

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

----------



NHẬP MÔN MẠNG MÁY TÍNH – IT005.Q111.1

BÁO CÁO THỰC HÀNH LAB 2

Phân tích gói tin HTTP với Wireshark

Giảng viên hướng dẫn: Nguyễn Thanh Nam

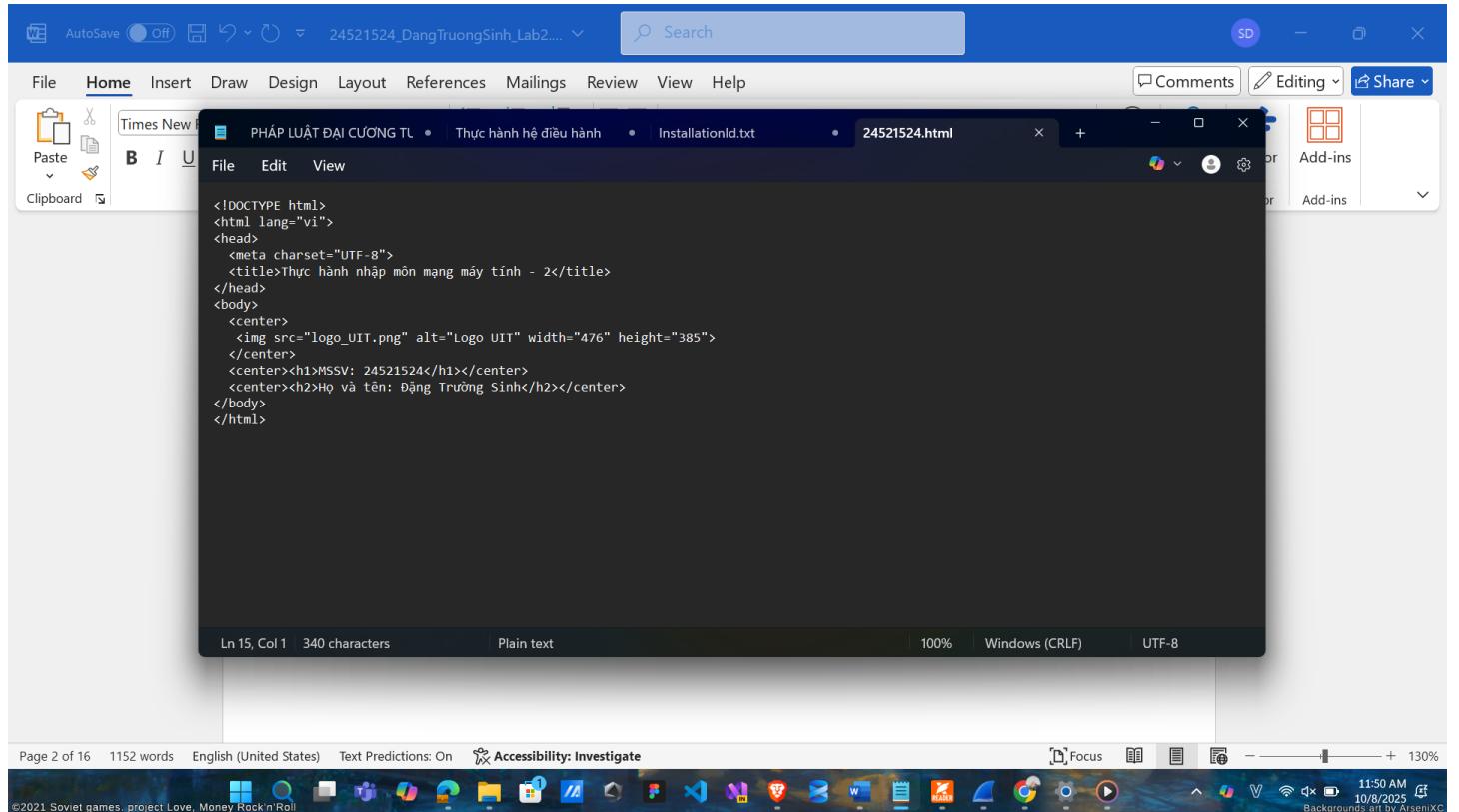
Sinh viên thực hiện: Đặng Trường Sinh – 24521524

© Tp. Hồ Chí Minh, 10/2025

1. Tạo một website đơn giản trên local host

a) Tạo 1 website sử dụng HTML đơn giản

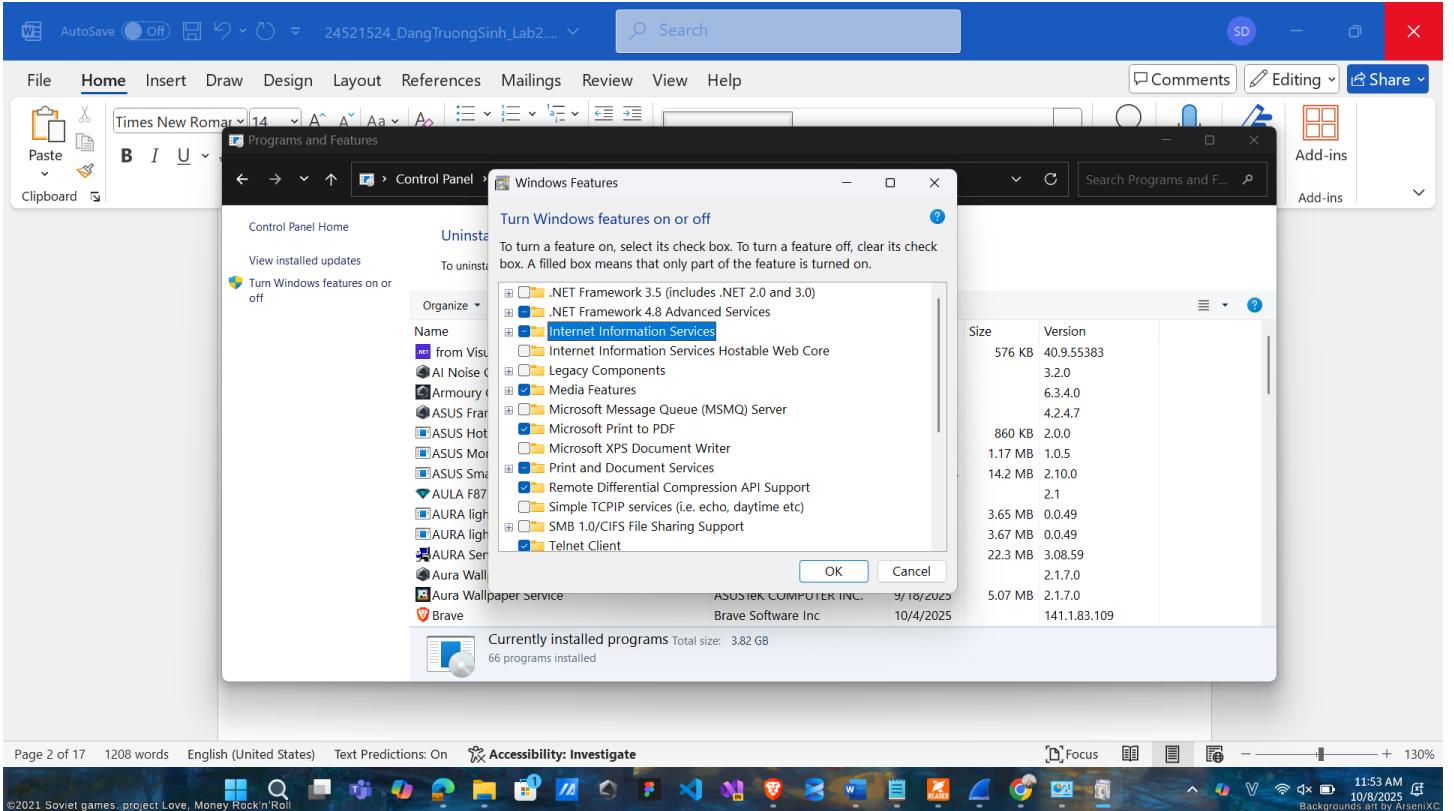
Bước 1: Mở notepad và tạo các dòng HTML như hình dưới và lưu file với định dạng 24521524.html:



Hình 1: Tạo 1 file HTML đơn giản

b) Cấu hình Webserver với IIS trên Windows

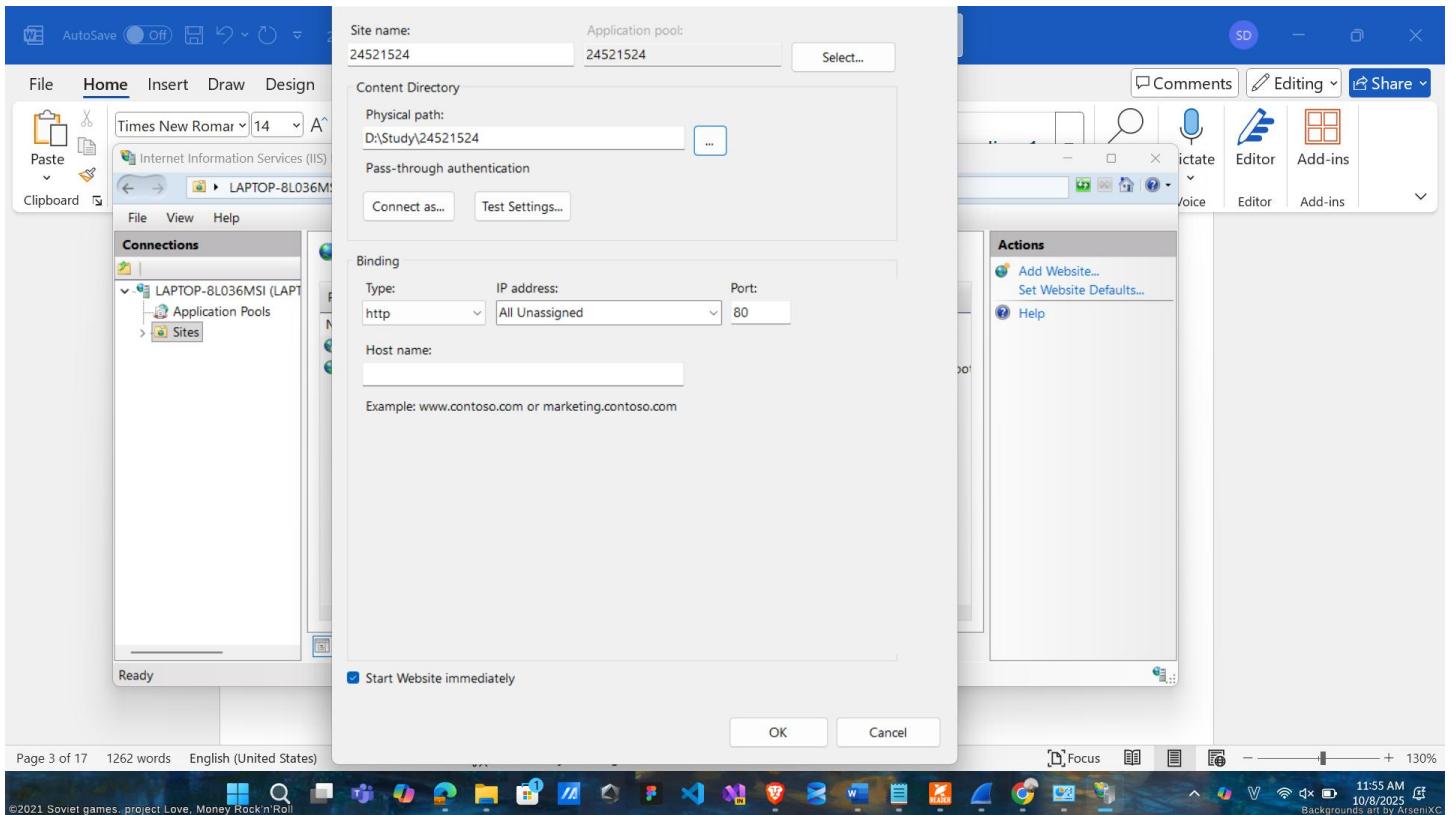
Bước 1: Bật dịch vụ IIS với các bước sau: Control Panel -> Programs and features -> Turn Windows Features on or off -> Chọn Internet Information Service -> OK



Hình 2: Bật dịch vụ ISS

Bước 2: Vào phần search tìm phần **Internet Information Services (IIS) Manager** để có thể tạo trang Web trên server.

Bước 3: Để tạo mới một Website, nhấp chuột phải vào **Site -> Add Website**. Đặt **Sitename** là MSSV (MSSV của sinh viên thực hiện), **Physical path** là tên folder tùy ý (Physical path của sinh viên thực hiện là như hình bên dưới).



Hình 3: Site name và Physical path

Bước 4: Truy cập vào website của mình với đường dẫn <http://localhost/24521524.html>

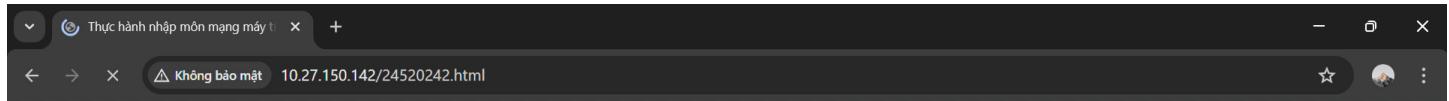


MSSV: 24521524

Họ và tên: Đặng Trường Sinh

Bước 5: Truy cập thử trang web của sinh viên khác từ trình duyệt bằng các gõ URL như sau:

A.B.C.D/MSSV.html với A.B.C.D là địa chỉ IP của máy tính mà bạn mình sử dụng. MSSV.html là file html mà bạn mình tạo ra.



↳

MSSV: 24520242

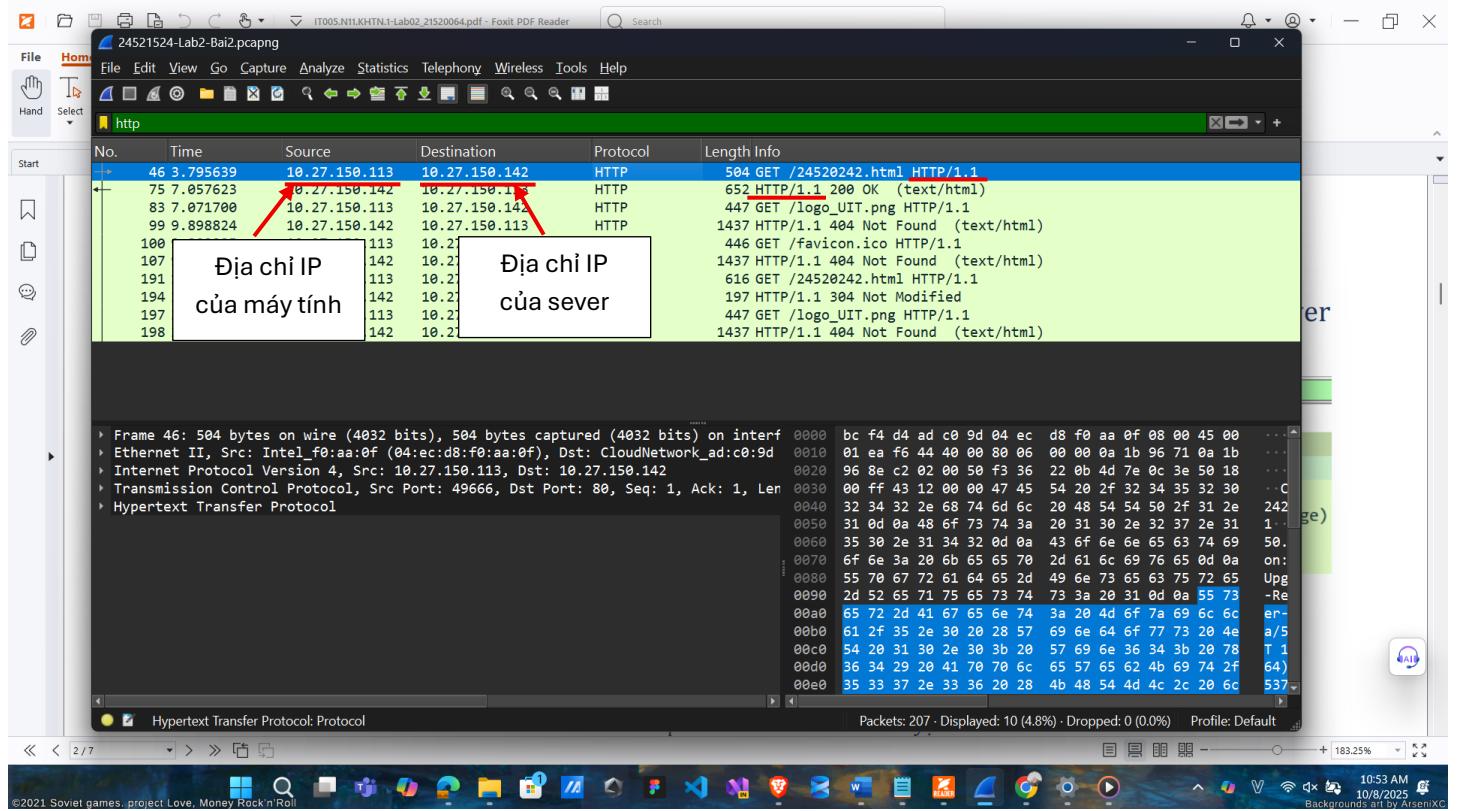
Họ và tên: Nguyễn Xuân Cường



Hình 5: Truy cập vào 1 website của sinh viên cùng lớp

2. HTTP GET / reponse 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?



Hình 6: Phiên bản HTTP của trình duyệt và của sever

Nhìn vào hình ta có thể thấy khi trình duyệt gửi yêu cầu đến sever thì gói tin **HTTP GET** có info của HTTP là **HTTP 1.1** do đó phiên bản HTTP mà trình duyệt sử dụng là **HTTP 1.1**

