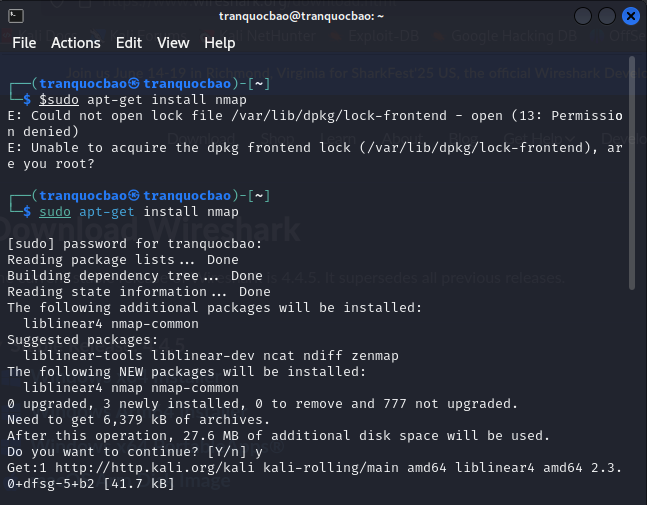
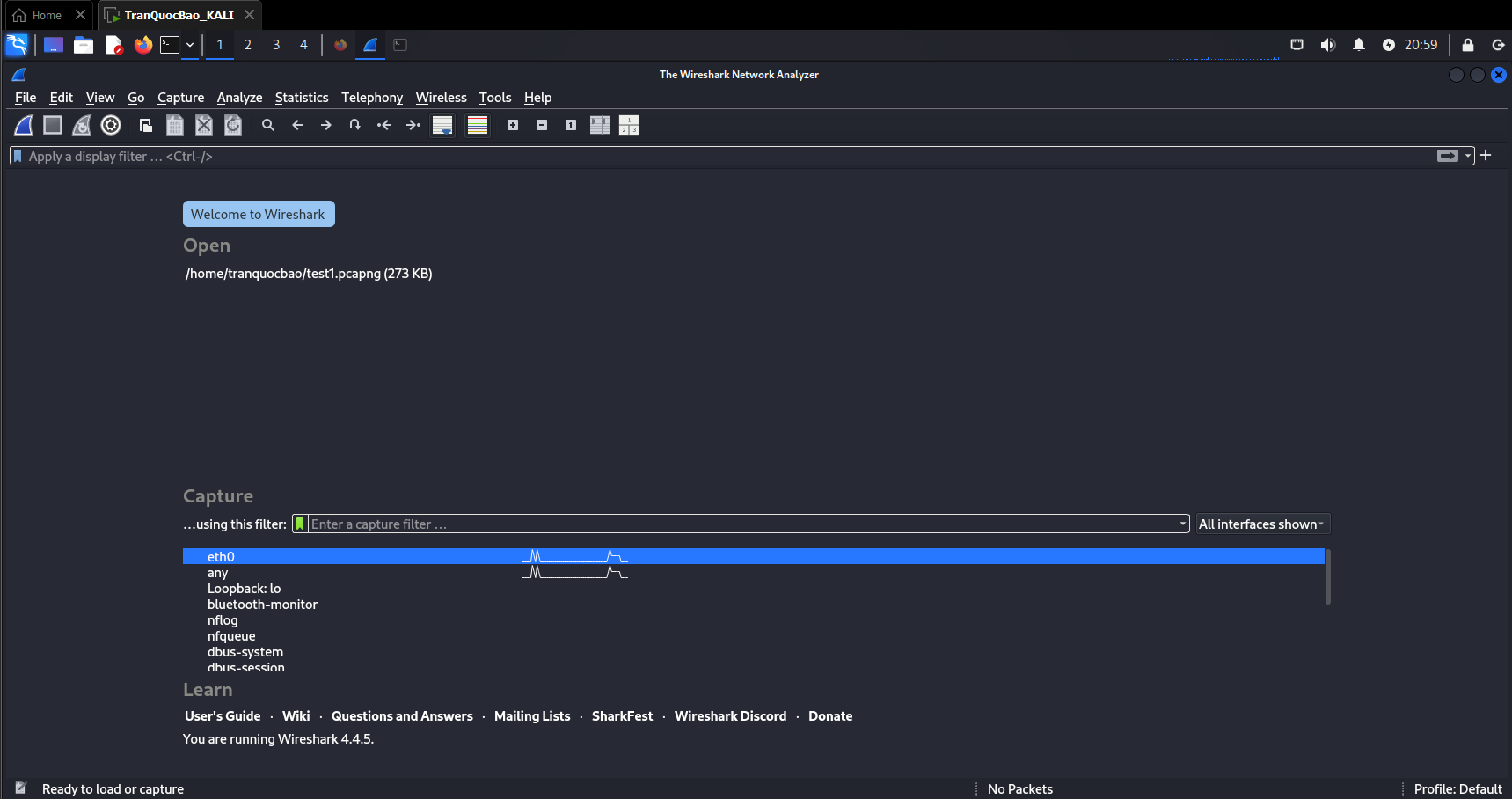
LAB 7

