step 1

after downloading a kernel extract it and then go inside the linux folder

create a new folder and name it hello (since we are making a hello world system call)

then go inside that folder

step 2

open the terminal in folder and make a c code file by typing gedit hello.c

and type the following code

#include <linux/kernel.h>

asmlinkage long sys\_hello(void)

{

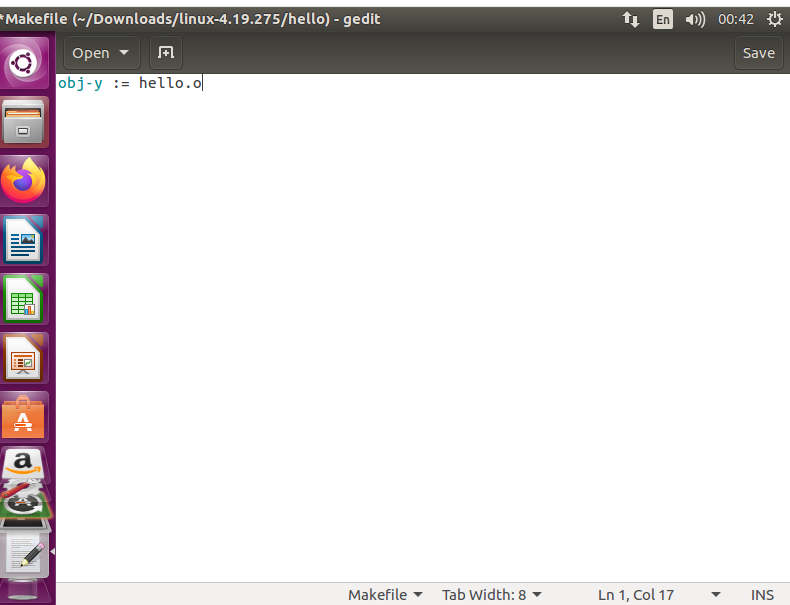
printk("Hello world\n");

return 0;

}

step 3

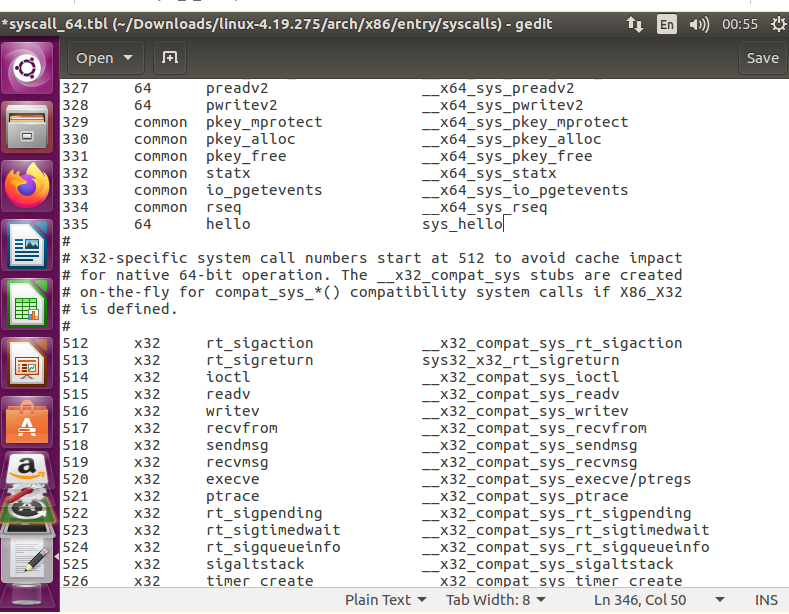
now create a makefile by typing makefile and put obj-y:=hello.o



