BÀI TẬP THỰC HÀNH CHƯƠNG 1

Họ và tên: Hồ Thị Minh Hằng

Mã sinh viên: 22174600024

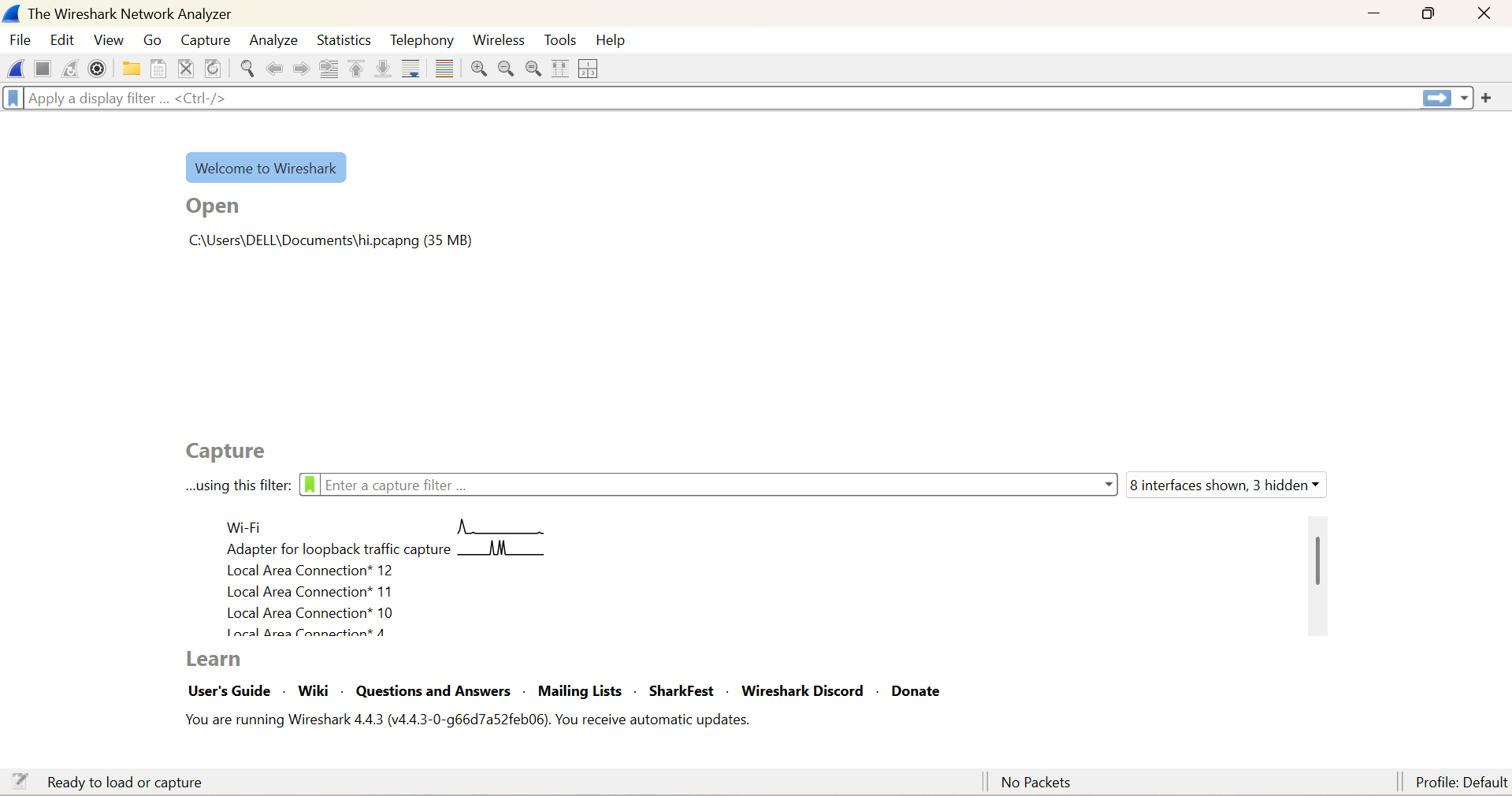
Lớp DHKL16A2HN

---------------------------------

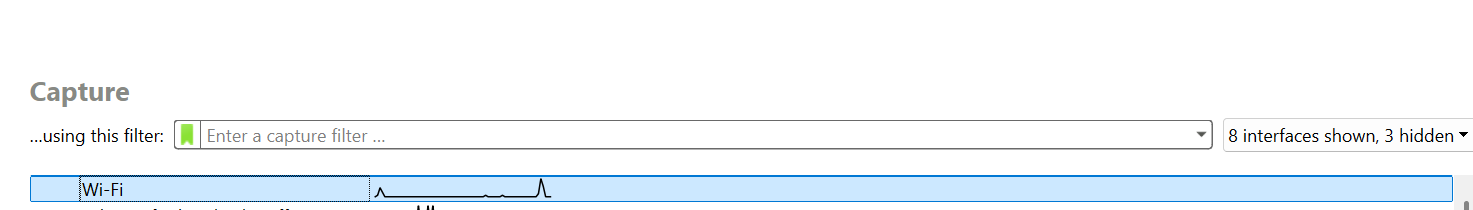
THỰC HÀNH: Hướng dẫn bắt quá trình bắt tay 3 bước TCP bằng Wireshark. Mục tiêu của bài thực hành này là bắt và phân tích quá trình bắt tay 3 bước TCP bằng Wireshark, giúp thấy trực tiếp các gói SYN, SYN-ACK, ACK.

