**Lý thuyết thực hành 1**

**Tên : Phan Thị Hoàng Oanh**

**MSSV : 1050080150**

**Lớp : 10-ĐH-CNPM2**

**LAB 1**

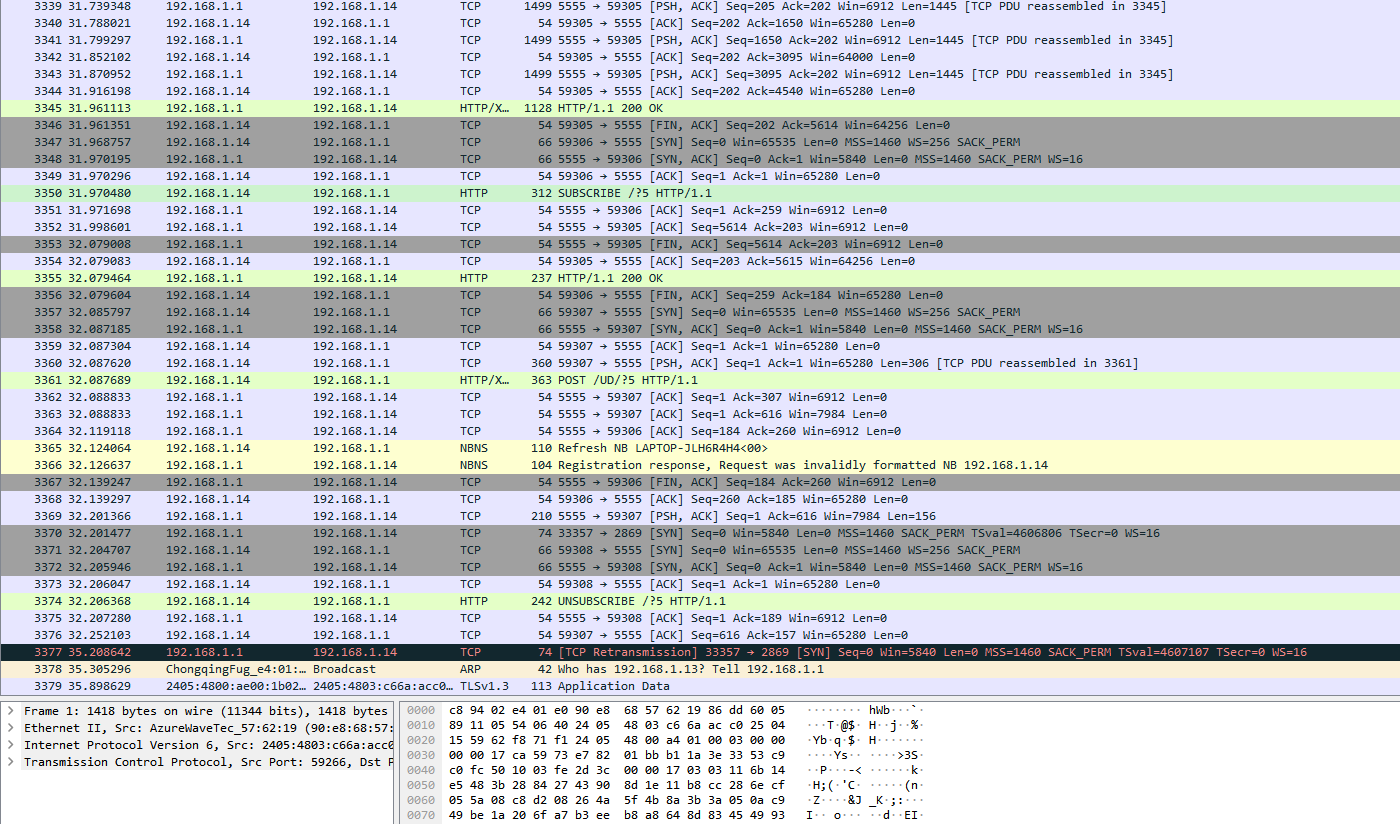
**1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói**

