**MẠNG MÁY TÍNH**

**ĐỒ ÁN WIRESHARK**

C:\Users\tdqua_000\Dropbox\SS-Slides\DeCuong-CDIO\Template CDIO v4.2\Templates\Hinh anh\LogoTruong.png

Bộ môn Mạng máy tính

Khoa Công nghệ thông tin

Đại học Khoa học tự nhiên TP HCM

# Thông tin SV

* 23127353 – Lương Văn Dũng
* 23127081 – Nguyễn Phan Hùng Linh
* 23127171 – Đỗ Duy Đông

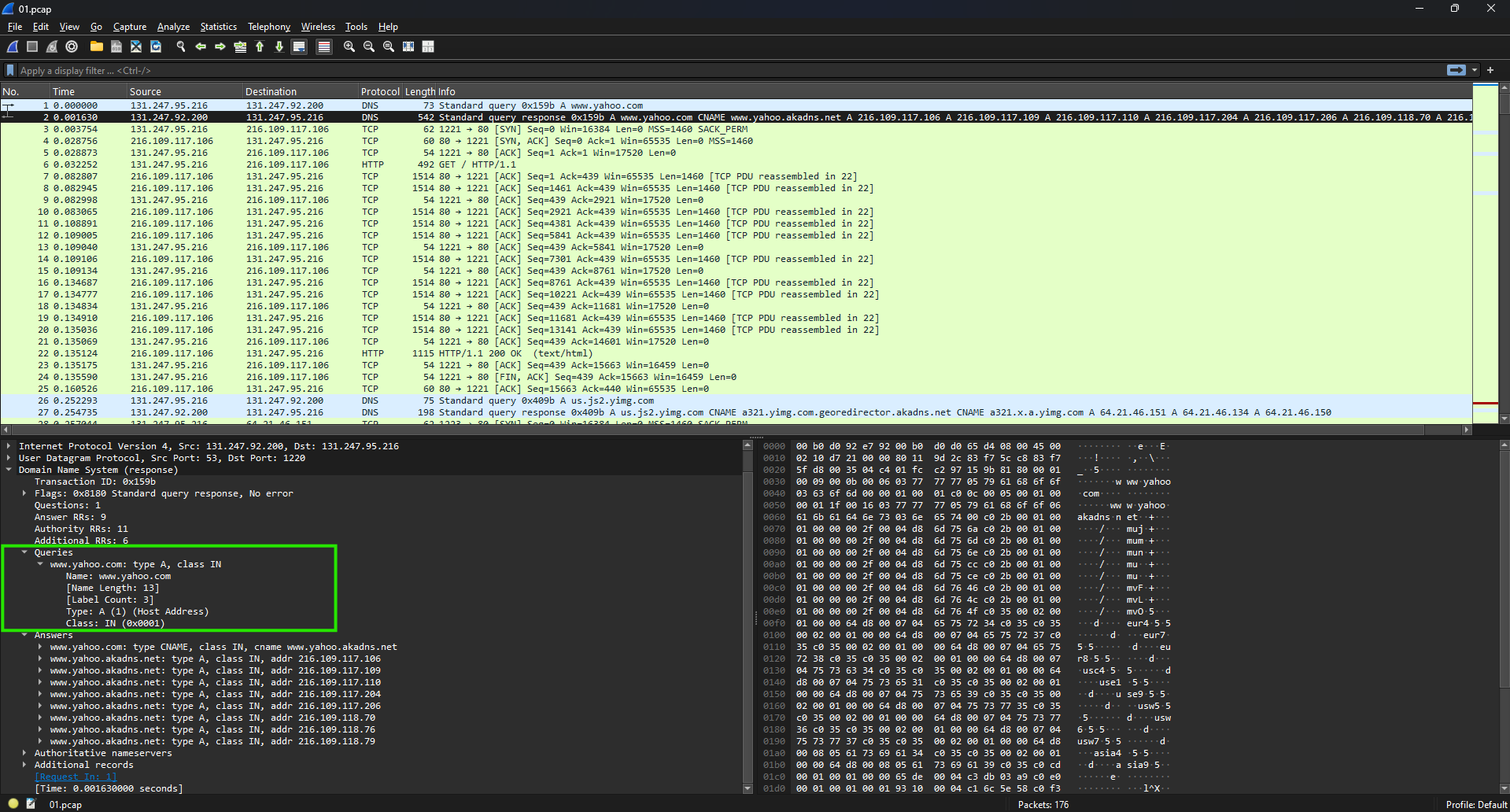
Lớp: 23CLC04

# BÀI LÀM

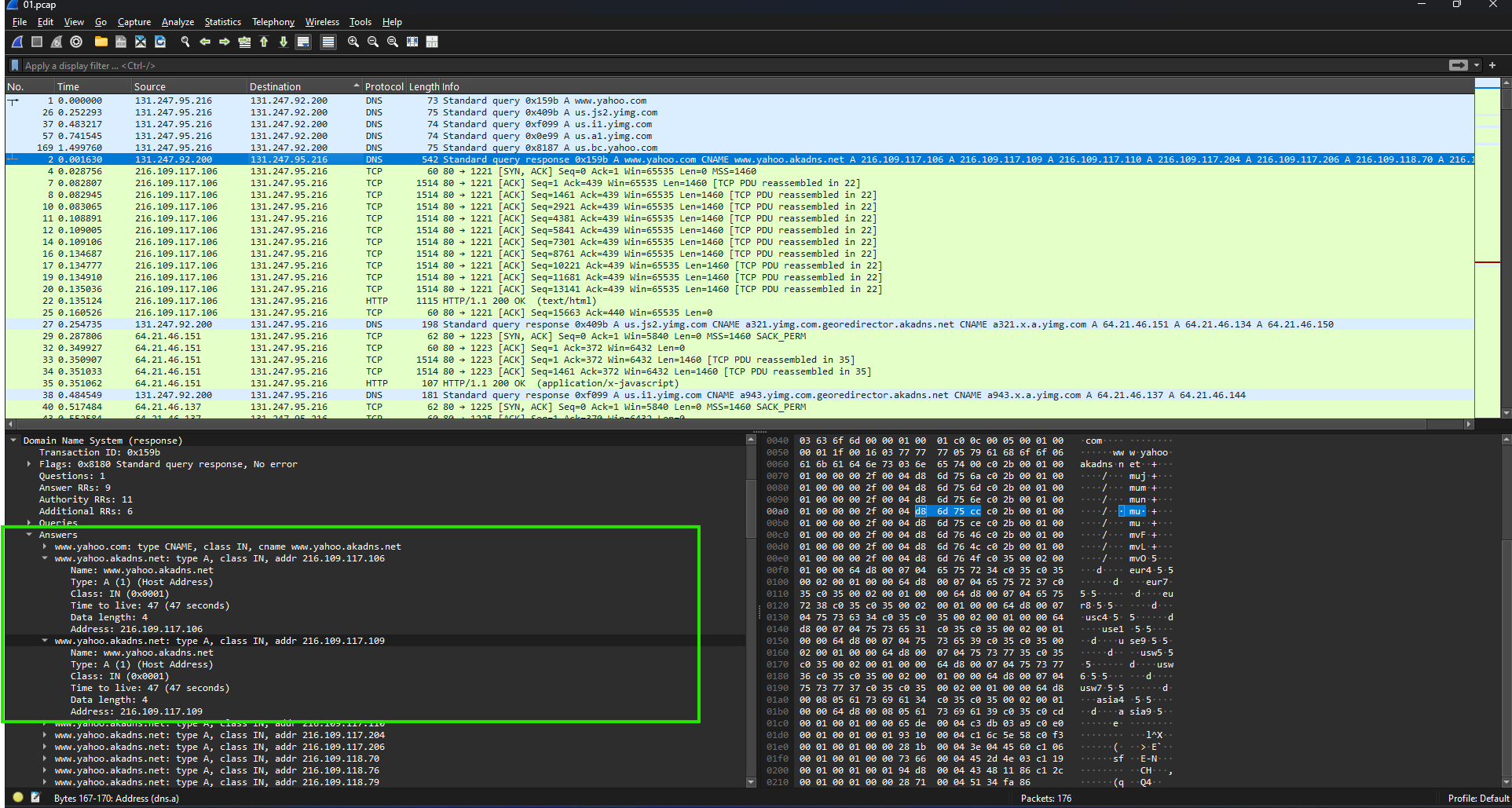
## HTTP

### 1.1 Truy vấn IP.

* + Tên miền của website là: www.yahoo.com



* 2 địa chỉ Ips của website này là:
* 216.109.117.106
* 216.109.117.109



### 1.2 Gói tin mà server đã gửi cho Client.

* Có 28 gói tin mà server đã gửi cho client

A screenshot of a computer

Description automatically generated

### 1.3 Gzip và Cookie.

* Trang web có sử dụng gzip để nén dữ liệu khi gửi đi

A screenshot of a computer

Description automatically generated

* Trang web không ghi cookie vì không thấy trường “Set-Cookie” trong header của HTTP response

### 1.4 Phân tích gói tin số 26 và 27.

* Gói tin số 26: Yêu cầu phân giải DNS từ client tới DNS server. Client muốn biết địa chỉ IP của tên miền us.js2.yimg.com.
* Gói tin số 27: Phản hồi của DNS server với yêu cầu từ client. DNS server trả về cho Client thông tin về tên miền này.
* Lý do phát sinh gói 26 và 27 là Client cần phân giải tên miền us.js2.yimg.com thành địa chỉ IP. Đây là điều cần thiết khi máy tính muốn kết nối đến một tên miền qua Internet.

