

Họ và tên: Bùi Lê Nhật Tri

MSSV: 23521634

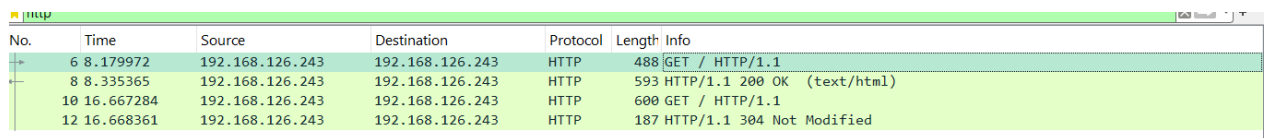
Lớp: IT005.P119

BÁO CÁO BÀI THỰC HÀNH LAB 2: PHÂN TÍCH GÓI TIN HTTP VỚI WIRESHARK

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

Trình duyệt đang sử dụng phiên bản HTTP 1.1

Phiên bản HTTP server đang sử dụng là HTTP 1.1

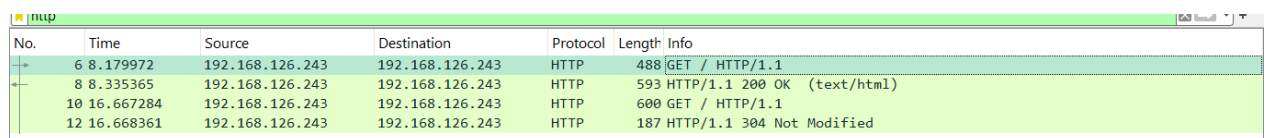


No.	Time	Source	Destination	Protocol	Length	Info
6	8.179972	192.168.126.243	192.168.126.243	HTTP	488	GET / HTTP/1.1
8	8.335365	192.168.126.243	192.168.126.243	HTTP	593	HTTP/1.1 200 OK (text/html)
10	16.667284	192.168.126.243	192.168.126.243	HTTP	600	GET / HTTP/1.1
12	16.668361	192.168.126.243	192.168.126.243	HTTP	187	HTTP/1.1 304 Not Modified

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

Địa chỉ ip của máy tính là: 192.168.126.243

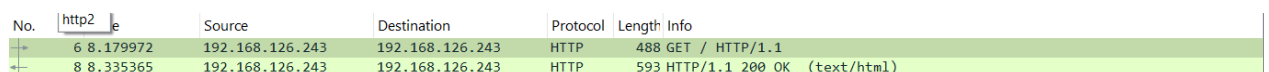
Địa chỉ ip của web server là: 192.168.126.243



No.	Time	Source	Destination	Protocol	Length	Info
6	8.179972	192.168.126.243	192.168.126.243	HTTP	488	GET / HTTP/1.1
8	8.335365	192.168.126.243	192.168.126.243	HTTP	593	HTTP/1.1 200 OK (text/html)
10	16.667284	192.168.126.243	192.168.126.243	HTTP	600	GET / HTTP/1.1
12	16.668361	192.168.126.243	192.168.126.243	HTTP	187	HTTP/1.1 304 Not Modified

3. Mã trạng thái (status code) trả về từ server là gì?

Mã trạng thái trả về từ server là: 200



No.	Time	Source	Destination	Protocol	Length	Info
6	8.179972	192.168.126.243	192.168.126.243	HTTP	488	GET / HTTP/1.1
8	8.335365	192.168.126.243	192.168.126.243	HTTP	593	HTTP/1.1 200 OK (text/html)

4. Server đã trả về cho trình duyệt bao nhiêu bytes nội dung?

Server đã trả về 324 bytes nội dung

No.	Time	Source	Destination	Protocol	Length	Info
6	8.179972	192.168.126.243	192.168.126.243	HTTP	488	GET / HTTP/1.1
8	8.335365	192.168.126.243	192.168.126.243	HTTP	593	HTTP/1.1 200 OK (text/html)
10	16.667284	192.168.126.243	192.168.126.243	HTTP	600	GET / HTTP/1.1
12	16.668361	192.168.126.243	192.168.126.243	HTTP	187	HTTP/1.1 304 Not Modified

