

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?

11658	17.661914	10.45.216.47	128.119.245.12	HTTP	569 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
11966	17.967177	128.119.245.12	10.45.216.47	HTTP	492 HTTP/1.1 200 OK (text/html)
11972	18.014379	10.45.216.47	128.119.245.12	HTTP	515 GET /favicon.ico HTTP/1.1
12209	18.321283	128.119.245.12	10.45.216.47	HTTP	538 HTTP/1.1 404 Not Found (text/html)

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 liệu 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).

11658	17.661914	10.45.216.47	128.119.245.12	HTTP	569 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
11966	17.967177	128.119.245.12	10.45.216.47	HTTP	492 HTTP/1.1 200 OK (text/html)

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.

11658	17.661914	10.45.216.47	128.119.245.12	HTTP	569 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
11966	17.967177	128.119.245.12	10.45.216.47	HTTP	492 HTTP/1.1 200 OK (text/html)
11972	18.014379	10.45.216.47	128.119.245.12	HTTP	515 GET /favicon.ico HTTP/1.1
12209	18.321283	128.119.245.12	10.45.216.47	HTTP	538 HTTP/1.1 404 Not Found (text/html)

> Frame 11966: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface > Ethernet II, Src: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0), Dst: Intel_4f:93:c2 (94:c > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.216.47 > Transmission Control Protocol, Src Port: 80, Dst Port: 56831, Seq: 1, Ack: 516, Len: 4 > Hypertext Transfer Protocol > Line-based text data: text/html (3 lines)	00d0 66 69 65 64 3a 20 54 75 65 2c 20 33 30 20 53 65 00e0 70 20 32 30 32 35 20 30 35 3a 35 39 3a 30 31 20 00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 31 2d 36 0100 33 66 66 65 37 32 65 30 39 39 65 34 22 0d 0a 41 0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 0130 67 74 68 3a 20 38 31 0d 0a 4b 65 65 70 2d 41 6c 0140 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 0150 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 0160 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0170 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 0180 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 0190 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 01a0 3e 0a 0d 6f 0e 67 72 61 74 73 6c 61 74 69 6f 0e 01b0 73 21 20 20 59 6f 75 27 76 65 20 64 6f 77 6e 6c 01c0 6f 61 64 65 64 20 74 68 65 20 66 69 72 73 74 20 01d0 5f 69 72 65 73 68 61 72 6b 20 6c 61 62 20 66 69 01e0 6c 65 21 0a 3c 2f 68 74 6d 6c 3e 0a	fied: Tu e, 30 Se p 2025 0 5:59:01 GMT:ETA g: "51-6 3ffe72e0 99e4"·A ccept-Ra nges: by tes·Con tent-Len gth: 81·Keep-Al ive: tim eout=5, max=100·Connect ion: Kee p-Alive ·Content -Type: t ext/html ; charse t=UTF-8 ···<html >·<congratulation s! You' ve downl oaded th e first Wireshar k lab fi le!</ht ml>·
--	--	--

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.

- 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?

11658	17.661914	10.45.216.47	128.119.245.12	HTTP	569 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
11966	17.967177	128.119.245.12	10.45.216.47	HTTP	492 HTTP/1.1 200 OK (text/html)

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

- 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.