### 1.5 Tại sao client lại cần hỏi địa chỉ IP cho domain?

* Tại gói tin số 37, tên miền được truy vấn là us.i1.yimg.com. Đây là một tên miền khác hoàn toàn ở gói 26( Tên miền gói 26: us.js2.yimg.com). Lý do Client lại cần hỏi địa chỉ IP cho domain này là vì một trang web không chỉ phụ thuộc vào 1 domain duy nhất. Nó có thể sử dụng nhiều tài nguyên được lưu trữ dưới nhiều tên miền khác nhau. Khi tải một trang web, nó thực hiện nhiều yêu cầu HTTP để tải từng thành phần của trang. Nếu bất kỳ thành phần nào nằm trên một domain mới thì Client sẽ phải gửi DNS query để phân giải tên miền đó sang địa chỉ IP.

### 1.6

1. Nhìn vào Host ở gói 42 và 48 ta thấy 2 gói đều có tên miền là us.i1.yimg.com. A screenshot of a computer

   Description automatically generatedA screenshot of a computer

   Description automatically generated

***Gói 42***  ***Gói 48***

1. Lý do mà hệ thống không cần yêu cầu DNS khác trước câu lệnh get thứ 2 là vì địa chỉ IP của tên miền us.i1.yimg.com đã được phân giải trước đó và được lưu trong DNS cache, nên client chỉ cần tái sử dụng địa chỉ IP đó.

### TCP stream.

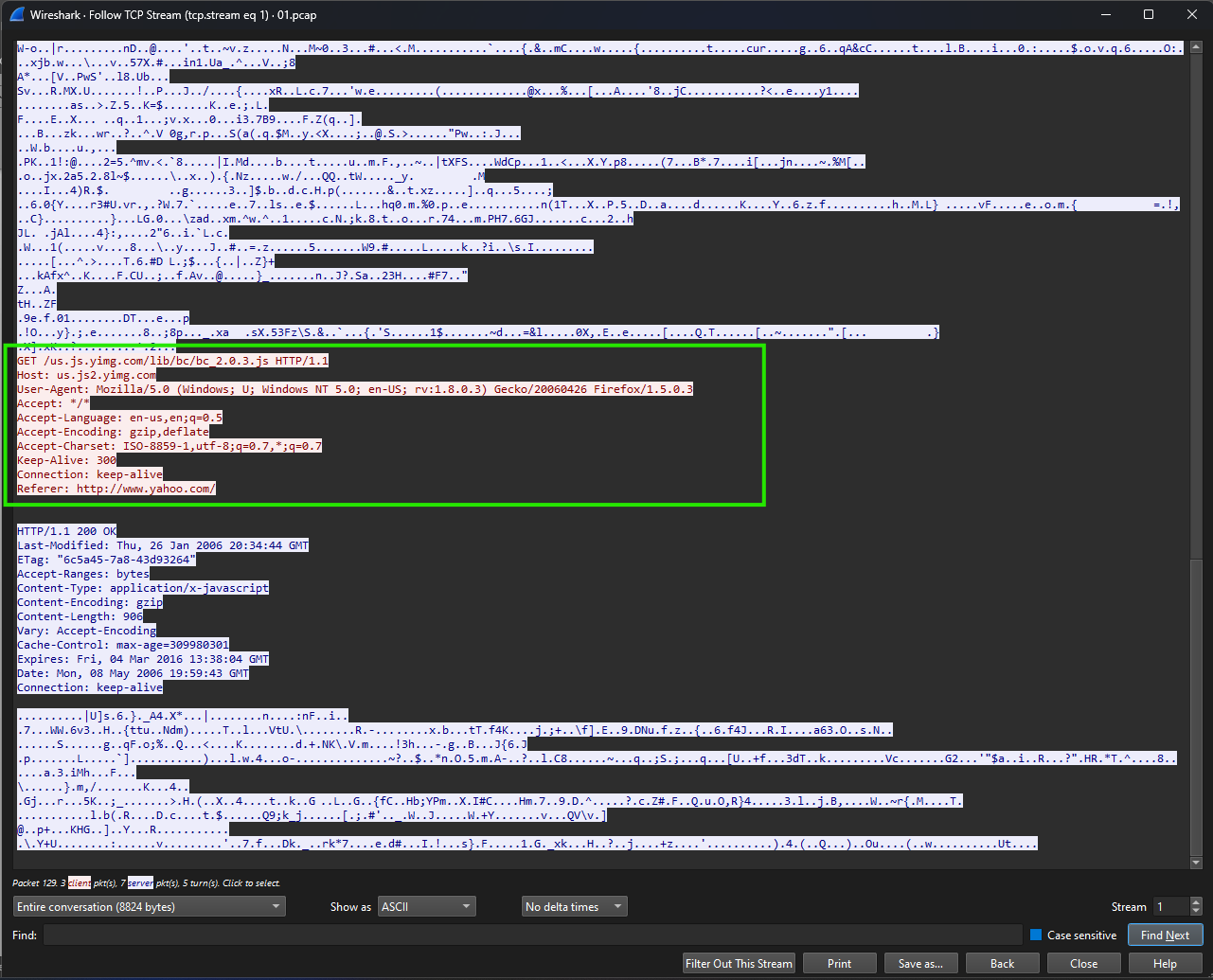
1. Có 3 HTTP request từ Client gửi đi.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated



1. IP của máy Client: 131.247.95.216
2. Loại HTTP connections là persistent HTTP. Vì phần tiêu đề của cả request và response đều có trường: Connection keep-alive.

A screenshot of a computer

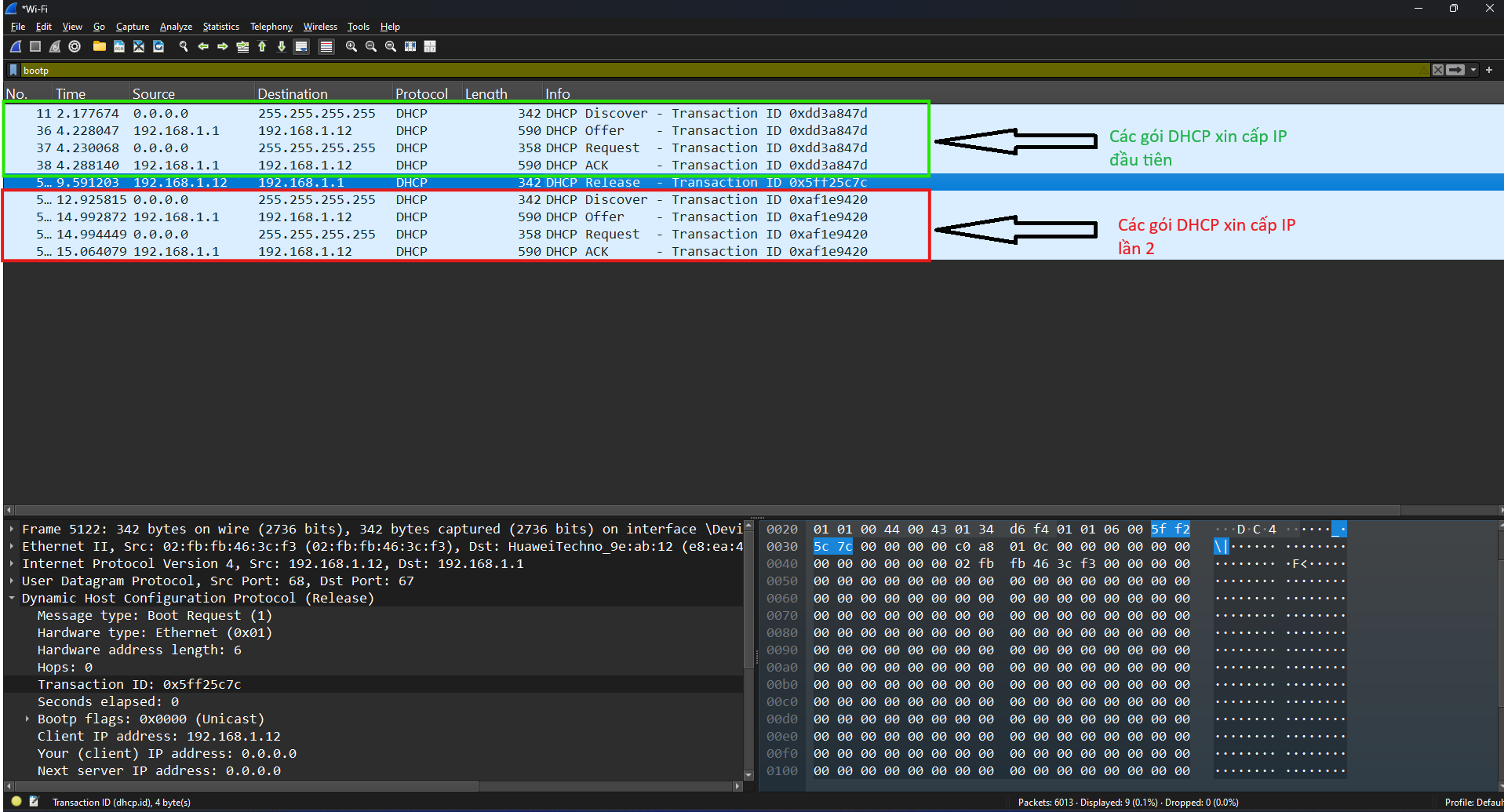
Description automatically generated

Cả 3 HTTP request đều có trường “Connection: keep-alive”.

