

**汇编语言与逆向技术实验报告**

**实验十： CTF（Capture The Flag）夺旗赛**

****

学 院 网络空间安全学院

专 业 信息安全

学 号 2212046

姓 名 王昱

班 级 信息安全班

1. **实验目的**
   1. 熟悉静态反汇编工具IDA Freeware；
   2. 掌握对二进制代码内部逻辑关系的分析；
   3. 掌握对二进制代码的修改和保存。
2. **实验原理**
3. CTF

CTF是一种流行的信息安全竞赛形式，可意译为“夺旗赛”。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。

CTF竞赛模式具体分为以下三类：

一、解题模式（Jeopardy）

在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含**逆向分析**、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

二、攻防模式（Attack-Defense）

在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

三、混合模式（Mix）

结合了解题模式与攻防模式的CTF[赛制](https://baike.baidu.com/item/%E8%B5%9B%E5%88%B6" \t "_blank)，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

1. 解题

Flag隐藏在game.exe的二进制代码中。通过对game.exe的修改，使game.exe能够顺利的执行，完成对Flag的解密。

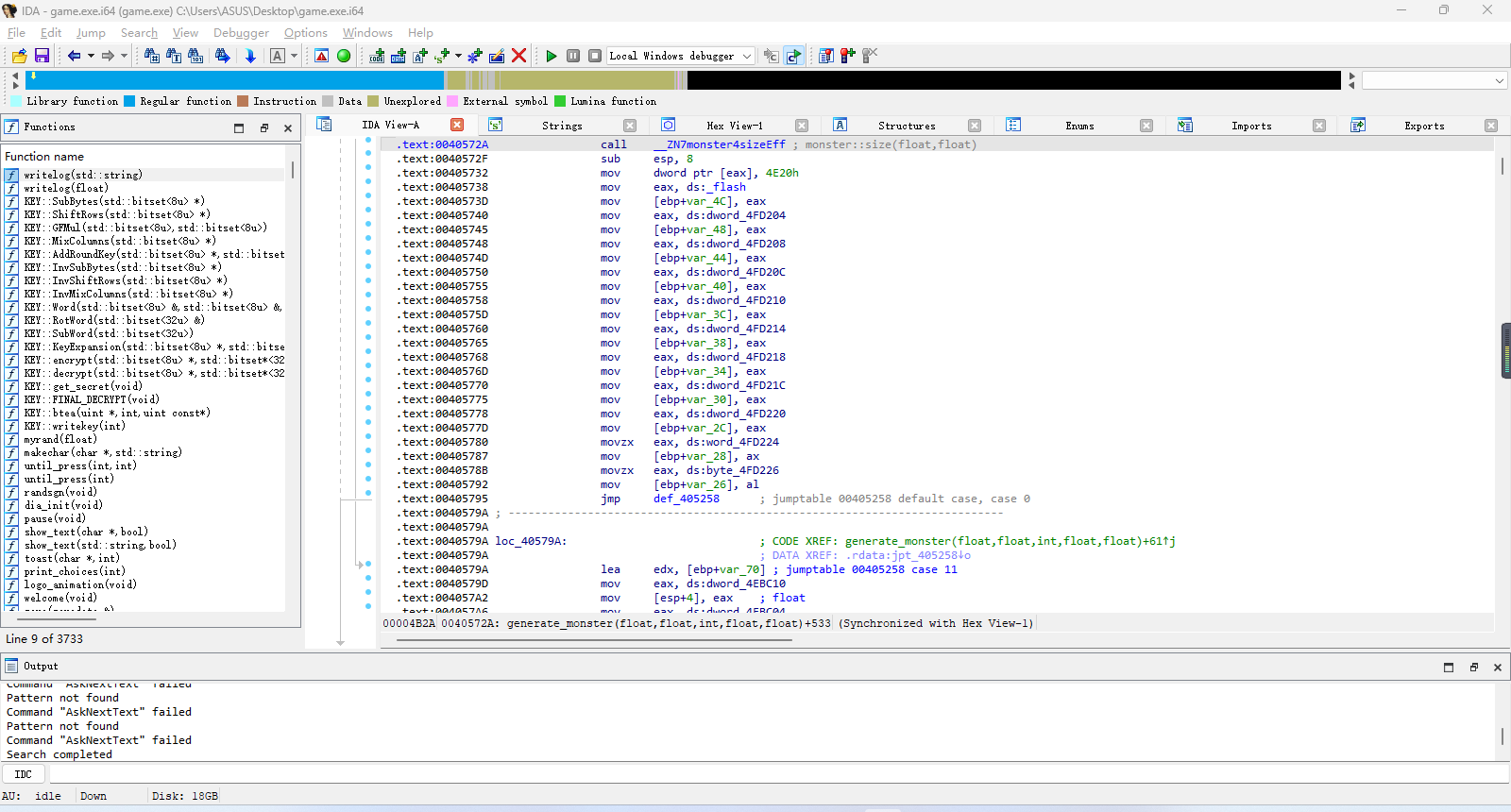
1. 技巧A：利用IDA Pro修改静态资源

* 第一步，在反汇编代码中（IDA View）找到静态资源。
* 第二步，在十六进制视图中（Hex View）找到指定区域，右键选择Edit对资源进行修改。修改完毕后，右键选择Apply changes应用修改。
* 第三步，点击Edit->Patch program->Apply patches to input file，建议选中创建备份的选项，完成修改。

1. 技巧B：利用IDA Pro修改汇编指令

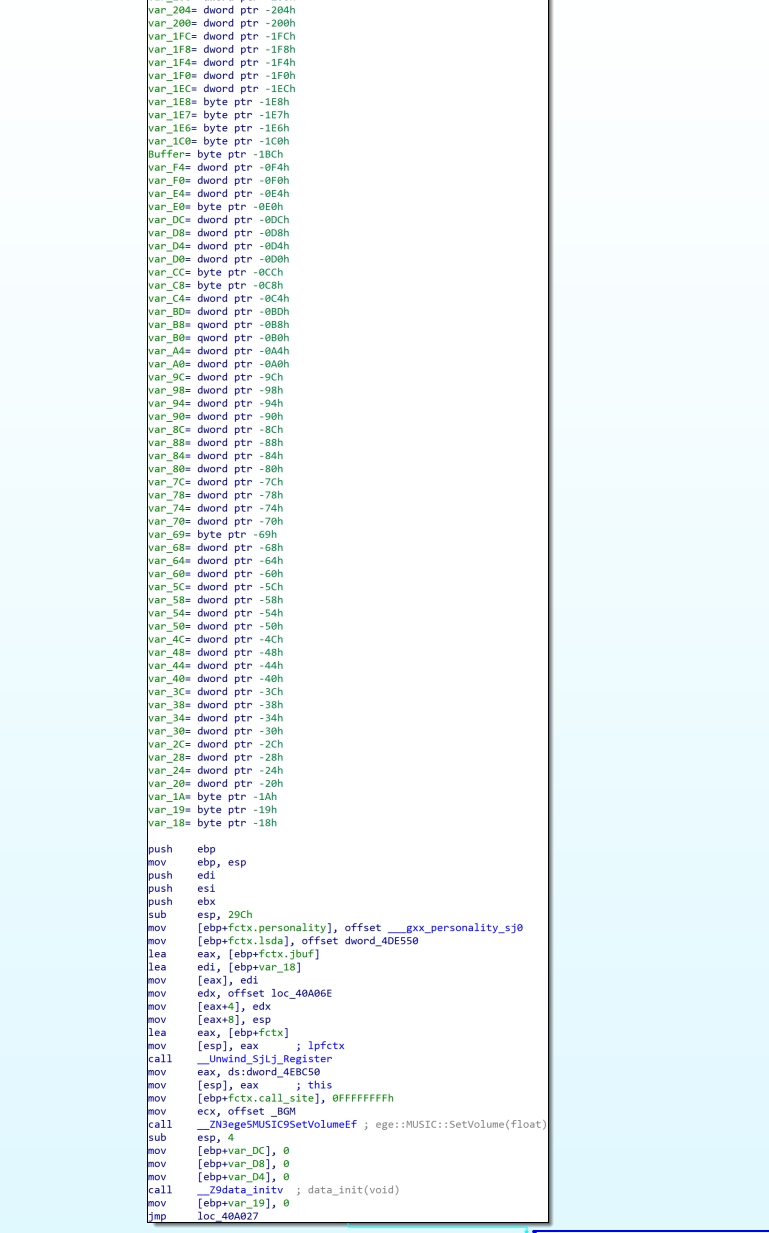
* 第一步，在反汇编代码中（IDA View）找到需要修改的汇编指令。
* 第二步，点击Edit->Patch program->Assemble，输入新的汇编指令。
* 第三步，点击Edit->Patch program->Apply patches to input file，建议选中创建备份的选项，完成修改。

