BÁO CÁO LAB 02

PHÂN TÍCH GÓI TIN HTTP VỚI WIRESHARK

Sniffing HTTP Traffic with Wireshark

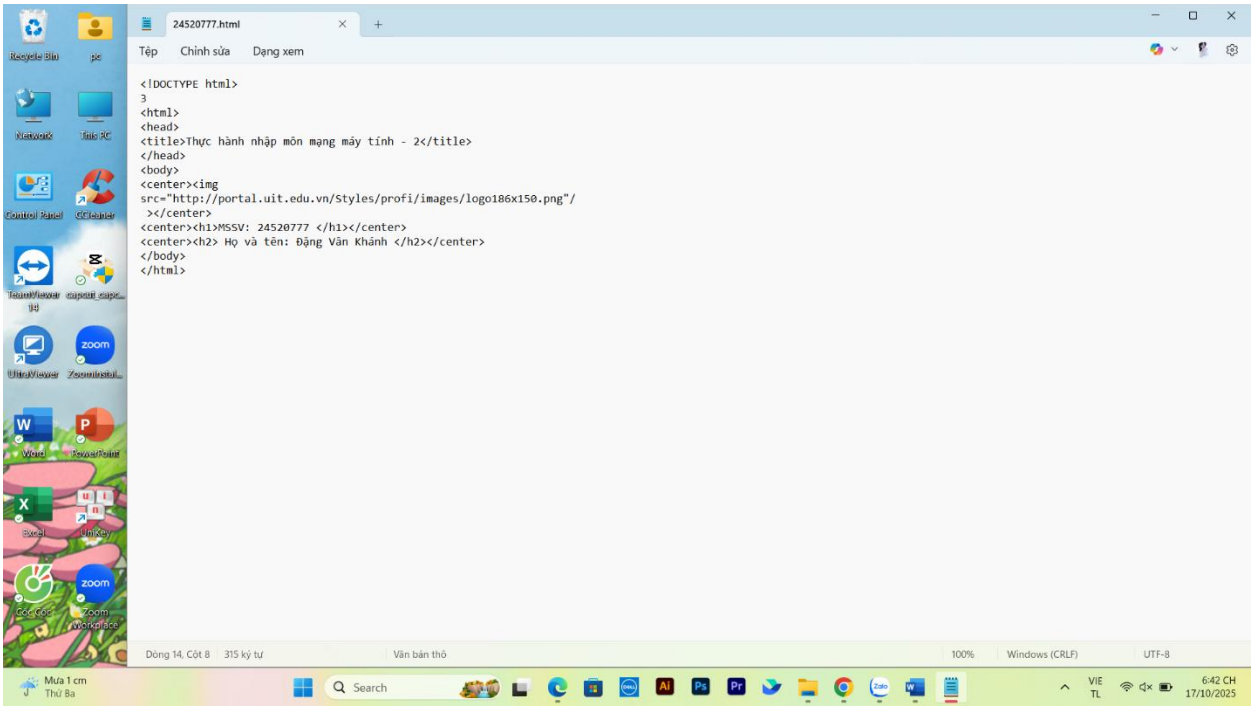
Giảng viên hướng dẫn thực hành: Nguyễn Thanh Nam

Đặng Vân Khánh – 24520777

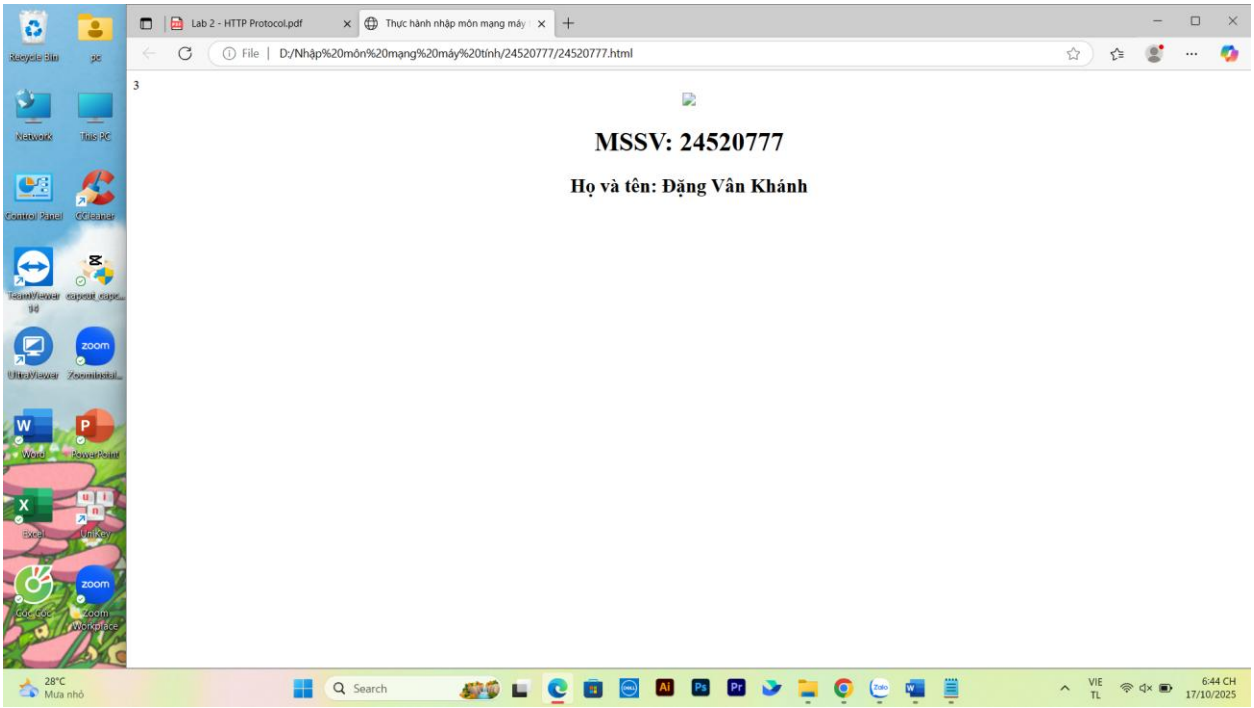
15-10-2025

I. Cài đặt xây dựng website đơn giản

Bước 1 + 2: Mở chương trình soạn thảo Notepad tạo các dòng html được lưu với tên MSSV.html

