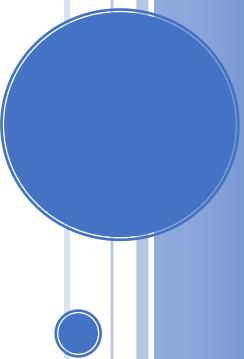




KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

REPORT

WIRESHARK



ĐẠI HỌC KHOA HỌC TỰ NHIÊN
ĐẠI HỌC QUỐC GIA TPHCM
KHOA CÔNG NGHỆ THÔNG TIN

Giảng Viên:

- Đỗ Hoàng Cường
- Huỳnh Thị Bảo Trân

Sinh viên:

- Nguyễn Đức Huy - 19127422

Tiến độ:

- Hoàn thành tất cả các bài tập

NỘI DUNG

1	ICMP	1
2	HTTP	5
3	FTP	12
4	Reference:	16

WIRESHARK

1 ICMP

- Mục đích của việc ping?

ping, viết tắt của Packet Internet Grouper (Groper), là một công cụ cho mạng máy tính sử dụng trên các mạng TCP/IP (chẳng hạn như Internet) để kiểm tra xem có thể kết nối tới một máy chủ cụ thể nào đó hay không, và ước lượng khoảng thời gian trễ trọn vòng để gửi gói dữ liệu cũng như tỉ lệ các gói dữ liệu có thể bị mất giữa hai máy. Công cụ này thực hiện nhiệm vụ trên bằng cách gửi một số gói tin ICMP đến máy kia và chờ phản hồi.

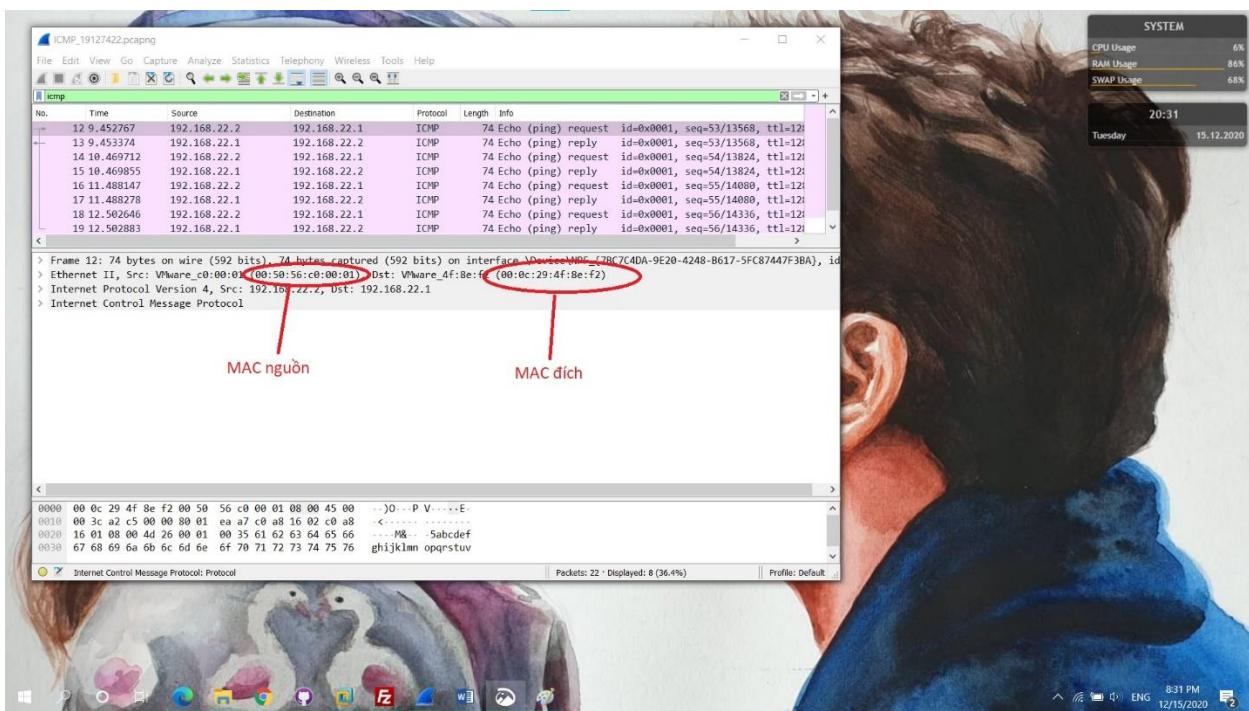
- Có bao nhiêu các gói tin trong quá trình ping

Có tổng cộng 8 gói tin trong quá trình ping, bên nguồn gửi 4 gói tin ICMP echo request, bên nhận trả về lại 4 gói tin ICMP echo reply

- Địa chỉ MAC nguồn? MAC đích?

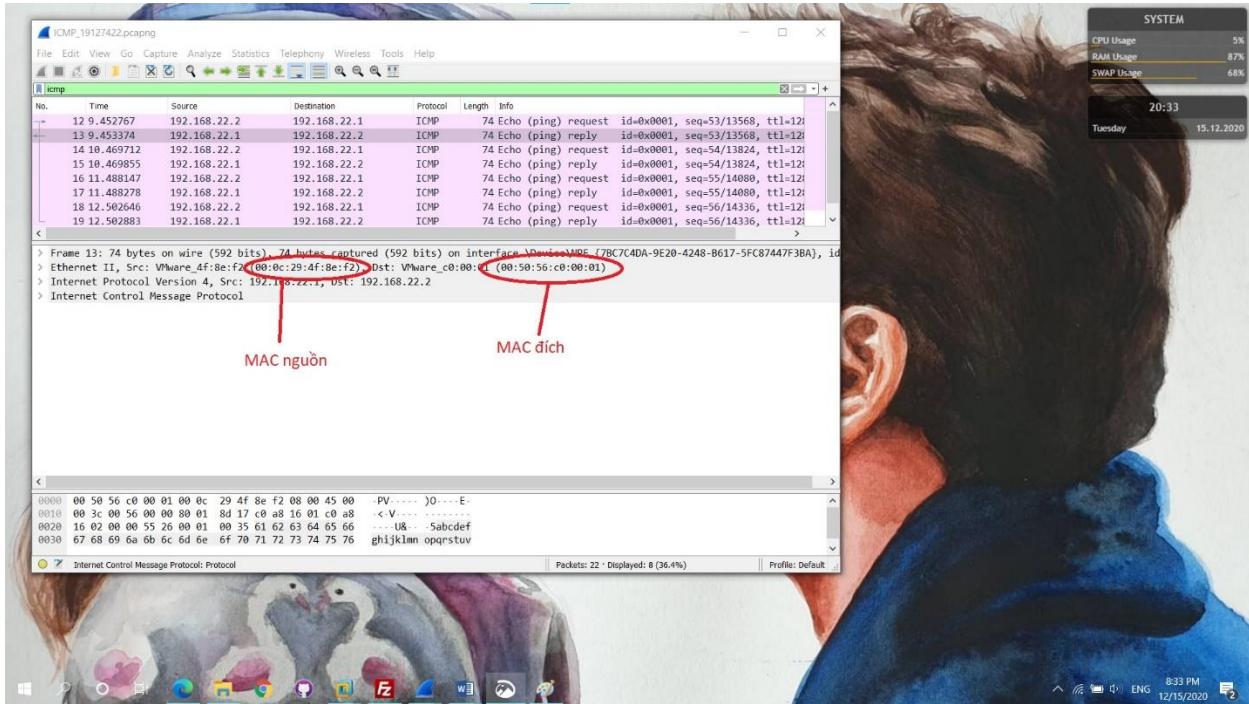
Gói tin request:

- Địa chỉ MAC nguồn là: 00:50:56:c0:00:01
- Địa chỉ MAC đích: 00:0c:29:4f:8e:f2



Gói tin reply:

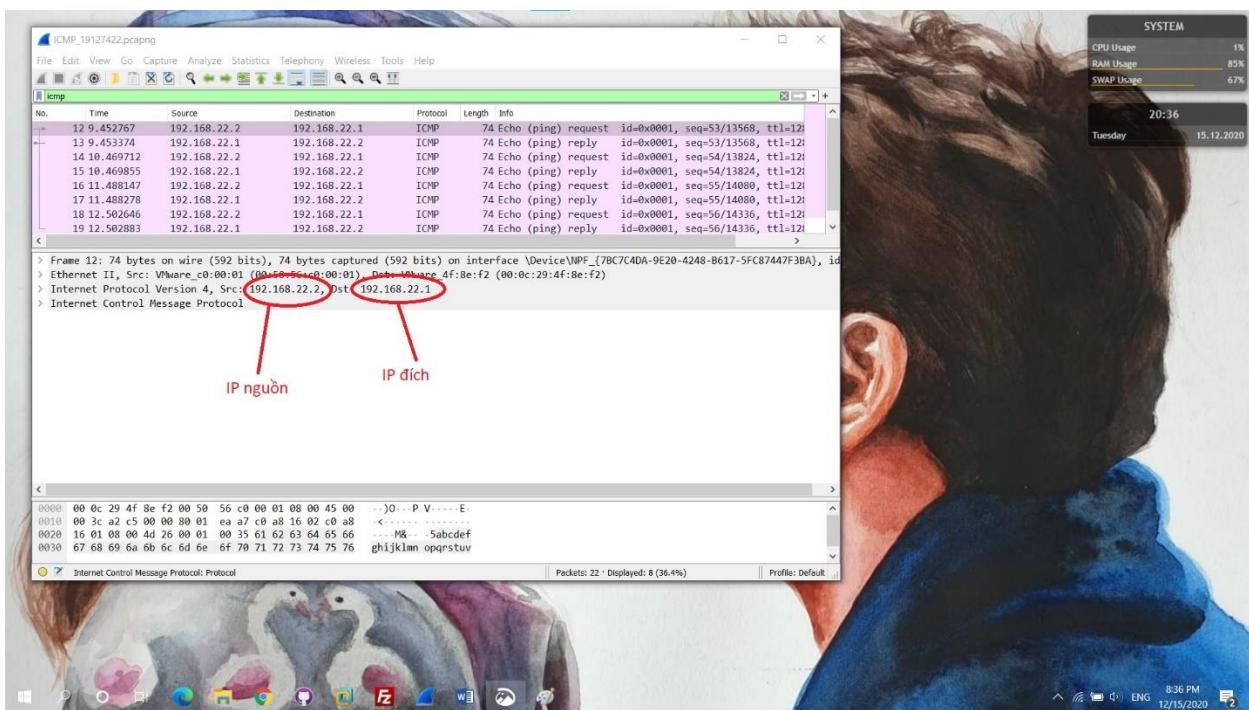
- Địa chỉ MAC nguồn là: : 00:0c:29:4f:8e:f2
- Địa chỉ MAC đích: 00:50:56:c0:00:01



● Địa chỉ IP nguồn? IP đích?

