

# **ECE361 – Computer Networks**

## **Wireshark Lab 1: HTTP**

First Name: \_\_\_\_Shaoyang\_\_\_\_ Last Name: \_\_\_\_Zhang\_\_\_\_

First Name: \_\_\_\_Leo\_\_\_\_ Last Name: \_\_\_\_Hanxu\_\_\_\_

**Group Details:**

Student #: 1005751660 Student #: 1006045067

**Mark:**

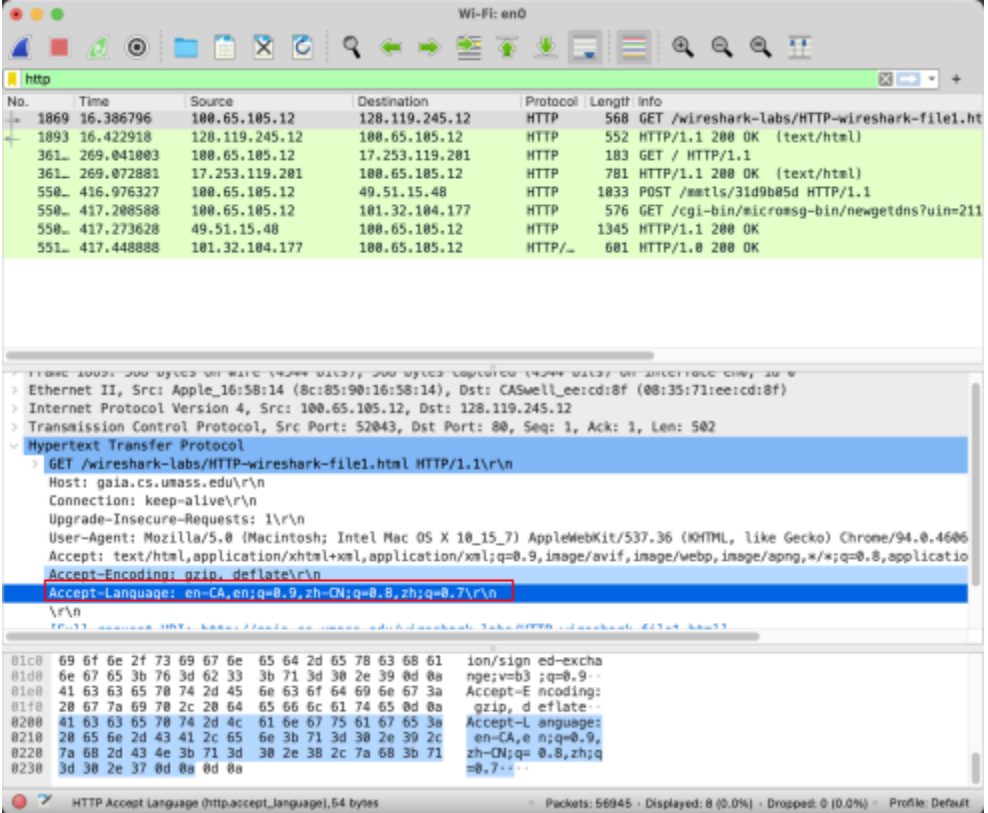
	<b>Question</b>	<b>Answer</b>
1	Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?	Both server and my browser are running HTTP version 1.1

Annotated  
Screenshot  
(if needed)

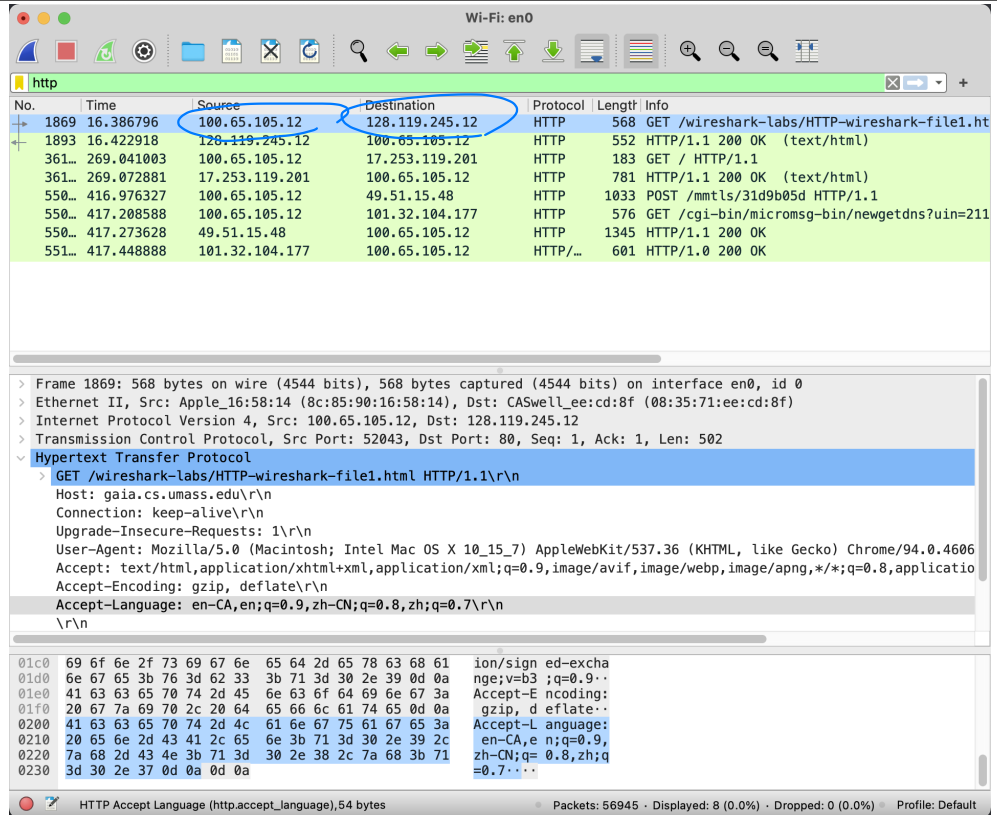
The image displays two screenshots of the Wireshark network protocol analyzer, showing HTTP traffic captured on the Wi-Fi interface (en0).

