Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 2a

1. The Basic HTTP GET/response interaction

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

ANSWER:

HTTP version 1.1 for both

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

ANSWER:

Accept-Language: en-US,en;q=0.9\r\n

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

ANSWER:

IP address of my computer: 192.168.1.12
IP address of gaia.cs.umass.edu server: 128.119.245.12

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

ANSWER:

200

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

ANSWER:

Last-Modified: Mon, 11 Oct 2021 05:59:02 GMT

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

ANSWER:

Content-Length: 128

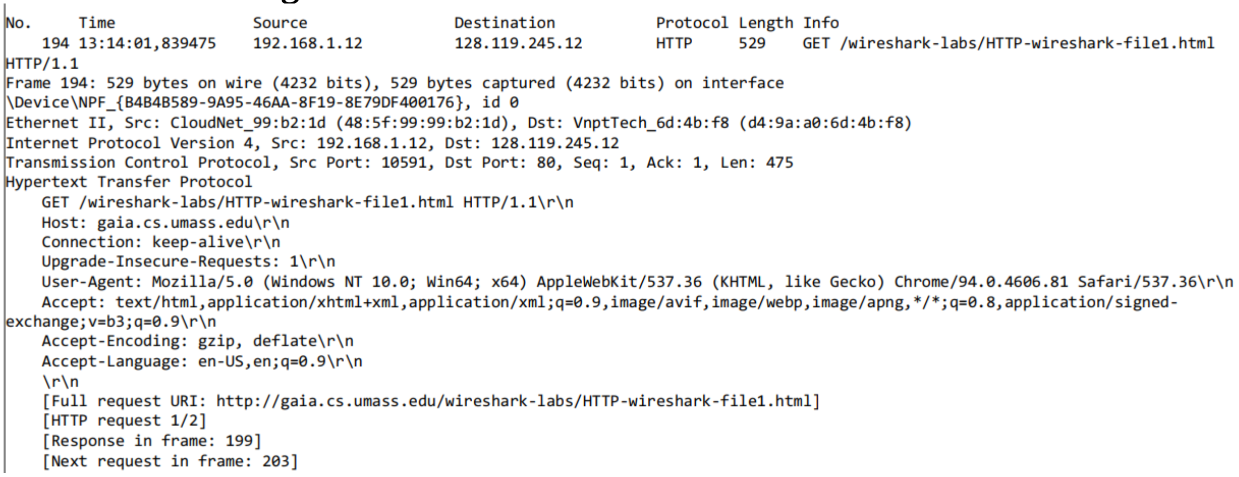
Question 7: By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

ANSWER:

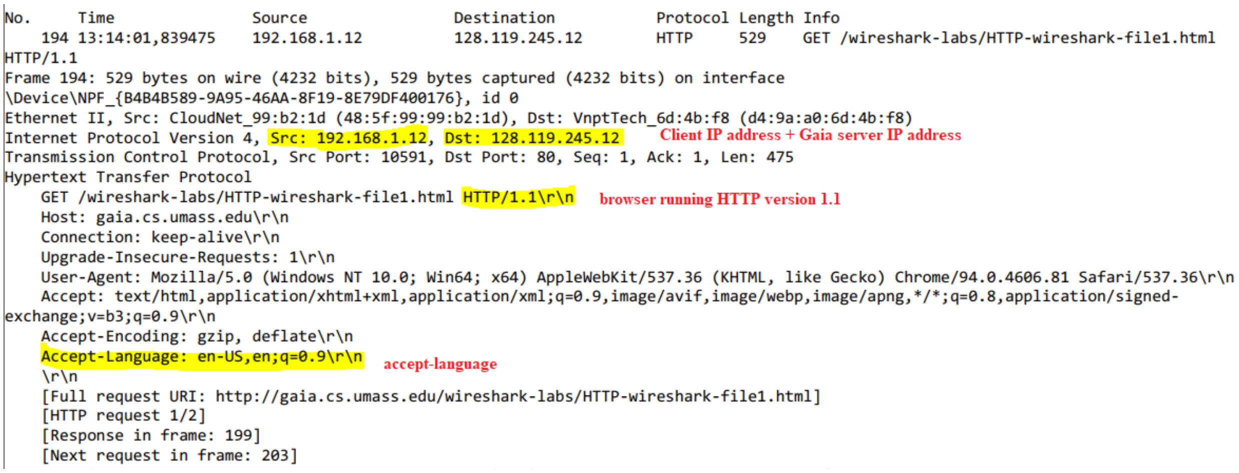
No, I do not see any headers displayed

Output Annotation:

*****GET message*****



```
No.     Time               Source                Destination           Protocol Length Info
    194 13:14:01,839475    192.168.1.12          128.119.245.12        HTTP     529    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 194: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 10591, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 199]
    [Next request in frame: 203]
```



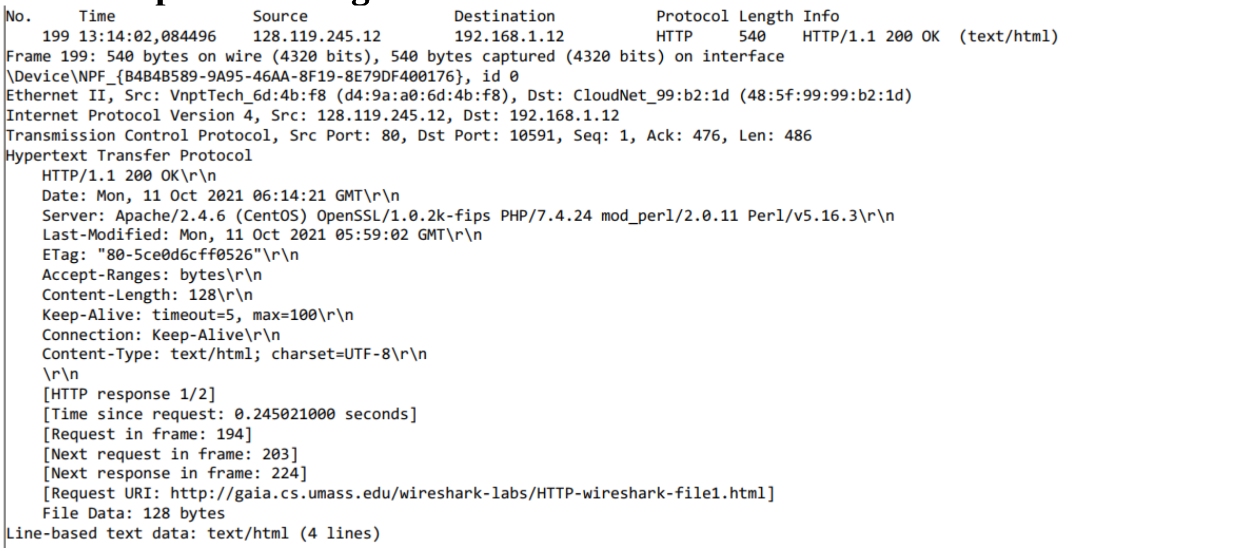
```
No.     Time               Source                Destination           Protocol Length Info
    194 13:14:01,839475    192.168.1.12          128.119.245.12        HTTP     529    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 194: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 10591, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 199]
    [Next request in frame: 203]
```

