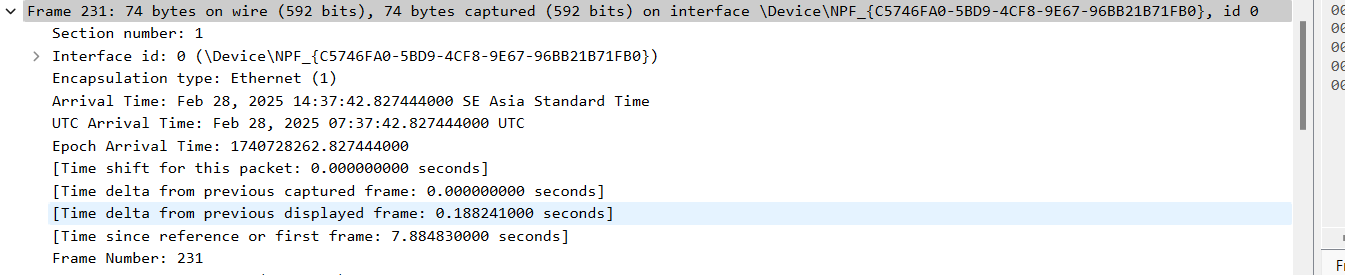
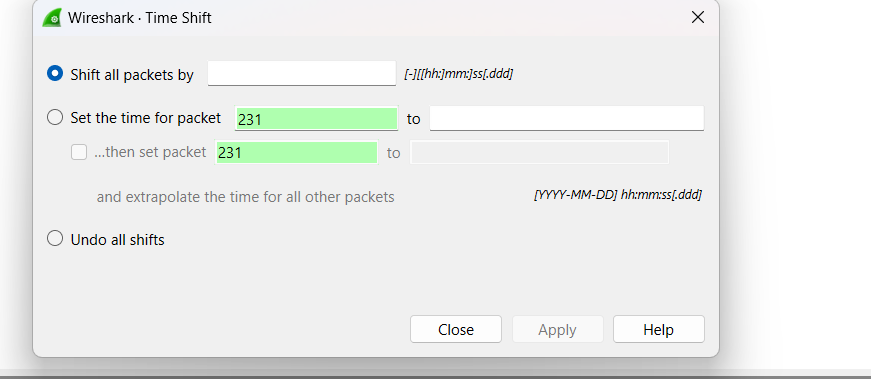
1.Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói

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.

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).

Các giao thức thường xuất hiện trong quá trình truy cập một website có thể bao gồm:

* **TCP (Transmission Control Protocol):** Là giao thức truyền tải chính được sử dụng trong hầu hết các ứng dụng mạng, bao gồm HTTP. TCP đảm bảo dữ liệu được truyền chính xác và đầy đủ, thông qua cơ chế xác nhận (acknowledgement) và kiểm tra lỗi.
* **DNS (Domain Name System):** Là giao thức dịch tên miền thành địa chỉ IP. Khi bạn truy cập một website, DNS sẽ chuyển tên miền (ví dụ, gaia.cs.umass.edu) thành địa chỉ IP tương ứng.
* **ARP (Address Resolution Protocol):** Dùng để ánh xạ giữa địa chỉ IP và địa chỉ MAC trong mạng LAN, giúp các thiết bị giao tiếp với nhau qua mạng.
* **ICMP (Internet Control Message Protocol):** Dùng để gửi các thông điệp điều khiển mạng, như ping, thông báo lỗi về việc không thể truy cập một địa chỉ IP.
* **TLS/SSL (Transport Layer Security / Secure Sockets Layer):** Là giao thức bảo mật được sử dụng trong HTTPS để mã hóa dữ liệu và bảo vệ sự riêng tư trong quá trình truyền tải giữa trình duyệt và server.

Để tìm thời gian này, bạn cần thực hiện các bước sau trong Wireshark:

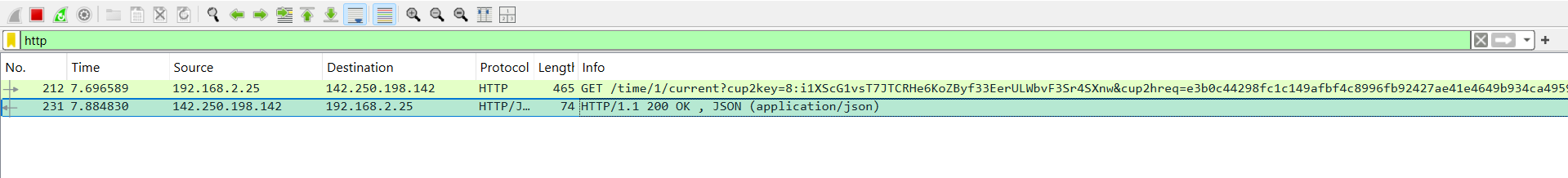
* Chọn gói tin HTTP GET đầu tiên từ một trong các website bạn truy cập.
* Chọn gói tin HTTP 200 OK trả về.
* Trong cột "Time" của Wireshark, bạn sẽ thấy thời gian tính từ lúc Wireshark bắt đầu bắt gói tin. Chênh lệch giữa thời gian của gói tin HTTP GET và HTTP 200 OK chính là thời gian phản hồi của server.

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 : 

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?

Quá trình này có thể được mô tả như sau:

1. **Gửi yêu cầu DNS:** Trình duyệt gửi yêu cầu DNS để chuyển tên miền của website thành địa chỉ IP.
2. **Gói tin DNS:** Gói tin DNS được gửi qua mạng, máy chủ DNS trả về địa chỉ IP của website.
3. **Kết nối TCP:** Trình duyệt thiết lập kết nối TCP với server web thông qua 3 bước bắt tay (3-way handshake).
4. **Gửi yêu cầu HTTP:** Sau khi kết nối TCP được thiết lập, trình duyệt gửi một yêu cầu HTTP (GET) đến server yêu cầu trang web.
5. **Nhận phản hồi HTTP:** Server trả về phản hồi HTTP (200 OK), gửi nội dung của trang web, bao gồm HTML, hình ảnh, và các tài nguyên khác.
6. **Hiển thị trang web:** Trình duyệt nhận và xử lý các tài nguyên, hiển thị nội dung của trang web cho người dùng.

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.