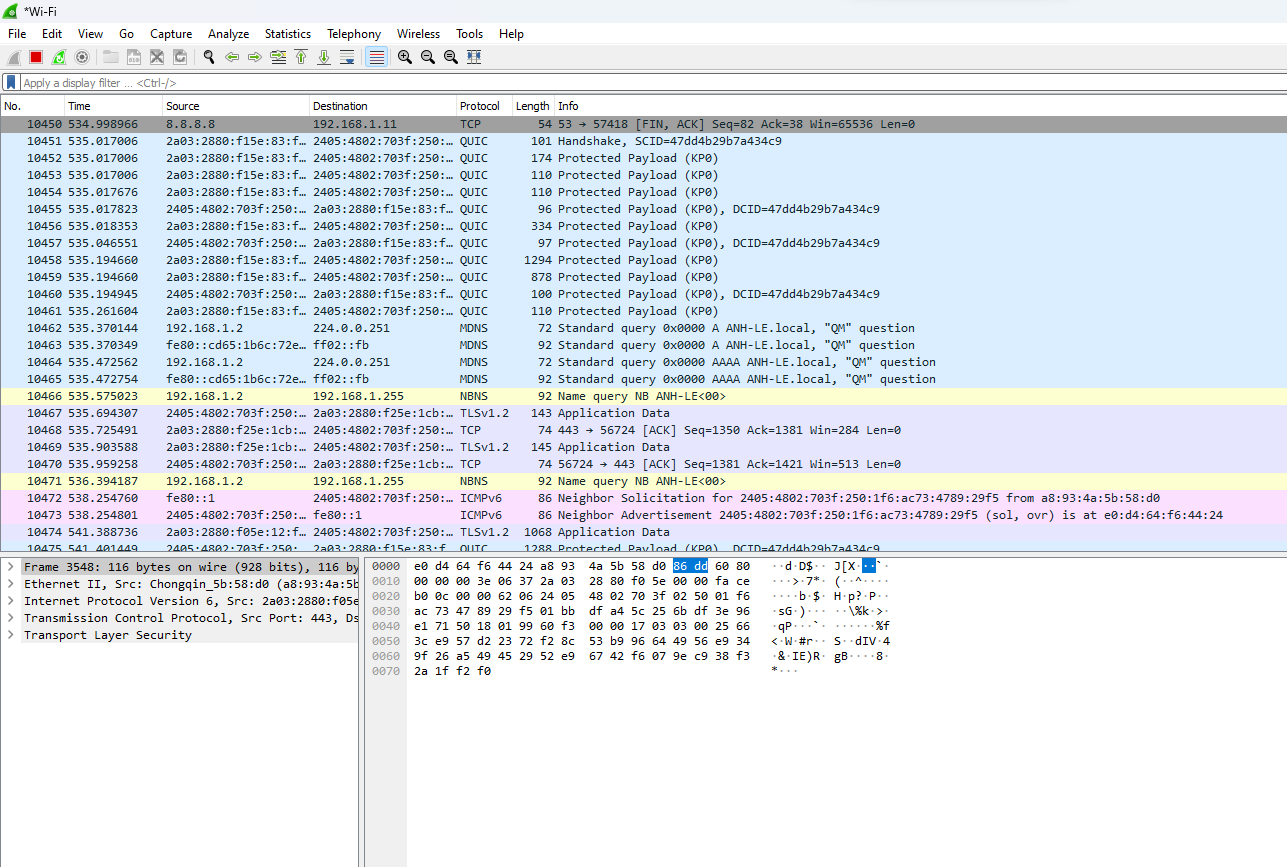
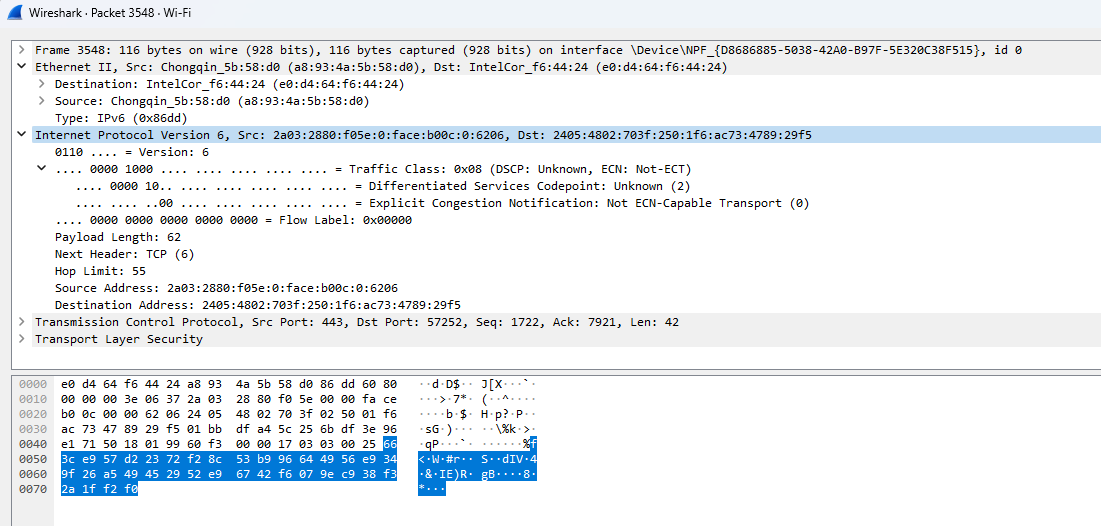
|  |  |
| --- | --- |
| Họ và tên: Trần Đức Trí | Nhóm: 21Nh15 |
| MSSV: 102210096 | Lớp: 21TCLC\_KHDL |

