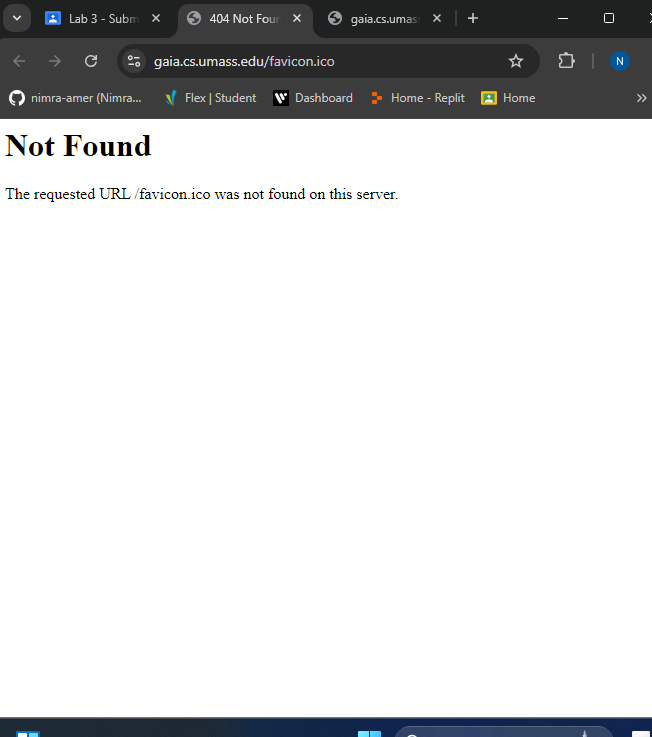
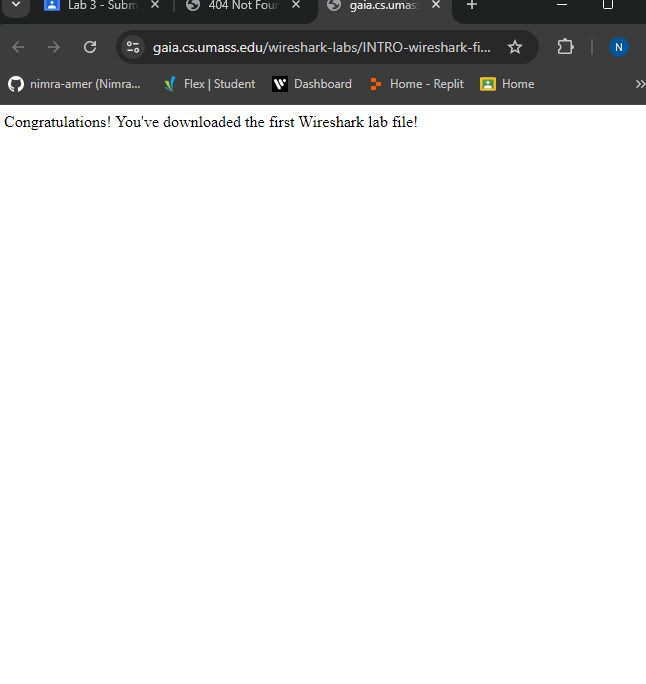
**Test Run:**

