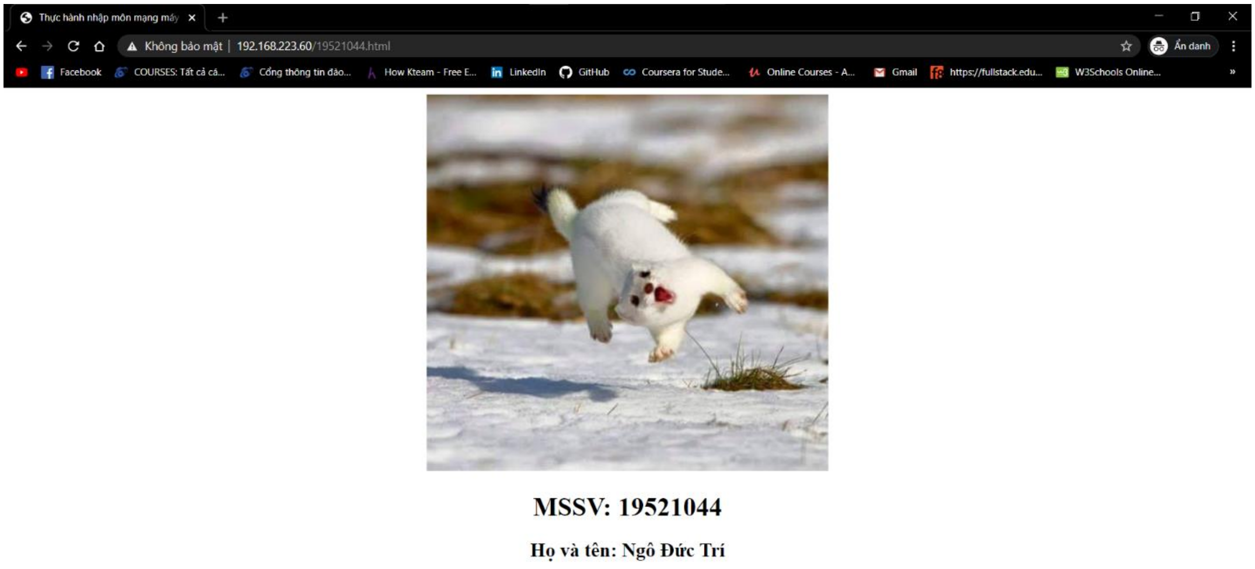
LAB2:PHÂN TÍCH GÓI TIN HTTP VỚI WIRESHARK



MSSV: 19521044

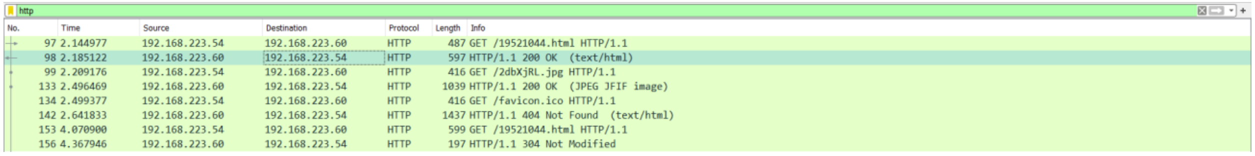
Họ và tên: Ngô Đức Trí

ĐÂY LÀ TRANG WEB ĐÃ LẤY ĐƯỢC CỦA BẠN NGÔ ĐỨC TRÍ

Câu 1:

Trình duyệt dùng phiên bản HTTP/1.1

Phiên bản HTTP server đang sử dụng là phiên bản HTTP/1.1

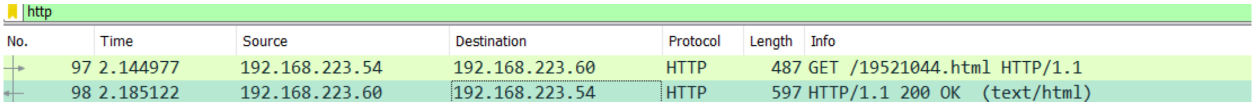


No.	Time	Source	Destination	Protocol	Length	Info
97	2.144977	192.168.223.54	192.168.223.60	HTTP	487	GET /19521044.html HTTP/1.1
98	2.185122	192.168.223.60	192.168.223.54	HTTP	597	HTTP/1.1 200 OK (text/html)
99	2.209176	192.168.223.54	192.168.223.60	HTTP	416	GET /2dbXjRL.jpg HTTP/1.1
133	2.496469	192.168.223.60	192.168.223.54	HTTP	1039	HTTP/1.1 200 OK (JPEG JFIF image)
134	2.499377	192.168.223.54	192.168.223.60	HTTP	416	GET /favicon.ico HTTP/1.1
142	2.641833	192.168.223.60	192.168.223.54	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
153	4.070900	192.168.223.54	192.168.223.60	HTTP	599	GET /19521044.html HTTP/1.1
156	4.367946	192.168.223.60	192.168.223.54	HTTP	197	HTTP/1.1 304 Not Modified

Câu 2:

Địa chỉ IP máy tinh là: 192.168.224.54

Địa chỉ IP Web Server là 192.168.223.60

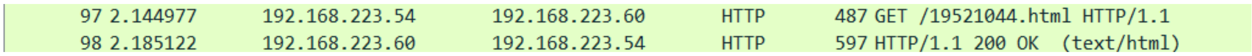


No.	Time	Source	Destination	Protocol	Length	Info
97	2.144977	192.168.223.54	192.168.223.60	HTTP	487	GET /19521044.html HTTP/1.1
98	2.185122	192.168.223.60	192.168.223.54	HTTP	597	HTTP/1.1 200 OK (text/html)

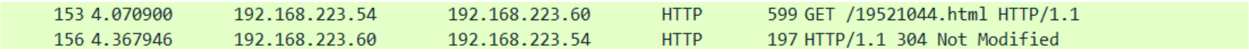
Câu 3:

Mã trạng thái (status code) lần đầu tiên truy cập là:200

Mã trạng thái (stastus code) lần thứ 2 truy cập là:304



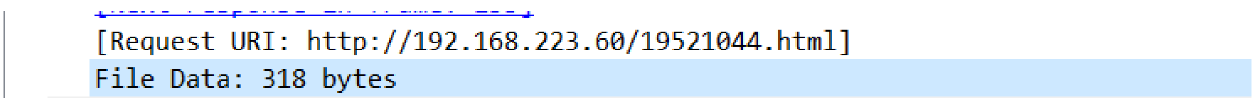
```
 97 2.144977    192.168.223.54    192.168.223.60    HTTP    487 GET /19521044.html HTTP/1.1
 98 2.185122    192.168.223.60    192.168.223.54    HTTP    597 HTTP/1.1 200 OK  (text/html)
```



```
153 4.070900    192.168.223.54    192.168.223.60    HTTP    599 GET /19521044.html HTTP/1.1
156 4.367946    192.168.223.60    192.168.223.54    HTTP    197 HTTP/1.1 304 Not Modified
```

Câu 4:

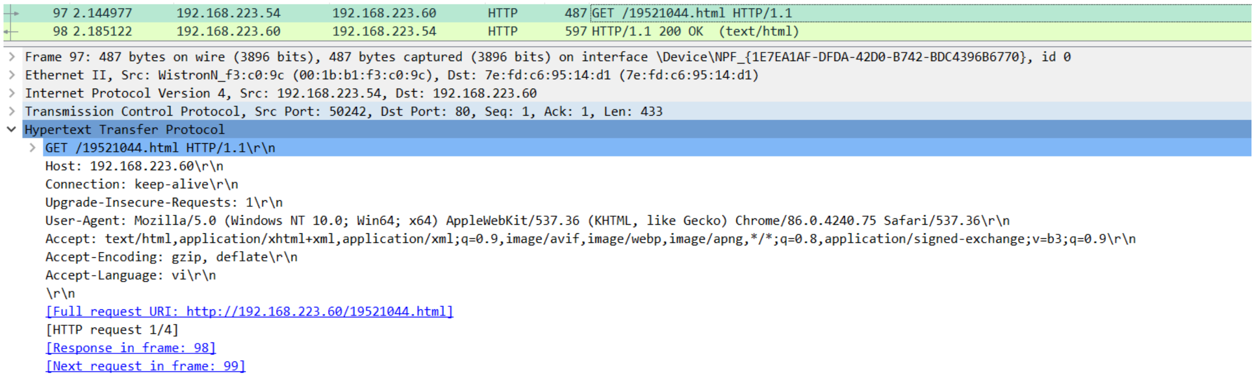
Server đã trả về cho trình duyệt 318 bytes nội dung



```
[Request URI: http://192.168.223.60/19521044.html]
File Data: 318 bytes
```

Câu 5:

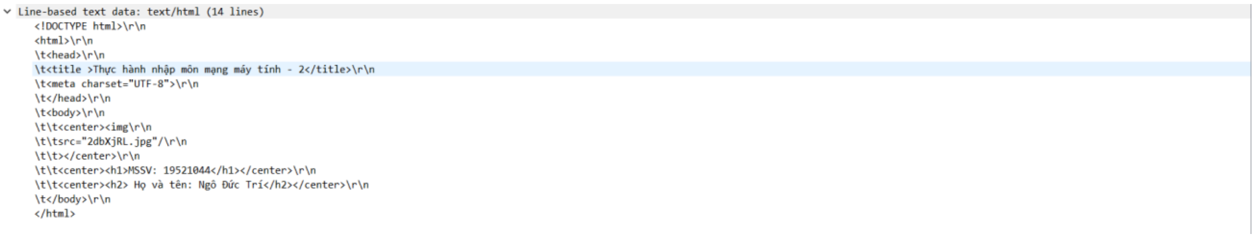
Không tìm thấy được dòng “IF-MODIFIEDSINCE” nội dung HTTP GET thứ 1



```
 97 2.144977   192.168.223.54   192.168.223.60   HTTP   487 GET /19521044.html HTTP/1.1
 98 2.185122   192.168.223.60   192.168.223.54   HTTP   597 HTTP/1.1 200 OK  (text/html)
> Frame 97: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF_{1E7EA1AF-DFDA-42D0-B742-BDC4396B6770}, id 0
> Ethernet II, Src: WistronN_f3:c0:9c (00:1b:b1:f3:c0:9c), Dst: 7e:fd:c6:95:14:d1 (7e:fd:c6:95:14:d1)
> Internet Protocol Version 4, Src: 192.168.223.54, Dst: 192.168.223.60
> Transmission Control Protocol, Src Port: 50242, Dst Port: 80, Seq: 1, Ack: 1, Len: 433
v Hypertext Transfer Protocol
  > GET /19521044.html HTTP/1.1\r\n
    Host: 192.168.223.60\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/86.0.4240.75 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\r\n
    \r\n
    [Full request URI: http://192.168.223.60/19521044.html]
    [HTTP request 1/4]
    [Response in frame: 98]
    [Next request in frame: 99]
```

Câu 6:

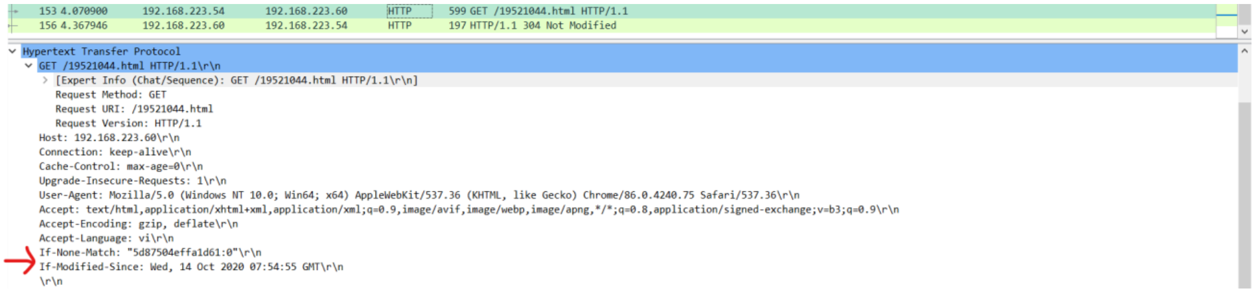
Server đã trả về nội dung của file HTML .Vì đây là lần đầu tiên mà Client gửi Request đến Server nên Server phản hồi lại file HTML đó



```
v Line-based text data: text/html (14 lines)
    <!DOCTYPE html>\r\n
    <html>\r\n
    \t<head>\r\n
    \t<title >Thực hành nhập môn mạng máy tính - 2</title>\r\n
    \t<meta charset="UTF-8">\r\n
    \t</head>\r\n
    \t<body>\r\n
    \t\t<center><img\r\n
    \t\tsrc="2dbXjRL.jpg"/\r\n
    \t\t></center>\r\n
    \t\t<center><h1>MSSV: 19521044</h1></center>\r\n
    \t\t<center><h2> Họ và tên: Ngô Đức Trí</h2></center>\r\n
    \t</body>\r\n
    </html>
```

Câu 7:

Nội dung của HTTP GET thứ 2 đã tìm thấy dòng “IF-MODIFIEDSINCE”



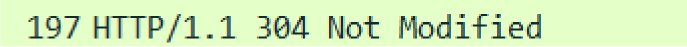
```
    153 4.070900    192.168.223.54    192.168.223.60    HTTP    599 GET /19521044.html HTTP/1.1
    156 4.367946    192.168.223.60    192.168.223.54    HTTP    197 HTTP/1.1 304 Not Modified

v Hypertext Transfer Protocol
  v GET /19521044.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /19521044.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /19521044.html
      Request Version: HTTP/1.1
    Host: 192.168.223.60\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/86.0.4240.75 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\r\n
    If-None-Match: "5d87504effa1d61:0"\r\n
    If-Modified-Since: Wed, 14 Oct 2020 07:54:55 GMT\r\n
    \r\n
```

Giá trị của IF-MODIFIED-SINCE là: Wed, 14 Oct 2020 07:54:55 GMT

Câu 8:

Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là 304 Not Modified



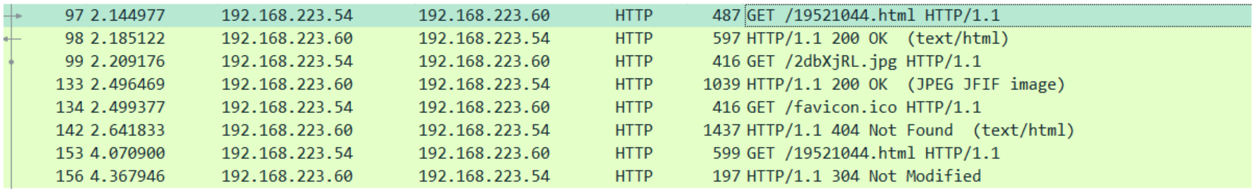
```
197 HTTP/1.1 304 Not Modified
```

304: có nghĩa là máy chủ chỉ ra không có gì thay đổi trang Web sau khi đã được Refresh thì URL cũng không cần chỉnh sửa lại

Server không thật sự gửi về nội dung của file .Vì nó đã được lưu trên cache của máy trước đó rồi

Câu 9:

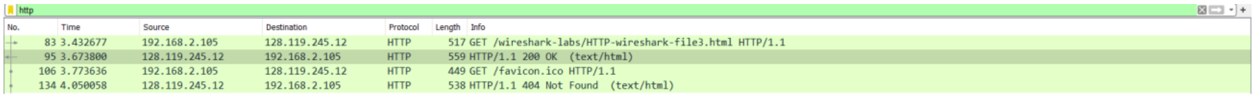
Trình duyệt đã gửi 4 HTTP GET. Đến địa chỉ IP là 192.168.223.60



```
 97 2.144977    192.168.223.54    192.168.223.60    HTTP     487 GET /19521044.html HTTP/1.1
 98 2.185122    192.168.223.60    192.168.223.54    HTTP     597 HTTP/1.1 200 OK  (text/html)
 99 2.209176    192.168.223.54    192.168.223.60    HTTP     416 GET /2dbXjRL.jpg HTTP/1.1
133 2.496469    192.168.223.60    192.168.223.54    HTTP    1039 HTTP/1.1 200 OK  (JPEG JFIF image)
134 2.499377    192.168.223.54    192.168.223.60    HTTP     416 GET /favicon.ico HTTP/1.1
142 2.641833    192.168.223.60    192.168.223.54    HTTP    1437 HTTP/1.1 404 Not Found  (text/html)
153 4.070900    192.168.223.54    192.168.223.60    HTTP     599 GET /19521044.html HTTP/1.1
156 4.367946    192.168.223.60    192.168.223.54    HTTP     197 HTTP/1.1 304 Not Modified
```

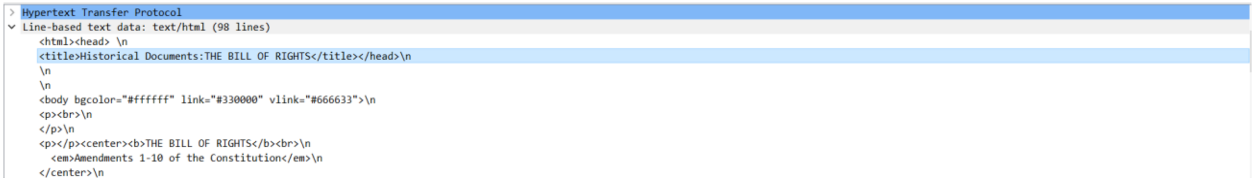
Câu 10:

Trình duyêt đã gửi 2 HTTP GET nhưng HTTP GET đầu tiên với HTTP/1.1.200 OK(text.html) là gói tin đã được Request thành công.



```
http
No.     Time        Source           Destination      Protocol  Length  Info
     83 3.432677    192.168.2.105    128.119.245.12   HTTP      517 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
     95 3.673800    128.119.245.12   192.168.2.105    HTTP      559 HTTP/1.1 200 OK  (text/html)
    106 3.773636    192.168.2.105    128.119.245.12   HTTP      449 GET /favicon.ico HTTP/1.1
    134 4.050058    128.119.245.12   192.168.2.105    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

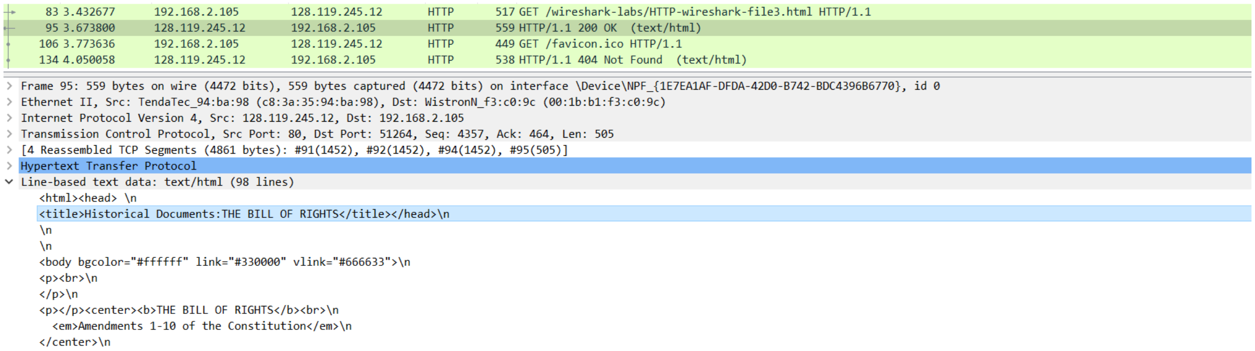
Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ 1 với HTTP/1.1 200 OK(text.html)



