Lab 1

SPECIAL EDITION

Làm quen với Wireshark

Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Tháng 03/2024
Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Làm quen với phần mềm **Wireshark** – công cụ bắt gói tin phổ biến, phục vụ việc nghiên cứu về hoạt động của các tầng mạng.

2. Kiến thức nền tảng

- Kiến thức về Mạng máy tính cơ bản, nguyên tắc hoạt động của mạng máy tính.

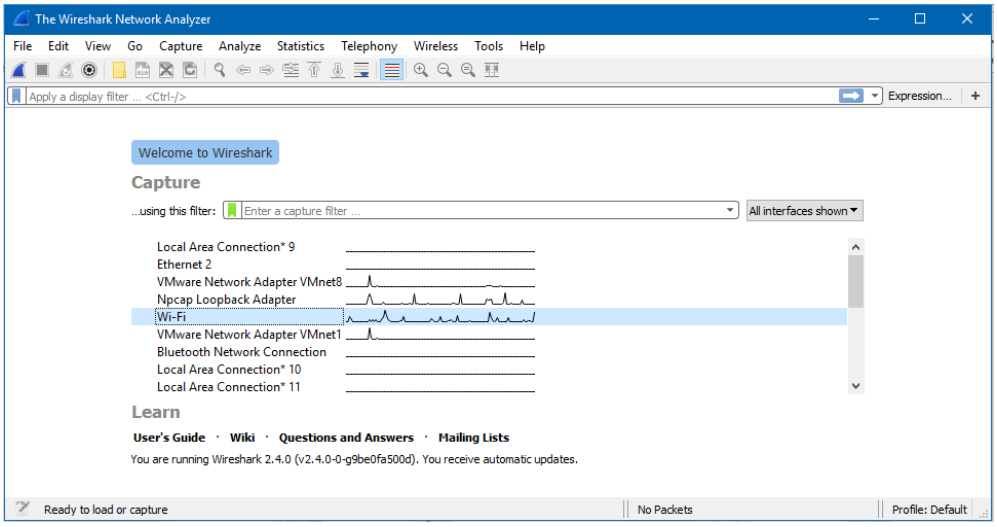
3. Môi trường thực hành

Sinh viên cần chuẩn bị trước máy tính có kết nối Internet và cài đặt các phần mềm:

Phần mềm Wireshark

Đây là phần mềm bắt gói tin trong mạng (sniffing) giúp theo dõi quá trình trao đổi dữ liệu trong mạng. Đối với môn học này, Wireshark giúp phân tích và hiểu rõ hơn hoạt động của các tầng (layer) của mạng.

Tải về bản mới nhất tại https://www.wireshark.org/download.html



Hình 1. Giao diện chính của Wireshark

B. THỰC HÀNH

1. Task 1: Mở đầu về Mạng máy tính

➲ *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).

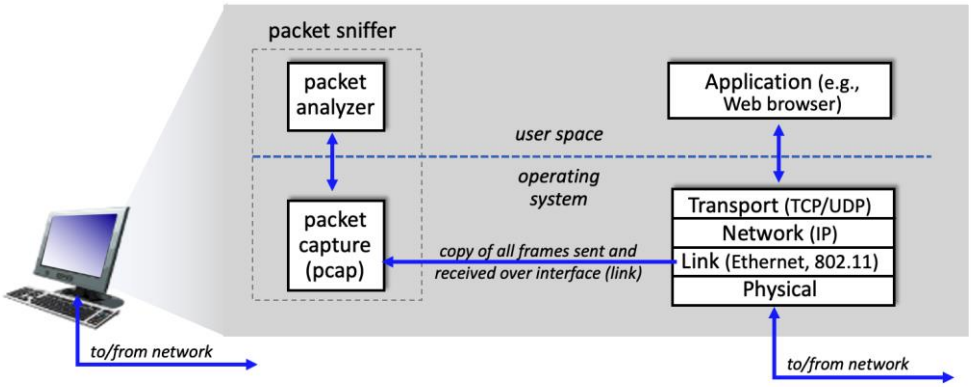
- Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

- 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

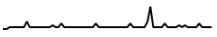
Wireshark là phần mềm bắt gói tin (packet sniffer) rất phổ biến và miễn phí chạy trên Windows, Linux, MacOS, hỗ trợ bắt gói tin và quan sát nội dung của các thông điệp được trao đổi bởi các giao thức tại các tầng mạng khác nhau.



