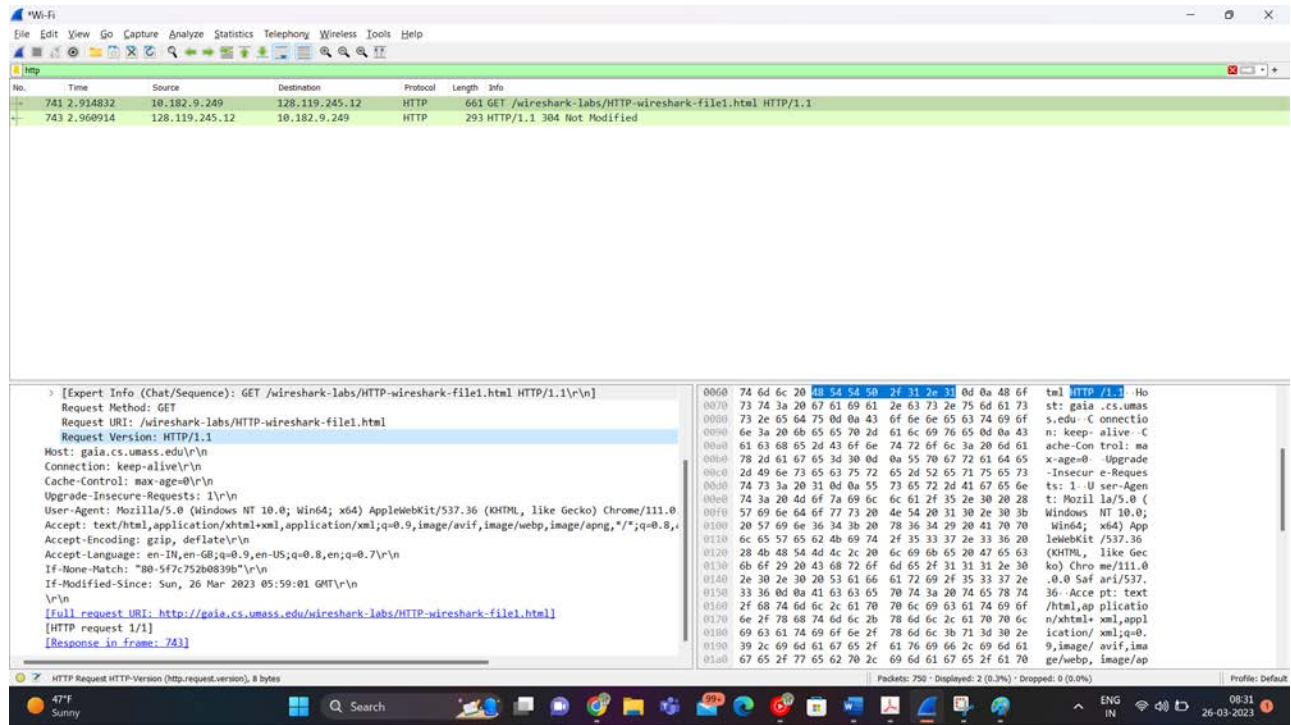


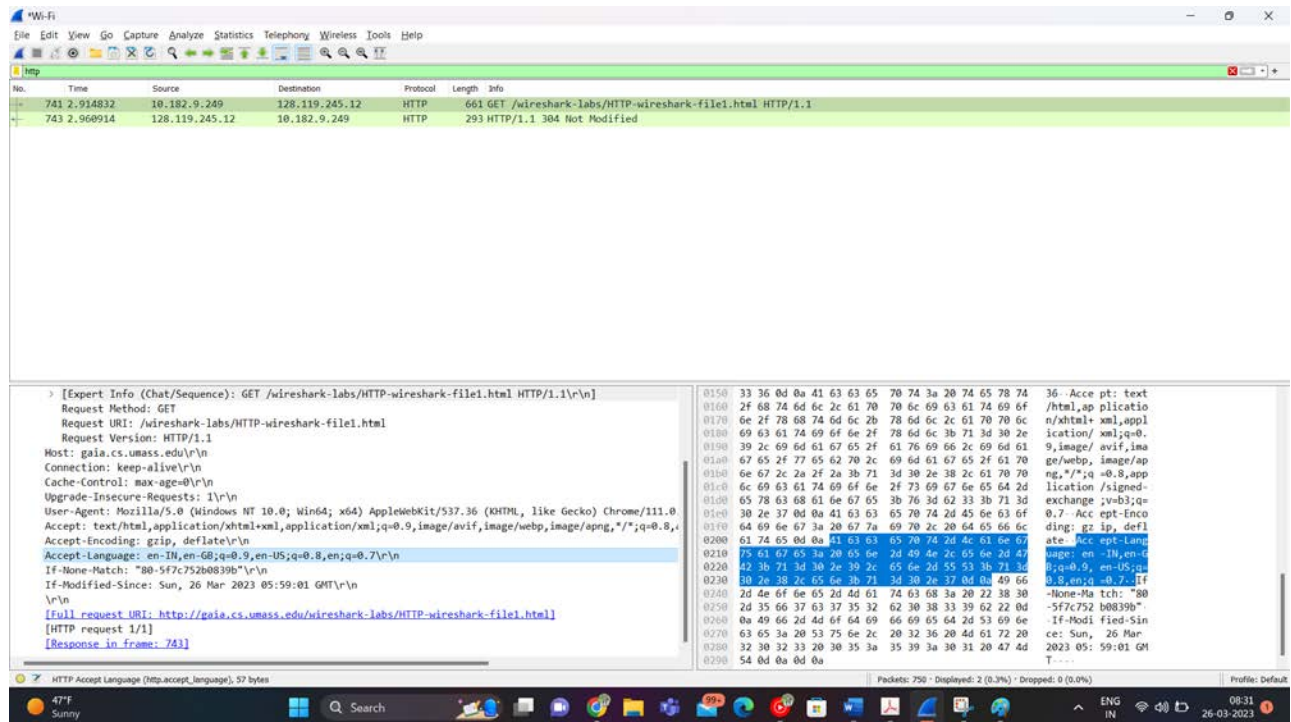
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Ans: Yes My browser and server both is running **HTTP with version of 1.1**



