

Computer Networking

(CSE 311)

HTTP Lab using Wireshark

Submitted By:

Shifat Jahan Shifa

Roll: 1301

BSSE 13th batch

Session: 2020-2021

Submitted To:

Dr. Md. Shariful Islam

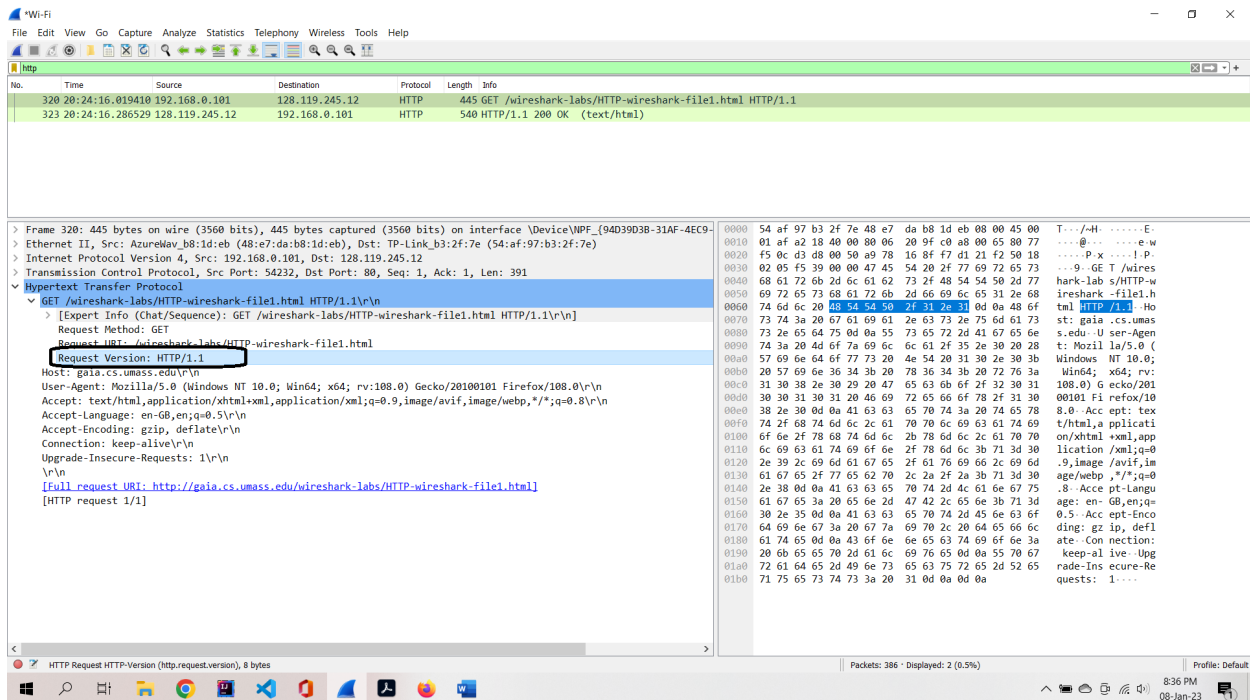
Professor

Institute of Information Technology

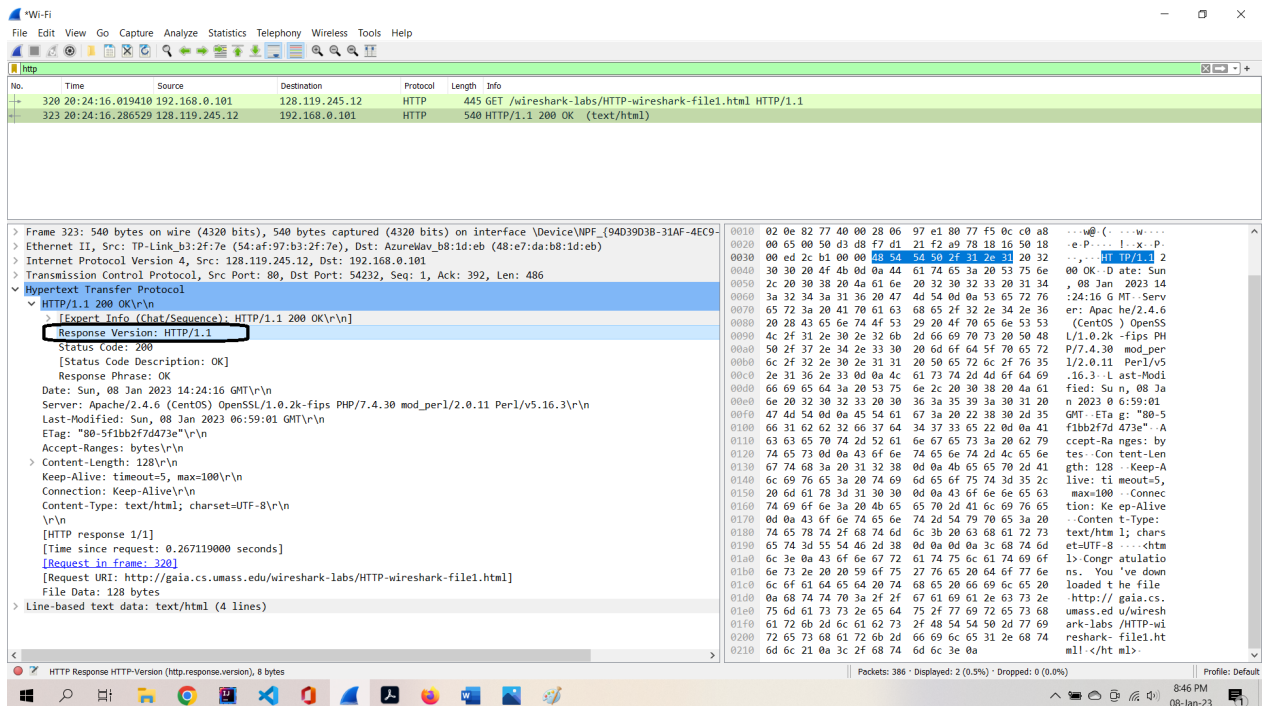
University of Dhaka

Date: 09/01/2023

Answer 1:

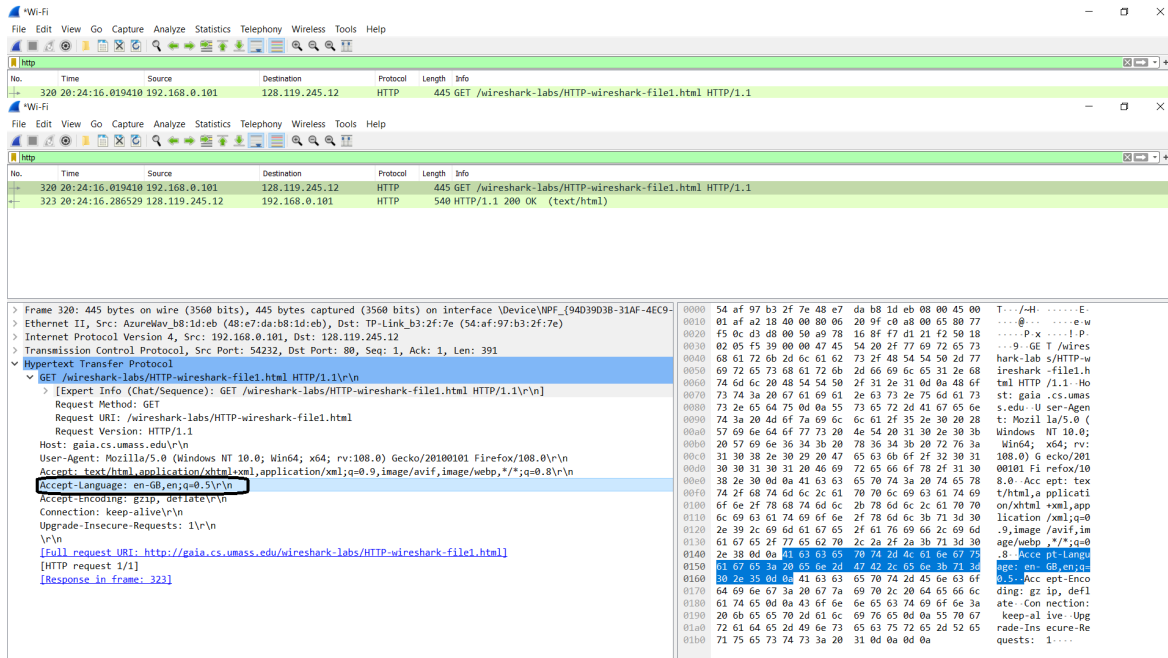


My browser runs http version: 1.1



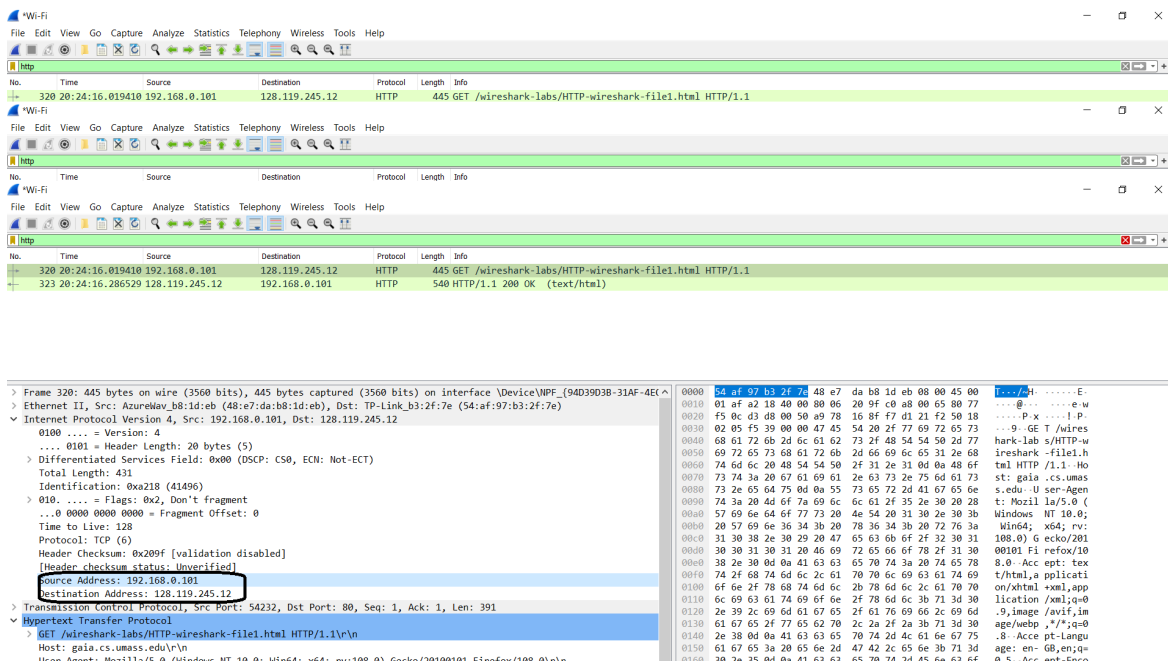
Server runs http version: 1.1

Answer 2:



Accept languages : en-GB,en;q=0.5\r\n

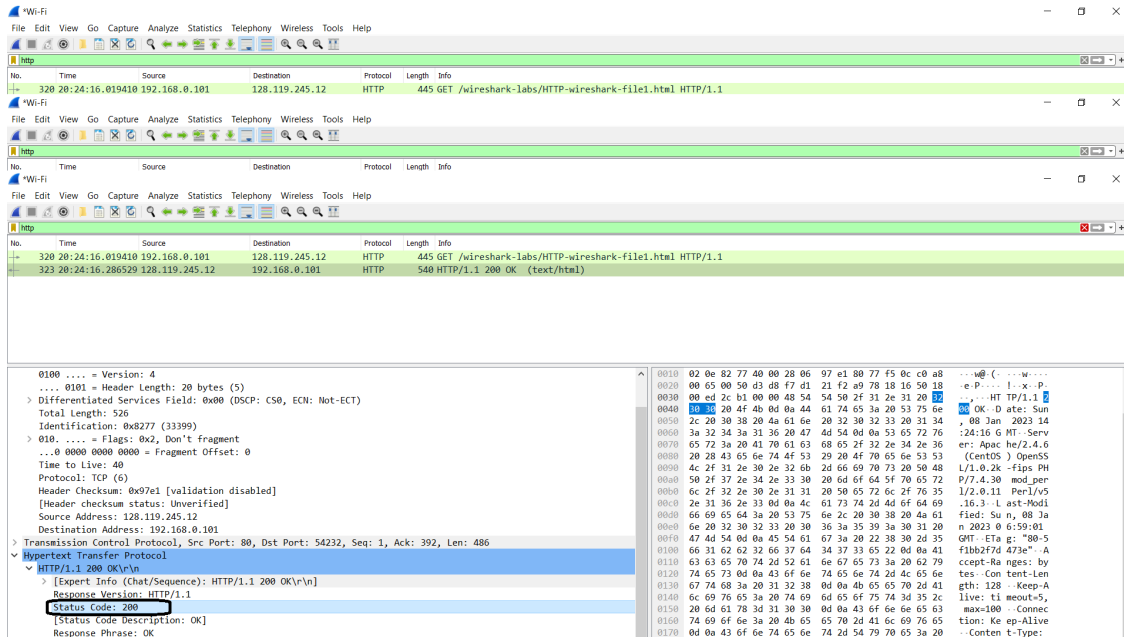
Answer 3:



IP address of my computer: 192.168.0.101

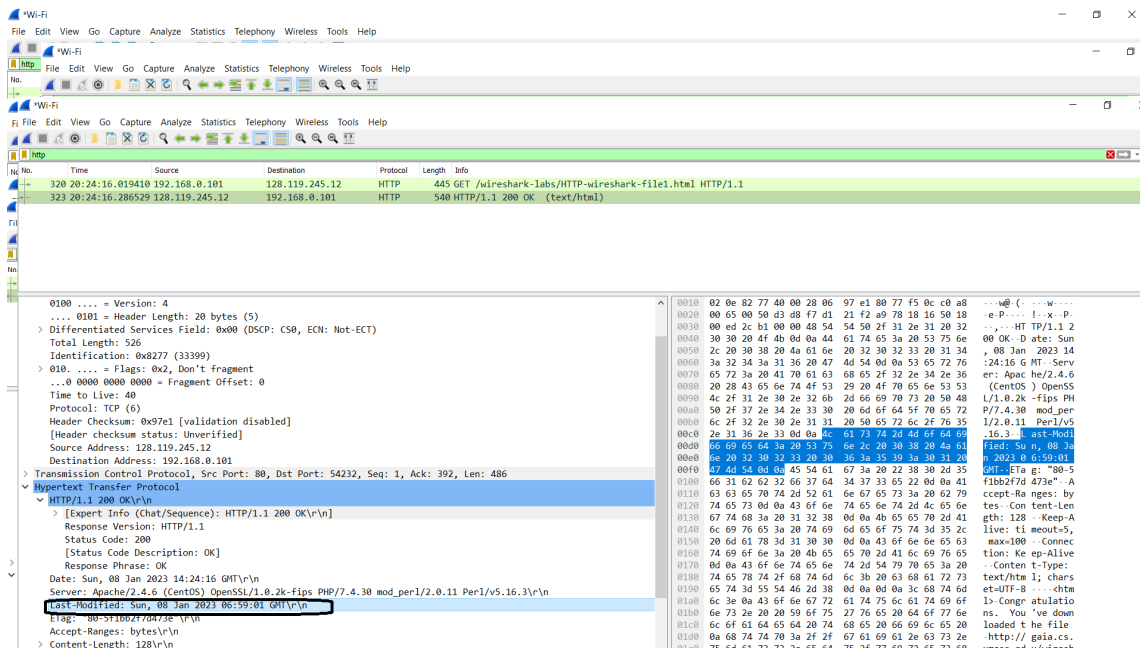
IP address of server: 128.119.245.12

Answer 4:



Status code: 200

Answer 5:



Last modified: sun, 08 jan 2023 06:59:01 GMT\r\n

Answer 6:

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows frame 323 with a content length of 128 bytes. The packet details pane on the right shows the HTTP response structure, including the status code 200 OK and the content length field. The packet bytes pane at the bottom shows the raw data of the packet.

