LAB 1 BẢO MẬT MẠNG MÁY TÍNH VÀ HỆ THỐNG

Họ và tên: Trần Quốc Bảo

MSSV: 1050080129

Lớp: K10\_ĐH\_CNPM2

1. Task 1: Mở đầu về Mạng máy tính

**1. Các loại thiết bị liên quan đến Mạng**

Một số thiết bị mạng phổ biến:

* **Router**: Thiết bị định tuyến, giúp kết nối mạng nội bộ với Internet.
* **Modem**: Chuyển đổi tín hiệu từ nhà cung cấp dịch vụ Internet (ISP) thành tín hiệu mạng có thể sử dụng.
* **Switch**: Chia sẻ kết nối mạng giữa nhiều thiết bị trong mạng nội bộ (LAN).
* **Access Point (AP)**: Thiết bị phát sóng Wi-Fi, mở rộng phạm vi kết nối không dây.
* **Card mạng (NIC)**: Thiết bị trên máy tính giúp kết nối mạng thông qua cổng Ethernet hoặc Wi-Fi.
* **Cáp mạng (Ethernet Cable)**: Dây dẫn tín hiệu mạng giữa các thiết bị.

**2. Những vấn đề có thể xảy ra nếu không có kết nối Internet trong 5 phút**

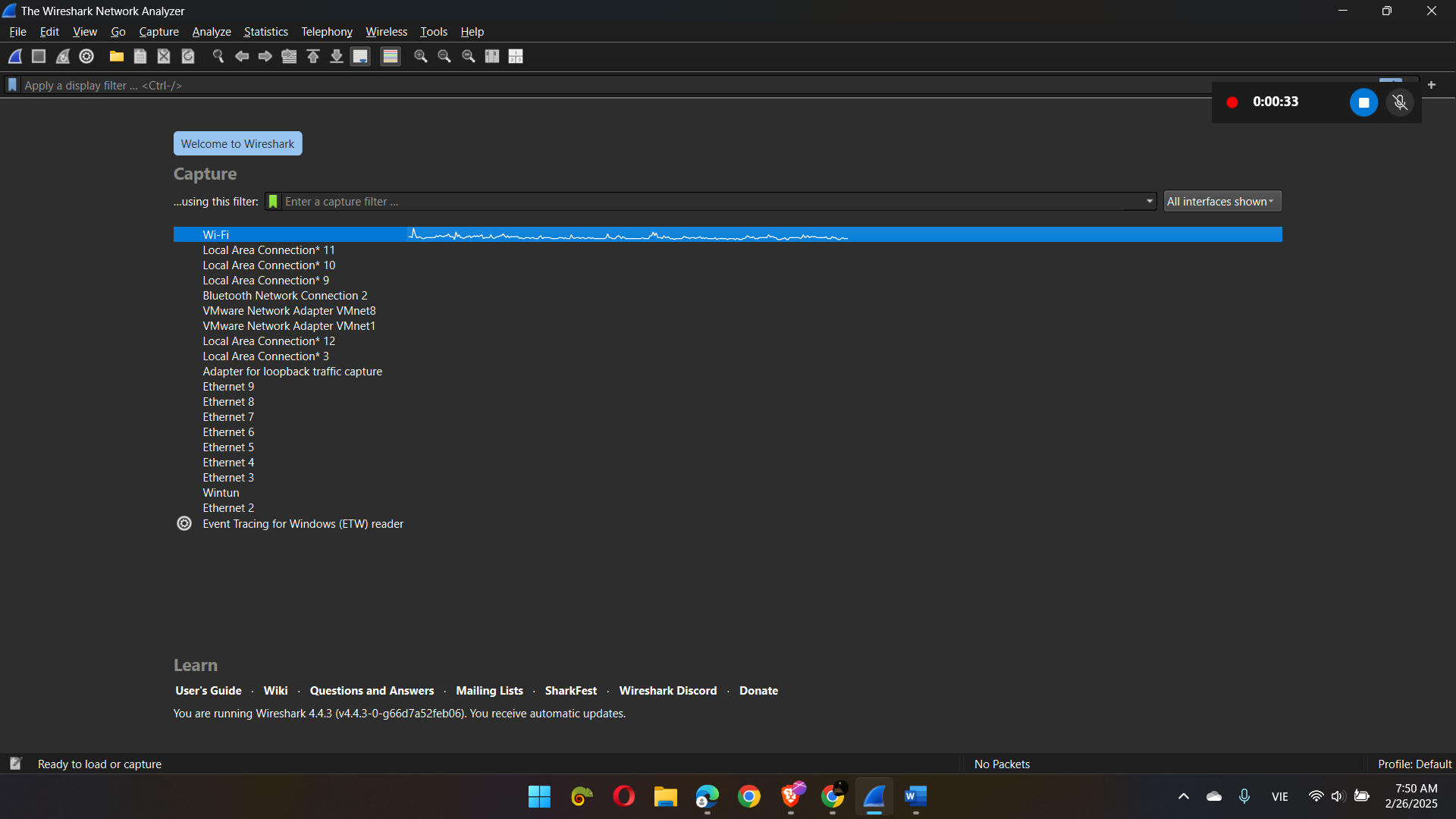
* Không thể truy cập các trang web, dịch vụ trực tuyến (Google, Facebook, YouTube, v.v.).
* Gián đoạn các cuộc họp, học tập và làm việc từ xa (Zoom, Microsoft Teams).
* Dịch vụ nhắn tin và email không thể gửi hoặc nhận tin nhắn.
* Các ứng dụng cần Internet (Spotify, Netflix, game online) không thể hoạt động.
* Ảnh hưởng đến các thiết bị IoT (camera an ninh, smart home).

