

汇编语言与逆向技术实验报告

Lab7 Capture The Flag

姓名：丁彦添 学号：1911406

首先不做任何修改，游玩一遍游戏，但是会发现很快就游戏结束了。游戏下方弹出死亡的提示窗口。



所以如果可以修改与死亡相关的代码就可以“永生”。


打开 IDA PRO，再打开 string 窗口。

Line 1 of 4179

000115F9 00000000004125F9: sub_4125DC+1D

Address	Length	Type	String
.data:004E1494	00000005	C	QEOj5
.data:004E14B0	00000005	C	\r<Uwh
.data:004E156C	00000005	C	-e[h
.data:004E158F	00000007	C	fY^*5#Q
.data:004E16F3	00000005	C	\\"Gbk\"
.data:004E1A25	00000005	C	^2c%
.data:004E1A85	00000007	C	m2;\vDEP
.data:004E1B26	00000005	C)Elk
.data:004E1B49	00000005	C	?/=Ox
.data:004E1CC8	00000005	C	z=rKs
.data:004E1DAD	00000005	C	N+vTi
.data:004E1E9C	00000005	C	xo\v_r
.data:004E1F3B	00000005	C	S;mBk
.data:004E1F9E	00000005	C	x*uqr
.data:004E2010	00000007	C	Gum*Mos
.data:004E20C0	00000005	C	GKEq)
.data:004E20DA	00000006	C	wr3_#/
.data:004E2124	00000005	C	*r~P~
.data:004E2215	00000006	C	N<%p=P
.data:004E22A1	00000006	C	s_nY\n
.data:004E23F1	00000006	C	J\c v5
.data:004E258A	00000005	C	6nH7x
.data:004E25D3	00000006	C	!+Z:'<
.data:004E269D	00000006	C	Z5OPj
.data:004E26BD	00000007	C	\v(1\ \a
.data:004E2700	00000005	C	7<)=Y
.data:004E286E	00000005	C	F~UbF
.data:004E292C	00000006	C	(!Mp>1
.data:004E29A6	00000005	C	v9j(
.data:004E2A9D	00000005	C	x\amVX
.data:004E2D49	00000006	C	IN_~G
.data:004E2D64	00000005	C	\x1B=\"\lb
.data:004E2DE2	00000005	C	vy?TW

按住Alt+T打开搜索框，搜索字符串died



String

找到表示游戏结束的位置

[S]	.rdata:004EB478	00000020	C	Z KEY DECRYPTING PROGRESS : 0%%
[S]	.rdata:004EB498	00000021	C	Z KEY DECRYPTING PROGRESS : 25%%
[S]	.rdata:004EB4BC	00000021	C	Z KEY DECRYPTING PROGRESS : 50%%
[S]	.rdata:004EB4E0	00000021	C	Z KEY DECRYPTING PROGRESS : 75%%
[S]	.rdata:004EB501	0000001A	C	Your health recovered %d.
[S]	.rdata:004EB51B	00000018	C	resource\\sound\\heal.wav
[S]	.rdata:004EB533	00000015	C	You got %d diamonds.
[S]	.rdata:004EB548	00000008	C	U died!
[S]	.rdata:004EB550	00000018	C	This skill needs %d MP!
[S]	.rdata:004EB568	00000019	C	resource\\sound\\wrong.wav
[S]	.rdata:004EB581	00000018	C	resource\\sound\\shot.wav
[S]	.rdata:004EB599	0000001D	C	resource\\sound\\sword_hit.wav
[S]	.rdata:004EB5B6	00000019	C	resource\\sound\\sword.wav
[S]	.rdata:004EB5CF	00000017	C	resource\\sound\\ice.wav
[S]	.rdata:004EB5E6	0000001C	C	resource\\sound\\firefall.wav
[S]	.rdata:004EB602	0000000A	C	%.1f/%.1f
[S]	.rdata:004EB60C	0000001D	C	HP: %.1f Score: %d fps: %.1f
[S]	.rdata:004EB738	00000012	C	resource\\fire.bmp
[S]	.rdata:004EB74A	00000014	C	resource\\fire_m.bmp
[S]	.rdata:004EB75E	00000010	C	resource\\bg.png
[S]	.rdata:004EB76E	00000012	C	resource\\head.bmp