Header Checksum: 0x9e1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.0.101
Transmission Control Protocol, Src Port: 80, Dst Port: 54232, Seq: 1, Ack: 392, Len: 486
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Sun, 08 Jan 2023 14:24:16 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Sun, 08 Jan 2023 06:59:01 GMT\r\nETag: "80-5f1bb2f7d473e"\r\nAccept-Ranges: bytes\r\nContent-Length: 128\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]
[Time since request: 0.26719000 seconds]
[Request in frame: 320]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[Content length: 128 bytes]

Content length: 128 bytes

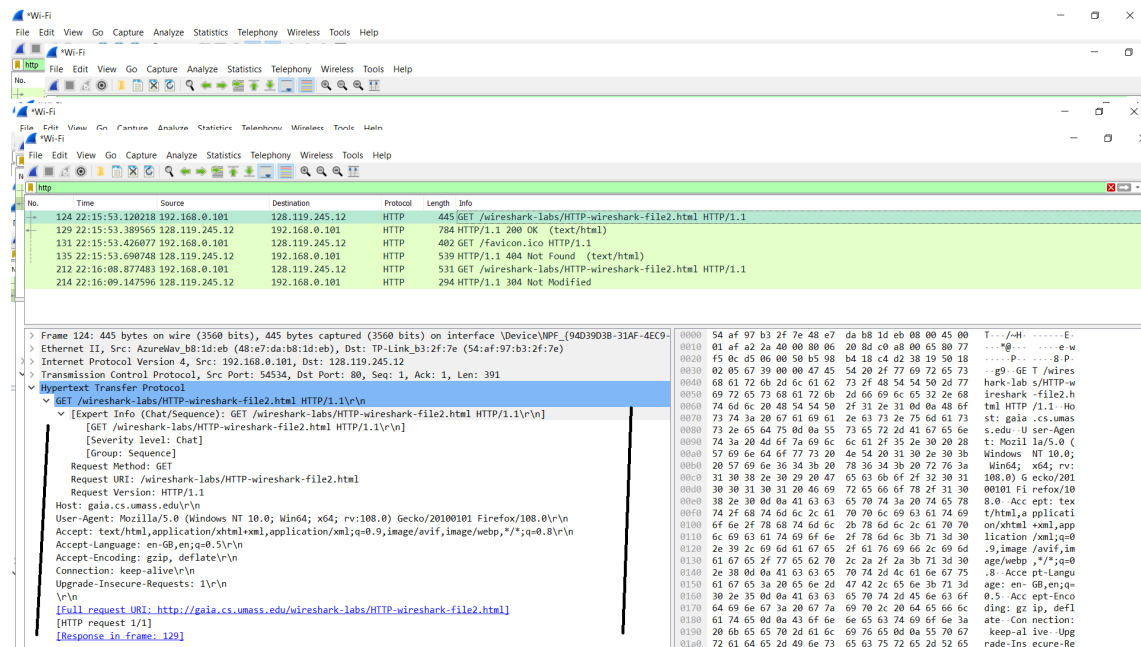
Answer 7:

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows frame 323 with a content length of 128 bytes. The packet details pane on the right shows the HTTP response structure, including the status code 200 OK and the content length field. The packet bytes pane at the bottom shows the raw data of the packet.

Header Checksum: 0x9e1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.0.101
Transmission Control Protocol, Src Port: 80, Dst Port: 54232, Seq: 1, Ack: 392, Len: 486
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Sun, 08 Jan 2023 14:24:16 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Sun, 08 Jan 2023 06:59:01 GMT\r\nETag: "80-5f1bb2f7d473e"\r\nAccept-Ranges: bytes\r\nContent-Length: 128\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]
[Time since request: 0.26719000 seconds]
[Request in frame: 320]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[Content length: 128 bytes]

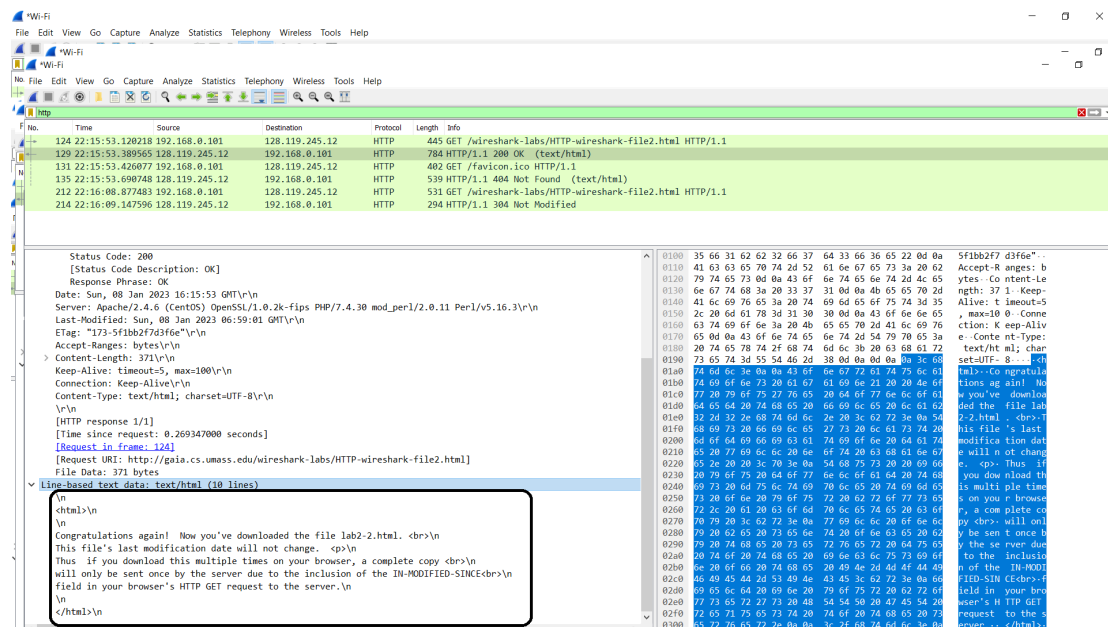
No. there is not any type header file that is in raw data but not in the packet listing window.