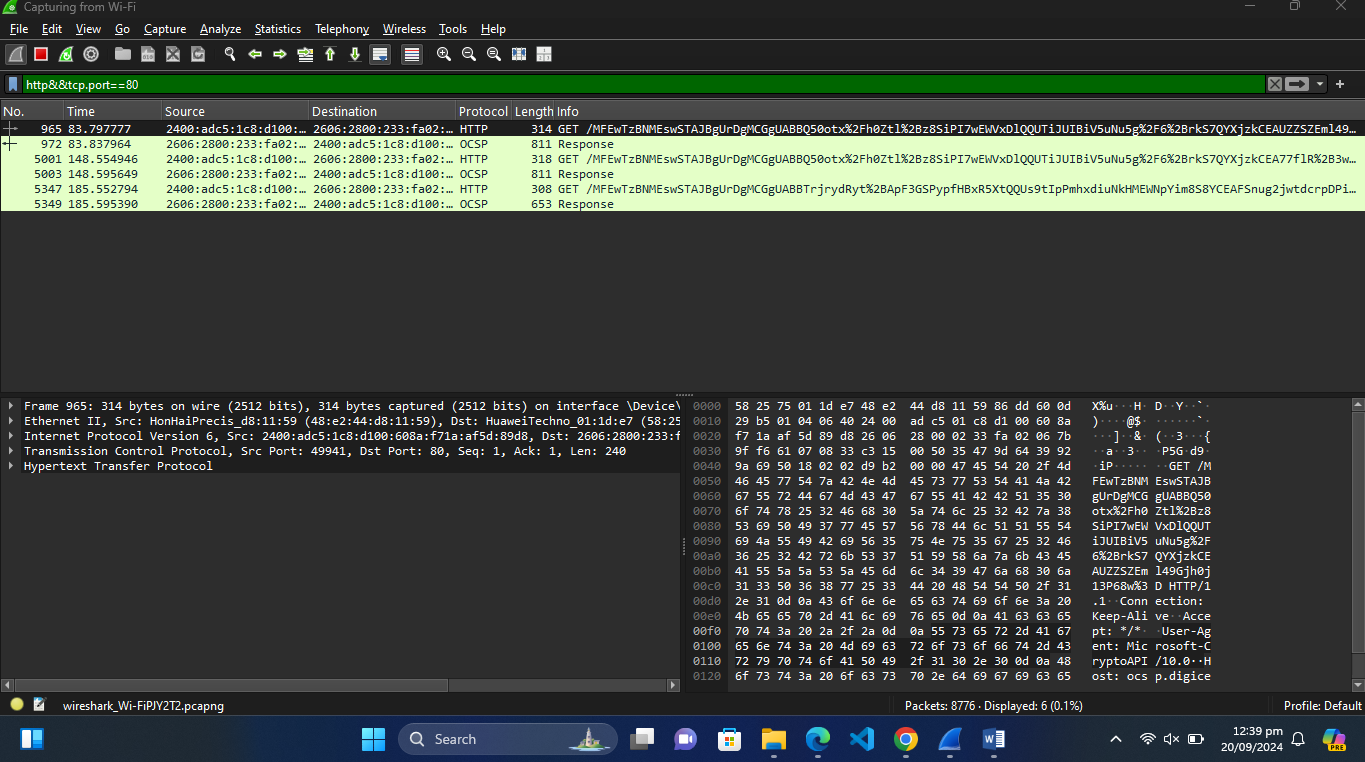
****

****

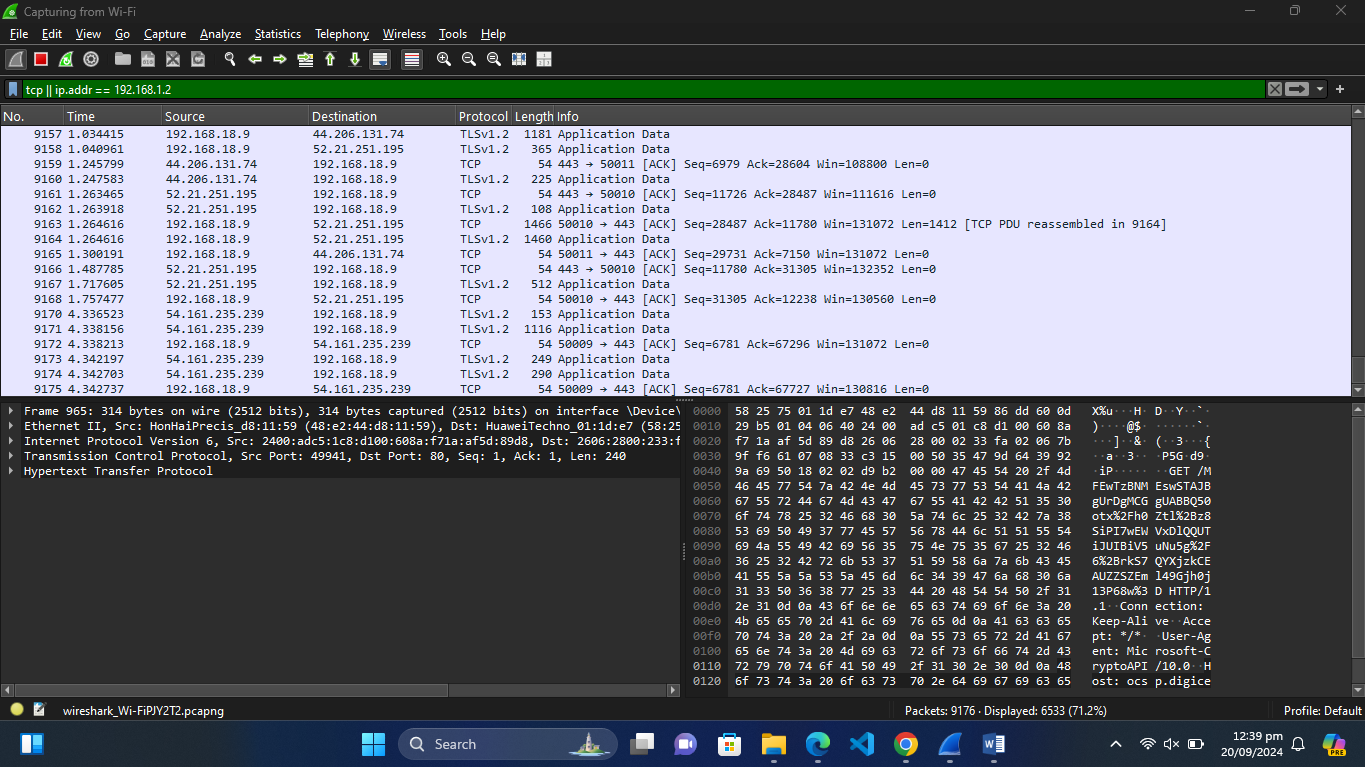
Didn’t use any file but the Wifi.

