Wireshark Lab 2

HTTP

Suraj Durgesht

(16EC06)

Instructor: Dr. Rajendra Hegadi

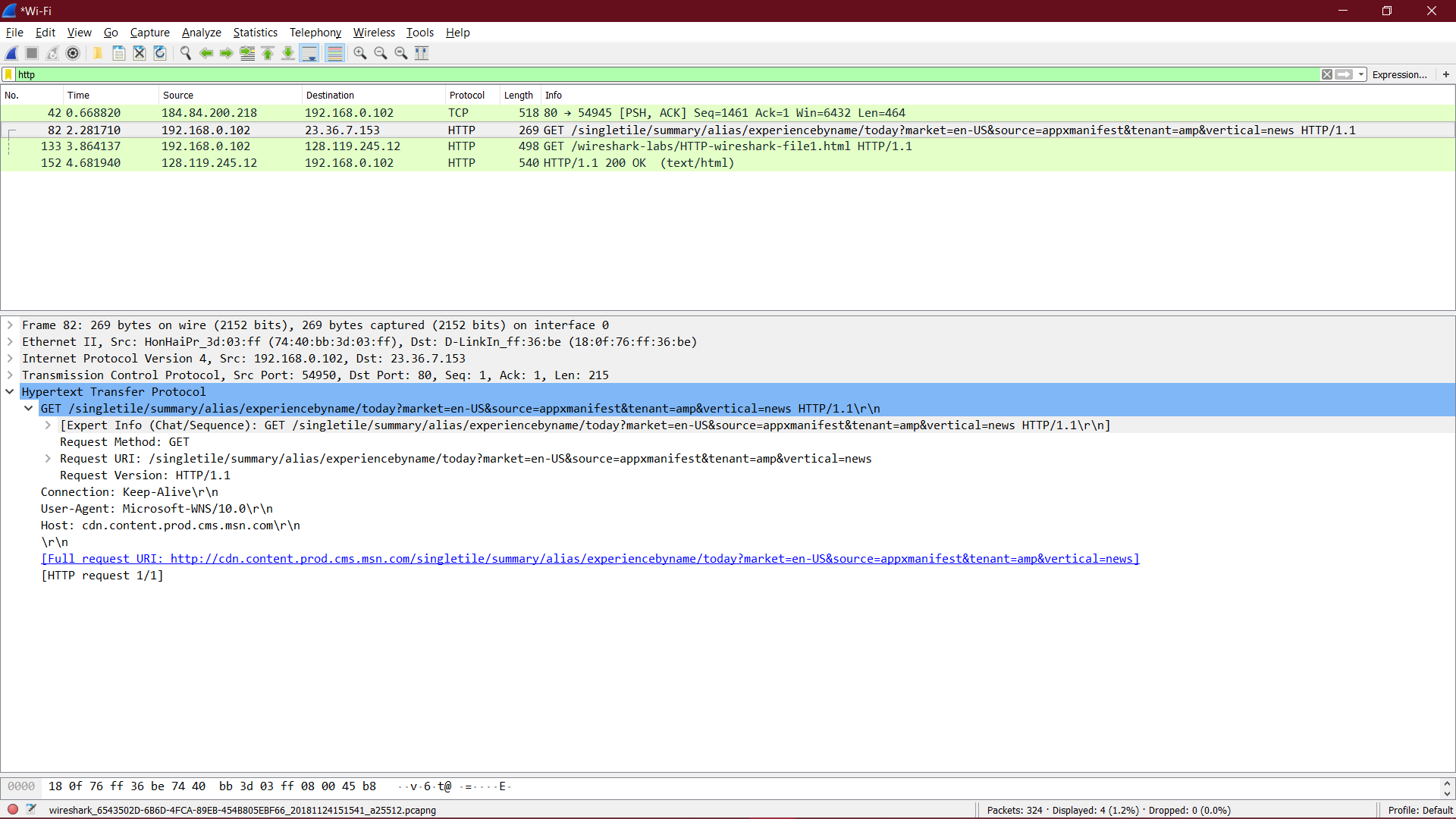
1. The following screen shots showing the HTTP GET and HTTP reply answer these questions:

Que1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server

running?

Solution:

Both are running HTTP 1.1



Que2. What languages does your browser indicate that it can accept to the server?

Solution:

Accept-Language: en-US, en;

Que3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Solution:

My IP address is 192.168.0.102 and the

server’s is 128.119.245.12

Que4. What is the status code returned from the server to your browser?

Solution:

HTTP/1.1 200 OK (text/html)

Que5. When was the HTML file that you are retrieving last modified at the server?