Answer 8:



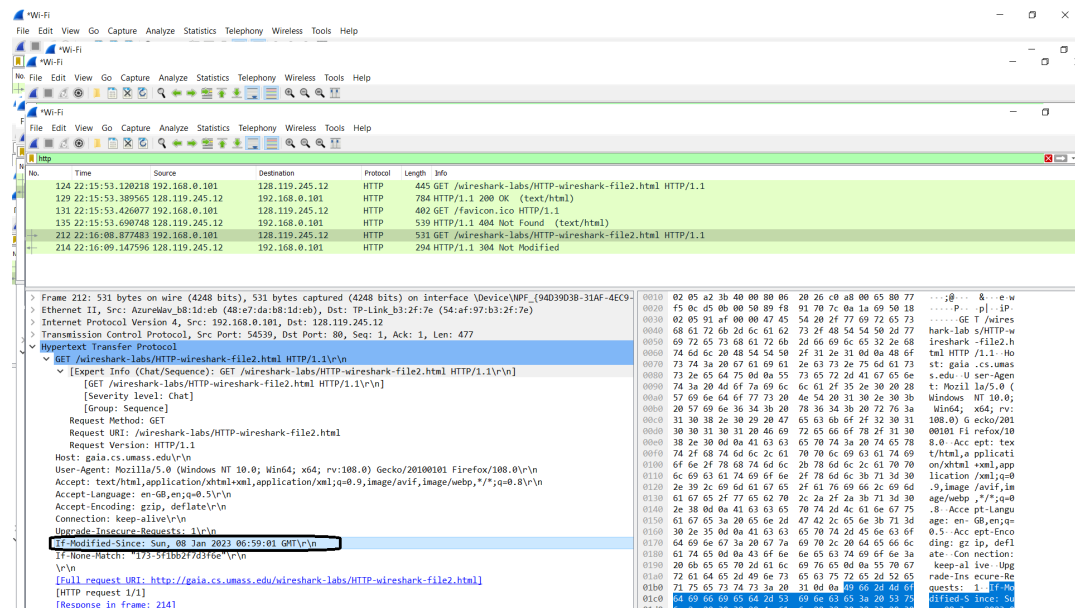
No. I don't see any "IF-MODIFIED-SINCE" line in HTTP GET.

Answer 9:



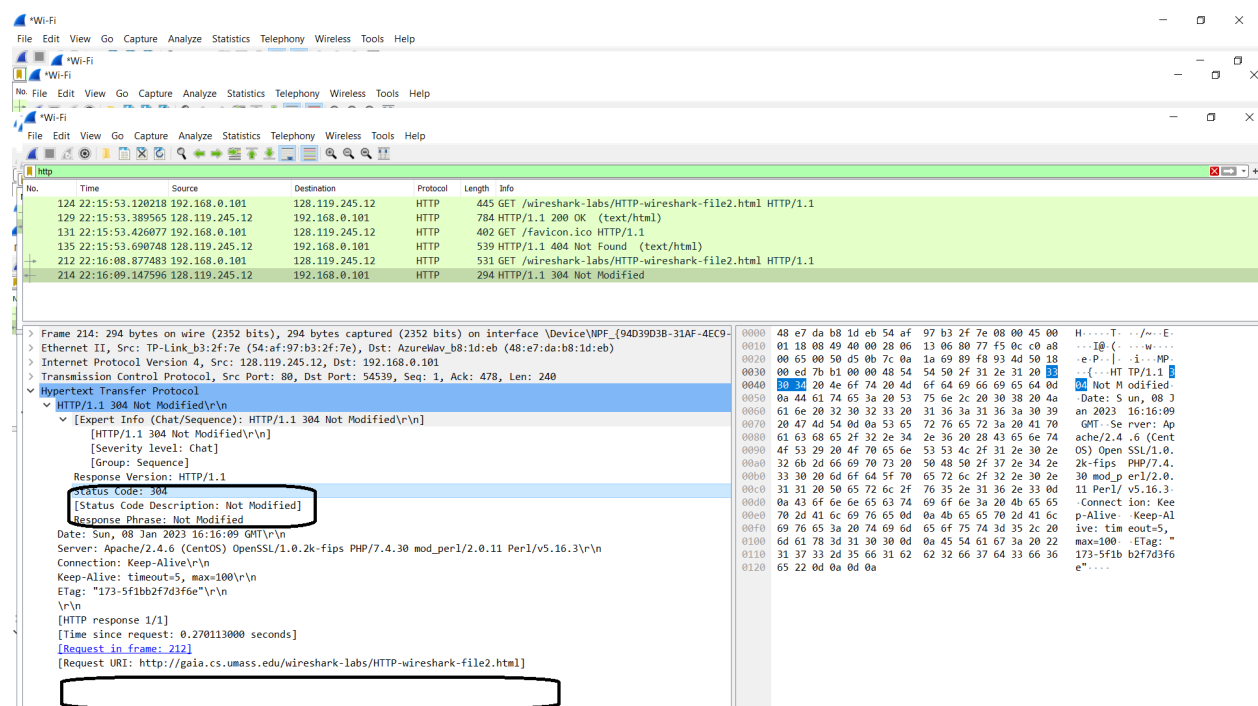
Yes. The server explicitly returns the contents of the file. (shown inside the black box in the image).