Client IP address + Gaia server IP address

browser running HTTP version 1.1

accept-language

*****Response message*****



```
No.     Time               Source                Destination           Protocol Length Info
    199 13:14:02,084496    128.119.245.12        192.168.1.12          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 199: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
Transmission Control Protocol, Src Port: 80, Dst Port: 10591, Seq: 1, Ack: 476, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 11 Oct 2021 06:14:21 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 11 Oct 2021 05:59:02 GMT\r\n
    ETag: "80-5ce0d6cff0526"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\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: 0.245021000 seconds]
    [Request in frame: 194]
    [Next request in frame: 203]
    [Next response in frame: 224]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

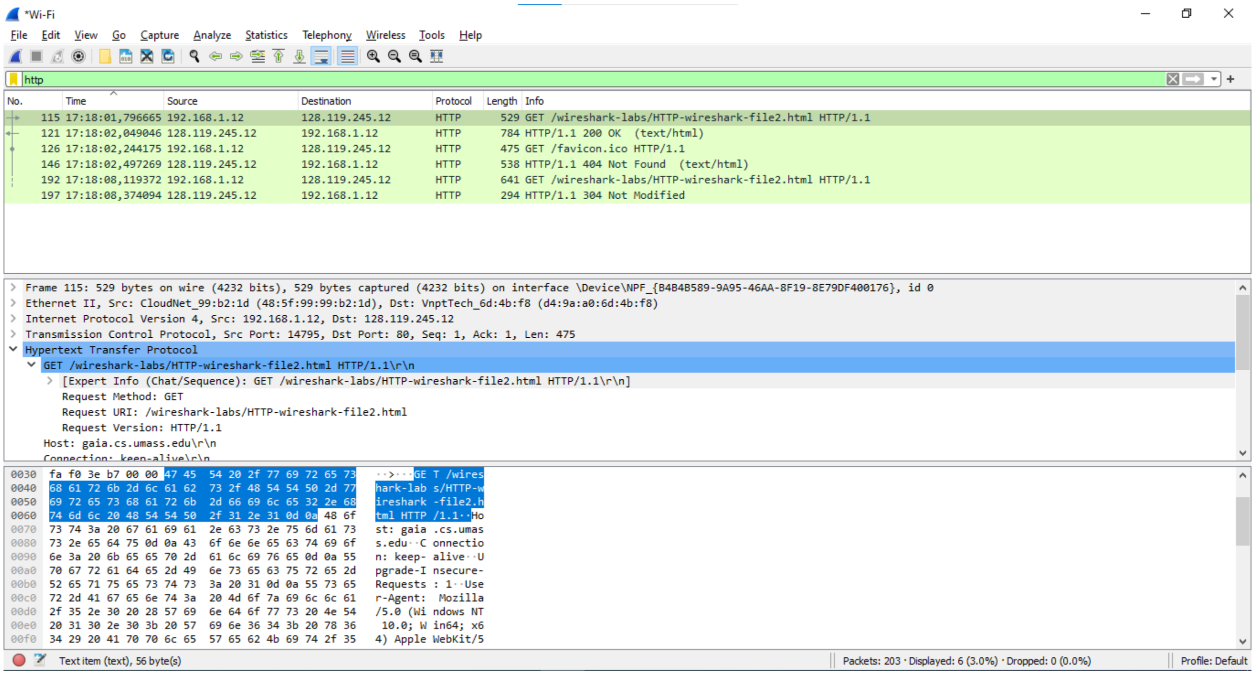
```
No.     Time           Source                Destination           Protocol Length Info
    199 13:14:02,084496    128.119.245.12        192.168.1.12          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 199: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
Transmission Control Protocol, Src Port: 80, Dst Port: 10591, Seq: 1, Ack: 476, Len: 486
Hypertext Transfer Protocol
server HTTP/1.1 200 OK\r\n  return status
running Date: Mon, 11 Oct 2021 06:14:21 GMT\r\n
HTTP Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
/1.1 Last-Modified: Mon, 11 Oct 2021 05:59:02 GMT\r\n  HTML file last-modified
    ETag: "80-5ce0d6cff0526"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n  content = 128 bytes
    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: 0.245021000 seconds]
    [Request in frame: 194]
    [Next request in frame: 203]
    [Next response in frame: 224]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

2. The HTTP CONDITIONAL GET/response interaction

Question 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?

ANSWER:

No, I do not see "IF-MODIFIED-SINCE" line in the 1st HTTP GET


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.  Time               Source          Destination     Protocol Length Info
 115 17:18:01,796665 192.168.1.12    128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 121 17:18:02,049046 128.119.245.12  192.168.1.12    HTTP      784 HTTP/1.1 200 OK  (text/html)
 126 17:18:02,244175 192.168.1.12    128.119.245.12  HTTP      475 GET /favicon.ico HTTP/1.1
 146 17:18:02,497269 128.119.245.12  192.168.1.12    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
 192 17:18:08,119372 192.168.1.12    128.119.245.12  HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 197 17:18:08,374094 128.119.245.12  192.168.1.12    HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Frame 115: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 14795, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

```
0030  fa f0 3e b7 00 00 47 45  54 20 2f 77 69 72 65 73   ··>···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
```

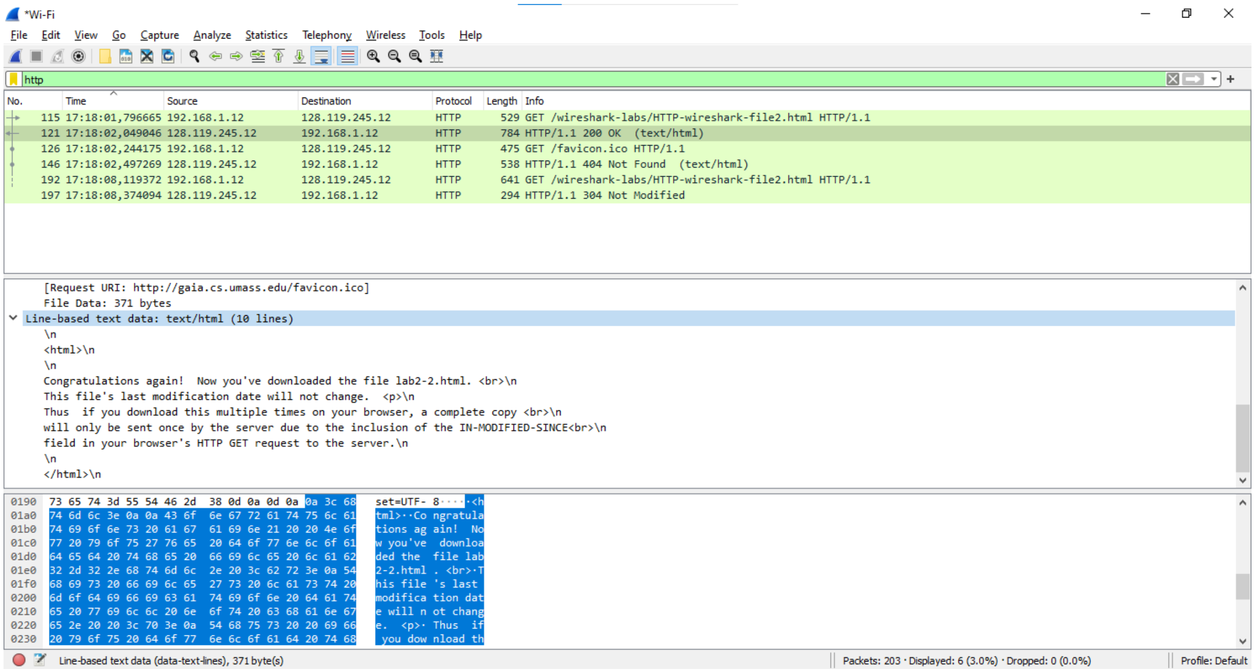
Text item (text), 56 byte(s) | Packets: 203 · Displayed: 6 (3.0%) · Dropped: 0 (0.0%) | Profile: Default

```
No.     Time               Source                Destination           Protocol Length Info
    115 17:18:01,796665    192.168.1.12          128.119.245.12        HTTP     529    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 115: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 14795, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 121]
    [Next request in frame: 126]
```

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

ANSWER:

Yes because we can see the contents in the line-based text data field.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

