

# Homework #3

School ID: 202355517

Name: 권민규

## 1. Plug your USB memory stick into your Linux Box and then monitor what happens on you system with `tail -f ....` command

우분투에서 usb 연결 시 이하의 파일 두 곳에 로그가 남는다고 한다.

- `/var/log/syslog`
- `/var/log/kern.log`

```
sudo tail -f /var/log/syslog
```

해당 명령어를 작동시켜놓은 채 USB를 연결하면 다음과 같은 로그가 남는다.

```
seworl@seworl ~$ sudo tail -f /var/log/syslog
[sudo] password for seworl:
Apr  3 01:01:30 Seworl systemd[1]: Starting Time & Date Service...
Apr  3 01:01:30 Seworl dbus-daemon[163]: [system] Successfully activated service 'org.freedesktop.timedate1'
Apr  3 01:01:30 Seworl systemd[1]: Started Time & Date Service.
Apr  3 01:01:32 Seworl snapd[187]: storehelpers.go:791: cannot refresh: snap has no updates available: "bare", "core22", "gtk-common-themes", "snapd", "ubuntu-desktop-installer"
Apr  3 01:02:00 Seworl systemd[1]: systemd-timedated.service: Deactivated successfully.
Apr  3 01:03:40 Seworl kernel: [ 439.038179] vhci_hcd: connection closed
Apr  3 01:03:40 Seworl kernel: [ 439.038466] vhci_hcd: stop threads
Apr  3 01:03:40 Seworl kernel: [ 439.038470] vhci_hcd: release socket
Apr  3 01:03:40 Seworl kernel: [ 439.038474] vhci_hcd: disconnect device
Apr  3 01:03:40 Seworl kernel: [ 439.038549] usb 1-1: USB disconnect, device number 2
Apr  3 01:04:24 Seworl kernel: [ 482.811703] vhci_hcd vhci_hcd.0: pdev(0) rhport(0) sockfd(3)
Apr  3 01:04:24 Seworl kernel: [ 482.811707] vhci_hcd vhci_hcd.0: devid(131079) speed(3) speed_str(high-speed)
Apr  3 01:04:24 Seworl kernel: [ 482.811732] vhci_hcd vhci_hcd.0: Device attached
Apr  3 01:04:24 Seworl kernel: [ 483.160309] usb 1-1: new high-speed USB device number 3 using vhci_hcd
Apr  3 01:04:24 Seworl kernel: [ 483.310505] usb 1-1: SetAddress Request (3) to port 0
Apr  3 01:04:24 Seworl kernel: [ 483.344676] usb 1-1: New USB device found, idVendor=0781, idProduct=5567, bcdDevice= 1.00
Apr  3 01:04:24 Seworl kernel: [ 483.344680] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Apr  3 01:04:24 Seworl kernel: [ 483.344681] usb 1-1: Product: Cruzer Blade
Apr  3 01:04:24 Seworl kernel: [ 483.344682] usb 1-1: Manufacturer: SanDisk
Apr  3 01:04:24 Seworl kernel: [ 483.344683] usb 1-1: SerialNumber: 04024818111723231136
```

```
sudo tail -f /var/log/kern.log
```

```

seworl@seworl ~$ sudo tail -f /var/log/kern.log
Apr  3 01:04:24 SeworL kernel: [ 483.344676] usb 1-1: New USB device found, idVendor=0781, idProduct=5567, bcdDevice= 1.00
Apr  3 01:04:24 SeworL kernel: [ 483.344680] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Apr  3 01:04:24 SeworL kernel: [ 483.344681] usb 1-1: Product: Cruzer Blade
Apr  3 01:04:24 SeworL kernel: [ 483.344682] usb 1-1: Manufacturer: SanDisk
Apr  3 01:04:24 SeworL kernel: [ 483.344683] usb 1-1: SerialNumber: 04024818111723231136
Apr  3 01:05:33 SeworL kernel: [ 551.643865] vhci_hcd: connection closed
Apr  3 01:05:33 SeworL kernel: [ 551.643999] vhci_hcd: stop threads
Apr  3 01:05:33 SeworL kernel: [ 551.644003] vhci_hcd: release socket
Apr  3 01:05:33 SeworL kernel: [ 551.644008] vhci_hcd: disconnect device
Apr  3 01:05:33 SeworL kernel: [ 551.644039] usb 1-1: USB disconnect, device number 3
Apr  3 01:05:53 SeworL kernel: [ 571.612771] vhci_hcd vhci_hcd.0: pdev(0) rhport(0) sockfd(3)
Apr  3 01:05:53 SeworL kernel: [ 571.612775] vhci_hcd vhci_hcd.0: devid(131079) speed(3) speed_str(high-speed)
Apr  3 01:05:53 SeworL kernel: [ 571.612801] vhci_hcd vhci_hcd.0: Device attached
Apr  3 01:05:53 SeworL kernel: [ 571.960411] usb 1-1: new high-speed USB device number 4 using vhci_hcd
Apr  3 01:05:53 SeworL kernel: [ 572.110382] usb 1-1: SetAddress Request (4) to port 0
Apr  3 01:05:53 SeworL kernel: [ 572.145682] usb 1-1: New USB device found, idVendor=0781, idProduct=5567, bcdDevice= 1.00
Apr  3 01:05:53 SeworL kernel: [ 572.145686] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Apr  3 01:05:53 SeworL kernel: [ 572.145687] usb 1-1: Product: Cruzer Blade
Apr  3 01:05:53 SeworL kernel: [ 572.145688] usb 1-1: Manufacturer: SanDisk
Apr  3 01:05:53 SeworL kernel: [ 572.145689] usb 1-1: SerialNumber: 04024818111723231136

