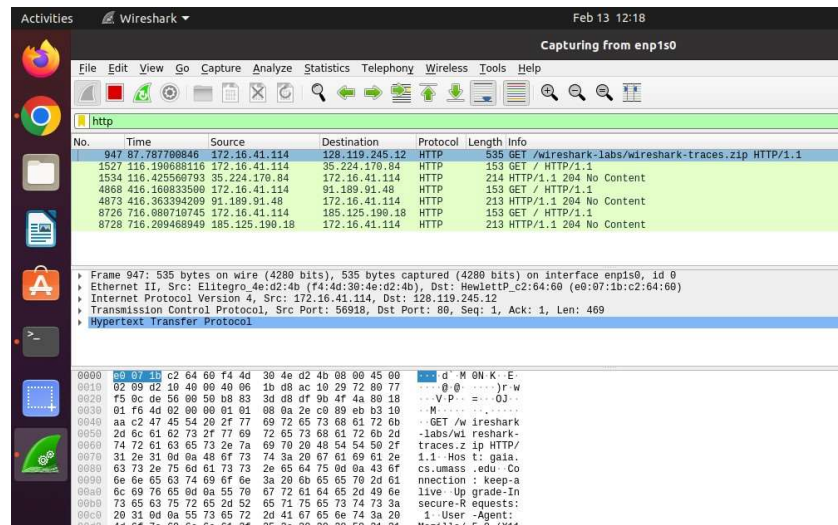


Name:	ATUL SHARMA
UID:	2021700060
Batch	D(DS)
Experiment No:	3
Aim:	Using wireshark for network protocol and packet transfer analysis.

Theory:

1. The Basic HTTP GET/response interaction



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

⑨ Our browser is running Http version 1.1.

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?

→: My browser indicates that it can accepts en-US and en to the server.

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

⑨ Our computer IP address is 172.16.41.114 and gaia.cs.umass.edu IP address is 128.119.245.12

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

⑨ Computer returned status code – 204

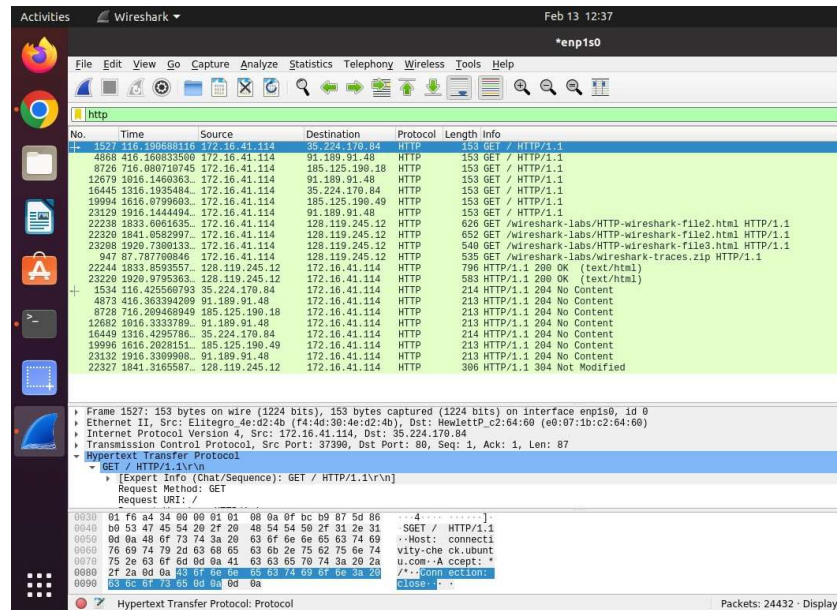
5. How many bytes of content are being returned to your browser?

⑨ 535 bytes.

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

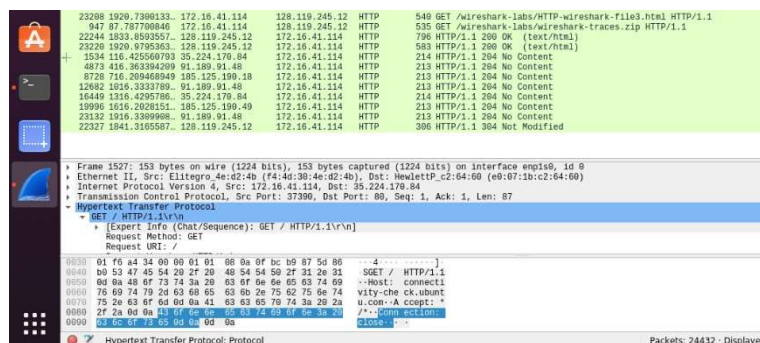
⑨ The timing is 716.21 s.

