Họ và tên: Lưu Thy Thy

MSSV: 1050080078

Lớp: 10\_ĐH\_CNPM1

**Làm quen với WireShark - BÀI TẬP 1 LÝ THUYẾT**

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

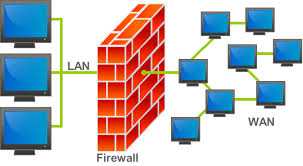
- Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).

Câu trả lời:

Các thiết bị mạng:

* Router (Bộ định tuyến)
* Modem
* Switch (Bộ chuyển mạch)
* Hub
* Access Point (AP – Điểm truy cập)
* FireWall (Tường lửa)
* Load Balancer
* Gateway
* Proxy Server

Hiện tại đang sử dụng FireWall



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

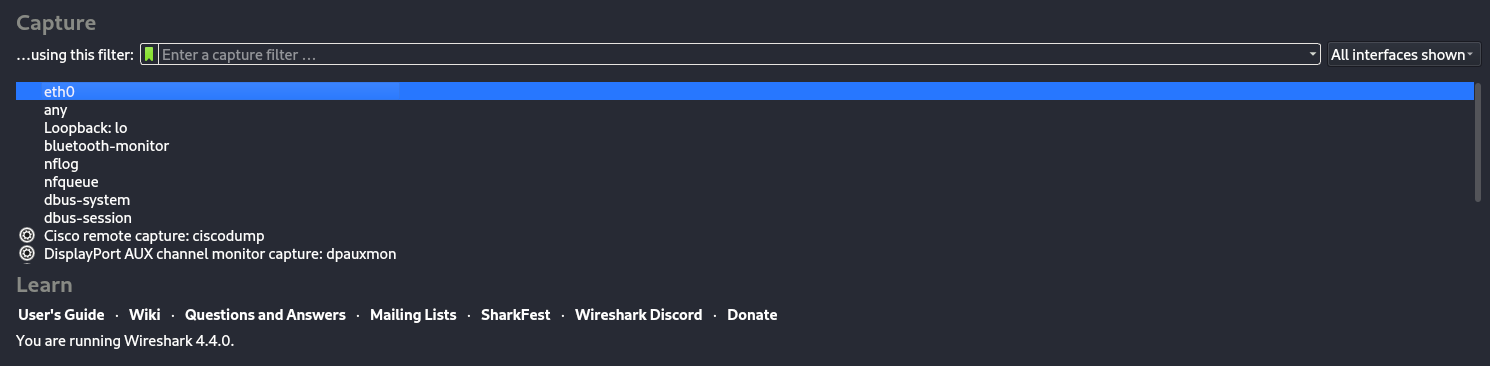
* Mất kết nối với các dịch vụ trực tuyến: Không thể truy cập website, ứng dụng đám mây, email, chat (Messenger, Zalo, Slack, etc.).
* Dừng các hoạt động liên quan đến mạng: Cuộc gọi qua Zoom/Google Meet bị gián đoạn, tải file bị dừng, phát trực tiếp bị ngắt.
* Làm việc nhóm bị gián đoạn: Không thể cập nhật tài liệu trên Google Docs, Notion, Figma,...
* Mất kết nối với API và cơ sở dữ liệu online: Các ứng dụng cần gửi yêu cầu API sẽ không hoạt động đúng.
* Giảm hiệu suất làm việc: Lập trình viên không thể cài đặt package qua npm/yarn, không truy cập tài liệu trên Stack Overflow.

- Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

* Hiểu nguyên lý hoạt động của mạng máy tính: Cách các thiết bị kết nối, truyền dữ liệu.
* Hiểu cách hoạt động của Internet & Web: Cách website hoạt động, truyền dữ liệu qua HTTP.
* Có kiến thức về bảo mật mạng: Các nguy cơ bảo mật (MITM, DDoS, SQL Injection, XSS) và cách phòng tránh.
* Biết cách kiểm tra và chẩn đoán lỗi mạng: Wireshark,...

