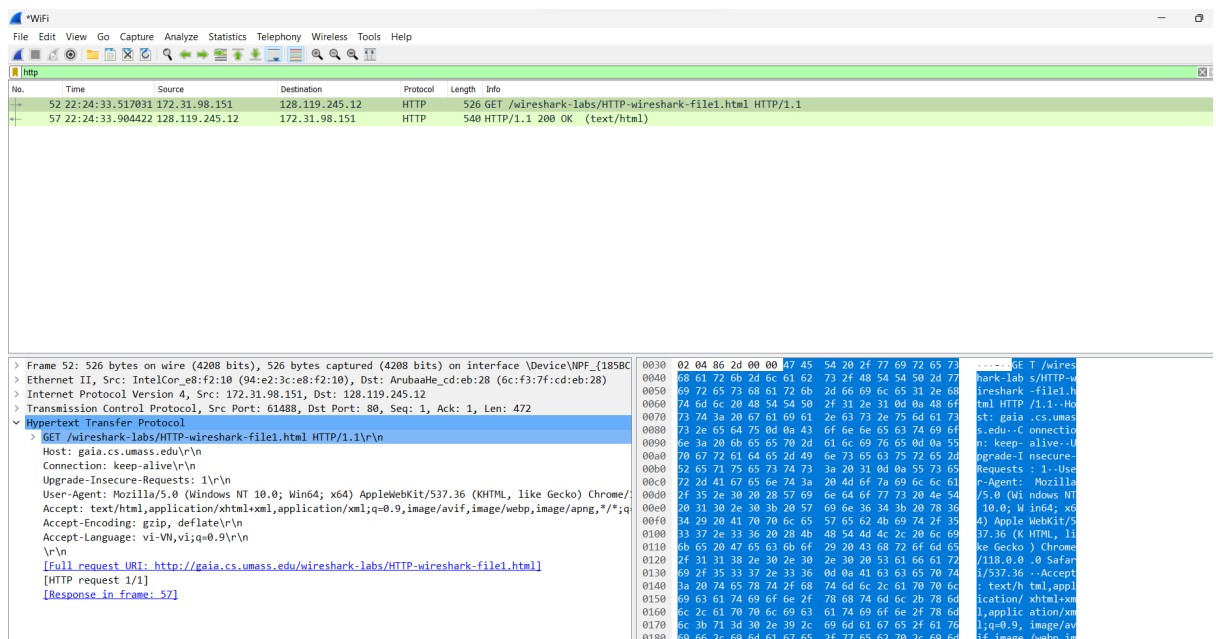


# Lab 02

## 1. The Basic HTTP GET/response interaction

Do the following:

1. Start up your web browser.
2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks, and in lower case) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
3. Wait a bit more than one minute (we'll see why shortly), 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.



Answer the following questions:

1. Is your browser running HTTP version 1.0, 1.1, or 2? 1.1

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

What version of HTTP is the server running? 1.1

HTTP/1.1 200 OK\r\n

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

## vi-VN and vi

No.	Time	Source	Destination	Protocol	Length	Info
52	22:24:33.517031	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
57	22:24:33.904422	128.119.245.12	172.31.98.151	HTTP	540	HTTP/1.1 200 OK (text/html)

Checksum: 0x862d [unverified]	0000	6c f3 7f cd eb 28 94 e2 3c e
[Checksum Status: Unverified]	0010	02 00 e0 ee 40 00 80 06 00 0
Urgent Pointer: 0	0020	f5 0c f0 30 00 50 ea 37 8c 7
> [Timestamps]	0030	02 04 86 2d 00 00 47 45 54 2
> [SEQ/ACK analysis]	0040	68 61 72 6b 2d 6c 61 62 73 2
TCP payload (472 bytes)	0050	69 72 65 73 68 61 72 6b 2d 6
> Hypertext Transfer Protocol	0060	74 6d 6c 20 48 54 54 50 2f 3
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n	0070	73 74 3a 20 67 61 69 61 2e 6
Host: gaia.cs.umass.edu\r\n	0080	73 2e 65 64 75 0d 0a 43 6f 6
Connection: keep-alive\r\n	0090	6e 3a 20 6b 65 65 70 2d 61 6
Upgrade-Insecure-Requests: 1\r\n	00a0	70 67 72 61 64 65 2d 49 6e 7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom	00b0	52 65 71 75 65 73 74 73 3a 2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*	00c0	72 2d 41 67 65 6e 74 3a 20 4
Accept-Encoding: gzip, deflate\r\n	00d0	2f 35 2e 30 20 28 57 69 6e 6
Accept-Language: vi-VN,vi;q=0.9\r\n	00e0	20 31 30 2e 30 3b 20 57 69 6
\r\n	00f0	34 29 20 41 70 70 6c 65 57 6
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]	0100	33 37 2e 33 36 20 28 4b 48 5
[HTTP request 1/1]	0110	6b 65 20 47 65 63 6b 6f 29 2
[Response in frame: 57]	0120	2f 31 31 38 2e 30 2e 30 2e 3
	0130	69 2f 35 33 37 2e 33 36 0d 0
	0140	3a 20 74 65 78 74 2f 68 74 6

