



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

-----&&-----

**BÁO CÁO ĐO ÁN THỰC HÀNH
MẠNG MÁY TÍNH**

**TÊN ĐO ÁN:
WIRESHARK**

LỚP: 21CLC05

NHÓM: 10

Thông tin nhóm:

20127601 Nguyễn Anh Quân

21127099 Nguyễn Tân Lộc

21127168 Bùi Phước Thiện

Giảng viên lý thuyết:

ThS. Huỳnh Thụy Bảo Trân

Hướng dẫn thực hành:

ThS. Chung Thùy Linh

MỤC LỤC

GIỚI THIỆU WIRESHARK	4
THÔNG TIN VỀ ĐỒ ÁN.....	5
KẾT QUẢ THỰC HIỆN ĐỒ ÁN.....	6
<i>Bài 1: Ping (2đ)</i>	6
1. Cho biết địa chỉ IP của host ping và host được ping?	6
2. Cho biết port được sử dụng là bao nhiêu? Nếu không có port thì giải thích tại sao?	6
3. Với gói tin ICMP request, thực hiện yêu cầu:	7
<i>Bài 2: UDP (2.5đ)</i>	12
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?.....	12
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 hình minh chứng bằng gói tin bắt được	12
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?	14
4. Protocol number của UDP là gì? (trả lời giá trị dạng hexadecimal và decimal)	15
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).....	15
6. Hãy cho biết mối quan hệ giữa port number trong những gói tin lọc được	16
<i>Bài 3: HTTP (2.5đ)</i>	17
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?	17
2. Tìm 7 TCP segments tiếp theo, tính từ TCP segment của HTTP POST đầu tiên ở câu 2 và trả lời những câu hỏi sau	18
3. Cho biết throughput (bytes transferred per unit time) cho kết nối upload file này, vui lòng cho biết cách tính.....	21
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	22
<i>Bài 4: Traceroute (3đ)</i>	28
1. Chụp hình kết quả bắt gói tin sau khi traceroute hoặc tracert (thấy được những gói tin liên quan)	28

2. Cho biết traceroute/tracert dùng để làm gì?	29
3. Cho biết địa chỉ IP của máy gửi request?	29
4. Cho biết cách máy tính xác định được địa chỉ IP của FIT	29
5. Sau khi xác định được IP của www.fit.hcmus.edu.vn, máy sẽ bắt đầu gửi gói tin đến FIT, trả lời những câu hỏi sau.....	31
ĐÁNH GIÁ THÀNH VIÊN	34
NGUYÊN TẮC HOẠT ĐỘNG NHÓM.....	35
BIÊN BẢN HỌP NHÓM PHÂN CÔNG	35
BIÊN BẢN HỌP NHÓM LẦN 1 NGÀY 4/12/2022	35
TÀI LIỆU THAM KHẢO.....	37

GIỚI THIỆU WIRESHARK

Lời đầu tiên, nhóm 10 xin gửi lời cảm ơn chân thành và sâu sắc đến cô **Huỳnh Thụy Bảo Trân** và cô **Chung Thùy Linh** - Giảng viên môn Mạng máy tính lớp 21CLC05 - Khoa Công nghệ thông tin đã hướng dẫn và truyền đạt đến nhóm 10 những kiến thức cơ sở, nền tảng để nhóm có đủ khả năng thực hiện thành công đồ án Wireshark.

Với kinh nghiệm còn hạn chế nên trong quá trình thực hiện đồ án nhóm sẽ có những sai sót nhất định. Nhóm 10 rất mong nhận được sự quan tâm và đánh giá đến từ cô **Huỳnh Thụy Bảo Trân** và cô **Chung Thùy Linh** để nhóm rút kinh nghiệm và hoàn thiện đồ án sau tốt hơn.

Tiếp theo, nhóm 10 sẽ giới thiệu sơ lược về Wireshark. Vậy Wireshark dùng để làm gì, cách sử dụng Wireshark như thế nào. Đầu tiên, Wireshark là ứng dụng phân tích mạng (Network Packet Analyzer). Công dụng của ứng dụng này là dùng để bắt, phân tích và xác định các vấn đề có liên quan đến network bao gồm: kết nối chậm, rót gói tin hoặc các truy cập bất thường. Thông qua Wireshark, quản trị viên có thể hiểu hơn về các Network Packets đang chạy trên hệ thống. Như vậy, việc xác định nguyên nhân gây ra lỗi cũng sẽ dễ dàng hơn.

Wireshark là công cụ cho phép giám sát gửi/nhận gói tin trên card mạng. Có 2 modes hoạt động: Open và Capture. Capture mode cho phép người dùng có thể xem trực tiếp các gói tin hiện tại đang ra/vào card mạng, và có thể lưu trữ lại với định dạng pcap file. Open mode cho phép người dùng đọc gói tin pcap file có sẵn.

Trên đây là những lời đầu tiên của nhóm 10 trong đồ án Wireshark. Một lần nữa, nhóm 10 xin chân thành cảm ơn cô **Huỳnh Thụy Bảo Trân** và cô **Chung Thùy Linh**.

Thành phố Hồ Chí Minh, ngày 09 tháng 12 năm 2022

NHÓM 10 (TH)- MẠNG MÁY TÍNH
Lớp 21CLC05, Khoa Công nghệ thông tin



THÔNG TIN VỀ ĐỒ ÁN

Mã học phần: CSC10008

Tên học phần: Mạng máy tính

Tên đồ án: Wireshark

Hình thức: Bài tập nhóm tìm hiểu + triển khai thử nghiệm + thảo luận

Mô tả:

- Bài 1: Ping (2đ)
- Bài 2: UDP (2.5đ)
- Bài 3: HTTP (2.5đ)
- Bài 4: Traceroute (3đ)

Giảng viên lý thuyết: ThS. Huỳnh Thụy Bảo Trân

Hướng dẫn bài tập: Ths. Chung Thùy Linh

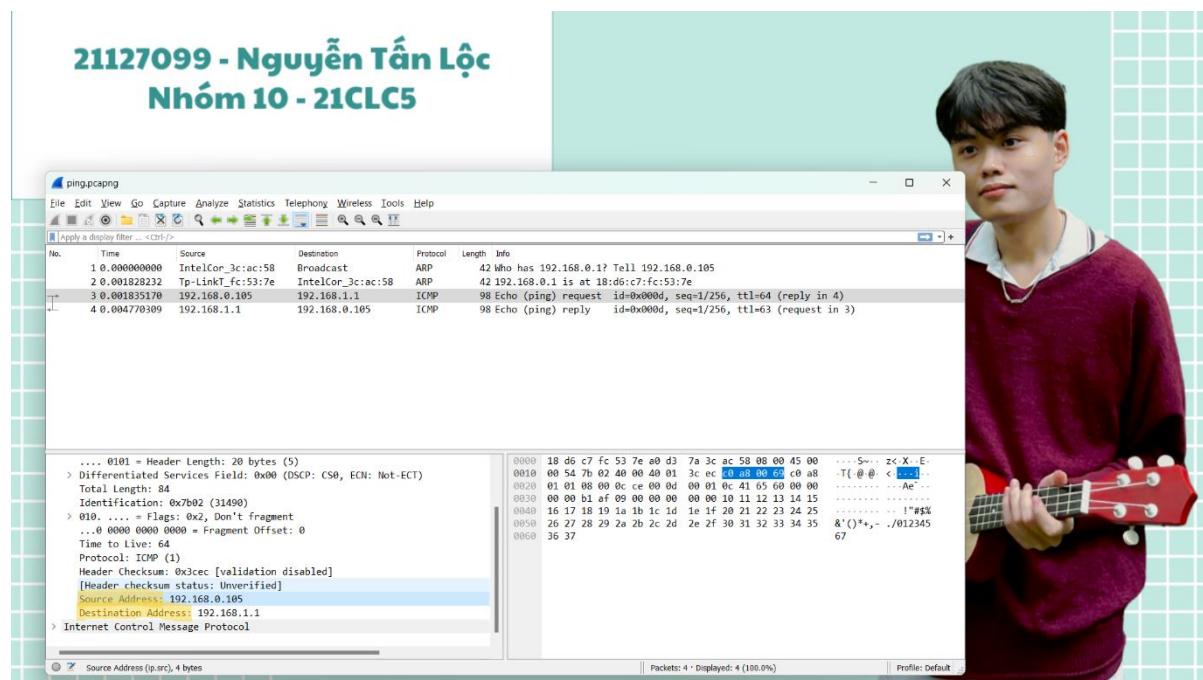
KẾT QUẢ THỰC HIỆN ĐỒ ÁN

Bài 1: Ping (2đ)

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. Trả lời các câu hỏi sau:

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

- Địa chỉ IP host ping là 192.168.0.105 (Source Port)
- Địa chỉ IP của host được ping là 192.168.1.1 (Destination Port)



Hình 1.1: Địa chỉ IP của host ping và host được ping

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

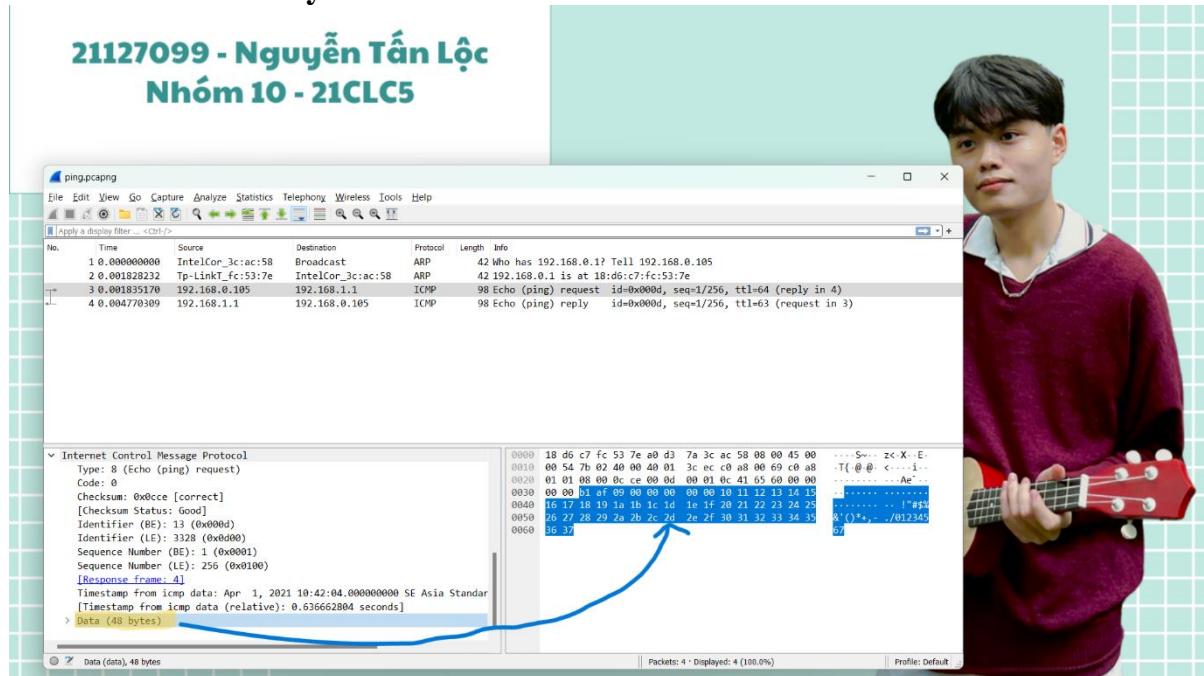
- Gói tin ICMP không có Port. Vì lệnh ping sử dụng giao thức ICMP và giao thức ICMP không có bất cứ khái niệm nào về Port. Giao thức ICMP được thiết kế để thực hiện giao tiếp thông tin trong tầng Network giữa các host và bộ định tuyến (tức là router), không phải giao tiếp giữa các quy trình trong tầng ứng dụng (tức là tầng Application). ICMP nằm trong gói tin IP và nó không chứa header của tầng Application. Trong khi đó Source Port và Destination Port được thêm vào header ở tầng Application. Các phần mềm mạng tự động phiên dịch thông điệp của ICMP, không cần Port để chuyển hướng thông điệp đó đến một quy trình của tầng ứng dụng (tức là tầng Application).

3. Với gói tin ICMP request, thực hiện yêu cầu:

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

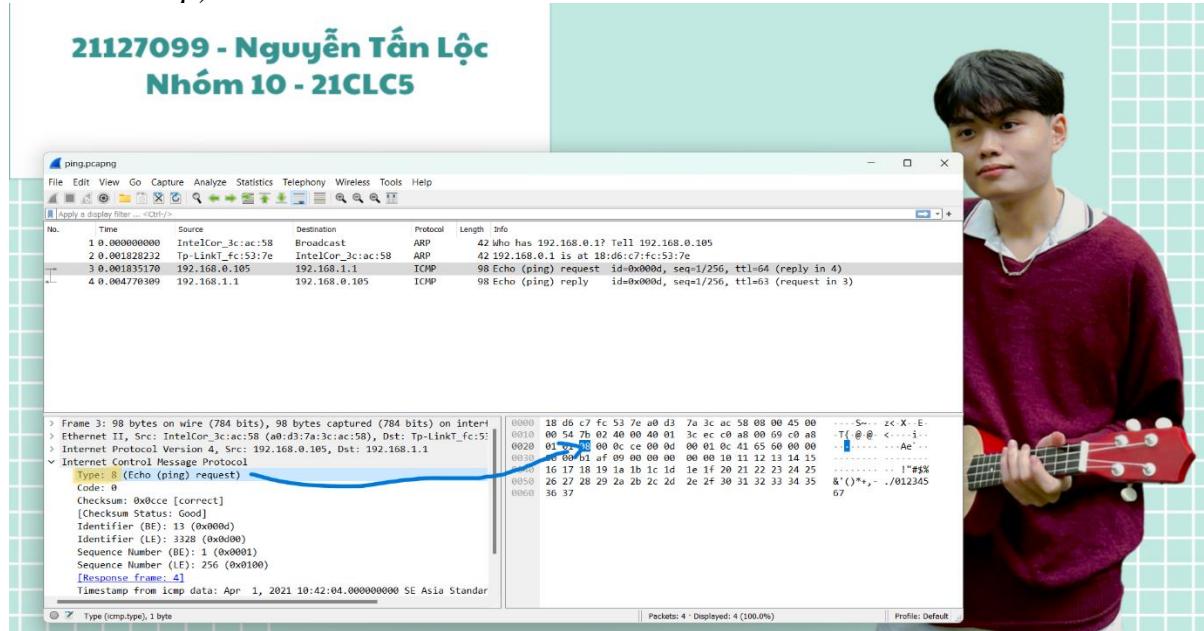
48 bytes	16 bytes	20 bytes	14 bytes
ICMP data	ICMP header	IP header	Ethernet header