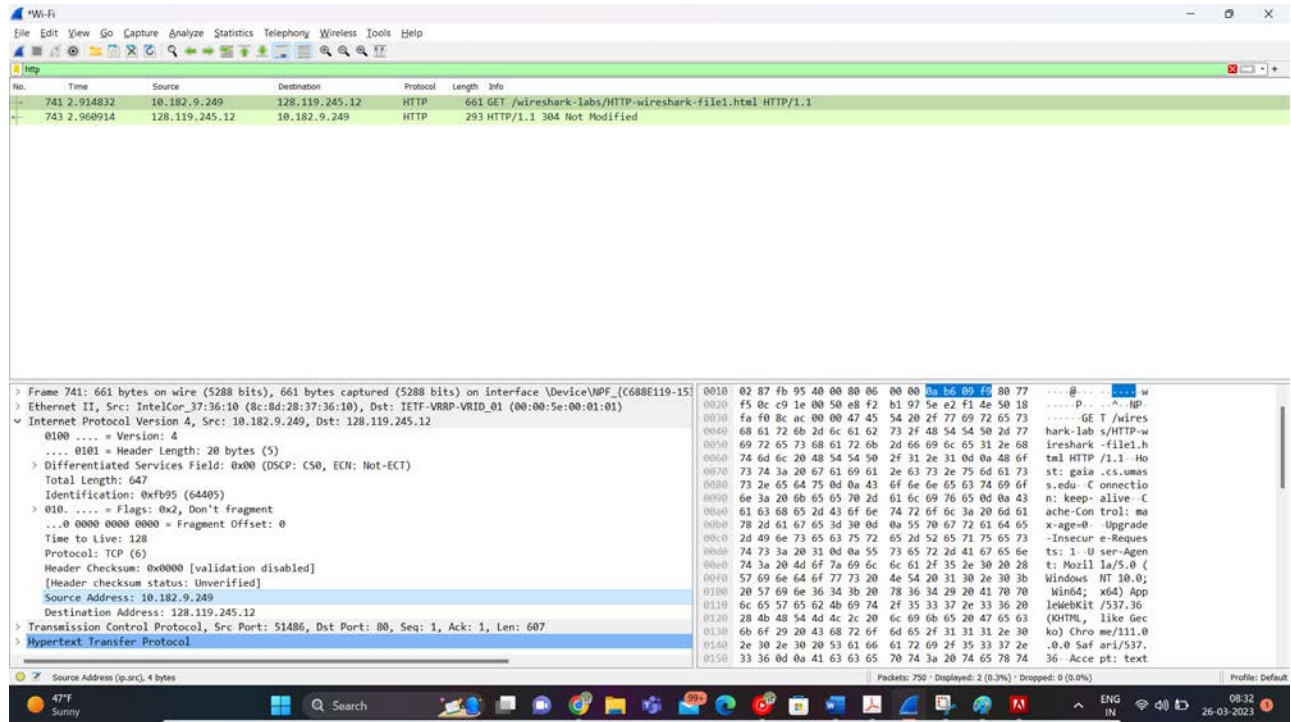
2. What languages (if any) does your browser indicate that it can accept to the server?

Ans: As highlighted in the Image the browser can accept **“en-IN,en-GB” to the server.**



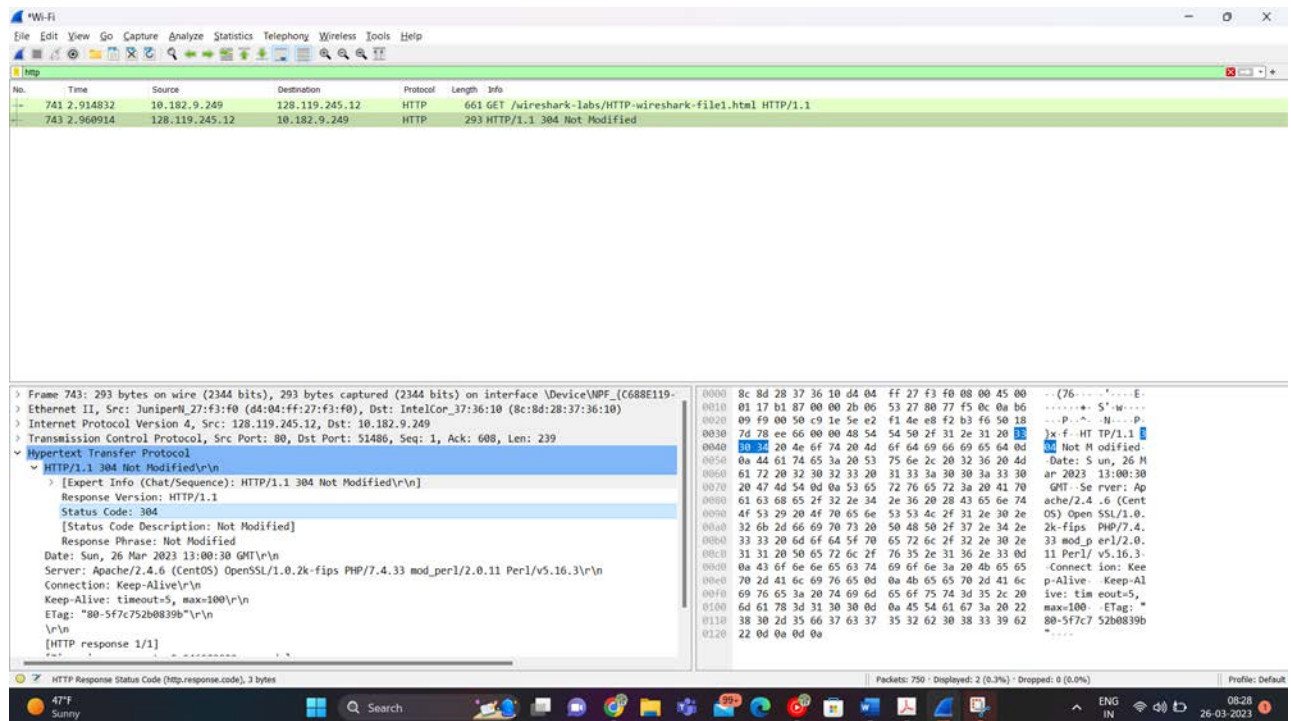
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Ans: The IP address of my **computer** is **10.182.9.249** and IP address of the **gaia.cs.umass.edu** server is **128.119.245.12**



