
目录

前言	1.1
砸壳ipa概览	1.2
常见砸壳工具	1.3
frida-ios-dump	1.3.1
dumpdecrypted	1.3.2
Clutch	1.3.3
bfinject	1.3.4
砸壳实例	1.4
frida-ios-dump实例	1.4.1
TikTok的ipa	1.4.1.1
抖音的ipa	1.4.1.2
YouTube的ipa	1.4.1.3
砸壳后	1.5
安装ipa	1.5.1
砸壳常见问题	1.6
无进度 0.00B 00:00	1.6.1
DeviceNotSupportedByThinning	1.6.2
app启动后崩溃	1.6.3
附录	1.7
参考资料	1.7.1

iOS逆向开发：砸壳ipa

- 最新版本： v1.0.0
- 更新时间： 20240717

简介

介绍iOS逆向中的砸壳脱壳出ipa方面的内容。主要包括什么是壳，为何要砸壳，常见砸壳工具，比如frida-ios-dump、dumpdecrypted、clutch等；以及举例介绍如何用frida-ios-dump砸壳YouTube、抖音等app得到ipa文件；以及砸壳出iap后的事情，包括ipa的安装；以及整理常见的问题及解决办法。

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_crack_shell_ipa](#): iOS逆向开发：砸壳ipa

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：砸壳ipa [book.crifan.org](#)
- iOS逆向开发：砸壳ipa [crifan.github.io](#)

离线下载阅读

- iOS逆向开发：砸壳ipa PDF
- iOS逆向开发：砸壳ipa ePub
- iOS逆向开发：砸壳ipa 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。如发现侵权，请通过邮箱联系我 [admin 艾特 crifan.com](mailto:admin@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：
2024-07-17 11:41:04

砸壳ipa概览

什么是壳?

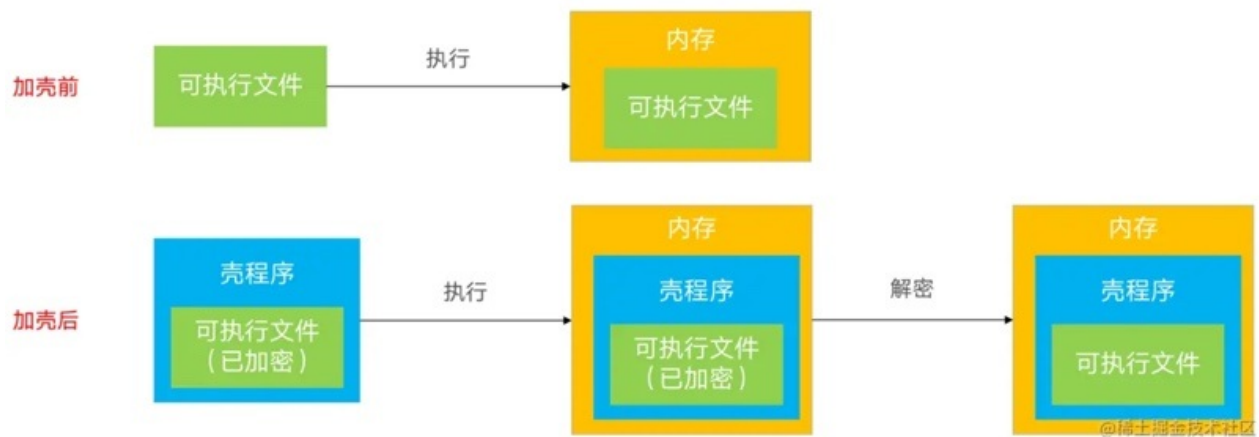
壳，在安全和逆向领域，泛指：用技术手段，给原程序额外加上一层保护程序

什么是iOS的app的壳?

iOS中的app，发布渠道一般都是 App Store。

从 App Store 下载的APP全都是经过苹果加密过的 ipa 包。

而Apple会为了安全，给app加密(使用Apple ID相关的对称加密算法)，这个过程俗称为：加壳，就像给app外部上加了一层壳



而加密后的 ipa 包，是无法继续后续的逆向过程的

- 后续的典型的逆向过程是
 - 用 IDA / Hopper 等去 反编译
 - 用 class-dump 等去 导出头文件
 - 说明
 - class-dump 直接去导出，未砸壳的，App Store 上的二进制的文件
 - 只能导出 CDStructures.h 这个空的头文件，无法得到想要的各种类的头文件
 - 对砸壳后的ipa，去用 MonkeyDev 动态调试
 - 等等

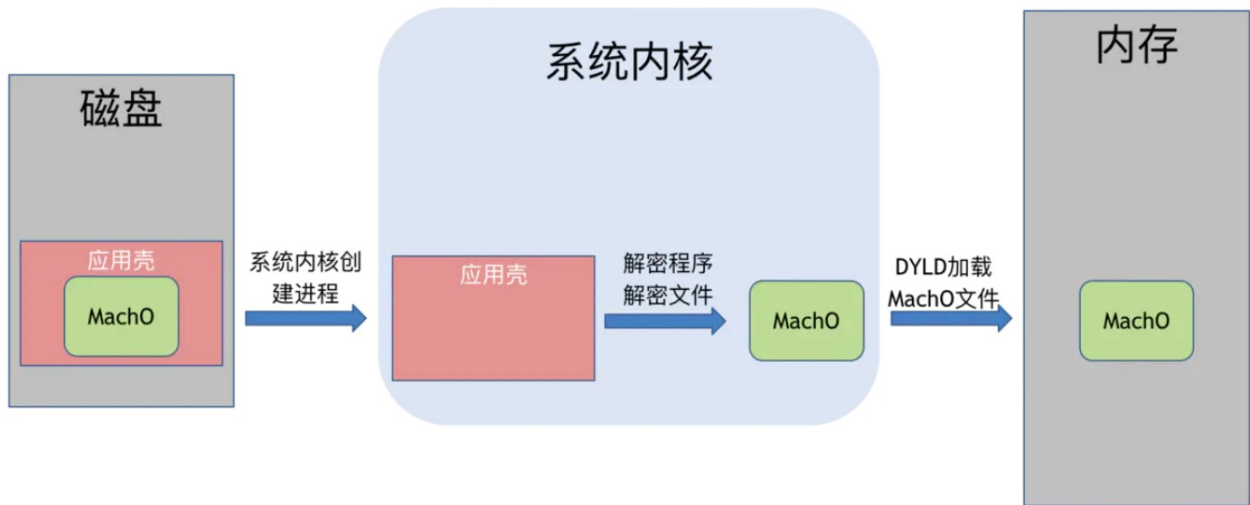
什么是iOS的砸壳 + 如何砸壳?

