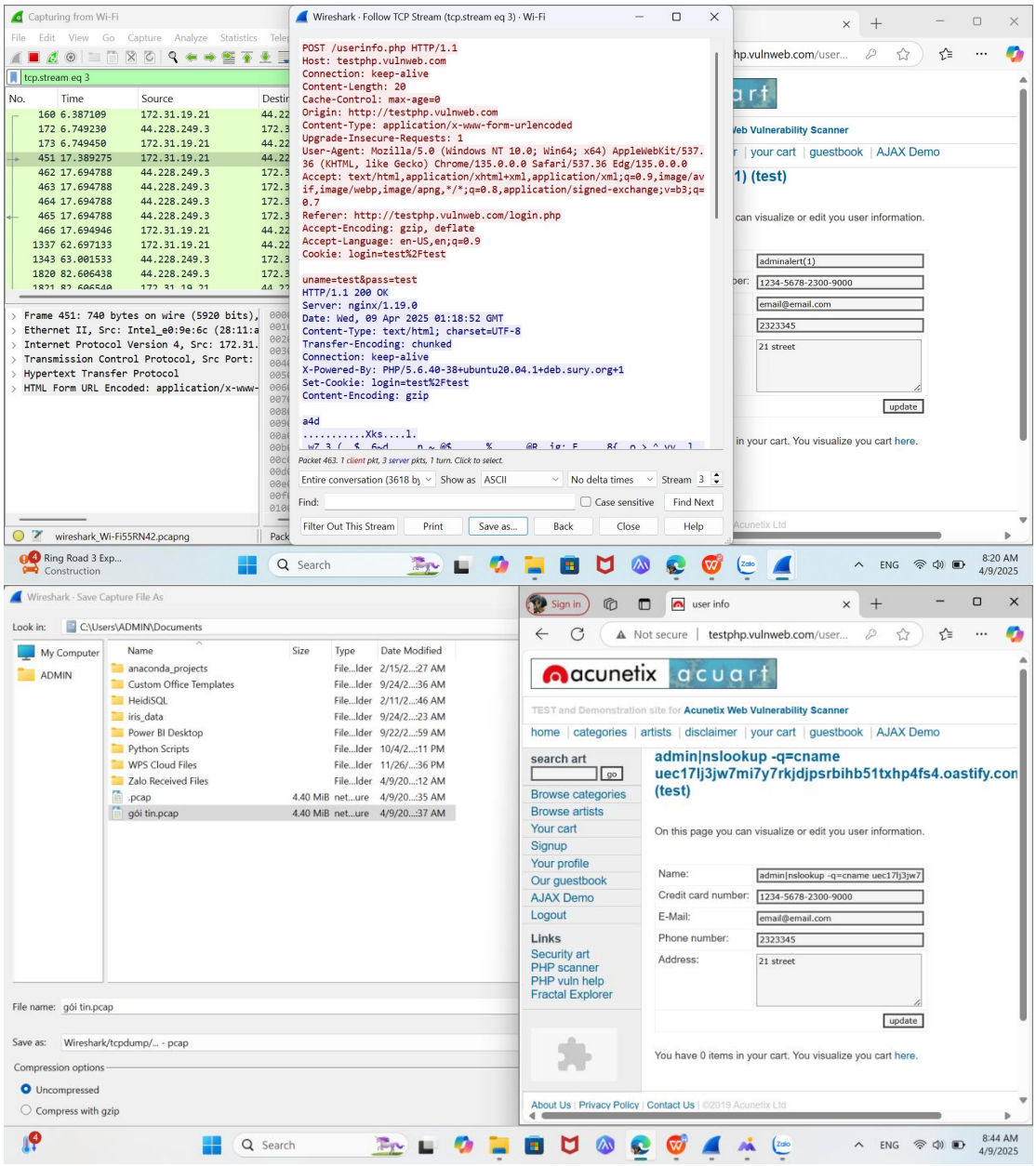
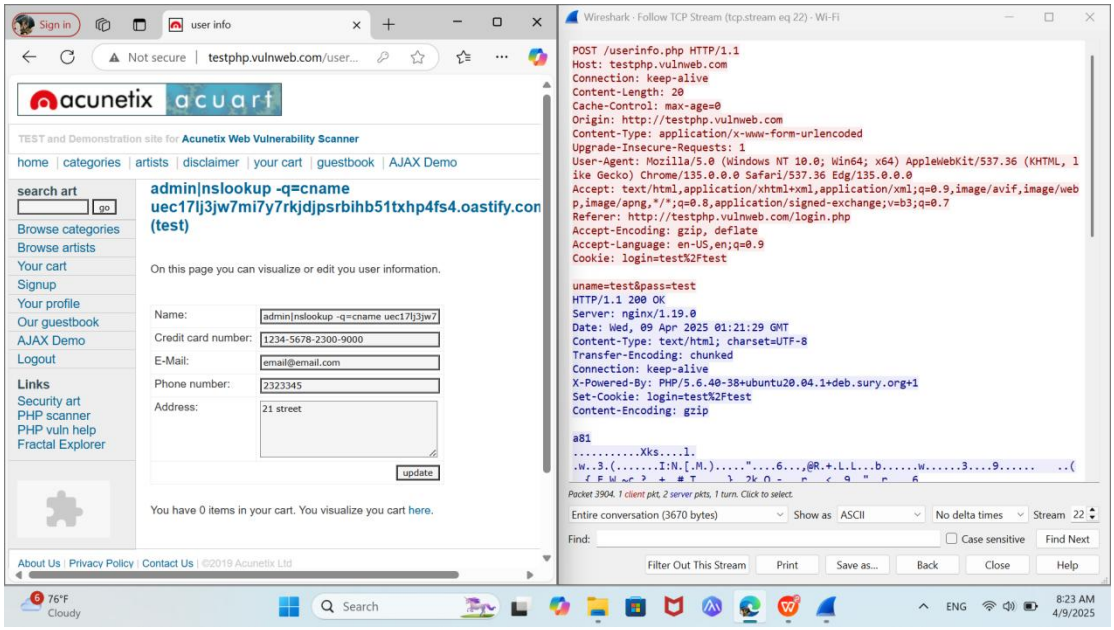
Nguyễn Thị Phương Anh-22174600085
Lê Thị Phương Linh-22174600057

