

**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 MÔN HỌC  
MẠNG MÁY TÍNH  
Wireshark**

**Giảng viên lý thuyết:** Thầy Đỗ Hoàng Cường  
**Giảng viên hướng dẫn thực hành:**

- Thầy Lê Hà Minh
- Thầy Nguyễn Thanh Quân

**Lớp:** 20TN

**Thành viên thực hiện:**

- 20120131 – Nguyễn Văn Lộc
- 20120536 – Võ Trọng Nghĩa
- 20120572 – Nguyễn Kiều Minh Tâm

**THÀNH PHỐ HỒ CHÍ MINH, THÁNG 4 NĂM 2022**

# Mục lục

<b>1</b>	<b>Thông tin của nhóm</b>	<b>3</b>
<b>2</b>	<b>Mức độ hoàn thành</b>	<b>3</b>
<b>3</b>	<b>Bài 1: Ping</b>	<b>4</b>
<b>4</b>	<b>Bài 2: HTTP</b>	<b>8</b>
<b>5</b>	<b>Bài 3: Traceroute</b>	<b>18</b>
<b>6</b>	<b>Bài 4: DHCP</b>	<b>24</b>
<b>7</b>	<b>Bài 5: FTP</b>	<b>25</b>
<b>8</b>	<b>Tài liệu tham khảo</b>	<b>31</b>

# Danh sách hình vẽ

1	Nội dung tập tin <i>ping.pcapng</i> . . . . .	4
2	Địa chỉ IP của host ping và host được ping . . . . .	5
3	Dộ dài Ethernet header . . . . .	6
4	Dộ dài IP header . . . . .	6
5	Dộ dài ICMP data và ICMP header . . . . .	7
6	Sơ đồ mạng . . . . .	7
7	Kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request . . . . .	8
8	Địa chỉ IP của host . . . . .	9
9	Địa chỉ IP của router . . . . .	9
10	Địa chỉ MAC của host . . . . .	10
11	Địa chỉ MAC của router . . . . .	11
12	Protocol phân giải tên miền . . . . .	11
13	Địa chỉ IP của HTTP server . . . . .	12
14	Nghi thức được DNS sử dụng . . . . .	13
15	Port sử dụng khi truy vấn DNS server . . . . .	13
16	Thời gian hoàn thành quá trình 3-way handshake . . . . .	14
17	Version HTTP . . . . .	15
18	Kết quả của câu query <i>udp.dstport==53</i> . . . . .	15
19	Các gói tin liên quan . . . . .	16
20	Quá trình gửi ACK . . . . .	17
21	Kết quả bắt gói tin sau khi tracert . . . . .	18
22	Địa chỉ IP của máy gửi request . . . . .	19
23	Gói tin DNS query . . . . .	20
24	Gói tin DNS query response . . . . .	21
25	Protocol được sử dụng . . . . .	22
26	TTL của gói tin cuối cùng trước khi nhận response . . . . .	23

27	Giao thức được FTP sử dụng . . . . .	25
28	Port truyền lệnh của client . . . . .	26
29	Mode truy xuất của client lên server . . . . .	27
30	Quá trình bắt tay 3 bước để tạo kết nối ban đầu . . . . .	27
31	Quá trình bắt tay 3 bước để tạo kết nối ban đầu . . . . .	28
32	Quá trình bắt tay 3 bước để tạo kết nối truyền dữ liệu . . . . .	28
33	Quá trình bắt tay 3 bước để tạo kết nối truyền dữ liệu . . . . .	29
34	Port truyền dữ liệu của FTP server và client . . . . .	30

## Danh sách bảng

1	Bảng phân công thành viên . . . . .	3
2	Kích thước gói tin ICMP request . . . . .	5

# 1 Thông tin của nhóm

MSSV	Họ và tên	Công việc
20120131	Nguyễn Văn Lộc	Bài 1 + 2
20120536	Võ Trọng Nghĩa	Bài 4 + L <sup>A</sup> T <sub>E</sub> X
20120572	Nguyễn Kiều Minh Tâm	Bài 3 + 5

Bảng 1: Bảng phân công thành viên

# 2 Mức độ hoàn thành

**Bài 1:** 100% (5/5)

**Bài 2:** 100% (14/14)

**Bài 3:** 100% (5/5)

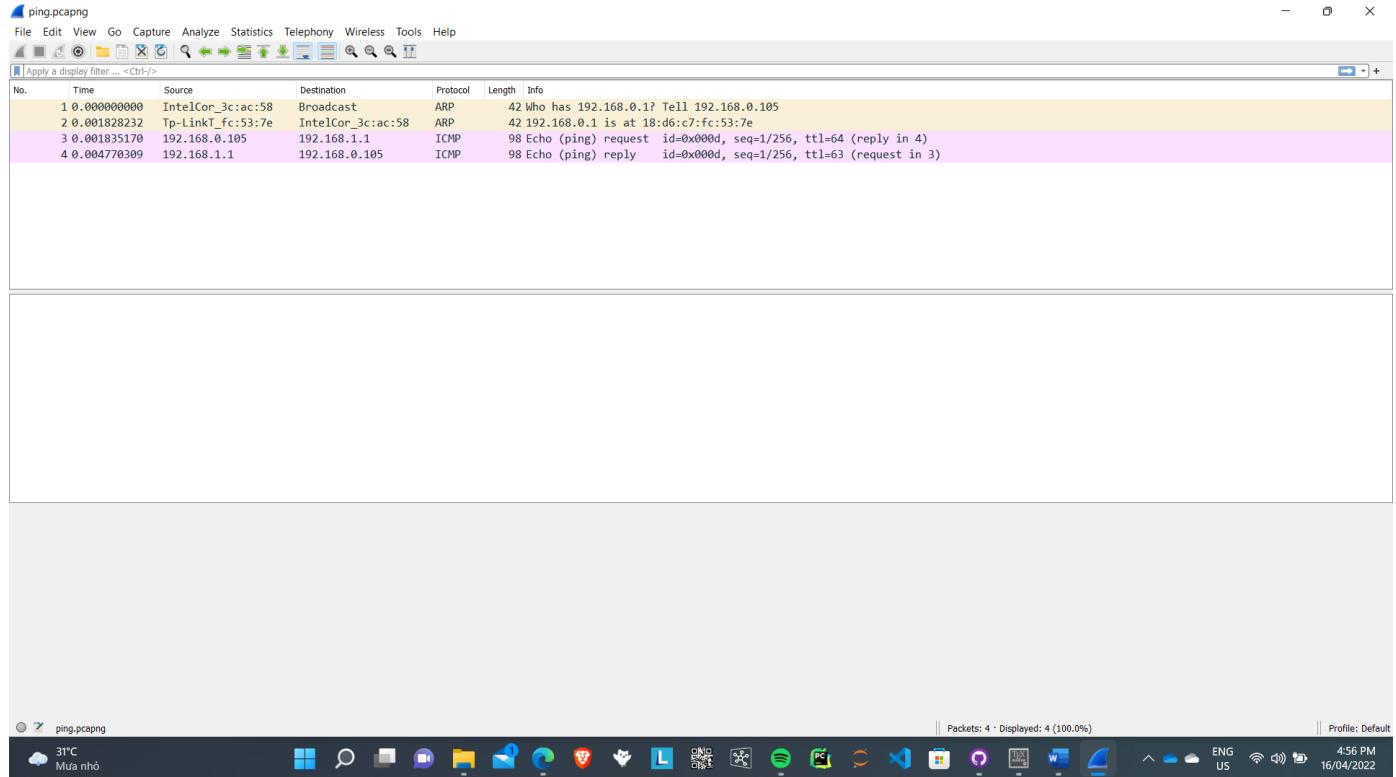
**Bài 4:**

**Bài 5:** 100% (8/8)

### 3 Bài 1: 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.

Nội dung tập tin ***ping.pcapng*** như sau.



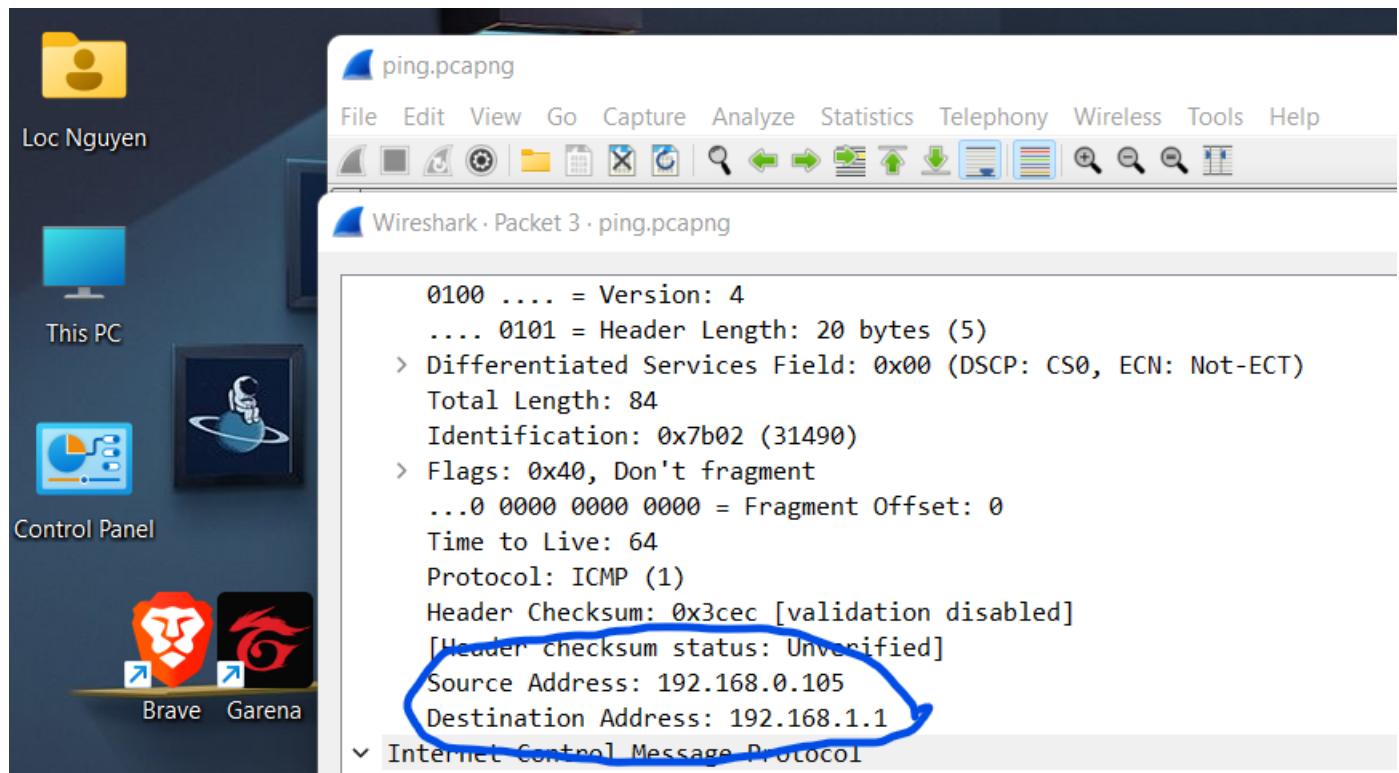
Hình 1: Nội dung tập tin ***ping.pcapng***

Trả lời các câu hỏi sau:

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**.



Hình 2: 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?**

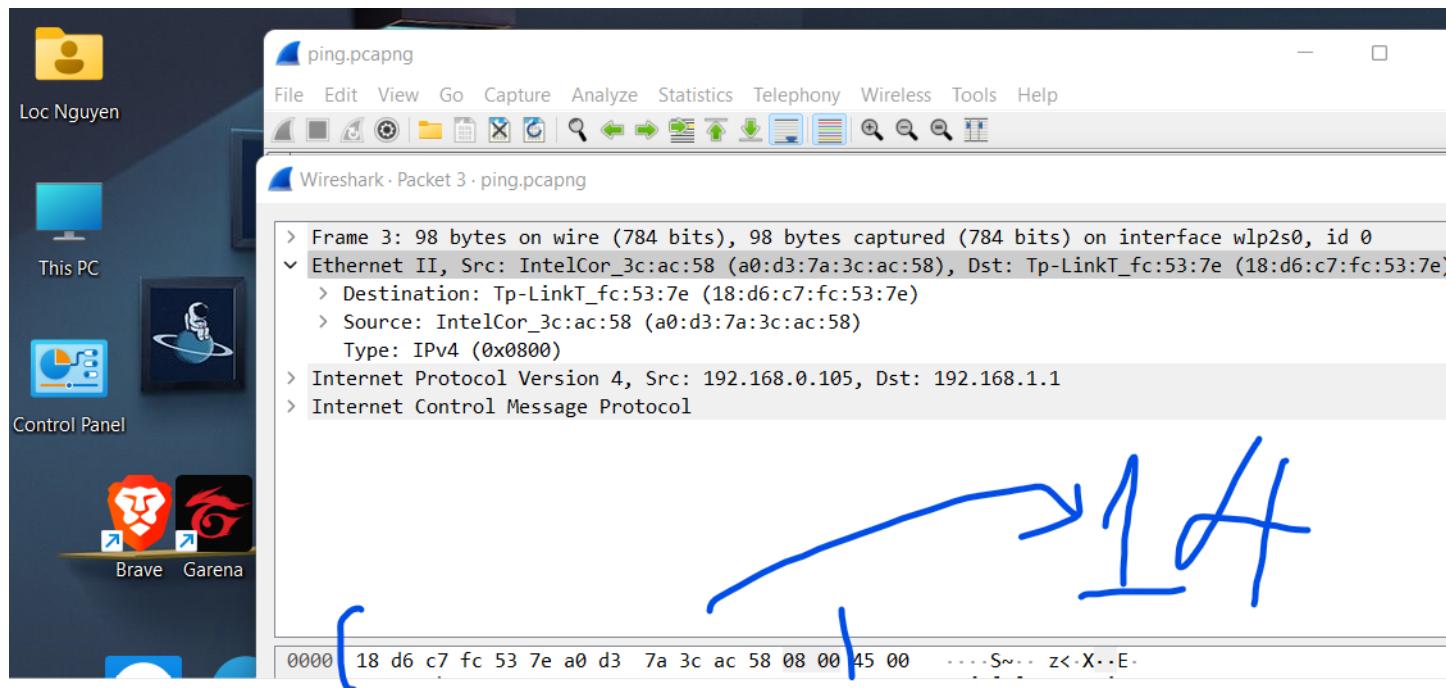
Không có source port number và destination port number.

Lý do: Lệnh ping sử dụng giao thức ICMP của mô hình TCP/IP. ICMP là giao thức ở tầng, còn port number được sử dụng ở tầng Application.

