Pandit Deendayal Energy University
School of Technology
Department of ICT
Academic Year: 2022-23
Computer Communication and Networking Lab
20IC306P

Name: Jankar Patel

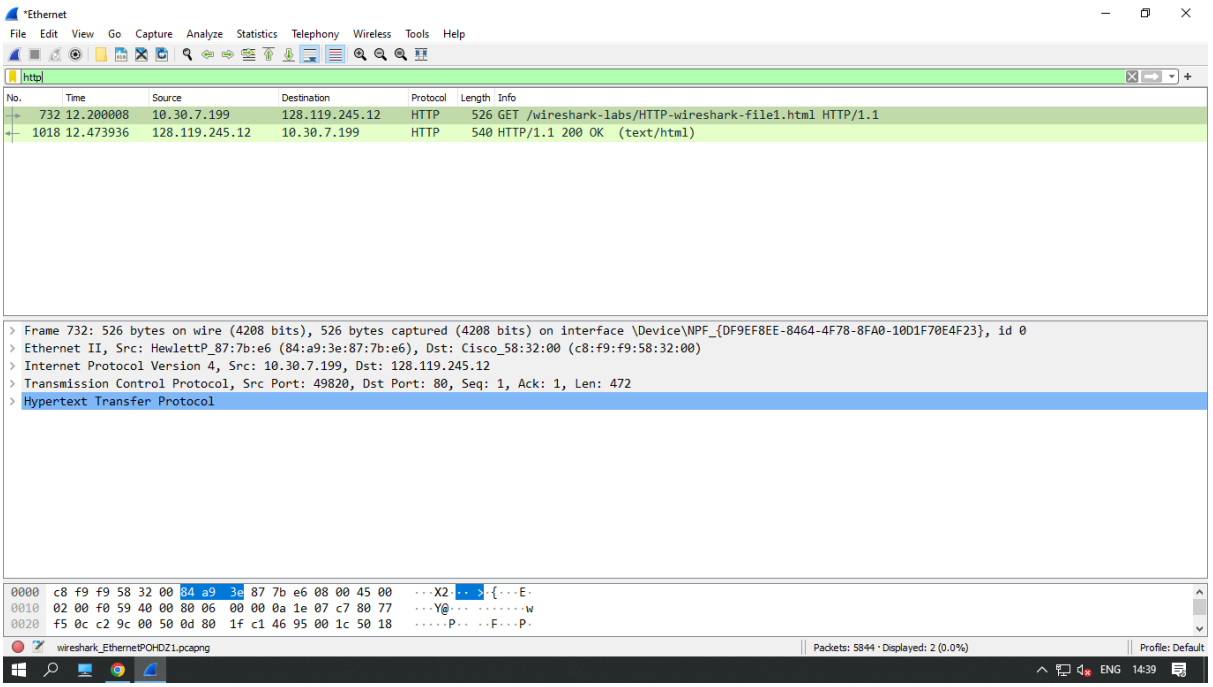
Roll No: 20BIT061

Experiment 3:

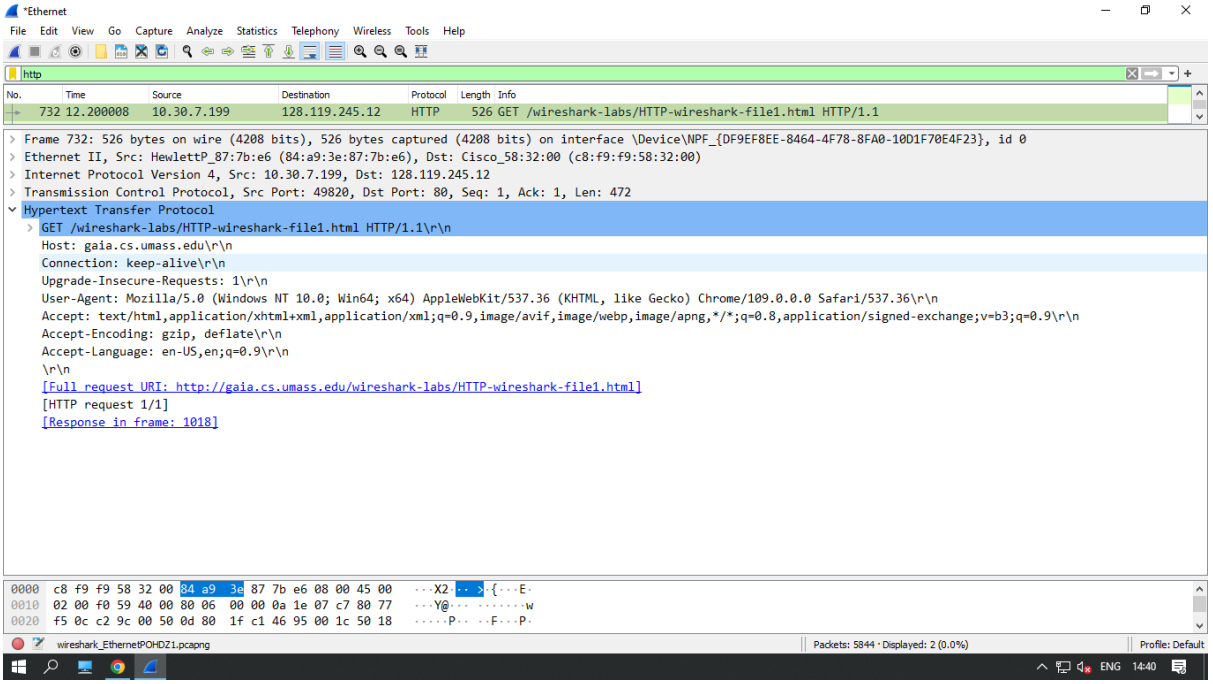
Aim: To understand the functionality of HTTP using Wire-shark and Packet Tracer