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

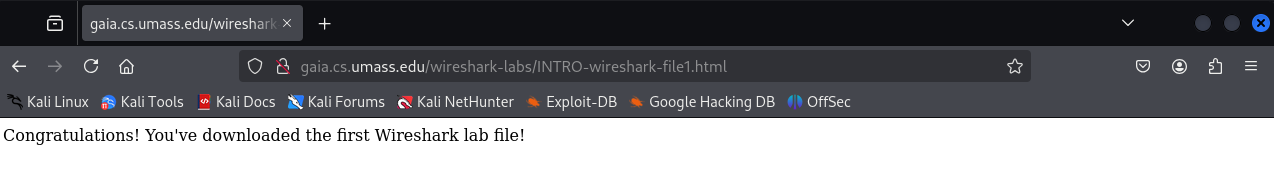
Bước 2: Tại phần Capture, chọn interface đang hoạt động chính trên máy để bắt đầu bắt gói tin.



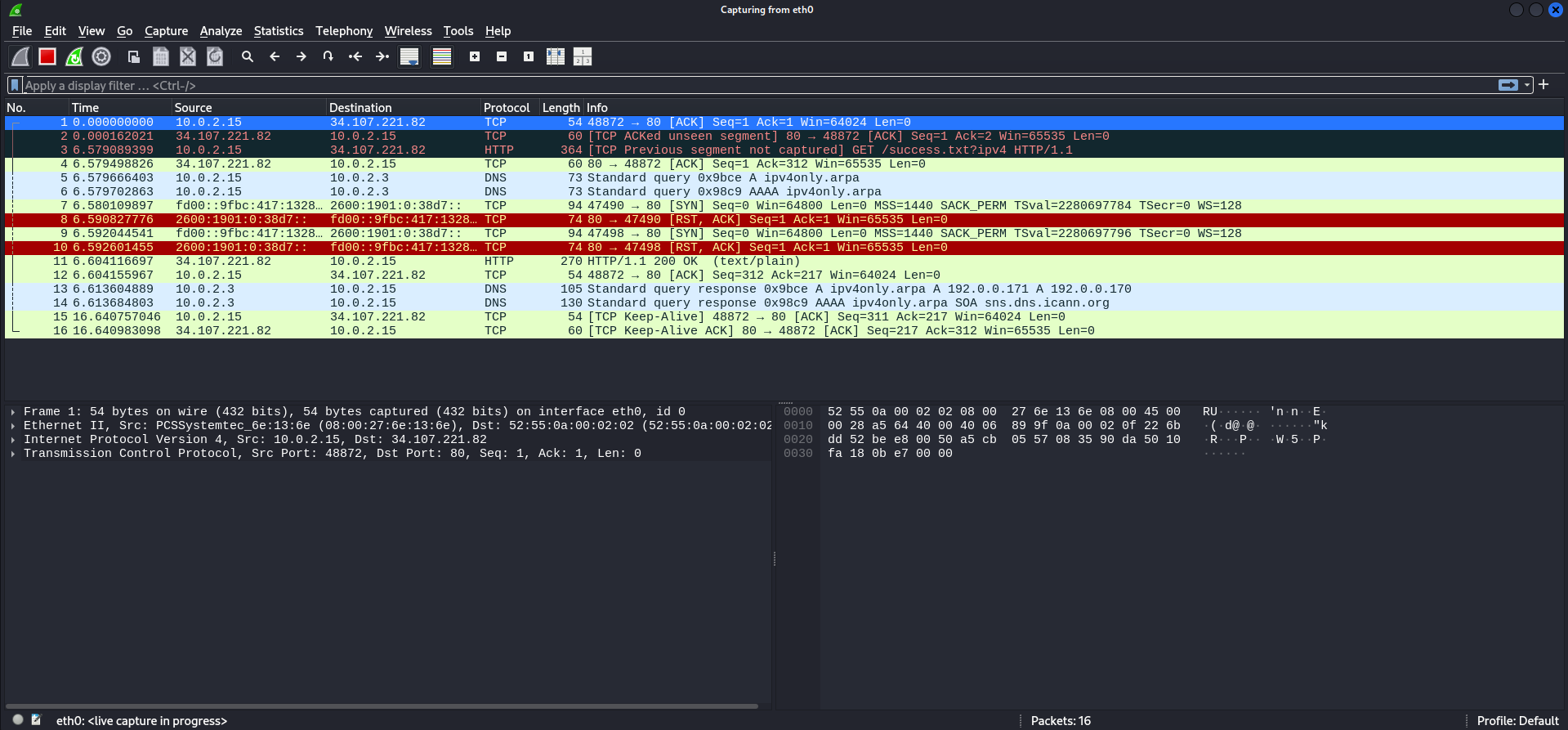
Bước 3: Sau đó, cửa sổ như Hình 4 sẽ xuất hiện và hiển thị kết quả bắt gói tin tại interface đã chọn.

