

Computer Network

Wireshark Lab 2a: HTTP v8.0

Lecturer: Mr. Nguyễn Mạnh Thìn

Student: Trần Quốc Anh - 1852247

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

- My browser running HTTP version 1.1
- The server is running HTTP version 1.1

No.	Time	Source	Destination	Protocol	Length	Info
61	2020-10-12 09:58:44.807428	191.16.7.88	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
65	2020-10-12 09:58:45.054559	128.119.245.12	191.16.7.88	HTTP	540	HTTP/1.1 200 OK (text/html)

> Frame 65: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{E2397F76-8016-46FA-AC39-760CEF8B7FE3}, id 0

> Ethernet II, Src: DrayTek_12:5a:18 (00:1d:aa:12:5a:18), Dst: HonHaiPr_2d:67:d1 (90:32:4b:2d:67:d1)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 191.16.7.88

> Transmission Control Protocol, Src Port: 80, Dst Port: 49574, Seq: 1, Ack: 485, Len: 486

▼ Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Mon, 12 Oct 2020 02:58:44 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sun, 11 Oct 2020 05:59:01 GMT\r\n

ETag: "80-5b15ee0e0d985"\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

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.247131000 seconds]

[\[Request in frame: 61\]](#)

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

- The language my browser indicates that it can accept to the server is: Vietnamese - VN

> Frame 73: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{E9168059-8D70-4814-8387-17E00F2E7DF0}, id 0

> Ethernet II, Src: Dell_78:00:40 (00:26:b9:78:00:40), Dst: DASANNet_ce:49:d7 (9c:65:ee:ce:49:d7)

> Internet Protocol Version 4, Src: 192.168.1.30, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 51012, Dst Port: 80, Seq: 1, Ack: 1, Len: 506

▼ 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/84.0.4147.89 Safari/537.36\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: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n

\r\n

[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\]](#)

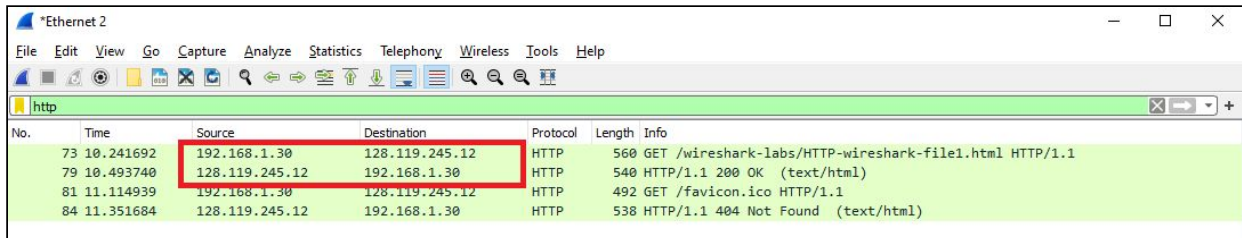
[HTTP request 1/2]

[\[Response in frame: 79\]](#)

[\[Next request in frame: 81\]](#)

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

- IP address of my computer: 192.168.1.30
- IP address of gaia.cs.umass.edu server: 128.119.245.12

