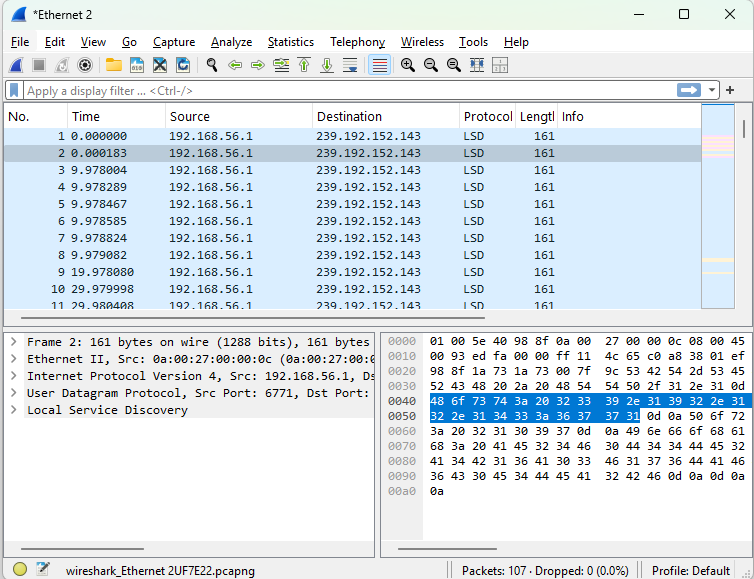
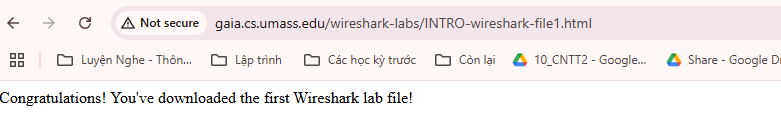
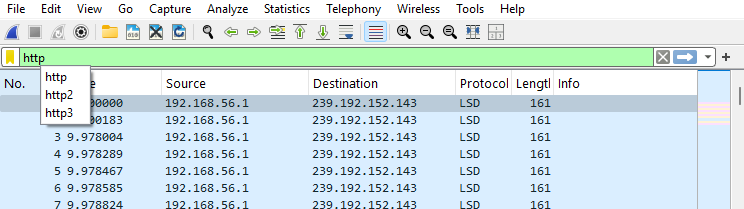
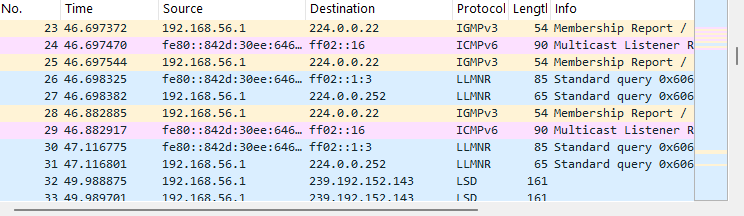
**Họ và tên : Trần Kim Thiện**