- What is the IP address of your computer? 172.31.98.151  
What is the IP address of the gaia.cs.umass.edu server? 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
52	22:24:33.517031	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
57	22:24:33.904422	128.119.245.12	172.31.98.151	HTTP	540	HTTP/1.1 200 OK (text/html)

[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
> Ethernet II, Src: IntelCor\_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaaHe\_cd:eb:28 (6c:f3:7f:cd:eb:28)  
v Internet Protocol Version 4, Src: 172.31.98.151, Dst: 128.119.245.12  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 512  
Identification: 0xe0ee (57582)  
> 010. .... = Flags: 0x2, Don't fragment  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 128  
Protocol: TCP (6)  
Header Checksum: 0x0000 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 172.31.98.151  
Destination Address: 128.119.245.12  
v Transmission Control Protocol, Src Port: 61488, Dst Port: 80, Seq: 1, Ack: 1, Len: 472

0010 02 00 e0 ee 40 00 8  
0020 f5 0c f0 30 00 50 e  
0030 02 04 86 2d 00 00 4  
0040 68 61 72 6b 2d 6c 6  
0050 69 72 65 73 68 61 7  
0060 74 6d 6c 20 48 54 5  
0070 73 74 3a 20 67 61 6  
0080 73 2e 65 64 75 0d 6  
0090 6e 3a 20 6b 65 65 7  
00a0 70 67 72 61 64 65 2  
00b0 52 65 71 75 65 73 7  
00c0 72 2d 41 67 65 6e 7  
00d0 2f 35 2e 30 20 28 5  
00e0 20 31 30 2e 30 3b 2  
00f0 34 29 20 41 70 70 6  
0100 33 37 2e 33 36 20 2  
0110 6b 65 20 47 65 63 6  
0120 2f 31 31 38 2e 30 2  
0130 69 2f 35 33 37 2e 3  
0140 3a 20 74 65 78 74 2

4. What is the **status code** returned from the **server to your browser**? 200 OK

No.	Time	Source	Destination	Protocol	Length	Info
52	22:24:33.517031	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
57	22:24:33.904422	128.119.245.12	172.31.98.151	HTTP	540	HTTP/1.1 200 OK (text/html)

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

Fri, 20 Oct 2023 05:59:02 GMT\r\n

TCP payload (486 bytes)
v Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Fri, 20 Oct 2023 15:24:28 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: Fri, 20 Oct 2023 05:59:02 GMT\r\n
ETag: "80-6081f91bbe297"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 128\r\n

6. How many **bytes of content** are being returned to your browser? 128 bytes

```

    TCP payload (480 bytes)
  v Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Fri, 20 Oct 2023 15:24:28 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mo
      Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT\r\n
      ETag: "80-6081f91bbe297"\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 1/1]
      [Time since request: 0.387391000 seconds]
      [Request in frame: 52]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wire:
      File Data: 128 bytes

```

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.

Nothing.

## 2. The HTTP CONDITIONAL GET/response interaction

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?

There is no “IF-MODIFIED-SINCE” line in the first HTTP GET.

The image displays a Wireshark network traffic capture. The top pane shows a list of captured packets, with the selected packet being an HTTP GET request for `/wireshark-labs/HTTP-wireshark-file2.html`. The middle pane shows the details of the selected packet, including the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII, with a highlighted section of the response body.

