

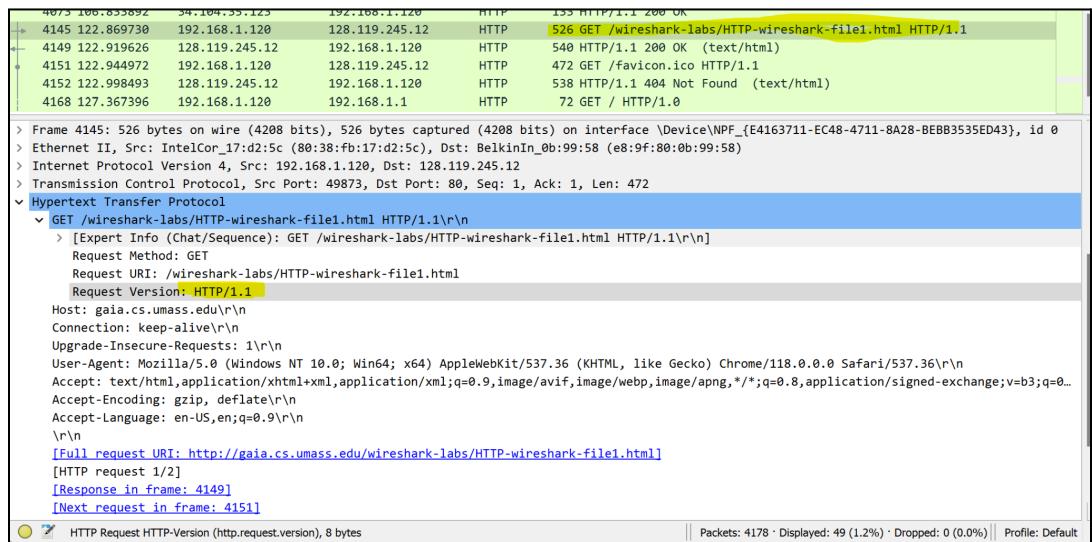
Name	Bayan Alsalem
ID	40105034
Lab section	COEN366 - FK-X

## First part: Wireshark Assignment

### 1. 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?**

My browser is running the HTTP Version 1.1 and the server is also running the HTTP Version 1.1 .



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

From the Accept-Language line, the accepted languages are: en-US and en. These correspond to English (US) and English.

```

> Frame 4145: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0
> Ethernet II, Src: IntelCor_17:d2:5c (80:38:fb:17:d2:5c), Dst: BelkinIn_0b:99:58 (e8:9f:80:0b:99:58)
> Internet Protocol Version 4, Src: 192.168.1.120, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49873, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
< 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/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...
      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-file1.html]
    [HTTP request 1/2]
    [Response in frame: 4149]
    [Next request in frame: 4151]

```

HTTP Request HTTP-Version (http.request.version), 8 bytes || Packets: 4178 · Displayed: 49 (1.2%) · Dropped: 0 (0.0%) || Profile: Default

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

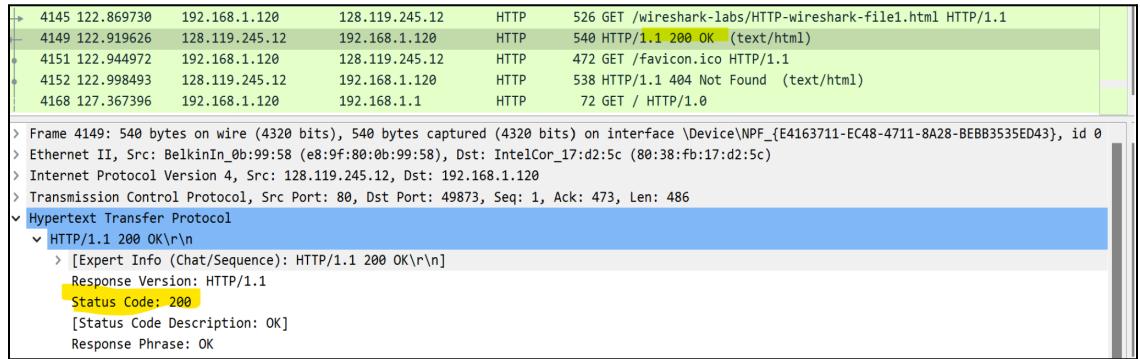
The source IP address corresponding to my machine is 192.168.1.120

