CMPE 472 – Computer Networks

Lab 1: HTTP (3 points)

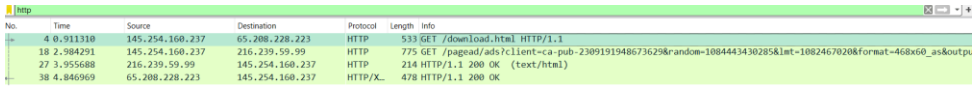
Please fill out this given form for your submissions.

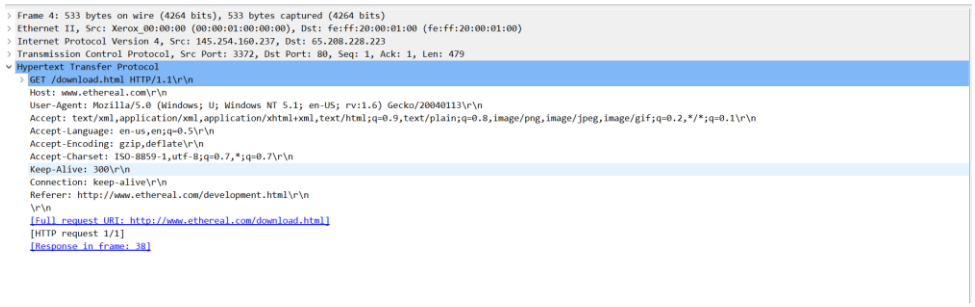
Questions

1. Open "http.cap" using Wireshark and fill in the table below inspecting frame 27. *(0.5 point)*

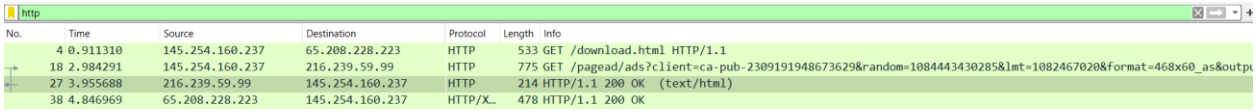
http version	accepted languages	return status	content length
HTTP 1.1	en-us,en;q=0.5	200 OK	1272

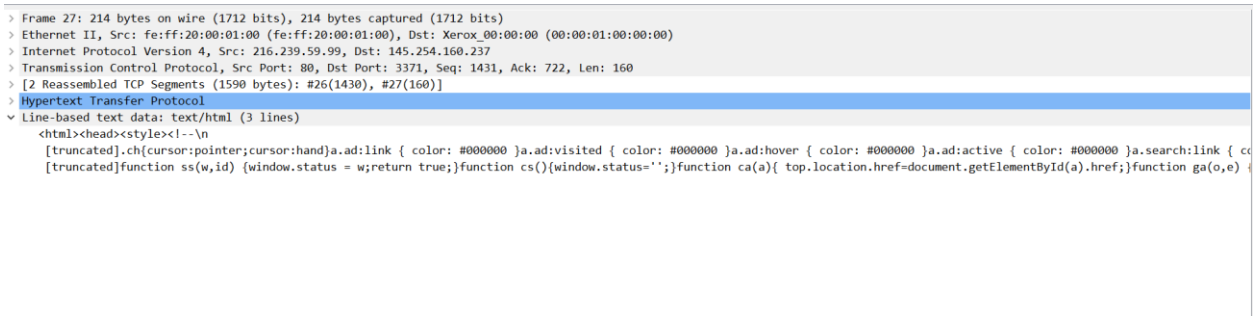
2. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET? *(0.5 points)* **No there is no IF-MODIFIED-SINCE line in the GET message**



