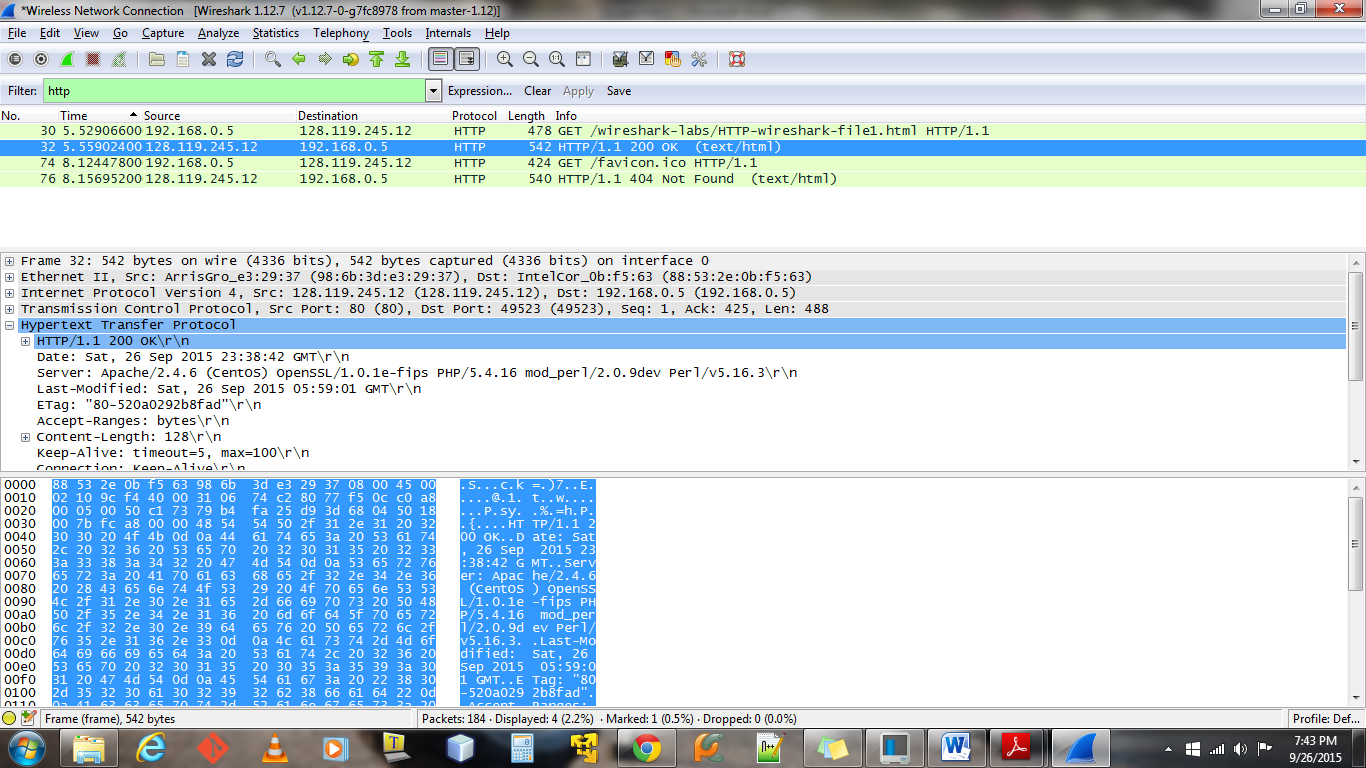
**Assignment 3 - Wireshark Lab: HTTP v6.1**

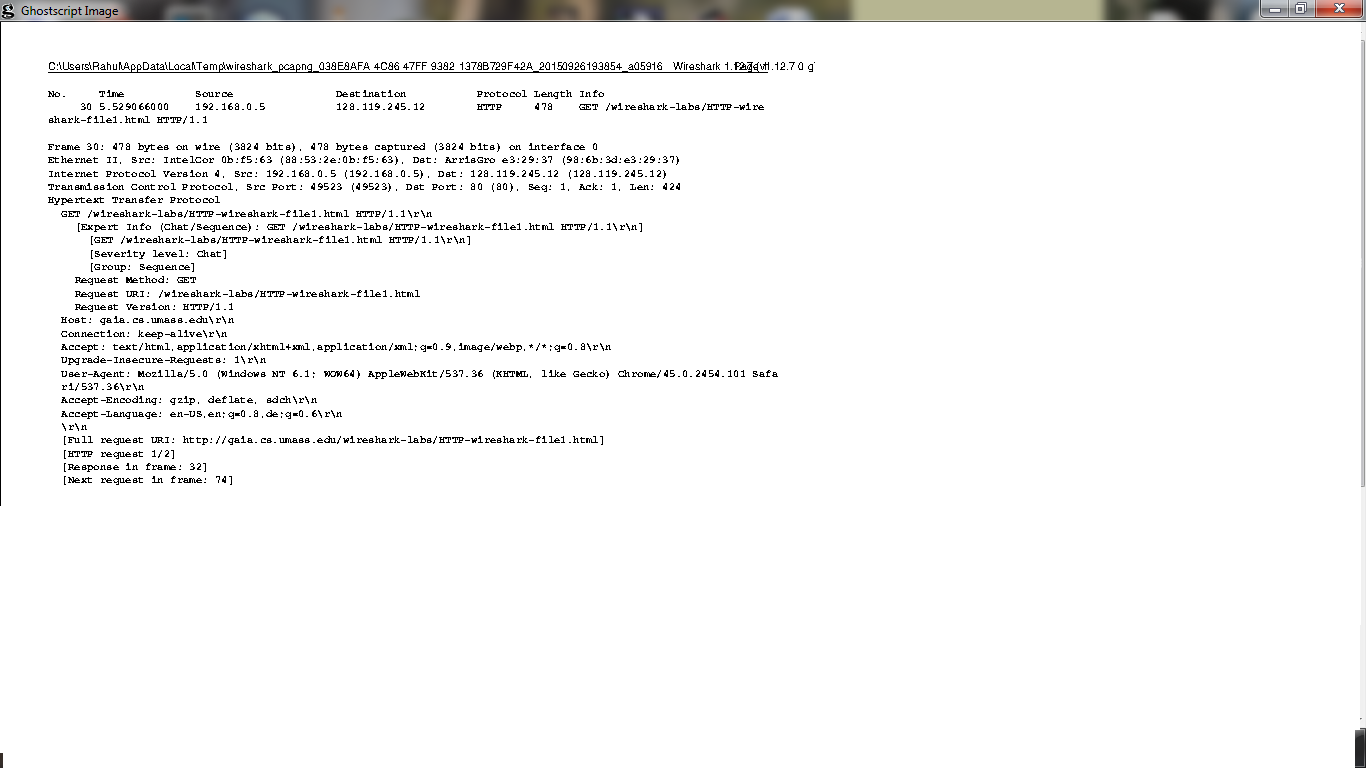
**Answer 1:** **The Basic HTTP GET/response interaction**