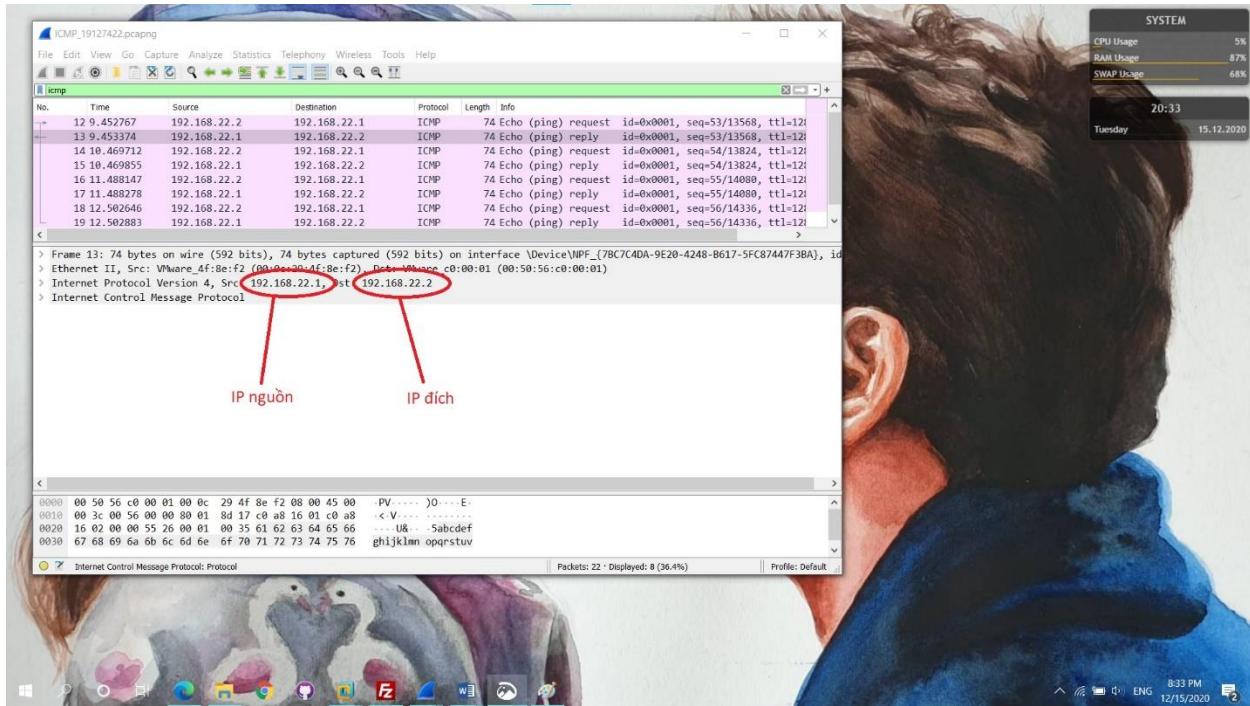
Gói tin request:

- Địa chỉ IP nguồn: 192.168.22.2 || Địa chỉ IP đích: 192.168.22.1



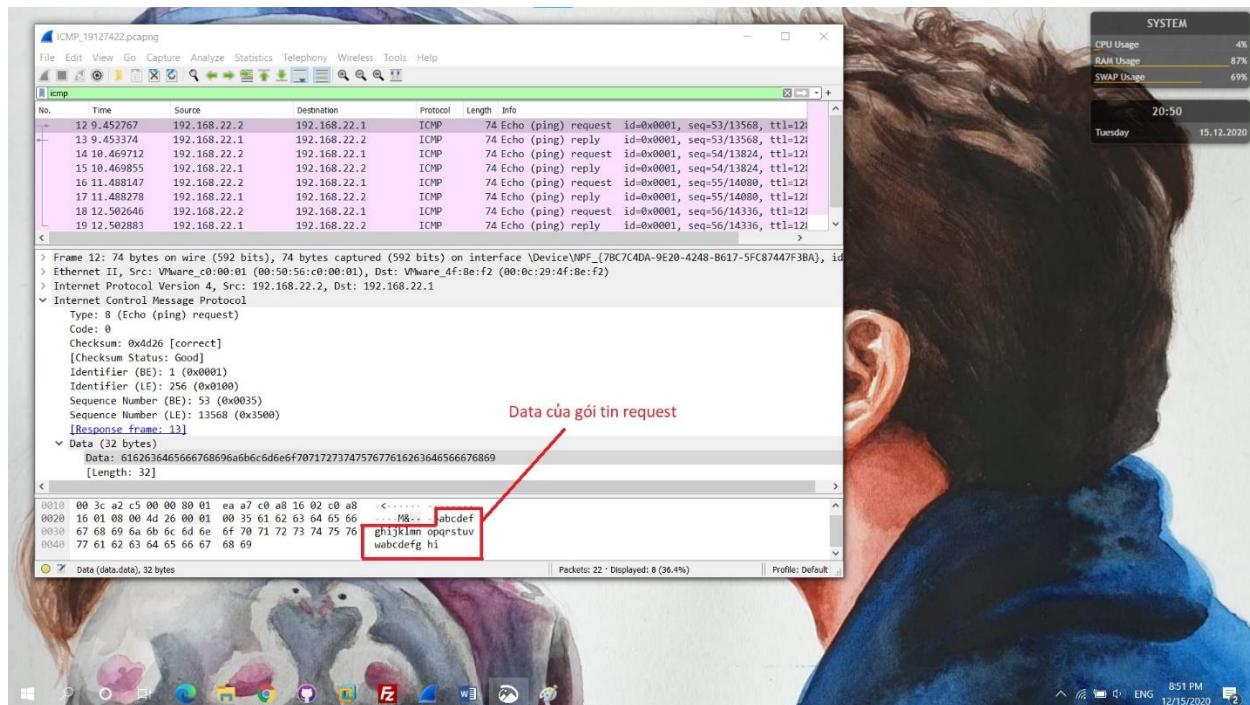
Gói tin reply

- Địa chỉ IP nguồn: 192.168.22.1
- Địa chỉ IP đích: 192.168.22.2

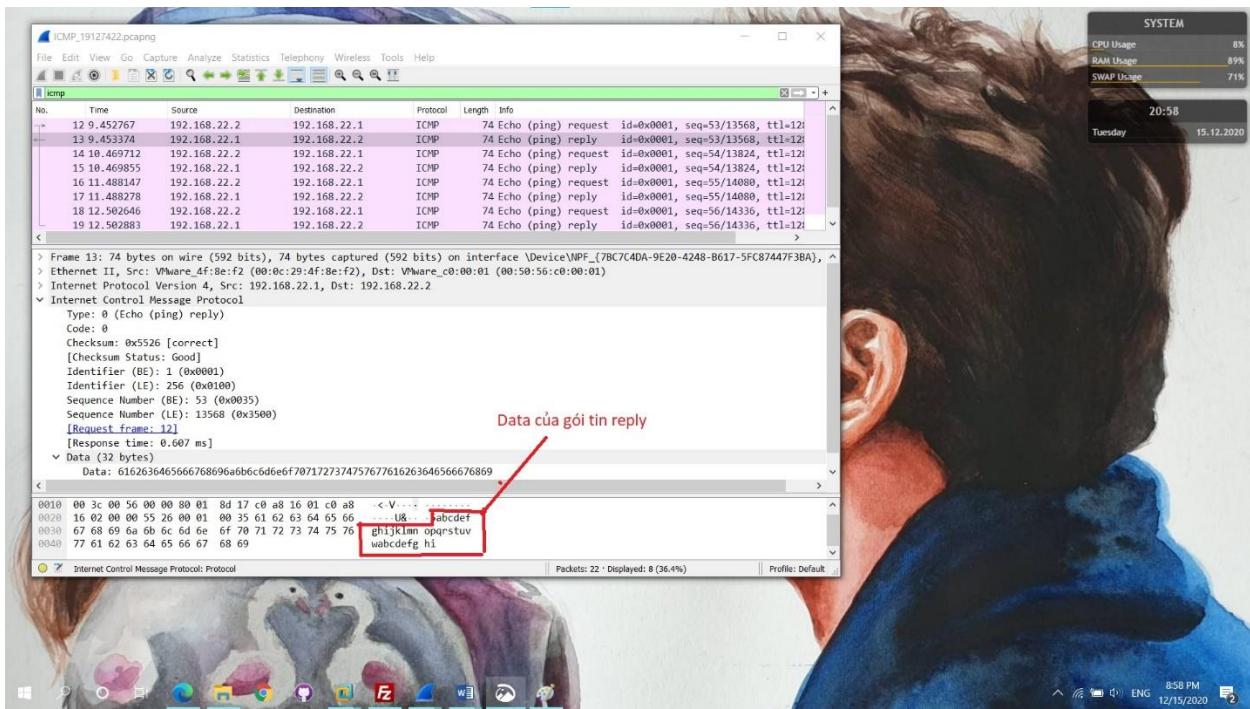


- Nội dung phần Data của gói tin ICMP?