Answer 10:



Yes. I see “IF-MODIFIED-SINCE” line in HTTP GET. IF-MODIFIED-SINCE header follows the information of the time when the file was last modified. We can see the “last-modified” time in the first response message.

Answer 11:

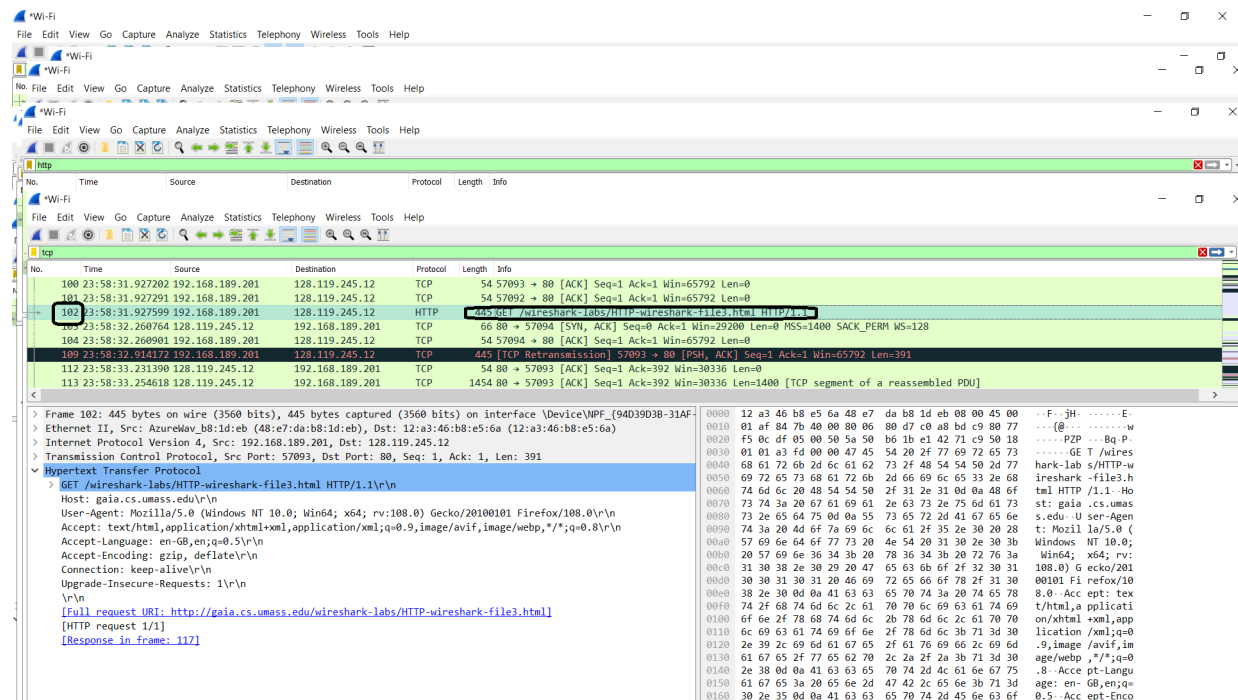


Status code: 304

Response phrase: Not Modified

We can see that this time, server explicitly didn't return the contents of the file. Since the file has not been modified.

Answer 12:



Browser sent 1 HTTP GET request message. Packet number 102 contains the GET message for BILL of RIGHTS.

Answer 13:

Wireshark packet capture showing a TCP segment of a reassembled PDU. The packet details pane shows the following information:

- Transmission Control Protocol, Src Port: 80, Dst Port: 57093, Seq: 1, Ack: 392, Len: 1400
- Source Port: 80
- Destination Port: 57093
- [Stream index: 3]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 1400]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 3779228105
- [Next Sequence Number: 1401 (relative sequence number)]
- Acknowledgment Number: 392 (relative ack number)
- Acknowledgment Number (raw): 1515239330
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x010 (ACK)
- Window: 237
- [Calculated window size: 30336]
- [Window size scaling factor: 128]
- Checksum: 0x3562 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [Time since first frame in this TCP stream: 1.851000000 seconds]
- [Time since previous frame in this TCP stream: 0.023228000 seconds]
- [SEQ/ACK analysis]
- [RRTT: 0.523580000 seconds]
- [Bytes in flight: 1400]
- [Bytes sent since last PSH flag: 1400]

The packet bytes pane shows the raw data of the TCP segment, including the sequence number 1401 and the acknowledgment number 392.

Packet number 113.

