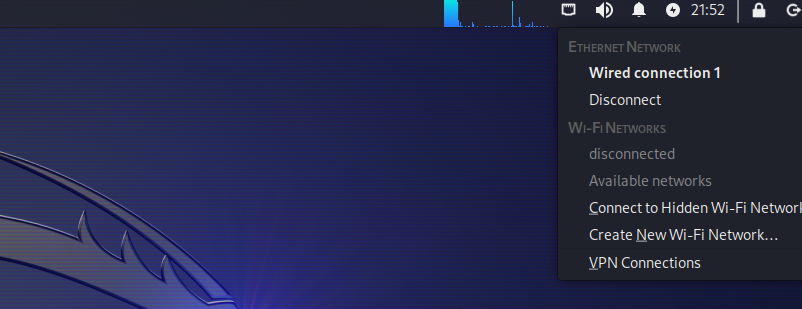
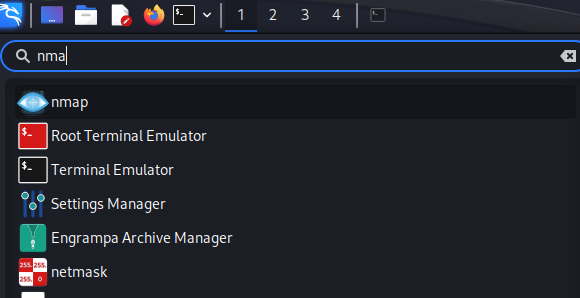


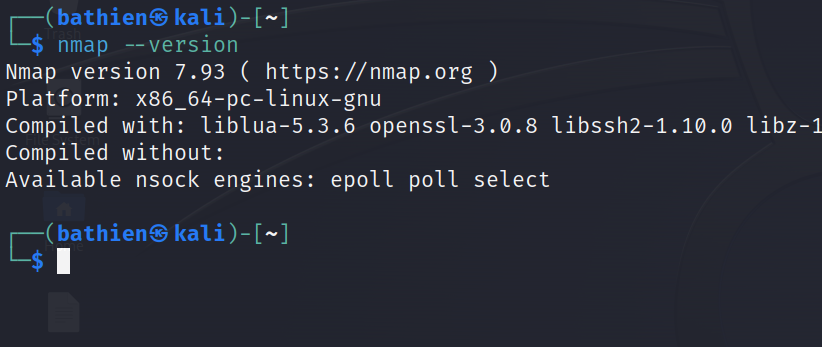
Chuẩn bị một máy ảo Kali linux



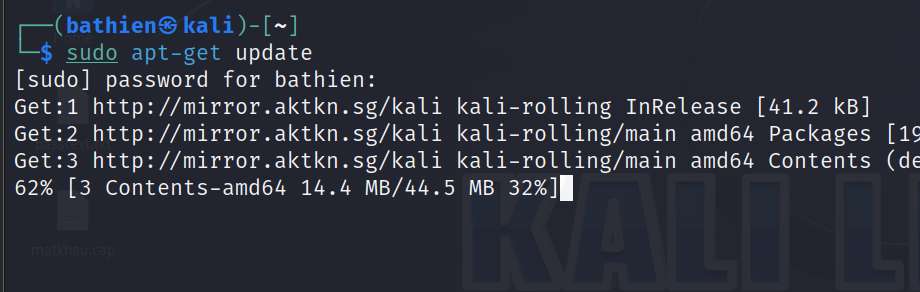
Ở đây đã được cấu hình 1 mạng wifi và 1 mạng eth0