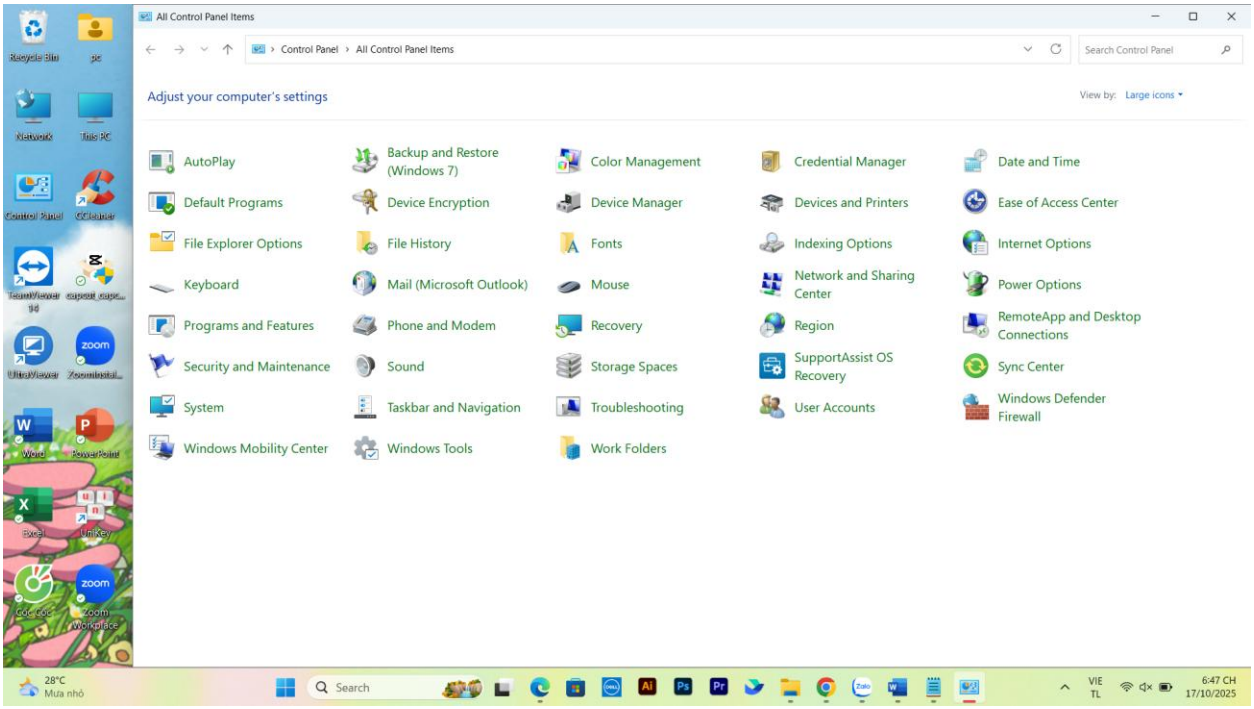


Bước 3: Website hiển thị

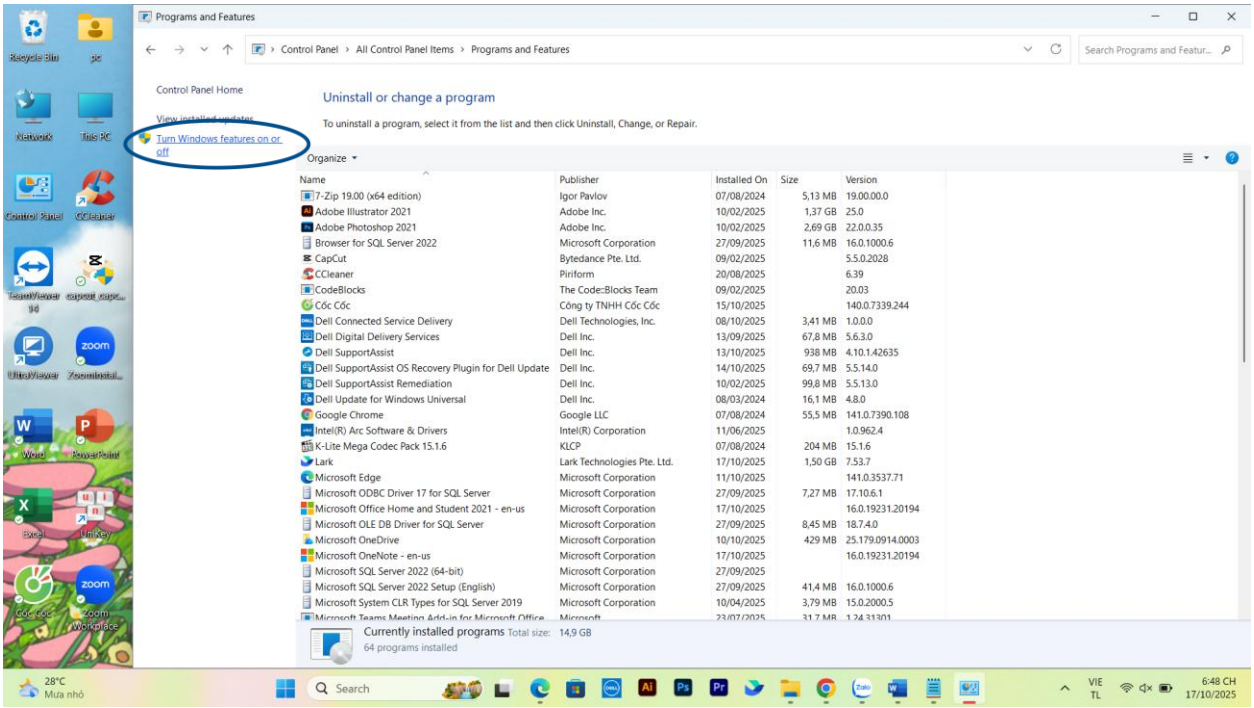


Cấu hình Webserver với IIS trên Windows

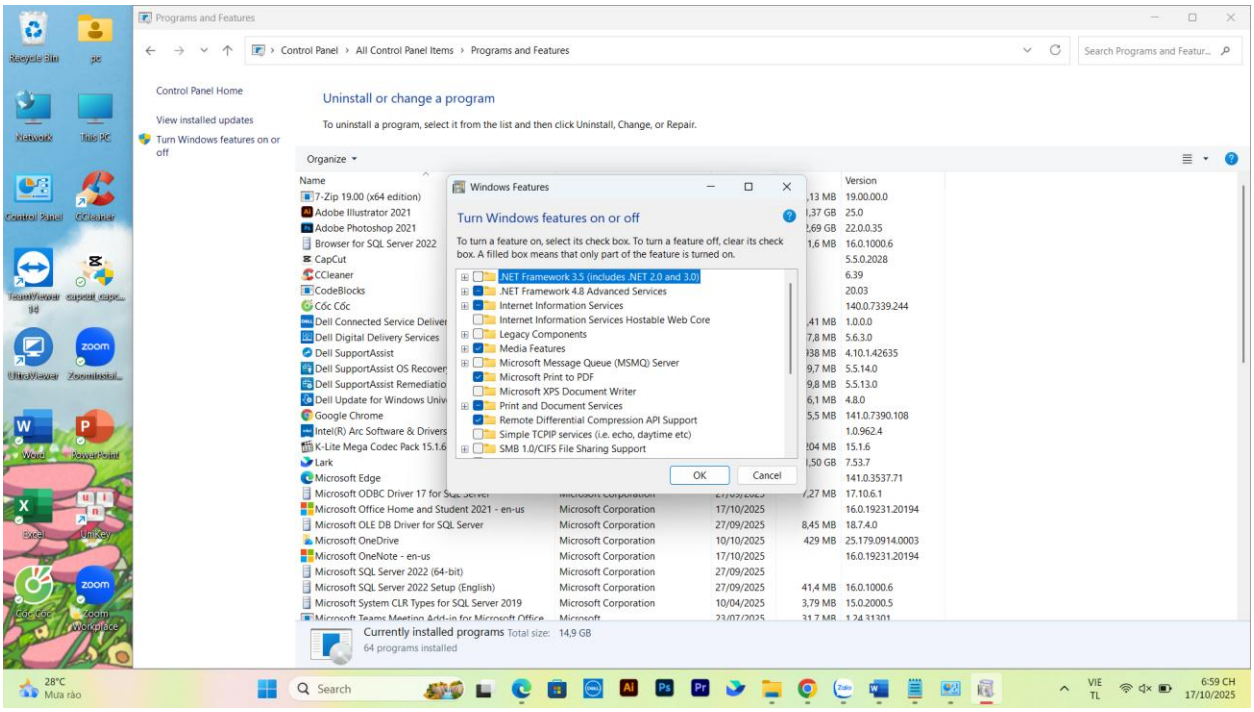
Bước 1: Control Panel



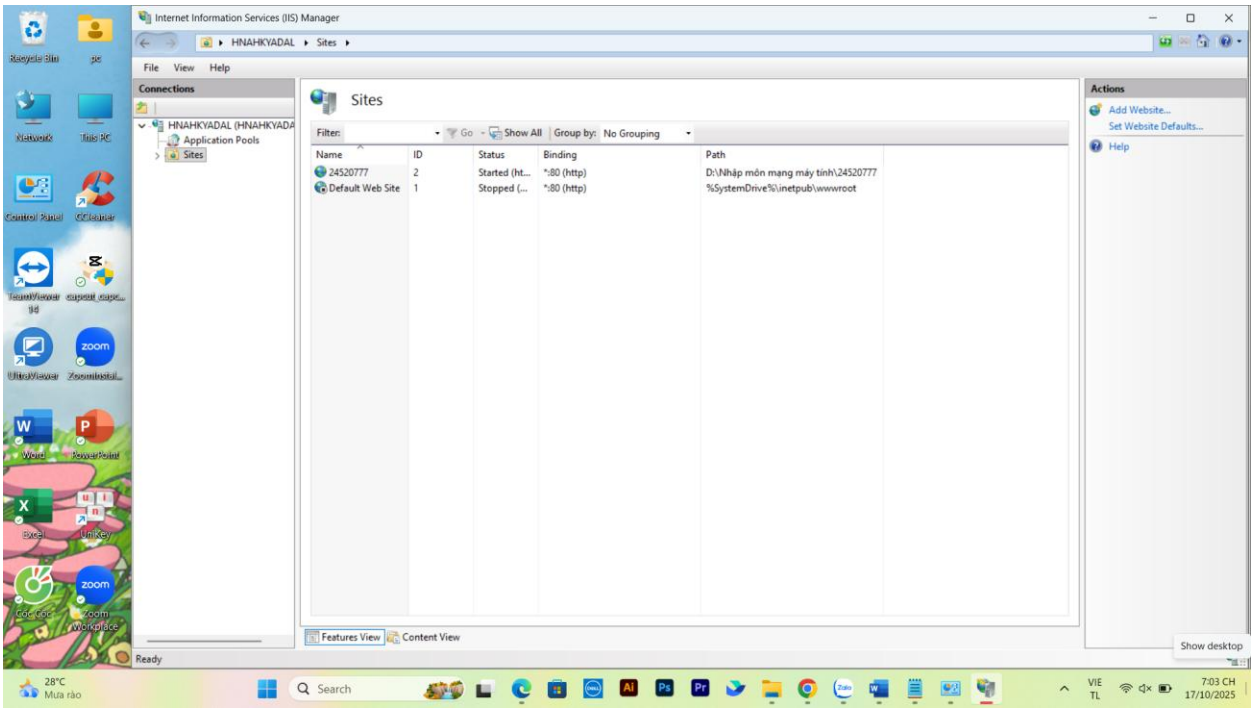
Bước 2: Program and features → Windows Features on or off được khoanh vùng màu xanh

