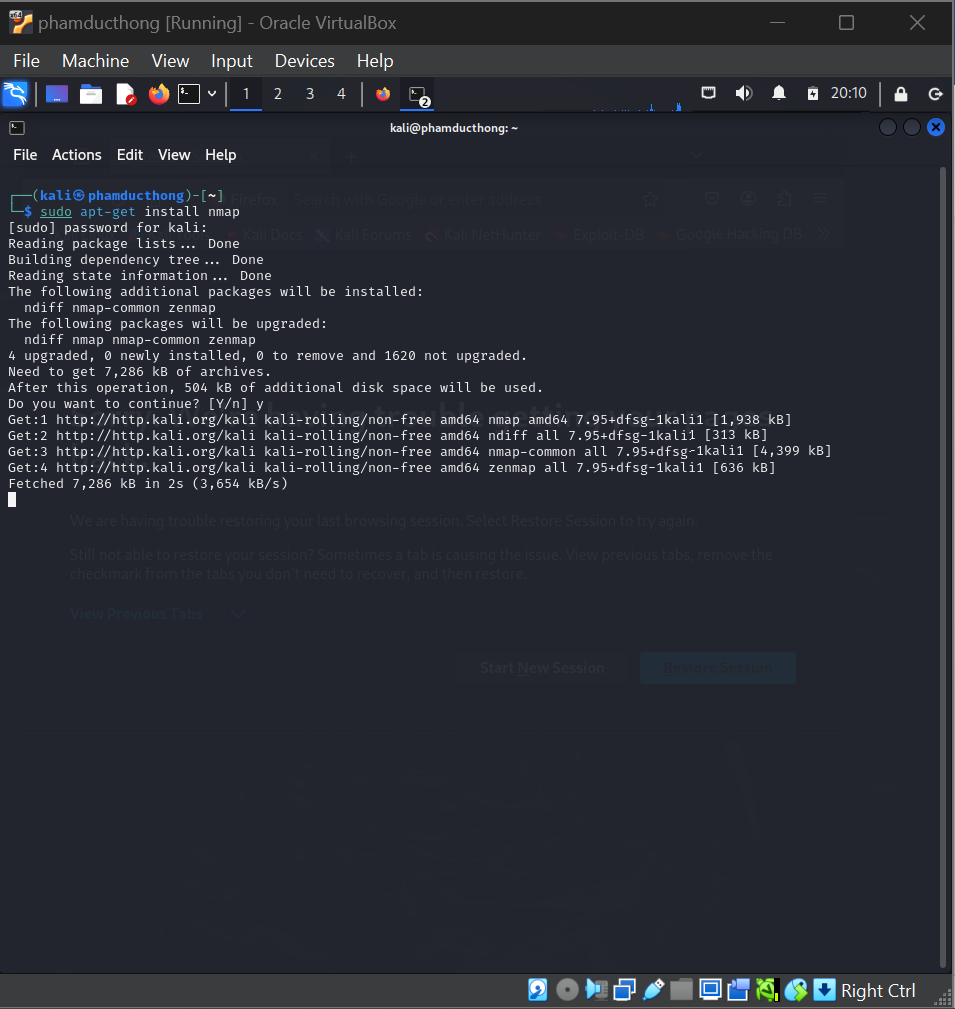
Phạm Đức Thông – 1050080119

CNPM2

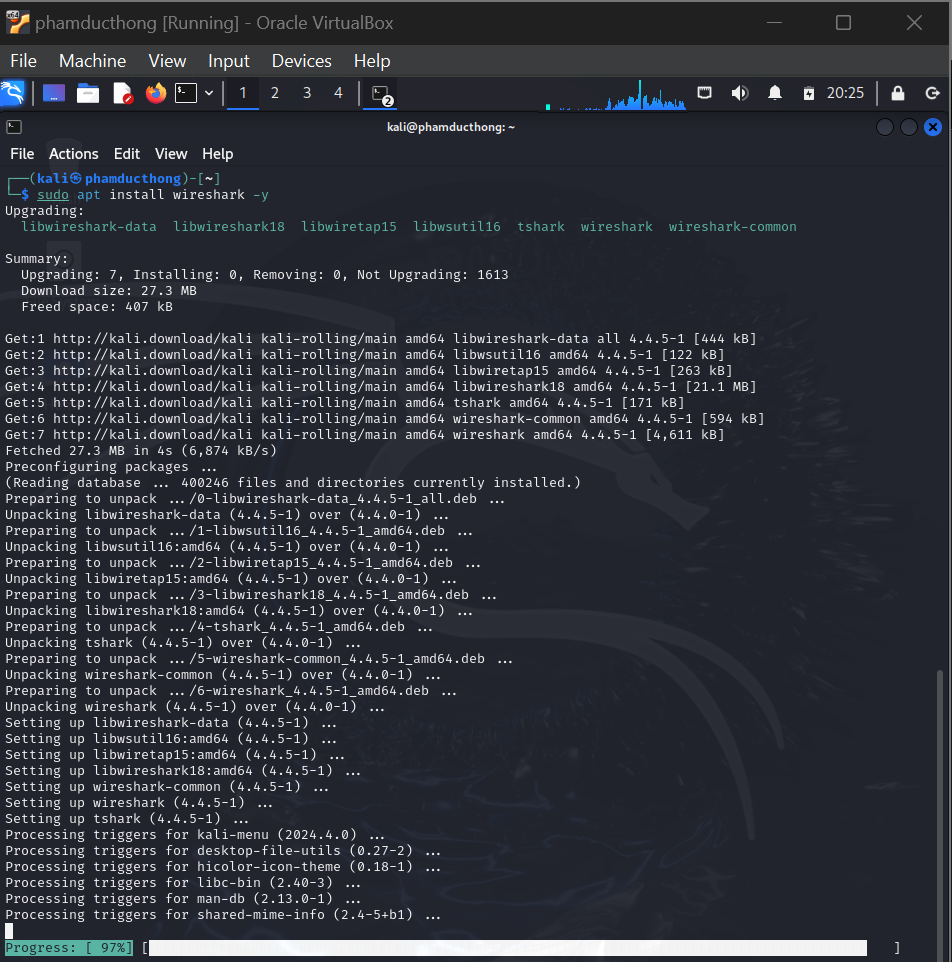
# 1

## 1.1

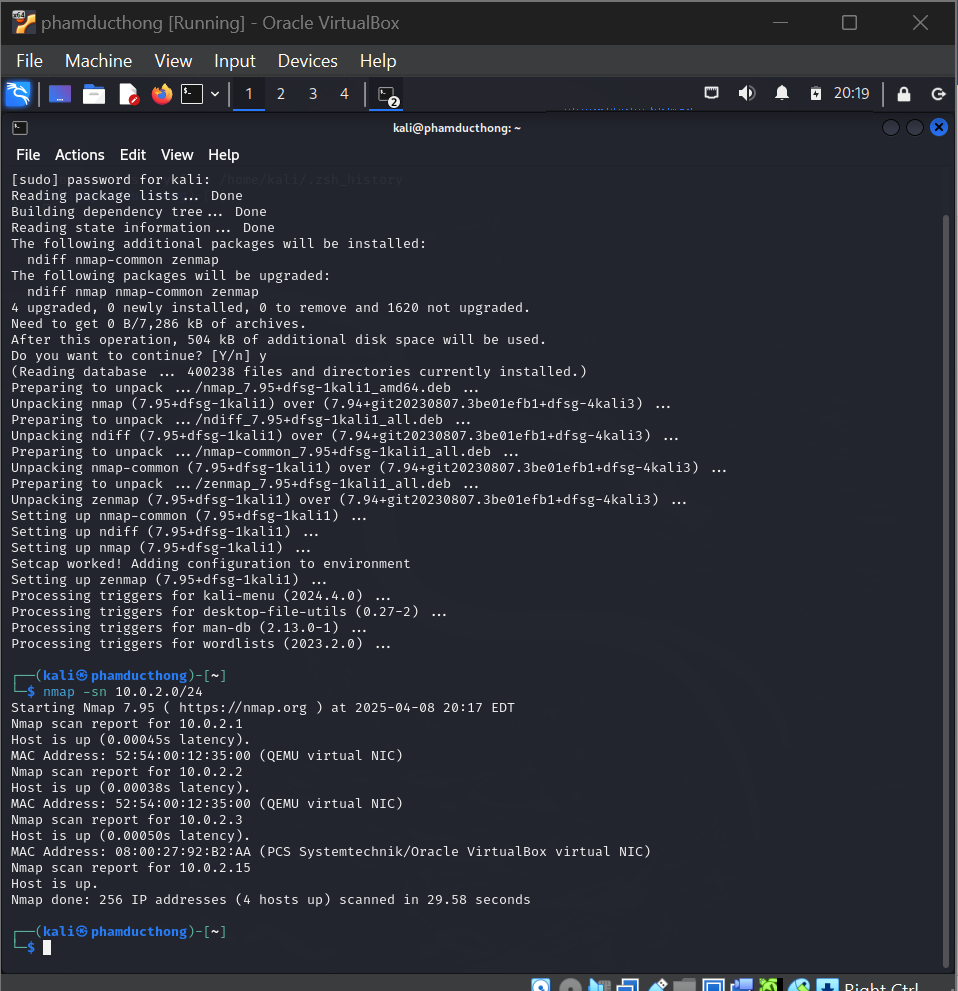
