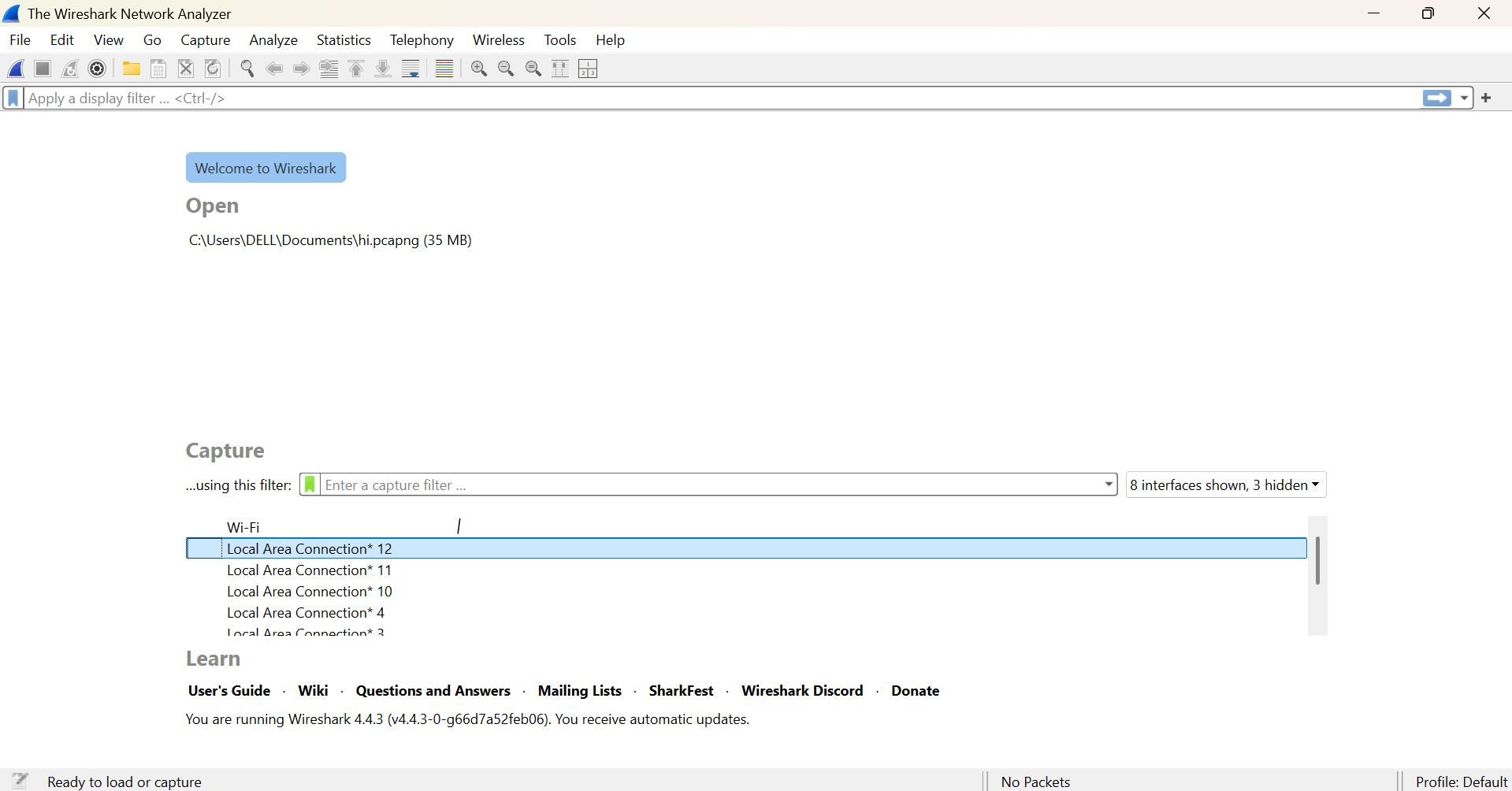
**Hồ Thị Minh Hằng – 22174600024 – DHKL16A2HN**

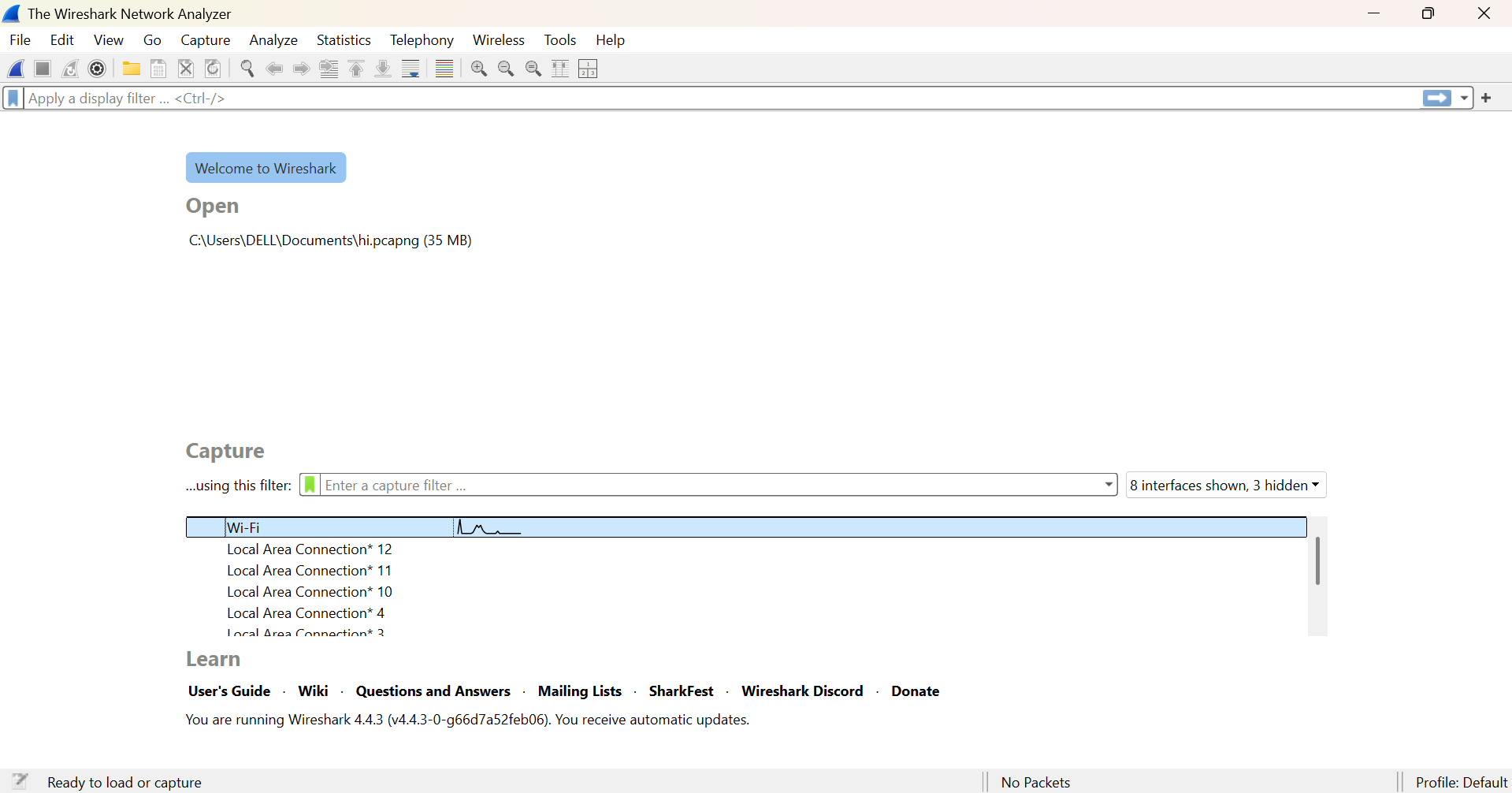
**Bài thực hành 1: Bắt gói tin Ethernet bằng Wireshark để phân tích các trường dữ liệu.**