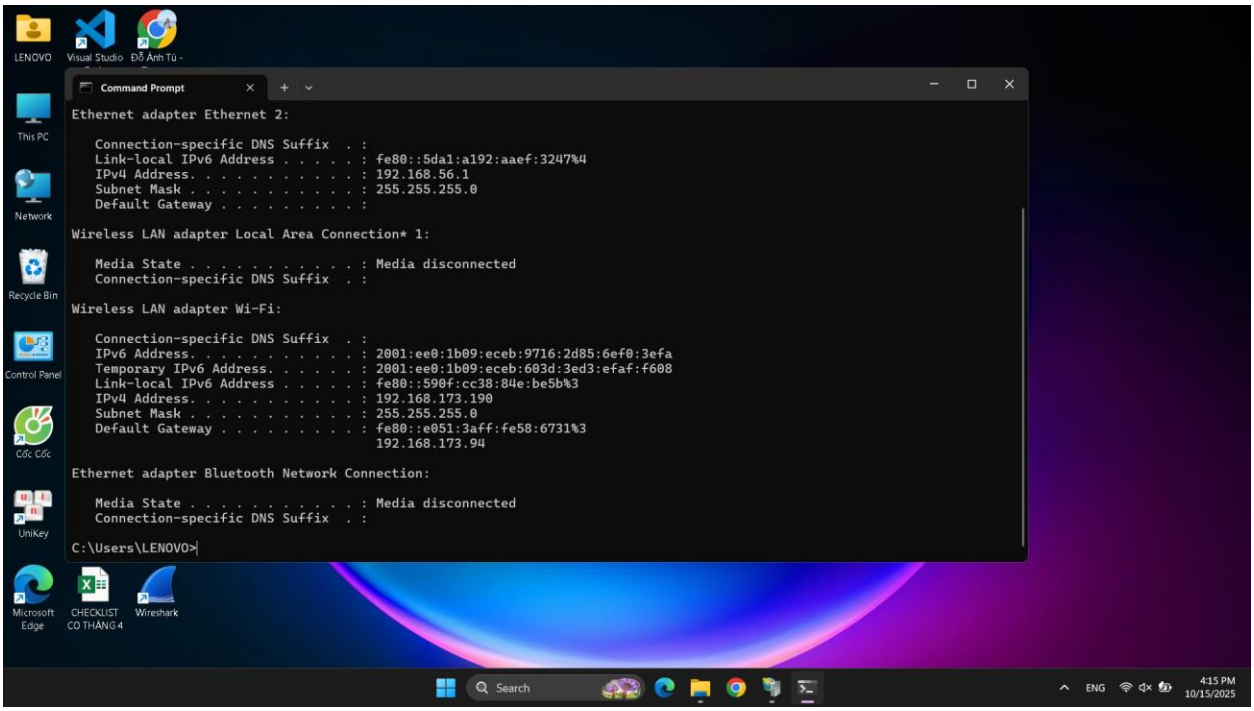


Bước 3: Chọn Internet Information Service

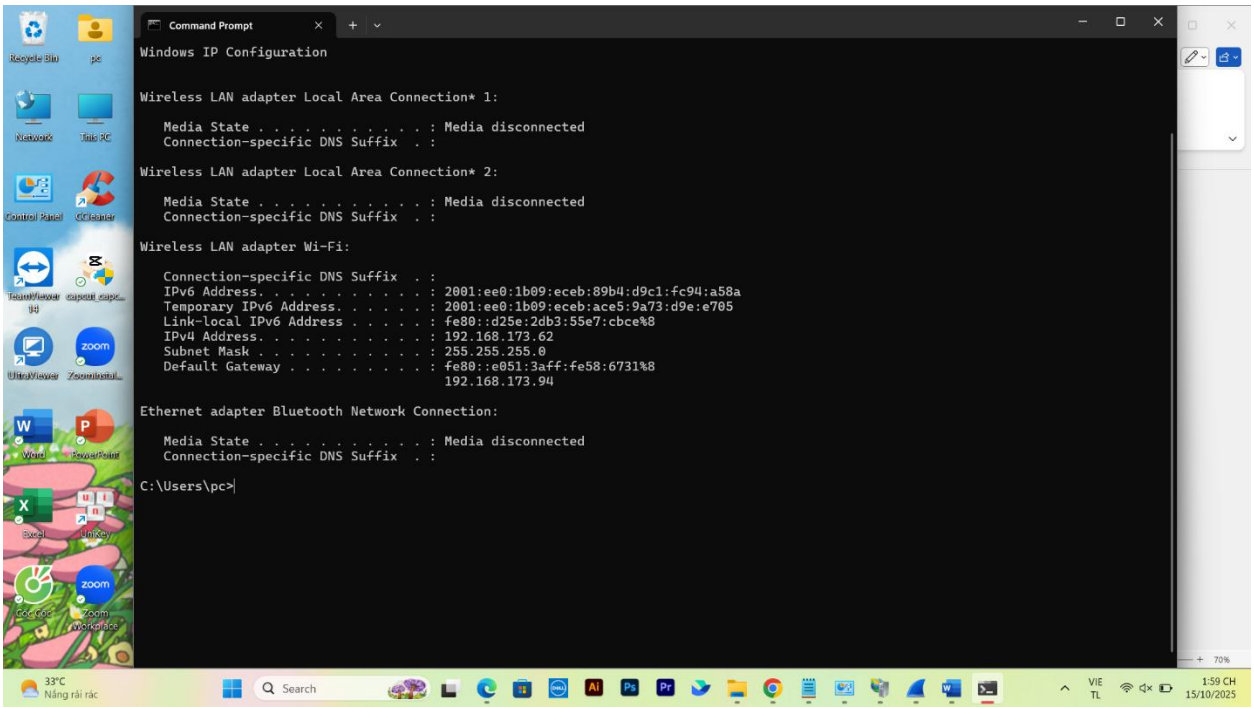


Bước 4: Add Website và truy cập trang web của bản thân





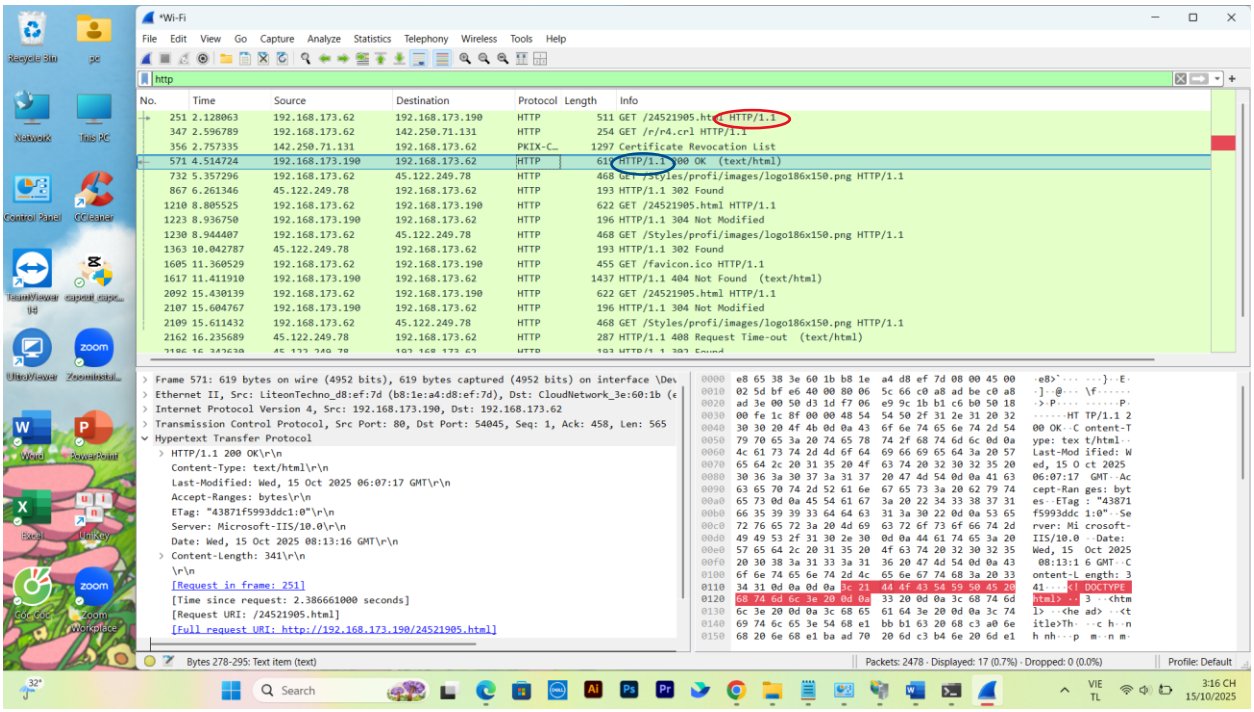