- ICMP data: 48 bytes



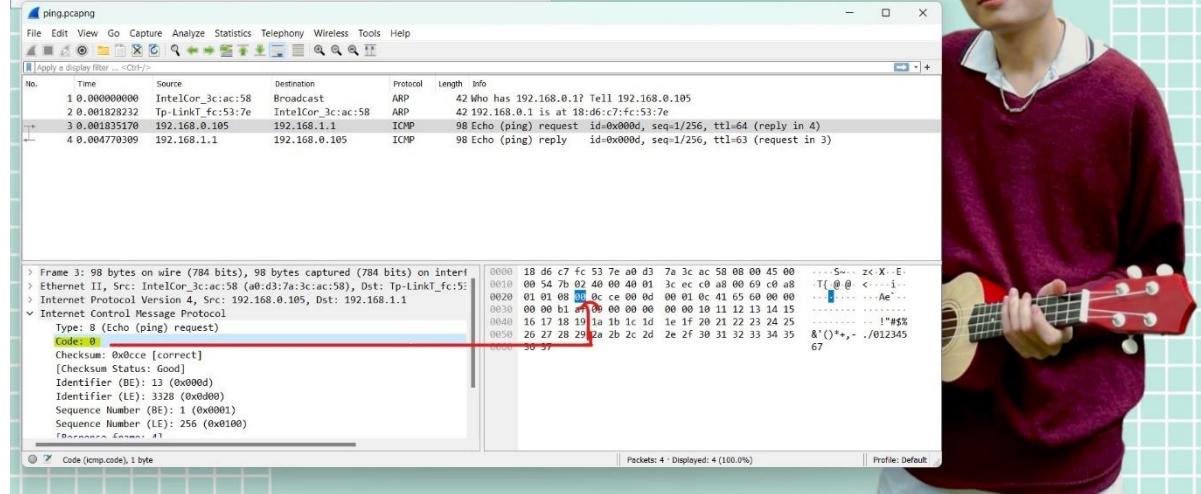
Hình 1.2: Kích thước của ICMP data (48 bytes)

- ICMP header: 64 bytes tổng – 48 bytes = 16 bytes (Kích thước của ICMP Header gồm các phần: Type, Code, Checksum, Identifier, Sequence number, timestamp)



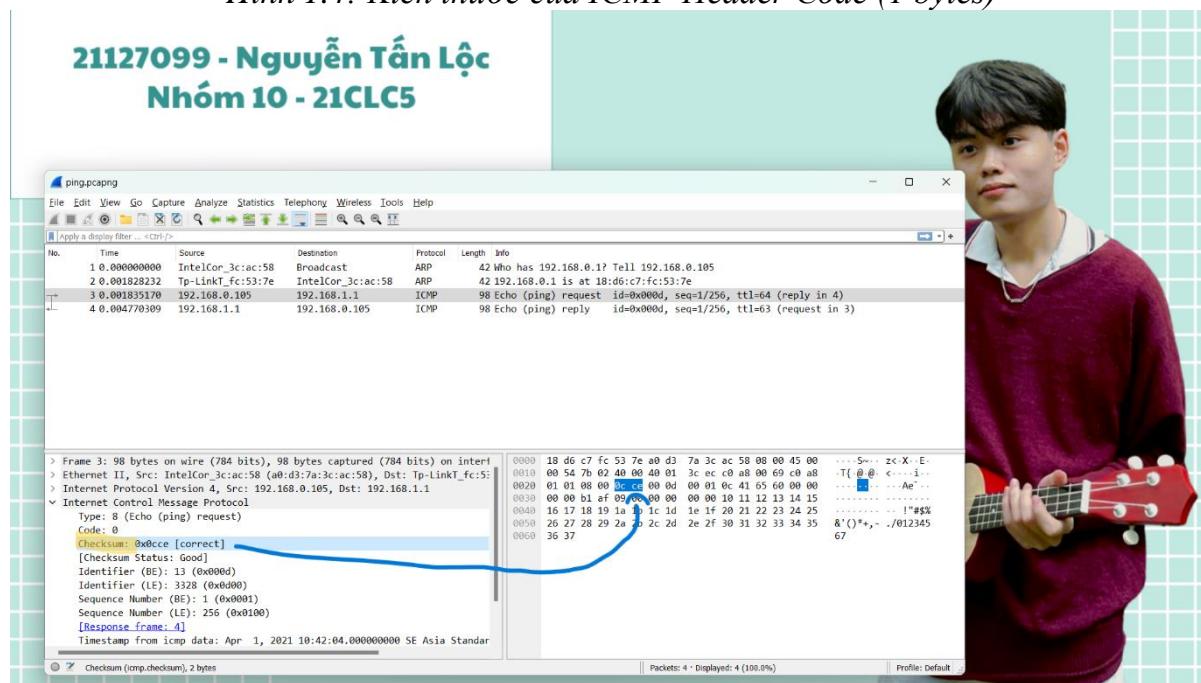
Hình 1.3: Kích thước của ICMP Header Type (1 bytes)

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



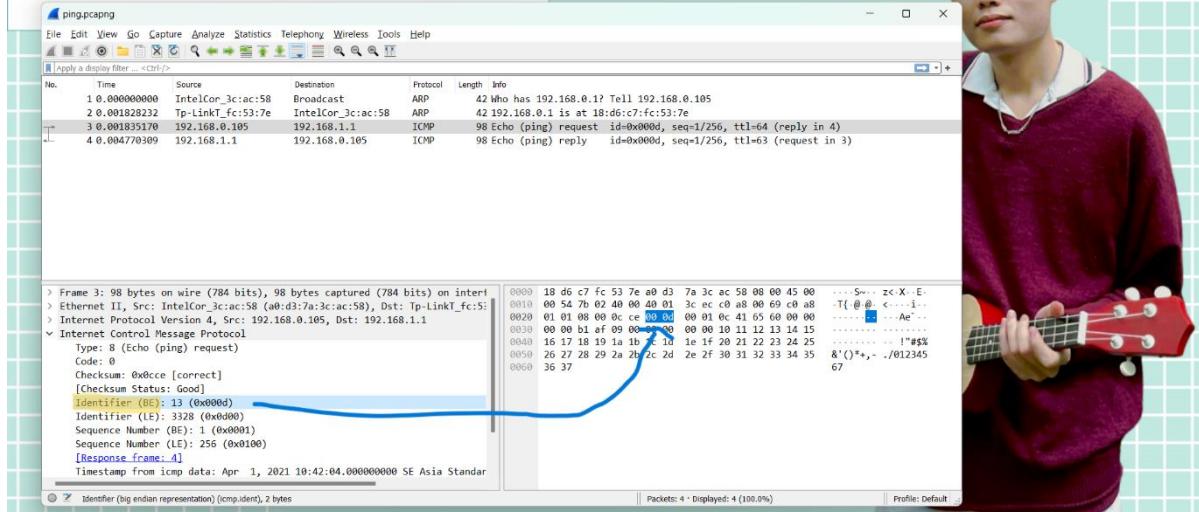
Hình 1.4: Kích thước của ICMP Header Code (1 bytes)

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



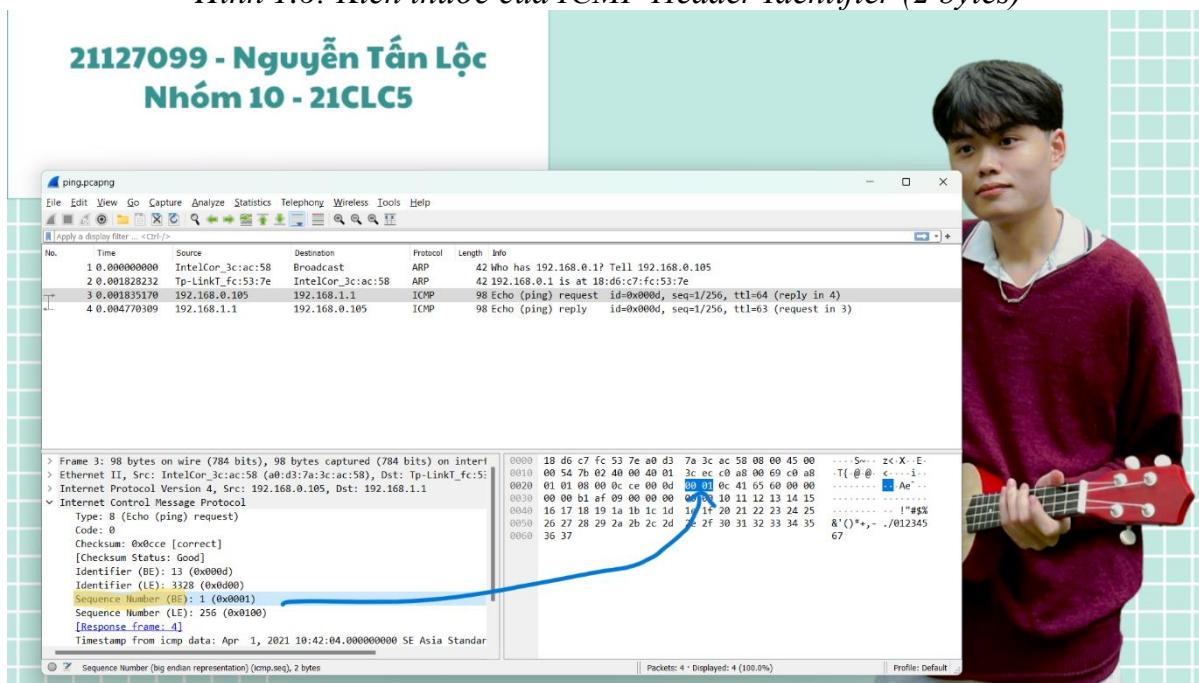
Hình 1.5: Kích thước của ICMP Header Checksum (2 bytes)

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



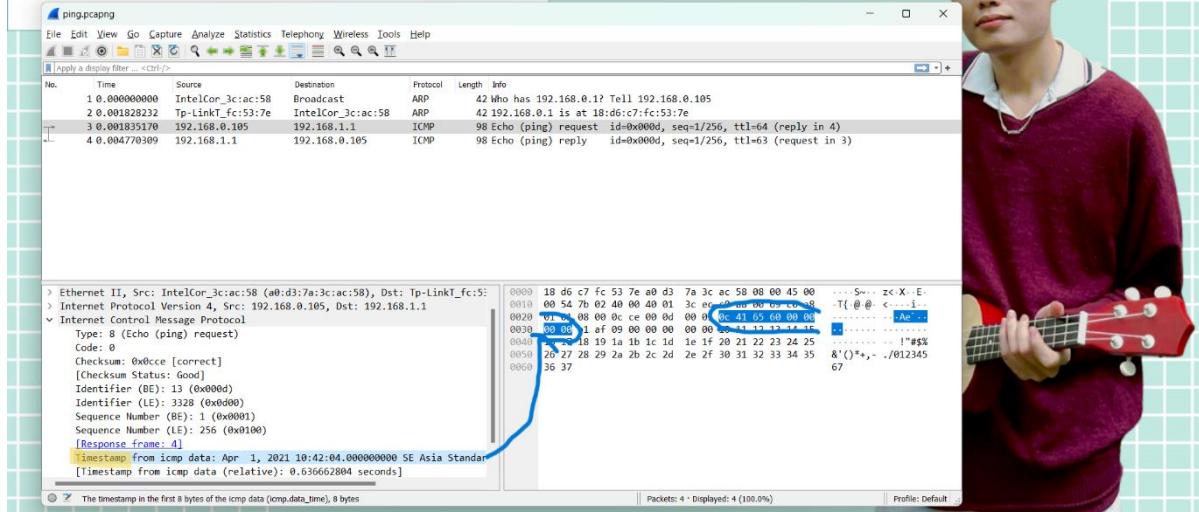
Hình 1.6: Kích thước của ICMP Header Identifier (2 bytes)

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



Hình 1.7: Kích thước của ICMP Header Sequence Number (2 bytes)

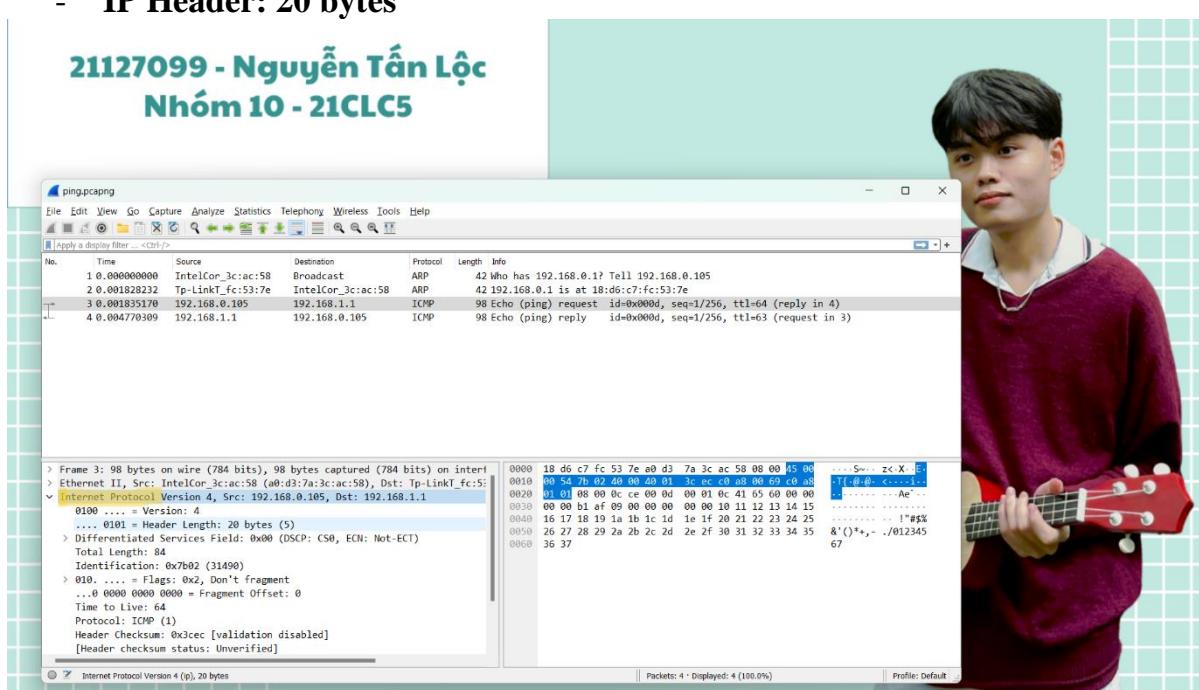
21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