**Top Screenshot:** The packet list shows a GET request (No. 1869, Time 16.386796, Source 100.65.105.12, Destination 128.119.245.12, Protocol HTTP, Length 568). The packet details pane shows the Hypertext Transfer Protocol section with the request line: `GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1`. The Host header is `gaia.cs.umass.edu`. The User-Agent is `Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606`. The Accept header is `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`. The Accept-Encoding is `gzip, deflate`. The Accept-Language is `en-CA,en;q=0.9,zh-CN;q=0.8,zh;q=0.7`.

**Bottom Screenshot:** The packet list shows the corresponding 200 OK response (No. 1893, Time 16.422918, Source 128.119.245.12, Destination 100.65.105.12, Protocol HTTP, Length 552). The packet details pane shows the Hypertext Transfer Protocol section with the status line: `HTTP/1.1 200 OK`. The Date header is `Mon, 04 Oct 2021 18:56:18 GMT`. The Server is `Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3`. The Last-Modified header is `Mon, 04 Oct 2021 05:59:02 GMT`. The ETag is `"80-5cd809c1a605a"`. The Accept-Ranges header is `bytes`. The Content-Length header is `128`. The Keep-Alive header is `timeout=5, max=100`. The Connection header is `Keep-Alive`. The Content-Type header is `text/html; charset=UTF-8`.

2	What languages (if any) does your browser indicate that it can accept to the server?	en-CA, zh-CN
Annotated Screenshot (if needed)	 <p>The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane at the top shows a packet from 100.65.105.12 to 128.119.245.12. The packet details pane shows the request structure, with the 'Accept-Language' header highlighted in red. The header value is 'en-CA,en;q=0.9,zh-CN;q=0.8,zh;q=0.7'. The packet bytes pane at the bottom shows the raw data of the request, including the 'Accept-Language' header.</p>	
3	What is the IP address of your computer? Of the gaia.cs.umass.edu server?	Own Address: 100.65.105.02 server address: 128.119.245.12

Annotated Screenshot (if needed)