**LAB 11: BẮT VÀ PHÂN TÍCH GÓI TIN VỚI WIRESHARK**

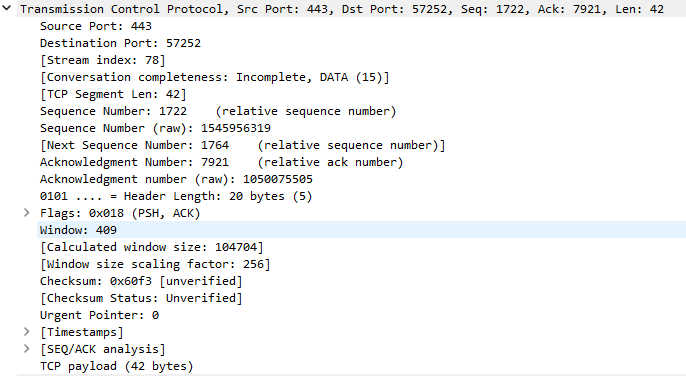
**1. Xem nội dung các gói tin bắt được trên cửa sổ WireShark**



*Xem địa chỉ nguồn, địa chỉ đích của từng gói tin*



*Xem nội dung các tiêu đề của mỗi gói tin*

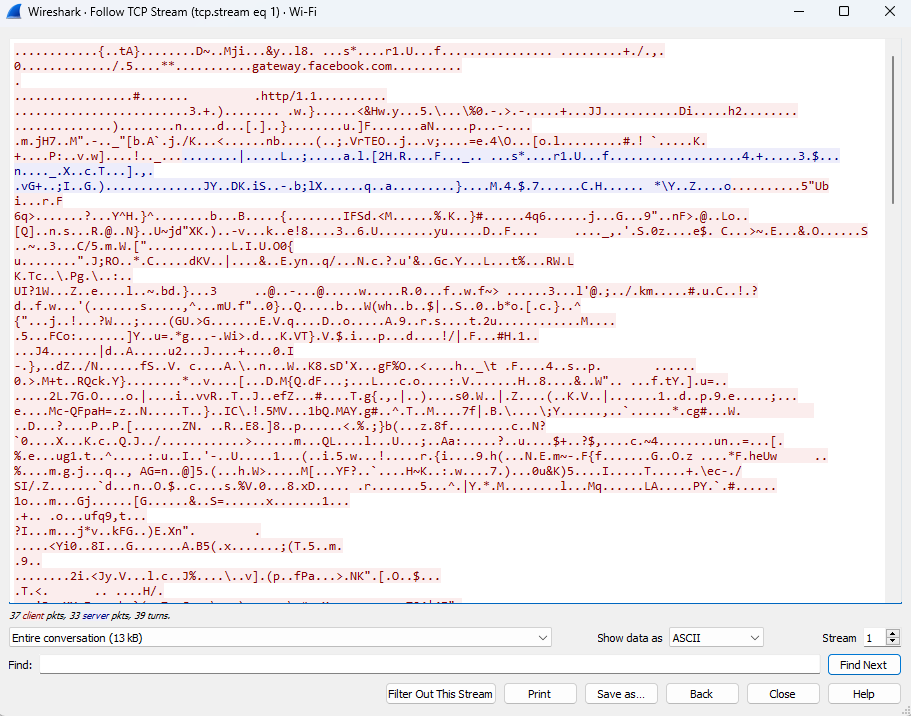


|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 443 | | | | | | | | 57252 |
| 1545956319 | | | | | | | | |
