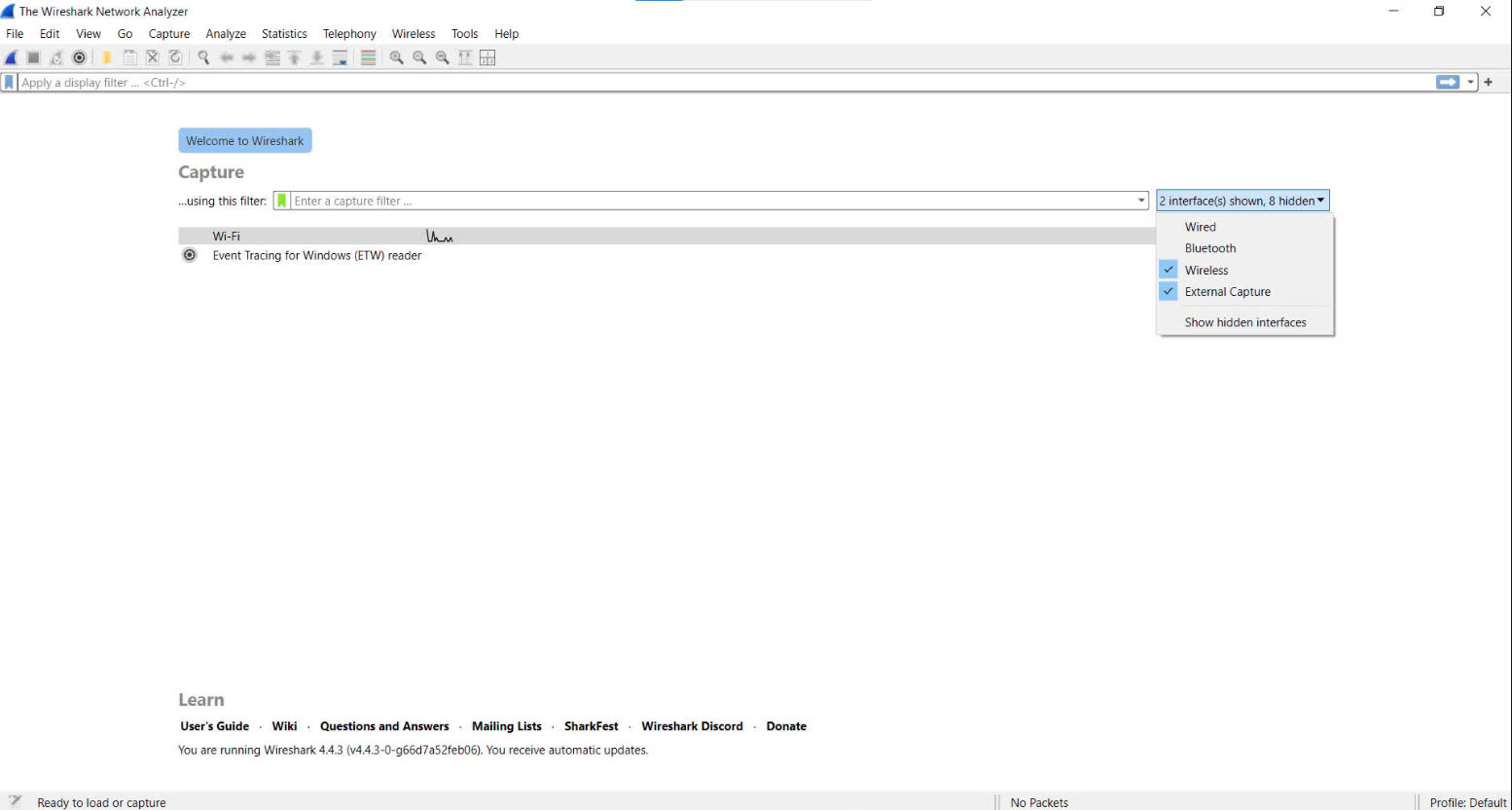
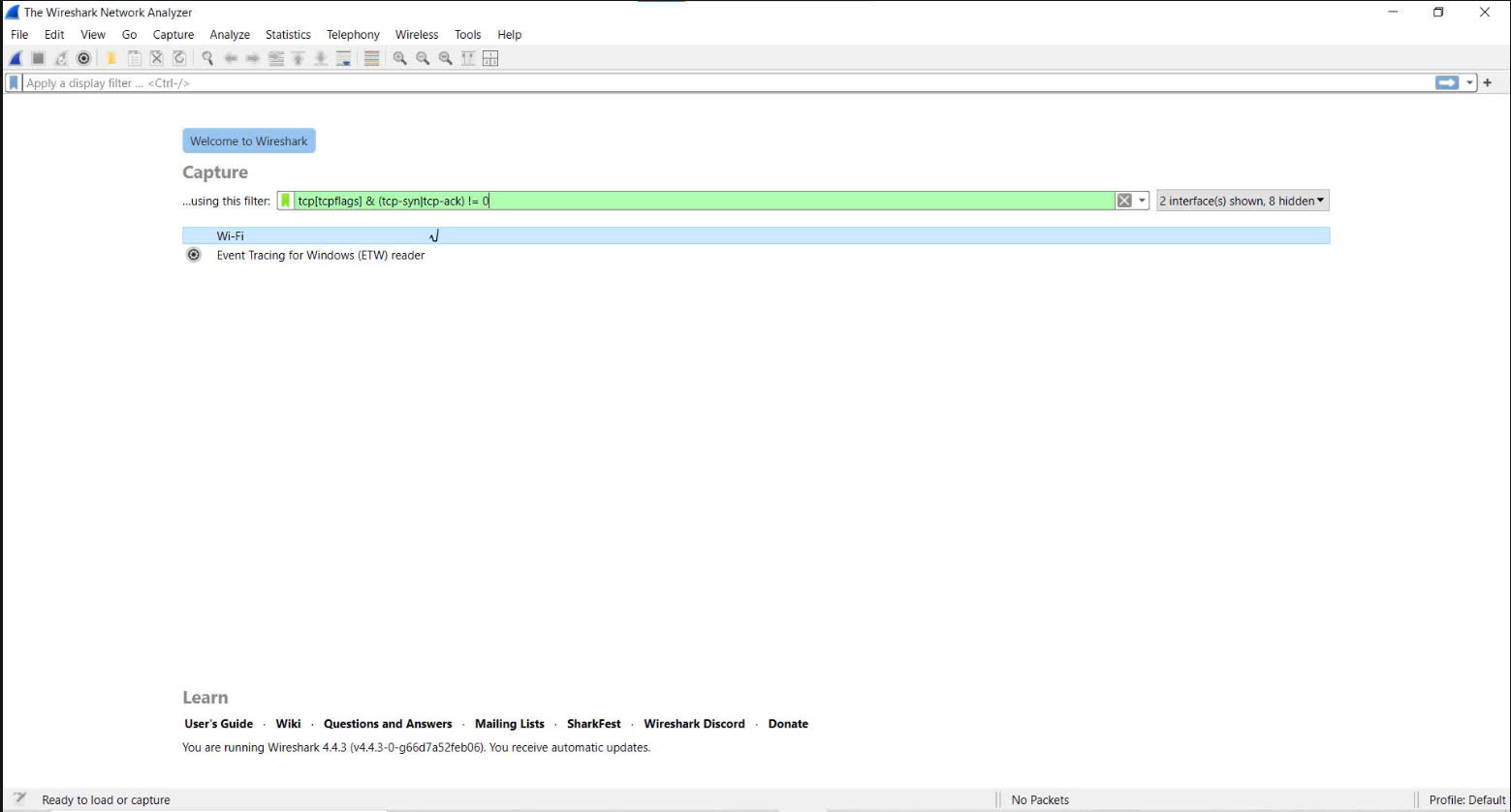