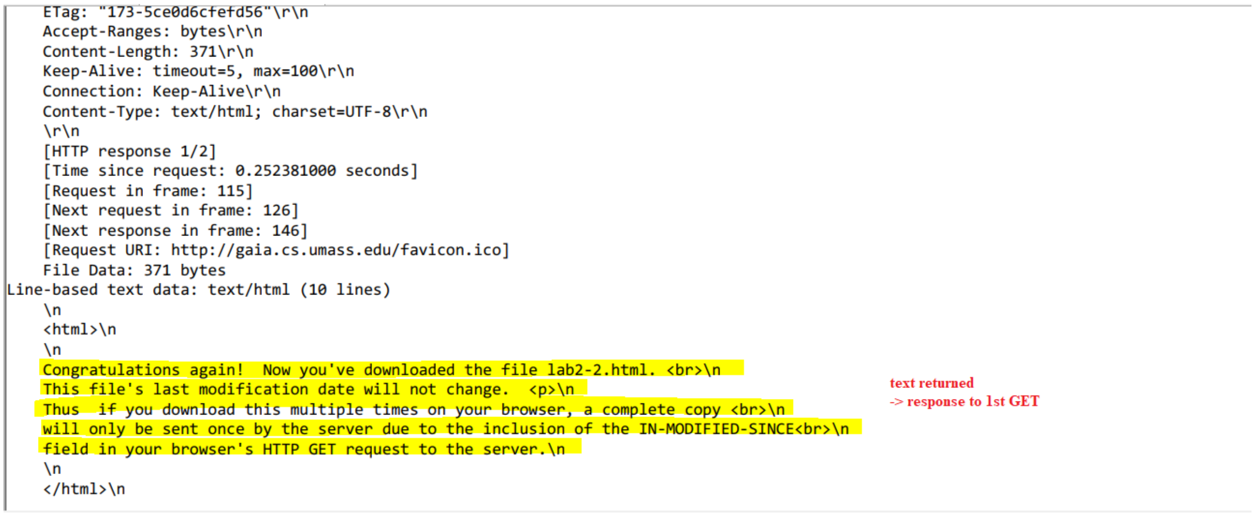
http

```
No.   Time             Source          Destination     Protocol Length Info
  115 17:18:01,796665 192.168.1.12    128.119.245.12  HTTP       529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  121 17:18:02,049046 128.119.245.12  192.168.1.12    HTTP       784 HTTP/1.1 200 OK  (text/html)
  126 17:18:02,244175 192.168.1.12    128.119.245.12  HTTP       475 GET /favicon.ico HTTP/1.1
  146 17:18:02,497269 128.119.245.12  192.168.1.12    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
  192 17:18:08,119372 192.168.1.12    128.119.245.12  HTTP       641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  197 17:18:08,374094 128.119.245.12  192.168.1.12    HTTP       294 HTTP/1.1 304 Not Modified
```

```
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

```
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>·T
01f0  68 69 73 20 66 69 6c 65  27 73 20 6c 61 73 74 20   his file 's last 
0200  6d 6f 64 69 66 69 63 61  74 69 6f 6e 20 64 61 74   modifica tion dat
0210  65 20 77 69 6c 6c 20 6e  6f 74 20 63 68 61 6e 67   e will n ot chang
0220  65 2e 20 20 3c 70 3e 0a  54 68 75 73 20 20 69 66   e.  <p>· Thus  if
0230  20 79 6f 75 20 64 6f 77  6e 6c 6f 61 64 20 74 68    you dow nload th
```

Line-based text data (data-text-lines), 371 byte(s) | Packets: 203 · Displayed: 6 (3.0%) · Dropped: 0 (0.0%) | Profile: Default



```
    ETag: "173-5ce0d6cfefd56"\r\n
    Accept-Ranges: bytes\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: 0.252381000 seconds]
    [Request in frame: 115]
    [Next request in frame: 126]
    [Next response in frame: 146]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

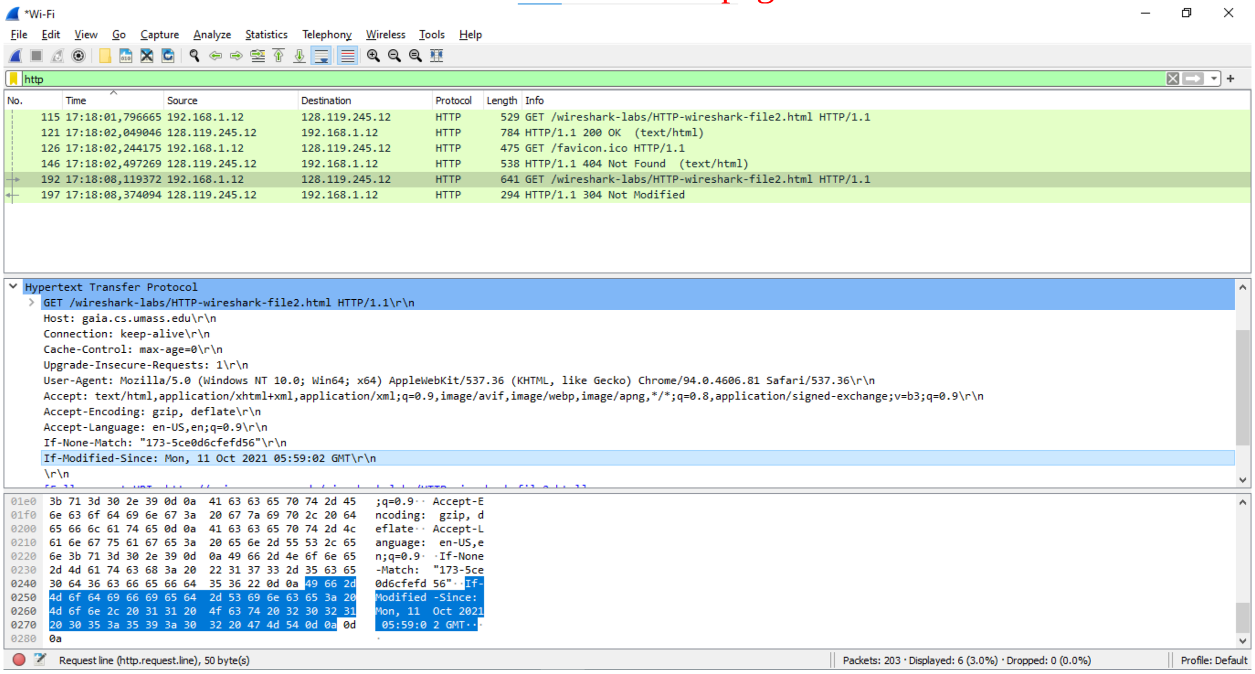
text returned
-> response to 1st GET

Question 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?

ANSWER:

Yes, I see.

In the 2nd HTTP message, an IF-MODIFIED-SINCE line is included, followed by the date and time that I last accessed to this webpage


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time              Source          Destination     Protocol Length Info
  115 17:18:01,796665 192.168.1.12    128.119.245.12  HTTP       529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  121 17:18:02,049046 128.119.245.12  192.168.1.12    HTTP       784 HTTP/1.1 200 OK  (text/html)
  126 17:18:02,244175 192.168.1.12    128.119.245.12  HTTP       475 GET /favicon.ico HTTP/1.1
  146 17:18:02,497269 128.119.245.12  192.168.1.12    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
  192 17:18:08,119372 192.168.1.12    128.119.245.12  HTTP       641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  197 17:18:08,374094 128.119.245.12  192.168.1.12    HTTP       294 HTTP/1.1 304 Not Modified
```

```
Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: en-US,en;q=0.9\r\n
    If-None-Match: "173-5ce0d6cfefd56"\r\n
    If-Modified-Since: Mon, 11 Oct 2021 05:59:02 GMT\r\n
    \r\n
```

```
01e0  3b 71 3d 30 2e 39 0d 0a  41 63 63 65 70 74 2d 45   ;q=0.9·· Accept-E
01f0  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 2c 20 64   ncoding:  gzip, d
0200  65 66 6c 61 74 65 0d 0a  41 63 63 65 70 74 2d 4c   eflate·· Accept-L
0210  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
0220  6e 3b 71 3d 30 2e 39 0d  0a 49 66 2d 4e 6f 6e 65   n;q=0.9· ·If-None
0230  2d 4d 61 74 63 68 3a 20  22 31 37 33 2d 35 63 65   -Match:  "173-5ce
0240  30 64 36 63 66 65 66 64  35 36 22 0d 0a 49 66 2d   0d6cfefd 56"··If-
0250  4d 6f 64 69 66 69 65 64  2d 53 69 6e 63 65 3a 20   Modified -Since: 
0260  4d 6f 6e 2c 20 31 31 20  4f 63 74 20 32 30 32 31   Mon, 11  Oct 2021
0270  20 30 35 3a 35 39 3a 30  32 20 47 4d 54 0d 0a 0d    05:59:0 2 GMT···
0280  0a                                                 ·
```

Request line (http.request.line), 50 byte(s) | Packets: 203 · Displayed: 6 (3.0%) · Dropped: 0 (0.0%) | Profile: Default

