BÁO CÁO BÀI THỰC HÀNH SỐ 7

PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG

Hồ ĐÌnh Nguyên

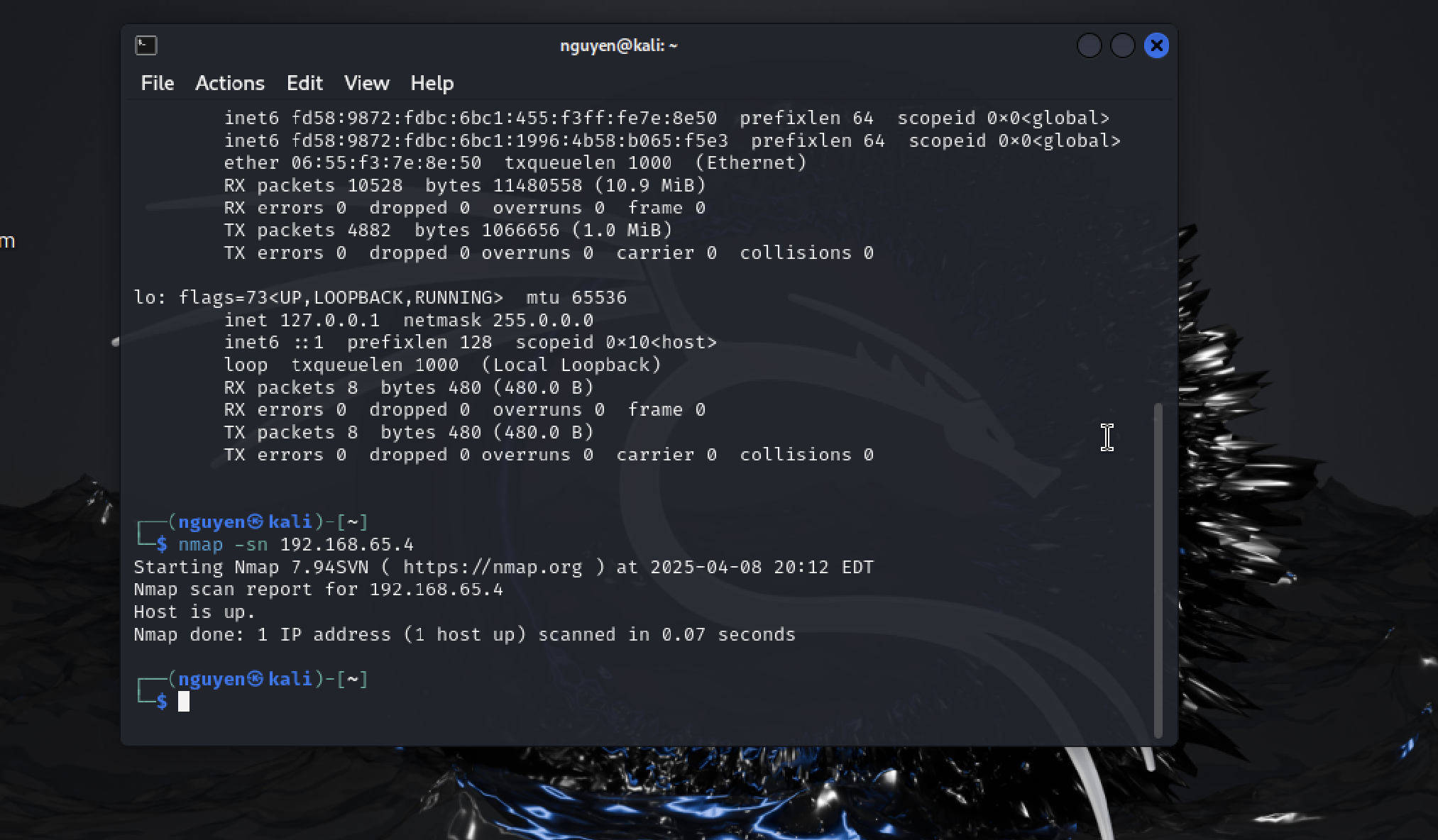
MSSV:1050080025

KẾT QUẢ THỰC HÀNH

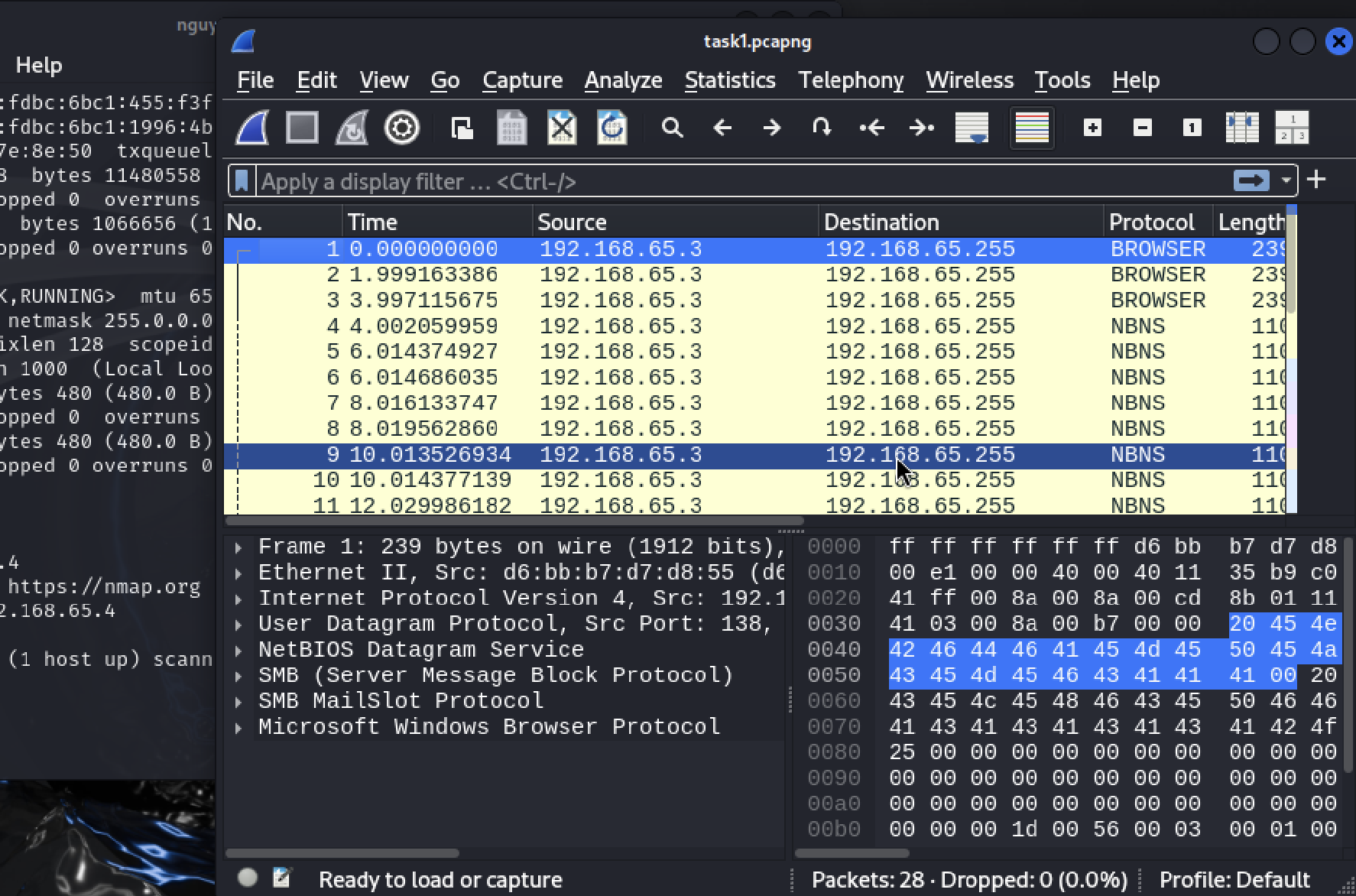
1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap

1.1

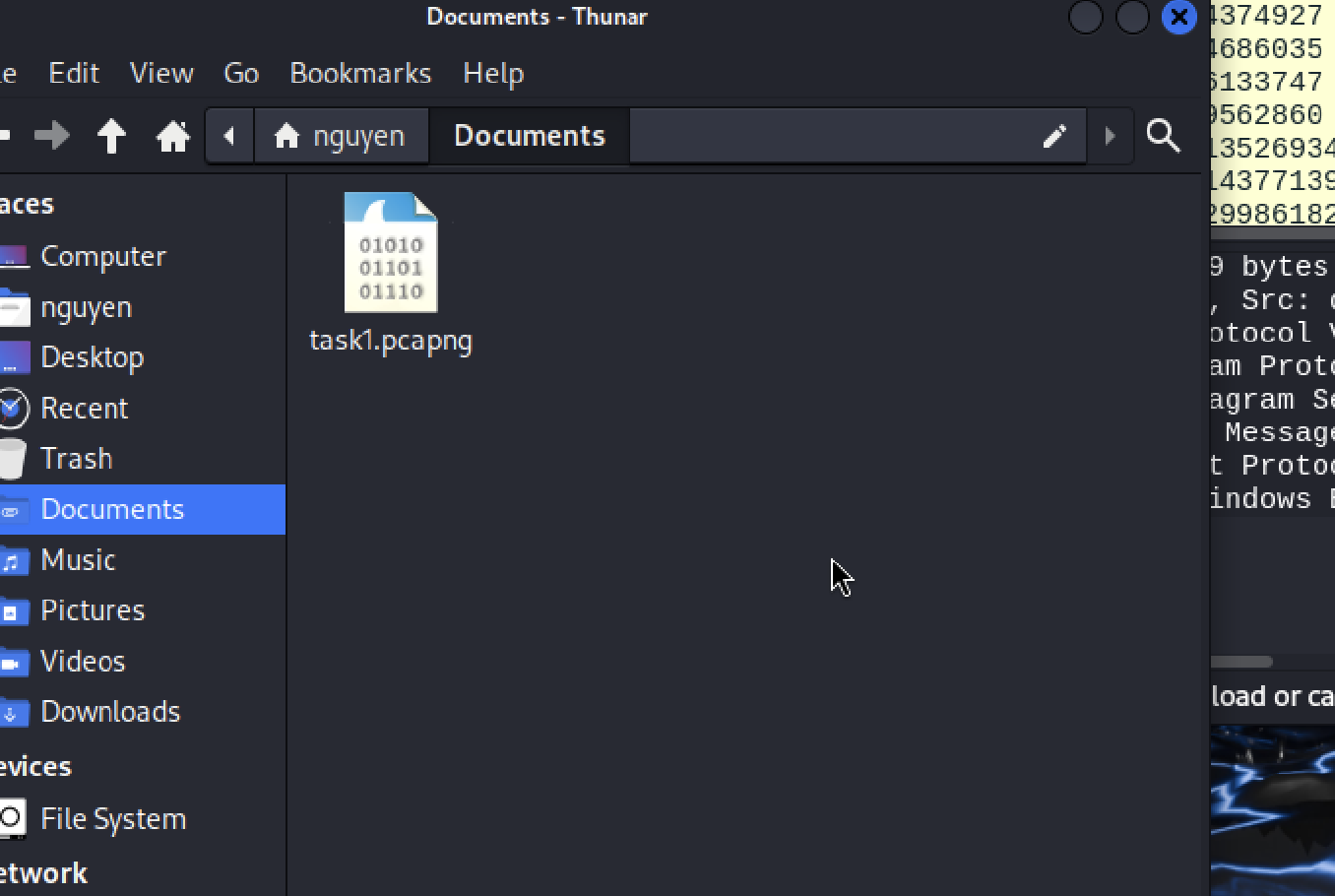
xem ip và thực hiện nmap

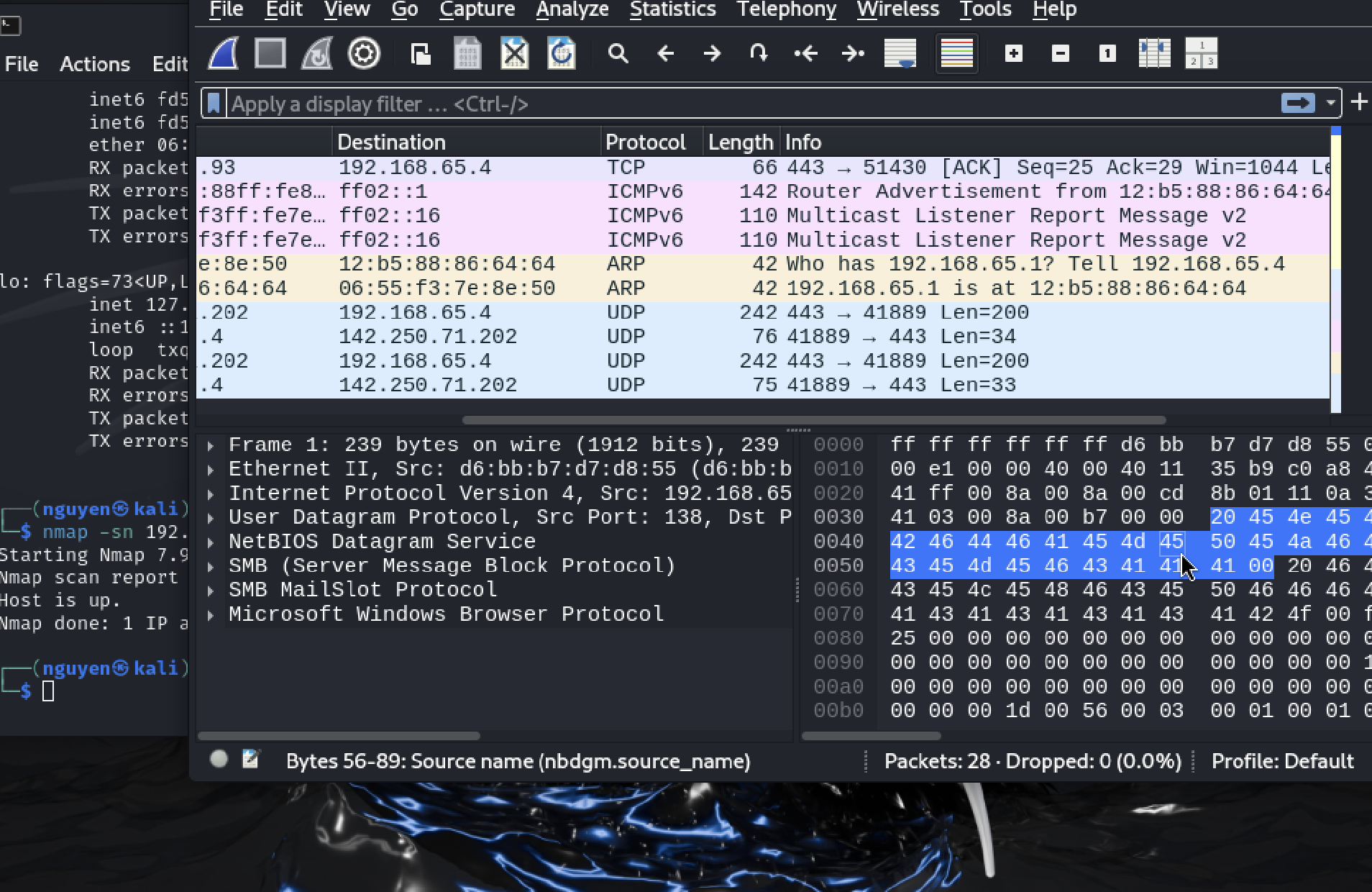


sau đó mở whiresark và xem bắt gói tin:



lưu file vs tên tak1:





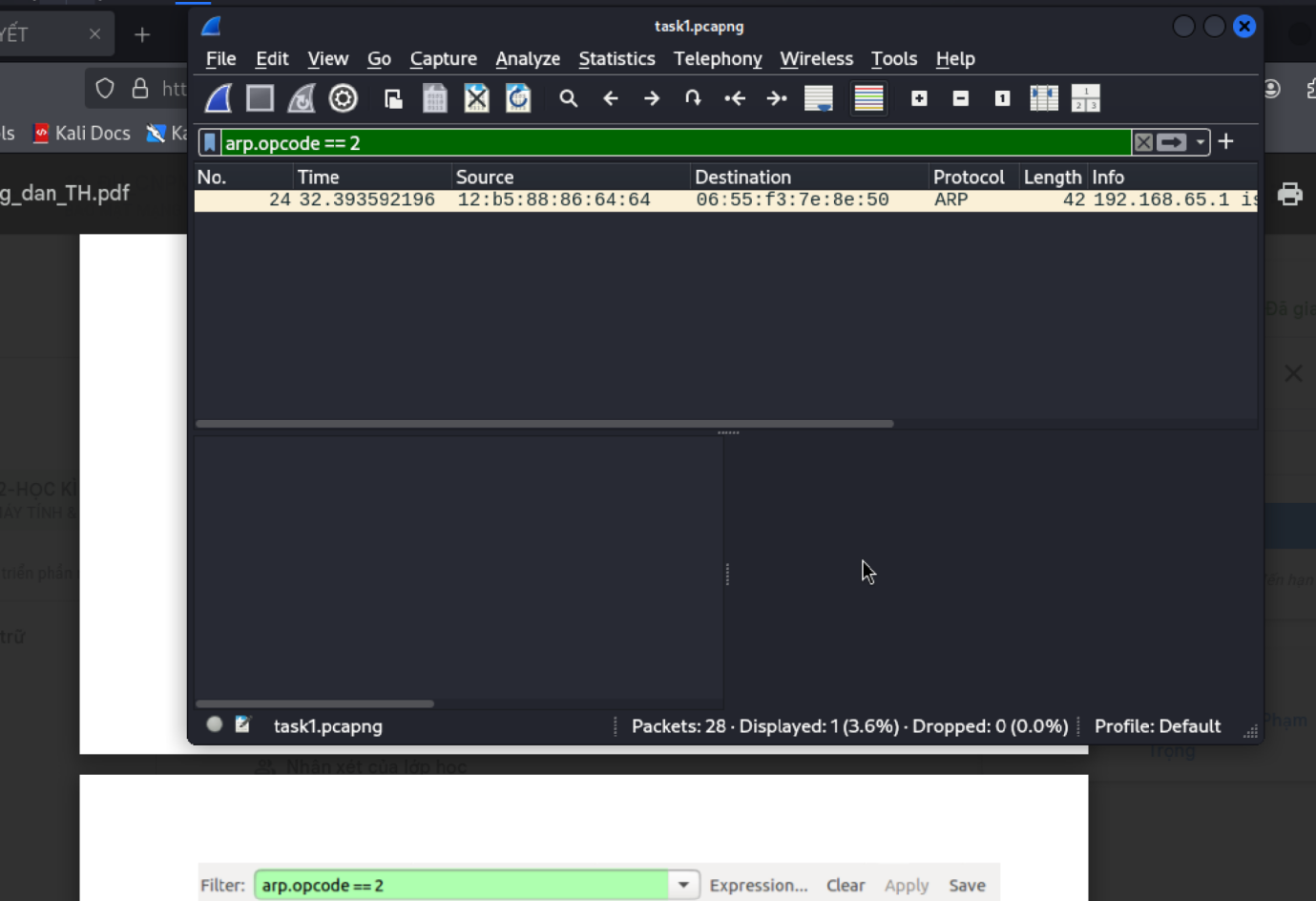
phân tích lưu lượng:Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn

công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.65.1

Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc, chúng ta có thể thấy

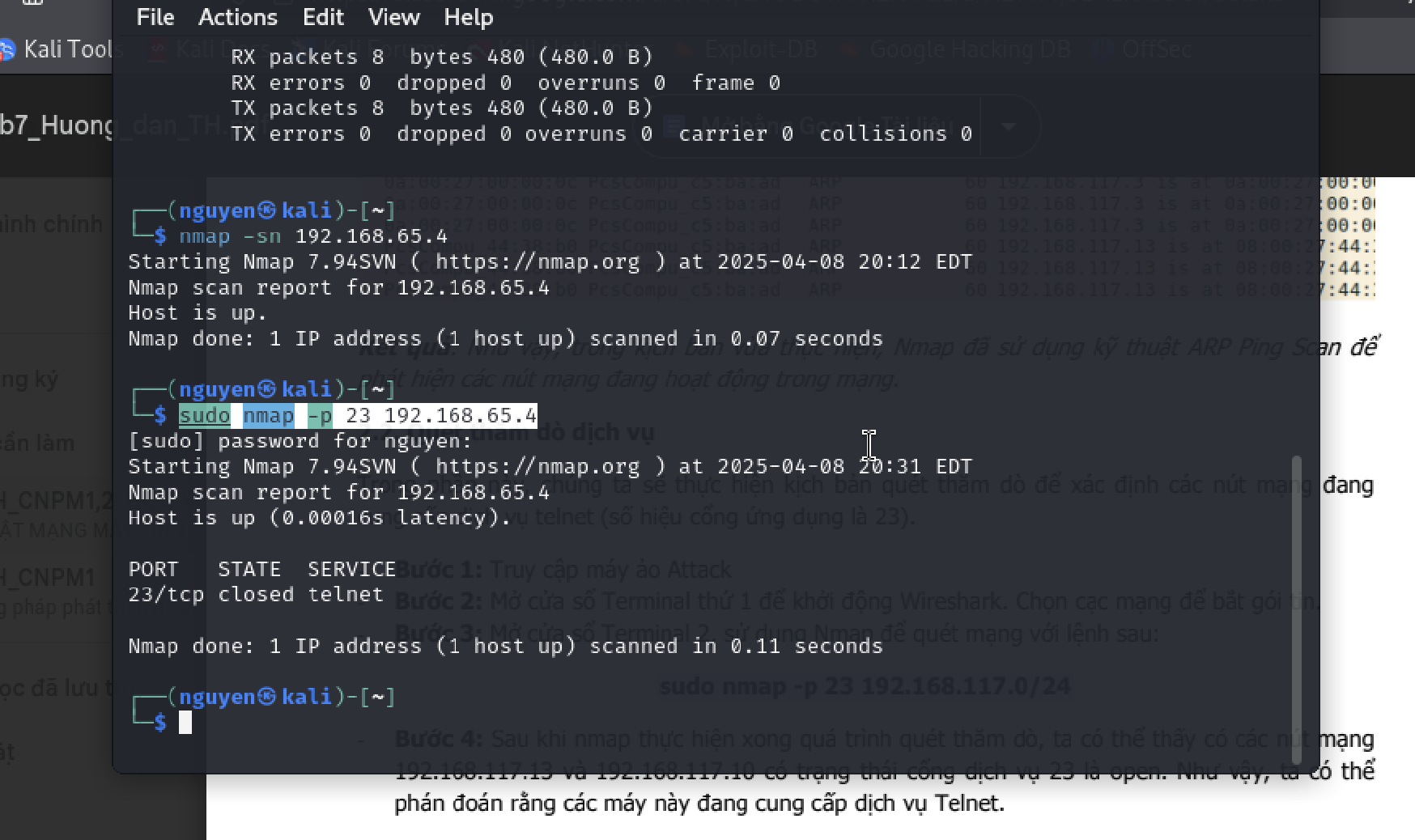
các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong

kết quả quét mạng bằng công cụ nmap.