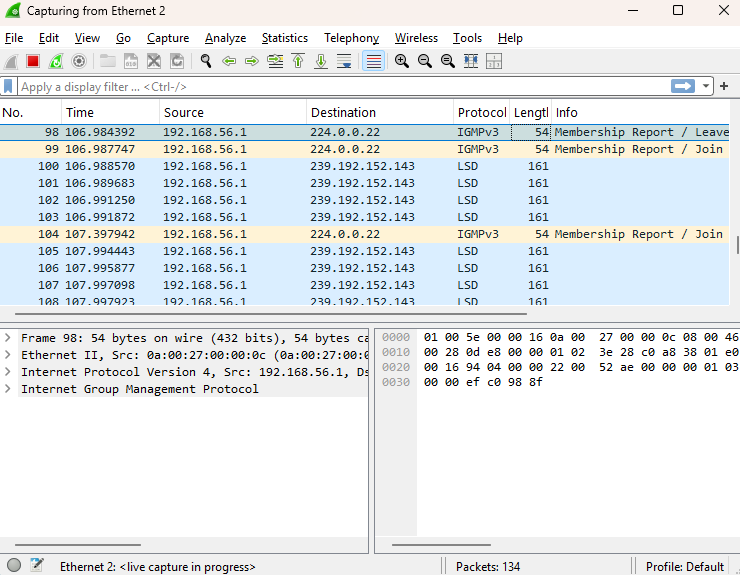
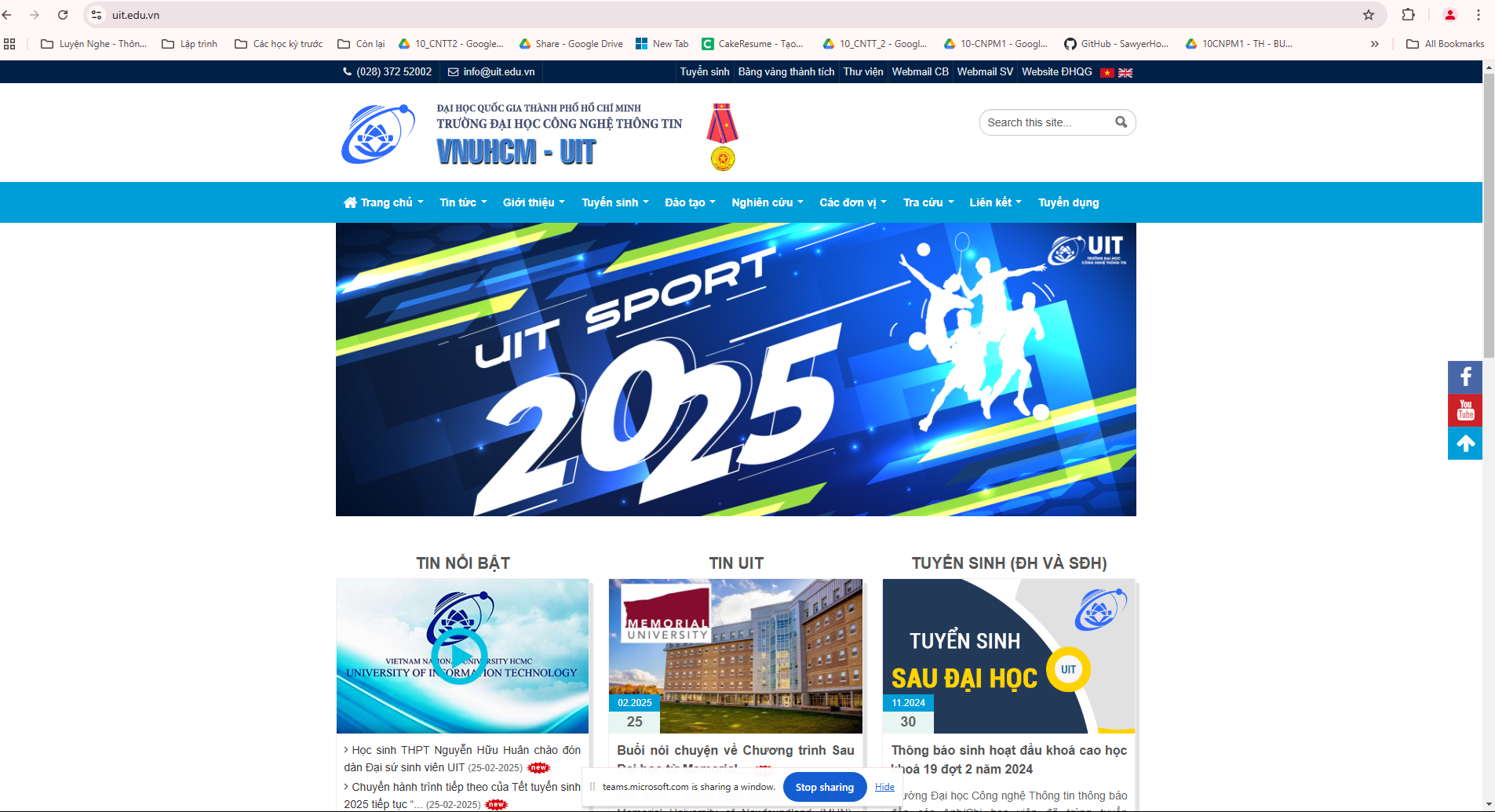
**MSSV : 1050080076**

