



Xây dựng phần mềm Giám sát truy cập mạng

Đồ án Cơ Sở Ngành Mạng - GVHD Ts. Huỳnh Công Pháp

Sinh viên: NGUYỄN HỮU HÙNG
Lớp: 13T1
Nhóm: 12

Nội dung



Giới thiệu đề tài



Cơ sở lý thuyết



Triển khai đề tài



Kết quả triển khai



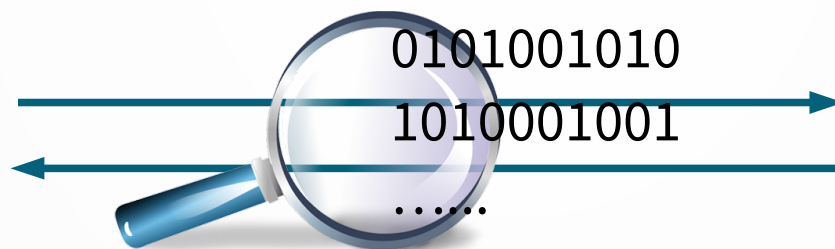
Kết luận và hướng phát triển

Giới thiệu đề tài

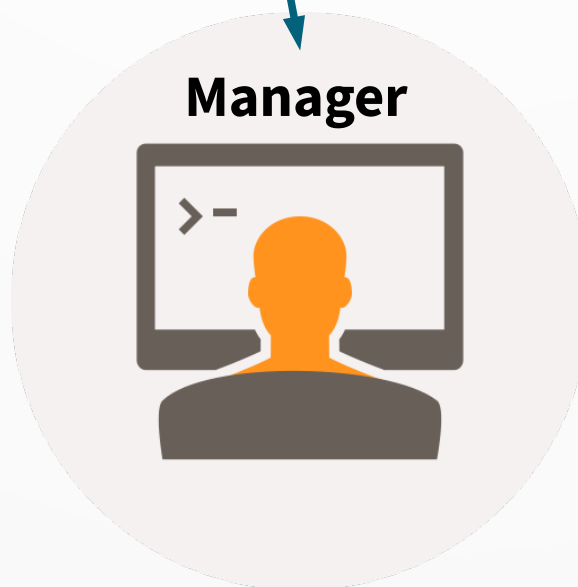


- Cùng với sự phát triển không ngừng của Công nghệ máy tính, mạng máy tính cũng trở nên ngày càng phổ biến và rộng rãi. Điều đó cũng có nghĩa là công việc quản lý sự truy cập của người dùng cũng trở nên phức tạp và khó khăn hơn.
- Bằng những kiến thức tích lũy được, những hiểu biết cơ bản về mạng máy tính và hệ điều hành, em đã xây dựng phần mềm Giám sát truy cập mạng nhằm phục vụ công việc quản lý truy cập của các user trong mạng LAN.