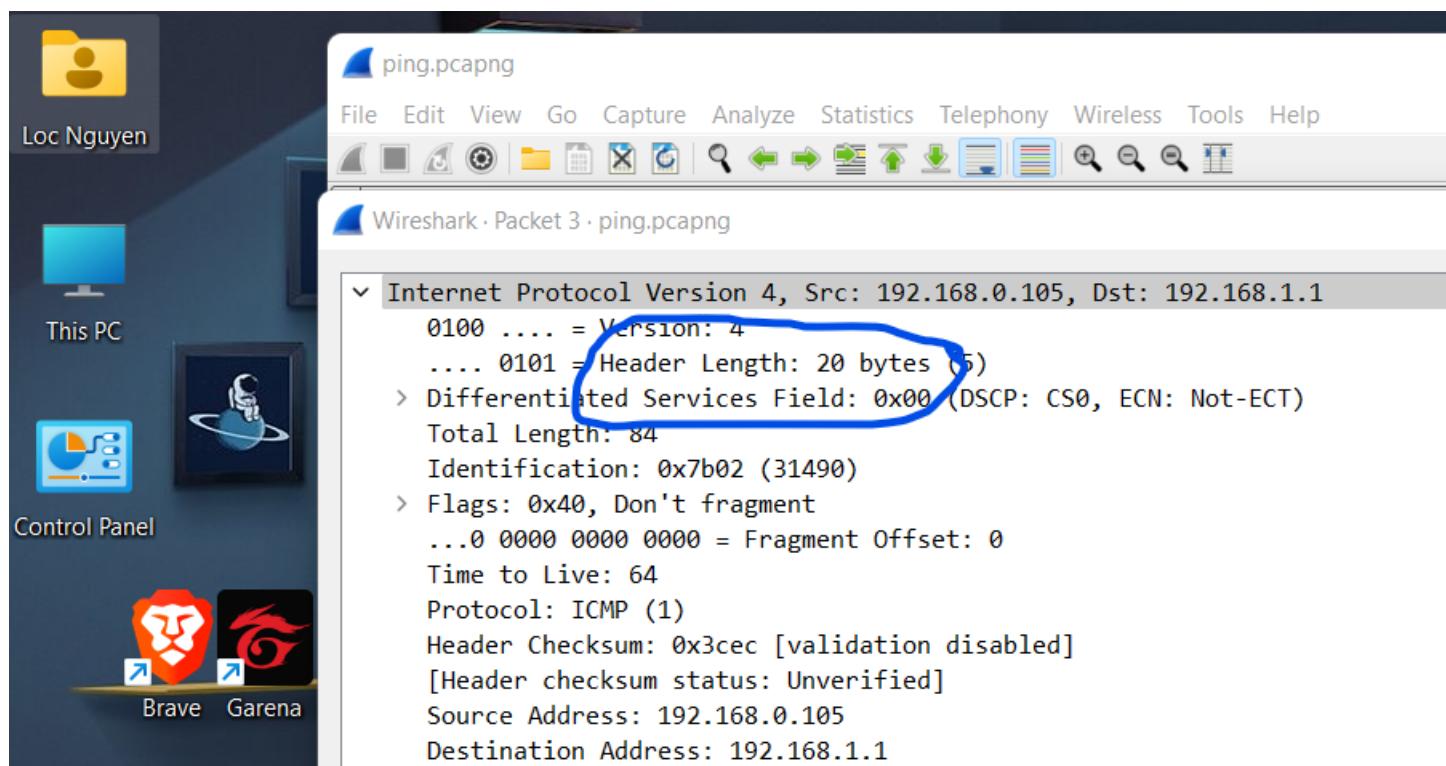
**3. Với gói tin ICMP request, cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)**

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

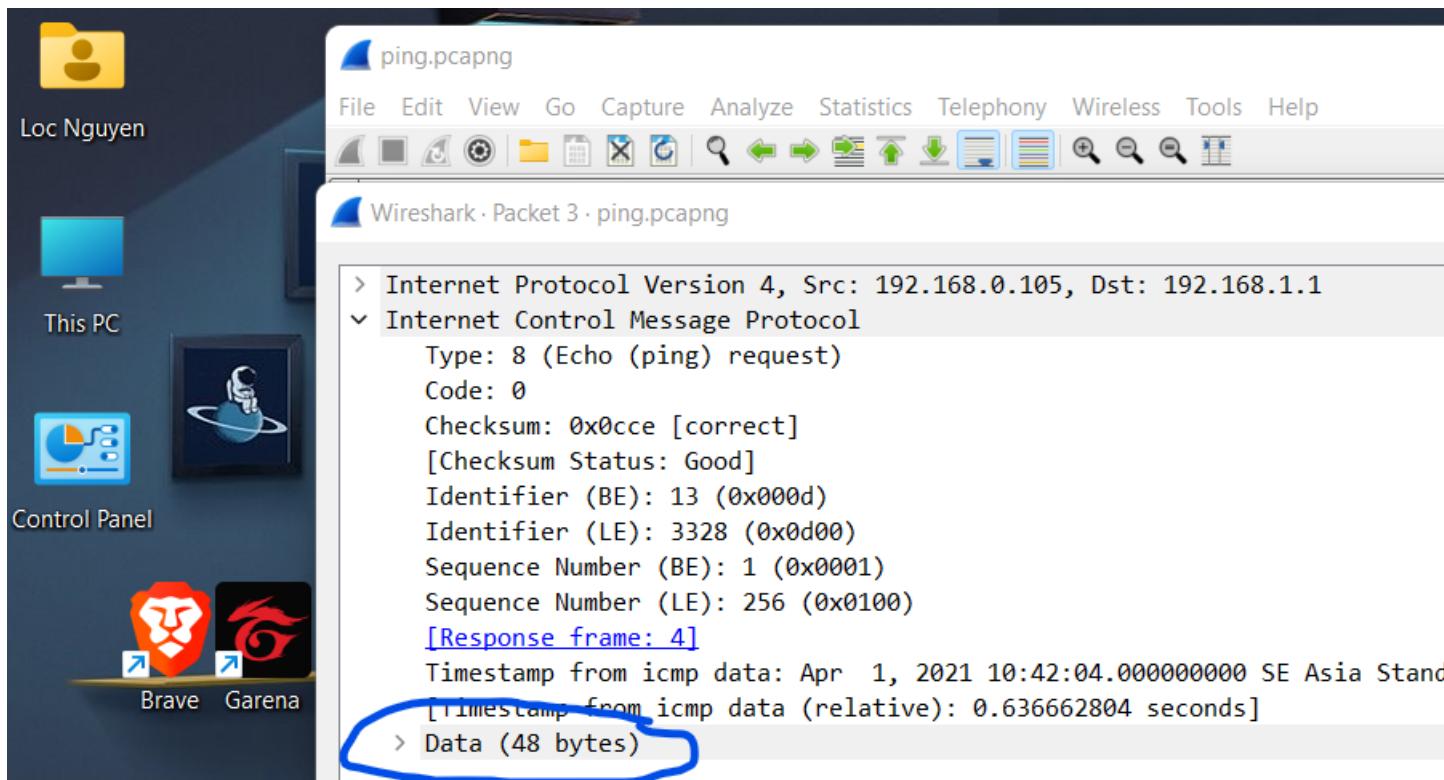
Bảng 2: Kích thước gói tin ICMP request



Hình 3: Độ dài Ethernet header



Hình 4: Độ dài IP header



Hình 5: Độ dài ICMP data và ICMP header

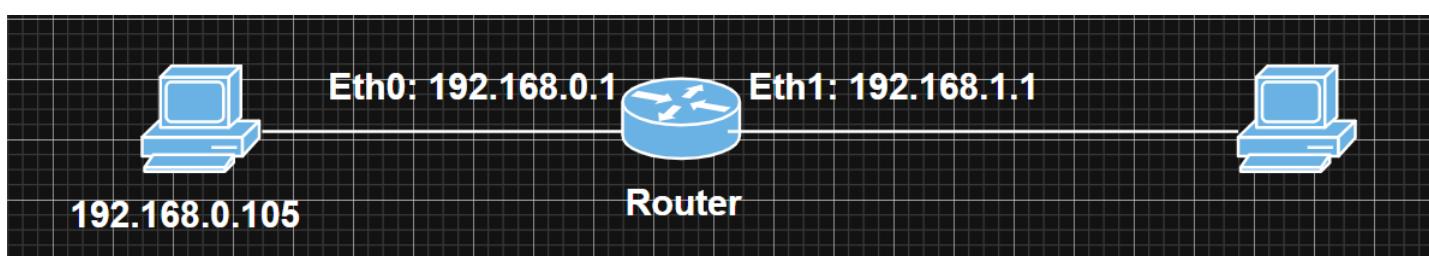
#### 4. Tại sao lại có 2 gói ARP?

ARP (viết tắt của cụm từ Address Resolution Protocol) là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network.

Khi ta sử dụng lệnh ping, host ping (192.168.0.105) thực hiện broadcast gói tin ARP request vào tất cả các host trong mạng LAN xem host nào có địa chỉ là 192.168.1.1 (host được ping). Host được ping sẽ gửi lại gói tin ARP reply, xác định địa chỉ MAC cần tìm (18:d6:c7:fc:53:7e) cho host ping.

#### 5. Hãy vẽ sơ đồ mạng logic dựa trên nội dung gói pcap đó.

Sơ đồ mạng logic dựa trên nội dung gói pcap trong bài như sau.



Hình 6: Sơ đồ mạng

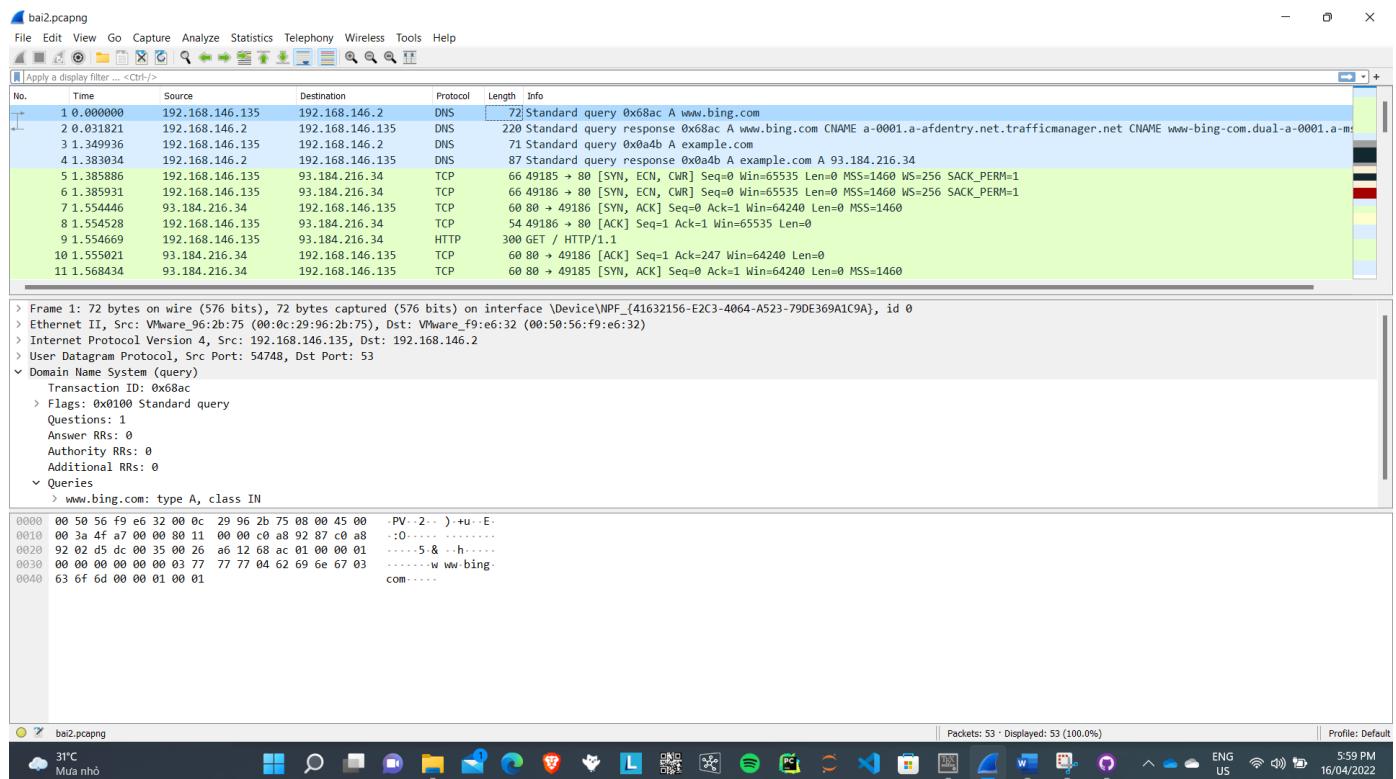
## 4 Bài 2: HTTP

Xóa cache browser trước khi truy cập trang web hoặc dùng ẩn danh. Dùng Wireshark để bắt gói tin khi truy cập vào website: <http://example.com>.

Việc bắt gói tin bằng Wireshark trong bài được thực hiện bằng **máy ảo**, sử dụng hệ điều hành **Windows Server 2012 R2**.

Kết quả bắt gói tin chi tiết được lưu trong tập tin **bai2.pcapng**.

**1. Chụp hình kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request (thấy được những gói tin liên quan).**



Hình 7: Kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request

### 2. Cho biết IP của host.

IP của host là: 192.168.146.135.

The screenshot shows the Windows Start Menu on the left and the Wireshark application window on the right. The Start Menu includes icons for Loc Nguyen, This PC, and Control Panel. The Wireshark window displays a list of network traffic from a file named 'bai2.pcapng'. The table highlights several source IP addresses (192.168.146.135, 192.168.146.2, 192.168.146.135, 192.168.146.135, 192.168.146.135, 192.168.146.135) with a blue oval, and destination IP addresses (192.168.146.2, 192.168.146.135, 192.168.146.2, 192.168.146.135, 93.184.216.34, 93.184.216.34) with a green oval.

No.	Time	Source	Destination
1	0.000000	192.168.146.135	192.168.146.2
2	0.031821	192.168.146.2	192.168.146.135
3	1.349936	192.168.146.135	192.168.146.2
4	1.383034	192.168.146.2	192.168.146.135
5	1.385886	192.168.146.135	93.184.216.34
6	1.385931	192.168.146.135	93.184.216.34
7	1.554446	93.184.216.34	192.168.146.135
8	1.554528	192.168.146.135	93.184.216.34

Hình 8: Địa chỉ IP của host

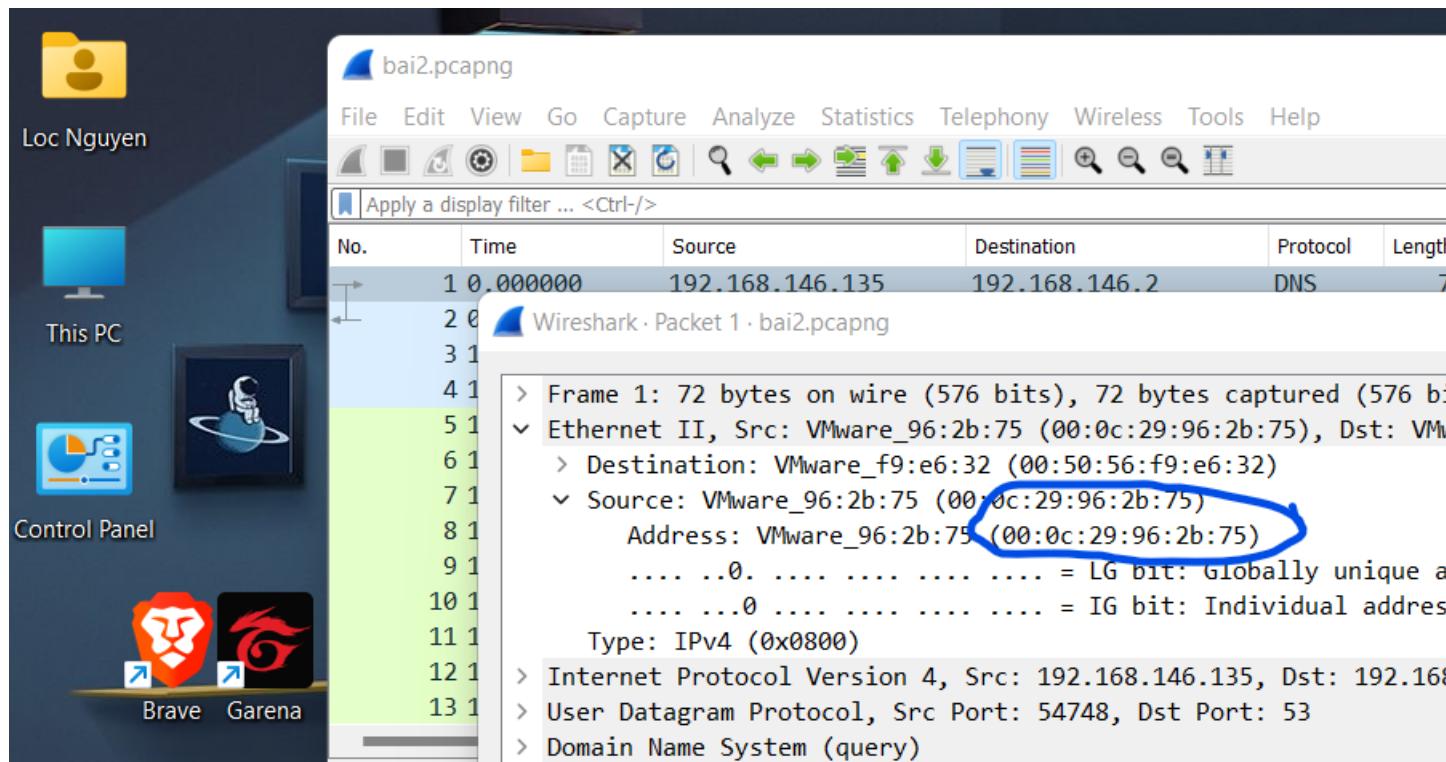
**3. Cho biết IP của router (default gateway) (nếu không thấy được thì trả lời không có và giải thích tại sao)**  
IP của router là: **192.168.146.2**.

