

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN

~~~~~\*~~~~~



# BÁO CÁO ĐỒ ÁN WIRESHARK

**Môn học: Mạng máy tính**

*Giáo viên hướng dẫn* : Lê Hà Minh  
*Sinh viên thực hiện* : 21120070 – Nhan Hữu Hiếu  
21120182 – Phan Trí Nhân  
21120183 – Trần Anh Tài  
*Lớp* : 21CTT2

HỒ CHÍ MINH – 2022

## MỤC LỤC

|                                             |           |
|---------------------------------------------|-----------|
| <b>I. BẢNG PHÂN CÔNG CÔNG VIỆC .....</b>    | <b>3</b>  |
| <b>II. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH .....</b> | <b>3</b>  |
| <b>III. NỘI DUNG BÁO CÁO .....</b>          | <b>4</b>  |
| <b>1. Bài 01: Ping .....</b>                | <b>4</b>  |
| 1.1. Câu 1 .....                            | 4         |
| 1.2. Câu 2 .....                            | 4         |
| 1.3. Câu 3 .....                            | 4         |
| <b>2. Bài 02: UDP .....</b>                 | <b>7</b>  |
| 2.1. Câu 1 .....                            | 7         |
| 2.2. Câu 2 .....                            | 7         |
| 2.3. Câu 3 .....                            | 8         |
| 2.4. Câu 4 .....                            | 8         |
| 2.5. Câu 5 .....                            | 8         |
| 2.6. Câu 6 .....                            | 8         |
| <b>3. Bài 03: HTTP .....</b>                | <b>8</b>  |
| 3.1. Câu 1 .....                            | 9         |
| 3.2. Câu 2 .....                            | 9         |
| 3.3. Câu 3 .....                            | 9         |
| 3.4. Câu 4 .....                            | 10        |
| <b>4. Bài 04: Traceroute .....</b>          | <b>11</b> |
| 4.1. Câu 1 .....                            | 12        |
| 4.2. Câu 2 .....                            | 13        |
| 4.3. Câu 3 .....                            | 13        |
| 4.4. Câu 4 .....                            | 13        |
| 4.5. Câu 5 .....                            | 14        |
| <b>IV. TÀI LIỆU THAM KHẢO .....</b>         | <b>18</b> |

## I. BẢNG PHÂN CÔNG CÔNG VIỆC

| STT | Họ và tên     | MSSV     | Nhiệm vụ                                   |
|-----|---------------|----------|--------------------------------------------|
| 1   | Nhan Hữu Hiếu | 21120070 | Làm bài 1, viết báo cáo, tìm tư liệu       |
| 2   | Phan Trí Nhân | 21120182 | Làm bài 4, hiệu chỉnh báo cáo, tìm tư liệu |
| 3   | Trần Anh Tài  | 21120183 | Làm bài 2, 3, tìm tư liệu                  |

## II. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH

| STT | Bài   | Đánh giá                                                                                                                                                                                                  | Mức độ hoàn thành |
|-----|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 1   | Bài 1 | Biết cách đọc pcap file, quan sát được các thông tin của một gói tin, giải thích được sự tồn tại của các gói tin ARP, vẽ được sơ đồ logic đường mạng tương ứng.                                           | 100%              |
| 2   | Bài 2 | Biết cách bắt, lọc gói tin trên card mạng, quan sát được các thông tin của một gói tin UDP, trả lời được các câu hỏi trong đề bài.                                                                        | 100%              |
| 3   | Bài 3 | Thực hiện đúng theo yêu cầu bắt gói tin trong đề, rút ra được các thông tin của máy chủ, quan sát được TCP segments, tính được throughput, áp dụng chức năng Flow Graph để vẽ quá trình trao đổi gói tin. | 100%              |
| 4   | Bài 4 | Biết cách traceroute để bắt gói tin, biết dùng kết quả bắt gói tin đó để trả lời các câu hỏi liên quan.                                                                                                   | 100%              |

### III. NỘI DUNG BÁO CÁO

#### 1. Bài 01: Ping

Mở *ping.pcapng* file (nội dung của file pcap là thông tin các gói tin gửi từ một máy sang một máy khác bằng lệnh ping) và trả lời các câu hỏi.

##### 3.1. Câu 1

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

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

The screenshot shows a Wireshark capture of a ping command. The packet list shows four packets:

| No. | Time        | Source            | Destination       | Protocol | Length | Info                                  |
|-----|-------------|-------------------|-------------------|----------|--------|---------------------------------------|
| 1   | 0.000000000 | IntelCor_3c:ac:58 | Broadcast         | ARP      | 42     | Who has 192.168.0.1? Tell 192.168.0.1 |
| 2   | 0.001828232 | TapLinkT_fc:53:7e | IntelCor_3c:ac:58 | ARP      | 42     | 192.168.0.1 is at 18:d6:c7:fc:53:7e   |
| 3   | 0.001835170 | 192.168.0.105     | 192.168.1.1       | ICMP     | 98     | Echo (ping) request id=0x000d, seq=   |
| 4   | 0.004770809 | 192.168.1.1       | 192.168.0.105     | ICMP     | 98     | Echo (ping) reply id=0x000d, seq=     |

The packet details pane shows the structure of the first packet (Frame 1: 42 bytes on wire):

- Frame 1: 42 bytes on wire (336 bits), 42 bytes capture
- Ethernet II, Src: IntelCor\_3c:ac:58 (a0:d3:7a:3c:ac:58)
- Address Resolution Protocol (request)

##### 3.2. Câu 2

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


Không có port được sử dụng trong các gói tin ARP và ICMP này vì ARP và ICMP là các giao thức hoạt động ở tầng Network, không phải ở tầng Transport.

##### 3.3. Câu 3

Với gói tin ICMP request:

- a) Cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

- # Nhan Hữu Hiếu - 21120070



## Wireshark - ping.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

| No. | Time        | Source            | Destination       | Protocol | Length | Info                                        |
|-----|-------------|-------------------|-------------------|----------|--------|---------------------------------------------|
| 1   | 0.000000000 | IntelCor_3c:ac:58 | Broadcast         | ARP      | 42     | Who has 192.168.0.1? Tell 192.168.0.105     |
| 2   | 0.001828232 | Tp-LinkT_fc:53:7e | IntelCor_3c:ac:58 | ARP      | 42     | 192.168.0.1 is at 18:d6:c7:fc:53:7e         |
| 3   | 0.001835170 | 192.168.0.105     | 192.168.1.1       | ICMP     | 98     | Echo (ping) request id=0x000d, seq=1/256, t |
| 4   | 0.004770309 | 192.168.1.1       | 192.168.0.105     | ICMP     | 98     | Echo (ping) reply id=0x000d, seq=1/256, t   |

> Ethernet II, Src: IntelCor\_3c:ac:58 (a0:d3:7a:3c:ac:58), Ds

> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.1

▼ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x0cce [correct]

[Checksum Status: Good]

Identifier (BE): 13 (0x000d)

Identifier (LE): 3328 (0x0d00)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

[Response frame: 4]

Timestamp from icmp data: Apr 1, 2021 10:42:04.000000000

[Timestamp from icmp data (relative): 0.636662804 second:

Data (48 bytes)

Data: blaf090000000000101112131415161718191a1b1c1d1e1f

[Length: 48]

0000 18 d6 c7 fc 53 7e a0 d3 7a 3c ac 58 08 00 45 00 ... S-

0010 00 54 7b 02 40 00 04 01 3c ec c0 a8 00 69 c0 a8 ... T{ @

0020 01 01 08 00 0c ce 00 00 00 01 0c 41 65 60 00 00 ...

