

**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

1	Thông tin của nhóm	3
2	Mức độ hoàn thành	3
3	Bài 1: Ping	4
4	Bài 2: HTTP	8
5	Bài 3: Traceroute	18
6	Bài 4: DHCP	24
7	Bài 5: FTP	26
8	Tài liệu tham khảo	32

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	Kết quả sau khi bắt gói tin DHCP	24
28	Nghi thức tầng Transport được DHCP message sử dụng	25
29	Giao thức được FTP sử dụng	26
30	Port truyền lệnh của client	27
31	Mode truy xuất của client lên server	28
32	Quá trình bắt tay 3 bước để tạo kết nối ban đầu	28
33	Quá trình bắt tay 3 bước để tạo kết nối ban đầu	29
34	Quá trình bắt tay 3 bước để tạo kết nối truyền dữ liệu	29
35	Quá trình bắt tay 3 bước để tạo kết nối truyền dữ liệu	30
36	Port truyền dữ liệu của FTP server và client	31

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 ^A T _E 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)

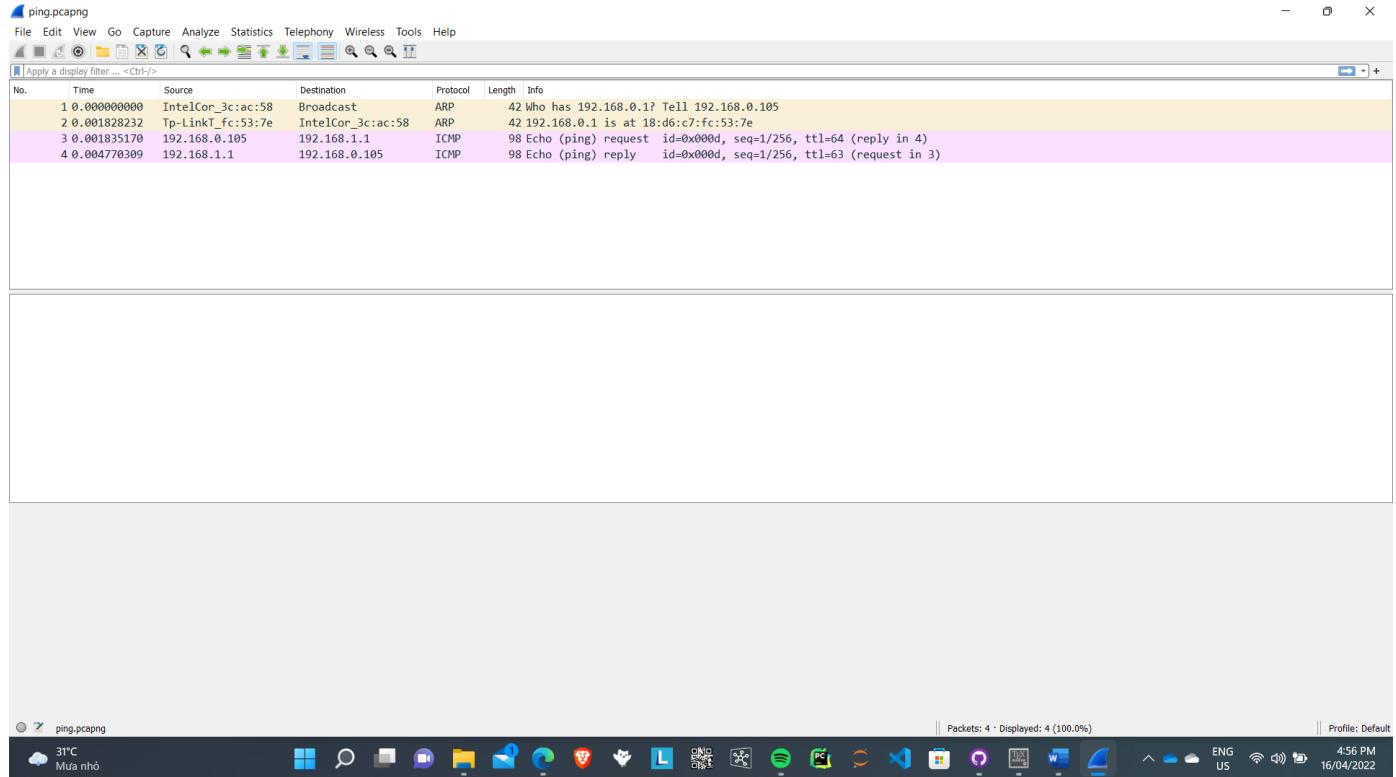
Bài 4:

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.



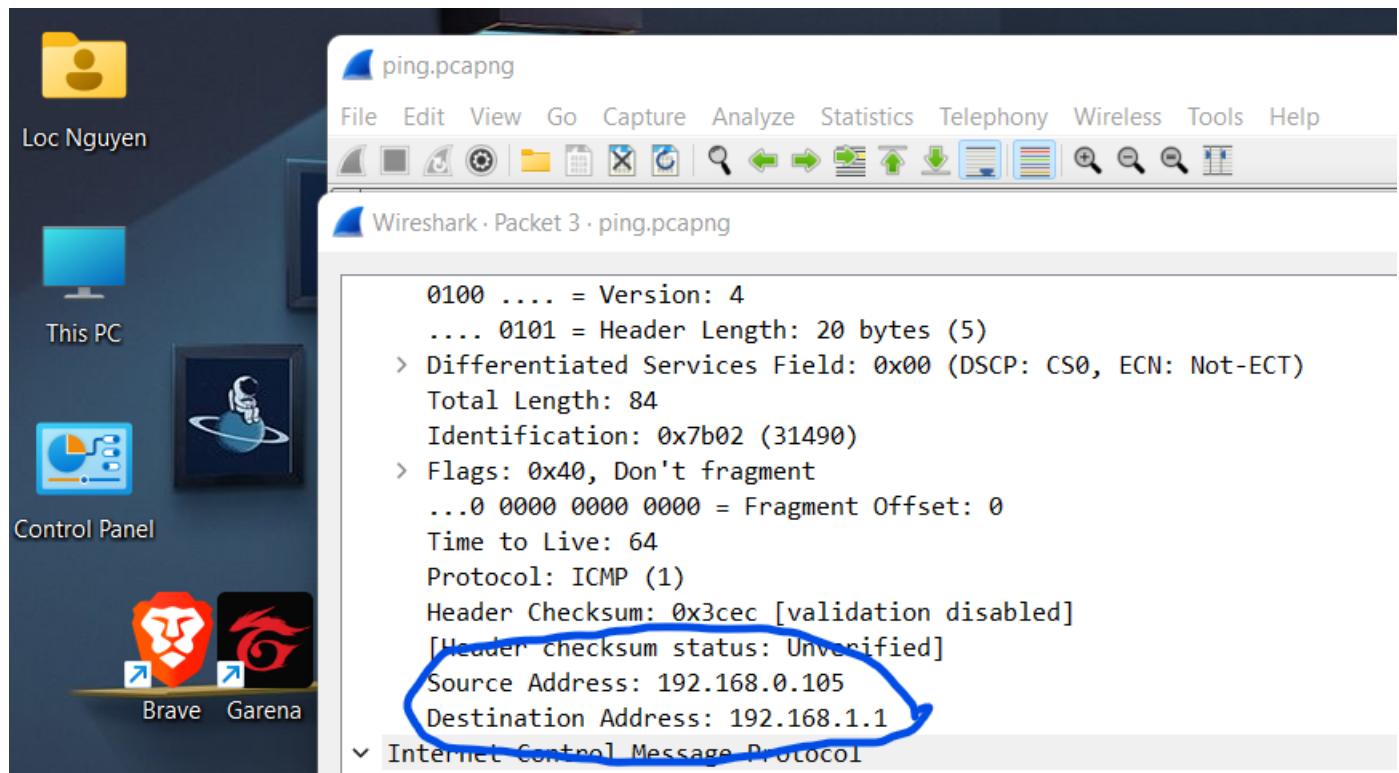
Hình 1: Nội dung tập tin ***ping.pcapng***

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?

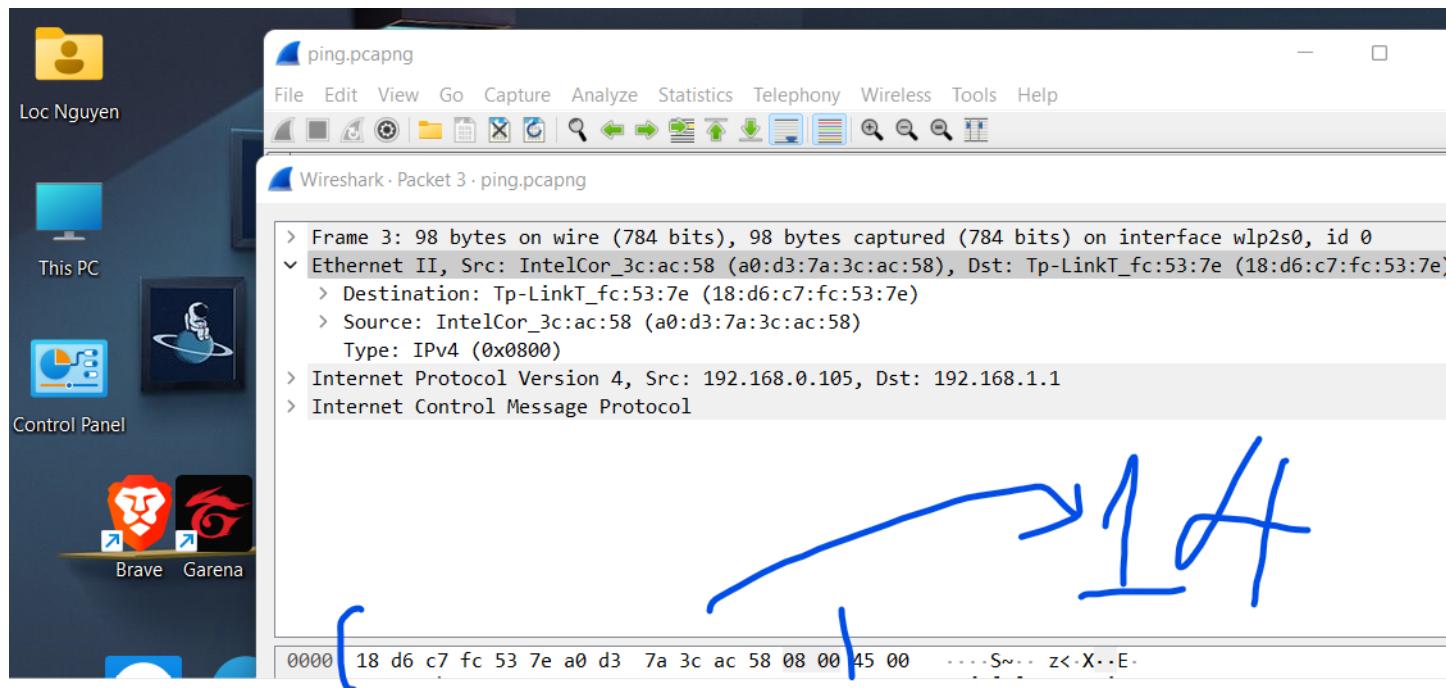
Không có source port number và destination port number.

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.

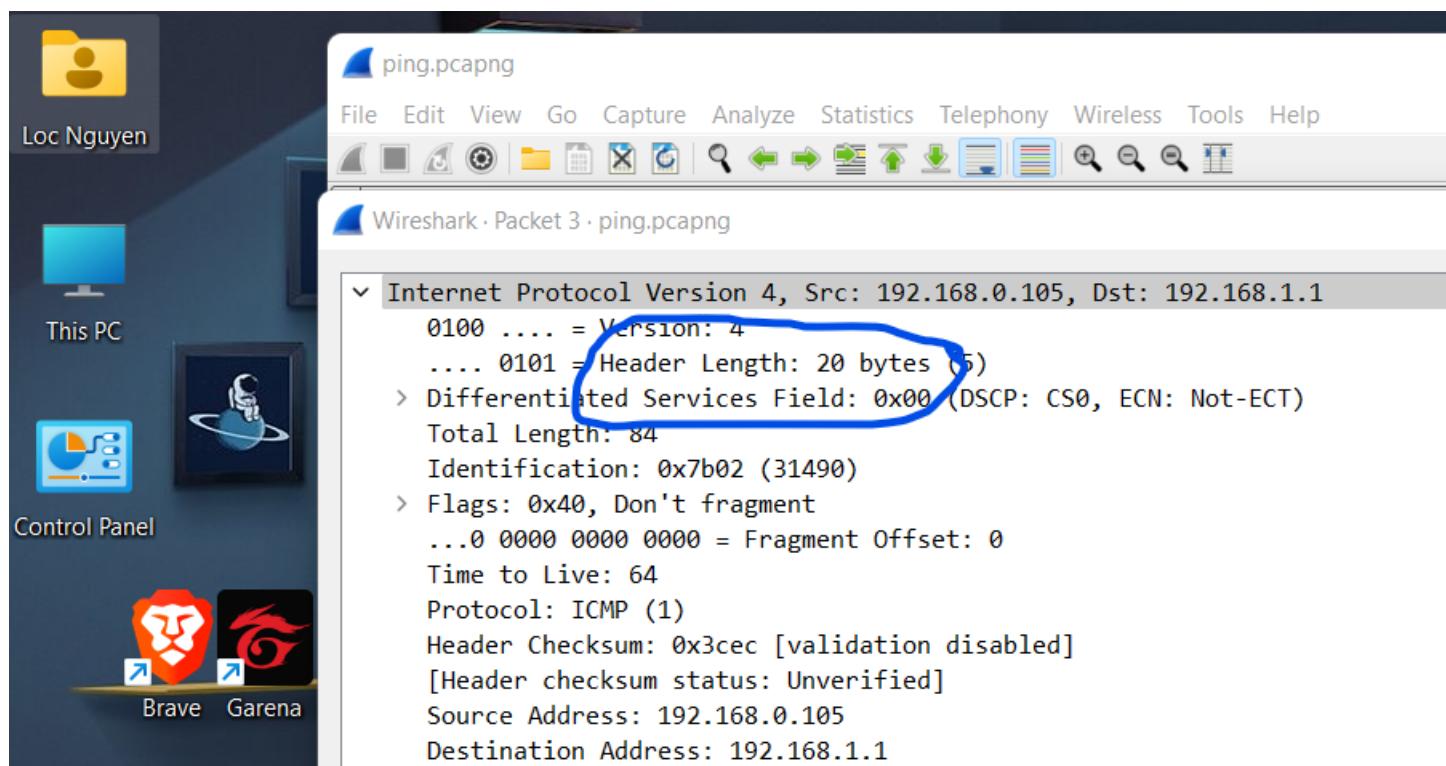
3. Với gói tin ICMP request, cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