Hình 2. Cấu trúc của việc bắt gói tin

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.

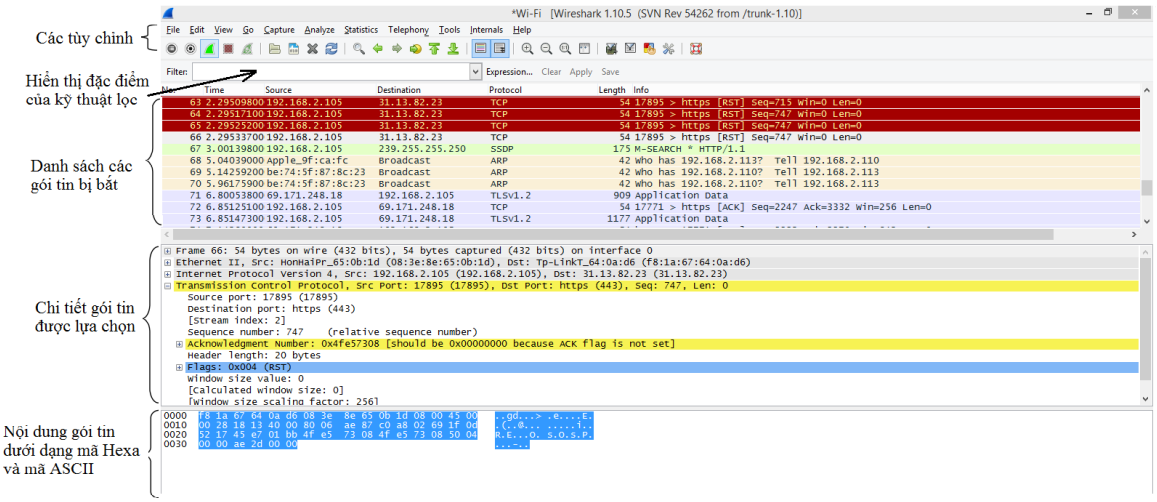
Giao diện chính khi mở Wireshark sẽ giống *Hình 1.*

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:

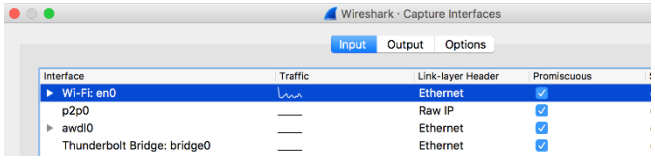
- *Kết nối có dây: Ethernet, Local Area Connection (LAN).*
- *Kết nối không dây: WiFi.*

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



Hình 3. 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 4. 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.

   - **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.
   - **Capture** menu cho phép bắt đầu bắt gói tin và thay đổi các tùy chỉnh
   - **Các button thường 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

2. **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.

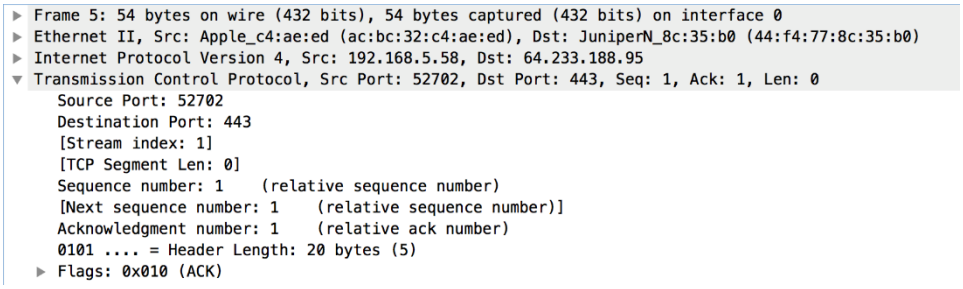
3. **Packet-listing windows**:

Hiển thị thông tin tóm tắt cho các gói tin đã bắt, bao gồm:

- 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.
- Source: địa chỉ nguồn
- Destination: địa chỉ đích.
- 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.

