目录

iOS逆向开发：越狱插件开发

- 最新版本：`v0.8.3`
- 更新时间：`20241014`

简介

介绍iOS逆向开发领域中，如何开发越狱插件tweak。先是概览，然后介绍基础知识：什么是tweak插件、tweak插件的开发手段；以及具体如何用Theos/Logos、iOSOpenDev、MonkeyDev去开发tweak插件；Theos中包括搭建Theos开发环境；以及整理相关心得。

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_jailbreak_tweak: iOS逆向开发：越狱插件开发

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：越狱插件开发 book.crifan.org
- iOS逆向开发：越狱插件开发 crifan.github.io

离线下载阅读

- iOS逆向开发：越狱插件开发 PDF
- iOS逆向开发：越狱插件开发 ePub
- iOS逆向开发：越狱插件开发 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

iOS越狱插件开发概述

iOS逆向领域中，常涉及到的领域是：

- iOS越狱插件tweak的开发
  - = 写hook代码，编译成tweak插件，实现特定的功能

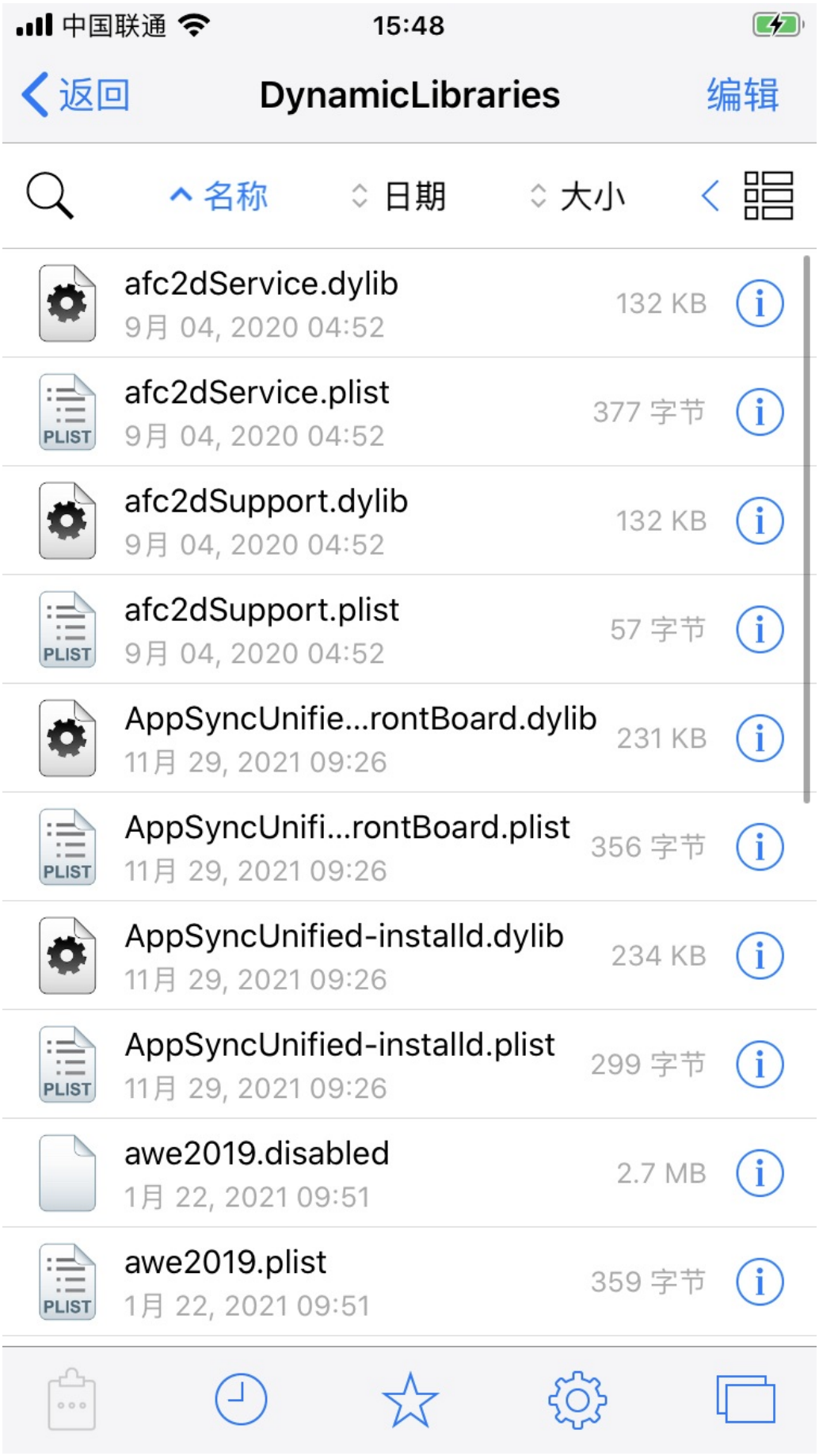
越狱插件开发基础知识

- 越狱插件
  - `越狱` = `jailbreak` = `jail` = `jb`
  - `插件` = `tweak` = `扩展` = `extension`
- 越狱插件开发工具/框架
  - 最常用=最基本的
    - `Theos` / `Logos`
  - 集成XCode带GUI的
    - `iOSOpenDev`
  - iOSOpenDev升级版 = 集成XCode和其他各种工具的更强的集成环境
    - `MonkeyDev`

tweak插件

关于tweak的详细介绍：

- `tweak`
  - 是什么：a dynamic library
    - all kinds of crack patches
  - 叫法：`tweak` = `插件` = `extension` = `扩展`
  - 原理：
    - 通过一个预定义的过滤器，被注入到特定的程序中，实现替代特定的Objective-C或Swift的方法函数，从而实现特定功能
    - 底层基于：`Cydia Substrate`
  - 名词
    - `越狱开发` = `jailbreak development` = `development of a Tweak` = `开发一个插件` = `插件开发`
  - 相关背景
    - iOS有2种 `动态库` = `dynamic library`
      - `dylib`
        - 举例：`libsqlite.dylib`，`libz.dylib` 等
      - `framework`
    - 现状
      - **iOS正向**开发：主要用 `framework`
        - 发布方式：`ipa` 包
