目录

iOS逆向：管理app和插件

- 最新版本：`v0.7`
- 更新时间：`20240319`

简介

整理iOS越狱后，iOS逆向app期间，如何管理app和相关越狱插件的方式和常见问题及解决办法。

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_manage_app_tweak: iOS逆向：管理app和插件

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：管理app和插件 book.crifan.org
- iOS逆向：管理app和插件 crifan.github.io

离线下载阅读

- iOS逆向：管理app和插件 PDF
- iOS逆向：管理app和插件 ePub
- iOS逆向：管理app和插件 Mobi

版权和用途说明

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

概览

iOS越狱后，iOS逆向期间，常会涉及到安装iOS的app和各种越狱插件。

其中：

- （待安装的）主要形式
  - app：`.ipa` 文件
    - `ipa` =**IP**hone **A**pplication
  - （越狱）插件：`.deb` 文件

下面详细介绍。

管理app

安装app

iOS越狱后，安装iOS的app（主要是 `ipa` 文件）的主要方式有：

- 电脑端
  - 爱思助手
  - MonkeyDev（调试并安装ipa）
  - Xcode
  - ideviceinstaller
- 手机端
  - Filza
  - 免签安装
    - TrollStore
    - Sideloadly
- 其他
  - iTools

免签安装ipa文件

有些越狱工具，比如 `XinaA15` ，推荐安装方式是： `TrollStore` ，其属于：免签安装ipa的工具。

- 免签安装ipa文件
  - 背景：iOS的app的安装，需要官方有效的签名才可以。
    - 但是个人版开发者账号，默认只有7天有效期
      - 过期后，需要重新签名，很是麻烦
  - 所以：出现了很多，相关的免签名，或者是辅助的sideloe的方式，去安装ipa的工具
  - 常见免签安装ipa的工具
    - `TrollStore`
    - `Sideloadly`

Filza

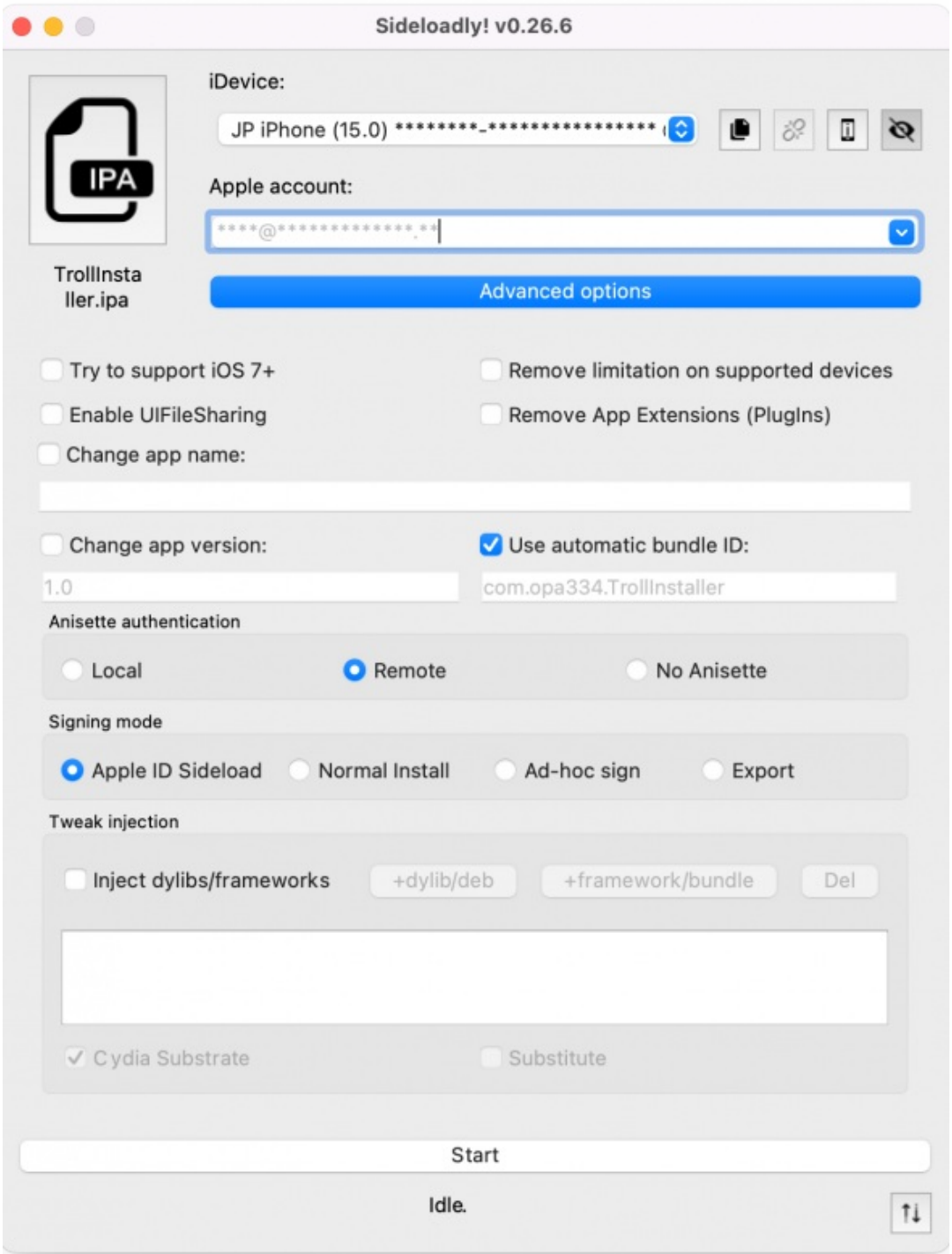
爱思助手

TrollStore

- `TrollStore`
  - 中文名： `巨魔` = `巨魔商店`
  - 作用：永久签名工具
    - 让你可以直接安装各种ipa文件
      - 它可以在不越狱的条件随意安装IPA，且不依赖证书就能做到“永久签名”
    - 内部逻辑：绕过iOS系统的限制
      - 普通ipa，签名无法通过校验，无法安装
        - 或者是用自己的AppleID签名，但是过了默认的7天限制，需要重新签名-》很麻烦
    - 效果：使用TrollStore我们可以随便签名各种修改版的IPA、应用多开等等
      - 只要系统满足安装要求，那就不用再依赖证书，安装的IPA“永久有效”
  - 作者： `opa334`
  - logo图标
    - 

  - 官网
    - 官方的github
      - opa334/TrollStore: Jailed iOS app that can install IPAs permanently with arbitary entitlements and root helpers because it trolls Apple (github.com)
        - https://github.com/opa334/TrollStore
    - 疑似的官网
      - TrollStore - Permanently Sideload Any IPAs For Free
        - https://trollstore.app
  - 安装
    - 概述：多种安装方式
      - 通过iPhone中的Safari浏览器安装
      - 通过ipa安装
      - 等等
    - 文档
      - https://github.com/opa334/TrollStore 中的： `Installation Guides`
        - 比如适用于此处 `iOS 15.1` 的 `iPhone 11` 的
          - TrollStore/install_trollhelperota_ios15.md at main · opa334/TrollStore · GitHub

iPhone中安装TrollStore

- 有多种安装方式
  - 通过 浏览器 安装TrollStore
    - iPhone中，用Safari打开链接：https://api.jailbreaks.app/troll
    - 具体步骤详见
      - TrollStore/install_trollhelperota_ios15.md at main · opa334/TrollStore · GitHub
  - 用 `Sideloadly` 安装TrollStore
    - 对应安装包：`TrollStore Installer IPA` = `TrollInstaller.ipa`
    - 

此处最后的选择是：

- 没用：Sideloadly去安装TrollStore的ipa

    - 因为TrollStore的ipa是旧版本，而另外缺找不到最新版本的TrollStore的ipa
        - 估计是：安装了旧版本TrollStore后，也可以通过OTA升级到最新版，但是懒得去弄
- 改用：参考官网github文档，去用Safari浏览器去安装TrollStore

