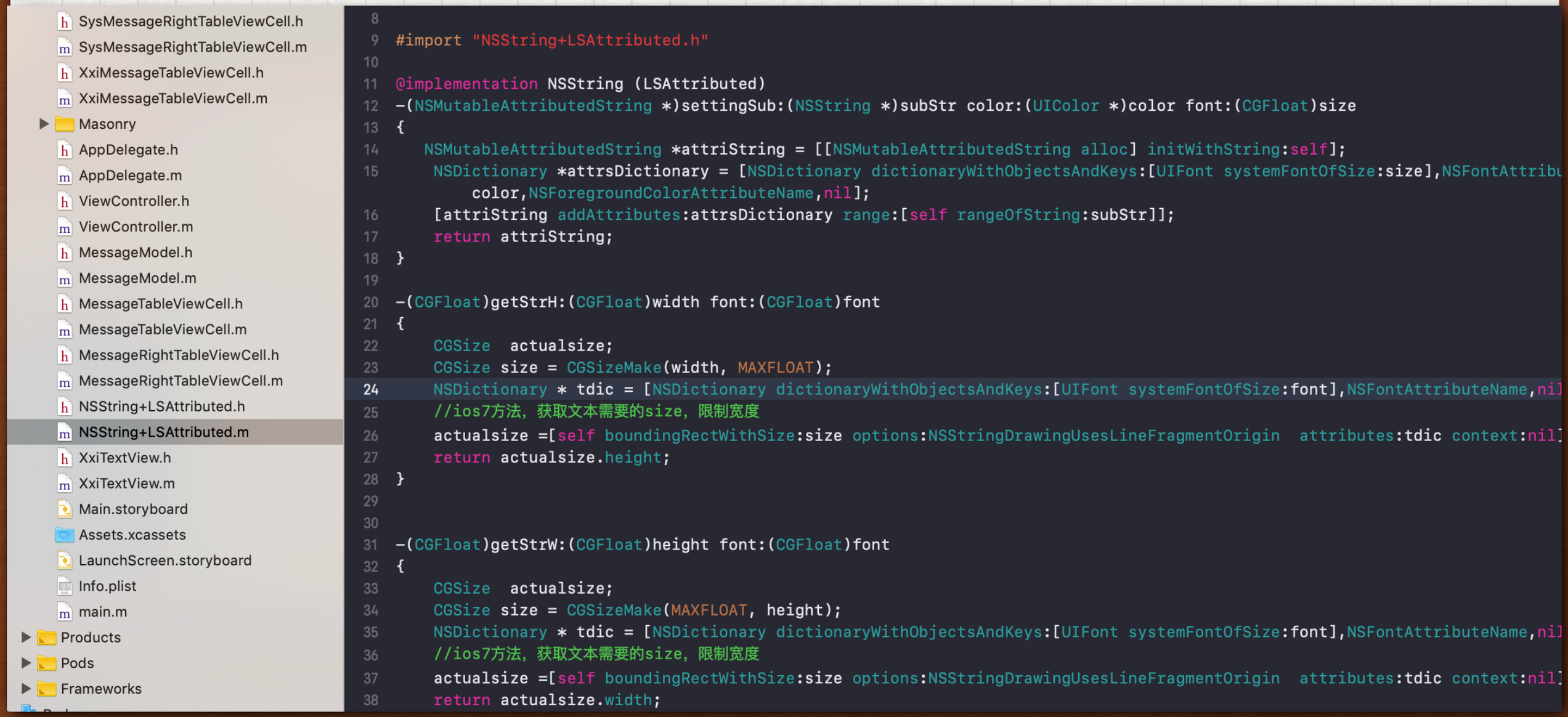
macOS系统中的反向工程

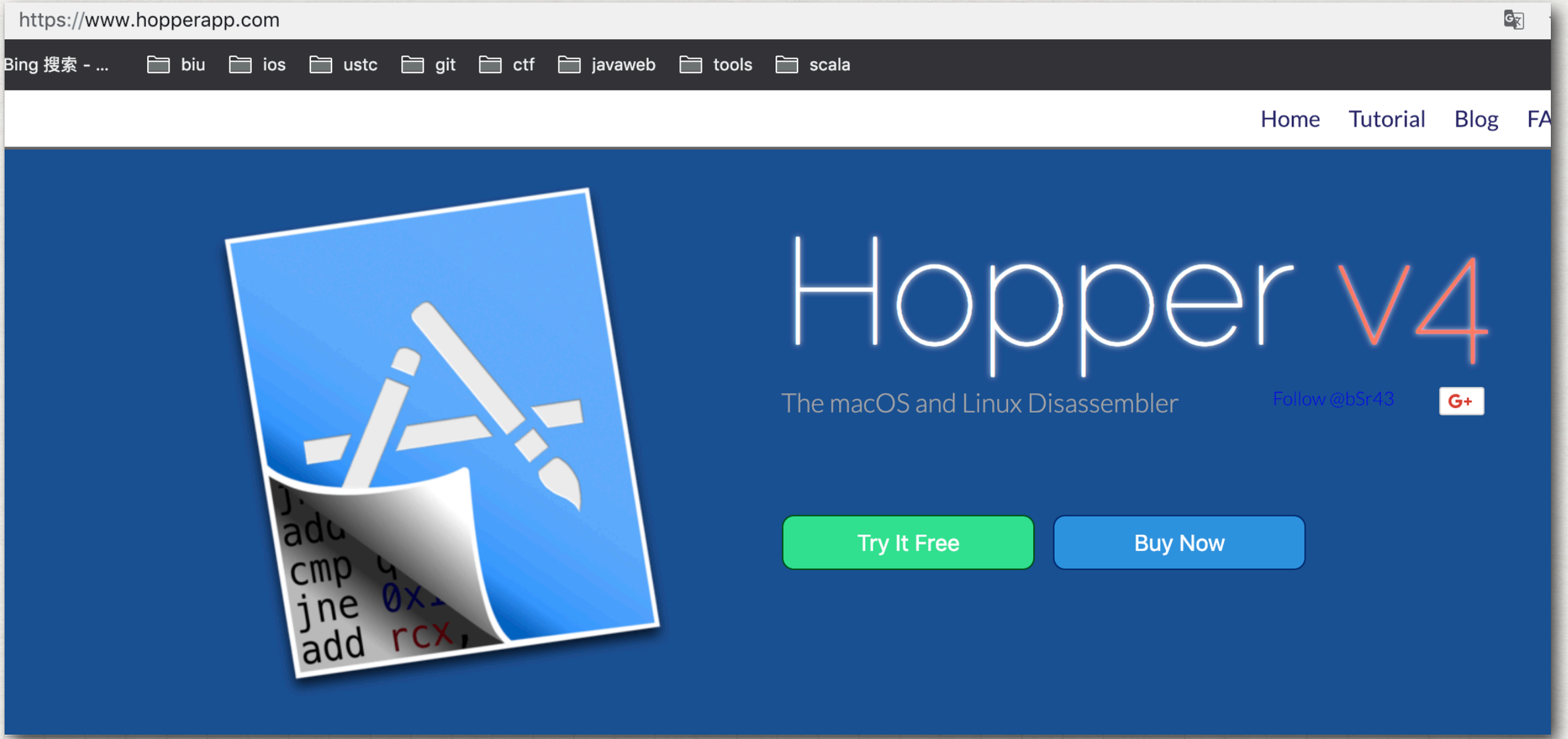
biu
github：biuy

macOS系统中的应用程序大多由Objective-C或者Swift编写

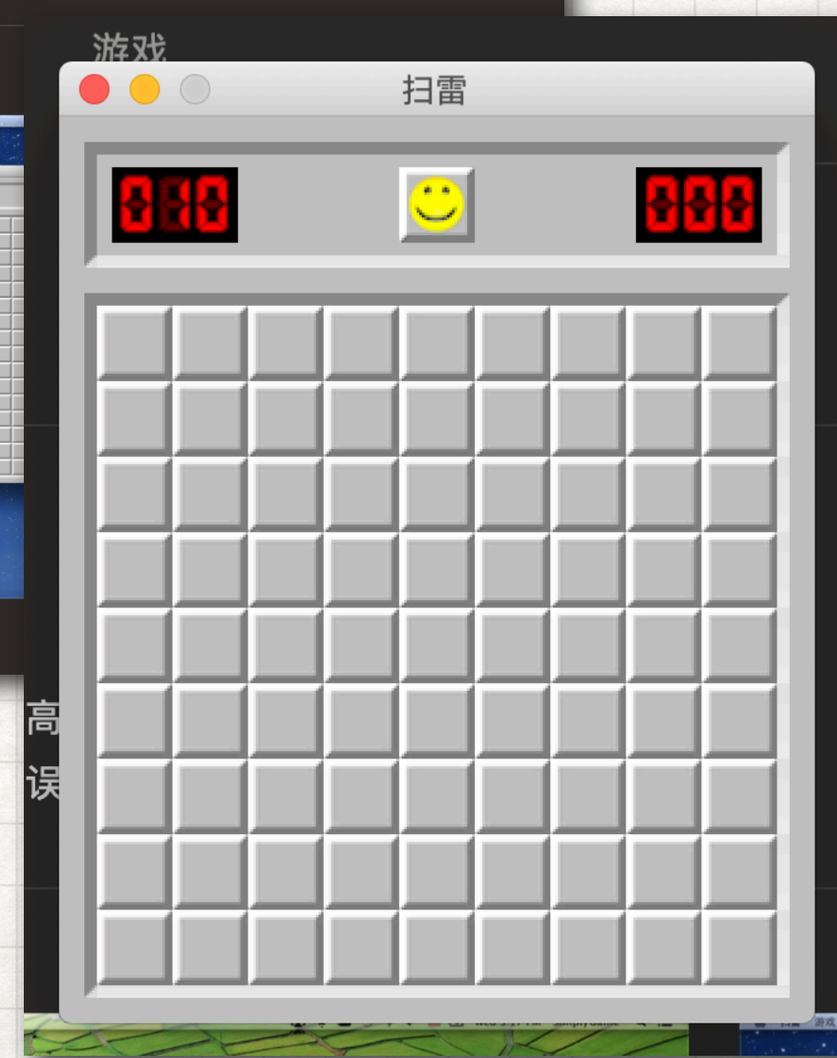
macOS中的原生可执行文件：Mach-O，一种用于可执行文件，目标代码，动态库，内核转储的文件格式。作为a.out格式的替代，Mach-O提供了更强的扩展性，并提升了符号表中信息的访问速度。

IDA Pro、Hopper Disassembler可用于多种操作系统的反汇编静态调试





1 反汇编工具Hopper Disassembler



macOS中的扫雷游戏 Minesweeper Deluxe

商店 窗口 帮助

5个安全帽
15个安全帽
30个安全帽
60个安全帽
90个安全帽

解锁完整版
恢复已购内容

扫雷

下局好运

完成度 38.03%，请再接再厉。你知道吗？可以使用安全帽避免触雷哦，请查看帮助了解使用方法。

新游戏 帮助 确认

扫雷

怎么玩?

控制
==========
鼠标左键开启方块，右键插旗标雷。(如果你用单键鼠标或触控板，使用 "Command(⌘)+点击" 或者 "Control(^)+点击" 代替右键。) 当数字与周围旗子数一致的话，左键点击数字可快速开启周围所有未插旗方块。