Cũng nhìn vào hình trên ta thấy sau khi nhận **request** từ trình duyệt thì sever phản hồi bằng 1 gói tin HTTP có nội dung **200 OK** và nhìn vào phần info ta thấy rằng phiên bản HTTP của sever là **HTTP 1.1**

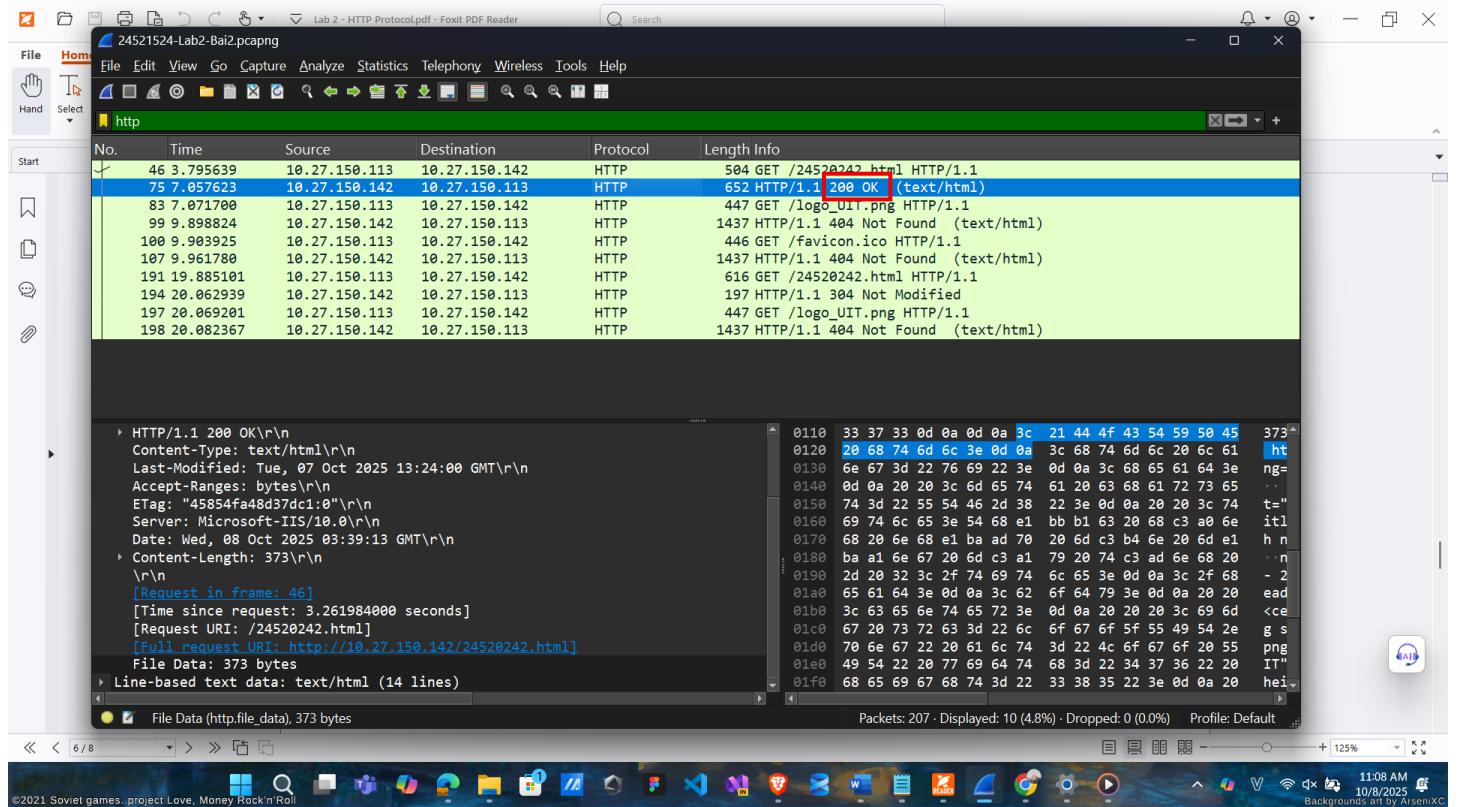
2. Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

Nhìn vào hình trên, ở phần gói tin HTTP mà trình duyệt yêu cầu thì địa chỉ IP trong source chính là địa chỉ IP của máy tính và phần IP trong phần Destination chính là địa chỉ IP của sever, do đó:

- Địa chỉ IP của máy tính: **10.27.150.113**
- Địa chỉ IP của sever: **10.27.150.142**

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

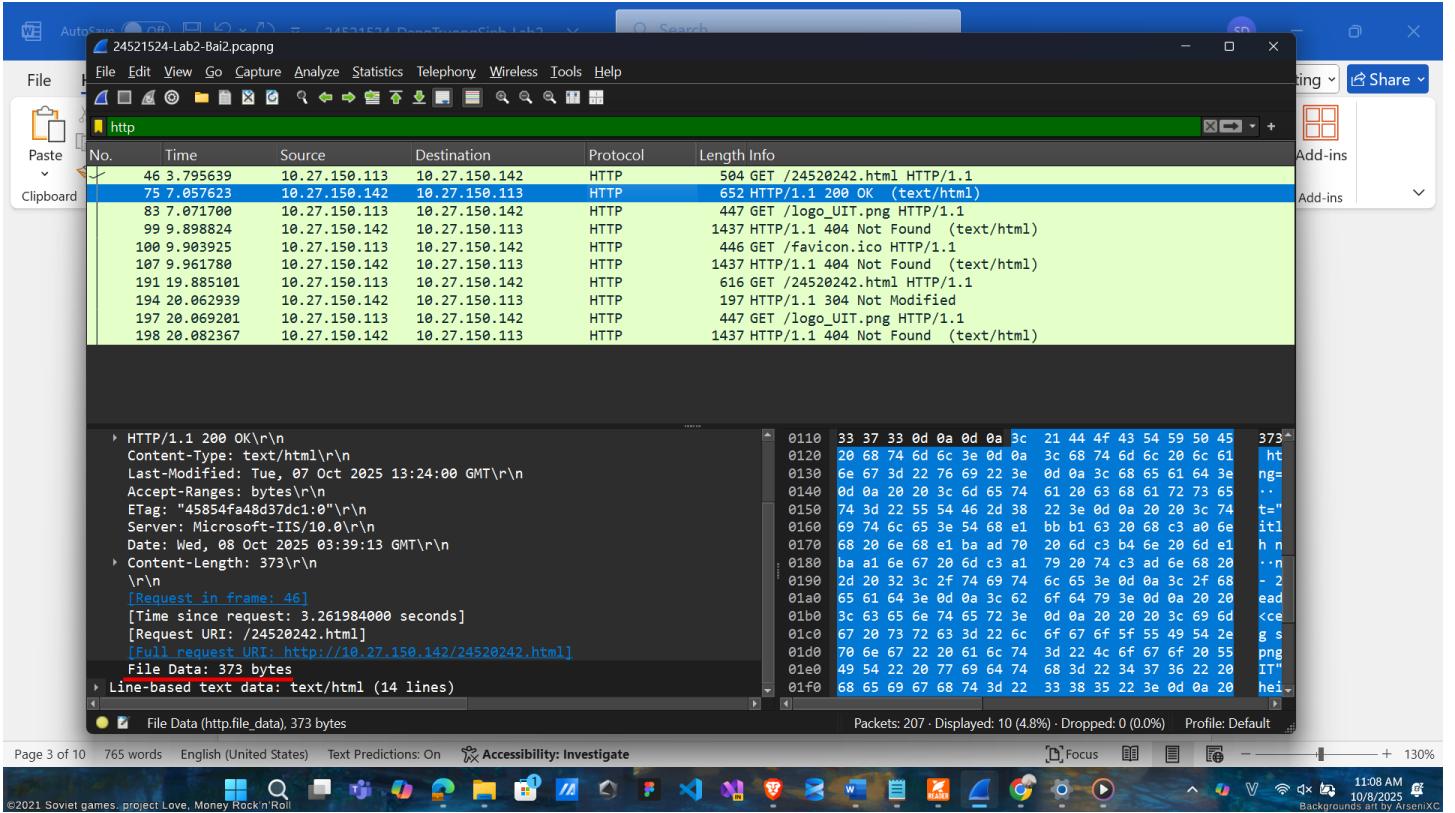
Mã trạng thái của code trả về sever là **200 OK**



