Wireshark Lab #2, HTTP

He Tianyang, 3022001441

September 28, 2024

Problem 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?**

Solutions:

The http version of my browser can be found in the HTTP GET request. The version of the server can be found in the HTTP OK reply. The details are shown in the Fig. 1 and Fig. 2. **It shows that the browser is running HTTP version 1.1, and the server is running HTTP version 1.1.**

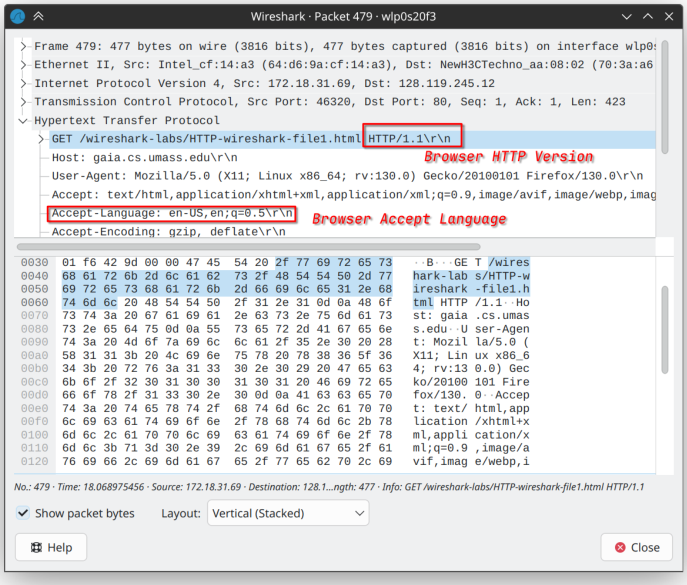
Question 2:

> **What language (if any) does your browser indicate that it can accept to the server?**

Also, inspect the `GET` request, and the `Accept-Language` field in `HTTP Headers` is shown in Fig. 1. **The browser indicates that it can accept `en-US, en` language to the server.**

Question 3:

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



```
> Frame 479: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface wlp0s
> Ethernet II, Src: Intel_cf:14:a3 (64:d6:9a:cf:14:a3), Dst: NewH3CTechno_aa:08:02 (70:3a:a6
> Internet Protocol Version 4, Src: 172.18.31.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 46320, Dst Port: 80, Seq: 1, Ack: 1, Len: 423
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

Browser HTTP Version

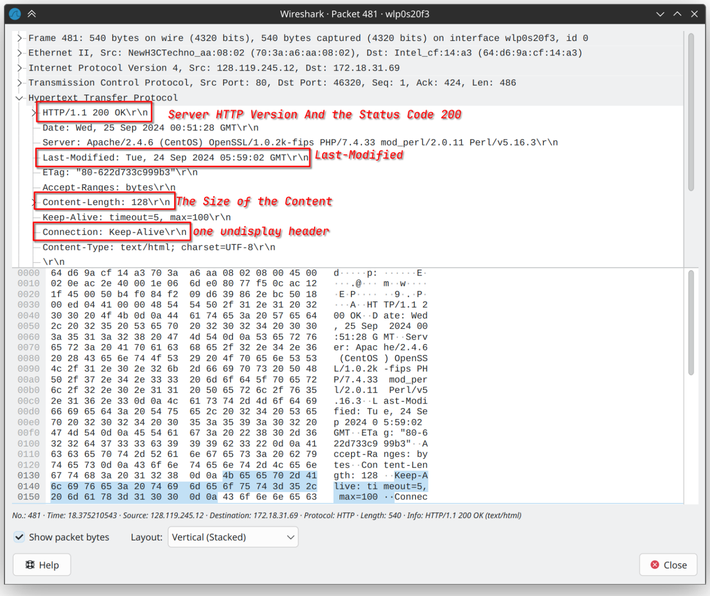
Browser Accept Language

```
0030  01 f6 42 9d 00 00 47 45  54 20 2f 77 69 72 65 73   ··B···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 31 2e 68   ireshark -file1.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 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  58 31 31 3b 20 4c 69 6e  75 78 20 78 38 36 5f 36   X11; Lin ux x86_6
00b0  34 3b 20 72 76 3a 31 33  30 2e 30 29 20 47 65 63   4; rv:13 0.0) Gec
00c0  6b 6f 2f 32 30 31 30 30  31 30 31 20 46 69 72 65   ko/20100 101 Fire
00d0  66 6f 78 2f 31 33 30 2e  30 0d 0a 41 63 63 65 70   fox/130. 0··Accep
00e0  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
00f0  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0100  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0110  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
0120  76 69 66 2c 69 6d 61 67  65 2f 77 65 62 70 2c 69   vif,imag e/webp,i
```

```
No.: 479 · Time: 18.068975456 · Source: 172.18.31.69 · Destination: 128.1...ngth: 477 · Info: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
```

Layout: Vertical (Stacked)

Figure 1: The HTTP version of the browser