```

wsl를 사용하고 있는 경우 USB를 연결하기 위해서 추가적인 작업을 해야할 필요가 있다.  
usbipd-win 을 설치해 usb 드라이브와 wsl을 연결해야 하나, 이번 과제에서는 생략한다.

## 2. Do not unplug your USB memory, however, use the command `umount` to unmount your USB memory file system on your Linux box - explain this procedure step

`df -h` 명령어를 통해 마운트된 디바이스의 경로를 확인한다.

```
df -h
```

```

seworl@seworl ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
none            3.9G  4.0K  3.9G   1% /mnt/wsl
none           220G  160G   61G  73% /usr/lib/wsl/drivers
none            3.9G    0  3.9G   0% /usr/lib/modules
none            3.9G    0  3.9G   0% /usr/lib/modules/5.15.146.1-microsoft-standard-WSL2
/dev/sdc        1007G   15G  941G   2% /
none            3.9G   88K  3.9G   1% /mnt/wslg
none            3.9G    0  3.9G   0% /usr/lib/wsl/lib
rootfs          3.8G  1.9M  3.8G   1% /init
none            3.9G  900K  3.8G   1% /run
none            3.9G    0  3.9G   0% /run/lock
none            3.9G    0  3.9G   0% /run/shm
tmpfs           4.0M    0  4.0M   0% /sys/fs/cgroup
none            3.9G   76K  3.9G   1% /mnt/wslg/versions.txt
none            3.9G   76K  3.9G   1% /mnt/wslg/doc
C:\             220G  160G   61G  73% /mnt/c
D:\             932G  198G  734G  22% /mnt/d
snapfuse        75M    75M    0 100% /snap/core22/1122
snapfuse       128K   128K    0 100% /snap/bare/5
snapfuse        74M    74M    0 100% /snap/core22/864
snapfuse        92M    92M    0 100% /snap/gtk-common-themes/1535
snapfuse        41M   41M    0 100% /snap/snapd/20290
snapfuse        40M   40M    0 100% /snap/snapd/21184
snapfuse       131M   131M    0 100% /snap/ubuntu-desktop-installer/1284
snapfuse       132M   132M    0 100% /snap/ubuntu-desktop-installer/1286
C:\Program Files\usbipd-win\WSL 220G  160G   61G  73% /run/usbipd-win
E:             115G   94M  115G   1% /mnt/e
seworl@seworl ~$

```

현재 `/mnt/e` 에 마운트되어 있는 것을 확인할 수 있다. 이를 `umount` 명령어를 통해 언마운트한다.

```
sudo umount /mnt/e
```