1. Quét thăm dò mạng

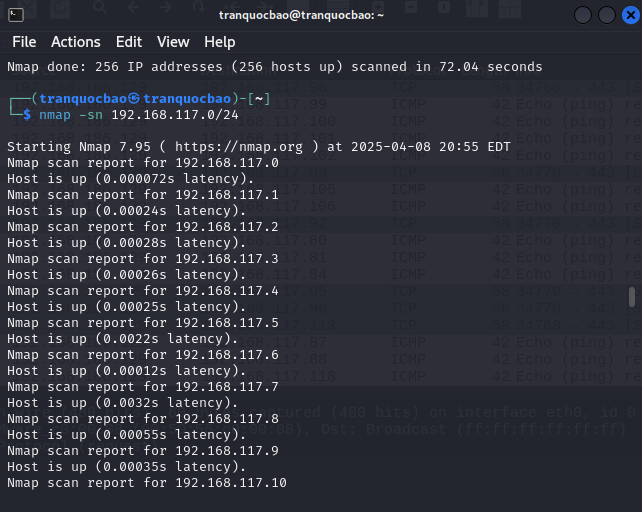
Bước 1: tải nmap



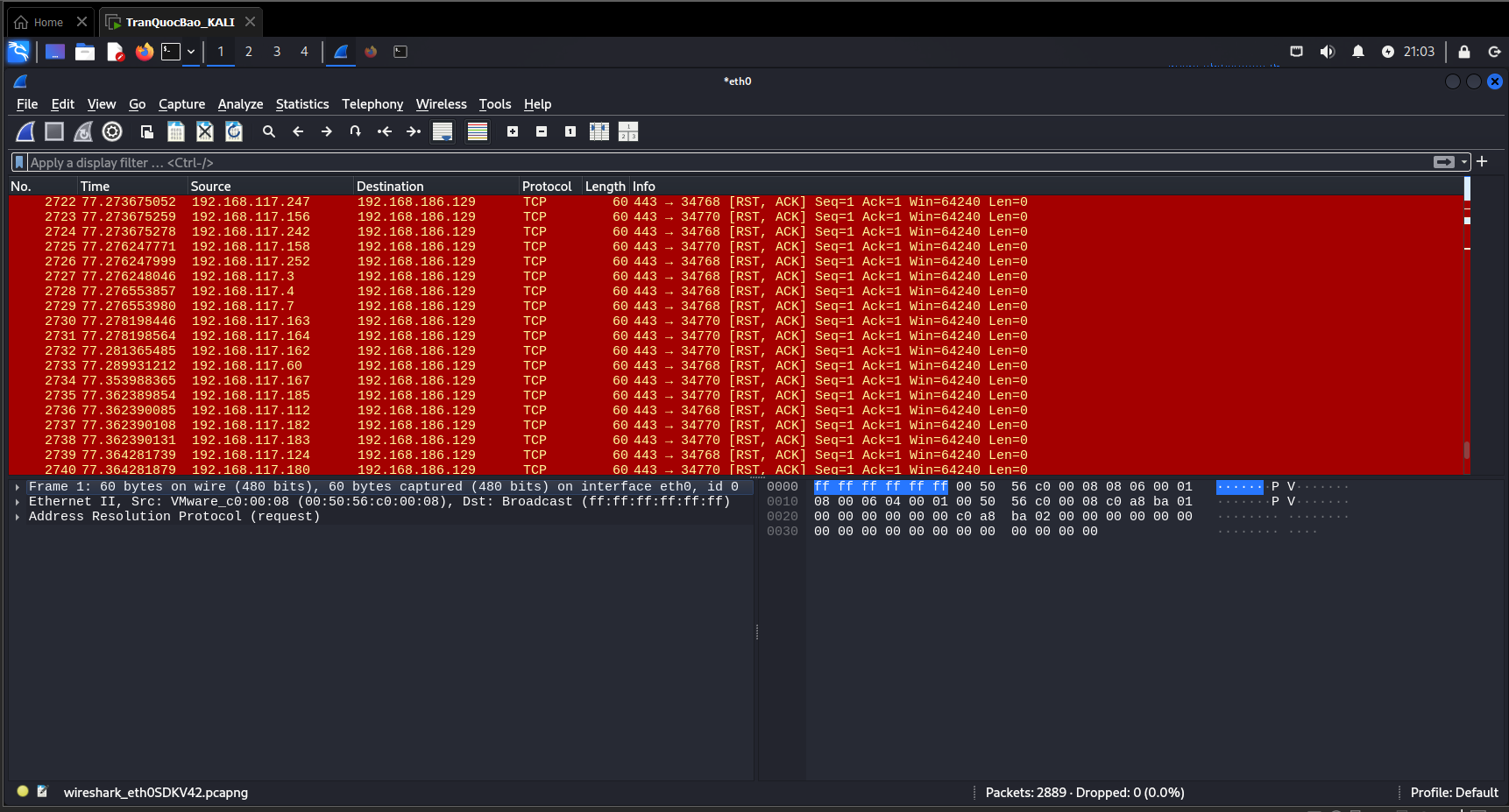