往上找到具体代码

```

.rdata:004EB533 , char aYouGotDDiamond[]
.rdata:004EB533 aYouGotDDiamond db 'You got %d diamonds.',
.rdata:004EB548 ; char aDied[]
.rdata:004EB548 aDied db 'U died!',0
.rdata:004EB550 ; char aThisSkillNeeds[]
.rdata:004EB550 aThisSkillNeeds db 'This skill needs %d MP
.rdata:004EB550

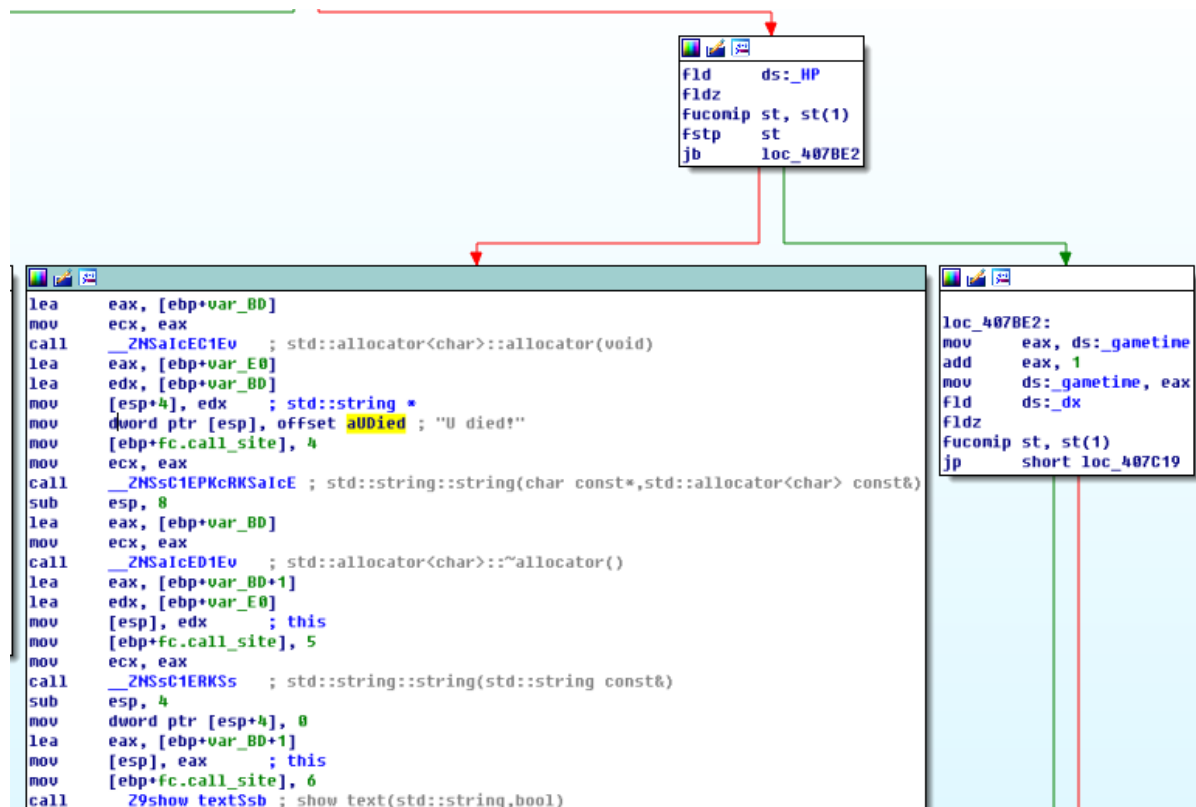
```

```

.text:00407AF7 loc_407AF7:                                ; CODE XREF: mainloop(void)+F2A7j
.text:00407AF7                                         ; mainloop(void)+F647j ...
.text:00407AF7      add      [ebp+var_38], 1
.text:00407AFB loc_407AFB:                                ; CODE XREF: mainloop(void)+F157j
.text:00407AFB      mov      eax, ds:_fstop
.text:00407B00      cmp      [ebp+var_38], eax
.text:00407B03      jle      loc_4079AB
.text:00407B09      fld      ds:_HP
.text:00407B0F      fldz
.text:00407B11      fucomip st, st(1)
.text:00407B13      fstp     st
.text:00407B15      jb       loc_407BE2
.text:00407B18      lea      eax, [ebp+var_BD]
.text:00407B21      mov      ecx, eax
.text:00407B23      call     __ZN5a1cEC1Ev ; std::allocator<char>::allocator(void)
.text:00407B28      lea      eax, [ebp+var_E0]
.text:00407B2E      lea      edx, [ebp+var_BD]
.text:00407B34      mov      [esp+4], edx ; std::string *
.text:00407B38      mov      dword ptr [esp], offset aUdied ; "U died!"
.text:00407B3F      mov      [ebp+fc.call_site], 4
.text:00407B49      mov      ecx, eax
.text:00407B4B      call     __ZN5sC1EPKcRK5a1cE ; std::string::string(char const*,std::allocator<char> const&)
.text:00407B50      sub      esp, 8
.text:00407B53      lea      eax, [ebp+var_BD]
.text:00407B59      mov      ecx, eax
.text:00407B5B      call     __ZN5a1cED1Ev ; std::allocator<char>::~~allocator()
.text:00407B60      lea      eax, [ebp+var_BD+1]
.text:00407B66      lea      edx, [ebp+var_E0]
.text:00407B6C      mov      [esp], edx ; this
.text:00407B6F      mov      [ebp+fc.call_site], 5
.text:00407B79      mov      ecx, eax
.text:00407B7B      call     __ZN5sC1ERK5s ; std::string::string(std::string const&)
.text:00407B80      sub      esp, 4
.text:00407B83      mov      dword ptr [esp+4], 0

