***A) 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?

A. Browser and Server are running HTTP version 1.1

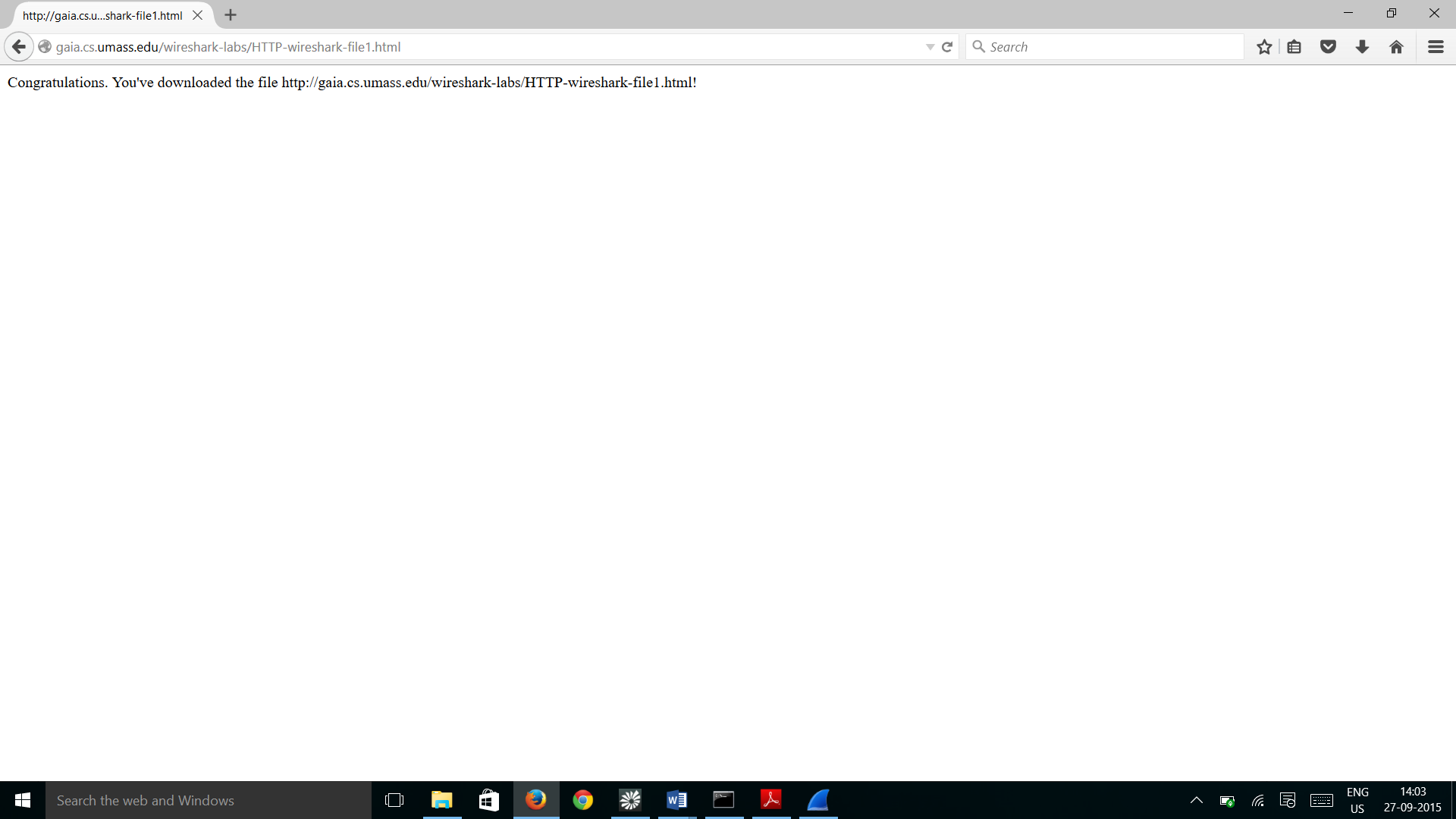
1. What languages (if any) does your browser indicate that it can accept to the server?

A. en-US, en

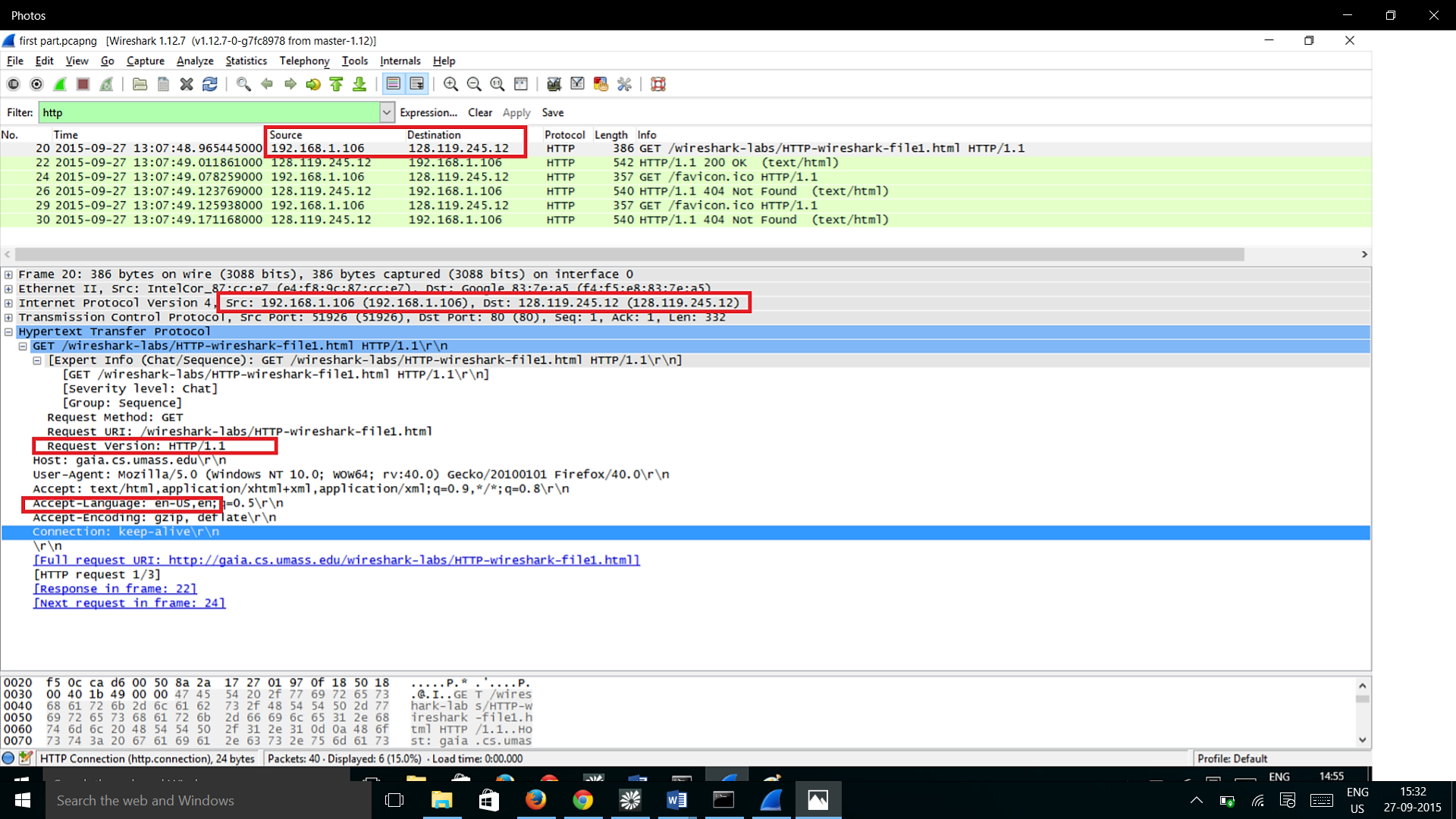
1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

