

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	2
2	Mức độ hoàn thành	2
3	Bài 1: Ping	3
4	Bài 2: HTTP	6
5	Bài 3: Traceroute	13
6	Tài liệu tham khảo	16

Danh sách hình vẽ

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

Danh sách bảng

1	Bảng phân công thành viên	2
2	Kích thước gói tin ICMP request	4

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

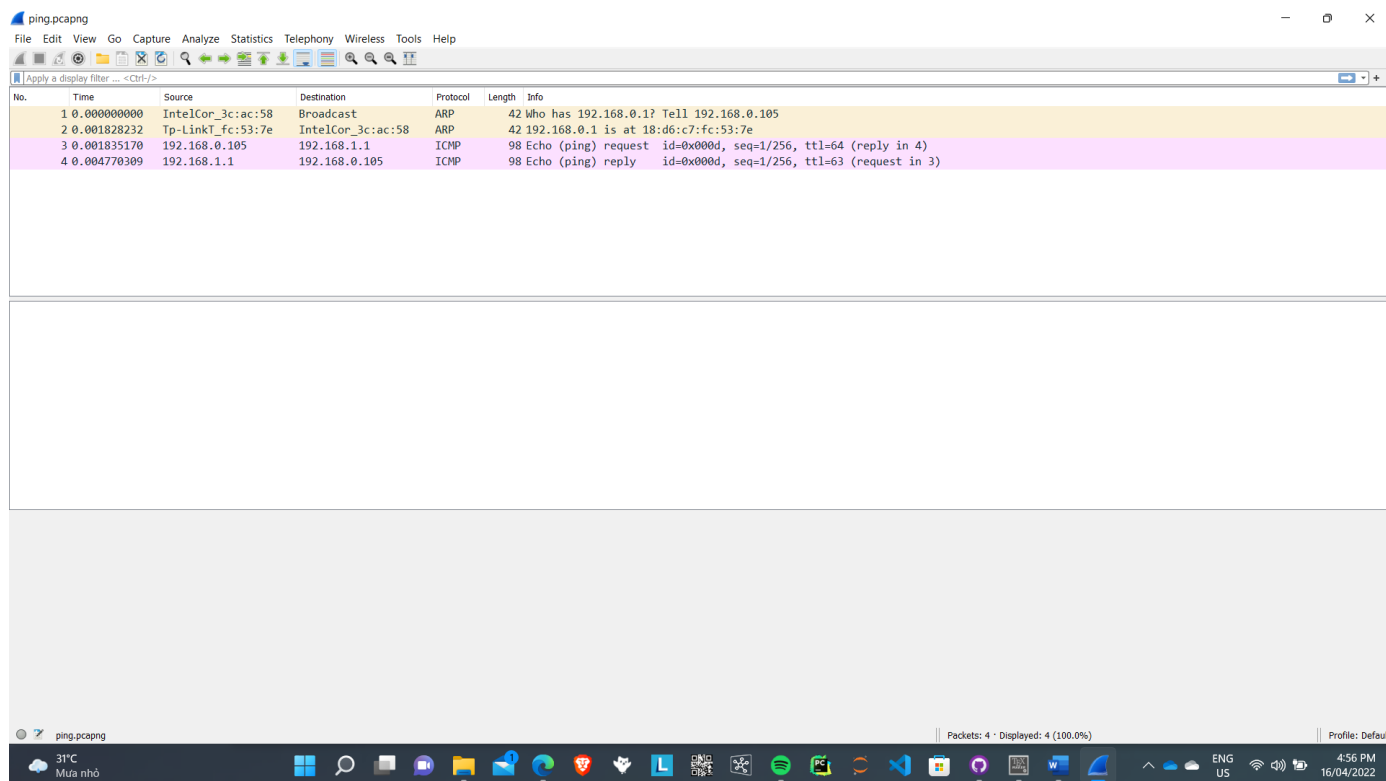
Bài 1: 100% (5/5)

Bài 2: 100% (14/14)

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.



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, ttl=64 (reply in 4)
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply id=0x000d, seq=1/256, ttl=63 (request in 3)

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**.

```

Protocol: ICMP (1)
Header Checksum: 0x3cec [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.105
Destination Address: 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?

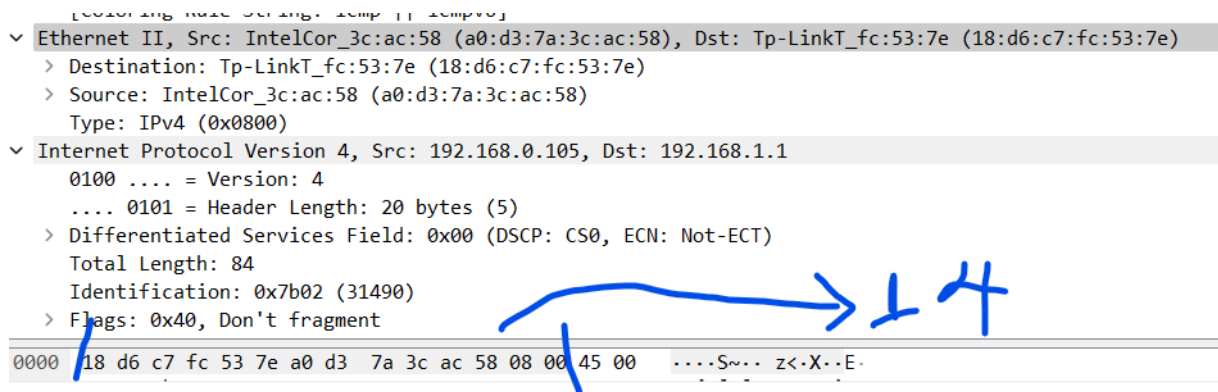
Không có source port number và destination port number.

