Faculty of Engineering & Technology
Electrical & Computer Engineering Department

ENCS4130

Wireshark HTTP ToDo

Prepared by : Tareq Shannak

ID Number : 1181404

Instructor : Dr. Ahmad Alsadeh

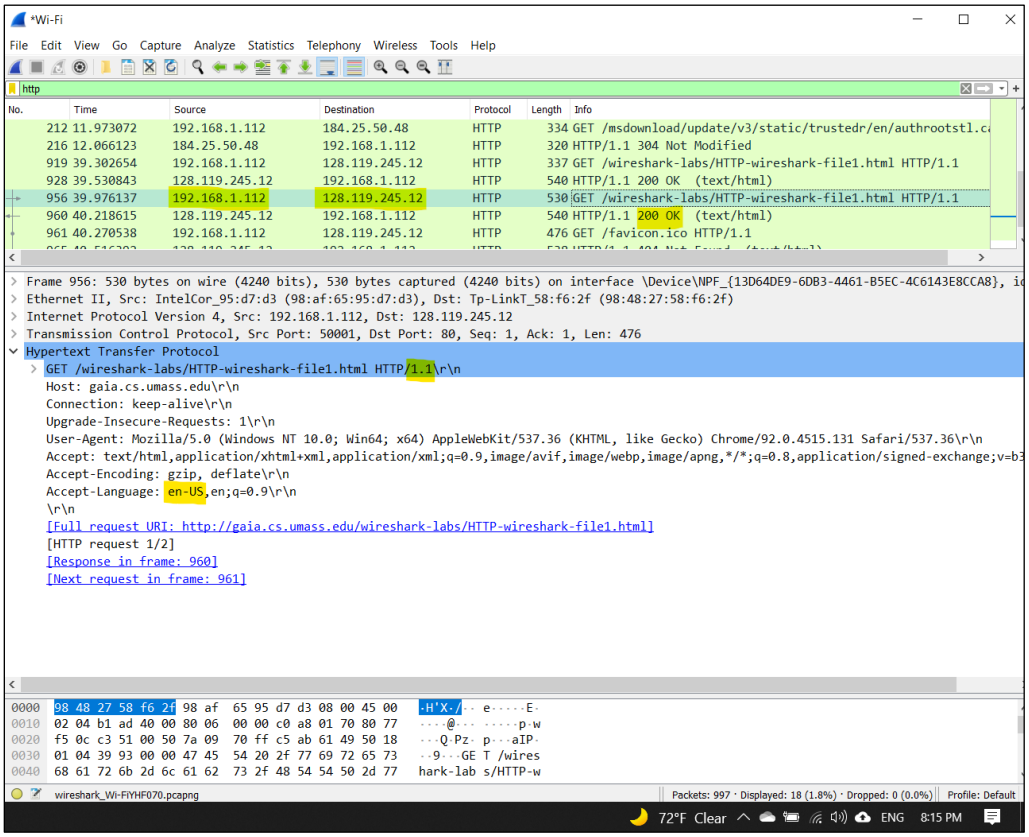
Teaching Assistant : Katy Sadi

Section : 2

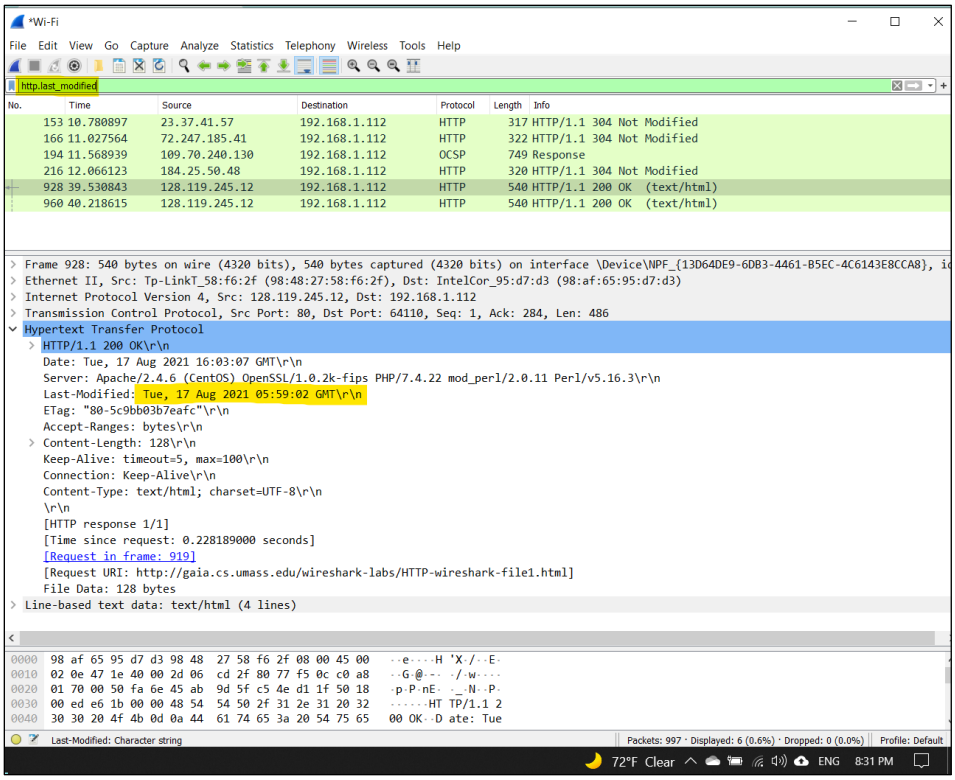
Date : August 17, 2021

The Basic HTTP GET/response interaction

By looking at the information in the HTTP GET and response messages, answer the following questions. If you're doing this lab as part of class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.