****

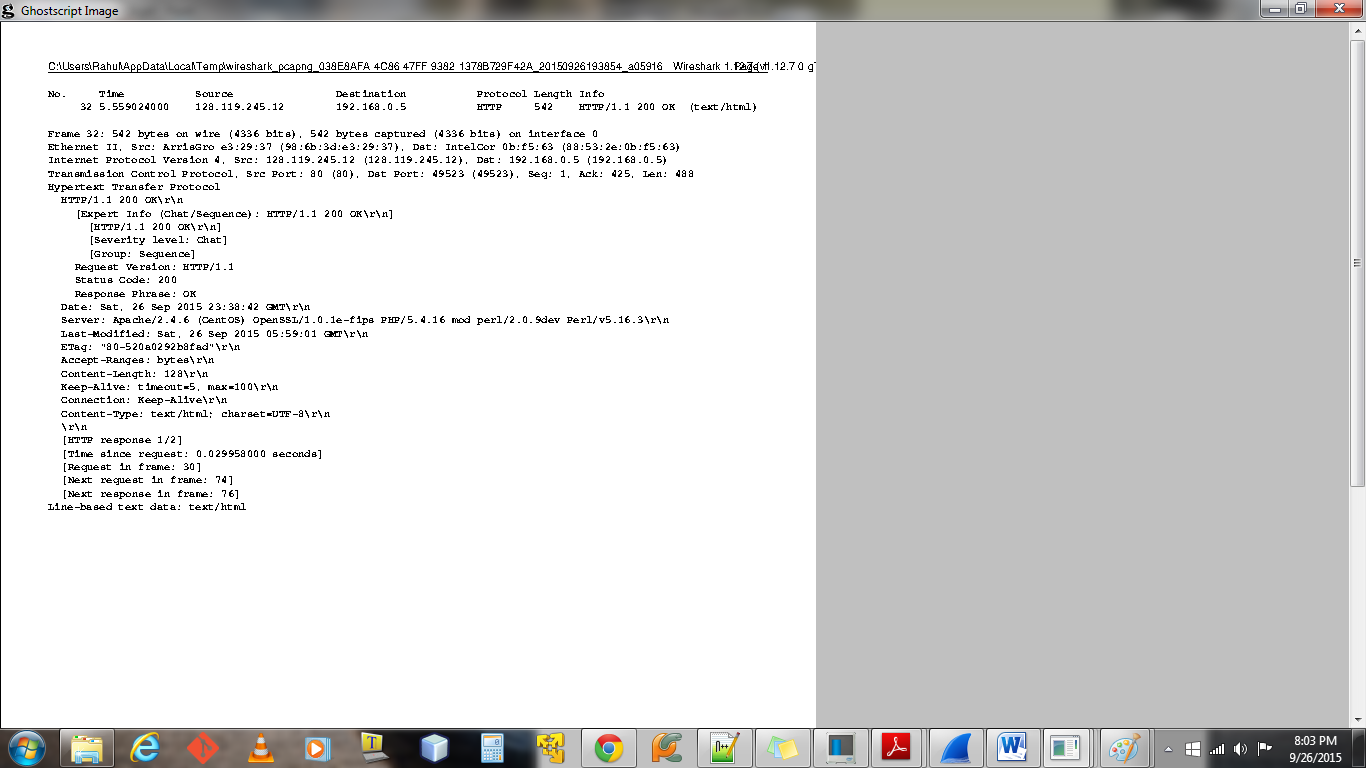
**1a. Browser Output**



**1b. Wireshark Output**



**1c. Request Packet Print**

****

**1d. Response Packet Print**

1. Browser is running **HTTP/1.1** version (from image 1c)



Server is running = **HTTP/1.1** (from image 1d)



1. The languages that the browser can detect are - **en-US ,en, de** (from image 1c) English – US Version, German



1. IP address of the computer is : **192.168.0.5** (from image 1c)



IP address of gaia.cs.umass.edu server : **128.119.245.12** (from image 1c)



