**ĐỒ ÁN WIRESHARK**

**Họ Tên : Phạm Minh Châu**

**MSSV : 18600031**

**Về báo cáo:**

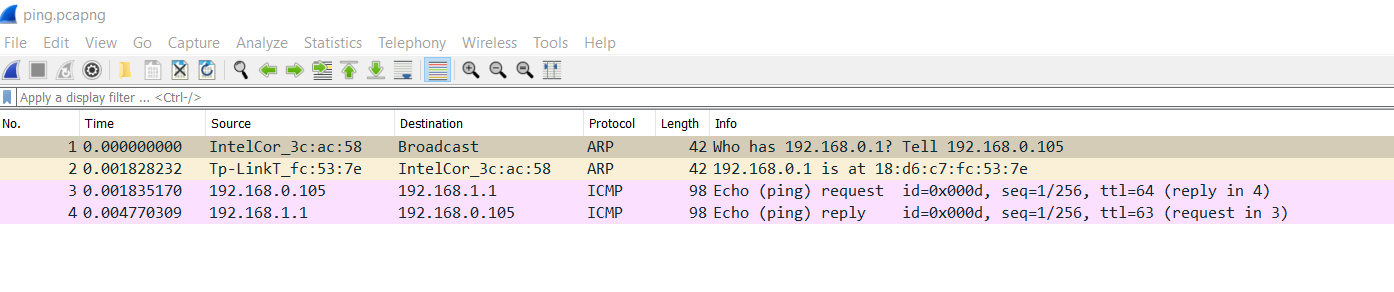
* Đánh giá mức độ hoàn thành từ 0 – 100% (Chú thích rõ những mục làm được,chưa làm được và còn bị lỗi)
* Trả lời các câu hỏi mà đồ án đưa ra
* Chụp hình để minh chứng cho câu trả lời (có tô đậm/ khoanh vùng cụ thể)

**BÀI LÀM**

## Bài 01: Ping (4đ)

1. Cho biết địa chỉ IP của host ping và host được ping?

* Địa chỉ IP Host ping: 192.168.1.1
* Địa chỉ IP Host được ping: 192.168.0.105



**2**. Cho biết port được sử dụng là bao nhiêu? Nếu không có port thì giải thích tại sao?

-Không thể biết được là port sử dụng bao nhiêu. Vì ICMP xuất phát từ tầng network gửi đi thì nó chỉ xuống tầng datalink thôi do đó khi bắt gói tin, ta không thể bắt được thông tin ở tầng application và tầng transport. Cho nên không thể biết được

**3**.Với gói tin ICMP request, cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

|  |  |  |  |
| --- | --- | --- | --- |
| **variable** | **8 bytes** | **20 bytes** | **14 bytes** |
| ICMP data | ICMP header | IP header | Ethernet header |

