“操作系统原理与实践”实验报告

地址映射与共享

一.跟踪地址映射的过程

1. 获得变量线性地址中的段内偏移值

```
[/usr/root]# a.out
The logical/virtual address of i is 0x00004004_
```

2. 找到gdt 表中获得当前进程的l dt 表所在位置。

```
ldtr:s=0x0068, dl=0x52d00068, dh=0x000082fd, valid=1
tr:s=0x0060, dl=0x52e80068, dh=0x00008bfd, valid=1
gdtr:base=0x00005cb8, limit=0x7ff
```

3. 根据ds 变量中的段选择子，从l dt 表所在位置得到数据段段基址。

ds=0x17,所以对应的是LDT表中第三项：

```
<bochs:7> xp /8w 0x00fd52d0
[bochs]:
0x00fd52d0 <bogus+       0>:    0x00000000      0x00000000      0x00000
003     0x10c0fa00
0x00fd52e0 <bogus+      16>:    0x00003fff      0x10c0f300      0x00000
000     0x00fd6000
```

得到段基址：0x10000000

4. 结合前面获得的段内偏移，得到变量的线性地址。

0x10000000 + 0x4004 =0x10004004 。验证：

```
<bochs:8> calc ds:0x4004
0x10004004 268451844
```

5. 根据线性地址查找页目录表，找到对应的页表位置（页表所在的页框号）

```
0x00000100 <bogus+     256>:    0x00fa6027
```

所以页表所在的页框号是0x00fa6。所以页表放在0x00fa6000开始的4k内存上。 6.根据线性地址中的页表序号，从页表中找到变量所在的页框号。 页表序号是4，显示这项内容：

```
<bochs:11> xp /w 0x00fa6000+4*4
[bochs]:
0x00fa6010 <bogus+       0>:    0x00fa3067
```

7. 根据页框号，结合线性地址中的页内偏移量（最后12个bit 组成）得到变量在内存中的物理地址

```
<bochs:12> xp /w 0x00fa3000+4
[bochs]:
0x00fa3004 <bogus+       0>:    0x12345678
```

二.Linux中的共享内存 实验代码： http://git.shiyanlou.com/gaoyuanhezhihao/shiyanlou_cs115/src/master/Lab7 可以参照前面信号量的实验，在操作系统中保存一个数组记录所有共享内存的信息。shmget函数申请内存页，同时在把相关内存记录下来。而shmat则把这个内存页 和当前进程线性空间关联起来。此时可以考虑进程64MB线性空间的最后区域。因为最后的128KB被用来保存进程程序的参数和环境变量，所以可以从到数128KB开始使用。可以参考put_page函数