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

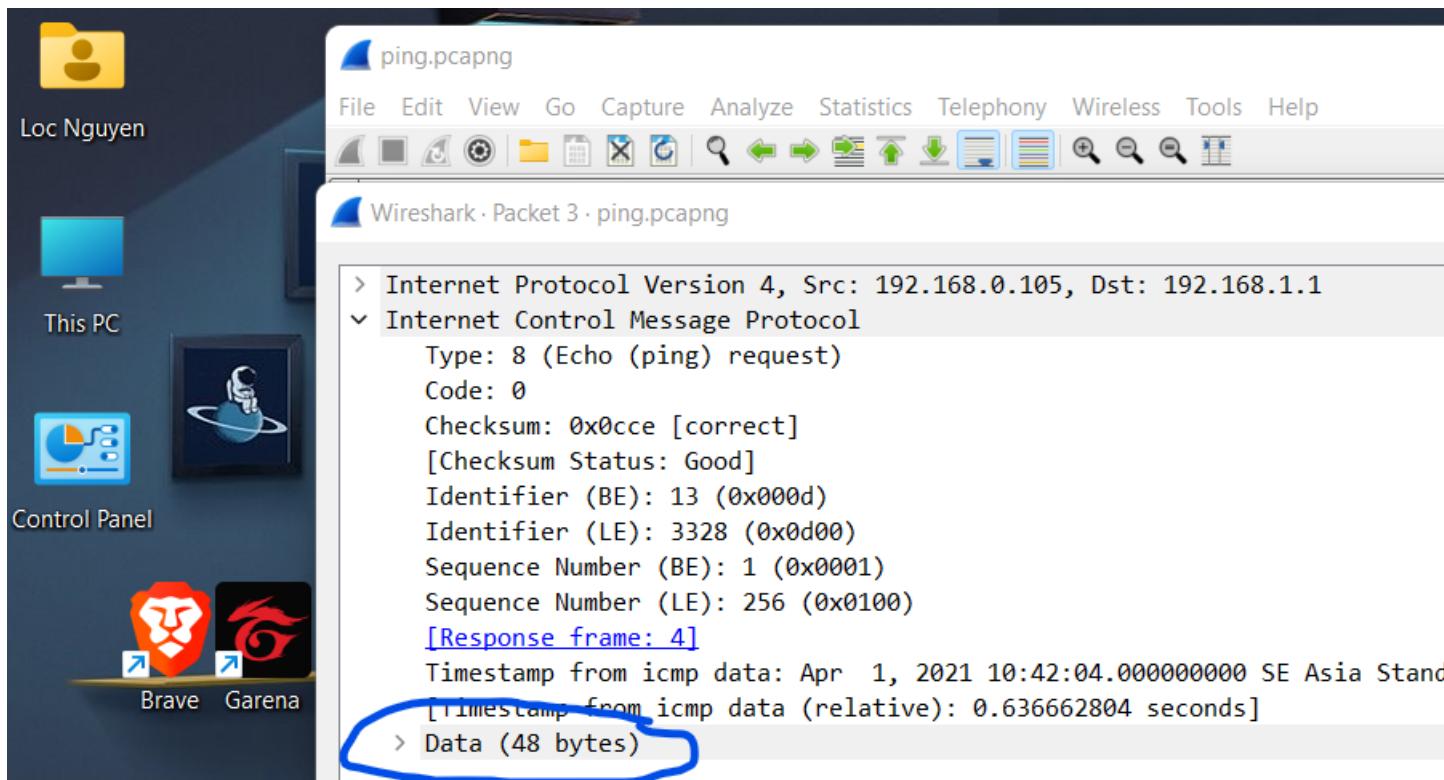
Bảng 2: Kích thước gói tin ICMP request



Hình 3: Độ dài Ethernet header



Hình 4: Độ dài IP header



Hình 5: Độ dài ICMP data và ICMP header

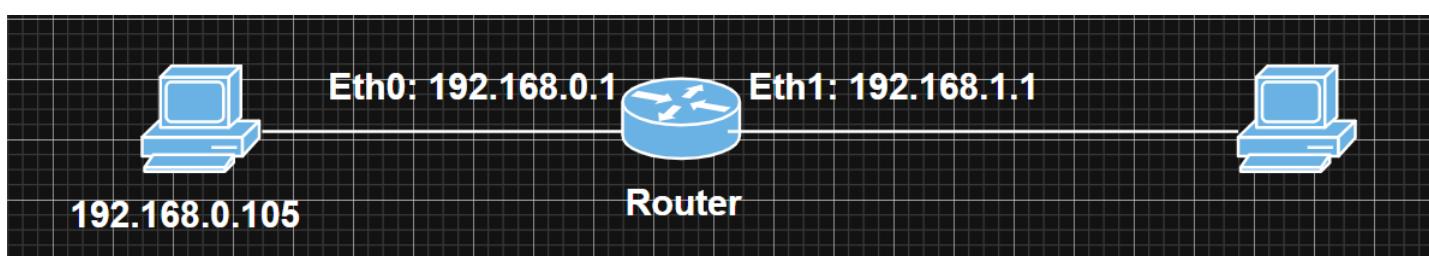
4. Tại sao lại có 2 gói ARP?

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

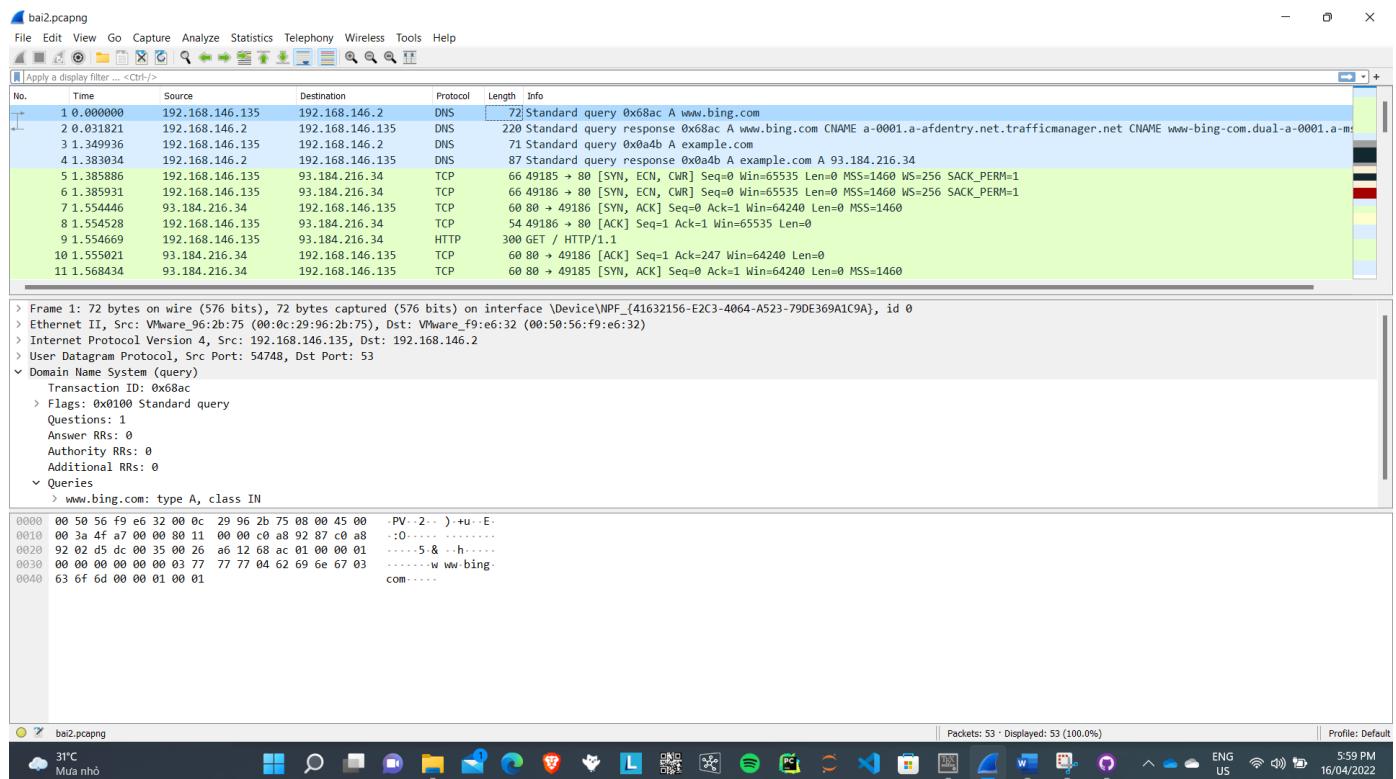
4 Bài 2: HTTP

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**.

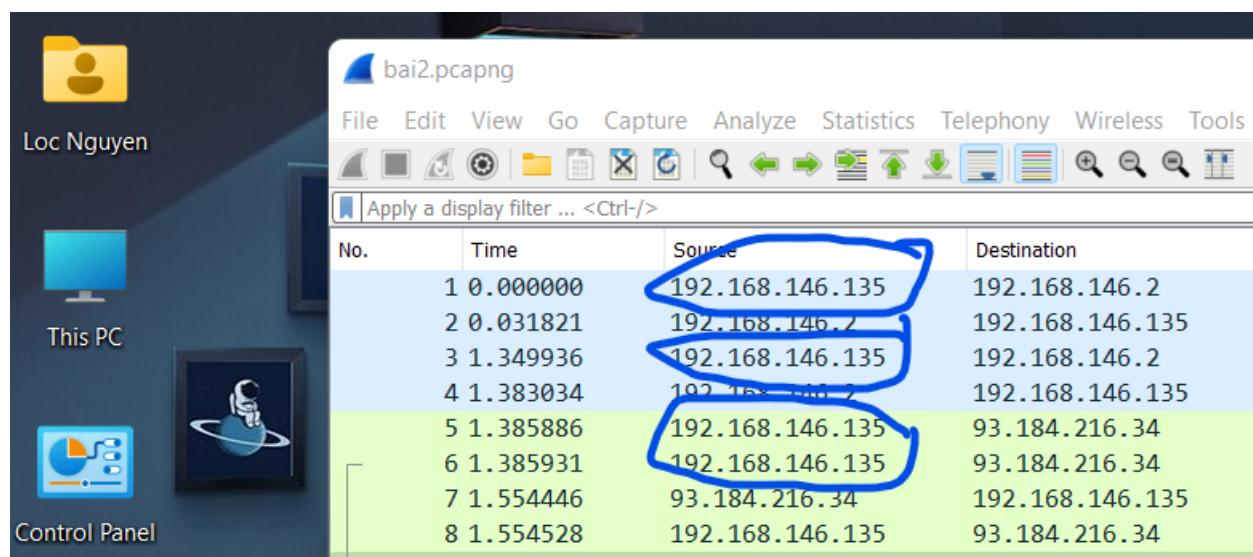
1. Chụp hình kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request (thấy được những gói tin liên quan).



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

2. Cho biết IP của host.

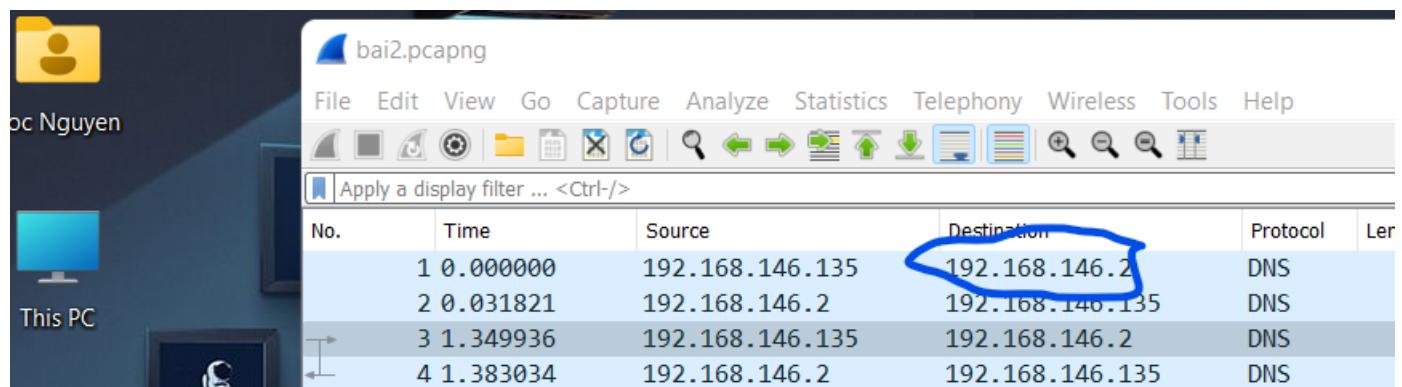
IP của host là: 192.168.146.135.



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

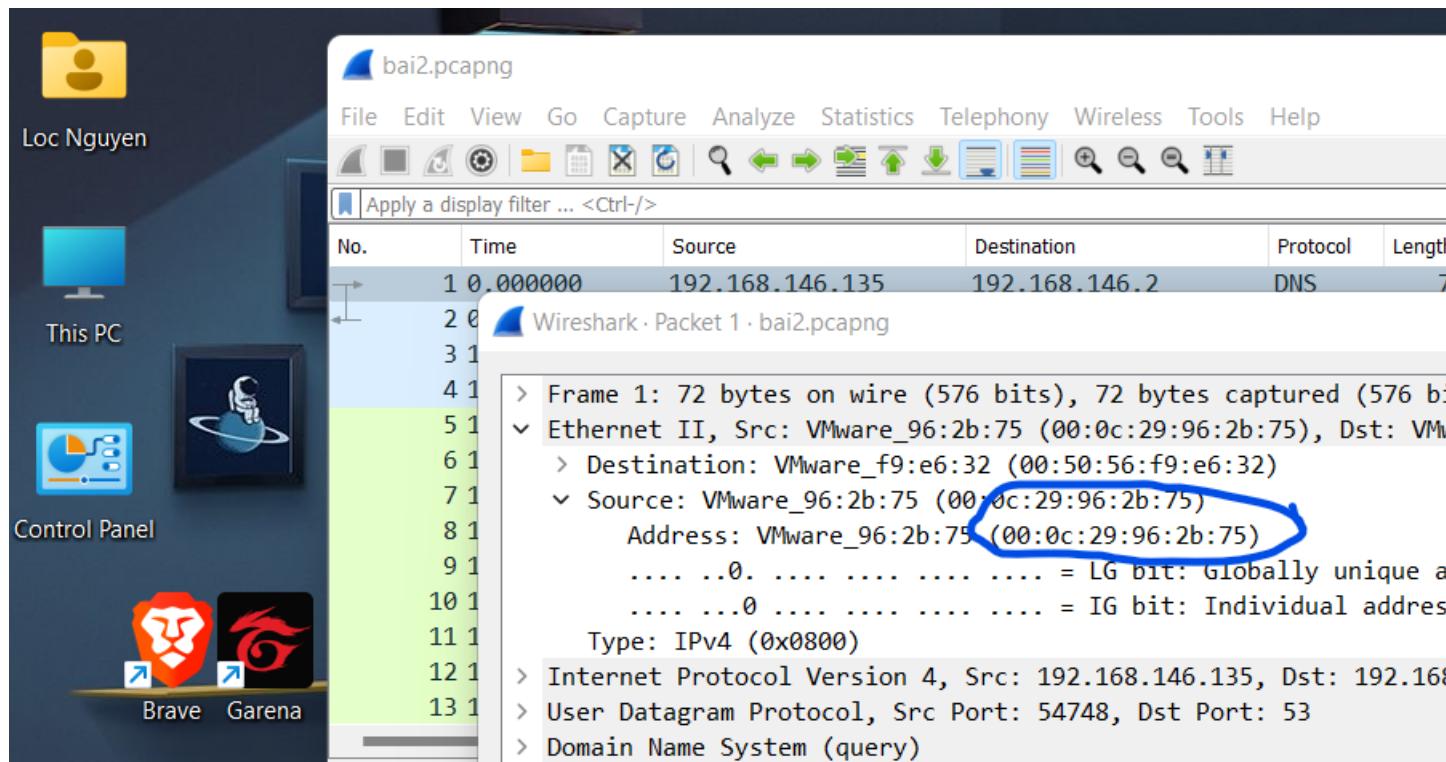
3. Cho biết IP của router (default gateway) (nếu không thấy được thì trả lời không có và giải thích tại sao)
 IP của router là: **192.168.146.2**.



