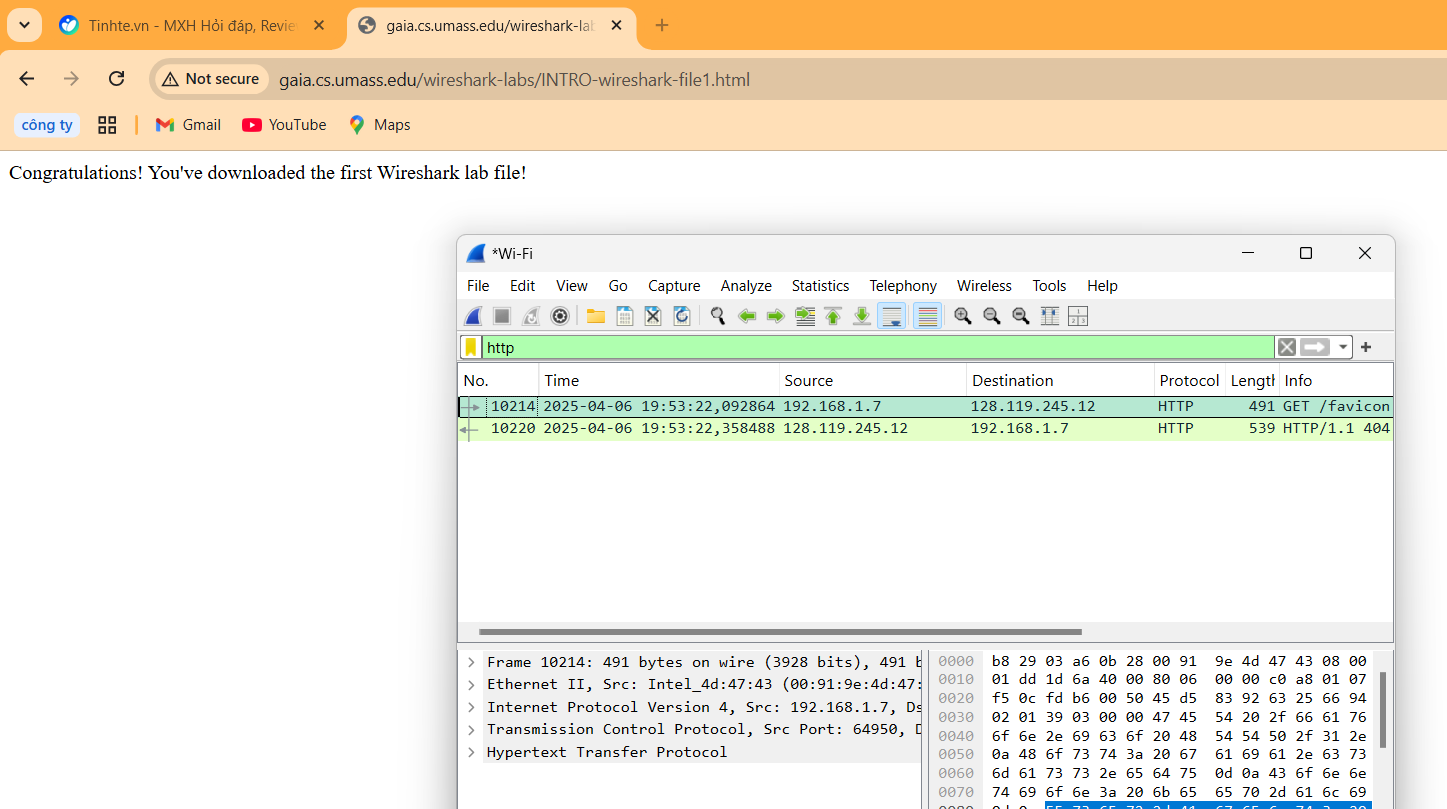
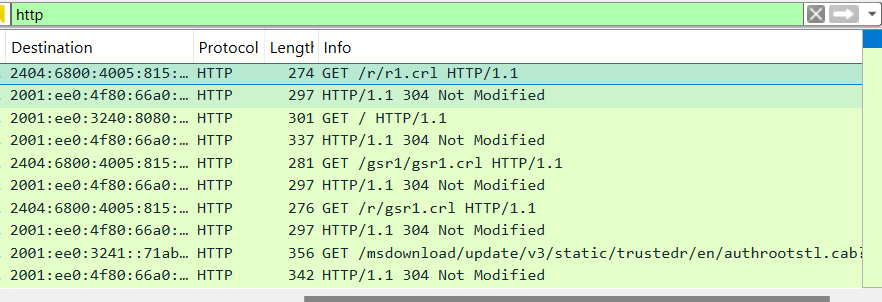
1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói

tin bắt được là bao nhiêu?





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.

* DNS (Domain Name System)  
  Chuyển đổi **tên miền (ví dụ: google.com)** thành **địa chỉ IP** để máy tính có thể định tuyến truy cập đúng server.
* TCP (Transmission Control Protocol)

Đảm bảo kết nối đáng tin cậy giữa hai máy (client-server), dữ liệu được truyền đúng thứ tự, không bị mất mát.