Hình 1.8: Kích thước của ICMP Header Timestamp (8 bytes)

- IP Header: 20 bytes

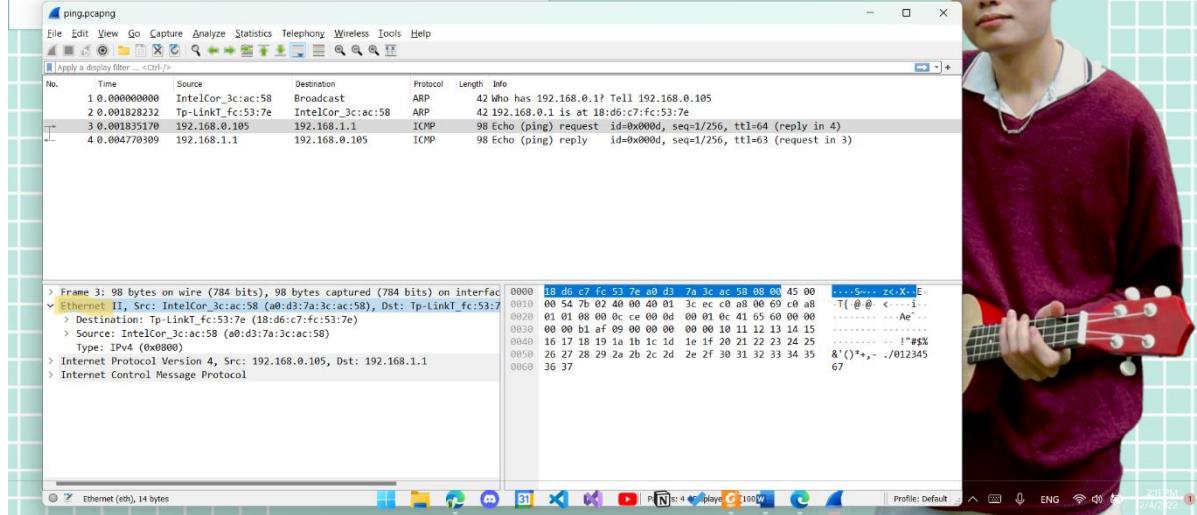
21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



Hình 1.9: Kích thước của IP Header (20 bytes)

- Ethernet header: 14 bytes

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5

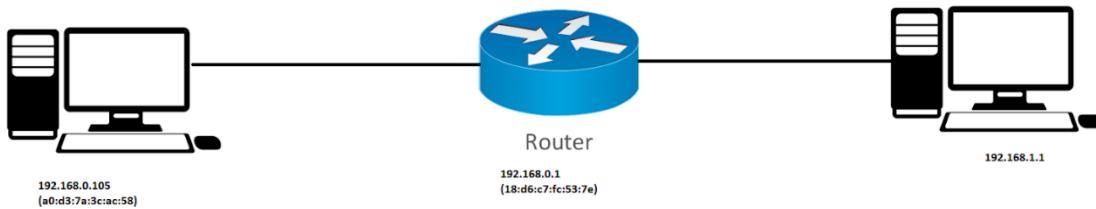


Hình 1.10: Kích thước của Ethernet Header (14 bytes)

- 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. ARP được các host trên mạng sử dụng để phân giải địa chỉ IP thành địa chỉ MAC. Để máy chủ A có địa chỉ IP là 192.168.0.105 (Source Host) muốn ping qua được máy chủ B có địa chỉ là 192.168.1.1(Destination Host) ở ngoài đường mạng thì nó cần phải thông qua router. Ở gói tin ARP thứ nhất thì máy chủ A có địa chỉ 192.168.0.105 sẽ gửi ARP request chứa IP router (192.168.0.1) theo kiểu broadcast đi trong đường mạng để tìm kiếm địa chỉ MAC của router do Source Host chưa biết địa chỉ MAC của router. Còn gói ARP thứ hai là khi đã nhận được đúng địa chỉ của router thì router sẽ trả về địa chỉ MAC của nó lại cho máy chủ A là máy chủ có Source Host. Tới đây máy chủ A mới có thể thực hiện ping ra đường mạng ngoài.

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



Hình 1.11: Sơ đồ logic của đường mạng

Bài 2: UDP (2.5d)

- Mở Wireshark và tiến hành bắt gói tin trên card mạng (có kết nối internet)
- Mở dòng lệnh và thực hiện lệnh sau: **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`
- Hãy trả lời các câu hỏi sau:
 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 www.fit.hcmus.edu.vn** có ý nghĩa: thực hiện truy vấn một miền cục bộ trên mạng riêng của mình và truy vấn đó là: gửi cho tôi địa chỉ IP của máy chủ: www.fit.hcmus.edu.vn
 - Dòng lệnh có dòng “non-authoritative answer”, có nghĩa rằng nó không cấu hình miền nhưng vẫn có thể cung cấp hồi đáp.



Hình 2.1: Thực hiện câu lệnh nslookup www.fit.hcmus.edu.vn

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 hình minh chứng bằng gói tin bắt được**

- UDP có tổng cộng 4 trường

Tên trường thông tin	Kích thước
Source Port	2 bytes
Destination Port	2 bytes
Length	2 bytes
Checksum	2 bytes

- Hình minh chứng:



21127168 - Bùi Phước Thiện

No.	Time	Source	Destination	Protocol	Length	Info
793 5.429575		192.168.0.1	192.168.0.102	DNS	152	Standard query reson
2162 13.209809		192.168.0.102	192.168.0.1	DNS	84	Standard query 0x0001
2164 13.216263		192.168.0.1	192.168.0.102	DNS	144	Standard query reson
2165 13.218454		192.168.0.102	192.168.0.1	DNS	80	Standard query 0x0002
2169 13.228254		192.168.0.1	192.168.0.102	DNS	161	Standard query reson
2170 13.231983		192.168.0.102	192.168.0.1	DNS	80	Standard query 0x0003
2176 13.243537		192.168.0.1	192.168.0.102	DNS	165	Standard query reson
2518 15.761004		192.168.0.102	192.168.0.1	DNS	75	Standard query 0x0084
2519 15.761239		192.168.0.102	192.168.0.1	DNS	75	Standard query 0x51fa

> Frame 2165: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{0B37E^
> Ethernet II, Src: IntelCor_bb:e7:ac (18:1d:ea:bb:e7:ac), Dst: TP-Link_cf:9e:74 (5c:a6:e6:cfc:9e:74)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 54969, Dst Port: 53
Source Port: 54969
Destination Port: 53
Length: 46
Checksum: 0x0784 [unverified]

0000 5c a6 e6 cf 9e 74 18 1d ea bb e7 ac 08 00 45 00 \....t.....E.
0001 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 01 B.....+....F.
0002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ..5.....
0003 00 00 00 00 00 00 00 03 77 77 03 66 69 74 05 68w.w fit.h
0040 63 6d 75 73 03 65 64 75 02 76 6e 00 00 01 00 01 cmus.edu.vn.....

Hình 2.2: Source Port: 54969



21127168 - Bùi Phước Thiện

No.	Time	Source	Destination	Protocol	Length	Info
793 5.429575		192.168.0.1	192.168.0.102	DNS	152	Standard query reson
2162 13.209809		192.168.0.102	192.168.0.1	DNS	84	Standard query 0x0001
2164 13.216263		192.168.0.1	192.168.0.102	DNS	144	Standard query reson
2165 13.218454		192.168.0.102	192.168.0.1	DNS	80	Standard query 0x0002
2169 13.228254		192.168.0.1	192.168.0.102	DNS	161	Standard query reson
2170 13.231983		192.168.0.102	192.168.0.1	DNS	80	Standard query 0x0003
2176 13.243537		192.168.0.1	192.168.0.102	DNS	165	Standard query reson
2518 15.761004		192.168.0.102	192.168.0.1	DNS	75	Standard query 0x0084
2519 15.761239		192.168.0.102	192.168.0.1	DNS	75	Standard query 0x51fa

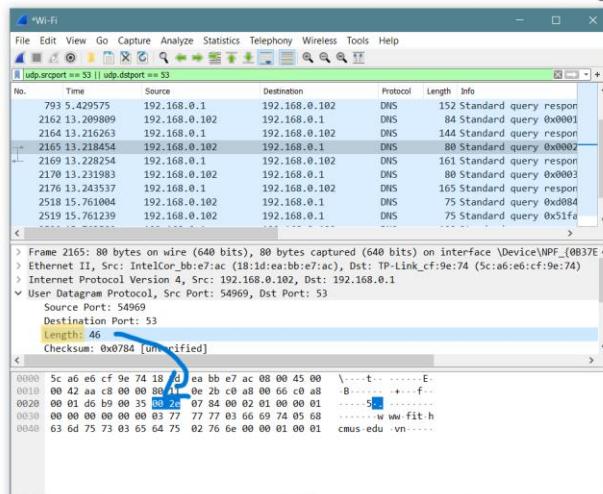
> Frame 2165: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{0B37E^
> Ethernet II, Src: IntelCor_bb:e7:ac (18:1d:ea:bb:e7:ac), Dst: TP-Link_cf:9e:74 (5c:a6:e6:cfc:9e:74)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 54969, Dst Port: 53
Source Port: 54969
Destination Port: 53
Length: 46
Checksum: 0x0784 [unverified]

0000 5c a6 e6 cf 9e 74 18 1d ea bb e7 ac 08 00 45 00 \....t.....E.
0001 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 01 B.....+....F.
0002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ..5.....
0003 00 00 00 00 00 00 00 03 77 77 03 66 69 74 05 68w.w fit.h
0040 63 6d 75 73 03 65 64 75 02 76 6e 00 00 01 00 01 cmus.edu.vn.....

Hình 2.3: Destination Port: 53



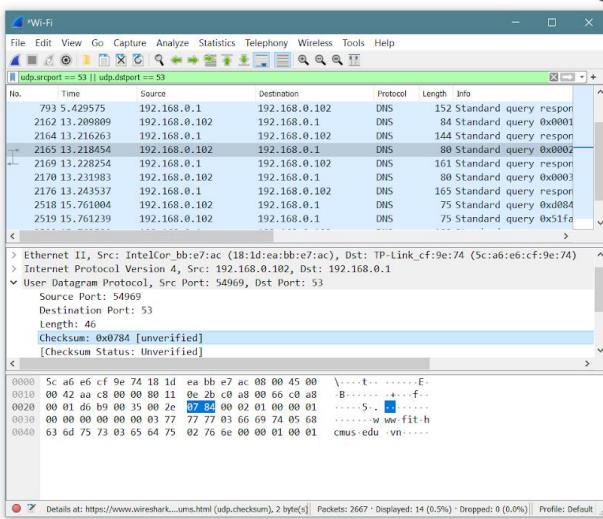
21127168 - Bùi Phước Thiện



Hình 2.4: Length: 46



21127168 - Bùi Phước Thiện



Hình 2.5: Checksum: 0x0784 [unverified]

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?

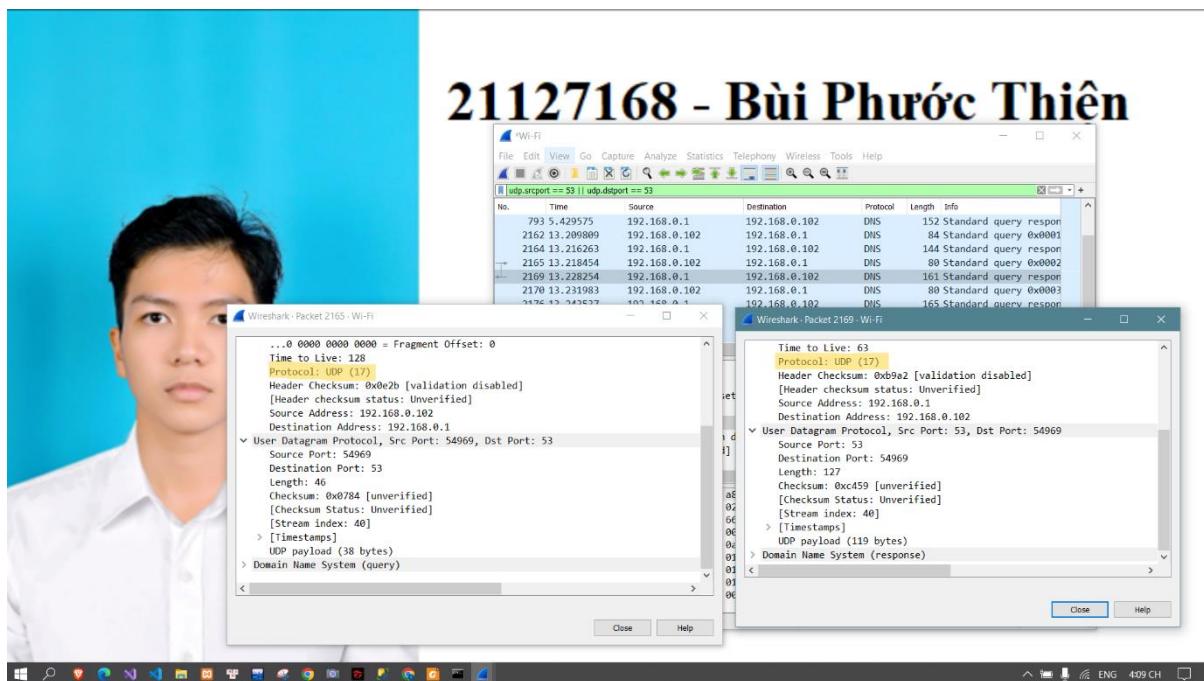
- Trường: Length trong header UDP.
- Giá trị hợp lệ của trường Length trong trường hợp tổng quát: từ 8 - 65535
- Giá trị: $46 = 2 * 16^1 + e * 16^0$
- Đơn vị: byte

- Trường này đang nói đến: kích thước của toàn bộ một datagram (gồm phần header và payload)

- Nếu gói tin chỉ có header, không có payload thì length cần có tối thiểu 8 bytes

