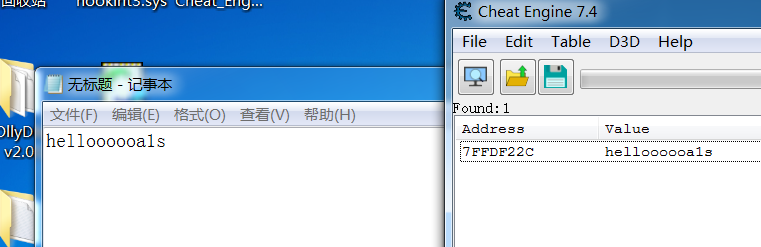
# 一、拆线性地址

这节课主要讲了在101012分页下如何拆线性地址得到物理地址。

线性地址=base+逻辑地址

所谓101012，就是把32位线性地址拆成10位-10位-12位，不管是什么分页，最后一定是12，12表示12位，也就是一个页的大小。2^12=4096=4KB



找到字符串的线性地址

7FFDF22C

0111 1111 1111 1101 1111 0010 0010 1100

按照10位-10位-12位来拆，不足12位的，高位补0，这样就得到了页目录项PDE,页表项PTE和页内偏移

0001 1111 1111 1ff

0011 1101 1111 3df

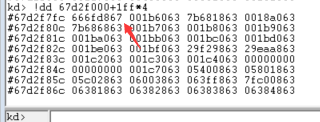
0010 0010 1100 22c

找CR3，等于 67d2f000



以CR3为基址，加上4乘以PDE，可以找到页表

!dd CR3+PDE\*4



页表是 666fd867，其中尾部的867是属性，把它清零就得到了页表基址666fd000

接下来通过页表+PTE\*4找物理页

!dd 666fd000+4\*3df



找到物理页是69c0a867 ，同样把属性为清零，物理页是69c0a000

然后加上页内偏移就能找到数据的物理地址：

!du 69c0a000+22c

