HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: KĨ THUẬT GIÁM SÁT AN TOÀN MẠNG

Phân tích gói tin 802.11 bằng công cụ Wireshark

Sinh viên thực hiện: Nguyễn Tuấn Đạt – B21DCAT058

Giảng viên hướng dẫn: THs. Ninh Thị Thu Trang

HÀ NỘI 3-2025

Mục lục

Nội dung và hướng dẫn bài thực hành

1. Mục đích

Giúp sinh viên nắm vững cách sử dụng Wireshark để thu thập, giám sát và phân tích các gói tin trong mạng

2. Yêu cầu đối với sinh viên

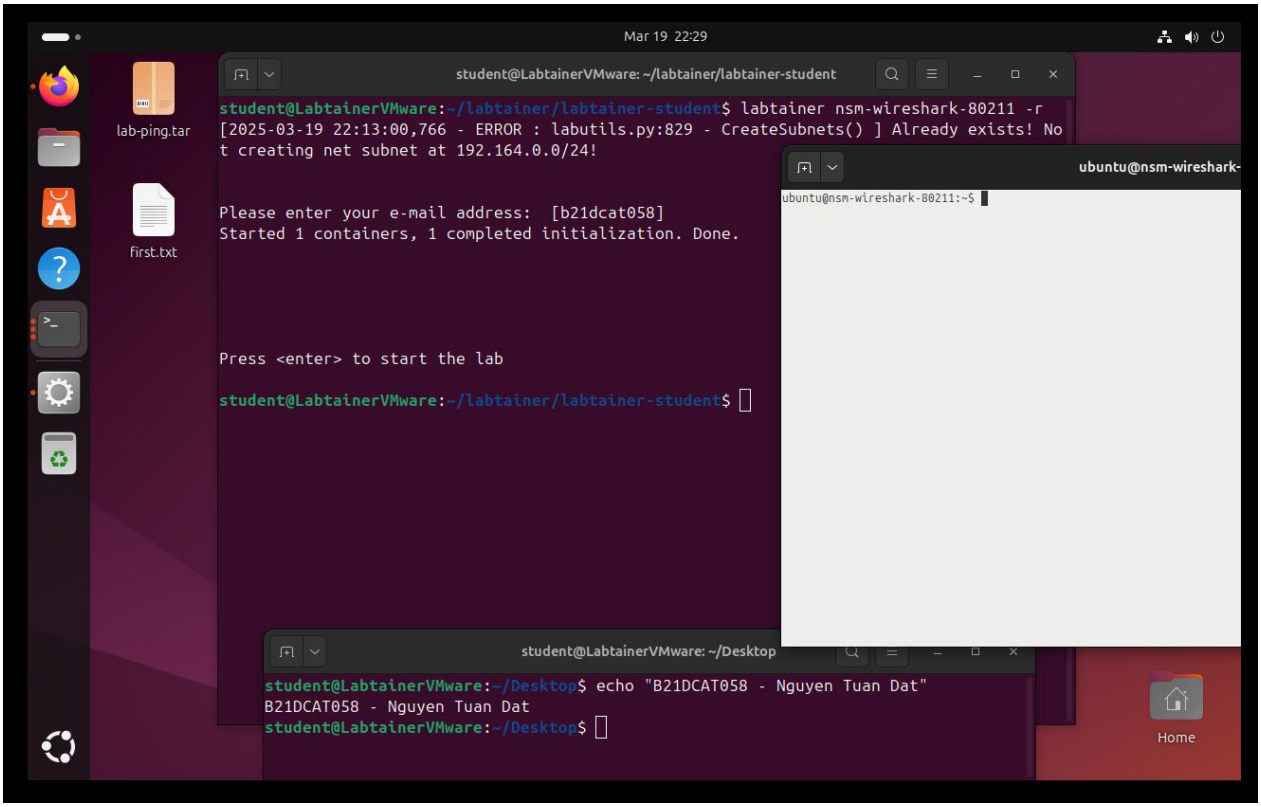
Có kiến thức cơ bản về hệ điều hành Linux, công cụ wireshark và chuẩn IEEE 802.11

3. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

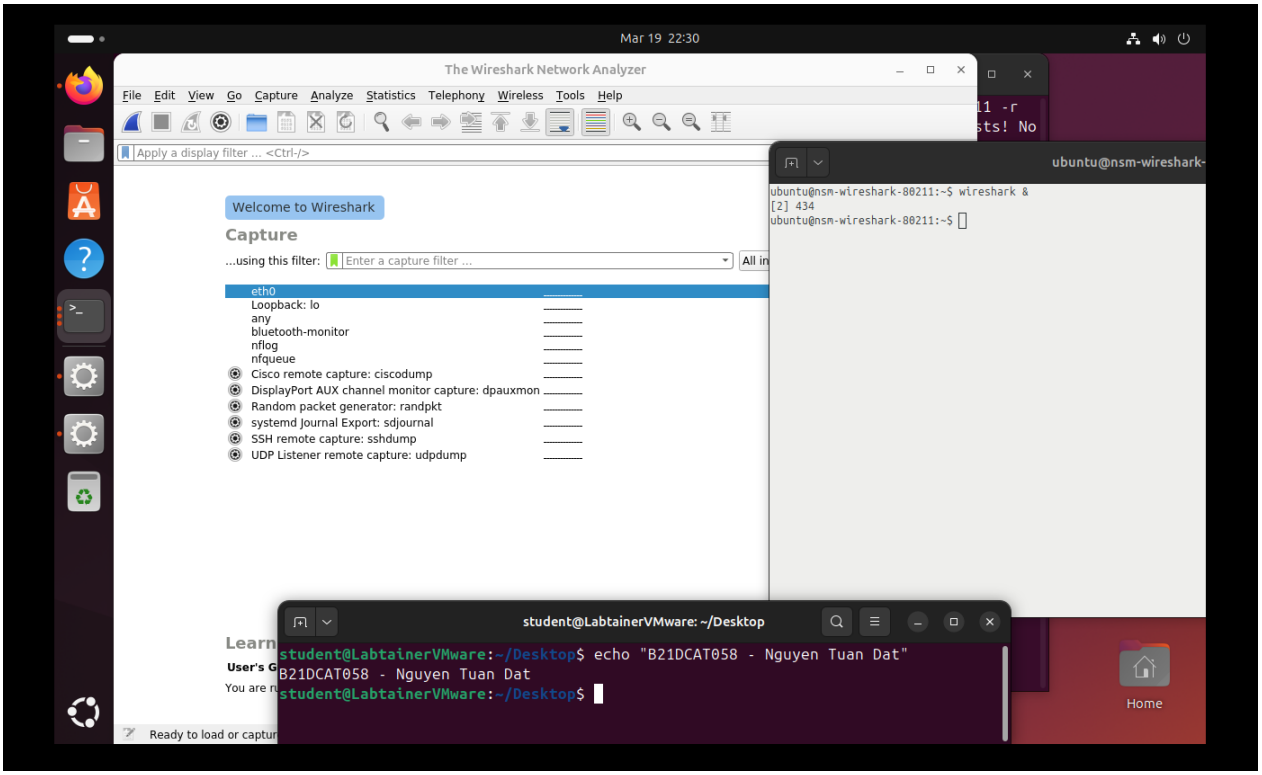
labtainer nsm-wireshark-80211



(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)

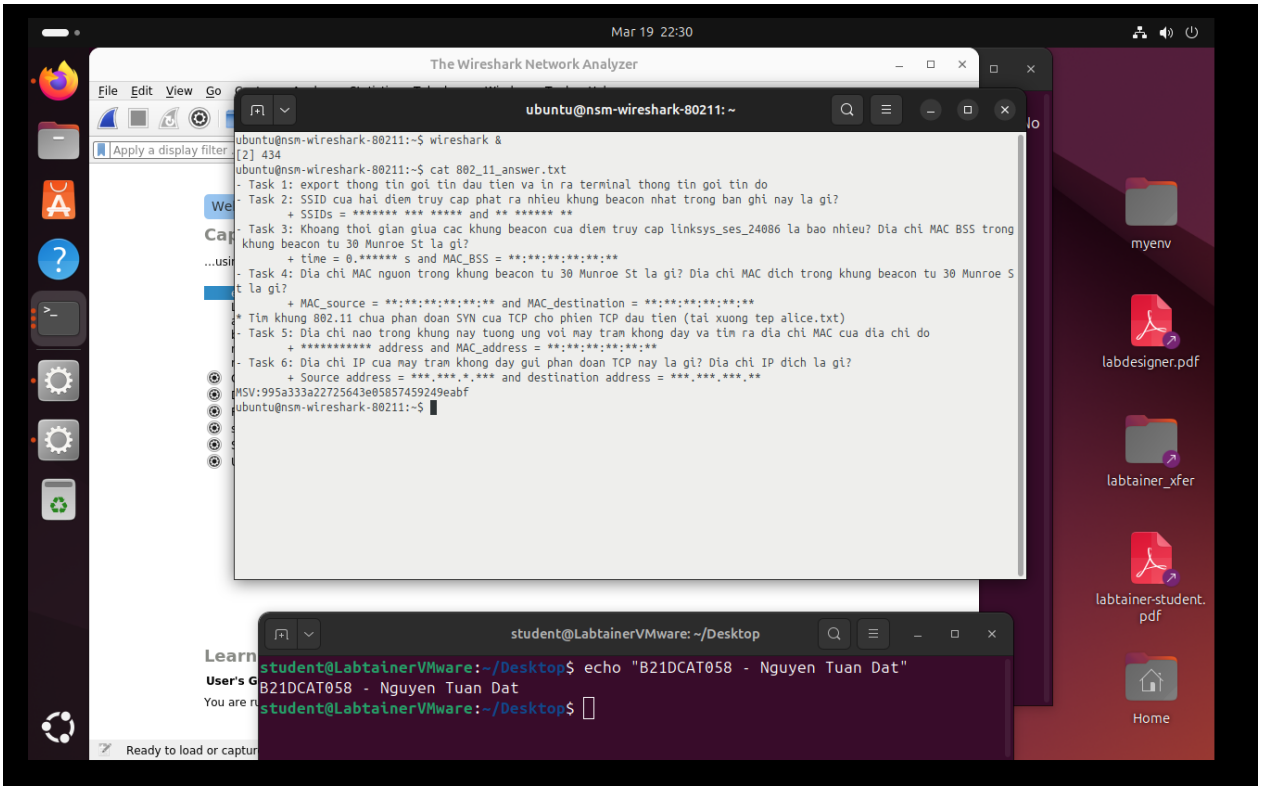
Sau khi khởi động xong một terminal ảo sẽ xuất hiện đại diện cho máy khởi chạy wireshark: nsm-wireshark-80211 và điền kết quả sau khi phân tích các gói tin .Trên terminal khởi chạy wireshark bằng câu lệnh:

Wireshark



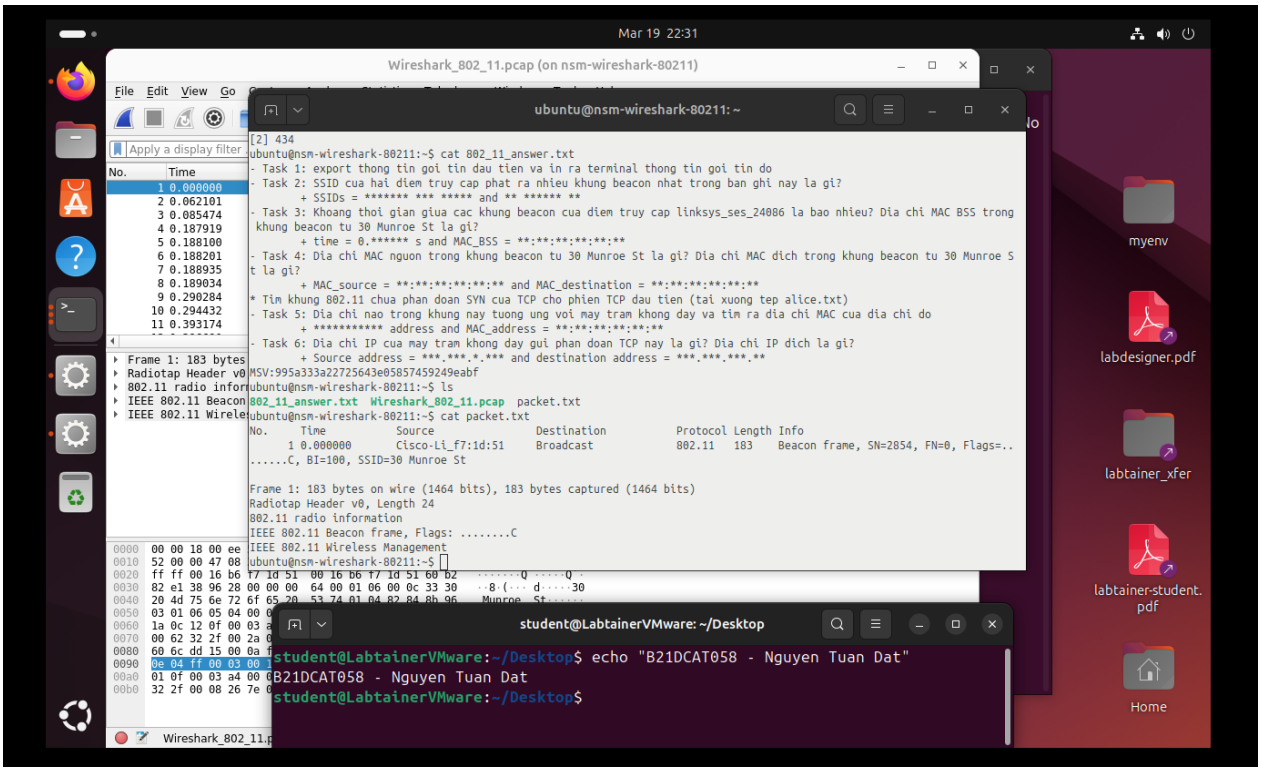
Trên máy nsm-wireshark-80211 mở file 802-11-answer chứa câu hỏi và form điền kết quả

Bài lab đã tạo sẵn 1 file 802_11_answer trong đó chứa nội dung là 1 chuỗi ngẫu nhiên và checkwork bằng mã hash đó để chống học sinh chống sao chép bài làm của nhau



Sinh viên đọc câu hỏi và phân tích các gói tin , kết quả sẽ điền vào file 802_11_answer và có câu hỏi sinh viên phải export bản ghi chứa kết quả để checkwork để chứng minh sinh viên đã làm bài

