

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN  
Khoa Công nghệ thông tin  
-----o0o-----



# MẠNG MÁY TÍNH

## Đồ án 2: WIRESHARK

Giảng viên: Huỳnh Thị Bảo Trân

Chung Thùy Linh

Thực hiện bởi:

22120096 – Kiều Trần Nhật Hào: Bài 2, Báo cáo

22120116 – Đoàn Gia Huệ: Bài 1

22120152 – Phạm Gia Khang: Bài 3, nhóm trưởng.

# GIỚI THIỆU

Báo cáo này tập trung vào việc thực hiện các thao tác liên quan đến phần mềm Wireshark, bao gồm việc bắt gói tin và kiểm tra ping. Wireshark, một công cụ mạnh mẽ cho việc phân tích dữ liệu mạng, đóng vai trò quan trọng trong việc theo dõi và hiểu rõ giao tiếp mạng. Bài báo cáo này nhấn mạnh vào quá trình bắt gói tin, một kỹ thuật quan trọng để theo dõi thông tin mạng và phát hiện vấn đề liên quan đến bảo mật.

Wireshark là công cụ mạng mạnh mẽ, cho phép bắt gói tin và phân tích dữ liệu mạng. Với giao diện đồ họa thân thiện, Wireshark giúp người dùng hiểu rõ giao tiếp mạng và giải quyết vấn đề một cách hiệu quả. Đây là công cụ không thể thiếu trong lĩnh vực quản lý và bảo mật mạng.

Bài báo cáo tập trung vào việc trả lời và thực hiện các câu hỏi của giảng viên về các thao tác khi sử dụng công cụ này để ping một và nhiều gói tin cụ thể.

Bằng cách này, báo cáo này không chỉ cung cấp kiến thức chi tiết về Wireshark mà còn hướng dẫn cách áp dụng kiến thức này vào thực tế thông qua việc thực hiện bài tập và phân tích kết quả.

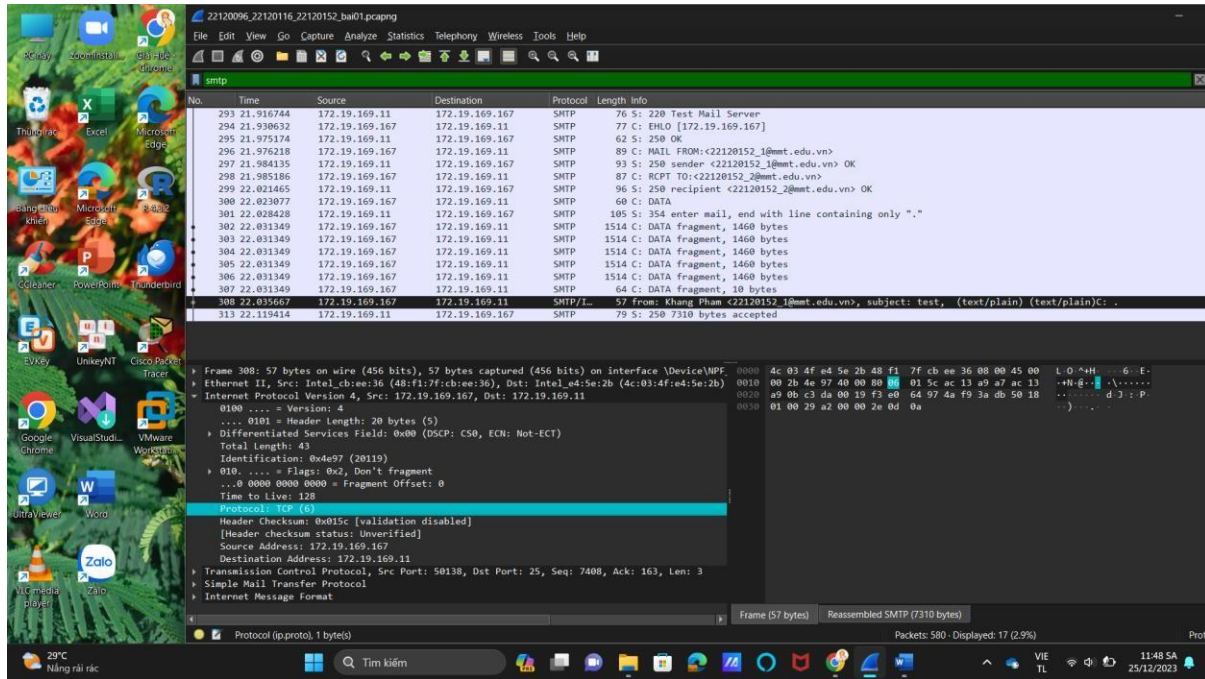
Bài báo cáo là công sức, thời gian, và chất xám của tập thể ba thành viên chúng em, mọi sự đóng góp của mỗi thành viên đều rất giá trị và vô cùng cần thiết, chúng em cảm ơn giảng đã đọc bài báo cáo đồ án này và luôn sẵn sàng tiếp thu những ý kiến, đóng góp, đánh giá quý báu của giảng viên. Chúng em xin cảm ơn!

## 1. Bài 1.

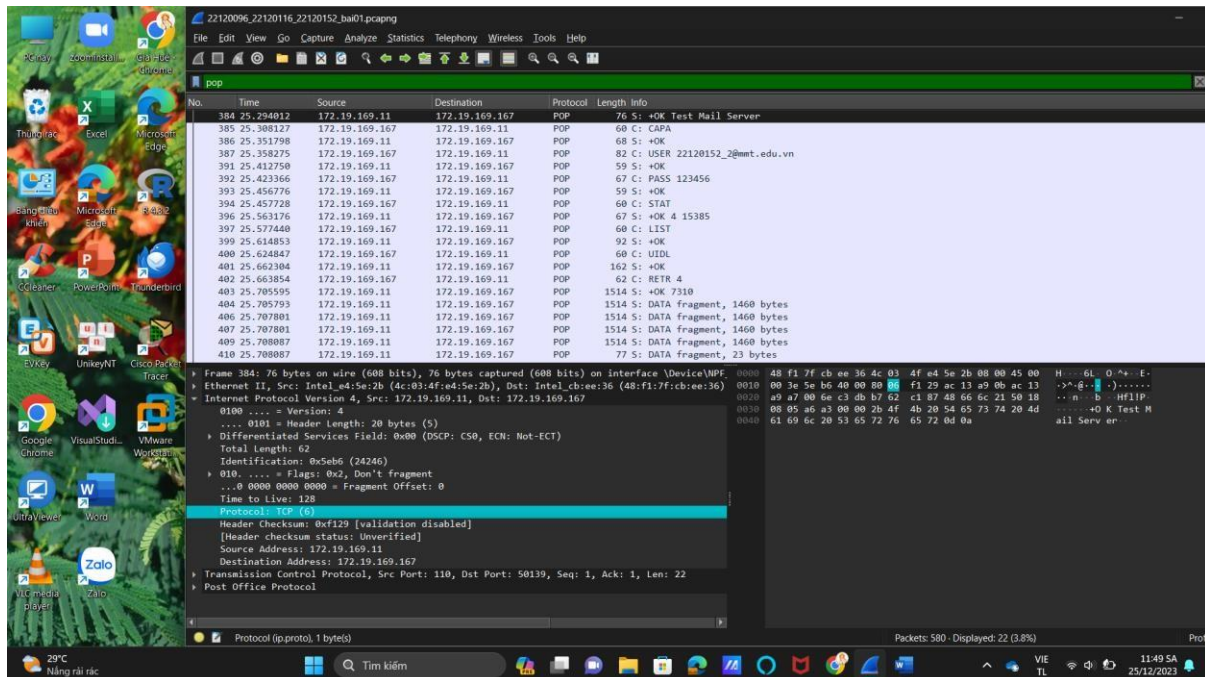
i. *Lọc các gói tin sử dụng giao thức smtp và pop3.*

SMTP:

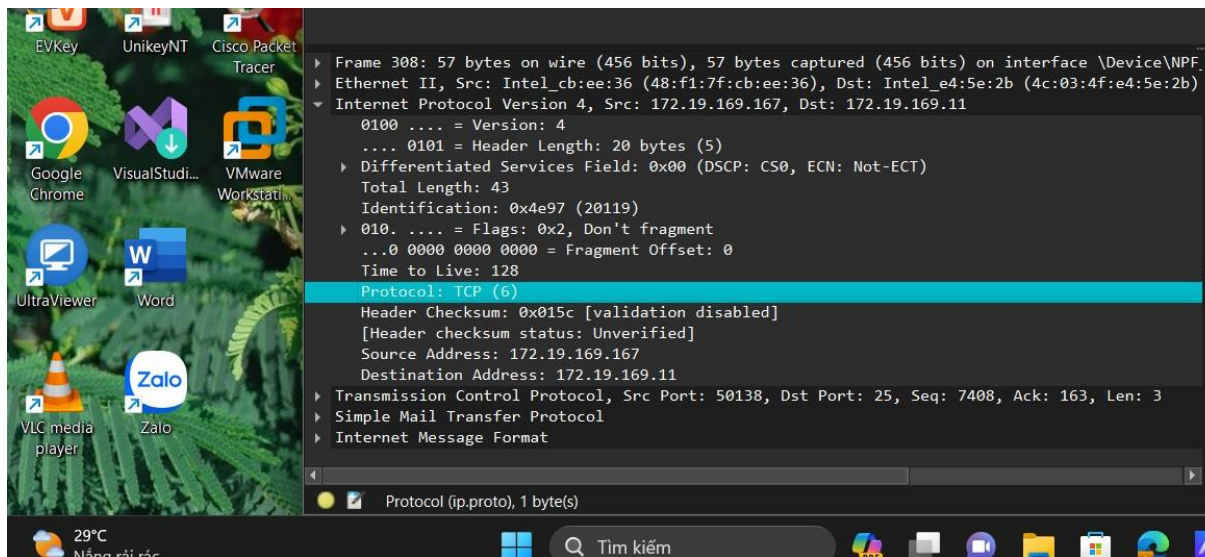
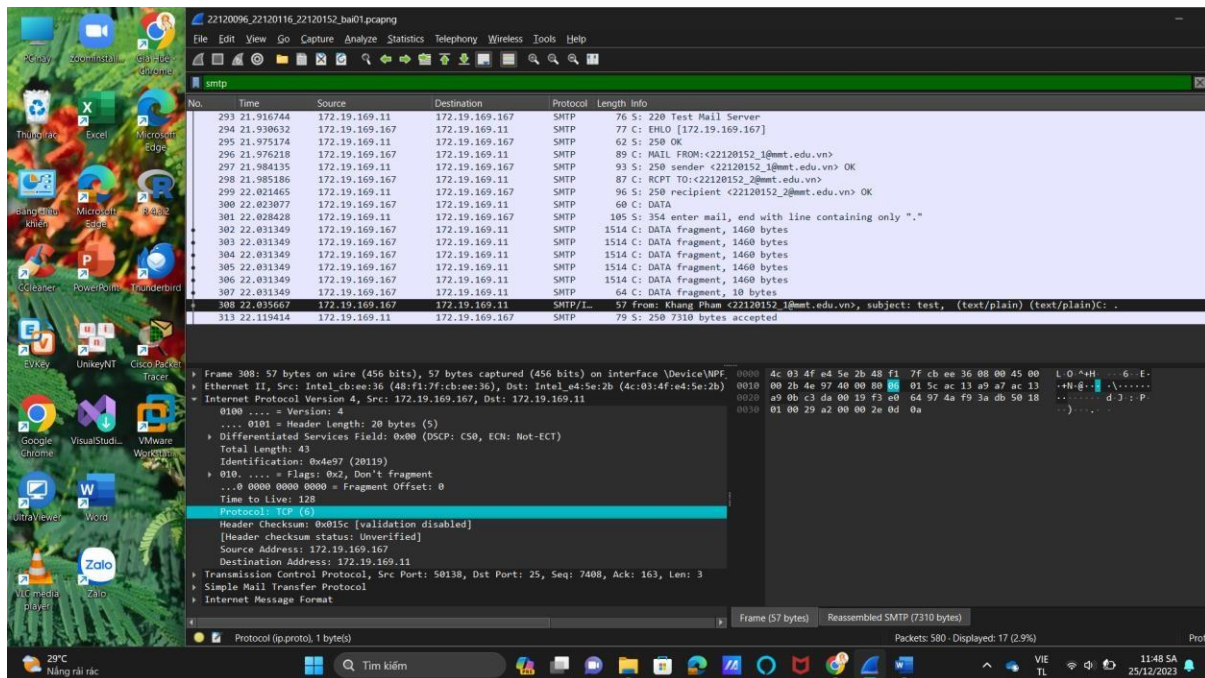
Trên thanh filter nhập: smtp