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

1. Mở Wireshark

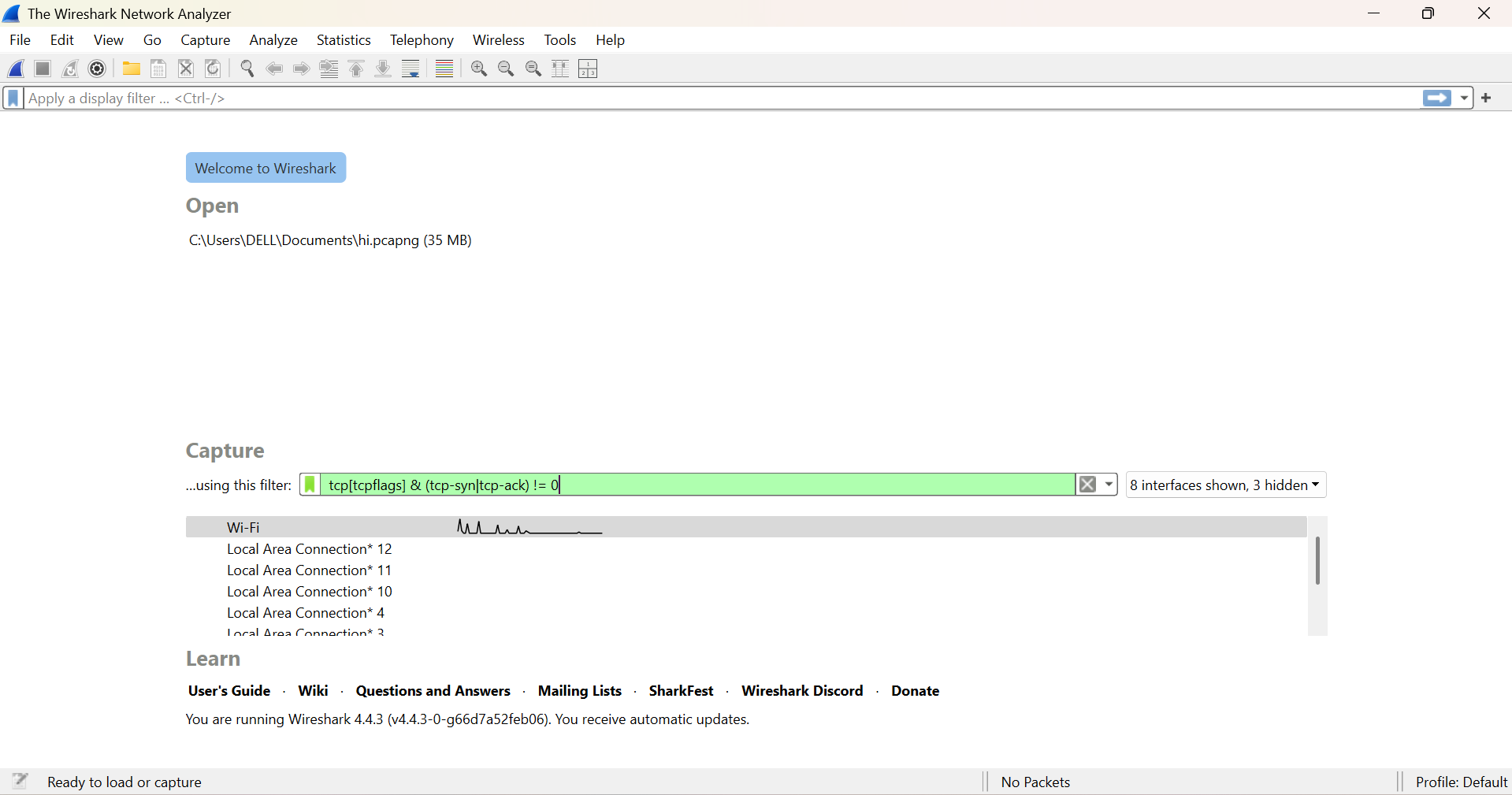


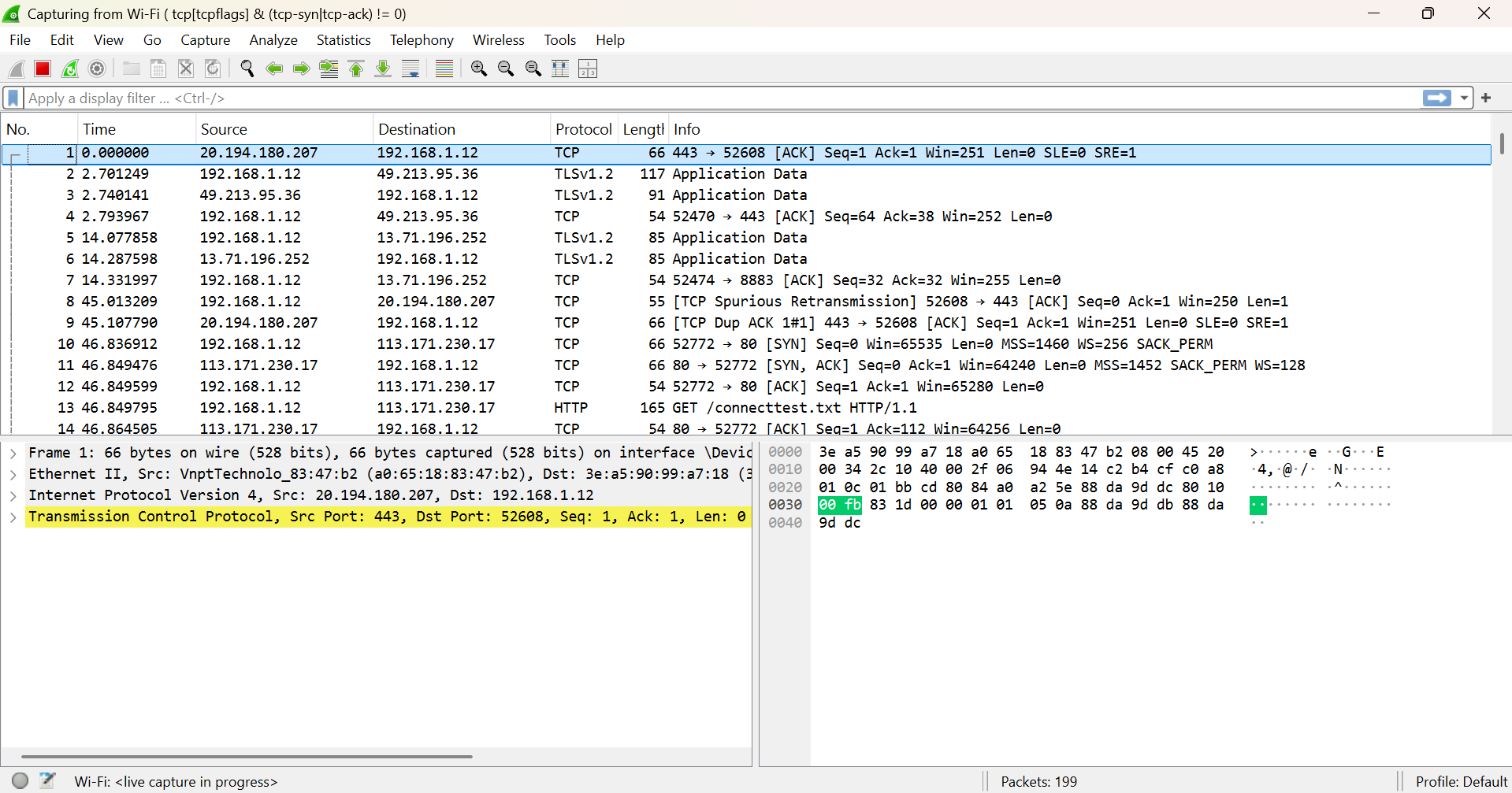
1. Chọn card mạng đang sử dụng kết nối Internet (Wi-Fi hoặc Ethernet).



1. Nhập bộ lọc để chỉ hiển thị gói tin TCP liên quan đến quá trình bắt tay:
   1. Nếu muốn lọc gói SYN hoặc ACK trong Capture Filter (ô nhập đ/k lọc), dùng cú pháp sau:

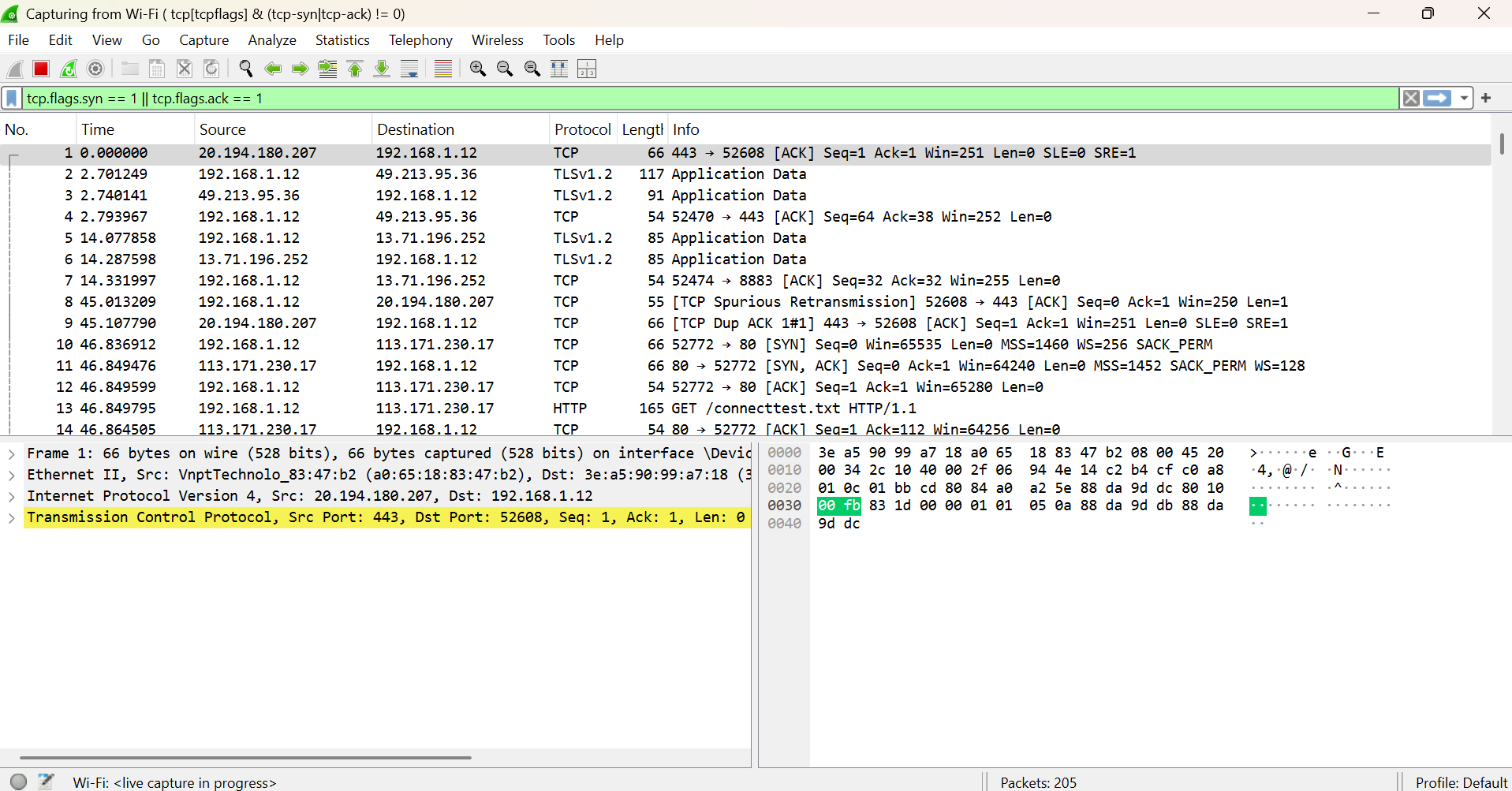




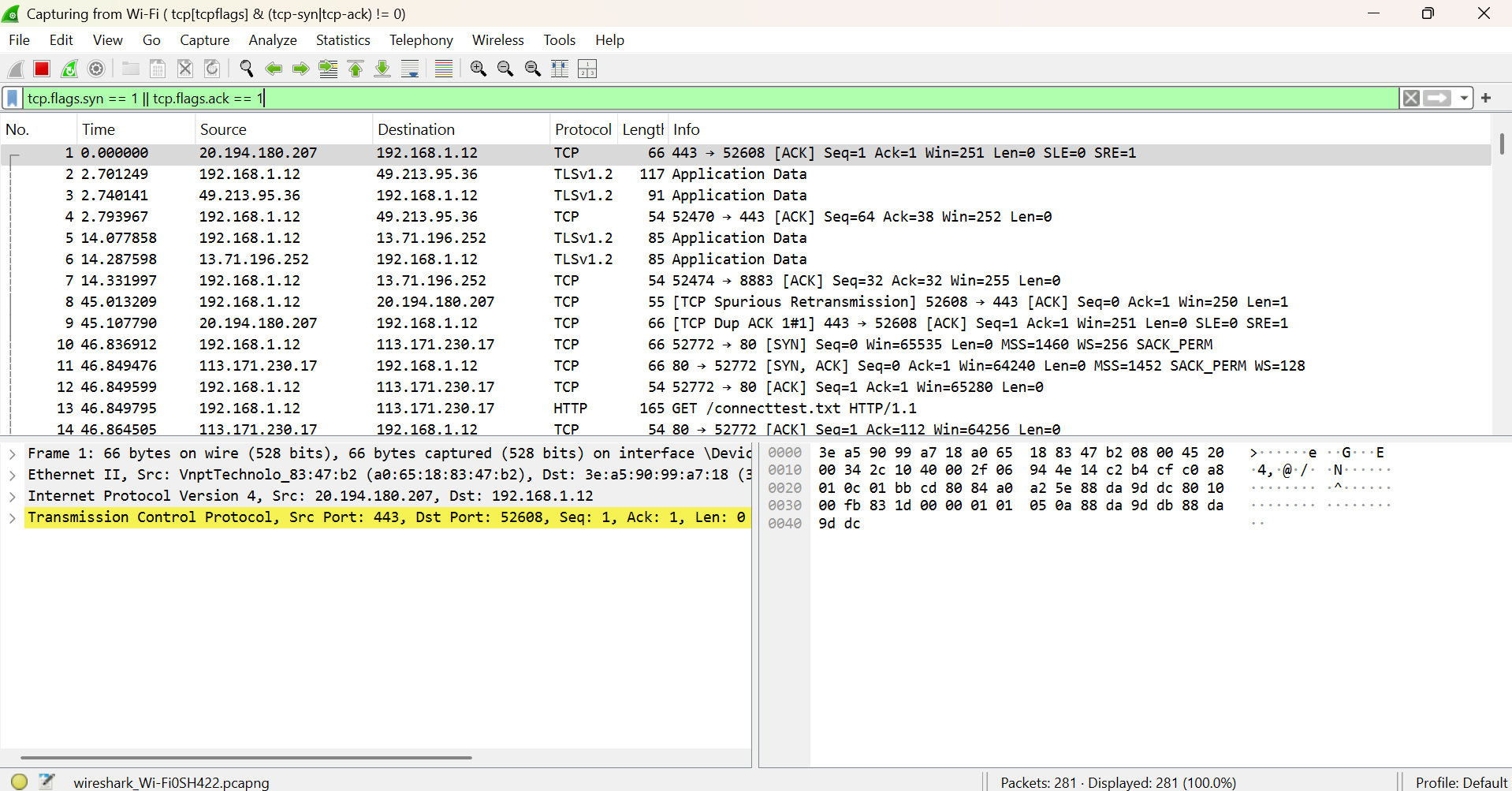


* 1. Nếu muốn lọc sau khi đã bắt gói tin (Display Filter), dùng cú pháp:





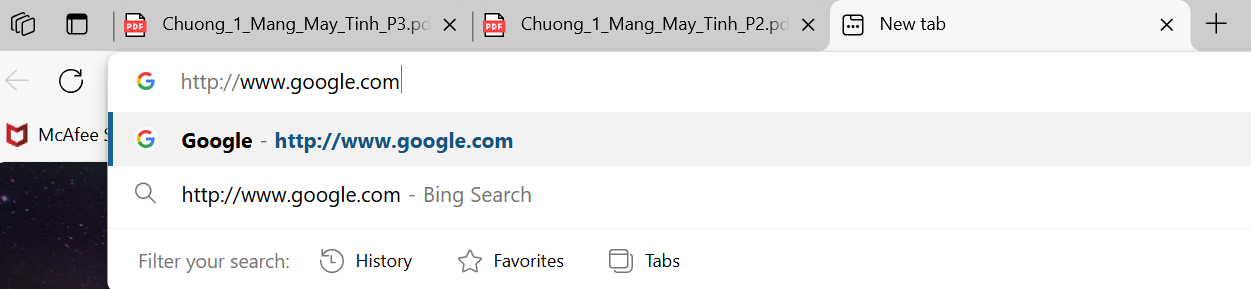
Lưu ý: Display Filter chỉ hoạt động sau khi đã bắt gói tin xong



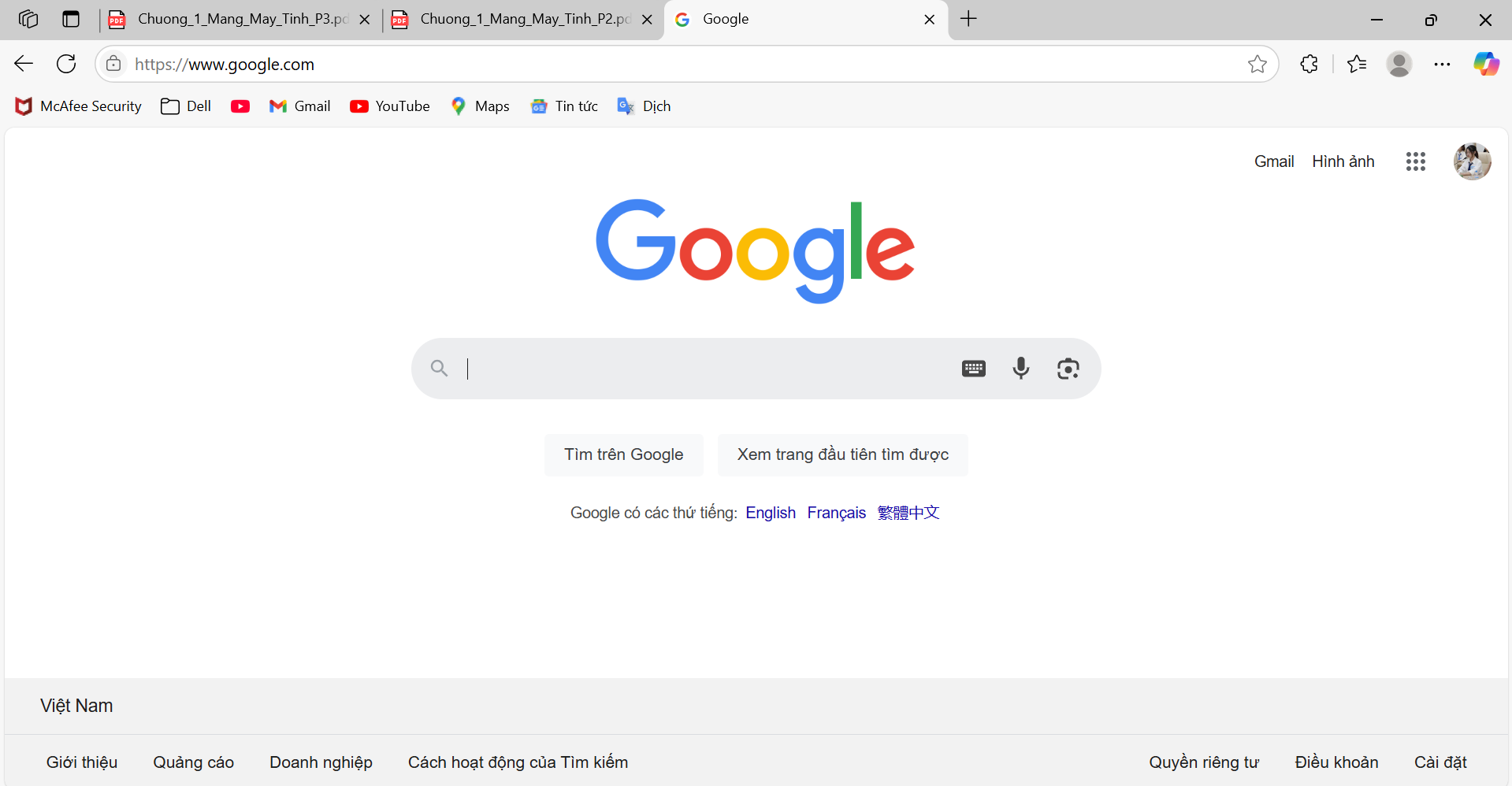
Bước 2: Khởi tạo kết nối TCP

Cách 1: Truy cập một trang web bằng trình duyệt

• Mở trình duyệt và nhập một URL: <http://www.google.com>



• Khi nhấn Enter, trình duyệt sẽ thực hiện kết nối TCP đến máy chủ web.