The screenshot shows the Wireshark application window displaying a list of network traffic from a file named 'bai2.pcapng'. The table highlights the destination IP address (192.168.146.2) with a blue oval.

No.	Time	Source	Destination	Protocol
1	0.000000	192.168.146.135	192.168.146.2	DNS
2	0.031821	192.168.146.2	192.168.146.135	DNS
3	1.349936	192.168.146.135	192.168.146.2	DNS
4	1.383034	192.168.146.2	192.168.146.135	DNS

Hình 9: Địa chỉ IP của router

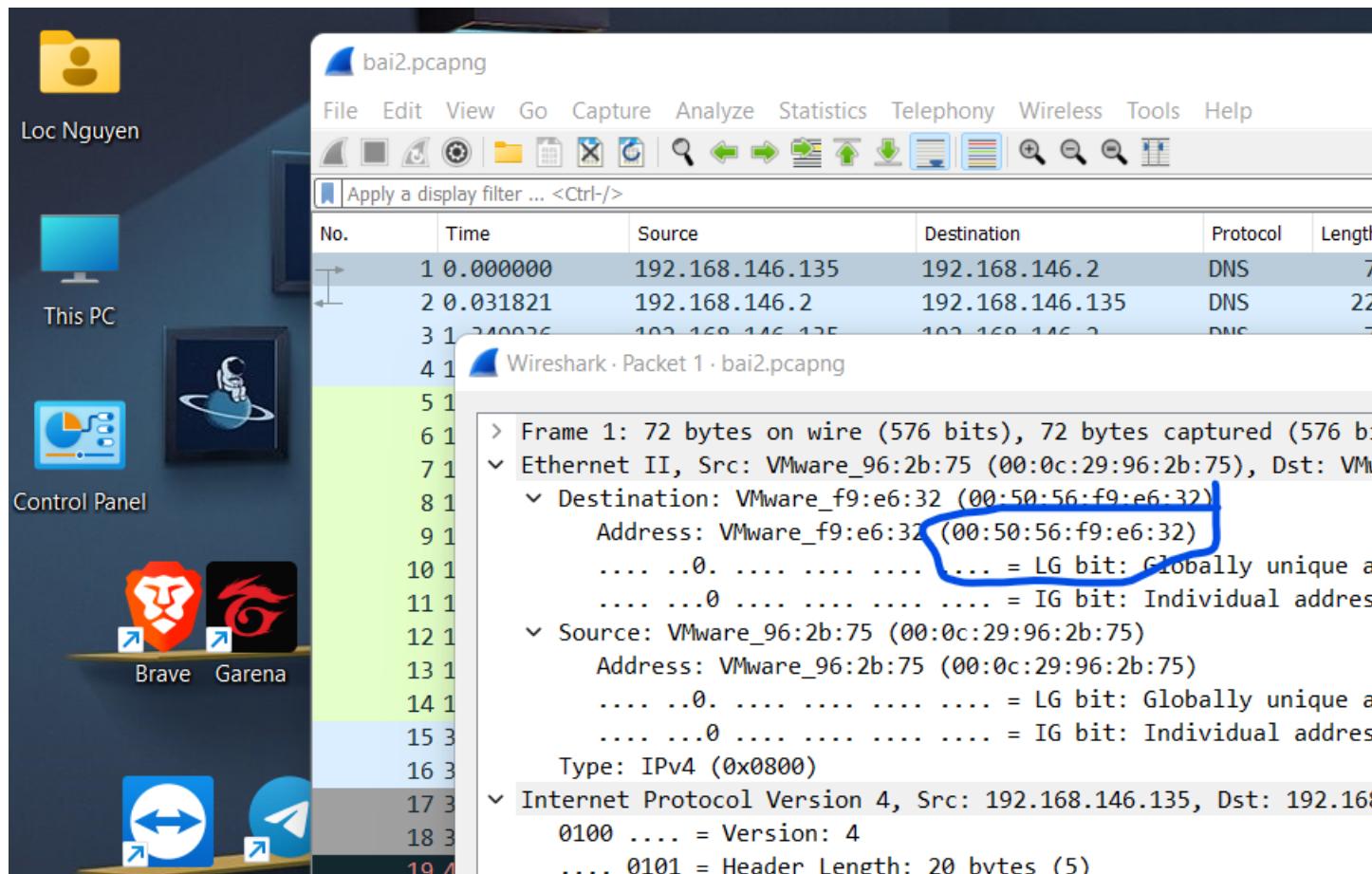
**4. Cho biết địa chỉ MAC của host.**  
Địa chỉ MAC của host là: **00:0c:29:96:2b:75**.



Hình 10: Địa chỉ MAC của host

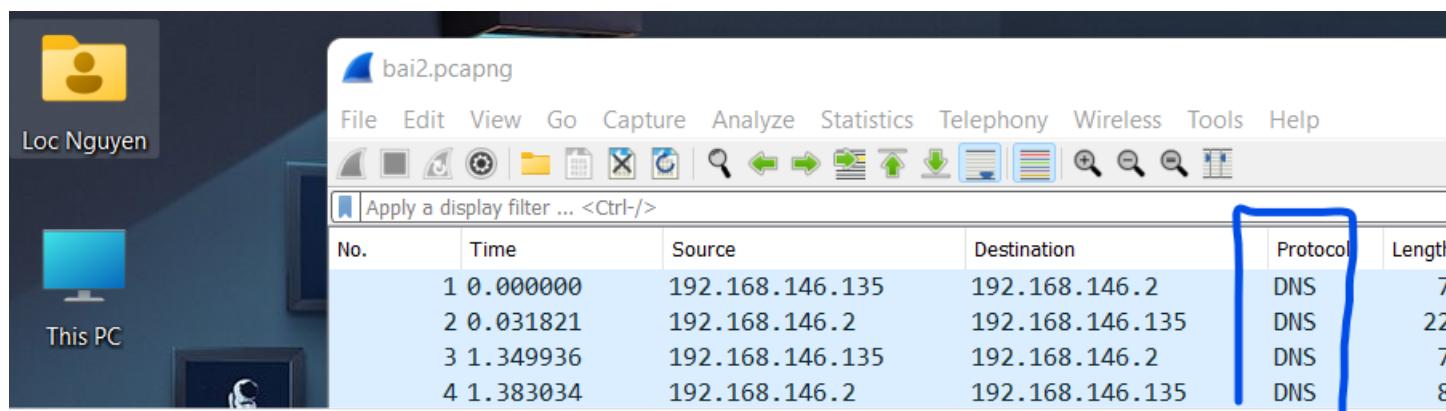
### 5. Cho biết địa chỉ MAC của router (default gateway).

Địa chỉ MAC của router là: 00:50:56:f9:e6:32.



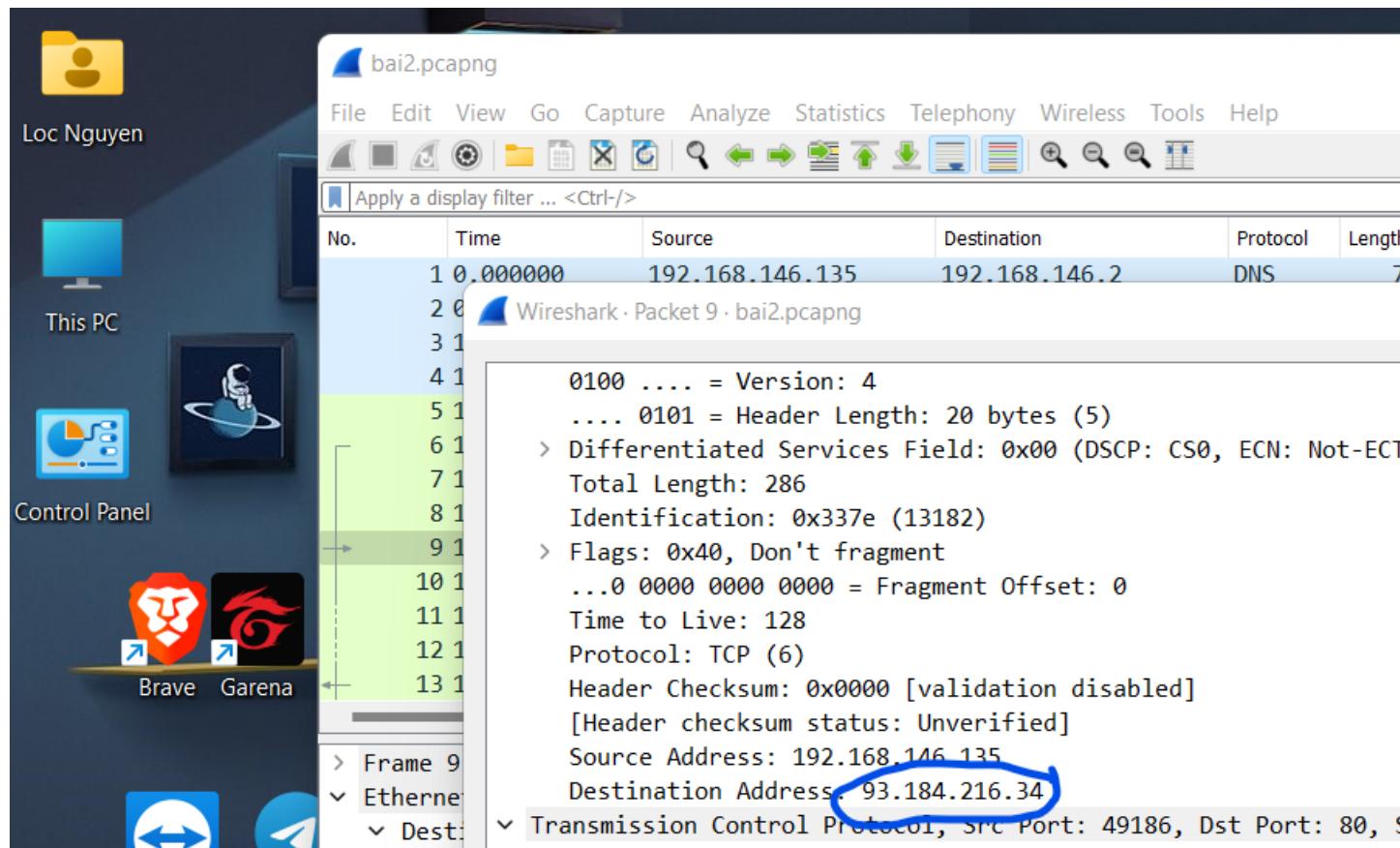
Hình 11: Địa chỉ MAC của router

**6. Protocol nào được sử dụng để phân giải tên miền của trang web?**  
Protocol được dùng để phân giải tên miền của trang web: **DNS**.



