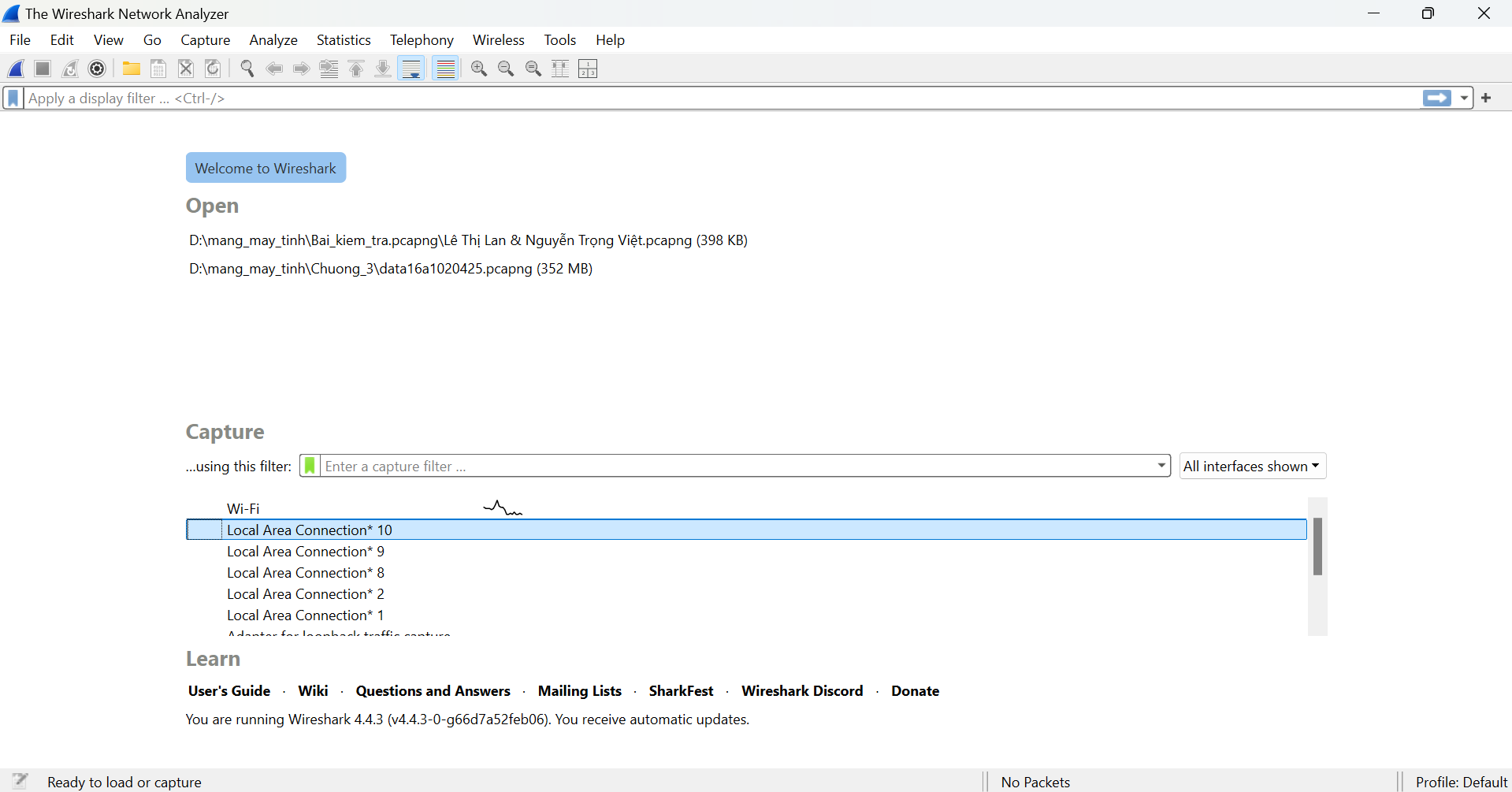
