Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên nắm vững các khái niệm cơ bản mà còn nâng cao khả năng nhận diện các nguy cơ bảo mật tiềm ẩn trong hệ thống mạng, từ đó biết cách phòng chống và bảo vệ hệ thống một cách hiệu quả.

Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ wireshark.

Nội dung thực hành

Khởi động bài lab:

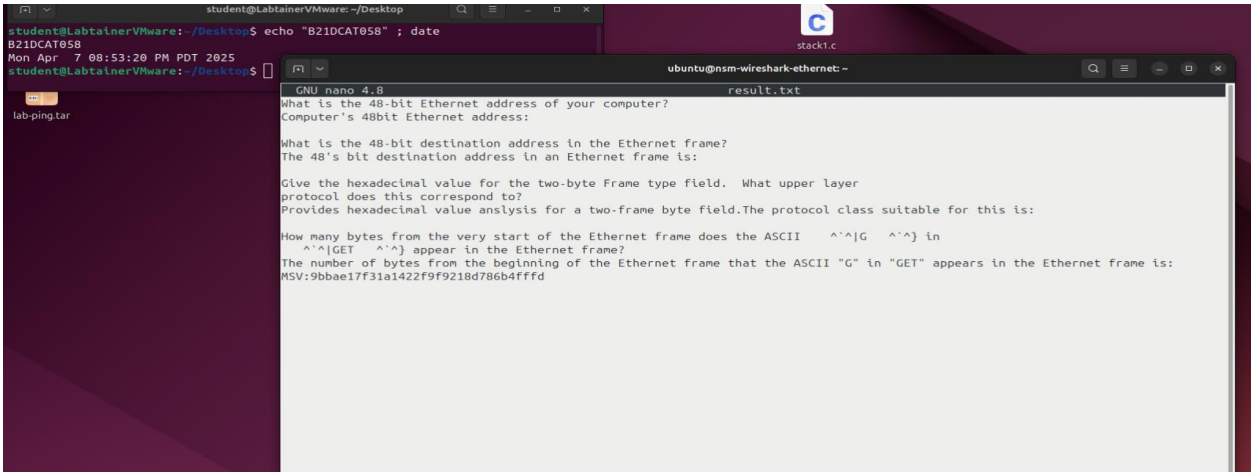
Vào terminal, gõ:

labtainer -r nsm-wireshark-ethernet

(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 một terminal ảo sẽ xuất hiện. Trên terminal thực hiện mở file result.txt để điền kết quả:

sudo nano result.txt

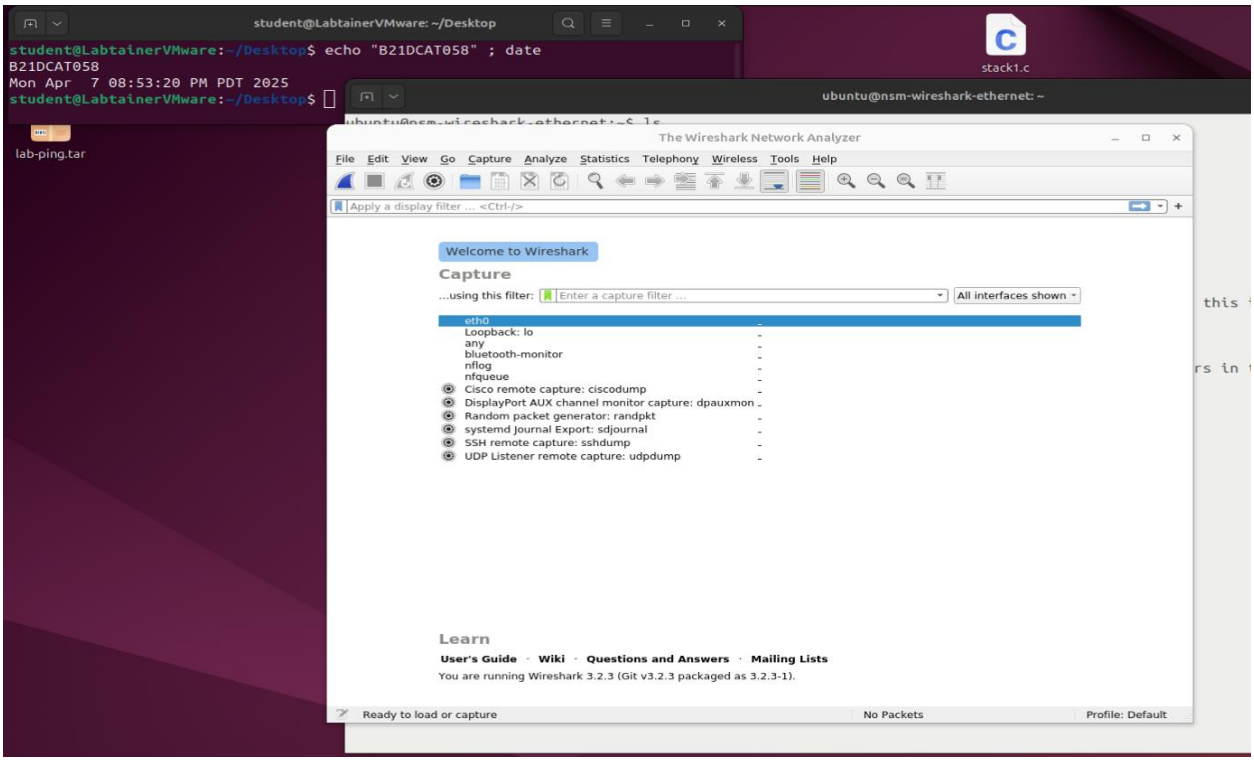


Bài lab đã tạo sẵn 1 file ethernet.pcap chứa nội dung các gói tin đã chụp. Chúng ta sẽ thực hiện mở file này bằng wireshark và thực hiện phân tích và trả lời câu hỏi trong file result.txt

Từ file ethernet.pcap ta sẽ tìm được các gói tin phù hợp với câu hỏi

Câu trả lời sẽ phải điền vào file *result.txt*.

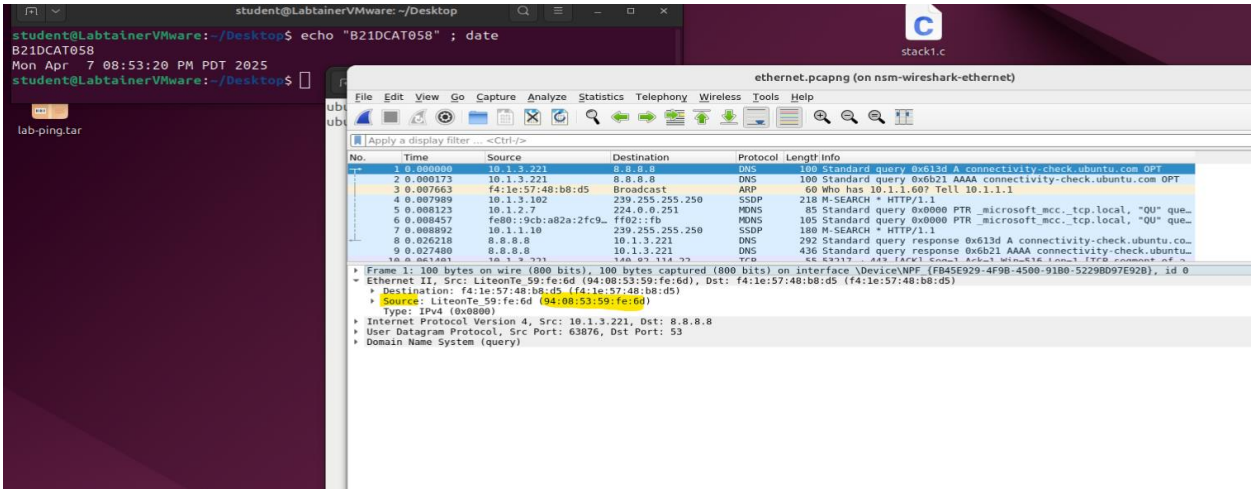
Thực hiện chạy lệnh “wireshark & ” để mở wireshark và phân tích gói tin:



Task 1: Địa chỉ MAC 48-bit của máy

➔ **Computer's 48bit Ethernet address:94:08:53:59:fe:6d**

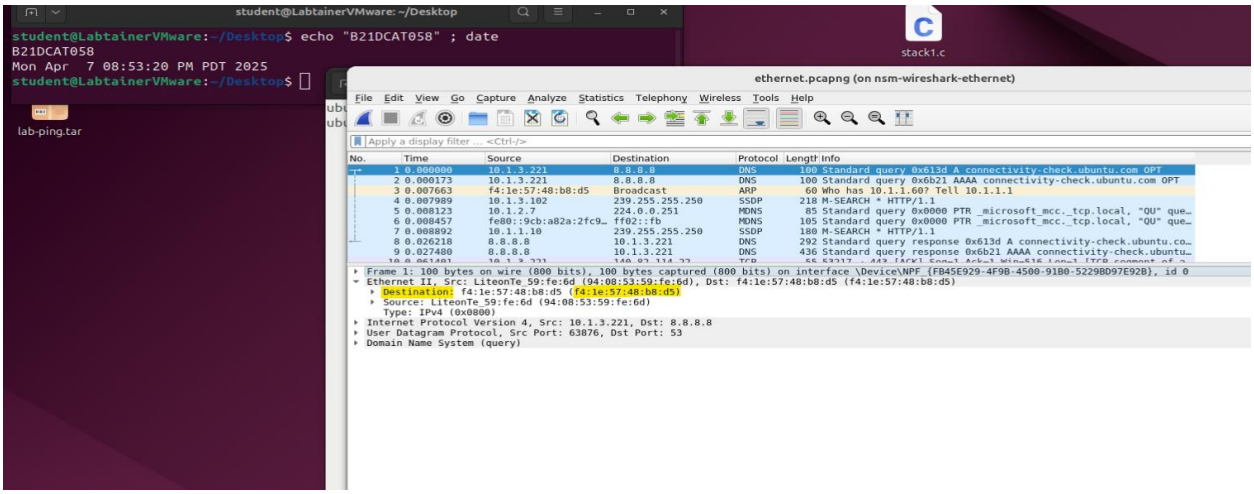
Trường **Source** trong phần Ethernet là địa chỉ MAC



Task 2: Địa chỉ MAC đích trong khung Ethernet

➔ **The 48's bit destination address in an Ethernet frame is:f4:1e:57:48:b8:d5**

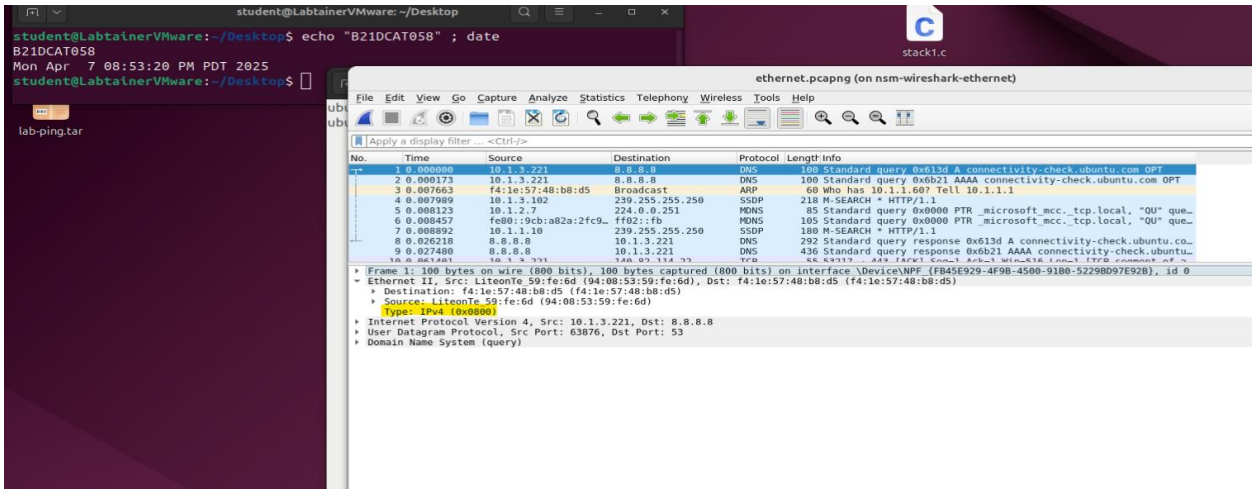
Trường **Destination** trong phần Ethernet chính là địa chỉ đích



Task 3: Giá trị Hex 2 byte của Frame Type + giao thức ứng với nó

➔ **Provides hexadecimal value anslysis for a two-frame byte field.The protocol class suitable for this is:0x0800**