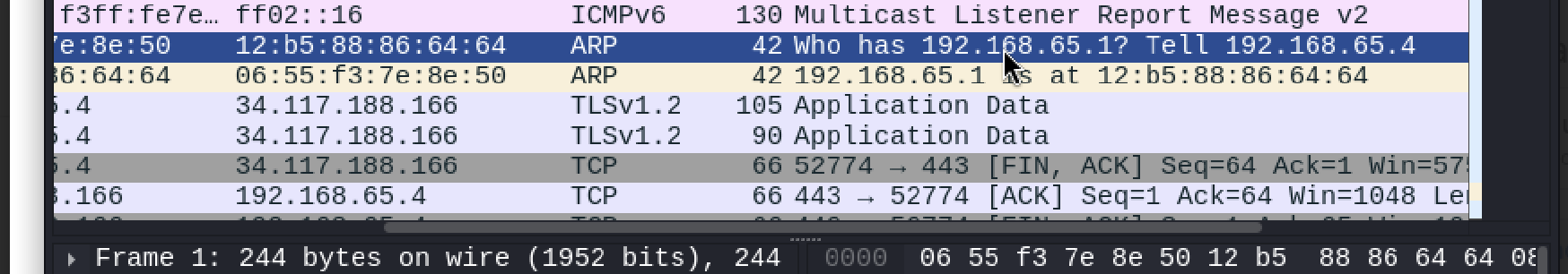
1.2

sudo nmap -p 23 192.168.65.4



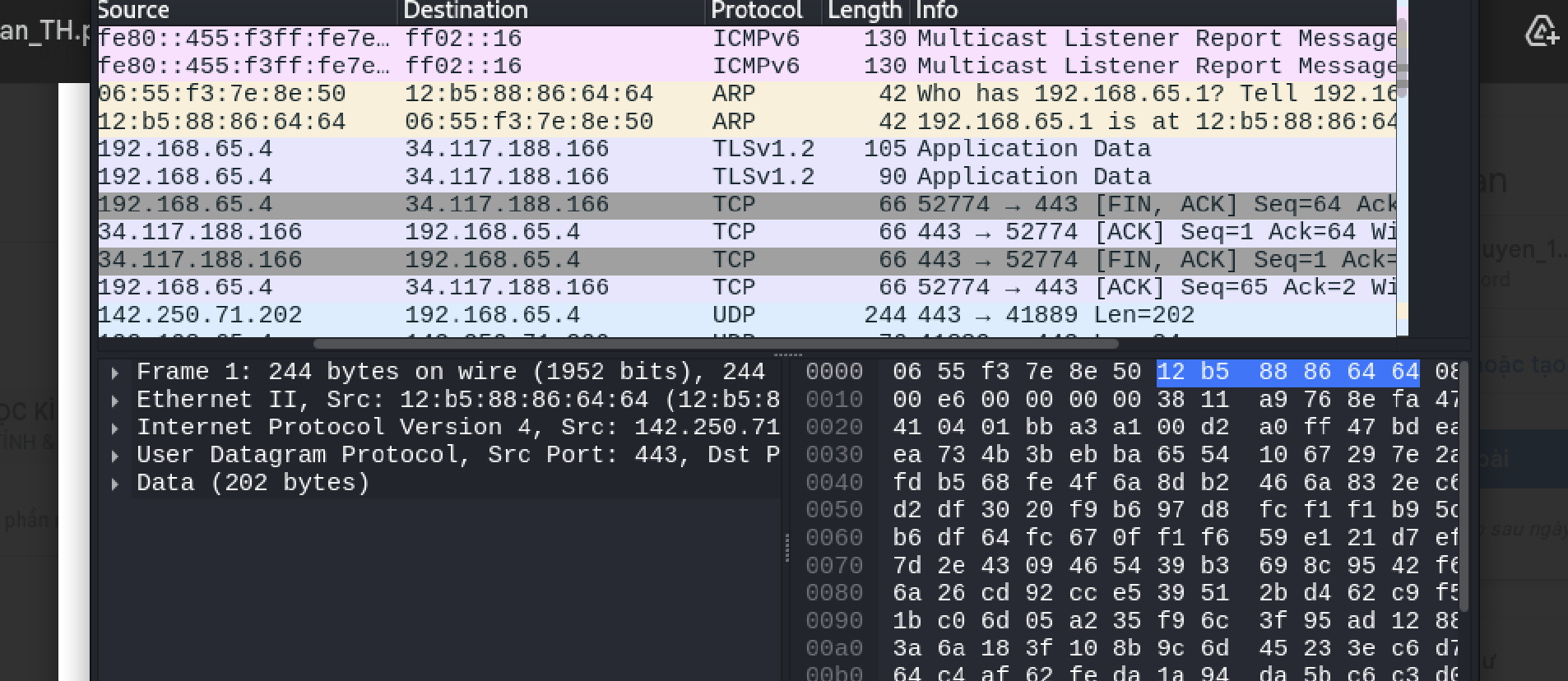
phân tích lưu lượng:Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn

công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.65.1



Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP

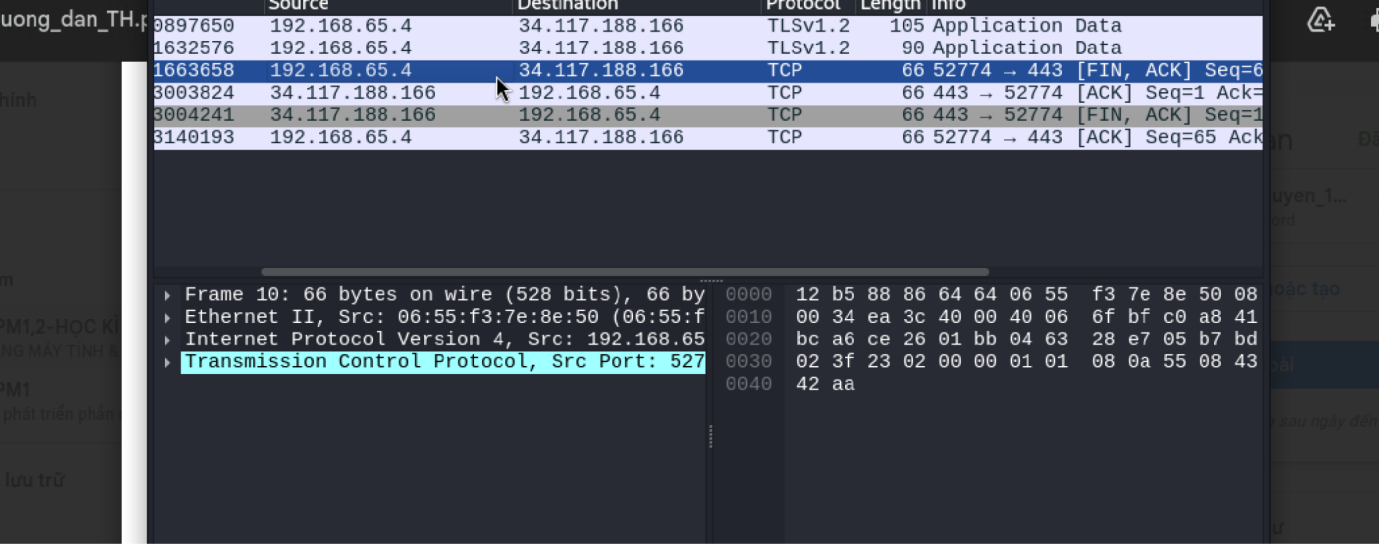
SYN được gửi tới cổng 23 của các máy đang hoạt động.



Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy

gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.65.4 về máy tấn công. Như vậy,

điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 34.117.188.166 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Telnet)

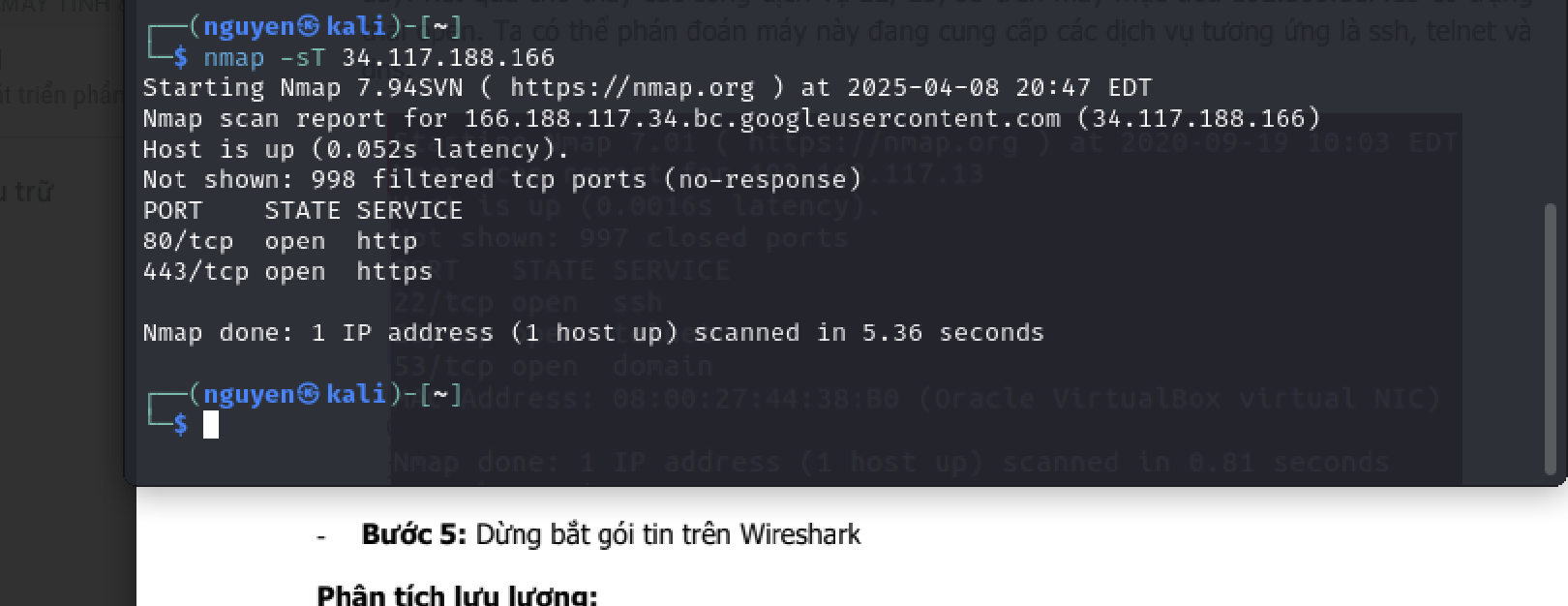


1.3

Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới

đây. Kết quả cho thấy các cổng dịch vụ 80,443 trên máy mục tiêu 34.117.188.166 có trạng

thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là http,https

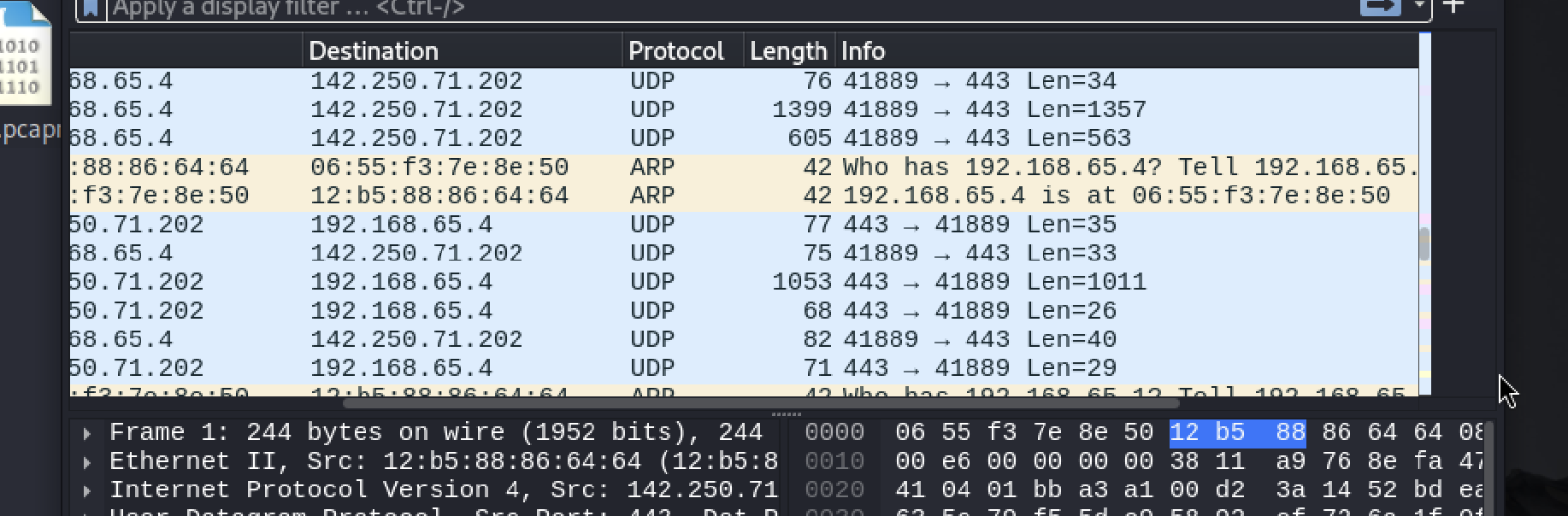


Phân tích lưu lượng:

Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra

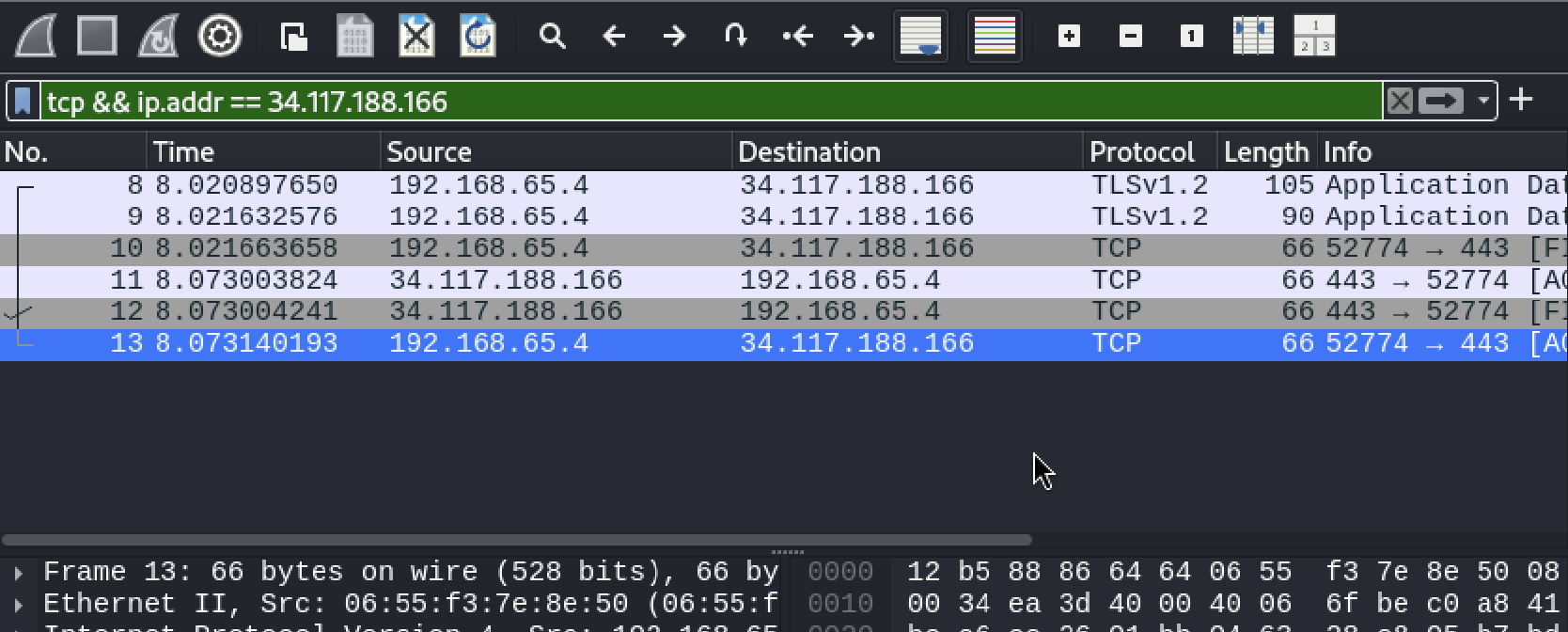
máy mục tiêu 34.117.188.166 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói 8 tin TCP SYN được gửi từ máy tấn công (192.168.65.4) tới máy mục tiêu là 34.117.188.166

Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.



Sử dụng giá trị tcp && ip.addr == 34.117.188.166 ta lọc được các gói tin TCP. Có thể nhận

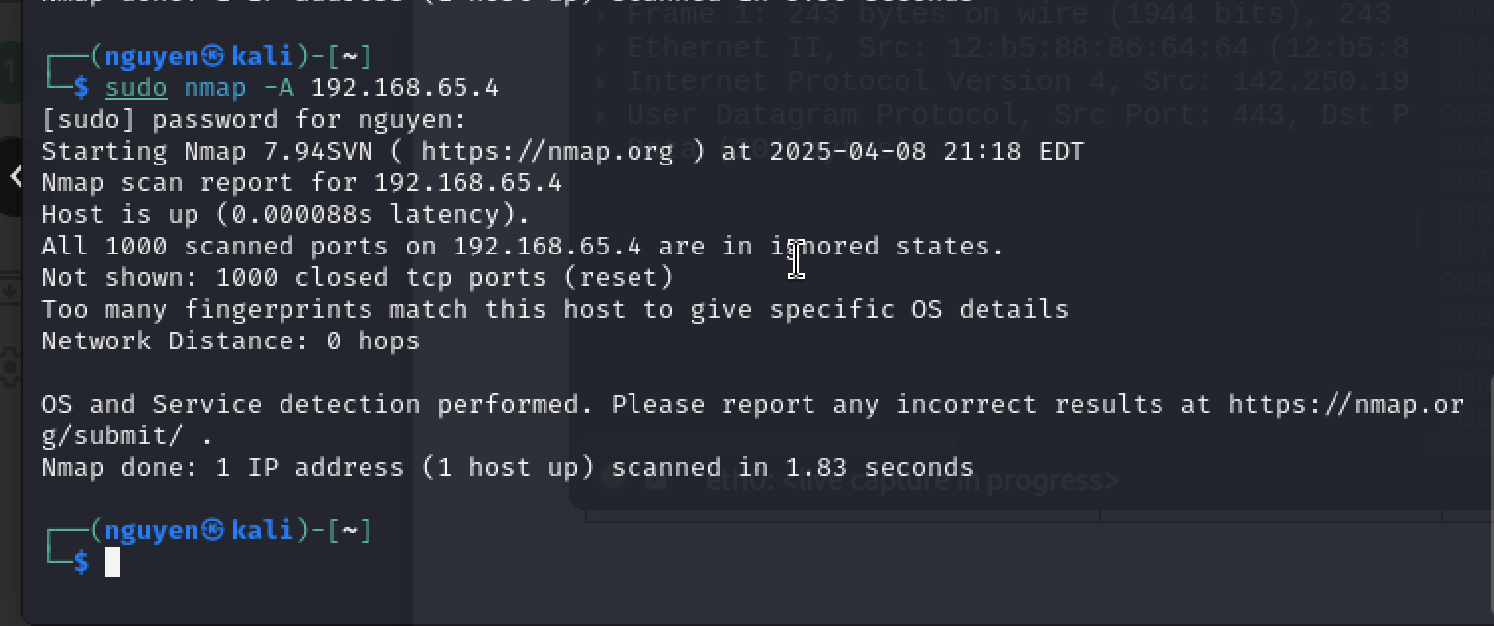
thấy một liên kết tới cổng 443 đã được thiết lập nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST để hủy kết nối này.