**Lớp : 10\_ĐH\_CNPM 1**

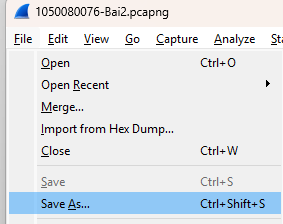


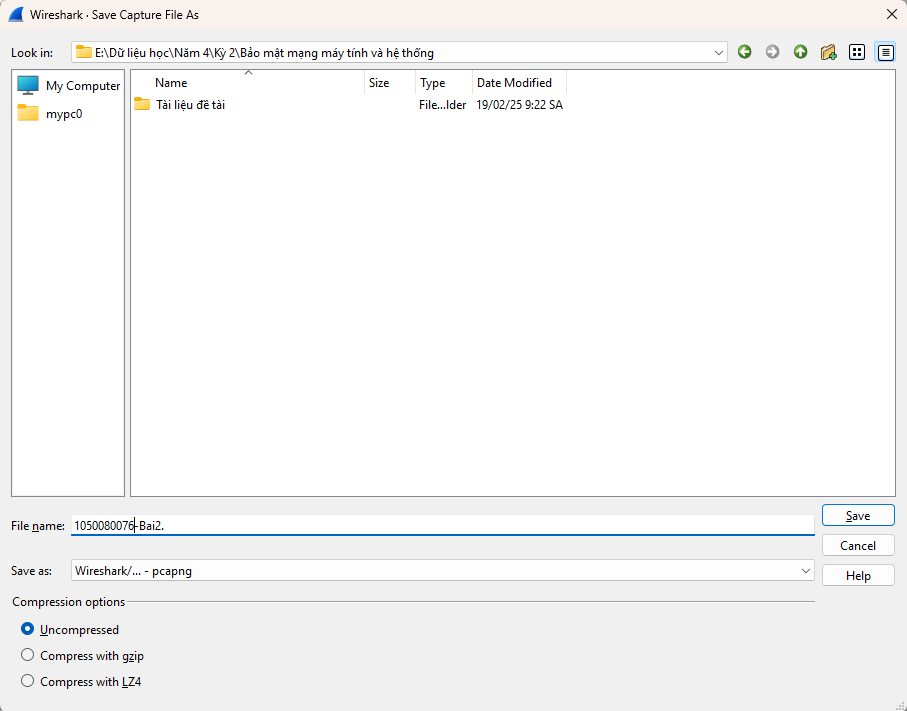


Chọn 1 website mà sinh viên thường hay truy cập, ví dụ uit.edu.vn,  
tinhte.vn,… và tiến hành bắt gói tin trên website đó



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

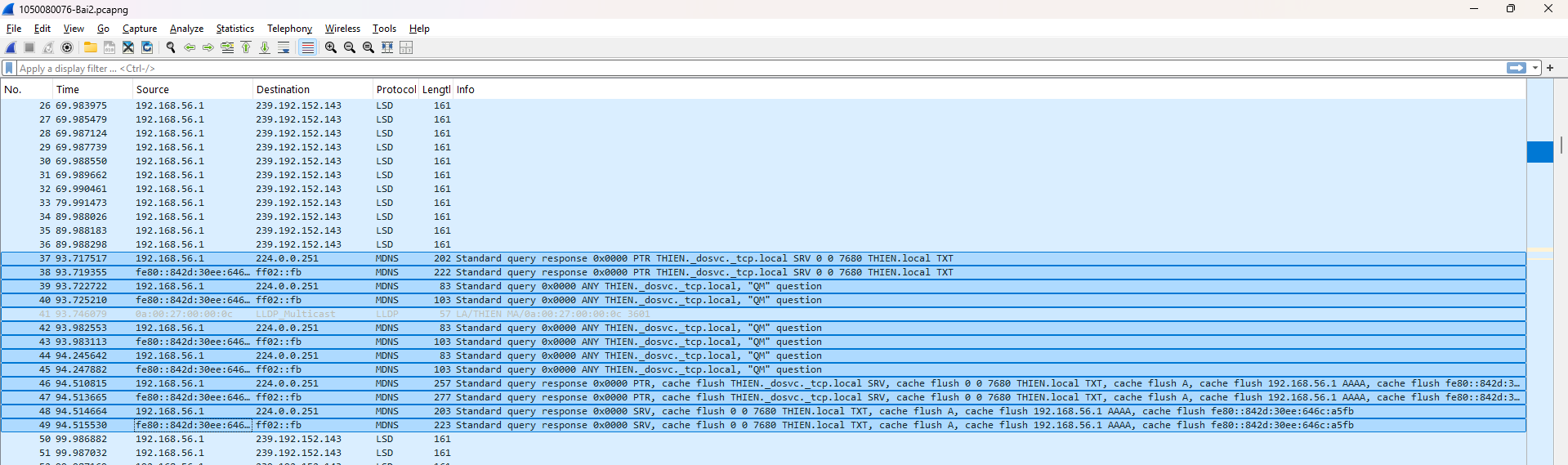




Phân tích kết quả bắt gói tin từ Wireshark :

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

Tổng thời gian bắt gói tin là 13 giây trên 50 giây tổng số gói tin bắt được

  
**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**

Bao gồm

**DNS (Domain Name System)**

Chức năng: Dịch tên miền (ví dụ: google.com) thành địa chỉ IP tương ứng để trình duyệt có thể kết nối với máy chủ web.