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

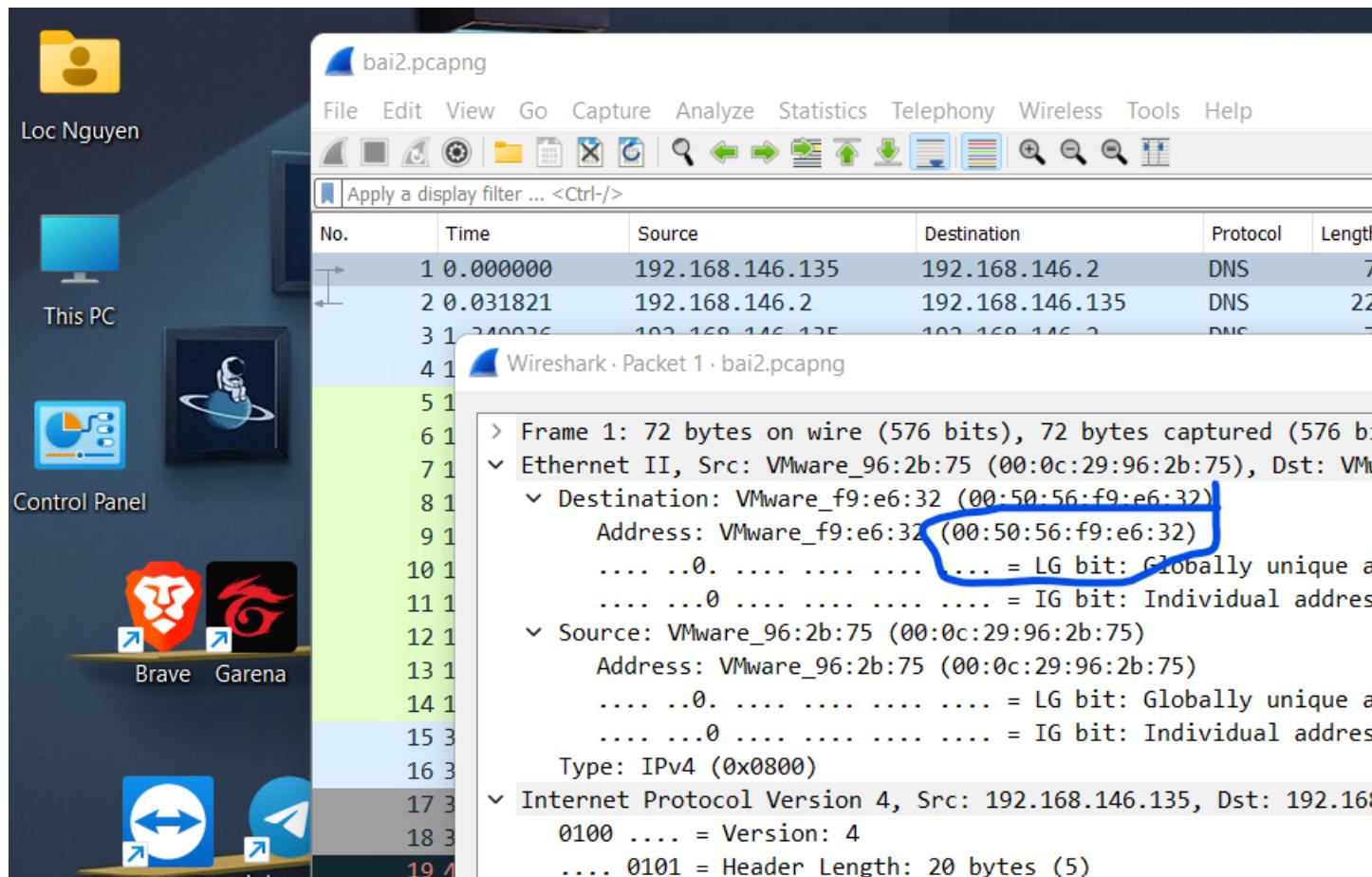
4. Cho biết địa chỉ MAC của host.
 Địa chỉ MAC của host là: **00:0c:29:96:2b:75**.



Hình 10: Địa chỉ MAC của host

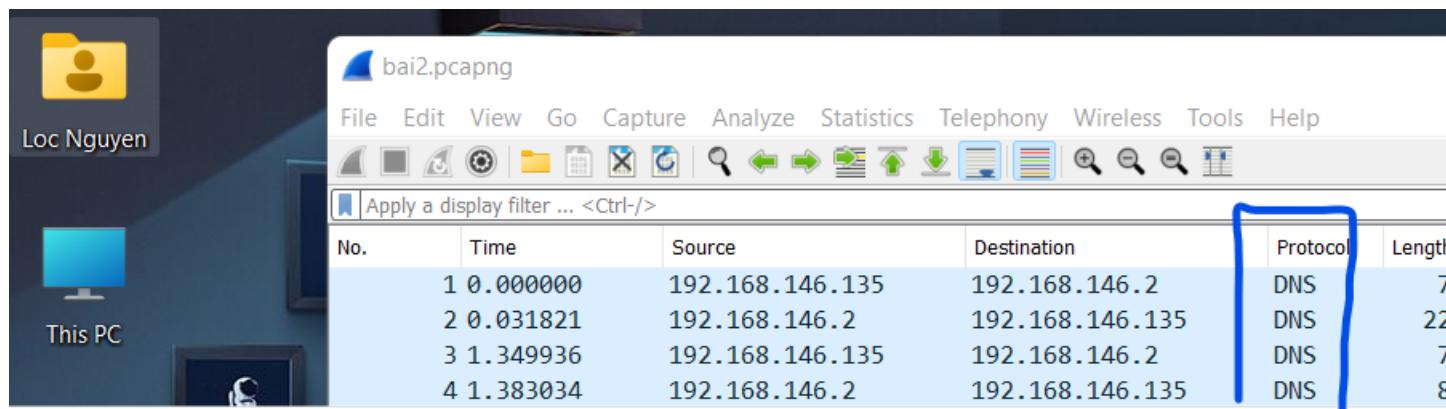
5. Cho biết địa chỉ MAC của router (default gateway).

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



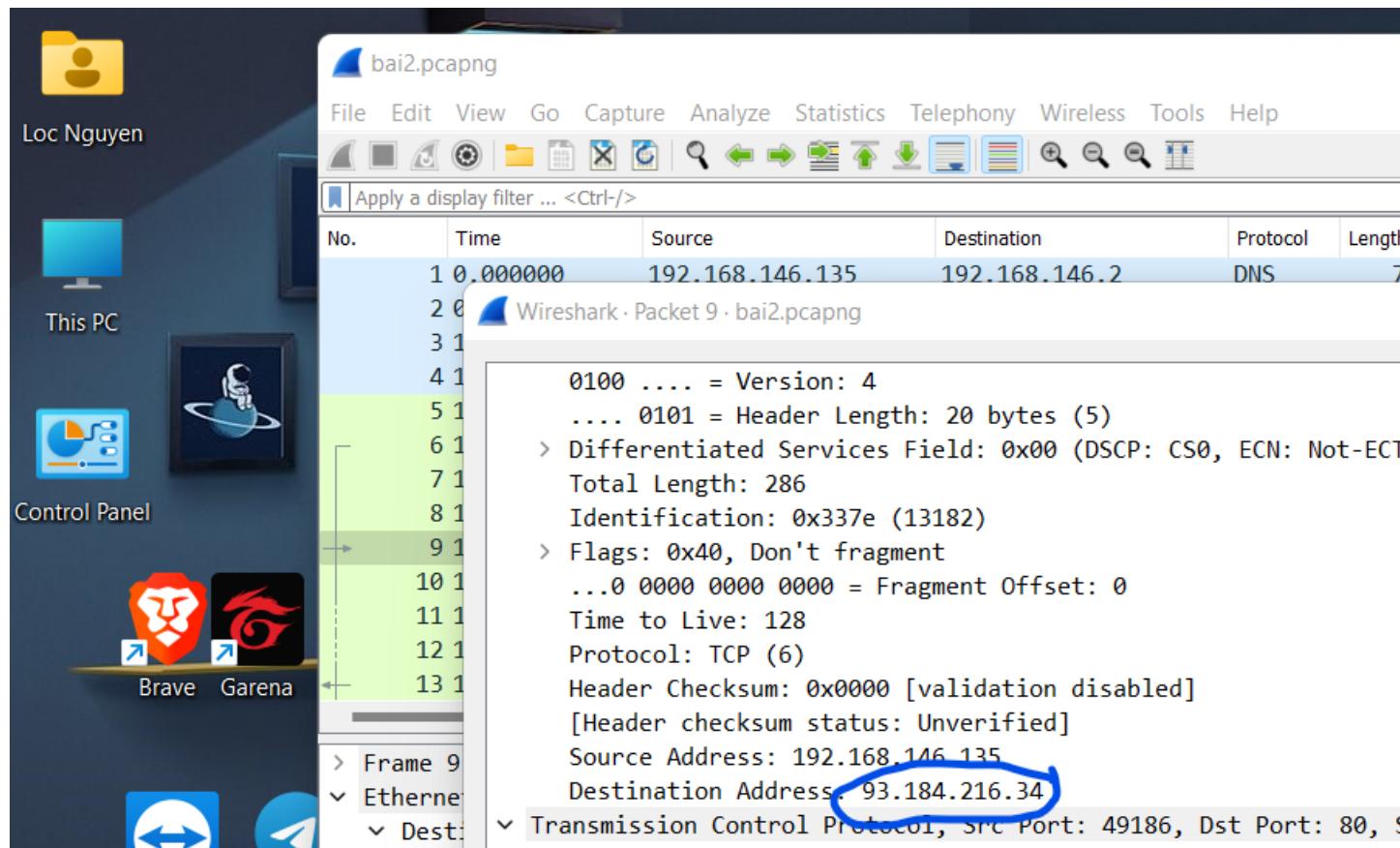
Hình 11: Địa chỉ MAC của router

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**.



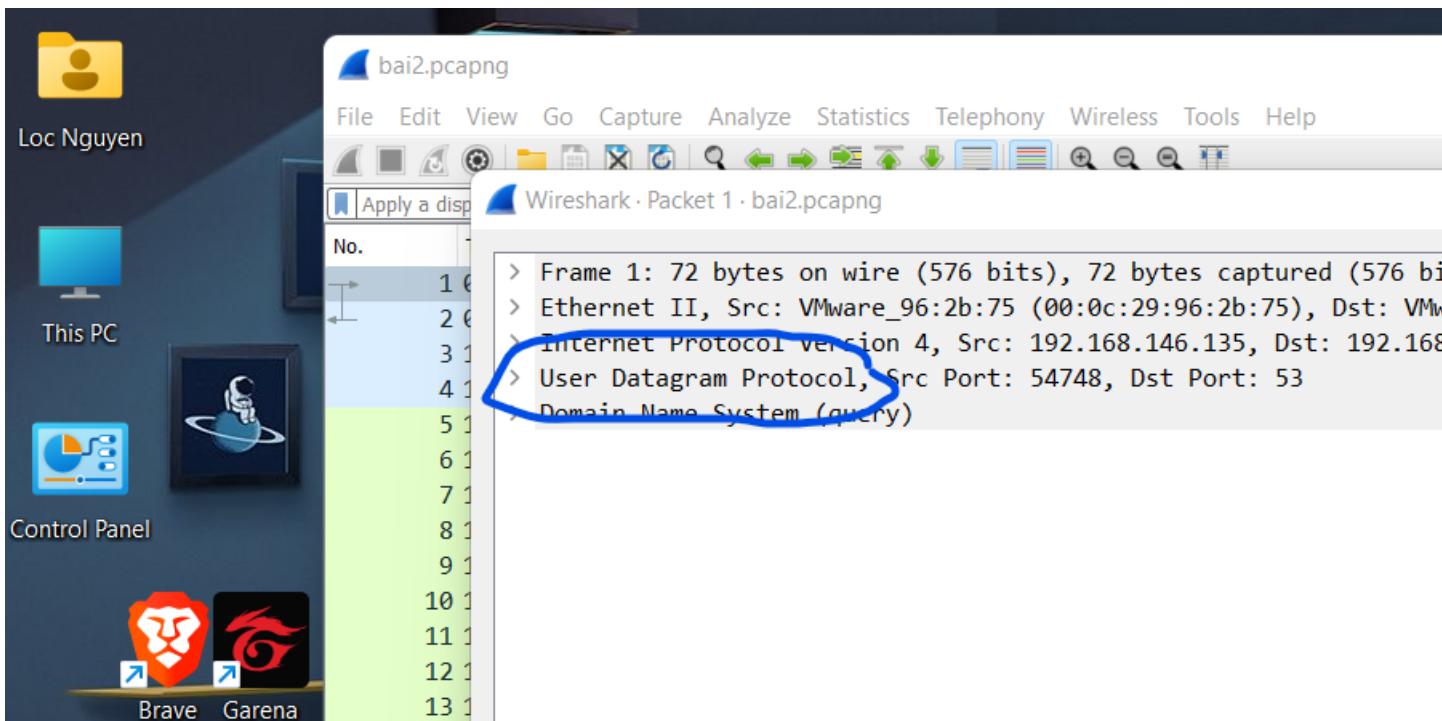
Hình 12: Protocol phân giải tên miền

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

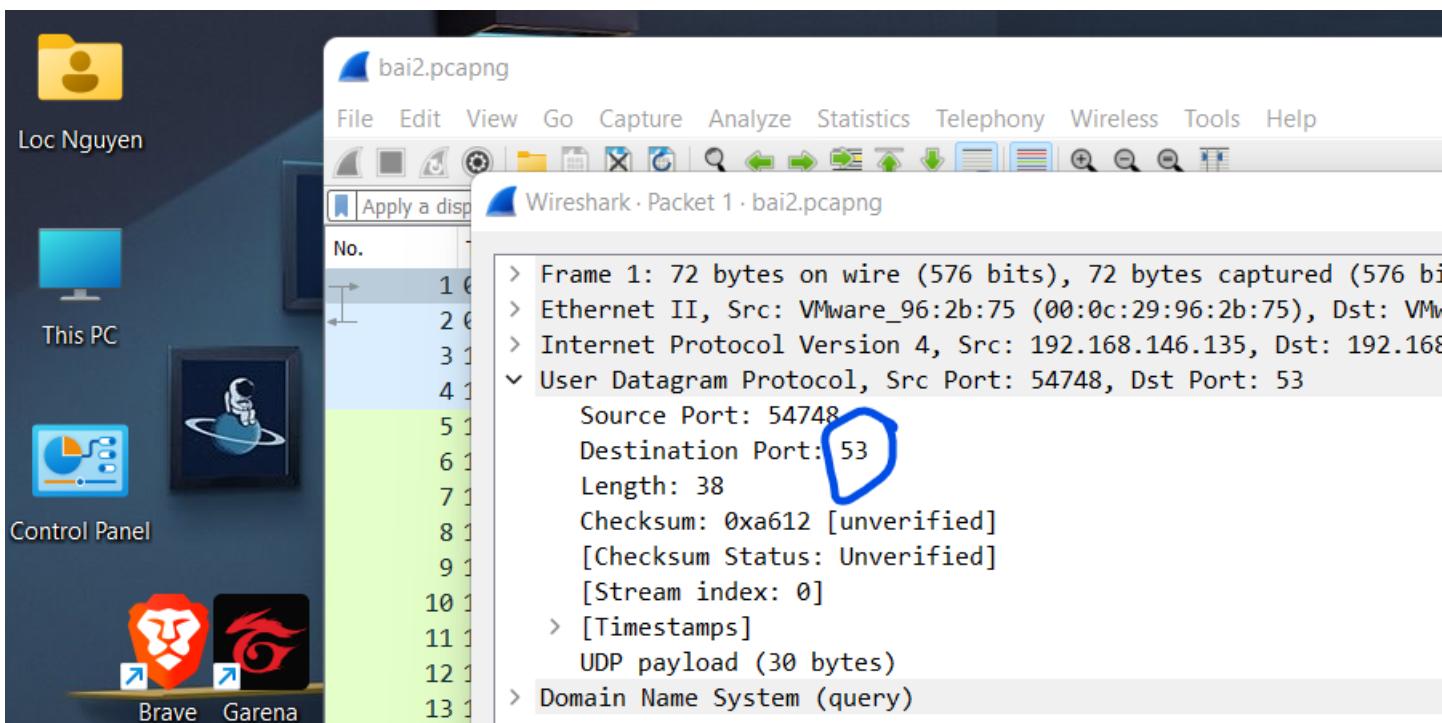
8. Cho biết protocol của tầng Transport được sử dụng bởi DNS.
DNS sử dụng protocol **UDP** của tầng Transport.