```

再向上溯源，发现一个条件判断语句，为了让它不跳转到死亡代码，所以把 jb 修改为 jmp，把条件跳转改为强制跳转。



再次进入游戏游玩，但是发现要通关必须得消灭足够多的怪物，所以再次在字符串窗口中搜索“You need to kill enough monsters!”

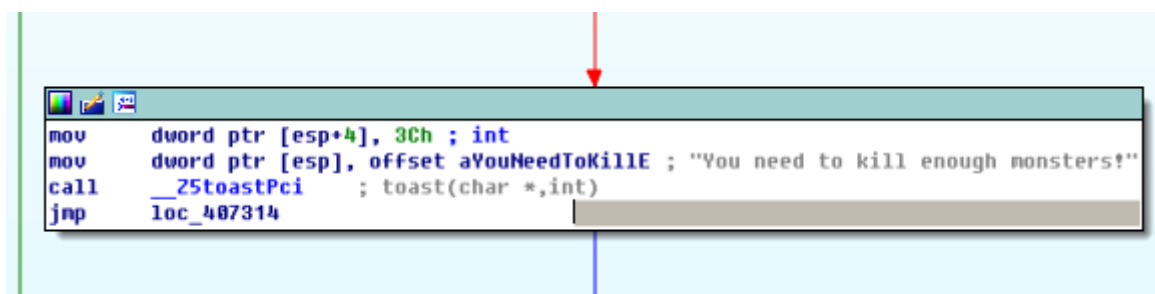
但是由于角色攻击力过低，一个一个把怪打完不现实，考虑直接跳过消灭怪物数量的判定，直接进入下一关。

```

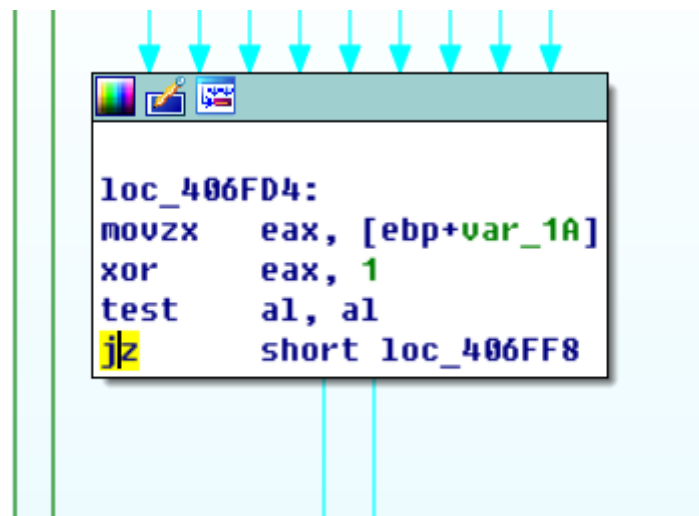
.rdata:004EB3D0          dd offset loc_4060F4
.rdata:004EB41C          ; std::string aZKeyDecrypted_
.rdata:004EB41C          aZKeyDecrypted_ db 'Z KEY DECRYPTED. CONGRATULATIONS.',0Ah,0
.rdata:004EB41C          ; DATA XREF: mainloop(void)+E1f0
.rdata:004EB43F          align 10h
.rdata:004EB440          ; char aYouNeedToKillE[]
.rdata:004EB440          aYouNeedToKillE db 'You need to kill enough monsters!',0
.rdata:004EB440          ; DATA XREF: mainloop(void)+556f0
.rdata:004EB462          ; CHAR aResourceSoundT[]
.rdata:004EB462          aResourceSoundT db 'resource\sound\tp.wav',0
.rdata:004EB462          ; DATA XREF: mainloop(void)+593f0
.rdata:004EB478          ; char aZKeyDecrypting[]
.rdata:004EB478          aZKeyDecrypting db 'Z KEY DECRYPTING PROGRESS : 0%',0
.rdata:004EB478          ; DATA XREF: mainloop(void)+645f0
.rdata:004EB478          ; mainloop(void)+4A1fj ...
.text:00406FD4
.text:00406FD4          movzx  eax, [ebp+var_1A]
.text:00406FD8          xor     eax, 1
.text:00406FDB          test   al, al
.text:00406FDD          jz      short loc_406FF8
.text:00406FDF          mov     dword ptr [esp+4], 3Ch ; int
.text:00406FE7          mov     dword ptr [esp], offset aYouNeedToKillE ; "You need to kill enough monsters!"
.text:00406FEE          call    __25toastPci ; toast(char *,int)
.text:00406FF3          jmp     loc_407314
.text:00406FF8          ; -----
.text:00406FF8