**Wireshark Filters:**

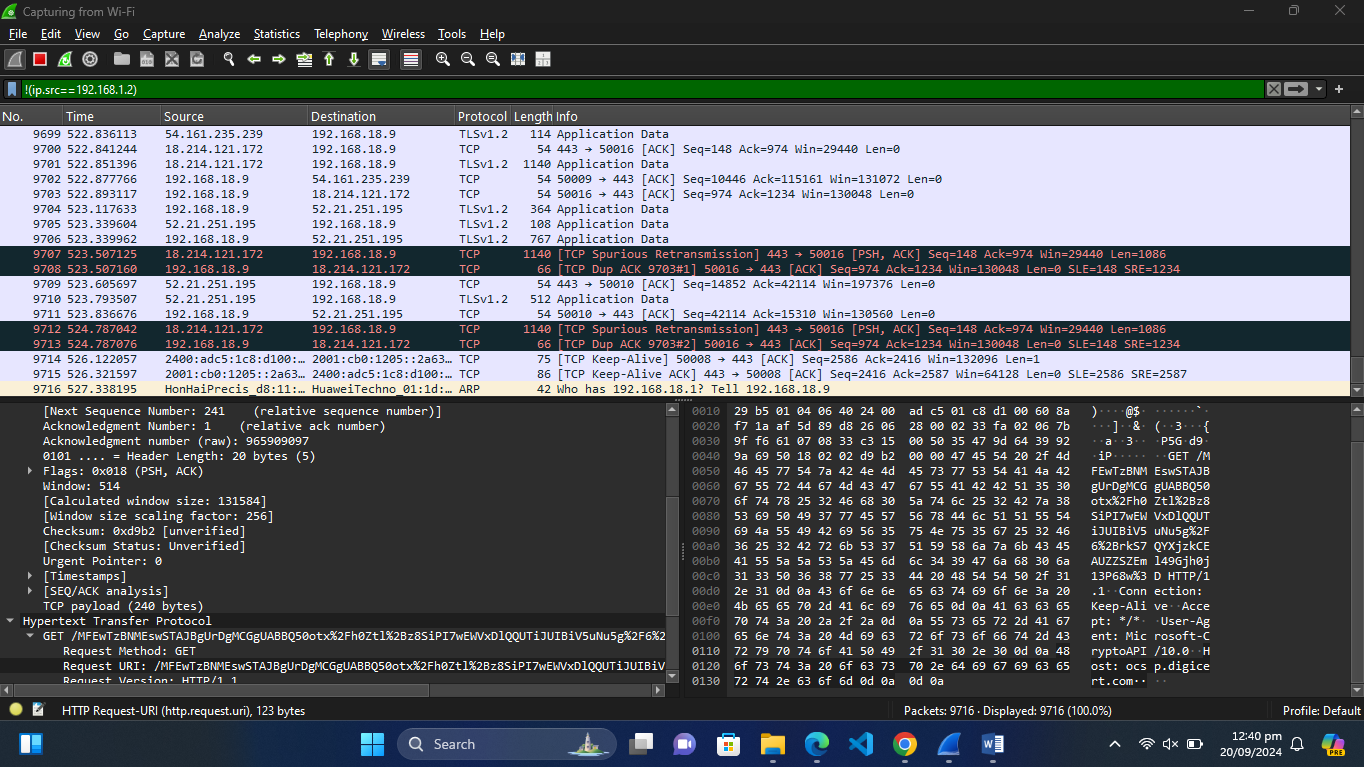
**in C++ e.g., a. http && tcp.port==80**

