

WireShark Lab - 1

BSSE 1204

http						
No.	Time	Source	Destination	Protocol	Length	Info
111	17:00:07.089749	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
121	17:00:07.405436	128.119.245.12	192.168.1.7	HTTP	540	HTTP/1.1 200 OK (text/html)
123	17:00:07.498210	192.168.1.7	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
128	17:00:07.818230	128.119.245.12	192.168.1.7	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 111: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAE0C0E0}, id 0
> Ethernet II, Src: ASUSTekC_b5:bb:21 (38:d5:47:b5:bb:21), Dst: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49779, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
▼ 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
 [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 [Severity Level: Chat]
 [Group: Sequence]
 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/98.0.4758.81 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: 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: 121]
 [Next request in frame: 123]

http						
No.	Time	Source	Destination	Protocol	Length	Info
111	17:00:07.089749	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
121	17:00:07.405436	128.119.245.12	192.168.1.7	HTTP	540	HTTP/1.1 200 OK (text/html)
123	17:00:07.498210	192.168.1.7	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
128	17:00:07.818230	128.119.245.12	192.168.1.7	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 121: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAE0C0E0}, id 0
> Ethernet II, Src: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed), Dst: ASUSTekC_b5:bb:21 (38:d5:47:b5:bb:21)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 49779, Seq: 1, Ack: 476, Len: 486
▼ Hypertext Transfer Protocol
 ▼ HTTP/1.1 200 OK\r\n
 ▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n
 [HTTP/1.1 200 OK\r\n
 [Severity Level: Chat]
 [Group: Sequence]
 Response Version: HTTP/1.1
 Status Code: 200
 [Status Code Description: OK]
 Response Phrase: OK
 Date: Fri, 04 Feb 2022 11:00:06 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
 Last-Modified: Fri, 04 Feb 2022 06:59:01 GMT\r\n
 ETag: "80-5d72bc92051cf"\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: 0.315687000 seconds]
 [Request in frame: 111]
 [Next request in frame: 123]
 [Next response in frame: 128]
 [Request URI: http://gaia.cs.umass.edu/favicon.ico]
 File Data: 128 bytes
 Line-based text data: text/html (4 lines)

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

Ans: My browser is running HTTP version 1.1. Also the HTTP version of running server is HTTP 1.1

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

Ans: en-US,en; It can accept English (US) to the server.

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

Ans: IP of my computer is 192.168.1.7 and the Ip of gaia.cs.umass.edu server is 128.119.245.12