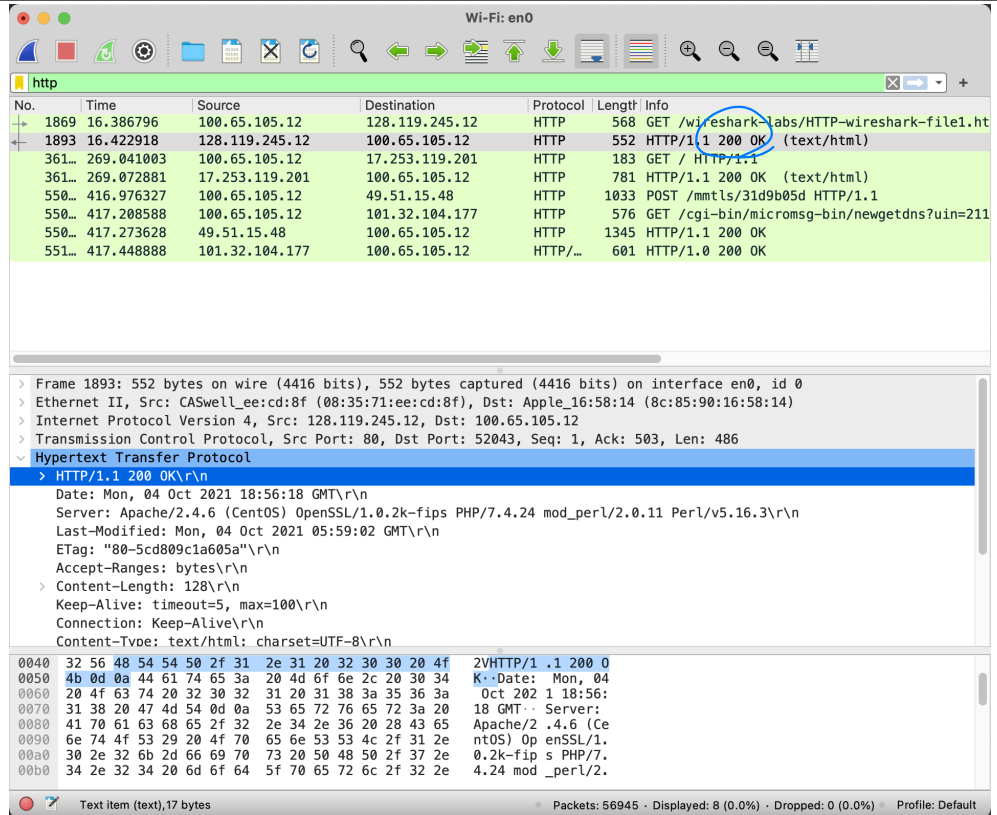


4

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

200

Annotated Screenshot (if needed)