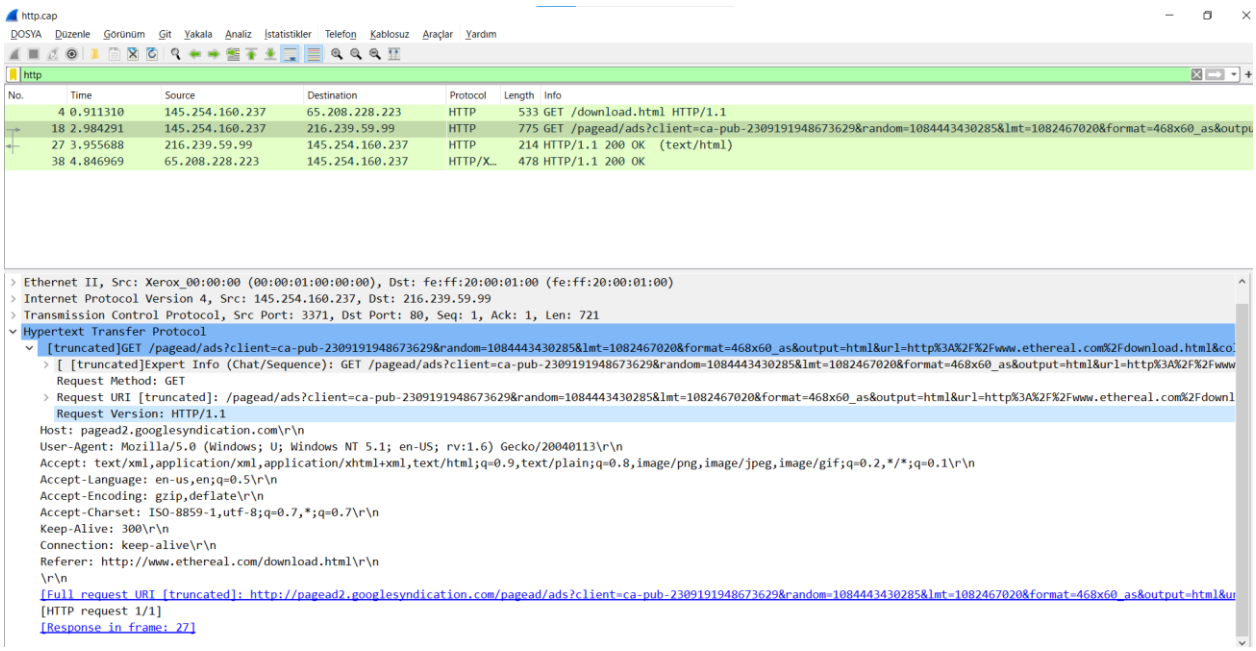


3. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? *(0.5 points)* **The "Line-Based Text Data" part of Wireshark displays what the server delivered back to my browser, more specifically, what the website displayed when I opened it up on my browser. The contents of the file were not, however, specifically returned by the server.**



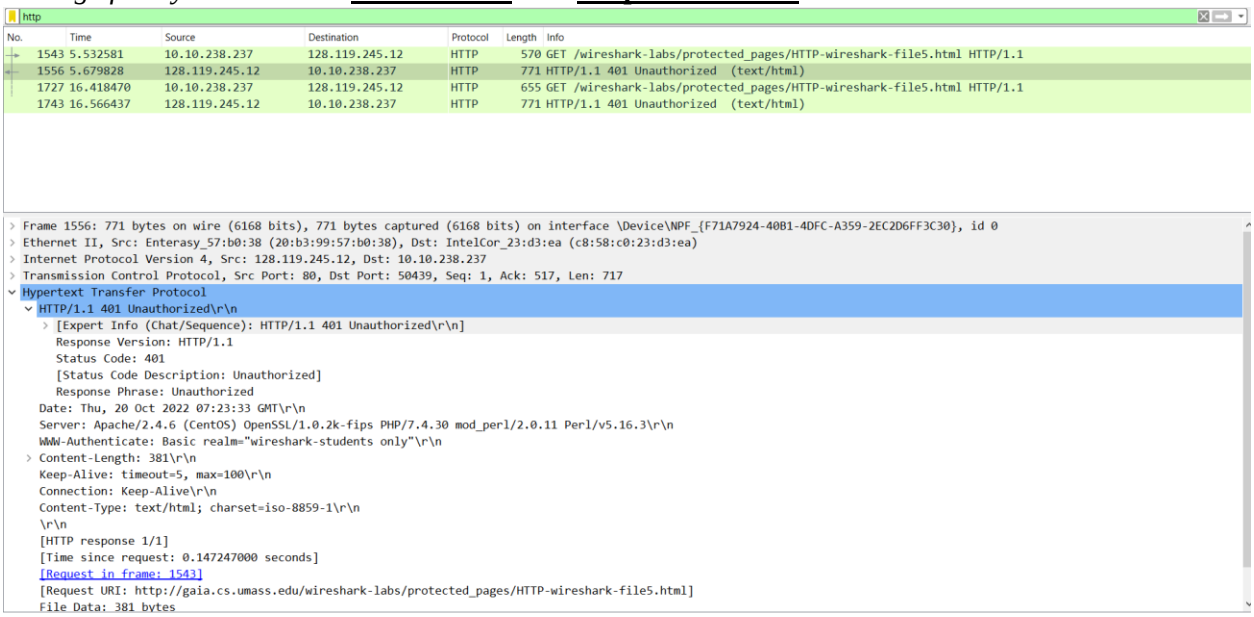


4. Now inspect the contents of the second HTTP GET request and compare it to the first get. Explain the differences. *(0.5 points)* **The differences of first get and second get is hosts, src ports, len**