参照前面信号量的实验，添加两个系统调用：shmget(),shmat()。在include/unistd.h中添加两个系统调用功能号

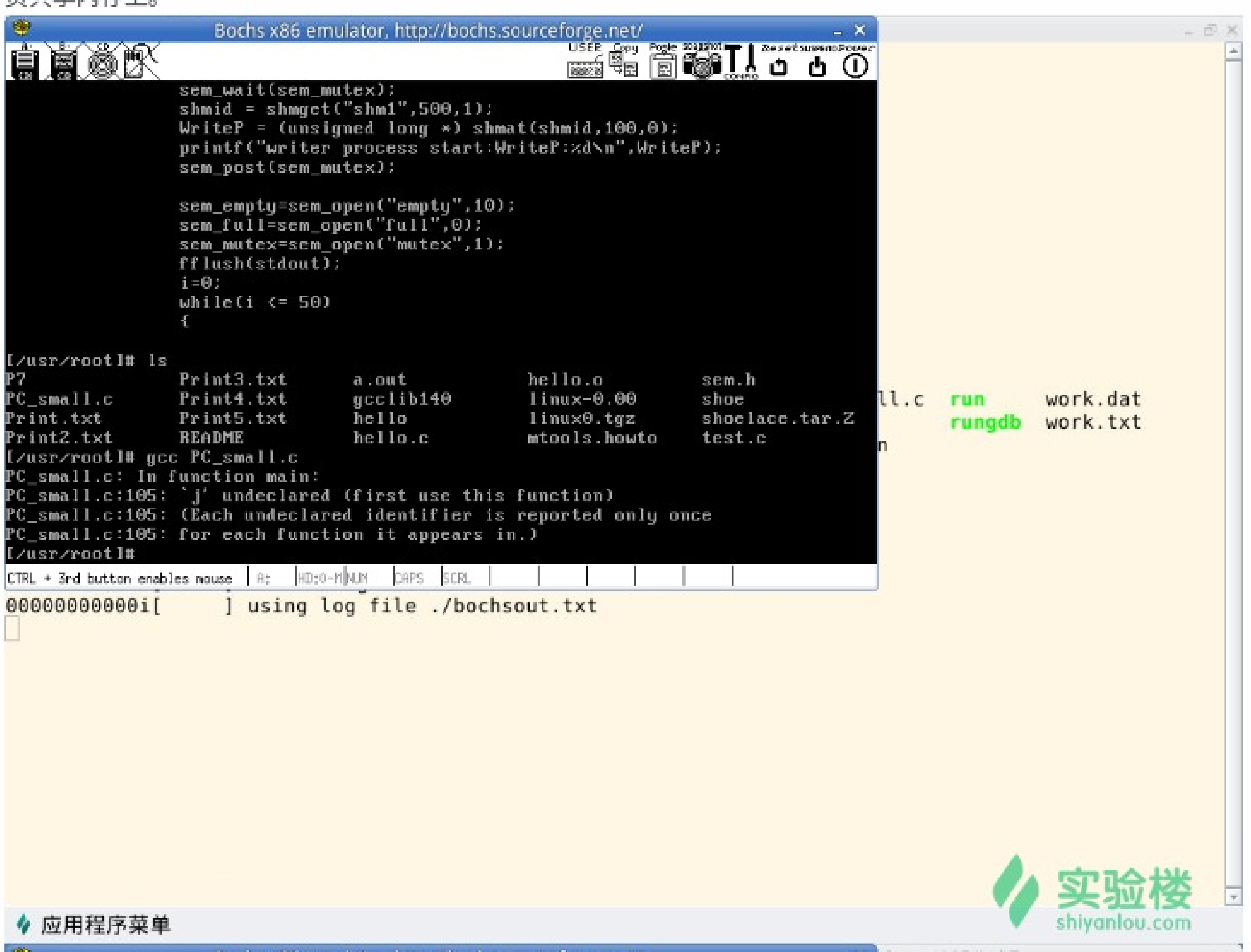
```
#define __NR_shmget     76
#define __NR_shmat      77
```

2.增加kernel/system_call.s中的nr_system_calls 3.在include/linux/sys.h 的sys_call_table 中添加这四个函数指针 4.新建mm/shm.c，在里面实现这两个系统调用函数。 整体的代码在这： http://git.shiyanlou.com/gaoyuanhezhihao/shiyanlou_cs115/src/master/Lab7/linux -0.11/mm/shm.c 操作系统对每块共享内存保存相应的信息，每块内存对应一个如下的结构体实例

```
struct    shm_Node{
        unsigned    long    FreePageAddr;
        char    name[ 20 ];
};
```