1. Status code returned from server: **200** (from image 1d)



1. The HTML File retrieved from the server was last modified at **Sat, 26 Sep 2015 05:59:01 GMT** (from image 1d)

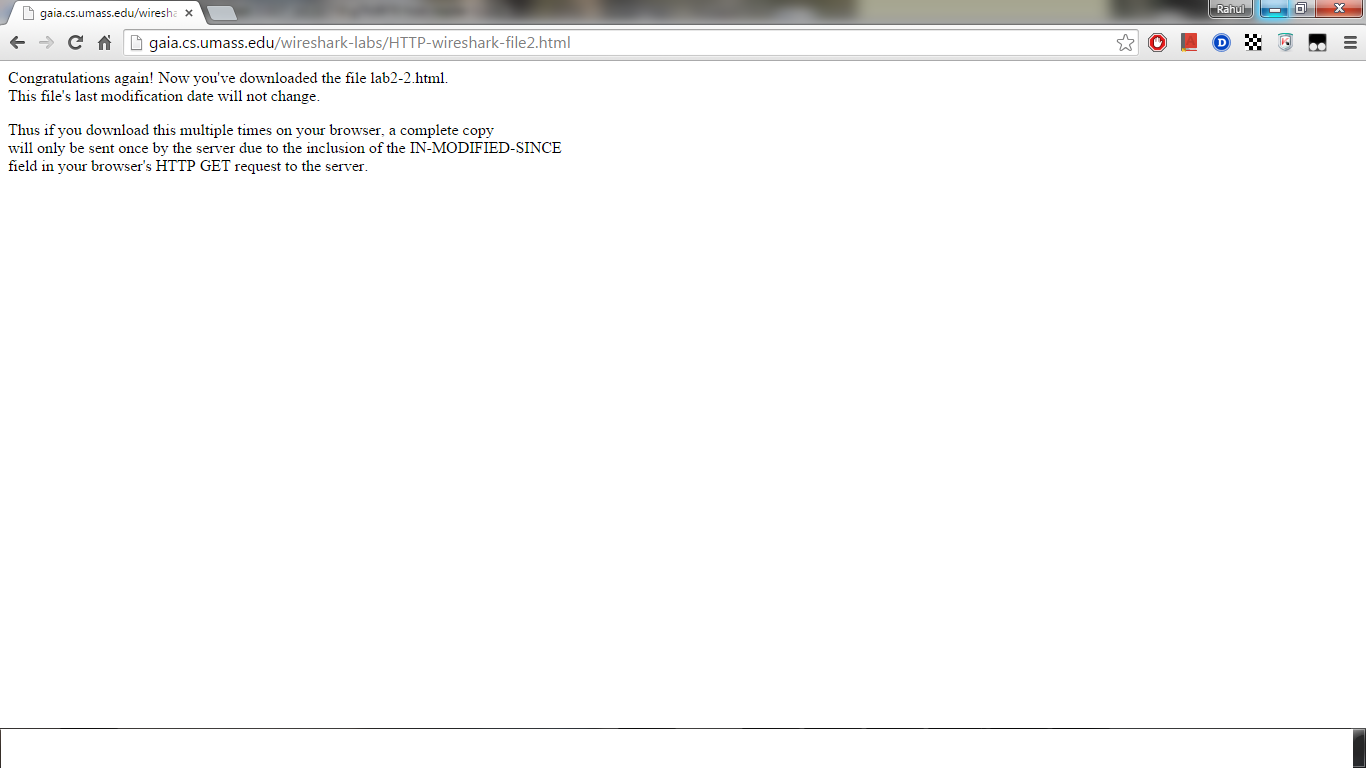


1. The number of bytes of content returned are : **128**

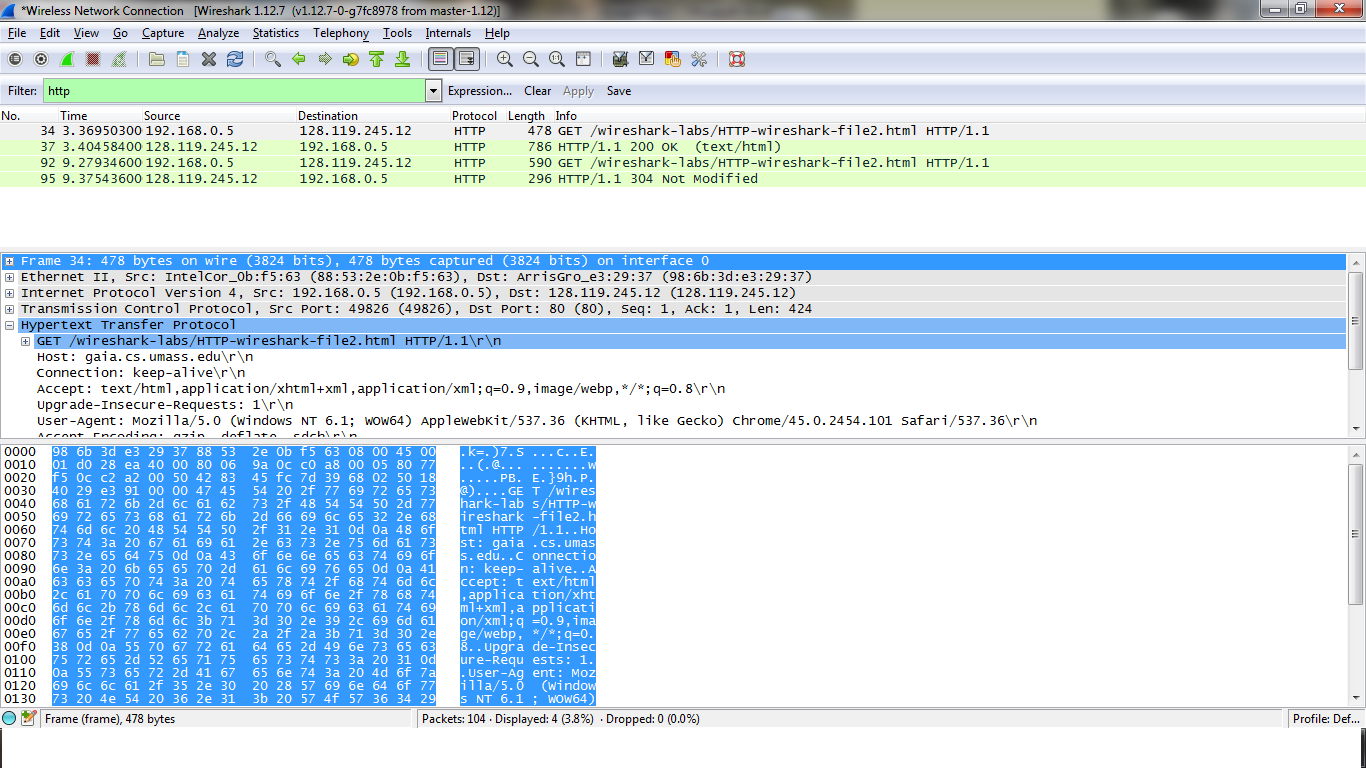


1. No extra headers are found that is not present in the packet content window.

