

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



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: KỸ 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

1. Mục đích.....	3
2. Yêu cầu đối với sinh viên	3
3. Nội dung thực hành.....	3
4. Kết thúc bài lab:	12

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

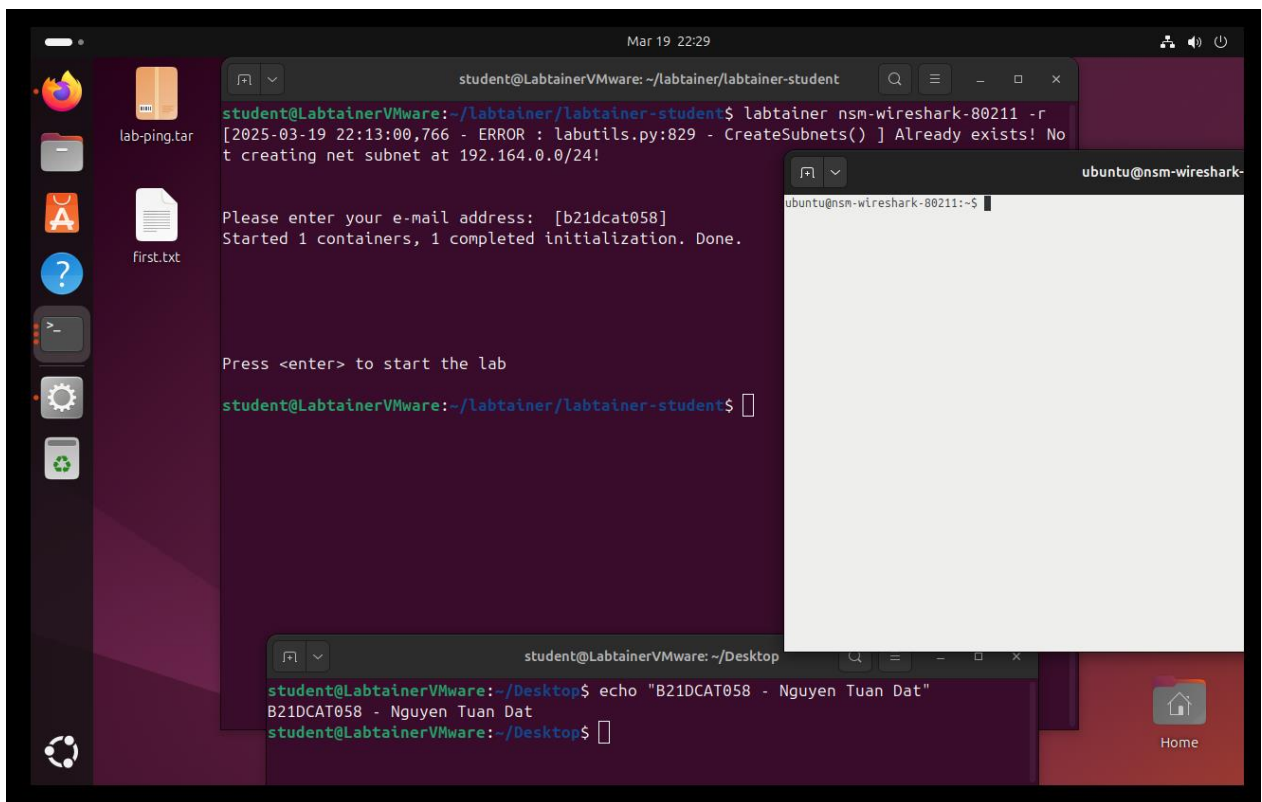
Có kiến thức cơ bản về hệ điều hành Linux, công cụ wireshark và chuẩn IEEE 802.11

3. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

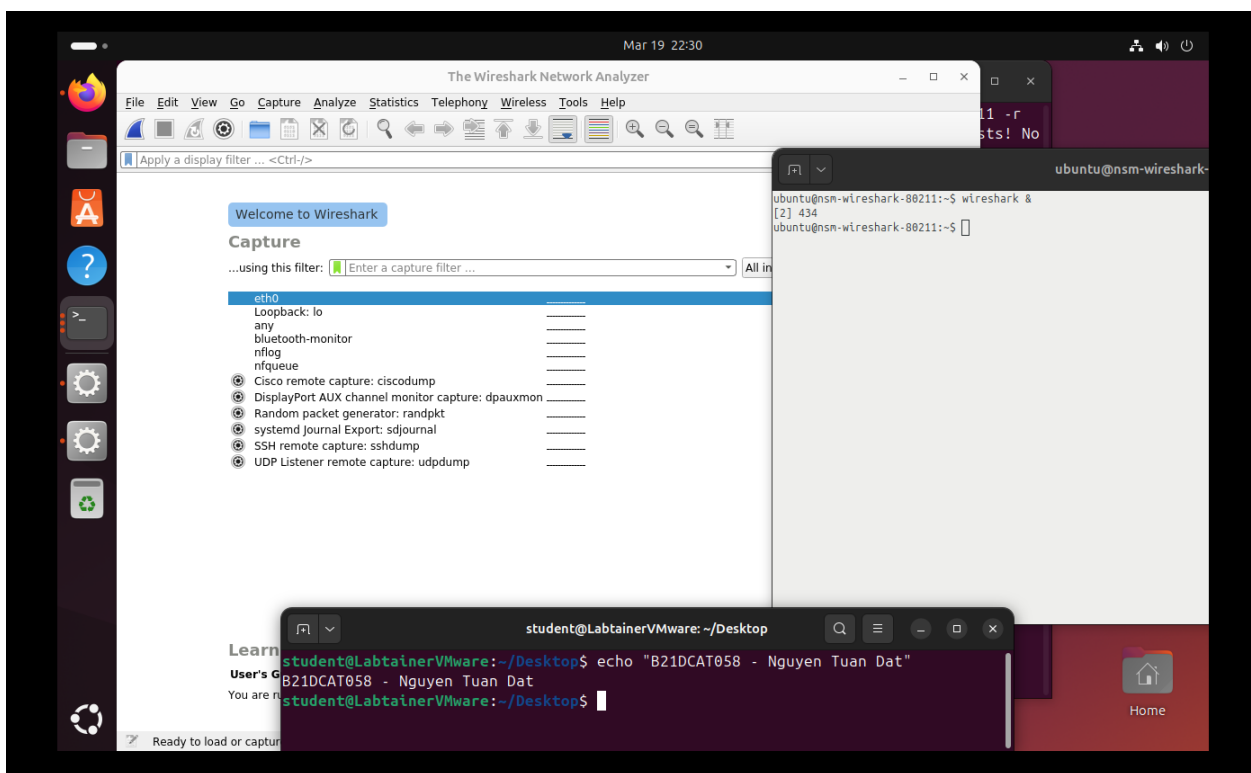
labtainer nsm-wireshark-80211



(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)

