Câu 1:

- Trình duyệt đang sử dụng là 1.1

```
321 12.566126    192.168.135.157    192.168.135.193    HTTP    539 GET /21522243.html HTTP/1.1
```

- Phiên bản HTTP Server đang sử dụng là HTTP/1.1\r\n

```
Hypertext Transfer Protocol
  GET /21522243.html HTTP/1.1\r\n
```

Câu 2:

- Địa chỉ IP của máy là 192.168.135.157 (mạng 4g tự phát)

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::30a0:89d9:a2fe:c770%17
   IPv4 Address. . . . . . . . . . . : 192.168.135.157
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.135.177
```

- Địa chỉ IP của web server là 192.168.135.193

```
321 12.566126    192.168.135.157    192.168.135.193    HTTP    539 GET /21522243.html HTTP/1.1
```

Câu 3:

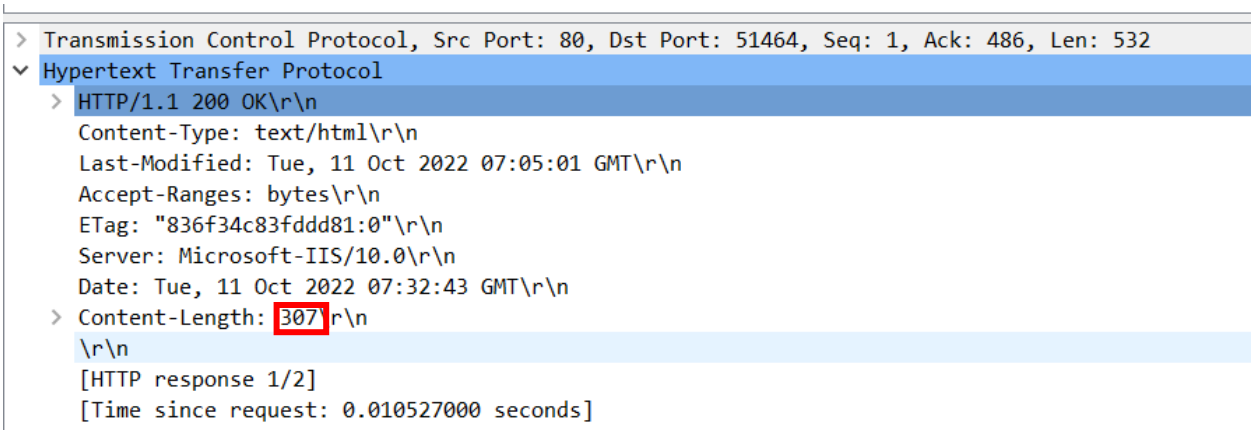
- Mã trạng thái trả về từ server: HTTP/1.1 200 OK\r\n (200)

```
No.  Time        Source           Destination      Protocol  Length  Info
321  12.566126   192.168.135.157  192.168.135.193  HTTP      539     GET /21522243.html HTTP/1.1
322  12.576653   192.168.135.193  192.168.135.157  HTTP      586     HTTP/1.1 200 OK  (text/html)
327  12.653299   192.168.135.157  118.69.123.142   HTTP      496     GET /Styles/profi/images/logo186x150.png HTTP/1.1
329  12.724602   118.69.123.142   192.168.135.157  HTTP      445     HTTP/1.1 301 Moved Permanently  (text/html)
385  26.867078   192.168.135.157  192.168.135.193  HTTP      651     GET /21522243.html HTTP/1.1
386  26.916806   192.168.135.193  192.168.135.157  HTTP      197     HTTP/1.1 304 Not Modified
```