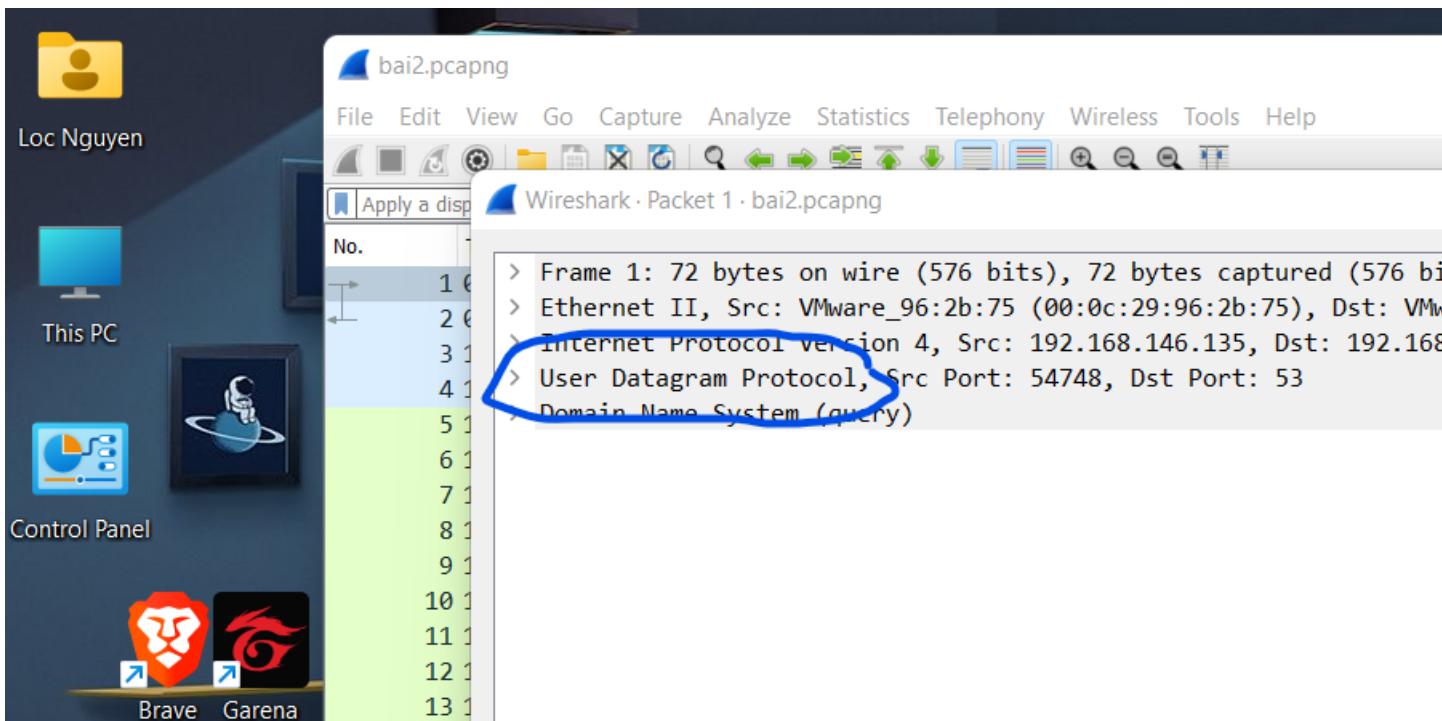
Hình 12: Protocol phân giải tên miền

**7. Cho biết IP của HTTP server.**  
Địa chỉ IP của HTTP server là: **93.184.216.34**.



Hình 13: Địa chỉ IP của HTTP server

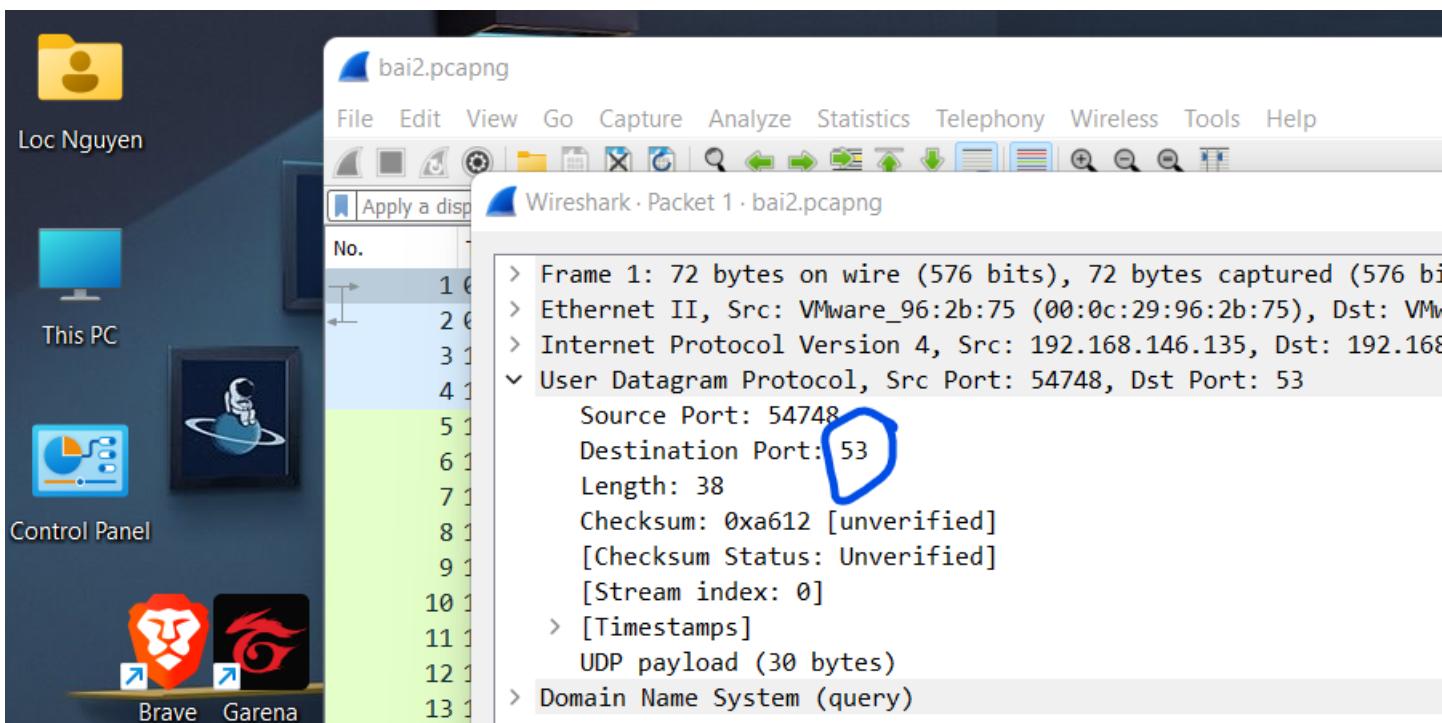
**8. Cho biết protocol của tầng Transport được sử dụng bởi DNS.**  
DNS sử dụng protocol **UDP** của tầng Transport.



Hình 14: Nghi thức được DNS sử dụng

### 9. Cho biết port sử dụng khi truy vấn DNS server.

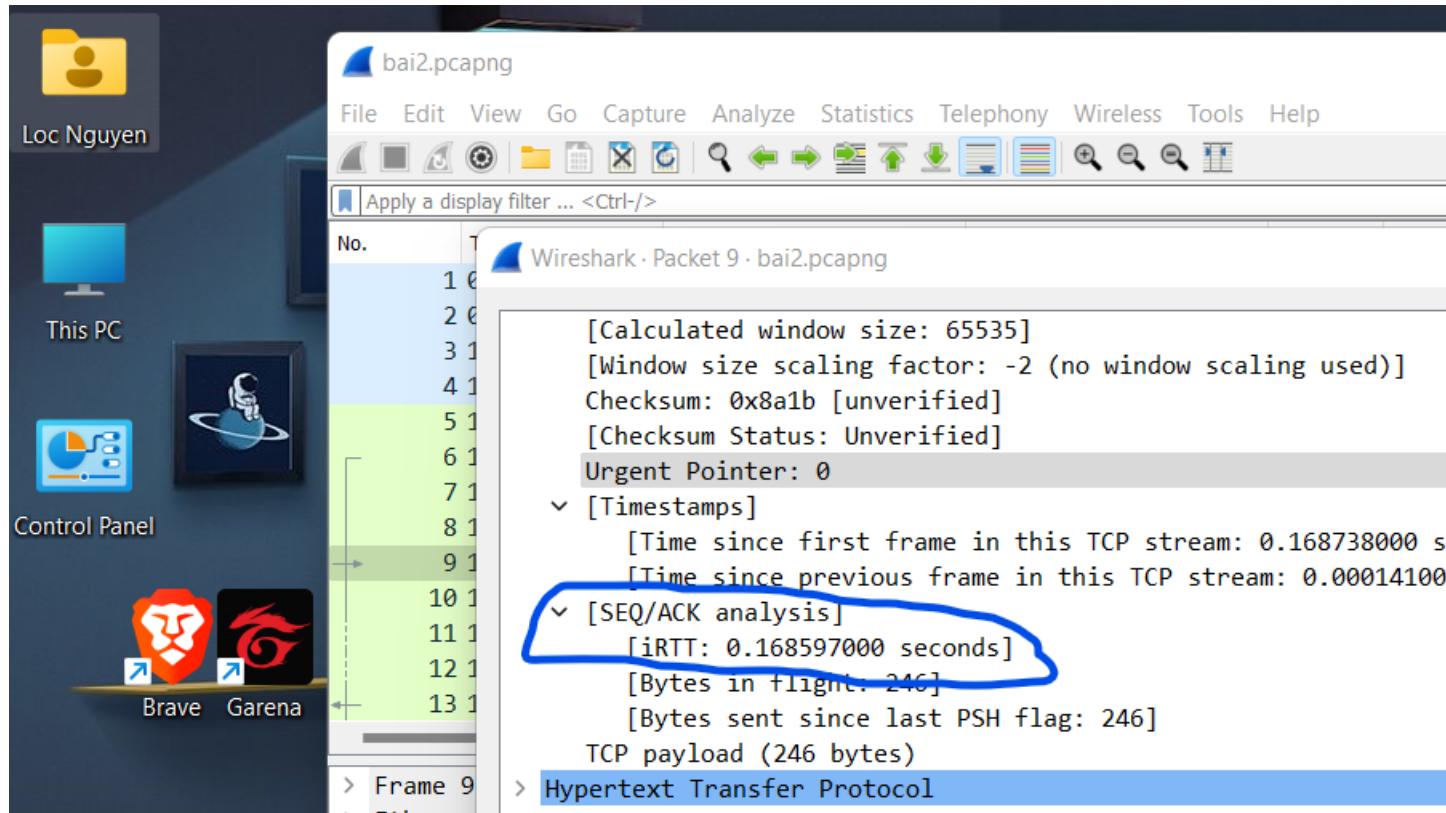
Port sử dụng khi truy vấn DNS server: **port 53**.



Hình 15: Port sử dụng khi truy vấn DNS server

### 10. Bao lâu thì quá trình bắt tay 3 bước (3-way handshake) hoàn thành?

Thời gian quá trình 3-way handshake hoàn thành: **0.168597000 giây.**



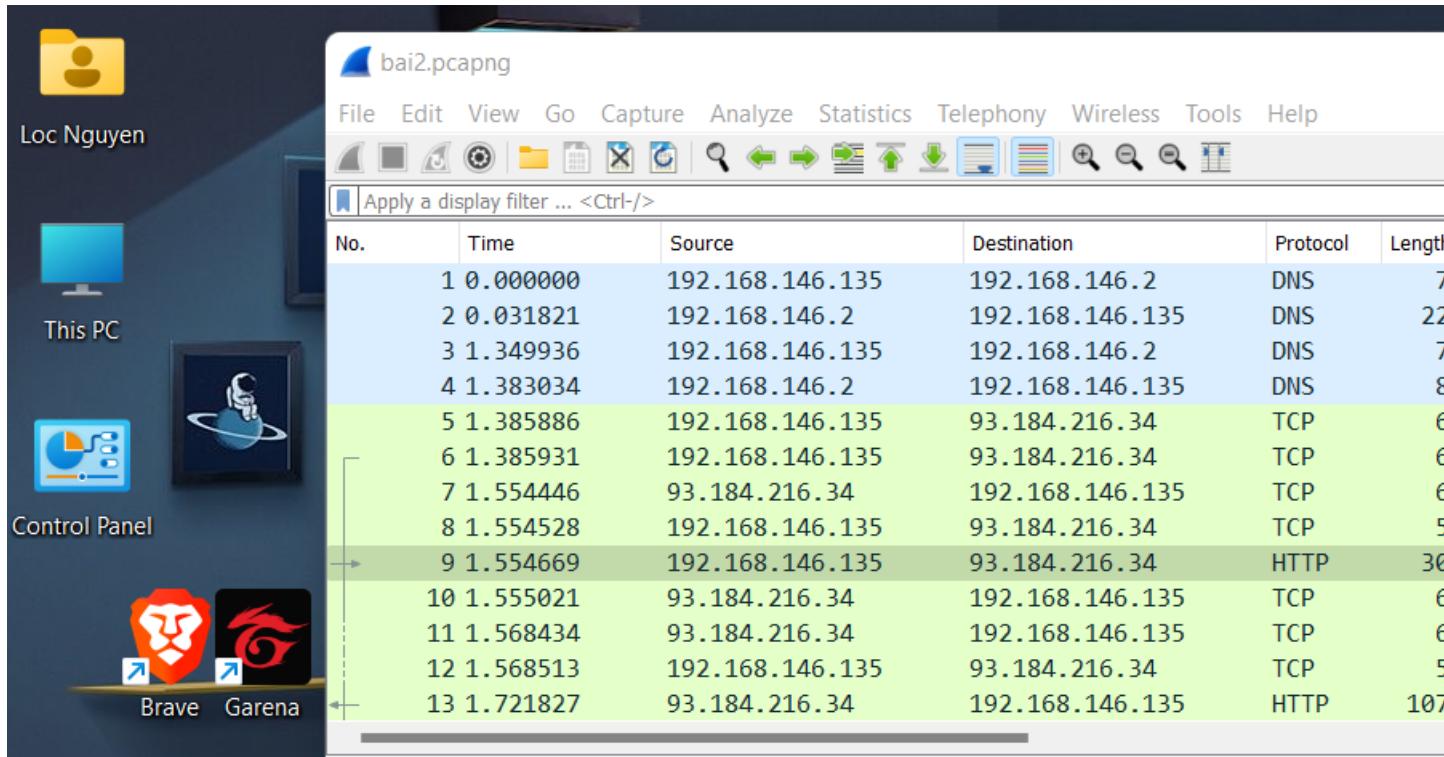
Hình 16: Thời gian hoàn thành quá trình 3-way handshake

**11. Cho biết host machine của website đang truy cập (Application - host field)**

Host machine của website đang truy cập là: **example.com**.

**12. Cho biết version HTTP mà trình duyệt web (bowser) đang sử dụng (Application).**

Version HTTP mà trình duyệt web đang sử dụng là: **HTTP/1.1**.

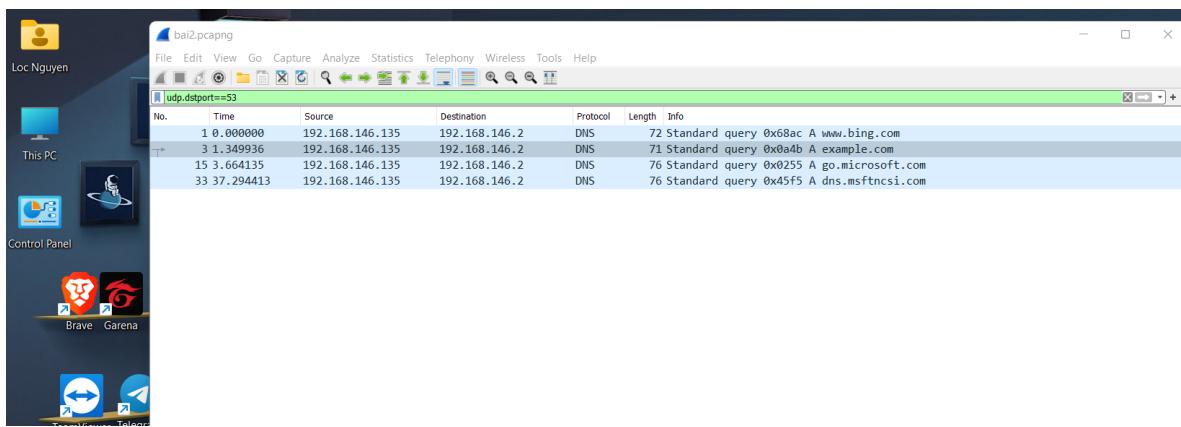


Hình 17: Version HTTP

13. Trong mục Filter, nhập câu query sau đây: `udp.dstport==53` và click apply. Hãy cho biết chức năng và kết quả của câu query vừa thực hiện.

Chức năng của câu query `udp.dstport==53`: lọc các gói tin có port đích là 53. Theo kết quả câu 9, port 53 được dùng bởi protocol DNS, có nghĩa là kết quả của câu query này cho ta danh sách các gói tin sử dụng truy vấn DNS server.