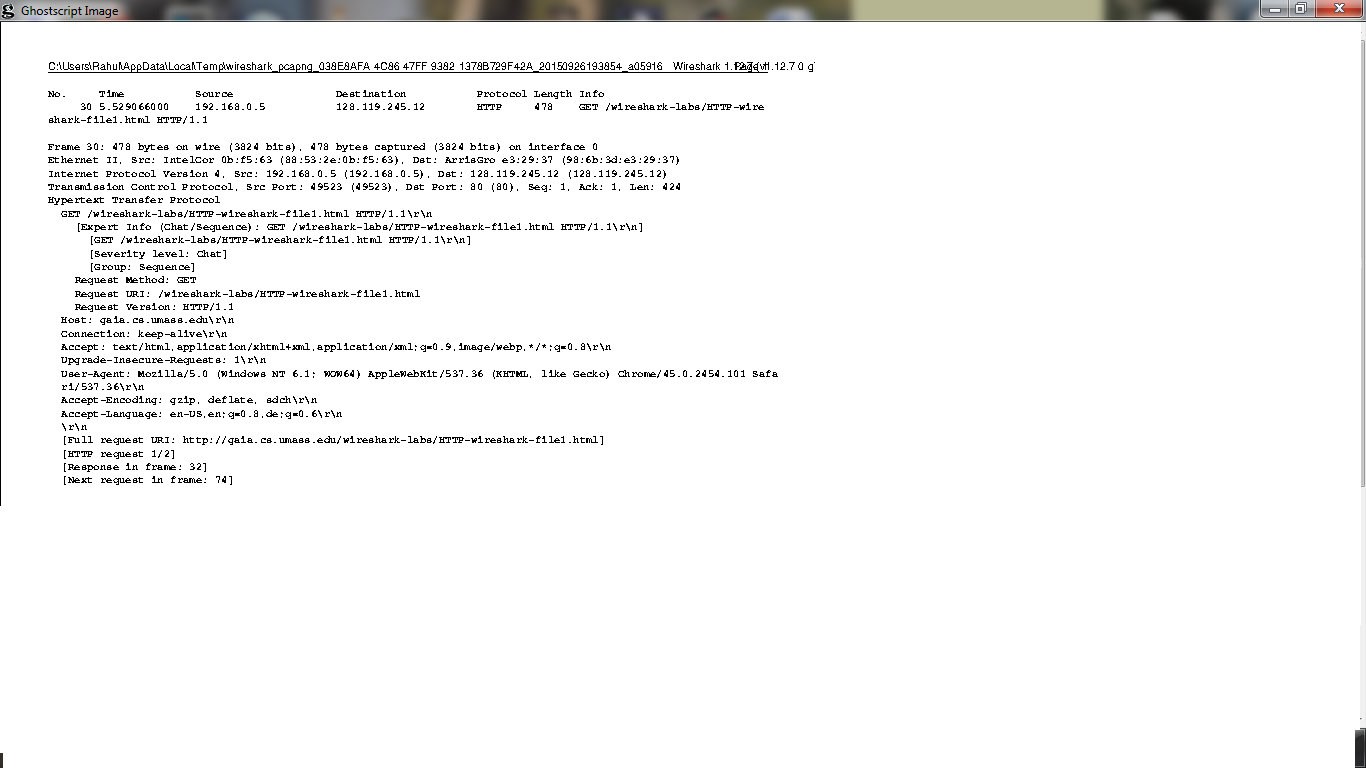
**Answer 2:** **The HTTP CONDITIONAL GET/response interaction**



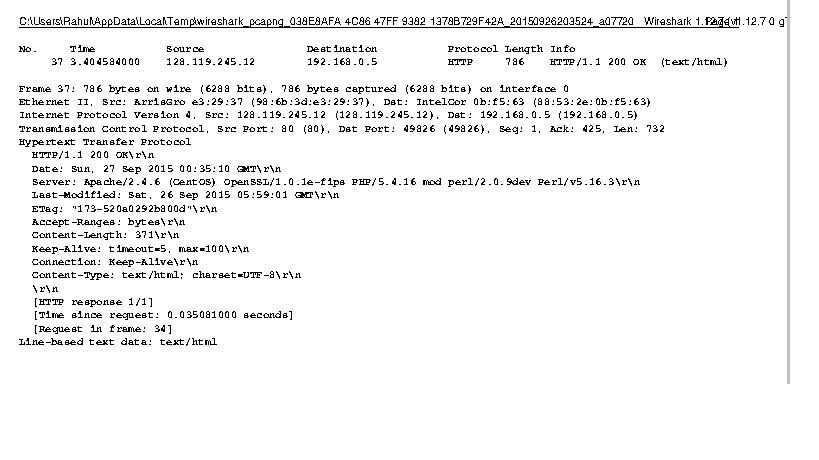
**2a. Browser Output**

****

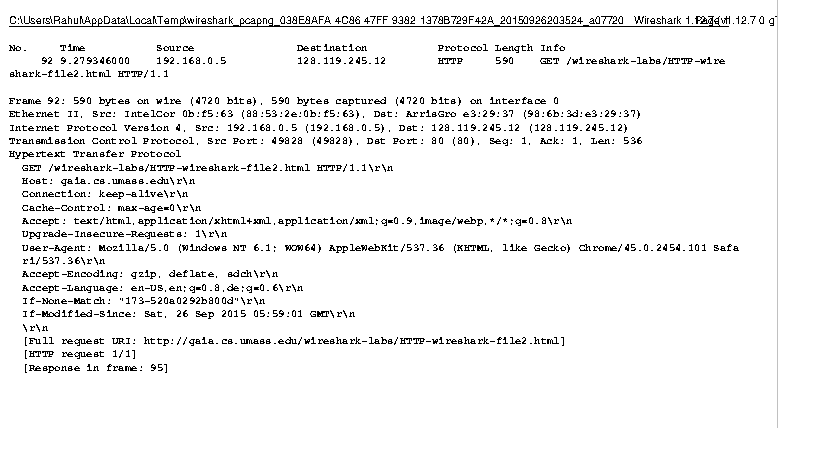
**2b. Wireshark Output**



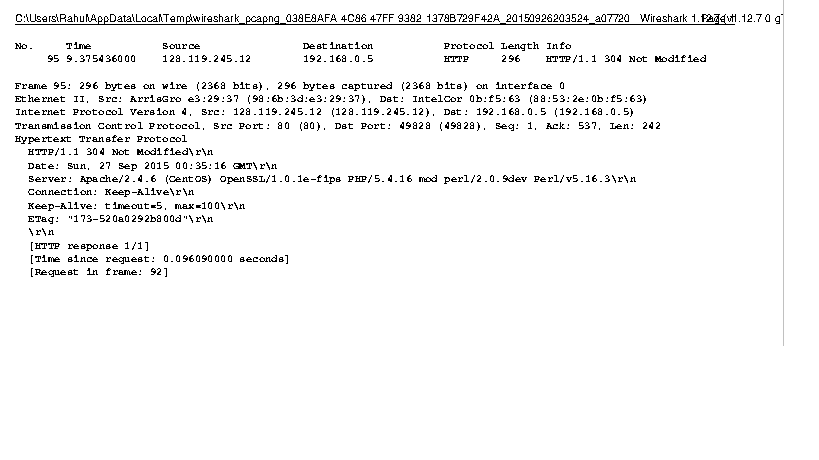
**2c. First Get Request to server**

****

**2d. First Response from server**

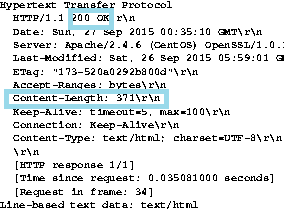


**2e. Second Get request to server**



**2f. Second Response from server**

1. From the above image (2c) it’s clear that there is **no** IF-MODIFIED-SINCE field is present in the first GET Request.
2. Yes server returns the contents of the file. It can be known from the **status code 200** and the **content –length 371** from image (2d)