Date: Fri, 11 Oct 2024 07:54:14 GMT\r\n	0100	6e 67 74 68 3a 20 33 32 34 0d 0a 0d 0a 3c 21 44	ngth: 32 4....<
> Content-Length: 324\r\n	0110	4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68	OCTYPE h tml>...<
\r\n	0120	74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74	tml>...<h ead>...<
[Request in frame: 6]	0130	69 74 6c 65 3e 54 68 e1 bb b1 63 20 68 c3 a0 6e	itle>Th...c h...
[Time since request: 0.155393000 seconds]	0140	68 20 6e 68 e1 ba ad 70 20 6d c3 b4 6e 20 6d e1	h nh...p m...n...
[Request URI: /]	0150	ba a1 6e 67 20 6d c3 a1 79 20 74 c3 ad 6e 68 20	...ng m...y t...n...
[Full request URI: http://192.168.126.243/]	0160	2d 20 32 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68	- 2</tit le>...<
File Data: 324 bytes	0170	65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63	ead>...<b ody>...<
Line-based text data: text/html (13 lines)	0180	65 6e 74 65 72 3e 3c 69 6d 67 0d 0a 73 72 63 3d	enter><i mg...src...
<!DOCTYPE html>\r\n	0190	22 68 74 74 70 3a 2f 2f 70 6f 72 74 61 6c 2e 75	"http:// portal...
	01a0	69 74 2e 65 64 75 2e 76 6e 2f 53 74 79 6c 65 73	it.edu.v n/Style...

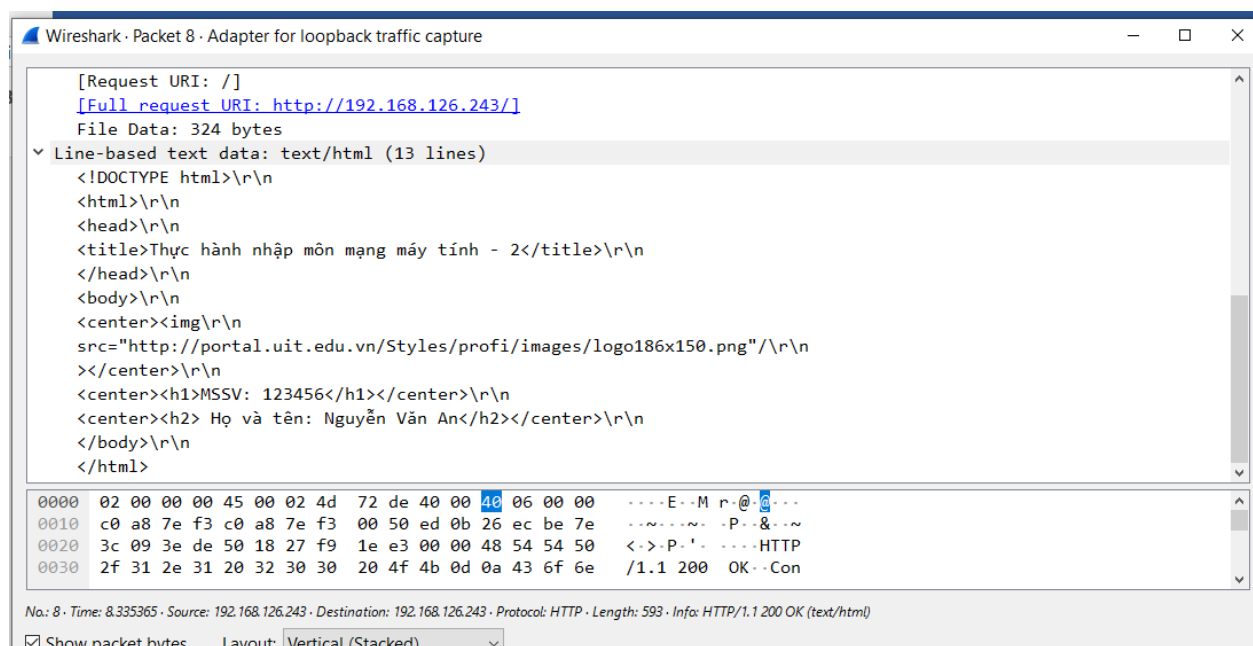
5. Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng “IF-MODIFIEDSINCE” hay không?

