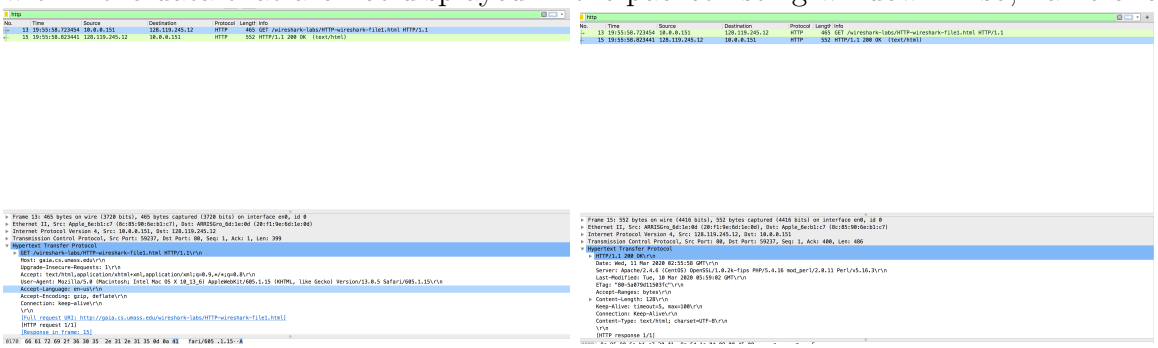
1. Wireshark Lab

The BASIC HTTP GET/response interaction

1.Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2.What languages (if any) does your browser indicate that it can accept to the server?
3.What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4.What is the status code returned from the server to your browser?
5.When was the HTML file that you are retrieving last modified at the server?
6.How many bytes of content are being returned to your browser?
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.

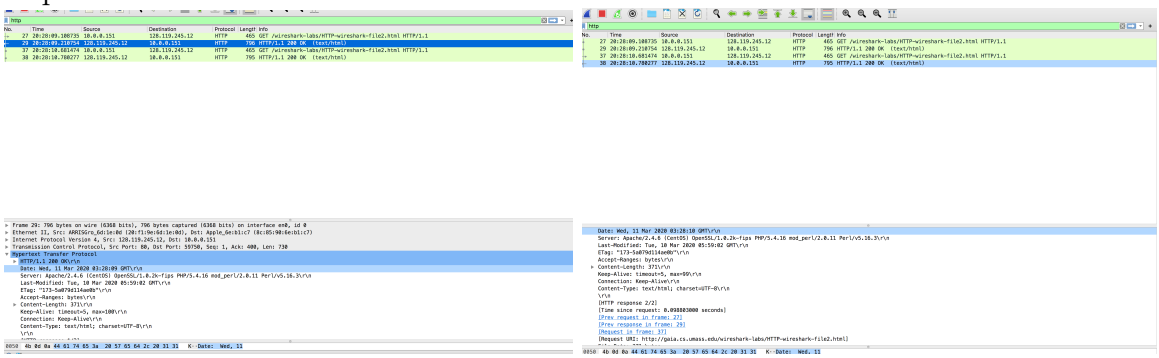


Solution. .
1 HTTP1.1
2 en-us
3 Mine: 10.0.0.151
Server:128.119.245.12
4 200 OK
5 Last-Modified: Tue, 10 Mar 2020 05:59:02 GMT
6 Content Length : 128 Bytes
7 No.