Giới thiệu đề tài



Monitoring



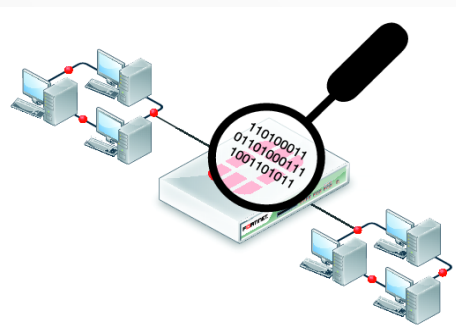
Cơ sở lý thuyết



Lý thuyết về Nguyên lý hệ điều hành



Hệ điều hành Linux, lập trình C/C++ trên linux



Hook network, bắt gói tin

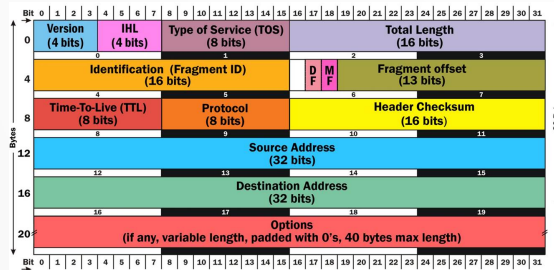


Lập trình đa luồng

Cơ sở lý thuyết

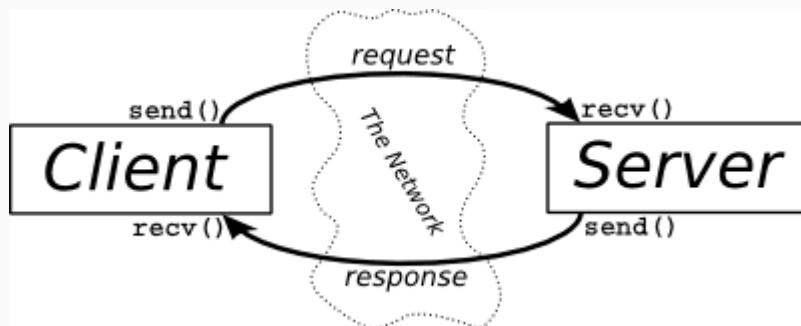


Lý thuyết về Lập trình mạng



Lý thuyết về các giao thức mạng

Cấu trúc của các gói tin IP, TCP, UDP, ICMP, MAC



Lập trình socket với mô hình client- server

Triển khai đề tài



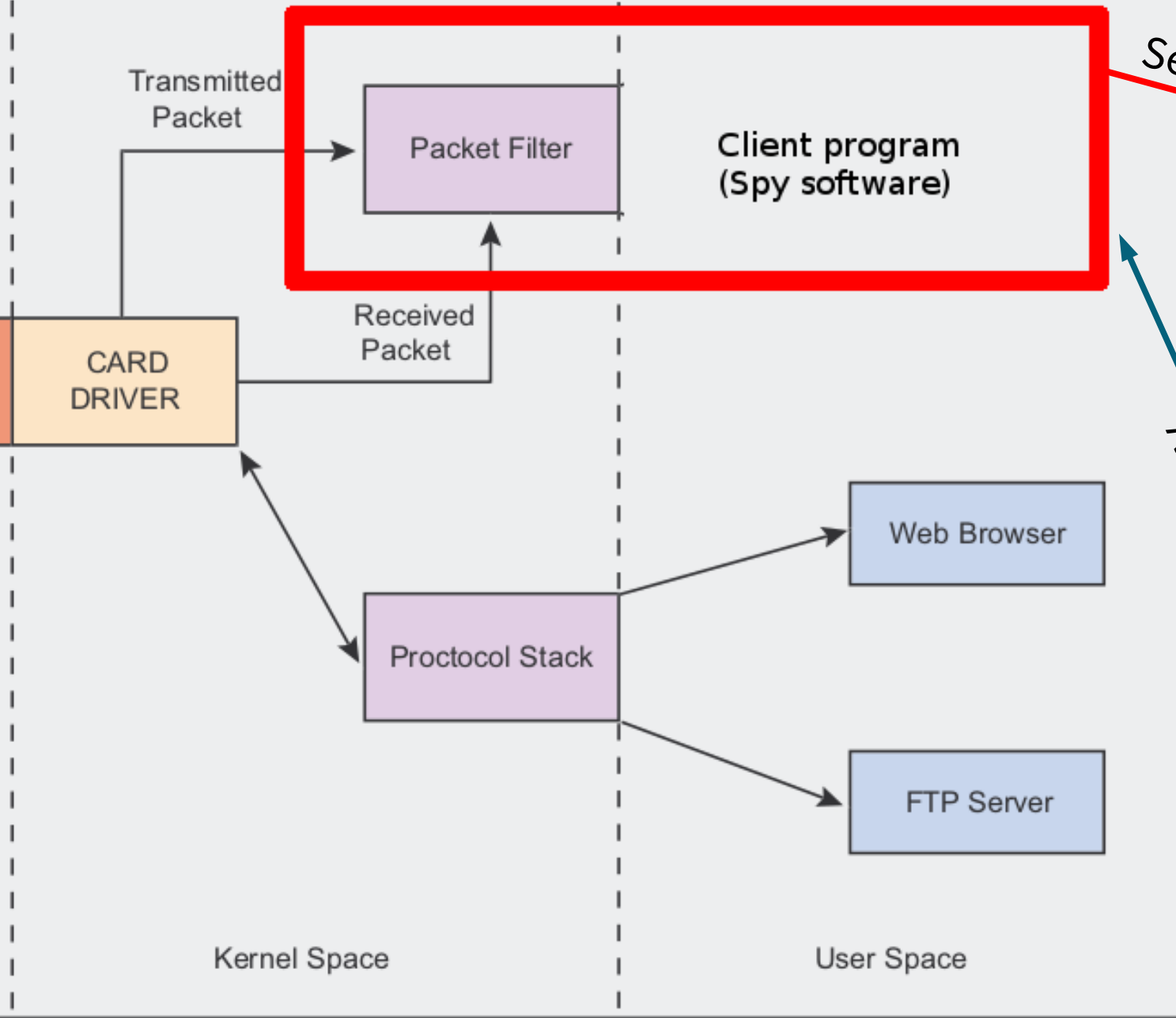