Địa chỉ IP của bạn Đỗ Ánh Tú (MSSV 24521905): 192.168.173.190



Địa chỉ IP máy bản thân: 192.168.173.62

II. Thực hành HTTP GET/respone có điều kiện

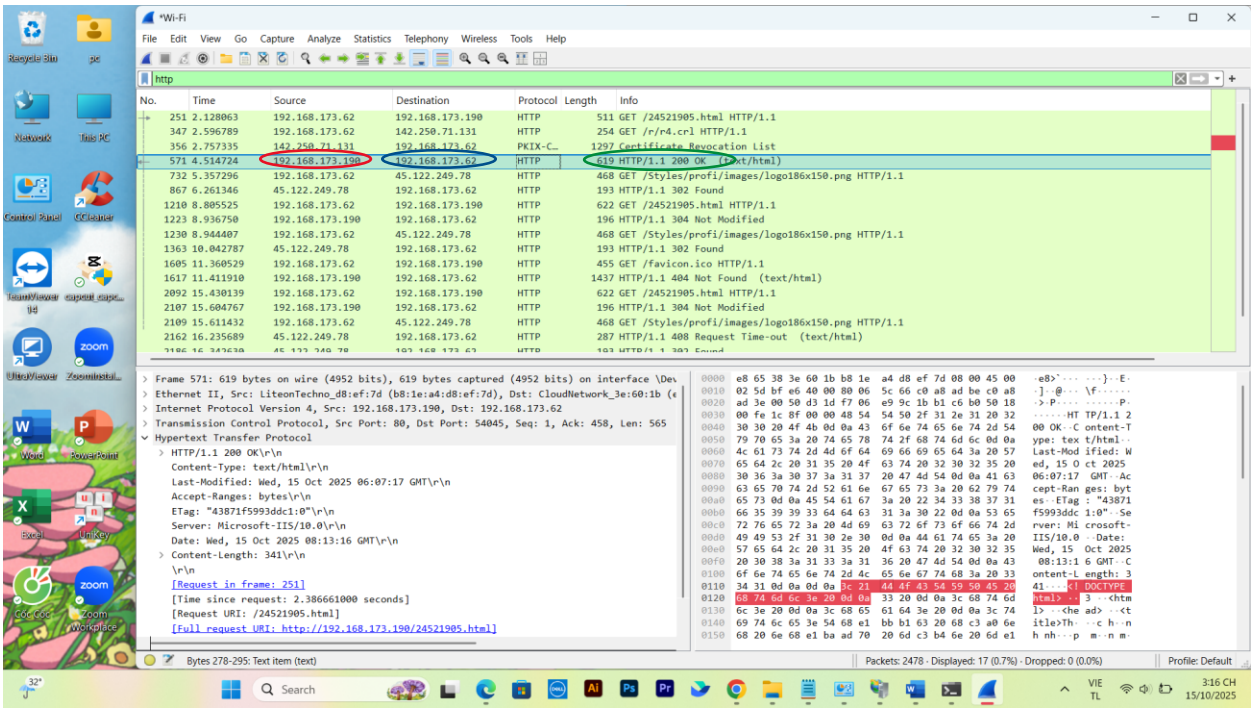
1.