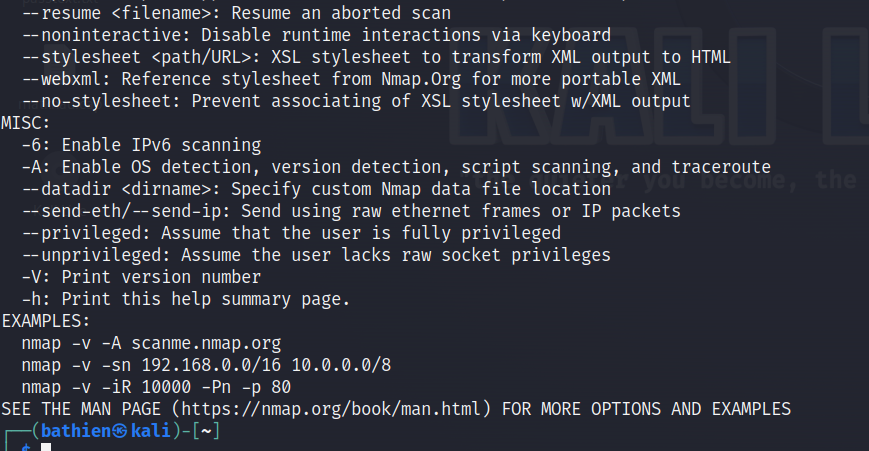
Đã được cài đặt sẵn nmap rồi



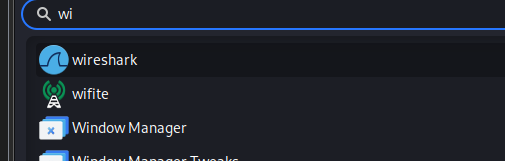
Kiểm tra phiên bản nmap