A. IP address of the computer is 192.168.1.106 and the IP address of the gaia.cs.umass.edu server is

128.119.245.12



HTTP GET Message



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

A. 200

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

A. Sun, 27 Sep 2015 05:59:01 GMT

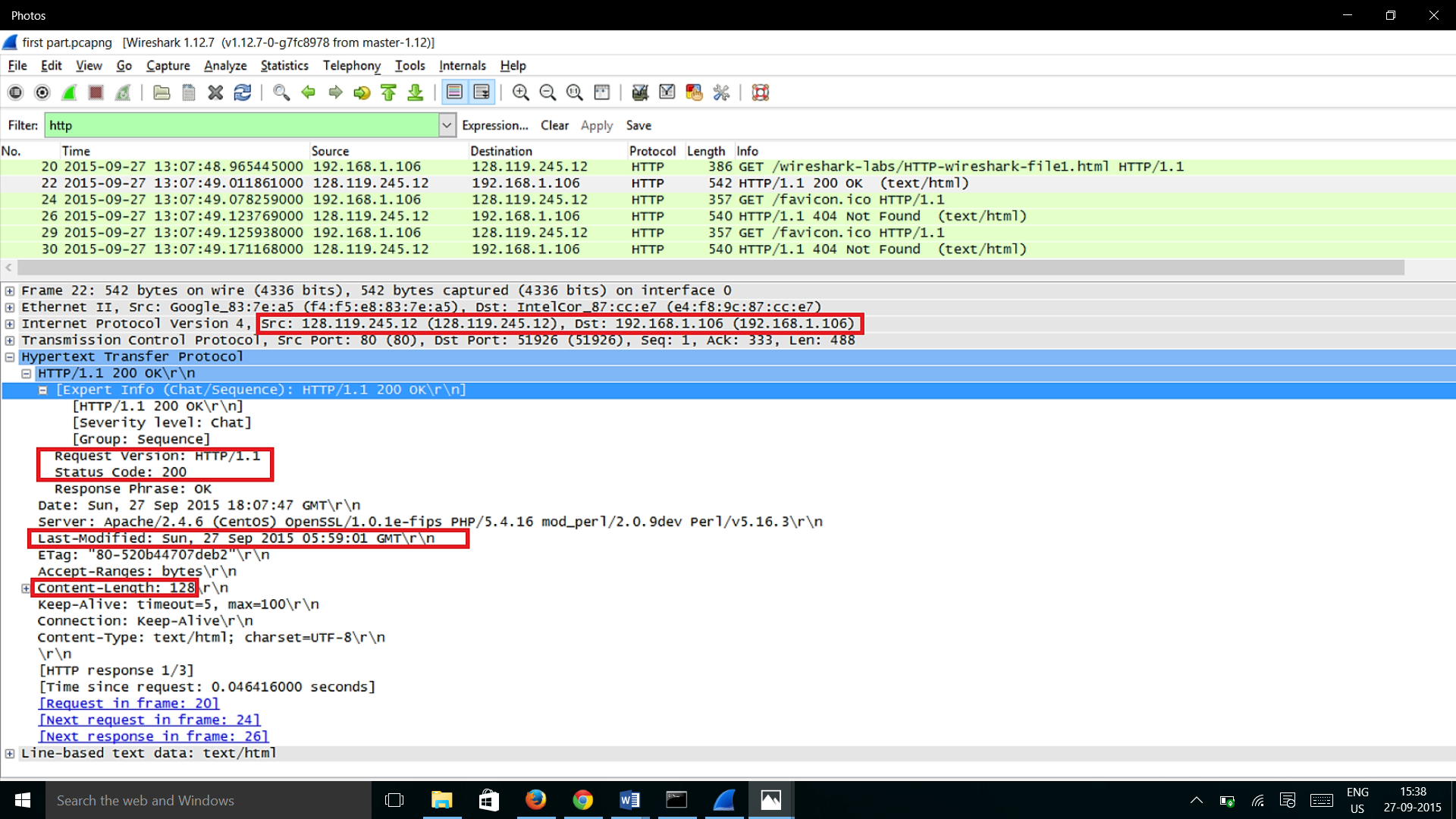
1. How many bytes of content are being returned to your browser?

A. 128 bytes

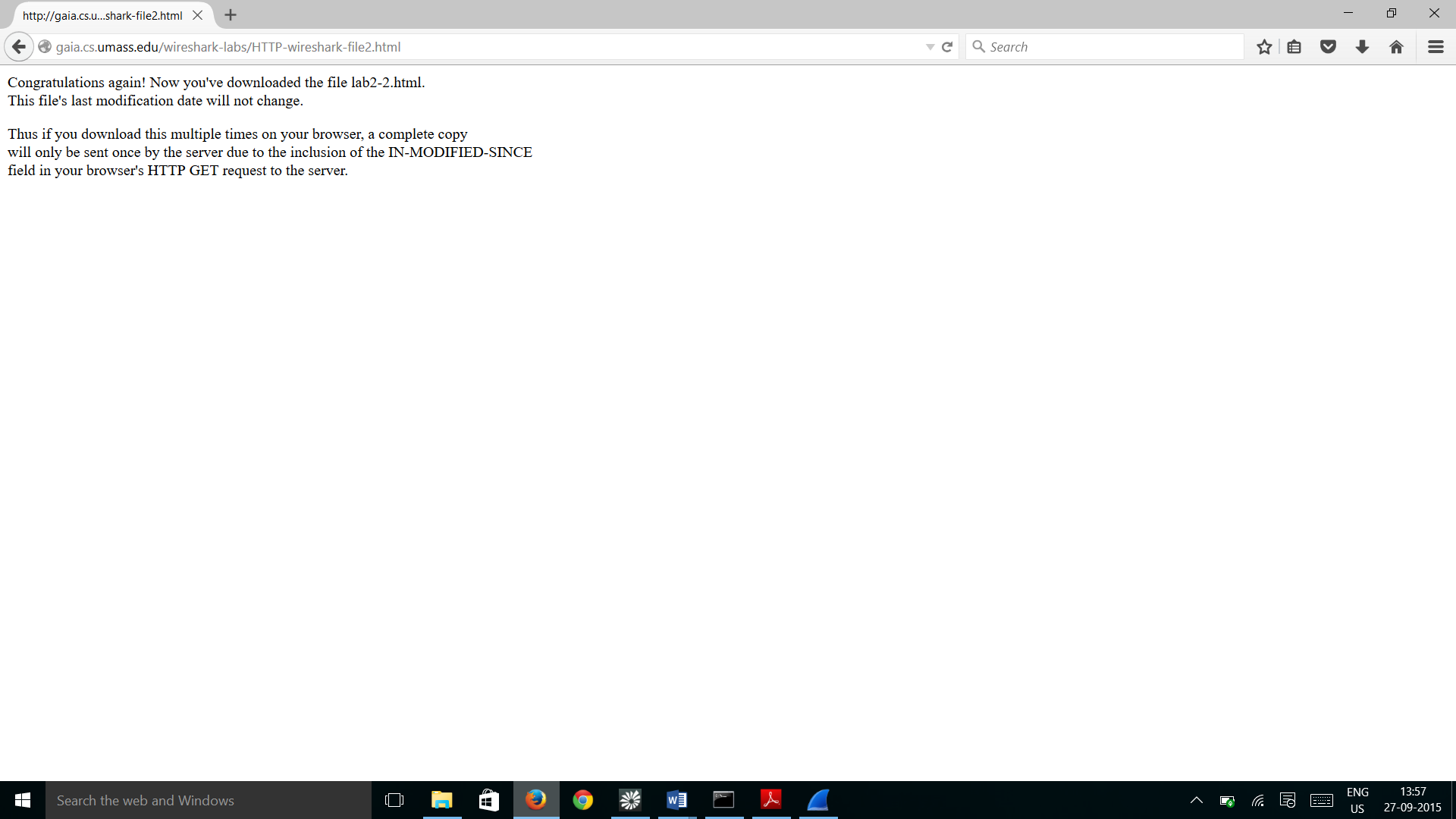
1. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

A. No there is no header like that and all the headers are displayed in the packet-listing window.

HTTP Response Message



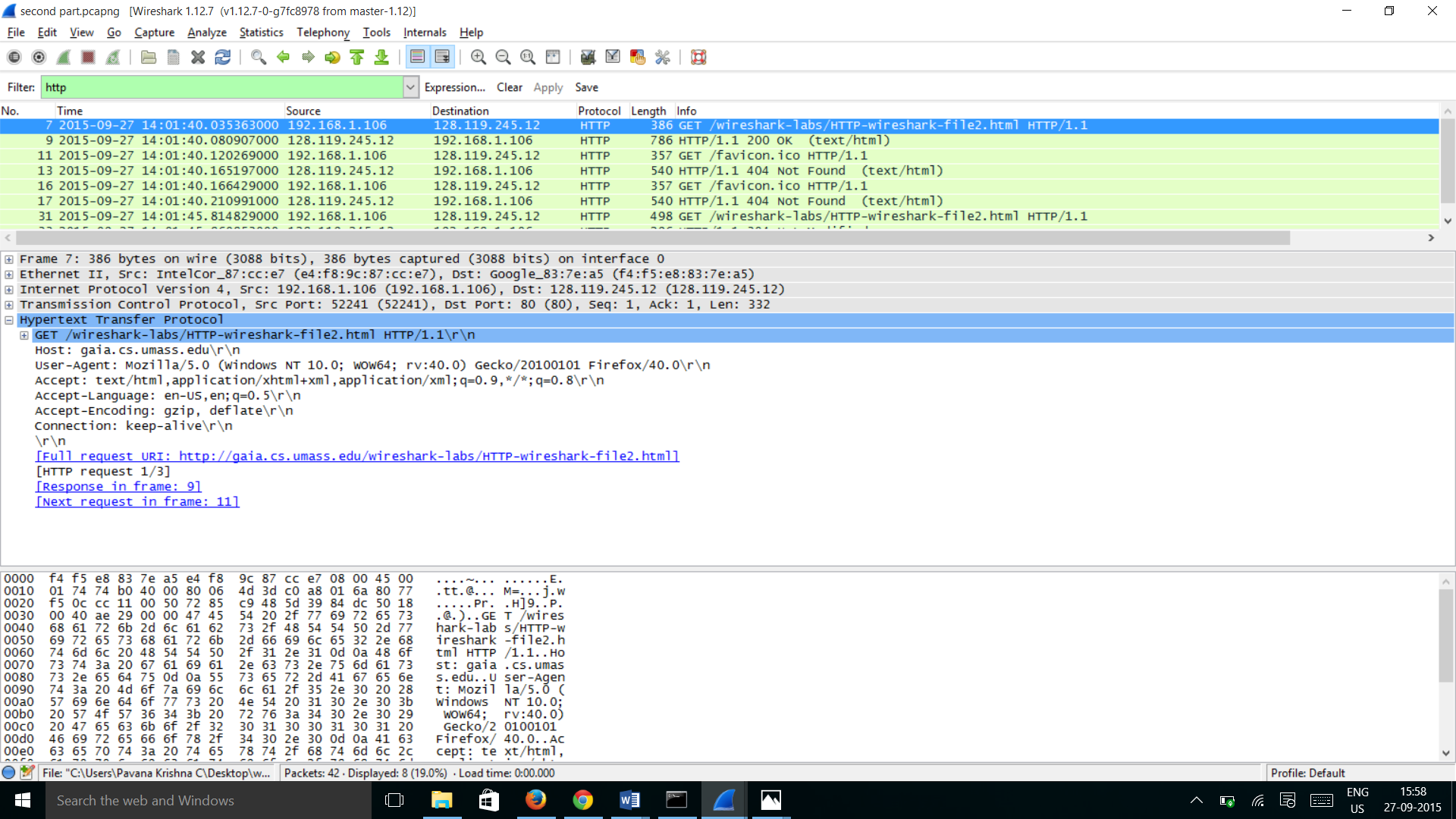
***B) The HTTP Conditional GET/Response Interaction***



1. 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?

