



# COMPUTER NETWORK

## Lab 2a

Student name: Nguyễn Minh Tâm  
ID: 1952968

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

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Ans: Both of them are version 1.1

```
> Frame 741: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64956, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
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]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1..Ho
> Frame 792: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_5e:45:34 (dc:fb:48:5e:45:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 64956, Seq: 1, Ack: 497, Len: 486
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: Sat, 16 Oct 2021 01:57:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
0030 00 ed af b6 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1. 2
```

2. What languages (if any) does your browser indicate that it can accept to the server?

Ans: vi-VN and en-US

```
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]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.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/94.0.4606.81 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: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n
0150 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c pplicati on/xhtmll
0160 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,app lication
0170 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 /xml;q=0 .9,image
0180 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 /avif,im age/webp
0190 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b ,image/a png,*/*;
01a0 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f q=0.8,ap plicatio
01b0 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 n/signed -exchang
01c0 65 3b 76 3d 62 33 3b 71 3d 30 2e 39 0d 0a 41 63 e;v=b3;q =0.9..Ac
01d0 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g
01e0 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 zip, def late..Ac
01f0 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 76 cept-Lan guage: v
0200 69 2d 56 4e 2c 76 69 3b 71 3d 30 2e 39 2c 65 6e i-VN,vi; q=0.9,en
0210 2d 55 53 3b 71 3d 30 2e 38 2c 65 6e 3b 71 3d 30 -US;q=0. 8,en;q=0
0220 2e 37 0d 0d 0d 0a .7..
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

My computer: 192.168.1.7

gaia.cs.umass.edu: 128.119.245.12



No.	Time	Source	Destination	Protocol	Length	Info
741	6.618024	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
792	6.883143	128.119.245.12	192.168.1.7	HTTP	540	HTTP/1.1 200 OK (text/html)

  

```
> Frame 741: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64956, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
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]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

  

```
0000  9c 65 ee c9 2d cf dc fb 48 5e 45 34 08 00 45 00  e.....H^E4...E-
0010  02 18 32 35 40 00 80 06 00 00 c0 a8 01 07 80 77  --25@.....w
0020  f5 0c fd bc 00 50 86 73 33 8a c2 47 96 b3 50 18  ....P-s3--G--P-
```

4. What is the status code returned from the server to your browser?

Ans: 200

```
> Frame 792: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_5e:45:34 (dc:fb:48:5e:45:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 64956, Seq: 1, Ack: 497, Len: 486
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: Sat, 16 Oct 2021 01:57:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

  

```
0030  00 ed af b6 00 00 48 54 54 50 2f 31 2e 31 20 82  ....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74  00 OK..D ate: Sat
```

5. When was the HTML file that you are retrieving last modified at the server?

Ans: Fri, 15 Oct 2021 05:59:01 GMT

```
> Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_5e:45:34 (dc:fb:48:5e:45:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 64956, Seq: 1, Ack: 497, Len: 486
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: Sat, 16 Oct 2021 01:57:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 15 Oct 2021 05:59:01 GMT\r\n
```

  

```
00c0  2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69  .16.3..Last-Modi
00d0  66 69 65 64 3a 20 46 72 69 2c 20 31 35 20 4f 63  fied: Fri, 15 Oc
00e0  74 20 32 30 32 31 20 30 35 3a 35 39 3a 30 31 20  t 2021 0 5:59:01
00f0  47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 35  GMT..ETa g: "80-5
```

6. How many bytes of content are being returned to your browser?

Ans: 128 bytes



▼ 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: Sat, 16 Oct 2021 01:57:56 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Fri, 15 Oct 2021 05:59:01 GMT\r\n

ETag: "80-5ce5de452c15f"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

---

0120	74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e	tes..Con tent-Len
0130	67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41	gth: 128 ..Keep-A

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Ans: I do not see any headers within the data that are not displayed in the packet-listing window



## II/ The HTTP CONDITIONAL GET/response interaction

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Ans: I do not see any “IF-MODIFIED-SINCE” line in the HTTP GET

