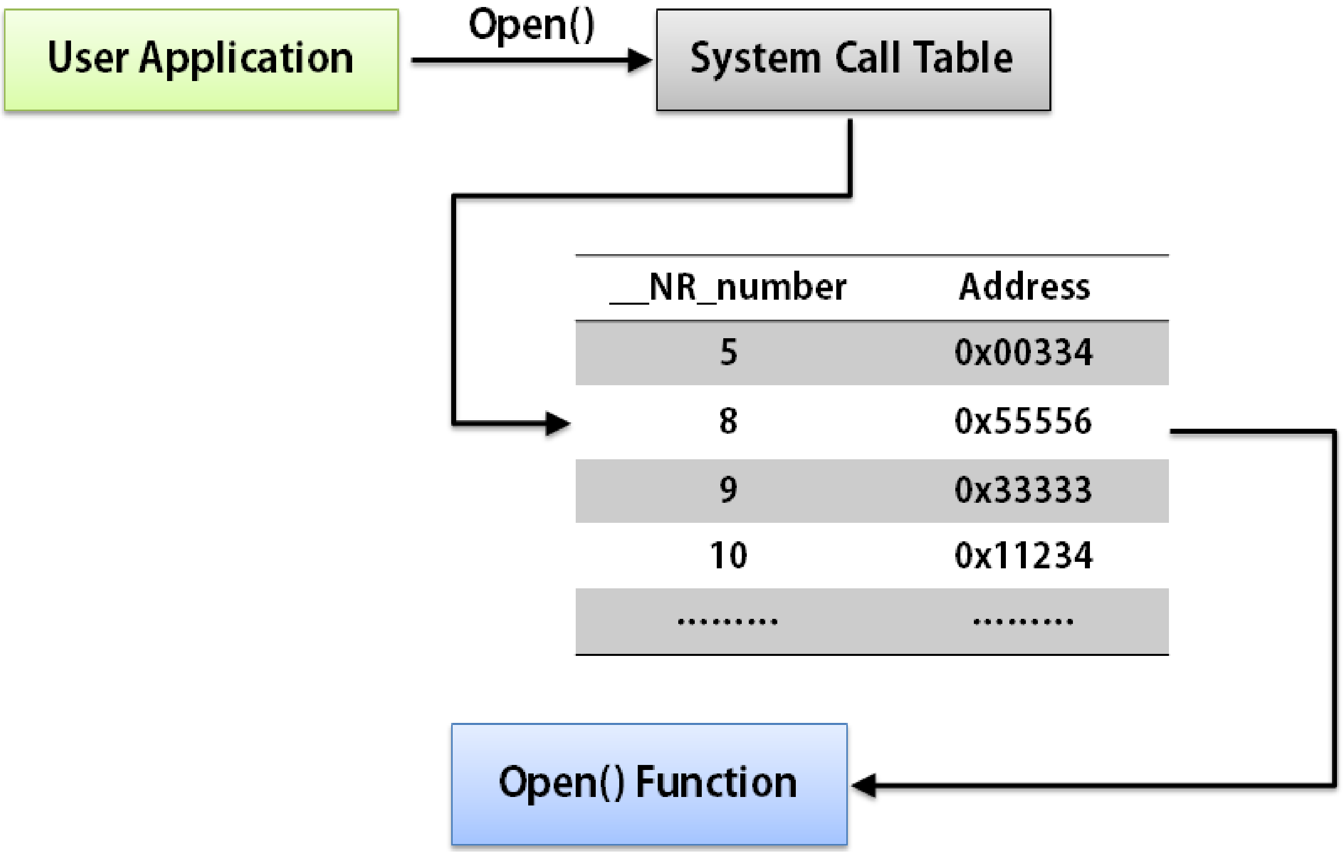
System Call Hooking

Original System Call



User Application

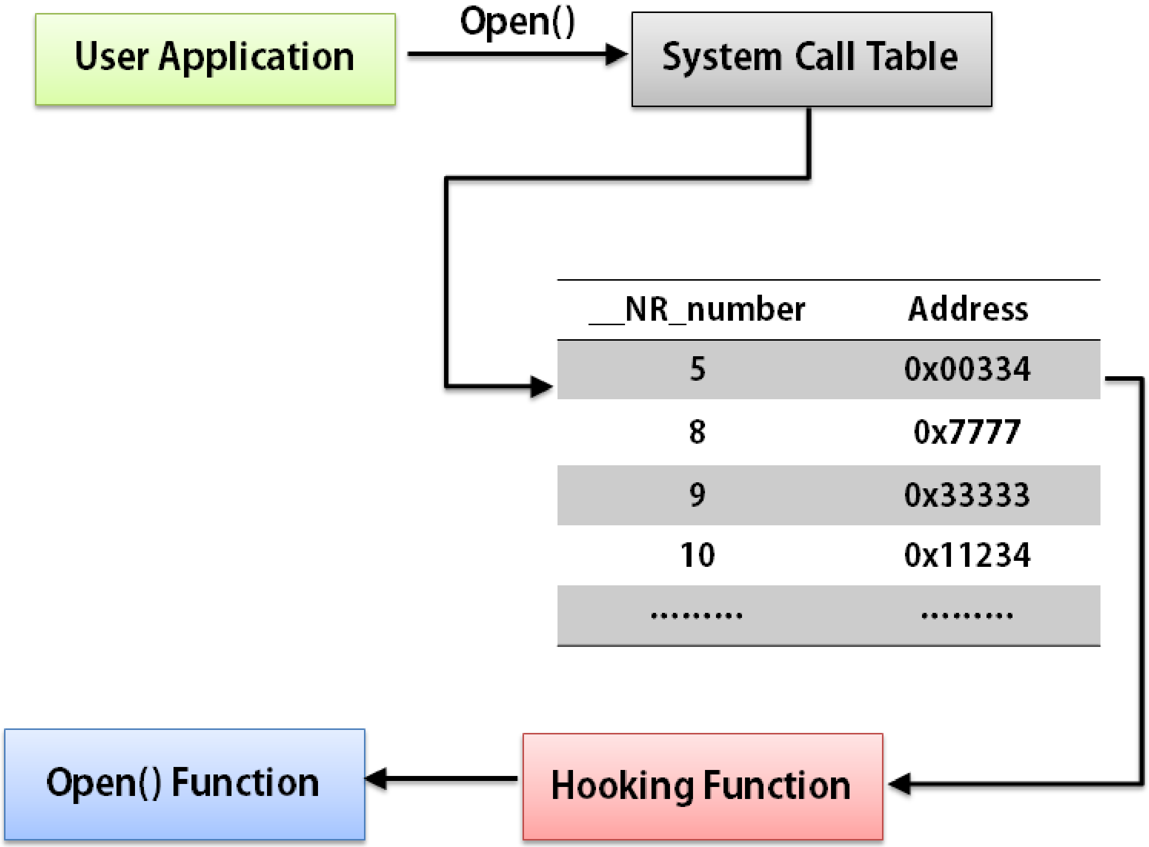
Open()

System Call Table

__NR_number	Address
5	0x00334
8	0x55556
9	0x33333
10	0x11234
………	………

Open() Function

Hooked System Call



User Application

Open()

