**·实验6 CTF（Capture The Flag）夺旗赛**

学号：2113662 姓名：张丛

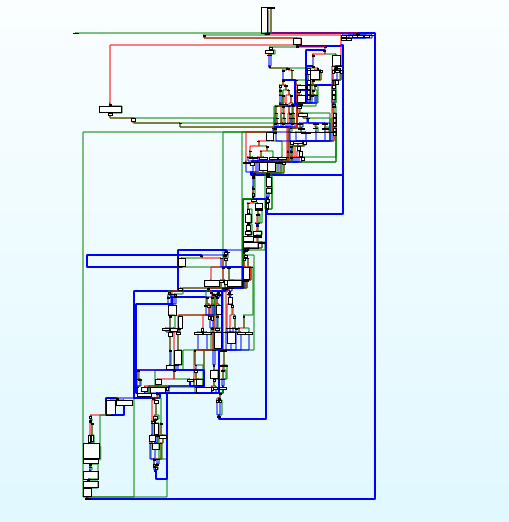
1. **实验目的**
   1. 熟悉静态反汇编工具IDA Freeware；
   2. 掌握对二进制代码内部逻辑关系的分析；
   3. 掌握对二进制代码的修改和保存。
2. **实验原理**
3. 解题

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 修改静态资源
2. 技巧B：利用IDA修改汇编指令
3. **逆向分析与具体修改**

**（1）**



可见整体代码的结构什么的复杂，实验的重点应该是逆向关键的代码、数据，从而通关，拿到flag

**（2）**



尝试进入游戏发现，主角血量非常脆弱，走位稍有不慎就died。

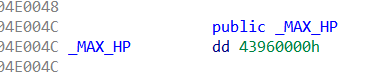
故修改血量。

修改方法：

1.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。

2.点击Edit->Patch program->Apply patches to input file，完成修改。

修改前：



修改后：





进入游戏：



此时可无视怪物的攻击前进。

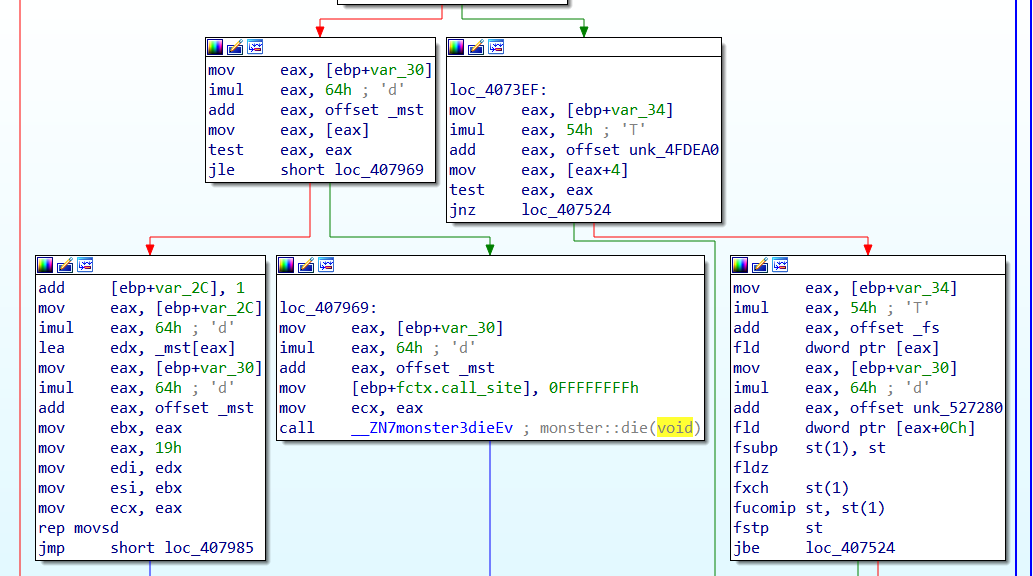
**（3）**

虽然不会died，但游戏无法推进



提示需要击杀足够的怪物

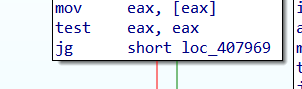
找到monster.die的函数



将jle修改为jg

修改方法为：

1. 点击Edit->Patch program->Assemble，输入新的汇编指令。
2. 点击Edit->Patch program->Apply patches to input file，完成修改。



再次进入，发现怪物全部死亡，剩下掉落物在原地：

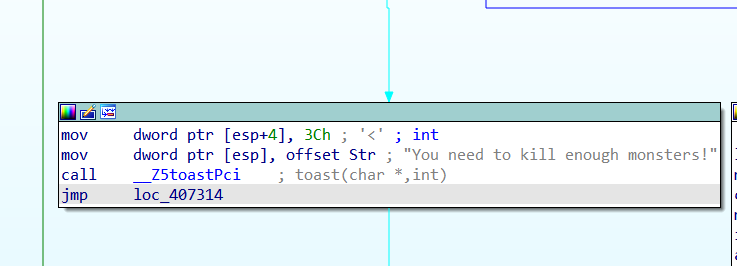


一路畅通无阻，直到来到地图最北方：

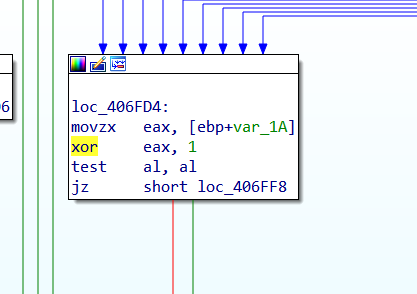


**（4）**

搜索“You need to kill enough monsters!”这句话：

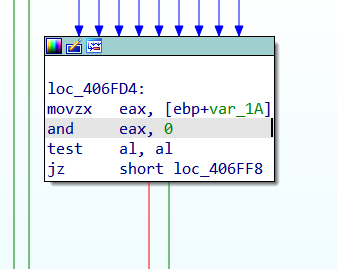


沿着红线往上找：



将 xor eax,1

修改为 and eax,0



再进入游戏，推进剧情，进入地图左下角的爱琴海：





完成结局，找到flag为：a2fdkd80xo.

**四、实验心得**

这次实验与之前几次不同，给我们一个小游戏，要求运用汇编与逆向知识通关并得到Flag。

这种形式我认为更贴近生活，更具体化地知道汇编与逆向的实现以及运用。