# 《操作系统》课第05次实验报告

|  |  |
| --- | --- |
| 学院: | 软件学院 |
| 姓名: | 张怡桢 |
| 学号: | 2013747 |
| 邮箱: | 2662765987@qq.com |
| 时间: | 10/16/2022 |

## 开篇感言

“你长大后想成为什么人？”

“什么意思？长大后我就不能成为我自己了吗？”

-- 《阿甘正传》

## 实验题目

使用系统调用列出所有进程

## 实验目标

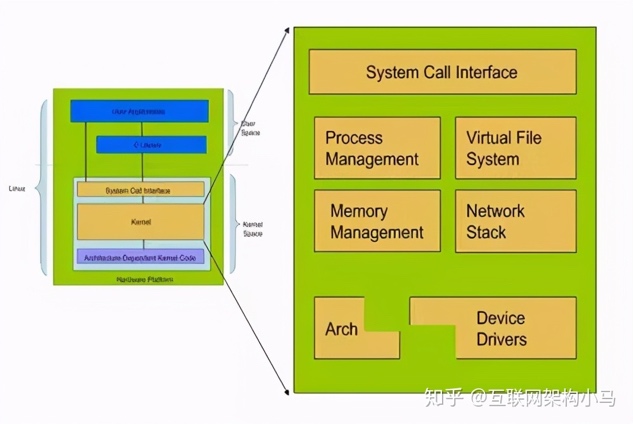
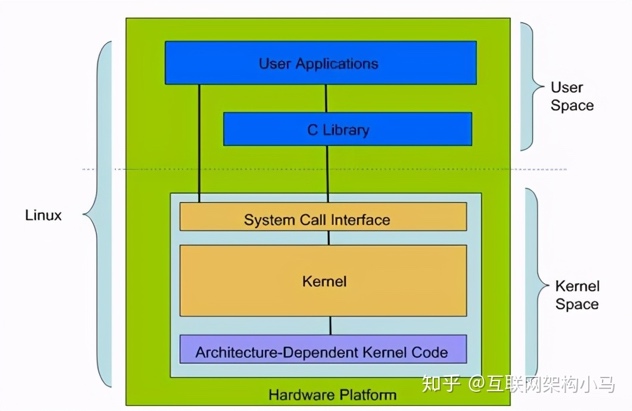
通过系统调用，打印出当前所有的进程的名字、进程 ID 号、父进程 ID 号、 进程状态、学号姓名