| 1050075505 | | | | | | | | |
| 20 | 000 | 0 | 1 | 1 | 0 | 0 | 0 | 104704 |
| 0x60f3 | | | | | | | | 0 |
|  | | | | | | | | |

*TCP header*

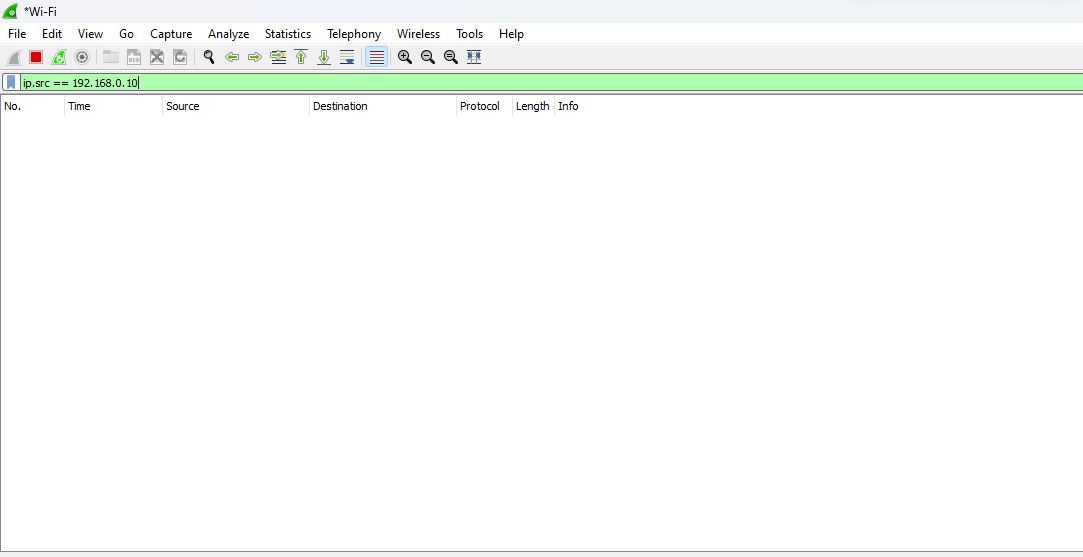
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0100 | 0101 | 0x00 | | 40 | | | |
| 0x065c | | | | 0 | 1 | 0 | 0 |
| 128 | | | TCP(6) | 0x0000 | | | |
| 192.168.1.1 | | | | | | | |
| 210.245.31.221 | | | | | | | |
|  | | | | | | | |

