



TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN - ĐHQG TP.HCM  
VNUHCM - UNIVERSITY OF SCIENCE

## KHOA CÔNG NGHỆ THÔNG TIN

### **ĐỒ ÁN THỰC HÀNH MẠNG MÁY TÍNH:**

### **WIRESHARK**

MÃ MÔN HỌC: CSC-10008\_21CLC04  
THỰC HIỆN: Nhóm 18, Lớp 21CLC04  
GVHD: **Đỗ Hoàng Cường**  
**Nguyễn Thanh Quân**  
**Huỳnh Thùy Bảo Trân**

Tp. Hồ Chí Minh, tháng 11 năm 2022

# **BIÊN BẢN PHÂN CÔNG CÔNG VIỆC NHÓM**

## **I. Danh sách nhóm và các nhiệm vụ được phân công:**

**Tên nhóm: nhóm 18**

STT	MSSV	Họ và tên	Nhiệm vụ được phân công	Ghi chú
1	21127627	Cao Nguyễn Khánh	Bài 1 + Bài 2 (1,2,3)	
2	21127711	Trịnh Minh Trung	Bài 2 (4,5,6) + Bài 3	Nhóm trưởng
3	21127535	Thành Thiện Nhân	Bài 4	

## **II. Đánh mức độ hoàn thành:**

STT	MSSV	Họ và tên	Đánh giá chung	Mức độ hoàn thành
1	21127627	Cao Nguyễn Khánh	Hoàn thành đầy đủ	100%
2	21127711	Trịnh Minh Trung	Hoàn thành đầy đủ	100%
3	21127535	Thành Thiện Nhân	Hoàn thành đầy đủ	100%

# MỤC LỤC

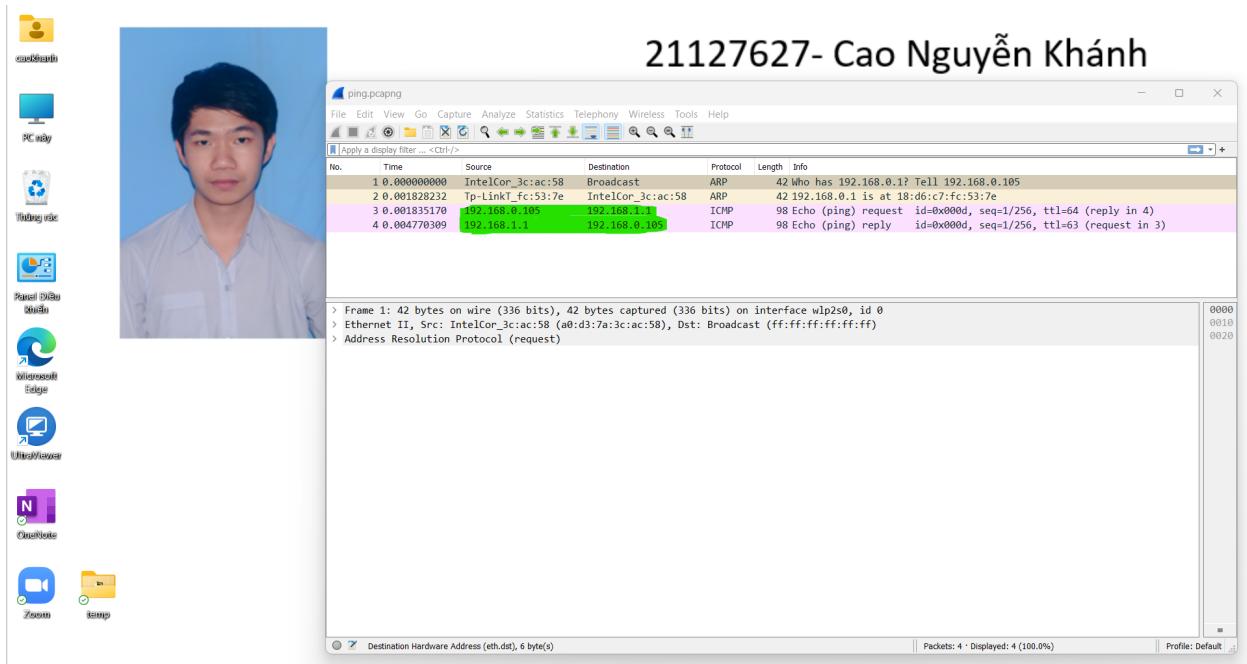
<b>Bài 1: PING</b>	<b>5</b>
1) Cho biết địa chỉ IP của host ping và host được ping?	5
2) Cho biết port được sử dụng là bao nhiêu? Nếu không có port thì giải thích tại sao?	5
3) Với gói tin ICMP request:	6
a. Cho biết kích thước (bytes) của từng phần trong diagram	6
b. Cho biết có bao nhiêu gói tin ARP? Giải thích tại sao lại có các gói tin ARP này, nếu ý nghĩa của các gói tin đó.	7
c. Dựa trên nội dung gói pcap, hãy vẽ sơ đồ logic của đường mạng	9
<b>Bài 2: UDP</b>	<b>9</b>
1) Câu lệnh “nslookup” trên có ý nghĩa gì?, trong phần trả lời trên màn hình dòng lệnh có dòng “Non-authoritative answer” có ý nghĩa gì?	9
2) Hãy cho biết có bao nhiêu trường thông tin trong phần header của gói tin UDP? Kể tên các trường thông tin trên, xác định kích thước của từng trường (bytes)	9
3) Hãy cho biết giá trị trong trường Length là bao nhiêu? đơn vị là gì? và trường này đang nói đến kích thước gì?	10
4) Protocol number của UDP là gì? (trả lời dưới dạng hexadecimal và decimal)	10
5) Lượng dữ liệu tối đa có thể đưa vào UDP Payload là bao nhiêu Bytes? (ghi công thức tính rõ ràng để ra được kết quả)	11
6) Hãy cho biết mối quan hệ giữa port number trong những gói tin lọc được	11
<b>Bài 3: HTTP</b>	<b>11</b>
1) Hãy cho biết địa chỉ IP của máy chủ gaia.cs.umass.edu. Port dịch vụ được máy chủ sử dụng để gửi và nhận các gói tin TCP segment là bao nhiêu?	11
2) Tìm 7 TCP segments tiếp theo, tính từ TCP segment của HTTP POST đầu tiên của câu 2	12
a. Cho biết No. của 7 TCP segment đó	12
b. Cho biết sequence number của 7 TCP segment đó	13
c. Cho biết No. của ACK báo nhận của 7 TCP segment đó	14
d. Lượng data gửi trong mỗi TCP segment đó	15
3) Cho biết throughput (byte transferred per unit time) cho kết nối upload file này, vui lòng cho biết cách tính	16

4) Vẽ quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (có ghi rõ SEQ number, ACK number của từng segment), dùng chức năng Flow Graph trong Wireshark nhưng yêu cầu chỉ vẽ giữa máy bạn và web server, không có những traffic ngoài luồng trong hình vẽ 19

<b>Bài 4: Traceroute</b>	<b>23</b>
1) Chụp hình kết quả bắt gói tin sau khi traceroute hoặc tracert (thấy được những gói tin liên quan)	23
2) Cho biết traceroute/tracert dùng để làm gì?	24
3) Cho biết địa chỉ IP của máy gửi request?	24
4) Cho biết cách máy tính xác định được địa chỉ IP của FIT	25
5) Sau khi xác định được IP của www.fit.hcmus.edu.vn, máy sẽ bắt đầu gửi gói tin đến FIT	26
a) Protocol được sử dụng của những gói tin sau đó là gì?	26
b) Có bao nhiêu gói tin được gửi đi (request) trước khi nhận được phản hồi đầu tiên cho những request?	27
c) Cho biết TTL của gói tin cuối cùng được gửi trước khi nhận được gói tin phản hồi đầu tiên cho những gói tin request?	28
d) Bạn có thấy thông tin port trong các gói tin gửi đi? Nếu có bạn nhận thấy port nguồn/dích của gói tin có gì đặc biệt? Nếu không thấy thông tin port, hãy giải thích nguyên nhân?	28
e) Gói tin phản hồi đầu tiên là trả lời cho gói tin request thứ mấy? (No.)	28

## Bài 1: PING

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



Host ping : 192.168.0.105

Host được ping: 192.168.1.1

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

- Không có port.
- Vì ICMP nằm ở tầng Network. ICMP nằm trong gói IP và nó không chứa header của tầng Application (Trong khi đó Source Port và Destination Port được thêm vào phần header ở tầng Application).

### 3) Với gói tin ICMP request:

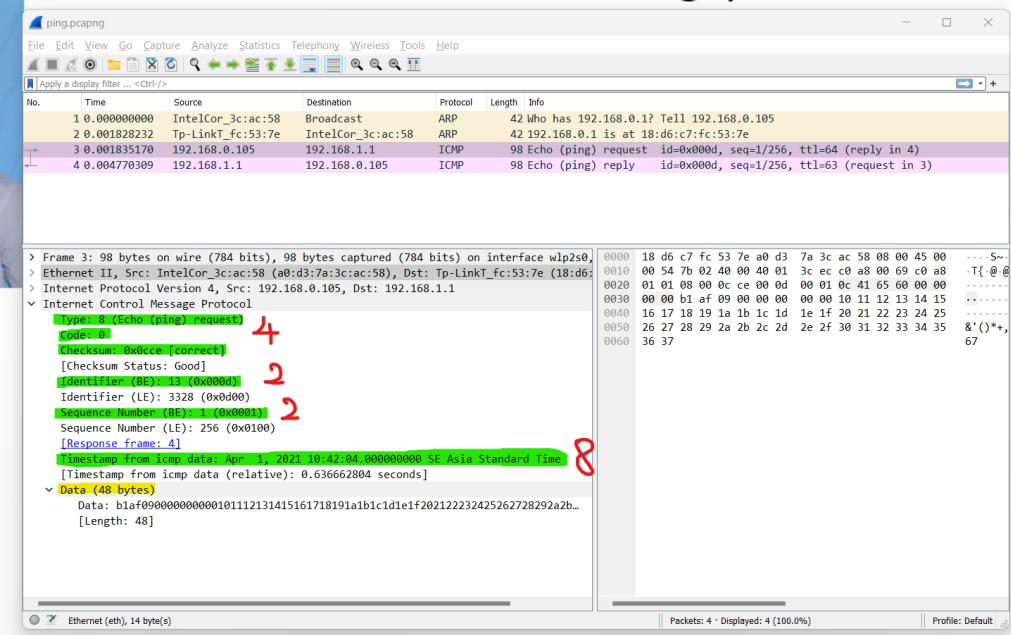
- a. Cho biết kích thước (bytes) của từng phần trong diagram