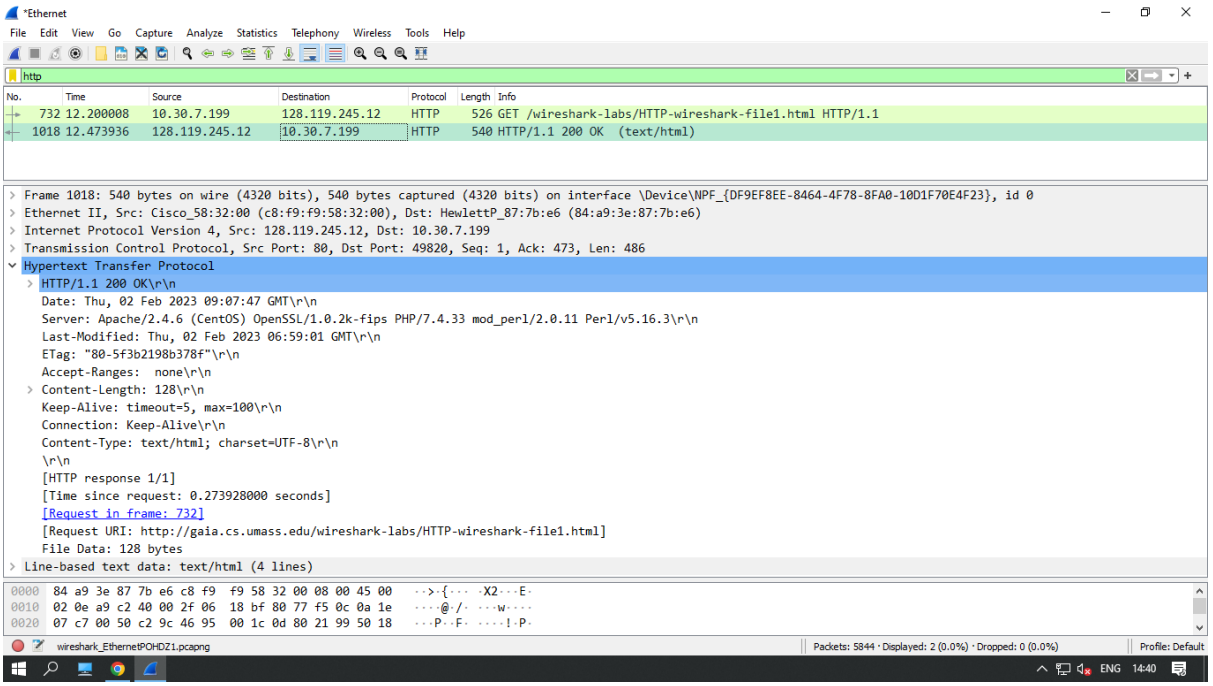
Software Tools required: - Wire-shark and Cisco packet tracer

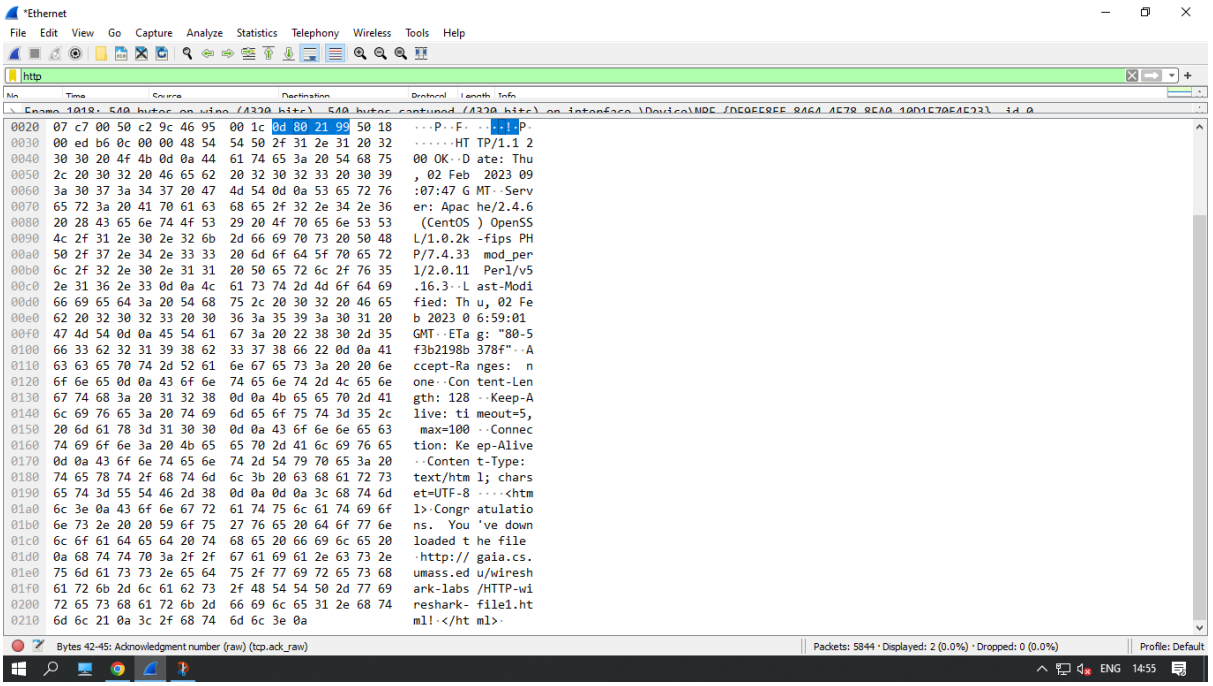
Task 1: Understand HTTP and capture HTTP packets through wire-shark and analyse those packets. Answer all the questions. Write down notes and remarks for your reference whenever required.