Hình 14: Nghi thức được DNS sử dụng

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

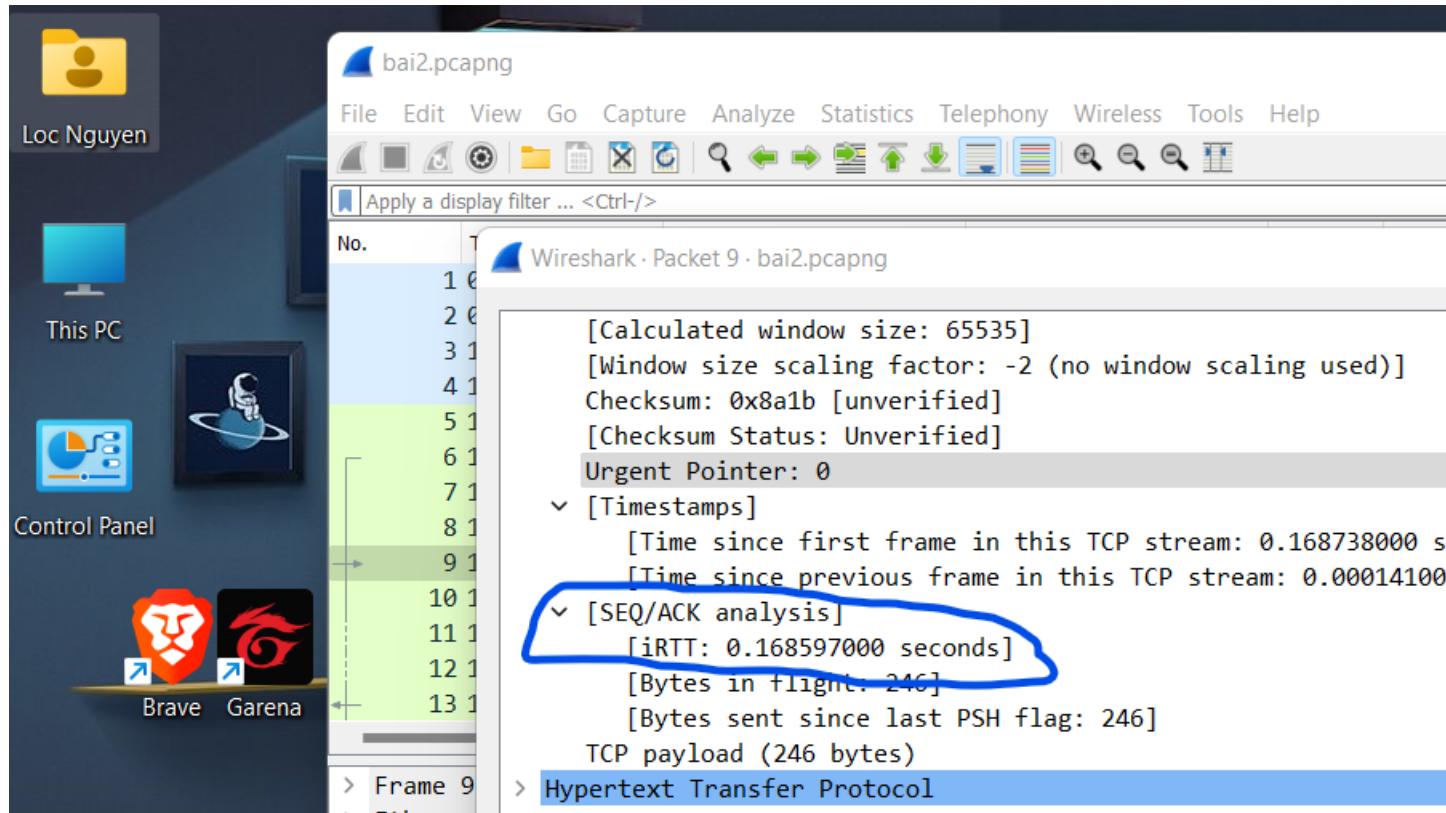
Port sử dụng khi truy vấn DNS server: **port 53**.



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.**



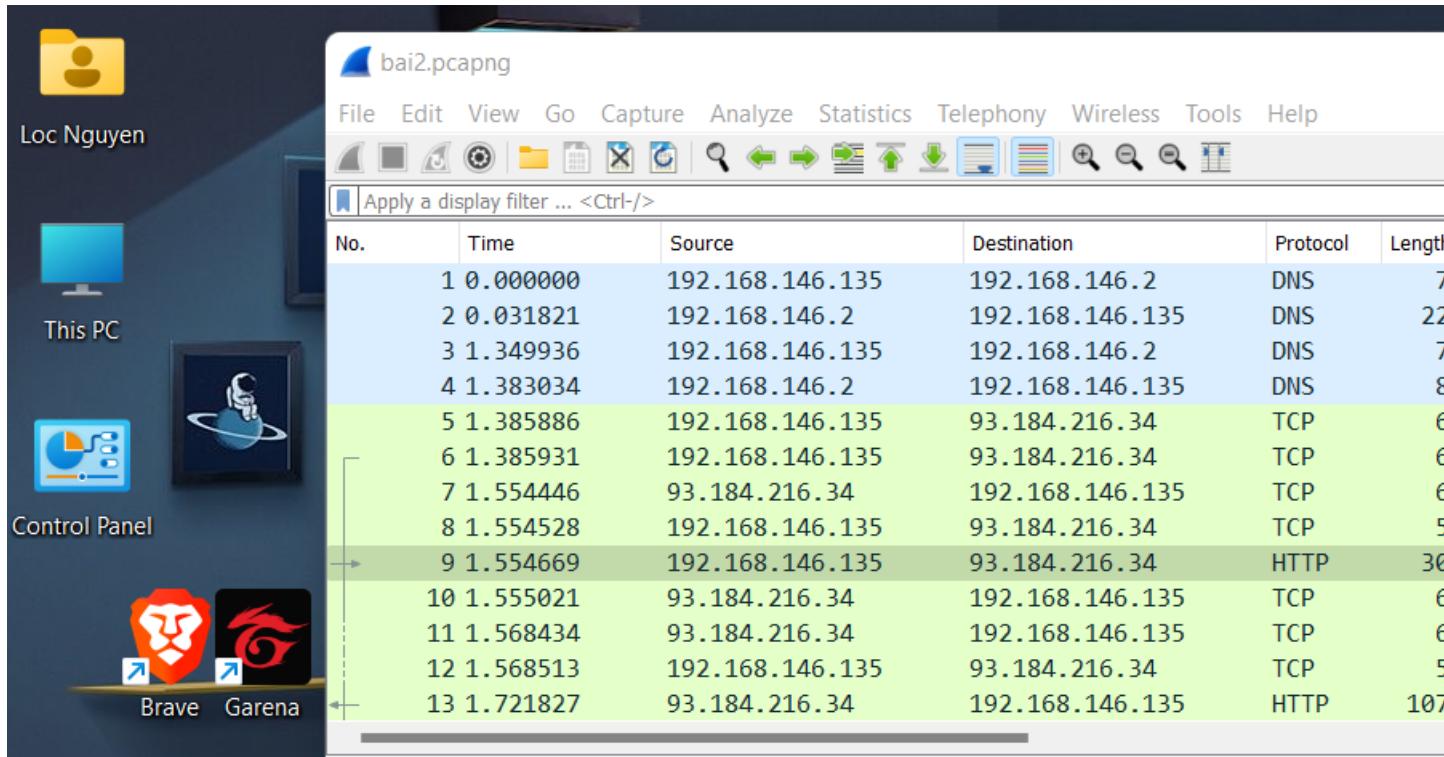
Hình 16: Thời gian hoàn thành quá trình 3-way handshake

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**.

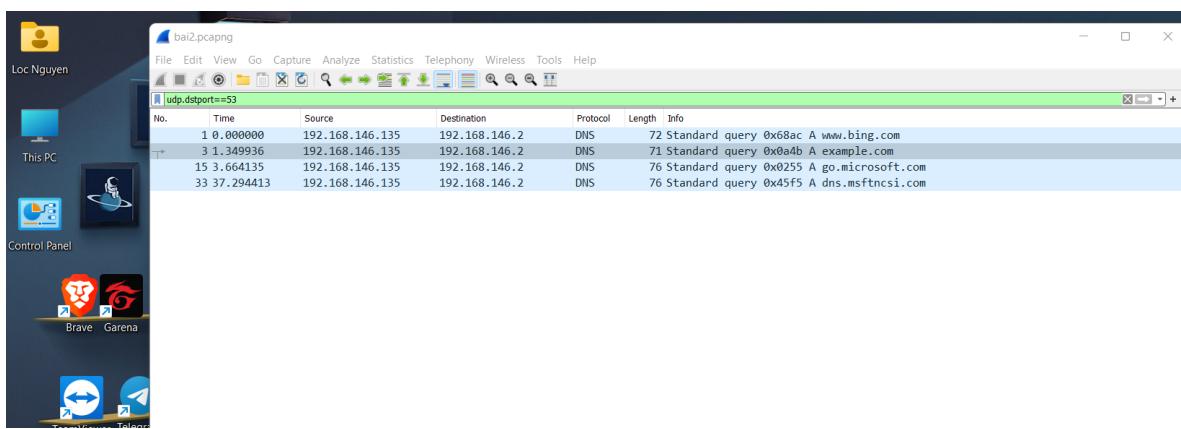


Hình 17: Version HTTP

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.

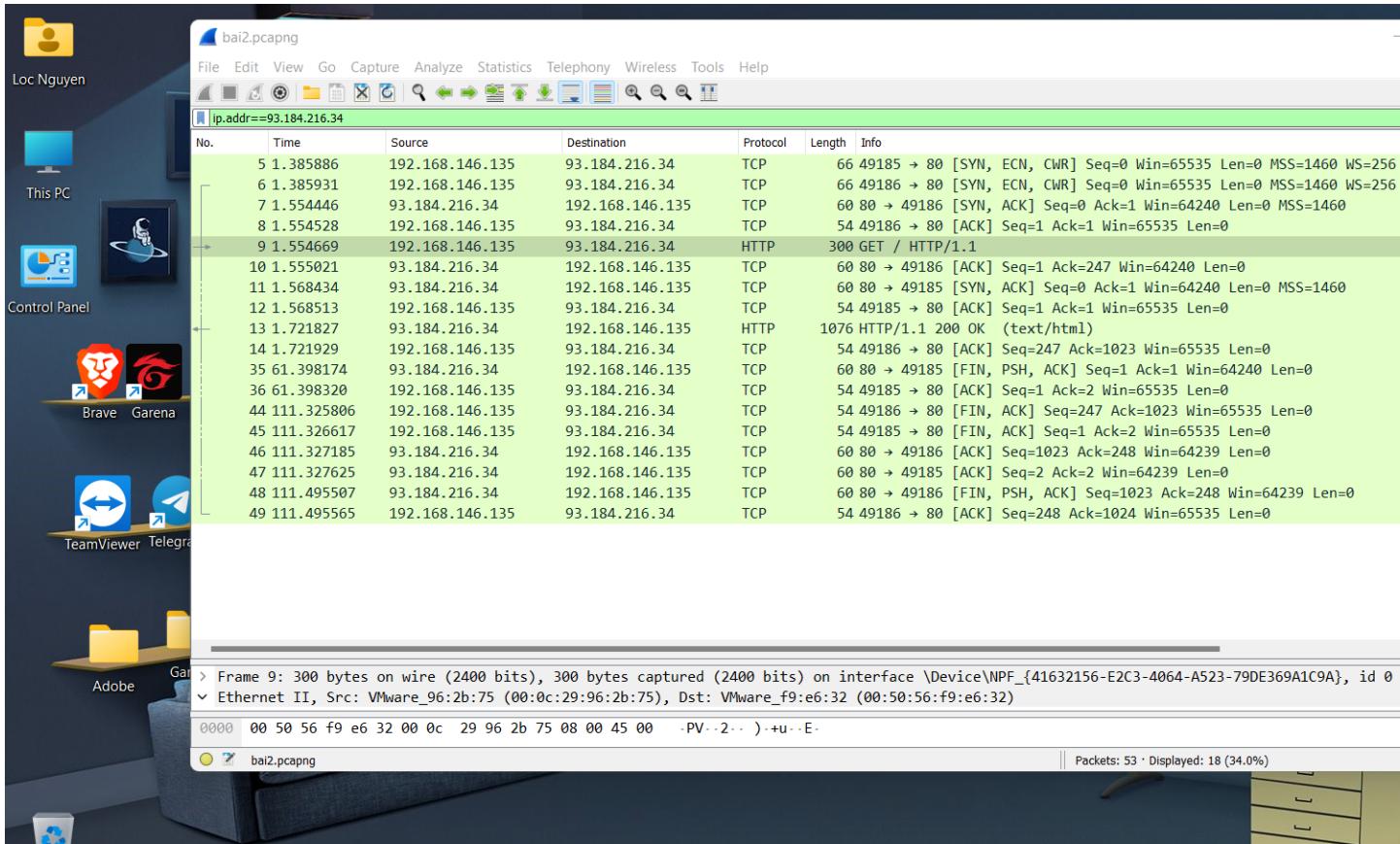
Kết quả của query này như sau.

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.

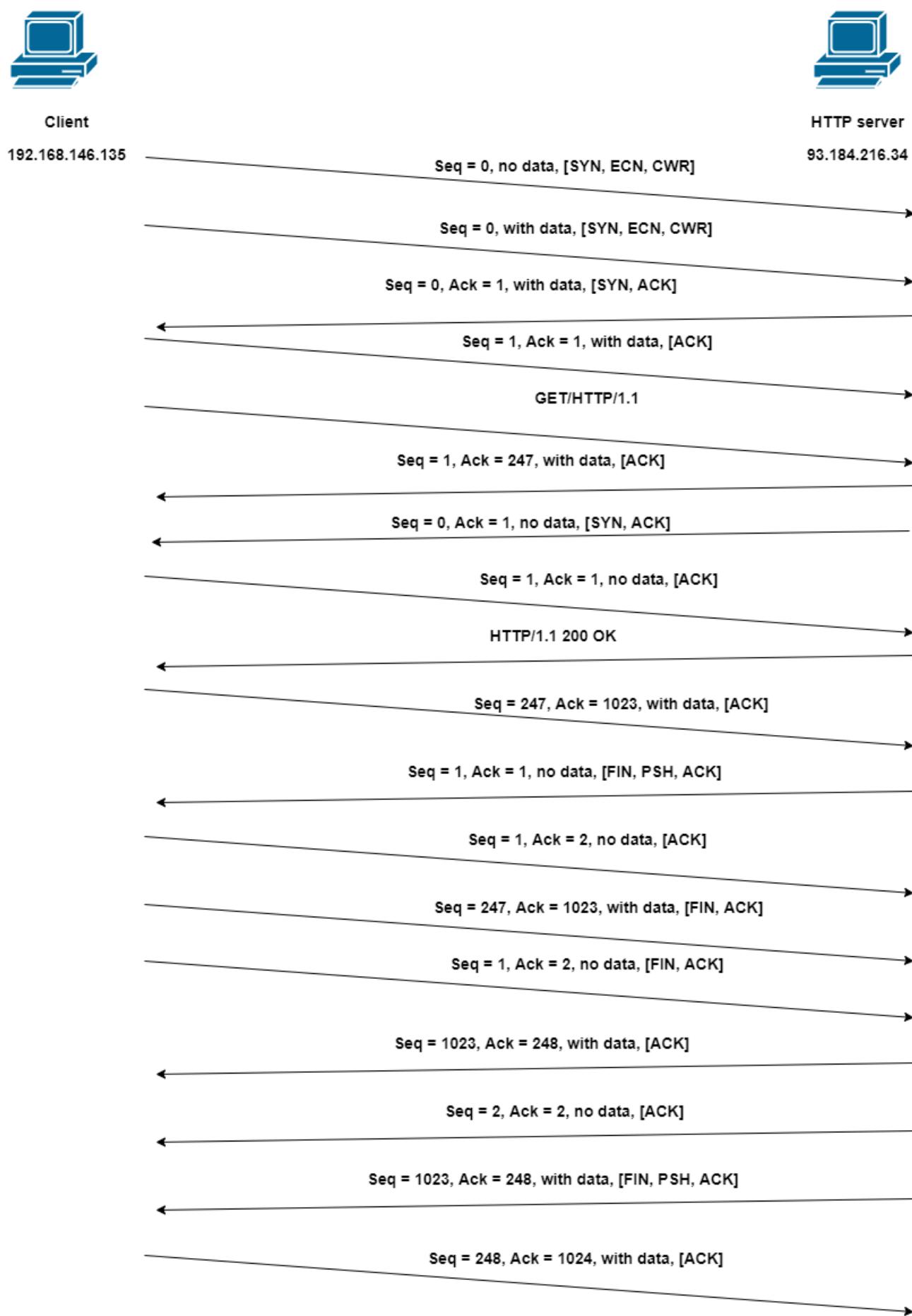
Các gói tin liên quan trong quá trình gửi ACK từ khi kết nối đến khi kết thúc nhận

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.

