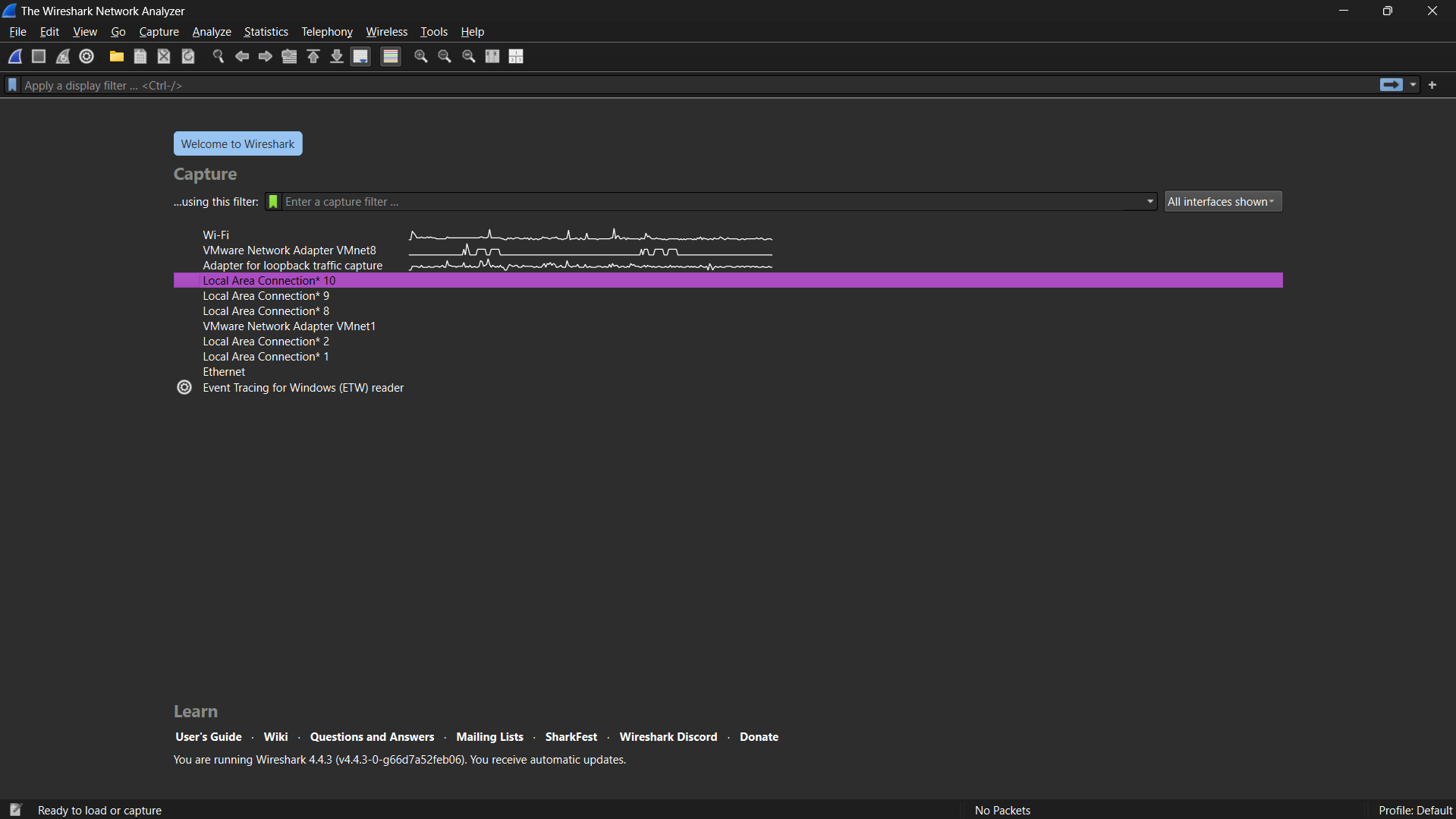
# Bài tập thực hành LAB 1 Bảo mật mạng máy tính và hệ thống

## 1.Task 1: Mở đầu về mạng máy tính

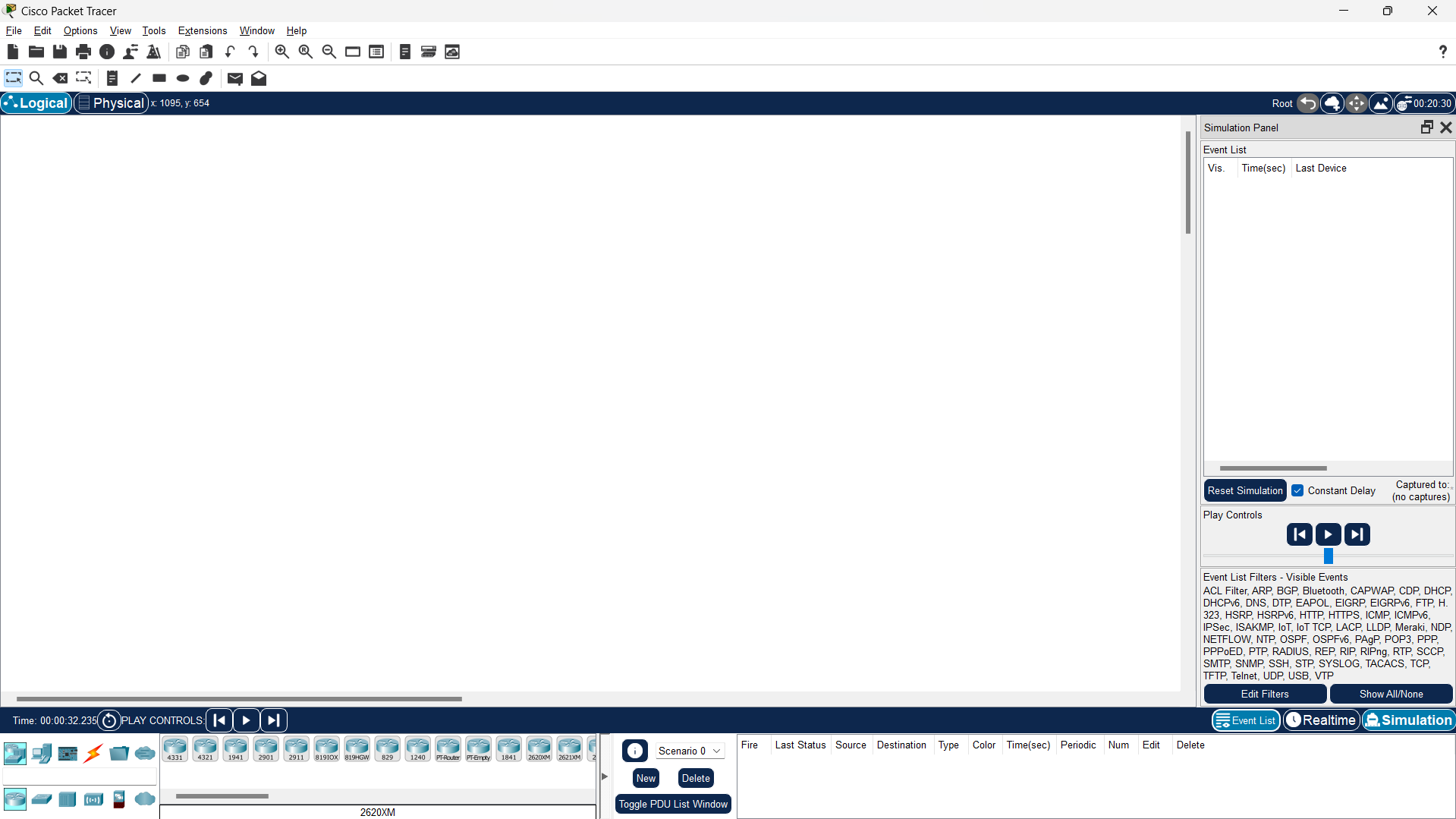
 Trước khi bắt đầu thực hành, sinh viên hãy trả lời các câu hỏi sau:

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

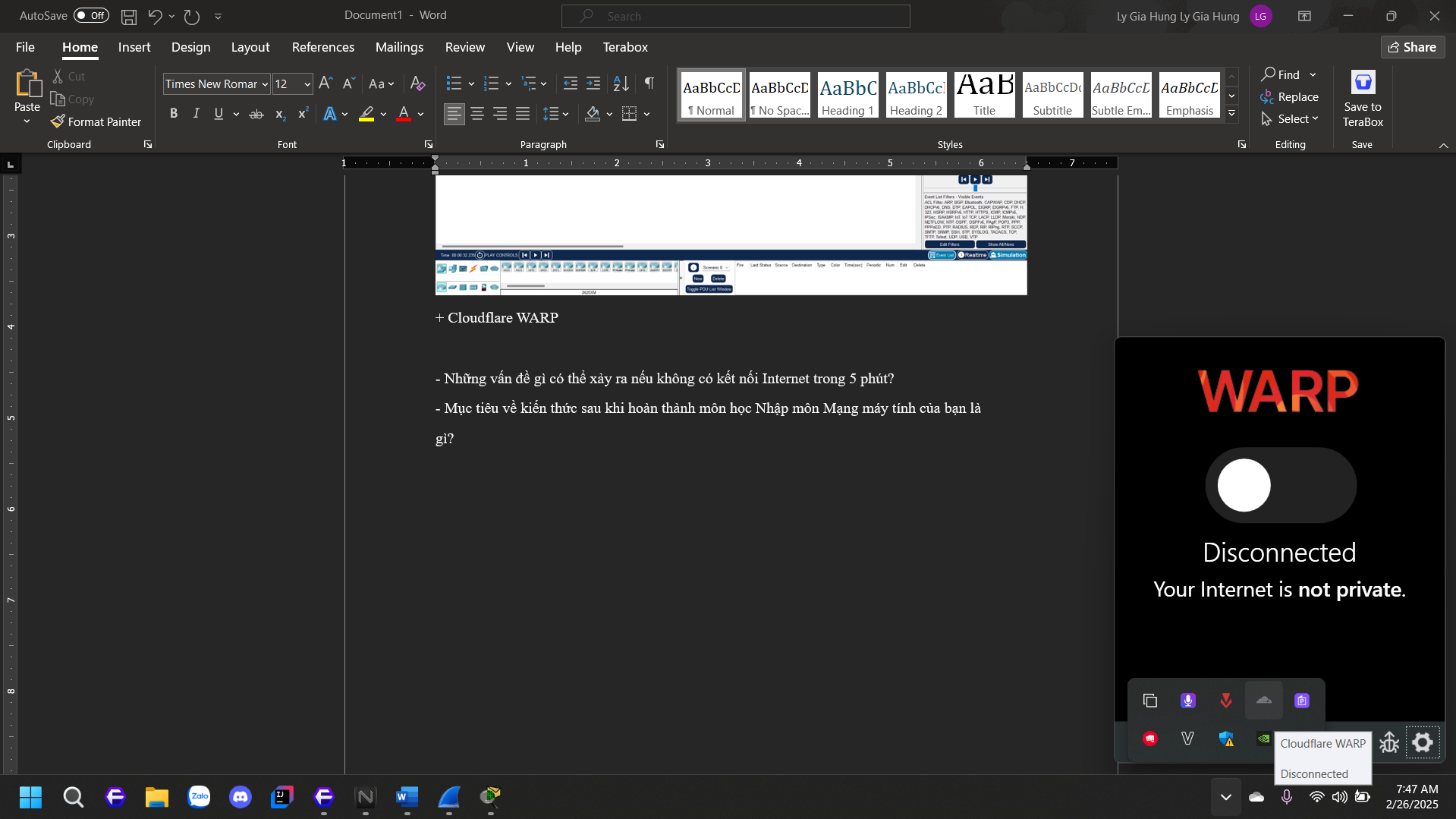
họa).

+ Wireshark

+ Cisco packet tracer



+ Cloudflare WARP



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

+ Mất kết nối với các công cụ làm việc trực tuyến, ngắt kết nối giao tiếp online, gián đoạn các giao dịch tài chính,…..

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

gì?

+ Có thêm kiến thức về bảo mật an ninh mạng và hệ thống, tránh bị tấn công ở mức tối thiểu nhất.

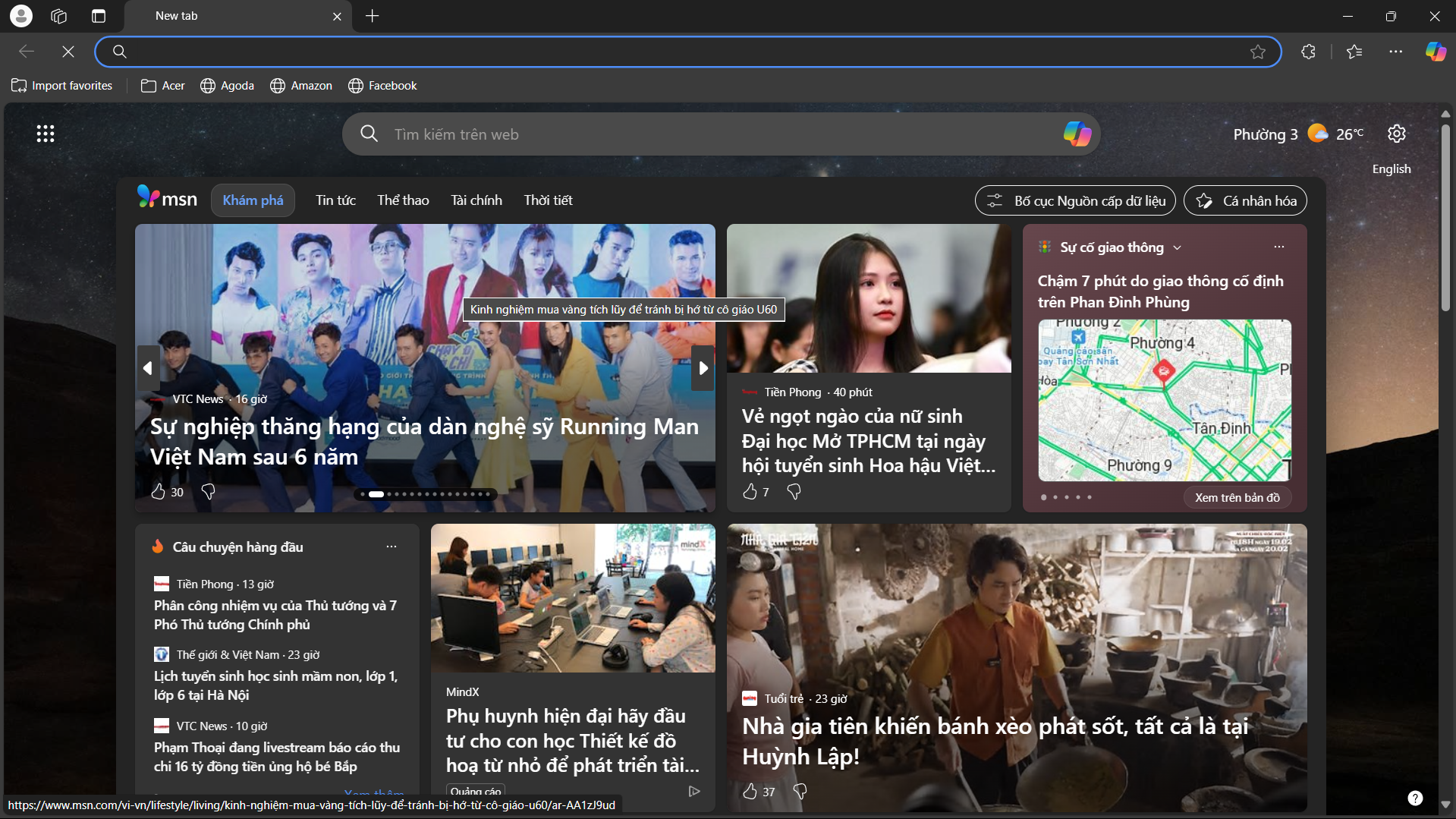
## 2.Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng.