想要破解分析iOS的app之前，需要 把这层壳砸破 = 砸壳 = 脱壳。

- 砸壳有两种机制
 - 静态砸壳：使用已知的解密方法对软件进行解密叫静态砸壳，静态砸壳难度大，需要知道其软件的加密算法才能对其解密
 - 现在没有这种工具
 - 动态砸壳

- 现在绝大多数工具都是用此方式

如何（动态）砸壳呢？就要先了解app运行机制：app程序运行起来都会直接在内存解密出原始代码



可以在越狱的设备里面通过内存 dump 方式提取解密后的程序，这种解密过程，也就是给app去壳的过程，又称为 砸壳 = 破壳

- 额外说明
 - 解密之后还需要手动恢复 Mach-O 头信息才能运行
 - 由于高版本非完美越狱里面，都没有删掉签名验证
 - 所以直接运行都会出现 killed 9
 - 需要手动签名之后才能使用

砸壳的前提

- 确保iOS设备（iPhone等）已越狱
 - 详见：
 - [iOS逆向开发：iPhone越狱](#)

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:
2023-10-08 09:58:16

砸壳工具

常用的iOS的app的砸壳的工具:

- `frida-ios-dump` : 最新, 最好用, 最常用
- 其他更早的工具
 - `dumpdecrypted`
 - 一般配合 `Cycript` 使用?
 - `clutch`
 - `bfinject`

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 11:35:03

frida-ios-dump

- frida-ios-dump
 - 一句话描述: Pull a decrypted IPA from a jailbroken device
 - Github
 - AloneMonkey/frida-ios-dump: pull decrypted ipa from jailbreak device
 - <https://github.com/AloneMonkey/frida-ios-dump>

下载

- 下载命令

```
git clone https://github.com/AloneMonkey/frida-ios-dump.git
```

- 下载后的文件的说明
 - `dump.py` : 最核心的文件, 用来砸壳的Python脚本
 - `requirements.txt` : Python依赖包的列表
 - 后续安装依赖的库, 需要用到

初始化环境

- 先安装Frida
 - 概述
 - (Win/Mac等) 电脑端

```
pip install frida
```
 - (iOS/Android等) 移动端
 - iPhone
 - Cydia -> 添加源 <https://build.frida.re> -> 安装插件: Frida
 - 详解
 - [安装Frida · 逆向调试利器: Frida](#)
- 再去安装依赖的其他的库
 - 直接用官网的依赖文件 `requirements.txt` 去安装

```
sudo pip install -r requirements.txt
```
 - 或已知需要哪些库, 手动安装

```
pip install paramiko scp tqdm
```
- USB端口转发
 - 目的: 方便本地直接访问对应端口, 即可映射为, 实际的iOS设备
 - 步骤
 - 概述

```
iproxy 2222 22
```

- 详解
 - [frida-ios-dump](#) 砸壳 TikTok 的 ipa 的实例

使用=砸壳

- 概述

- 查看 app 包名或 app 名称

- 方式1: `frida-ps`

```
frida-ps -Uai
```

- 方式2: `ideviceinstaller`

```
ideviceinstaller -l -o list_user
```

- 开始砸壳

- 命令

```
./dump.py iOSAppPackageOriOSAppName
```

- 举例

```
./dump.py com.zhiliaoapp.musically
```

```
./dump.py com.ss.iphone.ugc.Aweme
```

```
./dump.py com.google.ios.youtube
```

```
./dump.py YouTube
```

- 详解

- 详见后续章节: [frida-ios-dump](#) 实例

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:
2023-10-12 11:56:39

dumpdecrypted

- dumpdecrypted
 - 一句话描述: iOS的砸壳工具
 - Dumps decrypted iPhone Applications to a file
 - 资料
 - GitHub
 - stefanesser/dumpdecrypted: Dumps decrypted mach-o files from encrypted iPhone applications from memory to disk. This tool is necessary for security researchers to be able to look under the hood of encryption.
 - <https://github.com/stefanesser/dumpdecrypted>

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:
2022-10-21 17:12:54

Clutch

- Clutch
 - 是什么
 - Fast iOS executable dumper
 - a high-speed iOS decryption tool
 - 功能：脱壳=砸壳
 - 针对（越狱的）iOS设备，（解密）导出头文件
 - 支持平台
 - 所有iOS设备： iPhone/iPod Touch/iPad
 - 资料
 - GitHub
 - KJCracks/Clutch: Fast iOS executable dumper
 - <https://github.com/KJCracks/Clutch>
 - Wiki
 - Home · KJCracks/Clutch Wiki
 - <https://github.com/KJCracks/Clutch/wiki>
 - Tutorial · KJCracks/Clutch Wiki
 - <https://github.com/KJCracks/Clutch/wiki/Tutorial>
 - FAQ · KJCracks/Clutch Wiki
 - <https://github.com/KJCracks/Clutch/wiki/FAQ>

help语法

```
Clutch [OPTIONS]
-b --binary-dump    Only dump binary files from specified bundleID
-d --dump           Dump specified bundleID into .ipa file
-i --print-installed Print installed application
--clean            Clean /var/tmp/clutch directory
--version          Display version and exit
-? --help          Display this help and exit
```

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:
2022-10-21 11:52:29

bfinject

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:
2022-10-21 11:52:29

砸壳实例

此处介绍，具体如何用砸壳工具去砸壳出ipa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:
2022-10-21 17:23:08

frida-ios-dump实例

此处介绍，如何用 `frida-ios-dump` 去砸壳出iOS的app的ipa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:
2023-08-29 21:52:32

TikTok的ipa

给TikTok砸壳出ipa:

- 概述

```
./dump.py com.zhiliaoapp.musically
```

- 详解:

前提

- 前提: 越狱iPhone中已安装 TikTok
 - 注: 通过境外比如美区 AppleID 登录后的 AppStore 中才能搜索和下载 TikTok

砸壳ipa的步骤

(1) 先确认app包名

```
ideviceinstaller -l -o list_user
```

输出能看到:

- com.zhiliaoapp.musically, "268010", "TikTok"

得到 TikTok 包名是: com.zhiliaoapp.musically

(2) 确保Mac中当前Python中已安装frida (以及相关的库)