ICMP data = 48 bytes

ICMP header= 16 bytes



21127627- Cao Nguyễn Khánh

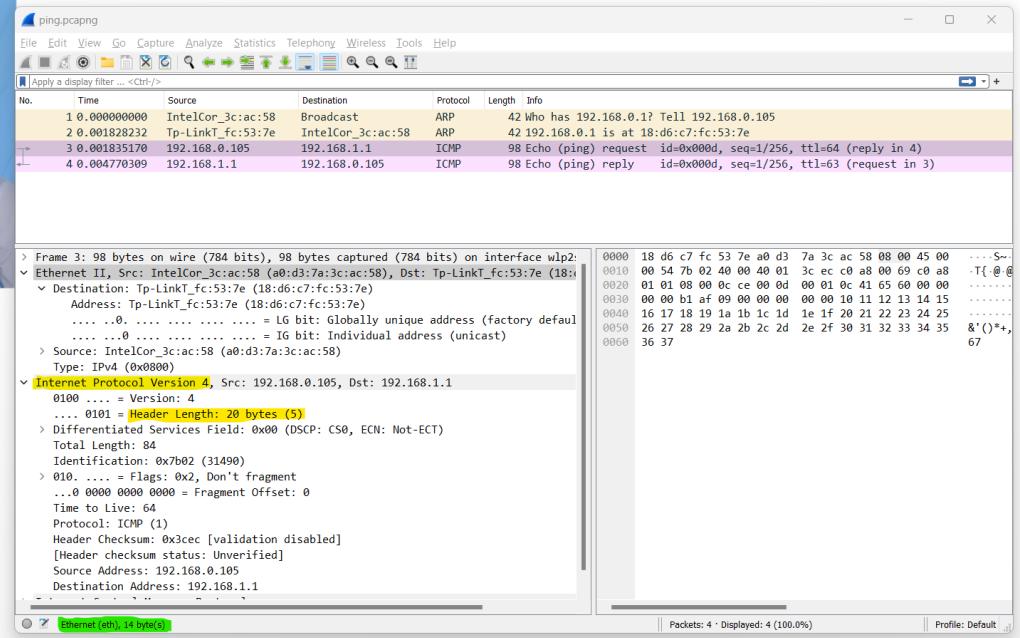


IP header= 20 bytes

Ethernet header = 14 bytes



21127627- Cao Nguyễn Khánh

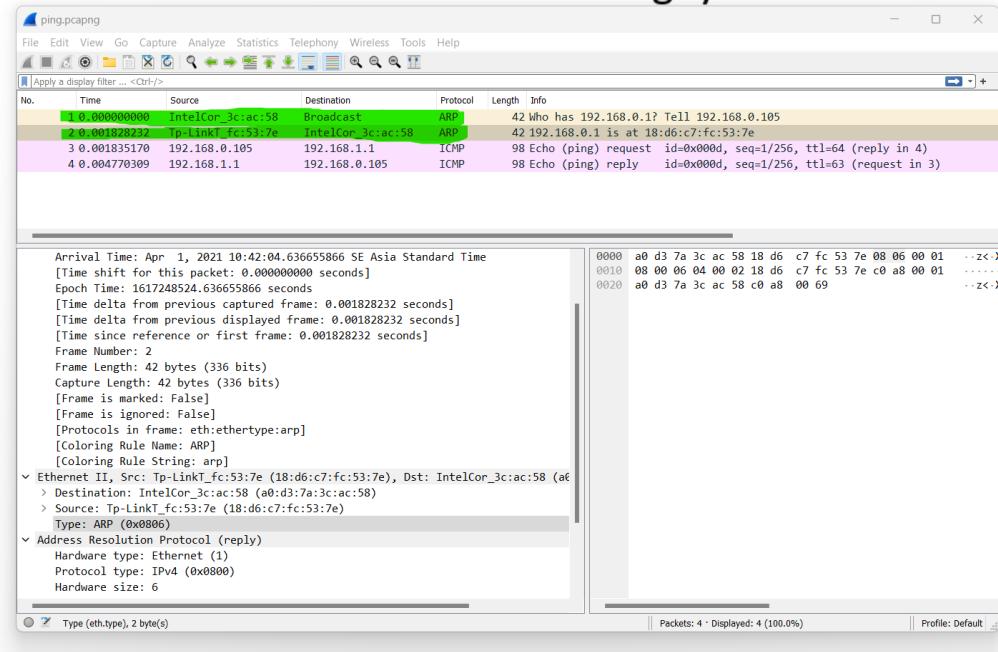


b. Cho biết có bao nhiêu gói tin ARP? Giải thích tại sao lại có các gói tin ARP này, nêu ý nghĩa của các gói tin đó.

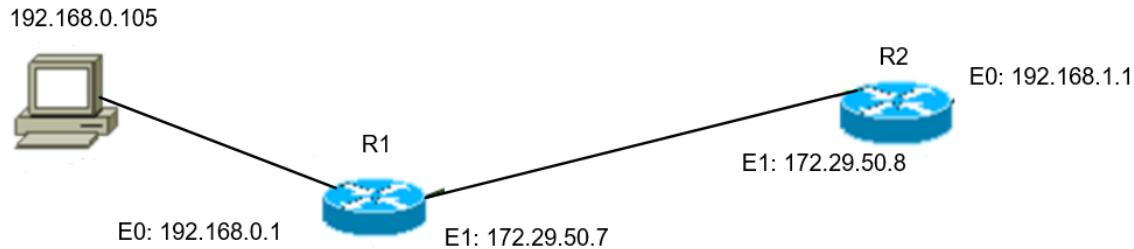
- Có 2 gói tin ARP trong file ping.pcapng
- Thiết bị gửi sử dụng ARP để có thể dịch địa chỉ IP sang địa chỉ MAC. Thiết bị sẽ gửi một request ARP đã chứa địa chỉ IP của thiết bị nhận. Tất cả thiết bị trên đoạn local network sẽ nhìn thấy thông điệp này. Tuy nhiên, chỉ thiết bị có địa chỉ IP chứa trong request mới có thể phản hồi lại với thông điệp mà chứa địa chỉ MAC của nó. Thiết bị gửi khi đó sẽ có đầy đủ các thông tin để gửi packet tới thiết bị nhận.



21127627- Cao Nguyễn Khanh



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



## Bài 2: UDP

1) Câu lệnh “nslookup” trên có ý nghĩa gì?, trong phần trả lời trên màn hình dòng lệnh có dòng "Non-authoritative answer" có ý nghĩa gì?

- Nslookup có ý nghĩa là giúp chúng ta tìm thấy thông tin máy chủ tên cho các tên miền bằng cách truy vấn hệ thống tên miền (DNS).
- Trong DNS, cái gọi là " non-authoritative answer "( câu trả lời không có thẩm quyền) đề cập đến các bản ghi DNS được lưu giữ trên các máy chủ DNS của bên thứ ba mà chúng thu được từ các máy chủ "authoritative answer " (có thẩm quyền )cung cấp nguồn dữ liệu gốc.

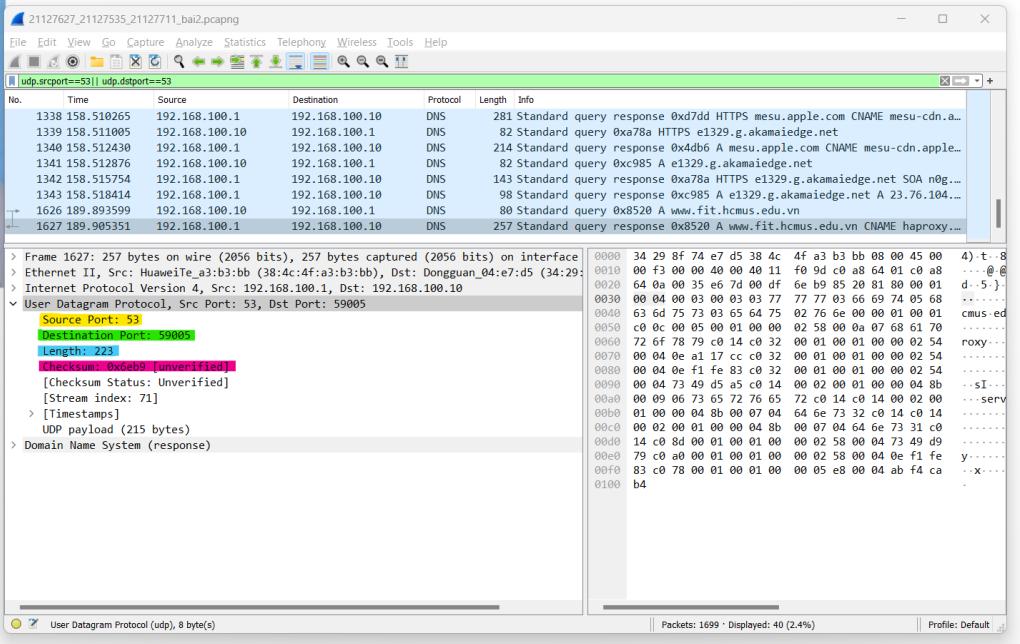
2) Hãy cho biết có bao nhiêu trường thông tin trong phần header của gói tin UDP? Kể tên các trường thông tin trên, xác định kích thước của từng trường (bytes)

Các trường thông tin trong phần header của gói tin UDP.