1. **实验过程**

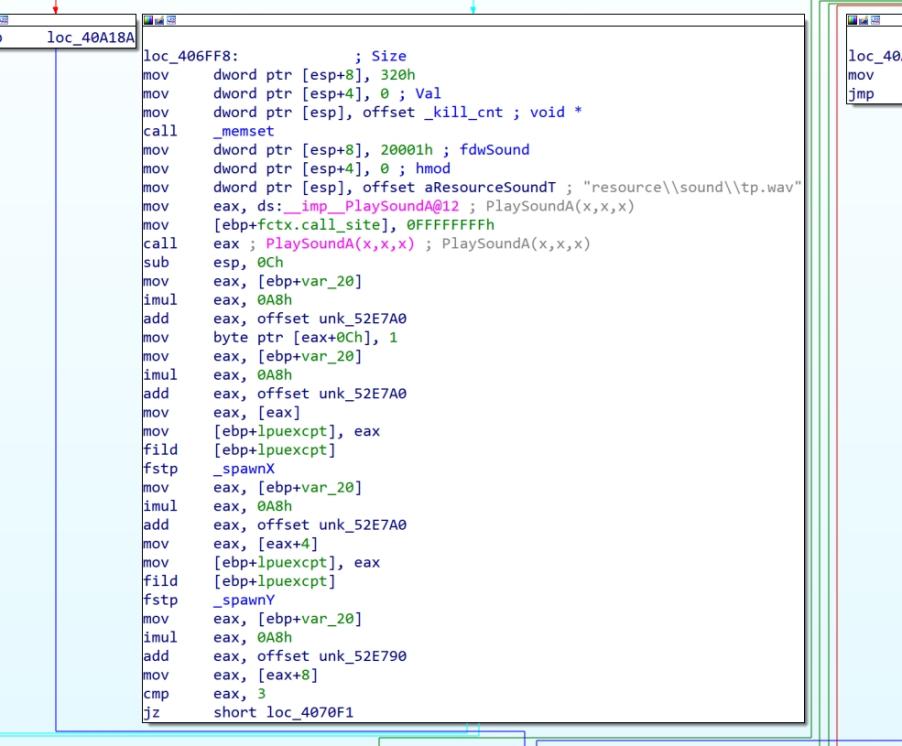
首先通过IDA Freeware打开程序：

**（一）**逆向分析game.exe二进制代码的主要逻辑结构和重要数据

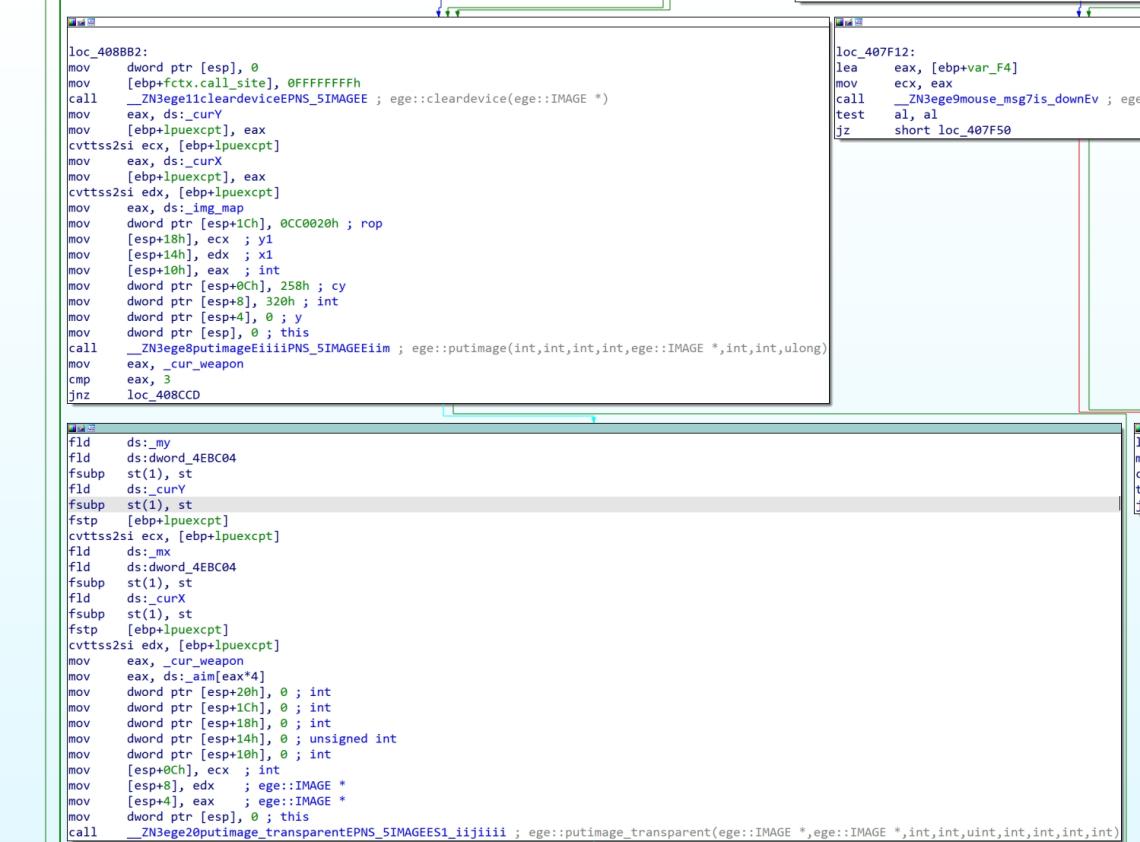
（1）主要逻辑结构



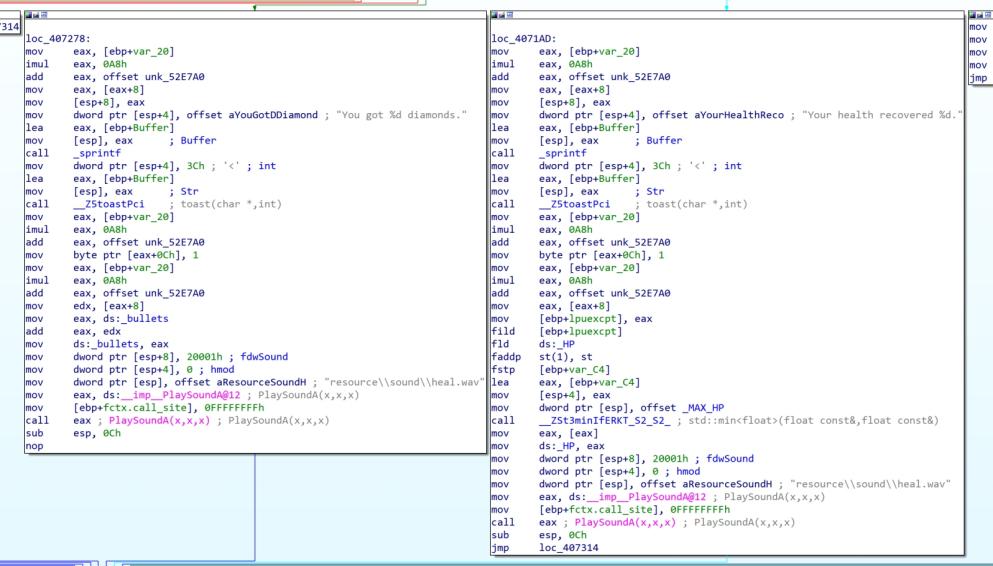
