日	쿺
н	

前言	1.1
iOSOpenDev概览	1.2
安装iOSOpenDev	1.3
确认安装成功	1.3.1
普通的插件开发流程	1.4
新建iOSOpenDev项目	1.4.1
初始化项目配置	1.4.2
搞懂.xm和.mm文件的逻辑	1.4.3
如何新增xm文件	1.4.3.1
写hook插件代码	1.4.4
调试插件代码	1.4.5
带界面的插件开发流程	1.5
前提和目标	1.5.1
基本流程	1.5.2
使用效果	1.5.3
常见问题	1.6
安装器遇到了一个错误	1.6.1
PrivateFramework directory not found	1.6.2
File not found XCode Specifications	1.6.3
.xm被识别为Audio音频文件	1.6.4
Expected unqualified-id	1.6.5
无法识别的特殊字符	1.6.5.1
Compile Sources中误添加了不支持的.xm	1.6.5.2
Host key verification failed	1.6.6
scp dest open No file or directory	1.6.7
An empty identity is not valid	1.6.8
control的Version版本号的改动会丢失	1.6.9
安装插件后桌面上看不到iOS的app图标	1.6.10
mach-o incompatible arch arm64 arm64e	1.6.11
Failed Logos Processor Could not open xm	1.6.12
经验心得	1.7
相关教程和代码	1.8
附录	1.9
参考资料	1.9.1

前言

## iOS逆向开发: iOSOpenDev开发插件

- 最新版本: v1.8.2
- 更新时间: 20250115

## 简介

介绍iOS逆向中如何用iOSOpenDev开发越狱插件tweak。先是对iOSOpenDev概览;然后介绍如何安装iOSOpenDev,以及 安装后确认安装成功;然后是普通的插件的开发流程,包括新建iOSOpenDev的Xcode项目、初始化项目的配置,其中包括 ssh免密登录、写hook插件tweak代码,包括如何新增文件、编译代码调试代码等;以及带UI界面的插件开发的流程,包括前 提和目标、基本流程、使用效果、常见问题等;以及常见问题和一些经验心得;常见问题包括初始化环境方面的问题和编译 调试方面的问题。

### 源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下:

#### HonKit源码

• crifan/ios\_re\_iosopendev\_tweak: iOS逆向开发: iOSOpenDev开发插件

#### 如何使用此HonKit源码去生成发布为电子书

详见: crifan/honkit\_template: demo how to use crifan honkit template and demo

#### 在线浏览

- iOS逆向开发: iOSOpenDev开发插件 book.crifan.org
- iOS逆向开发: iOSOpenDev开发插件 crifan.github.io

#### 离线下载阅读

- iOS逆向开发: iOSOpenDev开发插件 PDF
- iOS逆向开发: iOSOpenDev开发插件 ePub
- iOS逆向开发: iOSOpenDev开发插件 Mobi

### 版权和用途说明

此电子书教程的全部内容,如无特别说明,均为本人原创。其中部分内容参考自网络,均已备注了出处。如发现有侵权,请 通过邮箱联系我 admin <sup>艾特</sup> crifan.com,我会尽快删除。谢谢合作。

各种技术类教程,仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途,均与本人无关。

### 鸣谢

感谢我的老婆**陈雪**的包容理解和悉心照料,才使得我 crifan 有更多精力去专注技术专研和整理归纳出这些电子书和技术教 程,特此鸣谢。

### 其他

### 作者的其他电子书

本人 crifan 还写了其他 150+ 本电子书教程, 感兴趣可移步至:

crifan/crifan\_ebook\_readme: Crifan的电子书的使用说明

### 关于作者

关于作者更多介绍,详见:

关于CrifanLi李茂 – 在路上

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-01-15 16:29:09

# iOSOpenDev概览

在iOS逆向期间,往往涉及到去开发越狱插件tweak,其中常见的工具=框架之一就是: iosopenDev 。

- iOSOpenDev
  - 。 概述: iOS越狱插件tweak开发框架之一
    - 其他竞品
      - Theos/Logos
      - MonkeyDev
  - 。常用核心功能:支持基于XCode(的模板)去创建Logos的tweak越狱插件
  - o 官网
    - http://iosopendev.com/
    - 下载
      - http://iosopendev.com/download/
  - Github
    - https://github.com/kokoabim/iOSOpenDev
    - Wiki
      - https://github.com/kokoabim/iOSOpenDev/wiki
      - 对于Logos(=Theos?)的支持
        - https://github.com/kokoabim/iOSOpenDev/wiki/Logos-(Theos)-Support
      - 项目转换
        - https://github.com/kokoabim/iOSOpenDev/wiki/Convert-to-iOSOpenDev-Project

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-10-25 19:55:34

# 安装iOSOpenDev

#### 从官网iOSOpenDev—Download下载到: iOSOpenDev-1.6-2.pkg,双击去安装:



成功安装后,去 Xcode 中新建 iOS 项目,即可看到 iOSOpenDev 的的选项:

É	Xcode	File	Edit	View	Fine	d Navigate	Editor	Product	Debug	Source Cont	rol Window	Help	83		5 🔍	Ro-	0	8
0 0	•				▶													
8				5 D														
						No Selection												
						C.,	Choose a te	mplate for	your new	project:								
							Multiplatfo	orm iOS	macOS	watchOS t	vOS Other			(	🖲 Filter			
							Framew	ork & Libr	ary									
							iOSOpe	nDev									٦	
							Me	nu	1		î5				1			
																Touch		
							Action	Menu	Activato	or Listener	AssistantExter	sio	CaptainHo Tweak	ok	Cocc	a Touch		
								_							6	Sidi y		
							exec		3		1				1. A	and the summer	ш	
							Comma	nd-line	Empty	Project	Logos Twea	< I	NotificationC	enter	Prefere	nceLoad	er	
							То	ol					Widget		B	undle	ш	
							8	B	ex	ec							ш	
							SBSetting	is Toggle	XPC	Service							ш	
							obotting		Ares									
							Cance							Pr	evious	Ne	xt	

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-11-08 16:59:45

## 确认安装成功

### 环境变量

再去确认,是否把iOSOpenDev的相关环境变量,加到启动脚本(此处是 zsh , 所以是 ./zshrc ) 中了:

```
→ ~ cat ~/.zshrc | grep i0SOpenDev
export i0SOpenDevPath /opt/i0SOpenDev
export i0SOpenDevDevice=
export PATH /opt/i0SOpenDev/bin:$PATH
```

如果没有:

```
x crifan@licrifandeMacBook-Pro<sup>-</sup> /opt/i0S0penDevSetup/bin<sup>-</sup> cat ~/.zshrc + grep i0S0penDev
```

则自己手动去加上:

```
crifan@licrifandeMacBook-Pro<sup>r</sup> /opt/iOSOpenDevSetup/bin<sup>r</sup> vi ~/.zshrc
crifan@licrifandeMacBook-Pro<sup>r</sup> /opt/iOSOpenDevSetup/bin<sup>r</sup> cat ~/.zshrc | grep iOSOpenDev
export iOSOpenDevPath=/opt/iOSOpenDev
export iOSOpenDevDevice=
export PATH /opt/iOSOpenDev/bin:$PATH
crifan@licrifandeMacBook-Pro<sup>r</sup> /opt/iOSOpenDevSetup/bin<sup>r</sup> source ~/.zshrc
```

## Xcode中的iOSOpenDev的模板

确认是否有多出的template模板:

```
→ ~ 11 ~/Library/Developer/Xcode/
total 0
drwxr-xr-x 8 crifan staff 256B 10 14 11:13 DerivedData
srwxr-xr-x 1 crifan staff 0B 10 27 08:54 GPUToolsAgent.sock
drwxr-xr-x 3 crifan staff 96B 10 27 08:49 Templates
drwxr-xr-x 6 crifan staff 192B 10 20 22:37 UserData
drwxr-xr-x 5 crifan staff 160B 9 30 22:11 iOS Device Logs
drwxr-xr-x 4 crifan staff 128B 10 13 13:54 iOS DeviceSupport
→ ~ 11 ~/Library/Developer/Xcode/Templates
total 0
lrwxr-xr-x 1 root staff 25B 10 27 08:49 iOSOpenDev -> /opt/iOSOpenDev/templates
```

此处是有的:

- 多出了软链接:
  - o ~/Library/Developer/Xcode/Templates/iOSOpenDev
    - 指向的是:
      - /opt/iOSOpenDev/templates

以及接着去看看,具体有哪些模板:

```
→ ~ 11 /opt/iOSOpenDev/templates
total 48
drwxr-xr-x 5 root wheel 160B 10 27 08:32 Action Menu Plugin.xctemplate
drwxr-xr-x 6 root wheel 192B 10 27 08:32 Activator Listener.xctemplate
drwxr-xr-x 12 root wheel 384B 10 27 08:32 AssistantExtensions Extension.xctemplate
drwxr-xr-x 4 root wheel 128B 10 27 08:32 Base.xctemplate
drwxr-xr-x 6 root wheel 192B 10 27 08:32 CaptainHook Tweak.xctemplate
drwxr-xr-x 6 root wheel 192B 10 27 08:32 Command-line Tool.xctemplate
drwxr-xr-x 4 root wheel 128B 10 27 08:32 Command-line Tool.xctemplate
```

```
drwxr-xr-x 4 root wheel 128B 10 27 08:32 Empty Project.xctemplate
           1 root wheel
- rw-r--r--
                            18K 10 27 08:49 LICENSE
drwxr-xr-x
            6 root wheel
                            192B 10 27 08:32 Logos Tweak.xctemplate
drwxr-xr-x 5 root wheel 160B 10 27 08:32 ManPage.xctemplate
drwxr=xr=x 11 root wheel
                            352B 10 27 08:32 NotificationCenter Widget.xctemplate
drwxr=xr=x 12 root wheel
                            384B 10 27 08:32 PreferenceLoader Bundle.xctemplate
drwxr-xr-x 7 root wheel 224B 10 27 08:32 PreferenceLoader.xctemplate
                            352B 10 27 08:49 README.md
-rw-r--r--
           1 root wheel
drwxr=xr=x 5 root wheel
drwxr=xr=x 4 root wheel
                                 10 27 08:32 SBSettings Toggle.xctemplate
                            160B
                            128B 10 27 08:32 Unit Tests.xctemplate
drwxr=xr=x 7 root wheel 224B 10 27 08:32 XPC Service.xctemplate
```

很明显,部分模板,应该就是对应着界面中看到的各个模板:

#### 比如:

- Logos Tweak.xctemplate -> Logos Tweak
- Command-line Tool.xctemplate -> Command-line Tool
- PreferenceLoader Bundle.xctemplate -> PreferenceLoader Bundle

### iOSOpenDev中的内容

顺带再去看看,当前iOSOpenDev目录中的内容:

```
→ /opt 11
total 🛛
drwxr-xr-x 9 root wheel
                         288B 10 27 08:32 10SOpenDev
drwxr-xr-x 3 root wheel
                          96B 10 27 08:32 10SOpenDevSetup
drwxr-xr-x 3 root wheel
                           96B 10 27 08:32 iOSOpenDevUninstall
→ /opt cd iOSOpenDev
→ iOSOpenDev pwd
/opt/iOSOpenDev
→ iOSOpenDev 11
total 48
-rw-r--r--
            1 root wheel
                           18K 10 27 08:49 LICENSE
                           352B 10 27 08:49 README.md
-rw-r--r--
           1 root wheel
drwxr-xr-x 6 root wheel 192B 10 27 08:32 bin
drwxr-xr-x 2 root wheel
                           64B 10 27 08:32 frameworks
                           256B 10 27 08:32 include
drwxr-xr-x
           8 root wheel
drwxr-xr-x 5 root wheel 160B 10 27 08:32 lib
drwxr=xr=x 21 root wheel 672B 10 27 08:32 templates
→ iOSOpenDev ll bin
total 3000
-rwxr-xr-x 1 root wheel 428K 10 27 08:49 class-dump
-rwxr-xr-x 1 root wheel
                          628K 10 27 08:49 class-dump-z
-rwxr-xr-x 1 root wheel
                          59K 10 27 08:49 iosod
=rwxr=xr=x 1 root wheel 383K 10 27 08:49 ldid
→ iOSOpenDev ll frameworks
→ iOSOpenDev ll include
total 48
                            96B 10 27 08:32 ActionMenu
drwxr-xr-x
           3 root wheel
drwxr-xr-x 3 root wheel
                           96B 10 27 08:32 AssistantExtensions
drwxr-xr-x 3 root wheel
                           96B 10 27 08:32 CaptainHook
                           320B 10 27 08:32 libactivator
drwxr-xr-x 10 root wheel
drwxr-xr-x 3 root wheel
                           96B 10 27 08:32 logos
-rw-r--r-- 1 root wheel
                          21K 10 27 08:49 substrate.h
→ iOSOpenDev ll lib
total 1216
-rwxr-xr-x 1 root wheel
                           77K 10 27 08:49 libactionmenu.dylib
                          422K 10 27 08:49 libactivator.dylib
-rwxr-xr-x 1 root wheel
-rwxr-xr-x 1 root wheel
                          101K 10 27 08:49 libsubstrate.dvlib
→ iOSOpenDev ll templates
total 48
           5 root wheel 160B 10 27 08:32 Action Menu Plugin.xctemplate
drwxr=xr=x
drwxr=xr=x 6 root wheel
                           192B 10 27 08:32 Activator Listener.xctemplate
drwxr-xr-x 12 root wheel
                           384B 10 27 08:32 AssistantExtensions Extension.xctemplate
drwxr-xr-x 4 root wheel
                           128B 10 27 08:32 Base.xctemplate
drwxr=xr=x 6 root wheel
                           192B 10 27 08:32 CaptainHook Tweak.xctemplate
drwxr=xr=x
           6 root wheel
                           192B 10 27 08:32 Cocoa Touch Library.xctemplate
drwxr=xr=x 5 root wheel
                           160B 10 27 08:32 Command-line Tool.xctemplate
drwxr=xr=x 4 root wheel
                           128B 10 27 08:32 Debian Package.xctemplate
drwxr-xr-x 4 root wheel 128B 10 27 08:32 Empty Project.xctemplate
```

= rw= r = = r = =	1 root	wheel	18K 10 27	08:49	LICENSE
drwxr-xr-x	6 root	wheel	192B 10 27	08:32	Logos Tweak.xctemplate
drwxr-xr-x	5 root	wheel	160B 10 27	08:32	ManPage.xctemplate
drwxr-xr-x	<b>11</b> root	wheel	352B 10 27	08:32	NotificationCenter Widget.xctemplate
drwxr-xr-x	12 root	wheel	384B 10 27	08:32	PreferenceLoader Bundle.xctemplate
drwxr-xr-x	7 root	wheel	224B 10 27	08:32	PreferenceLoader.xctemplate
-rw-rr	1 root	wheel	352B 10 27	08:49	README.md
drwxr-xr-x	5 root	wheel	160B 10 27	08:32	SBSettings Toggle.xctemplate
drwxr-xr-x	4 root	wheel	128B 10 27	08:32	Unit Tests.xctemplate
drwxr-xr-x	7 root	wheel	224B 10 27	08:32	XPC Service.xctemplate

