Lab
2

BÁO CÁO BÀI THỰC HÀNH SỐ 2

Phân Tích Gói Tin HTTP Với WireShark

Sniffing HTTP Traffic with Wireshark

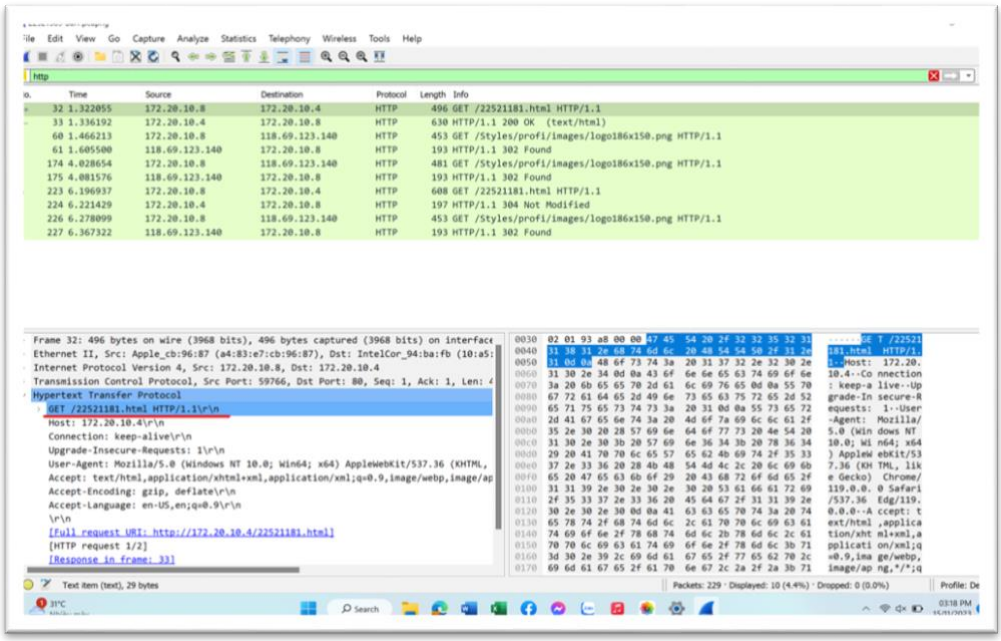
Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Lại Quan Thiên (22521385)
Thời gian thực hiện	15/11/2023 – 19/11/2023
Tự chấm điểm	10/10

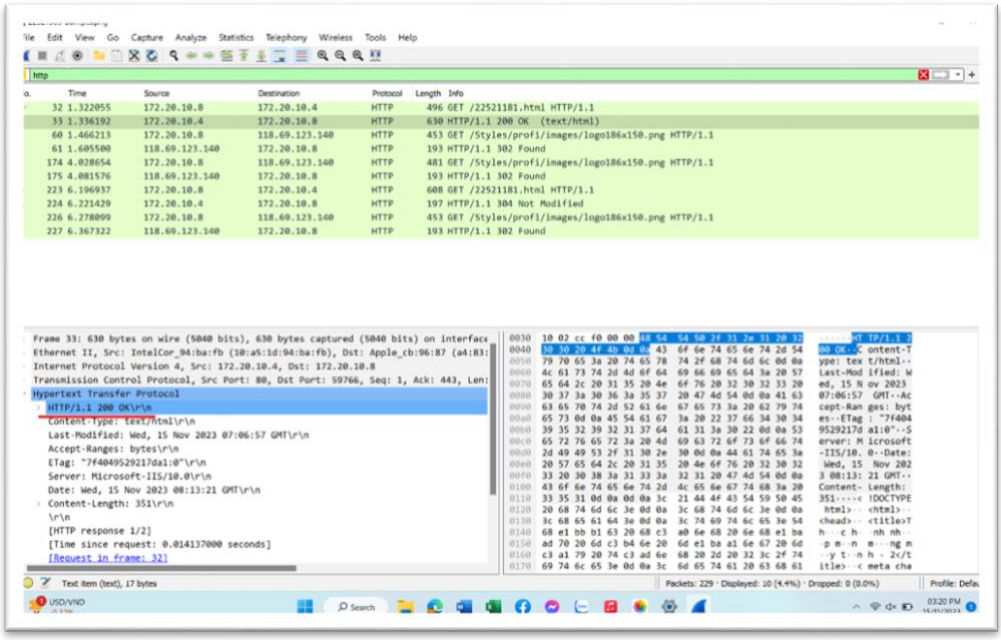
I. HTTP GET/response có điều kiện?

