天津大学

《计算机网络》

题目：Wireshark Lab: HTTP

学　院　　智能与计算学部

专　业　　计算机科学与技术

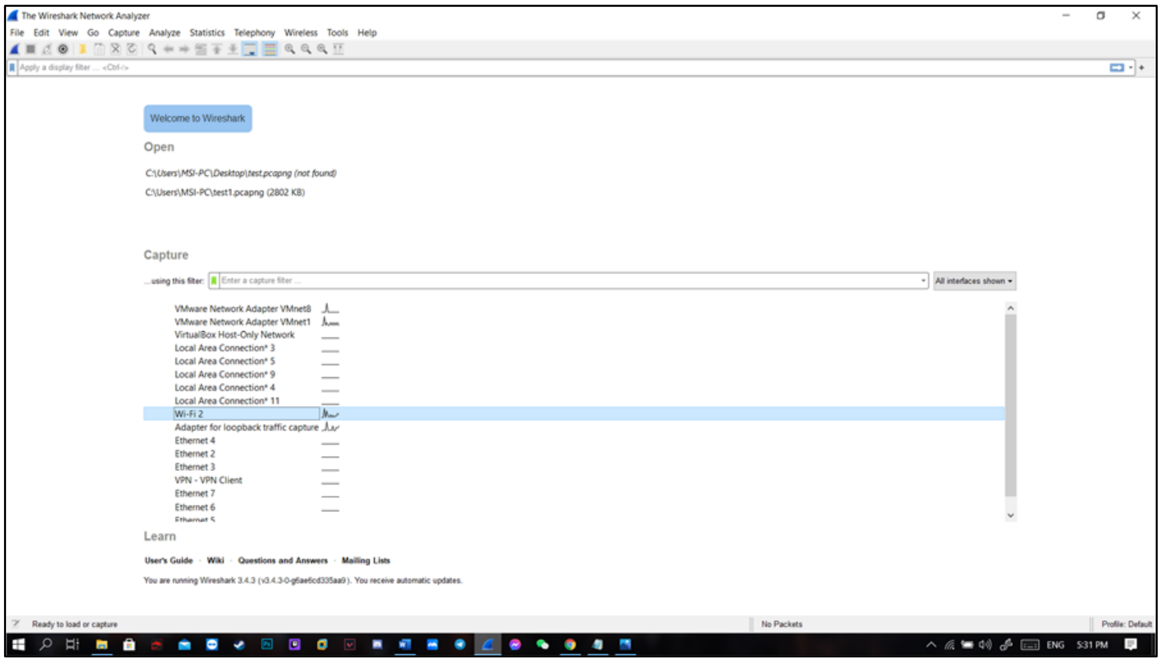
年　级　　2019

姓　名　　张明君（2 班）

学　号　　6319000359

2021 年 10 月 1 日

Before we start with this lab let's open Wireshark. You might be seeing a window "similar" to the one showed in the figure below.



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\MSI-PC\Desktop\test.pcapng (not found)
C:\Users\MSI-PC\test1.pcapng (2802 KB)
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
VirtualBox Host-Only Network
Local Area Connection* 3
Local Area Connection* 5
Local Area Connection* 9
Local Area Connection* 4
Local Area Connection* 11
Wi-Fi 2
Adapter for loopback traffic capture
Ethernet 4
Ethernet 2
Ethernet 3
VPN - VPN Client
Ethernet 7
Ethernet 6
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.4.3 (v3.4.3-0-g6ae6cd335aa9). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

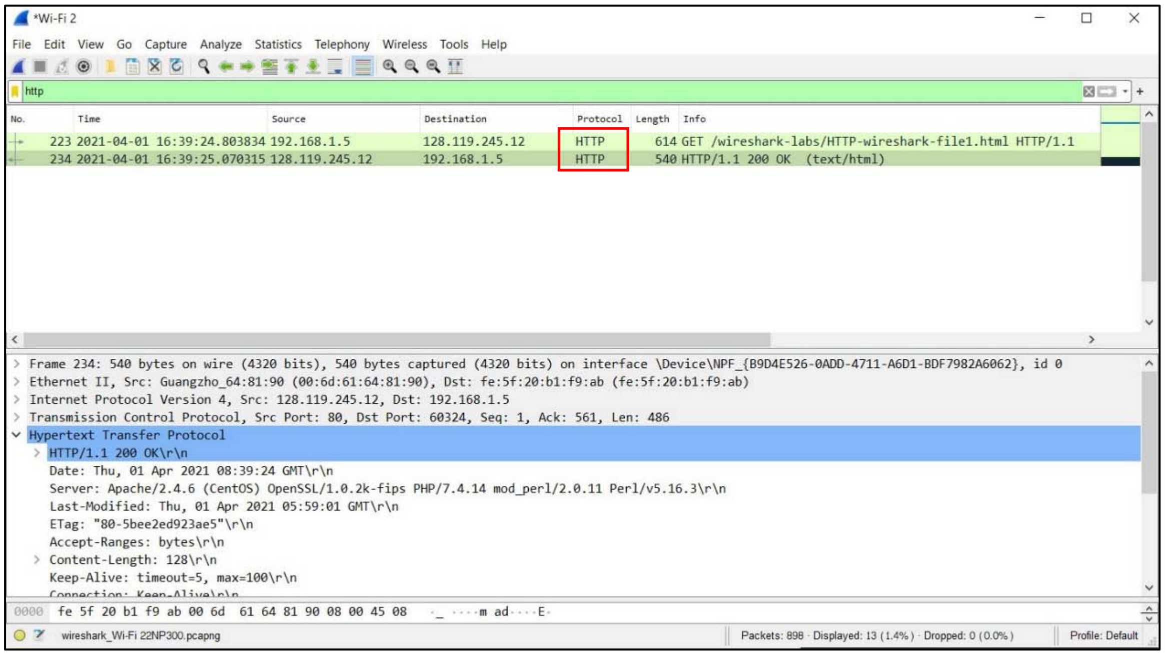
Figure 1:Wireshark interface

We already know how to start capture it in the last experiment. So, we don't want to talk about the specific thing of it anymore. Now we can start our Wireshark HTTP lab.

1. The Basic HTTP GET/response interaction

For the first part of this lab do the following:

(1) Start up your web browser.
(2) Start up the Wireshark packet Sniffer. Enter http in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
(3) Wait a bit more than one minute, and then begin Wireshark packet capture.
(4) Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html Your browser should display the very simple, one-line HTML file.
(5) Stop Wireshark packet capture.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time                        Source          Destination     Protocol Length Info
  223 2021-04-01 16:39:24.803834 192.168.1.5     128.119.245.12  HTTP     614 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  234 2021-04-01 16:39:25.070315 128.119.245.12  192.168.1.5     HTTP     540 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 234: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: Guangzho_64:81:90 (00:6d:61:64:81:90), Dst: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 60324, Seq: 1, Ack: 561, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 01 Apr 2021 08:39:24 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 01 Apr 2021 05:59:01 GMT\r\n
    ETag: "80-5bee2ed923ae5"\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
0000  fe 5f 20 b1 f9 ab 00 6d  61 64 81 90 08 00 45 08   ·_ ····m ad····E·
```

wireshark_Wi-Fi 22NP300.pcapng
Packets: 898 · Displayed: 13 (1.4%) · Dropped: 0 (0.0%)
Profile: Default

Figure 2:Wireshark Display after the first link that we put into browser

The above Figure shows in the packet-listing window that two HTTP messages were captured:

- The **GET** request message (from your browser to the gaia.cs.umass.edu web server)
- The response message from the server to your browser.

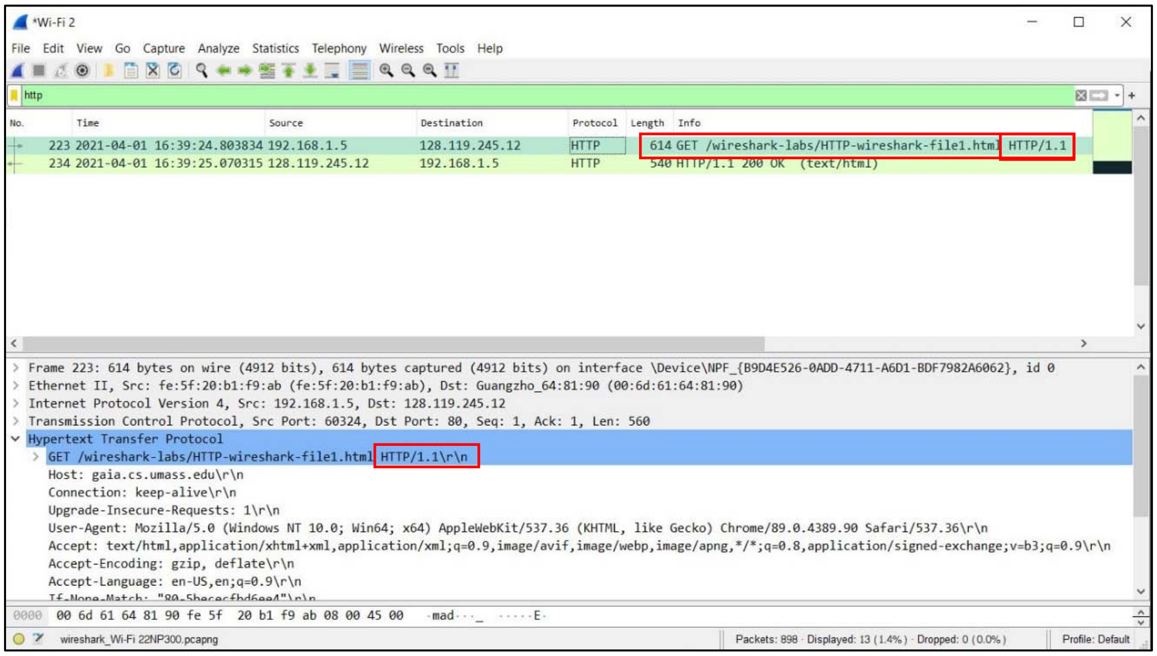
The HTTP response message consists of a status line, followed by header lines, followed by a blank line, followed by the entity body.

Note that since HTTP messages are carried inside a TCP segment, which are carried inside an IP datagram, which are carried within an Ethernet frame, Wireshark displays the Frame, Ethernet, IP, and TCP packet information as well.

However, because this lab is for HTTP let us ignore all non-HTTP data displayed, and let us extend the data displayed for "**Hypertext Transfer Protocol**".

By looking at the information in the HTTP GET and response messages, answer the following questions.

1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   You can see my Browser and Server are running **HTTP 1.1.**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time                        Source         Destination     Protocol Length Info
  223 2021-04-01 16:39:24.803834 192.168.1.5    128.119.245.12  HTTP        614 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  234 2021-04-01 16:39:25.070315 128.119.245.12 192.168.1.5     HTTP        540 HTTP/1.1 200 OK  (text/html)
```

