Name:	Bodhisatya Ghosh
Class:	CSE DS
Batch:	B
UID:	2021700026
Experiment:	3

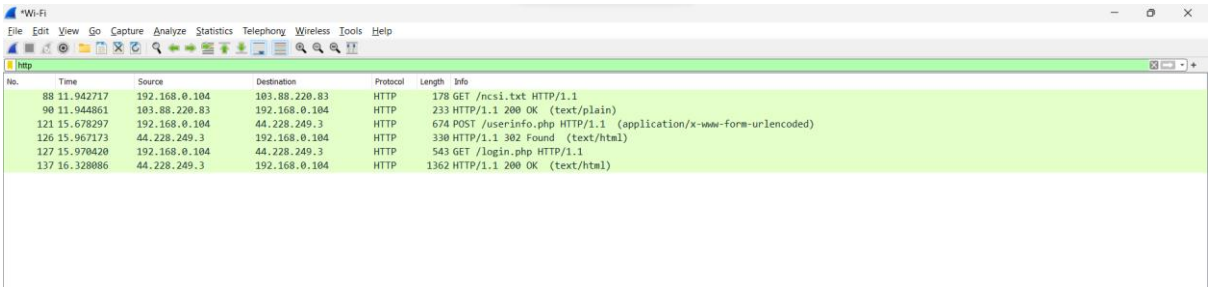
Aim: Experiment with Packet Analyzers – Wireshark. (Complete Various tasks given on website provided)

Task A: By looking at the information in the HTTP GET and response messages, answer the following (7) questions. When answering the following questions, you should print out the GET and response messages (to include the packet data in your own report, you may export the selected packet data as a text file. To do so, use the File->Export->File... window, select file type as Plain text, and choose "Selected packet" and indicate where in the message you've found the information that answers the following questions. (Note that the export procedure might differ based on the platform on which you are running Wireshark; e.g., SUN, Windows, etc.)

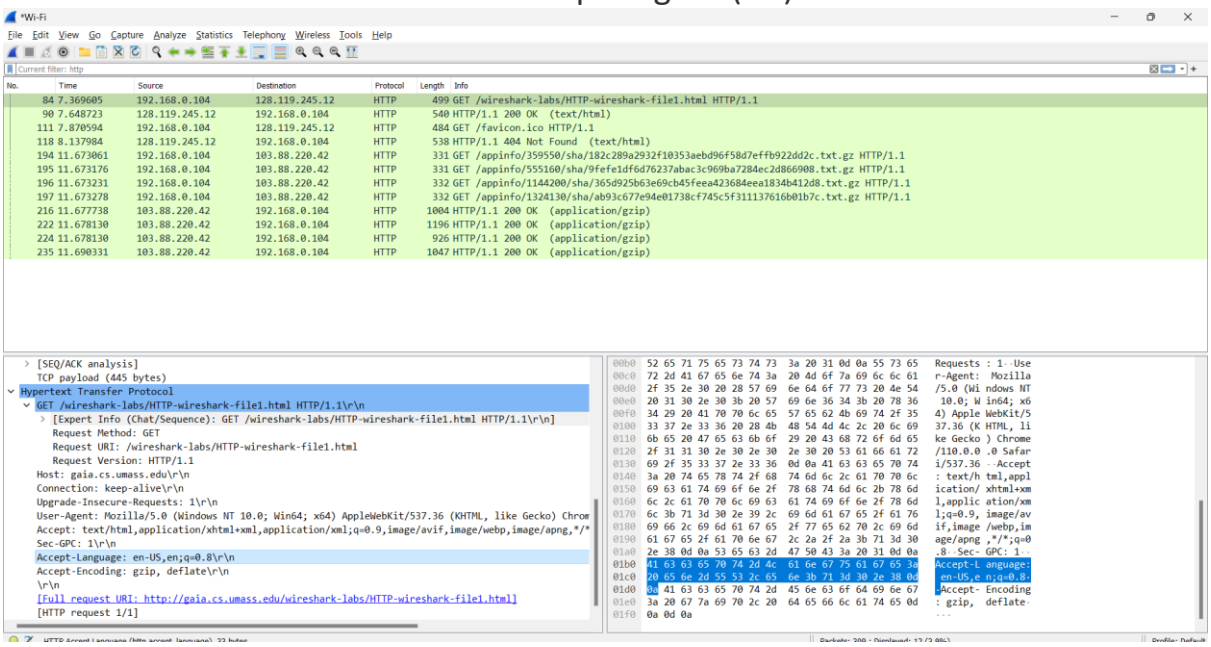
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. What is the status code returned from the server to your browser?
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?
7. By inspecting the raw data in the "packet bytes" pane, do you see any http headers within the data that are not displayed in the "packet details" pane? If so, name one.

