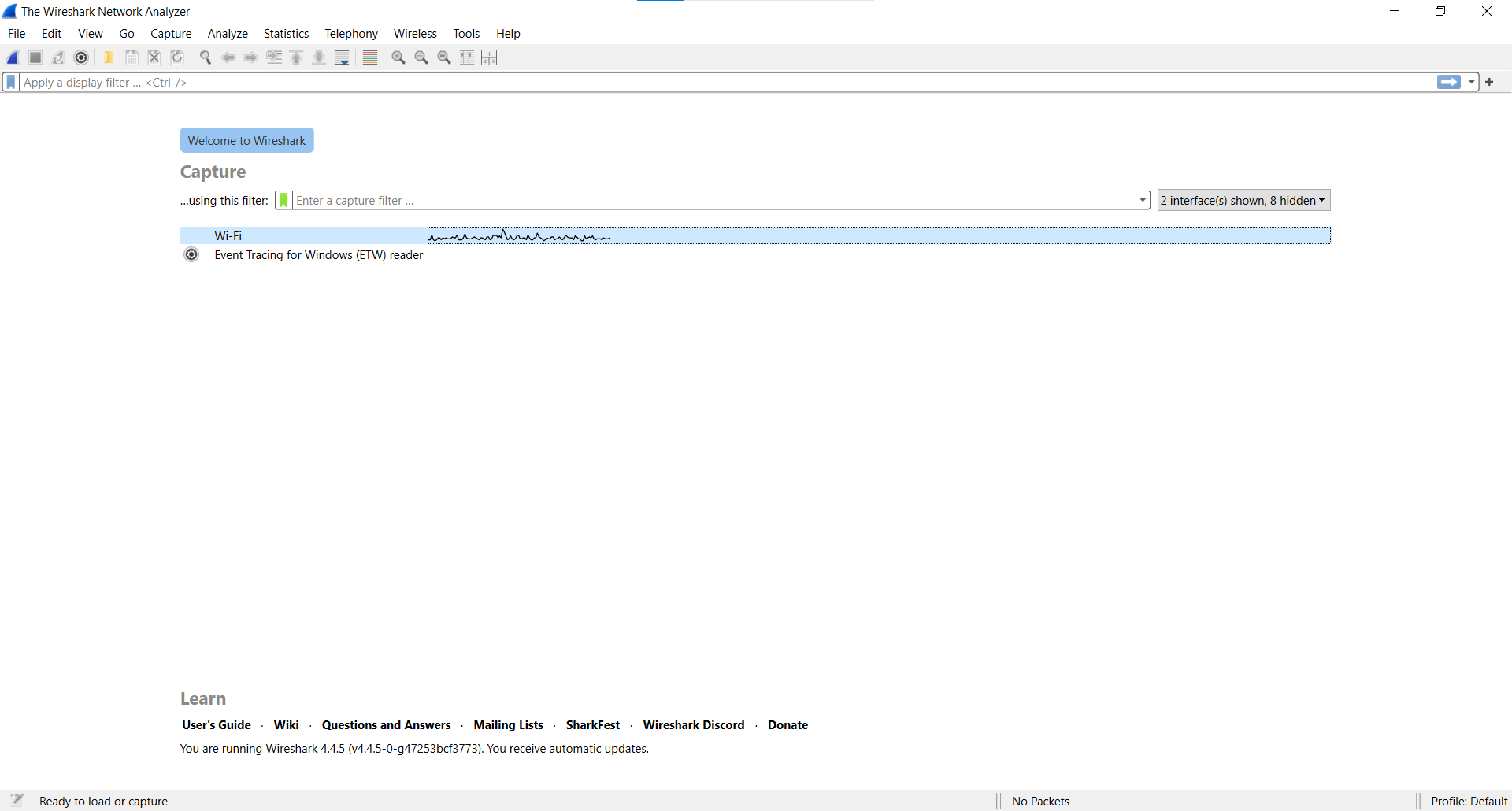
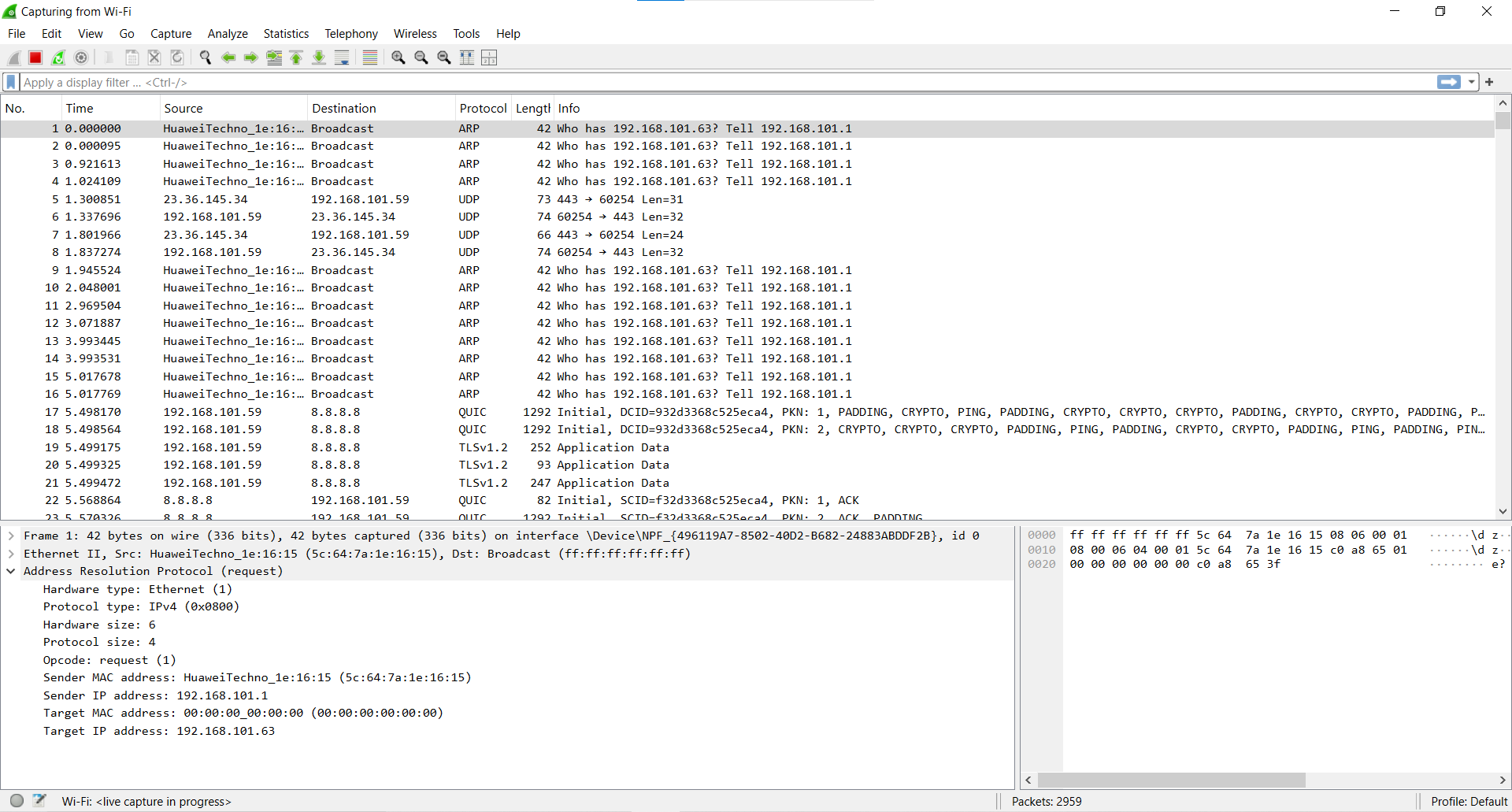
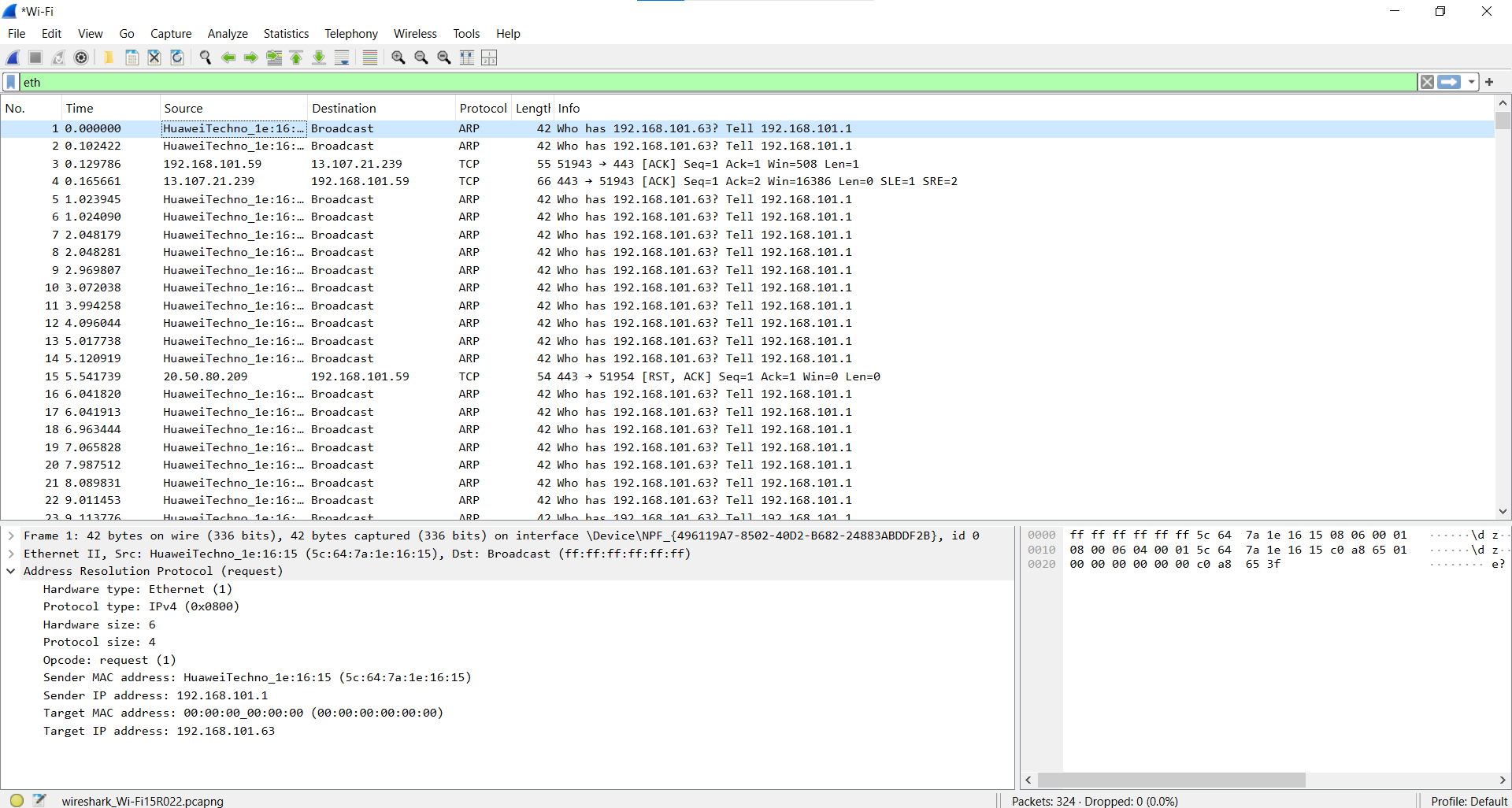
Bài thực hành 1: Bắt gói tin Ethernet bằng Wireshark để phân tích các trường dữ liệu.