1. From the image (2e) it’s clear that the **field IF-MODIFIED-SINCE is present** and the value is: **Sat, 26 Sep 2015 05:59:01 GMT**

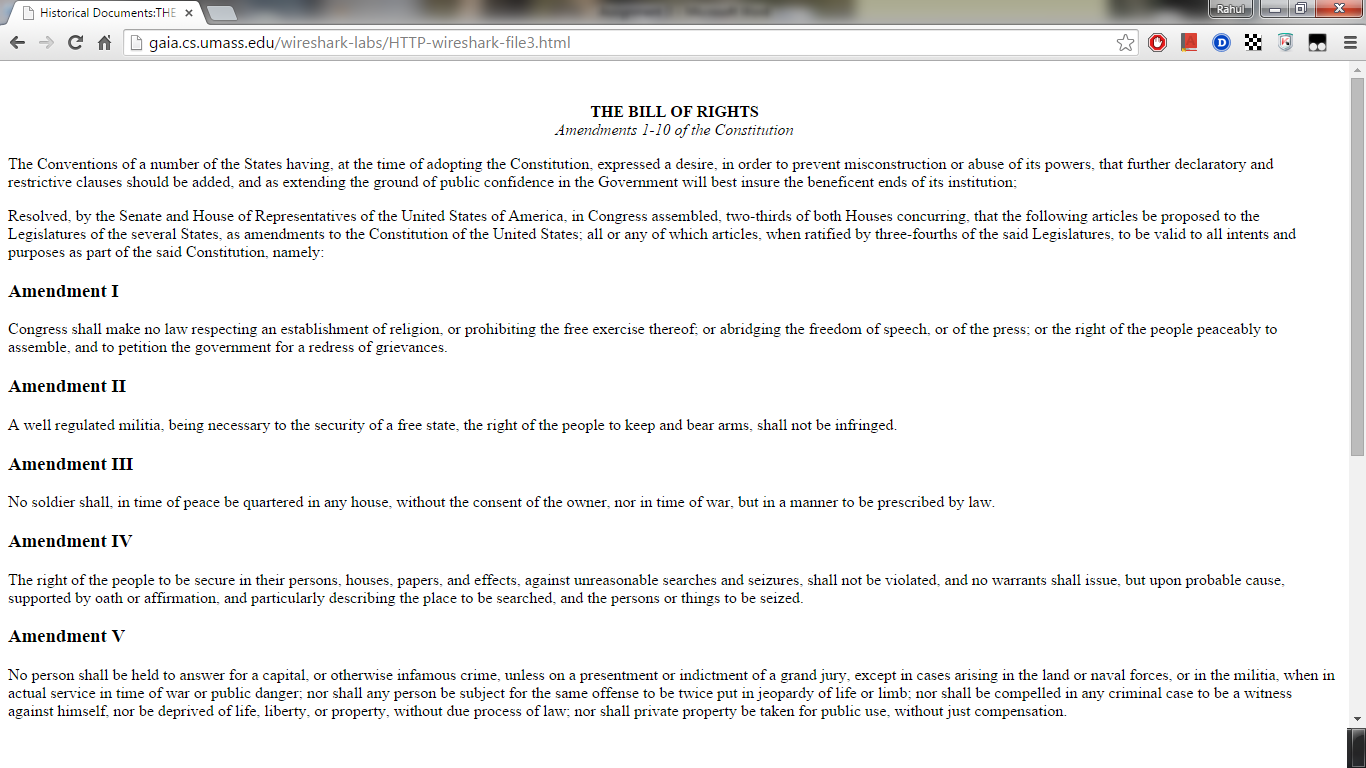


1. From the image (2f) the HTTP Status code is 304 and phrase is **NOT MODIFIED**

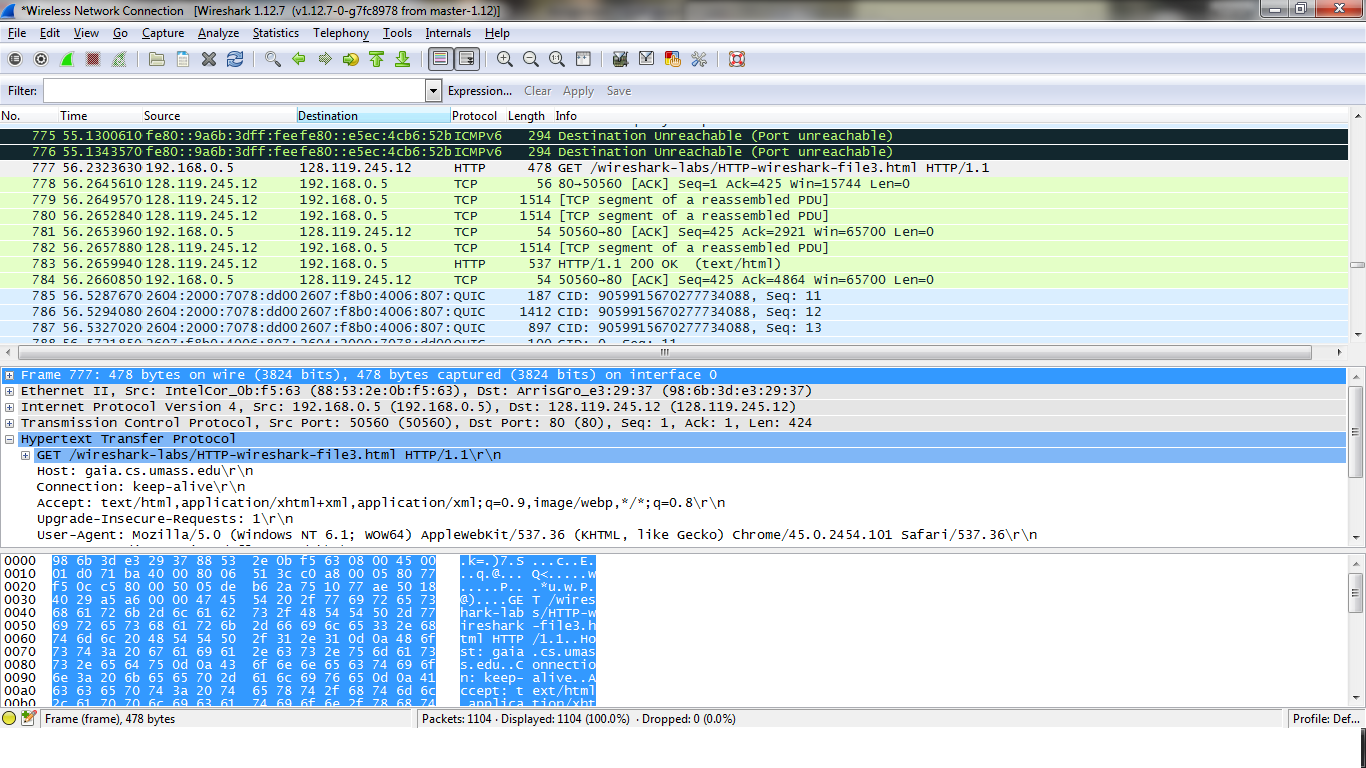


The server did not explicitly return the contents of the file .The server noticed that the file has not changed since **26 Sep 2015 05:59:01 GMT**, hence sent a **304** response code with phrase **NOT MODIFIED**

**Answer 3:** **Retrieving Long Documents**

****

**3a. Browser Output**

****

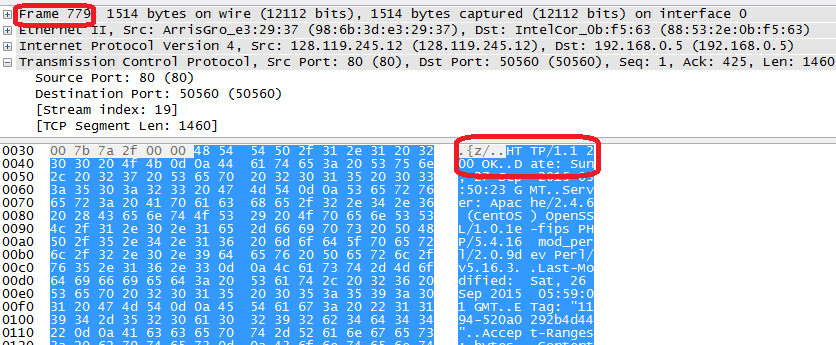
**3b. Wireshark Output**

1. **One** GET Request message is sent by the browser. The packet number that contains the GET message for the bill of rights is **777**



1. The packet number of the packet that contains the status code and the phrase associated with the response to the HTTP GET request is **779**



