Họ và tên: Nguyễn Bá Hùng

Lớp: 10ĐH\_CNPM

MSSV: 1050080264

**LAB 1: LÀM QUEN VỚI WIRESHARK**



# **1.** Task 1: Mở đầu về Mạng máy tí**nh**

 Trước khi bắt đầu thực hành, sinh viên hãy trả lời các câu hỏi sau:

* Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).
* Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?
* Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

# **2.** Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng

2.1 Giới thiệu và làm quen với Wireshark

Wireshark là phần mềm bắt gói tin (packet sniffer) rất phổ biến và miễn phí chạy trên Windows, Linux, MacOS, hỗ trợ bắt gói tin và quan sát nội dung của các thông điệp được trao đổi bởi các giao thức tại các tầng mạng khác nhau.

Ngoài ra, Wireshark còn phục vụ cho việc điều tra các chứng cứ số (forensic) liên quan đến các vụ án về mạng máy tính.

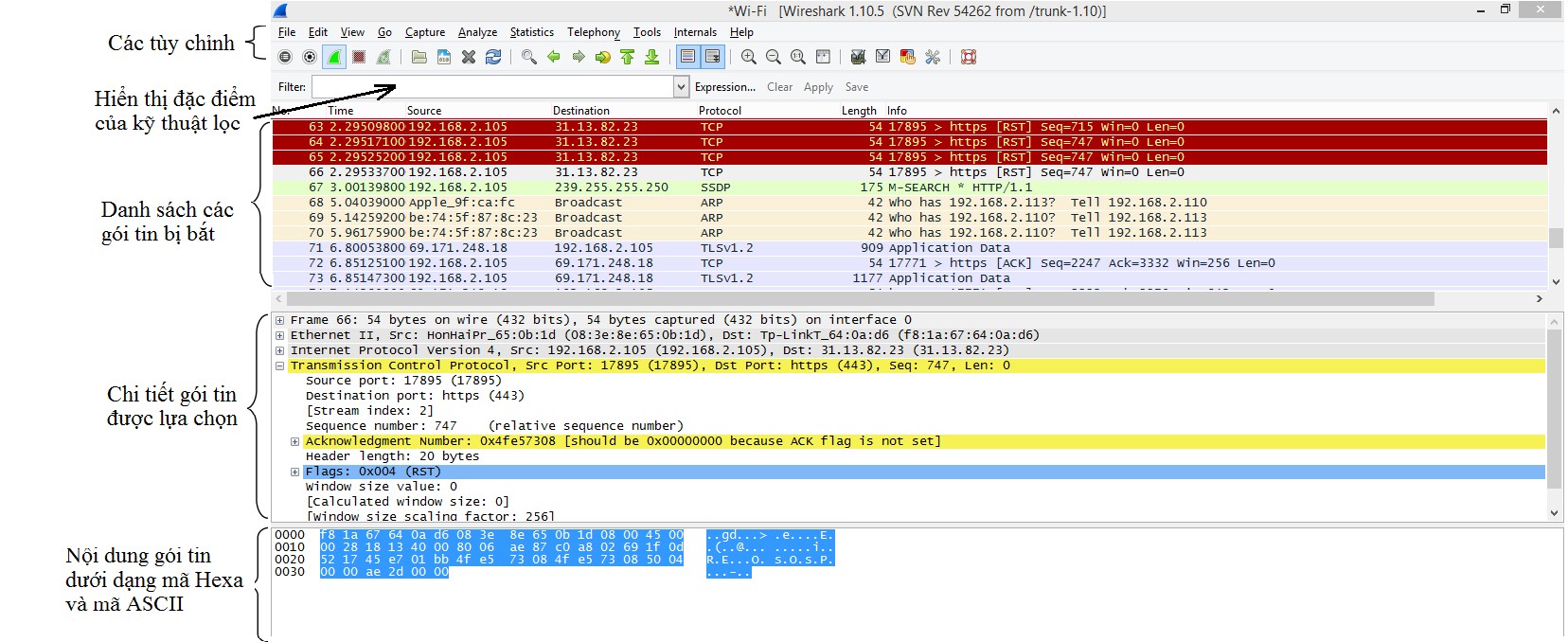
Giao diện chính khi mở Wireshark sẽ giống Hình 1.