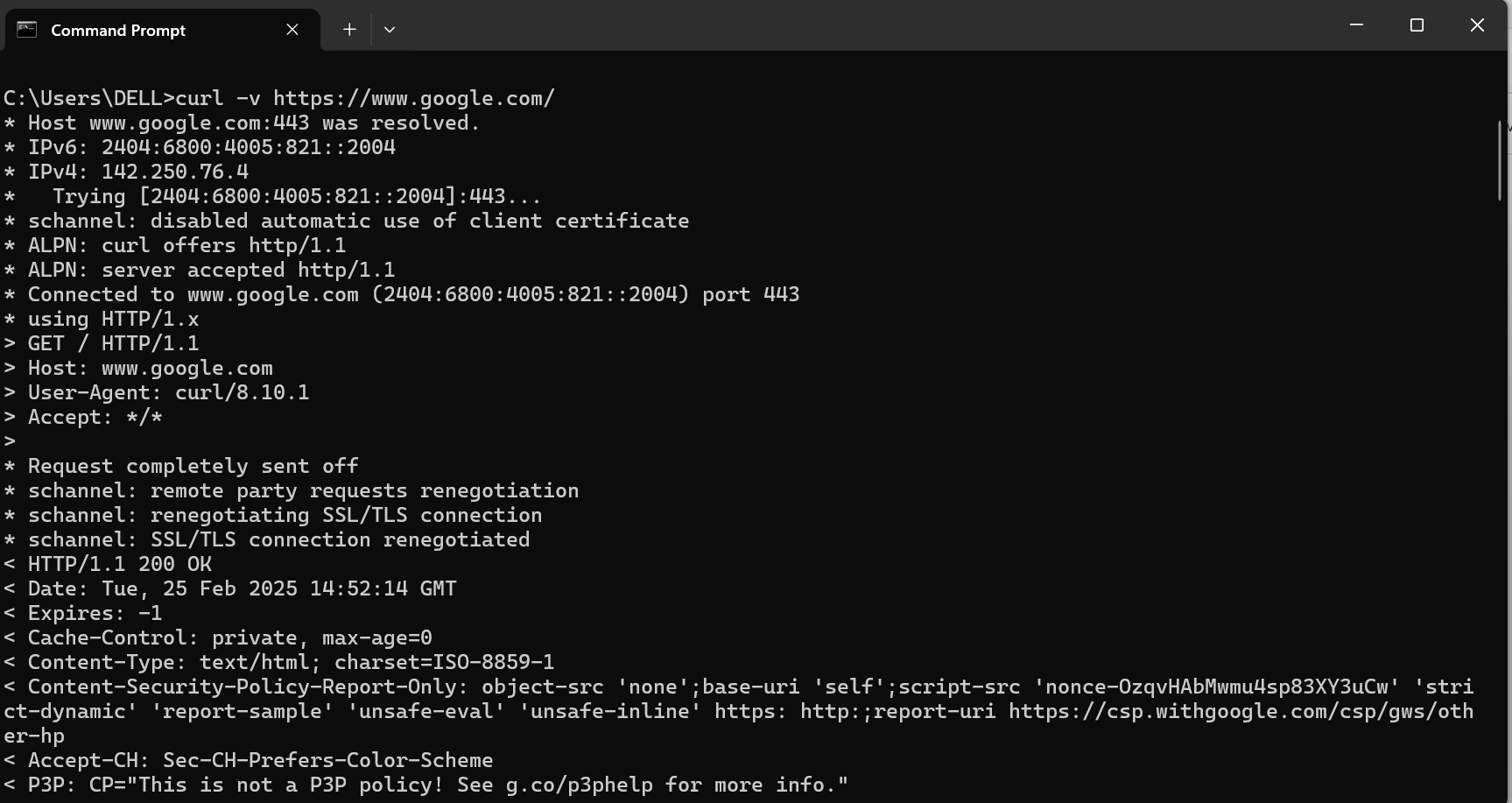


Cách 2: Sử dụng telnet để kết nối đến một máy chủ

Mở Command Prompt (Windows), nhập lệnh sau để mở kết nối TCP đến cổng 80 (HTTP) của Google



Nếu telnet hiển thị Connected to www.google.com, nghĩa là kết nối TCP đã được thiết lập.

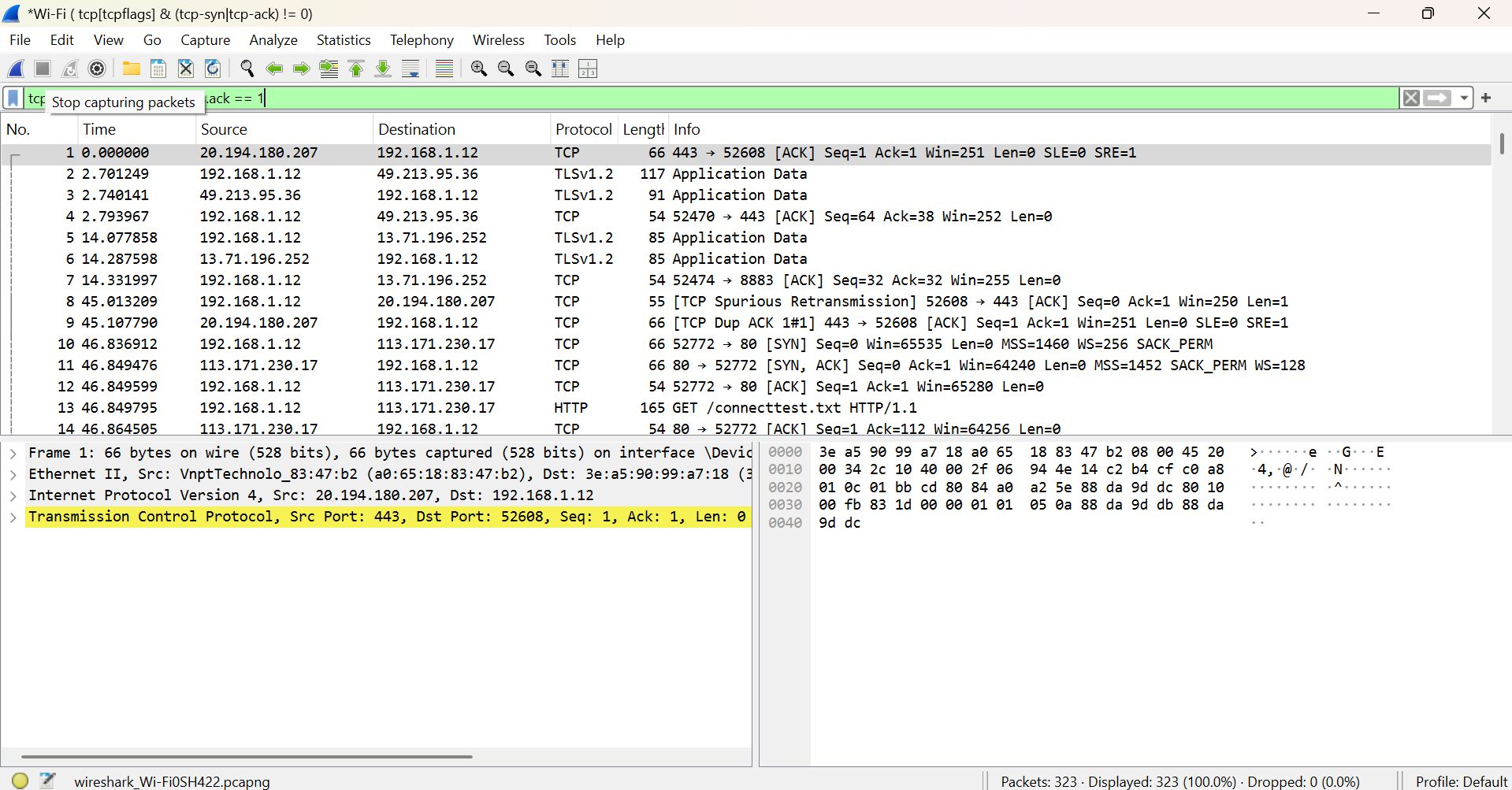




Bước 3: Phân tích gói tin trong Wireshark

Sau khi thực hiện một trong các bước trên, quay lại Wireshark và dừng thu thập gói tin.

