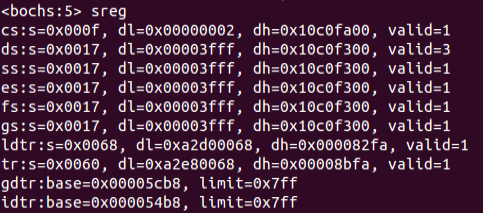
# Operating System Lab 4

**黄渝光 白广通**

**完成实验后，在实验报告中回答如下问题：**

1. **对于地址映射实验部分，列出你认为最重要的那几步（不超过4步），并给出你获得的实验数据。**
2. **test.c退出后，如果马上再运行一次，并再进行地址跟踪，你发现有哪些异同？为什么？**
3. （1）得到虚拟地址

通过sreg得到ds内容：

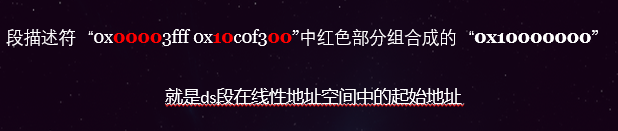


偏移地址0x3004

虚拟地址即为0x00173004

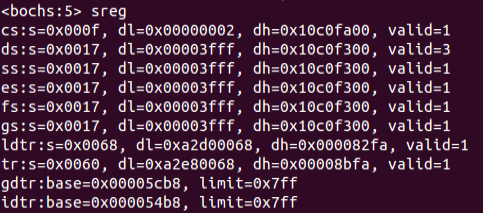
（2）得到线性地址

Ds段的段描述符的特定组合就是ds段在线性空间中的起始地址



以下是获得的流程：

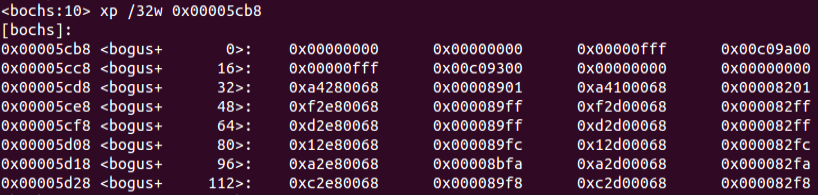
Sreg列出：



Ldtr保存的是LDT在GDT中的位置

ldtr的值是0x0068=0000000001101000（二进制），表示LDT表存放在GDT表的1101(二进制)=13

列出GDT前16项：

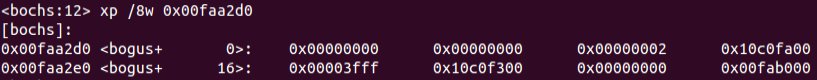


xp /2w 0x00005cb8 + 13 \* 8得到：



“0x**a2d0**0068 0x**00**0082**fa**”将其中的加粗数字组合为“**0x00faa2d0**”，这就是LDT表的物理地址

这就是LDT表的前4项内容了：



第3项“0x00003fff 0x10c0f300”就是搜寻好久的ds的段描述符了

段描述符“0x**0000**3fff 0x**10**c0f3**00**”中粗体字体部分组合成的“**0x10000000**”

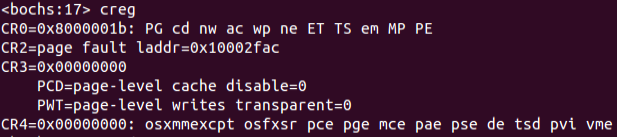
就是ds段在线性地址空间中的起始地址。

所以ds:0x3004的线性地址就是：0x10000000 + 0x3004 = 0x10003004

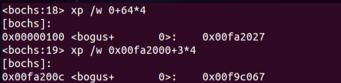
（3）得到物理地址

0x10003004的页目录号是64，页号3，页内偏移是4

IA-32下，页目录表的位置由CR3寄存器指引。“creg”命令可以看到：



页目录表的位置由CR3寄存器指引，为0



用“xp /w 0+64\*4”查看

页表所在物理页框号为0x00fa2，页表在物理内存的0x00fa2000位置

从该位置开始查找3号页表项，得到（xp /w 0x00fa2000+3\*4）

3号页表项: 0x00f9c067

线性地址0x10003004对应的物理页框号为0x00f9c

页内偏移0x004接到一起，得到0x00f9c004，这就是变量i的物理地址

1. 逻辑地址和虚拟地址不变，物理地址变了。

进程的每一次加载，操作系统将为其分配64M的虚拟地址空间，并且逻辑地址不变，操作系统根据进程的LDT在GDT中的nr来分配虚拟地址，前后两次运行的进程的nr没有变，因此虚拟地址没有变化。而物理地址因为页目录地址由操作系统放置，物理分页改变了而随之改变。