- Source port: 2 bytes
- Destination port: 2 bytes
- Length: 2 bytes
- Checksum: 2 bytes



21127627- Cao Nguyễn Khánh



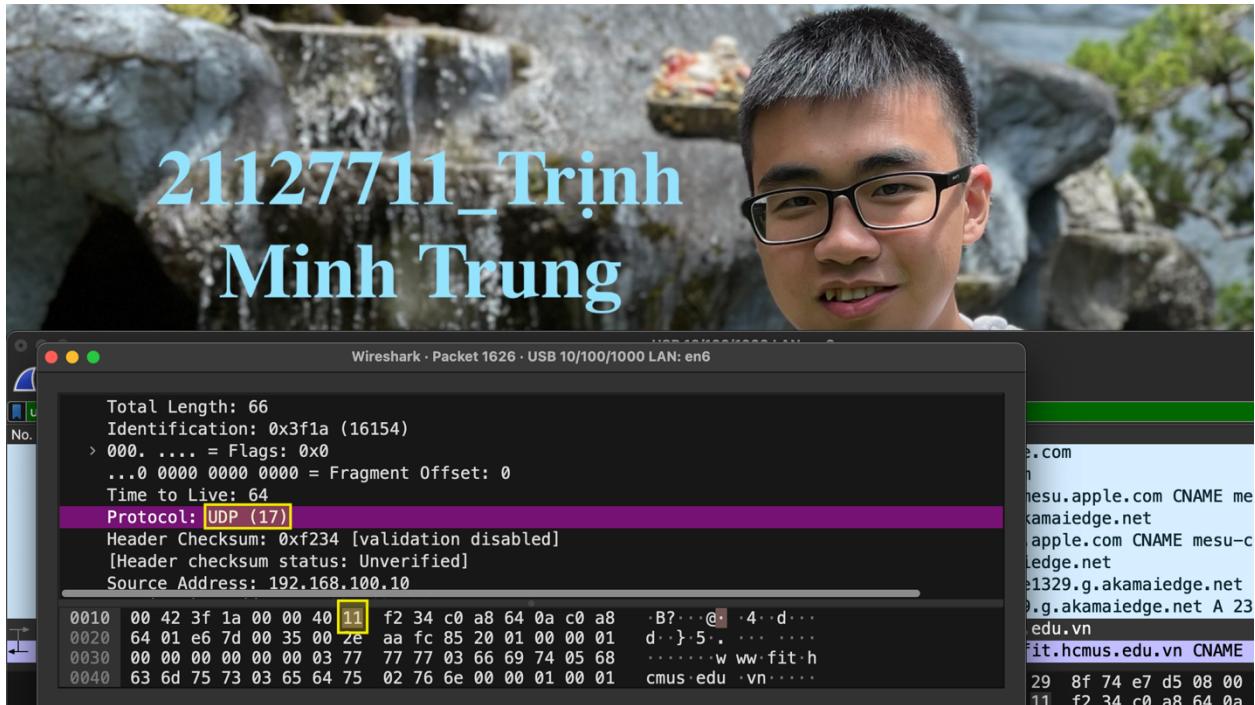
3) Hãy cho biết giá trị trong trường Length là bao nhiêu? đơn vị là gì? và trường này đang nói đến kích thước gì?

Giá trị trong trường length = 223. Trường này đang nói về độ dài của = UDP header + data.

4) Protocol number của UDP là gì? (trả lời dưới dạng hexadecimal và decimal)

Protocol number của UDP:

- Dưới dạng decimal là 17.
- Dưới dạng hexadecimal là 0x11.



5) Lượng dữ liệu tối đa có thể đưa vào UDP Payload là bao nhiêu Bytes? (ghi công thức tính rõ ràng để ra được kết quả)

Lượng dữ liệu tối đa có thể đưa vào UDP Payload là: 65527 (bytes)

$$\begin{aligned} \text{UDP Payload Max} &= \text{Header Length Max} - \text{Packet Header Byte} \\ &= (2^{16} - 1) - 8 = 65535 - 8 = 65527 \text{ (bytes)} \end{aligned}$$

6) Hãy cho biết mối quan hệ giữa port number trong những gói tin lọc được

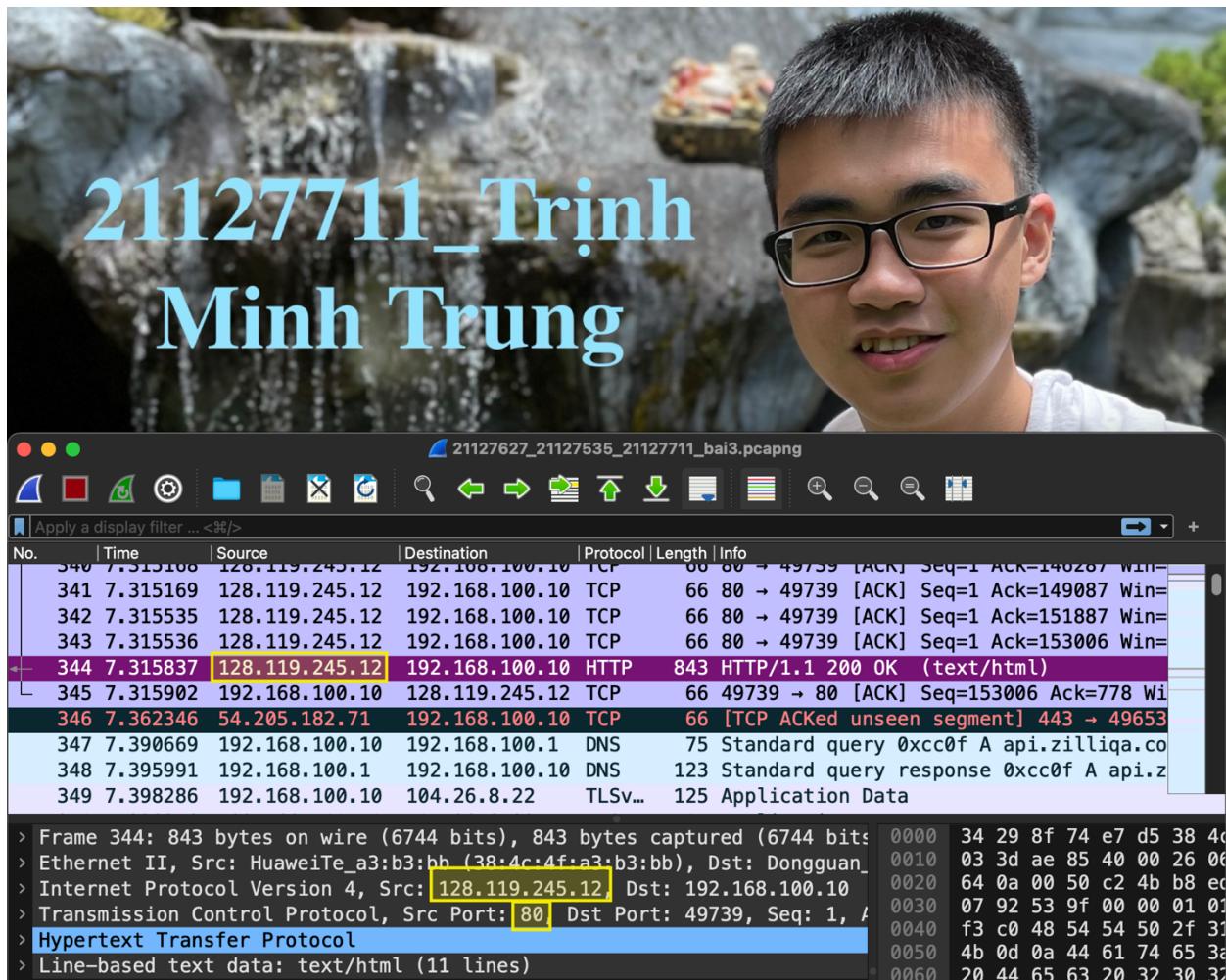
Trong 2 gói tin lọc được, Source port của gói tin gửi đi cũng là Destination port của gói tin phản hồi, ngược lại, Source port của gói tin phản hồi cũng chính là Destination port của gói tin gửi đi.

### Bài 3: HTTP

1) Hãy cho biết địa chỉ IP của máy chủ gaia.cs.umass.edu. Port dịch vụ được máy chủ sử dụng để gửi và nhận các gói tin TCP segment là bao nhiêu?

Địa chỉ IP của máy chủ gaia.cs.umass.edu là: 128.119.245.12

Port dịch vụ được máy chủ sử dụng để gửi và nhận các gói tin TCP segment là: 80



2) Tìm 7 TCP segments tiếp theo, tính từ TCP segment của HTTP POST đầu tiên của câu 2

a. Cho biết No. của 7 TCP segment đó

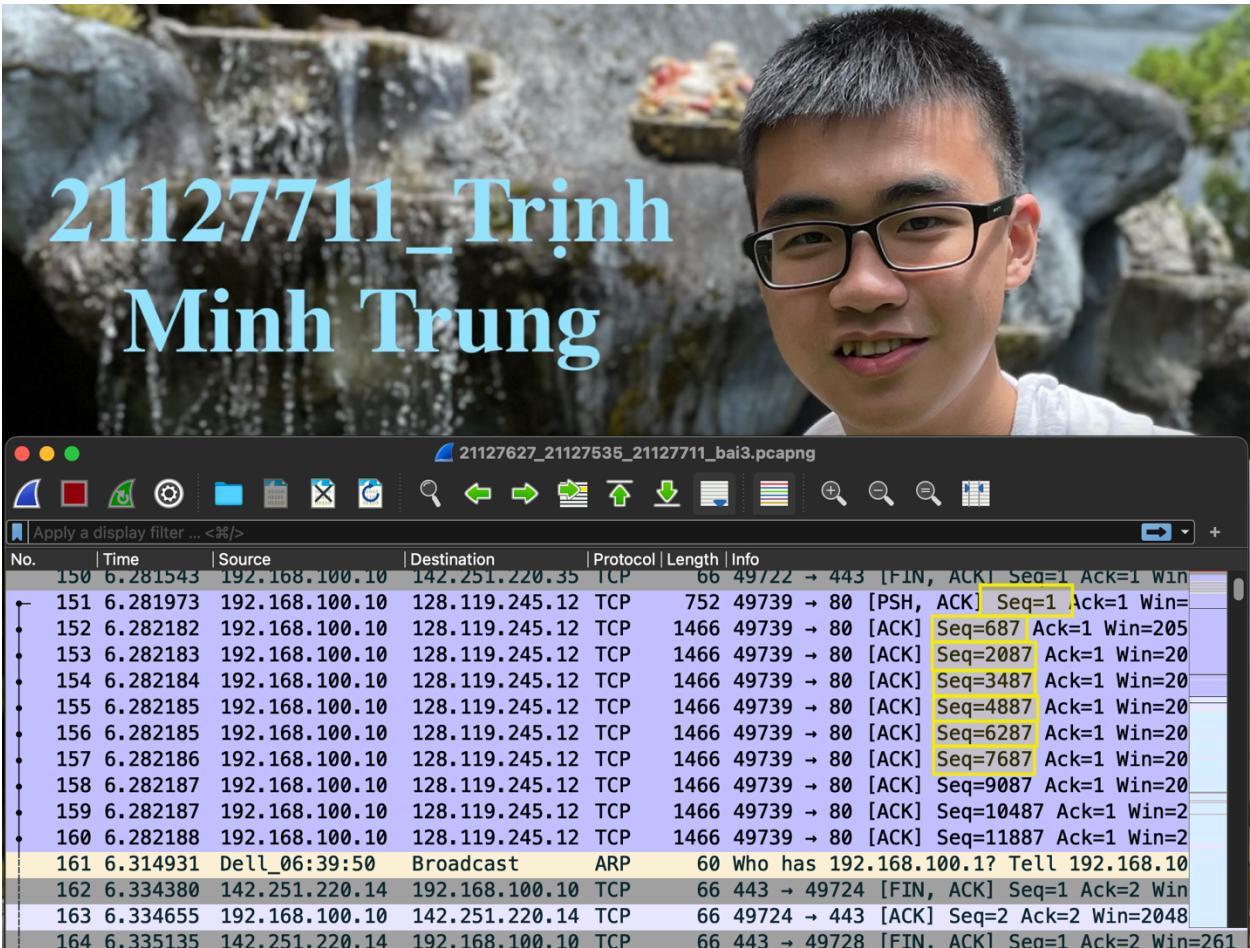
No. của 7 TCP segment tiếp theo tính từ TCP segment của HTTP POST đầu tiên là: 151, 152, 153, 154, 155, 156, 157.