****

**b. tcp || ip.addr=192.168.1.2**

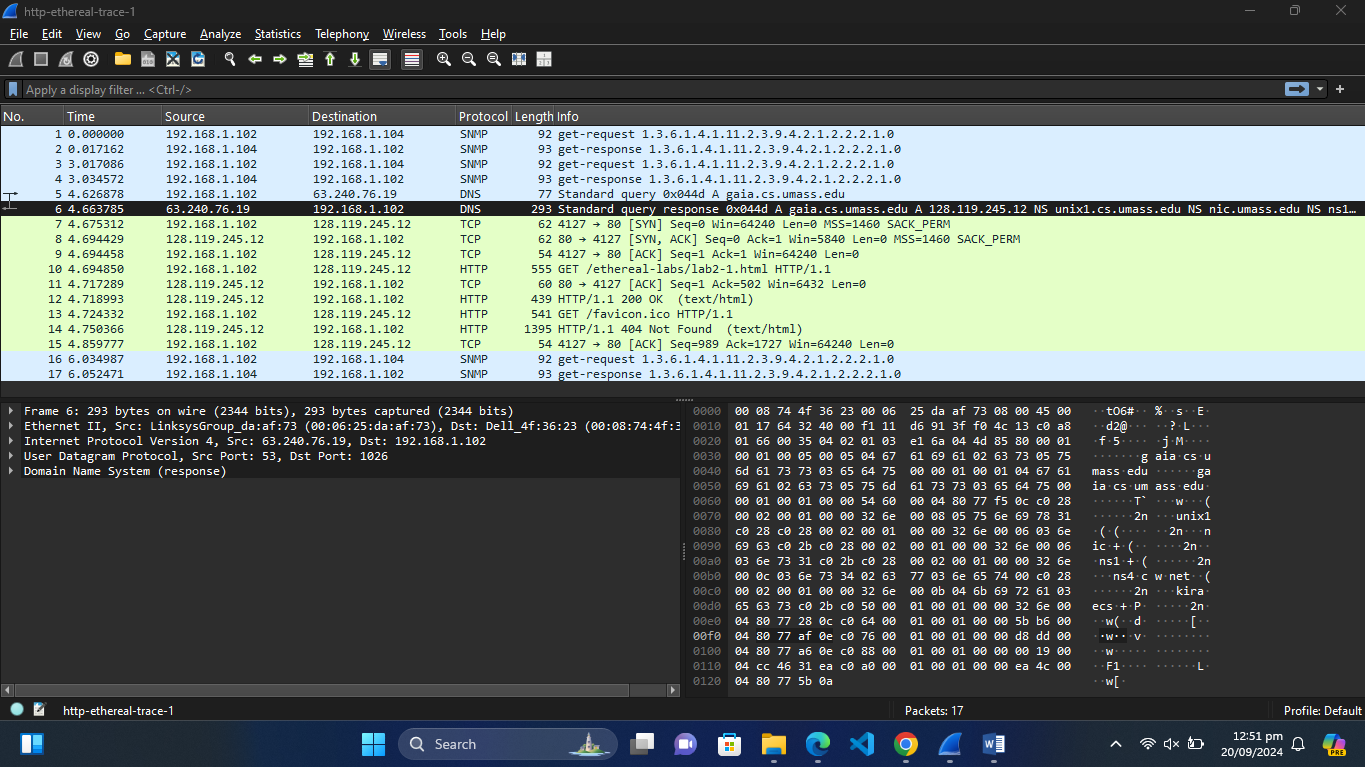
****

**c. !(ip.src==192.168.1.2)**

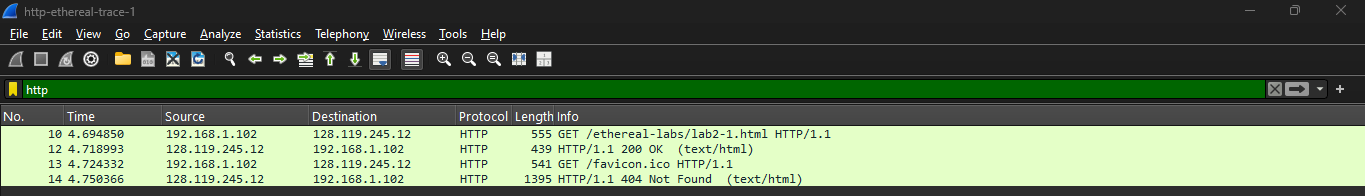
****

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

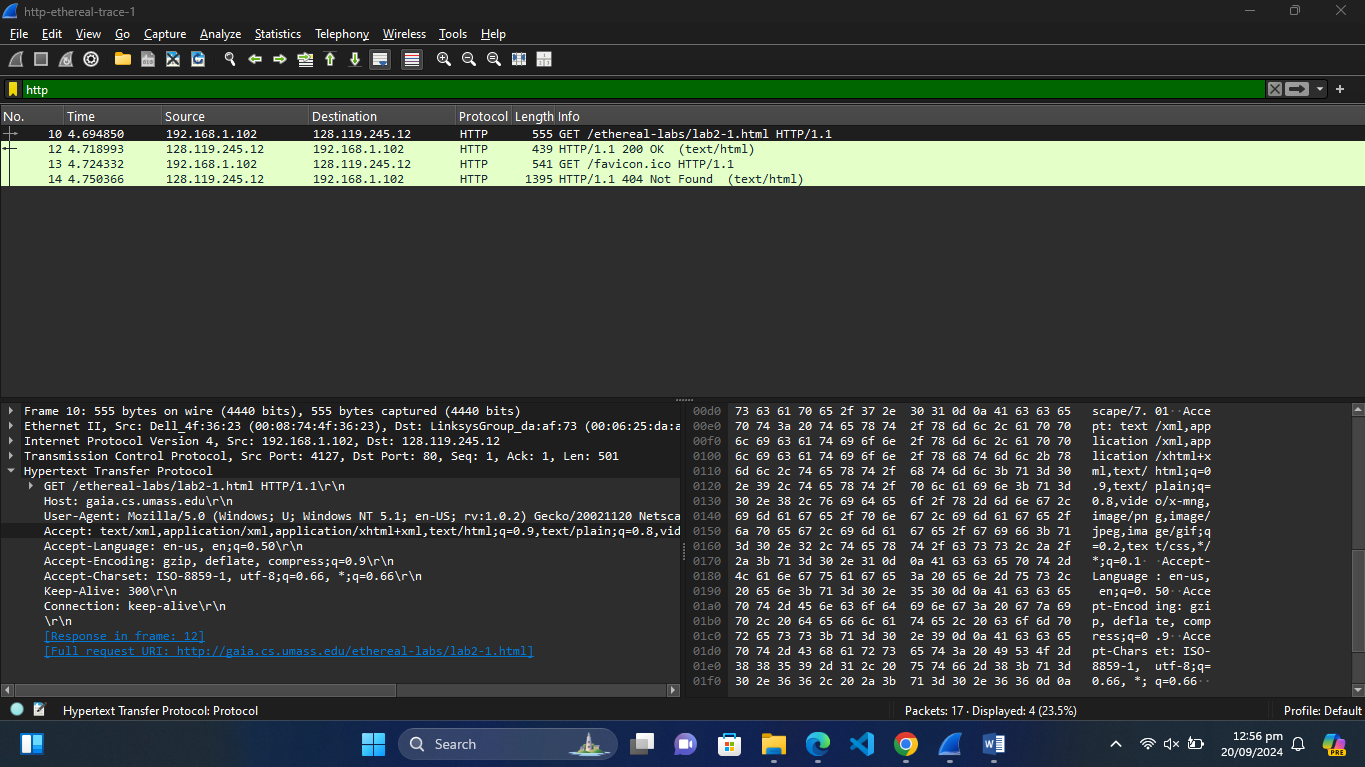
(A)