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

Ans: 200

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

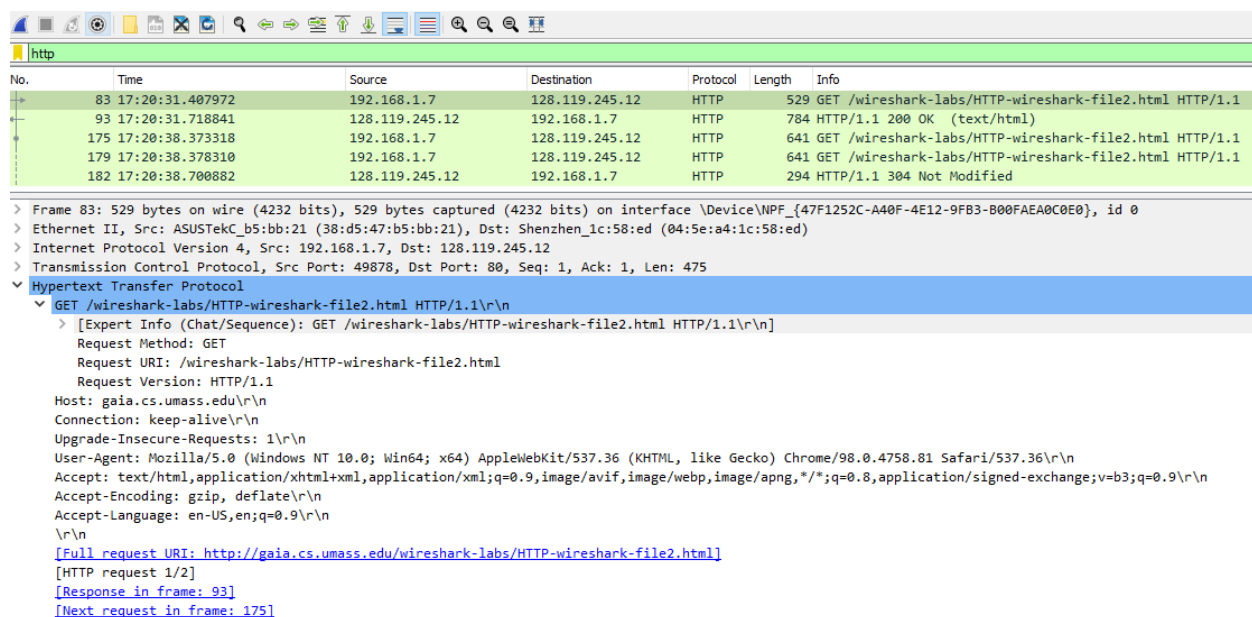
Ans: Fri, 04 Feb 2022 06:59:01 GMT

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

Ans: 128 bytes

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: No. All of the headers can be found in the raw data.



No.	Time	Source	Destination	Protocol	Length	Info
83	17:20:31.407972	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
93	17:20:31.718841	128.119.245.12	192.168.1.7	HTTP	784	HTTP/1.1 200 OK (text/html)
175	17:20:38.373318	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
179	17:20:38.378310	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
182	17:20:38.700882	128.119.245.12	192.168.1.7	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 83: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAEA0C0E0}, id 0
> Ethernet II, Src: ASUSTekC_b5:bb:21 (38:d5:47:b5:bb:21), Dst: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49878, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
▼ 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/98.0.4758.81 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: en-US,en;q=0.9\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: 93]
 [Next request in frame: 175]

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: No, there is no header named “IF-MODIFIED-SINCE” in the **first** HTTP GET request.

http						
No.	Time	Source	Destination	Protocol	Length	Info
83	17:20:31.407972	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
93	17:20:31.718841	128.119.245.12	192.168.1.7	HTTP	784	HTTP/1.1 200 OK (text/html)
175	17:20:38.373318	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
179	17:20:38.378310	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
182	17:20:38.700882	128.119.245.12	192.168.1.7	HTTP	294	HTTP/1.1 304 Not Modified