A. NO

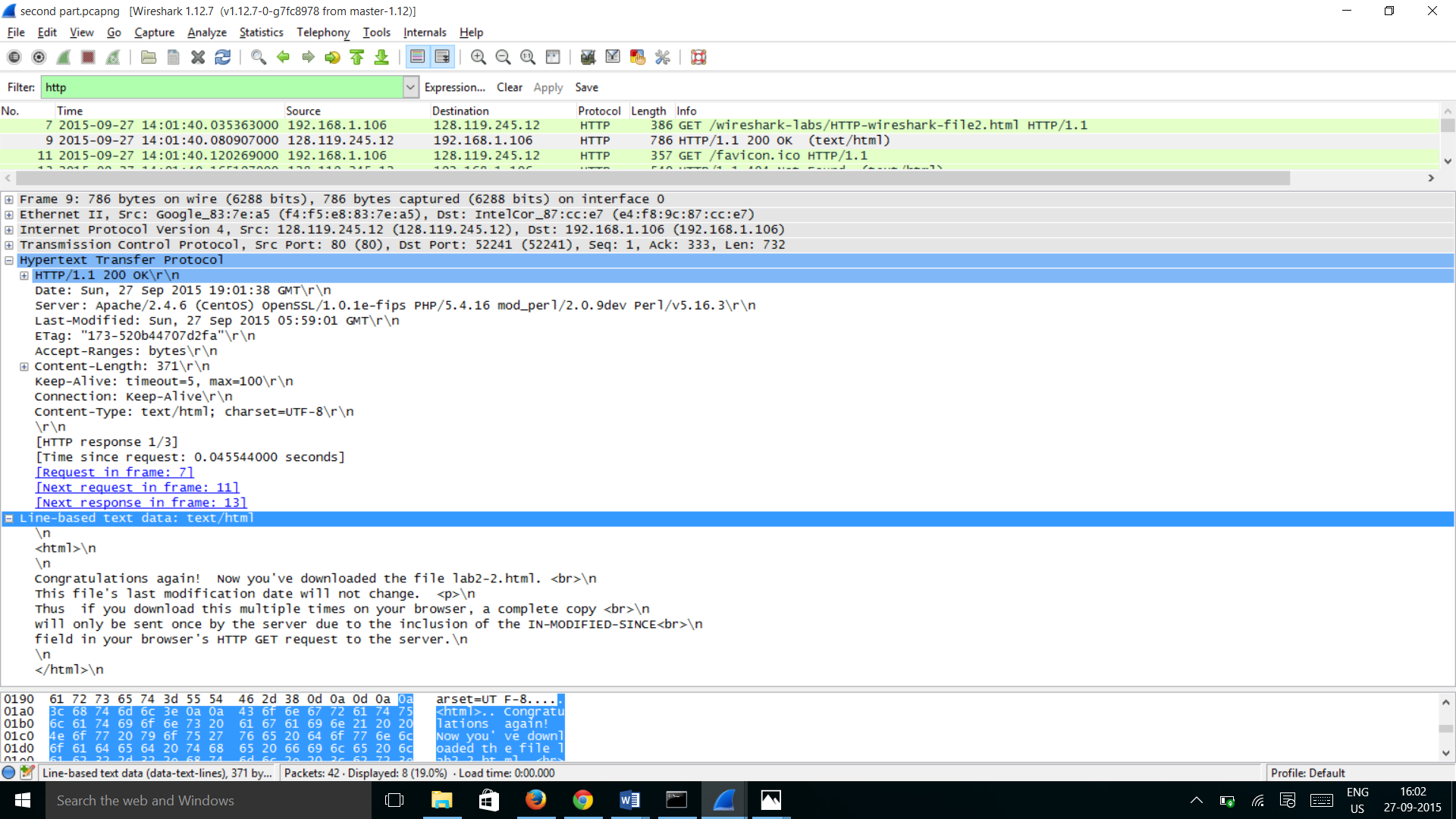
First GET Message



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

A. Yes the server explicitly return the contents of the file and we are able to see the contents in the Line-based text data: text/html field.

First Response Message

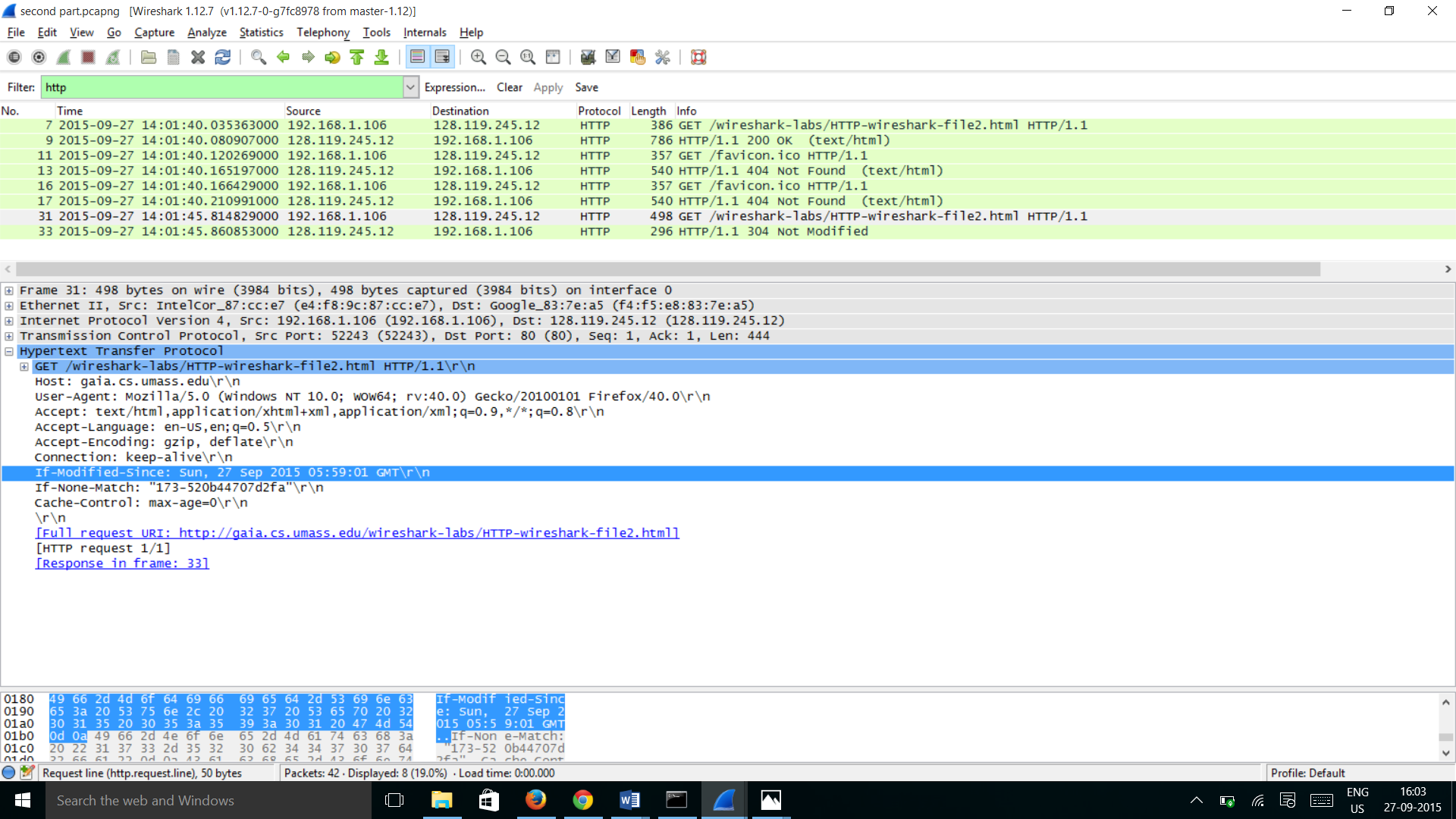


1. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

A. Yes. The information follows the “If-Modified-Since:” header is Sun, 27 Sep 2015 05:59:01 GMT,

The last modified date of the file from the previous GET request.