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.

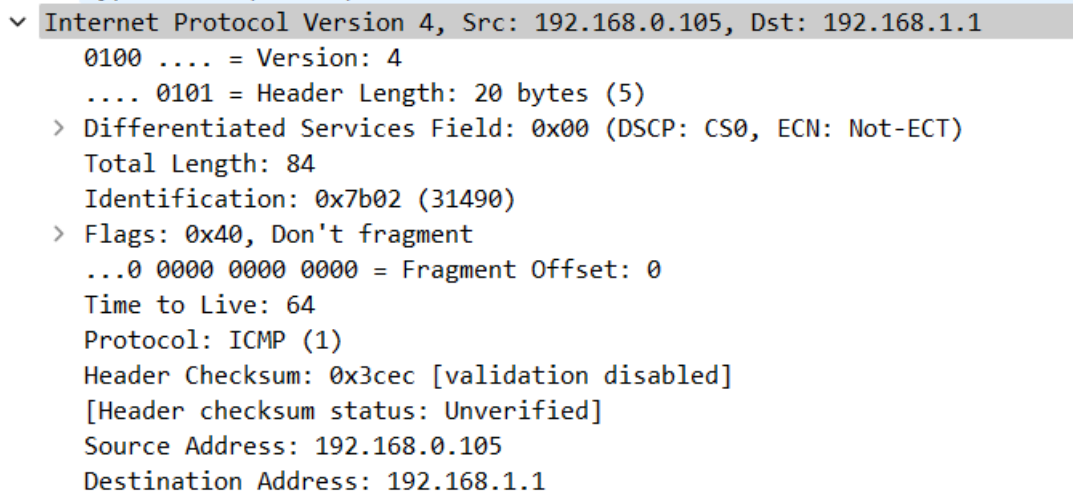
3. Với gói tin ICMP request, cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

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

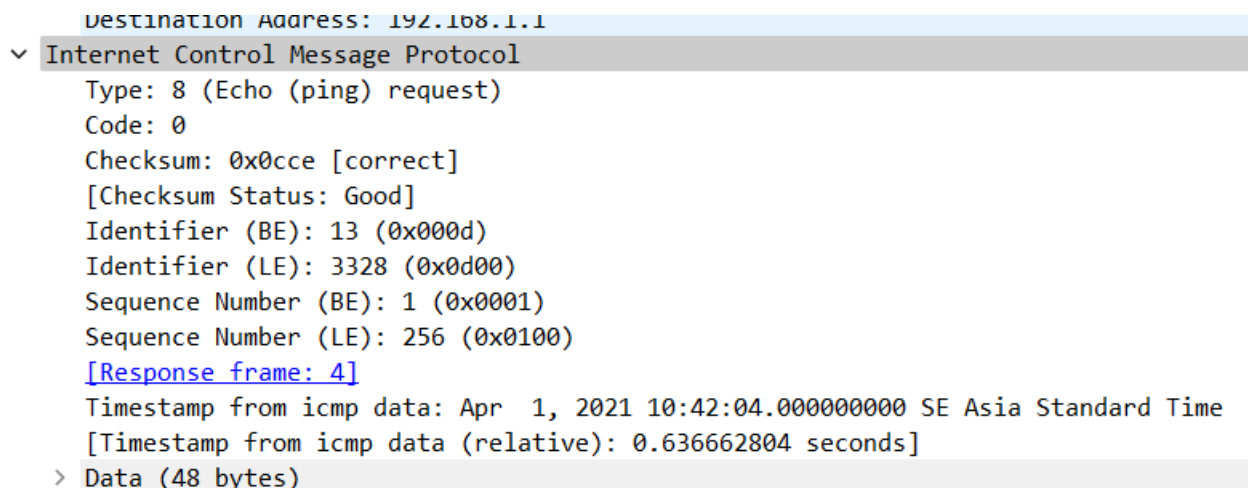
Bảng 2: Kích thước gói tin ICMP request



Hình 3: Độ dài Ethernet header



Hình 4: Độ dài IP header



Hình 5: Độ dài ICMP data và ICMP header

