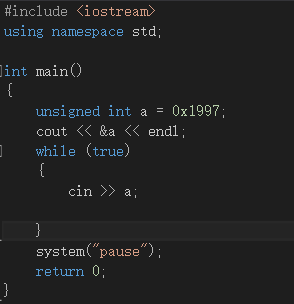
为了避免我下次再忘记怎么寻址，我写个文档记录下来好了。

第一步：随便写个demo，定义个变量，赋值，输出地址，让程序等待别死。



第二步：判断是否开启了PAE，即判断cr4第五位是否为1，为1则是开启



很明显我的虚拟机是开启的。

第三步：找到cr3的值，cr3在kprocess叫DirectoryBase



第四步：分析数据地址



因为开启了PAE，所以结构是

PDP->PDB->PTB->OFFSET

对应大小是：2位，9位，9位，12位

含义是：页目录指针->页目录项->页表->页内偏移

所以对应的数据是：

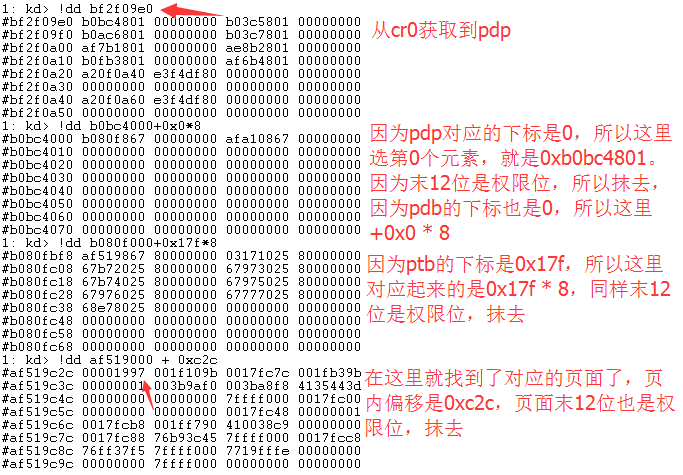
PDP : 0

PDB : 0

PTB : 0x17f

OFFSET : c2c

第五步：从cr3获取pdp，从pdp获取pdb，从pdb获取ptb



重点记一下：因为开启了PDE模式，页目录和页表项从32位扩展为了64位，因此这里每次都是\*8。如果是未开启PDE模式的话是\*4。