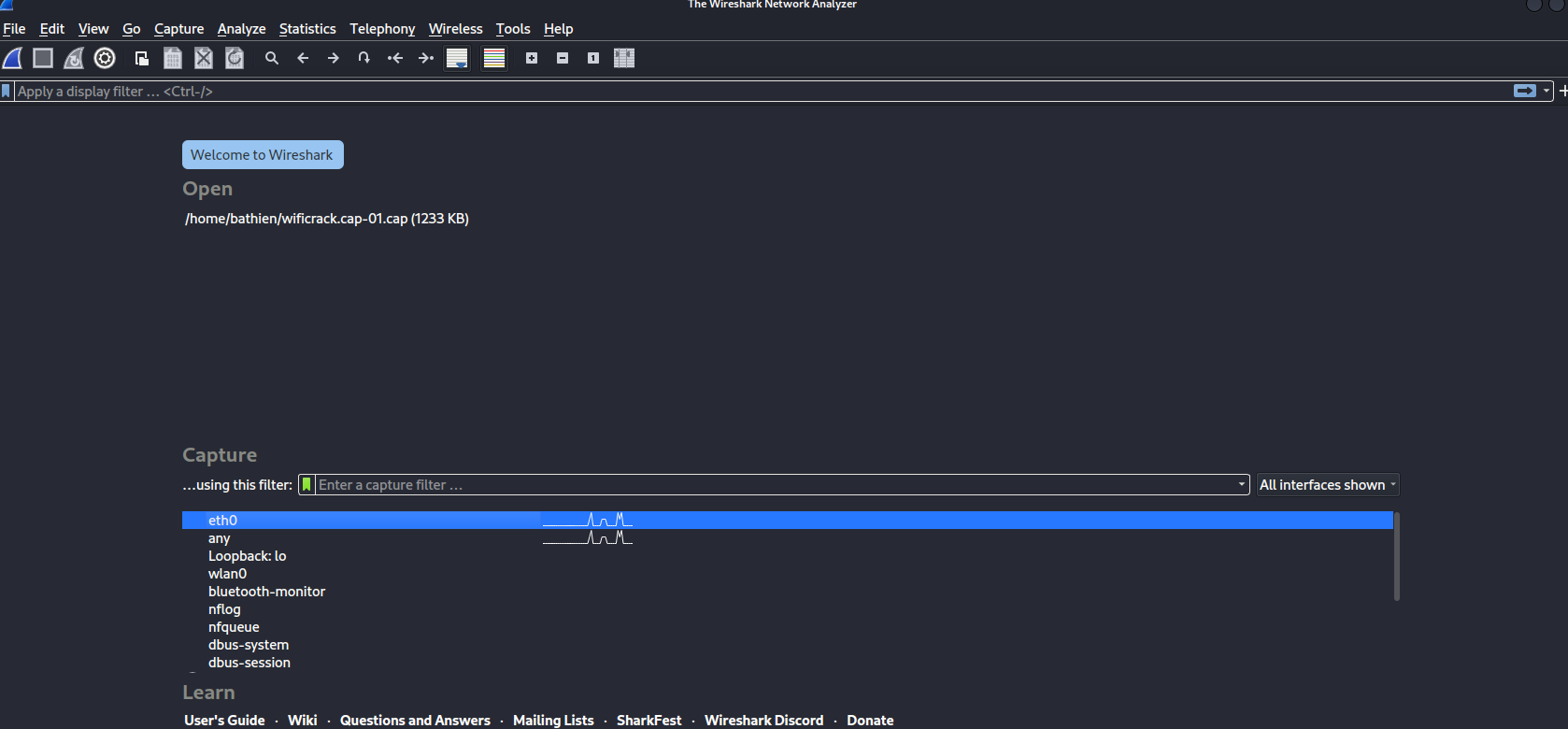
Update các gói



Chạy nmap

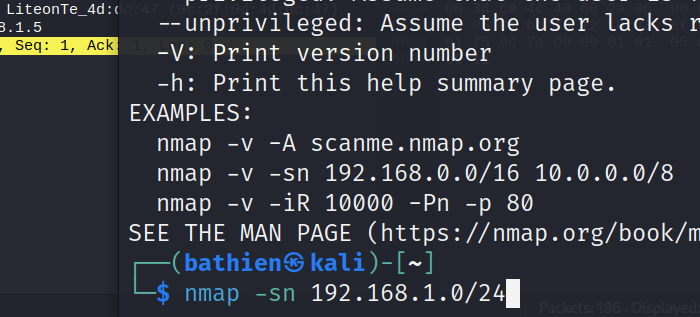


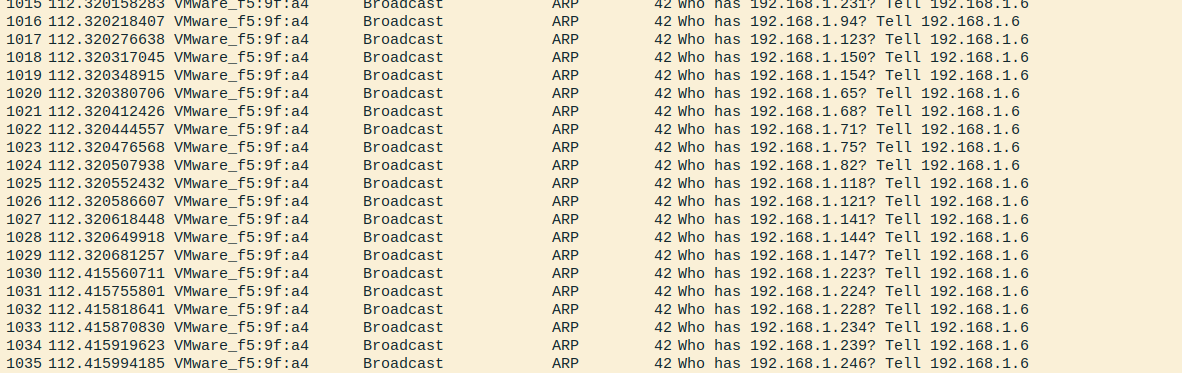