Response Phrase: OK
Date: Fri, 04 Feb 2022 11:20:31 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 04 Feb 2022 06:59:01 GMT\r\n
ETag: "173-5d72bc92049ff"\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 1/2]
[Time since request: 0.310869000 seconds]
[Request in frame: 83]
[Next request in frame: 175]
[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\nCongratulations again! Now you've downloaded the file lab2-2.html. <br>\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy <br>\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\nfield in your browser's HTTP GET request to the server.\n\n</html>
```

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

Ans: Yes, I can see the contents of the file under the “Line-based text data: text/html (10 lines)”.

http						
No.	Time	Source	Destination	Protocol	Length	Info
83	17:20:31.407972	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
93	17:20:31.718841	128.119.245.12	192.168.1.7	HTTP	784	HTTP/1.1 200 OK (text/html)
175	17:20:38.373318	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
179	17:20:38.378310	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
182	17:20:38.700882	128.119.245.12	192.168.1.7	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 175: 641 bytes on wire (5128 bits), 641 bytes captured (5128 bits) on interface Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAE0C0E0}, id 0
> Ethernet II, Src: ASUSTek_b5:bb:21 (38:d5:47:b5:bb:21), Dst: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49878, Dst Port: 80, Seq: 476, Ack: 731, Len: 587

> 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/98.0.4758.81 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: en-US,en;q=0.9\r\n
If-None-Match: "173-5d72bc92049ff"\r\n
If-Modified-Since: Fri, 04 Feb 2022 06:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]
[Prev request in frame: 83]

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. **If-Modified-Since: Fri, 04 Feb 2022 06:59:01 GMT**. This header is followed by **\r\n**

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows five packets. Packet 182 is selected, showing an HTTP 304 Not Modified response. The packet details pane on the right shows the structure of the response, including the status code 304 and the phrase 'Not Modified'. The raw data pane at the bottom shows the full HTTP response, including the status line 'HTTP/1.1 304 Not Modified' and the 'If-Modified-Since' header.

No.	Time	Source	Destination	Protocol	Length	Info
83	17:20:31.407972	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
93	17:20:31.718841	128.119.245.12	192.168.1.7	HTTP	784	HTTP/1.1 200 OK (text/html)
175	17:20:38.378318	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
179	17:20:38.378310	192.168.1.7	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
182	17:20:38.700882	128.119.245.12	192.168.1.7	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 182: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAE0C0E0}, id 0
> Ethernet II, Src: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed), Dst: ASUSTekC_b5:bb:21 (38:d5:47:b5:bb:21)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 49879, Seq: 1, Ack: 588, 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, 04 Feb 2022 11:20:38 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 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: "173-5d72bc92049ff"\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.322572000 seconds]
 [Request in frame: 179]
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

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: Status code = **304**. No, the server **doesn't** explicitly return the contents of the file as the file content is not modief.

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows five packets. Packet 142 is selected, showing an HTTP 200 OK response. The packet details pane on the right shows the structure of the response, including the status code 200 and the phrase 'OK'. The raw data pane at the bottom shows the full HTTP response, including the status line 'HTTP/1.1 200 OK' and the 'Content-Type' header.

No.	Time	Source	Destination	Protocol	Length	Info
142	18:55:25.230251	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
167	18:55:25.537216	128.119.245.12	192.168.1.7	HTTP	595	HTTP/1.1 200 OK (text/html)
170	18:55:25.668091	192.168.1.7	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
176	18:55:25.974302	128.119.245.12	192.168.1.7	HTTP	538	HTTP/1.1 404 Not Found (text/html)

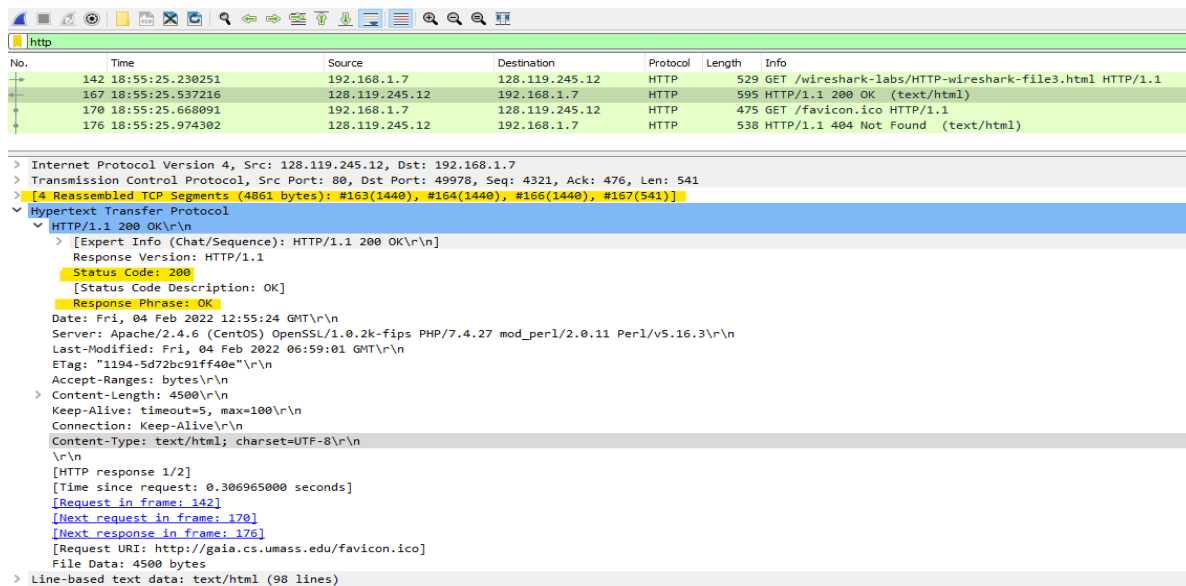
> Frame 142: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAE0C0E0}, id 0
> Ethernet II, Src: ASUSTekC_b5:bb:21 (38:d5:47:b5:bb:21), Dst: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49978, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
▼ Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file3.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/98.0.4758.81 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: en-US,en;q=0.9\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
 [HTTP request 1/2]

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: Two HTTP GET requests were sent from my browser to the server. Packet no 167 contains the GET message for the Bill or Rights.

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

Ans: Packet no 167 contains the status code and phrase associated with the response to the HTTP GET request.



No.	Time	Source	Destination	Protocol	Length	Info
142	18:55:25.230251	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
167	18:55:25.537216	128.119.245.12	192.168.1.7	HTTP	595	HTTP/1.1 200 OK (text/html)
170	18:55:25.668091	192.168.1.7	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
176	18:55:25.974302	128.119.245.12	192.168.1.7	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
Transmission Control Protocol, Src Port: 80, Dst Port: 49978, Seq: 4321, Ack: 476, Len: 541
4 Reassembled TCP Segments (4861 bytes): #163(1440), #164(1440), #166(1440), #167(541)
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: Fri, 04 Feb 2022 12:55:24 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 04 Feb 2022 06:59:01 GMT\r\n
ETag: "1194-5d72bc91ff40e"\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 1/2]
[Time since request: 0.306965000 seconds]
[Request in frame: 142]
[Next request in frame: 170]
[Next response in frame: 176]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 4500 bytes
Line-based text data: text/html (98 lines)

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

Ans: Status code = 200 and phrase in the response is 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: 4 TCP segments were needed to carry the single HTTP response.

No.	Time	Source	Destination	Protocol	Length	Info
46	19:26:28.126798	192.168.1.7	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
53	19:26:28.436615	128.119.245.12	192.168.1.7	HTTP	1355	HTTP/1.1 200 OK (text/html)
55	19:26:28.501933	192.168.1.7	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
64	19:26:28.810542	128.119.245.12	192.168.1.7	HTTP	785	HTTP/1.1 200 OK (PNG)
71	19:26:29.364417	192.168.1.7	178.79.137.164	HTTP	442	GET /8e_cover_small.jpg HTTP/1.1
77	19:26:29.648870	178.79.137.164	192.168.1.7	HTTP	225	HTTP/1.1 301 Moved Permanently
788	19:26:34.315376	192.168.1.7	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
793	19:26:34.320316	192.168.1.7	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
796	19:26:34.632583	128.119.245.12	192.168.1.7	HTTP	539	HTTP/1.1 404 Not Found (text/html)
897	19:26:48.489869	192.168.1.7	8.241.167.126	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?ae3a121f8222edac HTTP/1.1
898	19:26:48.540311	8.241.167.126	192.168.1.7	HTTP	404	HTTP/1.1 304 Not Modified