如果没有装, 要去安装:

```
pip install frida paramiko scp tqdm
```

(3) 另外新建一个终端, 开启端口映射

新建一个终端窗口 (或Tab), 去运行端口映射

```
iproxy 2222 22
```

(4) 确保frida版本一致: Mac中和iPhone中frida版本是一样的

说明:

- 如何查看frida版本
 - iPhone

```
frida-server --version
```

- Mac

```
pip show frida
```

- 如果frida版本不一致

- 后续会报错: Failed to enumerate applications unable to communicate with remote frida-server
 - Failed to enumerate applications: unable to communicate with remote frida-server; please ensure that major versions match and that the remote Frida has the feature you are trying to use
- 需要去确保一致
 - 举例:
 - 此处frida版本:
 - Mac: 16.0.2
 - iPhone: 15.1.27
 - 如何解决
 - 去iPhone中 Cydia 中升级frida到最新版 16.0.2

(5) 确保被砸壳的app已退出, 没在运行

可选? iPhone中被砸壳的app, 已退出, 不要已启动真正运行

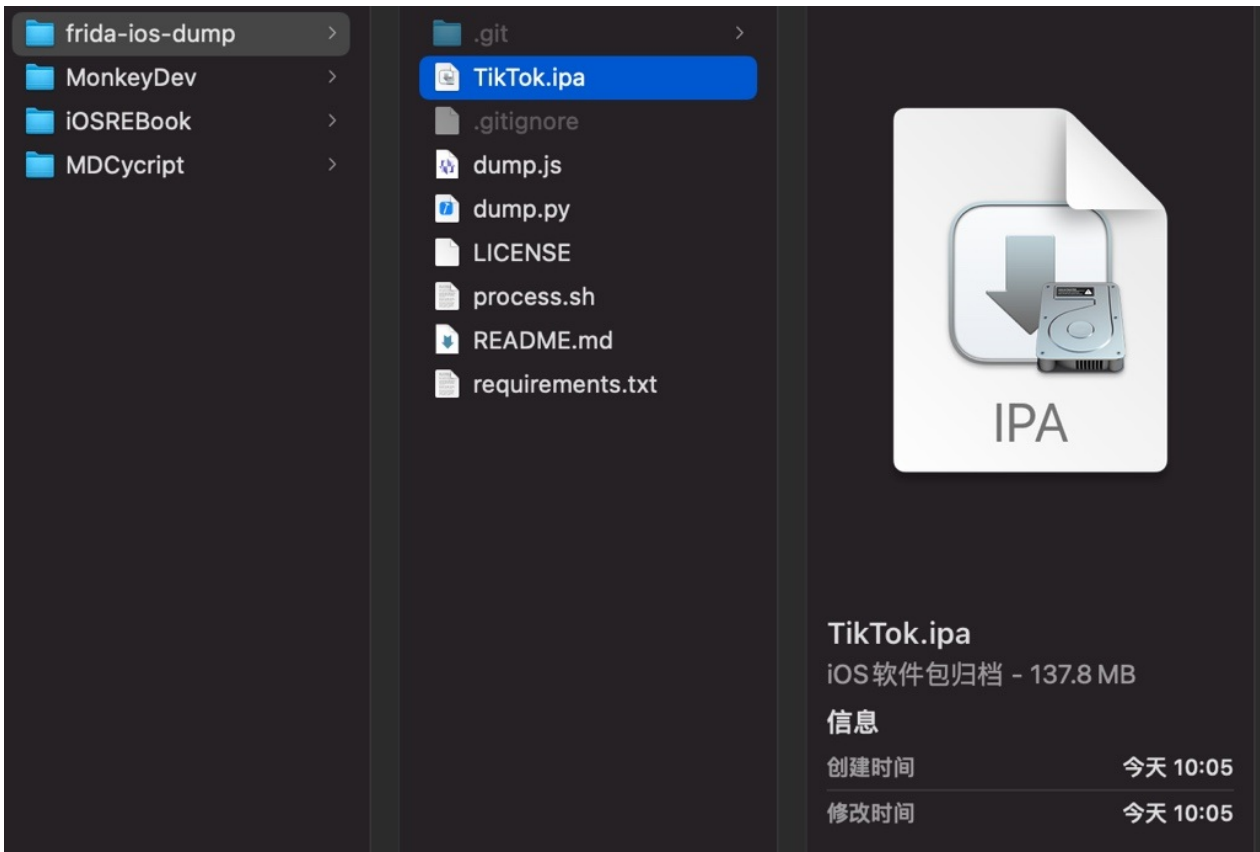
(6) 真正开始砸壳

- 概述

```
./dump.py com.zhiliiaoapp.musically
```

- 详解

```
crifan@licrifandeMacBook-Pro ~/dev/dev_src/ios_reverse/AloneMonkey/frida-ios-dump \
master` ./dump.py com.zhiliiaoapp.musically
Start the target app com.zhiliiaoapp.musically
Dumping TikTok to /var/folders/yy/46k2nmtx7nv344lm9zb6q66c0000gn/T
[frida-ios-dump]: Load libvcn.framework success.
[frida-ios-dump]: Load crypto.framework success.
[frida-ios-dump]: Load VolcEngineRTC.framework success.
[frida-ios-dump]: Load byteaudio.framework success.
[frida-ios-dump]: Load TikTokMSearchFramework.framework success.
[frida-ios-dump]: Load MuseDiscoverFramework.framework success.
[frida-ios-dump]: Load AAWELaunchTracker.framework success.
[frida-ios-dump]: Load RTCCFFmpeg.framework success.
[frida-ios-dump]: Load TTFMpeg.framework success.
[frida-ios-dump]: Load AAWEBootChecker.framework success.
[frida-ios-dump]: Load ffmpeg_dashdec.framework success.
[frida-ios-dump]: Load BDLRepairer.framework success.
[frida-ios-dump]: Load SCSDKCreativeKit.framework success.
[frida-ios-dump]: Load boringssl.framework success.
[frida-ios-dump]: MusicallyCore.framework has been loaded.
[frida-ios-dump]: Load SCSDKCoreKit.framework success.
start dump /private/var/containers/Bundle/Application/51BA1962-1A1E-40D8-AB83-E5BEACEF7
72C/TikTok.app/TikTok
```