Hình 1

Trình duyệt đang sử dụng phiên bản HTTP 1.1 được khoanh vùng màu đỏ.
Phiên bản HTTP server đang sử dụng là 1.1 được khoanh vùng màu xanh.

2.

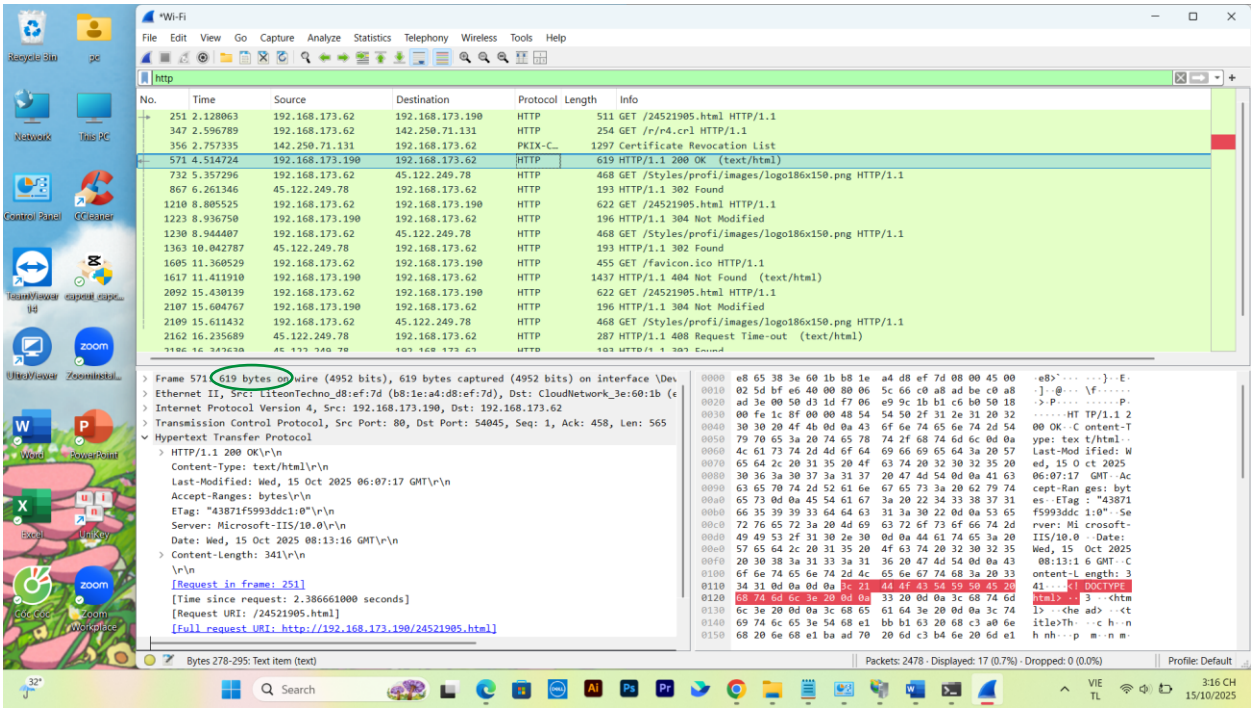


Hình 2

Địa chỉ IP của máy tính đang sử dụng là 192.168.173.62 được khoanh vùng màu đỏ ở *Hình 2*.
Của web server là 192.168.173.190 được khoanh vùng màu xanh ở *Hình 2*.

3. Mã trạng thái (status code) trả về từ server là: 200 OK được khoanh vùng màu xanh lá ở *Hình 2*.

4.

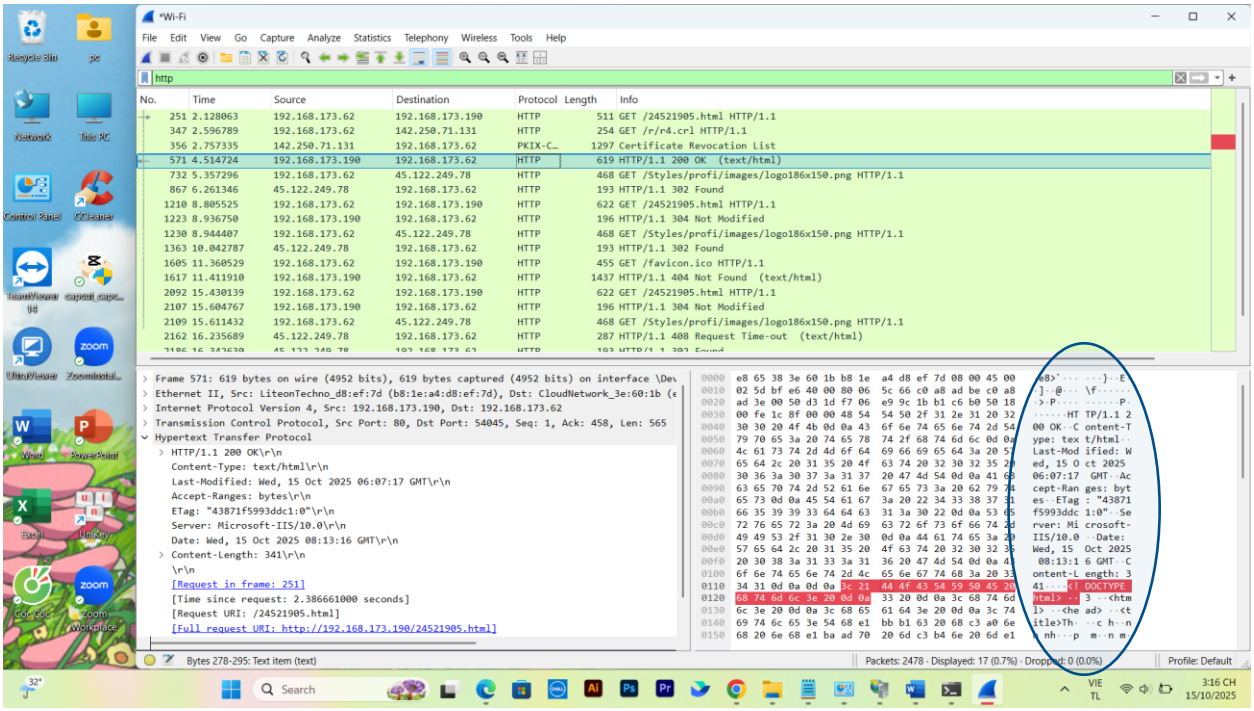


Hình 3

Server đã trả về cho trình duyệt 619 bytes nội dung được khoanh vùng màu xanh lá ở hình 3