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 (xem ảnh 1)
- Server đang sử dụng phiên bản HTTP 1.1 (xem ảnh 2)



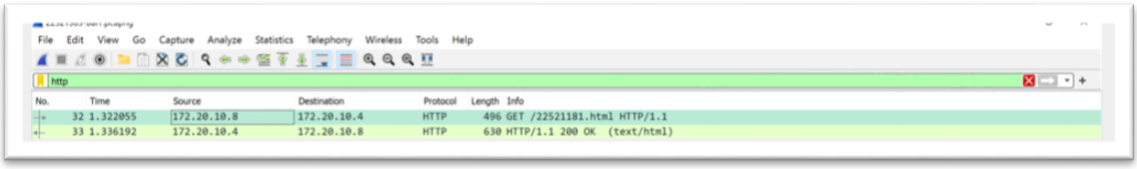
Ảnh 1



Ảnh 2

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

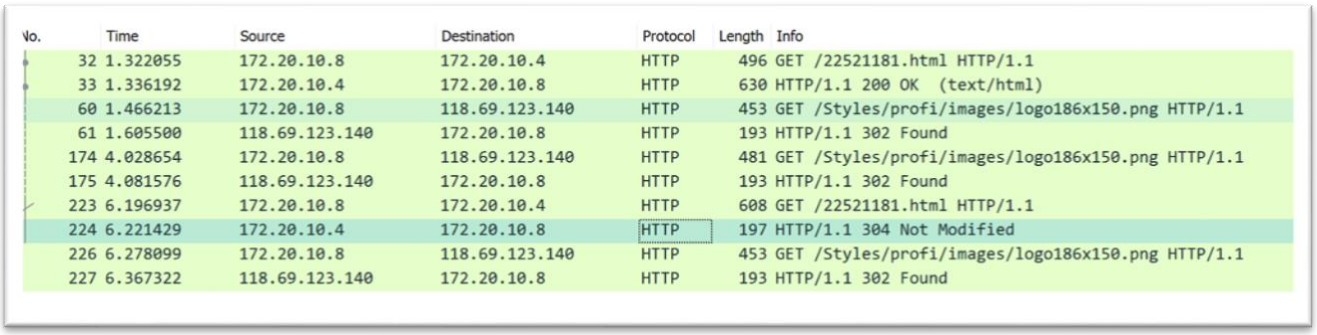
- Địa chỉ IP của máy tính là: 172.20.10.8 (xem ảnh 3)
- Địa chỉ IP của Web Server là: 172.20.10.4 (xem ảnh 3)



Ảnh 3

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

Các mã trạng thái là: 200 Ok; 302 Found; 304 Not Modified (xem ảnh 4)

