**汇编语言与逆向技术实验报告**

**Lab7 CTF（Capture The Flag）夺旗赛**

**学号：2112060 姓名：孙蕗 专业：信息安全**

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。

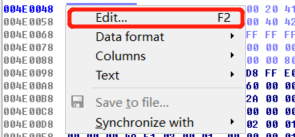


1. 技巧A：利用IDA 修改静态资源

* 第一步，在反汇编代码中（IDA View）找到静态资源。

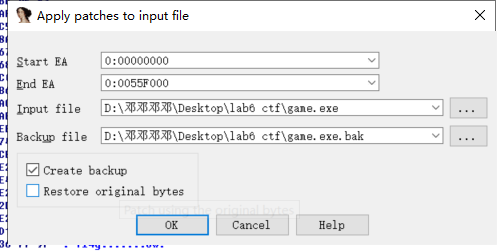


* 第二步，在十六进制视图中（Hex View）找到指定区域，右键选择Edit对资源进行修改。修改完毕后，右键选择Apply changes应用修改。





* 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。

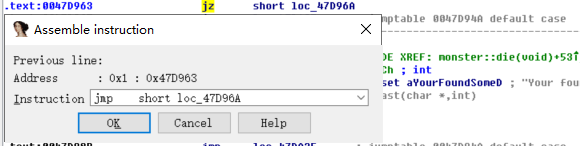


1. 技巧B：利用IDA修改汇编指令

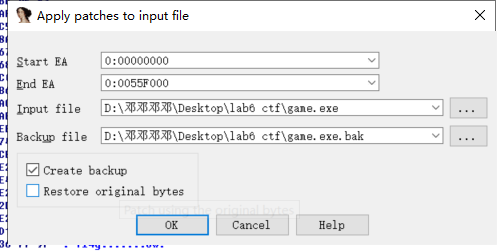
* 第一步，在反汇编代码中（IDA View）找到需要修改的汇编指令。



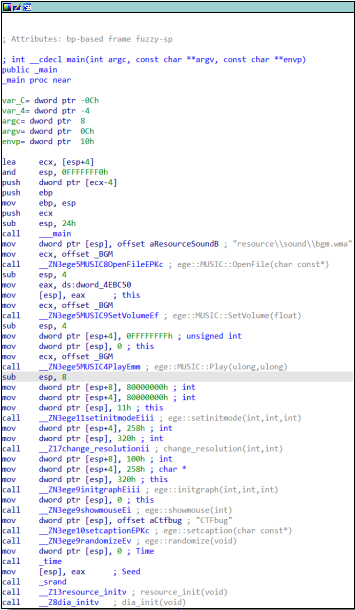
* 第二步，点击Edit->Patch program->Assemble，输入新的汇编指令。



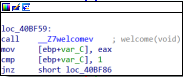
* 第三步，点击Edit->Patch program->Apply patches to input file，建议选中创建备份的选项，完成修改。



1. **实验报告**
2. 逆向分析game.exe二进制代码的主要逻辑结构和重要数据。
3. 修改game.exe二进制代码，获得最后的Flag。实验报告要说明逆向分析、代码修改的具体过程，以及最后获得的Flag。
4. 实验报告的提交时间：12月21日之前提交。
5. 逆向分析game.exe二进制代码的主要逻辑结构和重要数据