■

2. the HTTP CONDITIONAL GET/response interaction

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

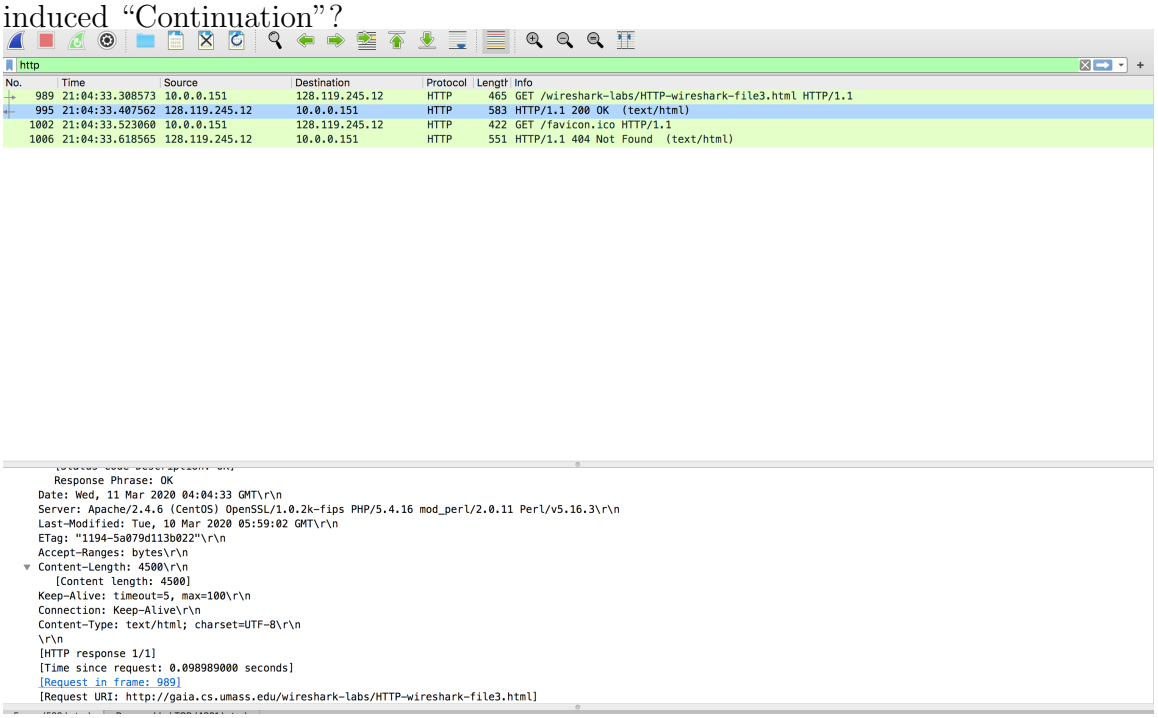


Solution. .
8 No
9Yes. We can see the content length, as well as the data associated with it in Line-based text data.
10 No.
11 Status code was 200 OK again. The browser(SAFARI) didn't cache my data. The data field contained all of the data

■

3. Retrieving Long Documents

12.How many HTTP GET request messages were sent by your browser?
13.How many data-containing TCP segments were needed to carry the single HTTP response?
14.What is the status code and phrase associated with the response to the HTTP GET request?
15.Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?



Solution. .
12 1.
13 1. The content length was 4500, and we needed 4 TCP segments to carry the data.
14 200 OK
15 No