```
Transmission Control Protocol, Src Port: 80, Dst Port: 51464, Seq: 1, Ack: 486, Len: 532
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Content-Type: text/html\r\n
  Last-Modified: Tue, 11 Oct 2022 07:05:01 GMT\r\n
  Accept-Ranges: bytes\r\n
  ETag: "836f34c83fddd81:0"\r\n
  Server: Microsoft-IIS/10.0\r\n
  Date: Tue, 11 Oct 2022 07:32:43 GMT\r\n
  Content-Length: 307\r\n
```

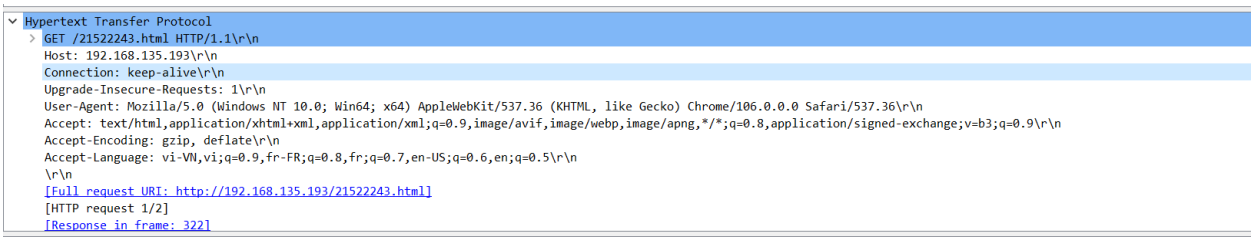
Câu 4:

- Server đã trả về cho trình duyệt 307 byte nội dung



Câu 5:

- Không có “IF – MODIFIED – SINCE”



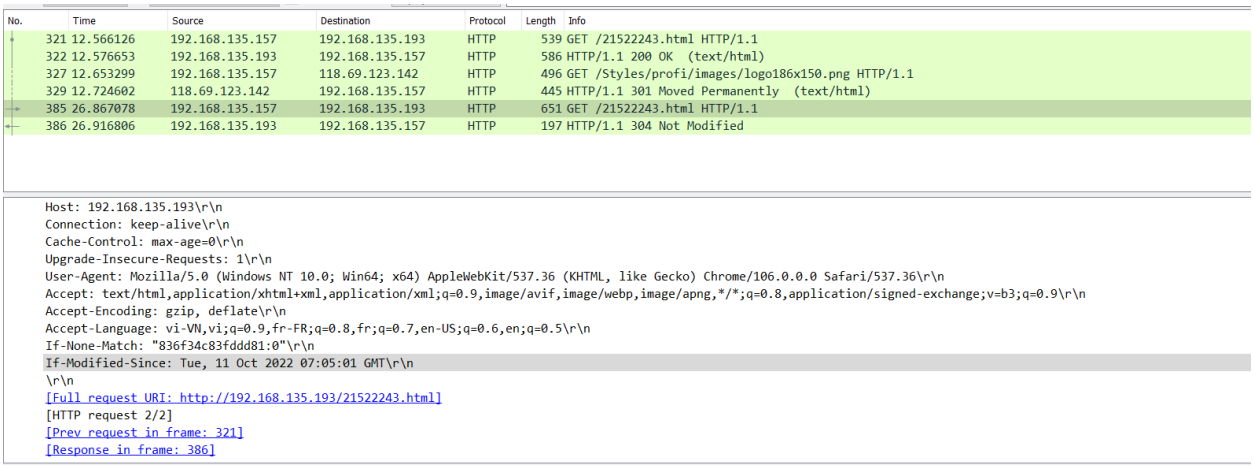
Câu 6:

- Server thật sự trả về nội dung của file HTML vì quá trình HTTP Request & HTTP Respone cơ bản diễn ra như sau: 1. Client yêu cầu file. 2. Server làm công việc đi tìm kiếm xem file ở đâu. *ở bước này nếu như file cần tim đã có sẵn ở bộ nhớ đệm cache thì sẽ lấy từ cache đem về còn nếu file yêu cầu thực sự chưa có ở cache thì sẽ thực hiện tiếp bước Server tìm thấy và trả về cho Client. 4. Client download file và hiển thị cho người dùng. - Như vậy ta thấy trong trường hợp này. Server có trả về nội dung của file HTML vì trước khi truy cập trang web ta đã xóa cache của trình duyệt, nên khi ta gởi Request GET đầu tiên lên server để yêu cầu server trả file về,file này chưa hề được lưu trong bộ nhớ Cache ở client nên sẽ tải file trực tiếp từ server