利用resource中的文件加载游戏声音



利用resource中的文件加载图片



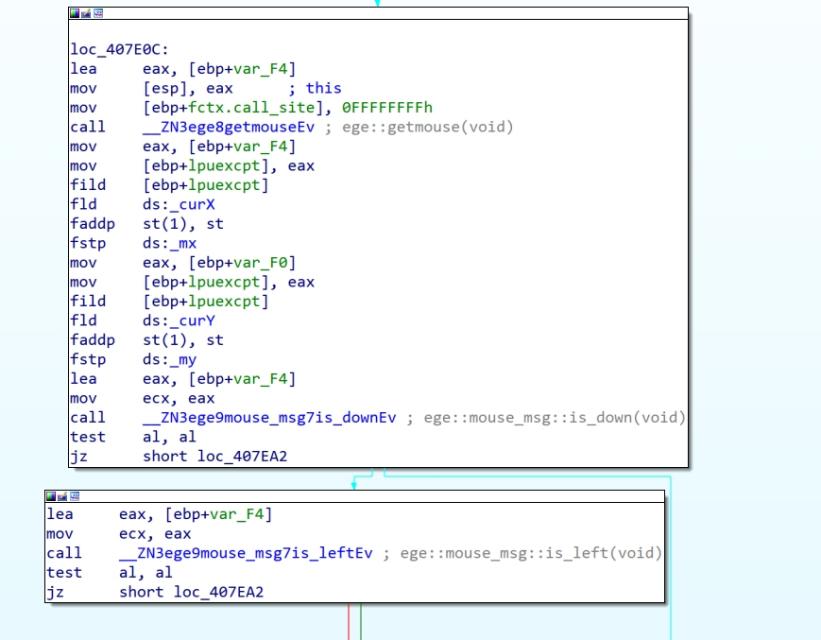
钻石和血量恢复



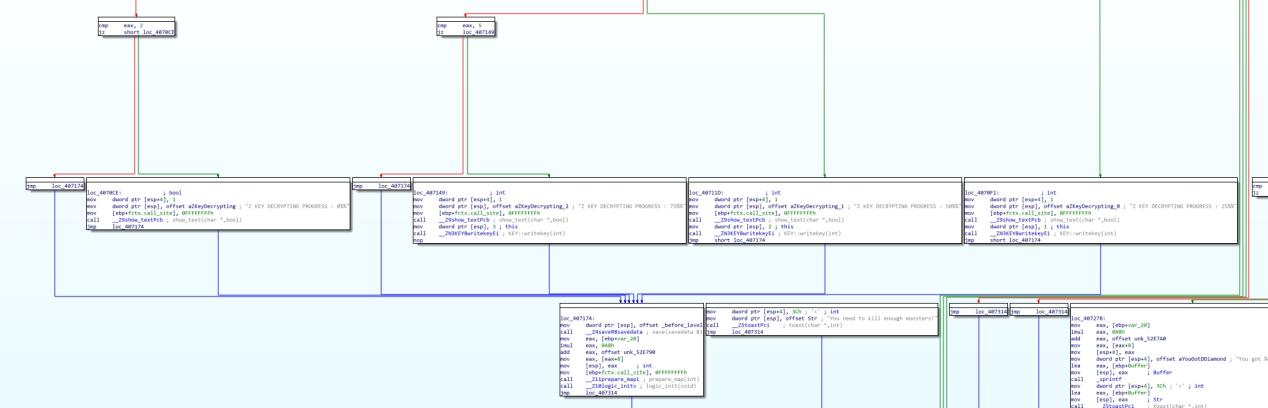
人物移动



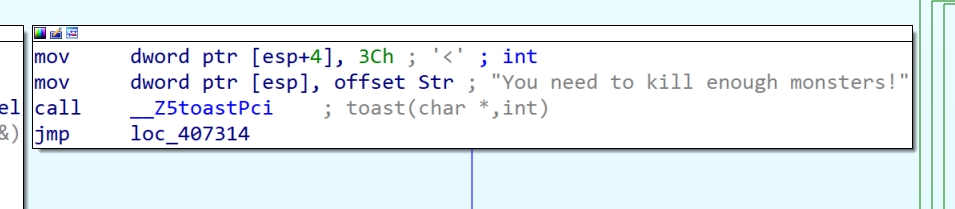