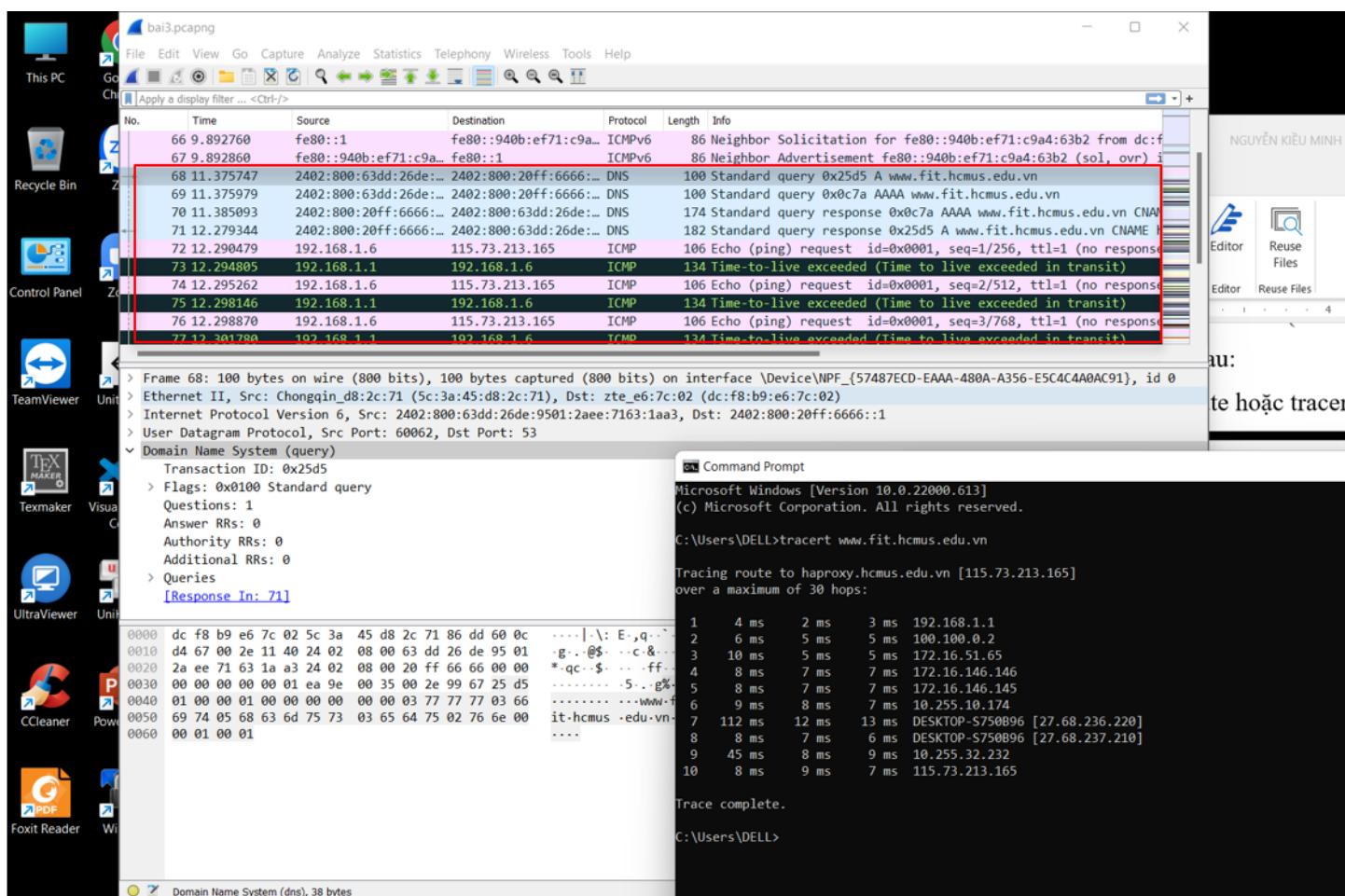
Bật wireshark để bắt gói tin lệnh traceroute từ máy của mình (có thể dùng máy ảo) đến ***www.fit.hcmus.edu.vn*** (FIT).

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).

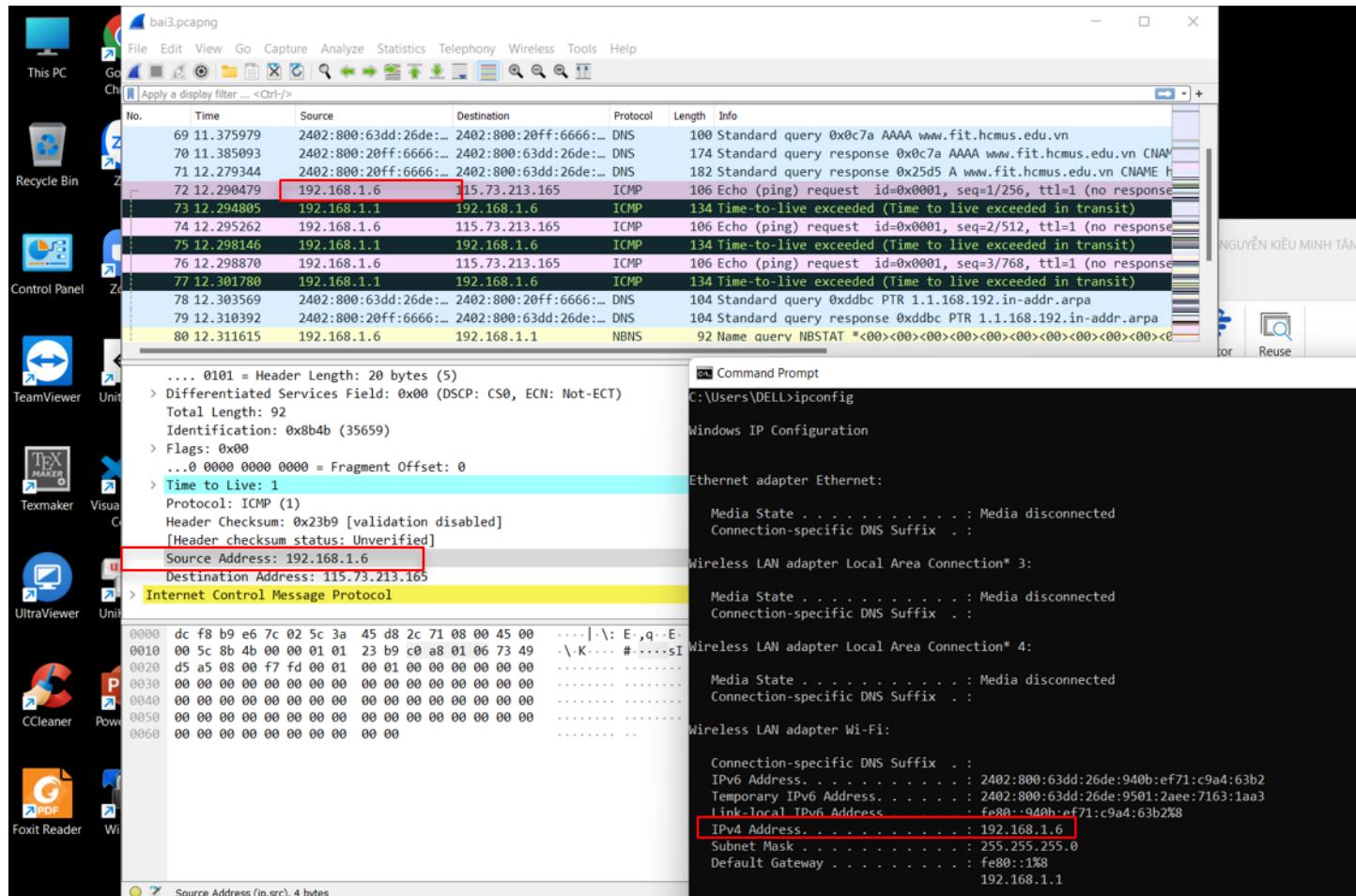
2. Cho biết traceroute/tracert dùng để làm gì?

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.^{1,2}

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

Địa chỉ IP của máy gửi request là 192.168.1.6.

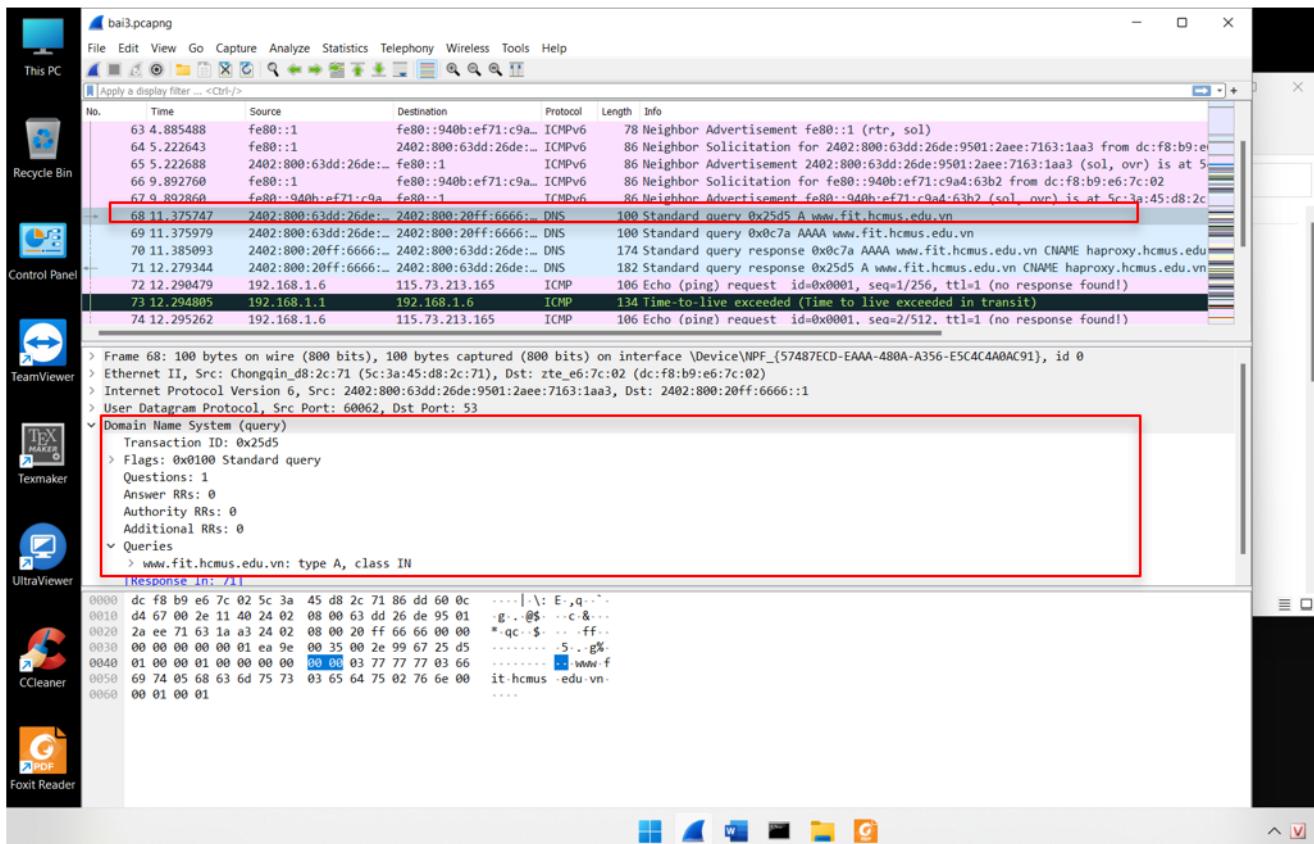


Hình 22: Địa chỉ IP của máy gửi request

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

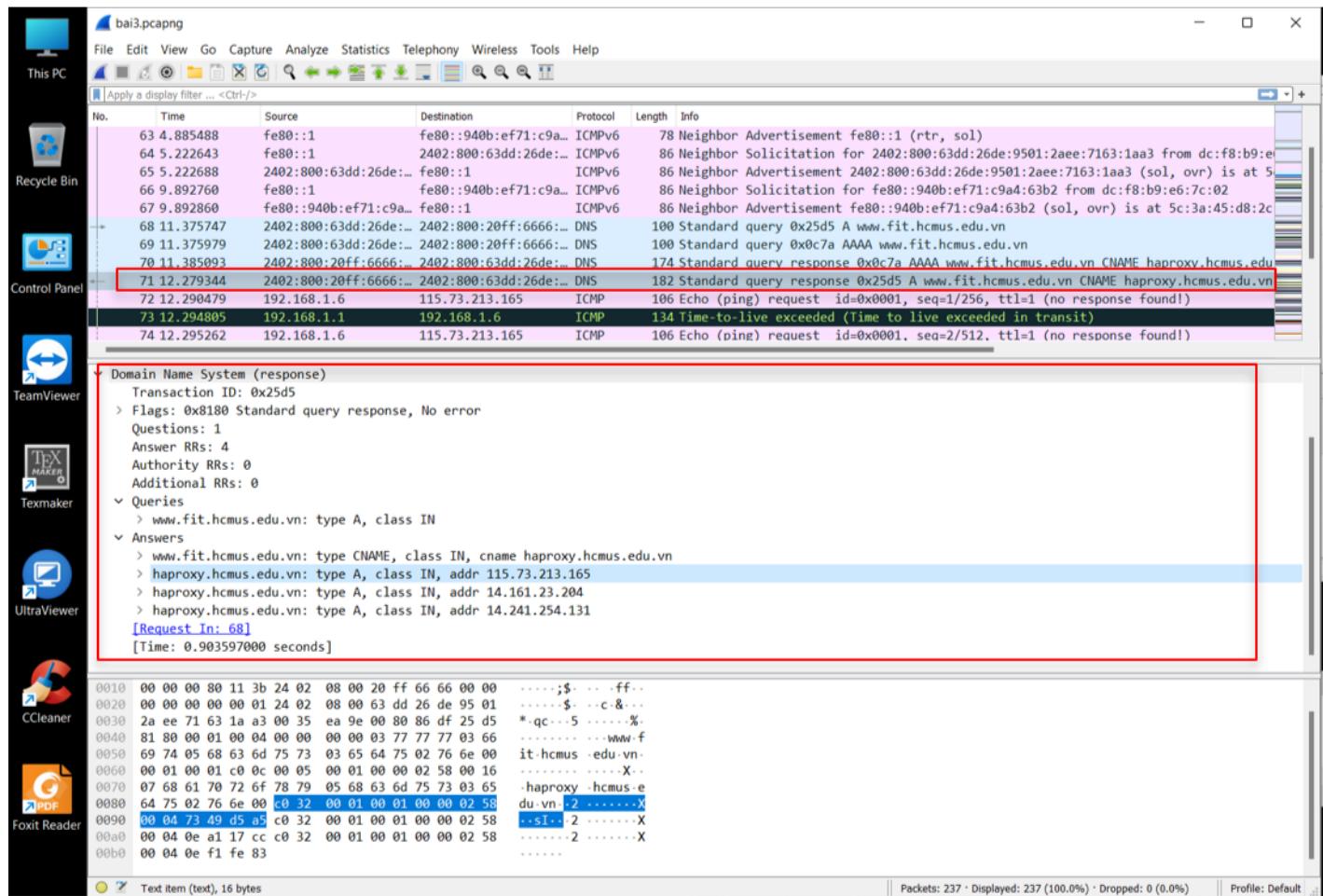
Máy tính sẽ gửi gói tin DNS query lên DNS server để “hỏi”, sau đó DNS Server sẽ trả lời qua gói tin DNS response.

- 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.

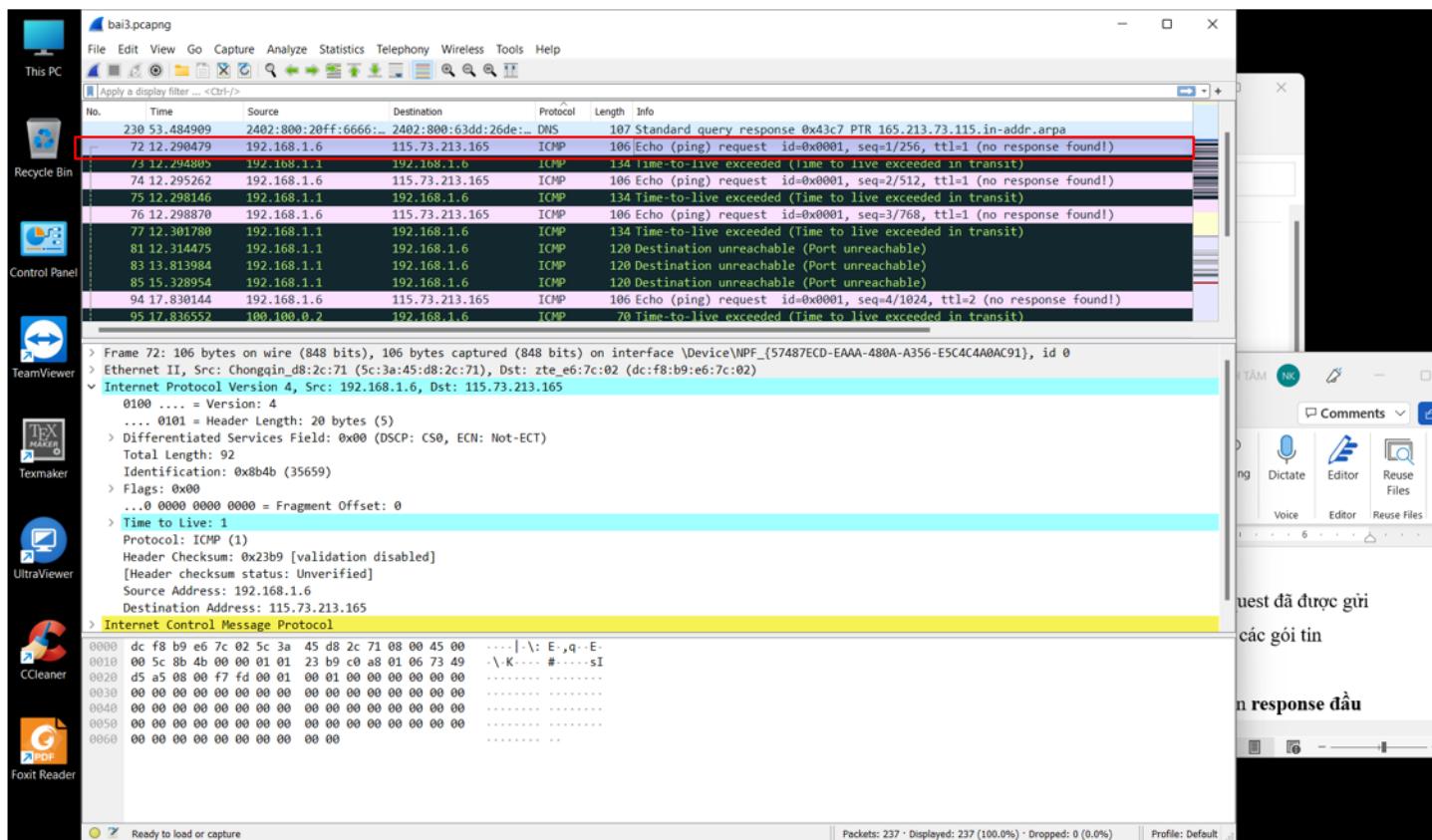


Hình 24: Gói tin DNS query response

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).



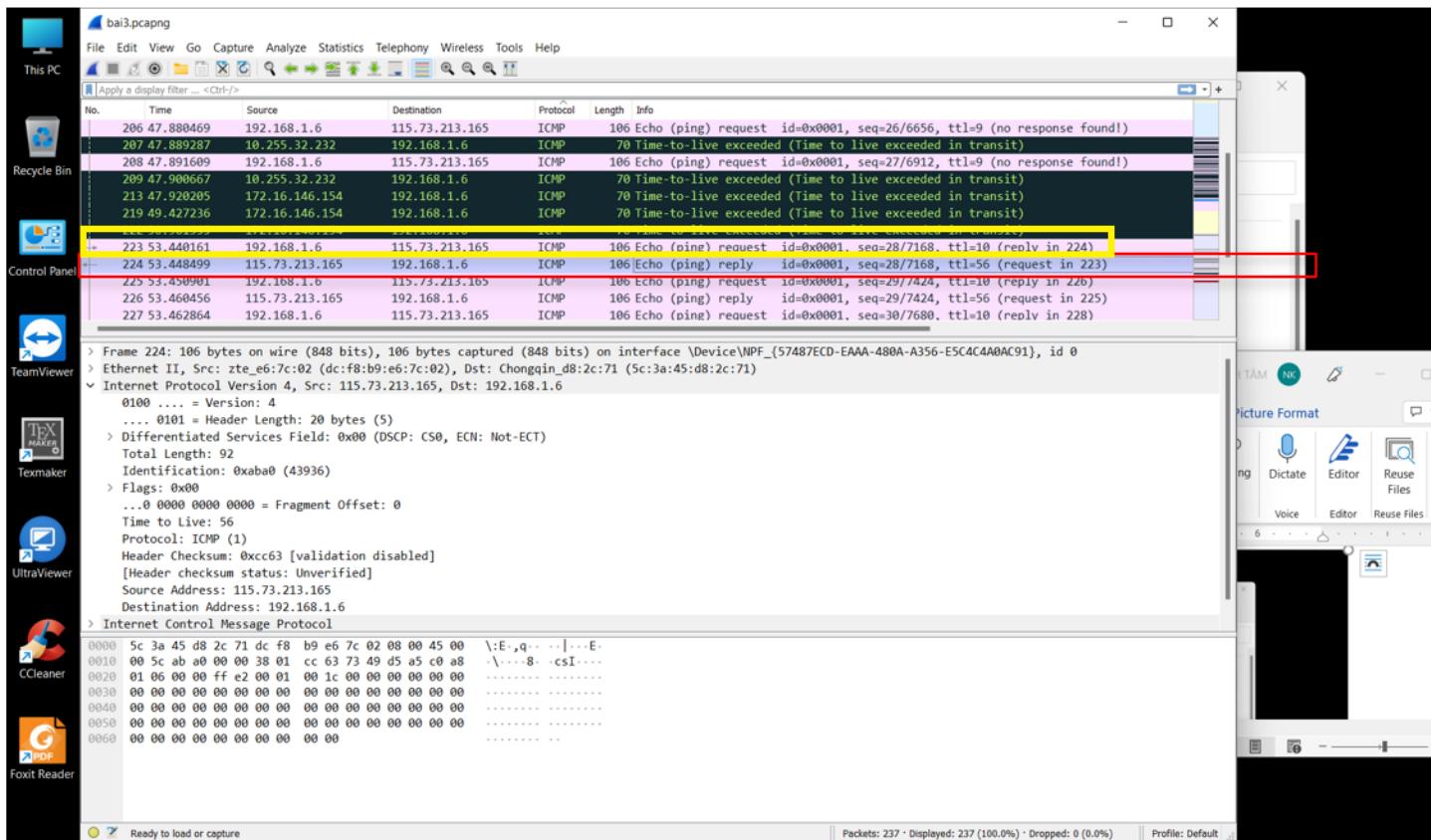
Hình 25: Protocol được sử dụng

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).

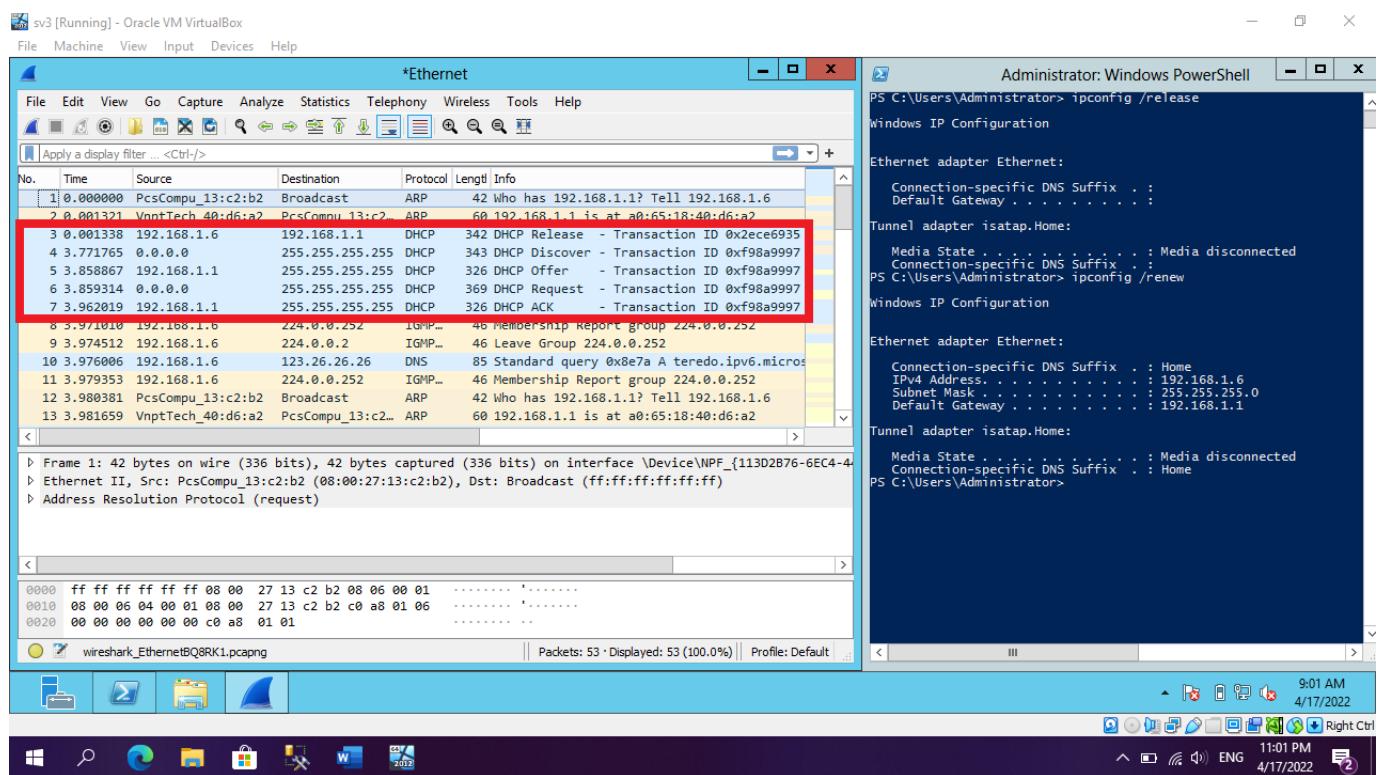
6 Bài 4: DHCP

Sử dụng lệnh ipconfig /release (xóa ip), và ipconfig /renew (xin lại ip mới) và bắt gói tin DHCP trong quá trình release và renew.

Bài tập bắt gói tin được thực hiện trên **máy ảo**, sử dụng hệ điều hành **Windows Server 2012**.

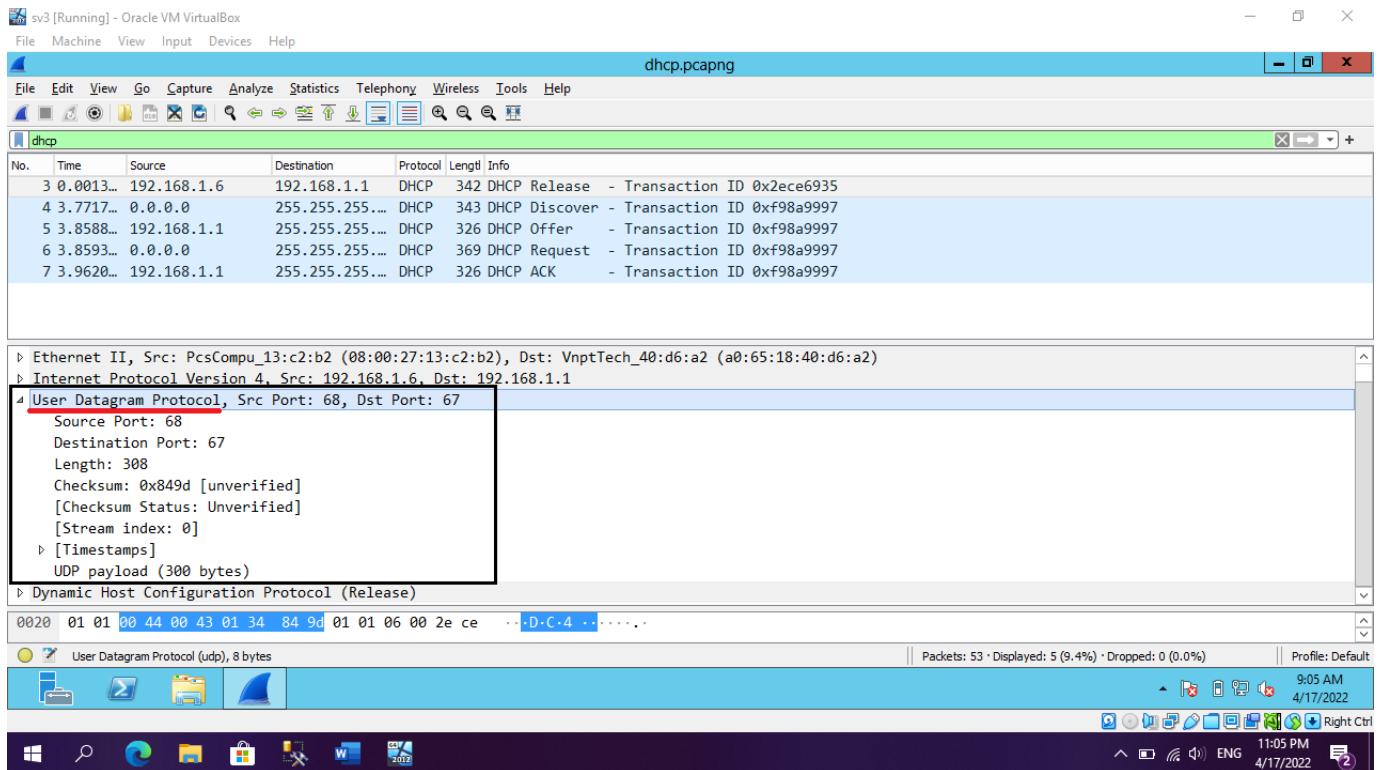
Trả lời các câu hỏi sau.