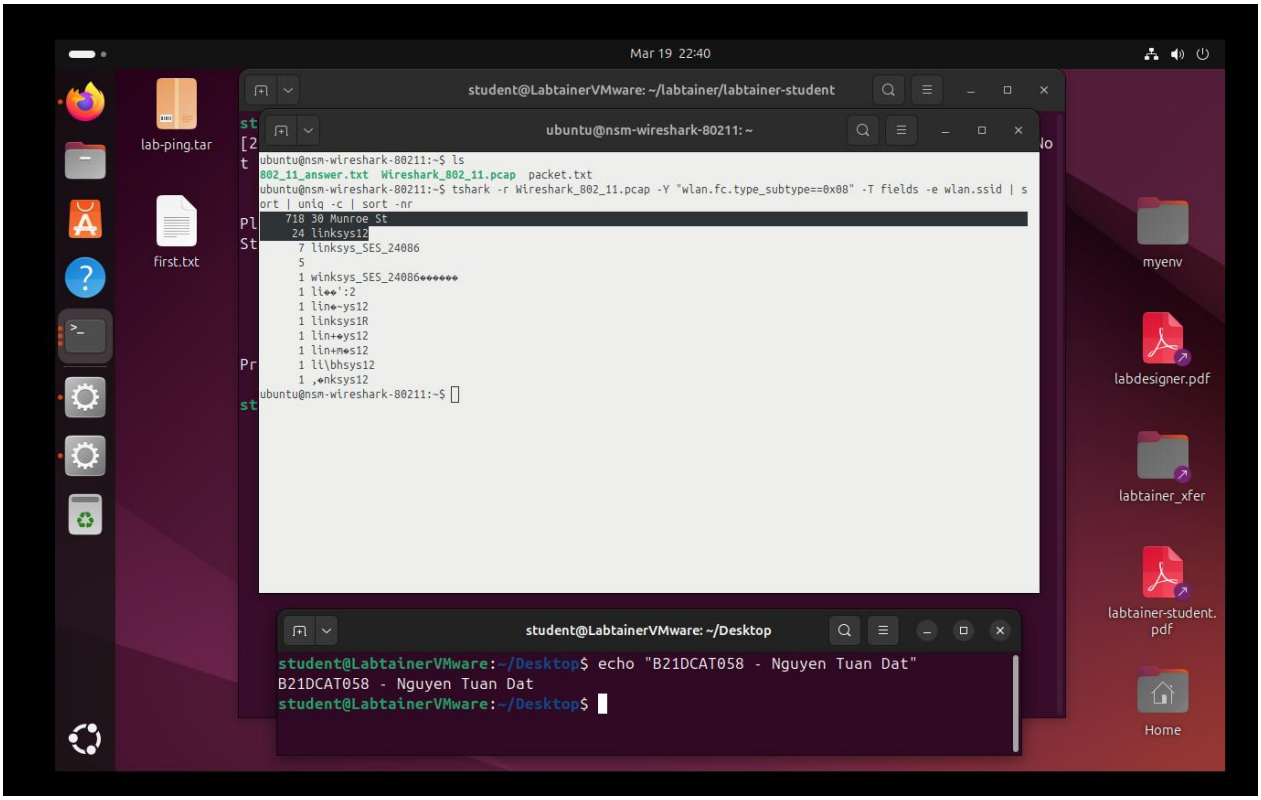
Task 1 : Export thông tin gói tin đầu tiên và in ra terminal thông tin gói tin đó ?



Task 2 : SSID của 2 điểm truy cập phát ra nhiều khung beacon nhất trong bản ghi này là gì: :