The destination IP address corresponding to the server is 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
2785	49.383667	192.168.1.120	204.79.197.203	HTTP	303	GET /ocsp/MFQwUjBQME4wTDAJBgUrDgMCggUABBRyOb3oPpcJ3XHZgxJCfx%2Bu...
2788	49.404262	204.79.197.203	192.168.1.120	OCSP	976	Response
2798	53.123741	192.168.1.120	34.104.35.123	HTTP	335	HEAD /edged1/release2/chrome_component/f6ilipx7xpptsg3gbxdawvql...
2799	53.146670	34.104.35.123	192.168.1.120	HTTP	644	HTTP/1.1 200 OK
2800	53.171597	192.168.1.120	34.104.35.123	HTTP	386	GET /edged1/release2/chrome_component/f6ilipx7xpptsg3gbxdawvql...
2867	53.238121	34.104.35.123	192.168.1.120	HTTP	107	HTTP/1.1 200 OK
2943	77.579109	192.168.1.120	34.104.35.123	HTTP	333	HEAD /edged1/release2/chrome_component/ackl2sjdn34fe6htecmpzgm4...
2944	77.600865	34.104.35.123	192.168.1.120	HTTP	645	HTTP/1.1 200 OK
2945	77.627010	192.168.1.120	34.104.35.123	HTTP	384	GET /edged1/release2/chrome_component/ackl2sjdn34fe6htecmpzgm4b...
3095	77.754791	34.104.35.123	192.168.1.120	HTTP	661	HTTP/1.1 200 OK
3175	106.116991	192.168.1.120	34.104.35.123	HTTP	327	HEAD /edged1/release2/chrome_component/j2hxfei2occ5siiujtlwgp6xi...
3176	106.136445	34.104.35.123	192.168.1.120	HTTP	606	HTTP/1.1 200 OK
3177	106.161868	192.168.1.120	34.104.35.123	HTTP	378	GET /edged1/release2/chrome_component/j2hxfei2occ5siiujtlwgp6xi...
4073	106.833892	34.104.35.123	192.168.1.120	HTTP	133	HTTP/1.1 200 OK
4145	122.869730	192.168.1.120	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
4149	122.919626	128.119.245.12	192.168.1.120	HTTP	540	HTTP/1.1 200 OK (text/html)
4151	122.944972	192.168.1.120	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
4152	122.998493	128.119.245.12	192.168.1.120	HTTP	538	HTTP/1.1 404 Not Found (text/html)
4168	127.367396	192.168.1.120	192.168.1.1	HTTP	72	GET / HTTP/1.0