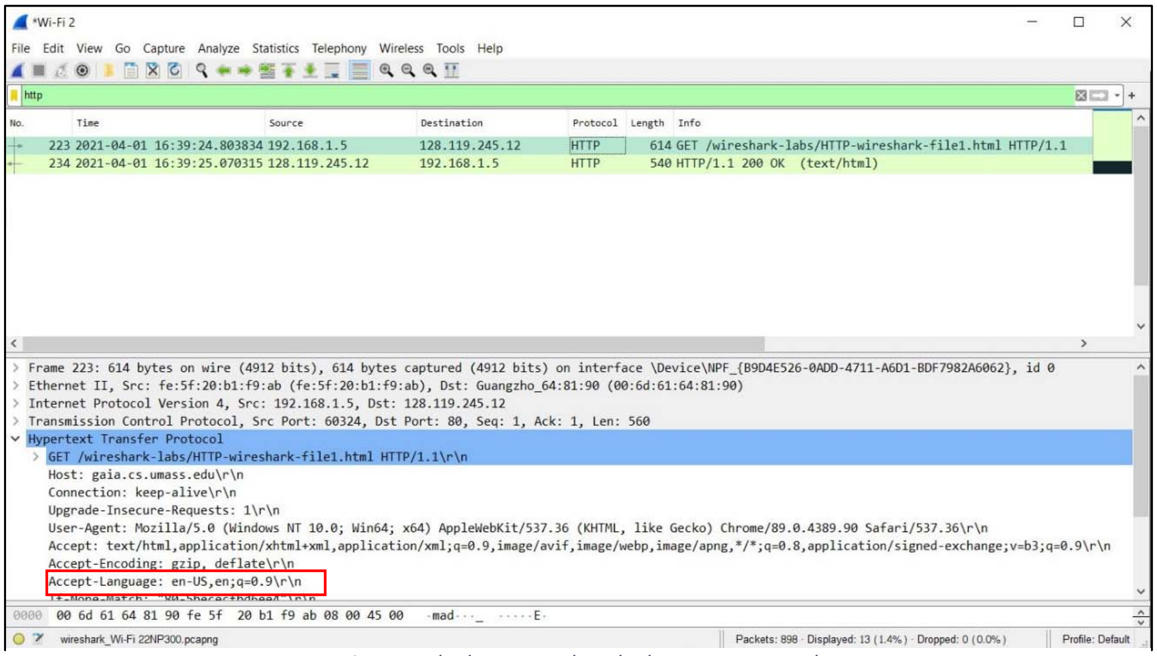
```
> Frame 223: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab), Dst: Guangzho_64:81:90 (00:6d:61:64:81:90)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60324, Dst Port: 80, Seq: 1, Ack: 1, Len: 560
v 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/89.0.4389.90 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
```

```
0000  00 6d 61 64 81 90 fe 5f  20 b1 f9 ab 08 00 45 00   ·mad···_ ·····E·
```

wireshark_Wi-Fi 22NP300.pcapng
Packets: 898 · Displayed: 13 (1.4%) · Dropped: 0 (0.0%)
Profile: Default

Figure 3:The server of the HTTP

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


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time                        Source         Destination     Protocol Length Info
  223 2021-04-01 16:39:24.803834 192.168.1.5    128.119.245.12  HTTP        614 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  234 2021-04-01 16:39:25.070315 128.119.245.12 192.168.1.5     HTTP        540 HTTP/1.1 200 OK  (text/html)
```

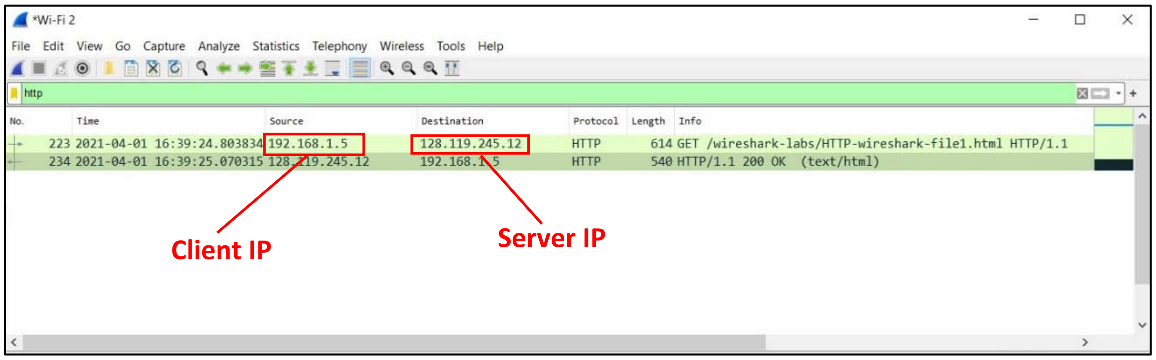
```
> Frame 223: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab), Dst: Guangzho_64:81:90 (00:6d:61:64:81:90)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60324, Dst Port: 80, Seq: 1, Ack: 1, Len: 560
v 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/89.0.4389.90 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
```

```
0000  00 6d 61 64 81 90 fe 5f  20 b1 f9 ab 08 00 45 00   ·mad···_ ·····E·
```

wireshark_Wi-Fi 22NP300.pcapng
Packets: 898 · Displayed: 13 (1.4%) · Dropped: 0 (0.0%)
Profile: Default

Figure 4:The language that the browser accepted

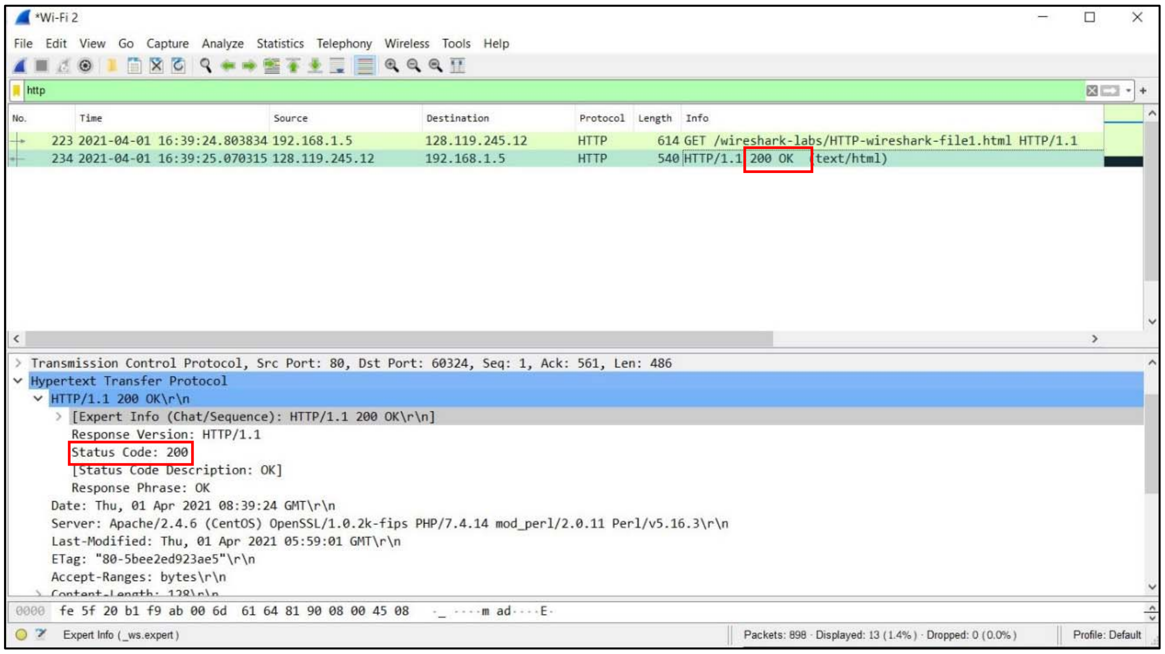
3) What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Client IP: 192.168.1.5
Server IP: 128.119.245.12
As shown in the Figure below you can get the IP information from the HTTP GET and response messages on the Packet Listing window of from the Internet Protocol line on the Packet-Header details window.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Client IP
Server IP