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:
2023-08-29 22:20:49

YouTube的ipa

此处介绍，具体如何用 `frida-ios-dump` 去砸壳 YouTube 的ipa文件：

- 概述

```
./dump.py com.google.ios.youtube
```

详解

先查看出Youtube的包名：

```
→ frida-ios-dump git:(master) ideviceinstaller -l -o list_user
CFBundleIdentifier, CFBundleVersion, CFBundleDisplayName
rn.notes.best, "11122019", "爱思极速版"
com.suiyi.foodshop1, "4911", "食行生鲜"
com.cisco.anyconnect, "4.6.03052", "AnyConnect"
com.baidu.BaiduMobile, "10.5.5.10", "百度"
com.ishuyin.iShuYin, "1.22", "爱书音"
com.evernote.iPhone.Evernote, "358974", "印象笔记"
com.alipay.iphoneclient, "10.1.2.091512", "支付宝"
ctrip.com, "8.3.0", "携程旅行"
com.Qting.QTTour, "8.0.1.4", "蜻蜓FM"
com.360buy.jdmobile, "7.3.6", "京东"
com.taobao.tmall, "10948419", "手机天猫"
com.netease.cloudmusic, "876", "网易云音乐"
com.tencent.mqq, "7.2.9.404", "QQ"
com.crifan.ShowSysInfo, "1", "ShowSysInfo"
com.tencent.xin, "8.0.16.35", "微信"
com.google.ios.youtube, "17.08.2", "YouTube"
developer.apple.wwdc-Release, "801.5.2", "Developer"
com.ss.iphone.ugc.Aweme, "179011", "抖音"
com.3WRHBSBW4.com.rileytestut.AltStore, "1", "AltStore"
```

其中有我们要找的 YouTube 的详细信息：

- com.google.ios.youtube, "17.08.2", "YouTube"
 - 包名: com.google.ios.youtube
 - 版本: 17.08.2
 - 名称: YouTube

砸壳的具体过程和输出日志：

```
→ frida-ios-dump git:(master) pwd
/Users/crifan/dev/DevSrc/iOS/AloneMonkey/frida-ios-dump

→ frida-ios-dump git:(master) ./dump.py com.google.ios.youtube
Start the target app com.google.ios.youtube
Dumping YouTube to /var/folders/2f/53mn2kn920dfq4ww2gdqfpxc0000gn/T
[frida-ios-dump]: Load widevine_cdm_secured_ios.framework success.
```

```
[frida-ios-dump]: Module_Framework.framework has been loaded.
start dump /private/var/containers/Bundle/Application/ECB295AB-1355-46D1-8580-273B2CE98
802/YouTube.app/YouTube
YouTube.fid: 100% ██████████ 16.3M/16.3M [00:00 00:00, 17.7MB/s]
start dump /private/var/containers/Bundle/Application/ECB295AB-1355-46D1-8580-273B2CE98
802/YouTube.app/Frameworks/widevine_cdm_secured_ios.framework/widevine_cdm_secured_ios
widevine_cdm_secured_ios.fid: 100% ██████████ 3.44M/3.44M [00:00 00:00, 24.2MB/s]
start dump /private/var/containers/Bundle/Application/ECB295AB-1355-46D1-8580-273B2CE98
802/YouTube.app/Frameworks/Module_Framework.framework/Module_Framework
Module_Framework.fid: 100% ██████████ 114M/114M [00:03 00:00, 36.6MB/s]
Localizable.strings: 190MB [00:44, 4.45MB/s]
0.00B [00:00, ?B/s]
Generating "YouTube.ipa"
```

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:
2023-08-29 22:16:39

砸壳后

砸壳后，得到ipa文件后，还有些事情要做：

- 确认app已解密 = 确认砸壳成功
- 安装ipa

确认app已解密

可以用 `otool` 查看字段`crypt`的值：

- `cryptid=1` : 已加密
- `cryptid=0` : 没加密=已解密

举例

- 官网原始版本，安装到iPhone中后的，抖音的二进制文件 `Aweme` : 已加密

```
→ Aweme.app otool -l Aweme | grep crypt
cryptoff 28672
cryptsize 4096
cryptid 1
```

- 砸壳后的抖音的ipa中的二进制文件 `Aweme` : 已解密

```
→ Aweme.app pwd
xxx/Aweme抖音/iPhone7-137black/Aweme.app
→ Aweme.app otool -l Aweme | grep crypt
cryptoff 28672
cryptsize 4096
cryptid 0
```

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:
2023-12-13 21:45:11

砸壳后安装ipa

砸壳得到ipa文件之后，如果后续需要动态调试，包括部分的静态分析，往往需要：

确保ipa可以正常安装

此时往往也会遇到很多问题：

- 安装ipa
 - **【已解决】** 换用Filza安装砸壳抖音ipa
 - **【已解决】** 越狱iPhone中删除之前通过ipa安装的抖音app
 - **【已解决】** 脱壳抖音ipa用爱思助手安装后启动失败闪退
 - **【已解决】** 把砸壳后抖音ipa安装到iPhone中
 - **【已解决】** 越狱iPhone中如何实现respring重启桌面SpringBoard
 - **【记录】** 对比研究抖音ipa不同方式安装后embedded.mobileprovision签名证书中appld的区别
 - **【已解决】** 确认抖音ipa的app内部是否有重签名证书文件embedded.mobileprovision
 - **【已解决】** iPhone中Filza安装17.8.0抖音ipa报错：Failed to verify code signature The application does not have a valid signature
 - **【已解决】** iPhone中Filza安装17.8.0抖音ipa报错：Application is missing the application identifier entitlement

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：
2022-10-21 17:28:52

砸壳常见问题

此处整理，砸壳出iap的常见问题和解决办法。

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:
2024-07-17 11:26:12

无进度：Load success 0.00B [00:00, ?B/s]

- 现象：frida-ios-dump 砸壳最后，虽然提示Load success，但是始终没有进度，进度是0

```
./dump.py com.ss.iphone.ugc.Aweme
Start the target app com.ss.iphone.ugc.Aweme
Dumping 抖音 to /var/folders/2f/53mn2kn920dfq4ww2gdqfpxc0000gn/T
...
[frida-ios-dump]: Load byteaudio.framework success.
0.00B [00:00, ?B/s]
```

