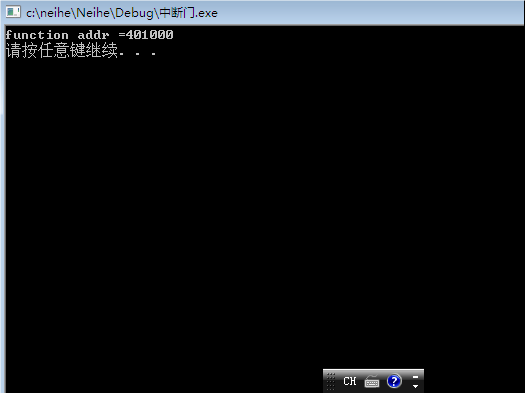
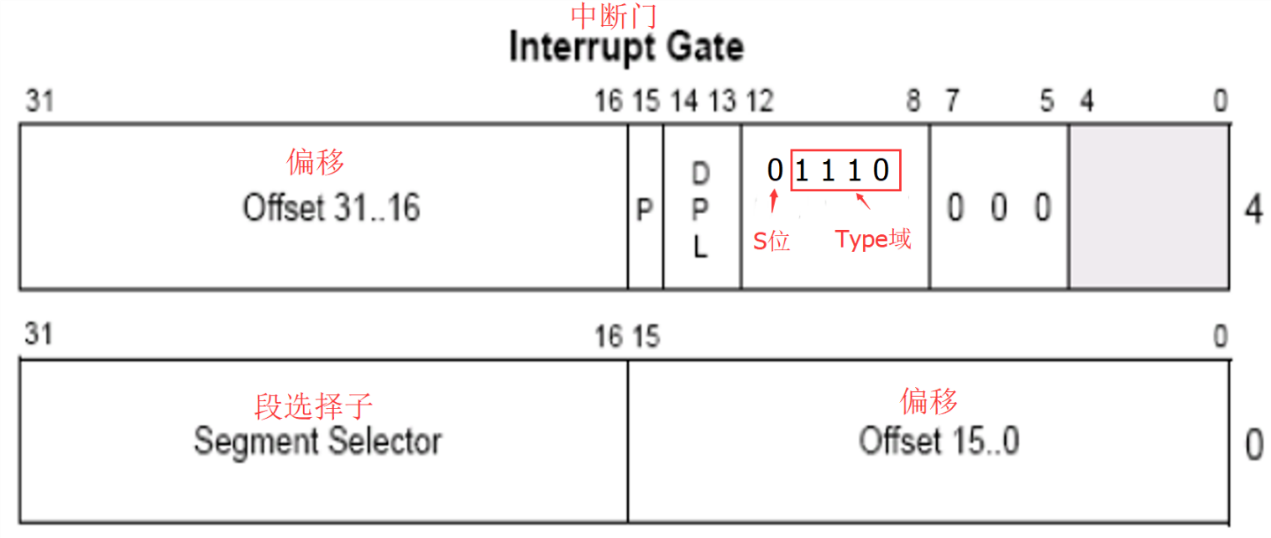
# 环境