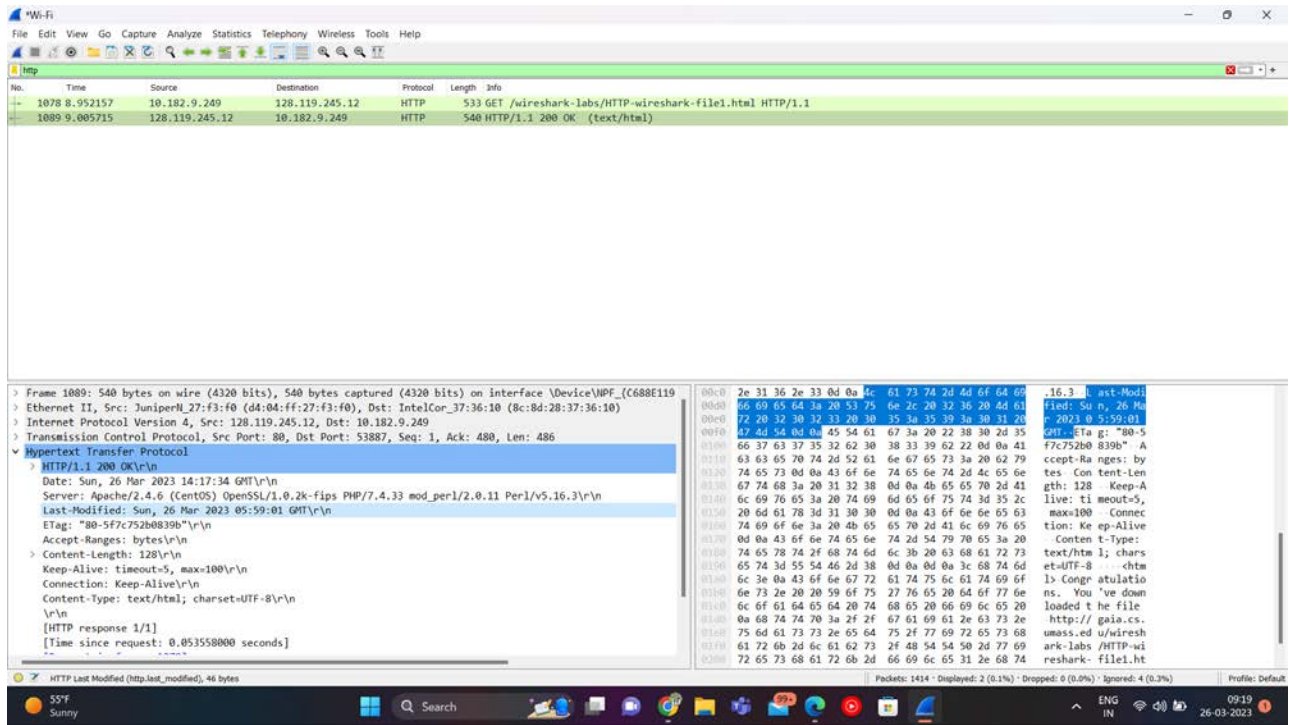
4. What is the status code returned from the server to your browser?

Ans: Status code which is returned from the server to the browser is **304**.