## 原理方法

3.1 Linux 内核概述：

Linux 内核是 Linux 操作系统（OS）的主要组件，也是计算机硬件与其进程之间的核心接口。它负责两者之间的通信，还要尽可能高效地管理资源。

之所以称为内核，是因为它在操作系统中就像果实硬壳中的种子一样，并且控制着硬件（无论是电话、笔记本电脑、服务器，还是任何其他类型的计算机）的所有主要功能。



3.2 进程：

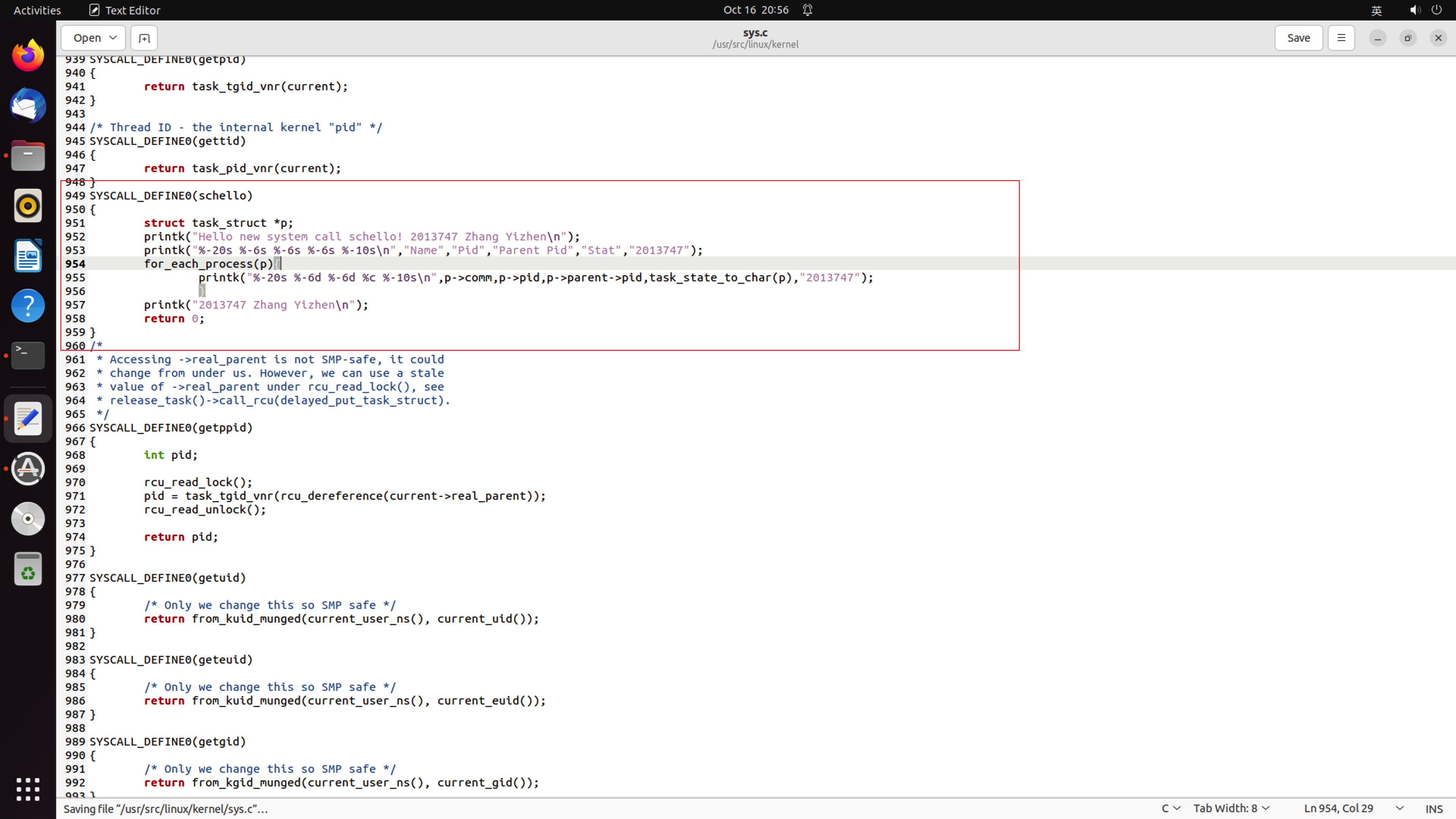
进程结构体:struct task\_struct \*p;

遍历所有进程：for\_each\_process(p) 获取进程状态：task\_state\_to\_char(struct task\_struct \*tsk)

## 具体步骤

### Step1 (Linux kernel 5.19)

kernel/sys.c 在文件SYSCALL\_DEFINE0(gettid)函数之后，添加如下行：



### Step2

进入 5.19.10 内核的文件夹，使用命令 sudo su 提升权限，然后运行  
make -j8

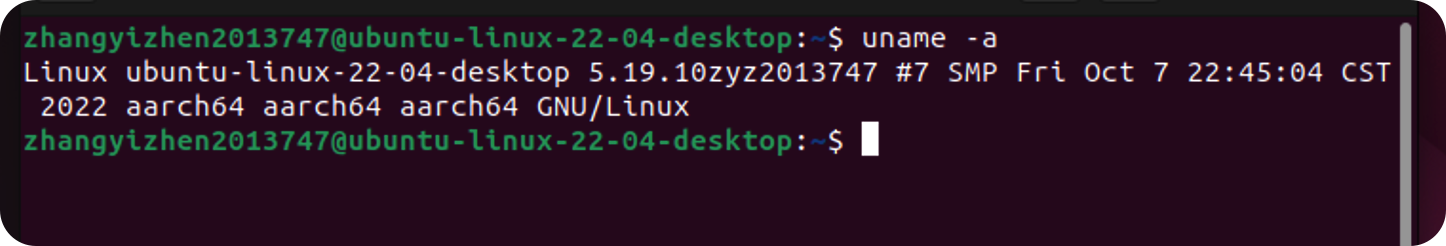
make

make modules\_install

make install

### Step 3

重启前查看版本号：



可以看见#7说明此编译版本序号为7

重新启动:

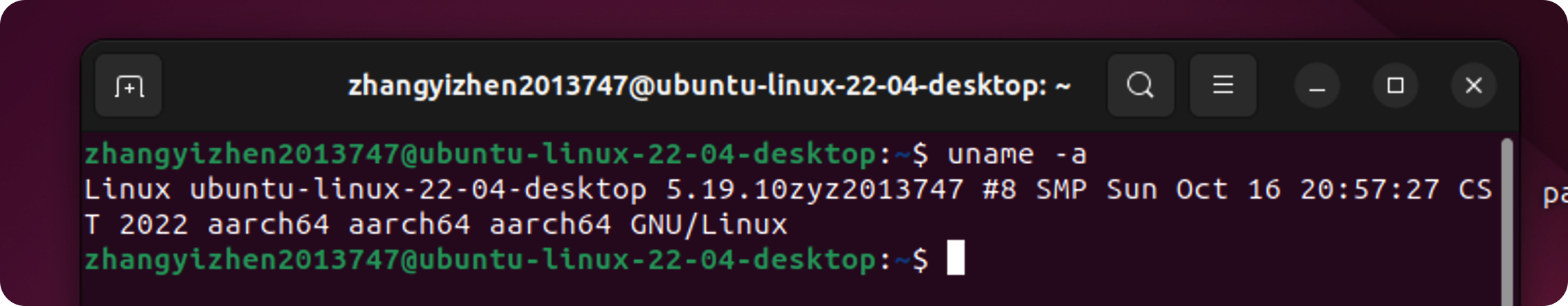
sudo reboot

可以看到有zyz2013747后缀的新版本，还有编译前的旧版本zyz2013747（old）的版本，选择新版本进入即可



确认新内核是否成功运行：

uname -a



可以看到经过多次编译后，编译版本序号已经为 8 了

### Step 4

编写用户态测试程序testschello.c

#include <unistd.h>  
#include <sys/syscall.h>  
#include <sys/types.h>  
#include <stdio.h>  
#define \_\_NR\_schello 451  
int main(int argc, char \*argv[])  
{  
 syscall(\_\_NR\_schello);  
 printf("ok! run dmesg | grep hello in terminal!\n");  
 return 0;  
}