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

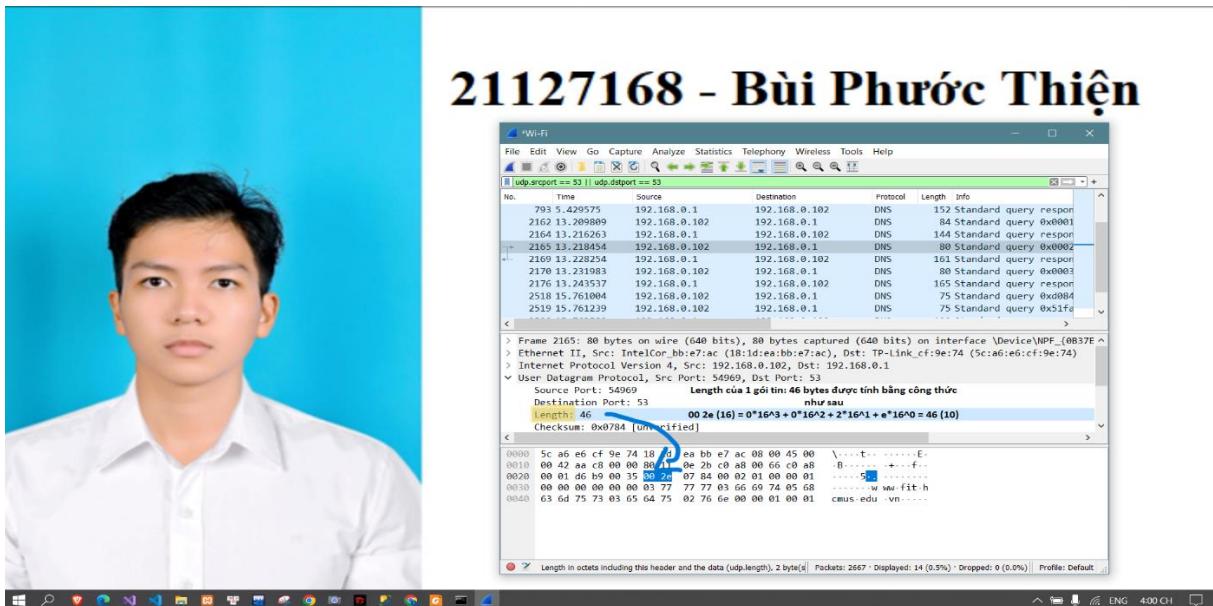
- Protocol number của UDP trong thập phân: 17
- Protocol number của UDP trong thập lục phân: 0x11 hex



Hình 2.6: Protocol Number: 17(10) = 0x11(16)

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)

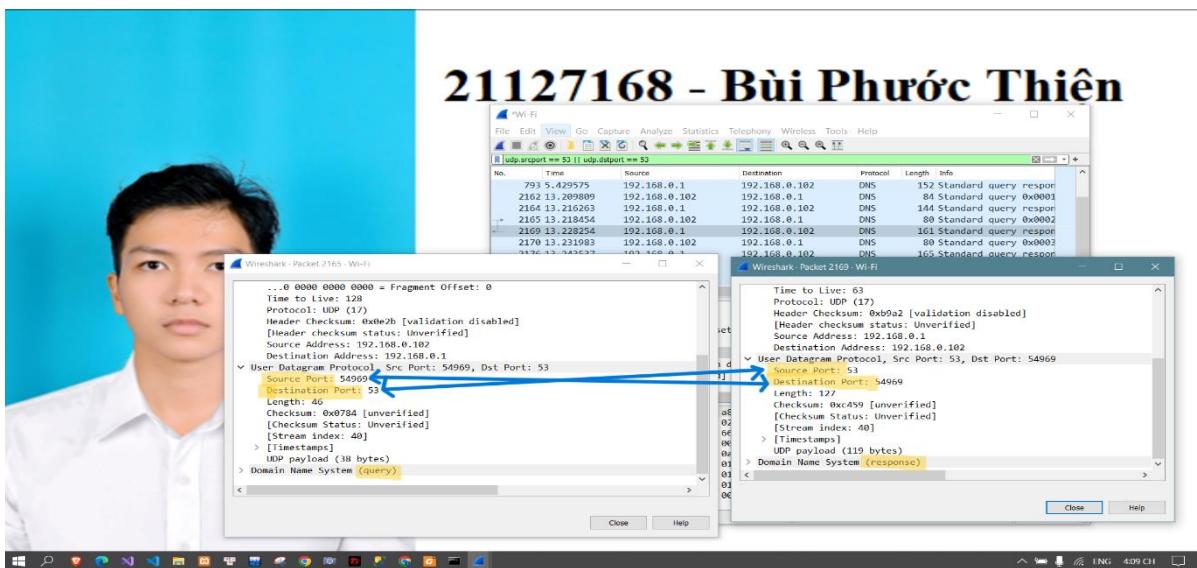
- Length được biểu diễn theo hệ cơ số 16 (00 2e).
 - Số lớn nhất trong hệ cơ số 16 có 4 chữ số là FFFF (16).
 - Length sẽ cho biết toàn bộ kích thước của datagram
- ⇒ Kích thước lớn nhất của datagram sẽ là 65535 (bytes).
- ⇒ Lượng dữ liệu tối đa có thể đưa vào UDP Payload = 65535 - 8 = 65527 (bytes)
 (trừ đi 8 bytes phải có ở phần Header)



Hình 2.7: Length

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

- Gói tin lọc được gồm 2 loại:
 - o Gói tin gửi đi (query) gửi từ Client (Source Port bất kì) đến DNS Server (có Port là 53).
 - o Gói tin phải hồi (response) gửi từ DNS Server (có port là 53) đến Client (có Port có giá trị giống như Source Port của gói tin gửi đi: query)
- Nói cách khác, Source Port của gói tin gửi đi (query) cũng là Destination Port của gói tin phải hồi (response). Ngược lại, Source Port của gói tin phải hồi (response) cũng là Destination Port của gói tin gửi đi (query)



Hình 2.8: Mối quan hệ giữa 2 gói tin gửi đi và gói tin phản hồi

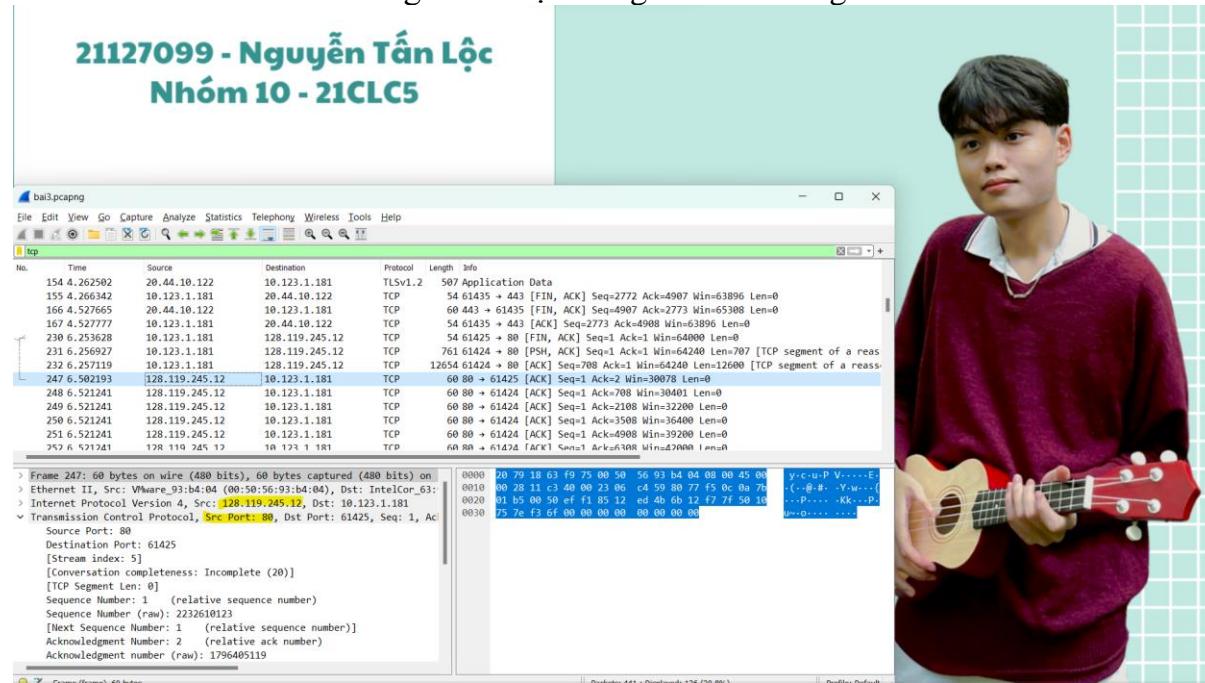
Bài 3: HTTP (2.5d)

- 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
- Dừng quá trình bắt gói tin và lọc ra những gói tin gửi đi hoặc gửi đến máy chủ gaia.cs.umass.edu

Hãy trả lời các câu hỏi sau:

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
- TCP Port number để gửi và nhận các gói tin TCP segment: 80.

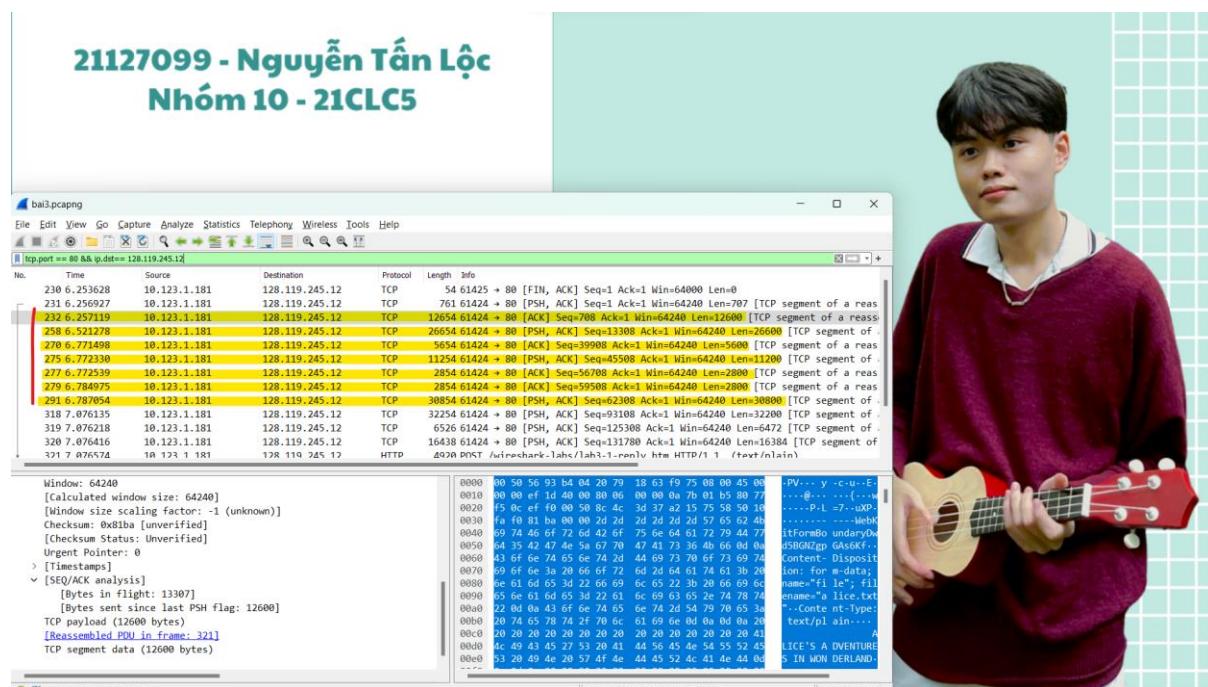


Hình 3.1: Thông tin địa chỉ IP của máy chủ và port dịch vụ

2. Tìm 7 TCP segments tiếp theo, tính từ TCP segment của HTTP POST đầu tiên ở câu 2 và trả lời những câu hỏi sau

a. Cho biết No. của 7 TCP segments đó

- No. 232
- No. 258
- No. 270
- No. 275
- No. 277
- No. 279
- No. 291

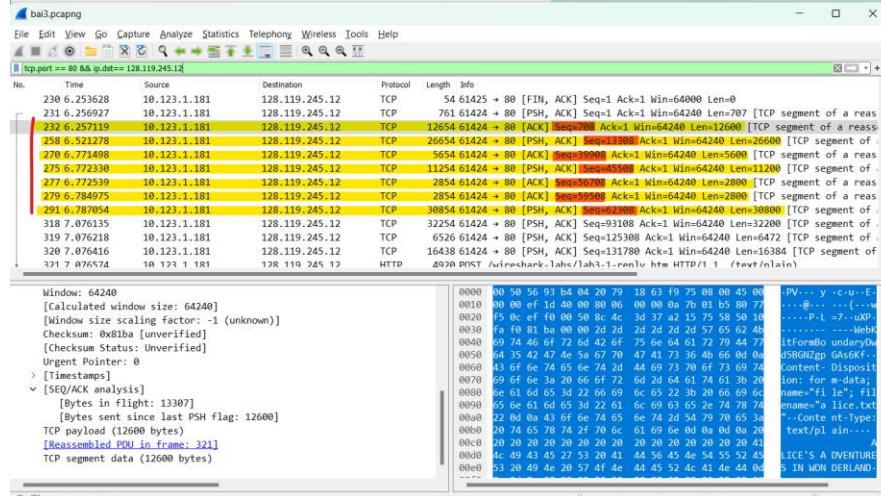


Hình 3.2: No. của các Segments

b. Cho biết sequence number của 7 TCP segments đó

- No. 232: 708
- No. 258: 13308
- No. 270: 39908
- No. 275: 45508
- No. 277: 56708
- No. 279: 59508
- No. 291: 62308