System Call Table

__NR_number	Address
5	0x00334
8	0x7777
9	0x33333
10	0x11234
....	....

Open() Function

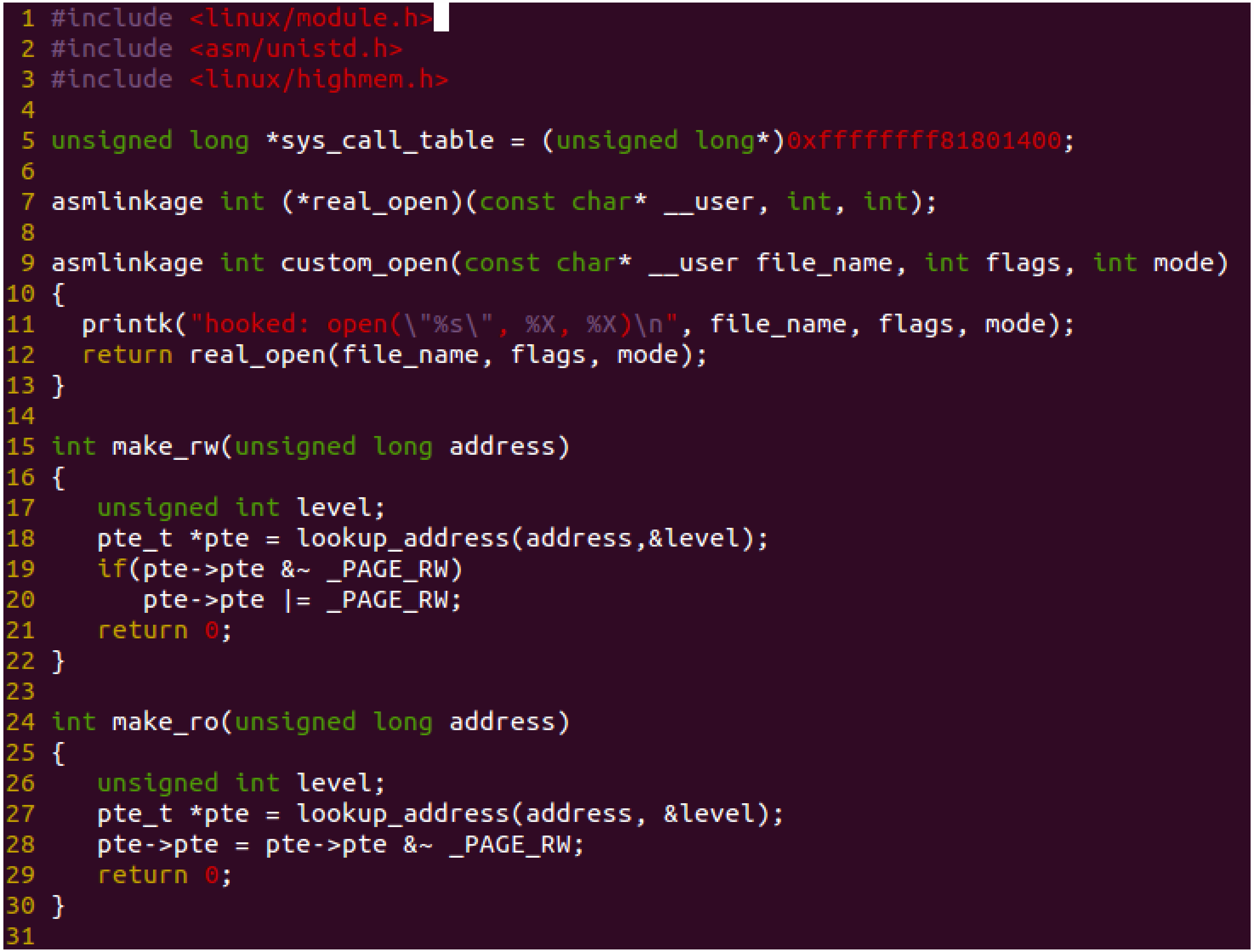
Hooking Function

Find System Call Table Address

```
$> sudo grep sys_call_table /boot/System.map-3.xx.xxxxx
```

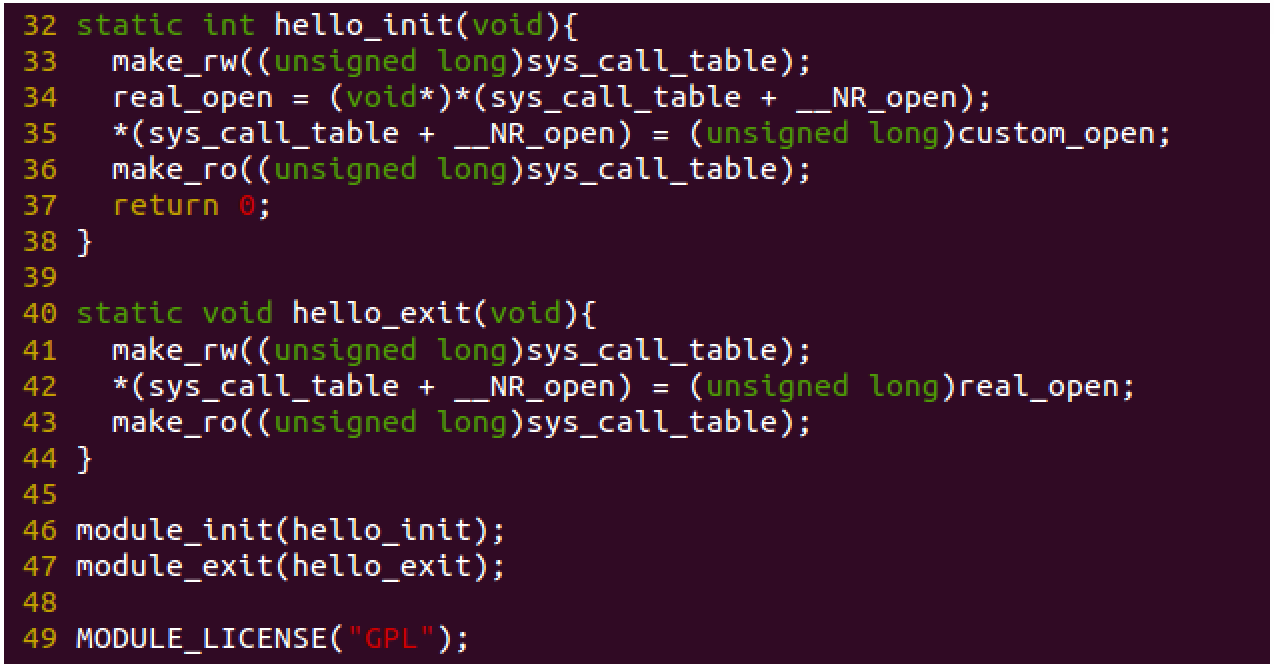
```
ffffffff81801400 R sys_call_table
```

sys_hook.c



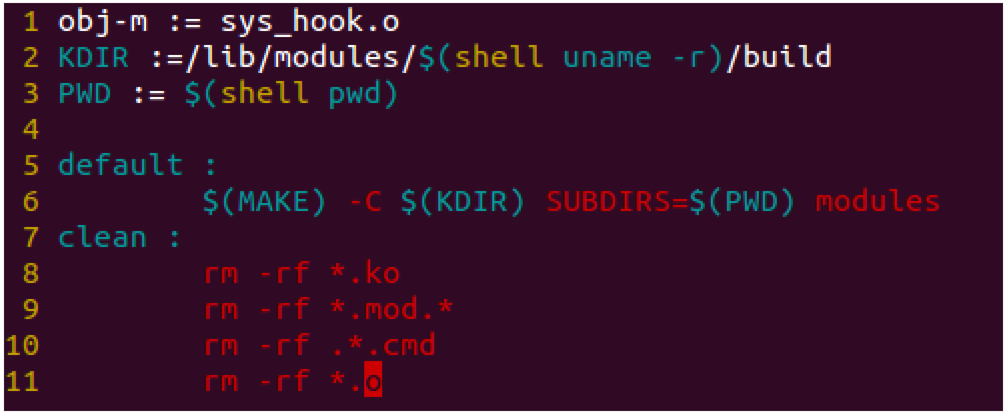
```
#include <linux/module.h>
#include <asm/unistd.h>
#include <linux/highmem.h>

unsigned long *sys_call_table = (unsigned long*)0xffffffff81801400;

asmlinkage int (*real_open)(const char* __user, int, int);

asmlinkage int custom_open(const char* __user file_name, int flags, int mode)
{
  printk("hooked: open(\"%s\", %X, %X)\n", file_name, flags, mode);
  return real_open(file_name, flags, mode);
}

int make_rw(unsigned long address)
{
   unsigned int level;
   pte_t *pte = lookup_address(address,&level);
   if(pte->pte &~ _PAGE_RW)
      pte->pte |= _PAGE_RW;
   return 0;
}

int make_ro(unsigned long address)
{
   unsigned int level;
   pte_t *pte = lookup_address(address, &level);
   pte->pte = pte->pte &~ _PAGE_RW;
   return 0;
}

```

sys_hook.c(cont’d)



```
static int hello_init(void){
  make_rw((unsigned long)sys_call_table);
  real_open = (void*)*(sys_call_table + __NR_open);
  *(sys_call_table + __NR_open) = (unsigned long)custom_open;
  make_ro((unsigned long)sys_call_table);
  return 0;
}

static void hello_exit(void){
  make_rw((unsigned long)sys_call_table);
  *(sys_call_table + __NR_open) = (unsigned long)real_open;
  make_ro((unsigned long)sys_call_table);
}

module_init(hello_init);
module_exit(hello_exit);

MODULE_LICENSE("GPL");
```

Makefile



```
obj-m := sys_hook.o
KDIR :=/lib/modules/$(shell uname -r)/build
PWD := $(shell pwd)

default :
        $(MAKE) -C $(KDIR) SUBDIRS=$(PWD) modules
clean :
        rm -rf *.ko
        rm -rf *.mod.*
        rm -rf .*.cmd
        rm -rf *.o
```

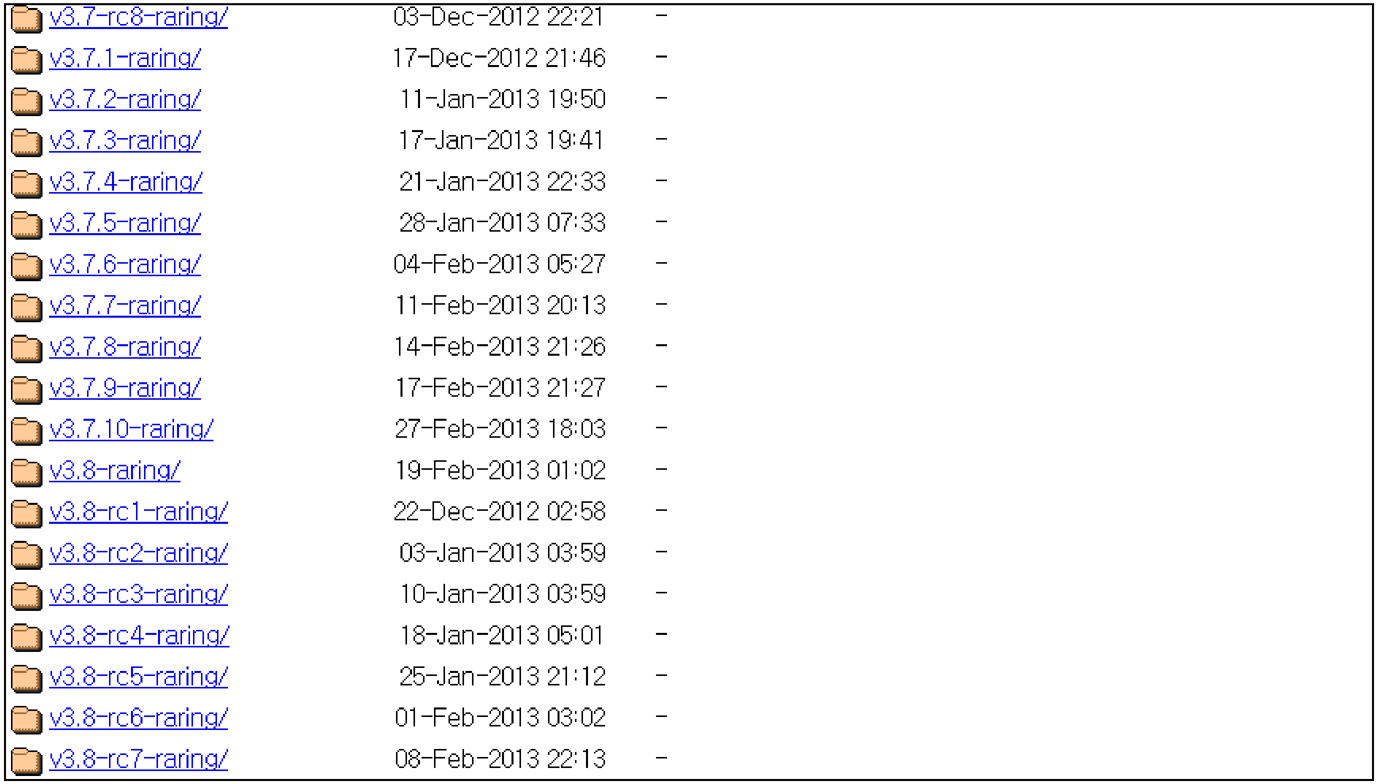
```
$>sudo insmod sys_hook.ko
$>sudo dmesg –C
$>ls
$>sudo dmesg
$>sudo rmmod sys_hook
```

Appendix

Kernel Up or Downgrade

1. Ubuntu PPA 접속

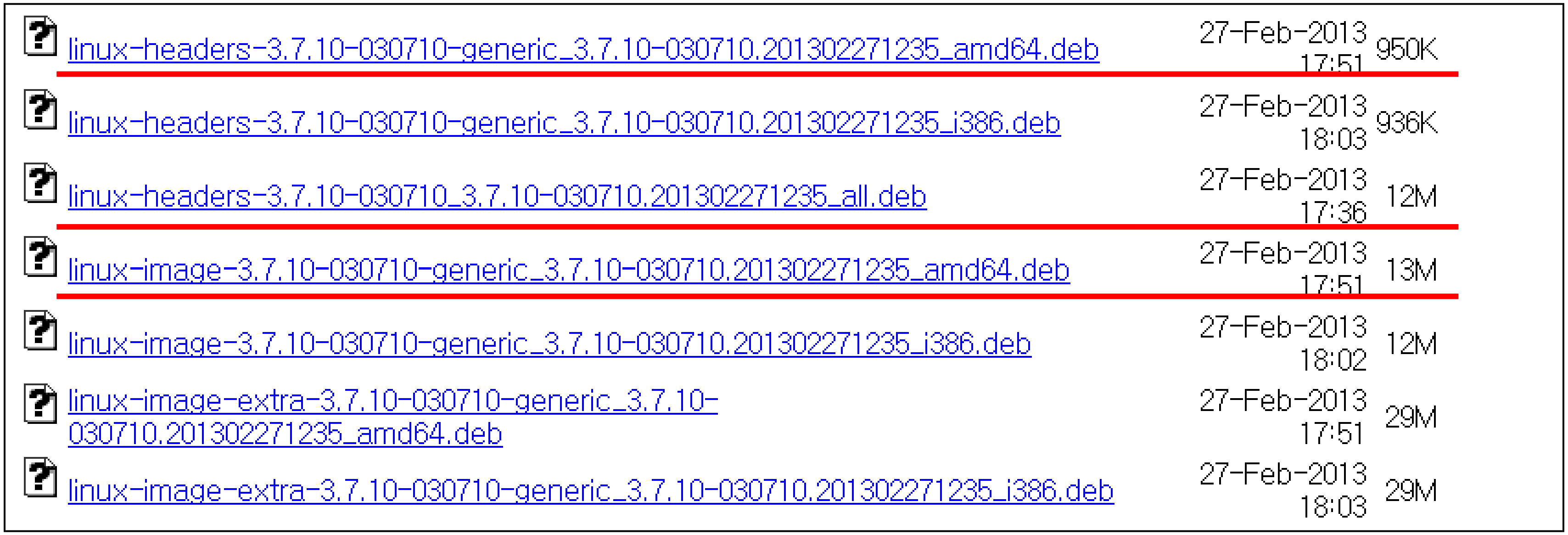
http://kernel.ubuntu.com/~kernel-ppa/mainline