Trong nội dung của HTTP GET đầu tiên KHÔNG thấy dòng “IF-MODIFIEDSINCE”

TCP payload (444 bytes)
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: 192.168.126.243\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/129.0.0.0 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Response in frame: 8]
[Full request URI: http://192.168.126.243/]

6. Xem xét nội dung phản hồi từ server. Server có thật sự trả về nội dung của file HTML hay không? Tại sao?

Server CÓ trả về nội dung của file HTML

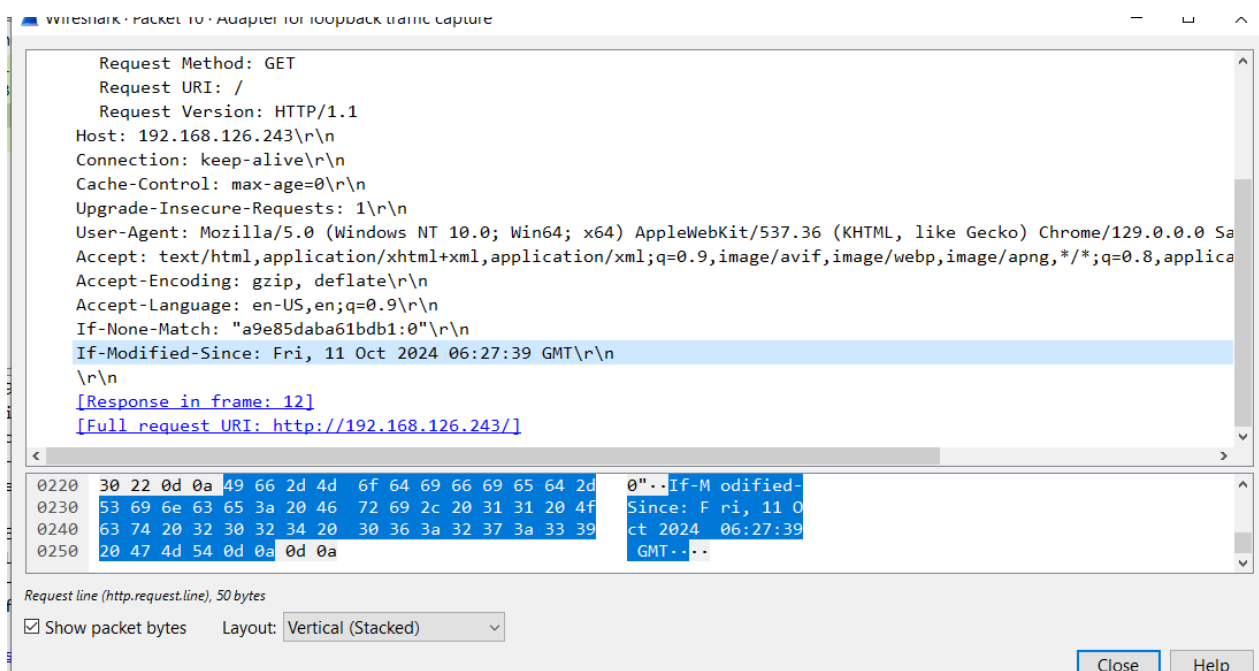


Giải thích: Vì ban đầu trước khi bắt gói tin, ta đã xóa cache rồi. Do đó, khi người dùng gửi request lên server, server sẽ kiểm tra xem trong cache có nội dung đó chưa. Nếu chưa thì server sẽ trả về nội dung của file đó cho người dùng. Ngược lại thì không. Vì trước khi bắt gói tin, ta đã xóa bộ nhớ cache rồi, nên server sẽ không tìm thấy file đó. Do đó, nội dung của file đó sẽ được trả về cho người dùng

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

Trong nội dung của HTTP GET thứ 2, CÓ xuất hiện dòng “IF-MODIFIEDSINCE”

Giá trị của “IF-MODIFIEDSINCE” là => If-Modified-Since: Fri, 11 Oct 2024 06:27:39 GMT