## DHCP

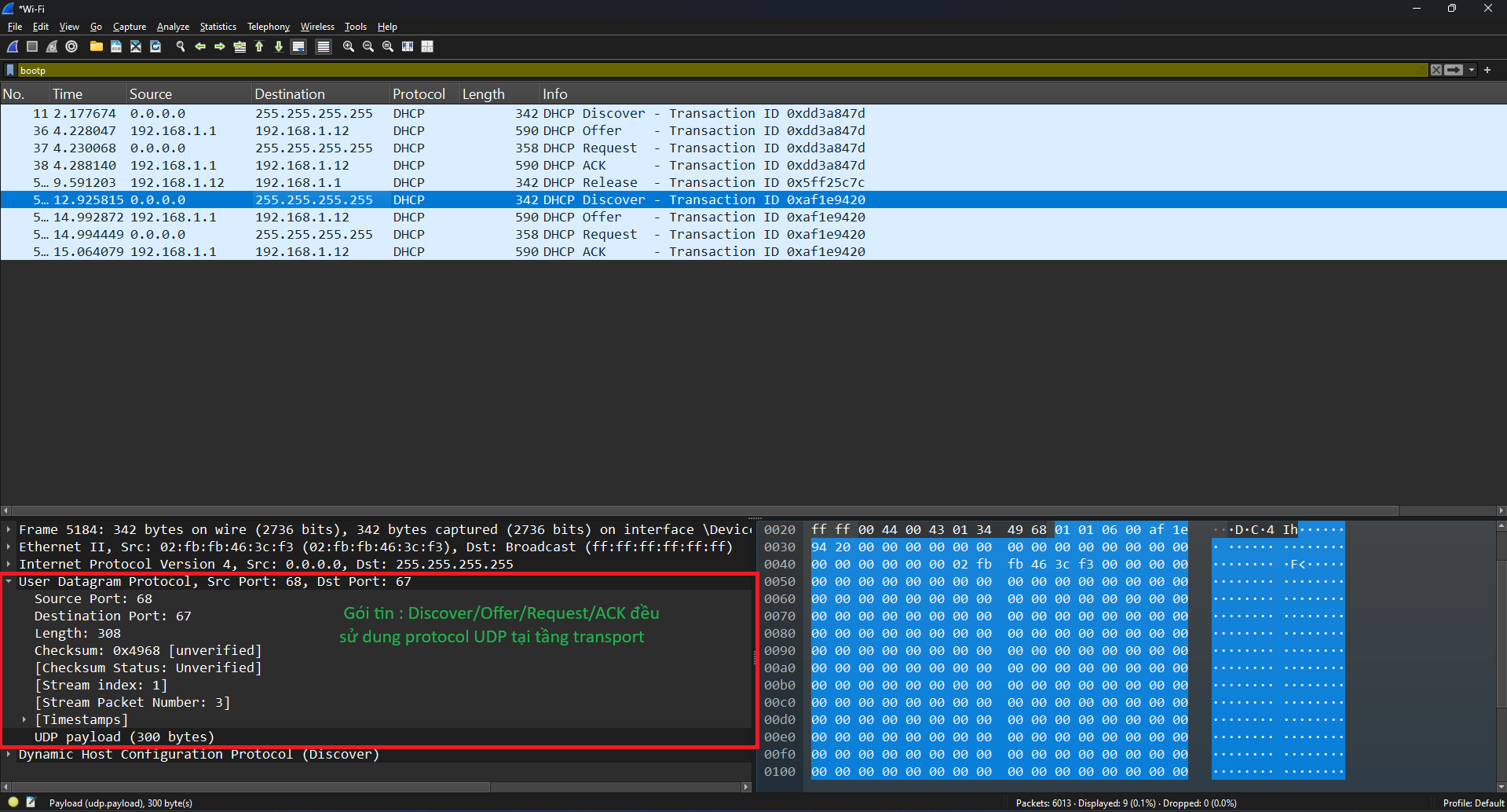
### 2.1 Lọc gói tin DHCP.

* Các gói tin DHCP bắt được: tổng cộng 8 gói tin cho 2 lần bắt, không tín 2 gói DHCP release.



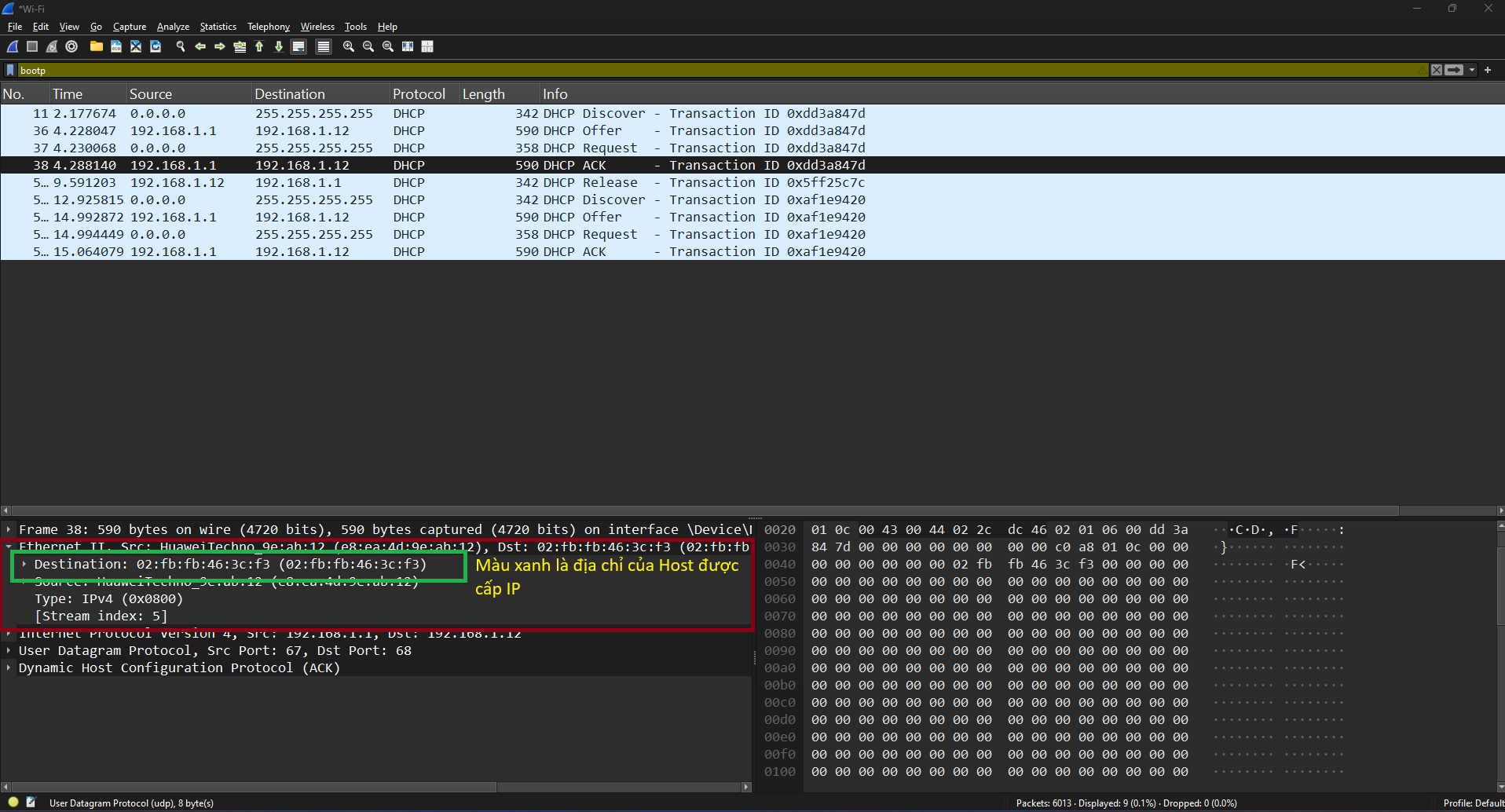
### 2.2 Giao thức tại tầng transport của DHCP.

* Tất cả các gói tin DHCP đều sử dụng giao thức UDP tại tầng transport.