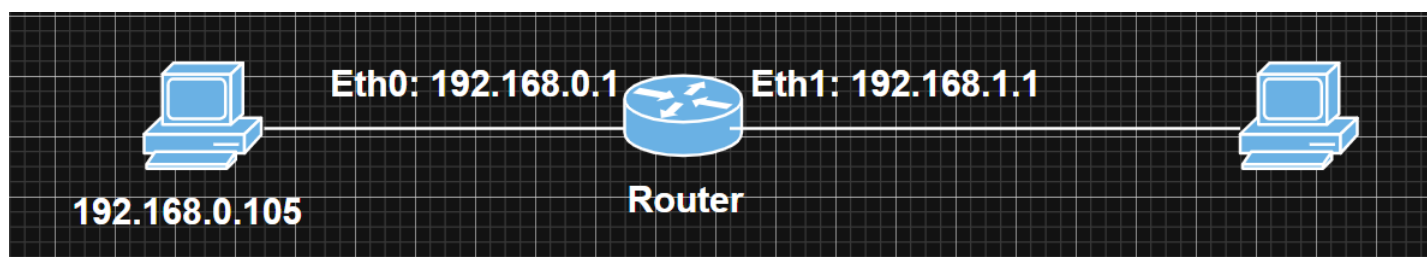
4. Tại sao lại có 2 gói ARP?

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

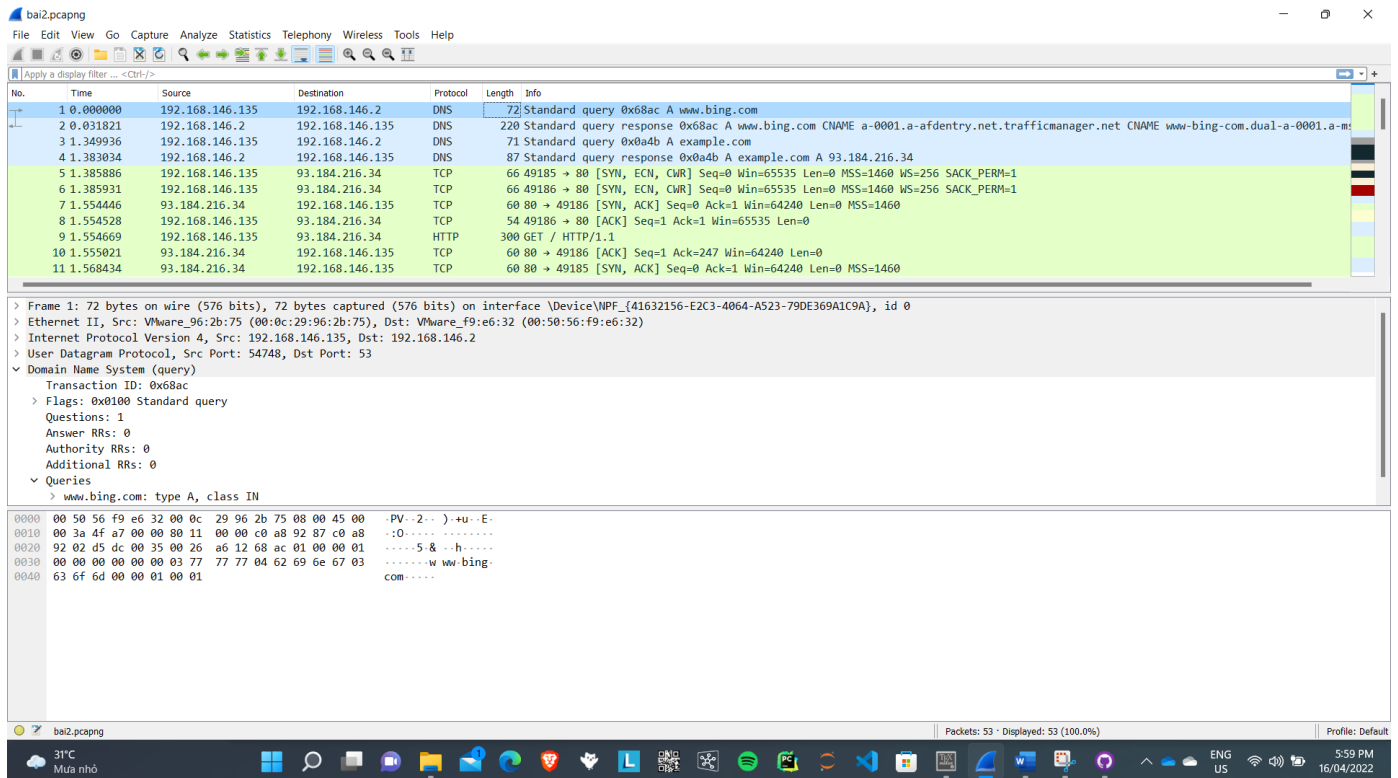
4 Bài 2: HTTP

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	Protocol	Length	Info
1	0.000000	192.168.146.135	192.168.146.2	DNS	72	Standard query 0x68ac
2	0.031821	192.168.146.2	192.168.146.135	DNS	220	Standard query respon
3	1.349936	192.168.146.135	192.168.146.2	DNS	71	Standard query 0x0a4b
4	1.383034	192.168.146.2	192.168.146.135	DNS	87	Standard query respon

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	Length	Info
1	0.000000	192.168.146.135	192.168.146.2	DNS	72	Standard query 0x68a...
2	0.031821	192.168.146.2	192.168.146.135	DNS	220	Standard query respon...
3	1.349936	192.168.146.135	192.168.146.2	DNS	71	Standard query 0x0a4...
4	1.383034	192.168.146.2	192.168.146.135	DNS	87	Standard query respon...

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**.

<ul style="list-style-type: none"> <ul style="list-style-type: none"> Destination: VMware_f9:e6:32 (00:50:56:f9:e6:32) <ul style="list-style-type: none"> Address: VMware_f9:e6:32 (00:50:56:f9:e6:32) <ul style="list-style-type: none">0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Source: VMware_96:2b:75 (00:0c:29:96:2b:75) <ul style="list-style-type: none"> Address: VMware_96:2b:75 (00:0c:29:96:2b:75) <ul style="list-style-type: none">0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast)

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**.

