HƯỚNG DẪN CHECK LƯU LƯỢNG DATA TRÊN WIRESHARK

1. **Chuẩn bị**:
    a. 1 laptop cài wireshark , có hỗ trợ bắt wifi và phát hotspot (cài đặt hệ điều hành từ win10 trở lên)
    b. 2 điện thoại để test:
        i. Điện thoại 1: Đăng ký gói cước data (Ví dụ: Mimax70)
        ii. Điện thoại 2: Không đăng ký data, dùng để bắt hotspot từ laptop . Điện thoại này dùng để truy cập vào app/web/wap của CP để check freedata
2. **Cách thức thực hiện như sau**:
    a. Điện thoại 1 có đăng ký gói data, phát hotspot cho Laptop → laptop bắt wifi và phát hotspot cho điện thoại 2.
    b. Trên điện thoại 2 thực hiện bắt wifi laptop, sau đó truy cập vào app/web/wap của CP, sử dụng các nội dung có khai báo freedata để kiểm tra
    c. Trên laptop bật wireshark để capture traffic sử dụng của điện thoại 2.
    d. Kiểm tra lưu lượng mà wireshark capture được xem vào các link nào, mất bao nhiêu data

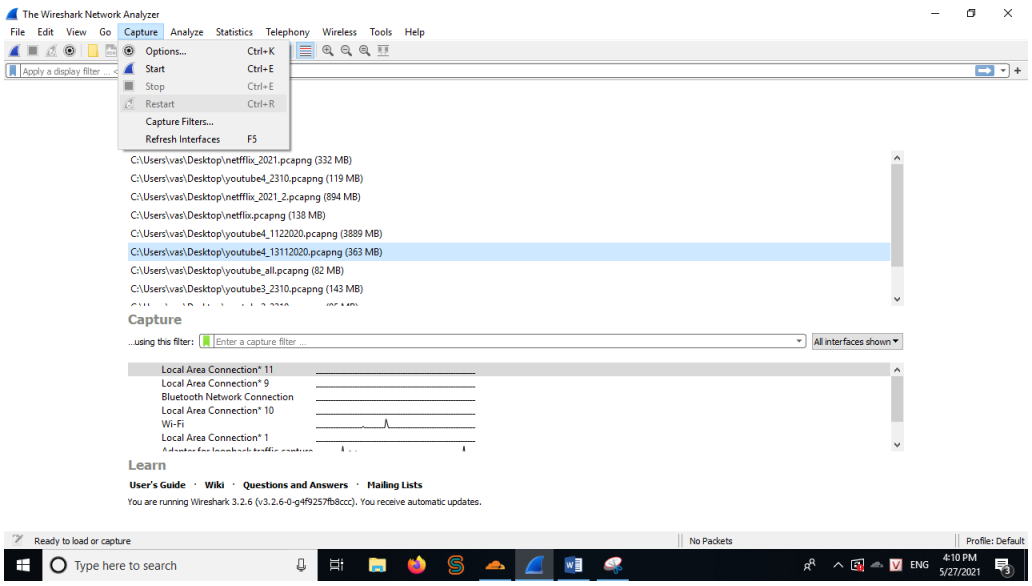
    Lưu ý:

    Tắt tất cả các app, tiền trình ngầm khi sử dụng điện thoại 2 để đảm bảo môi trường test freedata chính xác

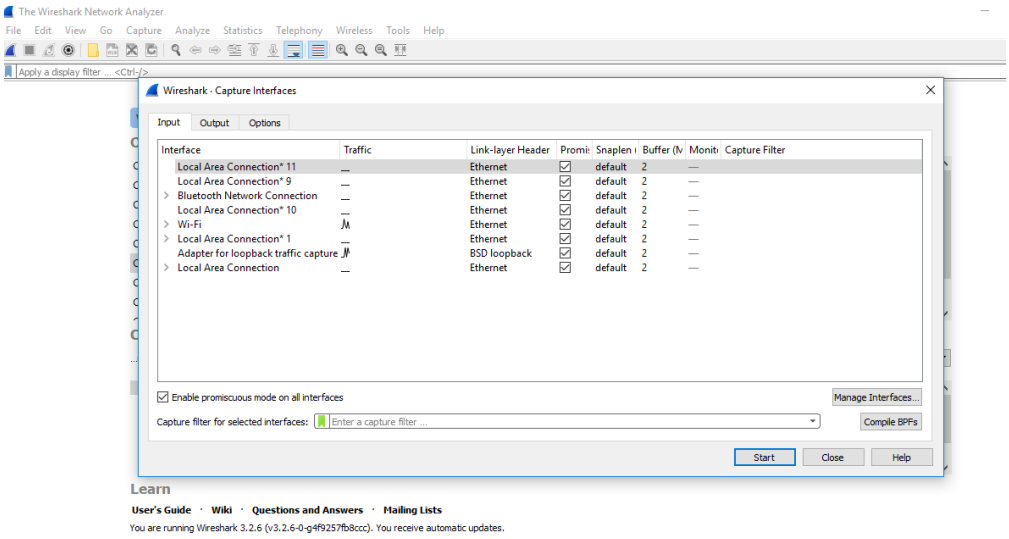
    Trên laptop tắt toàn bộ các ứng dụng làm việc, chỉ để chạy mỗi wireshark để test.

