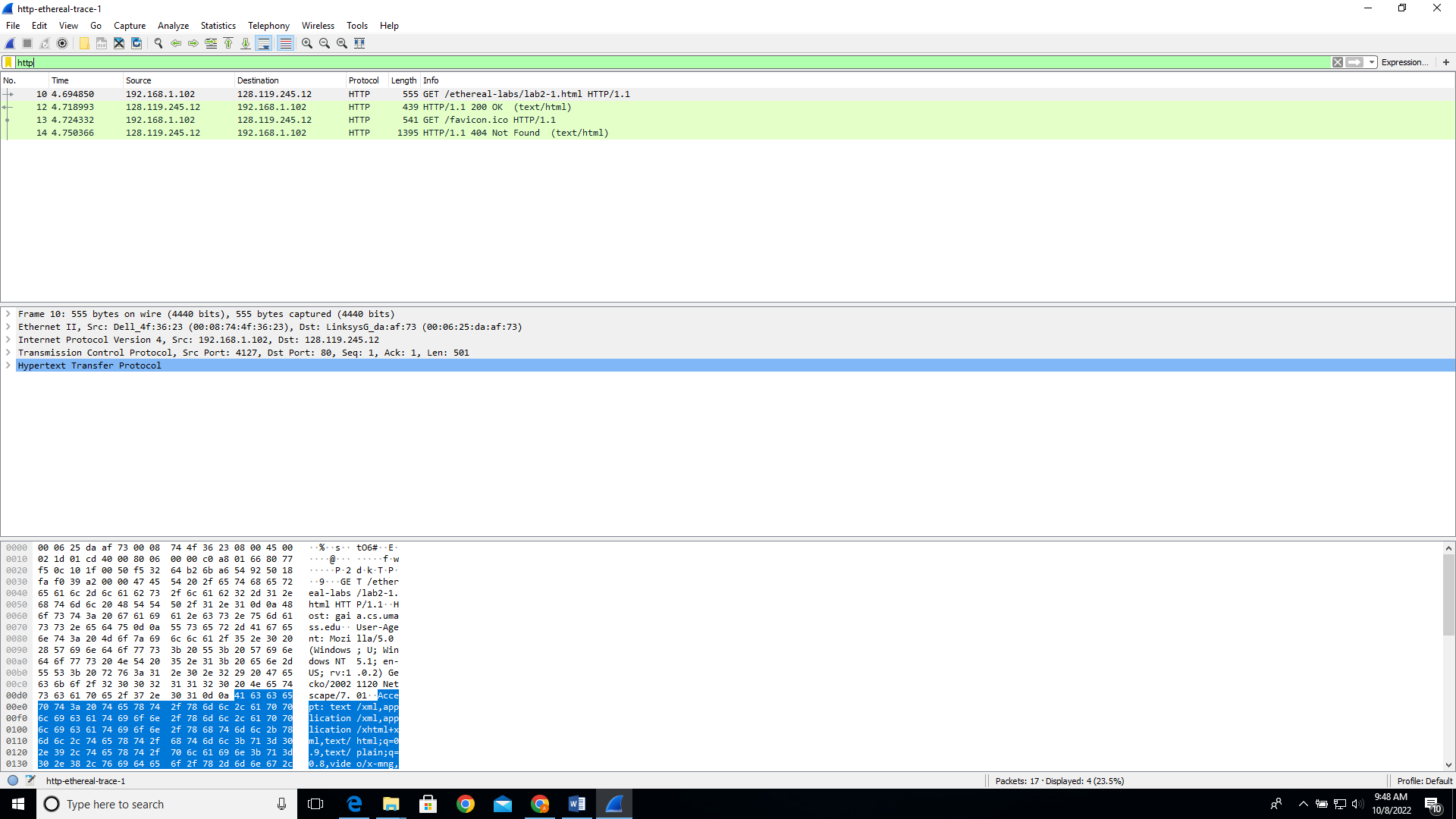
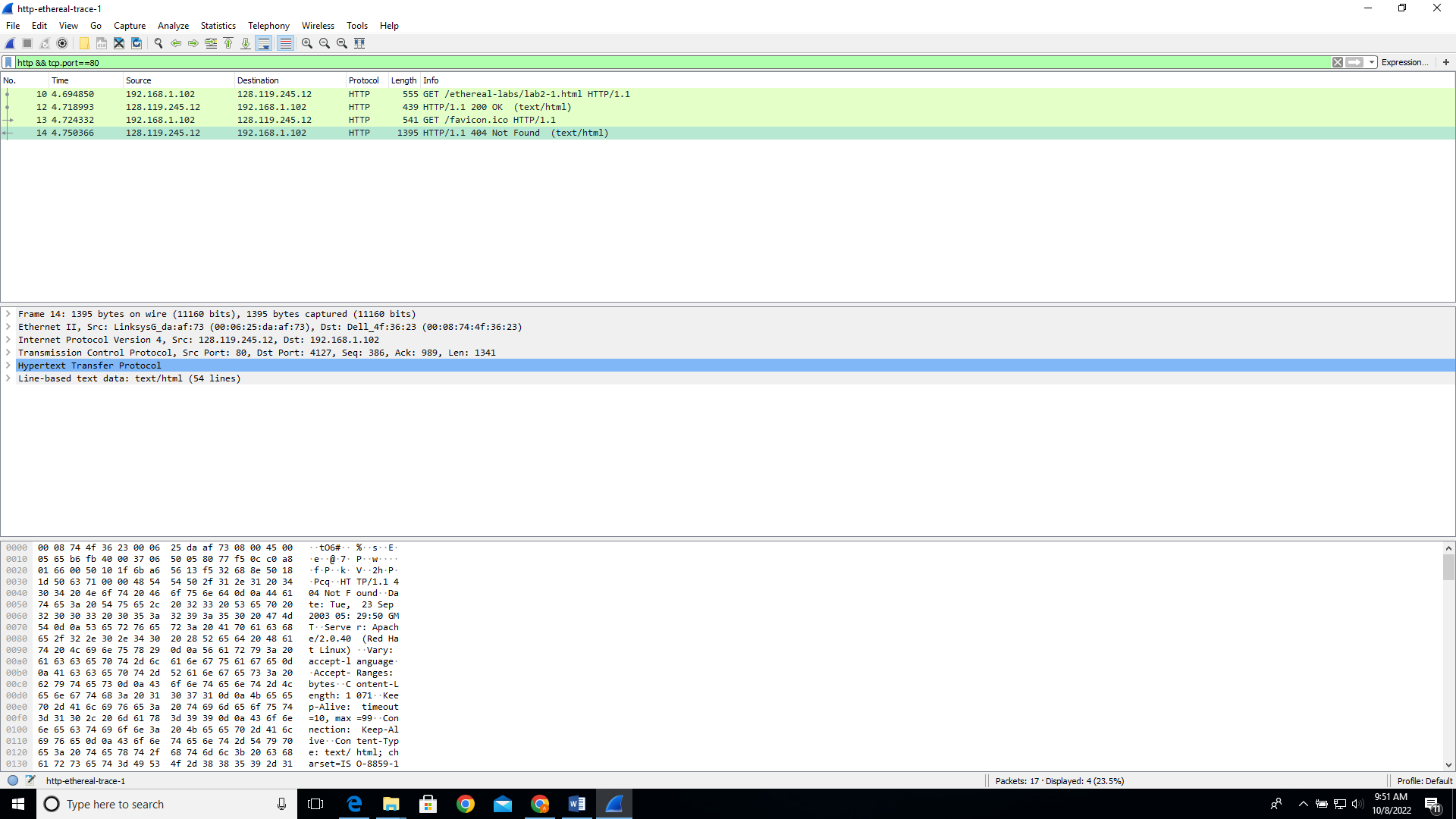
