

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running? (5 Points)

① My browser is running HTTP 1.1

No.	Time	Source	Destination	Protocol	Length Info
8.433274		10.110.23.232	128.119.245.12	HTTP	566 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8.456067		128.119.245.12	10.110.23.232	HTTP	540 HTTP/1.1 200 OK (text/html)
8.517959					
8.537329					

I have read and understood the course academic integrity policy

Torfan Liu

② Server is running HTTP 1.1

No.	Time	Source	Destination	Protocol	Length Info
8.433274		10.110.23.232	128.119.245.12	HTTP	566 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8.456067		128.119.245.12	10.110.23.232	HTTP	540 HTTP/1.1 200 OK (text/html)
8.517					
8.537					

2. What languages (if any) does your browser indicate that it can accept to the server? (5 Points)

WLAN		File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
http												
<b>Request URI: /wireshark-labs/HTTP-wireshark-file1.html</b>												
<b>Request Version: HTTP/1.1</b>												
<b>Host: gaia.cs.umass.edu</b>												
<b>Connection: keep-alive</b>												
<b>Upgrade-Insecure-Requests: 1</b>												
<b>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1</b>												
<b>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,appla</b>												
<b>Accept-Encoding: gzip, deflate</b>												
<b>Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.6,en;q=0.4</b>												
<b>[Full request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]</b>												

① zh-CN, ch ← Chinese

② en ← English

③ en-GB ← British English

④ en-US ← American English

3. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server? (5 Points)

No.	Time	Source	Destination	Protocol	Length Info
8.433274		10.110.23.232	128.119.245.12	HTTP	566 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8.456067		128.119.245.12	10.110.23.232	HTTP	540 HTTP/1.1 200 OK (text/html)

IP address of my computer : 10.110.23.232

IP address of server : 128.119.245.12

4. What is the status code returned from the server to your browser? (5 Points)

```
> Ethernet II, Src: JuniperN_02:17:f0 (00:21:59:02:17:f0), Dst: IntelCor_5c:47:9d (60:f2:62:5c:47:9d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.110.23.232
> Transmission Control Protocol, Src Port: 80, Dst Port: 51509, Seq: 1, Ack: 513, 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: Thu, 28 Sep 2023 21:01:26 GMT\r\n
```

Status code: 200

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

```
Response Phrase: OK
Date: Thu, 28 Sep 2023 21:01:26 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
Last-Modified: Thu, 28 Sep 2023 05:59:01 GMT\r\n
ETag: "80-606650133f6bc"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
```

Last modified      Thu 09/28/2023 05:59:01 CMT

6. How many bytes of content are being returned to your browser? (5 Points)

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5 max=100
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. (5 Points)

0000	60 f2 62 5c 47 9d 00 21	59 02 17 f0 08 00 45 00	^ b\G..! Y.....E..
0010	02 0e 89 bb 40 00 2e 06	29 55 80 77 f5 0c 0a 6e	....@... )U.w....n
0020	17 e8 00 50 d7 40 9e a1	75 dc 2d e3 de 17 50 18	...P@... u....P..
0030	00 ed 7b 63 00 00 48 54	54 50 2f 31 2e 31 20 32	..{c...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 54 68 75	00 OK [D ate: Thu
0050	2c 20 32 38 20 53 65 70	20 32 30 32 33 20 32 32	, 28 Sep 2023 22
0060	3a 32 36 3a 32 30 20 47	4d 54 0d 0a 53 65 72 76	:26:20 G MT..Serv
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 34 2e 36	er: Apac he/2.4.6
0080	20 28 43 65 6e 74 4f 53	29 20 4f 70 65 6e 53 53	(CentOS ) OpensS
0090	4c 2f 31 2e 30 2e 32 6b	2d 66 69 70 73 20 50 48	L/1.0.2k -fips PH
00a0	50 2f 37 2e 34 2e 33 33	20 6d 6f 64 5f 70 65 72	P/7.4.33 mod_per
00b0	6c 2f 32 2e 30 2e 31 31	20 50 65 72 6c 2f 76 35	l/2.0.11 Perl/v5
00c0	2e 31 36 2e 33 0d 0a 4c	61 73 74 2d 4d 6f 64 69	.16.3..L ast-Modi
00d0	66 69 65 64 3a 20 54 68	75 2c 20 32 38 20 53 65	fied: Th u, 28 Se
00e0	70 20 32 30 32 33 20 30	35 3a 35 39 3a 30 31 20	p 2023 0 5:59:01 ]

every thing for side by  
Asciil are list in the  
header, but none of them  
display in 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? (5 Points)

No

```
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
\r\n
```

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? (5 Points)

Yes, here show the content in HTML

The screenshot shows a Wireshark capture with two main entries. The first entry is a GET request from 10.110.23.232 to 128.119.245.12. The second entry is a response from 128.119.245.12 to 10.110.23.232. The response payload is displayed in the "Text" pane and includes the following HTML content:

```
<html>


Congratulations again! Now you've downloaded the file lab2-2.html. <br>
This file's last modification date will not change. <p>
Thus if you download this multiple times on your browser, a complete copy <br>
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
field in your browser's HTTP GET request to the server.<br>


</html>
```

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<sup>2</sup>? If so, what information follows the “IF-MODIFIED-SINCE:” header? (5 Points)

Yes, The following information is date and time.