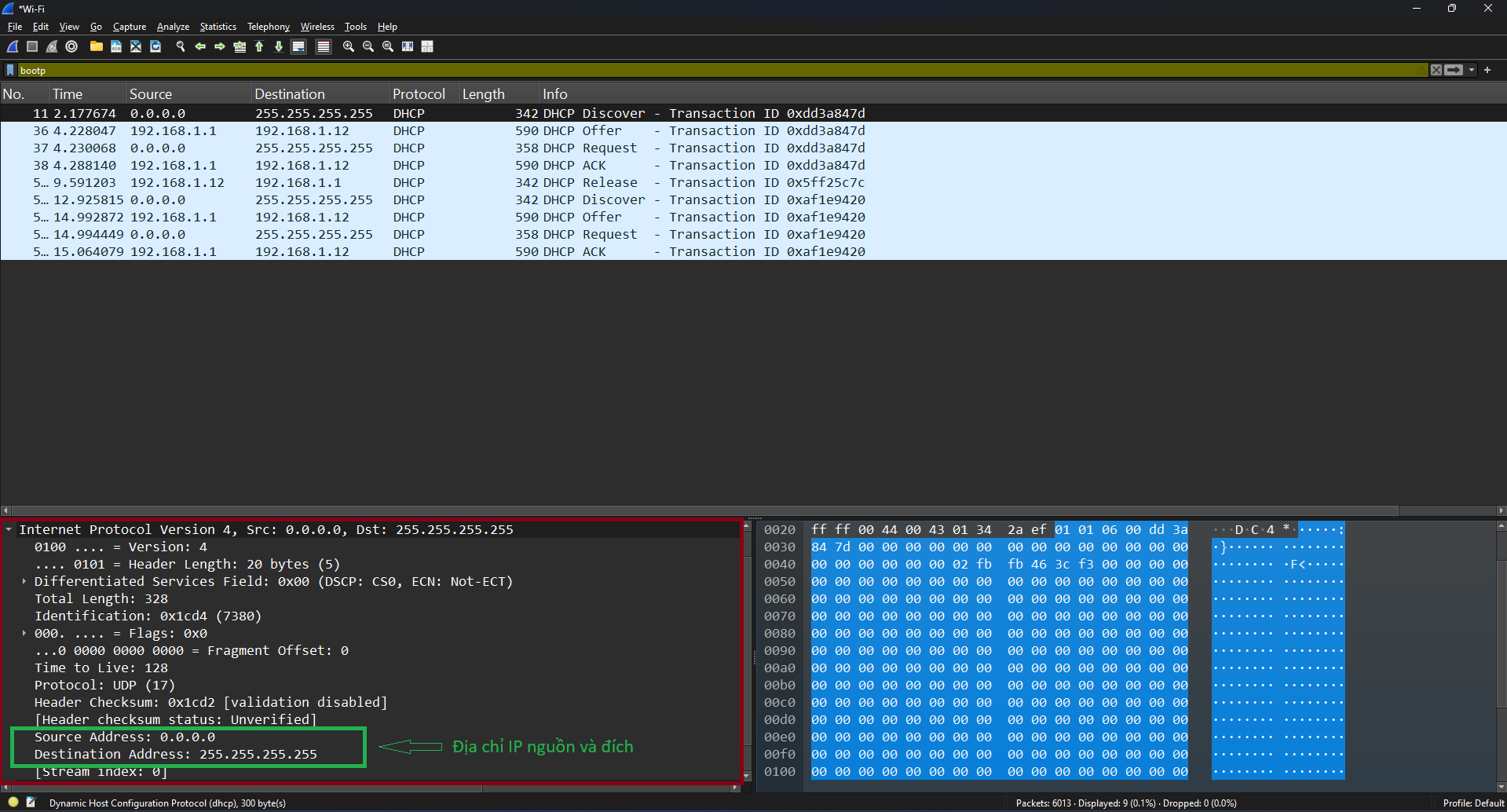
### 2.3 Địa chỉ của Host.

* Địa chỉ tại tầng link của host được cấp IP là: 02:fb:fb:46:3c:f3



### 2.4. Địa chỉ IP nguồn, IP đích.

* Ở 4 gói tin trong đợi xin cấp ip đầu tiên:
* Gói DHCP Discover:
  + Địa chỉ IP nguồn: 0.0.0.0
  + Địa chỉ IP đích: 255.255.255.255



* Gói DHCP Offer:
  + Địa chỉ IP nguồn: 192.168.1.1
  + Địa chỉ IP đích:192.168.1.12

A screenshot of a computer

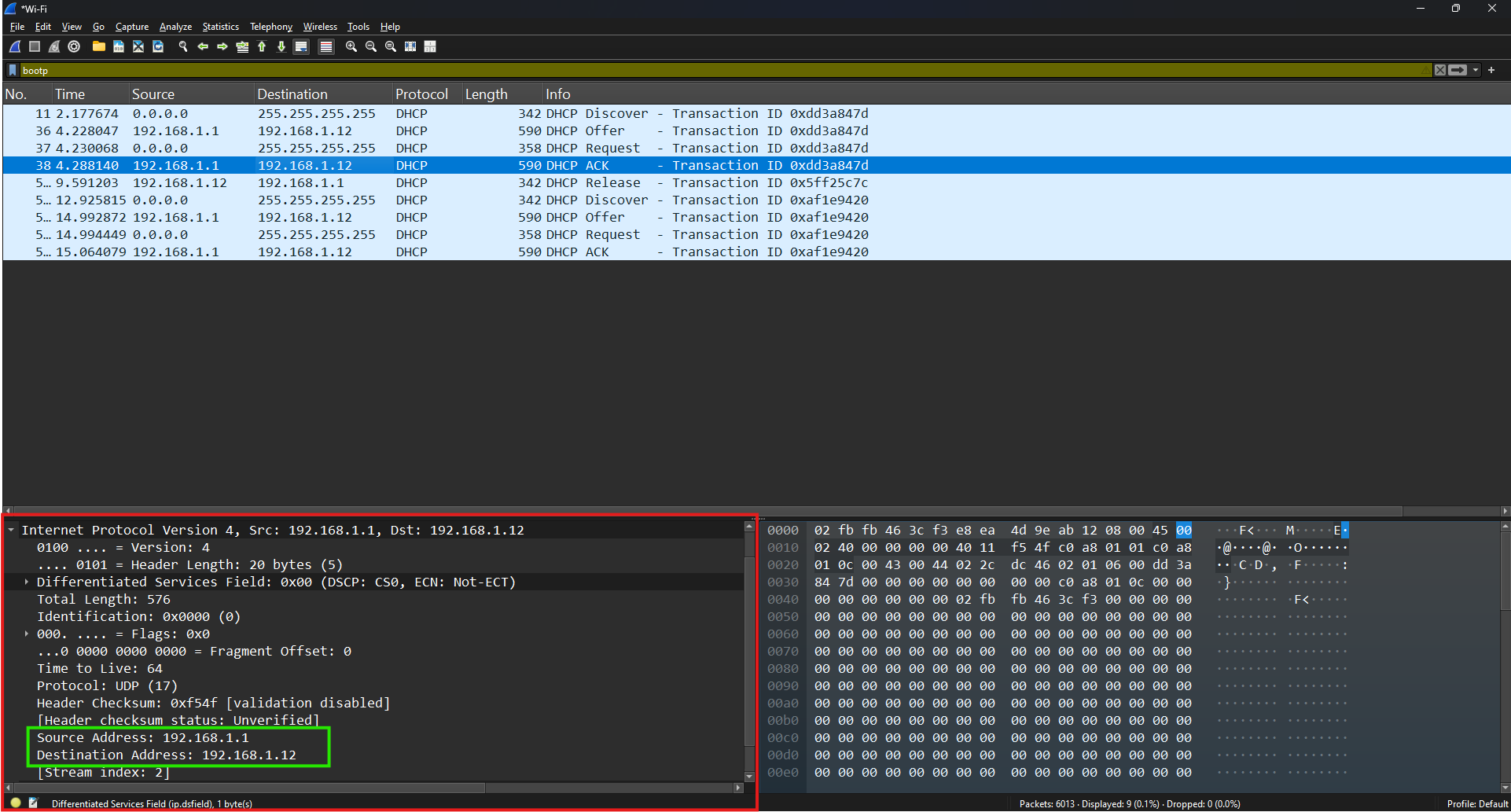
Description automatically generated

* Gói DHCP request:
  + Địa chỉ IP nguồn: 0.0.0.0
  + Địa chỉ IP đích: 255.255.255.255

A screenshot of a computer

Description automatically generated

* Gói DHCP ACK:
  + Địa chỉ IP nguồn: 192.168.1.12
  + Địa chỉ IP đích: 192.168.1.1



### 2.5. Điểm khác biệt giữa các giá trị trong gói tin DHCP Discover và DHCP Request.

|  |  |
| --- | --- |
| DHCP Discover | DHCP Request |
| Không có trường “Option 54” ở tầng Transport | Có trường “Option 54” ở tầng Transport, chứa địa chỉ IP mà client muốn yêu cầu |
| Ở trường “Option 53” giá trị 1 (Discover) thể hiện đây là gói tin để client tìm kiếm máy chủ DHCP trong mạng | Ở trường “Option 53” giá trị 3 (Request) thể hiện đây là gói tin yêu cầu địa chỉ IP cụ thể từ máy chủ DHCP trong mạng |

### 2.6. Giá trị Transaction-ID của 4 gói tin trong đợt xin cấp IP đầu tiên và 2 gói tin trong đợt xin cấp IP lần 2.

* 4 gói tin trong đợt xin cấp IP đầu tiên.
  + Transaction-ID ở gói DHCP Discover: 0xdd3a847d

A screenshot of a computer

Description automatically generated

* + Transaction-ID ở gói DHCP Offer: 0xdd3a847d

A screenshot of a computer

Description automatically generated

* + Transaction-ID ở gói DHCP Request: 0xdd3a847d

A screenshot of a computer

Description automatically generated

* + Transaction-ID ở gói DHCP ACK: 0xdd3a847d

A screenshot of a computer

Description automatically generated

* 2 gói tin trong đợt xin cấp IP lần 2:
  + Transaction-ID ở gói DHCP Request: 0xaf1e9420

