**Nội dung và hướng dẫn bài thực hành**

**Mục đích**

Giúp sinh viên tiếp cận với một số cách tìm kiếm thông tin và phát hiện ra dấu hiệu của chúng bằng wireshark.

**Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về Wireshark

**Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

*labtainer nsec\_wifi\_machunt*

*(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 student ảo sẽ xuất hiện.

* **Task 1: Exporting:**

Khởi động bài lab, học viên sẽ được cung cấp sẵn file *truylung.pcap*.

Sử dụng câu lệnh *wireshark* để mở phần mềm wireshark.

Chọn File -> Open -> truylung.pcap.

Biết trước thông tin đối tượng bị truy lùng đã có hoạt động ở một quán cà phê 9 tầng mây (SSID: 9\_tang\_may\_cafe) → sử dụng câu lệnh để lọc

*wlan contains <ssid>*

Mở rộng phần thông tin thuộc phần IEEE 802.11 → tìm transmitter address và ghi lại thông tin địa chỉ MAC.

Chọn File → Export specified packets → đặt tên là exported → tích vào ô Selected packets only → Save.

* **Task 2:** **Đối chiếu địa chỉ MAC** Với thông tin về địa chỉ MAC đã tìm thấy ở trên, kết hợp với file target-list.

Sử dụng câu lệnh *nano target-list* để mở danh sách và đối chiếu.

Ghi nhận lại tên của người dùng có địa chỉ MAC trùng với địa chỉ đã tìm được trước đó.

Sử dụng câu lệnh *gcc print.c -o target-name*để tạo file ghi kết quả*.*

Sử dụng câu lệnh ./target-name và nhập tên người sở hữu địa chỉ MAC đã đối chiếu.

**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.