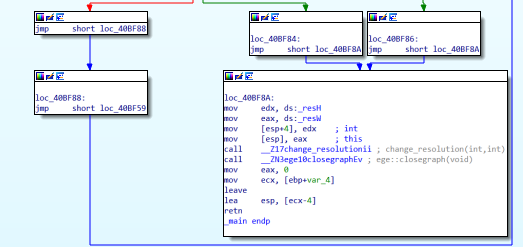


背景音乐，背景图片的播放和展示设置。包括如音量设置，打开文件设置，键盘移动设置等。



进入游戏界面

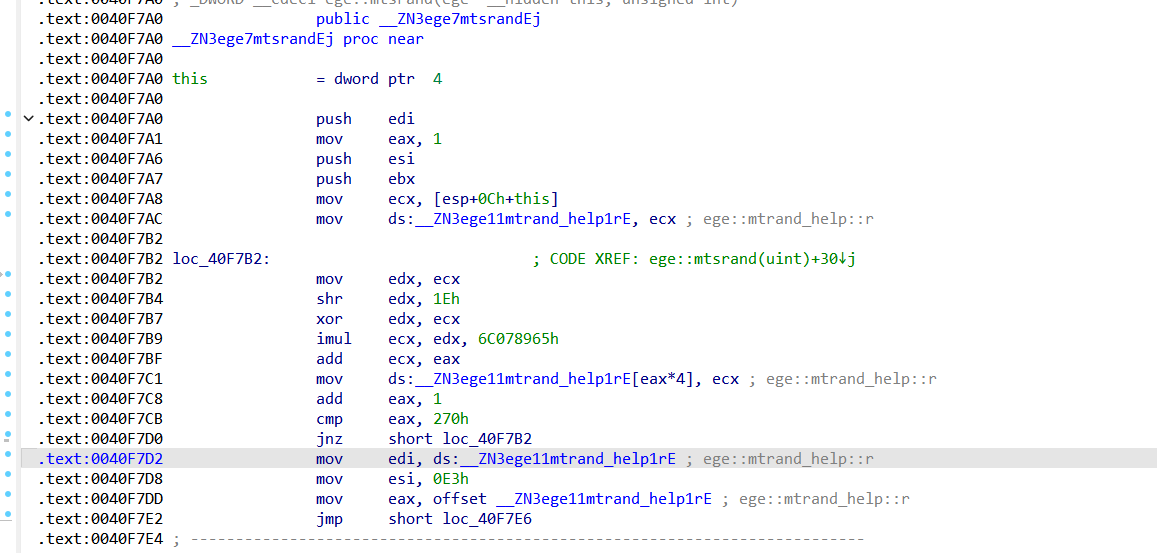