-
- 原因：未知。
- 解决办法：多试几次。
 - 想办法，用各种方式的，多试几次
 - 包括
 - 故意中断
 - 砸壳前，已启动app，或，不启动app
 - 等等
- 具体步骤：
 - 此处就是，某一次，在用：
 - `./dump.py com.ss.iphone.ugc.Aweme`
 - 启动后，也是同样卡死时
 - 注：当时抖音已正在运行了
 - Ctrl+C中断后，立刻再试：
 - `./dump.py com.ss.iphone.ugc.Aweme`
 - 结果就真的可以继续了。

DeviceNotSupportedByThinning

- 现象：此处把砸壳后的抖音ipa去安装到越狱iPhone中报错： DeviceNotSupportedByThinning

- 原因：
 - 此处的（抖音的app的）ipa是，Thinning瘦身后的
 - 即：上传到AppStore后的，只支持部分iPhone机型的安装包
 - 其中所支持的设备，不包含当前iPhone机型
 - 具体细节
 - Aweme抖音/已脱壳/Payload/Aweme.app/Info.plist

```

Info.plist — Aweme.app
Info.plist
28 <dict>
29   <key>SKAdNetworkIdentifier</key>
30   <string>238da61t44.skadnetwork</string>
31 </dict>
32 <dict>
33   <key>SKAdNetworkIdentifier</key>
34   <string>899VGT9G8.skadnetwork</string>
35 </dict>
36 <dict>
37   <key>SKAdNetworkIdentifier</key>
38   <string>r9hhd8ga5.skadnetwork</string>
39 </dict>
40 <dict>
41   <key>SKAdNetworkIdentifier</key>
42   <string>x2jnk7ly8.skadnetwork</string>
43 </dict>
44 <dict>
45   <key>SKAdNetworkIdentifier</key>
46   <string>3jtpea4u7.skadnetwork</string>
47 </dict>
48 </array>
49 <key>UISupportedDevices</key>
50 <array>
51   <string>iPhone10,1</string>
52   <string>iPhone10,4</string>
53   <string>iPhone12,8</string>
54   <string>iPhone9,1</string>
55   <string>iPhone9,3</string>
56 </array>
57 <key>DTAppStoreToolsBuild</key>
58 <string>13C88a</string>
59 <key>CFBundleName</key>
60 <string>Aweme</string>
61 <key>CFBundleSupportedPlatforms</key>
62 <array>
63   <string>iPhoneOS</string>
64 </array>
65 <key>NSCalendarUsageDescription</key>
66 <string>抖音需要获取您的日历权限，以便您正常使用促销提醒等服务</string>
67 <key>CFBundleDisplayName</key>
68 <string>抖音</string>
69 <key>UISupportedInterfaceOrientations-ipad</key>
70 <array>

```

- 解决办法：
 - 方法1：把当前机型，加到其支持列表中
 - 方法2：直接去掉机型限制
- 具体步骤

方法1

- 方法1：

解压 ipa , 得到 Payload 目录, 找到:

```
Payload/xxx.app/Info.plist
```

比如此处的:

```
Aweme抖音/已脱壳/Payload/Aweme.app/Info.plist
```

编辑: UISupportedDevices 部分, 加上自己的机型

此处最后是:

```
<key>UISupportedDevices</key>
<array>
  <string>iPhone9,1</string>
  <string>iPhone9,2</string>
  <string>iPhone9,3</string>
  <string>iPhone9,4</string>
  <string>iPhone10,1</string>
  <string>iPhone10,2</string>
  <string>iPhone10,3</string>
  <string>iPhone10,4</string>
  <string>iPhone10,5</string>
  <string>iPhone10,6</string>
  <string>iPhone11,2</string>
  <string>iPhone11,4</string>
  <string>iPhone11,6</string>
  <string>iPhone11,8</string>
  <string>iPhone12,1</string>
  <string>iPhone12,3</string>
  <string>iPhone12,5</string>
  <string>iPhone12,8</string>
  <string>iPhone13,1</string>
  <string>iPhone13,2</string>
  <string>iPhone13,3</string>
  <string>iPhone13,4</string>
  <string>iPhone14,2</string>
  <string>iPhone14,3</string>
  <string>iPhone14,4</string>
  <string>iPhone14,5</string>
</array>
```

注:

自己的机型, 可以去参考:

[Models - The iPhone Wiki](#)

比如:

```
iPhone7P 是 iPhone9,2 (另外: 美版是 iPhone9,4 )
```

方法2

- 方法2:

- 直接把 Info.plist 中的 UISupportedDevices 的部分，去掉。
 - 注：未验证是否有效，估计是有效的。

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:
2024-07-17 11:37:46

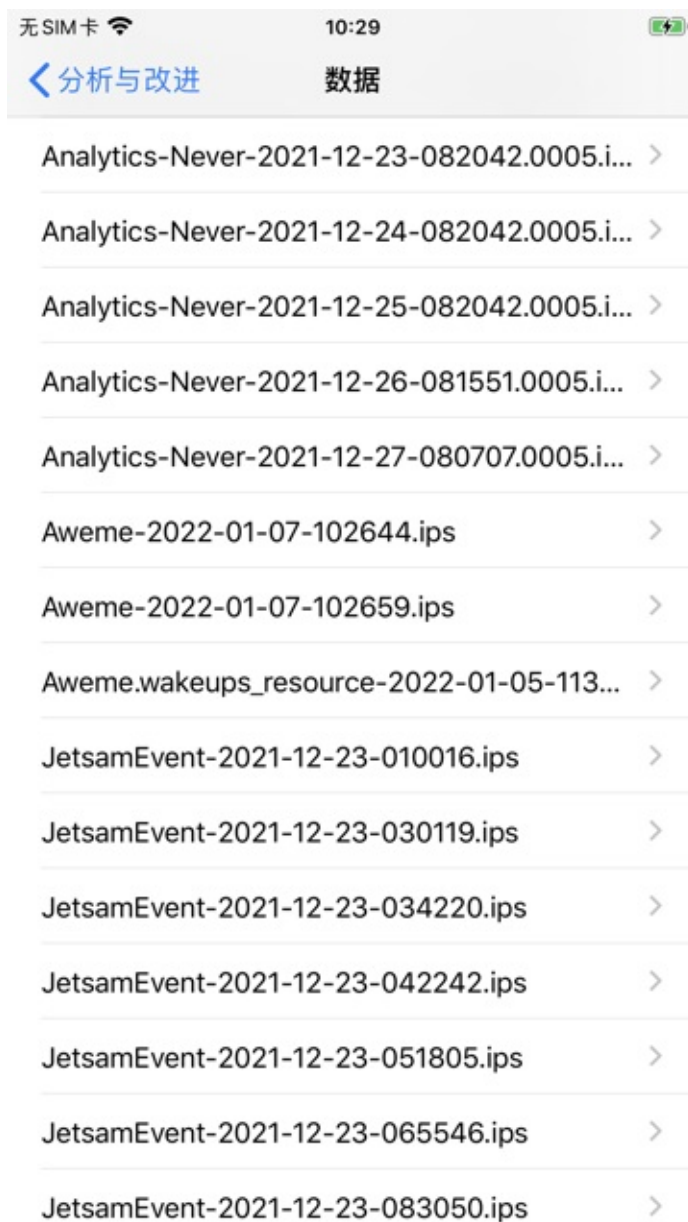
app启动后崩溃

- 现象：用frida-ios-dump砸壳后的app，启动后就崩溃
- 原因
 - 其实有多种可能
- 思路
 - 可以通过找app崩溃日志，而找到，具体错误的现象和找出背后的根本原因

通过ips崩溃日志找崩溃原因

举例：

抖音启动就闪退崩溃，此时去找crash崩溃日志：



打开对应的，Aweme的崩溃日志文件：

- Aweme-2022-01-07-102659.ips

o

```
{ "app_name": "Aweme", "timestamp": "2022-01-07 10:26:59.00 +0800", "app_version": "18.9.0", "slice_uuid": "31ed6d91-1868-36f5-89b8-c39fbf7d01e3", "adam_id": 0, "build_version": "189034", "bundleID": "com.ss.iphone.ugc.Aweme", "share_with_app_devs": 0, "is_first_party": 0, "bug_type": "109", "os_version": "iPhone OS 13.4.1 (17E262)", "incident_id": "C446C22E-347A-4340-8D68-637187E331B4", "name": "Aweme" }  
Incident Identifier: C446C22E-347A-4340-8D68-637187E331B4  
CrashReporter Key:   17234ceb2c5be537d1971110d8a3263466bb1250  
Hardware Model:      iPhone9,2  
Process:              Aweme [8782]  
Path:                 /private/var/containers/Bundle/Application/9AB25481-0AD3-435C-A02E-68F9623535BB/Aweme.app/Aweme  
Identifier:           com.ss.iphone.ugc.Aweme  
Version:              189034 (18.9.0)  
AppStoreTools:       13C88a  
Code Type:           ARM-64 (Native)  
Role:                 Foreground  
Parent Process:      launchd [1]
```

Coalition: com.ss.iphone.ugc.Aweme [4724]

Date/Time: 2022-01-07 10:26:59.5847 +0800
 Launch Time: 2022-01-07 10:26:58.4574 +0800
 OS Version: iPhone OS 13.4.1 (17E262)
 Release Type: User
 Baseband Version: 7.51.01
 Report Version: 104

Exception Type: EXC_CRASH (SIGABRT)
 Exception Codes: 0x0000000000000000, 0x0000000000000000
 Exception Note: EXC_CORPSE_NOTIFY
 Triggered by Thread: 0

Last Exception Backtrace:

(0x18d0ed5f0 0x18ce0fbcc 0x18d1430cc 0x18d142748 0x18cfc5edc 0x119d9a4dc 0x10ac42650 0x10ac418bc 0x10ac40b80 0x10ac40730 0x10ac33af8 0x10ac2036c 0x10bc2f940 0x10ac20080 0x10ac1fb48 0x10bc2e1c8 0x111713890 0x19118ea5c 0x1911907e8 0x191196084 0x19093d46c 0x190dec a38 0x19093df50 0x19093d9a4 0x19093dd7c 0x19093d63c 0x190941ad8 0x190d10dd4 0x190e05e7c 0x190941834 0x190e05d78 0x19094169c 0x1907b0f2c 0x1907afacc 0x1907b0c64 0x1911942d0 0x190d36284 0x19226720c 0x19228bd84 0x1922717ec 0x19228ba40 0x18cdb3524 0x18cd5c434 0x1922 b0440 0x1922b010c 0x1922b0634 0x18d06bb64 0x18d06bab6 0x18d06b244 0x18d066274 0x18d065c 34 0x1971af38c 0x19119822c 0x111714094 0x1049a7ca4 0x18ceed800)

Thread 0 name: Dispatch queue: com.apple.main-thread

Thread 0 Crashed:

0	libsystem_kernel.dylib	0x000000018cee2d88	0x18cebd000	+ 155016
1	libsystem_pthread.dylib	0x000000018cdfb1e8	0x18cdf9000	+ 8680
2	libsystem_c.dylib	0x000000018cd4e644	0x18ccdc000	+ 468548
3	libc++abi.dylib	0x000000018ceb6cc0	0x18cea4000	+ 76992
4	libc++abi.dylib	0x000000018cea8e10	0x18cea4000	+ 19984
5	libobjc.A.dylib	0x000000018ce0fe80	0x18ce0a000	+ 24192
6	libc++abi.dylib	0x000000018ceb614c	0x18cea4000	+ 74060
7	libc++abi.dylib	0x000000018ceb60e4	0x18cea4000	+ 73956
8	libdispatch.dylib	0x000000018cdb3538	0x18cd58000	+ 374072
9	libdispatch.dylib	0x000000018cd5c434	0x18cd58000	+ 17460
10	FrontBoardServices	0x00000001922b0440	0x19225b000	+ 349248
11	FrontBoardServices	0x00000001922b010c	0x19225b000	+ 348428
12	FrontBoardServices	0x00000001922b0634	0x19225b000	+ 349748
13	CoreFoundation	0x000000018d06bb64	0x18cfc3000	+ 691044
14	CoreFoundation	0x000000018d06bab6	0x18cfc3000	+ 690876
15	CoreFoundation	0x000000018d06b244	0x18cfc3000	+ 688708
16	CoreFoundation	0x000000018d066274	0x18cfc3000	+ 668276
17	CoreFoundation	0x000000018d065c34	0x18cfc3000	+ 666676
18	GraphicsServices	0x00000001971af38c	0x1971ac000	+ 13196
19	UIKitCore	0x000000019119822c	0x19076c000	+ 10666540
20	???	0x0000000111714094	0	+ 4587602068
21	Aweme	0x00000001049a7ca4	0x1049a0000	+ 31908
22	libdyld.dylib	0x000000018ceed800	0x18ceec000	+ 6144

Thread 1:

0	libsystem_pthread.dylib	0x000000018ce07738	0x18cdf9000	+ 59192
---	-------------------------	--------------------	-------------	---------

...