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

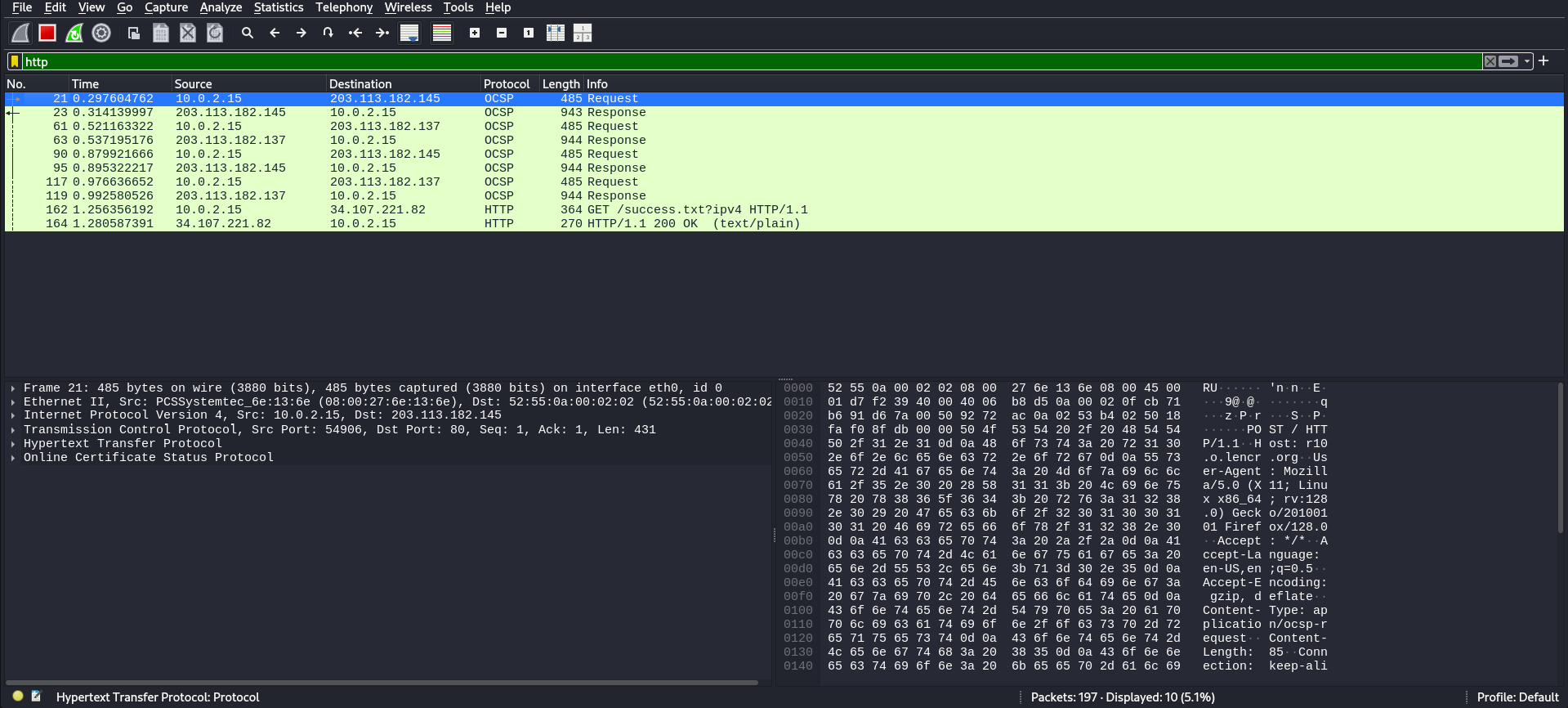


Bước 5: Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là một dòng chào mừng đơn giản), dừng bắt gói tin tại Wireshark.



Bước 6: Gõ “http” vào packet-display filter sau đó chọn Apply để Wireshark chỉ

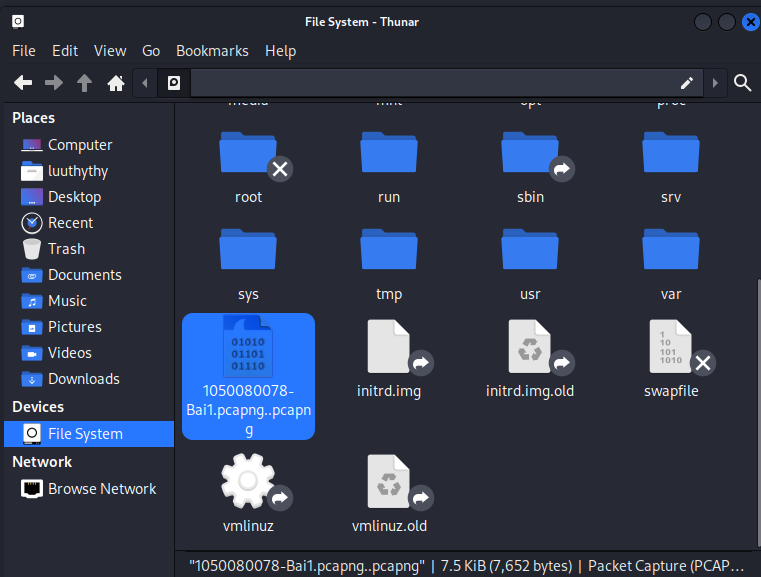
hiển thị các thông điệp HTTP trong packet-listing window.