Có cài sẵn wiresark chỉ cần bật lên

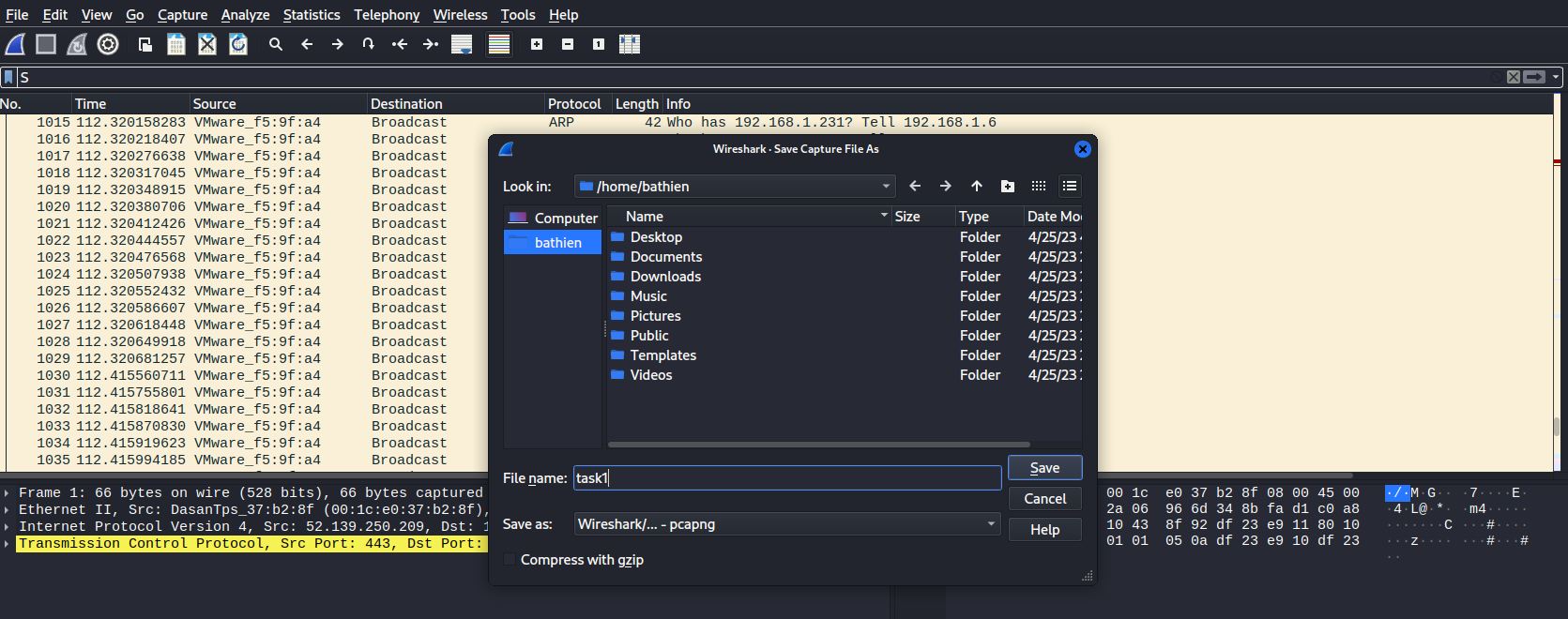


Chọn card mạng cần quét

**Kịch bản 1**

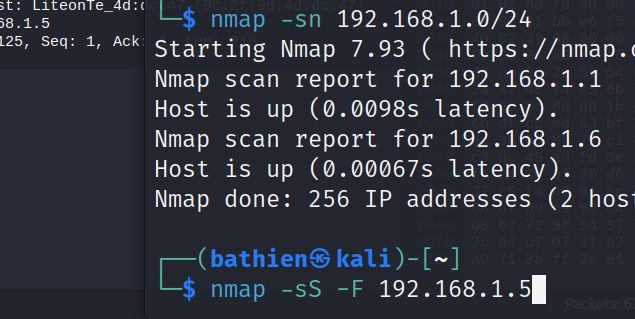


