**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**CHƯƠNG TRÌNH CHẤT LƯỢNG CAO**

**A picture containing logo

Description automatically generated**

**------------------------/\------------------------**

**ĐỒ ÁN BÁO CÁO ĐỒ ÁN WIRESHARK  
MÔN: MẠNG MÁY TÍNH**

**LỚP: 20CLC08**

**GV HƯỚNG DẪN: THẦY LÊ HÀ MINH (LÍ THUYẾT)**

**THẦY NGUYỄN THANH QUÂN (THỰC HÀNH)**

**Tuy Hòa, ngày 04 tháng 09 năm 2021**

**I. Thông tin của nhóm**

|  |  |  |
| --- | --- | --- |
| STT | MSSV | Họ và tên |
| 1 | 20127441 | Võ Minh Anh |
| 2 | 20127674 | Lê Đức Đạt |

**II. Bảng phân công:**

|  |  |
| --- | --- |
| **Tên thành viên** | **Nhiệm vụ** |
| Võ Minh Anh | - Cấu hình các thiết bị.  - Thực hiện các lệnh console cả hai bài.  - Làm câu 1, 2; lọc filter |
| Lê Đức Đạt | - Vẽ sơ đồ logic.  - Làm câu 3, 4.  - Bắt gói tin HTTP, DHCP |

* **Các nguồn tài liệu tham khảo(nếu có):**

[Bắt và Phân Tích gói tin DHCP bằng Wireshark - YouTube](https://www.youtube.com/watch?v=XcSZ-QTn1Zw)

[Thực Hành Phân Tích Gói Tin Với Wireshark - YouTube](https://www.youtube.com/watch?v=yfi7w9p3QnU)

**III. Mức độ hoàn thành:** 100%

**IV. Trả lời câu hỏi:**

**Bài 1:**

**Câu 1:**

IP của host ping: 192.168.0.105

IP của host được ping: 192.168.1.1

**Câu 2:**

Không có giá trị port. Vì:

+ Port chỉ sử trong giao thức TCP và UDP mà TCP/UDP là giao thức ở tầng 4

+ ICMP là giao thức ở lớp 3 nằm cùng tầng với IP trong bộ giao thức TCP/IP và khác tầng với TCP/UDP nên nó không chứa port (nó chỉ kết nối mạng với thông điệp ICMP echo và ICMP reply).

1. **Câu 3:**

|  |  |  |  |
| --- | --- | --- | --- |
| 48 byte | 8 byte | 20 byte | 14 bytes |
| ICMP data | ICMP header | IP header | Ethernet header |

**Câu 4:**

Vì lúc này chưa tim thấy địa chỉ(MAC) của đích nên nó sẽ gửi ARP Request bằng cách gửi cho tất cả các máy trong mạng lan (Broadcast) thì lúc này đích sẽ nhận được và gửi lại cho nguồn gói ARP Reply cho máy nguồn.

+) Gói ARP Request: Khởi tạo quá trình, bản tin ARP request mà nguồn gửi broadcast để tìm địa chỉ MAC của đích.

+) Gói ARP Reply: là bản tin mà đích sau khi nhận được ARP request sẽ đóng gói lại MAC của mình và gửi bản tin reply về cho nguồn.