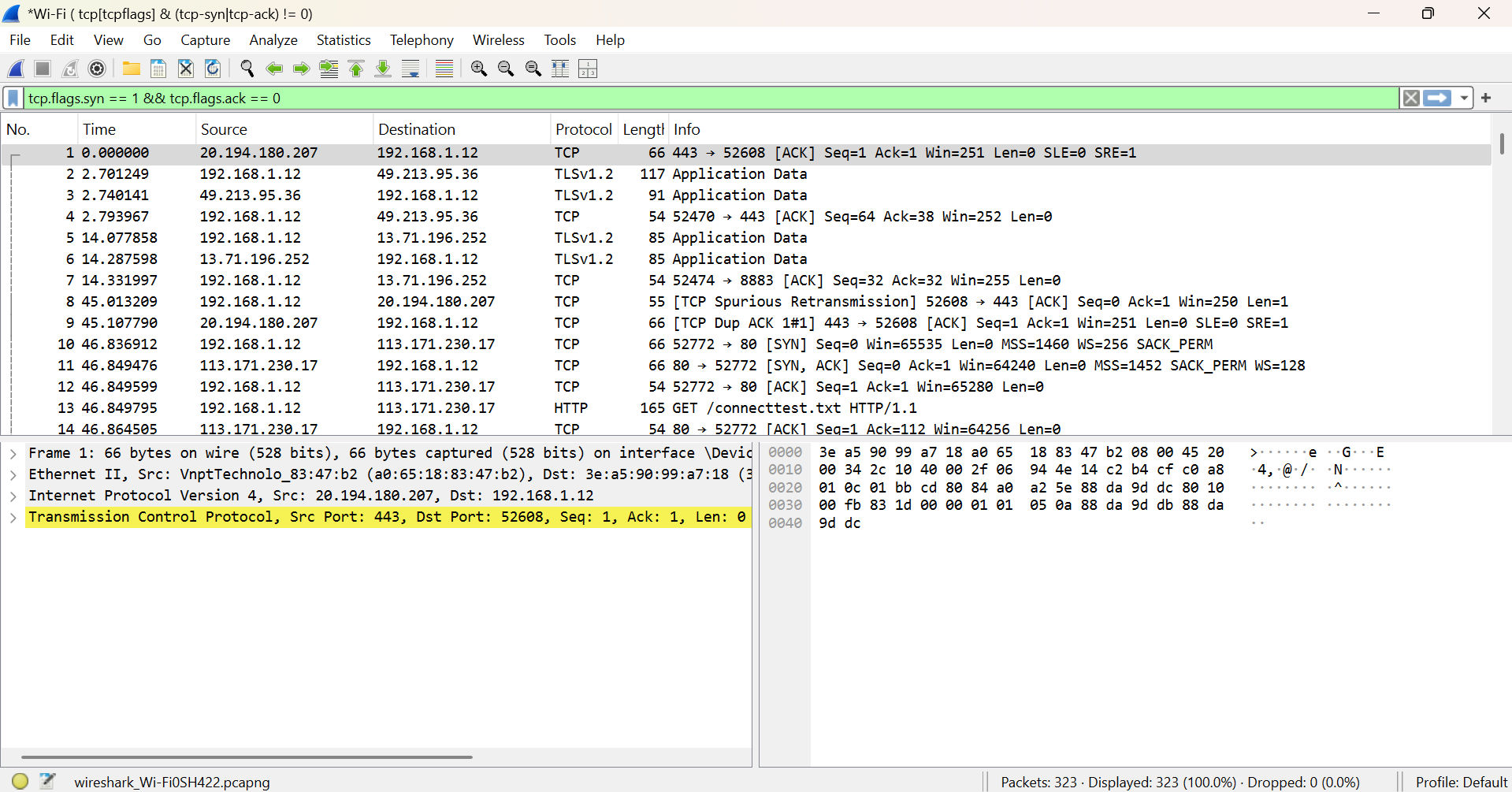
nhấn Stop Capture (nút vuông đỏ) sau khi lệnh Telnet thực hiện xong.



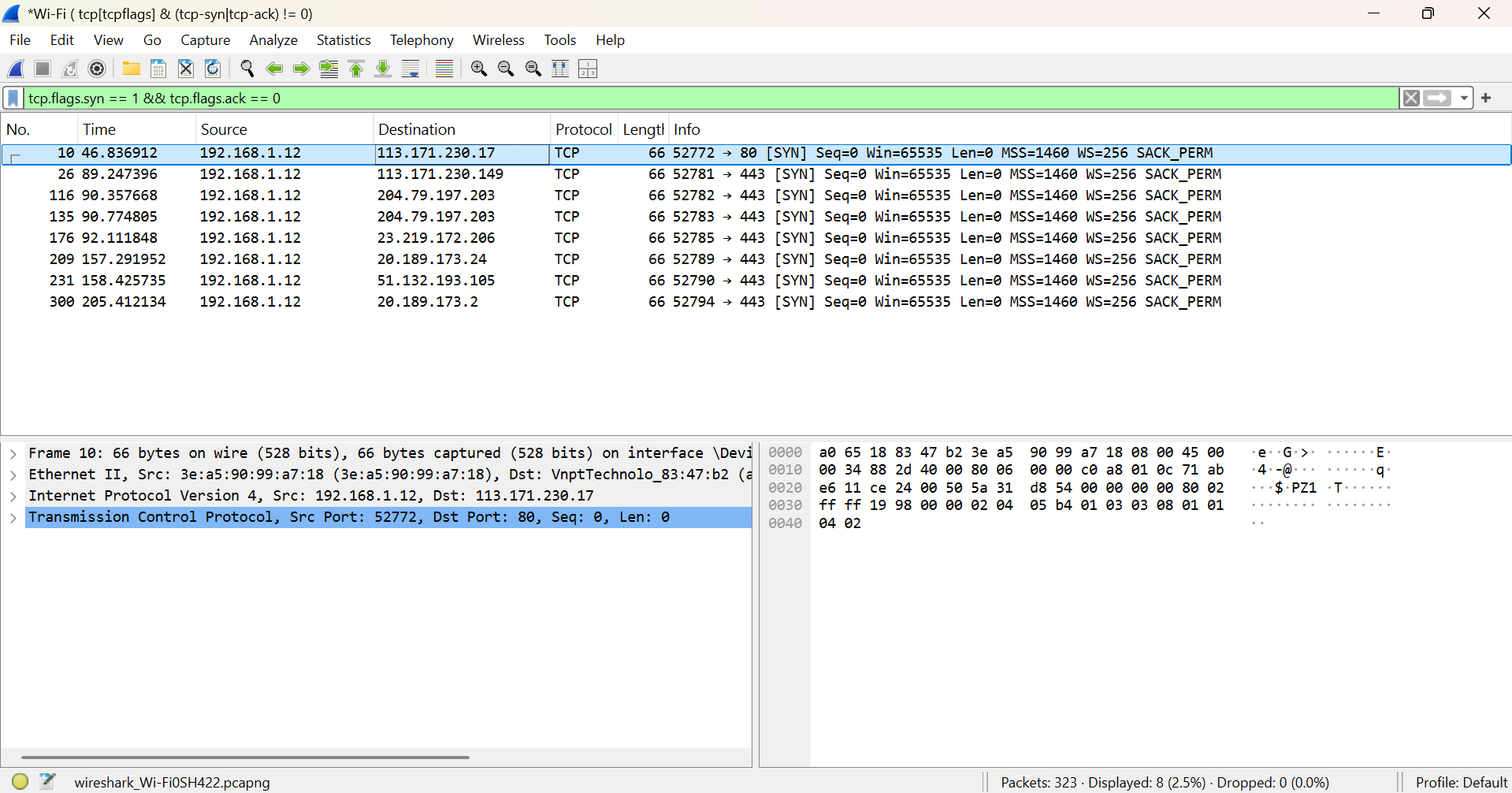
Chúng ta sẽ thấy một loạt gói TCP.