No.	Time	Source	Destination	Protocol	Length	Info
308	7.056070	128.119.245.12	192.168.100.10	TCP	66 80	→ 49739 [ACK] Seq=1 Ack=
309	7.056104	192.168.100.10	128.119.245.12	HTTP	1185	POST /wireshark-labs/lab3-1
310	7.056306	128.119.245.12	192.168.100.10	TCP	66 80	→ 49739 [ACK] Seq=1 Ack=
[110 Reassembled TCP Segments (153005 bytes): #151(686), #152(1400), #153(1400), #154(1400), #155(1400), #156(1400), #157(1400), #158(1400), #159(1400), #160(1400), #184(1400), #185(1400)]						
[Frame: 151, payload: 0-685 (686 bytes)]					0000	38 4c 4
[Frame: 152, payload: 686-2085 (1400 bytes)]					0010	04 93 0
[Frame: 153, payload: 2086-3485 (1400 bytes)]					0020	f5 0c 0
[Frame: 154, payload: 3486-4885 (1400 bytes)]					0030	08 08 2
[Frame: 155, payload: 4886-6285 (1400 bytes)]					0040	4f 34 6
[Frame: 156, payload: 6286-7685 (1400 bytes)]					0050	6e 20 7
[Frame: 157, payload: 7686-9085 (1400 bytes)]					0060	74 68 6
[Frame: 158, payload: 9086-10485 (1400 bytes)]					0070	67 20 7
[Frame: 159, payload: 10486-11885 (1400 bytes)]					0080	6f 66 2
[Frame: 160, payload: 11886-13285 (1400 bytes)]					0090	68 65 2
[Frame: 184, payload: 13286-14685 (1400 bytes)]					00a0	75 70 7
[Frame: 185, payload: 14686-16085 (1400 bytes)]					00b0	20 74 6
					00c0	65 70 2
					00d0	74 68 6
					00e0	66 66 2

b. Cho biết sequence number của 7 TCP segment đó

Sequence number của 7 TCP segment ứng với từng No. là: 151 1, 152 687, 153 2087, 154 3487, 155 4887, 156 6287, 157 7687.



c. Cho biết No. của ACK báo nhận của 7 TCP segment đó

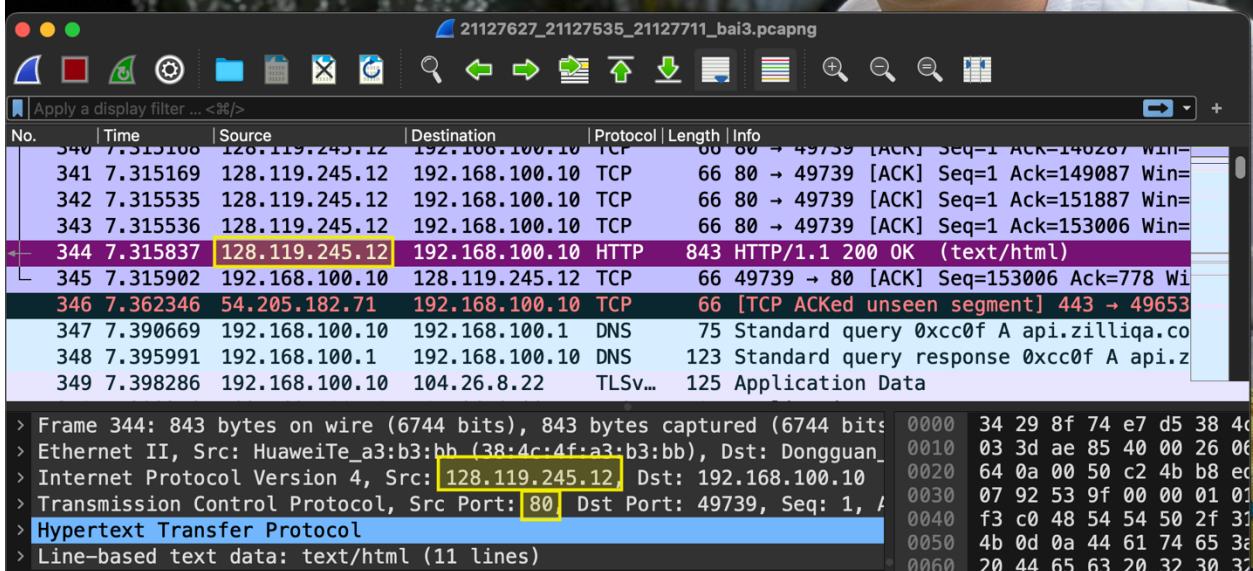
No. của ACK báo nhận của 7 TCP segment lọc được đều có giá trị là 1.



#### d. Lượng data gửi trong mỗi TCP segment đó

Lượng data gửi trong mỗi TCP segment ứng với từng No. của mỗi segment là: 151 686, 152 1400, 153 1400, 154 1400, 155 1400, 156 1400, 157 1400.

# 21127711\_Trịnh Minh Trung



3) Cho biết throughput (byte transferred per unit time) cho kết nối upload file này, vui lòng cho biết cách tính

Throughput cho kết nối upload này là: 197646.1348 (bytes)

Lượng dữ liệu được truyền đi trong kết nối này là:  $153005 - 1 = 153004$  (bytes)



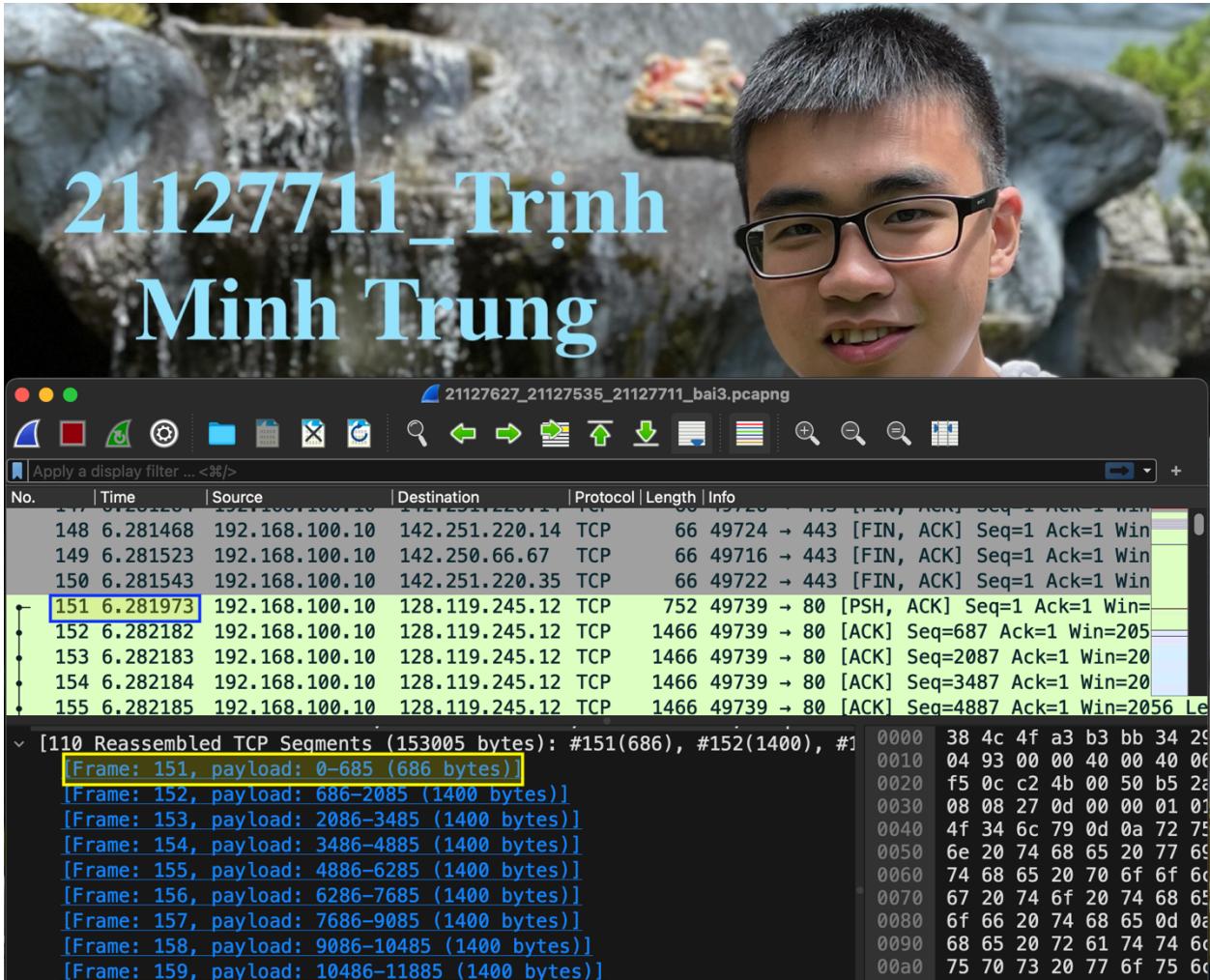
21127627_21127535_21127711_bai3.pcapng													
No.	Time	Source	Destination	Protocol	Length	Info							
308	7.056070	128.119.245.12	192.168.100.10	TCP	66	80 → 49739 [ACK]	Seq=1	Ack=74887	Win=1	...	...	...	...
309	7.056104	192.168.100.10	128.119.245.12	HTTP	1185	POST /wireshark-labs/lab3-1-reply.htm							
310	7.056306	128.119.245.12	192.168.100.10	TCP	66	80 → 49739 [ACK]	Seq=1	Ack=76287	Win=1	...	...	...	...
311	7.056482	128.119.245.12	192.168.100.10	TCP	66	80 → 49739 [ACK]	Seq=1	Ack=79087	Win=1426	...	...	...	...
> Ethernet II, Src: Dongguan_04:e7:d5 (34:29:8f:74:e7:d5), Dst: HuaweiTe_													
> Internet Protocol Version 4, Src: 192.168.100.10, Dst: 128.119.245.12													
> Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 1518													
` [110 Reassembled TCP Segments (153005 bytes): #151(686), #152(1400), #153(1400), #154(1400)]													
[Frame: 151, payload: 0-685 (686 bytes)]													
[Frame: 152, payload: 686-2085 (1400 bytes)]													
[Frame: 153, payload: 2086-3485 (1400 bytes)]													
[Frame: 154, payload: 3486-4885 (1400 bytes)]													

Thời gian phát sinh để truyền tập tin = Thời điểm gửi xong tệp tin – thời điểm bắt đầu gửi tệp tin =  $7.056104 - 6.281973 = 0.774131$  (s)

Thời điểm gửi xong tệp tin:

21127627_21127535_21127711_bai3.pcapng													
No.	Time	Source	Destination	Protocol	Length	Info							
309	7.056104	192.168.100.10	128.119.245.12	HTTP	1185	POST /wireshark-labs/lab3-1-reply.htm	HTTP/1.1	200	OK	(text/html)	...	...	...
344	7.315837	128.119.245.12	192.168.100.10	HTTP	843	HTTP/1.1	200	OK	(text/html)	...	...	...	...

Thời điểm bắt đầu gửi tệp tin:

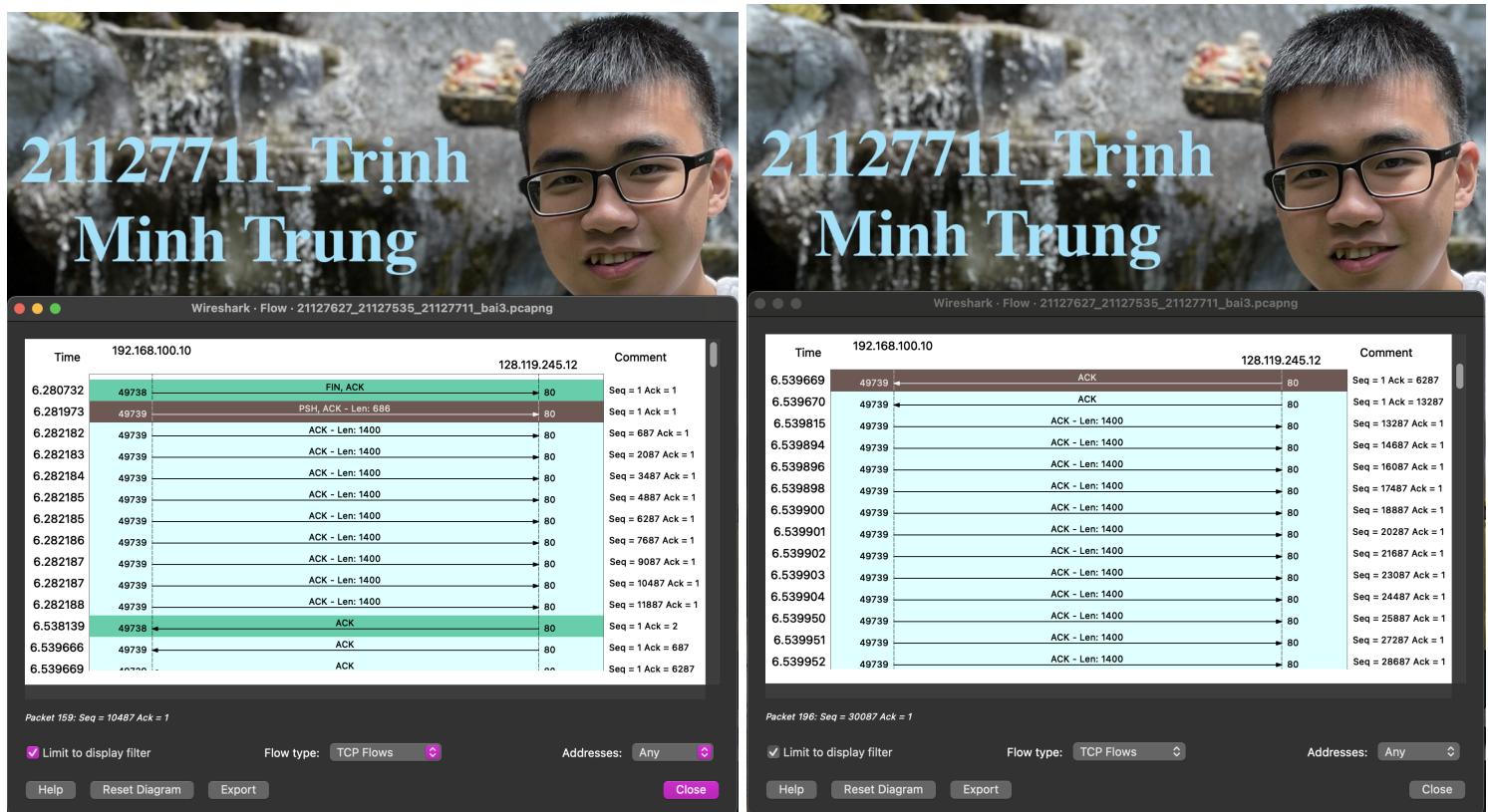


Công thức tính throughput:

$$\begin{aligned} \text{Throughput} &= \frac{\text{lượng dữ liệu được truyền đi}}{\text{thời gian phát sinh để truyền tập tin}} (\text{bytes}) \\ &= \frac{153004}{0.774131} = 197646.1348 (\text{bytes}) \end{aligned}$$

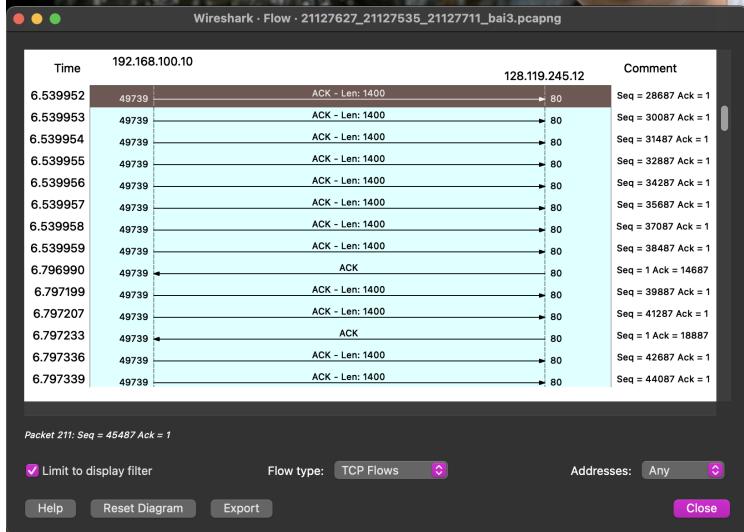
4) Vẽ quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (có ghi rõ SEQ number, ACK number của từng segment), dùng chức năng Flow Graph trong Wireshark nhưng yêu cầu chỉ vẽ giữa máy bạn và web server, không có những traffic ngoài luồng trong hình vẽ

Quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP được vẽ bằng chức năng Flow Graph như những hình sau đọc theo chiều từ trái sang phải, từ trên xuống dưới:

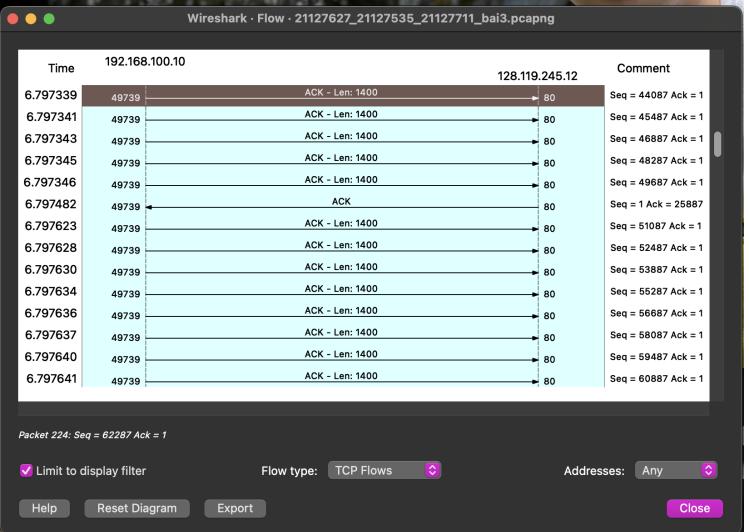




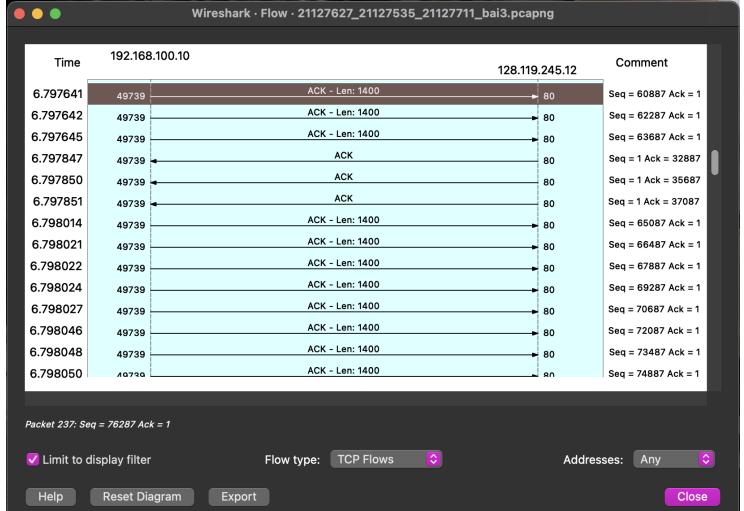
21127711\_Trịnh  
Minh Trung



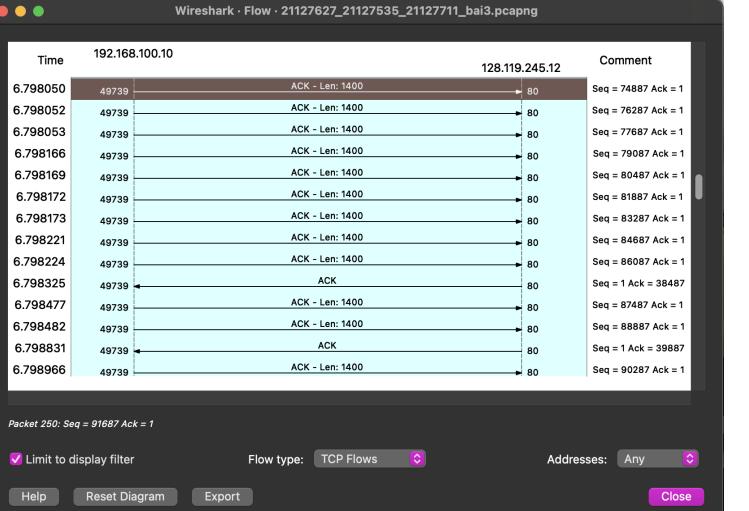
21127711\_Trịnh  
Minh Trung

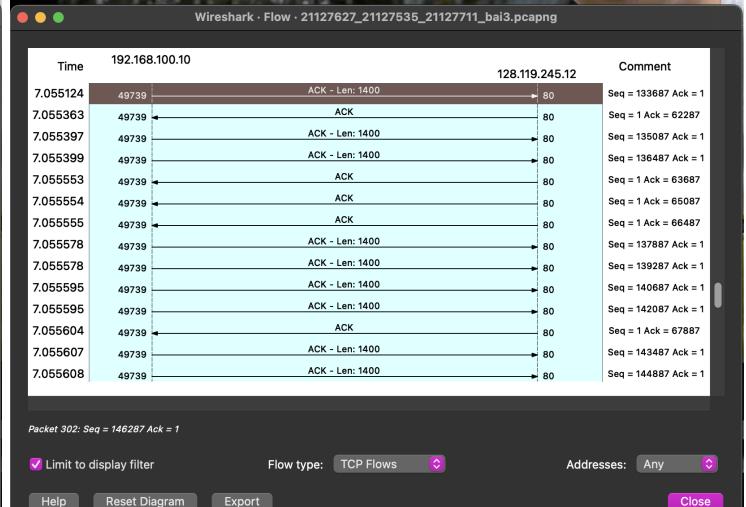
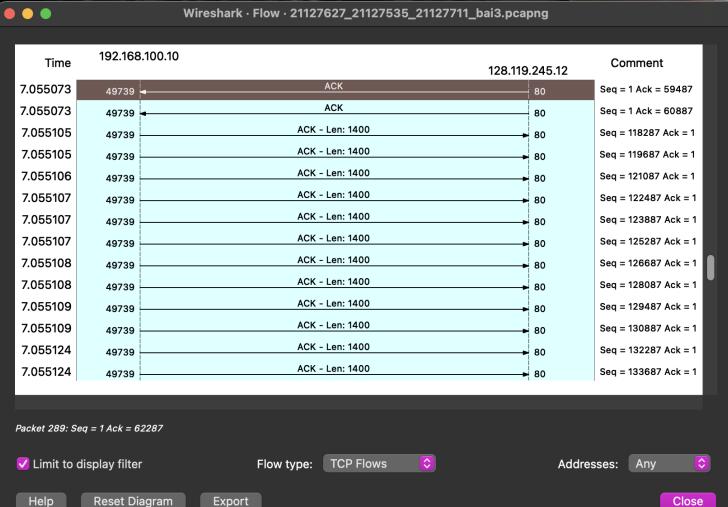
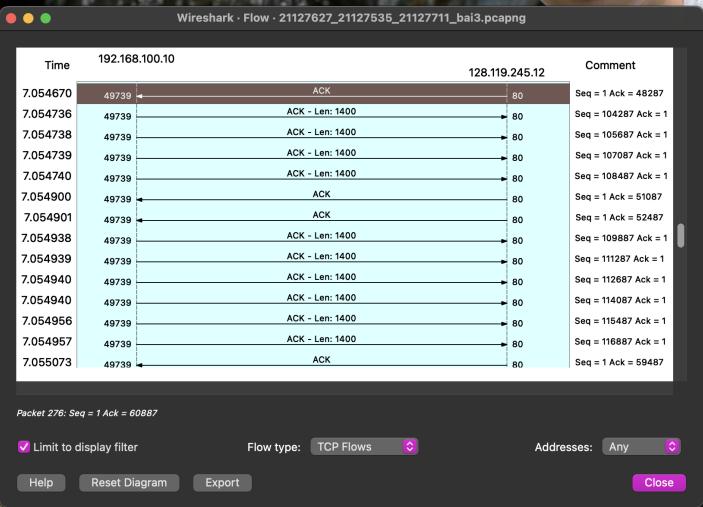
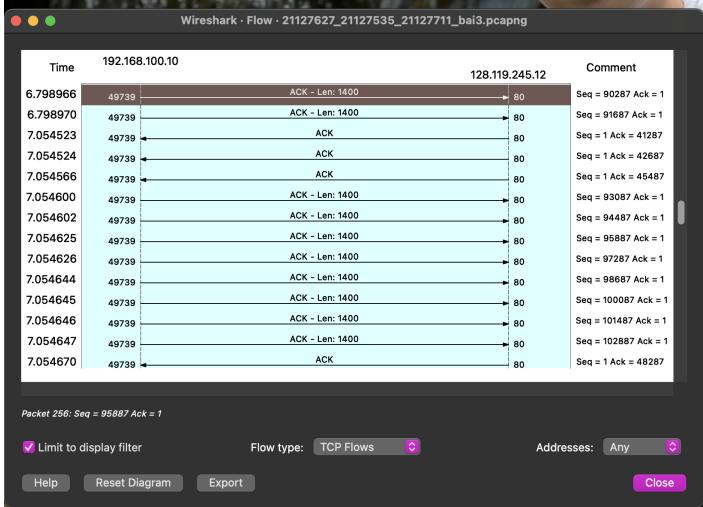