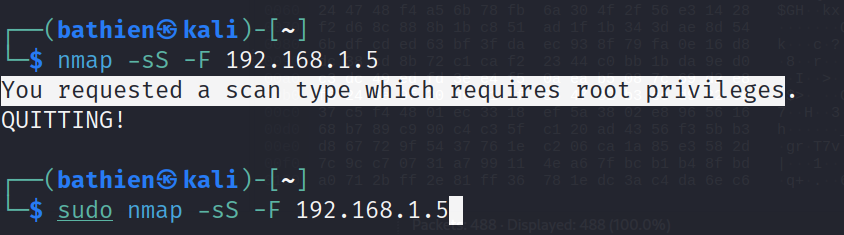


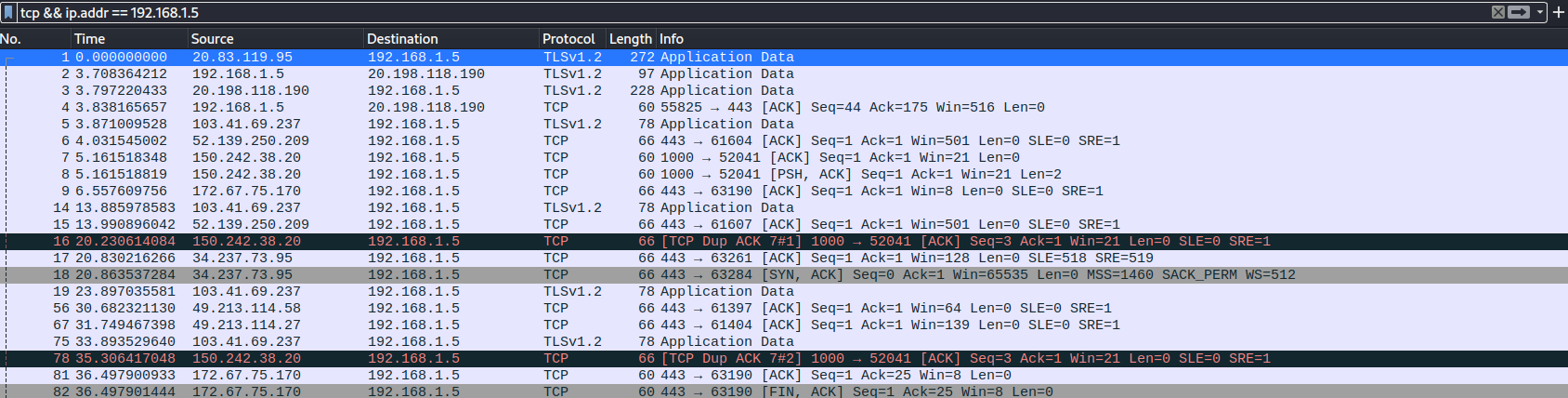


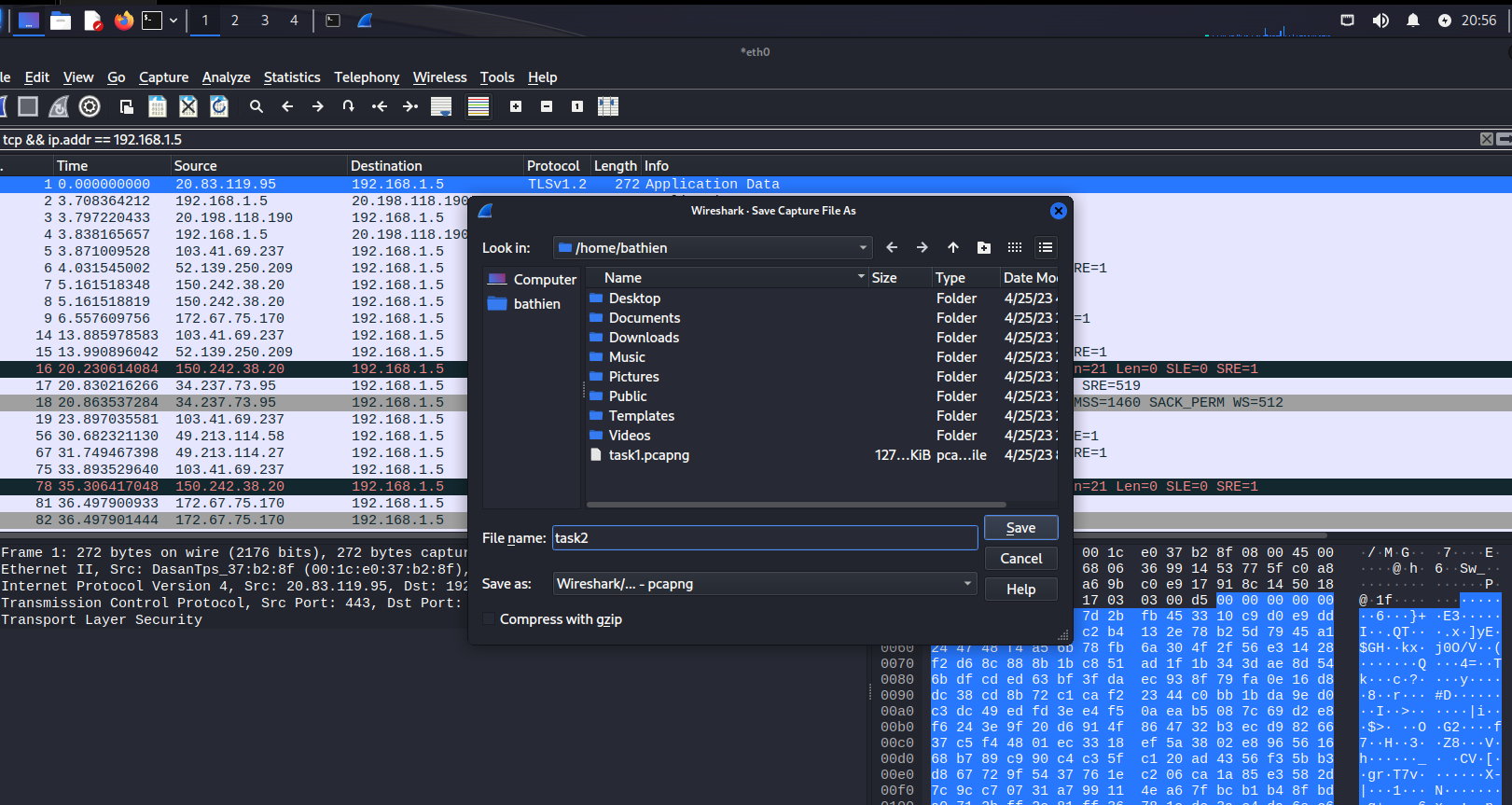
* Kỹ thuật ARP ping được sử dụng bởi nmap. Kỹ thuật này được sử dụng để tìm kiếm các thiết bị mạng bằng cách gửi yêu cầu ARP request và chờ đợi các thiết bị phản hồi với địa chỉ MAC của chúng.