### 2.1.Thử nghiệm bắt gói tin với Wireshark

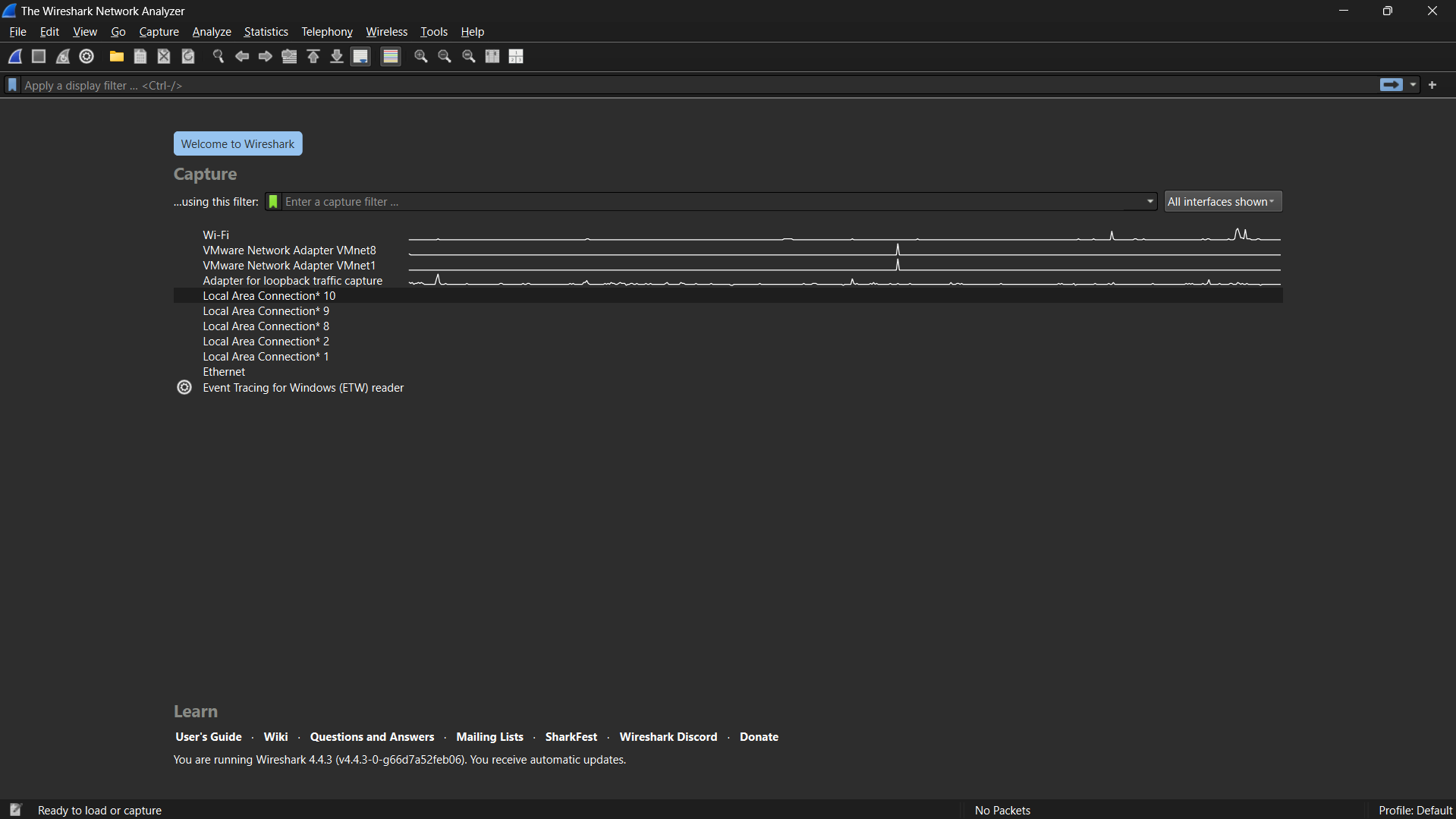
- Bước 1: Khởi động trình duyệt web bất kỳ như Google Chrome, Firefox, Edge,...

và phần mềm Wireshark (phiên bản mới nhất)

- Trình duyệt Edge.



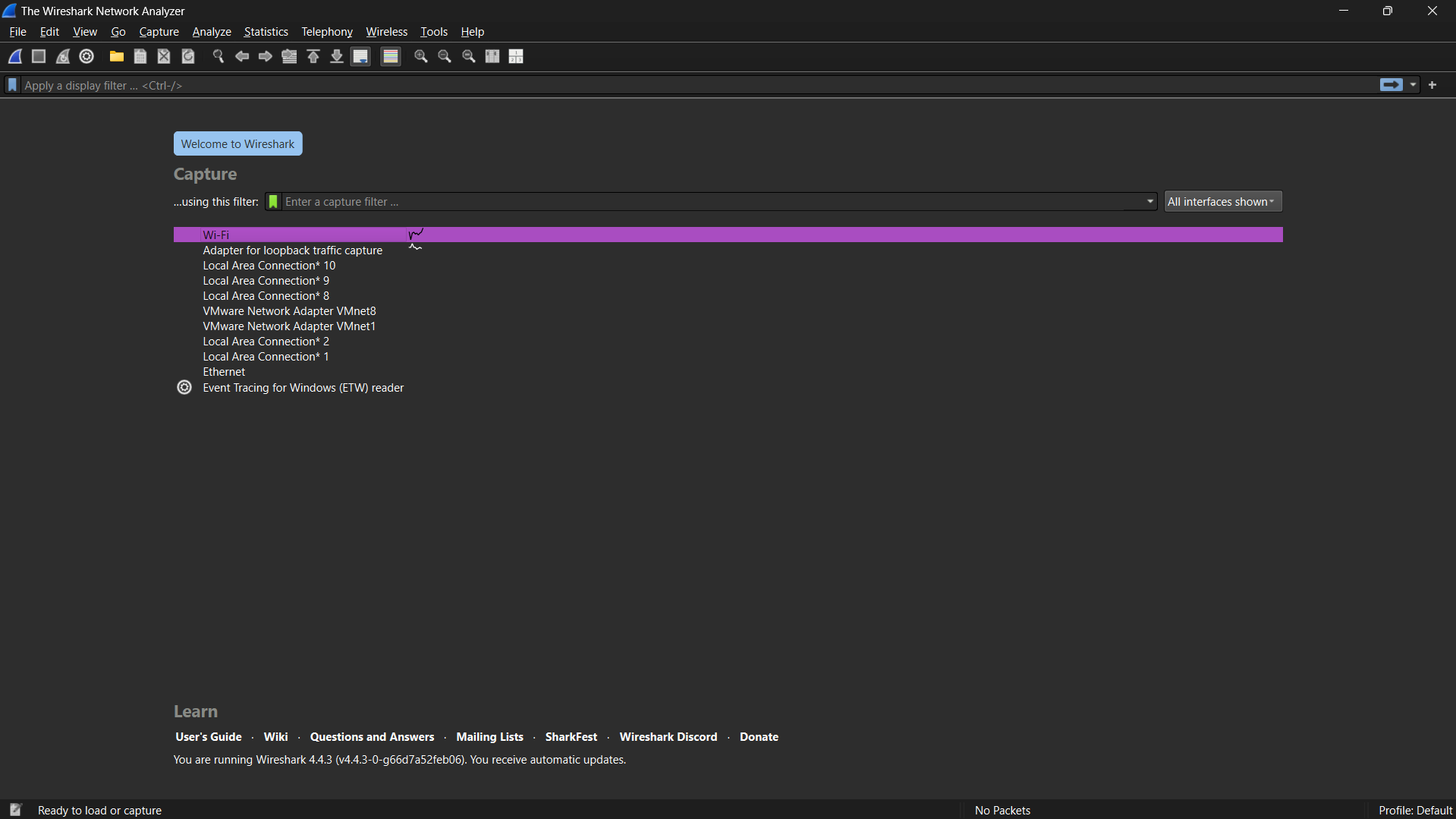
- Wireshark



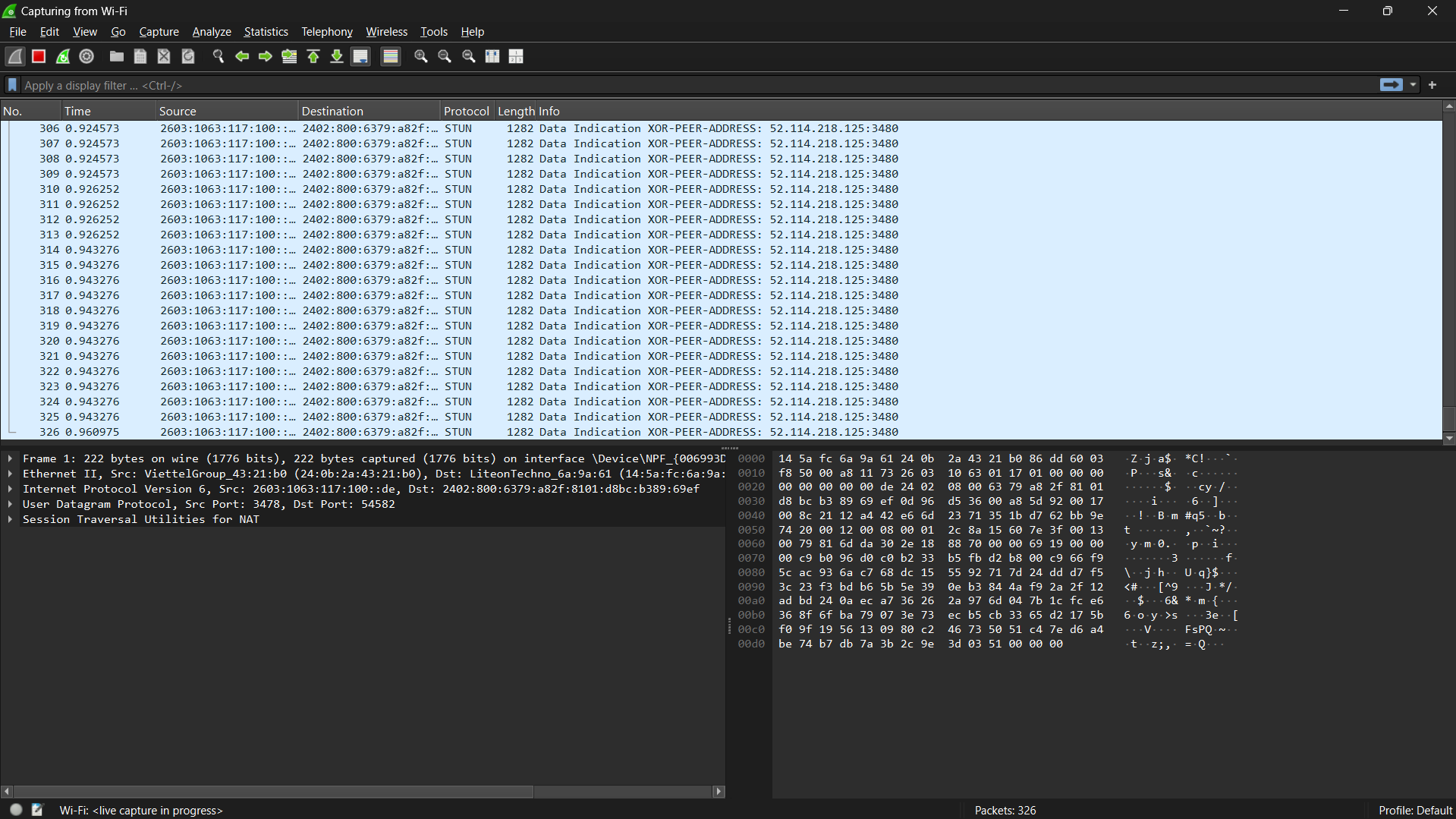
- Bước 2: Tại phần Capture, chọn interface đang hoạt động chính trên máy để bắt