```
No.  Time                        Source          Destination     Protocol Length Info
223  2021-04-01 16:39:24.803834  192.168.1.5     128.119.245.12  HTTP     614    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
234  2021-04-01 16:39:25.070315  128.119.245.12  192.168.1.5     HTTP     540    HTTP/1.1 200 OK  (text/html)
```

Figure 5:Client and Server IP address

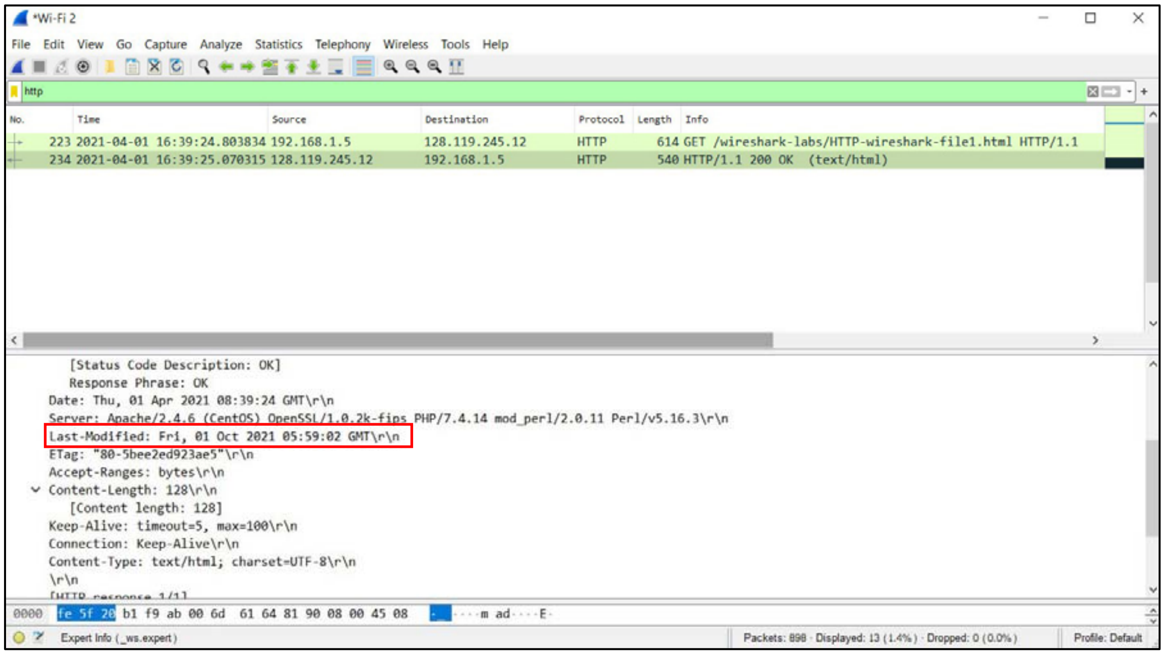
4) What is the status code returned from the server to your browser?
Status code: 200
The HTTP status code will give you information about the response to your HTTP request. For example: code 2xx (such as 200) means that the request was successfully completed.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time                        Source          Destination     Protocol Length Info
223  2021-04-01 16:39:24.803834  192.168.1.5     128.119.245.12  HTTP     614    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
234  2021-04-01 16:39:25.070315  128.119.245.12  192.168.1.5     HTTP     540    HTTP/1.1 200 OK  (text/html)

> Transmission Control Protocol, Src Port: 80, Dst Port: 60324, Seq: 1, Ack: 561, Len: 486
v Hypertext Transfer Protocol
  v 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: Thu, 01 Apr 2021 08:39:24 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 01 Apr 2021 05:59:01 GMT\r\n
    ETag: "80-5bee2ed923ae5"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n

0000  fe 5f 20 b1 f9 ab 00 6d  61 64 81 90 08 00 45 08   ·_ ····m ad····E·

Expert Info (_ws.expert)    Packets: 898 · Displayed: 13 (1.4%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 6:Status code returned from server

5) When was the HTML file that you are retrieving last modified at the server?
   - **Last modified: Fri, 01 Oct 2021 05:59:02 GMT**

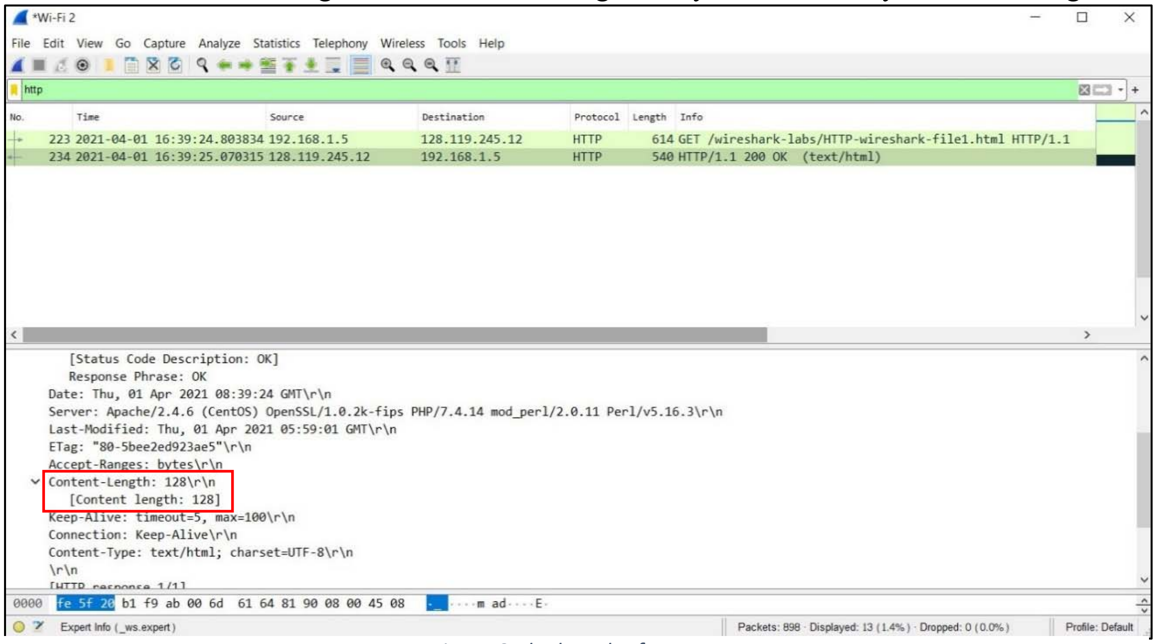

*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time                        Source          Destination     Protocol  Length  Info
  223 2021-04-01 16:39:24.803834 192.168.1.5     128.119.245.12  HTTP      614 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  234 2021-04-01 16:39:25.070315 128.119.245.12  192.168.1.5     HTTP      540 HTTP/1.1 200 OK  (text/html)

      [Status Code Description: OK]
      Response Phrase: OK
   Date: Thu, 01 Apr 2021 08:39:24 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
   Last-Modified: Fri, 01 Oct 2021 05:59:02 GMT\r\n
   ETag: "80-5bee2ed923ae5"\r\n
   Accept-Ranges: bytes\r\n
 v 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]

0000  fe 5f 20 b1 f9 ab 00 6d  61 64 81 90 08 00 45 08   ._ ····m ad····E·

Expert Info (_ws.expert)    Packets: 898 · Displayed: 13 (1.4%) · Dropped: 0 (0.0%)    Profile: Default
```

Notice that the document you just retrieved was last modified within a minute before you downloaded the document. That is because for this particular file, the gaia.cs.umass.edu server is setting the file's last-modified time to be the current time, and is doing so once per minute.

6) How many bytes of content are being returned to your browser?
   - **Content length: 128**

   The Content-Length will return the length in bytes of the body of the message.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time                        Source          Destination     Protocol  Length  Info
  223 2021-04-01 16:39:24.803834 192.168.1.5     128.119.245.12  HTTP      614 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  234 2021-04-01 16:39:25.070315 128.119.245.12  192.168.1.5     HTTP      540 HTTP/1.1 200 OK  (text/html)

      [Status Code Description: OK]
      Response Phrase: OK
   Date: Thu, 01 Apr 2021 08:39:24 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
   Last-Modified: Thu, 01 Apr 2021 05:59:01 GMT\r\n
   ETag: "80-5bee2ed923ae5"\r\n
   Accept-Ranges: bytes\r\n
 v 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]

0000  fe 5f 20 b1 f9 ab 00 6d  61 64 81 90 08 00 45 08   ._ ····m ad····E·

Expert Info (_ws.expert)    Packets: 898 · Displayed: 13 (1.4%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 8:The length 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.
   - **NO,** All the headers can be found in the raw data.

