

**Name : Hazem Morsy Hassan**

**ID : 16**

## 1) My HTTP version is 1.1 and the server's HTTP version is also 1.1.

### Client HTTP version

No.	Time	Source	Destination	Protocol	Length	Info
75	14:24:22.438808	192.168.0.102	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 75: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F}, 0  
Ethernet II, Src: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50)  
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 4046, Dst Port: 80, Seq: 1, Ack: 1, Len: 497  
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

### Server HTTP version :

No.	Time	Source	Destination	Protocol	Length	Info
87	14:24:22.580502	128.119.245.12	192.168.0.102	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 87: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F}, 0  
Ethernet II, Src: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102  
Transmission Control Protocol, Src Port: 80, Dst Port: 4046, Seq: 1, Ack: 498, Len: 486  
Hypertext Transfer Protocol  
HTTP/1.1 200 OK\r\n  
Date: Thu, 12 Nov 2020 12:24:22 GMT\r\n  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod\_perl/2.0.11 Perl/v5.16.3\r\n

## 2) It accept two languages which are English (USA) and Arabic (Egypt)

No.	Time	Source	Destination	Protocol	Length	Info
75	14:24:22.438808	192.168.0.102	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 75: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F}, 0  
Ethernet II, Src: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50)  
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 4046, Dst Port: 80, Seq: 1, Ack: 1, Len: 497  
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/86.0.4240.198 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=0.9\r\n  
Accept-Encoding: gzip, deflate\r\n  
Accept-Language: en-US,en;q=0.9,ar-EG;q=0.8,ar;q=0.7\r\n  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

- 3) The IP address of my computer (client) is 192.168.0.102 , The IP address of gaia.cs.umass.edu (server) is 128.119.245.12

```
No.      Time          Source           Destination      Protocol Length Info
1.1      75 14:24:22.438808 192.168.0.102    128.119.245.12   HTTP      551      GET /wireshark-labs/HTTP-wireshark-file1.html HTTP
Frame 75: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},
0
Ethernet II, Src: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4046, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
```

- 4) Status code is (200 ok)

```
No.      Time          Source           Destination      Protocol Length Info
87 14:24:22.580502 128.119.245.12    192.168.0.102   HTTP      540      HTTP/1.1 200 OK (text/html)
Frame 87: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B
0
Ethernet II, Src: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4046, Seq: 1, Ack: 498, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 12 Nov 2020 12:24:22 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

- 5) The file was last-modified on 12 november 2020 at 6:59:02 GMT

```
No.      Time          Source           Destination      Protocol Length Info
87 14:24:22.580502 128.119.245.12    192.168.0.102   HTTP      540      HTTP/1.1 200 OK (text/html)
Frame 87: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B
0
Ethernet II, Src: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4046, Seq: 1, Ack: 498, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 12 Nov 2020 12:24:22 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Thu, 12 Nov 2020 06:59:02 GMT\r\n
ETag: "80-5b3e3726eb737"\r\n
Accept-Ranges: bytes\r\n
```

## 6) The content length is 128 bytes.

```
No.      Time                Source                Destination           Protocol Length Info
  87 14:24:22.580502      128.119.245.12        192.168.0.102        HTTP      540      HTTP/1.1 200 OK (text/html)
Frame 87: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-
0
Ethernet II, Src: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4046, Seq: 1, Ack: 498, Len: 486
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 12 Nov 2020 12:24:22 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Thu, 12 Nov 2020 06:59:02 GMT\r\n
  ETag: "80-5b3e3726eb737"\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
```

## 7) No, all headers in raw data are in packet listing window

```
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: Thu, 12 Nov 2020 12:24:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2

060 3a 32 34 3a 32 32 20 47 4d 54 0d 0a 53 65 72 76 :24:22 G MT- Serv
070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS
090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
0a0 50 2f 37 2e 34 2e 31 32 20 6d 6f 64 5f 70 65 72 P/7.4.12 mod_per
0b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5
0c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3-Last-Modi
0d0 66 69 65 64 3a 20 54 68 75 2e 20 31 32 20 4a 6f fied: Th u 12 No
```

This is just a sample but all other raw data appeared in listing packet window.

## 8) IF MODIFIED SINCE doesn't appear in the request message because cache is empty.

```
No.      Time                Source           Destination      Protocol Length Info
 43 16:17:55.995092    192.168.0.102    128.119.245.12   HTTP      432    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP
1.1
Frame 43: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},
0
Ethernet II, Src: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 27591, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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-file2.html]
[HTTP request 1/2]
[Response in frame: 47]
[Next request in frame: 55]
```

## 9) Yes , the server returns the contents of the file explicitly as it is shown in line-based text data section.