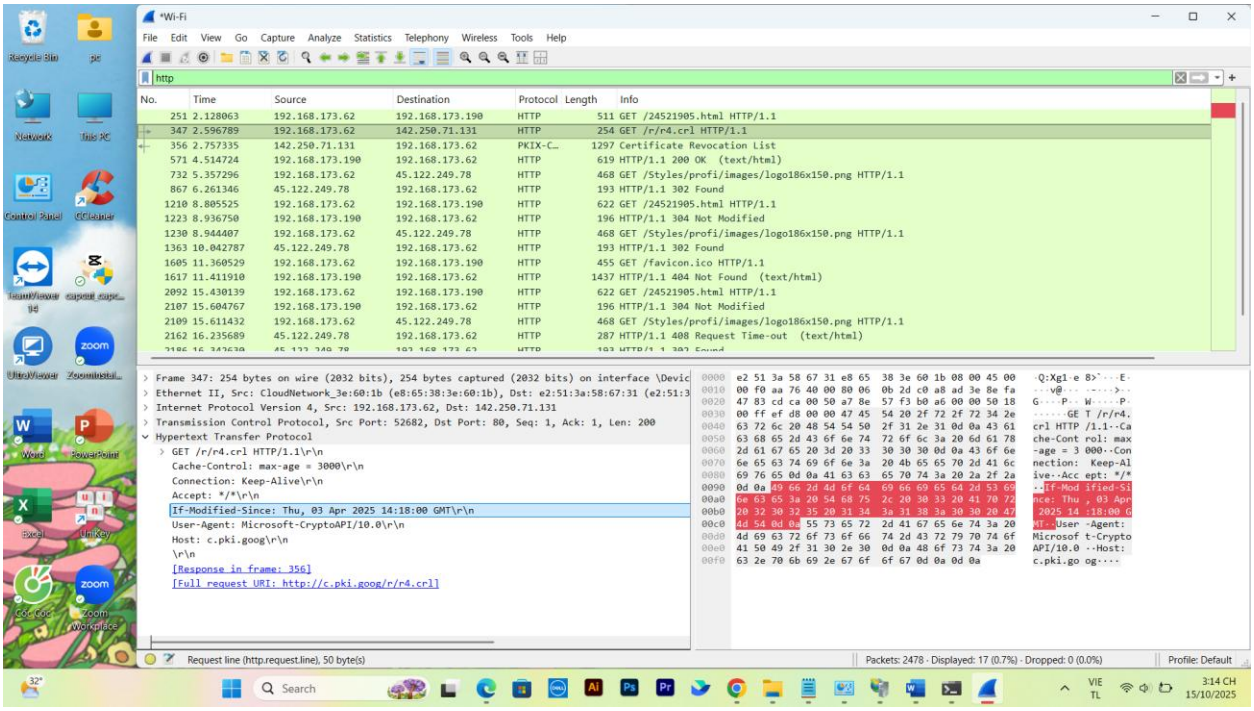
5. Xem xét nội dung của HTTP GET đầu tiên, không thấy dòng "IF-MODIFIED-SINCE"

6. Xem xét nội dung phản hồi từ server, server CÓ trả về nội dung của file HTML được khoanh vùng màu xanh dương
Do phản hồi mang mã trạng thái 200 OK trong cột Hex/ACII ta thấy được nội dung thực tế của một trang HTML bắt đầu bằng <!DOCTYPE html> và sau đó là các thẻ <html>, <head>, <title>, <body>,...



Hình 4

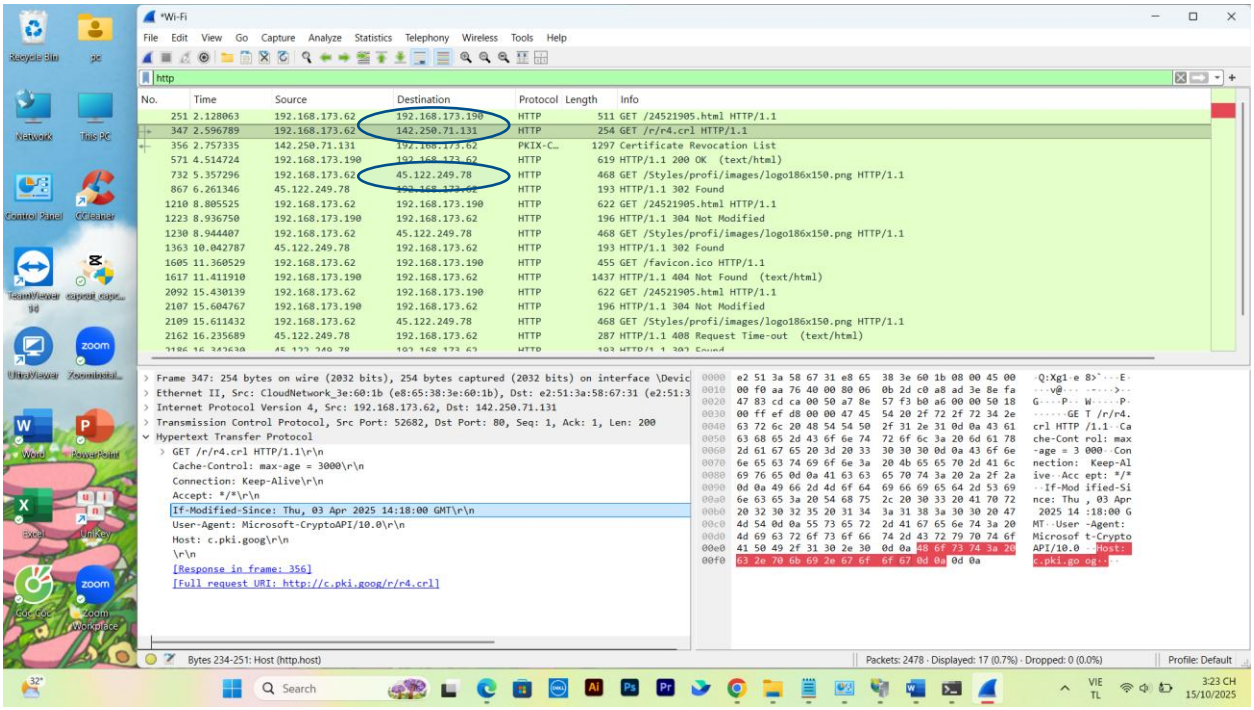
7.