    Khi bật wireshark lên test, chúng ta để cho wireshark chạy 1 lúc để load toàn bộ lưu lượng mà máy tính sử dụng trước khi test freedata. Lấy phần log lưu lượng này ra ngoài để sau khi test đối chiếu và loại trừ.

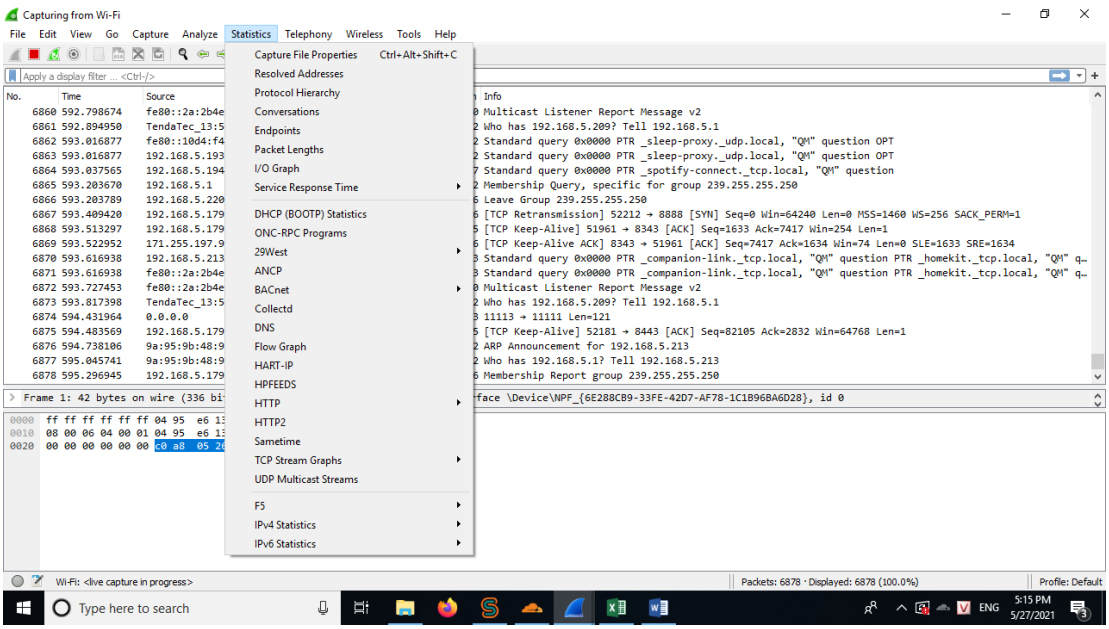
3. **Hướng dẫn thực hiện kiểm tra trên wireshark**:
    - **Bước 1**: Bật wireshark → Chọn captures -> Option. (xem hình bên dưới)



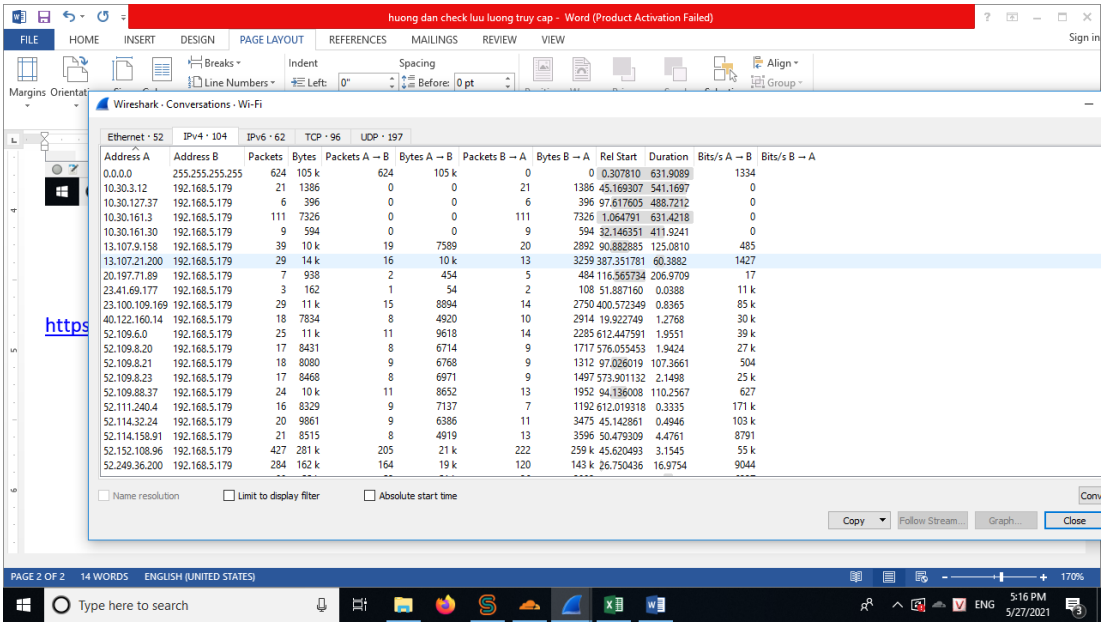
- **Bước 2**: Chọn Wifi → Start. (xem hình bên dưới)