Solution:

last modified == "Sat, 24 Nov 2018 06:59:02 GMT"

Que6. How many bytes of content are being returned to your browser?

Solution:

Content-Length: 128

Que7*.* 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:

No all of the headers can be found in the raw data.

1. The HTTP CONDITIONAL GET/response interaction

Que8. 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?

Solution: No

Que9. Inspect the contents of the server response. Did the server explicitly return the

contents of the file? How can you tell?

Solution:

Yes, because we can see the contents in the Line-based text data field.

Que10. 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?

Solution:

Yes. The information following is: last\_modified == "Sat, 24 Nov 2018 06:59:02 GMT" which is the date of the last modification of the file from the previous get request.

Que11. 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:

The status code and phrase returned from the server is HTTP/1.1 304 Not Modified. The server didn’t return the contents of the file since the browser loaded it from its cache.

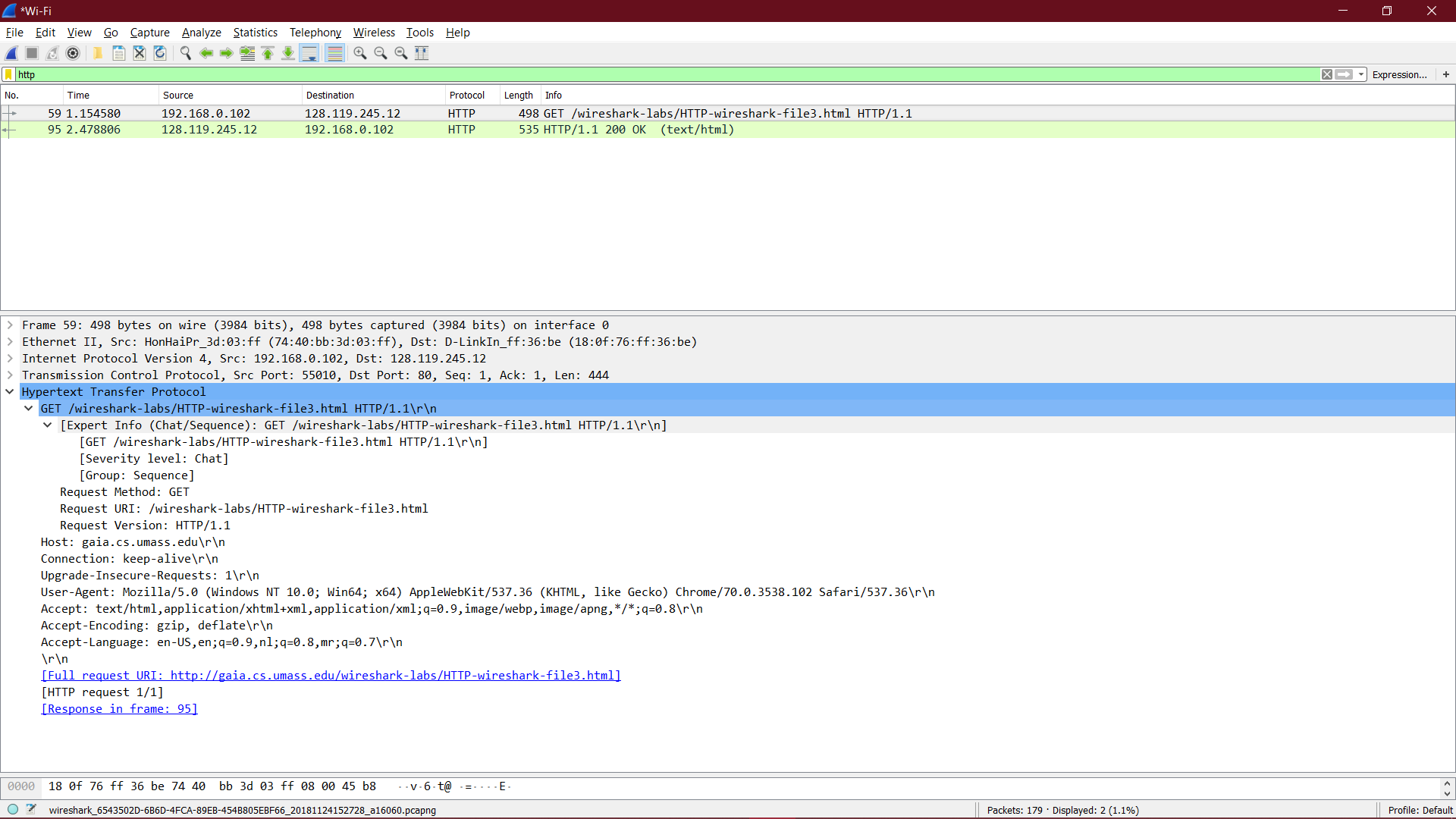
1. Retrieving Long Documents

Que12. 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?