Answers:

1. My browser is running HTTP version 1.1. The server is also running HTTP 1.1 version.

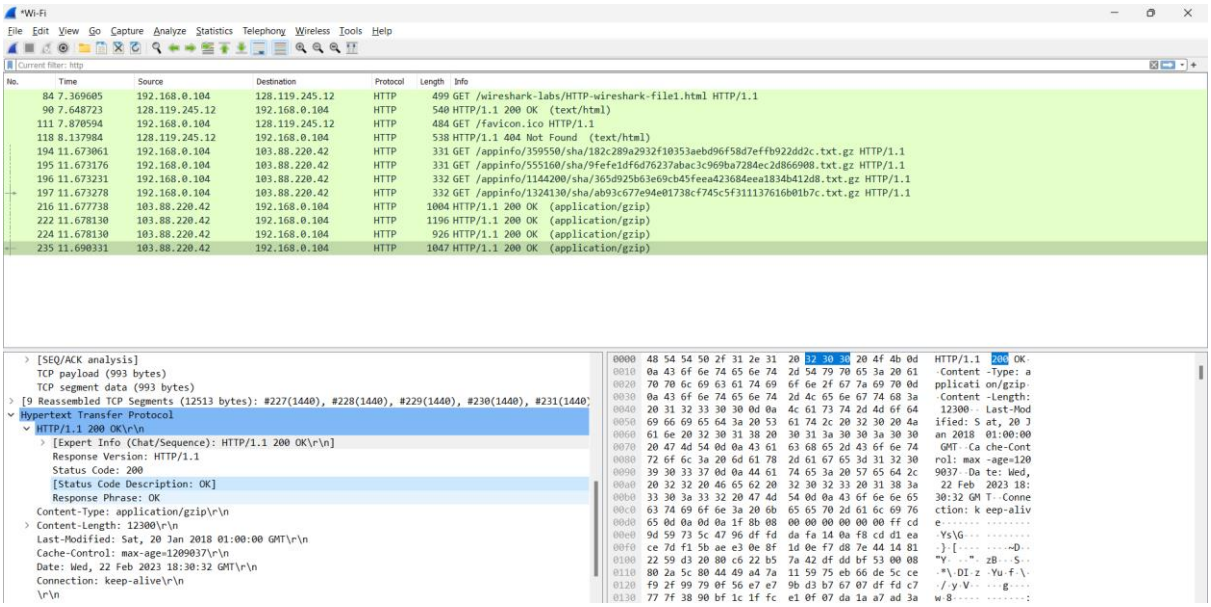


2. The browser indicates that it can accept English (US).

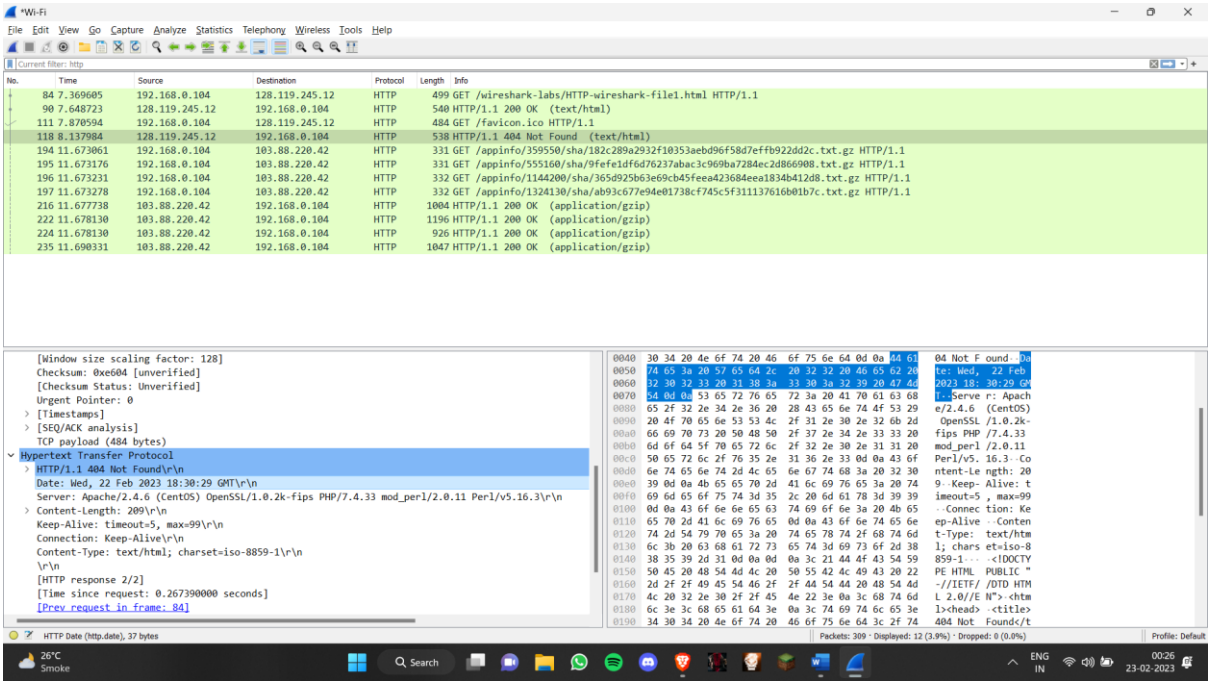