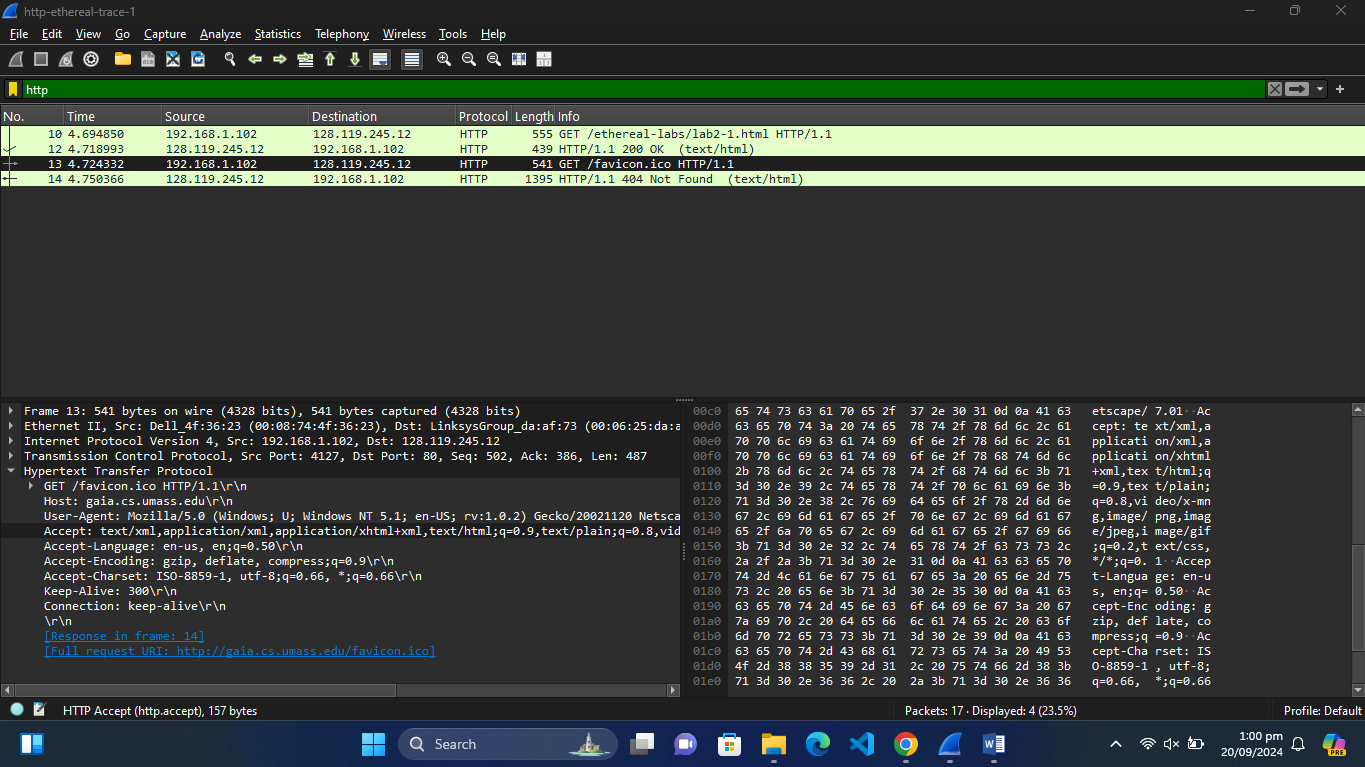


(B)



(C)



(D) 