移动鼠标



来判断目前游戏的进度,比较eax的值



将野怪击杀才能推进进度，这是后续修改游戏的关键，通过修改可以条件可以大大加快通过速度，无需和怪兽缠斗。



最终全部关卡完成，成功通关



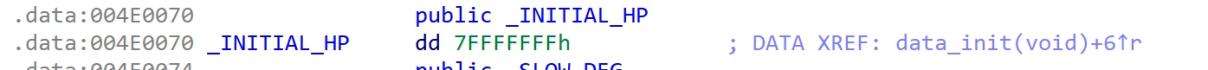
（2）重要数据

移动速度



最大血量和初始血量





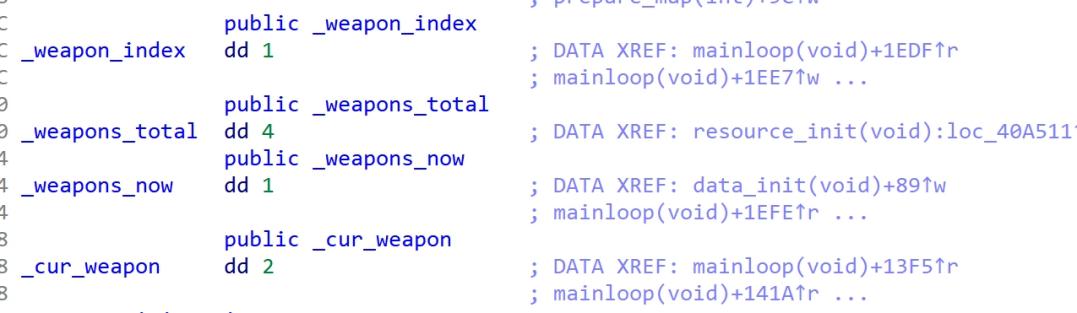
护甲



出生位置



武器



（二）修改game.exe二进制代码， 在实验报告中说明代码修改的具体过程

1.修改人物血量和运动速度

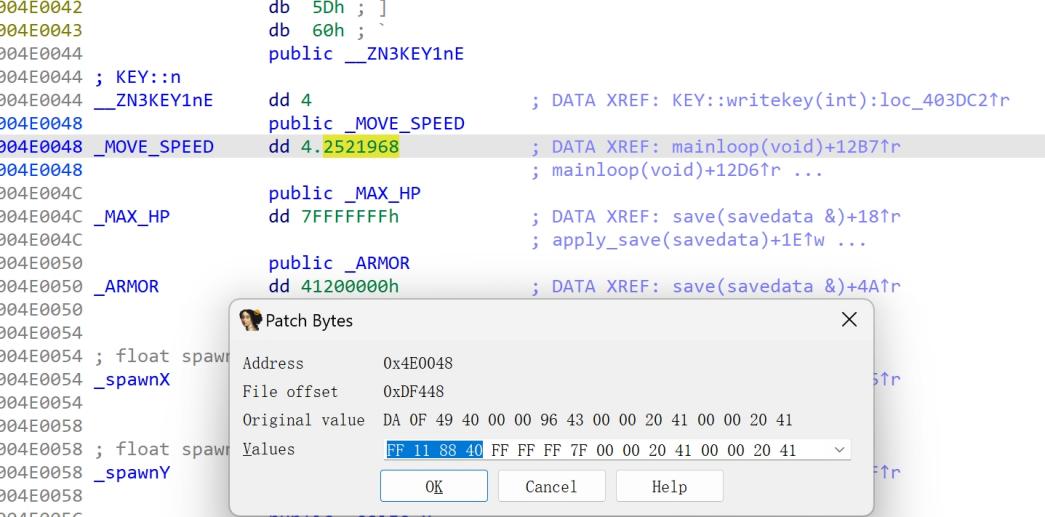
（1）运行game.exe，发现人物血量过少，很快就会死亡，我们通过修改人物的血量为无限大，即可解决这个问题。