```
> Frame 893: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61853, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
▼ 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/94.0.4606.81 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: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\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: 932]
```



9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Ans: Yes, the server explicitly returned the contents of the file by “Line-based text data” section

No.	Time	Source	Destination	Protocol	Length	Info
893	6.228532	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
932	6.497040	128.119.245.12	192.168.1.7	HTTP	784	HTTP/1.1 200 OK (text/html)

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 IF-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n

```

```

0190 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 0a 3c 68 set=UTF-8...<h
01a0 74 6d 6c 3e 0a 0a 43 6f 6e 67 72 61 74 75 6c 61 tml>..Co ngratula
01b0 74 69 6f 6e 73 20 61 67 61 69 6e 21 20 20 4e 6f tions ag ain! No
01c0 77 20 79 6f 75 27 76 65 20 64 6f 77 6e 6c 6f 61 w you've downloa
01d0 64 65 64 20 74 68 65 20 66 69 6c 65 20 6c 61 62 ded the file lab
01e0 32 2d 32 2e 68 74 6d 6c 2e 20 3c 62 72 3e 0a 54 2-2.html. <br>..T
01f0 68 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20 his file 's last
0200 6d 6f 64 69 66 69 63 61 74 69 6f 6e 20 64 61 74 modifika tion dat
0210 65 20 77 69 6c 6c 20 6e 6f 74 20 63 68 61 6e 67 e will n ot chang
0220 65 2e 20 20 3c 70 3e 0a 54 68 75 73 20 20 69 66 e. <p>.. Thus if
0230 20 79 6f 75 20 64 6f 77 6e 6c 6f 61 64 20 74 68 you dow nload th
0240 69 73 20 6d 75 6c 74 69 70 6c 65 20 74 69 6d 65 is multi ple time
0250 73 20 6f 6e 20 79 6f 75 72 20 62 72 6f 77 73 65 s on you r browse
0260 72 2c 20 61 20 63 6f 6d 70 6c 65 74 65 20 63 6f r, a com plete co

```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans: Yes, I see an “IF-MODIFIED-SINCE:” line the HTTP GET.

If-Modified-Since: Fri, 15 Oct 2021 05:59:01 GMT

6826	31.445134	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
6919	31.696765	128.119.245.12	192.168.1.7	HTTP	784	HTTP/1.1 200 OK (text/html)
11614	52.848679	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
11672	53.099393	128.119.245.12	192.168.1.7	HTTP	294	HTTP/1.1 304 Not Modified

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
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/94.0.4606.81 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: vi-VN,v;q=0.9\r\n
If-None-Match: "172-5ce5de452b98f"\r\n
If-Modified-Since: Fri, 15 Oct 2021 05:59:01 GMT\r\n

```