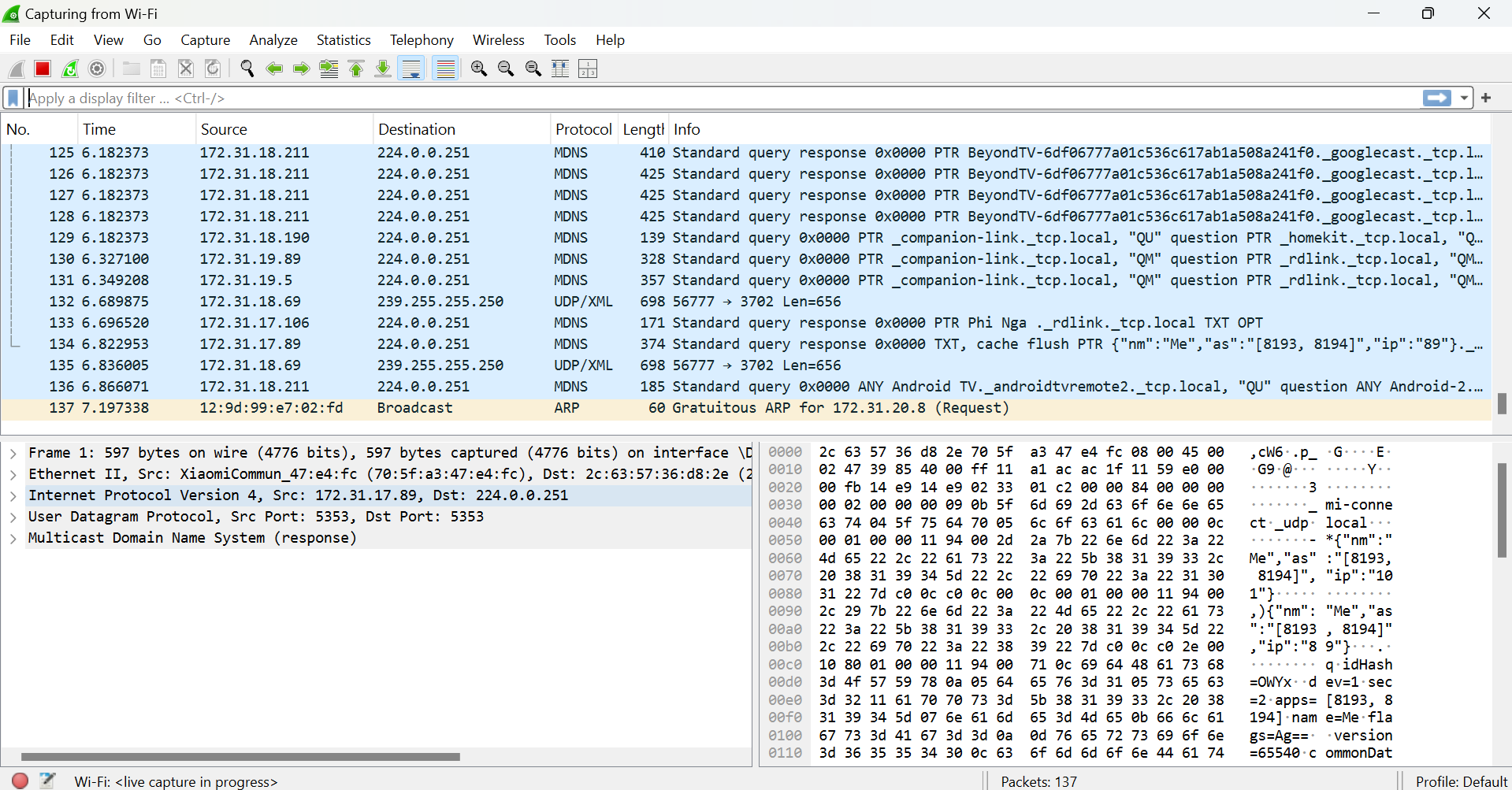
**BÀI KIỂM TRA**