**Bước 1: Mở Wireshark và chọn giao diện mạng**

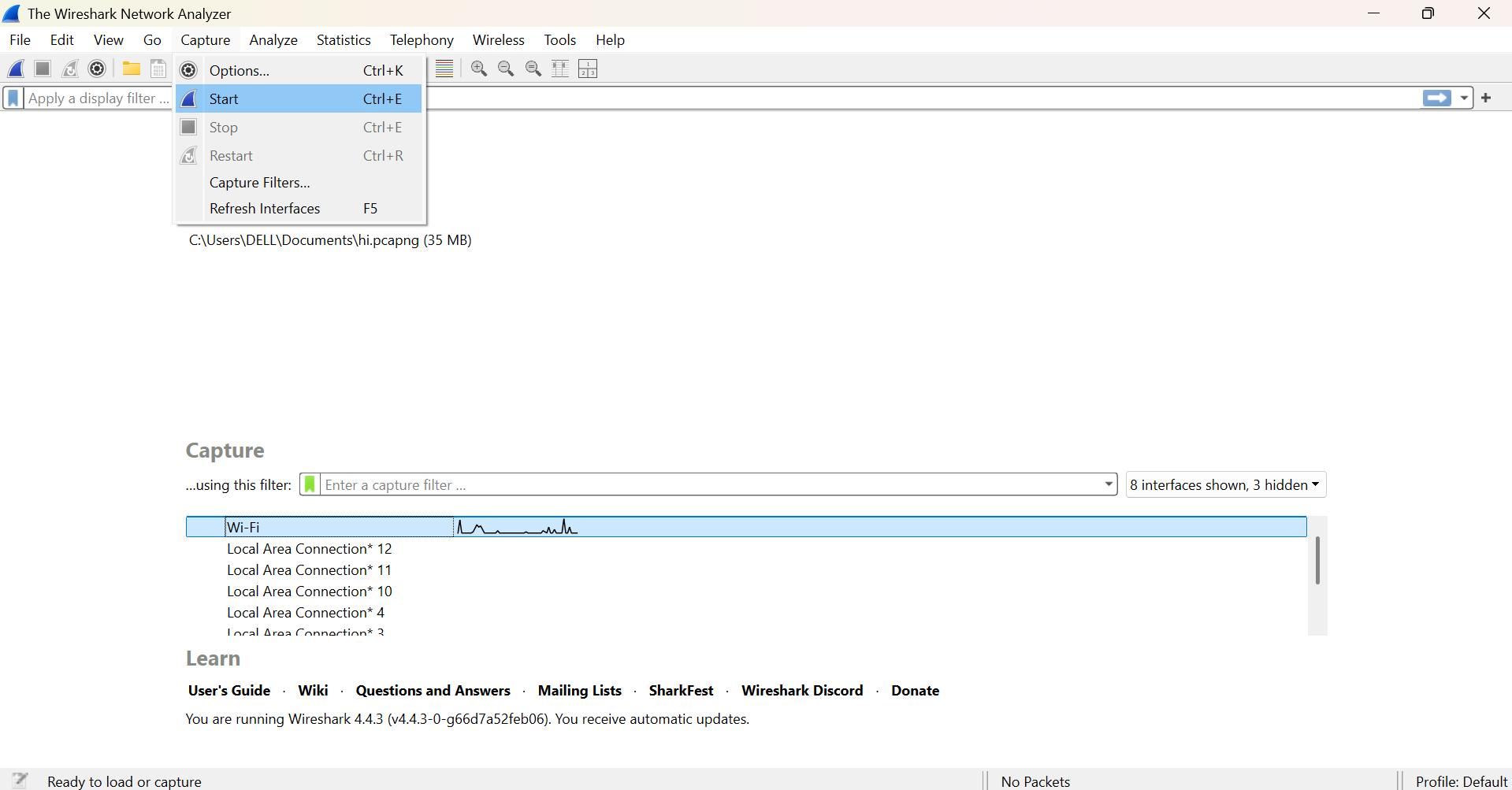
1. **Mở Wireshark**



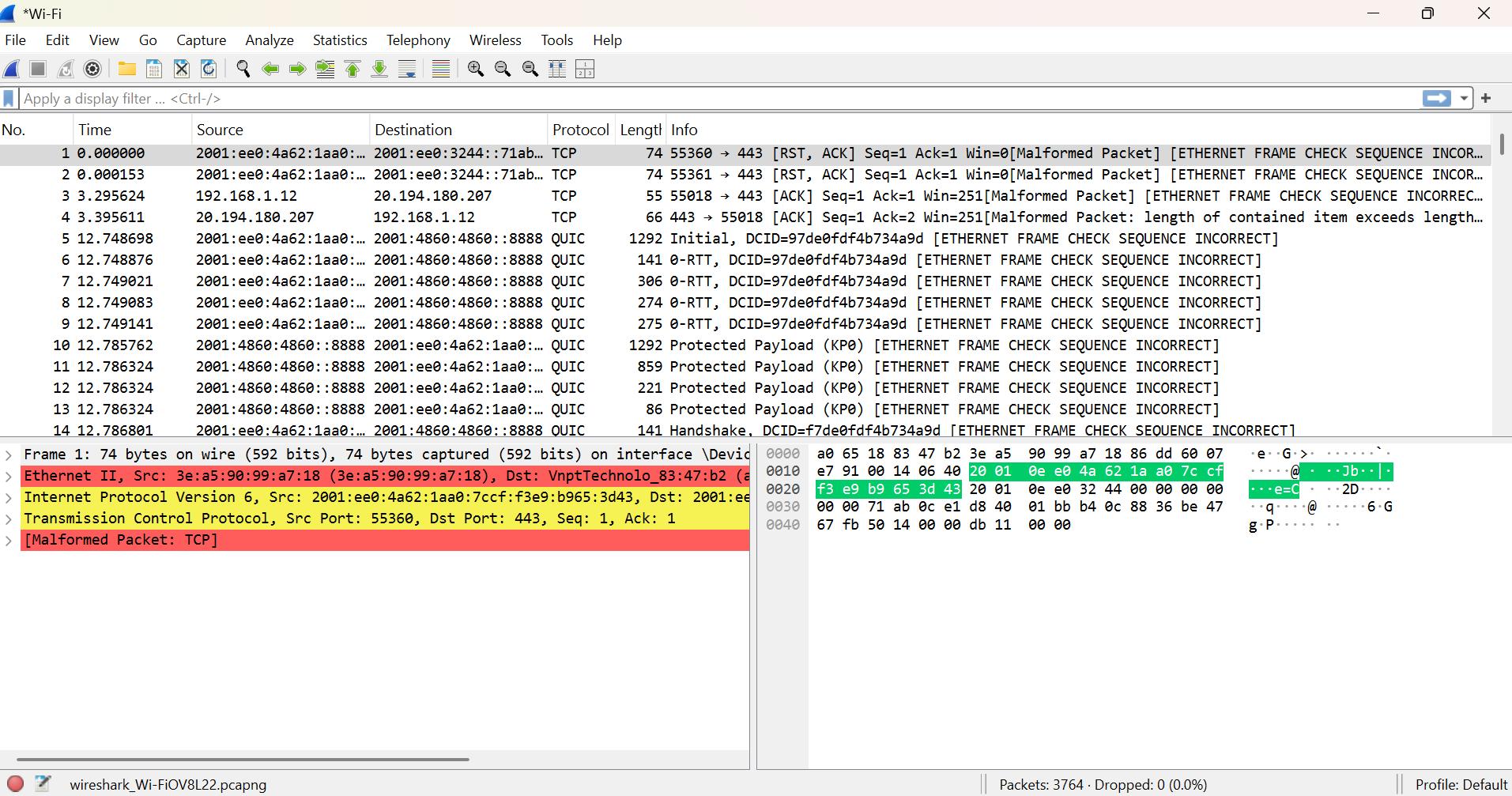
1. **Chọn giao diện mạng đang sử dụng. Em chọn Wifi**