1. The Basic HTTP GET/response interaction

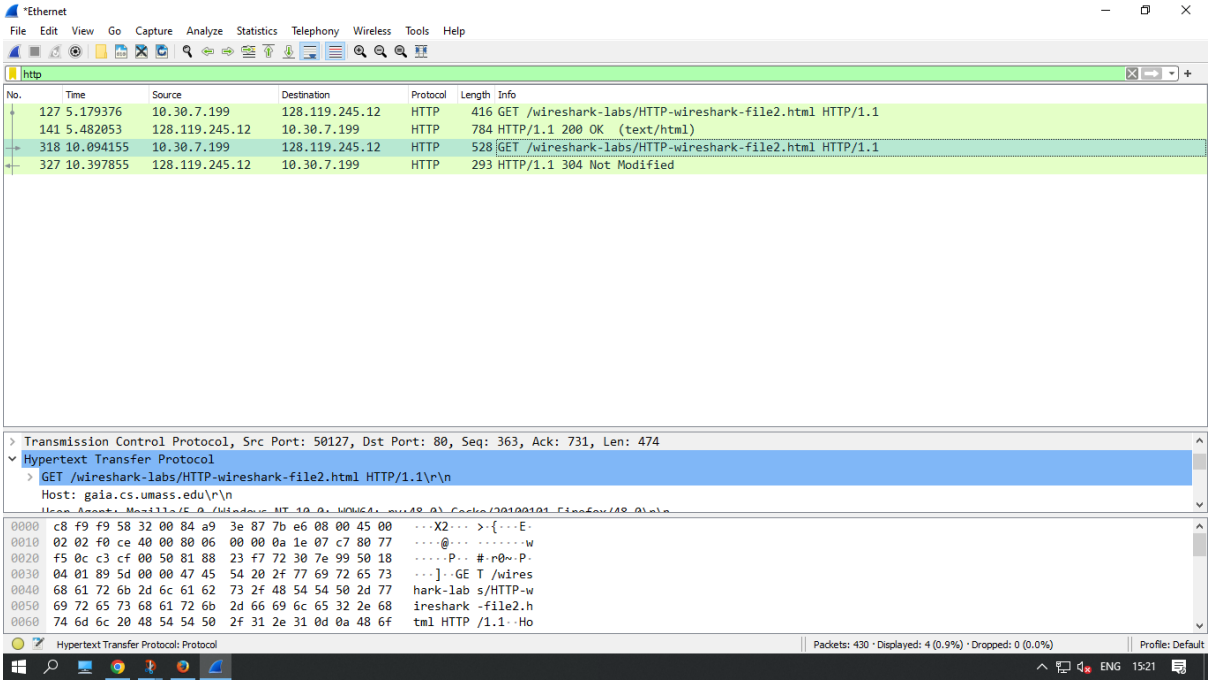


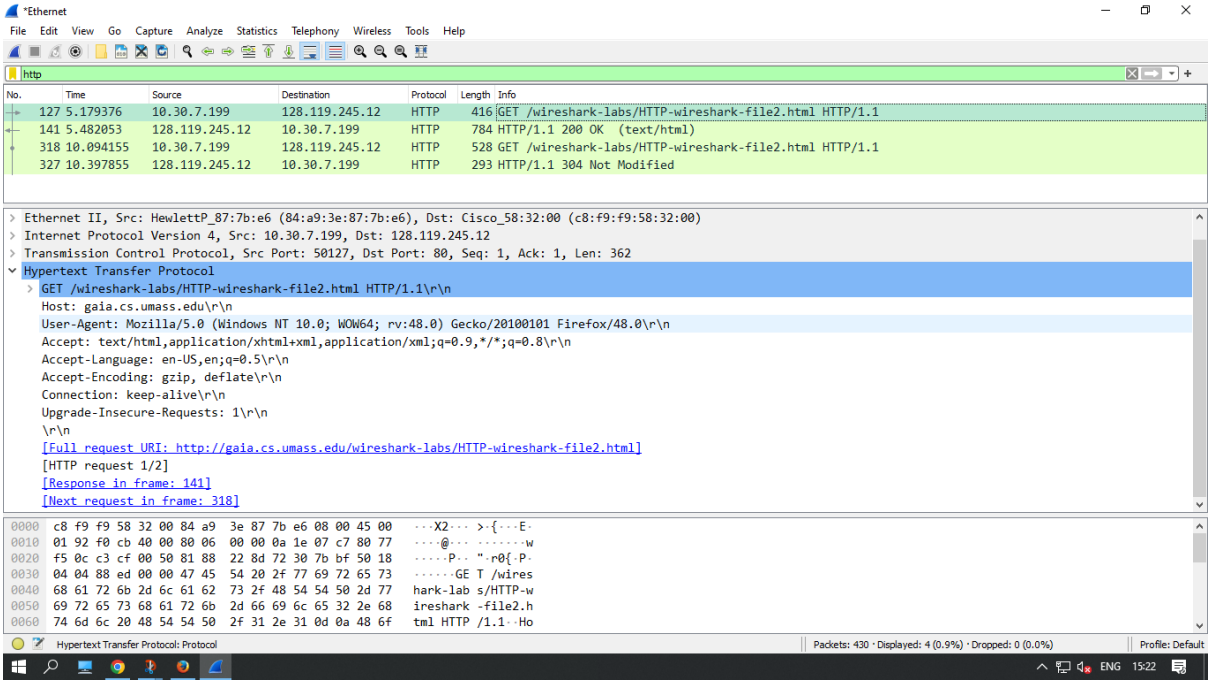


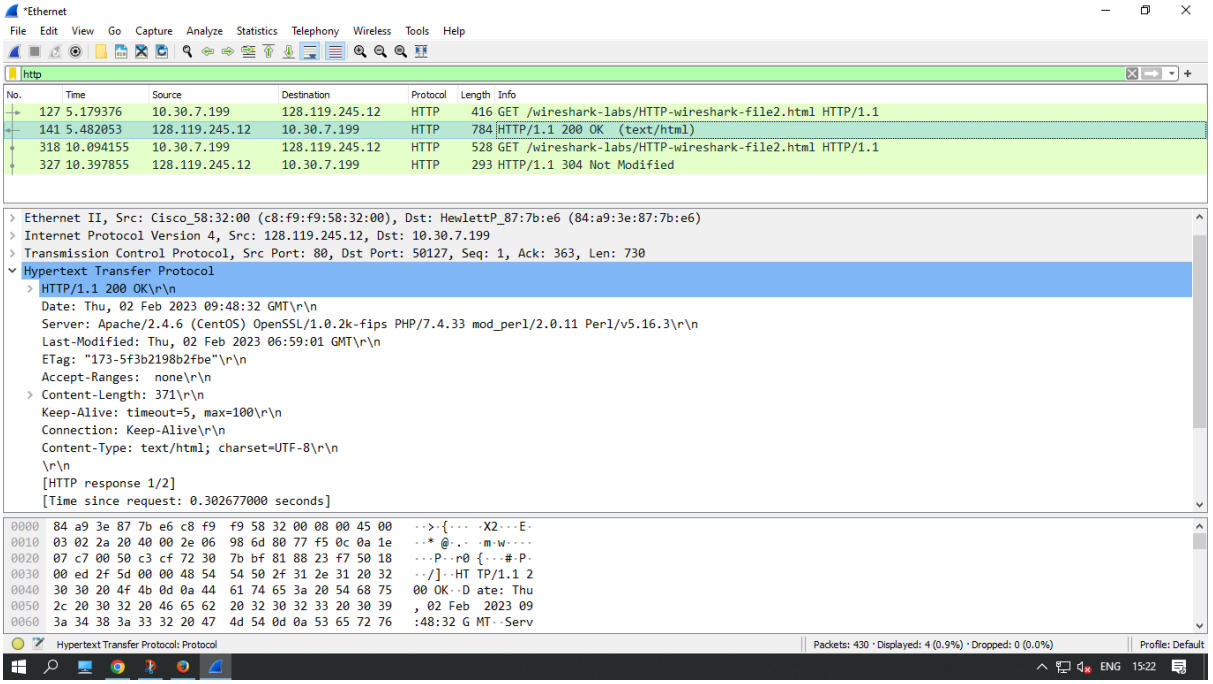


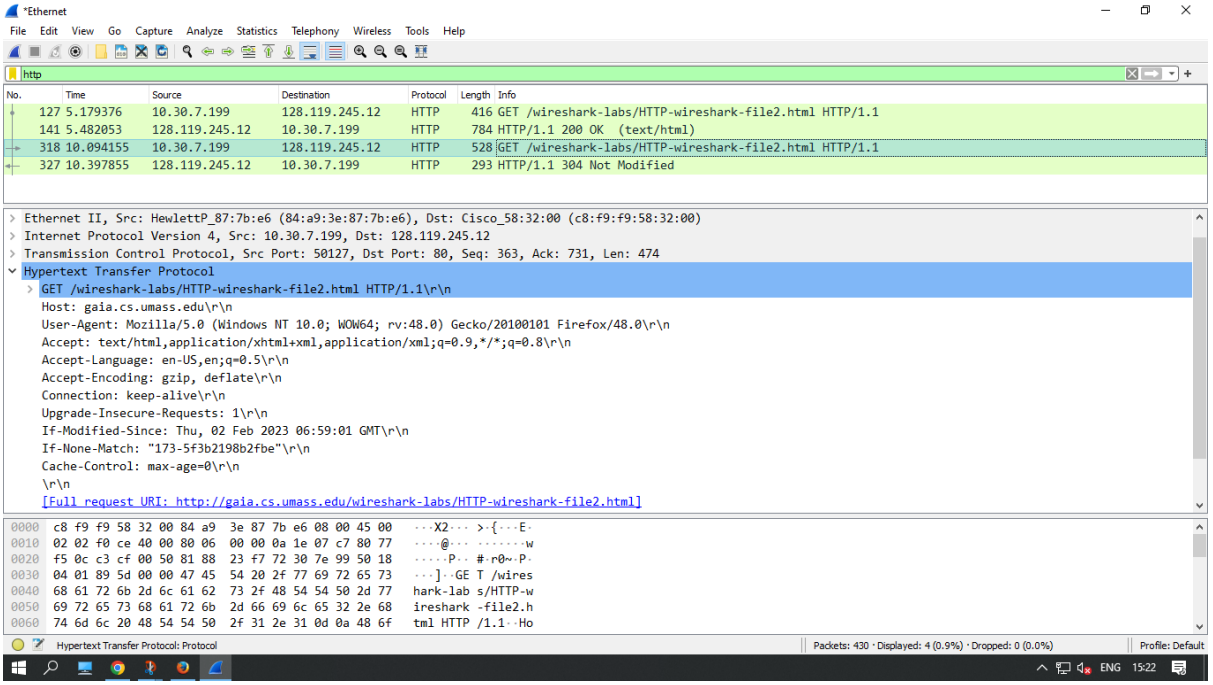
1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?
   Ans: Browser and the server both running on HTTP 1.1 Version.
2. What languages (if any) does your browser indicate that it can accept to the server?
   Ans: It indicates that the server accepts the English US Language.
3. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?
   Ans: Computer IP Address: 10.30.7.199, Server IP Address: 128.119.245.12
