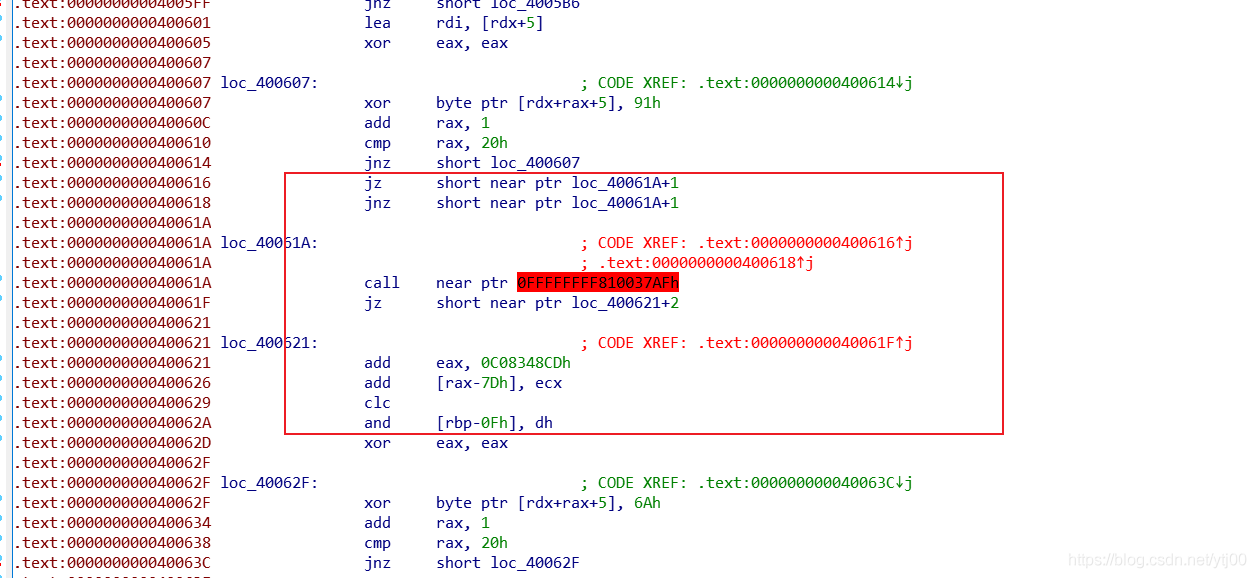
Ida花指令混淆技巧--完全nop

无壳，ida64打开，发现不能f5，而且也没有main函数，判断应该是用了混淆

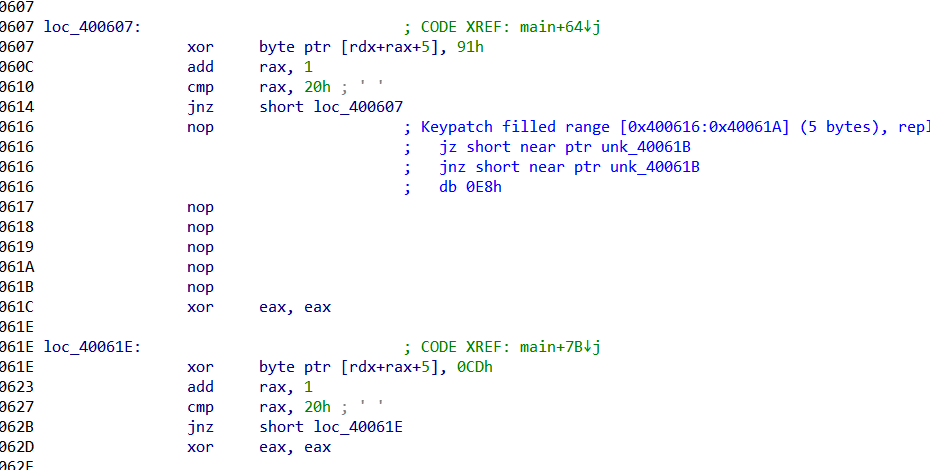
从上往下看汇编代码，找到第一处问题



这里jz和jnz一看就有问题，大概有四五处吧，nop掉，p声明函数

但我在自己做的时候发现nop掉jz和jnz跳转的addr+1 的addr处为nop后，c代码化addr+1处的代码，p声明main函数失败

后来发现不仅仅addr处的单行db要nop，jz和jnz两条语句也完全要nop掉就可以p声明main函数了



Angr见脚本

本题是因为没有输入所以要直接在内存中设置符号变量--注意不要选取内存中的位置（可能会失败），可以选取内存外的数据

另外需要设置相关寄存器的值，虽然没有rdi代表的变量，但在汇编中可以很明确地看到rdi代表了相关的字符串进行计算，所以也要设置rdi的值