**3. Mục tiêu kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính**

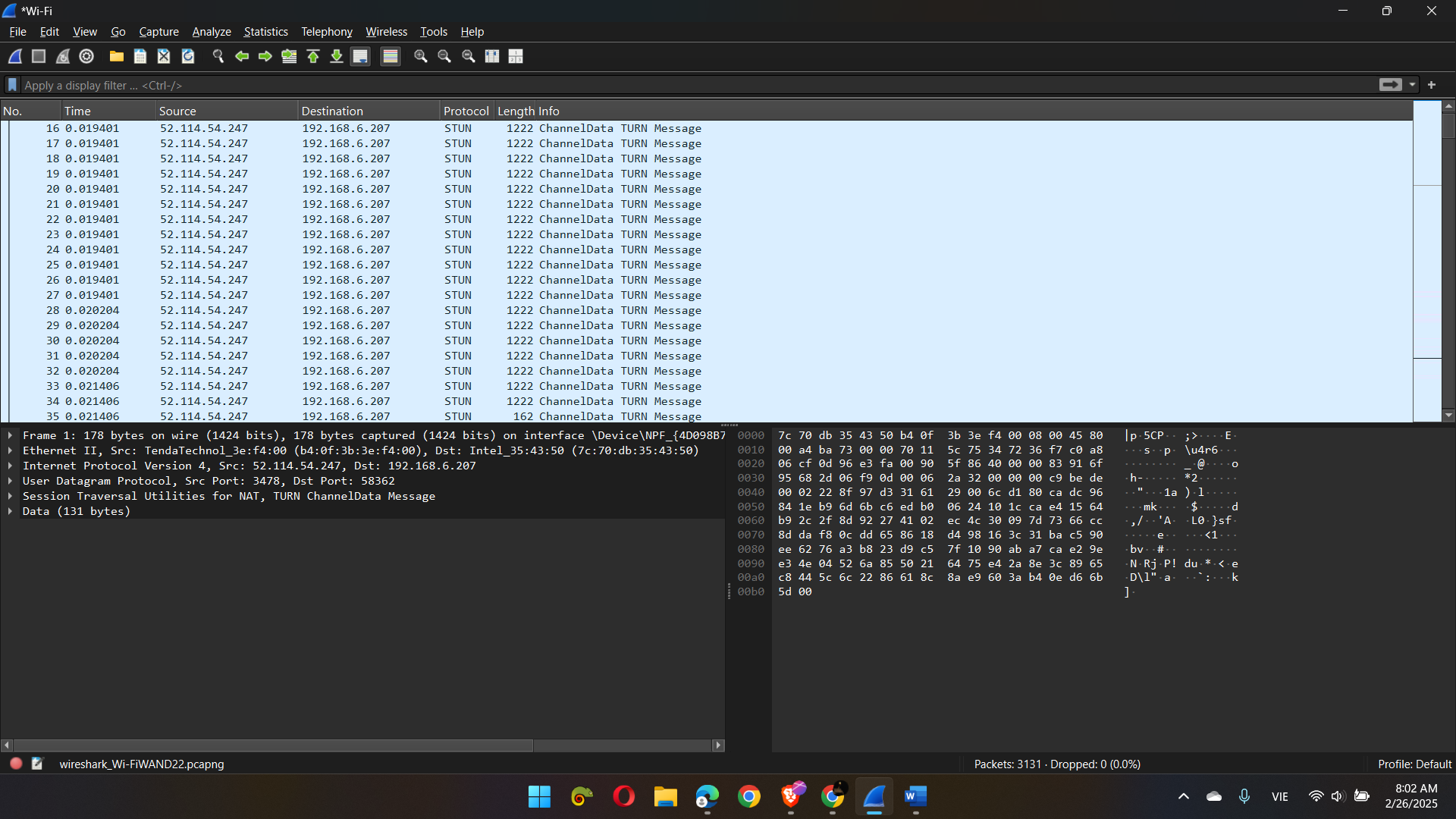
* Hiểu được các khái niệm cơ bản về mạng máy tính (LAN, WAN, TCP/IP, DNS, DHCP...).
* Biết cách thiết lập và cấu hình mạng nội bộ, kết nối Internet.
* Nắm vững các giao thức mạng quan trọng như HTTP, FTP, ICMP...
* Biết cách khắc phục sự cố mạng cơ bản.
* Hiểu về bảo mật mạng, tường lửa, VPN, và cách bảo vệ hệ thống mạng.
* Có thể ứng dụng kiến thức vào thực tế như cấu hình thiết bị mạng, giám sát và tối ưu hóa mạng.