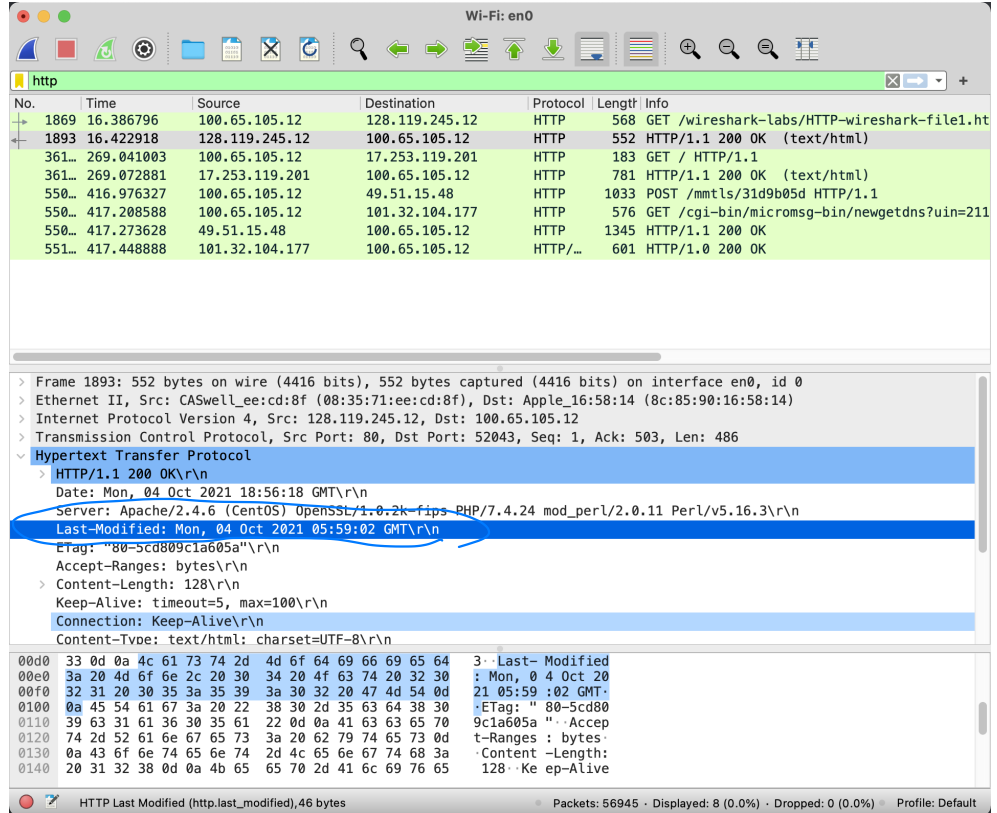


5

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

Mon, 04, Oct. 2021 05:59:02 GMT

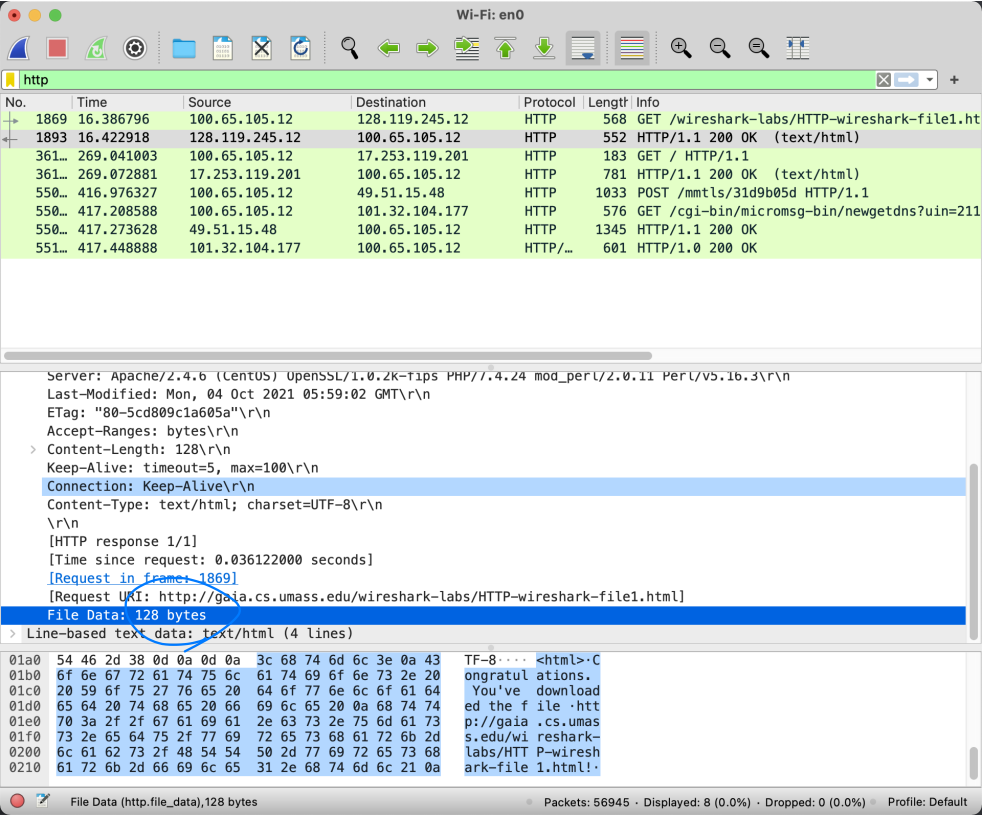
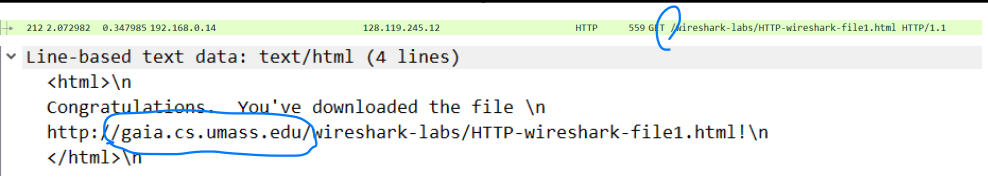
Annotated  
Screenshot  
(if needed)



6

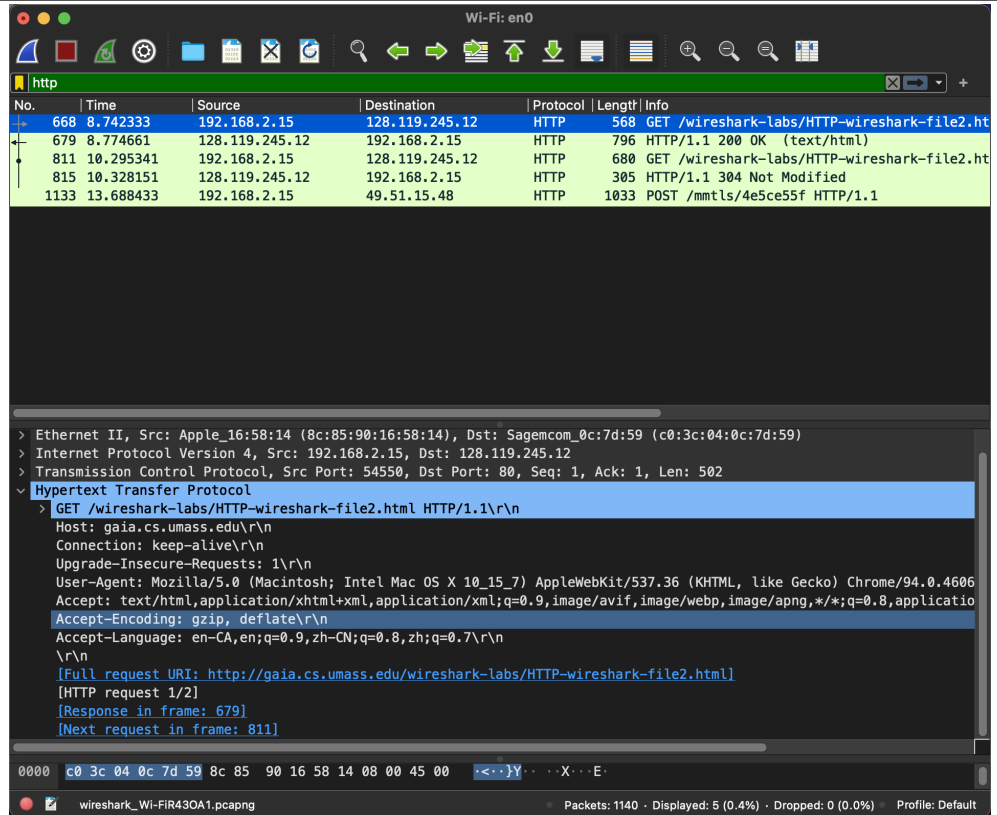
How many bytes of content are  
being returned to your browser?