Hình 5

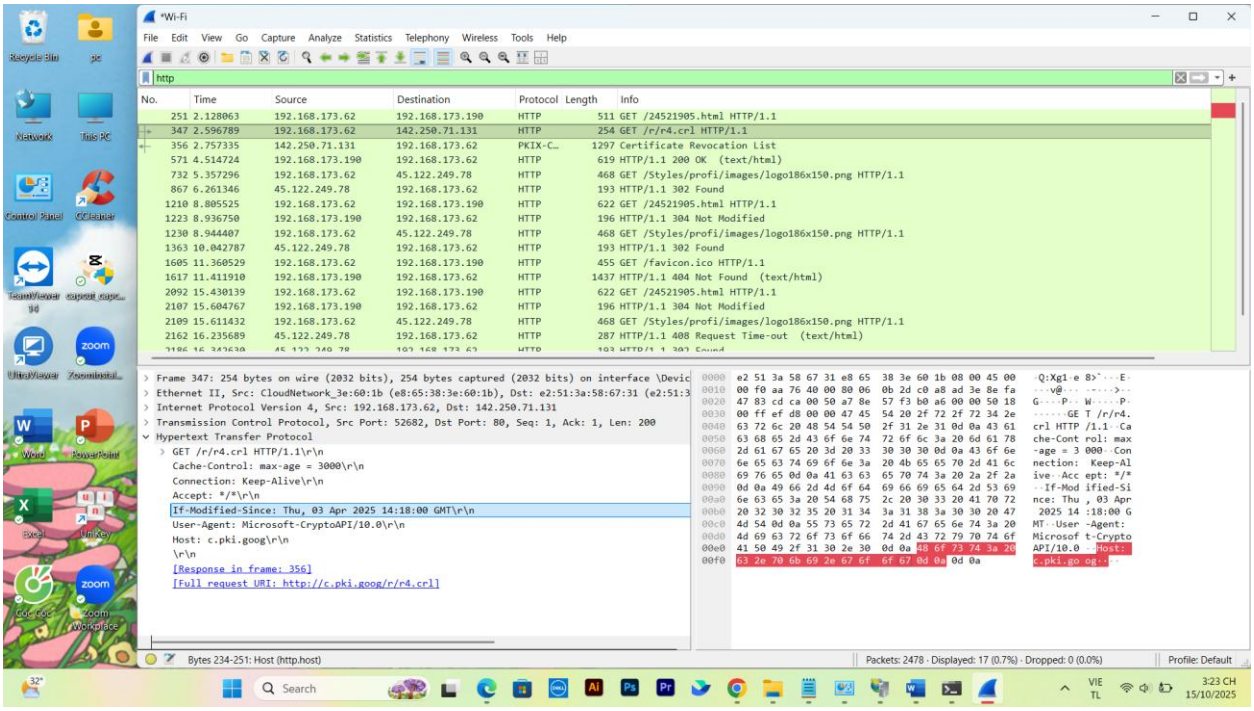
Xem xét nội dung của HTTP GET thứ 2 có dòng “IF-MODIFIED-SINCE”.

8. Mã trạng thái HTTP được trả về từ server tương ứng HTTP GET thứ 2 là:
   304 Not Modified
   Ý nghĩa:
   - Server thông báo rằng file trên server chưa bị thay đổi kể từ thời điểm được chỉ định trong If-Modified-Since. Vì vậy, client không cần tải lại toàn bộ nội dung file - trình duyệt (hoặc ứng dụng) có thể dùng bản đã lưu trong bộ nhớ cache.