1. **Nhấn Start để bắt gói tin.**



**Sau khi nhấn start, ta được các gói tin:**

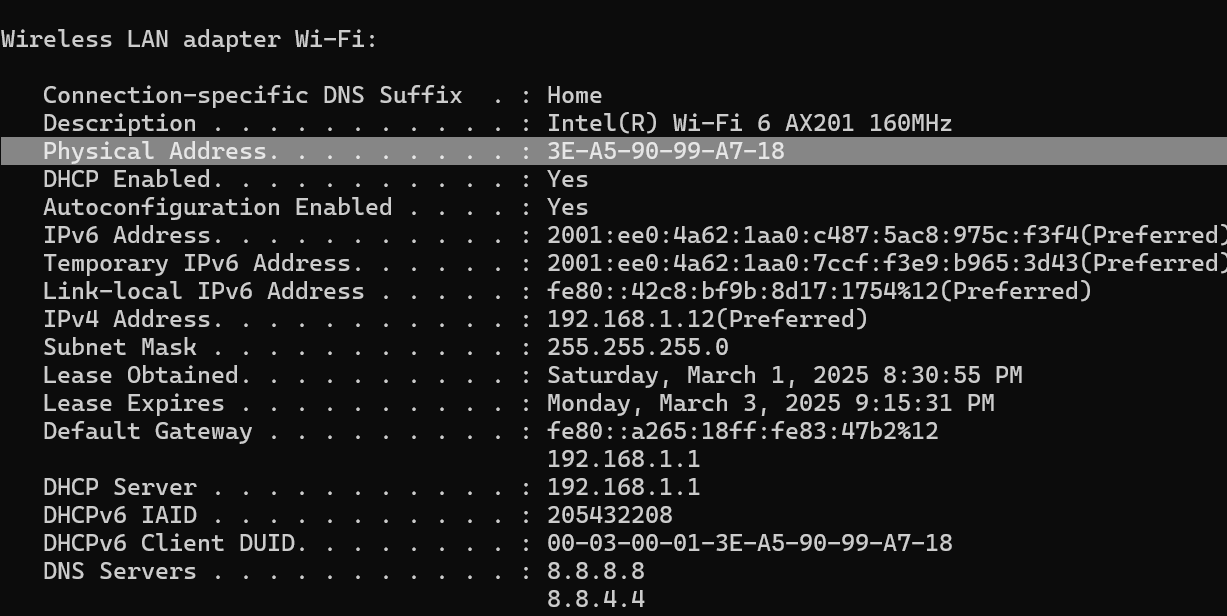


**Bước 2: Bắt gói tin Ethernet**

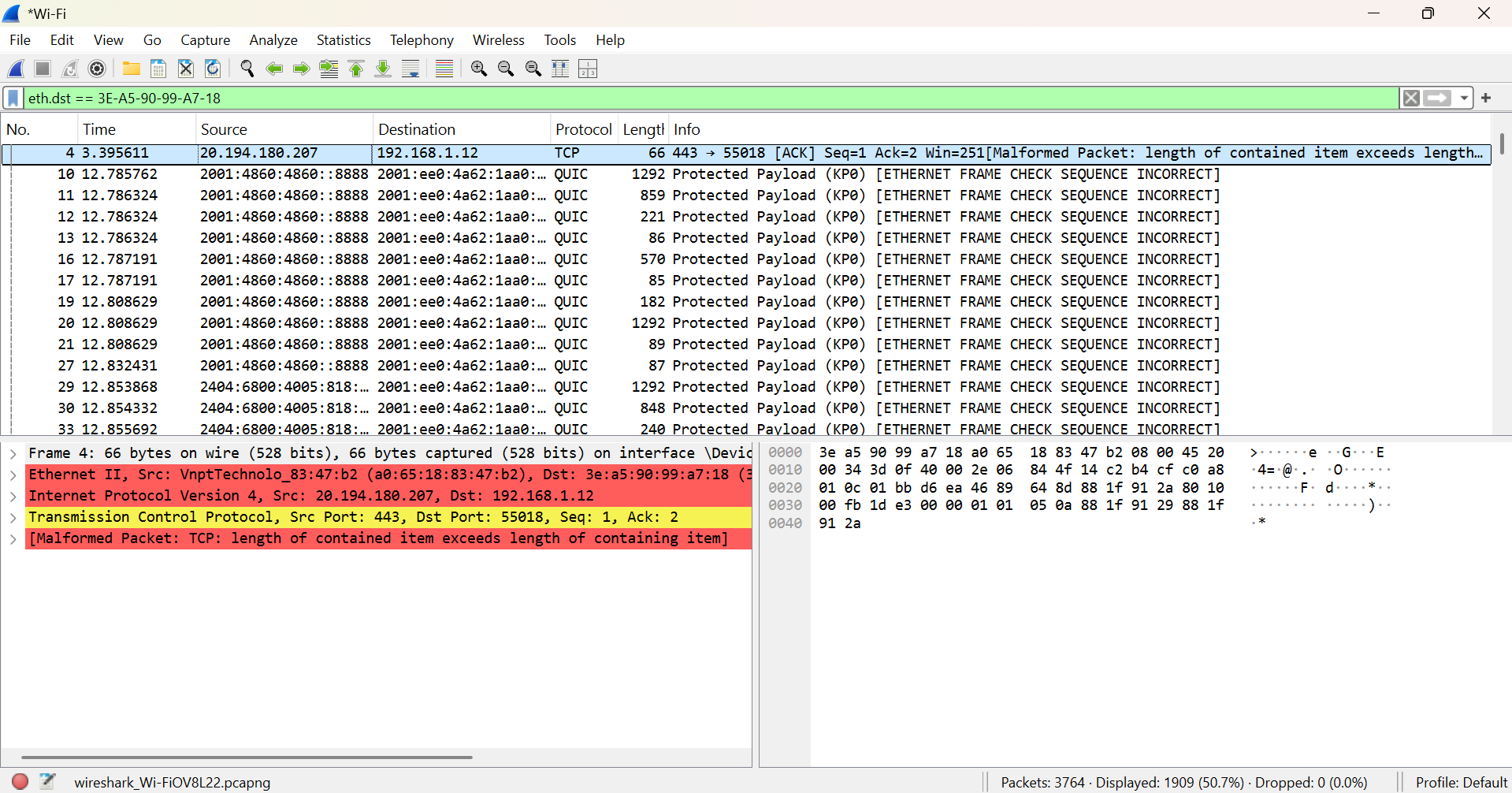
Để lọc chỉ các gói tin Ethernet, nhập vào thanh Filter: eth.dst == xx:xx:xx:xx:xx:xx (Địa chỉ mac cụ thể)

Địa chỉ mac của em là: **3E-A5-90-99-A7-18**

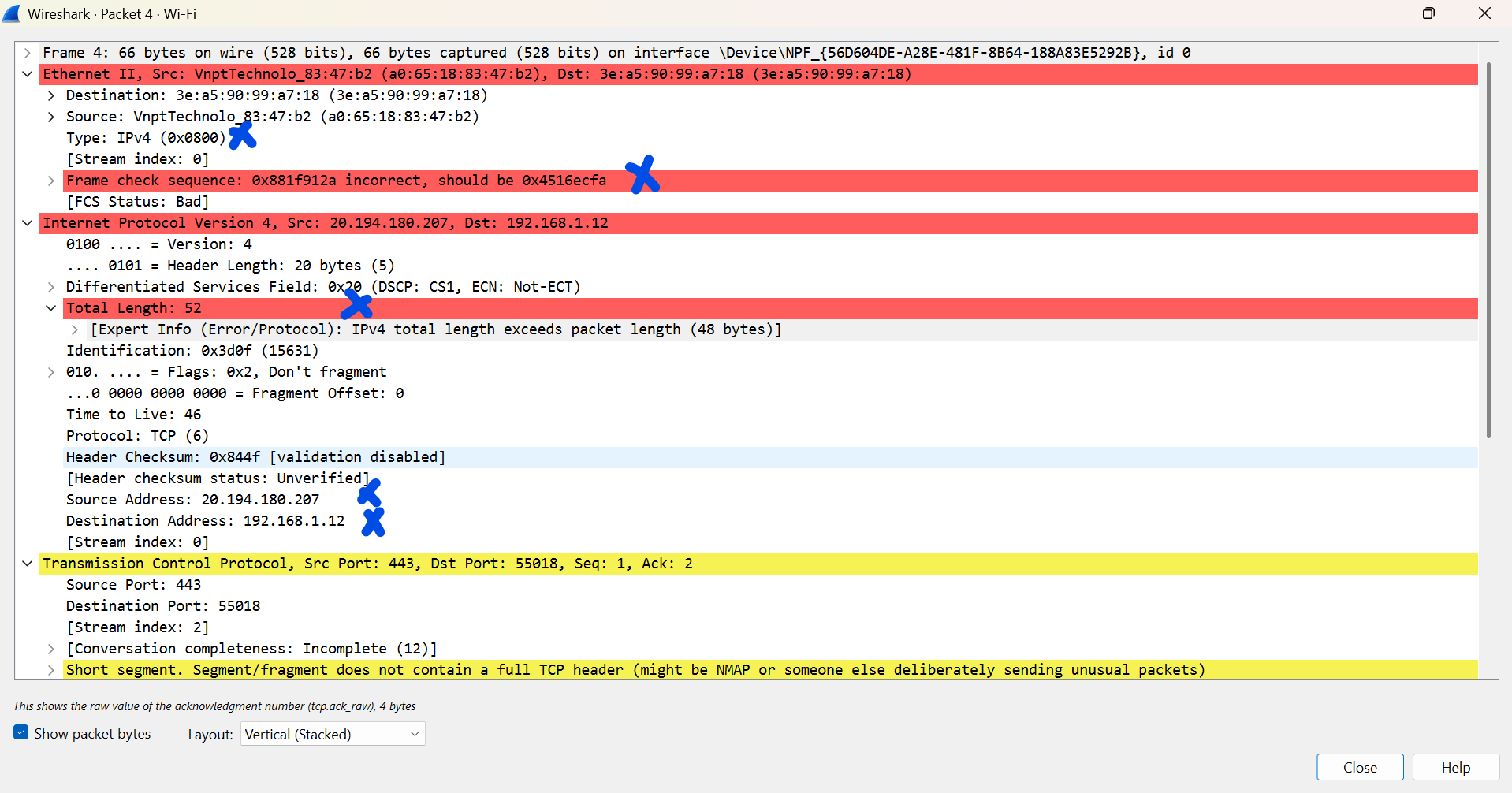
Vậy em sẽ nhập vào thanh Filter là: **eth.dst == 3E-A5-90-99-A7-18**