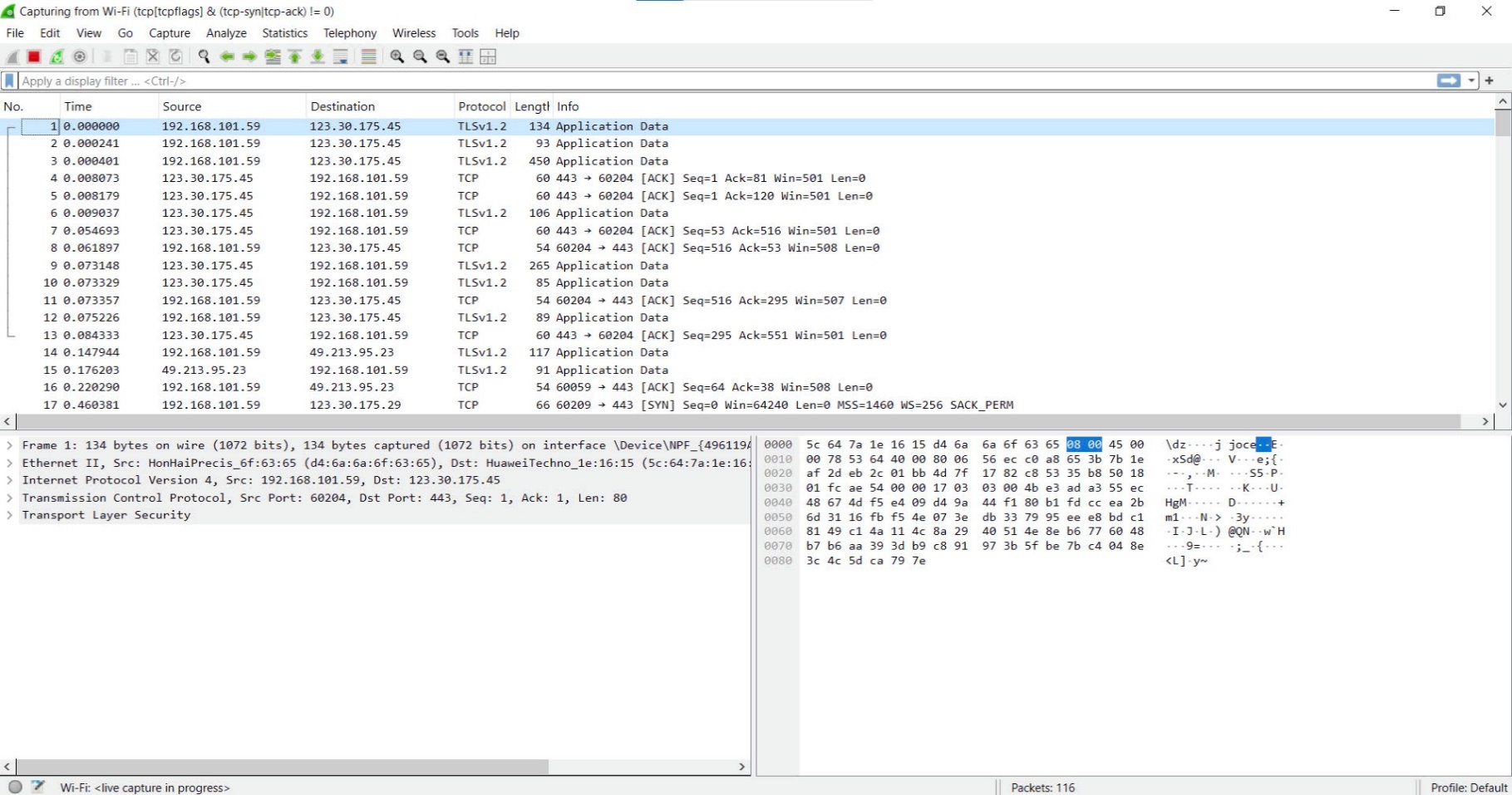