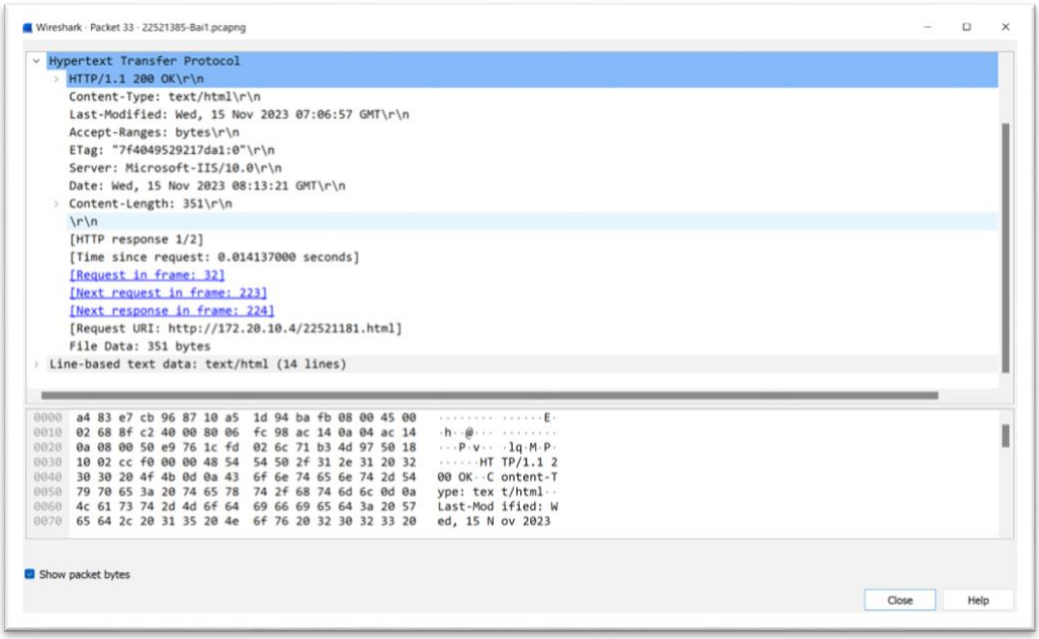


No.	Time	Source	Destination	Protocol	Length	Info
32	1.322055	172.20.10.8	172.20.10.4	HTTP	496	GET /22521181.html HTTP/1.1
33	1.336192	172.20.10.4	172.20.10.8	HTTP	630	HTTP/1.1 200 OK (text/html)
60	1.466213	172.20.10.8	118.69.123.140	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
61	1.605500	118.69.123.140	172.20.10.8	HTTP	193	HTTP/1.1 302 Found
174	4.028654	172.20.10.8	118.69.123.140	HTTP	481	GET /Styles/profi/images/logo186x150.png HTTP/1.1
175	4.081576	118.69.123.140	172.20.10.8	HTTP	193	HTTP/1.1 302 Found
223	6.196937	172.20.10.8	172.20.10.4	HTTP	608	GET /22521181.html HTTP/1.1
224	6.221429	172.20.10.4	172.20.10.8	HTTP	197	HTTP/1.1 304 Not Modified
226	6.278099	172.20.10.8	118.69.123.140	HTTP	453	GET /Styles/profi/images/logo186x150.png HTTP/1.1
227	6.367322	118.69.123.140	172.20.10.8	HTTP	193	HTTP/1.1 302 Found