Chương trình SERVER



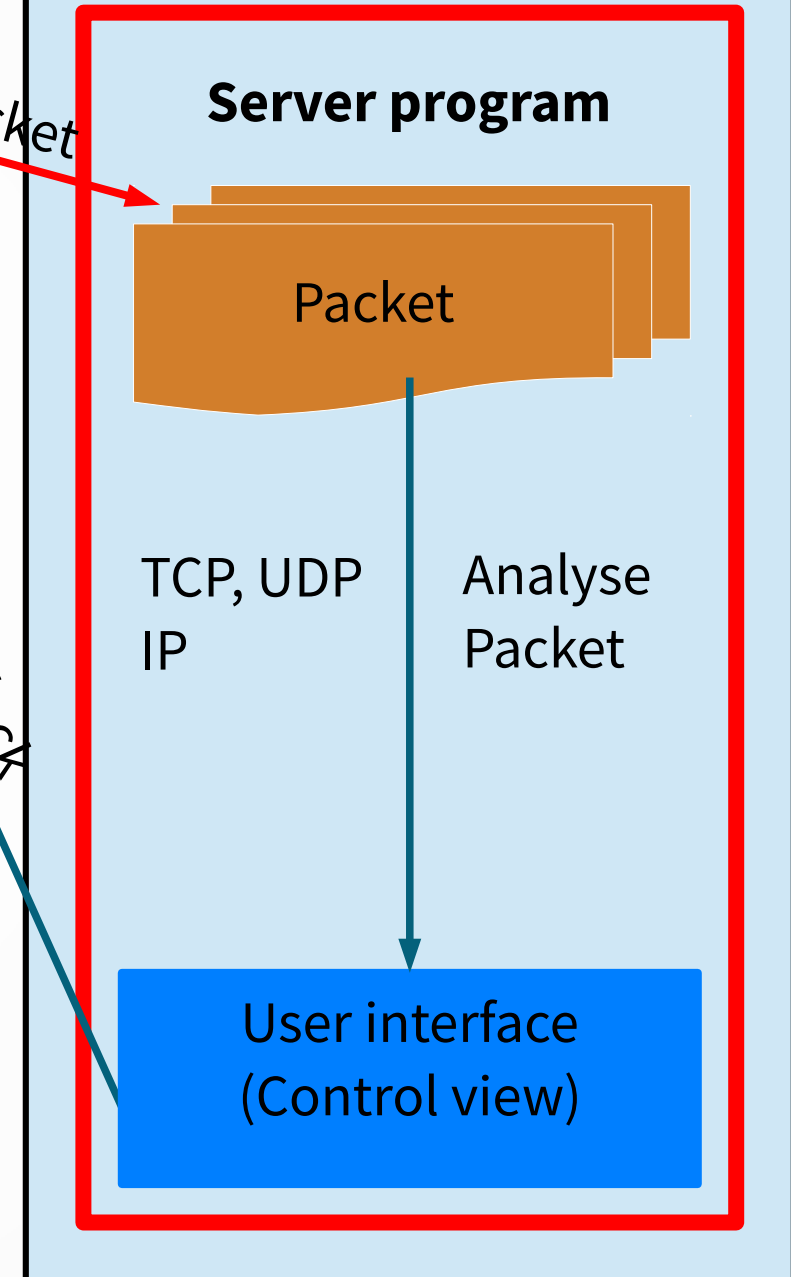
Được xây dựng bằng ngôn ngữ java, có giao diện, thực hiện các nhiệm vụ sau:

- *Tiếp nhận kết nối của các chương trình client trên máy khách*
- *Thu thập dữ liệu trả về từ chương trình client (trong đó có các gói tin mà chương trình client hook được từ máy khách)*
- *Phân tích các gói tin bắt được từ dạng thô sang dạng đọc được*
- *Ra lệnh điều khiển chương trình client chặn hoặc bỏ chặn máy khách truy cập đến địa chỉ ip nào đó*
- *Truy vấn thông tin của địa chỉ ip*