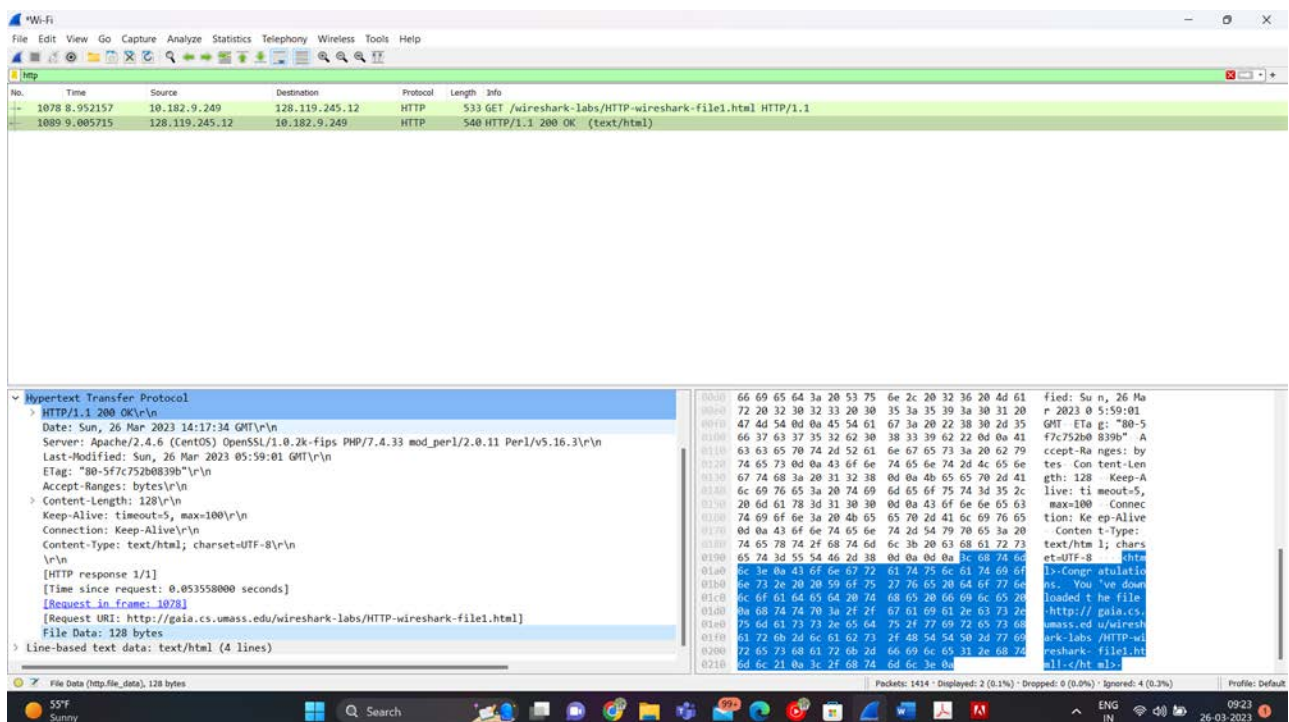
5. When was the HTML file that you are retrieving last modified at the server?

Ans: Sun, 26 Mar 2023 05:59:01 GMT\r\n as last modified at the server



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

Ans: 128 bytes of content





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: **No**, I do not see any headers within the data in the packet-listing window. As all of the data can be found in raw data.

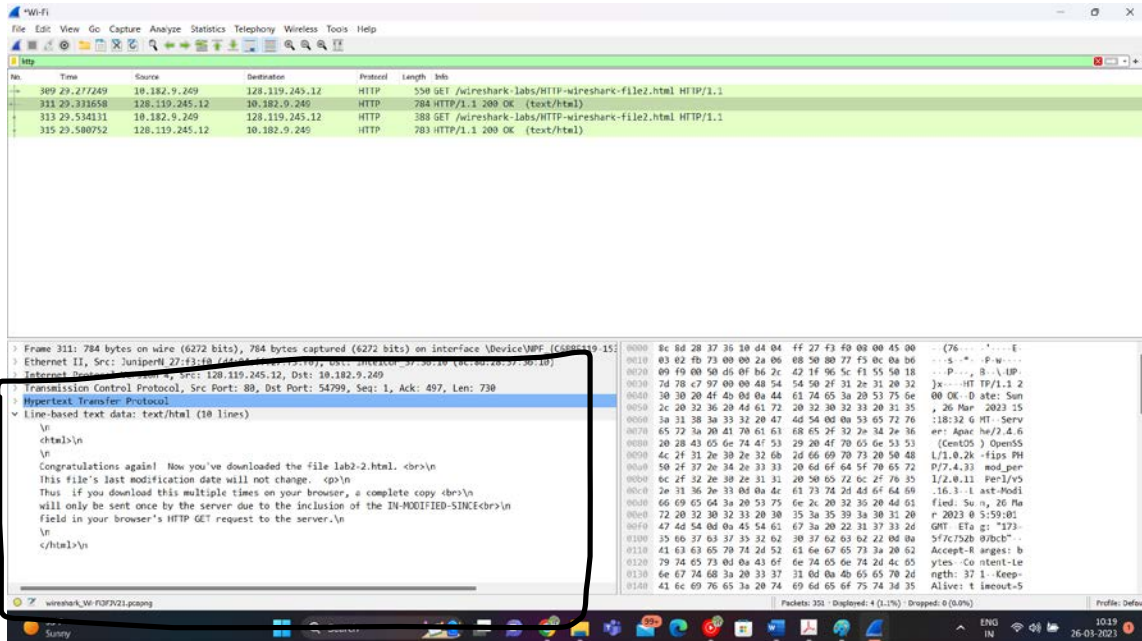
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

Ans: **No**, I can see there is "IF-MODIFIED-SINCE" line in the HTTP GET.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets: a GET request (No. 449), a 200 OK response (No. 452), and two subsequent GET requests (Nos. 1930 and 1932). The packet details pane for packet 449 shows the HTTP GET request with the following fields: [Severity level: Chat], [Group: Sequence], Response Version: HTTP/1.1, Status Code: 200, [Status Code Description: OK], Response Phrase: OK, Date: Sun, 26 Mar 2023 14:45:11 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: Sun, 26 Mar 2023 05:59:01 GMT\r\n, ETag: "80-5f7c752b0839b"\r\n, Accept-Ranges: bytes\r\n, Content-Length: 128\r\n, [Content length: 128], 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 1/1]. The packet bytes pane shows the raw data of the response, which includes the status line: 200 OK (text/html).