Trong ô Display Filter, nhập bộ lọc sau để chỉ hiển thị gói SYN:



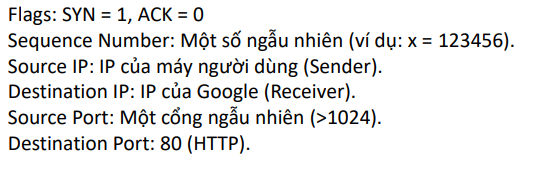


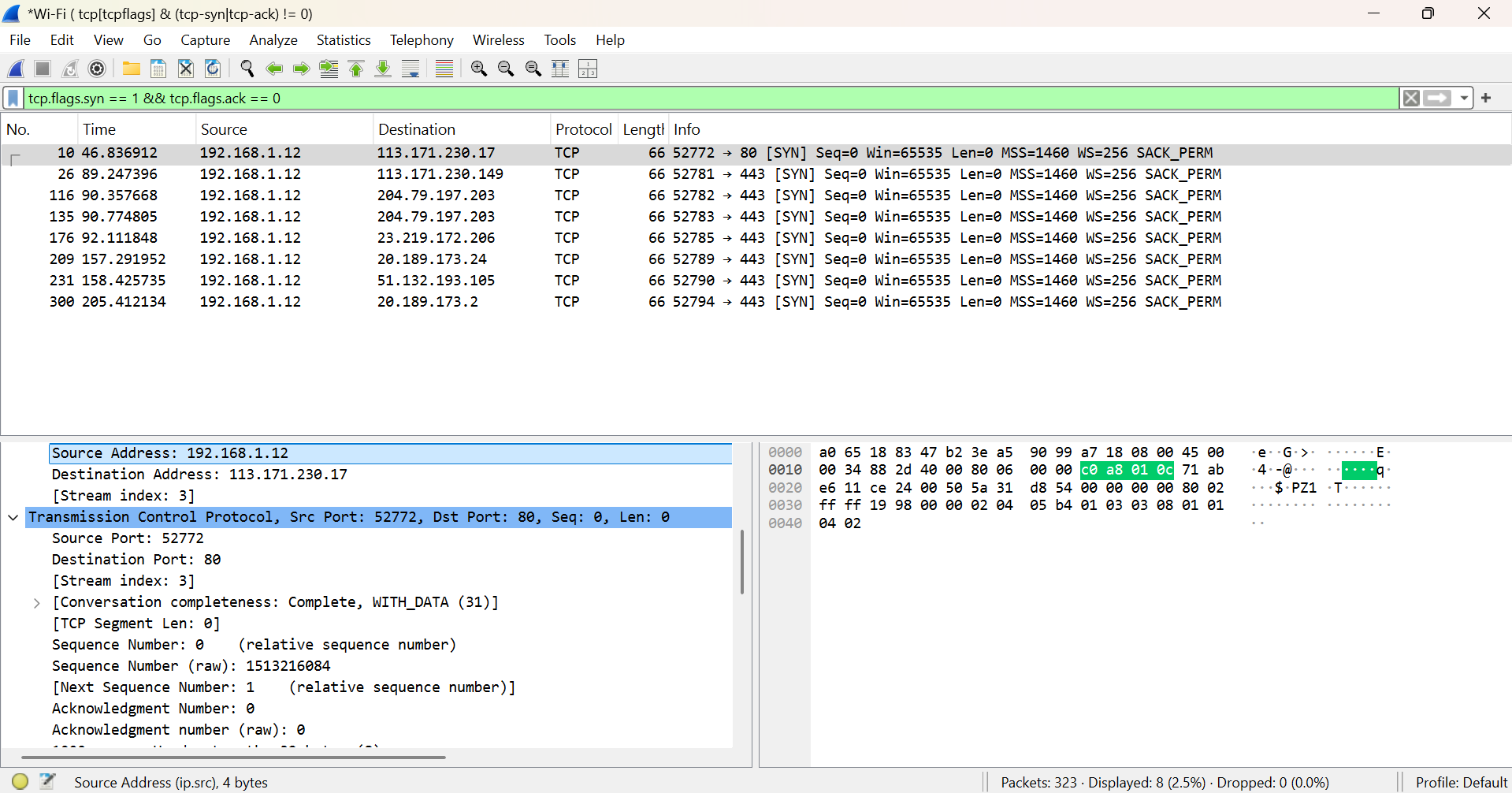
Nhấn Enter sẽ thấy gói SYN đầu tiên được gửi từ máy của mình đến [www.google.com](http://www.google.com)