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5

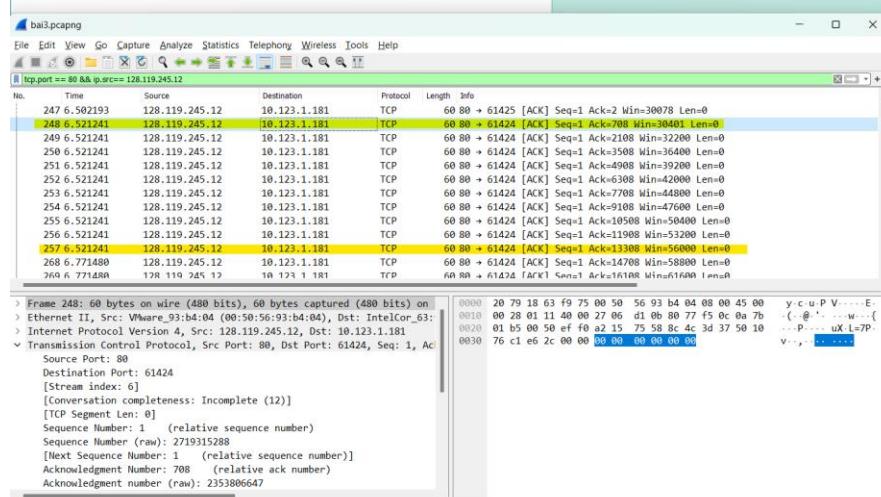


Hình 3.3: Sequence Number của 7 TCP đó

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

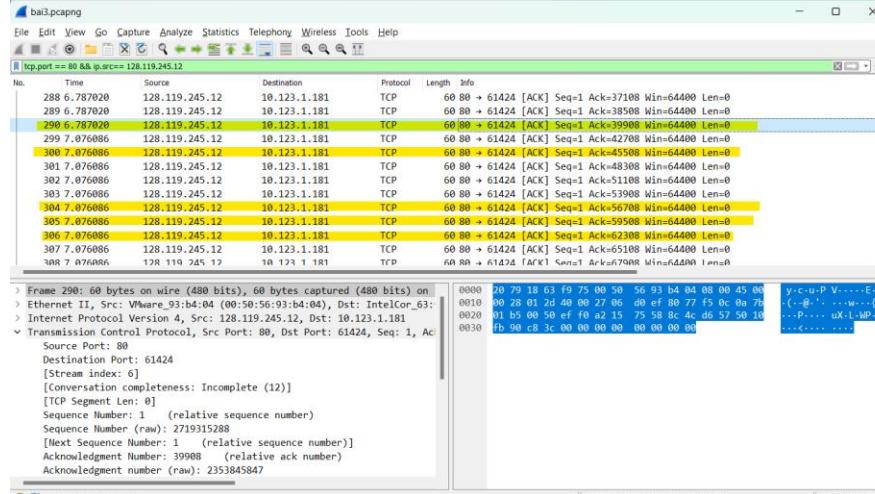
- No. 248 tương ứng với No 232
- No. 257 tương ứng với No 258
- No. 290 tương ứng với No 270
- No. 300 tương ứng với No 275
- No. 304 tương ứng với No 277
- No. 305 tương ứng với No 279
- No. 306 tương ứng với No 291

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



Hình 3.4: No. ACK báo nhận của các Segments (1)

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5

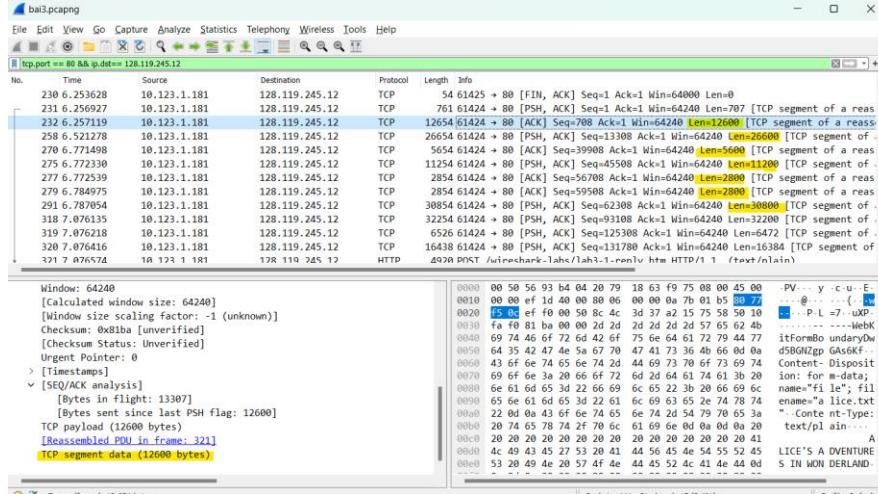


Hình 3.5: Số ACK báo nhận của các Segments (2)

d. Lượng data gửi trong mỗi TCP segment đó

- Lượng data tính bằng đơn vị byte
- Số 232: 12600 bytes
- Số 258: 26600 bytes
- Số 270: 5600 bytes
- Số 275: 11200 bytes
- Số 277: 2800 bytes
- Số 279: 2800 bytes
- Số 291: 30800 bytes

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



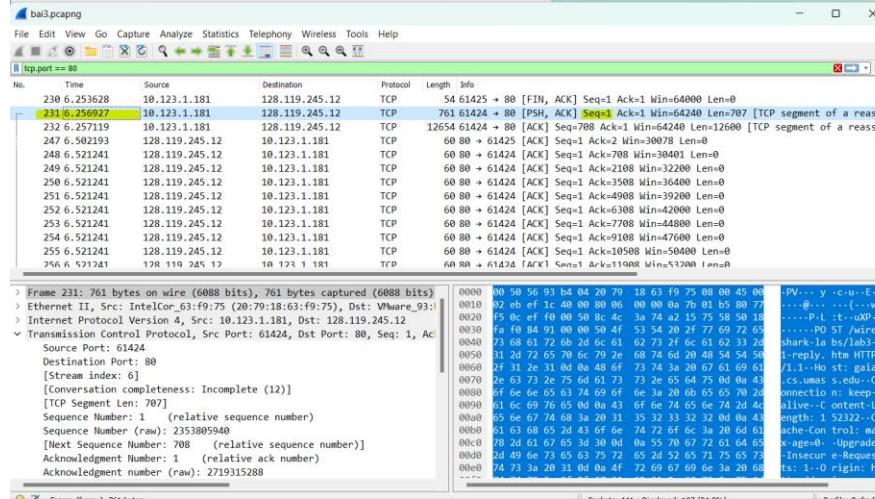
Hình 3.6: Lượng data gửi trong mỗi Segment

3. Cho biết throughput (bytes transferred per unit time) cho kết nối upload

file này, vui lòng cho biết cách tính

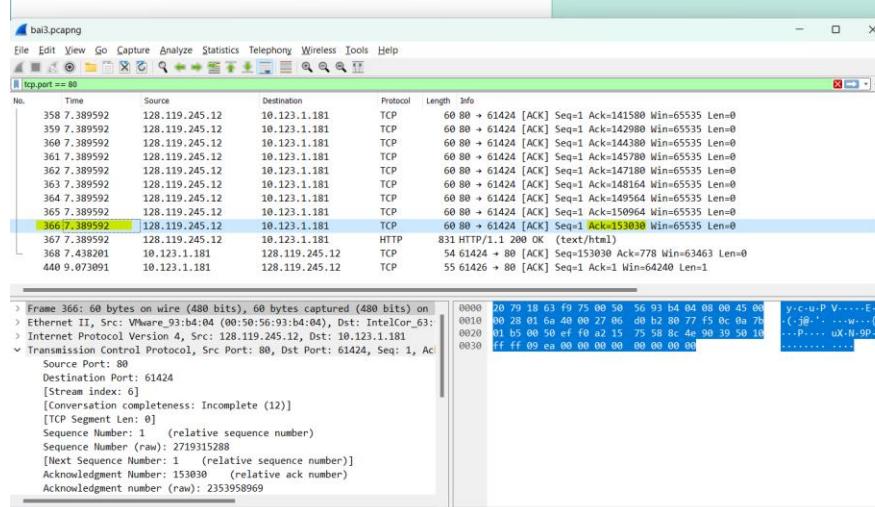
- Việc tính toán throughput TCP phần lớn phụ thuộc vào việc lựa chọn khoảng thời gian trung bình. Chọn khoảng thời gian trung bình là toàn bộ thời gian kết nối. Sau đó, throughput trung bình cho kết nối TCP này được tính bằng tỷ lệ giữa tổng lượng dữ liệu và tổng thời gian truyền. Tổng lượng dữ liệu được truyền có thể được tính bằng chênh lệch giữa Sequence Number của TCP Segment đầu tiên (No. 231) và ACK Number của ACK cuối cùng (No. 366). Do đó, tổng dữ liệu là $153030 - 1 = 153029$ -byte. Toàn bộ thời gian truyền là chênh lệch giữa thời gian của TCP đầu tiên (No. 231) và thời gian ACK cuối cùng (No. 366). Do đó, tổng thời gian truyền là $7.389592 - 6.256927 = 1.132665$ giây. Do đó, throughput cho kết nối TCP được tính là $153029 / 1.132665 = 135105.2606$ bytes/s.
- ⇒ Công thức tính Throughput=Total data/total time. (tổng dữ liệu truyền đi/tổng thời gian upload)

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5



Hình 3.7: TCP đầu tiên

21127099 - Nguyễn Tân Lộc Nhóm 10 - 21CLC5

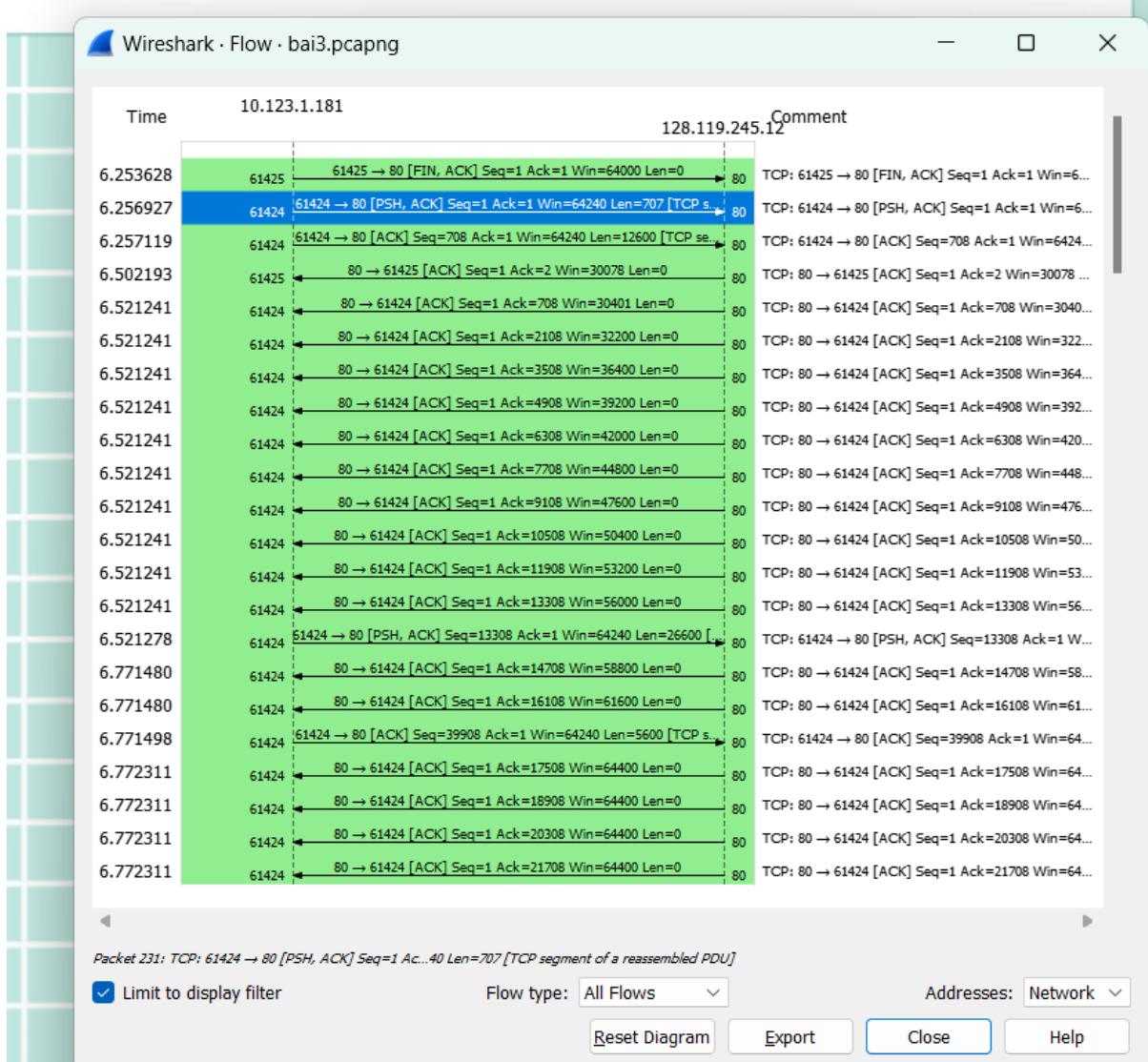


Hình 3.8: ACK cuối cùng

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

21127099 - Nguyễn Tân Lộc

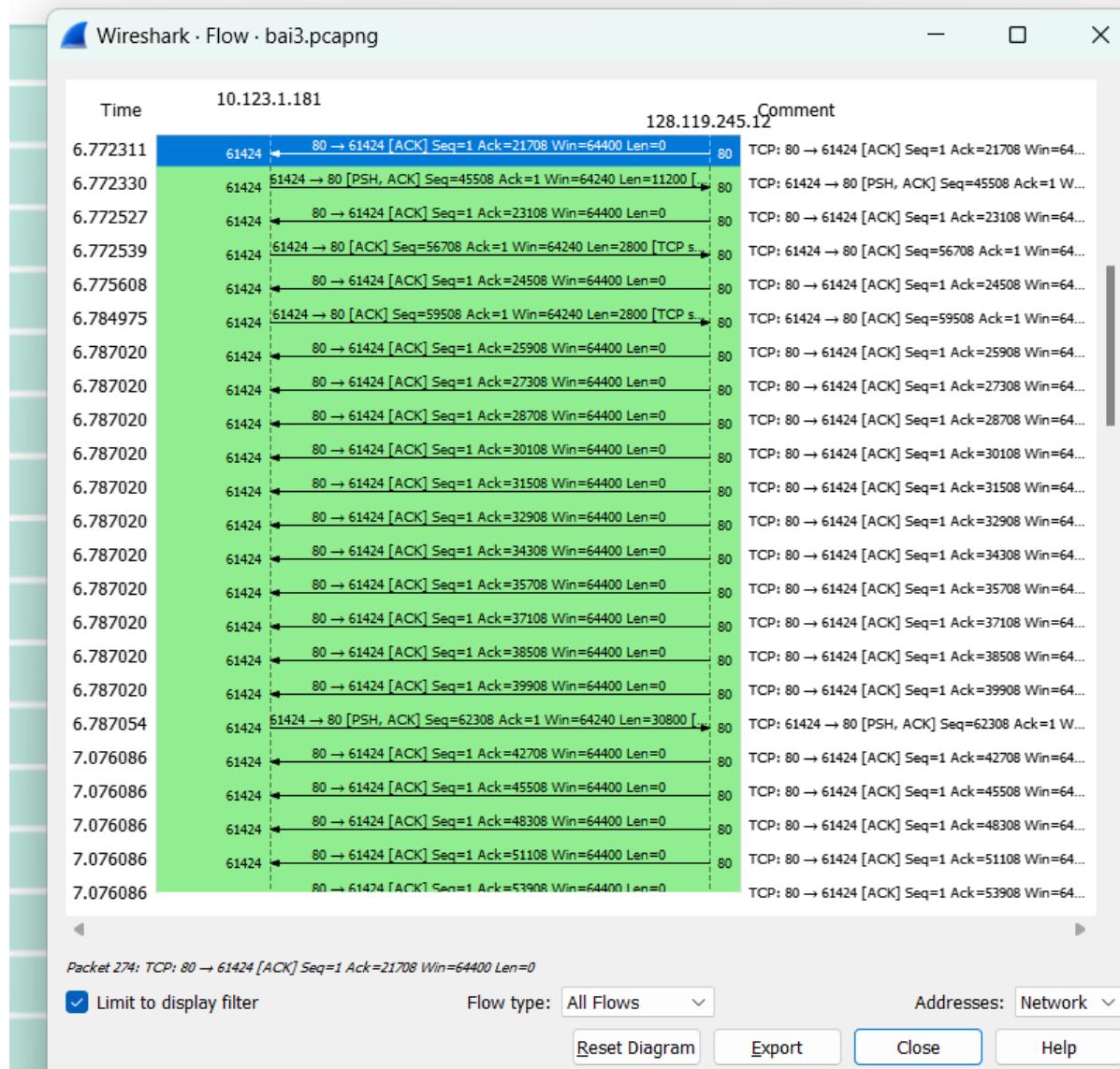
Nhóm 10 - 21CLC5



Hình 3.9: Quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (1)