从中可以看出：

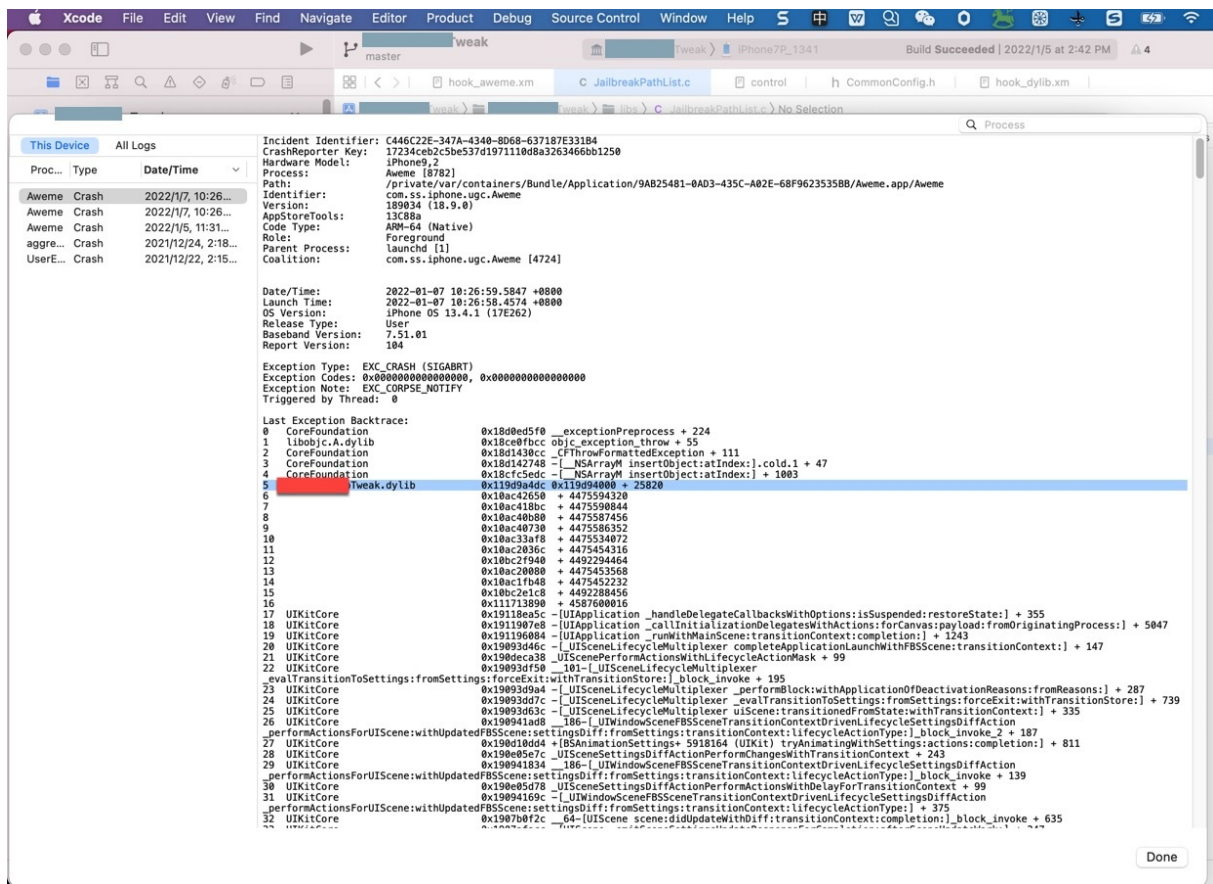
- 二进制文件：
 - `/private/var/containers/Bundle/Application/9AB25481-0AD3-435C-A02E-68F9623535BB/Aweme.app/Aweme`