把Initial HP和MAX HP通过edit中patch program的change BYTE将其十六进制数地址存储改为FFFFFF7F，即可将生命值修改至无穷。



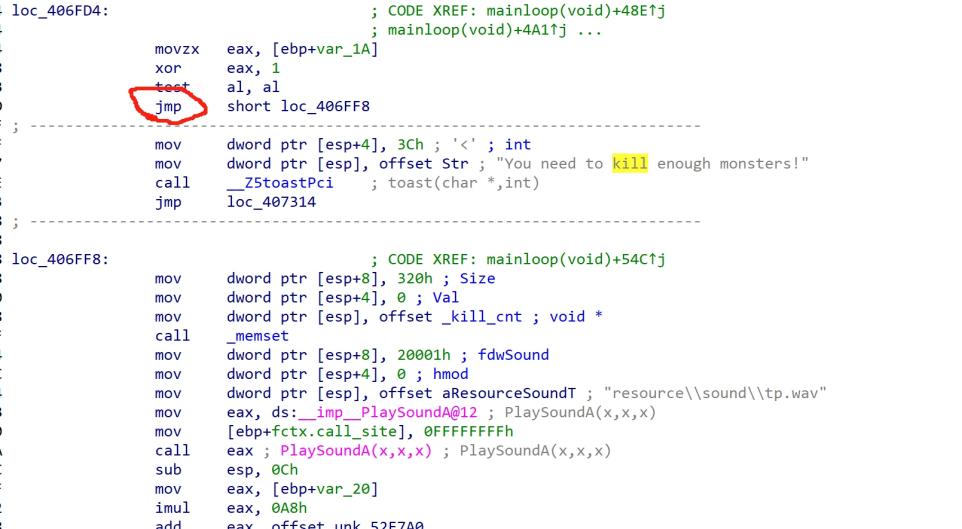
（2）游戏过程中，角色移动速度过慢，影响通关速度，但是速度不可提升太快，因为有些道路速度过快难以找到位置通过，所以要将速度适当提高