POP3:



Trên thanh filter nhập: pop

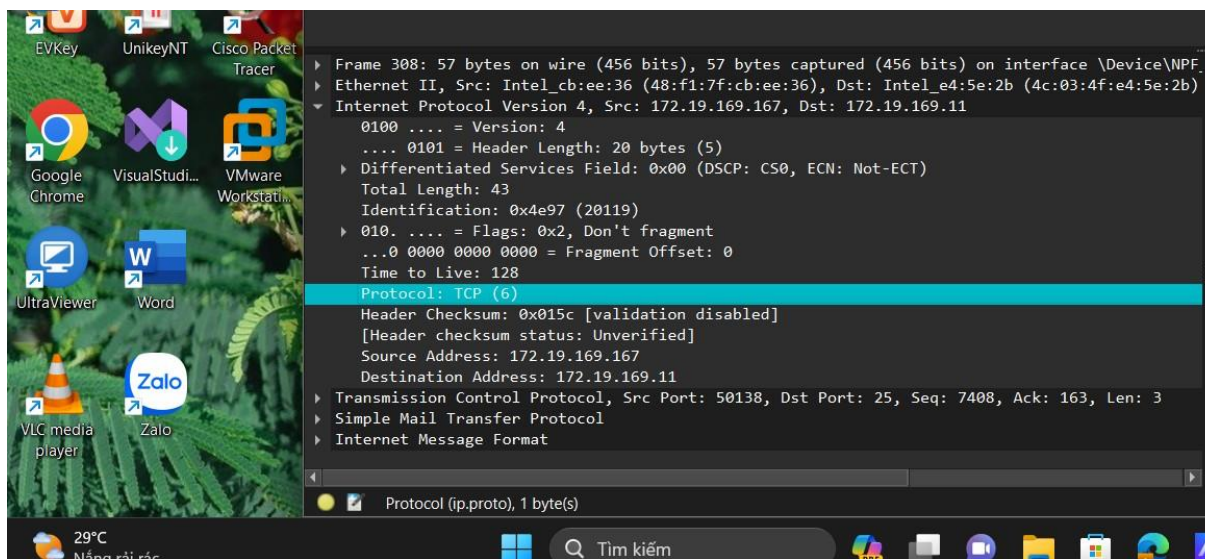
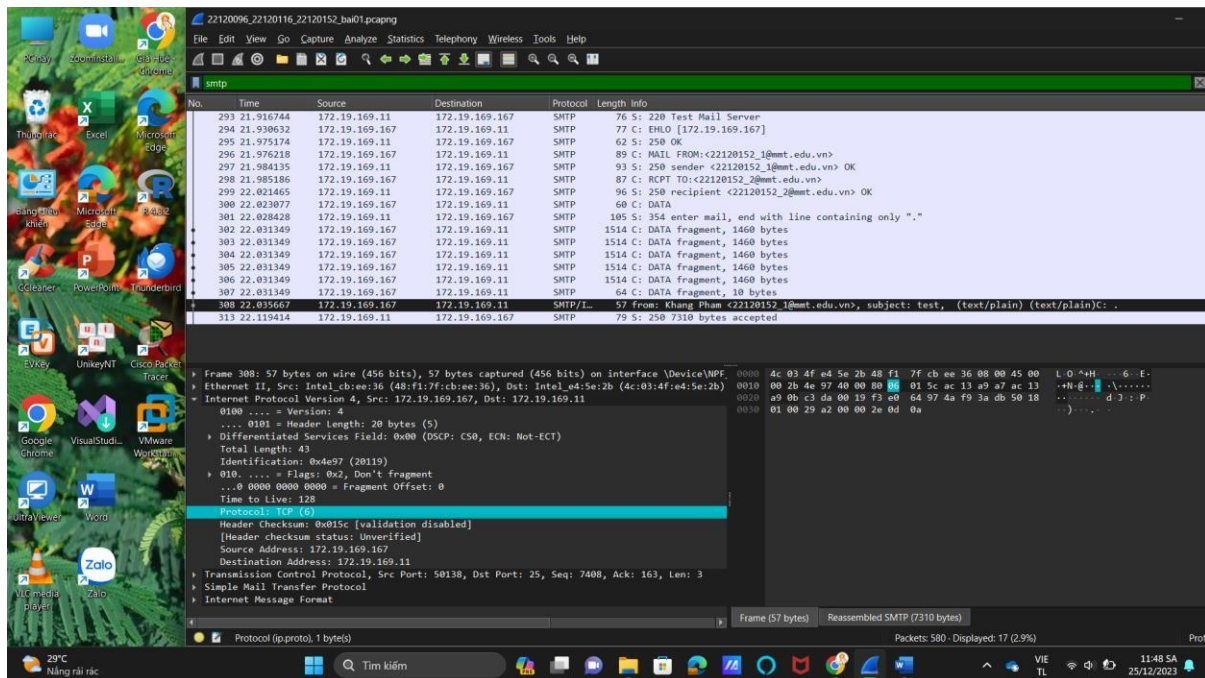


- ii. Quan sát lưu lượng được ghi lại trong ngăn danh sách gói tin bắt được. Hãy chỉ ra giao thức được sử dụng tại tầng transport của gói tin SMTP và POP3

SMTP: giao thức được sử dụng tại tầng transport: TCP

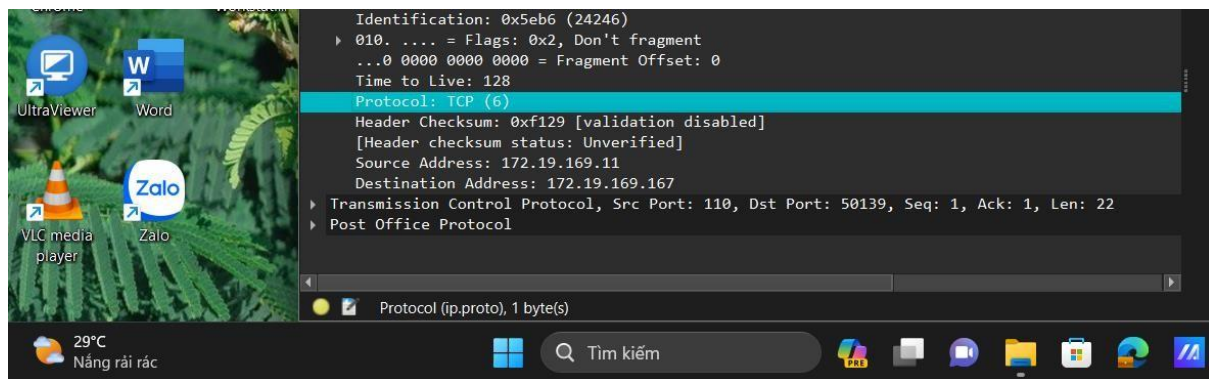
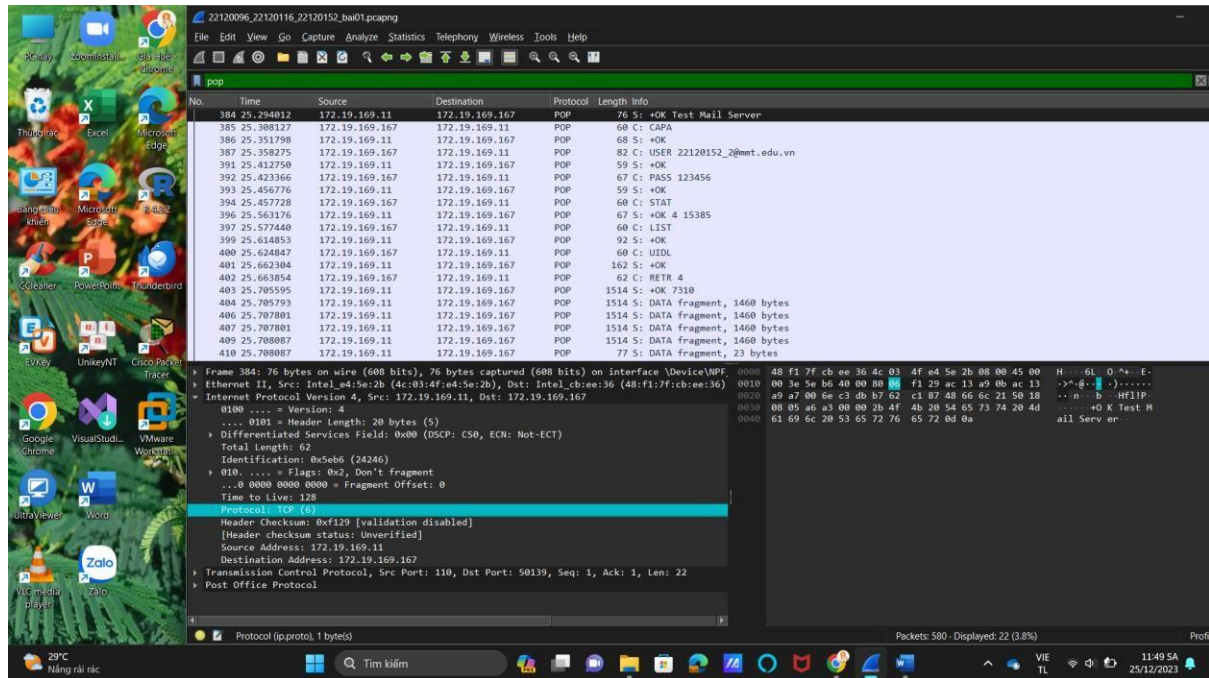
Trên thanh filter nhập: smtp