4. What is the status code returned from the server to your browser?
   Ans: Status Code 200 OK returned from the server.
5. When was the HTML file that you are retrieving last modified at the server?
   Ans: HTML file was modified: Thursday, 02 Feb 2023 06:59:01 GMT.
6. How many bytes of content are being returned to your browser?
   Ans: The length of content returned is 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.
   Ans: None, All the headers are visible.

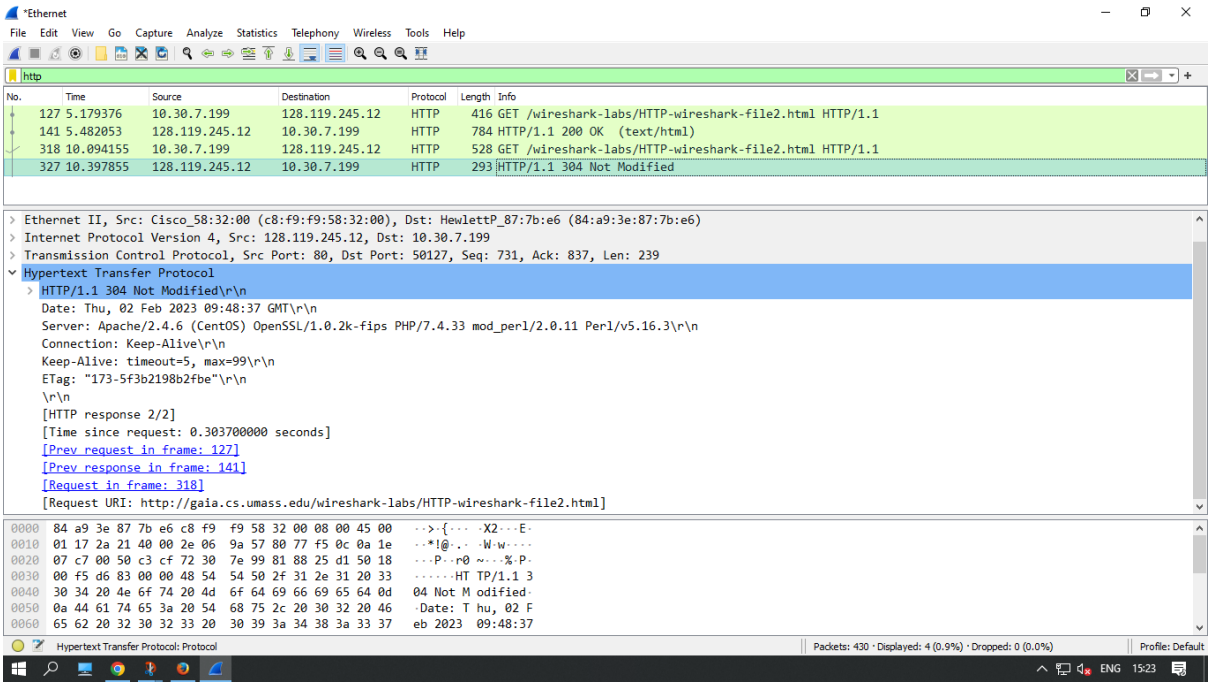
2. The HTTP CONDITIONAL GET/response interaction