step4

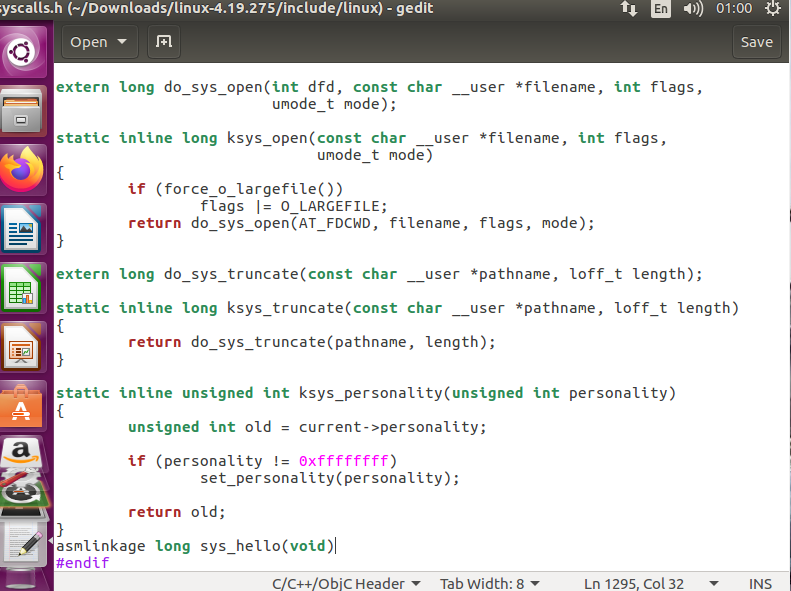
go into the directory in /arch/x86/entry/syscalls/syscall\_64.tbl.

and edit a system call



step5

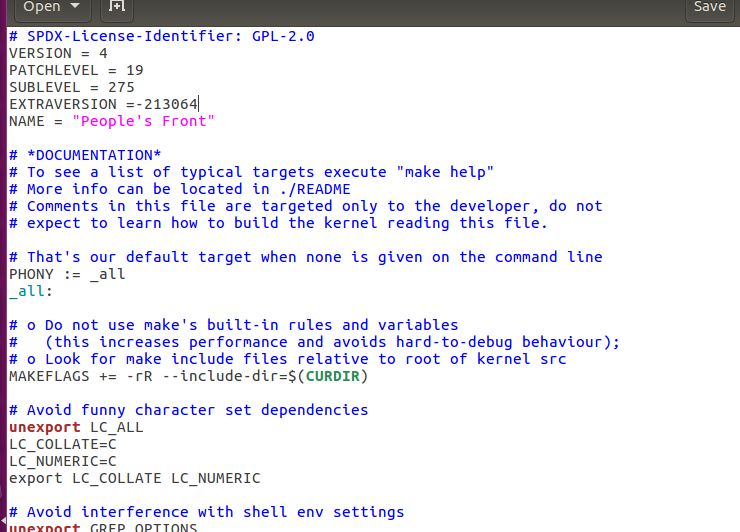
type gedit include/linux/syscalls.h and paste the prototype of function hello in end of file

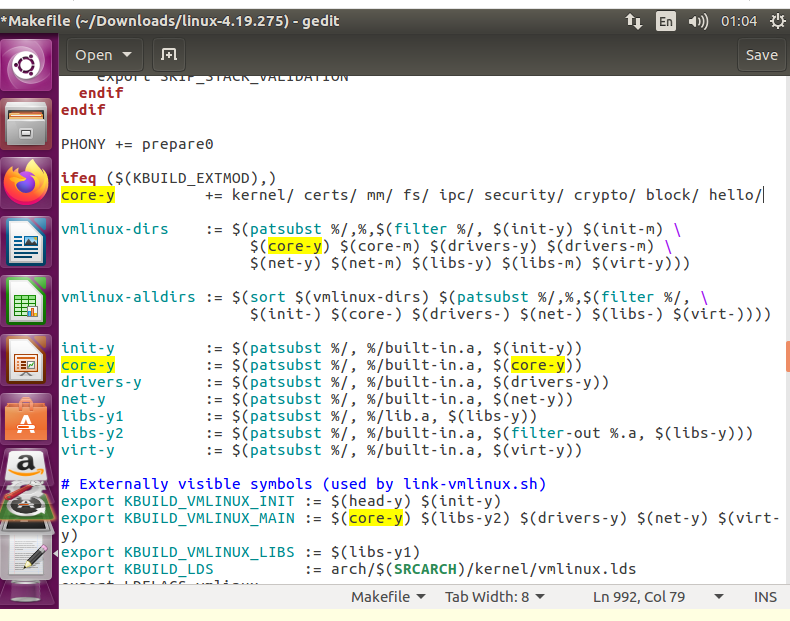


step6

changing version and editing hello system call type make file and edit extraversion=-213064