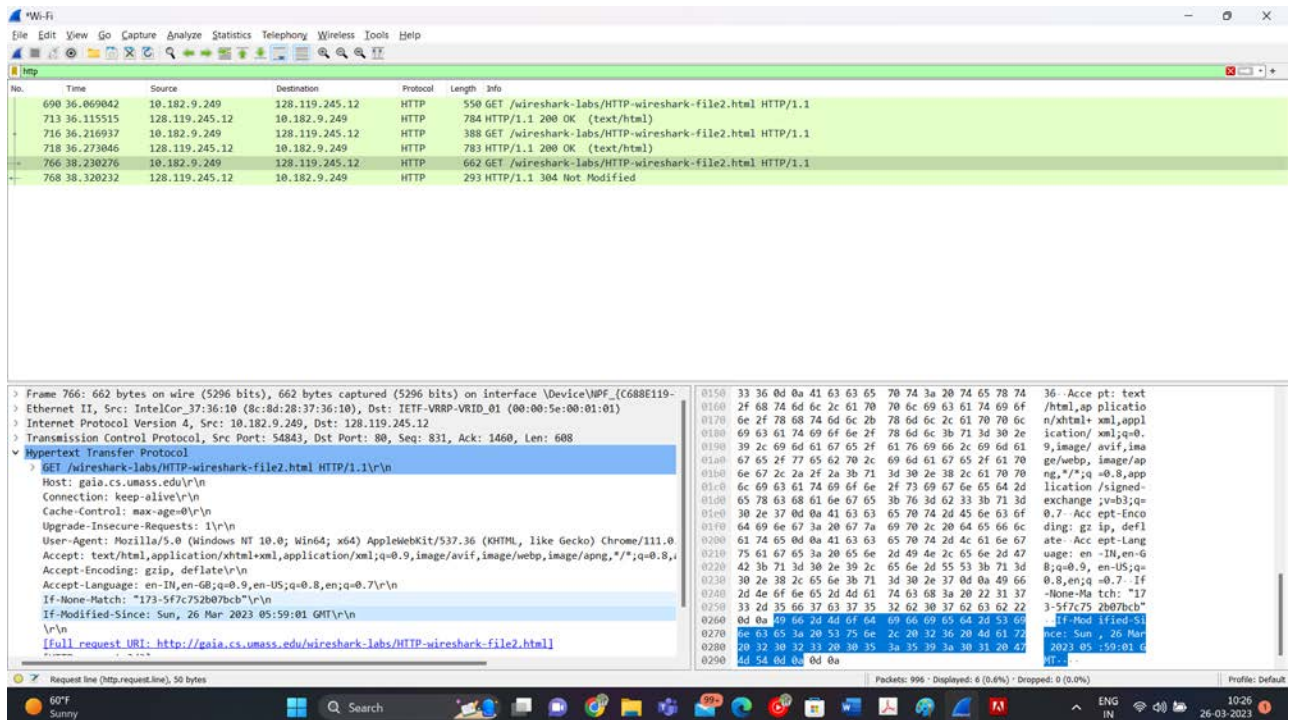
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Ans: Yes as you can see the **Line-based text data** with 10 lines



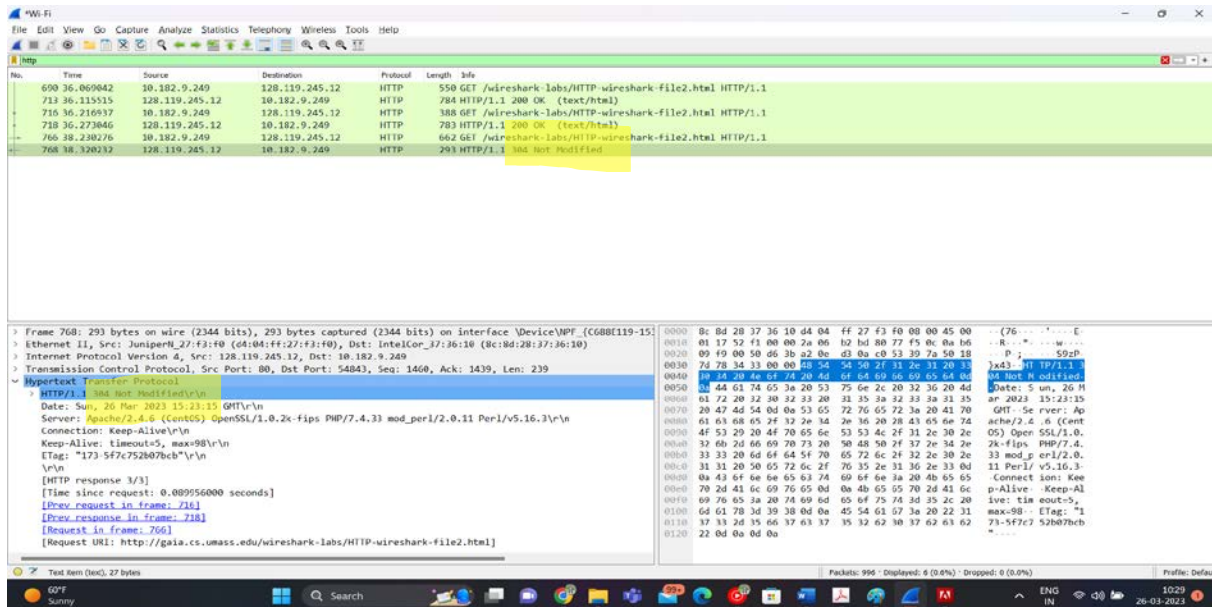
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans: **Yes**, second HTTP GET request from the browser to the server we can see that “IF-MODIFIED-SINCE:” line in the HTTP GET” as you can see in the image below.