0030 00 00 51 af 09 00 00 00 00 00 11 12 13 14 15 ...


0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ...

0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 ... &'()\*+ ,

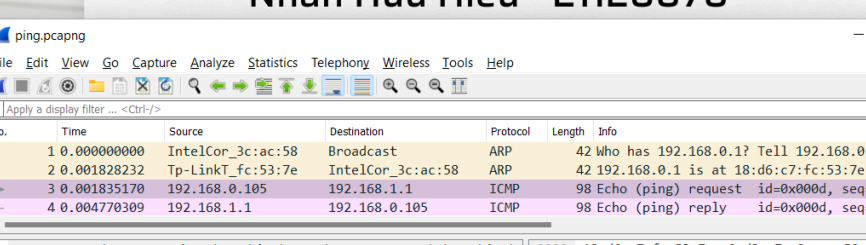
0060 36 37 ... 67

Packets: 4 · Displayed: 4 (100.0%)

Profile: Default

- 

## Nhan Hữu Hiếu - 21120070



The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows four packets. The selected packet (No. 3) is an ICMP Echo (ping) request from 192.168.0.105 to 192.168.1.1. The packet details pane on the right shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and ICMP Echo (ping) request data. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Tóm lại, ta có bảng thể hiện kích thước từng phần (đơn vị byte) trong diagram như sau:

|           |             |           |                 |
|-----------|-------------|-----------|-----------------|
| 48        | 16          | 20        | 14              |
| ICMP data | ICMP header | IP header | Ethernet header |

*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 đó:

- Gói tin thứ nhất: Khi source host muốn ping đến destination host ở ngoài đường mạng mà chưa biết địa chỉ MAC của destination host thì thiết bị nguồn sẽ tạo ARP request gồm địa chỉ MAC và IP của nguồn và địa chỉ IP của đích rồi gửi ARP request đến toàn mạng (broadcast).

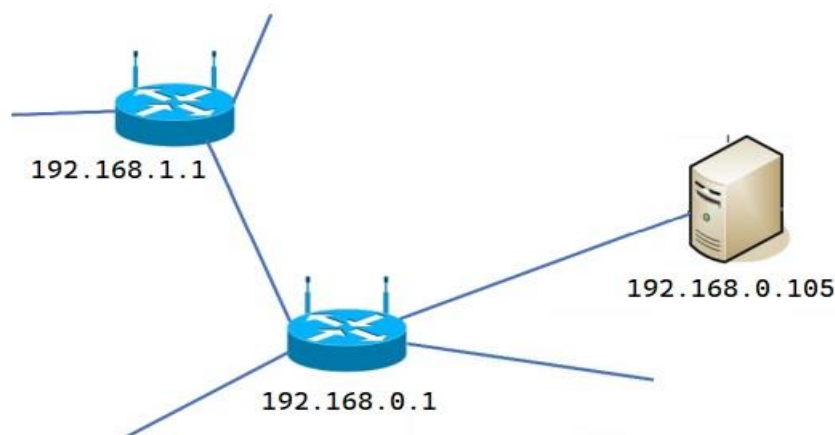
Ý nghĩa: gói tin ARP đầu tiên gửi yêu cầu xác định xem có tồn tại thiết bị cần tìm với địa chỉ IP tương ứng không.

- Gói tin thứ hai: Mặc dù tất cả các thiết bị trong mạng này sẽ nhận được ARP request nhưng chỉ có thiết bị có địa chỉ IP được đề cập trong request mới có thể phản hồi với địa chỉ MAC tương ứng, địa chỉ đó được chứa trong gói tin thứ hai này và gửi trả lại cho source host.

Ý nghĩa: gói tin ARP thứ hai phản hồi, xác định có tồn tại thiết bị cần tìm với địa chỉ IP tương ứng không.

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

Sơ đồ logic của đường mạng dựa theo nội dung gói pcap như sau:





## 2. Bài 02: UDP

Tiến hành các bước sau:

- Mở Wireshark và tiến hành bắt gói tin trên card mạng (có kết nối internet).
- Mở dòng lệnh và thực hiện lệnh `nslookup www.fit.hcmus.edu.vn`.
- Tạm dừng quá trình bắt gói tin.
- Thực hiện lọc gói tin bằng dòng lệnh `udp.srcport==53||udp.dstport==53`.

Sau đó trả lời các câu hỏi.

### 2.1. Câu 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?

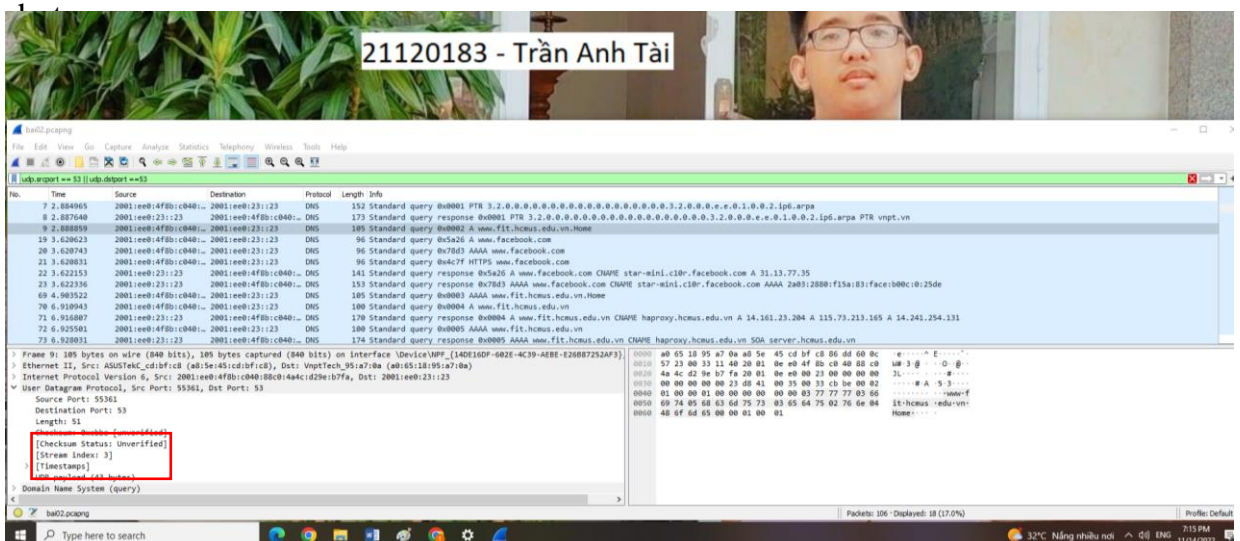
- Câu lệnh “nslookup” trên là một tiện ích chuẩn đoán DNS (cung cấp thông tin về vấn đề DNS nhiều hơn lệnh PING).