**Kịch bản 2**





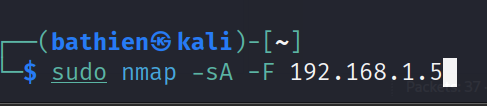


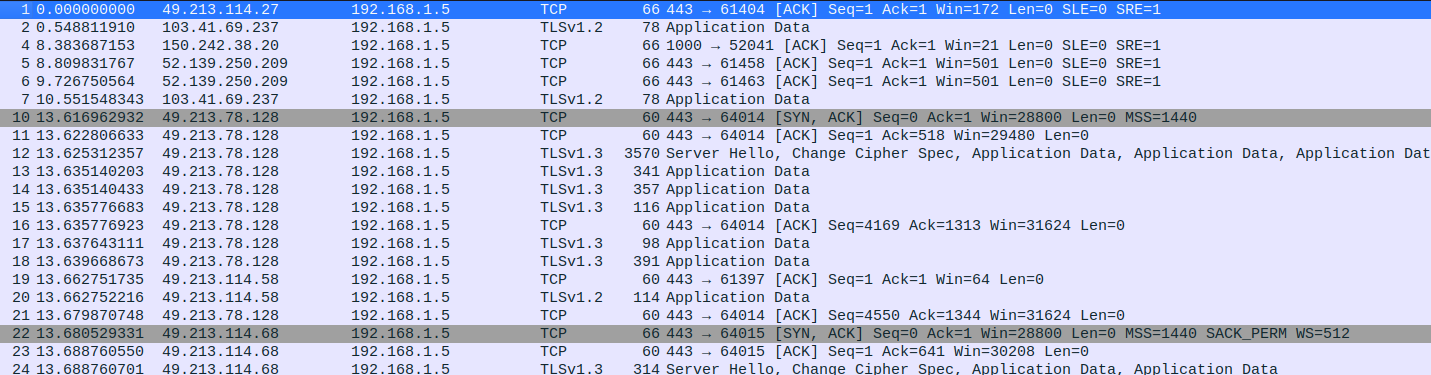


* Dựa trên kết quả bắt gói tin của file task2.pcap, ta thấy các gói tin gửi đi bởi nmap có chứa cờ SYN, điều này cho thấy rằng nmap đã sử dụng kỹ thuật quét TCP SYN scan để quét các cổng trên máy mục tiêu. Kỹ thuật quét này thường được sử dụng để quét mạng nhanh chóng và ẩn danh, bởi vì nó không hoàn thành quá trình kết nối TCP hoàn chỉnh với máy mục tiêu. Thay vào đó, nó gửi các gói tin SYN và đợi phản hồi từ máy mục tiêu để xác định cổng nào đang mở.

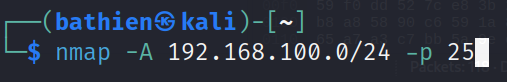
**Kịch bản 3**

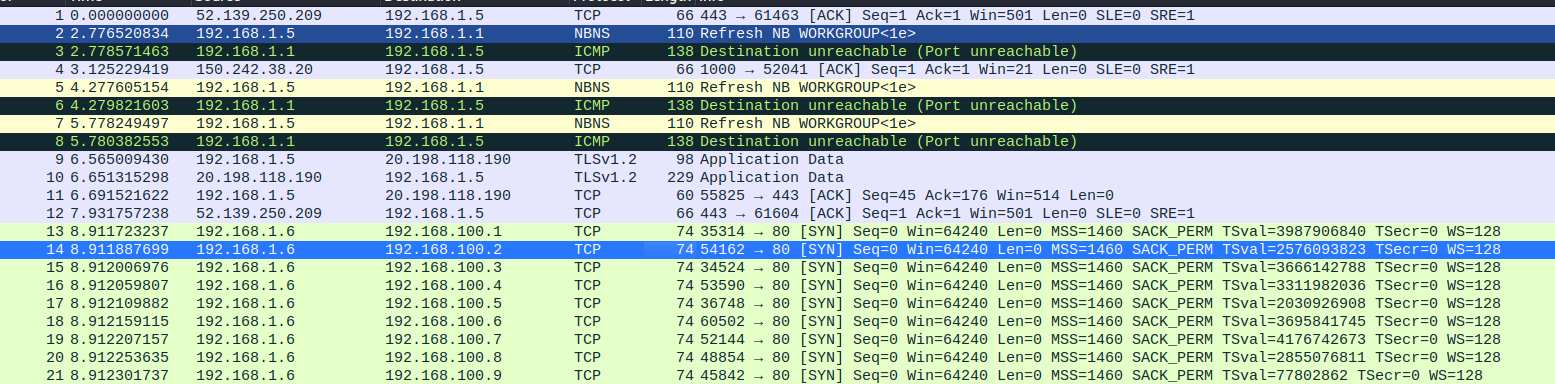
* Lệnh quét nmap "-sA" được sử dụng để thực hiện quét ACK scan. Kỹ thuật này sử dụng các gói tin ACK để xác định xem một máy chủ có đang mở một cổng hay không. Nếu máy chủ gửi trả lời RST, có nghĩa là cổng đó không mở. Nếu không có phản hồi, có thể xác định rằng cổng đó đang được mở hoặc bị chặn bởi firewall.