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

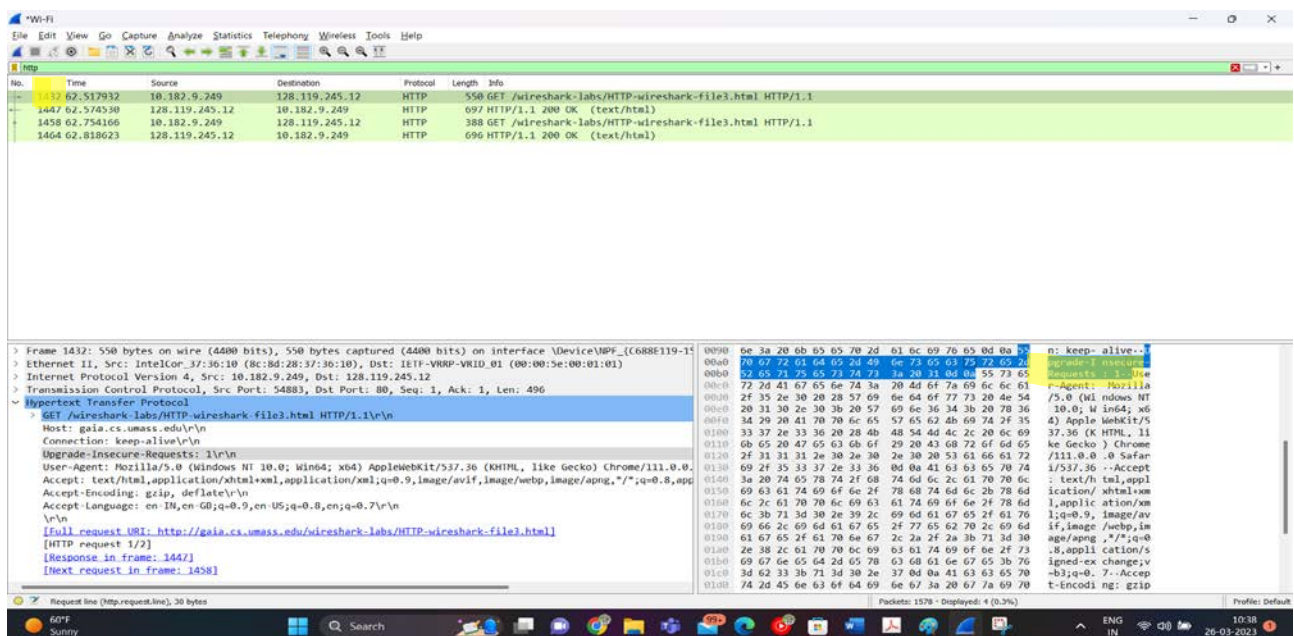
Ans: The phrase returned for the second one is **“HTTP1.1/ 304 Not Modified”**. As the server did not return the contents of the file but the browser returned the contents from the cache memory.



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: There is **One** HTTP GET request message which was sent by my browser.

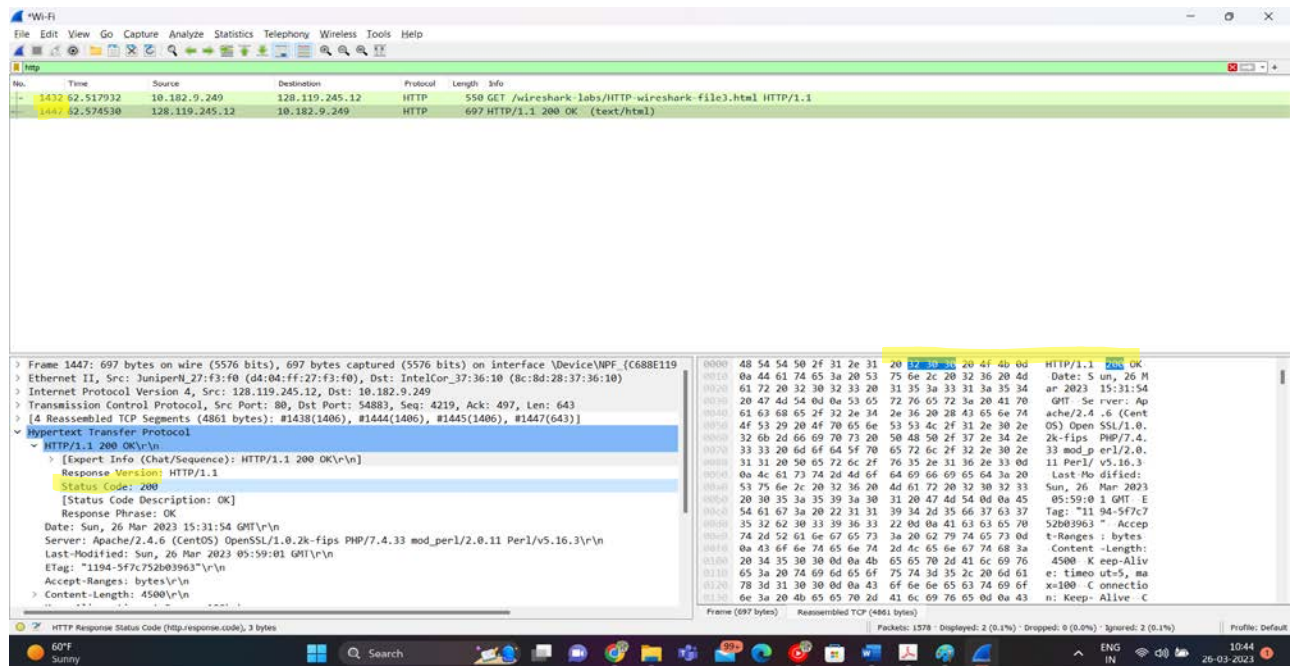
Packet Number 1432 has the trace content of the GET message from the browser