4. Packet details window:

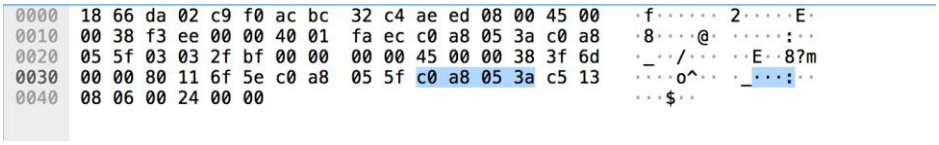
Cung cấp các thông tin chi tiết về gói tin được chọn từ packet-listing window.



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.

5. 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.

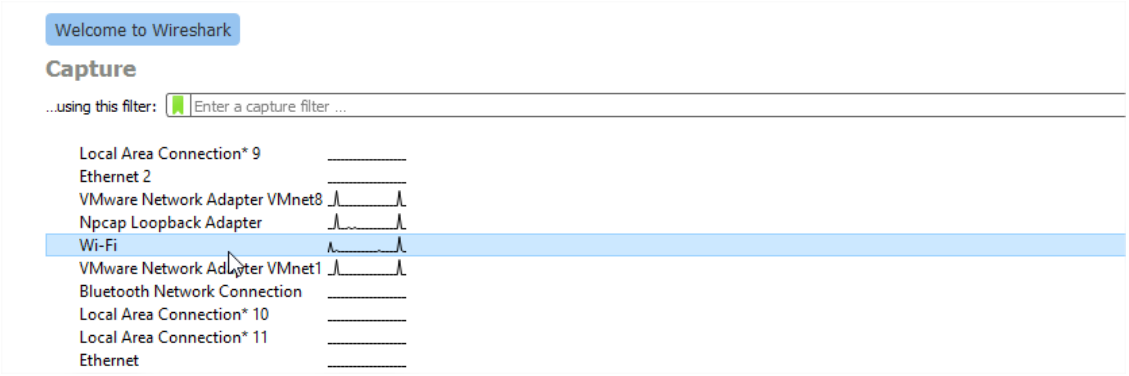
2.2 Thử nghiệm bắt gói tin với Wireshark

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

- **Bước 1:** Khởi động trình duyệt web bất kỳ như *Google Chrome, Firefox, Edge*,... và phần mềm Wireshark (phiên bản mới nhất)

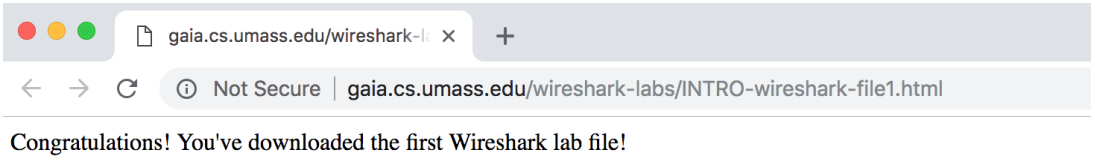
  Lưu ý: *Nếu sử dụng Wireshark cài đặt sẵn trong các máy tính tại phòng Lab, hãy kiểm tra và cập nhật Wireshark lên phiên bản mới nhất trước khi thực hành.*
- **Bước 2:** Tại phần **Capture**, chọn interface đang hoạt động chính trên máy để bắt đầu bắt gói tin.