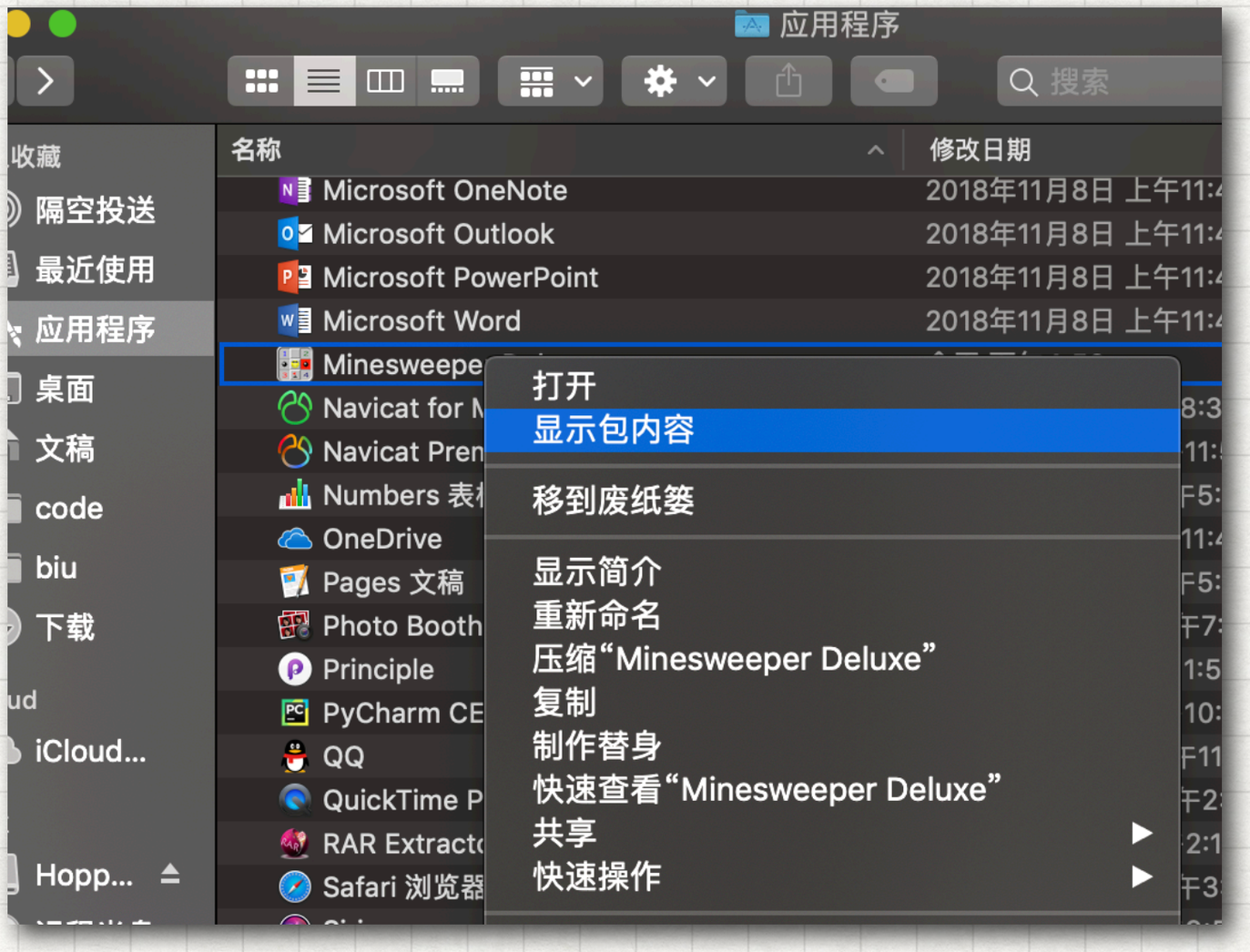
如何获胜
==========
首先开启盘面上的任一方块，下面要么是空的，要么是数字，要么是雷。是雷你就...大侠重来吧。是数字就表示周围八个方块中还有多少雷。根据这些信息继续开启方块或标雷。全部没雷的方块打开后就赢了。简单吧？那么开始冲排行版吧!

级别
==========
初级: 9x9, 10个地雷
中级: 16x16, 40个地雷
高级: 30x16, 99个地雷
自定义: 最多60x32, 999个地雷

使用安全帽
==========
使用 "Alt/Option+左键点击" 可以保证安全。如果方块下面是雷会被插棋，如果下面不是雷会正常打开。每次会用掉一个安全帽。游戏中随时按下 "Alt/Option" 键可以看安全帽数量。安全帽用完了可以在商店菜单中添加，也可以通过分享你的成绩获得免费安全帽。

确认

macOS中应用程序的目录结构

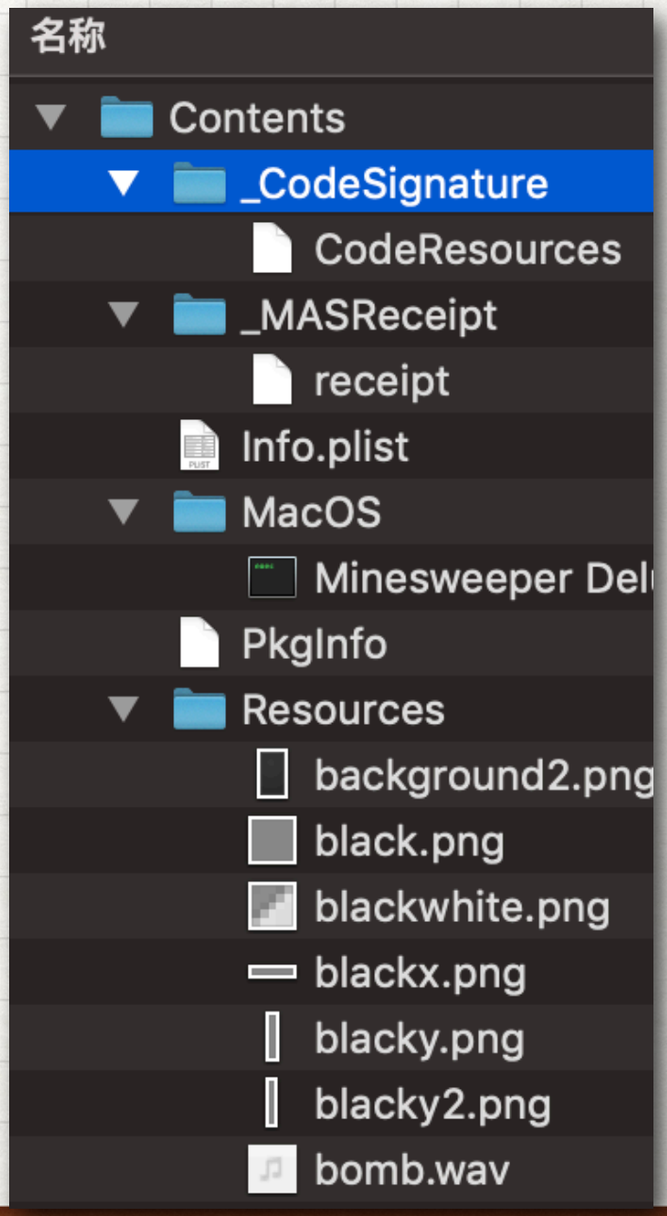


macOS中应用程序的目录结构

_CodeSignature：文件的 hash 列表。CodeResources包含 bundle 中所有其他文件的列表。这个属性列表只有一项 files，键是文件名，值通常是 Base64 格式的散列值。如果键表示的文件是可选的，那么值本身也是一个字典，这个字典有一个 hash 键和一个 optional 键（布尔值 true）。它的作用是用来判断一个应用程序是否完好无损，能够防止不小心修改或损坏资源文件。

