Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên làm quen với công cụ phân tích mạng Wireshark và giao thức ICMP

Yêu cầu đối với sinh viên

Có kiến thức cơ bản về công cụ Wireshark.

Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

labtainer nsm-wireshark-icmp

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong terminal ảo sẽ xuất hiện. Bài lap tạo sẵn một file icmp-qna chứa câu hỏi và chỉ dẫn của bài lab

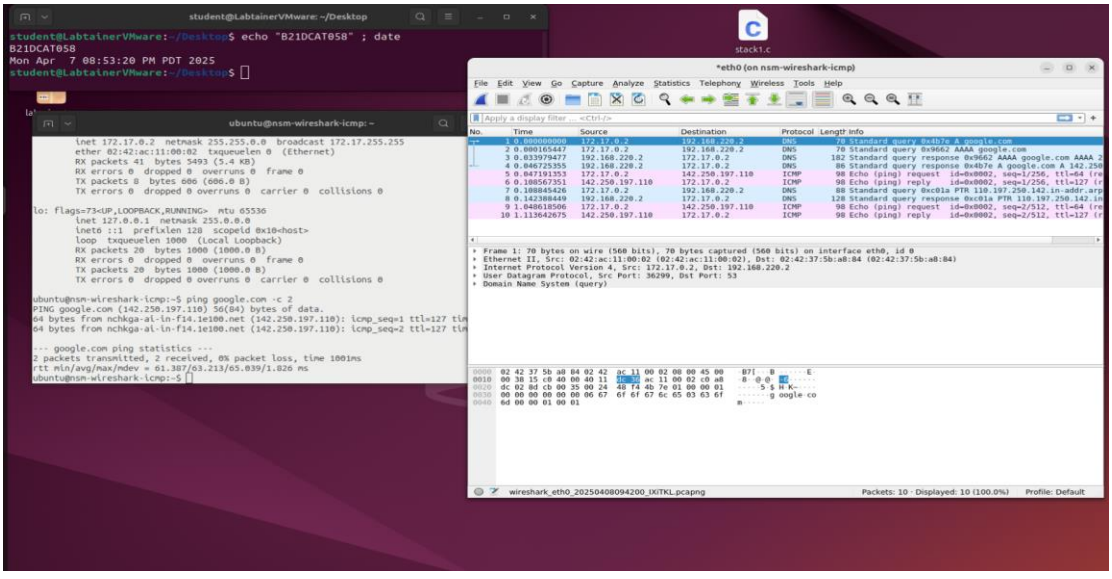
Sinh viên tạo thêm một terminal mới để mở wireshark