Ứng dụng: Hỗ trợ truy cập website bằng tên miền thay vì địa chỉ IP.

**TCP (Transmission Control Protocol)**

Chức năng: Giao thức điều khiển truyền vận, đảm bảo dữ liệu được gửi đến đúng địa chỉ và theo đúng thứ tự.

Ứng dụng: Gửi dữ liệu đáng tin cậy trên Internet như tải file, gửi email, duyệt web.

**ARP (Address Resolution Protocol)**

Chức năng: Chuyển đổi địa chỉ IP thành địa chỉ MAC trong mạng cục bộ (LAN).

Ứng dụng: Cho phép các thiết bị trong cùng một mạng giao tiếp với nhau bằng cách tìm địa chỉ phần cứng của nhau.

**LSD**

Có thể ám chỉ đến “Link State Database” trong các giao thức định tuyến trạng thái liên kết (ví dụ: OSPF). Trong trường hợp này, LSD là cơ sở dữ liệu lưu trữ thông tin về trạng thái của các liên kết và các router trong mạng, hỗ trợ quá trình tính toán đường đi tối ưu theo thuật toán Dijkstra.

Ngoài ra, trong một số bối cảnh khác, “LSD” cũng có thể được hiểu là “Local Service Discovery”, một chuẩn cho phép các thiết bị trong cùng một mạng tự động phát hiện và công bố các dịch vụ mà chúng cung cấp mà không cần cấu hình thủ công.

**IGMP v3 (Internet Group Management Protocol version 3)**

Là phiên bản thứ ba của giao thức IGMP, được sử dụng để quản lý các thành viên của nhóm multicast trên mạng IP.

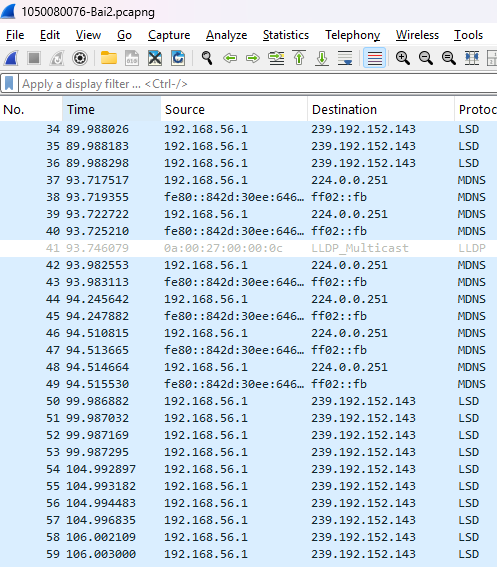
IGMP v3 cải tiến so với các phiên bản trước bằng cách hỗ trợ lọc nguồn, cho phép các host chỉ nhận dữ liệu từ những nguồn multicast cụ thể, giúp tối ưu hóa băng thông và nâng cao bảo mật cho các ứng dụng multicast.

**MDSN**

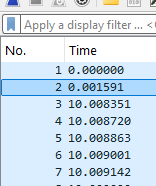
Có khả năng là một chuẩn liên quan đến phân phối multicast trong các môi trường mạng phức tạp, giúp quản lý và điều phối việc gửi dữ liệu multicast qua các domain hoặc subnet khác nhau.

Một khả năng khác là đây có thể là nhầm lẫn với “mDNS” (Multicast DNS), giao thức cho phép phân giải tên máy chủ trong mạng cục bộ mà không cần máy chủ DNS trung tâm, thường được sử dụng trong các mạng nhỏ như gia đình hoặc văn phòng nhỏ.