          - 用（开发者个人 或 企业）证书，把代码编译封装到 `ipa` 包，然后去安装到iOS(iPhone)中
            - 当然也有不小的限制，但是支持普通非越狱手机
      - **iOS逆向**开发(主要是插件Tweak开发)：主要用 `dylib`
        - 发布方式：`deb` 包
          - 只能在越狱后的iOS（iPhone）中安装
  - tweak的位置
    - `/Library/MobileSubstrate/DynamicLibraries`
      - 存放了多种文件
        - `dylib`
        - `plist`：定义插件的hook的范围
        - `bundle`：插件的资源文件
      - 截图举例



tweak开发手段

- 开发越狱插件的主要手段/工具/框架 = dylib-level tweaking/hooking/detouring
  - 底层机制和原理
    - 基于: CydiaSubstrate
      - 直接调用
        - Direct calling of substrate functions (MSHookXxx family)
    - Substitute
    - `CaptainHook`
      - ure C/ObjC way of doing things, header-only, uses many #define's under the hood
      - Use it if you don't want to lose syntax highlighting and navigation support in IDE project
    - `fishhook`
      - Pure C way of doing things
      - facebook 开源的一个库
        - https://github.com/facebook/fishhook
          - facebook/fishhook: A library that enables dynamically rebinding symbols in Mach-O binaries running on iOS
    - `AutoHook`
      - Creating tweaks without Logos directly from Xcode
        - Tutorial Creating tweaks without Logos directly from Xcode : jailbreakdevelopers (reddit.com)
    - Object-oriented method of hooking with pre-post-instead semantic
      - https://github.com/steipete/Aspects
    - Method Swizzle
      - 通过Runtime交换方法的实现
  - 相对上层的（集成/封装）工具
    - Theos/Logos
    - iOSOpenDev
    - MonkeyDev