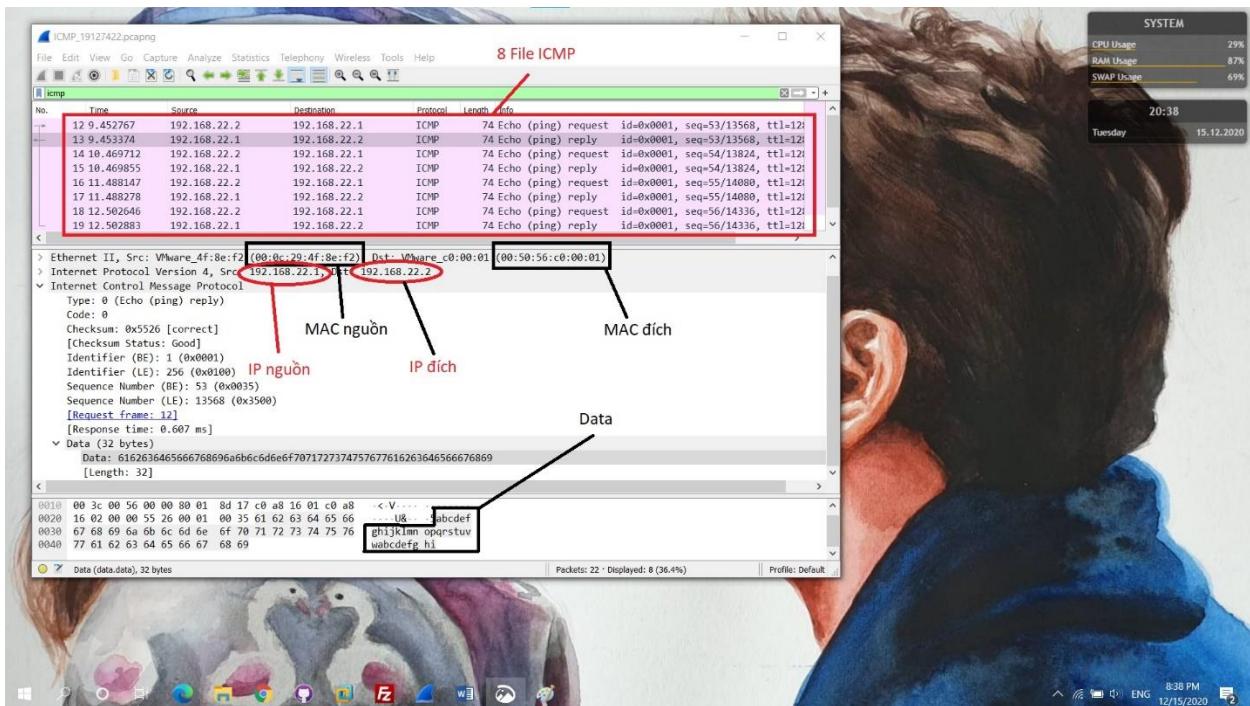
Nội dung phần data của gói tin request: abcdefghijklmnopqrstuvwxyz (32 byte)



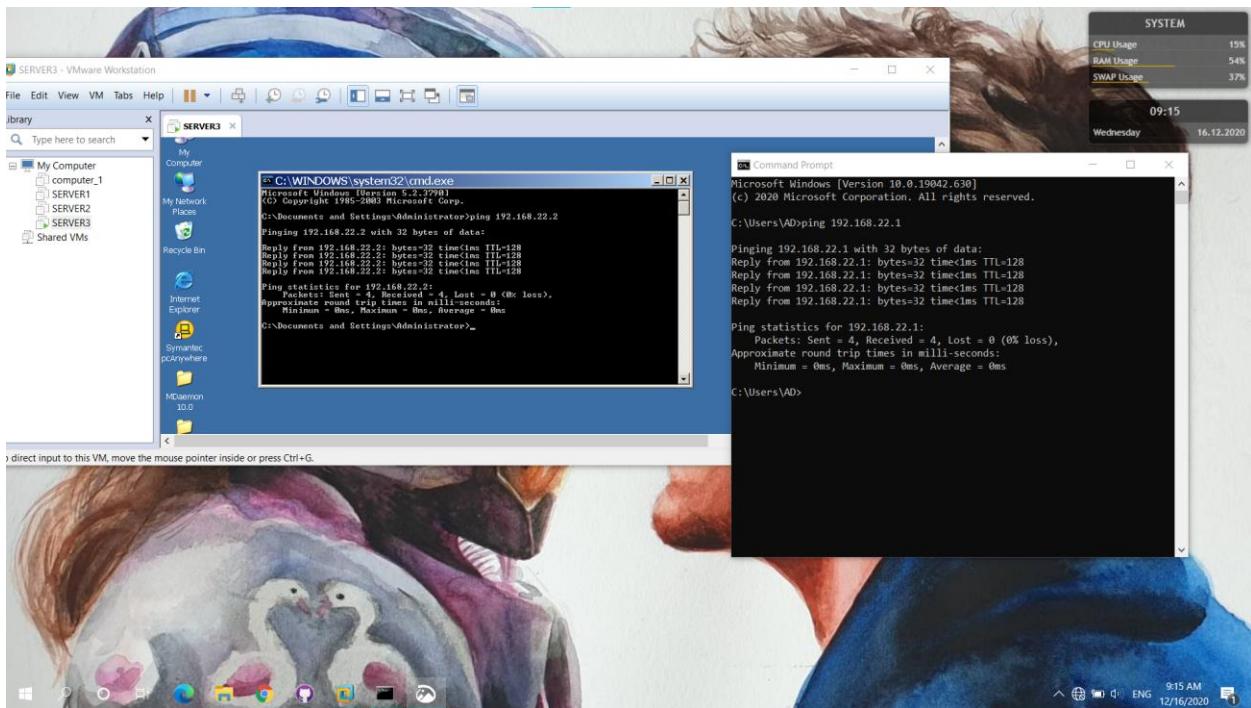
Nội dung phần Data của gói tin Reply: abcdefghijklmnopqrstuvwxyzwabcdeghi (32 byte)



Gói tin reply:



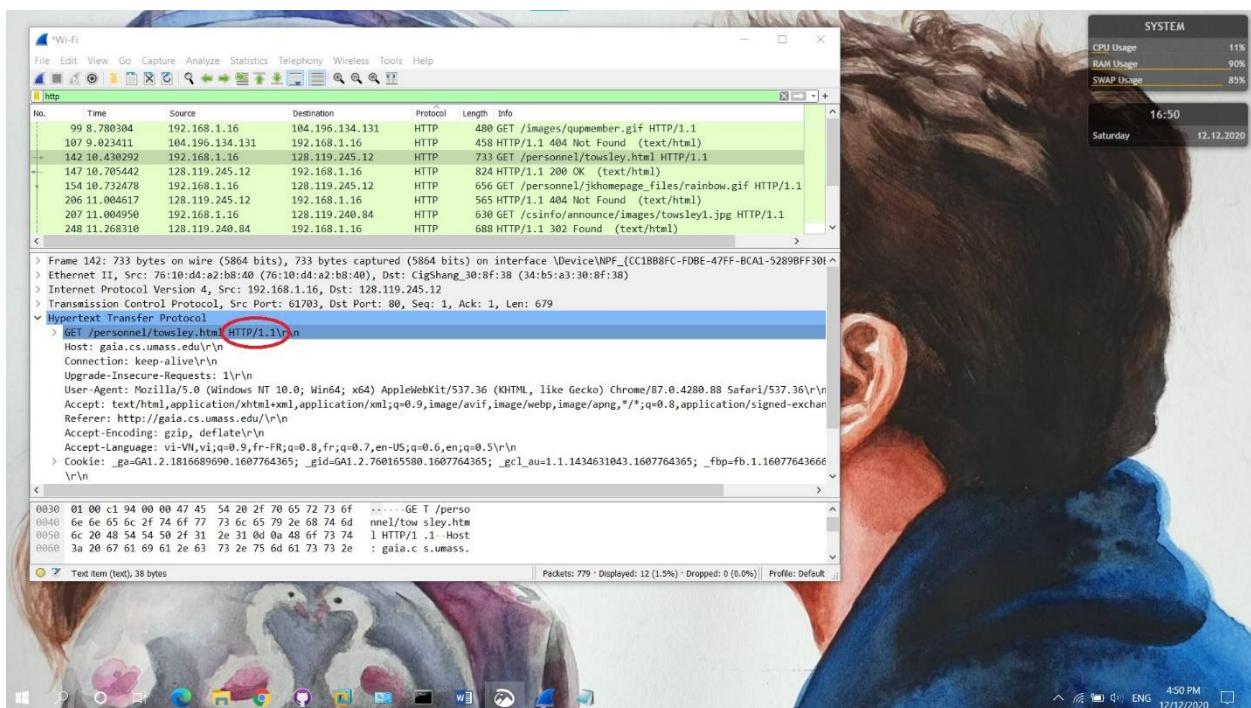
Ping giữa máy thật và máy ảo:



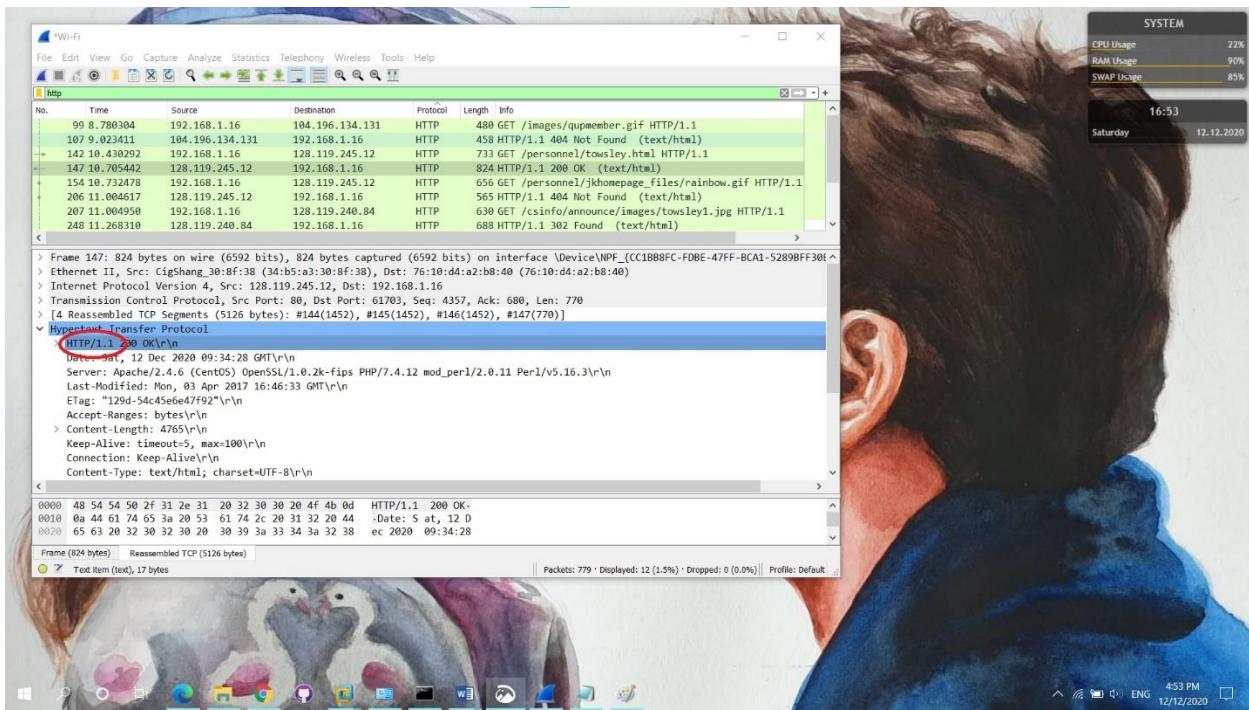
2 HTTP

- Trình duyệt của bạn chạy HTTP phiên bản 1.0 hay 1.1? Phiên bản của HTTP được server chạy là bao nhiêu?