```
No.      Time                Source           Destination      Protocol Length Info
 47 16:17:56.129111    128.119.245.12    192.168.0.102    HTTP      784    HTTP/1.1 200 OK (text/html)
Frame 47: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{495AEA71-B264-4AB-
0
Ethernet II, Src: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80, Dst Port: 27591, Seq: 1, Ack: 379, Len: 730
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 12 Nov 2020 14:17:56 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Thu, 12 Nov 2020 06:59:02 GMT\r\n
  ETag: "173-5b3e3726eab7f"\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 1/2]
[Time since request: 0.134019000 seconds]
[Request in frame: 43]
[Next request in frame: 55]
[Next response in frame: 56]
[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)
  \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) IF MODIFIED SINCE appears in the second HTTP request because the web page is cached , the information are the last modified date that appears in the first request.**

No.	Time	Source	Destination	Protocol	Length	Info
55	16:18:00.192920	192.168.0.102	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 55: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F}, 0

Ethernet II, Src: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 27591, Dst Port: 80, Seq: 379, Ack: 731, Len: 490

Hypertext Transfer Protocol

```

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: Thu, 12 Nov 2020 06:59:02 GMT\r\n
If-None-Match: "173-5b3e3726eab7f"\r\n
Cache-Control: max-age=0\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

**11) The status code is (304) with statement (not modified) , No the contents of file is not returned by the server itself because the data cached in proxy server is correct and not modified since the first time the page was retrieved so content of page will be retrieved from the proxy server.**

No.	Time	Source	Destination	Protocol	Length	Info
56	16:18:00.331747	128.119.245.12	192.168.0.102	HTTP	293	HTTP/1.1 304 Not Modified

Frame 56: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F}, 0

Ethernet II, Src: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102

Transmission Control Protocol, Src Port: 80, Dst Port: 27591, Seq: 731, Ack: 869, Len: 239

Hypertext Transfer Protocol

```

HTTP/1.1 304 Not Modified\r\n
Date: Thu, 12 Nov 2020 14:18:00 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5b3e3726eab7f"\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.138827000 seconds]
[Prev request in frame: 43]
[Prev response in frame: 47]
[Request in frame: 55]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

12) There is one HTTP request that the client send to the server , the packet number is (26)

No.	Time	Source	Destination	Protocol	Length	Info
26	17:14:02.188653	192.168.0.102	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP

1.1  
Frame 26: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},  
0  
Ethernet II, Src: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50)  
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 28753, Dst Port: 80, Seq: 1, Ack: 1, Len: 378  
Hypertext Transfer Protocol  
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n  
Host: gaia.cs.umass.edu\r\n  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0\r\n

13) The response is sent in packet number (32)

No.	Time	Source	Destination	Protocol	Length	Info
32	17:14:02.459017	128.119.245.12	192.168.0.102	HTTP	559	HTTP/1.1 200 OK (text/html)

0  
Frame 32: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},  
0  
Ethernet II, Src: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102  
Transmission Control Protocol, Src Port: 80, Dst Port: 28753, Seq: 4357, Ack: 379, Len: 505  
[4 Reassembled TCP Segments (4861 bytes): #28(1452), #29(1452), #31(1452), #32(505)]  
Hypertext Transfer Protocol  
HTTP/1.1 200 OK\r\n  
Date: Thu, 12 Nov 2020 15:14:02 GMT\r\n

14) The status code is 200 with statement OK

No.	Time	Source	Destination	Protocol	Length	Info
32	17:14:02.459017	128.119.245.12	192.168.0.102	HTTP	559	HTTP/1.1 200 OK (text/html)

0  
Frame 32: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},  
0  
Ethernet II, Src: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102  
Transmission Control Protocol, Src Port: 80, Dst Port: 28753, Seq: 4357, Ack: 379, Len: 505  
[4 Reassembled TCP Segments (4861 bytes): #28(1452), #29(1452), #31(1452), #32(505)]  
Hypertext Transfer Protocol  
HTTP/1.1 200 OK\r\n  
Date: Thu, 12 Nov 2020 15:14:02 GMT\r\n  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod\_perl/2.0.11 Perl/v5.16.3\r\n  
Last-Modified: Thu, 12 Nov 2020 06:59:02 GMT\r\n  
ETag: "1194-5b3e3726e49d7"\r\n  
Accept-Ranges: bytes\r\n  
Content-Length: 4500\r\n