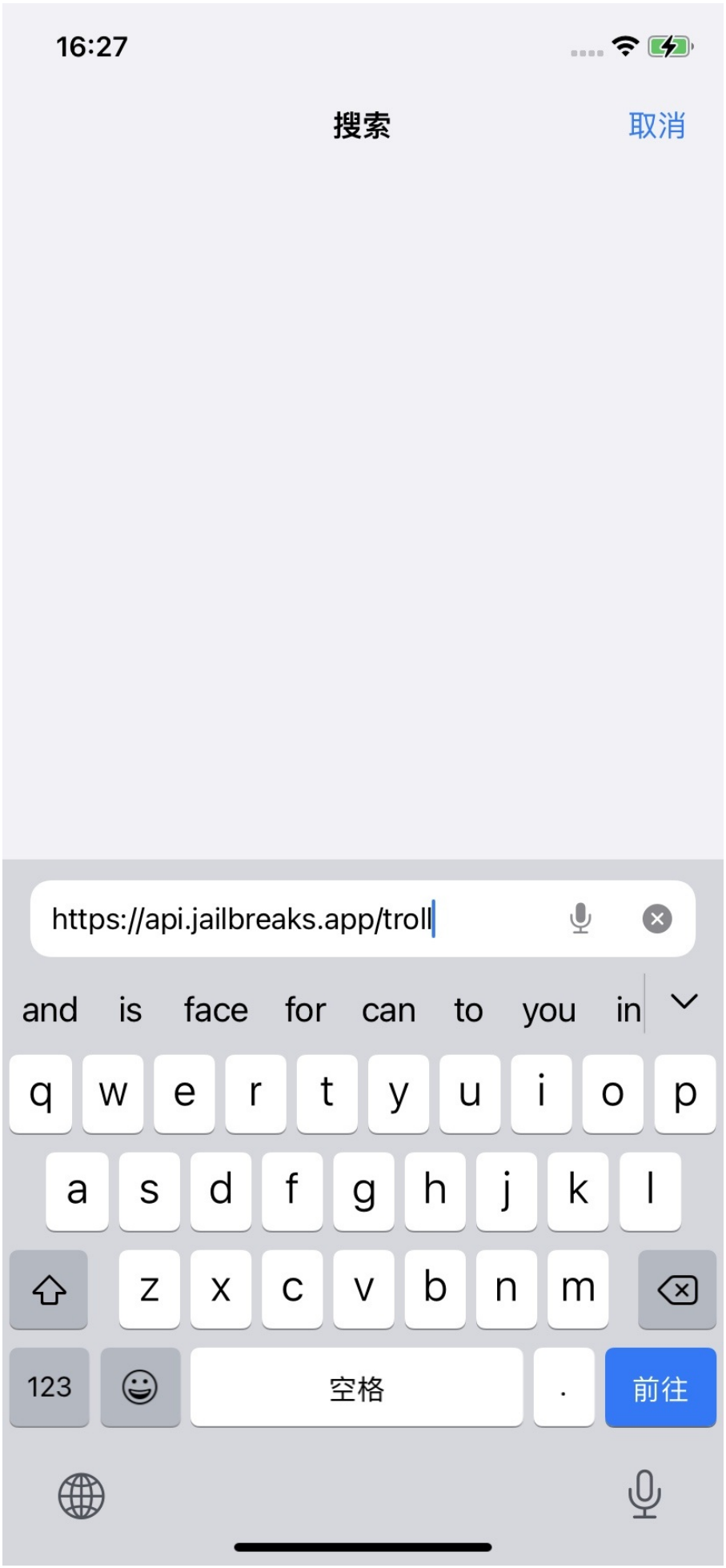
iPhone11中用Safari浏览器去安装TrollStore

核心步骤

iPhone->Safari浏览器-》打开地址 https://api.jailbreaks.app/troll -》“在iTunes中打开此页” 的弹框中：打开 -》“jailbreak.app想要安装TrollHelper”的弹框中：安装 -》桌面出现app图标JB，显示：正在安装 ->桌面上新增app：GTA Car Tracker -》点击进入GTA Car Tracker-》app标题是TrollStore Helper -》点击Install TrollStore-》稍等一会，iPhone重启-》桌面上出现：TrollStore

详细解释

- iPhone->Safari浏览器-》打开地址 https://api.jailbreaks.app/troll
    -


16:27
搜索
取消
https://api.jailbreaks.app/troll
and is face for can to you in
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
空格
.
前往

- -》“在iTunes中打开此页”？弹框中：打开
  -


16:27
在“iTunes”中打开此页?
取消
打开
搜索或输入网站名称

- -》“jailbreak.app想要安装TrollHelper”的弹框中：安装
  -


16:27
网页版
Bai du 百度
输入搜索词
百度一下
YY直播
百变主播 颜艺俱佳
超多精彩 尽在YY
立即观看
“jailbreaks.app”想要安装
“TrollHelper”
取消
安装
置顶
专题片
置顶
央视财经
在“球王”贝利灵柩前与他人自拍，国际足联主席因凡蒂诺…
红星新闻
2022年五个反腐细节
鲁网
大小
baidu.com

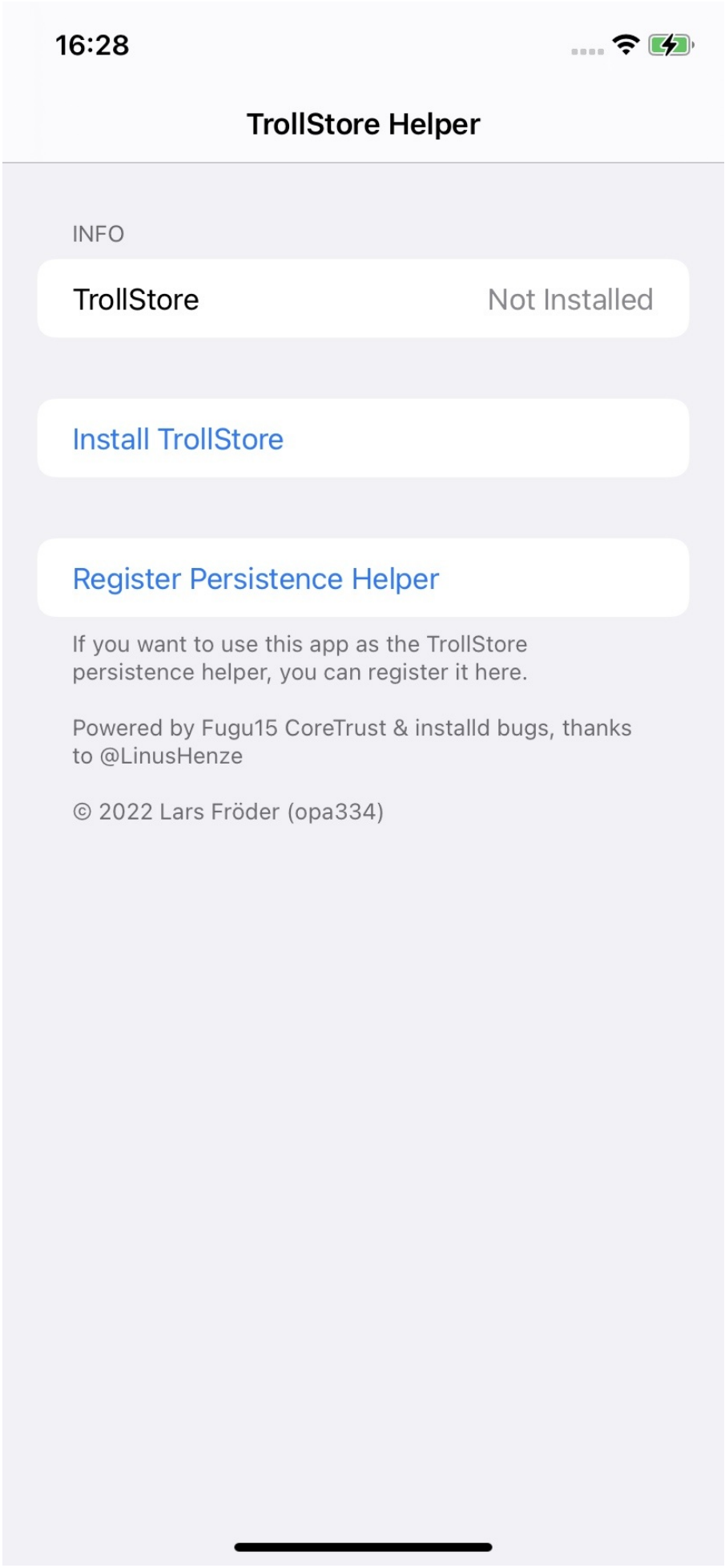
- -》桌面出现app图标JB，显示：正在安装
  -


16:27
天气
查找
快捷指令
家庭
通讯录
文件
股市
翻译
图书
iTunes Store
Watch
提示
实用工具
爱思极速版
计算器
Apple Store
电话
正在安装...
1

- ->桌面上新增app：GTA Car Tracker
  -


16:27
天气
查找
快捷指令
家庭
通讯录
文件
股市
翻译
图书
iTunes Store
Watch
提示
实用工具
爱思极速版
计算器
Apple Store
电话
GTA Car Tracker
GTA CAR TRACKER
1

- -》点击进入GTA Car Tracker-》app标题是TrollStore Helper
  -


16:28
TrollStore Helper
INFO
TrollStore
Not Installed
Install TrollStore
Register Persistence Helper
If you want to use this app as the TrollStore persistence helper, you can register it here.
Powered by Fugu15 CoreTrust & installd bugs, thanks to @LinusHenze
© 2022 Lars Fröder (opa334)

- -》点击Install TrollStore-》稍等一会，iPhone重启-》桌面上出现：TrollStore
  -


16:28
天气
查找
快捷指令
家庭
通讯录
文件
股市
翻译
图书
iTunes Store
Watch
提示
实用工具
爱思极速版
计算器
Apple Store
电话
GTA Car Tracker
TrollStore
1