21127099 - Nguyễn Tân Lộc

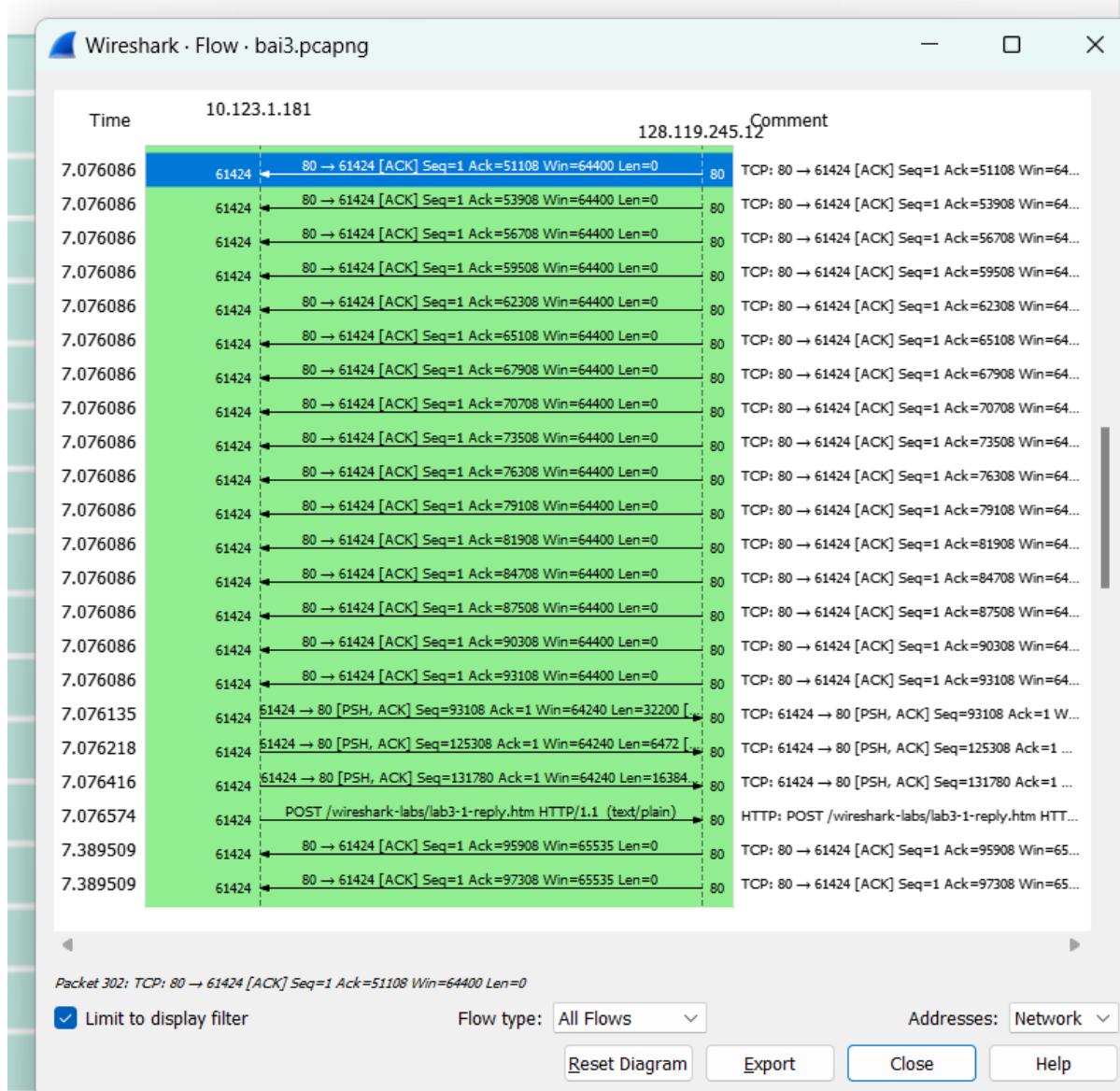
Nhóm 10 - 21CLC5



Hình 3.10: Quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (2)

21127099 - Nguyễn Tân Lộc

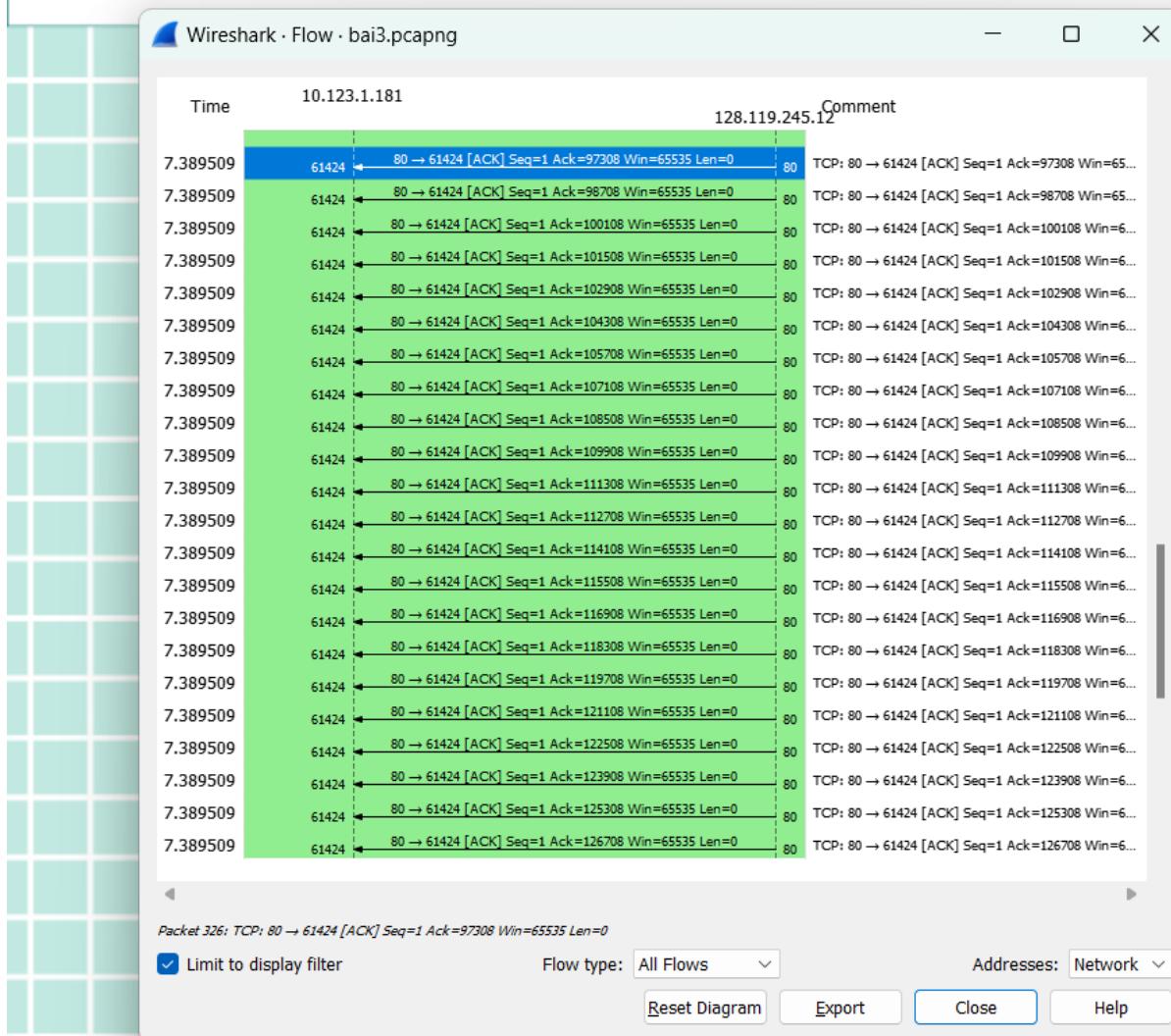
Nhóm 10 - 21CLC5



Hình 3.11: Quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (3)

21127099 - Nguyễn Tân Lộc

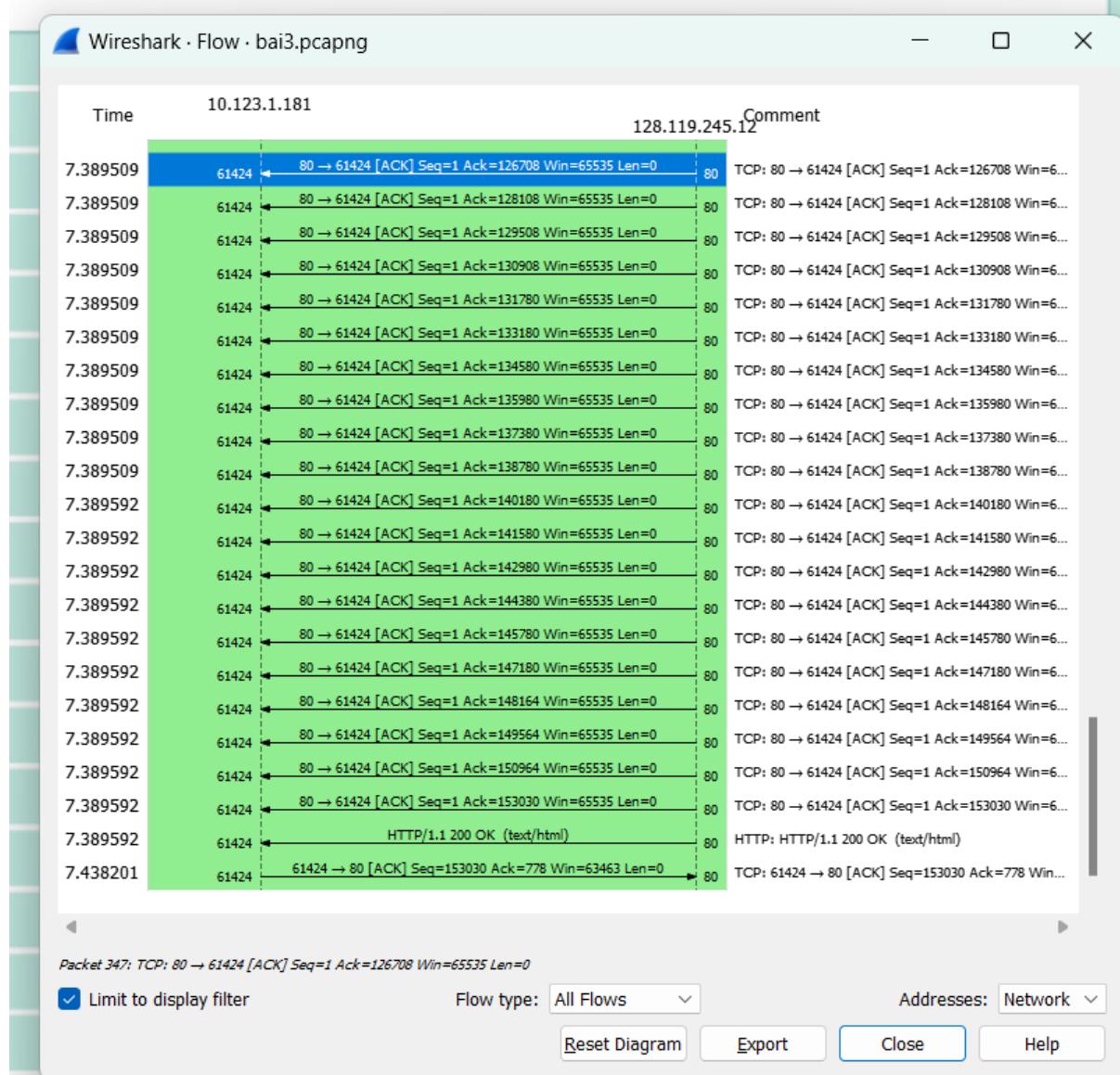
Nhóm 10 - 21CLC5



Hình 3.12: Quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (4)