Solution:

There was 1 HTTP GET request message sent by my browser as seen in the screenshot. first packet number.



Que13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Solution: packet 2(filter HTTP)

Que14. What is the status code and Phrase in the response?

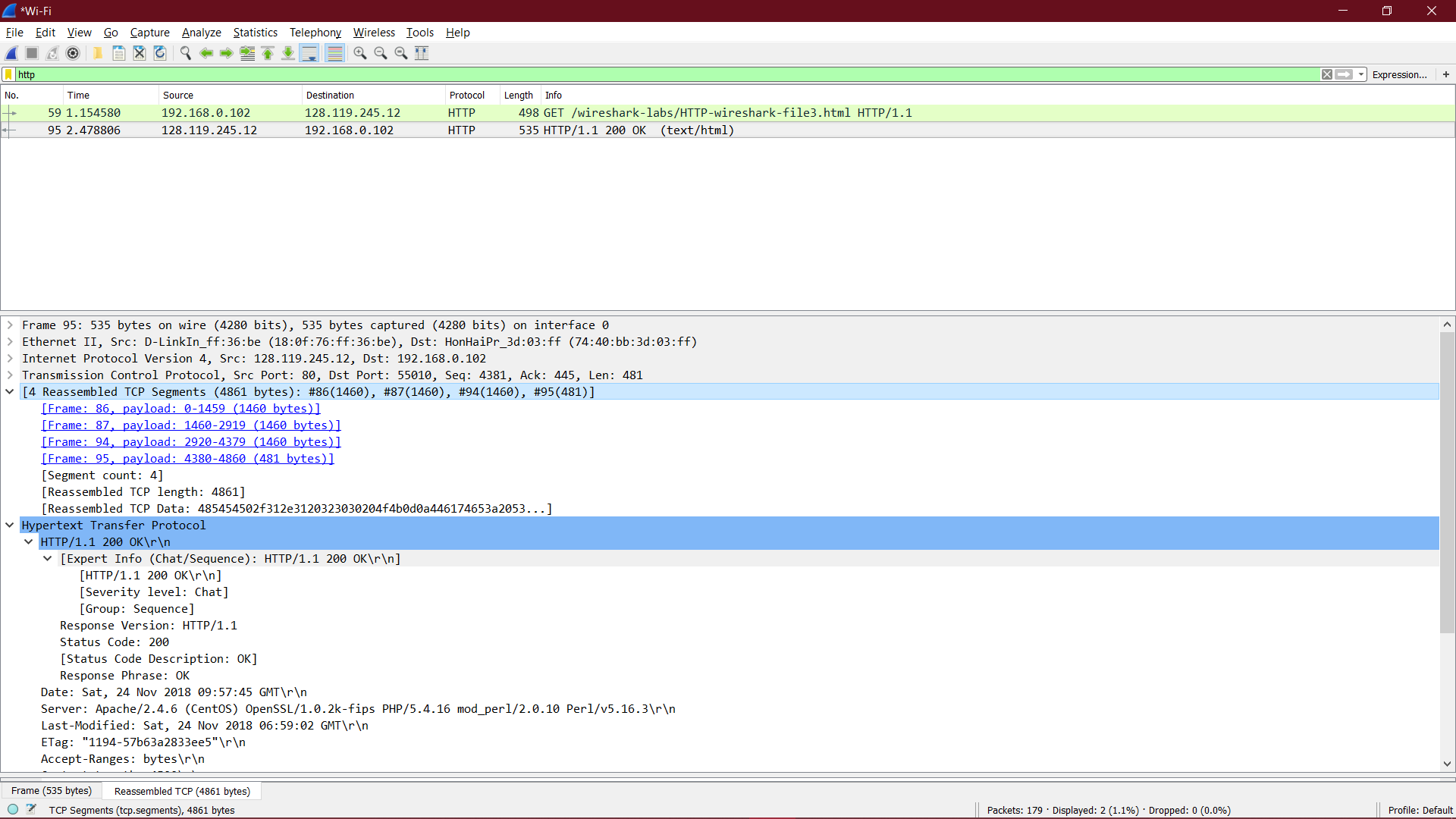
Solution: 200 OK

Que15. How many data-containing TCP segments were needed to carry the single HTTP

response and the text of the Bill of Rights?

Solution:

There were 4 data containing TCP segments containing 1460,1460,1460, and 481 bytes respectively for a total of 4861 bytes.