2. The HTTP CONDITIONAL GET/response interaction

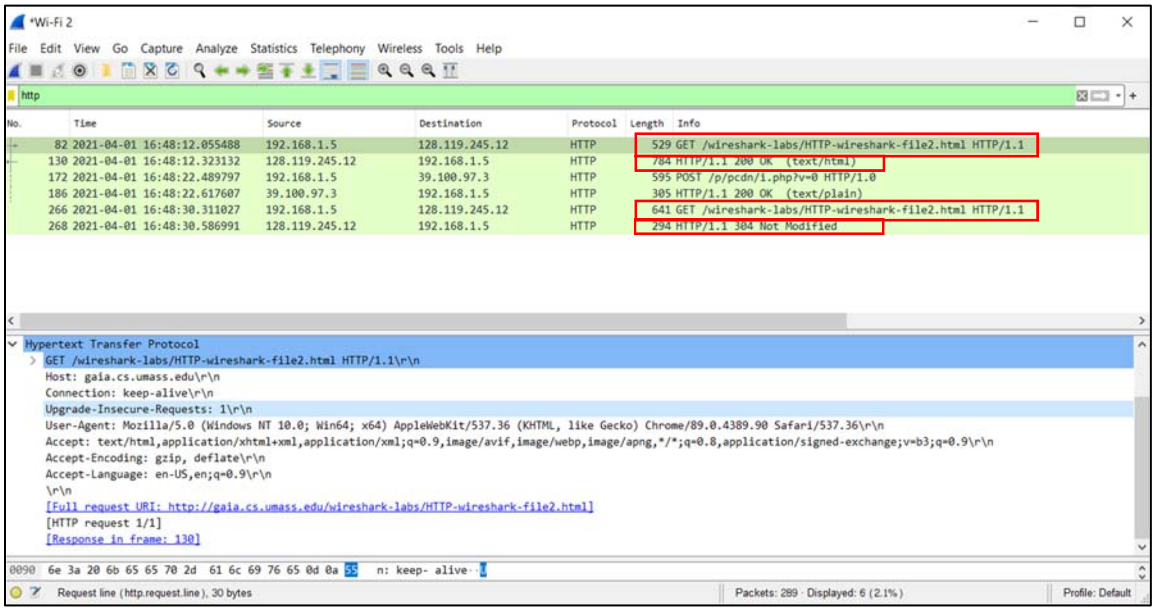
For the next series of question do the following:

- Start up your web browser.
- Empty the browser's cache (clear recent history on your browser; no information of webpages opened should be stored on your pc).
- Start up the Wireshark packet Sniffer, and start the packet capture.
- Enter the following URL into your browser

  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

  (Your browser should display a very simple five-line HTML file.)

- Quickly enter the same URL into your browser again (or simply refresh the page on your browser)
- Stop Wireshark packet capture, and enter "http" in the display-filter, so that only captured HTTP messages will be displayed later in the packet-listing window.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time                        Source           Destination      Protocol  Length  Info
   82 2021-04-01 16:48:12.055488   192.168.1.5      128.119.245.12   HTTP       529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  130 2021-04-01 16:48:12.323132   128.119.245.12   192.168.1.5      HTTP       784 HTTP/1.1 200 OK  (text/html)
  172 2021-04-01 16:48:22.489797   192.168.1.5      39.100.97.3      HTTP       595 POST /p/pcdn/i.php?v=0 HTTP/1.0
  186 2021-04-01 16:48:22.617607   39.100.97.3      192.168.1.5      HTTP       305 HTTP/1.1 200 OK  (text/plain)
  266 2021-04-01 16:48:30.311027   192.168.1.5      128.119.245.12   HTTP       641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  268 2021-04-01 16:48:30.586991   128.119.245.12   192.168.1.5      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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 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 1/1]
    [Response in frame: 130]
```

```
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
```

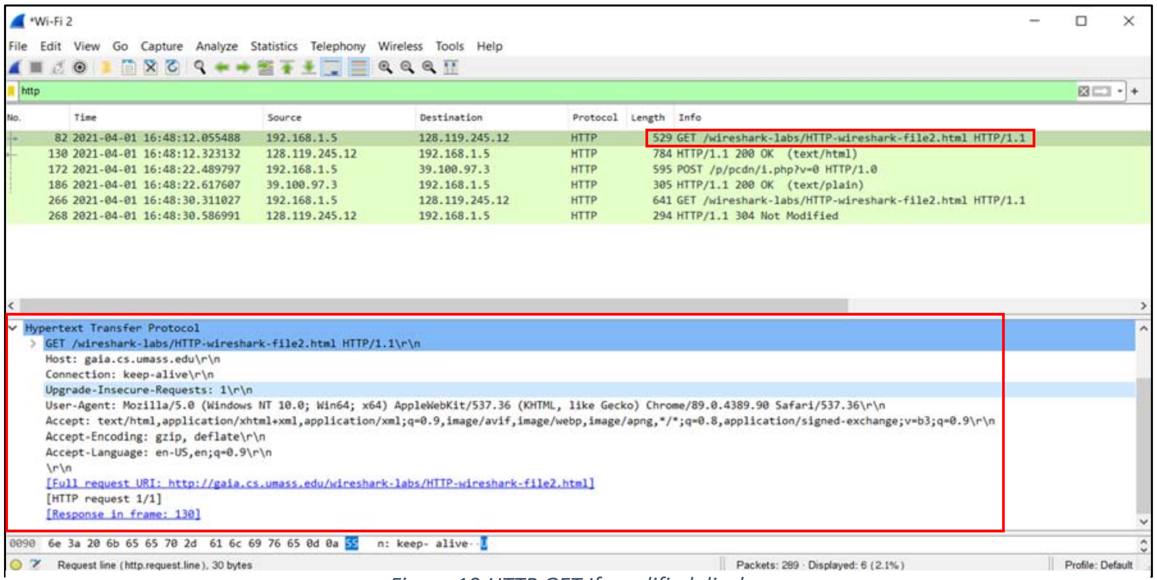
```
Request line (http.request.line), 30 bytes        Packets: 289 · Displayed: 6 (2.1%)        Profile: Default
```

Figure 9:Wireshark Display after the second link that we put into browser

As shown in the figure we will get two **HTTP GET** request, one from the first time we enter the URL with the respective **200 OK** response message and the second **HTTP GET** from refreshing the page (or reentering the URL) with a **304 Not Modified** response message.

Answer the following questions:

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?
    - NO, As you can see in the figure below there is no line with “**IF-MODIFIED-SINCE**” in the Packet-headers details of the **HTTP GET** request. This is because we are looking at the first **HTTP GET** request and our browser didn’t not have any previous data about the URL we opened.



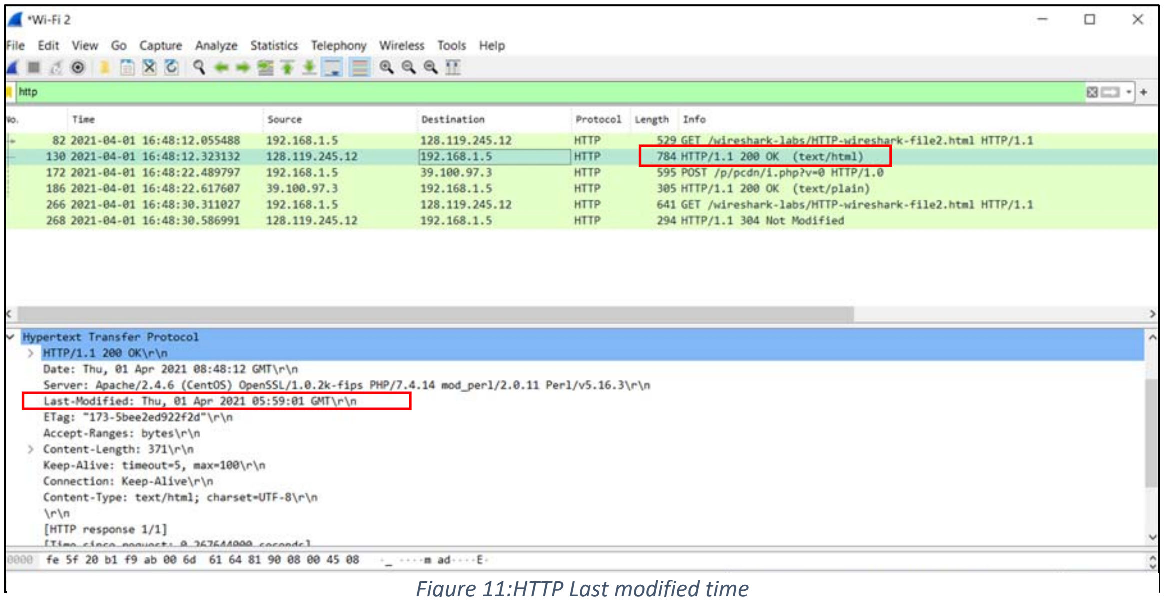
```
No.   Time                        Source          Destination     Protocol  Length  Info
  82 2021-04-01 16:48:12.055488   192.168.1.5     128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 130 2021-04-01 16:48:12.323132   128.119.245.12  192.168.1.5     HTTP      784 HTTP/1.1 200 OK  (text/html)
 172 2021-04-01 16:48:22.489797   192.168.1.5     39.100.97.3     HTTP      595 POST /p/pcdn/i.php?v=0 HTTP/1.0
 186 2021-04-01 16:48:22.617607   39.100.97.3     192.168.1.5     HTTP      305 HTTP/1.1 200 OK  (text/plain)
 266 2021-04-01 16:48:30.311027   192.168.1.5     128.119.245.12  HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 268 2021-04-01 16:48:30.586991   128.119.245.12  192.168.1.5     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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 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 1/1]
    [Response in frame: 130]
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
Request line (http.request.line), 30 bytes          Packets: 289 · Displayed: 6 (2.1%)          Profile: Default
```

*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

Figure 10:HTTP GET If-modified display

9) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
    - We can tell the server returned the content of the file because as shown in the figure we can see the content of the last modified time message in the Packet-header details window.



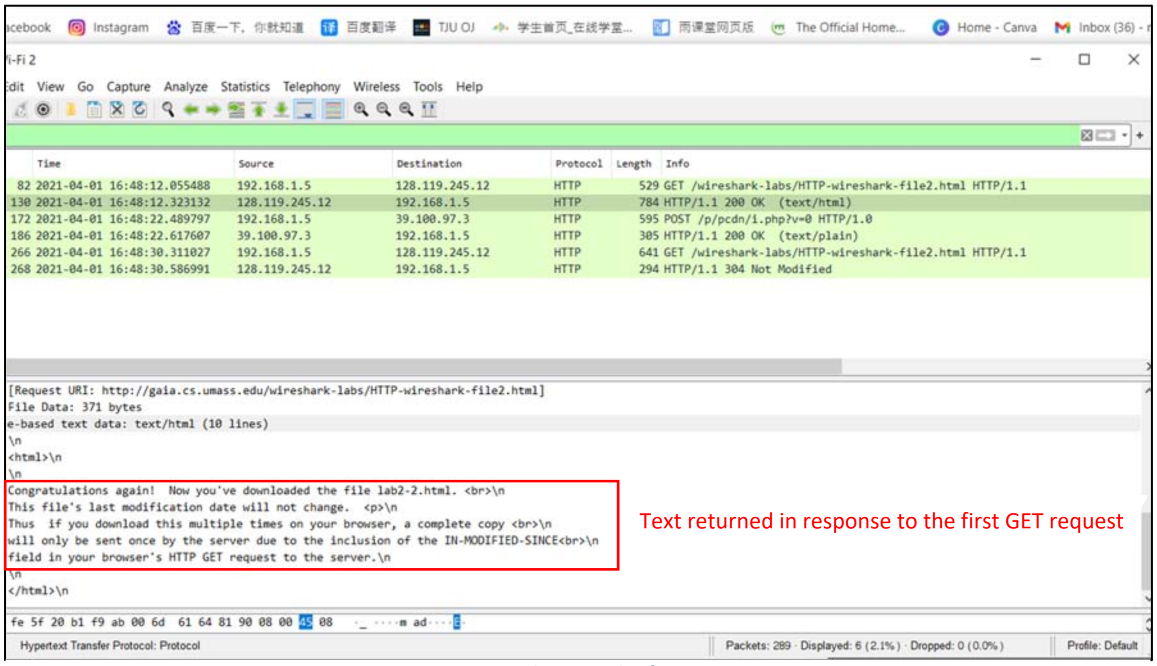
```
No.   Time                        Source          Destination     Protocol  Length  Info
  82 2021-04-01 16:48:12.055488   192.168.1.5     128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 130 2021-04-01 16:48:12.323132   128.119.245.12  192.168.1.5     HTTP      784 HTTP/1.1 200 OK  (text/html)
 172 2021-04-01 16:48:22.489797   192.168.1.5     39.100.97.3     HTTP      595 POST /p/pcdn/i.php?v=0 HTTP/1.0
 186 2021-04-01 16:48:22.617607   39.100.97.3     192.168.1.5     HTTP      305 HTTP/1.1 200 OK  (text/plain)
 266 2021-04-01 16:48:30.311027   192.168.1.5     128.119.245.12  HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 268 2021-04-01 16:48:30.586991   128.119.245.12  192.168.1.5     HTTP      294 HTTP/1.1 304 Not Modified
```