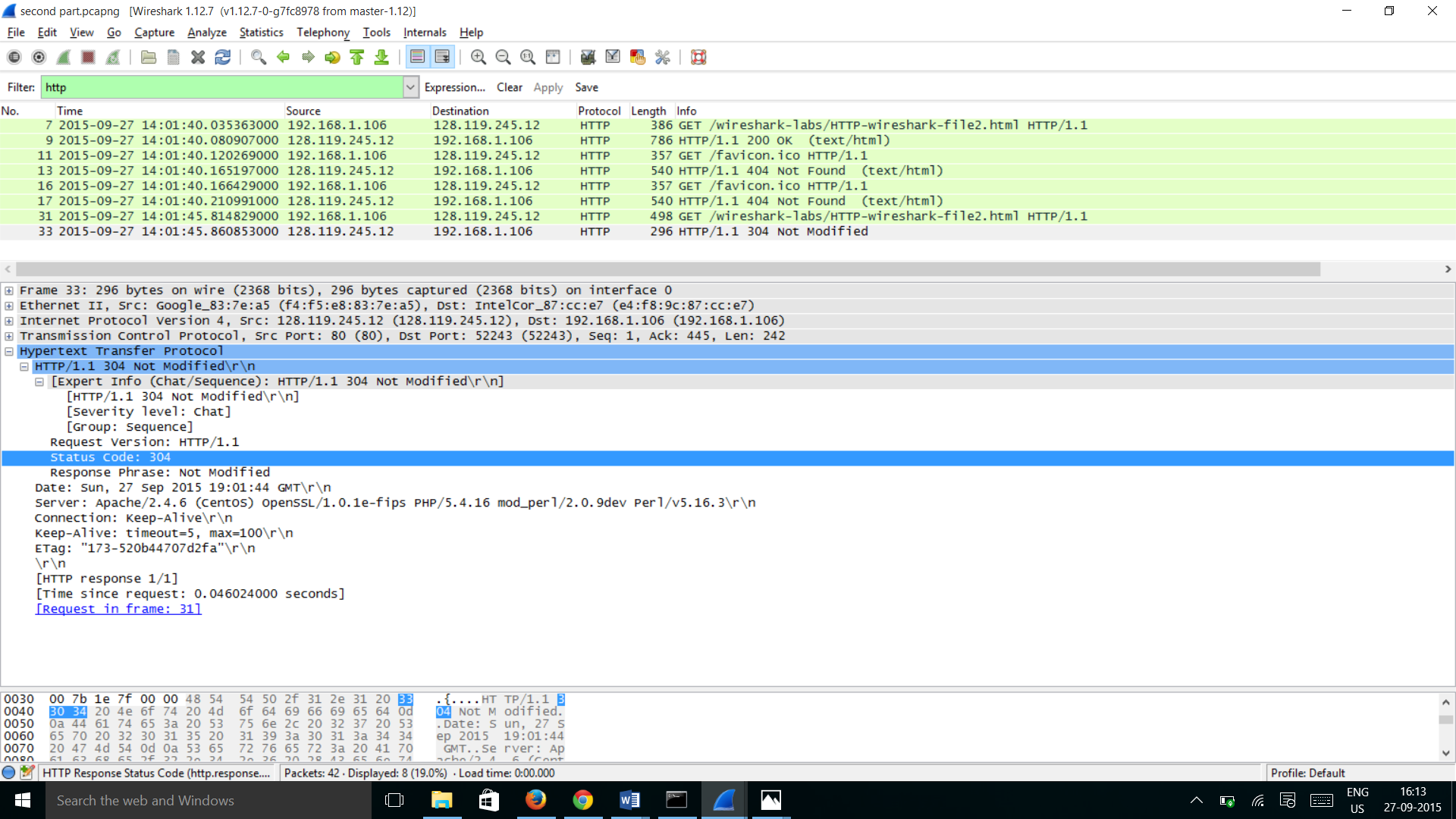
Second HTTP GET Message



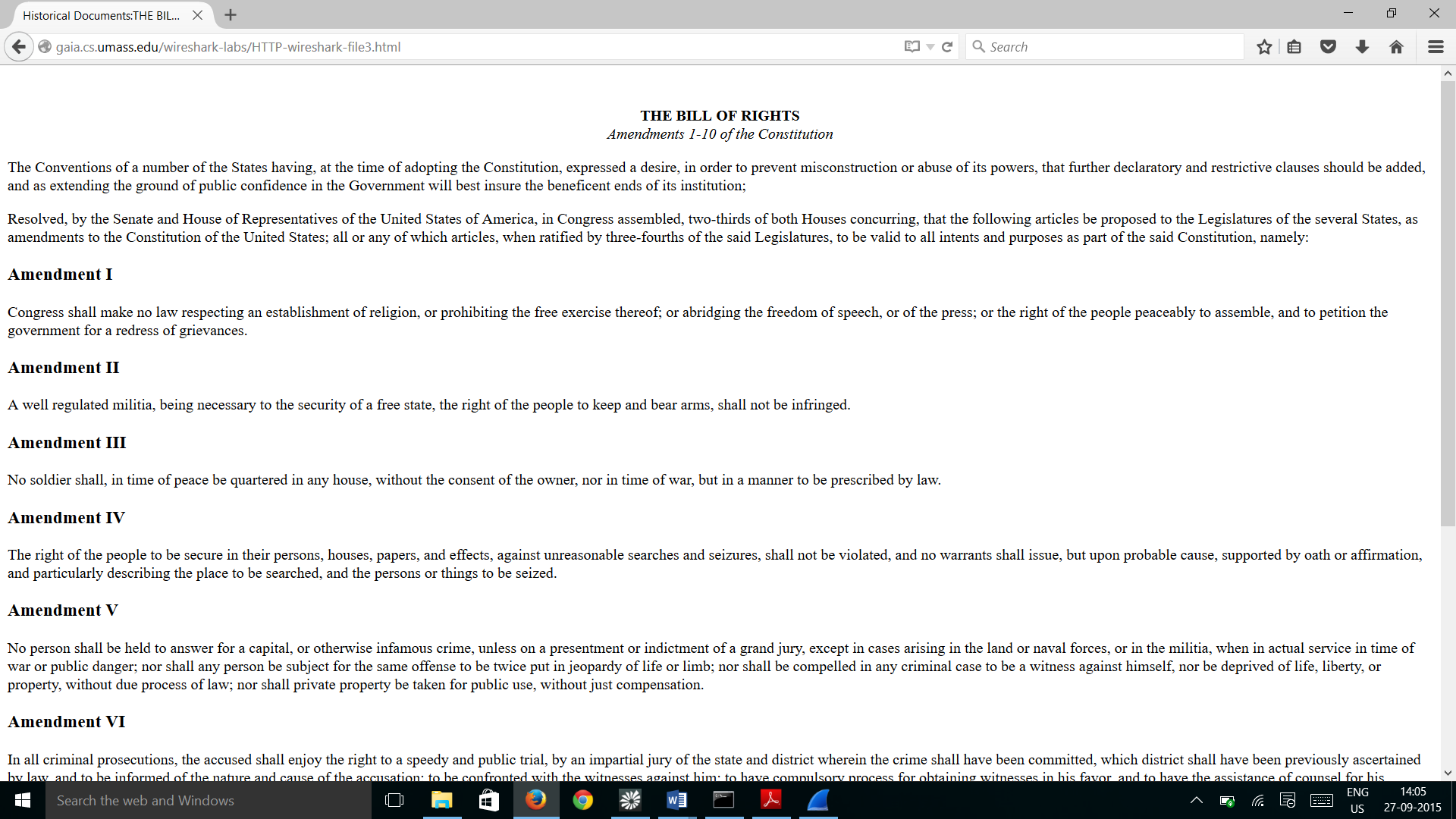
1. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

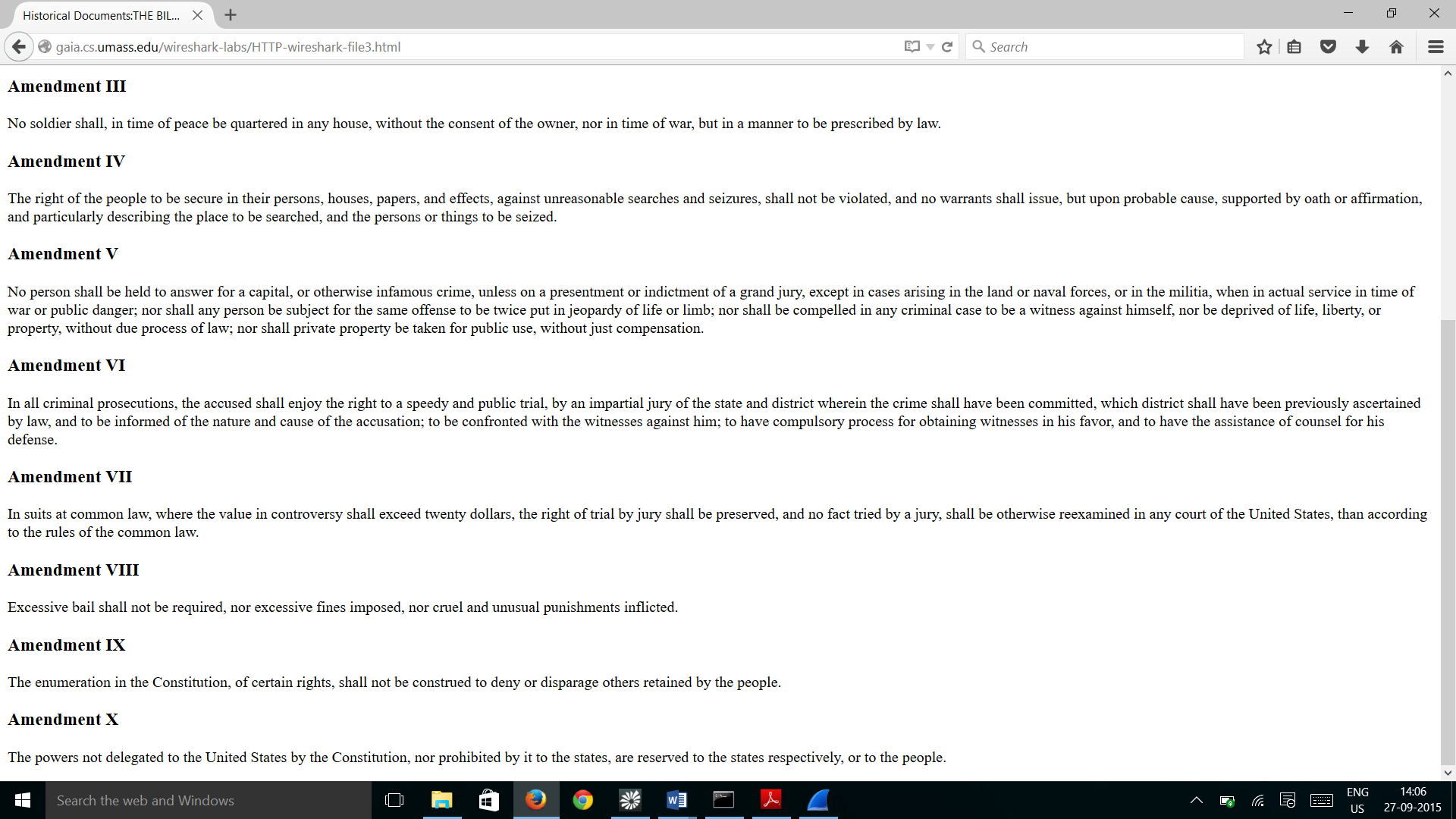
A. Status code is “304” and the response phrase is “Not Modified”. No the server did not return the contents of the file as they are loaded from the cache.