*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
127 5.179376 10.30.7.199 128.119.245.12 HTTP 416 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
141 5.482053 128.119.245.12 10.30.7.199 HTTP 784 HTTP/1.1 200 OK (text/html)
318 10.094155 10.30.7.199 128.119.245.12 HTTP 528 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
327 10.397855 128.119.245.12 10.30.7.199 HTTP 293 HTTP/1.1 304 Not Modified
Ethernet II, Src: Cisco_58:32:00 (c8:f9:f9:58:32:00), Dst: HewlettP_87:7b:e6 (84:a9:3e:87:7b:e6)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.30.7.199
Transmission Control Protocol, Src Port: 80, Dst Port: 50127, Seq: 1, Ack: 363, Len: 730
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 02 Feb 2023 09:48:32 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Thu, 02 Feb 2023 06:59:01 GMT\r\n
ETag: "173-5f3b2198b2fbe"\r\n
Accept-Ranges: none\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.302677000 seconds]
0000 84 a9 3e 87 7b e6 c8 f9 f9 58 32 00 08 00 45 00
0010 03 02 2a 20 40 00 2e 06 98 6d 80 77 f5 0c 0a 1e
0020 07 c7 00 50 c3 cf 72 30 7b bf 81 88 23 f7 50 18
0030 00 ed 2f 5d 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75
0050 2c 20 30 32 20 46 65 62 20 32 30 32 33 20 30 39
0060 3a 34 38 3a 33 32 20 47 4d 54 0d 0a 53 65 72 76
Hypertext Transfer Protocol: Protocol
Packets: 430 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%)
Profile: Default
ENG 15:22

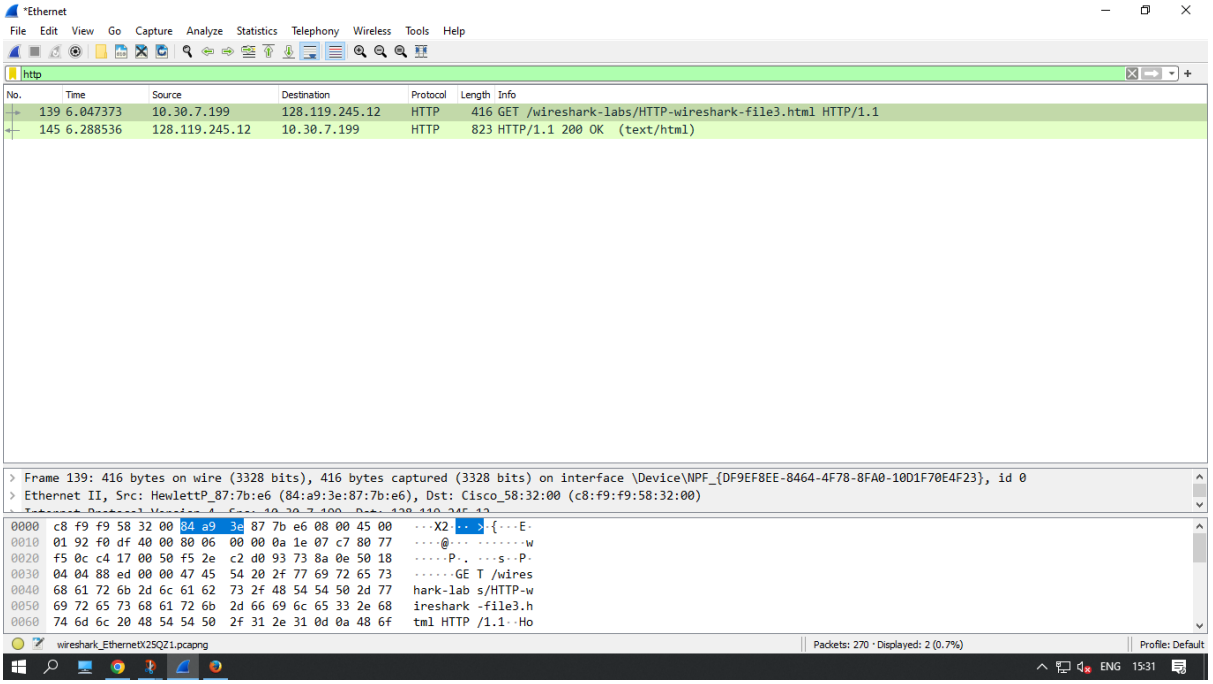

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
127 5.179376 10.30.7.199 128.119.245.12 HTTP 416 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
141 5.482053 128.119.245.12 10.30.7.199 HTTP 784 HTTP/1.1 200 OK (text/html)
318 10.094155 10.30.7.199 128.119.245.12 HTTP 528 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
327 10.397855 128.119.245.12 10.30.7.199 HTTP 293 HTTP/1.1 304 Not Modified
Ethernet II, Src: HewlettP_87:7b:e6 (84:a9:3e:87:7b:e6), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
Internet Protocol Version 4, Src: 10.30.7.199, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50127, Dst Port: 80, Seq: 363, Ack: 731, Len: 474
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Thu, 02 Feb 2023 06:59:01 GMT\r\n
If-None-Match: "173-5f3b2198b2fbe"\r\n
Cache-Control: max-age=0\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
0000 c8 f9 f9 58 32 00 84 a9 3e 87 7b e6 08 00 45 00
0010 02 02 f0 ce 40 00 80 06 00 00 0a 1e 07 c7 80 77
0020 f5 0c c3 cf 00 50 81 88 23 f7 72 30 7e 99 50 18
0030 04 01 89 5d 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
Hypertext Transfer Protocol: Protocol
Packets: 430 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%)
Profile: Default
ENG 15:22