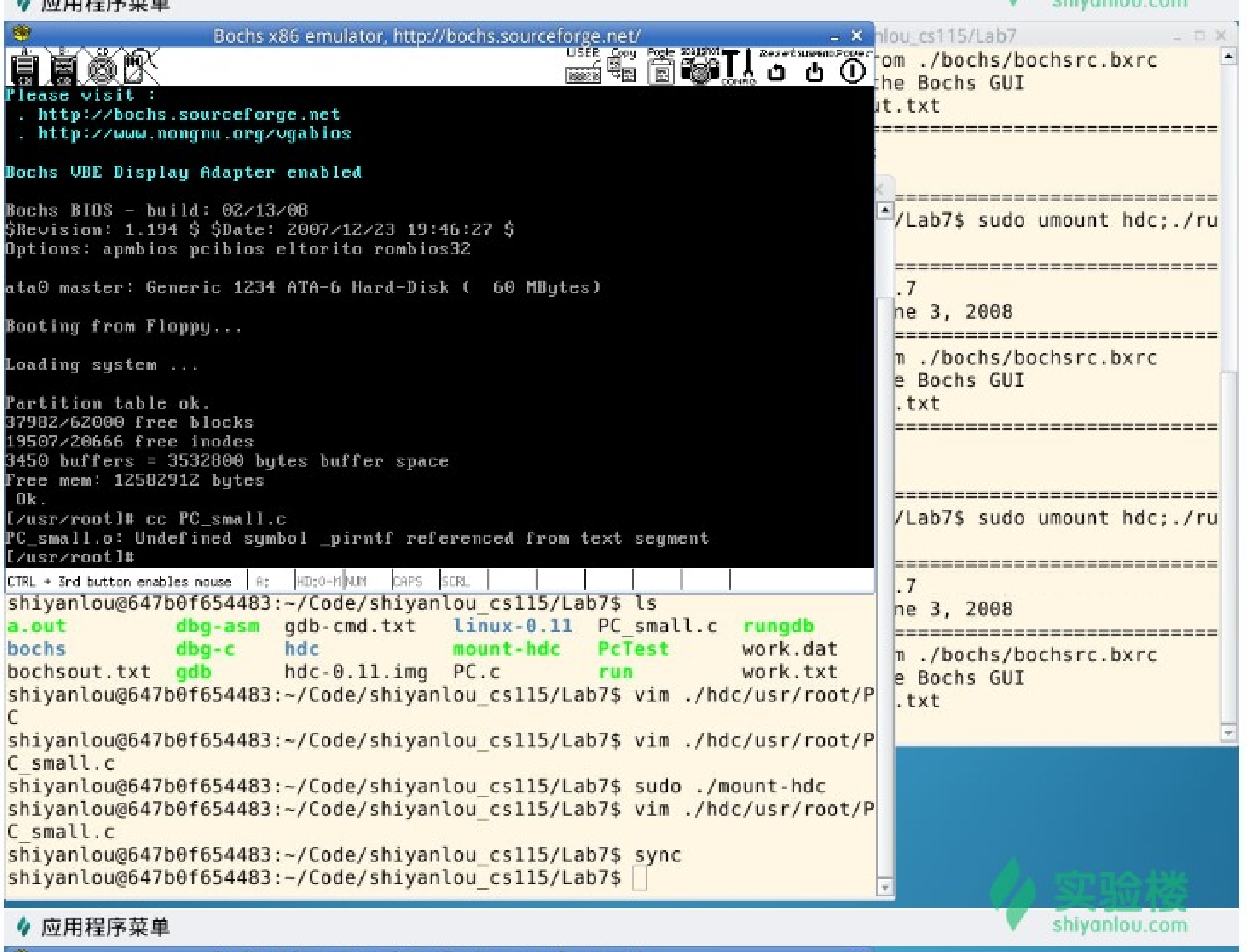
系统中通过`struct    shm_Node    ShmNodeArray[MAX_SHMARRAY_NUM]={0};`来维护这些共享内存。这个方法只是一时求快之举，限制了最大的共享内存数量。可以考虑使用链数据结构。 shmget函数参数主要是一个字符串，代表需要申请的共享内存的名称。函数首先检查是否已经存在这样的一个共享内存，如果存在，则把这块共享内存的id返回。否则申请一页空闲内存，在系统记录中新建一条记录。

shmat函数首先在共享内存数组中查找对应的项，再获得当前进程线性地址空间倒数132KB的地址，然后通过调用put_page函数把这个线性地址绑定到共享内存页中。这样当前进程倒数132KB~倒数128KB之间的那页就映射到了这页共享内存上。