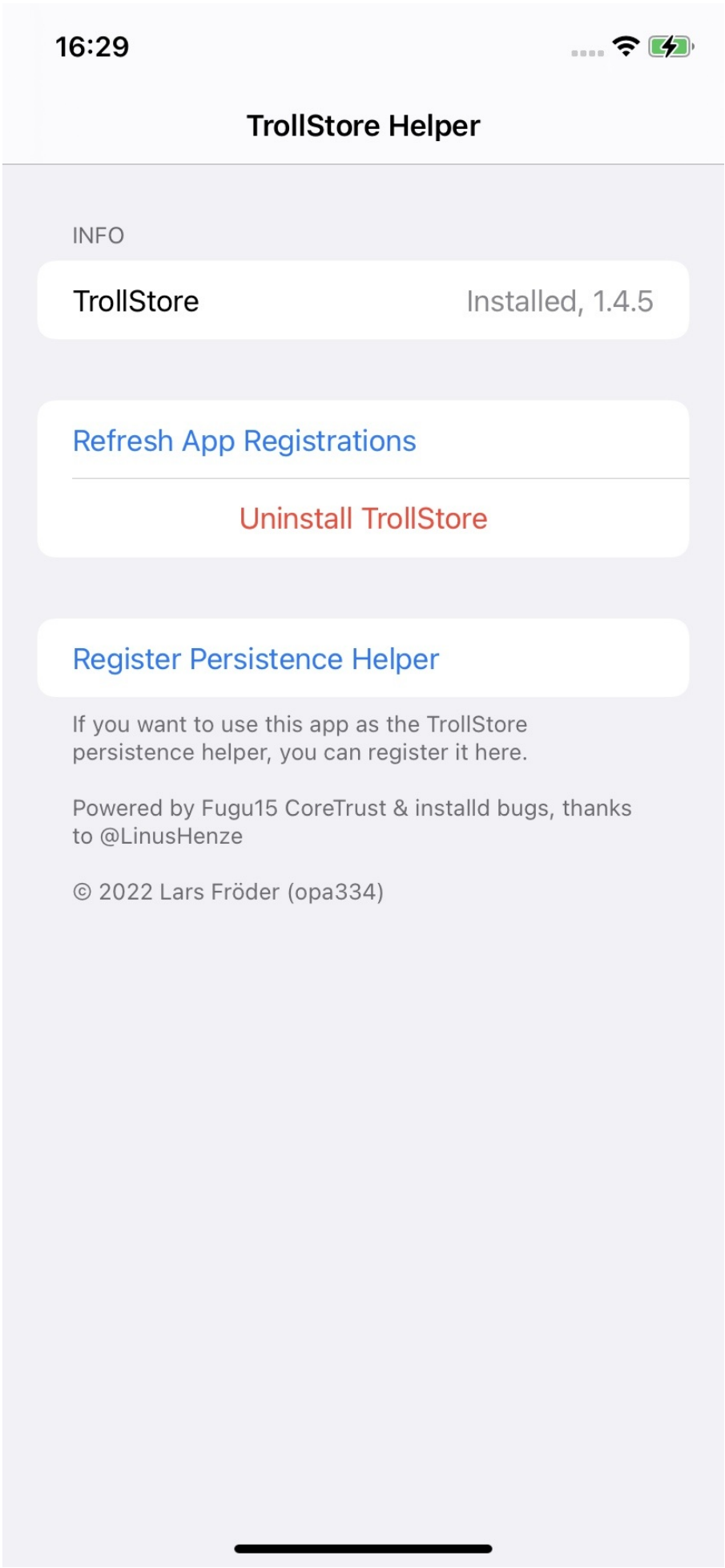
安装TrollStore后

把TrollStore设置为持续存在

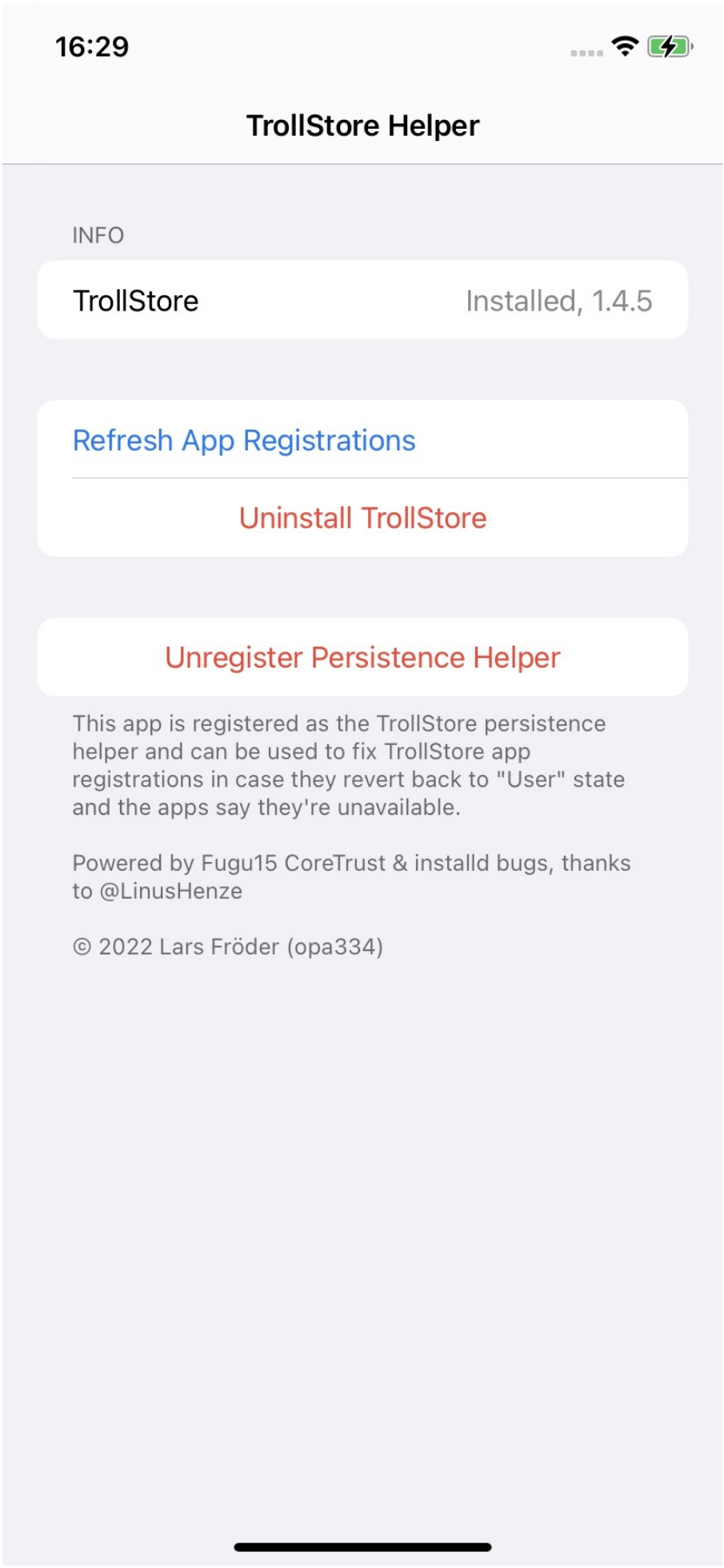
在iPhone中安装了TrollStore后，为了使后续系统图标刷新等操作，不会导致TrollStore无法正常使用，比如变成User用户模式或打不开

所以需要去：

- 把TrollStore设置为持续存在 `Persistence`
  - 核心思路：找个（自己平时不用的）系统app 或 （比如此处）就用上面的 `GTA Car Tracker` ，去设置为 `Persistence Helper`
  - 具体步骤：点击 `GTA Car Tracker`
    - -》 `Register Persistence Helper`
      -


16:29
TrollStore Helper
INFO
TrollStore
Installed, 1.4.5
Refresh App Registrations
Uninstall TrollStore
Register Persistence Helper
If you want to use this app as the TrollStore persistence helper, you can register it here.
Powered by Fugu15 CoreTrust & installd bugs, thanks to @LinusHenze
© 2022 Lars Fröder (opa334)

- 注册后的效果是
  -

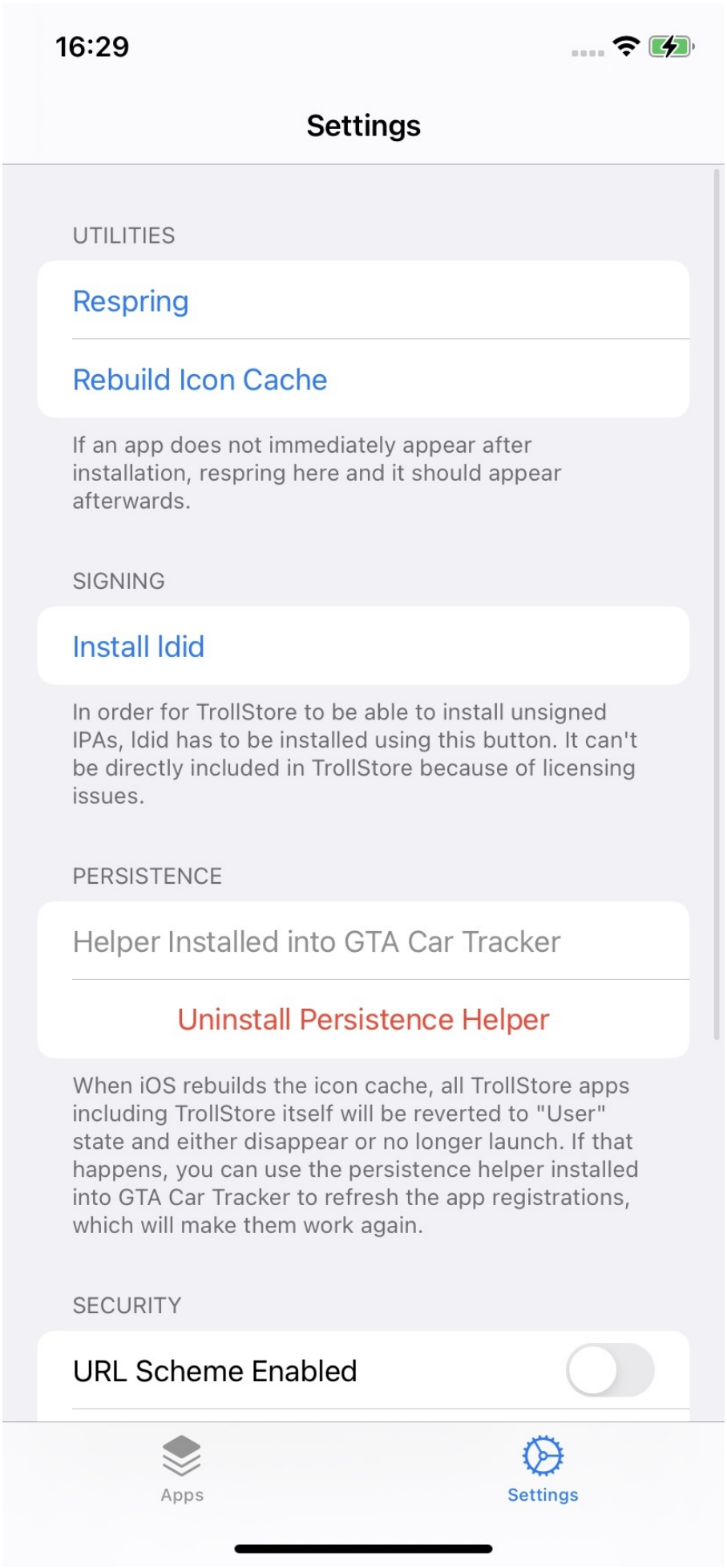

16:29
TrollStore Helper
INFO
TrollStore
Installed, 1.4.5
Refresh App Registrations
Uninstall TrollStore
Unregister Persistence Helper
This app is registered as the TrollStore persistence helper and can be used to fix TrollStore app registrations in case they revert back to "User" state and the apps say they're unavailable.
Powered by Fugu15 CoreTrust & installd bugs, thanks to @LinusHenze
© 2022 Lars Fröder (opa334)

    - 详细过程参考官网文档：
        - TrollStore/install_trollhelperota_ios15.md at main · opa334/TrollStore · GitHub
    - 注意：
        - 后续不能删除 `TrollStore Helper` ==此处的 `GTA Car Tracker`
            - 因为：上面通过GTA Car Tracker == TrollStore Helper，点击了其中的：Register Persistence Helper，意思是把GTA Car Tracker作为了一个系统的app，用于后续TrollStore的永久保持的功能，所以以后不能删除此app：GTA Car Tracker