Hình 7: Mã trạng thái của sever trả về

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

Để xem được số byte nội dung mà trình duyệt trả về ta chọn gói tin **HTTP GET** đầu tiên, số bytes nội dung mà sever trả về nằm trong phần **Hypertext Transfer Protocol -> File Data**

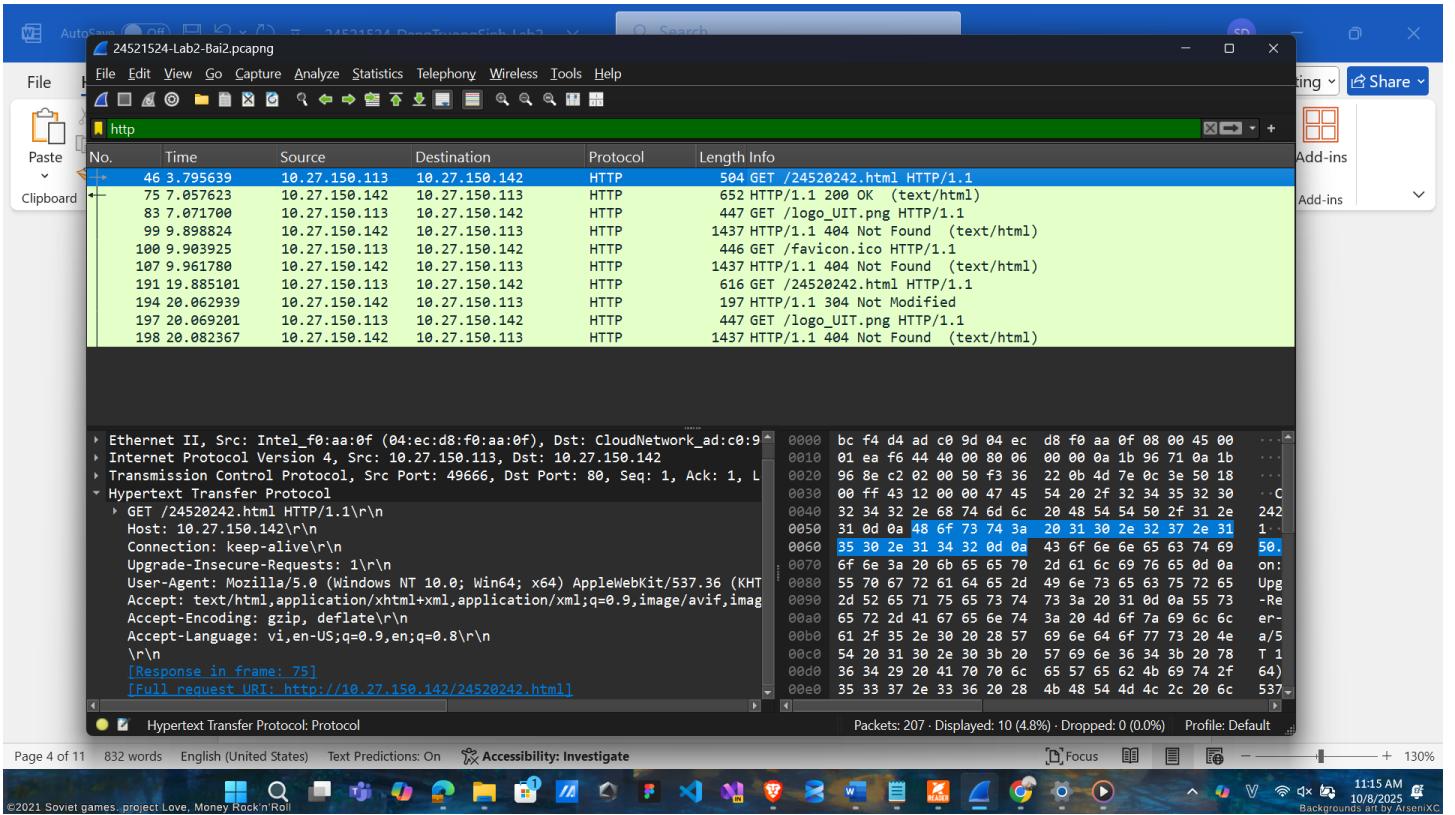


Hình 8: Số bytes mà sever đã trả về cho trình duyệt

- Nhìn vào hình ta có thể thấy sever đã trả về cho trình duyệt **373 bytes** nội dung

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

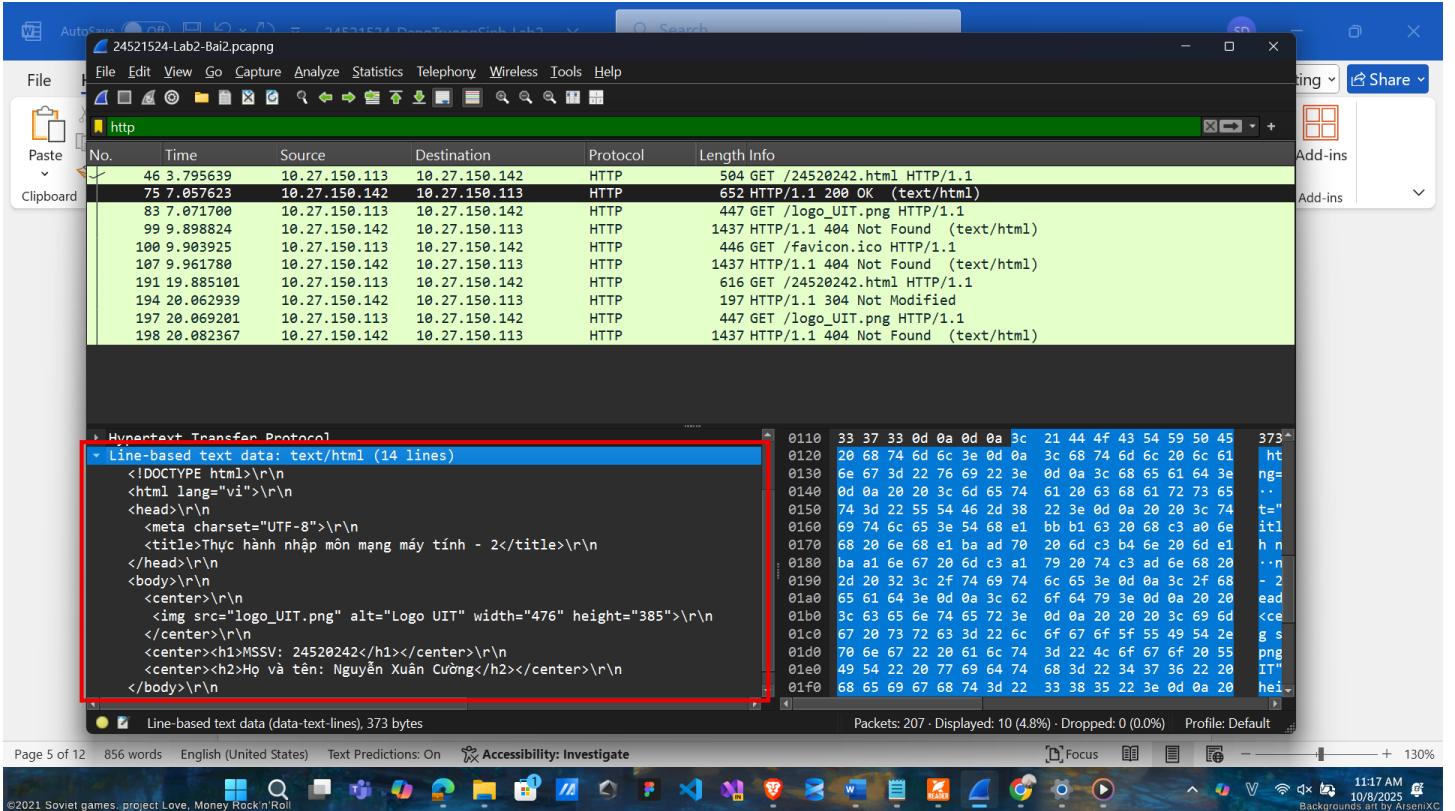
- Sau khi xem xét nội dung HTTP GET đầu tiên thì **không thấy** dòng “**IF-MODIFIED-SINCE**”



