INTERNET PROTOCOL LAB ASSIGNEMNET -3

Name: **Siriparapu Sparshika**

Roll No: **CYS22006**

Date: **20-10-2022**

Analyzing HTTP requests and responses using Wireshark

Aim:

To explore the web application protocols using protocol analyzer

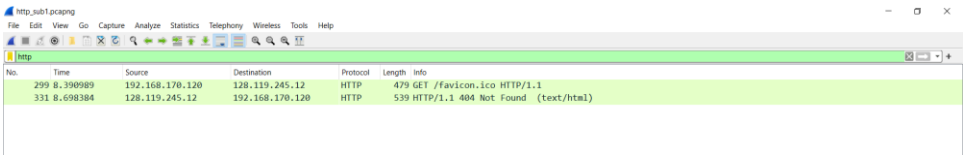
1.)

By looking at the information in the HTTP GET and response messages, answer the following

questions.

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

A. HTTP version is 1.1

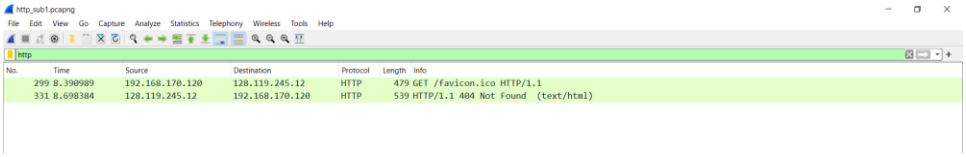


2. What languages (if any) do your browser indicate that it can accept to the server?

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Source:192.168.17.120

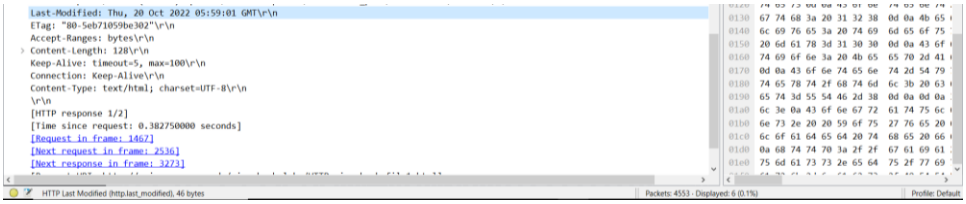
Destination:128.119.245.12



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

404 not found

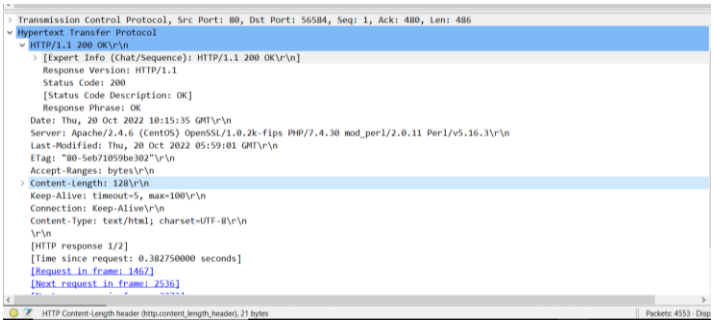
5. When was the HTML file that you are retrieving last modified at the server?



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

Last modified

: Identify malicious activities on n/w



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.

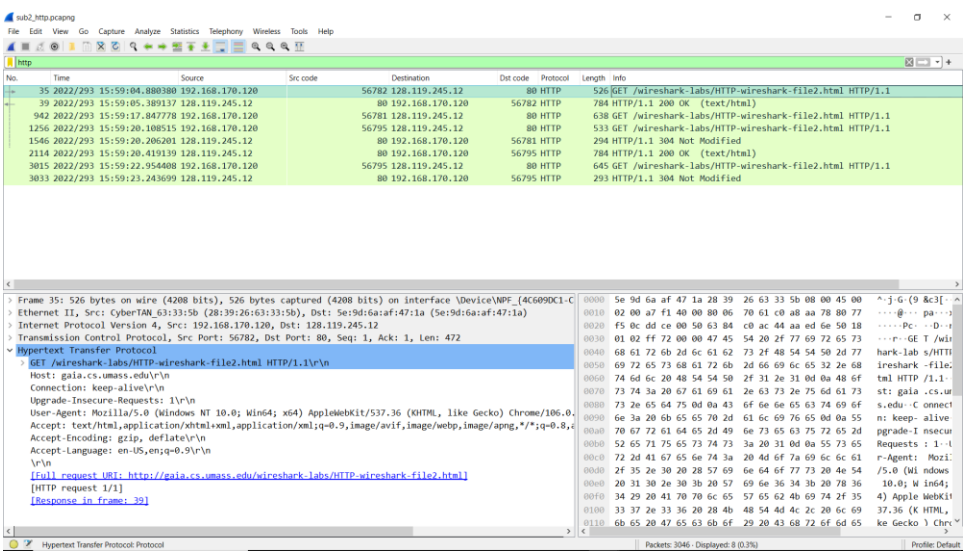
A. No

2.)

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?