Tại cửa sổ đầu tiên, bạn sẽ thấy danh sách các card mạng (hay network interface) trong mục Capture. Quan sát bên phải tên interface sẽ có minh họa thể hiện cho hoạt động trao đổi dữ liệu trong mạng, khi có dấu hiệu như thì có thể nhận định đang có dữ liệu trao đổi qua interface đó.

Tùy theo loại kết nối và hệ điều hành đang sử dụng, tên của các interface sẽ khác nhau. Ví dụ, tên các interface thông thường trên Windows như sau:

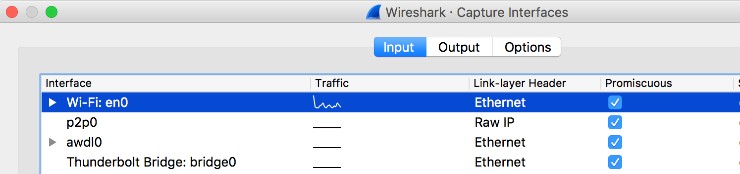
* Kết nối có dây: Ethernet, Local Area Connection (LAN).
* Kết nối không dây: WiFi.

Sau đó, giao diện bắt gói tin sẽ xuất hiện như sau.



Hình 2.Giao diện chính của Wireshark trong suốt quá trình bắt và phân tích gói tin

Lưu ý: Để có thể bắt được các gói tin đi qua nó, card mạng cần được kích hoạt chế độ Promiscuous (mặc định sẽ được kích hoạt sẵn trong Wireshark)



Hình 3.Có thể vào Capture > Options để theo dõi cài đặt trên từng interface

Giao diện Wireshark gồm có 5 thành phần chính từ trên xuống:

1. Command menus: chứa các menu thực hiện các chứng năng chính của Wireshark. Chúng ta quan tâm chủ yếu đến File và Capture.

 o File menu chứa các tùy chọn cho phép lưu các gói tin đã bắt được (Save) dưới dạng file .pcapng hoặc mở file chứa các gói tin đã bắt từ trước. o Capture menu cho phép bắt đầu bắt gói tin và thay đổi các tùy chỉnh o Các button thườn dùng:

* + - * - Bắt đầu bắt gói tin trên card mạng đã chọn.  - Dừng quá trình bắt gói tin



* + - * - Khởi động lại quá trình bắt gói tin hiện tại
      * - Mở Capture Options để thay đổi các tùy chỉnh

1. Packet-display filter: Tên giao thức và các thông tin khác có thể được nhập vào đây để lọc các gói tin trong packet-listing window.

Ví dụ, để lọc các gói tin HTTP (các gói tin liên quan đến việc truy cập web), ta gõ “http” vào khung này và chọn Apply.



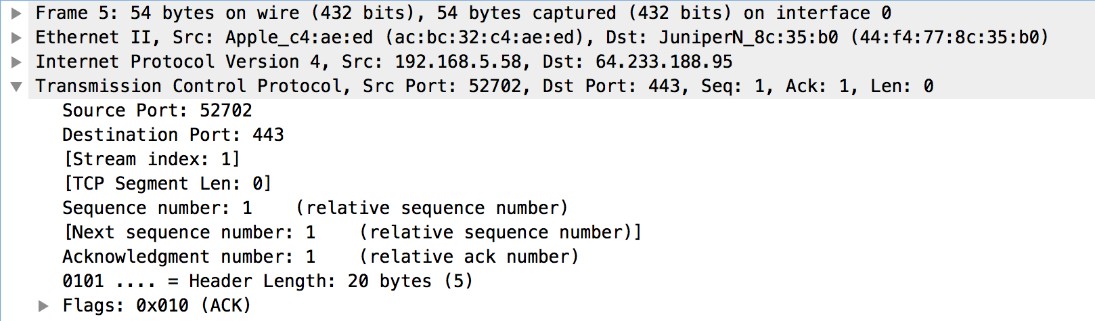
1. Packet-listing windows:

Hiển thị thông tin tóm tắt cho các gói tin đã bắt, bao gồm: o No: Số thứ tự (số này được gán bởi Wireshark, không phải số thứ tự chứa trong header của gói tin)

* + - Time: mốc thời gian gói tin bị bắt. o Source: địa chỉ nguồn o Destination: địa chỉ đích. o Protocol: loại giao thức, chỉ hiển thị giao thức hoạt động ở tầng cao nhất.
    - Length: độ dài (kích thước) gói tin.
    - Info thông tin đặc tả cho giao thức đó.