21127099 - Nguyễn Tân Lộc

Nhóm 10 - 21CLC5

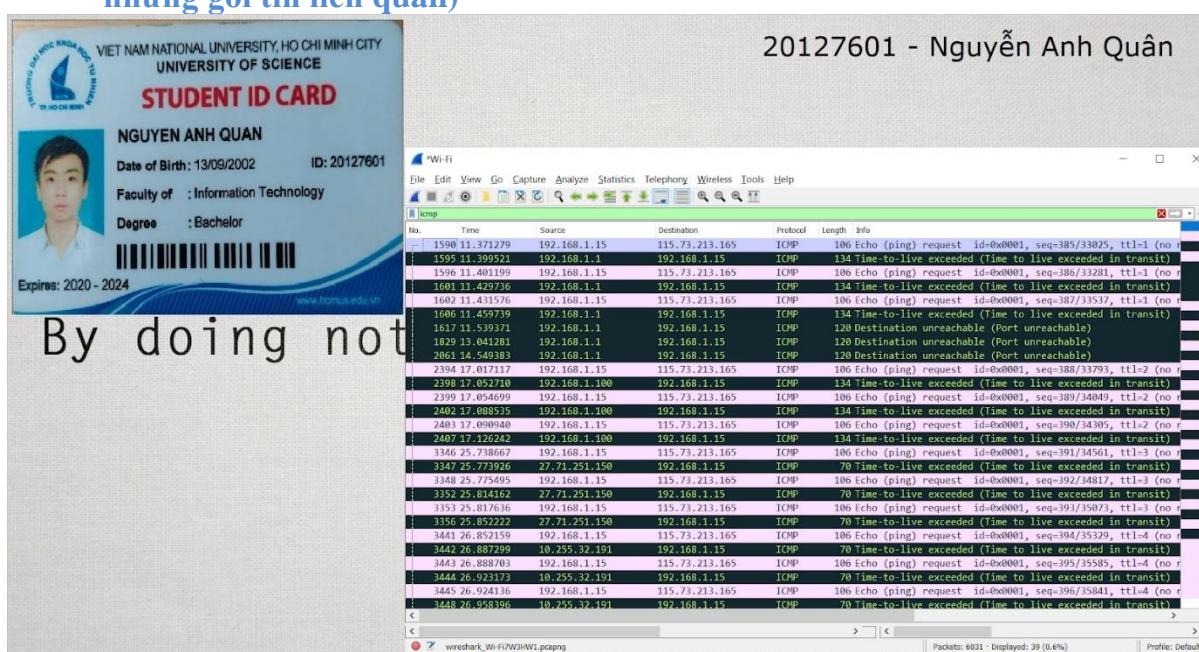


Hình 3.13: Quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (5)

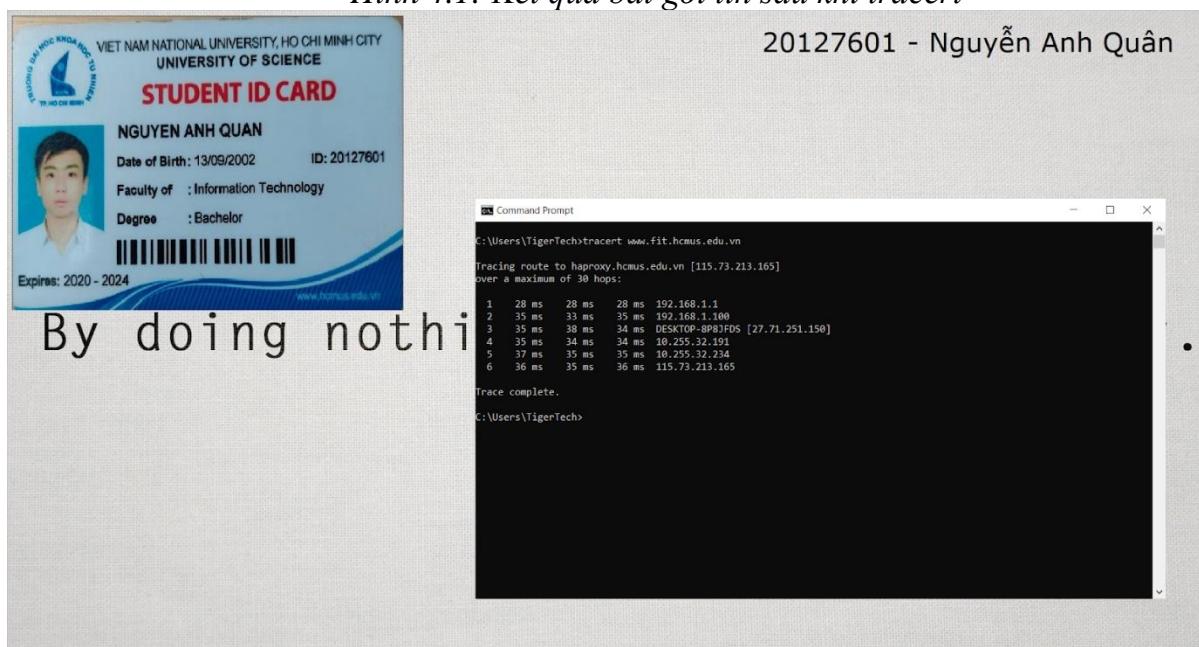
Bài 4: Traceroute (3d)

- Nếu bạn dùng Windows thì dùng lệnh **tracert**, nếu bạn dùng Unix/Linux/macOS thì bạn dùng lệnh **traceroute**. Lưu ý kết quả bắt gói tin trên Windows và Unix/Linux/macOS sẽ khác nhau, vì vậy câu trả lời phụ thuộc bạn dùng OS nào.
- Bật Wireshark để bắt gói tin lệnh **traceroute** từ máy của mình (có thể dùng máy ảo) đến www.fit.hcmus.edu.vn (FIT). Trả lời những câu hỏi sau:

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



Hình 4.1: Kết quả bắt gói tin sau khi tracerert



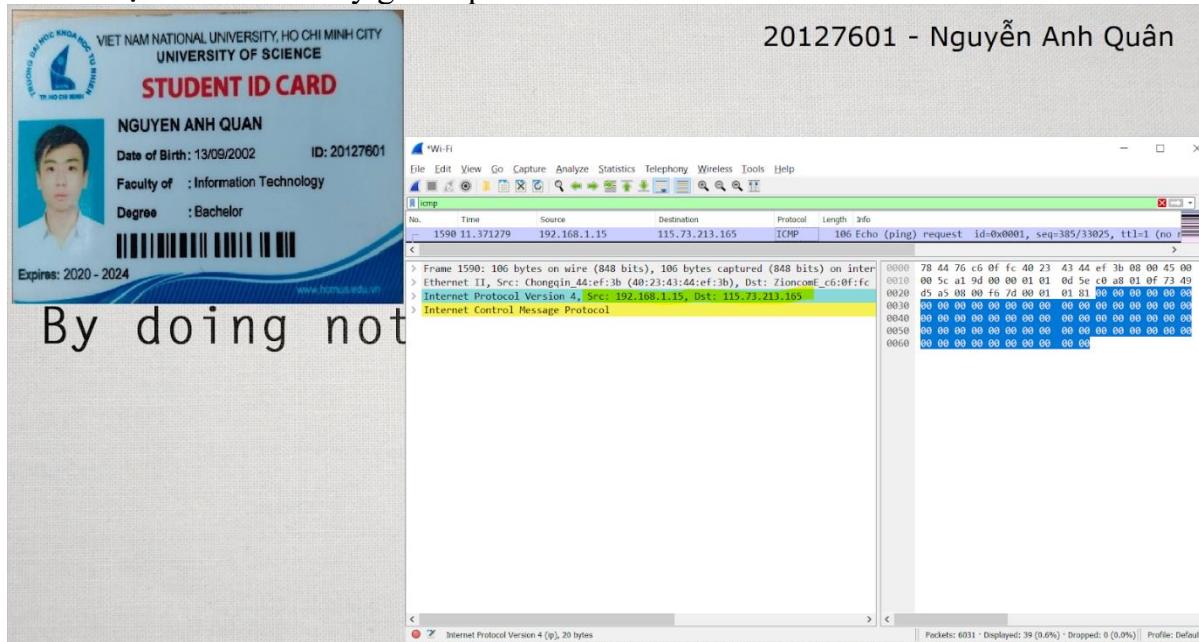
Hình 4.2: Thực hiện tracerert

2. Cho biết traceroute/tracert dùng để làm gì?

- Xác định đường đi từ nguồn tới đích hay kiểm tra đường đi của một gói tin IP . tạo các đường đi tối ưu
- Biết được tốc độ phản hồi khi gói tin đi qua các thiết bị tầng Network trên mạng
- Biết được số trạm, tên cụ thể các trạm mà gói tin đã đi qua trên đường tới đích . xem coi có trạm nào bị nghẽn không
- Nếu có trạm bị nghẽn thì kiểm xem có con đường nào khác để tiếp đến đích không

3. Cho biết địa chỉ IP của máy gửi request?

- Địa chỉ IP của máy gửi request là 192.168.1.15

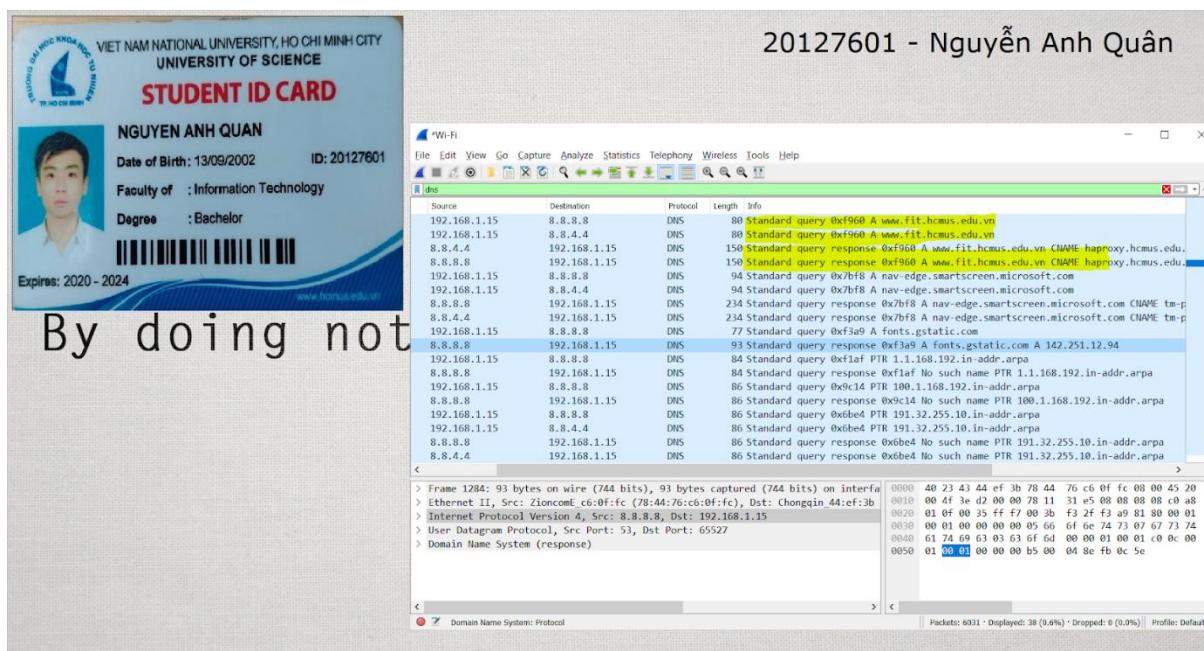


Hình 4.3: Địa chỉ IP của máy chủ request

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

- Bước 1: Người dùng sẽ gửi request tìm kiếm địa chỉ IP ứng với tên miền “www.fit.hcmus.vn” lên local DNS server.
- Bước 2: Local DNS server sẽ kiểm tra xem trong dữ liệu có sẵn, có địa chỉ IP nào được chuyển đổi từ tên miền giống với tên miền mà mình cần kiểm hay không.
- Bước 3: Nếu đã có rồi thì tiến thẳng tới bước 9. Nếu không có, local DNS server sẽ đi hỏi root DNS server và sang bước 4.
- Bước 4: Root DNS server sẽ trả lời local DNS server về DNS server quản lý tên miền “.vn”.
- Bước 5: Local DNS server sẽ đi hỏi DNS server quản lý tên miền “.vn” và nó sẽ trả lời local DNS server về DNS server quản lý tên miền “.edu.vn”.

- Bước 6: Local DNS server sẽ hỏi tiếp DNS server quản lý tên miền “.edu.vn” và nó sẽ trả lời Local DNS server về DNS server quản lý tên miền “hcmus.edu.vn”.
- Bước 7: Local DNS server sẽ hỏi tiếp DNS server quản lý tên miền “hcmus.edu.vn” và nó sẽ trả lời local DNS server về DNS server quản lý tên miền “fit.hcmus.edu.vn”.
- Bước 8: Local DNS server sẽ hỏi tiếp DNS server quản lý tên miền “fit.hcmus.edu.vn” và đó chính là server quản lý tên miền là “www.fit.hcmus.edu.vn”, nó sẽ trả lời thông tin về địa chỉ IP tương ứng của web đó cho local DNS server.
- Bước 9: Cuối cùng, local DNS server sẽ chuyển thông tin về cho người dùng.

