1

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

**Làm quen với Wireshark**

Wireshark Getting Started

**Môn học: Nhập môn Mạng máy tính**

|  |  |
| --- | --- |
| **Sinh viên thực hiện** | Lại Quan Thiên (22521385) |
| **Thời gian thực hiện** | 04/10/2023 – 05/10/2023 |
| **Tự chấm điểm** | 10/10 |

**File 22521385-Bai1.pcapng:**

**1. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?**

- Tổng thời gian bắt gói tin: 2.650154 giây

- Tổng số gói tin bắt được: 162 gói

A screenshot of a computer

Description automatically generated

**2. Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol).**

**Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.**

- 3 giao thức khác nhau trong cột Protocol: HTTP, UDP, TCP

- Mô tả:

+ HTTP (Hypertext Transfer Protocol):

*Chức năng:* HTTP là giao thức sử dụng trong trình duyệt web và máy chủ web để truyền tải dữ liệu giữa client và server. Nó được sử dụng chủ yếu để truy cập và trao đổi thông tin trên World Wide Web.

*Đặc điểm chính:* HTTP hoạt động dựa trên mô hình yêu cầu/hồi đáp (request/response). Client gửi yêu cầu HTTP đến server, và server gửi phản hồi HTTP chứa dữ liệu trang web hoặc thông tin cần thiết trở lại cho client. Giao thức này thường sử dụng cổng 80 cho kết nối.

+ UDP (User Datagram Protocol):

*Chức năng:* UDP là giao thức truyền tải dữ liệu qua mạng mà không đảm bảo tính toàn vẹn hoặc giao diện. Nó thường được sử dụng cho các ứng dụng cần truyền tải dữ liệu nhanh và không cần đảm bảo mọi gói dữ liệu đều đến đích.

*Đặc điểm chính:* UDP là giao thức không kết nối, nghĩa là không có quá trình thiết lập kết nối như TCP. Nó truyền gói dữ liệu (datagram) độc lập, không đảm bảo thứ tự hoặc tính toàn vẹn dữ liệu. UDP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể.

+ TCP (Transmission Control Protocol):

*Chức năng:* TCP là giao thức truyền tải dữ liệu qua mạng với tính toàn vẹn, đảm bảo thứ tự và kiểm soát lưu lượng. Nó thường được sử dụng cho các ứng dụng cần độ tin cậy trong việc truyền tải dữ liệu.

*Đặc điểm chính:* TCP hoạt động dựa trên mô hình kết nối, bắt đầu bằng quá trình thiết lập kết nối giữa client và server. Nó đảm bảo rằng dữ liệu được chia thành các gói, gửi đúng thứ tự và đảm bảo tính toàn vẹn. TCP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể và thường sử dụng cổng 80 cho HTTP.

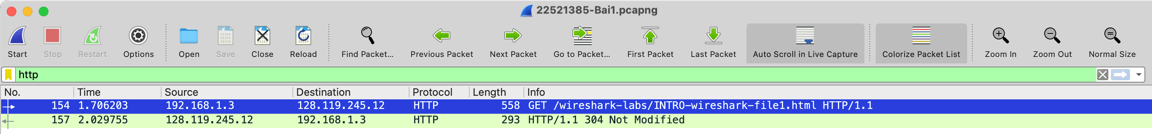
**Gõ “http” vào packet-display filter sau đó chọn Apply để Wireshark chỉ hiển thị các thông điệp HTTP trong packet-listing window. Sau đó trả lời các câu hỏi sau:**

**3. Có bao nhiêu gói tin HTTP? Tỉ lệ % số gói tin HTTP/Tổng số gói tin?**

- Có 2 gói tin HTTP trên tổng số 162 gói

- Tỉ lệ: 1,23%

**4. Có bao nhiêu gói tin HTTP GET?** Có 1 gói tin HTTP GET.

****

**5. Tìm và xác định gói tin HTTP GET đầu tiên được gửi đến web server gaia.cs.umass.edu?**

Một số thông tin của gói tin này (xem ảnh):

- Số: 154

- Host: gaia.cs.umass.edu

**A screenshot of a computer

Description automatically generated**

**6. Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?**

Một số thông tin của gói tin này (xem ảnh):

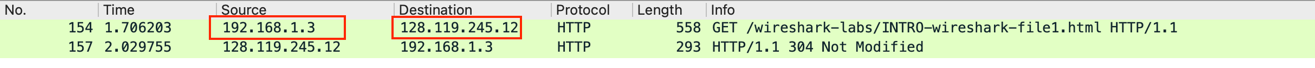
A screenshot of a computer

Description automatically generated

**7. Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin**

**phản hồi (Câu 6)?** Mất 0,323552 giây

**8. Dự đoán địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính đang sử dụng là gì? Tại sao?**



- Địa chỉ IP của “gaia.cs.umass.edu” là: 128.119.245.12

+ Xem trong phần Destination của WireShark

+ Hoặc dùng lệnh “nslookup gaia.cs.umass.edu” trên Terminal macOS

- Địa chỉ IP của máy tính đang sử dụng: *192.168.1.3*

+ Xem trong phần Source của WireShark

+ Hoặc vào System Settings -> Wifi -> Details -> TCP/IP -> IP address

- Giải thích: Ta biết rằng, Source là địa chỉ nguồn và Destination là địa chỉ đích. Do đó, khi truy cập trang web, IP từ máy tính sẽ gửi Request đến trang web ta cần truy cập, ở đây có host là gaia.cs.umass.eduvà nó cũng là địa chỉ đích. Dựa vào điều này, ta có thể dự đoán/xác định được địa chỉ IP của máy tính và trang web. Ngoài ra, ta có thể dùng lệnh trên Termianl để xác định (như đã trình bày ở trên)