```

01b0 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c /apng,*/*;q=0.8,
01c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e applicat ion/sign
01d0 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 ed-excha nge;v=b3
01e0 3b 71 3d 30 2e 39 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.9.. Accept-E
01f0 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d
0200 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c eflate.. Accept-L
0210 61 6e 67 75 61 67 65 3a 20 76 69 2d 56 4e 2c 76 anguage: vi-VN,v
0220 69 3b 71 3d 30 2e 39 0d 0a 49 66 2d 4e 6f 6e 65 i;q=0.9.. If-None
0230 2d 4d 61 74 63 68 3a 20 22 31 37 33 2d 35 63 65 -Match: "173-5ce
0240 35 64 65 34 35 32 62 39 38 66 22 0d 0a 49 66 2d 5de452b9 8f"..If-
0250 4d 6f 64 69 66 69 65 64 2d 53 69 6e 63 65 3a 20 Modified-Since:
0260 46 72 69 2c 20 31 35 20 4f 63 74 20 32 30 32 31 Fri, 15 Oct 2021
0270 20 30 35 3a 35 39 3a 30 31 20 47 4d 54 0d 0a 0d 05:59:01 GMT..

```

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



Ans:

HTTP status code is 304.

Response phrase: Not Modified.

The server did not explicitly return the contents of the file because there is no change in the file.

6826	31.445134	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
6919	31.696765	128.119.245.12	192.168.1.7	HTTP	784	HTTP/1.1 200 OK (text/html)
11614	52.848679	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
11672	53.099393	128.119.245.12	192.168.1.7	HTTP	294	HTTP/1.1 304 Not Modified

  

Hypertext Transfer Protocol	
HTTP/1.1 304 Not Modified\r\n	
> [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]	
Response Version: HTTP/1.1	
Status Code: 304	
[Status Code Description: Not Modified]	
Response Phrase: Not Modified	
Date: Sat, 16 Oct 2021 02:33:54 GMT\r\n	
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 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: "173-5ce5de452b98f"\r\n	
\r\n	
[HTTP response 1/1]	
[Time since request: 0.250714000 seconds]	

  

0030	00 ee ff f0 00 00 48 54 54 50 2f 31 2e 31 20 33	.....HT TP/1.1
0040	30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04	Not Modified



### III/ Retrieving Long Documents

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Ans: Only 1 HTTP GET request message was sent. The packet number in the trace contains the GET message for the Bill or Rights is 677

No.	Time	Source	Destination	Protocol	Length	Info
677	5.598704	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
703	5.865368	128.119.245.12	192.168.1.7	HTTP	559	HTTP/1.1 200 OK (text/html)

  

> Frame 677: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF\_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0

> Ethernet II, Src: IntelCor\_Se:45:34 (dc:fb:48:5e:45:34), Dst: DASAMNet\_c9:2d:cf (9c:65:ee:c9:2d:cf)

> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 58250, Dst Port: 80, Seq: 1, Ack: 1, Len: 496

> 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]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file3.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/94.0.4606.81 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

0000 9c 65 ee c9 2d cf dc fb 48 5e 45 34 00 00 45 00 ..e...L^E4..E

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Ans: The packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request: 703

No.	Time	Source	Destination	Protocol	Length	Info
677	5.598704	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
703	5.865368	128.119.245.12	192.168.1.7	HTTP	559	HTTP/1.1 200 OK (text/html)

  

> 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: Sat, 16 Oct 2021 02:47:34 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Fri, 15 Oct 2021 05:59:01 GMT\r\n

ETag: "1194-5ce5de45282df"\r\n

Accept-Ranges: bytes\r\n

> Content-Length: 4500\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: 0.266664000 seconds]

[Request in frame: 677]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

File Data: 4500 bytes

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK

14. What is the status code and phrase in the response?

Ans: Using the figure above.

Status Code: 200 and Response Phrase: OK.



15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Ans: 2 data-containing TCP segments were needed

No.	Time	Source	Destination	Protocol	Length	Info
677	5.598704	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
703	5.865368	128.119.245.12	192.168.1.7	HTTP	559	HTTP/1.1 200 OK (text/html)

  

> Frame 703: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A670-F43EE85AE96D}, id 0
> Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_Se:45:34 (dc:fb:48:5e:45:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 58250, Seq: 4357, Ack: 497, Len: 505
> [2 Reassembled TCP Segments (4861 bytes): #702(4356), #703(505)]
[Frame: 702, payload: 0-4355 (4356 bytes)]
[Frame: 703, payload: 4356-4860 (505 bytes)]
[Segment count: 2]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205361742c203136204f63742032...]
> 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 53 61 74 2c 20 31 36 20 4f	-Date: Sat, 16 Oct 2021 02:47:34
0020	63 74 20 32 30 32 31 20 30 32 3a 34 37 3a 33 34	GMT--Server: Apache/2.4.6 (CentOS) Open SSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3
0030	20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70	-Last-Modified: Fri, 15 Oct 2021 05:59:01 GMT--E
0040	61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74	Tag: "11 94-5ce5d
0050	4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e	
0060	32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e	
0070	32 34 2d 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e	
0080	31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d	
0090	0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20	
00a0	46 72 69 2c 20 31 35 20 4f 63 74 20 32 30 32 31	
00b0	20 30 35 3a 35 39 3a 30 31 20 47 4d 54 0d 0a 45	
00c0	54 61 67 3a 20 22 31 31 39 34 2d 35 63 65 35 64	



## IV/ HTML Documents with Embedded Objects

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Ans: There were 3 HTTP GET request messages sent.

The initial page “HTTP-wireshark-file4.html” and the figure “pearson.png” were sent to the IP address: 128.119.245.12.

The figure “8E\_cover\_small.jpg” was sent to the IP address: 178.79.137.164.

No.	Time	Source	Destination	Protocol	Length	Info
519	3.777938	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
574	4.042686	128.119.245.12	192.168.1.7	HTTP	1355	HTTP/1.1 200 OK (text/html)
586	4.090306	192.168.1.7	128.119.245.12	HTTP	496	GET /pearson.png HTTP/1.1
635	4.365195	128.119.245.12	192.168.1.7	HTTP	761	HTTP/1.1 200 OK (PNG)
684	4.596337	192.168.1.7	178.79.137.164	HTTP	463	GET /8E_cover_small.jpg HTTP/1.1
708	4.801853	178.79.137.164	192.168.1.7	HTTP	225	HTTP/1.1 301 Moved Permanently

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Ans: By checking the TCP port, I can see that the 2 images were received over 2 different TCP port connections which are 54087 and 64414. Therefore, they were downloaded serially.

No.	Time	Source	Destination	Protocol	Length	Info
519	3.777938	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
574	4.042686	128.119.245.12	192.168.1.7	HTTP	1355	HTTP/1.1 200 OK (text/html)
586	4.090306	192.168.1.7	128.119.245.12	HTTP	496	GET /pearson.png HTTP/1.1
635	4.365195	128.119.245.12	192.168.1.7	HTTP	761	HTTP/1.1 200 OK (PNG)
684	4.596337	192.168.1.7	178.79.137.164	HTTP	463	GET /8E_cover_small.jpg HTTP/1.1
708	4.801853	178.79.137.164	192.168.1.7	HTTP	225	HTTP/1.1 301 Moved Permanently