언마운트 이후에는 `df -h` 명령어를 통해 마운트된 디바이스가 없는 것을 확인할 수 있다.

```

snapfuse        132M   132M    0 100% /snap/ubuntu-desktop-installer/1286
C:\Program Files\usbipd-win\WSL 220G  160G   61G  73% /run/usbipd-win
E:             115G   94M  115G   1% /mnt/e
seworl@seworl ~$ sudo umount /mnt/e
sudo: umount: command not found
x seworl@seworl ~$ sudo umount /mnt/e
seworl@seworl ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
none            3.9G  4.0K  3.9G   1% /mnt/wsl
none           220G  160G   61G  73% /usr/lib/wsl/drivers
none            3.9G    0  3.9G   0% /usr/lib/modules
none            3.9G    0  3.9G   0% /usr/lib/modules/5.15.146.1-microsoft-standard-WSL2
/dev/sdc        1007G   15G  941G   2% /
none            3.9G   88K  3.9G   1% /mnt/wslg
none            3.9G    0  3.9G   0% /usr/lib/wsl/lib
rootfs          3.8G  1.9M  3.8G   1% /init
none            3.9G  900K  3.8G   1% /run
none            3.9G    0  3.9G   0% /run/lock
none            3.9G    0  3.9G   0% /run/shm
tmpfs           4.0M    0  4.0M   0% /sys/fs/cgroup
none            3.9G   76K  3.9G   1% /mnt/wslg/versions.txt
none            3.9G   76K  3.9G   1% /mnt/wslg/doc
C:\             220G  160G   61G  73% /mnt/c
D:\             932G  198G  734G  22% /mnt/d
snapfuse        75M    75M    0 100% /snap/core22/1122
snapfuse       128K   128K    0 100% /snap/bare/5
snapfuse        74M    74M    0 100% /snap/core22/864
snapfuse        92M    92M    0 100% /snap/gtk-common-themes/1535
snapfuse        41M   41M    0 100% /snap/snapd/20290
snapfuse        40M   40M    0 100% /snap/snapd/21184
snapfuse       131M   131M    0 100% /snap/ubuntu-desktop-installer/1284
snapfuse       132M   132M    0 100% /snap/ubuntu-desktop-installer/1286
C:\Program Files\usbipd-win\WSL 220G  160G   61G  73% /run/usbipd-win
seworl@seworl ~$

```

### 3. Change your home directory permission like this

- Only you can access your home directory (Use googling to find out the way of creation a new user account). The others cannot access your home directory
- To verify it, create a new user with a userID "Hacker" on you Linux box and try to access your home directory

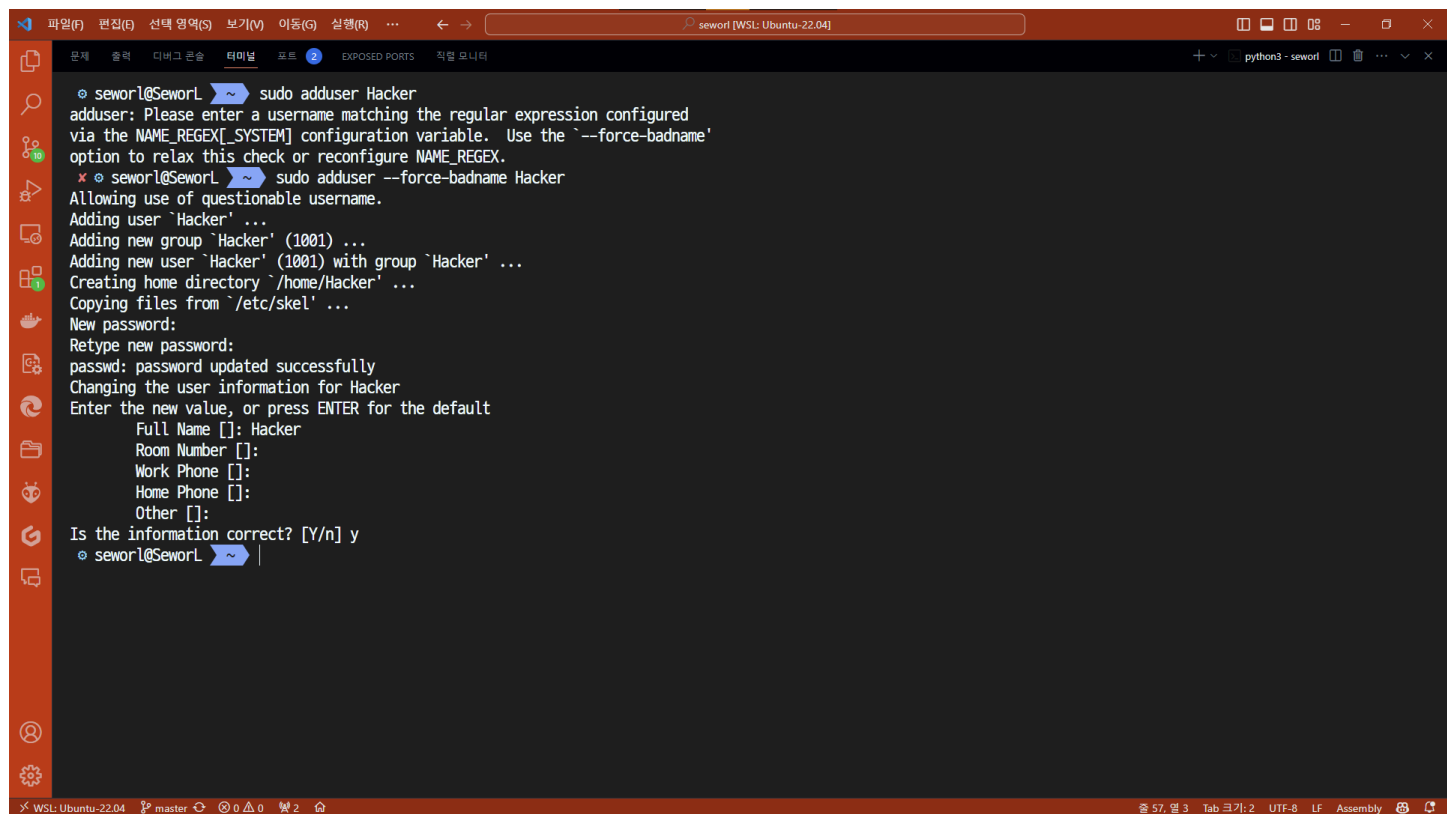
유저를 생성하기 위해 `adduser` 명령어를 사용한다.