```

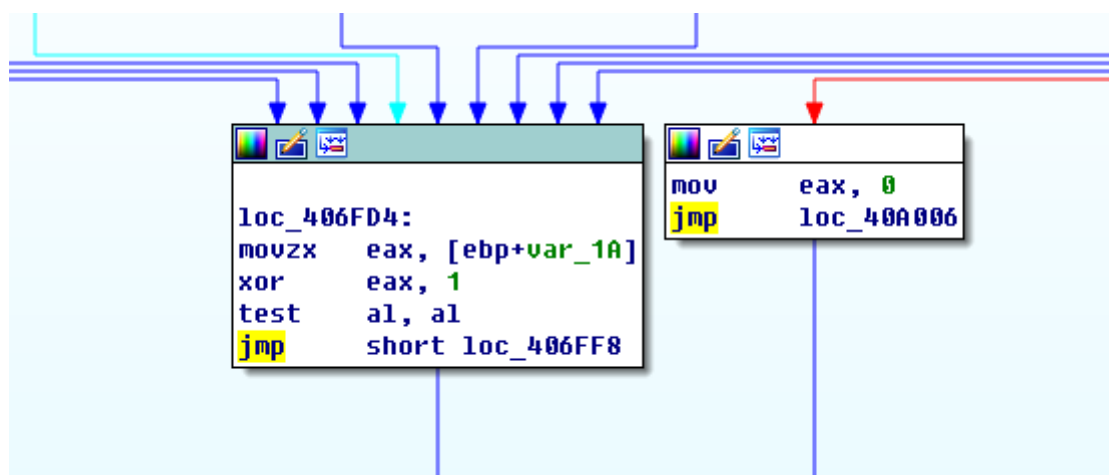
像修改死亡代码一样找到相关的代码



双击箭头向上寻找，并修改代码



将jz指令改成jmp指令



再次进入游戏，成功不死并且进入下一关。

本游戏一共有四五张地图，第一关海岛加大海，一直往上走到第二关沼泽，第二关一直往上走到第三关，往上走再到第四关雪地。雪地过完了之后又回到第一关的场景，进入左下角的爱琴海到最终获得flag的场景，靠近西羽言，获得flag。

最终获得的 flag 截图如下：



Flag 内容

flag{a2fdkd80xo}