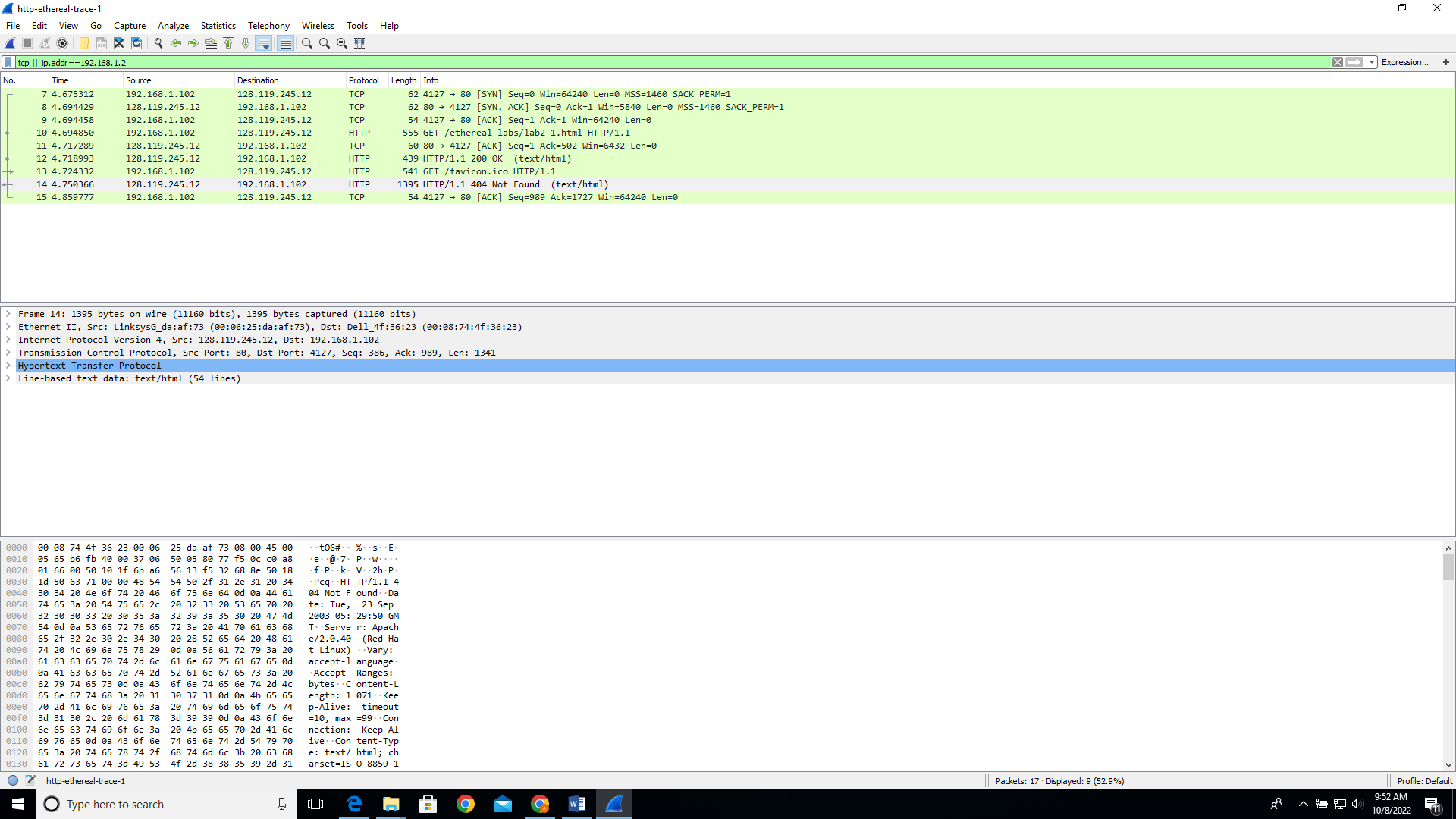