```
> Frame 481: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface wlp0s20f3, id 0
> Ethernet II, Src: NewH3CTechno_aa:08:02 (70:3a:a6:aa:08:02), Dst: Intel_cf:14:a3 (64:d6:9a:cf:14:a3)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.31.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 46320, Seq: 1, Ack: 424, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 25 Sep 2024 00:51:28 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: Tue, 24 Sep 2024 05:59:02 GMT\r\n
    ETag: "80-622d733c999b3"\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
```

Server HTTP Version And the Status Code 200

Last-Modified

The Size of the Content

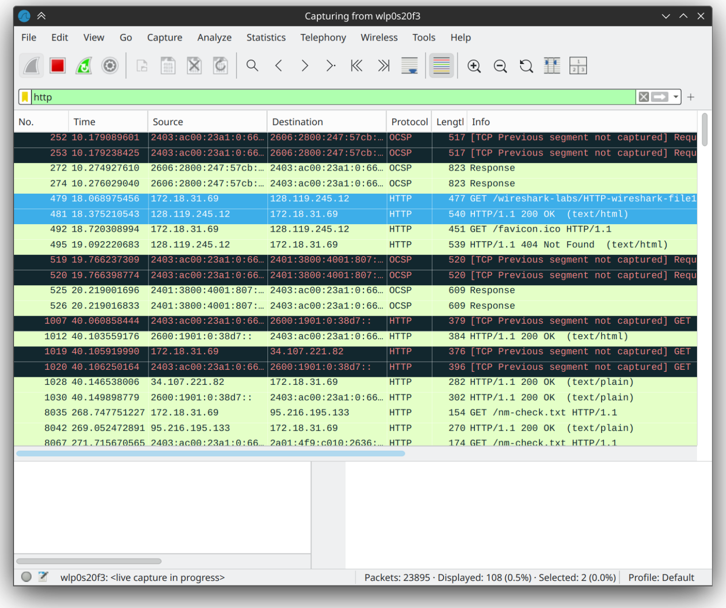
one undisplay header

```
0000  64 d6 9a cf 14 a3 70 3a  a6 aa 08 02 08 00 45 00   d·····p: ······E·
0010  02 0e ac 2e 40 00 1e 06  6d e0 80 77 f5 0c ac 12   ····.@·· m··w····
0020  1f 45 00 50 b4 f0 84 f2  09 d6 39 86 2e bc 50 18   ·E·P···· ··9·.·P·
0030  00 ed 04 41 00 00 48 54  54 50 2f 31 2e 31 20 32   ···A··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 57 65 64   00 OK··D ate: Wed
0050  2c 20 32 35 20 53 65 70  20 32 30 32 34 20 30 30   , 25 Sep  2024 00
0060  3a 35 31 3a 32 38 20 47  4d 54 0d 0a 53 65 72 76   :51:28 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 54 75  65 2c 20 32 34 20 53 65   fied: Tu e, 24 Se
00e0  70 20 32 30 32 34 20 30  35 3a 35 39 3a 30 32 20   p 2024 0 5:59:02
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 36   GMT··ETa g: "80-6
0100  32 32 64 37 33 33 63 39  39 39 62 33 22 0d 0a 41   22d733c9 99b3"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
```