Bước 7: Tìm 2 thông điệp HTTP GET được gửi từ máy tính đến

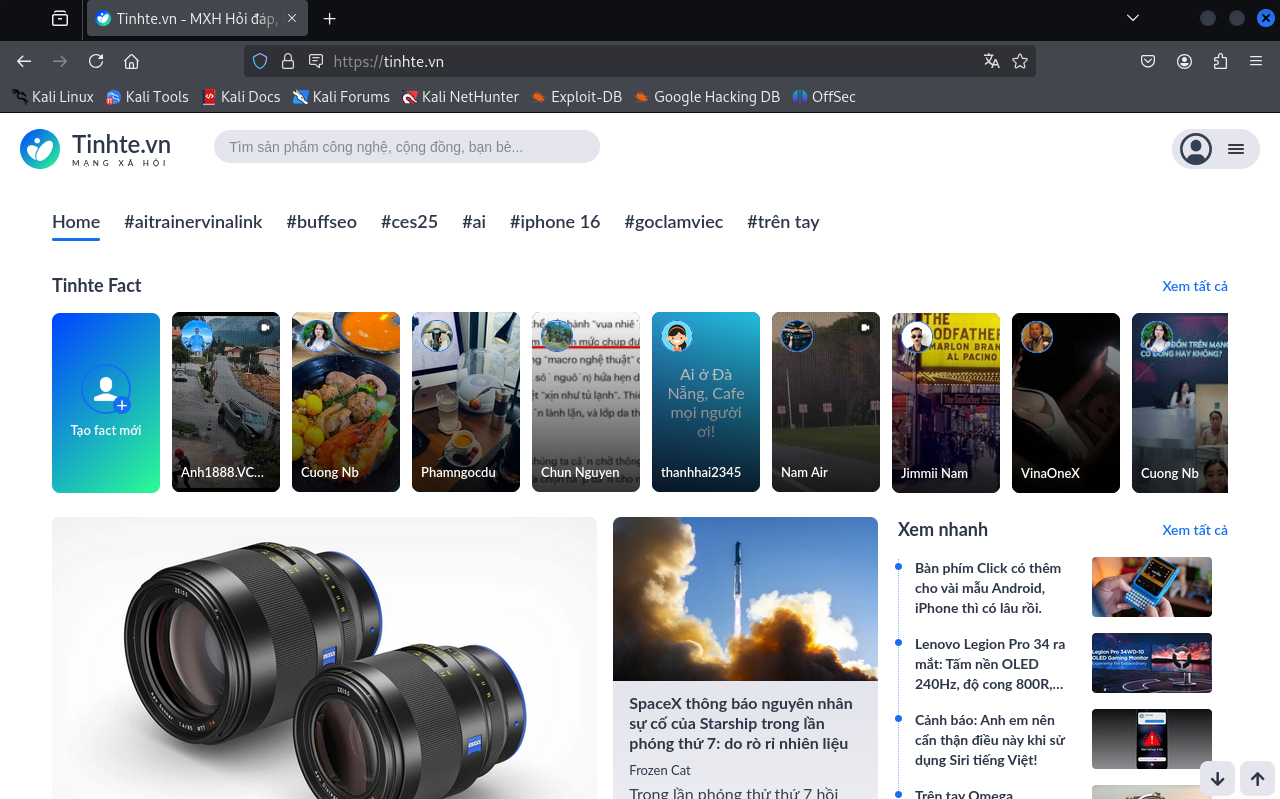
gaia.cs.umass.edu server (tìm trong packet-listing window đoạn chứa GET theo sau bởi gaia.cs.umass.edu) và HTTP 200 OK được trả về từ server đến máy tính hiện tại. Sau khi chọn thông điệp HTTP GET, các thông tin về Ethernet frame, IP datagram, TCP segment và HTTP header sẽ được hiển thị ở packet-header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