Second Response Message



***C) Retrieving Long Documents***

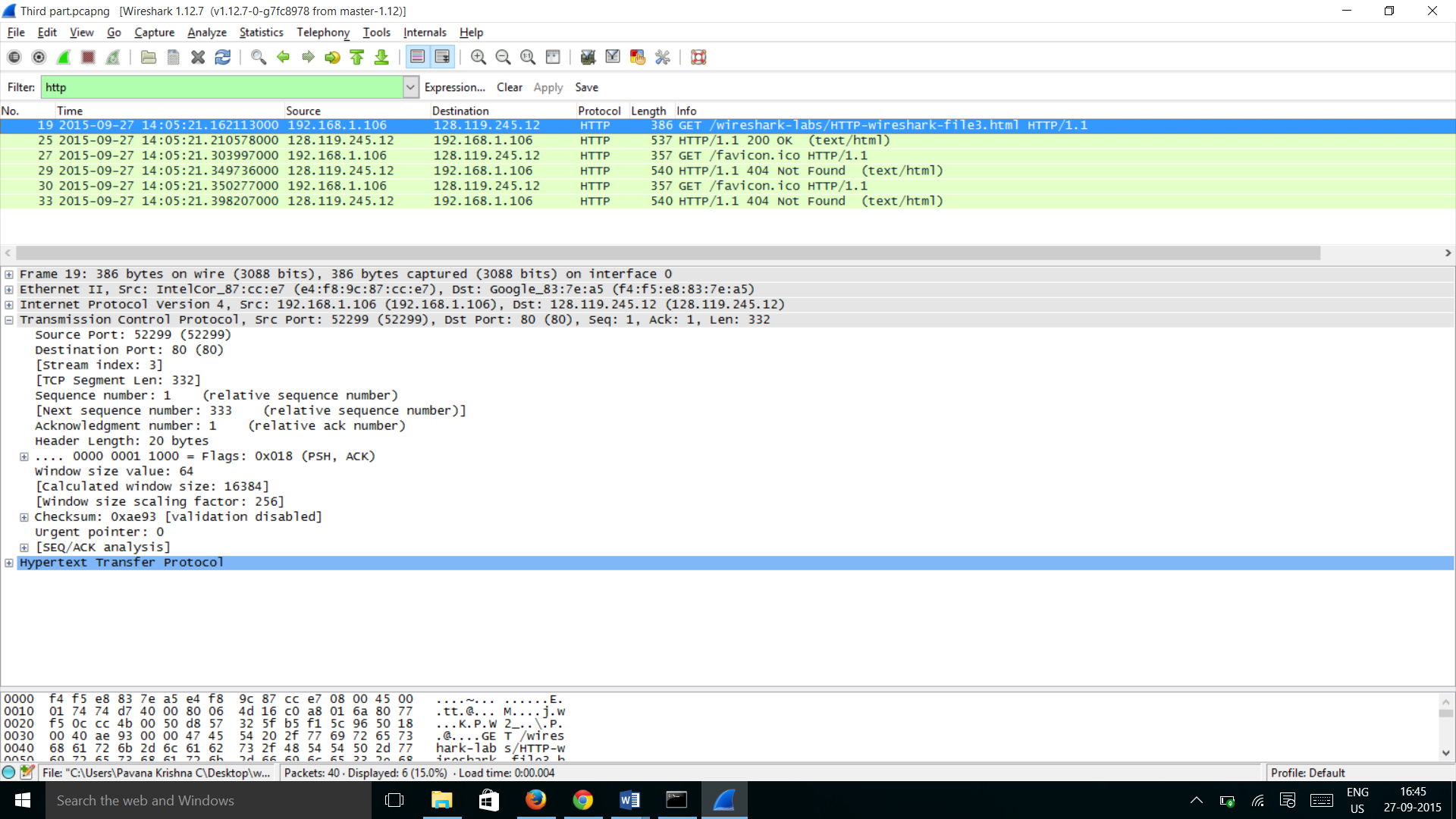




12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

A. Number of HTTP Get Request message sent by browser is 1. The packet number in the trace contains the GET message for the Bill or Rights is 19.

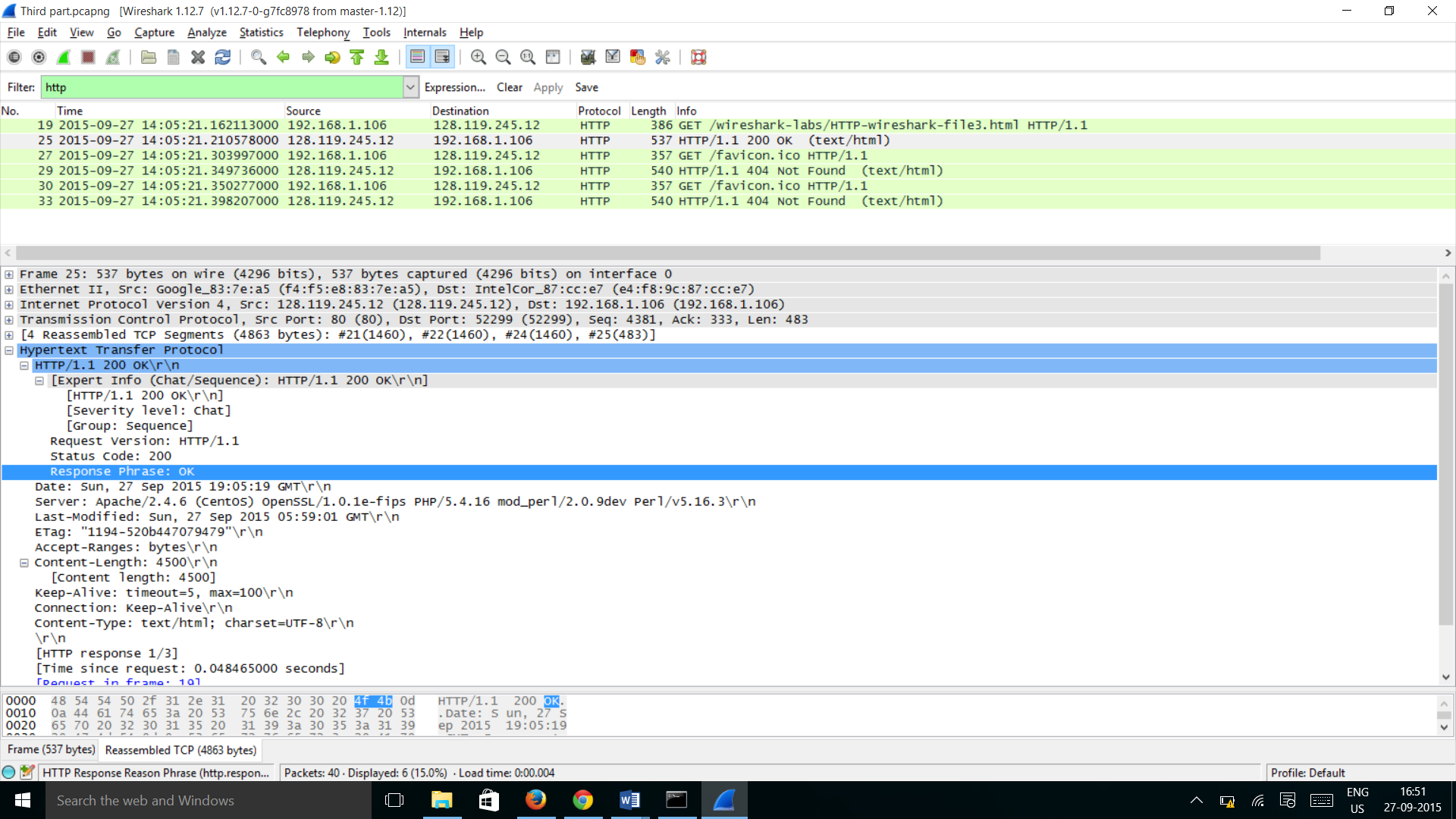
GET Request Message



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

A. 25.

Response



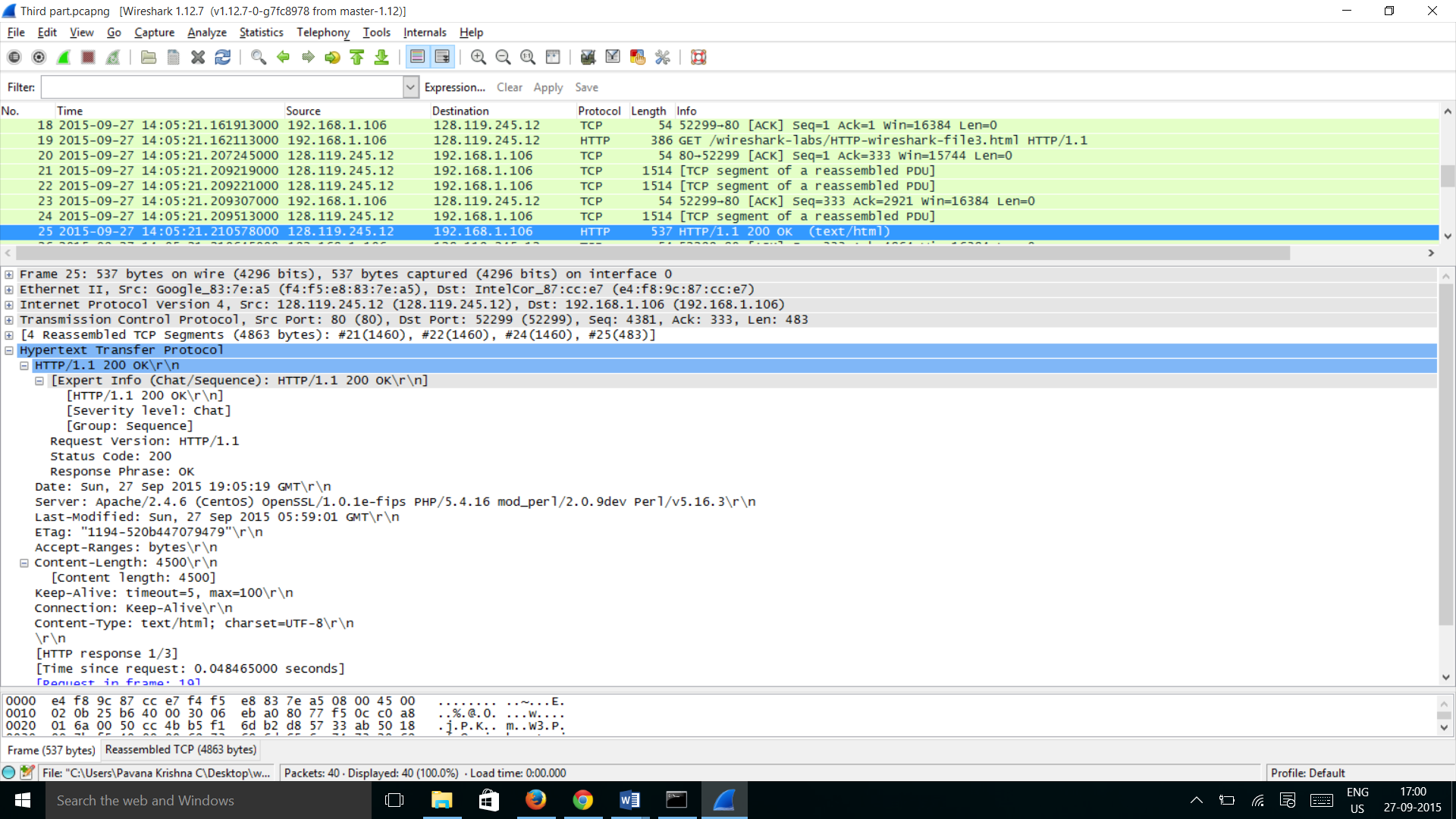
14. What is the status code and phrase in the response?