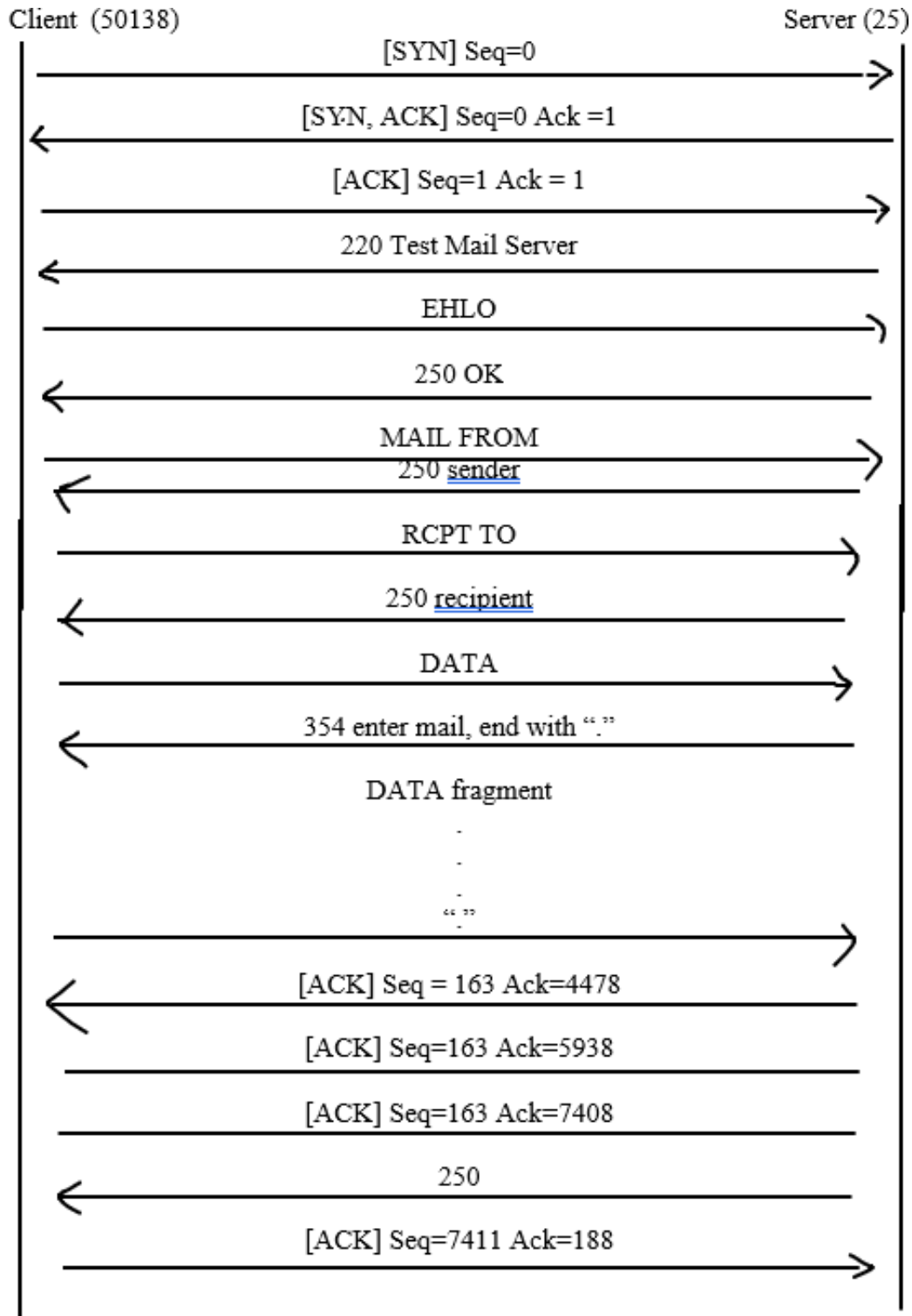


POP3: giao thức được sử dụng tại tầng transport: TCP

Trên thanh filter nhập: tcp

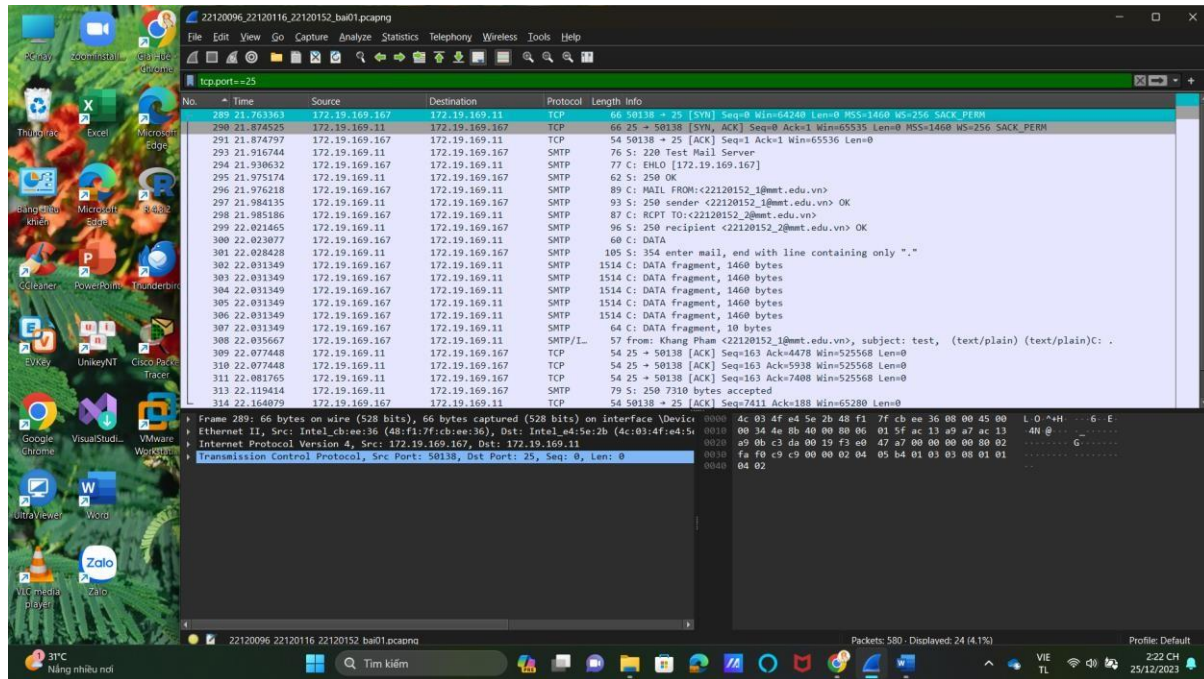


iii. *Vẽ quá trình trao đổi gói tin giữa SMTP server và SMTP client.*



- iv. *Lọc gói tin theo giao thức sử dụng tại tầng transport của gói tin SMTP. Cho biết ý nghĩa 3 gói tin đầu tiên trong danh sách. Ghi rõ thông tin sequence number, acknowledgement number của những gói tin này.*

Trên thanh filter nhập: tcp.port==25



3 gói tin đầu tiên thể hiện quá trình bắt tay 3 bước giữa SMTP client và SMTP server:

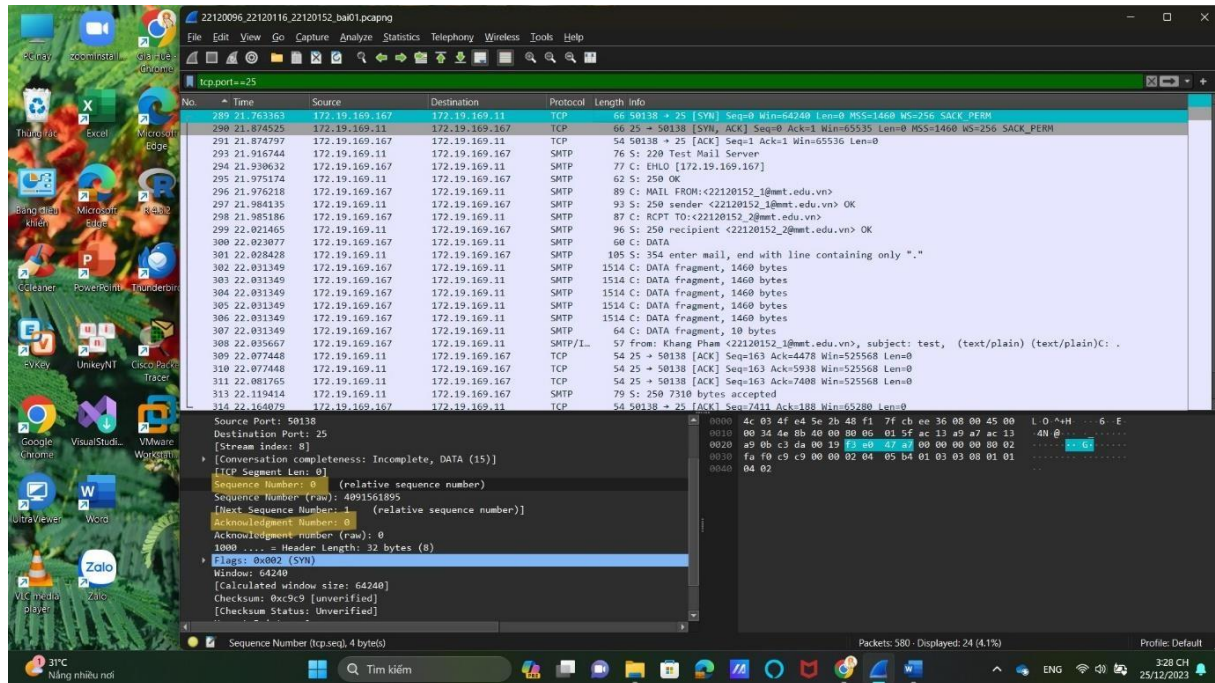
1. Gói Tin Mở Đầu (SYN):

Ý Nghĩa: Gói tin này được gửi từ máy khách (SMTP client) đến máy chủ (SMTP server) để bắt đầu quá trình mở kết nối.