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-11-08 16:58:58

# 普通的插件开发流程

TODO:

- 【已解决】Mac中用iOSOpenDev开发iOS的theos的Logos的tweak插件
- 【已解决】给iOSOpenDev的Logos的tweak的XCode项目去做基本配置

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-11-08 17:03:23

# 新建iOSOpenDev的Xcode项目

Xcode 中新建 iOS 项目,选择: iOSOpenDev -> Logos Tweak :



然后填写项目信息:

Choose options for your new project:		
Team:	Mao Li	
Product Name	iOSBypassJailbreak	
Company Identifier	com.crifan	
Bundle Identifier	com.crifan.iOSBypassJailbreak	
	Include Simple PreferenceLoader	
Cancel		Previous Next
Barloci		

比如iOSBypassJailbreak的:

- Product Name : iOSBypassJailbreak
- Company Bundle : com.crifan
- Bundle Identifier:自动生成出 com.crifan.iOSBypassJailbreak

点击 Next 继续,即可新建出,看起来和普通 Xcode 没多大区别的项目:

	I iOSBypass Jailbroak	m incourse lailbrack ) 📑 information 1321 incourse lailbrack: Baadu   Today at 21:23 🔟	
	Юзвуразззанотеак		
	器 〈 〉 🛛 iOSBypass	ailbreak.xcodeproj  ₹ □	<b>►</b> ⊘ ⊘
✓ ➡ iOSBypassJailbreak	iOSBypassJailbreak		Identity and Type
✓		General Resource Tags Build Settings Build Phases Build Rules	Name iOSBypassJailbreak
(1) iOSBypassJailbreak.xm	PROJECT	✓ Identity	Location Absolute
	🔣 iOSBypassJailbreak		Full Path /Users/crifan/dev/dev_root/
> Supporting Files	TARGETS		crifan/iOSBypassJailbreak/ iOSBypassJailbreak.xcodepr
> 📰 Frameworks	🟦 iOSBypassJailbreak		oj O
		Choose Info.plist File	Project Document
			Project Format Xcode 13.0-compatible 📀
			Organization
		✓ Deployment Info	Class Prefix
		iOS 13.0 ¢ 🔽 iPhone	Text Settings
		MiPad	Indent Using Spaces
		Show "Designed for iPad" Run Destination on Apple Silicon ()	Widths 4 0 4 0
			Iab Indent
		✓ Frameworks and Libraries	
		Name Filters Embed	
		🚔 Foundation.framework Always Used 💿 🗸 Do Not Embed 🗘	
		✓ Development Assets	
		Add development assets here	
+ 🖘 Filter			

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-11-08 16:05:21

# 初始化配置iOSOpenDev的Xcode项目

## 去掉 Deploymen Info 中的 Mac 和确保iOS版本一致

此处,先去做第一个配置方面的改动:

• TARGETS -> General -> Deploymen Info: 去掉 Mac,因为我们开发的是 ios 的插件,不需要发布到 Mac,且设置好iOS 的最低版本

ο

•

PROJECT -> Info -> Deployment Target -> iOS Deployment Target , 也要同步设置 iOS 的最低版本

0

### 导入依赖库 libsubstrate.dylib

把 libsubstrate.dylib (一般在 /opt/iOSOpenDev/lib/libsubstrate.dylib ):

•••	< > lib 返回/前进			Refre	Sh Finder.app	<b>亡</b> 新建文件夹	Ⅲ \$ 显示	ःः <b>~</b> 群组	○ × 操作	① 共享		Q 搜索
个人收藏 ④ 下载 晉 dev 晉 crifan_self	t > 用程序 > lumes > me >	iOSOpenDev iOSOpenDevUninstal iOSOpenDevSetup iMonkeyDev	>    > > >	<ul> <li>README.md</li> <li>LICENSE</li> <li>frameworks</li> <li>templates</li> </ul>		liba	substrate.dylib actionmenu.dylib activator.dylib		<b>libsubstr</b> Unix可执行 <b>信息</b>	r <b>ate.dyl</b> i 亍文件 - 1	<b>ib</b> 03 КВ	
 ✿ crifan ▲ 应用程序 — mac	pleInternal > 源库 > res > 户 >	<ul> <li>theos</li> <li>metasploit-framewor</li> <li>cisco</li> </ul>	> k > >	iib include bin		ц				 更多	今天 	21:30
阿 隔空投送 iCloud	a mac > 🚞 opt > 🚞 i	OSOpenDev > 🚞 lib > 🦳 libsul	bstrate.dylik		+015) 4540					_		
iOSBypassJa	A $\diamond$ $\phi$ $\Box$ $\Box$	器   く >     m iOSBypas 区 iOSBypassJailbreak	sJailbreak.>	远拜 J T坝 (; (m 🛛 iOSB)	ңз щ) , 154.3 passJailbreak.x	codeoroj						₹   🕀
<ul> <li>iOSBypass</li> <li>iOSBypass</li> <li>iOSBypass</li> </ul>	sJailbreak assJailbreak.xm	PROJECT				d Set ings		Build Rule	) Filter			
> Package	assoandreak.mm e ting Files	iOSBypassJailbreak TARGETS iOSBypass Jailbreak	> Dep > Run	endencies (0 item I Script	;)							
> 🔤 Framewori	KS	<u>т</u> Юзвураззјаногеак	> Con	npile Sources (1 ite	m)							
			Ƴ Lin⊧	k Binary With Libra	ies (1 item)					Stat	us	
				₽ Fo	undation.framev	work 🔸				Req	luired ≎	
			> Hea	+ -			Drag to reorder	linked binar	ies			
			> Run	Script								

导入到项目中的: Targets -> YourProjectName -> Build Phases -> Link Binary With Libraries

	🛃 iOSBypassJailbreak	â iOSBypass	Jailbreak 🔪 📒 iPhone	/_1331	iOSBypassJail	break: <b>Ready</b>   Today at 21:4	13	+
	器   < >     m* iOSBypas	sJailbreak.xm	iOSBypassJailb	reak.xcodeproj				
✓ ➡ iOSBypassJailbreak	🖾 iOSBypassJailbreak							
✓ ■ iOSBypassJailbreak		Gener	al Resource Tags	Build Settings	Build Phases	Build Rules		
m iOSBypassJailbreak.xm	PROJECT					Filter		
iOSBypassJailbreak.mm	🙆 iOSBypassJailbreak	> Dependen	icies (0 items)					
> Supporting Files	TARGETS							
> 📷 Frameworks	🏦 iOSBypassJailbreak	> Run Scrip	t					
		> Compile S	ources (1 item)					
		✓ Link Binar	ry With Libraries (2 ite	ms)				
			Name				Status	
			音 Foundation.	framework			Required 🗘	
			n libsubstrate	dylib			Required 🗘	
					Drag to reorder	linked binaries		
		> Headers (	0 items)					
		> Run Scrip	t					×

# 设置被hook的app包名或二进制文件名

去把要hook的,被拦截的app的包名,加到被hook的包名的列表中:

```
YourProjectName -> YourProjectName -> Package -> Libarary -> MobileSubstrate -> DynamicLibraries -
```

> CurrentProjectBundleIdentifier.plist

在 Root -> Filter -> Bundles , 会看到 Item 0:

- Type : String
- Value: 填入你要hook的app的包名
  - o 举例

■ com.crifan.ShowSystemInfo

	🙆 iOSBypassJai 🏦 iOSBypassJail	break 🔪 📋 iPhone7_1331	iOSBypassJailbreak: <b>Ready</b>   Today at 21:45		
■ 🛛 ☶ ♀ & � & ☞ 🗆 🗏	器   く >     m" iOSBypassJailbreak.xm	liOSBypassJailbreak.plist			
∽ 🚨 iOSBypassJailbreak	🚨 iOSBypassJailbreak $ angle \equiv$ iOSBreak $ angle \equiv$	Package $ angle$ 🔚 Library $ angle$ 🔚 Mobit	rate $ angle \equiv$ Dynraries $ angle \boxplus$ iOSBypassJailbreak	plist $ angle$ No Selection	Identity and Type
iOSBypassJailbreak	Кеу	Туре	Value		Name iOSBypassJailbreak.plist
m iOSBypassJailbreak.xm	√ Root	Dictionary	(1 item)		Type Default - Property List XML 🕃
m iOSBypassJailbreak.mm	✓ Filter	Dictionary	(1 item)		Location Relative to Group
🗸 🚞 Package	✓ Bundles	Array	(1 item)		iOSBypassJailbreak.plist 🛛 🚞
> 🚞 DEBIAN		O Suing O	com.cman.snowsysteminio		Full Path /Users/crifan/dev/dev_root/
🗸 🚞 Library					iOSBypassJailbreak/
MobileSubstrate					Package/Library/ MobileSubstrate/
🗸 🚞 DynamicLibraries					DynamicLibraries/
					iOSBypassJailbreak.plist 🛛 🕥
> 🚞 Supporting Files					On Demand Resource Tags
> 🚍 Frameworks					
					Aud to a target to enable tagging
					Localization
					Localiza
					Localize
					Target Membership
					🔲 🏛 iOSBypassJailbreak
+ 🐨 Filter					

- 另外
  - 。 如果要新增一行
    - 移动到 Item 0 所在的行,会看到出现个 = m号 , 点击 m号 , 会新增一行

#### 如何hook二进制?

如果需要hook二进制,则是新建 Array 类型的(和 Bundles 并列的) Executables 子项,再加上对应的二进制文件名 举例:

• hook二进制: akd = AuthKit.framework 的daemon进程

o

此时,对应的 plist 文件内容是:

• jailAppleAccount/Package/Library/MobileSubstrate/DynamicLibraries/jailAppleAccount.plist

```
<?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">
  <key>Filter</key>
  <dict>
   <key>Executables</key>
    <array>
     <string>akd</string>
     <string>amsaccountsd</string>
     <string>AppleMediaServices</string>
     <string>AppleAccount</string>
     <string>Preferences</string>
    </array>
    <key>Bundles</key>
    <array>
     <string>com.apple.Preferences</string>
    </array>
 </dict>
</dict>
</plist>
```

## 更新iOSOpenDev相关设置

### 设置iPhone的IP

把此处要把iOS调试设备(iPhone)中的IP地址:

🖬 中国电信 🗢	15:21	
<b>く</b> 无线局域网	crifan_wifi	
忽略此网络		
自动加入		
低数据模式	hiPhone上的App减	小网络数据
的使用。 IPV4地址		
配置IP		自动 >
IP地址		192.168.1.27
子网掩码		255.255.255.0
路由器		192.168.1.1

续租

此处是: 192.168.1.27

去加到配置中去:

• iOSOpenDevDevice = 192.168.1.27

	iOSBypassJailbreak main	🏦 iOSBypassJailbreak 🔪 🚦 iPhone7_1331	Build Succeeded   2022/11/4 at 22:54 💧 43	+	
	🔠 I < > 🔣 iOSBypas	ssJailbreak.xcodeproj			
	IOSBypassJailbreak			< 🛆 >	Identity and Type
	n	General Resource Tags Build Settings	Ruild Phases Ruild Rules		Name iOSBypassJailbreak
					Location Absolute
Framoworke	PROJECT	Basic Customized All Combined Levels +			Location Absolute
	🔼 iOSBypassJailbreak	Violation of 'self = [super init]' Rule	Yes ≎		Full Path /Users/crifan/dev/dev_root/crifan/
	TARGETS	Violation of Reference Counting Rules	Yes ≎		iOSBypassJailbreak/ iOSBypassJailbreak.xcodeproj 💿
	iOSBypassJailbreak	Static Analysis - Issues - Security			
		Setting	m iOSBvoassJailbreak		Project Document
		Floating Point Value Used as Loop Counter	No ô		Project Format Xcode 13.0-compatible
		Misuse of Keychain Services API	Yes 0		Organization
		Unchecked Return Values	Yes ≎		Class Prefix
		Use of 'getpw', 'gets' (Buffer Overflow)	Yes ≎		
		Use of 'mktemp' or Predictable 'mktemps'	Yes ≎		Text Settings
		Use of 'rand' Functions	No 0		Indept Lision Concer
		Use of 'strcpy' and 'strcat'	No ≎		indent osing opaces
		Use of 'vfork'	Yes ≎		Widths 4 0 4 0
					Viran lines
		V Static Analysis - Issues - Unused Code			
			🏛 iOSBypassJailbreak		
		Dead Stores	Yes ≎		
		Redundant Expressions	No ≎		
		Redundant Nested 'if' Conditions	No ≎		
		✓ User-Defined			
			🏛 iOSBypassJailbreak		
		iOSOpenDevBuildPackageOnAnyBuild	NO		
		iOSOpenDevCopyOnBuild	NO		
		> iOSOpenDevDevice	192.168.1.27		
		iOSOpenDevInstallOnAnyBuild	NO		
		iOSOpenDevInstallOnProfiling	YES		
		iOSOpenDevPath	/opt/iOSOpenDev		
		iOSOpenDevRespringOnInstall	YES		
	+ - Griter	iOSOpenDevUsePackageVersionPList	YES		
+ 🖘 Filter 🕐 단					

### 更新iOSOpenDevUsePackageVersionPList为NO,确保版本更新能生效

以及参考后续的:

control的Version版本号的改动会丢失

再去从:

• iOSOpenDevUsePackageVersionPList = YES

改为:

• iOSOpenDevUsePackageVersionPList = NO

#### 更新后的配置是:

iOSOpenDevBuildPackageOnAnyBuild NO iOSOpenDevCopyOnBuild NO iOSOpenDevDevice 192.168.1.27 iOSOpenDevInstallOnAnyBuild NO iOSOpenDevInstallOnProfiling YES iOSOpenDevPath /opt/iOSOpenDev iOSOpenDevRespringOnInstall YES iOSOpenDevUsePackageVersionPList NO



另外,理论上,去把对应变量加到环境变量:

```
→ ~ cat ~/.zshrc | grep i0S0penDevDevice
export i0S0penDevDevice=192.168.1.27
```

效果应该也是一样的。

## 确保ssh登录且是ssh免密登录

- 此处要弄好SSH登录,且是ssh免密登录
  - 背景
    - 在 xcode + iOSOpenDev 的编译安装最后阶段,涉及到,自动通过ssh访问iPhone设备,把生成的 .deb 插件的文 件下载和安装到iPhone中
    - 此时就需要先准备好环境:确保 Mac 中可以, ssh的免密登录iPhone
  - o 概述
    - 先用ssh登录一次iPhone
      - ∎ 命令

ssh root@192.168.1.27

- 输入密码
  - OpenSSH 的默认密码是: alpine
- 即可登录到iPhone中
- 把ssh的key拷贝到iPhone中
  - 命令

ssh-copy-id root@192.168.1.27

- 输入密码: alpine
- 详解
  - ssh免密登录 · iOS越狱开发:常用越狱插件

crifan.org,使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-01-15 15:43:08

## 搞懂.xm和.mm文件的逻辑

此处,在真正,新增hook代码文件,写hook代码之前,要去:

搞懂 iOSOpenDev 中 .xm 和 .mm 文件的逻辑

此处核心内容是:

- .xm : 原始的hook插件的代码
- .mm : 从 .xm 自动 (在 Build 后) 自动生成的文件

->

- 所以=结果
  - 。 iOSOpenDev新增(hook代码逻辑的)文件时
    - 是: .xm 文件
    - 不是: .mm 文件
  - 。 写hook插件=添加hook代码逻辑时, 改动的文件
    - 是: .xm 文件
    - 而不是: .mm 文件
  - 你每次改动更新 .xm 后
    - iOSOpenDev内部会自动从最新的 .xm 生成最新的 .mm 文件
      - 因此, 旧的 .mm 文件(的内容) 会被新的 .mm 文件(的内容) 覆盖掉
        - 所以即使,如果,你之前改动了 .mm 文件,也是没用的,会被覆盖掉的
  - Xcode最终去编译(内部其实是iOS的 clang 编译器)时
    - 不支持: .xm
      - 万一 xcode 的 Compile Sources 中(由于失误而)加入了 .xm 文件,则会导致编译报错
        - 具体详见: Compile Sources中误添加了不支持的.xm
    - 只支持: .mm
      - 所以接下来,要去把 .mm 加到 compile Souces ,供Xcode最终编译用
  - o 首次 ( xcode -> Build ) 编译时, 会从 .xm , 生成额外的 .mm 文件
    - 首次时=只用做一次
      - 概述
        - 需要你去 xcode ->右键-> Add Files to
        - 去把 .mm 文件加进来(导入进来,弹框选项记得选择: Copy items if needed
        - 此时, 对应的 xcode -> Targets -> Build Phases -> Compile Sources 中, 就可以看到对应的 .mm 文件 了
      - 详见
        - 如何新增xm文件
    - 注
      - 后续则无需重复添加 .mm 文件

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 11:33:14

# 如何新增( .xm 和 .mm )文件

对于想要新增hook代码逻辑, 而去新增 .xm 文件的相关逻辑是:

#### 具体步骤是:

- 新建 .xm 文件
  - xcode ->选中要新增文件所属的位置 -> 右键 -> New File -> iOS -> Other -> Empty ->输入文件 名: yourFilename.xm -> Create



ios macOs	watchos tvos briverk			Filter
Other				
	S	FILELIST	CLIPS	CONFIG
Empty	Assembly File	Build Phase File List	CLIPS File	Configuration Settings File
exp	- and - new USC/SD20207 The one-	pch		STOREKIT
Exports File	Markdown File	PCH File	Shell Script	StoreKit Configuration File
P				
TESTPLAN				
Test Plan				
Cancel Favorites		Save As: yourFilename.	Prev	ious Next
Cancel Favorites Downloads dev crifan_self Applications	< > ∷≡ ✓ Previous 7 Da	Save As: yourFilename.: Tags:	Prev xm vHookTempl 📀 🖍	ious Next
Cancel Favorites Downloads dev crifan_self Applications iCloud	< > ∷≡ ↓ Previous 7 Da	Save As: yourFilename. Tags: Image: I	Prev xm vHookTempI ② へ Date Added 前天 16:48	ious Next ) Q Search ~ Date Modifi 前天 16:51
Cancel Favorites Downloads dev crifan_self Applications iCloud iCloud Drive	<>i i v Previous 7 Da hook_native hook_native	Save As: yourFilename.: Tags: Image: Image: JosopenDe ioSOpenDe iys e_misc.mm e_misc.xm	Prev xm vHookTempI ② へ Date Added 前天 16:48 前天 16:32	ious Next Q Search ~ Date Modifi 前天 16:51 前天 16:51
Cancel Favorites Downloads dev crifan_self Applications iCloud iCloud Drive Documents	✓ > := ▼ Previous 7 Da ⇒ hook_native ⇒ hook_native ⇒ hook_iOS_C	Save As: yourFilename. Tags: Tags: iOSOpenDe ys e_misc.mm e_misc.xm DbjC_specific.mm DbjC_specific.mm	Prev xm vHookTempl ② へ Date Added 前天 16:48 前天 16:32 前天 15:31 前天 15:31	ious Next Q Search V Date Modifi 前天 16:51 前天 16:51
Cancel Favorites Downloads dev crifan_self Applications iCloud Cicloud Drive Documents Documents Desktop	Image: Second state       Previous 7 Da       Image: Second state	Save As: yourFilename Tags: Tags: Tags: iOSOpenDe ys e_misc.mm e_misc.xm DbjC_specific.mm DbjC_specific.xm DbjC_commonClass.mm	Prev xm vHookTempl ⑦ へ Date Added 前天 16:48 前天 16:32 前天 15:31 前天 15:30 前天 15:29	ious Next Q Search
Cancel Favorites Downloads dev crifan_self Applications iCloud iCloud Drive Documents Desktop Shared	Image: Second state     Image: Second state       Previous 7 Da       Image: Second state	Save As: yourFilename. Tags: Tags: iOSOpenDe ys a_misc.mm a_misc.xm ObjC_specific.mm ObjC_CommonClass.mm ObjC_CommonClass.xm	Prev           xm         〇           vHookTempl         〇         ヘ           Date Added         前天 16:48         前天 16:32         南天 15:31           前天 15:30         前天 15:29         前天 15:28         一	ious Next Q Search
Cancel Favorites Downloads Circlan_self Applications Cloud Circloud Drive Documents Desktop Circlans Shared Tags	Image: Second state     Image: Second state       Previous 7 Date       Image: Second state	Save As: yourFilename. Tags: Tags: iOSOpenDe ys a_misc.mm a_misc.xm ObjC_specific.mm ObjC_Specific.xm ObjC_CommonClass.mm ObjC_CommonClass.xm Group	Prev           xm            vHookTempl         〇           Date Added         前天 16:48           前天 16:32         前天 16:32           前天 15:31         前天 15:30           前天 15:29         前天 15:28	ious Next Q Search
Cancel         Favorites         ③ Downloads         급 dev         급 crifan_self         ▲ Applications         iCloud         △ iCloud Drive         △ Documents         □ Desktop         급 Shared         Tags         ● 黄色	Image: Second state       Previous 7 Da       Image: Decision state       Image: Decision state <t< td=""><td>Save As: yourFilename.: Tags:</td><td>Prev           xm         ①           vHookTempl         ②           Date Added         前天 16:48           前天 16:32         前天 16:32           前天 15:31         前天 15:29           前天 15:29         前天 15:28</td><td>ious Next Q Search</td></t<>	Save As: yourFilename.: Tags:	Prev           xm         ①           vHookTempl         ②           Date Added         前天 16:48           前天 16:32         前天 16:32           前天 15:31         前天 15:29           前天 15:29         前天 15:28	ious Next Q Search
Cancel         Favorites         ④ Downloads         圖 dev         □ crifan_self         ▲ Applications         iCloud         △ iCloud Drive         卧 Documents         □ Desktop         晉 Shared         Tags         ● 黄色         ● 绿色	Frevious 7 Date Previous 7 Date hook_native hook_native hook_iOS_C hook_iOS_C hook_iOS_C hook_iOS_C hook_iOS_C hook_iOS_C hook_iOS_C	Save As: yourFilename.: Tags: Tags: Tags: iOSOpenDe ys a_misc.mm a_misc.xm DbjC_specific.mm DbjC_specific.xm DbjC_CommonClass.mm DbjC_CommonClass.xm Group Targets I nook_iOS Targets I nook_iOS	Prev         xm         vHookTempl         Date Added         前天 16:48         前天 16:32         前天 15:31         前天 15:29         前天 15:28	ious Next Q Search
Cancel         Pavorites         Downloads         dev         crifan_self         Applications         iCloud         iCloud Drive         Documents         Desktop         Shared         Tags         黄色         绿色         灰色	Frevious 7 Da Previous 7 Da hook_native hook_nos_co hook_iOS_co hook_iOS_co hook_iOS_co hook_iOS_co hook_iOS_co hook_iOS_co	Save As: yourFilename.: Tags: Tags: Tags: iOSOpenDe ys e_misc.xm DbjC_specific.mm DbjC_specific.xm DbjC_CommonClass.mm DbjC_CommonClass.xm Group  hook_iOS Targets  m iOSO	vHookTempl       〇         Date Added       前天 16:48         前天 16:32       前天 16:32         前天 15:31       前天 15:29         前天 15:29       前天 15:28         penDevHookTemplate	ious Next Q Search V Date Modifi 前天 16:51 前天 16:51 前天 16:48 前天 16:48
Cancel         Favorites         ④ Downloads         ☐ dev         ☐ crifan_self         ▲ Applications         iCloud         △ iCloud Drive         ● Documents         ■ Desktop         ● Shared         Tags         ● 黄色         ● 灰色         ● 灰色         ● 紫色	Previous 7 Da Previous 7 Da hook_native hook_iOS_C hook_iOS_C hook_iOS_C hook_iOS_C hook_iOS_C hook_iOS_C	Save As: yourFilename.: Tags: Tags: Tags: Tags: Tags: iOSOpenDe ioSOpe	vHookTempl       〇         Date Added       前天 16:48         前天 16:32       前天 16:32         前天 15:31       前天 15:30         前天 15:29       前天 15:28         penDevHookTemplate	ious Next Q Search
Cancel         Pavorites         Downloads         dev         crifan_self         Applications         iCloud         iCloud Drive         Documents         Desktop         Shared         Tags         黄色         換色         灰色         繁色         繁色         重要	Image: Second	Save As: yourFilename. Tags: Tags: Tags: Tags: iOSOpenDe ys a_misc.mm a_misc.xm DbjC_specific.mm DbjC_specific.xm DbjC_CommonClass.mm DbjC_CommonClass.xm Group hook_iOS Targets $\checkmark$ m iOSO	vHookTempl       〇         Date Added       前天 16:48         前天 16:32       前天 16:32         前天 15:31       前天 15:30         前天 15:29       前天 15:28         penDevHookTemplate	ious Next Q Search V Date Modifi 前天 16:51 前天 16:51 前天 16:51 前天 16:51 前天 16:51 前天 16:42
Cancel         Pavorites         Downloads         dev         crifan_self         Applications         iCloud         iCloud Drive         Documents         Desktop         Shared         Tags         黄色         頻色         繁色         繁色         繁色         重要         藍色	Image: Second state       Previous 7 Da       Previou	Save As: yourFilename.: Tags: Tags: Tags: Tags: Tags: iOSOpenDe ys e_misc.mm bjC_specific.mm bjC_specific.mm bjC_specific.xm bjC_CommonClass.mm bjC_CommonClass.xm Group Targets $?$ $m$ iOSO	Prev xm vHookTempl ③ へ Date Added 前天 16:48 前天 16:32 前天 15:31 前天 15:29 前天 15:28	ious Next Q Search Date Modiff 前天 16:5 <sup>2</sup> 前天 16:5 <sup>2</sup> 前天 16:4 <sup>2</sup> 前天 16:4 <sup>2</sup> ① 〇

- 会从 yourFilename.xm 生成 yourFilename.mm
  - 注:此时Xcode项目中是看不到的,但是文件系统中(比如通过Finder)是可以看到 .mm 文件的
- 把 .mm 文件加到 Compile Sources 中

• 右键-> Add Files to {yourProjectName} -> 选择(刚新生成的) yourFilename.mm

Ś	Xcode	File	Edit	View	Find	Navigate	Editor	Product	Debug	Integrate	Window	Help	
•							P ioso	benDevHoo	kTempla	te			iOS
		D C	A.					< $>$ $>$ $>$ $>$ $>$ $>$ $>$ $>$ $>$ $>$	t 🛛 🗷	iOSOpenDe	e.xcodeproj		🗏 contro
~ 🛃	iOSOpen iOSOp libs libs hool m <sup>*</sup> hool m <sup>*</sup> hool	DevHoo enDevF <_native ook_nat ook_nat <_iOS	okTemp lookTer ive_mis ive_mis	olate mplate sc.xm sc.mm			<pre>iOSOpe 1 /* 2 3 4 5 */ 6 7 st. 8</pre>	File: ho Functior Author:	nplate ) bok_iOS_C 1: hook i Crifan L cing* Las	∎ iOSOpenDe DbjC_Commo iOS ObjC c i stUpdate =	vHookT∈) ■ nClass.xm ommon clas @"2024112	hook_ s rel 3_153	OS) M <sup>*</sup> h ated fun 1";
	mi ha mi ha mi ha mi ha v im Pack v im Di ≣ ≣ v im Lii	pok_iOS pok_iOS pok_iOS pok_iOS cost_iOS cage EBIAN control control	<u>objC</u> <u>objC</u> <u>objC</u> <u>objC</u>	<u>Commo</u> Commo _specific _specific	nClass. nClass. xm mm	xm Sho mm Ope Ope Ope Sho New	w in Finder n in Tab n in New W n with Exte n As w File Insp v File	/indow rnal Editor ector				>	
	~	Mobile	Substra	ate		Add	Files to "i	OSOpenDev	HookTem	plate"			
	$\sim$	🗋 Dyna	amicLib	oraries		Add	Package D	ependencie	es				
		⊞ iO	SOpen	DevHook	Templa	te.pl Dele	ete						1
<ul> <li>Supporting Files</li> <li>Frameworks</li> <li>libsubstrate.dylib</li> <li>Foundation.framework</li> </ul>			New New New	New Group New Group with Folder New Group from Selection						:r);			
						Boo Boo	kmark "ho kmark "ho	ok_iOS_Obj ok_iOS_Obj	C_Commo C_Commo	onClass.xm" onClass.xm"	Line 384		
						Sort	by Name by Type						
						Find	in Selecte	d Groups					
						Sou	rce Contro					>	:_apple] 'oString
						Mig	ate to Stri	ng Catalog					
						Proj	ect Naviga	tor Help					