```
> Frame 586: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54087, Dst Port: 80, Seq: 497, Ack: 1302, Len: 442
  Source Port: 54087
  Destination Port: 80
  [Stream index: 3]
  [TCP Segment Len: 442]
  Sequence Number: 497 (relative sequence number)
  Sequence Number (raw): 2487044650
  [Next Sequence Number: 939 (relative sequence number)]
  Acknowledgment Number: 1302 (relative ack number)
  Acknowledgment number (raw): 1245562003
0020 f5 0c d3 47 00 50 94 3d 4a 2a 4a 3d c4 93 50 18 .G.P.= J*J=...P.
```

No.	Time	Source	Destination	Protocol	Length	Info
519	3.777938	192.168.1.7	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
574	4.042686	128.119.245.12	192.168.1.7	HTTP	1355	HTTP/1.1 200 OK (text/html)
586	4.090306	192.168.1.7	128.119.245.12	HTTP	496	GET /pearson.png HTTP/1.1
635	4.365195	128.119.245.12	192.168.1.7	HTTP	761	HTTP/1.1 200 OK (PNG)
684	4.596337	192.168.1.7	178.79.137.164	HTTP	463	GET /8E_cover_small.jpg HTTP/1.1
708	4.801853	178.79.137.164	192.168.1.7	HTTP	225	HTTP/1.1 301 Moved Permanently

