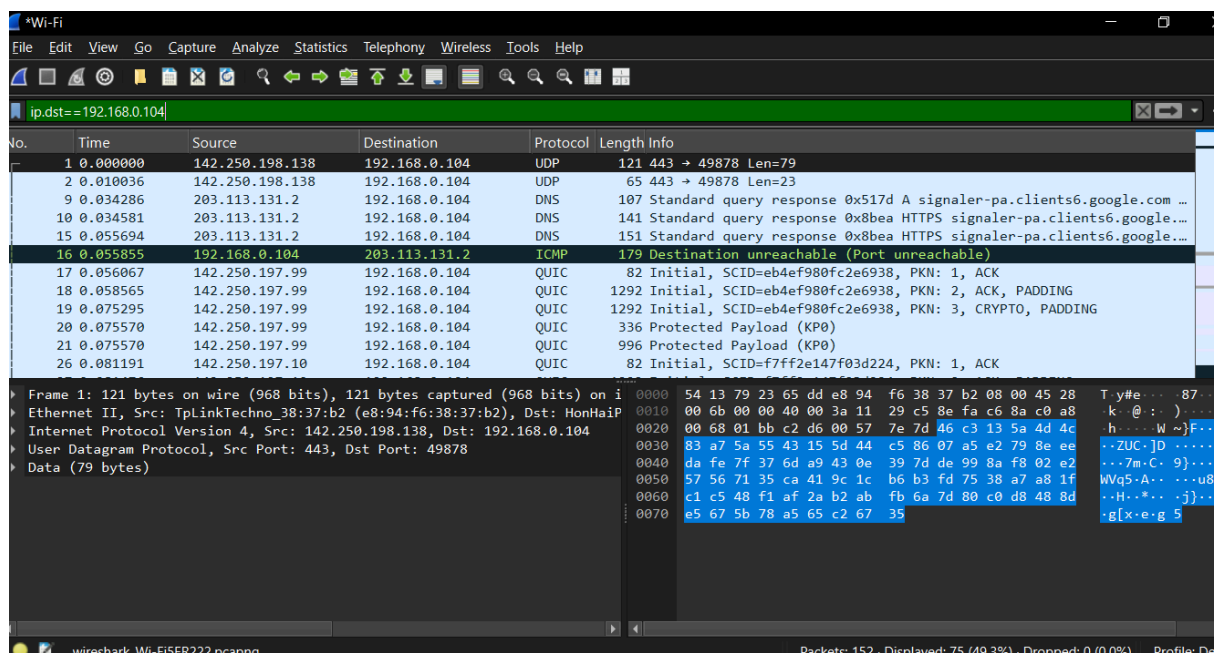


## Bài thực hành chương 1

**Bài thực hành 1: Bắt gói tin Ethernet bằng Wireshark để phân tích các trường dữ liệu.**

### I. Mở Wireshark và chọn giao diện mạng

1. Mở Wireshark.
2. Chọn giao diện mạng đang sử dụng (Ethernet hoặc Wi-Fi).
3. Nhấn Start để bắt gói tin. Sau khi lọc được các gói tin, ta có hình ảnh bắt được các gói tin Ethernet như sau:



**II. Chụp ảnh 1 gói tin hoàn chỉnh và đánh dấu các trường quan trọng. Sau đây ảnh là 1 gói tin hoàn chỉnh**

```
Frame 16: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{8552E941-2828-4B70-B903-270DCD5A98A4}, id 0
Ethernet II, Src: HonHaiPrecis_23:65:dd (54:13:79:23:65:dd), Dst: TpLinkTechno_38:37:b2 (e8:94:f6:38:37:b2)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 203.113.131.2
Internet Control Message Protocol

0000  e8 94 f6 38 37 b2 54 13 79 23 65 dd 08 00 45 00  ...87.T.y#e...E-
0010  00 a5 c2 20 00 00 80 01 68 b3 c0 a8 00 68 cb 71  ...h...h.q
0020  83 02 03 03 0d 08 00 00 00 00 45 00 00 89 04 5a  ...E...Z
0030  40 00 3f 11 27 86 cb 71 83 02 c0 a8 00 68 00 35  @?..q...h5
0040  fe 85 00 75 66 30 8b ea 81 80 00 01 00 00 00 01  ...uf0...
0050  00 00 0b 73 69 67 6e 61 6c 65 72 2d 70 61 08 63  ...signa ler-pa c
0060  6c 69 65 6e 74 73 36 06 67 6f 6f 67 6c 65 03 63  lients6 google c
0070  6f 6d 00 00 41 00 01 06 67 6f 6f 67 6c 65 03 63  om A...google c
0080  6f 6d 00 00 06 00 01 00 00 00 10 00 26 03 6e 73  om...& ns
0090  31 c0 31 09 64 6e 73 2d 61 64 6d 69 6e c0 31 2b  1 1 dns- admin 1+
00a0  ae 7e c9 00 00 03 84 00 00 03 84 00 00 07 08 00  ...
00b0  00 00 3c
```

### Đánh dấu các trường quan trọng:

- Địa chỉ MAC đích (Destination MAC): e8:94:f6:38:37:b2
  - o Chức năng: Xác định thiết bị nhận gói tin trong mạng LAN.
- Địa chỉ MAC nguồn (Source MAC): 54:13:79:23:65:dd.
  - o Chức năng: Xác định thiết bị gửi gói tin
- EtherType: 0x0800 → **IPv4**
  - o Chức năng: Cho biết loại giao thức bên trong gói tin, ở đây là IPv4.