CydiaSubstrate

- `CydiaSubstrate` = `Cydia Substrate` = `Cydia Mobile Substrate`
  - 旧称：`MobileSubstrate`
  - 概述：Cydia中的hook框架
    - The powerful code modification platform behind Cydia
    - Powerful Code Insertion Platform
    - a framework and development library
      - used by developers to reasonably sanely (and hopefully safely) make modifications to code written by other developers and running in other processes, even if multiple people are attempting to modify the same thing; this library is the foundation of most of the interesting hacks found on the iPhone.
  - 额外说明
    - `MobileSubstrate` 是 `Cydia` 实现的基础
      - 现有的越狱开发环境一般使用的是 Theos/Logos 或者 iOSOpenDev
        - 这两者hook功能都是对MobileSubstrate API的封装
  - 反破解
    - `MobileSubstrate` 是基于 `DYLD_INSERT_LIBRARIES` 方式实现的
      - 有些应用（如美团）为了阻止他人的破解，采用了一些措施阻止了DYLD_INSERT_LIBRARIES这种注入方式
        - 核心：加编译参数，Restricted Segment of Header 禁止改动加载的库
          - `-Wl,-sectcreate,__RESTRICT,__restrict,/dev/null`
        - 最新情况
          - 新版dyld早已废弃此种手段了
            - 从iOS10开始，这种防护手段已失效
  - 功能
    - 允许实时修改代码
      - 第三方开发者调用其API，可以实现给IOS系统打补丁，改变系统或者应用的运行行为。
      - Substrate makes it easy to modify software, even without the source code, and in a way that allows users to easily choose which changes they want
  - 机制=原理
    - injection mechanism 注入机制
    - 自己写插件=扩展=substrate extensions，利用API，实现特定功能
      - Developers support this by building their changes as "substrate extensions" that are loaded into all of the processes they want to take control of.
      - By using the provided API to make all changes in memory, multiple developers can safely adapt the same parts of the target program to their purposes.
    - 实现原理
      - 在MAC与IOS平台上，动态库的后缀一般是dylid，而加载这些动态库的程序叫做
        - dynamic linker=dynamic loader=dyld
      - 这个程序有很多的环境变量来设置程序的一些行为，最为常用的一个环境变量叫做
        - DYLD_INSERT_LIBRARIES
      - 它是一个使用冒号分隔的动态库路径字符串，表示一个将要加载运行的动态库额外依赖的其它动态库
      - 通过这个环境变量，我们就可以向应用中注入自己的动态库，进而改变应用运行时的特定行为
      - 而这种方式，也正是mobileSubstrate所使用的最基本方法
  - Cydia Substrate extensions
    - =run-time patches
  - 主要模块
    - MobileHooker
      - used to replace system functions
        - This process is known as hooking
      - 核心函数API

        - MSHookMessage
            - 非线程安全
            - 用于替换原函数实现
            - 在OC的Runtime机制上实现的
        - MSHookMessageEx
            - 线程安全
            - 用于 hook Objective-C 方法
                - 在OC的Runtime机制上实现的
        - MSHookFunction
            - 用于 hook C 语言函数
                - 主要用于C/C++函数
            - 与OC不同，它另有一套自己的实现方式
        - 非公开的：MSHookProcess
    - MobileLoader
        - loads 3rd-party patching code into the running application
            - 将指定目录下的补丁文件（动态库文件）加载到指定的程序中
        - `/Library/MobileSubstrate/DynamicLibraries/`
        - 举例