```
No.: 481 · Time: 18.375210543 · Source: 128.119.245.12 · Destination: 172.18.31.69 · Protocol: HTTP · Length: 540 · Info: HTTP/1.1 200 OK (text/html)
```

Layout: Vertical (Stacked)

Figure 2: The HTTP version of the server



http

No.	Time	Source	Destination	Protocol	Lengtl	Info
252	10.179089601	2403:ac00:23a1:0:66…	2606:2800:247:57cb:…	OCSP	517	[TCP Previous segment not captured] Requ
253	10.179238425	2403:ac00:23a1:0:66…	2606:2800:247:57cb:…	OCSP	517	[TCP Previous segment not captured] Requ
272	10.274927610	2606:2800:247:57cb:…	2403:ac00:23a1:0:66…	OCSP	823	Response
274	10.276029040	2606:2800:247:57cb:…	2403:ac00:23a1:0:66…	OCSP	823	Response
479	18.068975456	172.18.31.69	128.119.245.12	HTTP	477	GET /wireshark-labs/HTTP-wireshark-file1
481	18.375210543	128.119.245.12	172.18.31.69	HTTP	540	HTTP/1.1 200 OK (text/html)
492	18.720308994	172.18.31.69	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
495	19.092220683	128.119.245.12	172.18.31.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)
519	19.766237309	2403:ac00:23a1:0:66…	2401:3800:4001:807:…	OCSP	520	[TCP Previous segment not captured] Requ
520	19.766398774	2403:ac00:23a1:0:66…	2401:3800:4001:807:…	OCSP	520	[TCP Previous segment not captured] Requ
525	20.219001696	2401:3800:4001:807:…	2403:ac00:23a1:0:66…	OCSP	609	Response
526	20.219016833	2401:3800:4001:807:…	2403:ac00:23a1:0:66…	OCSP	609	Response
1007	40.060858444	2403:ac00:23a1:0:66…	2600:1901:0:38d7::	HTTP	379	[TCP Previous segment not captured] GET
1012	40.103559176	2600:1901:0:38d7::	2403:ac00:23a1:0:66…	HTTP	384	HTTP/1.1 200 OK (text/html)
1019	40.105919990	172.18.31.69	34.107.221.82	HTTP	376	[TCP Previous segment not captured] GET
1020	40.106250164	2403:ac00:23a1:0:66…	2600:1901:0:38d7::	HTTP	396	[TCP Previous segment not captured] GET
1028	40.146538006	34.107.221.82	172.18.31.69	HTTP	282	HTTP/1.1 200 OK (text/plain)
1030	40.149898779	2600:1901:0:38d7::	2403:ac00:23a1:0:66…	HTTP	302	HTTP/1.1 200 OK (text/plain)
8035	268.747751227	172.18.31.69	95.216.195.133	HTTP	154	GET /nm-check.txt HTTP/1.1
8042	269.052472891	95.216.195.133	172.18.31.69	HTTP	270	HTTP/1.1 200 OK (text/plain)
8067	271.715670565	2403:ac00:23a1:0:66…	2a01:4f9:c010:2636:…	HTTP	174	GET /nm-check.txt HTTP/1.1

wlp0s20f3: <live capture in progress>   Packets: 23895 · Displayed: 108 (0.5%) · Selected: 2 (0.0%)   Profile: Default

Figure 3: The IP address of the computer and the server

Inspect the `GET` request, and looking for the `source` and the `destination` IP address. The details are shown in the Fig. 3. **The IP address of my computer is `172.18.31.69` and the IP address of the server is `128.119.245.12`.**

Question 4:

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

Inspect the `HTTP OK` reply, and the `Status Code` field in `HTTP` is shown in Fig. 2. **The status code returned from the server to the browser is `200 OK`.**

Question 5:

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

Inspect the `HTTP OK` reply, and the `Last-Modified` field in `HTTP` is shown in Fig. 2. **The HTML file was last modified on the server on `Tue, 24 Sep 2024 05:59:02 GMT`.**

Question 6:

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

Inspect the HTTP OK reply, and the Content-Length field in HTTP is shown in Fig. 2. **The number of bytes of content being returned to the browser is 128.**

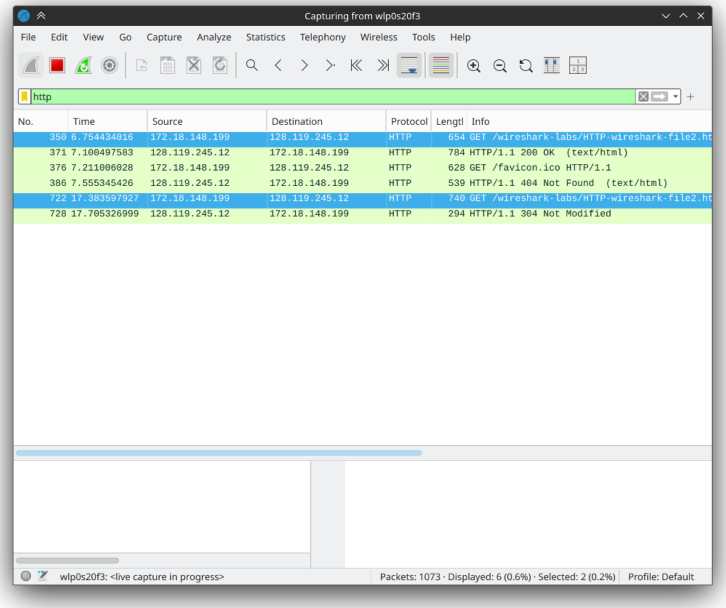
Question 7:

> **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?**

Inspect the HTTP OK reply, and the Raw field in HTTP is shown in Fig. 2. **Yes, there are headers within the data that are not displayed in the packet-listing window. For example:** `Content-Type: text/html; charset=UTF-8`, `Connection: keep-alive`, **etc.**

Problem 2. The HTTP CONDITIONAL GET/response

Follow the instructions, open the target URL in the browser, and inspect the HTTP GET request and the HTTP OK reply. The results are shown in Fig. 4.



http

No.	Time	Source	Destination	Protocol	Lengtl	Info
350	6.754434016	172.18.148.199	128.119.245.12	HTTP	654	GET /wireshark-labs/HTTP-wireshark-file2.ht
371	7.100497583	128.119.245.12	172.18.148.199	HTTP	784	HTTP/1.1 200 OK (text/html)
376	7.211006028	172.18.148.199	128.119.245.12	HTTP	628	GET /favicon.ico HTTP/1.1
386	7.555345426	128.119.245.12	172.18.148.199	HTTP	539	HTTP/1.1 404 Not Found (text/html)
722	17.383597927	172.18.148.199	128.119.245.12	HTTP	740	GET /wireshark-labs/HTTP-wireshark-file2.ht
728	17.705326999	128.119.245.12	172.18.148.199	HTTP	294	HTTP/1.1 304 Not Modified

wlp0s20f3: <live capture in progress> Packets: 1073 · Displayed: 6 (0.6%) · Selected: 2 (0.2%) Profile: Default

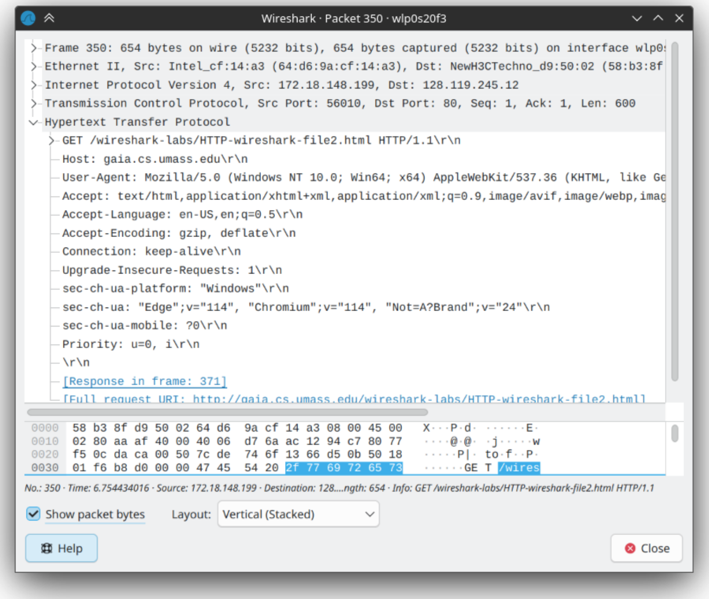
Figure 4: The HTTP CONDITIONAL GET/response

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?

The details of the first `HTTP GET` request are shown in Fig. 5. **No, there is no `IF-MODIFIED-SINCE` line in the HTTP GET.**