■ 其中勾选: Copy items if needed

	P main	ic ic	)SOpenDevHookTemplate > J <sup>a</sup> Any IOS Device (arm64)	Build Succeeded   2024/11/23 at 16:51 🔒 11 👘
🗎 🛛 🔍 🔍 🖉 🗖				
v 🔝 iOSOpenDevHookTemplate	IOSOpenDevHo	okTemplate ) 🚞 IOSOpenDevHookTemplate ) 🚞 hook_IO	S ) M hook_IOS_ObjC_CommonClass.xm ) No Selection	
<ul> <li>iOSOpenDevHookTemplate</li> <li>iibs</li> </ul>	Favorites Downloads		iOSOpenDevHookTempI	Q. Search
<ul> <li>hook_native_mise.xmi</li> <li>hook_native_mise.xmi</li> <li>hook_05_ObleC_Commodeling</li> <li>hook_05_ObleC_commodeling</li> <li>hook_05_ObleC_specificam</li> <li>hook_05_ObleC_specificam</li> <li>hook_05_ObleC_specificam</li> <li>control</li> <li>Library</li> <li>Library</li> <li>UsOpenDevidonTerris</li> <li>Supporting Files</li> <li>Frameworks</li> <li>Busubstrate dytls</li> <li>Foundation.framework</li> </ul>	<ul> <li>dev</li> <li>dev</li> <li>dev</li> <li>dev</li> <li>dev</li> <li>Applications</li> <li>Applications</li> <li>Recents</li> <li>Cloud Drive</li> <li>Documents</li> <li>Desktop</li> <li>Shared</li> <li>Tras</li> <li>Ke</li> <li>Ke</li> <li>Ke</li> <li>Al Tags</li> <li>Matic</li> <li>Photos</li> <li>Movies</li> </ul>	Previous 7 Days         Import_050_010_50_mmClass.mmI         Import_050_0_mmClass.mmI         Import_050_0_mmClass.mmI         Import_050_0_mmClass.mmI         Import_050_0_mmClass.mmI         Import_050_0_mmClass.mmI         Import_050_0_mmClass.mmI         Import_050_mmClass.mmI         Import_050_0_mmClass.mmI         Import_050_0_mm	<pre>rlime 1 "/Uwor/cr(fm/dor/doc_rost/cr(fm/glthd/J000cen 1005pmDeviewStRepLite/J005pendevHeartepLite/HeartepLite/HeartepLite/ static NSStrings LastUpdate = 0"20241123_1331"; #ipport "Cr(fmLit);" #upport "Cr(fmLi</pre>	Devidosit men Late/ IC_CommonClass.sm"
		New Folder Hide Options		Cancel

- 项目文件列表中,即可新增对应文件 yourFilename.mm
- o 项目的待编译的 Compile Sources 文件中,也包含了对应的 .mm 文件
  - Targets -> Build Phase -> Compile Sources 中有了刚加入的 .mm 文件



■ 这样后续编译代码时,才能真正编译到对应hook代码

crifan.org,使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 11:44:25

# 写hook插件代码

```
新建 iOSOpenDev 的项目中的 .xm 文件(此处是 iOSBypassJailbreak.xm )生成的默认代码,来自模板,一般是:
       // Logos by Dustin Howett
      // See http://iphonedevwiki.net/index.php/Logos
      #error iOSOpenDev post-project creation from template requirements (remove these lines after completed) -- \lambda
                 Link to libsubstrate.dylib: \
                 (1) go to TARGETS > Build Phases > Link Binary With Libraries and add /opt/iOSOpenDev/lib/libsubstrate.dylib \
                 (2) remove these lines from ".xm files (not ".mm files as they're automatically generated from ".xm files)
         hook ClassName
              (id)sharedInstance
                    10g
                 return %orig
              (\texttt{void}) \texttt{messageWithNoReturnAndOneArgument}: (\texttt{id}) \texttt{originalArgument} = \texttt{origin
                   10g
                 %orig(originalArgument);
                 // or, for exmaple, you could use a custom value instead of the original argument: %orig(customValue);
               (id)messageWithReturnAndNoArguments
                   10g
                 id originalReturnOfMessage
                                                                                                                  orig
                 // for example, you could modify the original return value before returning it: [SomeOtherClass doSomethingToThisO
      bject:originalReturnOfMessage];
                 return originalReturnOfMessage
         end
```

去删除掉,或注释掉,改为自己的hook的代码。

### 附录

#### demo示例代码

比如此处仅用于演示的代码:



```
#import <UIKit/UIKit.h
//#import <SpringBoard/SpringBoard.h>
// #import <Preferences/Preferences.h>
#import <os/log.h
hook UIDevice
 (NSString )name
    os_log(OS_LOG_DEFAULT, "test hook UIDevice name");
    return @"Tweaked_name";
  (NSString )systemName
    os_log(OS_LOG_DEFAULT, "test hook UIDevice systemName");
   return @"Tweaked_systemName";
  (NSString )systemVersion
    os_log(OS_LOG_DEFAULT, "test hook UIDevice systemVersion");
   return @"Tweaked_systemVersion";
  (NSString *)model
    os_log(OS_LOG_DEFAULT, "test hook UIDevice model");
    return @"Tweaked_model";
end
```

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-01-15 16:05:36

# 调试插件代码

接下来就是典型的插件开发流程了:

- 写代码 = 写hook代码 = 写tweak插件代码 = 改动 .xm 文件
- 编译代码 -》确保语法没错,可以正常编译
  - Xcode -> Product -> Build



- 调试和运行 -》把hook插件代码编译所生成的插件(.deb 文件)安装到iOS设备(iPhone)中,测试插件效果
  - Product -> Build For -> Profiling

gate	Editor	Product Deb	oug Source Contro	ol V	Window H	Help
🛃 iO:	SBypas	Run Test		ີສR ເສບ	lailbreak 〉	iPhone7_133
昭   く		Profile		: ¥ I	Jailbreak.pli	st
🛃 iose	BypassJa	Analvze	$\mathbf{v}$	жв	ailbreak.xm	angle No Selection
35 36	// // re	Archive				
37	//}	Build For		>	Running	ፚ <b></b> ቘR
38	11	Perform Action		>	Testing	ĵ ĉ <mark>ж</mark> ሀ
39 40	//%enc	Build		жв	Profiling	ዕዝበ
41	#1mpoi	Clean Ruild Fol	der 750	90 L		
42	// #in					
44	#impor	Clean Test Res	uits A	. <del>76</del> K		
45		Stop		ж.		
46 47	%hook	Build Documer	tation ^û	r₩D		
48	- (NSS	Chave Duild Fal	dax in Findax			
49 50	1		der in Finder		o name!!)	ю.
50	re	Export Localiza	ations		e name /	La A
52	}	Import Localiza	ations			
53						
54	– (NSS	Scheme		>		
55	{	Destination		>	a avatam	In mall <b>A</b>
57		Tost Plan		,	e systemm	
58	}					
59		Xcode Cloud		>		
60	– (NSS					

## 确认插件安装成功

- iPhone中看到自己的插件
  - o Cydia -> 已安装 -> 最近 能看到自己的插件:

•川中国电信 중 ※ 21:57	
用户 专业人士 最近	
2022年11月4日	
<b>iOSBypassJailbreak</b> 来自 未知 / 本地 (系统)	
2022年10月8日	
Cydia Installer 来自 apt.bingner.com (软件包) graphical iPhone front-end for APT	
2022年6月27日	
<b>ReProvision Reborn</b> 来自 Havoc (Applications) Re-sign applications on your device	
2022年6月24日	
<b>Frida</b> 来自 build.frida.re (开发) Inject JavaScript to explore iOS apps over USB.	
2022年6月14日	
Mask 来自 未知 / 本地 (系统)	
2022年6月10日	
Altl ict Cydia 软件源 变更 已安装	✓

• 点击插件,可以看到插件基本信息



• 点击插件的文件,可以看到文件列表

💷 中国电信 🗢	21:58	(
く详情	已安装文件	
Library		
MobileSubst	rate	
DynamicLi	braries	
iOSBypas	ssJailbreak.dylib	
iOSBypas	ssJailbreak.plist	
,, F	1 13	

## 确认插件的确正常工作

• 打开被测试的=被hook的app,看到此处测试代码:更改信息信息,显示是我们hook代码中的值,表示hook成功

0

- 查看对应log日志
  - Xcode -> Window -> Devices and Simulators -> Devices ->选中 Connected 中自己的iPhone设备-> Open Console ->打 开 Console = 控制台,显示出对应iPhone的log日志
    - 其中就有你的插件的log日志
      - 如果没有,则自己去右上角,搜索对应关键字,即可搜到
    - 此处贴出,后续更新了代码后的相关log

• • •	<b>控制台</b> 36条信息		● ⑤ S₂ ⑧ Ĉ ● ① Q 任— × hook_ 15年 現在 活动 1899 ■新聞入 18个 共常	0 S S S C 0 ₫ Q ₫ hook_						
🗖 licrifan的 Mac	类型 时间	进程	信息							
iPhone7_1331	15:55:44.789584+9899	ShowSystemInfo	hook dyld.xm_loposlocalCtor 85fc37b1: dylib ctor. cfoHookEnable dyld=True							
	15:55:44.700603+0800	ShowSystemInfo	hook dyld.xm getJbDylibImgIdxList: origImageCount=368 → outJbDylibIdxList=0x102430e30. *outJbDylibIdxList=0x201e	48000. ibDvlibIdxList						
· 崩溃报告	15:55:44.700618+0800	ShowSystemInfo	hook_dyld.xm initDylibImageIdxList: g0rigImageCount=368, gJbDylibIdxList=0x281e48000, gJbDylibIdxListLen=0 -> gHc	okedImageCount=368						
Soin 18#	15:55:44.700778+0800	ShowSystemInfo	hook_misc.xm _logosLocalCtor_298f95e1: misc ctor, cfgHookEnable_misc=True							
	15:55:44.700870+0800	ShowSystemInfo	hook_dylib.xm _logosLocalCtor_432aca3a: dylib ctor, cfgHookEnable_dylib=True, cfgHookEnable_dylib_dladdr=True							
日心报告	15:55:44.700890+0800	ShowSystemInfo	hook_syscall.xm _logosLocalCtor_9431c87f: syscall ctor, cfgHookEnable_syscall=True							
* 诊断报告	15:55:44.700906+0800	ShowSystemInfo	hook_writeFile_iOS.xm _logosLocalCtor_0353ab4c: writeFile_iOS ctor, cfgHookEnable_writeFileiOS=False							
Mac分析数据	15:55:44.700939+0800	ShowSystemInfo	hook_openFile_iOS.xm _logosLocalCtor_bf822969: openFile_iOS ctor, cfgHookEnable_openFileiOS=True							
system.log	15:55:44.700956+0800	ShowSystemInfo	hook_openFile_C.xm _logosLocalCtor_605ff764: openFile_C ctor, cfgHookEnable_openFileC=True							
	15:55:44.701021+0800	ShowSystemInfo	hook_init.xm _logosLocalCtor_93db85ed: Init ctor							
	15:55:44.701037+0800	ShowSystemInfo	hook_init.xm _logosLocalCtor_93db85ed: cfgHookEnable=True							
	15:55:44.701052+0800	ShowSystemInfo	hook_init.xm _logosLocalCtor_93db85ed: inited random char							
	15:55:44.701069+0800	ShowSystemInfo	hook_sysctl.xm _logosLocalCtor_03afdbdó: sysctl ctor, cfgHookEnable_sysctl=True, cfgHookEnable_sysctl_sysctl=True							
	15:55:44.701107+0800	ShowSystemInfo	hook_mach0.xm _logosLocalCtor_c24cd76e: Mach-O ctor, cfgHookEnable_macho=True							
	15:55:44.730421+0800	ShowSystemInfo	hook_dyld.xm NSVersionOfLinkTimeLibrary: libraryName=UIKit -> rtLtLibVer=341114981							
	ShowSystemInfo (iOSBypassJaill 子系统: 类别: <缺少描述> 详细信.	oreak.dylib)	202	2-11-08 15:55:44.700584						
	hook_dyld.xm _logosiccalCtor_88fc37b1: dylib ctor, cfgHookEnable_dyld=True									

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-07-20 14:39:40

# 带界面的插件开发流程

TODO:

- 【未解决】用XCode开发iOS的app用于配置改机软件参数
- 【已解决】越狱iPhone中安装deb包后iOS的反越狱插件没生效
- 【已解决】把iOS的app和iOS的tweak插件打包成独立的deb安装包
- 【记录】越狱iPhone中安装iOS的app和tweak合并出的deb安装包
- 【已解决】越狱iOS如何用Theos开发带GUI图形界面的插件
- 【记录】重新给iOSOpenDev的tweak加app打包deb看看app是否有权限写入Preferences目录
- 【已解决】iOS的writeToURL报错: NSCocoaErrorDomain Code 513 You don't have permission to save the file in the folder Preferences
- 【已解决】iOSOpenDev的tweak中读取app保存出的配置文件参数
- 【已解决】iOSOpenDev的XCode编译报错: An empty identity is not valid when signing a binary for the product type Application
- 【已解决】对比研究FakeWeChatLoc和自己的XCode项目的目录结构区别
- 【已解决】给iOS的XCode项目中新增iOSOpenDev的Project Navigator的目录和文件

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-01-06 22:40:32
# 前提和目标

- 前提
  - 。 已实现:基于XCode用iOSOpenDev的Logos Tweak去创建出tweak插件
  - 。已实现:用XCode开发出普通的带UI界面的iOS的app
    - 比如:实现了机型选择的功能
- 目标
  - 。和tweak和app合并成单个deb安装包=单个tweak插件(安装出来后,带UI界面的tweak插件)

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-01-06 22:36:06

# 基本流程

TODO:

- 【已解决】XCode 13.1中Build Settings中Code Signing Identity没有Don't Sign Code选项
- 【已解决】XCode中编译设置参数中如何新增User-Defined自定义参数
- 【已解决】XCode项目中新增iOSOpenDev的Package目录到Target目录中

### 把Xcode中iOS的app项目转换成iOSOpenDev的项目

把普通的XCode项目,去改造成iOSOpenDev的项目:

核心步骤:

只需参考官网教程:

Convert to iOSOpenDev Project · kokoabim/iOSOpenDev Wiki (github.com)

只是有几个细节,需要更新和补充:

#### 最新XCode(13.1)中: Code Signing Identity没有Don't Sign Code选项

解决办法: 给 PROJECT -> Build Settings -> User-Defined ->增加参数:

• CODE\_SIGNING\_ALLOWED=NO

详见:

• 【已解决】XCode 13.1中Build Settings中Code Signing Identity没有Don't Sign Code选项

#### 新版XCode中找不到新建User-Defined参数的入口

```
解决办法: 选择 PROJECT (和或 TARGETS 中的某个 target) -> Build Settings -》最顶部
(和 Basic、 Customized、 All、 Combined 所在的同)一行的最右边有个加号 -》 Add User-Defined Setting
```

详见:

• 【已解决】XCode中编译设置参数中如何新增User-Defined自定义参数

#### 给Target的目录中新建Package

要点: 选中自己项目的 Target 目录-》右键-》 New Group

即可新建组=Group=子目录

详见:

• 【已解决】XCode项目中新增iOSOpenDev的Package目录到Target目录中

### app和tweak之间的通信

对于iOSOpenDev的app,想要和tweak插件之间通信,主要是互相共享配置参数,此处是通过:配置文件

具体做法是:

#### app端

MuJiaBaiHuoApp的ViewController.m

#### 写入配置:

```
- (void) saveConfig:(NSDictionary ) curCfgDict {
    NSLog (@"curCfgDict=%@", curCfgDict);
    NSString curCfgFile = [[NSBundle mainBundle] objectForInfoDictionaryKey:@"MUJIABAIHUO_CONFIG_FILE"];
    NSLog (@"curCfgFile@rde = [NSString stringWithFormat:@"file://%@", curCfgFile];
    NSLog (@"curCfgFile@rde = [NSString stringWithFormat:@"file://%@", curCfgFile];
    NSLog (@"curCfgFile@rde = [NSURL @rde = [NSURL @r
```

#### 到对应的配置文件:

/var/mobile/Library/Preferences/MuJiaBaiHuo.plist

注:

• MUJIABAIHUO\_CONFIG\_FILE 是加的 User-Defined 的参数

0

。 且: 同时加 MUJIABAIHUO\_CONFIG\_FILE=\$(MUJIABAIHUO\_CONFIG\_FILE) 到 info.plist , 才生效

	P MuJiaBaiHuoApp	🔝 MuJiaBail	HuoApp 🔪 📒 iPhone7	Fir				
📁 🖂 🎞 Q 🛆 🗇 🗊 🗆 🗐	🗄 I < 🖂 🗏 🖪 control	🖽 Info.plist 🛛 🛄 REA	DME.md MViewController.m					
✓ ➡ MuJiaBaiHuoApp	🔼 MuJiaBaiHuoApp $ angle \equiv$ MuJia	🔀 MuJiaBaiHuoApp > 🚞 MuJiaBaiHuoApp > 🖽 Info.plist > No Selection						
C README.md	Key	Туре	Value					
🗸 🚞 MuJiaBaiHuoApp	Information Property List		(2 items)					
m main.m	MUJIABAIHUO_CONFIG_FIL	E 🗘 😋 🖨 String 🗧	\$ \$(MUJIABAIHUO_CONFIG_FILE)					
Info plist	> Application Scene Manifest	Dictionary	(2 items)					
V Package								

#### tweak端

MuJiaBaiHuoTweak的MuJiaBaiHuoTweak.xm

```
const NSString CONFIG_FILE = @"/var/mobile/Library/Preferences/MuJiaBaiHuo.plist";

(NSString `)model
{
    os_log(OS_LOG_DEFAULT, "MuJiaBaiHuoTweak hook UIDevice model");
    NSString hookedModel = @"Tweaked_model";
    NSDictionary 'curCfgDict = [[NSDictionary alloc] initWithContentsOfFile:(NSString `)CONFIG_FILE];
    os_log(OS_LOG_DEFAULT, "MuJiaBaiHuoTweak curCfgDict=%{public}@", curCfgDict);
    if (curCfgDict) {
        NSString 'phoneIdStr = [curCfgDict objectForKey:@"phoneId"];
        os_log(OS_LOG_DEFAULT, "MuJiaBaiHuoTweak phoneIdStr=%{public}@", phoneIdStr);
        hookedModel = phoneIdStr;
        os_log(OS_LOG_DEFAULT, "MuJiaBaiHuoTweak hookedModel=%{public}@", hookedModel);
    }
}
```

```
os_log(OS_LOG_DEFAULT, "MujiaBaiHuoTweak return hookedModel=%{public}@", hookedModel);
return hookedModel;
}
```

#### 即可:

#### 从配置文件中

/var/mobile/Library/Preferences/MuJiaBaiHuo.plist

```
读取出之前保存的 NSDictionary, 获取到参数 phoneId 的值。
```

# 把tweak和app合并成单个deb文件

#### 此处把:

- tweak: 的Package包中的Library文件夹
  - 。 去掉DEBIAN目录
    - 中的control
      - 无需tweak的control
- app:的Package的目录中的所有内容
  - Applications
  - DEBIAN
    - control
      - 需要app的control文件

```
合并到一起后的效果:
```

• •	•			control — N	MuJiaBaiHuoDeb
Сh	资源管理器		! control	×	
	<ul> <li>MUJIABAIHUODEB</li> <li>deb/Package</li> <li>Applications/MuJiaBaiHuoApp.app</li> <li>Base.lproj</li> <li>LaunchScreen.storyboardc</li> <li>01J-lp-oVM-view-Ze5-6b-2t3.nib</li> <li>Info.plist</li> <li>UIViewController-01J-lp-oVM.nib</li> <li>Main.storyboardc</li> <li>BYZ-38-t0r-view-8bC-Xf-vdC.nib</li> <li>ChooseTypeVcld.nib</li> <li>fBk-hL-0DN-view-AjQ-Og-Kvs.nib</li> <li>Info.plist</li> <li>UIViewController-BYZ-38-t0r.nib</li> <li>Info.plist</li> <li>MuJiaBaiHuoApp</li> <li>PkgInfo</li> <li>README.md</li> <li>Library/MobileSubstrate/DynamicLibra</li> <li>MuJiaBaiHuoTweak.plist</li> </ul>	ries	deb > Packa 1 Pac 2 Nam 3 Ver 4 Des 5 Sec 6 Dep 7 Con 8 Rep 9 Pri 10 Arc 11 Aut 12 dev 13 Hom 14 Dep 15 Mai 16 Ico 17 18	age > DEBIAN > ! control kage: com.crifan.MuJiaBail he: 沐家百货 sion: 2021.11.04-2 coription: ttion: System hends: firmware (>= 5.0) fflicts: blaces: cority: optional thitecture: iphoneos-arm thor: Crifan : hepage: biction: intainer: in:	НиоАрр
对应的	目录结构:				



Finder中的效果:

• Applications

0

DEBIAN

0

• Library

o

关于目录中的各个文件的详细解释:

- Package : 要打包的根目录
  - Applications

- MuJiaBaiHuoApp.app
  - 拷贝自: iOS的app的XCode项目下的LatestBuild
    - LatestBuild中保存了每次最新编译之后的版本



Replaces: 8

11 Author: Crifan

dev: Homepage: 12 13

Depiction:

Maintainer: Crifan Icon:

14

17 18

1 15 16

м

Priority: optional Architecture: iphoneos-arm

• Library

- MobileSubstrate
  - DynamicLibraries
    - MuJiaBaiHuoTweak.dylib

V DEBIAN

🖻 control

h AppDelegate.h

M AppDelegate.m

h SceneDelegate.h M SceneDelegate.m

h ViewController.h m ViewController.m

🗙 Main.storyboard

h PhoneType.h m PhoneType.m 🔄 Assets.xcassets X LaunchScreen.storyboard

h ChooseTypeTableViewController.h M ChooseTypeTableViewController....

- 拷贝自: iOS的tweak的XCode项目下的LatestBuild
  - LatestBuild中保存了每次最新编译之后的版本



运行脚本去打包出deb

./buildPackage.sh

• log输出举例

```
    → 20220302 pwd
    /Users/crifan/dev/DevRoot/zry/MuJiaBaiHuo/MuJiaBaiHuoDeb/20220302
    → 20220302 ../buildPackage.sh
    dpkg-deb: 正在 'MuJiaBaiHuo.deb' 中构建软件包 'com.crifan.mujiabaihuoapp'.
```

即可得到deb插件安装包: MuJiaBaiHuo.deb



注:

• 如何安装

。 通过 Filza 或命令行 dpkg (命令是 dpkg -i filename.deb )去安装deb文件,即可安装到iPhone中。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-01-06 23:01:29

# 使用效果

# 插件安装后的效果

Cydia中可以看到安装后的插件:



其中详情中, 点击 文件系统内容, 可以看到包含的详细内容:



其中就有 Applications 和 Library

## 插件的使用效果

iOS的app部分:

桌面上的Logo=iOS的app的图标:



点击启动后,显示主界面:

■□中国移动 

・□ 中国移动 

・

下午10:57

选择机型 当前所选机型

点击 选择机型,出现:机型列表

🖬 中国移动 🗢	下午	10:57	
iPhone 6			
iPhone7,2			
iPhone 6 Pl	us		
iPhone7,1			
iPhone 6s			
iPhone8,1			
iPhone 6s P	lus		
iPhone8,2			
iPhone SE -	一代		
iPhone8,4	(9)(7)		
iPhone 7			
iPhone9.1			
iPhone 7 美	版		
iPhone9,3			
iPhone 7 Plu	us		
iPhone9,2			
iDhono 7 Dl	16 羊垢		
iPhone9.4	us 天似		
ii nonee,4			
iPhone 8			
iPhone10,1			
iPhone 8 美	版		
iPhone10,4			

去选择一个: iPhone 6(iPhone7,2)

选择机型

**■**目中国移动 **奈**下午6:39 🛛 🚱

iPhone 6 (iPhone7,2)

然后回去打开,被hook的普通的iOS的app: showSysInfo 可以检测当前机型,是我们所hook选择的机型:

내 中国移动 🗢	下午6:42	
v20	211026_2139	
获取name	name	
获取 systemName	systemName	
获取systemVersion	systemVersion	
获取model	iPhone7,2	
获取 sysctl	hw.machine	
	generation	
	variant	
	A number	
获取IDFV	identifierForVendor	
获取运营商信息	allowsVOIP	
	carrierName	
	isoCountryCode	
	mobileCountryCode	
	mobileNetworkCode	1
获取状态栏 运营商	serviceString	

-》说明上述的:tweak插件,iOS的app(用于配合插件做配置),是生效的。

注:

对应保存到了配置文件中的内容是:

phoneId=iPhone7,2

내 中国移动 🗢	下午6:49	
完成	MuJiaBaiHuo.plist	存储
▼ Root	Dic	tionary[1] (i)
phoneId	i	Phone7,2 (i)

-》至此,跑通了:

- 带UI界面的tweak插件=单个deb文件,集成了包含了
  - ∘ app
    - 实现用户UI界面
    - 选择配置,保存配置到配置文件 /var/mobile/Library/Preferences/MuJiaBaiHuo.plist
  - tweak
    - 实现hook功能
    - 返回的值,根据配置文件中保存的值决定

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-07-19 15:34:12

# 常见问题

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-10-25 19:30:01

# 安装器遇到了一个错误,导致安装失败

安装到最后,报错: 安装失败 安装器遇到了一个错误,导致安装失败



#### 解决办法:

其实此时 iOSOpenDev 的主体文件已安装到了默认的位置 /opt 中, 接着去用工具初始化即可解决问题:

cd /opt/iOSOpenDevSetup/bin sudo ./iod-setup base sudo ./iod-setup sdk -sdk iphoneos

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:32:42

# PrivateFramework directory not found XCode iPhoneOS15.0.sdk

iod-setup sdk -sdk iphoneos 时报错:

```
→ bin sudo ./iod-setup sdk -sdk iphoneos
Setting up iPhoneOS 15.0 SDK...
Modifying SDK settings...
Symlinking to private frameworks header files...
PrivateFramework directory not found: /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Develope
r/SDKs/iPhoneOS15.0.sdk/System/Library/PrivateFrameworks
```

原因:

此处是比较新的 xCode 13 和对应的 iOS 15

->而最新版XCode和iOS早已将私有库PrivateFrameworks移走了

->即 iPhoneOSxx.xx.sdk/System/Library/ 下面没有 PrivateFrameworks 了

解决办法:

- 自己之后是否用到私有库PrivateFrameworks
  - **。**否
    - 直接新建一个空目录即可

ad /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/iPhoneOS15.0.s
dk/System/Library
sudo mkdir PrivateFrameworks

**。**是

- 除了新建目录外,还要把相关iPhoneOS版本的私有库的内容放过去
  - 先要找到相关iPhoneOS的PrivateFrameworks
    - 举例
      - iPhoneOS 9.2 的 sdk ,可以从这里下载到:

 zhangkn/knPrivateFrameworks: /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDK s/iPhoneOS9.2.sdk/System/Library/PrivateFrameworks (github.com)

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:32:47

### File not found XCode Specifications iPhoneOSPackageTypes.xcspec

iod-setup sdk -sdk iphoneos 报错:

→ bin sudo ./iod-setup sdk -sdk iphoneos
Password:
Setting up iPhoneOS 15.0 SDK...
Modifying SDK settings...
Symlinking to private frameworks header files...
Adding specifications to platform...
File not found: /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/Library/Xcode/Specif
ications/iPhoneOSPackageTypes.xcspec

原因:

找不到specifications

解决办法:

下载别人给的:

- 4个iPhoneOS的spec文件
- 4个iPhoneSimulator的spec文件

分别放到对应位置,即可。

下载来源:

- 来源1:
  - iosopendev专用Specifications.zip
- 来源2:
  - 越狱开发:用iosOpenDev配置越狱开发环境 编写第一个hello world\_我的杯洗具的博客-CSDN博客

下载后,可以看到Specifications中有8个spec。

分别新建Specifications目录:

```
sudo mkdir /Applications/Xcode.app/Contents/Developer/Platforms/iPhone0S.platform/Developer/Library/Xcode/Specificati
ons
sudo mkdir /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/Library/Xcode/Spec
ifications
```

再去

- 移动文件
  - **。**把
    - 4个 iPhoneOS 的文件
      - iPhoneOSPackageTypes.xcspec
      - iPhoneOSPackageTypes.xcspec.iOSOpenDev
      - iPhoneOSProductTypes.xcspec
      - iPhoneOSProductTypes.xcspec.iOSOpenDev
    - 放到:
      - /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/Library/Xcode/Spe cifications

**。**把:

- 4个 iPhoneSimulator 的文件
  - iPhone Simulator PackageTypes.xcspec
  - iPhone Simulator PackageTypes.xcspec.iOSOpenDev

- iPhone Simulator ProductTypes.xcspec
- iPhone Simulator ProductTypes.xcspec.iOSOpenDev
- 放到:
  - /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/Library/Xcod e/Specifications

#### 放好后是:

```
→ Xcode ll /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/Library/Xcode/Specificat
ions
total 48
-rwxr-xr-x@ 1 crifan wheel
                             3.2K 12 24 2015 iPhoneOSPackageTypes.xcspec
-rwxr-xr-x@ 1 crifan wheel
                             5.4K 12 24 2015 iPhoneOSPackageTypes.xcspec.iOSOpenDev
                            4.0K 12 24 2015 iPhoneOSProductTypes.xcspec
-rwxr-xr-x@ 1 crifan wheel
-rwxr-xr-x@ 1 crifan wheel
                            6.4K 12 24 2015 iPhoneOSProductTypes.xcspec.iOSOpenDev
→ Xcode ll /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/Library/Xcode/Spe
cifications
total 4
-rwxr-xr-x@ 1 crifan wheel 3.4K 12 24 2015 iPhone Simulator PackageTypes.xcspec
-rwxr-xr-x@ 1 crifan wheel 6.9K 12 24 2015 iPhone Simulator PackageTypes.xcspec.iOSOpenDev
-rwxr-xr-x@ 1 crifan wheel
                             3.4K 12 24 2015 iPhone Simulator ProductTypes.xcspec
-rwxr-xr-x@ 1 crifan wheel 6.1K 12 24 2015 iPhone Simulator ProductTypes.xcspec.iOSOpenDev
```