```
> Hypertext Transfer Protocol
v 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
```

Câu 11:

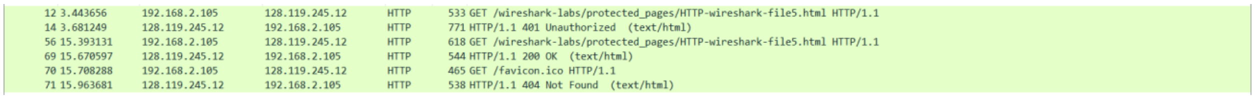
Cần 1 TCP segments để chứa hết HTTP response và nội dung của The Bill of Right



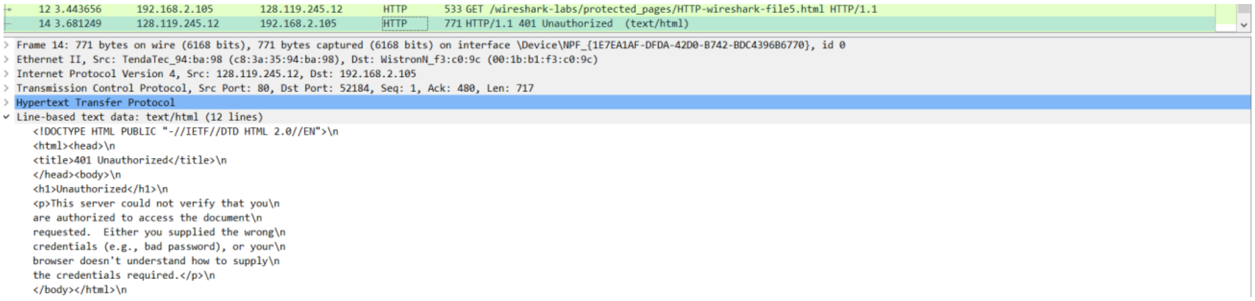
```
   83 3.432677     192.168.2.105     128.119.245.12    HTTP     517 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   95 3.673800     128.119.245.12    192.168.2.105     HTTP     559 HTTP/1.1 200 OK  (text/html)
  106 3.773636     192.168.2.105     128.119.245.12    HTTP     449 GET /favicon.ico HTTP/1.1
  134 4.050058     128.119.245.12    192.168.2.105     HTTP     538 HTTP/1.1 404 Not Found  (text/html)

> Frame 95: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{1E7EA1AF-DFDA-42D0-B742-BDC4396B6770}, id 0
> Ethernet II, Src: TendaTec_94:ba:98 (c8:3a:35:94:ba:98), Dst: WistronN_f3:c0:9c (00:1b:b1:f3:c0:9c)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.105
> Transmission Control Protocol, Src Port: 80, Dst Port: 51264, Seq: 4357, Ack: 464, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #91(1452), #92(1452), #94(1452), #95(505)]
> Hypertext Transfer Protocol
v 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
```

Câu 12:



```
   12 3.443656    192.168.2.105     128.119.245.12    HTTP    533 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   14 3.681249    128.119.245.12    192.168.2.105     HTTP    771 HTTP/1.1 401 Unauthorized  (text/html)
   56 15.393131   192.168.2.105     128.119.245.12    HTTP    618 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   69 15.670597   128.119.245.12    192.168.2.105     HTTP    544 HTTP/1.1 200 OK  (text/html)
   70 15.708288   192.168.2.105     128.119.245.12    HTTP    465 GET /favicon.ico HTTP/1.1
   71 15.963681   128.119.245.12    192.168.2.105     HTTP    538 HTTP/1.1 404 Not Found  (text/html)
```

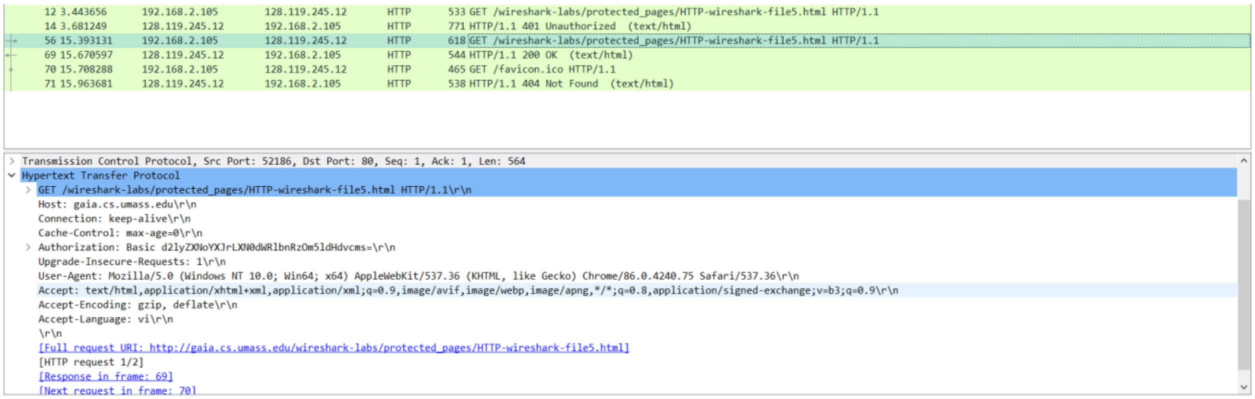


```
  12 3.443656    192.168.2.105     128.119.245.12    HTTP    533 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  14 3.681249    128.119.245.12    192.168.2.105     HTTP    771 HTTP/1.1 401 Unauthorized  (text/html)

> Frame 14: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{1E7EA1AF-DFDA-42D0-B742-BDC4396B6770}, id 0
> Ethernet II, Src: TendaTec_94:ba:98 (c8:3a:35:94:ba:98), Dst: WistronN_f3:c0:9c (00:1b:b1:f3:c0:9c)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.105
> Transmission Control Protocol, Src Port: 80, Dst Port: 52184, Seq: 1, Ack: 480, Len: 717
> Hypertext Transfer Protocol
v Line-based text data: text/html (12 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>401 Unauthorized</title>\n
    </head><body>\n
    <h1>Unauthorized</h1>\n
    <p>This server could not verify that you\n
    are authorized to access the document\n
    requested.  Either you supplied the wrong\n
    credentials (e.g., bad password), or your\n
    browser doesn't understand how to supply\n
    the credentials required.</p>\n
    </body></html>\n
```

Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là 401 Unauthorized:Yêu cầu chứng thực

Câu 13:



```
   12 3.443656    192.168.2.105     128.119.245.12    HTTP    533 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   14 3.681249    128.119.245.12    192.168.2.105     HTTP    771 HTTP/1.1 401 Unauthorized  (text/html)
   56 15.393131   192.168.2.105     128.119.245.12    HTTP    618 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   69 15.670597   128.119.245.12    192.168.2.105     HTTP    544 HTTP/1.1 200 OK  (text/html)
   70 15.708288   192.168.2.105     128.119.245.12    HTTP    465 GET /favicon.ico HTTP/1.1
   71 15.963681   128.119.245.12    192.168.2.105     HTTP    538 HTTP/1.1 404 Not Found  (text/html)

> Transmission Control Protocol, Src Port: 52186, Dst Port: 80, Seq: 1, Ack: 1, Len: 564
v 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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 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\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/2]
    [Response in frame: 69]
    [Next request in frame: 70]
```

Khi thực hiện xong đăng nhập username và password,thì khi đó trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới xuất hiện trong HTTP GET thứ 2 là:Authorization

Authorization với mã là Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

Tài khoản và mật khẩu đã được mã hóa tại đây để đảm bảo an toàn cho mỗi Client