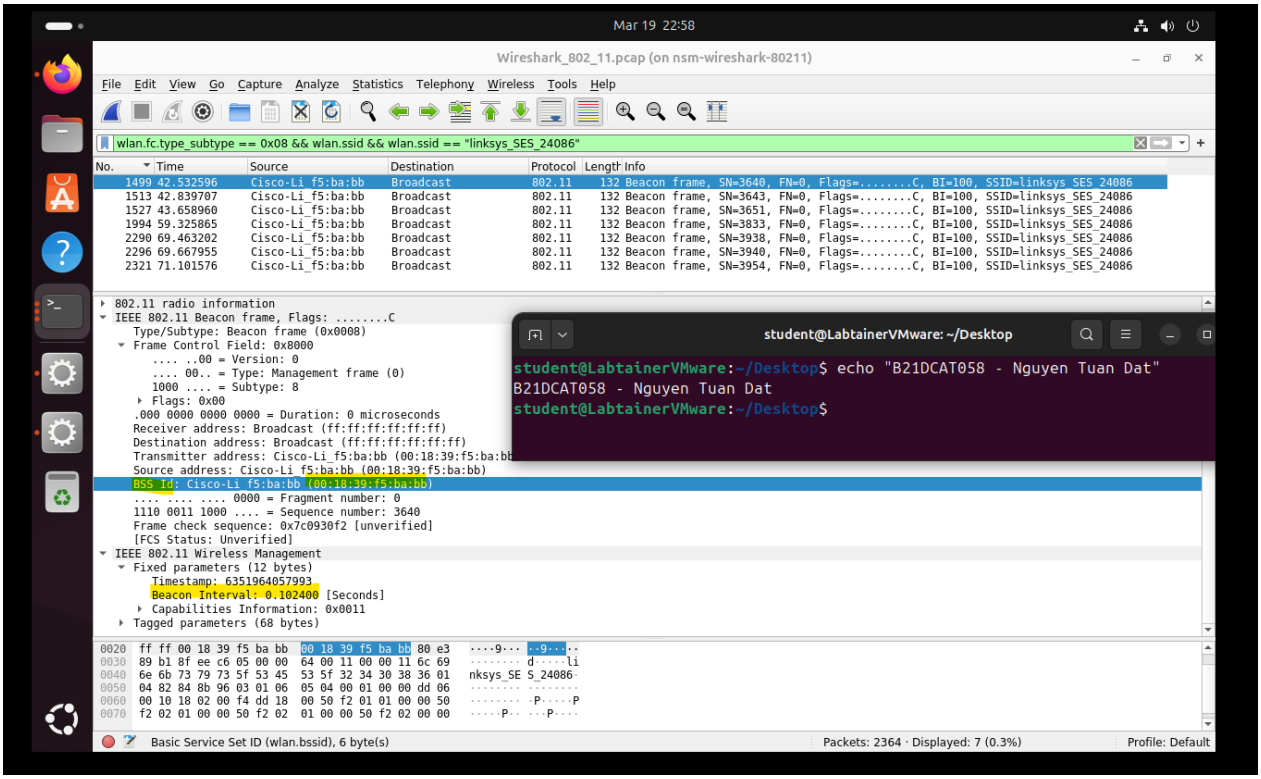
➔ **linksys12 và 30 Munroe St**

tshark -r your_capture_file.pcapng -Y "wlan.fc.type_subtype==0x08" -T fields -e wlan.ssid | sort | uniq -c | sort -nr



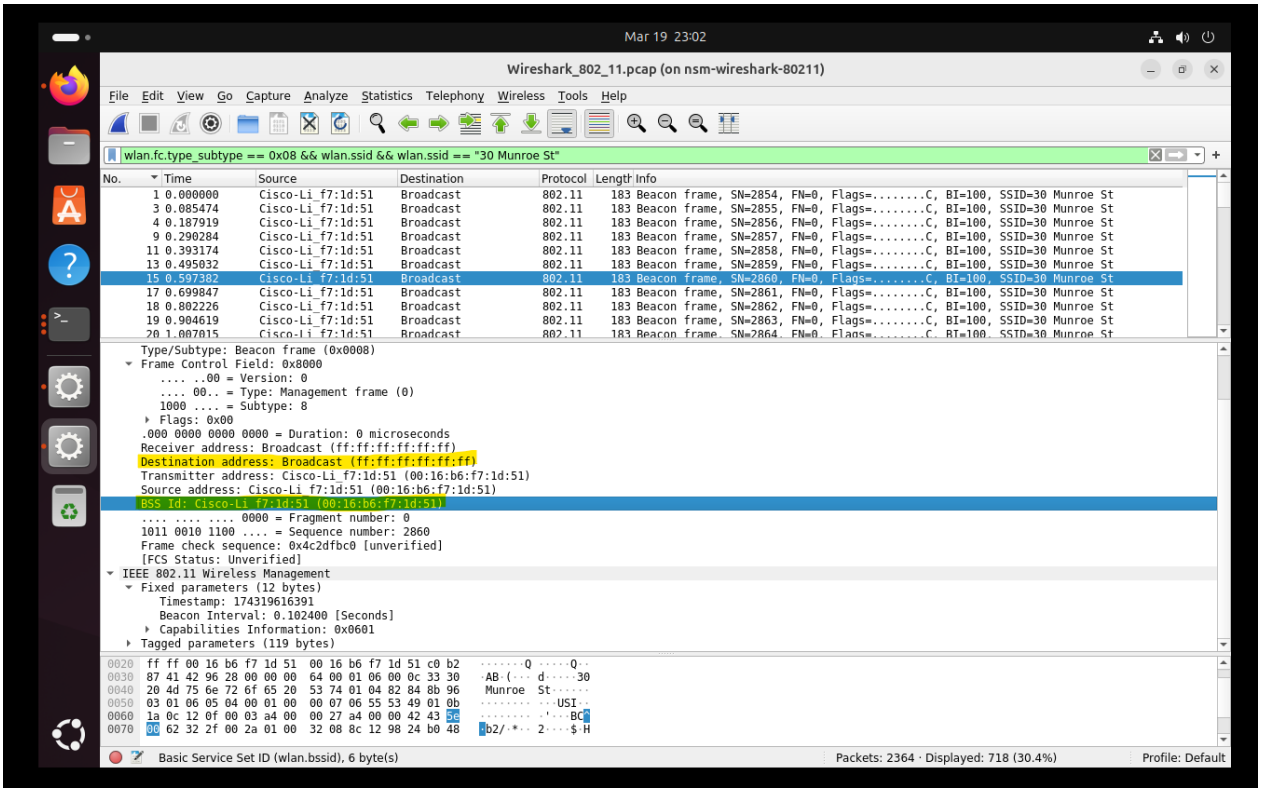
Task 3 : Khoảng thời gian giữa các khung beacon của điểm truy cập linksys_ses_24086 là bao nhiêu ?