**tin bắt được là bao nhiêu?**

Web 1

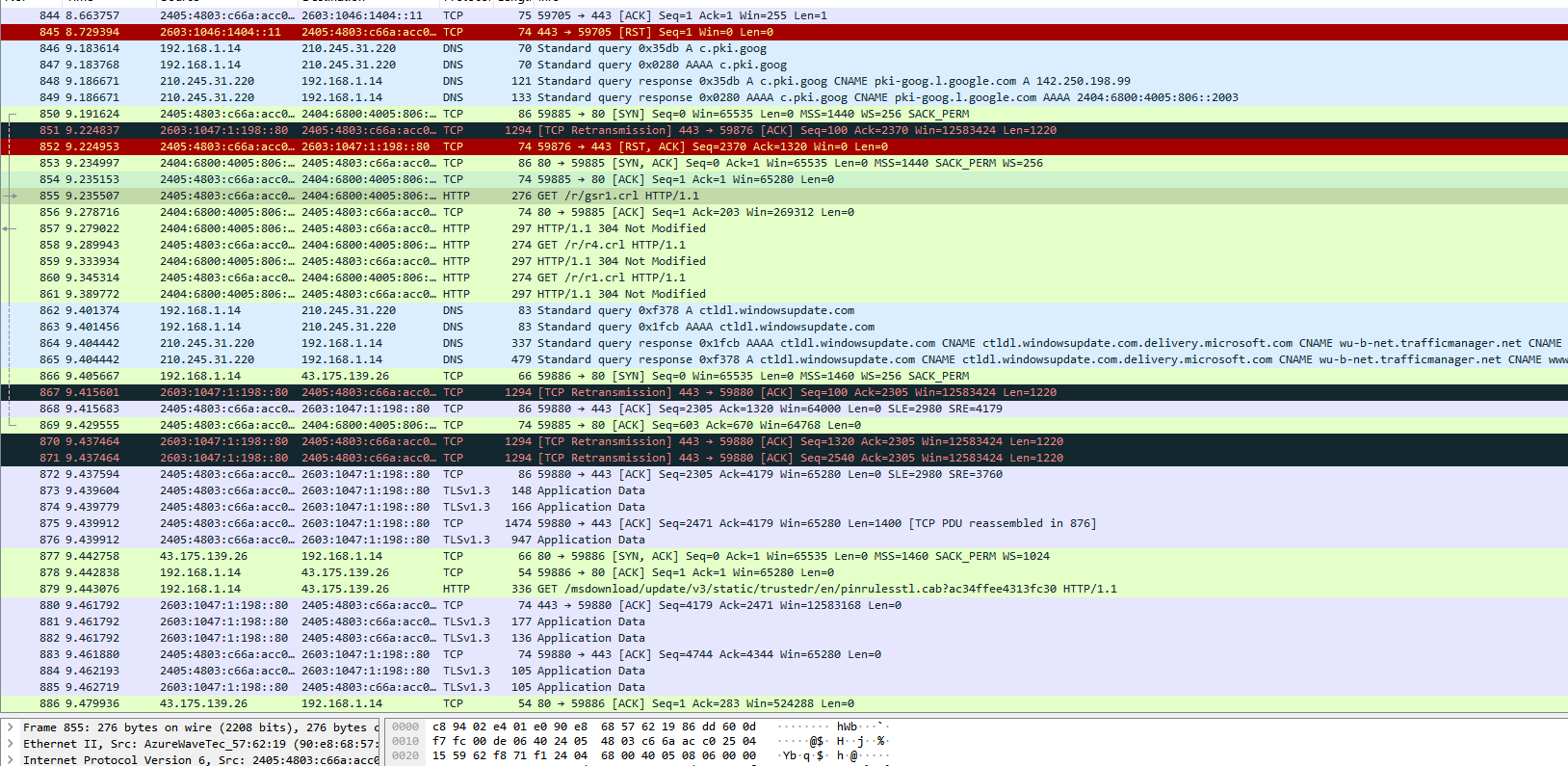
Tổng số gói tin : 3322

Tổng thời gian : 31.4s



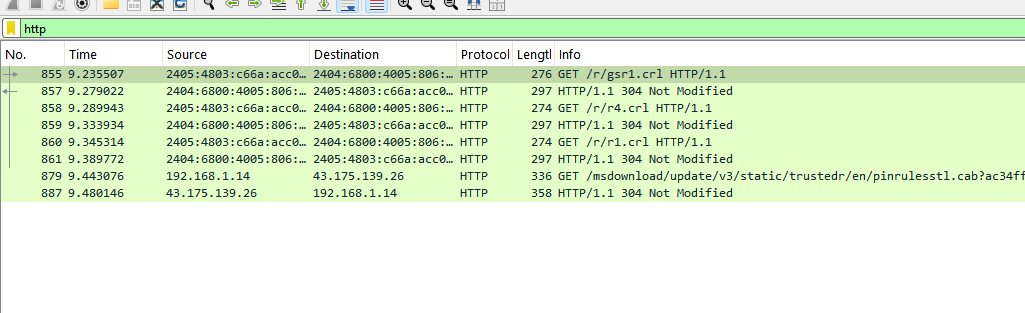
Web 2

Tổng số gói tin : 855

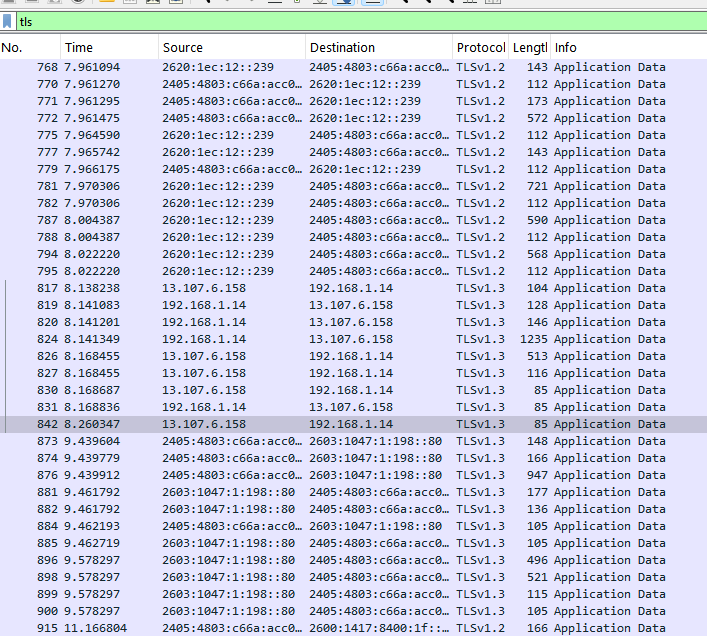
Tổng thời gian : 9.23s