Sequence Number: Seq=0

Acknowledgement Number: Ack= 0



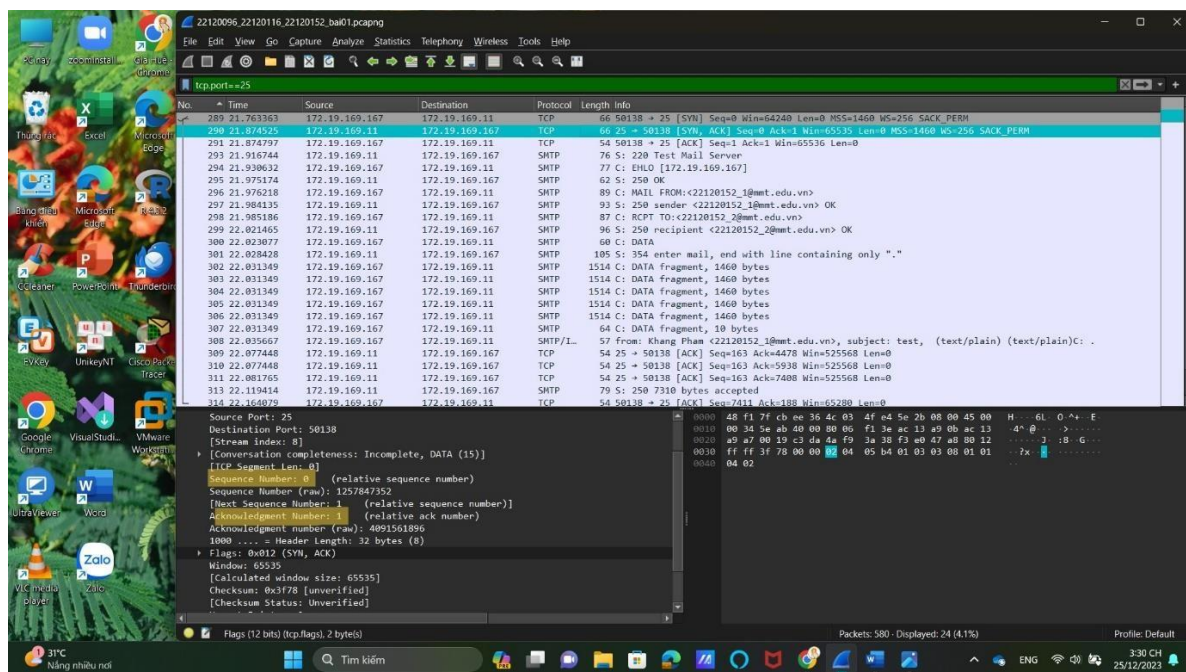


## 2. Gói Tin Phản Hồi (SYN-ACK):

Ý Nghĩa: Máy chủ (SMTP server) phản hồi bằng cách gửi gói tin này cho máy khách để xác nhận rằng nó đã nhận được yêu cầu mở kết nối (SYN) và sẵn sàng thiết lập kết nối.

Sequence Number: Seq=0

Acknowledgement Number: Giá trị này bằng với Sequence Number của gói tin SYN tương ứng, cộng thêm 1. Ack=1

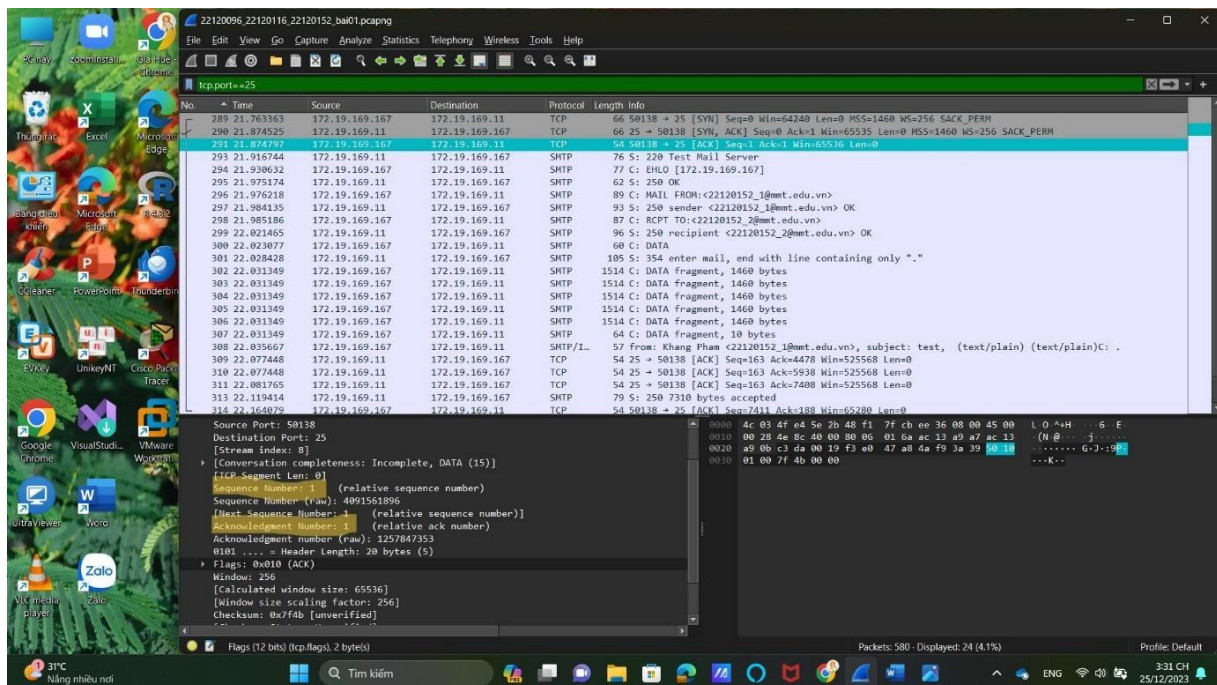


## 3. Gói Tin Xác Nhận (ACK):

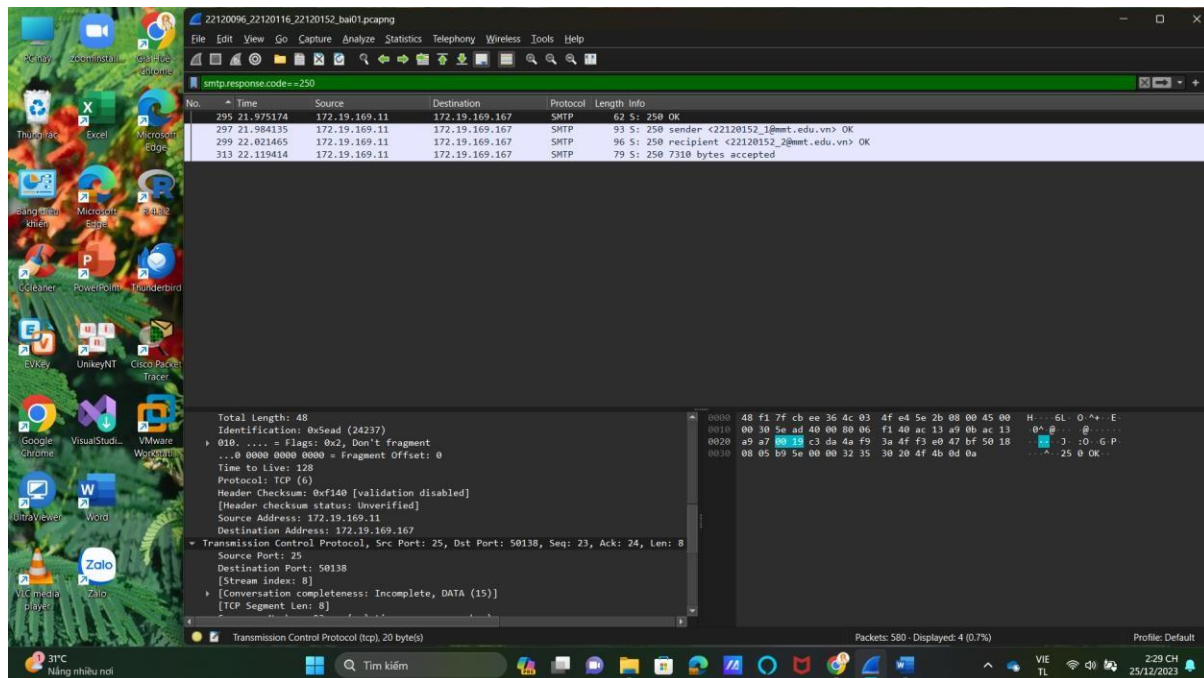
Ý Nghĩa: Máy khách (SMTP client) xác nhận rằng nó đã nhận được phản hồi từ máy chủ và đã sẵn sàng bắt đầu truyền tải dữ liệu.

Thông Tin Sequence Number: Seq=1

Acknowledgement Number: Giá trị này bằng với Sequence Number của gói tin SYN-ACK tương ứng, cộng thêm 1. Ack=1



- v. *Lọc các gói tin SMTP có nhãn 221 hay 250 (nếu không nhìn thấy gói tin có nhãn 221). Quan sát chi tiết những gói tin này và cho biết giá trị các trường “Response Code”, “Response Parameter”. Cho biết ý nghĩa các thông số này.*



Trên thanh filter nhập: smtp.response.code==250

1. Gói Tin No.295:
  - Nội dung gói tin: "S: 250 OK"
  - Response Code: 250
  - Response Parameter: OK
  - Ý Nghĩa: Máy chủ SMTP đã xử lý thành công yêu cầu hoặc lệnh trước đó và sẵn sàng tiếp nhận các lệnh tiếp theo.
2. Gói Tin No.297:
  - Nội dung gói tin: "S: 250 sender 22120152\_1@mmt.edu.vn OK"
  - Response Code: 250
  - Response Parameter: sender 22120152\_1@mmt.edu.vn OK
  - Ý Nghĩa: Máy chủ SMTP thông báo rằng địa chỉ người gửi ("sender") đã được chấp nhận thành công.
3. Gói Tin No.299:
  - Nội dung gói tin: "S: 250 recipient 22120152\_2@mmt.edu.vn OK"
  - Response Code: 250
  - Response Parameter: recipient 22120152\_2@mmt.edu.vn OK

- Ý Nghĩa: Máy chủ SMTP thông báo rằng địa chỉ người nhận ("recipient") đã được chấp nhận thành công.