and edit hello/ after core-y

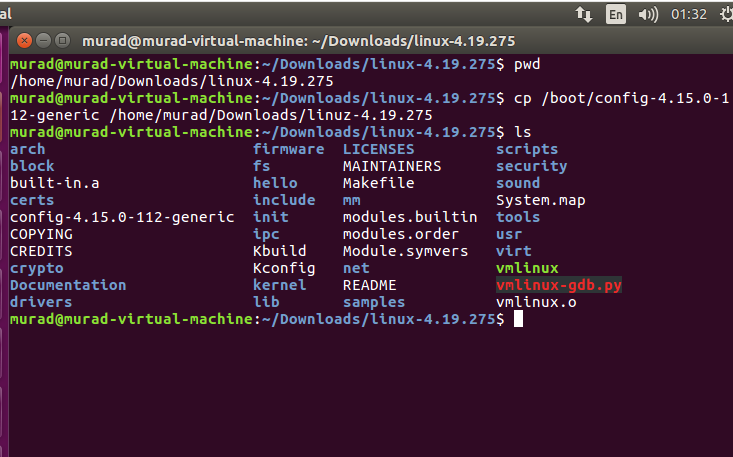




step7

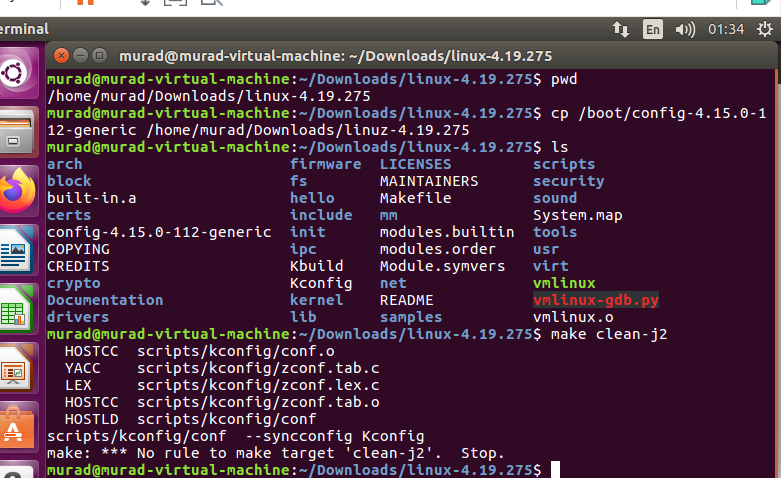
type ls /boot |grep config

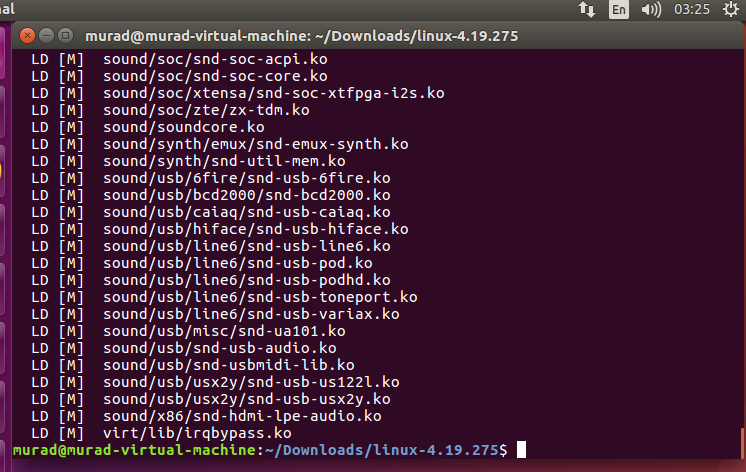
copy the config of current kernel into new one