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

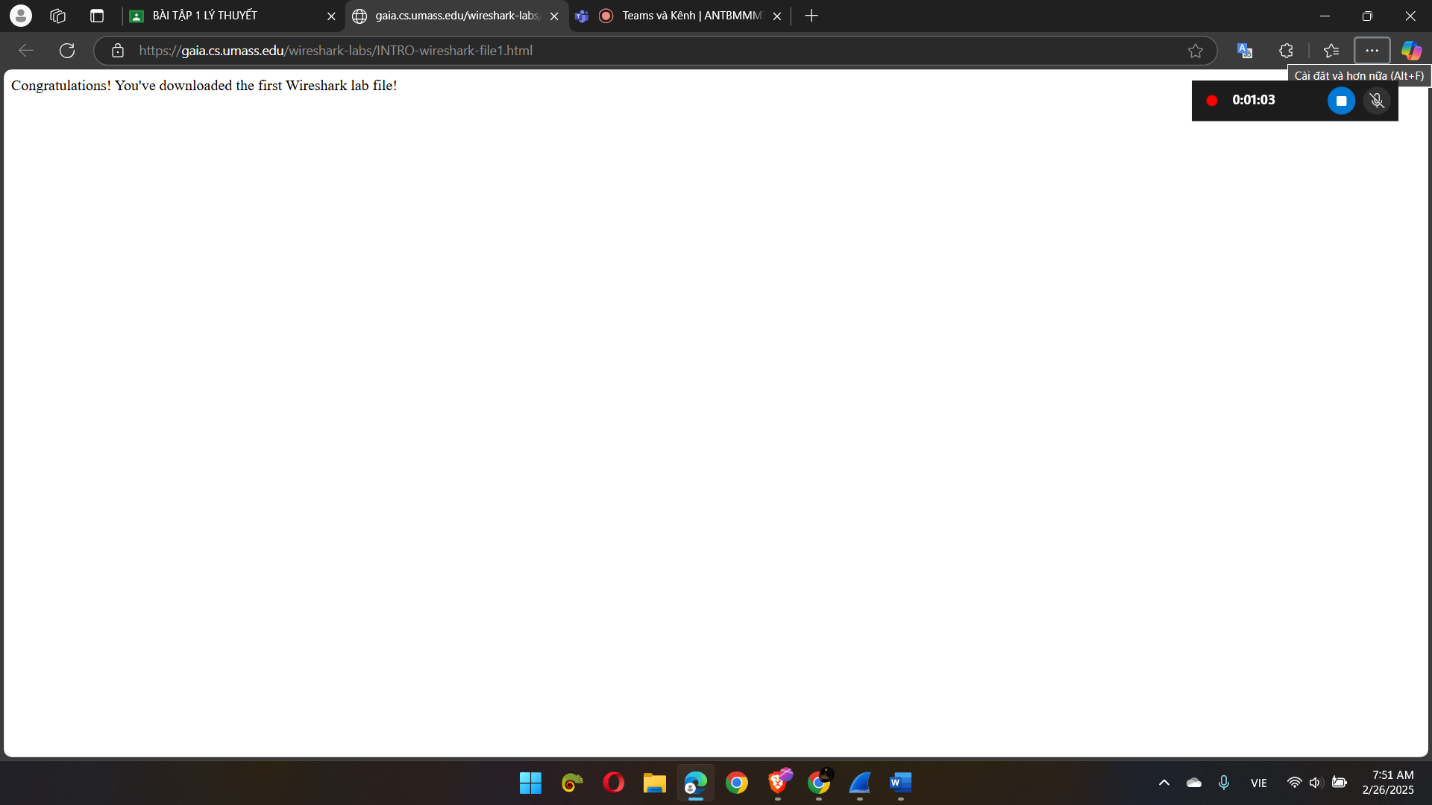
Bước 1: Chọn interface mạng phù hợp