#### 另外,新建usr的bin目录:

sudo mkdir /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/usr/bin

#### 即可。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:28:54

## .xm 被识别为Audio音频文件

- 问题: iOSOpenDev 的 xcode 中, 默认的 .xm 被识别成音频文件, 无法显示对应的源代码
  - 。<br/>具体现象
    - xm的文件的图标是 小喇叭
    - 且右边显示的是: 音乐的图标
    - 右边文件类型Type显示是: Default XM audio file
  - o 图



- 解决办法:
  - 先去:改变.xm的文件类型
    - Xcode右边的文件属性-> Type , 从 Default XM audio file 改为 Objective-C++ Source (或 Objective-C Source )



- 再去改变 .xm 的文件的打开方式
  - Xcode左边文件列表->右键 .xm 文件-> Open As -> Source Code



● 即可正常显示 .xm 为ObjC的代码,并且带语法高亮了,且文件图标是 .m 的图标



• .xm 文件, 默认会被 xcode 识别为 音频文件

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 11:50:08

# Expected unqualified-id

此错误,有2种情况=可能性:

- 无法识别的特殊字符
- Compile Sources 不支持.xm作为源码去编译

```
下面分别详细解释:
```

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 10:48:58

# 无法识别的特殊字符

# 现象

iOSOpenDev的 .xm 文件编译报错:

Expected unqualified-id



### 原因

此处(由于之前某些操作,比如从别处复制粘贴过来一些内容,而导致的).xm 源码中,有,此处不支持的,特殊的,控制 字符

此处Xcode源码编译器中:无法看到此(不可见的)特殊字符

可以换用VSCode去打开查看到,特殊的,控制字符:

NSXPCConnection
%hook NSXPCConnection
- (void)resume{
<pre>NSLog(@"jailAuthKitAkd NSXPCConnection resume");</pre>
····%orig;
- (void)activate{
<pre>NSLog(@"jailAuthKitAkd NSXPCConnection activate");</pre>
····%orig;
*en0
//(id)initWithListanarEndnaint+(NEVDCListanarEndnaint+)andnaint5
//- (1)/ii(mathiistenerindpoint.(NSArtiistenerindpoint)*/endpoint?
//···Id newcome - soiray, //···Id newCome - soiray,
// return new Cont
//(id)initWithMachServiceName:(NSString-*)name-options:(NSXPCConnectionOptions)options{
//···id newConn = %orig;
//NSLog(@"jailAuthKitAkd-NSXPCConnection-name=%@,options=%lu->-newConn=%@", name, (unsigned-long)options, newConn);
//return-newConn;
//}
//(id)initWithServiceName:(NSString-*)serviceName{
// ··· id newConn = %orig;
// ··· NSLog(@"jailAuthKitAkd NSXPCConnection serviceName=%@ -> newConn=%@", serviceName, newConn);
//····return-newConn;

放大显示效果,可以看到此处特殊字符=控制字符=不可见字符,是: SOH == Start of Header == 标题开始

C Unti	tled-5 ♀	h	AKAnisette
25	//}		
26			
27	//- (id)	init	WithMachS
28	//···id	new	/Conn ·= ·%o
29	// · · · NS	Log (	@"jailAut
30	// re	turn	newConn;
31	//}		
32			
33	//- (id)	init	WithServi
34	// id	new	/Conn ·= ·%o
35	// NS	Log (	@"jailAut
36	// re	turn	• newConn;
37	//}		
38			
39	SOH		

• 注:

• 关于特殊的、不可见的、控制字符的细节,详见:字符编码详解

### 解决办法

(借助于VSCode,在能看到)此特殊的不可见的控制字符(的前提下),去删除掉

### 具体步骤

复制Xcode中的代码,粘贴到VSCode中

然后: VSCode-》查看-》外观-》显示控制字符-》找到对应不支持的特殊的控制字符,去删除即可

🗯 Coo	e 文件	编辑	选择	查看	转到	运行	终端	窗口	帮助	6							
• • •				命令面 打开视	듒… !图…					$\leftarrow$						, <b>◯</b> iOS_:	syste
ſŊ		搜索		外观 编辑器 资源管	術局 理器	<b>&gt;</b> ን ዕже	全) 禅 居	屏 模式 [ #   中布局	K Z]			Untit	led-5	ਸ਼੍	h	AKAnise	etteF
Q	>	_N ect	SXF t	搜索 源代码 运行 扩展	管理		<ul> <li>✓ 主( 辅)</li> <li>✓ ボ)</li> <li>✓ 活)</li> </ul>	側边栏 助侧边栏 态栏 动栏	ŧ			25 26	//}	(			h C a
وم		未抄	2到约	问题 输出 调试控 终端	制台		面前和	板 右移动主 板位置 齐面板	Ξ侧栏		L 36 < <	27 28 29	//- ( // //	(1a) id NS	new Log(	vConn = (@"jailA	nse %or: uthl
ک م		置扫 文件	₽除, ⊧-打	自动换 粘滞滚	行 [动		✓ 缩 ✓ 痕) ✓ 显)	略图 迹导航 示空格				30 31	//••• //}	• re	turr	n∙newCon	n;
å>							✓ 显; 放; 缩/ 重	示控制字 大 小 置缩放[]	≌符 ¥Numi	Pad0]		32 33	//	(id)	init	WithSer	vic °or
												94 35 36	// // //	NS re	Log( turr	(@"jailA newCon	uthl
												37 38 39	//}				
												40 41					

注:

• 关于VSCode支持显示不可见的控制字符,详见:代码编辑器常用功能·史上最好用的编辑器: VSCode

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 10:48:16

### Compile Sources 中误添加了不支持的 .xm

#### 现象

iOSOpenDev中,新增.xm 文件后,尝试去编译

结果代码:

%hookf(char \*, getenv, const char\* name){

其中的 %hookf ,编译报错:

Expected unqualified-id



#### 原因

#### 直接原因

iOS的clang编译器无法识别(Logos的)语法:%hookf

#### 根本原因

之前新增.xm 文件时,无意间,不知道是哪里不小心, (把)导致了.xm ,被加到了Xcode (+iOSOpenDev)中的 compile sources 中了

而此处,iOSOpenDev的最终的所支持的代码逻辑对应的源代码文件的格式:

- 不支持: .xm
- 只支持: .mm

#### 而此处,背后的 .xm 和 .mm 的逻辑,详见:

.xm和.mm文件的逻辑

### 解决办法

- 1. 去 Compile Sources 中, 把 .xm 文件移除掉
- 2. Xcode重新编译 Build
  - 目的:从.xm 中编译生成对应的.mm 文件
- 3. 再去把新生成的 .mm 文件, 加到 Compile Sources 中, 即可正常编译

#### 具体步骤

Xcode -> Targets -> Build Phases -> Compile Sources

如果有 .xm 文件:则(点击) 去删除掉

再去 Xcode -> Build :

对于新增的 .xm 文件,则会生成新的对应的 .mm 文件

然后再去:

xcode ->项目主目录->右键-> Add Files to ... -> 选择新生成的对应的 .mm 文件,且勾选: Copy items if needed -> Add , 即可把 .mm 加到项目中

最后: Xcode -> Targets -> Build Phases -> Compile Sources

#### 只保留正常的 .mm 文件(和其他的 .c 、 .m 等文件):



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 11:22:31

## Host key verification failed

```
• 现象:
```

Xcode编译期间报错:

Preparing to run Xcode Build Phase ... Signing /Users/crifan/Library/Developer/Xcode/DerivedData/iOSBypassJailbreak-bfqgivvncccwmeaykhtbtvgylkkq/Build/Produ cts/Release-iphoneos/iOSBypassJailbreak.dylib with ldid ... Done.  $\label{eq:copying state} Copying \ /Users/crifan/Library/Developer/Xcode/DerivedData/i0SBypassJailbreak-bfqgivvncccwmeaykhtbtvgylkkq/Build/Produ \ (Copying \ /Users/crifan/Library/Developer/Xcode/Der$ cts/Release-iphoneos/iOSBypassJailbreak.dylib to package directory at /Users/crifan/dev/dev\_root/crifan/iOSBypassJail break/iOSBypassJailbreak/Package/Library/MobileSubstrate/DynamicLibraries... Preparing to build package Setting control file /Users/crifan/dev/dev\_root/crifan/iOSBypassJailbreak/iOSBypassJailbreak/Package/DEBIAN/control V ersion field to 1.0-1 using /Users/crifan/dev/dev\_root/crifan/iOSBypassJailbreak/iOSBypassJailbreak/PackageVersion.pl ist ... Done. Building package ... Done.  $\label{eq:creating_zip_loss} Creating\_zip\_loss_creating\_zip\_zip\_loss_creating\_zip\_$ os-arm.zip ... Done. Host key verification failed. Failed to create directory /var/root/iOSOpenDevPackages on device 192.168.1.27 Command PhaseScriptExecution failed with a nonzero <u>exit</u> code

- 原因:没有ssh免密登录
- 解决办法:设置好ssh免密登录
- 具体步骤概述
  - 1. 先

ssh root@192.168.1.27

```
■ 默认密码: alpine
```

2. 再

ssh-copy-id root@192.168.1.27

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:31:22

### scp: dest open ""/var/root/iOSOpenDevPackages/xxx.deb"": No such file or directory

#### 现象

• Mac M2 Max中,用iOSOpenDev去编译deb插件到iPhone8,结果报错:

0

Creating zip /Users/crifan/dev/dev\_root/iosReverse/AppleStore/dynamicDebug/iOSOpenDev/jailAppleAccount/Packages/com.crifan.jailAppleAccount\_1.7.4\_iphoneos-arm.zip... Done.

scp: dest open ""/var/root/iOSOpenDevPackages/com.crifan.jailAppleAccount\_1.7.4\_iphoneos-arm.deb"": No such file or d
irectory

scp: failed to upload file /Users/crifan/dev/dev\_root/iosReverse/AppleStore/dynamicDebug/iOSOpenDev/jailAppleAccount/
Packages/com.crifan.jailAppleAccount\_1.7.4\_iphoneos-arm.deb to "/var/root/iOSOpenDevPackages/com.crifan.jailAppleAcco
unt\_1.7.4\_iphoneos-arm.deb"

Failed to copy file /Users/crifan/dev/dev\_root/iosReverse/AppleStore/dynamicDebug/iOSOpenDev/jailAppleAccount/Package s/com.crifan.jailAppleAccount\_1.7.4\_iphoneos-arm.deb to device 192.168.2.13 at directory /var/root/iOSOpenDevPackages Command PhaseScriptExecution failed with a nonzero <u>exit</u> code

作为对比:

旧的Mac(Intel的Mac),则没遇到这个错误。

对应细节是:

- 旧Mac:正常编译
  - 之前的Xcode版本: v13.2.1
  - о scp: змв
    - FAT格式, 支持 x86\_64 和 arm64e
- 新Mac: 会报错
  - o 错误信息: scp: dest open ""/var/root/iOSOpenDevPackages/xxx.deb"": No such file or directory
  - 。 最新Xcode版本: v14.3
  - SCD: 416KB
    - FAT格式, 支持 x86\_64 和 arm64e

### 原因

iOSOpenDev插件编译后安装deb期间,底层过程是对应脚本控制的

• /opt/iOSOpenDev/bin/iosod

```
其底层负责此处拷贝的命令是:
```

```
function copyFileToDevice() # args: sourceFile, targetDir, hostAddress, hostPort
{
    scp -PShostPort "$sourceFile" root@ShostAddressi"\"$targetFilePath\"" || \
```

而报错的原因,估计是:

新版Mac的CPU是ARM的Apple Silcon,对应的很多二进制,也是arm版本的

对应的scp,估计也是arm版本,其和旧的X86的scp,估计不太一样?

导致对于此处 scp中,带双引号的路径和文件,支持不够好,无法识别,所以报错找不到文件

#### 解决办法

• 去掉scp命令中的(文件和目录中的)双引号

#### 具体步骤

把 /opt/iOSOpenDev/bin/iosod 中的:

scp -P\$hostPort "\$sourceFile" root@shostAddress:"\"\$targetFilePath\"" || \

#### 改为:

scp -P\$hostPort \$sourceFile root@\$hostAddress\_\$targetFilePath || \

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:45:24

## An empty identity is not valid when signing a binary for the product type 'Dynamic Library'

### 现象

M2 Max Mac + Xcode 14.3.1 中, 新建iOSOpenDev项目, 去Build编译, 报错:

An empty identity is not valid when signing a binary for the product type 'Dynamic Library'

#### 拷贝出的详细错误信息:

Build target HookWhatsApp of project HookWhatsApp with configuration Debug error: An empty identity is not valid when signing a binary for the product <u>type</u> 'Dynamic Library'\_ (in target 'HookW hatsApp' from project 'HookWhatsApp')

An empty identity is not valid when signing a binary for the product type 'Dynamic Library'.