Ảnh 4

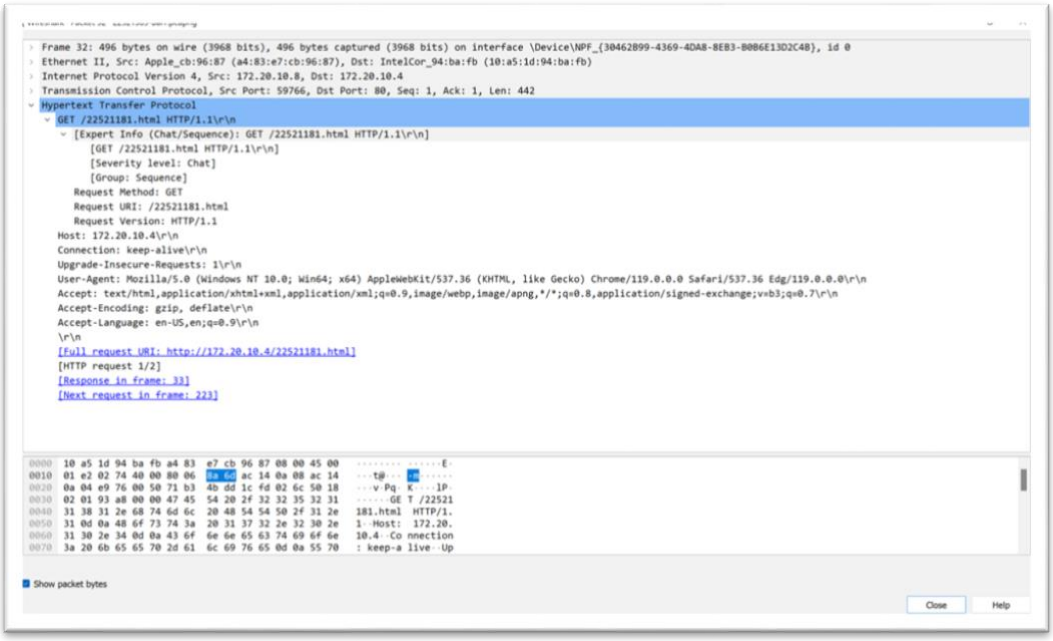
4. Server đã trả về cho trình duyệt tổng cộng bao nhiêu bytes nội dung?

Server đã trả về cho trình duyệt tông cộng 351 bytes nội dung. (xem ảnh 5)



Ảnh 5

5. Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng "IF-MODIFIED-SINCE" hay không? => Không thấy dòng "IF-MODIFIED-SINCE" (xem ảnh 6)



Ảnh 6

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?

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.

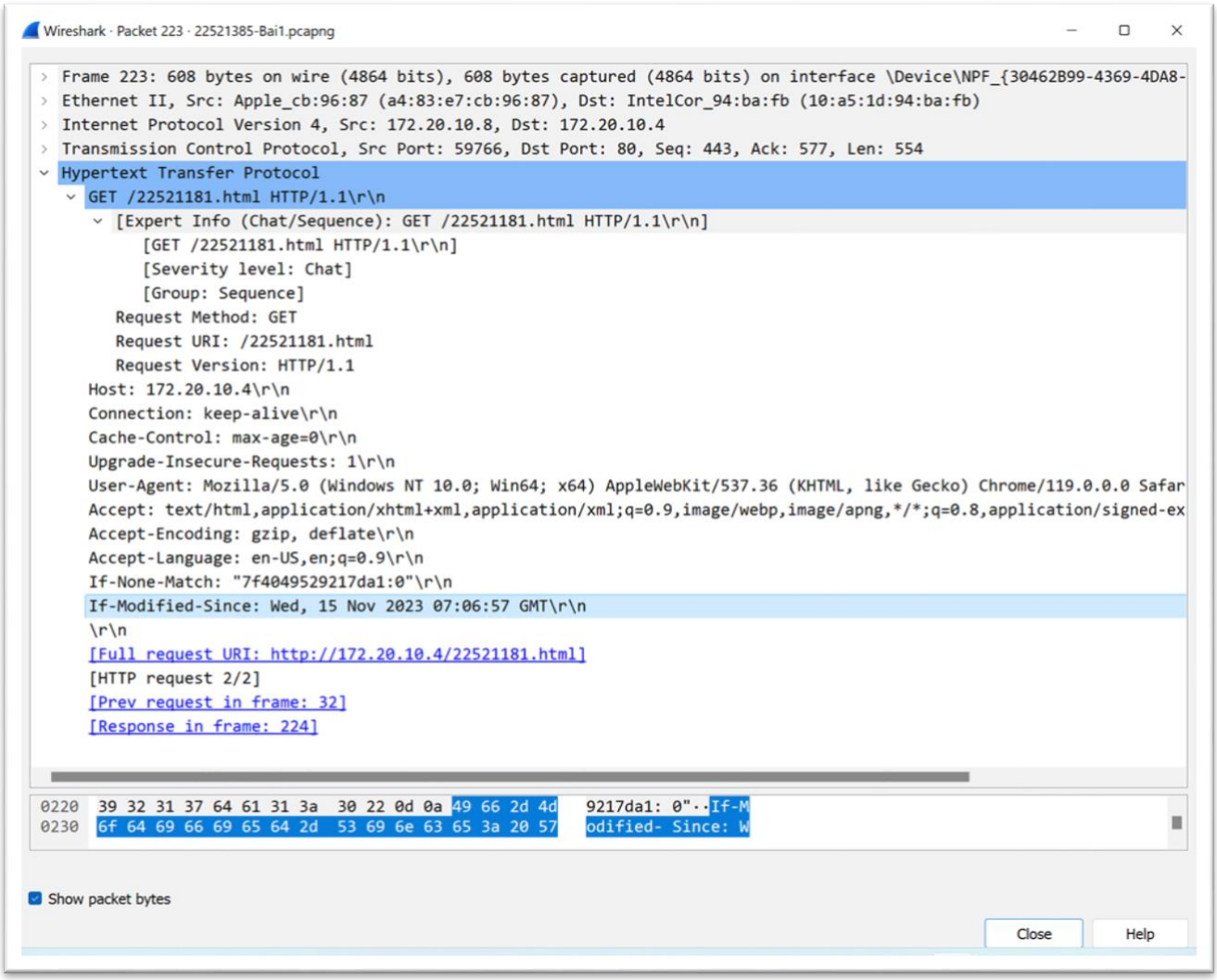
+ TRACE: Nội dung thông điệp chứa thông báo yêu cầu khi máy chủ nhận được.