No.	Time	Source	Destination	Protocol	Length	Info
114	23:35:04.906527	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
118	23:35:05.295638	128.119.245.12	172.31.98.151	HTTP	784	HTTP/1.1 200 OK (text/html)
119	23:35:05.343291	172.31.98.151	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
120	23:35:05.732494	128.119.245.12	172.31.98.151	HTTP	538	HTTP/1.1 404 Not Found (text/html)
12177	23:43:37.778975	172.31.98.151	209.197.3.8	HTTP	336	GET /msdownload/update/v3/static/trusted/en/authrootstl.cab?404a600afc71dc66 HTTP/1.1
12180	23:43:37.811185	209.197.3.8	172.31.98.151	HTTP	319	HTTP/1.1 304 Not Modified

Details of the selected packet (No. 118):

- [Next Sequence Number: 473 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 1649484389
- 0101 .... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 516
- [Calculated window size: 132096]
- [Window size scaling factor: 256]
- Checksum: 0x862d [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (472 bytes)
- 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/118.0.0.0 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: vi-VN,vi;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: 118]
  - [Next request in frame: 119]

Packet bytes (hexadecimal and ASCII):

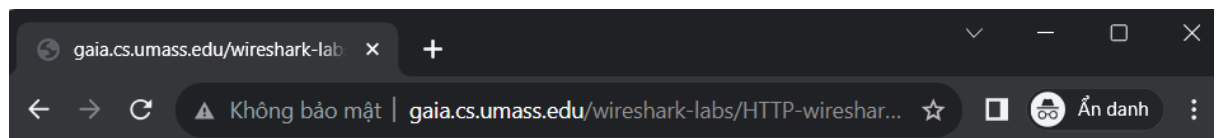
```

0010  02 00 e1 3b 40 00 80 06 00 00
0020  f5 0c f4 c4 00 50 e8 26 33 65
0030  02 04 86 2d 00 00 47 45 54 20
0040  68 61 72 6b 2d 6c 61 62 73 2f
0050  69 72 65 73 68 61 72 6b 2d 66
0060  74 6d 6c 20 48 54 54 50 2f 31
0070  73 74 3a 20 67 61 69 61 2e 63
0080  73 2e 65 64 75 6d 0a 43 0f 0e
0090  65 3a 20 6b 65 65 70 2d 61 6c
00a0  70 67 72 61 64 65 2d 49 6e 73
00b0  52 65 71 75 65 73 74 73 3a 20
00c0  72 2d 41 67 65 6e 74 3a 20 4d
00d0  2f 35 2e 30 20 28 57 69 6e 64
00e0  20 31 30 2e 30 3b 20 57 69 6e
00f0  34 29 20 41 70 70 6c 65 57 65
0100  33 37 2e 33 36 20 28 4b 48 54
0110  6b 65 20 47 65 63 6b 6f 29 20
0120  2f 31 31 38 2e 30 2e 30 2e 30
0130  69 2f 35 33 37 2e 33 36 0d 0a
0140  3a 20 74 65 78 74 2f 68 74 6d
0150  69 63 61 74 69 6f 6e 2f 78 68
0160  6c 2c 61 70 70 6c 69 63 61 74
0170  6c 3b 71 3d 30 2e 39 2c 69 6d
0180  69 66 2c 69 6d 61 67 65 2f 77
0190  61 67 65 2f 61 70 6e 67 2c 2a
01a0  2e 38 2c 61 70 70 6c 69 63 61
01b0  69 67 6e 65 64 2d 65 78 63 68
01c0  3d 62 33 3b 71 3d 30 2e 37 0d
01d0  74 2d 45 6e 63 6f 64 69 6e 67
01e0  2c 20 64 65 66 6c 61 74 65 0d
01f0  74 2d 4c 61 6e 67 75 61 67 65
0200  4e 2c 76 69 3b 71 3d 30 2e 39
  
```

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

The server did explicitly return the contents of the file. Wireshark includes a section titled “Line-Based Text Data” which shows what the server sent back to my browser which is specifically what the website showed when I brought it up on my browser

Wireshark packet capture showing an HTTP GET request and response. The response is a 200 OK status with a text/html content type. The packet details pane shows the HTTP response structure, including headers like Date, Server, Last-Modified, ETag, and Accept-Ranges. The packet bytes pane shows the raw data of the response, which is a 371-byte HTML document.



Congratulations again! Now you've downloaded the file lab2-2.html.  
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server.

- 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<sup>4</sup>? If so, what information follows the “IF-MODIFIED-SINCE:” header?

There is an “IF-MODIFIED-SINCE” line in the second HTTP GET. The information follows are “Tue, 22 Aug 2023 18:02:30 GMT”.

Wireshark capture showing HTTP traffic. The selected packet is a GET request for a file that has not been modified.