|  |  |
| --- | --- |
| **Họ và tên thành viên** | **Mã sinh viên** |
| Lê Thị Lan | 22174600093 |
| Nguyễn Trọng Việt | 22174600095 |

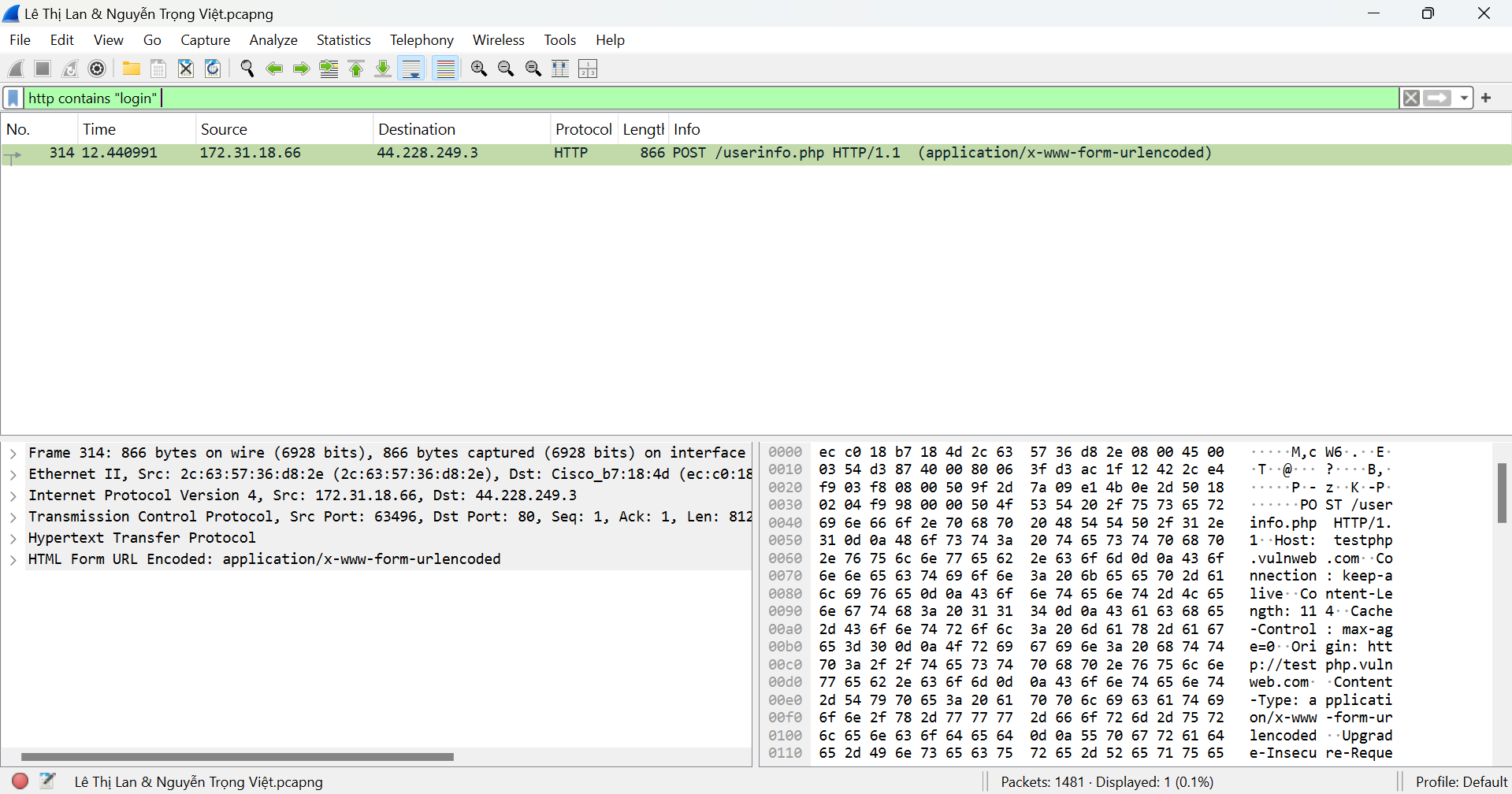
NỘI DUNG THỰC HIỆN:

Bước 1: Mở Wireshark, chọn card mạng, bắt gói tin truy cập 1 trang web.