CodeResources

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>files</key>
    <dict>
        <key>Resources/ChangeLog</key>
        <data>
        /omrqzsR0+jWweLic0dUHre4LzY=
        </data>
        <key>Resources/English.lproj/InfoPlist.strings</key>
        <dict>
            <key>hash</key>
            <data>
            MiLKDDnrUKr4EmuvhS5VQwxHGK8=
            </data>
            <key>optional</key>
            <true/>
        </dict>
```

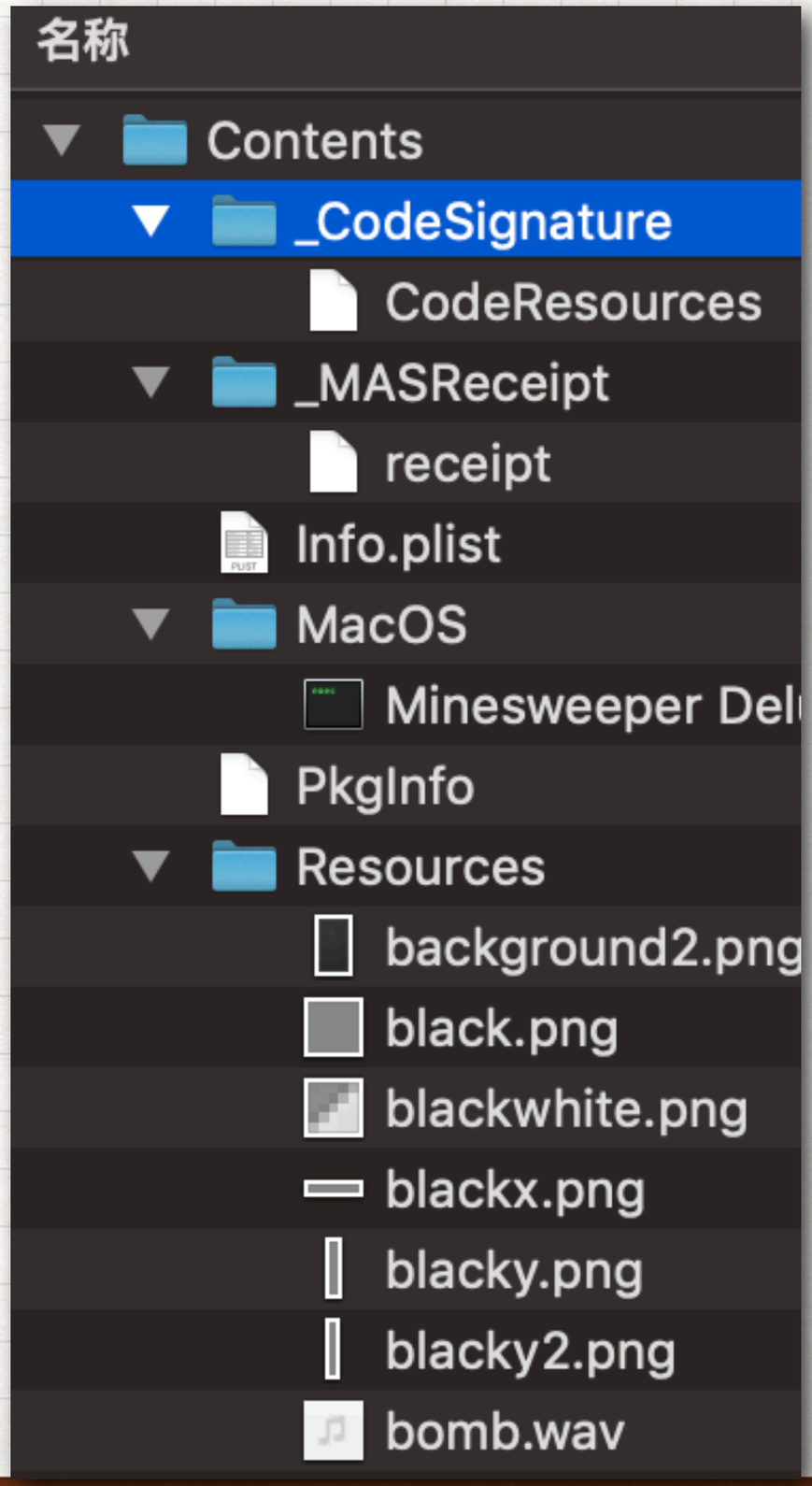


macOS中应用程序的目录结构

_MASReceipt：Mac App Store Receipts

info.plist：保存了 bundle 的元数据信息，判定依赖关系和其他属性

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.(
"http://www.apple.com/DTDs/PropertyList-1.0.dt(
<plist version="1.0">
<dict>
    <key>BuildMachineOSBuild</key>
    <string>12E55</string>
    <key>CFBundleDevelopmentRegion</key>
    <string>English</string>
    <key>CFBundleExecutable</key>
    <string>Minesweeper Deluxe</string>
    <key>CFBundleIconFile</key>
    <string>icon</string>
    <key>CFBundleIdentifier</key>
    <string>com.sg.minesweepermac</string>
    <key>CFBundleInfoDictionaryVersion</key>
    <string>6.0</string>
    <key>CFBundleName</key>
    <string>Minesweeper Deluxe</string>
    <key>CFBundlePackageType</key>
    <string>APPL</string>
    <key>CFBundleShortVersionString</key>
    <string>1.2</string>
    <key>CFBundleSignature</key>
    <string>????</string>
    <key>CFBundleVersion</key>
```