21127711\_Trịnh  
Minh Trung



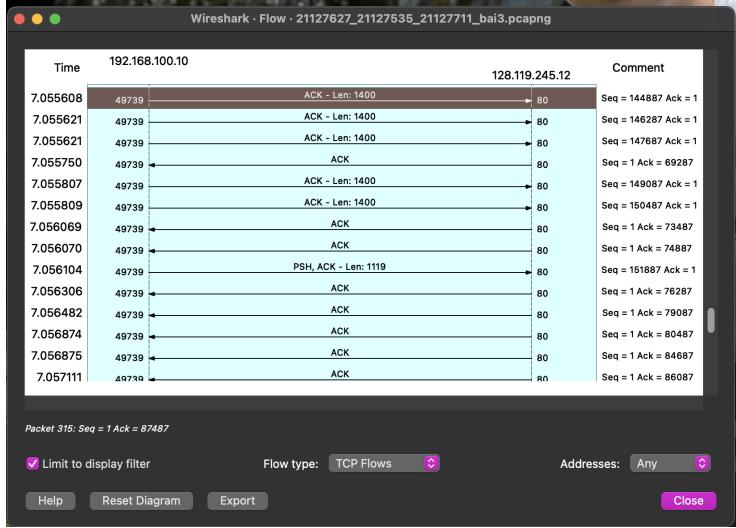
21127711\_Trịnh  
Minh Trung



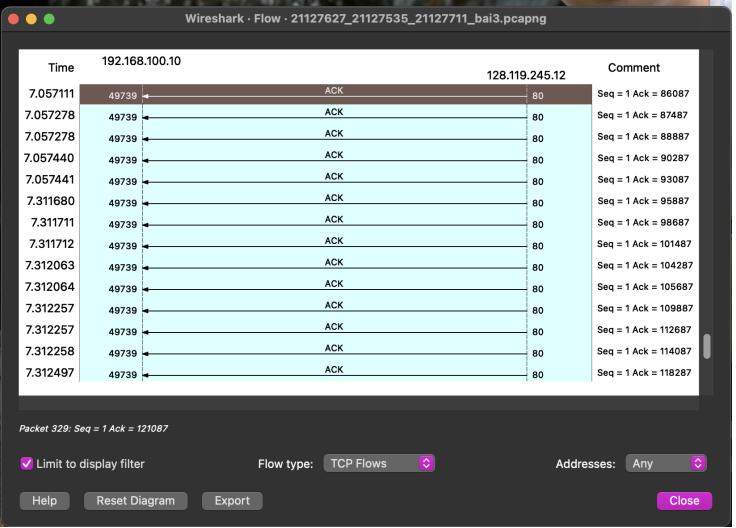




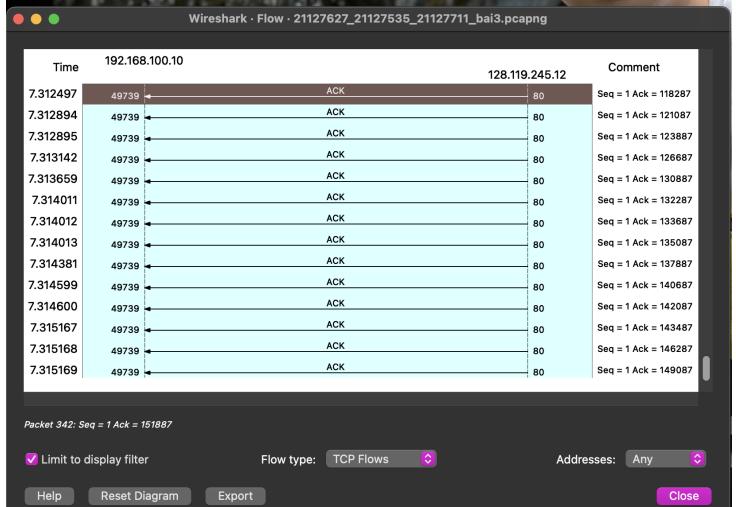
21127711\_Trịnh  
Minh Trung



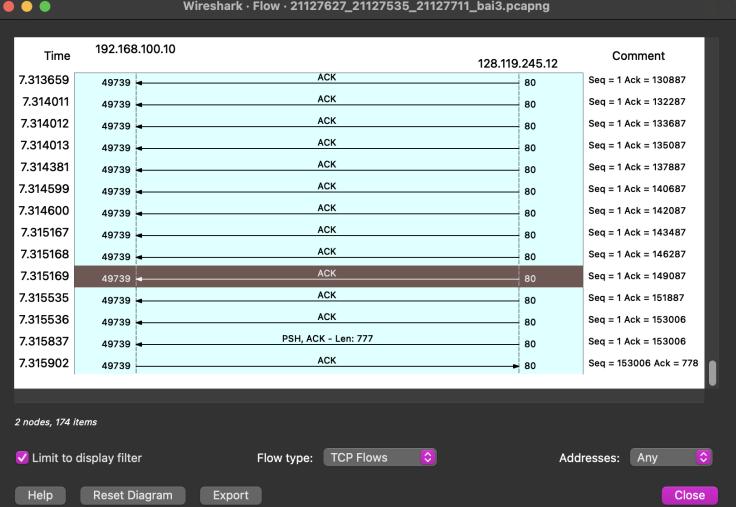
21127711\_Trịnh  
Minh Trung



21127711\_Trịnh  
Minh Trung



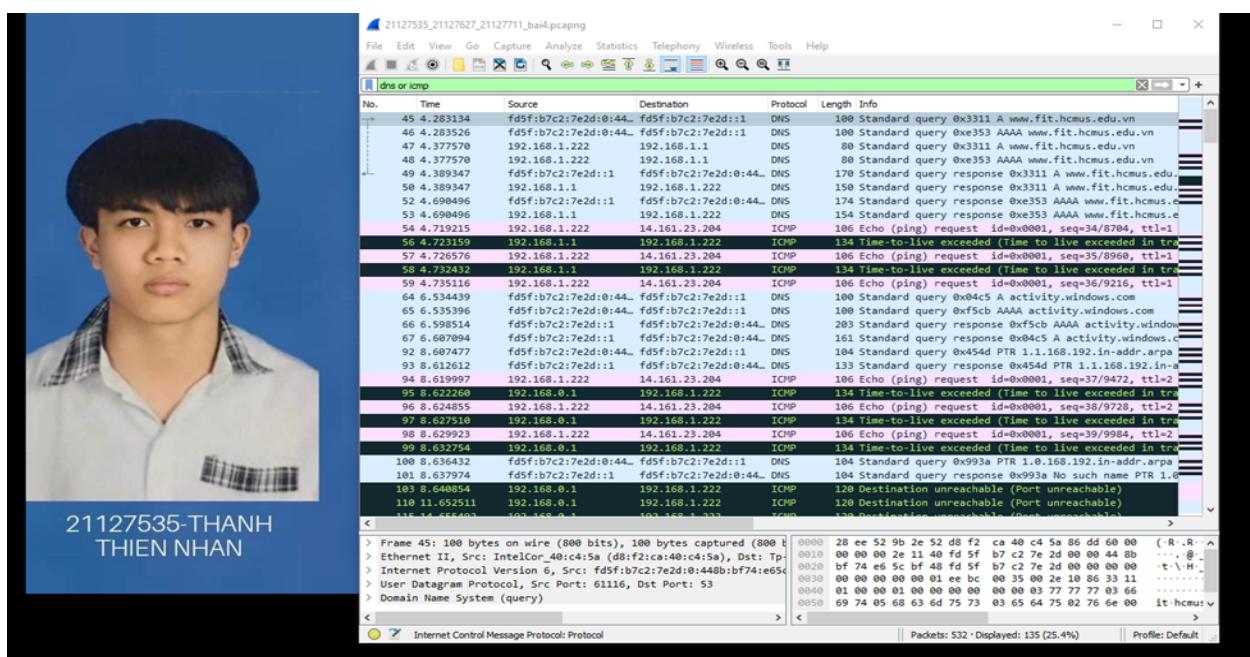
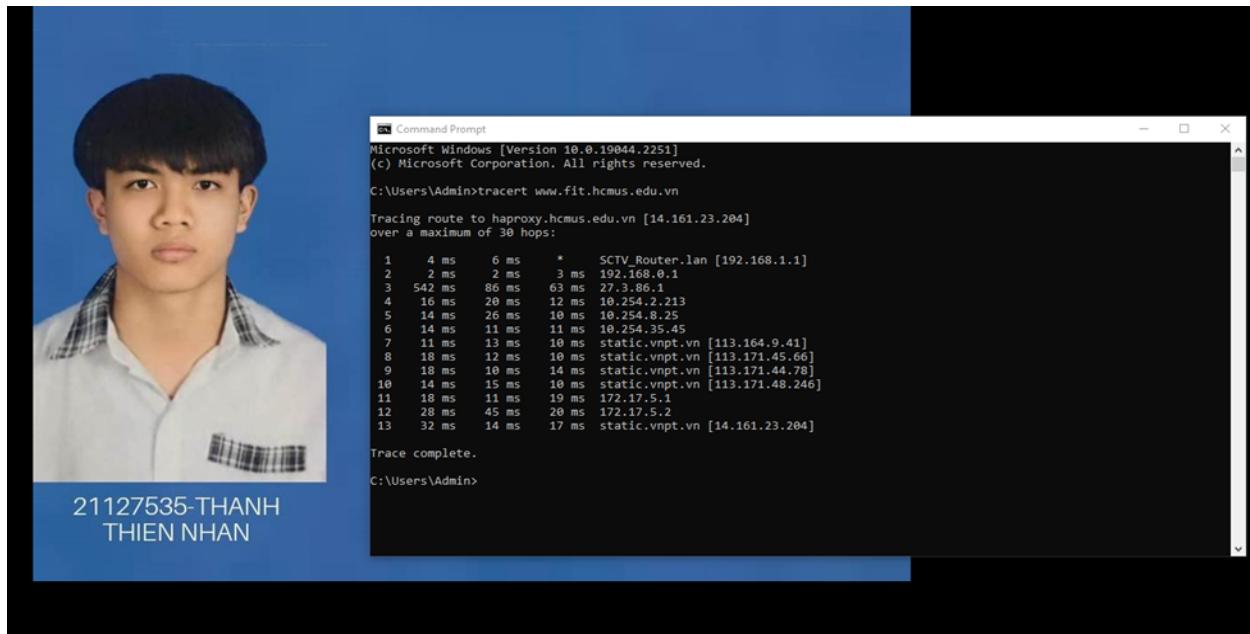
21127711\_Trịnh  
Minh Trung



## Bài 4: Traceroute

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

Kết quả bắt gói tin sau khi dùng lệnh “tracert fit.hcmus.edu.vn”:

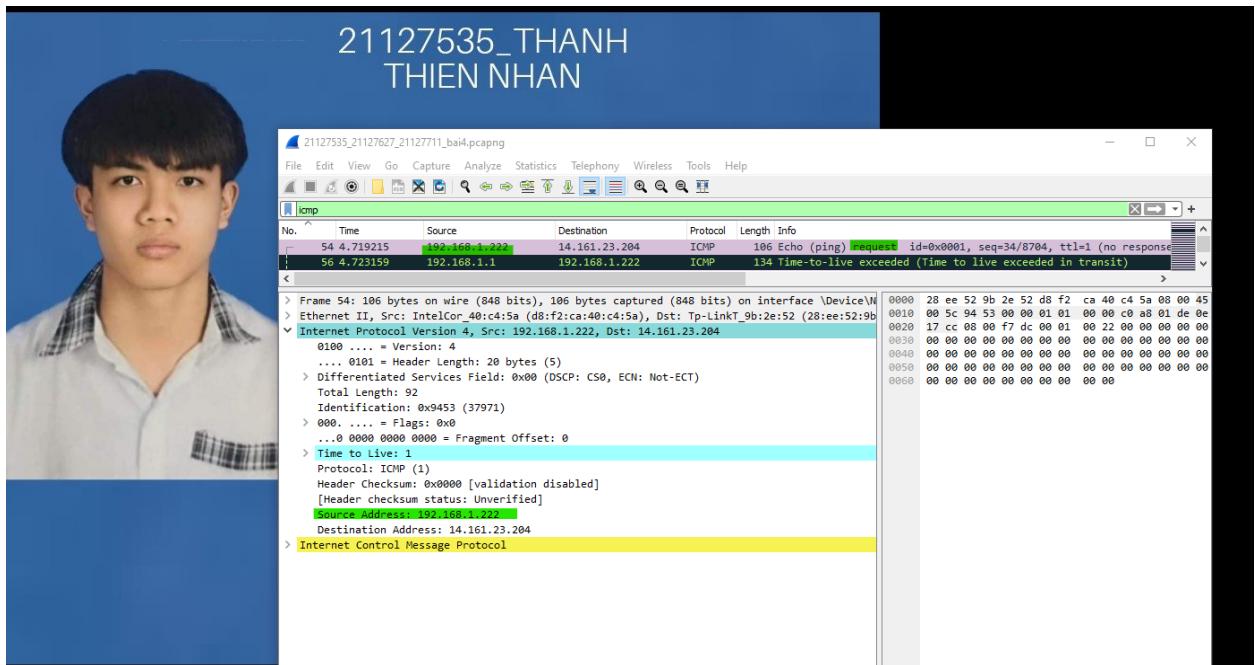


## 2) Cho biết traceroute/tracert dùng để làm gì?

Traceroute/Tracert là công cụ dòng lệnh trên nền tảng Windows, được sử dụng để hiển thị một số chi tiết về đường đi mà một gói tin đi từ thiết bị đang sử dụng (computer, host...) đến nơi được chỉ định, từ đó quản trị viên có thể giải quyết được các vấn đề kết nối một cách tốt hơn. Nói cách khác, Traceroute/Tracert là công cụ xác định đường đi từ nguồn đến đích của một gói giao thức mạng Internet (còn gọi là IP).