A screenshot of a computer

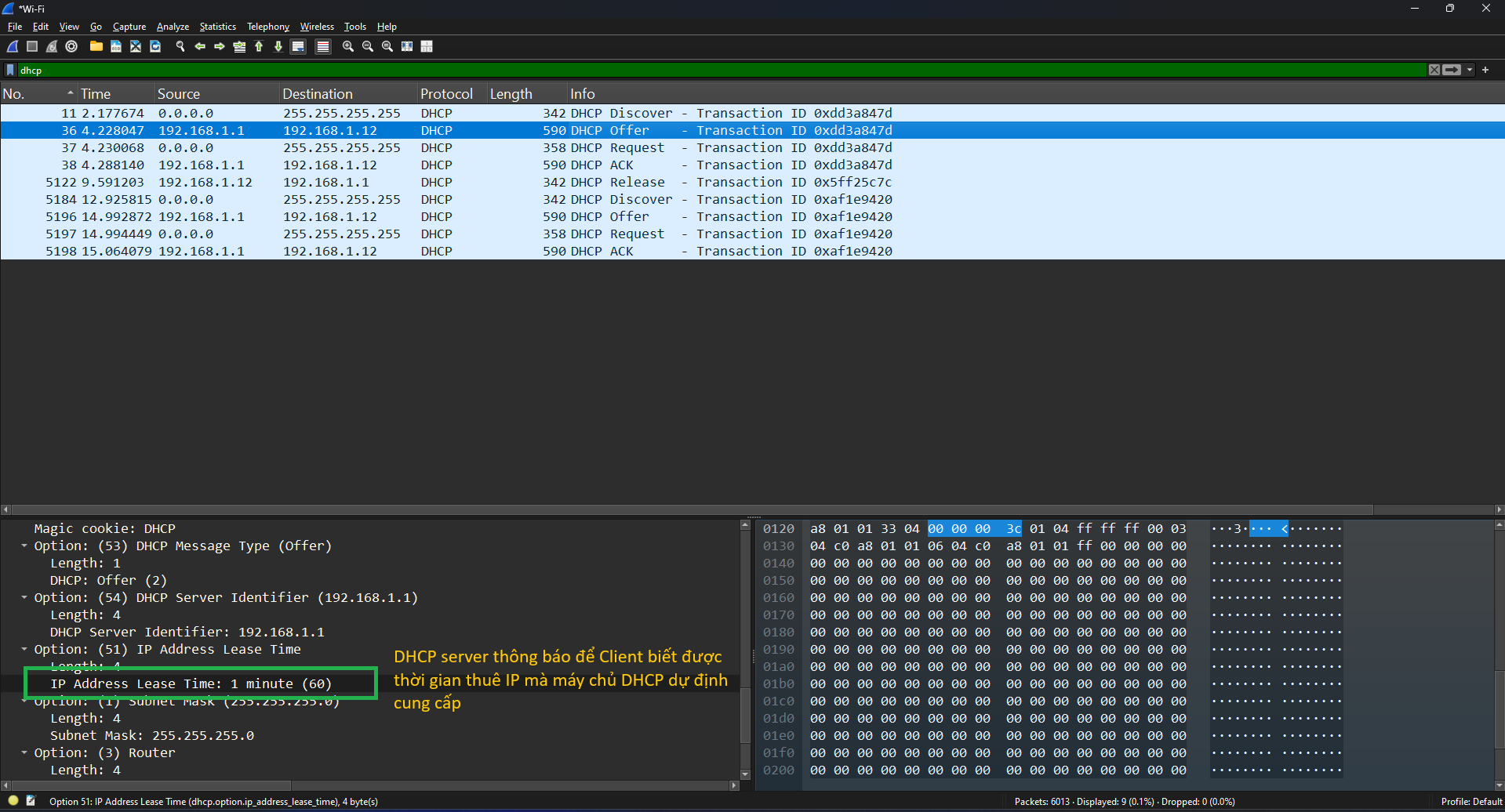
Description automatically generated

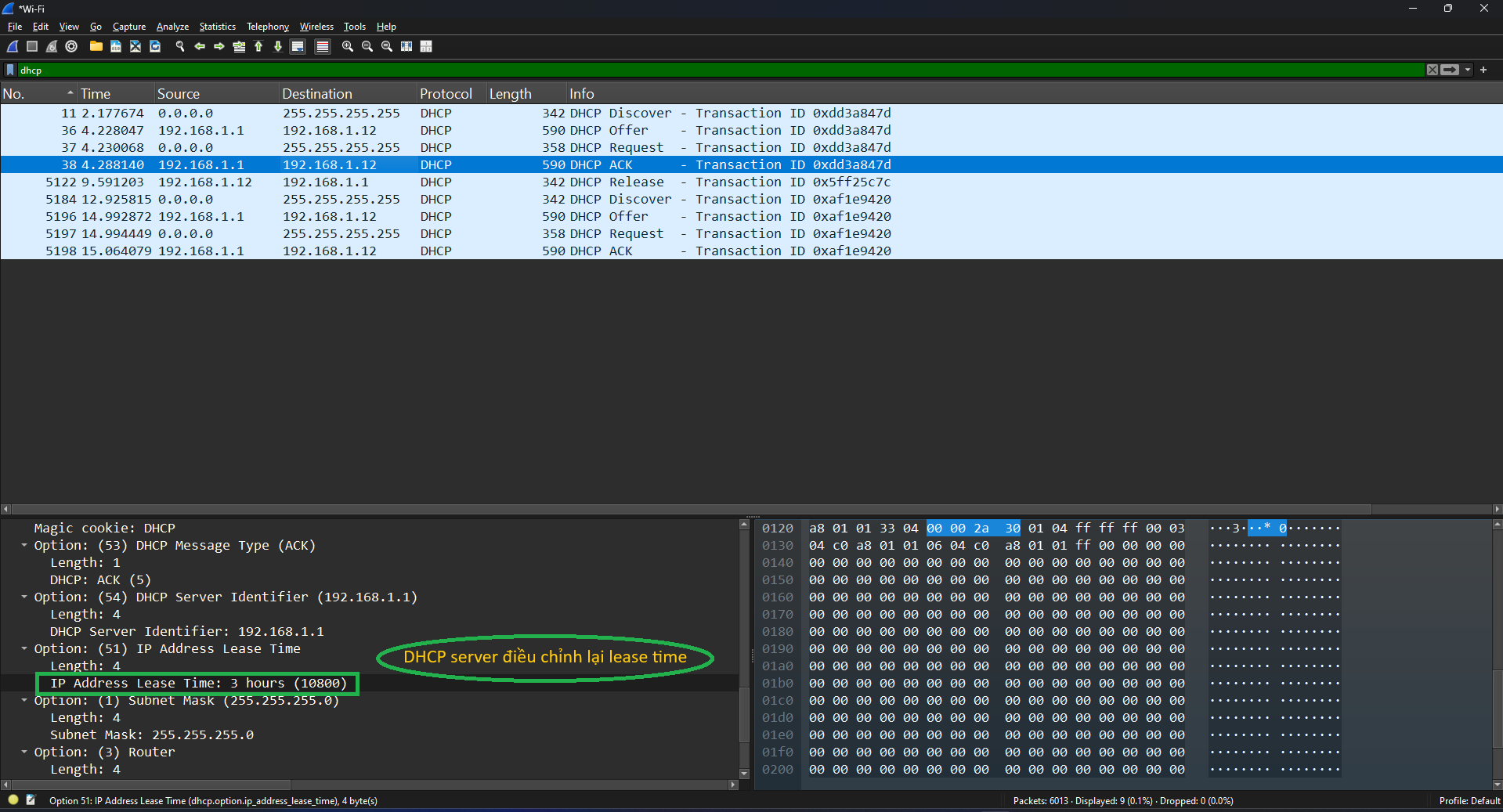
* + Transaction-ID ở gói DHCP ACK: 0xaf1e9420

A screenshot of a computer

Description automatically generated

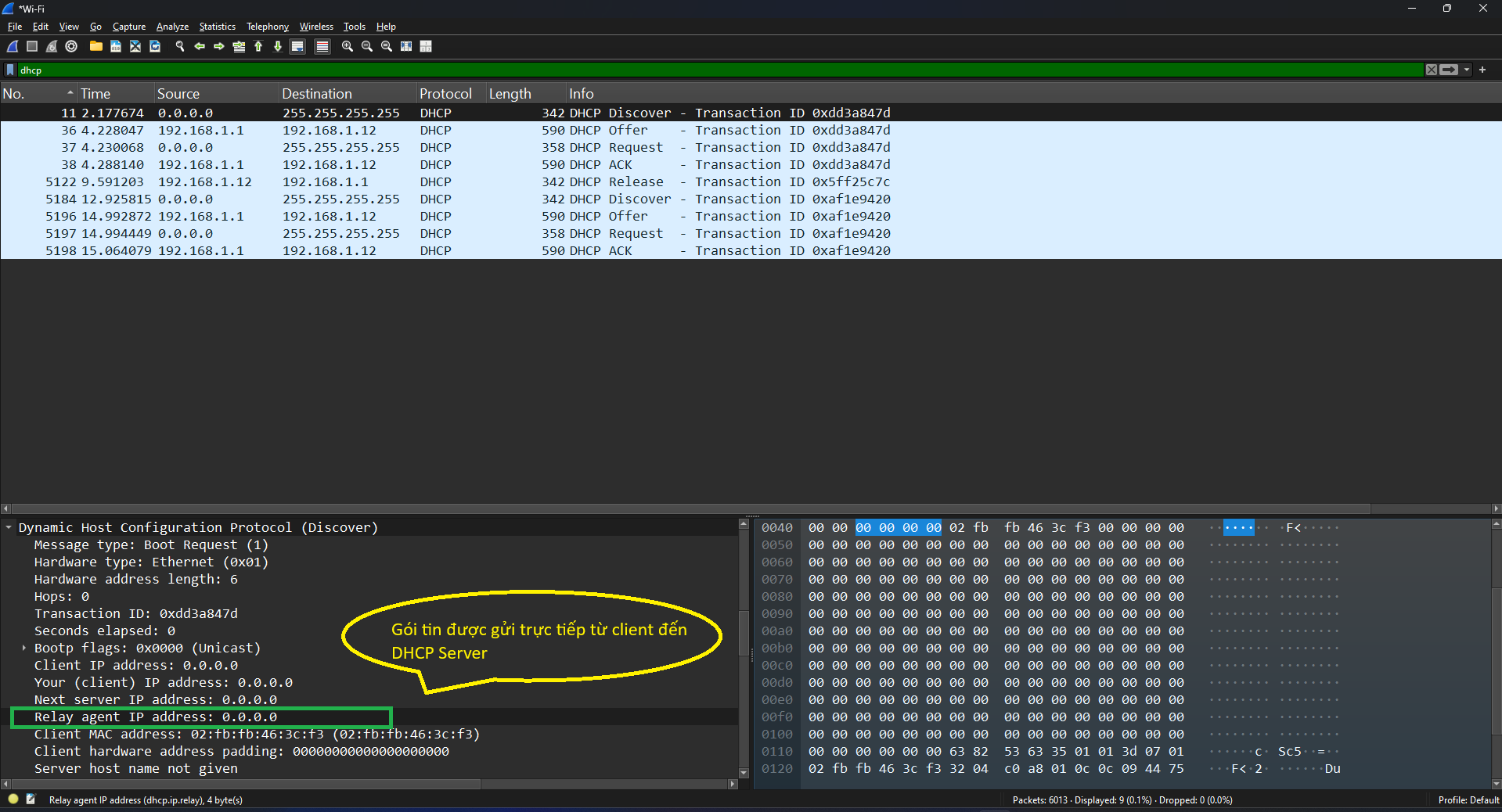
### 2.7. Ý nghĩa và giá trị của trường thông tin “lease-time”.