```
No.     Time                Source                Destination           Protocol Length Info
    192 17:18:08,119372     192.168.1.12          128.119.245.12        HTTP     641    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 192: 641 bytes on wire (5128 bits), 641 bytes captured (5128 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 13034, Dst Port: 80, Seq: 1, Ack: 1, Len: 587
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: en-US,en;q=0.9\r\n
    If-None-Match: "173-5ce0d6cfefd56"\r\n
    If-Modified-Since: Mon, 11 Oct 2021 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
```

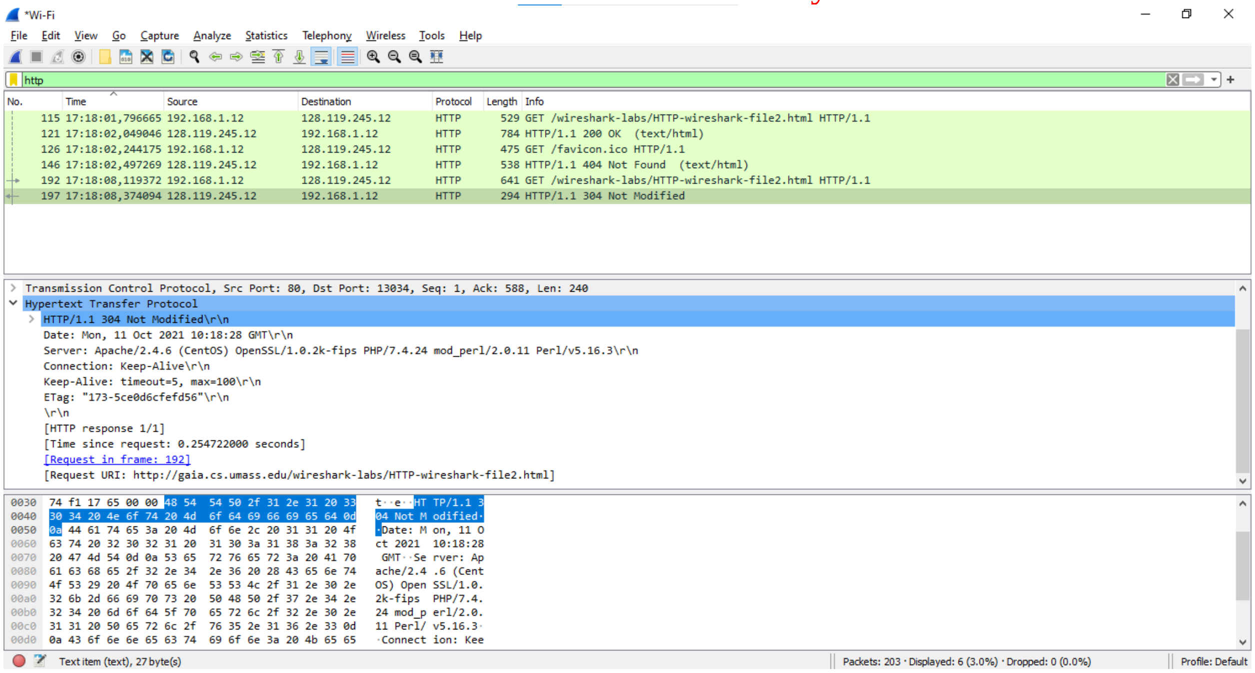
"IF-MODIFIED-SINCE:" line in the 2nd HTTP GET

<u>Question 11:</u> 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.

ANSWER:

The HTTP status code is "304: Not Modified"

The server did not return the contents of the file because the browser simply retrieved the contents from its cache. If the file had been modified since last access, it would have returned the contents of the file, instead it simply told the browser to retrieve the old file from its cached memory.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.     Time               Source          Destination     Protocol Length Info
    115 17:18:01,796665 192.168.1.12    128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    121 17:18:02,049046 128.119.245.12  192.168.1.12    HTTP      784 HTTP/1.1 200 OK  (text/html)
    126 17:18:02,244175 192.168.1.12    128.119.245.12  HTTP      475 GET /favicon.ico HTTP/1.1
    146 17:18:02,497269 128.119.245.12  192.168.1.12    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
    192 17:18:08,119372 192.168.1.12    128.119.245.12  HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    197 17:18:08,374094 128.119.245.12  192.168.1.12    HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 13034, Seq: 1, Ack: 588, Len: 240
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Mon, 11 Oct 2021 10:18:28 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5ce0d6cfefd56"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.254722000 seconds]
    [Request in frame: 192]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0030  74 f1 17 65 00 00 48 54  54 50 2f 31 2e 31 20 33   t··e··HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 31 31 20 4f   ·Date: M on, 11 O
0060  63 74 20 32 30 32 31 20  31 30 3a 31 38 3a 32 38   ct 2021  10:18:28
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
00b0  32 34 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   24 mod_p erl/2.0.
00c0  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
00d0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
```

Text item (text), 27 byte(s) | Packets: 203 · Displayed: 6 (3.0%) · Dropped: 0 (0.0%) | Profile: Default

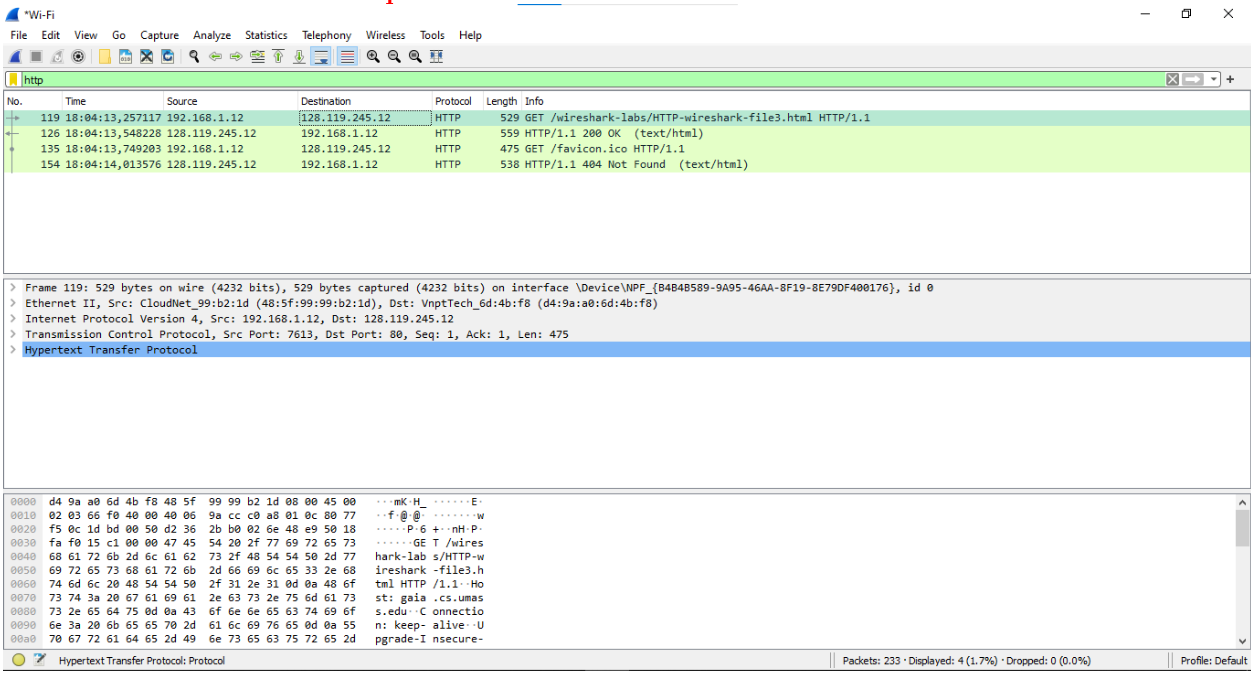
```
No.     Time                Source                Destination           Protocol Length Info
    197 17:18:08,374094     128.119.245.12        192.168.1.12          HTTP     294    HTTP/1.1 304 Not Modified
Frame 197: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
Transmission Control Protocol, Src Port: 80, Dst Port: 13034, Seq: 1, Ack: 588, Len: 240
Hypertext Transfer Protocol                304 Not Modified
    HTTP/1.1 304 Not Modified\r\n          =>The file has not been modified
    Date: Mon, 11 Oct 2021 10:18:28 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5ce0d6cfefd56"\r\n
    \r\n           the text is not returned
    [HTTP response 1/1]
    [Time since request: 0.254722000 seconds]
    [Request in frame: 192]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

3. Retrieving Long Documents

Question 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?

ANSWER:

There is 1 HTTP GET request


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

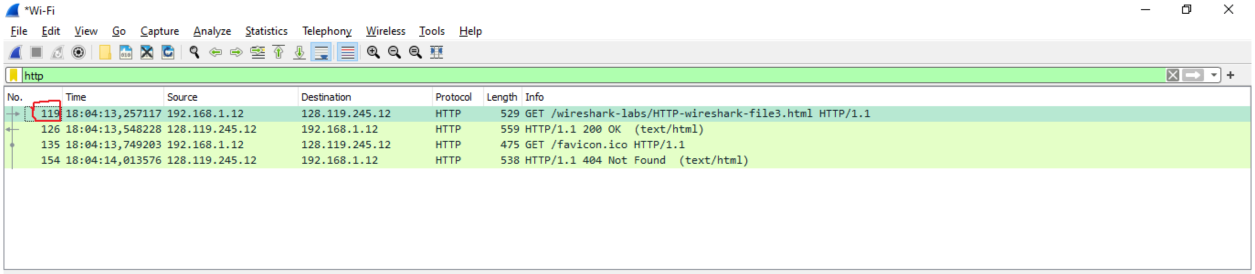
```
No.     Time            Source          Destination     Protocol Length Info
    119 18:04:13,257117 192.168.1.12    128.119.245.12  HTTP       529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    126 18:04:13,548228 128.119.245.12  192.168.1.12    HTTP       559 HTTP/1.1 200 OK  (text/html)
    135 18:04:13,749203 192.168.1.12    128.119.245.12  HTTP       475 GET /favicon.ico HTTP/1.1
    154 18:04:14,013576 128.119.245.12  192.168.1.12    HTTP       538 HTTP/1.1 404 Not Found  (text/html)

> Frame 119: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 7613, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
> Hypertext Transfer Protocol

0000  d4 9a a0 6d 4b f8 48 5f  99 99 b2 1d 08 00 45 00   ···mK·H_ ······E·
0010  02 03 66 f0 40 00 40 06  9a cc c0 a8 01 0c 80 77   ··f·@·@· ·······w
0020  f5 0c 1d bd 00 50 d2 36  2b b0 02 6e 48 e9 50 18   ·····P·6 +··nH·P·
0030  fa f0 15 c1 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68   ireshark -file3.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-

Hypertext Transfer Protocol: Protocol    Packets: 233 · Displayed: 4 (1.7%) · Dropped: 0 (0.0%)    Profile: Default
```

Packet number in the trace contains the GET message for the Bill or Rights: 119

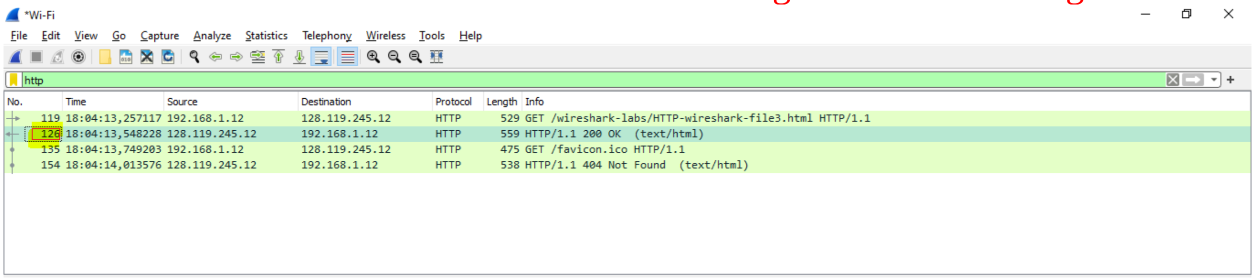

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.     Time            Source          Destination     Protocol Length Info
    119 18:04:13,257117 192.168.1.12    128.119.245.12  HTTP       529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    126 18:04:13,548228 128.119.245.12  192.168.1.12    HTTP       559 HTTP/1.1 200 OK  (text/html)
    135 18:04:13,749203 192.168.1.12    128.119.245.12  HTTP       475 GET /favicon.ico HTTP/1.1
    154 18:04:14,013576 128.119.245.12  192.168.1.12    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

<u>Question 13</u> Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

ANSWER:

Packet number in the trace contains the GET message for the Bill or Rights: 126

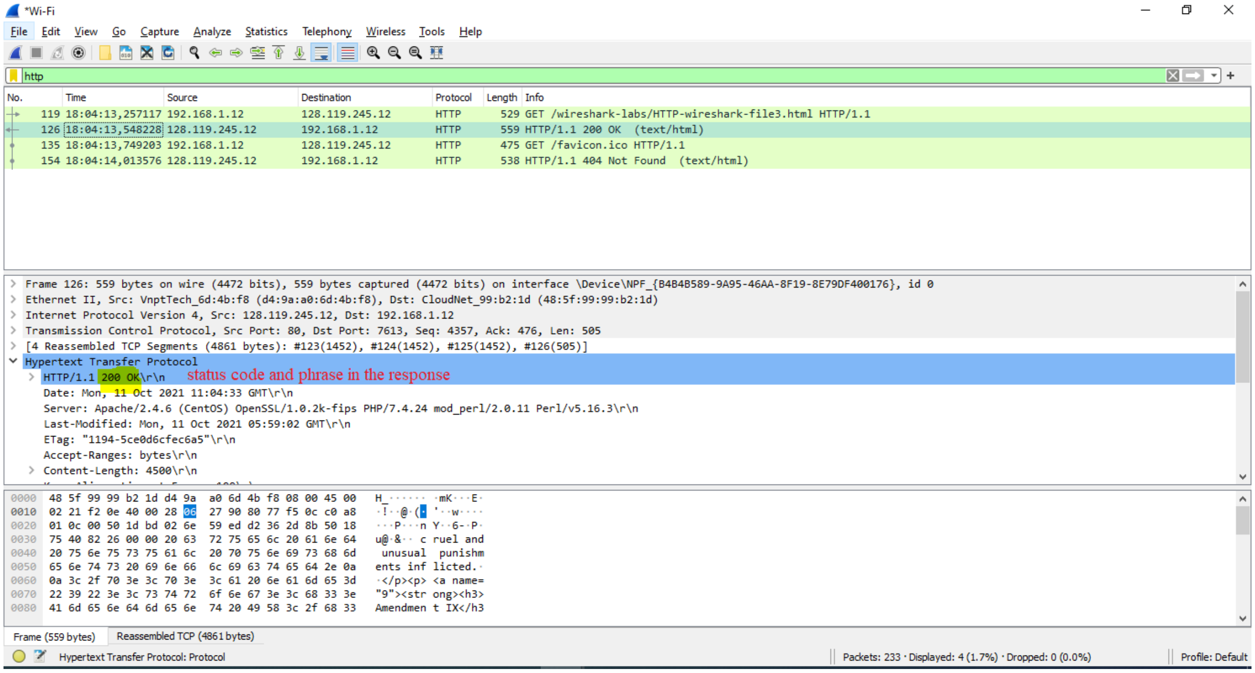

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time               Source          Destination      Protocol Length Info
  119 18:04:13,257117 192.168.1.12    128.119.245.12   HTTP      529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  126 18:04:13,548228 128.119.245.12  192.168.1.12     HTTP      559 HTTP/1.1 200 OK  (text/html)
  135 18:04:13,749203 192.168.1.12    128.119.245.12   HTTP      475 GET /favicon.ico HTTP/1.1
  154 18:04:14,013576 128.119.245.12  192.168.1.12     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

<u>Question 14:</u> What is the status code and phrase in the response?

ANSWER:

200 OK


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time               Source          Destination      Protocol Length Info
  119 18:04:13,257117 192.168.1.12    128.119.245.12   HTTP      529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  126 18:04:13,548228 128.119.245.12  192.168.1.12     HTTP      559 HTTP/1.1 200 OK  (text/html)
  135 18:04:13,749203 192.168.1.12    128.119.245.12   HTTP      475 GET /favicon.ico HTTP/1.1
  154 18:04:14,013576 128.119.245.12  192.168.1.12     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 126: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
> Transmission Control Protocol, Src Port: 80, Dst Port: 7613, Seq: 4357, Ack: 476, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #123(1452), #124(1452), #125(1452), #126(505)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 11 Oct 2021 11:04:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 11 Oct 2021 05:59:02 GMT\r\n
    ETag: "1194-5ce0d6cfec6a5"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
```

status code and phrase in the response

```
0000  48 5f 99 99 b2 1d d4 9a  a0 6d 4b f8 08 00 45 00   H_······ ·mK···E·
0010  02 21 f2 0e 40 00 28 06  27 90 80 77 f5 0c c0 a8   ·!··@·(· '··w····
0020  01 0c 00 50 1d bd 02 6e  59 ed d2 36 2d 8b 50 18   ···P···n Y··6-·P·
0030  75 40 82 26 00 00 20 63  72 75 65 6c 20 61 6e 64   u@·&·· c ruel and
0040  20 75 6e 75 73 75 61 6c  20 70 75 6e 69 73 68 6d    unusual  punishm
0050  65 6e 74 73 20 69 6e 66  6c 69 63 74 65 64 2e 0a   ents inf licted.·
0060  0a 3c 2f 70 3e 3c 70 3e  3c 61 20 6e 61 6d 65 3d   ·</p><p> <a name=
0070  22 39 22 3e 3c 73 74 72  6f 6e 67 3e 3c 68 33 3e   "9"><str ong><h3>
0080  41 6d 65 6e 64 6d 65 6e  74 20 49 58 3c 2f 68 33   Amendmen t IX</h3
```

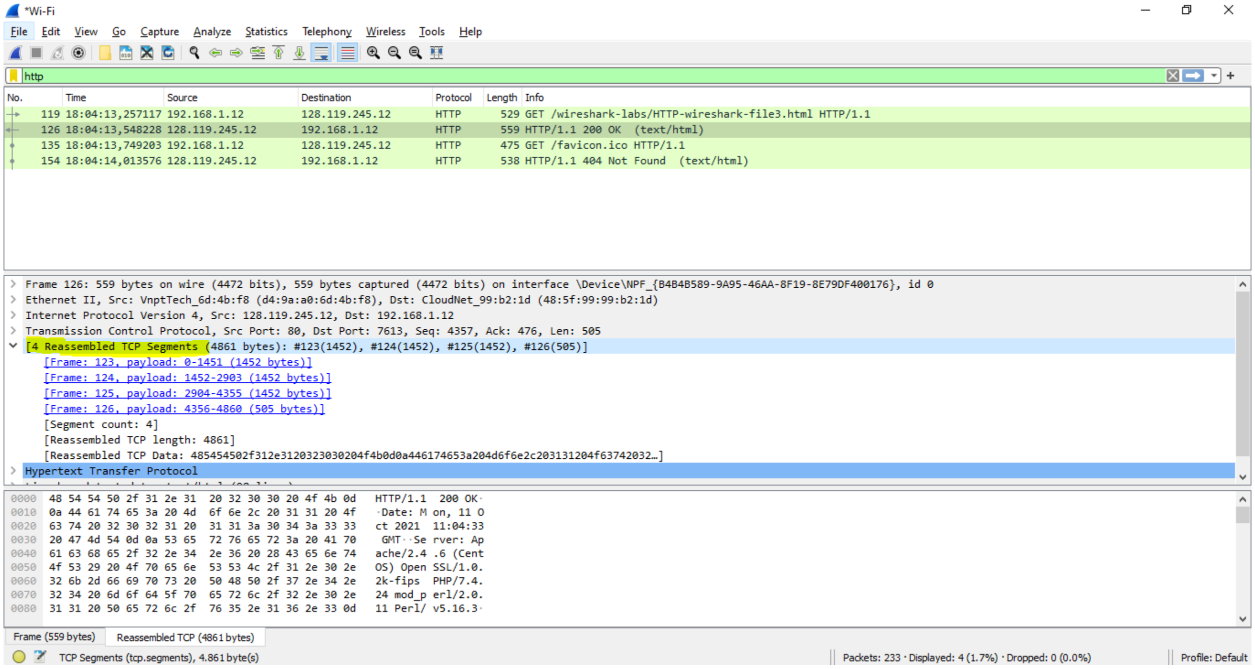
Frame (559 bytes) | Reassembled TCP (4861 bytes)

Hypertext Transfer Protocol: Protocol | Packets: 233 · Displayed: 4 (1.7%) · Dropped: 0 (0.0%) | Profile: Default

<u>Question 15:</u> How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

ANSWER:

4 data-containing TCP segments


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time               Source          Destination     Protocol  Length Info
  119 18:04:13,257117 192.168.1.12    128.119.245.12  HTTP        529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  126 18:04:13,548228 128.119.245.12  192.168.1.12    HTTP        559 HTTP/1.1 200 OK  (text/html)
  135 18:04:13,749203 192.168.1.12    128.119.245.12  HTTP        475 GET /favicon.ico HTTP/1.1
  154 18:04:14,013576 128.119.245.12  192.168.1.12    HTTP        538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 126: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
> Transmission Control Protocol, Src Port: 80, Dst Port: 7613, Seq: 4357, Ack: 476, Len: 505
v [4 Reassembled TCP Segments (4861 bytes): #123(1452), #124(1452), #125(1452), #126(505)]
    [Frame: 123, payload: 0-1451 (1452 bytes)]
    [Frame: 124, payload: 1452-2903 (1452 bytes)]
    [Frame: 125, payload: 2904-4355 (1452 bytes)]
    [Frame: 126, payload: 4356-4860 (505 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203131204f63742032…]
> Hypertext Transfer Protocol
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 31 31 20 4f   ·Date: M on, 11 O
0020  63 74 20 32 30 32 31 20  31 31 3a 30 34 3a 33 33   ct 2021  11:04:33
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  32 34 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   24 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
```

Frame (559 bytes) | Reassembled TCP (4861 bytes)

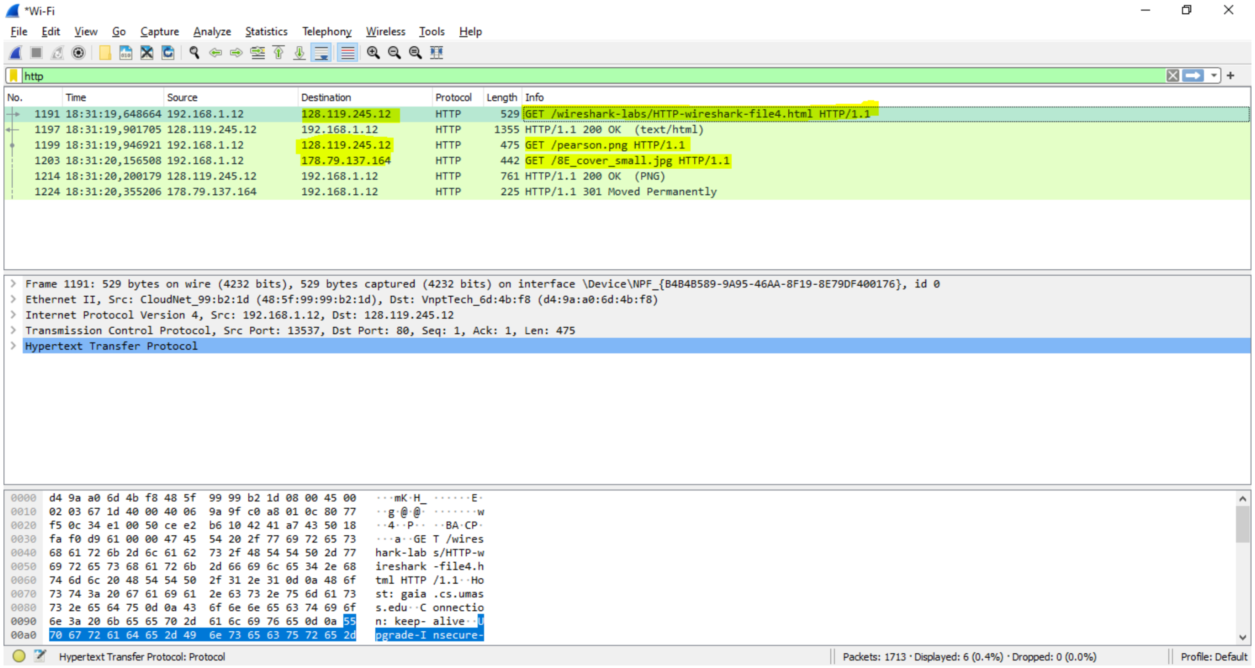
TCP Segments (tcp.segments), 4.861 byte(s) | Packets: 233 · Displayed: 4 (1.7%) · Dropped: 0 (0.0%) | Profile: Default

4. HTML Documents with Embedded Objects

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

ANSWER:

There were 3 HTTP GET requests sent to the following Internet addresses: 128.119.245.12, 128.119.245.12, 178.79.137.164


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time               Source          Destination     Protocol  Length Info
 1191 18:31:19,648664 192.168.1.12    128.119.245.12  HTTP        529 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 1197 18:31:19,901705 128.119.245.12  192.168.1.12    HTTP       1355 HTTP/1.1 200 OK  (text/html)
 1199 18:31:19,946921 192.168.1.12    128.119.245.12  HTTP        475 GET /pearson.png HTTP/1.1
 1203 18:31:20,156508 192.168.1.12    178.79.137.164  HTTP        442 GET /8E_cover_small.jpg HTTP/1.1
 1214 18:31:20,200179 128.119.245.12  192.168.1.12    HTTP        761 HTTP/1.1 200 OK  (PNG)
 1224 18:31:20,355206 178.79.137.164  192.168.1.12    HTTP        225 HTTP/1.1 301 Moved Permanently
```

```
> Frame 1191: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 13537, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
> Hypertext Transfer Protocol
```