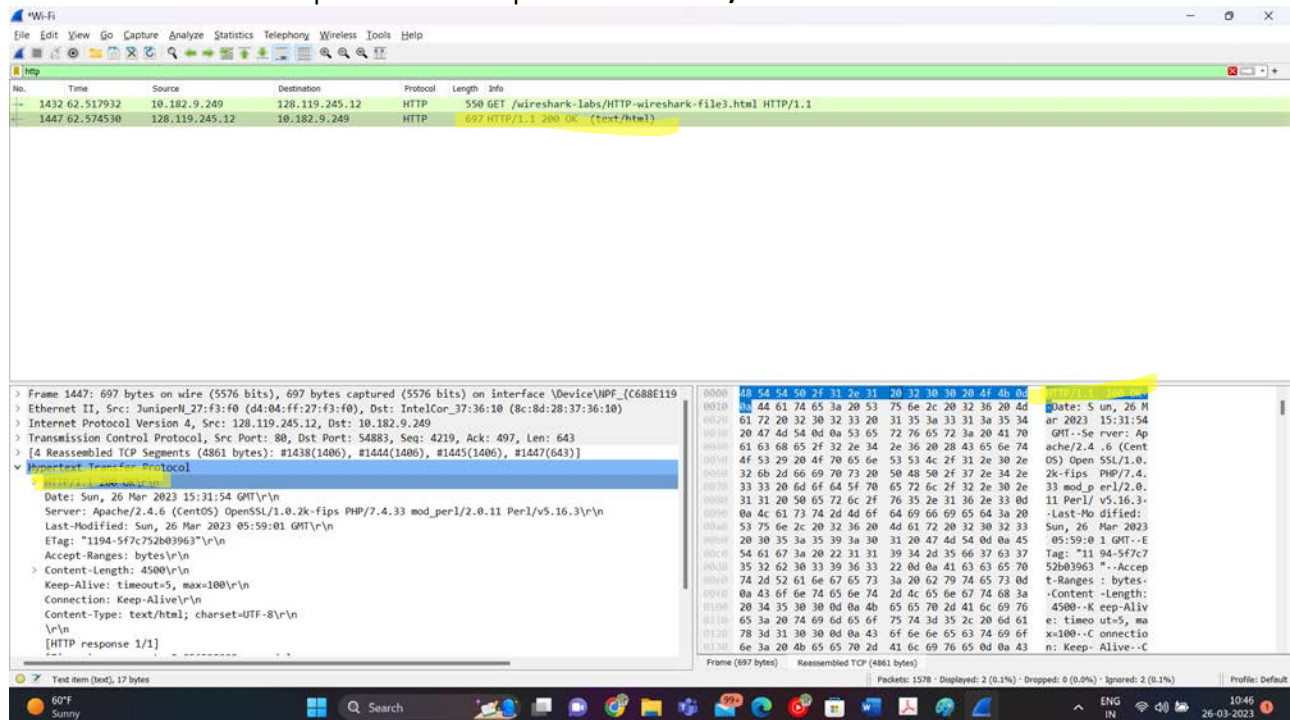
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Ans: The **1447 packet number** in the trace contains the status code and phrase associated with the response to the HTTP GET request



14. What is the status code and phrase in the response?

Ans: The status code and phrase in the response is "HTTP1.1/ 200 OK"



15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Ans: The Data was sent in **4 Reassembled Segments** as you can see the segment count as 4

The image shows a Wireshark packet capture of an HTTP response. The packet list at the top shows two packets: a GET request (No. 1432) and a 200 OK response (No. 1447). The response packet is selected, and the packet details pane shows the following structure:

- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0xf7c7 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- > [Timestamps]
- > [SEQ/ACK analysis]
- TCP payload (643 bytes)
- TCP segment data (643 bytes)
- 4 Reassembled TCP Segments (4861 bytes): #1438(1406), #1444(1406), #1445(1406), #1447(643)
- [From: 1438, payload: 0-1405 (1406 bytes)]
- [From: 1444, payload: 1406-2811 (1406 bytes)]
- [From: 1445, payload: 2812-4217 (1406 bytes)]
- [From: 1447, payload: 4218-4860 (643 bytes)]
- [Segment count: 4]
- [Reassembled TCP length: 4861]
- [Reassembled TCP Data: 485454502f312e312032303020464b0d0a4461746553a2053756e2c203236204d61722032\_...]
- > Hypertext Transfer Protocol
- > Line-based text data: text/html (98 lines)

The packet bytes pane on the right shows the raw data of the selected packet, starting with the HTTP status line: HTTP/1.1 200 OK.