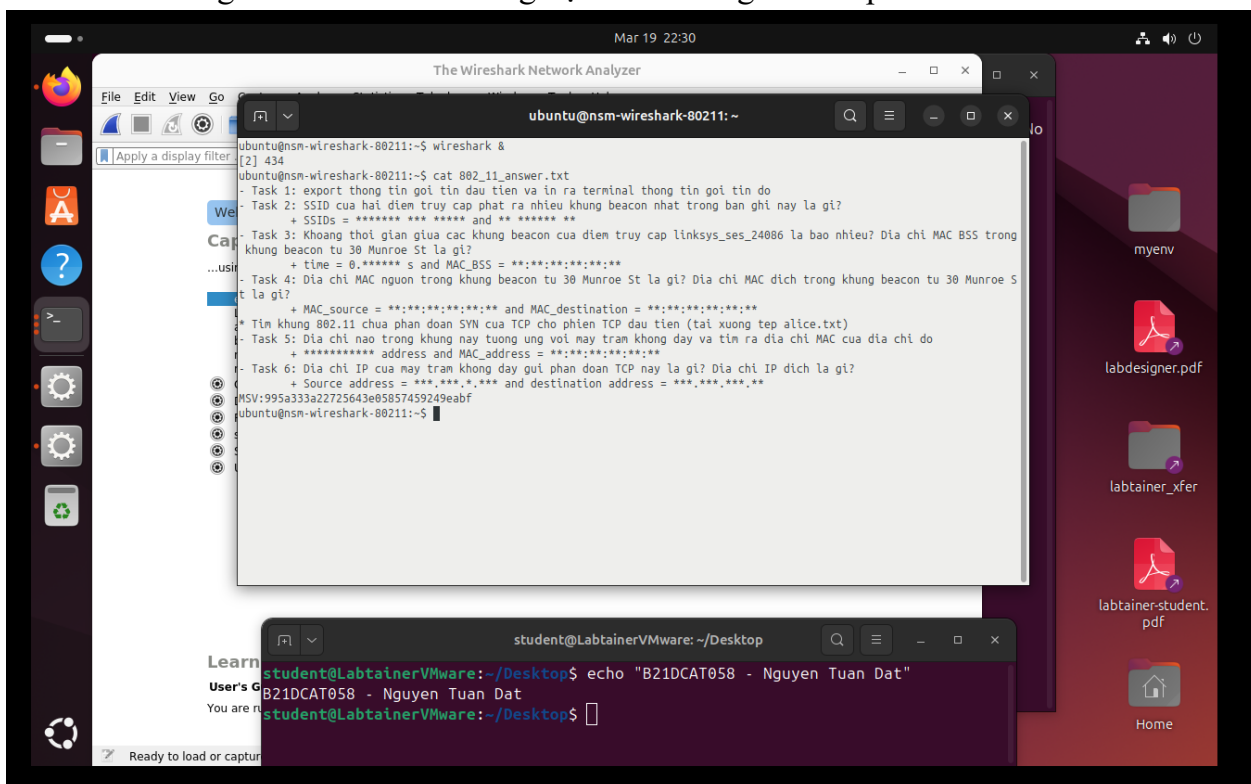
Sau khi khởi động xong một terminal ảo sẽ xuất hiện đại diện cho máy khởi chạy wireshark: nsm-wireshark-80211 và điền kết quả sau khi phân tích các gói tin .Trên terminal khởi chạy wireshark bằng câu lệnh:

Wireshark



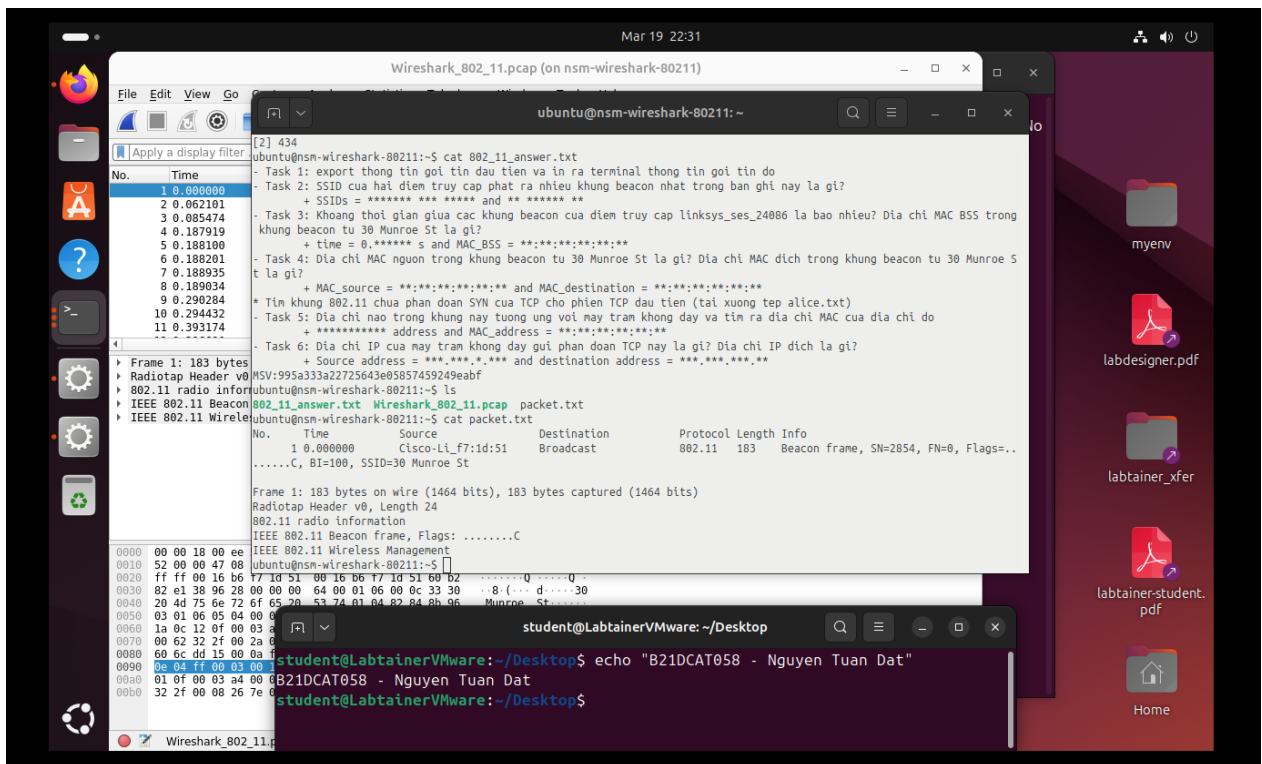
Trên máy nsm-wireshark-80211 mở file 802-11-answer chứa câu hỏi và form điền kết quả

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

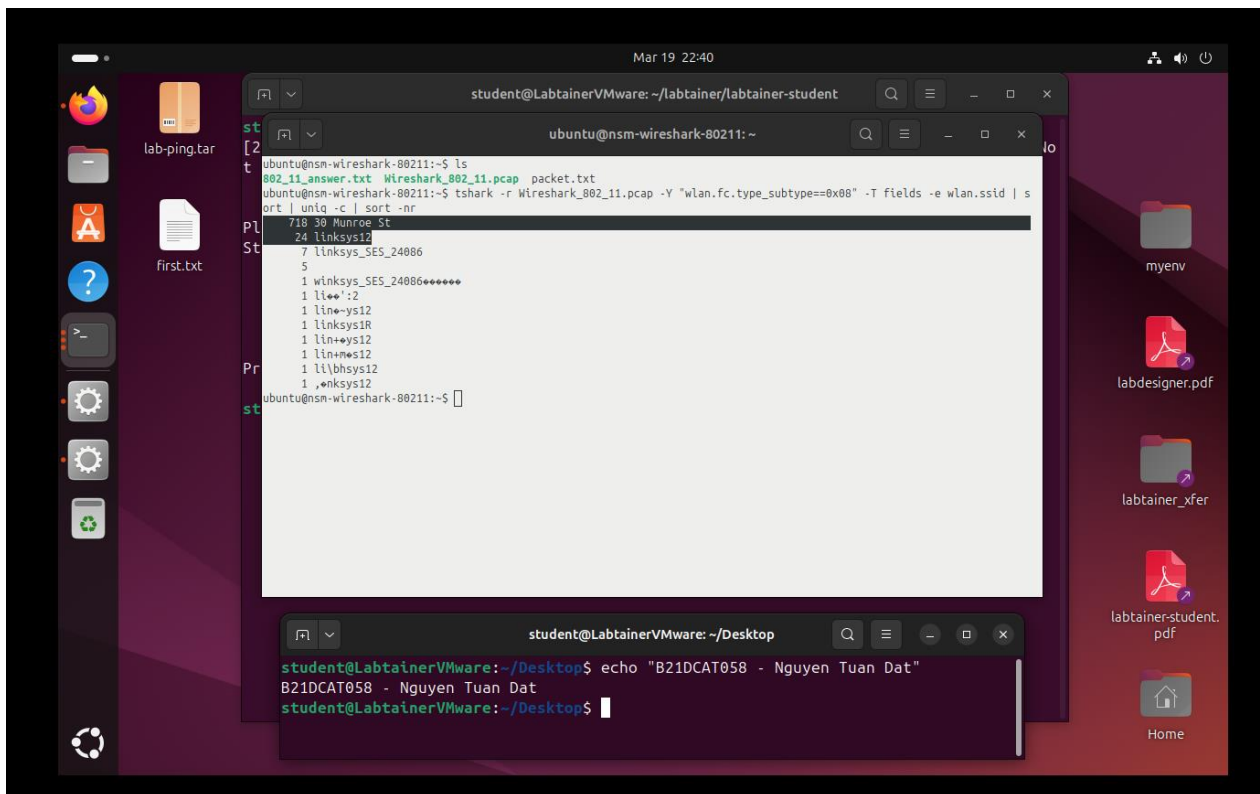
Task 1 : Export thông tin gói tin đầu tiên và in ra terminal thông tin gói tin đó ?