注：多次尝试用：

- XCode->Window->Devices and Simulators-》 View Devices logs

◦

最后才看到，解析后的日志，带库（但仍没有解析出函数名）的：

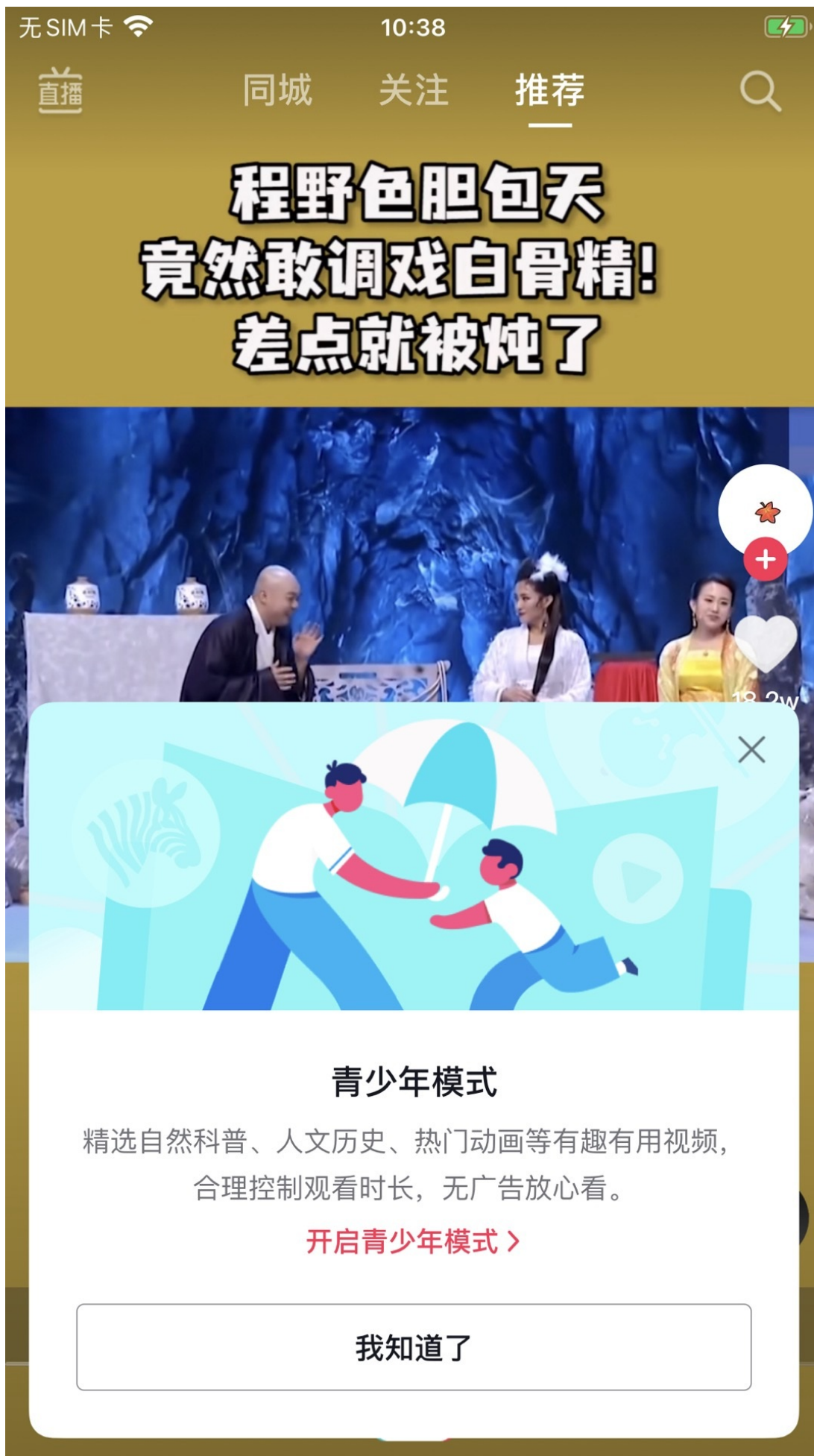


总之，确定是自己的插件导致的了。

重新安装一下反越狱检测插件试试

即可解决问题：

抖音可以正常启动了：



反推：

此处crash是由于之前的代码，hook了https的SSL证书，但是新iPhone测试机中没有Charles证书，导致的崩溃。

之前另外一个iPhone测试机已解决了，但是此处iPhone没安装新版插件。

重新安装修复后的版本：

```

19
20 // to fix Charles capture https show Unknown issue
21 // https://bbs.pediy.com/thread-270700.htm
22 // https://iosre.com/t/topic/20202/46
23
24 #define CHARLES_CERT_FILE @"Library/PreferenceLoader/Preferences/charles/charles-ssl-proxying-certificate.cer"
25
26 %hook TTNetworkManagerChromium
27
28 - (NSArray *)ServerCertificate {
29     iosLogDebug(@"%s", "");
30     NSArray* serverCertList = %orig();
31     iosLogDebug(@"serverCertList=%{(public)@}", serverCertList);
32
33     /// NSString *serverCertListStr = [NSArray nsStrListToStr:serverCertList isSortList:FALSE isAddIndexPrefix:TRUE];
34     /// NSString *serverCertListStr = [CrifanLibHookiOS nsStrListToStr:serverCertList isSortList:FALSE isAddIndexPrefix:TRUE];
35     iosLogInfo(@"serverCertListStr=%{(public)@}", serverCertListStr);
36
37     /// return nil;
38     return serverCertList;
39
40     NSMutableArray* newCertList = [NSMutableArray arrayWithArray: serverCertList];
41     iosLogDebug(@"newCertList=%{(public)@}, newCertList.count=%{(public)lu}", newCertList, [newCertList count]);
42     NSString *certResourcePath = CHARLES_CERT_FILE;
43     iosLogDebug(@"certResourcePath=%{(public)@}", certResourcePath);
44
45     NSFileManager *defaultManager = [NSFileManager defaultManager];
46     BOOL isExistedCert = [defaultManager fileExistsAtPath: certResourcePath];
47     iosLogInfo(@"isExistedCert=%s", boolToStr(isExistedCert));
48     if (isExistedCert) {
49         NSData *certP12Data = [NSData dataWithContentsOfFile: certResourcePath];
50         iosLogDebug(@"certP12Data=%{(public)@}", certP12Data);
51         [newCertList addObject: certP12Data];
52         iosLogDebug(@"newCertList=%{(public)@}, newCertList.count=%{(public)lu}", newCertList, [newCertList count]);
53     }
54     NSMutableArray* retNewCertList = [newCertList copy];
55     iosLogDebug(@"retNewCertList=%{(public)@}, retNewCertList);
56     return retNewCertList;
57 }
58
59 %end

```

即可解决问题。

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：
2024-07-17 11:38:18

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:
2022-03-17 20:39:28

参考资料

- 【已解决】 iPhone中tiktok国际版砸壳出ipa文件
- 【已解决】 iOS版抖音的砸壳脱壳
- 【已解决】 Mac中用frida-ios-dump给iOS版抖音脱壳出ipa
- 【已解决】 用frida-ios-dump给17.8.0版本抖音砸壳ipa
- 【已解决】 Mac中用frida-ios-dump去砸壳出YouTube的ipa文件
- 【已解决】 iPhone中查看已安装app的包名
- 【已解决】 用frida-ios-dump砸壳报错：Failed to enumerate applications unable to communicate with remote frida-server
- 【已解决】 iPhone中Cydia中安装升级最新版的16.0.2的Frida
- 【已解决】 frida-ios-dump砸壳报错：ModuleNotFoundError No module named frida
- 【已解决】 iOS的二进制用otool看不到crypt以及MachOView看不到LC_ENCRYPTION_INFO_64字段
- 【已解决】 frida-ios-dump砸壳抖音卡死无进度：0.00B 00:00
- 【已解决】 脱壳后抖音app启动就崩溃闪退
- 【已解决】 砸壳后抖音ipa安装失败：DeviceNotSupportedByThinning
-
- [iOS逆向开发：iPhone越狱](#)
- [安装Frida · 逆向调试利器：Frida](#)
-
- [frida-ps | Frida · A world-class dynamic instrumentation toolkit](#)
- [\[iOS\]判断ipa是否脱壳_风浅月明的博客-CSDN博客_ipa脱壳](#)
- [\[iOS逆向\]18、砸壳 - 简书 \(jianshu.com\)](#)
- [十、iOS逆向之《越狱砸壳/ipa脱壳》 - 简书 \(jianshu.com\)](#)
- [iOS逆向：App脱壳/ipa破解-华盟网 \(77169.net\)](#)
- [iOS逆向攻防实战 - 掘金 \(juejin.cn\)](#)
- [Models - The iPhone Wiki](#)
-

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:
2024-07-17 11:17:13