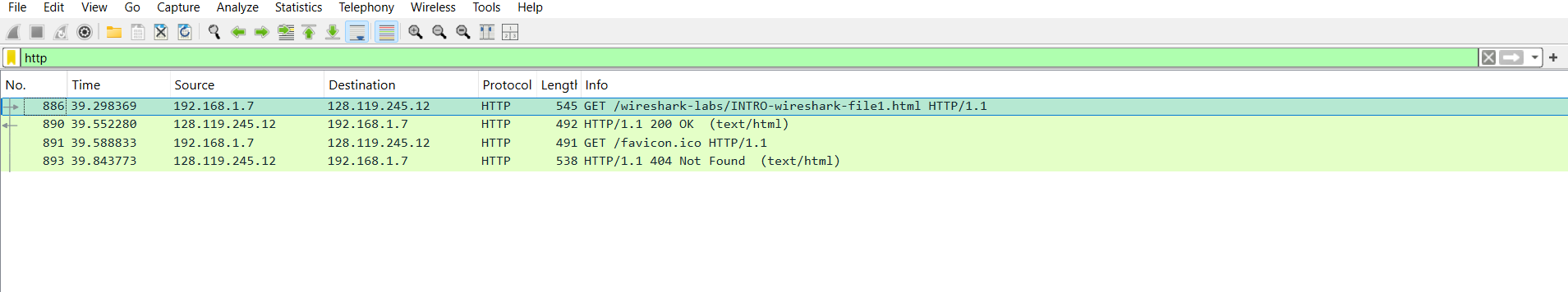
* HTTP (Hypertext Transfer Protocol)  
  Giao thức truyền tải **nội dung web** như HTML, ảnh, CSS, JS... từ server về trình duyệt.
* TLSv1.2 / TLSv1.3 (Transport Layer Security) Mã hóa dữ liệu truyền qua Internet để đảm bảo an toàn, thường dùng trong các kết nối HTTPS.
* ARP (Address Resolution Protocol)  
  Dùng để tìm **địa chỉ MAC tương ứng với địa chỉ IP** trong mạng LAN – hỗ trợ kết nối ở tầng mạng.

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).



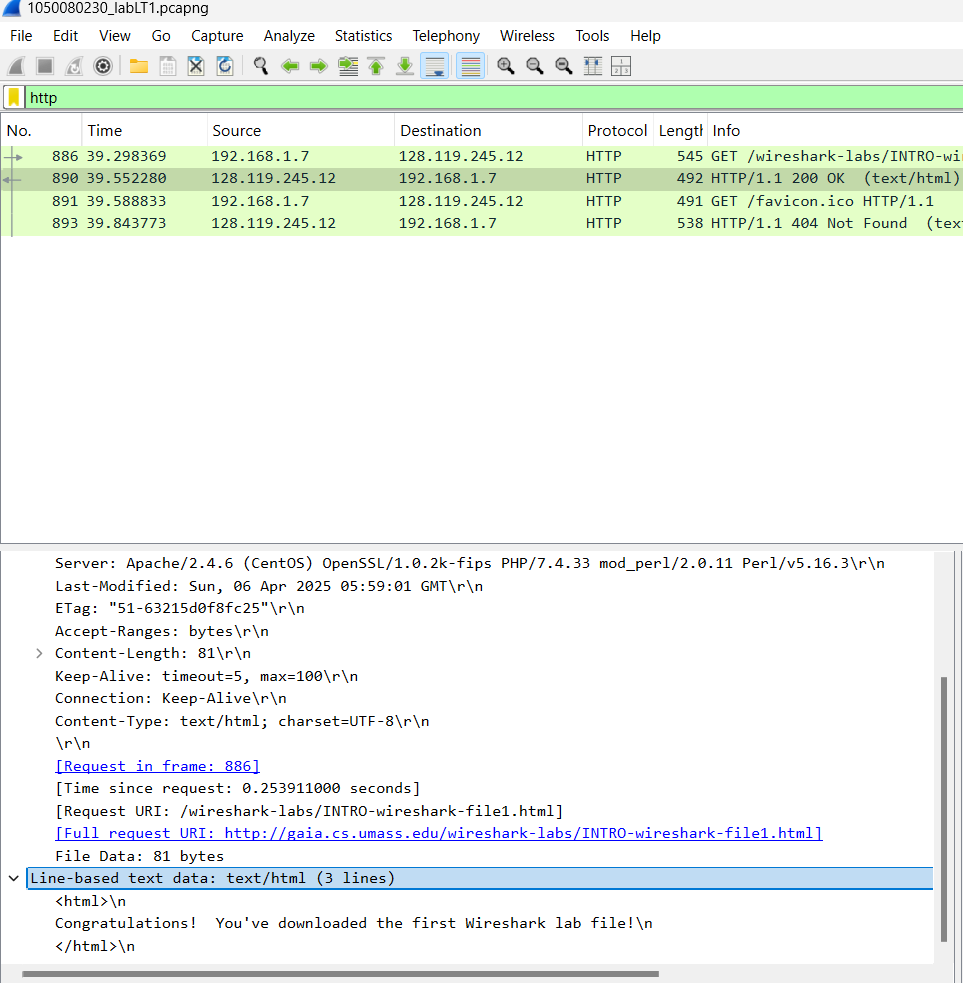
* Thời gian từ khi gửi HTTP GET đến khi nhận được HTTP 200 OK là khoảng 0.254 giây.

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?

| **Thông tin** | **Địa chỉ IP** |
| --- | --- |
| Website gaia.cs.umass.edu | 128.119.245.12 |
| Máy tính đang sử dụng (Client) | 192.168.1.7 |

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.

Mở rộng: 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 ví dụ minh họa.

B1: Người dùng nhập ”http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html”

B2: Trình duyệt thực hiện phân giải tên miền (DNS) để tìm địa chỉ IP của gaia.cs.umass.edu  
→ Kết quả là địa chỉ IP: 128.119.245.12.

B3: Trình duyệt gửi yêu cầu HTTP GET tới địa chỉ IP đó (gói số **886**):

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

B4: Máy chủ phản hồi HTTP 200 OK (gói 890) cùng với nội dung trang HTML:

Congratulations! You've downloaded the first Wireshark lab file!

B5: Trình duyệt hiển thị nội dung đó cho người dùng.

