

I. The Basic HTTP GET/response interaction

1. Http 1.1

No.	Time	Source	Destination	Protocol	Length	Info
77	3.864524	10.0.0.11	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
96	4.019861	128.119.245.12	10.0.0.11	HTTP	540	HTTP/1.1 200 OK (text/html)

2. French / English US GB

Accept-Encoding: gzip, deflate\r\n

Accept-Language: fr,fr-FR;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n\r\n

3. My computer : 10.0.0.11

Server : 128.119.245.12

4. 200 OK

Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n

5. Last-Modified: Mon, 22 Nov 2021 06:59:02 GMT\r\n

96	4.019861	128.119.245.12	10.0.0.11	HTTP	540	HTTP/1.1 200 OK (text/html)
101	4.084478	10.0.0.11	128.119.245.12	HTTP	514	GET /favicon.ico HTTP/1.1

<

> Frame 96: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CC5F4EEA-CBA4-4F...}

> Ethernet II, Src: HeightsT_44:57:1a (00:b8:c2:44:57:1a), Dst: IntelCor_e4:ef:b7 (34:41:5d:e4:ef:b7)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.11

> Transmission Control Protocol, Src Port: 80, Dst Port: 50750, Seq: 1, Ack: 515, Len: 486

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Mon, 22 Nov 2021 12:26:10 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Mon, 22 Nov 2021 06:59:02 GMT\r\n

ETag: "80-5d15b28eade71"\r\n

Accept-Ranges: bytes\r\n

6. [Content length: 128]

Content-Length: 128\r\n

[Content length: 128]

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

7. .

II. The HTTP CONDITIONAL GET/response interaction

8. No there is no “IF-MODIFIED-SINCE” line in the HTTP GET.

No.	Time	Source	Destination	Protocol	Length	Info
93	3.446995	10.0.0.11	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
108	3.602485	128.119.245.12	10.0.0.11	HTTP	784	HTTP/1.1 200 OK (text/html)
231	10.171865	10.0.0.11	128.119.245.12	HTTP	680	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
234	10.330245	128.119.245.12	10.0.0.11	HTTP	294	HTTP/1.1 304 Not Modified
421	11.476642	10.0.0.11	128.119.245.12	HTTP	680	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
815	11.634050	128.119.245.12	10.0.0.11	HTTP	293	HTTP/1.1 304 Not Modified
979	12.706480	10.0.0.11	128.119.245.12	HTTP	680	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
982	12.872663	128.119.245.12	10.0.0.11	HTTP	293	HTTP/1.1 304 Not Modified
1869	14.191975	10.0.0.11	128.119.245.12	HTTP	680	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2268	14.347857	128.119.245.12	10.0.0.11	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 93: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits) on interface \Device\NPF_{CC5F4EEA-CBA4-4F20-A6D7-92330528288A}, id 0
> Ethernet II, Src: IntelCor_e4:ef:b7 (34:41:5d:e4:ef:b7), Dst: HeightsT_44:57:1a (00:b8:c2:44:57:1a)
> Internet Protocol Version 4, Src: 10.0.0.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60796, Dst Port: 80, Seq: 1, Ack: 1, Len: 514

▼ 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]

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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36 Edg/96.0.1054.29\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: fr,fr-FR;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
\r\n

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

We can see the content into the line-based text data part where we can see all the html code that was display on my web browser.

We also can see that the http response is 1/1 so we can be sure that we didn't miss anything.

No.	Time	Source	Destination	Protocol	Length	Info
93	3.446995	10.0.0.11	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
108	3.602485	128.119.245.12	10.0.0.11	HTTP	784	HTTP/1.1 200 OK (text/html)
231	10.171865	10.0.0.11	128.119.245.12	HTTP	680	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
234	10.330245	128.119.245.12	10.0.0.11	HTTP	294	HTTP/1.1 304 Not Modified
421	11.476642	10.0.0.11	128.119.245.12	HTTP	680	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
815	11.634050	128.119.245.12	10.0.0.11	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 108: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{CC5F4EEA-CBA4-4F20-A6D7-92330528288A}, id 0
> Ethernet II, Src: HeightsT_44:57:1a (00:b8:c2:44:57:1a), Dst: IntelCor_e4:ef:b7 (34:41:5d:e4:ef:b7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 60796, Seq: 1, Ack: 515, Len: 730

