



**Gökhan Özeloğlu - 21627557**

**Burak Yılmaz - 21627868**

**BBM 453 Computer Networks Lab - HTTP Lab Assignment**

**Group ID: 1**

## IP Address of the computer: 192.168.1.41

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

560	9.032190	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
619	9.178643	128.119.245.12	192.168.1.41	HTTP	540 HTTP/1.1 200 OK (text/html)
643	9.507729	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
654	9.647751	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)

  

>	Frame 619: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
>	Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)
>	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.41
>	Transmission Control Protocol, Src Port: 80, Dst Port: 50146, Seq: 1, Ack: 497, Len: 486
>	Hypertext Transfer Protocol
>	HTTP/1.1 200 OK\r\n
>	Date: Wed, 21 Oct 2020 19:07:29 GMT\r\n
>	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
>	Last-Modified: Wed, 21 Oct 2020 05:59:04 GMT\r\n
>	Etag: "80-5b2280b756e2e"\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

  

>	Transmission Control Protocol, Src Port: 80, Dst Port: 50146, Seq: 1, Ack: 497, Len: 486
>	Hypertext Transfer Protocol
>	HTTP/1.1 200 OK\r\n
>	Date: Wed, 21 Oct 2020 19:07:29 GMT\r\n

HTTP 1.1 version.

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

560	9.032190	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
619	9.178643	128.119.245.12	192.168.1.41	HTTP	540 HTTP/1.1 200 OK (text/html)
643	9.507729	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
654	9.647751	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)

  

>	Frame 560: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
>	Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxelCom_35:a4:27 (08:26:97:35:a4:27)
>	Internet Protocol Version 4, Src: 192.168.1.41, Dst: 128.119.245.12
>	Transmission Control Protocol, Src Port: 50146, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
>	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/86.0.4240.75 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: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
>	\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/86.0.4240.75 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: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
```

You can see from the accepted languages. It accepts tr-TR and en-US and en.

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

560	9.032190	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
619	9.178643	128.119.245.12	192.168.1.41	HTTP	540 HTTP/1.1 200 OK (text/html)
643	9.507729	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
654	9.647751	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)

My computer ip address is 192.168.1.41 and gaia.cs.umass.edu server's ip address is 128.119.245.12.

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

560	9.032190	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
619	9.178643	128.119.245.12	192.168.1.41	HTTP	540 HTTP/1.1 200 OK (text/html)
643	9.507729	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
654	9.647751	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)

200 OK.

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

560	9.032190	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
619	9.178643	128.119.245.12	192.168.1.41	HTTP	540 HTTP/1.1 200 OK (text/html)
643	9.507729	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
654	9.647751	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)

```
> Frame 619: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.41
> Transmission Control Protocol, Src Port: 80, Dst Port: 50146, Seq: 1, Ack: 497, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 21 Oct 2020 19:07:29 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 21 Oct 2020 05:59:04 GMT\r\n
    ETag: "80-5b2280b756e2e"\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
```

```

Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 21 Oct 2020 19:07:29 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 21 Oct 2020 05:59:04 GMT\r\n

```

Last-Modified: Wed, 21 Oct 2020 05:59:04 GMT.

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

No.	Time	Source	Destination	Protocol	Length	Info
560	9.032190	192.168.1.41	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
619	9.178643	128.119.245.12	192.168.1.41	HTTP	540	HTTP/1.1 200 OK (text/html)
643	9.507729	192.168.1.41	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
654	9.647751	128.119.245.12	192.168.1.41	HTTP	538	HTTP/1.1 404 Not Found (text/html)

  

```

> Frame 619: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.41
> Transmission Control Protocol, Src Port: 80, Dst Port: 50146, Seq: 1, Ack: 497, Len: 486
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 21 Oct 2020 19:07:29 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 21 Oct 2020 05:59:04 GMT\r\n
    ETag: "80-5b2280b756e2e"\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

```

128 bytes. It can be seen from the screenshot.

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.

No, The raw data must match up exactly with what is shown in the packet-listing window.

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?

820	5.986433	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
897	6.142185	128.119.245.12	192.168.1.41	HTTP	784 HTTP/1.1 200 OK (text/html)
1090	7.249559	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
1126	7.400100	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)
2582	15.918924	192.168.1.41	128.119.245.12	HTTP	662 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2608	16.077342	128.119.245.12	192.168.1.41	HTTP	294 HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file2.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/86.0.4240.75 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: tr-TR,tr;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 1/2]

[Response in frame: 897]

[Next request in frame: 1090]

No, there is no line called “IF-MODIFIED-SINCE”.

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

820	5.986433	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
897	6.142185	128.119.245.12	192.168.1.41	HTTP	784 HTTP/1.1 200 OK (text/html)
1090	7.249559	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
1126	7.400100	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)
2582	15.918924	192.168.1.41	128.119.245.12	HTTP	662 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2608	16.077342	128.119.245.12	192.168.1.41	HTTP	294 HTTP/1.1 304 Not Modified

[Next response in frame: 1126]

[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 IF-MODIFIED-SINCE<br>\n

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

\n

</html>\n

You can see the contents of the server response. Yes it explicitly returns the contents because it is the first request and we cleaned the cache before we did the experiment.

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?

820	5.986433	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
897	6.142185	128.119.245.12	192.168.1.41	HTTP	784 HTTP/1.1 200 OK (text/html)
1090	7.249559	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
1126	7.400100	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)
2582	15.918924	192.168.1.41	128.119.245.12	HTTP	662 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2608	16.077342	128.119.245.12	192.168.1.41	HTTP	294 HTTP/1.1 304 Not Modified

  

▼ Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

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/86.0.4240.75 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: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n

If-None-Match: "173-5b2280b74ba7d"\r\n

If-Modified-Since: Wed, 21 Oct 2020 05:59:04 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

If-Modified-Since: Wed, 21 Oct 2020 05:59:04 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.

No.	Time	Source	Destination	Protocol	Length	Info
820	5.986433	192.168.1.41	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
897	6.142185	128.119.245.12	192.168.1.41	HTTP	784	HTTP/1.1 200 OK (text/html)
1090	7.249559	192.168.1.41	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
1126	7.400100	128.119.245.12	192.168.1.41	HTTP	538	HTTP/1.1 404 Not Found (text/html)
2582	15.918924	192.168.1.41	128.119.245.12	HTTP	662	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2608	16.077342	128.119.245.12	192.168.1.41	HTTP	294	HTTP/1.1 304 Not Modified

```

> Frame 2608: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.41
> Transmission Control Protocol, Src Port: 80, Dst Port: 50307, Seq: 1, Ack: 609, 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: Wed, 21 Oct 2020 19:43:16 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Connection: Keep-Alive\r\n

```

We get a HTTP/1.1 304 Not Modified Response.  
No because we get the content of the first response.

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?

No.	Time	Source	Destination	Protocol	Length	Info
1638	12.630419	192.168.1.41	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1728	12.785349	128.119.245.12	192.168.1.41	HTTP	559	HTTP/1.1 200 OK (text/html)
1856	13.160147	192.168.1.41	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
1928	13.306204	128.119.245.12	192.168.1.41	HTTP	538	HTTP/1.1 404 Not Found (text/html)

  

```

> Frame 1638: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxelCom_35:a4:27 (08:26:97:35:a4:27)
> Internet Protocol Version 4, Src: 192.168.1.41, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50406, 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/86.0.4240.75 Safari/537.36\r\n

```

Just one. Packet number is 1638.

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

No.	Time	Source	Destination	Protocol	Length	Info
1638	12.630419	192.168.1.41	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1728	12.785349	128.119.245.12	192.168.1.41	HTTP	559	HTTP/1.1 200 OK (text/html)
1856	13.160147	192.168.1.41	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
1928	13.306204	128.119.245.12	192.168.1.41	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Packet number is 1728.

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

No.	Time	Source	Destination	Protocol	Length	Info
1638	12.630419	192.168.1.41	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1728	12.785349	128.119.245.12	192.168.1.41	HTTP	559	HTTP/1.1 200 OK (text/html)
1856	13.160147	192.168.1.41	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
1928	13.306204	128.119.245.12	192.168.1.41	HTTP	538	HTTP/1.1 404 Not Found (text/html)

HTTP/1.1 200 OK.

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

1638	12.630419	192.168.1.41	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1728	12.785349	128.119.245.12	192.168.1.41	HTTP	559 HTTP/1.1 200 OK (text/html)
1856	13.160147	192.168.1.41	128.119.245.12	HTTP	482 GET /favicon.ico HTTP/1.1
1928	13.306204	128.119.245.12	192.168.1.41	HTTP	538 HTTP/1.1 404 Not Found (text/html)

  

```

> Frame 1728: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.41
> Transmission Control Protocol, Src Port: 80, Dst Port: 50406, Seq: 4357, Ack: 497, Len: 505
v [4 Reassembled TCP Segments (4861 bytes): #1723(1452), #1724(1452), #1727(1452), #1728(505)]
  [Frame: 1723, payload: 0-1451 (1452 bytes)]
  [Frame: 1724, payload: 1452-2903 (1452 bytes)]
  [Frame: 1727, payload: 2904-4355 (1452 bytes)]
  [Frame: 1728, payload: 4356-4860 (505 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057...]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)

```

  

```

> Frame 1728: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: ZyxelCom_35:a4:27 (08:26:97:35:a4:27), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.41
> Transmission Control Protocol, Src Port: 80, Dst Port: 50406, Seq: 4357, Ack: 497, Len: 505
v [4 Reassembled TCP Segments (4861 bytes): #1723(1452), #1724(1452), #1727(1452), #1728(505)]
  [Frame: 1723, payload: 0-1451 (1452 bytes)]
  [Frame: 1724, payload: 1452-2903 (1452 bytes)]
  [Frame: 1727, payload: 2904-4355 (1452 bytes)]
  [Frame: 1728, payload: 4356-4860 (505 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057...]

```

As you can see just above the screen shot, there are 4861 byte and 4 TCP segments.

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

3192	10.758293	192.168.1.34	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
3227	10.905067	128.119.245.12	192.168.1.34	HTTP	1127 HTTP/1.1 200 OK (text/html)
3236	10.948890	192.168.1.34	128.119.245.12	HTTP	482 GET /pearson.png HTTP/1.1
3273	11.095569	128.119.245.12	192.168.1.34	HTTP	761 HTTP/1.1 200 OK (PNG)
3336	11.386861	192.168.1.34	128.119.245.12	HTTP	456 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
3571	11.903827	128.119.245.12	192.168.1.34	HTTP	1184 HTTP/1.1 200 OK (JPEG JFIF image)

There are 3 HTTP GET requests to ip addresses 128.119.245.12 but the file paths are different.



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

3192	10.758293	192.168.1.34	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
3227	10.905067	128.119.245.12	192.168.1.34	HTTP	1127 HTTP/1.1 200 OK (text/html)
3236	10.948890	192.168.1.34	128.119.245.12	HTTP	482 GET /pearson.png HTTP/1.1
3273	11.095569	128.119.245.12	192.168.1.34	HTTP	761 HTTP/1.1 200 OK (PNG)
3336	11.386861	192.168.1.34	128.119.245.12	HTTP	456 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
3571	11.903827	128.119.245.12	192.168.1.34	HTTP	1184 HTTP/1.1 200 OK (JPEG JFIF image)

Based on the above screen shot(in question 16), two images were downloaded **serially**, because when the first request was sent to the server it waited the response and then sent the other get request so we can understand from that two images were downloaded serially.

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

2633	12.229985	172.20.10.2	128.119.245.12	HTTP	566 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2750	12.560185	128.119.245.12	172.20.10.2	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
9948	32.061599	172.20.10.2	128.119.245.12	HTTP	651 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
10011	32.271146	128.119.245.12	172.20.10.2	HTTP	544 HTTP/1.1 200 OK (text/html)

```
> Frame 2750: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
> Ethernet II, Src: d6:a3:3d:8e:b9:64 (d6:a3:3d:8e:b9:64), Dst: IntelCor_d6:b0:37 (48:45:20:d6:b0:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 52140, 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: Thu, 22 Oct 2020 09:25:41 GMT\r\n
    < Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    < WWW-Authenticate: Basic realm="wireshark-students only"\r\n
```

HTTP/1.1 401 Authorization Required was the initial response.

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

2633	12.229985	172.20.10.2	128.119.245.12	HTTP	566 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2750	12.560185	128.119.245.12	172.20.10.2	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
9948	32.061599	172.20.10.2	128.119.245.12	HTTP	651 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
10011	32.271146	128.119.245.12	172.20.10.2	HTTP	544 HTTP/1.1 200 OK (text/html)

  

> Frame 9948: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Device\NPF\_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0

> Ethernet II, Src: IntelCor\_d6:b0:37 (48:45:20:d6:b0:37), Dst: d6:a3:3d:8e:b9:64 (d6:a3:3d:8e:b9:64)

> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 52139, 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: GETRequest URI: /wireshark-labs/protected\_pages/HTTP-wireshark-file5.htmlRequest Version: HTTP/1.1Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nAuthorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzM5ldHdvcms=\r\n

New field is the Authorization field.