Trình duyệt đang chạy HTTP phiên bản 1.1

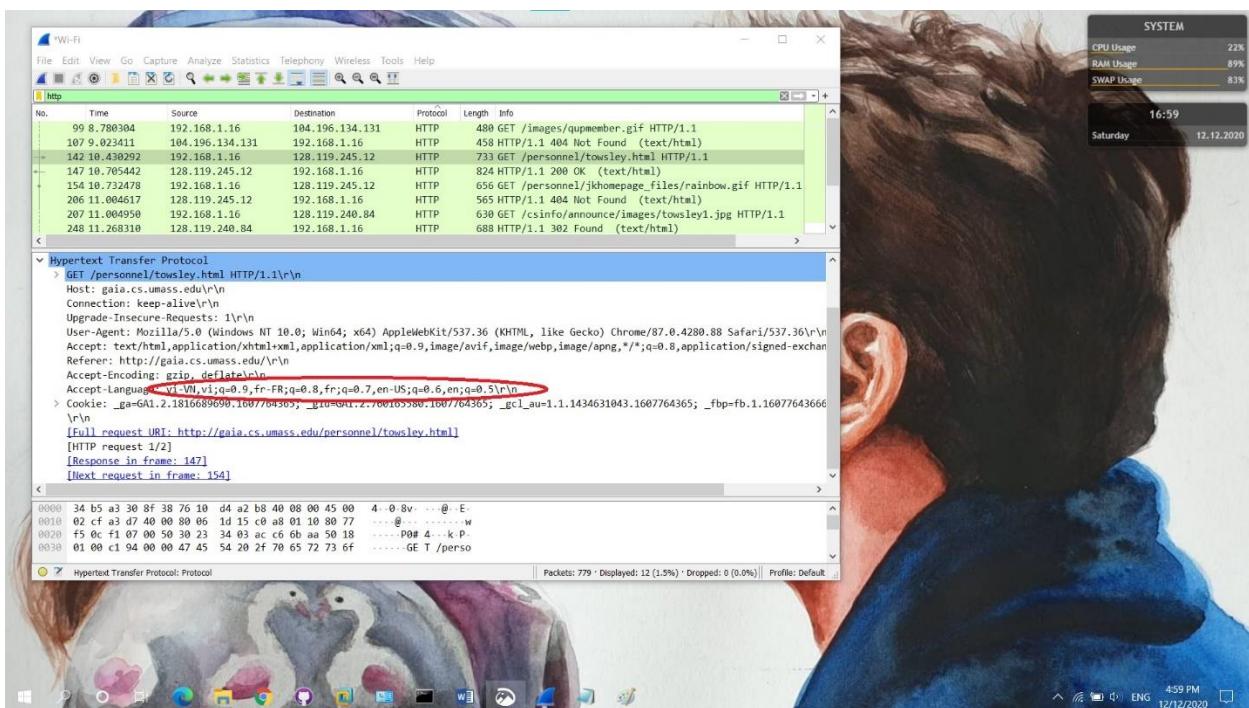


Phiên bản của HTTP được server chạy là: 1.1



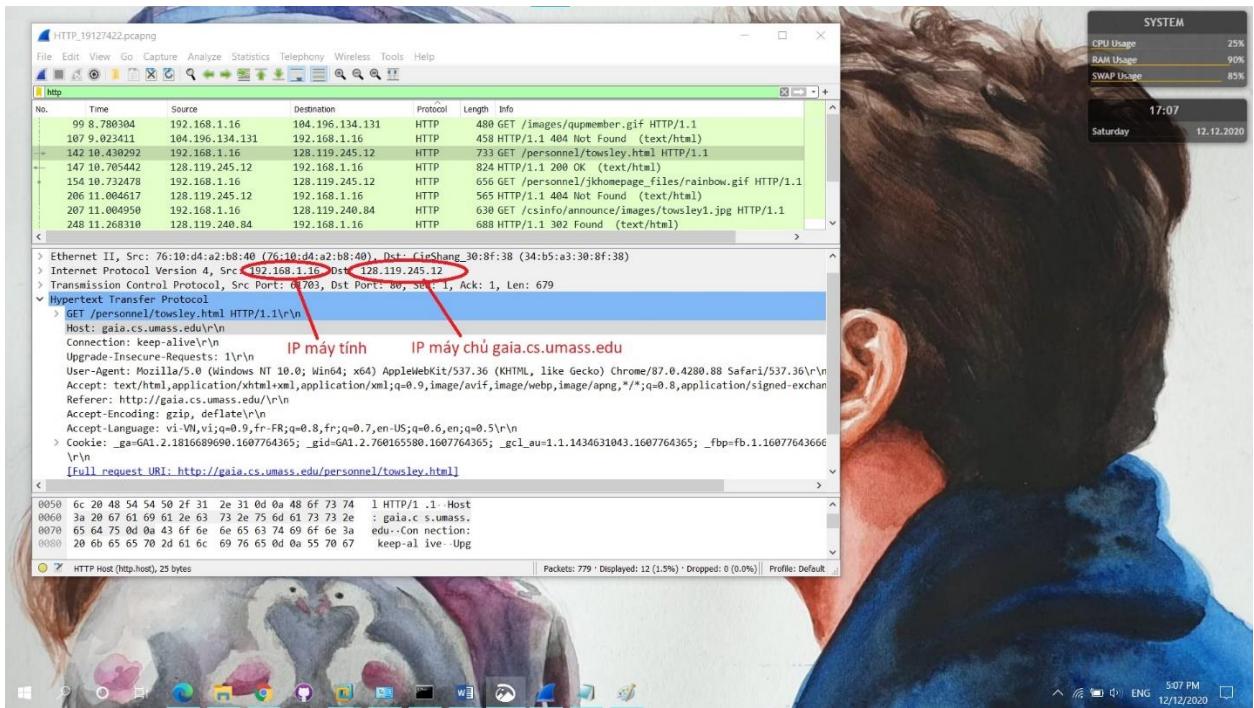
- Ngôn ngữ mà trình duyệt web của bạn chỉ ra nó có thể chấp nhận server?

Ngôn ngữ mà trình duyệt web chỉ ra nó có thể chấp nhận server: vi-VN, vi, fr-FR, fr, en-US, en



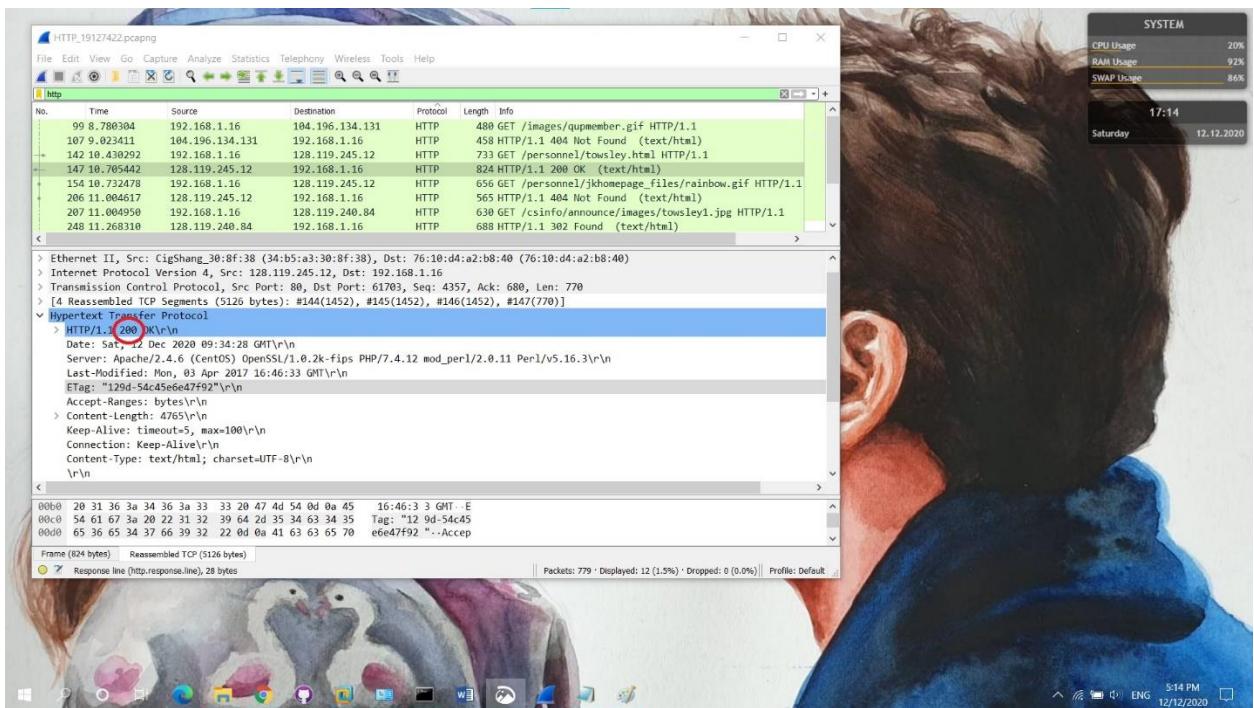
- Địa chỉ IP của máy bạn và gaia.cs.umass.edu server?

Địa chỉ IP máy tính: **192.168.1.16** || Địa chỉ IP máy chủ gaia.cs.umass.edu: **128.119.245.12**



- Mã trả về từ server cho trình duyệt của bạn và ý nghĩa của nó?