labtainer nsm-wireshark-icmp

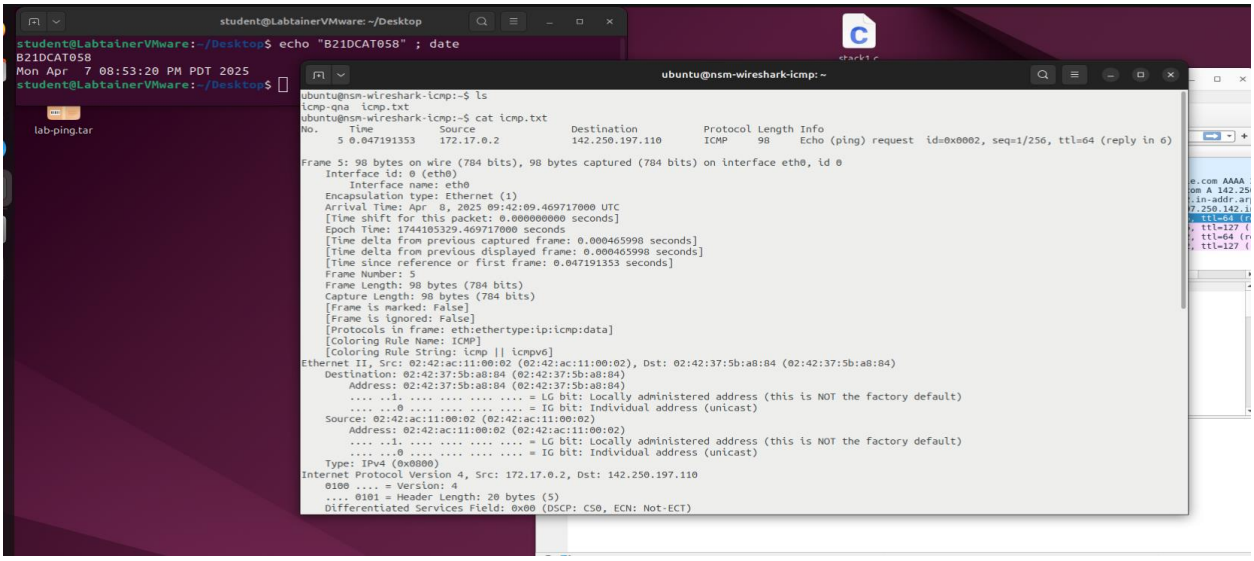
wireshark

Tại terminal còn lại sinh viên chạy lệnh ping bất kỳ (vd: google.com)

Ping google.com



Tại wireshark sinh viên chọn eth0 để xem các gói tin bắt được. chọn một gói ping request bất kỳ rồi export ra file icmp.txt. Lưu ý phải mở rộng tất cả các trường trước khi export

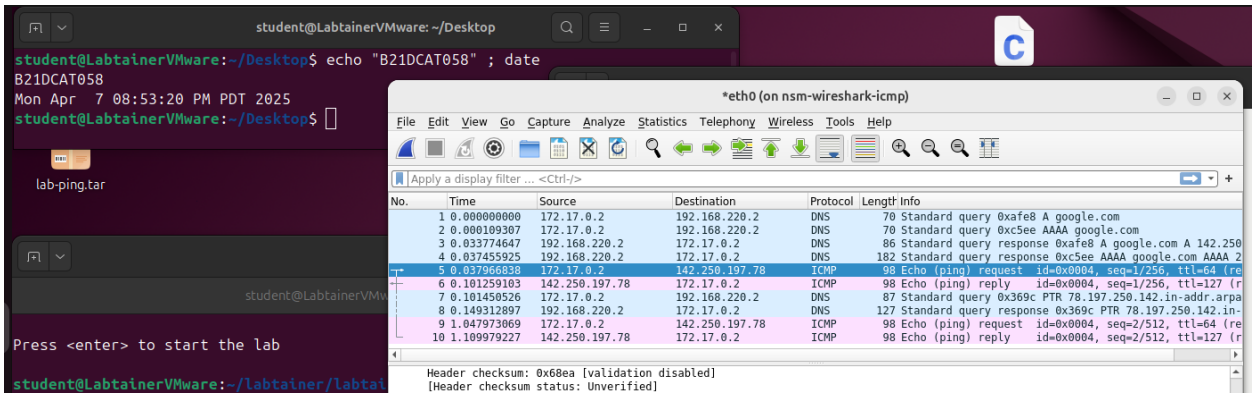


Sau khi export file thành công, sinh viên mở lại file icmp-qna để trả lời câu hỏi liên quan đến gói tin vừa bắt được

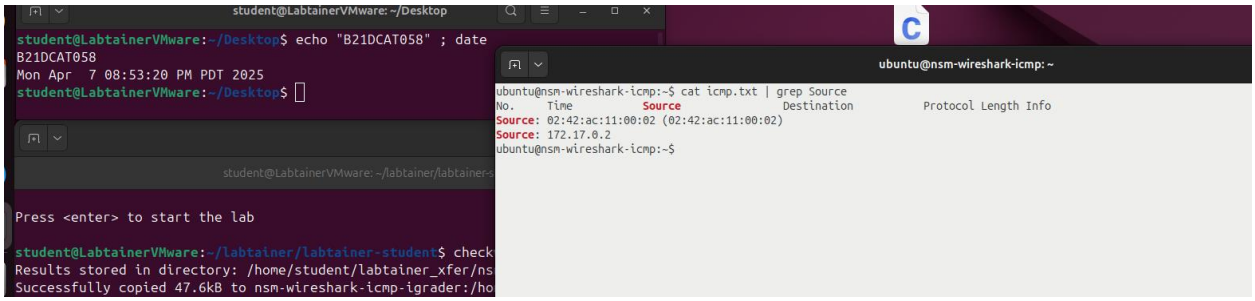
nano icmp-qna

Các câu hỏi trong bài thực hành này bao gồm:

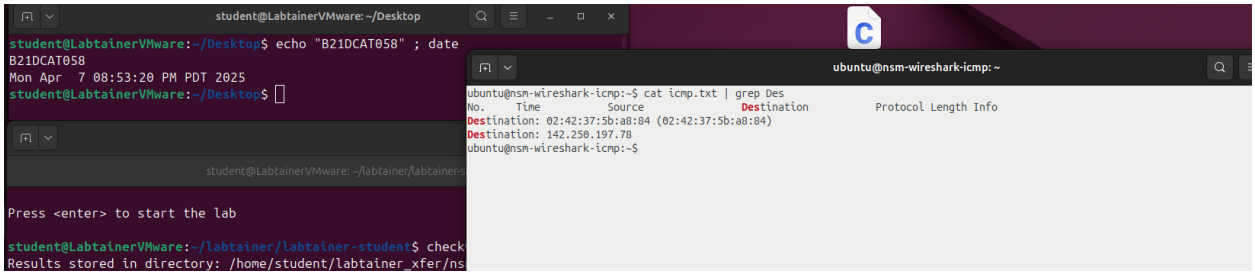
- Gói tin có số cổng nguồn và đích không? Không
- Số thứ tự của gói tin: 5



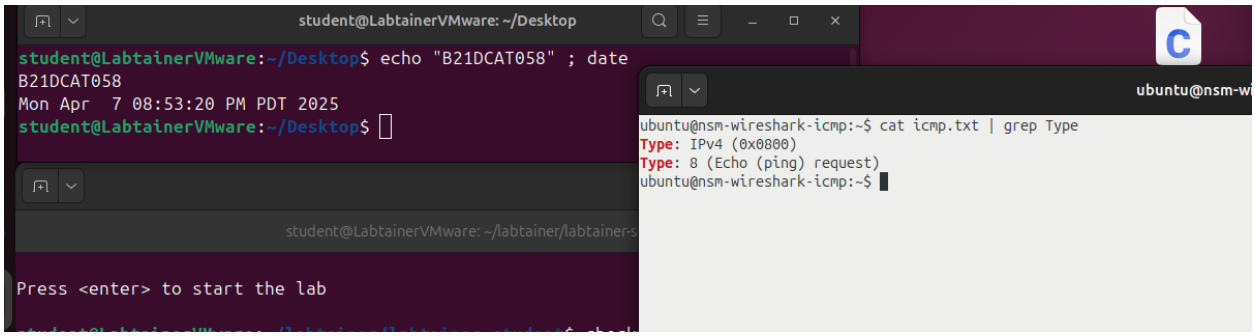
- Địa chỉ nguồn: 172.17.0.2



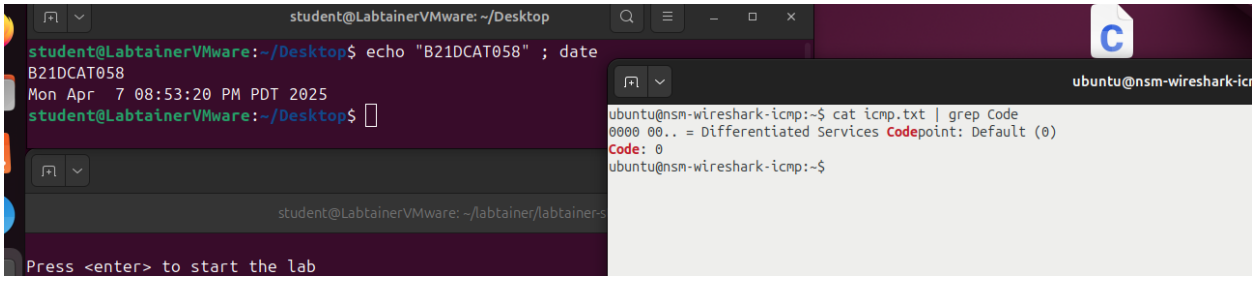
- Địa chỉ đích: 142.250.197.78



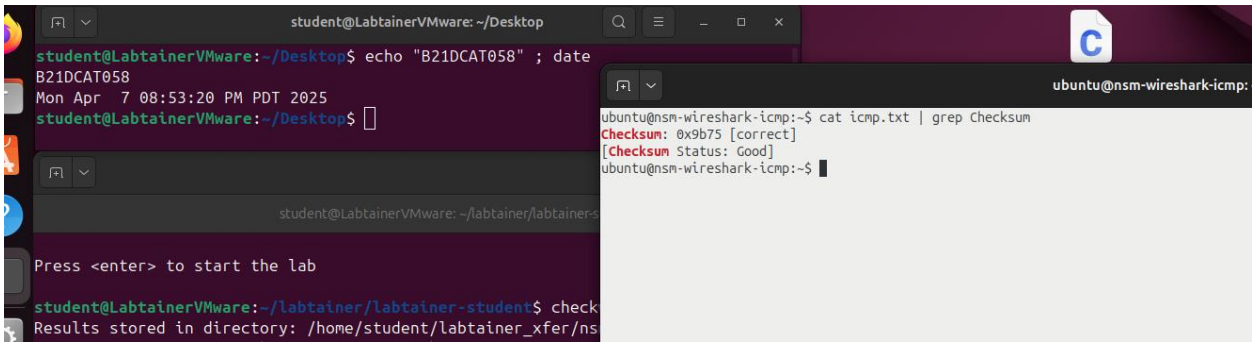
- Giá trị trường type number: 8



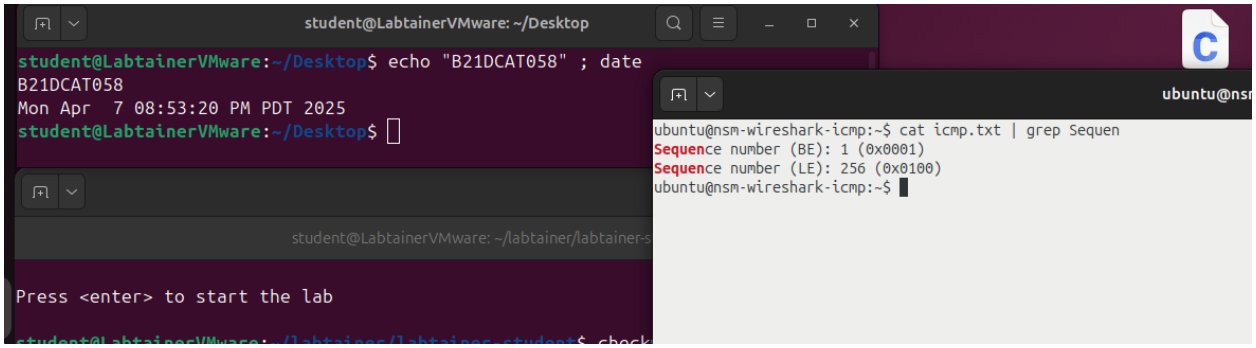