The screenshot shows a Wireshark capture with several entries. The fifth entry is a GET request from 10.110.23.232 to 128.119.245.12. The details pane for this packet shows the following headers:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
If-None-Match: "173-606650133eeec"\r\n
If-Modified-Since: Thu, 28 Sep 2023 05:59:01 GMT\r\n
\r\n
```

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. (5 Points)

Status code and phrase : 304 Not Modified.

No contents return

Wireshark - Packet 235 · WLAN

Frame 235: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF\_{14B1}^  
Ethernet II, Src: Juniper\_N\_02:17:f0 (00:21:59:02:17:f0), Dst: IntelCor\_5c:47:9d (60:f2:62:5c:47:9d)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.110.23.232  
Transmission Control Protocol, Src Port: 80, Dst Port: 55947, 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

Wireshark - Packet 235 · WLAN

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\nConnection: Keep-Alive\r\nKeep-Alive: timeout=5, max=100\r\nETag: "173-606650133eeec"\r\n\r\n[HTTP response 1/9]  
[Time since request: 0.020333000 seconds]  
[Request in frame: 231]  
[Next request in frame: 253]  
[Next response in frame: 254]  
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

I think it is because of the contents is already save in local cache. And when header containing "IF-MODIFIED-SINCE:" when client sent request in the second time. Also server check the contents is indeed not changed then, server just reply "Not Modified" in header instead of send back whole contents. It probably design for save internet resource.

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? (5 Points)

① only one HTTP GET

② packet number 23

Time	Source IP	Destination IP	Protocol	Description
22.2.106082	10.110.23.232	128.119.245.12	TCP	54 00/35 → 80 [ACK] Seq=1 ACK=1 Win=131328 Len=0
23 2.106218	10.110.23.232	128.119.245.12	HTTP	552 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
24 2.122001	128.119.245.12	10.110.23.232	TCP	56 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=0
25 2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
26 2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
27 2.124871	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=2921 Win=131328 Len=0
28 2.125050	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=2921 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
29 2.125050	128.119.245.12	10.110.23.232	HTTP	535 HTTP/1.1 200 OK (text/html)
30 2.125131	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=4862 Win=131328 Len=0
31 2.133054	142.250.65.174	10.110.23.232	TLSv1.2	121 Application Data

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? (5 Points)

number 29

Time	Source IP	Destination IP	Protocol	Description
22.2.106082	10.110.23.232	128.119.245.12	TCP	54 00/35 → 80 [ACK] Seq=1 ACK=1 Win=131328 Len=0
23 2.106218	10.110.23.232	128.119.245.12	HTTP	552 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
24 2.122001	128.119.245.12	10.110.23.232	TCP	56 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=0
25 2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
26 2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
27 2.124871	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=2921 Win=131328 Len=0
28 2.125050	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=2921 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
29 2.125050	128.119.245.12	10.110.23.232	HTTP	535 HTTP/1.1 200 OK (text/html)
30 2.125131	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=4862 Win=131328 Len=0
31 2.133054	142.250.65.174	10.110.23.232	TLSv1.2	121 Application Data

14. What is the status code and phrase in the response? (5 Points)

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? (5 Points)

There are three TCP segments carry text of Bill of Rights

Time	Source IP	Destination IP	Protocol	Description
22.2.106082	10.110.23.232	128.119.245.12	TCP	54 00/35 → 80 [ACK] Seq=1 ACK=1 Win=131328 Len=0
23 2.106218	10.110.23.232	128.119.245.12	HTTP	552 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
24 2.122001	128.119.245.12	10.110.23.232	TCP	56 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=0
25 2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
26 2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
27 2.124871	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=2921 Win=131328 Len=0
28 2.125050	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=2921 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
29 2.125050	128.119.245.12	10.110.23.232	HTTP	535 HTTP/1.1 200 OK (text/html)
30 2.125131	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=4862 Win=131328 Len=0
31 2.133054	142.250.65.174	10.110.23.232	TLSv1.2	121 Application Data