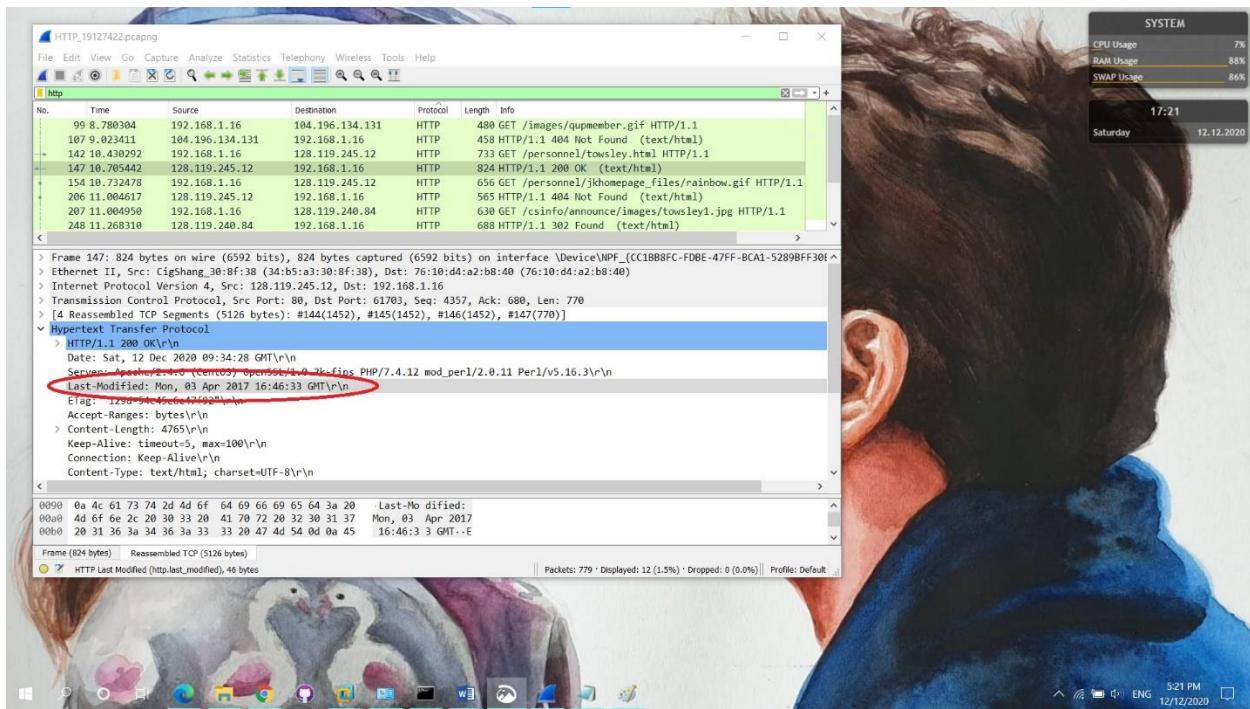
Mã trả về từ server cho trình duyệt là: **200**



Ý nghĩa của mã **200 OK**: Request đã được tiếp nhận và xử lý thành công. Các Response thực tế trả về sẽ phụ thuộc vào phương thức HTTP của Request. Trong một GET Request, Response sẽ chứa một thực thể tương ứng với các tài nguyên yêu cầu, trong một POST Request, Response sẽ chứa một thực thể mô tả hoặc chứa các kết quả của các action.

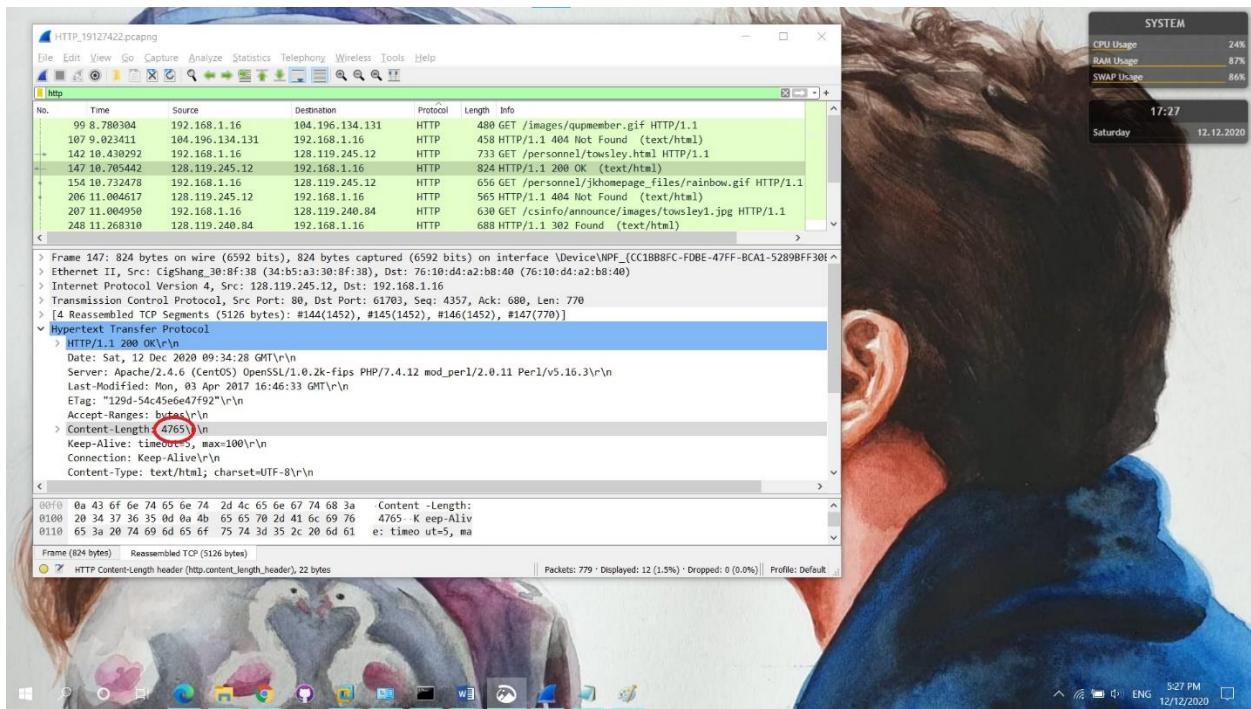
- Thời điểm file HTML mà bạn đang nhận được chỉnh sửa lần cuối ở server?

Thời điểm file HTML nhận được chỉnh sửa lần cuối ở server là: **Mon, 03 Apr 2017 16:46:33 GMT**



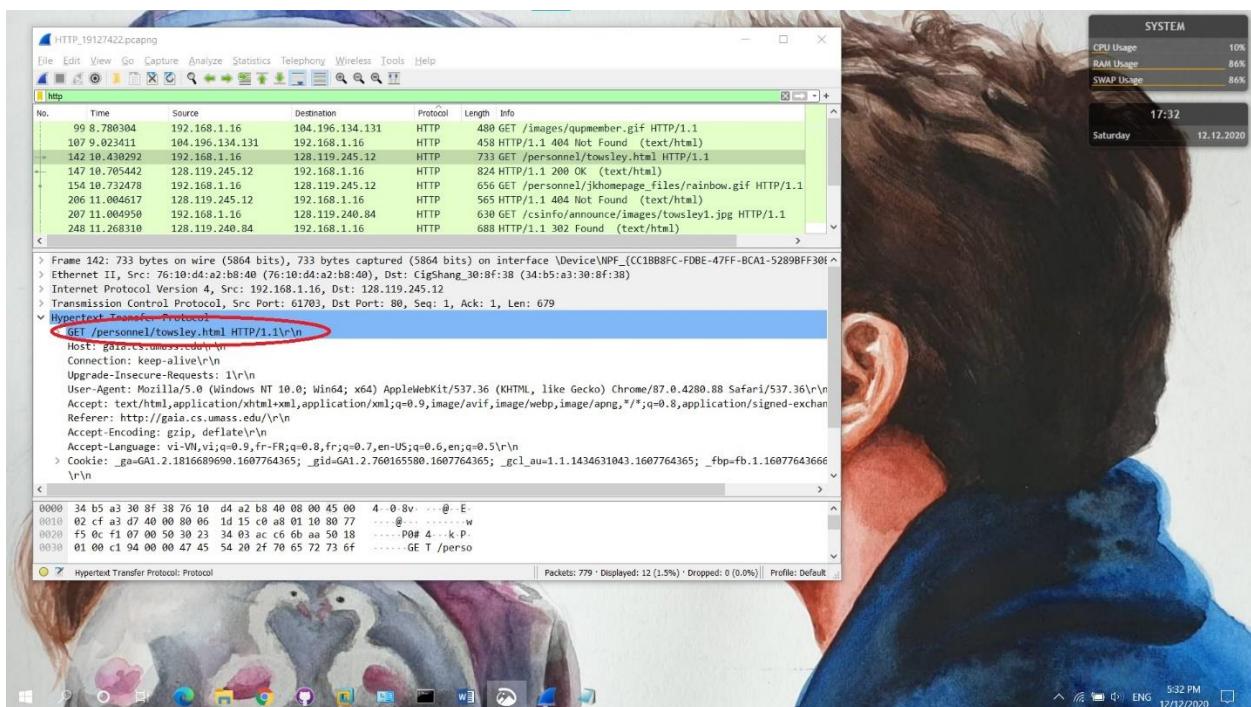
- Có bao nhiêu byte trong nội dung được trả về cho trình duyệt của bạn?