根据不同条件判断跳转到相应函数的位置



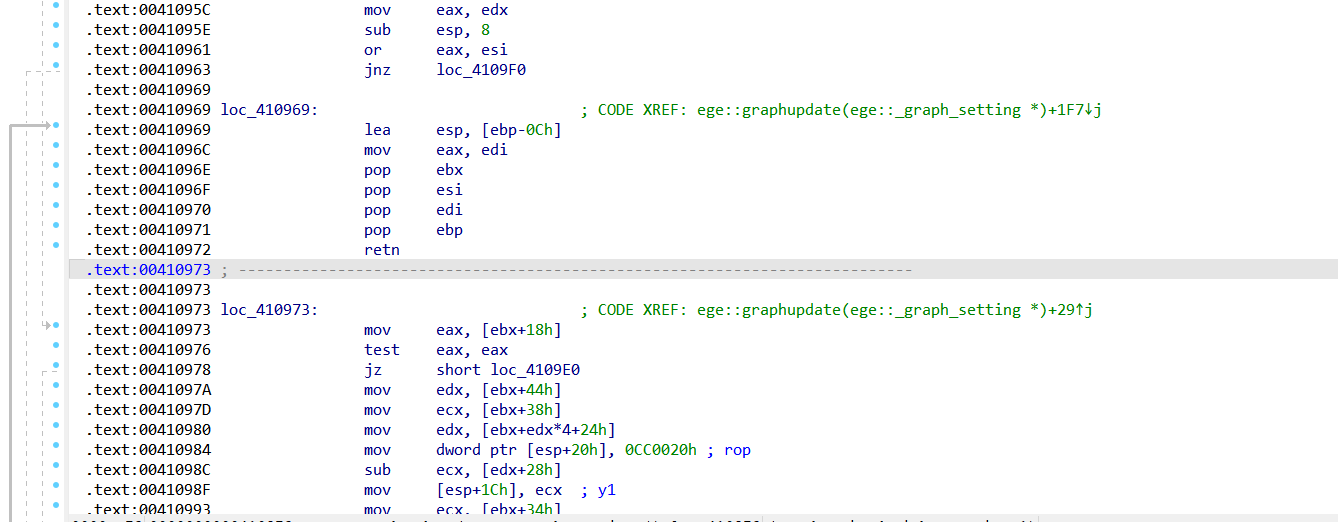
达到一定的条件进行判断，使用特殊技能



游戏帮助提示



背景图片UI界面展示，以及背景切换





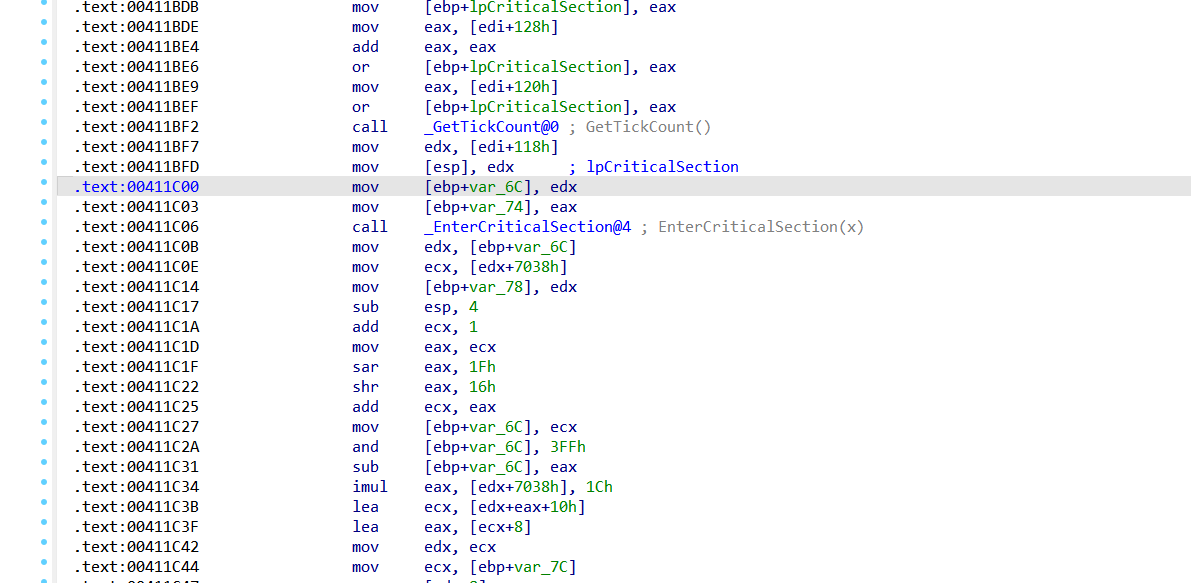