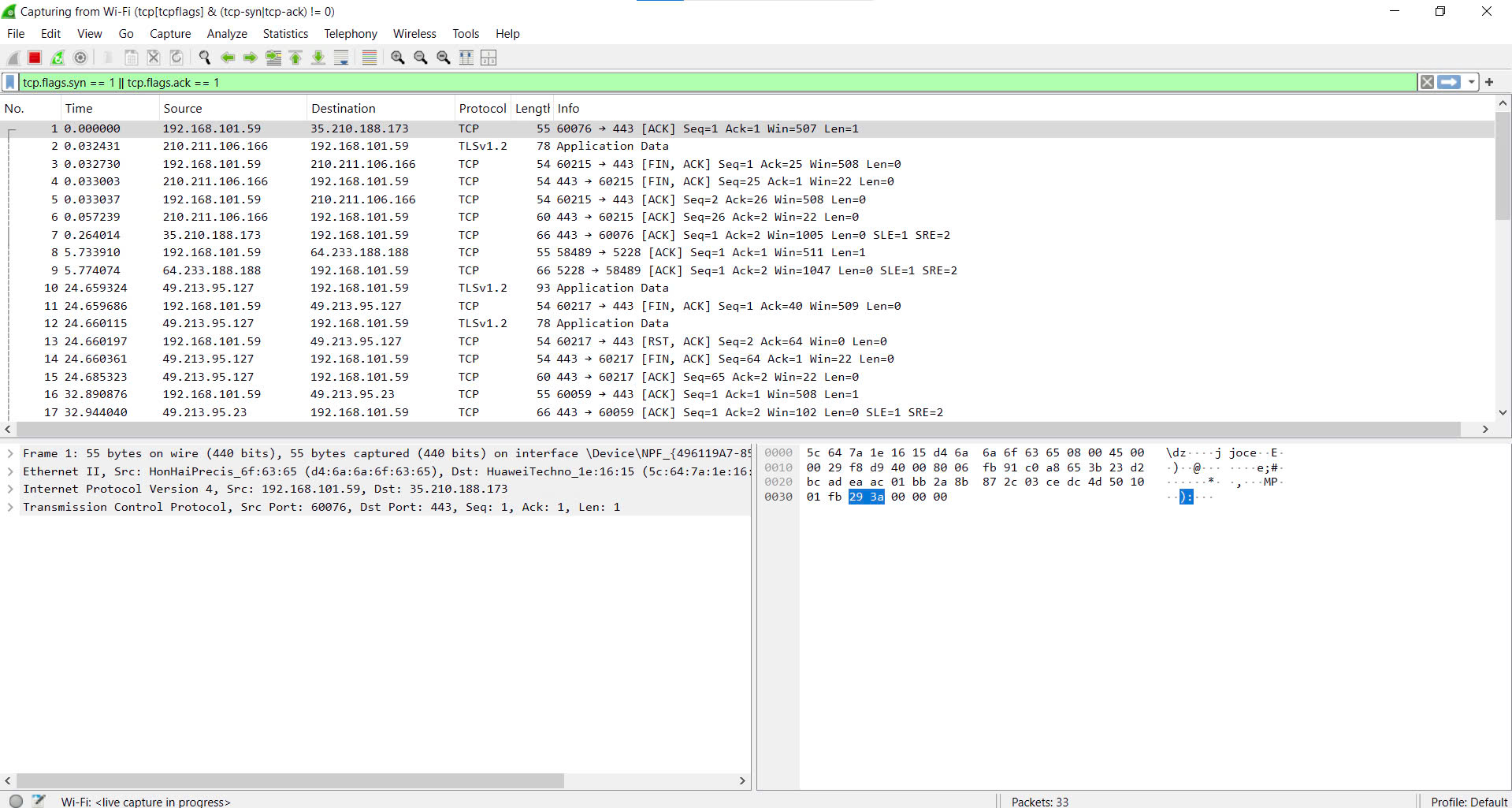
**BÀI THỰC HÀNH 1**