➔ **time = 0.102400 and MAC_BSS = 00:18:39:f5:ba:bb**

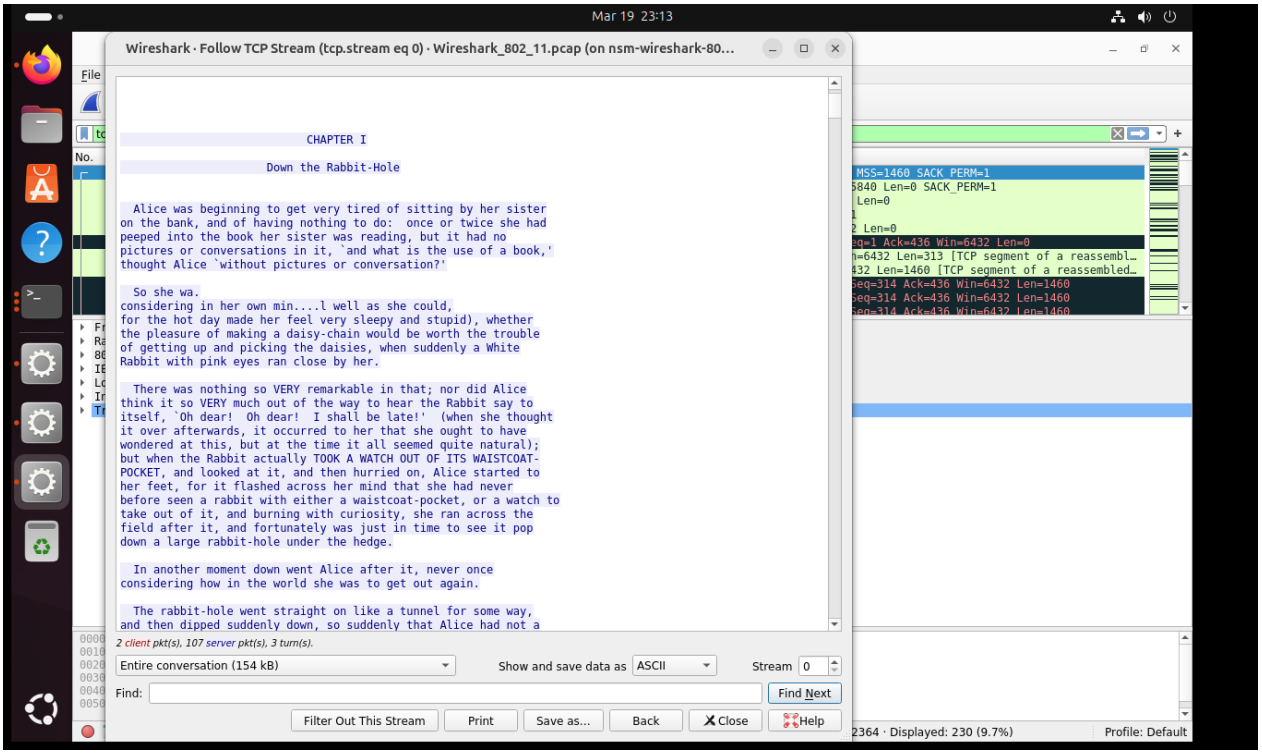


Task 4 : Địa chỉ MAC nguồn trong khung beacon từ 30 Munroe St là gì ? Địa chỉ MAC đích trong khung ?

➔ **MAC_source = 00:16:b6:f7:1d:51 and MAC_destination = ff:ff:ff:ff:ff:ff**



*Tìm khung 802.11 chứa phân đoạn SYN của TCP cho phiên TCP đầu tiên(tải xuống tệp alice.txt)