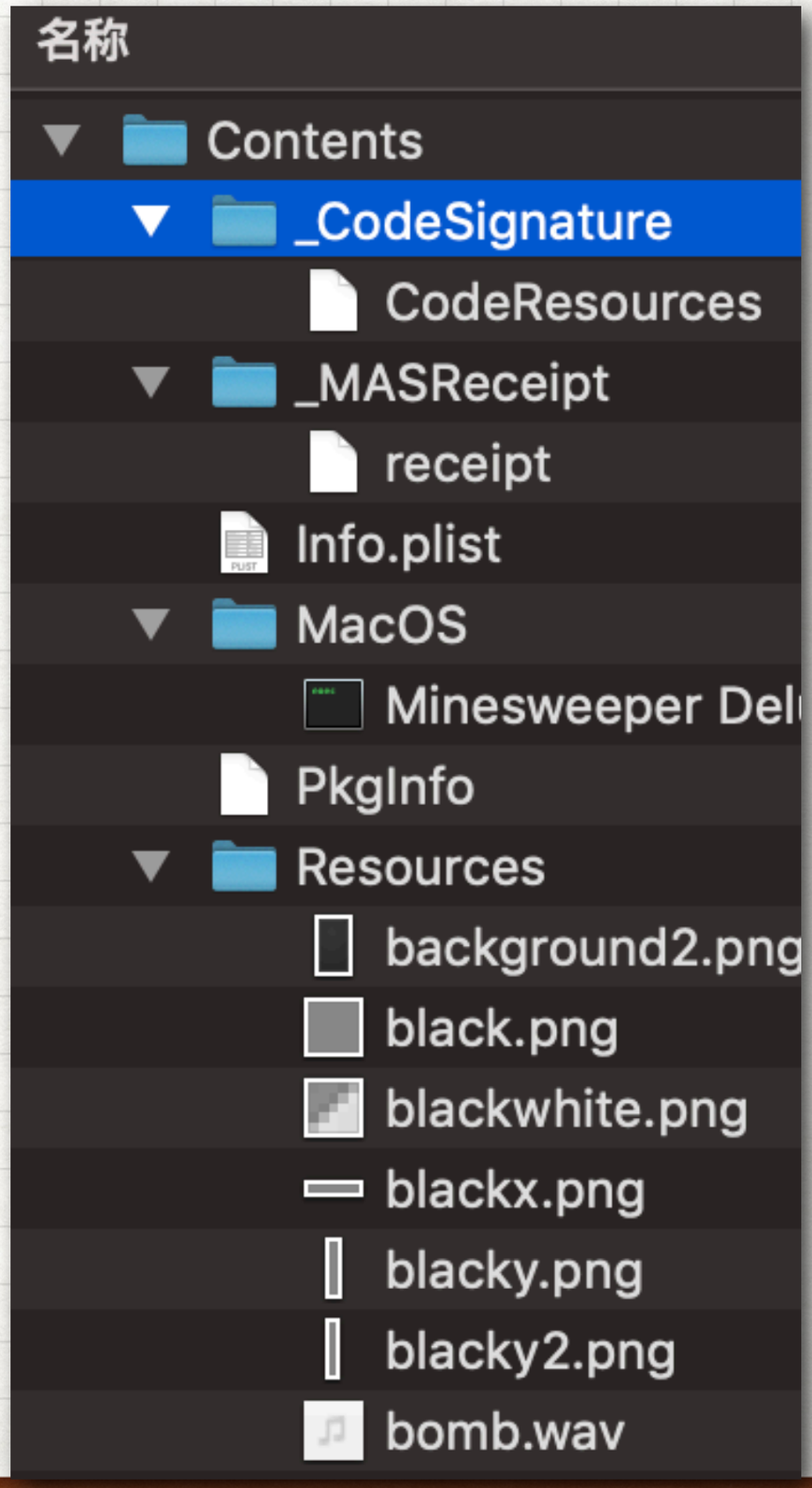
一个标准的 info.plist 文件包含以下条目

- CFBundleDevelopmentRegion: 如果找不到用户指定的语言，就表示默认的语言。
- CFBundleDisplayName：显示给用户的 bundle 名称。
- CFBundleDocumentTypes：这个 bundle 关联的文档类型。
- CFBundleExecutable：这个 bundle 中实际的可执行文件（二进制文件或库文件）。
- CFBundleLconFile：在 Finder 视图中显示的图标文件。
- CFBundleIdentifier：逆 DNS 表示法的标识符。Bundle Id（之后会用到）
- CFBundleName：bundle 的名称（限制在 16 个字符之内）。
- CFBundlePackageType：表示一个 4 字母的代码，例如 APPL = application
- CFBundleSignature：bundle 的4 字母短命。
- CFBundleURLTypes：这个 bundle 关联的 URL。这是一个字典，值指定了这个 bundle 处理的 URL scheme 以及处理方式。

作者：大王叫我来巡山_Cong
链接：https://www.jianshu.com/p/e33412176310
來源：简书
简书著作权归作者所有，任何形式的转载都请联系作者获得授权并注明出处。

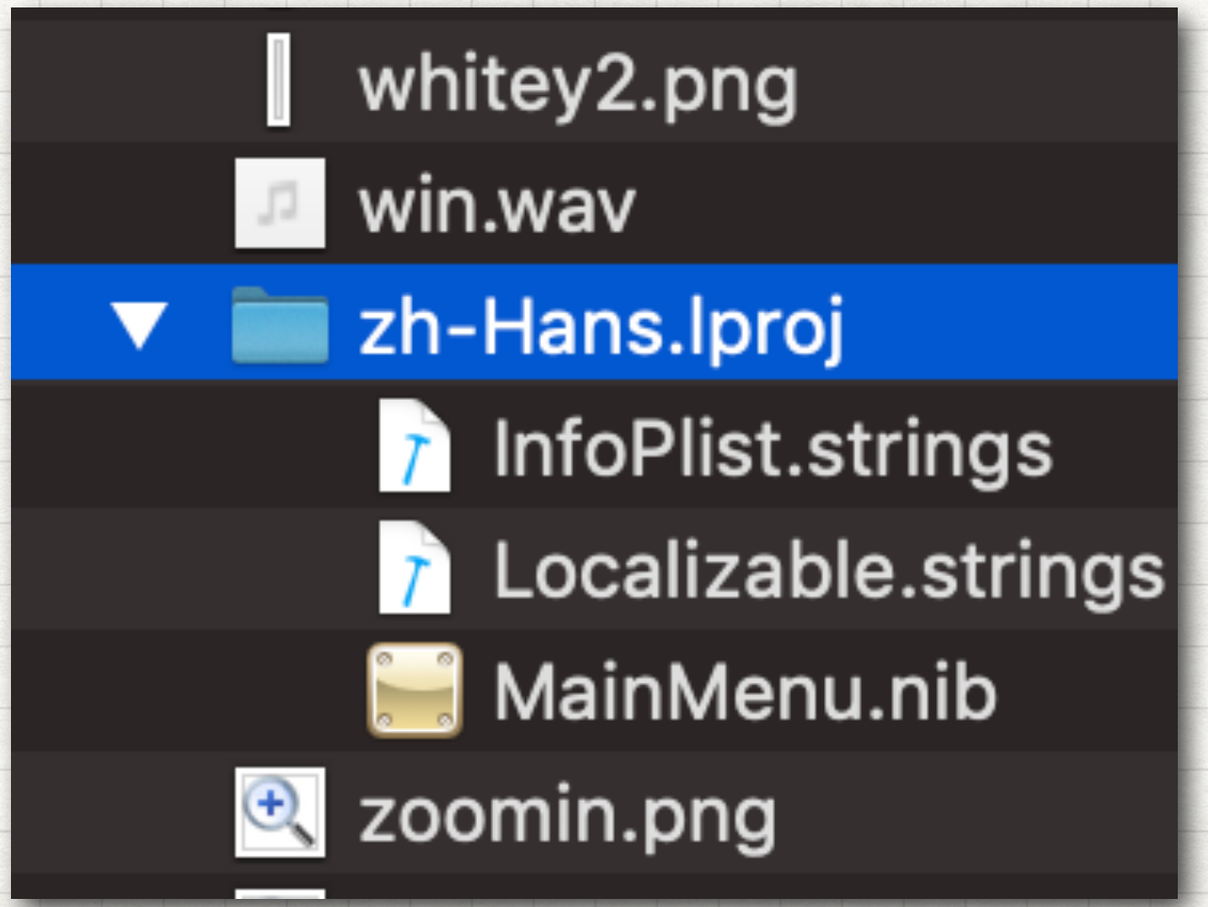
PkgInfo：包的 8 字节标识符

Resources：资源文件



MainMenu.nib 文件是二进制的 plist 文件，其中保存了应用程序中 GUI 组件的位置信息和设置信息。

（Interface Builder 编辑.xib 文件的文本版本，然后再将这些文件打包成二进制格式）



2　　BBEdit——html和文本编辑器，可识别二进制的plist文件

打开MainMenu.nib

untitled text 2

(New Document)

```
2356                <integer>2147483647</integer>
2357                <key>NSOnImage</key>
2358                <dict>
2359                    <key>CF$UID</key>
2360                    <integer>39</integer>
2361                </dict>
2362                <key>NSTitle</key>
2363                <dict>
2364                    <key>CF$UID</key>
2365                    <integer>169</integer>
2366                </dict>
2367            </dict>
2368            <string>15个安全帽</string>
2369            <string>buy15Robot:</string>
2370            <dict>
2371                <key>$class</key>
2372                <dict>
```

可见安全帽与一个Robot的函数相关

Find — Evaluation (30 days left)

Find: 安全帽

Replace:

Matching: Case sensitive Entire word Grep

Search in: Selected text only Wrap around

Next
Previous
First
Find All
Extract
Replace
Replace All

在Hopper Disassembler中拖入Minesweeper Deluxe

Minesweeper Deluxe.hop

Labels | Proc. | Strings

Robot

Tag Scope

-[minesweepermacAppDelegate buy...
-[minesweepermacAppDelegate buy1...
-[minesweepermacAppDelegate buy...
-[minesweepermacAppDelegate buy...
-[minesweepermacAppDelegate buy...
-[ControlLayer useRobot]
-[ControlLayer updateRobotNumber]
-[ControlLayer setRobotNumber:]
-[ControlLayer setRobotVisible:]
-[GameplayLayer useRobotAtRow:at...
-[GameplayLayer useRobot]
-[GameState robot]
-[GameState setRobot:]
-[InAppPurchaseManager purchase5r...
-[InAppPurchaseManager purchase1...
-[InAppPurchaseManager purchase3...
-[InAppPurchaseManager purchase6...
-[InAppPurchaseManager purchase9...
objc_ivar_offset_GameplayLayer_useR...
objc_ivar_offset_GameState_robot
cfstring_addrobotdetail
cfstring_addrobottitle
cfstring_robot
cfstring_com_sg_minesweepermac_r...
cfstring_com_sg_minesweepermac_r...
cfstring_com_sg_minesweepermac_r...
cfstring_com_sg_minesweepermac_r...
cfstring_com_sg_minesweepermac_r...
-[CCProgressTimer boundaryTexCoo...
__objc_proto_CCRGBAProtocol_inst_...
__objc_proto_CCRGBAProtocol_opt_in...