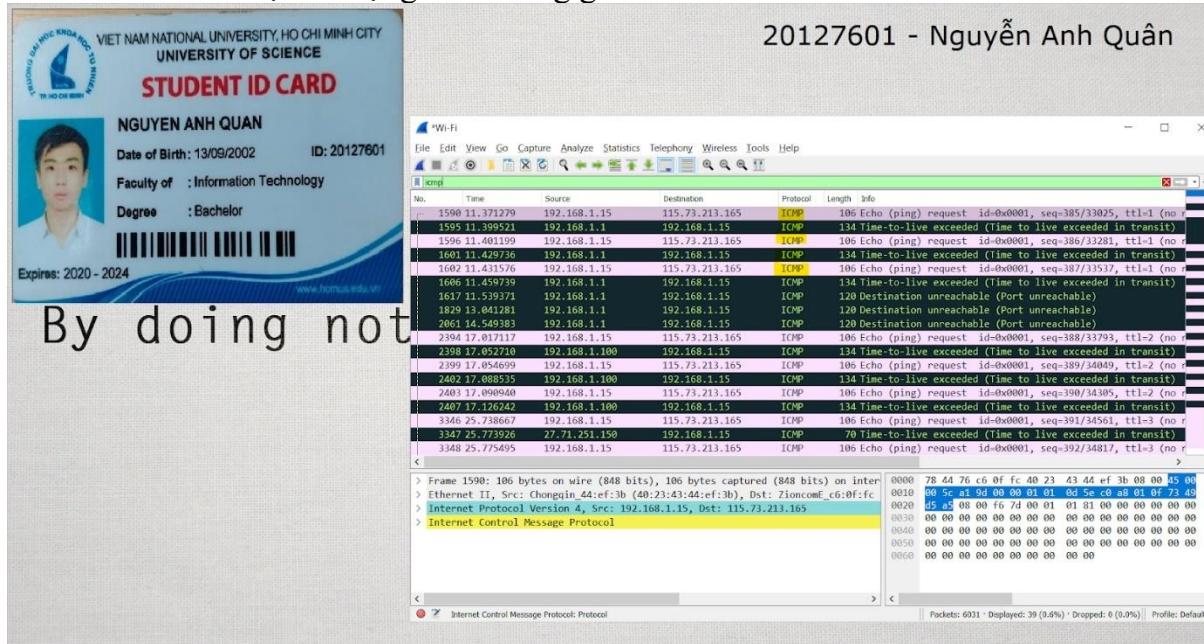


Hình 4.4: Hình minh họa

5. Sau khi xác định được IP của www.fit.hcmus.edu.vn, máy sẽ bắt đầu gửi gói tin đến FIT, trả lời những câu hỏi sau

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

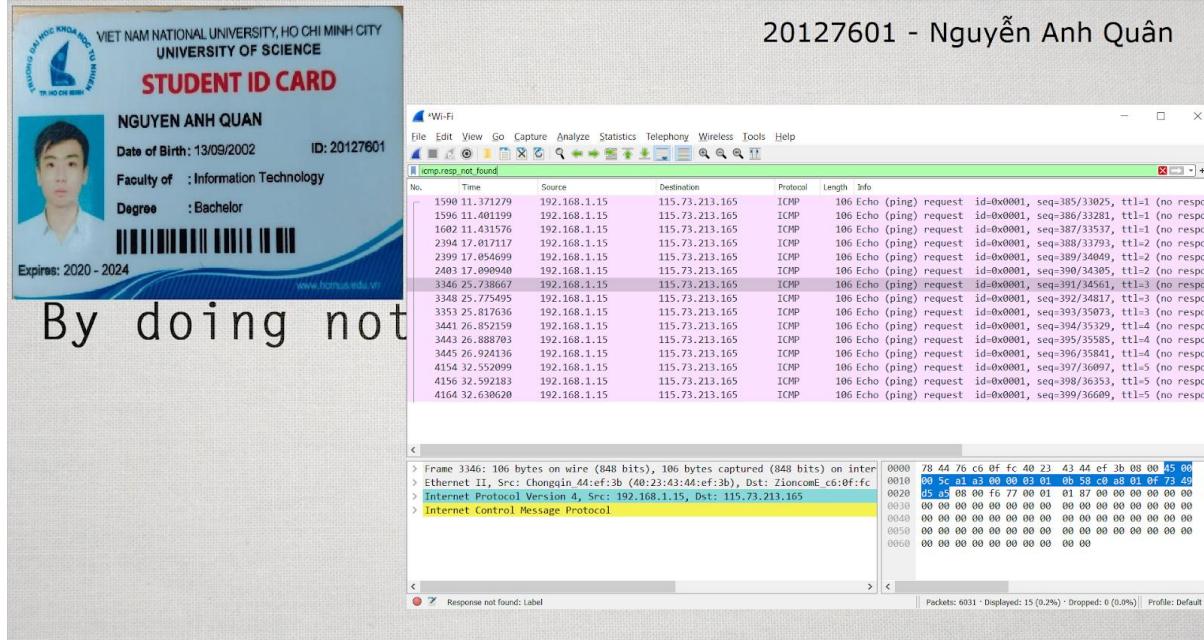
- Protocol được sử dụng của những gói tin sau đó là ICMP.



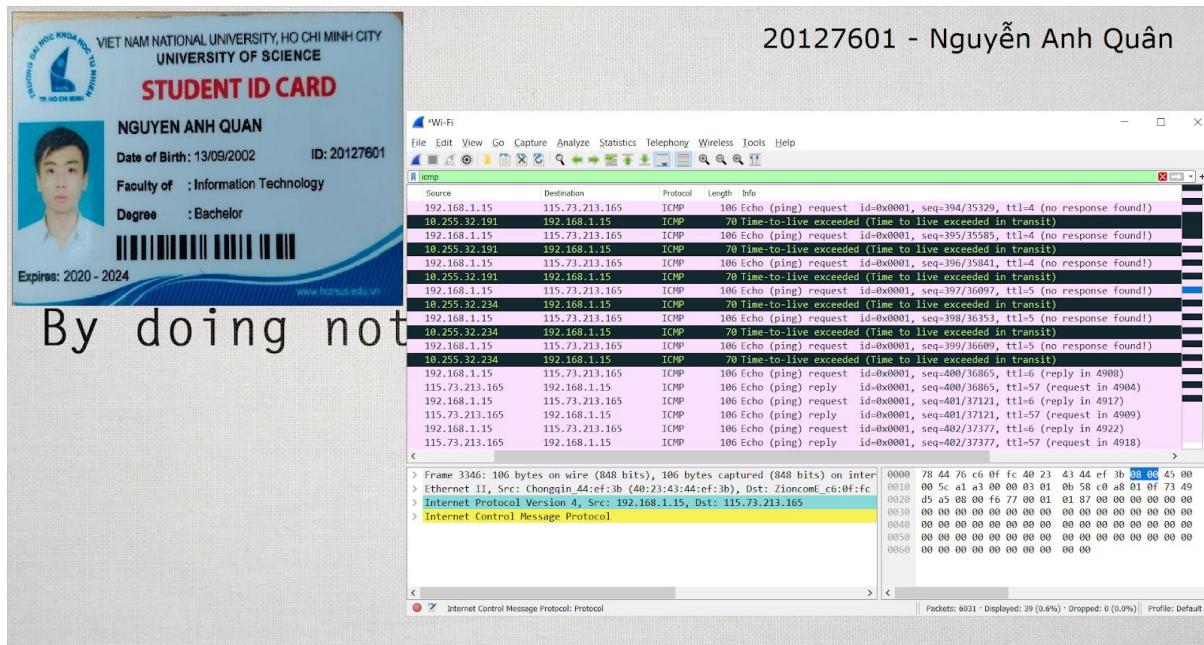
Hình 4.5: ICMP

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

- Có 15 gói tin được gửi đi trước khi nhận câu trả lời đầu tiên.



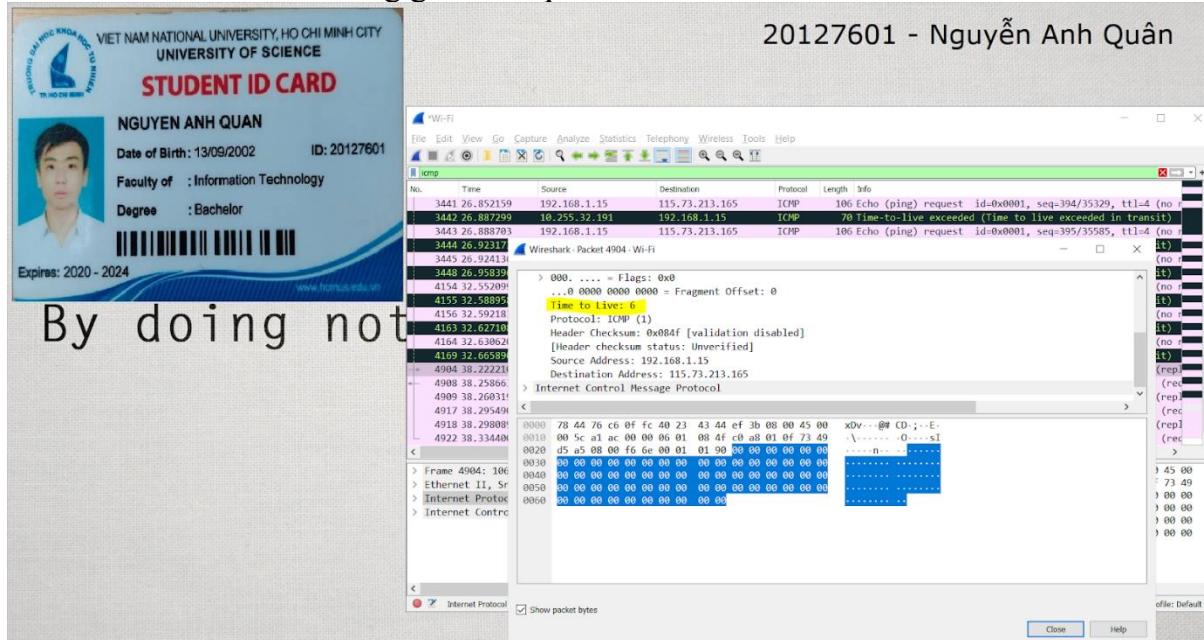
Hình 4.6: Số lượng gói tin chưa được gửi đi



Hình 4.7: Số lượng gói tin đã nhận phản hồi

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 response đầu tiên trả lời cho những gói tin request là: 6



Hình 4.8: TTL của gói tin

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?

- Trong các gói gửi đi thì không có thông tin của port xuất hiện. Tracert xác định đường đi đến một đích bằng cách gửi gói echo ICMP đến đó mà giao thức ICMP không có khái niệm về Port bởi nó được thiết kế để thực hiện giao tiếp thông tin trong tầng Network (ở lệnh tracert này thì nó được thể hiện dưới dạng tên các hop và chuyển sang các hop tiếp theo)

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

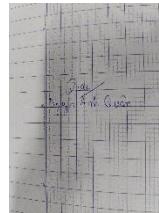
- Gói tin response đầu tiên là trả lời cho gói tin request thứ 4904.

The screenshot displays two windows. On the left is a "STUDENT ID CARD" for Nguyen Anh Quan, showing details like Date of Birth: 13/09/2002, Faculty of: Information Technology, Degree: Bachelor, and Expiry: 2020 - 2024. On the right is a Wi-Fi traffic capture window titled "icmp". The list shows several ICMP Echo requests (ping) from source 192.168.1.15 to destination 115.73.213.165, all with TTL=4. The first response (packet 4904) is highlighted in pink, indicating it is the first reply to a request. The packet details show it is an ICMP Echo reply (id=0x0001, seq=400/36865, ttl=6). The hex dump shows the ICMP message structure.

No.	Time	Source	Destination	Protocol	Length	Info
3441	26.852159	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=394/35329, ttl=4 (no route)
3442	26.887299	10.255.32.191	192.168.1.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3443	26.888703	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=395/35585, ttl=4 (no route)
3444	26.923173	10.255.32.191	192.168.1.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3445	26.924136	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=396/35841, ttl=4 (no route)
3446	26.958396	10.255.32.191	192.168.1.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4154	32.552099	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=397/36097, ttl=5 (no route)
4155	32.588958	10.255.32.234	192.168.1.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4156	32.592183	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=398/36353, ttl=5 (no route)
4163	32.627108	10.255.32.234	192.168.1.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4164	32.630620	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=399/36689, ttl=5 (no route)
4169	32.665899	10.255.32.234	192.168.1.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
+ 4904	38.222210	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=400/36865, ttl=6 (rep)
+ 4908	38.258963	115.73.213.165	192.168.1.15	ICMP	106	Echo (ping) reply id=0x0001, seq=400/36865, ttl=5 (req)
4909	38.260919	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=401/37121, ttl=6 (rep)
4917	38.295490	115.73.213.165	192.168.1.15	ICMP	106	Echo (ping) reply id=0x0001, seq=401/37121, ttl=5 (req)
4918	38.298089	192.168.1.15	115.73.213.165	ICMP	106	Echo (ping) request id=0x0001, seq=402/37377, ttl=6 (rep)
4922	38.334080	115.73.213.165	192.168.1.15	ICMP	106	Echo (ping) reply id=0x0001, seq=402/37377, ttl=5 (req)

Hình 4.9: Vị trí gói tin phản hồi đầu tiên

ĐÁNH GIÁ THÀNH VIÊN

STT	MSSV	Họ và tên	Mức độ hoàn thành công việc	Nhận xét	Chữ ký
1	20127601	Nguyễn Anh Quân	100%	Hoàn thành tốt công việc	
2	21127099	Nguyễn Tấn Lộc	100%	Hoàn thành tốt công việc, làm báo cáo đẹp	
3	21127168	Bùi Phước Thiện	100%	Hoàn thành tốt công việc	

NGUYÊN TẮC HOẠT ĐỘNG NHÓM

1. Chọn không gian làm việc nhóm hợp lý
2. Luôn đến đúng giờ
3. Xác định mục tiêu chung
4. Trưởng nhóm cần có năng lực quản lý
5. Biết lắng nghe
6. Hỗ trợ, giúp đỡ nhau
7. Tôn trọng ý kiến
8. Tăng cường giao tiếp
9. Có trách nhiệm với công việc được giao
10. Luôn thẳng thắn
11. Báo cáo tiến độ làm việc

BIÊN BẢN HỌP NHÓM PHÂN CÔNG

BIÊN BẢN HỌP NHÓM LẦN 1 NGÀY 4/12/2022

❖ *Ghi chú*

Nhóm 10			Lớp HP: 21CLC5
STT	MSSV	Họ và tên	Email
1	20127601	Nguyễn Anh Quân	20127601@student.hcmus.edu.vn
2	21127099	Nguyễn Tân Lộc	ntloc21@clc.fitus.edu.vn
3	21127168	Bùi Phước Thiện	bpthien21@clc.fitus.edu.vn

- Có mặt: 3
- Vắng mặt: 0
- Mục tiêu cuộc họp:
 - Hoàn thành phần tìm hiểu đồ án
 - Phân chia công việc làm báo cáo
- Địa điểm: Google Meet
- Thời gian bắt đầu cuộc họp: 13h00 ngày 4/12/2022
- Thời gian kết thúc cuộc họp: 17h30 ngày 4/12/2022

❖ **Kết quả**

- Nhóm hoàn thành phần tìm hiểu đồ án
- Nhóm phân công người thực hiện làm báo cáo
- Nhóm nêu ý kiến sau khi thực hiện quá trình tìm hiểu
- Deadline là 9/12/2022

❖ **Bảng phân công công việc**

STT	Họ và tên	Phân công	Ngày bắt đầu	Ngày kết thúc
1	Nguyễn Anh Quân	Bài 4	13:00 4/12/2022	17:30 4/12/2022
2	Nguyễn Tân Lộc	Bài 1 + Báo cáo	13:00 4/12/2022	17:30 9/12/2022
3	Bùi Phước Thiện	Bài 2	13:00 4/12/2022	17:30 4/12/2022
4	Cả nhóm thực hiện	Bài 3	13:00 4/12/2022	17:30 4/12/2022

TÀI LIỆU THAM KHẢO

- Computer Networking: A Top-Down Approach, sixth edition, James F. Kurose, Keith W. Ross.
- Slide bài giảng, tài liệu thực hành bộ môn Mạng Máy Tính - trường đại học Khoa Học Tự Nhiên.
- Mai Văn Cường - Trần Trung Dũng - Trần Hồng Ngọc - Lê Ngọc Sơn - Lê Giang Thanh - Trương Thị Mỹ Trang - Đào Anh Tuấn, *Giáo trình Mạng máy tính*, NXB Khoa học và Kỹ thuật, Xuất bản năm 2020
- <https://quantrimang.com/cong-nghe/kien-thuc-ve-giao-thuc-mang-tcp-ip-48>
- <https://www.hackingarticles.in/working-of-traceroute-using-wireshark/>
- <https://www.youtube.com/watch?v=c99g8k8JzkU>
- <https://www.youtube.com/watch?v=yfi7w9p3QnU>

---HẾT---