1. **4 protocols:**

SNMP, DNS, TCP, HTTP

1. **Time:**

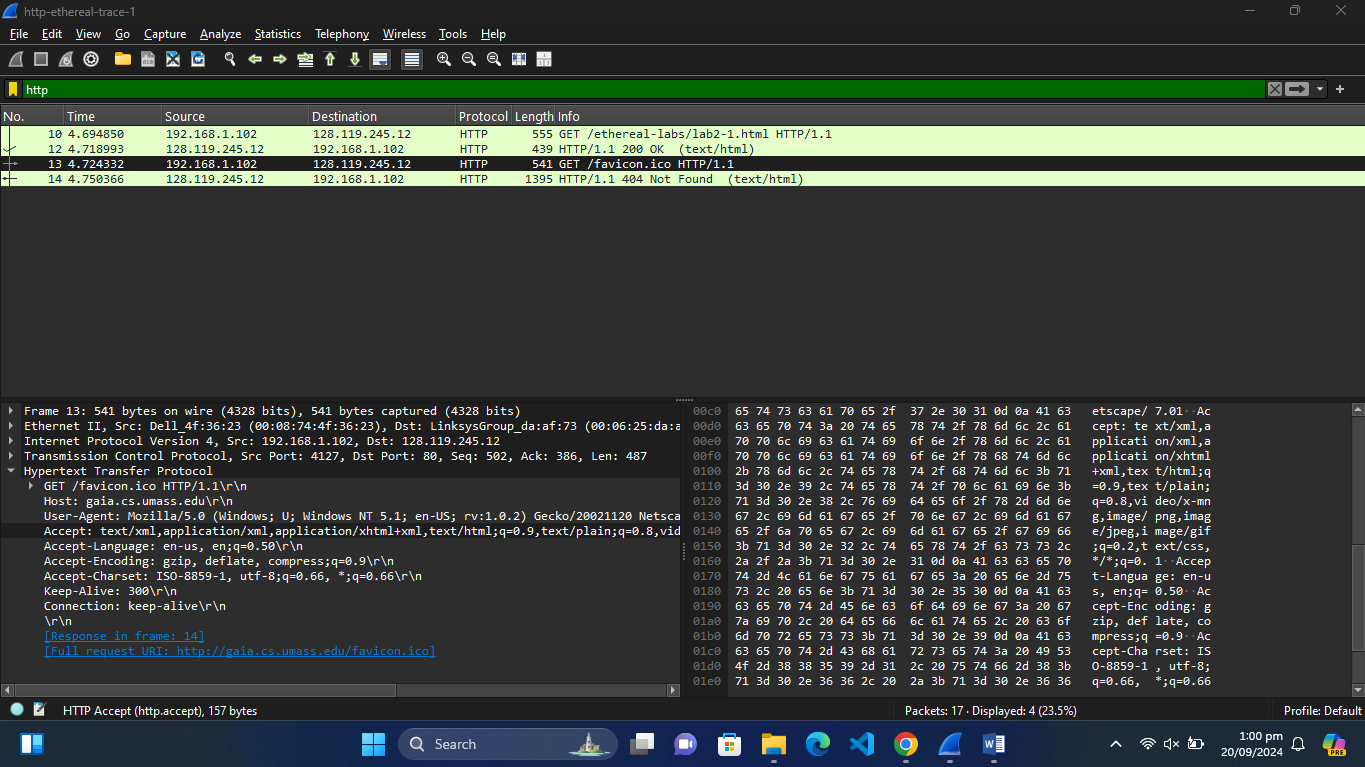
The first get message was sent in 4.694850 seconds and second get message was sent in 4.724332 seconds.

1. **Successful/Not:**

The second Get request was not successful. It was identified by the error message it displayed, HTTP/1.1 404 Not Found (text/html).

C:\Users\Nimra Amer\Pictures\Screenshots\8.png

1. The browser is running HTTP version 1.1

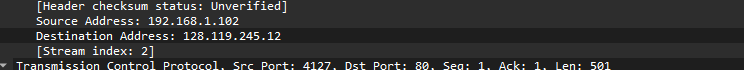


1. My browser’s Accept-Language: en-us, en;q=0.50\r\n

C:\Users\Nimra Amer\Pictures\Screenshots\6.png

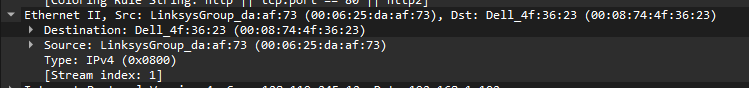
1. The source IP address is: 192.168.1.102

The destination IP address is: 128.119.245.12

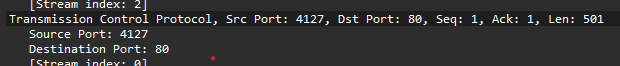


1. Mac Address: Source: LinksysGroup\_da:af:73 (00:06:25:da:af:73)

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



1. Source Port : 4127 , Destination Port : 80



Port 80 is the default port used by HTTP

1. 200 and 400

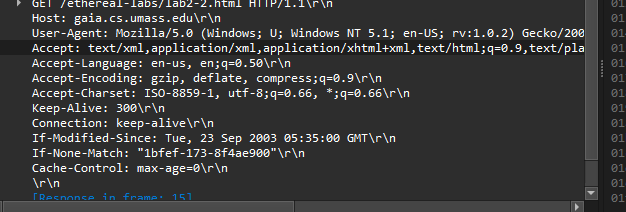
C:\Users\Nimra Amer\Pictures\Screenshots\8.png



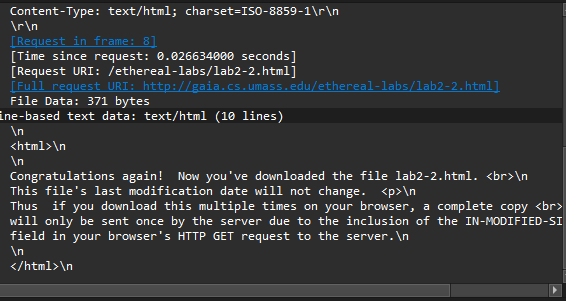
1. 