128 Bytes

<p>Annotated Screenshot (if needed)</p>		
<p>7</p>	<p>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.</p>	<p>http://gaia.cs.umass.edu it does not show the hostname in the packet listing window</p>
<p>Annotated Screenshot (if needed)</p>		
<p>8</p>	<p>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?</p>	<p>NO</p>



Annotated  
Screenshot  
(if needed)

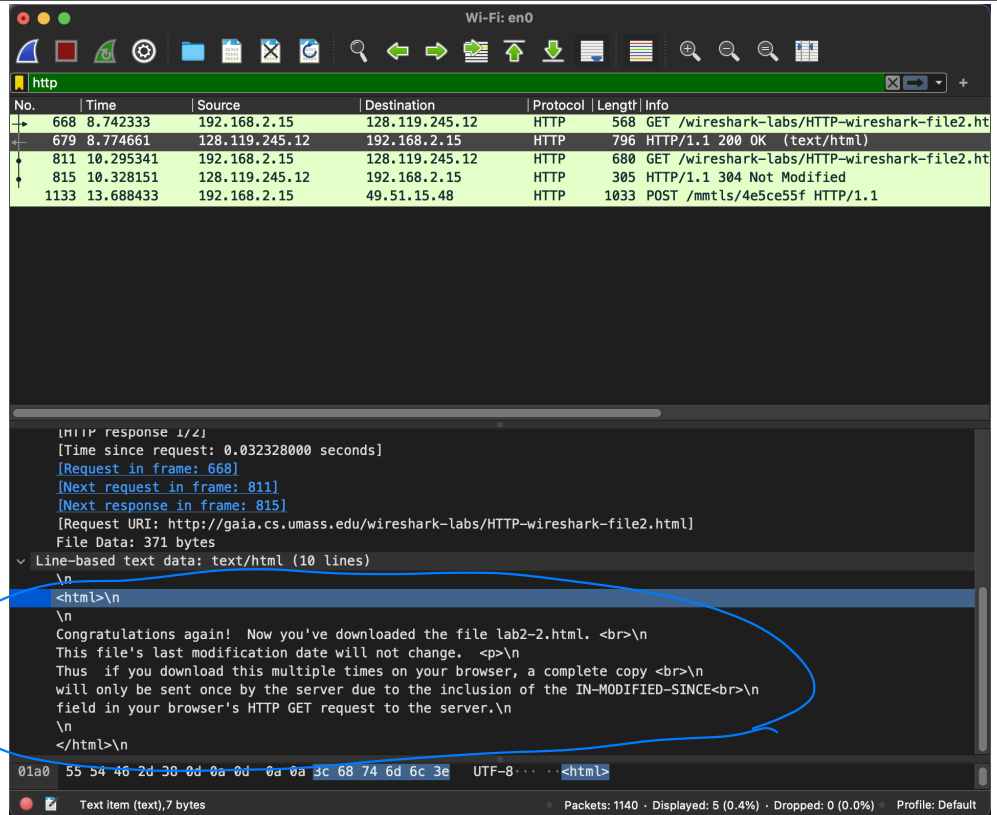


9

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

yes, we can see from line based-text data field, the content of the html file is displayed

Annotated  
Screenshot  
(if needed)

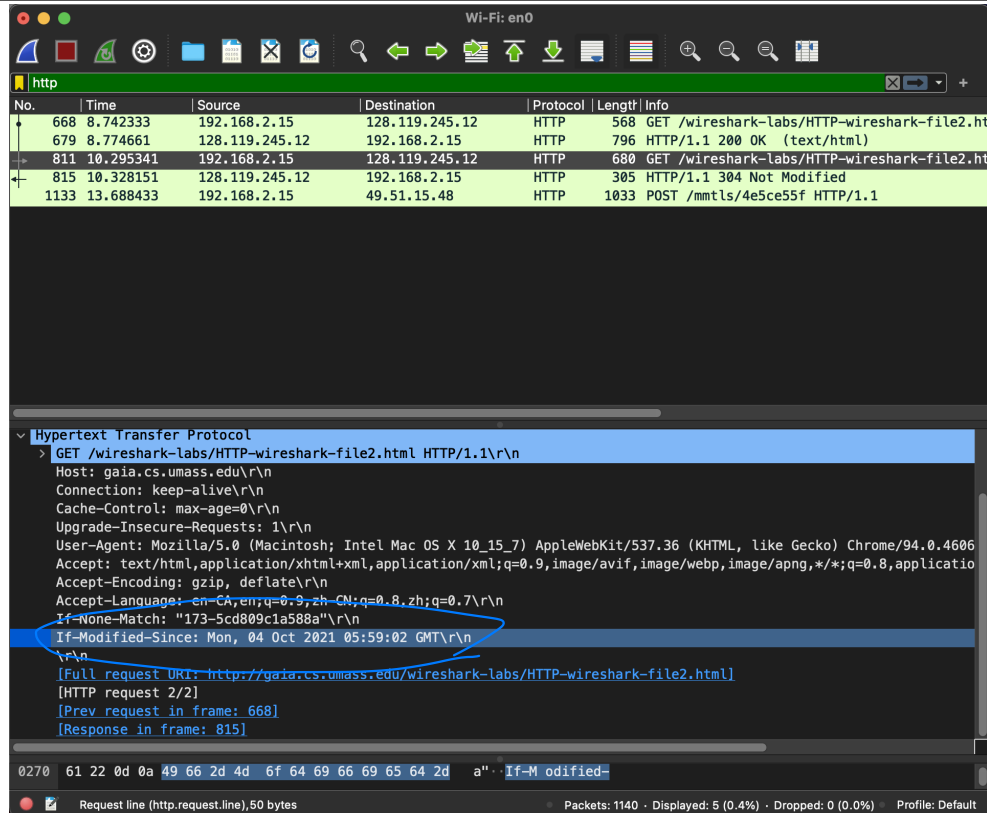


10

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,  
Mon, 04, Oct. 2021 05:59:02 GMT