기본적으로 유저 이름은 소문자로만 가능한데, `--force-badname` 옵션을 사용하면 대문자도 가능하다.

```
sudo adduser --force-badname Hacker
```

패스워드는 `powerhacker` 로 설정했다.

풀네임은 `Hacker` 로 설정했다.



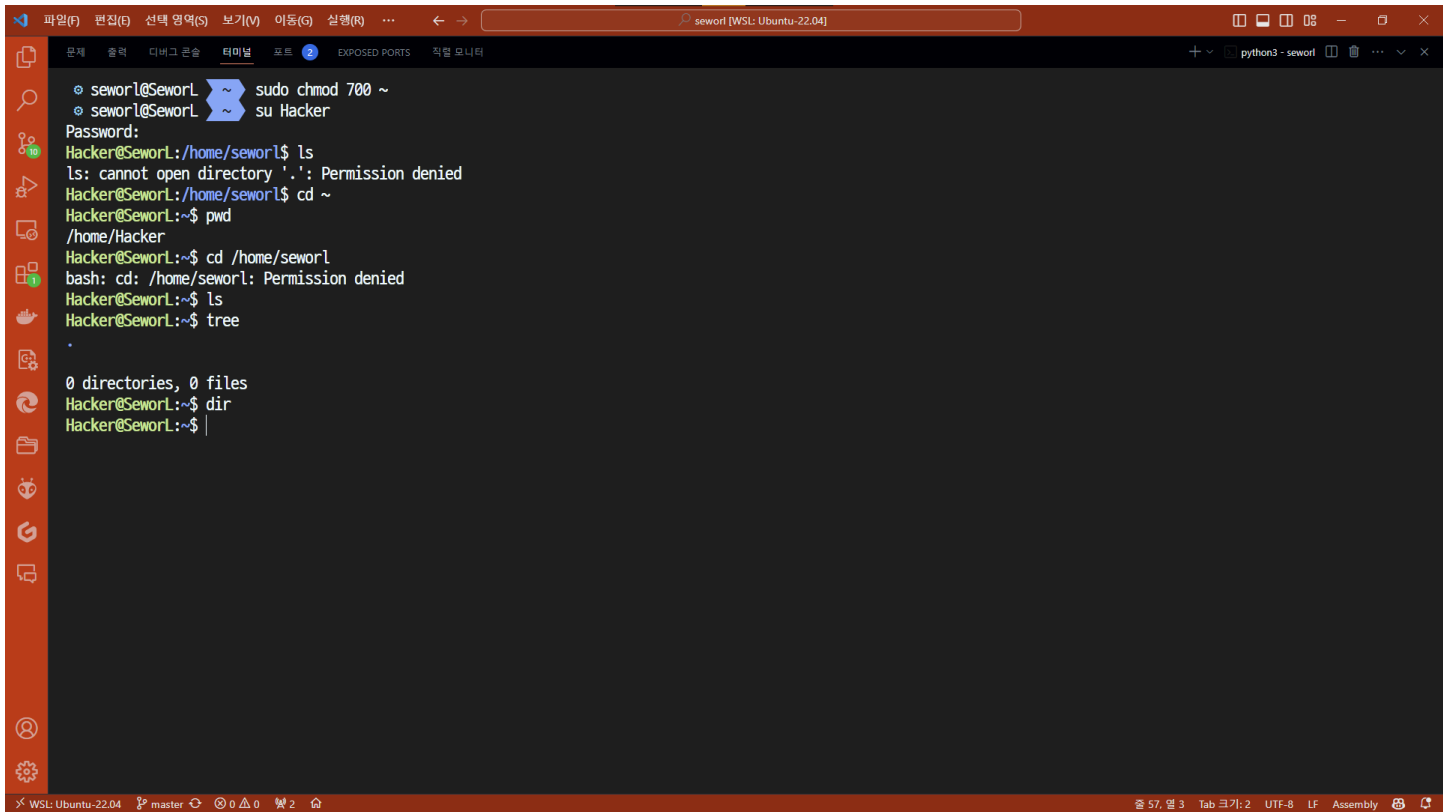
```
seworl@seworl ~$ sudo adduser Hacker
adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX[_SYSTEM] configuration variable. Use the '--force-badname'
option to relax this check or reconfigure NAME_REGEX.
seworl@seworl ~$ sudo adduser --force-badname Hacker
Adding use of questionable username.
Adding user `Hacker' ...
Adding new group `Hacker' (1001) ...
Adding new user `Hacker' (1001) with group `Hacker' ...
Creating home directory `/home/Hacker' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for Hacker
Enter the new value, or press ENTER for the default
Full Name []: Hacker
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
seworl@seworl ~$
```