Demo Version

```
0000000100058bf4        pop     rbx
0000000100058bf5        pop     rbp
0000000100058bf6        jmp     rax                                     ; _objc_msgSend
                      ; endp

        ; ================ B E G I N N I N G   O F   P R O C E D U R E ================

                    -[minesweepermacAppDelegate buy5Robot:]:
0000000100058bf8        push    rbp                                     ; Objective C Implementation defined at 0x1000ec148 (instance method), DATA XREF=0x1000ec
0000000100058bf9        mov     rbp, rsp
0000000100058bfc        push    rbx
0000000100058bfd        push    rax
0000000100058bfe        mov     rsi, qword [0x1000f7fc0]                ; @selector(dismissLeaderboardView), argument "selector" for method _objc_msgSend
0000000100058c05        mov     rbx, qword [_objc_msgSend_1000c5278]
0000000100058c0c        mov     rax, rbx
0000000100058c0f        call    rax                                     ; _objc_msgSend
0000000100058c11        mov     rsi, qword [0x1000f7f18]                ; @selector(getInstance), argument "selector" for method _objc_msgSend
0000000100058c18        mov     rdi, qword [objc_cls_ref_InAppPurchaseManager] ; argument "instance" for method _objc_msgSend
0000000100058c1f        mov     rax, rbx
0000000100058c22        call    rax                                     ; _objc_msgSend
0000000100058c24        mov     rsi, qword [0x1000f8010]                ; @selector(purchase5robot), argument "selector" for method _objc_msgSend
0000000100058c2b        mov     rdi, rax                                ; argument "instance" for method _objc_msgSend
0000000100058c2e        mov     rax, rbx
0000000100058c31        add     rsp, 0x8
0000000100058c35        pop     rbx
0000000100058c36        pop     rbp
0000000100058c37        jmp     rax                                     ; _objc_msgSend
                      ; endp

        ; ================ B E G I N N I N G   O F   P R O C E D U R E ================

                    -[minesweepermacAppDelegate buy15Robot:]:
0000000100058c39        push    rbp                                     ; Objective C Implementation defined at 0x1000ec160 (instance method), DATA XREF=0x1000ec
0000000100058c3a        mov     rbp, rsp
0000000100058c3d        push    rbx
0000000100058c3e        push    rax
0000000100058c3f        mov     rsi, qword [0x1000f7fc0]                ; @selector(dismissLeaderboardView), argument "selector" for method _objc_msgSend
0000000100058c46        mov     rbx, qword [_objc_msgSend_1000c5278]
0000000100058c4d        mov     rax, rbx
0000000100058c50        call    rax                                     ; _objc_msgSend
0000000100058c52        mov     rsi, qword [0x1000f7f18]                ; @selector(getInstance), argument "selector" for method _objc_msgSend
0000000100058c59        mov     rdi, qword [objc_cls_ref_InAppPurchaseManager] ; argument "instance" for method _objc_msgSend
0000000100058c60        mov     rax, rbx
0000000100058c63        call    rax                                     ; _objc_msgSend
0000000100058c65        mov     rsi, qword [0x1000f8018]                ; @selector(purchase15robot), argument "selector" for method _objc_msgSend
0000000100058c6c        mov     rdi, rax                                ; argument "instance" for method _objc_msgSend
0000000100058c6f        mov     rax, rbx
0000000100058c72        add     rsp, 0x8
0000000100058c76        pop     rbx
```

Address 0x100058bf8, Segment __TEXT, -[minesweepermacAppDelegate buy5Robot:] + 0, Section __text, file offset 0x58bf8

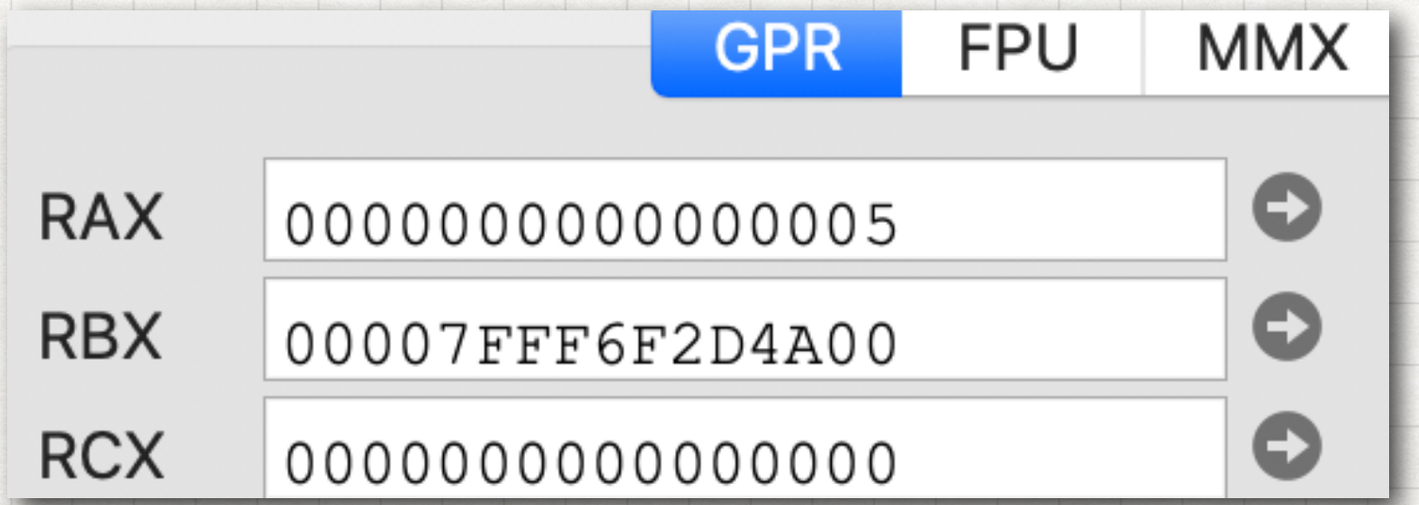
-[minesweepermacAppDelegate buy...
-[minesweepermacAppDelegate buy1...
-[minesweepermacAppDelegate buy...
-[minesweepermacAppDelegate buy...
-[minesweepermacAppDelegate buy...
-[ControlLayer useRobot]
-[ControlLayer updateRobotNumber]
-[ControlLayer setRobotNumber:]
-[ControlLayer setRobotVisible:]
-[GameplayLayer useRobotAtRow:at...
-[GameplayLayer useRobot]
-[GameState robot]
-[GameState setRobot:]

搜索Robot选择其中的函数
-[GameState robot]
设置断点

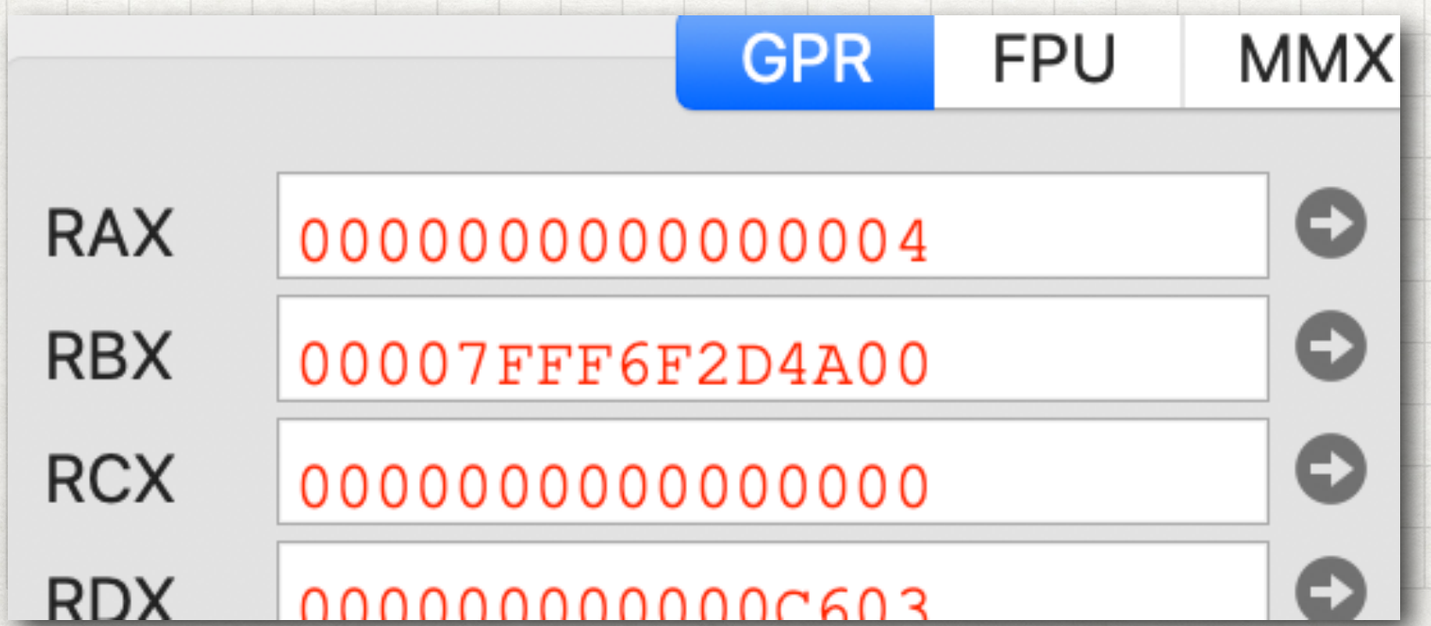
```
        ; ================ B E G I N N I N G   O F   P R O C E D U R E ======

 -[GameState robot]:
push        rbp             ; Objective C Implementation defined at 0x1000ee6d8 (
mov         rbp, rsp
mov         rax, qword [objc_ivar_offset_GameState_robot]
mov         eax, dword [rdi+rax]
pop         rbp
ret
```

