汇编语言与逆向技术实验报告

Lab7 - Game/CTF（Capture The Flag）夺旗赛

学号：2110957　　姓名：蒋薇　　专业： 计算机科学与技术

一、 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；

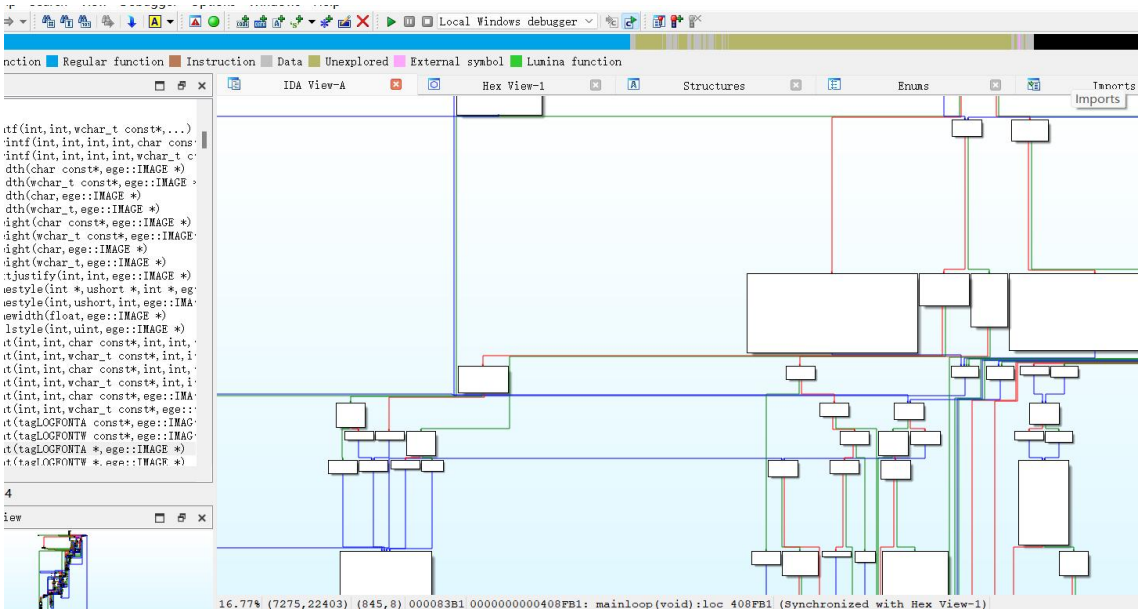
3、掌握对二进制代码的修改和保存。

二、 实验原理

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。

三、 三：实验内容

1. 逆向分析 game.exe 二进制代码的主要逻辑结构和重要数据。



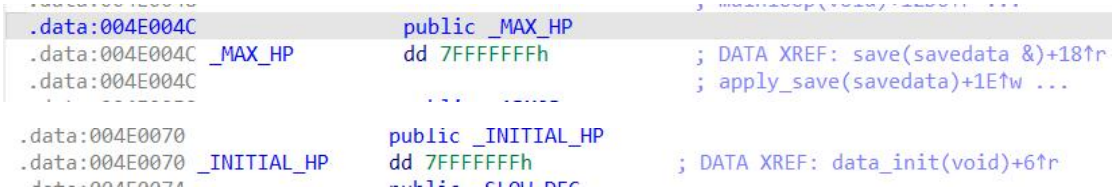
```
.data:004E0042                db  5Dh ; ]
.data:004E0043                db  60h ; `
.data:004E0044                public __ZN3KEY1nE
.data:004E0044 ; KEY::n
.data:004E0044 __ZN3KEY1nE    dd 4                    ; DATA XREF: KEY::writekey(int):loc_403DC2↑r
.data:004E0048                public _MOVE_SPEED
.data:004E0048 _MOVE_SPEED    dd 3.1415925            ; DATA XREF: mainloop(void)+12B7↑r
.data:004E0048                                        ; mainloop(void)+12D6↑r ...
.data:004E0048                                        ; 移动速度
.data:004E004C                public _MAX_HP
.data:004E004C _MAX_HP        dd 43960000h            ; DATA XREF: save(savedata &)+18↑r
.data:004E004C                                        ; apply_save(savedata)+1E↑w ...
.data:004E004C                                        ; 血量
.data:004E0050                public _ARMOR
.data:004E0050 _ARMOR         dd 41200000h            ; DATA XREF: save(savedata &)+4A↑r
.data:004E0050                                        ; apply_save(savedata)+44↑w ...
.data:004E0054                public _spawnX
.data:004E0054 ; float spawnX
.data:004E0054 _spawnX        dd 41200000h            ; DATA XREF: logic_init(void)+A5↑r
.data:004E0054                                        ; mainloop(void)+5DC↑w
.data:004E0058                public _spawnY
.data:004E0058 ; float spawnY
.data:004E0058 _spawnY        dd 43960000h            ; DATA XREF: logic_init(void)+9F↑r
.data:004E0058                                        ; mainloop(void)+5FF↑w
000DF448 00000000004E0048: .data:_MOVE_SPEED (Synchronized with Hex View-1)
```

2. 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。

1. 进入游戏，人物生命值极有限，_MAX_HP,_INITIAL_HP 改为无限，如下：

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

点击 Edit->Patch program->Apply patches to input file

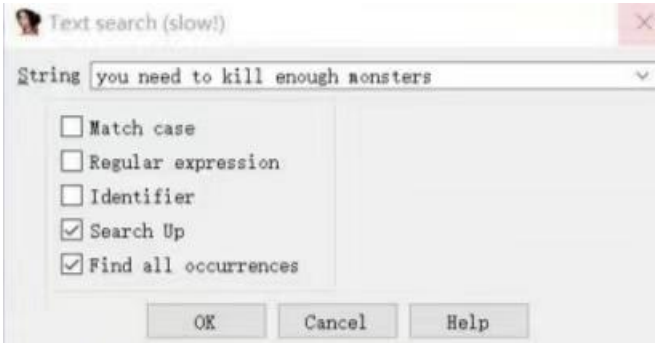


2. 要想从第二个界面进入第三个界面，发现“You need to kill enough monsters”,修改

在反汇编代码中（IDA View）找到需要修改的汇编指令

点击 Edit->Patch program->Assemble，输入新的汇编指令

点击 Edit->Patch program->Apply patches to input file



3. 按照地图指示和人物对话信息可通关，得 Flag


83%
0K/s
0.1K/s
KEY DECRYPTED. CONGRATULATIONS.
flag{a2fdkd80xo}
1.$/1.$