v3.7-rc8-raring/	03-Dec-2012 22:21	-
v3.7.1-raring/	17-Dec-2012 21:46	-
v3.7.2-raring/	11-Jan-2013 19:50	-
v3.7.3-raring/	17-Jan-2013 19:41	-
v3.7.4-raring/	21-Jan-2013 22:33	-
v3.7.5-raring/	28-Jan-2013 07:33	-
v3.7.6-raring/	04-Feb-2013 05:27	-
v3.7.7-raring/	11-Feb-2013 20:13	-
v3.7.8-raring/	14-Feb-2013 21:26	-
v3.7.9-raring/	17-Feb-2013 21:27	-
v3.7.10-raring/	27-Feb-2013 18:03	-
v3.8-raring/	19-Feb-2013 01:02	-
v3.8-rc1-raring/	22-Dec-2012 02:58	-
v3.8-rc2-raring/	03-Jan-2013 03:59	-
v3.8-rc3-raring/	10-Jan-2013 03:59	-
v3.8-rc4-raring/	18-Jan-2013 05:01	-
v3.8-rc5-raring/	25-Jan-2013 21:12	-
v3.8-rc6-raring/	01-Feb-2013 03:02	-
v3.8-rc7-raring/	08-Feb-2013 22:13	-

Kernel Up or Downgrade(cont’d)

2. 버전에 맞는 3개의 파일 다운로드(32bit/i386 or 64bit/amd64)



linux-headers-3.7.10-030710-generic_3.7.10-030710.201302271235_amd64.deb	27-Feb-2013 17:51	950K
linux-headers-3.7.10-030710-generic_3.7.10-030710.201302271235_i386.deb	27-Feb-2013 18:03	936K
linux-headers-3.7.10-030710_3.7.10-030710.201302271235_all.deb	27-Feb-2013 17:36	12M
linux-image-3.7.10-030710-generic_3.7.10-030710.201302271235_amd64.deb	27-Feb-2013 17:51	13M
linux-image-3.7.10-030710-generic_3.7.10-030710.201302271235_i386.deb	27-Feb-2013 18:02	12M
linux-image-extra-3.7.10-030710-generic_3.7.10-030710.201302271235_amd64.deb	27-Feb-2013 17:51	29M
linux-image-extra-3.7.10-030710-generic_3.7.10-030710.201302271235_i386.deb	27-Feb-2013 18:03	29M

Kernel Up or Downgrade (cont’d)

3. Image → header_all → header amd64(i386) 설치

```
$>sudo dpkg -i linux-image-3.7.10-030710-generic_3.7.10-030710.201302271235_amd64.deb

$>sudo dpkg -i linux-headers-3.7.10-030710_3.7.10-030710.201302271235_all.deb

$>sudo dpkg -i linux-headers-3.7.10-030710-generic_3.7.10-030710.201302271235_amd64.deb
```

Kernel Up or Downgrade(cont’d)

4. Grub 설정 or grub-customizer 설치

```
$>sudo add-apt-repository ppa:danielrichter2007/grub-customizer

$>sudo apt-get update

$>sudo apt-get install grub-customizer
```

5. 재부팅