**Quan sát danh sách gói tin được bắt:**



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



* **Destination MAC Address:** 192.168.1.12
* **Source MAC Address:** 20.194.180.207
* **EtherType:** IPv4 (0x0800)
* **Payload:** 52 bytes
* **Frame Check Sequence:** 0x881f912a incorrect, should be 0x4516ecfa

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

Ta thấy EtherType ≥ 1536 (0x0600), đây là Ethernet II, với loại phổ biến: IPv4 (0x0800)



Trả lời các câu hỏi:

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

- Địa chỉ MAC nguồn trong gói tin của em là: 20.194.180.207

- Địa chỉ MAC đích trong gói tin của em là: 192.168.1.12

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

- Gói tin này được sử dụng giao thức IPv4 ở tầng trên

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

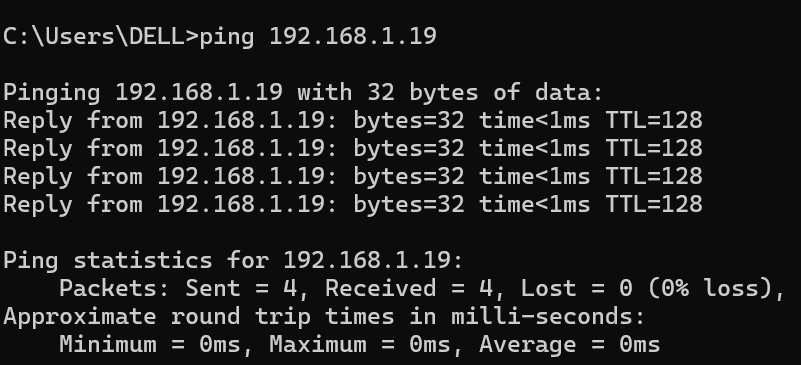
- Không có trường Padding vì Kích thước gói tin và các header đều hợp lý nên không cần Padding.

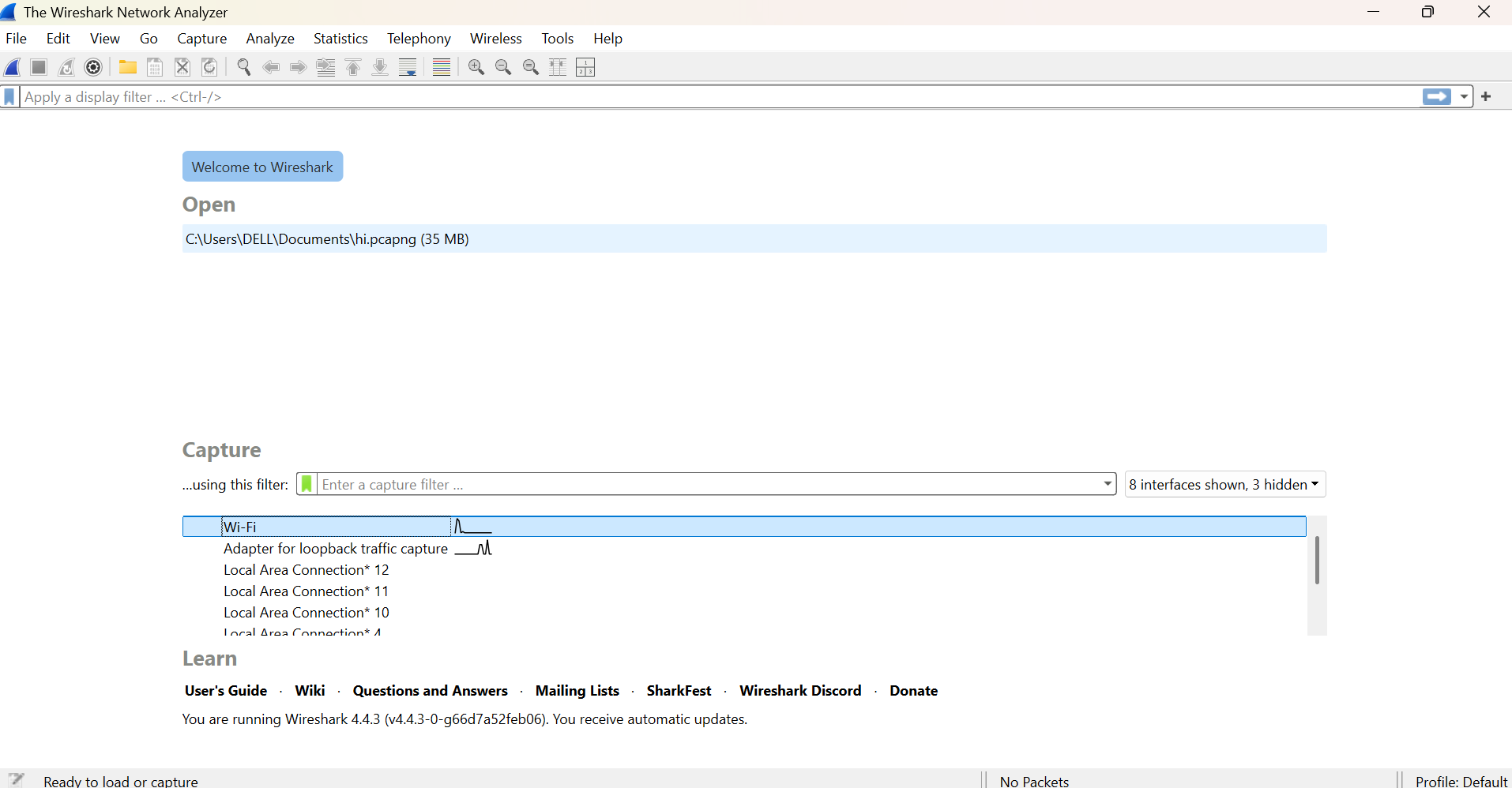
Nếu có thì Padding có tác dụng để đảm bảo kích thước tối thiểu của Ethernet Frame là 64 bytes, giúp truyền dữ liệu ổn định và phát hiện lỗi tốt hơn. Padding chỉ là các byte phụ, không ảnh hưởng tới dữ liệu thật và sẽ bị loại bỏ ở thiết bị nhận.

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

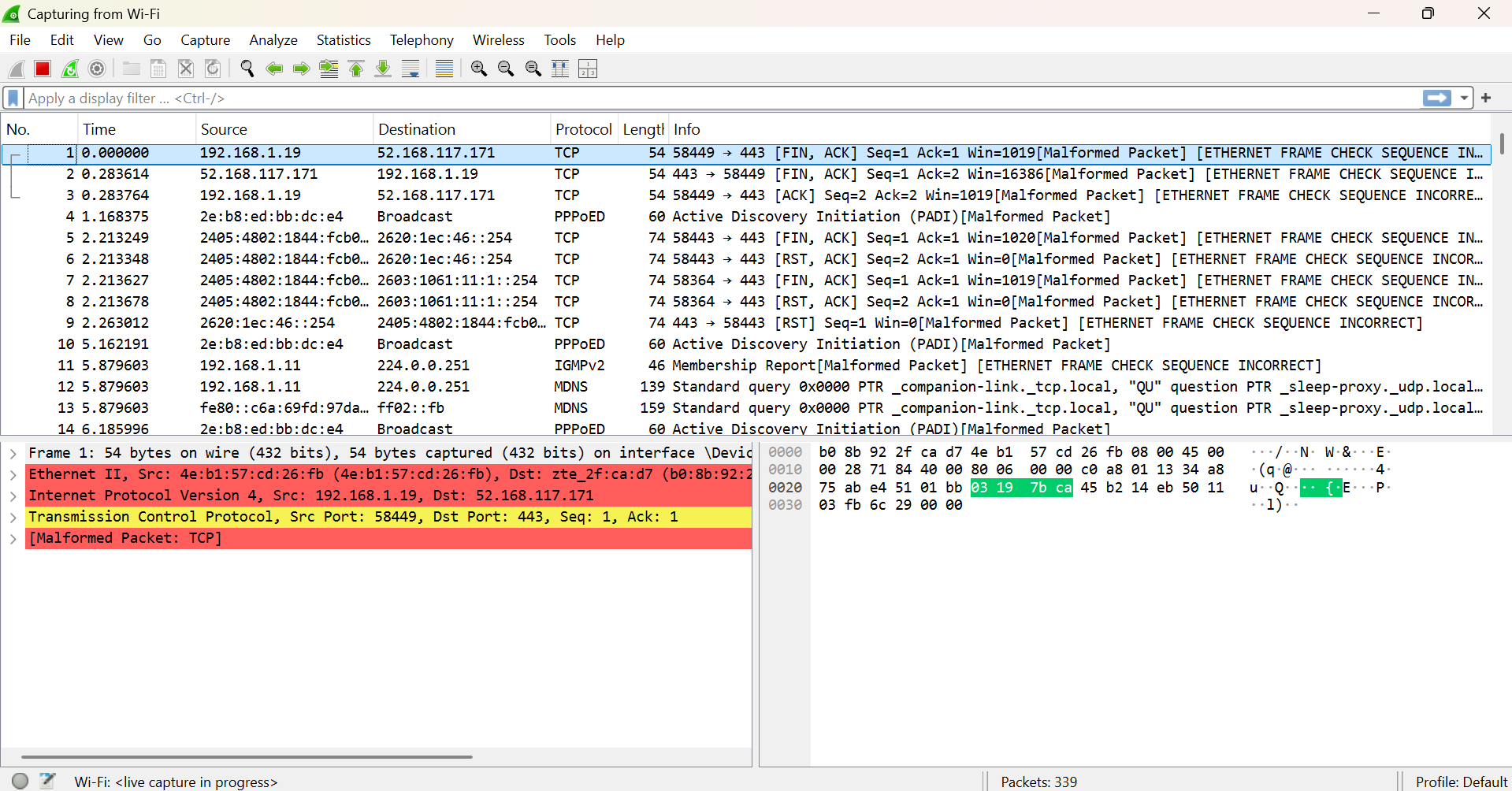
- Frame Check Sequence: 0x881f912a incorrect, should be 0x4516ecfa cho thấy mã CRC trong gói tin bị sai. should be 0x4516ecfa: Đây là mã CRC đúng mà Wireshark tính ra dựa trên dữ liệu thực tế của gói tin. Vì vậy CRC của gói tin không hợp lệ.