通过Hopper debug server中进行调试。每次按下option键时都会遇到断点。可见每次只要使用安全帽，都会进入到这个函数。



使用完一次安全帽以后rax寄存器里保存的该函数的返回值从5变成了4。



```
                    -[GameState robot]:
000000010006389d        push        rbp                                         ; Obj
000000010006389e        mov         rbp, rsp
00000001000638a1        mov         rax, qword [objc_ivar_offset_GameState_robot]
00000001000638a8        mov         eax, dword [rdi+rax]
00000001000638ab        pop         rbp
00000001000638ac        ret
                       ; endp
```

分析这个函数可知

在00000001000638a8处，rax的低32位（eax）中的值被修改为dword[rdi+rax]

我们可以将它直接修改为一个固定的值比如1，使得安全帽永远都是一个。

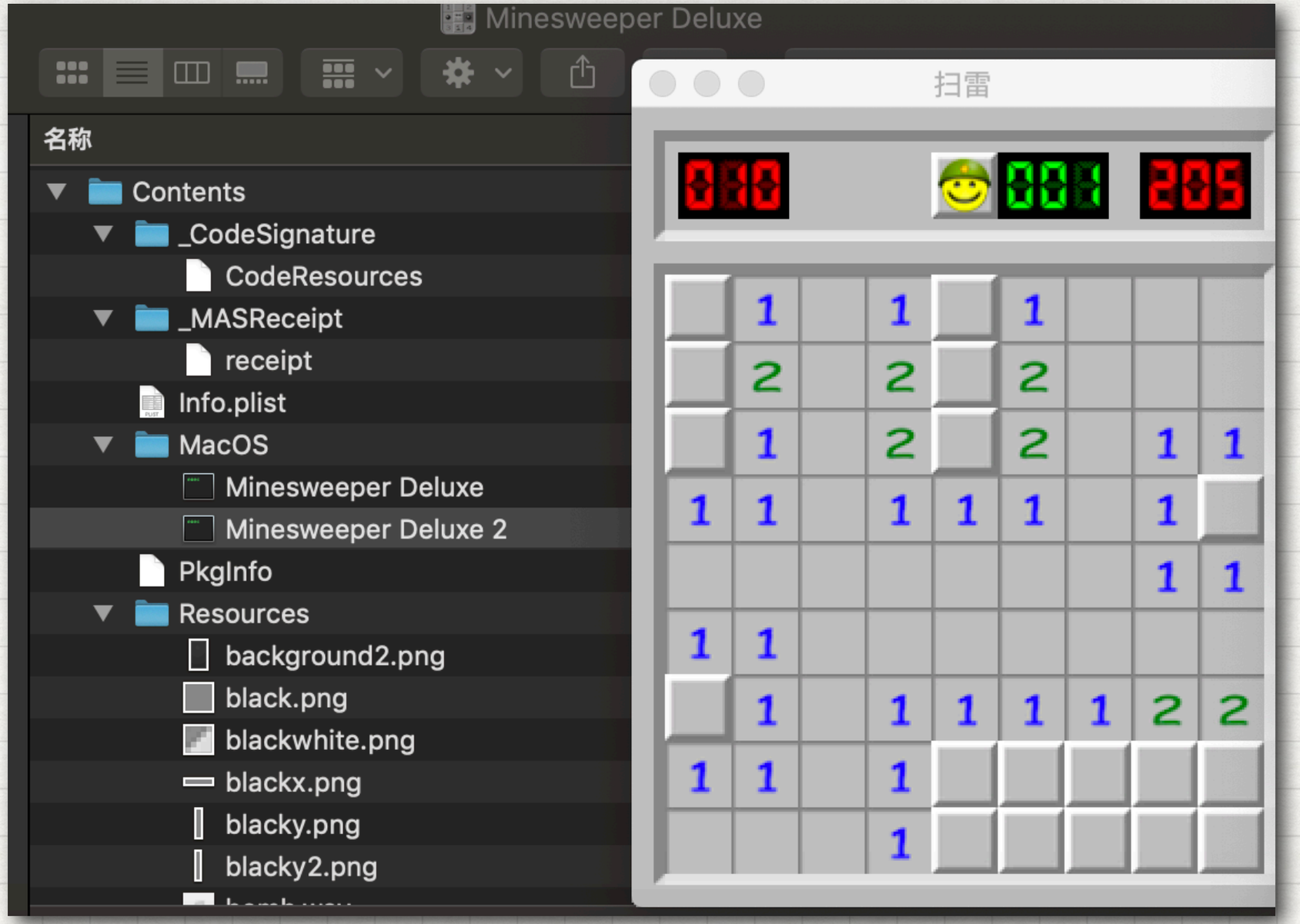
```
                    -[GameState robot]:
000000010006389d        push        rbp                                         ; Obj
000000010006389e        mov         rbp, rsp
0000000100063 8a1       mov         rax, qword [objc_ivar_offset_GameState_robot]
0000000100063 8a8       mov         eax, dword [rdi+rax]
0000000100063 8ab       pop         rbp
00000010
```

mov al, 0x1

CPU mode: Generic

```
                    -[GameState robot]:
000000010006389d        push        rbp                                         ;
000000010006389e        mov         rbp, rsp
00000001000638a1        mov         rax, qword [objc_ivar_offset_GameState_robot]
00000001000638a8        mov         al, 0x1
                      ; endp
00000001000638aa        nop
00000001000638ab        pop         rbp
00000001000638ac        ret
-----------------------------------------------------------------------------
```