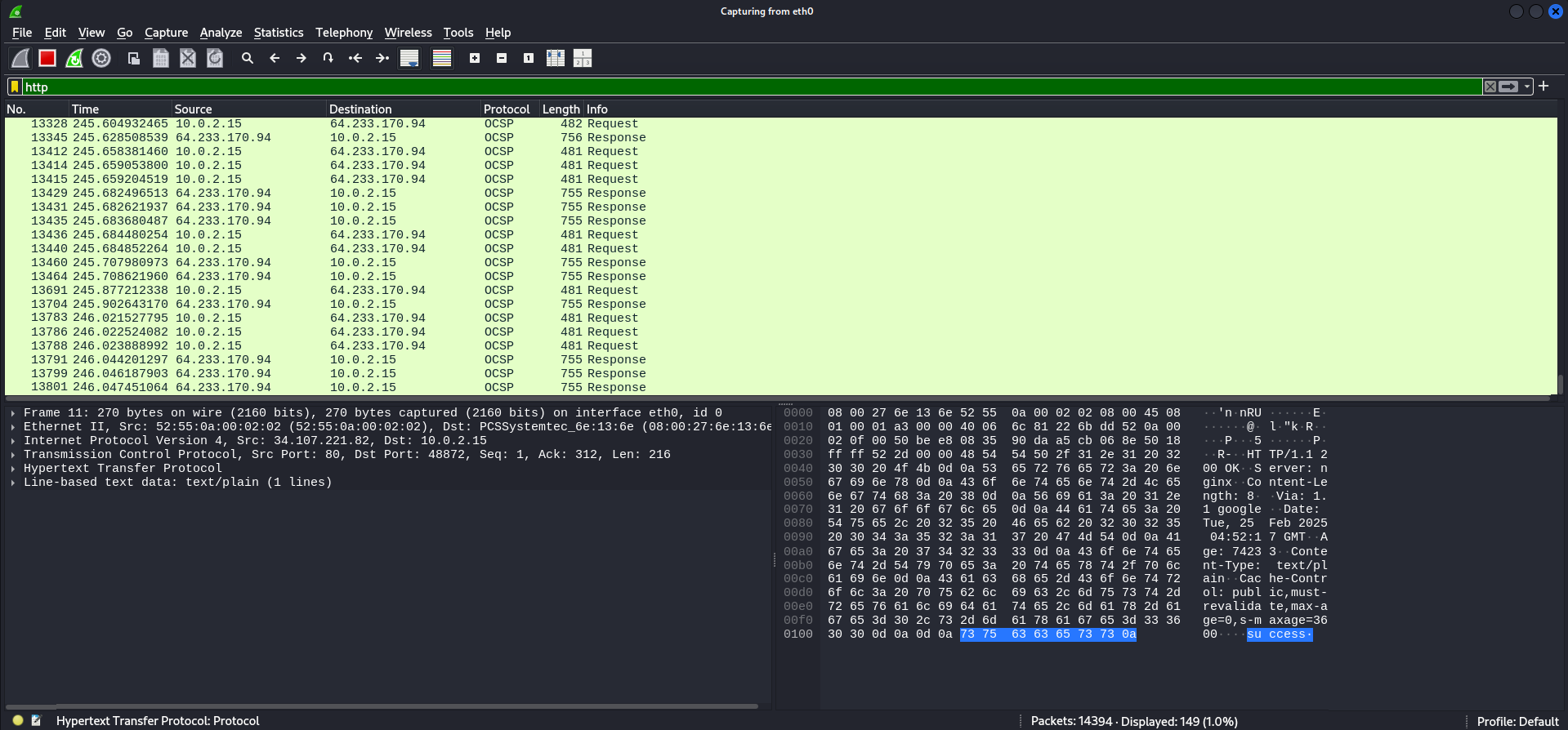
Bước 8: Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng MSSV-Bai1.pcapng.



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





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

Tổng thời gian bắt gói tin: 5 giây (tính từ gói tin đầu tiên đến gói tin cuối cùng).

Tổng số gói tin bắt được: 2 gói tin (hiển thị ở góc dưới của Wireshark hoặc trong thống kê "Capture File Properties").

2. 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.

Câu trả lời :

* TCP (Transmission Control Protocol): Giao thức điều khiển truyền tải, đảm bảo dữ liệu được gửi chính xác giữa các thiết bị.
* UDP (User Datagram Protocol): Giao thức truyền tải không kết nối, nhanh hơn nhưng không đảm bảo tính toàn vẹn của dữ liệu.
* DNS (Domain Name System): Chuyển đổi tên miền thành địa chỉ IP.
* TLS (Transport Layer Security): Mã hóa dữ liệu để bảo mật khi truyền qua mạng, thường thấy trong HTTPS.
* ARP (Address Resolution Protocol): Xác định địa chỉ MAC tương ứng với một địa chỉ IP trong mạng nội bộ.

3. 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).

Câu trả lời: Trong khoảng 30 giây – 1 phút

4. 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.

5. 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?

Địa chỉ IP của gaia.cs.umass.edu: 34.07.221.82

Địa chỉ IP của website thử nghiệm khác: 64.233.170.94

6. 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.

Máy tính gửi yêu cầu DNS để lấy địa chỉ IP của trang web.

Thiết lập kết nối TCP với máy chủ bằng cơ chế bắt tay 3 bước (SYN → SYN-ACK → ACK).

Máy khách gửi yêu cầu HTTP GET (hoặc HTTPS nếu trang web bảo mật).

Máy chủ phản hồi bằng HTTP 200 OK, gửi dữ liệu HTML, CSS, JavaScript,...

Trình duyệt phân tích và hiển thị nội dung trang web.