Họ tên: Hồ Minh Đại

Lớp: 10\_ĐH\_CNPM3

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

tin bắt được là bao nhiêu?

- Thời gian bắt được khoảng 5s

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.

Khi không áp dụng bộ lọc “http” trong Wireshark, các giao thức xuất hiện trong cột Protocol sẽ bao gồm nhiều loại khác nhau liên quan đến quá trình truy cập website. Dưới đây là 5 giao thức phổ biến có thể xuất hiện và mô tả ngắn gọn về chức năng của chúng:

1. **TCP (Transmission Control Protocol)**
   * *Chức năng*: Đảm bảo truyền dữ liệu đáng tin cậy giữa hai thiết bị qua mạng bằng cách thiết lập kết nối, kiểm soát luồng dữ liệu và xử lý lỗi. Đây là giao thức nền tảng cho HTTP.
2. **IP (Internet Protocol)**
   * *Chức năng*: Định tuyến và chuyển tiếp các gói tin qua mạng dựa trên địa chỉ IP. IP chịu trách nhiệm đưa dữ liệu từ nguồn đến đích.
3. **DNS(Domain Name System)**
   * *Chức năng*: Phân giải tên miền (như gaia.cs.umass.edu) thành địa chỉ IP để máy tính có thể kết nối đến máy chủ tương ứng.
4. **ARP (Address Resolution Protocol)**
   * *Chức năng*: Ánh xạ địa chỉ IP sang địa chỉ MAC (Media Access Control) trong mạng cục bộ để các thiết bị có thể giao tiếp trực tiếp với nhau.
5. **UDP (User Datagram Protocol)**
   * *Chức năng*: Cung cấp phương thức truyền dữ liệu nhanh nhưng không đảm bảo độ tin cậy, thường được dùng cho các ứng dụng như streaming hoặc DNS trong một số trường hợp

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).

 **Cách tính**: Trong Wireshark, tìm gói tin chứa HTTP GET đầu tiên (dòng “GET /…” trong phần Hypertext Transfer Protocol) và ghi lại giá trị thời gian trong cột Time. Sau đó, tìm gói tin HTTP 200 OK tương ứng (dòng “HTTP/1.1 200 OK”) và ghi lại thời gian. Lấy thời gian của HTTP 200 OK trừ đi thời gian của HTTP GET để ra kết quả.

 **Ví dụ giả định**:

* Website 1 (gaia.cs.umass.edu):
  + HTTP GET gửi lúc: 3.398919 giây.
  + HTTP 200 OK nhận lúc: 3.431008 giây.
  + Thời gian = 3.431008 - 3.398919 = **0.032089 giây** (32,089 ms)
* Website 2 (giả định một website khác):
  + HTTP GET gửi lúc: 5.123456 giây.
  + HTTP 200 OK nhận lúc: 5.167890 giây.
  + Thời gian = 5.167890 - 5.123456 = **0.044434 giây** (44,434 ms).

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.

* **Trả lời**: Có, nội dung “Congratulations! You've downloaded the first Wireshark lab file!” sẽ nằm trong các gói tin HTTP bắt được, cụ thể là trong phần thân (entity body) của gói tin phản hồi HTTP 200 OK từ máy chủ gaia.cs.umass.edu.
* **Vị trí**: Để tìm trong Wireshark:
  1. Áp dụng bộ lọc “http” để chỉ hiển thị các gói tin HTTP.
  2. Tìm gói tin “HTTP/1.1 200 OK” tương ứng với yêu cầu GET tới đường dẫn như “/wireshark-labs/HTTP-wireshark-file1.html”.
  3. Trong cửa sổ Packet Details, mở rộng phần “Hypertext Transfer Protocol” và cuộn xuống “Line-based text data” hoặc “HTML” (nếu có). Nội dung này sẽ xuất hiện dưới dạng văn bản thô trong phần dữ liệu (Data) của gói tin.
  4. Bạn cũng có thể kiểm tra cửa sổ Packet Bytes để xem dữ liệu dạng hex và ASCII, nơi chuỗi “Congratulations…” sẽ hiển thị rõ ràng.

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 của gaia.cs.umass.edu**: Theo tài liệu tham khảo, địa chỉ IP của gaia.cs.umass.edu là **128.119.245.12**.

 **Địa chỉ IP của website đã chọn ở bước 10**: Vì bạn không cung cấp thông tin về website thứ hai ở “bước 10”, tôi không thể xác định chính xác. Bạn cần kiểm tra trong Wireshark bằng cách xem địa chỉ IP đích (Destination IP) trong gói tin HTTP GET gửi tới website đó.

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.

1. **Phân giải tên miền (DNS)**: Máy tính gửi yêu cầu DNS để phân giải tên miền (gaia.cs.umass.edu) thành địa chỉ IP (128.119.245.12). Gói tin DNS Request và DNS Response sẽ xuất hiện trong Wireshark.
2. **Thiết lập kết nối TCP (3-way handshake)**: Máy tính khởi tạo kết nối TCP với máy chủ qua ba bước:
   * Gửi gói tin SYN.
   * Nhận gói tin SYN-ACK từ máy chủ.
   * Gửi gói tin ACK để hoàn tất kết nối.
3. **Gửi yêu cầu HTTP GET**: Sau khi kết nối TCP được thiết lập, trình duyệt gửi gói tin HTTP GET tới máy chủ (ví dụ: “GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1”) để yêu cầu nội dung.
4. **Nhận phản hồi HTTP từ máy chủ**: Máy chủ trả về gói tin HTTP 200 OK kèm theo dữ liệu (HTML, hình ảnh, v.v.). Dữ liệu này được chia thành nhiều đoạn TCP nếu lớn.
5. **Trình duyệt hiển thị nội dung**: Sau khi nhận đủ dữ liệu, trình duyệt xử lý và hiển thị nội dung (như “Congratulations!...”) cho người dùng.
6. **Đóng kết nối**: Khi hoàn tất, kết nối TCP có thể được đóng bằng gói tin FIN hoặc RST.