Trong bước này, em mở lại file http.pcapng đã lưu bằng Wireshark và phân tích các gói tin theo từng tầng trong mô hình OSI như sau:

Tầng 1 – Physical (Vật lý)

- Không thể hiện trực tiếp trong Wireshark.
- Đây là tầng truyền dữ liệu thực tế qua cáp mạng hoặc sóng Wi-Fi.

Tầng 2 – Data Link (Liên kết dữ liệu)

- Sử dụng giao thức: **Ethernet II**
- Có thể quan sát các thông tin như:
  - **MAC nguồn (Source MAC)**: ví dụ 08:00:27:aa:bb:cc
  - **MAC đích (Destination MAC)**: ví dụ 08:00:27:dd:ee:ff

Tầng 3 – Network (Mạng)

- Sử dụng giao thức: **IP (Internet Protocol)**
- Thông tin có thể thấy:
  - **IP nguồn (Source IP)**: ví dụ 192.168.1.5
  - **IP đích (Destination IP)**: ví dụ 172.217.161.46
  - **TTL (Time to Live)**: số lần hop còn lại, ví dụ 64

Tầng 4 – Transport (Giao vận)

- Giao thức: **TCP**
- Thông tin hiển thị:
  - **Cổng nguồn (Source port)**: ví dụ 52344
  - **Cổng đích (Destination port)**: ví dụ 80 (HTTP)
  - Có thể quan sát **bắt tay TCP 3 bước (SYN, SYN-ACK, ACK)**

Tầng 5 – Session (Phiên)

- Quá trình thiết lập và duy trì phiên TCP nằm ở tầng này.
- Dựa vào chuỗi gói TCP có thể xác định một phiên kết nối đang được thiết lập.

Tầng 6 – Presentation (Trình bày)

- Không hiển thị rõ trong Wireshark.
- Tầng này xử lý mã hóa/giải mã nếu có (trong HTTPS thì sẽ dùng SSL/TLS).
- Với HTTP thì dữ liệu thường không được mã hóa.

Tầng 7 – Application (Ứng dụng)

- Giao thức: **HTTP**
- Có thể thấy rõ các trường:
  - **GET / POST**
  - **Host**, **User-Agent**, **Cookie**, v.v.
- Dễ dàng quan sát nội dung truy vấn nếu là HTTP (vì không mã hóa).

Kết luận:
File http.pcapng chứa dữ liệu HTTP cho phép quan sát rõ các tầng từ tầng 2 đến tầng 7. Qua Wireshark, sinh viên có thể lọc và phân tích chi tiết các gói tin mạng tương ứng với từng lớp trong mô hình OSI.
