PHỤ LỤC 1

**LÀM QUEN VỚI CÔNG CỤ WIRESHAKR**

**Mục tiêu:**

Cung cấp cho sinh viên các kỹ năng cơ bản sử dụng phần mềm Wireshark, bao gồm:

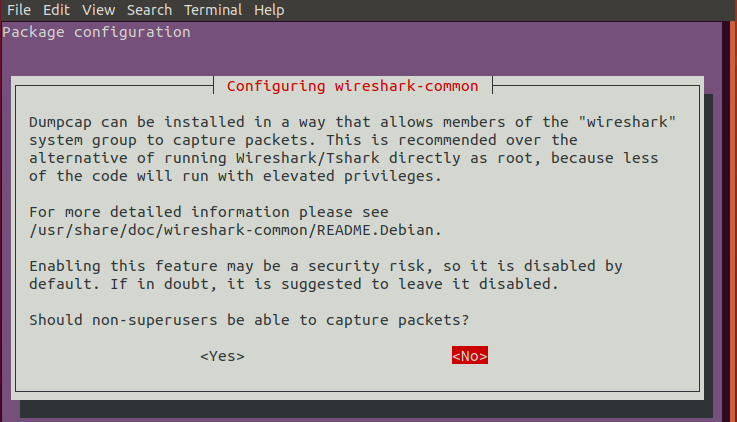
* Cài đặt công cụ trên hệ điều hành Ubuntu 18.04
* Sử dụng Wireshark để bắt các gói tin trên máy trạm
* Quan sát cách thức dữ liệu được đóng gói theo chồng giao thức TCP/IP

**Nội dung**

**1. Cài đặt Wireshark trên hệ điều hành Ubuntu 18.04**

Wireshark là một công cụ kiểm tra, theo dõi và phân tích dữ liệu trao đổi giữa máy tính cài đặt công cụ này với các máy tính khác trong mạng. Sau đây, chúng ta sẽ cài đặt Wireshark trên hệ điều hành Ubuntu 18.04

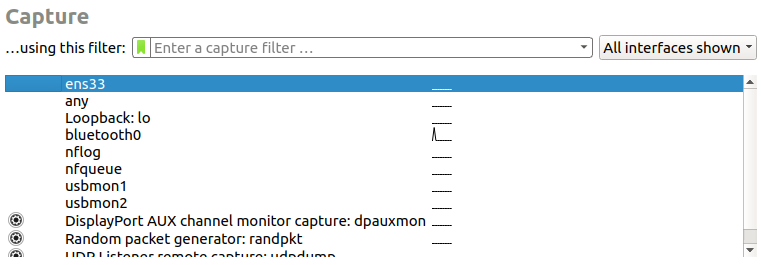
Mở cửa sổ Terminal và thực hiện lệnh **sudo apt-get install wireshark -y** để cài đặt Wireshark. Trong quá trình cài đặt, chọn No khi gặp thông báo sau:



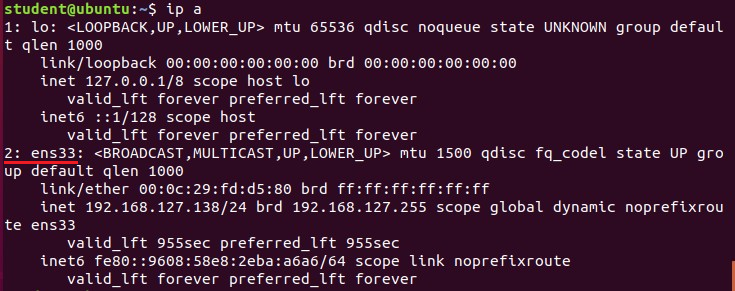
**2. Giới thiệu giao diện làm việc của Wireshark**

- Bước 1: Trên cửa sổ Terminal gõ lệnh **sudo wireshark** để khởi động phần mềm. Bỏ qua các cảnh báo nếu có.

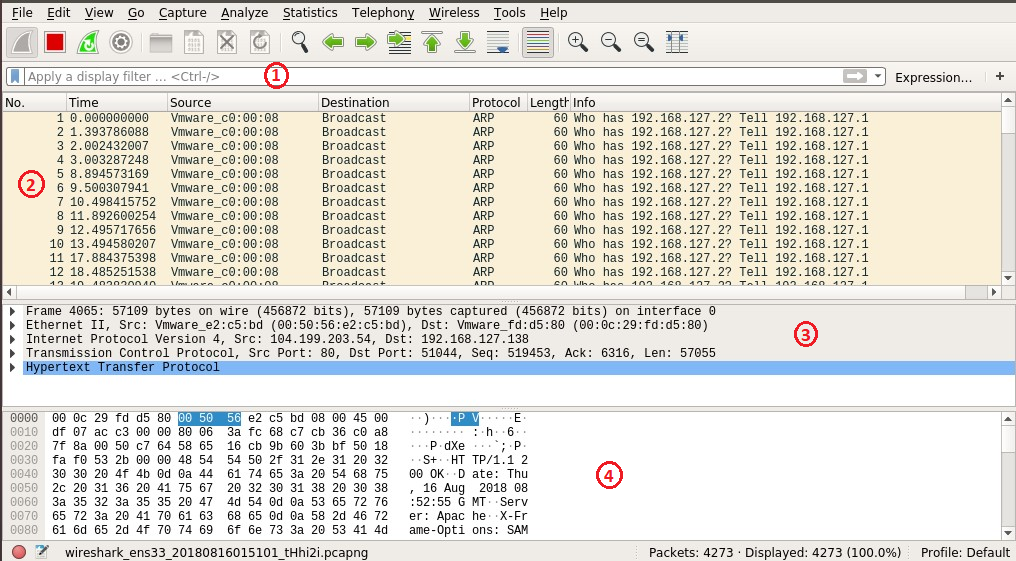
- Bước 2: Sau khi Wireshark khởi động thành công, các bạn nhìn thấy danh sách các cổng giao tiếp khác nhau trên máy tính mà Wireshark có thể bắt các gói tin trên đó.