```
Hypertext Transfer Protocol
Line-based text data: text/html (13 lines)
    <!DOCTYPE html>\r\n
    <html>\r\n
    <head>\r\n
    <title>Thuc hanh nhap mon mang may tinh - 2</title>\r\n
    </head>\r\n
    <body>\r\n
    <center><img\r\n
    src="http://portal.uit.edu.vn/Styles/profi/images/logo186x150.png"/\r\n
    ></center>\r\n
    <center><h1>MSSV: 123456</h1></center>\r\n
    <center><h2> Ho va ten: Nguyen Van An</h2></center>\r\n
    </body>\r\n
    </html>
```

Câu 7:

- HTTP Get thứ 2 không có nhưng HTTP Get thứ 3 có, giá trị là: Tue, 11 Oct 2022 07:05:01 GMT\r\n

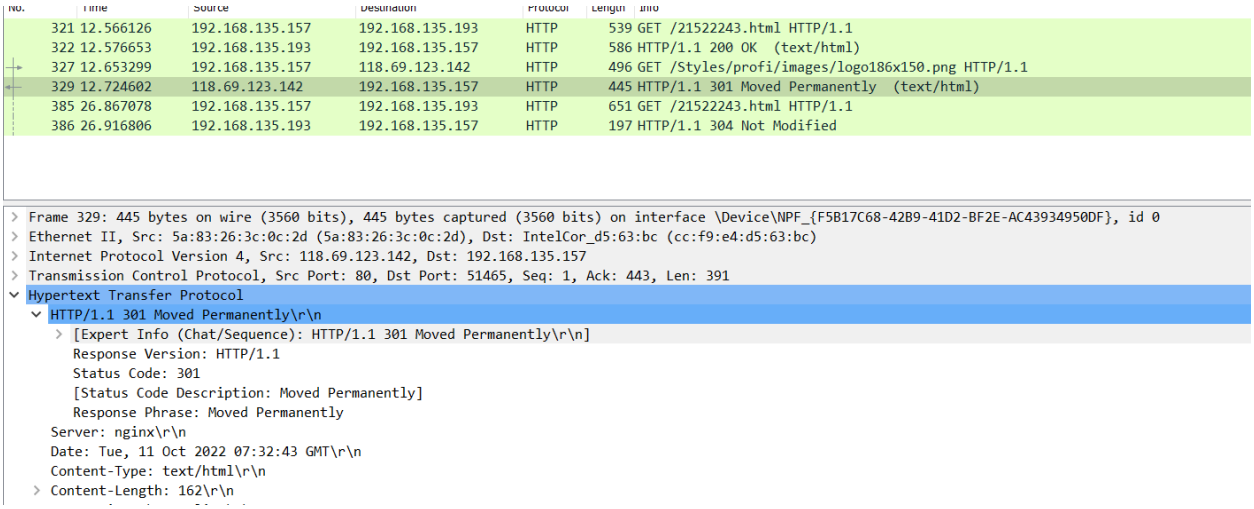


No.	Time	Source	Destination	Protocol	Length	Info
321	12.566126	192.168.135.157	192.168.135.193	HTTP	539	GET /21522243.html HTTP/1.1
322	12.576653	192.168.135.193	192.168.135.157	HTTP	586	HTTP/1.1 200 OK (text/html)
327	12.653299	192.168.135.157	118.69.123.142	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
329	12.724602	118.69.123.142	192.168.135.157	HTTP	445	HTTP/1.1 301 Moved Permanently (text/html)
385	26.867078	192.168.135.157	192.168.135.193	HTTP	651	GET /21522243.html HTTP/1.1
386	26.916806	192.168.135.193	192.168.135.157	HTTP	197	HTTP/1.1 304 Not Modified