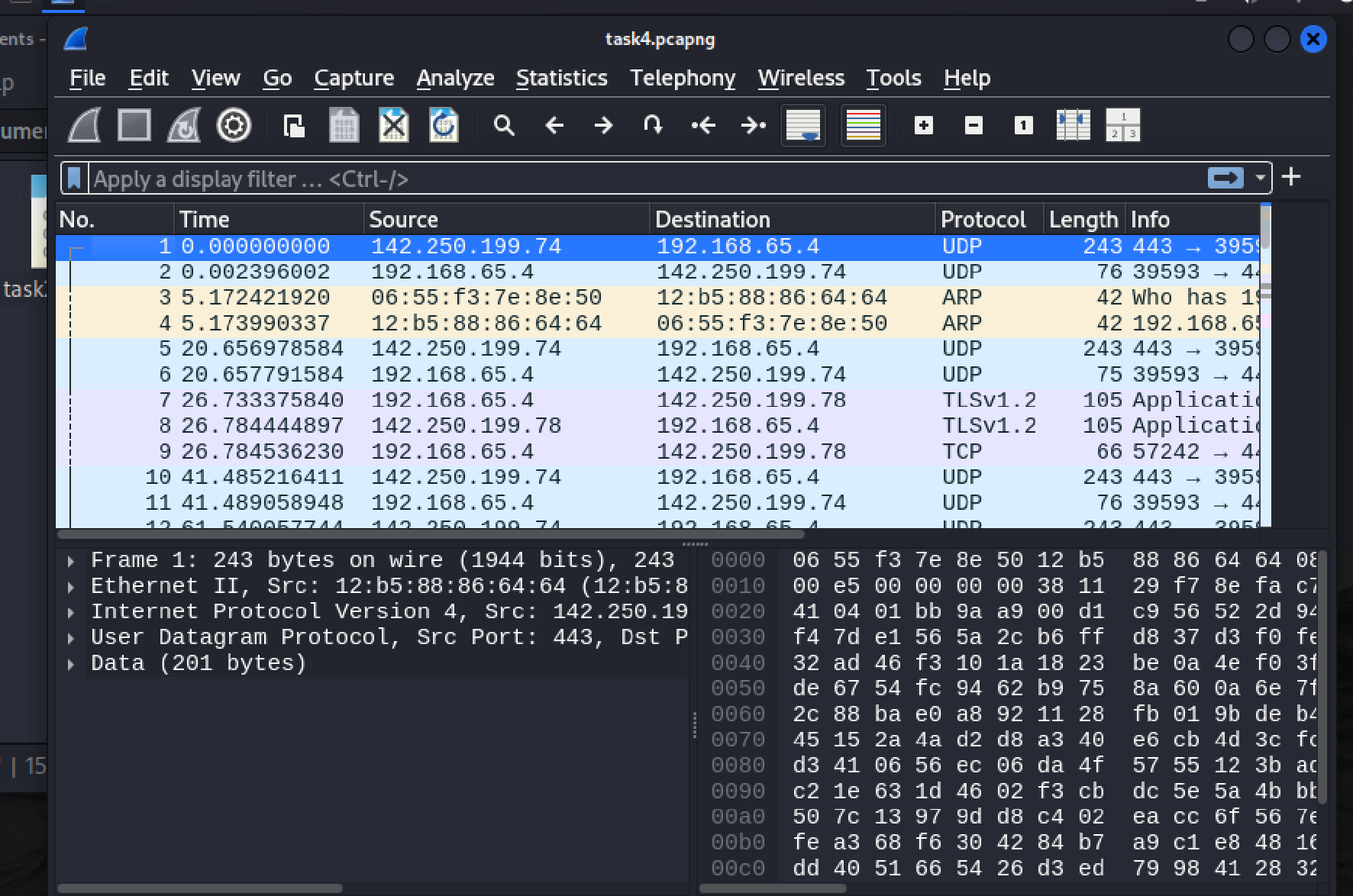
2 Thu thập thông tin hệ thống

thông tin hệ điều hành:

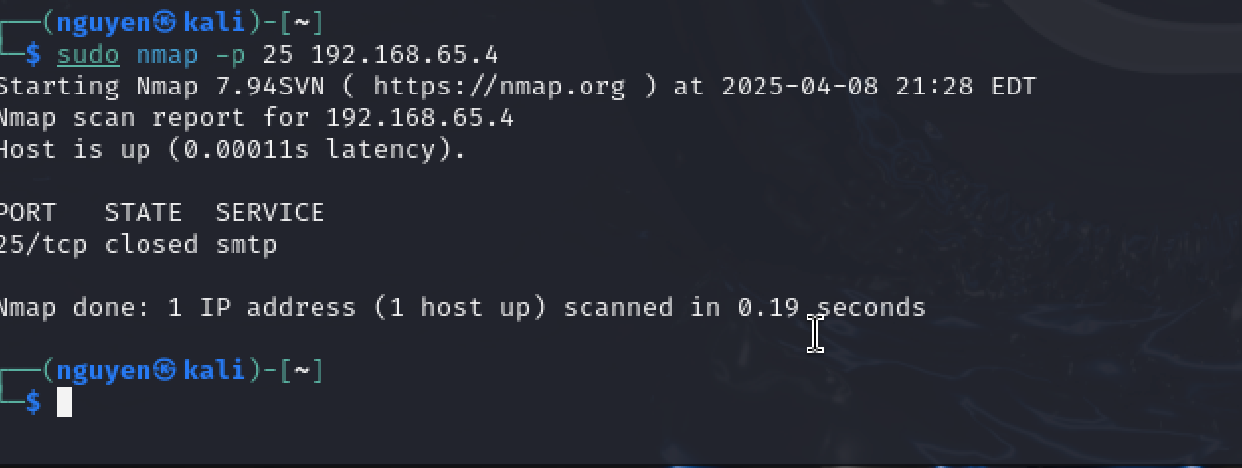
sudo nmap -A 192.168.65.4



chạy whiresark và lưu file tên task4



Câu lệnh email:sudo nmap -p 25 192.168.65.4



1. Tìm kiếm thông tin về các lỗ hổng

|  |  |  |
| --- | --- | --- |
| Phần mềm dịch vụ | Số CVE | Mô tả ngắn gọn |
| Postfix 3.4.10 | CVE-2020-6102 | Thực thi mã từ xa |
| OpenSSH 8.2 | CVE-2020-14145 | Tiết lộ thông tin |