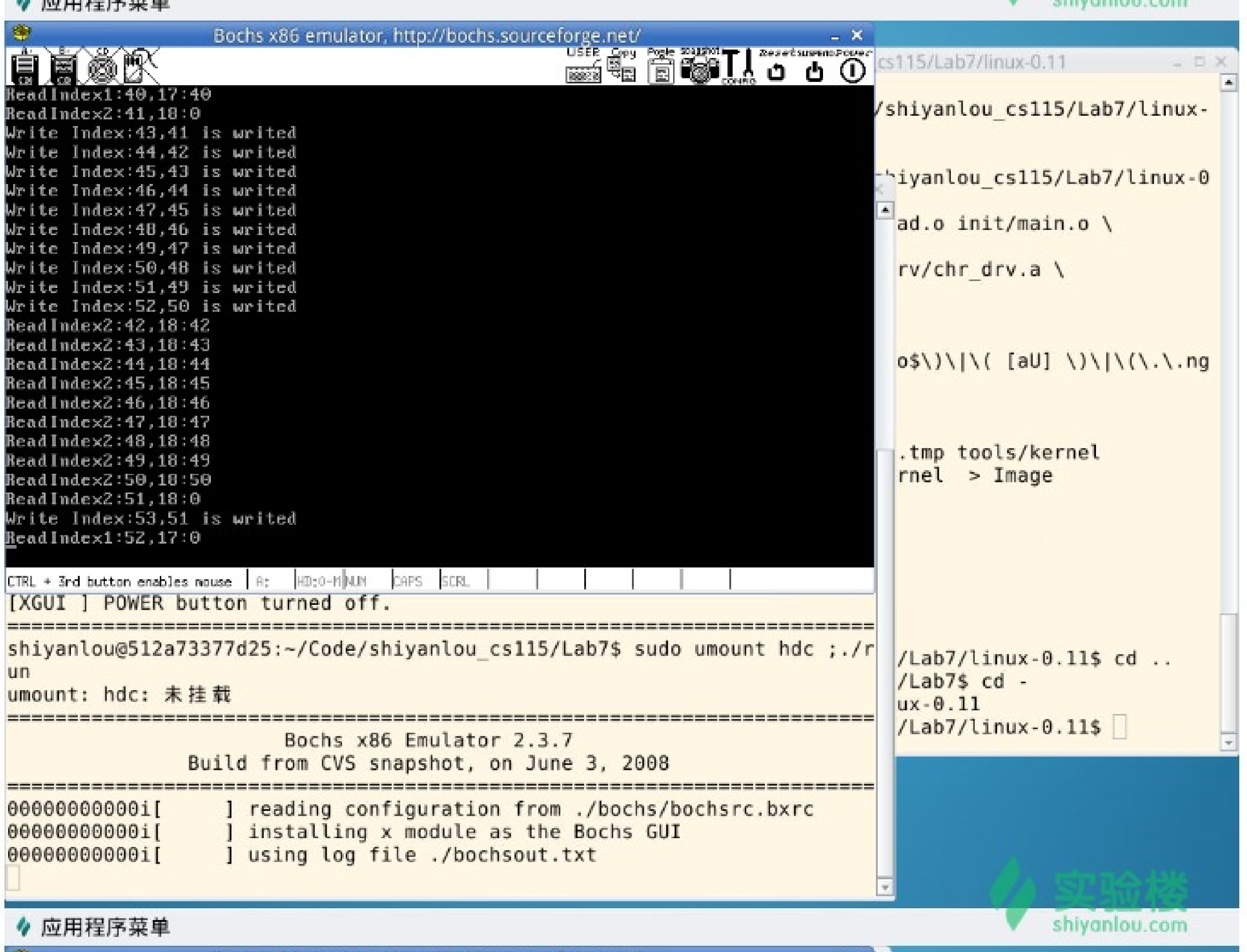
```
            sem_wait(sem_mutex);
            shmid = shmget("shm1",500,1);
            WriteP = (unsigned long *) shmat(shmid,100,0);
            printf("writer process start:WriteP:%d\n",WriteP);
            sem_post(sem_mutex);

            sem_empty=sem_open("empty",10);
            sem_full=sem_open("full",0);
            sem_mutex=sem_open("mutex",1);
            fflush(stdout);
            i=0;
            while(i <= 50)
            {

[/usr/root]# ls
P7          Print3.txt    a.out       hello.o        sem.h
PC_small.c  Print4.txt    gcclib140   linux-0.00     shoe
Print.txt   Print5.txt    hello       linux0.tgz     shoelace.tar.Z
Print2.txt  README        hello.c     mtools.howto   test.c
[/usr/root]# gcc PC_small.c
PC_small.c: In function main:
PC_small.c:105: `j' undeclared (first use this function)
PC_small.c:105: (Each undeclared identifier is reported only once
PC_small.c:105: for each function it appears in.)
[/usr/root]#
```

```
00000000000i[      ] using log file ./bochsout.txt
```



