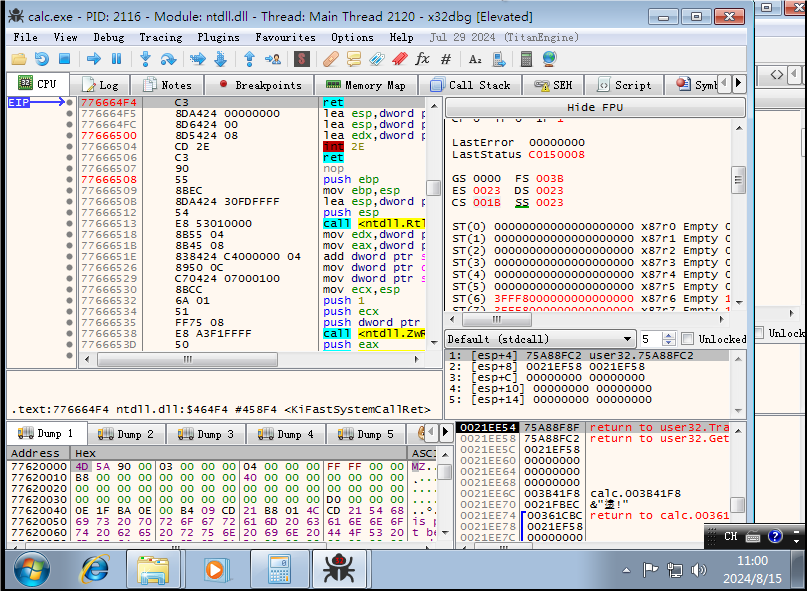
# 环境

环境：win7x86



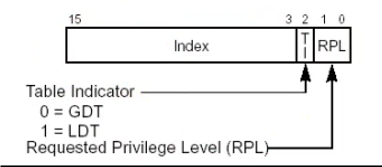
X32dbg附加计算器

DS=0023

分析DS

# 分析DS

## 2.1段选择符



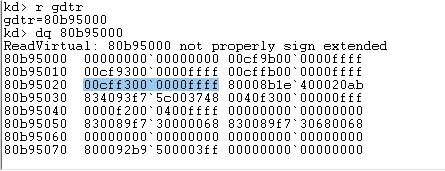
DS=0023 （ 0000 0000 0010 0011 ） 4b&FFFC 0100 1010

Index=4 （0000 0000 0010 0） //这就是段描述符的index

Table Indicator=0 （0） //是gdtr还是ldtr 全局描述表还是本地描述表 0=全局

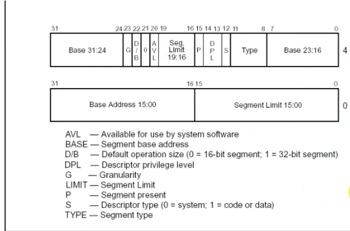
RPL=3 （11） //request privilege leave请求特权级别3=R3，就是三环代码

## 段描述符



Index=4，索引从0开始，看第五个

段描述符为：00cff300`0000ffff



特别提示：首先看S 位，为1才用这个结构解析，再看P位，是否有效

根据这个图的结构拆分00cff300`0000ffff

Base=00000000 //这是基址

G=1 //g=0，Segment按照字节算，g=1，Segment按照页算，一页4kb

Segment最大值为fffff，一页4kb=0x1000,所以(fffff+1)\*0x1000=4G,不是页的话最多0xFFFFF

0x100000=1M

D/B=1 //是32位还是16位，DB位

AVL=0 //用户自定义的操作

Segment=fffff //扩展范围

P=1 //有效位，置零这个段失去作用

DPL=3 //descriptor privilege leave描述特权级别3=R3，就是三环代码

S=1 //如果是系统段，有中断门，调用门等就是0，

//数据段、代码段是1，如果是1才用这个结构分析

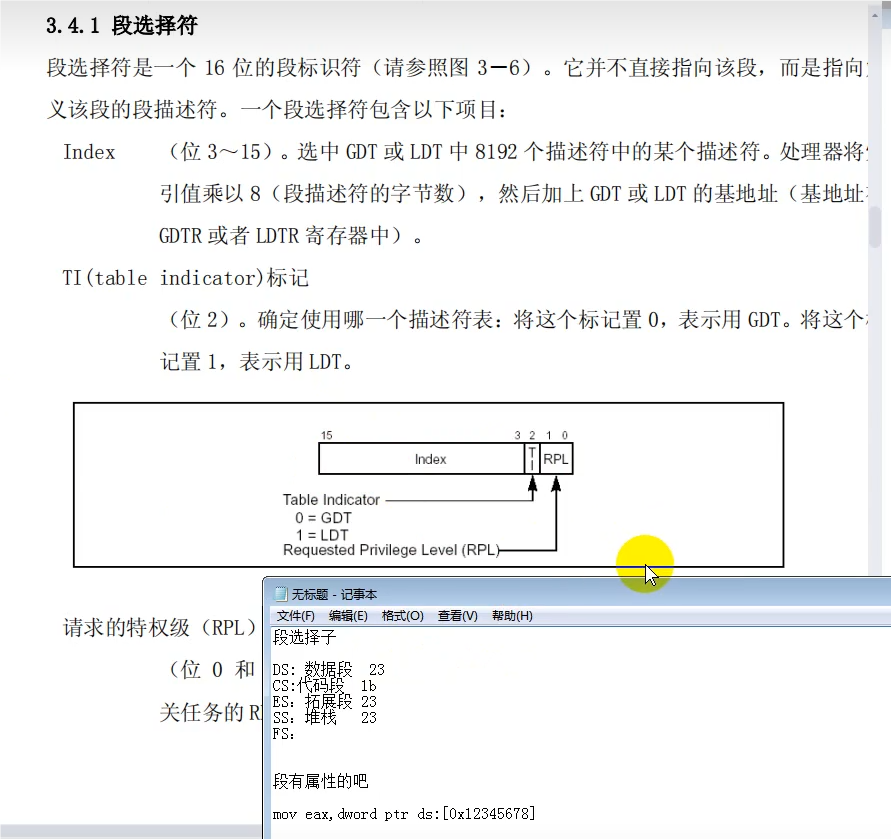
Type=3 //第1位表示是代码段， 第3位表示是否可写，第4位表示是否被访问过

//第二位表示扩展方向，向上扩展=0，表示Segment范围内的地址可以访问

//向上扩展=1，表示Segment范围内的地址不可以访问

# 资料

## 段选择符



## 段描述符