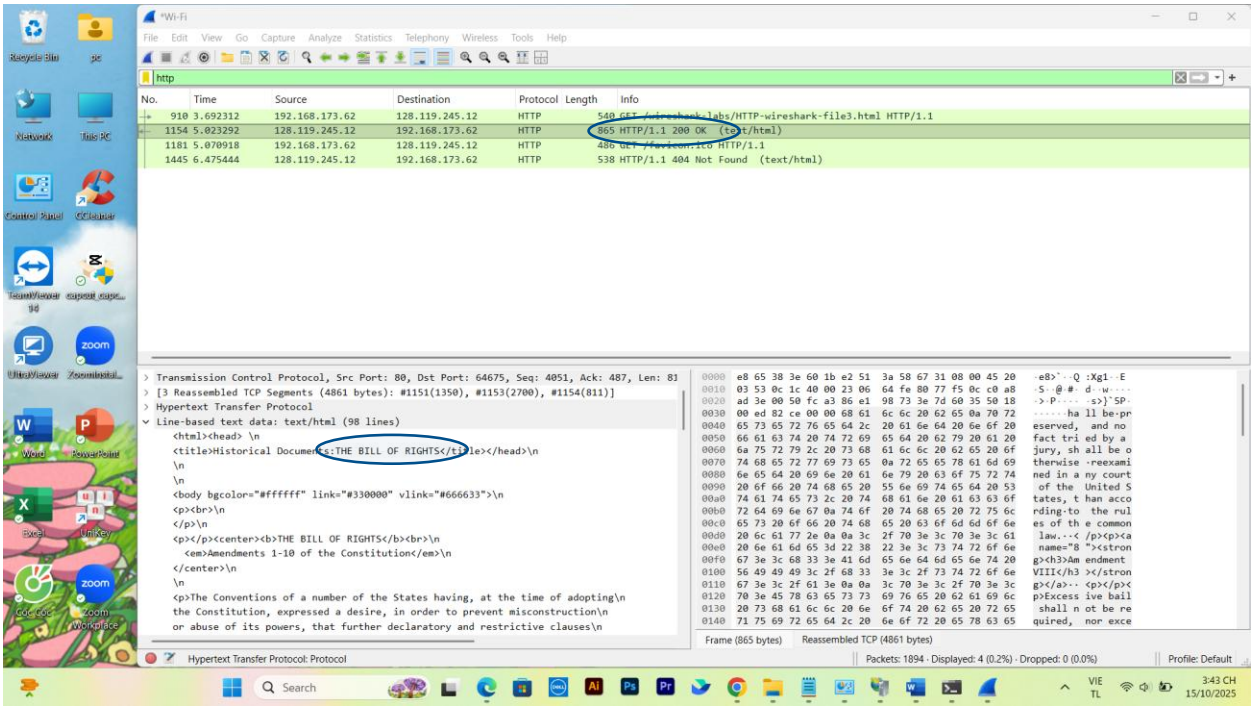
Hình 6

9. Trình duyệt đã gửi 8 HTTP GET đến những địa chỉ IP:
   192.168.173.190
   192.168.71.131
   45.122.249.78



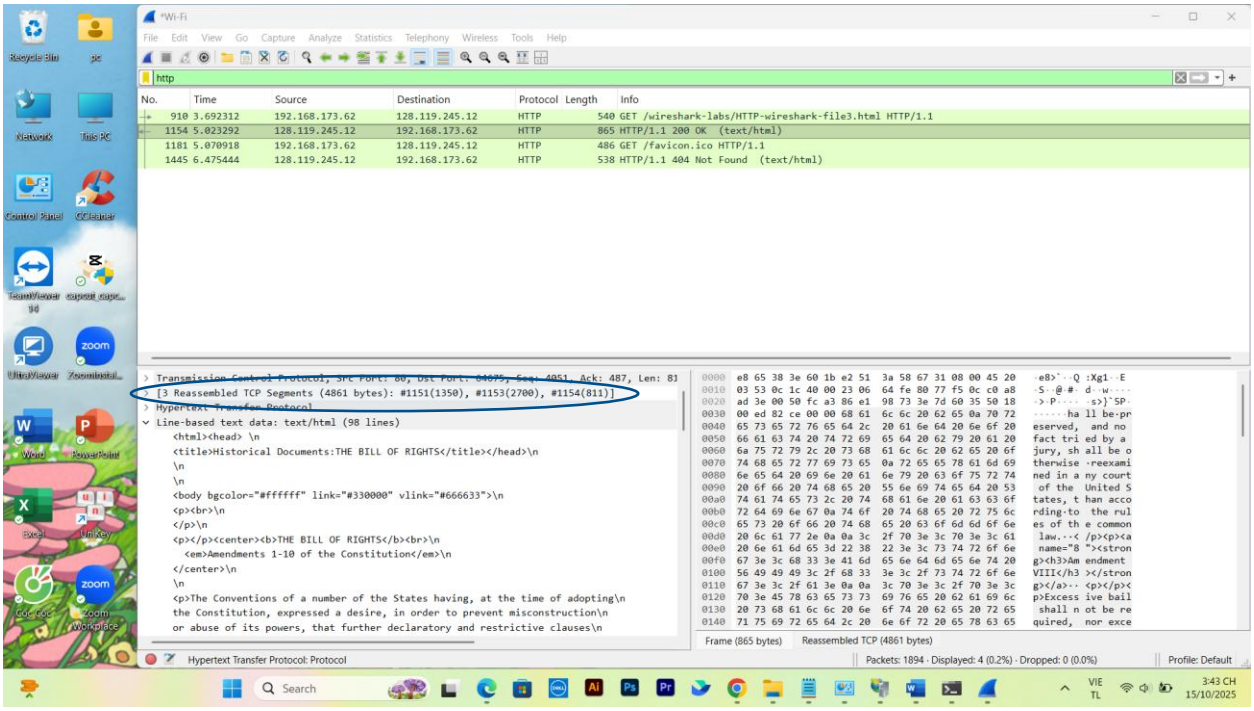
Hình 7

10. Trình duyệt đã gửi 8 HTTP GET. Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ 1



Hình 8

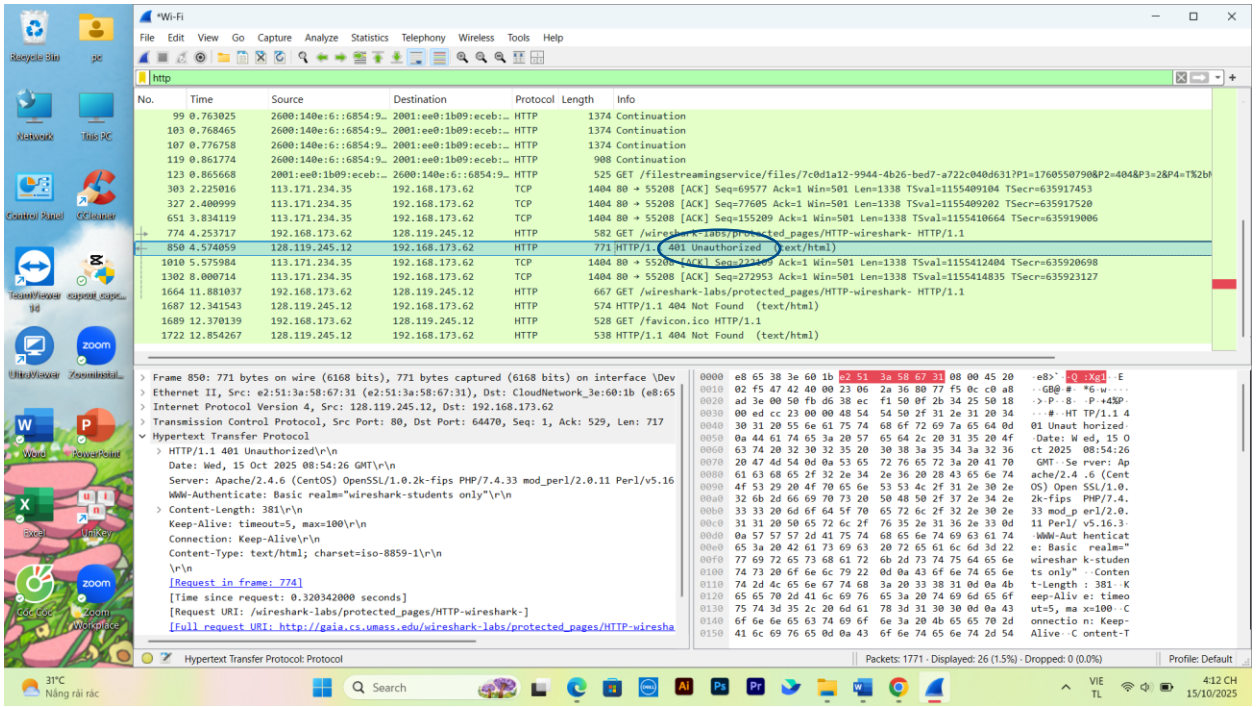
11. Cần 3 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights.



Hình 9

12. Mã trạng thái: 401 Unauthorized

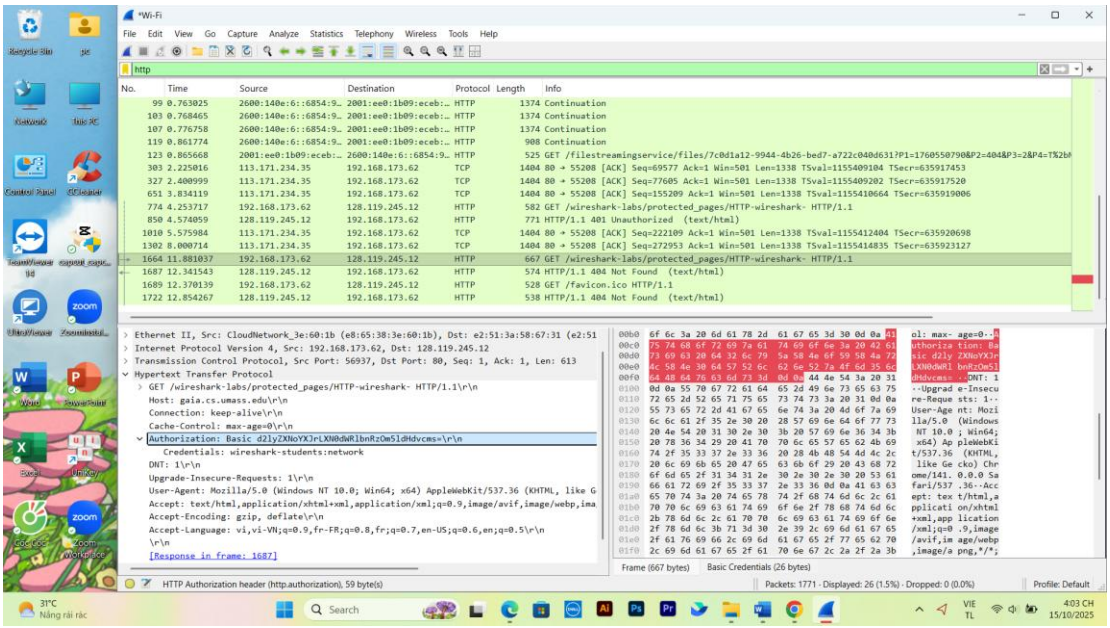
Ý nghĩa: Máy chủ từ chối xử lý yêu cầu vì người dùng chưa xác thực được, cần xác thực lại



Hình 10

13. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu mới xuất hiện: Authorization

    Trong đó phần Credentials gồm: wireshark-student: network là user name và password.



Hình 11