1. HTML Documents with Embedded Objects

Que16. How many HTTP GET request messages did your browser send? To which

Internet addresses were these GET requests sent?

Solution:

There were three HTTP GET messages sent: packet (to get the base file), packet (to get the Pearson logo) and packet (to get the 5th edition textbook cover). There were 3 HTTP GET requests sent to the following Internet addresses:

a) 128.119.245.12

b) 128.119.240.90

c) 165.193.123.218.

Que17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel?

Solution:

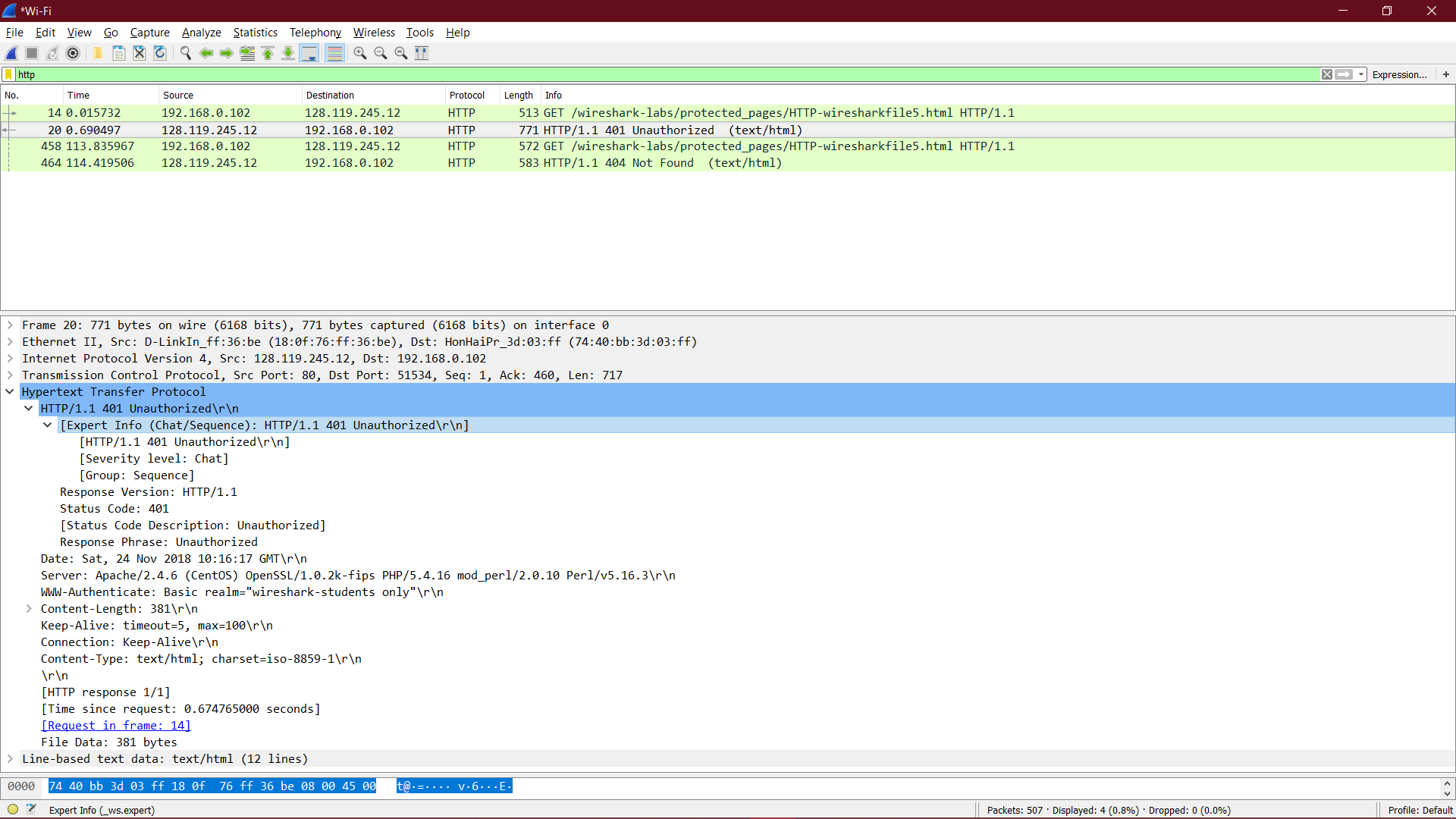
By checking the TCP port, we can see if our files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

5 HTTP Authentication

Que18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

Solution:

Status code: 401, Phrase: unauthorized



Que19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Solution:

The HTTP GET includes the Authorization: Basic: field