#### 原因

- 不是很清楚
  - 。只是大概知道,属于Xcode的自动管理codesign签名方面的问题

### 解决办法

- 思路1: 禁用自动签名
- 思路2:给 identity 设置某个合适的值(这样就不是empty空了)

### 具体步骤

#### 思路1:禁用自动签名

- Xcode -> PROJECT -> {YourProjectName} -> Build Settings -> User-Defined ->
  - (点击左上角的 加号 = → Add User-Defined Setting )

• HookWhatsApp main	$\widehat{\mathbb{m}}$ HookWhatsApp $ angle$	iPhone7_1331		
昱   < >     田 Hook'	WhatsApp.plist M <sup>*</sup> HookWhatsApp.xm	HookWhatsApp.xcod	leproj	
HookWhatsApp				
)		Info	Build Settings Package Dependencie	es
	+ Basic Customized All Co	mbined Levels		
PROJECT	Add Conditional Setting	ith Grand Central Dispatch No	• •	
\Lambda HookWhatsApp	Add Lloor Defined Setting	Number and CFNumberRef Yes	s ≎	
	Add Oser-Defined Setting I libkern	Reference Counting Rules Yes	s ≎	
TADGETS	Violation of Mach Interface G	enerator Conventions Yes	s ≎	
AROLIS				
🛅 HookWhatsApp				
	✓ Static Analysis - Issues - C++			
	Setting		HookWhatsApp	
	Moves of Universal Reference	es Ye	s ≎	
	Use-After-Move Errors in C+	+ Ye	s (Aggressive) ≎	
	<ul> <li>Static Analysis - Issues - Objective-C</li> <li>Setting</li> </ul>		HookWhatsApp	
	@synchronized with nil mute:	X Ye:	S 🗘	
	Improper Instance Cleanup In	realloc re	s ≎	
	Michod Signatures Mismatch		s •	
	Misuse of Objective-C gener	ics fe	s ~	
	Violation of Iself - [super init	l' Pulo Vo	s *	
	Violation of Reference Count	ing Rules Yes	s ≎	
	✓ Static Analysis - Issues - Security	_		
	Setting		HookWhatsApp	
	Floating Point Value Used as	Loop Counter No	• •	
	Misuse of Keychain Services	API Ye	s ≎	
	Unchecked Return Values	Ye	s ≎	
	Use of 'getpw', 'gets' (Buffer	Overflow) Yes	s ≎	
	Use of 'mktemp' or Predictab	ole 'mktemps' Ye	s ≎	
	Use of 'rand' Functions	No	•	
	Use of 'strcpy' and 'strcat'	No	• •	
	Use of 'vfork'	Ye	s ≎	
	v Statia Analysia Jacuas Haussid Ord	•		
	Static Analysis - Issues - Unused Cod	e 	HookWhatsApp	
	Dead Stores	Va	e û	
	Redundant Expressions	Te:	5 V	
	Redundant Nested 'if' Condit	ions No	•	
	✓ User-Defined			
	Setting		HookWhatsApp	
Filter	iOSOpenDevPath	/or	ot/iOSOpenDev	

o 新增选项: CODE\_SIGNING\_ALLOWED = NO

•• •	► P main	▲ HookWhatsApp > IPhone7_1331		Building   27/29 🔾 🔺 6 👛	+	
	3 88 I < > I = ⊞ Hor	xkWhatsApp.plist   M° HookWhatsApp.xm   🏸 Build Hool	kWhatsApp - Log 👘 🖉 Build HookWhatsApp - Log	HookWhatsApp.xcodeproj	₽ 🗉	<b>)</b> (9)
HookWhatsApp	M HookWhatsApp				< 🔺 >	Identity and Type
HopkWhatsApp	0		Info Build Settings Package Dependencies			Name HookWhatsApp
✓  ≡ libs		I Date Controled All Constants Louis		<b>A</b>		Location Absolute
× ≡ ios	PROJECT	+ Basic Customized All Combined Levers	mariled was "	U Piller		
m Heeki esi08 m	A NookWhateAnn	Violation of IOKit and libkern Reference Counting	Rules Yes :			Full Path (Users/crifan/dey/dev_r-
h noverstaloo h	-	Violation of Mach Interface Generator Convention	ns Yes≎			iosReverse/WhatsApp/
n open-selos.n	^					iOSOpenDey WhatsAp
h CritanLibiOS.h	A TARGETS					HookWhatsApp/
h HookLogiOS.h	A ft HookWhatsApp	V Static Analysis - Issues - Caa				HookWhatsApp.xcode
OpenFileiOS.m	A	Settion	HonkWhatsAnn			Project Document
CrifanLibiOS.m	A	Menor of Universal Deferences	Vec 1			riojeot boounient
~ 🎬 c		Lise-After-Move Frons in Cast	Yas (Annacolus) :			Project Format Xcode 14.0-compatib
h CrifanLib.h	^		(in the second sec			Organization
C crifani lib c						Class Prefix
C Heekkingteane ver		and the second second second second				
ni Hookwilatskpp.kiii	2	<ul> <li>Static Analysis - Issues - Objective-C</li> </ul>				Text Settings
III HookWhatsApp.mm	A	Setting	MookWhatsApp			Indent Using Spaces
Package		@synchronized with nil mutex	Yes 0			Widthe d.A
V III DEBIAN		Improper Instance Cleanup in '-dealloc'	Yes D			Tab In
control.txt	A	Method Signatures Mismatch	tes o Vice n			🗹 Wrap lines
control	A	Linused bars	Yes 0			
Library		Violation of 'self = [super init]' Rule	Yes 0			
✓		Violation of Reference Counting Rules	Yes 0			
Dynamici ibrarias						
Heeldthateten pliet						
TookwhatsApp.plist	°	Static Analysis - Issues - Security				
Supporting Files		Setting	A HookWhatsApp			
PackageVersion.plist		Eloating Point Value Lised as Loop Counter	No 2			
h HookWhatsApp-Prefix.pch		Misuse of Keychain Services API	Yes 0			
Frameworks		Unchecked Return Values	Yes 0			
fibsubstrate.dylib		Use of 'getpw', 'gets' (Buffer Overflow)	Yes 0			
C Foundation.framework		Use of 'mktemp' or Predictable 'mktemps'	Yes 0			
		Use of 'rand' Functions	No 0			
		Use of 'stropy' and 'stroat'	No 0			
		Use of "vfork"	Yes ≎			
		Static Analysis - Issues - Unused Code				
		Setting	A HookWhatsApp			
		Dead Stores	Yes 0			
		Redundant Expressions	No 0			
		Redundant Nested 'If' Conditions	No 0			
		V User-Defined				
		Setting	A HookWhatsApp			
		> CODE SIGNING ALLOWED	NO			
	+ - ® Elter	1000 - un Dau Barth	(antii050non Bau			

- 额外说明
  - 如果还不行,多试几次Clean:
    - Xcode -> Product -> Clean Build Folders
    - Xcode -> Product -> Clean All Issues

#### 思路2:给ldentity设置某个合适的值

- Xcode -> TARGETS -> {YourProjectName} -> Build Settings -> Signing
  - 。 设置相关参数值
    - Code Sign Identity 设置为: ( Automatic 中的) Apple Development
    - Development Team 设置为: 你自己的Apple开发者账号 = 此处是: Mao Li
  - o 效果图

 _										
	P iOSOpenDevHookTemplate	e 1	🗈 iOSOpenDevHookTemplate ) 🎤 Any iOS Dev	vice (arm64)	Build Succeeded   2024/11/23 at 16:51					
🖿 🛛 🗋 🔍 🗛 🖉 🖉 🗖	⊞ I < > I ⊞ iOSOpenDevTe	emplate.plist	IOSOpenDevHoplate.xcodeproj	control m <sup>*</sup> hook_iOS_C	bjmmonClass.xm m* hook_iOSspecific					
✓  → iOSOpenDevHookTemplate	iOSOpenDevHookTemplate									
iOSOpenDevHookTemplate	General Resource Tags Build Settings Build Phases Build Rules									
> 🚞 libs		+ Basic	Customized All Combined Levels							
∽  mis hook_native	PROJECT		System Header Search Paths							
m* hook_native_misc.xm	🖾 iOSOpenDevHookTemplate		Use Header Maps	Yes ≎						
m* hook_native_misc.mm			User Header Search Paths							
✓	TARGETS									
m <sup>*</sup> hook_iOS_ObjC_CommonClass.xm	a iOSOnonDavideokTomplata									
m* hook_iOS_ObjC_CommonClass.mm	in losopenberrioskiemplate	✓ Signing								
m* hook_iOS_ObjC_specific.xm			Setting	iOSOpenDevHookTemplate	8					
m hook iOS ObiC specific.mm			Code Signing Entitlements							
V 📷 Package		,	Code Signing Identity	Apple Development						
V DEBIAN			Code Signing Style	Automatic ¢	CODE_SIGN_IDENTITY=Apple Development					
Control.txt			Development Team	Mao Li ≎						
control			Enable App Sandbox	No ≎						
Library			Enable Hardened Runtime	No ≎						
MobileSubstrate			Enable User Selected Files	None ©						
Dynamicl ibraries			Launch Constraint Process Plist							
iOSOpenDevHookTemplate plist			Launch Constraint Responsible Process Plist							
> Supporting Files			Library Load Constraint Plist							
Frameworks			Other Code Signing Flags							
in libeubetrate dylib			Provisioning Profile	Automatic C						
Coundation framework										

#### 不要设置Code Sign Identity为 Apple Development: xxx

#### 此处之前设置了:

• Xcode -> TARGETS -> {YourProjectName} -> Build Settings -> Signing -> Code Sign Identity ->设置为(Certificates in Keychain 中的) Apple Development: Mao Li (UBFSP2P5PM)
结果会报错:

o

/Users/crifan/dev/dev\_root/crifan/github/iOSOpenDevHookTemplate/iOSOpenDevHookTemplate/iOSOpenDevHookTemplate.xcodepr oj iOSOpenDevHookTemplate has conflicting provisioning settings. iOSOpenDevHookTemplate is automatically signed, but code signing identity Apple Development: Mao Li (UBFSP2P5PM) has been manually specified. Set the code signing identi ty value to "Apple Development" in the build settings editor, or switch to manual signing in the Signing Capabiliti es editor.

Construction of the state of	•••
<ul> <li>Schwarzschwarz</li></ul>	
	<ul> <li>III USOpenDevidoxItemplate 3 issue:</li> <li>III USOpenDevidoxItemplate has conflicting provisioning statistics of the source of the source</li></ul>
	🐨 Filter 🕘 🕲

然后改为上面说的( Automatic 中的) Apple Development , 才彻底解决了此处报错的问题。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-01-15 16:28:28

# control的Version版本号的改动会丢失

● 现象:

项目中的 .plist 中的 Version 的值, 默认是 1.0-1

当想要去改动版本号,比如改为 2023.07.19.2126 ,结果重新编译后,改动后的Version值丢失,又恢复到之前的默认值 1.0-1 了

- 解决办法
  - TARGETS -> Build Settings -> User-Defined -> iOSOpenDevUsePackageVersionPList 从(默认的) YES 改为 NO



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:50:51

# 安装插件后桌面上看不到iOS的app图标

- 现象:带UI界面的tweak或app, (通过Filza)安装到iPhone中后,桌面上看不到iOS的app的图标
- 原因: iPhone的UI界面没有刷新=icon图标没有刷新
- 解决办法:
- o uicache
  - 如果是通过Filza安装deb的话
    - Filza的安装完成界面的点击右上角: 动作 -> 选择: UIcache
      - 冬

₊山 中国移动 🗢	下午10:22	<b>1</b>
完成	_2021.11.04.deb	动作
[exec dpkg -i] bash-5.0# dpkg -i	"'/	
2021.1	L1.04.deb" ;	
(Reading database		
(Reading database	5%	
(Reading database	10%	
(Reading database	15%	
(Reading database	20%	
(Reading database	20%	
(Reading database	35%	
(Readi		
(Readi	动作	
(Readi	-511	
(Readi		
(Readi	注销	
(Readi		
(Read)	vienden	
(Read)	uicache	
(Readi		
(Readi	取消	
(Reading uncounter		
(Reading database	100%	
(Reading database	4498 files and	
directories currer	ntly installed.)	
Preparing to unpac	ck /	
)_2021.1	L1.04.deb	
$(2021 \ 11 \ 04-2)$ over	an (2021 11 04 2)	
Setting up com cri	ifan.r	
(2021.11.04-2)		
Processing trigger	rs for cydia (1.1.36	)
bash-5.0#		

- 稍等片刻-》桌面上即可出现iOS的app的logo图标了
  - 注:此时点击 注销 = Respring = 重启SpringBoard ,虽然理论上可行,但实际是无效的,无法让桌面 出现app图标的
- 如果不是,则可以单独命令行去运行: uicache

.

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:53:57

# mach-o file, but is an incompatible architecture have 'arm64', need 'arm64e'

### 现象

iOSOpenDev的Xcode编译出了插件dylib插件,但是启动加载时报错:

'/private/preboot/xxx/procursus/Library/MobileSubstrate/DynamicLibraries/jailAppleAccount.dylib' (mach-o file, but is an incompatible architecture (have 'arm64', need 'arm64e'))

•••	<b>控制台</b> 6 条信息		00 S S O O O O E v jailAppleAccount 哲停 現在 活动 清除 重新载入 简介 共享
	□ 所有信息 错误和故障		存储
二 licrifan的MacBook Pro	类型 时间	进程	信息
🚺 iPhone8_150 🛛 🗢	14:50:37.206463+0800	Preferences	正在修复 path=/private/preboot/3B92D6F7C3FE6444A715B312E418498574E442DAB2F6D9E18B58B762F71D145
iPhone11_151	14:50:37.206568+0800	jailbreakd	/private/preboot/3B92D6F7C3FE6444A715B312E418498574E442DAB2F6D9E18B58B762F71D1455B7E2E1C2DD39
	14:50:37.207165+0800	Preferences	tweakinject 注入失败原因:dlopen(/var/Liy/Library/MobileSubstrate/DynamicLibraries/jailAppleAcco
▲ 崩溃报告	14:50:37.207319+0800	jailbreakd	/var/Liy/Library/MobileSubstrate/DynamicLibraries/jailAppleAccount.dylib
⊗ Spin报告	14:50:37.207370+0800	Preferences	正在修复 path=/private/preboot/3B92D6F7C3FE6444A715B312E418498574E442DAB2F6D9E18B58B762F71D145!
▶ 日志报告	14:50:37.207648+0800	jailbreakd	/private/preboot/3B92D6F7C3FE6444A715B312E418498574E442DAB2F6D9E18B58B762F71D1455B7E2E1C2DD39
☆ 診断 据告			
System.log			
	Preferences (TweakInject.dvlib)		易失
	子系统: 类别: <缺少描述> 详细信息		2023-03-21 14:50:37:207165+0800
	tweakinject 注入失敗原因:dlopen(/var/Liy/L jallAppleAccount.dylib (mach-o file, but is jallAppleAccount.dylib (mach-o file, ybriv procursus/Library/MobileSubstrate/Dynam jallAppleAccount.dylib (no such file), <sup>7</sup> /usr/ 3892D6F7C3FE6444A715B312E418498574 jailAppleAccount.dylib (mach-o file, but is	ibrary/MobileSubst an incompatible ar ate/preboot/3B921 icLibraries/jailAppl ik/jailAppleAccour E442DAB2F6D9E18 an incompatible ar	rate/DynamicLibraries/jailAppleAccount.dvilb, 0x0009): tried: //var/Liy/Library/MobileSubstrate/DynamicLibraries/ chitecture (have 'arm642', peed'arm64e')), //usr/local/lib/jailAppleAccount.dvilb' (ne such file), //usr/lib/ per/32F5444715831254148675442420AB2F602F618587927110156872E512CD029128184E6D10C68015028/ eAccount.dvilb' (mach-o file, but is an incompatible architecture (have 'arm64', need 'arm64e')), //usr/local/lib/ tt dyilb' (no such file), //ortwal/preboot/ 18588762F71014558752E1C2D0391281B4E6D10C689150C8/procursus/Library/MobileSubstrate/DynamicLibraries/ chitecture (have <>

### 原因

此处目标设备 iPhone11 的 CPU 是 A12 ,其架构是 arm64e 的,而插件代码编译出的架构是针对 arm64 的,不兼容,所以报 错

### 解决办法

• Xcode中去把架构改为(包含=支持) arm64e

# 具体步骤

- Xcode -> TARGETS -> YourProjectName -> Build Settings -> Architectures -> Architectures

   从默认的: \$(ARCHS\_STANDARD) == arm64, armv7
  - o 改为: Other 的 arm64 arm64e

如此,即可确认所编译出来的代码(插件),支持arm64e了。

### 注

- 如果额外引用到库文件,则也要确保库文件是支持此处的arm64e的
  - 比如此处遇到 libsubstrate.dylib , 就是:

- 默认(iOSOpenDev自带的)不支持arm64e,最后是另外找支持arm64e的 ■ 比如
  - - XinaA15越狱后的iPhone11中有
      - /private/preboot/3B92D6F7C3FE6444A715B312E418498574E442DAB2F6D9E18B58B762F71D1455B7E2E1C2DD39 12B1B4E6D10C6B9150C8/procursus/usr/lib/libsubstrate.dylib
        - 大小: 218KB
        - (就是我们要的)FAT格式的,支持2种架构: arm64 和 arm64e
- 去拷贝替换掉原先的: Mac 中的 /opt/iOSOpenDev/lib/libsubstrate.dylib
- 才顺利编译和链接,才能确保插件正常工作

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 09:55:24

# Failed Logos Processor outputted Could not open xm file

# 现象

#### 之前iOSOpenDev中,主项目目录下面,新建**子目录**:

<b>É Xcode</b> File Edit View	Find	Navigate	Editor	Product	Debug	Integrat
			P iOSO	penDevHoo	okTempla	te
🗎 🛛 🗋 🔍 🖉 🖉		=	× ₂" 閉	I < > pro	oj n	า๋ hook_iOs
✓		М	🛃 iOSOpe	nDevHookTer	mplate 👌 🗎	iOSOpen
<ul> <li>iOSOpenDevHookTemplate</li> <li>ibs</li> <li>hook_native</li> <li>hook_native_misc.xm</li> <li>hook_native_misc.mm</li> <li>hook_iOS</li> <li>m<sup>+</sup> hook_iOS_ObjC_Comn</li> <li>m<sup>+</sup> hook_iOS_ObjC_Comn</li> <li>m<sup>+</sup> hook_iOS_ObjC_Comn</li> </ul>	Show in Open in Open in Open w Open A Show Fil	n Finder n Tab n New Wind vith Externa s ile Inspecto e	ow I Editor pr		>	ojC_Com DS ObjC i tUpdate n" " S.h"
m <sup>+</sup> hook_iOS_ObjC_speci	Add File Add Pa Delete New Gr New Gr	e es to "iOSC ckage Depe roup roup withou roup from S	epenDevHo endencies t Folder election	ookTemplate	9"	= @"app ences =
<ul> <li>DynamicLibraries</li> <li>iOSOpenDevHo</li> <li>Supporting Files</li> <li>Frameworks</li> <li>libsubstrate.dylib</li> <li>Foundation.framework</li> </ul>	Add Lin Bookma Sort by Sort by Find in Source	e Bookmar ark "iOSOp Name Type Selected G Control	k enDevHoo roups	kTemplate"	 >	n proto ing *cu nmonLog ns ing *cu FALSE;
	Project	Navigator I	Help	// -	- contair	ToStrin ix: ix:

在子目录中,新增 .xm 文件:

- iOSOpenDevHookTemplate
  - hook\_iOS



会导致编译报错:

Preparing to run Xcode Build Phase for Logos Processor... Logos Processor: hook\_iOS\_ObjCCommonClass.xm - hook\_iOS\_ObjCCommonClass.mm... Failed Logos Processor Logos Processor outputted: Could not open /Users/crifan/dev/dev\_root/crifan/github/iOSOpenDevHookTemplate/iOSOpenDev



### 原因

(看来是) iOSOpenDev中,不支持子目录 == 如果把 .xm 放在子目录中,则 Logos Processor 则会找不到,导致编译报错

### 解决办法

#### 【推荐】思路1:用虚拟目录

Xcode中,右键新建目录时:

- 不用: New Group
   o -> 创建物理上的,文件系统上,真实的:子目录
- 改用: New Group without folder
  - -> Xcode中虚拟的子目录 = 物理上的, 文件系统上的子目录: 是没有的, 是不存在的

<b>É Xcode</b> File	Edit	View	Find	Navigate	Editor	Product
					iOSOp main	penDevH
	Q 🔬			Ξ	盟 < >	Ē
iOSOpenDevHo	okTempla	te		М	🛃 iOSOper	nDevHookTen
🛅 iOSOpenDev					1 Day	kage: com
> 🖿 libs	Show Ir	h Finder				n: 202
m <sup>†</sup> hook_iOS_	Open ir	Tab				ption:
m <sup>*</sup> hook_iOS_	Open ir	New Wi	ndow			s: fir
m <sup>t</sup> book iOS	Open w	of the Exteri	hal Edito	or		.cts:
✓ ■ Package		5				ty: op
V DEBIAN	Show F	ile Inspec	tor			ecture
🗐 contro	New Fil	e				: CIII
E contro	Add File	es to "iOs	SOpenD	evHookTem	plate"	ge: ht
V 📕 Library	Add Pa	ckage De	penden	cies		iner:
	Delete					
⊞ iC	New Gr	oup				
> 🖿 Supporting	New Gr	oup with	out Fold	er		
	New Gr	oup from	Selecti	on		
m libsubstrat	Add Lin	e Bookm	ark			
Foundation	Bookma	ark "iOSC	DpenDev	/HookTemp	late"	
	Sort by	Name				
	Sort by	Туре				
	Find in	Selected	Groups			
	Source	Control				>
	Migrate	to String	g Catalo	g		
	Project	Navigato	r Help			

#### 效果

(1) Xcode中文件夹图标

虚拟文件夹和真实文件夹:图标,略有不同:

- 文件夹左下角的小三角
  - o 虚拟文件夹:有
  - 真实文件夹:没有



(2) Xcode中虚拟的子目录 = 物理上的, 文件系统上的子目录: 是没有的, 是不存在的

Finder中,是看不到(Xcode中的虚拟的)子目录的:



#### 【不推荐】思路2: 放弃创建子目录

Xcode中的iOSOpenDev中,新增文件时:不用 New Group,即: 只能把所有 .xm (和对应的 .mm 文件,都直接放到根目录下,没有子目录了 -》虽然当文件多时,逻辑上不够清晰,但是至少能凑合用 crifan.org,使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 12:05:46

84

# 心得

TODO:

- 【未解决】XCode调试警告: was compiled with optimization stepping may behave oddly variables may not be available
- 【未解决】iOSOpenDev的XCode的tweak插件编译尝试去掉优化加上调试信息
- •
- 【已解决】iOSOpenDev的XCode调试iPhone6报错: Unable to install The application could not be verified
- 【已解决】XCode中删除掉User-Defined的自定义参数
- •
- 【已解决】iOSOpenDev的XCode的iOS的tweak插件中实现ObjC的通用全局函数
- 【已解决】iOSOpenDev的XCode的iOS插件运行报错: ImageLoaderMachO doModInitFunctions和\_logosLocalInit
- 【已解决】iOS代码报错: objc Class is implemented in both app and dylib One of the two will be used Which one is undefined
- •
- 【已解决】iOSOpenDev的XCode项目编译报错: iPhone Developer no identity found
- 【已解决】调试iOSOpenDev的XCode的iOS的app
- 【已解决】研究iOSOpenDev的XCode项目编译过程以确保如何链接自定义.c文件的.o文件
- 【已解决】iOSOpenDev的XCode项目偶尔编译非常慢卡死
- 【已解决】iOSOpenDev的XCode中新增.c和.h文件并正常编译
- 【已解决】如何把XCode的iOS的app项目转换成iOSOpenDev的项目
- 【已解决】对比研究FakeWeChatLoc和自己的XCode项目的目录结构区别
- 【已解决】iOSOpenDev的XCode调试iPhone7报错: Unable to install A system application with the given bundle identifier is already installed on the device and cannot be replaced
- 【记录】更新iOSOpenDev的Logos插件的code signing签名配置
- 【已解决】XCode中iOSOpenDev开发插件代码报错: No matching function for call to strcpy
- 【已解决】XCode中iOSOpenDev的Tweak项目中Build Settings中User-Defined中添加和引用变量THEOS
- 【记录】研究XCode中clang编译mm文件的过程和编译参数
- 【记录】深究为何此处XCode编译strcpy会报错No matching function for call to
- 【未解决】把之前theos的tweak改机剩余功能移植到iOSOpenDev的XCode中
- •

### .xm 文件和 .mm 文件

TODO:

- 【已解决】Xcode中xm源码中无法看到和添加断点
- 【已解决】iOSOpenDev的XCode中.xm文件包含.c中函数找不到报错: Undefined symbols for architecture arm64 referenced from
- 【已解决】XCode的iOSOpenDev项目报错: Failed Logos Processor Could not open xm
- 【已解决】iOSOpenDev的XCode中如何把Tweak的xm代码拆分成多个文件模块
- 【未解决】iOSOpenDev的iosod的bug修复:Logos的预处理不支持group子目录中的xm文件

#### 代码高亮

- 【已解决】iOSOpenDev的XCode中新增xm文件设置为Logos语法高亮但无效
- 【已解决】让XCode的iOSOpenDev中Logos的xm文件支持语法高亮

# iOSOpenDev内部逻辑和过程

TODO:

- 【未解决】研究iOSOpenDev的XCode项目编译过程以确保如何链接自定义.c文件的.o文件
- 【已解决】XCode编译iOSOpenDev的Logo Tweak项目报错: Command PhaseScriptExecution failed with a nonzero exit code Failed to locate Logos Processor
- 【未解决】XCode中编译iOSOpenDev的Logos的Tweak时shell从sh换为zsh
- 【已解决】给iOS的XCode项目中新增iOSOpenDev的Project Navigator的目录和文件
- 【已解决】XCode项目中新增iOSOpenDev的Package目录到Target目录中
- 【已解决】XCode中如何把libsubstrate.dylib动态库导入到Link Binary With Libraries

# 如何卸载带UI的插件app

• 通过Cydia去卸载已安装的(带UI界面的)插件tweak即可

步骤:

Cydia -> 已安装 -> 最近 ->找到插件->进入详情页



点击右上角的 卸载:

💷 中国移动 🗢	下午11:08			
取消	确认	确认		
	继续队列	>		
更改				
卸载		沐家百货		

即可卸载掉插件。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 11:49:52

# 相关教程和代码

- 相关教程
  - 。 推荐用这个方式去iOS逆向调试
    - iOS逆向调试: Xcode+iOSOpenDev
- 代码
  - 。 iOSOpenDev的hook插件代码开发的模板
    - iOSOpenDevHookTemplate
      - Github
        - https://github.com/crifan/iOSOpenDevHookTemplate
          - crifan/iOSOpenDevHookTemplate: Crifan's iOSOpenDev Hook Template, for common iOS ObjC Class, native C functions, other misc
      - 代码
        - hook\_iOS\_ObjC\_CommonClass.xm
          - https://github.com/crifan/iOSOpenDevHookTemplate/blob/main/iOSOpenDevHookTemplate/iOS
             OpenDevHookTemplate/hook\_iOS\_ObjC\_CommonClass.xm
        - hook\_iOS\_ObjC\_specific.xm
          - https://github.com/crifan/iOSOpenDevHookTemplate/blob/main/iOSOpenDevHookTemplate/iOS
             OpenDevHookTemplate/hook\_iOS\_ObjC\_specific.xm
        - hook\_native\_misc.xm
          - https://github.com/crifan/iOSOpenDevHookTemplate/blob/main/iOSOpenDevHookTemplate/iOS
             OpenDevHookTemplate/hook\_native\_misc.xm

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-01-15 16:06:33

# 附录

下面列出相关参考资料。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-11-08 10:39:15

# 参考资料

- 【整理】iOS越狱插件开发工具: iOSOpenDev
- 【已解决】把iOS的app和iOS的tweak插件打包成独立的deb安装包
- 【已解决】把iOSOpenDev的tweak加app的deb文件安装到已越狱的iPhone中
- 【已解决】如何把普通iOS的app的XCode项目和iOSOpenDev的Logos插件tweak集成到一起
- 【已解决】如何把XCode的iOS的app项目转换成iOSOpenDev的项目
- 【已解决】给iOSOpenDev的app和tweak用配置文件互相通信
- 【已解决】已越狱iPhone中卸载tweak加app的deb插件
- 【记录】确认iPhone中安装后的tweak加app是否正常使用
- 【已解决】把iOSOpenDev的tweak插件和app合并打包成deb文件
- 【已解决】把iOSOpenDev的tweak加app的deb文件安装到已越狱的iPhone中
- 【已解决】iOSOpenDev的XCode去Build For Profiling安装后iPhone桌面上找不到iOS的app的图标
- 【已解决】用Filza安装tweak加app的deb后iPhone桌面中仍没出现iOS的app的logo图标
- 【已解决】ssh登录iPhone失败: Host key verification failed
- 【已解决】Mac中安装iOSOpenDev
- 【已解决】Mac中安装iOSOpenDev报错:安装器遇到了一个错误,导致安装失败
- 【已解决】Mac中初始化iOSOpenDev环境并新建插件项目
- 【已解决】iOSOpenDev设置SDK报错: File not found XCode Specifications iPhoneOSPackageTypes.xcspec
- 【已解决】iOSOpenDev设置SDK报错: PrivateFramework directory not found XCode iPhoneOS15.0.sdk
- 【已解决】用iOSOpenDev去开发带GUI图形界面的iOS的app和tweak插件集成在一起的插件deb包
- 【已解决】iOS逆向:如何去hook一个进程而不是带包名的iOS的app
- 【已解决】XCode中iOSOpenDev中修改control的Version版本号无效会被重置
- 【未解决】iOS逆向akd:新建iOSOpenDev的Xcode插件项目
- 【已解决】iOSOpenDev的插件dylib注入iPhone11失败: mach-o file but is an incompatible architecture have arm64 need arm64e
- 【已解决】寻找支持arm64e的libsubstrate.dylib
- 【已解决】Xcode项目中引用新的libsubstrate.dylib无效:始终链接是旧的库文件
- 【已解决】Mac M2 Max中iOSOpenDev编译报错: An empty identity is not valid when signing a binary for the product type Dynamic Library
- 【已解决】XCode中删除用户自定义配置User-Defined中的 CODE\_SIGNING\_ALLOWED=NO
- 【已解决】Mac中iOSOpenDev编译报错scp dest open /var/root/iOSOpenDevPackages/xxx.deb No such file or directory
- 【已解决】iOSOpenDev的XCode中xm代码%hookf编译报错: Expected unqualified-id
- 【已解决】Xcode中Logos插件hook代码编译报错: Expected unqualified-id
- 【规避解决】Xcode中iOSOpenDev编译报错: Failed Logos Processor outputted Could not open sub folder xm
- •
- iosOpenDev-install 失败官方wiki无法解决看这里(尝试有效) PoloKey 博客园 (cnblogs.com)
- zhangkn/knPrivateFrameworks:

/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/iPhoneOS9.2.sdk/System /Library/PrivateFrameworks (github.com)

- iosopendev专用Specifications.zip
- 越狱开发:用iosOpenDev配置越狱开发环境 编写第一个hello world\_我的杯洗具的博客-CSDN博客
- jackrex/FakeWeChatLoc: 手把手教你制作一款iOS越狱App (github.com)
- ios An empty identity is not valid when signing a binary for the product type 'Application' in xcode version 10.2 Stack Overflow
- •

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2024-11-25 11:50:56