<ul style="list-style-type: none"> <ul style="list-style-type: none"> Destination: VMware_f9:e6:32 (00:50:56:f9:e6:32) <ul style="list-style-type: none"> Address: VMware_f9:e6:32 (00:50:56:f9:e6:32) <ul style="list-style-type: none">0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Source: VMware_96:2b:75 (00:0c:29:96:2b:75) <ul style="list-style-type: none"> Address: VMware_96:2b:75 (00:0c:29:96:2b:75) <ul style="list-style-type: none">0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast)

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**.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.146.135	192.168.146.2	DNS	72	Standard query 0x68a
2	0.031821	192.168.146.2	192.168.146.135	DNS	220	Standard query respon
3	1.349936	192.168.146.135	192.168.146.2	DNS	71	Standard query 0x0a4
4	1.383034	192.168.146.2	192.168.146.135	DNS	87	Standard query respon

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**.

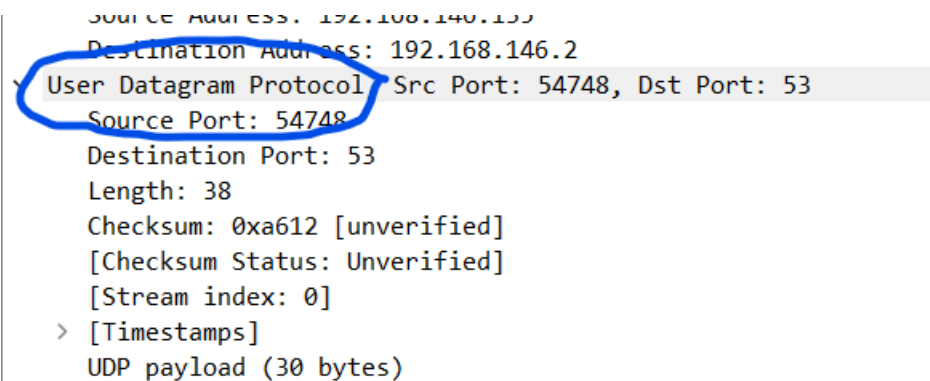
9	1.554669	192.168.146.135	93.184.216.34	HTTP	300	GET / HTTP/1.1
10	1.555021	93.184.216.34	192.168.146.135	TCP	60	80 → 49186 [AC
11	1.568434	93.184.216.34	192.168.146.135	TCP	60	80 → 49185 [SY
12	1.568513	192.168.146.135	93.184.216.34	TCP	54	49185 → 80 [AC
13	1.721827	93.184.216.34	192.168.146.135	HTTP	1076	HTTP/1.1 200 0
14	1.721929	192.168.146.135	93.184.216.34	TCP	54	49186 → 80 [AC
15	3.664135	192.168.146.135	192.168.146.2	DNS	76	Standard query
16	3.781313	192.168.146.2	192.168.146.135	DNS	171	Standard query
17	3.783903	192.168.146.135	23.36.101.95	TCP	66	49187 → 443 [S
18	3.784009	192.168.146.135	23.36.101.95	TCP	66	49188 → 443 [S
19	4.793020	192.168.146.135	23.36.101.95	TCP	66	[TCP Retransmi
20	4.793078	192.168.146.135	23.36.101.95	TCP	66	[TCP Retransmi
21	6.702065	192.168.146.135	23.36.101.95	TCP	66	[TCP Retransmi

Address: VMware_f9:e6:32 (00:50:56:f9:e6:32)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)
▼ Source: VMware_96:2b:75 (00:0c:29:96:2b:75)
Address: VMware_96:2b:75 (00:0c:29:96:2b:75)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.146.135, Dst: 93.184.216.34
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 286
Identification: 0x337e (13182)
> Flags: 0x40, Don't fragment

Hình 13: Địa chỉ IP của HTTP server

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

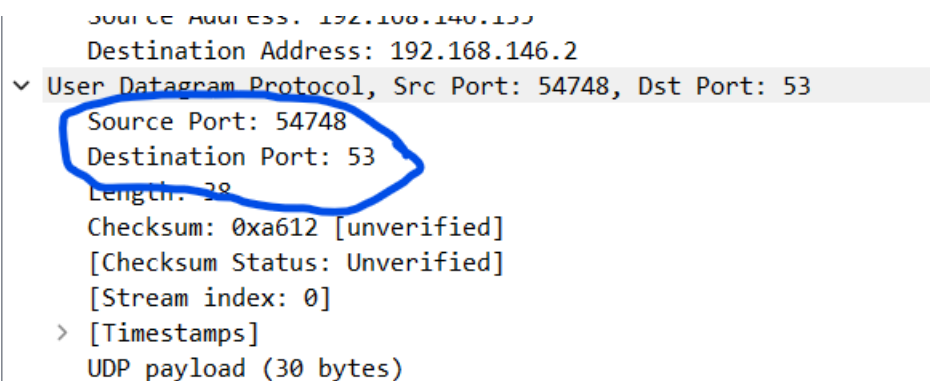
DNS sử dụng protocol **UDP** của tầng Transport.