*Lưu ý: Để biết các cổng mạng của máy tính, trên cửa sổ Terminal gõ lệnh* **ip a.** Như kết quả hiển thị dưới đây, ta có thể thấy tên cổng mạng của máy tính là ens33



- Bước 3: Nhấp đúp vào cổng mạng, chúng ta sẽ thấy giao diện làm việc của Wireshark như sau:



* Thanh công cụ : Xem mục **Help** của phần mềm để biết thêm chi tiết
* Vùng 1 : Tạo bộ lọc cho phép quan sát các gói tin thỏa mãn yêu cầu nào đó
* Vùng 2 : Danh sách các gói tin đã bắt.
* ***No.*** : Số thứ tự gói tin
* ***Time*** : thời điểm bắt (tính bằng giây kể từ khi bắt đầu)
* ***Source*** : Địa chỉ nguồn của gói tin
* ***Destination*** : Địa chỉ đích của gói tin
* ***Protocol*** : Giao thức.
* ***Length*** : Kích thước
* ***Info*** : các thông tin chính về gói tin (thường lấy từ header của gói tin)
* Vùng 3 : Các nội dung phân tích được ở tất cả các tầng trong mô hình TCP/IP.
* Vùng 4 : Nội dung thực tế của gói tin

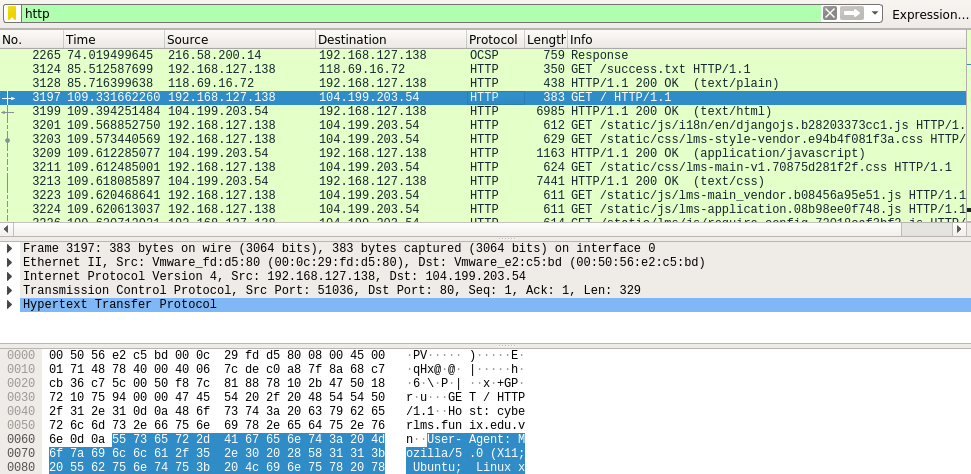
- Bước 4: Mở trình duyệt và truy cập vào trang http://cyberlms.funix.edu.vn

- Bước 5: Ngừng bắt gói tin bằng cách nhấp vào biểu tượng  trên thanh công cụ. Chúng ta có thể lưu dữ liệu bắt được trên files có định dạng **.pcapng**

**3. Quan sát gói tin trên Wireshark**

Trong phần này, chúng ta sẽ thử quan sát một gói tin mà Wireshark bắt được. Chúng ta sẽ có các bài thực hành sau để phân tích nội dung cụ thể của các loại gói tin khác nhau.

- Bước 1: Nhập vào bộ lọc xâu **http** chúng ta sẽ thấy trên cửa sổ chỉ hiển thị các gói tin có Protocol là HTTP tương tự như dưới đây.Có thể bỏ qua các gói tin với tên giao thức khác được xây dựng dựa trên HTTP như OCSP



- Bước 2: Lựa chọn một gói tin có thông số như sau để quan sát:

Destination: 104.199.203.54

Info: GET / HTTP/1.1

- Bước 3: Chúng ta sẽ thấy cấu trúc gói tin được hiển thị trên vùng 3, còn nội dung gói tin dưới dạng hexa và mã ASCII được hiển thị trên vùng 4. Quan sát ở vùng 3, chúng ta sẽ thấy gói tin này có các tiêu đề đóng gói theo chồng giao thức TCP/IP như sau:

* Tầng liên kết dữ liệu: Ethernet
* Tầng mạng: Internet Protocol version 4 (IPv4)
* Tầng giao vận: Tranmission Control Protocol (TCP)
* Tầng ứng dụng: Hypertext Transfer Protocol (HTTP)

**Kết luận**

Với nội dung mà các bạn vừa thực hiện, các bạn đã làm quen được với cách thức cài đặt công cụ Wireshark và sử dụng dụng nó để bắt các gói tin trên máy tính.