3. IP of computer: 192.168.0.104
   IP of server: 128.119.245.12

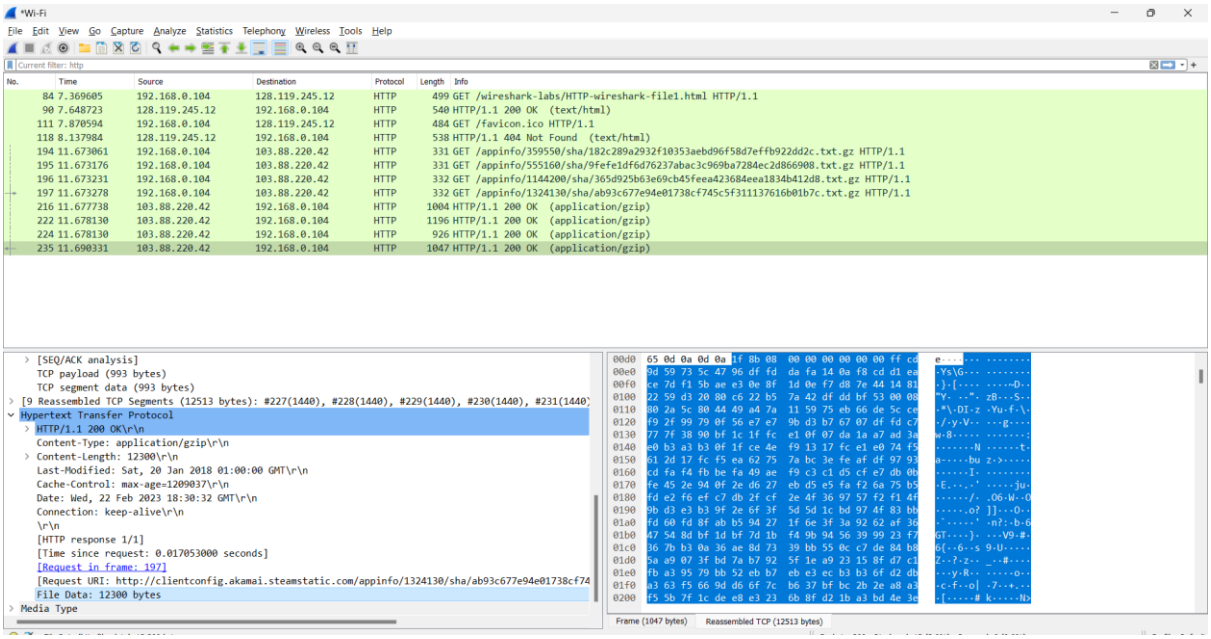
4. The returned status code is : 200



5. The HTML file was last modified on Wednesday, 22 February 2023 18:30:29 GMT



6. 12300 Bytes of total data is transferred.