```
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 01 Apr 2021 08:48:12 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 01 Apr 2021 05:59:01 GMT\r\n
    ETag: "173-5bee2ed922f2d"\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 1/1]
0000  fe 5f 20 b1 f9 ab 00 6d  61 64 81 90 08 00 45 08   ·_ ····m ad····E·
```

*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

Figure 11:HTTP Last modified time

In the other hand, We also can see the returned message from the second link that we have been retrieved in the browser base on Line-based text data in the figure below.



```
    Time                        Source            Destination       Protocol  Length  Info
 82 2021-04-01 16:48:12.055488  192.168.1.5       128.119.245.12    HTTP      529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
130 2021-04-01 16:48:12.323132  128.119.245.12    192.168.1.5       HTTP      784 HTTP/1.1 200 OK  (text/html)
172 2021-04-01 16:48:22.489797  192.168.1.5       39.100.97.3       HTTP      595 POST /p/pcdn/i.php?v=0 HTTP/1.0
186 2021-04-01 16:48:22.617607  39.100.97.3       192.168.1.5       HTTP      305 HTTP/1.1 200 OK  (text/plain)
266 2021-04-01 16:48:30.311027  192.168.1.5       128.119.245.12    HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
268 2021-04-01 16:48:30.586991  128.119.245.12    192.168.1.5       HTTP      294 HTTP/1.1 304 Not Modified

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
e-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

fe 5f 20 b1 f9 ab 00 6d  61 64 81 90 08 00 45 08   ·_ ····m ad····E·
```

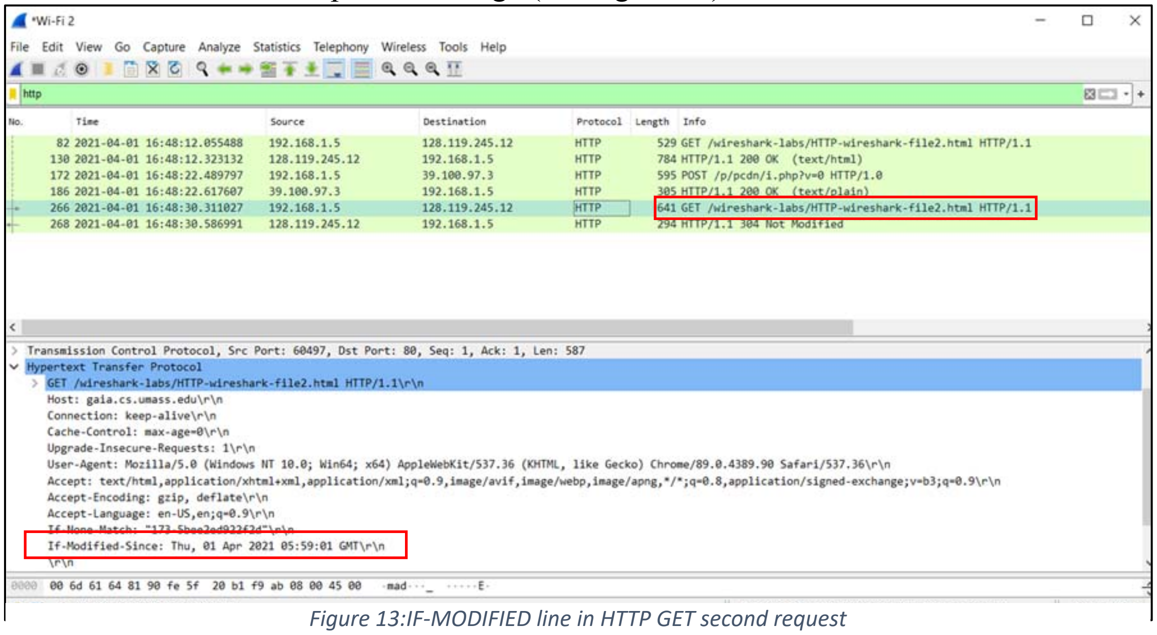
Text returned in response to the first GET request

acebook
Instagram
百度一下，你就知道
百度翻译
TJU OJ
学生首页_在线学堂...
雨课堂网页版
The Official Home...
Home - Canva
Inbox (36)
i-Fi 2
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Hypertext Transfer Protocol: Protocol
Packets: 289 · Displayed: 6 (2.1%) · Dropped: 0 (0.0%)
Profile: Default

Figure 12:Returned text in the first GET request

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?

- As shown in the figure on the second **HTTP GET** request we could find the "**IF-MODIFIED-SINCE**" line. This line is followed by "**Thu, 01 Apr 2021 05:59:01 GMT**" Which is the date shown in the "**Last-Modified**" field of the first HTTP response message (See figure 12).

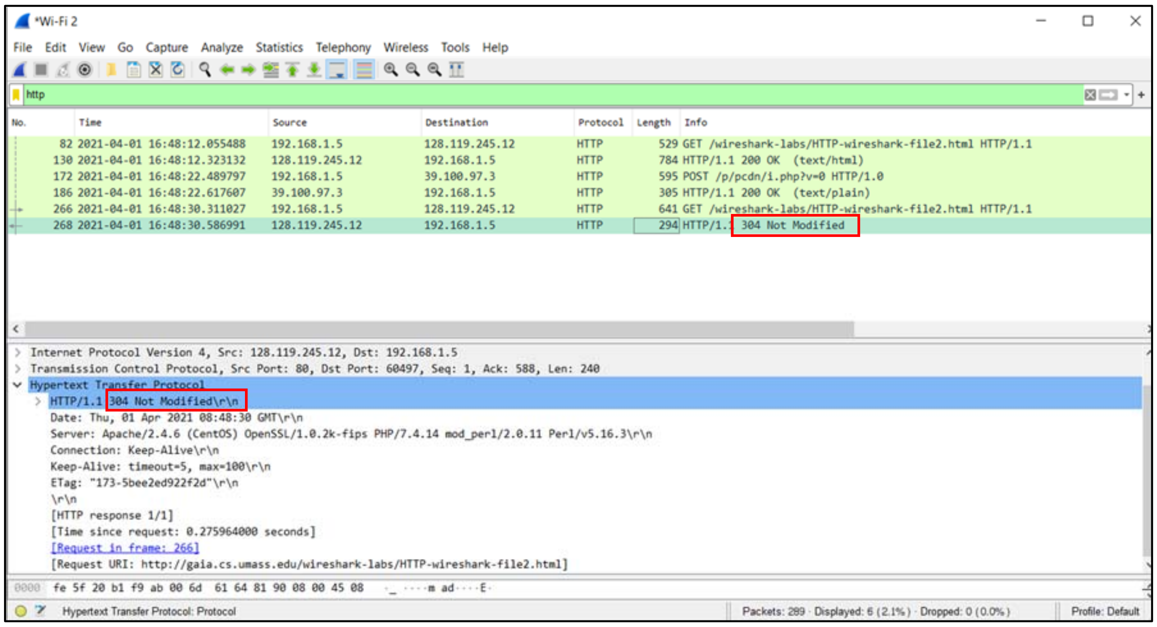