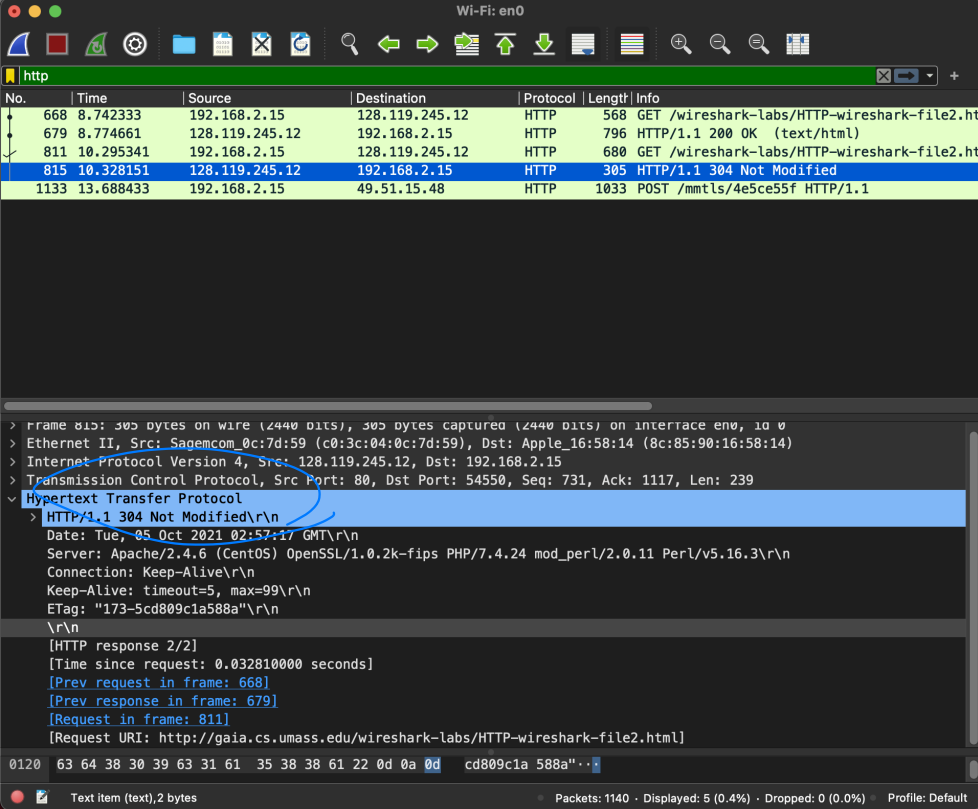
Annotated  
Screenshot  
(if needed)