2. The HTTP CONDITIONAL GET/response interaction



7. 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 No, I do not see an “IF-MODIFIED-SINCE” line in the HTTP GET.
8. 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.
⑨ The HTTP status code and phrase returned from the server is 200 (OK). Yes, the server explicitly returned the contents of the file.

3. Retrieving Long Documents

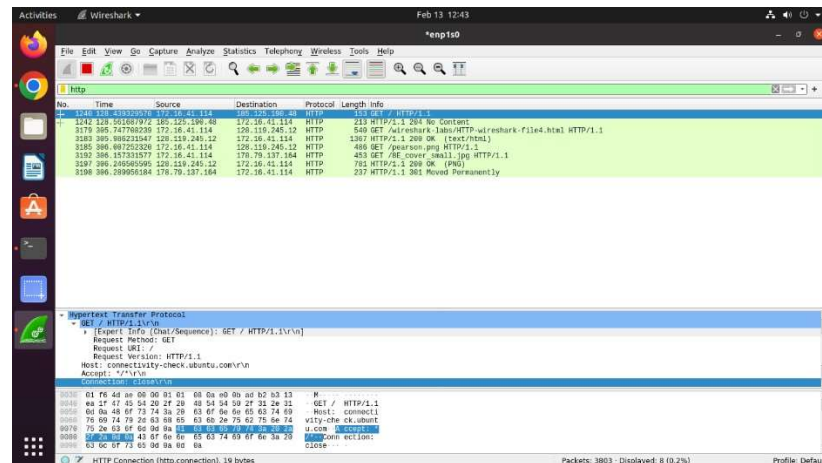


	<p>9. How many HTTP GET request messages were sent by your browser?</p>
--	---

- 9 My browser sent two HTTP GET request message.
10. What is the status code and phrase associated with the response to the HTTP GET request?
- 9 The status code and phrase associated with the response to the HTTP GET request is 200 and “OK” respectively.
11. Q15) Is there any HTTP header information in the transmitted data associated with TCP segmentation?
- 9 No, there are no HTTP header information in the transmitted data associated with TCP segmentation.

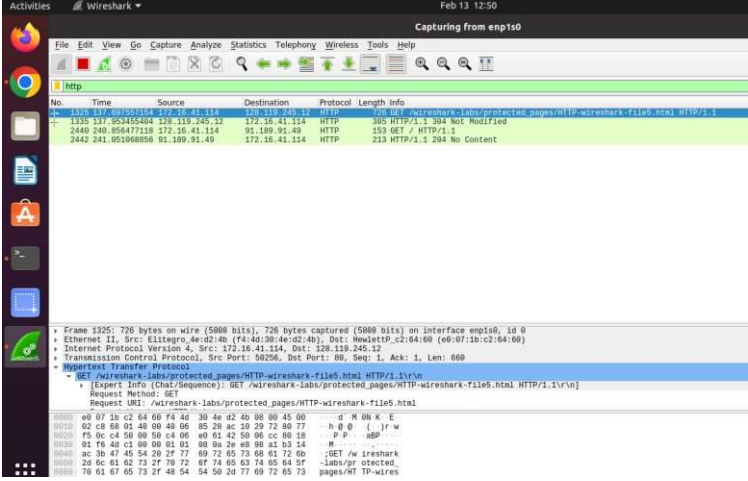
HTML Documents with Embedded Objects

4.



- How many HTTP GET request messages were sent by your browser? To which
12. Internet addresses were these GET requests sent?
- 9 My browser sent three HTTP GET request messages. Addresses are /wiresharklabs/HTTP-wireshark-file4.html, /pearson.png and /8E_cover_small.jpg.
13. Can you tell whether your browser downloaded by two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
- 9 Images were downloaded serially.

5. HTTP Authentication

	 <p>The screenshot shows the Wireshark interface with a packet list on the left and packet details on the right. The packet list shows an HTTP GET request (No. 1325) and its response (No. 1326). The packet details pane shows the response status code 304 and the phrase 'Not Modified'.</p> <p>14. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?</p> <p>⑨ The server’s response in response to the initial HTTP GET message from my browser is 304 and phrase is “Not Modified”.</p>
<p>Conclusion:</p>	<p>Through this experiment , I learnt wireshark software and how we can use it to analyze packet transfer and it also help in getting total number of bytes transferred, time take and IP address of sender and receiver.</p>