- “Non-authoritative answer” có ý nghĩa: dù DNS server không được cấu hình miền nhưng vẫn có thể cung cấp hồi đáp.

### 2.2. Câu 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)

Có 4 trường thông tin trong phần header của gói tin UDP. Trường Source Port: 2 bytes, trường Destination Port: 2 bytes, trường Length: 2 bytes, trường Checksum: 2

21120183 - Trần Anh Tài



The screenshot shows the Wireshark interface with a packet capture of a UDP packet. The packet list shows a packet from 2001:eeb:4fb0:c040:: to 2001:eeb:23:123 on port 53. The packet details pane shows the UDP header with Source Port 55361, Destination Port 53, Length 51, and Checksum 0x0000. The packet bytes pane shows the raw data of the packet.

### 2.3. Câu 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 là 51. Đơn vị là byte. Trường này đang nói độ dài của header và data ( $8+43=51$  bytes).

### 2.4. Câu 4

*Protocol number của UDP là gì? (trả lời giá trị dạng hexadecimal và decimal)*

Protocol number của UDP là 17 (decimal) và 11 (hexadecimal).

### 2.5. Câu 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)*

Vì length là 2 bytes (16 bits)  $\Rightarrow$  Lượng dữ liệu tối đa có thể đưa vào UDP payload là  $2^{16} - 1 - 8 = 65527$  bytes.

### 2.6. Câu 6

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

Xét 1 cặp gói tin trong đó gói tin thứ 2 trả lời cho gói tin thứ nhất, khi đó: source port của gói gửi đi là destination port của gói nhận, destination port của gói đi là source port của gói nhận

## 3. Bài 03: HTTP

*Tiến hành các bước sau:*

- Tải file theo link sau: <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>.
- Dùng trình duyệt web truy cập trang: <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.
- Mở Wireshark và tiến hành bắt gói tin trên card mạng (có kết nối internet).
- Thực hiện chọn đường dẫn đến file *alice.txt* vừa download, chọn Upload *alice.txt* file trên trình duyệt.
- Dùng quá trình bắt gói tin và lọc ra những gói tin gửi đi hoặc gửi đến máy chủ *gaia.cs.umass.edu*.



*Sau đó, trả lời các câu hỏi.*

### **3.1. Câu 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

### **3.2. Câu 2**

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

*a) Cho biết No. của 7 TCP segments đó*

No. của 7 TCP segments lần lượt là: 18, 19, 25, 29, 34, 36, 39.

*b) Cho biết No. của 7 TCP segments đó*

Sequence number của 7 TCP segments lần lượt là 1, 750, 13818, 15270, 41406, 44310, 58830.

*c) Cho biết No. của 7 TCP segments đó*

No. của ACK báo nhận của 7 TCP segments là: 1.

*d) Cho biết No. của 7 TCP segments đó*

Lượng data gửi trong 7 TCP segments lần lượt là 749, 13068, 1452, 26136, 2904, 14520, 17424 (bytes).

### **3.3. Câu 3**

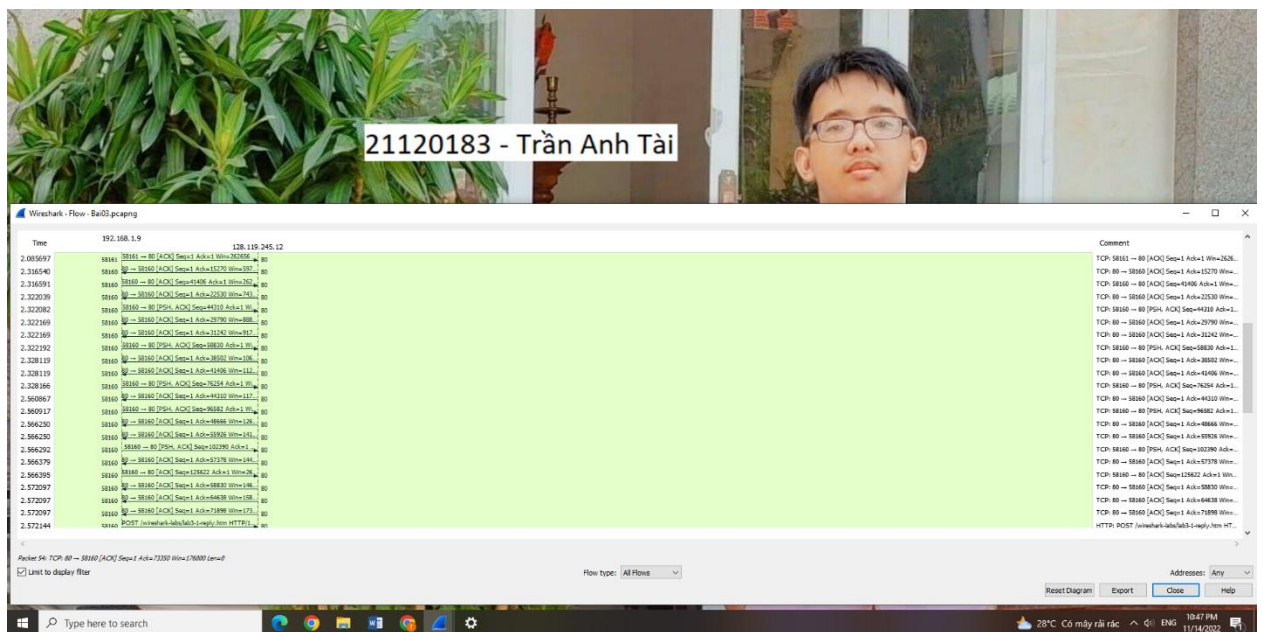
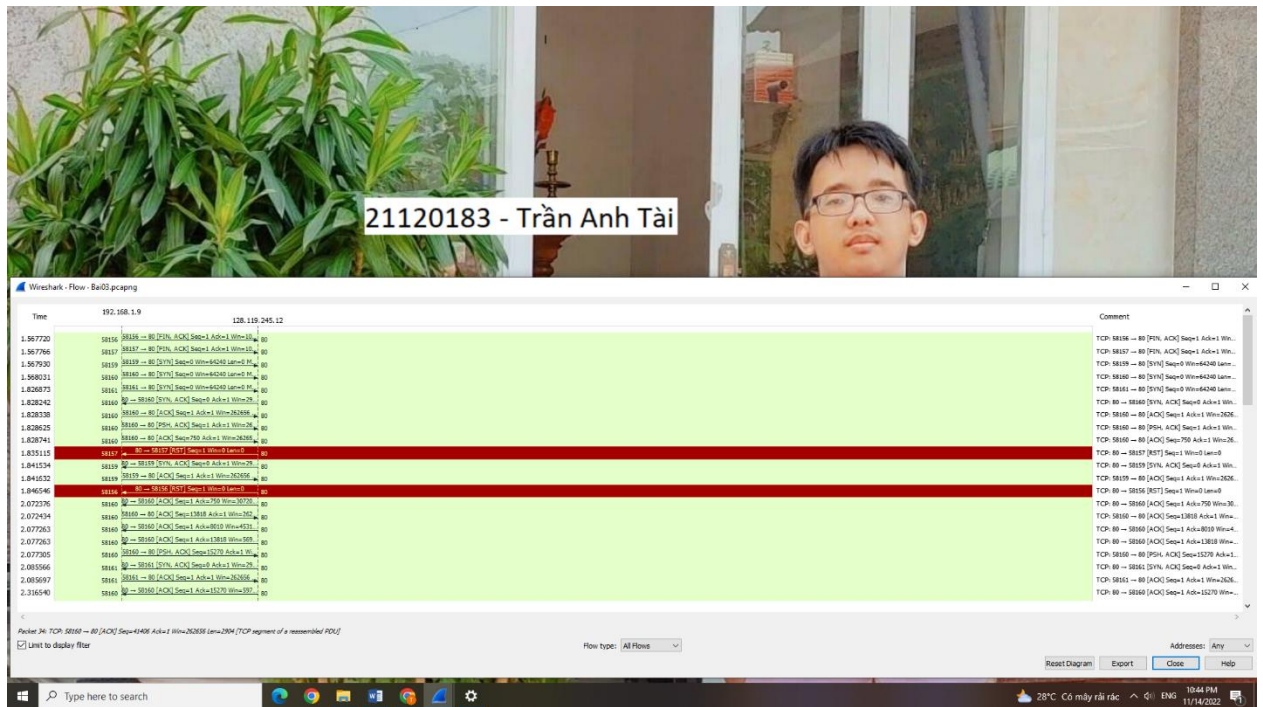
*Cho biết throughput (bytes transferred per unit time) cho kết nối upload file này, vui lòng cho biết cách tính*