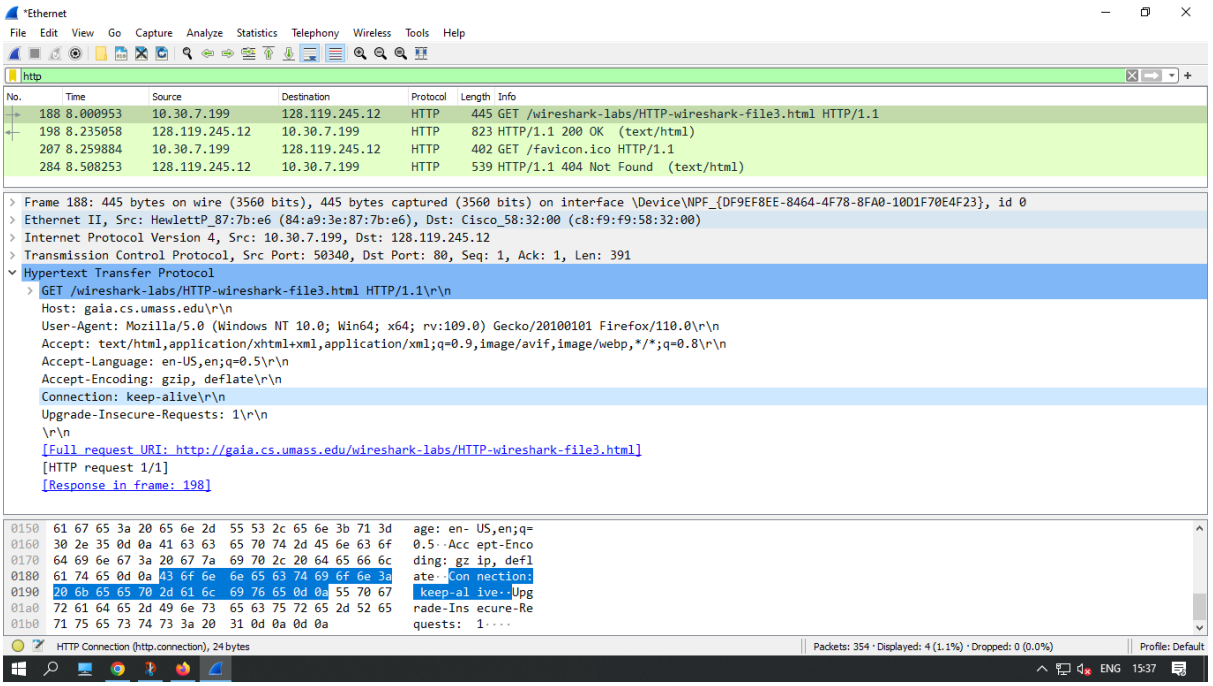


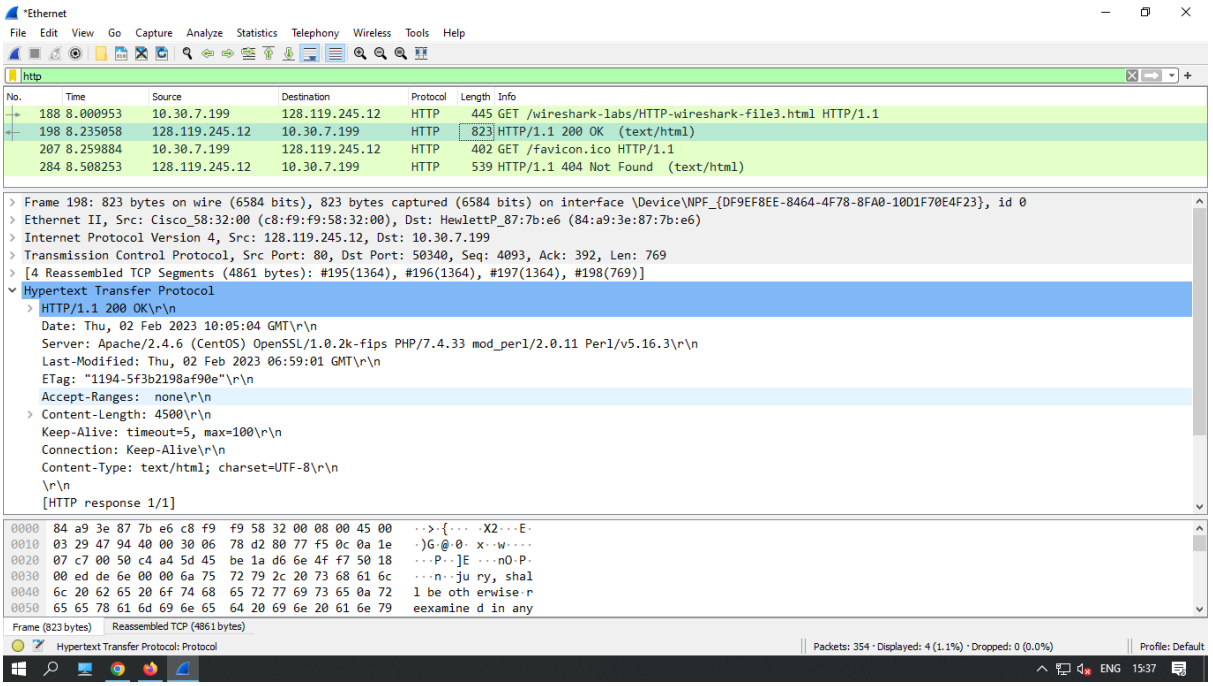
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
   Ans: Yes, the line is present in the GET request. it consists Thu, 02 Feb 2023 06:59:01 GMT.
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   Ans: Server responded with code 200 OK status code.
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[1]? If so, what information follows the “IF-MODIFIED-SINCE:” header?
    Ans: Yes, The line is present in the second response, but it responded with 304 not modified status code.
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.
    Ans: In the second response server responded with 304 NOT MODIFIED code. server is not returning explicitly.