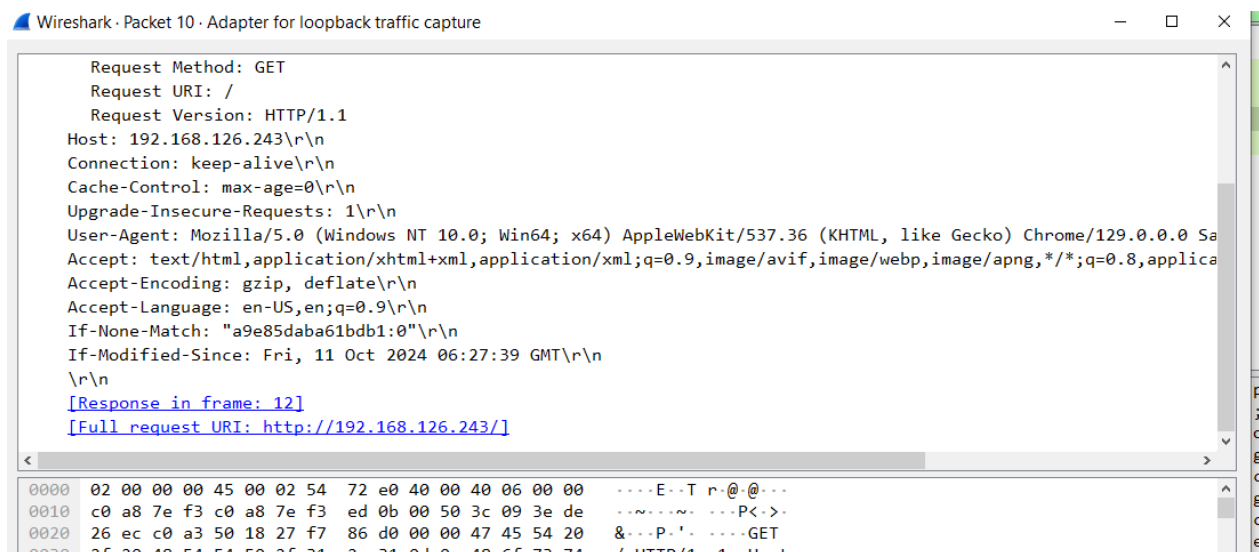
8. Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thực sự gửi về nội dung của file hay không? Giải thích.

Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là: **304**

Ý nghĩa: Trạng thái này cho ta biết là nội dung của trang web trên chưa bị sửa đổi hay nói cách khác là nội dung của trang web đó vẫn giống với nội dung của lần request trước đó.

http2					
No.	Time	Source	Destination	Protocol	Length Info
6	8.179972	192.168.126.243	192.168.126.243	HTTP	488 GET / HTTP/1.1
8	8.335365	192.168.126.243	192.168.126.243	HTTP	593 HTTP/1.1 200 OK (text/html)
10	16.667284	192.168.126.243	192.168.126.243	HTTP	600 GET / HTTP/1.1
12	16.668361	192.168.126.243	192.168.126.243	HTTP	187 HTTP/1.1 304 Not Modified

Giải thích: Server không thực sự gửi về nội dung của file, bởi vì lúc này, trong bộ nhớ cache của ta đã có nội dung của file đó ở lần gửi request đầu tiên (được minh chứng thông qua trạng thái 304 NOT MODIFIED được trả về), do đó, lúc này, server sẽ không gửi lại nội dung đó cho người dùng nữa.



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

Trình duyệt đã gửi 2 HTTP GET

Gửi đến địa chỉ IP: 192.168.126.243

No.	Time	Source	Destination	Protocol	Length	Info
6	8.179972	192.168.126.243	192.168.126.243	HTTP	488	GET / HTTP/1.1
8	8.335365	192.168.126.243	192.168.126.243	HTTP	593	HTTP/1.1 200 OK (text/html)
10	16.667284	192.168.126.243	192.168.126.243	HTTP	600	GET / HTTP/1.1
12	16.668361	192.168.126.243	192.168.126.243	HTTP	187	HTTP/1.1 304 Not Modified