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Tue, 23 Nov 2021 08:40:35 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Tue, 23 Nov 2021 06:59:01 GMT\r\n

ETag: "173-5d16f46b89069"\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: 0.155490000 seconds]
[Request in frame: 93]
[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.
\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
\n

will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE
\n

field in your browser's HTTP GET request to the server.\n

\n

</html>\n

10. Yes, there is a line "IF-MODIFIED-SINCE:".

It shows the date the last time I ask for those web pages, if the content was modified after this, we need to download it again and not to use what we have in the cache.

```
93 3.446995 10.0.0.11 128.119.245.12 HTTP 568 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
108 3.602485 128.119.245.12 10.0.0.11 HTTP 784 HTTP/1.1 200 OK (text/html)
231 10.171865 10.0.0.11 128.119.245.12 HTTP 680 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
234 10.330245 128.119.245.12 10.0.0.11 HTTP 294 HTTP/1.1 304 Not Modified
421 11.476642 10.0.0.11 128.119.245.12 HTTP 680 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

> Frame 231: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits) on interface \Device\NPF_{CC5F4EEA-CBA4-4F20-A6D7-923305282B8A}, id 0
> Ethernet II, Src: IntelCor_e4:ef:b7 (34:41:5d:e4:ef:b7), Dst: HeightsT_44:57:1a (00:b8:c2:44:57:1a)
> Internet Protocol Version 4, Src: 10.0.0.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60797, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
▼ 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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36 Edg/96.0.1054.29\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: fr,fr-FR;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  If-None-Match: "173-5d16f46b89069"\r\n
  If-Modified-Since: Tue, 23 Nov 2021 06:59:01 GMT\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/4]
  [Response in frame: 234]
  [Next request in frame: 421]
```

11. HTTP/1.1 304 Not Modified\r\n

The server didn't return the content he return the information that the content didn't get modified so the web browser will use what he have on his cache that is exactly the same content instead of asking it again.

III. Retrieving Long Documents

12. The browser send 2 GET messages.

2172 / 3215 are the packet numbers

No.	Time	Source	Destination	Protocol	Length	Info
2172	5.448806	10.0.0.11	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2194	5.611575	128.119.245.12	10.0.0.11	HTTP	559	HTTP/1.1 200 OK (text/html)
3215	5.961494	10.0.0.11	3.222.239.149	HTTP	427	GET /pulse?authon&user=F3EAD8380B2077F5B0AA2428AA407A50&ur1_heartbeat=1,0,182,182,0&db_conn=1,0,0,0 HTTP/1.1
3562	6.114406	3.222.239.149	10.0.0.11	HTTP	194	HTTP/1.1 200 OK