```
Host: 192.168.135.193\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/106.0.0.0 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,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n
If-None-Match: "836f34c83fddd81:0"\r\n
If-Modified-Since: Tue, 11 Oct 2022 07:05:01 GMT\r\n
\r\n
[Full request URI: http://192.168.135.193/21522243.html]
[HTTP request 2/2]
[Prev request in frame: 321]
[Response in frame: 386]
```

Câu 8:

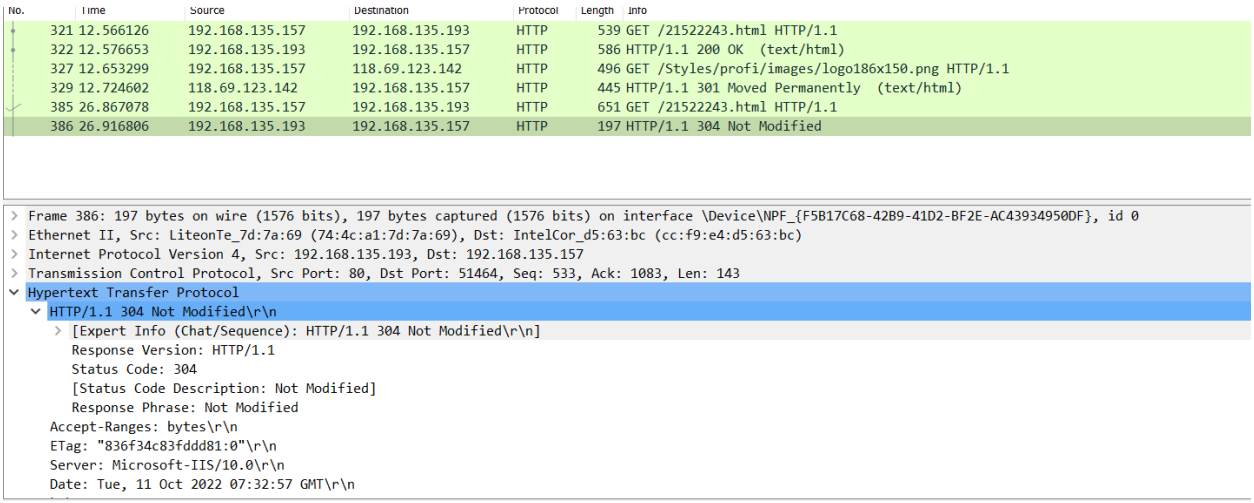
- HTTP Get thứ 2 là: HTTP/1.1 301 Moved Permanently\r\n (301, có nghĩa là URL của tài nguyên được yêu cầu đã được thay đổi vĩnh viễn. URL mới được đưa ra trong phản hồi.)



No.	Time	Source	Destination	Protocol	Length	Info
321	12.566126	192.168.135.157	192.168.135.193	HTTP	539	GET /21522243.html HTTP/1.1
322	12.576653	192.168.135.193	192.168.135.157	HTTP	586	HTTP/1.1 200 OK (text/html)
327	12.653299	192.168.135.157	118.69.123.142	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
329	12.724602	118.69.123.142	192.168.135.157	HTTP	445	HTTP/1.1 301 Moved Permanently (text/html)
385	26.867078	192.168.135.157	192.168.135.193	HTTP	651	GET /21522243.html HTTP/1.1
386	26.916806	192.168.135.193	192.168.135.157	HTTP	197	HTTP/1.1 304 Not Modified

