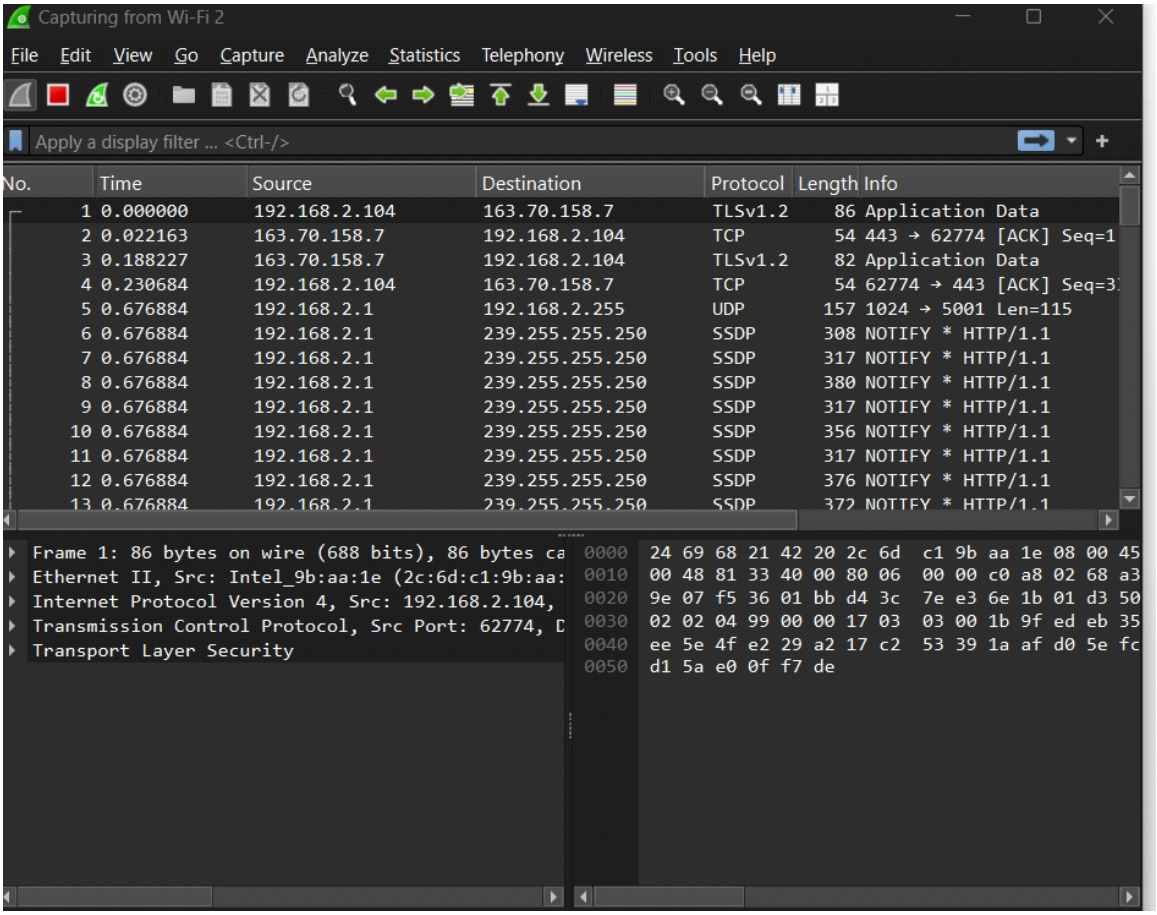
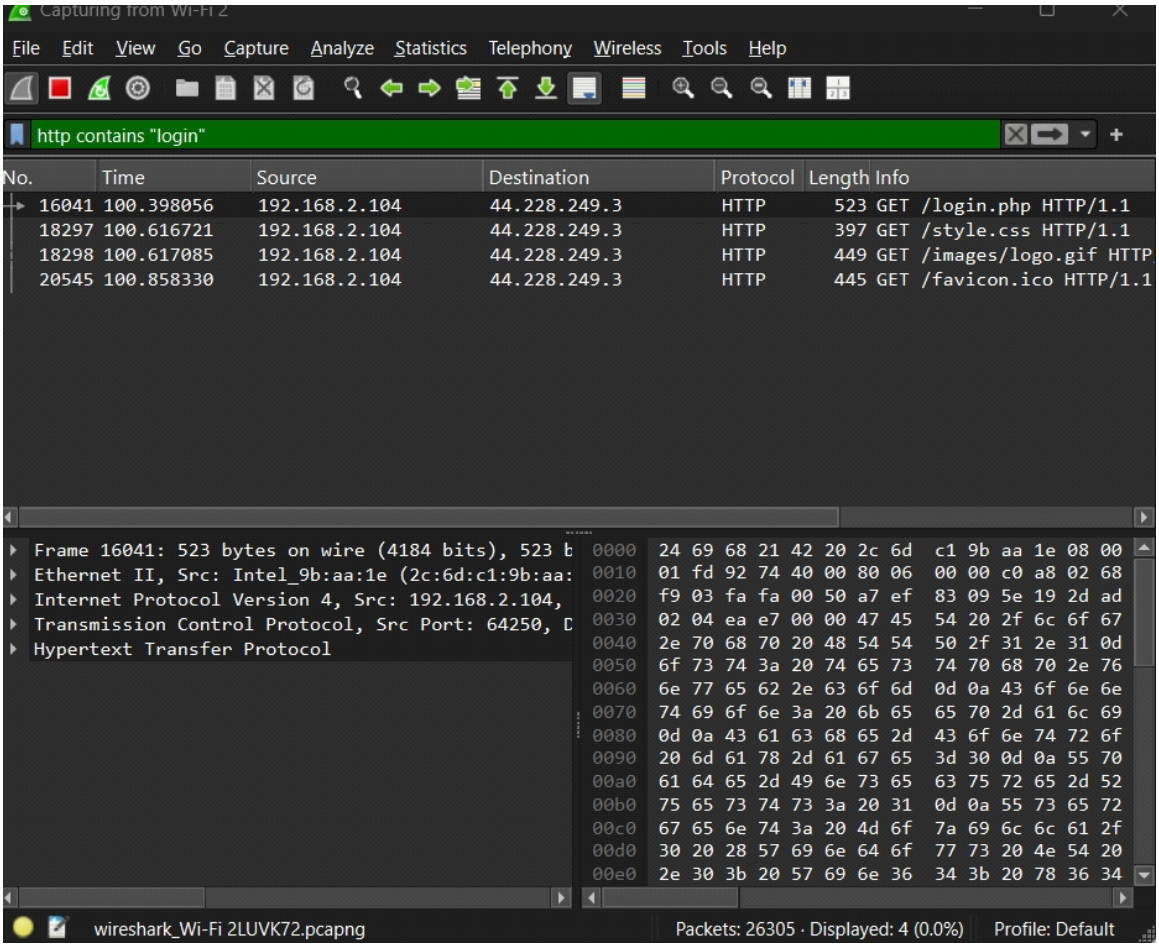
Bài kiểm tra