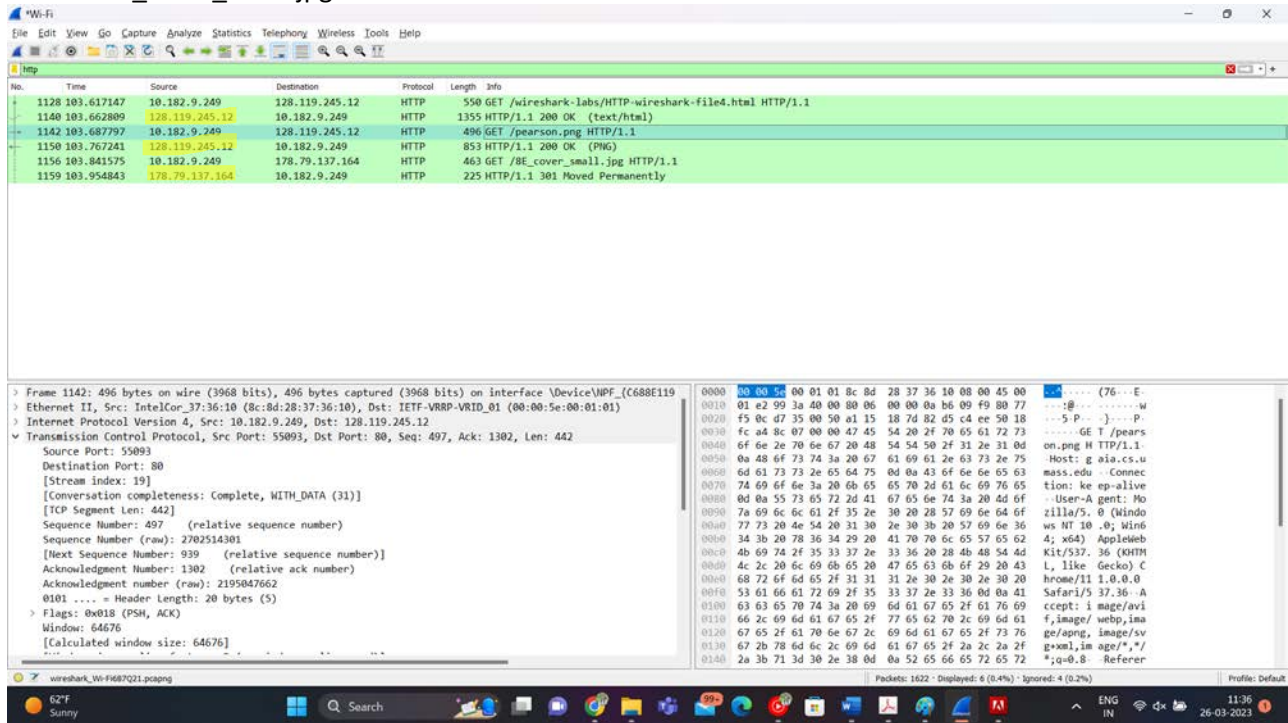
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Ans : The browser has sent **3 HTTP GET request** messages. They are **the home page, pearson.png** and

**8E\_cover\_small.jpg**

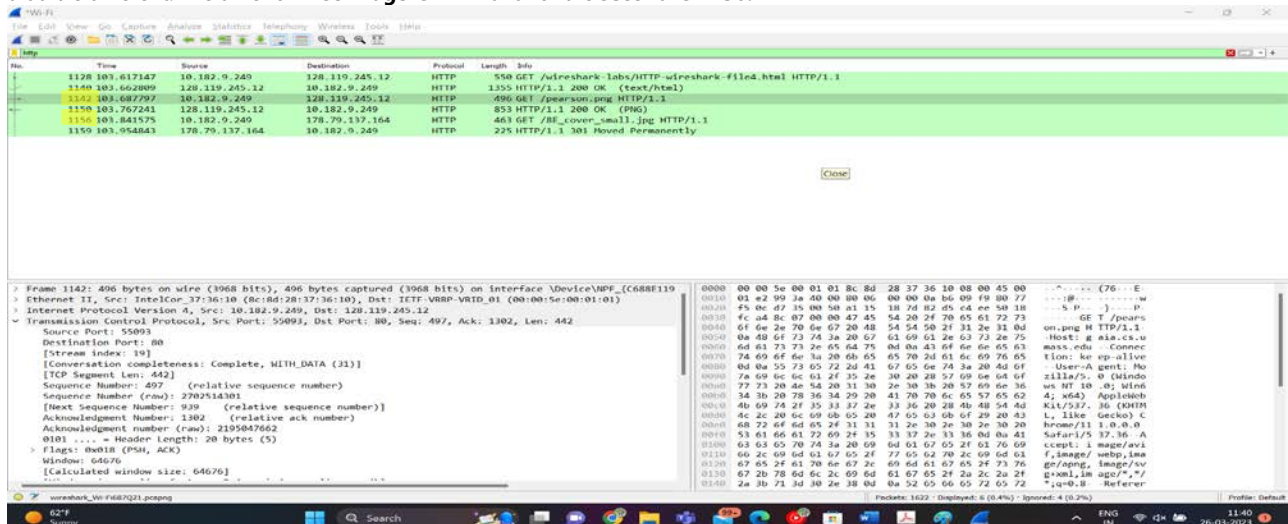
The IP address for those are:

- Home page is **128.119.245.12**
- Pearson.png is **128.119.245.12**
- 8E\_cover\_small.jpg is **178.79.137.164**

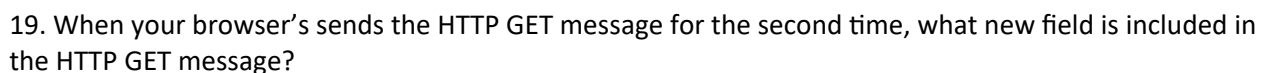


17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Ans: My browser downloaded the image files **serially** as two images separately. As **the time period** noted in the image you can observe that it is different. The time for **first image is 1142** and for the **second is 1156**.



Ans: The Server Response is **HTTP/1.1 401 Unauthorized** and the Status code is **401**.



**Wireshark**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
304	4.015504	10.182.9.249	128.119.245.12	HTTP	556	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
320	4.064555	128.119.245.12	10.182.9.249	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
351	11.130249	10.182.9.249	128.119.245.12	HTTP	620	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
353	11.176444	128.119.245.12	10.182.9.249	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

```

Frame 351: 629 bytes on wire (5032 bits), 629 bytes captured (5032 bits) on interface \Device\NPF_{C68BE119-...}
Ethernet II, Src: IntelCor_73:36:10 (8c:8d:28:37:36:10), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.182.9.249, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55417, Dst Port: 80, Seq: 1, Ack: 1, Len: 575
Hypertext Transfer Protocol
> GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoYXZlcmVkaWVvcms=\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,i
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en-Q=0.7\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-]
[HTTP request 1/]
    
```

HTTP Authorization header (http.authorization): 47 bytes

Packets: 923 · Displayed: 4 (0.4%) · Ignored: 10 (1.1%) Profile: Default