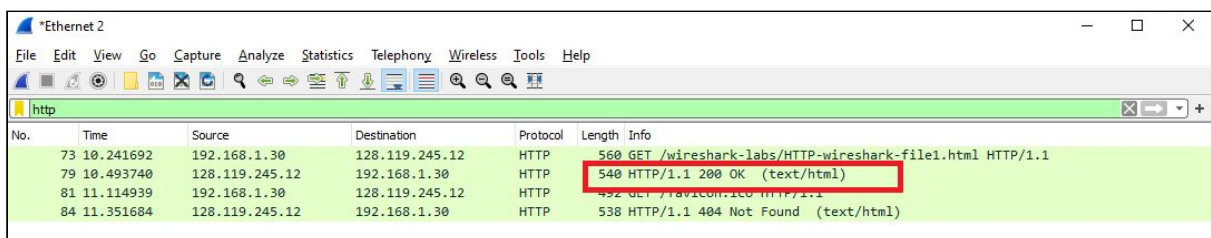


The screenshot shows a Wireshark packet capture on the 'http' filter. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
73	10.241692	192.168.1.30	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
79	10.493740	128.119.245.12	192.168.1.30	HTTP	540	HTTP/1.1 200 OK (text/html)
81	11.114939	192.168.1.30	128.119.245.12	HTTP	492	GET /favicon.ico HTTP/1.1
84	11.351684	128.119.245.12	192.168.1.30	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

- The status code is "200 OK"

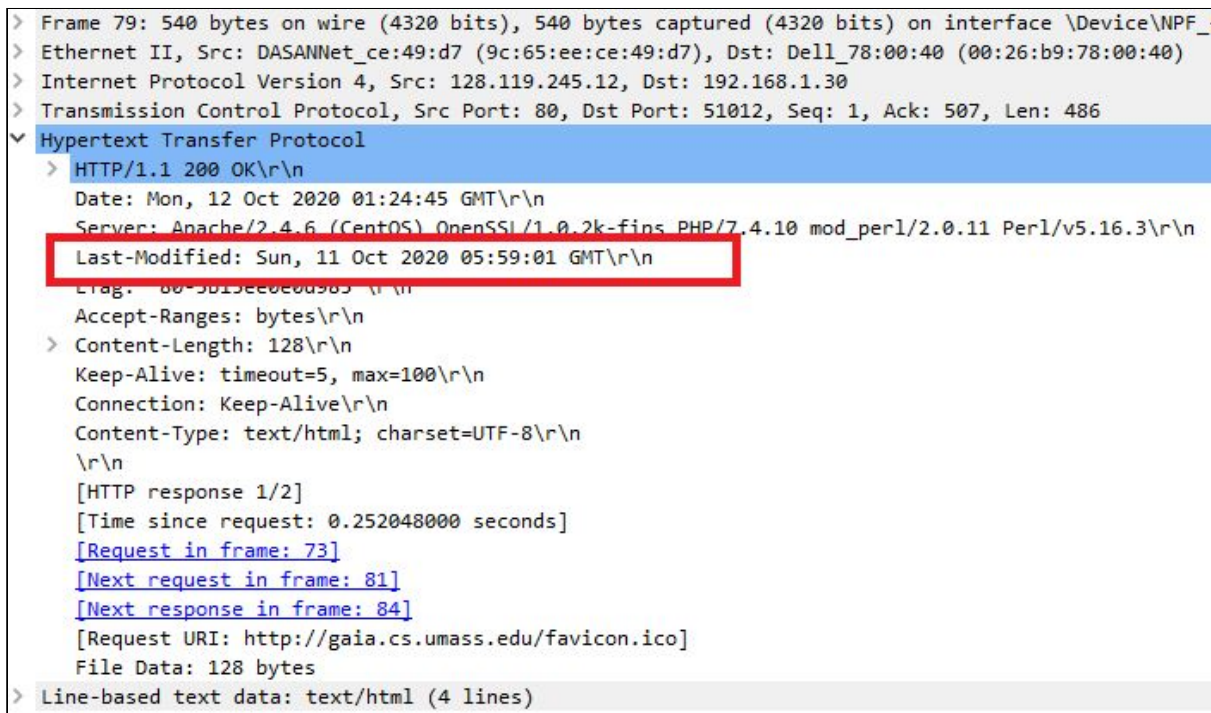


The screenshot shows the same Wireshark packet capture, but with the packet details pane expanded for packet 79. The details show:

- HTTP/1.1 200 OK (text/html)

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

- The HTML was last modified at the server on Sunday, 11 October 2020, 05:59:01 GMT



The screenshot shows the packet details pane for packet 79, expanded to show the 'Hypertext Transfer Protocol' section. The details are as follows:

- HTTP/1.1 200 OK\r\n
- Date: Mon, 12 Oct 2020 01:24:45 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
- Last-Modified: Sun, 11 Oct 2020 05:59:01 GMT\r\n
- ETag: 80-5b19ee0e0d905\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
- Content-Type: text/html; charset=UTF-8\r\n
- \r\n
- [HTTP response 1/2]
- [Time since request: 0.252048000 seconds]
- [Request in frame: 73]
- [Next request in frame: 81]
- [Next response in frame: 84]
- [Request URI: http://gaia.cs.umass.edu/favicon.ico]
- File Data: 128 bytes

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

- 128 bytes of content are being returned to my browser

```

> Frame 79: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_
> Ethernet II, Src: DASANNet_ce:49:d7 (9c:65:ee:ce:49:d7), Dst: Dell_78:00:40 (00:26:b9:78:00:40)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.30
> Transmission Control Protocol, Src Port: 80, Dst Port: 51012, Seq: 1, Ack: 507, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 12 Oct 2020 01:24:45 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 11 Oct 2020 05:59:01 GMT\r\n
    ETag: "80-5b15ee0e0d985"\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
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.252048000 seconds]
    [Request in frame: 73]
    [Next request in frame: 81]
    [Next response in frame: 84]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 128 bytes
  > Line-based text data: text/html (4 lines)

```

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.
 - There is no different headings between the two windows
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?
 - There is no “IF-MODIFIED-SINCE” line in the HTTP GET message.
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
 - The server did explicitly return the contents of the file


```
Etag: "173-5b15ee0e0d1b5"\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 1/3]
[Time since request: 0.236343000 seconds]
[Request in frame: 154]
[Next request in frame: 172]
[Next response in frame: 176]
[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)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
</html>\r\n
```

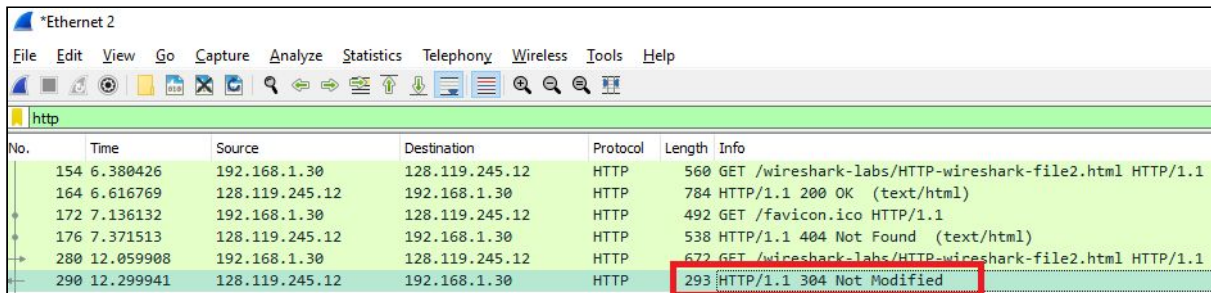
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

- There is an “IF-MODIFIED-SINCE:” line in the HTTP GET. The information follows is the date and time that I last accessed the webpage.

```
> Frame 280: 672 bytes on wire (5376 bits), 672 bytes captured (5376 bits) on interface \Device\NPF...
> Ethernet II, Src: Dell_78:00:40 (00:26:b9:78:00:40), Dst: DASANNet_ce:49:d7 (9c:65:ee:ce:49:d7)
> Internet Protocol Version 4, Src: 192.168.1.30, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51247, Dst Port: 80, Seq: 945, Ack: 1215, Len: 618
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) C...
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8...
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en,vi-VN;q=0.9,vi;q=0.8,fr-FR;q=0.7,fr;q=0.6,en-US;q=0.5\r\n
If-None-Match: "173-5b15ee0e0d1b5"\r\n
If-Modified-Since: Sun, 11 Oct 2020 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 3/3]
[Prev request in frame: 172]
[Response in frame: 290]
```

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.