Answer 14:

Wireshark packet capture showing a HTTP 200 OK response. The packet details pane shows the following information:

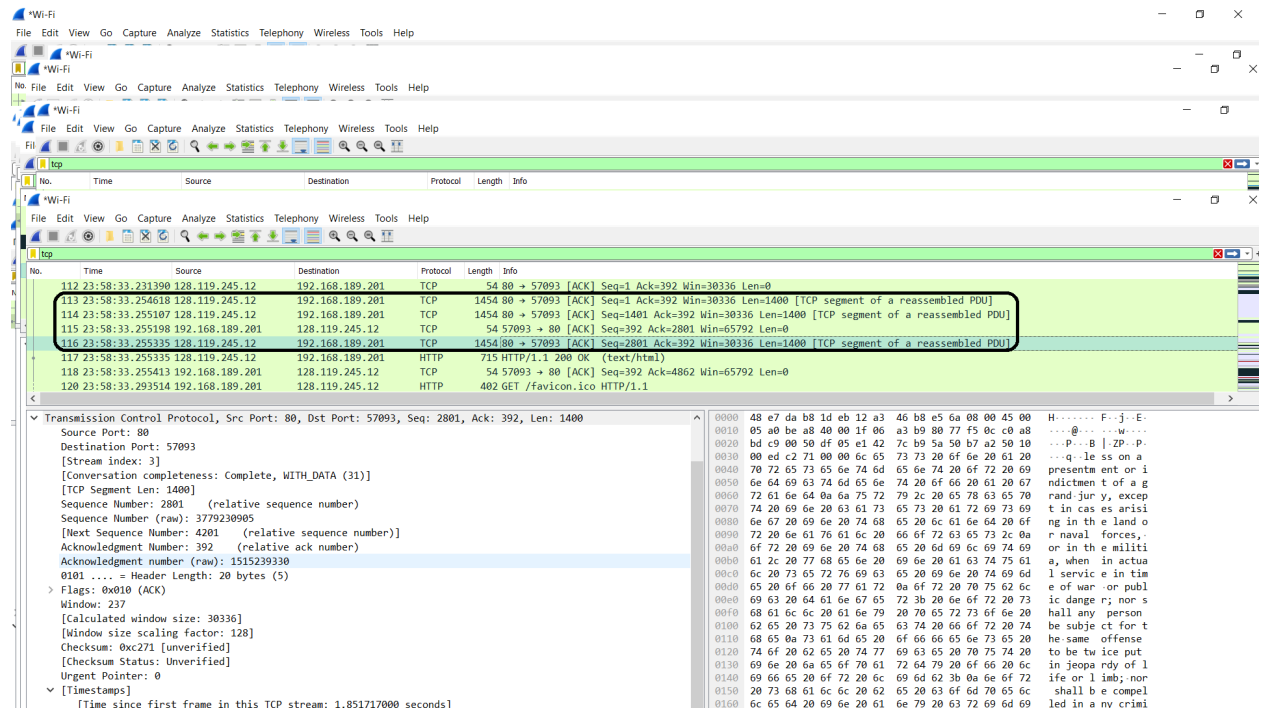
- [Bytes in flight: 2061]
- [Bytes sent since last PSH flag: 4861]
- TCP payload (661 bytes)
- TCP segment data (661 bytes)
- [4 Reassembled TCP Segments (4861 bytes): #113(1400), #114(1400), #116(1400), #117(661)]
- [Frame: 113, payload: 0-1305 (1400 bytes)]
- [Frame: 114, payload: 1306-2799 (1400 bytes)]
- [Frame: 116, payload: 2800-4199 (1400 bytes)]
- [Frame: 117, payload: 4200-4860 (661 bytes)]
- [Segment count: 4]
- [Reassembled TCP length: 4861]
- [Reassembled TCP Data: 485454502f312e3128323030204f4b0d0a46174653a2053756e2c203038204a616e2032..]
- HyperText Transfer Protocol
- > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
- Response: 200 OK
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Sun, 08 Jan 2023 17:58:32 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
- Last-Modified: Sun, 08 Jan 2023 06:59:01 GMT\r\n
- Etag: "1194-5f1bb27fc9d" \r\n
- Accept-Ranges: bytes\r\n
- [Content-Length: 4500]
- Keep-Alive: timeout=5, max=100\r\n

The packet bytes pane shows the raw data of the HTTP response, including the status code 200 and the response phrase 'OK'.