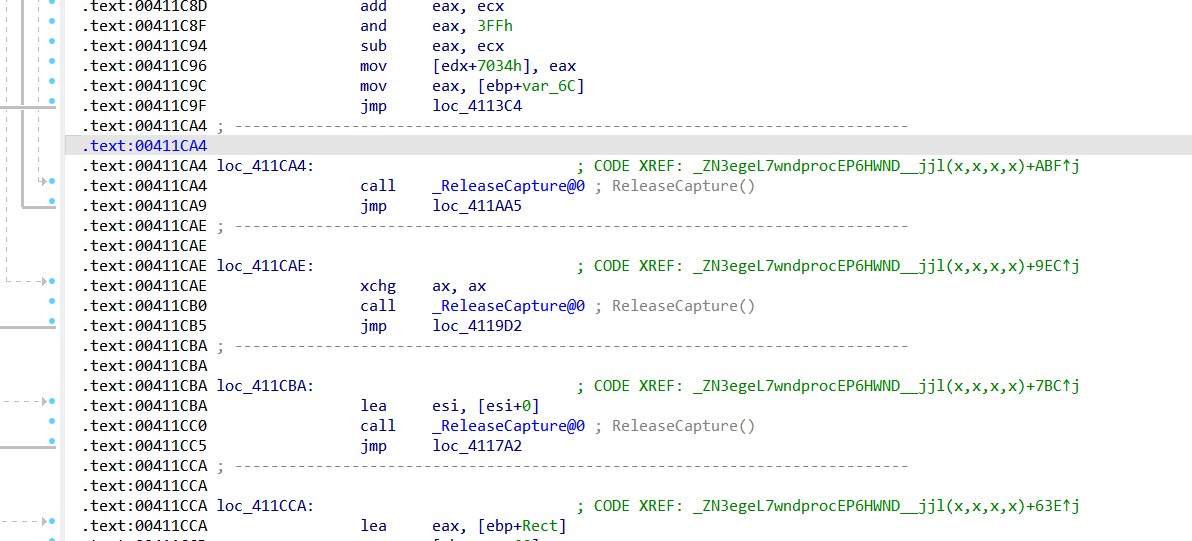
得到key

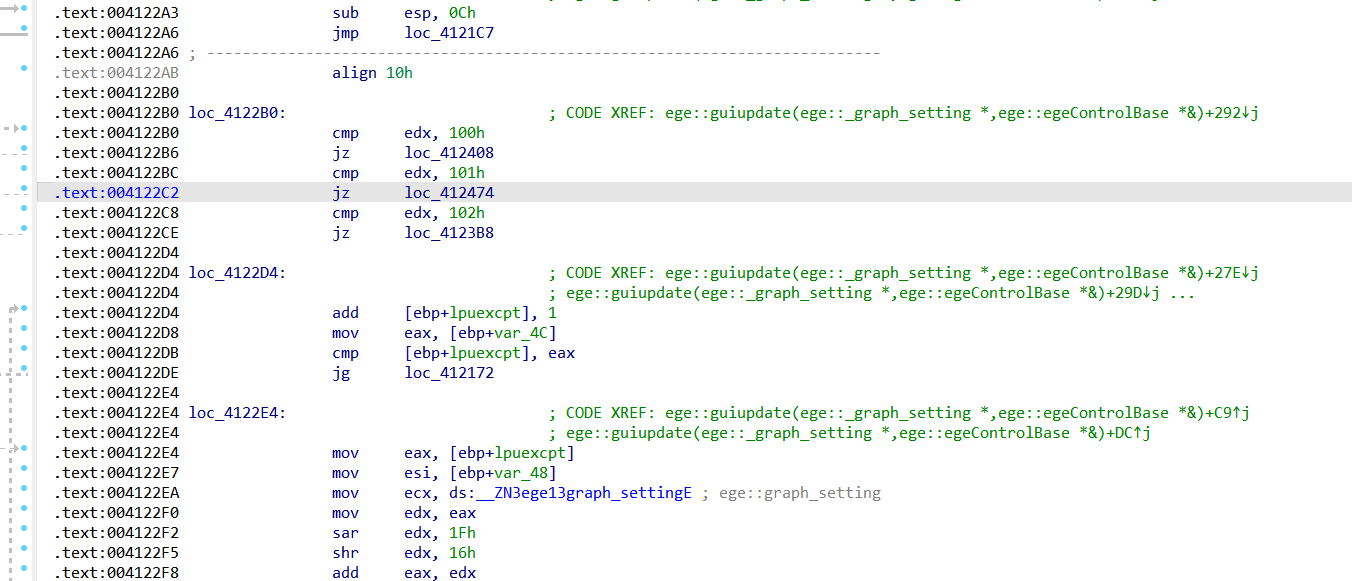


获得坐标和游戏界面大小



进入游戏关键区域