=> 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.

Ảnh 7

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?

- Có thấy dòng IF-MODIFIED-SINCE (xem ảnh 8)
- Giá trị của IF-MODIFIED-SINCE: Wed, 15 Nov 2023 07:06:57 GMT\r\n



Ảnh 8

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?

- 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.

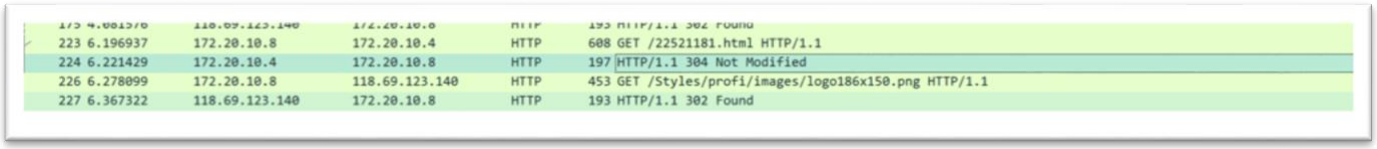
- Server không thực sự gởi về nội dung của file. Giải thích:

+ 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.

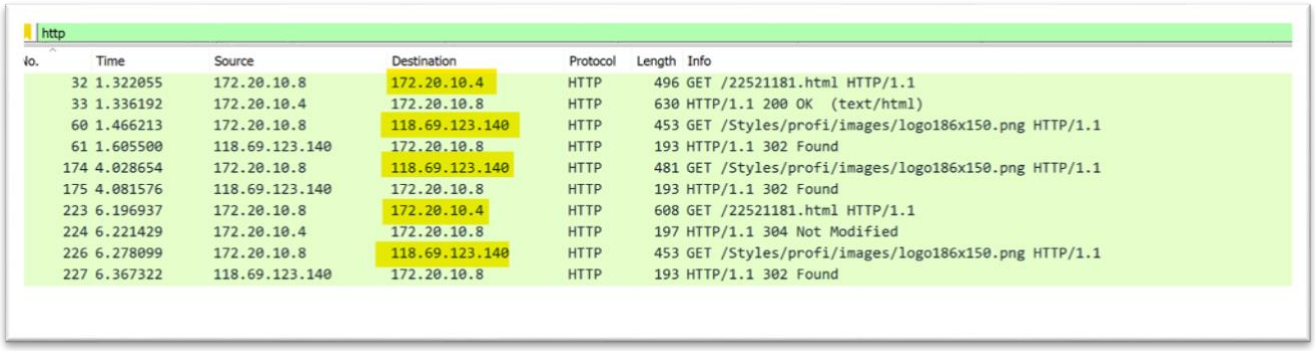


Ảnh 9

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

Trình duyệt đã gửi 5 HTTP GET đến các địa chỉ IP sau (xem ảnh 10):