### III. Trả lời các câu hỏi:

Câu 1: Địa chỉ MAC nguồn và đích trong gói tin của Anh/Chị là gì?

Ethernet II (Lớp liên kết dữ liệu - Layer 2)

- Địa chỉ MAC nguồn (Src MAC): HonHaiPrecis\_23:65:dd (54:13:79:23:65:dd)
- Địa chỉ MAC đích (Dst MAC): e8:94:f6:38:37:b2

☐ Ý nghĩa: Gói tin này đang được truyền từ 54:13:79:23:65:dd. đến e8:94:f6:38:37:b2

### Câu 2. Gói tin này sử dụng giao thức nào ở tầng trên (IPv4, IPv6, ARP,...)?

Gói tin này sử dụng giao thức:

- EtherType: 0x0800 (IPv4)

### Câu 3. Có trường Padding không? Nếu có, nó có tác dụng gì?

Dựa vào hình ảnh Wireshark, ta thấy tổng độ dài của gói tin là 179 bytes.

- Trong đó:
  - o Ethernet Header: 14 bytes.
  - o IPv4 Header: 20 bytes.
  - o ICMP Header: 8 bytes.
  - o Dữ liệu (Payload): 147 bytes

- Trong gói tin của không có **Padding**, vì tổng kích thước 179 bytes lớn hơn mức tối thiểu 64 bytes.

### Nếu có Padding, tác dụng là gì?

Trong các gói tin có Payload < 64 bytes, Padding giúp:

- Đảm bảo frame Ethernet đủ 64 bytes để tránh lỗi trên mạng
- Giúp card mạng xử lý đúng gói tin, tránh lỗi truyền tải.
- Không ảnh hưởng đến dữ liệu, vì Padding chỉ là các byte rỗng (0x00).

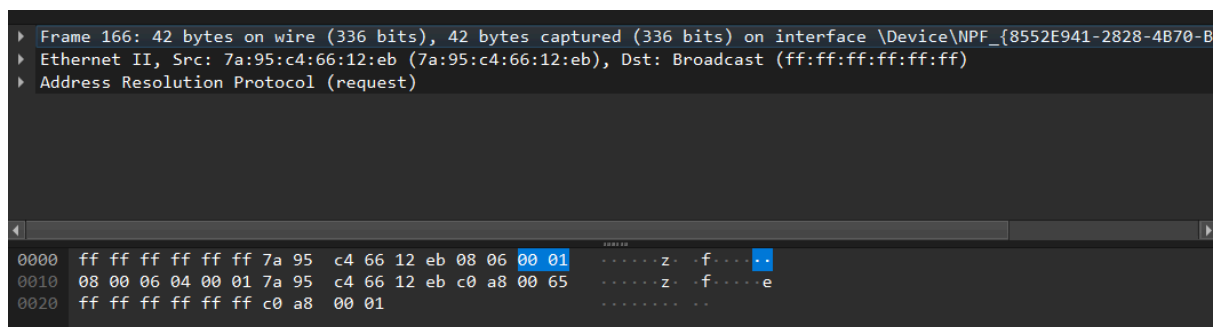
### Câu 4. Kiểm tra CRC của gói tin có hợp lệ không?

Sau khi kiểm tra CRC thì không có gói tin nào bị lỗi, CRC hợp lệ.

### Bài thực hành 2

I. Chọn frame đầu tiên của giao thức ARP, quan sát chi tiết nội dung frame và trả lời các câu hỏi sau:

a) Đây là frame đầu tiên của giao thức ARP



#### 1. Địa chỉ đích (Target - Máy nhận ARP Request)

- MAC Address: ff:ff:ff:ff:ff:ff
- NIC Manufacturer: Không có (Vì đây là địa chỉ Broadcast)
- NIC Serial Number: Không có

#### 2. Địa chỉ nguồn (Sender - Máy gửi ARP Request)

- MAC Address: 7a:95:c4:66:12:eb
- NIC Manufacturer: 7a:95:c4
- NIC Serial Number: 66:12:eb

II. Chọn frame thứ hai của giao thức ARP hiển thị ở cửa sổ Packet List, hãy trả lời các câu hỏi sau:

b) Đây là frame thứ hai của giao thức ARP hiển thị ở cửa sổ Packet List

```

> Frame 3641: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8552E941-2828-4B70-B903-270DCD5A98A4}, id 0
> Ethernet II, Src: 7a:95:c4:66:12:eb (7a:95:c4:66:12:eb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff 7a 95 c4 66 12 eb 08 06 00 01  .....z...f...b.
0010  08 00 06 04 00 01 7a 95 c4 66 12 eb c0 a8 00 65  .....z...f....e
0020  ff ff ff ff ff c0 a8 00 01  .....

```

## 1. Địa chỉ MAC đích (Target - Máy nhận ARP Request)

- MAC Address: ff:ff:ff:ff:ff:ff (Broadcast – gửi đến tất cả thiết bị trong mạng)
- NIC Manufacturer: Không xác định (do đây là địa chỉ Broadcast)
- NIC Serial Number: Không xác định

## 2. Địa chỉ nguồn (Sender - Máy gửi ARP Request)

- MAC Address: 7a:95:c4:66:12:eb
- NIC Manufacturer: 7a:95:c4
- NIC Serial Number: 66:12:eb