No.	Time	Source	Destination	Protocol	Length	Info
114	23:35:04.906527	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
118	23:35:05.295638	128.119.245.12	172.31.98.151	HTTP	784	HTTP/1.1 200 OK (text/html)
119	23:35:05.343291	172.31.98.151	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
120	23:35:05.732494	128.119.245.12	172.31.98.151	HTTP	538	HTTP/1.1 404 Not Found (text/html)
12177	23:43:37.778975	172.31.98.151	209.197.3.8	HTTP	336	GET /msdownload/update/v3/static/trusted/en/authrootstl.cab?404a600afc71dc66 HTTP/1.1
12180	23:43:37.811185	209.197.3.8	172.31.98.151	HTTP	319	HTTP/1.1 304 Not Modified

Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 876927313  
[Next Sequence Number: 283 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 812151769  
0101 .... = Header Length: 20 bytes (5)  
> Flags: 0x018 (PSH, ACK)  
Window: 514  
[Calculated window size: 131584]  
[Window size scaling factor: 256]  
Checksum: 0xe4b8 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
> [Timestamps]  
> [SEQ/ACK analysis]  
TCP payload (282 bytes)  
> Hypertext Transfer Protocol  
> GET /msdownload/update/v3/static/trusted/en/authrootstl.cab?404a600afc71dc66 HTTP/1.1\r\n  
Connection: Keep-Alive\r\n  
Accept: \*/\*\r\n  
If-Modified-Since: Tue, 22 Aug 2023 18:02:30 GMT\r\n  
If-None-Match: "606786d122d5d91:0"\r\n  
User-Agent: Microsoft-CryptoAPI/10.0\r\n  
Host: ctldl.windowsupdate.com\r\n  
\r\n  
[Full request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/authrootstl.cab?404a600afc71dc66]  
[HTTP request 1/1]  
[Response in frame: 12180]

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 HTTP status code is “304: Not Modified”.

This is because it has not received the content explicitly since the content was not modified in the first time requested, but in the second time there is no need to download the file again.

Wireshark capture showing HTTP traffic. The selected packet is a 304 Not Modified response.

No.	Time	Source	Destination	Protocol	Length	Info
114	23:35:04.906527	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
118	23:35:05.295638	128.119.245.12	172.31.98.151	HTTP	784	HTTP/1.1 200 OK (text/html)
119	23:35:05.343291	172.31.98.151	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
120	23:35:05.732494	128.119.245.12	172.31.98.151	HTTP	538	HTTP/1.1 404 Not Found (text/html)
12177	23:43:37.778975	172.31.98.151	209.197.3.8	HTTP	336	GET /msdownload/update/v3/static/trusted/en/authrootstl.cab?404a600afc71dc66 HTTP/1.1
12180	23:43:37.811185	209.197.3.8	172.31.98.151	HTTP	319	HTTP/1.1 304 Not Modified

[Next Sequence Number: 266 (relative sequence number)]  
Acknowledgment Number: 283 (relative ack number)  
Acknowledgment number (raw): 876927595  
0101 .... = Header Length: 20 bytes (5)  
> Flags: 0x018 (PSH, ACK)  
Window: 131  
[Calculated window size: 67072]  
[Window size scaling factor: 512]  
Checksum: 0x7382 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
> [Timestamps]  
> [SEQ/ACK analysis]  
TCP payload (265 bytes)  
> Hypertext Transfer Protocol  
> HTTP/1.1 304 Not Modified\r\n  
Date: Fri, 20 Oct 2023 16:43:32 GMT\r\n  
Surrogate-Control: public;hw-h2proxy, max-age=900;hw-h2proxy\r\n  
Accept-Ranges: bytes\r\n  
ETag: "606786d122d5d91:0"\r\n  
X-HW: 1697820212.cdn4-pxy019-hkg02.hk1.ev,1697820212.cds215.hk1.c\r\n  
X-CCC: CN\r\n  
X-CID: 9\r\n  
\r\n  
[HTTP response 1/1]  
[Time since request: 0.032210000 seconds]  
[Request in frame: 12177]  
[Request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/authrootstl.cab?404a600afc71dc66]