**Bước 1: Mở Wireshark và bắt đầu thu thập gói tin**

1.Mở Wireshark  
2. Chọn card mạng đang sử dụng kết nối Internet (Wi-Fi hoặc Ethernet).  


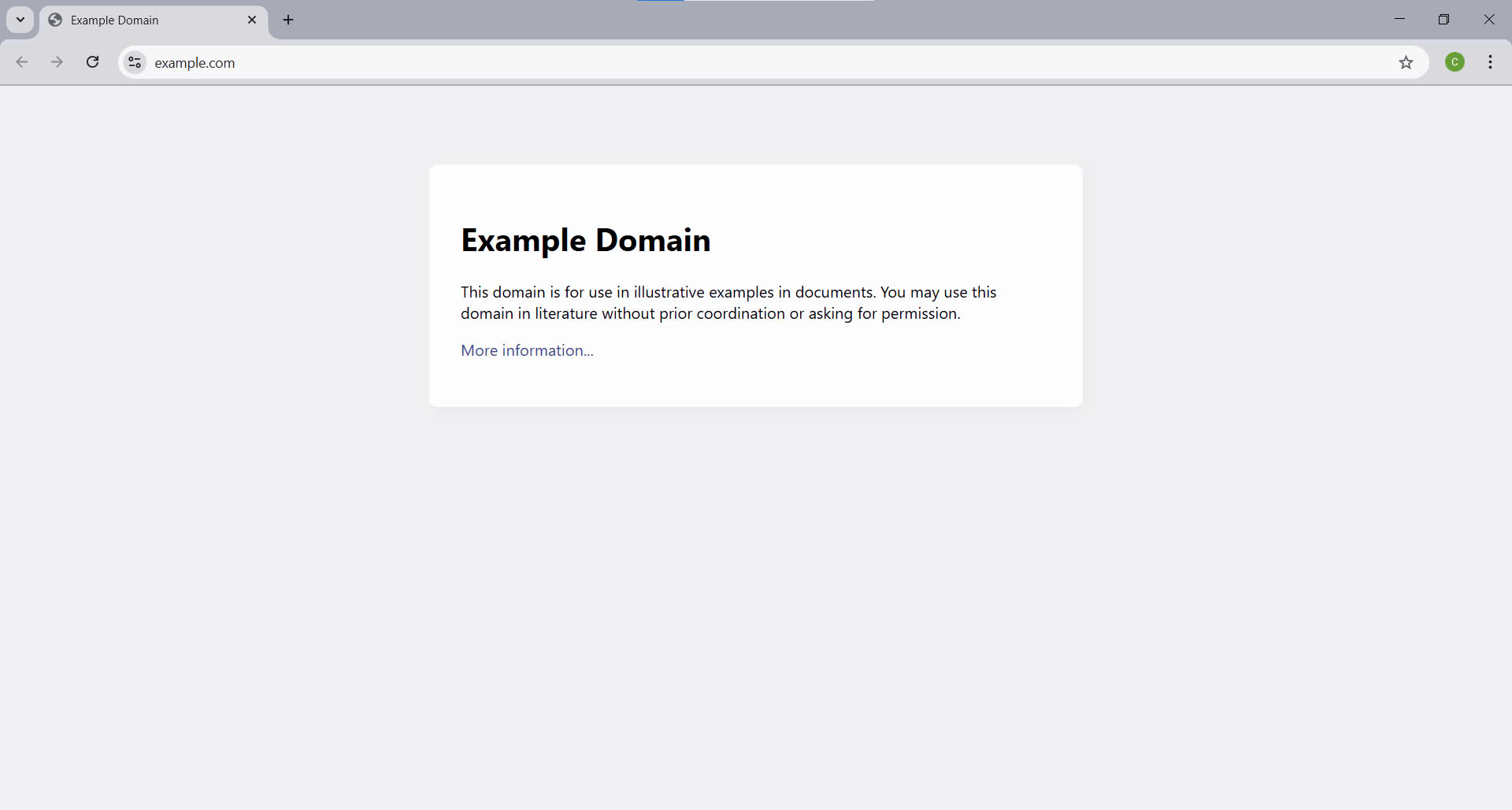
3. Nhập bộ lọc để chỉ hiển thị gói tin TCP liên quan đến quá trình bắt tay:   
3.1. Nếu muốn lọc gói SYN hoặc ACK trong Capture Filter (ô nhập đ/k lọc), dùng cú pháp sau:  
tcp[tcpflags] & (tcp-syn|tcp-ack) != 0  