1. Chụp hình kết quả sau khi bắt được gói tin (thấy những gói tin DHCP trong quá trình release, renew).



Hình 27: Kết quả sau khi bắt gói tin DHCP

2. DHCP message dùng UDP hay TCP tại tầng Transport? Tại sao? DHCP sử dụng nghi thức UDP tại tầng Transport.



Hình 28: Nghi thức tầng Transport được DHCP message sử dụng

Nguyên nhân: Trong quá trình **release**, client cần giải phóng IP hiện tại, dẫn đến việc không có địa chỉ IP nguồn để có thể thực hiện kết nối TCP. Trong quá trình **renew**, client chưa có địa chỉ (**0.0.0.0**) và không biết địa chỉ của DHCP server nên phải thực hiện gửi tin tới địa chỉ broadcast (**255.255.255.255**), chỉ có thể thực hiện thông qua giao thức phi kết nối như là UDP.

3. Mục đích của DHCP release message là gì? DHCP client có đảm bảo lúc nào cũng nhận được ACK message từ server? Chuyện gì xảy ra nếu DHCP release message của client bị mất?

Mục đích: thông báo việc giải phóng địa chỉ IP (của máy gửi) đến DHCP server.

DHCP server **không** gửi message ACK đối với DHCP Release message.

Nếu như DHCP message của client bị mất, DHCP server **phải chờ** cho hết thời gian cấp của IP đó, mới có thể cấp lại cho client khác.

4. Một người cấu hình DHCP server cho modem của một quán cafe với thời gian cấp là 8 tiếng, và cấp IP thuộc đường mạng 192.168.1.0/24 với range IP từ 192.168.1.10 đến 192.168.1.100. Giả sử bắt đầu ngày mới và modem này được mở lên vào lúc 7:00 AM. Người uống cafe đến uống, ai cũng truy cập vào mạng wifi để truy cập Internet. Lượng khách cứ đi vào ra liên tục từ 7:00 AM đến 11:00 AM. Khi đến 11:00 AM, thì quán đón vị khách thứ 92 (và trong quán chỉ còn 20 khách đang uống và truy cập Internet) và người này không thể nào truy cập được Internet mặc dù đã nhập đúng pass Wifi. Hỏi:

a. Chuyện gì đã xảy ra mà vị khách thứ 92 không thể truy cập được Internet?

- Có 91 địa chỉ từ 192.168.1.10 đến 192.168.1.100.
- Thời gian cấp cho DHCP server là 8 tiếng.
- Thời điểm mở quán và modem vào lúc 7:00AM. Giả sử vị khách đầu tiên đến đúng lúc đó và rời đi, thì phải đến 3:00PM (sau 8 tiếng) thì địa chỉ đó mới được DHCP server thu hồi lại để cấp cho client mới.
- Vậy nên khi vị khách 92 đến nhưng không truy cập được là do DHCP server đã cấp hết địa chỉ (91 IP), và chưa đến thời điểm thu hồi nên không có IP cho vị khách này.

b. Vậy những vị khách tiếp theo 93, 94, có truy cập được hay không?

Và có thể truy cập vào thời điểm nào?

Những vị khách tiếp theo cũng không thể truy cập được vào thời điểm đó. Họ chỉ có thể truy cập sau 3:00PM và trong quán phải có ít hơn 91 người.

c. Chủ quán cafe nên làm gì để vị khách thứ 92 có thể truy cập được Internet và hướng giải quyết để khắc phục tình trạng này về sau là gì?

Cách khắc phục đơn giản là **khởi động lại modem**. Khi ấy, dữ liệu về các IP được cấp sẽ được xóa và các máy tính trong mạng sẽ gửi request lên DHCP server để lấy lại IP. Tuy nhiên, cách này sẽ gây trải nghiệm không tốt với người dùng (mạng đột nhiên bị ngắt), và không phải lúc nào cũng biết được IP đã được cấp hết chưa.

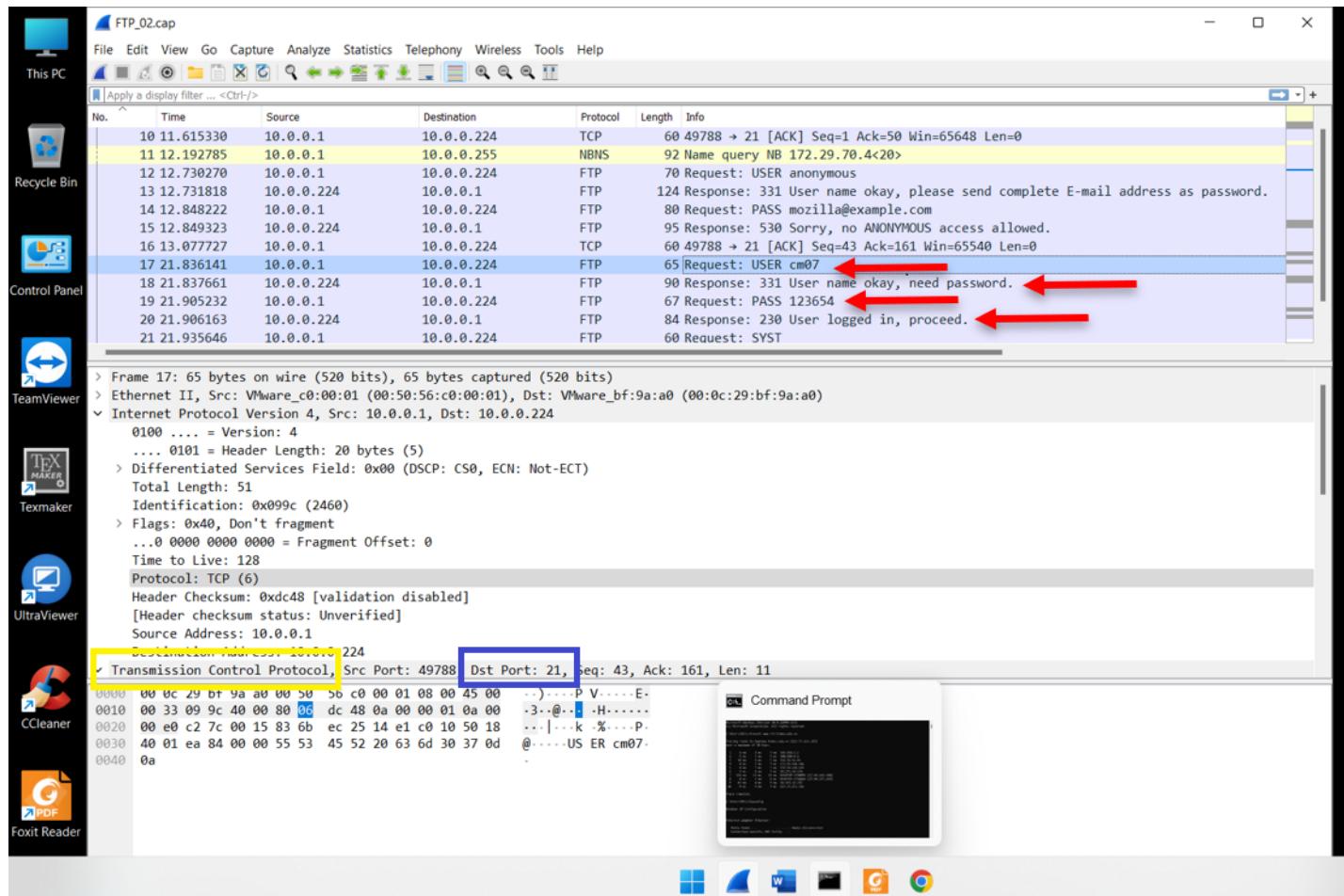
Hướng giải quyết về sau: Do đây là quán cafe, hầu hết mọi người chỉ ở lại quán khoảng 1 tiếng, số người truy cập cùng lúc không quá nhiều (đến 11:00AM chỉ có 20 khách ở quán) nên ta có thể giảm thời gian cấp xuống (1 - 2 tiếng). Đối với quán có quy mô lớn, lượng người truy cập cùng lúc nhiều (lớn hơn 91) thì cần phải mở rộng range IP của DHCP server.

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 29).



Hình 29: Giao thức được FTP sử dụng

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

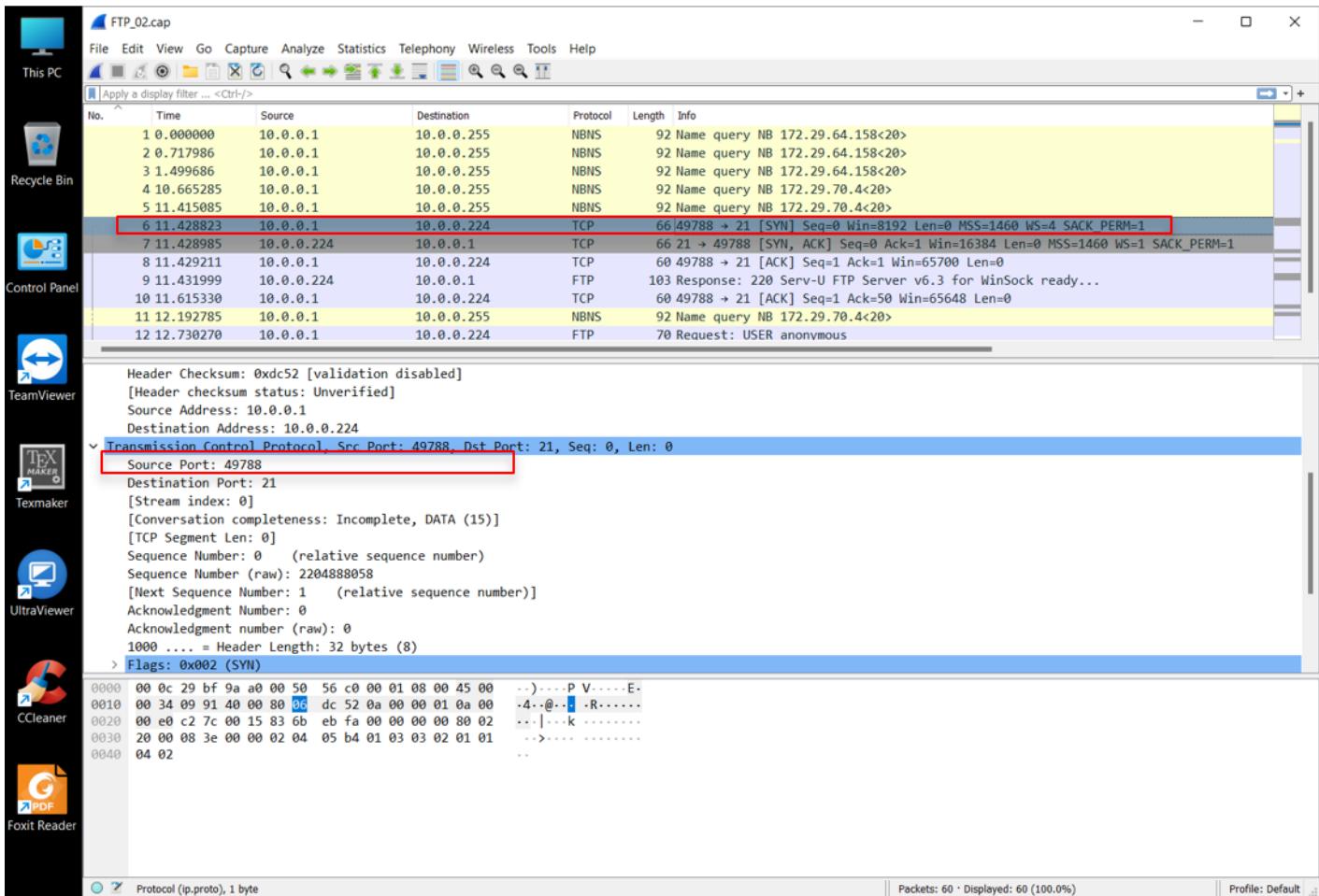
Port mặc định của FTP Server để nhận kết nối là 21 (phần đóng khung màu xanh trong hình 29).

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 29 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?**

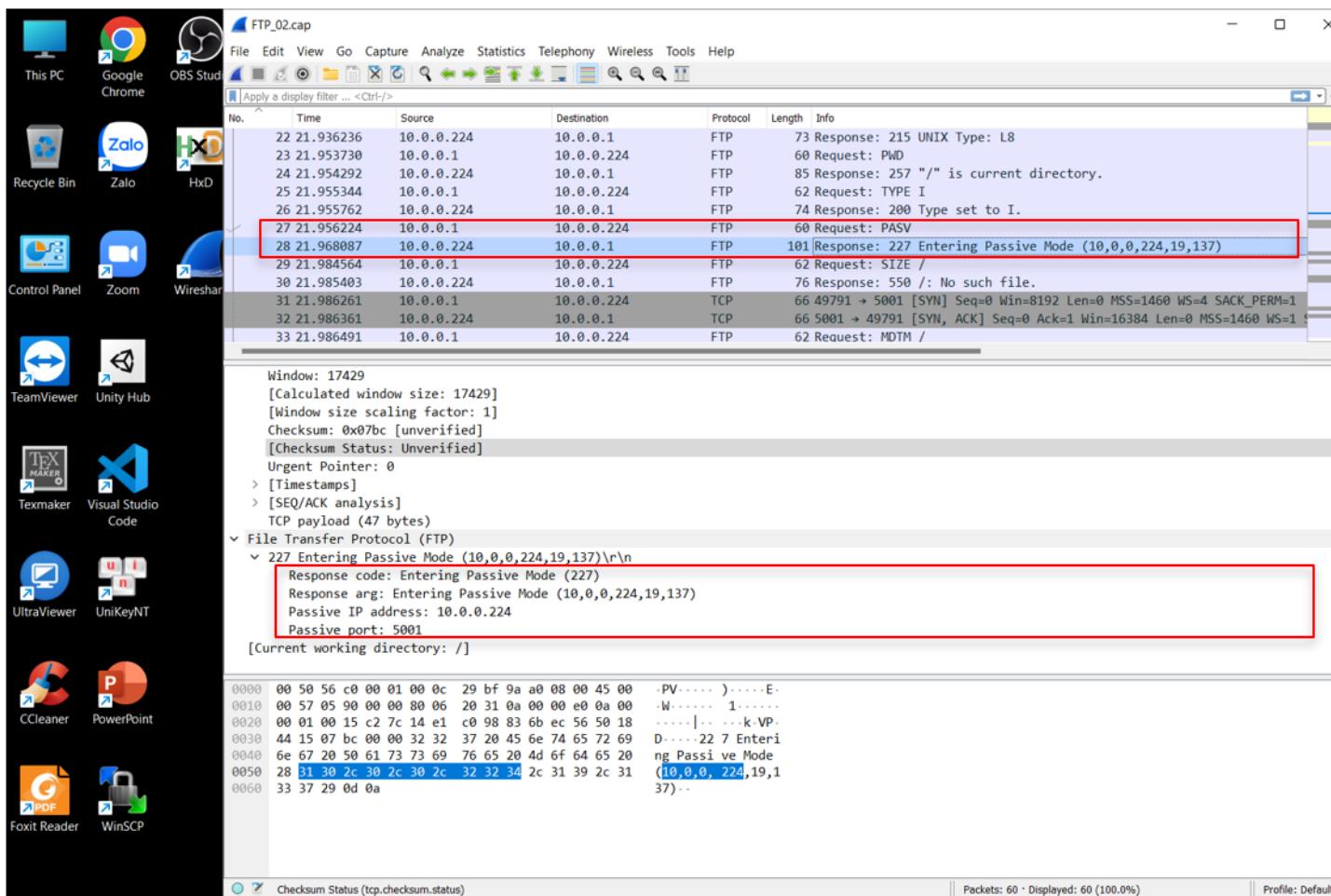
Port truyền lệnh của client là port 49788.