Có **4765 byte** trong nội dung được trả về cho trình duyệt

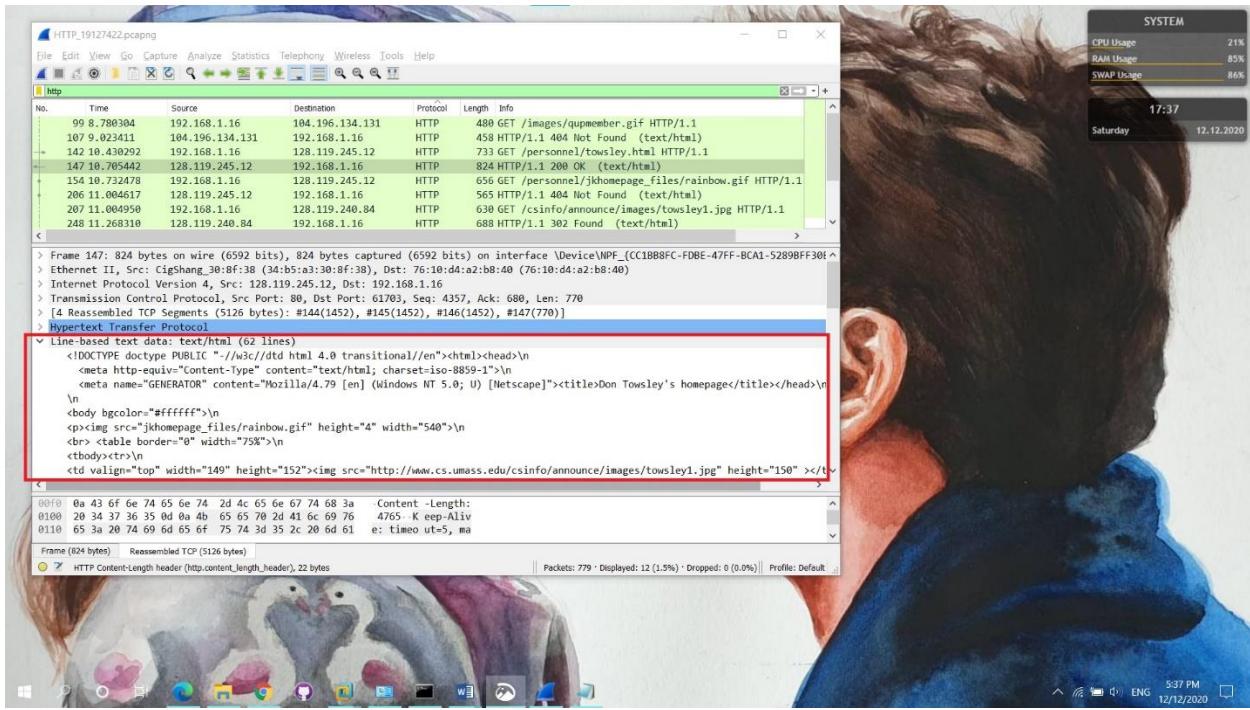


- Kiểm tra nội dung của yêu cầu HTTP GET đầu tiên từ trình duyệt của bạn tới server. Bạn có thấy 1 dòng “IF-MODIFIED-SINCE” trong HTTP GET?

Không thấy 1 dòng “IF-MODIFIED-SINCE” trong HTTP GET

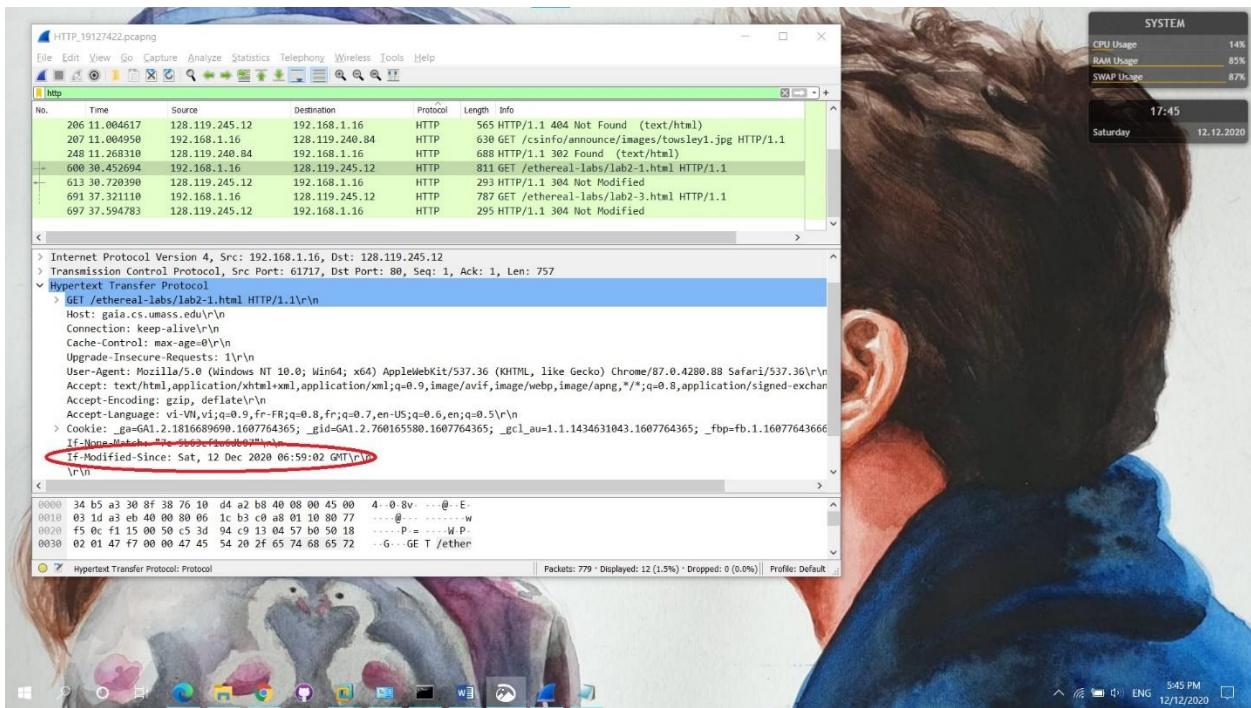


- Kiểm tra các nội dung phản hồi của server. Server có trả về nội dung của file một cách rõ ràng không? **Trả lời:** Máy chủ đã phản hồi. Có thể thấy rõ nội dung của file mà server trả về trong mục Line-base text data

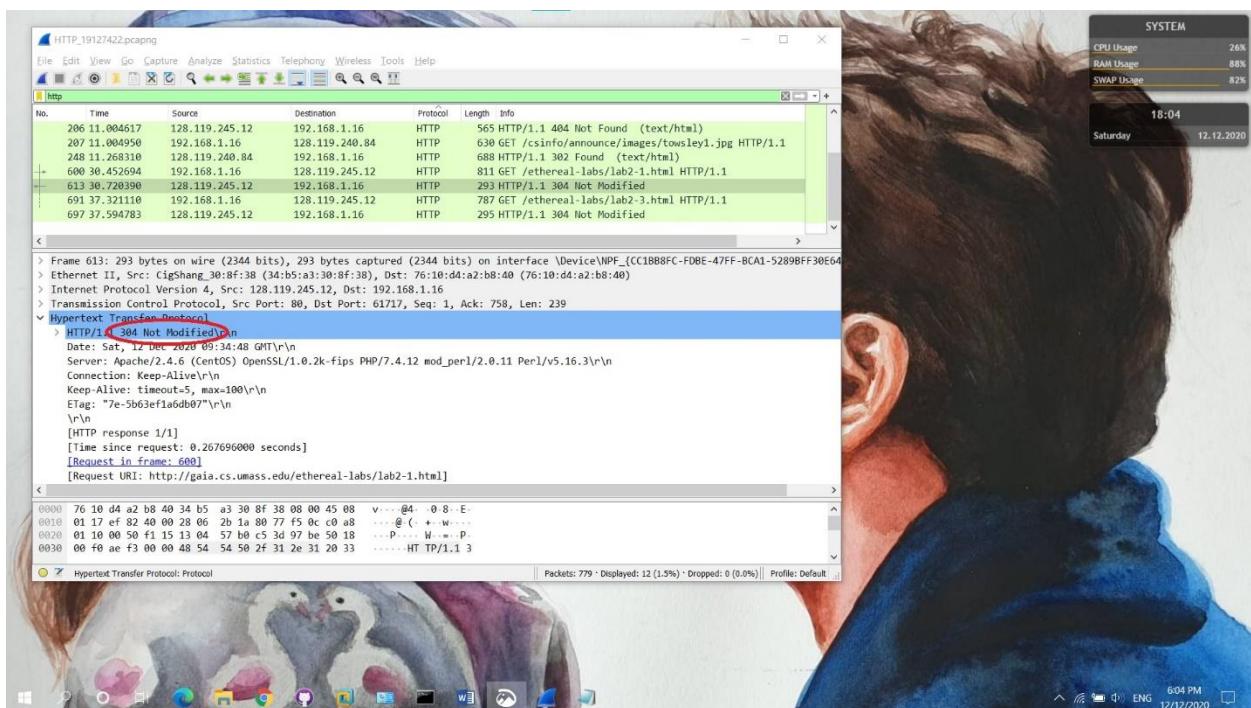


- Tiếp theo kiểm tra các nội dung của yêu cầu HTTP GET thứ hai từ trình duyệt của bạn tới server. Bạn có thấy dòng “IF-MODIFIED-SINCE” trong HTTP GET? Nếu có thì đó là thông tin gì sau “IF-MODIFIED-SINCE:” header? Cho biết ý nghĩa của nó?
Có thấy dòng “IF-MODIFIED-SINCE” trong HTTP GET. Thông tin sau tiêu đề:
Sat, 12 Dec 2020 06:50:02 GMT

Ý nghĩa: **nơi URL chưa được sửa đổi kể từ ngày xác định**, nếu như nội dung trang web được trình duyệt lưu lại trong bộ nhớ cache. Và lần sau nếu truy cập nữa thì trình duyệt sẽ gửi. Nếu như không có bất kì thay đổi nào thì server sẽ gửi một status code 304. Sau đó trình duyệt sẽ load nội dung được lưu trong bộ nhớ cache đã lưu trước đó.