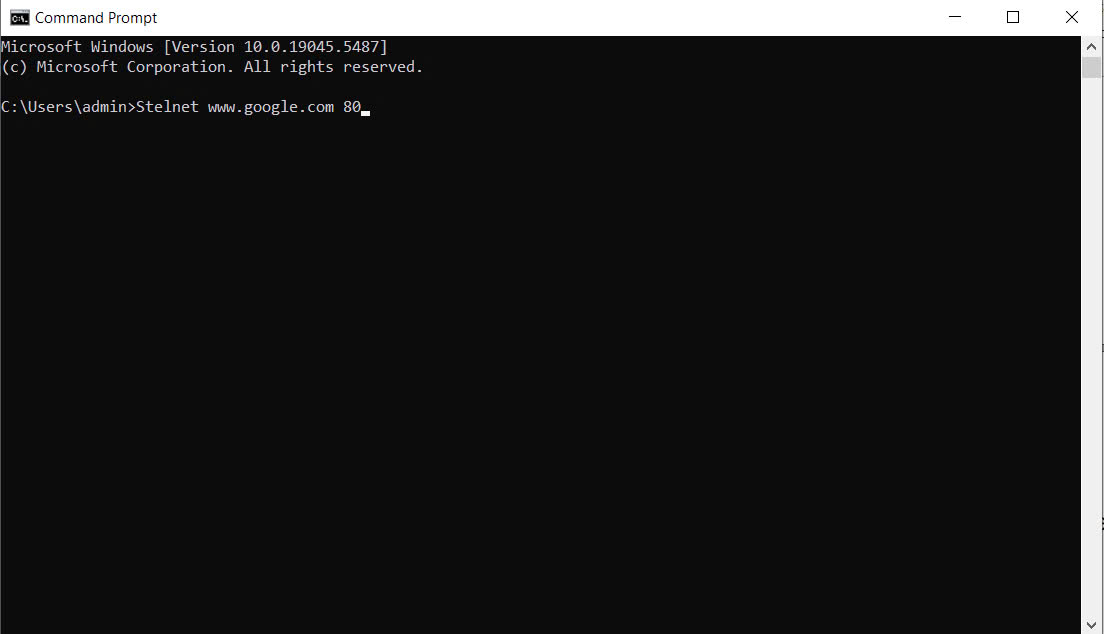
Ấn ENTER => KẾT QUẢ :  
  


3.2. Nếu muốn lọc sau khi đã bắt gói tin (Display Filter), dùng cú pháp:  
 tcp.flags.syn == 1 || tcp.flags.ack == 1  
  


Lưu ý: Display Filter chỉ hoạt động sau khi đã bắt gói tin xong.