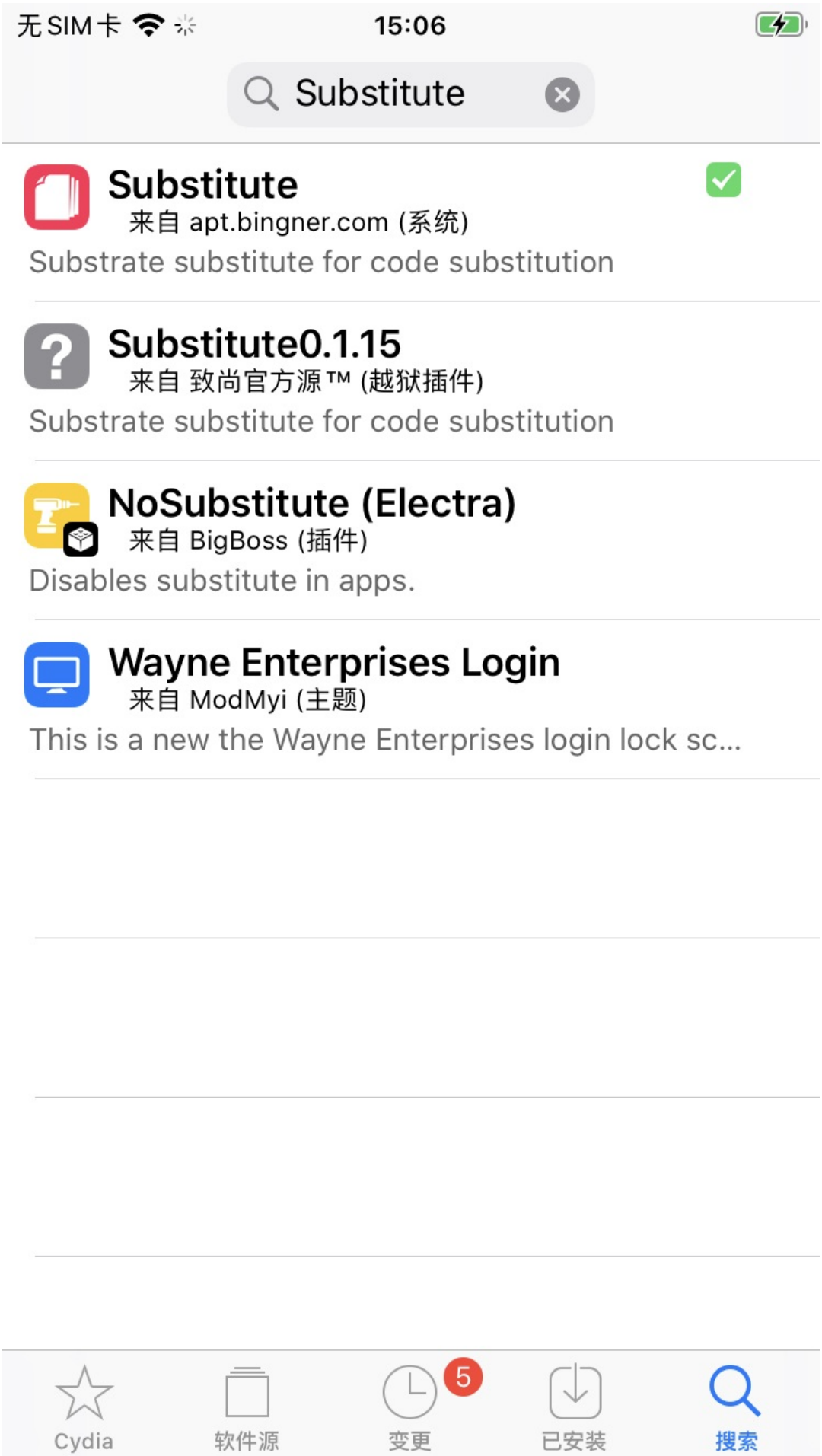
```
Filter = {
  CoreFoundationVersion = (550.32, 675.00);
  Executables = ("mediaserverd");
  Bundles = ( "com.apple.MobileSMS", "net.whatsapp.WhatsApp" );
  Mode = "Any";
};
```