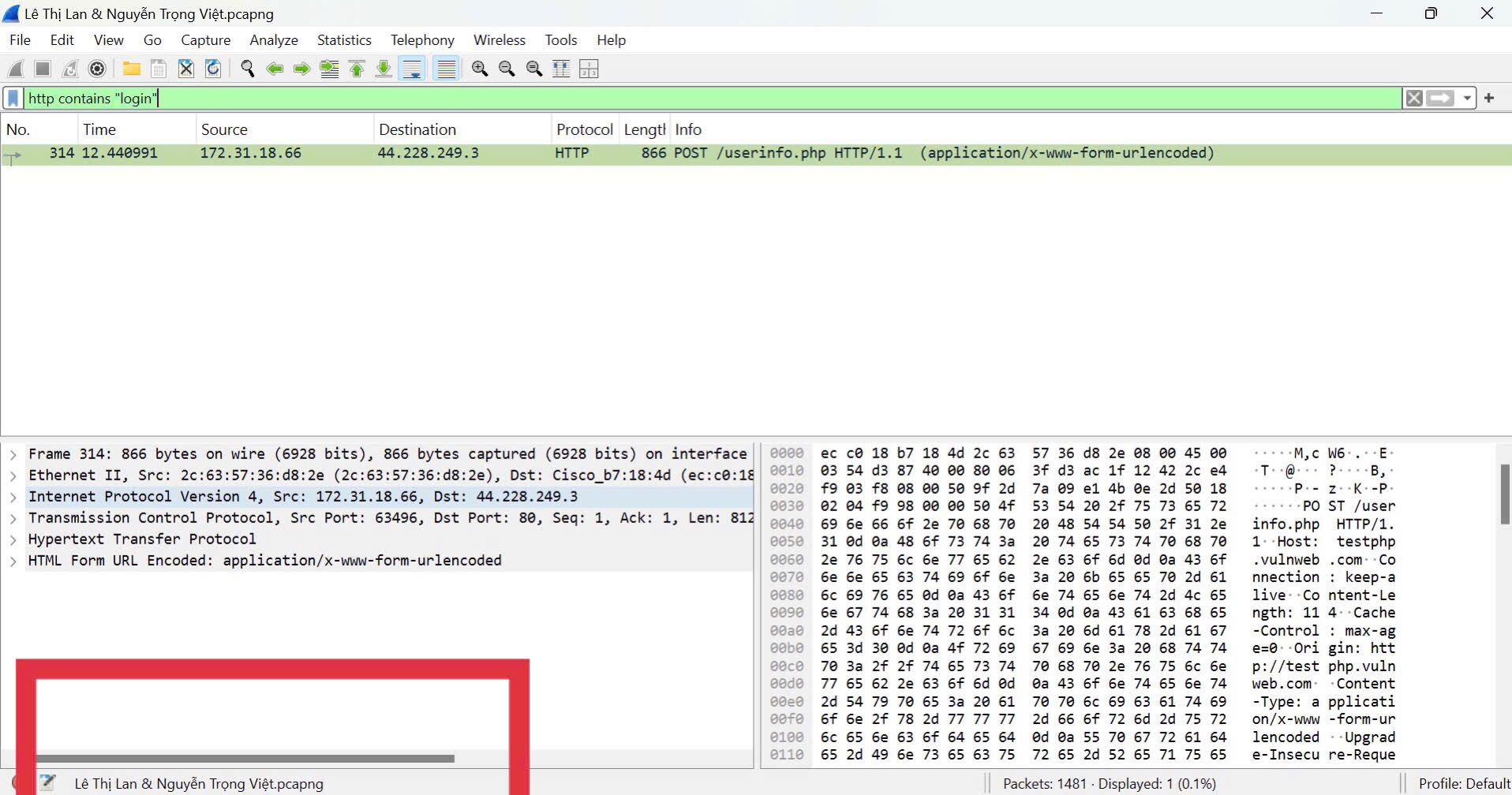




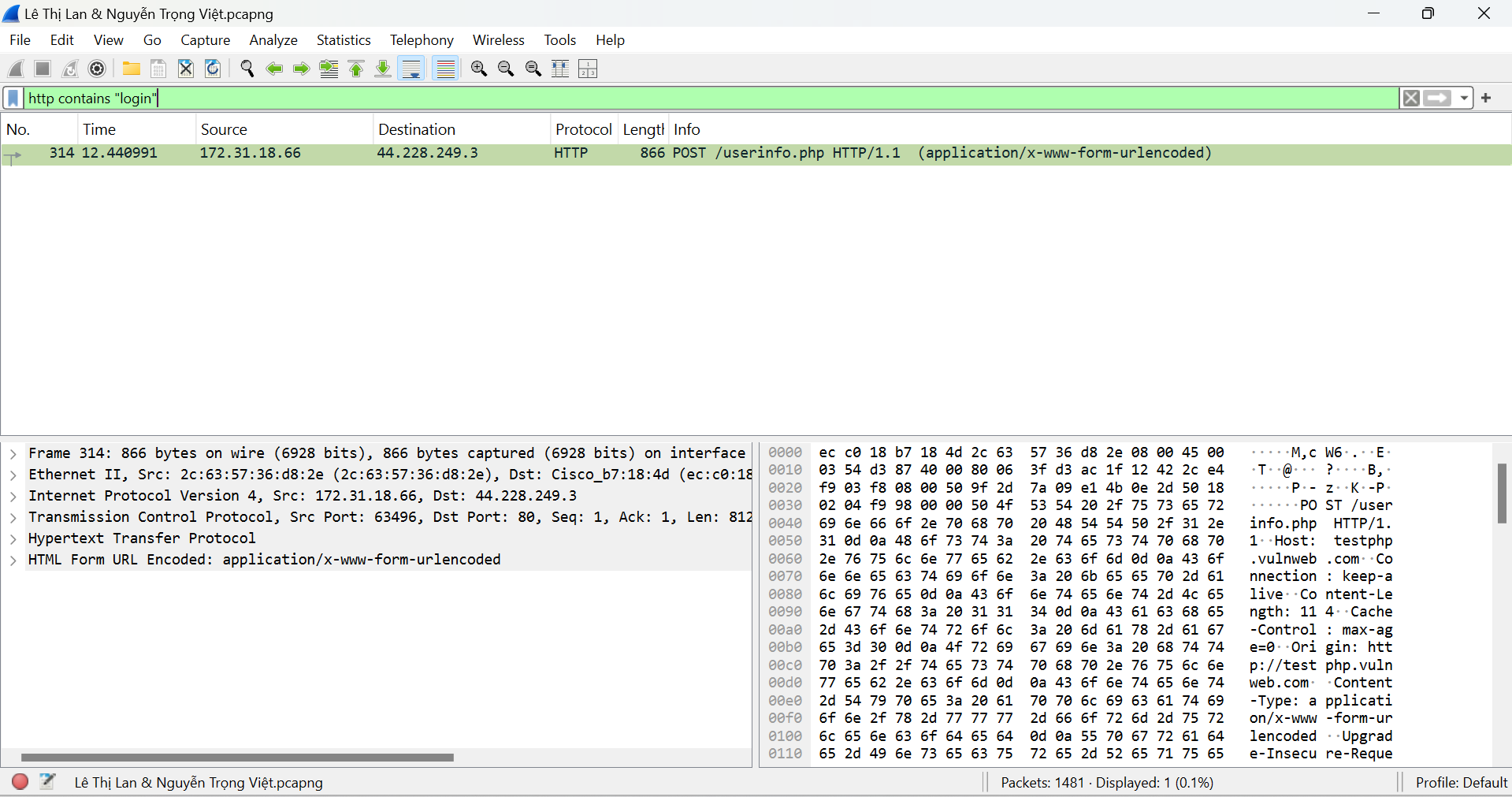
Bước 2: Lọc giao thức HTTP, truy cập một trang login, quan sát gói gửi dữ liệu:



Bước 3: Lưu file kết quả bắt gói tin



Bước 4: Mở lại file đã lưu, phân tích từng lớp trong mô hình OSI



**Phân tích từng lớp:**

Lớp 1: Physical Layer (Vật lý)

* Wireshark không thể hiển thị trực tiếp lớp vật lý, vì lớp này liên quan đến bit, tín hiệu điện, cáp mạng, Wi-Fi...
* Tuy nhiên, nó là lớp đảm bảo dữ liệu (bit) được truyền vật lý giữa hai thiết bị.

➡ Không có dữ liệu trong PCAP về lớp này, nhưng nó vẫn hoạt động ngầm phía dưới.

Lớp 2: Data Link Layer (Liên kết dữ liệu)

* Giao thức: Ethernet II
* Thông tin chính:
  + MAC nguồn: Địa chỉ MAC của máy gửi
  + MAC đích: Địa chỉ MAC của máy nhận
  + Có thể kèm theo: CRC, frame check...

Lớp 3: Network Layer (Mạng)

* Giao thức: IP (IPv4)
* Thông tin chính:
  + IP nguồn: IP máy gửi (ví dụ: 192.168.1.100)
  + IP đích: IP máy đích (ví dụ: 64.38.232.25)
  + Các trường khác: TTL, Header Checksum, Fragment Offset..

Lớp 4: Transport Layer (Vận chuyển)

* Giao thức: TCP
* Thông tin chính:
  + Cổng nguồn: ví dụ: 59213
  + Cổng đích: 80 (HTTP)
  + Các trường như: Seq, Ack, Window Size, Flags (SYN, ACK, PSH...)

Lớp 5: Session Layer (Phiên)

* Mục đích: Quản lý phiên kết nối (session), thiết lập và duy trì trạng thái.
* Trong HTTP, session được thể hiện qua:
  + Header Cookie để duy trì đăng nhập
  + Header Connection: keep-alive để giữ phiên TCP