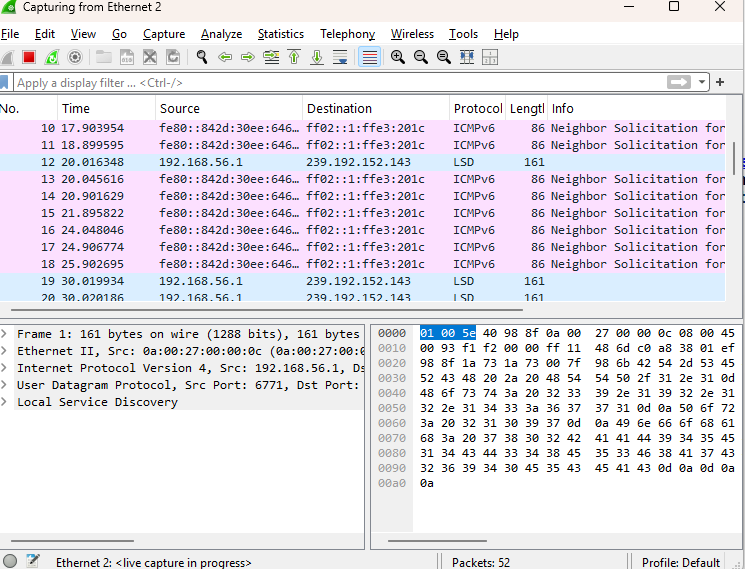
Nếu MDSN được định nghĩa khác, cần xác nhận thêm từ nguồn tài liệu chuyên ngành để có mô tả chính xác.



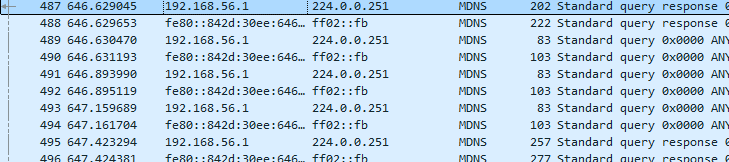
**3. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200  
OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị  
của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính  
bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).**



**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?**



**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 (Phân tích qua Wireshark)**

Khi bạn nhập một URL vào trình duyệt và nhấn **Enter**, quá trình tải trang web sẽ trải qua các bước chính sau:

**Gửi yêu cầu phân giải tên miền (DNS Request)**

* Máy tính kiểm tra bộ nhớ cache DNS cục bộ. Nếu không có, nó gửi một **gói DNS request** đến máy chủ DNS để lấy địa chỉ IP của trang web.
* Máy chủ DNS phản hồi với **gói DNS response**, cung cấp địa chỉ IP của máy chủ web.

**Gói tin trong Wireshark**:

* Giao thức: **DNS**
* Gói tin chính: **Standard Query (A record) → Standard Query Response**

**Thiết lập kết nối TCP với máy chủ web**

* Trình duyệt gửi yêu cầu **TCP 3-way handshake** để tạo kết nối với máy chủ web:
  1. **SYN**: Máy tính gửi yêu cầu mở kết nối đến máy chủ.
  2. **SYN-ACK**: Máy chủ xác nhận yêu cầu.
  3. **ACK**: Máy tính hoàn tất bắt tay, kết nối TCP được thiết lập.

**Gói tin trong Wireshark**:

* Giao thức: **TCP**
* Gói tin chính: **SYN → SYN-ACK → ACK**

**Bắt đầu giao tiếp bằng giao thức HTTPS**

* Nếu trang web sử dụng HTTPS, máy khách và máy chủ thực hiện **TLS Handshake** để mã hóa dữ liệu.
* Quá trình này bao gồm trao đổi **chứng chỉ SSL/TLS**, tạo khóa phiên để mã hóa thông tin.

**Gói tin trong Wireshark**:

* Giao thức: **TLSv1.2 / TLSv1.3**
* Gói tin chính: **Client Hello → Server Hello → Certificate Exchange**

**Gửi yêu cầu HTTP(S) để tải nội dung trang web**

* Sau khi kết nối được thiết lập, trình duyệt gửi **gói tin HTTP GET** để yêu cầu nội dung trang web.
* Máy chủ phản hồi với **gói HTTP Response (200 OK)** chứa dữ liệu HTML, CSS, JavaScript, hình ảnh,…

**Gói tin trong Wireshark**:

* Giao thức: **HTTP hoặc HTTPS**
* Gói tin chính: **GET /index.html → HTTP 200 OK**

**Trình duyệt hiển thị nội dung trang web**

* Trình duyệt tải và hiển thị các nội dung dựa trên dữ liệu nhận được.
* Nếu trang có nhiều tài nguyên (ảnh, video, script), nó sẽ gửi thêm nhiều yêu cầu GET để lấy dữ liệu bổ sung.

**Gói tin trong Wireshark**:

* Giao thức: **HTTP(S), TCP, TLS**
* Gói tin chính: **GET /style.css → 200 OK** (cho file CSS), **GET /logo.png → 200 OK** (cho hình ảnh),…