```
> Frame 329: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{F5B17C68-42B9-41D2-BF2E-AC43934950DF}, id 0
> Ethernet II, Src: 5a:83:26:3c:0c:2d (5a:83:26:3c:0c:2d), Dst: IntelCor_d5:63:bc (cc:f9:e4:d5:63:bc)
> Internet Protocol Version 4, Src: 118.69.123.142, Dst: 192.168.135.157
> Transmission Control Protocol, Src Port: 80, Dst Port: 51465, Seq: 1, Ack: 443, Len: 391
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
    Server: nginx\r\n
    Date: Tue, 11 Oct 2022 07:32:43 GMT\r\n
    Content-Type: text/html\r\n
  > Content-Length: 162\r\n
```

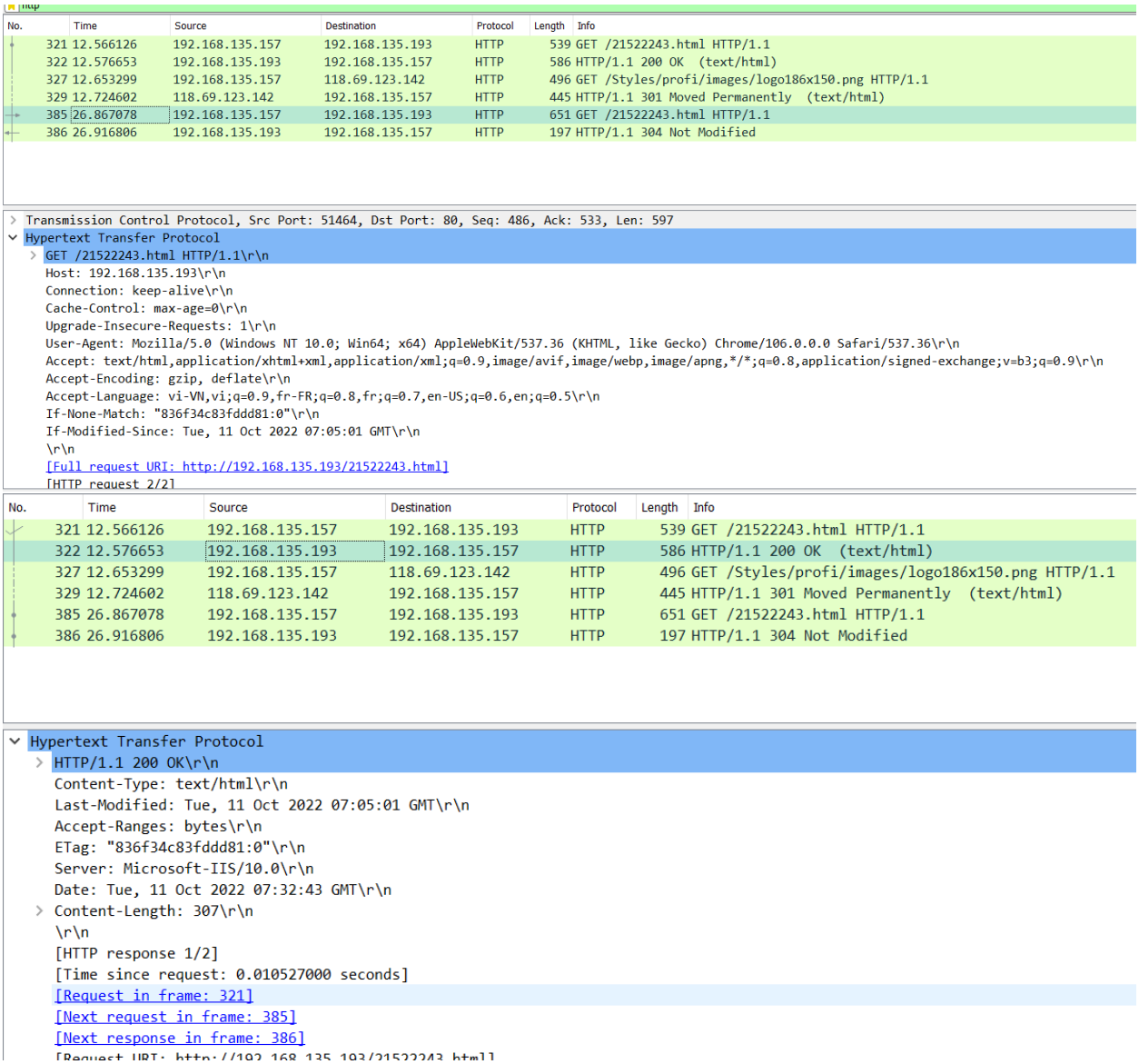
- HTTP Get thứ 3 là: HTTP/1.1 304 Not Modified\r\n (304, có nghĩa là điều này được sử dụng cho mục đích lưu vào bộ nhớ đệm. Nó cho máy khách biết rằng phản hồi chưa được sửa đổi, vì vậy máy khách có thể tiếp tục sử dụng cùng một phiên bản phản hồi được lưu trong bộ nhớ cache.)



No.	Time	Source	Destination	Protocol	Length	Info
321	12.566126	192.168.135.157	192.168.135.193	HTTP	539	GET /21522243.html HTTP/1.1
322	12.576653	192.168.135.193	192.168.135.157	HTTP	586	HTTP/1.1 200 OK (text/html)
327	12.653299	192.168.135.157	118.69.123.142	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
329	12.724602	118.69.123.142	192.168.135.157	HTTP	445	HTTP/1.1 301 Moved Permanently (text/html)
385	26.867078	192.168.135.157	192.168.135.193	HTTP	651	GET /21522243.html HTTP/1.1
386	26.916806	192.168.135.193	192.168.135.157	HTTP	197	HTTP/1.1 304 Not Modified

```
> Frame 386: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface \Device\NPF_{F5B17C68-42B9-41D2-BF2E-AC43934950DF}, id 0
> Ethernet II, Src: LiteonTe_7d:7a:69 (74:4c:a1:7d:7a:69), Dst: IntelCor_d5:63:bc (cc:f9:e4:d5:63:bc)
> Internet Protocol Version 4, Src: 192.168.135.193, Dst: 192.168.135.157
> Transmission Control Protocol, Src Port: 80, Dst Port: 51464, Seq: 533, Ack: 1083, Len: 143
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Accept-Ranges: bytes\r\n
    ETag: "836f34c83fddd81:0"\r\n
    Server: Microsoft-IIS/10.0\r\n
    Date: Tue, 11 Oct 2022 07:32:57 GMT\r\n
```

- Server không thực sự gửi nội dung của file



No.	Time	Source	Destination	Protocol	Length	Info
321	12.566126	192.168.135.157	192.168.135.193	HTTP	539	GET /21522243.html HTTP/1.1
322	12.576653	192.168.135.193	192.168.135.157	HTTP	586	HTTP/1.1 200 OK (text/html)
327	12.653299	192.168.135.157	118.69.123.142	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
329	12.724602	118.69.123.142	192.168.135.157	HTTP	445	HTTP/1.1 301 Moved Permanently (text/html)
385	26.867078	192.168.135.157	192.168.135.193	HTTP	651	GET /21522243.html HTTP/1.1
386	26.916806	192.168.135.193	192.168.135.157	HTTP	197	HTTP/1.1 304 Not Modified

