Lab

BÁO CÁO BÀI THỰC HÀNH SỐ 2

Phân tích gói tin HTTP với Wireshark

Sniffing HTTP Traffic with Wireshark

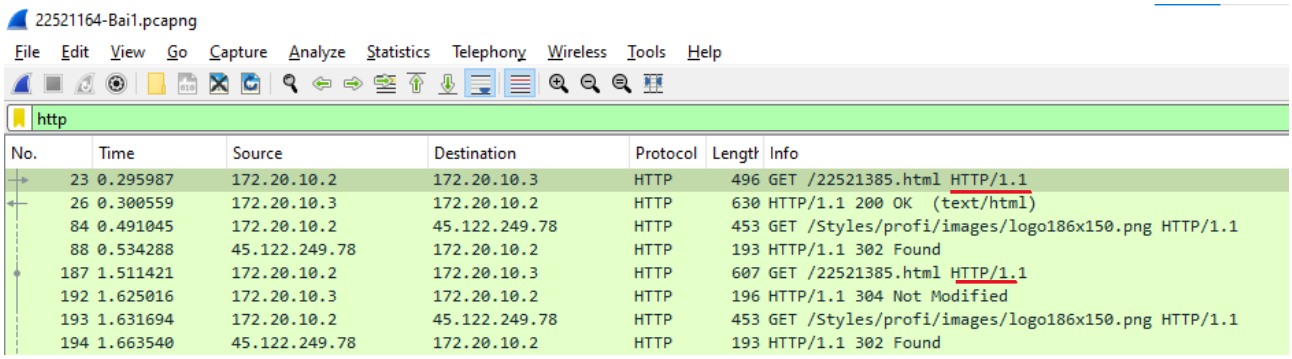
Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Mai Nguyễn Nam Phương (22521164)
Thời gian thực hiện	04/10/2023 – 11/10/2023
Tự chấm điểm	10/10

TRẢ LỜI CÁC CÂU HỎI

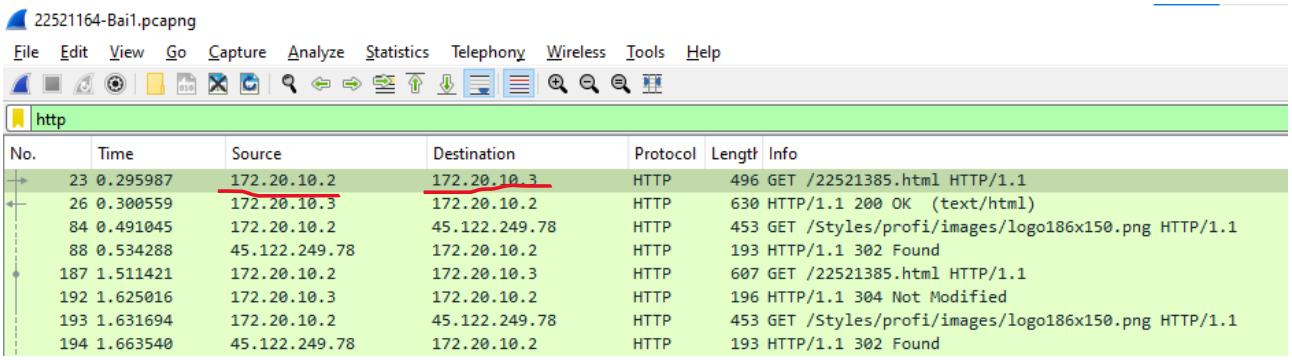
Câu 1. Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?

Trả lời: Trình duyệt đang sử dụng phiên bản HTTP 1.1, phiên bản của HTTP server là 1.1