User computer



Monitor computer



Triển khai đề tài

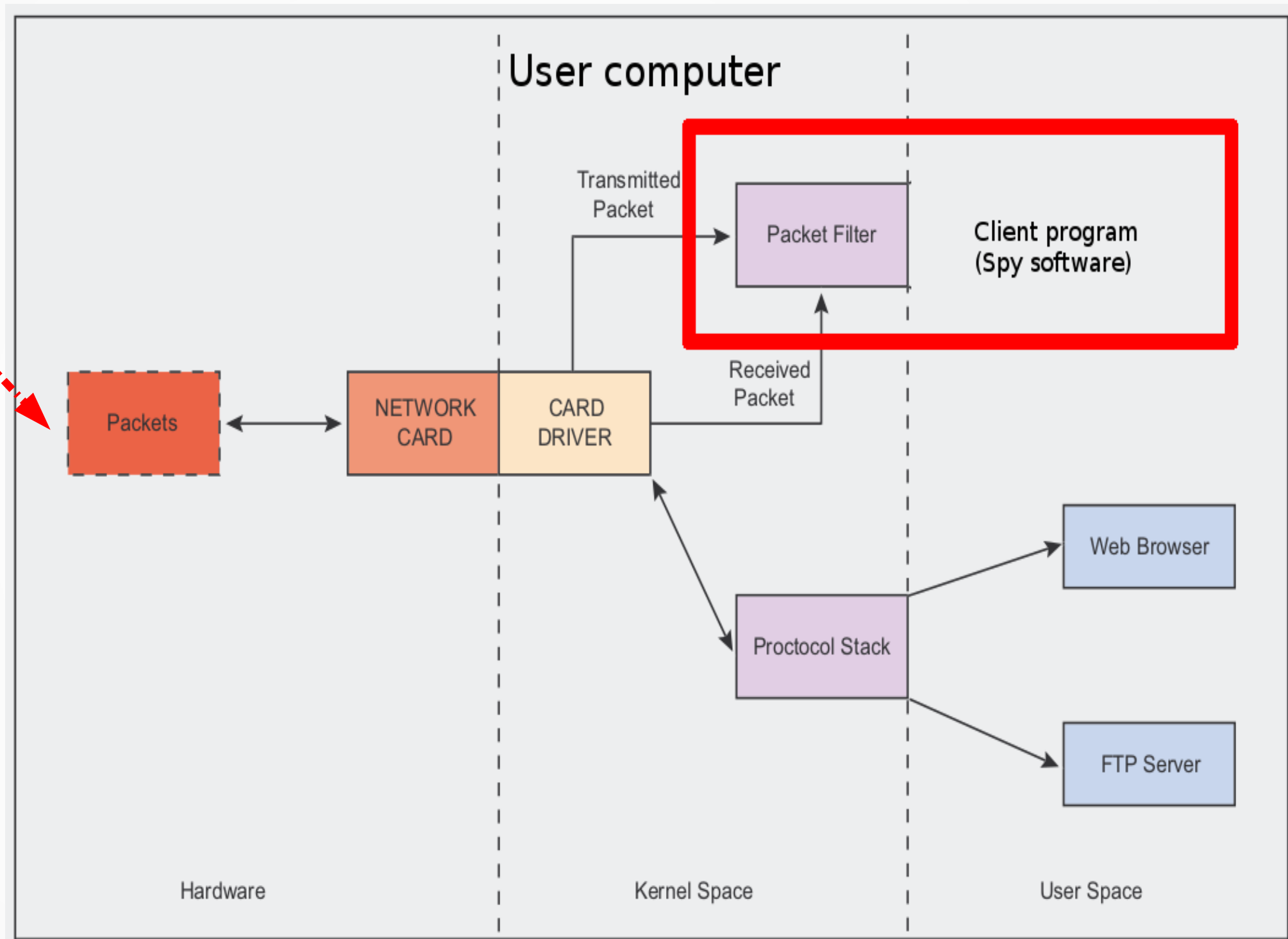
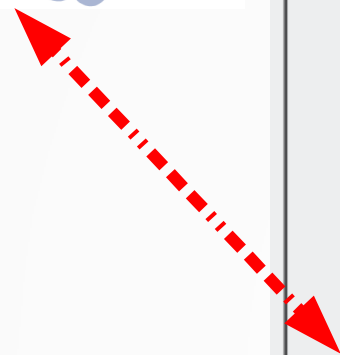


Chương trình CLIENT

Được xây dựng bằng ngôn ngữ C/C++, cho phép chạy ngầm trên máy khách, thực hiện các nhiệm vụ sau:

- *Mở cổng kết nối đến chương trình server, sẵn sàng nghe lệnh từ server*
- *Gửi danh sách các device có thể bắt gói tin đến chương trình server*
- *Trực tiếp bắt gói tin giao tiếp của máy khách và gửi đến server*
- *Tiến hành chặn, bỏ chặn địa chỉ ip theo lệnh của chương trình server*





