

Tutorial

Current:

username: fptlab

password: 111111

▼ SSH enable connection to Car

- Cài đặt SSH
 - Window

[Get started with OpenSSH for Windows | Microsoft Learn](#)



Enable OpenSSH for Windows Server 2025

Starting with Windows Server 2025, OpenSSH is now installed by default. You can also enable or disable the `sshd` service in Server Manager.

GUI PowerShell

To enable SSHD using Server Manager:

1. In **Server Manager**, on the navigation pane to the left, select **Local Server**.
2. In the **Properties** window, locate **Remote SSH Access**.
3. Select **Disabled** to enable the OpenSSH service.

Note

If you need to allow or restrict specific users or groups from using OpenSSH for remote access, add them to the **OpenSSH Users** user group.

- Ubuntu

```
sudo apt-get install openssh-server
```

- Sử dụng màn hình rời, bàn phím, chuột connect vào Car và đăng nhập wifi thủ công
 - Sau khi Car connect wifi



wlan0: 192.168.1.103 ⇒ nhớ IP address này để connect SSH với Car

- Mở Terminal ở máy Local(your laptop) và thực hiện ssh theo cú pháp sau, gõ yes và nhập mật khẩu cho username nếu có yêu cầu

```
ssh <username>@<IP_adress>  
ví dụ: ssh fptlab@192.168.1.103
```

Màn hình ssh thành công ở window(ubuntu is same)

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\monsi> ssh fptlab@192.168.1.103
fptlab@192.168.1.103's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.9.201-tegra aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Nov  7 12:16:24 2024 from 192.168.1.250
(env) fptlab@fptlab-desktop:~$ |

```

Nhập mật khẩu cho username đã setting ở bước 1

▼ If got Error:

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: POSSIBLE DNS SPOOFING DETECTED!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The ECDSA host key for raspberrydonkey has changed,
and the key for the corresponding IP address 2402:800:63a5:cffb:abff:5897:b954:ff50
is unknown. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:5rAiVNRBQuLL81WqrLDiAb5vuxlD1vPLfv5s5fZLUZM.
Please contact your system administrator.
Add correct host key in C:\\Users\\PhucPhan/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in C:\\Users\\PhucPhan/.ssh/known_hosts:3
ECDSA host key for raspberrydonkey has changed and you have requested strict checking.
Host key verification failed.

```

When you create a new instance, it is a new virtualized computer. So, when you return to the same IP address, your computer recognizes that it's not the same computer as before. While this can, in some scenarios, indicate malicious activity as the warning indicates, in this scenario, it is expected and fine.

Solution: Edit the .ssh/known_hosts file

- Chạy lệnh để edit file
~/.ssh/known_hosts
- Xóa dòng chứa hostname của Car

```
raspberrypi,2402:800:63a5:e7bb:30a:7924:31cb:2400 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAAE
rasp,2402:800:63a5:e7bb:e65f:1ff:feaf:bbd5 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGmRfE
raspberryydonkey,2402:800:63a5:cfb:259d:8eee:22d1:d9ae ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNT
```

or using code below

```
ssh-keygen -R [IP_ADDRESS]
```

▼ Collect Data for training

- After connect ssh to car run this command in terminal :

```
cd ~/mycar
```

```
python manage.py drive --js
```

- Access the web UI through

```
<ip_address>:8887  
EX: 192.168.1.103:8887
```

- Controller:

```

self.button_down_trigger_map = {
    'a_button': self.toggle_mode,
    'b_button': self.toggle_manual_recording,
    'x_button': self.erase_last_N_records,
    'y_button': self.emergency_stop,
    'right_shoulder': self.increase_max_throttle,
    'left_shoulder': self.decrease_max_throttle,
    'options': self.toggle_constant_throttle,
}

self.axis_trigger_map = {
    'left_stick_horz': self.set_steering,
    'right_stick_vert': self.set_throttle,
    # Forza Mode
    'right_trigger': self.magnitude(),
    'left_trigger': self.magnitude(reversed = True),
}

```

Some caution buttons:

- R1, R2: Adjust throttle scale(tăng giảm tốc độ)
- Y: Emergency stop(dừng khẩn cấp)
- B: Start recording (take data)(bắt đầu ghi ảnh vào data folder)
- X: Delete last 100 records(xóa 100 ảnh gần đây nhất)
- A: Change mode (User, Half-Auto, Full-Auto)

Khuyến khích số lượng record ≥ 20000

▼ Training

- Chuyển data sang Local PC để train(window ubuntu same)

Trong terminal ở localPC(your laptop after ssh to Car) use sftp to copy your data folder

```
sftp username@hostname  
ex: sftp fptlab@192.168.1.103
```

```
lcd /path/to/store/data/in/local/PC  
ex: lcd C:\Users\<YourUsername>\Downloads
```

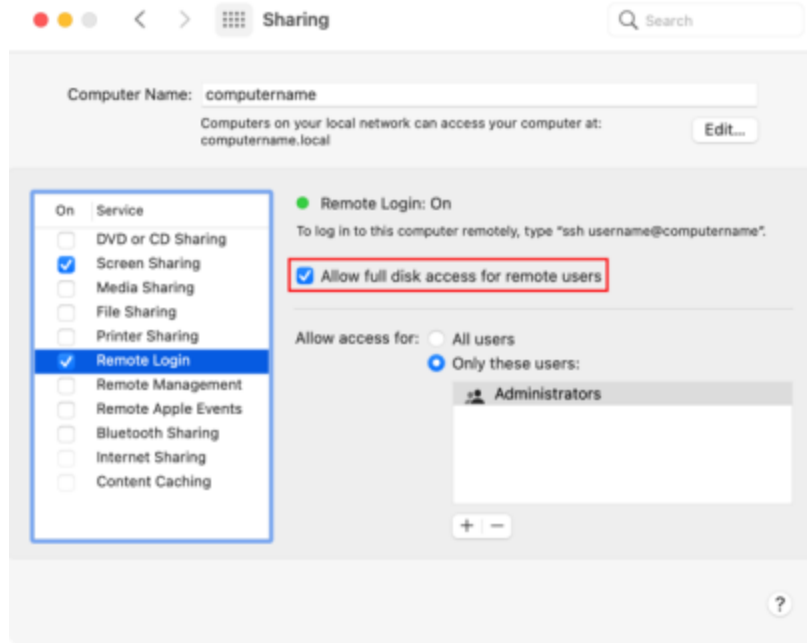
```
get /path/to/data/in/car/filename.tar.gz  
ex: get mycar/data/data.tar.gz
```

- o MacOS

<https://derflounder.wordpress.com/2021/09/29/enabling-full-disk-access-for-ssh-on-macos-big-sur-using-a-management-profile/>

Enabling full disk access for SSH on macOS Big Sur using a management profile

When connecting via SSH to a remote Mac running macOS Big Sur, Apple's user-level privacy controls apply. You can access data in the home folder of the account you're using to connect, but you can't access or alter protected data in other account's home folders. For most use cases, this is fine.



- **Error: CUDNN_STATUS_INTERNAL_ERROR**

Set the `TF_FORCE_GPU_ALLOW_GROWTH` environment variable to true.

In your terminal, run this command.

```
export TF_FORCE_GPU_ALLOW_GROWTH=true
```

- Upload file nén data lên gg drive
- Truy cập google colab(colab.google) upload file Training_Model.ipynb và train
 - chọn runtime GPU T4
 - Run all

▼ Copy model back to car

- Dùng sftp để put trained model pilot back to car.

```
sftp username@hostname
```

```
lcd path/to/trained/Model/model.tflite or model.h5
```

```
put model.tflite /path/to/directory/store/model/in/car
```

- Đặt xe vào vị trí thuận lợi cho việc lái xe.

▼ Run Car

```
cd ~/mycar/
```

Web:

```
<ip_address>:8887
```

Chạy web thường

```
python manage.py drive
```

Chạy với joystick

```
python manage.py drive --js
```

Chạy model tự động lái(Auto Pilot)

```
python manage.py drive --model ~/mycar/models/mypilot.h5  
or  
python manage.py drive --model ~/mycar/models/mypilot.tflite --type  
tflite_linear
```