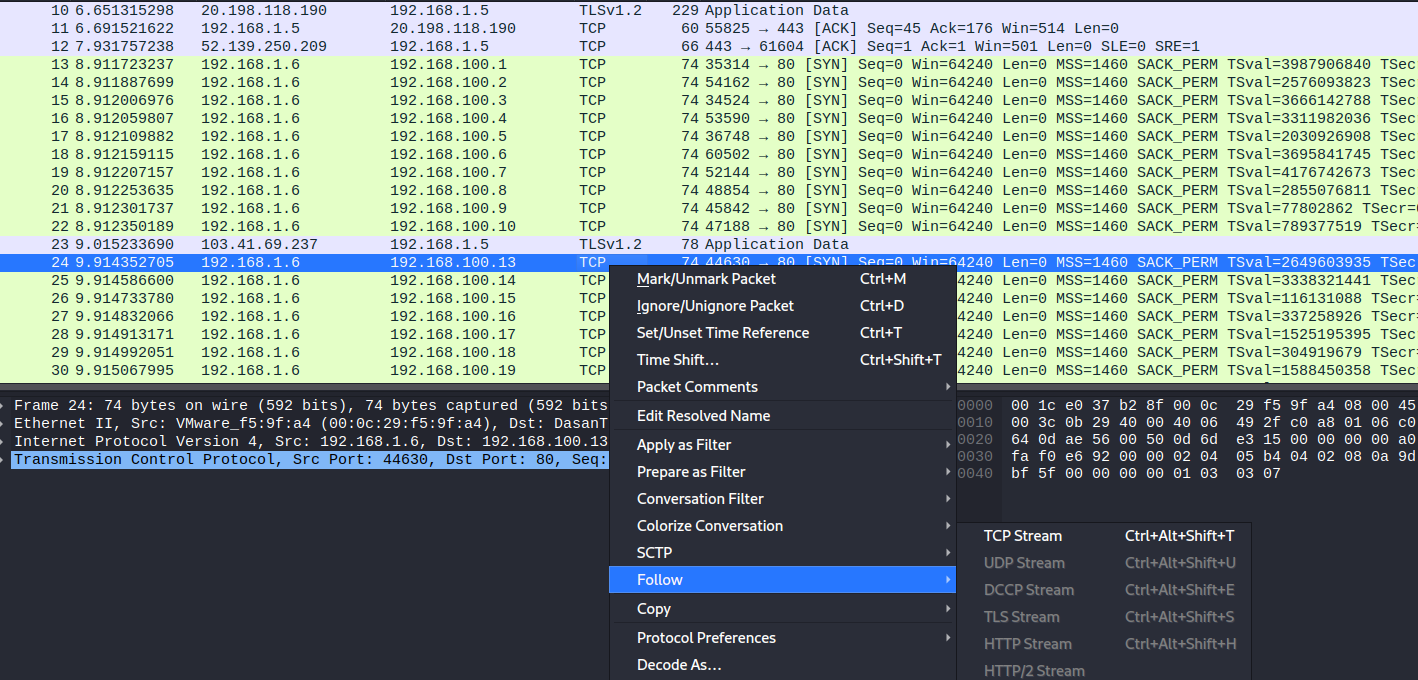




**Số 4**







//xong