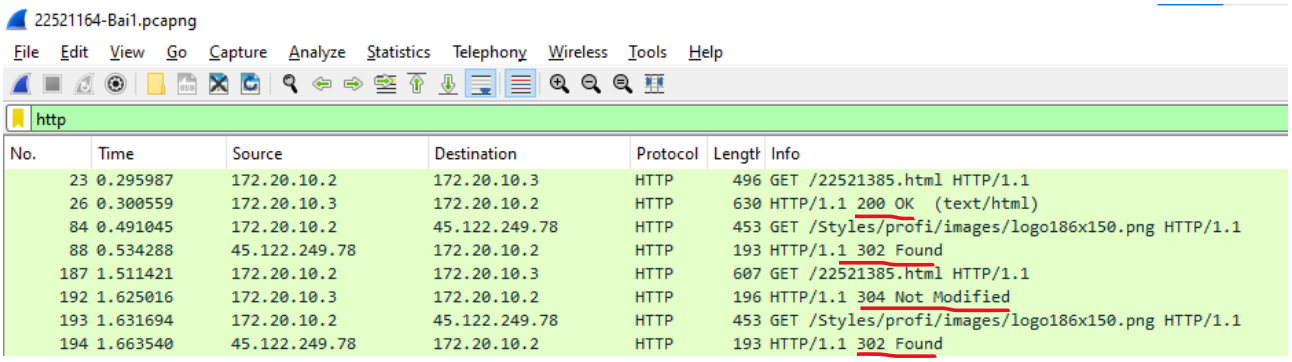
Câu 2. Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

Trả lời: Địa chỉ IP của máy tính là 172.20.10.2, của web server là 172.20.10.3



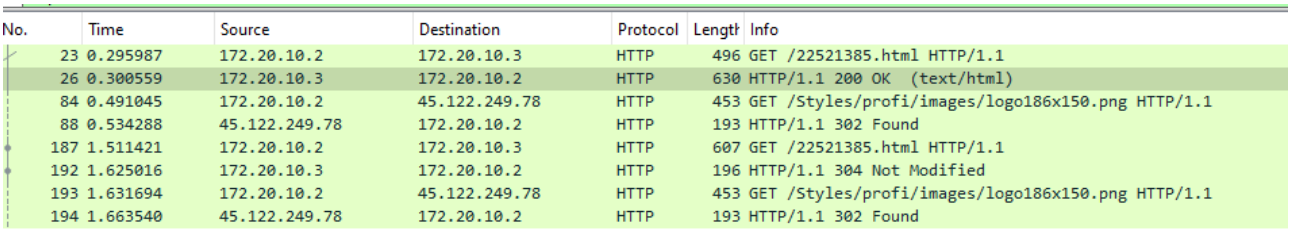
Câu 3. Các mã trạng thái (status code) trả về từ server là gì?

Bao gồm các mã 200 OK, 304 Not Modified, 302 Found

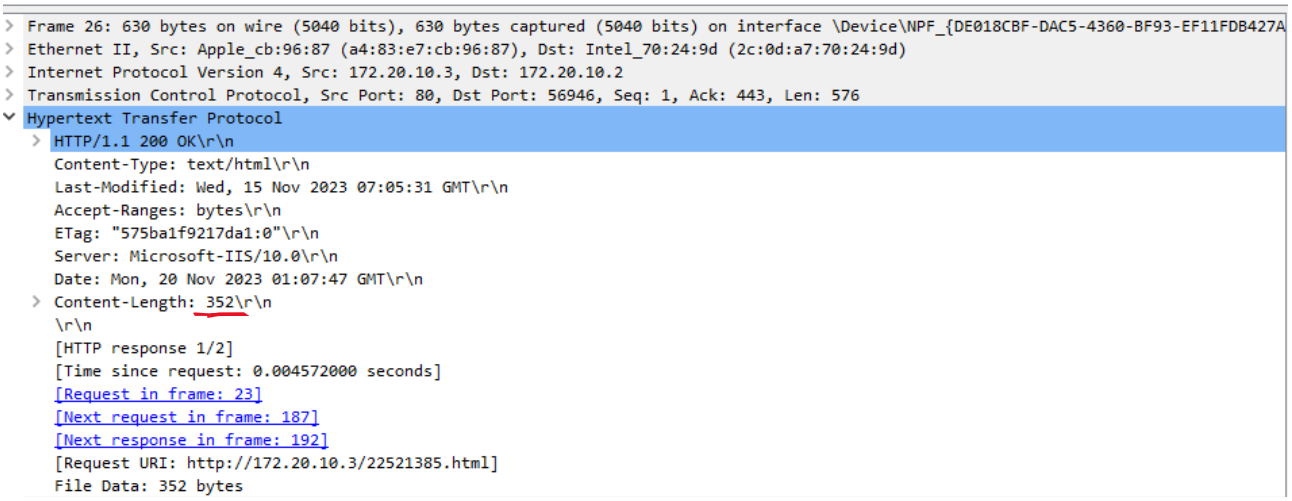


Câu 4: Server đã trả về cho trình duyệt tổng cộng bao nhiêu bytes nội dung?