* + Ý nghĩa: Là khoảng thời gian mà một thiết bị được phép sử dụng địa chỉ IP mà DHCP server cung cấp. Khi gần hết thời gian thuê Client sẽ gửi một gói DHCP request. Nếu DHCP server đồng ý thì lease time sẽ được gia hạn giúp quản lý tài nguyên IP hiệu quả.
  + Giá trị của trường thông tin “lease-time” trong gói tin bắt được là:
    - * Ở gói DHCP Offer trong lần xin cấp IP đâu tiên “Lease Time” có giá trị là: 1 phút
      * Ở gói DHCP ACK trong lần đầu tiên, “Lease Time có giá trị là: 3 giờ



### 2.8. DHCP relay agent

* Trường “Relay agent IP address” trong phần Header cho biết có Relay Agent hay không. Trong các gói DHCP bắt được, trường “Relay agent IP address” có giá trị là 0.0.0.0 nên không thông qua bất kỳ Relay Agent nào.



## ICMP

### 3.1. MSS (maximum segment size) và MTU (maximum transmission unit).

* **MSS** là kích thước tối đa của phần dữ liệu trong một gói TCP, không tính header.
* **MTU** là kích thước tối đa của một gói tin bao gồm cả header, được sử dụng trên lớp liên kết dữ liệu.
* MSS không thể lớn hơn MTU, vì MSS được giới hạn bởi kích thước MTU của mạng để tránh phân mảnh gói tin.

### 3.2. MTU trên card mạng kết nối internet.

* MTU trên card mạng kết nối internet có giá trị là: 1500 bytes

A screenshot of a computer

Description automatically generated

### . Kích thước các phần của gói ICMP tại tầng network.

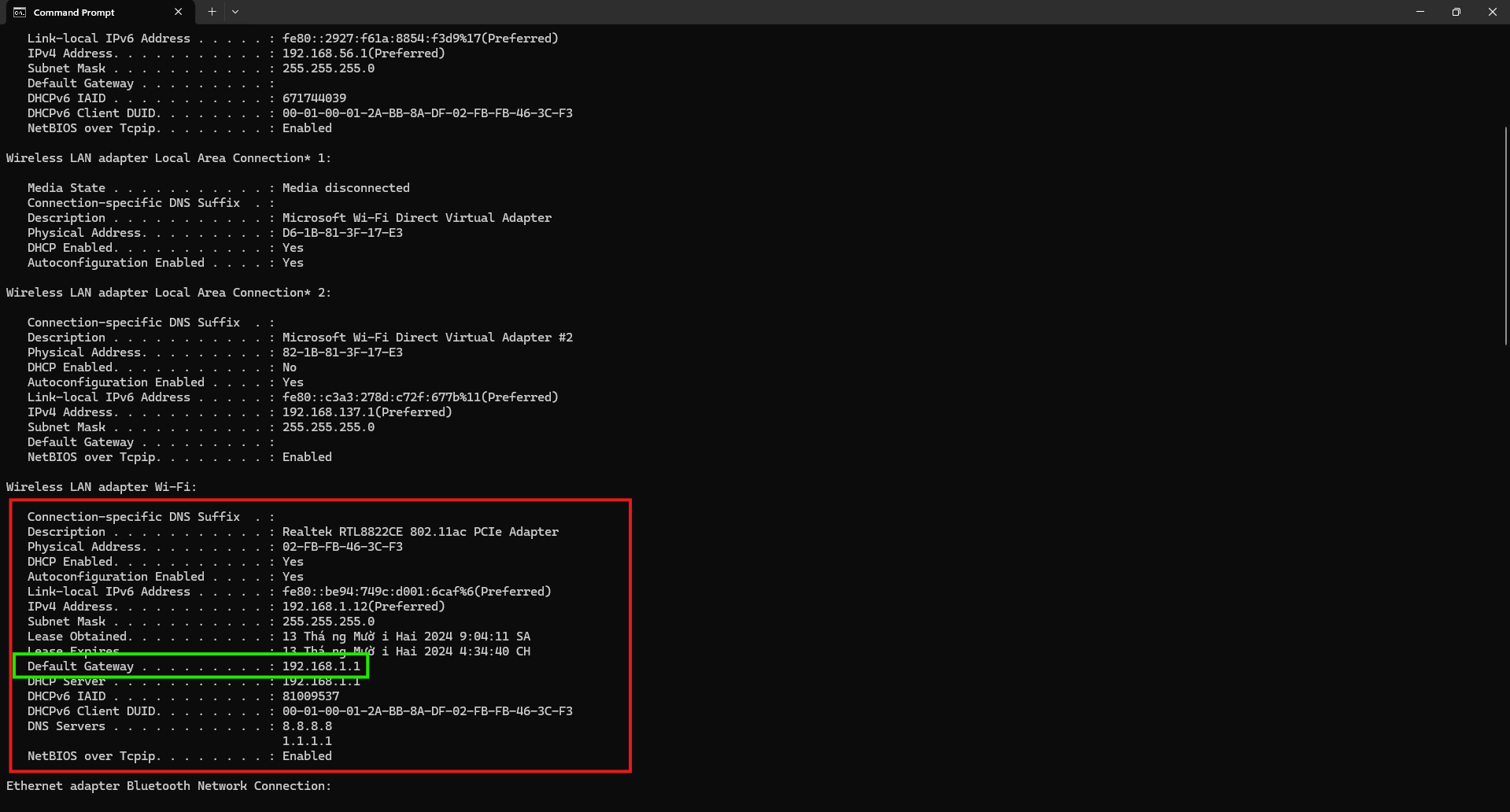
* Kích thước của các phần của gói ICMP tại tầng mạng cơ bản (network) là:
  + - * Phần Header ICMP: 8 bytes
      * Phần Data: 1492 bytes. (1500bytes MTU – 8bytes ICMP Header)
* Vì vậy, kích thước tối đa của phần data trong một gói tin ICMP tại tầng mạng sẽ là 1492 bytes khi MTU là 1500 bytes. Do trừ đi 8 bytes cho phần header ICMP từ tổng kích thước MTU 1500 bytes.

### . Kích thước các phần của gói ICMP tại tầng Data link.

* Tại tầng Data Link, ngoài phần header và data của ICMP, còn có thêm phần header của tầng Data Link. Phần header này thường có kích thước 14 bytes.
* Kích thước các phần của gói ICMP tại tầng Data Link khi MTU là 1500 bytes sẽ là:
* Phần header Data Link: 14 bytes
* Phần header ICMP: 8 bytes
* Phần data ICMP: 1500 - 14 - 8 = 1478 bytes