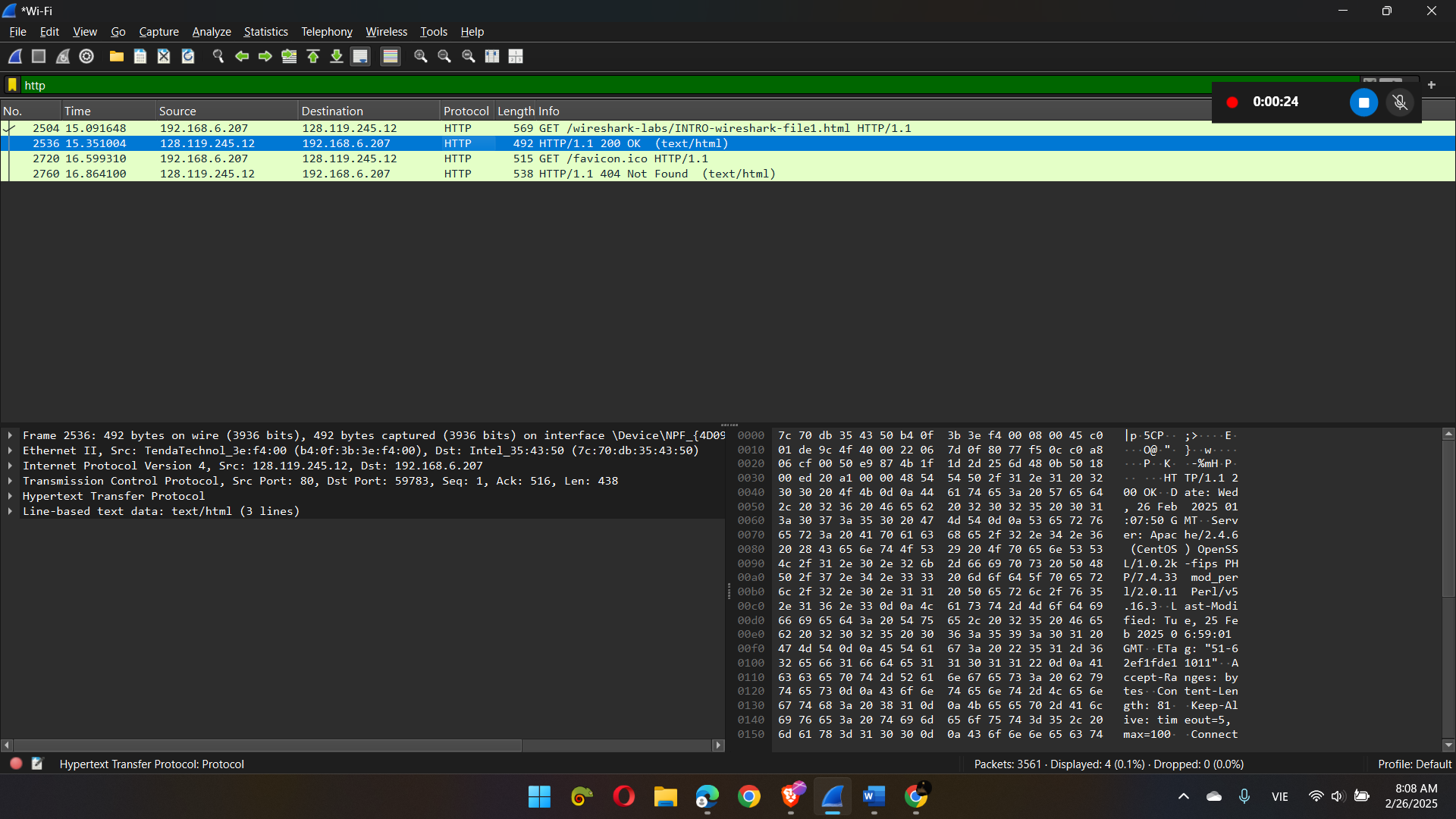
Bước 2: Kết quả bắt gói tin



Bước 3: Mở trình duyệt web: <http://ygaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