Trả lời: Server đã trả về 352 bytes nội dung



No.	Time	Source	Destination	Protocol	Length	Info
23	0.295987	172.20.10.2	172.20.10.3	HTTP	496	GET /22521385.html HTTP/1.1
26	0.300559	172.20.10.3	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
84	0.491045	172.20.10.2	45.122.249.78	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
88	0.534288	45.122.249.78	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
187	1.511421	172.20.10.2	172.20.10.3	HTTP	607	GET /22521385.html HTTP/1.1
192	1.625016	172.20.10.3	172.20.10.2	HTTP	196	HTTP/1.1 304 Not Modified
193	1.631694	172.20.10.2	45.122.249.78	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
194	1.663540	45.122.249.78	172.20.10.2	HTTP	193	HTTP/1.1 302 Found



```
> Frame 26: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface \Device\NPF_{DE018CBF-DAC5-4360-BF93-EF11FDB427A
> Ethernet II, Src: Apple_cb:96:87 (a4:83:e7:cb:96:87), Dst: Intel_70:24:9d (2c:0d:a7:70:24:9d)
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 172.20.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 56946, Seq: 1, Ack: 443, Len: 576
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: text/html\r\n
    Last-Modified: Wed, 15 Nov 2023 07:05:31 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: "575ba1f9217da1:0"\r\n
    Server: Microsoft-IIS/10.0\r\n
    Date: Mon, 20 Nov 2023 01:07:47 GMT\r\n
  > Content-Length: 352\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.004572000 seconds]
    [Request in frame: 23]
    [Next request in frame: 187]
    [Next response in frame: 192]
    [Request URI: http://172.20.10.3/22521385.html]
    File Data: 352 bytes
```

Câu 5. Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng “IF-MODIFIED-SINCE” hay không?

Trả lời: Không có

Câu 6. Xem xét nội dung phản hồi từ server đối với HTTP GET đầu tiên. Server có trả về nội dung của file HTML hay không? Mã trạng thái đi kèm là gì? Giải thích ý nghĩa.

Trả lời: Quá trình cơ bản diễn ra như sau:

- Máy tính yêu cầu file (lệnh get)
- Máy chủ nhận được yêu cầu sẽ đi tìm kiếm xem file ở đâu.

+ Nếu như file cần tìm đã có sẵn ở bộ nhớ đệm cache thì sẽ lấy từ cache trả về.
+ Nếu file yêu cầu thực sự chưa có ở cache thì thực hiện tiếp.

- Sau đó, máy chủ tìm thấy file và trả về lại máy.

- Máy tải file và hiển thị cho người dung => Do đó, Server có trả về nội dung của file HTML.Vì trước khi truy cập trang web ta đã xóa cache nên khi ta chạy GET Request đầu tiên cho máy chủ, file chưa hề lưu trong bộ nhớ cache nên máy chủ sẽ tải trực tiếp file về

- Mã trạng thái đi kèm là 200 OK: Yêu cầu đã thành công.

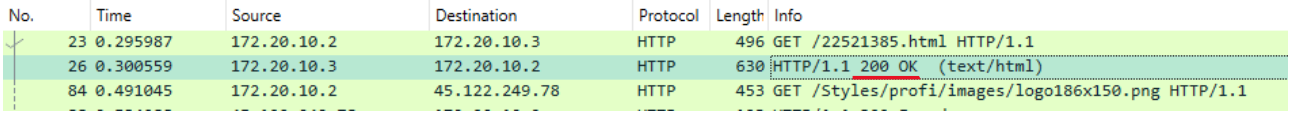
Ý nghĩa của thành công còn phụ thuộc vào phương thức HTTP là gì:

+ GET: Tài nguyên đã được tìm nạp và được truyền trong nội dung thông điệp.

+ HEAD: Các header thực thể nằm trong nội dung thông điệp.

+ PUT hoặc POST: Tài nguyên mô tả kết quả của hành động được truyền trong nội dung thông điệp.

