [Group: Sequence]  
    Request Method: GET  
    Request URI: /wireshark-labs/protected\_pages/HTTP-wireshark-  
    Request Version: HTTP/1.1  
    Host: gaia.cs.umass.edu\r\n    Connection: keep-alive\r\n    Cache-Control: max-age=0\r\n    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbz0m5ldHdvcmss=\r\n        [Credentials: wireshark-students:network]  
    Upgrade-Insecure-Requests: 1\r\n

Authorization field