■

4. HTML Documents with Embedded Objects

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

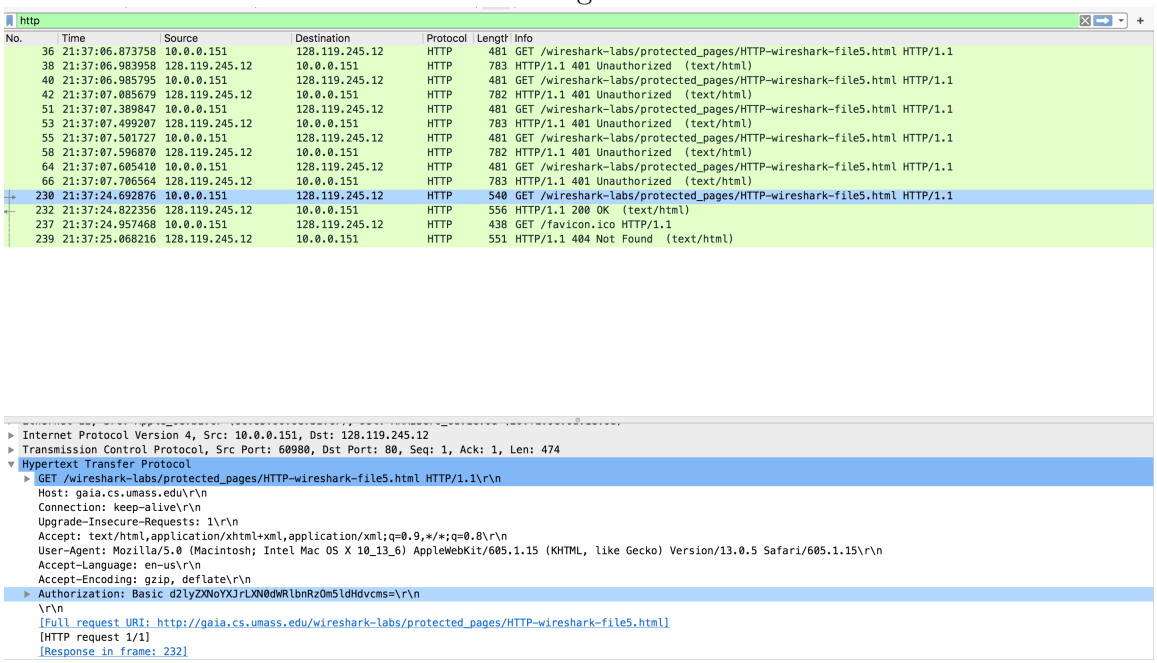
No.	Time	Source	Destination	Protocol	Length	Info
2194	21:24:55.723334	10.0.0.151	128.119.245.12	HTTP	465	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2198	21:24:55.819600	128.119.245.12	10.0.0.151	HTTP	1139	HTTP/1.1 200 OK (text/html)
2200	21:24:55.828544	10.0.0.151	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
2204	21:24:55.919881	128.119.245.12	10.0.0.151	HTTP	781	HTTP/1.1 200 OK (PNG)
2210	21:24:55.921402	10.0.0.151	128.119.245.12	HTTP	494	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
4067	21:24:56.307736	128.119.245.12	10.0.0.151	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

Solution. .
16 3. All of them were sent to 128.119.245.12
17 By checking the TCP ports we can see how the files were downloaded. In this case the 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

■

5. HTTP Authentication

18.What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
19.When your browser's sends the HTTP GET message for the second time, whatnew field is included in the HTTP GET message?



http

No.	Time	Source	Destination	Protocol	Length	Info
36	21:37:06.873758	10.0.0.151	128.119.245.12	HTTP	481	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
38	21:37:06.983958	128.119.245.12	10.0.0.151	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
40	21:37:06.985795	10.0.0.151	128.119.245.12	HTTP	481	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
42	21:37:07.085679	128.119.245.12	10.0.0.151	HTTP	782	HTTP/1.1 401 Unauthorized (text/html)
51	21:37:07.389847	10.0.0.151	128.119.245.12	HTTP	481	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
53	21:37:07.499207	128.119.245.12	10.0.0.151	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
55	21:37:07.501727	10.0.0.151	128.119.245.12	HTTP	481	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
58	21:37:07.596870	128.119.245.12	10.0.0.151	HTTP	782	HTTP/1.1 401 Unauthorized (text/html)
64	21:37:07.605410	10.0.0.151	128.119.245.12	HTTP	481	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
66	21:37:07.706564	128.119.245.12	10.0.0.151	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
230	21:37:24.692876	10.0.0.151	128.119.245.12	HTTP	540	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
232	21:37:24.822356	128.119.245.12	10.0.0.151	HTTP	556	HTTP/1.1 200 OK (text/html)
237	21:37:24.957468	10.0.0.151	128.119.245.12	HTTP	438	GET /favicon.ico HTTP/1.1
239	21:37:25.068216	128.119.245.12	10.0.0.151	HTTP	551	HTTP/1.1 404 Not Found (text/html)

```
▶ Internet Protocol Version 4, Src: 10.0.0.151, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 60980, Dst Port: 80, Seq: 1, Ack: 1, Len: 474
▼ 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
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.5 Safari/605.1.15\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
  ▶ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\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: 232]
```

Solution. .
18 Status code : 401. Phrase : Unauthorized
19 Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms= ° ■