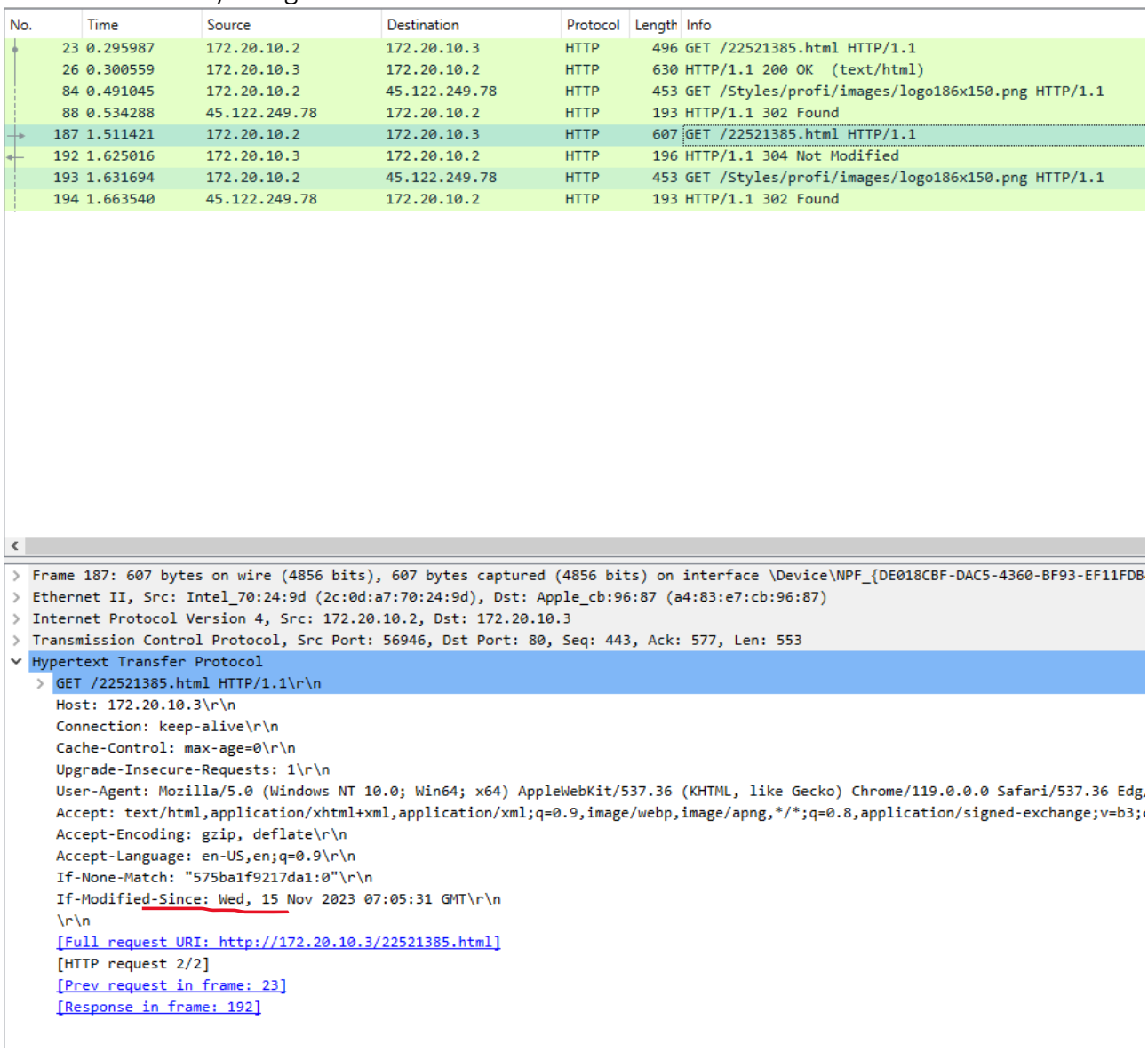
+ TRACE: Nội dung thông điệp chứa thông báo yêu cầu khi máy chủ nhận được. => Ta chỉ xét phương thức GET cho bài này, do đó ý nghĩa của mã 200 ở đây là: Tài nguyên đã được tìm nạp và được truyền trong nội dung thông điệp.



No.	Time	Source	Destination	Protocol	Length	Info
23	0.295987	172.20.10.2	172.20.10.3	HTTP	496	GET /22521385.html HTTP/1.1
26	0.300559	172.20.10.3	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
84	0.491045	172.20.10.2	45.122.249.78	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1

Câu 7. Xem xét nội dung của HTTP GET thứ 2. Bạn có thấy dòng “IF-MODIFIED-SINCE” hay không? Nếu có, giá trị của IF-MODIFIED-SINCE là gì?

Trả lời: Ta có thấy dòng IF-MODIFIED-SINCE



Giá trị của If-Modified-Since: Wed, 15 Nov 2023 07:05:31 GMT

Câu 8. Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thật sự gửi về nội dung của file hay không? Giải thích

Trả lời: - Mã trạng thái HTTP được trả về từ Server tương ứng với lần GET thứ 2 là: 304 Not Modified.

- 304 Not Modified: Code này được sử dụng cho mục đích caching. Nó cho client biết rằng phản hồi chưa được điều chỉnh, nên client có thể tiếp tục sử dụng cùng phiên bản phản hồi trong bộ nhớ cache.

- Server không thực sự gởi về nội dung của file. Giải thích:

+ Ở lần GET đầu tiên: file chúng ta Request không có sẵn trong cache nên phải lên trực tiếp máy chủ để lấy về và khi đó máy chủ phản hồi lại nội dung mà ta cần, đồng thời lưu vào cache của trình duyệt đó.

+ Ở lần GET thứ 2 ta lại gửi một Request trùng ở lần GET đầu tiên và vì nó đã được lưu trong cache ở trình duyệt. Nên ta có thể thấy được 2 Request trùng nhau

thông qua dòng If-modified-since, nó sẽ trả về nội dung giống như ở lần GET đầu tiên.

⇨ Nên lúc này ta chỉ nhận file được lấy tại Cache mà không cần lên Máy chủ để lấy => Server không trả về nội dung đó nữa và phản hồi với mã trạng thái 304.

No.	Time	Source	Destination	Protocol	Length	Info
23	0.295987	172.20.10.2	172.20.10.3	HTTP	496	GET /22521385.html HTTP/1.1
26	0.300559	172.20.10.3	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
84	0.491045	172.20.10.2	45.122.249.78	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
88	0.534288	45.122.249.78	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
187	1.511421	172.20.10.2	172.20.10.3	HTTP	607	GET /22521385.html HTTP/1.1
192	1.625016	172.20.10.3	172.20.10.2	HTTP	196	HTTP/1.1 304 Not Modified
193	1.631694	172.20.10.2	45.122.249.78	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
194	1.663540	45.122.249.78	172.20.10.2	HTTP	193	HTTP/1.1 302 Found

Câu 9. Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

Trả lời: Trình duyệt đã gửi 4 HTTP GET, đến 2 địa chỉ IP 172.20.10.3 và 45.122.249.78

http

No.	Time	Source	Destination	Protocol	Length	Info
23	0.295987	172.20.10.2	172.20.10.3	HTTP	496	GET /22521385.html HTTP/1.1
26	0.300559	172.20.10.3	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
84	0.491045	172.20.10.2	45.122.249.78	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
88	0.534288	45.122.249.78	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
187	1.511421	172.20.10.2	172.20.10.3	HTTP	607	GET /22521385.html HTTP/1.1
192	1.625016	172.20.10.3	172.20.10.2	HTTP	196	HTTP/1.1 304 Not Modified
193	1.631694	172.20.10.2	45.122.249.78	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
194	1.663540	45.122.249.78	172.20.10.2	HTTP	193	HTTP/1.1 302 Found