Status code: 200

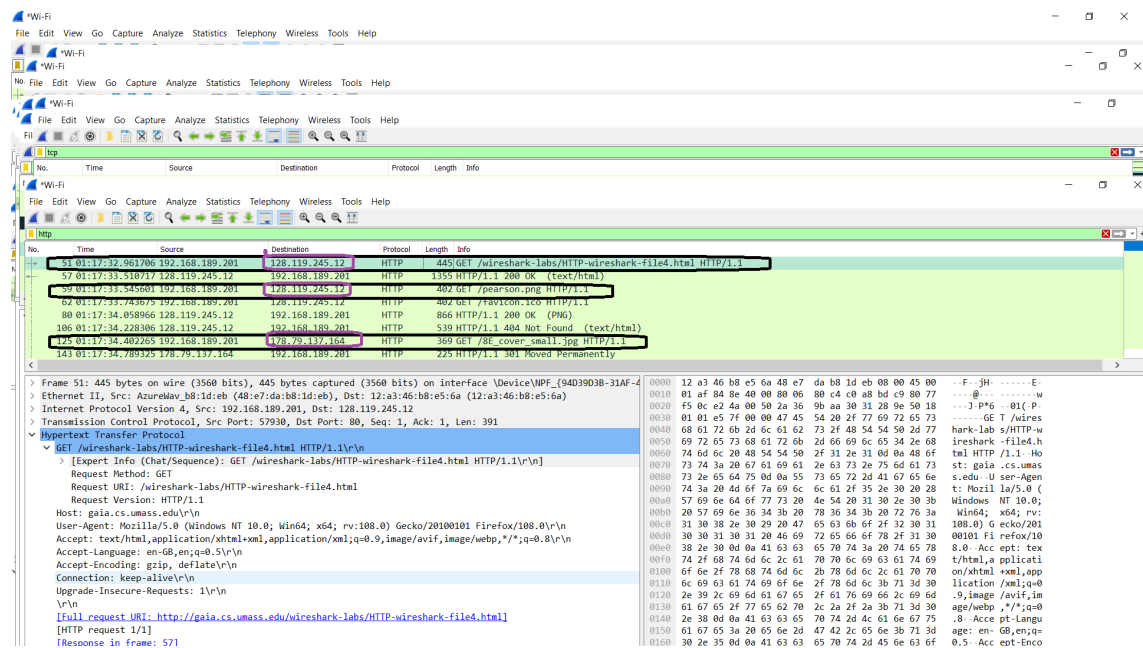
phrase: Ok

answer 15:



Three segments. (113,114,116 in the trace).

Answer 16:



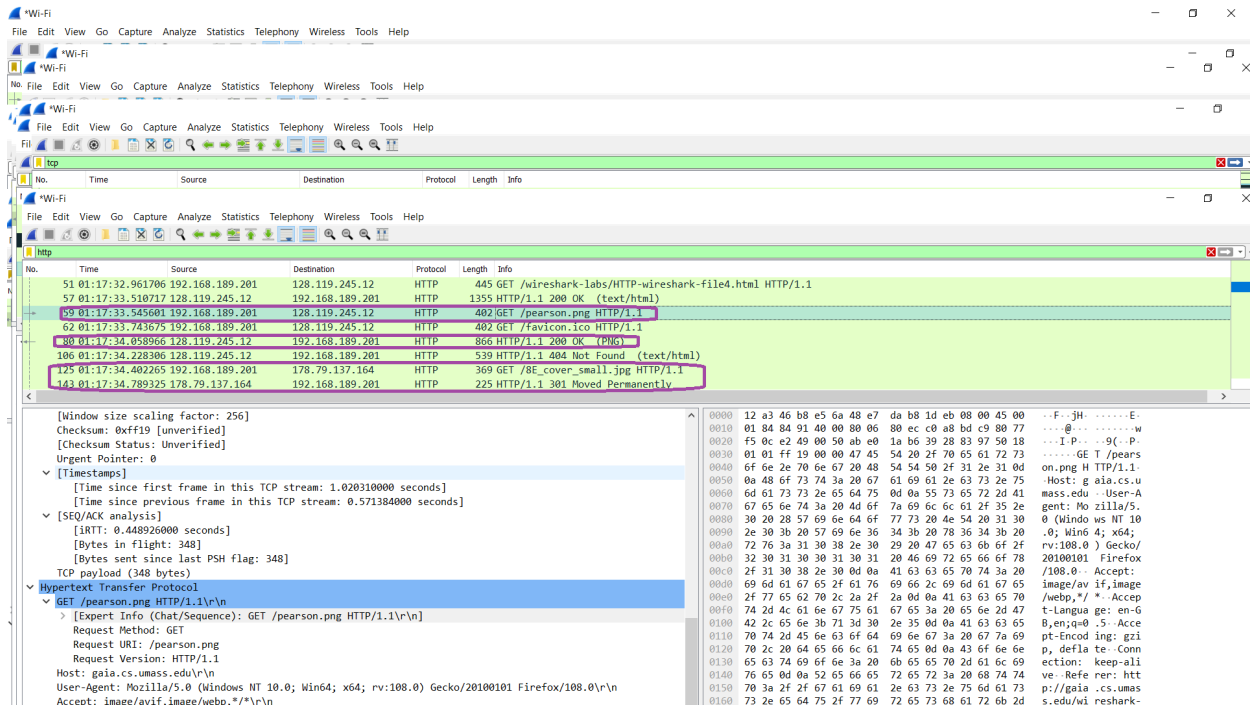
Three HTTP GET request messages were sent. These were sent to IP addresses →

a) 128.119.245.12

b) 128.119.245.12

c) 178.79.137.164

Answer 17:



The two images were downloaded from two websites serially. Because GET message for first image was in 59th packet and GET message for the second image was in 80th packet. As the response message for the first GET message for the first image was in 62nd packet which is before 80th packet. So, they were download from two websites serially.

Answer 18:

The image shows a Wireshark capture of an HTTP 401 Unauthorized response. The packet list shows a GET request for /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html. The packet details pane shows the response status code 401 and the phrase 'Unauthorized'. The packet bytes pane shows the raw data of the response, including the status line: HTTP/1.1 401 Unauthorized.

Packet 124: HTTP 401 Unauthorized

Response Code: 401
Response Phrase: Unauthorized

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3

WWW-Authenticate: Basic realm="wireshark-students only"

Content-Length: 381

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Status code: 401 and Phrase: Unauthorized

Answer 19:

The image shows a Wireshark capture of an HTTP GET request. The packet list shows a GET request for /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html. The packet details pane shows the request method GET, the request URI, and the Authorization header. The packet bytes pane shows the raw data of the request, including the Authorization header: Authorization: Basic d2lyZXNoVXNlLXN0dWlbnRzOm5ldHdvcm0=.

Packet 187: GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1

Request Method: GET

Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Upgrade-Insecure-Requests: 1

Authorization: Basic d2lyZXNoVXNlLXN0dWlbnRzOm5ldHdvcm0=

Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html

Response in frame: 192

Next request in frame: 199

(Authorization: Basic) field is newly included in HTTP GET message. Under this field, there is credentials information (username and password).