13. The number of the packet is 2194

14. 200 OK

15. There is 4 data containing TCP segments

```
2172 5.448806 10.0.0.11 128.119.245.12 HTTP 568 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2194 5.611575 128.119.245.12 10.0.0.11 HTTP 559 HTTP/1.1 200 OK (text/html)
3215 5.961494 10.0.0.11 3.222.239.149 HTTP 427 GET /pulse?authon&user=F3EAD8380B2077F5B0AA2428AA407A50&ur1_heartbeat=1,0,182,182,0&db_conn=1,0,0,0 HTTP/1.1
3562 6.114406 3.222.239.149 10.0.0.11 HTTP 194 HTTP/1.1 200 OK

> Frame 2194: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{CC5F4EEA-CBA4-4F20-A6D7-923305282B8A}, id 0
> Ethernet II, Src: HeightsT_44:57:1a (00:b8:c2:44:57:1a), Dst: IntelCor_e4:ef:b7 (34:41:5d:e4:ef:b7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 64719, Seq: 4357, Ack: 515, Len: 505
▼ [4 Reassembled TCP Segments (4861 bytes): #2190(1452), #2191(1452), #2193(1452), #2194(505)]
  [Frame: 2190, payload: 0-1451 (1452 bytes)]
  [Frame: 2191, payload: 1452-2903 (1452 bytes)]
  [Frame: 2193, payload: 2904-4355 (1452 bytes)]
  [Frame: 2194, payload: 4356-4860 (505 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205475652c203233204e6f762032.]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

IV. HTML Documents with Embedded Objects

16. The browser send 3 http GET request messages.

The first one to 128.119.245.12 : [Full request URI:

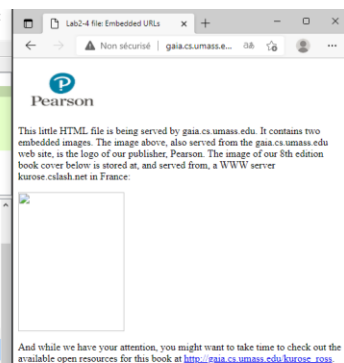
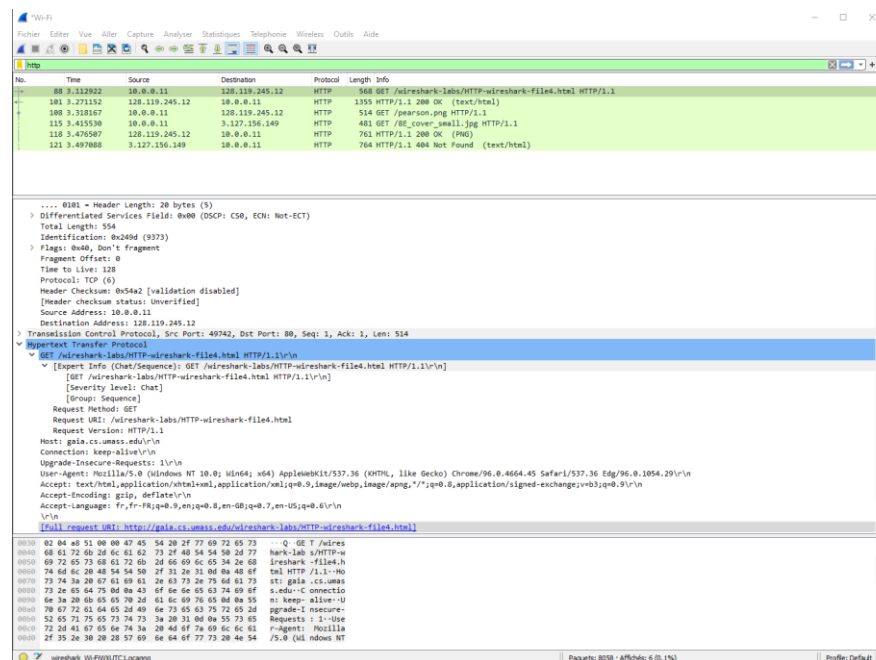
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>]

The second to 128.119.245.12 : [Full request URI:

<http://gaia.cs.umass.edu/pearson.png>]

The third one to 3.127.156.149: [Full request URI:

http://kurose.cslash.net/8E_cover_small.jpg]



17. The browser download the images in serially. We can see different request at different time, each request get response before another request was send. We request and responses images one by one.

V. HTTP Authentication

18. [HTTP/1.1 401 Unauthorized\r\n]

70	3.591658	10.0.0.11	128.119.245.12	584	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
85	3.749336	128.119.245.12	10.0.0.11	771	HTTP/1.1 401 Unauthorized (text/html)
246	17.170251	10.0.0.11	3.222.239.149	427	GET /pulse?author&user=F3EAD838DB2077F5B8AA2428AA407A50&ur1_heartbeat=1,0,173,173,0&db_conn=1,0,0,0,0 HTTP/1.1
247	17.322242	3.222.239.149	10.0.0.11	194	HTTP/1.1 200 OK
339	26.384137	10.0.0.11	128.119.245.12	669	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
351	26.540287	128.119.245.12	10.0.0.11	544	HTTP/1.1 200 OK (text/html)

19. At the second time , The GET request added username and password to get authorize access

Cache-Control: max-age=0\r\n

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM05ldHdvcm5=\r\n

Credentials: wireshark-students:network

Upgrade-Insecure-Requests: 1\r\n