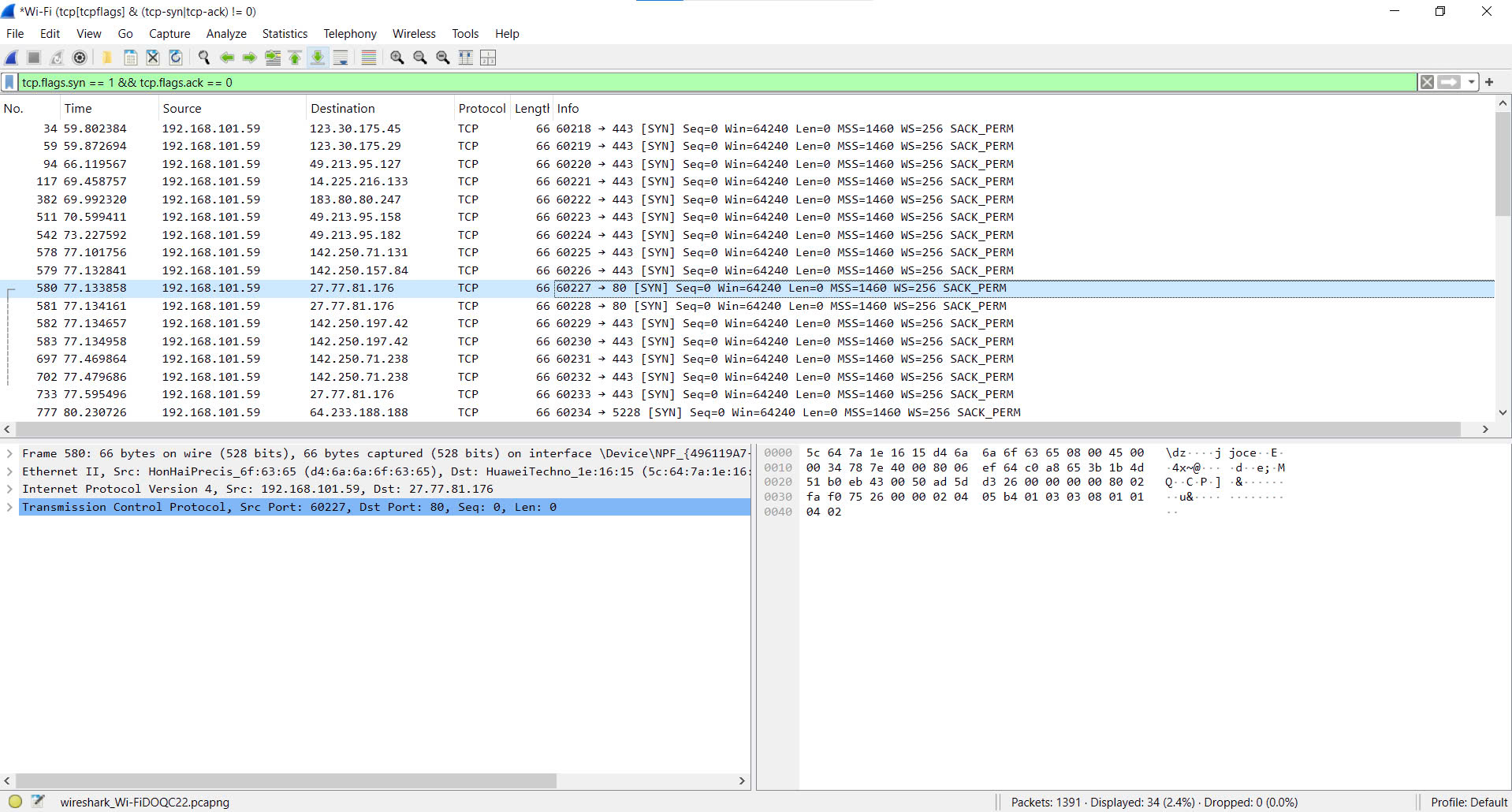
**Bước 2: Khởi tạo kết nối TCP**

Cách 1: Truy cập một trang web bằng trình duyệt  
Mở trình duyệt và nhập một URL (ví dụ: http://www.example.com).   
• Khi nhấn Enter, trình duyệt sẽ thực hiện kết nối TCP đến máy chủ web.  


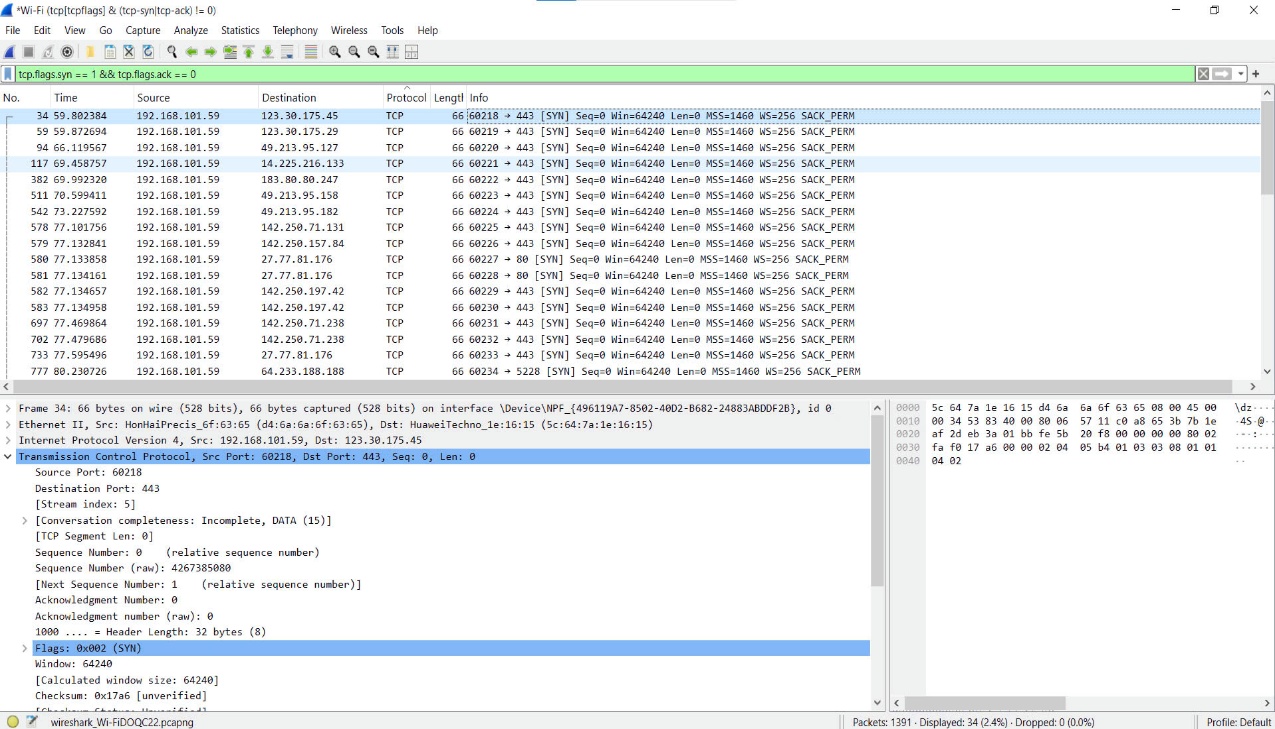
Cách 2: Sử dụng telnet để kết nối đến một máy chủ   
•Mở Command Prompt (Windows) hoặc Terminal (Linux/macOS).   
•Nhập lệnh sau để mở kết nối TCP đến cổng 80 (HTTP) của Google  
 telnet www.google.com 80   
  