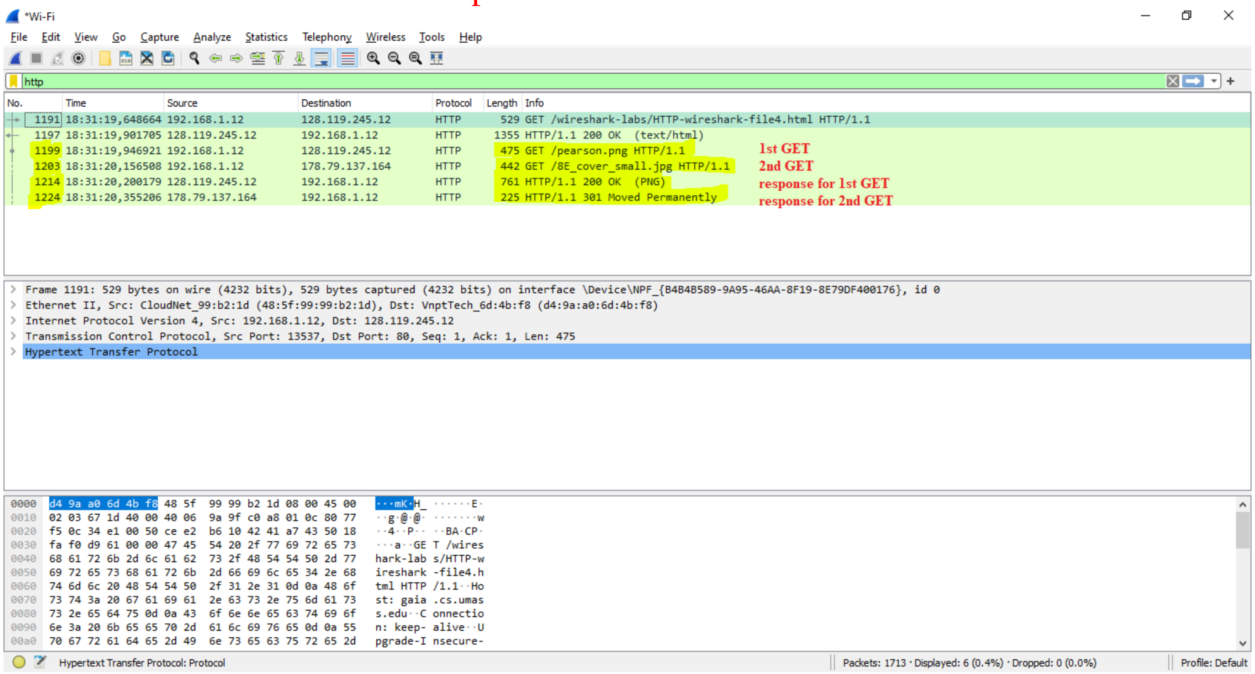
```
0000  d4 9a a0 6d 4b f8 48 5f  99 99 b2 1d 08 00 45 00   ···mK·H_ ······E·
0010  02 03 67 1d 40 00 40 06  9a 9f c0 a8 01 0c 80 77   ··g·@·@· ·······w
0020  f5 0c 34 e1 00 50 ce e2  b6 10 42 41 a7 43 50 18   ··4··P·· ··BA·CP·
0030  fa f0 d9 61 00 00 47 45  54 20 2f 77 69 72 65 73   ···a··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
```

Hypertext Transfer Protocol: Protocol | Packets: 1713 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%) | Profile: Default

Question 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.

ANSWER:

The downloads occurred in parallel:
+ The 2 GET messages for the images are in packets 1199 and 1203.
+ The response for these messages are in packets 1214, and 1224.
Thus the request for the 2nd image file (packet 1203) was made **BEFORE** packet 1214, the first image file was received.
=> The downloads occurred in parallel


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1191	18:31:19,648664	192.168.1.12	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1197	18:31:19,901705	128.119.245.12	192.168.1.12	HTTP	1355	HTTP/1.1 200 OK (text/html)
1199	18:31:19,946921	192.168.1.12	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
1203	18:31:20,156508	192.168.1.12	178.79.137.164	HTTP	442	GET /8E_cover_small.jpg HTTP/1.1
1214	18:31:20,200179	128.119.245.12	192.168.1.12	HTTP	761	HTTP/1.1 200 OK (PNG)
1224	18:31:20,355206	178.79.137.164	192.168.1.12	HTTP	225	HTTP/1.1 301 Moved Permanently

1st GET
2nd GET
response for 1st GET
response for 2nd GET

```
> Frame 1191: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 13537, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
> Hypertext Transfer Protocol
```

```
0000  d4 9a a0 6d 4b f8 48 5f  99 99 b2 1d 08 00 45 00   ···mK·H_ ······E·
0010  02 03 67 1d 40 00 40 06  9a 9f c0 a8 01 0c 80 77   ··g·@·@· ·······w
0020  f5 0c 34 e1 00 50 ce e2  b6 10 42 41 a7 43 50 18   ··4··P·· ··BA·CP·
0030  fa f0 d9 61 00 00 47 45  54 20 2f 77 69 72 65 73   ···a··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
```