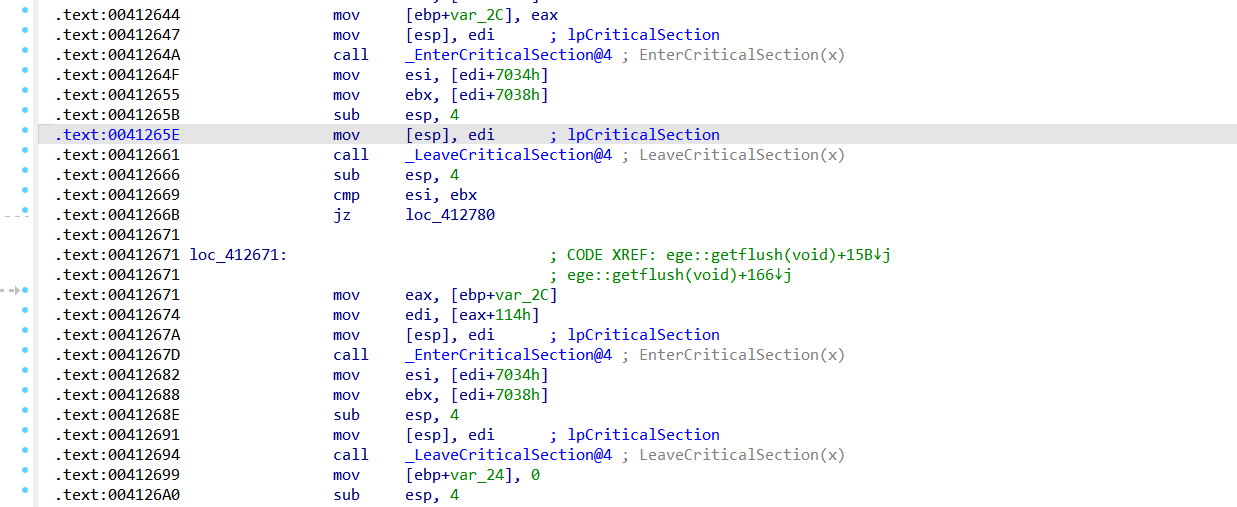




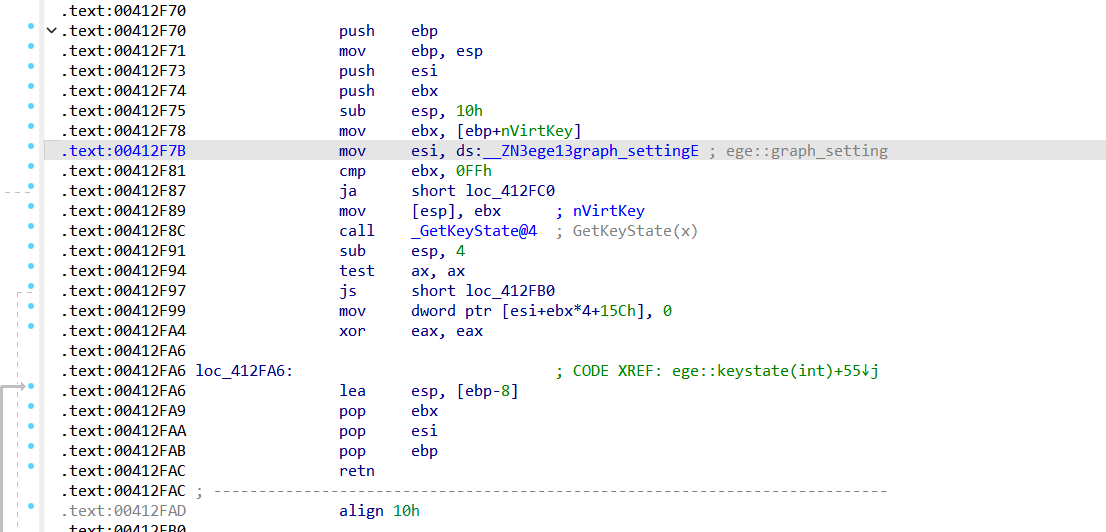
鼠标滚动特效切换



UI更新

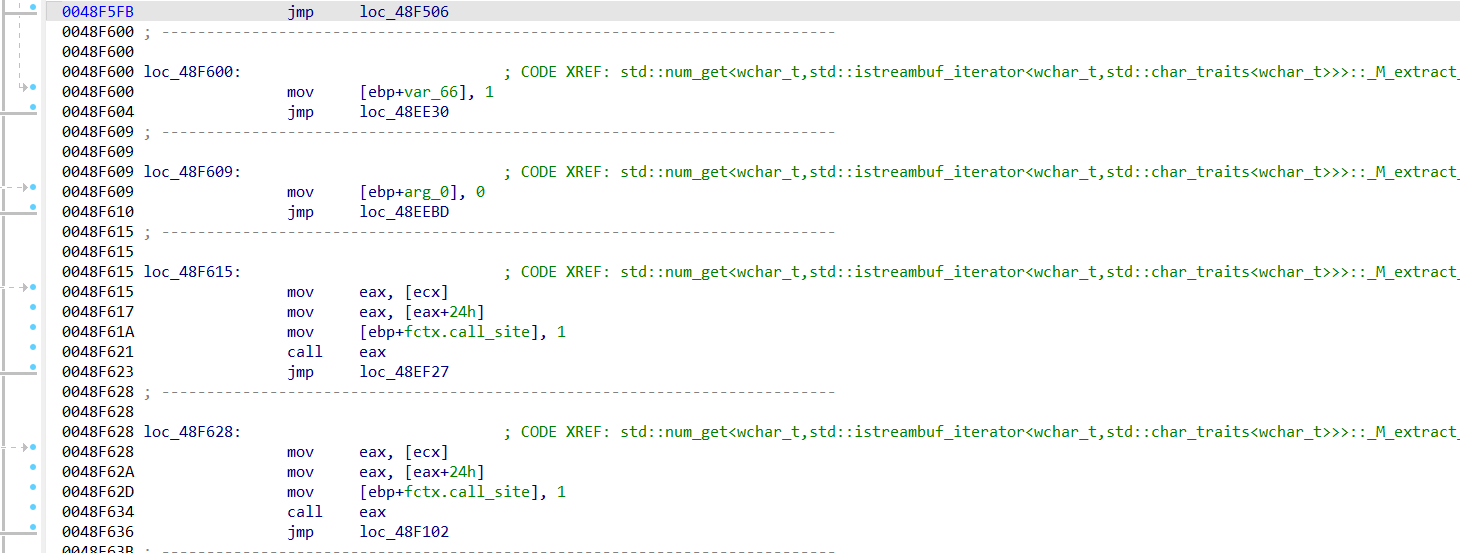


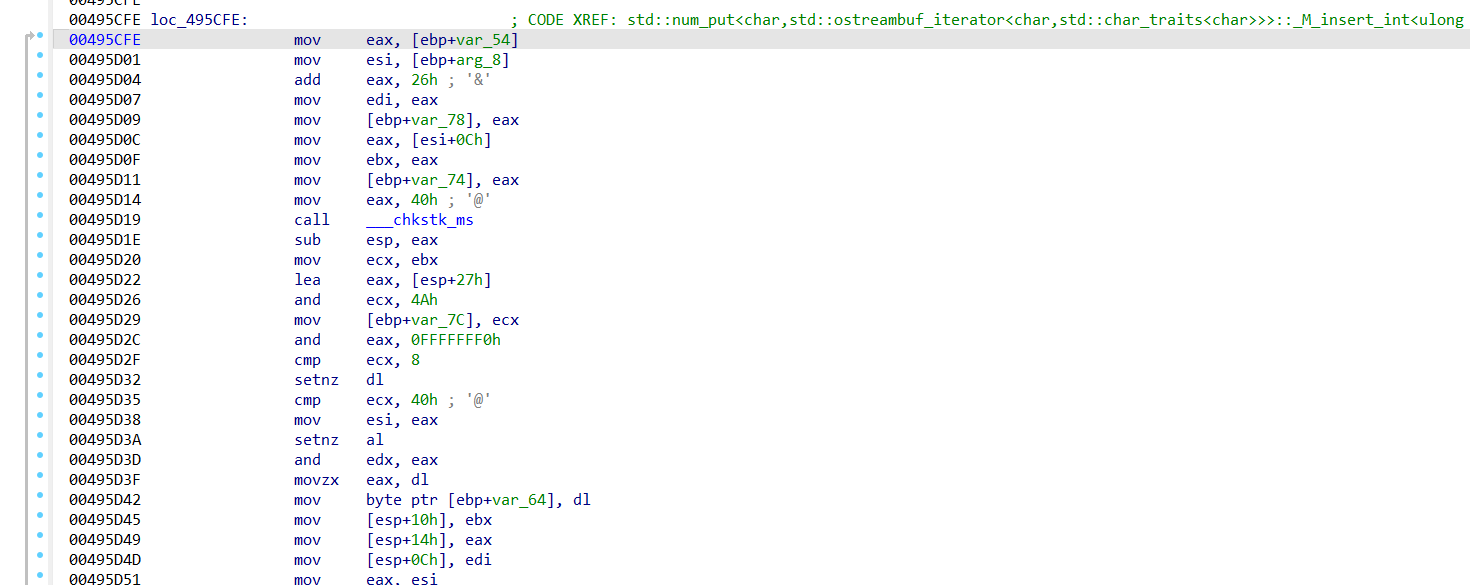