  
Nếu telnet hiển thị Connected to www.google.com, nghĩa là kết nối TCP đã được thiết lập

**Bước 3: Phân tích gói tin trong Wireshark**   
Sau khi thực hiện một trong các bước trên, quay lại Wireshark và dừng thu thập gói tin. Nhấn Stop Capture (nút vuông đỏ) sau khi lệnh Telnet thực hiện xong. Chúng ta sẽ thấy một loạt gói TCP. Trong ô Display Filter, nhập bộ lọc sau để chỉ hiển thị gói SYN:   
tcp.flags.syn == 1 && tcp.flags.ack == 0

Nhấn Enter, bạn sẽ thấy gói SYN đầu tiên được gửi từ máy của mình đến [www.google.com](http://www.google.com)

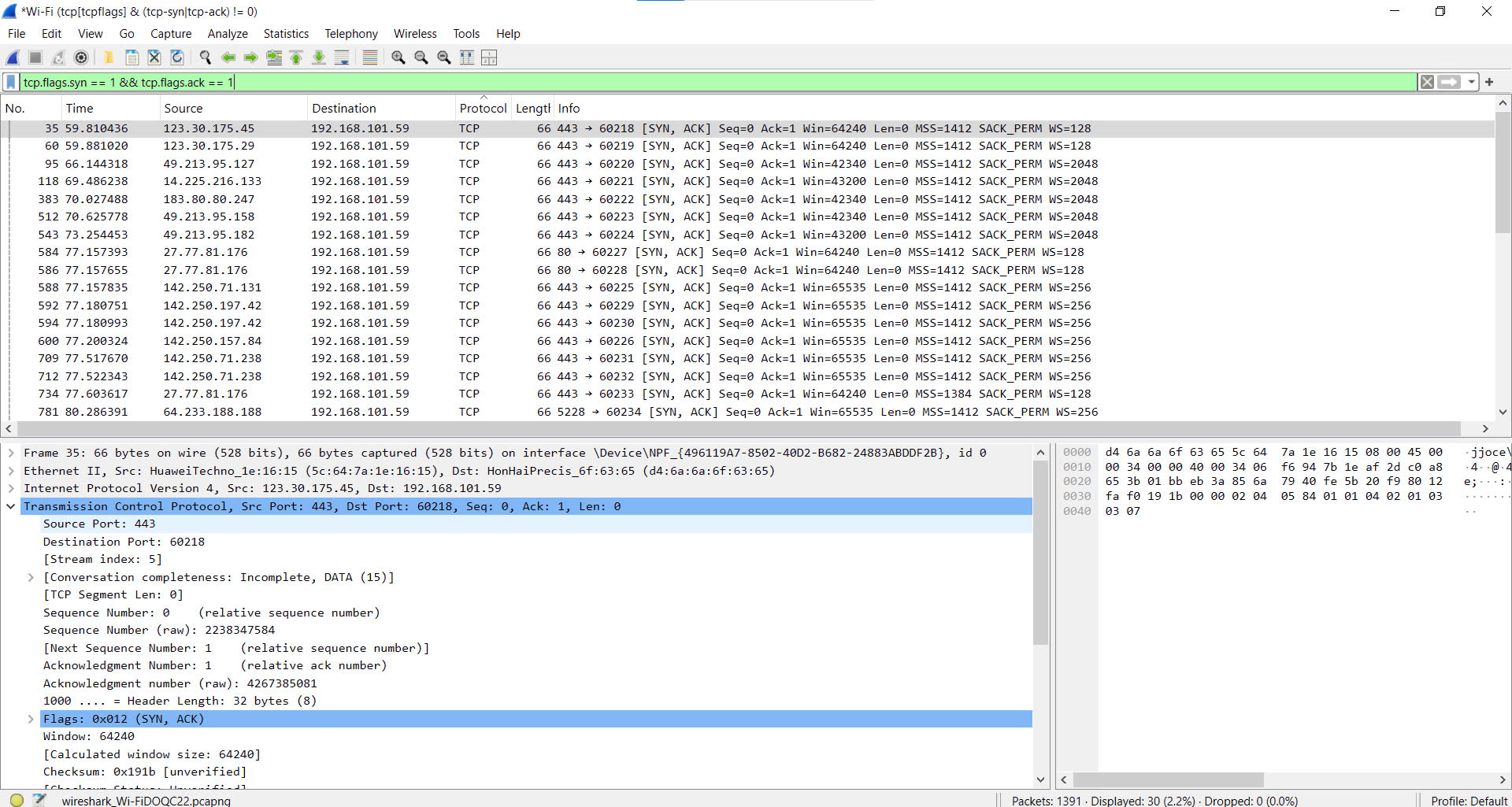


**Bước 4: Phân tích gói SYN**

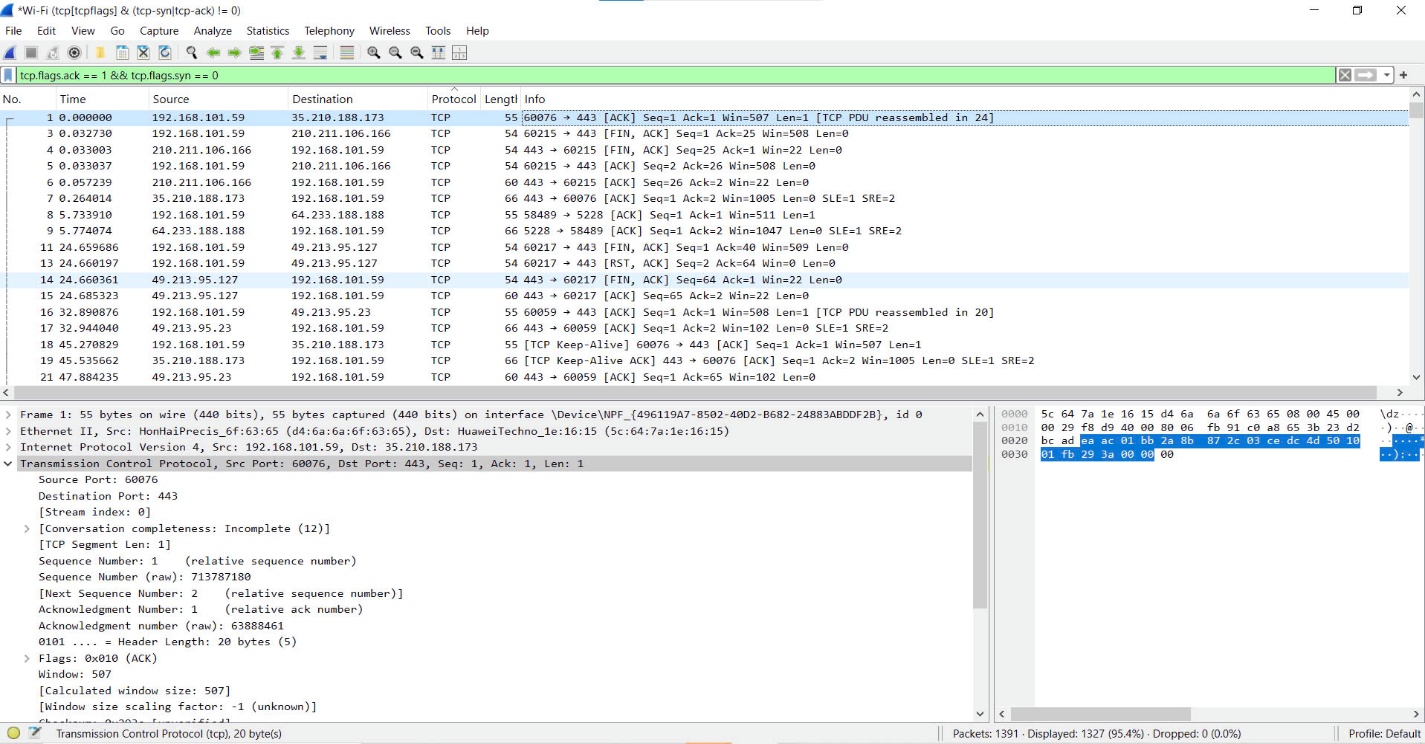
Nhấp vào gói SYN để xem chi tiết. Trong phần Transmission Control Protocol (TCP), kiểm tra các thông tin:   
Flags: SYN = 1, ACK = 0   
Sequence Number: Một số ngẫu nhiên (ví dụ: x = 123456).   
Source IP: IP của máy người dùng (Sender).   
Destination IP: IP của Google (Receiver).   
Source Port: Một cổng ngẫu nhiên (>1024).   
Destination Port: 80 (HTTP).   
  
  
Xác nhận đây là gói SYN khởi tạo kết nối TCP.

**Bước 5: Tìm gói SYN-ACK và ACK để quan sát toàn bộ bắt tay 3 bước**

Tìm gói SYN-ACK từ Google:   
Nhập bộ lọc: tcp.flags.syn == 1 && tcp.flags.ack == 1

  
Kiểm tra: • Flags: SYN = 1, ACK = 1   
 • Acknowledgment Number: x + 1 (phản hồi từ Google).

Tìm gói ACK từ máy người dùng: tcp.flags.ack == 1 && tcp.flags.syn == 0

  
Kiểm tra: Flags: ACK = 1   
Acknowledgment Number: y + 1 (phản hồi từ máy người dùng)