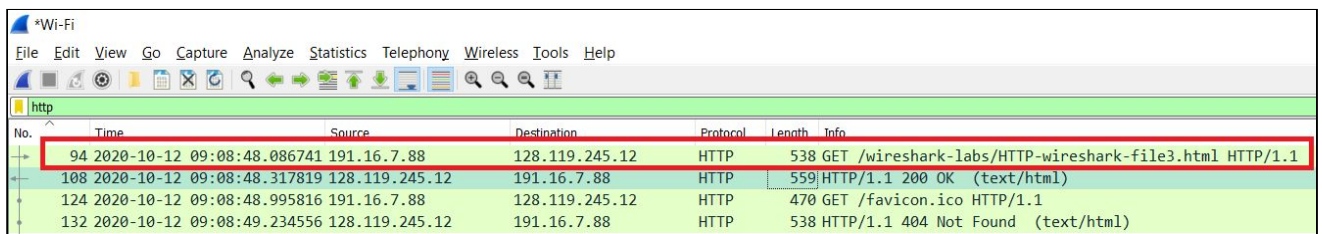
- The HTTP status code and phrase is “304 Not Modified”
- The server did not explicitly return the contents of the file because the browser retrieved the contents from its cache. If the file had been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.



No.	Time	Source	Destination	Protocol	Length	Info
154	6.380426	192.168.1.30	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
164	6.616769	128.119.245.12	192.168.1.30	HTTP	784	HTTP/1.1 200 OK (text/html)
172	7.136132	192.168.1.30	128.119.245.12	HTTP	492	GET /favicon.ico HTTP/1.1
176	7.371513	128.119.245.12	192.168.1.30	HTTP	538	HTTP/1.1 404 Not Found (text/html)
280	12.059908	192.168.1.30	128.119.245.12	HTTP	672	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
290	12.299941	128.119.245.12	192.168.1.30	HTTP	293	HTTP/1.1 304 Not Modified

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?

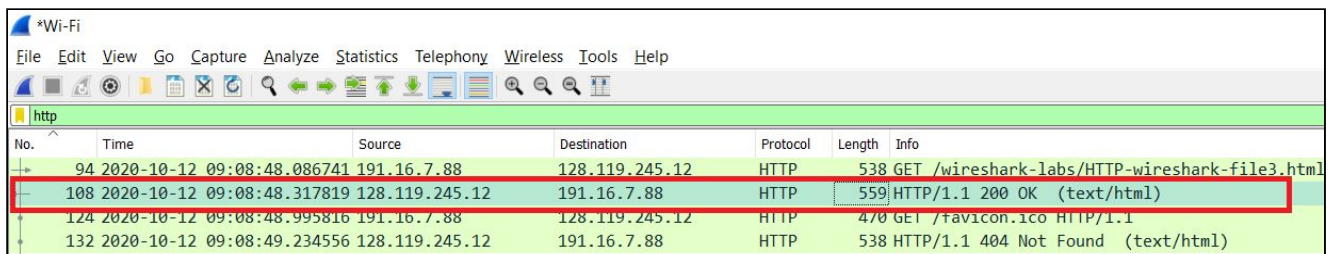
- My browser sends 1 HTTP GET request messages. Packet number in the trace contains the GET message is 94



No.	Time	Source	Destination	Protocol	Length	Info
94	2020-10-12 09:08:48.086741	191.16.7.88	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
108	2020-10-12 09:08:48.317819	128.119.245.12	191.16.7.88	HTTP	559	HTTP/1.1 200 OK (text/html)
124	2020-10-12 09:08:48.995816	191.16.7.88	128.119.245.12	HTTP	470	GET /favicon.ico HTTP/1.1
132	2020-10-12 09:08:49.234556	128.119.245.12	191.16.7.88	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

- Packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request is 108



No.	Time	Source	Destination	Protocol	Length	Info
94	2020-10-12 09:08:48.086741	191.16.7.88	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
108	2020-10-12 09:08:48.317819	128.119.245.12	191.16.7.88	HTTP	559	HTTP/1.1 200 OK (text/html)
124	2020-10-12 09:08:48.995816	191.16.7.88	128.119.245.12	HTTP	470	GET /favicon.ico HTTP/1.1
132	2020-10-12 09:08:49.234556	128.119.245.12	191.16.7.88	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

- The status code and phrase is “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?