- Cho biết mã trả về từ server cho HTTP GET thứ hai? Server có trả về rõ ràng nội dung của các file? Giải thích tại sao lại như vậy?
 Mã trả về từ server cho HTTP GET thứ hai là: **HTTP/1.1 304 Not Modified**. Máy chủ đã không trả về nội dung của tệp kể từ khi trình duyệt tải nó từ bộ nhớ cache của nó (do



em đã làm nháp 1 lần trước khi bắt gói tin nên lần bắt sau nó không trả về mã 200 ở lần 1)

3 FTP

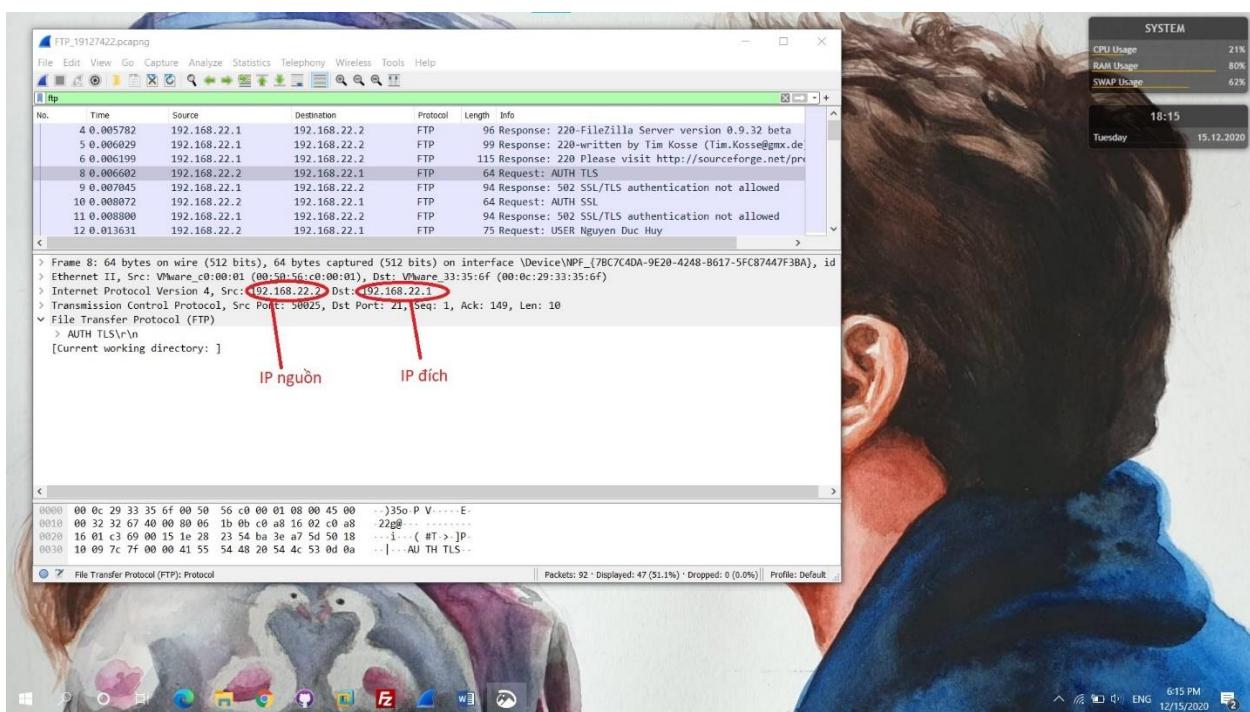
- Có bao nhiêu loại gói tin FTP? Giải thích ý nghĩa từng gói?

Có 2 loại gói tin FTP:

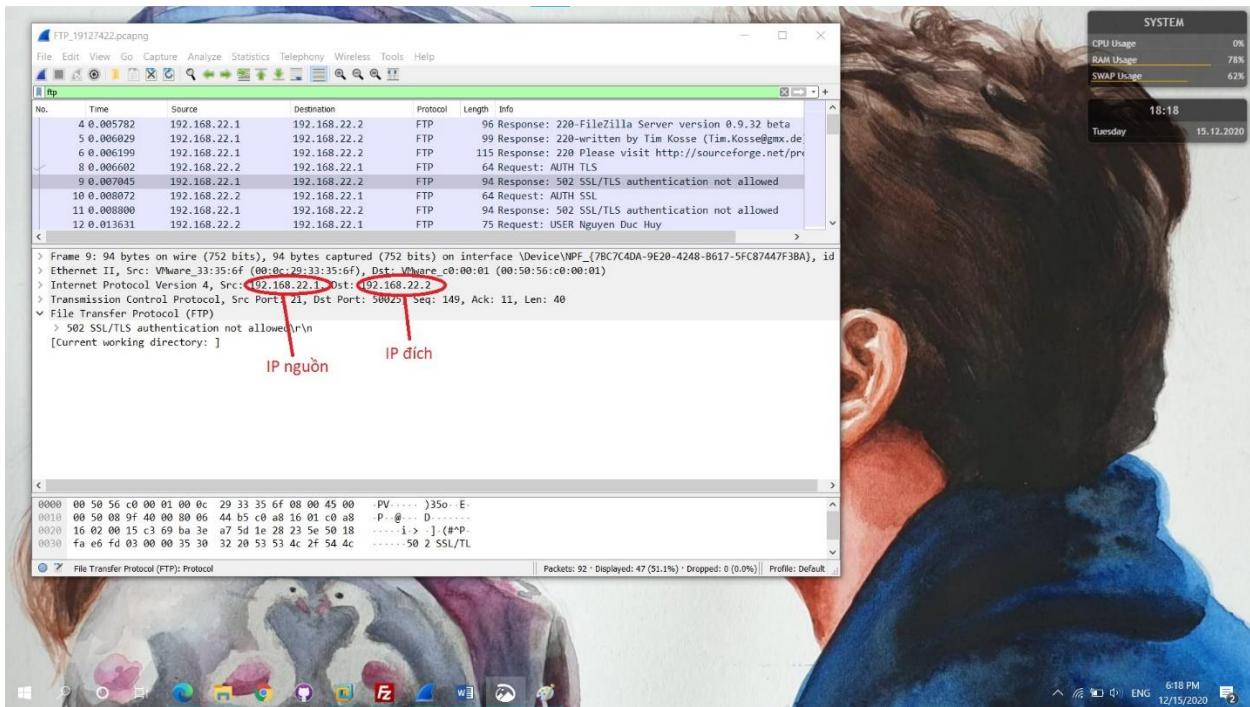
- User FTP: Người dùng FTP yêu cầu một tài khoản trên máy chủ và cho phép người dùng truy cập bất kỳ tập tin mà họ có thể truy cập nếu họ đã đăng nhập.
- Anonymous FTP: FTP ẩn danh là dành cho những người không có tài khoản và được sử dụng để cung cấp quyền truy cập vào các tệp cụ thể cho thế giới nói chung.

- IP nguồn, IP đích của các gói tin FTP?

Gói tin request: IP nguồn: 192.168.22.2 || IP đích: 192.168.22.1

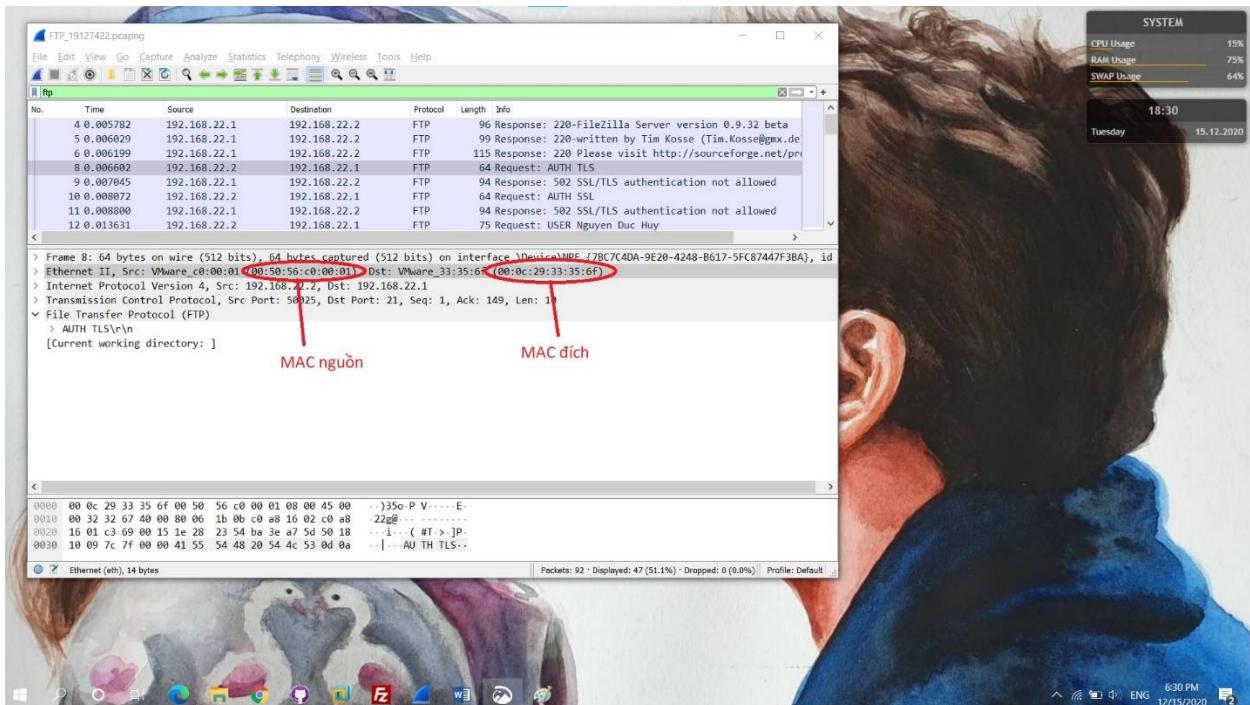


Gói tin response: IP nguồn: 192.168.22.1 || IP đích: 192.168.22.2

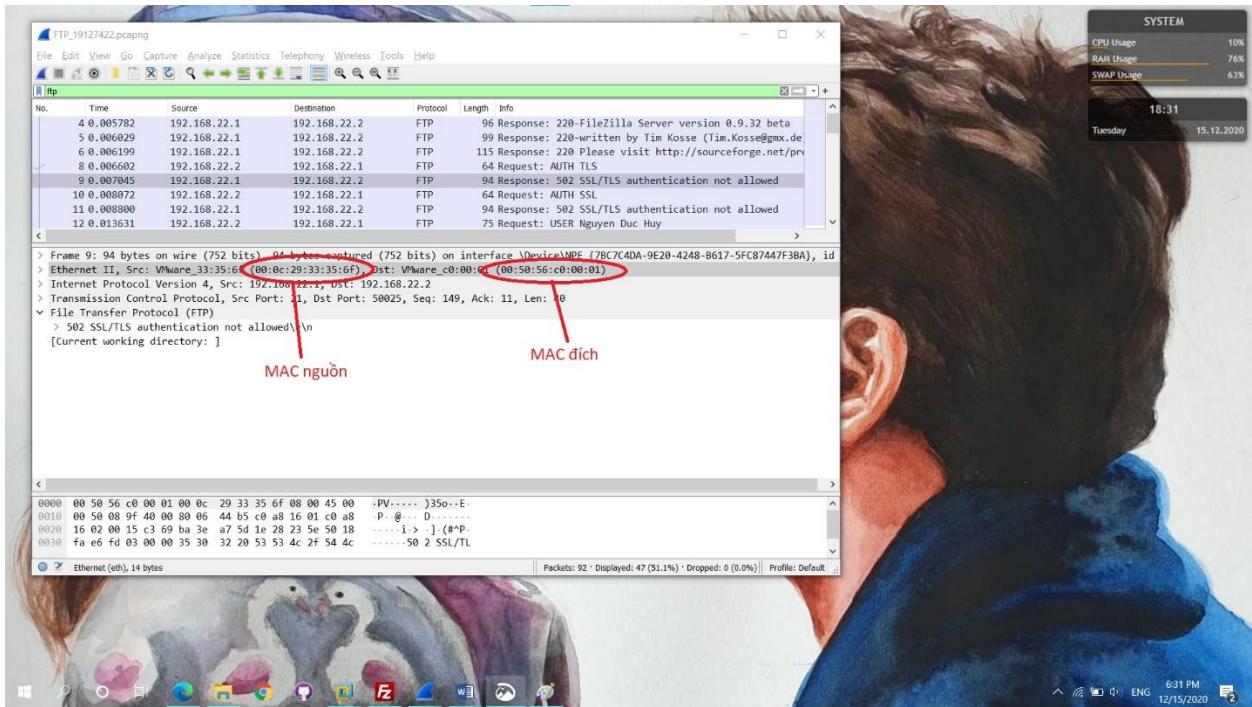


- MAC nguồn, MAC đích của các gói tin FTP?