4. Gói Tin No.313:

- Nội dung gói tin: "S: 250 7310 bytes accepted"
- Response Code: 250
- Response Parameter: 7310 bytes accepted
- Ý Nghĩa: Máy chủ SMTP thông báo rằng dữ liệu thư có dung lượng 7310 bytes đã được chấp nhận thành công.



## 2. Bài 2.

### i. Cho biết địa chỉ của host ping và host được ping?

- Địa chỉ host ping: 192.168.0.105.
- Địa chỉ host được ping: 192.168.1.1.

### ii. Cho biết port được sử dụng là bao nhiêu, nếu không có thì giải thích tại sao?

- Không thể lấy được thông tin về port.
- Giải thích: Giao thức được sử dụng là giao thức ICMP.

Giao thức ICMP (Internet Control Message Protocol) được sử dụng trong quá trình ping không sử dụng khái niệm "port" như các giao thức khác như TCP hoặc UDP. ICMP được thiết kế để truyền tải các tin nhắn kiểm soát và thông báo lỗi, không chứa thông tin về cổng (port). Đặc biệt, nó hoạt động ở tầng mạng (network layer) trong mô hình OSI, không liên quan đến các cổng tại tầng transport layer (tầng vận chuyển) như TCP hoặc UDP.

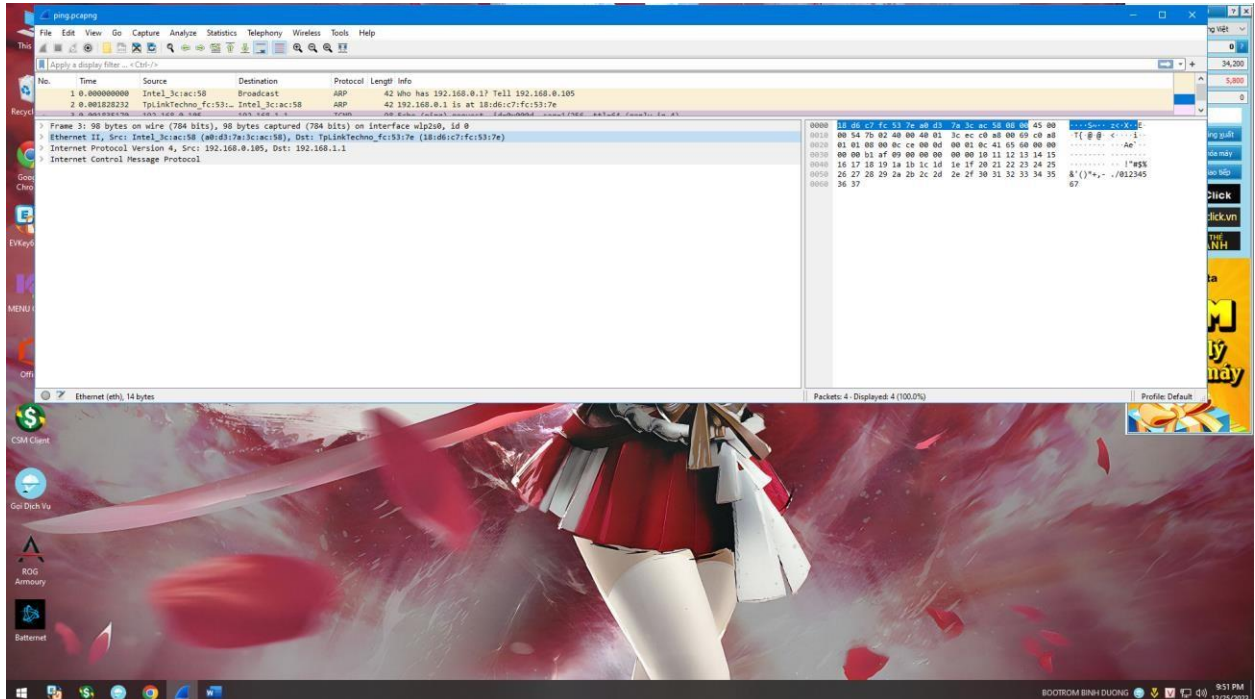
Khi thực hiện lệnh ping, nó tạo ra các gói tin ICMP Echo Request và chờ đợi gói tin ICMP Echo Reply từ máy chủ đích. Người dùng sẽ không thấy thông tin về cổng trong quá trình này vì ICMP không tham gia truyền tải dữ liệu theo kiểu "cổng" như trong các giao thức khác.

Port là một khái niệm chủ yếu liên quan đến giao thức transport layer như TCP và UDP để xác định dịch vụ hay ứng dụng cụ thể nào đang gửi hay nhận dữ liệu. ICMP không có cơ chế này, nó chỉ tập trung vào truyền thông tin kiểm soát giữa các thiết bị trong mạng.

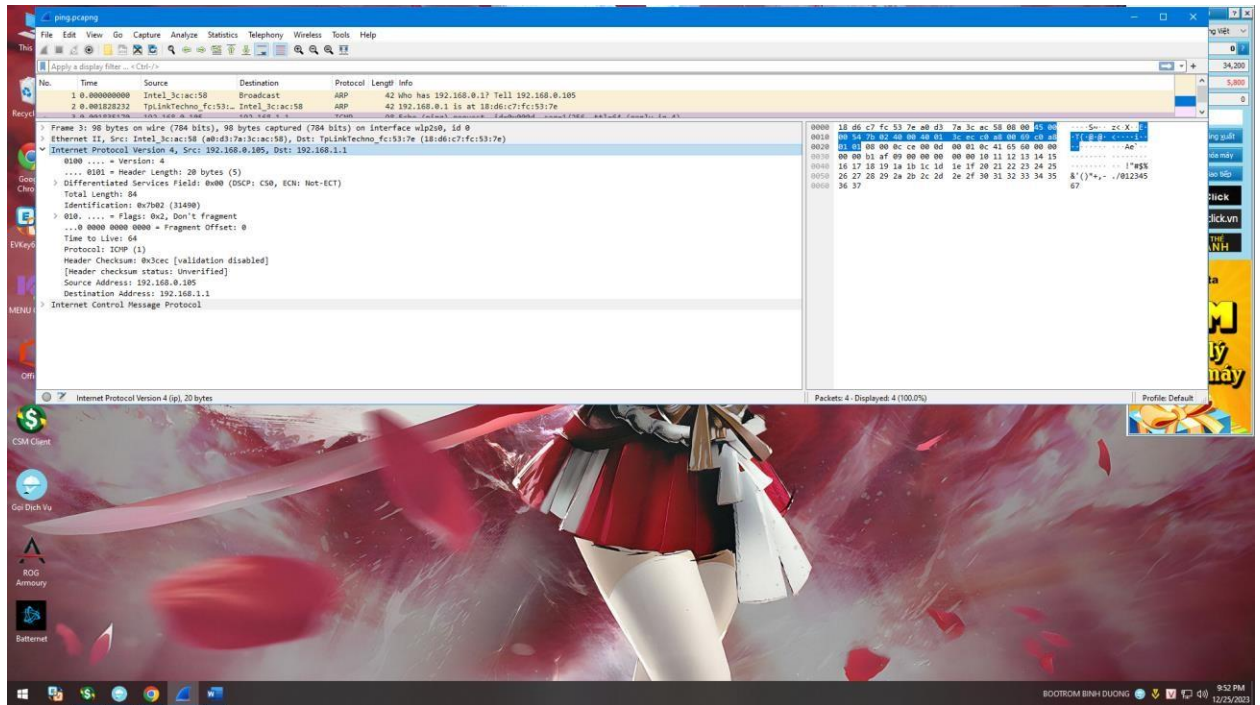
### iii. Với gói tin ICMP request, cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