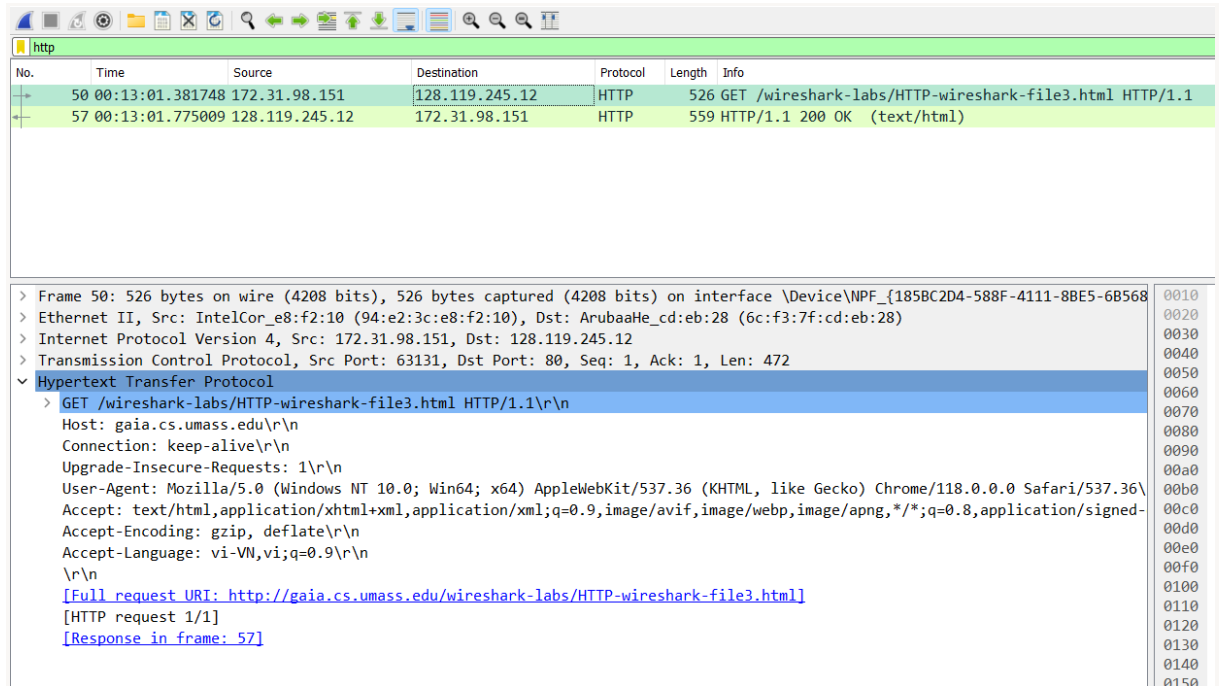
### 3. Retrieving Long Documents

Answer the following questions:

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?

My browser only sent 1 HTTP GET request to the server.

Packet number 50.



The image shows a Wireshark packet capture window. The top pane displays a list of packets. Packet 50 is highlighted, showing it is an HTTP GET request to /wireshark-labs/HTTP-wireshark-file3.html. Packet 57 is also highlighted, showing it is the HTTP 200 OK response. The bottom pane shows the details of the selected packet (50), which is an HTTP GET request. The details include the host (gaia.cs.umass.edu), connection (keep-alive), user-agent (Mozilla/5.0), and the full request URI.

No.	Time	Source	Destination	Protocol	Length	Info
50	00:13:01.381748	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
57	00:13:01.775009	128.119.245.12	172.31.98.151	HTTP	559	HTTP/1.1 200 OK (text/html)

Details of Packet 50:

- Frame 50: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF\_{185BC2D4-588F-4111-8BE5-6B568}
- Ethernet II, Src: IntelCor\_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaaHe\_cd:eb:28 (6c:f3:7f:cd:eb:28)
- Internet Protocol Version 4, Src: 172.31.98.151, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 63131, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
- Hypertext Transfer Protocol
  - GET /wireshark-labs/HTTP-wireshark-file3.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/118.0.0.0 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: vi-VN,vi;q=0.9\r\n
  - \r\n
  - [Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>]
  - [HTTP request 1/1]
  - [Response in frame: 57]

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

Packet number 57.



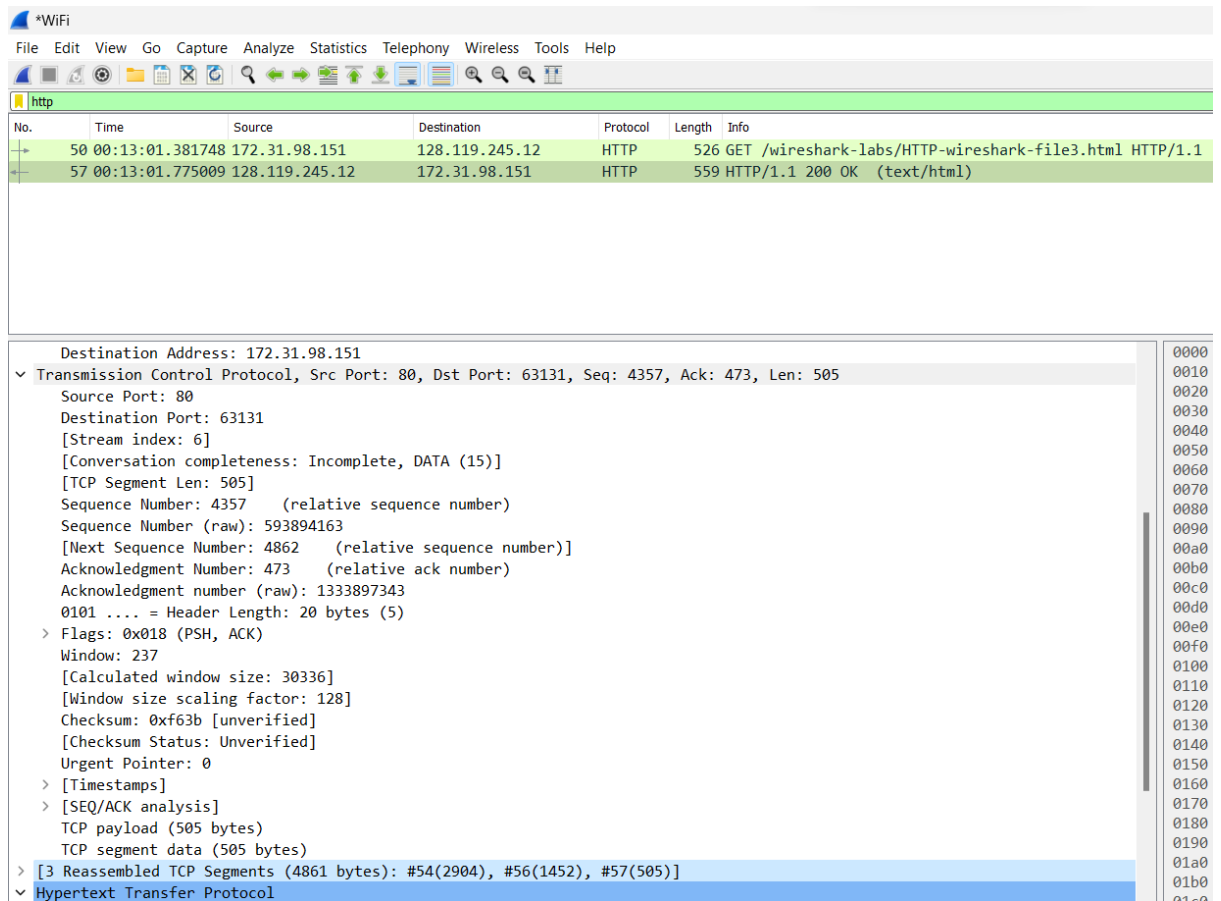
*WiFi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
50	00:13:01.381748	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
57	00:13:01.775009	128.119.245.12	172.31.98.151	HTTP	559	HTTP/1.1 200 OK (text/html)
> Frame 57: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B568} 0000 94 > Ethernet II, Src: ArubaaHe_cd:eb:28 (6c:f3:7f:cd:eb:28), Dst: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10) 0010 02 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.31.98.151 0020 62 > Transmission Control Protocol, Src Port: 80, Dst Port: 63131, Seq: 4357, Ack: 473, Len: 505 0030 00 > [3 Reassembled TCP Segments (4861 bytes): #54(2904), #56(1452), #57(505)] 0040 20 > Hypertext Transfer Protocol 0050 65 > HTTP/1.1 200 OK\r\n 0060 0a Date: Fri, 20 Oct 2023 17:12:56 GMT\r\n 0070 22 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 0080 41 Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT\r\n 0090 3e ETag: "1194-6081f91bb985f"\r\n 00a0 3c Accept-Ranges: bytes\r\n 00b0 75 Content-Length: 4500\r\n 00c0 20 Keep-Alive: timeout=5, max=100\r\n 00d0 66 Connection: Keep-Alive\r\n 00e0 2c Content-Type: text/html; charset=UTF-8\r\n 00f0 6f \r\n 0100 20 [HTTP response 1/1] 0110 68 [Time since request: 0.393261000 seconds] 0120 20 [Request in frame: 50] 0130 70 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html] 0140 22 File Data: 4500 bytes 0150 65 Line-based text data: text/html (98 lines) 0160 73 0170 3c 0180 72 0190 20						

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

The code and phrase in the response was 200 OK

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

3 Reassembled TCP Segments (4861 bytes): #54(2904), #56(1452), #57(505)



#### 4. HTML Documents with Embedded Objects

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

Answer the following questions:

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

My browser sent 3 http GET message requests. It sent to the internet address of the main html page and the location of the images:

Initial Page address: 128.119.245.12

Pearson Logo: 128.199.245.12

Pearson book, 5th Edition: 172.31.98.151

*WiFi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
43	06:52:34.661421	172.31.98.151	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
47	06:52:35.006180	128.119.245.12	172.31.98.151	HTTP	1355	HTTP/1.1 200 OK (text/html)
48	06:52:35.019534	172.31.98.151	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
61	06:52:35.366583	128.119.245.12	172.31.98.151	HTTP	761	HTTP/1.1 200 OK (PNG)
73	06:52:35.611321	172.31.98.151	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
77	06:52:35.814187	178.79.137.164	172.31.98.151	HTTP	225	HTTP/1.1 301 Moved Permanently

> Frame 43: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B568}	0000	6c f3 7f cd eb 28
> Ethernet II, Src: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaaHe_cd:eb:28 (6c:f3:7f:cd:eb:28)	0010	02 00 e1 84 40 00
> Internet Protocol Version 4, Src: 172.31.98.151, Dst: 128.119.245.12	0020	f5 0c fa 3b 00 50
> Transmission Control Protocol, Src Port: 64059, Dst Port: 80, Seq: 1, Ack: 1, Len: 472	0030	02 04 86 2d 00 00
> Hypertext Transfer Protocol	0040	68 61 72 6b 2d 6c
	0050	69 72 65 73 68 61
	0060	74 6d 6c 20 48 54
	0070	73 74 3a 20 67 61
	0080	73 7a 65 64 75 6d

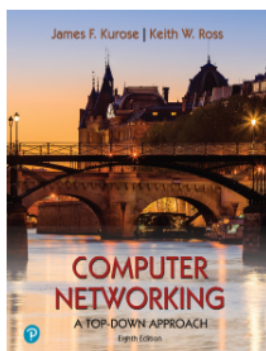
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

The two photos were downloaded sequentially by the browser.

The first image “pearson.png” was requested and retrieved the 200 OK status. The second image was requested and first retrieved failed with “301 moved permanently”. I believe this is the situation since the first image was requested and transmitted by the browser before the second image. If they had been operating concurrently, both files would have been requested and returned in the same time period. However, in this example, the second image was requested only after the first image was returned.



This little HTML file is being served by [gaia.cs.umass.edu](http://gaia.cs.umass.edu). It contains two embedded images. The image above, also served from the [gaia.cs.umass.edu](http://gaia.cs.umass.edu) web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server [kurose.cslash.net](http://kurose.cslash.net) in France:



And while we have your attention, you might want to take time to check out the available open resources for this book at [http://gaia.cs.umass.edu/kurose\\_ross](http://gaia.cs.umass.edu/kurose_ross).

## 5 HTTP Authentication

http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html  
The username is “wireshark-students” (without the quotes), and the password is “network”

Answer the following questions<sup>5</sup>:

- What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

State code: 401

Phase: Unauthorized

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows four packets: a GET request (No. 156), an unauthorized response (No. 167), a second GET request (No. 422), and a 200 OK response (No. 432). Packet 167 is selected, showing its details in the middle pane and its raw bytes in the bottom pane. The details pane for packet 167 shows an HTTP 1.1 401 Unauthorized response with a WWW-Authenticate header and a Content-Length of 381. The raw bytes pane shows the hexadecimal representation of the response, which includes the status line and the body of the response.

No.	Time	Source	Destination	Protocol	Length	Info
156	07:31:26.412004	172.31.98.151	128.119.245.12	HTTP	549	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
167	07:31:26.801370	128.119.245.12	172.31.98.151	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
422	07:31:36.900400	172.31.98.151	128.119.245.12	HTTP	634	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
432	07:31:37.295061	128.119.245.12	172.31.98.151	HTTP	544	HTTP/1.1 200 OK (text/html)

Frame 167: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF\_{185BC2D4-588F-4111-8BE5-6B56} 0030 00 ed fd fd 00 00 48 54 54 50 2f 31 2e  
> Ethernet II, Src: ArubaHe\_cd:eb:28 (6c:f3:7f:cd:eb:28), Dst: IntelCor\_e8:f2:10 (94:e2:3c:e8:f2:10) 0040 30 31 20 55 6e 61 75 74 68 6f 72 69 7a  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.31.98.151 0050 0a 44 61 74 65 3a 20 53 61 74 2c 20 32  
> Transmission Control Protocol, Src Port: 80, Dst Port: 65161, Seq: 1, Ack: 496, Len: 717 0060 63 74 20 32 30 32 33 20 30 30 3a 33 31  
> Hypertext Transfer Protocol 0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a  
> HTTP/1.1 401 Unauthorized\r\n 0080 61 63 68 65 2f 32 2e 34 2e 36 20 28 43  
Date: Sat, 21 Oct 2023 00:31:21 GMT\r\n 0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31  
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 00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 37  
WWW-Authenticate: Basic realm="wireshark-students only"\r\n 00b0 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32  
Content-Length: 381\r\n 00c0 31 31 20 50 65 72 6c 2f 76 35 2e 31 36  
Keep-Alive: timeout=5, max=100\r\n 00d0 0a 57 57 57 2d 41 75 74 68 65 6e 74 69  
Connection: Keep-Alive\r\n 00e0 65 3a 20 42 61 73 69 63 20 72 65 61 6c  
Content-Type: text/html; charset=iso-8859-1\r\n 00f0 77 69 72 65 73 68 61 72 6b 2d 73 74 75  
\r\n 0100 74 73 20 6f 6e 6c 79 22 0d 0a 43 6f 6e  
[HTTP response 1/1] 0110 74 2d 4c 65 6e 67 74 68 3a 20 33 38 31  
[Time since request: 0.389366000 seconds] 0120 65 65 70 2d 41 6c 69 76 65 3a 20 74 69  
[Request in frame: 156] 0130 75 74 3d 35 2c 20 6d 61 78 3d 31 30 30  
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html] 0140 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65  
File Data: 381 bytes 0150 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e  
0160 79 70 65 3a 20 74 65 78 74 2f 68 74 6d  
0170 63 68 61 72 73 65 74 3d 69 73 6f 2d 38  
0180 2d 31 0d 0a 0d 0a 3c 21 44 4f 43 54 59  
0190 48 54 4d 4c 20 50 55 42 4c 49 43 20 22  
01a0 49 45 54 46 2f 2f 44 54 44 20 48 54 4d  
01b0 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d  
01c0 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e

- When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n

The permission field has been added as a new field. This is included because, along with our request, we supplied the server a username and password indicating that we were permitted to see the page.

\*WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Time	Source	Destination	Protocol	Length	Info
156 07:31:26.412004	172.31.98.151	128.119.245.12	HTTP	549	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
167 07:31:26.801370	128.119.245.12	172.31.98.151	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
422 07:31:36.900400	172.31.98.151	128.119.245.12	HTTP	634	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
432 07:31:37.295061	128.119.245.12	172.31.98.151	HTTP	544	HTTP/1.1 200 OK (text/html)

> Frame 422: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface \Device\NPF\_{185BC2D4-588F-4111-8BE5-600000000000} (08:00:27:00:00:00), Dst: ArubaaHe\_cd:eb:28 (6c:f3:7f:cd:eb:28)

> Ethernet II, Src: IntelCor\_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaaHe\_cd:eb:28 (6c:f3:7f:cd:eb:28)

> Internet Protocol Version 4, Src: 172.31.98.151, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 65159, Dst Port: 80, Seq: 1, Ack: 1, Len: 580

> Hypertext Transfer Protocol

> GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.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 d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmcs=\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/118.0.0.0 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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/protected\_pages/HTTP-wireshark-file5.html]

[HTTP request 1/1]

[Response in frame: 432]

00c0 78 2d 61 67 65 3d 30 0d 0a  
00d0 7a 61 74 69 6f 6e 3a 20 42  
00e0 6c 79 5a 58 4e 6f 59 58 4a  
00f0 52 6c 62 6e 52 7a 4f 6d 35  
0100 73 3d 0d 0a 55 70 67 72 61  
0110 63 75 72 65 2d 52 65 71 75  
0120 0d 0a 55 73 65 72 2d 41 67  
0130 7a 69 6c 6c 61 2f 35 2e 30  
0140 77 73 20 4e 54 20 31 30 2e  
0150 34 3b 20 78 36 34 29 20 41  
0160 4b 69 74 2f 35 33 37 2e 33  
0170 4c 2c 20 6c 69 6b 65 20 47  
0180 68 72 6f 6d 65 2f 31 31 38  
0190 53 61 66 61 72 69 2f 35 33  
01a0 67 2f 31 31 38 2e 30 2e 32  
01b0 0a 41 63 63 65 70 74 3a 20  
01c0 6d 6c 2c 61 70 70 6c 69 63  
01d0 68 74 6d 6c 2b 78 6d 6c 2c  
01e0 74 69 6f 6e 2f 78 6d 6c 3b  
01f0 6d 61 67 65 2f 77 65 62 70  
0200 61 70 6e 67 2c 2a 2f 2a 3b  
0210 70 70 6c 69 63 61 74 69 6f  
0220 64 2d 65 78 63 68 61 6e 67