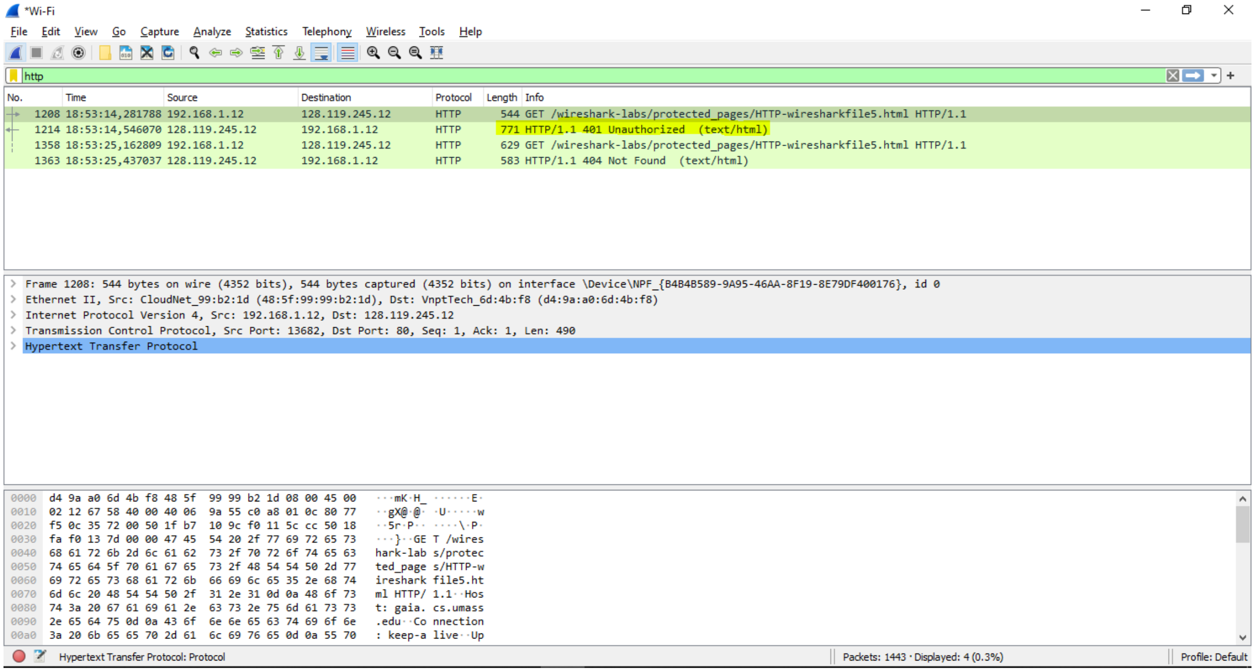
Hypertext Transfer Protocol: Protocol | Packets: 1713 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%) | Profile: Default

5 HTTP Authentication

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

ANSWER:

Initial HTTP GET response: 401 Unauthorized


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.     Time            Source          Destination     Protocol Length Info
   1208 18:53:14,281788 192.168.1.12    128.119.245.12  HTTP       544 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
   1214 18:53:14,546070 128.119.245.12  192.168.1.12    HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
   1358 18:53:25,162809 192.168.1.12    128.119.245.12  HTTP       629 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
   1363 18:53:25,437037 128.119.245.12  192.168.1.12    HTTP       583 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 1208: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
> Ethernet II, Src: CloudNet_99:b2:1d (48:5f:99:99:b2:1d), Dst: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 13682, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
> Hypertext Transfer Protocol
```

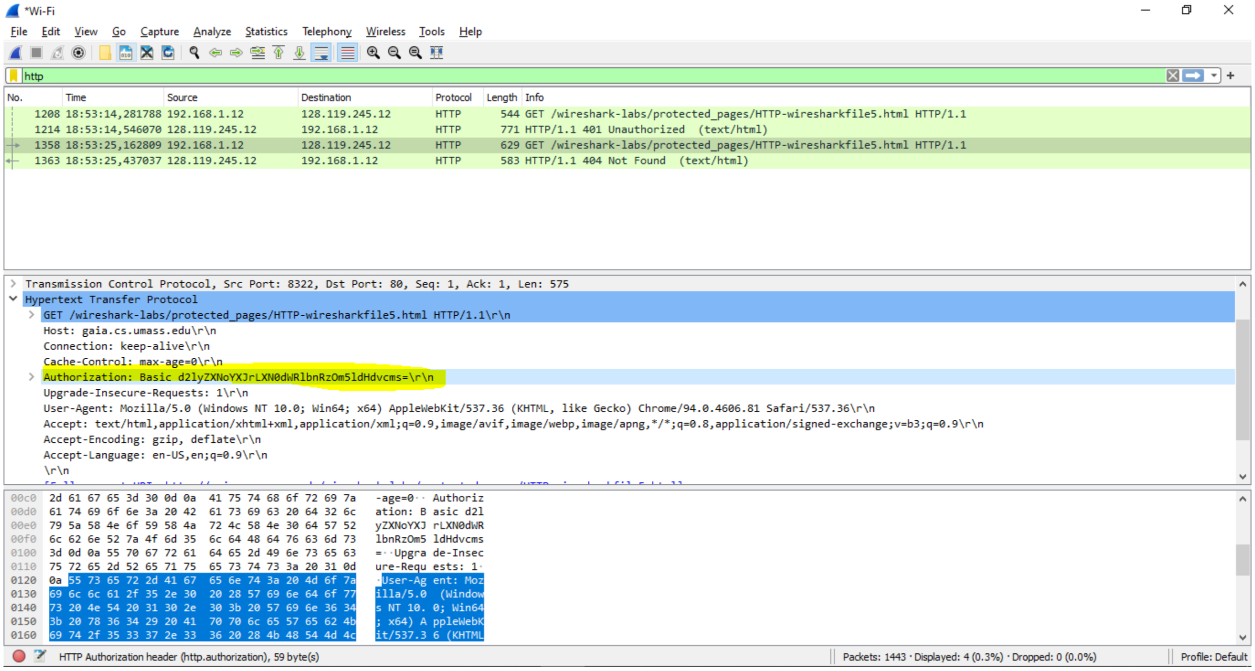
```
0000  d4 9a a0 6d 4b f8 48 5f  99 99 b2 1d 08 00 45 00   ···mK·H_ ······E·
0010  02 12 67 58 40 00 40 06  9a 55 c0 a8 01 0c 80 77   ··gX@·@· ·U·····w
0020  f5 0c 35 72 00 50 1f b7  10 9c f0 11 5c cc 50 18   ··5r·P·· ····\·P·
0030  fa f0 13 7d 00 00 47 45  54 20 2f 77 69 72 65 73   ···}··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  66 69 6c 65 35 2e 68 74   ireshark file5.ht
0070  6d 6c 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   ml HTTP/ 1.1··Hos
0080  74 3a 20 67 61 69 61 2e  63 73 2e 75 6d 61 73 73   t: gaia. cs.umass
0090  2e 65 64 75 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .edu··Co nnection
00a0  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 55 70   : keep-a live··Up
```

Hypertext Transfer Protocol: Protocol | Packets: 1443 · Displayed: 4 (0.3%) | Profile: Default

<u>Question 19:</u> When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

ANSWER:

The HTTP GET includes the Authorization: Basic: field


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.     Time            Source          Destination     Protocol Length Info
   1208 18:53:14,281788 192.168.1.12    128.119.245.12  HTTP       544 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
   1214 18:53:14,546070 128.119.245.12  192.168.1.12    HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
   1358 18:53:25,162809 192.168.1.12    128.119.245.12  HTTP       629 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
   1363 18:53:25,437037 128.119.245.12  192.168.1.12    HTTP       583 HTTP/1.1 404 Not Found  (text/html)
```

```
> Transmission Control Protocol, Src Port: 8322, Dst Port: 80, Seq: 1, Ack: 1, Len: 575
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html 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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: en-US,en;q=0.9\r\n
    \r\n
```

```
00c0  2d 61 67 65 3d 30 0d 0a  41 75 74 68 6f 72 69 7a   -age=0·· Authoriz
00d0  61 74 69 6f 6e 3a 20 42  61 73 69 63 20 64 32 6c   ation: B asic d2l
00e0  79 5a 58 4e 6f 59 58 4a  72 4c 58 4e 30 64 57 52   yZXNoYXJ rLXN0dWR
00f0  6c 62 6e 52 7a 4f 6d 35  6c 64 48 64 76 63 6d 73   lbnRzOm5 ldHdvcms
0100  3d 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   =··Upgra de-Insec
0110  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
0120  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0130  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0140  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0150  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0160  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
```

HTTP Authorization header (http.authorization), 59 byte(s) | Packets: 1443 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%) | Profile: Default