A. Status Code is 200 and Response Phrase is Ok.

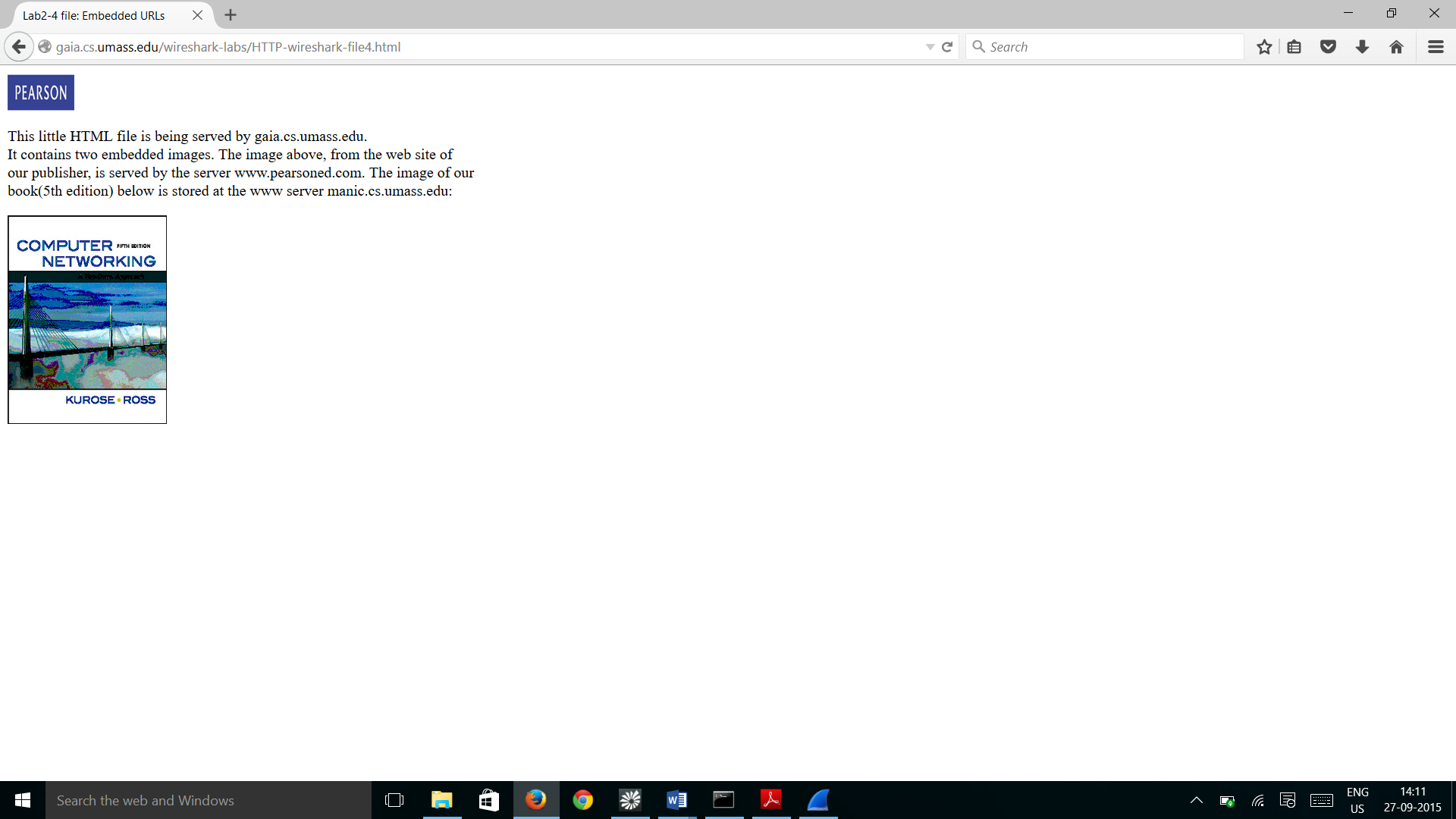
15. How many data-containing TCP segments were needed to carry the single HTTP and the text of the Bill of Rights?

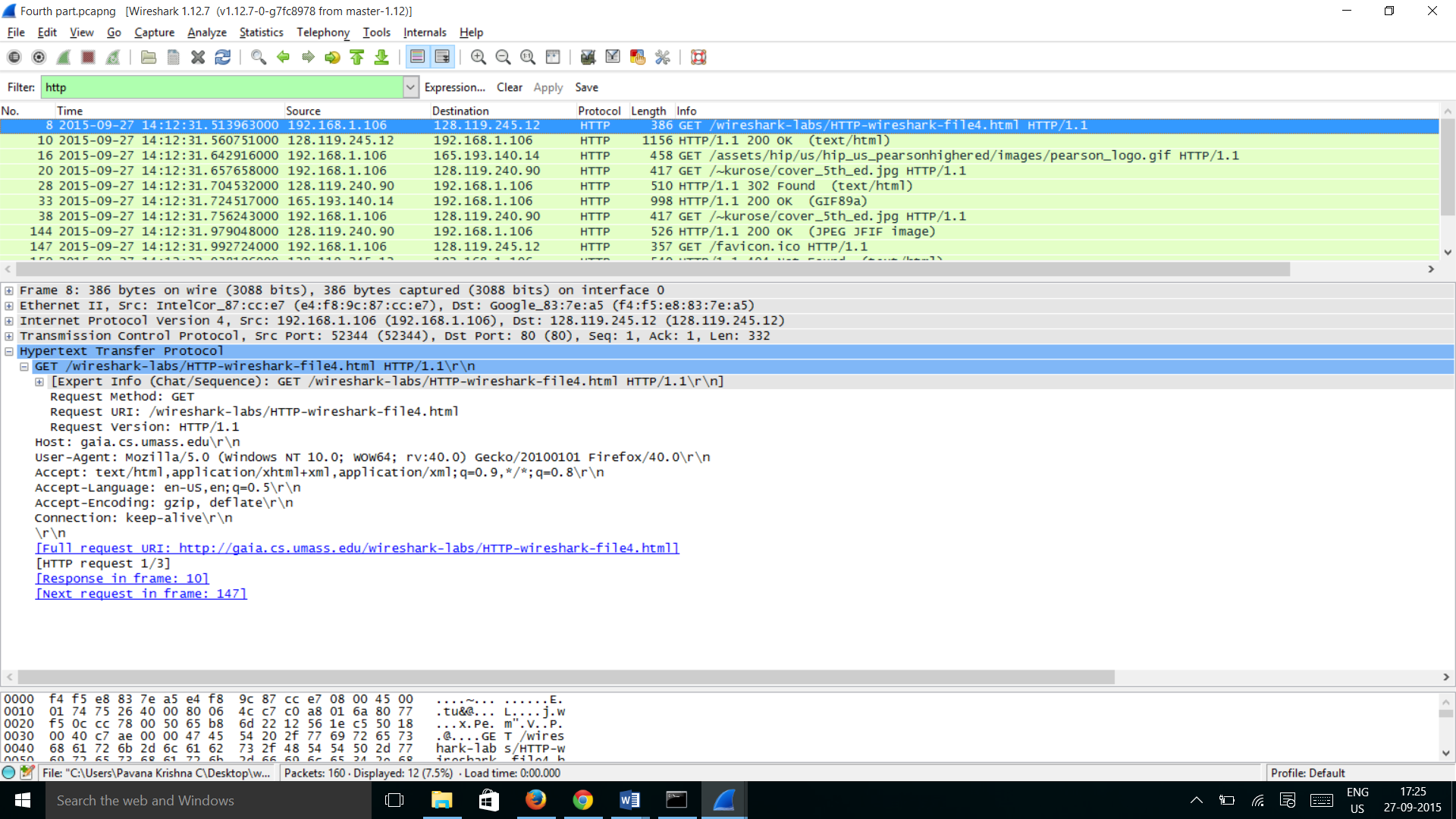
1. 5 data containing TCP segments are needed to carry the single HTTP and text of the Bill of Rights and then reassembled.