1. Packet details window:

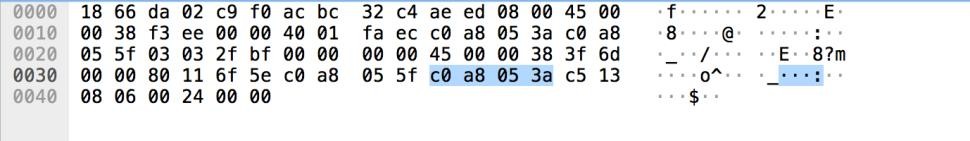
Cung cấp các thông tin chi tiết về gói tin được chọn từ packet-listing window.



Các thông tin này bao gồm chi tiết về Ethernet frame (giả sử gói tin được gửi và nhận thông qua Ethernet interface), IP datagram, TCP hoặc UDP segment và cuối cùng là thông tin về giao thức ở tầng cao nhất.

1. Packet Raw data

Hiển thị toàn bộ nội dung của gói tin dưới dạng ASCII và hexadecimal.



Thực ra, bản chất của mỗi gói tin bắt được chính là phần dữ liệu thô này. Các nội dung hiển thị tại phần 3, 4 do Wireshark phân tích và trực quan hóa để người dùng thuận tiện theo dõi.

2.2 Thử nghiệm bắt gói tin với Wireshark

 Sinh viên thực hành theo các bước sau tại môi trường đã chuẩn bị:

Khởi động trình duyệt web bất kỳ như Google Chrome, Firefox, Edge,... và phần mềm Wireshark (phiên bản mới nhất)

Lưu ý: Nếu sử dụng Wireshark cài đặt sẵn trong các máy tính tại phòng Lab, hãy kiểm tra và cập nhật Wireshark lên phiên bản mới nhất trước khi thực hành.

A screenshot of a computer

AI-generated content may be incorrect.

Tại phần Capture, chọn interface đang hoạt động chính trên máy để bắt đầu bắt gói tin.

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó, cửa sổ như Hình 4 sẽ xuất hiện và hiển thị kết quả bắt gói tin tại interface đã chọn.

A screenshot of a computer

AI-generated content may be incorrect.