*IP Header*

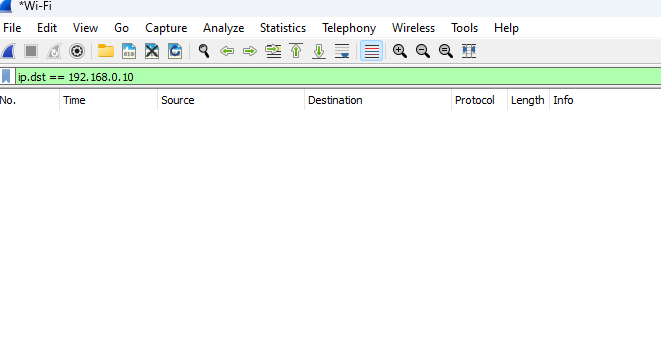


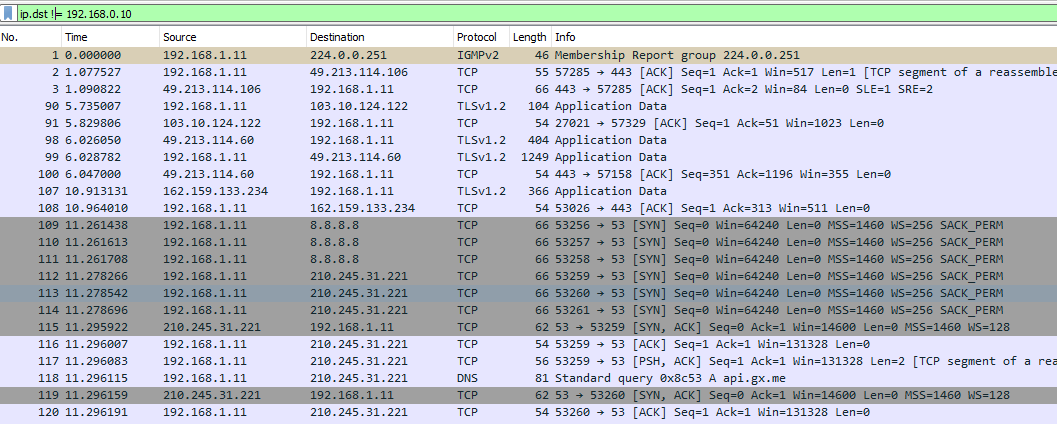
*Xem nội dung hexa, ascii của từng gói tin*