环境：win7x86



拿到方法的地址，通过修改段描述符来跳转到这个方法



kd> r idtr

idtr=80b95400

修改idtr表的第32位

8\*32+0x80b95400=80b95500

kd> dq 80b95400 l 60

ReadVirtual: 80b95480 not properly sign extended

80b95400 83e88e00`00080200 83e88e00`00080390

80b95410 00008500`00580000 83e8ee00`00080800

Int 3 是 83e8ee00`00080800

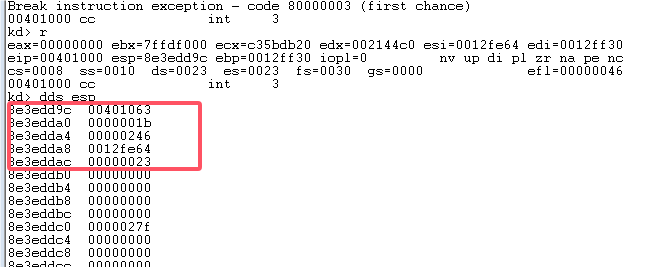
Int32跳转到int3

0040ee00`00080100

修改80b95500为0040ee00`00080100

kd> eq 80b95400 0040ee00`00080100

WriteVirtual: 80b95500 not properly sign extended

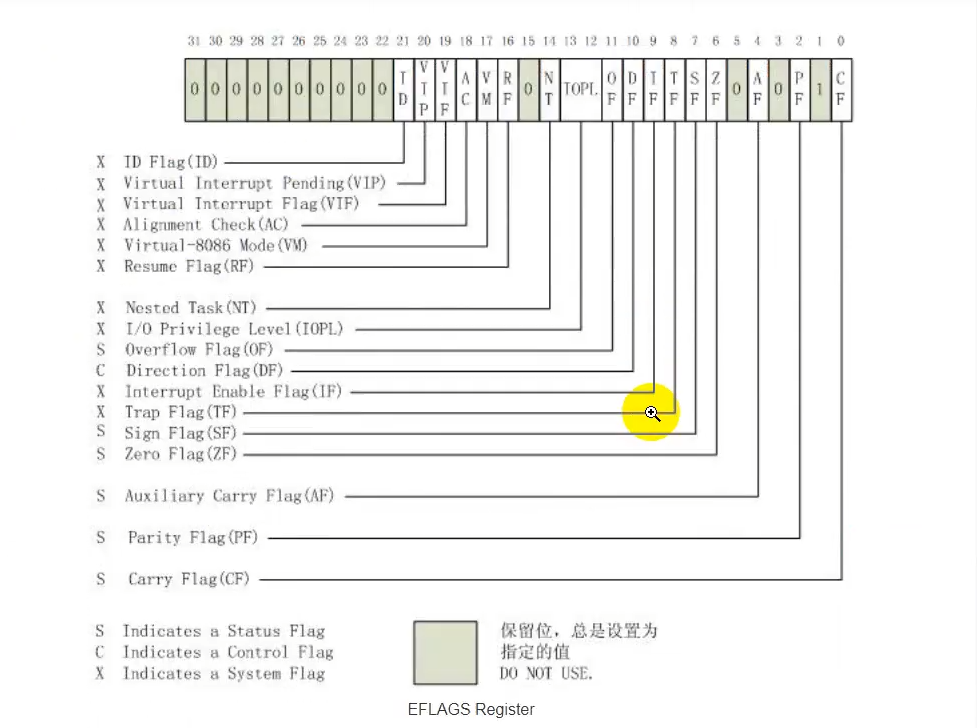


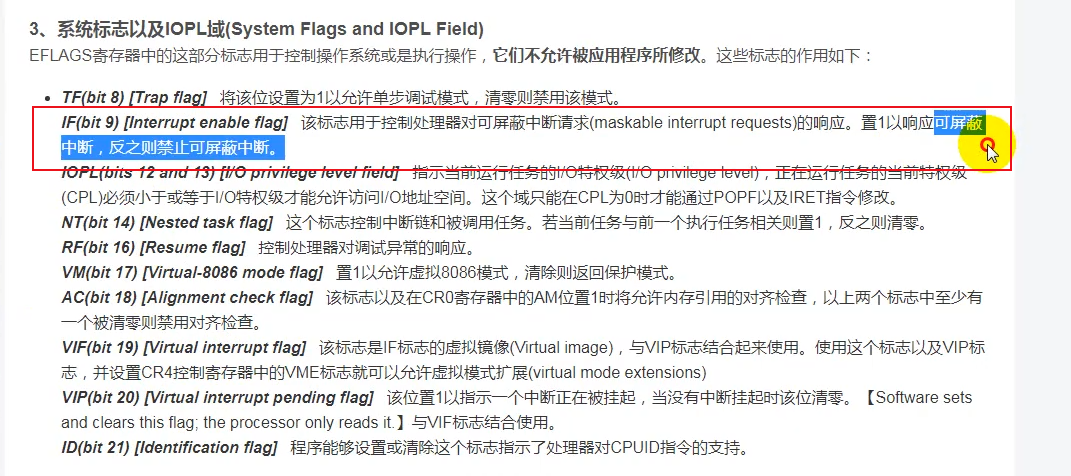
在代码中断了下来，查看esp

可以看到eip、cs、eflags、esp、ss

# 资料

Eflags寄存器





S位等于0时， Type的含义 1100为调用门，1110为中断门

