National University of Computer and Emerging Sciences

Laboratory Manuals

for

Computer Networks - Lab

(CL -3001)

Course Instructor	Mr. Nauman Moazzam
Lab Instructor	Miss. Shinawar Naeem
Section	BCS-5D
Semester	Fall 2024

Department of Computer Science
FAST-NU, Lahore, Pakistan

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

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

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

	Time	Source	D
10	4.694850	192.168.1.102	1
12	4.718993	128.119.245.12	1
13	4.724332	192.168.1.102	1
14	4.750366	128.119.245.12	1

9.413843

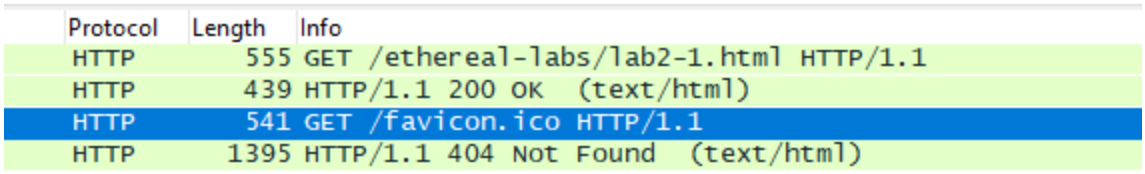
3- Was the second Get Request successful? How can you tell it from the corresponding response packet?

No, we can tell from the status code that the requested resource was not found. Thus, the request was not successful.

By looking at the information in the HTTP GET and Response Messages for **BOTH the HTTP Requests**, answer the following questions

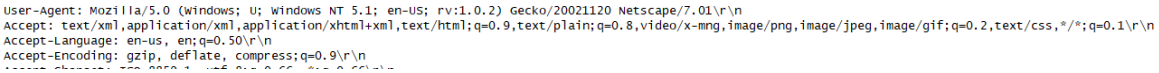
4. Is your **browser** running HTTP version 1.0 or 1.1? What **version** of HTTP is the server running?

The browser is running HTTP version 1.1



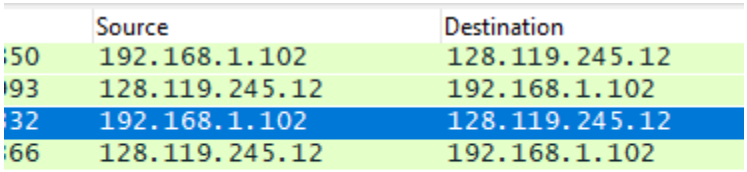
5. What **languages** (if any) does your **browser** indicate that it can accept to the server?

The browser indicated EN and EN-US locale.

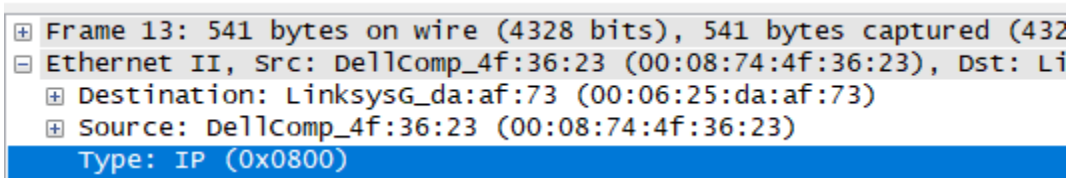


6. What is the **IP address** of the gaia.cs.umass.edu server and your computer?

My Computer = 192.168.1.102
Server = 128.119.245.12

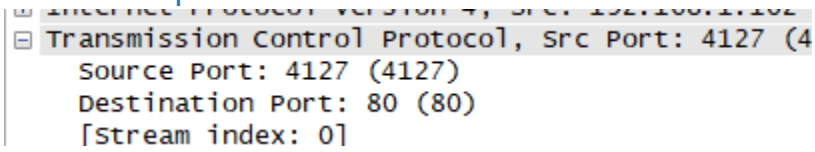


7. What is the **MAC address** of the server and your computer?



Server: 00:06:25:da:af:73
Computer: 00:08:74:4f:36:23

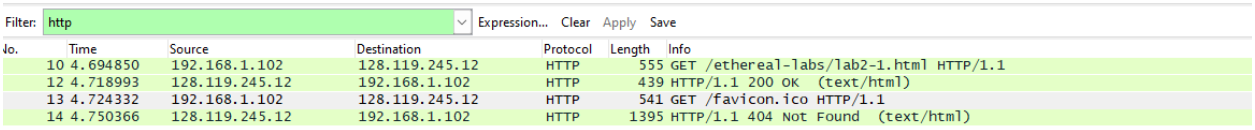
8. What is sending and receiving **Port Number**? What does Port No. 80 represents?