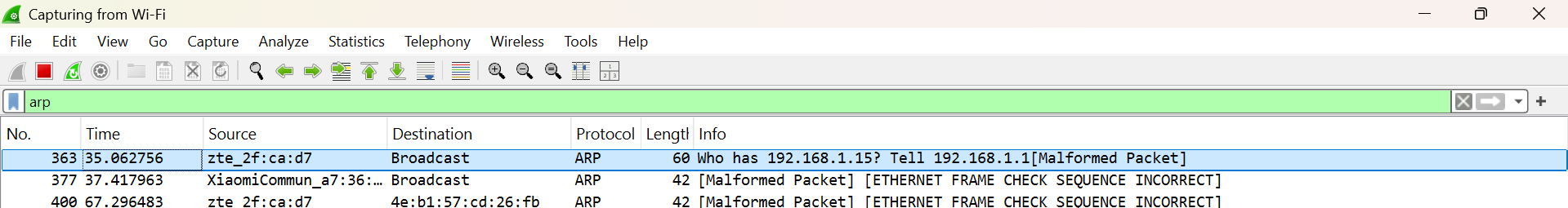
**Bài thực hành 2: Thực hiện lệnh ping và bắt gói lại**

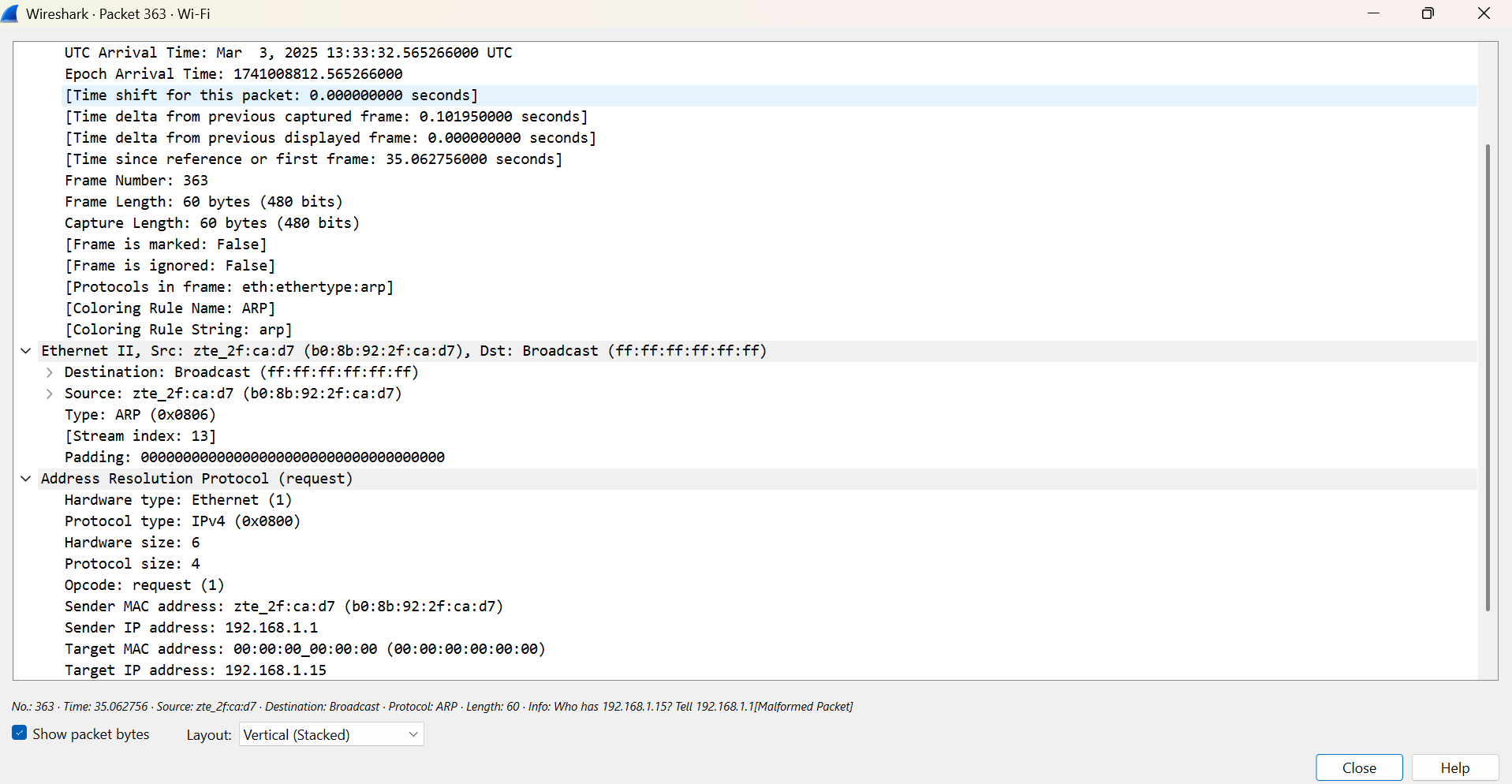




Chọn frame đầu tiên của giao thức ARP, quan sát chi tiết nội dung frame và trả lời các câu hỏi:







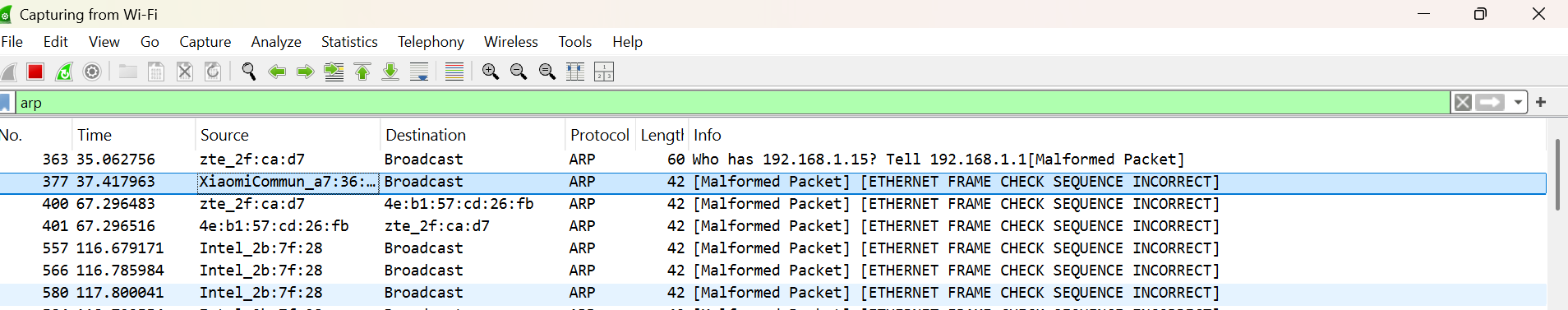
**Địa chỉ đích:**

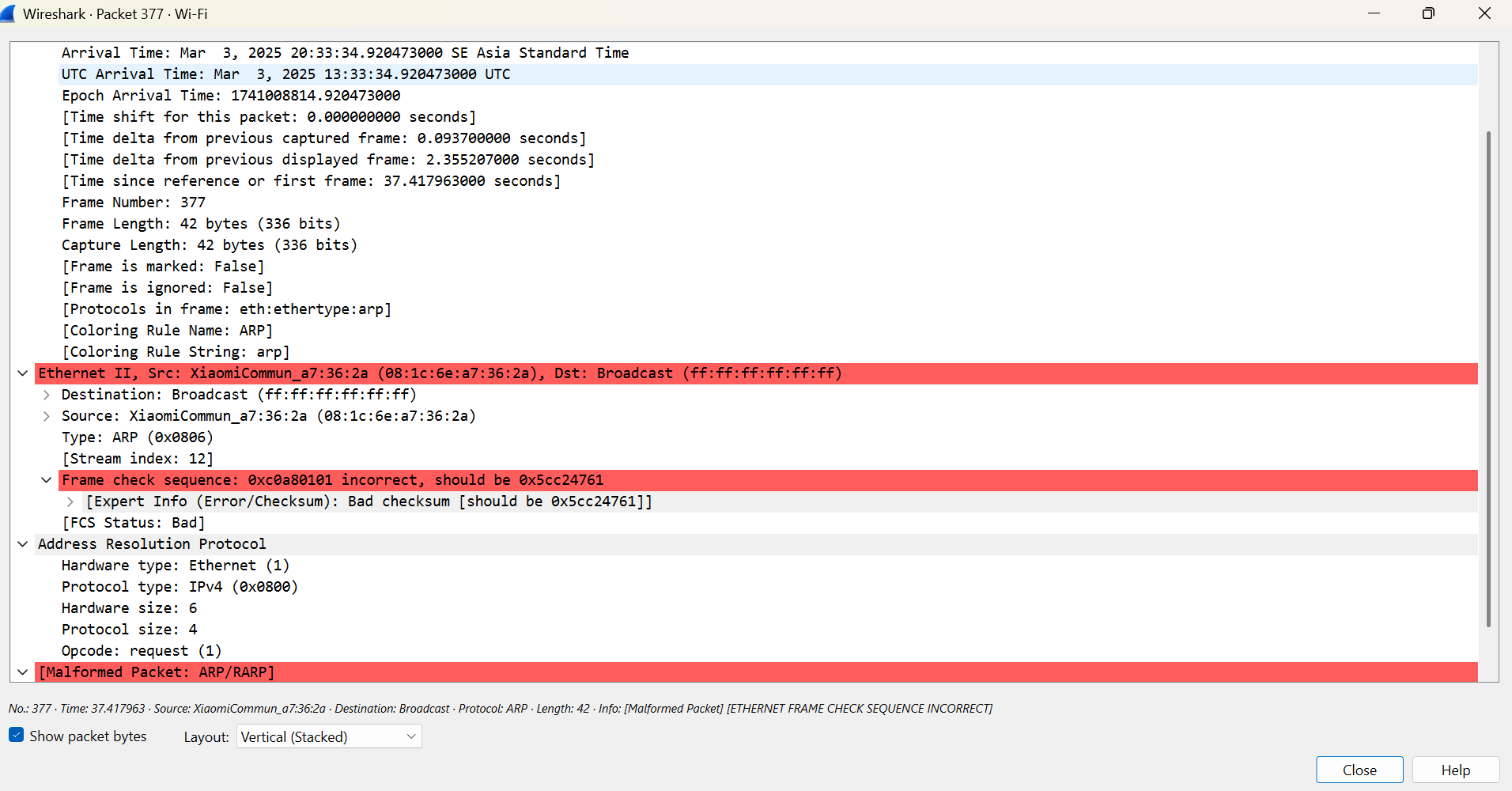
* **MAC address:** ff:ff:ff:ff:ff:ff (Broadcast — gửi đến tất cả các thiết bị trong mạng cục bộ).
* **NIC manufacturer:** Không áp dụng (do là địa chỉ broadcast).
* **NIC serial number:** Không áp dụng (do là địa chỉ broadcast).

**Địa chỉ nguồn:**

* **MAC address:** b0:8b:92:2f:ca:d7
* **NIC manufacturer:** Phần đầu (b0:8b:92) có thể dùng để xác định nhà sản xuất.
* **NIC serial number:** 2f:ca:d7 (phần còn lại của MAC address).

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





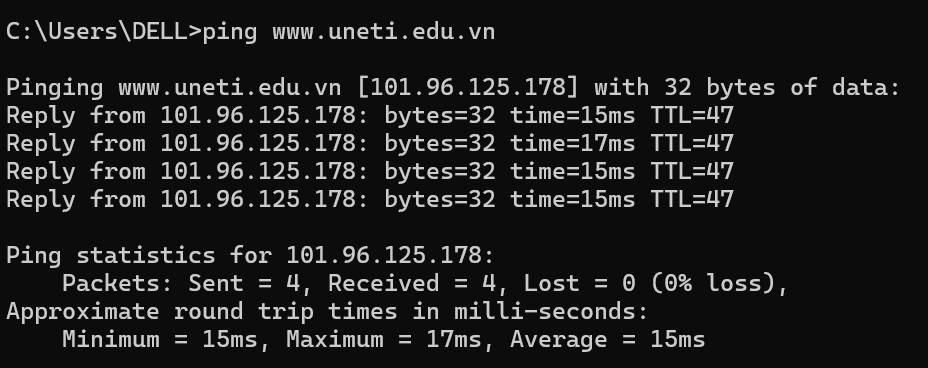
**Địa chỉ đích:**

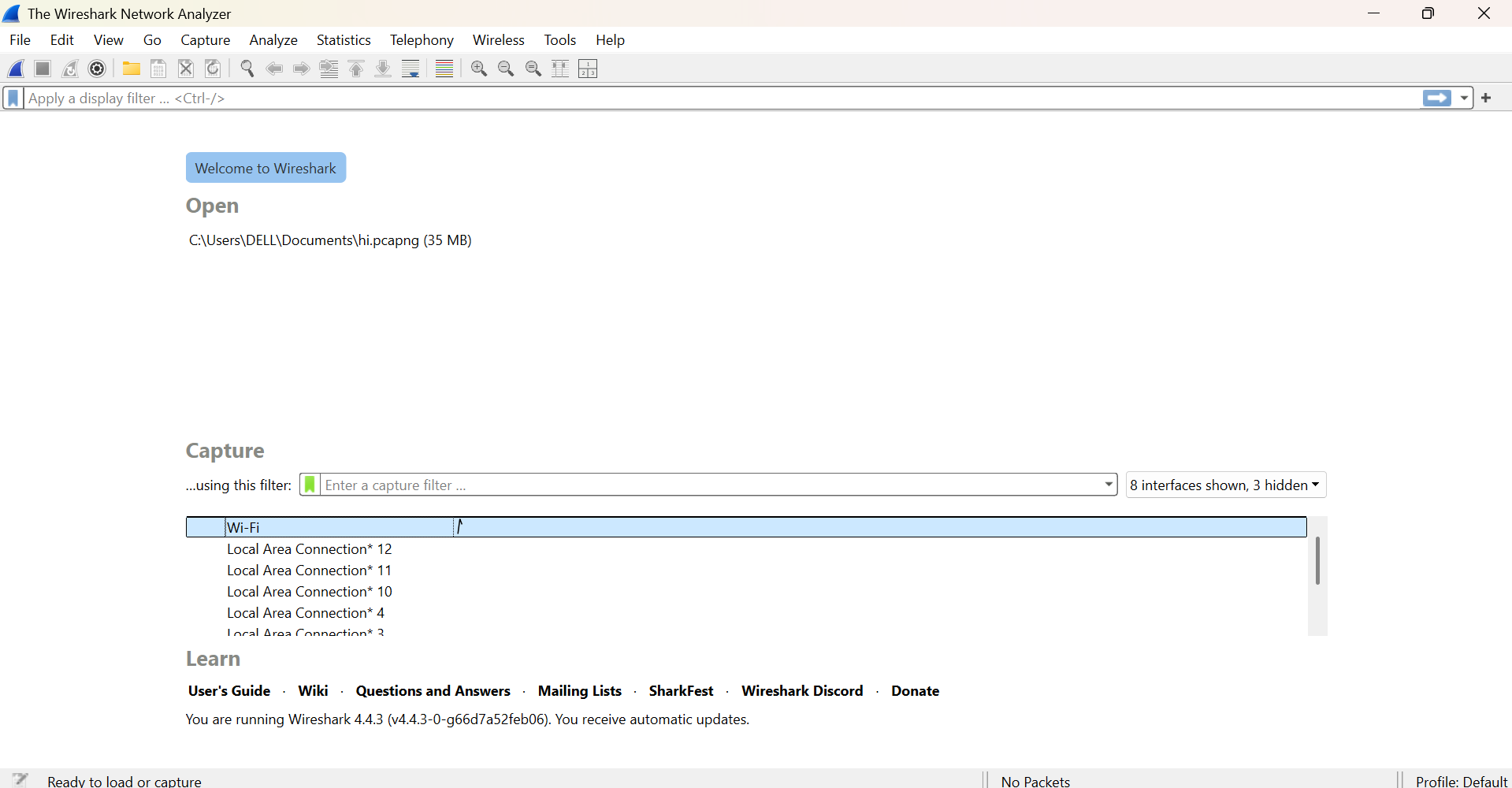
* **MAC address:** ff:ff:ff:ff:ff:ff (Broadcast — gửi đến tất cả các thiết bị trong mạng cục bộ).
* **NIC manufacturer:** Không áp dụng (do là địa chỉ broadcast).
* **NIC serial number:** Không áp dụng (do là địa chỉ broadcast).