đầu bắt gói tin.

- Dùng wifi chọn interface wifi

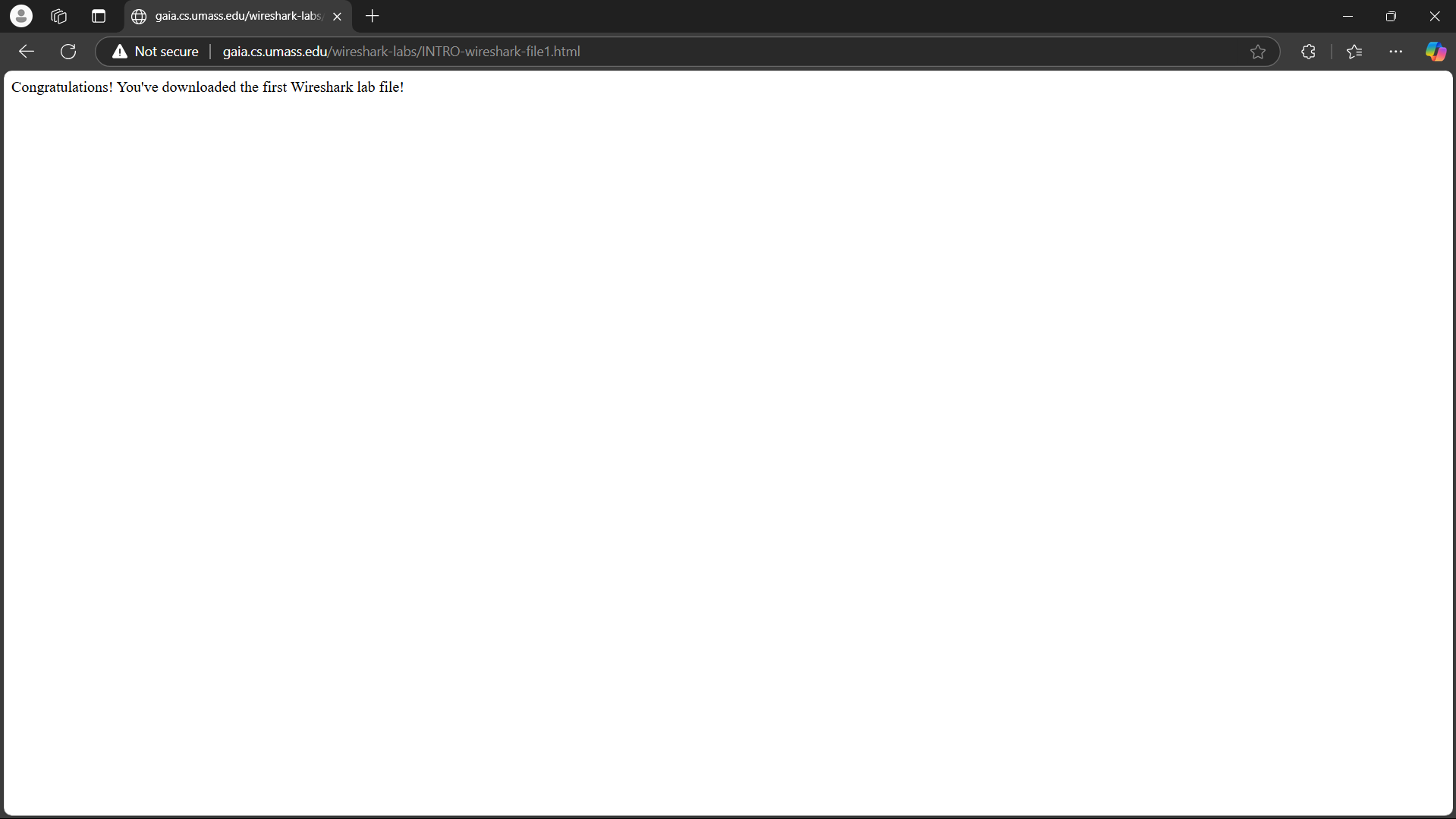


- Sau khi chọn



- Bước 3: Mở trình duyệt web và chỉ truy cập vào website có địa chỉ như sau

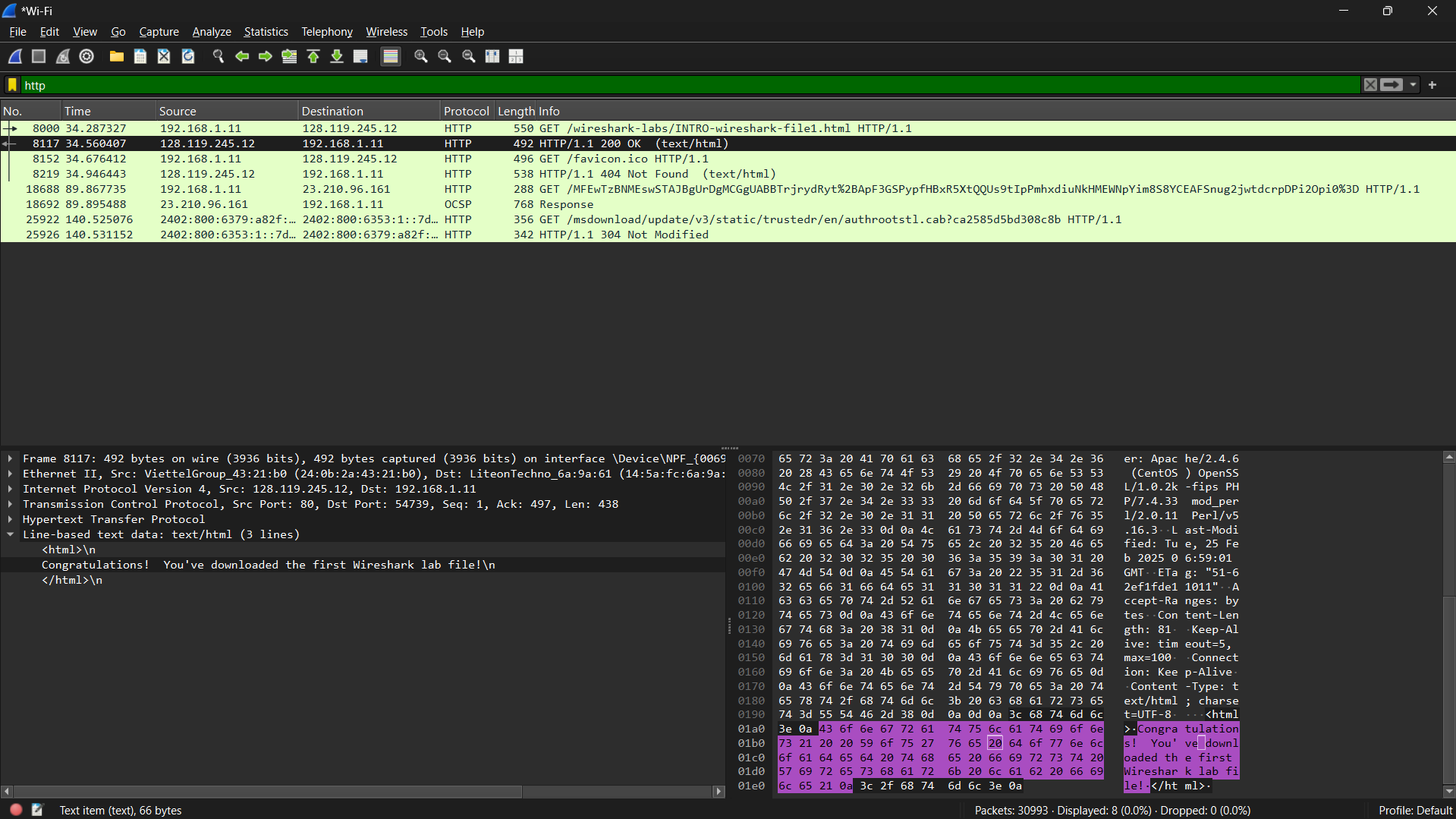
<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>