1. Tại sao lại có 2 gói ARP?

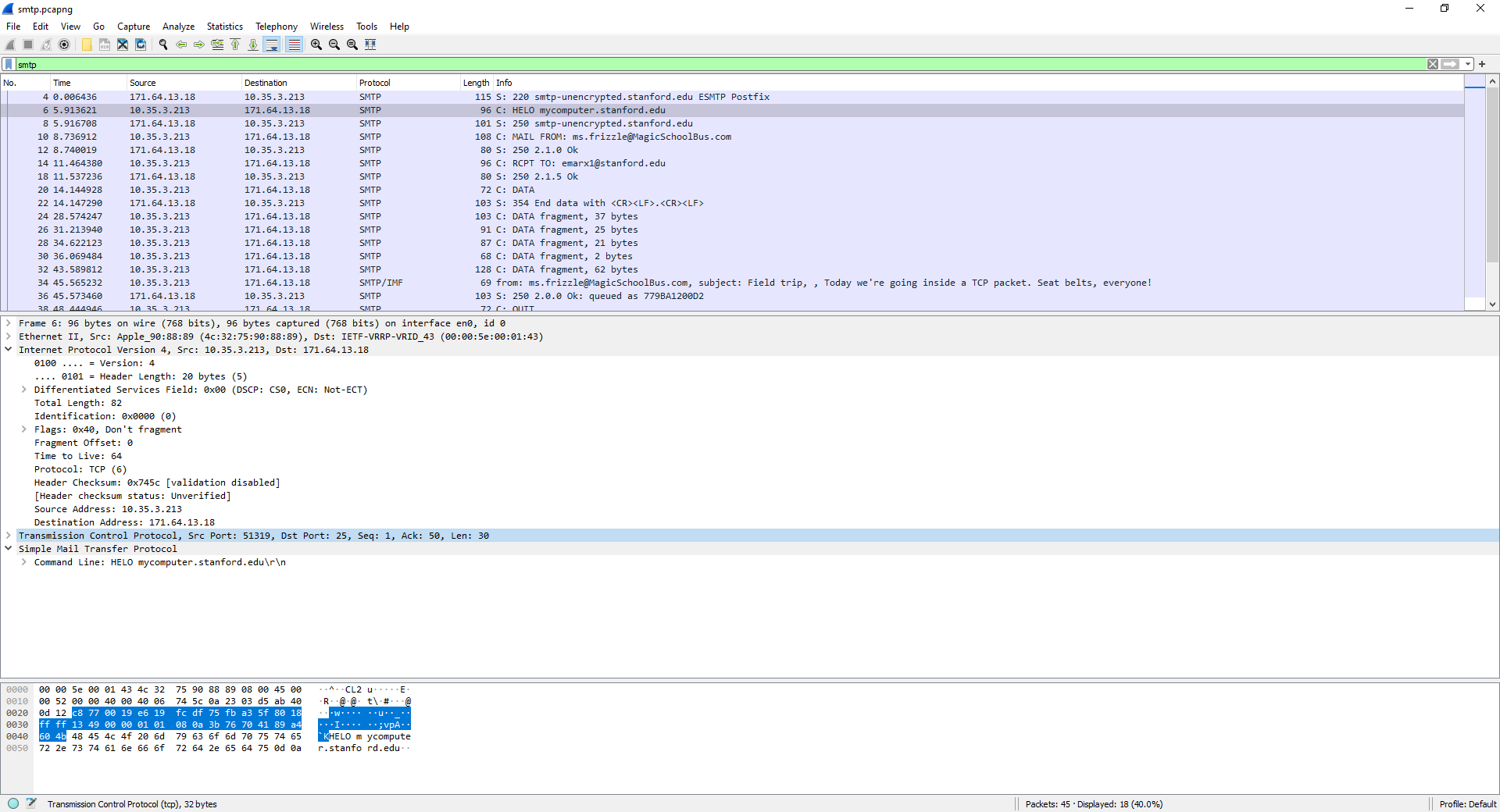
-Vì có 2 dạng bảng tin trong ARP một được gửi từ nguồn đến đích, và một được gửi từ đích tới nguồn.

