|  |
| --- |
| HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  **KHOA CÔNG NGHỆ THÔNG TIN 1** |
|  |
| **BÀI THỰC HÀNH 15**  **THỰC TẬP CƠ SỞ** |
| **Họ và tên : Đinh Quang Hiếu**  **Mã sinh viên: B19DCAT065**  **Giảng viên giảng dạy: Hoàng Xuân Dậu** |
| **HÀ NỘI, THÁNG 5/2022** |

## Bài 15: Lập trình client/server để trao đổi thông tin an toàn

**I. Giới thiệu chung**

### 1. Mục đích

**•** Tìm hiểu về cơ chế client/server, lập trình client/server dựa trên socket, cài đặt giao thức đơn giản để trao đổi thông tin an toàn.

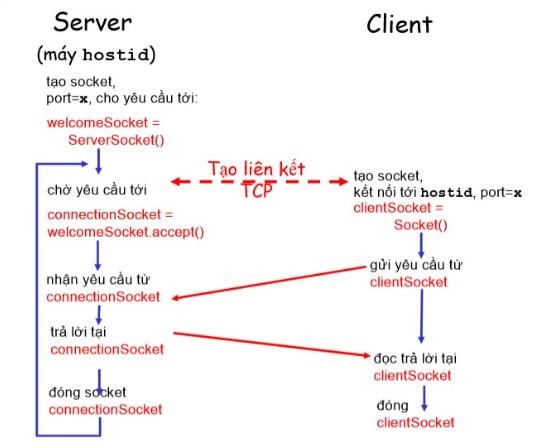
### 2. Yêu cầu

* Tìm hiểu lý thuyết o Socket

▪ Là điểm cuối (end-point) trong liên kết truyền thông hai chiều (two-way communication) biểu diễn kết nối giữa Client – Server ▪ Phân loại Socket:

* Stream Socket: Dựa trên giao thức TCP, thiết lập giao tiếp 2 chiều; đảm bảo dữ liệu được truyền đến nơi nhận một cách đáng tin cậy, đúng tuần tự.
* Datagram Socket: Dựa trên giao thức UDP, không yêu cầu có sự thiết lập kết nối giữa 2 process; ưu điểm là tốc độ giao thức nhanh.

o Lập trình socket với TCP



• Chuẩn bị

o Phần mềm Wireshark

o Môi trường Python

### 3. Các bước thực hiện

#### 3.1 Lập trình client và server với TCP socket

1. *Các bước thực hiện* o Lập trình client

Text

Description automatically generated

Text

Description automatically generated

* + Lập trình server

Text

Description automatically generated

Text

Description automatically generated

* + Chạy server sau đó chạy client
  + Client gửi thông điệp cá nhận hóa cho server: “Hello, I am B19DCAT205 client.”
  + Server nhận được hiển thị thông điệp nhận được và gửi lại client thông điệp: server gửi lại “Hello, I am B19DCAT205 server”

A screenshot of a computer

Description automatically generated with medium confidence

* + Sử dụng Wireshark để bắt các thông tin đã gửi từ client đến server và ngược lại

Graphical user interface, text

Description automatically generated

1. *Kết quả cần đạt được*

o Chạy thành công client và server theo mục tiêu ban đầu

o Bắt được các bản tin trao đổi giữa client và server trong Wireshark

#### 3.2 Trao đổi thông điệp giữa client và server và đảm bảo tính toàn vẹn của thông điệp khi trao đổi

*a) Các bước thực hiện* o Từ client và server, sửa đổi để sao cho: khi gửi thông điệp sẽ gửi kèm theo giá trị băm của (thông điệp+key) để phía bên kia kiểm tra xác minh tính toàn vẹn. Hai bên có thể thống nhất một giá trị key trước đó.

Tạo hash module trong Python:

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

* Thay đổi giá trị key tại client và thực hiện gửi lại, nếu không đáp ứng tính toàn vẹn cần thông báo: “The received message has lost its integrity.”