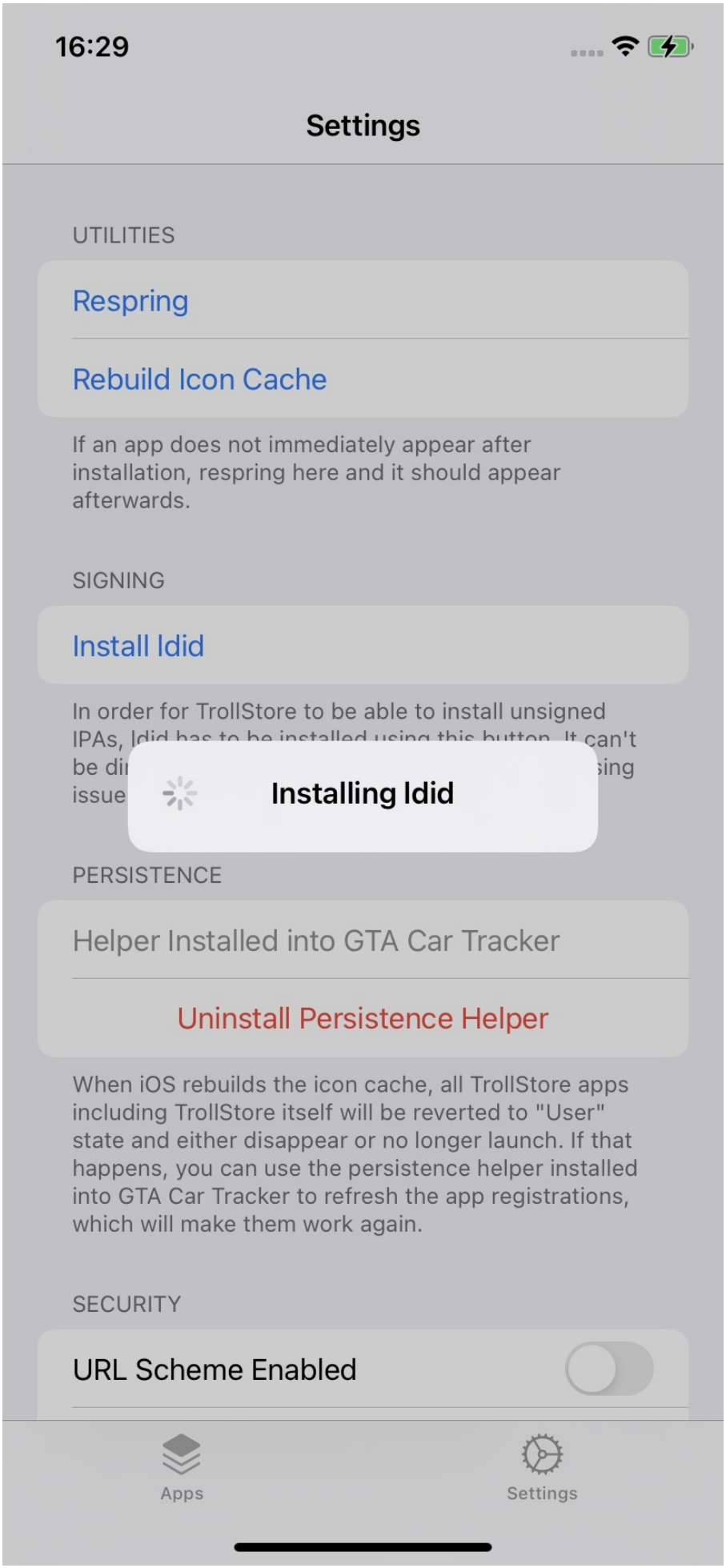
初始化配置TrollStore

安装完毕TrollStore后，还需要：

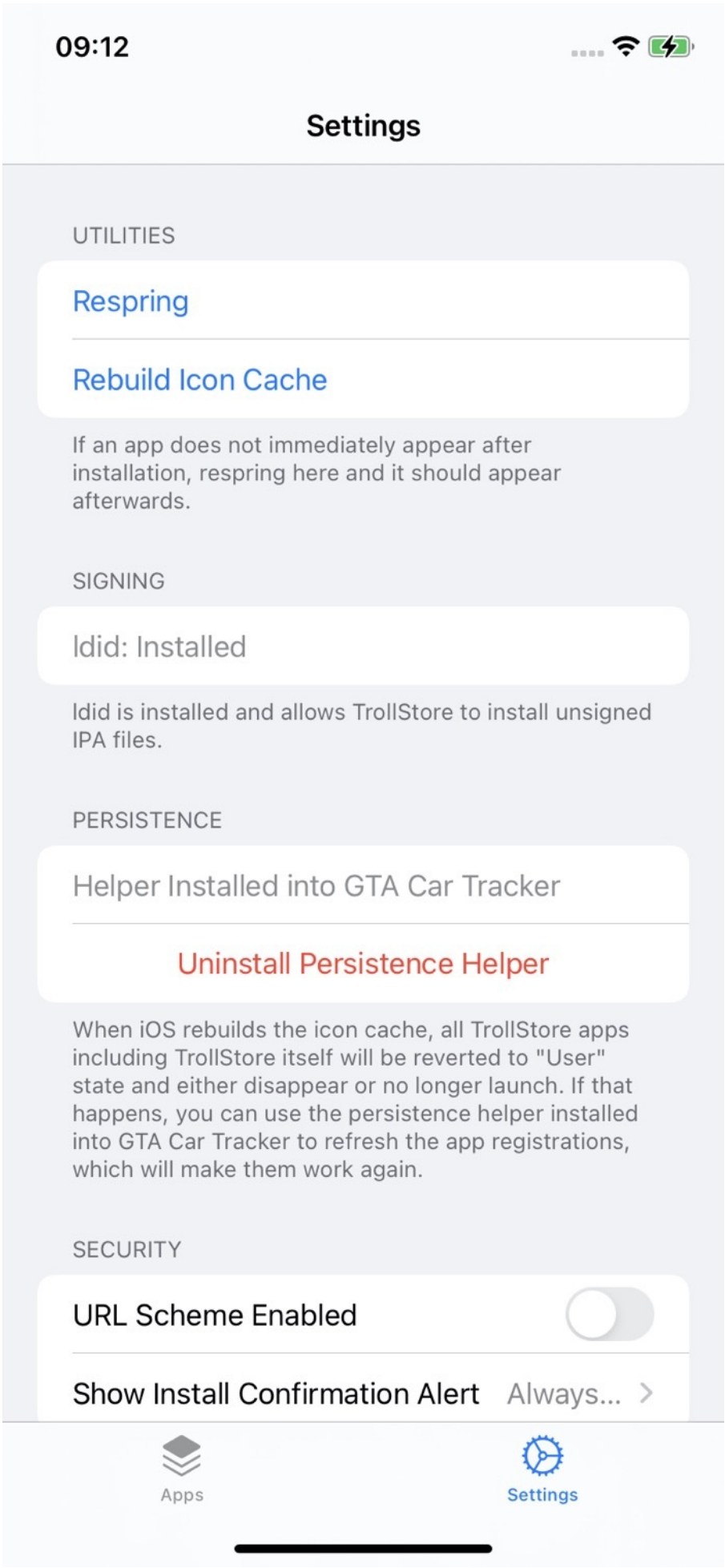
- 初始化配置TrollStore
    - 核心步骤：TrollStore -> Settings -> Install ldid
    - 详细步骤
        - TrollStore-> Settings -> Install ldid
            -


16:29
Settings
UTILITIES
Respring
Rebuild Icon Cache
If an app does not immediately appear after installation, respring here and it should appear afterwards.
SIGNING
Install ldid
In order for TrollStore to be able to install unsigned IPAs, ldid has to be installed using this button. It can't be directly included in TrollStore because of licensing issues.
PERSISTENCE
Helper Installed into GTA Car Tracker
Uninstall Persistence Helper
When iOS rebuilds the icon cache, all TrollStore apps including TrollStore itself will be reverted to "User" state and either disappear or no longer launch. If that happens, you can use the persistence helper installed into GTA Car Tracker to refresh the app registrations, which will make them work again.
SECURITY
URL Scheme Enabled
Apps
Settings

- 显示正在安装：`Installing ldid`
  -


16:29
Settings
UTILITIES
Respring
Rebuild Icon Cache
If an app does not immediately appear after installation, respring here and it should appear afterwards.
SIGNING
Install ldid
In order for TrollStore to be able to install unsigned IPAs, ldid has to be installed using this button. It can't be di sing issue
Installing ldid
PERSISTENCE
Helper Installed into GTA Car Tracker
Uninstall Persistence Helper
When iOS rebuilds the icon cache, all TrollStore apps including TrollStore itself will be reverted to "User" state and either disappear or no longer launch. If that happens, you can use the persistence helper installed into GTA Car Tracker to refresh the app registrations, which will make them work again.
SECURITY
URL Scheme Enabled
Apps
Settings

- ldid安装完毕后
  -


09:12
Settings
UTILITIES
Respring
Rebuild Icon Cache
If an app does not immediately appear after installation, respring here and it should appear afterwards.
SIGNING
ldid: Installed
ldid is installed and allows TrollStore to install unsigned IPA files.
PERSISTENCE
Helper Installed into GTA Car Tracker
Uninstall Persistence Helper
When iOS rebuilds the icon cache, all TrollStore apps including TrollStore itself will be reverted to "User" state and either disappear or no longer launch. If that happens, you can use the persistence helper installed into GTA Car Tracker to refresh the app registrations, which will make them work again.
SECURITY
URL Scheme Enabled
Show Install Confirmation Alert
Always...
Apps
Settings

- 会看到文字提示：`ldid is installed and allows TrollStore to install unsigned IPA files`