Hình 9: Nội dung của HTTP GET đầu tiên

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

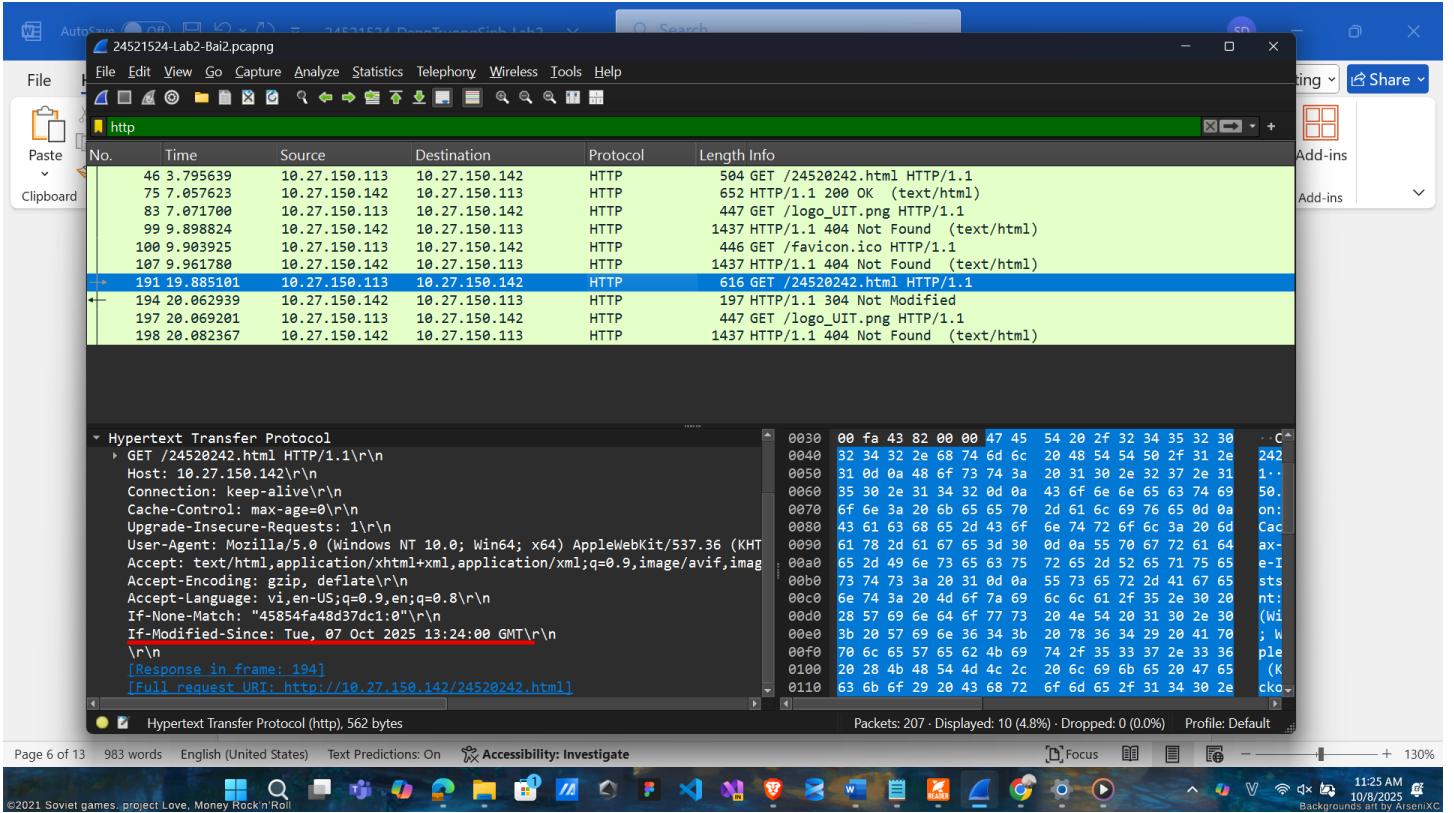
- Khi xem xét nội dung phản hồi từ sever. Sever có trả nội dung của file HTML
- Vì khi trình duyệt gửi yêu cầu lên sever, sever sẽ xem xét cache của trình duyệt có chứa nội dung của file đó chưa nếu chưa thì sever sẽ trả về nội dung của file đó, còn ngược lại thì sever sẽ không trả về nội dung nữa. Do trước khi truy cập trang web ta đã xoá hết cache nên khi truy cập sever kiểm tra cache và không thấy cache chứa nội dung của file cho nên sever sẽ trả nội dung về cho trình duyệt.



Hình 10: Nội dung mà sever trả về

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?

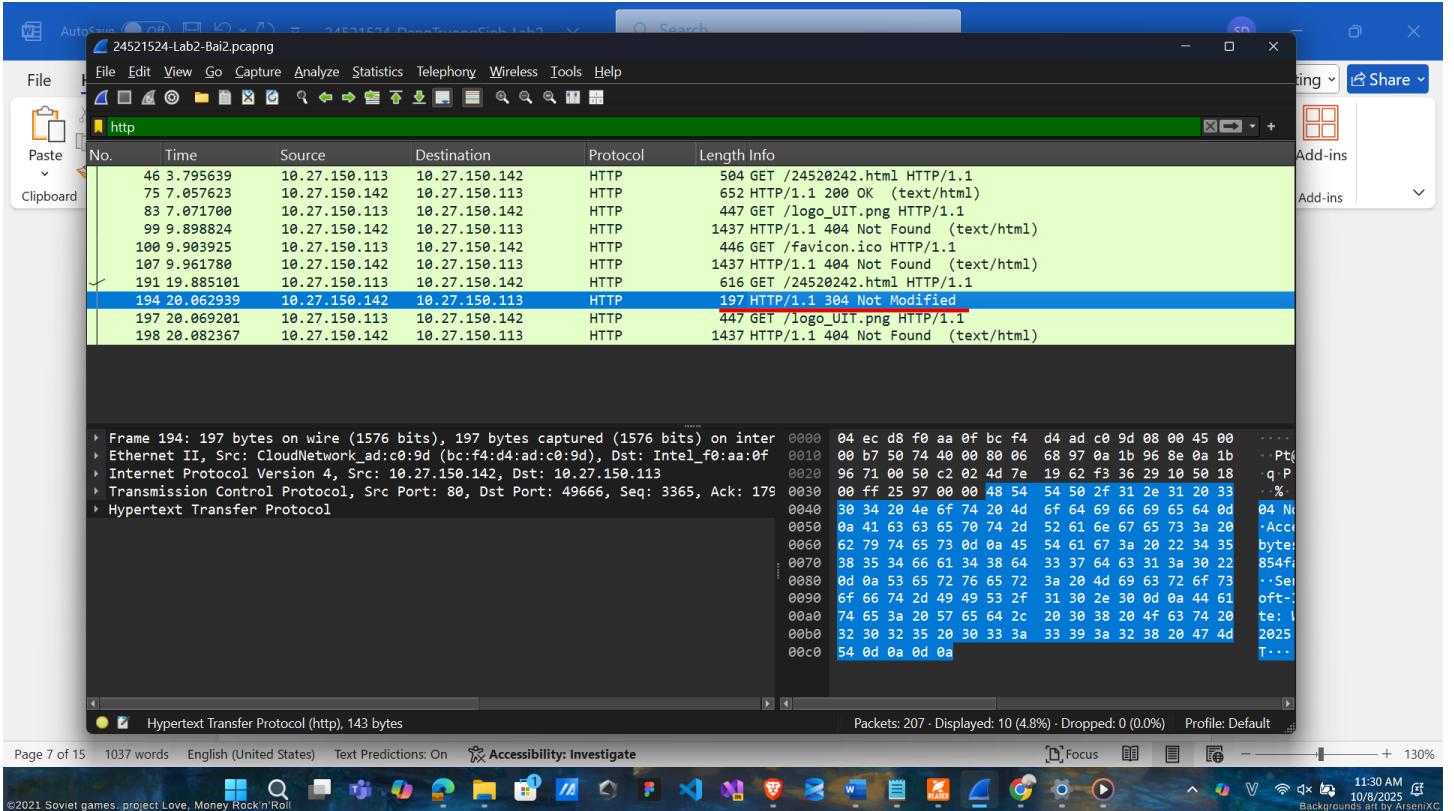
- Xem xét nội dung của HTTP GET thứ 2. Ta thấy có dòng “IF-MODIFIED-SINCE” xuất hiện.
- Giá trị của IF-MODIFIED-SINCE là: Tue, 07 Oct 2025 13:24:00 GMT



Hình 11: Giá trị của If-Modified-Since

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.