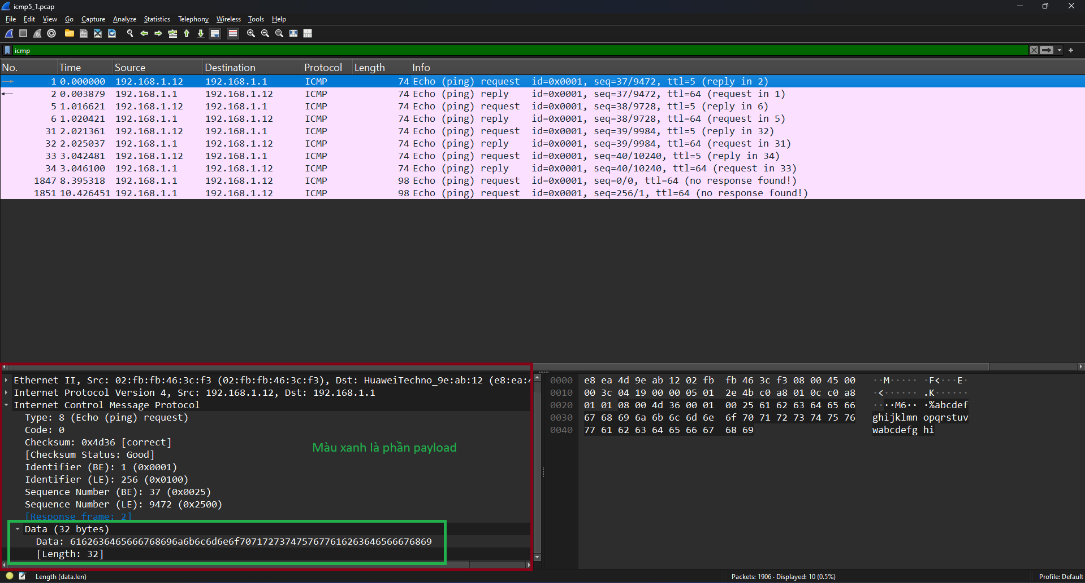
A screenshot of a computer

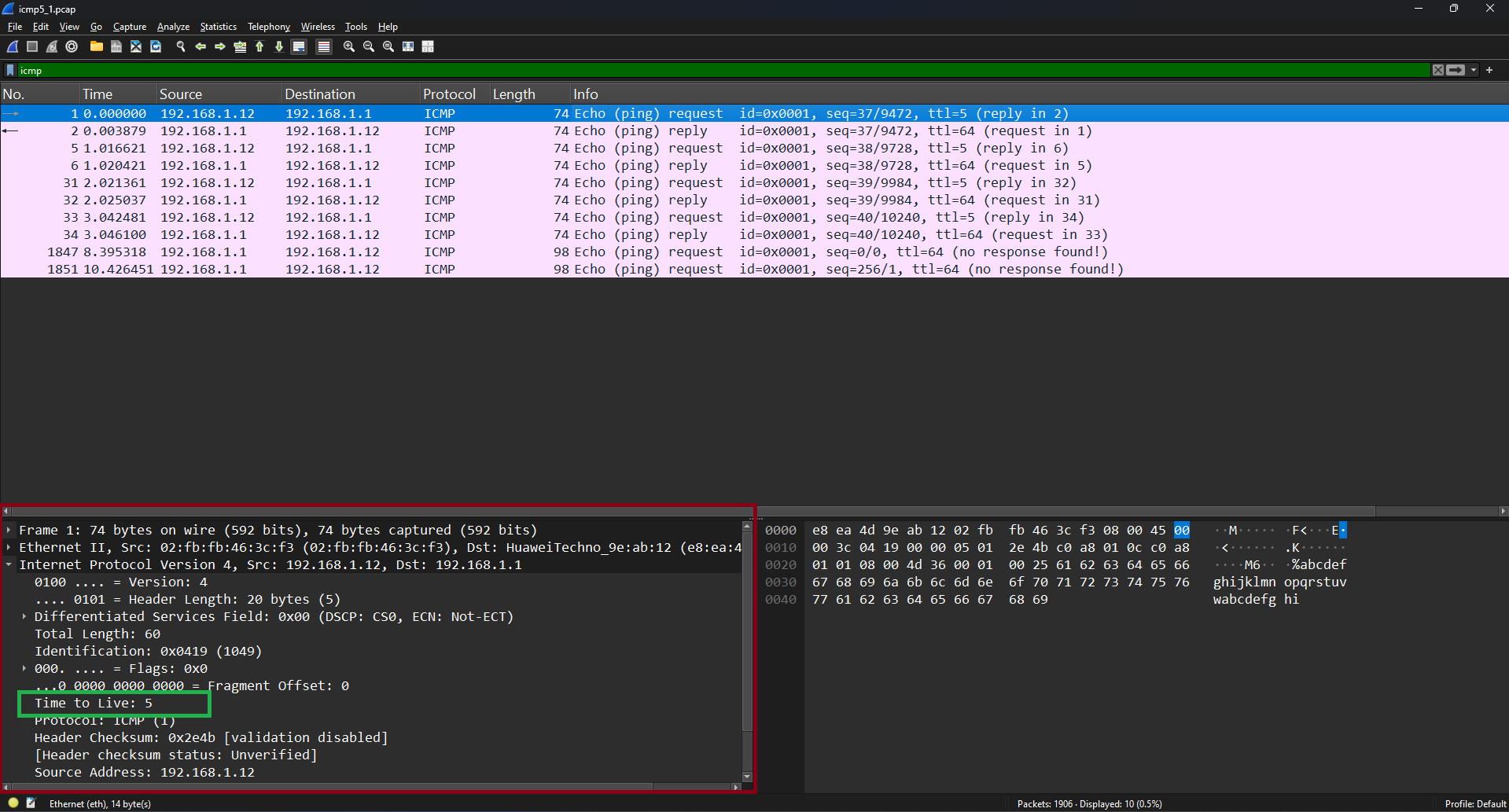
Description automatically generated



### 3.5. Ping IP và bắt gói tin

* **ping -i 5 192.168.1.1**
  + Data trong ICMP payload là: 32 bytes ở mỗi gói ICMP request hoặc ICMP reply.

****

* + Time to live:

- ICMP request: 5

**ICMP Request**

A screenshot of a computer

Description automatically generated- ICMP Replay: 64

**ICMP reply**

* **ping -l 33 192.168.1.1**
  + Data trong ICMP payload là: 33 bytes ở mỗi gói ICMP request hoặc ICMP reply.

**A screenshot of a computer

Description automatically generated**

* + Time to live :