常见错误

Error downloading ldid Code 1001 请求超时

如果 `installing ldid` 期间：

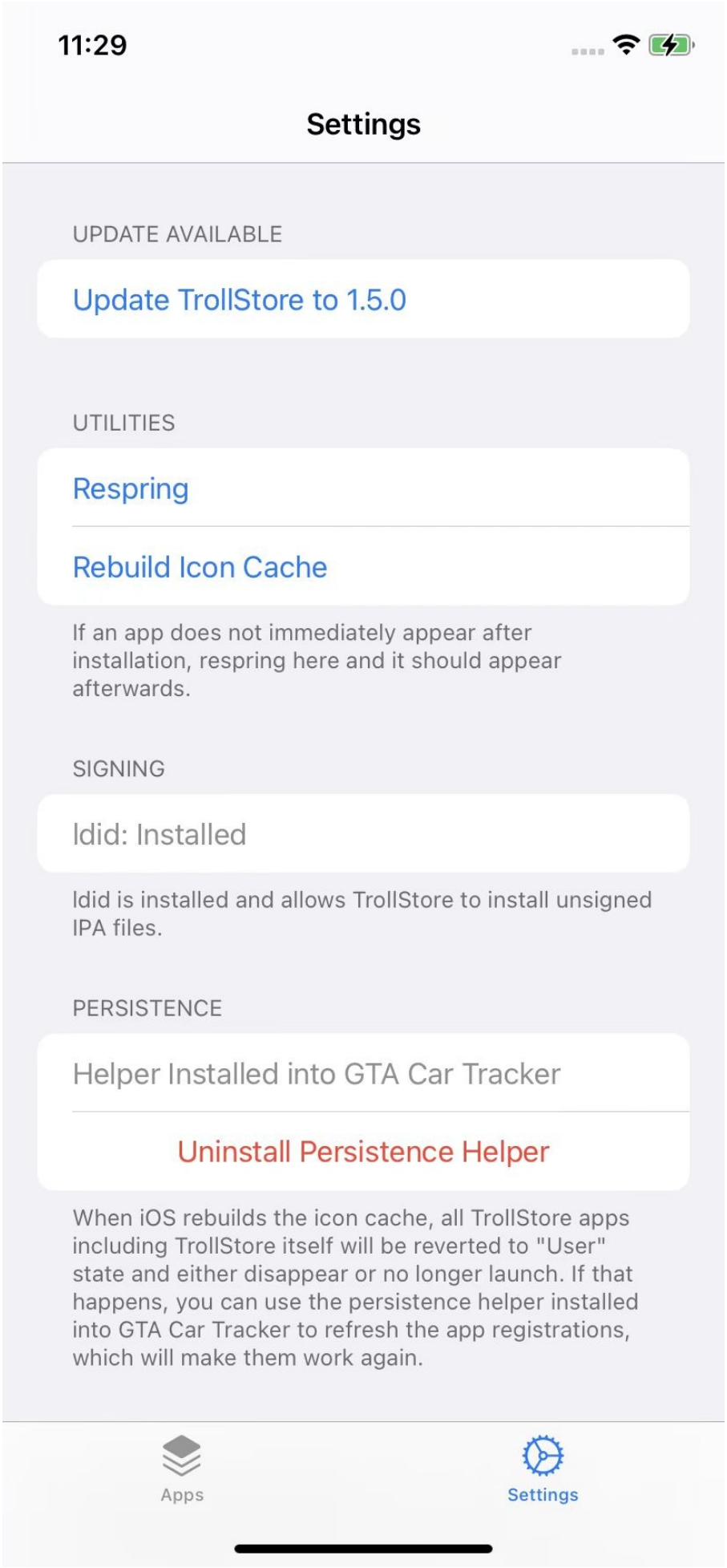
- 报错：Error downloading ldid Code 1001 请求超时
  -


16:30
Settings
UTILITIES
Error
Error downloading ldid: Error Domain=NSURLErrorDomain Code=-1001 "请求超时。" UserInfo={_kCFStreamErrorCodeKey=-2102, NSUnderlyingError=0x281e55ec0 {Error Domain=kCFErrorDomainCFNetwork Code=-1001 "(null)" UserInfo={_kCFStreamErrorCodeKey=-2102, _kCFStreamErrorDomainKey=4}}, _NSURLErrorFailingURLSessionTaskErrorKey=LocalDownloadTask <55DCDA91-DF7B-4F91-8881-7C8F74864595>.<2>, _NSURLErrorRelatedURLSessionTaskErrorKey=("LocalDownloadTask <55DCDA91-DF7B-4F91-8881-7C8F74864595>.<2>"), NSLocalizedDescription=请求超时。, NSErrorFailingURLStringKey=https://github.com/opa334/ldid/releases/download/v2.1.5-procursus5/ldid, NSErrorFailingURLKey=https://github.com/opa334/ldid/releases/download/v2.1.5-procursus5/ldid, _kCFStreamErrorDomainKey=4}
Close
URL Scheme Enabled
Apps
Settings

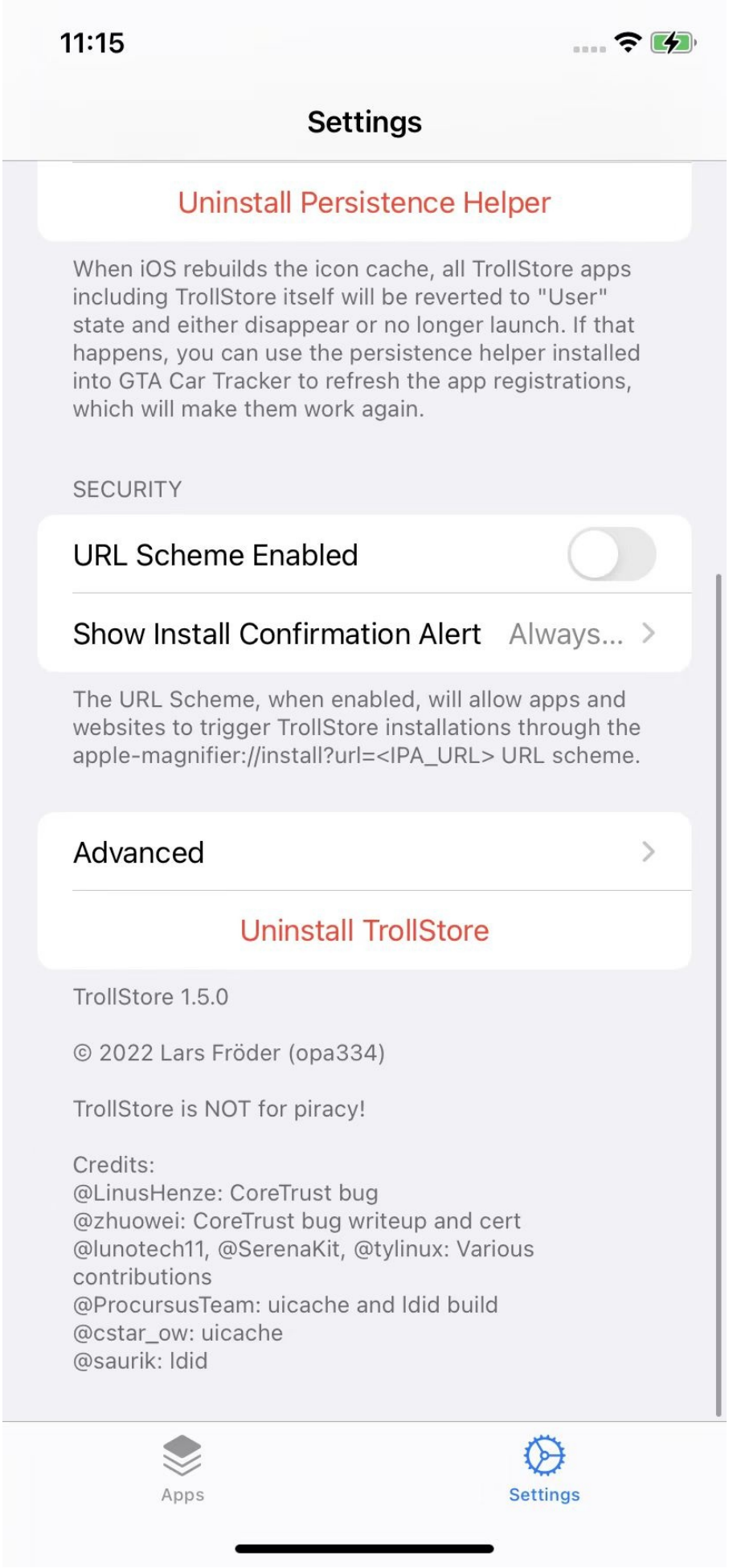
- 原因：无法访问外网（https://github.com/xxx）
- 解决办法：用Shadowrocket小火箭，加上代理，确保翻墙后可以正常上外网
  - 详见
    - 【已解决】给iOS 15.1的iPhone 11去翻墙科学上网安装代理

升级TrollStore

- 升级TrollStore
  - TrollStore中如果有新版本，则会有对应新版本提示
    - 此处的：Update TrollStore to 1.5.0
      -

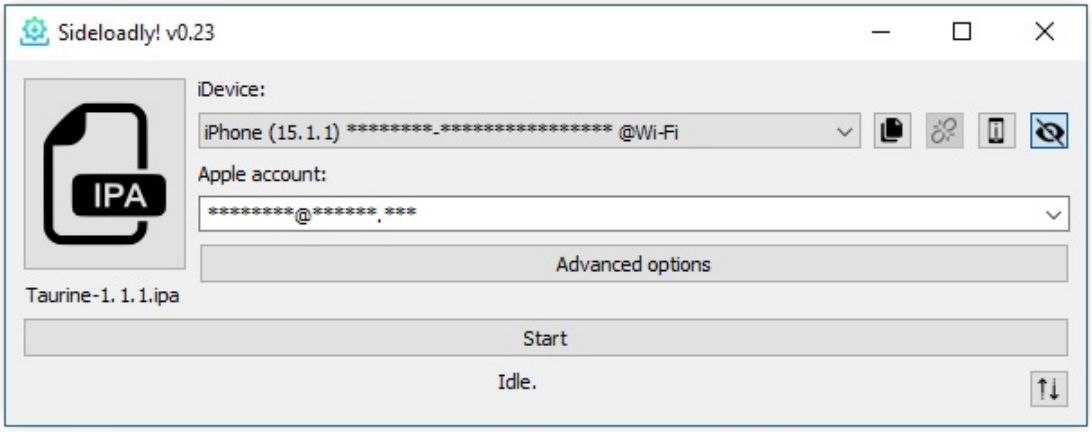

11:29
Settings
UPDATE AVAILABLE
Update TrollStore to 1.5.0
UTILITIES
Respring
Rebuild Icon Cache
If an app does not immediately appear after installation, respring here and it should appear afterwards.
SIGNING
ldid: Installed
ldid is installed and allows TrollStore to install unsigned IPA files.
PERSISTENCE
Helper Installed into GTA Car Tracker
Uninstall Persistence Helper
When iOS rebuilds the icon cache, all TrollStore apps including TrollStore itself will be reverted to "User" state and either disappear or no longer launch. If that happens, you can use the persistence helper installed into GTA Car Tracker to refresh the app registrations, which will make them work again.
Apps
Settings