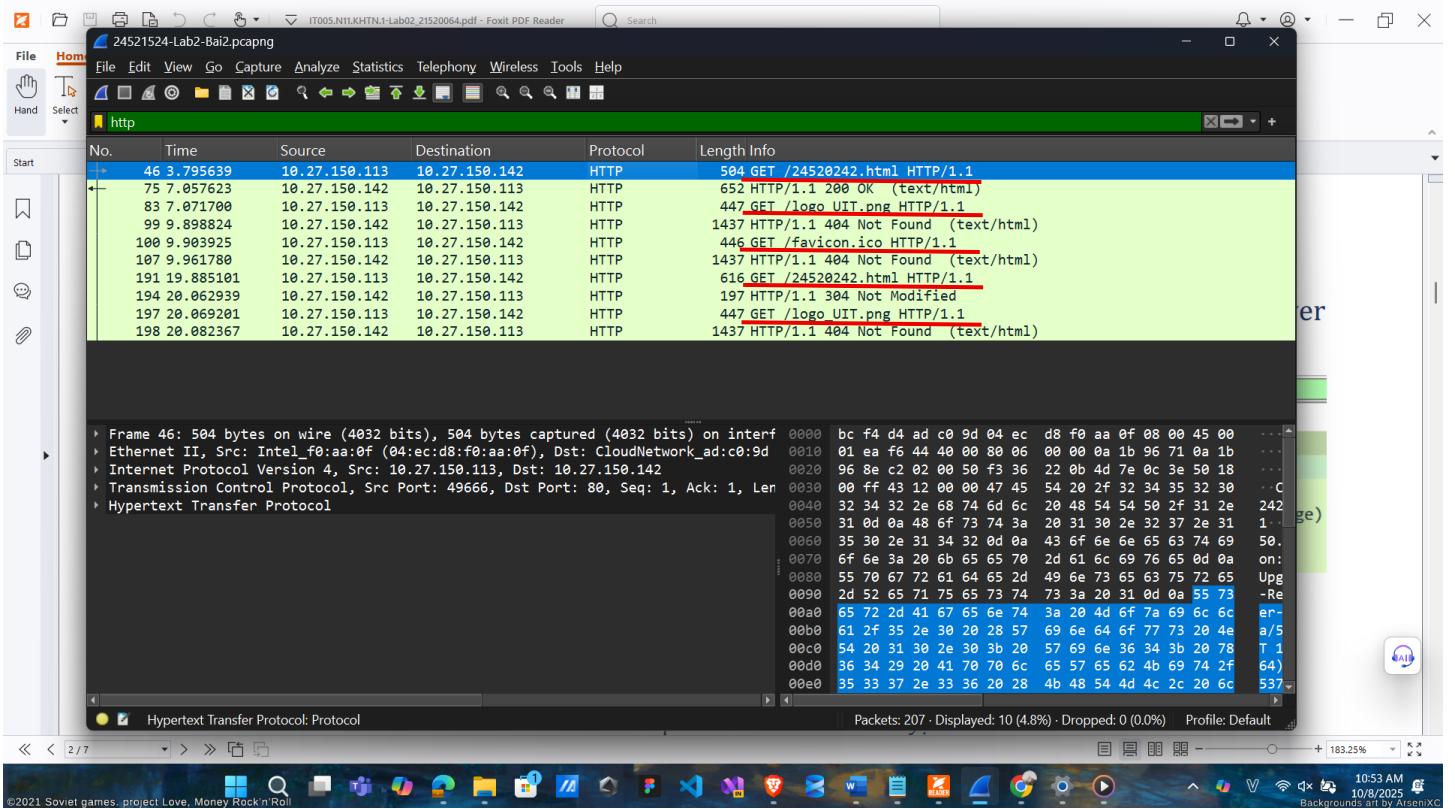
- Mã trạng thái HTTP được trả về từ sever tương ứng với **HTTP GET thứ 2 là 304 Not Modified**
- Ý nghĩa của nó là nội dung của trang web không có gì thay đổi từ lần **request** trước đó.
- Nhìn vào ảnh ta có thể thấy sever không gửi về nội dung nội dung như lần **GET** đầu tiên
- Vì lúc này, trong bộ 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, sever sẽ không gửi lại nội dung đó cho người dùng nữa.



Hình 11: Mã trạng thái ứng với HTTP GET thứ 2

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

- Nhìn hình ta có thể thấy trình duyệt đã gửi 5 HTTP GET. Và cả 5 đều đến địa chỉ IP **10.27.150.142**