- 172.20.10.4
- 118.69.123.140

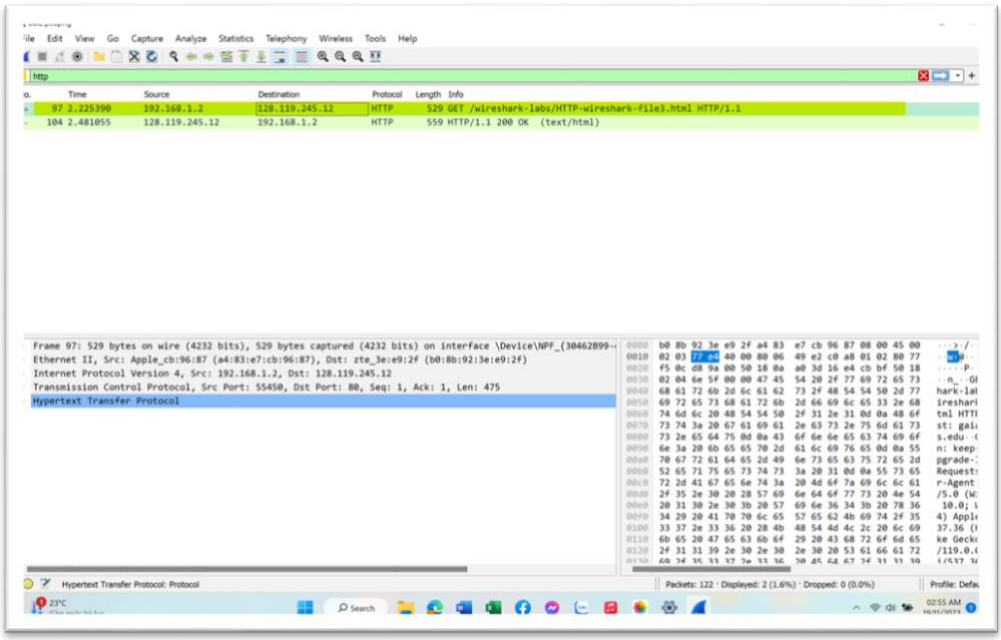


Ảnh 10

II. Truy cập các trang HTTP dài.

10. Trình duyệt đã gửi bao nhiêu HTTP GET?

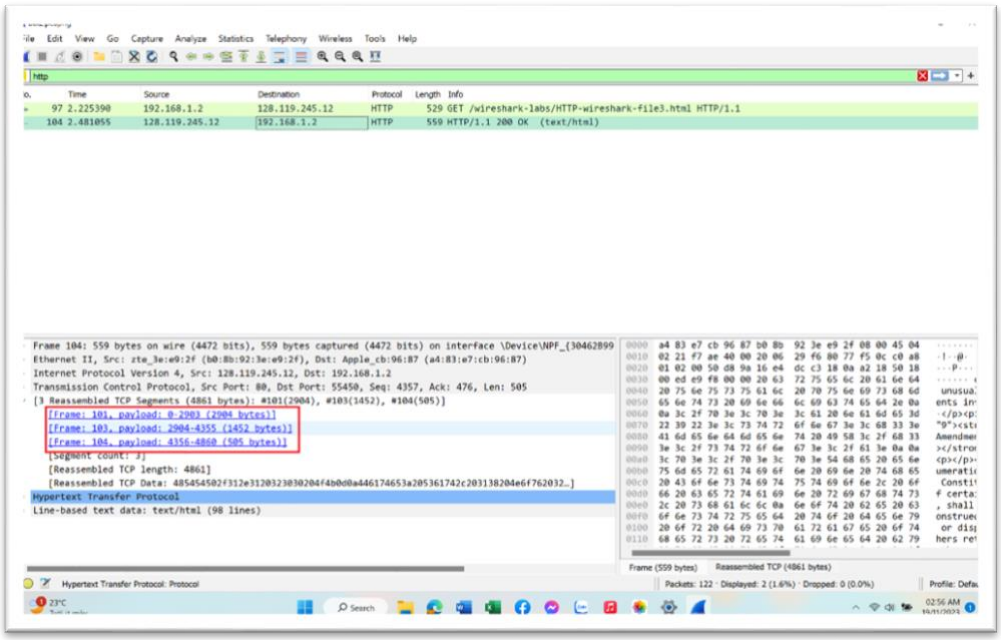
Trình duyệt đã gửi 1 HTTP GET (xem ảnh 11)