```
> Frame 684: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 178.79.137.164
> Transmission Control Protocol, Src Port: 64414, Dst Port: 80, Seq: 1, Ack: 1, Len: 409
  Source Port: 64414
  Destination Port: 80
  [Stream index: 8]
  [TCP Segment Len: 409]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3705028877
  [Next Sequence Number: 410 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2675106424
0020 89 a4 fb 9e 00 50 dc d6 41 0d 9f 72 e2 78 50 18 .A.P..A...xP.
```



## V/ HTTP Authentication

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Ans: We get a response: 'HTTP/1.1 401 Unauthorized'.

Status code: 401.

Response phrase: Unauthorized.

No.	Time	Source	Destination	Protocol	Length	Info
913	6.329059	192.168.1.7	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
940	6.593451	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3276	26.590631	192.168.1.7	128.119.245.12	HTTP	651	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3298	26.854577	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

  

> Frame 940: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF\_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0

> Ethernet II, Src: DASANNet\_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor\_5e:45:34 (dc:fb:48:5e:45:34)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7

> Transmission Control Protocol, Src Port: 80, Dst Port: 50761, Seq: 1, Ack: 513, 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: Sat, 16 Oct 2021 03:25:19 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod\_perl/2.0.11 Perl/v5.16.3\r\n

  

0030 00 ed ba ce 00 00 48 54 54 50 2f 31 2e 31 20 34 .....HT TP/1.1 4

0040 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0d 01 Unaut horized.

0050 0a 44 61 74 65 3a 20 53 61 74 2c 20 31 36 20 4f .Date: S at, 16 O

0060 63 74 20 32 30 32 31 20 30 33 3a 32 35 3a 31 39 ct 2021 03:25:19

0070 20 47 4d 54 0d 00 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap

19. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Ans:

The screenshot of the first HTTP GET message:

No.	Time	Source	Destination	Protocol	Length	Info
913	6.329059	192.168.1.7	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
940	6.593451	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3276	26.590631	192.168.1.7	128.119.245.12	HTTP	651	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3298	26.854577	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

  

> Frame 913: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device\NPF\_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0

> Ethernet II, Src: IntelCor\_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet\_c9:2d:cf (9c:65:ee:c9:2d:cf)

> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 50761, Dst Port: 80, Seq: 1, Ack: 1, Len: 512

> 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 HTTP/1.1\r\n]

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

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/94.0.4606.81 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: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n

\r\n

[Full request URI: [http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-file5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)]

[HTTP request 1/1]

[Response in frame: 940]

The screenshot of the second HTTP GET message:



No.	Time	Source	Destination	Protocol	Length	Info
913	6.329059	192.168.1.7	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
940	6.593451	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3276	26.590631	192.168.1.7	128.119.245.12	HTTP	651	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3298	26.854577	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

  

> Frame 3276: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61450, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
> 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 HTTP/1.1\r\n]
> 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
> Connection: keep-alive\r\n
> Cache-Control: max-age=0\r\n
> Authorization: Basic d2lkZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n
> Credentials: wideshark-students:network
> Upgrade-Insecure-Requests: 1\r\n
> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 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: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n
> \r\n

  

00c0	78 2d 61 67 65 3d 30 0d	0a 41 75 74 68 6f 72 68	x-age=0	Authori
00d0	7a 61 74 69 6f 6e 3a 20	42 61 73 69 63 20 64 32	zation: Basic d2	
00e0	6c 6b 5a 58 4e 6f 59 58	4a 72 4c 58 4e 30 64 57	lkZXNoYXJrLXN0dW	
00f0	52 6c 62 6e 52 7a 4f 6d	35 6c 64 48 64 76 63 6d	RlbnRzOm5ldHdvcm	
0100	73 3d 0d 0d	55 70 67 72 61 64 65 2d 49 6e 73 65	s=.	Upgr ade-Inse

Comparing these two HTTP GET messages, it is easy to find that the second HTTP GET message contains the 'Authorization' field.

The username (wideshark-students) and password (network) that I entered are encoded in the string of characters (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=) following the "Authorization: Basic" header in the client's HTTP GET message.