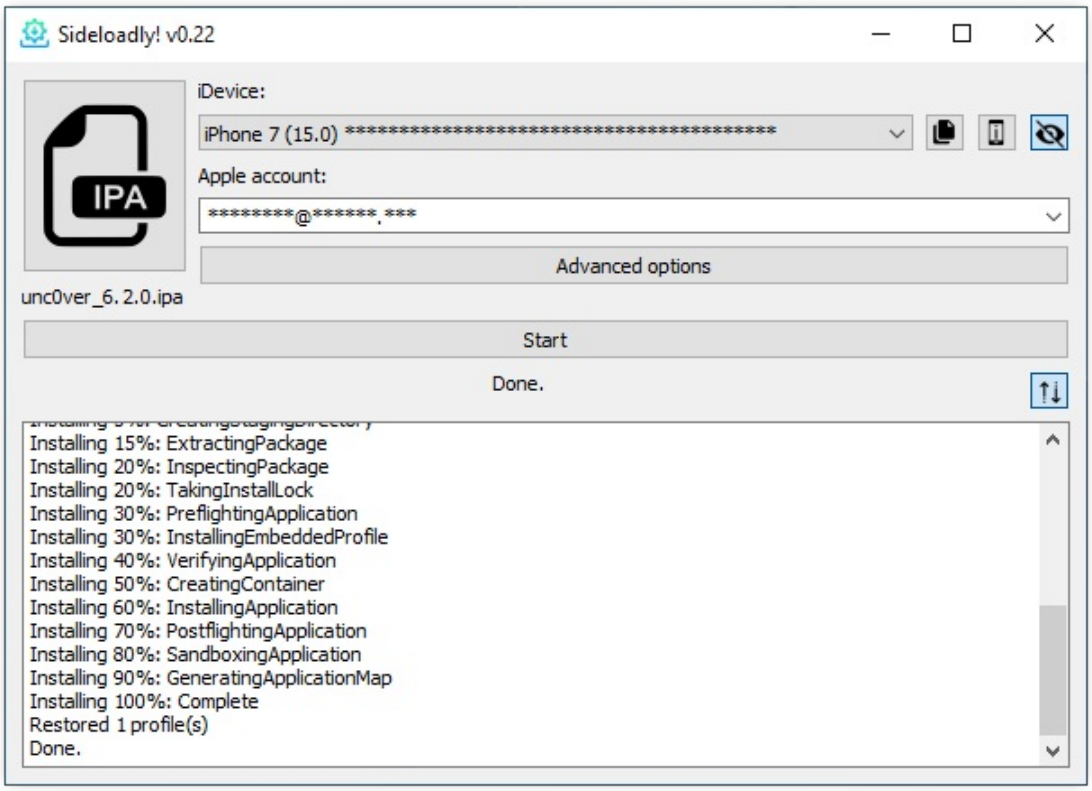
- 点击继续安装即可
  - 注：同理，确保能上外网，否则会出现下载失败的情况
- 更新后：1.5.0
  -

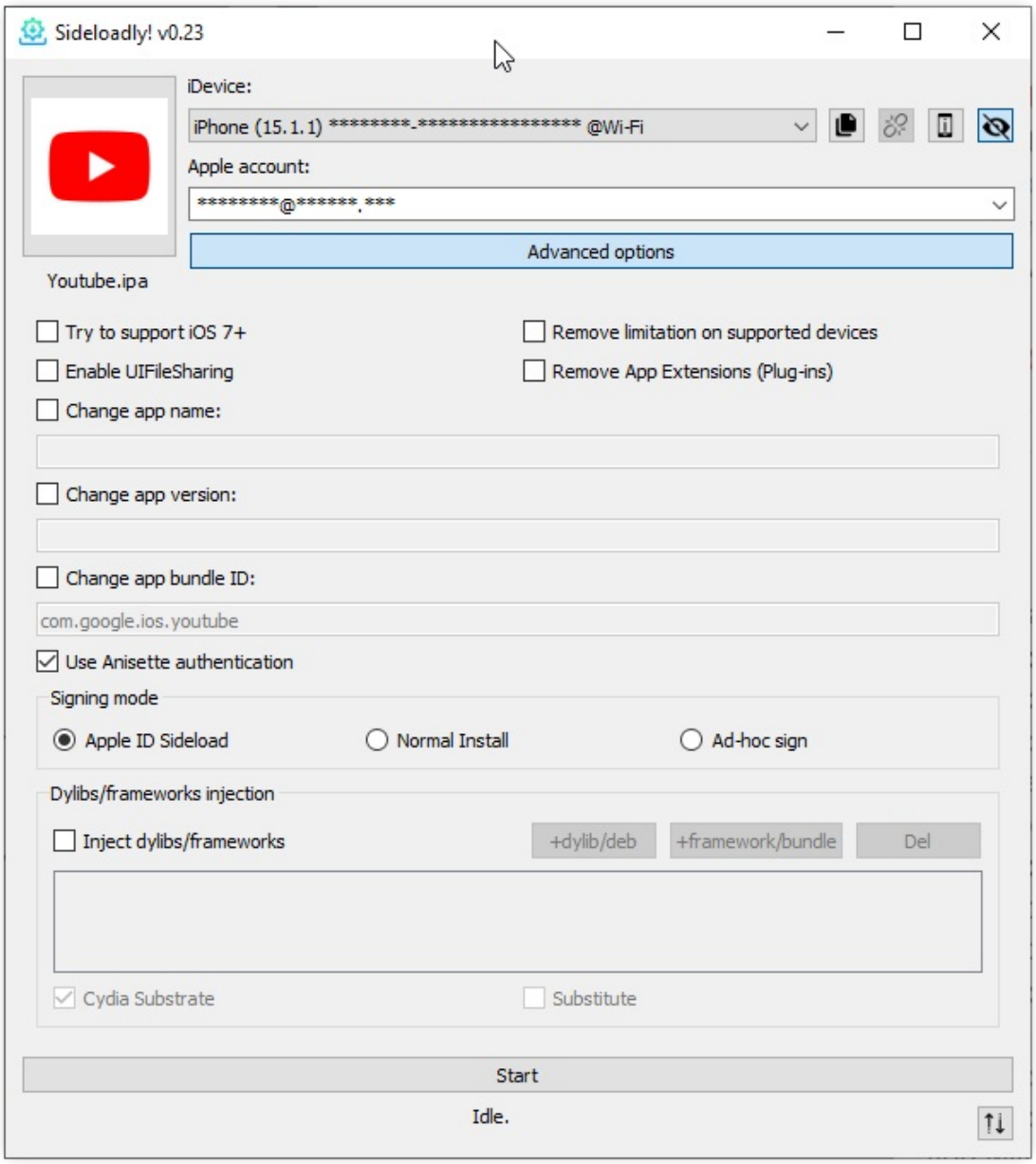

11:15
Settings
Uninstall Persistence Helper
When iOS rebuilds the icon cache, all TrollStore apps including TrollStore itself will be reverted to "User" state and either disappear or no longer launch. If that happens, you can use the persistence helper installed into GTA Car Tracker to refresh the app registrations, which will make them work again.
SECURITY
URL Scheme Enabled
Show Install Confirmation Alert
Always...
The URL Scheme, when enabled, will allow apps and websites to trigger TrollStore installations through the apple-magnifier://install?url=<IPA_URL> URL scheme.
Advanced
Uninstall TrollStore
TrollStore 1.5.0
© 2022 Lars Fröder (opa334)
TrollStore is NOT for piracy!
Credits:
@LinusHenze: CoreTrust bug
@zhuowei: CoreTrust bug writeup and cert
@lunotech11, @SerenaKit, @tylinux: Various contributions
@ProcursusTeam: uicache and ldid build
@cstar_ow: uicache
@saurik: ldid
Apps
Settings