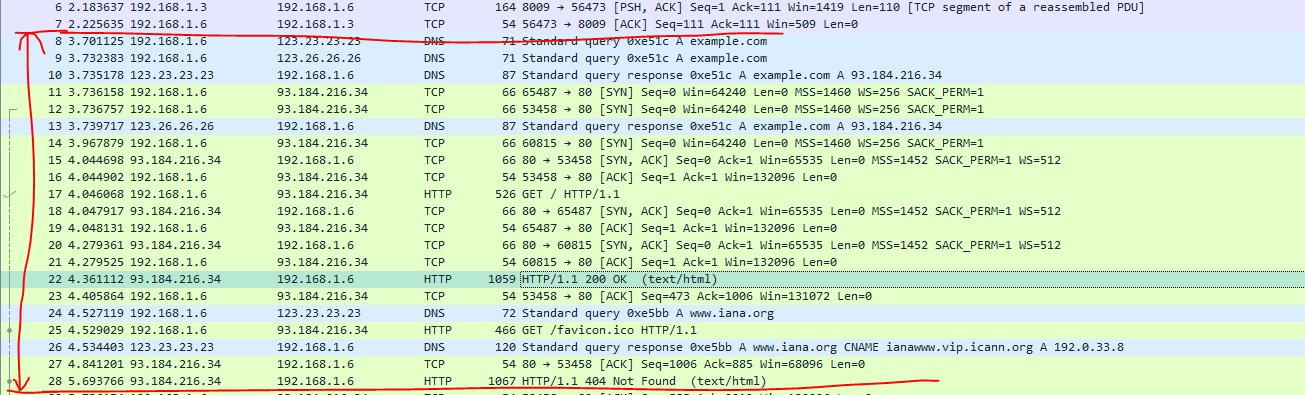
**Câu 5:** Sơ đồ mạng logic:

A picture containing text, table

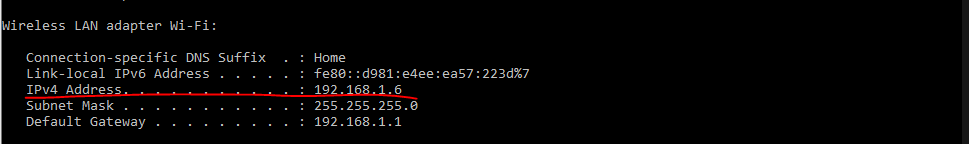
Description automatically generated

**Bài 2:**

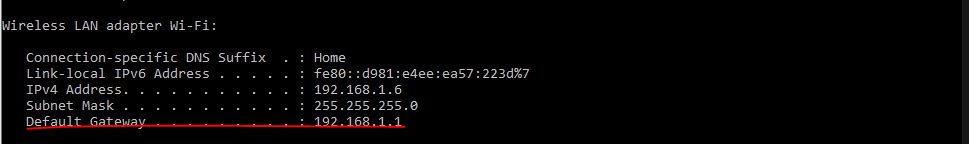
**Câu 1:** Kết quả bắt gói tin



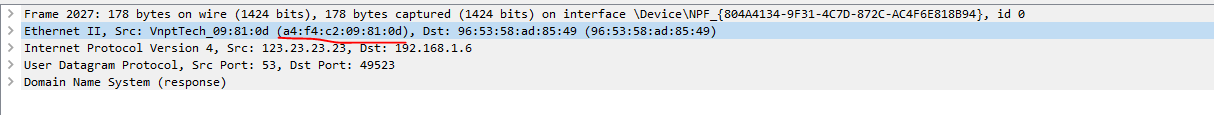
**Câu 2:** IP của host: 192.168.1.6



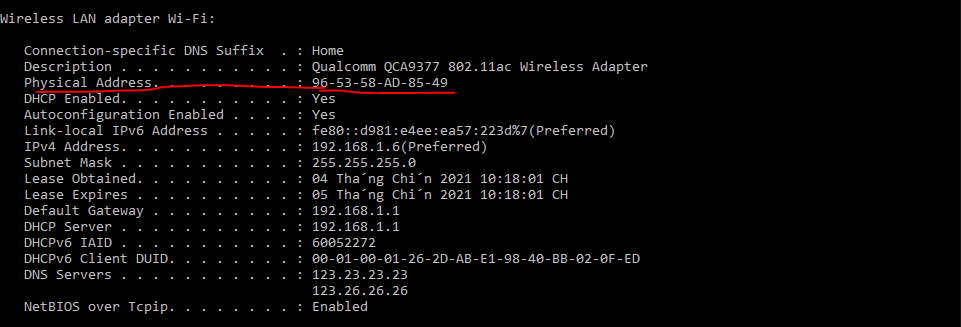
**Câu 3:** IP của router: 192.168.1.1



**Câu 4:** Địa chỉ MAC của host: a4:f4:c2:09:81:0d

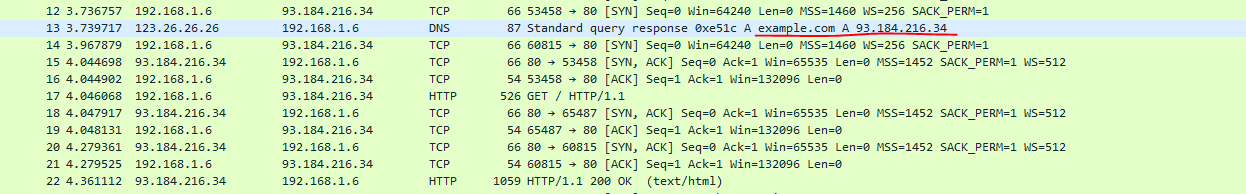


**Câu 5:** Địa chỉ MAC của router:96:53:58:ad:85:49



**Câu 6:** DNS được sử dụng để phân giải tên miền của trang web

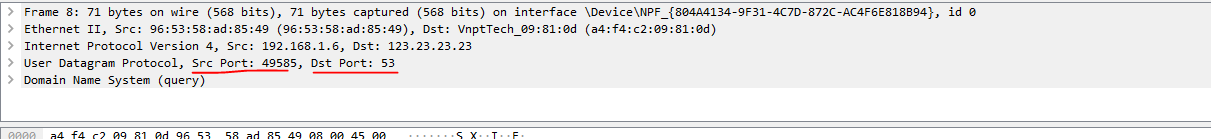
**Câu 7:** IP của HTTP server : 93.184.216.34



**Câu 8:** UDP được sử dụng bởi DNS

**Câu 9:** Source Port là : 49585

Destination Port là : 53



**Câu 10:** Quá trình bắt tay 3 bước hoàn thành sau 0.077023 giây



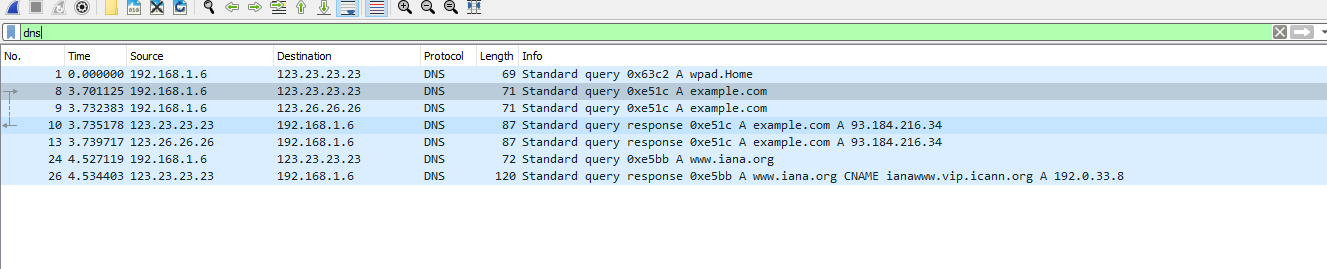
0,985770 – 0,908747 = 0,077023 giây

**Câu 11:** Host machine của Web đang truy cập là : www.example.com

**Câu 12:** Version HTTP đang sử dụng: HTTP/1.1

**Câu 13:** câu query vừa thực hiện giúp lọc ra các gói tin sử dụng UDP ở tầng Transport và có destination port = 53.

Kết quả:



**Câu 14:**

Client

Server

Seq = 0

Seq = 0, ACK = 1

Seq = 1, ACK = 1

GET / HTTP/1.1

Seq = 0, ACK = 1

Seq = 1, ACK = 1

Seq = 1, ACK = 1

Seq = 0, ACK = 1

HTTP/1.1 200 OK

Seq = 473, ACK = 1006

GET /favicon.ico HTTP/1.1

Seq = 1006, ACK = 885

HTTP/1.1 404 Not Found

**Bài 3:**

**Câu 1:**

A picture containing background pattern

Description automatically generated

Text

Description automatically generated with medium confidence

**Câu 2: Tracert/Traceroute** là công cụ dòng lệnh nền tảng Windows dùng để xác định đường đi từ nguồn tới đích của một gói Giao thức mạng Internet (IP - Internet Protocol). **Tracert** tìm đường tới đích bằng cách gửi các thông báo Echo Request (yêu cầu báo hiệu lại) Internet Control Message Protocol (ICMP) tới từng đích. Sau mỗi lần gặp một đích, giá trị Time to Live (TTL), tức thời gian cần để gửi đi sẽ được tăng lên cho tới khi gặp đúng đích cần đến. Đường đi được xác định từ quá trình này.

**Câu 3**: 192.168.1.1

**Câu 4**: khi chuẩn bị phân tích, sẽ có dòng này:

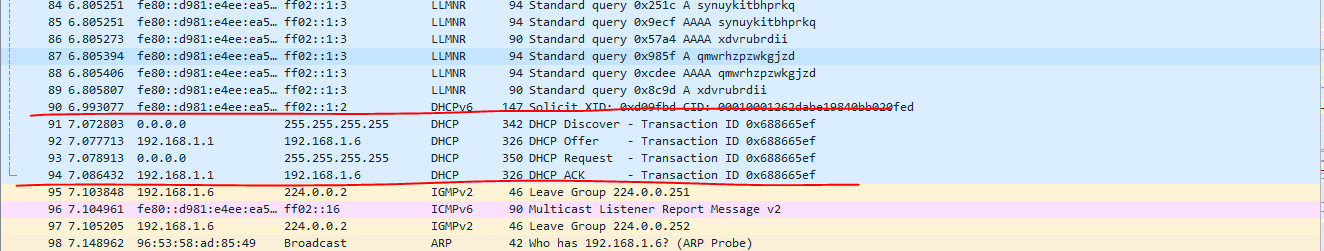
Tracing route to haproxy.hcmus.edu.vn [**14.241.254.131**].

Dòng đỏ chính là địa chỉ IP của FIT.

**Câu 5**:

**Bài 4:**

**Câu 1:** Kết quả chụp màn hình



**Câu 2:**

DHCP message dùng UDP tại tầng transport.

Vì: chức năng của DHCP là cung cấp một cách tự động để phân phối, cập nhật địa chỉ IP và một số thông tin cấu hình khác trên mạng nên cần độ trễ thấp.

Mặt khác UDP là giao thức kiểm soát đường truyền, được sử dụng chủ yếu để thiết lập các kết nối có độ trễ thấp và không chịu lỗi giữa các ứng dụng trên internet.

Vì vậy DHCP message dùng UDP tốt nhất.

**Câu 3:**

* Mục đích của DHCP release: để cho biết DHCP server mà client đã sử dụng địa chỉ IP này, muốn giải phóng địa chỉ IP và xóa bất cứ thuê bao nào đang tồn tại.
* DHCP Server có đảm bảo lúc nào cũng nhận được ACK message từ Client? KHÔNG.
* Nếu thông điệp DHCP release bị mất thì sau đó địa chỉ IP sẽ được dùng cho đến khi hết hạn thời gian.  
  **Câu 4:**

a. DHCP server cho modem của quán café đó đã cấp hết IP cho 91 người nên người thứ 92 không thể truy cập được Internet

b. Vậy những vị khách tiếp theo 93, 94, ....cũng không truy cập được. Những vị khách này phải chờ đợi sau 8 h nữa mới được truy cập.

c. Chủ quán reset lại modem để cấp ip lại cho người trong quán, nên gia hạn thời gian tự động cập nhật lại IP là 3-4 tiếng