Bước 2: khởi động wiresharks



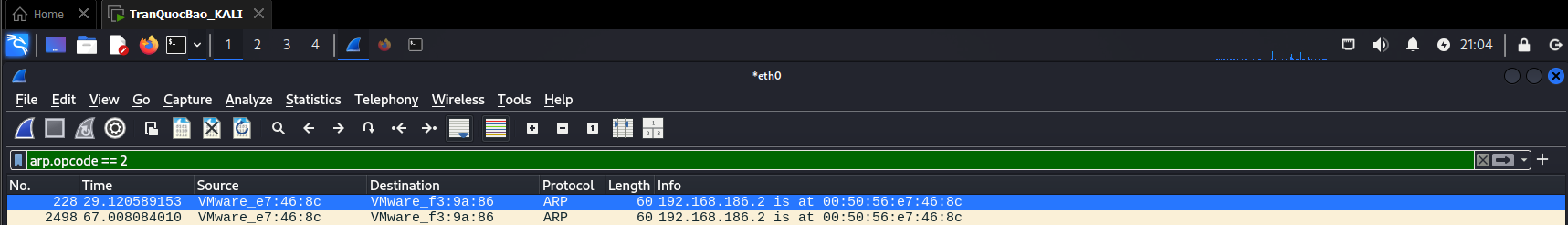
Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng



Bước 4: Dừng bắt gói tin trên Wireshark

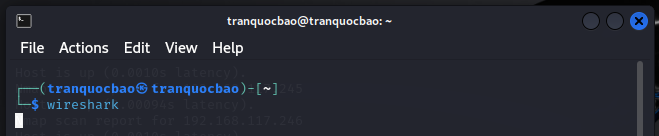


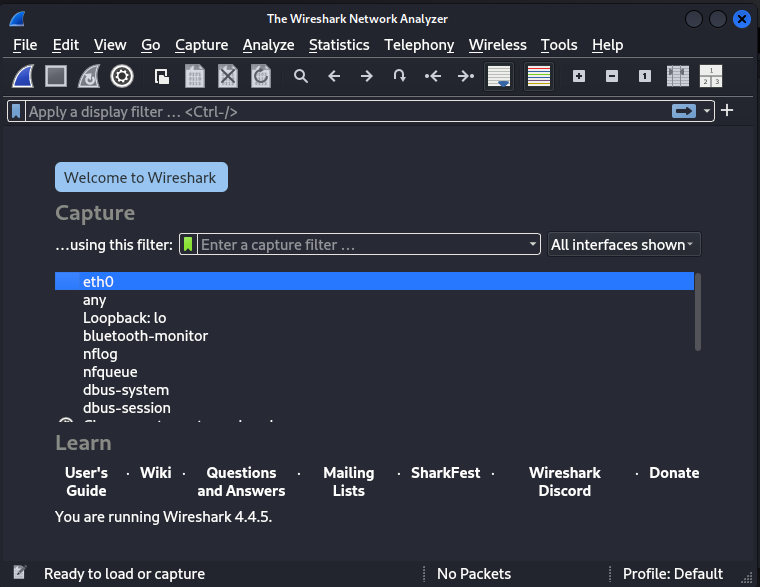
Bước 5: Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc



1. Quét thăm dò mạng

Bươc 1: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.