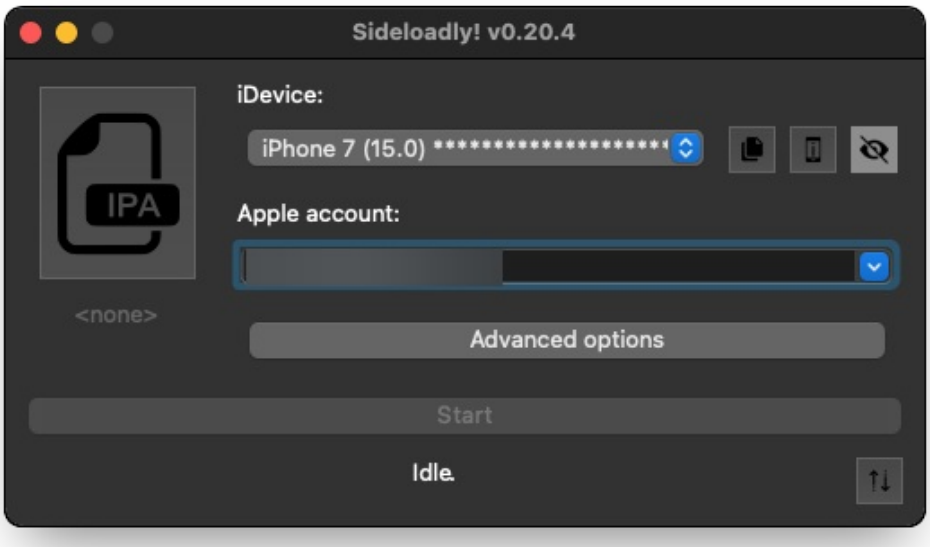
Sideloadly

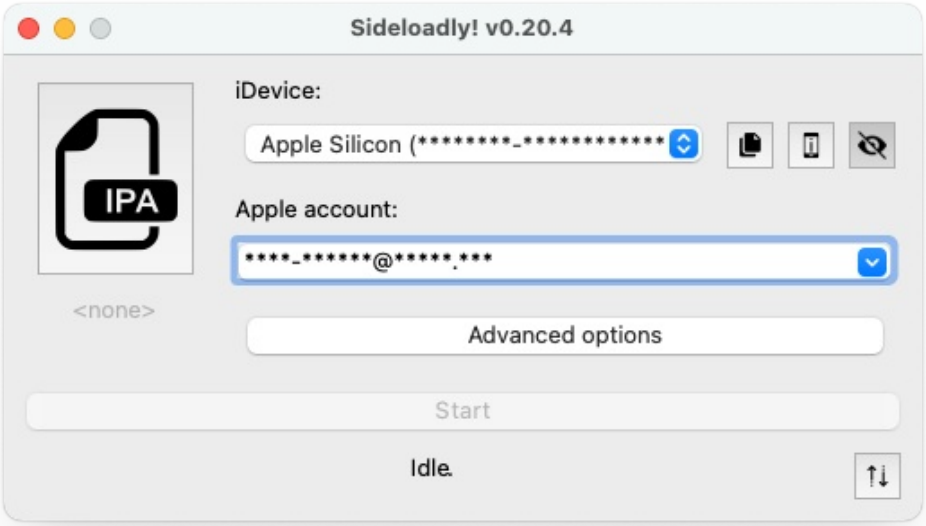
- `Sideloadly`
  - 官网
    - https://sideloadly.io/
      - Sideloadly - iOS, Apple Silicon & TV Sideloading
    - https://sideloadly.app/
      - Sideloadly - Permanently Sideload IPA files FREE (Installer)
  - 下载地址
    - Mac
      - https://sideloadly.app/SideloadlySetup.dmg
    - Win
      - 64bit
        - https://sideloadly.app/SideloadlySetup64.exe
      - 32bit
        - https://sideloadly.app/SideloadlySetup32.exe
  - 截图
    - 

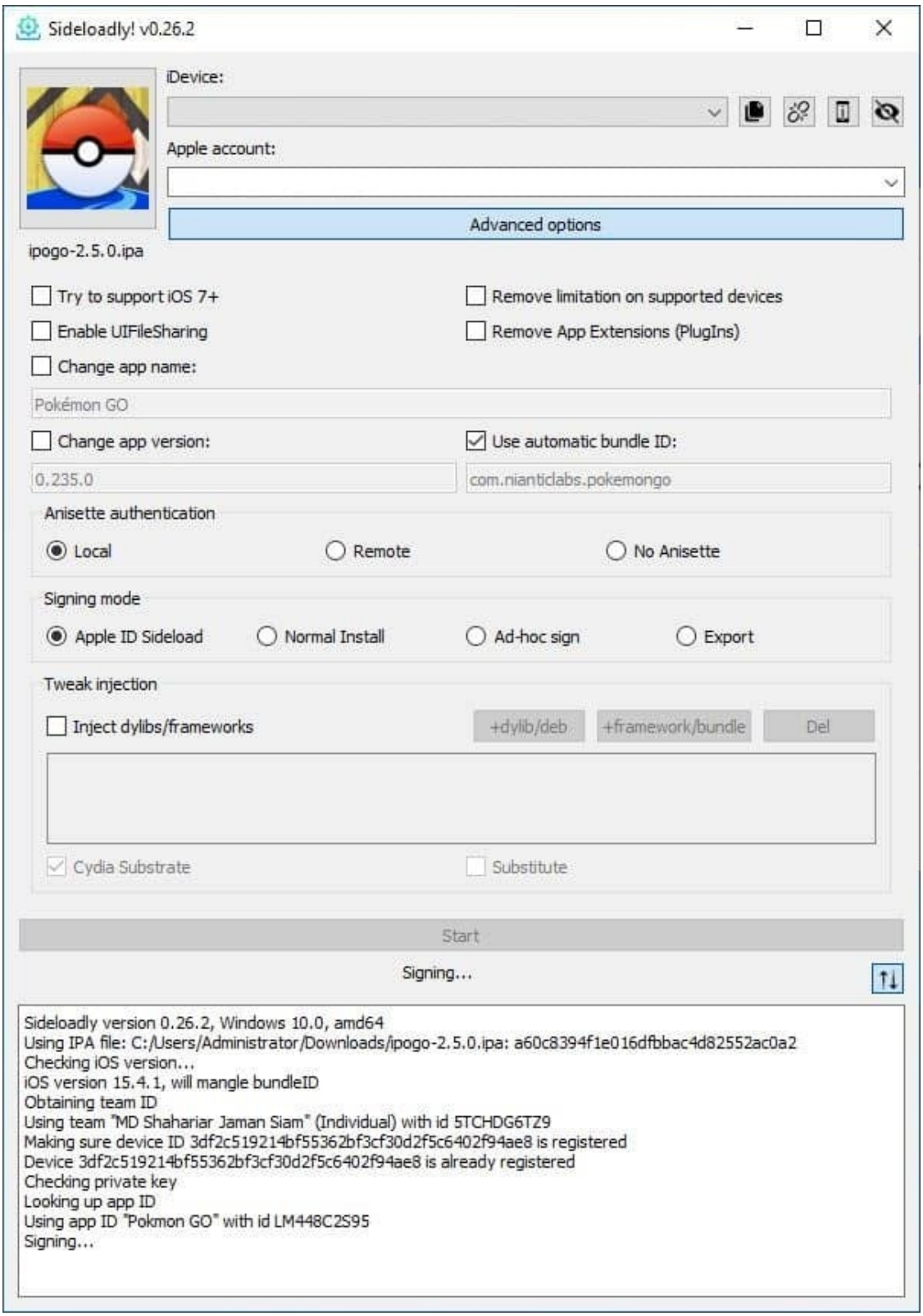

Sideloadly! v0.23
IPA
iDevice:
iPhone (15.1.1) ********-********** @Wi-Fi
Apple account:
********@******.***
Advanced options
Taurine-1.1.1.ipa
Start
Idle.

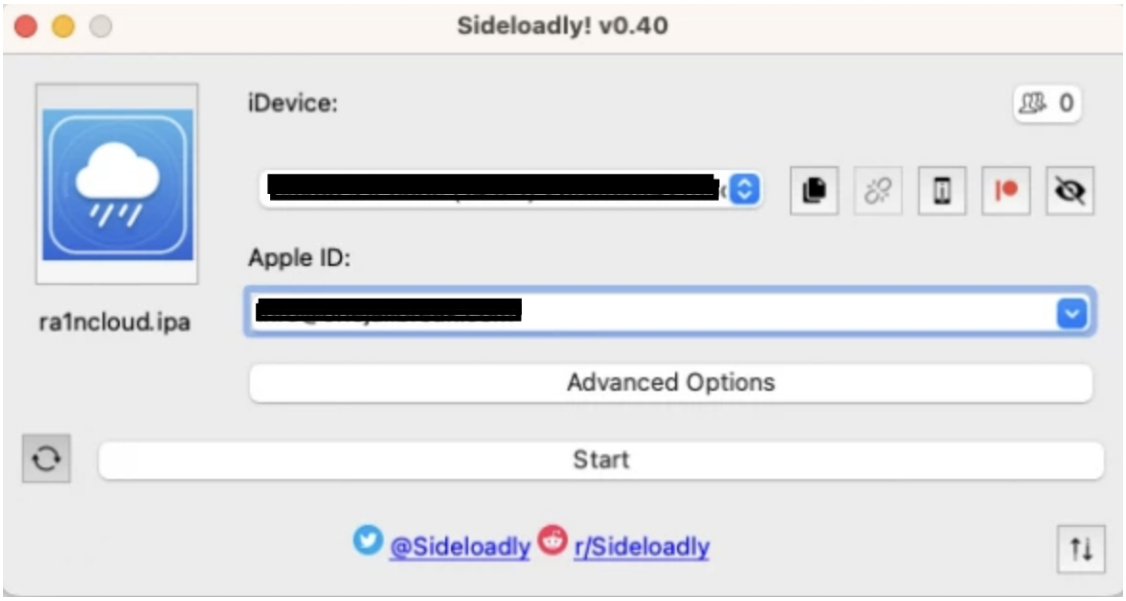

Sideloadly! v0.22
IPA
iDevice:
iPhone 7 (15.0) **
Apple account:
********@******.***
Advanced options
unc0ver_6.2.0.ipa
Start
Done.
Installing 15%: ExtractingPackage
Installing 20%: InspectingPackage
Installing 20%: TakingInstallLock
Installing 30%: PreflightingApplication
Installing 30%: InstallingEmbeddedProfile
Installing 40%: VerifyingApplication
Installing 50%: CreatingContainer
Installing 60%: InstallingApplication
Installing 70%: PostflightingApplication
Installing 80%: SandboxingApplication
Installing 90%: GeneratingApplicationMap
Installing 100%: Complete
Restored 1 profile(s)
Done.


Sideloadly! v0.23
iDevice:
iPhone (15.1.1) ********_********** @Wi-Fi
Apple account:
********@******.***
Advanced options
Youtube.ipa
Try to support iOS 7+
Remove limitation on supported devices
Enable UIFileSharing
Remove App Extensions (Plug-ins)
Change app name:
Change app version:
Change app bundle ID:
com.google.ios.youtube
Use Anisette authentication
Signing mode
Apple ID Sideload
Normal Install
Ad-hoc sign
Dylibs/frameworks injection
Inject dylibs/frameworks
+dylib/deb
+framework/bundle
Del
Cydia Substrate
Substitute
Start
Idle.


Sideloadly! v0.20.4
iDevice:
iPhone 7 (15.0) **********
Apple account:
IPA
<none>
Advanced options
Start
Idle.


Sideloadly! v0.20.4
iDevice:
Apple Silicon (********-**********
Apple account:
****_******@*****.***
IPA
<none>
Advanced options
Start
Idle.