**Bảng thông tin kích thước của từng thành phần (đơn vị: byte):**

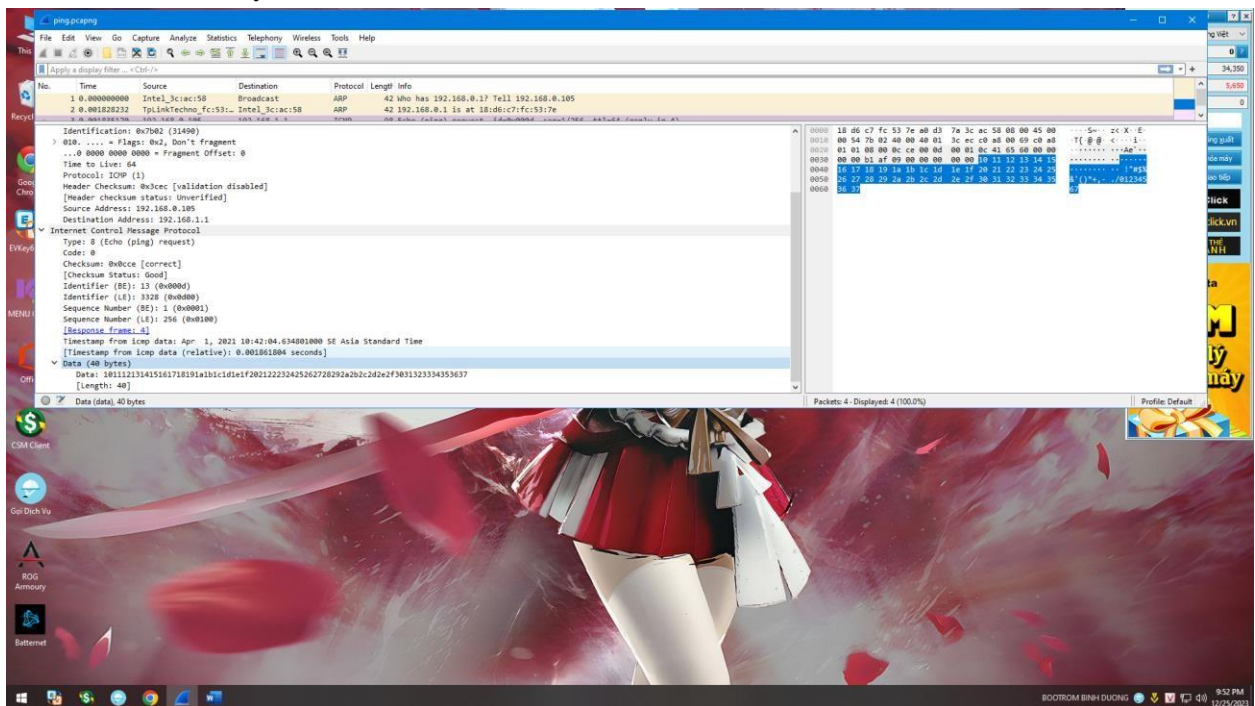
- Ethernet header: 14 byte



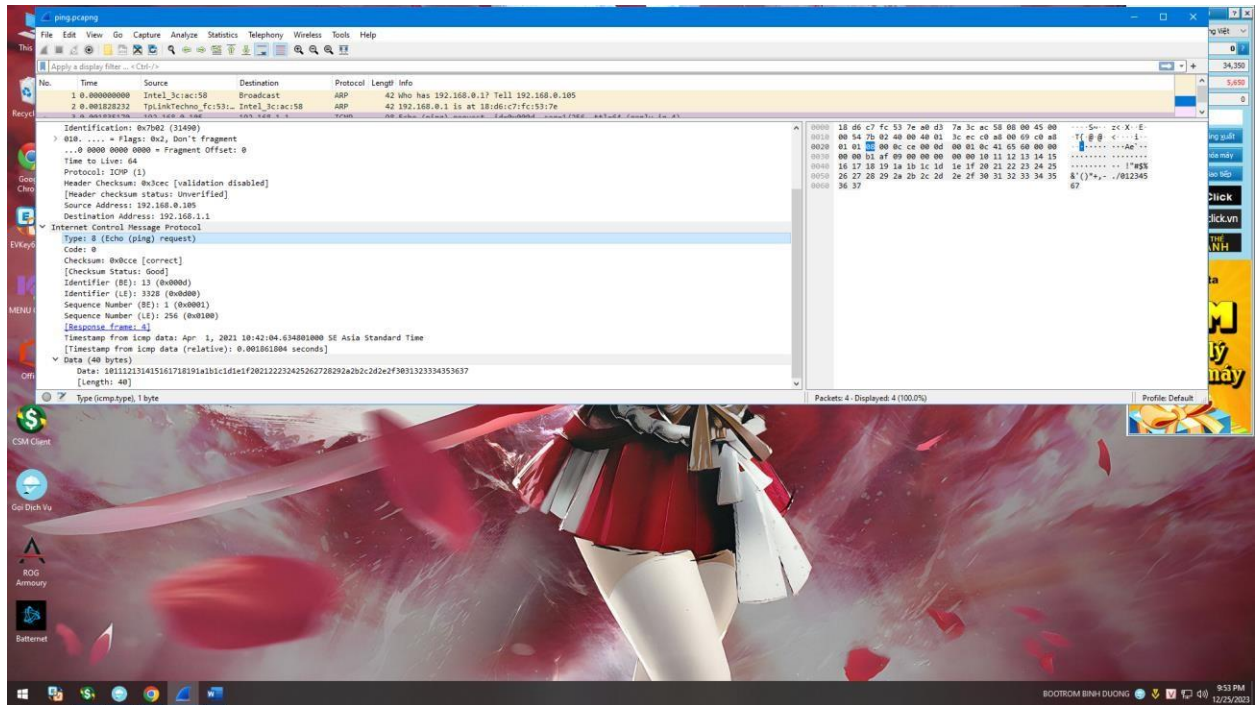
- IP header: 20 byte



- ICMP data: 40 byte



- ICMP header: 8 byte



Tên gói	ICMP data	ICMP header	IP header	Ethernet header
No.3: Request	40	8	20	14

iv. *Cho biết có bao nhiêu gói tin ARP? Giải thích tại sao lại có các gói tin ARP này, nêu ý nghĩa của các gói tin đó?*

- Có hai gói tin ARP.
- Mục đích chung của hai gói tin ARP (Address Resolution Protocol) trong quá trình thực hiện lệnh ping bằng ICMP là thiết lập sự tương ứng giữa địa chỉ IP và địa chỉ MAC (vật lý) của các thiết bị trong mạng. Dưới đây là mục đích chi tiết của mỗi gói tin ARP:

+ ARP Request:

Khi thực hiện lệnh ping, máy tính của bạn cần biết địa chỉ MAC (địa chỉ vật lý) của máy chủ đích.

Máy tính sẽ gửi một gói tin ARP Request để hỏi "Ai có địa chỉ IP là X.X.X.X?". Điều này được thực hiện để định danh địa chỉ MAC tương ứng với địa chỉ IP của máy chủ đích.

+ ARP Reply:

Máy chủ đích sau khi nhận được gói tin ARP Request sẽ phản hồi bằng một gói tin ARP Reply chứa thông tin địa chỉ MAC của nó.

Các máy tính trong mạng còn lại cũng sẽ cập nhật bảng ARP của họ với thông tin mới nhận được.

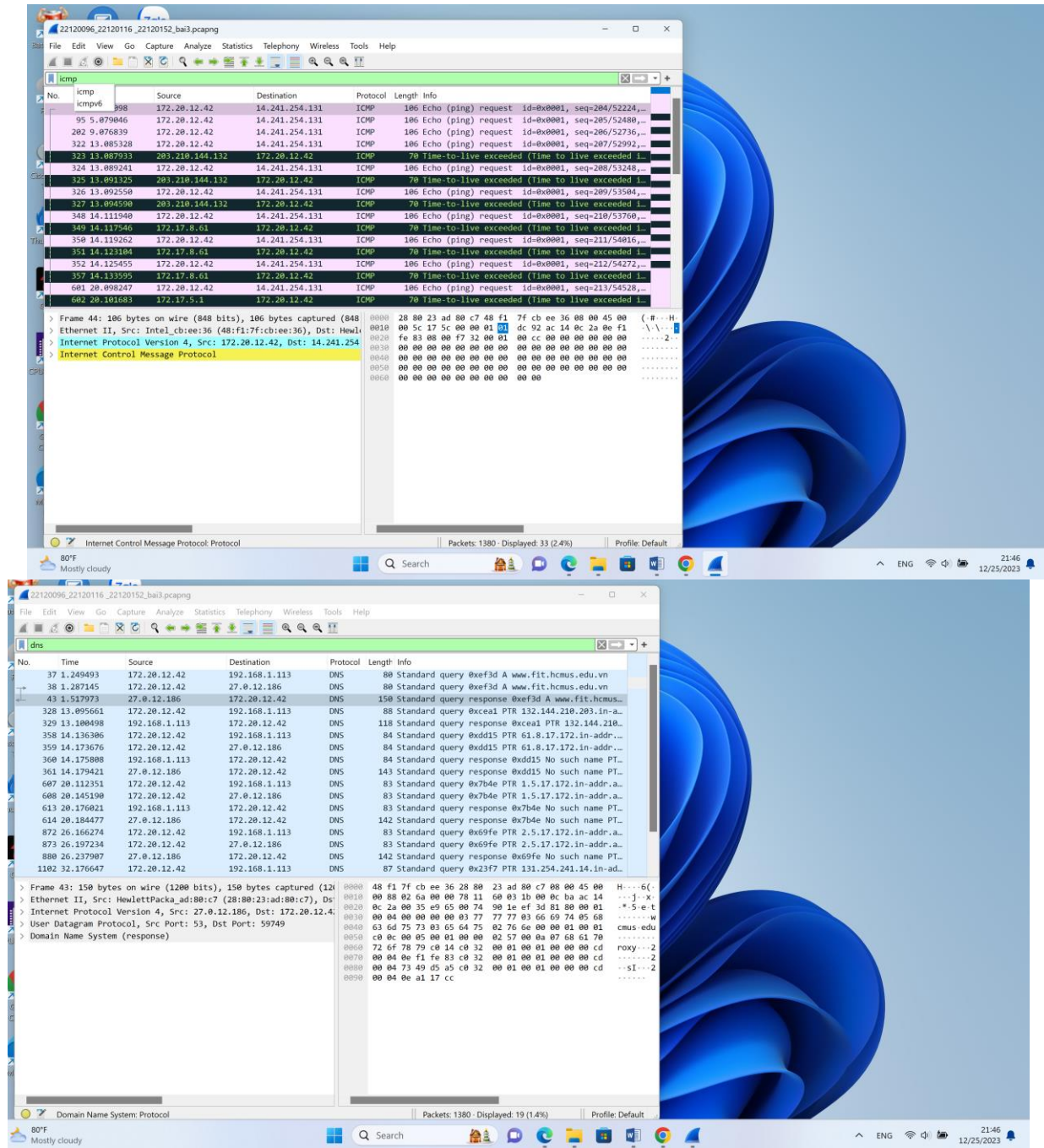
v. *Dựa trên nội dung gói pcap, hãy vẽ sơ đồ logic của đường mạng.*

3. Bài 3.

vi. *Chụp hình kết quả bắt gói tin sau khi traceroute hoặc tracert (thấy được những gói tin liên quan)*

Các hình ảnh liên quan đến các gói tin bắt được:





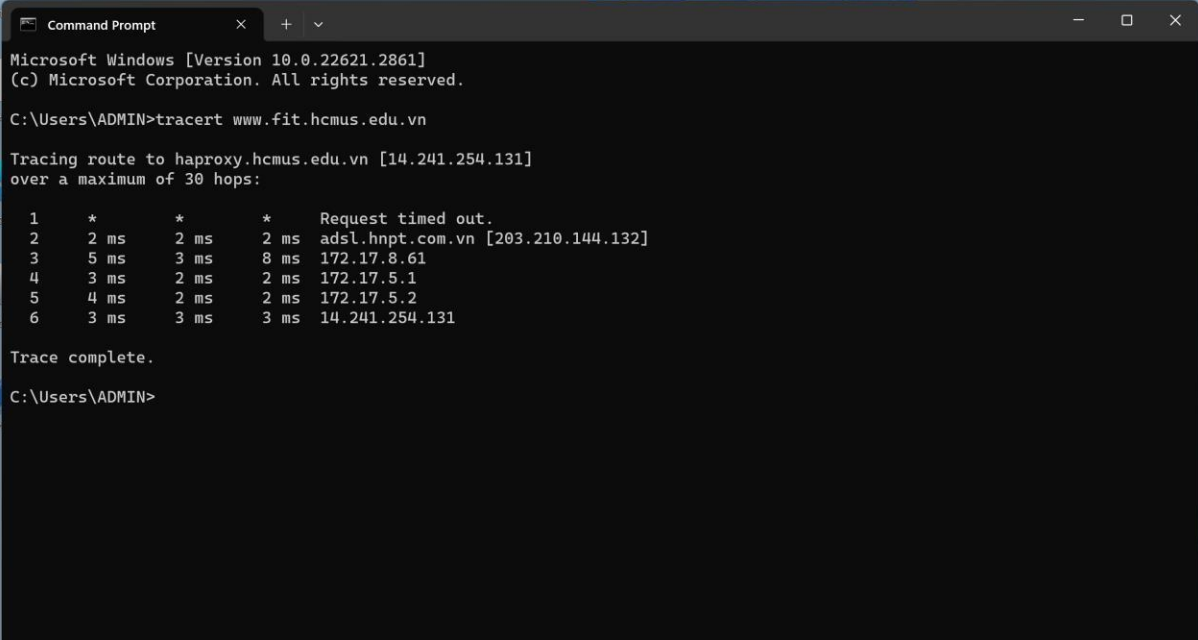
### vii. Cho biết chức năng của lệnh traceroute/tracert?