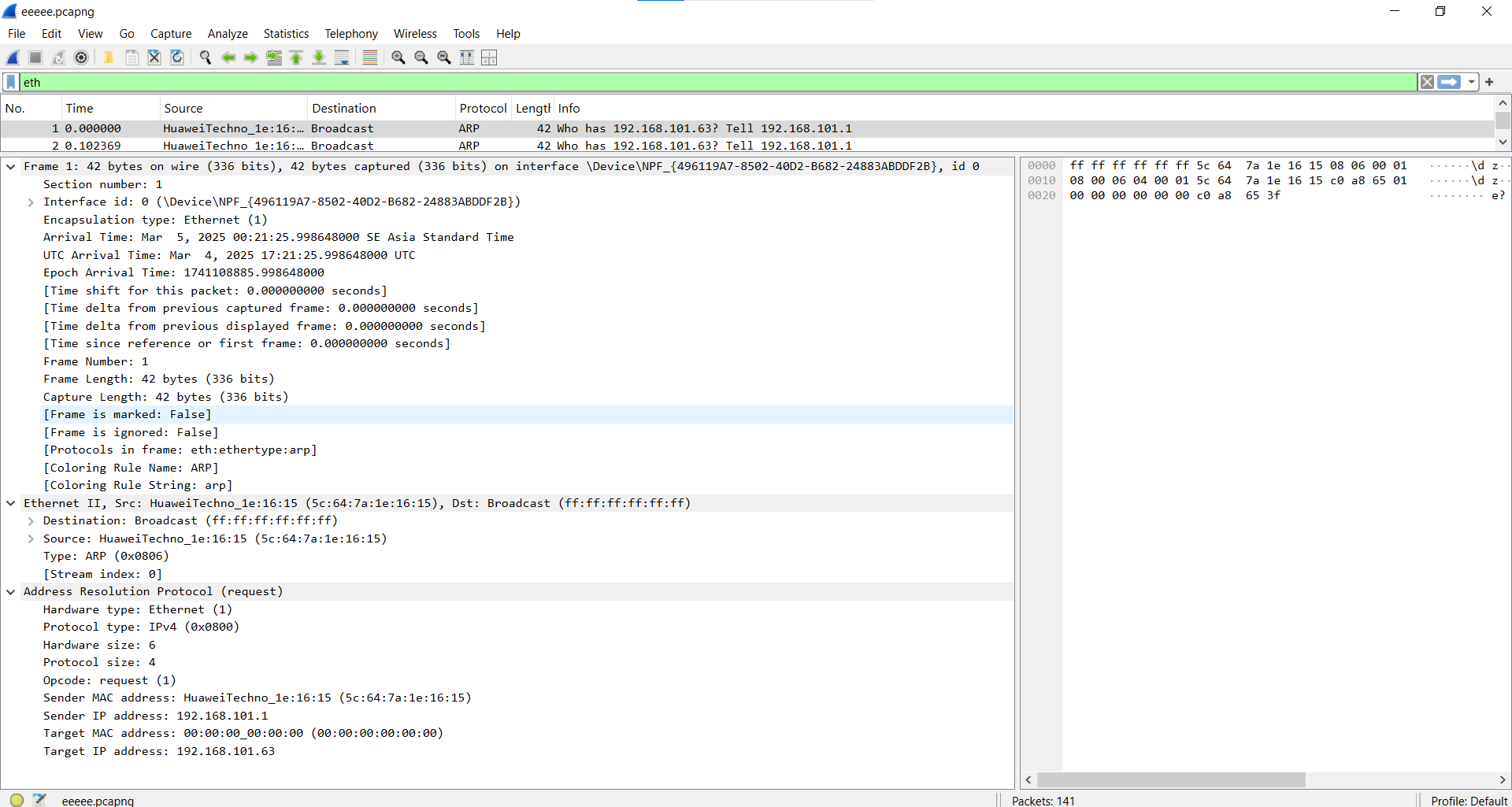
**Bước 1: Mở Wireshark và chọn giao diện mạng**1.Mở **Wireshark**  
2.Chọn **giao diện mạng** đang sử dụng (Ethernet hoặc Wi-Fi)