- Bước 4: Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là

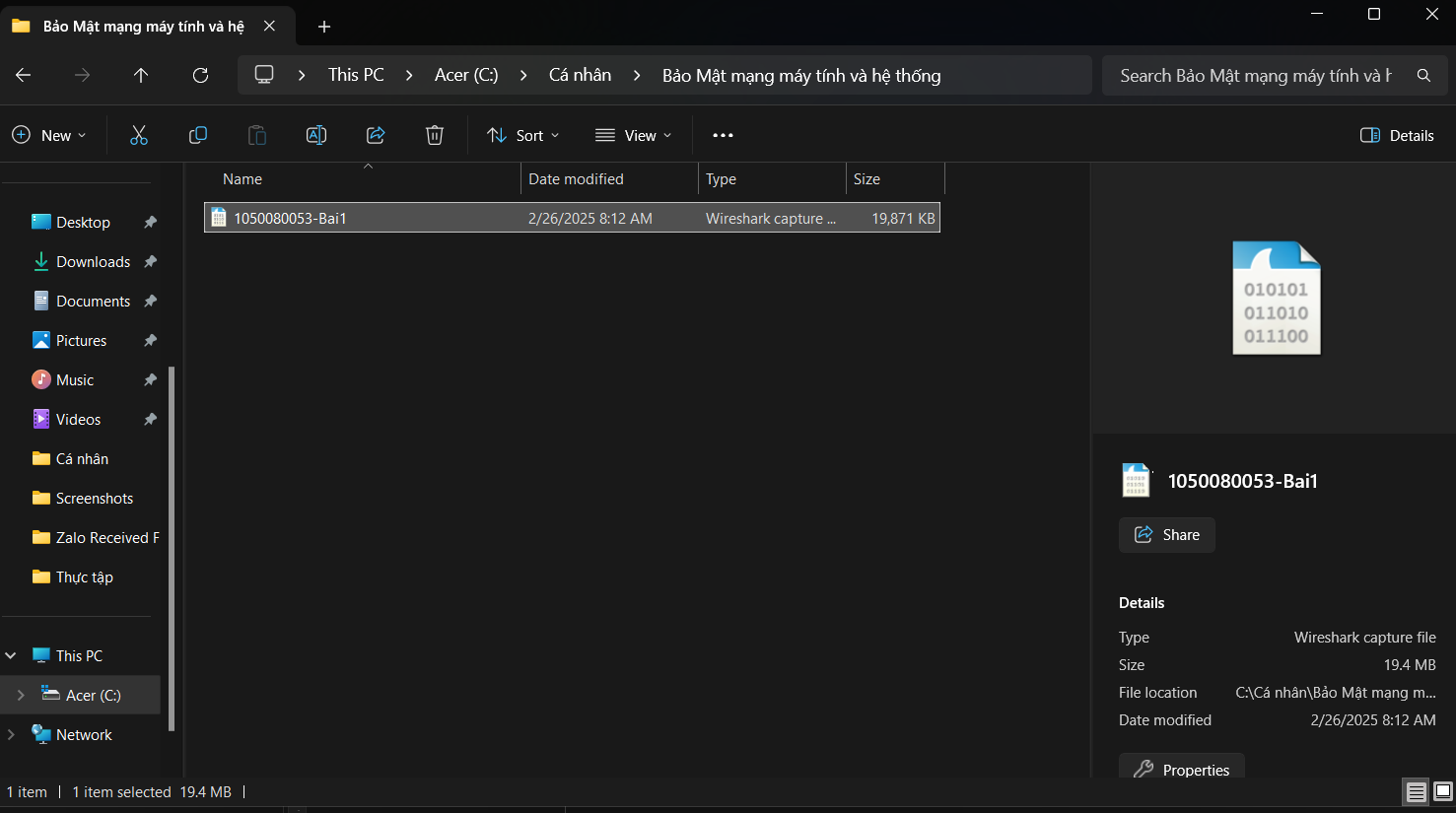
một dòng chào mừng đơn giản), dừng bắt gói tin tại Wireshark.

- Ta thu được kết quả



- Bước 5: Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng

MSSV-Bai1.pcapng. Ví dụ: 1050080053-Bai1.pcapng.



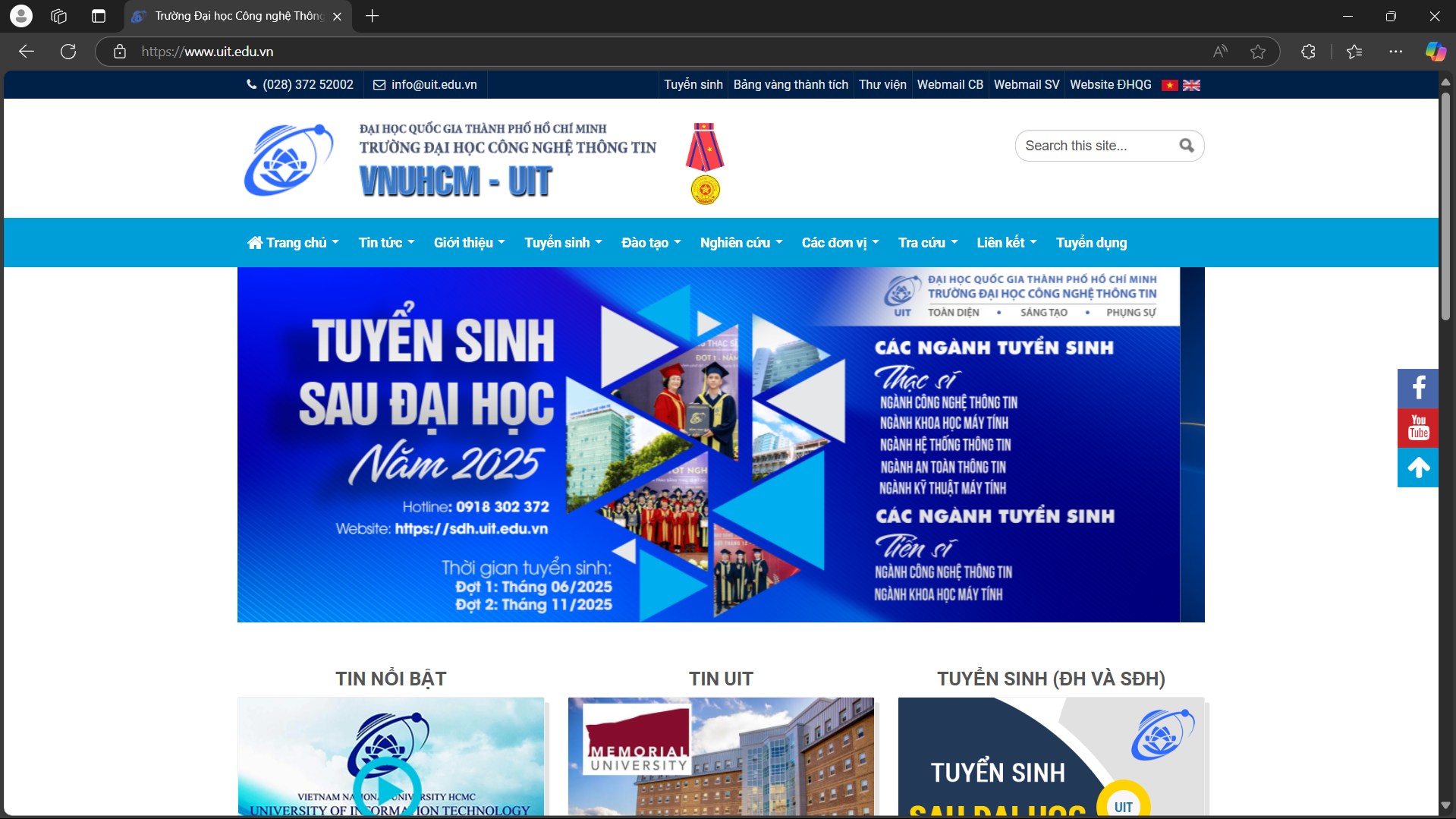
- Bước 6: Chọn 1 website mà sinh viên thường hay truy cập, ví dụ uit.edu.vn,