Sideloadly! v0.26.2
iDevice:
Apple account:
Advanced options
ipogo-2.5.0.ipa
Try to support iOS 7+
Remove limitation on supported devices
Enable UIFileSharing
Remove App Extensions (PlugIns)
Change app name:
Pokémon GO
Change app version:
Use automatic bundle ID:
0.235.0
com.nianticlabs.pokemongo
Anisette authentication
Local
Remote
No Anisette
Signing mode
Apple ID Sideload
Normal Install
Ad-hoc sign
Export
Tweak injection
Inject dylibs/frameworks
+dylib/deb
+framework/bundle
Del
Cydia Substrate
Substitute
Start
Signing...
Sideloadly version 0.26.2, Windows 10.0, amd64
Using IPA file: C:/Users/Administrator/Downloads/ipogo-2.5.0.ipa: a60c8394f1e016dfbbac4d82552ac0a2
Checking iOS version...
iOS version 15.4.1, will mangle bundleID
Obtaining team ID
Using team "MD Shahariar Jaman Siam" (Individual) with id 5TCHDG6TZ9
Making sure device ID 3df2c519214bf55362bf3cf30d2f5c6402f94ae8 is registered
Device 3df2c519214bf55362bf3cf30d2f5c6402f94ae8 is already registered
Checking private key
Looking up app ID
Using app ID "Pokmon GO" with id LM448C2S95
Signing...



Xcode

MonkeyDev

- MonkeyDev（调试并安装ipa）
  - 但是会出现问题
    - 【未解决】iOS逆向AppleStore：为何MonkeyDev调试安装ipa后运行会出现各种出错
      - iOS的app，即使是 砸壳版本
        - dpkg安装ipa：（都可以）正常使用，不会出错
        - Xcode+MonkeyDev调试安装：打开后各种错误，且无法彻底解决
          - 对于Apple Store：
            - app group path问题
            - Charles抓包证书出错问题
            - （从iCloud）同步Apple账户失败
          - 对于之前的抖音
            - NSString空字符串崩溃问题
            - 等等
      - ->最后已确认是重签名期间导致entitlement权限丢失，从而导致后续运行期间出现各种问题

ideviceinstaller

help语法

```
➜  ~ ideviceinstaller --help
Usage: ideviceinstaller OPTIONS

Manage apps on iOS devices.

OPTIONS:
  -u, --udid UDID    Target specific device by UDID.
  -n, --network        Connect to network device.
  -l, --list-apps    List apps, possible options:
       -o list_user     - list user apps only (this is the default)
       -o list_system    - list system apps only
       -o list_all     - list all types of apps
       -o xml         - print full output as xml plist
  -i, --install ARCHIVE    Install app from package file specified by ARCHIVE.
                           ARCHIVE can also be a .ipcc file for carrier bundles.
  -U, --uninstall APPID    Uninstall app specified by APPID.
  -g, --upgrade ARCHIVE    Upgrade app from package file specified by ARCHIVE.
  -L, --list-archives    List archived applications, possible options:
       -o xml         - print full output as xml plist
  -a, --archive APPID    Archive app specified by APPID, possible options:
       -o uninstall     - uninstall the package after making an archive
       -o app_only     - archive application data only
       -o docs_only     - archive documents (user data) only
       -o copy PATH     - copy the app archive to directory PATH when done
       -o remove     - only valid when copy PATH is used: remove after copy
  -r, --restore APPID    Restore archived app specified by APPID
  -R, --remove-archive APPID  Remove app archive specified by APPID
  -o, --options        Pass additional options to the specified command.
  -w, --notify-wait        Wait for app installed/uninstalled notification
                            to before reporting success of operation
  -h, --help         prints usage information
  -d, --debug         enable communication debugging
  -v, --version        print version information

Homepage:     https://libimobiledevice.org
Bug Reports:  https://github.com/libimobiledevice/ideviceinstaller/issues
```

卸载app

此处顺带介绍，如何卸载app：

ideviceinstaller

举例：

```
➜  ~ ideviceinstaller -U com.ss.iphone.ugc.Aweme
Uninstalling 'com.ss.iphone.ugc.Aweme'
Uninstall: RemovingApplication (50%)
Uninstall: GeneratingApplicationMap (90%)
Uninstall: Complete
```

管理插件

安装插件

iOS越狱后，安装iOS的（越狱）插件=tweak=plugin（主要是`deb`文件）的主要方式有：

- Filza
- dpkg
- ideviceinstaller ?

deb文件

- deb文件 == deb包
  - 根据是否带UI界面分
    - 普通的不带UI界面的插件=deb文件=deb包
    - 类似独立app的带UI界面的tweak插件

Filza

dpkg

- dpkg
  - 安装过程分很多步骤
    - TODO：把多个步骤整理过来
- 概述
  - 安装deb `-i` == `-install`

    ```
    dpkg -i xxx.deb
    ```

  - 卸载deb `-r` == `-remove`

    ```
    dpkg -r xxx.deb
    ```

  - 查看deb信息 `-s` == `-see`

    ```
    dpkg -s xxx.deb
    ```

用dpkg安装deb

举例

- Reveal2Loader

  ```
  dpkg -i Reveal2Loader_1.0-6_iphoneos-arm.deb
  ```

- theos

  ```
  dpkg -i /tmp/_theos_install.deb
  ```

- iOSGods

  ```
  dpkg -i "/var/mobile/Documents/com.iosg.mobs_5.25+iOSGods.com_iphoneos-arm.deb"
  ```

- 其他

  ```
  dpkg -i "/var/root/当当关注查件17.8-9.deb"
  ```

dpkg版本信息

- iPhone8-150

  ```
  iPhone8-150:~ root# which dpkg
  /usr/bin/dpkg
  iPhone8-150:~ root# dpkg --version
  Debian 'dpkg' package management program version 1.21.9 (iphoneos-arm).
  This is free software; see the GNU General Public License version 2 or
  later for copying conditions. There is NO warranty.
  ```

- Crifan-iPhone6

  ```
  ➜  ~ ssh root@192.168.0.54
  Crifan-iPhone6:~ root# which dpkg
  /usr/bin/dpkg
  Crifan-iPhone6:~ root# dpkg --version
  Debian 'dpkg' package management program version 1.19.7 (iphoneos-arm).
  ```

```
This is free software; see the GNU General Public License version 2 or
later for copying conditions. There is NO warranty.
```

dkpg相关命令工具

- dpkg
- dpkg-deb
- dpkg-divert
- dpkg-genbuildinfo
- dpkg-query
- dpkg-split
- dpkg-trigger

->

- XinaA15越狱后的iPhone11中

```
iPhone11-151:~ root# ls -lh /private/preboot/3B92D6F7C3FE6444A715B312E418498574E442DAB2F6D9E18B58B762F71D1455B7E2E1C2DD3912B1B4E6D10C6B9150C8/procursus/usr/bin/
...
-rwxrwxrwx 1 root wheel 116K Feb  2 21:55 dpkg*
-rwxrwxrwx 1 root wheel  72K Feb  2 21:55 dpkg-deb*
-rwxrwxrwx 1 root wheel 172K Jan 18 15:08 dpkg-divert*
-rwxr-xr-x 1 root wheel  21K Jan 18 15:08 dpkg-maintscript-helper*
-rwxrwxrwx 1 root wheel  89K Feb  2 21:55 dpkg-query*
-rwxr-xr-x 1 root wheel 4.1K Jan 18 15:08 dpkg-realpath*
-rwxrwxrwx 1 root wheel 109K Jan 18 15:08 dpkg-split*
-rwxrwxrwx 1 root wheel 112K Jan 18 15:08 dpkg-statoverride*
-rwxrwxrwx 1 root wheel 115K Jan 18 15:08 dpkg-trigger*
```

- 使用Termux部署Python3的Android系统中

```
$ ls -l usr/bin/
...
-rwx------    1 u0_a260  u0_a260     265696 Jul  1 13:56 dpkg
-rwx------    1 u0_a260  u0_a260     134416 Jul  1 13:56 dpkg-deb
-rwx------    1 u0_a260  u0_a260     134320 Jul  1 13:56 dpkg-divert
-rwx------    1 u0_a260  u0_a260      10822 Jul  1 13:56 dpkg-genbuildinfo
-rwx------    1 u0_a260  u0_a260     134312 Jul  1 13:56 dpkg-query
-rwx------    1 u0_a260  u0_a260     134128 Jul  1 13:56 dpkg-split
-rwx------    1 u0_a260  u0_a260      68560 Jul  1 13:56 dpkg-trigger
```

启用和禁用插件

- `iCleaner Pro`
  - iCleaner Pro · iOS越狱开发：常用越狱插件 (crifan.org)

常见问题

卸载后app图标残留

TODO：

- 【已解决】ideviceinstaller卸载iPhone中app后导致无法快捷键截图
- 【已解决】越狱iPhone中如何实现respring重启桌面SpringBoard

附录

下面列出相关参考资料。

参考资料

- 【未解决】iOS逆向AppleStore：用debugserver+lldb调试ipa
- 【基本解决】Android系统中使用Termux部署Python3的Flask项目
- 【已解决】iOS逆向Apple账号：搭建Reveal环境去调试UI界面元素
- 【未解决】XinaA15是如何重签名debugserver而加上权限task_for_pid-allow能调试任意进程的
- 【已解决】theos中make的输出信息中是否支持verbose详情模式
- 【已解决】Sileo中安装Filza报错：Depends zip unzip gzip unrar p7zip
- 【记录】研究改机软件黑豹deb解压后的目录结构和文件内容
- 【记录】反越狱插件：别人测试抖音效果
-
- iCleaner Pro · iOS越狱开发：常用越狱插件 (crifan.org)
-
- 2021-03-01-使用Unicorn模拟运行破解简单的IOS-IPA-Crackme | huhu's blog (huhu0706.github.io)
- XLsn0w/Cydia: 微信公众号: XLsnow => Cydia插件 Logos语言 开发Tweak.xm Cydia Substrate 注入dylib iOS逆向工程开发 越狱Jailbreak deb插件 - fishhook / Frida / iOSOpenDev / Cycript / MachOView / IDA / Hopper Disassembler / MonkeyDev / Class-dump / Theos / Reveal / Dumpdecryptd / FLEX / 汇编Assembly / CaptainHook / lldb/LLVM/XNU/Darwin/iOS Reverse (github.com)
-