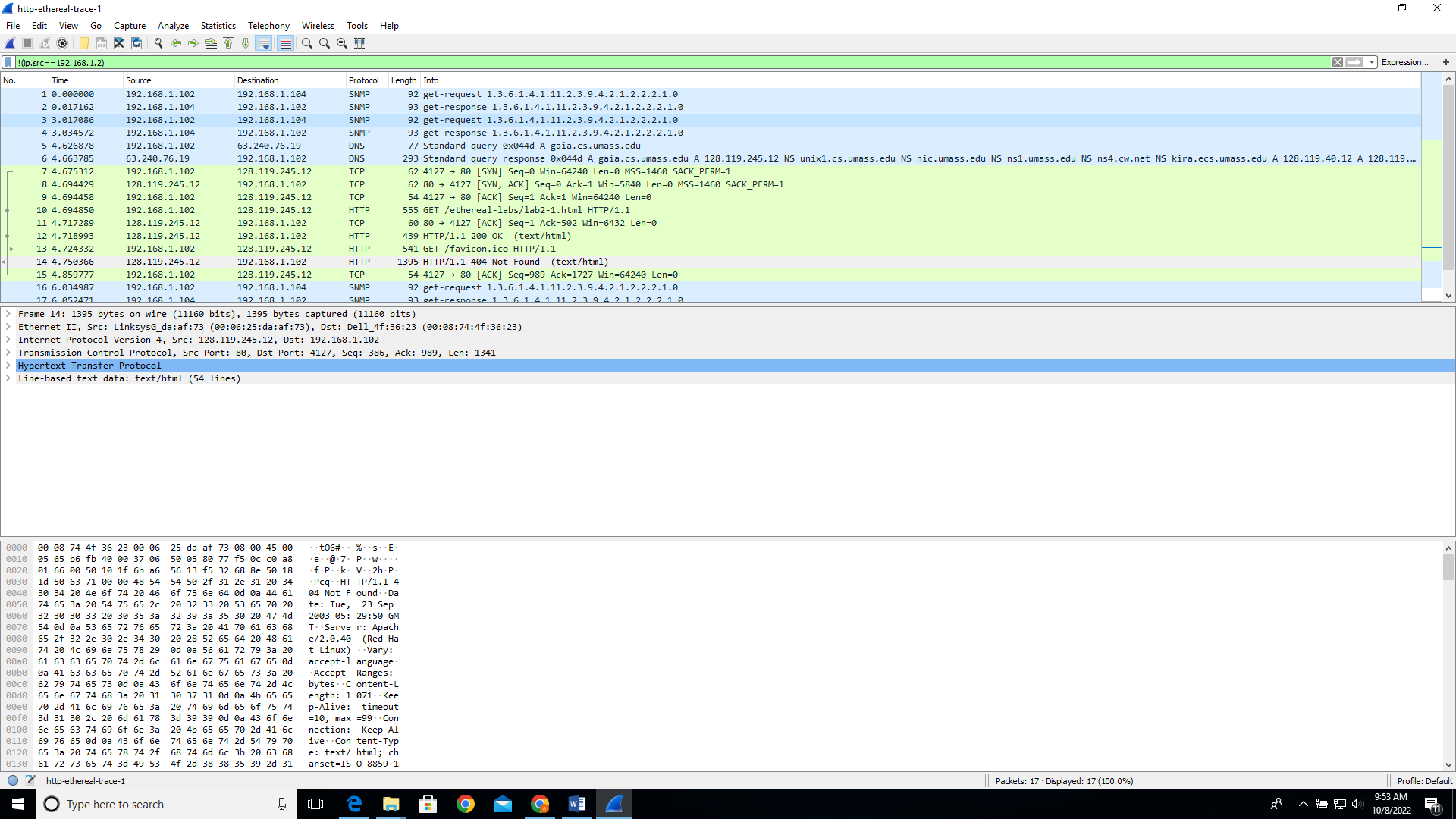
**To make combinations of different filters, you can use (&amp;&amp;, ||, !) signs as used**