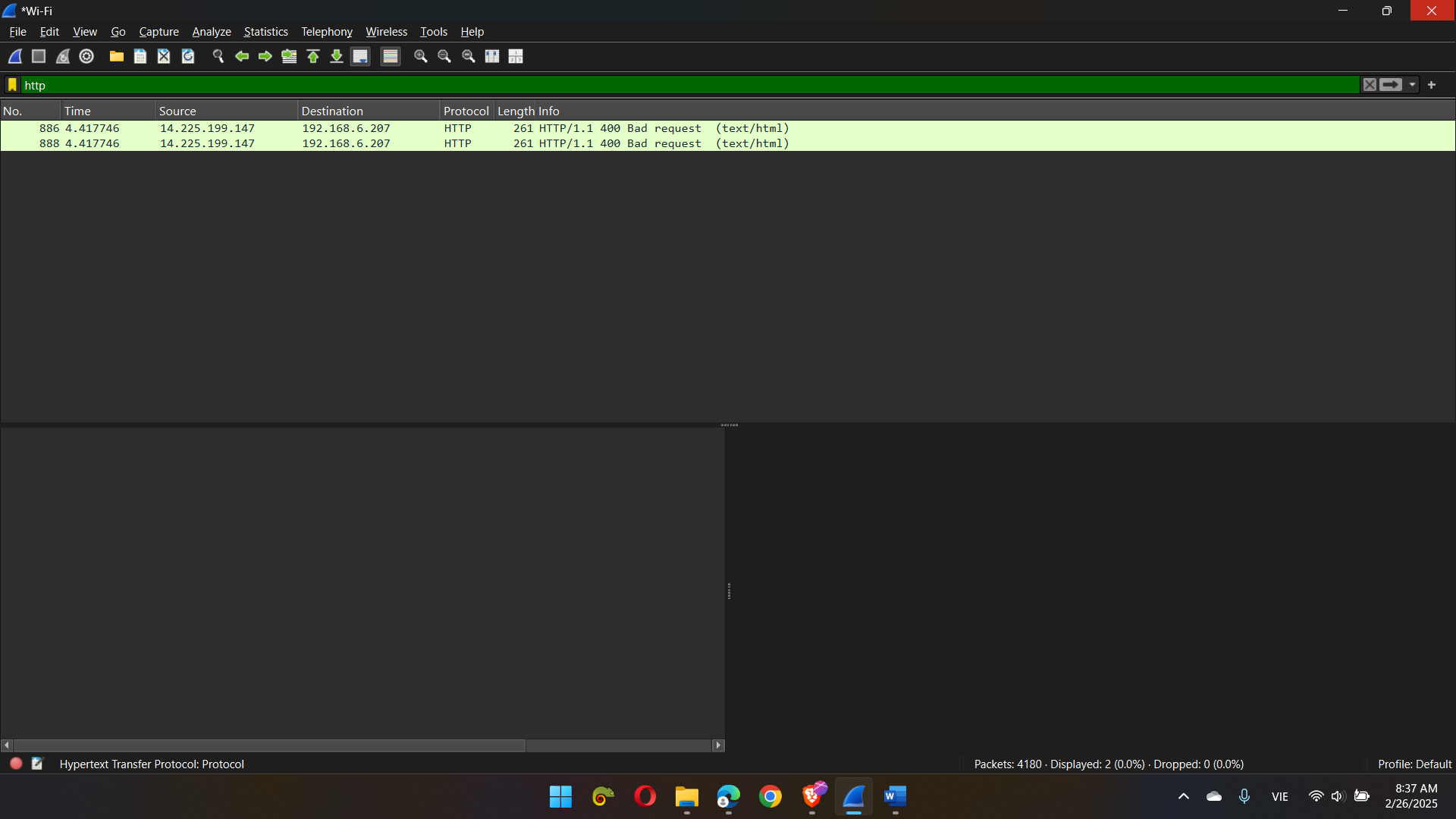


Bước 4: Dừng bắt gói tin và tìm http



Bước 5: thử lại với website của trường:

<https://daotao.hcmunre.edu.vn/sinhvien/tracuu/hocphi>



* 1. 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?

Web gaia: 11.924325

Web trường: 16.482287

* + 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.

 **STUN (Session Traversal Utilities for NAT)**: Giao thức này giúp các thiết bị đằng sau bộ định tuyến NAT hoặc tường lửa xác định địa chỉ IP công cộng và cổng được liên kết của chúng. Điều này rất hữu ích trong các ứng dụng truyền thông thời gian thực như VoIP, nơi các thiết bị cần biết cách chúng được nhìn thấy từ mạng bên ngoài.

 **TCP (Transmission Control Protocol)**: TCP là một giao thức truyền tải hướng kết nối, đảm bảo việc truyền dữ liệu đáng tin cậy giữa các thiết bị trên mạng. Nó chia dữ liệu thành các gói nhỏ, gửi chúng đi, và đảm bảo rằng tất cả các gói được nhận và sắp xếp đúng thứ tự tại đích.

 **RTCP (RTP Control Protocol)**: RTCP hoạt động cùng với RTP (Real-time Transport Protocol) để giám sát chất lượng dịch vụ và truyền thông trong các ứng dụng truyền thông thời gian thực. Nó cung cấp thông tin phản hồi về hiệu suất truyền tải, giúp điều chỉnh các tham số để duy trì chất lượng truyền thông.

 **UDP (User Datagram Protocol)**: UDP là một giao thức truyền tải không kết nối, cho phép truyền dữ liệu nhanh chóng mà không cần thiết lập kết nối trước. Mặc dù không đảm bảo việc truyền dữ liệu đáng tin cậy như TCP, nhưng nó hữu ích trong các ứng dụng yêu cầu tốc độ cao và có thể chấp nhận mất mát dữ liệu, như streaming video hoặc game trực tuyến.

 **TLSv1.2 (Transport Layer Security version 1.2)**: TLSv1.2 là một phiên bản của giao thức bảo mật TLS, cung cấp mã hóa và bảo mật cho dữ liệu truyền tải giữa các ứng dụng trên mạng. Nó đảm bảo rằng dữ liệu không bị đọc trộm hoặc giả mạo trong quá trình truyền, và thường được sử dụng trong các giao dịch web an toàn như ngân hàng trực tuyến và mua sắm trực tuyến.

* 1. 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).

7.688468 - 7.429019 = 0.259449

* 1. Nội dung có nằm trong các gói tinh bắt được và nằm ở gói tin 200 OK

Địa chỉ IP của web gaia: 128.119.245.12

Địa chỉ IP của web trường: 14.225.199.147

Địa chỉ IP chính của máy đang kết nối Internet là **192.168.6.207**.

* 1. DNS Query -> TCP Handshake -> TLS Handshake (nếu là HTTPS) -> Gửi HTTP Request -> Nhận HTTP Response -> Hiển thị trang web