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**

Wireshark 802_11.pcap (on nsm-wireshark-80211)

Filter: wlan.fc.type_subtype == 0x08 && wlan.ssid && wlan.ssid == "linksys_SES_24086"

No.	Time	Source	Destination	Protocol	Length	Info
1499	42.532596	Cisco-Li f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1513	42.839787	Cisco-Li f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3643, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1527	43.658960	Cisco-Li f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3651, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1994	59.325865	Cisco-Li f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3833, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2290	69.463202	Cisco-Li f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3938, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2296	69.667955	Cisco-Li f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3940, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2321	71.101576	Cisco-Li f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3954, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086

802.11 radio information

- IEEE 802.11 Beacon frame, Flags:C
 - Type/Subtype: Beacon frame (0x0008)
 - Frame Control Field: 0x0000
 -00.. = Version: 0
 -00.. = Type: Management frame (0)
 - 1000..... = Subtype: 8
 - Flags: 0x00
 -0000 0000 0000 = Duration: 0 microseconds
 - Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Transmitter address: Cisco-Li f5:ba:bb (00:18:39:f5:ba:bb)
 - Source address: Cisco-Li f5:ba:bb (00:18:39:f5:ba:bb)
 - BSSID: Cisco-Li f5:ba:bb (00:18:39:f5:ba:bb)
 -0000 = Fragment number: 0
 - 1110 0011 1000..... = Sequence number: 3640
 - Frame check sequence: 0x7c930f2 [unverified]
 - [FCS Status: Unverified]
- IEEE 802.11 Wireless Management
 - Fixed parameters (12 bytes)
 - Timestamp: 6351964057993
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x0011
 - Tagged parameters (68 bytes)

Basic Service Set ID (wlan.bssid), 6 byte(s)

Packets: 2364 - Displayed: 7 (0.3%)

Profile: Default

```
student@LabtainerVMware:~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058 - Nguyen Tuan Dat"
B21DCAT058 - Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$
```

