

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**  
**TRƯỜNG ĐẠI HỌC BÁCH KHOA**  
**KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH**



**MẠNG MÁY TÍNH THỰC HÀNH - CO3094**

---

**Báo cáo:**

**Lab2a**

---

**Giảng viên hướng dẫn:** Vũ Thành Tài

**Sinh viên:** Lê Đức Cường

Thành phố Hồ Chí Minh, tháng 3 năm 2025



## 1 The Basic HTTP GET/response interaction

### 1.1 Question 1

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

My browser is running HTTP version 1.1

The server is also running HTTP version 1.1.

148...	152.831202	192.168.31.87	128.119.245.12	HTTP	568 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
148...	153.091865	128.119.245.12	192.168.31.87	HTTP	540 HTTP/1.1 200 OK (text/html)
148...	153.260964	192.168.31.87	128.119.245.12	HTTP	514 GET /favicon.ico HTTP/1.1
149...	153.522450	128.119.245.12	192.168.31.87	HTTP	538 HTTP/1.1 404 Not Found (text/html)

### 1.2 Question 2

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

My browser indicates that it will accept English-US and English languages from the server.

### 1.3 Question 3

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

The IP address of my computer is 192.168.31.87

The IP address of the server is 128.119.245.12

### 1.4 Question 4

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

The status code returned was 200 OK

### 1.5 Question 5

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

The file was last modified on Thursday, March 13, 2025 at 05:59:01 GMT

```
▶ Frame 14855: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
▶ Ethernet II, Src: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f), Dst: Intel_93:30:aa (54:6c:00:93:30:aa)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.31.87
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50133, Seq: 1, Ack: 515, Len: 486
- Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 13 Mar 2025 09:34:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.18.0\r\n
    Last-Modified: Thu, 13 Mar 2025 05:59:01 GMT\r\n
    ETag: "80-6303304c1ed01"\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
    [Request in frame: 14817]
    [Time since request: 0.260663000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file1.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
  ▶ Line-based text data: text/html (4 lines)
```

## 1.6 Question 6

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

128 bytes of content are being returned

## 1.7 Question 7

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

No

# 2 The HTTP CONDITIONAL GET/response interaction

## 2.1 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?

No there is no IF-MODIFIED-SINCE line in the GET message.



## 2.2 Question 9

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

Yes, I saw it in the packet the server return.

```
▶ Frame 6424: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF...
▶ Ethernet II, Src: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f), Dst: Intel_93:30:aa (54:6c:eb:93:30:aa)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.31.87
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 52769, Seq: 1, Ack: 515, Len: 730
▶ Hypertext Transfer Protocol
  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
```

## 2.3 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?

Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage

```
▶ Ethernet II, Src: Intel_93:30:aa (54:6c:eb:93:30:aa), Dst: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f)
▶ Internet Protocol Version 4, Src: 192.168.31.87, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 60975, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
▶ 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/80.0.4012.91 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n
  If-None-Match: "173-6303304c1e531"\r\n
  If-Modified-Since: Thu, 13 Mar 2025 05:59:01 GMT\r\n
  \r\n
  [Response in frame: 7427]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

## 2.4 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 HTTP status code is “304: Not Modified”

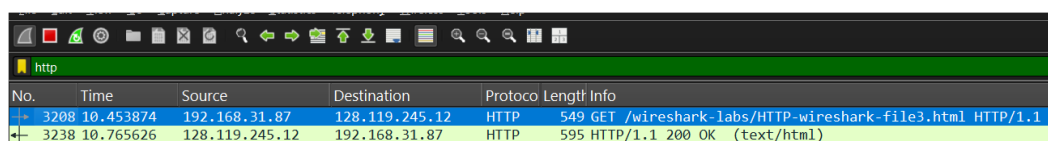
The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.

## 3 Retrieving Long Documents

### 3.1 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?

My browser only sent 1 HTTP GET request to the server. The Packet that contained the GET message was packet number 3208.

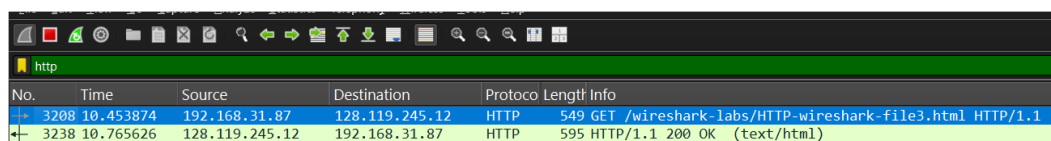


No.	Time	Source	Destination	Protocol	Length	Info
3208	10.453874	192.168.31.87	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3238	10.765626	128.119.245.12	192.168.31.87	HTTP	595	HTTP/1.1 200 OK (text/html)

### 3.2 Question 13

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

The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 3238.



No.	Time	Source	Destination	Protocol	Length	Info
3208	10.453874	192.168.31.87	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3238	10.765626	128.119.245.12	192.168.31.87	HTTP	595	HTTP/1.1 200 OK (text/html)

### 3.3 Question 14

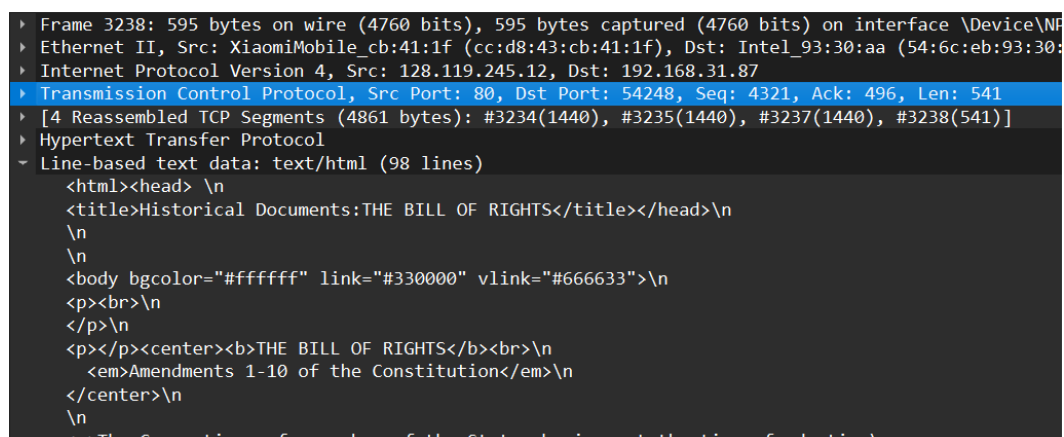
What is the status code and phrase in the response?

The code and phrase in the response was 200 OK

### 3.4 Question 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 four.



```
Frame 3238: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF...
Ethernet II, Src: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f), Dst: Intel_93:30:aa (54:6c:eb:93:30:aa)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.31.87
Transmission Control Protocol, Src Port: 80, Dst Port: 54248, Seq: 4321, Ack: 496, Len: 541
[4 Reassembled TCP Segments (4861 bytes): #3234(1440), #3235(1440), #3237(1440), #3238(541)]
Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
<html><head> \n
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
\n
\n
<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
<p><br>\n
</p>\n
<p></p><center><b>THE BILL OF RIGHTS</b><br>\n
<em>Amendments 1-10 of the Constitution</em>\n
</center>\n
\n
\n
<p>The Conventions of a number of the States having at the time of adopting...
```

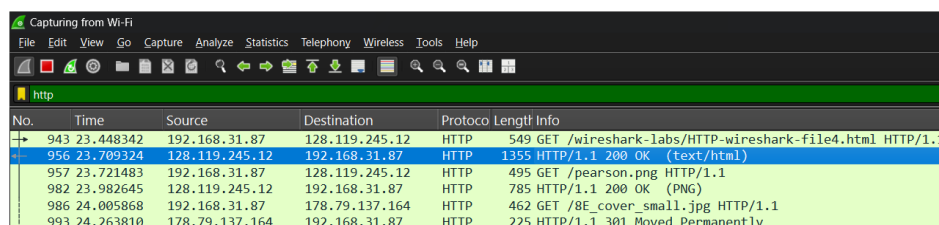
## 4 HTML Documents with Embedded Objects

### 4.1 Question 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.

- Initial Page address: 128.119.245.12
- pearson: 128.119.245.12
- 8E\_cover\_small: 178.79.137.164



No.	Time	Source	Destination	Protocol	Length	Info
943	23.448342	192.168.31.87	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
956	23.709324	128.119.245.12	192.168.31.87	HTTP	1355	HTTP/1.1 200 OK (text/html)
957	23.721483	192.168.31.87	128.119.245.12	HTTP	495	GET /pearson.png HTTP/1.1
982	23.982645	128.119.245.12	192.168.31.87	HTTP	785	HTTP/1.1 200 OK (PNG)
986	24.005868	192.168.31.87	178.79.137.164	HTTP	462	GET /8E_cover_small.jpg HTTP/1.1
993	24.263810	178.79.137.164	192.168.31.87	HTTP	225	HTTP/1.1 301 Moved Permanently

### 4.2 Question 17

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

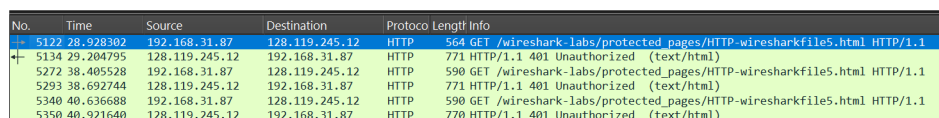
I think my browser downloaded the two images sequentially because the arrival times of the two images are different.

## 5 HTTP Authentication

### 5.1 Question 18

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

The servers initial response was "401 Unauthorized "



No.	Time	Source	Destination	Protocol	Length	Info
5122	28.928382	192.168.31.87	128.119.245.12	HTTP	564	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
5134	29.200795	128.119.245.12	192.168.31.87	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
5272	38.405528	192.168.31.87	128.119.245.12	HTTP	590	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
5293	38.692744	128.119.245.12	192.168.31.87	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
5340	40.636688	192.168.31.87	128.119.245.12	HTTP	590	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
5350	40.921640	128.119.245.12	192.168.31.87	HTTP	770	HTTP/1.1 401 Unauthorized (text/html)



## 5.2 Question 19

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

I think it is Authorization.

No.	Time	Source	Destination	Protocol	Length	Info
5122	28.928302	192.168.31.87	128.119.245.12	HTTP	564	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
5134	29.204795	128.119.245.12	192.168.31.87	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
5272	38.405528	192.168.31.87	128.119.245.12	HTTP	598	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
5293	38.692744	128.119.245.12	192.168.31.87	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