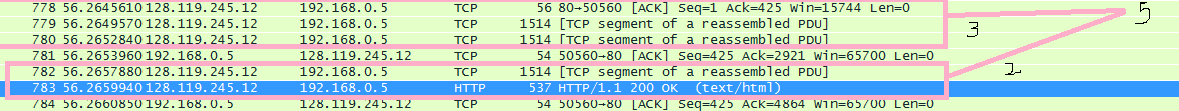


1. The status code is **200** and the phrase is **OK** in the response

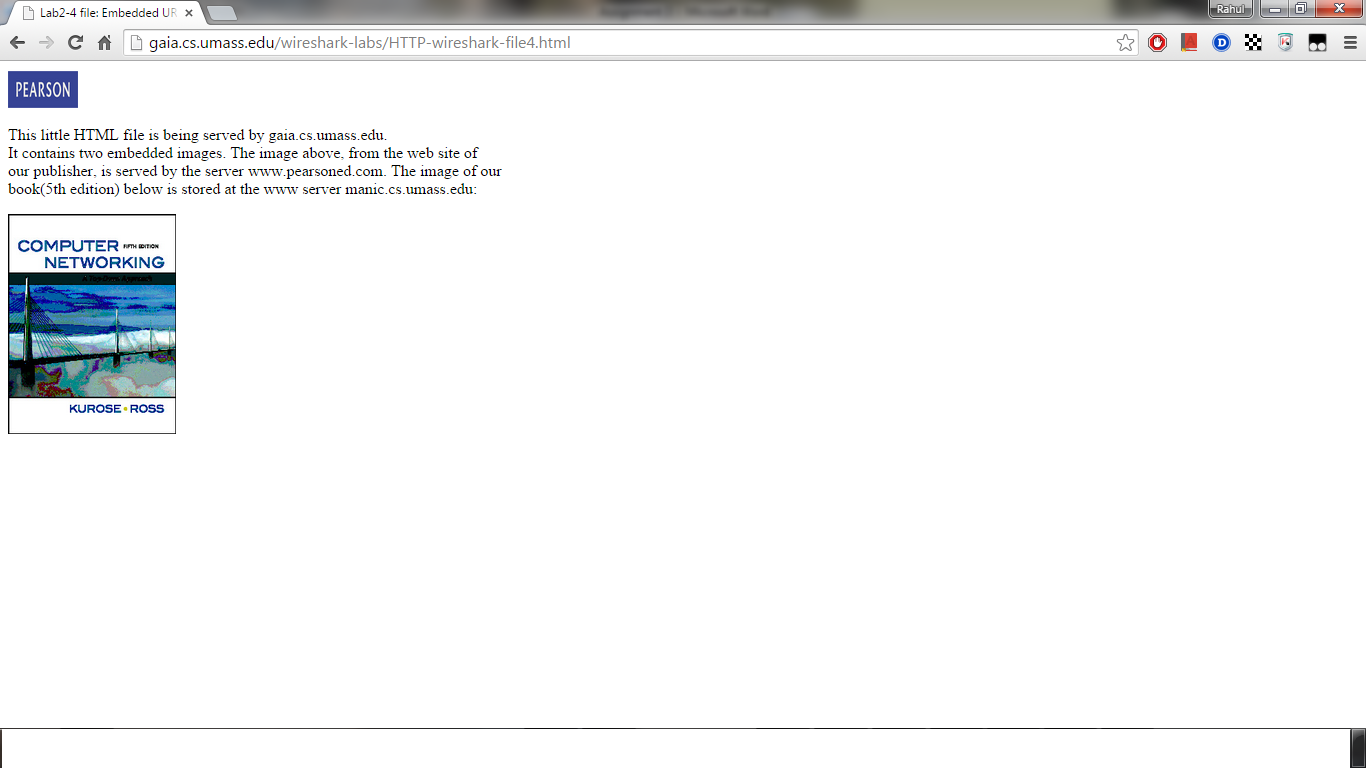




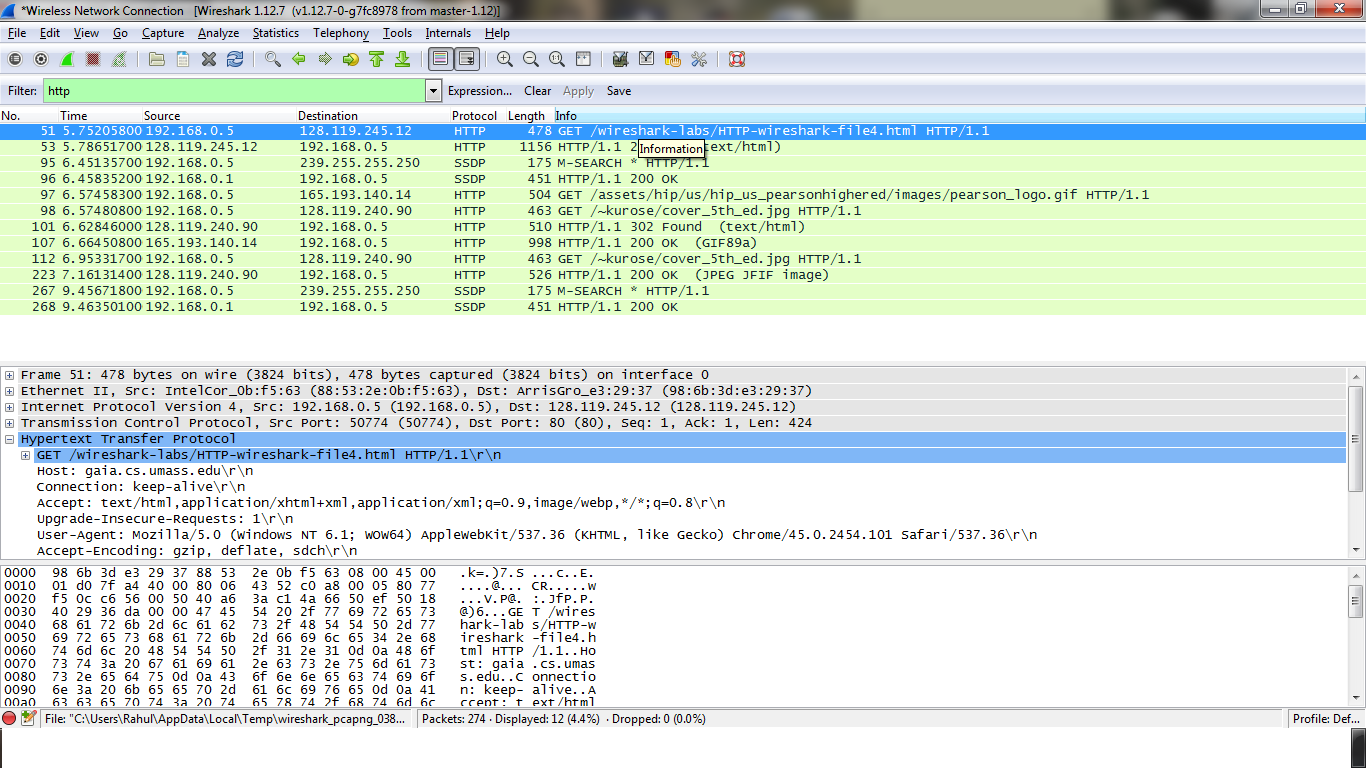
1. The number of data containing TCP Segments to carry the single HTTP response and the text of bill of rights is **5**



**Answer 4:** **HTML Documents with Embedded Objects**

****

**4a. Browser Output**

****

**4b. Wireshark Output**

1. The HTTP GET Request messages sent are **4.** They are -
2. GET Request for the **HTTP-wireshark-file4.html** to **gaia.cs.umass.edu (Address : 128.119.245.12)**



1. GET Request for the **pearson\_logo.gif** to [**www.pearsonhighered.com**](http://www.pearsonhighered.com) **(Address: 165.193.140.14)**



1. GET Request for the **cover\_5th-ed.jpg** to **manic.cs.umass.edu (Address: 128.119.240.90)**



1. Since the GET Request for **pearson\_logo.gif** to [**www.pearsonhighered.com**](http://www.pearsonhighered.com)returns **302** page moved status, there is another redirect GET Request for **pearson\_logo.gif** to **caite.cs.umass.edu (Address: 128.119.240.90)**



1. The two images were downloaded in parallel.

The first GET request was sent at **6.57458300**



The second GET request was sent at **6.57480800** without waiting for 200 status code for the first GET request.



This means both the requests were sent in parallel and each response was handled by the browser asynchronously as the browser did not wait for first GET Request’s response before sending the next GET Request.