Bước 1: Mở Wireshark, chọn card mạng, bắt gói khi truy cập một 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 (.pcapng).

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

Lớp Mạng (Network Layer)

Mô tả: Định tuyến gói tin (packet) từ client đến server qua địa chỉ IP.

Liên quan:

+ Trình duyệt gửi HTTP request đến địa chỉ IP của

testphp.vulnweb.com (DNS resolved).

+ Giao thức: IP (Internet Protocol)

Lớp Giao vận (Transport Layer)

Mô tả: Đảm bảo truyền dữ liệu đáng tin cậy giữa các thiết bị.

Liên quan:

+ Giao thức: TCP (Transmission Control Protocol).

+ HTTP hoạt động dựa trên TCP, qua cổng 80 (hoặc 443 với

HTTPS).

+ Giữ kết nối qua Connection: keep-alive.

Lớp Phiên (Session Layer)

Mô tả: Quản lý phiên giao tiếp giữa client và server.

Liên quan:

+ Session login bằng cookie: login=test/test.

+ Logout qua logout.php → quản lý trạng thái đăng nhập.

+ Giữ kết nối lâu dài: keep-alive.

Lớp Trình bày (Presentation Layer)

Mô tả: Biến đổi, mã hóa dữ liệu.

Liên quan:

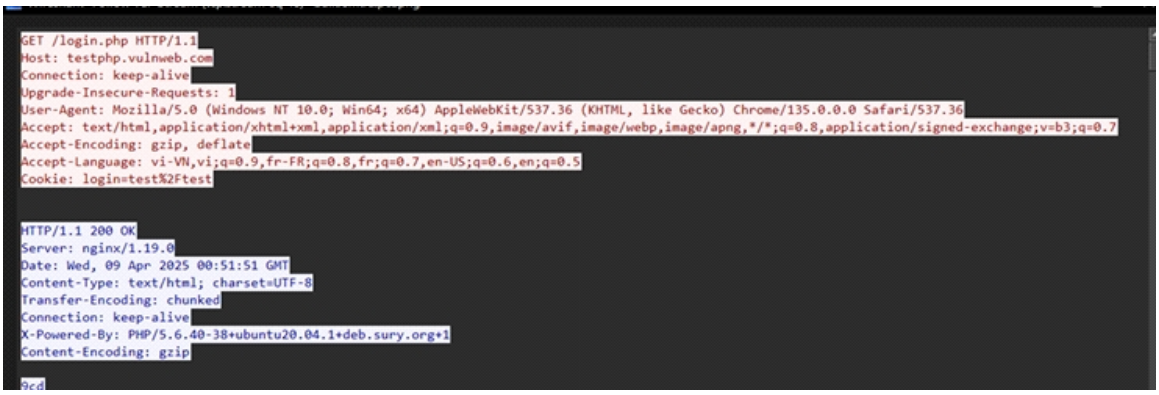
+ Gửi và nhận HTML, CSS → trình duyệt hiển thị nội dung.

+ Mã hóa/giải mã ký tự: charset=UTF-8 (server) và iso-8859-2

(HTML).

Bước 5: Sử dụng tính năng Protocol Hierarchy hoặc Follow TCP Stream để

quan sát toàn cục



Đặc điểm	Mô tả
Loại giao thức	TCP là giao thức tầng 4 (transport layer), nền tảng cho HTTP tầng 7.
Kết nối	Sử dụng keep-alive giữ kết nối TCP mở, giảm overhead tái thiết lập.
Đảm bảo thứ tự	TCP chia nhỏ dữ liệu thành segment và đảm bảo đúng thứ tự khi đến nơi.
Đảm bảo độ tin cậy	Tự động gửi lại gói tin nếu bị mất trong quá trình truyền.
Kiểm soát lưu lượng	Điều chỉnh lượng dữ liệu gửi để không vượt quá khả năng tiếp nhận.
Kiểm soát tắc nghẽn	Tự động giảm tốc độ gửi khi phát hiện nghẽn mạng.