**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**

Lọc http



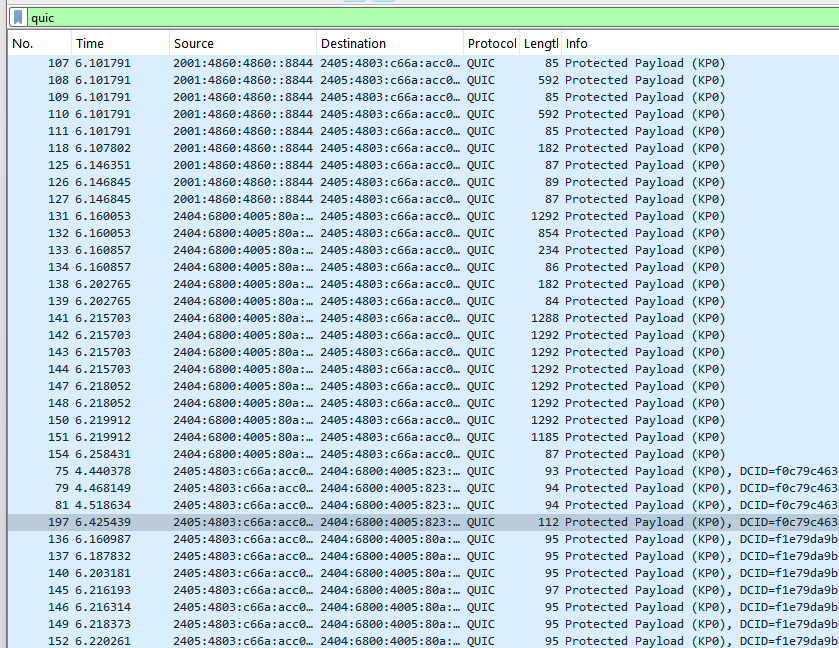
Tls



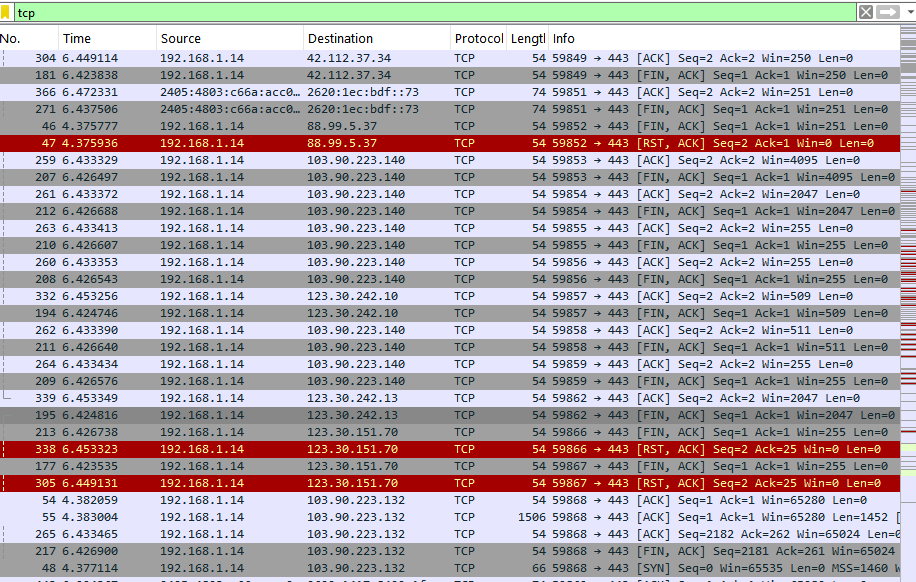
Nhờ vào các chức năng này, TLS đóng vai trò quan trọng trong việc bảo vệ thông tin nhạy cảm khi truyền qua mạng, đảm bảo an toàn cho người dùng và hệ thống.