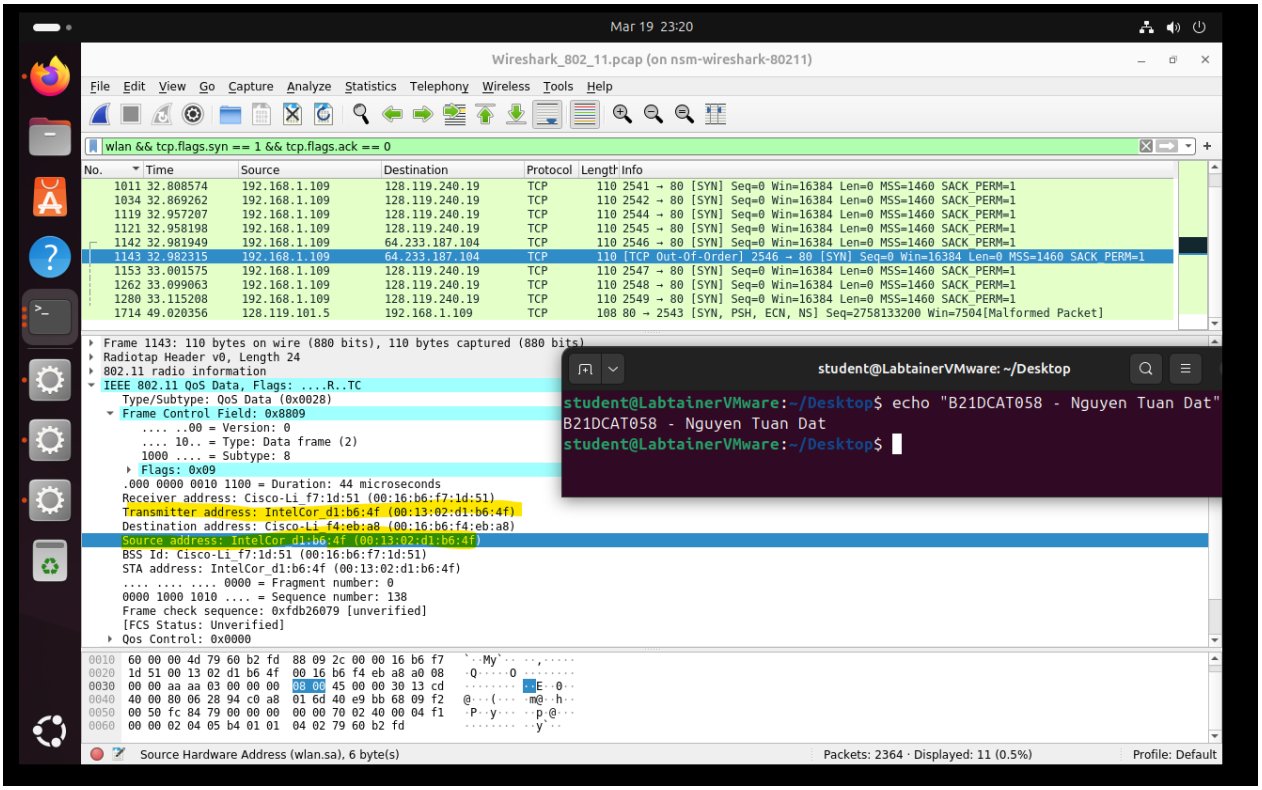
Task 5 : Địa chỉ nào trong khung này tương ứng với máy trạm không dây và tìm ra địa chỉ MAC của đích ?

➔ **Transmitter address and MAC_address = 00:13:02:d1:b6:4f**

Lọc các gói tin 802.11 và lọc các gói TCP có cờ SYN được đặt (bắt đầu phiên TCP) và không có cờ ACK (để đảm bảo đây là gói SYN đầu tiên, không phải SYN/ACK).

wlan && tcp.flags.syn == 1 && tcp.flags.ack == 0

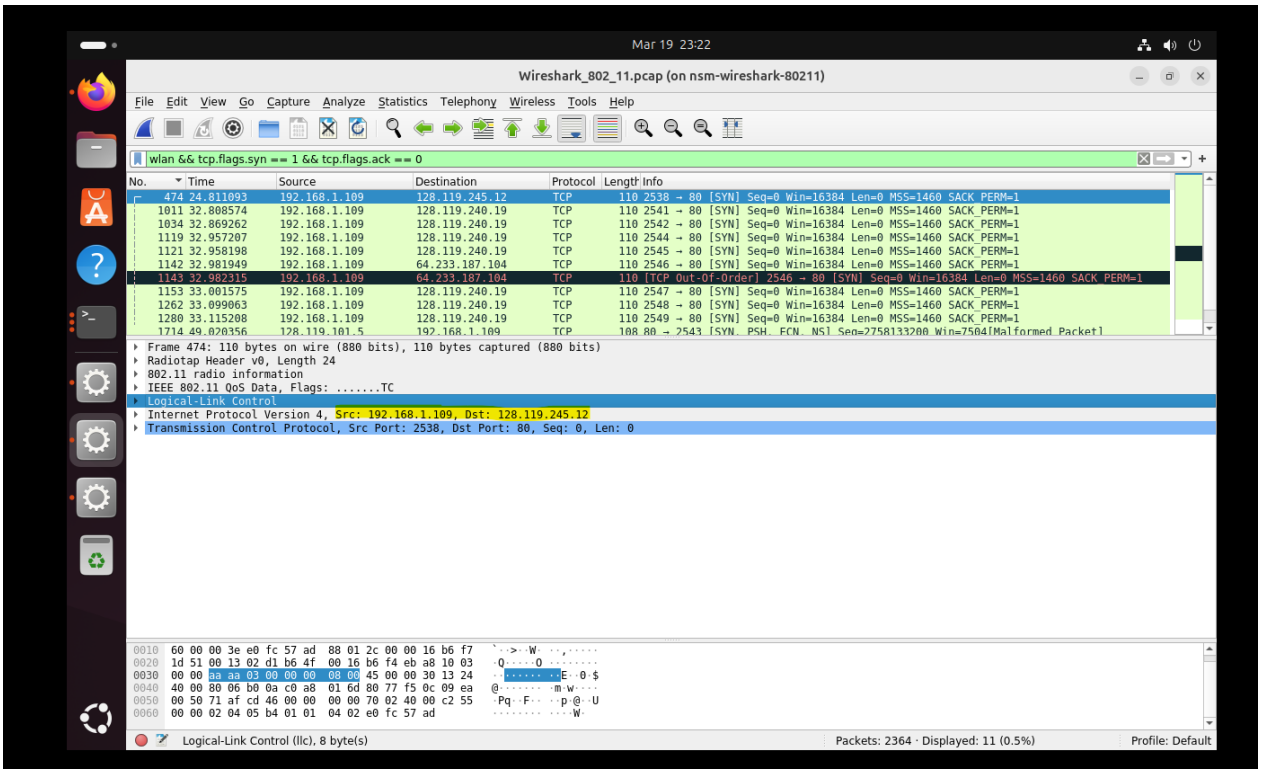
Sau khi lọc, chọn 1 gói tin bất kì, Chọn IEEE 802.11 Qos Data . Chọn Frame control Field để xem kĩ hơn.