进入关键区域离开关键区域



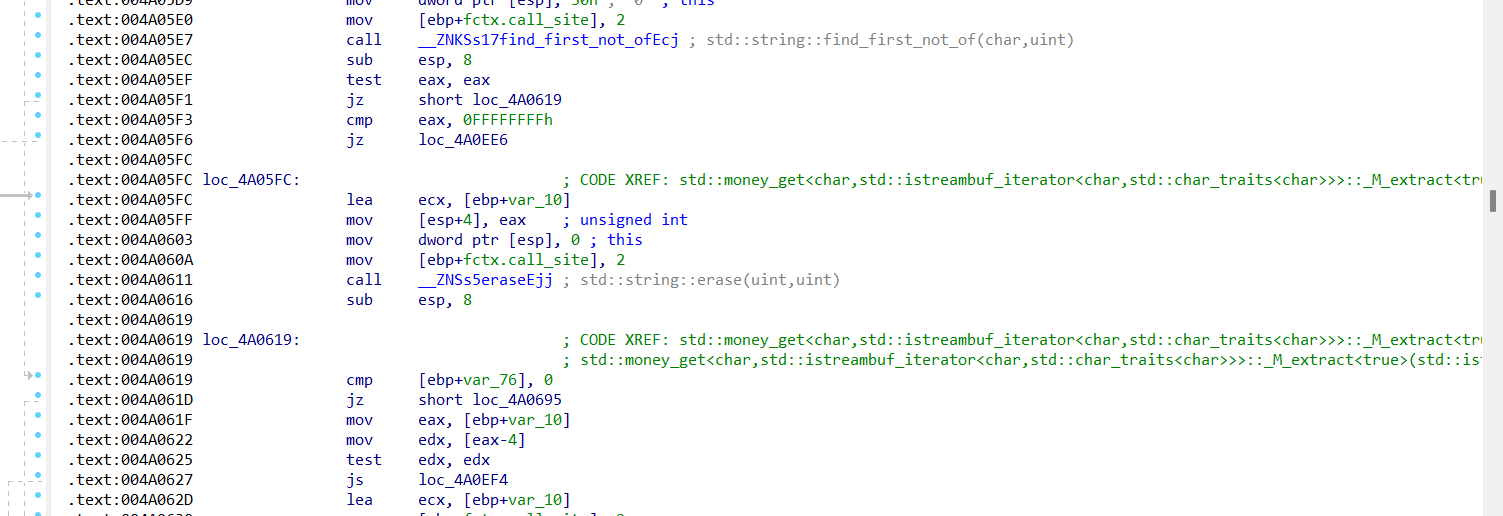
获取键盘状态

（15）





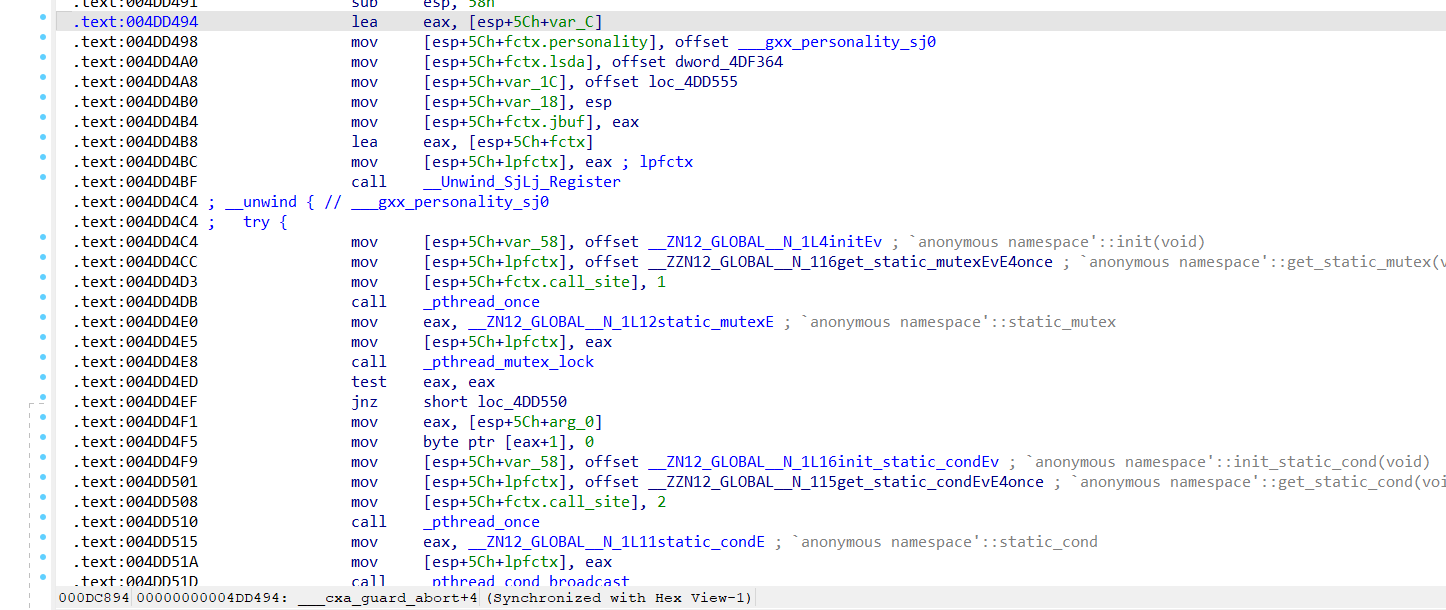
（16）