    - Safe mode
        - 容错处理
        - 第三方开发者通过MobileSubstrate向系统注入自定义代码时，如果考虑不周就可能导致终端设备处于崩溃的状态。MobileLoader会捕获这个崩溃异常，然后让设备进入SafeMode状态，在这个状态下，所有的第三方补丁都将被禁用，开发者可以比较从容的恢复设备。
        - 注入别的进程并改变其逻辑一定存在风险，难免会造成程序崩溃的现象，如果崩溃的是SpringBoard等系统进程，则会造成系统瘫痪。为了避免这类情况，SafeMode会捕获SIGABRT、SIGILL、SIGBUS、SIGSEGV、SIGSYS这几种信号，捕获到目标信号后SafeMode会使设备进入安全模式，在安全模式下所有第三方插件(即dylib)都会被禁用，便于修复系统
        - When a extension crashed the SpringBoard, MobileLoader will catch that and put the device into safe mode
        - In safe mode all 3rd-party extensions will be disabled.
        - The following signals will invoke safe mode
            - SIGABRT
            - SIGILL
            - SIGBUS
            - SIGSEGV
            - SIGSYS
- iOS
    - 前提：
        - iOS设备已越狱
        - 已安装Cydia = Cydia Installer
    - 安装：通过Cydia安装
        - Cydia Substrate · Cydia (saurik.com)
            - https://cydia.saurik.com/package/mobilesubstrate/
- 安卓
    - 包名：com.saurik.substrate
    - apk
        - http://www.cydiasubstrate.com/download/com.saurik.substrate.apk
- 资料

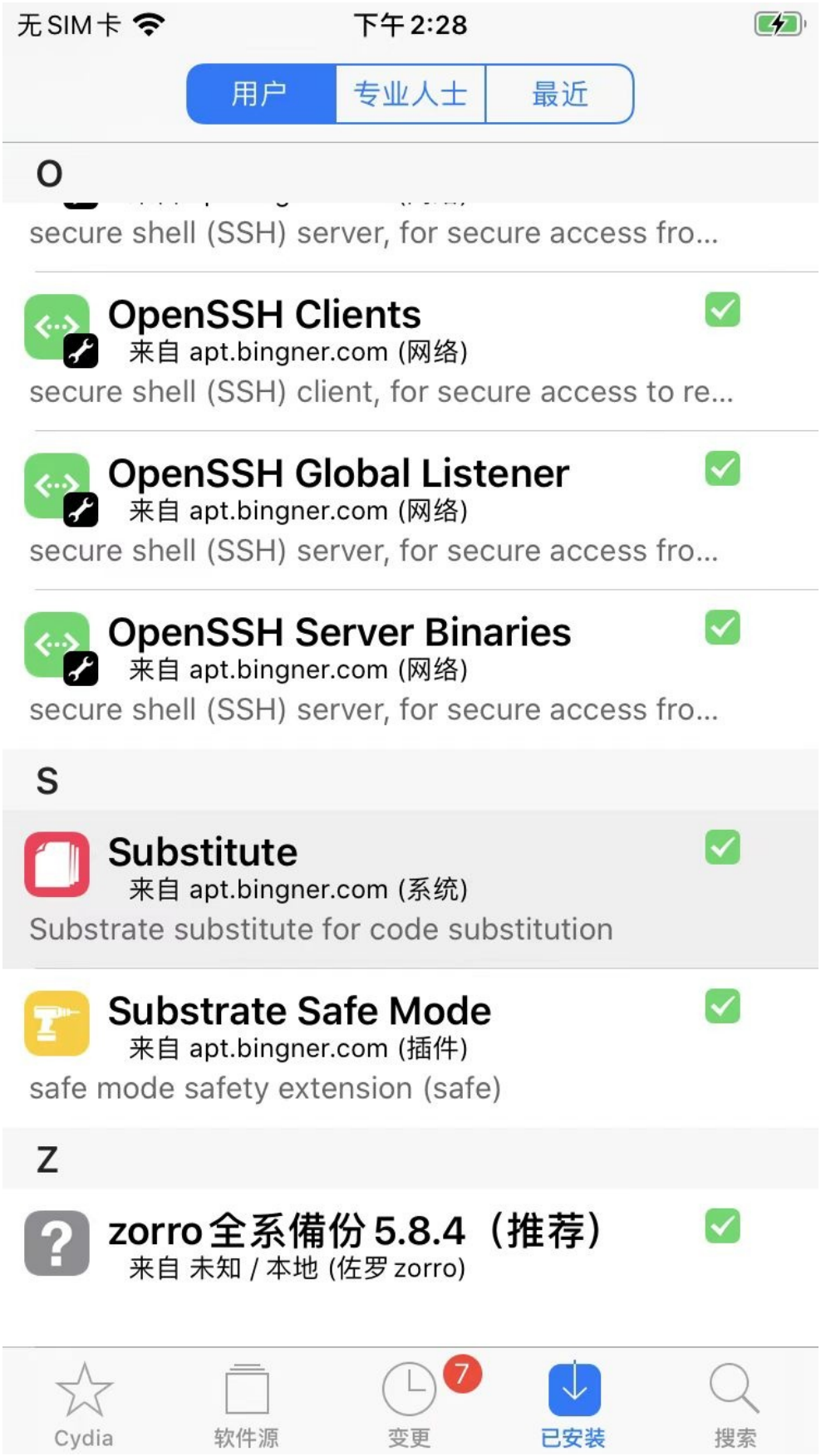
        - 官网 Cydia Substrate
            - http://www.cydiasubstrate.com/
        - 快速上手 Getting Started
        - 常见问题 FAQ | Cydia Substrate
            - Why are the APIs namespaced with "MS”? FAQ | Cydia Substrate
                - API前缀：MS = MobileSubstrate
                    - 最早时：Mobile指的是MobileSafari, MobileMail等
    - 相关
        - The iPhone Wiki
            - https://www.theiphonewiki.com/
                - The iPhone Wiki is an unofficial wiki dedicated to collecting, storing and providing information on the internals of Apple's amazing iDevices
                - We hope to pass this information on to the next generation of hackers so that they can go forth into their forebears' footsteps and break the ridiculous bonds Apple has put on their amazing mobile devices.
            - 越狱Jailbreak
                - https://www.theiphonewiki.com/wiki/Jailbreak
        - 类似框架
            - Cycript