Kết quả triển khai



Chương trình SERVER

Monitor



List of hosts:

[Host] localhost

localhost

Search IP



IP Address:

Capture packets



Interface:

wlan0



Filter:

ip



Visited IP address:

No.	IP address	Host name
0	192.168.1.51	android-b3b9b5d991bc115d
1	224.0.0.251	224.0.0.251
2	192.168.1.19	192.168.1.19
3	192.168.1.1	192.168.1.1
4	239.255.255.250	239.255.255.250
5	52.77.150.113	ec2-52-77-150-113.ap-southeast-1.compute.amaz...
6	157.240.13.35	edge-star-mini-shv-02-sin6.facebook.com
7	52.221.146.195	ec2-52-221-146-195.ap-southeast-1.compute.ama...
8	224.0.0.22	igmp.mcast.net
9	217.16.180.236	217.16.180.236
10	0.0.0.0	0.0.0.0
11	255.255.255.255	255.255.255.255
12	192.168.1.57	nhan-ngoc



Packet data:

[MAC Header]		
	-Destination MAC:	3c:33:00:55:f2:d0
	-Source MAC:	ac:64:62:d6:64:28
	-Ether type:	2048
[IP Header]		
	-Version:	4
	-Header length:	5 DWORDS or 20 BYTES
	-Type of service:	32
	-Total length:	52 BYTES
	-Identification:	51175
	-Do not fragment:	1
	-More fragment:	0
	-Fragment offset:	0
	-Time to live:	239
	-Protocol:	6



Packet header:

No.	Sour MAC	Dest MAC	Sour IP	Dest IP	Sour port	Dest port	Protocol	Length	Info
0	dc:6d:cd:88:68:4f	01:00:5e:00:00:fb	192.168.1.51	224.0.0.251	5353	5353	UDP	121	
1	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	44322	UDP	117	
2	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	44322	UDP	117	
3	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	33687	UDP	117	
4	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	52.221.146.195	44994	443	TCP	52	[ACK]=3919796848; [SEQ]=36746...
5	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	52.221.146.195	192.168.1.19	443	44994	TCP	52	[ACK]=3674699174; [SEQ]=39197...
6	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	217.16.180.236	192.168.1.19	443	40646	TCP	52	[ACK]=1147110219; [SEQ]=12120...
7	60:92:17:00:b9:82	ff:ff:ff:ff:ff:ff	0.0.0.0	255.255.255.255	68	67	UDP	328	
8	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	192.168.1.1	47048	53	UDP	66	
9	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	47048	UDP	115	
10	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	192.168.1.1	60017	53	UDP	74	
11	60:92:17:00:b9:82	01:00:5e:00:00:fb	192.168.1.57	224.0.0.251	5353	5353	UDP	98	
12	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	60017	UDP	109	
13	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	192.168.1.1	44104	53	UDP	71	

[Host] localhost

Search IP

IP Address:

Capture packets

Interface:
wlan0

Filter:
ip


▶

■

📁


↺↻

Khung điều khiển chương trình client ở máy khách

 Visited IP address:

No.	IP address	Host name
0	192.168.1.51	android-b3b9b5d991bc115d
1	224.0.0.251	224.0.0.251
2	192.168.1.19	192.168.1.19
3	192.168.1.1	192.168.1.1
4	239.255.255.250	239.255.255.250
5	52.77.150.113	ec2-52-77-150-113.ap-southeast-1.compute.amaz...
6	157.240.13.35	edge-star-mini-shv-02-sin6.facebook.com
7	52.221.146.195	ec2-52-221-146-195.ap-southeast-1.compute.ama...
8	224.0.0.22	igmp.mcast.net
9	217.16.180.236	217.16.180.236
10	0.0.0.0	0.0.0.0
11	255.255.255.255	255.255.255.255
12	192.168.1.57	nhan-ngoc


Danh sách các địa chỉ ip mà máy khách truy cập

 Packet data:

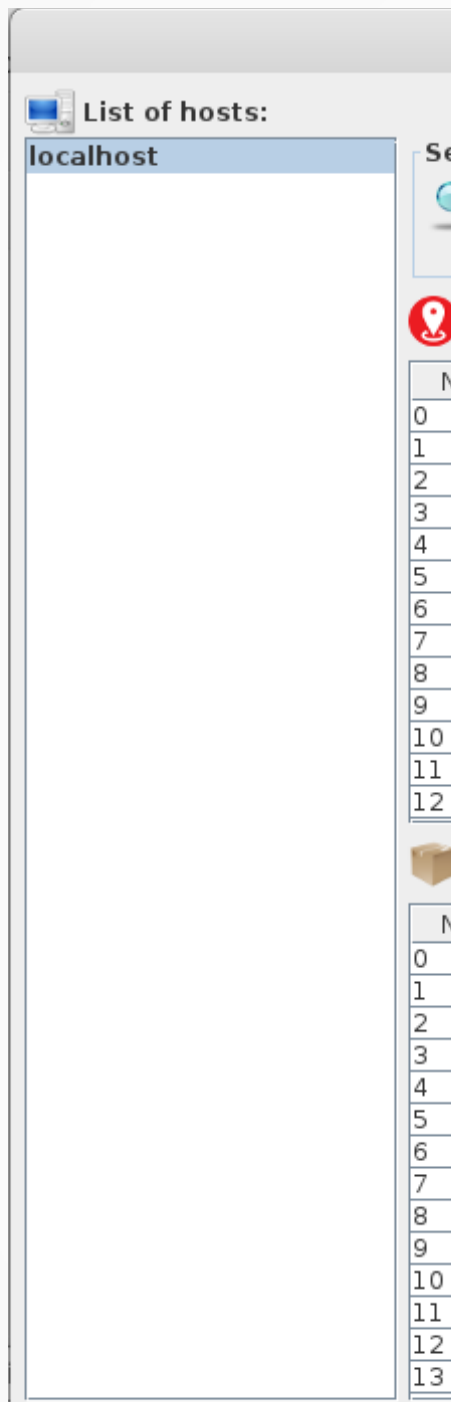
[MAC Header]		
	-Destination MAC:	3c:33:00:55:f2:d0
	-Source MAC:	ac:64:62:d6:64:28
	-Ether type:	2048
[IP Header]		
	-Version:	4
	-Header length:	5 DWORDS or 20 BYTES
	-Type of service:	32
	-Total length:	52 BYTES
	-Identification:	51175
	-Do not fragment:	1
	-More fragment:	0
	-Fragment offset:	0
	-Time to live:	239
	-Protocol:	6

Cấu trúc của gói tin phân tích được

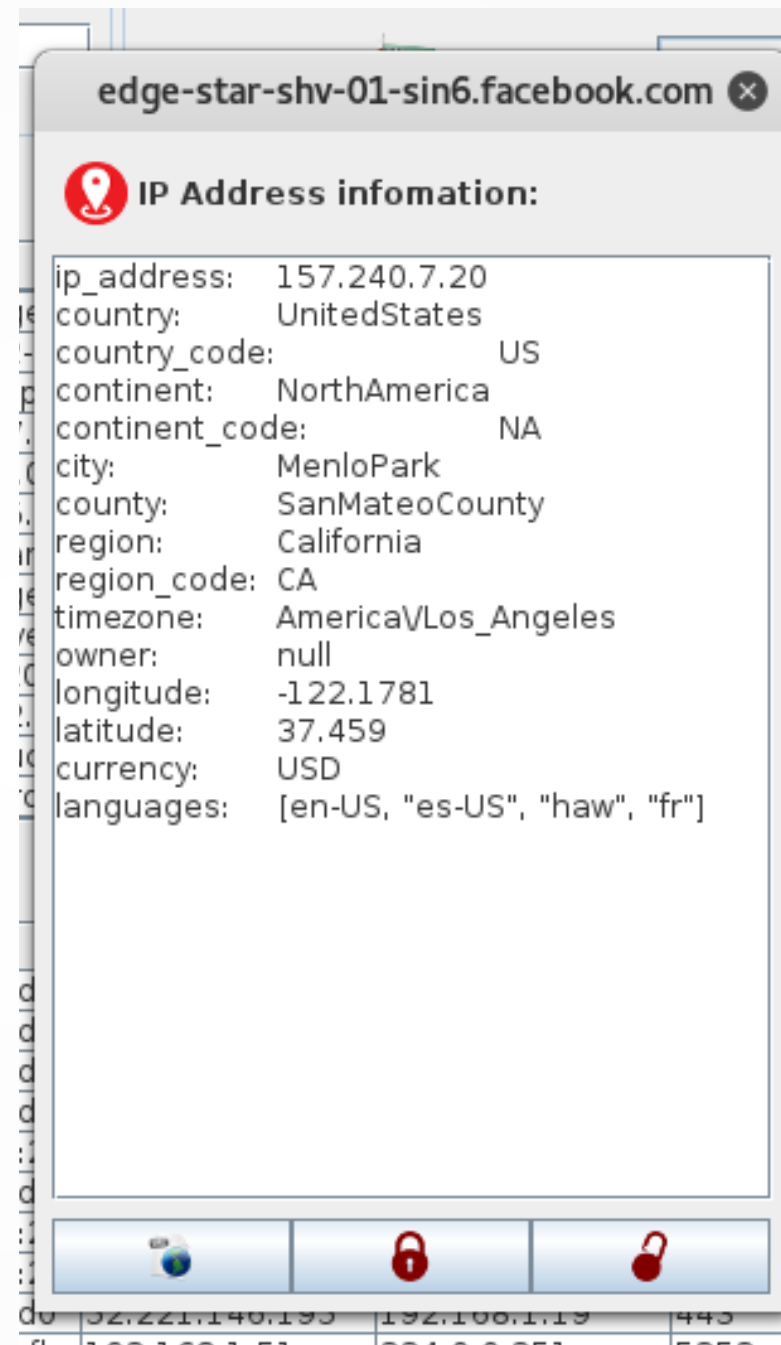
Danh sách các gói tin gửi về từ chương trình client