A screenshot of a computer

Description automatically generated

**File 22521385-Bai2.pcapng:**

**9. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?**

- Tổng thời gian bắt gói tin: 3,933490 giây

- Tổng số gói tin bắt được: 56 gói

A screenshot of a computer

Description automatically generated

**10. Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol). Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.**

- 3 giao thức khác nhau trong cột Protocol: HTTP, UDP, TCP

- Mô tả:

+ HTTP (Hypertext Transfer Protocol):

*Chức năng:* HTTP là giao thức sử dụng trong trình duyệt web và máy chủ web để truyền tải dữ liệu giữa client và server. Nó được sử dụng chủ yếu để truy cập và trao đổi thông tin trên World Wide Web.

*Đặc điểm chính:* HTTP hoạt động dựa trên mô hình yêu cầu/hồi đáp (request/response). Client gửi yêu cầu HTTP đến server, và server gửi phản hồi HTTP chứa dữ liệu trang web hoặc thông tin cần thiết trở lại cho client. Giao thức này thường sử dụng cổng 80 cho kết nối.

+ UDP (User Datagram Protocol):

*Chức năng:* UDP là giao thức truyền tải dữ liệu qua mạng mà không đảm bảo tính toàn vẹn hoặc giao diện. Nó thường được sử dụng cho các ứng dụng cần truyền tải dữ liệu nhanh và không cần đảm bảo mọi gói dữ liệu đều đến đích.

*Đặc điểm chính:* UDP là giao thức không kết nối, nghĩa là không có quá trình thiết lập kết nối như TCP. Nó truyền gói dữ liệu (datagram) độc lập, không đảm bảo thứ tự hoặc tính toàn vẹn dữ liệu. UDP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể.

+ TCP (Transmission Control Protocol):

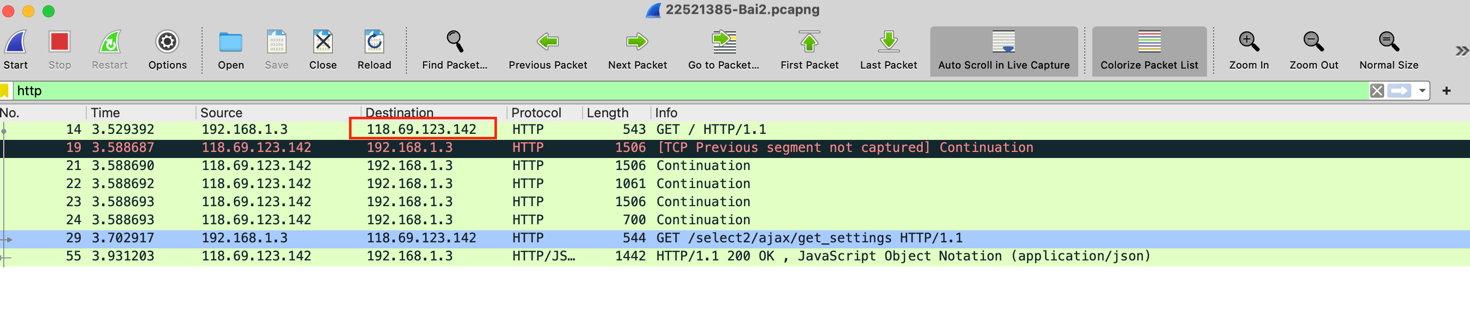
*Chức năng:* TCP là giao thức truyền tải dữ liệu qua mạng với tính toàn vẹn, đảm bảo thứ tự và kiểm soát lưu lượng. Nó thường được sử dụng cho các ứng dụng cần độ tin cậy trong việc truyền tải dữ liệu.

*Đặc điểm chính:* TCP hoạt động dựa trên mô hình kết nối, bắt đầu bằng quá trình thiết lập kết nối giữa client và server. Nó đảm bảo rằng dữ liệu được chia thành các gói, gửi đúng thứ tự và đảm bảo tính toàn vẹn. TCP sử dụng cổng để xác định dịch vụ hoặc ứng dụng cụ thể và thường sử dụng cổng 80 cho HTTP.

**11. Tìm cách để xác định địa chỉ IP của trang web đã chọn ở Bước 8. Địa chỉ IP trang web đã chọn là gì?**

- Cách xác định địa chỉ IP của trang web celuit.edu.vn:

+ Xem trong phần Destination của WireShark:



+ Hoặc dùng lệnh “nslookup celuit.edu.vn” trên Terminal macOS:

**A screenshot of a computer

Description automatically generated**

- Do đó, địa chỉ IP của “celuit.edu.vn” là:

+ Name: celuit.edu.vn

+ IP Address: 118.69.123.142

**12. Số lượng gói tin và khối lượng dữ liệu được gửi (trao đổi) giữa Địa chỉ trang**

**web ở trên (Câu 11) và máy tính đang sử dụng ?**

- Địa chỉ trang web đã chọn ở Bước 8: *118.69.123.142*

- Địa chỉ máy tính đang sử dụng: *192.168.1.3*

- Vậy số lượng gói tin trao đổi là 20, khối lượng dữ liệu là 14kB

A screenshot of a computer

Description automatically generated