* Mã hóa dữ liệu, xác thực danh tính (qua chứng chỉ SSL/TLS), và đảm bảo toàn vẹn dữ liệu.
* Thường kết hợp với TCP (ví dụ: HTTPS) hoặc UDP (DTLS) để bảo mật giao tiếp.

quic

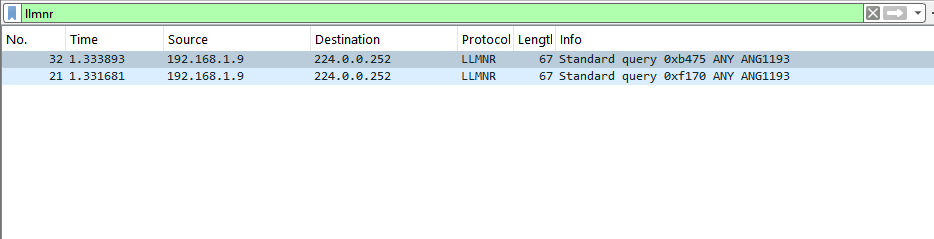


* Giao thức dựa trên UDP, tích hợp sẵn TLS 1.3 để giảm độ trễ kết nối.
* Hỗ trợ multiplexing (nhiều luồng độc lập), tránh tắc nghẽn do head-of-line blocking.
* Tối ưu cho HTTP/3, phù hợp mạng di động hoặc mất gói.

TCP

* Giao thức hướng kết nối, đảm bảo truyền dữ liệu đáng tin cậy, đúng thứ tự.
* Sử dụng cơ chế xác nhận (ACK), truyền lại gói mất, và kiểm soát tắc nghẽn.
* Dùng cho ứng dụng cần độ chính xác cao (web, email, file transfer).

llmnr

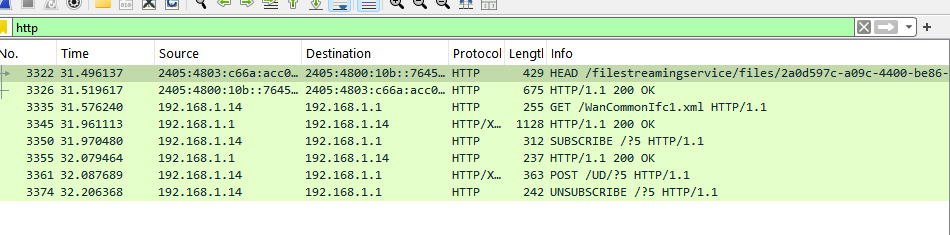


· **Giải quyết tên (Name Resolution):** LLMNR giúp các thiết bị trong một mạng con có thể xác định các thiết bị khác chỉ bằng tên máy tính mà không cần sự hỗ trợ từ máy chủ DNS.

· **Hoạt động trong mạng cục bộ:** LLMNR chỉ hoạt động trong các mạng nội bộ (local network), giúp các thiết bị giao tiếp mà không cần phải kết nối với Internet.

· **Sử dụng Multicast:** Khi một thiết bị muốn giải quyết tên máy, nó gửi một yêu cầu multicast tới tất cả các thiết bị khác trong mạng cục bộ, và các thiết bị có tên phù hợp sẽ phản hồi.

**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).**



1. **Gói tin HTTP GET đầu tiên**:
   * **No. 3335**
   * **Thời gian:** 31.57640
   * **Source:** 192.168.1.14
   * **Destination:** 192.168.1.1
   * **Yêu cầu:** GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2. **Gói tin HTTP 200 OK đầu tiên**:
   * **No. 4344**
   * **Thời gian:** 31.961113
   * **Source:** 192.168.1.1
   * **Destination:** 192.168.1.14
   * **Phản hồi:** HTTP/1.1 200 OK

**Tính thời gian phản hồi**

0.384873

**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.**