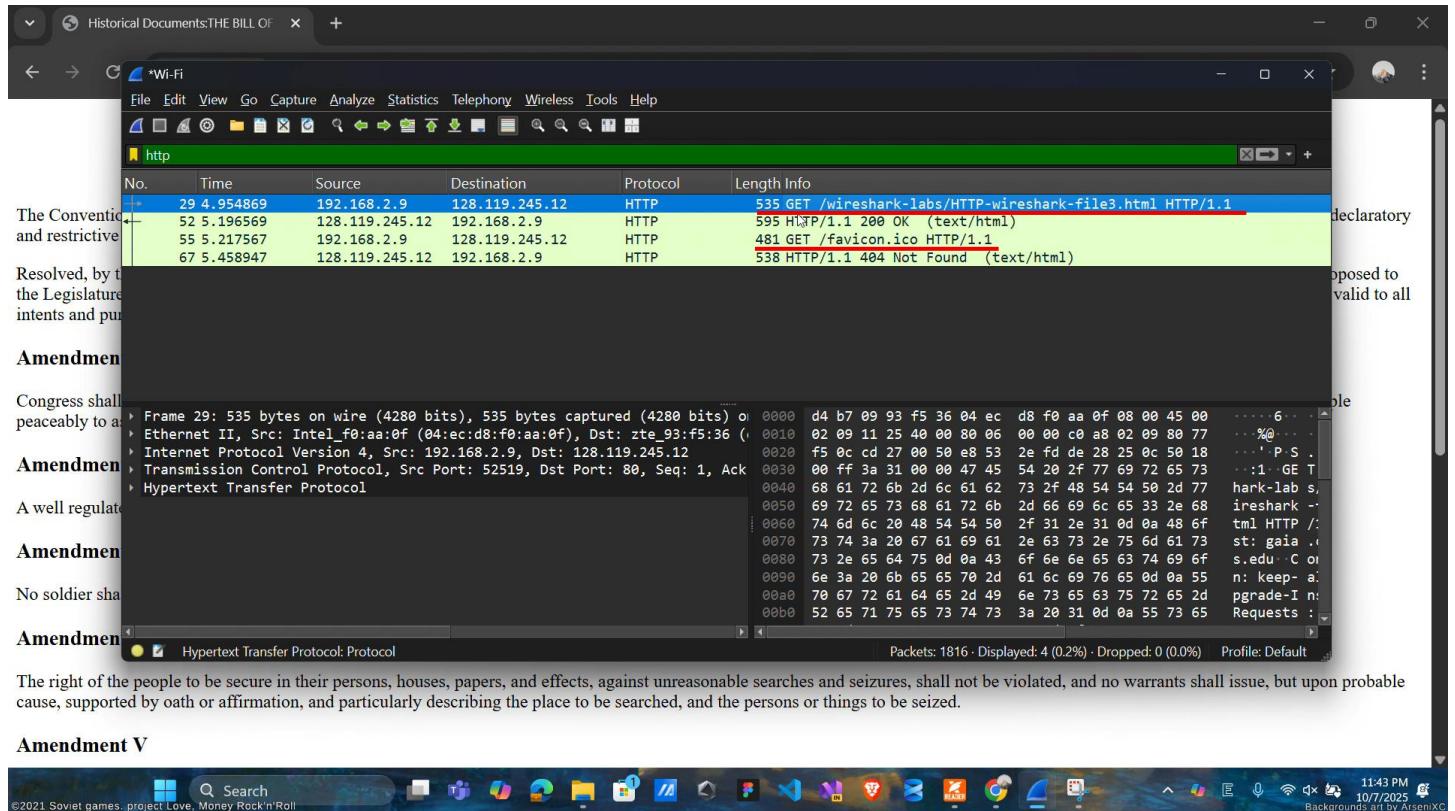


Hình 12: Số lượng HTTP GET mà trình duyệt đã gửi

3. Truy cập các trang HTTP dài

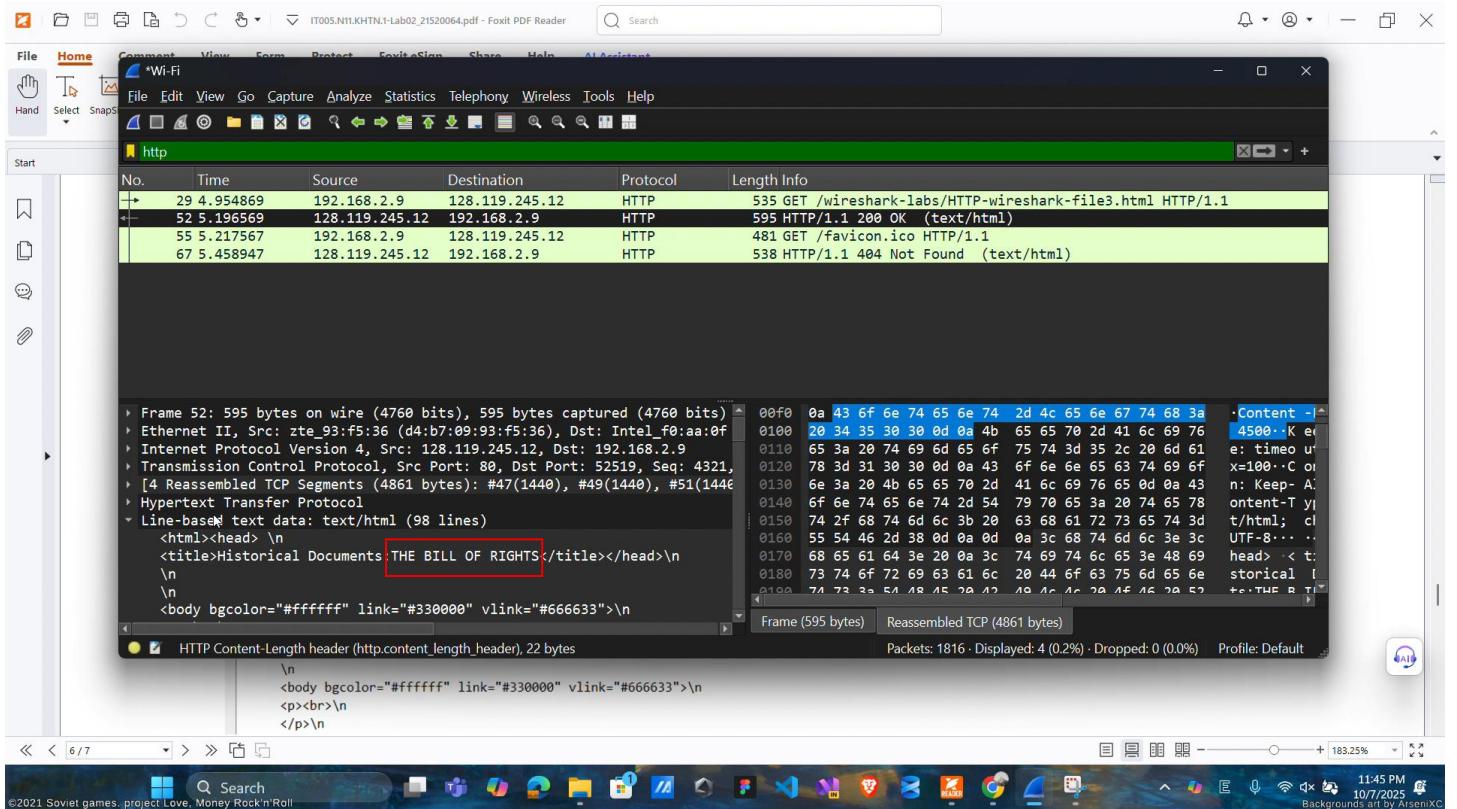
10.Trình duyệt đã gửi bao nhiêu HTTP GET? Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy?

- Trình duyệt đã gửi 2 HTTP GET.



Hình 13: Số HTTP GET mà trình duyệt đã gửi

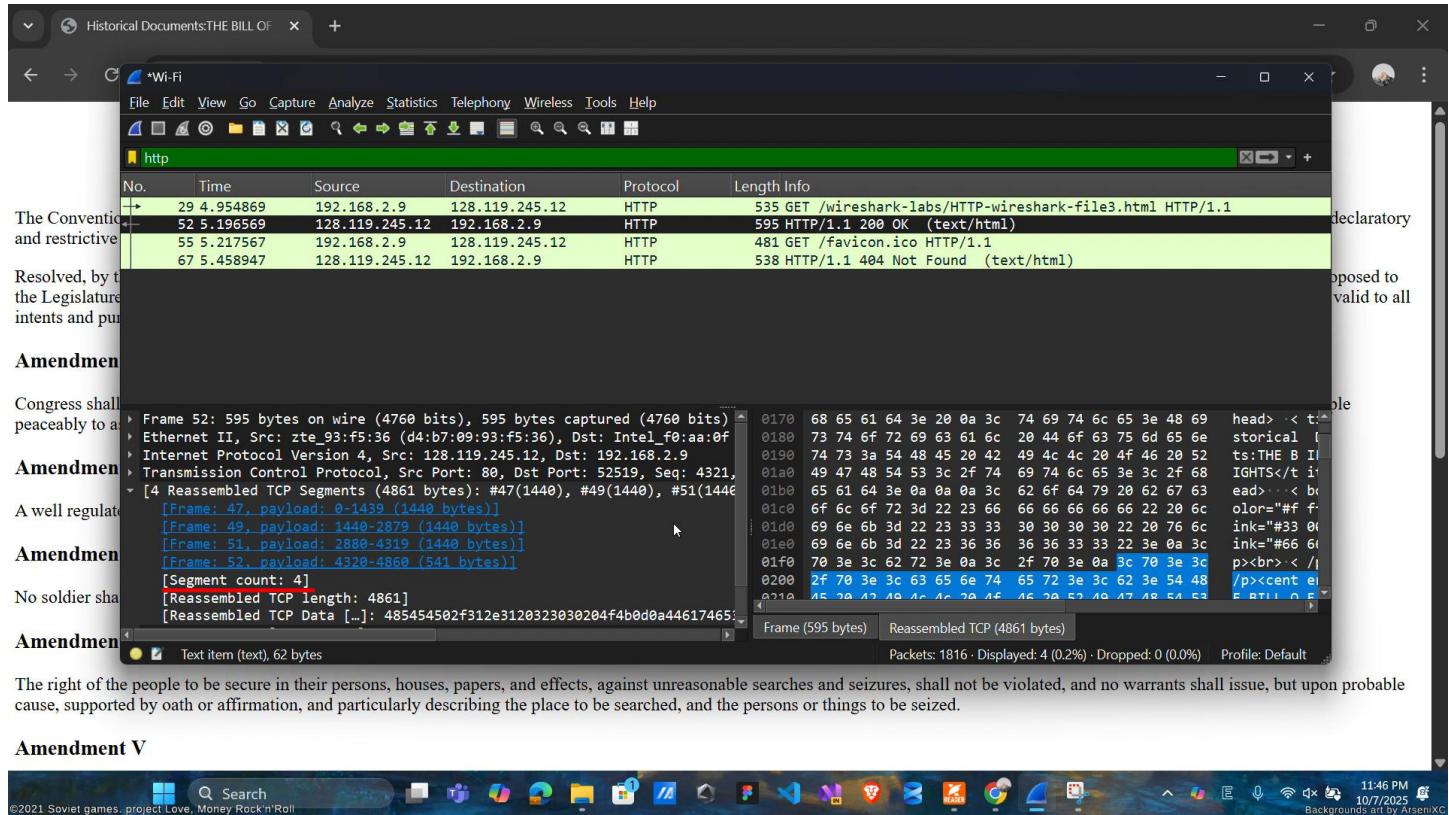
- Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi đầu tiên (**200 OK**)



Hình 14: Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi đầu tiên

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

Nhìn vào hình dưới ta có thể thấy **Segment count** là 4. Do đó, ta cần 4 **TCP segments** để chứa hết **HTTP response** và nội dung của The Bill of Rights.