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

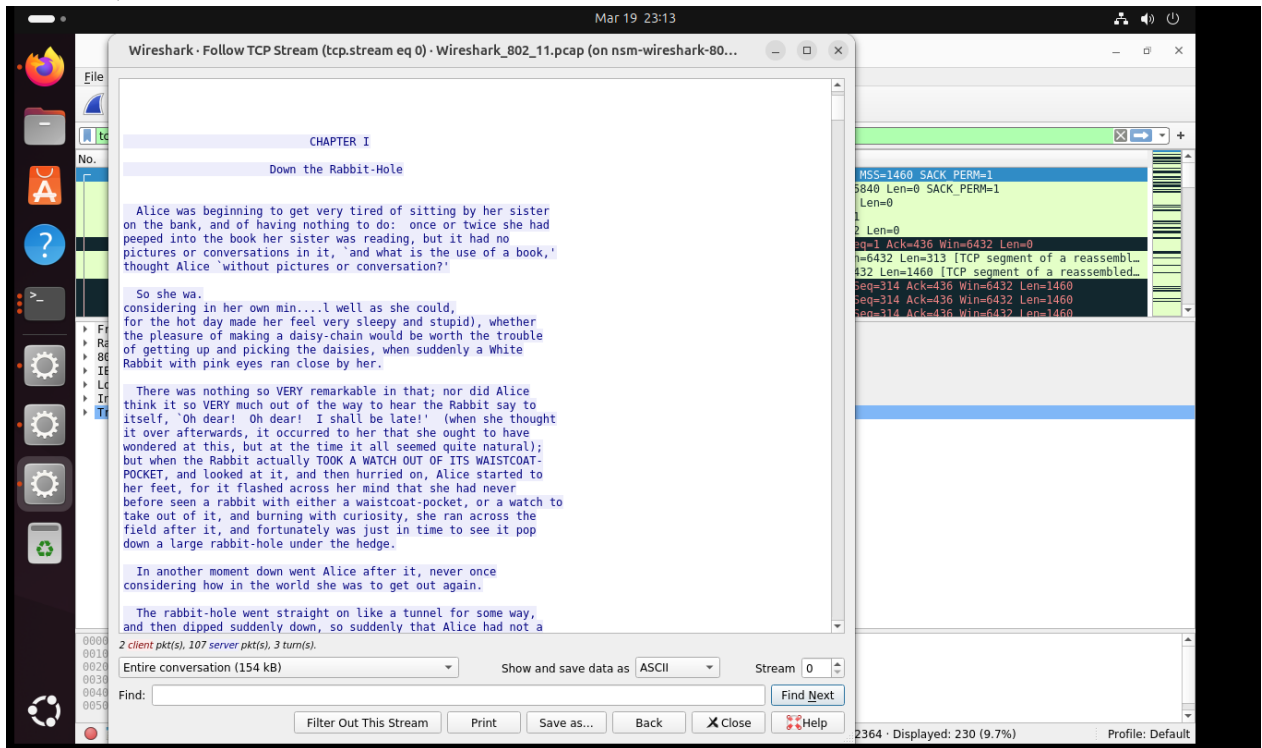
➔ **MAC_source = 00:16:b6:f7:1d:51 and MAC_destination = ff:ff:ff:ff:ff:ff**

The image shows a Wireshark capture of IEEE 802.11 Beacon frames. The filter applied is `wlan.fc.type_subtype == 0x08 && wlan.ssid && wlan.ssid == "30 Munroe St"`. The packet list shows several beacon frames from source `Cisco-Li f7:1d:51` to destination `Broadcast`. The selected packet (No. 15) is expanded to show details:

- Type/Subtype: Beacon frame (0x0008)
- Frame Control Field: 0x0000
 -00 = Version: 0
 -00.. = Type: Management frame (0)
 - 1000.... = Subtype: 8
 - Flags: 0x00
 - .000 0000 0000 0000 = Duration: 0 microseconds
- Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
- Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
- Transmitter address: Cisco-Li f7:1d:51 (00:16:b6:f7:1d:51)
- Source address: Cisco-Li f7:1d:51 (00:16:b6:f7:1d:51)
- BSS id: Cisco-Li f7:1d:51 (00:16:b6:f7:1d:51)
-0000 = Fragment number: 0
- 1011 0010 1100 = Sequence number: 2860
- Frame check sequence: 0x4c2dfbc0 [unverified]
- [FCS Status: Unverified]
- IEEE 802.11 Wireless Management
 - Fixed parameters (12 bytes)
 - Timestamp: 174319616391
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x0601
 - Tagged parameters (119 bytes)