Hình 30: Port truyền lệnh của client

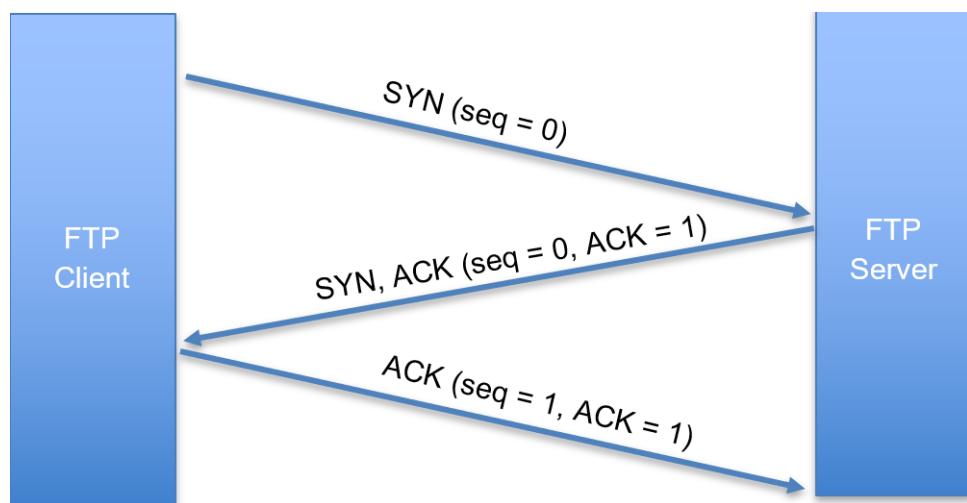
e. Client truy xuất lên server theo mode nào: active hay passive?

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

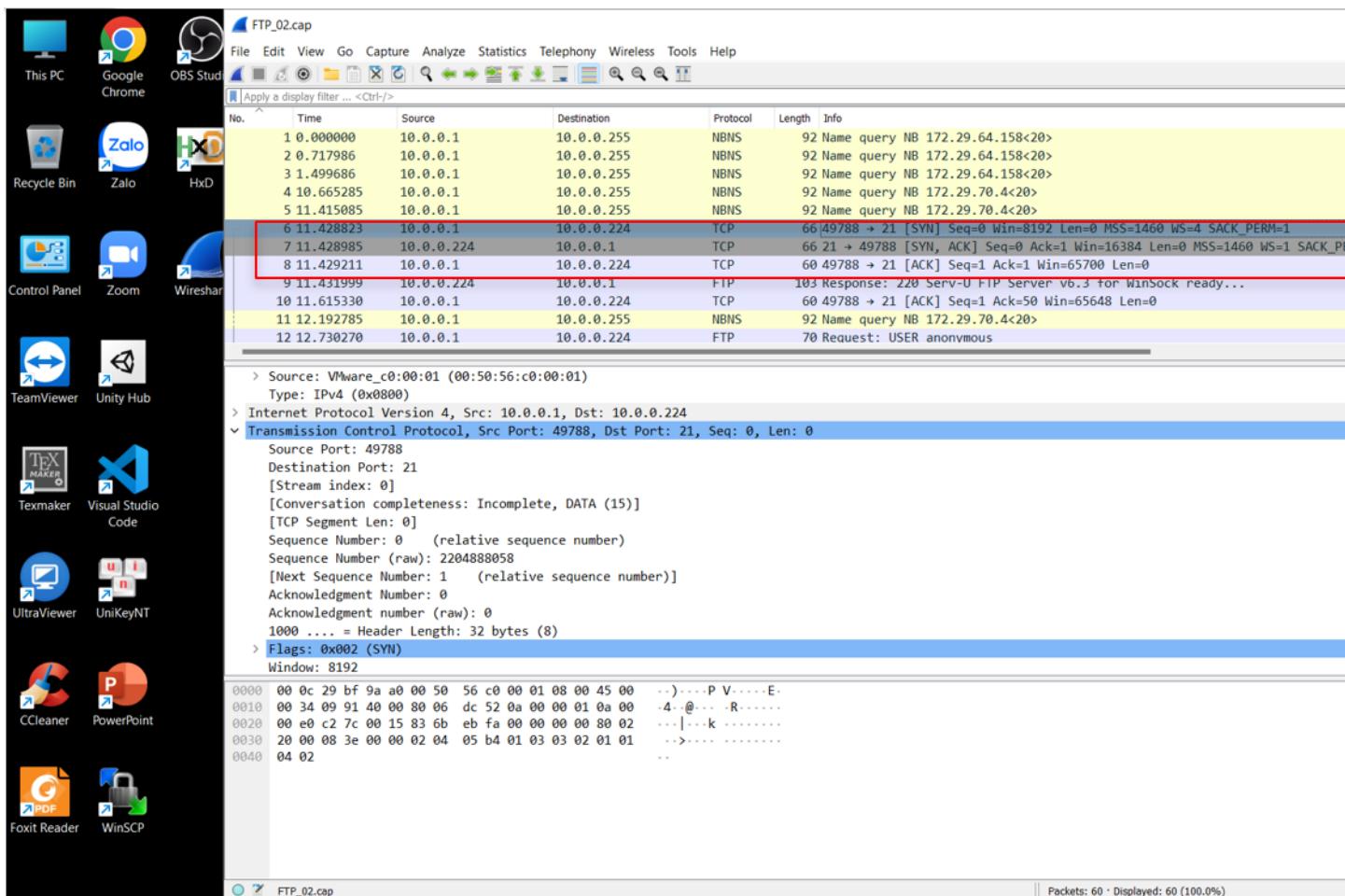


Hình 31: Mode truy xuất của client lên server

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.

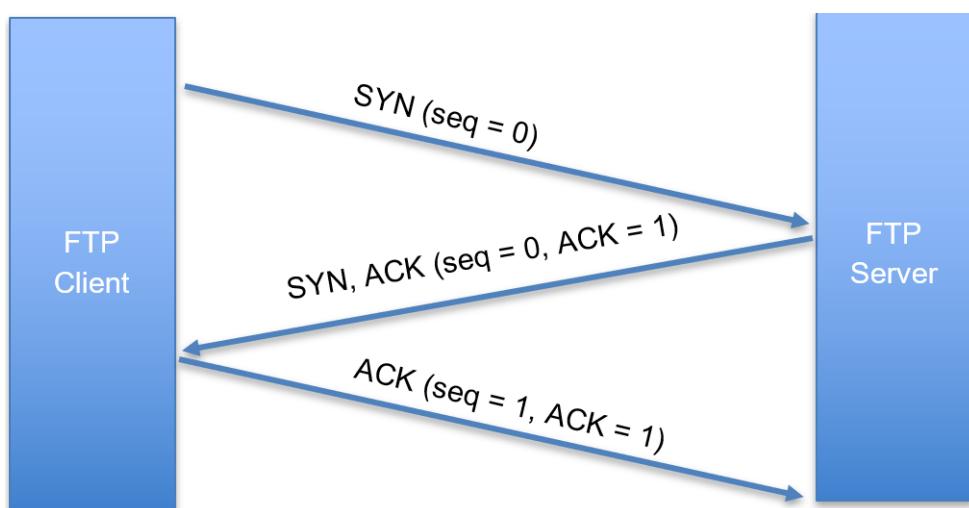


Hình 32: Quá trình bắt tay 3 bước để tạo kết nối ban đầu

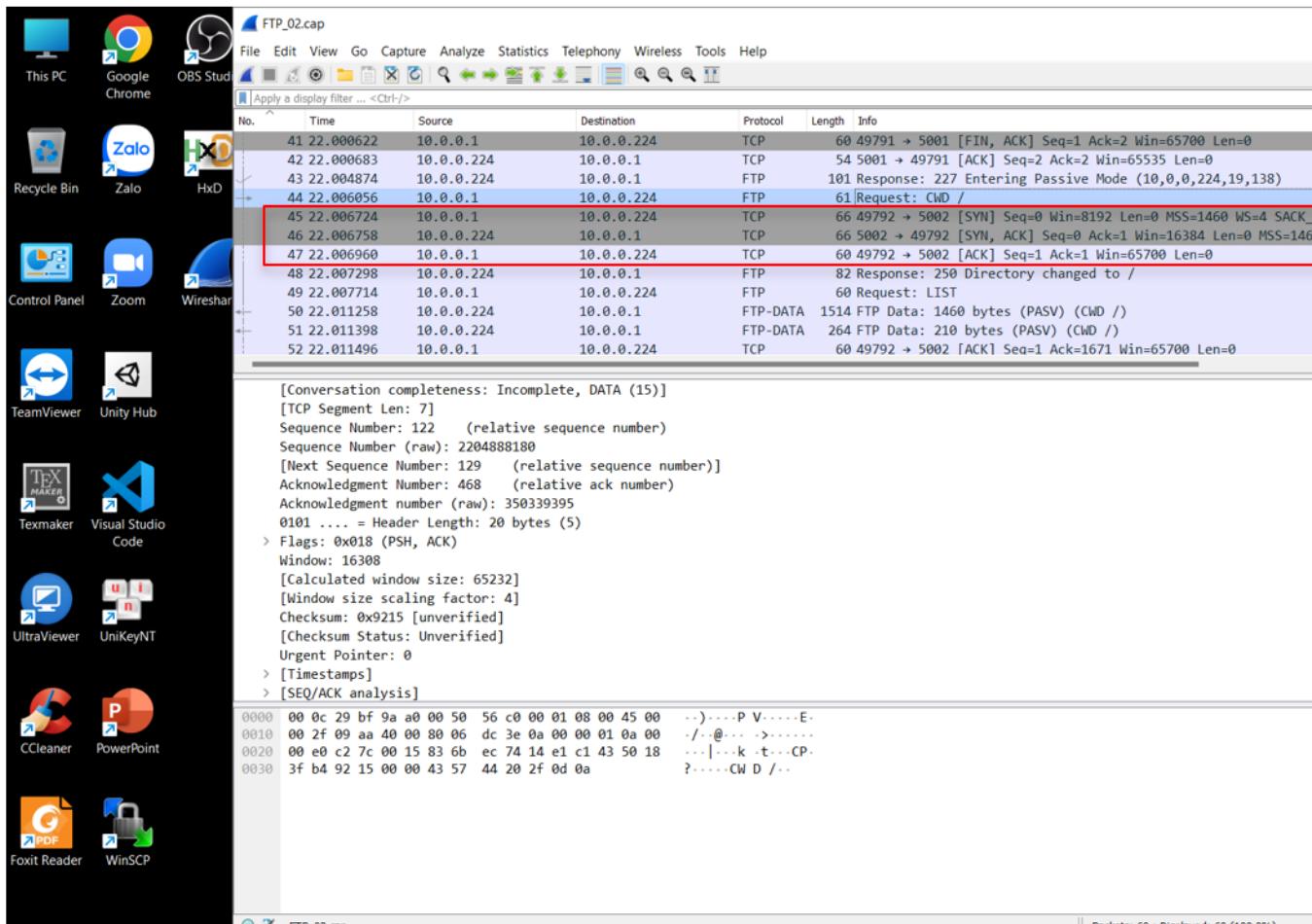


Hình 33: Quá trình bắt tay 3 bước để tạo kết nối ban đầu

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



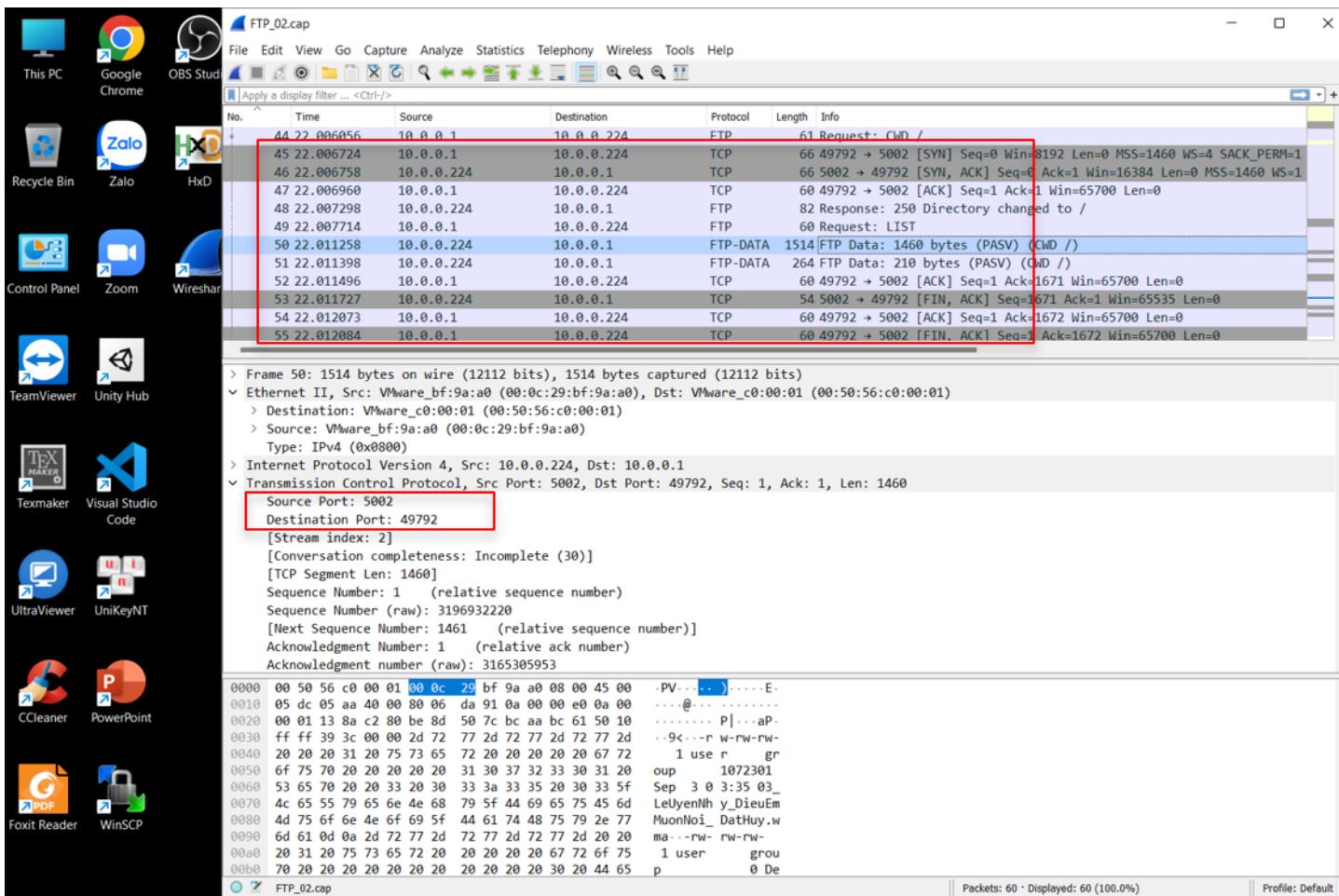
Hình 34: Quá trình bắt tay 3 bước để tạo kết nối truyền dữ liệu



Hình 35: 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 36 (ứng với gói tin số 50, chuyển data từ FTP server sang FTP client) cũng nêu ra port tương ứng.



Hình 36: 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.*