Install nmap



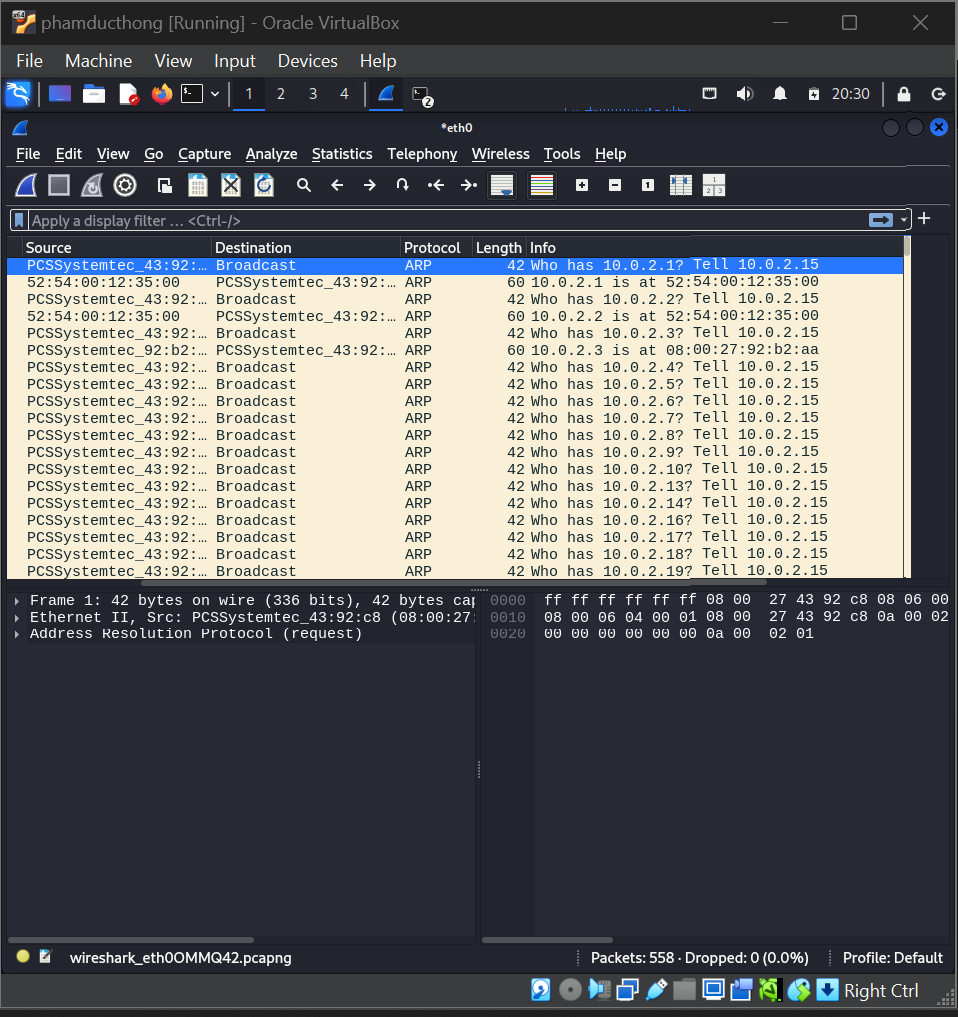
Install wireshark



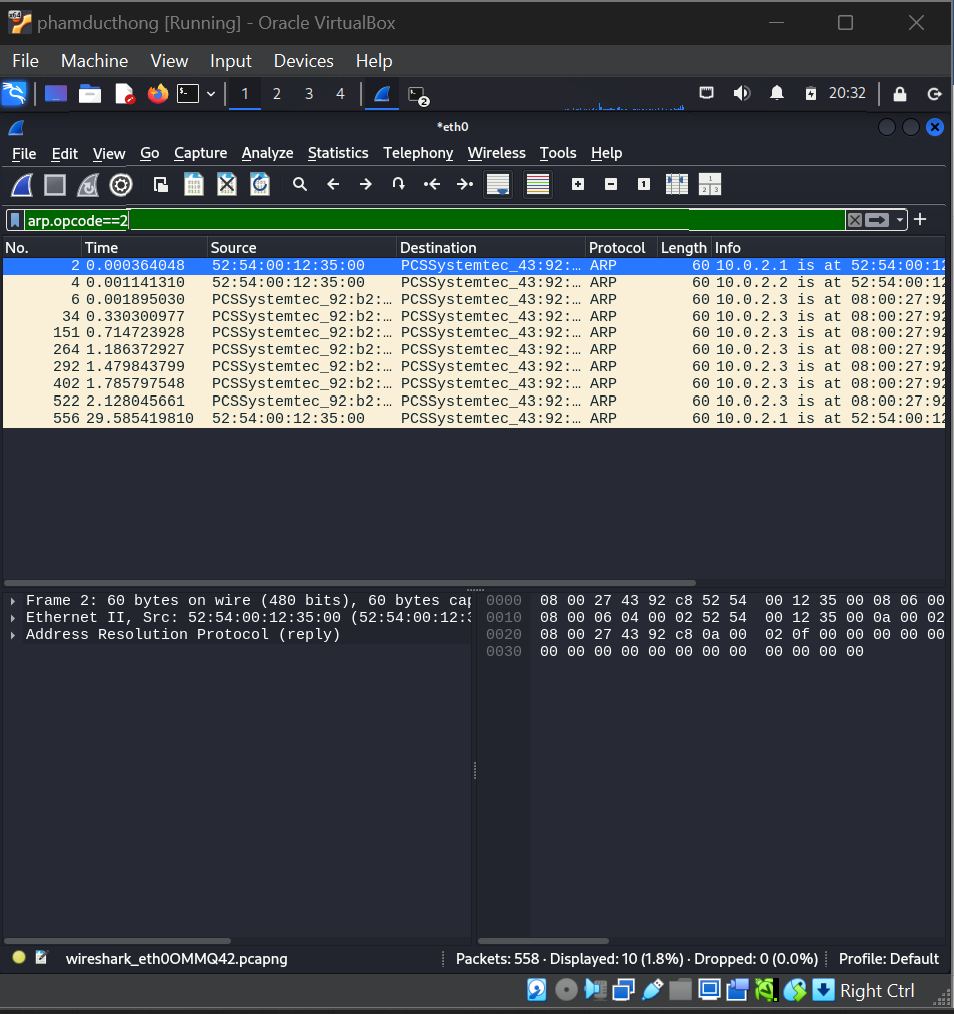