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

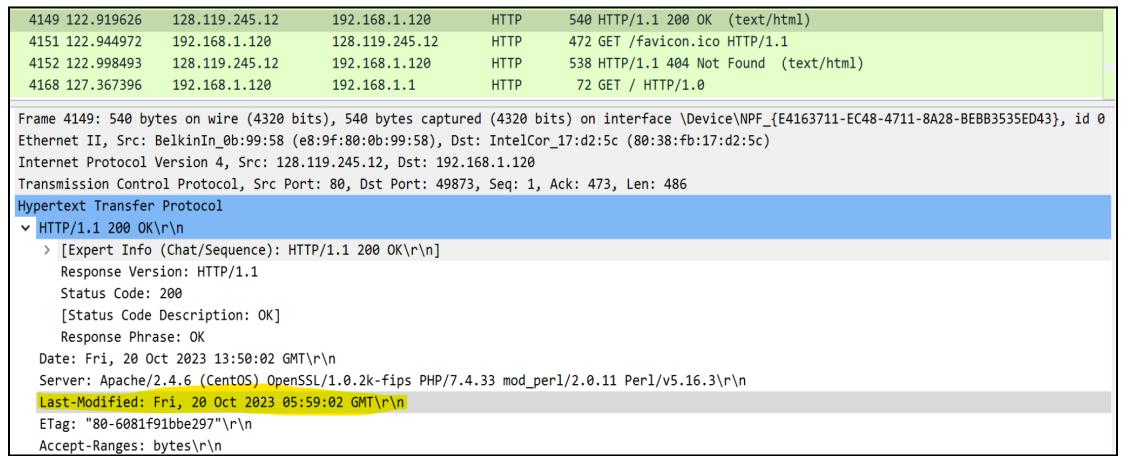
The status code is 200.



Frame 4149: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0  
> Ethernet II, Src: BelkinIn\_0b:99:58 (e8:9f:80:0b:99:58), Dst: IntelCor\_17:d2:5c (80:38:fb:17:d2:5c)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.120  
> Transmission Control Protocol, Src Port: 80, Dst Port: 49873, Seq: 1, Ack: 473, Len: 486  
HTTP/1.1 200 OK\r\n[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]  
Response Version: HTTP/1.1  
Status Code: 200  
[Status Code Description: OK]  
Response Phrase: OK

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

It was last modified on Fri, 20 Oct 2023 05:59:02 GMT.



Frame 4149: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0  
> Ethernet II, Src: BelkinIn\_0b:99:58 (e8:9f:80:0b:99:58), Dst: IntelCor\_17:d2:5c (80:38:fb:17:d2:5c)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.120  
> Transmission Control Protocol, Src Port: 80, Dst Port: 49873, Seq: 1, Ack: 473, Len: 486  
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: Fri, 20 Oct 2023 13:50:02 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: Fri, 20 Oct 2023 05:59:02 GMT\r\nETag: "80-6081f91bbe297"\r\nAccept-Ranges: bytes\r\n

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

128 Bytes.

4149	122.919626	128.119.245.12	192.168.1.120	HTTP	540 HTTP/1.1 200 OK (text/html)
4151	122.944972	192.168.1.120	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
4152	122.998493	128.119.245.12	192.168.1.120	HTTP	538 HTTP/1.1 404 Not Found (text/html)
4168	127.367396	192.168.1.120	192.168.1.1	HTTP	72 GET / HTTP/1.0

**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.**

I see no header in the packet content window that was not in the packet-listing window.

## 2. 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?**

I do not see the “IF-MODIFIED-SINCE” line.

882	507.153485	192.168.1.120	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
884	507.205146	128.119.245.12	192.168.1.120	HTTP	784 HTTP/1.1 200 OK (text/html)
915	536.639427	192.168.1.120	128.119.245.12	HTTP	638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
921	536.690072	128.119.245.12	192.168.1.120	HTTP	294 HTTP/1.1 304 Not Modified
935	549.245301	192.168.1.120	128.119.245.12	HTTP	638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
941	549.294517	128.119.245.12	192.168.1.120	HTTP	294 HTTP/1.1 304 Not Modified

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

Yes the server returned the content of the HTML file.

The screenshot shows a Wireshark capture of an HTTP session. The selected packet is a response to a GET request for 'HTTP-wireshark-file2.html'. The packet details show the following:

- HTTP/1.1 200 OK (text/html)
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Fri, 20 Oct 2023 15:02:13 GMT
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3
- Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT
- ETag: "173-6081f91bbdac7"
- Accept-Ranges: bytes
- Content-Length: 371
- Keep-Alive: timeout=5, max=100
- Connection: Keep-Alive
- Content-Type: text/html; charset=UTF-8

The content pane displays the HTML response body, which includes a congratulatory message about downloading the file and information about the 'IF-MODIFIED-SINCE' header.

Yellow highlights are present on the status bar at the bottom right and on the content pane, likely indicating specific areas of interest.

**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?**

Yes. I see the “IF-MODIFIED-SINCE:” line. It has the following information: Fri, 20 Oct 2023 05:59:02 GMT.

882 507.153485	192.168.1.120	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
884 507.205146	128.119.245.12	192.168.1.120	HTTP	784 HTTP/1.1 200 OK (text/html)
915 536.639427	192.168.1.120	128.119.245.12	HTTP	638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
921 536.690072	128.119.245.12	192.168.1.120	HTTP	294 HTTP/1.1 304 Not Modified
935 549.245301	192.168.1.120	128.119.245.12	HTTP	638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
941 549.294517	128.119.245.12	192.168.1.120	HTTP	294 HTTP/1.1 304 Not Modified
> Frame 915: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0				
> Ethernet II, Src: IntelCor_17:d2:5c (80:38:fb:17:d2:5c), Dst: BelkinIn_0b:99:58 (e8:9f:80:0b:99:58)				
> Internet Protocol Version 4, Src: 192.168.1.120, Dst: 128.119.245.12				
> Transmission Control Protocol, Src Port: 50454, Dst Port: 80, Seq: 1, Ack: 1, Len: 584				
▼ 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				
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/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/*/*;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: "173-6081f91bbdac7"\r\n				
If-Modified-Since: Fri, 20 Oct 2023 05:59:02 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: 921]				

## 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

The status code is 304 and the phrase is Not modified. The server did not explicitly return the content of the HTML file because it was not modified so the server kept the previous content of the file.

915 536.639427	192.168.1.120	128.119.245.12	HTTP	638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
921 536.690072	128.119.245.12	192.168.1.120	HTTP	294 HTTP/1.1 304 Not Modified
935 549.245301	192.168.1.120	128.119.245.12	HTTP	638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
941 549.294517	128.119.245.12	192.168.1.120	HTTP	294 HTTP/1.1 304 Not Modified
> Frame 921: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0				
> Ethernet II, Src: BelkinIn_0b:99:58 (e8:9f:80:0b:99:58), Dst: IntelCor_17:d2:5c (80:38:fb:17:d2:5c)				
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.120				
> Transmission Control Protocol, Src Port: 80, Dst Port: 50454, Seq: 1, Ack: 585, 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]				
Response Version: HTTP/1.1				
Status Code: 304				
[Status Code Description: Not Modified]				
Response Phrase: Not Modified				
Date: Fri, 20 Oct 2023 15:02:43 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: "173-6081f91bbdac7"\r\n				
\r\n				
[HTTP response 1/1]				
[Time since request: 0.050645000 seconds]				
[Request in frame: 915]				
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]				

### 3. 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?**

The browser sent 1 HTTP GET request message. The packet number that contains the Bill of Rights is 286.

No.	Time	Source	Destination	Protocol	Length	Info
284	140.498789	192.168.1.120	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
289	140.548451	128.119.245.12	192.168.1.120	HTTP	535	HTTP/1.1 200 OK (text/html)
335	166.732752	192.168.1.120	66.130.63.18	HTTP	178	GET /ncsi.txt HTTP/1.1
337	166.747387	66.130.63.18	192.168.1.120	HTTP	233	HTTP/1.1 200 OK (text/plain)

> Frame 289: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF\_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0  
> Ethernet II, Src: BelkinIn\_0b:99:58 (e8:9f:80:0b:99:58), Dst: IntelCor\_17:d2:5c (80:38:fb:17:d2:5c)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.120  
> Transmission Control Protocol, Src Port: 80, Dst Port: 50620, Seq: 4381, Ack: 473, Len: 481  
> [4 Reassembled TCP Segments (4861 bytes): #286(1460), #287(1460), #288(1460), #289(481)]

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

The packet number is 289.