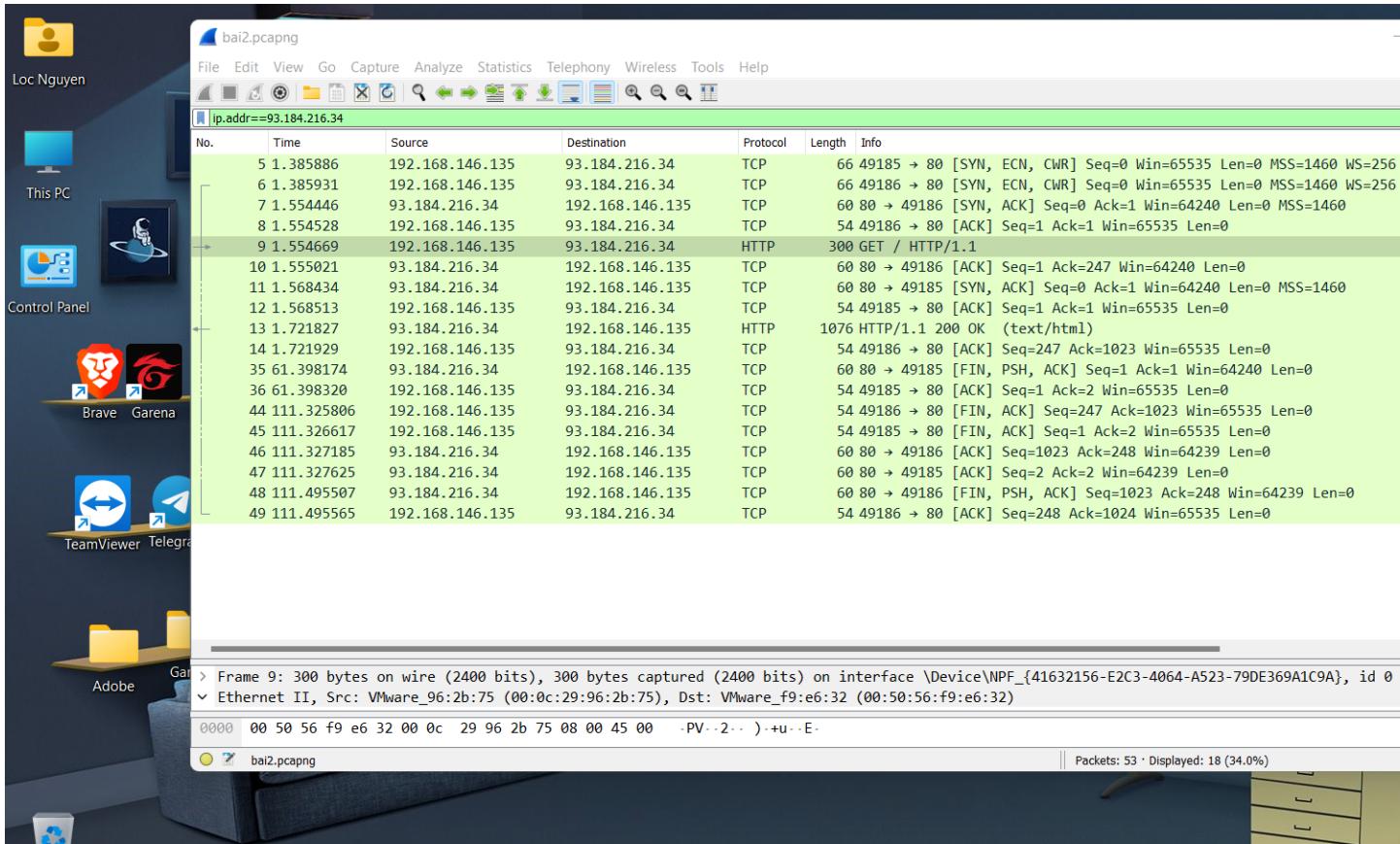
Kết quả của query này như sau.

Hình 18: Kết quả của câu query `udp.dstport==53`

14. Vẽ hình quá trình gửi ACK (gồm Sequence number, Acknowledgement number) từ khi kết nối đến khi kết thúc nhận data giữa client và HTTP server.

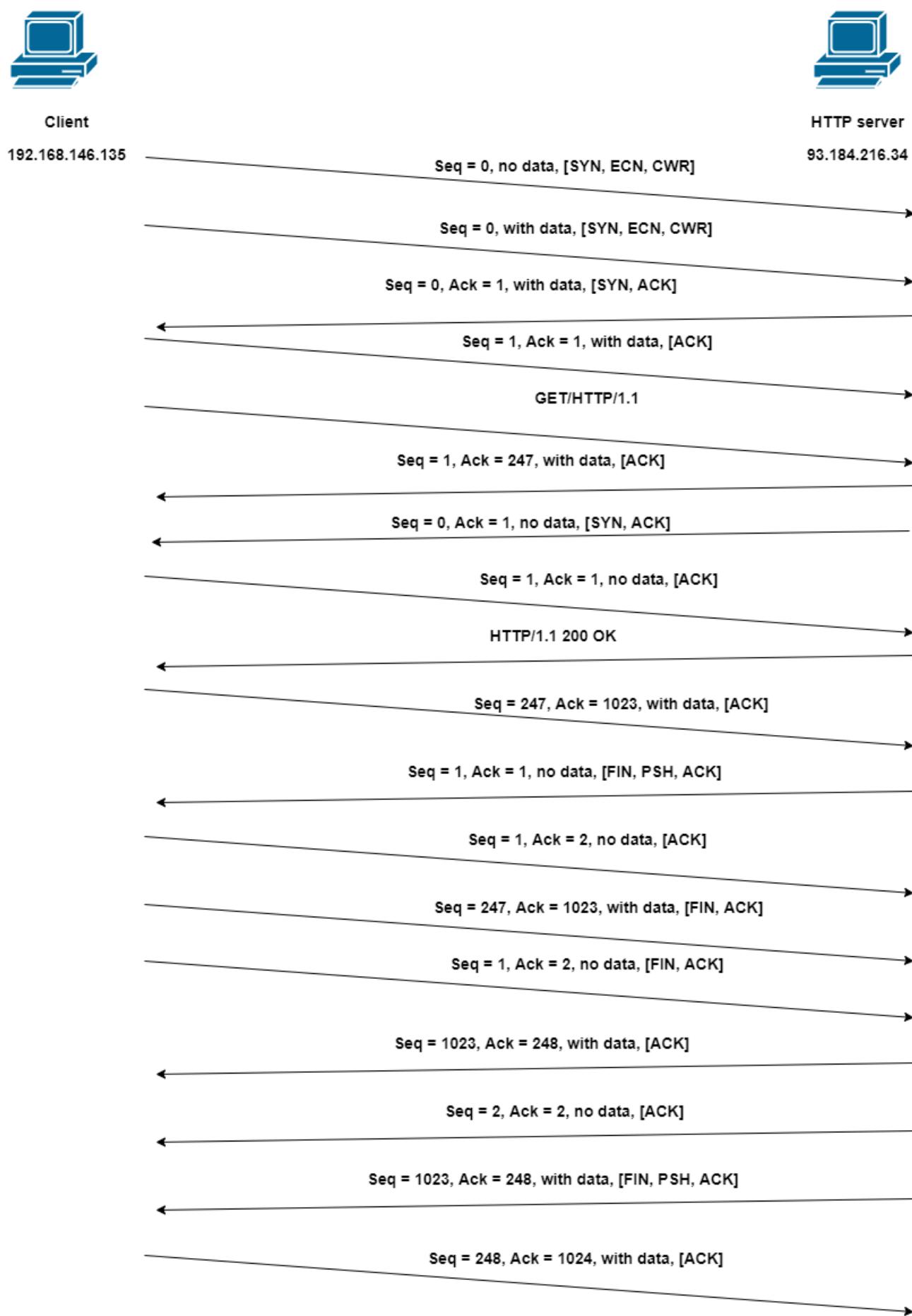
Các gói tin liên quan trong quá trình gửi ACK từ khi kết nối đến khi kết thúc nhận

data giữa client và HTTP server như sau.



Hình 19: Các gói tin liên quan

Quá trình gửi ACK từ khi kết nối đến khi kết thúc nhận data giữa client và HTTP server.



Hình 20: Quá trình gửi ACK

## 5 Bài 3: Traceroute

Nếu bạn dùng Window thì dùng lệnh ***tracert***, nếu bạn dùng Linux/iOS thì bạn dùng lệnh ***traceroute***. Lưu ý kết quả bắt gói tin trên Window và Linux/iOS sẽ khác nhau, vì vậy câu trả lời phụ thuộc bạn dùng OS nào.

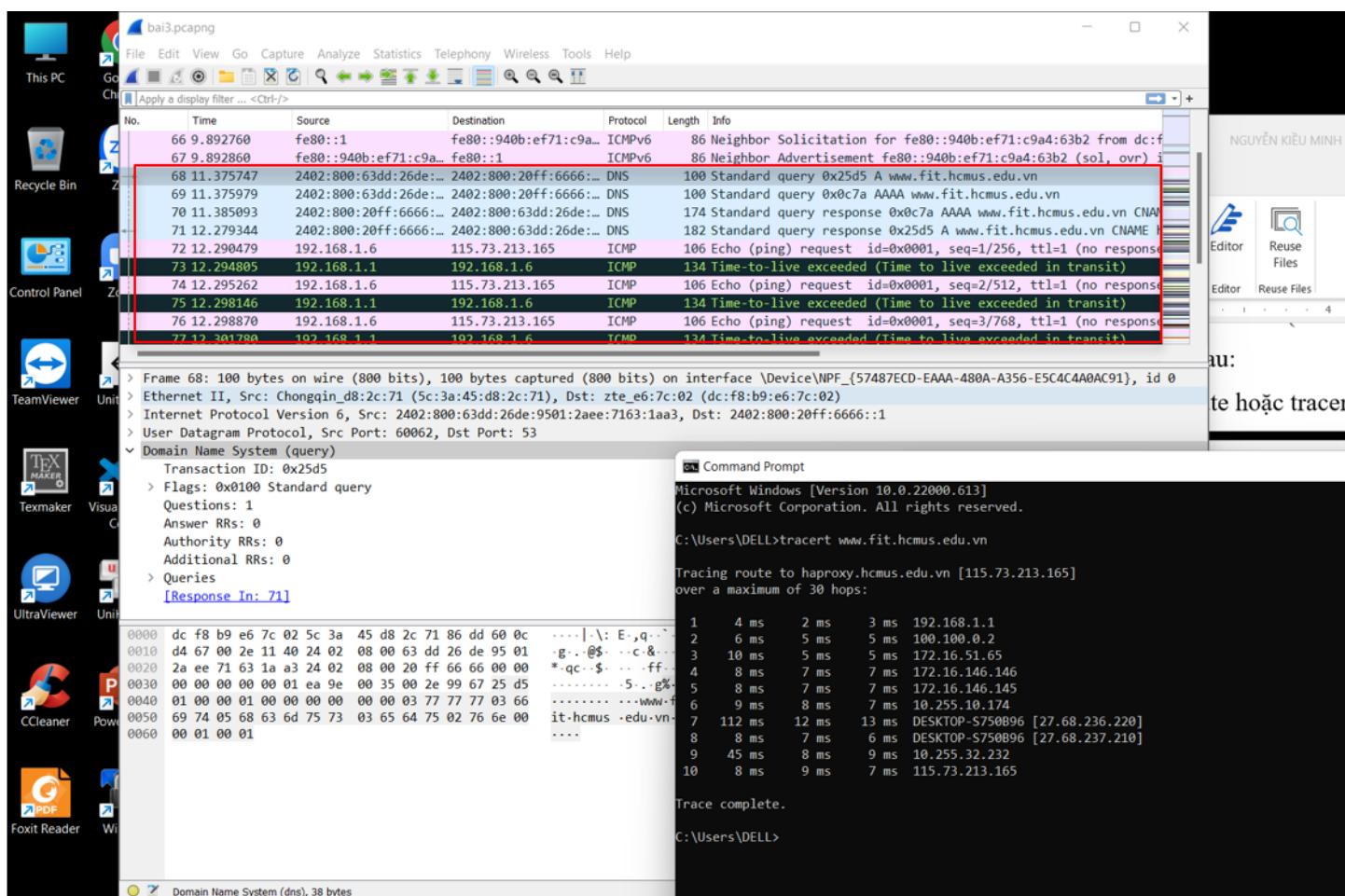
Bật wireshark để bắt gói tin lệnh traceroute từ máy của mình (có thể dùng máy ảo) đến ***www.fit.hcmus.edu.vn*** (FIT).

Bài tập được thực hiện trên máy tính sử dụng hệ điều hành **Windows 11**.

Kết quả bắt gói tin chi tiết được lưu trong tập tin ***bai3.pcapng***.

### 1. 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 tracert như sau.



Hình 21: Kết quả bắt gói tin sau khi tracert

Các gói tin được bắt tính từ lệnh tracert được thể hiện ở phần đóng khung màu đỏ trên hình vẽ. Đó là các gói tin đầu tiên bắt đầu từ khi tracert (gói tin số 68).

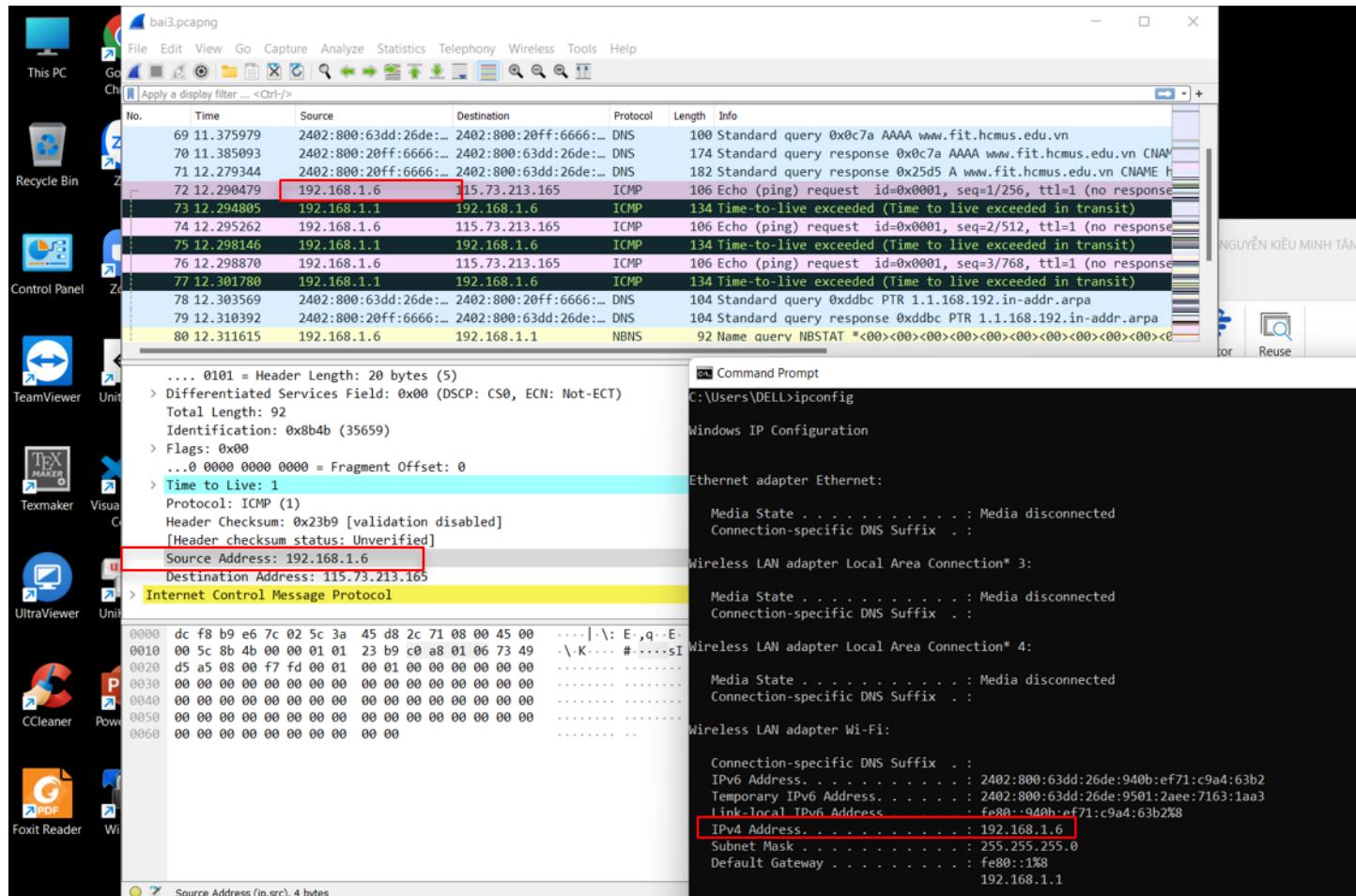
### 2. Cho biết traceroute/tracert dùng để làm gì?