## Bài 02: SMTP (6đ)

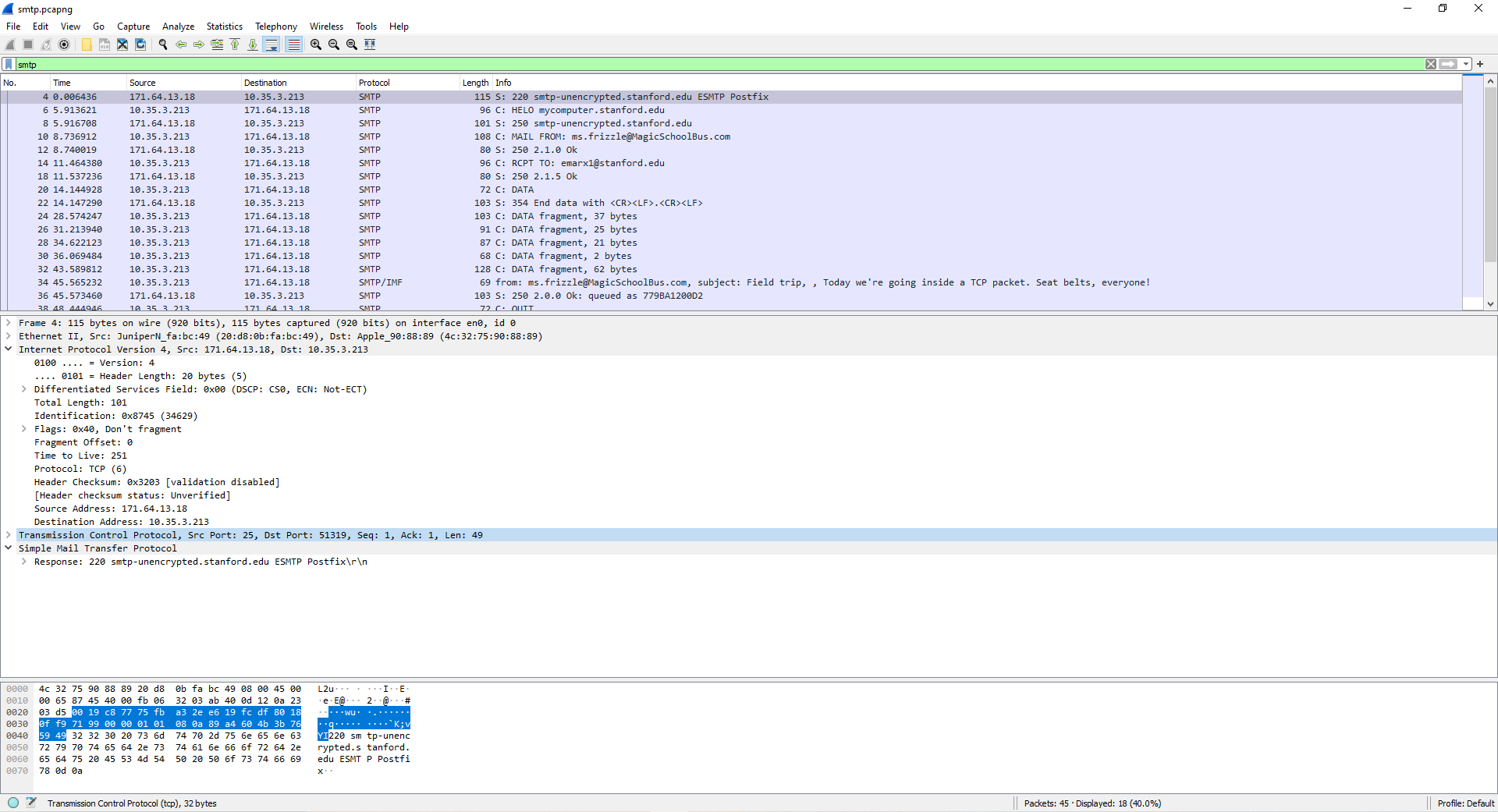
**1.SMTP dùng để làm gì ?**

SMTP là 3 chữ cái đầu viết tắt của Simple Mail Transfer Protocol dịch ra có nghĩa là giao thức truyền tải thư tín đơn giản hóa. Và giao thức này thực hiện nhiệm vụ chính là gửi mail còn việc nhận mail hay truy xuất dữ liệu mail server sẽ có giao thức IMAP hay POP3 đảm nhiệm.