tinhte.vn,... và tiến hành bắt gói tin trên website đó

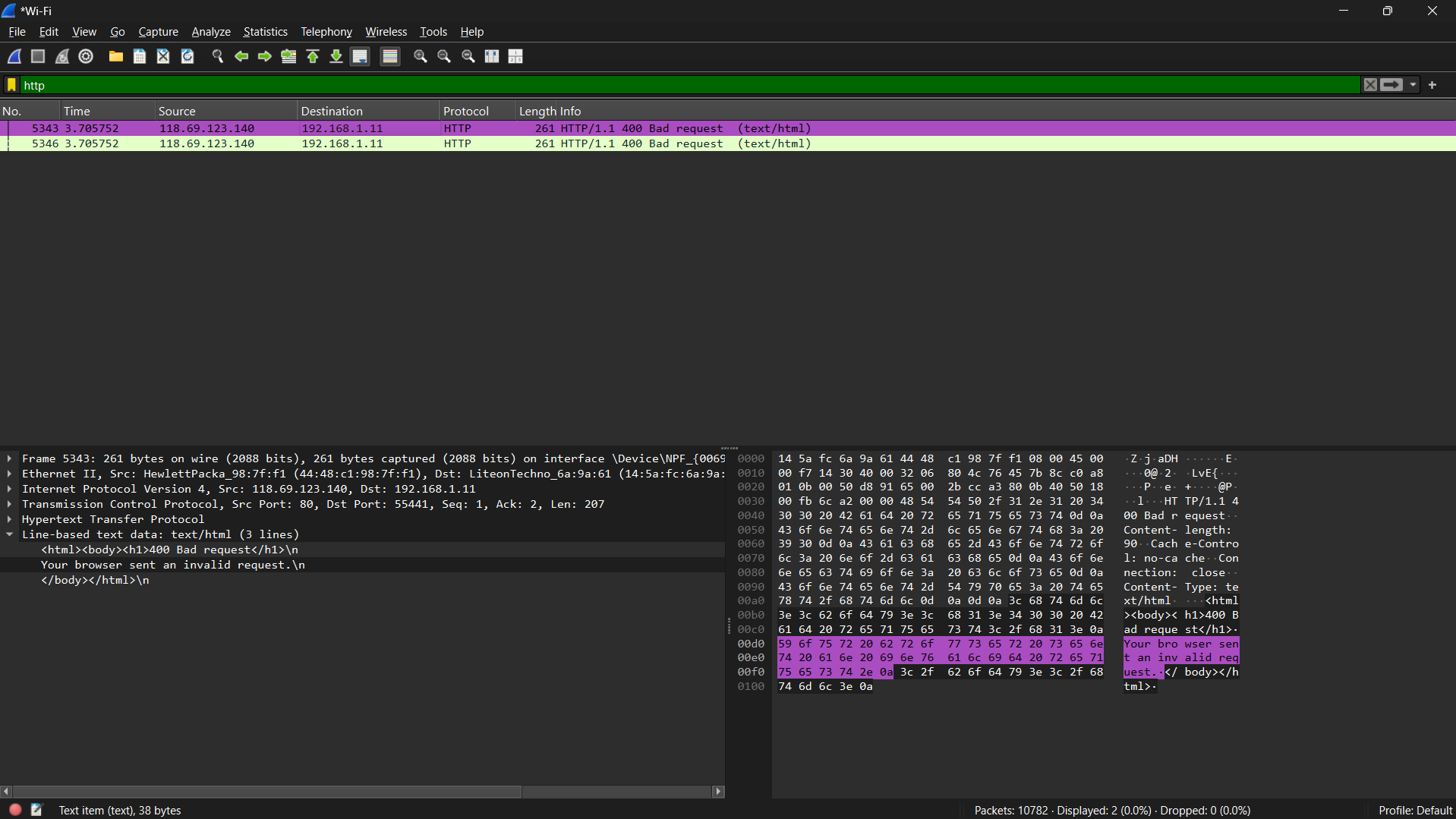
Lặp lại các bước 3-4-5 với một website khác có chứa nhiều thông tin hơn mà

sinh viên thường truy cập. Ví dụ: tuoitre.vn, uit.edu.vn,...

- Trang web : uit.edu.vn

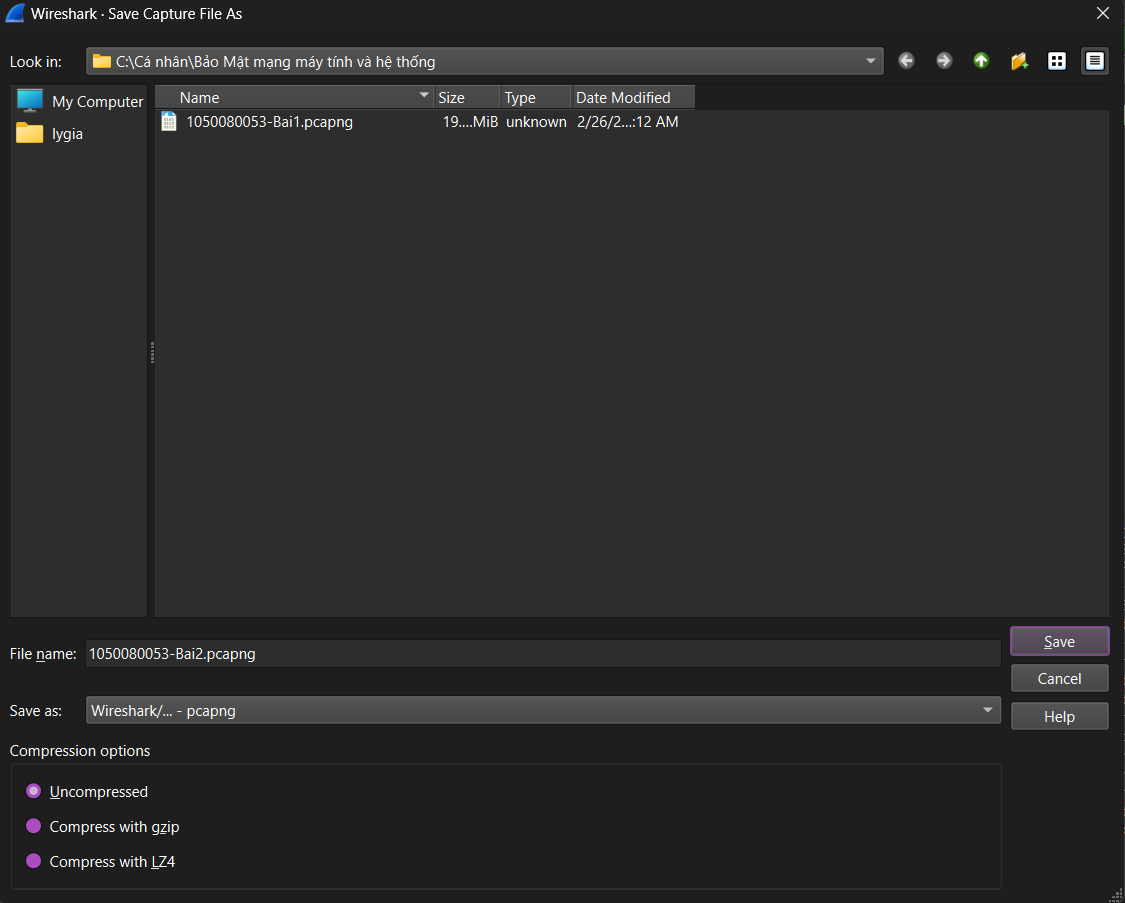


- Wireshark:



- Bước 7: Lưu lại tập tin sau khi bắt được ở website thứ 2 thành file pcapng có tên