Hình 14: Nghi thức được DNS sử dụng

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

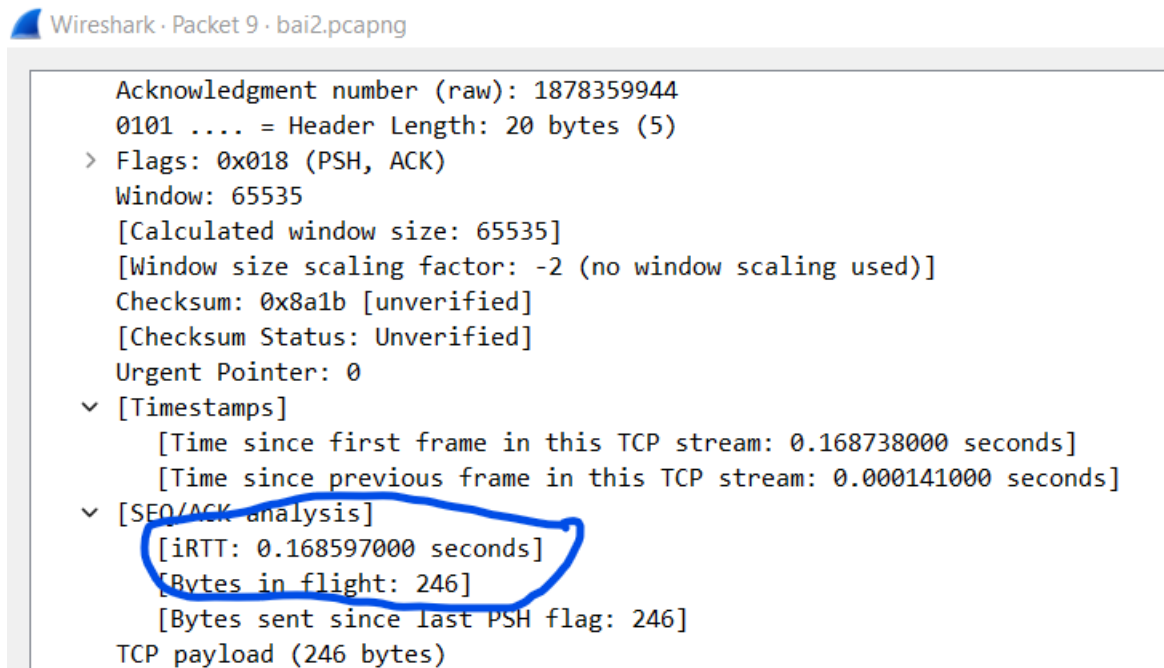
Port sử dụng khi truy vấn DNS server: **port 53**.



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 (browser) đang sử dụng (Application).

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

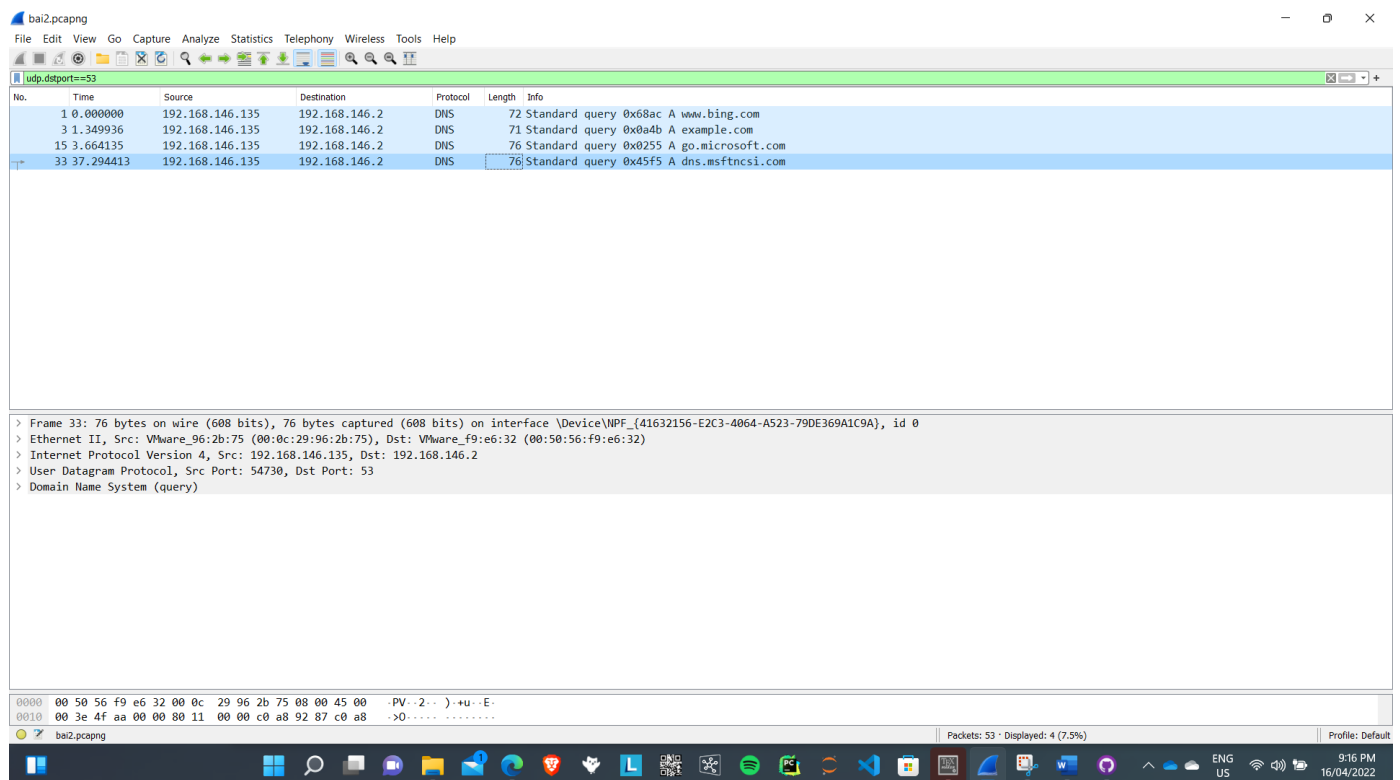
8	1.554528	192.168.146.135	93.184.216.34	TCP	54 49186 → 80 [ACK]
9	1.554669	192.168.146.135	93.184.216.34	HTTP	300 GET / HTTP/1.1
10	1.555021	93.184.216.34	192.168.146.135	TCP	60 80 → 49186 [ACK]
11	1.568434	93.184.216.34	192.168.146.135	TCP	60 80 → 49185 [SYN, A

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.