**2. Lọc các gói tin theo địa chỉ IP nguồn**

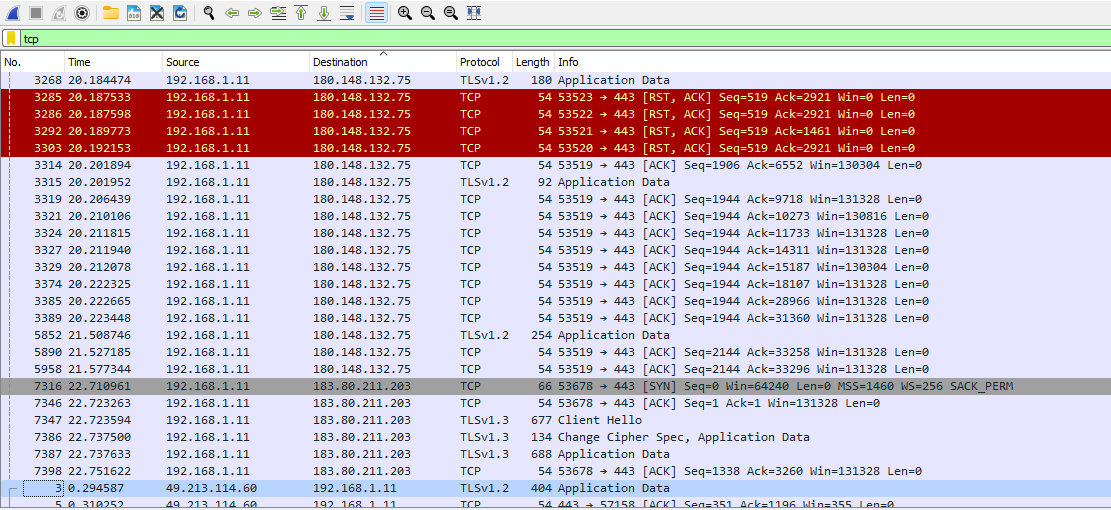


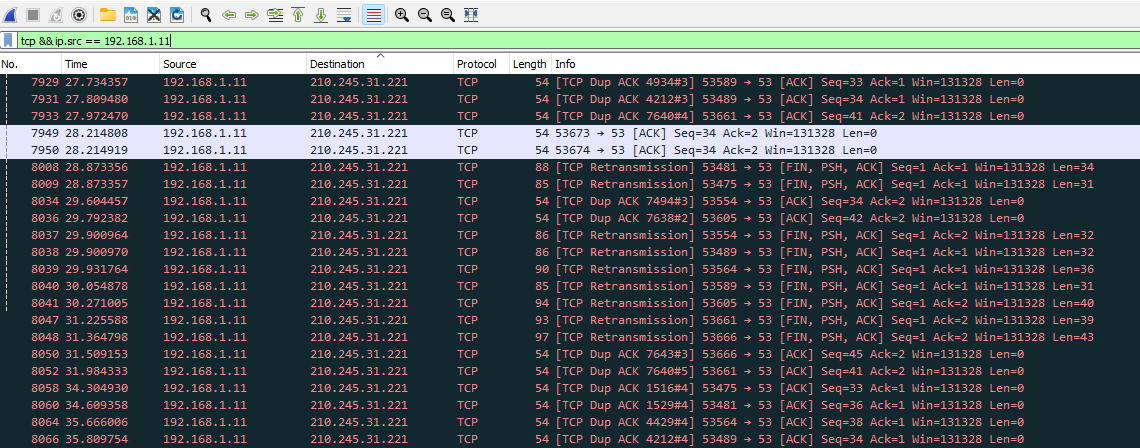
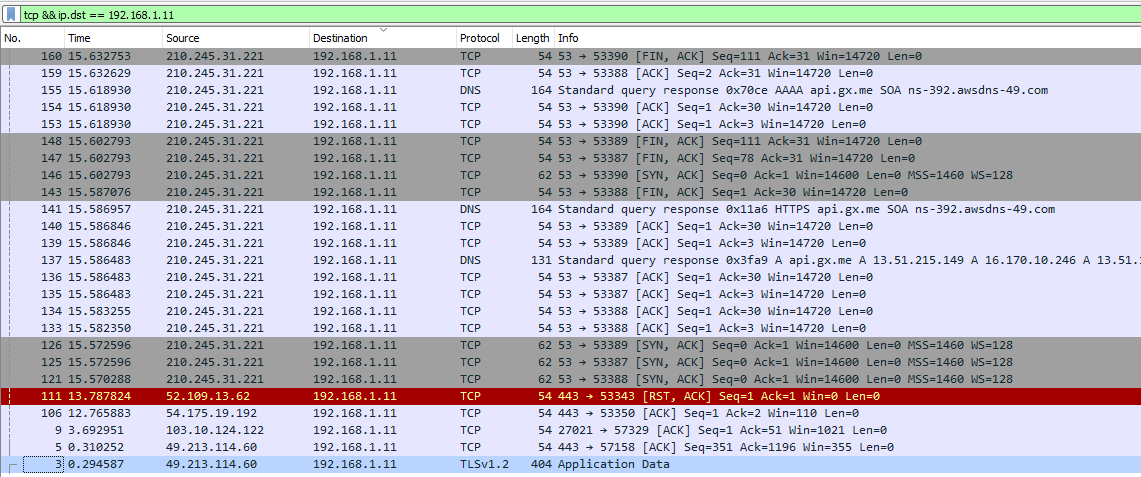
**3. Lọc các gói tin theo địa chỉ IP đích**