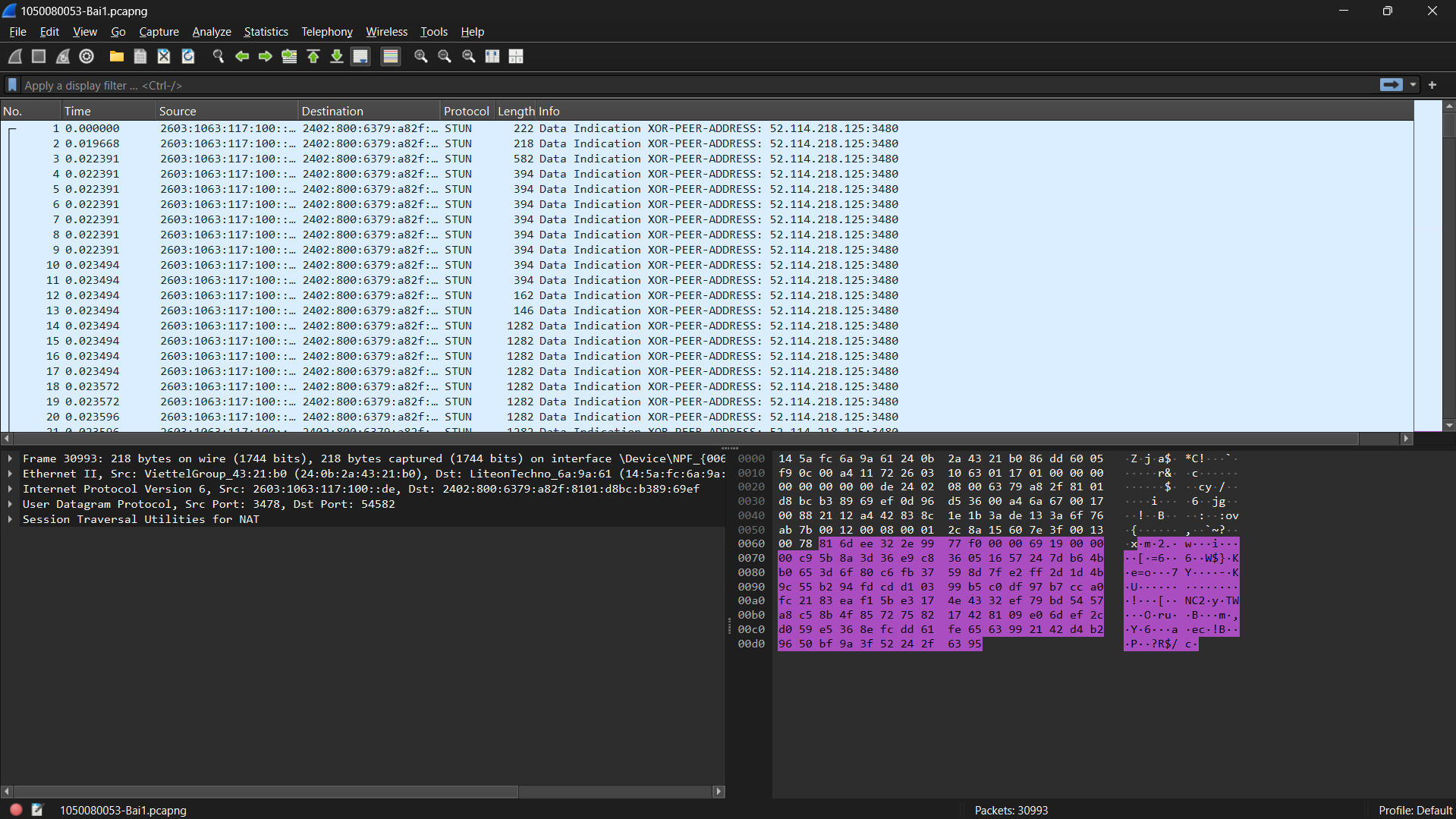
dạng MSSV-Bai2.pcapng



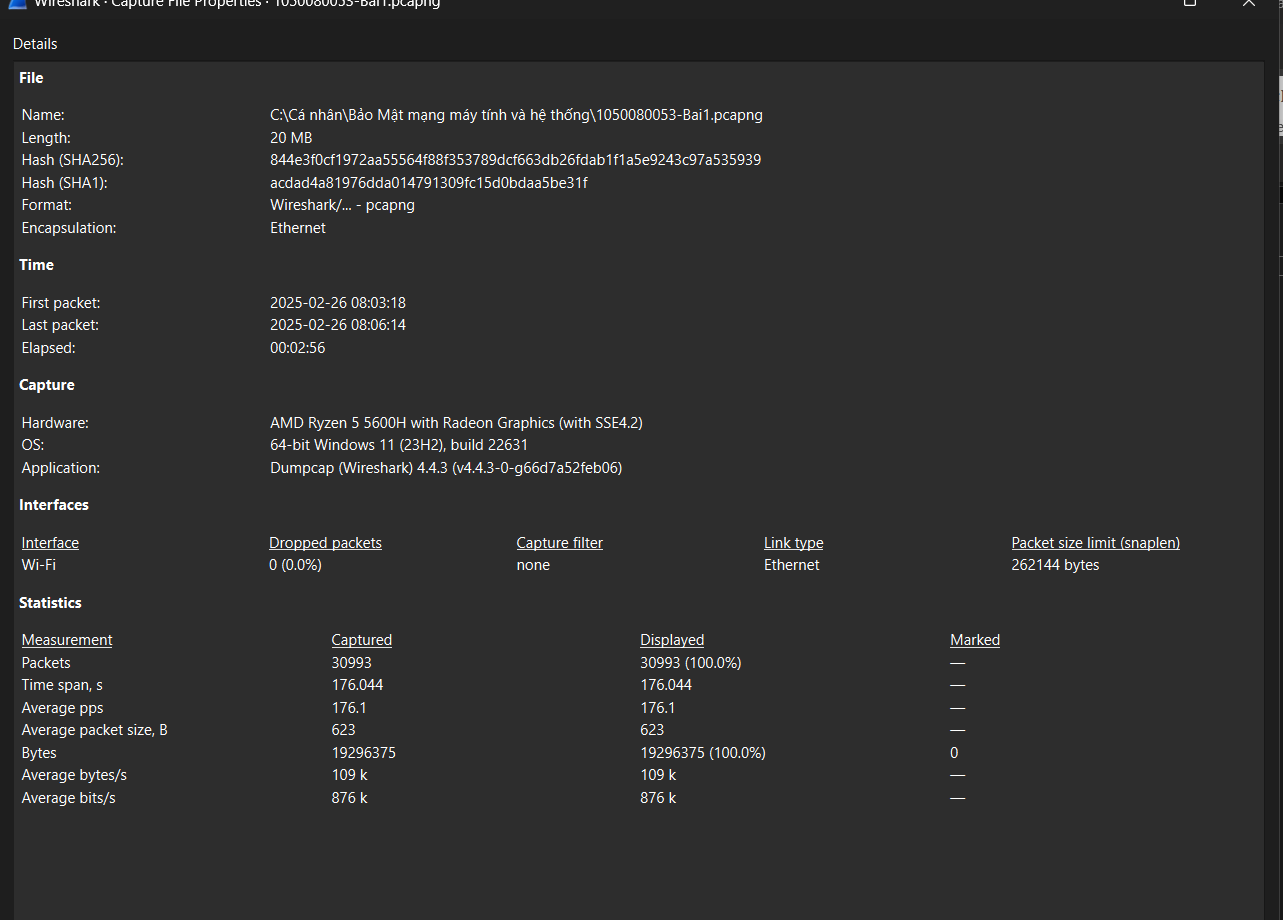
### 2.2.Phân tích kết quả bắt gói tin từ Wireshark

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

- Mở file 1050080053-Bai1.pcapng



- Trên thanh menu chọn Statistics 🡪 Capture file properties để biết thông tin.



- Ở đây thời gian thực hiện bắt gói tin là 176,044 giây với tổng gói tin bắt được là 30993 gói.

#### 2.2.2. 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.

- Tổng 5 giao thức là: RTCP, TCP, TLSv1.2, ARP, IGMPv2

- Chức năng chính:

+ RTCP (RTP Control Protocol): Hỗ trợ giám sát chất lượng truyền tải trong RTP (Real-time Transport Protocol), dùng trong truyền âm thanh, video (VoIP, streaming).

+ TCP (Transmission Control Protocol): Giao thức kết nối tin cậy, đảm bảo dữ liệu được gửi đầy đủ, đúng thứ tự và không bị mất (dùng trong HTTP, FTP, email).

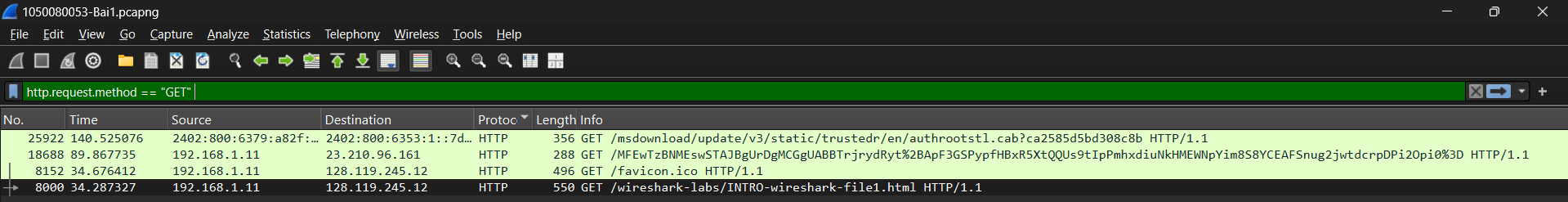
+ TLSv1.2 (Transport Layer Security v1.2): Giao thức mã hóa bảo mật dữ liệu trên Internet, dùng trong HTTPS, VPN để bảo vệ thông tin tránh bị đánh cắp.