Traceroute/tracert dùng để xác định vết đường đi của gói tin giữa hai host: source host và destination host. Thông tin này được thể hiện qua các gói tin ICMP (gói tin IP có trường protocol = 1). Và dựa vào thông tin tương ứng trên các trường của thông điệp

ICMP, host nguồn xác định được địa chỉ IP của các router trên đường truyền.<sup>1,2</sup>

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

Địa chỉ IP của máy gửi request là 192.168.1.6.

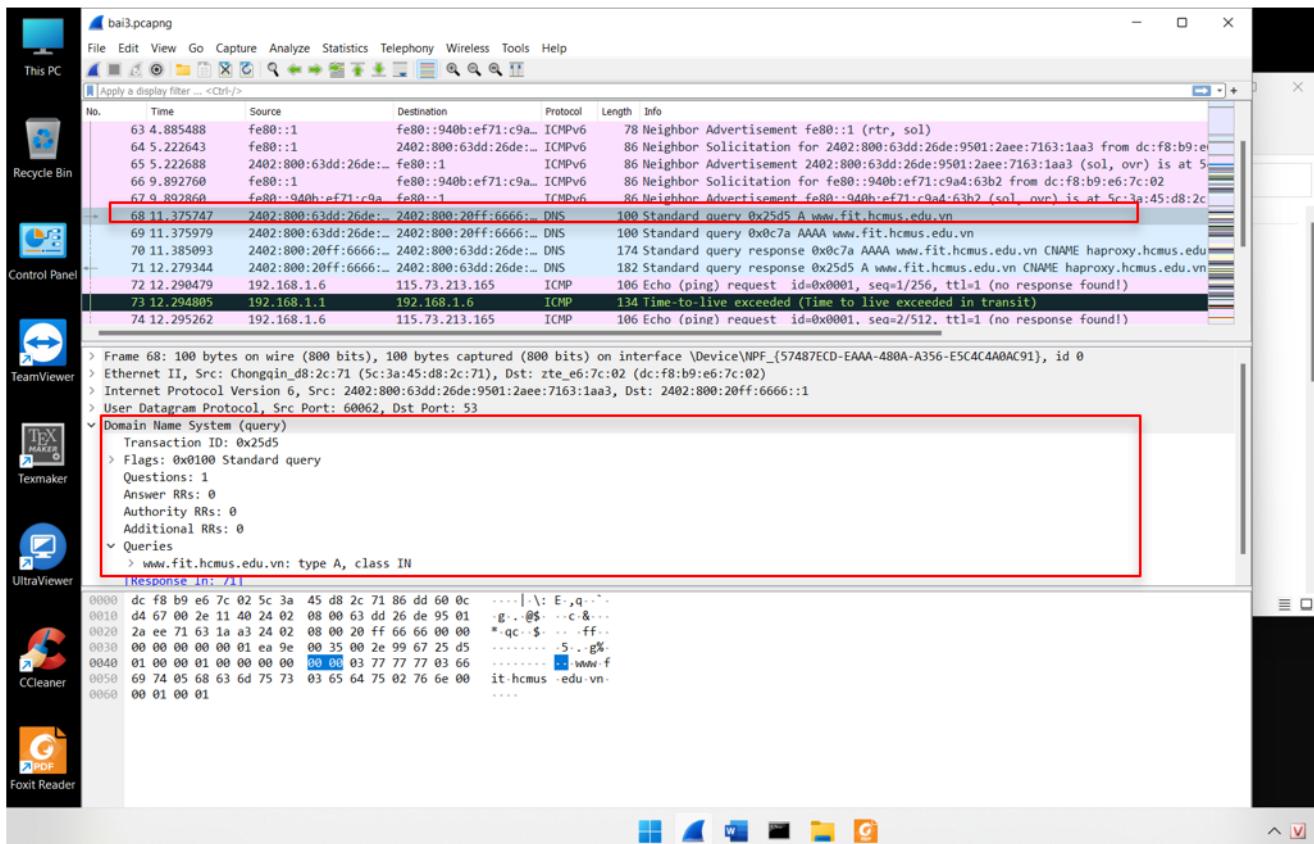


Hình 22: Địa chỉ IP của máy gửi request

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

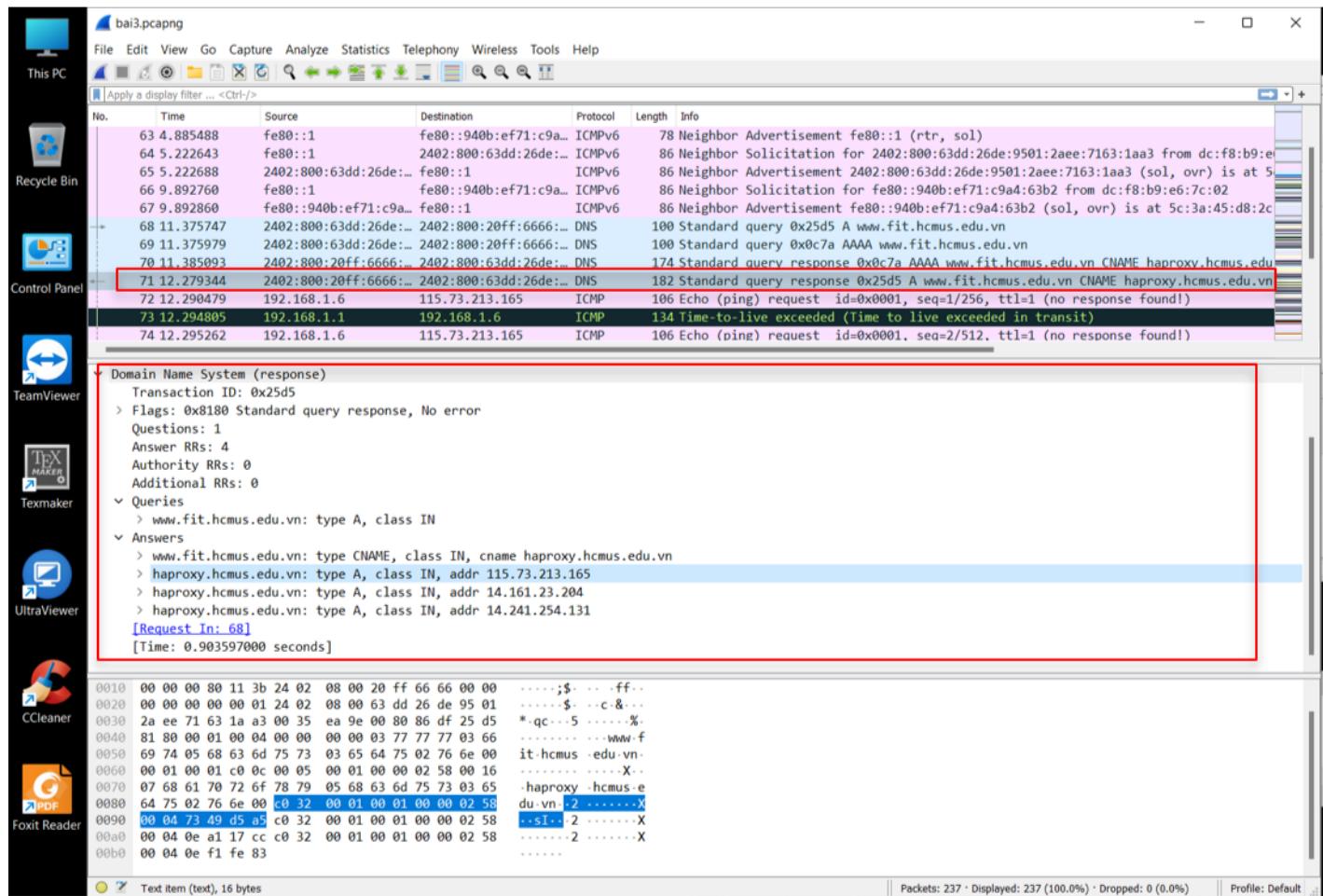
Máy tính sẽ gửi gói tin DNS query lên DNS server để “hỏi”, sau đó DNS Server sẽ trả lời qua gói tin DNS response.

- Gói tin DNS query được gửi từ destination host là gói tin số 68 (được lưu trong file bai3.pcapng).



Hình 23: Gói tin DNS query

- Và gói tin trả lời tương ứng là gói tin số 71 (được lưu trong file **bai3.pcapng**). Hình vẽ cho thấy có FIT có 3 địa chỉ IP 115.73.213.165, 14.161.23.204, 14.241.254.131. Trong lần này traceroute được thực hiện tới địa chỉ IP 115.73.213.165.

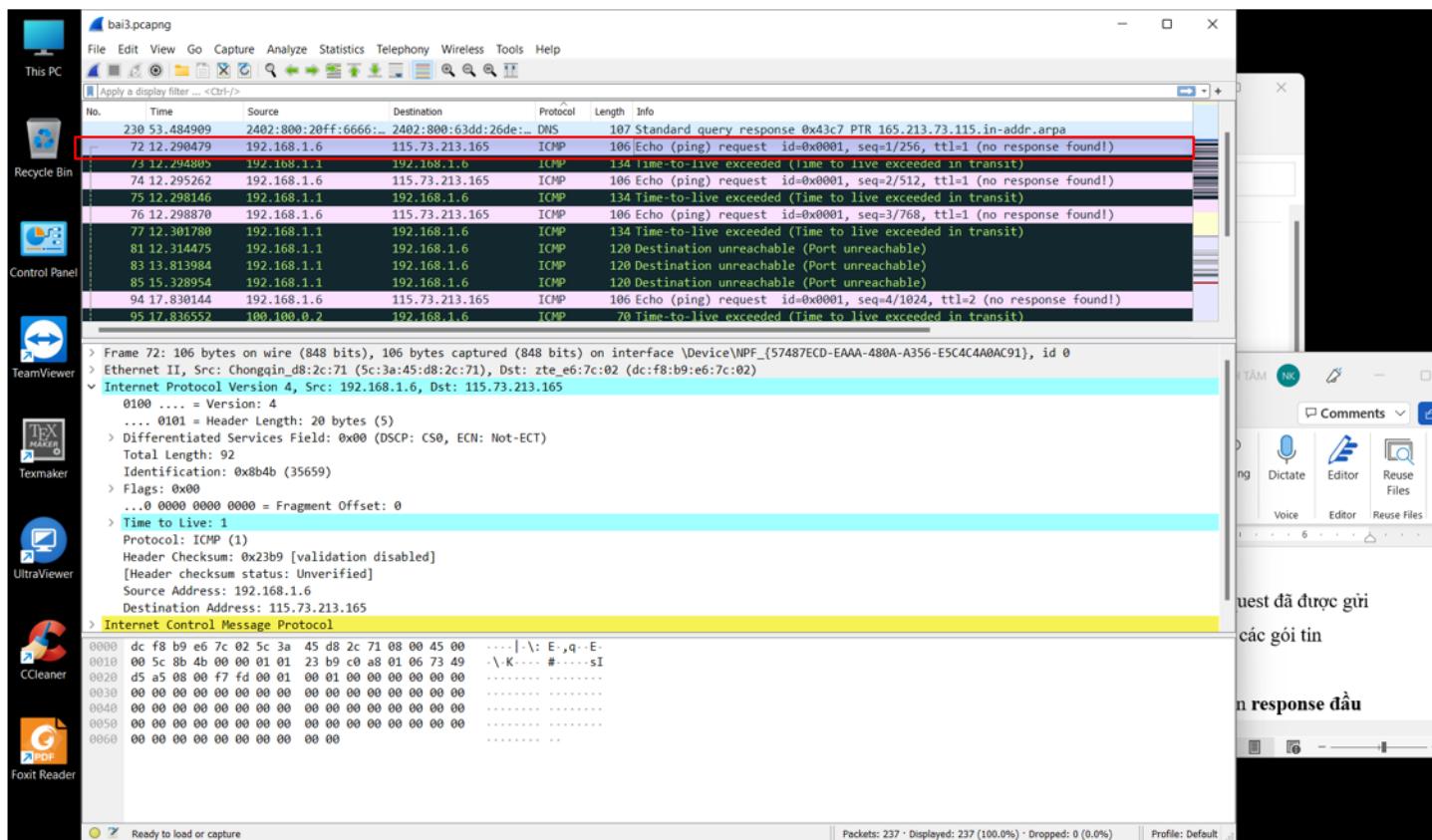


Hình 24: Gói tin DNS query response

**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 trong những gói tin sau đó là ICMP, bắt đầu từ gói tin số 72 trong file **bai3.pcapng** (phần đóng khung màu đỏ trong hình 25).



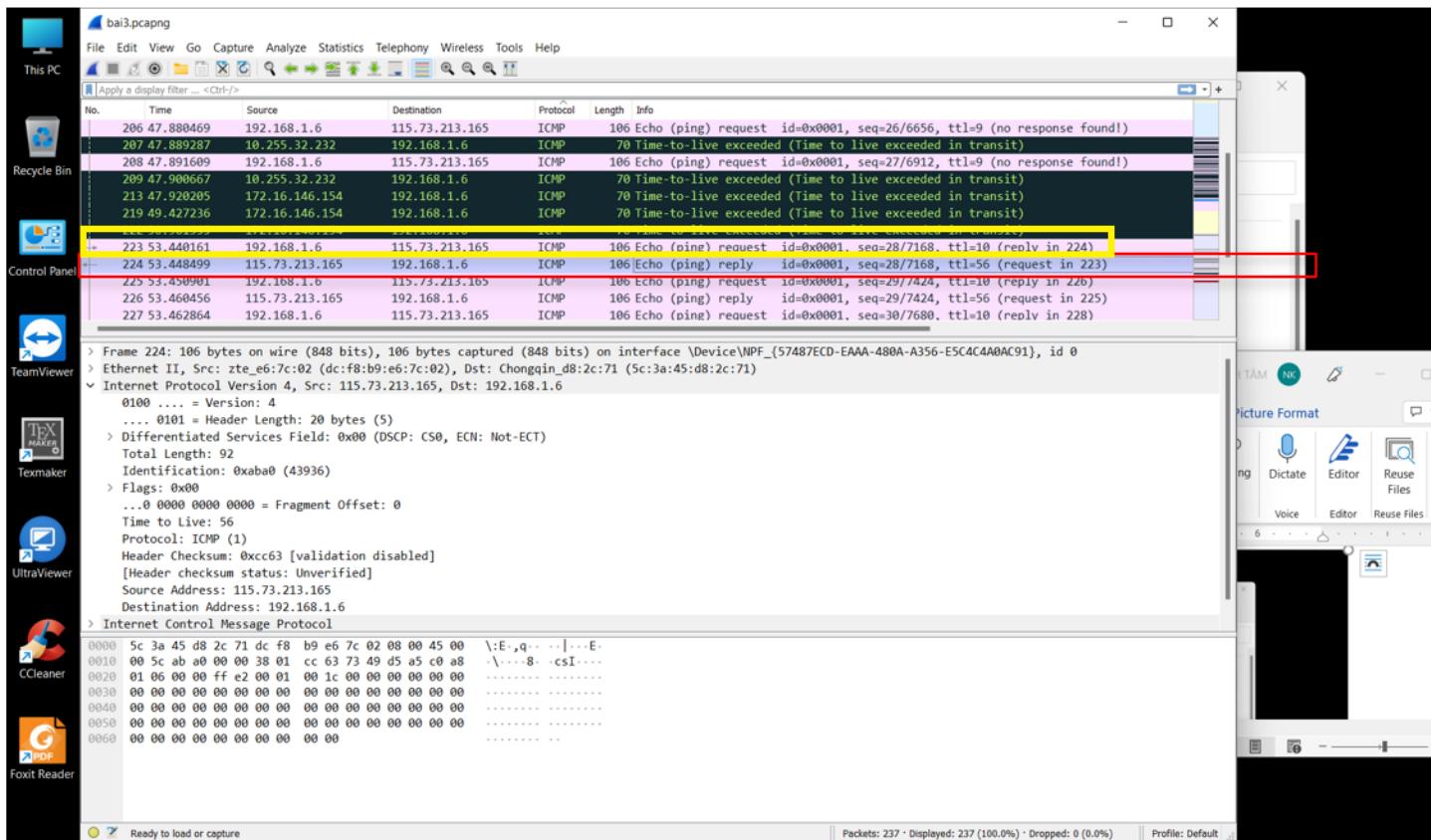
Hình 25: Protocol được sử dụng

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?)