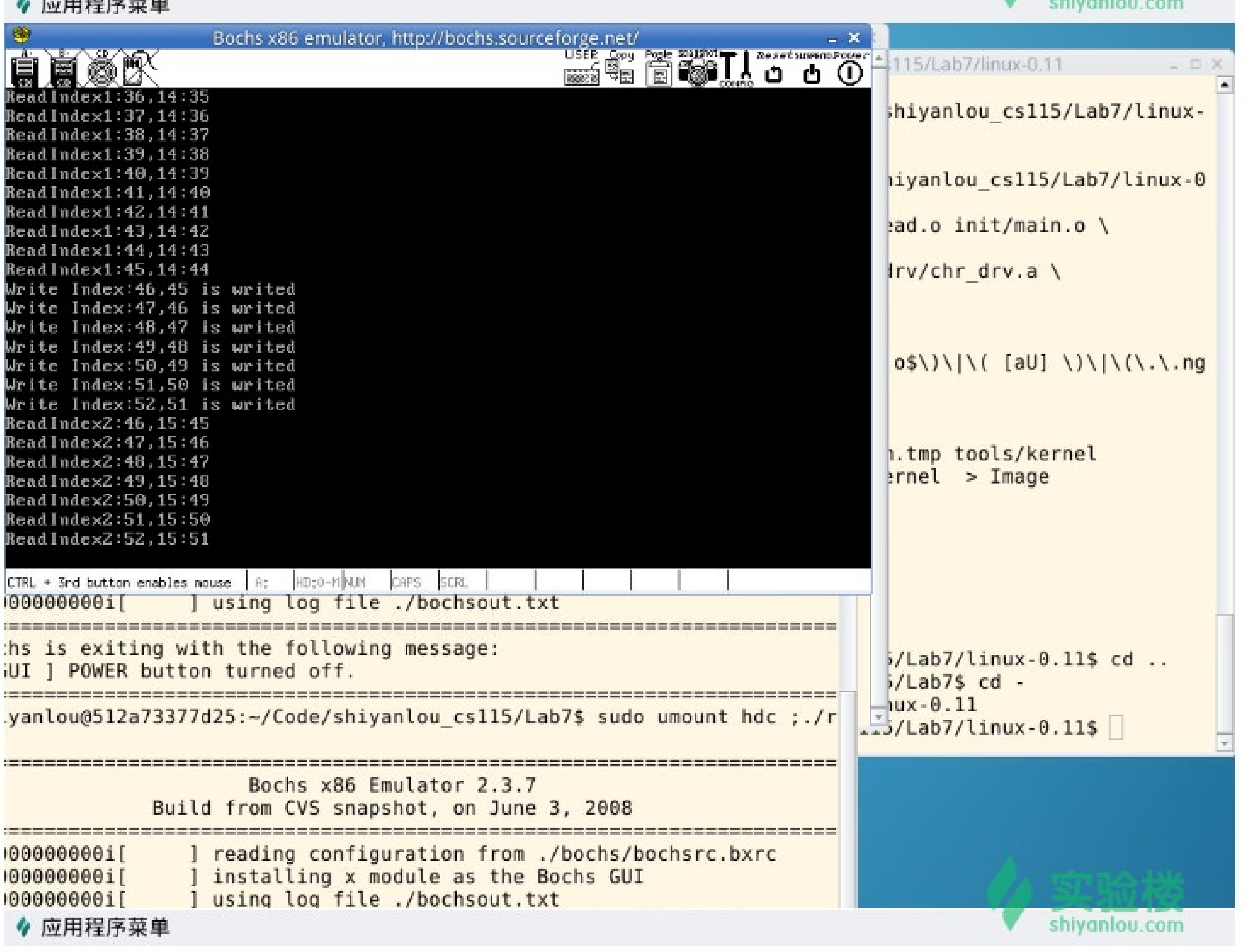
```
Please visit :
 . http://bochs.sourceforge.net
 . http://www.nongnu.org/vgabios

Bochs VBE Display Adapter enabled

Bochs BIOS - build: 02/13/08
$Revision: 1.194 $ $Date: 2007/12/23 19:46:27 $
Options: apmbios pcibios eltorito rombios32

ata0 master: Generic 1234 ATA-6 Hard-Disk (  60 MBytes)

Booting from Floppy...

Loading system ...

Partition table ok.
37982/62000 free blocks
19507/20666 free inodes
3450 buffers = 3532800 bytes buffer space
Free mem: 12582912 bytes
 Ok.
[/usr/root]# cc PC_small.c
PC_small.o: Undefined symbol _pirntf referenced from text segment
[/usr/root]#
```

```
shiyanlou@647b0f654483:~/Code/shiyanlou_cs115/Lab7$ ls
a.out        dbg-asm  gdb-cmd.txt   linux-0.11  PC_small.c  rungdb
bochs        dbg-c    hdc           mount-hdc   PcTest      work.dat
bochsout.txt gdb      hdc-0.11.img  PC.c        run         work.txt
shiyanlou@647b0f654483:~/Code/shiyanlou_cs115/Lab7$ vim ./hdc/usr/root/P
C
shiyanlou@647b0f654483:~/Code/shiyanlou_cs115/Lab7$ vim ./hdc/usr/root/P
C_small.c
shiyanlou@647b0f654483:~/Code/shiyanlou_cs115/Lab7$ sudo ./mount-hdc
shiyanlou@647b0f654483:~/Code/shiyanlou_cs115/Lab7$ vim ./hdc/usr/root/P
C_small.c
shiyanlou@647b0f654483:~/Code/shiyanlou_cs115/Lab7$ sync
shiyanlou@647b0f654483:~/Code/shiyanlou_cs115/Lab7$
```



```
ReadIndex1:40,17:40
ReadIndex2:41,18:0
Write Index:43,41 is writed
Write Index:44,42 is writed
Write Index:45,43 is writed
Write Index:46,44 is writed
Write Index:47,45 is writed
Write Index:48,46 is writed
Write Index:49,47 is writed
Write Index:50,48 is writed
Write Index:51,49 is writed
Write Index:52,50 is writed
ReadIndex2:42,18:42
ReadIndex2:43,18:43
ReadIndex2:44,18:44
ReadIndex2:45,18:45
ReadIndex2:46,18:46
ReadIndex2:47,18:47
ReadIndex2:48,18:48
ReadIndex2:49,18:49
ReadIndex2:50,18:50
ReadIndex2:51,18:0
Write Index:53,51 is writed
ReadIndex1:52,17:0
```

```
[XGUI ] POWER button turned off.