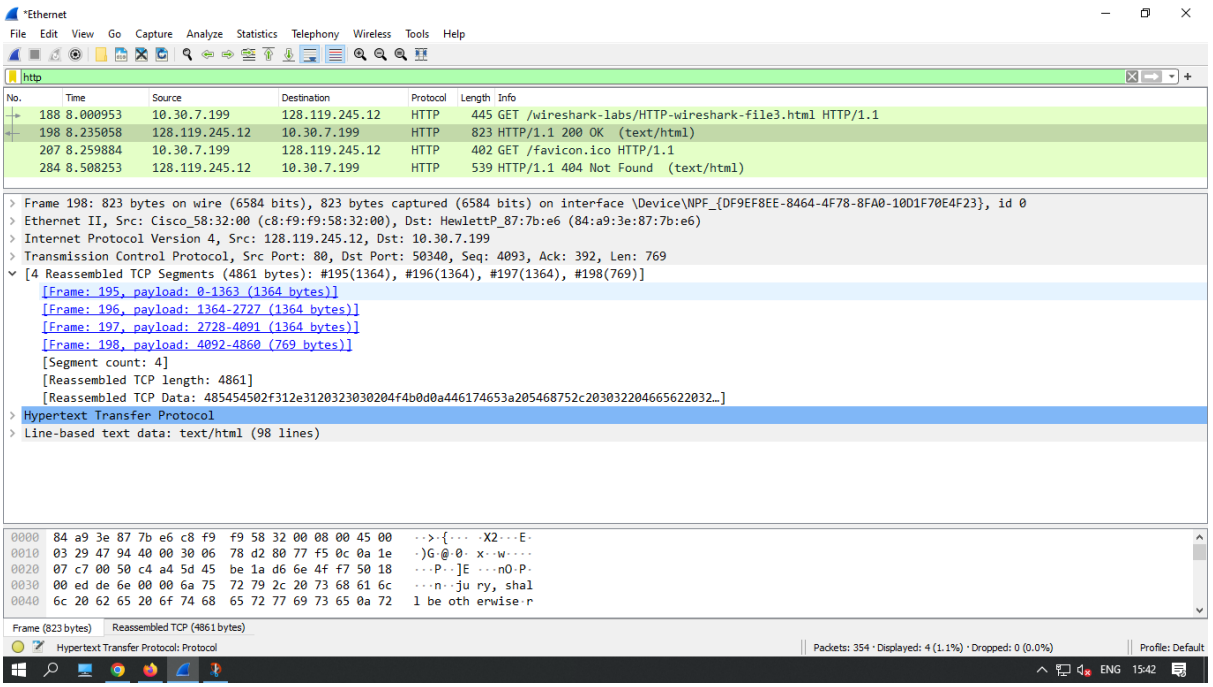
1

3. Retrieving Long Documents









Answer the following questions[2]:

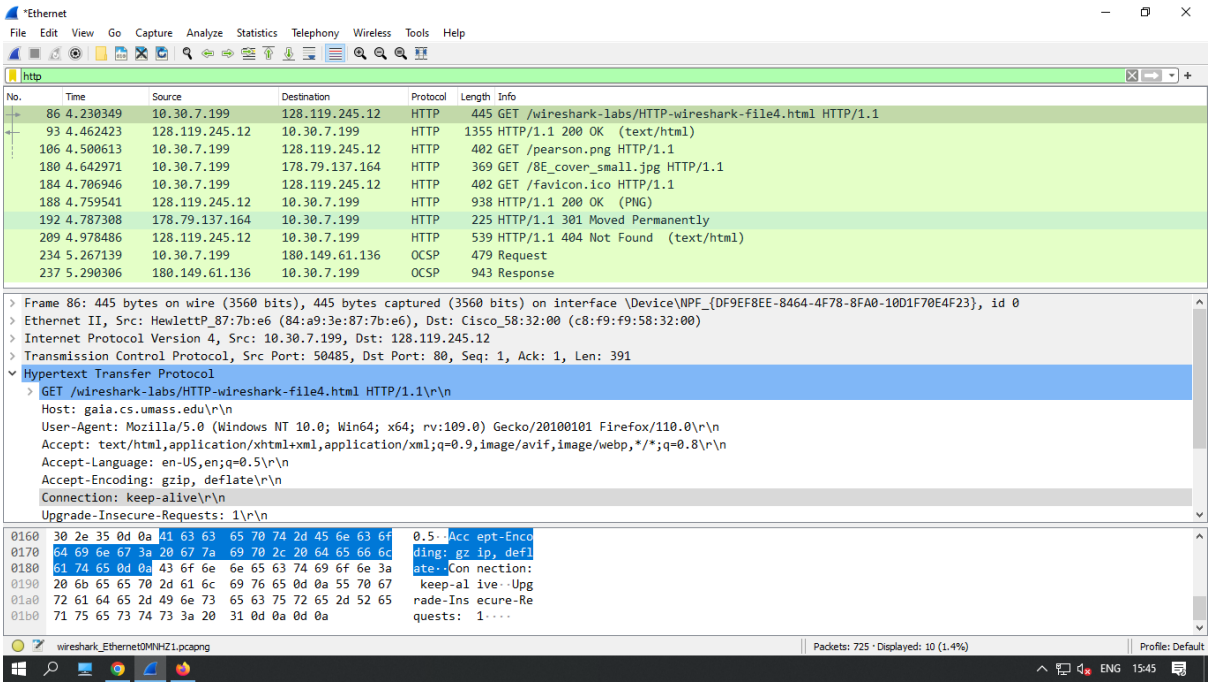
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
    Ans: One GET request is sent to the server. Packet number is 188.
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

2

Ans: Packet number is 198.