`sudo chmod 700 ~` 명령어를 통해 홈 디렉토리의 권한을 변경한다.

```
sudo chmod 700 ~
```

이후 Hacker 계정으로 접속해 접근을 시도한다.

```
su Hacker
cd ~
```



```
seworl@seworl ~$ sudo chmod 700 ~
seworl@seworl ~$ su Hacker
Password:
Hacker@seworl:/home/seworl$ ls
ls: cannot open directory '.': Permission denied
Hacker@seworl:/home/seworl$ cd ~
Hacker@seworl:~$ pwd
/home/Hacker
Hacker@seworl:~$ cd /home/seworl
bash: cd: /home/seworl: Permission denied
Hacker@seworl:~$ ls
Hacker@seworl:~$ tree
.
0 directories, 0 files
Hacker@seworl:~$ dir
Hacker@seworl:~$ |
```

퍼미션이 거부되었다는 것을 확인할 수 있다.

## 4. Make a subdirectory named `foohaha` . Change permission mode into `drw-r--r--` . What happend if you try to access the `foohaha` directory?

`mkdir` 명령어를 통해 `foohaha` 디렉토리를 생성한다.

```
mkdir foohaha
```

`drw-r--r--` 은 `744` 로 표현할 수 있다. `chmod` 명령어를 통해 권한을 변경한다.

```
sudo chmod 744 foohaha
```

```
seworl@SeworL ~$ mkdir fooaha
seworl@SeworL ~$ sudo chmod 744 fooaha
seworl@SeworL ~$ su Hacker
Password:
Hacker@SeworL:/home/seworl$ cd fooaha/
bash: cd: fooaha/: Permission denied
Hacker@SeworL:/home/seworl$ cd fooaha/
bash: cd: fooaha/: Permission denied
Hacker@SeworL:/home/seworl$
```

`execute` 권한이 없기 때문에 디렉토리에 접근할 수 없다.

다만 `Read` 권한이 있기 때문에 `ls` 명령어를 통해 디렉토리 내부를 확인할 수는 있다.