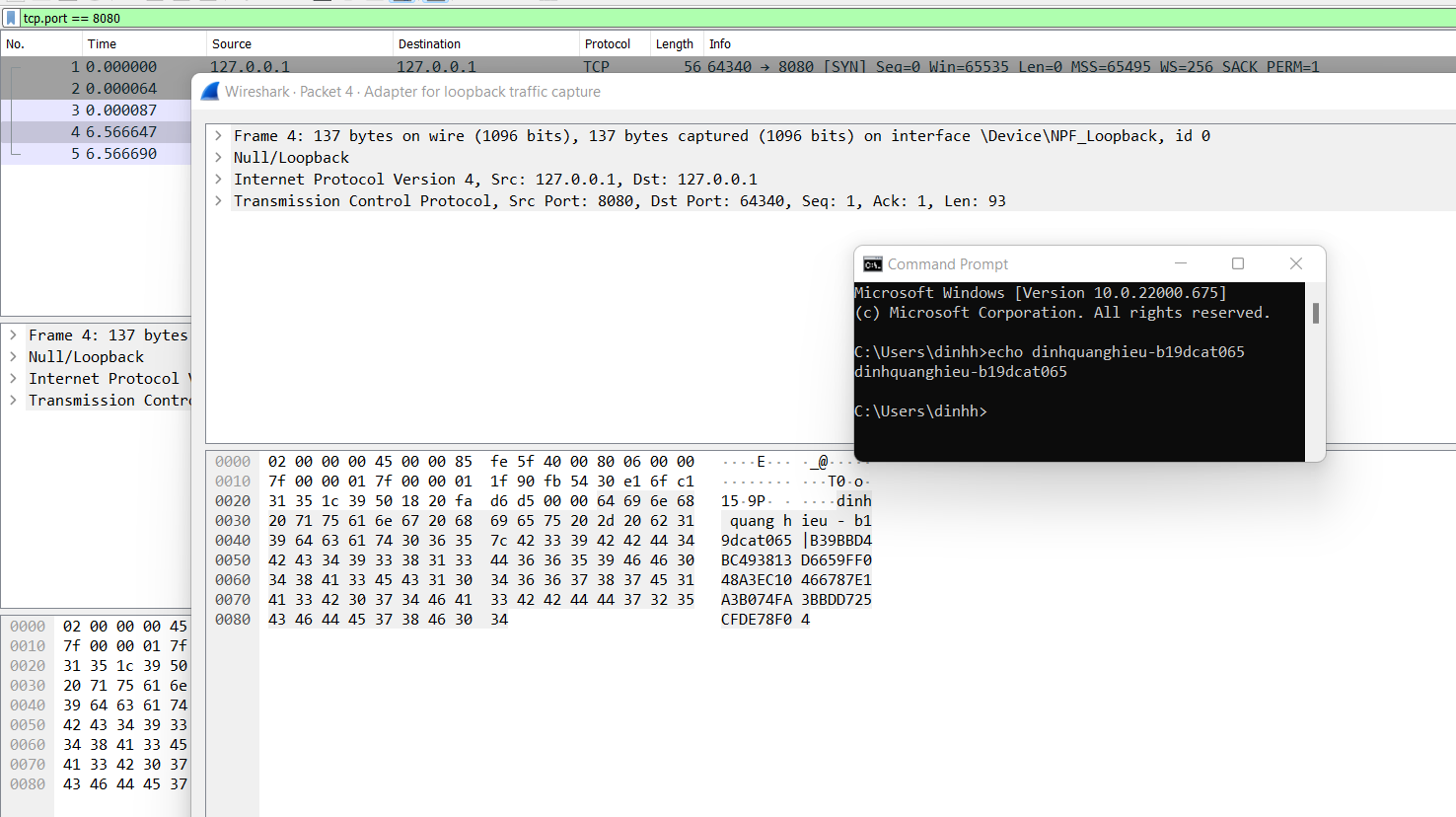
A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

* Bắt được các bản tin trao đổi giữa client và server trong Wireshark

 *b) Kết quả cần đạt được*

o Chạy thành công client và server theo mục tiêu ban đầu, bắt được các bản tin trao đổi giữa client và server trong Wireshark