Substitute

- Substitute
  - 是什么：一个插件注入系统
    - 和Substrate（==CydiaSubstrate）类似
      - 是Substrate的替代品
  - 用途
    - 可以基于Substitute的API函数，开发插件，实现各种hook
  - Substitute的函数
    - API函数
      - 包含
        - `SubGetImageByName`
        - `SubFindSymbol`
        - `SubHookFunction`
        - `SubHookMessageEx`
      - （好像分别）对应着 CydiaSubstrate 的
        - `MSGetImageByName`
        - `MSFindSymbol`
        - `MSHookFunction`
        - `MSHookMessageEx`
    - 其他底层函数
      - substitute.h
        - `substitute_open_image`
        - `substitute_close_image`
        - `substitute_find_private_syms`
        - `substitute_sym_to_ptr`
        - `substitute_interpose_imports`
        - `substitute_hook_objc_message`
        - `substitute_free_created_imp`
  - 作者：Comex
  - 官网
    - 没有官网，只有GitHub
      - comex/substitute: A free runtime modification library. (github.com)
        - 但是：作者已放弃维护了
      - 其他人的fork后的
        - MidnightTeam/substitute: A free runtime modification library. (github.com)
  - 下载
    - 只能网上找到其他地方去下载
      - Package: Substitute • com.ex.substitute • Bingn... (ios-repo-updates.com)
        - 2.2.3版本
          - https://apt.bingner.com/debs/1443.00/com.ex.substitute_2.2.3_iphoneos-arm.deb
    - 或者从Cydia中搜：Substitute，可以找到并安装对应插件


无 SIM 卡
15:06
Substitute
Substitute
来自 apt.bingner.com (系统)
Substrate substitute for code substitution
Substitute0.1.15
来自 致尚官方源™ (越狱插件)
Substrate substitute for code substitution
NoSubstitute (Electra)
来自 BigBoss (插件)
Disables substitute in apps.
Wayne Enterprises Login
来自 ModMyi (主题)
This is a new the Wayne Enterprises login lock sc...
Cydia
软件源
变更
5
已安装
搜索