========================================================================
shiyanlou@512a73377d25:~/Code/shiyanlou_cs115/Lab7$ sudo umount hdc ;./r
un
umount: hdc: 未挂载
========================================================================
                      Bochs x86 Emulator 2.3.7
              Build from CVS snapshot, on June 3, 2008
========================================================================
00000000000i[      ] reading configuration from ./bochs/bochsrc.bxrc
00000000000i[      ] installing x module as the Bochs GUI
00000000000i[      ] using log file ./bochsout.txt
```



```
ReadIndex1:36,14:35
ReadIndex1:37,14:36
ReadIndex1:38,14:37
ReadIndex1:39,14:38
ReadIndex1:40,14:39
ReadIndex1:41,14:40
ReadIndex1:42,14:41
ReadIndex1:43,14:42
ReadIndex1:44,14:43
ReadIndex1:45,14:44
Write Index:46,45 is writed
Write Index:47,46 is writed
Write Index:48,47 is writed
Write Index:49,48 is writed
Write Index:50,49 is writed
Write Index:51,50 is writed
Write Index:52,51 is writed
ReadIndex2:46,15:45
ReadIndex2:47,15:46
ReadIndex2:48,15:47
ReadIndex2:49,15:48
ReadIndex2:50,15:49
ReadIndex2:51,15:50
ReadIndex2:52,15:51
```

```
000000000i[      ] using log file ./bochsout.txt
========================================================================
hs is exiting with the following message:
UI ] POWER button turned off.
========================================================================
yanlou@512a73377d25:~/Code/shiyanlou_cs115/Lab7$ sudo umount hdc ;./r

========================================================================
                      Bochs x86 Emulator 2.3.7
              Build from CVS snapshot, on June 3, 2008
========================================================================
000000000i[      ] reading configuration from ./bochs/bochsrc.bxrc
000000000i[      ] installing x module as the Bochs GUI
000000000i[      ] using log file ./bochsout.txt
```

0