5. Change your shell prompt that displays as follows:

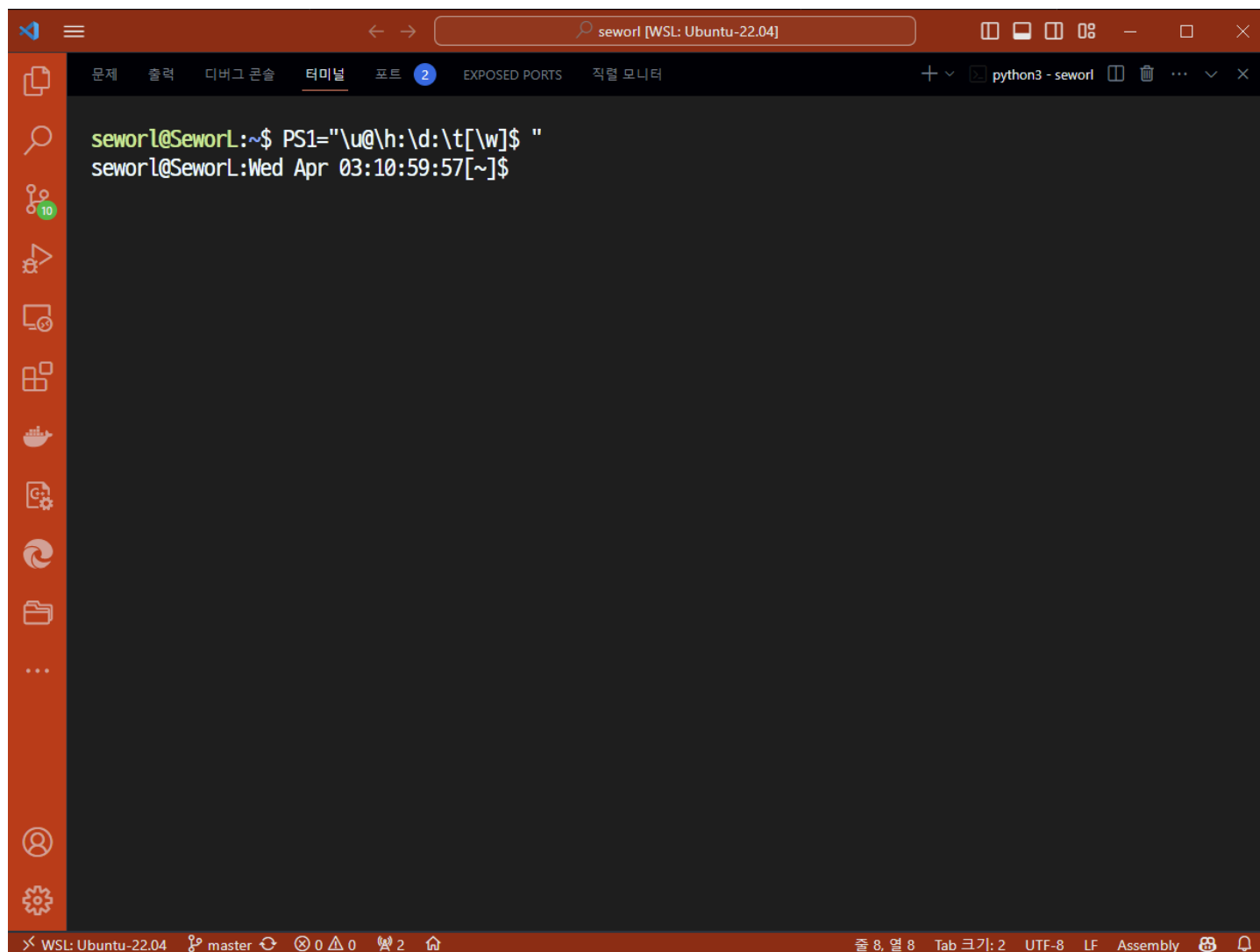
```
userID@hostName:date:time[the current working direcotry]$
```

아래 명령어를 사용한다.

```
PS1="\u@\h:\d:\t[\w]$ "
```

프롬프트를 표시하는 변수인 `PS1` 에 값을 할당한다.

`\u` 는 유저 이름, `\h` 는 호스트 이름, `\d` 는 날짜, `\t` 는 시간, `\w` 는 현재 작업 디렉토리를 나타낸다.



```
seworl@SeworL:~$ PS1="\u@\h:\d:\t[\w]$ "  
seworl@SeworL:Wed Apr 03:10:59:57[~]$
```

영구적으로 변경하려면 해당 명령어를 `~/.bashrc` 파일에 추가하면 된다.