Task 6 : Địa chỉ IP của máy trạm không dây gửi phân đoạn TCP này là gì ? Địa chỉ IP đích là gì ?

➔ **Source address = 192.168.1.109 and destination address = 128.119.245.12**

Trong gói tin ta chọn ở task 5, ta thấy Internet Protocol Vesion 4 hiện thị địa chỉ IP của máy trạm không dây gửi phân đoạn TCP và Địa chỉ IP đích

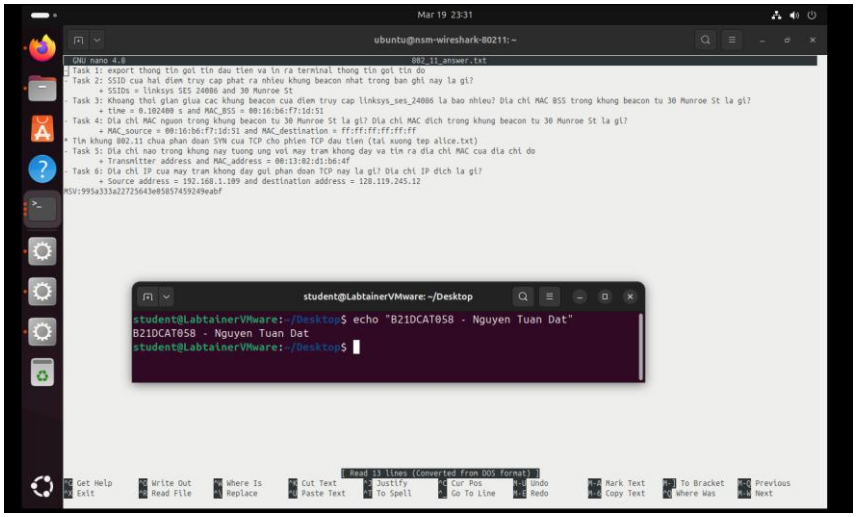


4. Kết thúc bài lab:

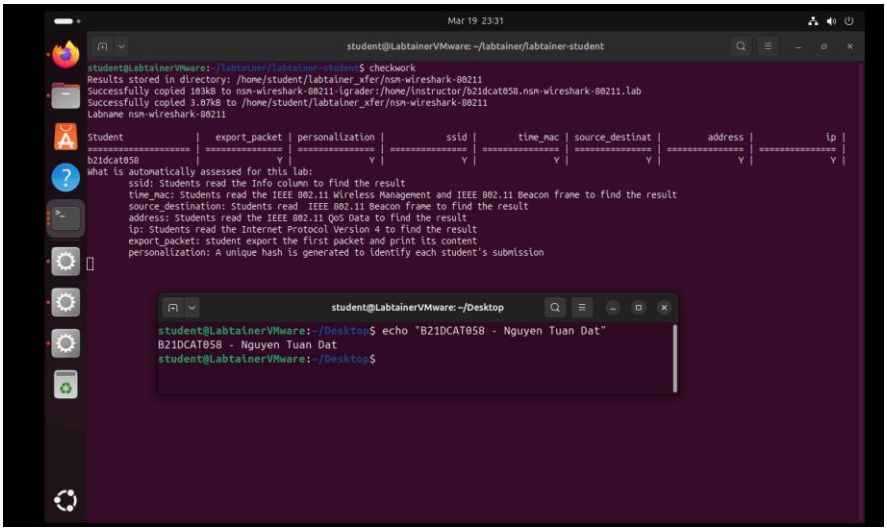
Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab nsm-wireshark-80211

File 802_11_answer.txt :



Thực hiện checkwork bài nsm-wireshark-80211 :



Hình 9 : Checkwork

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-80211