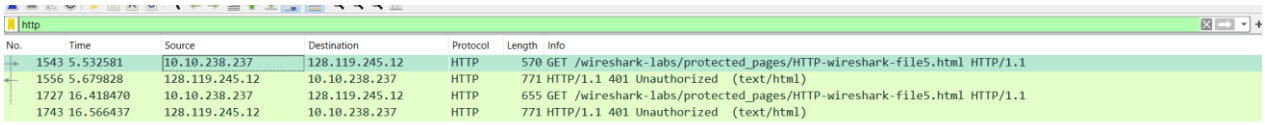


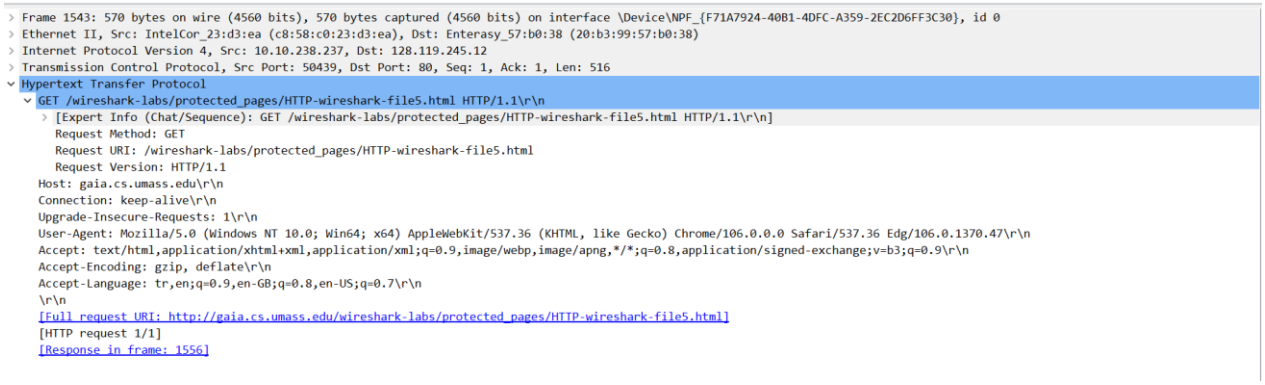
5. Now answer questions 18 and 19 from prelab. You should add related screenshots. *(1 points)*

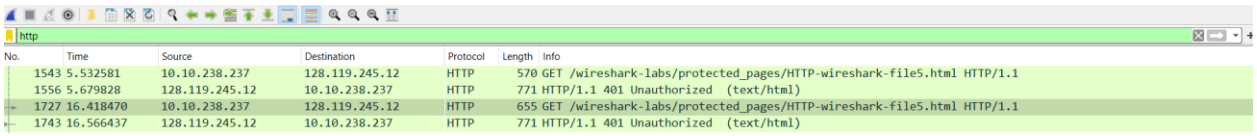
18. *What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?* **Status code: 401 Response Phrase: Unathorized**

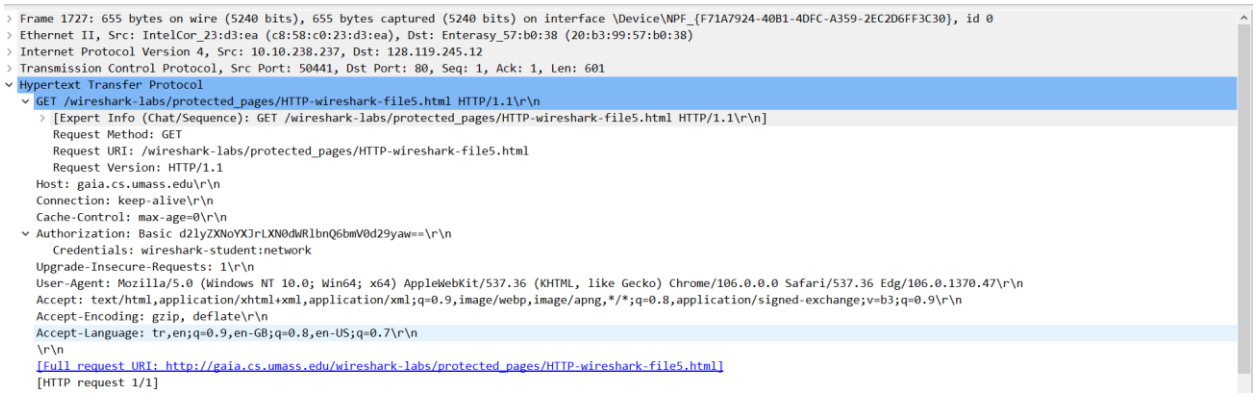


19. *When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?* **New field is now included is the authorization field. (Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnQ6bmV0d29yaw==\r\n)**






http
No. Time Source Destination Protocol Length Info
1543 5.532581 10.10.238.237 128.119.245.12 HTTP 570 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1556 5.679828 128.119.245.12 10.10.238.237 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)
1727 16.418470 10.10.238.237 128.119.245.12 HTTP 655 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1743 16.566437 128.119.245.12 10.10.238.237 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)


Frame 1727: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Device\NPF_{F71A7924-40B1-4DFC-A359-2EC2D6FF3C30}, id 0
Ethernet II, Src: IntelCor_23:d3:ea (c8:58:c0:23:d3:ea), Dst: Enterasy_57:b0:38 (20:b3:99:57:b0:38)
Internet Protocol Version 4, Src: 10.10.238.237, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50441, Dst Port: 80, Seq: 1, Ack: 1, Len: 601
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnQ6bmV0d29yaw==\r\n
Credentials: wireshark-student:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 Edg/106.0.1370.47\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]