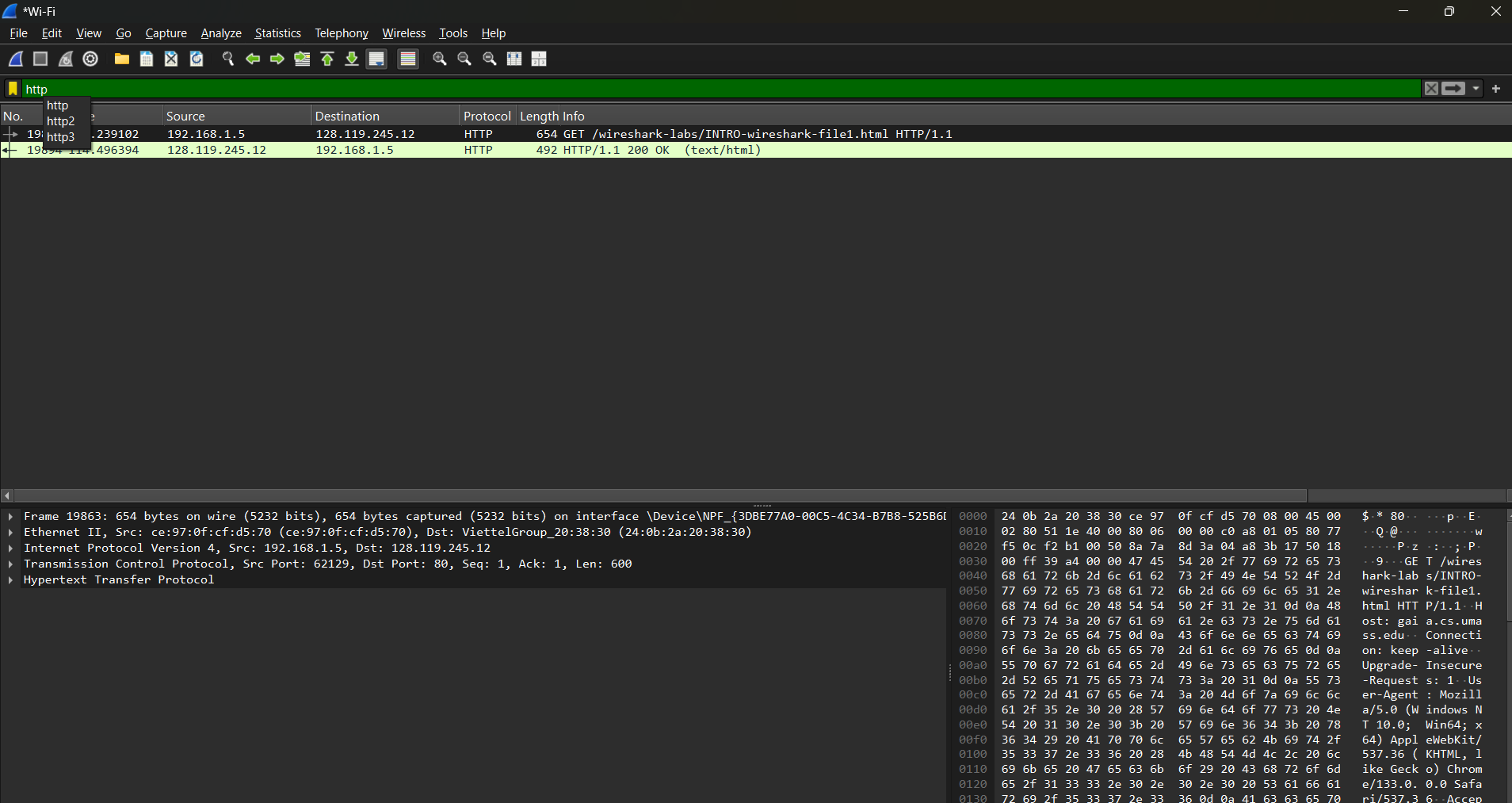
Mở trình duyệt web và chỉ truy cập vào website có địa chỉ như sau <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> Đây là một website đơn giản có nội dung như sau:

A screenshot of a computer

AI-generated content may be incorrect.

## Hình 5.Truy cập website wireshark-file1 thành công

Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là một dòng chào mừng đơn giản), dừng bắt gói tin tại Wireshark.



## Hình 6.Kết quả bắt gói tin sau khi dừng bắt gói tin

Gõ “http” vào packet-display filter sau đó chọn Apply để Wireshark chỉ hiển thị các thông điệp HTTP trong packet-listing window.

A screenshot of a computer

AI-generated content may be incorrect.

## Hình 7.Lọc các gói tin HTTP từ kết quả bắt gói tin

Tìm 2 thông điệp HTTP GET được gửi từ máy tính đến

gaia.cs.umass.edu server (tìm trong packet-listing window đoạn chứa GET theo

sau bởi gaia.cs.umass.edu) và HTTP 200 OK được trả về từ server đến máy tính hiện tại. Sau khi chọn thông điệp HTTP GET, các thông tin về Ethernet frame, IP datagram, TCP segment và HTTP header sẽ được hiển thị ở packet-header window.

Lưu ý: Gói tin trả về HTTP – 200 OK chỉ xuất hiện khi bắt gói tin ở lần truy cập đầu tiên trên trình duyệt.

Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng MSSV-Bai1.pcapng. Ví dụ: 18521006-Bai1.pcapng.

A screenshot of a computer

AI-generated content may be incorrect.

Chọn biểu tượng Start capturing packets để bắt đầu quá trình bắt gói tin mới.

A screenshot of a computer

AI-generated content may be incorrect.

 Chọn 1 website mà sinh viên thường hay truy cập, ví dụ uit.edu.vn, tinhte.vn,… và tiến hành bắt gói tin trên website đó

Lặp lại các bước 4-5-6-7 với một website khác có chứa nhiều thông tin hơn mà sinh viên thường truy cập. Ví dụ: tuoitre.vn, uit.edu.vn,…

* Ở đây em chọn website: https://daotao.hcmunre.edu.vn/

Tiến hành bắt gói tin tương tự:

A screenshot of a computer

AI-generated content may be incorrect.