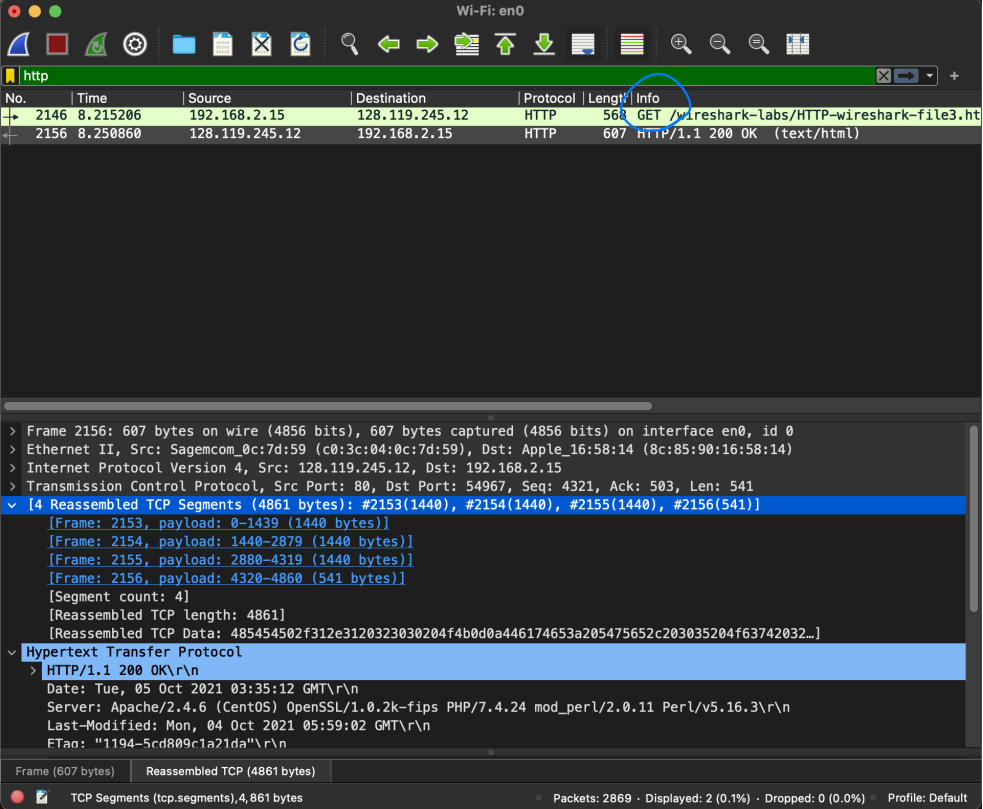
11

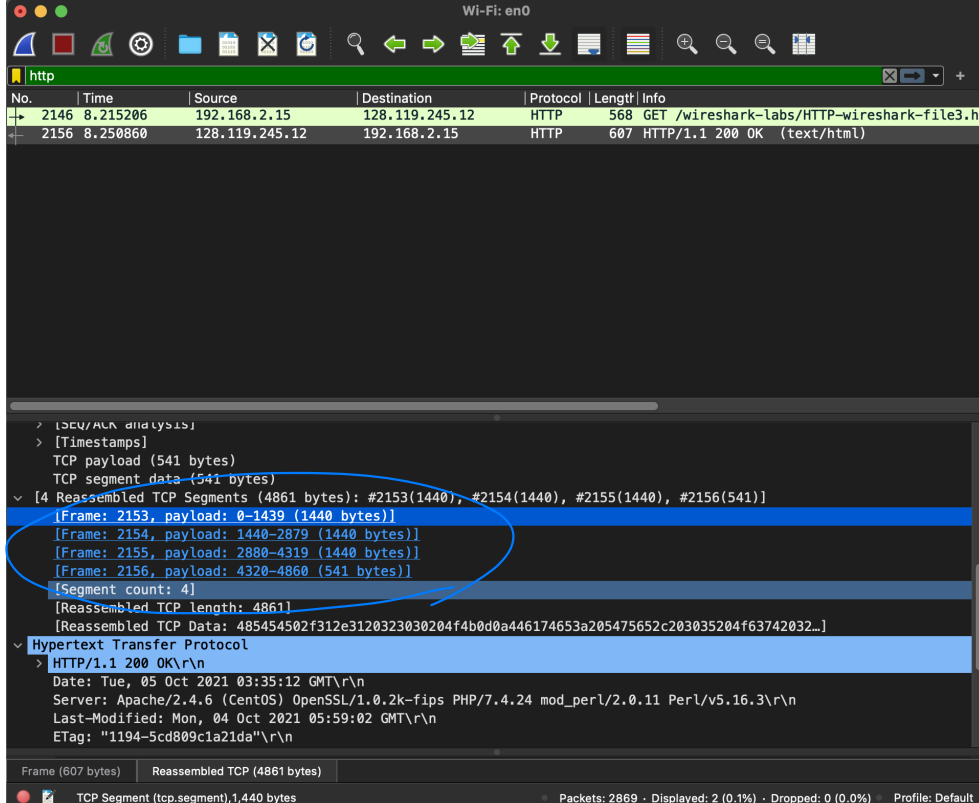
What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

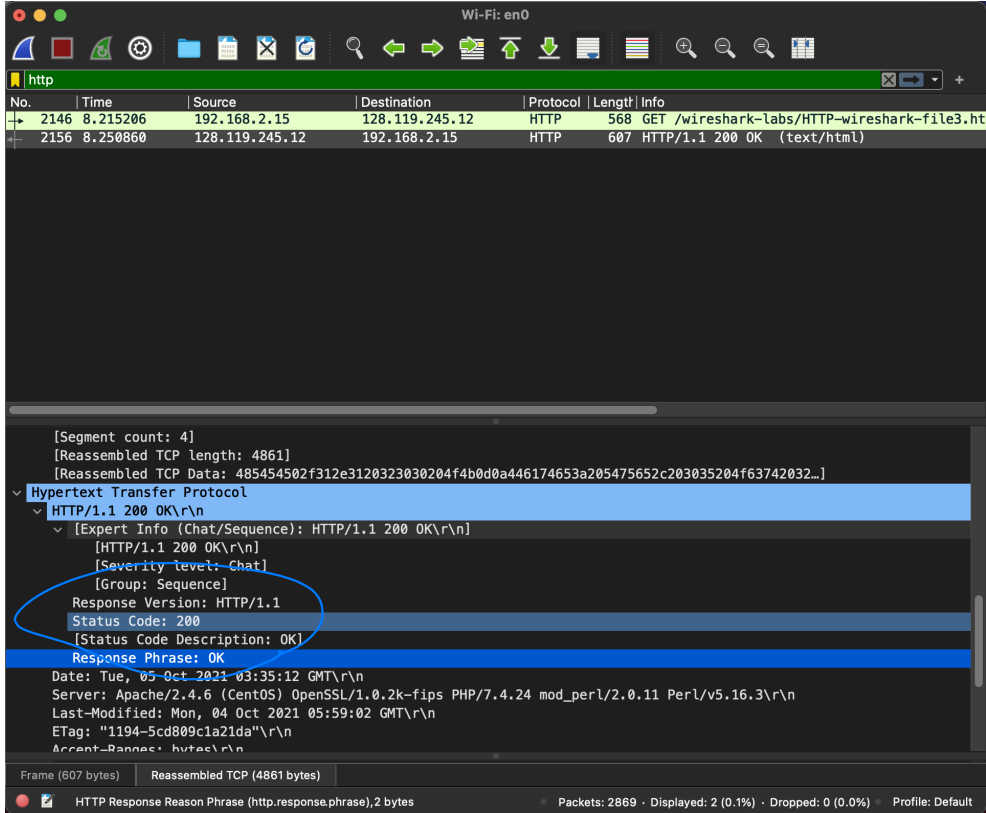
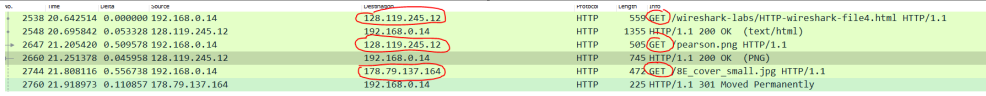
304 Not Modified. It does not return the content of the file. The client sends a request to the server and the server checks the file modified date and sends the NOT MODIFIED status because the file has not been modified since last sent. The server does not send the file again to the client, so there is no contents of the file in the packet. The client will get the file from local web cache.