Ảnh 11

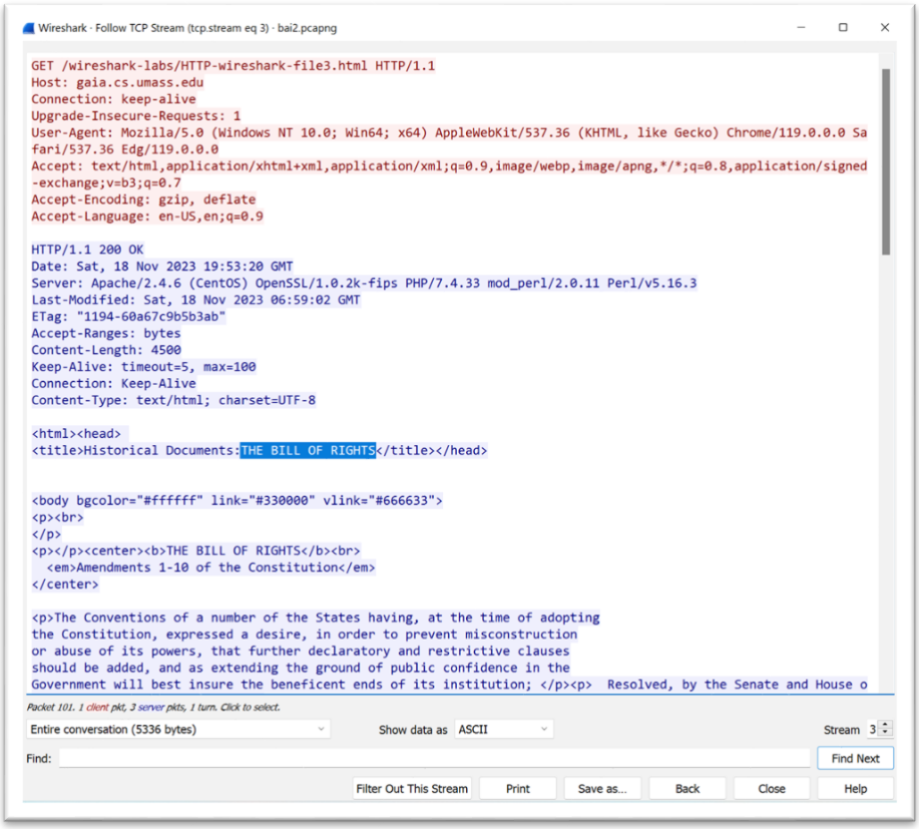
11. Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

Cần 3 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights.



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

Dòng "THE BILL OF RIGHTS" được chứa trong gói tin phản hồi thứ nhất.