Tính từ gói tin request đầu tiên (gói tin số 72) có tổng cộng **28 gói tin** request đã được gửi trước khi nhận được response message đầu tiên (gói tin số 224), không kể các gói tin không liên quan khác.

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?

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 10 (gói tin 223, phần đóng khung màu vàng trong hình 26).



Hình 26: TTL của gói tin cuối cùng trước khi nhận response

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 gửi đi không tìm thấy thông tin port. Vì nghỉ thức ICMP hoạt động ở tầng Network, trong khi số hiệu port là “địa chỉ” của ứng dụng, được sử dụng ở tầng Application.

e. Gói tin response đầu tiên là trả lời cho gói tin request thứ mấy? (No.)  
Gói tin response đầu tiên (gói tin số 224) trả lời cho gói tin request thứ 28 (gói tin số 223) (phần đóng khung màu đỏ trong hình 26).

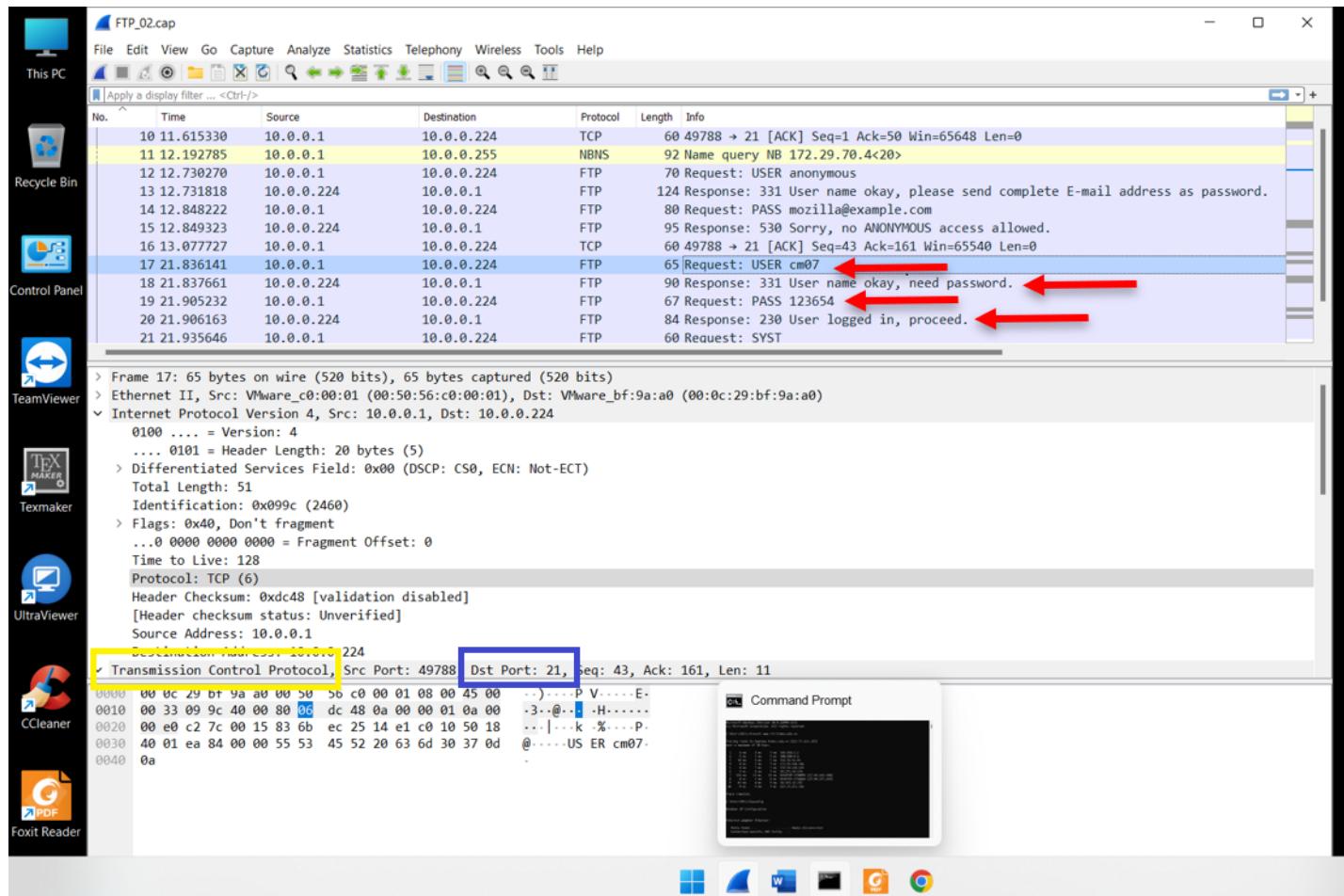
## 6 Bài 4: DHCP

## 7 Bài 5: FTP

Cho tập tin FTP\_02.cap, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau.

a. **FTP sử dụng giao thức nào UDP hay TCP?**

FTP sử dụng giao thức TCP (phần đóng khung màu vàng trong hình 27).



Hình 27: Giao thức được FTP sử dụng

b. Port mặc định của FTP Server để nhận kết nối là bao nhiêu?

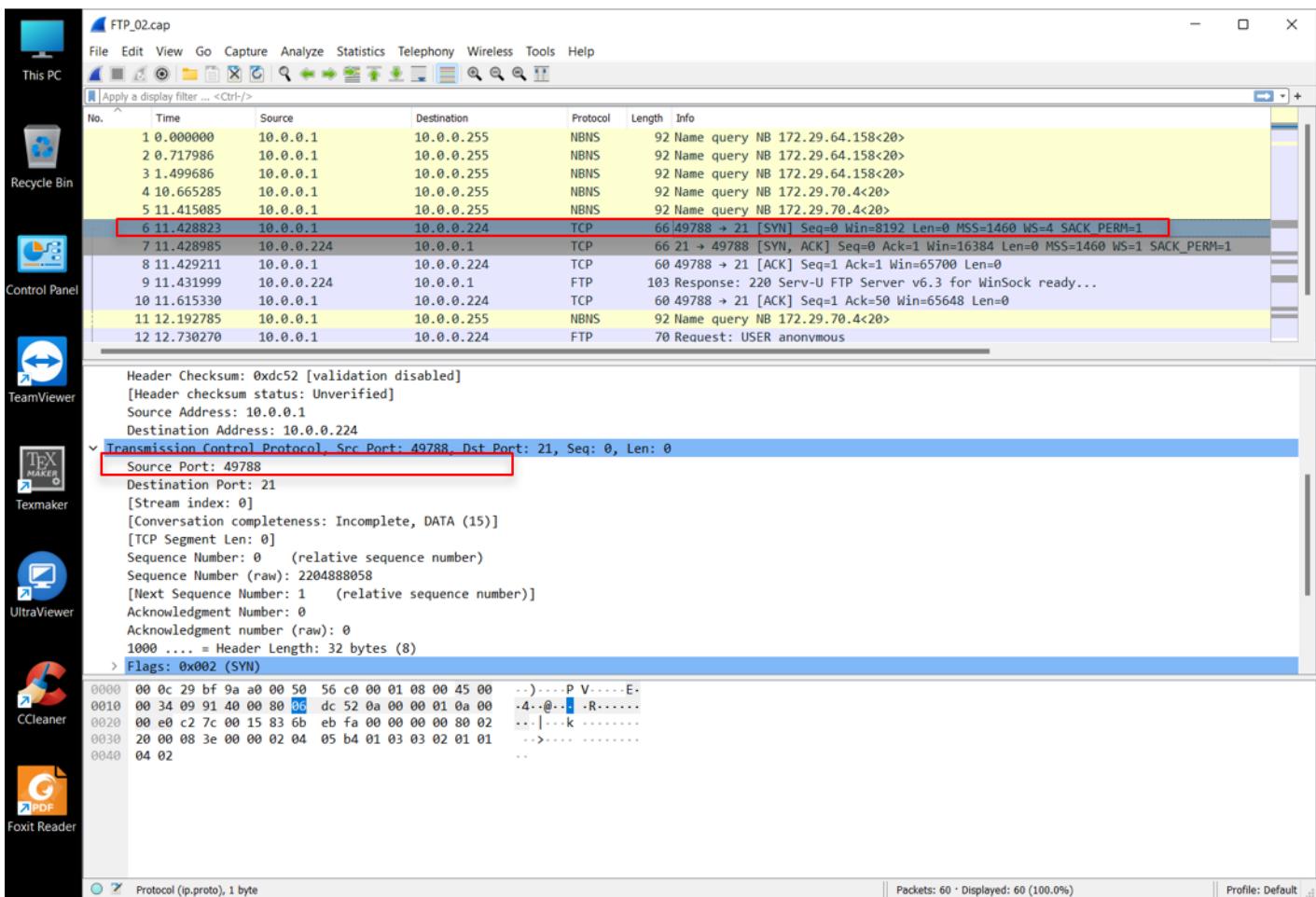
Port mặc định của FTP Server để nhận kết nối là 21 (phần đóng khung màu xanh trong hình 27).

c. Username và password của người dùng là gì?

Username của người dùng là cm07, password là 123654. Các mũi tên màu đỏ trên hình 27 chỉ hiện vị trí thông tin các gói tin tương ứng (các gói tin request, số 17, 19; và các gói tin response tương ứng, số 18, 20). Còn user anonymous ở phía trên không được cho phép kết nối (các gói tin 12 đến 15).

d. Port truyền lệnh của client là bao nhiêu?

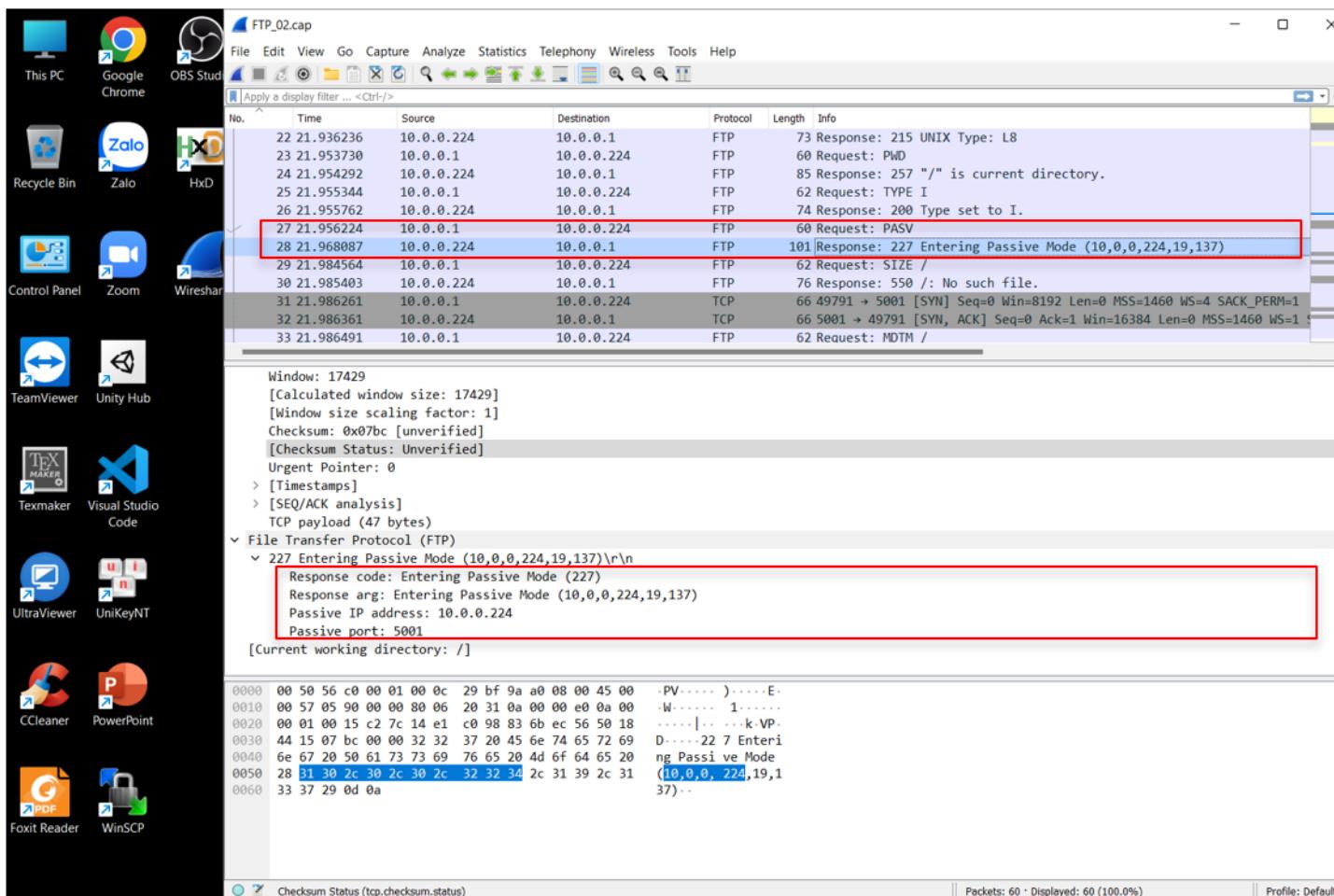
Port truyền lệnh của client là port 49788.



Hình 28: Port truyền lệnh của client

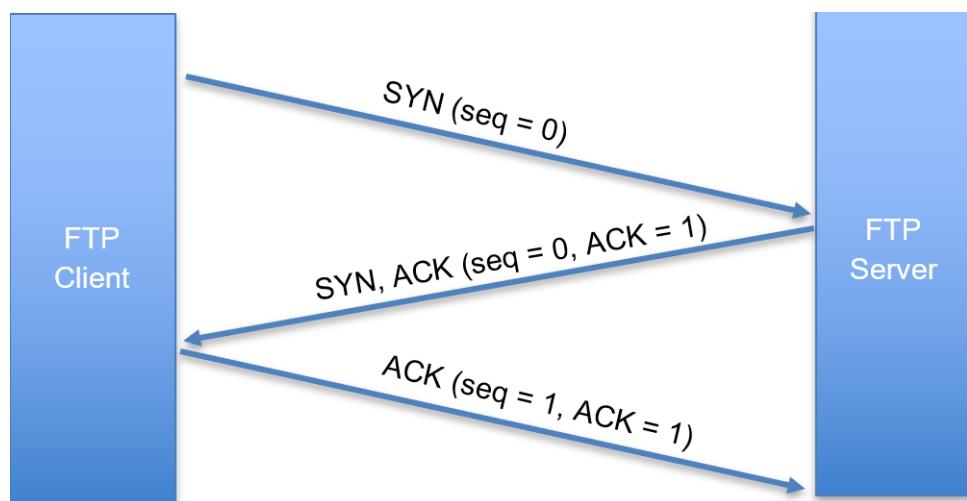
### e. Client truy xuất lên server theo mode nào: active hay passive?