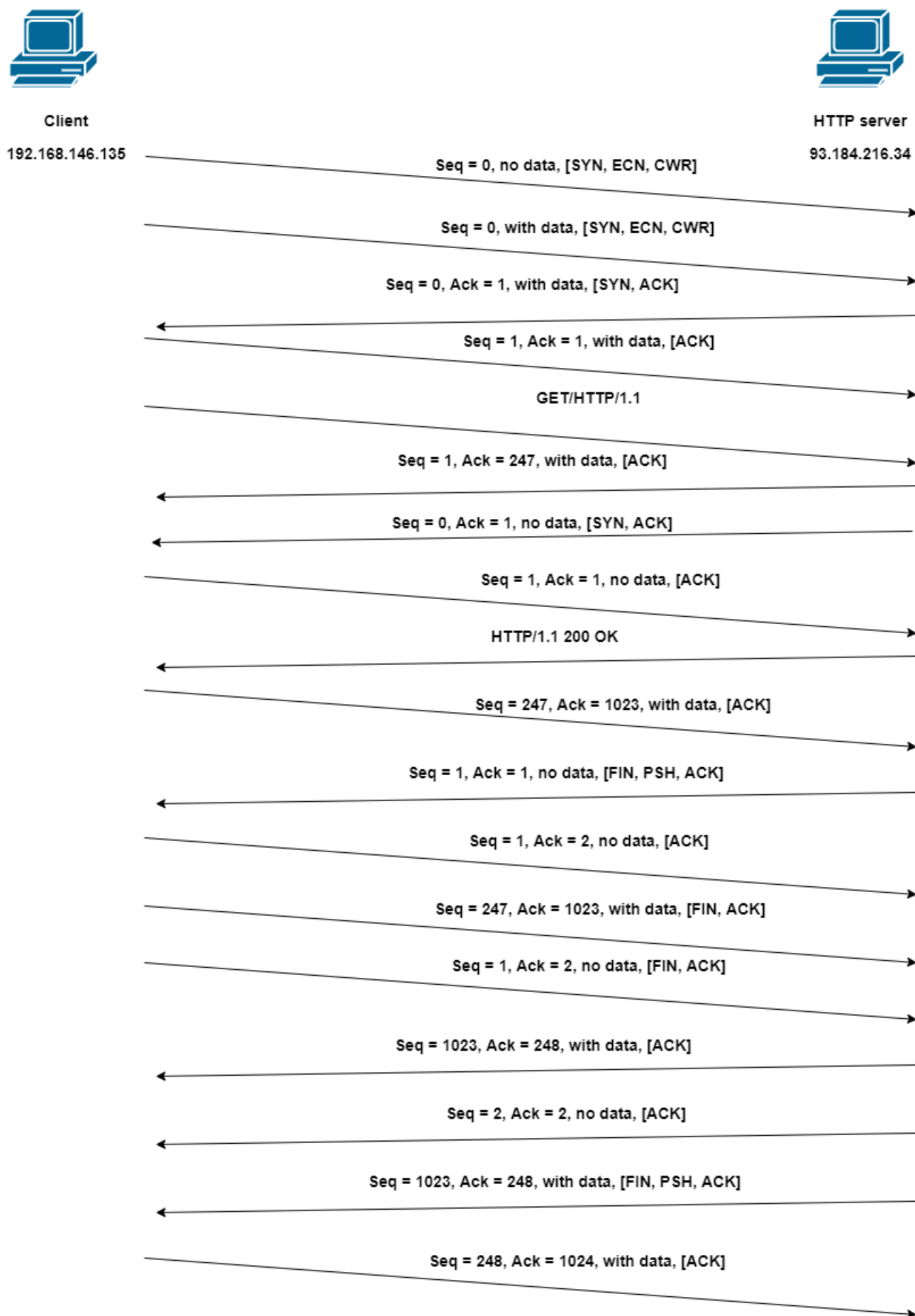
Kết quả của query này như sau.



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.

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



Hình 19: 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.