A. No

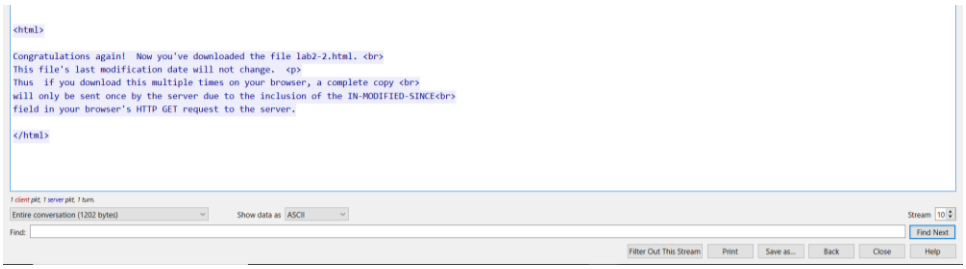


9. Inspect the contents of the server response. Did the server explicitly return the contents of the

file? How can you tell?

A. Yes

Destination address = source address should be same



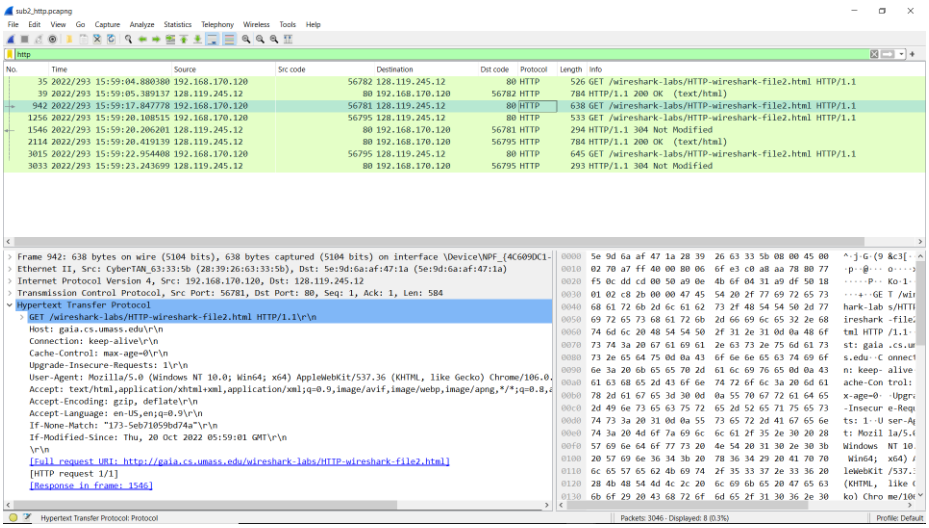
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do

you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? What information follows the “IF-MODIFIED

SINCE:” header?

A. Yes

It contains: Thu, 20 Oct 2022 05:59:01 GMT\r\n

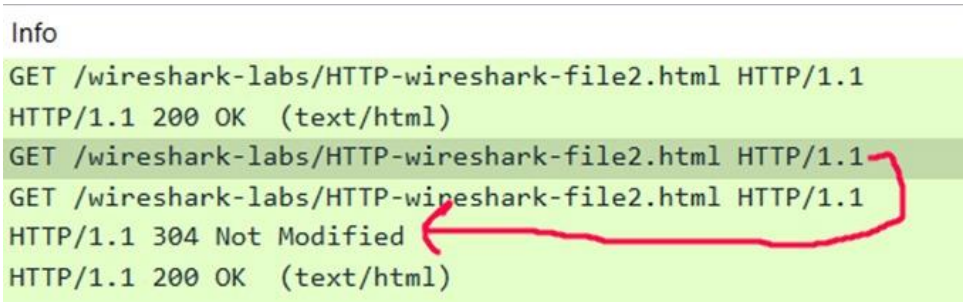


11. What is the HTTP status code and phrase returned from the server in response to this second

HTTP GET? Did the server explicitly return the file's contents? Explain.

For the first request the content sent request with html

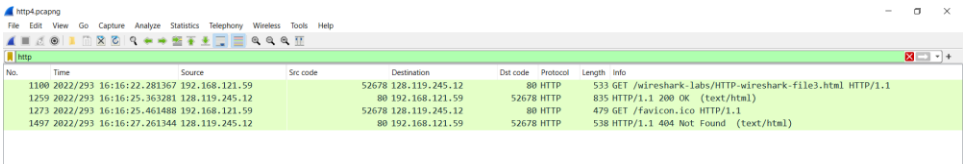
For second it didn't modify so it doesn't return the content



3.)

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?



-First packet number in the trace contains the GET message for the Bill or Rights

13. Which packet number in the trace contains the status code and phrase associated with the

response to the HTTP GET request?

1259	2022/293 16:16:25.363281	128.119.245.12	80	192.168.121.59	52678	HTTP	835 HTTP/1.1 200 OK (text/html)

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

Status code – 200, phrase - Ok

1259	2022/293 16:16:25.363281	128.119.245.12	80	192.168.121.59	52678	HTTP	835 HTTP/1.1 200 OK (text/html)

15. How many data-containing TCP segments were needed to carry the single HTTP response and

the text of the Bill of Rights?