Client truy xuất lên server theo mode mặc định là active. Muốn chuyển sang mode passive client cần gửi gói tin request PASV.

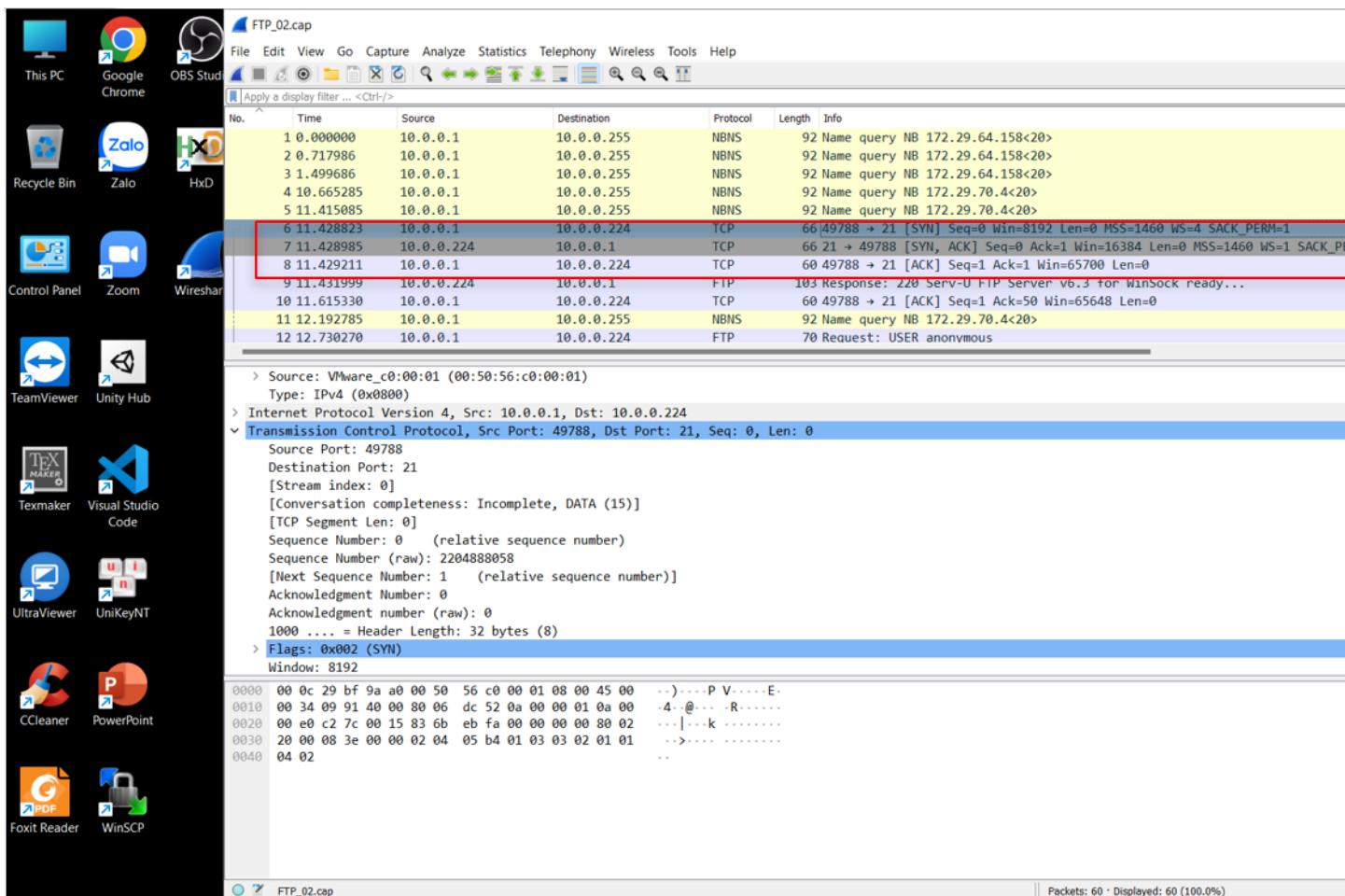


Hình 29: Mode truy xuất của client lên server

f. Chỉ ra quá trình bắt tay 3 bước của client và server để tạo kết nối ban đầu khi thực hiện username và password.

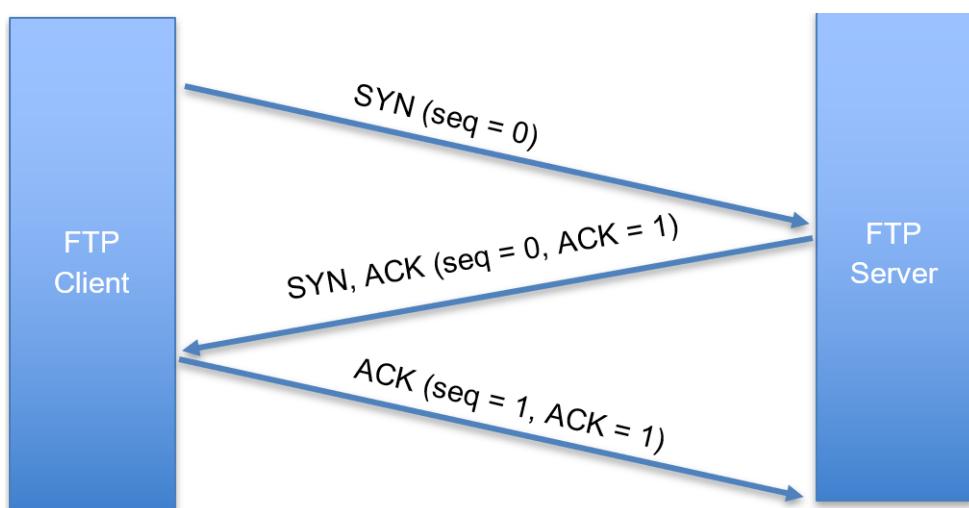


Hình 30: Quá trình bắt tay 3 bước để tạo kết nối ban đầu

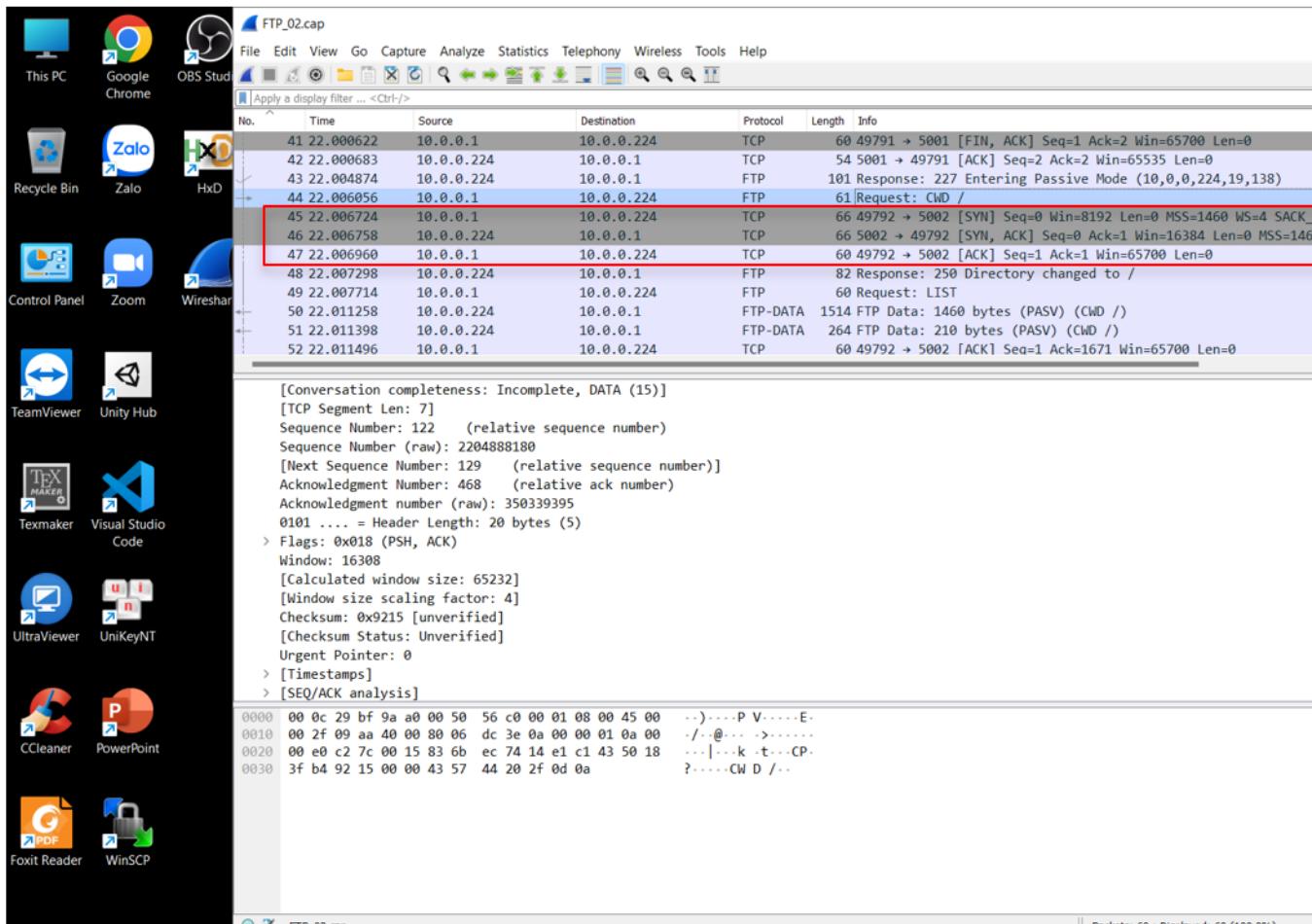


Hình 31: Quá trình bắt tay 3 bước để tạo kết nối ban đầu

g. Chỉ ra quá trình bắt tay 3 bước của client và server để tạo kết nối truyền dữ liệu.



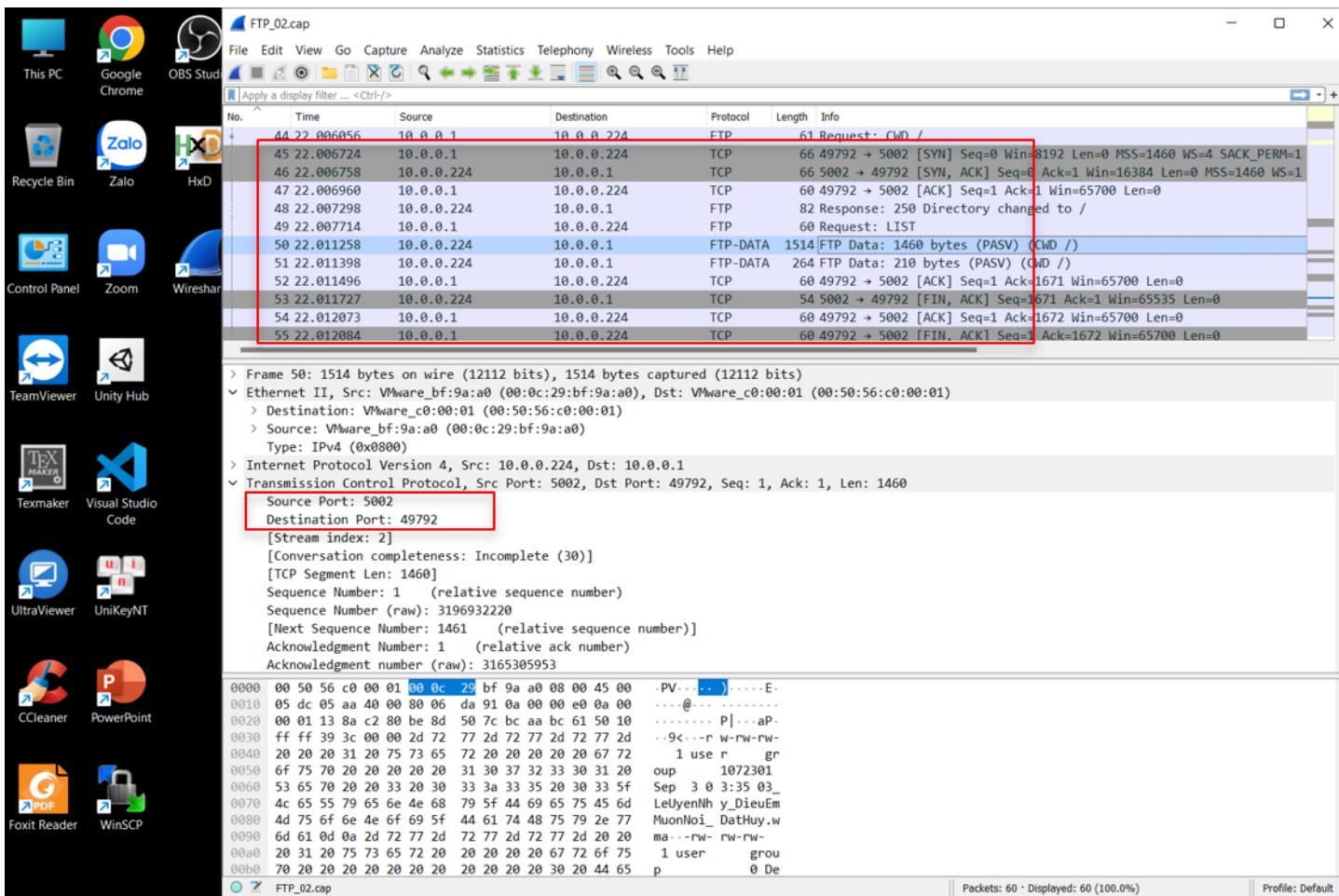
Hình 32: Quá trình bắt tay 3 bước để tạo kết nối truyền dữ liệu



Hình 33: Quá trình bắt tay 3 bước để tạo kết nối truyền dữ liệu

#### **h. Port truyền dữ liệu của FTP server và client là bao nhiêu?**

Port truyền dữ liệu của FTP server và client tương ứng là 5002 và 49792. Kết nối này được tạo bởi quá trình bắt tay ba bước ở câu g nêu trên, cụ thể thể hiện ở các gói tin số 45, 46, 47. Các gói tin liên quan được kẻ khung màu đỏ ở phía trên, khung màu đỏ ở hình 34 (ứng với gói tin số 50, chuyển data từ FTP server sang FTP client) cũng nêu ra port tương ứng.



Hình 34: Port truyền dữ liệu của FTP server và client

Trước đó, port truyền dữ liệu của FTP Server và Client tương ứng là 5001 và 49791 (thông tin tương ứng ở các gói tin 31, 32, 34 thể hiện quá trình bắt tay ba bước được nêu ở câu g), và bị ngắt kết nối (các gói tin [FIN,ACK] và [ACK] từ 39 – 42 thể hiện quá trình này).

## 8 Tài liệu tham khảo

### References

- [1] Keith W. Ross James F. Kurose. *Computer Networking: A Top-Down Approach.* 6th ed. Pearson, 2013, p. 354. ISBN: 978-0-13-285620-1.
- [2] Khoa Công nghệ Thông tin. *Slides bài giảng môn học Mạng máy tính.*