```
Transmission Control Protocol, Src Port: 51464, Dst Port: 80, Seq: 486, Ack: 533, Len: 597
Hypertext Transfer Protocol
  GET /21522243.html HTTP/1.1\r\n
  Host: 192.168.135.193\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/106.0.0.0 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,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n
  If-None-Match: "836f34c83fddd81:0"\r\n
  If-Modified-Since: Tue, 11 Oct 2022 07:05:01 GMT\r\n
  \r\n
  [Full request URI: http://192.168.135.193/21522243.html]
  [HTTP request 2/2]
```

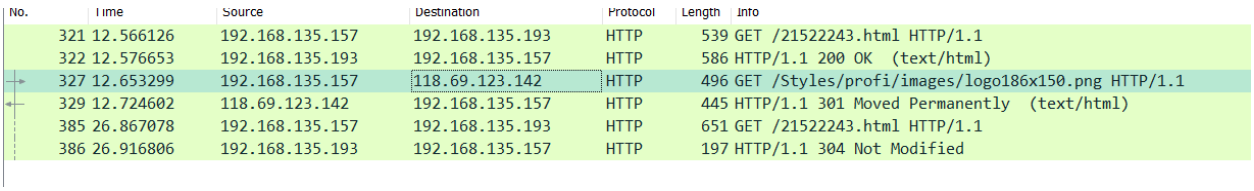
No.	Time	Source	Destination	Protocol	Length	Info
321	12.566126	192.168.135.157	192.168.135.193	HTTP	539	GET /21522243.html HTTP/1.1
322	12.576653	192.168.135.193	192.168.135.157	HTTP	586	HTTP/1.1 200 OK (text/html)
327	12.653299	192.168.135.157	118.69.123.142	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
329	12.724602	118.69.123.142	192.168.135.157	HTTP	445	HTTP/1.1 301 Moved Permanently (text/html)
385	26.867078	192.168.135.157	192.168.135.193	HTTP	651	GET /21522243.html HTTP/1.1
386	26.916806	192.168.135.193	192.168.135.157	HTTP	197	HTTP/1.1 304 Not Modified

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Content-Type: text/html\r\n
  Last-Modified: Tue, 11 Oct 2022 07:05:01 GMT\r\n
  Accept-Ranges: bytes\r\n
  ETag: "836f34c83fddd81:0"\r\n
  Server: Microsoft-IIS/10.0\r\n
  Date: Tue, 11 Oct 2022 07:32:43 GMT\r\n
  Content-Length: 307\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.010527000 seconds]
  [Request in frame: 321]
  [Next request in frame: 385]
  [Next response in frame: 386]
  [Request URI: http://192.168.135.193/21522243.html]
```

- Ở hình ảnh trên giúp ta so sánh được giữa lần GET 1 và lần GET 2, ở lần GET đầu tiên file chúng ta request không có sẵn trong cache nên ta phải lên trực tiếp server để lấy về và khi server phản hồi lại nội dung chúng ta cần cũng đồng thời lưu một vào cache của trình duyệt luôn kèm theo Header Last-Modified để kèm theo thời gian cuối cùng chỉnh sửa file và thông số Etag dung để đại diện cho file đó.Nhưng ở lần GET 2 ta lại gởi một request trùng ở GET 1 và nó đã được lưu trong cache trình duyệt ở lần responde 1. Ta có thểthấy được 2 Request trùng nhau thông qua dòng Etag và If-modified-since trả về giá trị giống ở lần 1, nên lúc này ta chỉ cần lấy lại file này tại Cache mà không cần lên Server để lấy nên Server không trả về nội dung đó nữa và phản hồi với mã trạng thái 304

Câu 9:

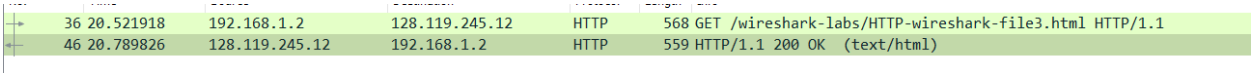
- Có 3 cái Get, đến những địa chỉ: 192.168.135.193 và 118.69.123.142