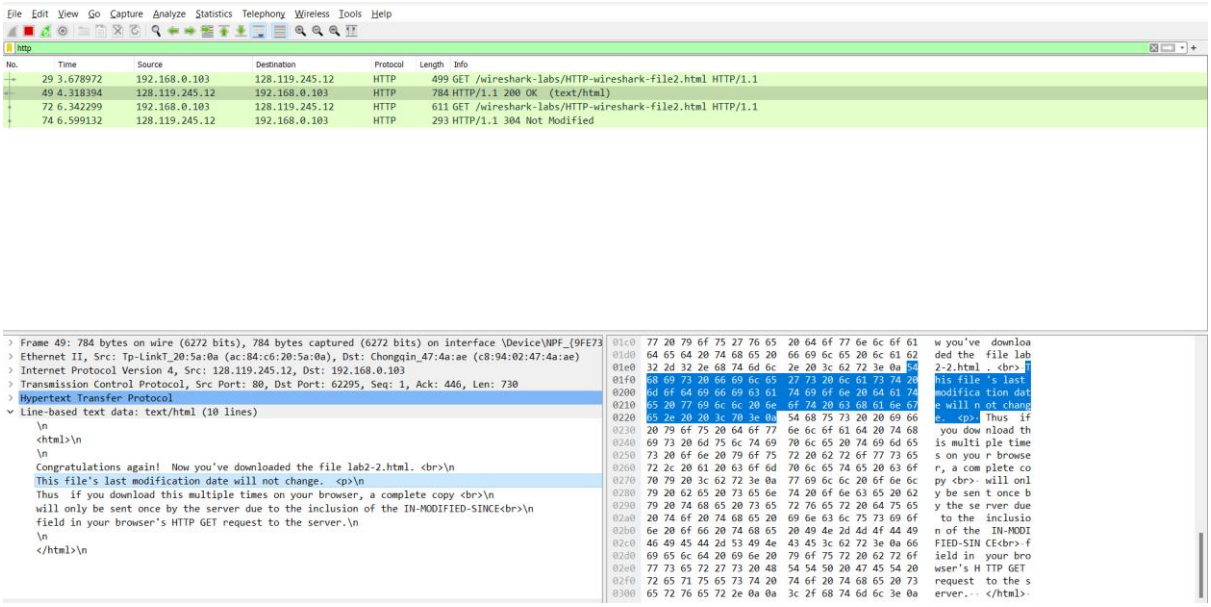
7.

Task B: For questions 8-11, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

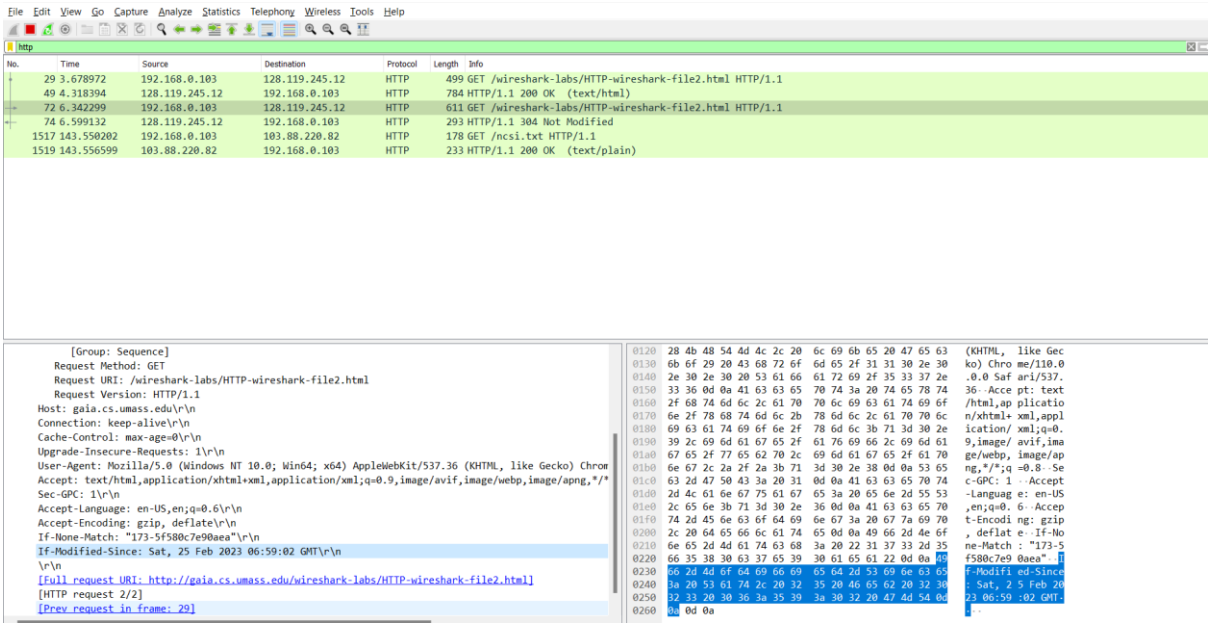
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
10. Now inspect the contents of the 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?
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.