- ICMP request: 128

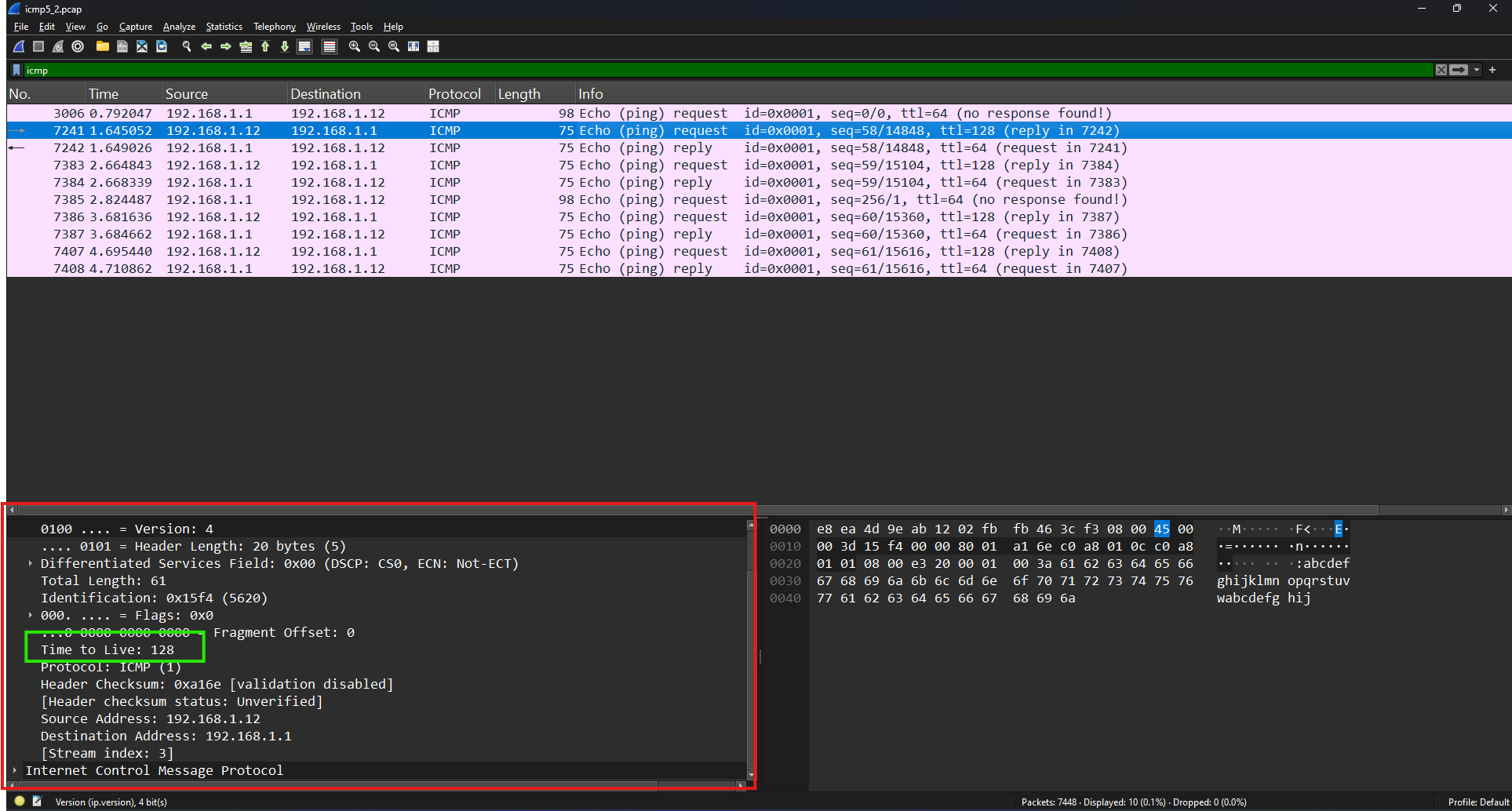
**ICMP request**

A screenshot of a computer

Description automatically generated

- ICMP reply: 64

**ICMP reply**



### 3.6. Ping và bắt gói tin

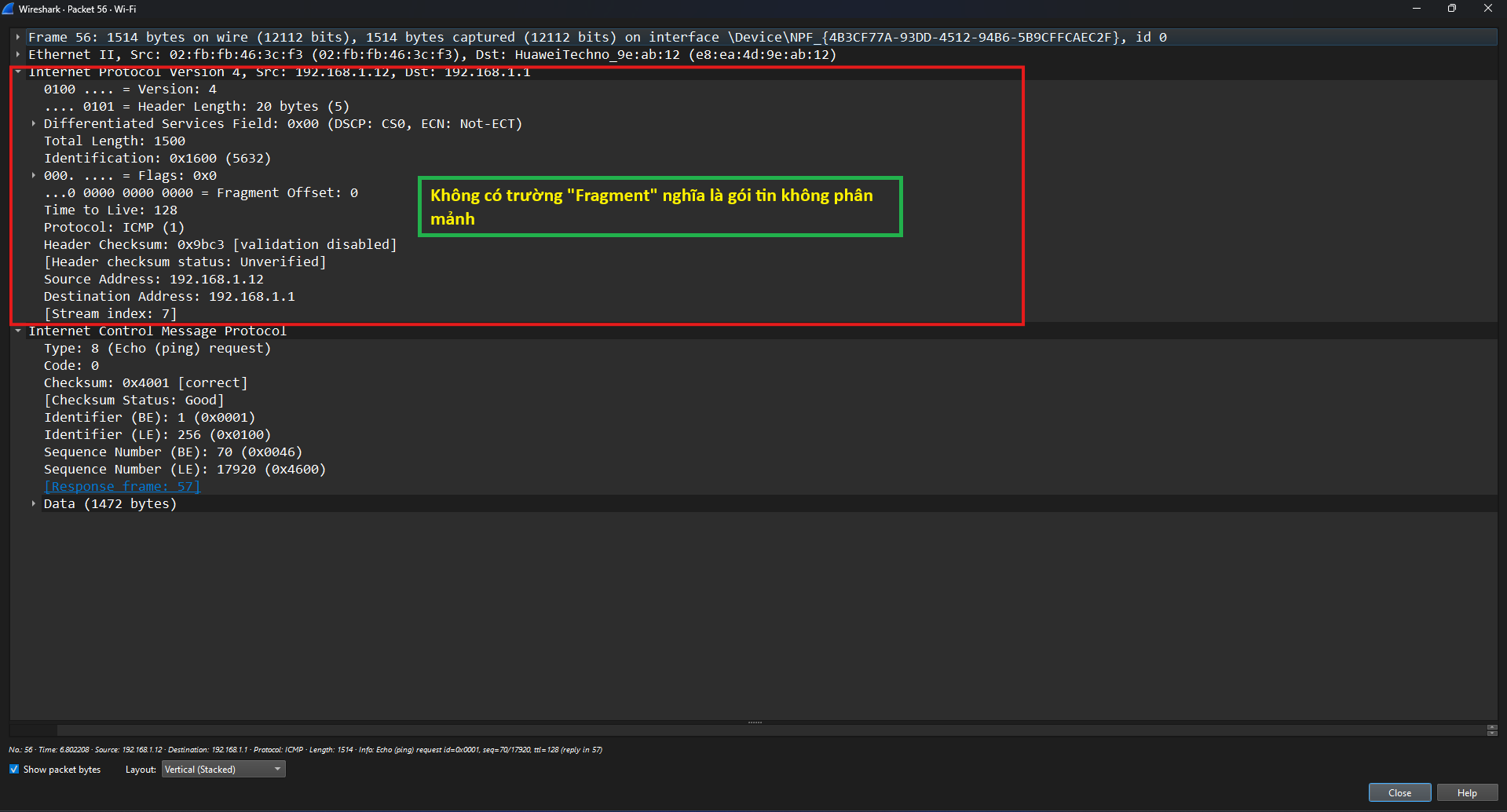
* + **ping -l 1472 192.168.1.1**
* Data trong ICMP payload là 1472 bytes ở mỗi gói ICMP request hoặc ICMP reply.

A screenshot of a computer

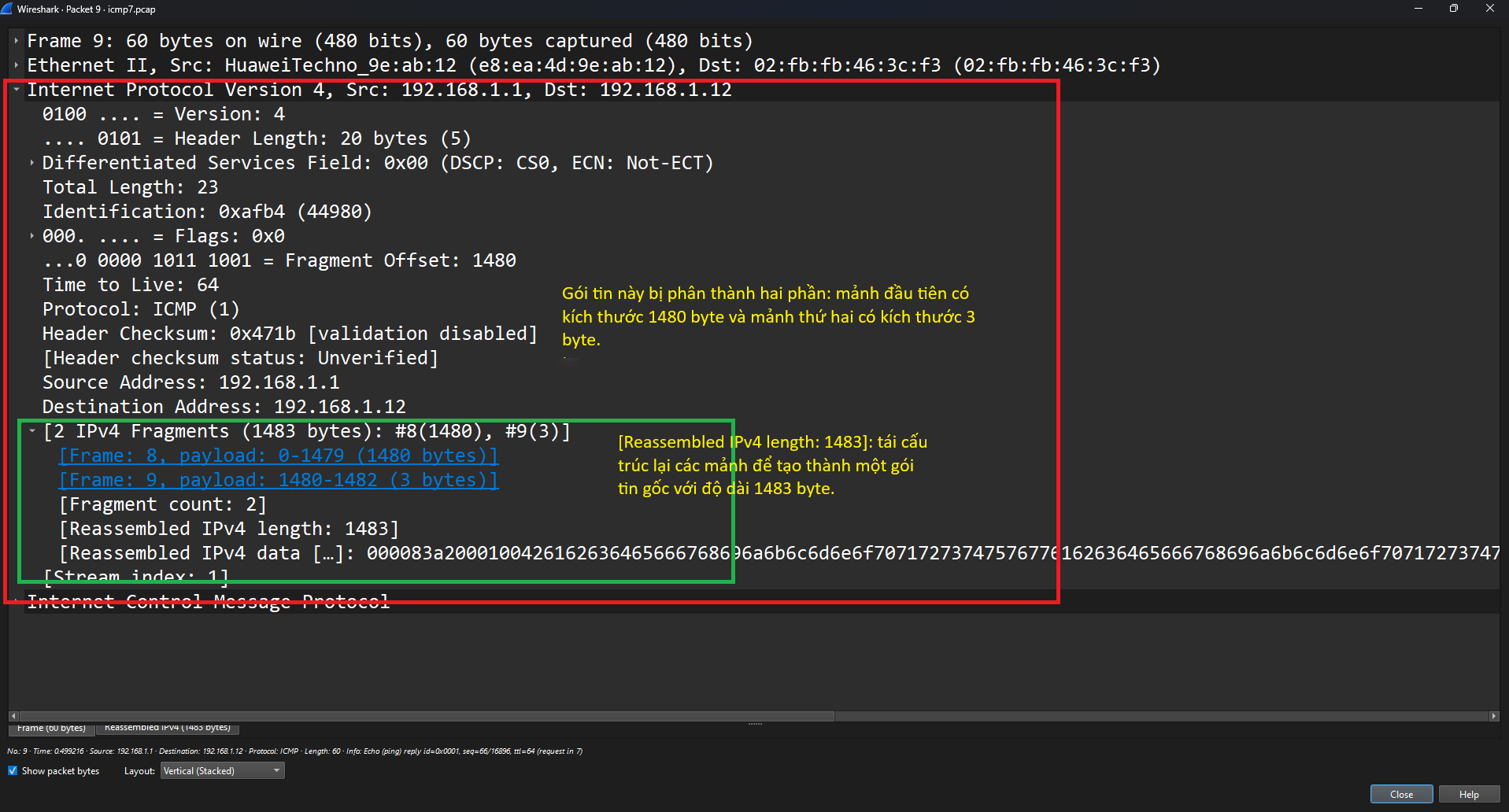
Description automatically generated

### 3.7. Ping và bắt gói tin

* + **ping -l 1475 192.168.1.1**
* Data trong ICMP payload là 1475 bytes bytes ở mỗi gói ICMP request hoặc ICMP reply.
* Gói tin ở câu 6 có tổng kích thước là: 1472(ICMP Payload) + 20(IP header) + 8(ICMP header) = 1500 bytes.
* Tương tự, gói tin ở câu 7 có tổng kích thước là 1475 + 20 + 8 = 1503 bytes.
* Điểm khác nhau giữa 2 gói tin này là:
  + Tổng kích thước gói tin ở câu 6 bằng với giá trị MTU mặc định (1500bytes). Do đó gói tin sẽ được truyền đi thành công mà không cần phân mảnh.
  + Tổng kích thước gói tin ở câu 7 (1503 bytes) lớn hơn MTU. Nên gói tin này sẽ phân mảnh khi truyền đi.

****

**Gói tin câu 6**

****

**Gói tin câu 7**

### 3.8. Ping và bắt gói tin

* Không bắt được bất kỳ gói tin nào khi gõ lệnh “**ping -f  -l 1475 192.168.1.1”** trên **terminal**. Lý do trong câu lệnh ping trên đã sử dụng cờ “-f” nghĩa là yêu cầu không phân mảnh gói tin. Kích thước của gói tin trong trường hợp này là 1475 bytes, điều này dẫn đến vượt quá kích thướng MTU. Do đó gói tin này sẽ bị loại bỏ.