 Packet header:

No.	Sour MAC	Dest MAC	Sour IP	Dest IP	Sour port	Dest port	Protocol	Length	Info
0	dc:6d:cd:88:68:4f	01:00:5e:00:00:fb	192.168.1.51	224.0.0.251	5353	5353	UDP	121	
1	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	44322	UDP	117	
2	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	44322	UDP	117	
3	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	33687	UDP	117	
4	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	52.221.146.195	44994	443	TCP	52	[ACK]=3919796848; [SEQ]=36746...
5	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	52.221.146.195	192.168.1.19	443	44994	TCP	52	[ACK]=3674699174; [SEQ]=39197...
6	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	217.16.180.236	192.168.1.19	443	40646	TCP	52	[ACK]=1147110219; [SEQ]=12120...
7	60:92:17:00:b9:82	ff:ff:ff:ff:ff:ff	0.0.0.0	255.255.255.255	68	67	UDP	328	
8	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	192.168.1.1	47048	53	UDP	66	
9	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	47048	UDP	115	
10	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	192.168.1.1	60017	53	UDP	74	
11	60:92:17:00:b9:82	01:00:5e:00:00:fb	192.168.1.57	224.0.0.251	5353	5353	UDP	98	
12	ac:64:62:d6:64:28	3c:33:00:55:f2:d0	192.168.1.1	192.168.1.19	53	60017	UDP	109	
13	3c:33:00:55:f2:d0	ac:64:62:d6:64:28	192.168.1.19	192.168.1.1	44104	53	UDP	71	



Danh sách các
máy khách
trong mạng LAN



Giao diện
truy vấn
thông tin
của 1 địa chỉ ip

```
IP Header
|-IP Version      : 4
|-IP Header Length : 5 DWORDS or 20 Bytes
|-Type Of Service : 0
|-IP Total Length  : 62 Bytes(Size of Packet)
|-Identification   : 60646
|-TTL              : 64
|-Protocol         : 17
|-Checksum         : 15775
|-Source IP        : 192.168.1.13
|-Destination IP   : 203.113.131.2
```

```
UDP Header
|-Source Port      : 58416
|-Destination Port : 53
|-UDP Length       : 42
|-UDP Checksum     : 16932
```

```
Data Payload
.....www
.facebook.com...
..
```