5 TCP Segments in between the GET Request and Response



***D) HTML Documents with Embedded Objects0***





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

A. There are 4 HTTP GET request messages sent by the browser and the internet addresses are mentioned below.

128.119.245.12

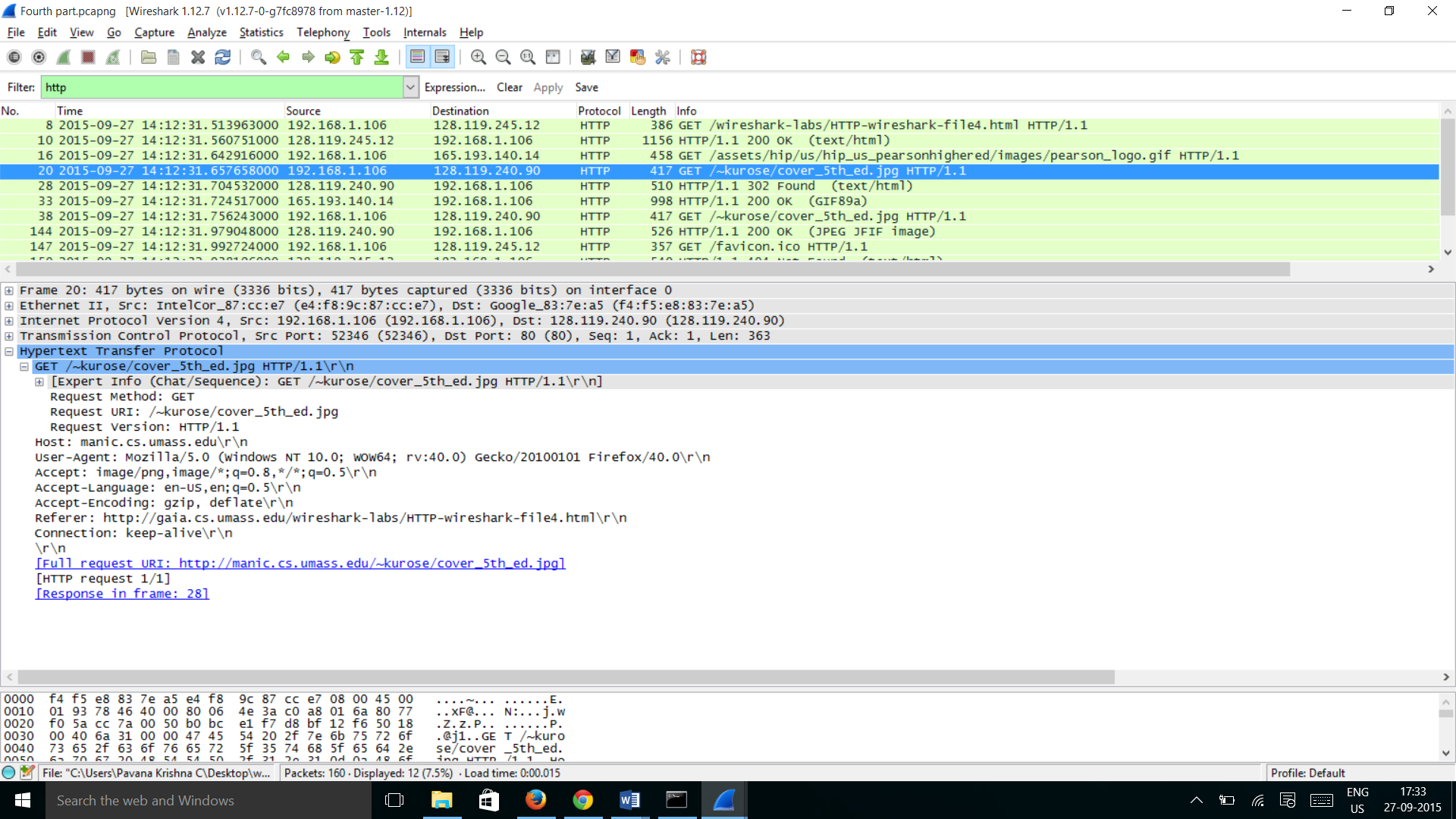
128.119.240.90

165.193.140.14

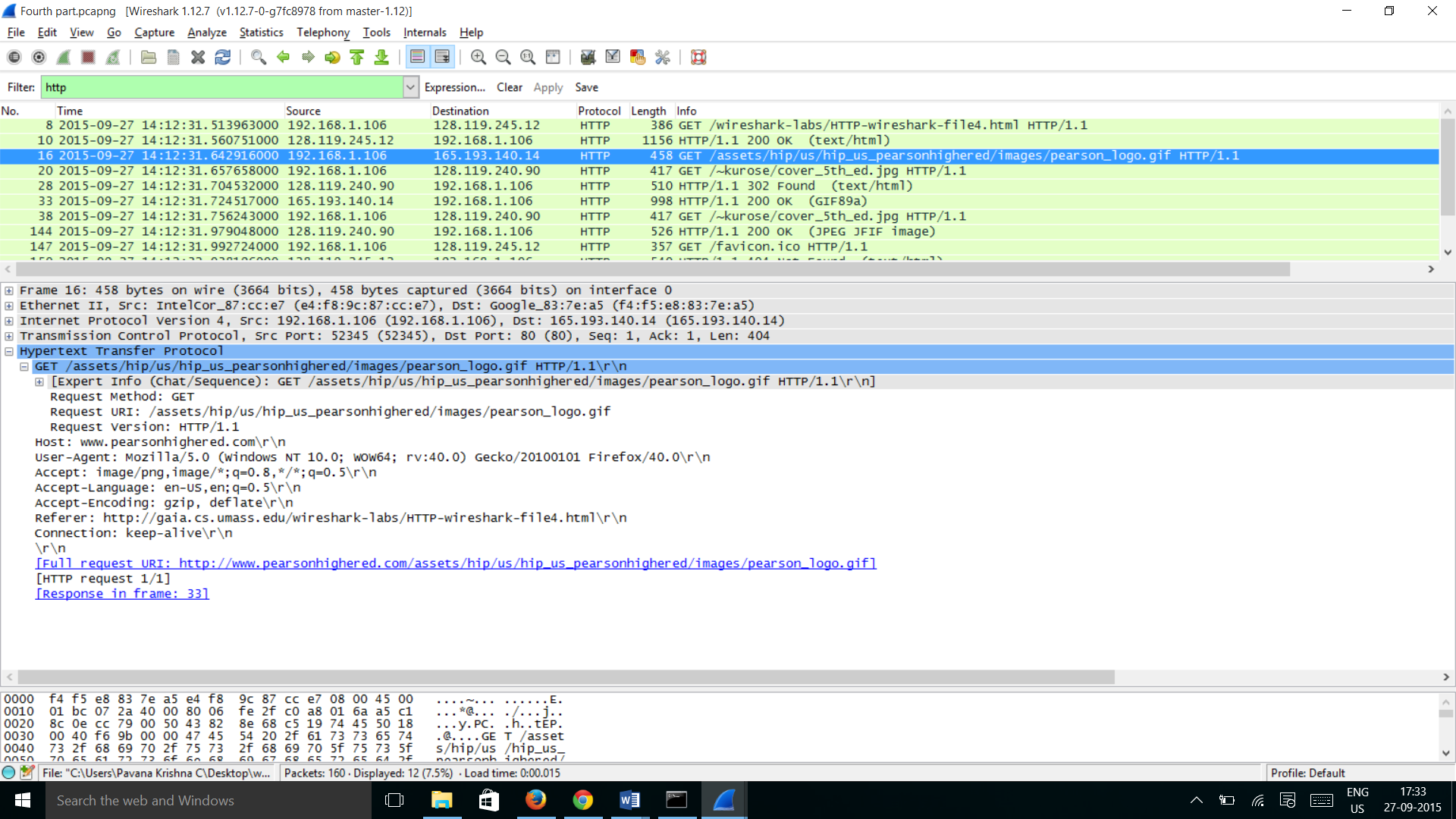
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