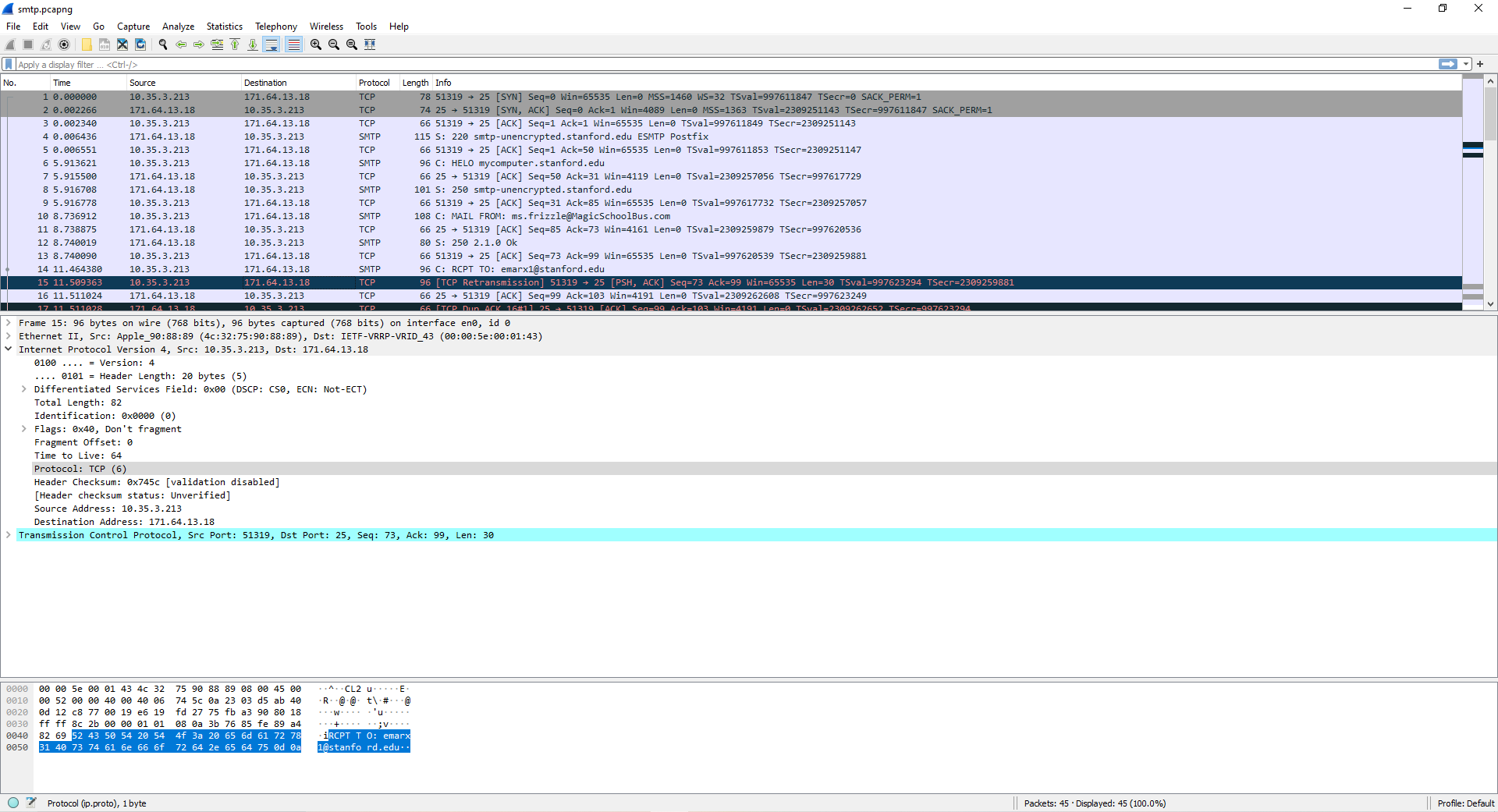
**2.Cho biết port của SMTP server?**



**3.Cho biết port của Client?**



**4.Protocol mà SMTP dùng ở tầng Transport?**



**5.Cho biết:**

* 1. Gói tin thứ mấy khởi đầu cho kết nối?

-Gói tin thứ 3

* 1. Cờ gì được sử dụng để nhận dạng là packet đầu tiên được sử dụng để khởi đầu cho kết nối?

-  Bắt đầu connection với máy chủ bằng cách gửi một packet với cờ "SYN" đến máy chủ.

* 1. Gói tin thứ mấy chứa 220 response từ SMTP server?