吃diamond得的血量

1. 



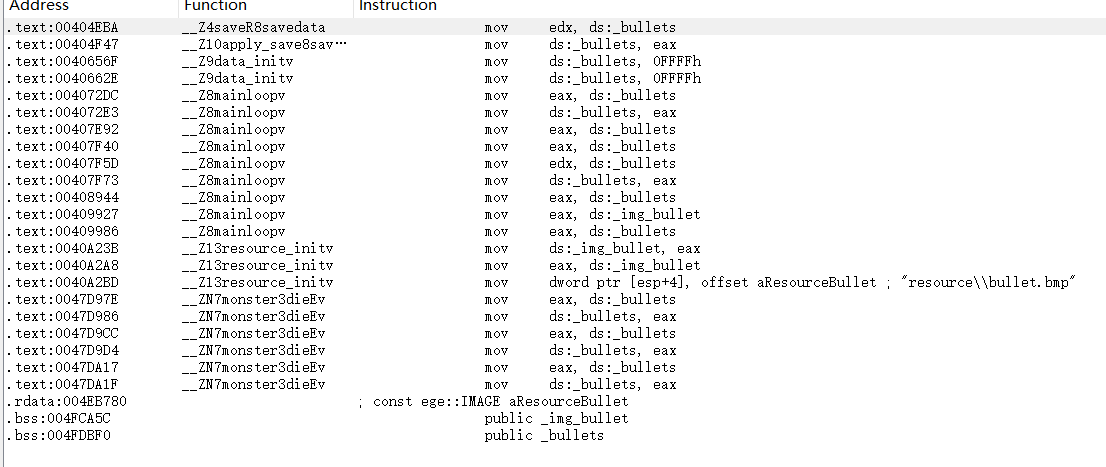


1. 修改game.exe二进制代码，获得最后的Flag。

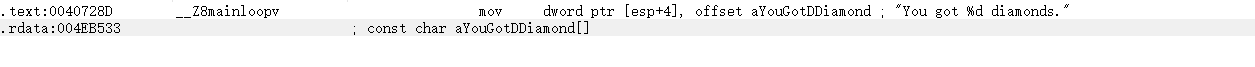


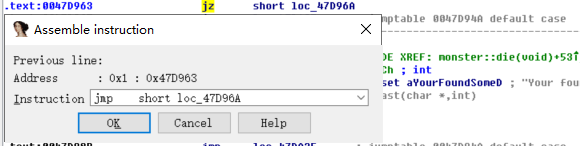


更改血量，移动速度，最大血量,双方掉血量等



到第二关发现有钻石，应该吃掉会有相应加血量

****



到第四关发现血量点满也无法通过，需要分析代码结构。根据游戏第四关代码的分析和实际操作，应将jz换成jnp

Flag：