<p>Annotated Screenshot (if needed)</p>		
<p>12<sup>1</sup></p>	<p>How many HTTP GET request messages were sent by your browser?</p>	<p>1</p>

<sup>1</sup> Yes, questions 12 through 15 are different in this document than the lab handout. **You must answer the questions found in *this* document.**

<p>Annotated Screenshot (if needed)</p>	 <p>The screenshot shows a Wireshark capture of an HTTP GET request. The packet list at the top shows two segments (2154 and 2156) for a single GET request. The packet details pane shows the reassembled TCP segments (4 segments) and the HTTP response structure.</p>	
<p>13</p>	<p>How many data-containing TCP segments were needed to carry the single HTTP response?</p>	<p>4</p>

Annotated Screenshot (if needed)	 <p>The screenshot shows a Wireshark capture of an HTTP transaction. The packet list at the top shows two packets: a GET request (No. 2146) and a 200 OK response (No. 2156). The details pane for the selected packet (No. 2156) shows the following structure:</p> <ul style="list-style-type: none"> <li>Frame: 2153, payload: 0-1439 (1440 bytes)</li> <li>Frame: 2154, payload: 1440-2879 (1440 bytes)</li> <li>Frame: 2155, payload: 2880-4319 (1440 bytes)</li> <li>Frame: 2156, payload: 4320-4860 (541 bytes)</li> <li>Segment count: 4</li> <li>Reassembled TCP length: 4861</li> <li>Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205475652c203035204f63742032...</li> <li>Hypertext Transfer Protocol <ul style="list-style-type: none"> <li>HTTP/1.1 200 OK\r\n</li> <li>Date: Tue, 05 Oct 2021 03:35:12 GMT\r\n</li> <li>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n</li> <li>Last-Modified: Mon, 04 Oct 2021 05:59:02 GMT\r\n</li> <li>ETag: "1194-5cd809c1a21da"\r\n</li> </ul> </li> </ul>	
14	What is the status code and phrase associated with the response to the HTTP GET request?	Status Code: 200 Status Phrase: OK

Annotated Screenshot (if needed)		
15	Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?	No, the new version of Wireshark does not have this feature
Annotated Screenshot (if needed)	the Wireshark display. Earlier versions of Wireshark used the “Continuation” phrase to indicated that the entire content of an HTTP message was broken across multiple TCP segments.. We stress here that there is no “Continuation” message in HTTP!	
16	How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?	3
Annotated Screenshot (if needed)		
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.	downloaded the two images serially, because according to the time stamp, the client sends the request to the first server and gets the first image and then sends the second request to the second server and gets the second image.

Annotated Screenshot (if needed)	2538	20.642514	0.000000	192.168.0.14	128.119.245.12	HTTP	559	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
	2548	20.695842	0.053328	128.119.245.12	192.168.0.14	HTTP	1355	HTTP/1.1 200 OK (text/html)
	2647	21.205420	0.509578	192.168.0.14	128.119.245.12	HTTP	505	GET /pearson.png HTTP/1.1
	2660	21.251378	0.045958	128.119.245.12	192.168.0.14	HTTP	745	HTTP/1.1 200 OK (PNG)
	2744	21.808116	0.556738	192.168.0.14	178.79.137.164	HTTP	472	GET /8E_cover_small.jpg HTTP/1.1
	2760	21.918973	0.110857	178.79.137.164	192.168.0.14	HTTP	225	HTTP/1.1 301 Moved Permanently
	<i>Questions 18 and 19 omitted</i>							