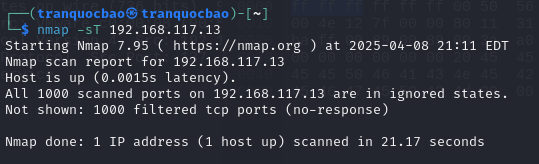


Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

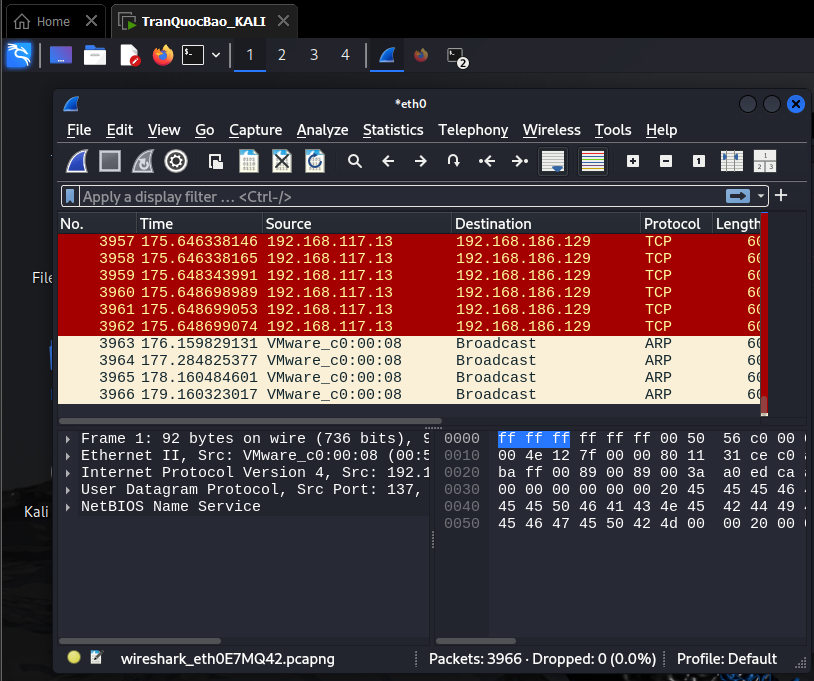
nmap -sT 192.168.117.13



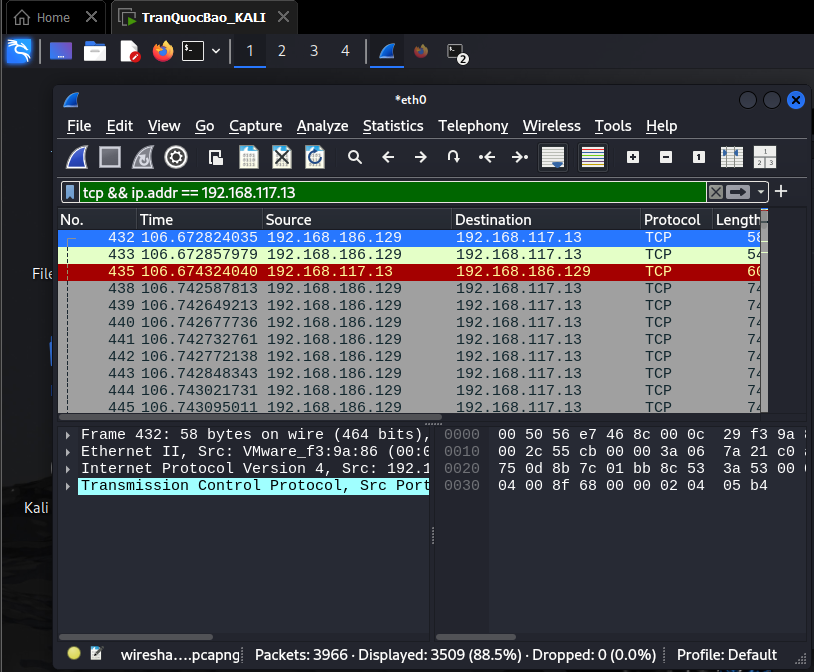
Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây.



Bước 5: Dừng bắt gói tin trên Wireshark



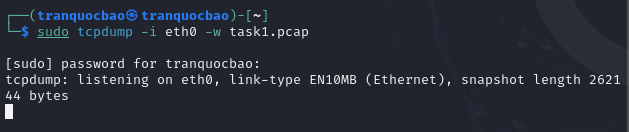
Sử dụng giá trị tcp && ip.addr == 192.168.117.13 ta lọc được các gói tin TCP.



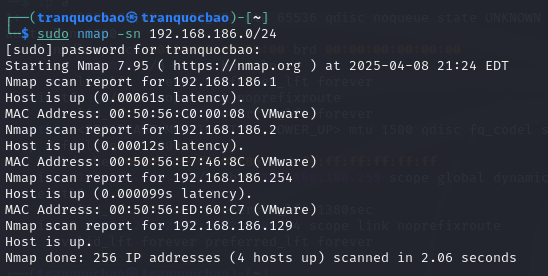
3.1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap

3.1.1. Kịch bản 1

Bước 1: Bắt gói bằng tcpdump bash

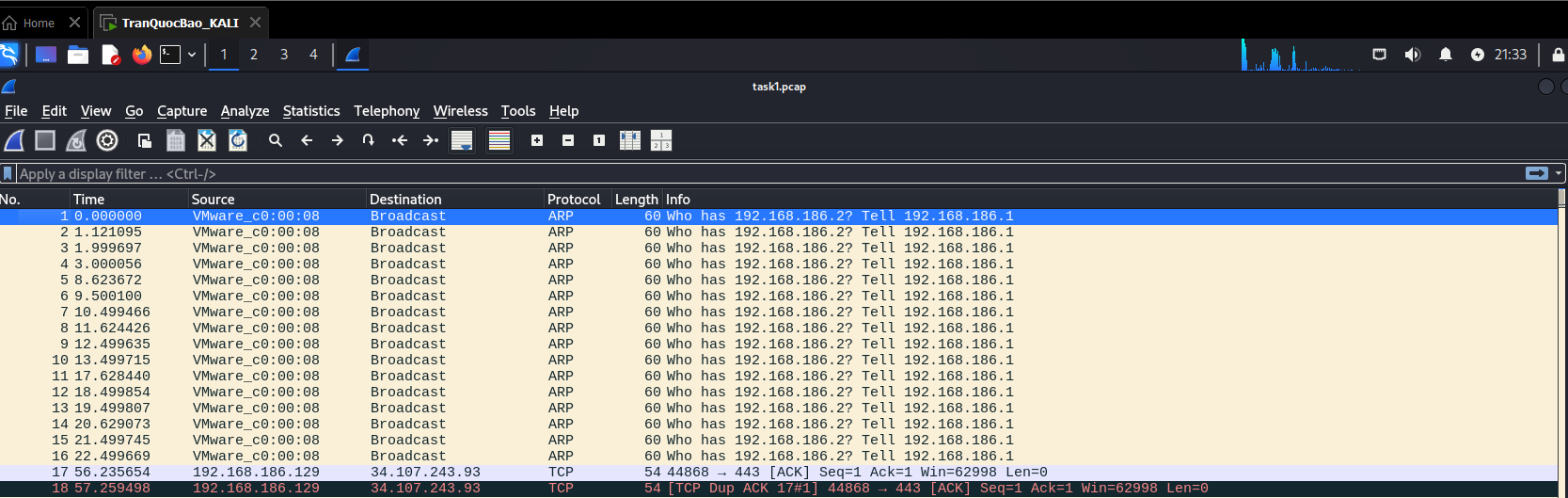


Bước 2: Quét bằng nmap ở terminal khác bash



Bước 3: Gói tin



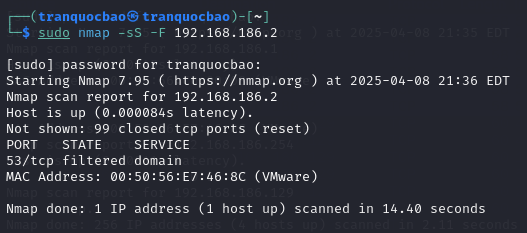


3.1.2. Kịch bản 2

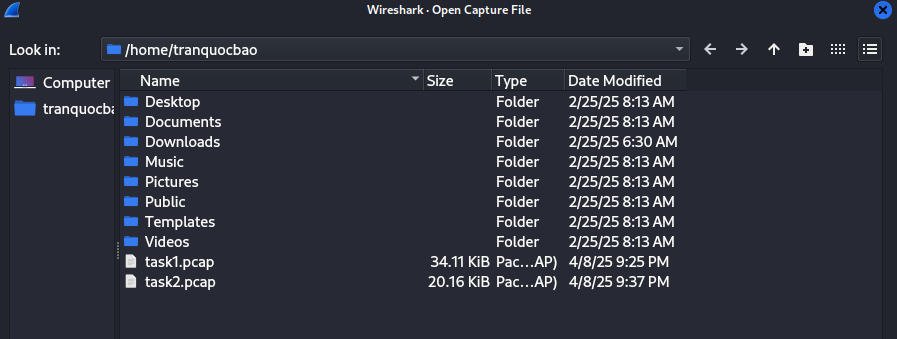
1. Bắt gói bằng tcpdump (Terminal 1):