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

Squence Number: 1513216084

Source IP:192.168.1.12

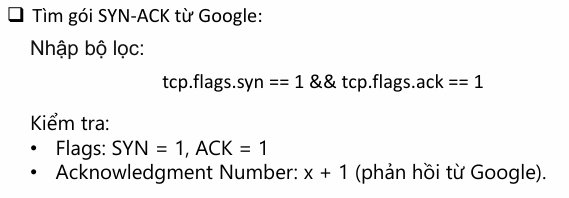
Destination IP: 113.171.230.17

Source Port: 52772

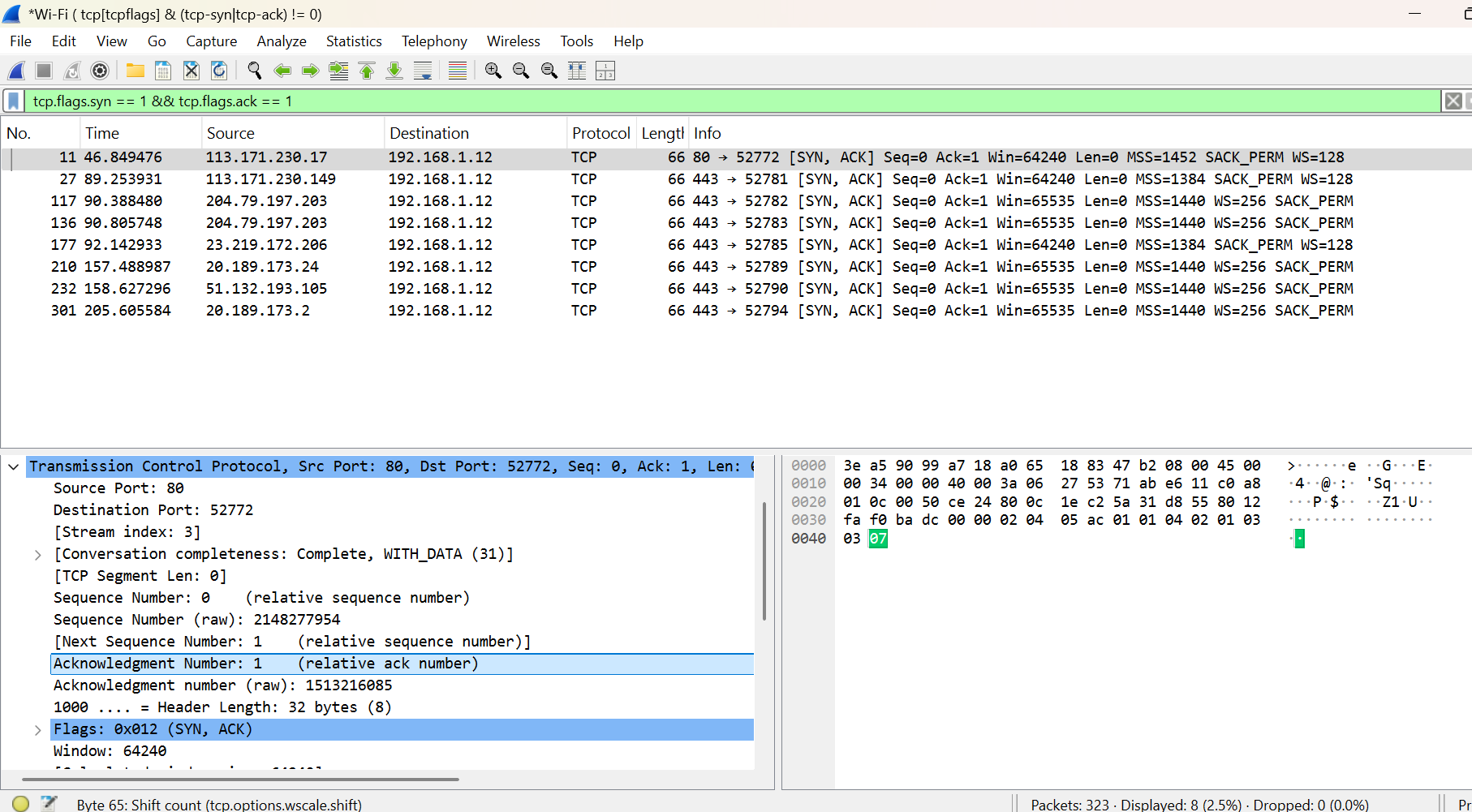
Destination Port: 80

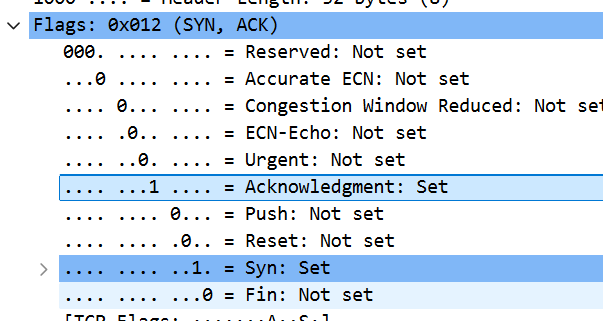
Xác nhận đây là gói SYN khởi tạo kết nối TCP.

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



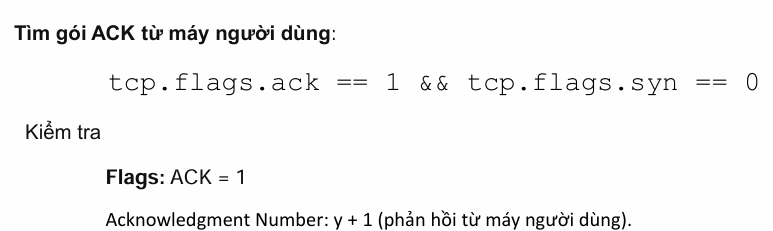
Sau khi thực hiện:



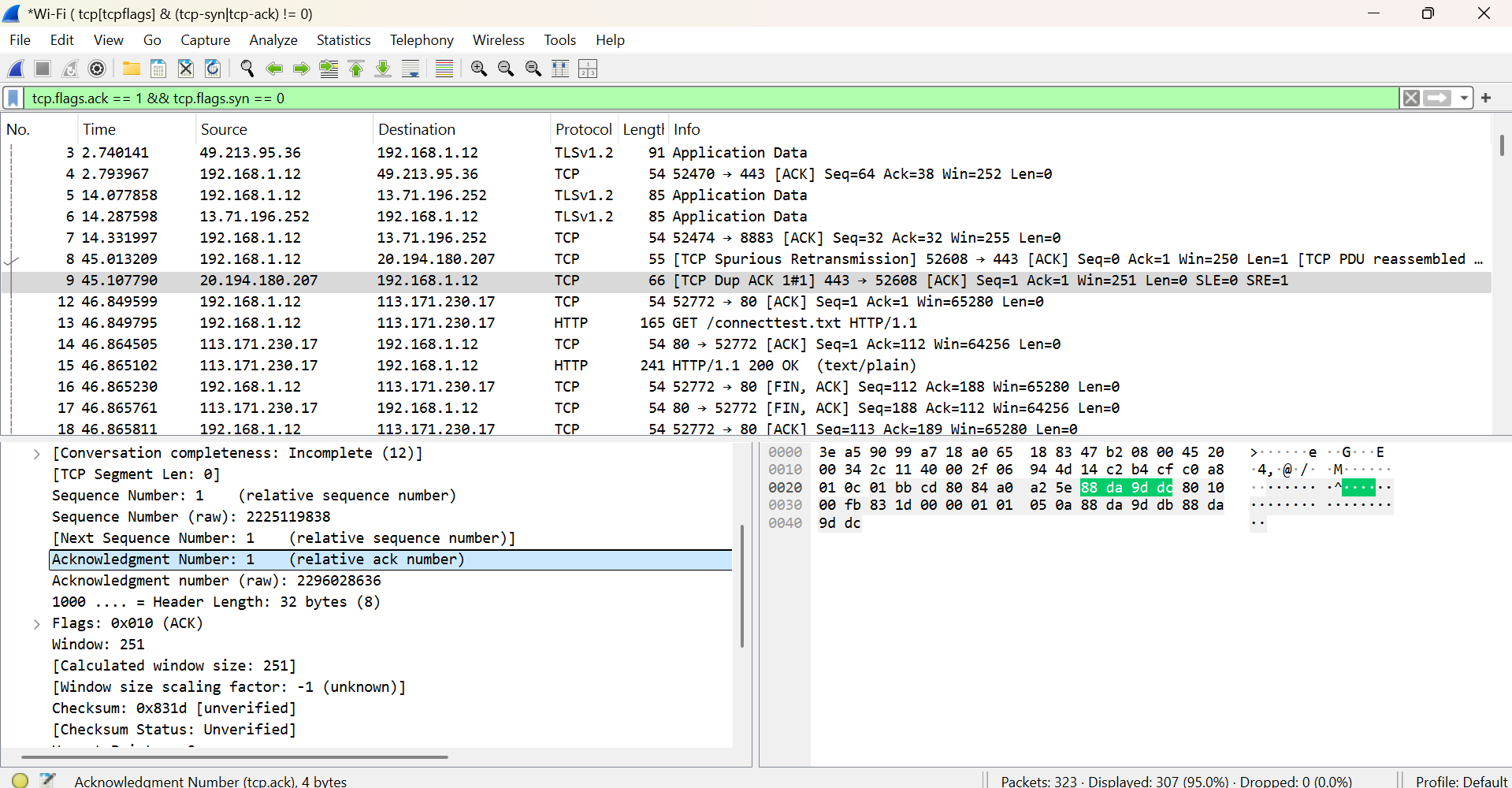


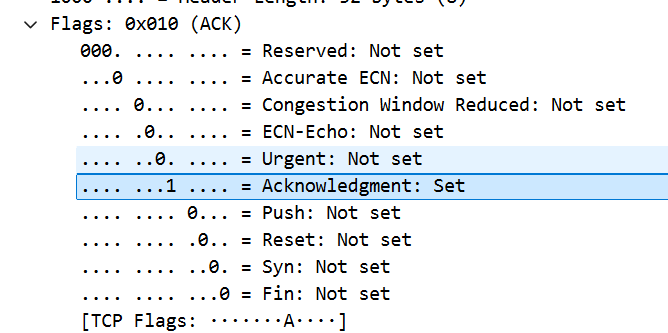
Ta thấy: Flags: SYN = 1, ACK = 1

Acknowledgment Number: 1



Sau khi thực hiện:





Ta thấy:

Ta thấy: Flags: ACK = 1

Acknowledgment Number: 1