No.	Time	Source	Destination	Protocol	Length	Info
284	140.498789	192.168.1.120	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
289	140.548451	128.119.245.12	192.168.1.120	HTTP	535	HTTP/1.1 200 OK (text/html)
335	166.732752	192.168.1.120	66.130.63.18	HTTP	178	GET /ncsi.txt HTTP/1.1
337	166.747387	66.130.63.18	192.168.1.120	HTTP	233	HTTP/1.1 200 OK (text/plain)

> Frame 289: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF\_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0  
> Ethernet II, Src: BelkinIn\_0b:99:58 (e8:9f:80:0b:99:58), Dst: IntelCor\_17:d2:5c (80:38:fb:17:d2:5c)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.120  
> Transmission Control Protocol, Src Port: 80, Dst Port: 50620, Seq: 4381, Ack: 473, Len: 481  
> [4 Reassembled TCP Segments (4861 bytes): #286(1460), #287(1460), #288(1460), #289(481)]  
▼ 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]

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

The status code is **200** and the phrase is **OK**.

```

▼ 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

```

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

4 TCP segments were needed to carry the single HTTP response.

No.	Time	Source	Destination	Protocol	Length	Info
284	140.498789	192.168.1.120	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
289	140.548451	128.119.245.12	192.168.1.120	HTTP	535	HTTP/1.1 200 OK (text/html)
335	166.732752	192.168.1.120	66.130.63.18	HTTP	178	GET /ncsi.txt HTTP/1.1
337	166.747387	66.130.63.18	192.168.1.120	HTTP	233	HTTP/1.1 200 OK (text/plain)

> Frame 289: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF\_{E4163711-EC48-4711-8A28-BEBB3535ED43}, id 0  
> Ethernet II, Src: BelkinIn\_0b:99:58 (e8:9f:80:0b:99:58), Dst: IntelCor\_17:d2:5c (80:38:fb:17:d2:5c)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.120  
> Transmission Control Protocol, Src Port: 80, Dst Port: 50620, Seq: 4381, Ack: 473, Len: 481  
> [4. Reassembled TCP Segments (4861 bytes): #286(1460), #287(1460), #288(1460), #289(481)]  
▼ 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

## 4. HTML Documents with Embedded Object

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

The browser sent out 3 HTTP GET requests,

- the first one to '/wireshark-labs/HTTPwireshark-file4.html'
- the second to '/pearson.png'
- the third to '/8E\_cover\_small.jpg'

373	47.300314	192.168.1.120	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
377	47.348278	128.119.245.12	192.168.1.120	HTTP	1355 HTTP/1.1 200 OK (text/html)
378	47.359109	192.168.1.120	128.119.245.12	HTTP	472 GET /pearson.png HTTP/1.1
383	47.414370	128.119.245.12	192.168.1.120	HTTP	745 HTTP/1.1 200 OK (PNG)
390	47.547845	192.168.1.120	178.79.137.164	HTTP	439 GET /8E_cover_small.jpg HTTP/1.1
392	47.639761	178.79.137.164	192.168.1.120	HTTP	225 HTTP/1.1 301 Moved Permanently
943	54.425962	192.168.1.120	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
947	54.476527	128.119.245.12	192.168.1.120	HTTP	539 HTTP/1.1 404 Not Found (text/html)

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

**Explain.**

According to the time section of the GET requests and responses, the two images were downloaded *serially*. Because, the first GET request gets a response containing a PNG at time 47.359109 while the next GET request for the JPEG is at 47.547845. There is a difference or delay between the two requests of 0.189

373	47.300314	192.168.1.120	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
377	47.348278	128.119.245.12	192.168.1.120	HTTP	1355 HTTP/1.1 200 OK (text/html)
378	47.359109	192.168.1.120	128.119.245.12	HTTP	472 GET /pearson.png HTTP/1.1
383	47.414370	128.119.245.12	192.168.1.120	HTTP	745 HTTP/1.1 200 OK (PNG)
390	47.547845	192.168.1.120	178.79.137.164	HTTP	439 GET /8E_cover_small.jpg HTTP/1.1
392	47.639761	178.79.137.164	192.168.1.120	HTTP	225 HTTP/1.1 301 Moved Permanently
943	54.425962	192.168.1.120	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
947	54.476527	128.119.245.12	192.168.1.120	HTTP	539 HTTP/1.1 404 Not Found (text/html)

## 5. HTTP Authentication

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

The status code is 401 and the phrase is Unauthorized.

This Wireshark capture shows a sequence of four frames. Frame 107 is a GET request from 192.168.1.120 to 192.119.245.12. Frame 111 is a 401 Unauthorized response from 192.119.245.12 to 192.168.1.120. Frame 164 is another GET request from 192.168.1.120 to 192.119.245.12. Frame 169 is a 404 Not Found response from 192.119.245.12 to 192.168.1.120. The details pane for the 401 response shows the status code 401 and the phrase Unauthorized.

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

The new included field is Authorization.

This Wireshark capture shows the same sequence of frames as the previous one, but with additional details for the second GET request (Frame 164). The details pane for this frame shows the inclusion of an 'Authorization' header with the value 'Basic d2lyZXNoYXJrLXN0dWlbnRz0m51dHdvcmss=' and a 'Credentials' value of 'wireshark-students:network'. Other headers shown include Host: gaia.cs.umass.edu, Connection: keep-alive, Cache-Control: max-age=0, and Upgrade-Insecure-Requests: 1.

# What did you learn?

From the Wireshark lab, I have learned how to use Wireshark to capture and analyze network traffic to investigate different aspects of the HTTP protocol. This included understanding the basic GET/response interaction, examining HTTP message formats, retrieving large HTML files, retrieving HTML files with embedded objects, and exploring HTTP authentication.

In particular, the lab has taught me how to use Wireshark to identify the various fields and parameters in HTTP messages and how to interpret the different types of status codes that can be encountered during an HTTP transaction.

Overall, the lab provided a practical introduction to the use of Wireshark as a tool for network analysis, and the insights gained can be valuable for next labs.

## Second part: Socket Programming Assignment

### The Python Code

```
from socket import *

def handle_request(request):
    lines = request.split('\n')
    first_line = lines[0]
    words = first_line.split(' ')
    filename = words[1]

    if filename == '/coen366':
        filename = 'coen366.html'
    else:
        filename = 'error.html'

    return filename

def create_http_response(filename):
    try:
        with open(filename, 'r') as file:

            content = file.read()
            response = f"HTTP/1.1 200
OK\nContent-Length: {len(content)}\nContent-Type:
text/html\n\n{content}"

    except FileNotFoundError:

        response = "HTTP/1.1 404 Not Found\n\nFile
Not Found"
```

```
    return response

def main():

    HOST = '127.0.0.1'
    PORT = 12000

    server_socket = socket(AF_INET, SOCK_STREAM)
    server_socket.bind((HOST, PORT))
    server_socket.listen(1)

    print(f"Server is running on the port {PORT}")

    while True:

        client_socket, client_address =
server_socket.accept()
        request = client_socket.recv(PORT).decode()

        filename = handle_request(request)
        response = create_http_response(filename)

        client_socket.send(response.encode())
        client_socket.close()

if __name__ == "__main__":
    main()
```

## Screenshot of the HTML File from the browser



// CONTENT OF the html file.

# Welcome to COEN 366

Course info:

- Given by Prof. Chadi Assi
- Prof's email: [chadi.assi@concordia.ca](mailto:chadi.assi@concordia.ca)
- There are three TAs for this course:
  - Shreya Khisa
  - Ali Amhaz
  - Y A Joarder

## What did you learn?

From this assignment, I have learned more about Socket Programming and how to write an http server code in python. Also, how to establish a connection between the client and the server.