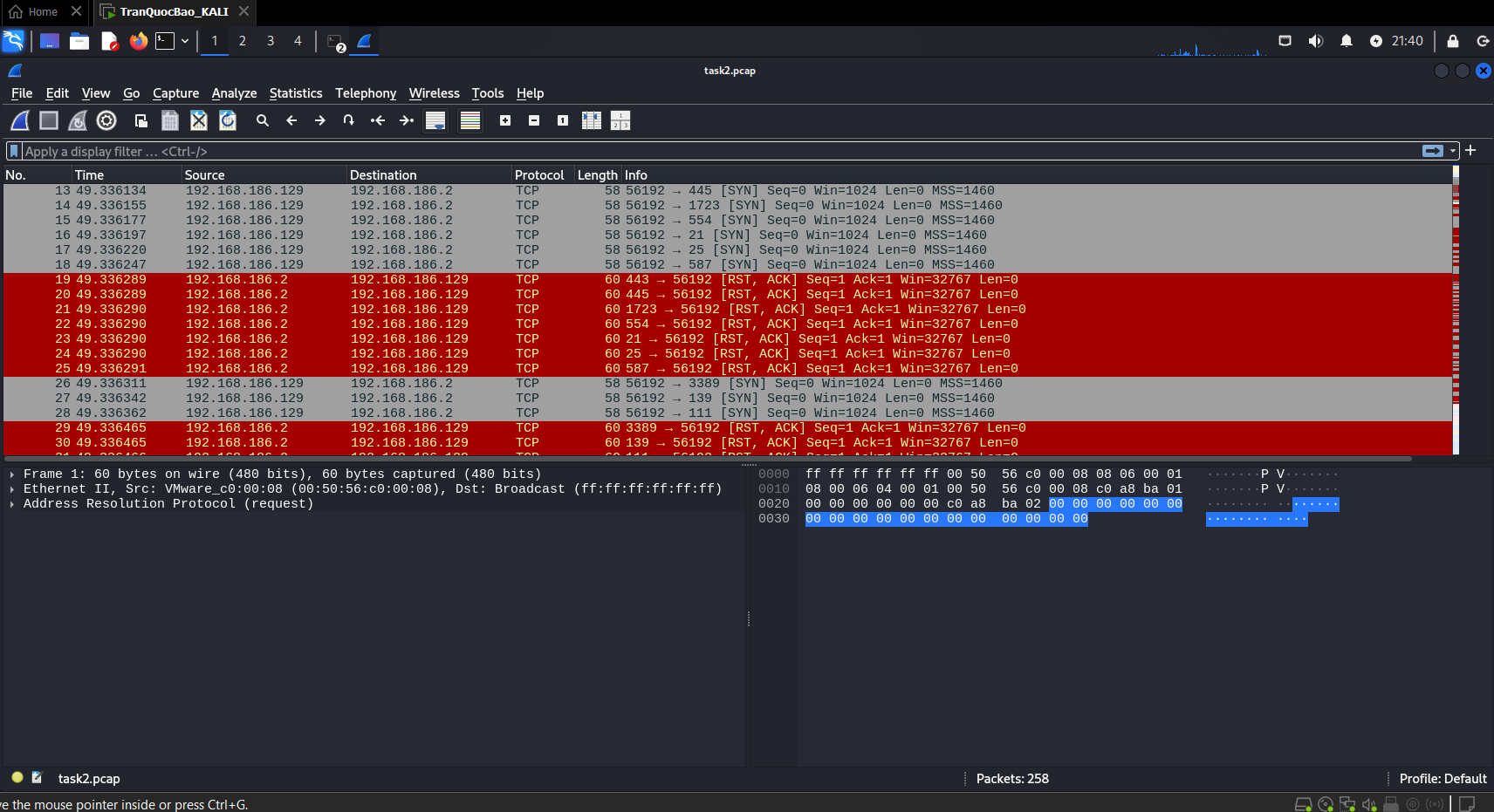


2. Quét bằng Nmap (Terminal 2):



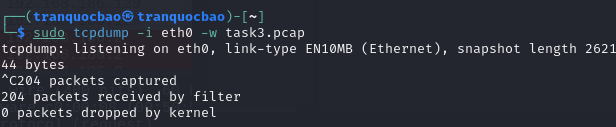
1. Gói tin



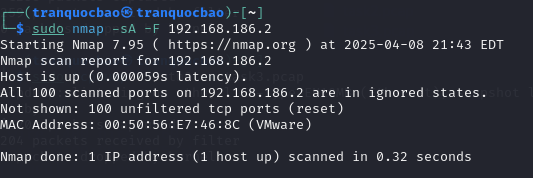


Kịch bản 3: ACK scan

Bước 1: Bắt gói bằng tcpdump (Terminal 1)



1. Quét bằng Nmap (Terminal 2):



1. Gói tin