A. 3

Filter btw http response we got should be servers ip address. Reassembled-updated data. We have only 3 tcp reassembled because it depends on the size of the data and there is no fix number of reassembled data.

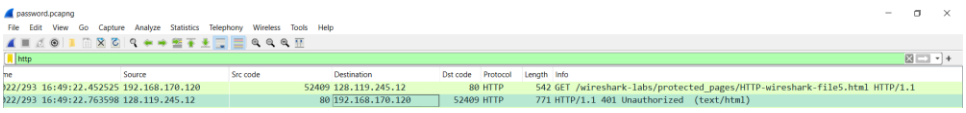
1254	2022/293 16:16:25.360163	128.119.245.12	80	192.168.121.59	52678	TCP	54 80 → 52678 [ACK] Seq=1 Ack=480 Win=30336 Len=0
1255	2022/293 16:16:25.360249	128.119.245.12	80	192.168.121.59	52678	TCP	1414 80 → 52678 [ACK] Seq=1 Ack=480 Win=30336 Len=1360 [TCP segment
1256	2022/293 16:16:25.360294	128.119.245.12	80	192.168.121.59	52678	TCP	1414 80 → 52678 [ACK] Seq=1361 Ack=480 Win=30336 Len=1360 [TCP segm
1257	2022/293 16:16:25.360463	192.168.121.59	52678	128.119.245.12	80	TCP	54 52678 → 80 [ACK] Seq=480 Ack=2721 Win=66560 Len=0
1258	2022/293 16:16:25.362219	128.119.245.12	80	192.168.121.59	52678	TCP	1414 80 → 52678 [ACK] Seq=2721 Ack=480 Win=30336 Len=1360 [TCP segm
1259	2022/293 16:16:25.363281	128.119.245.12	80	192.168.121.59	52678	HTTP	835 HTTP/1.1 200 OK (text/html)

4.)

16. What is the server's response (status code and phrase) in response to the initial HTTP GET

message from your browser?

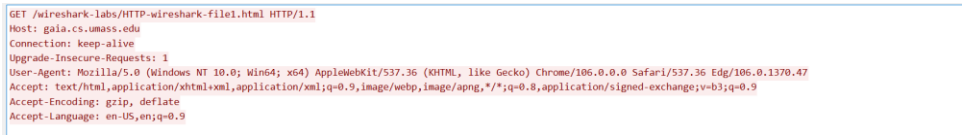
Status code 401, phrase - Unauthorized



17. When your browser sends the HTTP GET message for the second time, what new field is included

in the HTTP GET message?

For first get request we wont have any authorization header



But whereas for second get we have Authorization

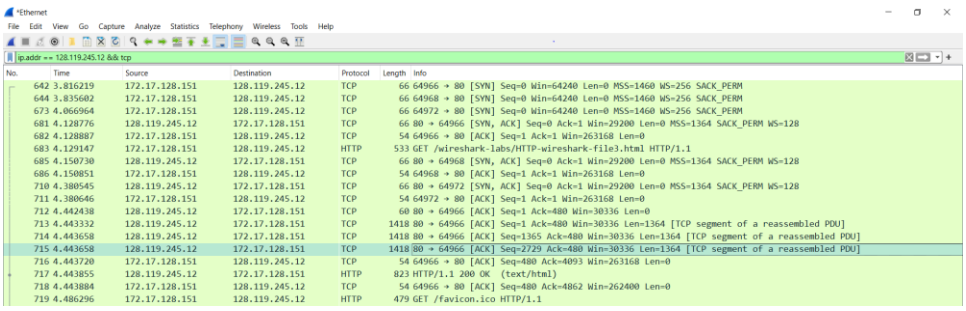
<u>Result:</u>

Thus, explored the web application protocols using protocol analyzer successfully.

Notes:

To analyze we use tcp not http

Ip.addrr==128.119.245.12 && tcp



Http-tcp working for transferring protocol, tcp sharing on behalf of http,
so we get the same data
in some cases

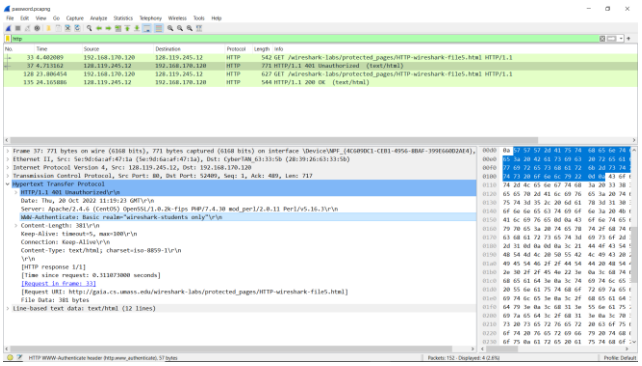
tcp.stream eq 10

we get the same thing for follow for both tcp and http

Ex: website to YouTube
In the obj if we see
there's one page we see html page and another is some data
I.e., due to vulnerabilities.

- means path and it contains data to be explored

authorization



401,304,200

We are getting credentials, and password is encrypted using bay 64

We are using basic authorization tech