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent? (5 Points)

3 HTTP GET request

No.	Time	Source	Destination	Protocol	Length	Info
630	3.192628	10.110.23.232	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html
640	3.211569	128.119.245.12	10.110.23.232	HTTP	1355	HTTP/1.1 200 OK (text/html)
684	3.383861	10.110.23.232	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
693	3.402328	128.119.245.12	10.110.23.232	HTTP	745	HTTP/1.1 200 OK (PNG)
697	3.457309	10.110.23.232	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
699	3.526943	178.79.137.164	10.110.23.232	HTTP	225	HTTP/1.1 301 Moved Permanently

for the first two request, 128.119.245.12

for the cover image, 178.79.137.164

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain. (10 Points)

626 3.192066	128.119.245.12	10.110.23.232	TCP	66 80 → 62790 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128		
628 3.192220	10.110.23.232	128.119.245.12	TCP	54 62790 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0		
630 3.192628	10.110.23.232	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1		
631 3.193340	128.119.245.12	10.110.23.232	TCP	66 80 → 62791 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128		
632 3.193396	10.110.23.232	128.119.245.12	TCP	54 62791 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0		
634 3.2086	142.13.140.120	10.110.23.232	TCP	12 62791 → 62790 [ACK] Seq=1 Ack=1 Win=131328 Len=0		
635 3.209164	128.119.245.12	10.110.23.232	TCP	56 80 → 62790 [ACK] Seq=1 Ack=473 Win=30336 Len=0		
640 3.211569	128.119.245.12	10.110.23.232	HTTP	1355 HTTP/1.1 200 OK (text/html)		
647 3.254993	10.110.23.232	128.119.245.12	TCP	54 62790 → 80 [ACK] Seq=473 Ack=1302 Win=130048 Len=0		
648 3.27510	10.110.23.232	142.251.40.138	TCP	54 62790 → 403 [ACK] Seq=1302 Ack=1302 Win=130048 Len=0		
688 3.388183	155.33.2.2	10.110.23.232	DNS	156 Standard query response 0xb993 HTTP...		
689 3.388757	10.110.23.232	178.79.137.164	TCP	66 62794 → 80 [SYN] Seq=0 Win=64240 Len=...		
690 3.400798	128.119.245.12	10.110.23.232	TCP	1514 80 → 62790 [ACK] Seq=1302 Ack=891 W...		
691 3.400798	128.119.245.12	10.110.23.232	TCP	1514 80 → 62790 [ACK] Seq=2762 Ack=891 W...		
692 3.400887	10.110.23.232	128.119.245.12	TCP	54 62790 → 80 [ACK] Seq=891 Ack=4222 W...		
693 3.402328	128.119.245.12	10.110.23.232	HTTP	745 HTTP/1.1 200 OK (PNG)		
694 3.444598	10.110.23.232	128.119.245.12	TCP	54 62790 → 80 [ACK] Seq=891 Ack=4913 W...		
695 3.457004	178.79.137.164	10.110.23.232	TCP	66 80 → 62794 [SYN, ACK] Seq=0 Ack=1 W...		
696 3.457074	10.110.23.232	178.79.137.164	TCP	54 62794 → 80 [ACK] Seq=1 Ack=1 Win=13...		
697 3.457309	10.110.23.232	178.79.137.164	HTTP	439 GET /8E_cover_small.jpg HTTP/1.1		
698 3.526943	178.79.137.164	10.110.23.232	TCP	56 80 → 62794 [ACK] Seq=1 Ack=386 Win=...		
699 3.526943	178.79.137.164	10.110.23.232	HTTP	225 HTTP/1.1 301 Moved Permanently		

The IP 178.79.137.164 only send packet after all packet from IP 128.119.245.12 finished send all packet, it follow the time order. No packets from different sources are set alternately even once. Besides, there are two request one after another for two image.

so, two images was sent serially, I think.

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? (5 Points)

in the first time. response is 401 Unauthorized.

159 4.658533	10.110.23.232	128.119.245.12	HTTP	542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
161 4.676293	128.119.245.12	10.110.23.232	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
291 30.149794	10.110.23.232	128.119.245.12	HTTP	627 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
296 30.168915	128.119.245.12	10.110.23.232	HTTP	544 HTTP/1.1 200 OK (text/html)

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? (5 Points)

Wireshark · Packet 159 · WLAN

```
[GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
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/117.0.0.0 S
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
\r\n
```

Wireshark · Packet 291 · WLAN

```
[Group: Sequence]
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 d2lyZXNoYXJrLXN0dWRLbnRzOm5ldHdvcms=\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/117.0.0.0 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
```

0030	02 01 9a 31 00 00 47 45	54 20 2f 77 69 72 65 73	...1..GE T /wires
0040	68 61 72 6b 2d 6c 61 62	73 2f 70 72 6f 74 65 63	hark-lab s/protect
0050	74 65 64 5f 70 61 67 65	73 2f 48 54 54 50 2d 77	ted_page s/HTTP-w
0060	69 72 65 73 68 61 72 6b	2d 66 69 6c 65 35 2e 68	ireshark -file5.h
0070	74 6d 6c 20 48 54 54 50	2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1..Ho
0080	73 74 3a 20 67 61 69 61	2e 63 73 2e 75 6d 61 73	st: gaia .cs.umass
0090	73 2e 65 64 75 0d 0a 43	6f 6e 6e 65 63 74 69 6f	s.edu..C onnectio

Cache-control: max-age = 0  
and Authorization information and credentials