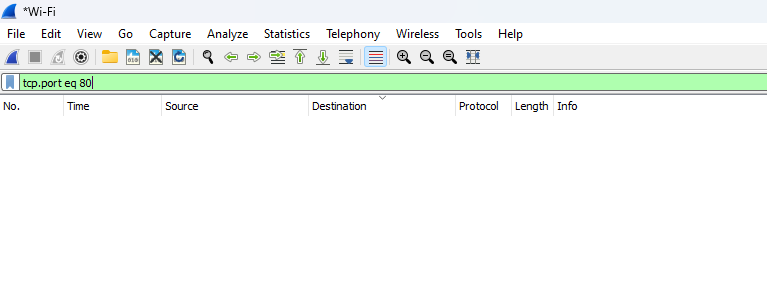




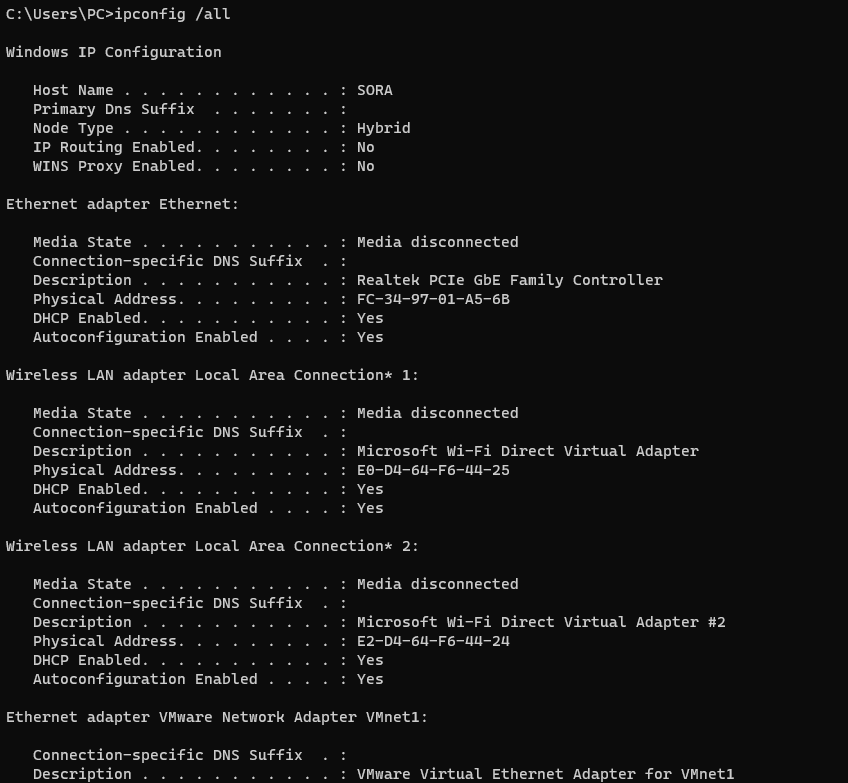
**4. Lọc các gói tin theo giao thức TCP**