Lưu lại tập tin sau khi bắt được ở website thứ 2 thành file pcapng có tên dạng MSSV-Bai2.pcapng

A screenshot of a computer

AI-generated content may be incorrect.

2.3 Phân tích kết quả bắt gói tin từ Wireshark

1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

Trang web 1: Bắt được 2909 gói tin

Tổng thời gian: 8.48s

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

Trang web 2: Bắt được 2460 gói tin

Tổng thời gian: 8.8s

1. Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc “http” khi truy cập 2 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.
2. **TCP (Transmission Control Protocol)**:
   1. **Chức năng**: TCP là giao thức truyền tải dữ liệu đáng tin cậy trong các mạng máy tính. Nó đảm bảo rằng dữ liệu được truyền đến đích mà không bị mất mát, thông qua việc phân mảnh và tổ chức lại các gói tin.
3. **UDP (User Datagram Protocol)**:
   1. **Chức năng**: UDP là giao thức truyền tải không có kết nối, ít phức tạp hơn so với TCP. Nó không đảm bảo độ tin cậy trong việc truyền tải dữ liệu, nhưng có tốc độ nhanh hơn, thường được sử dụng trong các ứng dụng yêu cầu tốc độ như video streaming hoặc các cuộc gọi VoIP.
4. **DNS (Domain Name System)**:
   1. **Chức năng**: DNS chuyển đổi tên miền (domain names) như "example.com" thành địa chỉ IP mà các máy tính có thể sử dụng để kết nối với nhau trong mạng Internet.
5. **ARP (Address Resolution Protocol)**:
   1. **Chức năng**: ARP được sử dụng để ánh xạ địa chỉ IP đến địa chỉ MAC (Media Access Control) trong một mạng nội bộ (LAN), giúp các thiết bị trong mạng xác định nhau.
6. **SSL/TLS (Secure Sockets Layer / Transport Layer Security)**:
   1. **Chức năng**: SSL và TLS là các giao thức mã hóa được sử dụng để bảo vệ sự riêng tư và tính toàn vẹn của dữ liệu trong quá trình truyền tải qua mạng, đặc biệt là trong các giao dịch qua HTTPS.
7. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).

Bài 1:

A green line on a black background

AI-generated content may be incorrect.

Bài 2:

A screenshot of a computer

AI-generated content may be incorrect.

1. Nội dung hiển thị trên trang web gaia.cs.umass.edu

A screenshot of a computer

AI-generated content may be incorrect.

“Congratulations! You've downloaded the first Wireshark lab file!” có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.

1. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?
2. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó.

|  |
| --- |
| Mở rộng: Theo bạn, địa chỉ IP dùng để làm gì và có cách nào khác để xem địa chỉ IP của máy tính và của một website khác hay không? Hãy thực hiện ví dụ minh họa. |



# **1.** Yêu cầu

* Sinh viên tìm hiểu và thực hành theo hướng dẫn. Thực hiện báo cáo cá nhân.
* Sinh viên báo cáo kết quả thực hiện và nộp bài gồm:
  + Báo cáo chi tiết (lưu ý xuất thành file .PDF), trình bày cụ thể các yêu cầu trong bài thực hành (có ảnh minh họa) và giải thích các vấn đề kèm theo.
  + 2 file MSSV-Bai1.pcapng và MSSV-Bai2.pcapng thu được từ việc bắt gói tin bằng Wireshark theo yêu cầu của bài thực hành.

Đặt tên file báo cáo theo định dạng như mẫu:

MSSV\_HoTen\_BaoCaoLabX

Ví dụ: 18521007\_NguyenVanA\_Lab1

Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

* Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

**10**

**2.** Đánh **giá:**

Sinh viên hiểu và tự thực hiện được bài thực hành, trả lời đầy đủ các yêu cầu đặt ra, khuyến khích trình bày báo cáo chi tiết, rõ ràng.



Bài thực hành được xây dựng dựa trên Wireshark Lab: Getting Started - Supplement to Computer Networking: A Top-Down Approach, 7th ed., J.F Kurose and K.W Ross.



# Chúc các em hoàn thành tốt

Link ytb: <https://youtu.be/_35UyuIrUK4>

Link Git: