**Lab 1: Làm quen với Wireshark**

B.Thực hành

1. Task 1: Mở đầu về Mạng máy tính

- Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).

Router: Thiết bị định tuyến, giúp kết nối các mạng với nhau và chuyển tiếp dữ liệu giữa chúng.

Ảnh minh họa:



Switch: Thiết bị chuyển mạch, kết nối các thiết bị trong cùng một mạng LAN và chuyển tiếp dữ liệu giữa chúng.

Ảnh minh họa:



Modem: Thiết bị điều chế/giải điều chế, chuyển đổi tín hiệu số từ máy tính sang tín hiệu tương tự để truyền qua đường dây điện thoại hoặc cáp, và ngược lại.

Ảnh minh họa:



Access Point (Điểm truy cập không dây):

Thiết bị cho phép các thiết bị không dây kết nối vào mạng LAN.

Ảnh minh họa:



Thiết bị đầu cuối, kết nối mạng thông qua Wifi hoặc mạng di động.

Firewall:

Thiết bị hoặc phần mềm bảo vệ mạng khỏi các truy cập trái phép.

Ảnh minh họa:



Firewall network device

- Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

Giao tiếp bị gián đoạn:

* Không thể gửi/nhận email, tin nhắn, cuộc gọi video.
* Mạng xã hội, các ứng dụng nhắn tin trực tuyến không hoạt động.

Công việc bị ảnh hưởng:

* Không thể truy cập các tài liệu, ứng dụng trực tuyến.
* Giao dịch trực tuyến, thanh toán điện tử bị gián đoạn.

Các hoạt động kinh doanh phụ thuộc vào internet sẽ bị ngưng trệ.

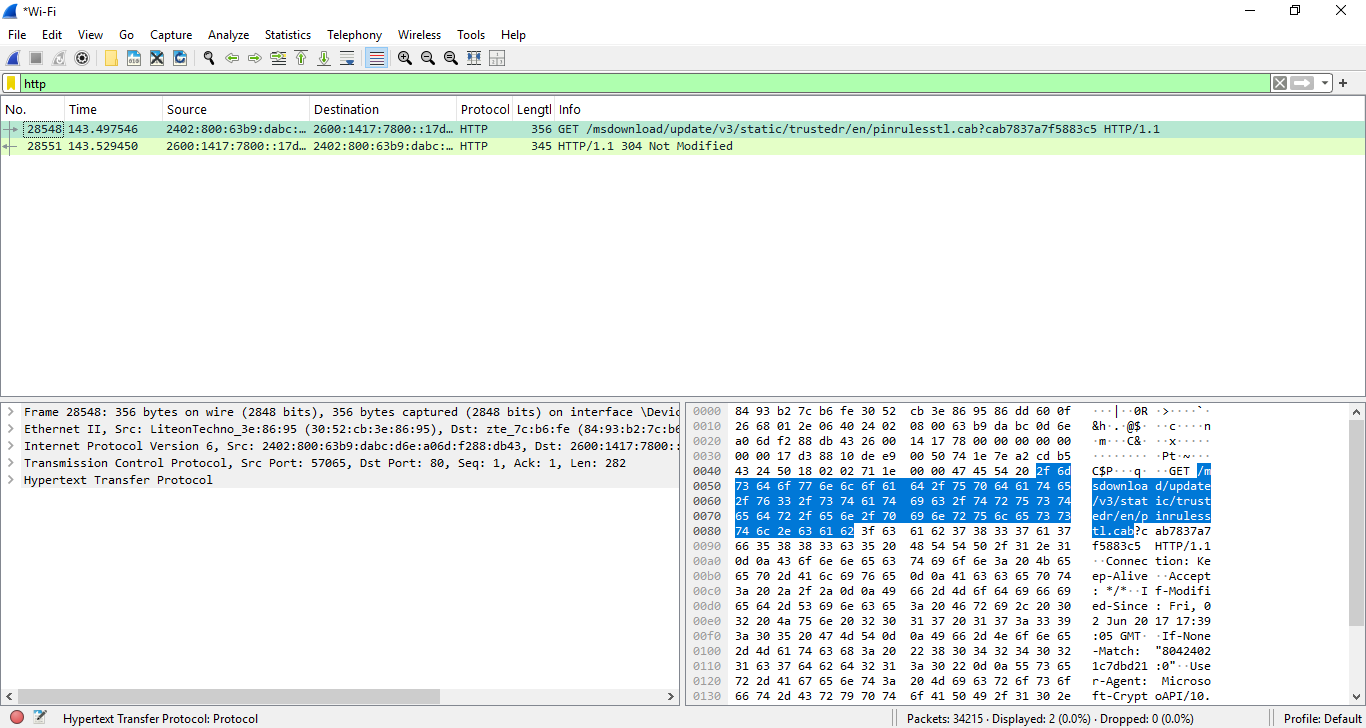
Thông tin bị thiếu hụt:

* Không thể truy cập tin tức, thông tin cập nhật.
* Việc tìm kiếm thông tin trên internet bị gián đoạn.

Các thiết bị IoT (Internet of Things) không hoạt động: Các thiết bị nhà thông minh, các thiết bị giám sát từ xa sẽ bị mất kết nối.

- Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

* Hiểu rõ các khái niệm cơ bản về mạng máy tính (mô hình OSI, TCP/IP, địa chỉ IP, giao thức mạng, v.v.).
* Nắm vững cách thức hoạt động của các thiết bị mạng (router, switch, modem, v.v.).
* Có khả năng phân tích và giải quyết các vấn đề mạng cơ bản.
* Biết cách sử dụng các công cụ phân tích mạng (như Wireshark) để theo dõi và kiểm tra lưu lượng mạng.
* Hiểu về các vấn đề bảo mật mạng cơ bản.
* Có thể thiết kế một mạng Lan đơn giản.
* Có thể cấu hình các thiết bị mạng cơ bản.



**Trả lời ngắn gọn: Lab 1 - Wireshark**

**Tổng thời gian bắt gói tin & số gói tin thu được**

* **Mở file .pcapng trên Wireshark**, xem cột **Time** để lấy thời gian từ gói đầu đến gói cuối.
* **Xem tổng số gói tin** trong packet-list (số cuối cùng trong cột No).

**Giao thức xuất hiện khi không lọc HTTP & chức năng**

* **HTTP**: Giao thức truyền tải nội dung web.
* **TCP**: Giao thức vận chuyển tin cậy, thiết lập kết nối.
* **DNS**: Dịch tên miền (VD: google.com → IP).
* **ARP**: Tìm địa chỉ MAC từ địa chỉ IP trong mạng LAN.
* **ICMP**: Kiểm tra kết nối mạng (VD: ping).

**Thời gian từ HTTP GET đến HTTP 200 OK**

* **Lọc gói HTTP**, tìm **HTTP GET đầu tiên** và **HTTP 200 OK đầu tiên**.
* **Trừ giá trị cột Time của hai gói tin** để tính thời gian phản hồi.

**Nội dung "Congratulations!" có trong gói tin không?**

* **Dò gói tin HTTP 200 OK** → xem **Packet Details** → kiểm tra phần **HTML Data**.
* Nếu có, chụp màn hình vị trí hiển thị nội dung.

**Địa chỉ IP của server & máy tính**

* **IP của server**: Tìm gói HTTP, xem **cột Destination**.
* **IP của máy tính**: Tìm gói HTTP GET, xem **cột Source**.

**Diễn biến truy cập website**

1. Trình duyệt gửi **DNS Request** để lấy IP của trang web.
2. Thiết lập kết nối **TCP (Three-way handshake)**.
3. Gửi **HTTP GET** để yêu cầu nội dung trang web.
4. Server phản hồi **HTTP 200 OK** kèm dữ liệu HTML.
5. Trình duyệt hiển thị nội dung trang web.