No.	Time	Source	Destination	Protocol	Length	Info
321	12.566126	192.168.135.157	192.168.135.193	HTTP	539	GET /21522243.html HTTP/1.1
322	12.576653	192.168.135.193	192.168.135.157	HTTP	586	HTTP/1.1 200 OK (text/html)
327	12.653299	192.168.135.157	118.69.123.142	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
329	12.724602	118.69.123.142	192.168.135.157	HTTP	445	HTTP/1.1 301 Moved Permanently (text/html)
385	26.867078	192.168.135.157	192.168.135.193	HTTP	651	GET /21522243.html HTTP/1.1
386	26.916806	192.168.135.193	192.168.135.157	HTTP	197	HTTP/1.1 304 Not Modified

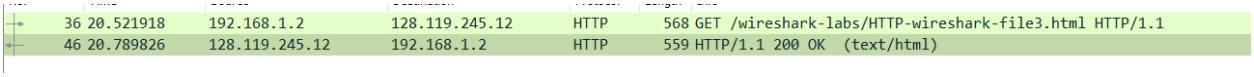
Câu 10:

- Trình diệt gửi 1 get



36	20.521918	192.168.1.2	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
46	20.789826	128.119.245.12	192.168.1.2	HTTP	559	HTTP/1.1 200 OK (text/html)

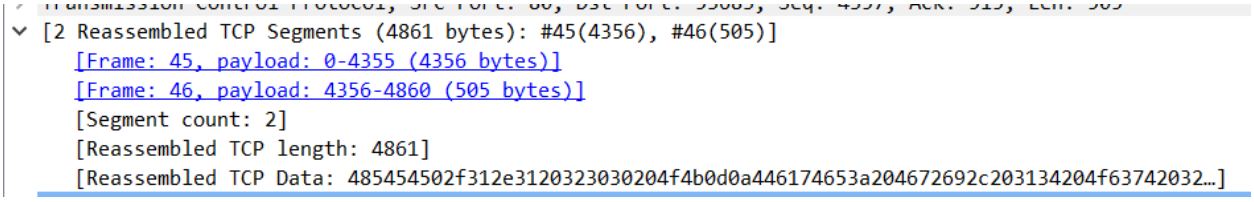
- Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ 46



36	20.521918	192.168.1.2	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
46	20.789826	128.119.245.12	192.168.1.2	HTTP	559	HTTP/1.1 200 OK (text/html)

Câu 11:

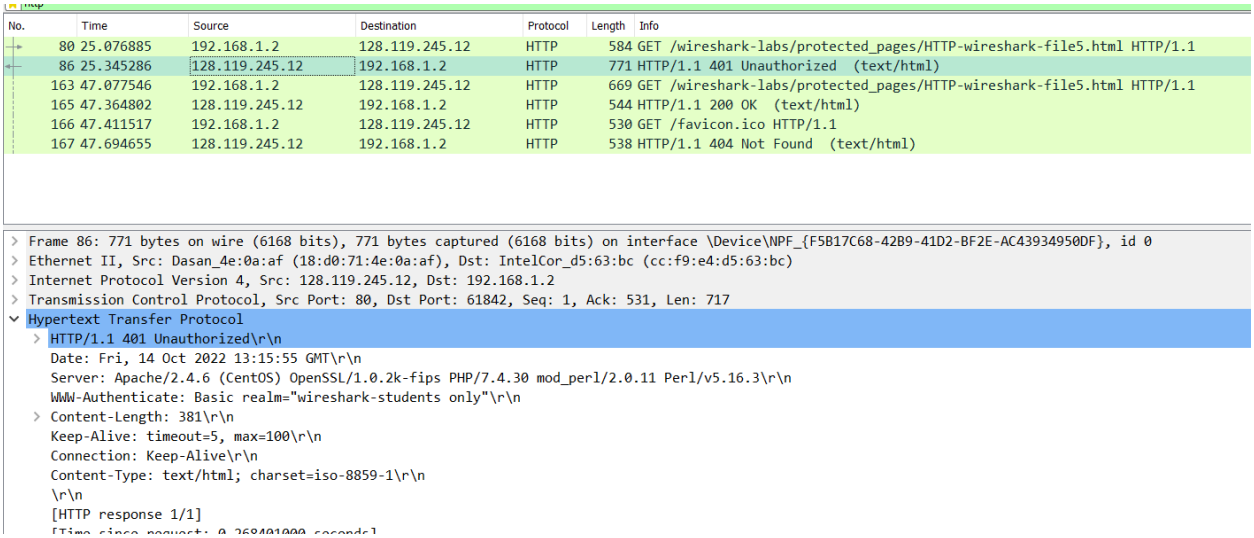
- Cần 2 TCP segments để chứa hết HTTP respone.



```
[2 Reassembled TCP Segments (4861 bytes): #45(4356), #46(505)]
    [Frame: 45, payload: 0-4355 (4356 bytes)]
    [Frame: 46, payload: 4356-4860 (505 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203134204f63742032…]
```

Câu 12:

- Mã trạng thái là 401. 401 Unauthorized: Header yêu cầu không chứa mã xác thực cần thiết và client bị từ chối truy cập.