The packet bytes pane shows the raw data, including the MAC addresses `ff ff 00 16 b6 f7 1d 51` and `00 16 b6 f7 1d 51 c0 b2`.

*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

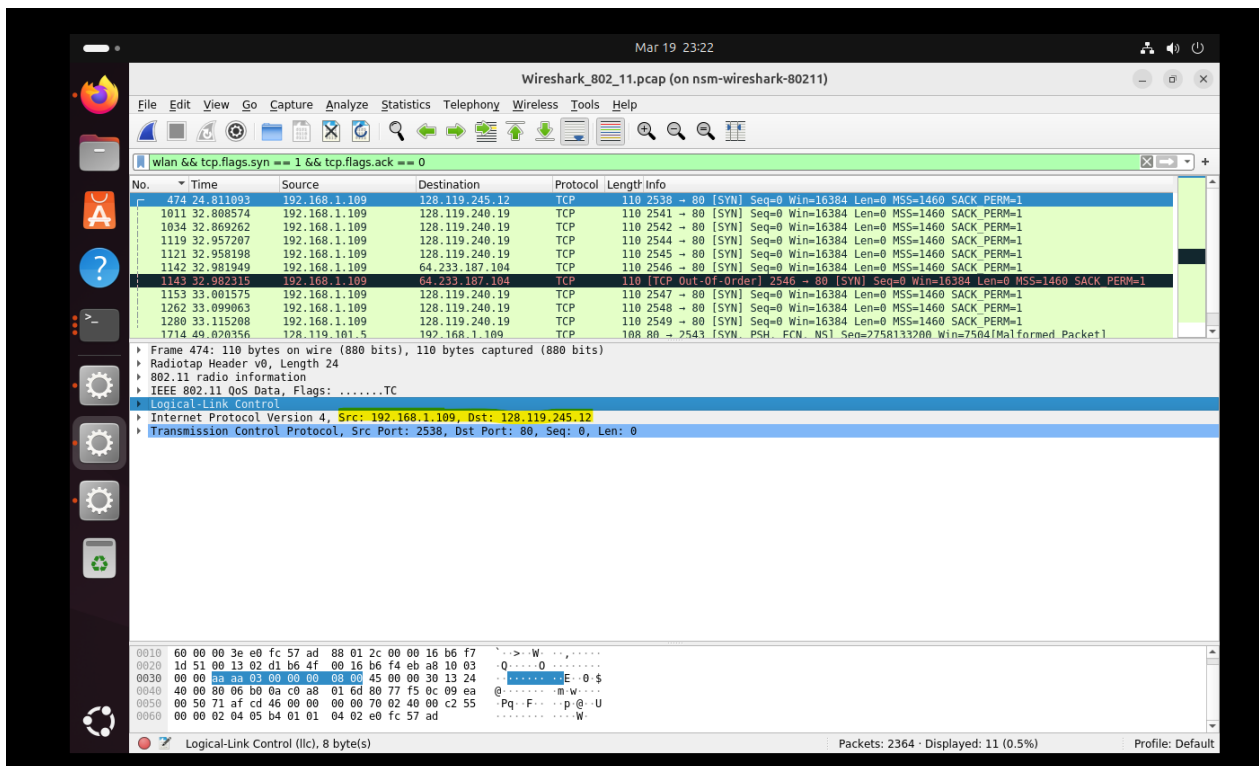
Sau khi lọc, chọn 1 gói tin bất kì, Chọn IEEE 802.11 QoS Data . Chọn Frame control Field để xem kĩ hơn.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The filter bar at the top shows the applied filter: `wlan && tcp.flags.syn == 1 && tcp.flags.ack == 0`. The packet list pane shows several captured packets, with packet 1143 selected. The packet details pane for packet 1143 shows the IEEE 802.11 QoS Data structure, with the Frame Control field expanded to show details like Duration, Receiver address, Transmitter address (00:13:02:d1:b6:4f), Destination address, BSS Id, STA address, Fragment number, Frame check sequence, and QoS Control. A terminal window in the foreground shows the command `echo "B21DCAT058 - Nguyen Tuan Dat"` being executed.