Ví dụ*: Khi đang sử dụng Wifi để kết nối Internet, chọn interface Wifi.*



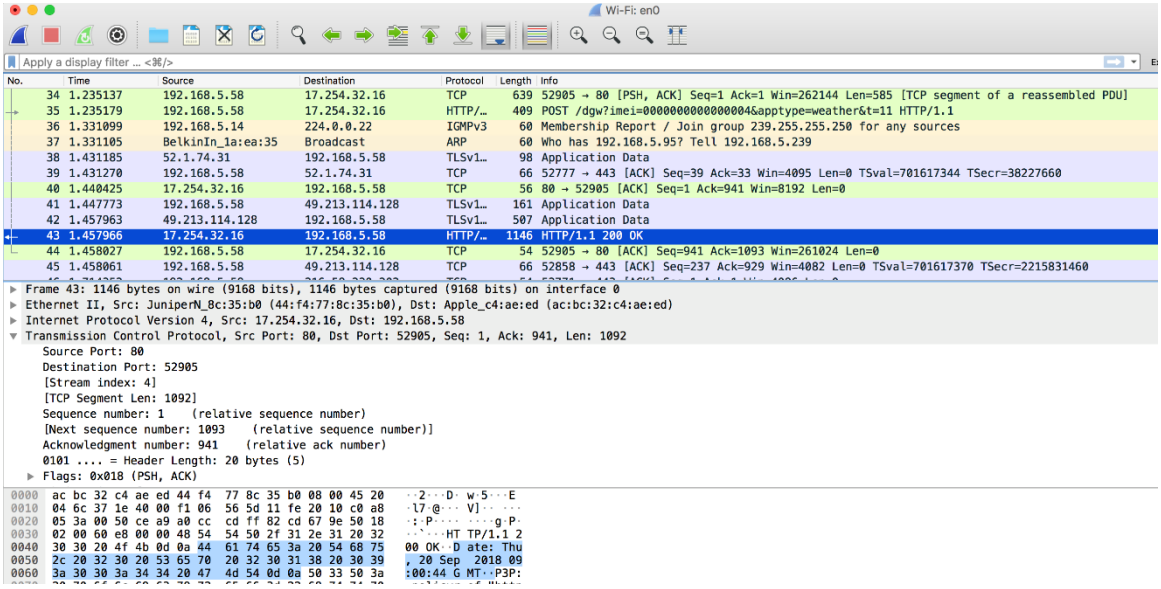
Hình 5. Chọn interface mạng phù hợp

- **Bước 3:** Sau đó, cửa sổ như *Hình 4* sẽ xuất hiện và hiển thị kết quả bắt gói tin tại interface đã chọn.
- **Bước 4:** 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:



Hình 6. Truy cập website wireshark-file1 thành côn

- **Bước 5:** 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 7. Kết quả bắt gói tin sau khi dừng bắt gói tin

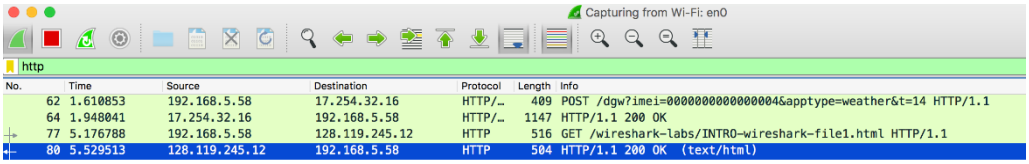
Lưu ý: *Phải dừng bắt gói tin ngay sau khi đã truy cập thành công vào trang web trên để tránh bắt các gói tin không cần thiết, làm tăng dung lượng file .pcapng khi lưu lại.*

Cửa sổ chính của Wireshark bây giờ giống như ***Hình 7***. Bạn đã có các gói tin chứa đầy đủ các thông điệp được trao đổi giữa máy tính và web server. Thông điệp HTTP

trao đổi với web server **gaia.cs.umass.edu** phải xuất hiện đâu đó trong các gói tin được bắt.

Có nhiều loại gói tin được hiển thị *(tương ứng với nhiều giao thức).* Mặc dù bạn chỉ đơn thuần truy cập một trang web nhưng cũng có nhiều giao thức khác chạy bên dưới mà bạn không thấy được.

- **Bước 6:** Gõ "**http**" vào **packet-display filter** sau đó chọn Apply để Wireshark chỉ hiển thị các thông điệp HTTP trong packet-listing window.