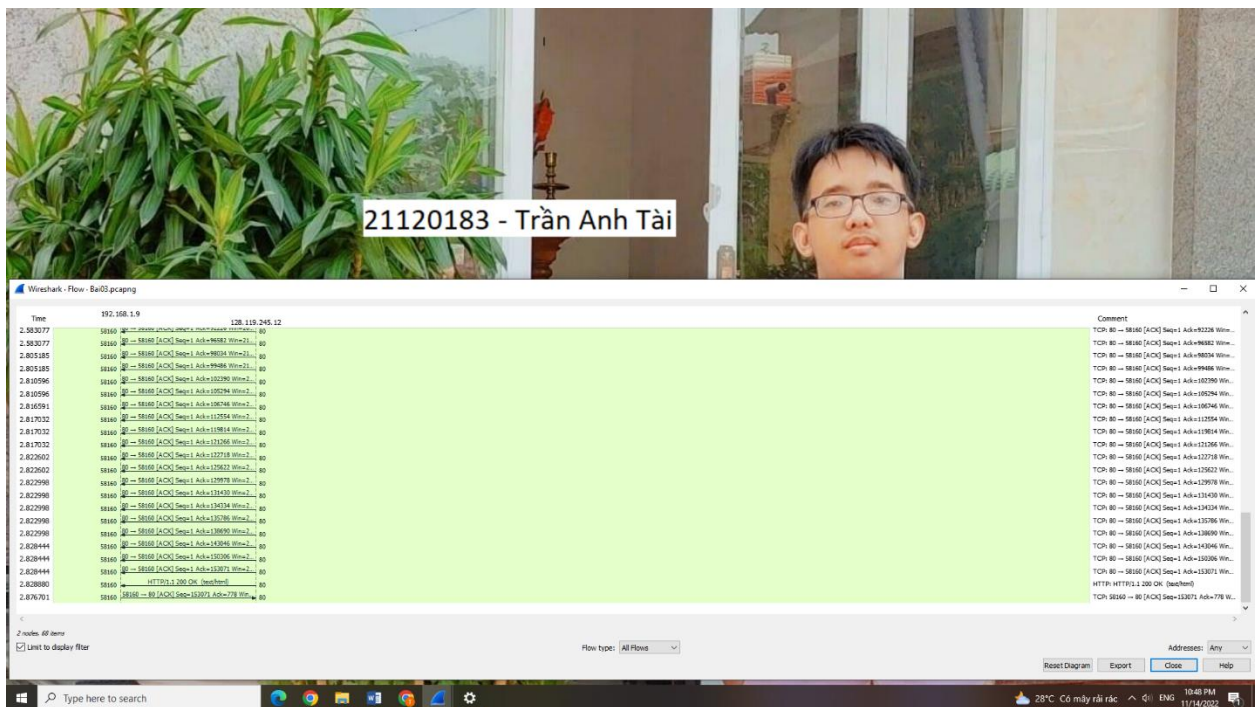
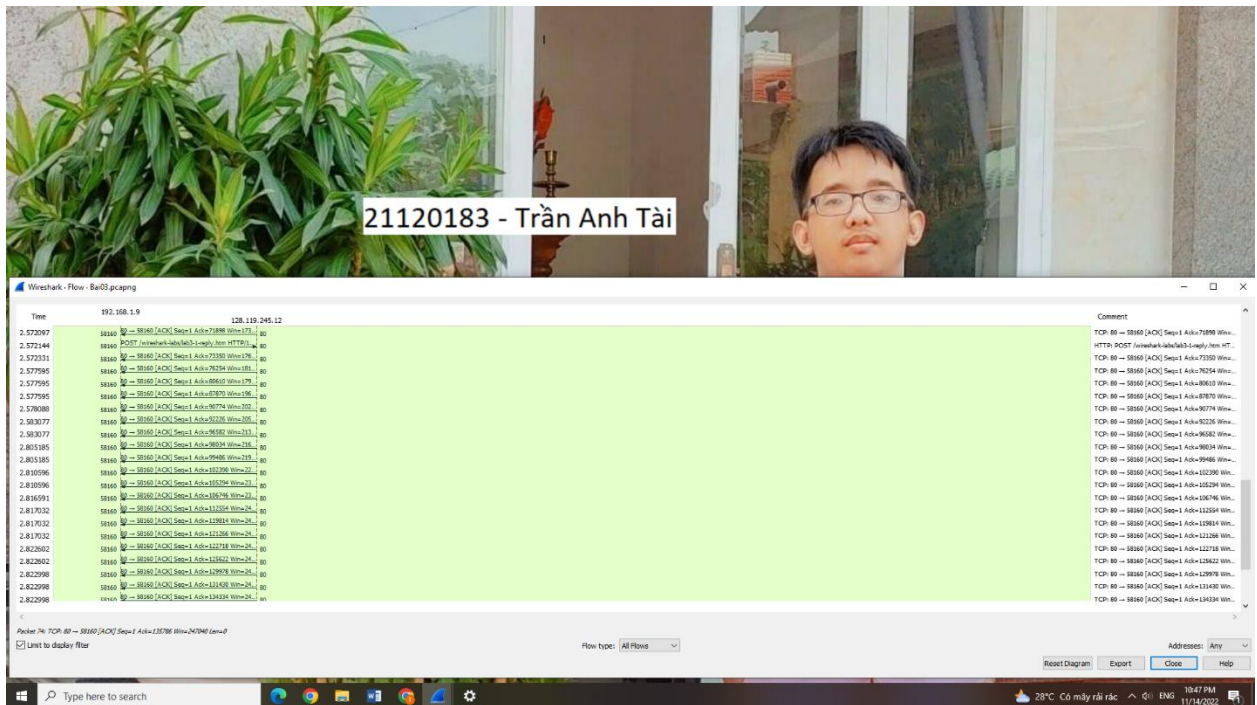
Throughput (bytes transferred per unit time) cho kết nối upload file này = Tổng Length của tất cả gói tin / thời gian truyền nhận =  
(54\*6+60\*43+66\*6+803+831+1506+2958\*2+5862+13122+14574+17478+20382+23286+24599+26190) bytes / (2.876701-1.567720) s = 120589.2217 bytes/s.

### 3.4. Câu 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 được yêu cầu trong đề bài được vẽ như sau:





#### 4. Bài 04: Traceroute

Bật Wireshark để bắt gói tin lệnh *tracert/traceroute* từ máy của mình (có thể dùng máy ảo) đến [www.fit.hcmus.edu.vn](http://www.fit.hcmus.edu.vn) (FIT). Sau đó trả lời các câu hỏi.



#### 4.1. Câu 1

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

Ảnh chụp kết quả bắt gói tin sau khi tracert, thấy được những gói tin liên quan.

The screenshot shows a Windows desktop with various application icons at the top. A Wireshark window is open, displaying a list of captured ICMP packets. The filter is set to 'icmp'. The packets are listed in a table with columns: No., Time, Source, Destination, Protocol, Length, and Info. The 'Info' column shows '106 Echo (ping) request' for most packets, but several show '70 Time-to-live exceeded'. To the right, a Command Prompt window shows the output of a 'tracert' command, displaying the route from the user's machine to 'haproxy.hcmus.edu.vn' with IP addresses and response times. The user's name '21120182 PHAN TRÍ NHÂN' is visible in the top right corner of the screenshot.

| No.   | Time       | Source          | Destination   | Protocol | Length | Info                  |
|-------|------------|-----------------|---------------|----------|--------|-----------------------|
| 10337 | 105.278058 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 10783 | 109.128242 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11355 | 113.100554 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11818 | 117.103170 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11820 | 117.118214 | 203.210.144.132 | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded |
| 11821 | 117.120891 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11822 | 117.128965 | 203.210.144.132 | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded |
| 11823 | 117.131749 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11825 | 117.138630 | 203.210.144.132 | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded |
| 11879 | 118.155704 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11882 | 118.164534 | 172.17.8.61     | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded |
| 11883 | 118.167218 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11885 | 118.186812 | 172.17.8.61     | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded |
| 11886 | 118.190108 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |
| 11887 | 118.203468 | 172.17.8.61     | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded |
| 12174 | 123.753859 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request   |

This screenshot is similar to the one above, showing a Wireshark window with a list of ICMP packets. The filter is still 'icmp'. The 'Info' column shows '106 Echo (ping) request' for most packets, but several show '70 Time-to-live exceeded'. To the right, a Command Prompt window shows the output of a 'tracert' command, displaying the route from the user's machine to 'haproxy.hcmus.edu.vn' with IP addresses and response times. The user's name '21120182 PHAN TRÍ NHÂN' is visible in the top right corner of the screenshot.

| No.   | Time       | Source        | Destination   | Protocol | Length | Info                        |
|-------|------------|---------------|---------------|----------|--------|-----------------------------|
| 12182 | 123.839109 | 172.17.5.1    | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time |
| 12184 | 123.842757 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |
| 12188 | 123.934802 | 172.17.5.1    | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time |
| 12189 | 123.937714 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |
| 12194 | 123.981793 | 172.17.5.1    | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time |
| 12736 | 129.516465 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |
| 12739 | 129.539077 | 172.17.5.2    | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time |
| 12740 | 129.542031 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |
| 12741 | 129.564725 | 172.17.5.2    | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time |
| 12742 | 129.567744 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |
| 12744 | 129.573617 | 172.17.5.2    | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time |
| 13323 | 135.161752 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |
| 13325 | 135.172048 | 14.161.23.204 | 172.20.20.64  | ICMP     | 106    | Echo (ping) reply id=0x0    |
| 13326 | 135.173280 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |
| 13328 | 135.189198 | 14.161.23.204 | 172.20.20.64  | ICMP     | 106    | Echo (ping) reply id=0x0    |
| 13329 | 135.191243 | 172.20.20.64  | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x0  |

## 4.2. Câu 2

*Cho biết traceroute/tracert dùng để làm gì?*

Tracert/Traceroute, nghĩa đen là “truy vết đường đi” là công cụ để kiểm tra đường đi của gói dữ liệu, xem nó đã đi qua các trạm nào, mất bao lâu để đi qua, trạm nào bị nghẽn, có bị không kết nối hay không? trạm đó bị nghẽn thì có con đường nào khác để đến đích hay không? Thực tế càng qua nhiều trạm thì càng chậm và càng có rủi ro bị time out (mất kết nối).

## 4.3. Câu 3

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

IP của máy gửi request là 172.20.20.64

The screenshot displays a Windows desktop environment. In the foreground, a Wireshark window is open, showing a packet capture of ICMP ping requests. The packet list pane shows several packets, with the first one (No. 10337) highlighted. The packet details pane shows the ICMP Echo (ping) request. The packet bytes pane shows the raw data. The desktop background features a portrait of Phan Trí Nhân with the number 21120182. The taskbar shows various application icons, including This PC, Recycle Bin, Control Panel, Unity Hub, Spotify, Zalo, Zoom, and Microsoft Teams.

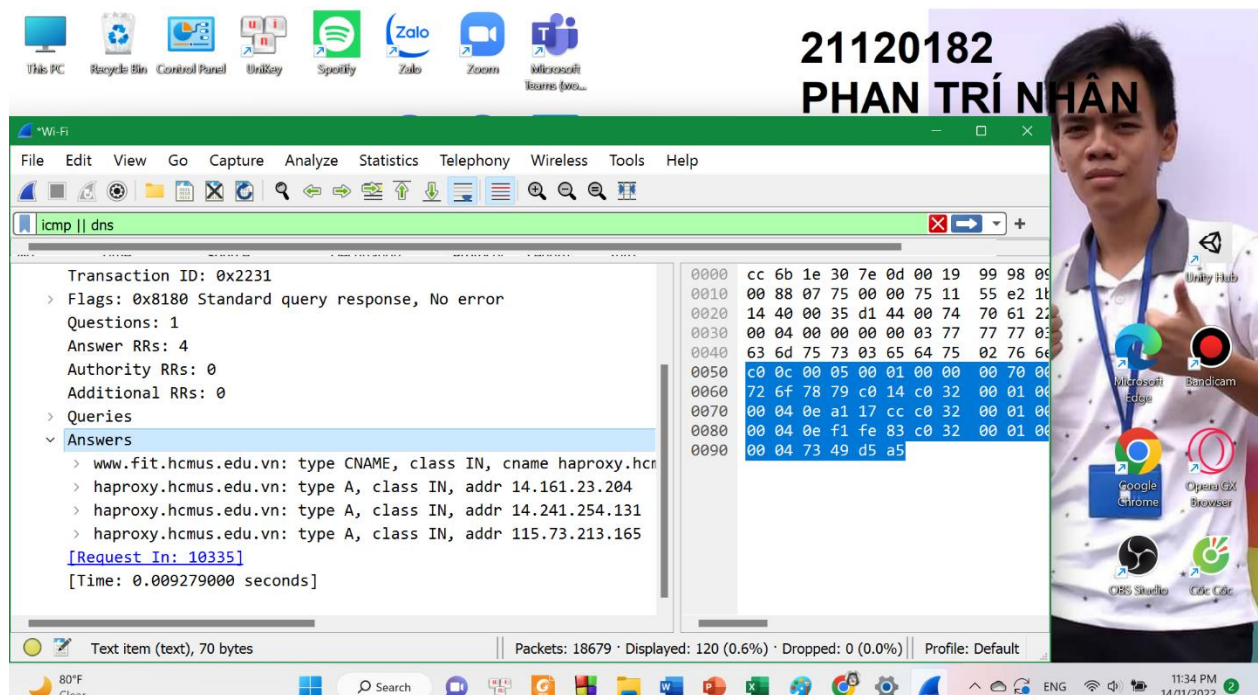
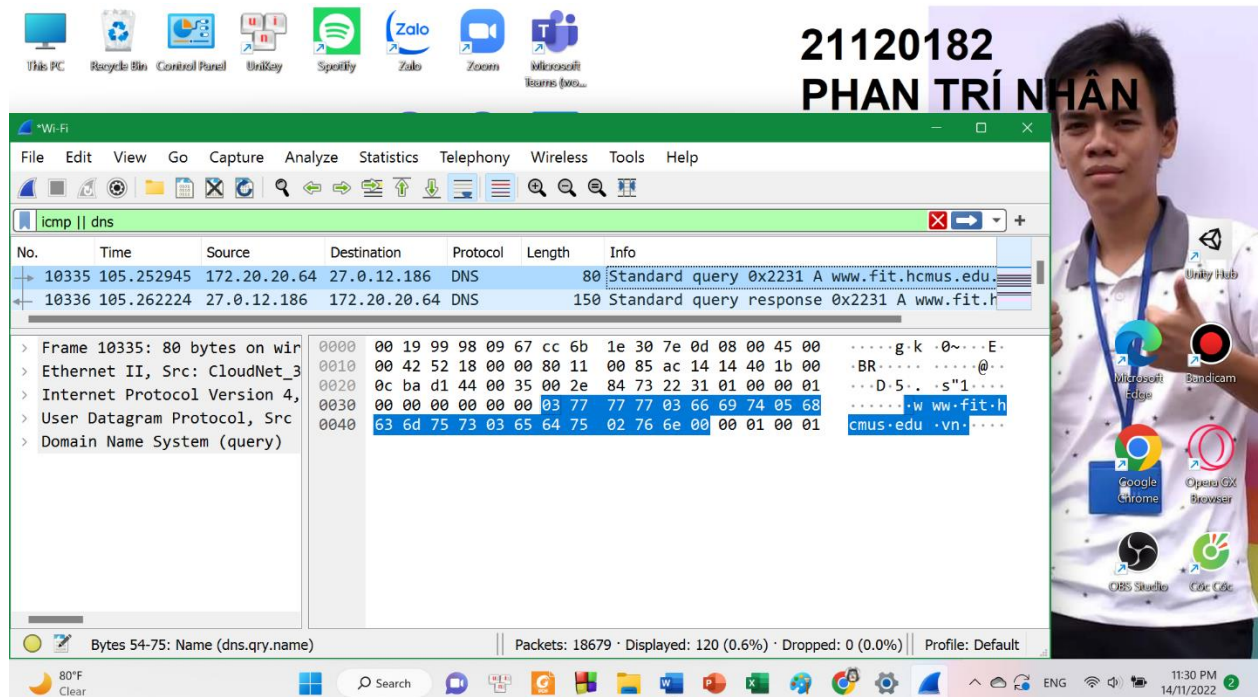
| No.   | Time       | Source          | Destination   | Protocol | Length | Info                          |
|-------|------------|-----------------|---------------|----------|--------|-------------------------------|
| 10337 | 105.278058 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 10783 | 109.128242 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11355 | 113.100554 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11818 | 117.103170 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11820 | 117.118214 | 203.210.144.132 | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time t |
| 11821 | 117.120891 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11822 | 117.128965 | 203.210.144.132 | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time t |
| 11823 | 117.131749 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11825 | 117.138630 | 203.210.144.132 | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time t |
| 11879 | 118.155704 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11882 | 118.164534 | 172.17.8.61     | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time t |
| 11883 | 118.167218 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11885 | 118.186812 | 172.17.8.61     | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time t |
| 11886 | 118.190108 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |
| 11887 | 118.203468 | 172.17.8.61     | 172.20.20.64  | ICMP     | 70     | Time-to-live exceeded (Time t |
| 12174 | 123.753859 | 172.20.20.64    | 14.161.23.204 | ICMP     | 106    | Echo (ping) request id=0x000  |

## 4.4. Câu 4

*Cho biết cách máy tính xác định được địa chỉ IP của FIT*

Cách máy tính xác định được địa chỉ IP của FIT: Máy tính gửi truy vấn (query) tên miền “www.fit.hcmus.edu.vn” đến DNS Server và DNS Server gửi về gói tin response chứa thông tin IP của hostname.





#### 4.5. Câu 5

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

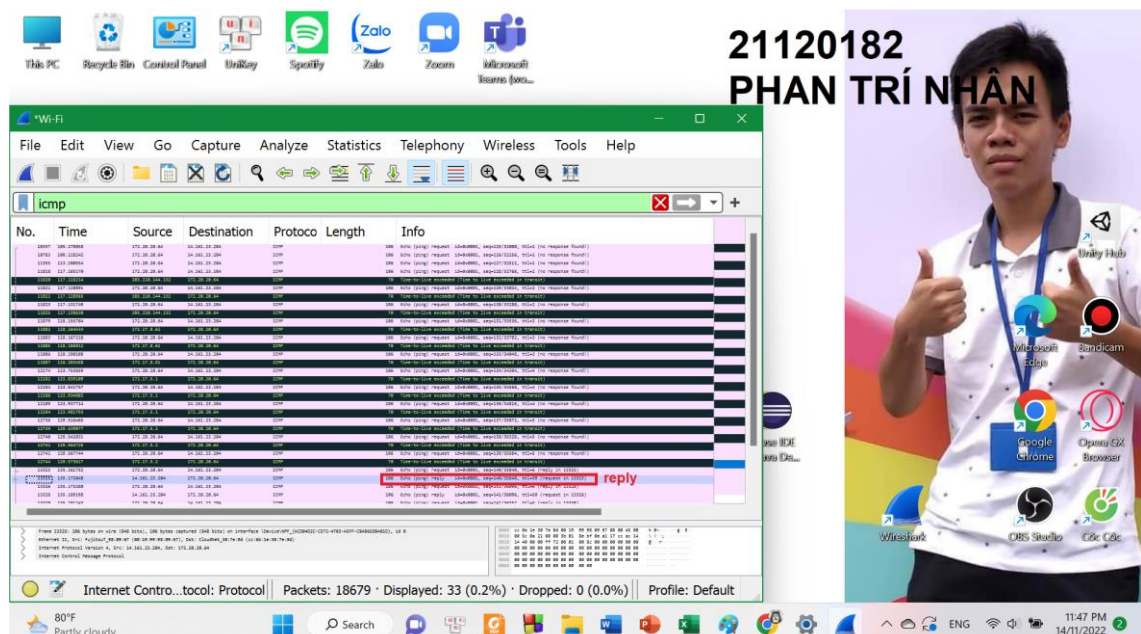
Trả lời các câu hỏi sau:

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

Protocol (Phương thức) được sử dụng của những gói tin đó là ICMP.

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

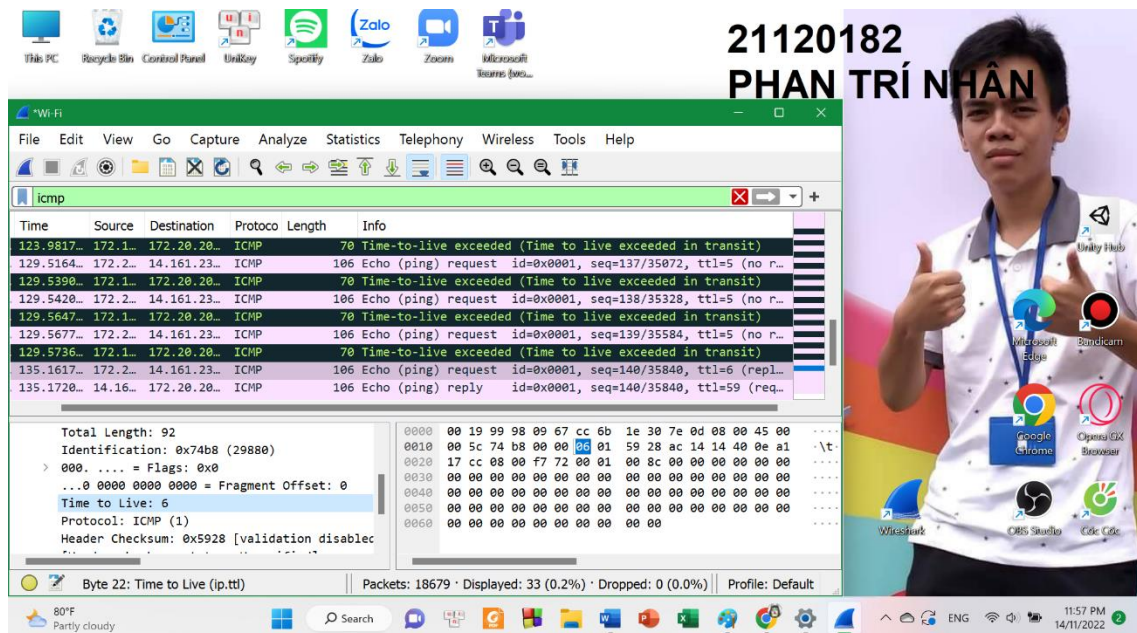
Có thể thấy 16 gói tin request ICMP trước khi nhận được reply (phản hồi) đầu tiên cho request (mỗi 3 gói tin liên tiếp nhau có cùng ttl lần lượt là 1,2,3,4,5).



- 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?

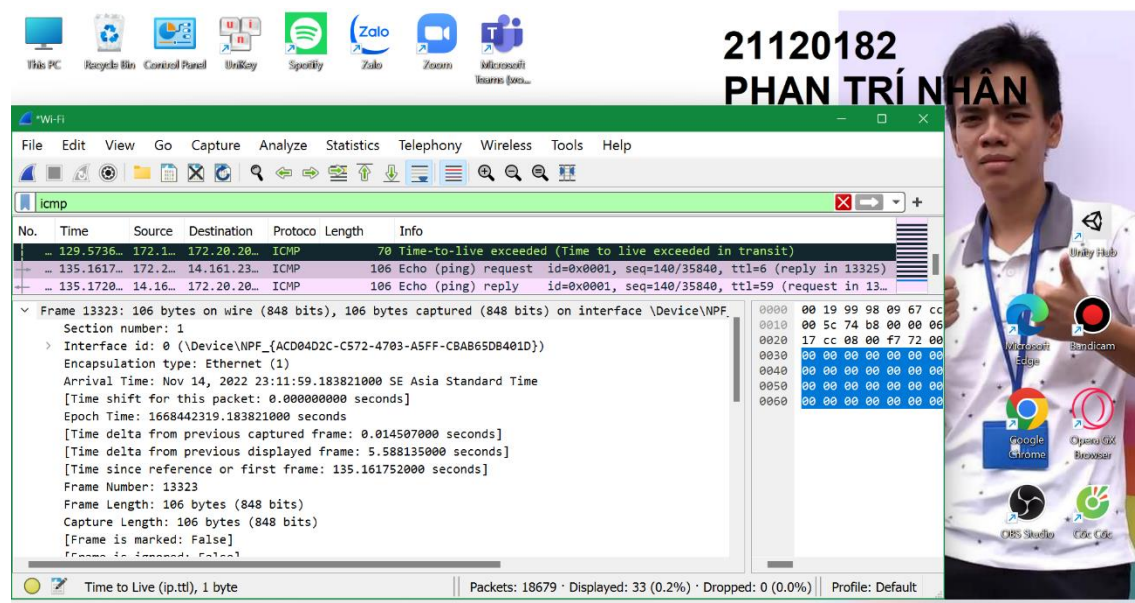
TTL (Time to live đề cập đến lượng thời gian hoặc “hops” mà một packet được thiết lập để tồn tại trong mạng trước khi bị router loại bỏ) của gói tin request cuối cùng được gửi trước khi gói tin phản hồi đầu tiên cho những request là 6.





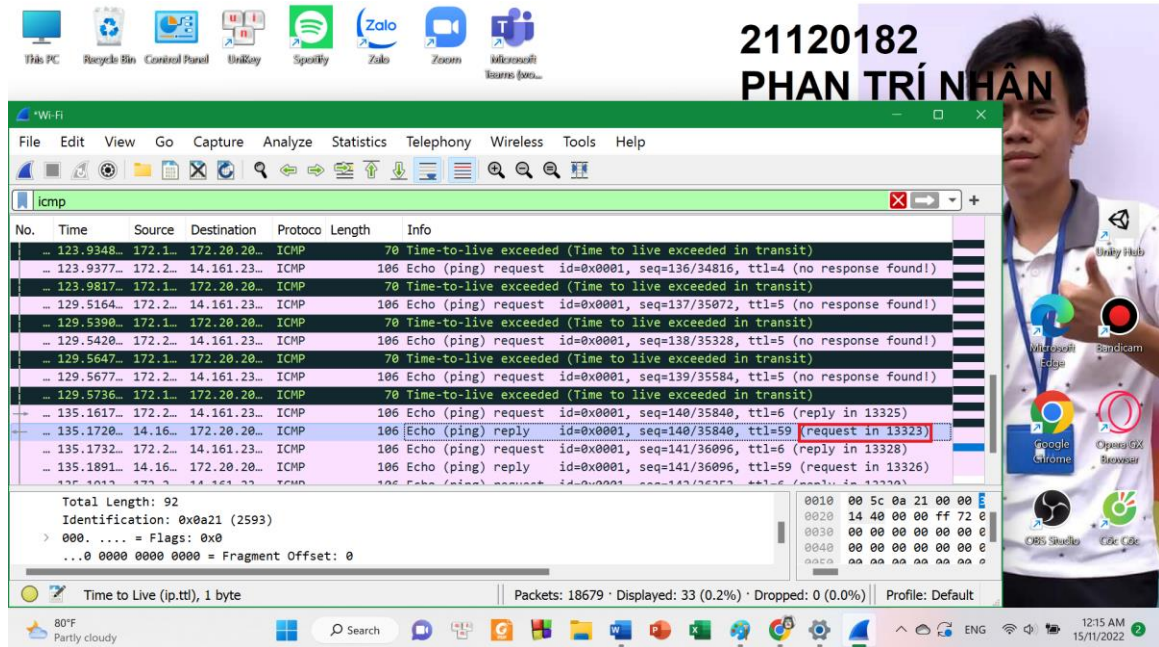
- d) *Bạn có thấy thông tin port trong các gói tin gửi đi? Nếu có bạn nhận thấy port nguồn/đích của gói tin có gì đặc biệt? Nếu không thấy thông tin port, hãy giải thích nguyên nhân?*

Trong các gói tin ICMP được gửi đi thì không thấy có thông tin port. Vì ICMP là một giao thức được thiết kế ở tầng Network dùng để giao tiếp thông tin “Host-to-Host” thông qua các router. ICMP trong gói IP và không chứa các header “Source-Port” hay “Destination-Port” vì chúng là các header ở tầng Application.



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

Gói tin reply đầu tiên là trả lời cho gói tin request thứ 16, No. 13323.



#### IV. TÀI LIỆU THAM KHẢO

1. James Kurose, Keith Ross, *Computer Networking A Top-Down Approach, 7th Edition*.
2. Mai Văn Cường và nnk (2020), *Giáo trình Mạng máy tính*, Nhà xuất bản Khoa học và Kỹ thuật.
3. *Tài liệu lý thuyết môn Mạng máy tính*.
4. *What Is Wireshark and How Is It Used?*  
<https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>
5. *How to Use Wireshark to Capture, Filter and Inspect Packets*,  
<https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets>
6. *Ping: ICMP vs. ARP*, <https://www.linux.com/news/ping-icmp-vs-arp/>
7. *Sử dụng NSLOOKUP để chuẩn đoán DNS Server*,  
<https://quantrimang.com/cong-nghe/su-dung-nslookup-de-chuan-doan-dns-server-44280#:~:text=Khi%20b%E1%BA%A1n%20c%E1%BA%A7n%20nh%E1%B%81u%20th%C3%B4ng,s%E1%BA%B5n%20trong%20Windows%20v%C3%A0%20UNIX.>
8. *Tìm hiểu giao thức TCP và UDP*, <https://viblo.asia/p/tim-hieu-giao-thuc-tcp-va-udp-jvEla11x1kw>.
9. *IP Protocol number là gì*,  
<https://www.forum.vnpro.org/forum/ccna%C2%AE/icnd-2-routing-access-list/29140-ip-protocol-number-l%C3%A0-g%C3%AC>
10. *Tìm hiểu UDP với Wireshark*, [https://cuuduongthancong.com/dlf/197498/mang-may-tinh/lap-10\\_tim-hieu-udp-voi-wireshark.pdf](https://cuuduongthancong.com/dlf/197498/mang-may-tinh/lap-10_tim-hieu-udp-voi-wireshark.pdf)

=====HẾT=====