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 Version 4 hiển thị địa chỉ IP của máy trạm không dây gửi phân đoạn TCP và Địa chỉ IP đích

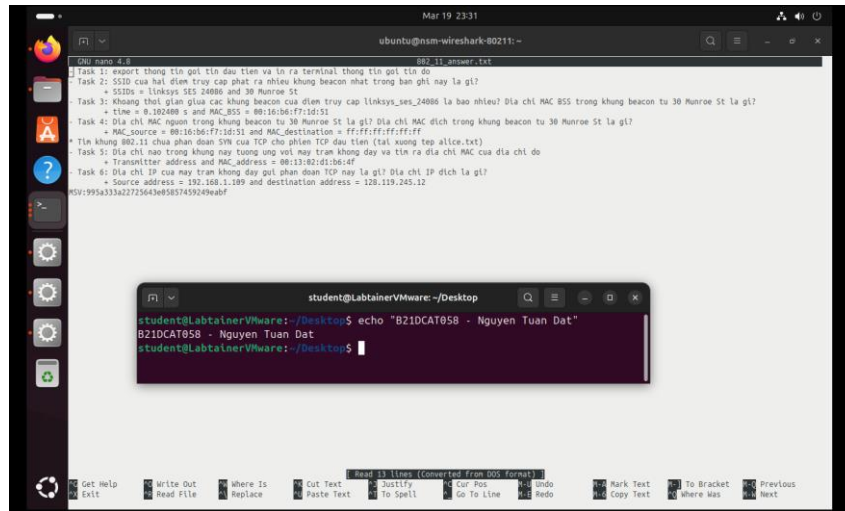


4. Kết thúc bài lab:

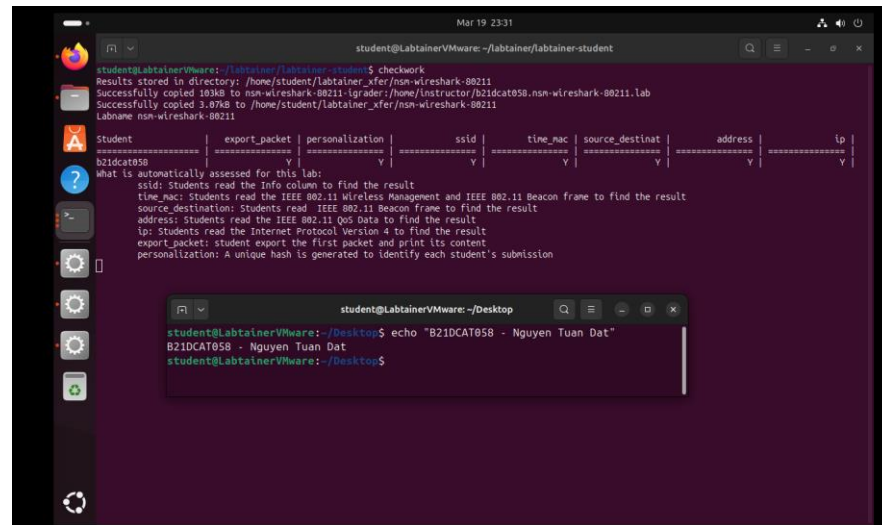
Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

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