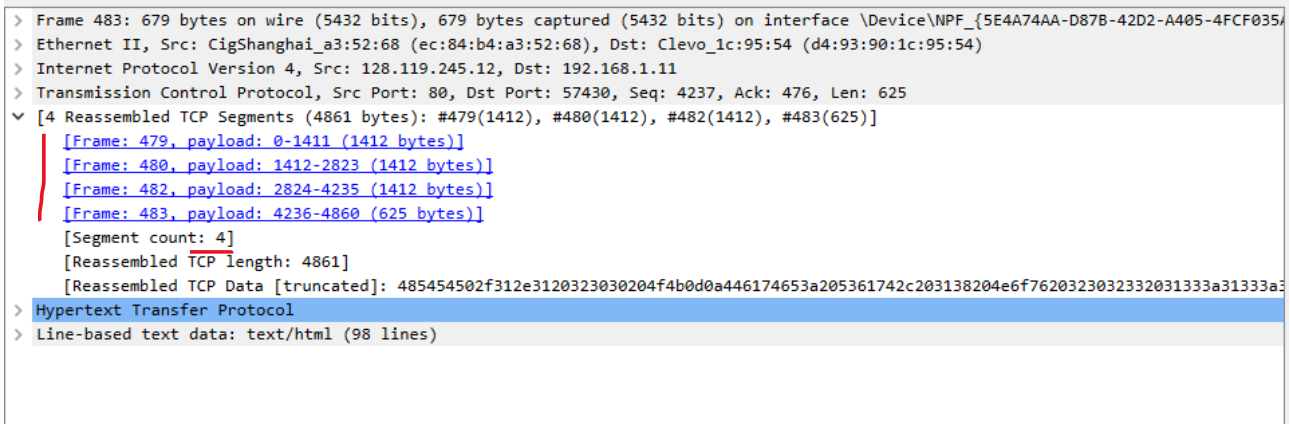
Câu 10. Trình duyệt đã gửi bao nhiêu HTTP GET?

Trả lời: Trình duyệt đã gửi 2 HTTP GET

No.	Time	Source	Destination	Protocol	Length	Info
405	2.245585	192.168.1.11	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
483	2.512817	128.119.245.12	192.168.1.11	HTTP	679	HTTP/1.1 200 OK (text/html)
490	2.559070	192.168.1.11	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
555	2.825546	128.119.245.12	192.168.1.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Câu 11. Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

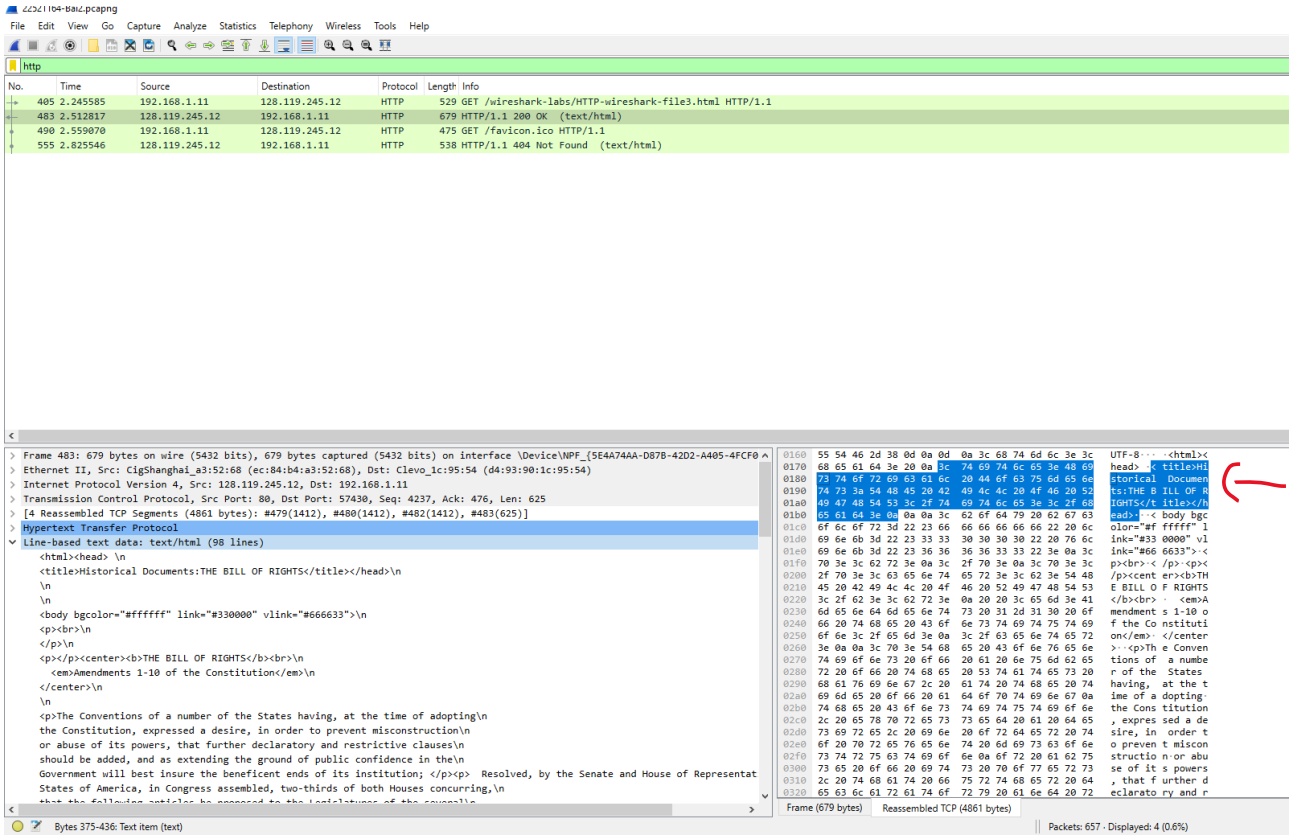
Trả lời:



Dựa trên hình ảnh trên ta sẽ thấy cần 4 TCP segments để chứa hết response và nội dung của The Bill of Rights

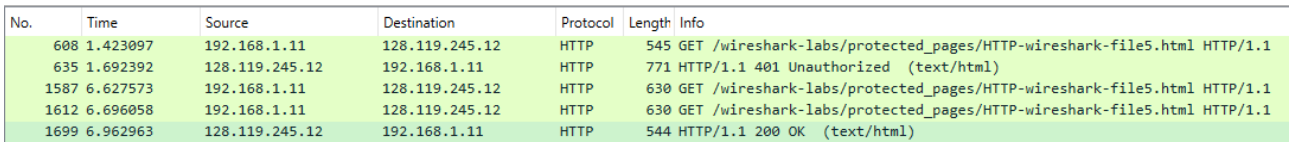
Câu 12. Dòng chữ "THE BILL OF RIGHTS" được chứa trong gói tin phản hồi thứ mấy?

Trả lời:



Được chứa trong gói tin phản hồi thứ nhất

Câu 13. Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?

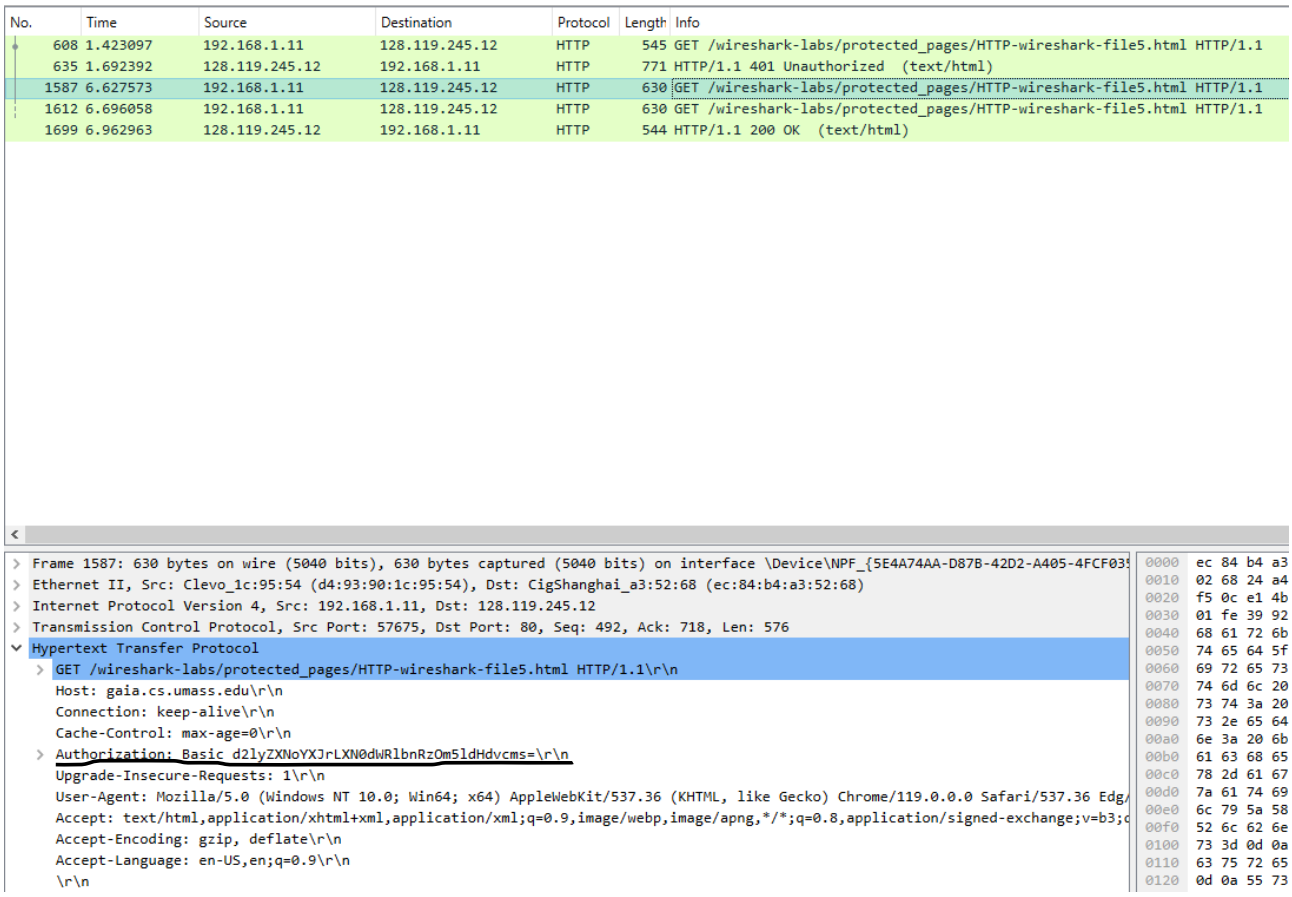


No.	Time	Source	Destination	Protocol	Length	Info
608	1.423097	192.168.1.11	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
635	1.692392	128.119.245.12	192.168.1.11	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1587	6.627573	192.168.1.11	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1612	6.696058	192.168.1.11	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1699	6.962963	128.119.245.12	192.168.1.11	HTTP	544	HTTP/1.1 200 OK (text/html)

Mã trạng thái được trả về là 401 Unauthorized

Ý nghĩa: là một phản hồi từ máy chủ web cho biết người dùng hoặc máy ứng dụng không có quyền truy cập tài nguyên được yêu cầu. Mã này thông báo rằng yêu cầu không được chấp nhận vì người dùng chưa xác thực hoặc xác thực không thành công. Ví dụ: cấm truy cập 1 file trong thư mục nào đó trong hosting đối với người dùng dù có được link

Câu 14. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?