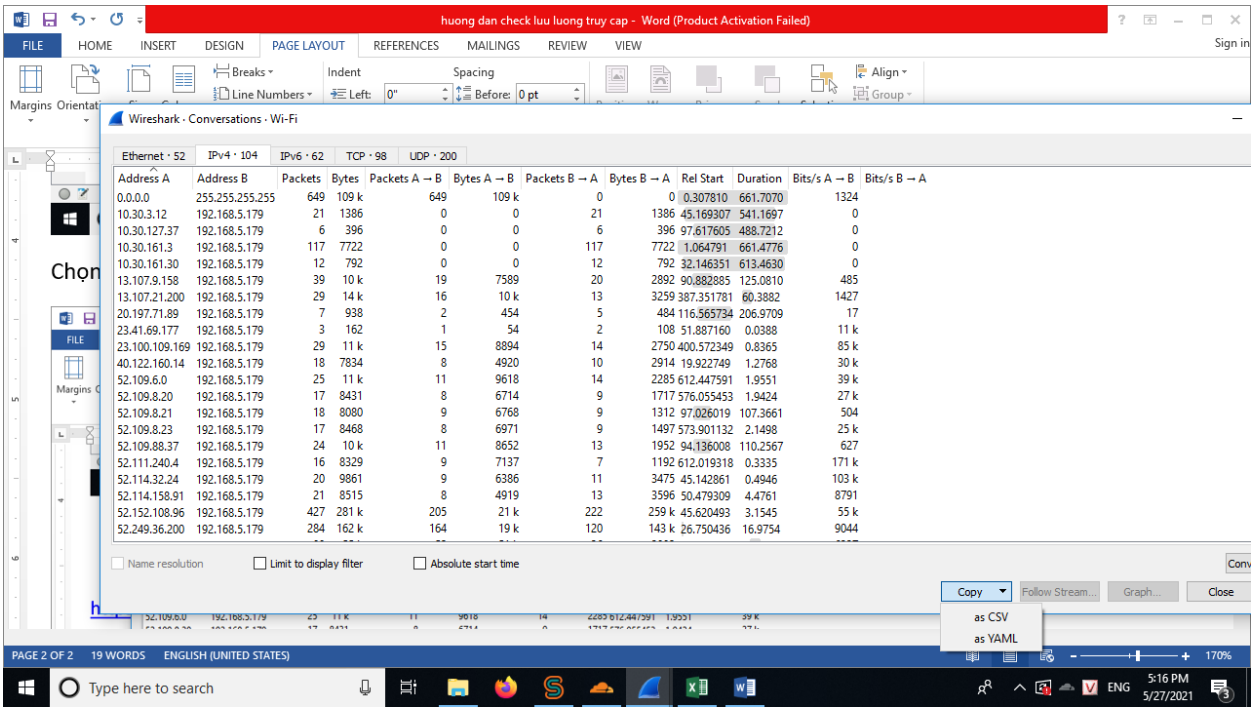


- **Bước 3**: Chọn Statistics → Conversations. (xem hình bên dưới)



- **Bước 4**: Chọn Copy → định dạng csv. (xem hình bên dưới)





- **Bước 5**: Copy ra excel dữ liệu capture và căn chỉnh dữ liệu trong excel
  - Căn chỉnh dữ liệu trong data để phân tách ra từng cột như sau: data → Text to columns → Delimited → Other → “,” ➔ Việc này để phân tác data ra từng cột riêng rẽ giúp check data hiệu quả hơn từ dữ liệu thô đã capture được.
  - Quan tâm chủ yếu đến cột adress A , adress B, bytes với bytes với giá trị >100k.
  - So sánh với dữ liệu đã khai báo freedata với các dữ liệu check mất data nhiều để đánh giá và xem xét cụ thể lỗi.