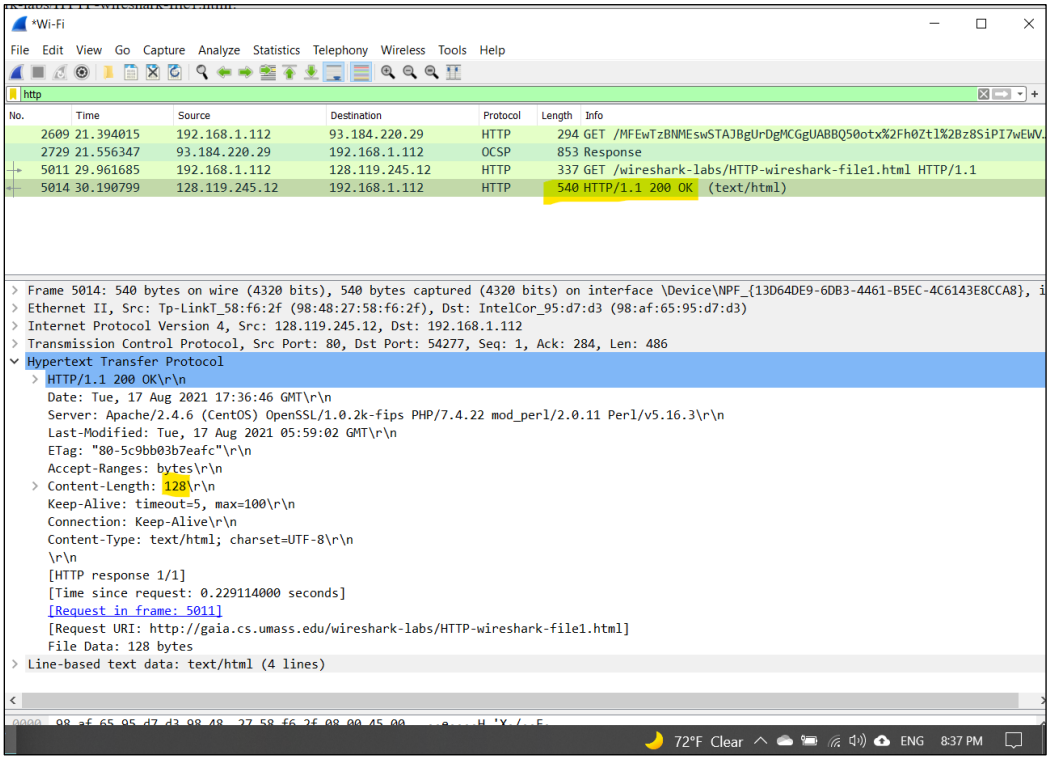


1. **Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?**
   HTTP1.1
2. **What languages (if any) does your browser indicate that it can accept to the server?**
   en-US (US English)
3. **What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?**
   IP address of my computer: 192.168.1.112
   IP address of the gaia.cs.umass.edu server: 128.119.245.12
4. **What is the status code returned from the server to your browser?**
   200 OK
5. **When the HTML file that you are retrieving was last modified at the server?**



Tue, August 17, 2021 5:59:02 GMT

6. How many bytes of content are being returned to your browser?



128 Bytes

7. **By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.**

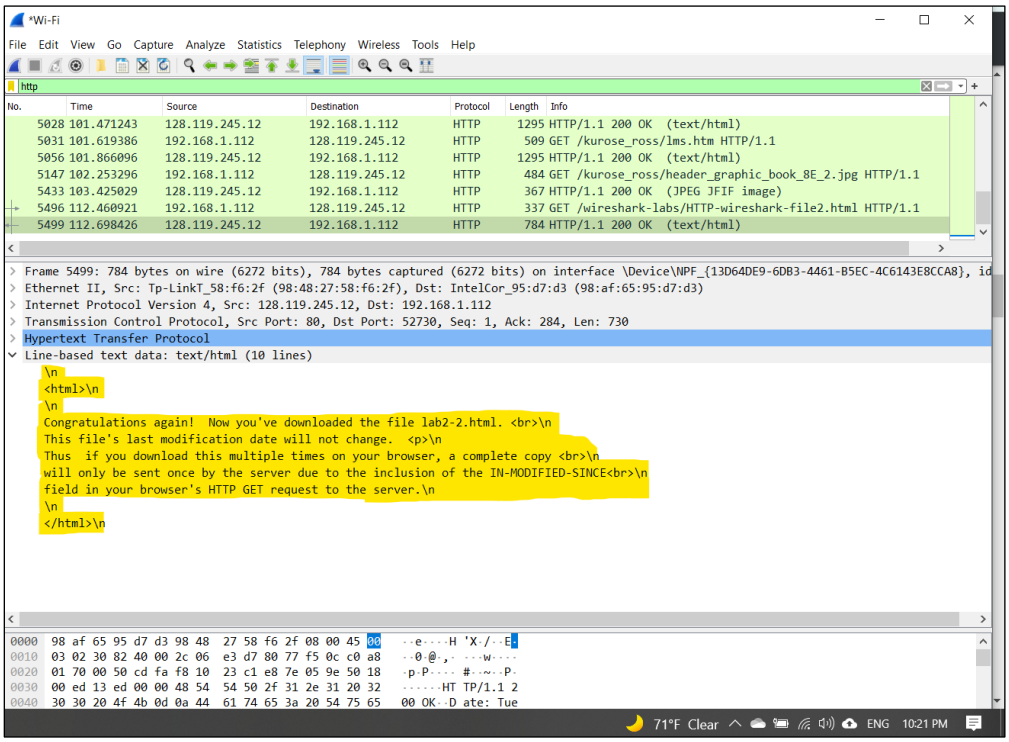
   No.

The HTTP CONDITIONAL GET/response interaction

8. **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?**

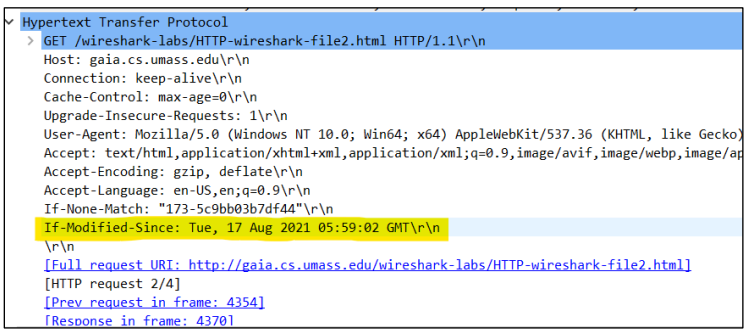
   No.

9. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**



10. **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?**

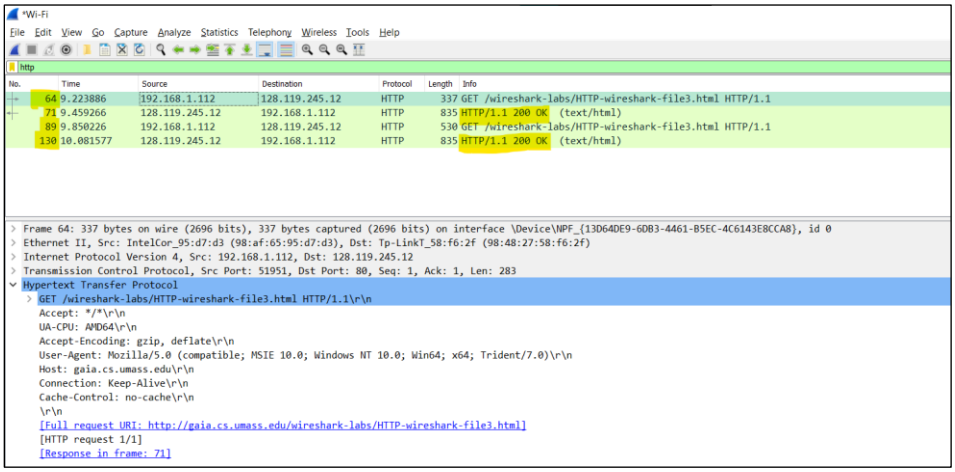
    Yes.



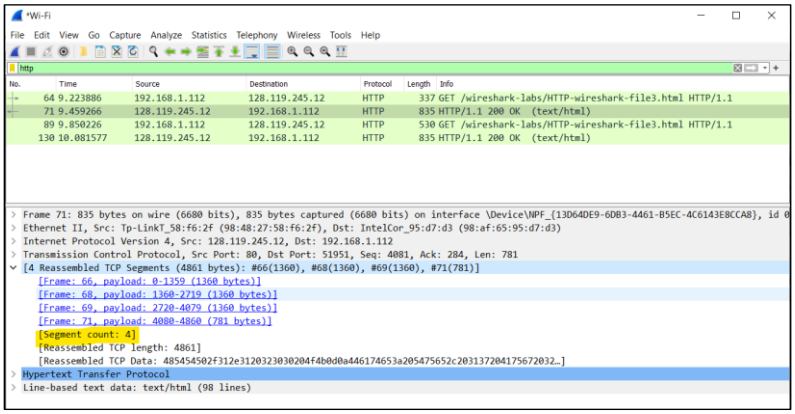
11. **What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.**

    We get a HTTP/1.1 304 Not Modified Response. This is much shorter than the full response packet seen previously.

Retrieving Long Documents



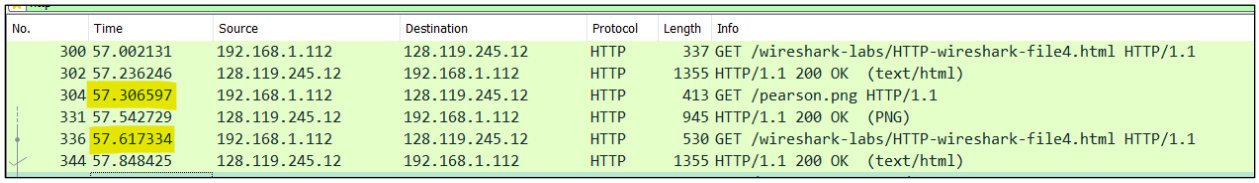
12. **How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?**
    Two, packet numbers = 64 and 89.
13. **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**
    Packet numbers = 71 and 130
14. **What is the status code and phrase in the response?**
    HTTP1.1/200 OK
15. **How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?**



4 TCP Segments.

HTML Documents with Embedded Objects

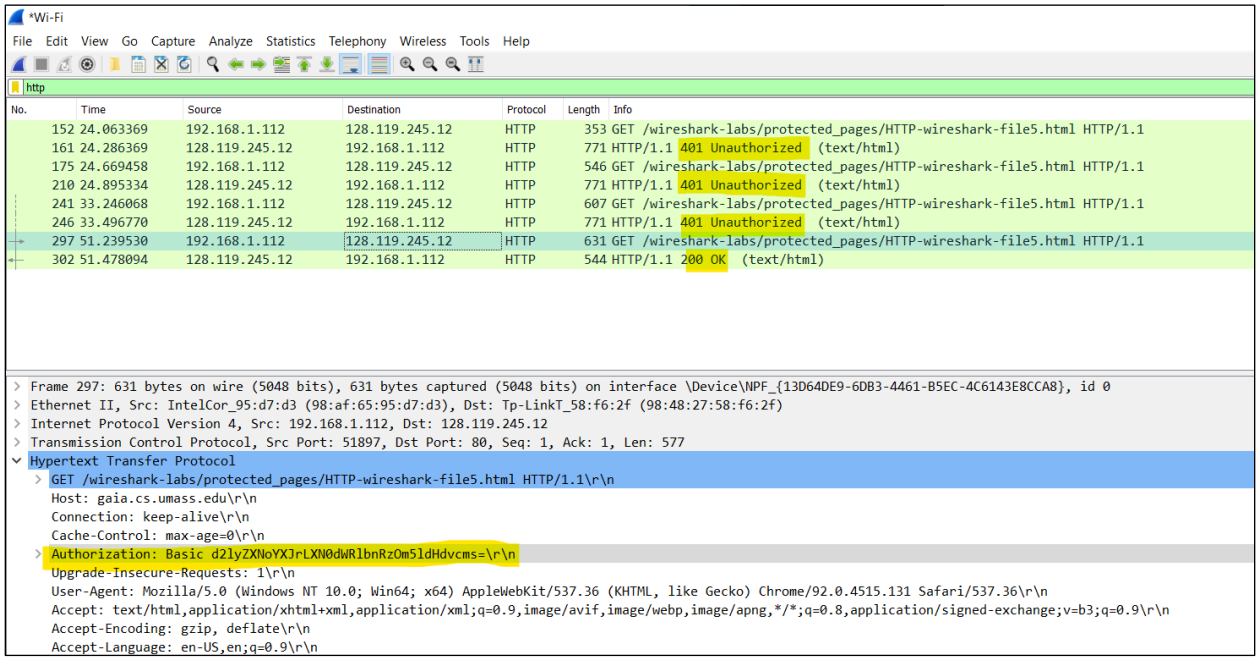
16. **How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?**
    Three, 128.119.245.12 178.79.137.164
17. **Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**



No.	Time	Source	Destination	Protocol	Length	Info
300	57.002131	192.168.1.112	128.119.245.12	HTTP	337	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
302	57.236246	128.119.245.12	192.168.1.112	HTTP	1355	HTTP/1.1 200 OK (text/html)
304	57.306597	192.168.1.112	128.119.245.12	HTTP	413	GET /pearson.png HTTP/1.1
331	57.542729	128.119.245.12	192.168.1.112	HTTP	945	HTTP/1.1 200 OK (PNG)
336	57.617334	192.168.1.112	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
344	57.848425	128.119.245.12	192.168.1.112	HTTP	1355	HTTP/1.1 200 OK (text/html)

The browser downloaded the two images in serially. I believe this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been requested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back.

HTTP Authentication



18. **What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?**
    HTTP/1.1 401 Unauthorized
19. **When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?**
    Authorization field as shown in the above picture.