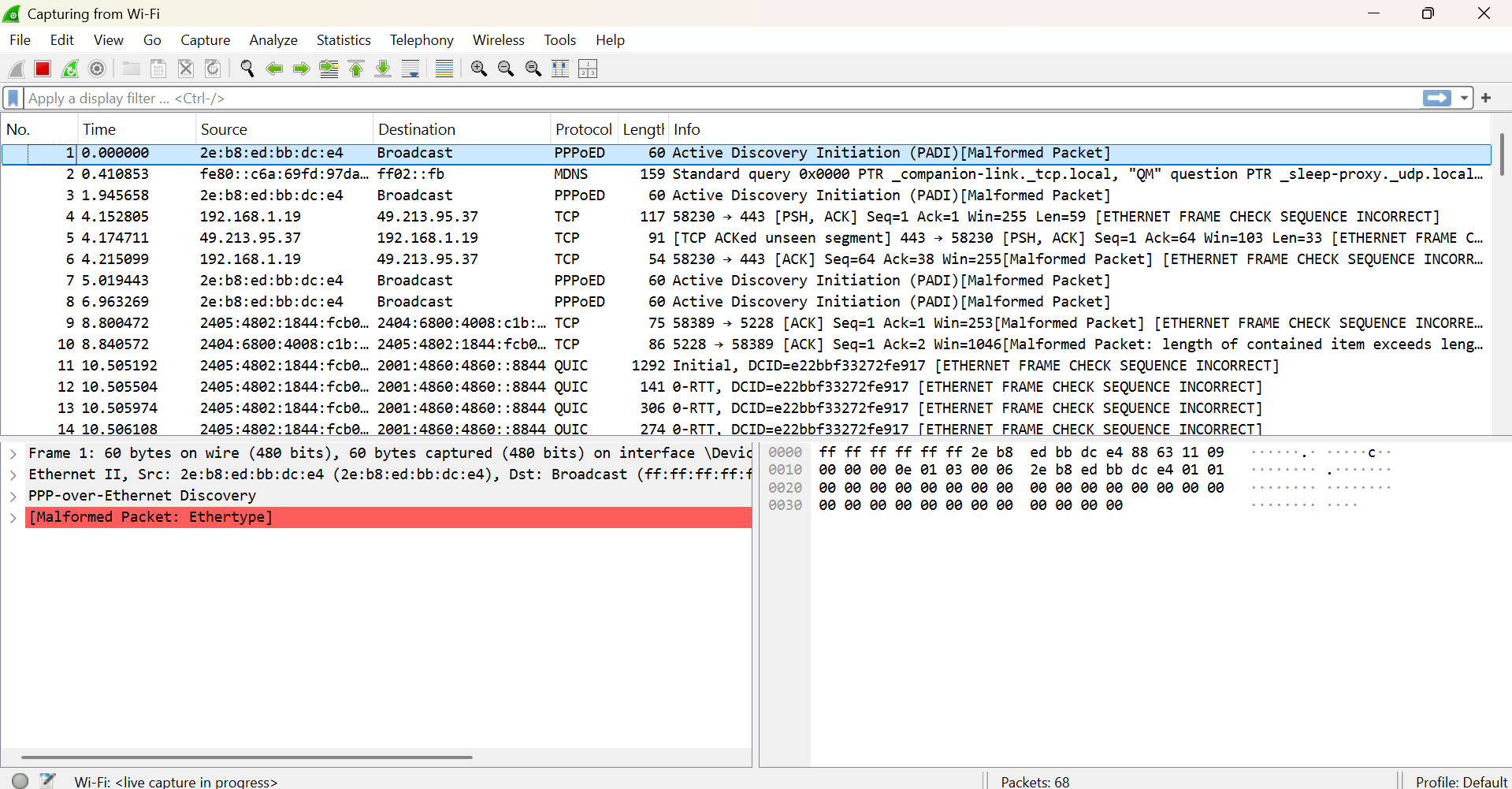
**Địa chỉ nguồn:**

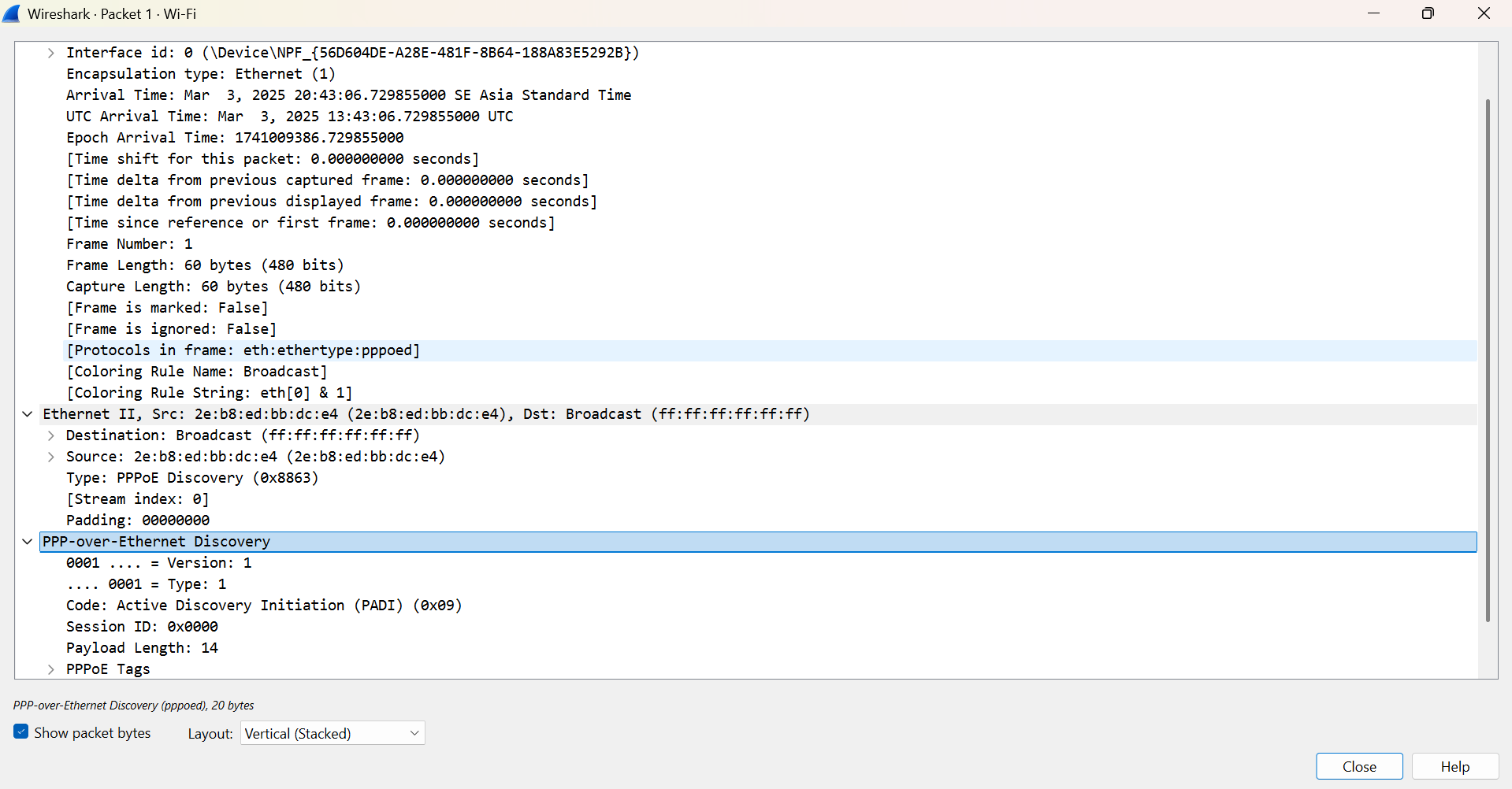
* **MAC address:** 08:1c:6e:a7:36:2a
* **NIC manufacturer:** Phần đầu (08:1c:6e) có thể dùng để xác định nhà sản xuất. Trong trường hợp này, tên có vẻ như là **Xiaomi** dựa trên gợi ý trong ảnh.
* **NIC serial number:** a7:36:2a (phần còn lại của MAC address).

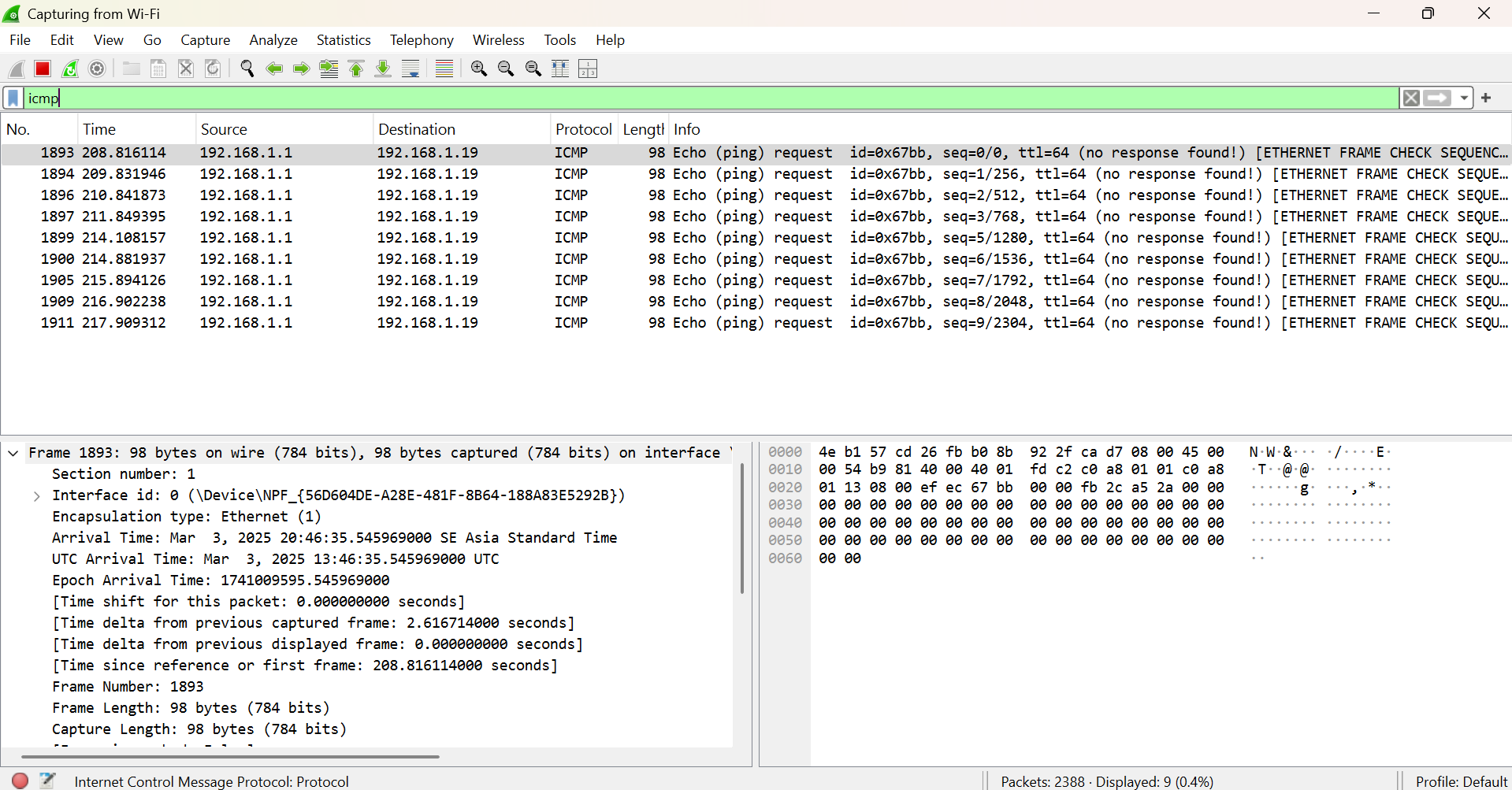
**Bài tập: thực hiện lệnh ping đến một server ngoài Internet đồng thời bắt gói (chẳng hạn www.uneti.edu.vn). Dựa vào việc thu thập thông tin trong các gói tin bắt được có thể biết được địa chỉ MAC của server này không? Tại sao?**

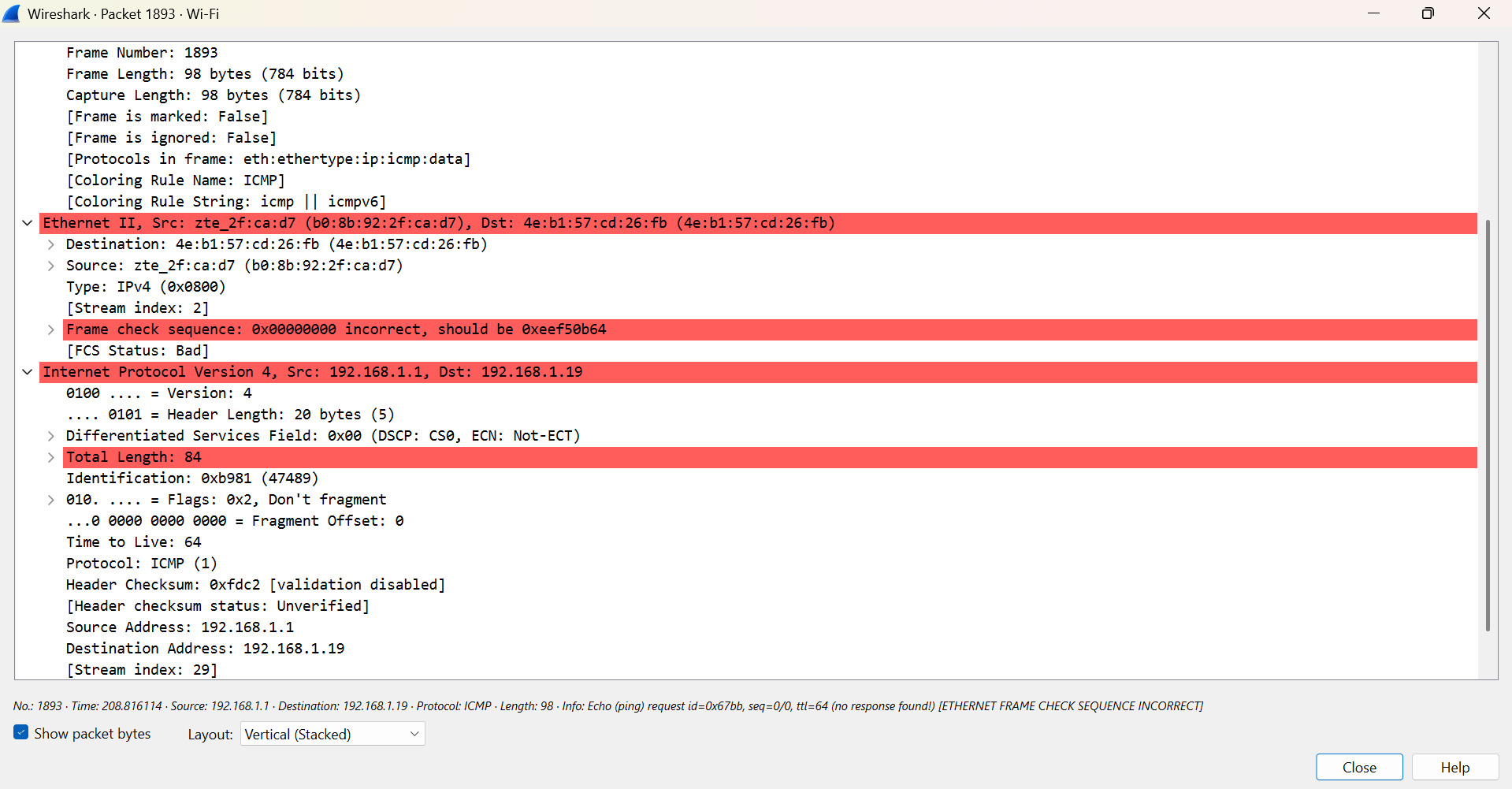
****

****

****







Khi thực hiện lệnh ping đến một server ngoài Internet và bắt gói tin bằng Wireshark, không thể biết được địa chỉ MAC của server đó. Nguyên nhân là do địa chỉ MAC chỉ hoạt động trong phạm vi mạng LAN và không được truyền đi trên toàn bộ hành trình của gói tin qua các mạng trung gian.

Cụ thể, khi một gói tin rời khỏi mạng nội bộ, các router trên đường đi sẽ thay thế địa chỉ MAC nguồn và đích bằng địa chỉ MAC của chính chúng để chuyển tiếp gói tin đến chặng tiếp theo. Chỉ địa chỉ IP đích là được giữ nguyên trong suốt quá trình truyền dữ liệu qua các mạng. Trong hình ảnh Wireshark, địa chỉ MAC được hiển thị là của một thiết bị trung gian, có thể là router trong mạng nội bộ, chứ không phải của server ngoài Internet.

Do đó, việc bắt gói tin ICMP từ lệnh ping chỉ có thể cung cấp địa chỉ MAC của các thiết bị trong cùng mạng LAN hoặc của các thiết bị trung gian gần nhất, không thể xác định địa chỉ MAC của server ở bên ngoài mạng.