5340	40.636688	192.168.31.87	128.119.245.12	HTTP	598	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
5350	40.921640	128.119.245.12	192.168.31.87	HTTP	778	HTTP/1.1 401 Unauthorized (text/html)
8211	236.017355	192.168.31.87	128.119.245.12	HTTP	598	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
8221	236.288593	128.119.245.12	192.168.31.87	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
126.	342.509719	192.168.31.87	128.119.245.12	HTTP	617	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
126.	342.771876	128.119.245.12	192.168.31.87	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
126.	343.992846	192.168.31.87	128.119.245.12	HTTP	598	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
126.	344.253985	128.119.245.12	192.168.31.87	HTTP	778	HTTP/1.1 401 Unauthorized (text/html)
258.	540.220089	192.168.31.87	128.119.245.12	HTTP	624	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
258.	540.488355	128.119.245.12	192.168.31.87	HTTP	583	HTTP/1.1 404 Not Found (text/html)

Frame 25888: 649 bytes on wire (5192 bits), 649 bytes captured (5192 bits) on interface \Device\NPF{...}	0030	82 05 57 f1 00 00 87 45 54 20 2f 77 69 72 65 73	W...GET /wires
Ethernet II, Src: Intel 93:30:aa (54:6c:eb:93:30:aa), Dst: XiaomiMobile_cb41:1f (cc:d8:43:cb41:1f)	0040	68 61 72 6b 2d 6e 61 62 73 2f 70 72 6f 74 65 63	hark-lab s/protoc
Internet Protocol Version 4, Src: 192.168.31.87, Dst: 128.119.245.12	0050	74 65 64 5f 70 61 67 65 73 2f 48 54 54 50 2d 77	ted_page s/HTTP-w
Transmission Control Protocol, Src Port: 56559, Dst Port: 80, Seq: 1, Ack: 1, Len: 595	0060	69 72 65 73 68 61 72 6b 6e 69 6c 65 35 2e 68 74	reshark file5.ht
Hypertext Transfer Protocol	0070	6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73	ml HTTP/1.1, 404
GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n	0080	74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73	t: gala, cs.umass
Request Method: GET	0090	2e 65 64 75 0d 0a 43 6f 6e 65 63 74 69 6f 6e	.edu-co nnection
Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html	00a0	3a 20 60 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61	. keep-a live-ca
Request Version: HTTP/1.1	00b0	63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78	che-Cont rol: max
Host: gaia.cs.umass.edu\r\n	00c0	2d 61 67 65 3d 30 0d 0a 41 75 74 68 6f 72 69 7a	age-d- Authoriz
Connection: keep-alive\r\n	00d0	61 74 69 6f 6e 3a 20 42 61 73 69 61 20 64 32 6c	e-Icon: B asic-d21
Cache-Control: max-age=0\r\n	00e0	79 5a 58 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 52	yZNovX3 rLXNkdR
Authorization: Basic d2lyZMOvX3JlXW0ddklbnk2Om5ldhdvcms=\r\n	00f0	6c 62 6e 52 7a 4f 6d 35 6c 64 68 64 76 63 6d 73	lbnk2Om5ldhdvcms
Upgrade-Insecure-Requests: 1\r\n	0100	3d 8d 0a 55 70 67 72 61 64 6c 2d 49 6e 73 65 63	--Upgra de Insec
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36	0110	75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d	ure-Requ ests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng	0120	0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a	-User-Ag ents: Moz
Accept-encoding: gzip, deflate\r\n	0130	69 6c 6c 61 2f 35 2e 30 20 20 57 69 6e 64 6f 77	11la/5.0 (window
Accept-language: vi,en-US;q=0.9,en;q=0.8\r\n			
\r\n			