Sử dụng nmap để quét mạng



Phân tích lưu lượng



Các gói tin ARP Reply được gửi lại

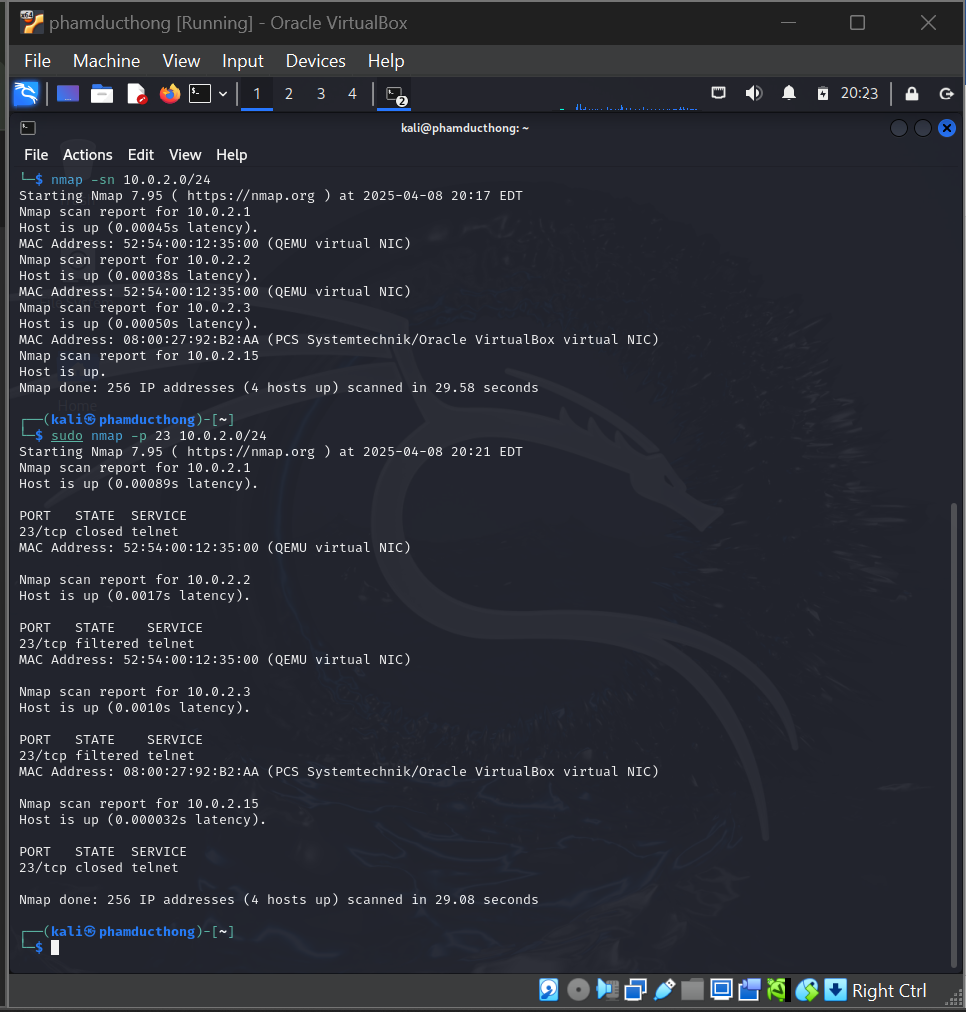


Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò:

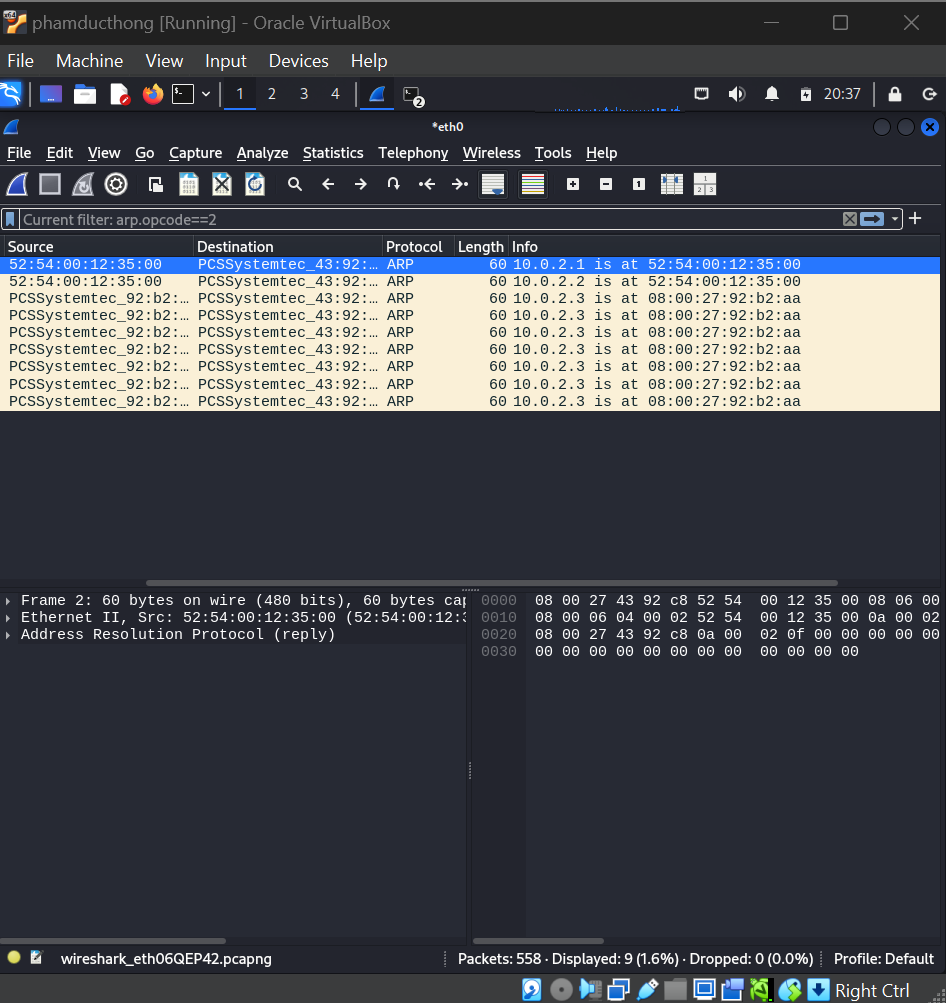
-sn (ping scan) là kỹ thuật quét thăm dò host (Host Discovery) không quét cổng.

## 1.2

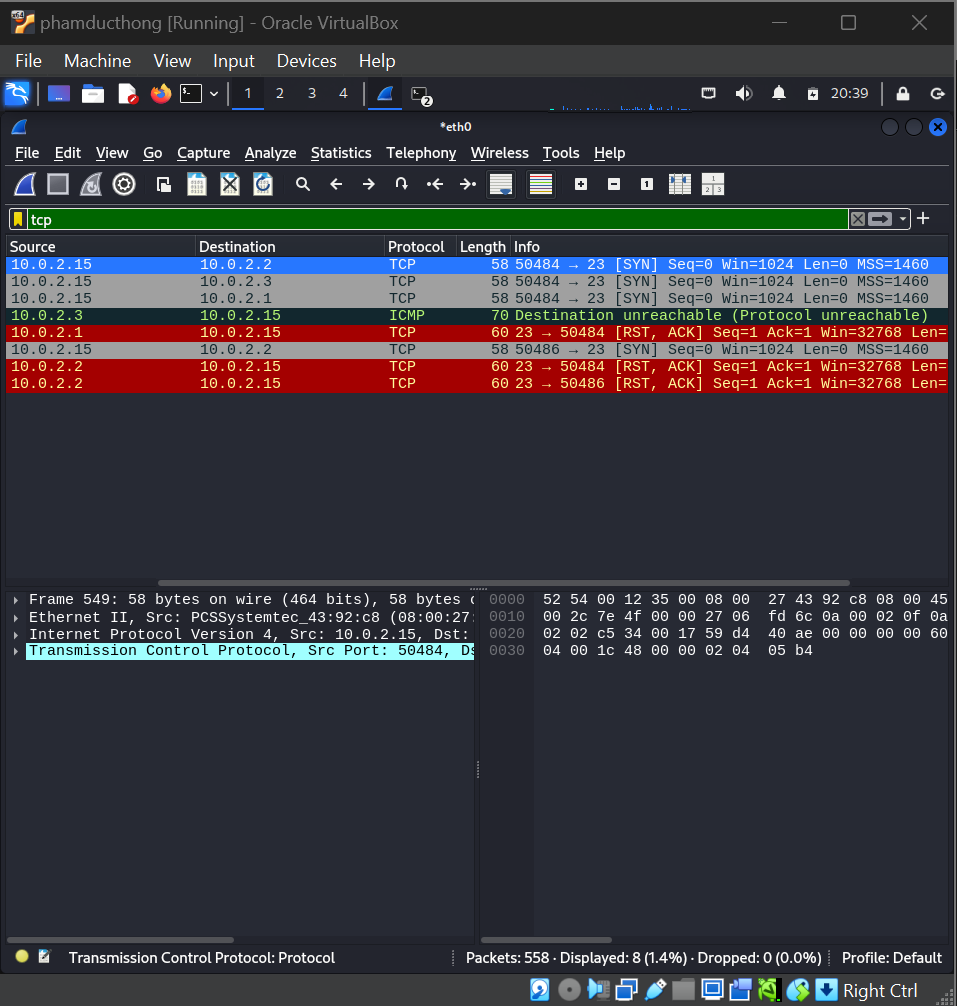
Quét thăm dò dịch vụ



Máy tấn công gửi các gói tin ARP tới máy trong mạng 10.0.2.0/24



Wireshark bắt được gói tin phù hợp với nmap trả về

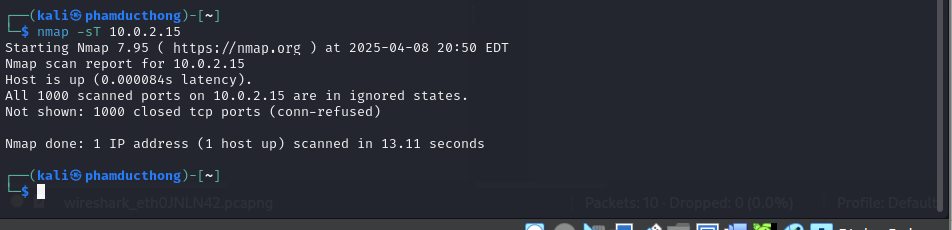


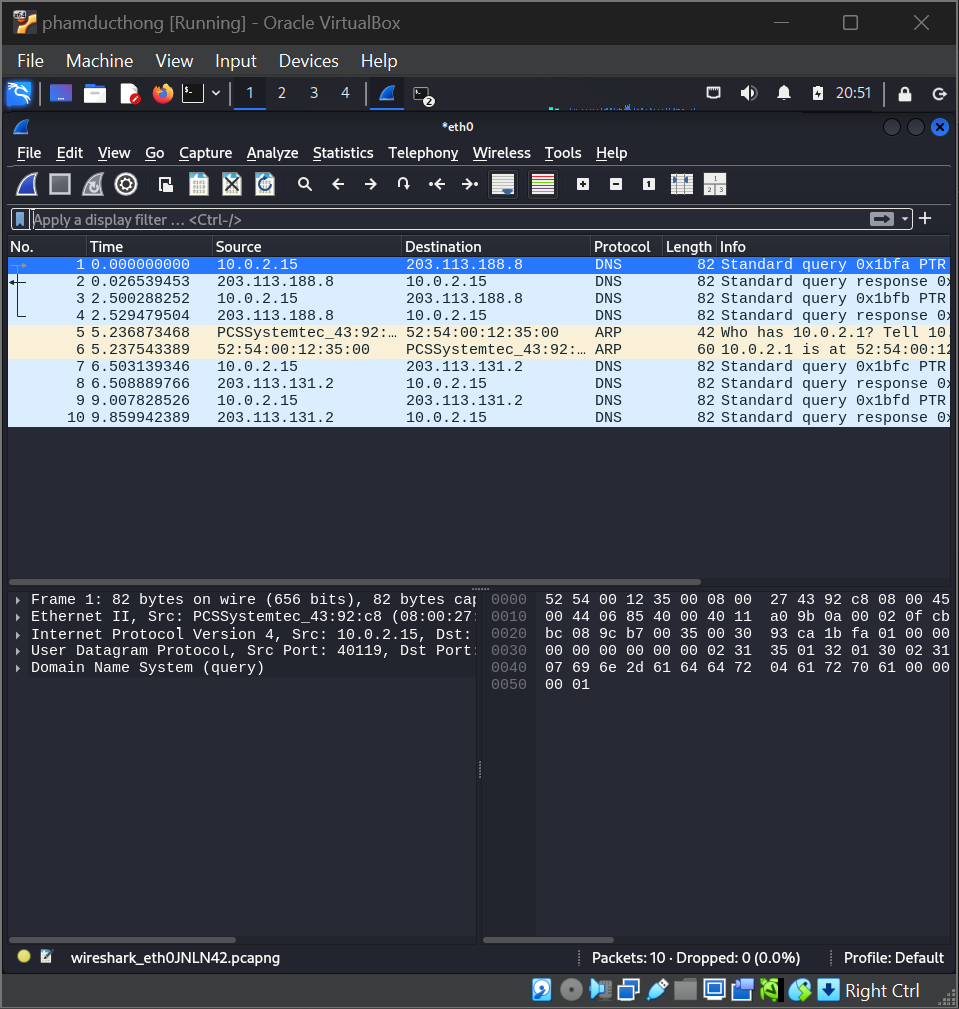
Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò:

Lệnh này thực hiện quét cổng 23 (Telnet) trên toàn bộ dải IP 10.0.2.0/24.

## 1.3

Quét cổng dịch vụ

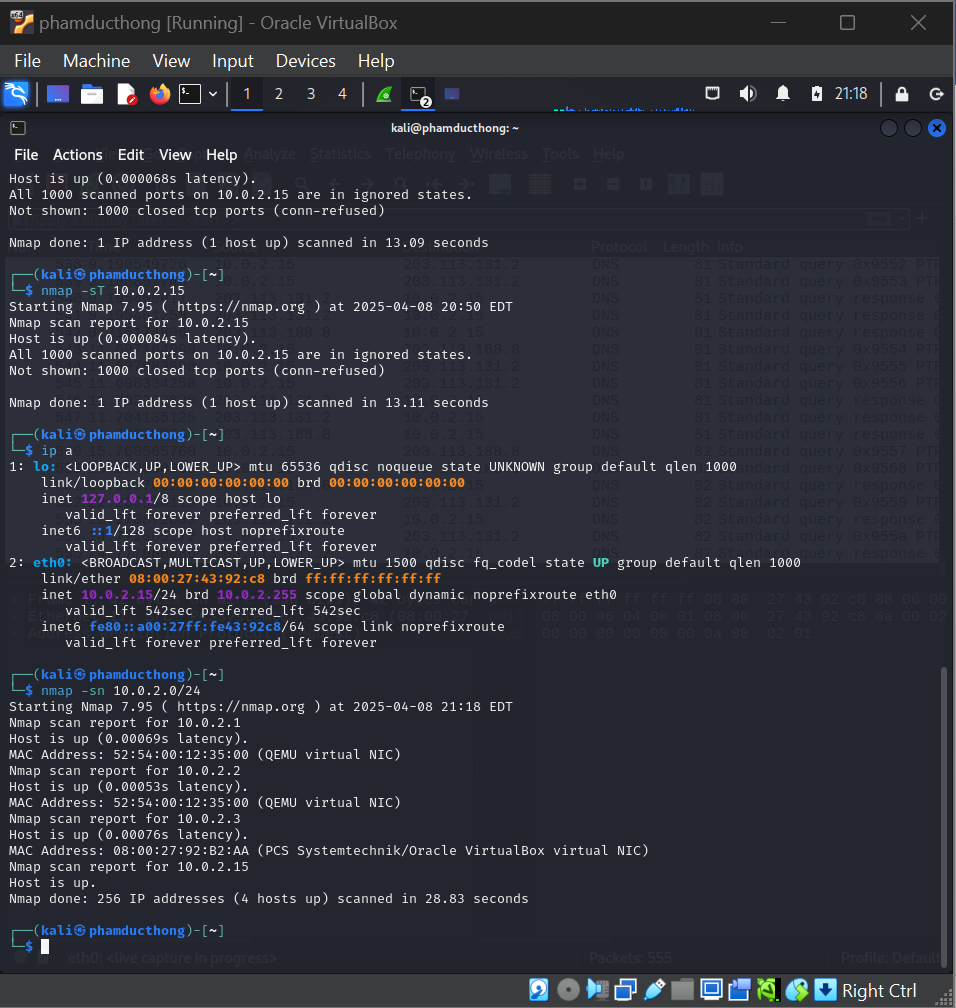




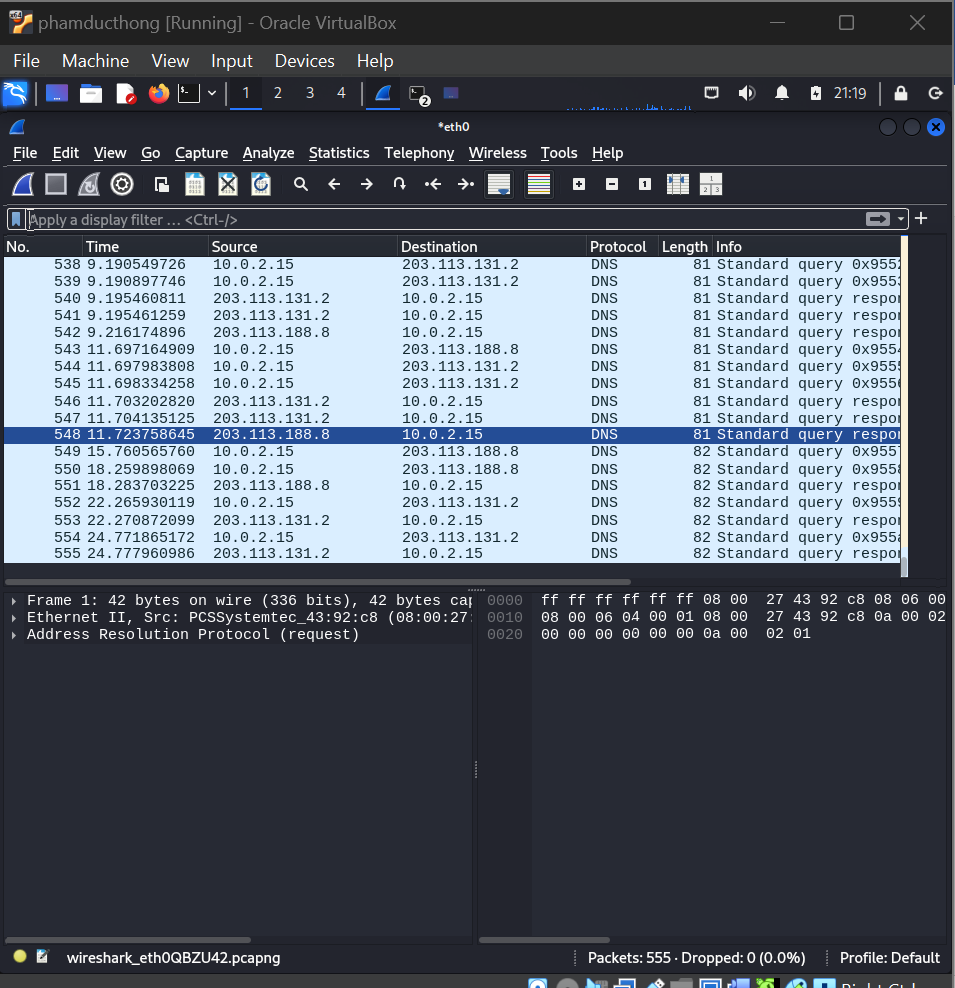
Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì:

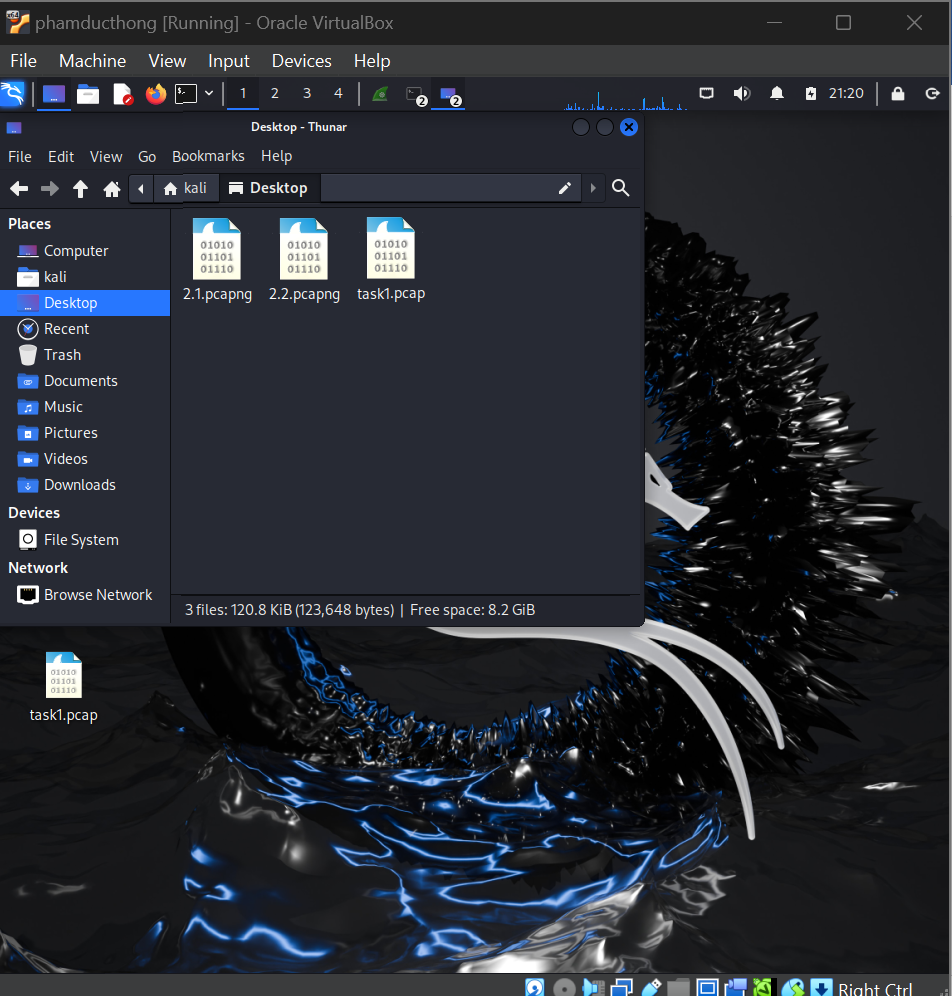
-sT là TCP Connect Scan – kỹ thuật quét dùng đầy đủ TCP 3-way handshake (SYN → SYN-ACK → ACK).

Kịch bản 1

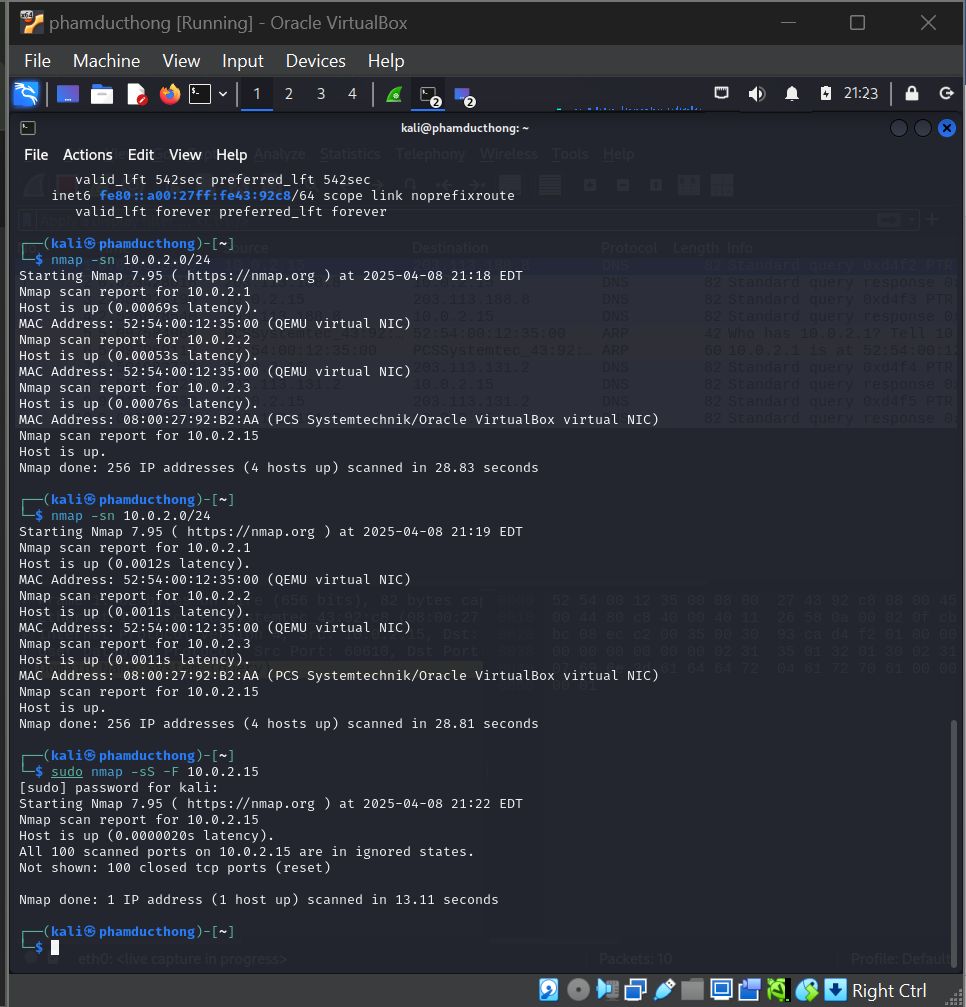


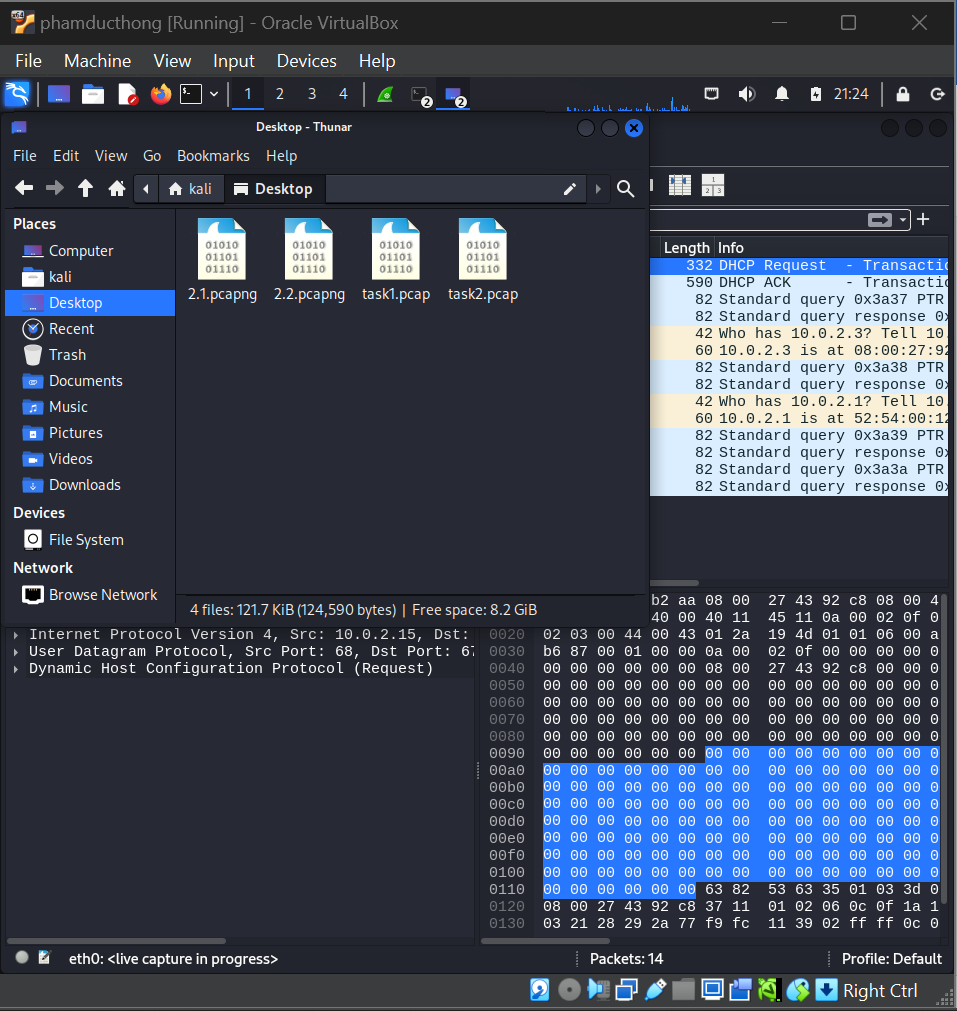
Task 1.pcap





Kịch bản 2





Kịch bản 3