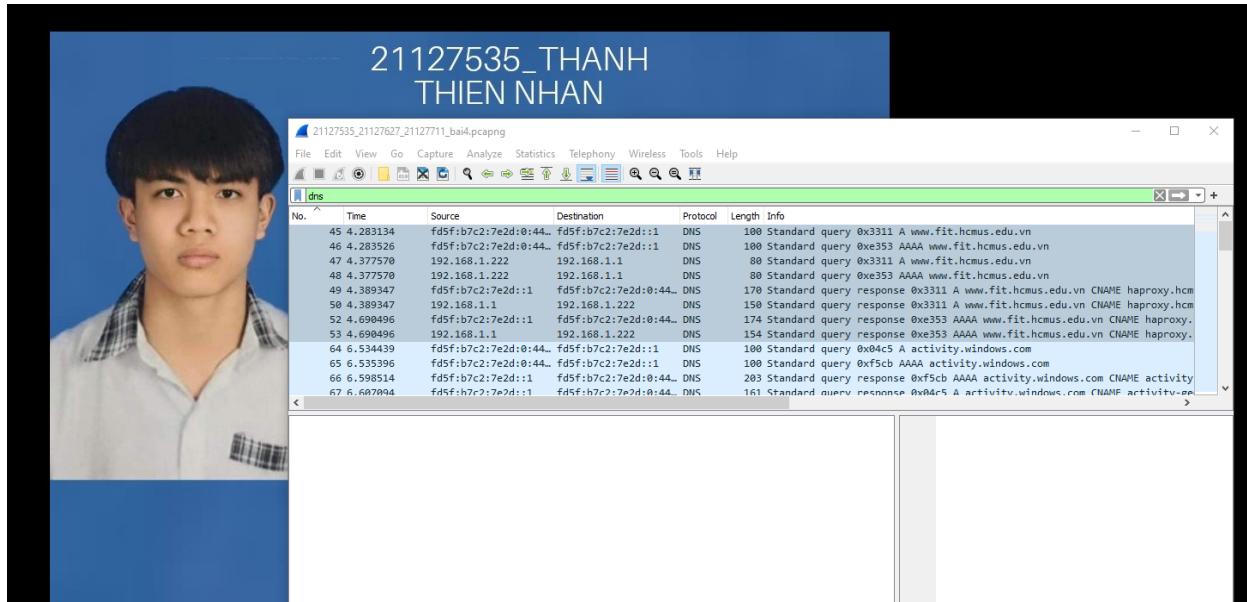
## 3) Cho biết địa chỉ IP của máy gửi request?

Địa chỉ IP của máy gửi request là: 192.168.1.222



#### 4) Cho biết cách máy tính xác định được địa chỉ IP của FIT

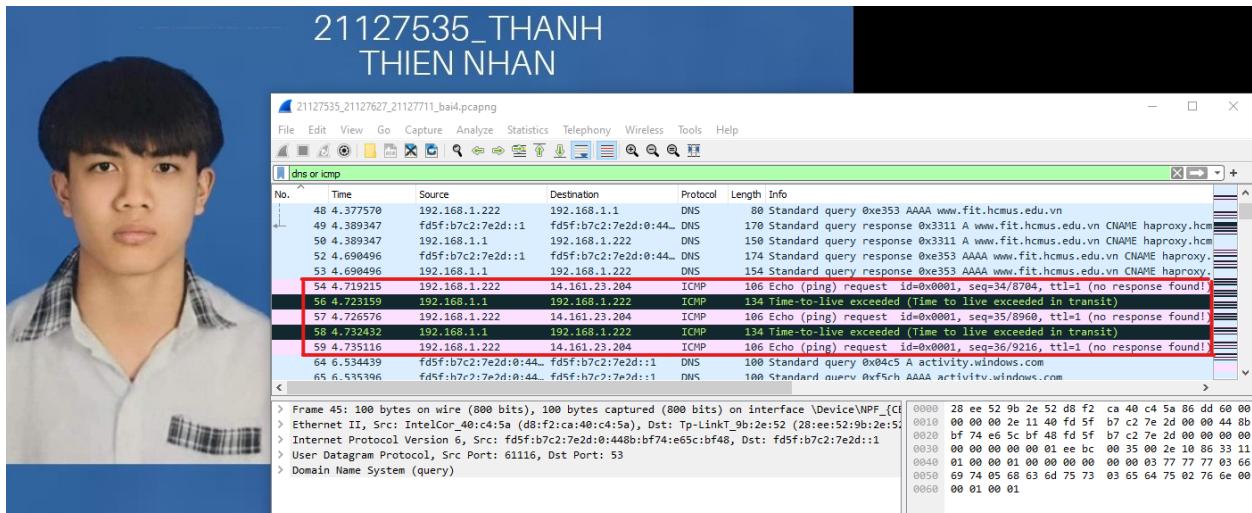
Để máy tính xác định được địa chỉ IP của FIT thì nó sẽ gửi đi các gói tin DNS đến router. Lúc này router sẽ kết nối đến DNS server, DNS server sẽ “dịch” (translate) ra địa chỉ IP của FIT từ tên miền “www.fit.hcmus.edu.vn” đến cho router, và từ đó router sẽ trả về cho máy địa chỉ IP của FIT.



5) Sau khi xác định được IP của www.fit.hcmus.edu.vn, máy sẽ bắt đầu gửi gói tin đến FIT

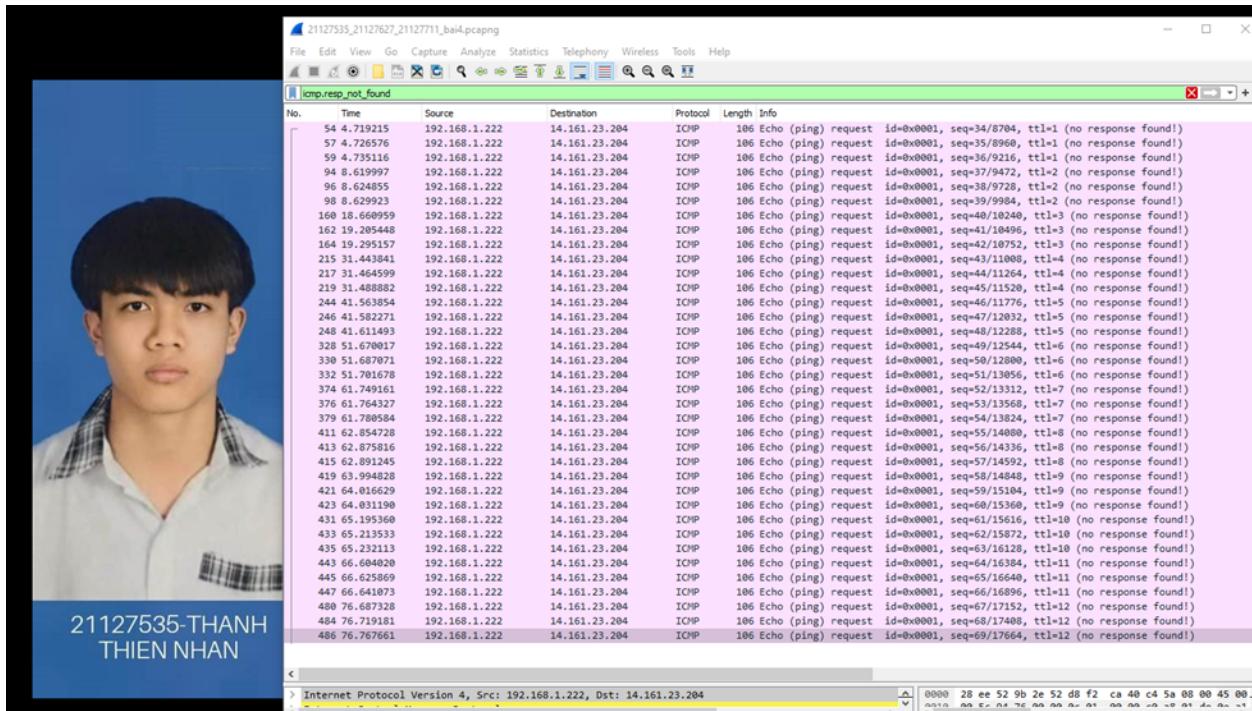
a) Protocol được sử dụng của những gói tin sau đó là gì?

Protocol được sử dụng của những gói tin sau đó là ICMP

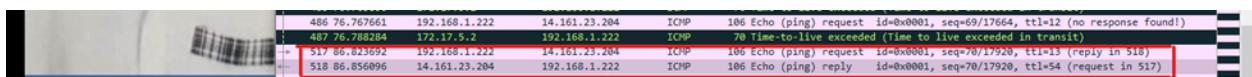


b) Có bao nhiêu gói tin được gửi đi (request) trước khi nhận được phản hồi đầu tiên cho những request?

Có 37 gói tin được gửi đi (request) trước khi nhận được phản hồi đầu tiên cho request



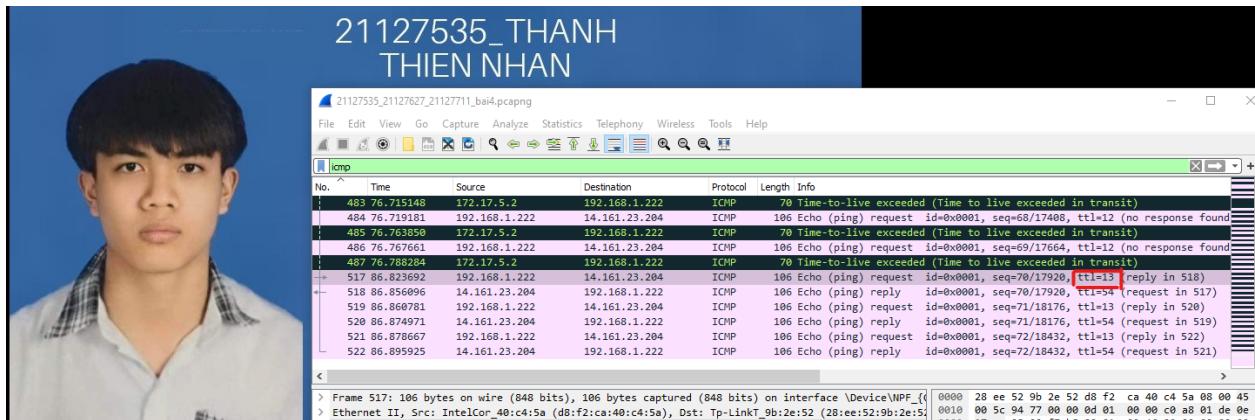
36 gói tin đầu tiên



Gói tin thứ 37 ở No. 517 và phản hồi đầu tiên (reply) ở No. 518

- c) Cho biết TTL của gói tin cuối cùng được gửi trước khi nhận được gói tin phản hồi đầu tiên cho những gói tin request?

TTL của gói tin cuối cùng được gửi trước khi nhận được gói tin phản hồi đầu tiên cho những gói tin request là: TTL=13



- 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?

Em không thấy thông tin **port** trong các gói tin gửi đi.

Giải thích: Lệnh Tracert xác định đường đi đến một đích bằng cách gửi gói echo ICMP đến đích đó. Mà gói tin ICMP không có port vì nó được thiết kế ở tầng Network dùng để giao tiếp thông tin giữa các host và router, không phải giữa các quy trình tầng Application. ICMP nằm trong gói IP và nó không chứa header của tầng Application (trong khi đó Source Port và Destination Port được thêm vào header ở tầng Application).

- e) Gói tin phản hồi đầu tiên là trả lời cho gói tin request thứ mấy? (No.)  
Gói tin phản hồi đầu tiên là trả lời cho gói tin request thứ 37 (No. 517)