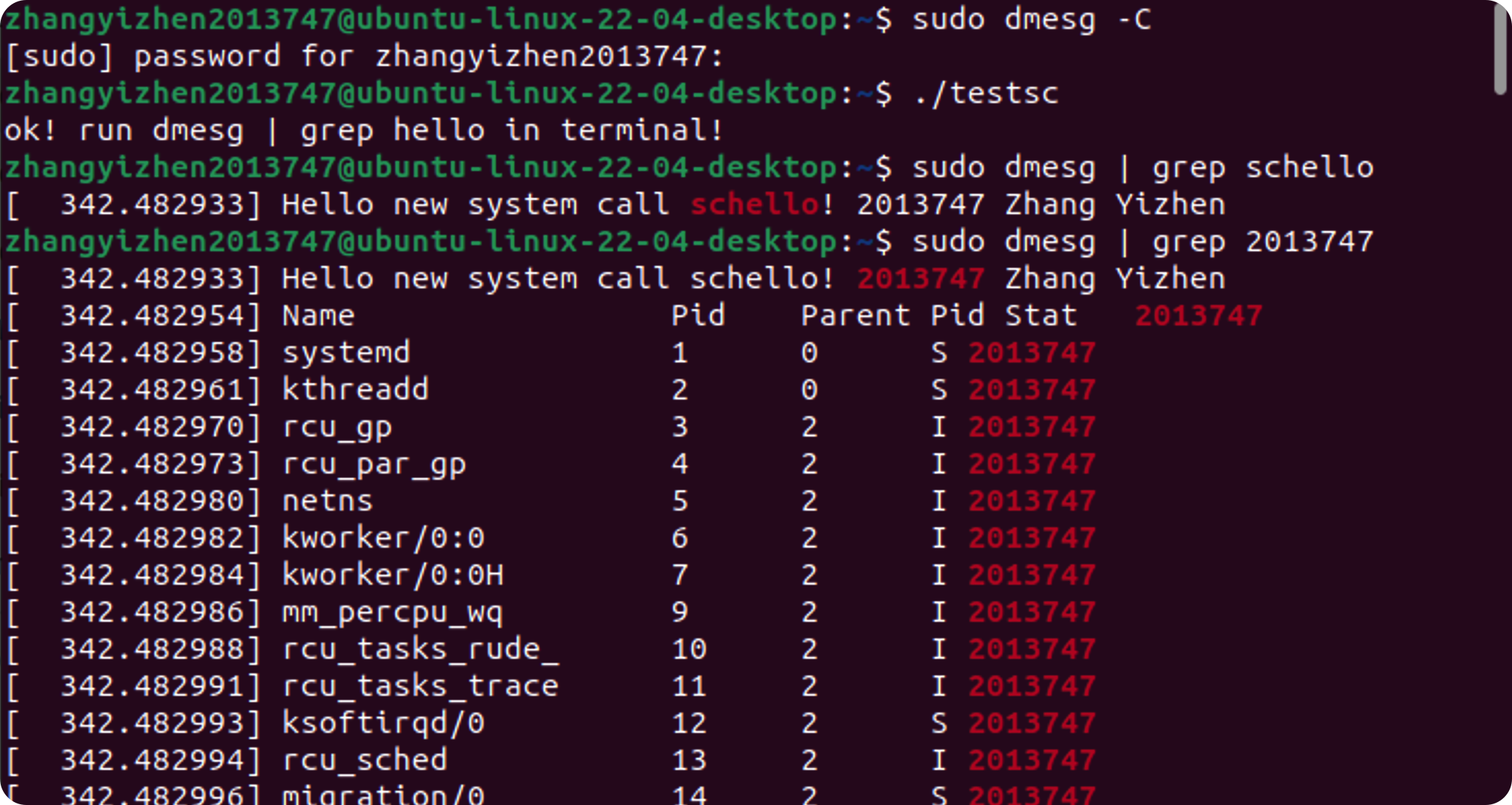
### Step 5

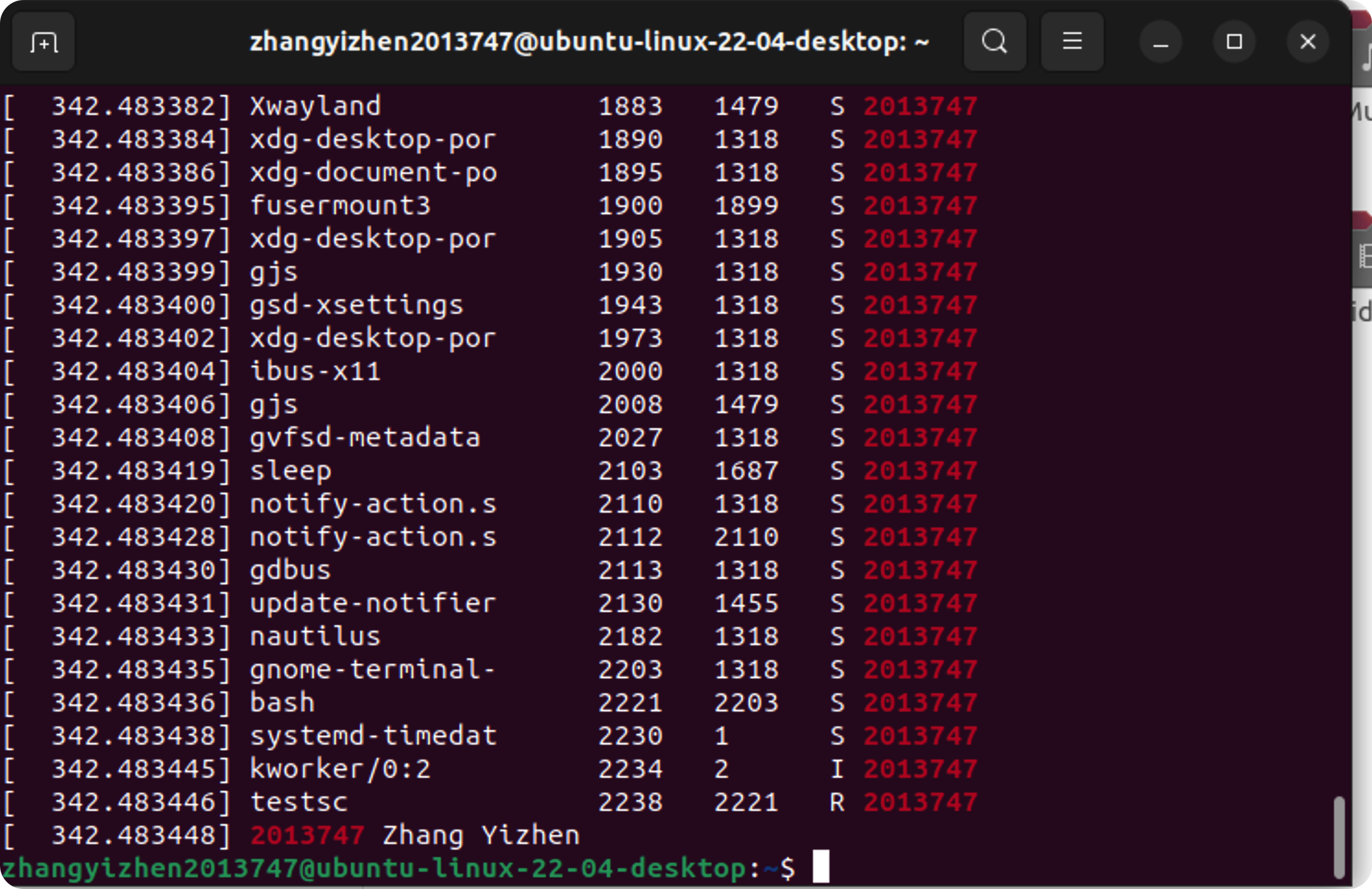
编译用户态测试程序testschello.c，并执行

gcc -o testsc testschello.c  
  
$ sudo dmesg -C  
  
./testsc  
  
$ sudo dmesg | grep schello  
  
[ 342.482933] Hello new system call schello! 2013747 Zhang Yizhen

$ sudo dmesg | grep 2013747

查看结果，部分进程如下：





## 总结心得

* 1. state 状态

state 状态比较特殊，需要将状态用 task\_state\_to\_char（）函数将状态转换为 字符，该参数直接传入 task\_struct 类型的 p 即可。遍历查看所有进程发现，本 机存在的进程状态基本上分为 S（睡眠）、T（停止）、R（运行），除此之外 Linux 还有三种进程状态：D（磁盘睡眠）、X（死亡状态）、Z（僵尸状态）。

详情如下：

（1）R运行状态（runing）：并不意味着进程一定在运行中，也可以在运行队列里；

（2）S睡眠状态（sleeping）：进程在等待事件完成；（浅度睡眠，可以被唤醒）

（3）D磁盘睡眠状态（Disk sleep）:不可中断睡眠（[深度](https://so.csdn.net/so/search?q=%E6%B7%B1%E5%BA%A6&spm=1001.2101.3001.7020)睡眠，不可以被唤醒，通常在磁盘写入时发生）

（4）T停止状态（stopped）：可以通过发送SIGSTOP信号给进程来停止进程，可以发送SIGCONT信号让进程继续运行

（5）X死亡状态（dead）:该状态是返回状态，在任务列表中看不到；

（6）Z僵尸状态（zombie）:子进程退出，父进程还在运行，但是父进程没有读到子进程的退出状态，子进程进入僵尸状态；

（7）t追踪停止状态（trancing stop）

5.2 sudo dmesg | grep 2013747

这个命令后面要跟着检索输出的内容，原有的 hello 是因为 schello 包含 hello， 这也是上一次实验 hello 输出标红的原因。为此，将程序每一行后都加入学号以方便检索输出。

## 参考资料

1. [Linux进程六种状态（R、S、D、T、Z、X）](https://blog.csdn.net/weixin_44164489/article/details/112431609)
2. [Linux dmesg 命令](https://www.runoob.com/linux/linux-comm-dmesg.html)