Chức năng của lệnh tracert:

Tracert là công cụ dòng lệnh kiểm tra đường đi của gói tin từ nguồn (source) đến đích (destination) của giao thức IP.

Bằng cách hoạt động gửi thông báo Echo request ICMP (Internet Control Message Protocol) tới từng đích. Sau mỗi lần gặp 1 đích, giá trị Time to live (TTL), tức thời gian cần gửi đi sẽ tăng lên cho tới khi gặp đúng đích. Đường đi được xác định từ quá trình này





```
Microsoft Windows [Version 10.0.22621.2861]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ADMIN>tracert www.fit.hcmus.edu.vn

Tracing route to haproxy.hcmus.edu.vn [14.241.254.131]
over a maximum of 30 hops:

  1  *      *      *      Request timed out.
  2  2 ms   2 ms   2 ms   adsl.hnpt.com.vn [203.210.144.132]
  3  5 ms   3 ms   8 ms   172.17.8.61
  4  3 ms   2 ms   2 ms   172.17.5.1
  5  4 ms   2 ms   2 ms   172.17.5.2
  6  3 ms   3 ms   3 ms   14.241.254.131

Trace complete.

C:\Users\ADMIN>
```

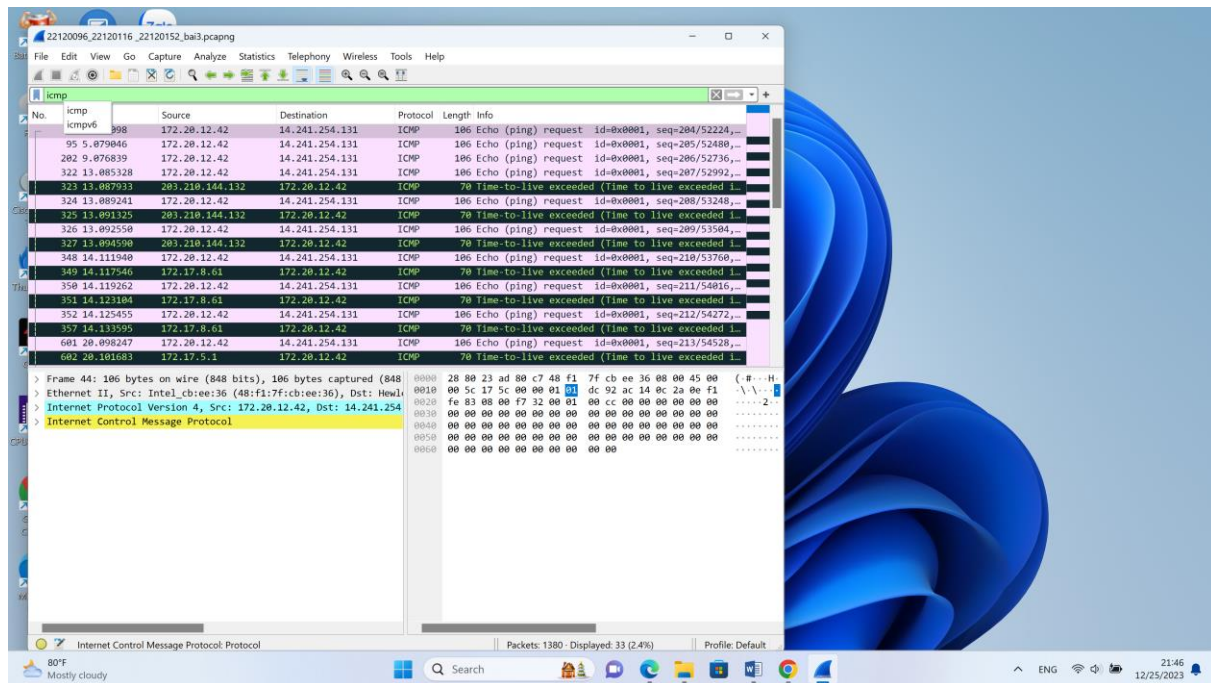
Đọc report của tracert:

- + 1 hàng thể hiện thông tin 1 hop
- + Cột số ngoài cùng bên trái liệt kê thứ tự các router mà gói tin đi qua
- + Cột ngoài cùng bên phải thể hiện tên miền của router và địa chỉ IP tương ứng
- + 3 cột ở giữa thể hiện thời gian gửi các packet ICMP đến router và ngược lại
- + Dấu hoa thị “\*”: Request time out, điều này cho thấy router mà nó tiếp cận đã được cấu hình để từ chối các packet ICMP

*viii. Cho biết địa chỉ IP của máy gửi request?*

IP của máy gửi request: 172.20.12.42

Ta có thể kiểm tra bằng cách:



Dựa vào kết quả các gói tin bắt được bằng ICMP ta có thể thấy gói tin đầu tiên( No. 44) bắt được có source IP là: 172.20.12.42. Đối chiếu lại với IPv4 của máy tính bằng lệnh ipconfig theo bảng sau:

#### Wireless LAN adapter Wi-Fi:

```

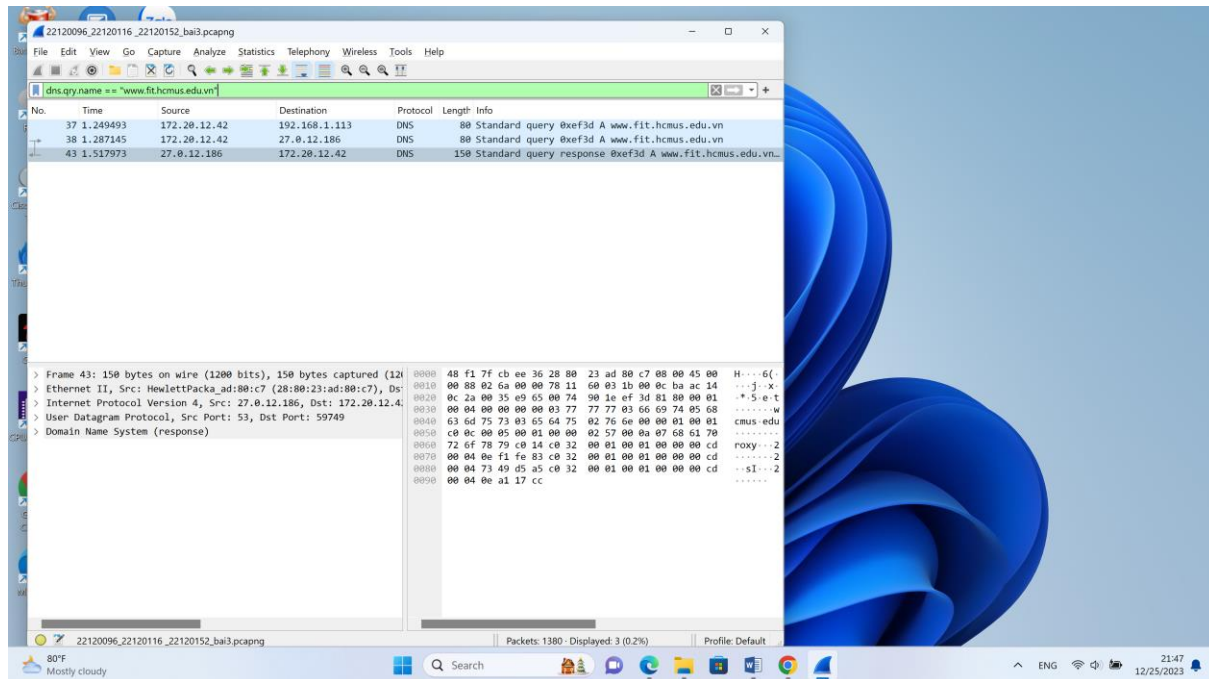
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::ab61:65da:9e56:877e%27
IPv4 Address. . . . . : 172.20.12.42
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.20.0.1

```

Ở đây IPv4 là: 172.20.12.42, hoàn toàn trùng khớp. Do đó, IP máy gửi request là IP của máy thực hiện lệnh tracert.

- ix. *Quan sát và chỉ rõ những gói tin dùng xác định địa chỉ IP của FIT từ tên miền trong danh sách các gói tin bắt được. Cho biết các gói tin này dùng giao thức gì tại tầng ứng dụng trong mô hình TCP/IP*

Trên thanh filter của wireshark sử dụng lệnh dns.qry.name=="www.fit.hcmus.edu.vn" ta được kết quả dưới đây:



Trong đó, 2 gói tin đầu xác định địa chỉ IP của FIT từ tên miền trong danh sách các gói tin bắt được và gói tin thứ 3 là gói tin phản hồi.