```
No.    Time                        Source            Destination       Protocol  Length  Info
    82 2021-04-01 16:48:12.055488  192.168.1.5       128.119.245.12    HTTP      529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   130 2021-04-01 16:48:12.323132  128.119.245.12    192.168.1.5       HTTP      784 HTTP/1.1 200 OK  (text/html)
   172 2021-04-01 16:48:22.489797  192.168.1.5       39.100.97.3       HTTP      595 POST /p/pcdn/i.php?v=0 HTTP/1.0
   186 2021-04-01 16:48:22.617607  39.100.97.3       192.168.1.5       HTTP      305 HTTP/1.1 200 OK  (text/plain)
   266 2021-04-01 16:48:30.311027  192.168.1.5       128.119.245.12    HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   268 2021-04-01 16:48:30.586991  128.119.245.12    192.168.1.5       HTTP      294 HTTP/1.1 304 Not Modified

> Transmission Control Protocol, Src Port: 60497, Dst Port: 80, Seq: 1, Ack: 1, Len: 587
v 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/89.0.4389.90 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: "173-5bee2ed922f2d"\r\n
    If-Modified-Since: Thu, 01 Apr 2021 05:59:01 GMT\r\n
    \r\n

0000  00 6d 61 64 81 90 fe 5f  20 b1 f9 ab 08 00 45 00   ·mad···_ ·····E·
```

*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

Figure 13:IF-MODIFIED line in HTTP GET second request

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.
    - We can see in the figure that the Status Code is **304 Not Modified**. In this case the server didn't return the content because the browser already had it from its cache.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time                        Source          Destination     Protocol Length Info
   82 2021-04-01 16:48:12.055488  192.168.1.5     128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  130 2021-04-01 16:48:12.323132  128.119.245.12  192.168.1.5     HTTP      784 HTTP/1.1 200 OK  (text/html)
  172 2021-04-01 16:48:22.489797  192.168.1.5     39.100.97.3     HTTP      595 POST /p/pcdn/i.php?v=0 HTTP/1.0
  186 2021-04-01 16:48:22.617607  39.100.97.3     192.168.1.5     HTTP      305 HTTP/1.1 200 OK  (text/plain)
  266 2021-04-01 16:48:30.311027  192.168.1.5     128.119.245.12  HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  268 2021-04-01 16:48:30.586991  128.119.245.12  192.168.1.5     HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 60497, Seq: 1, Ack: 588, Len: 240
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Thu, 01 Apr 2021 08:48:30 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 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: "173-5bee2ed922f2d"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.275964000 seconds]
    [Request in frame: 266]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0000  fe 5f 20 b1 f9 ab 00 6d  61 64 81 90 08 00 45 08   ·_ ····m ad····E·
```

Hypertext Transfer Protocol: Protocol
Packets: 289 · Displayed: 6 (2.1%) · Dropped: 0 (0.0%)
Profile: Default

Figure 14:HTTP status code 304 Not Modified

3. Retrieving Long Documents

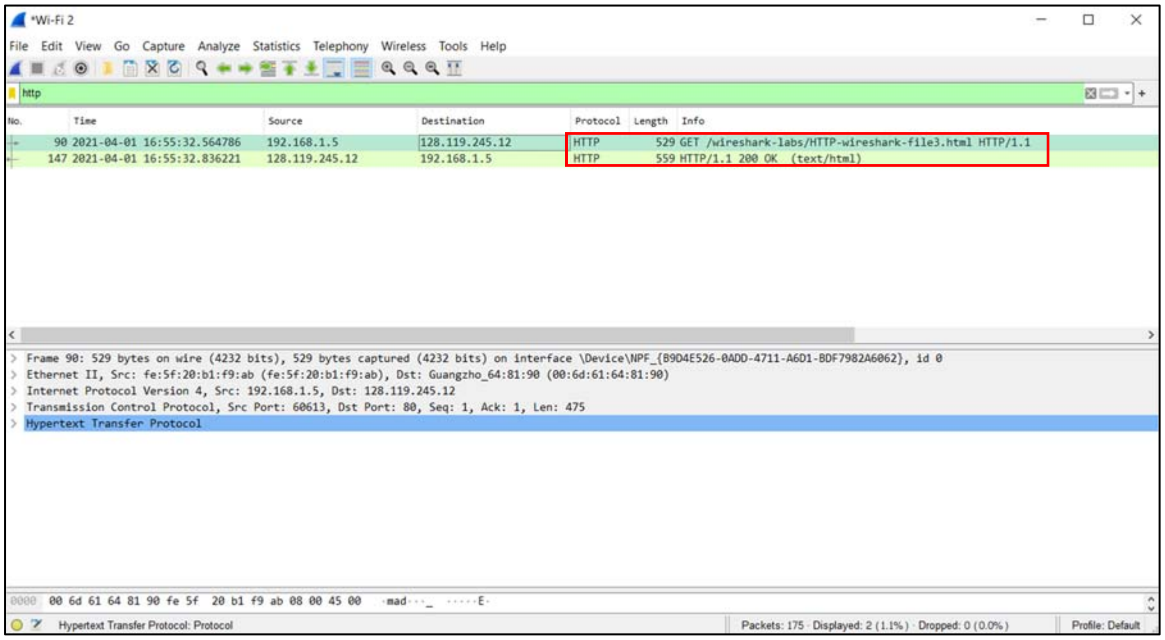
In previous questions, the documents retrieved have been simple and short HTML files. In the next series of question you will see what happens when we download a long HTML file. Do the following:

- Start up your web browser, and make sure your browser's cache is cleared.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser

  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

  Your browser should display the rather lengthy US Bill of Rights.

- Stop Wireshark packet capture, and enter "http" in the display-filter-specification window.

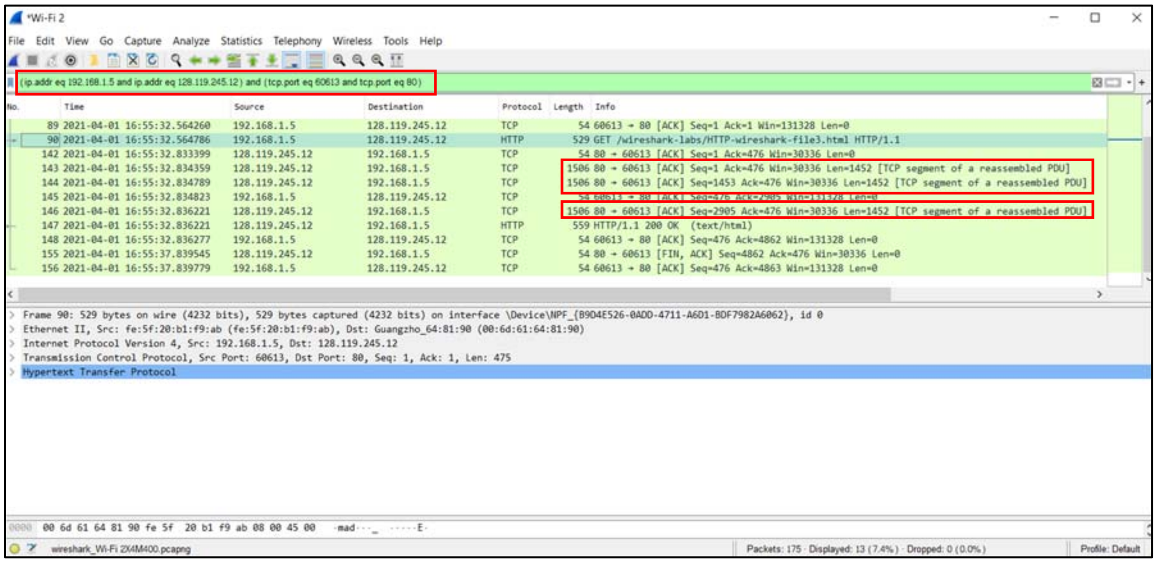


```
http

No.   Time                        Source          Destination     Protocol Length Info
   90 2021-04-01 16:55:32.564786  192.168.1.5     128.119.245.12  HTTP     529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  147 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     HTTP     559 HTTP/1.1 200 OK  (text/html)

> Frame 90: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab), Dst: Guangzho_64:81:90 (00:6d:61:64:81:90)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60613, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
> Hypertext Transfer Protocol

0000  00 6d 61 64 81 90 fe 5f  20 b1 f9 ab 08 00 45 00   ·mad···_ ·····E·

Hypertext Transfer Protocol: Protocol    Packets: 175 · Displayed: 2 (1.1%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 15:Wireshark Display after the third link that we put into browser

In the packet-listing window, I could see my **HTTP GET** message, followed by a multiple-packet **TCP** response to your **HTTP GET** request in the *figure 16* below.

By entering http on the display-filter I just got the **HTTP GET** request and the response. To see the **TCP** responses right-click one of the packets select Conversation Filter and then select **TCP**. After that we will see the **TCP** and **HTTP** respond in the figure below.



```
(ip.addr eq 192.168.1.5 and ip.addr eq 128.119.245.12) and (tcp.port eq 60613 and tcp.port eq 80)

No.   Time                        Source          Destination     Protocol Length Info
   89 2021-04-01 16:55:32.564260  192.168.1.5     128.119.245.12  TCP       54 60613 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   90 2021-04-01 16:55:32.564786  192.168.1.5     128.119.245.12  HTTP     529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  142 2021-04-01 16:55:32.833399  128.119.245.12  192.168.1.5     TCP       54 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=0
  143 2021-04-01 16:55:32.834359  128.119.245.12  192.168.1.5     TCP     1506 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
  144 2021-04-01 16:55:32.834789  128.119.245.12  192.168.1.5     TCP     1506 80 → 60613 [ACK] Seq=1453 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
  145 2021-04-01 16:55:32.834823  192.168.1.5     128.119.245.12  TCP       54 60613 → 80 [ACK] Seq=476 Ack=2905 Win=131328 Len=0
  146 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     TCP     1506 80 → 60613 [ACK] Seq=2905 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
  147 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     HTTP     559 HTTP/1.1 200 OK  (text/html)
  148 2021-04-01 16:55:32.836277  192.168.1.5     128.119.245.12  TCP       54 60613 → 80 [ACK] Seq=476 Ack=4862 Win=131328 Len=0
  155 2021-04-01 16:55:37.839545  128.119.245.12  192.168.1.5     TCP       54 80 → 60613 [FIN, ACK] Seq=4862 Ack=476 Win=30336 Len=0
  156 2021-04-01 16:55:37.839779  192.168.1.5     128.119.245.12  TCP       54 60613 → 80 [ACK] Seq=476 Ack=4863 Win=131328 Len=0

> Frame 90: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab), Dst: Guangzho_64:81:90 (00:6d:61:64:81:90)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60613, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
> Hypertext Transfer Protocol

0000  00 6d 61 64 81 90 fe 5f  20 b1 f9 ab 08 00 45 00   ·mad···_ ·····E·

wireshark_Wi-Fi 2X4M400.pcapng    Packets: 175 · Displayed: 13 (7.4%) · Dropped: 0 (0.0%)    Profile: Default
```

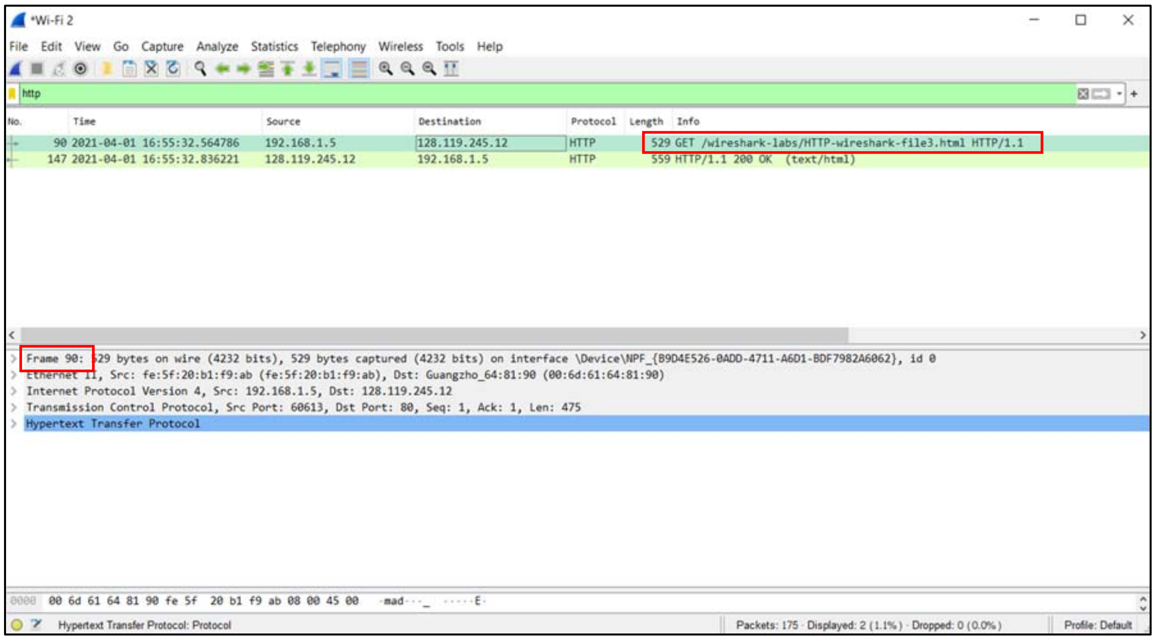
Figure 16:TCP responded message

There are multiple **TCP** packets because the HTML file is very long, 4500 bytes which is too large to fit in one **TCP** packet. Therefore, the HTTP response message is broken into several parts, with each part being contained within a separate **TCP** segment.

As you can see, Wireshark indicates each **TCP** segment as a separate packet, and the fact that the single **HTTP** response was fragmented across multiple **TCP** packets is indicated by the "**TCP segment of a reassembled PDU**" in the Info column of the Wireshark display.

Now we have to answer the following question:

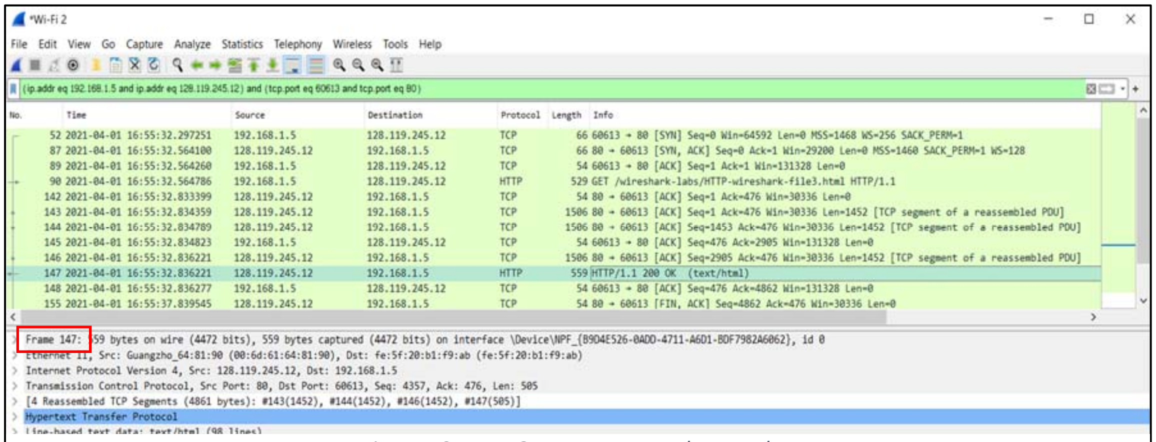
12) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
    - There is only one **HTTP GET** request. As we can see the **HTTP GET** request was capture on frame 90.



```
http

No.   Time                        Source          Destination     Protocol Length Info
   90 2021-04-01 16:55:32.564786  192.168.1.5     128.119.245.12  HTTP     529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  147 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     HTTP     559 HTTP/1.1 200 OK  (text/html)

> Frame 90: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab), Dst: Guangzho_64:81:90 (00:6d:61:64:81:90)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60613, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
> Hypertext Transfer Protocol

0000  00 6d 61 64 81 90 fe 5f  20 b1 f9 ab 08 00 45 00   ·mad···_ ·····E·

Hypertext Transfer Protocol: Protocol          Packets: 175 · Displayed: 2 (1.1%) · Dropped: 0 (0.0%)     Profile: Default
```

Figure 17:HTTP GET request frame

13) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    - Packet number (frame) **147**.

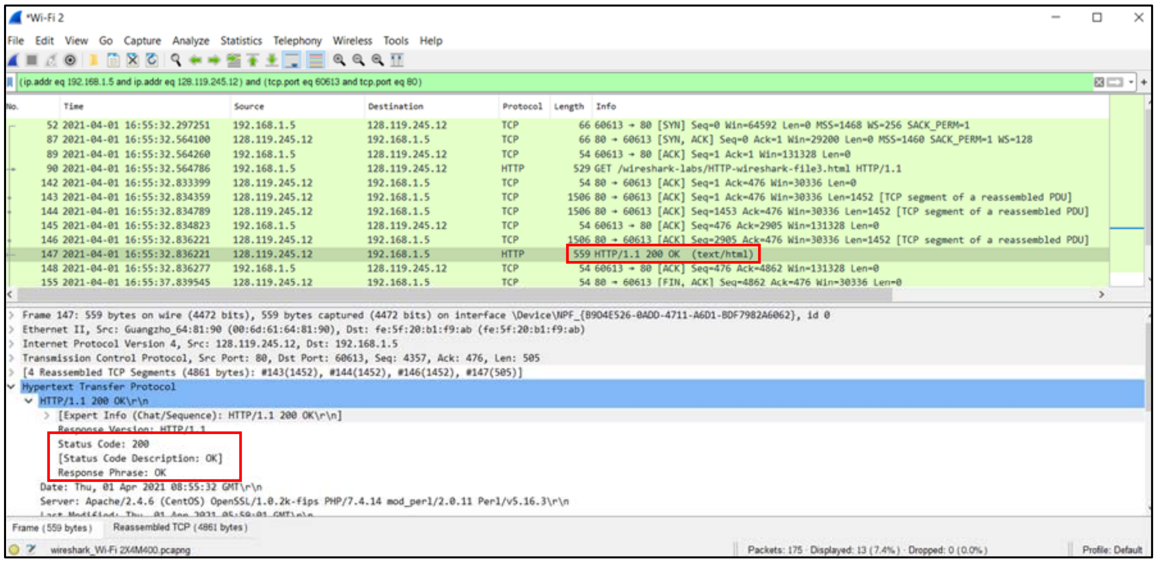


```
(ip.addr eq 192.168.1.5 and ip.addr eq 128.119.245.12) and (tcp.port eq 60613 and tcp.port eq 80)

No.   Time                        Source          Destination     Protocol Length Info
   52 2021-04-01 16:55:32.297251  192.168.1.5     128.119.245.12  TCP        66 60613 → 80 [SYN] Seq=0 Win=64592 Len=0 MSS=1468 WS=256 SACK_PERM=1
   87 2021-04-01 16:55:32.564100  128.119.245.12  192.168.1.5     TCP        66 80 → 60613 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
   89 2021-04-01 16:55:32.564260  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   90 2021-04-01 16:55:32.564786  192.168.1.5     128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  142 2021-04-01 16:55:32.833399  128.119.245.12  192.168.1.5     TCP        54 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=0
  143 2021-04-01 16:55:32.834359  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
  144 2021-04-01 16:55:32.834789  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=1453 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
  145 2021-04-01 16:55:32.834823  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=476 Ack=2905 Win=131328 Len=0
  146 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=2905 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
  147 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     HTTP      559 HTTP/1.1 200 OK  (text/html)
  148 2021-04-01 16:55:32.836277  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=476 Ack=4862 Win=131328 Len=0
  155 2021-04-01 16:55:37.839545  128.119.245.12  192.168.1.5     TCP        54 80 → 60613 [FIN, ACK] Seq=4862 Ack=476 Win=30336 Len=0

> Frame 147: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{B9D4E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: Guangzho_64:81:90 (00:6d:61:64:81:90), Dst: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 60613, Seq: 4357, Ack: 476, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #143(1452), #144(1452), #146(1452), #147(505)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

Figure 18:HTTP GET response packet number

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

- The Status Code and phrase in the response is **200 OK**.

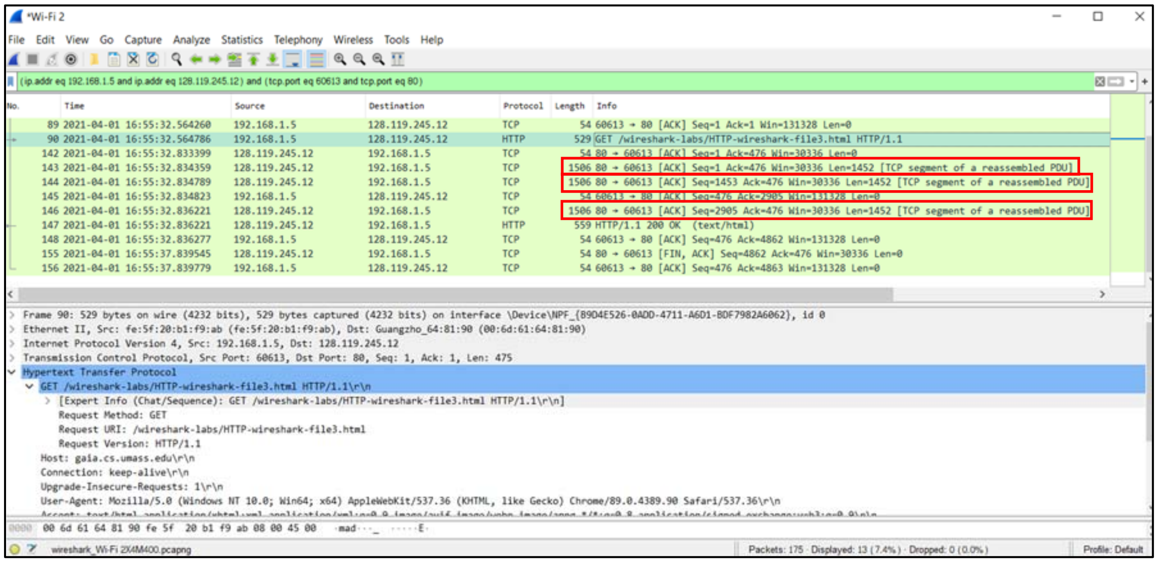


```
(ip.addr eq 192.168.1.5 and ip.addr eq 128.119.245.12) and (tcp.port eq 60613 and tcp.port eq 80)

No.  Time                        Source          Destination     Protocol Length Info
 52 2021-04-01 16:55:32.297251  192.168.1.5     128.119.245.12  TCP        66 60613 → 80 [SYN] Seq=0 Win=64592 Len=0 MSS=1468 WS=256 SACK_PERM=1
 87 2021-04-01 16:55:32.564100  128.119.245.12  192.168.1.5     TCP        66 80 → 60613 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 89 2021-04-01 16:55:32.564260  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 90 2021-04-01 16:55:32.564786  192.168.1.5     128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
142 2021-04-01 16:55:32.833399  128.119.245.12  192.168.1.5     TCP        54 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=0
143 2021-04-01 16:55:32.834359  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
144 2021-04-01 16:55:32.834789  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=1453 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
145 2021-04-01 16:55:32.834823  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=476 Ack=2905 Win=131328 Len=0
146 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=2905 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
147 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     HTTP      559 HTTP/1.1 200 OK  (text/html)
148 2021-04-01 16:55:32.836277  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=476 Ack=4862 Win=131328 Len=0
155 2021-04-01 16:55:37.839545  128.119.245.12  192.168.1.5     TCP        54 80 → 60613 [FIN, ACK] Seq=4862 Ack=476 Win=30336 Len=0

> Frame 147: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{8904E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: Guangzho_64:81:90 (00:6d:61:64:81:90), Dst: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 60613, Seq: 4357, Ack: 476, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #143(1452), #144(1452), #146(1452), #147(505)]
v Hypertext Transfer Protocol
  v 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: Thu, 01 Apr 2021 08:55:32 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n

Frame (559 bytes)   Reassembled TCP (4861 bytes)
wireshark_Wi-Fi 2X4M400.pcapng     Packets: 175 · Displayed: 13 (7.4%) · Dropped: 0 (0.0%)     Profile: Default
```

Figure 19:Status code and response

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

- There are 3 packets data-containing with the "**TCP segment of a reassembled PDU**" indication that needed to carry the single HTTP response.



```
(ip.addr eq 192.168.1.5 and ip.addr eq 128.119.245.12) and (tcp.port eq 60613 and tcp.port eq 80)

No.  Time                        Source          Destination     Protocol Length Info
 89 2021-04-01 16:55:32.564260  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 90 2021-04-01 16:55:32.564786  192.168.1.5     128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
142 2021-04-01 16:55:32.833399  128.119.245.12  192.168.1.5     TCP        54 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=0
143 2021-04-01 16:55:32.834359  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=1 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
144 2021-04-01 16:55:32.834789  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=1453 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
145 2021-04-01 16:55:32.834823  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=476 Ack=2905 Win=131328 Len=0
146 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     TCP      1506 80 → 60613 [ACK] Seq=2905 Ack=476 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
147 2021-04-01 16:55:32.836221  128.119.245.12  192.168.1.5     HTTP      559 HTTP/1.1 200 OK  (text/html)
148 2021-04-01 16:55:32.836277  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=476 Ack=4862 Win=131328 Len=0
155 2021-04-01 16:55:37.839545  128.119.245.12  192.168.1.5     TCP        54 80 → 60613 [FIN, ACK] Seq=4862 Ack=476 Win=30336 Len=0
156 2021-04-01 16:55:37.839779  192.168.1.5     128.119.245.12  TCP        54 60613 → 80 [ACK] Seq=476 Ack=4863 Win=131328 Len=0

> Frame 90: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{8904E526-0ADD-4711-A6D1-BDF7982A6062}, id 0
> Ethernet II, Src: fe:5f:20:b1:f9:ab (fe:5f:20:b1:f9:ab), Dst: Guangzho_64:81:90 (00:6d:61:64:81:90)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60613, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.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/89.0.4389.90 Safari/537.36\r\n

0000  00 6d 61 64 81 90 fe 5f  20 b1 f9 ab 08 00 45 00   ·mad···_ ······E·
wireshark_Wi-Fi 2X4M400.pcapng     Packets: 175 · Displayed: 13 (7.4%) · Dropped: 0 (0.0%)     Profile: Default
```

Figure 20:Data containing TCP segments