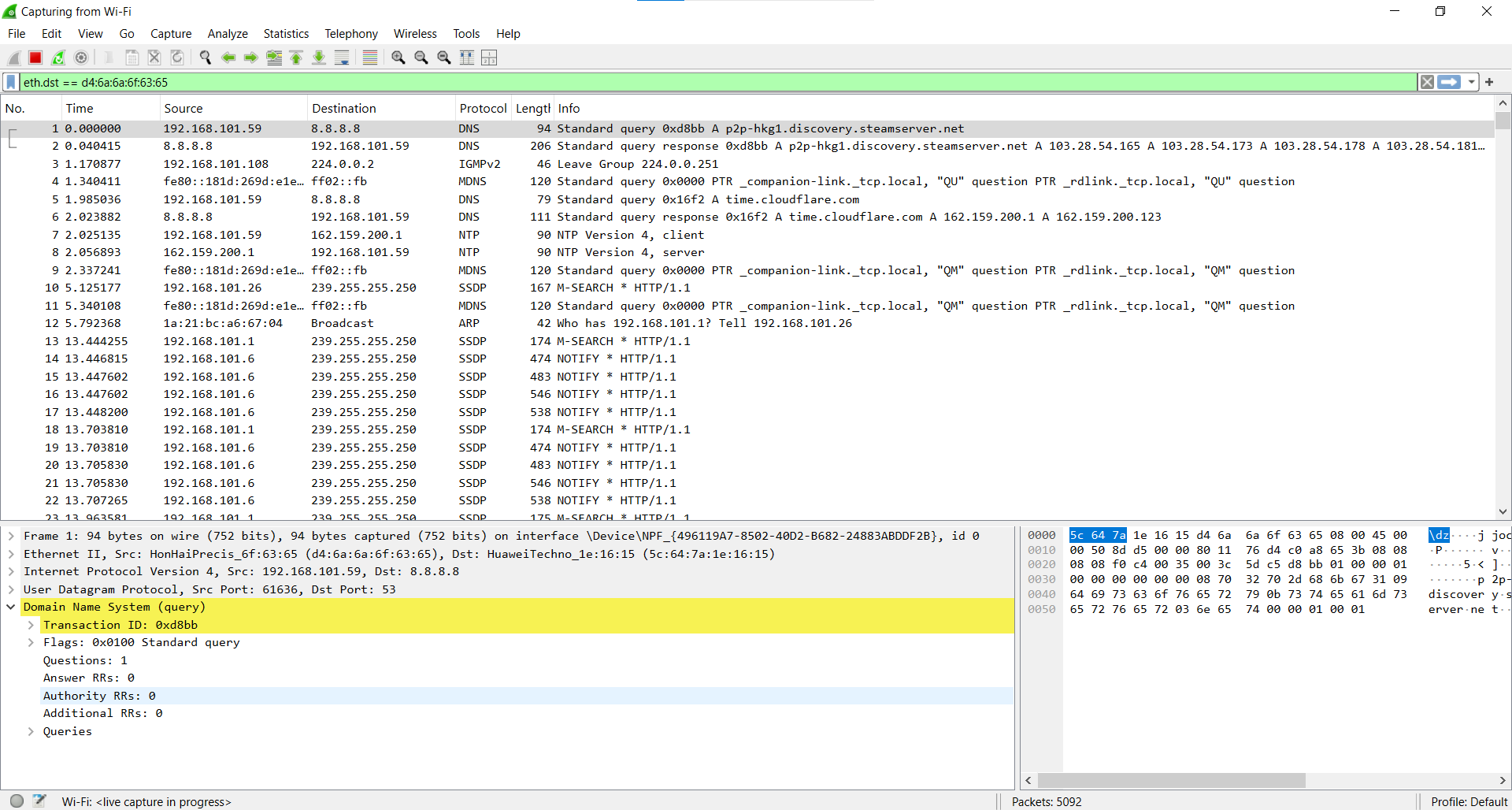
  
3.Nhấn **Start** để bắt gói tin

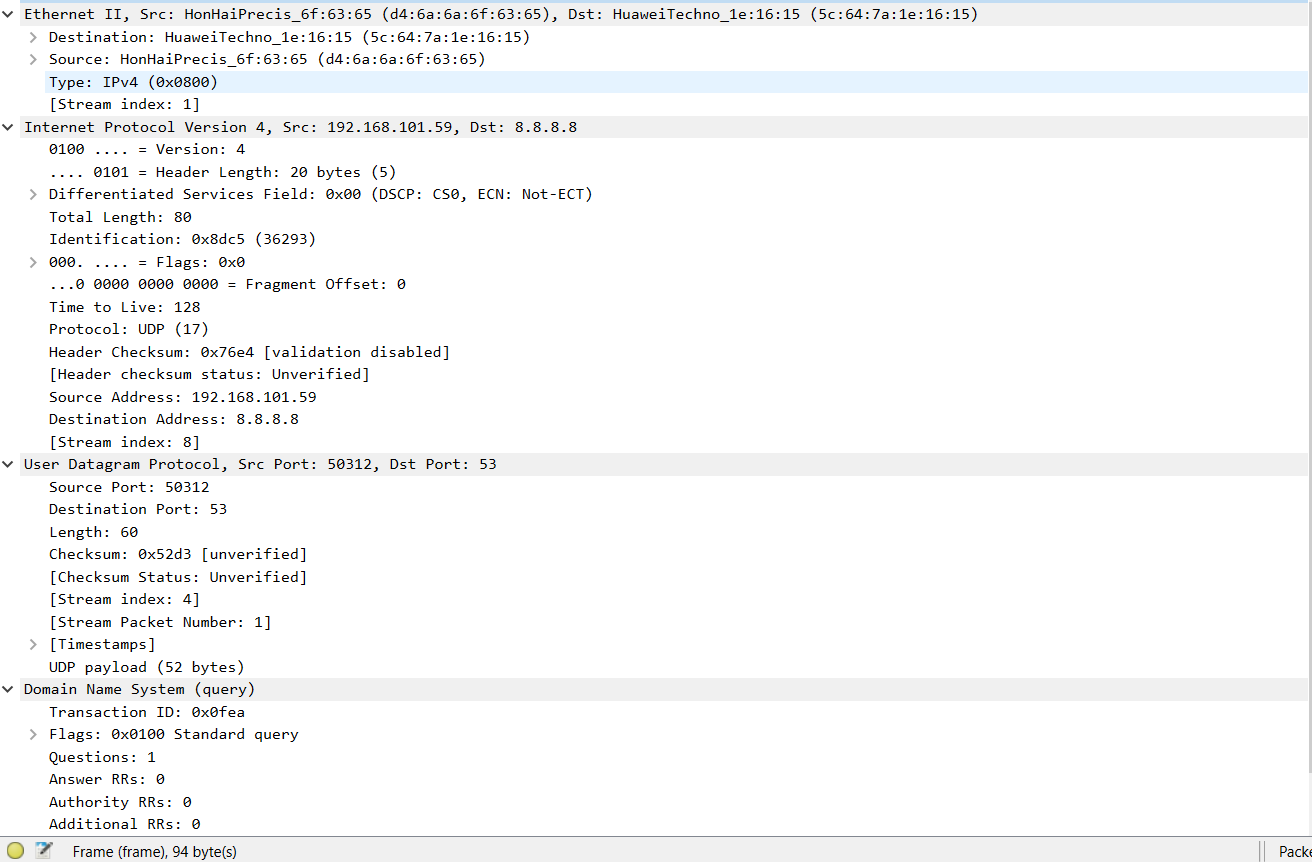


**Bước 2: Bắt gói tin Ethernet**Để lọc chỉ các gói tin Ethernet, nhập vào thanh Filter:  
**ethernet**

****

**  
eth.dst == xx:xx:xx:xx:xx:xx**để lọc theo địa chỉ MAC đích cụ thể





eth.dst == d4:6a:6a:6f:63:65

**Bước 3: Phân tích gói tin Ethernet**

**-Destination MAC Address** (6 bytes): địa chỉ MAC là 5c:64:7e:1c:16:15

**-Source MAC Address** (6 bytes): Địa chỉ MAC là d4:6a:6a:6f:63:65  
**-EtherType hoặc Length (2 bytes):**.

Ta thấy **EtherType = 0x0800**, có nghĩa là **IPv4** (theo bảng phân loại)