Hình 8. Lọc các gói tin HTTP từ kết quả bắt gói tin

- **Bước 7:** 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.*

- **Bước 8:** Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng *MSSV-Task1.pcapng.* Ví dụ: *25520001-Task1.pcapng*.
- **Bước 9:** Chọn biểu tượng **Start capturing packets** để bắt đầu quá trình bắt gói tin mới.
- **Bước 10:** 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. Lưu ý, website này phải có sử dụng **https://...**

Lặp lại các bước **4-5** với website đã chọn tại Bước 10.

- **Bước 11:** Lưu lại tập tin sau khi bắt được ở website thứ 2 thành file pcapng có tên dạng *MSSV-Task2.pcapng.*

2.3 Phân tích kết quả bắt gói tin từ Wireshark

➲ *Sinh viên tự thực hiện các bước thực hành như hướng dẫn tại phần 2.2 để có được 2 file kết quả pcapng từ Wireshark. Lần lượt mở từng file tương ứng với 2 website trên và trả lời các câu hỏi sau:*

Lưu ý: *Trình bày câu trả lời kèm theo ảnh chụp màn hình tương ứng vị trí đã quan sát được thông tin trên Wireshark.*

***Dựa vào file *MSSV-Task1.pcapng*, sinh viên thực hiện trả lời các câu hỏi sau:**

1. Tổng thời gian bắt gói tin đối với website đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?
2. Trong các gói tin bắt được, có tổng cộng bao nhiêu gói tin HTTP?
3. 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 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.
4. Xác định gói tin HTTP GET đầu tiên gửi đến website đã thử nghiệm. Cho biết gói tin này cơ bản dùng để làm gì?

   Gợi ý: Quan sát thông tin trong packet details window hay Info của gói tin.
5. Xác định gói tin phản hồi của gói tin HTTP GET ở câu 4, thông tin nào xác định điều đó?
6. Tính thời gian từ khi gói tin **HTTP GET** đầu tiên được gửi cho đến khi có gói tin phản hồi **HTTP 200 OK** đối với 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).*
7. Nội dung hiển thị trên trang web gaia.cs.umass.edu

   "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.
8. Hãy tìm hiểu về định dạng của địa chỉ IP và thử phỏng đoán địa chỉ IP của **gaia.cs.umass.edu** là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

9. Từ các nội dung trên, hãy mô tả cơ bản khi truy cập một website (ví dụ website đã thử nghiệm ở trên) thì quá trình gửi và nhận gói tin đã hoạt động như thế nào? Trình duyệt mà bạn đang sử dụng đóng vai trò gì?

Lưu ý: Mô tả lại quá trình này một cách cơ bản dựa trên gói tin từ khi nhập đường dẫn website đến khi website được hiển thị đầy đủ.

***Dựa vào file *MSSV-Task2.pcapng*, sinh viên thực hiện trả lời các câu hỏi sau:**

10. Khi sử dụng bộ lọc "http" như ở đối với website ở Task 1 thì kết quả thu được như thế nào, có các gói tin HTTP tương tự không?
11. Tìm cách xác định địa chỉ IP của website đã chọn là bao nhiêu? Địa chỉ IP của máy tính bạn lúc này là bao nhiêu?
12. Sử dụng thành phần packet-display filter để hiển thị đầy đủ quá trình trao đổi gói tin giữa máy tính của bạn và website bằng cú pháp: ip.addr==<địa chỉ IP của máy tính> && ip.addr==<địa chỉ IP của website> . Cho biết rằng bạn có thể thấy được nội dung trả về của website không? Mô tả.
13. Hãy chỉ ra **ít nhất 2 gói tin** mà bạn cho rằng là quan trọng khi truy cập website này. Tìm hiểu và mô tả ngắn gọn các giao thức này. Giải thích.

Câu hỏi số 14: 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 thực hiện để minh họa điều đó. Tìm được càng nhiều cách càng tốt.

C. YÊU CẦU & ĐÁNH GIÁ

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 *(trình bày theo template đã thống nhất)*, 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-Task1.pcapng*** và ***MSSV-Task2.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: **Mã lớp-LabX_MSSV** *Ví dụ: IT005.O25.1-Lab01_25520001* 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.

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.

D. TÀI LIỆU THAM KHẢO

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.

HẾT

Chúc các em hoàn thành tốt