```
> Frame 350: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface wlp0:
> Ethernet II, Src: Intel_cf:14:a3 (64:d6:9a:cf:14:a3), Dst: NewH3CTechno_d9:50:02 (58:b3:8f
> Internet Protocol Version 4, Src: 172.18.148.199, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56010, Dst Port: 80, Seq: 1, Ack: 1, Len: 600
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    sec-ch-ua-platform: "Windows"\r\n
    sec-ch-ua: "Edge";v="114", "Chromium";v="114", "Not=A?Brand";v="24"\r\n
    sec-ch-ua-mobile: ?0\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 371]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

0000  58 b3 8f d9 50 02 64 d6  9a cf 14 a3 08 00 45 00   X···P·d· ······E·
0010  02 80 aa af 40 00 40 06  d7 6a ac 12 94 c7 80 77   ····@·@· ·j·····w
0020  f5 0c da ca 00 50 7c de  74 6f 13 66 d5 0b 50 18   ·····P|· to·f··P·
0030  01 f6 b8 d0 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires

No.: 350 · Time: 6.754434016 · Source: 172.18.148.199 · Destination: 128....ngth: 654 · Info: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
```

☑ Show packet bytes   Layout: Vertical (Stacked)

Figure 5: The first HTTP GET request

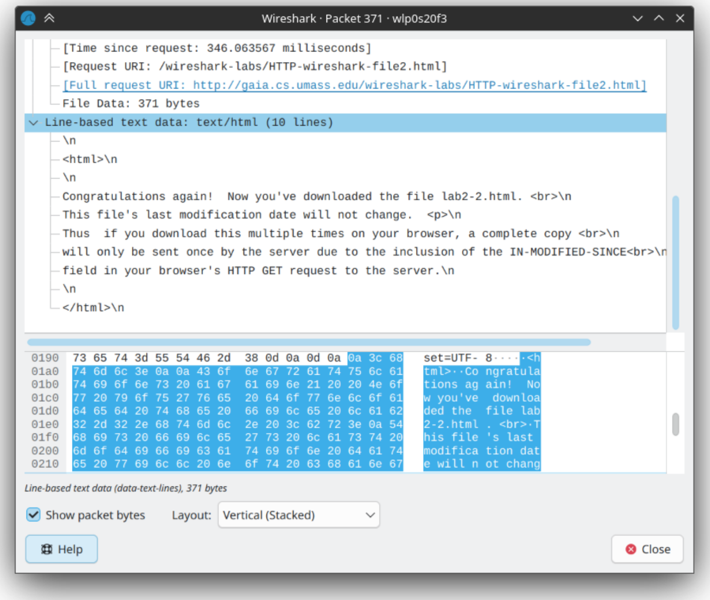
Question 9:

Inspect the contents of the server response. Did the server explicitly return the contents of the file?

The details of the server response are shown in Fig. 6. From the `text-based response message`, we can see that the server explicitly returns the contents of the file. **Therefore, yes, the server explicitly returns the contents of the file.**

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?



```
[Time since request: 346.063567 milliseconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
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
```

Line-based text data (data-text-lines), 371 bytes

☑ Show packet bytes   Layout: Vertical (Stacked)

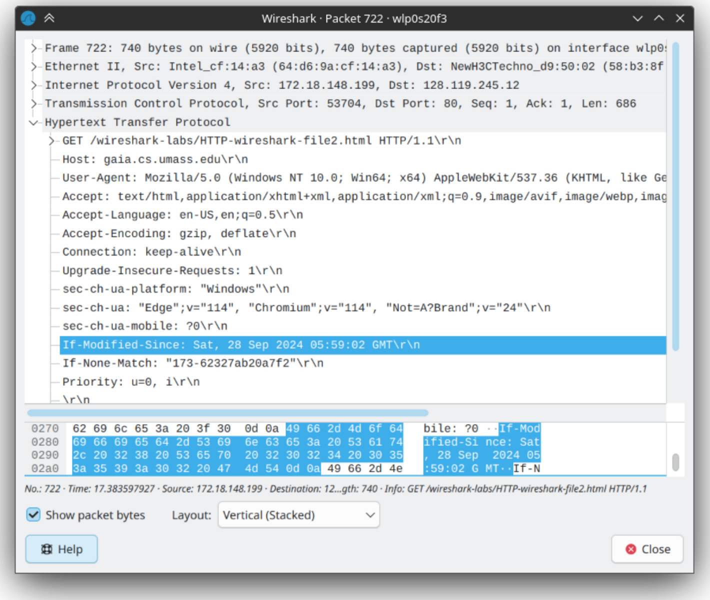
Figure 6: The first HTTP GET response

The details of the second `HTTP GET` request are shown in Fig. 7. The `IF-MODIFIED-SINCE` line is visible in the selected field. **There is an `IF-MODIFIED-SINCE` line in the HTTP GET request. The information following the `IF-MODIFIED-SINCE` header is `Sat, 28 Sep 2024 05:59:02 GMT`,** which is the time the file was last modified, as indicated in the first response.

Question 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.**

The details of the second server response are shown in Fig. 8. From the selected field, we can see that the server returns the status code `304 Not Modified`. **The server did not explicitly return the file's contents.** This status code indicates that the file has not been modified since it was last retrieved by the browser, so the server does not resend the file's contents. **This is the purpose of a conditional GET, which leverages the browser's cache to reduce network traffic.**



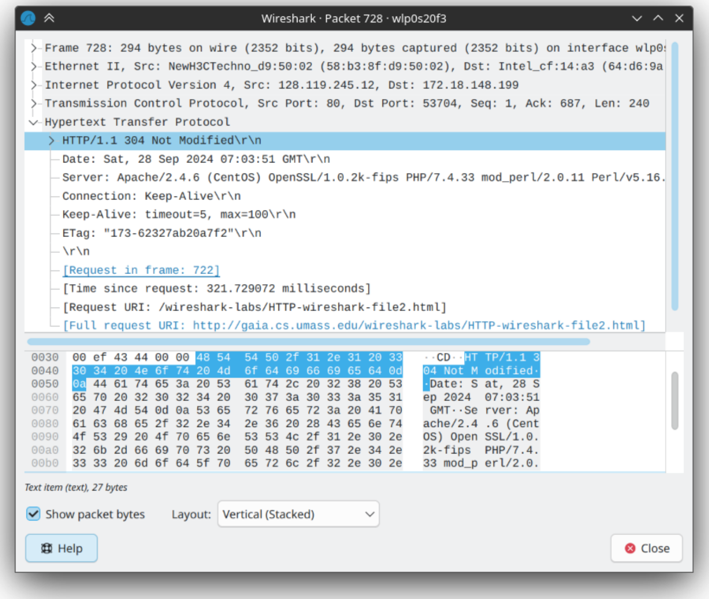
```
Frame 722: 740 bytes on wire (5920 bits), 740 bytes captured (5920 bits) on interface wlp0s
Ethernet II, Src: Intel_cf:14:a3 (64:d6:9a:cf:14:a3), Dst: NewH3CTechno_d9:50:02 (58:b3:8f
Internet Protocol Version 4, Src: 172.18.148.199, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53704, Dst Port: 80, Seq: 1, Ack: 1, Len: 686
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    sec-ch-ua-platform: "Windows"\r\n
    sec-ch-ua: "Edge";v="114", "Chromium";v="114", "Not=A?Brand";v="24"\r\n
    sec-ch-ua-mobile: ?0\r\n
    If-Modified-Since: Sat, 28 Sep 2024 05:59:02 GMT\r\n
    If-None-Match: "173-62327ab20a7f2"\r\n
    Priority: u=0, i\r\n
    \r\n

0270  62 69 6c 65 3a 20 3f 30  0d 0a 49 66 2d 4d 6f 64   bile: ?0 ··If-Mod
0280  69 66 69 65 64 2d 53 69  6e 63 65 3a 20 53 61 74   ified-Si nce: Sat
0290  2c 20 32 38 20 53 65 70  20 32 30 32 34 20 30 35   , 28 Sep  2024 05
02a0  3a 35 39 3a 30 32 20 47  4d 54 0d 0a 49 66 2d 4e   :59:02 G MT··If-N
```

No.: 722 · Time: 17.383597927 · Source: 172.18.148.199 · Destination: 12...gth: 740 · Info: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

☑ Show packet bytes   Layout: Vertical (Stacked)

Figure 7: The second HTTP GET request



```
Frame 728: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface wlp0s
Ethernet II, Src: NewH3CTechno_d9:50:02 (58:b3:8f:d9:50:02), Dst: Intel_cf:14:a3 (64:d6:9a
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.148.199
Transmission Control Protocol, Src Port: 80, Dst Port: 53704, Seq: 1, Ack: 687, Len: 240
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 28 Sep 2024 07:03:51 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.
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-62327ab20a7f2"\r\n
    \r\n
    [Request in frame: 722]
    [Time since request: 321.729072 milliseconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

0030  00 ef 43 44 00 00 48 54  54 50 2f 31 2e 31 20 33   ··CD··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 53  61 74 2c 20 32 38 20 53   ·Date: S at, 28 S
0060  65 70 20 32 30 32 34 20  30 37 3a 30 33 3a 35 31   ep 2024  07:03:51
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  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
```

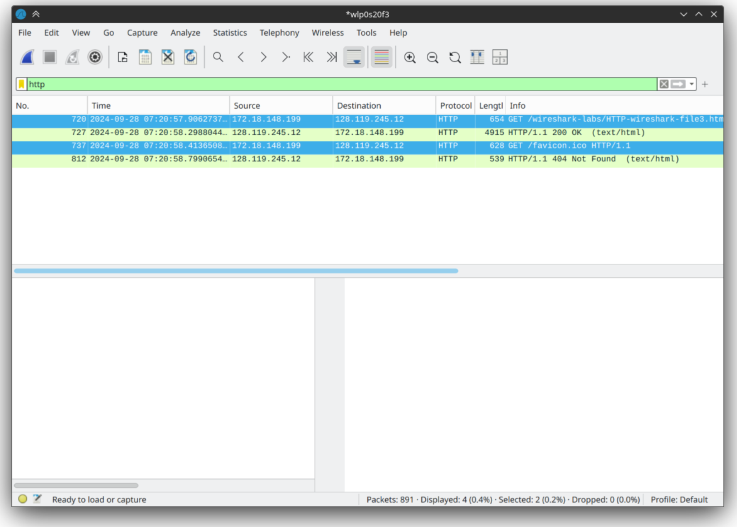
Text item (text), 27 bytes

☑ Show packet bytes   Layout: Vertical (Stacked)

Figure 8: The second HTTP GET response

Problem 3. Retrieving Long Documents

Following the instructions, open the target URL in the browser, and inspect the `HTTP GET` request and the `HTTP OK` reply. The results are shown in Fig. 9.



http

No.	Time	Source	Destination	Protocol	Lengtl	Info
720	2024-09-28 07:20:57.9062737…	172.18.148.199	128.119.245.12	HTTP	654	GET /wireshark-labs/HTTP-wireshark-file3.htm
727	2024-09-28 07:20:58.2988044…	128.119.245.12	172.18.148.199	HTTP	4915	HTTP/1.1 200 OK (text/html)
737	2024-09-28 07:20:58.4136508…	172.18.148.199	128.119.245.12	HTTP	628	GET /favicon.ico HTTP/1.1
812	2024-09-28 07:20:58.7990654…	128.119.245.12	172.18.148.199	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Ready to load or capture

Packets: 891 · Displayed: 4 (0.4%) · Selected: 2 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

Figure 9: The HTTP GET/response for 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?**

Inspect the `HTTP GET` request, as shown in Fig. 9. There are 2 `HTTP GET` request messages. The packet number in the trace that contains the GET message for the Bill of Rights is the first `HTTP GET` request, which is packet No. 720.

Question 13:

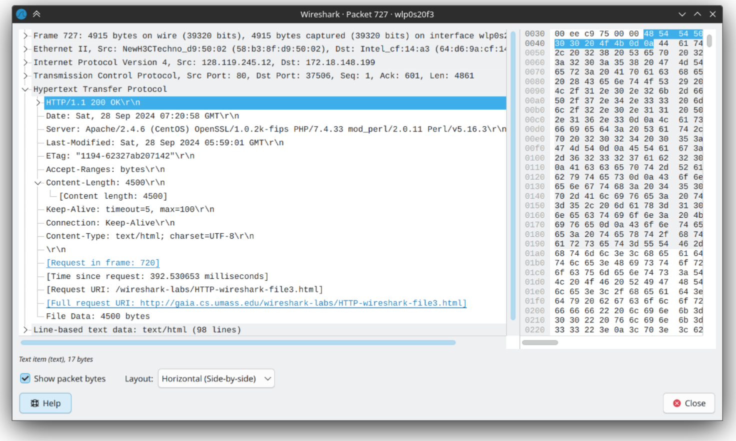
> **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**

Inspect the corresponding ‘HTTP OK‘ reply for packet No. 720, as shown in Fig. 9. It indicates a response code of `200 OK`. The packet number in the trace that contains the status code and phrase associated with the response to the HTTP GET request is packet No. 727.

Question 14:

What is the status code and phrase in the response?

Inspect the `HTTP OK` reply, focusing on the `Status Code` field in `HTTP`, as shown in Fig. 10. The status code and phrase in the response is `200 OK`, which is highlighted as the selected field.



```
> Frame 727: 4915 bytes on wire (39320 bits), 4915 bytes captured (39320 bits) on interface wlp0s2
> Ethernet II, Src: NewH3CTechno_d9:50:02 (58:b3:8f:d9:50:02), Dst: Intel_cf:14:a3 (64:d6:9a:cf:14
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.148.199
> Transmission Control Protocol, Src Port: 80, Dst Port: 37506, Seq: 1, Ack: 601, Len: 4861
v Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Sat, 28 Sep 2024 07:20:58 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: Sat, 28 Sep 2024 05:59:01 GMT\r\n
      ETag: "1194-62327ab207142"\r\n
      Accept-Ranges: bytes\r\n
    v Content-Length: 4500\r\n
        [Content length: 4500]
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [Request in frame: 720]
      [Time since request: 392.530653 milliseconds]
      [Request URI: /wireshark-labs/HTTP-wireshark-file3.html]
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
      File Data: 4500 bytes
> Line-based text data: text/html (98 lines)
```

```
0030  00 ee c9 75 00 00 48 54  54 50
0040  30 30 20 4f 4b 0d 0a 44  61 74
0050  2c 20 32 38 20 53 65 70  20 32
0060  3a 32 30 3a 35 38 20 47  4d 54
0070  65 72 3a 20 41 70 61 63  68 65
0080  20 28 43 65 6e 74 4f 53  29 20
0090  4c 2f 31 2e 30 2e 32 6b  2d 66
00a0  50 2f 37 2e 34 2e 33 33  20 6d
00b0  6c 2f 32 2e 30 2e 31 31  20 50
00c0  2e 31 36 2e 33 0d 0a 4c  61 73
00d0  66 69 65 64 3a 20 53 61  74 2c
00e0  70 20 32 30 32 34 20 30  35 3a
00f0  47 4d 54 0d 0a 45 54 61  67 3a
0100  2d 36 32 33 32 37 61 62  32 30
0110  0a 41 63 63 65 70 74 2d  52 61
0120  62 79 74 65 73 0d 0a 43  6f 6e
0130  65 6e 67 74 68 3a 20 34  35 30
0140  70 2d 41 6c 69 76 65 3a  20 74
0150  3d 35 2c 20 6d 61 78 3d  31 30
0160  6e 65 63 74 69 6f 6e 3a  20 4b
0170  69 76 65 0d 0a 43 6f 6e  74 65
0180  65 3a 20 74 65 78 74 2f  68 74
0190  61 72 73 65 74 3d 55 54  46 2d
01a0  68 74 6d 6c 3e 3c 68 65  61 64
01b0  74 6c 65 3e 48 69 73 74  6f 72
01c0  6f 63 75 6d 65 6e 74 73  3a 54
01d0  4c 20 4f 46 20 52 49 47  48 54
01e0  6c 65 3e 3c 2f 68 65 61  64 3e
01f0  64 79 20 62 67 63 6f 6c  6f 72
0200  66 66 66 22 20 6c 69 6e  6b 3d
0210  30 30 22 20 76 6c 69 6e  6b 3d
0220  33 33 22 3e 0a 3c 70 3e  3c 62
```

Text item (text), 17 bytes

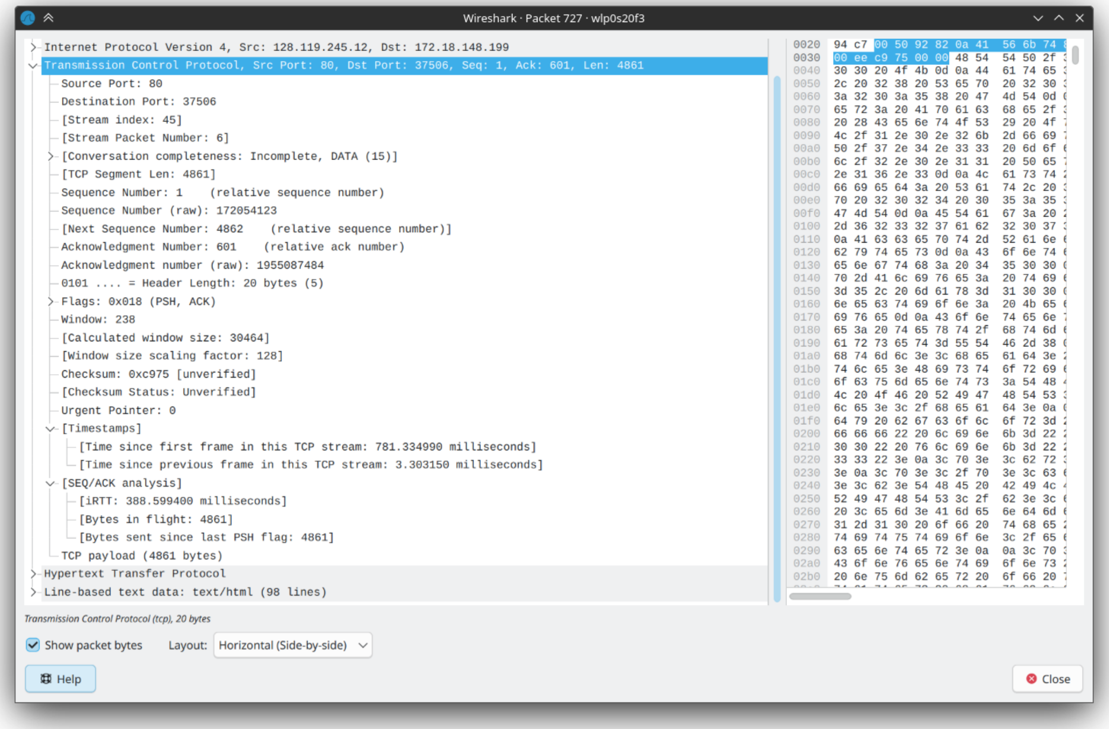
☑ Show packet bytes Layout: Horizontal (Side-by-side)

Figure 10: The HTTP OK reply for long documents

Question 15:

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

Inspect the `HTTP OK` response, and observe the `TCP` field in `HTTP` as shown in Fig. 11. Only one TCP segment contains data, sufficient to carry both the single HTTP response and the text of the Bill of Rights, with a packet length of `4861 bytes`.