**Tổng kích thước gói tin (Frame Size)** = **94 bytes**

**MAC Header (Destination + Source + EtherType)** = **6 + 6 + 2 = 14 bytes**

**FCS (nếu có, thường 4 bytes, nhưng Wireshark có thể không hiển thị)**

**Tính Payload:**

Payload = Tổng kích thước - MAC Header - FCS  
**Payload = 94 - 14 - 4 = 76 bytes**

**-Payload (Data & Padding - 46 đến 1500 bytes)**: 76 bytes

-Trong Ethernet, nếu phần dữ liệu của gói tin (Payload) nhỏ hơn 46 bytes, trường Padding sẽ được thêm vào để đảm bảo kích thước tối thiểu của gói tin là 64 bytes.Tuy nhiên, tổng kích thước gói tin của bạn là **94 bytes**, nên Payload của nó đã lớn hơn 46 bytes, **không cần Padding**.

**Frame Check Sequence (CRC - 4 bytes)**: Gói tin **không có FCS**

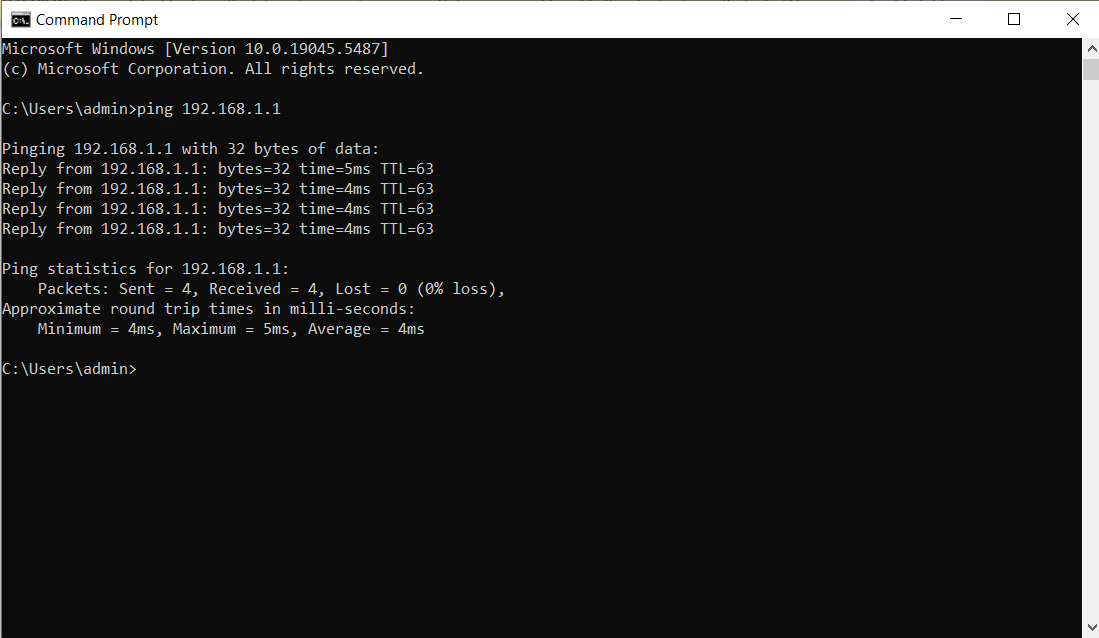
**Bước 4: Kiểm tra loại gói tin Ethernet**

Ảnh hiển thị **Ethernet II,** có nghĩa là **EtherType ≥ 1536 ,**

**0x0800**→ IPv4

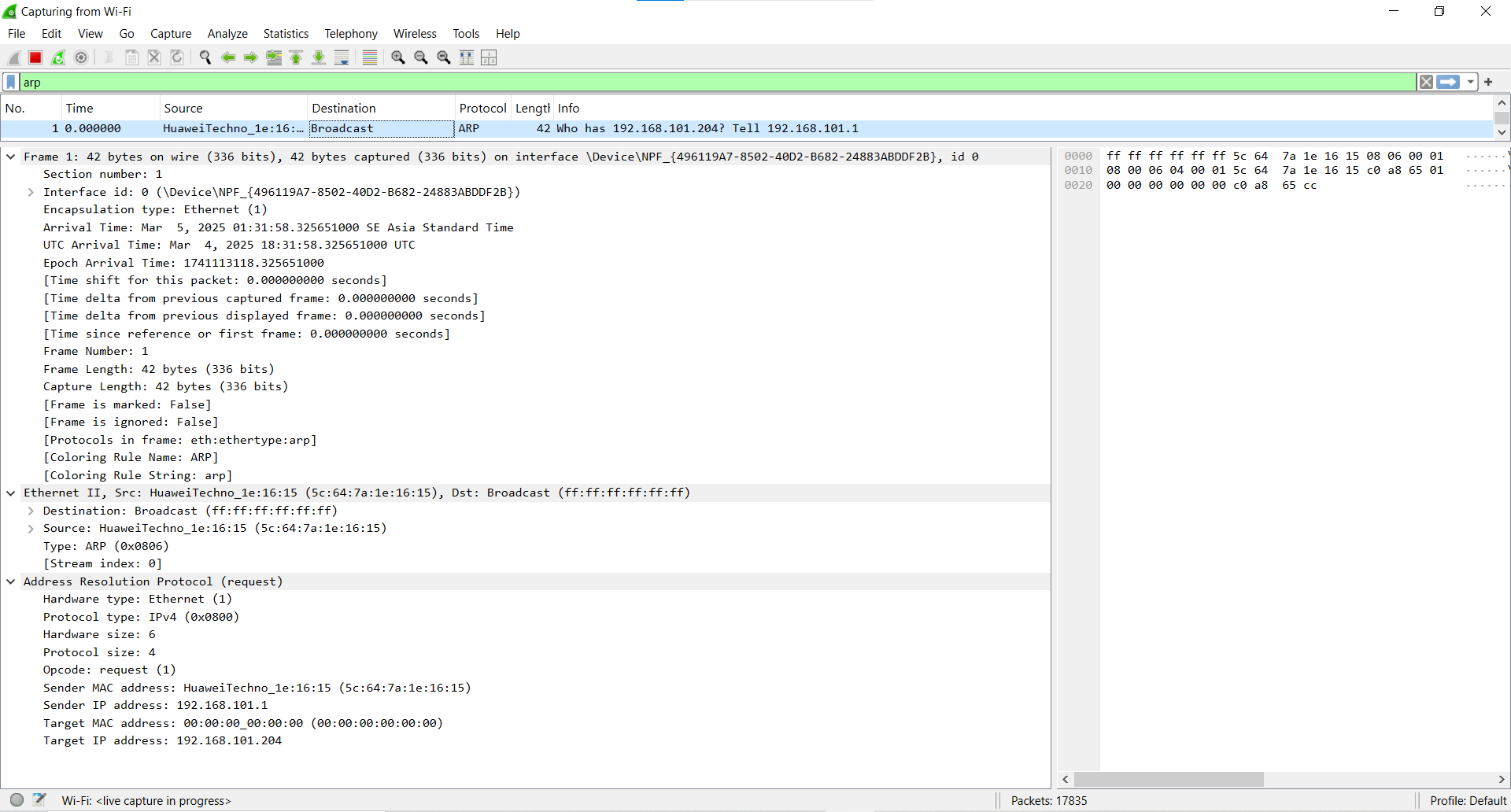
**Bài thực hành 2**

1. Thực hiện lại ping



2)Thực hiện bắt gói ARP

\* Chọn frame đầu tiên của giao thức ARP hiển thị ở cửa sổ Packet List



- **Địa chỉ đích:**

**Địa chỉ MAC:** ff:ff:ff:ff:ff:ff

**Nhà sản xuất NIC:** Không có vì đây là địa chỉ **broadcast**

**Số sê-ri NIC:** Không có vì đây là địa chỉ **broadcast**

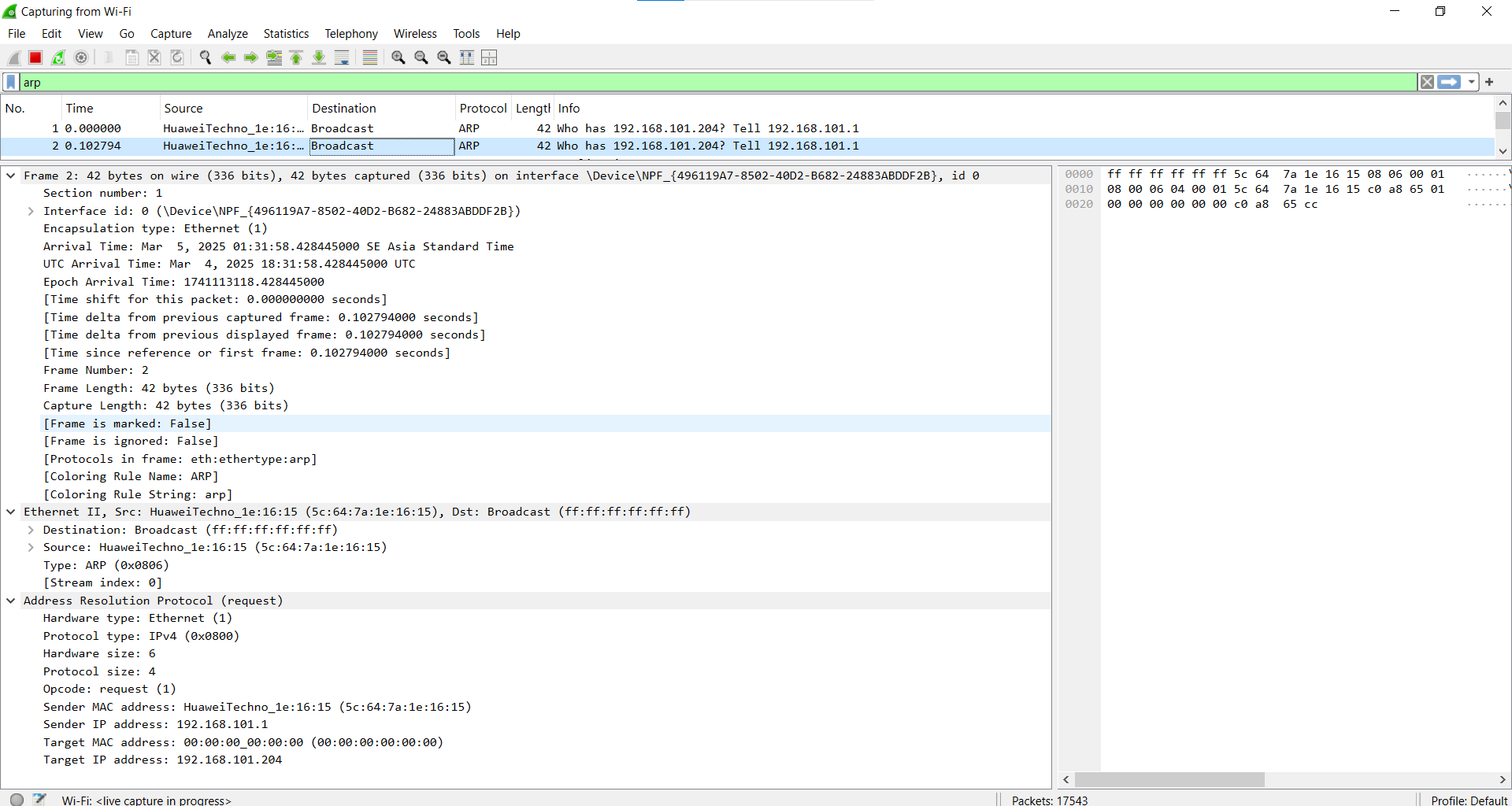
- **Địa chỉ nguồn:**

**Địa chỉ MAC:** 5c:64:7a:1e:16;15

**Nhà sản xuất NIC:** Huawei Technologies Co., Ltd.

**Số sê-ri NIC:** 1e:16:15

\* Chọn frame thứ hai của giao thức ARP hiển thị ở cửa sổ Packet List



Chọn frame thứ hai của giao thức ARP hiển thị ở cửa sổ Packet List, hãy trả lời các câu hỏi sau:  
Địa chỉ đích:  
MAC address: 00:00:00:00:00:00

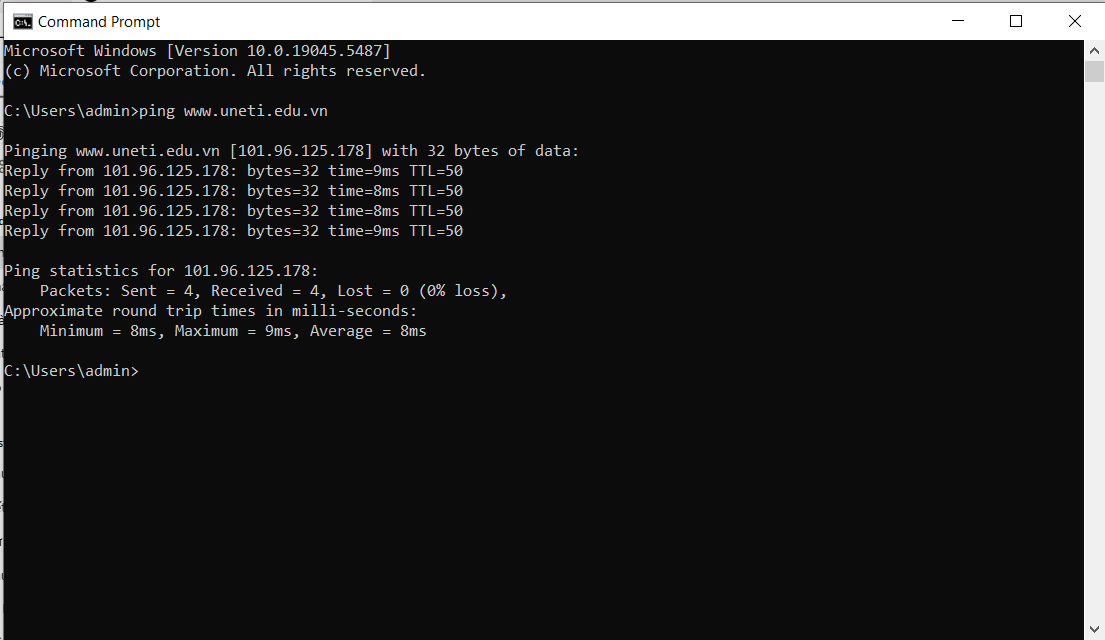
NIC manufacturer: Không có

NIC serial number: Không có   
Địa chỉ nguồn:  
MAC address: 5c:64:7e:1e:16:15

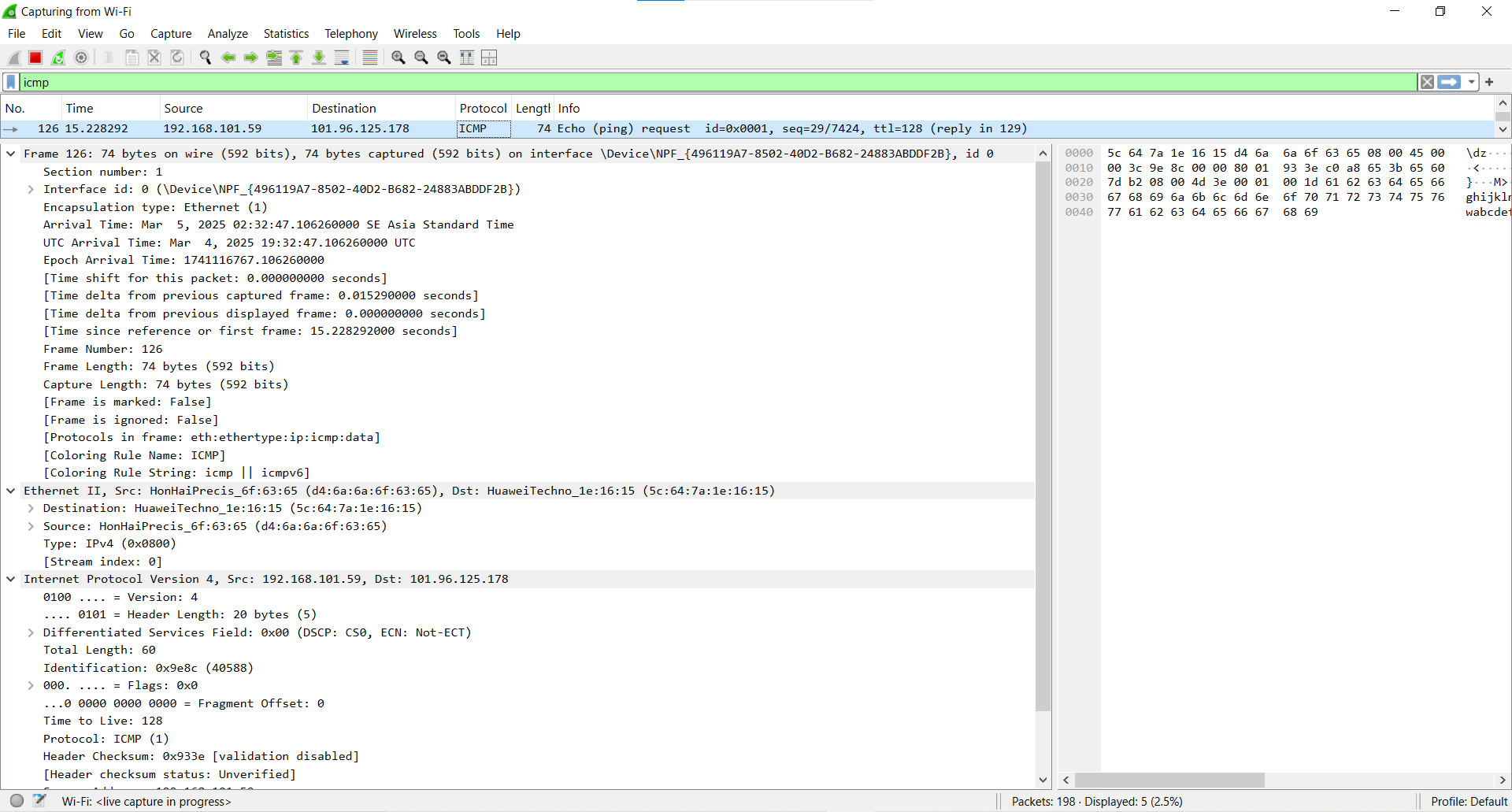
NIC manufacturer: Huawei Technologies Co., Ltd.  
NIC serial number: 1e:16:15

**Bài tập:** Thực hiện lệnh ping đến một server ngoài Internet đồng thời bắt gói (chẳng hạn www.uneti.edu.vn). Dựa vào việc thu thập thông tin trong các gói tin bắt được có thể biết được địa chỉ MAC của server này không? Tại sao?

**Thực hiện lệnh ping đến www.uneti.edu.vn**



**Lọc các gói tin ICMP trong Wireshark.**



**\*** Dựa vào gói tin 126, ta thấy:

**Độ dài gói tin:** 74 bytes (592 bits)

Địa chỉ MAC nguồn: d4:6a:6a:6f:63:65 (HonHaiPrecision - thiết bị gửi)

Địa chỉ MAC đích: 5c:64:7a:1e:16:15 (HuaweiTechno - router/gateway)

Địa chỉ IP nguồn: 192.168.101.59 (máy tính của bạn)

Địa chỉ IP đích: 101.96.125.178 (địa chỉ IP của www.uneti.edu.vn)

**Phiên bản IP:** IPv4

**\* Không thể biết được địa chỉ MAC của server từ gói tin bắt được.**

**Lý do:**

**- Địa chỉ MAC chỉ có giá trị trong cùng một mạng LAN**

Gói tin trong hình là một gói ICMP (ping) từ máy bạn (192.168.101.59) đến server (101.96.125.178).

Địa chỉ MAC trong gói tin chỉ thể hiện **máy bạn và router/gateway gần nhất** (chứ không phải server).

Khi gói tin rời khỏi mạng LAN, router sẽ thay đổi địa chỉ MAC của nó trước khi gửi đi trên internet.

**- Gói tin truyền qua nhiều router, mỗi router thay đổi MAC**

Khi đi qua internet, gói tin phải qua nhiều router trung gian.

Mỗi lần gói tin đi qua router, địa chỉ MAC nguồn và đích **bị thay đổi** để phù hợp với mạng LAN của router đó.

Vì vậy, bạn **chỉ thấy địa chỉ MAC của router gần nhất,** không phải của server đích.