step 8

clean kernel by typing make clean -j2 and then type make -j2

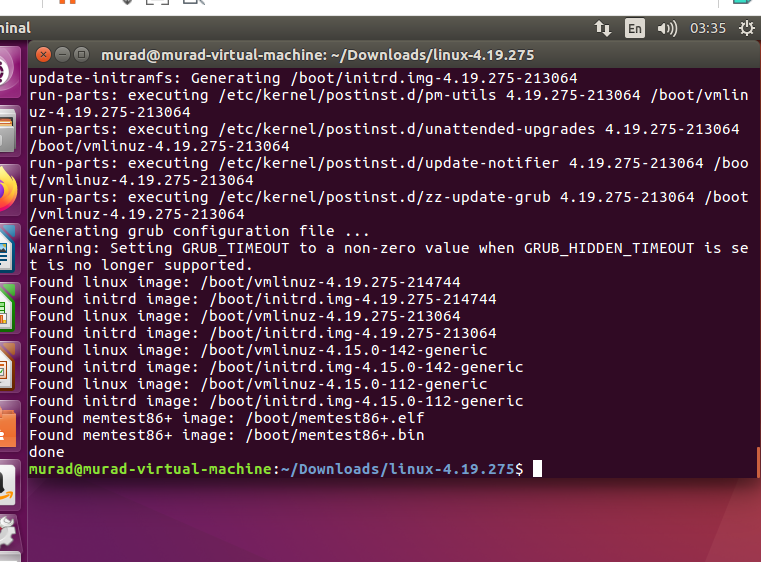




step 9

now we have to install kernel

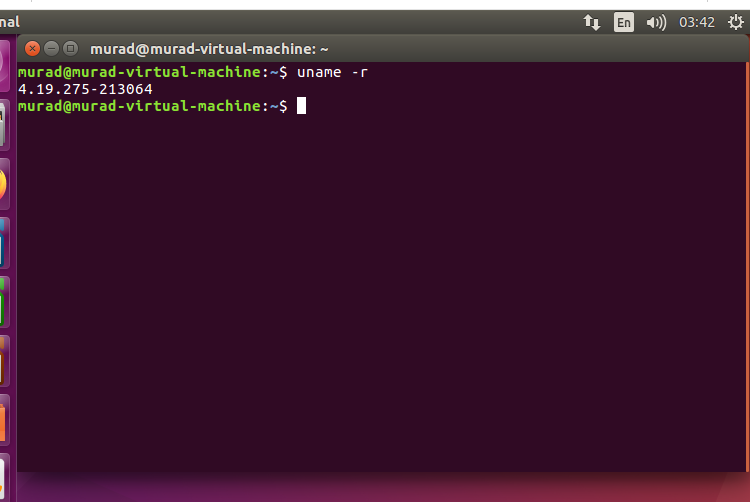
type sudo make modules\_install install



now restart by shutdown -r

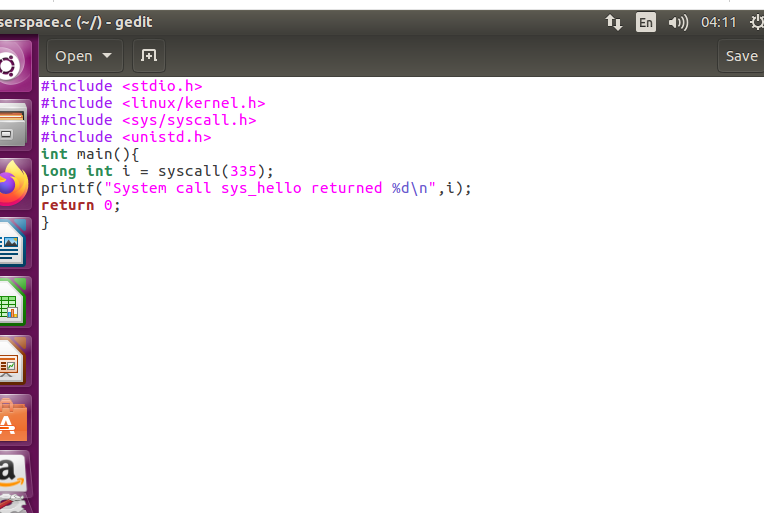
step 10

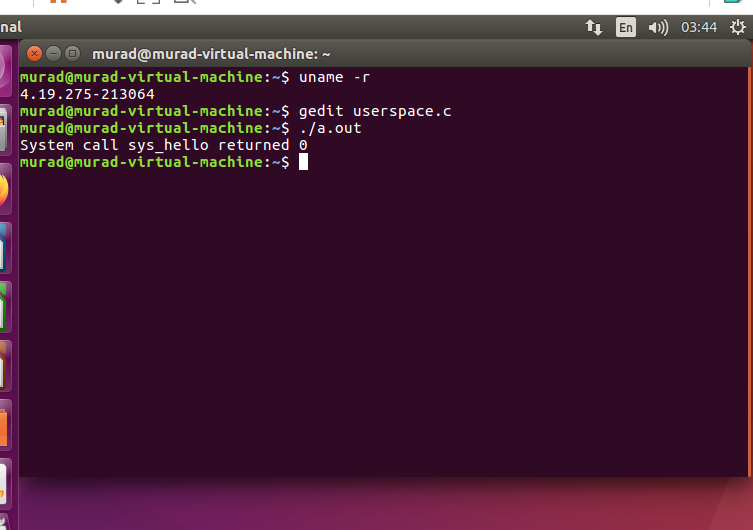
enter uname -r in terminal



step 11

make a userspace file and type the following code in screenshot





and here it is our hello world in the last screenshot after running dmesg command