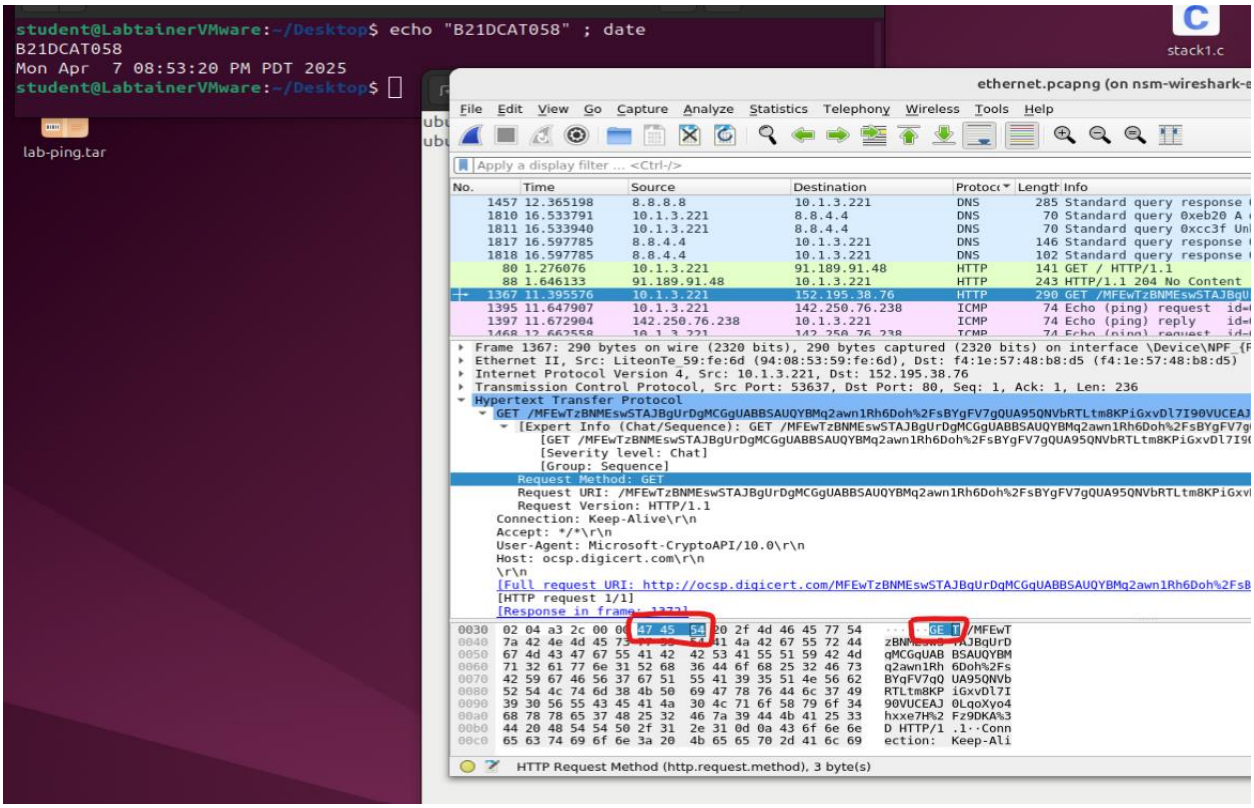
Trong phần **Ethernet II**, xem mục **Type**



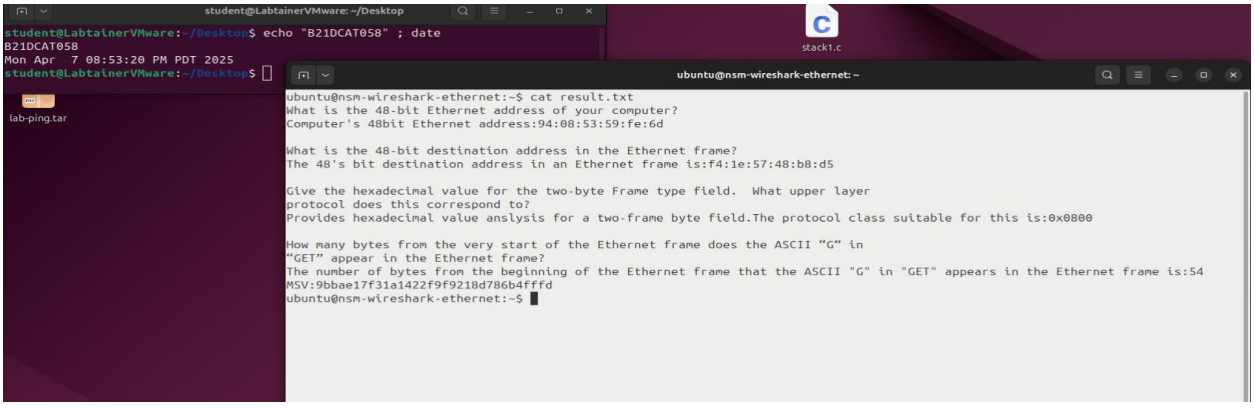
Task 4: Vị trí byte chứa ASCII “G” trong “GET”

➔ **The number of bytes from the beginning of the Ethernet frame that the ASCII "G" in "GET" appears in the Ethernet frame is:54**

Chọn gói HTTP chứa phương thức “GET”, vào khung Packet Bytes → bên phải có chuỗi ASCII, tìm chữ **G** trong “GET” → Di chuột lên, phía dưới sẽ hiển thị byte offset



Kết thúc bài lab:



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

stoplab nsm-wireshark-ethernet

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:

startlab –r nsm-wireshark-ethernet