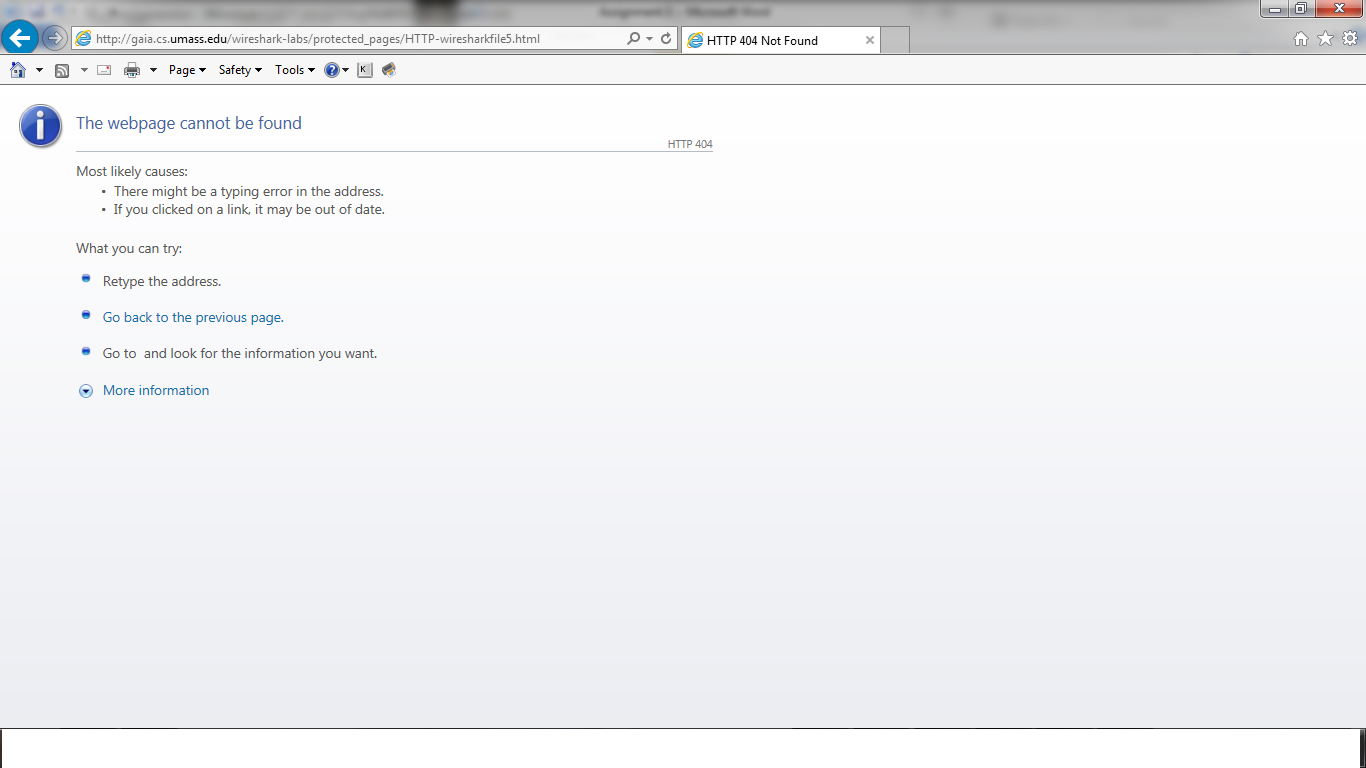
The first response was received at **6.62846000** which is the response for the first GET Request



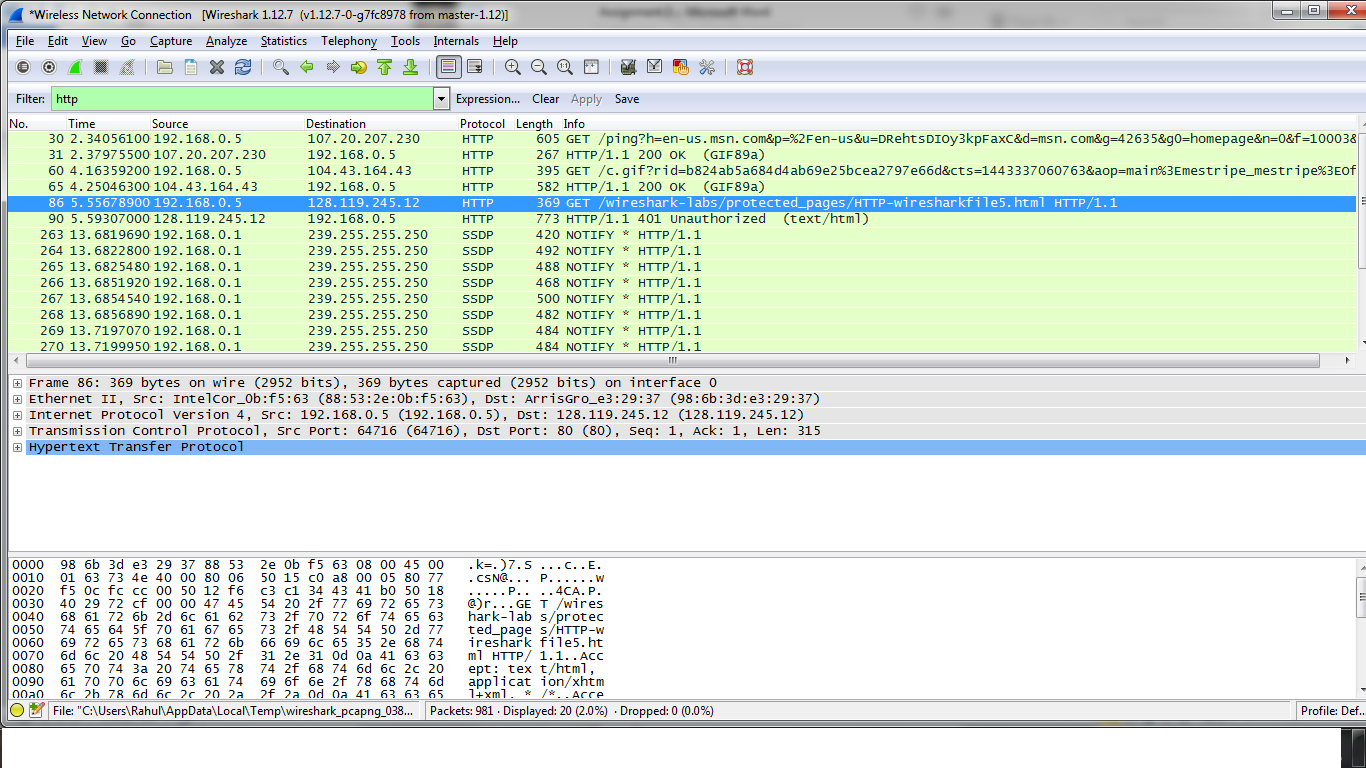
The second response was received at **6.66450800** which is the response for the second GET request.



**Answer 5:** **HTTP Authentication**

****

**4a. Browser Output**



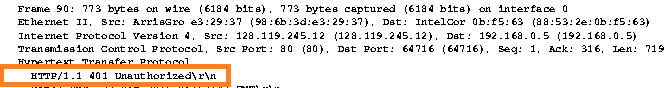
**4b. Wireshark Output**

1. The server’s response to the initial HTTP GET message is –

Status Code – **401**

Status Phrase - **Unauthorized**





1. The new field included in the HTTP GET message is the **Authorization** Field