```

> Frame 55: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface \Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAEAB0C0E}, id 0
> Ethernet II, Src: ASUSTekC_b5:bb:21 (38:d5:47:b5:bb:21), Dst: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49798, Dst Port: 80, Seq: 476, Ack: 1302, Len: 421
> Hypertext Transfer Protocol
  > GET /pearson.png HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.81 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\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/pearson.png]
    [HTTP request 2/3]
    [Prev request in frame: 46]
    [Response in frame: 64]
    [Next request in frame: 788]

```

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

Ans: 6 GET requests messages were sent. The IP Addresses are: 128.119.245.12 178.79.137.164, 8.241.167.126

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: This can be answered by examining the TCP port on which these two images were transmitted. If the TCP ports are different, then these images were downloaded serially otherwise parallelly. We have observed that the two images were transported into two different TCP ports. Therefore, it denotes different ports and thus the images were downloaded **serially**.

No.	Time	Source	Destination	Protocol	Length	Info
8	21:19:46.580877	192.168.1.7	128.119.245.12	HTTP	571	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
12	21:19:46.868794	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
125	21:19:56.348386	192.168.1.7	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
129	21:19:56.351646	192.168.1.7	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
134	21:19:56.637886	128.119.245.12	192.168.1.7	HTTP	544	HTTP/1.1 200 OK (text/html)


```

> Frame 129: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface \Device\NPF_{47F1252C-A40F-4E12-9FB3-B00FAEAB0C0E}, id 0
> Ethernet II, Src: ASUSTekC_b5:bb:21 (38:d5:47:b5:bb:21), Dst: Shenzhen_1c:58:ed (04:5e:a4:1c:58:ed)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50177, Dst Port: 80, Seq: 1, Ack: 1, Len: 576
> Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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 d2lyZXNoYXJrLXNldm91bnR1bWZ0eS1ldHdvcm91\r\n
    Credentials: wireshark-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/98.0.4758.81 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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 134]

```

18. What is the server's response (status code and phrase) in response to the initial

HTTP GET message from your browser?

Ans: Status code = 401 and response was Unauthorized.

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

Ans: Authorization Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5="