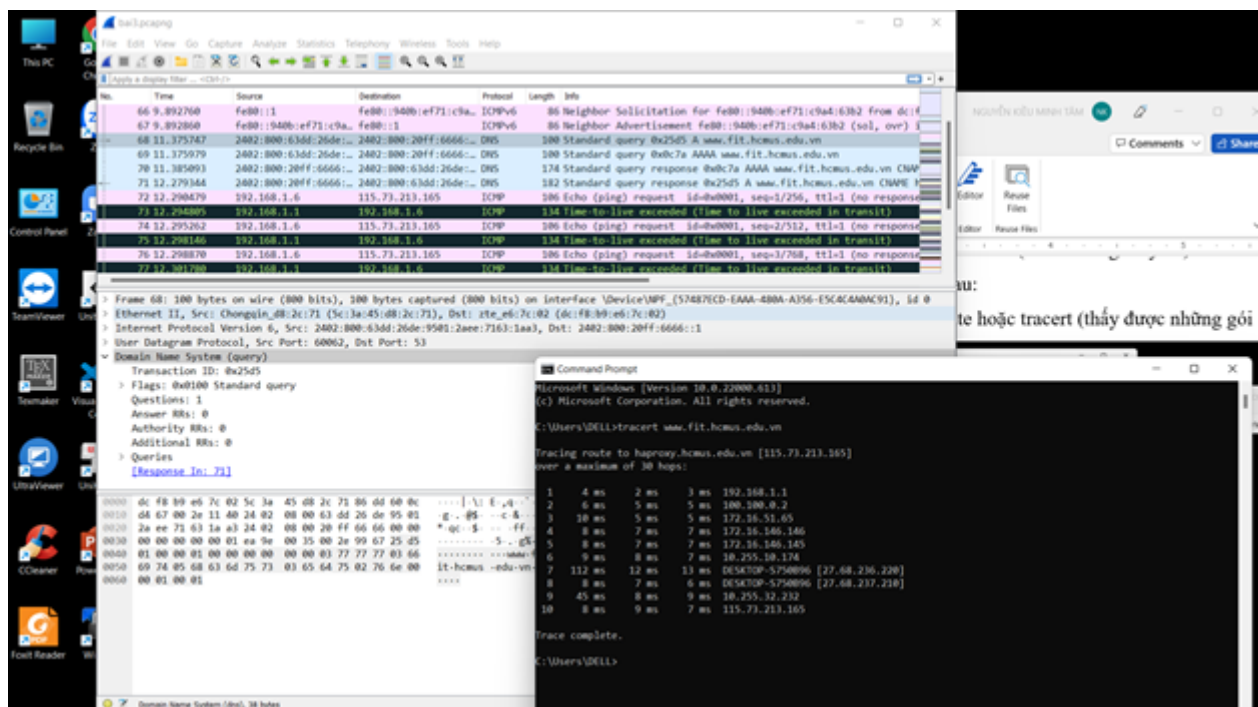
Bật wireshark để bắt gói tin lệnh traceroute từ máy của mình (có thể dùng máy ảo) đến **www.fit.hcmus.edu.vn** (FIT).

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 20: Kết quả bắt gói tin sau khi tracert

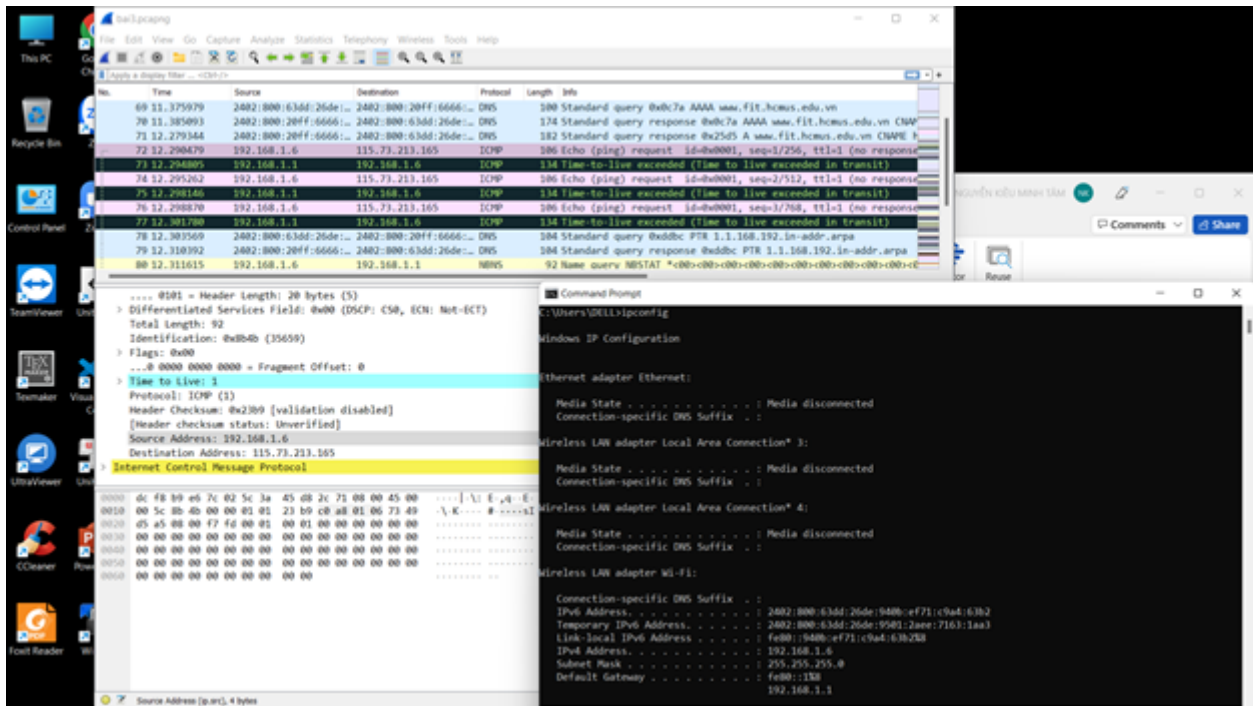
Các gói tin được bắt tính từ lệnh tracert được thể hiện ở phần đóng khung màu đỏ trên hình vẽ. Đó là các gói tin đầu tiên bắt đầu từ khi tracert (gói tin số 68).

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.^{2,1}

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

Địa chỉ IP của máy gửi request là 192.168.1.6.

