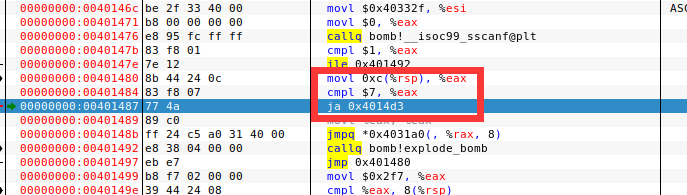
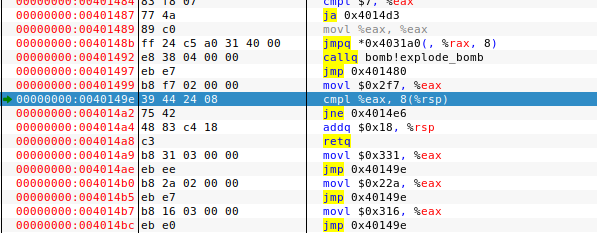
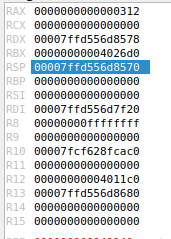


由第3关刚开始的函数可以知道应该是输入了两个整数，结果放到rsp偏移量分别为0xC和0x8的位置(第一个数偏移为0xC，第二个数偏移为0x8)，偏移即十进制的12和8，是两个4字节的整数。



读取之后将rsp偏移为0xC(第一个数)放到%eax寄存器中，然后将这个数与7比较，如果大于7就跳转到0x4014d3(这个位置将执行爆炸函数，我们不应让这个函数执行)，因此必须让输入的第一个数小于或等于7。





第二次比较时，比较了rsp偏移8处的数据(也就是输入的第二个数)和eax寄存器，通过EDB软件动态分析可知此时eax寄存器中的数为0x312(十进制的786)，如果两数不相等就执行爆炸函数，因此可知此处第二个数应该输入786。