**in C++ e.g.,**









**In-Lab Statement 1: Analyzing HTTP Protocol**

**(10)**

**1- List up to 4 different protocols that appear in the protocol column in the unfiltered packet-listing window.**

1. SNMP
2. HTTP
3. TCP
4. DNS

**2) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?**

0.024143000 seconds

**3) Was the second Get Request successful? How can you tell it from the corresponding response packet?**

No it was not successful, the status code is Not found.

**4) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?**

Browser is running Http 1.1

Server is running Http 1.1

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

en-us , en

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

Server IP address is Destination IP address: 128.119.245.12

Computer IP address is Source IP address: 192.168.1.102

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

SERVER: Destination: LinksysG\_da:af:73 (00:06:25:da:af:73)

COMPUTER: Source: Dell\_4f:36:23 (00:08:74:4f:36:23)

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

Source Port: 4127

Destination Port: 80

Port Number 80 is used by HTTP

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

200 for 1st request

and 404 for 2nd request

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

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n for 1st request

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

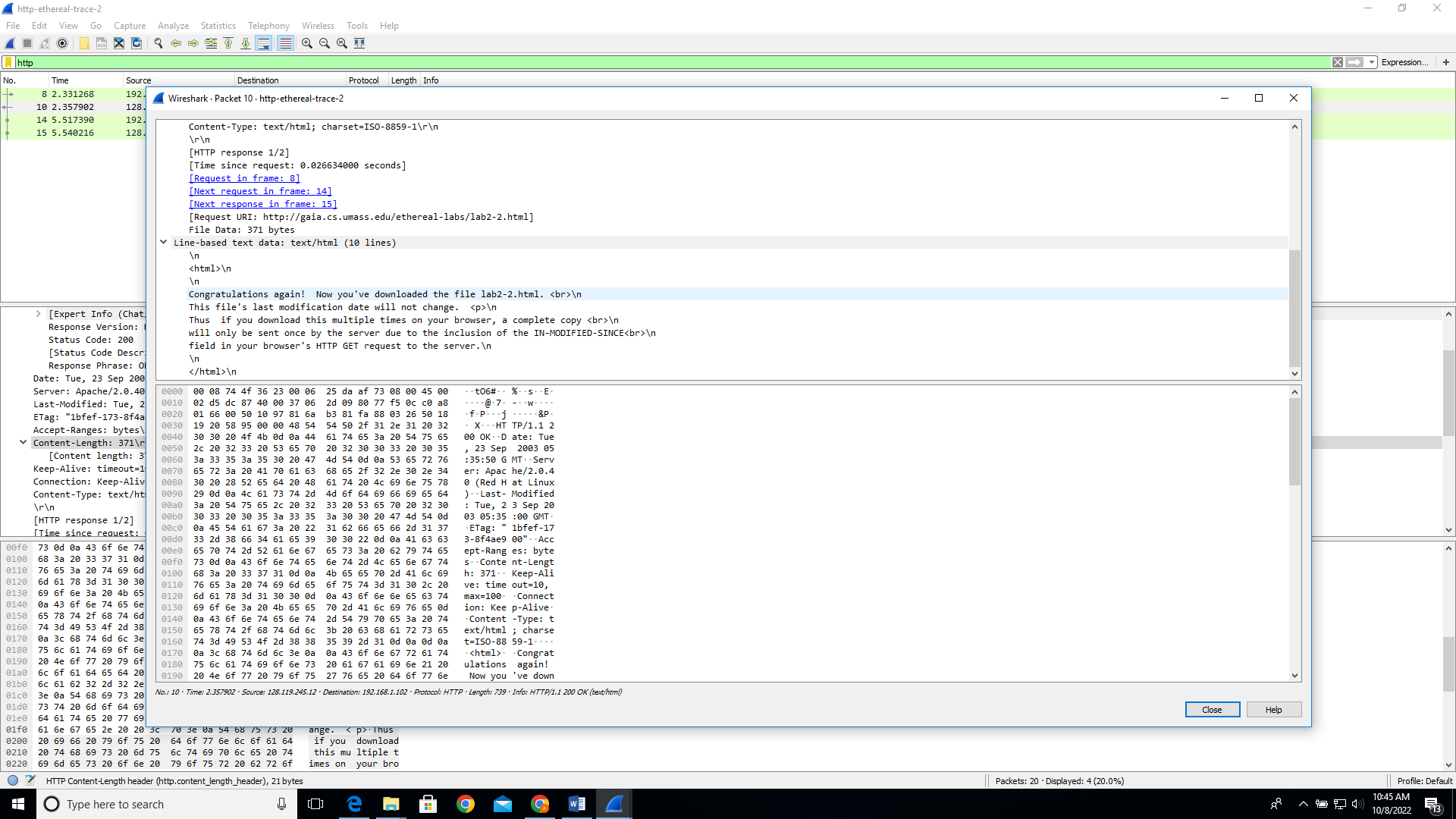
73 bytes

**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?**

No because it is not a conditional get.

1. **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?**



Yes because message says congratulations..

Content-Length: 371\r\n]

Yes because bytes are 371 bytes way too many.

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? What is meant by this information?**

**Yes,**

If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n

This means it shows the when the website was last modified in the cache.

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 your answer.**

Status code is 404.

Response Phrase: Not Modified

. Not explicitly return. Because not modified since the time specified.