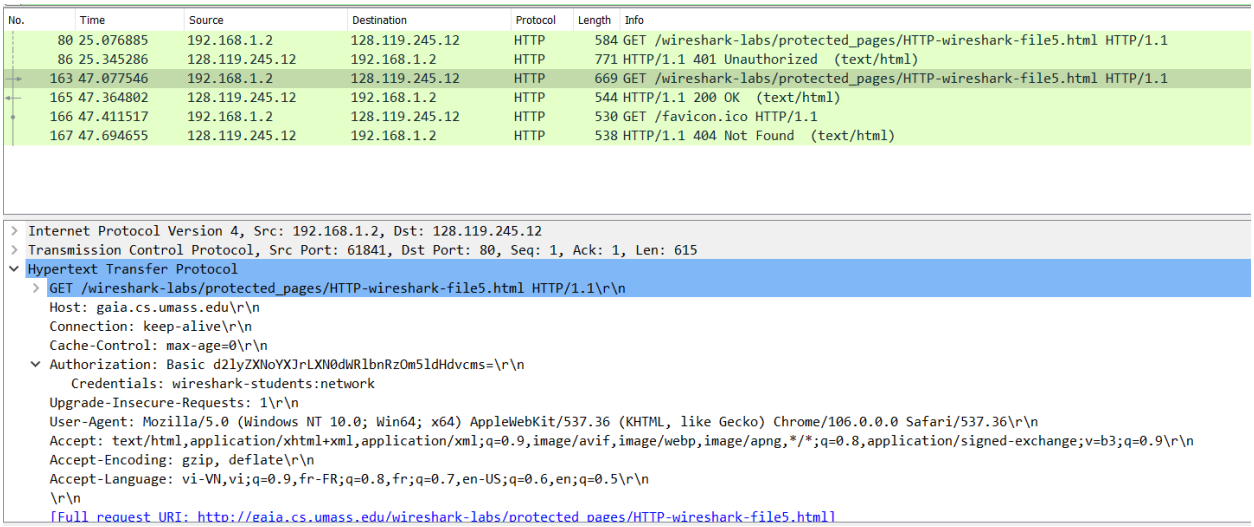


No.	Time	Source	Destination	Protocol	Length	Info
80	25.076885	192.168.1.2	128.119.245.12	HTTP	584	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
86	25.345286	128.119.245.12	192.168.1.2	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
163	47.077546	192.168.1.2	128.119.245.12	HTTP	669	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
165	47.364802	128.119.245.12	192.168.1.2	HTTP	544	HTTP/1.1 200 OK (text/html)
166	47.411517	192.168.1.2	128.119.245.12	HTTP	530	GET /favicon.ico HTTP/1.1
167	47.694655	128.119.245.12	192.168.1.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
> Frame 86: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{F5B17C68-42B9-41D2-BF2E-AC43934950DF}, id 0
> Ethernet II, Src: Dasan_4e:0a:af (18:d0:71:4e:0a:af), Dst: IntelCor_d5:63:bc (cc:f9:e4:d5:63:bc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 61842, Seq: 1, Ack: 531, Len: 717
v Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Fri, 14 Oct 2022 13:15:55 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
```

Câu 13:

- Xuất hiện một trường dữ liệu mới là trường authorizationtrong HTTP GET 2. Wireshark bắt được username và password được ngăn cách bởi kí tự“:”(wireshark-students:network)



No.	Time	Source	Destination	Protocol	Length	Info
80	25.076885	192.168.1.2	128.119.245.12	HTTP	584	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
86	25.345286	128.119.245.12	192.168.1.2	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
163	47.077546	192.168.1.2	128.119.245.12	HTTP	669	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
165	47.364802	128.119.245.12	192.168.1.2	HTTP	544	HTTP/1.1 200 OK (text/html)
166	47.411517	192.168.1.2	128.119.245.12	HTTP	530	GET /favicon.ico HTTP/1.1
167	47.694655	128.119.245.12	192.168.1.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61841, Dst Port: 80, Seq: 1, Ack: 1, Len: 615
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
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 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,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```