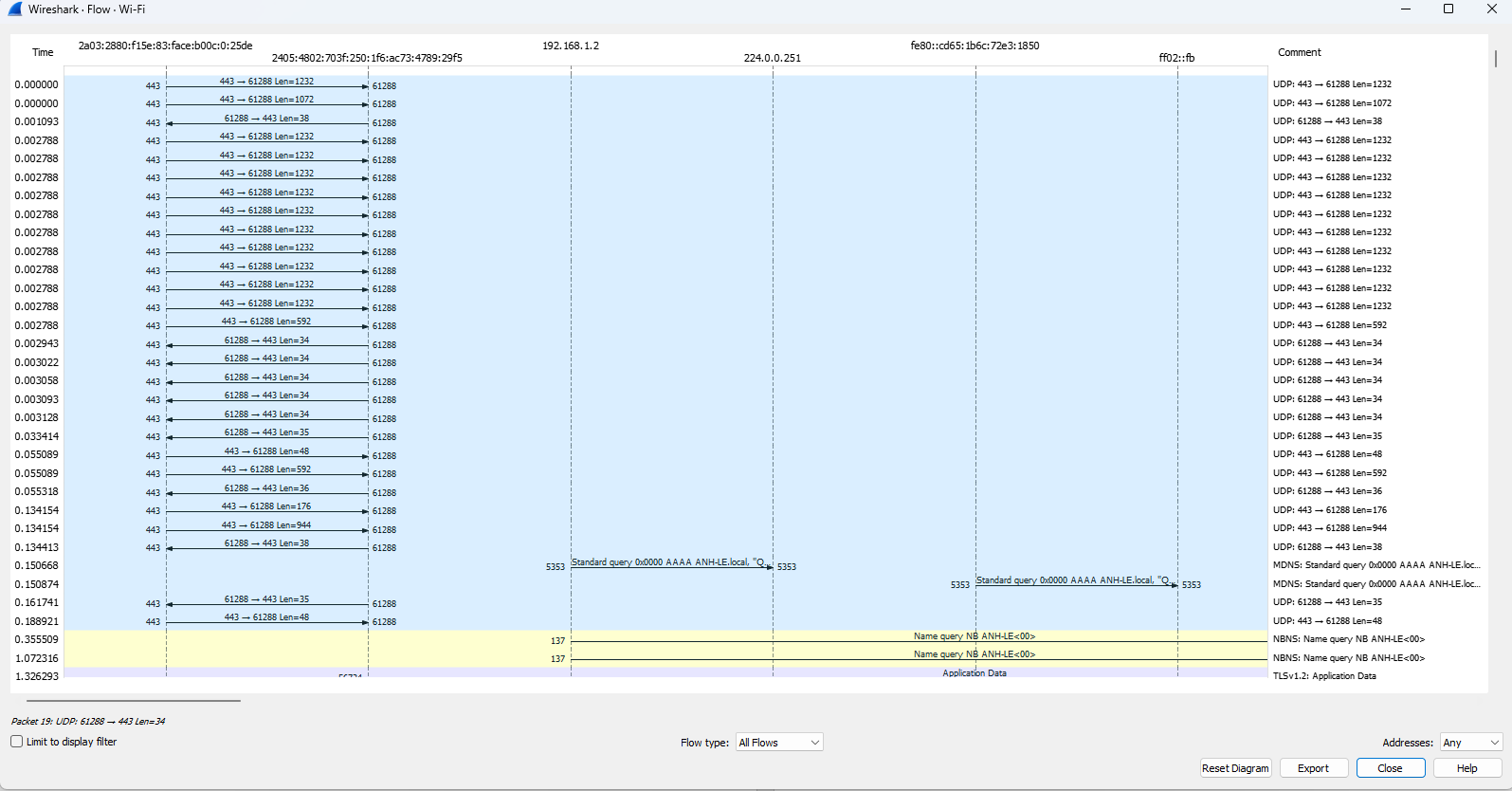




**5. Phân tích quá trình bắt tay 3 bước TCP bằng WireShark**





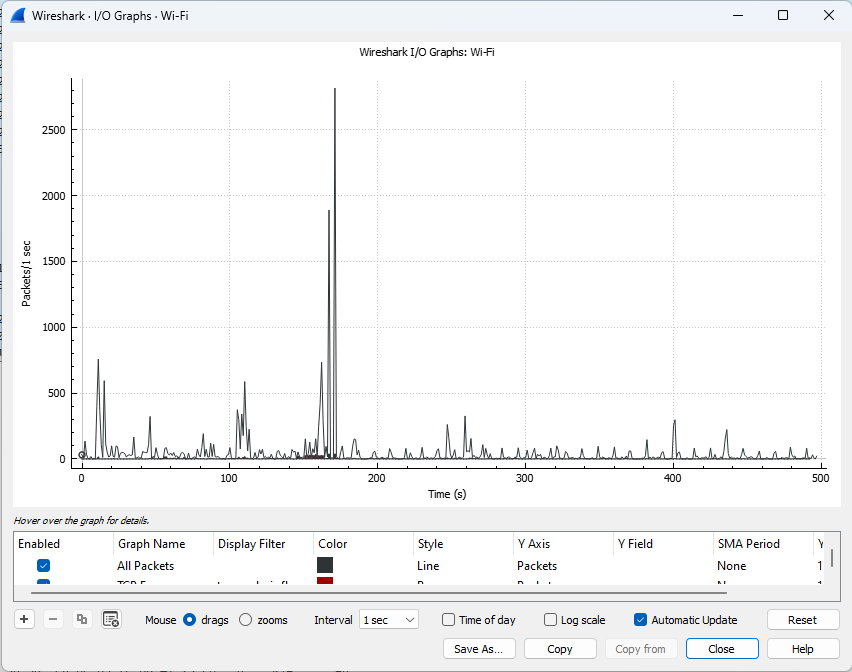
  Giải thích:

a)      A gởi gói tin có cờ SYN = 1 (yêu cầu kết nối), giá trị segment khởi đầu có thứ tự là seq(A) = 0.

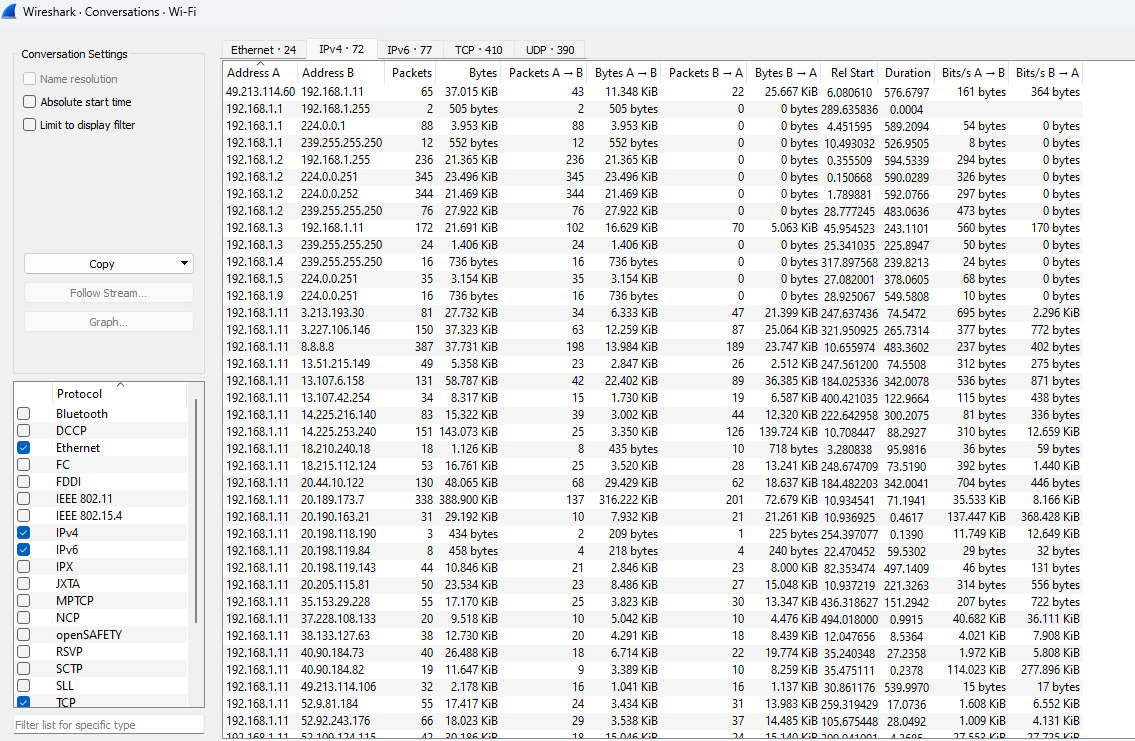
b)      B đồng ý kết nối trả lời gói tin có cờ SYN = 1, ACK = 1 và giá trị seq(B) = 0, ack = seq(A) + 1 = 0 + 1 = 1 (đã nhận gói tin 0 của A và chờ gói tin 1).

c)      A xác nhận thiết lập kết nối trả lời gói tin có cờ ACK = 1; giá trị ack = seq(B) + 1 = 0 = 1 (nghĩa là đã nhận gói tin 0 của B và chờ gói tin 1).

**6. Xem đồ thị I/O graph thống kê gói tin bắt được**



**7. Xem thống kê gói tin bắt được**

****