**In-Lab Statement 2 : Analyzing HTTP Protocol**

**(10)**

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

One

**6. Which packet number in the trace contains the GET message for The Bill of Rights?**

Packet Number 08

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

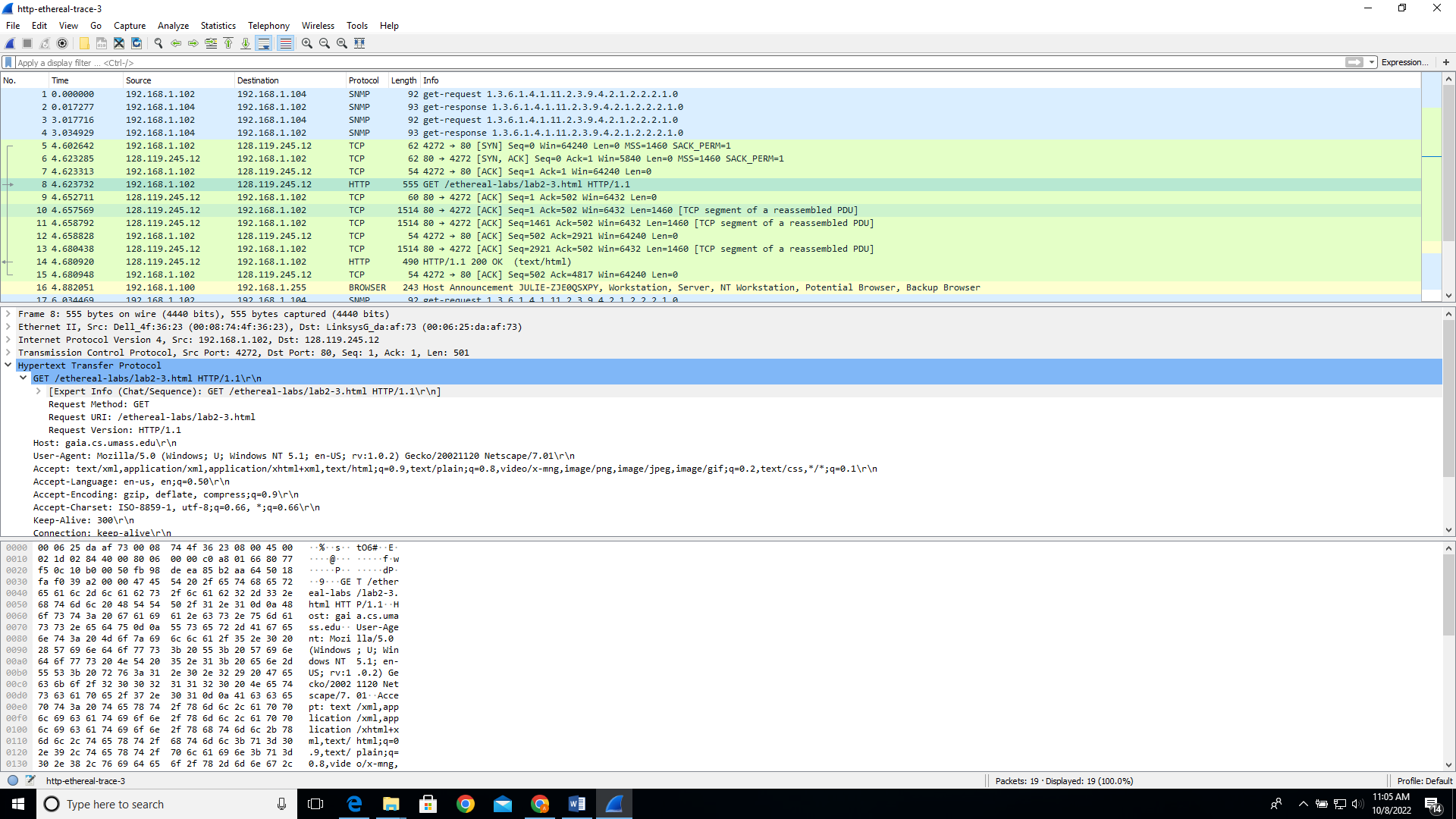
Packet number 14

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

Status Code: 200

Response Phrase: OK

**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?**



3 TCP segments

Packet Numbers are : 10,11,13

**In-Lab Statement 3: Trick Question (10)**

**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 variouspackets add up to a total of 4500 Bytes.**

Length of text is 4500 bytes

Content-Length: 4500\r\n

These are carried in tcp segments that approximately add up to the value 4500 bytes

Packet size is 490 bytes

(Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits))\

Length of tcp segments is 1460 \*3+490 =4380+490= 4870 bytes.