- 3 data-containing TCP segments were needed.

```
> Frame 108: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{E...}
> Ethernet II, Src: DrayTek_12:5a:18 (00:1d:aa:12:5a:18), Dst: HonHaiPr_2d:67:d1 (90:32:4b:2d:67:d1)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 191.16.7.88
> Transmission Control Protocol, Src Port: 80, Dst Port: 65183, Seq: 4357, Ack: 485, Len: 505
> [3 Reassembled TCP Segments (4861 bytes): #106(1452), #107(2904), #108(505)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

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

- My browser sent 3 HTTP GET request messages.
- Page address: 128.119.245.12
- Pearson logo: 128.119.245.12
- Book cover: 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
197	2020-10-12 09:26:17.834387	191.16.7.88	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
211	2020-10-12 09:26:18.075776	128.119.245.12	191.16.7.88	HTTP	1127	HTTP/1.1 200 OK (text/html)
212	2020-10-12 09:26:18.109622	191.16.7.88	128.119.245.12	HTTP	470	GET /pearson.png HTTP/1.1
239	2020-10-12 09:26:18.353817	128.119.245.12	191.16.7.88	HTTP	761	HTTP/1.1 200 OK (PNG)
261	2020-10-12 09:26:18.611372	191.16.7.88	128.119.245.12	HTTP	444	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
340	2020-10-12 09:26:19.325931	128.119.245.12	191.16.7.88	HTTP	1184	HTTP/1.1 200 OK (JPEG JFIF image)

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

- The browser downloaded the two images serially. Because the first image was requested and sent before the second image was requested by the browser. If they were downloaded in parallel the time period would be the same.

No.	Time	Source	Destination	Protocol	Length	Info
197	2020-10-12 09:26:17.834387	191.16.7.88	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
211	2020-10-12 09:26:18.075776	128.119.245.12	191.16.7.88	HTTP	1127	HTTP/1.1 200 OK (text/html)
212	2020-10-12 09:26:18.109622	191.16.7.88	128.119.245.12	HTTP	470	GET /pearson.png HTTP/1.1
239	2020-10-12 09:26:18.353817	128.119.245.12	191.16.7.88	HTTP	761	HTTP/1.1 200 OK (PNG)
261	2020-10-12 09:26:18.611372	191.16.7.88	128.119.245.12	HTTP	444	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
340	2020-10-12 09:26:19.325931	128.119.245.12	191.16.7.88	HTTP	1184	HTTP/1.1 200 OK (JPEG JFIF image)

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

- The servers initial response was "401 Unauthorized"

No.	Time	Source	Destination	Protocol	Length	Info
391	2020-10-12 09:52:12.324593	191.16.7.88	128.119.245.12	HTTP	549	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
400	2020-10-12 09:52:12.576546	128.119.245.12	191.16.7.88	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

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 field included in the HTTP GET message is “Authorization”, which was included because we sent username and password with our request.

```
> Frame 7095: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface \Device\NPF_{E2397F76-8016-46FA-AC39-760CEF8B7FE3}, id 0
> Ethernet II, Src: HonHaiPr_2d:67:d1 (90:32:4b:2d:67:d1), Dst: DrayTek_12:5a:18 (00:1d:aa:12:5a:18)
> Internet Protocol Version 4, Src: 191.16.7.88, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49535, Dst Port: 80, Seq: 1, Ack: 1, Len: 580
√ Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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
    > Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\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 Edg/86.0.622.38\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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
    [HTTP request 1/1]
    [Response in frame: 7106]
```