找到MOVE\_SPEED通过edit中patch program的change BYTE将其十六进制数地址修改为FF118840，即可提高速度

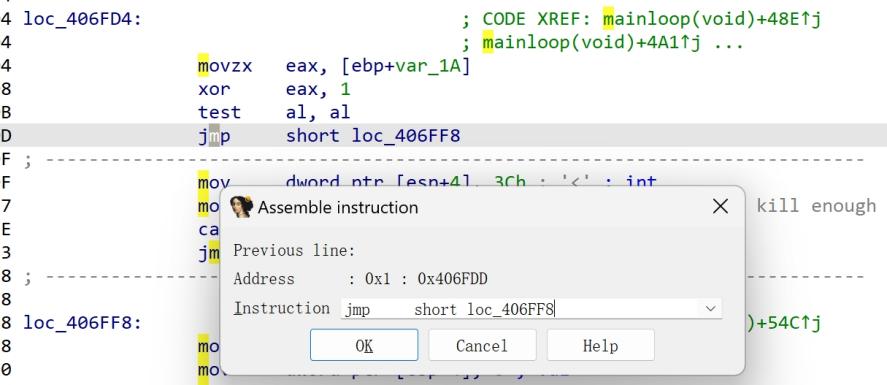


2.修改通关条件

在游戏进行的过程中，我们发现只有当击杀完所有的怪兽游戏才能够进入下一关，我们只要修改这个条件语句的跳转，即可快速通关。

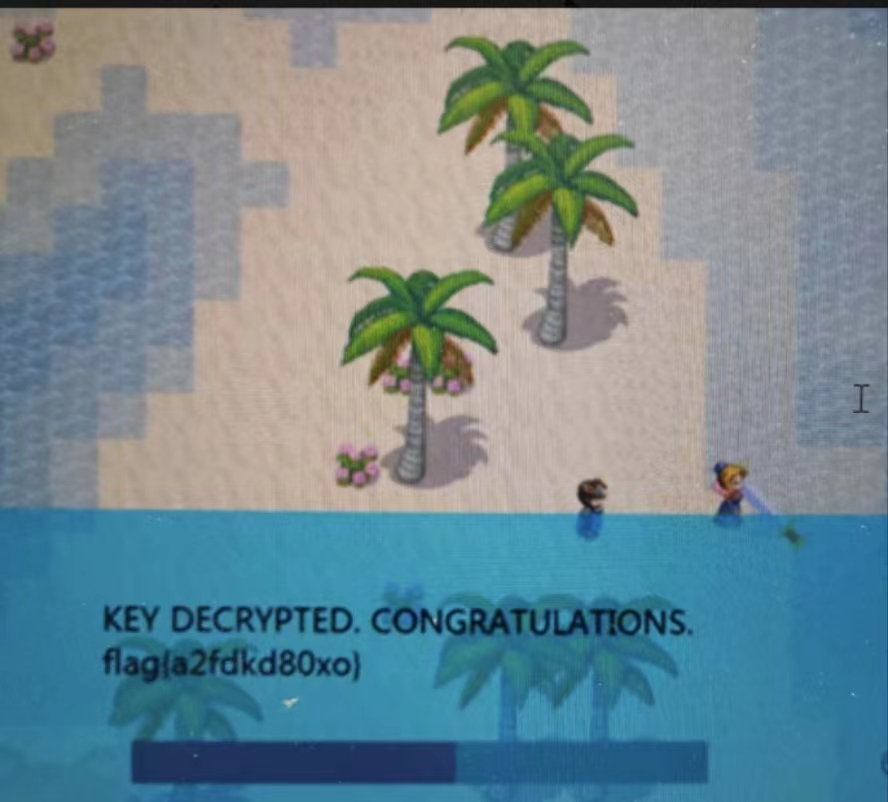


通过IDA的search找到提示语“You need to kill enough monsters!”所在位置，发现原先为jz short loc\_406FF8，说明若满足一定条件才会跳转到loc\_406FF8。为了将“You need to kill enough monsters!”跳过，利用edit中patch program的assemble将jz修改为jmp，即可无条件跳转到loc\_406FF8，大大提高了通关速度。



最终即可找到公主顺利通关

（三）实验成功flag截图



1. **实验结论及心得体会**

**本次实验是一次非常有趣且实用的实验，让我体会到了逆向技术的用处，第一次有了“开挂”的感觉。这也是本学期最后一次汇编实验，收获很大，学习到了很多知识，受益匪浅。**