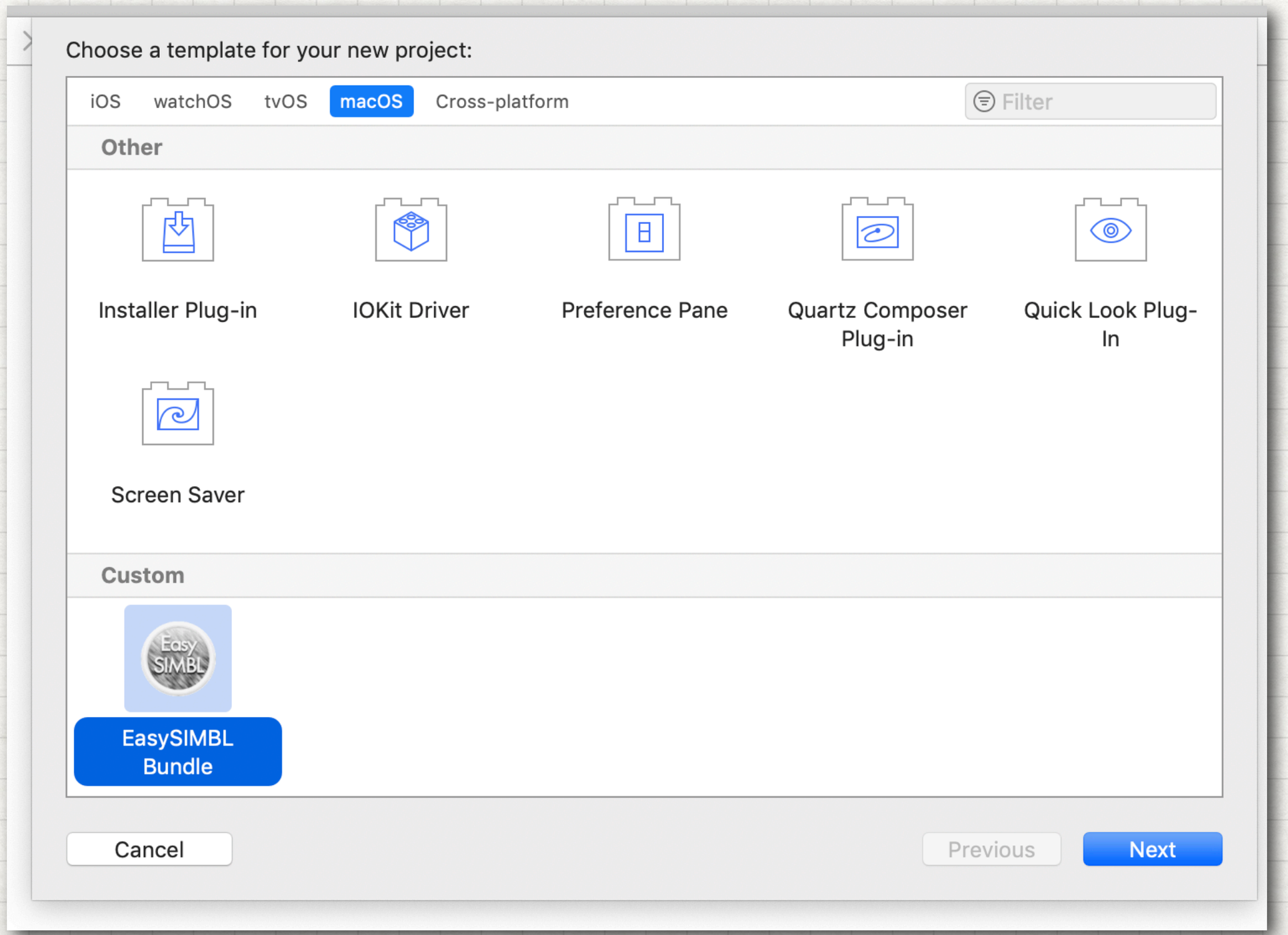
修改如图，再导出二进制文件放到包中覆盖



打开Minesweep Deluxe 2，如图，安全帽一直都有一个。

也可以自己编写一个破解补丁

IDE环境：Xcode
导入一个自定义模板



Info.plist

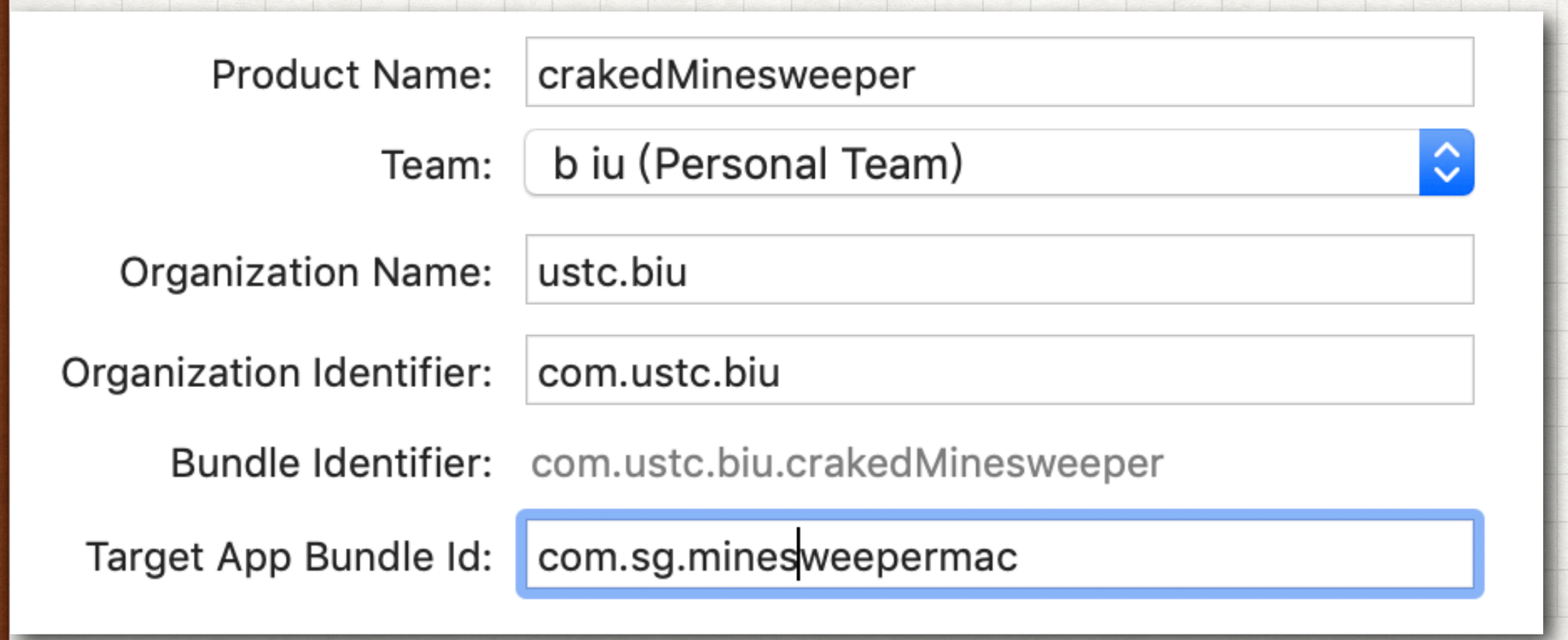
```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>BuildMachineOSBuild</key>
    <string>12E55</string>
    <key>CFBundleDevelopmentRegion</key>
    <string>English</string>
    <key>CFBundleExecutable</key>
    <string>Minesweeper Deluxe</string>
    <key>CFBundleIconFile</key>
    <string>icon</string>
    <key>CFBundleIdentifier</key>
    <string>com.sg.minesweepermac</string>
```

.* Aa “” bundleId Find Find Prev Find All

ASCII, 1 match Tab Size: 4 XML

Bundle Id-PPT第9页在Minesweeper的Info.plist文件中

Target App Bundle Id中填入要破解的软件的Bundle Id



Hook：使用SIMBL(帮助第三方开发人员修改和添加使用Cocoa环境开发的应用程序的功能，而无需访问源代码)

将目标代码加载到特定应用程序中

GameState类 robot方法

```
+ (void)hookGameState {
    NSError *error;
    [self jr_swizzleMethod:@selector(robot)
                withMethod:@selector(craked_robot)
                     error:&error];
    if (error) {
        NSLog(@"+++++hookGameState error: %@", error);
    }
}

- (int)craked_robot {
    return 1;
}
```

函数返回值始终为1（rax寄存器中值始终为1）

把robot成员变量用cracked_robot替代

mySIMBL——扩展包(plug in)管理软件

Home | Software | Contact

culater.

SIMBL

Problem:
Some applications do about 90% of what I want.

Solution:
Develop my own applications.

Better Solution:
Patch the application myself...

Links and Downloads

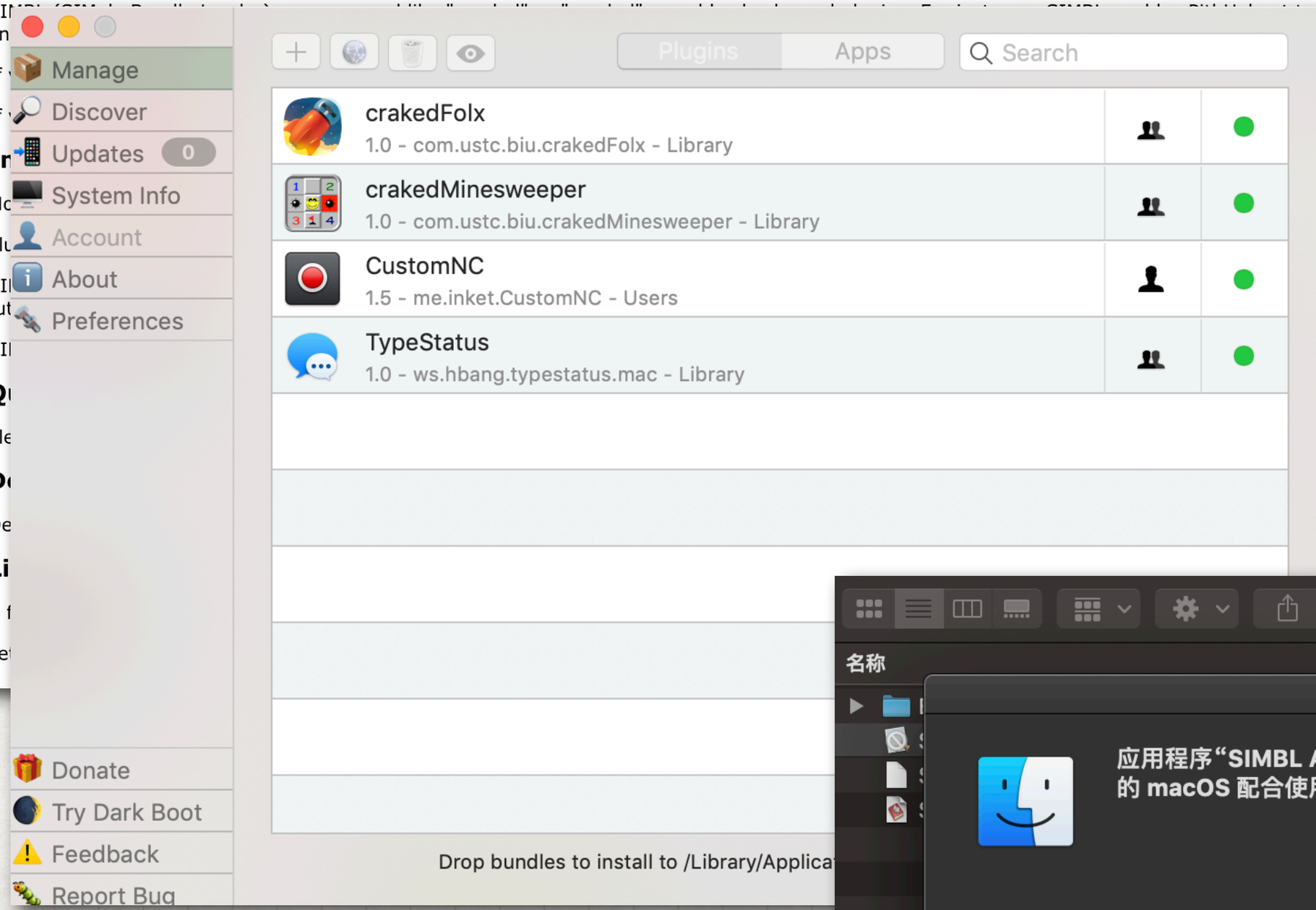
SIMBL-0.9.9.zip (Snow Leopard and Leopard)