Cấu trúc của một gói tin UDP
đã được phân tích bởi chương trình client

Kết quả triển khai



Chương trình CLIENT

Nội dung của một gói tin thô mà client hook được từ card mạng

IP Header

```
45 00 00 3E EC E6 40 00 40 11 3D 9F C0 A8 01 0D
CB 71 83 02
```

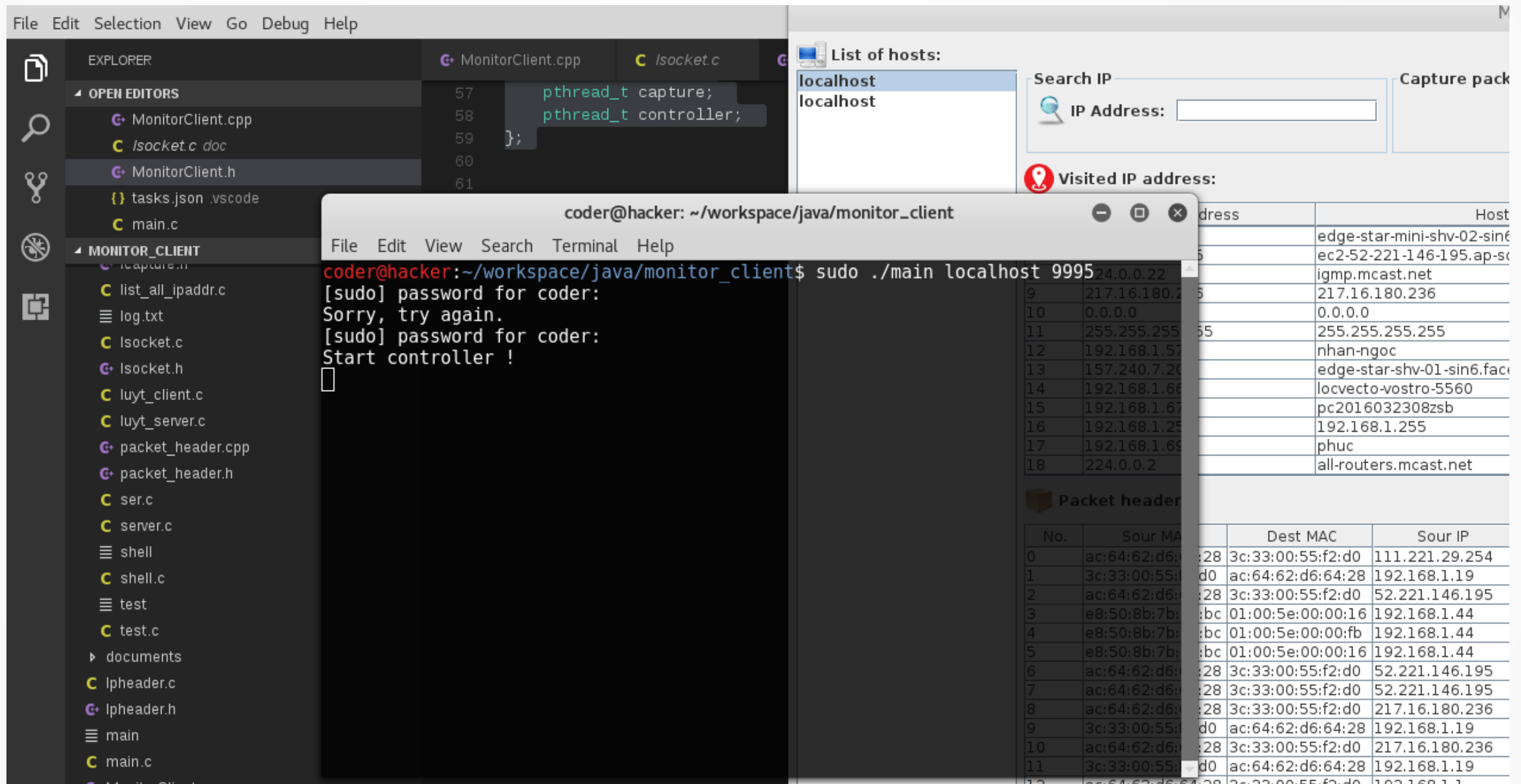
UDP Header

```
E4 30 00 35 00 2A 42 24
```

Data Payload

```
D2 E6 01 00 00 01 00 00 00 00 00 00 03 77 77 77
08 66 61 63 65 62 6F 6F 6B 03 63 6F 6D 00 00 01
00 01
```

Chương trình client (không có giao diện) được chạy bằng dòng lệnh trên một máy ảo



Kết luận và hướng phát triển



Qua việc xây dựng một phần mềm như thế này, em đã có thể tiếp xúc những trường hợp thực tế xảy ra trong kĩ thuật lập trình với hệ điều hành Linux cũng như có cơ hội để hiểu thêm về nguyên lý hoạt động của đường truyền, cấu trúc của gói tin như thế nào

Phần mềm giám sát mạng này có thể được tiếp tục phát triển để áp dụng cho mạng Internet, mạng diện rộng bằng cách thông qua một máy chủ có địa chỉ IP public. Có thể phát triển thêm nhiều chức năng như hiển thị vị trí địa chỉ IP trên Google Map, chức năng cảnh báo cho người dùng máy khách đang truy cập nội dung không hợp lệ...

Kết thúc CẢM ƠN ĐÃ THEO DÕI

Đồ án Cơ Sở Ngành Mạng - GVHD Ts. Huỳnh Công Pháp

Sinh viên: NGUYỄN HỮU HÙNG
Lớp: 13T1
Nhóm: 12