Answers:

8. No, there is no “IF-MODIFIED-SINCE” line in the first HTTP GET.
9. Yes, the server explicitly returned the contents of the file as seen below

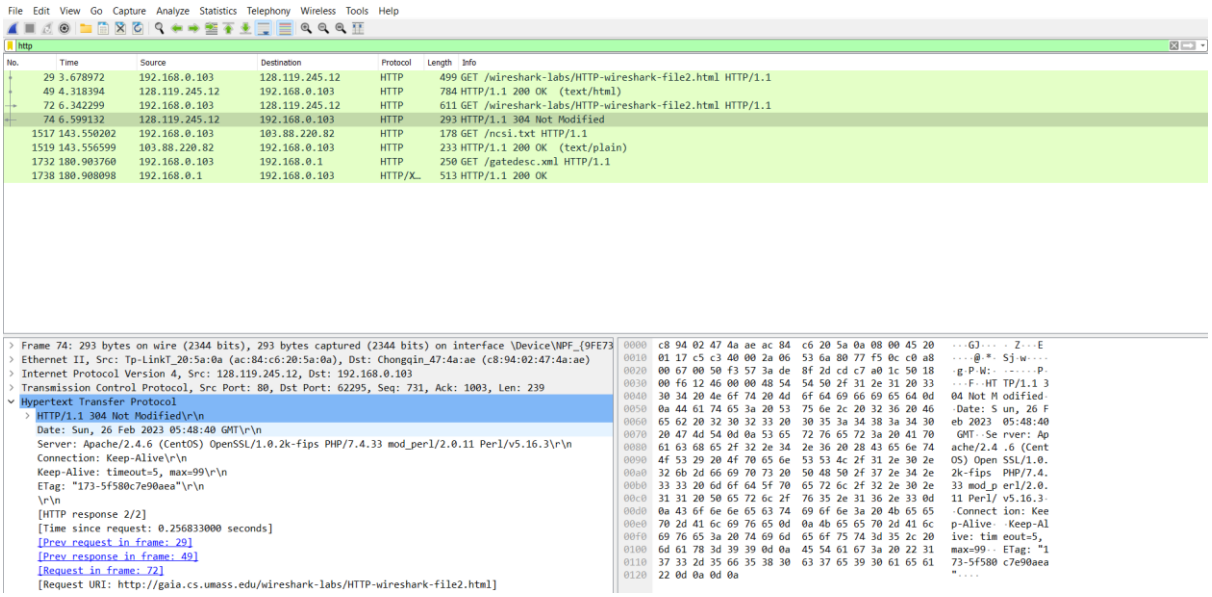


10. Yes, there is an “IF-MODIFIED-SINCE:” line in the second HTTP GET.



This header shows the last date at which the file was last modified.

11. The HTTP status code returned after second GET request is 304. No, the server did not return any file. The phrase returned was “NOT MODIFIED”.



Task C: For questions 12-15, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

12. How many HTTP GET request messages were sent by your browser?
13. How many data-containing TCP segments were needed to carry the single HTTP response?
14. What is the status code and phrase associated with the response to the HTTP GET request?
15. Is there any HTTP header information in the transmitted data associated with TCP segmentation?

Answers:

12. 1 HTTP GET request was sent by the browser.
13. 4 data-containing TCP segments were needed to carry the single HTTP response.
14. Status code returned : 200(OK)
15. NAA

Task D: For questions 16-17, first write a brief but precise answer for each of the above questions, then write a paragraph explaining and

discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
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.

Answers:

16. 3 HTTP GET messages were sent by my browser. The addresses to which they were sent to are
    i. wireshark-labs/HTTP-wireshark-file4.html
    ii. /8E_cover_small.jpg
    iii. /pearson.png
17. As we can see, the last modified date and time of both files are exactly the same. Therefore, we can say both responses were enacted parallelly.

Conclusion: In this experiment I have learnt how to analyze a network and it's components using a packet sniffer like WireShark.