14. What is the status code and phrase in the response?
    Ans: Status code 200 OK in response.
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
    Ans: 4 TCP segments carry single HTTP.

4. HTML Documents with Embedded Objects

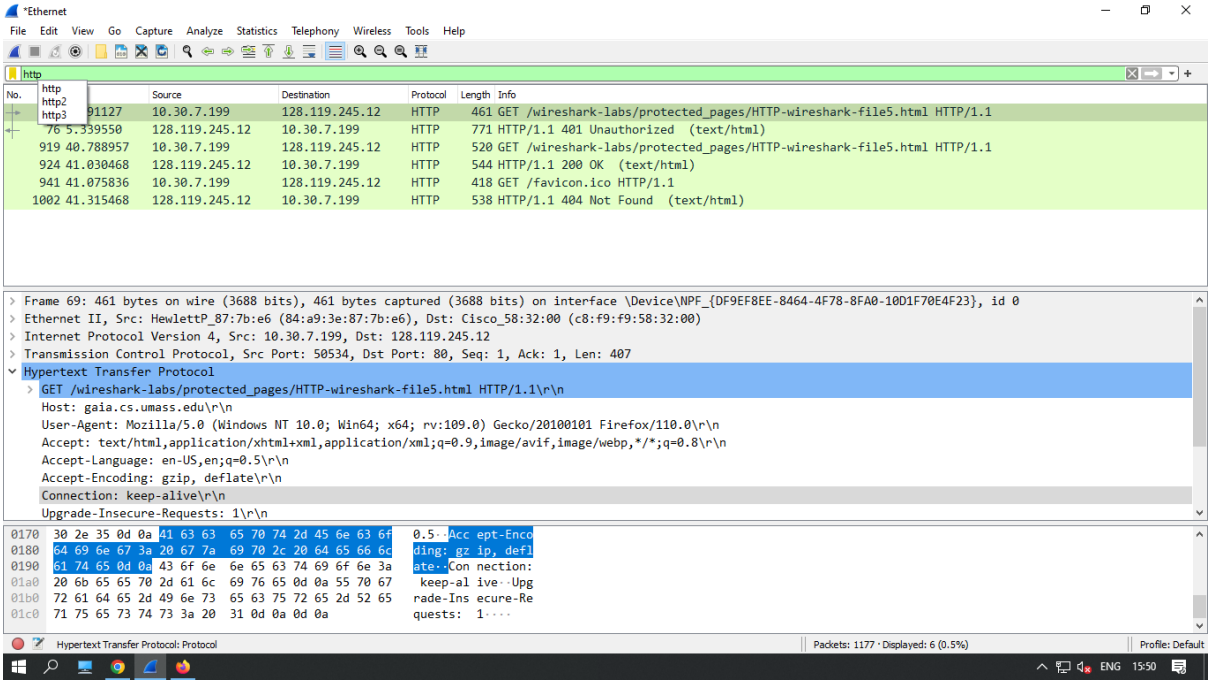


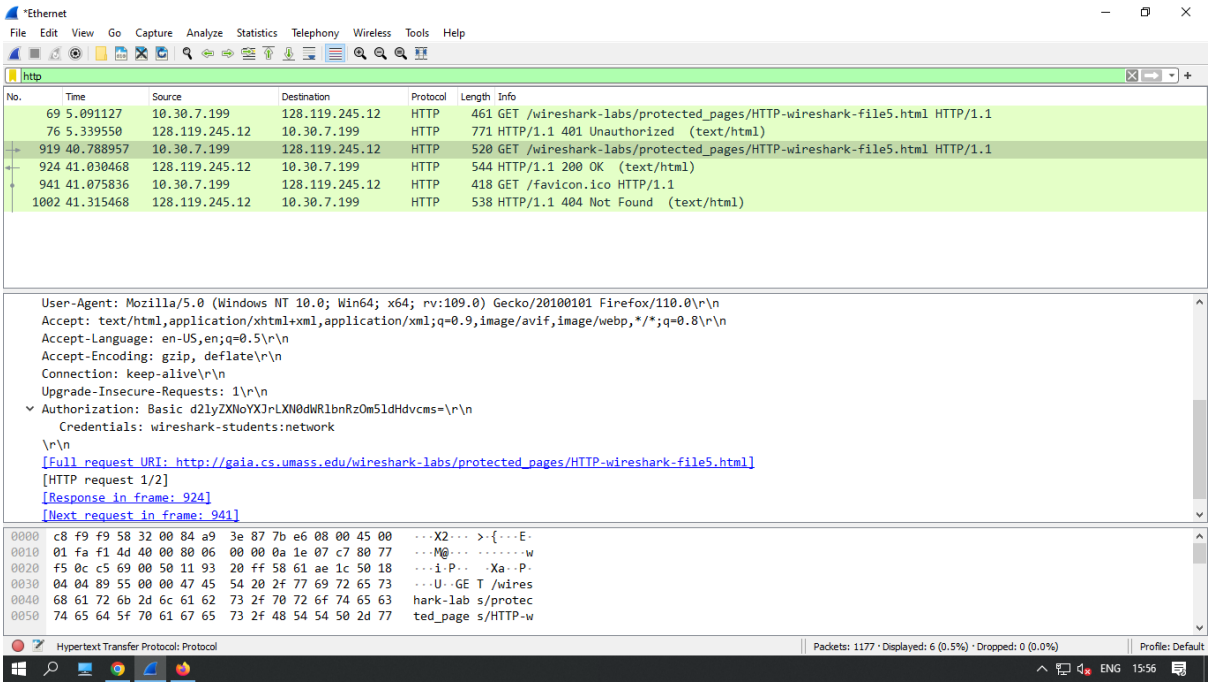
Answer the following questions[3]:

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    Ans: Three HTTP GET requests are sent. Address are 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 websites in parallel? Explain.
    Ans: Downloaded Parallel.

3

5 HTTP Authentication





Answer the following questions9:

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Ans: 401 Unauthorized and 200 OK status code.

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

Ans: Authorization.

Task 2: Configure a web server and use HTTP in packet tracer. Use a step by step approach with proper understanding of each step.