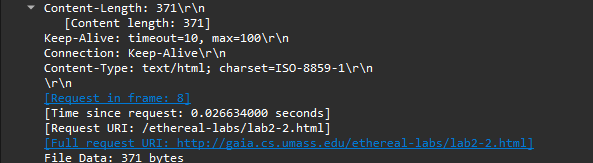
**The HTTP CONDITIONAL GET/response interaction**

1. Yes.



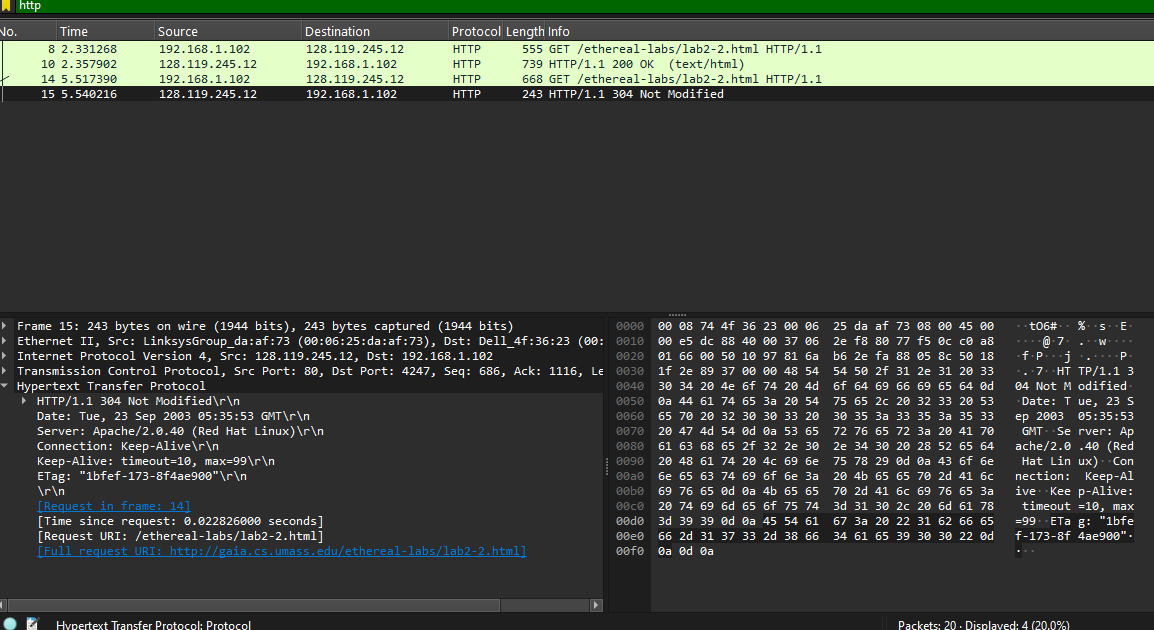
1. Yes, the server has explicitly returned the contents. It is inspected because the content if readable and the content length is the same as the content.





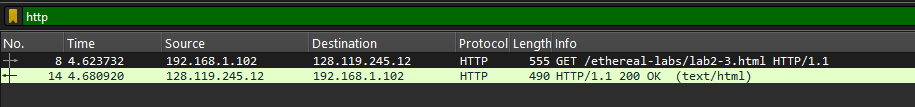
1. 

Yes, it is visible, and the information indicates that the server should only send the sources that have been modified since the date provided.

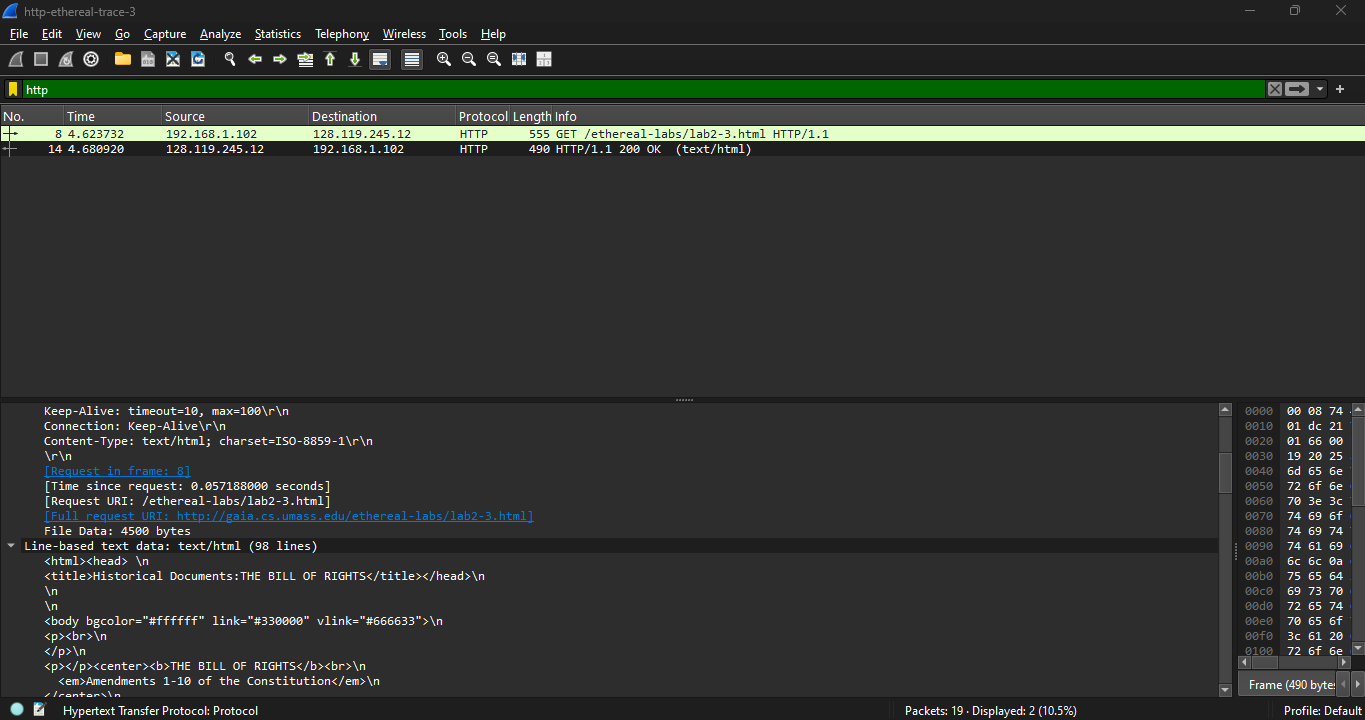
1. The status code returned is 304 with the message not modified. No, the content was not returned. it can be identified by the error message. 