-Gói tin thứ 5

**6. Cho biết:**

1. Gói tin thứ mấy client báo đã nhận được 220 response từ Server?

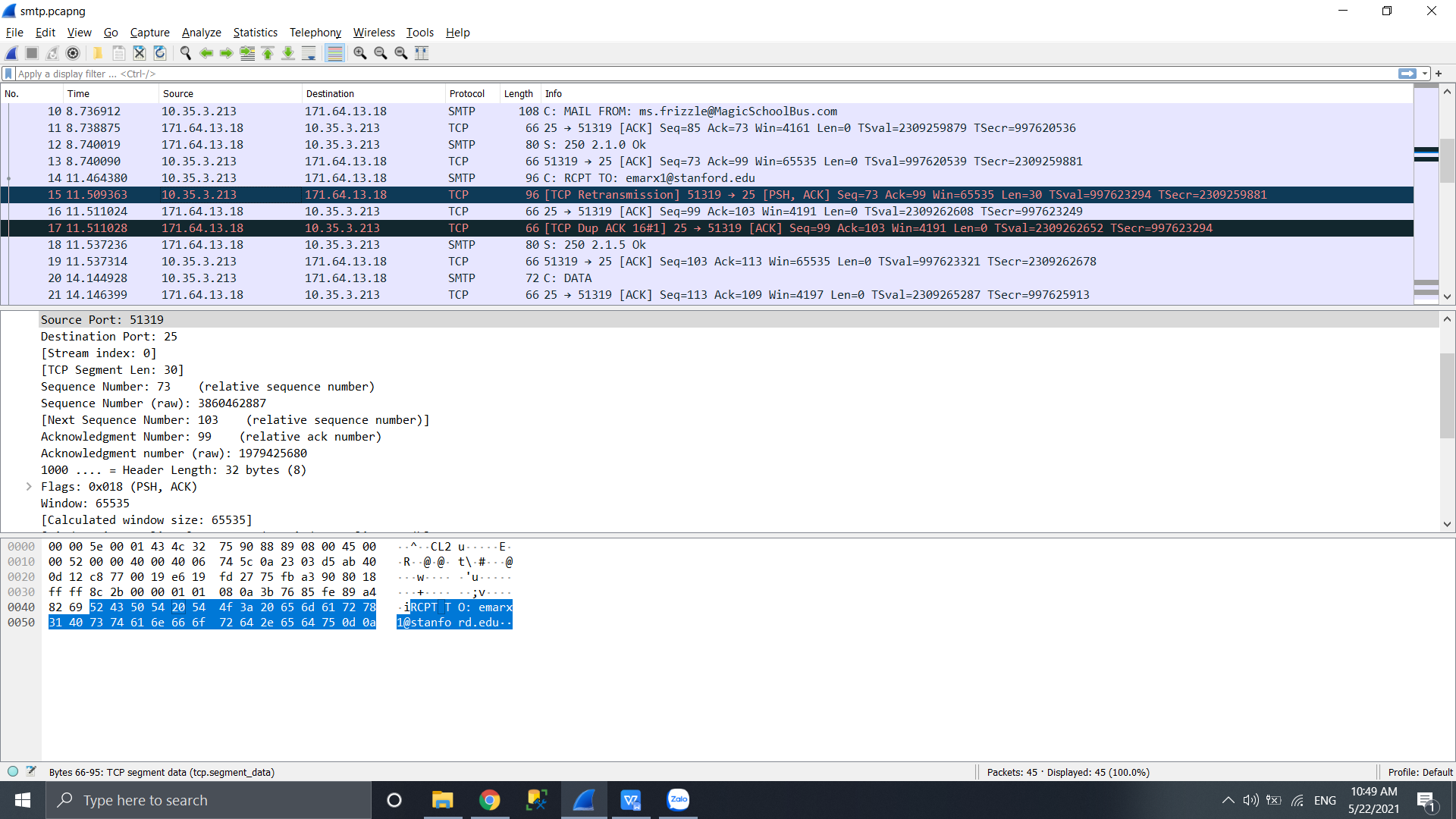
-Gói tin thứ 2

1. Cho biết ACK number của gói tin báo đã nhận được 220 response từ Server?
2. Xem xét ACK number, thì bạn sẽ thấy rằng nó lớn hơn chiều dài data của 220 response từ Server, điều đó có nghĩa là client đã nhận thêm 1 bytes trước khi nhận được 220. Cho biết data gì mà client đã nhận trước 220?
3. Tiếp theo, hãy nhìn sequence number of gói acknowledgement 220 là 1, nghĩa là client đã gửi 1 byte trước khi nhận gửi gói 220 acknowledgement. Cho biết data gì mà client đã gửi trước 220?

**7. Wireshark đánh dấu gói tin thứ 15 và 17 là duplicates. Cho biết những gói tin nào duplicate**

* 1. Packet 15 là của: ? (giải thích)
  2. Packet 17 là của: ? (giải thích)

**8.Filter với "tcp.len > 0", có bao nhiêu gói tin được hiển thị khi sử dụng filter?**



ĐÁNH GIÁ

|  |  |
| --- | --- |
| **Mức độ hoàn thành** | 80% |
| **Câu chưa làm được** | 6.2, - 6.3 - 6.4 - 7.1 - 7.2 |
| **Chụp hình để minh chứng** | CÓ |