No.	Time	Source	Destination	Protocol	Length	Info
608	1.423097	192.168.1.11	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
635	1.692392	128.119.245.12	192.168.1.11	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1587	6.627573	192.168.1.11	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1612	6.696058	192.168.1.11	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1699	6.962963	128.119.245.12	192.168.1.11	HTTP	544	HTTP/1.1 200 OK (text/html)

```
Frame 1587: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface \Device\NPF_{5E4A74AA-D87B-42D2-A405-4FCF03
Ethernet II, Src: Clevo_1c:95:54 (d4:93:90:1c:95:54), Dst: CigShanghai_a3:52:68 (ec:84:b4:a3:52:68)
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57675, Dst Port: 80, Seq: 492, Ack: 718, Len: 576
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/119.0.0.0 Safari/537.36 Edg/
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
```

```
0000  ec 84 b4 a3
0010  02 68 24 a4
0020  f5 0c e1 4b
0030  01 fe 39 92
0040  68 61 72 6b
0050  74 65 64 5f
0060  69 72 65 73
0070  74 6d 6c 20
0080  73 74 3a 20
0090  73 2e 65 64
00a0  6e 3a 20 6b
00b0  61 63 68 65
00c0  78 2d 61 67
00d0  7a 61 74 69
00e0  6c 79 5a 58
00f0  52 6c 62 6e
0100  73 3d 0d 0a
0110  63 75 72 65
0120  0d 0a 55 73
```

Trường dữ liệu mới xuất hiện là trường Authoriration