+ ARP (Address Resolution Protocol): Dùng để tìm địa chỉ MAC của thiết bị trong mạng dựa trên địa chỉ IP, giúp các thiết bị giao tiếp với nhau trong mạng LAN.

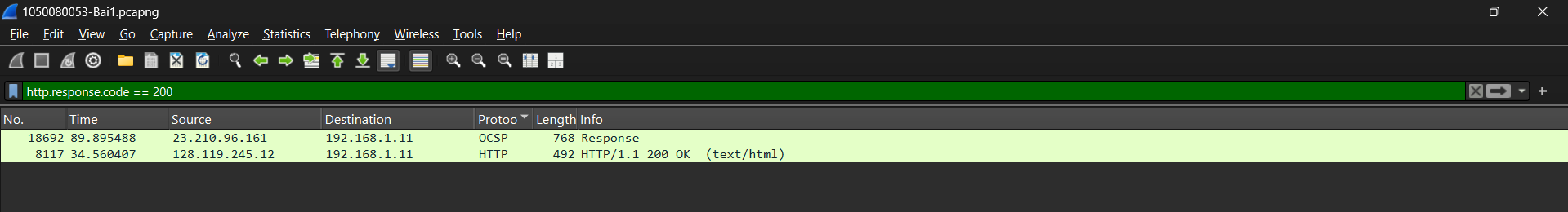
+ IGMPv2 (Internet Group Management Protocol v2): Hỗ trợ quản lý nhóm multicast trong mạng IPv4, giúp thiết bị tham gia hoặc rời khỏi nhóm multicast (dùng trong IPTV, phát sóng trực tuyến).

#### 2.2.3. 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).

- Lọc gói tin http.request.method == "GET" ta thu được như sau:



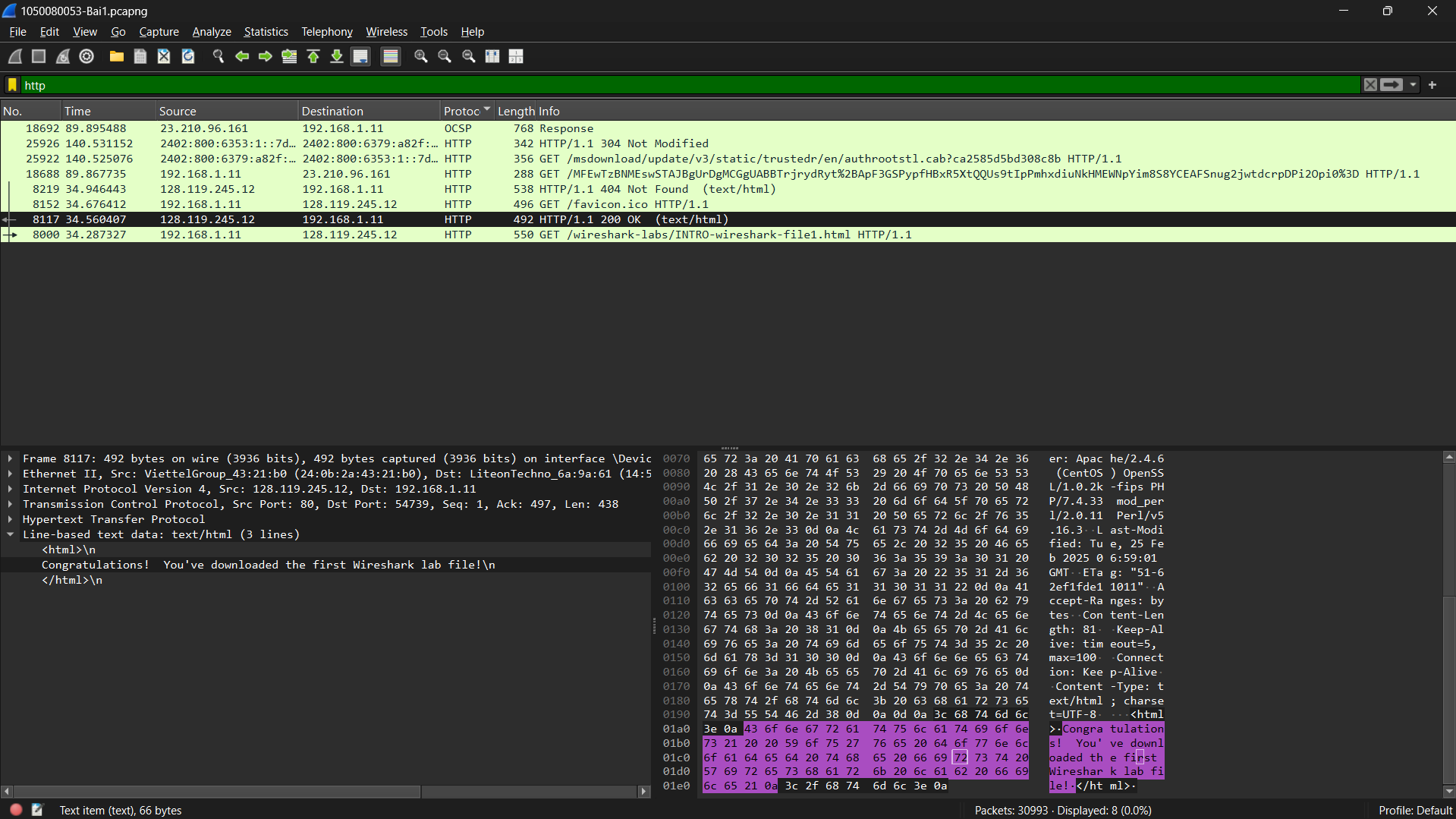
- Có thời gian là: 34.287327 giây. Kế tiếp lọc gói tin http.response.code == 200



- Có thời gian là: 34.560407 giây. Vậy thời gian mất đi là 0.27308 giây.

#### 2.2.4. 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.

- Có thu được đoạn “Congratulations! You've downloaded the first Wireshark lab file!” nằm ở góc dưới bên phải



#### 2.2.5. 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 là: 128.119.245.12

#### 2.2.6. 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. Diễn biến khi truy cập một trang web (dựa trên bắt gói tin Wireshark)

Khi bạn nhập URL vào trình duyệt và nhấn Enter, quá trình diễn ra như sau:

1.Tra cứu DNS (DNS Lookup)

+ Trình duyệt cần biết địa chỉ IP của website (vì URL là dạng chữ).

+ Máy gửi gói tin DNS Query đến máy chủ DNS để lấy địa chỉ IP của trang web.

+ Máy chủ DNS phản hồi với DNS Response, chứa địa chỉ IP của website.

2.Thiết lập kết nối TCP (TCP Handshake)

+ Máy khách (client) mở kết nối đến địa chỉ IP server bằng giao thức TCP.

- Quá trình bắt tay 3 bước (Three-way Handshake) diễn ra:

+ Client → Server: Gửi SYN (yêu cầu kết nối).

+ Server → Client: Phản hồi SYN-ACK.

+ Client → Server: Gửi ACK, hoàn tất kết nối.

3️.Thiết lập bảo mật TLS (nếu HTTPS, TLS Handshake)

+ Nếu trang web sử dụng HTTPS, client và server tiến hành TLS Handshake để thiết lập kết nối an toàn.

+ Quá trình này gồm việc trao đổi chứng chỉ SSL/TLS và mã hóa dữ liệu.

4️.Gửi yêu cầu HTTP (HTTP Request)

+ Sau khi kết nối xong, client gửi HTTP GET Request đến server để yêu cầu nội dung trang web.

+ Gói tin có thể chứa cookies, user-agent, headers, v.v.

5️.Nhận phản hồi từ server (HTTP Response)

+ Server xử lý request và phản hồi bằng HTTP 200 OK kèm theo dữ liệu trang web (HTML, CSS, JS, hình ảnh,...).

+ Nếu tài nguyên không tồn tại, server có thể trả về HTTP 404 Not Found.

6️.Hiển thị trang web

+ Trình duyệt nhận dữ liệu, render nội dung trang web.

+ Nếu trang có ảnh, CSS, JS, trình duyệt tiếp tục gửi các request bổ sung để tải thêm tài nguyên.