```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.148.199
v Transmission Control Protocol, Src Port: 80, Dst Port: 37506, Seq: 1, Ack: 601, Len: 4861
    Source Port: 80
    Destination Port: 37506
    [Stream index: 45]
    [Stream Packet Number: 6]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 4861]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 172054123
    [Next Sequence Number: 4862    (relative sequence number)]
    Acknowledgment Number: 601    (relative ack number)
    Acknowledgment number (raw): 1955087484
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 238
    [Calculated window size: 30464]
    [Window size scaling factor: 128]
    Checksum: 0xc975 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  v [Timestamps]
      [Time since first frame in this TCP stream: 781.334990 milliseconds]
      [Time since previous frame in this TCP stream: 3.303150 milliseconds]
  v [SEQ/ACK analysis]
      [iRTT: 388.599400 milliseconds]
      [Bytes in flight: 4861]
      [Bytes sent since last PSH flag: 4861]
    TCP payload (4861 bytes)
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

```
0020  94 c7 00 50 92 82 0a 41  56 6b 74
0030  00 ee c9 75 00 00 48 54  54 50 2f
0040  30 30 20 4f 4b 0d 0a 44  61 74 65
0050  2c 20 32 38 20 53 65 70  20 32 30
0060  3a 32 30 3a 35 38 20 47  4d 54 0d
0070  65 72 3a 20 41 70 61 63  68 65 2f
0080  20 28 43 65 6e 74 4f 53  29 20 4f
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74
00d0  66 69 65 64 3a 20 53 61  74 2c 20
00e0  70 20 32 30 32 34 20 30  35 3a 35
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20
0100  2d 36 32 33 32 37 61 62  32 30 37
0110  0a 41 63 63 65 70 74 2d  52 61 6e
0120  62 79 74 65 73 0d 0a 43  6f 6e 74
0130  65 6e 67 74 68 3a 20 34  35 30 30
0140  70 2d 41 6c 69 76 65 3a  20 74 69
0150  3d 35 2c 20 6d 61 78 3d  31 30 30
0160  6e 65 63 74 69 6f 6e 3a  20 4b 65
0170  69 76 65 0d 0a 43 6f 6e  74 65 6e
0180  65 3a 20 74 65 78 74 2f  68 74 6d
0190  61 72 73 65 74 3d 55 54  46 2d 38
01a0  68 74 6d 6c 3e 3c 68 65  61 64 3e
01b0  74 6c 65 3e 48 69 73 74  6f 72 69
01c0  6f 63 75 6d 65 6e 74 73  3a 54 48
01d0  4c 20 4f 46 20 52 49 47  48 54 53
01e0  6c 65 3e 3c 2f 68 65 61  64 3e 0a
01f0  64 79 20 62 67 63 6f 6c  6f 72 3d
0200  66 66 66 22 20 6c 69 6e  6b 3d 22
0210  30 30 22 20 76 6c 69 6e  6b 3d 22
0220  33 33 22 3e 0a 3c 70 3e  3c 62 72
0230  3e 0a 3c 70 3e 3c 2f 70  3e 3c 63
0240  3e 3c 62 3e 54 48 45 20  42 49 4c
0250  52 49 47 48 54 53 3c 2f  62 3e 3c
0260  20 3c 65 6d 3e 41 6d 65  6e 64 6d
0270  31 2d 31 30 20 6f 66 20  74 68 65
0280  74 69 74 75 74 69 6f 6e  3c 2f 65
0290  63 65 6e 74 65 72 3e 0a  0a 3c 70
02a0  43 6f 6e 76 65 6e 74 69  6f 6e 73
02b0  20 6e 75 6d 62 65 72 20  6f 66 20
```

Transmission Control Protocol (tcp), 20 bytes

☑ Show packet bytes   Layout: Horizontal (Side-by-side)

Figure 11: The TCP segment for long documents