**15) There are four TCP segments in total three of them of size (1452 bytes) and the last one is 505 bytes**

```
No.      Time                Source                Destination            Protocol Length Info
 32 17:14:02.459017    128.119.245.12        192.168.0.102          HTTP      559      HTTP/1.1 200 OK (text/html)
Frame 32: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B682-FF9AA9A}
0
Ethernet II, Src: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80, Dst Port: 28753, Seq: 4357, Ack: 379, Len: 505
[4 Reassembled TCP Segments (4861 bytes): #28(1452), #29(1452), #31(1452), #32(505)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 12 Nov 2020 15:14:02 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Thu, 12 Nov 2020 06:59:02 GMT\r\n
```

**16) There are three HTTP requests (one for text and other two for two images) , all of them to the same destination (128.119.245.12)**

```
No.      Time                Source                Destination            Protocol Length Info
 41 20:15:57.306263    192.168.0.102        128.119.245.12        HTTP      432      GET /wireshark-labs/HTTP-wireshark-file4.html HTTP
1.1
Frame 41: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},
0
Ethernet II, Src: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1363, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
```

```
No.      Time                Source                Destination            Protocol Length Info
 45 20:15:57.572882    192.168.0.102        128.119.245.12        HTTP      389      GET /pearson.png HTTP/1.1
Frame 45: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},
0
Ethernet II, Src: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1364, Dst Port: 80, Seq: 1, Ack: 1, Len: 335
Hypertext Transfer Protocol
  GET /pearson.png HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0\r\n
  Accept: image/webp,*/*\r\n
```

```
No.      Time                Source                Destination            Protocol Length Info
 65 20:15:58.083623    192.168.0.102        128.119.245.12        HTTP      403      GET /~kurose/cover_5th_ed.jpg HTTP/1.1
Frame 65: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B682-FF9AA9A1AD2F},
0
Ethernet II, Src: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1367, Dst Port: 80, Seq: 1, Ack: 1, Len: 349
Hypertext Transfer Protocol
  GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n
  Host: manic.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0\r\n
  Accept: image/webp,*/*\r\n
```



17) The images are downloaded in series because the first image (logo) is retrieved from the server before the second image is requested from the client.

No.	Time	Source	Destination	Protocol	Length	Info
45	20:15:57.572882	192.168.0.102	128.119.245.12	HTTP	389	GET /pearson.png HTTP/1.1

Frame 45: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-E0-000000000000}

Ethernet II, Src: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12

  

No.	Time	Source	Destination	Protocol	Length	Info
52	20:15:57.722639	128.119.245.12	192.168.0.102	HTTP	762	HTTP/1.1 200 OK (PNG)

Frame 52: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-E0-000000000000}

Ethernet II, Src: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102

  

No.	Time	Source	Destination	Protocol	Length	Info
65	20:15:58.083623	192.168.0.102	128.119.245.12	HTTP	403	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

Frame 65: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9A-E0-000000000000}

Ethernet II, Src: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12

18) Status code is (401) with statement (unauthorized).

No.	Time	Source	Destination	Protocol	Length	Info
14	21:04:40.348322	128.119.245.12	192.168.0.102	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Frame 14: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF\_{495AEA71-B264-4AB4-B682-FF9A-E0-000000000000}

Ethernet II, Src: Tp-LinkT\_c0:41:50 (d4:6e:0e:c0:41:50), Dst: LiteonTe\_5d:37:d1 (cc:b0:da:5d:37:d1)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102

Transmission Control Protocol, Src Port: 80, Dst Port: 2188, Seq: 1, Ack: 394, Len: 717

Hypertext Transfer Protocol

HTTP/1.1 401 Unauthorized\r\n

Date: Thu, 12 Nov 2020 19:04:40 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod\_perl/2.0.11 Perl/5.16.3 lib

## 19) Authorization field is added which has the encoded data (username and password) to base64

```
No.      Time          Source            Destination      Protocol Length  Info
44  21:04:53.302228  192.168.0.102    128.119.245.12  HTTP           506      GET /wireshark-labs/protected_pages/HTTP-
wiresharkfile5.html HTTP/1.1
Frame 44: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface \Device\NPF_{495AEA71-B264-4AB4-B682-FF9AA9A1}
0
Ethernet II, Src: LiteonTe_5d:37:d1 (cc:b0:da:5d:37:d1), Dst: Tp-LinkT_c0:41:50 (d4:6e:0e:c0:41:50)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 2192, Dst Port: 80, Seq: 1, Ack: 1, Len: 452
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
  Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmMs=\r\n
    Credentials: wireshark-students:network
\r\n
```