Wireshark · Follow TCP Stream (tcp.stream eq 3) · bai2.pcapng
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
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/119.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Date: Sat, 18 Nov 2023 19:53:20 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sat, 18 Nov 2023 06:59:02 GMT
ETag: "1194-60a67c9b5b3ab"
Accept-Ranges: bytes
Content-Length: 4500
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<html><head>
<title>Historical Documents:THE BILL OF RIGHTS</title></head>
<body bgcolor="#ffffff" link="#330000" vlink="#666633">

THE BILL OF RIGHTS
Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting
the Constitution, expressed a desire, in order to prevent misconstruction
or abuse of its powers, that further declaratory and restrictive clauses
should be added, and as extending the ground of public confidence in the
Government will best insure the beneficent ends of its institution; Resolved, by the Senate and House o
Packet 101. 1 client pkt, 3 server pkts, 1 turn. Click to select.
Entire conversation (5336 bytes)
Show data as ASCII
Stream 3
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

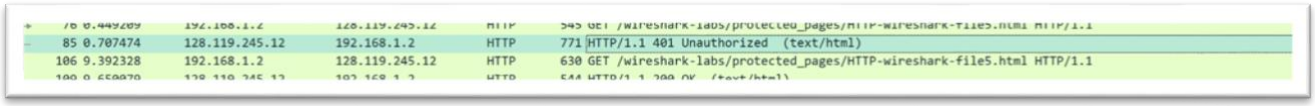
Ảnh 12

III. Chứng thực HTTP

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

- Mã trạng thái trong HTTP response tương ứng với HTTP GET đầu tiên là 401 Unauthorized.

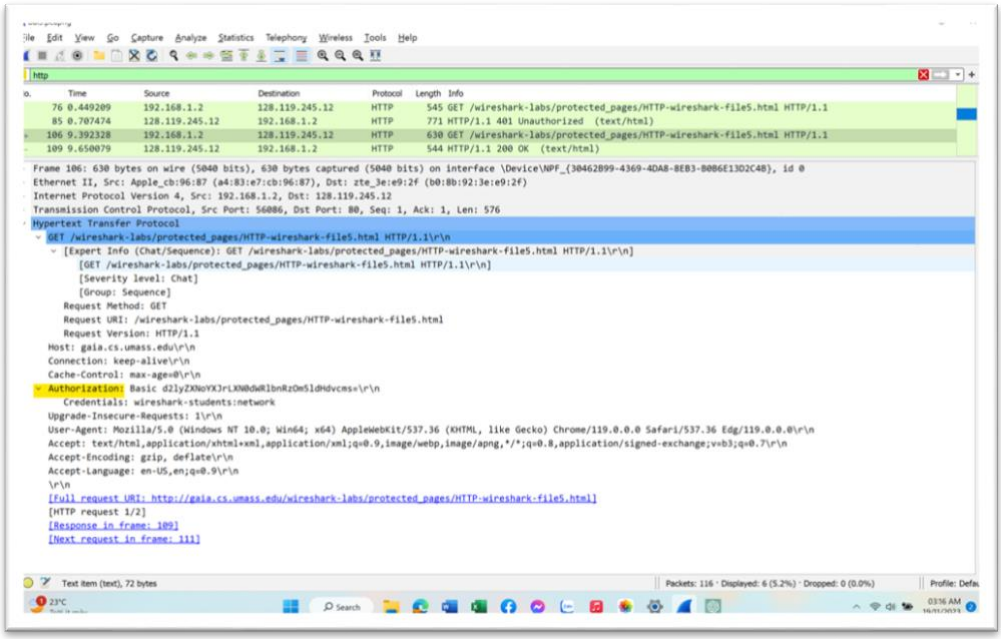
- Mã trạng thái HTTP 401 Unauthorized là một mã trả lời từ máy chủ web cho một yêu cầu HTTP mà máy chủ không chấp nhận do thiếu thông tin xác thực hợp lệ. Nó thường được sử dụng để yêu cầu người dùng cung cấp thông tin đăng nhập hoặc token xác thực để có quyền truy cập tài nguyên được yêu cầu. (xem ảnh 13)



Ảnh 13

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

Khi trình duyệt gửi HTTP GET lần thứ 2, xuất hiện một trường dữ liệu mới là trường Authorization trong HTTP GET.



Ảnh 14