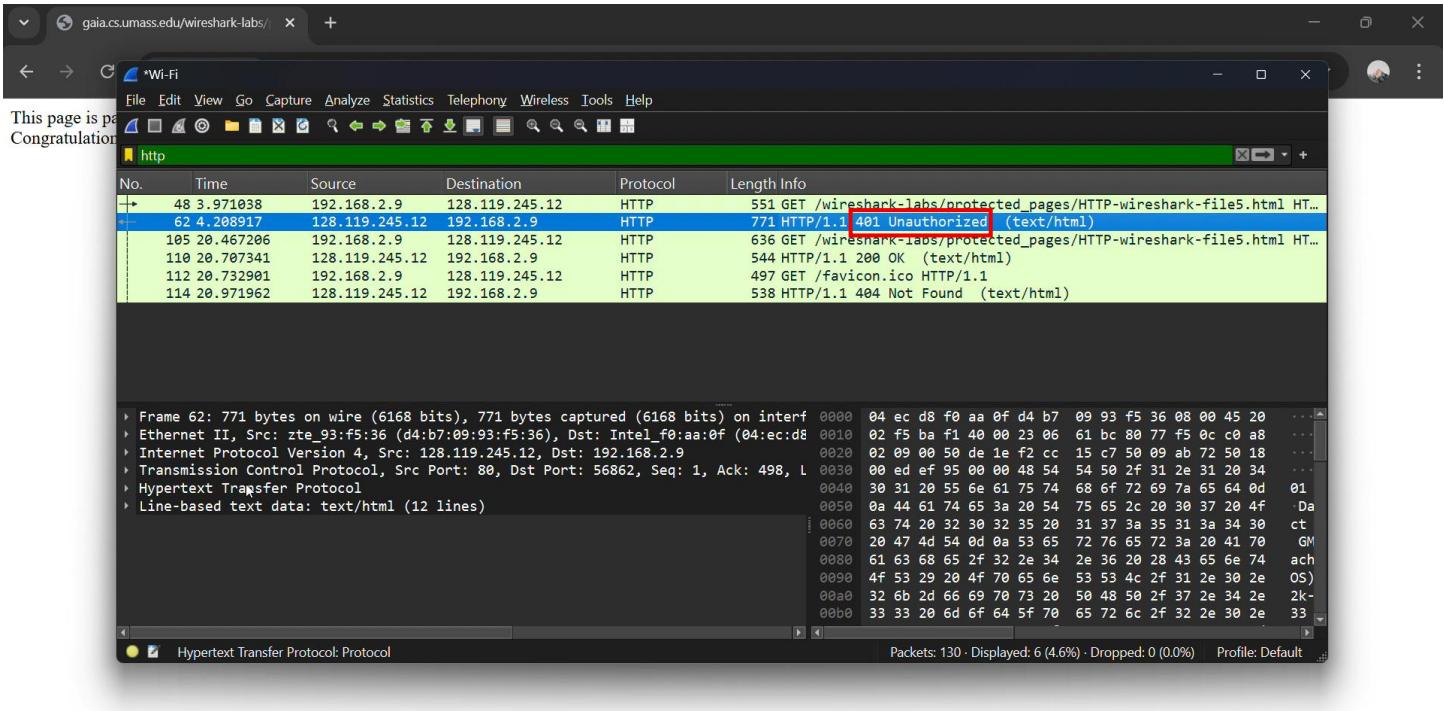


Hình 15: Số TCP segments cần để chứa hết HTTP reponse và nội dung của The Bill of Rights

4. Chứng thực HTTP

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

- Nhìn vào hình dưới, ta thấy **HTTP response** tương ứng với **HTTP GET** 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.

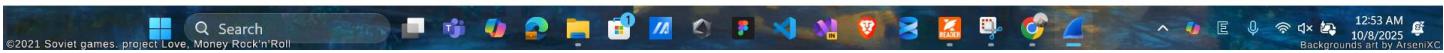
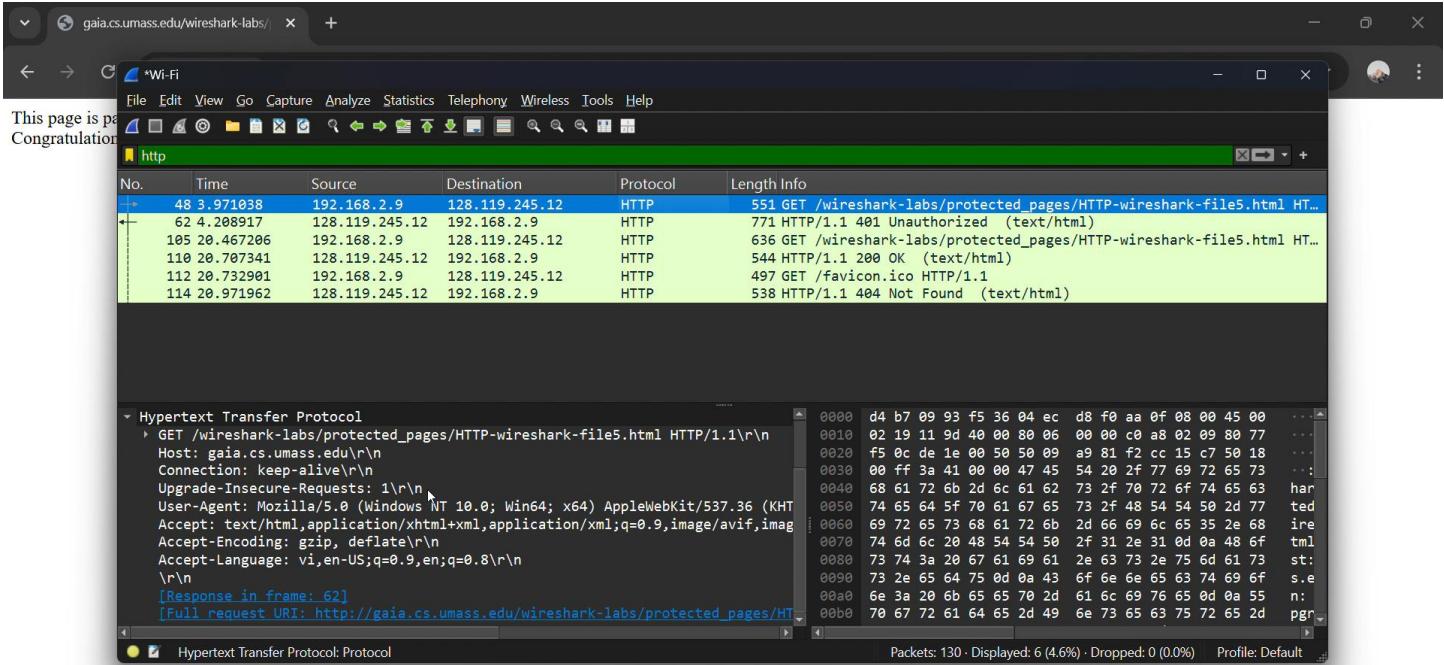


Hình 16: Mã trạng thái trong **HTTP reponse** tương ứng với **HTTP GET** đầu tiên

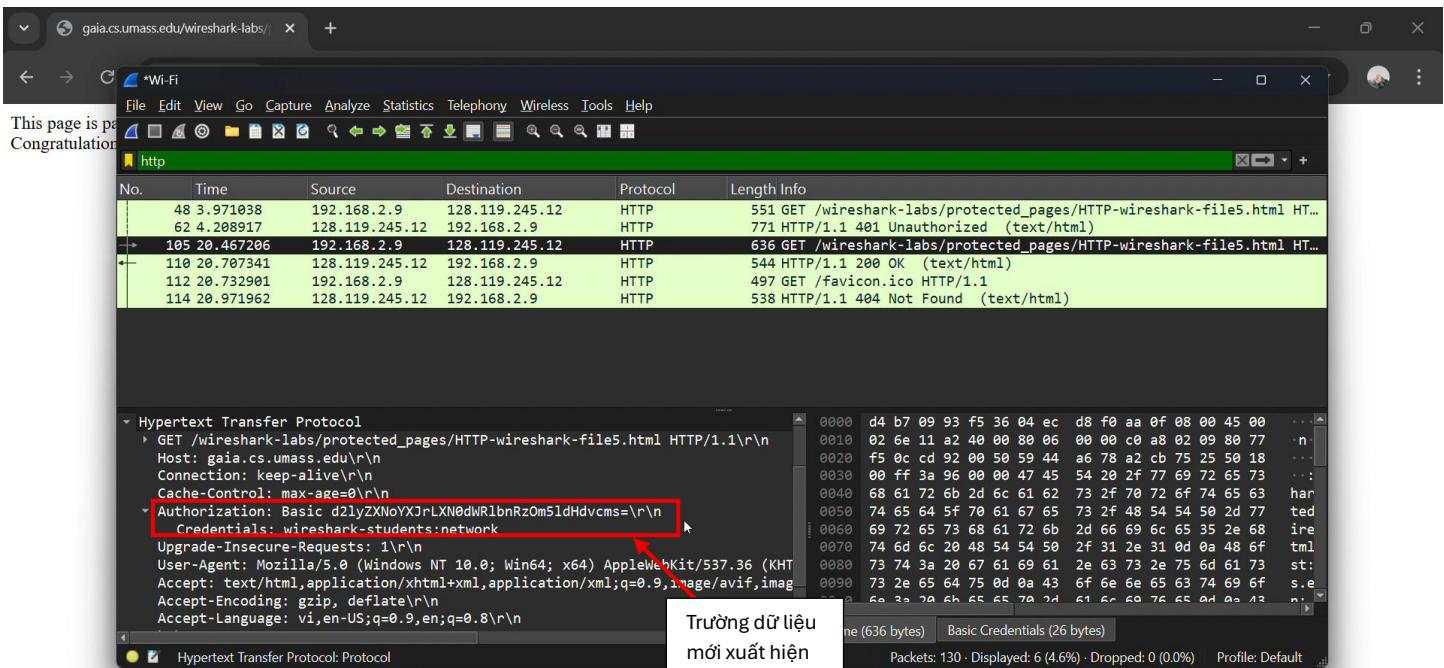
13. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?

- Khi so sánh giữa nội dung gói tin **HTTP GET** lần thứ 1 và lần thứ 2, ta thấy rằng, trong nội dung của **HTTP GET** lần thứ 2 xuất hiện trường dữ liệu mới: **Authorization**.
- Trong trường dữ liệu mới đó, ta thấy nội dung **Credentials** nó lưu giữ thông tin **username** và **password** mà ta phải nhập vào nếu muốn truy cập vào trang web.

Lab02 – Phân tích gói tin HTTP với Wireshark



Hình 17: Nội dung gói tin **HTTP GET** lần thứ nhất



Hình 18: Nội dung gói tin **HTTP GET** lần thứ hai