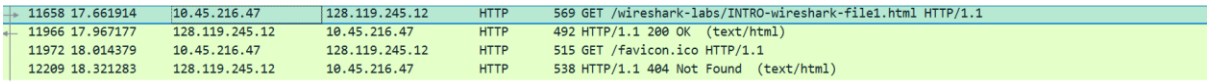
24521066 – Nguyễn Hoàng Hải Minh – Lab1

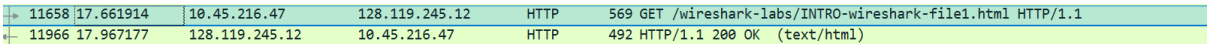
1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?



Tổng số gói tin bắt được là 4. Tổng thời gian là: 18.321283 – 17.661914 = 0.659369

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.
   - QUIC (Quick UDP Internet Connections) là một giao thức truyền thông do Google phát triển, sau này được chuẩn hóa bởi IETF, với mục tiêu thay thế TCP + TLS + HTTP/2. Nó chạy trên nền UDP và mang nhiều tính năng cải tiến: thiết lập kết nối nhanh, bảo mật tích hợp sẵn, giảm độ trễ và tăng hiệu quả truyền dữ liệu,…
   - MDNS (Multicast DNS) là một giao thức trong mạng máy tính dùng để phân giải tên miền trong mạng cục bộ (LAN) mà không cần máy chủ DNS trung tâm: phân giải tên miền nội bộ, sử dụng multicast, khám phá dịch vụ,…
   - TCP (Transmission Control Protocol) là một trong những giao thức quan trọng nhất của bộ giao thức Internet (TCP/IP). Nó chạy trên lớp Transport (tầng vận chuyển) và thường đi kèm với IP (TCP/IP): kết nối hướng liên kết, truyền dữ liệu tin cậy, điều khiển luồng,…
   - DHCP (Dynamic Host Configuration Protocol) là giao thức nằm ở lớp ứng dụng (Application Layer) trong mô hình TCP/IP, dùng để cấp phát tự động các thông số mạng cho thiết bị trong mạng LAN/WAN: tự động cấp phát địa chỉ IP, quản lý tập trung địa chỉ IP
   - UDP (User Datagram Protocol) là một giao thức vận chuyển (Transport Layer) trong bộ TCP/IP, hoạt động song song với TCP nhưng có đặc điểm nhanh – gọn – không đảm bảo tin cậy: truyền dữ liệu không đảm bảo, phân mảnh dữ thành datagram,…

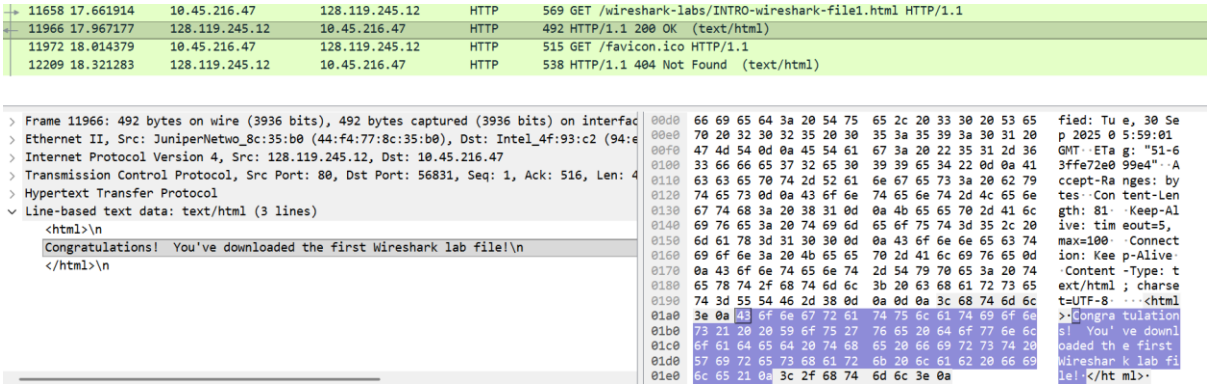
3. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).



Thời gian từ khi gói tin Get được gửi cho đến khi 200 OK là: 17.967177 – 17.661914 = 0.305263

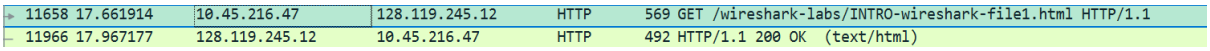
4. Nội dung hiển thị trên trang web gaia.cs.umass.edu
"Congratulations! You've downloaded the first Wireshark lab file!"
có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác

định vị trí của nội dung này trong các gói tin bắt được.



Nội dung trên có nằm trong các gói tin HTTP bắt được, nó nằm trong gói tin 200 OK và trong phần data, nó nằm từ cột 01a0 tới 01e0.

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 là 128.119.245.12
Địa chỉ IP của máy tính đang sử dụng là 10.45.216.47

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.
   - Trong Wireshark, khi bắt đầu truy cập một trang web, trước tiên ta thấy các gói tin từ máy tính (địa chỉ IP nguồn) gửi đến máy chủ để phân giải tên miền, sau đó nhận lại phản hồi DNS chứa địa chỉ IP của máy chủ web. Tiếp theo, xuất hiện chuỗi gói tin giữa IP máy tính và IP máy chủ web để thiết lập kết nối. Sau khi kết nối đã sẵn sàng, máy tính gửi gói HTTP Request (GET) đến máy chủ web, và nhận lại các gói HTTP chứa mã HTML (200 OK). Tiếp đó, trình duyệt tiếp tục gửi thêm nhiều gói HTTP Request để lấy các tài nguyên phụ theo yêu cầu và nhận về các gói phản hồi tương ứng. Cuối cùng, toàn bộ dữ liệu được trình duyệt xử lý và hiển thị thành trang web hoàn chỉnh cho người dùng để xem.