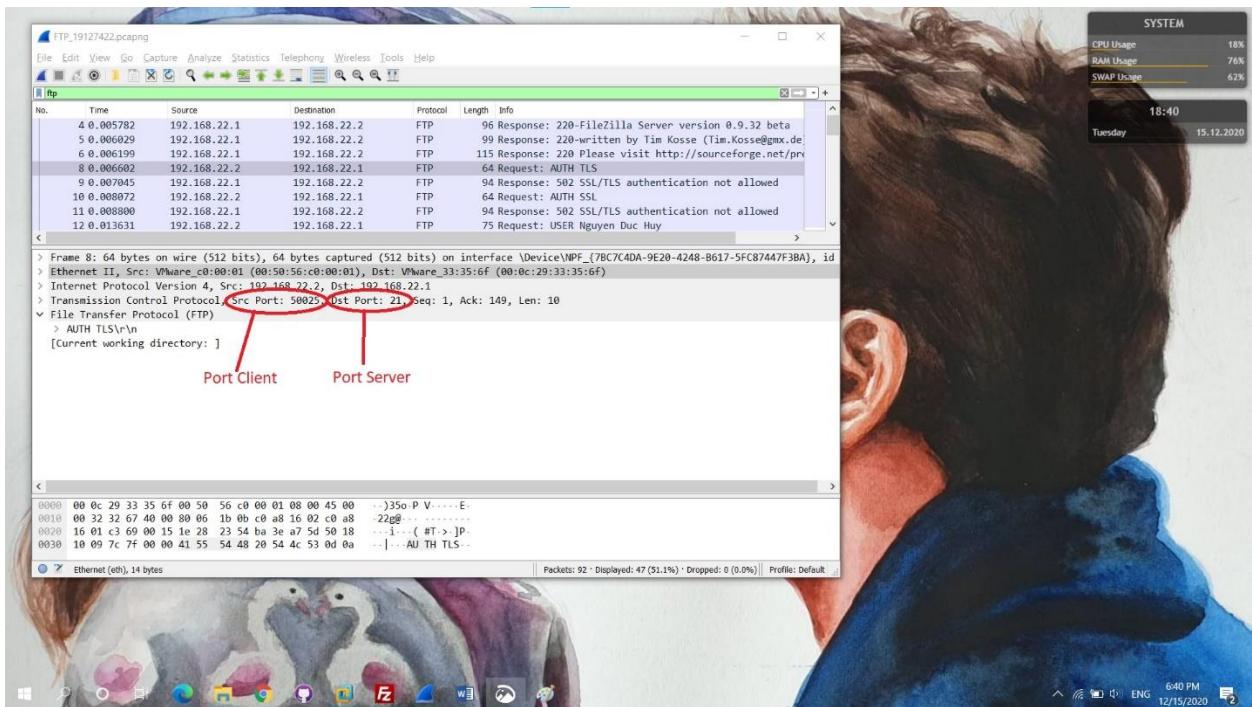
Gói tin request: MAC nguồn: (00:50:56:c0:00:01) || MAC đích: (00:0c:29:33:35:6f)



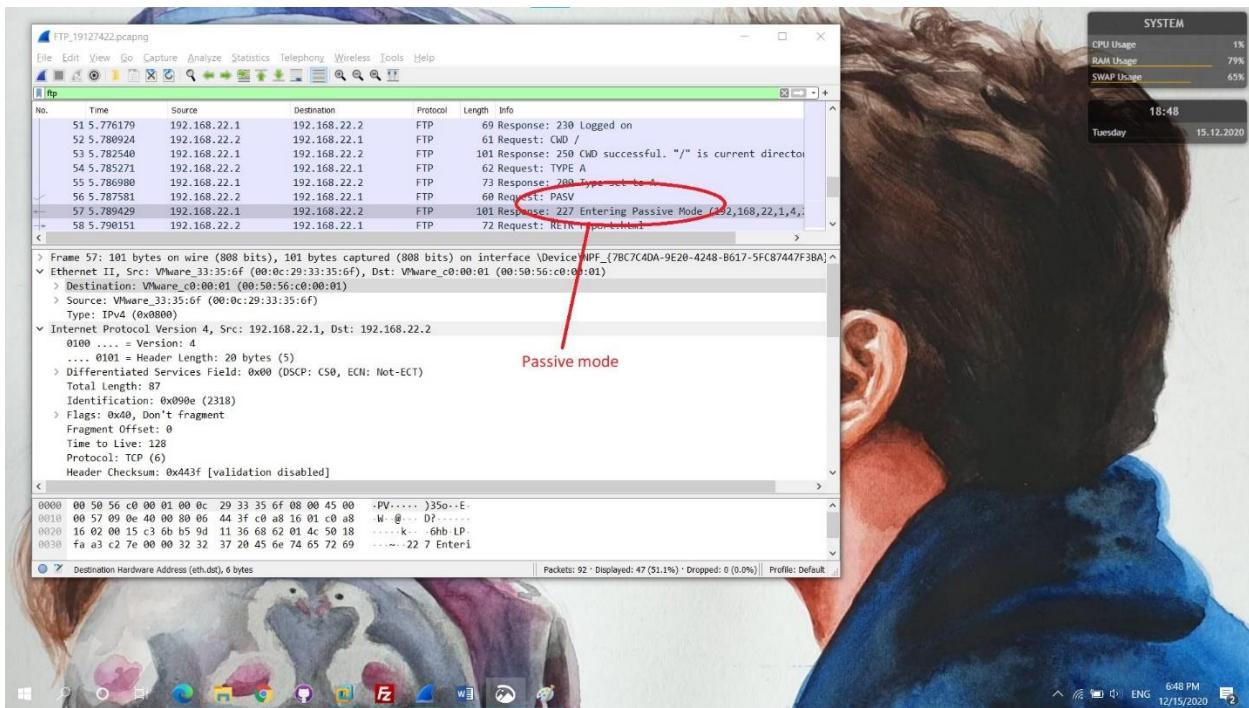
Gói tin response: MAC nguồn: (00:0c:29:33:35:6f) || MAC đích: (00:50:56:c0:00:01)



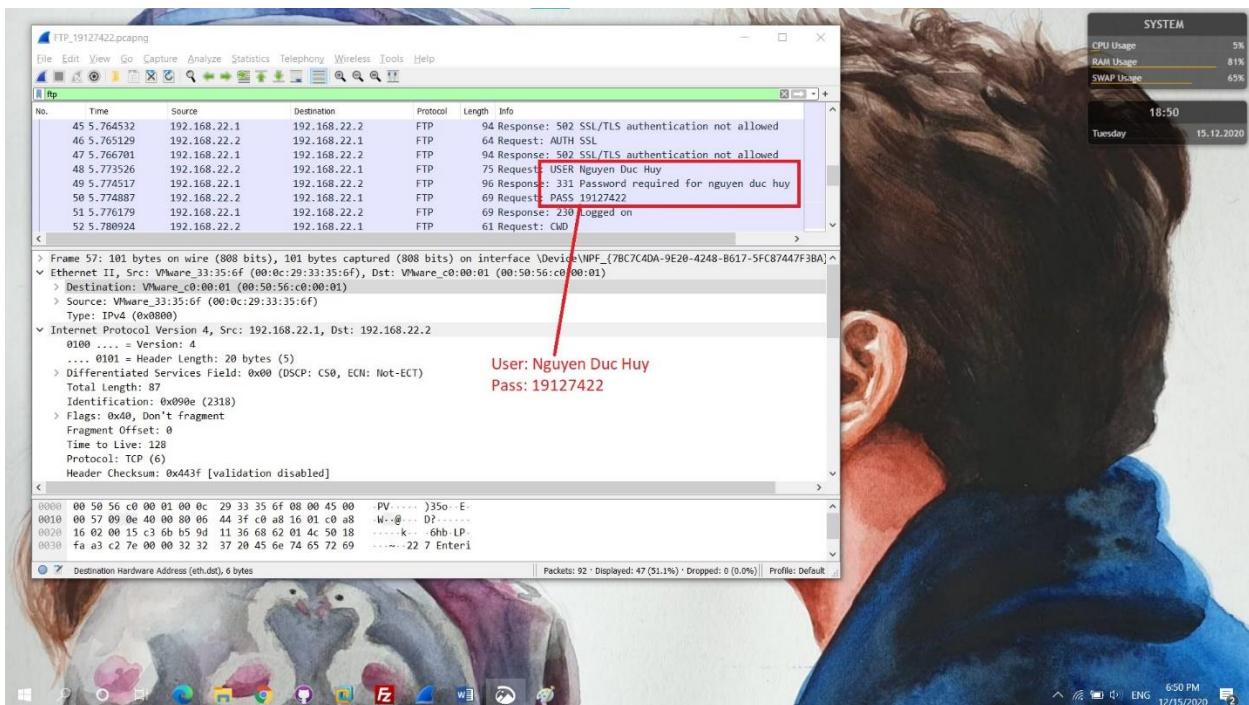
- FTP sử dụng port ở server và client là bao nhiêu?



- FTP đang sử dụng mode passive hay active?



- Chúng ta có lấy được thông tin user và password từ các gói tin FTP không?
Lấy được thông tin user và password từ các gói tin FTP:



4 Reference:

- [1].[Chapter 8\] 8.2 File Transfer \(ait.ac.th\)](#)
- [2].[ping – Wikipedia tiếng Việt](#)