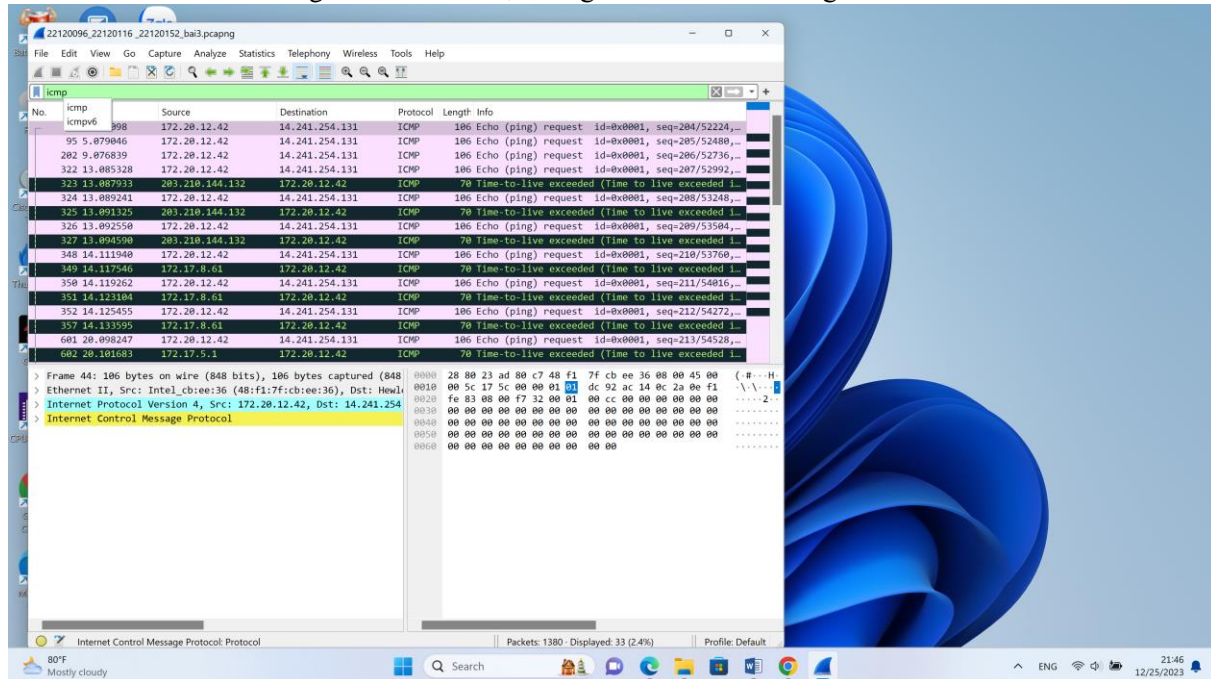
Kiểm tra gói tin đầu tiên bắt được tại mục Internet Protocol Version 4:

Ta có thể thấy giao thức được sử dụng là: DNS

x. **Câu 5:**

a. Protocol được sử dụng của những gói tin sau đó là gì?

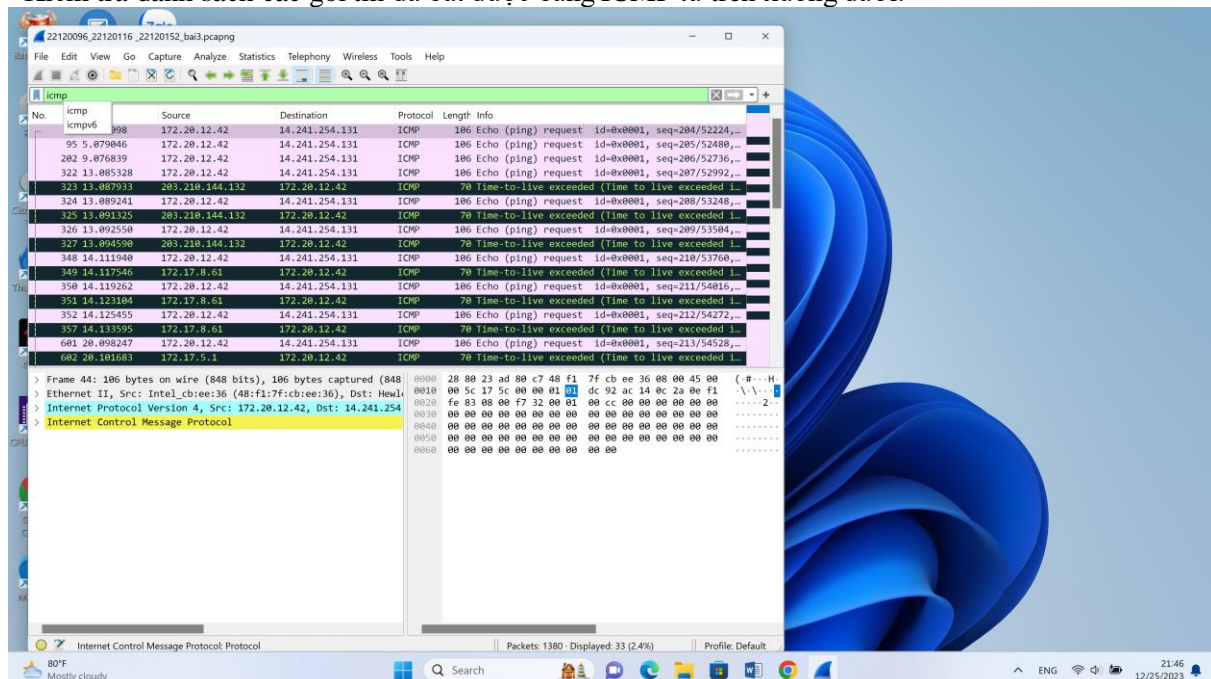
Kiểm tra danh sách các gói tin đã bắt được bằng ICMP từ trên xuống dưới:



Giao thức được sử dụng là: ICMP

b. Có bao nhiêu gói tin được gửi đi (request) trước khi nhận được response đầu tiên trả lời cho những request? (Hay nói một cách khác là: lệnh trace\* sẽ gửi request message đi, và nhận về response. Vậy có bao nhiêu gói tin request đã gửi đi đến khi nhận được gói tin response đầu tiên?)

Kiểm tra danh sách các gói tin đã bắt được bằng ICMP từ trên xuống dưới:





Ta có thể thấy gói tin có No.1097 là gói có info chưa reply đầu tiên: Nghĩa là đây là gói tin response đầu tiên. Do đó, ta sẽ đếm số gói tin từ đầu đến trước gói tin này( bao gồm các gói tin được tô đen là các gói tin đã bị mất đi trong lúc truyền)

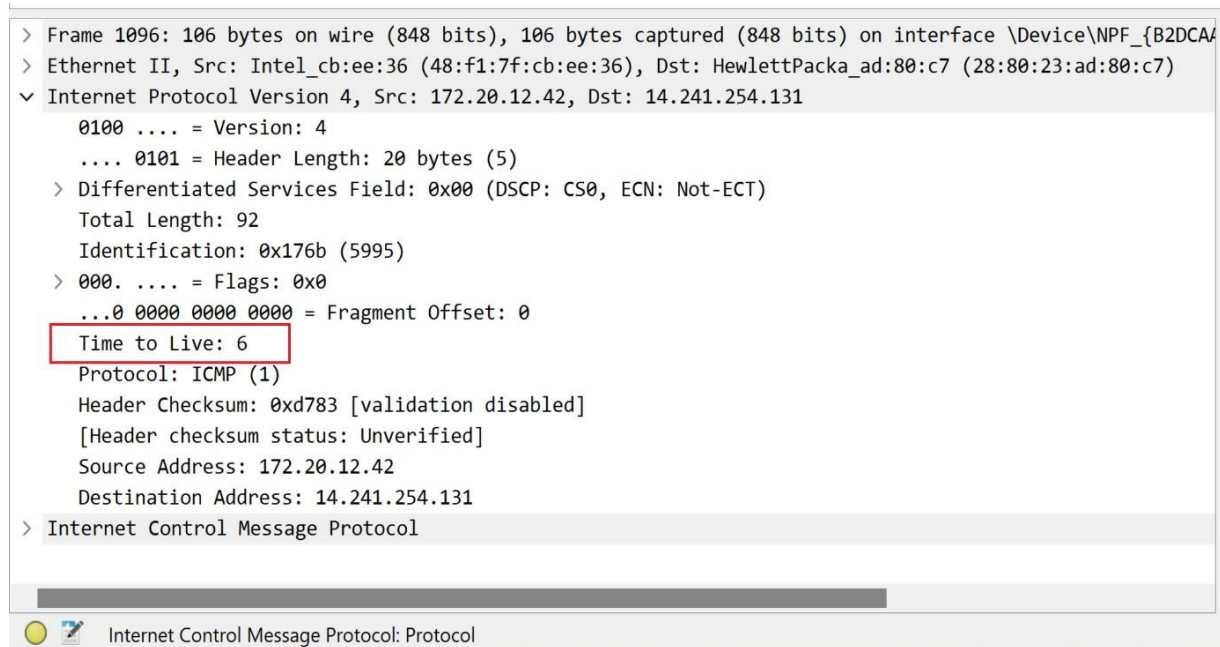
Có tổng cộng: 28 gói tin

c. Cho biết TTL của gói tin cuối cùng được gửi trước khi nhận được gói tin response đầu tiên trả lời cho những gói tin request?

Trên thanh filter chuyển sang ICMP

1096	32.159382	172.20.12.42	14.241.254.131	ICMP	106 Echo (ping) request	id=0x0001, seq=219/56064, ttl=6 (reply in 1097)
1097	32.162772	14.241.254.131	172.20.12.42	ICMP	106 Echo (ping) reply	id=0x0001, seq=219/56064, ttl=59 (request in 1096)

Gói tin có No. 1097 là gói tin response đầu tiên do đó gói tin No.1096 là gói tin request cuối cùng trước khi nhận được response đầu tiên, ta kiểm tra gói tin đó:



Thấy được TTL của gói tin là: 6

d. Bạn có thấy thông tin port trong các gói tin gửi đi? Nếu có bạn nhận thấy port nguồn/đích của gói tin có gì đặc biệt? Nếu không thấy thông tin port, hãy giải thích nguyên nhân?

Các gói tin không có port, vì các gói tin gửi bằng giao thức ICMP ở tầng Network, do đó các gói tin này không có port

e. Gói tin response đầu tiên là trả lời cho gói tin request thứ mấy? (No.)

871	26.164637	172.17.5.2	172.20.12.42	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1096	32.159382	172.20.12.42	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=219/56064, ttl=6 (reply in 1097)
1097	32.162772	14.241.254.131	172.20.12.42	ICMP	106 Echo (ping) reply id=0x0001, seq=219/56064, ttl=59 (request in 1096)

Dựa vào thông tin gói tin reply đầu tiên, ta có thể thấy dòng request in 1096 tức là gói tin này trả lời cho gói tin có No. là 1096 là gói tin ở trên