SIMBL-0.8.2.tbz (Leopard and Tiger)

Donate

Development Related News

SIMBL source code



r just your account.

ormation, you can read the SIMBL section in my brief

sted, feel free to edit the list on the wiki.

破解高级版

修改if中的判断

```
</dict>
<string>高级</string>
<string>3</string>
<string>expert</string>
<dict>
    <key>$class</key>
    <dict>
        <key>CF$UID</key>
```

Find — Evaluation (24 days left)

Find: 高级

Replace:

Next | Previous | First | Find All | Extract | Replace

expert

Tag Scope

- -[minesweepermacAppDelegate start...
- -[GameState expert1]
- -[GameState setExpert1:]
- -[GameState expert2]
- -[GameState setExpert2:]
- -[GameState expert3]
- -[GameState setExpert3:]
- objc_ivar_offset_minesweepermacAp...
- objc_ivar_offset_GameState_expert1
- objc_ivar_offset_GameState_expert2
- objc_ivar_offset_GameState_expert3
- cfstring_grp_com_sg_minesweeper_e...
- cfstring_expert
- cfstring_expert1
- cfstring_expert2
- cfstring_expert3
- +[CCTexture2D bitsPerPixelForForm...
- -[CCTexture2D bitsPerPixelForFormat]

Remove HI/LO macros Remove potentially dead cod

```
void -[minesweepermacAppDelegate startNewGameExpert:](void
    rdx = arg2;
    rbx = self;
    [self dismissLeaderboardView];
    if ([[GameState sharedInstance] fullgame] != 0x0) {
            rax = [GameState sharedInstance];
            [rax setDifficulty:0x2];
            rax = [GameState sharedInstance];
            [rax save];
            [rbx->beginner setState:0x0];
            [rbx->intermediate setState:0x0];
            [rbx->expert setState:0x1];
            [rbx->custom setState:0x0];
            [rbx->window_ setIsVisible:0x0];
            rdi = rbx->window_;
            intrinsic_movaps(var_40, 0x0);
            [rdi setFrame:0x1 display:0x0 animate:r8];
            [rbx->window_ center];
            rax = [GameManager sharedGameManager];
            [rax runSceneWithID:0x65];
            [rbx->window_ setIsVisible:0x1];
    }
    else {
            [rbx unlockFullgame:0x0];
    }
    return;
}
```

将je修改为jne

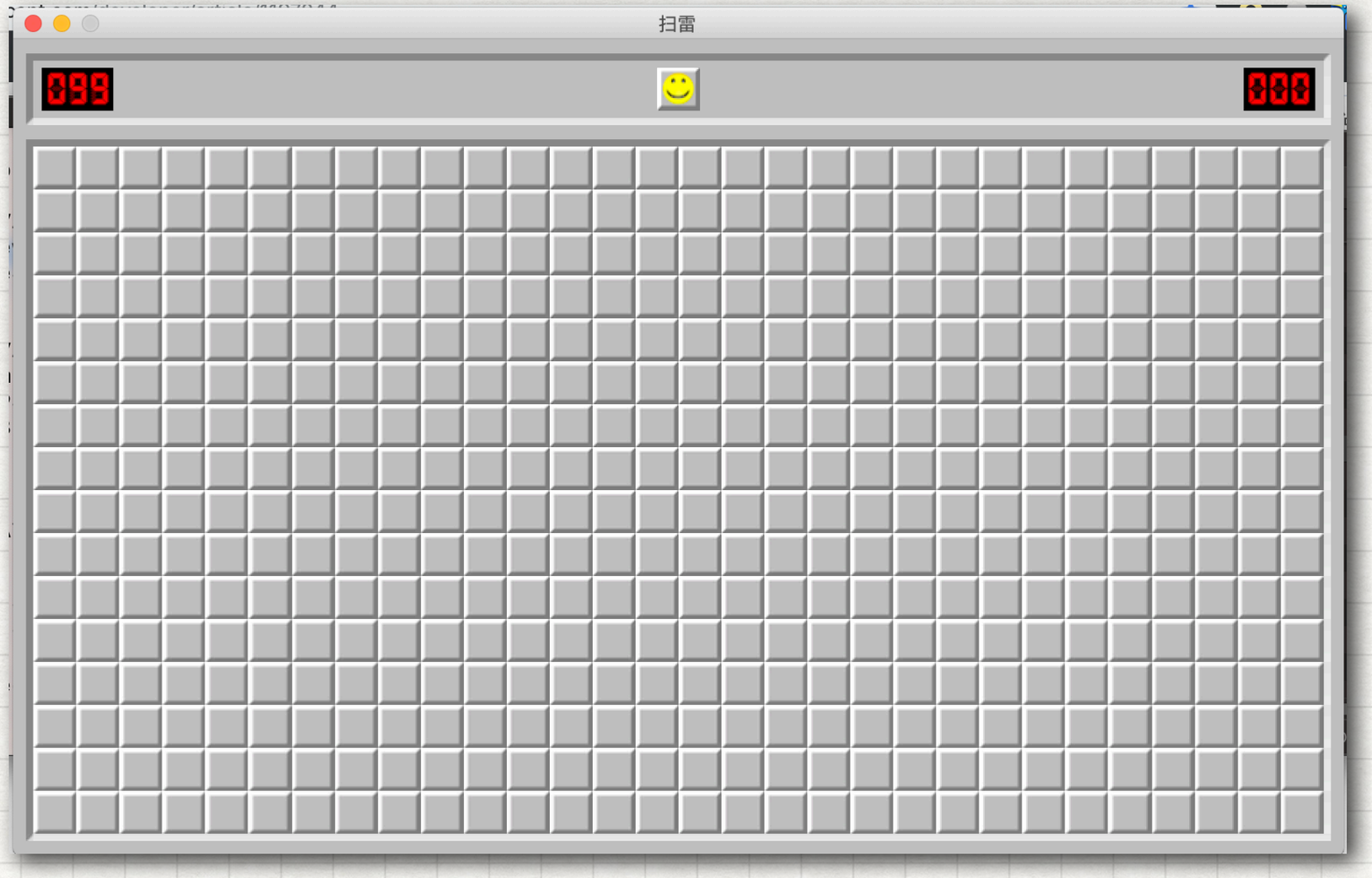
```
0000001000589c1          call     r14
0000001000589c4          test     al, al
0000001000589c6          je       loc_100058b24

jne loc_100058b24
CPU mode:  Generic
Assemble and Go Next

000000100058a07          mov      rdi, rax
000000100058a0a          call     r14
000000100058a0d          mov      rax, qword [objc_ivar_offset_minesweepermacApp
```

```
000000010005898d         push     rbx
000000010005898e         sub      rsp, 0x48
0000000100058992         mov      rbx, rdi
0000000100058995         mov      rsi, qword [0x1000f7fc0]                  ; @selec
000000010005899c         mov      r14, qword [_objc_msgSend_1000c5278]
00000001000589a3         call     r14                                       ; _objc_
00000001000589a6         mov      rsi, qword [0x1000f7bb0]                  ; @selec
00000001000589ad         mov      rdi, qword [objc_cls_ref_GameState]       ; argume
00000001000589b4         call     r14                                       ; _objc_
00000001000589b7         mov      rsi, qword [0x1000f7ef8]                  ; @selec
00000001000589be         mov      rdi, rax                                  ; argume
00000001000589c1         call     r14                                       ; _objc_
00000001000589c4         test     al, al
00000001000589c6         jne      -[minesweepermacAppDelegate startNewGameExpert:]+71

00000001000589cc         mov      rsi, qword [0x1000f7bb0]                  ; @selec
00000001000589d3         mov      rdi, qword [objc_cls_ref_GameState]       ; argume
0000                                                                        ; _objc_
0000                                                                        ; @selec
```



高级版解锁