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

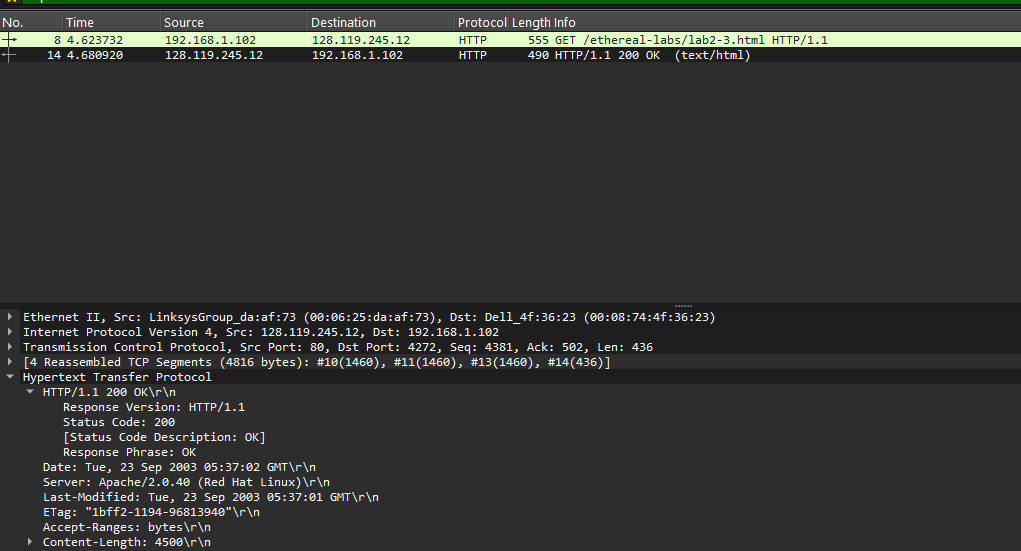
1. 1



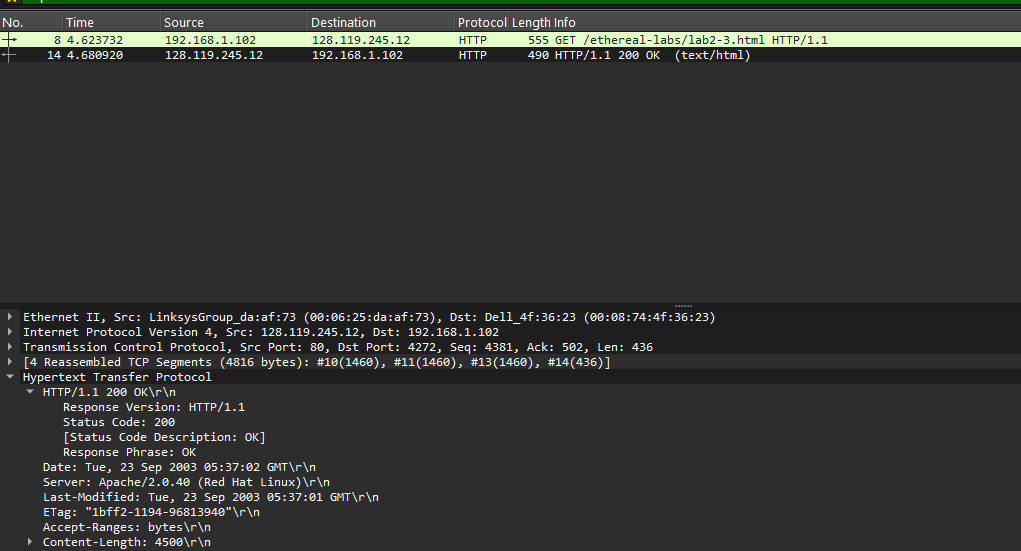
1. Packet no.: 14



1. Packet Number: 14



1. Status Code: 200 , Phrase Ok



1. 4



**In-Lab Statement 3: Trick Question**

Length : 4500



The 490 bytes contain HTTP headers and some text. The 4500 bytes’ content can be divided into TCP segments with each segment containing a short part of data. By summing up the data of all the segments we will most probably get the number 4500