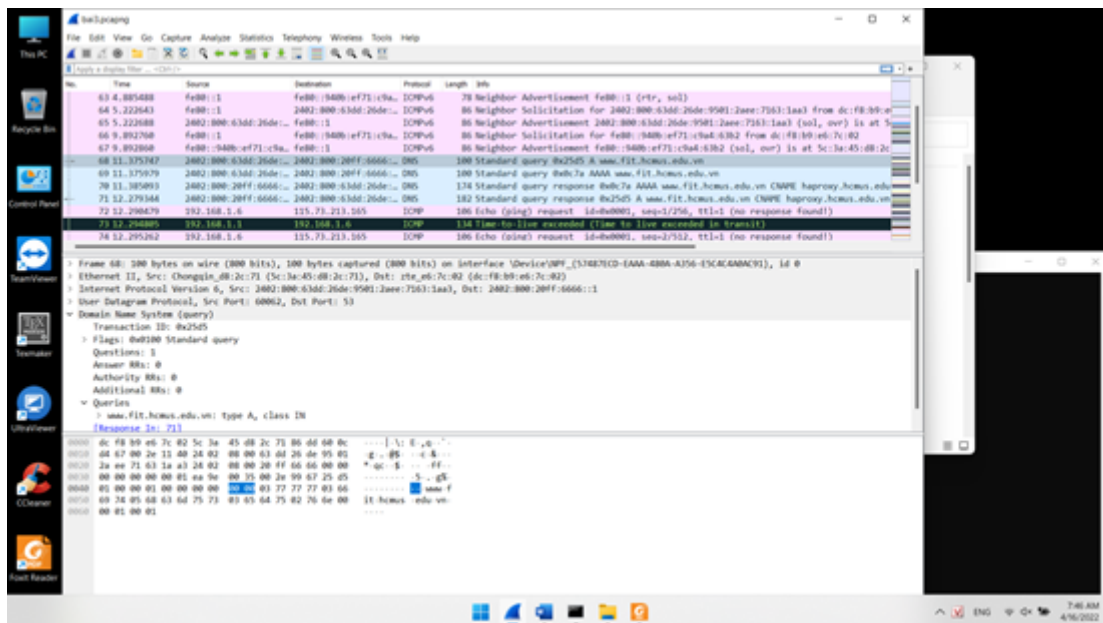


Hình 21: Địa chỉ IP của máy gửi request

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.

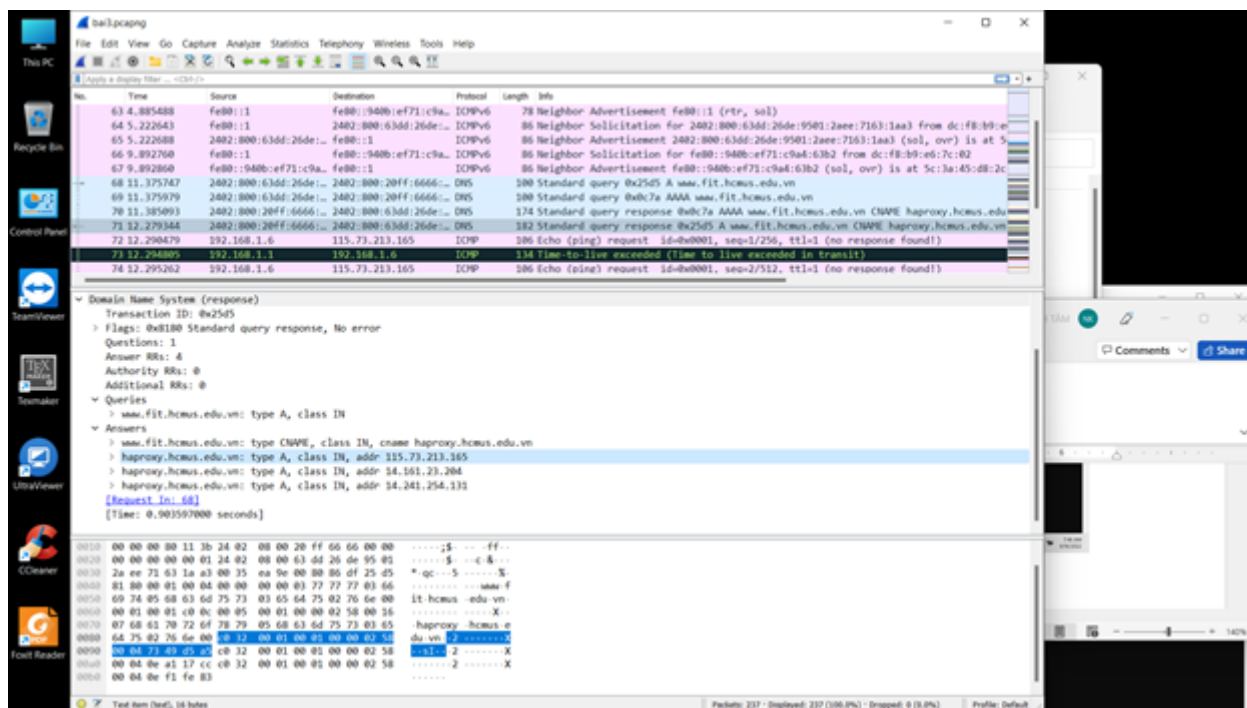
- Gói tin DNS query được gửi từ destination host là gói tin số 68 (được lưu trong file bai3.pcapng).



Hình 22: 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 23: Gói tin DNS query response

6 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*.