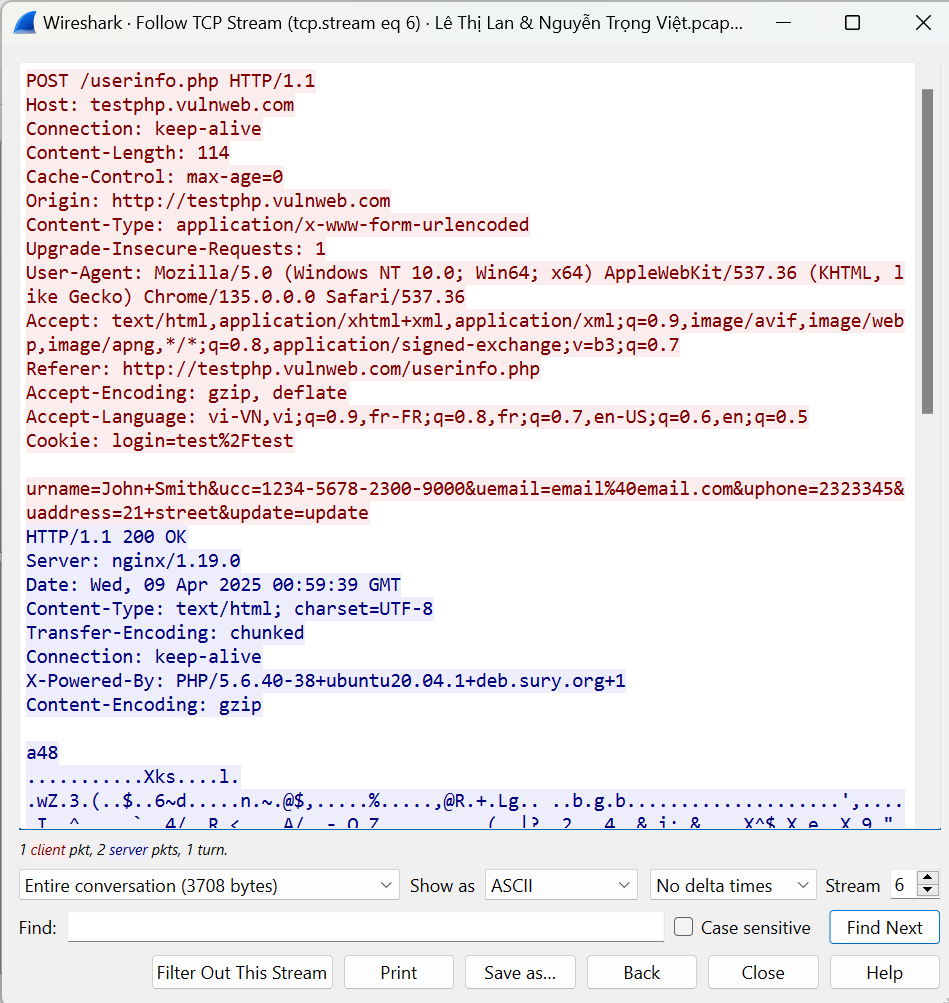
Lớp 6: Presentation Layer (Trình bày)

* Chịu trách nhiệm mã hóa/giải mã, nén/giải nén dữ liệu.
* Trong HTTP, có thể thấy qua:
  + Content-Encoding: gzip → máy chủ trả về nội dung gzip nén
  + Content-Type: application/x-www-form-urlencoded → kiểu dữ liệu gửi đi

Lớp 7: Application Layer (Ứng dụng)

* Giao thức: HTTP
* Là lớp mà người dùng "thấy" khi sử dụng trình duyệt, gửi form,...

Bước 5: Sử dụng tính năng Protocol Hierarchy hoặc TCP Stream để quan sát toàn cục



Bước 6: Viết mã Python dùng thư viện PyShark để truy xuất thông tin tầng 2 và tầng 3 từ file .pcapng.

import pyshark

# Đường dẫn đến file .pcapng đã thu được bằng Wireshark

file\_path = r'D:\học kỳ 2\_ năm 3\Mạng máy tính và truyền số liệu\Lê Thị Lan & Nguyễn Trọng Việt.pcapng'

# Tạo đối tượng đọc file gói tin

cap = pyshark.FileCapture(file\_path, use\_json=True, keep\_packets=False)

# Duyệt qua từng gói tin trong file

for i, pkt in enumerate(cap):

    try:

        print(f"\n=== Gói {i+1} ===")

        # Tầng 2: Data Link Layer (Ethernet)

        if 'eth' in pkt:

            print("Tầng 2 - MAC nguồn (Source MAC):", pkt.eth.src)

            print("Tầng 2 - MAC đích (Destination MAC):", pkt.eth.dst)

        # Tầng 3: Network Layer (IP)

        if 'ip' in pkt:

            print("Tầng 3 - IP nguồn (Source IP):", pkt.ip.src)

            print("Tầng 3 - IP đích (Destination IP):", pkt.ip.dst)

            print("Tầng 3 - Giao thức:", pkt.ip.proto)

    except Exception as e:

        print(f"Lỗi tại gói #{i+1}: {e}")

    # Giới hạn số gói để xem (tùy chọn)

    if i >= 10:

        break

Dưới đây là kết quả:

