Laraib Akhtar

21l-5294

Lab 3

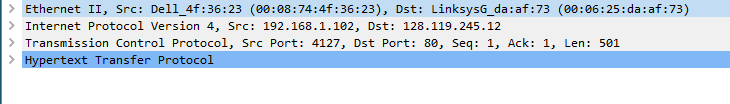
Bcs-5b1

In-Lab Statement 1: Analyzing HTTP Protocol

**Use the http-ethereal-trace-1 packet trace to answer the questions below apply the “http” filter**

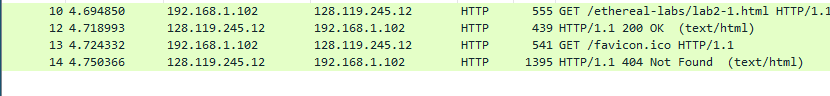
1- List up to 4 different protocols that appear in the protocol column in

the unfiltered packet-listing window.



2- How long did it take from when the HTTP GET message was sent until

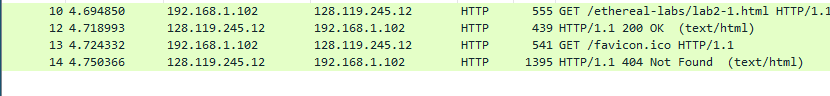
the HTTP OK reply was received?



time = 4.750366

3- Was the second Get Request successful? How can you tell it from the

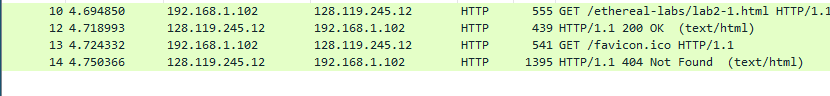
corresponding response packet?



Response code of second get request is 404 which is not successful.

4. Is your browser running HTTP version 1.0 or 1.1? What version of

HTTP is the server running?



http version 1.1

5. What languages (if any) does your browser indicate that it can accept

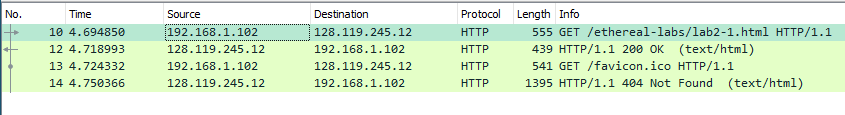
to the server?



En-us

6. What is the IP address of the gaia.cs.umass.edu server and your

computer?



Computer: 192.168.1.102

gaia.cs.umass.edu: 128.119.245.12

7. What is the MAC address of the server and your computer?



Src: computer

Dst: server

8. What is sending and receiving Port Number? What does Port No. 80

represents?

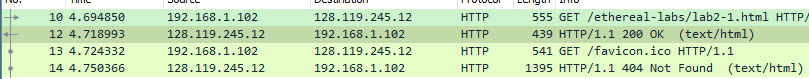


Source: sending

Destination: receiving

Port 80 represents an http request

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

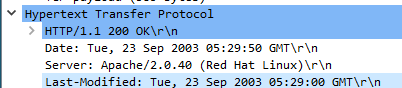


Status code to 1st get request: 200 OK

Status code to 2nd get request: 404 Not Found

10. When was the HTML file, that you are retrieving, last modified at

the server?



11. How many bytes of total packet content are being returned to your

browser?

Total packet content to first get : 439 bytes

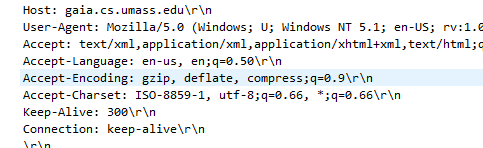
Total packet content to second get : 1395 bytes

Total: 1834 bytes

**Use the http-ethereal-trace-2 packet trace to answer the questions below and apply the “http” filter**

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?



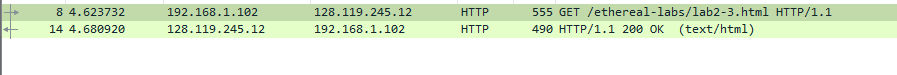
No

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

the contents of the file? How can you tell from the Packet Bytes Window?

In-Lab Statement 2 : Analyzing HTTP Protocol

5. How many HTTP GET request messages did your browser send?



1

6. Which packet number in the trace contains the GET message for The Bill

of Rights?



No. 8

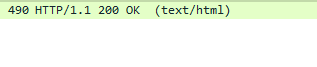
7. Which packet number in the trace contains the status code and phrase

associated with the response to the HTTP GET request?



No. 14

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



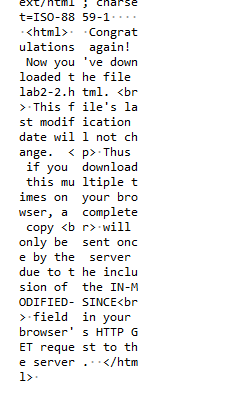
9. How many data-containing TCP segments were needed to carry the single

HTTP response and the text of the Bill of Rights? What are the numbers of

those packets?



4 segments. 10,11,13,14



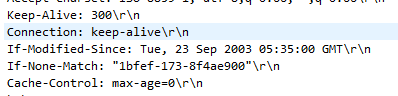
The explicit data has been returned

3. 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? What is meant by this information?



Yes. It shows the last date and time of modification made.

4. 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 your answer



Status code: 304 Not modified.

No it did not explicitly return the contents of the file since they were not modified so there was no need to send them again

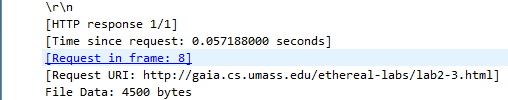
In-Lab Statement 3: Trick Question

What is the length of the text for The Bill of Rights in bytes? How do

you justify this length of text when your Response Packet Size is only

490 bytes? Give complete explanation how the length of text in various

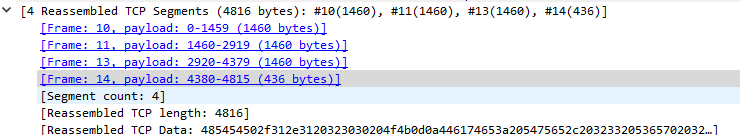
packets add up to a total of 4500 Bytes.



It is 4500 bytes. However, response packet is only



490 bytes. This is because the file was divided into multiple TCP segments which added to the file size of upto 4816 bytes.



Although the file size is of 4500 bytes which consists of Data, However, the additional 316 bytes comes from the tcp headers. There were a total of 4 headers each header containing 79 bytes.