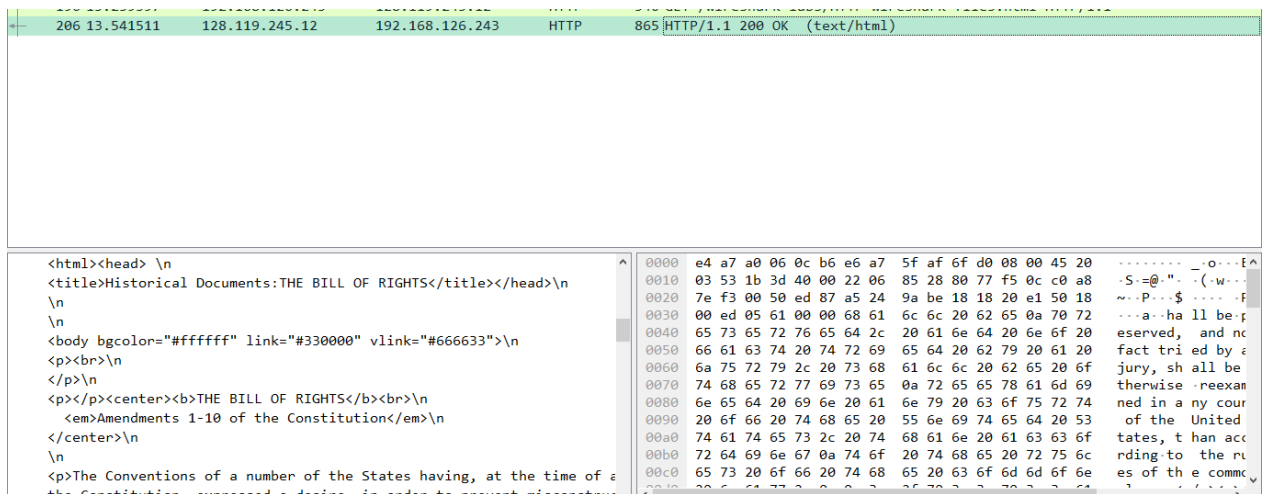
10. Trình duyệt đã gửi bao nhiêu HTTP GET? Dòng “THE BILL OF RIGHTS”

được chứa trong gói tin phản hồi thứ mấy?

Trình duyệt đã gửi 1 HTTP GET

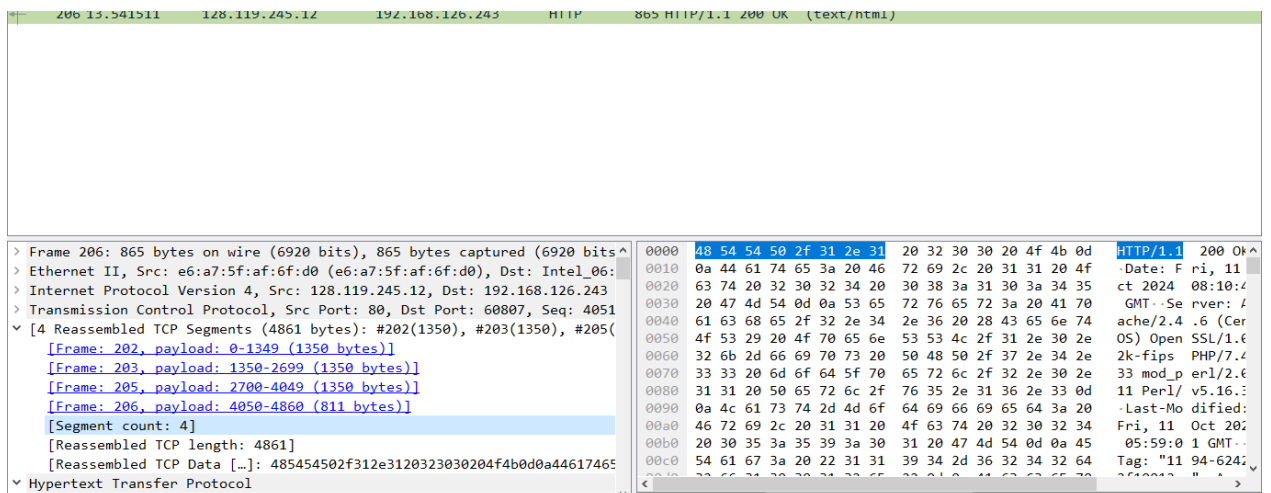
No.	Time	Source	Destination	Protocol	Length	Info
196	13.239397	192.168.126.243	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
206	13.541511	128.119.245.12	192.168.126.243	HTTP	865	HTTP/1.1 200 OK (text/html)

Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy 1



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

Cần tới 4 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights



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

Mã trạng thái đầu tiên là 401 Unauthorized

Mã trạng thái 401 Unauthorized cho ta biết trang web đó yêu cầu thông tin đăng nhập của người dùng. Do đó, response trên trả về 401 Unauthorized vì ban đầu ta chưa nhập username và password tương ứng.