Sending: 4127
Receiving: 80

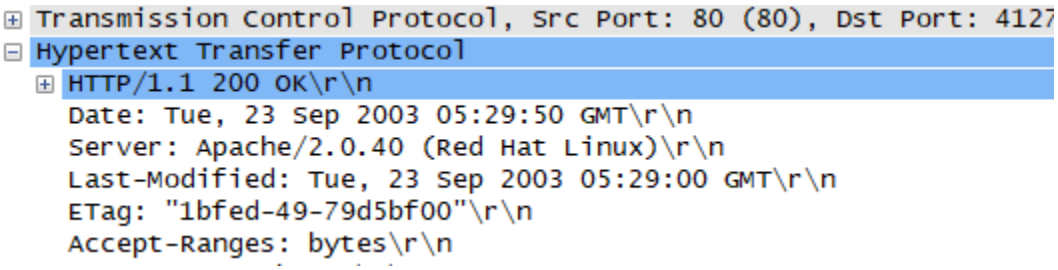
Port 80 represents HTTP Protocol.

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



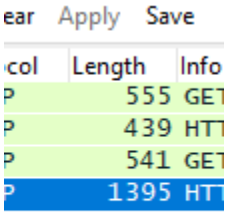
200 and 404 statuses were returned by the server.

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

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



bytes of total packet content = 555 + 439 + 541 + 1395 = 2930 bytes

<u>The HTTP CONDITIONAL GET/response interaction</u>

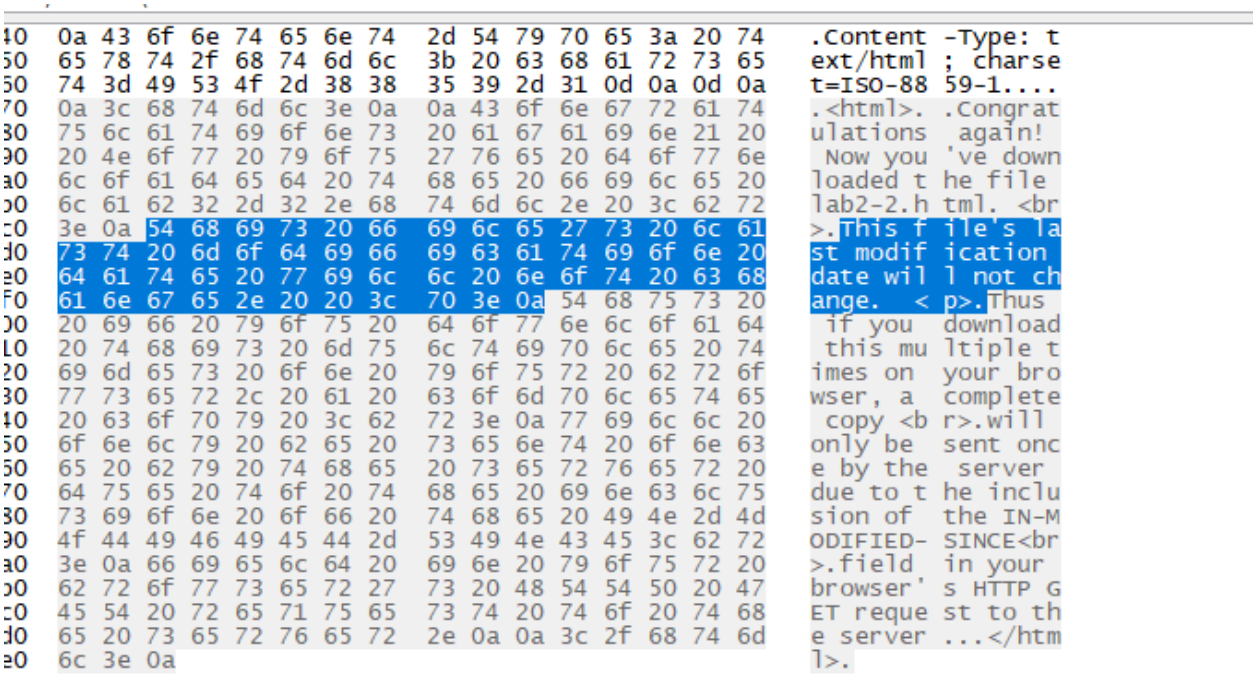
Use the http-ethereal-trace-2 packet trace to answer the questions below and apply the "http" filter

Answer the following questions:

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, the first get does not have last modified.