Bước 1:





Code:

```
import pyshark

def parse_layers(file_path):
    cap = pyshark.FileCapture(file_path, display_filter='eth || ip || ipv6')

    print(" Phân tích các gói tin tầng 2 và tầng 3 trong file .pcapng:\n")

    for i, pkt in enumerate(cap):
        if i >= 10:
            break

        print(f"  Gói tin {i + 1}:")

        # Tầng 2: Ethernet
        if 'eth' in pkt:
            eth = pkt.eth
            print("   Layer 2 - Ethernet:")
            print(f"    MAC nguồn: {eth.src}")
            print(f"    MAC đích:  {eth.dst}")
            print(f"    Ether Type: {eth.type}")

        # Tầng 3: IPv4
        if 'ip' in pkt:
            ip = pkt.ip
            print("   Layer 3 - IPv4:")
            print(f"    IP nguồn: {ip.src}")
            print(f"    IP đích:  {ip.dst}")
            print(f"    Giao thức: {ip.proto}")

        # Tầng 3: IPv6
        elif 'ipv6' in pkt:
            ipv6 = pkt.ipv6
            print("   Layer 3 - IPv6:")
            print(f"    IP nguồn: {ipv6.src}")
            print(f"    IP đích:  {ipv6.dst}")
            print(f"    Next Header: {ipv6.nxt}")

        print("-" * 40)

    cap.close()

# Gọi hàm với đường dẫn file (bạn cần viết đúng đường dẫn nếu dùng trên máy mình)
parse_layers("tcp(1).pcapng")
```

Kết quả:

```
Phân tích các gói tin tầng 2 và tầng 3 trong file .pcapng:
```

Nhận xét:
Gói tin HTTP
Gói HTTP là một gói tin hoạt động ở tầng 7 - Application Layer trong mô hình OSI.

Giao thức sử dụng: HTTP (HyperText Transfer Protocol)

Tầng vận chuyển: TCP (thường là cổng 80)

Đặc điểm:

Dữ liệu truyền là văn bản thuần túy, có thể đọc được bằng mắt thường (GET, POST, Header, Body...).

Khi bắt gói trong Wireshark, bạn có thể xem toàn bộ nội dung của gói HTTP như tiêu đề (header), nội dung (body), cookie, v.v.

HTTP: Dễ đọc, không bảo mật.

HTTPS: Bảo mật, mã hóa toàn bộ nội dung.

Gói HTTPS cũng là giao thức tầng 7, nhưng có đặc điểm:

Giao thức: HTTPS = HTTP + TLS/SSL (bảo mật)

Tầng vận chuyển: TCP (thường là cổng 443)

Đặc điểm:

Dữ liệu được mã hóa, không đọc được bằng mắt thường.

Bạn không thể thấy nội dung HTTP bên trong nếu không có khóa giải mã.

Chỉ có thể thấy quá trình bắt tay TLS (TLS handshake), chứng chỉ, v.v.