A. By verifying the TCP ports we can find out whether the files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

TCP port of First image



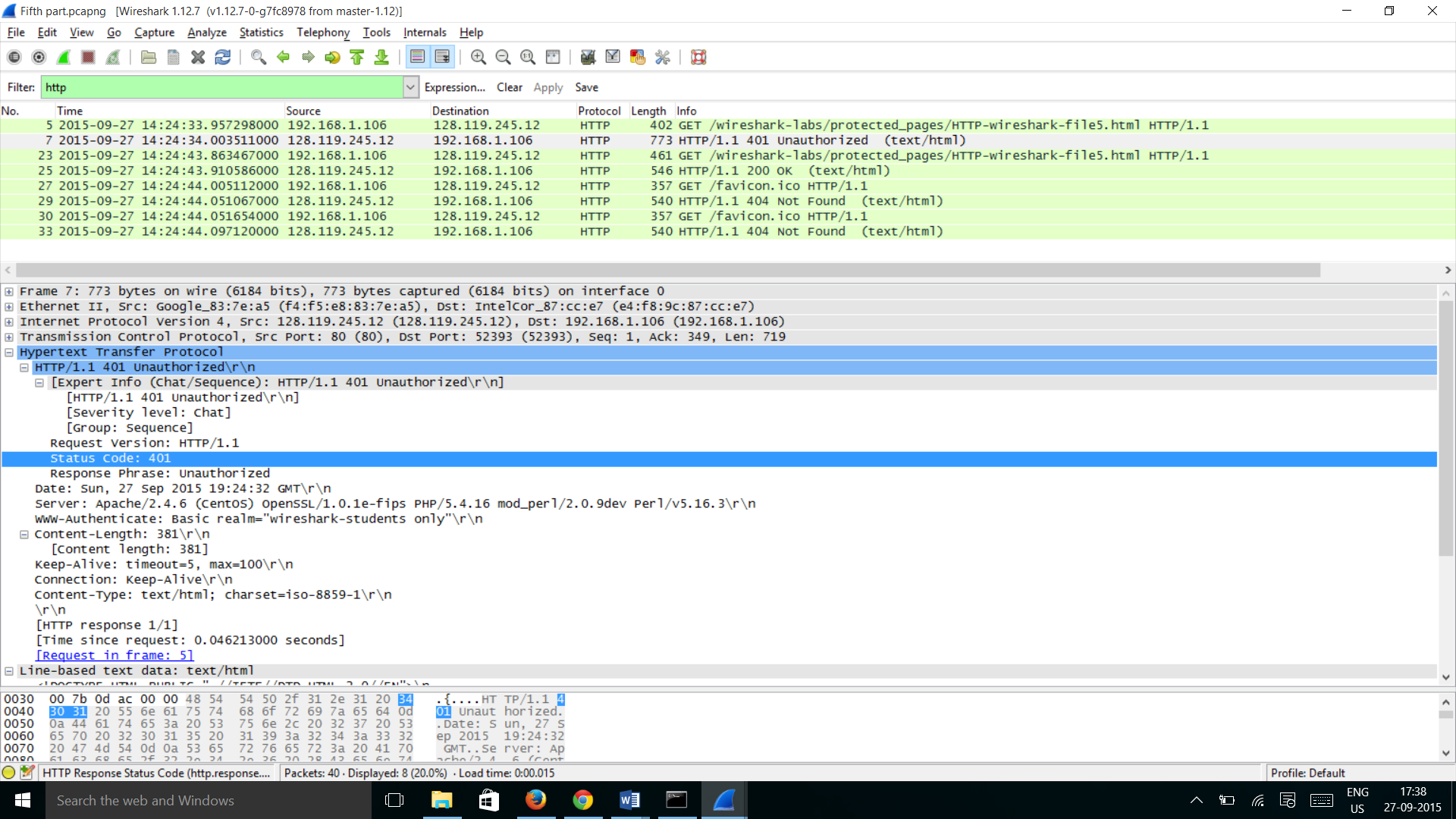
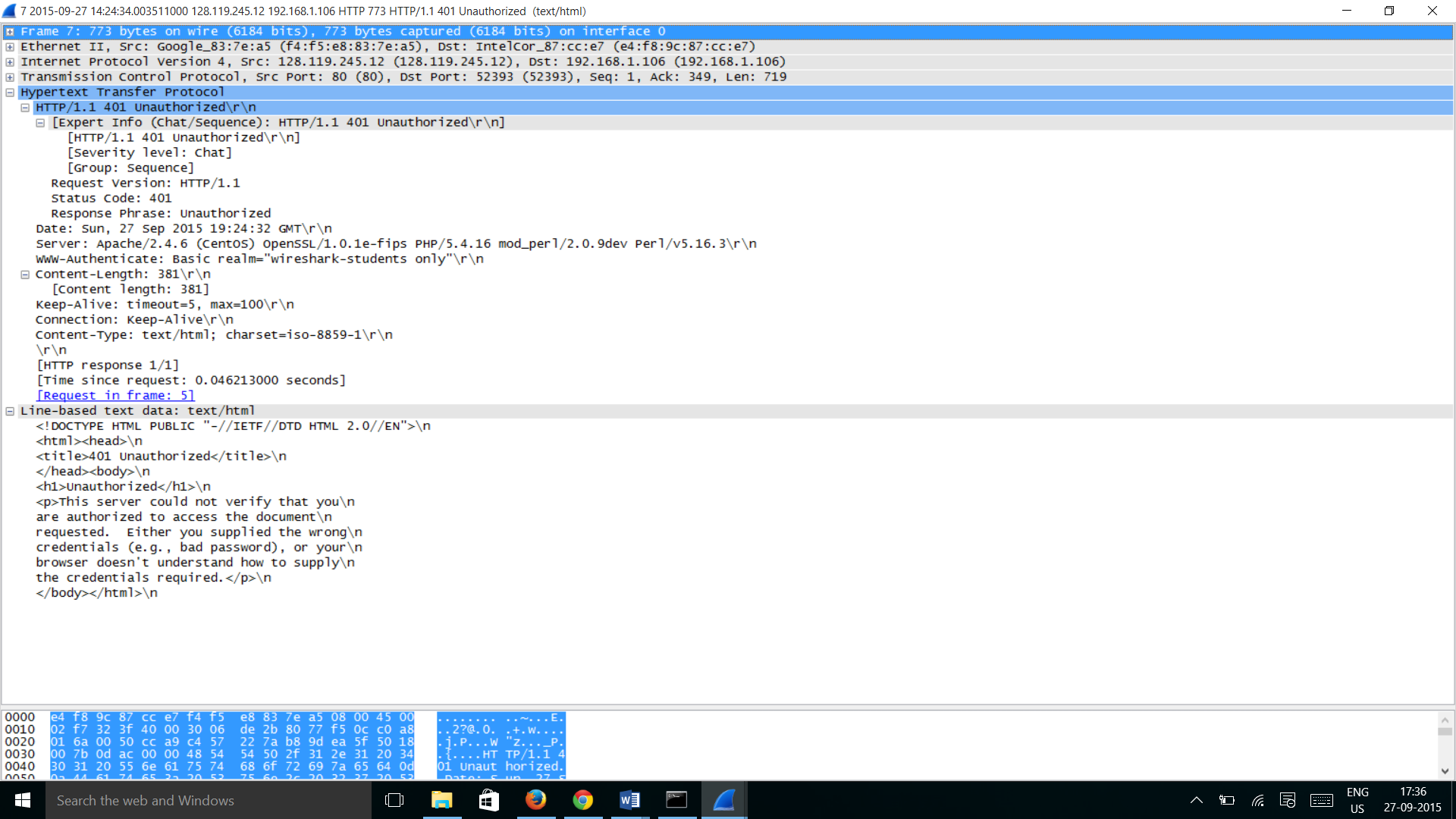
TCP port of Second image



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

A. Status code is 401 and Response phrase is Unauthorized.

First Server Response



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

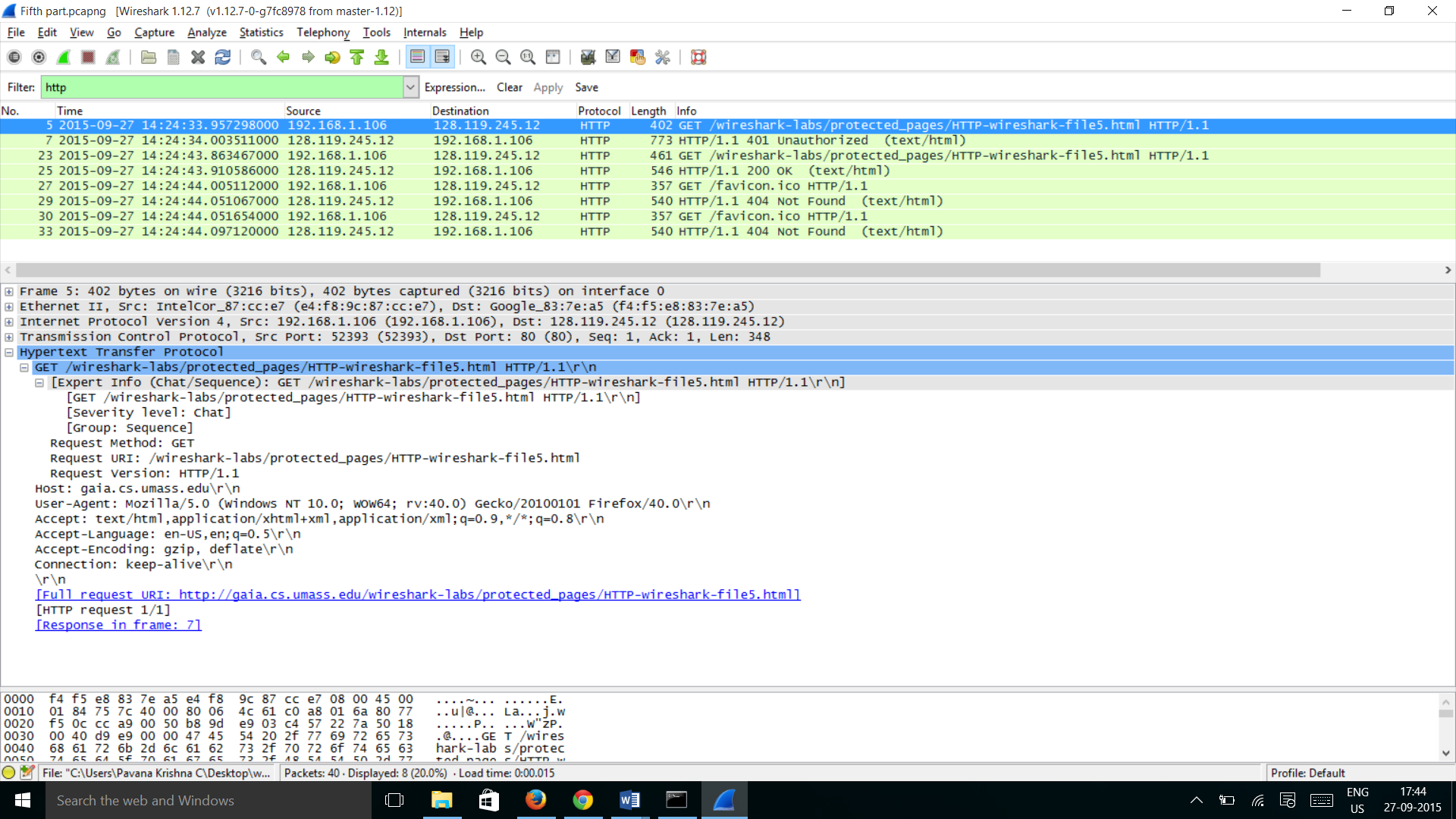
A. Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

Credentials: wireshark-students:network

\r\n

The above mentioned field is added in the second HTTP GET message.

First Get request



Second Get request