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?



```
40  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   .Content -Type: t
50  65 78 74 2f 68 74 6d 6c  3b 20 63 68 61 72 73 65   ext/html ; charse
60  74 3d 49 53 4f 2d 38 38  35 39 2d 31 0d 0a 0d 0a   t=ISO-88 59-1....
70  0a 3c 68 74 6d 6c 3e 0a  0a 43 6f 6e 67 72 61 74   .<html>. .Congrat
80  75 6c 61 74 69 6f 6e 73  20 61 67 61 69 6e 21 20   ulations  again!
90  20 4e 6f 77 20 79 6f 75  27 76 65 20 64 6f 77 6e    Now you 've down
a0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file
b0  6c 61 62 32 2d 32 2e 68  74 6d 6c 2e 20 3c 62 72   lab2-2.h tml. <br
c0  3e 0a 54 68 69 73 20 66  69 6c 65 27 73 20 6c 61   >.This f ile's la
d0  73 74 20 6d 6f 64 69 66  69 63 61 74 69 6f 6e 20   st modif ication
e0  64 61 74 65 20 77 69 6c  6c 20 6e 6f 74 20 63 68   date wil l not ch
f0  61 6e 67 65 2e 20 20 3c  70 3e 0a 54 68 75 73 20   ange.  < p>.Thus
00  20 69 66 20 79 6f 75 20  64 6f 77 6e 6c 6f 61 64    if you  download
10  20 74 68 69 73 20 6d 75  6c 74 69 70 6c 65 20 74    this mu ltiple t
20  69 6d 65 73 20 6f 6e 20  79 6f 75 72 20 62 72 6f   imes on  your bro
30  77 73 65 72 2c 20 61 20  63 6f 6d 70 6c 65 74 65   wser, a  complete
40  20 63 6f 70 79 20 3c 62  72 3e 0a 77 69 6c 6c 20    copy <b r>.will
50  6f 6e 6c 79 20 62 65 20  73 65 6e 74 20 6f 6e 63   only be  sent onc
60  65 20 62 79 20 74 68 65  20 73 65 72 76 65 72 20   e by the  server
70  64 75 65 20 74 6f 20 74  68 65 20 69 6e 63 6c 75   due to t he inclu
80  73 69 6f 6e 20 6f 66 20  74 68 65 20 49 4e 2d 4d   sion of  the IN-M
90  4f 44 49 46 49 45 44 2d  53 49 4e 43 45 3c 62 72   ODIFIED- SINCE<br
a0  3e 0a 66 69 65 6c 64 20  69 6e 20 79 6f 75 72 20   >.field  in your
b0  62 72 6f 77 73 65 72 27  73 20 48 54 54 50 20 47   browser' s HTTP G
c0  45 54 20 72 65 71 75 65  73 74 20 74 6f 20 74 68   ET reque st to th
d0  65 20 73 65 72 76 65 72  2e 0a 0a 3c 2f 68 74 6d   e server ...</htm
e0  6c 3e 0a                                          l>.
```

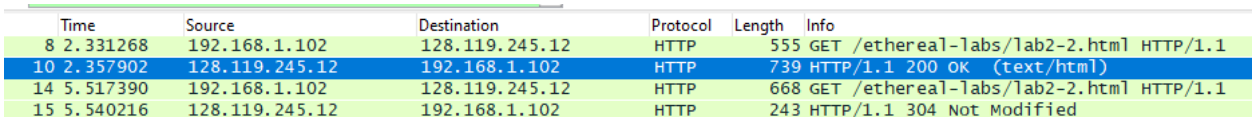
We see the contents from right hand side.

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?**

```
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US
Accept: text/xml,application/xml,application/xhtml+xml,tex
Accept-Language: en-us, en;q=0.50\r\n
Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
If-None-Match: "1bfef-173-8f4ae900"\r\n
Cache-Control: max-age=0\r\n
\r\n
```

True
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT
This means data is retrieved from the web cache. This means it is the last time it got the data from the origin server.

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



	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Its sends 304 status code not modified.

This means that cache has the latest version of the file.

In-Lab Statement 2 : *Analyzing HTTP Protocol*

(10)

Retrieving Long Documents

In our examples thus far, the documents retrieved have been simple and short HTML files. Let's next see what happens when we **download a long HTML file**. Do the following:

In the packet-listing window, you should see your HTTP GET message, followed by a **multiple-packet TCP response** to your HTTP GET request. This multiple-packet response deserves a bit of explanation. The **HTTP RESPONSE MESSAGE** consists of a status line, followed by header lines, followed by a blank line, followed by the entity body. In the case of our HTTP GET, the entity body in the response is the *entire* requested HTML file. In our case here, the HTML file is rather long, and at **4500 bytes is too large to fit in one TCP packet.** The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment. In recent versions of Wireshark, Wireshark indicates each **TCP segment as a separate packet**, and the fact that the single HTTP response was fragmented across multiple TCP packets is indicated by the **"TCP segment of a reassembled PDU"** in the Info column of the Wireshark display.

- **Use the http-ethereal-trace-3 packet trace to answer the questions below and apply the "http" filter**

Answer the following questions:

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

   The browser sent only 1 get request.

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

   The packet number that contained the get message is 8.

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

   The packet number that contained the get message is 14.

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

   The status code is 200 and the phrase is 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?

   The number of data containing TCP segments is 4. Their respective packet numbers are 9, 10 ,11, 13.

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.

If we sum the length of the tcp data packets it exceeds 4500 because it contains some overhead information like the header for each tcp packet. If we disregard that, then the size of the content comes out to be exactly 4500.