- Giá trị trường code number: 0



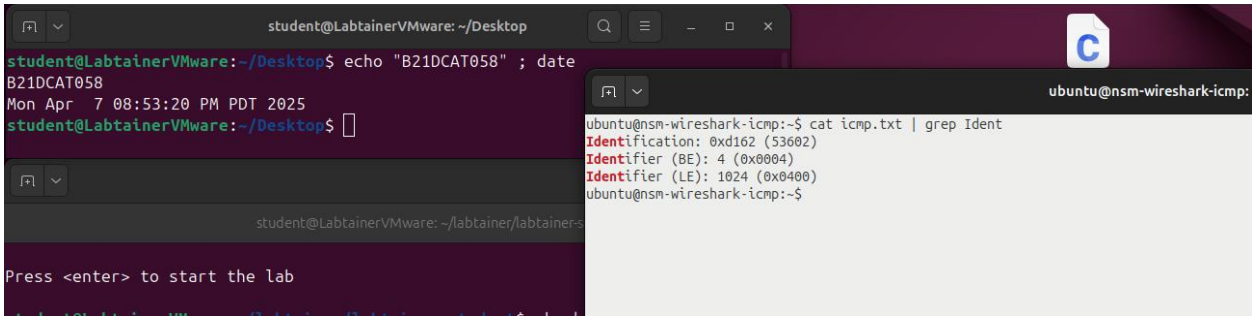
- Giá trị trường checksum: 0x9b75



- Giá trị trường Sequence Number (BE): 1



- Giá trị trường Identifier(BE)



Định dạng lại file icmp.txt để có thể checkwork:

sed -i 's/^[[:space:]]//' icmp.txt*

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer –r nsm-wireshark-icmp