- 对应现象
  - 用unc0ver越狱后，会自动安装
    - Substitute的app：桌面上可以看到Substitute的图标
    - 

- Substitute的插件
  - Cydia中可以看到Substitute插件
    - 

Tweak越狱插件开发

TODO：

- 【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】已越狱iPhone中卸载tweak加app的deb插件
- 【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】iOS的writeToURL报错：NSCocoaErrorDomain Code 513 You don’t have permission to save the file in the folder Preferences
- 【已解决】XCode中iOS用Objective-C去保存配置信息写入配置文件
- 【已解决】给iOSOpenDev的app和tweak用配置文件互相通信
- 【已解决】iOS插件tweak开发：提取公共函数检测是否越狱和解析出真正路径
- 【记录】把iOS被测app的包名加到反越狱检测插件的plist的Filter中

越狱框架和机制

- 【已解决】寻找Substitute的deb安装包文件
- 【整理】hook框架 hook Framework hooking library
- 【已解决】用dpkg导出并得到Substitute的deb安装包包含的文件列表
- 【已解决】越狱iOS中Substitute相关的文件
- 【已解决】Substitute相关动态库包含哪些API接口函数
- 【整理】iOS越狱后的app：Substitute

Theos/Logos

TODO：

- 【整理】iOS越狱插件开发工具：theos
- 【已解决】Mac中theos的tweak的编译并安装到iPhone
- 【已解决】Mac中theos的make install报错：ssh connect to host port 22 Connection refused
- 【已解决】Mac中初始化和安装Theos开发环境
- 【未解决】越狱iOS如何用Theos开发带GUI图形界面的插件
- 【已解决】Mac中用theos开发最简单的插件的demo：加锁屏左上角加红色框
- 【已解决】theos中确认%log的syslog系统日志是否生效
- 【无法解决】iPhone6中iOS的tweak插件hook更新系统参数不生效
- 【整理】iOS中的Frameworks框架
- 【已解决】Mac中theos用模板创建项目代码并更改代码
- 【已解决】iOS的tweak的Logos代码报错：%orig requires arguments when hooking variadic functions
- 【已解决】iOS越狱插件开发中%hookf和MSHookFunction的关系
-
- 【未解决】越狱iOS如何用Theos开发带GUI图形界面的插件
- 【记录】学习Theos的文档内容：theos-ref仓库
- 【已解决】Mac中theos用模板创建项目代码并更改代码
- 【已解决】Mac中theos的tweak的编译并安装到iPhone
- 【无法解决】iPhone6中iOS的tweak插件hook更新系统参数不生效
- 【已解决】Mac中用theos开发最简单的插件的demo：加锁屏左上角加红色框
- 【已解决】用XCode开发一个Objective-C的iOS的带GUI的app供配合测试theos修改系统参数是否生效
- 【已解决】用Objective-C的iOS的app作为theos开发的tweak插件去hook修改iPhone6的系统参数

- iOS Tweak进阶 – 六阿哥博客 (6ag.cn)
  - 好好学习该贴，有很多有价值的内容值得学习
    - 比如：logify.pl的用法

- `Theos/Logos`
  - just brief DSL wrapper around `CydiaSubstrate`, Special DSL that is translated to C. General-purpose solution to start with

Theos概述

Logos

- Logos
  - 是什么：Theos开发套件的一个组件，通过一系列预处理指令，实现了写hook方法更简单和简洁
    - Logos is a component of the Theos development suite that allows method hooking code to be written easily and clearly, using a set of special preprocessor directives
  - 概述
    - The syntax provided by Logos greatly simplifies the development of MobileSubstrate extensions ("tweaks") which can hook other methods throughout the OS
      - In this context, "method hooking" refers to a technique used to replace or modify methods of classes found in other applications on the OS
  - Logos的指令directives
    - Block level
      - `%group`

        - `%hook`
        - `%new`
        - `%subclass`
        - `%property`
        - `%end`
    - Top level
        - `%config`
            - Configuration Flags
        - `%hookf`
        - `%ctor`
        - `%dtor`
    - Function level
        - `%init`
        - `%class`
        - `%c`
        - `%orig`
        - `%log`

Theos

- Theos
    - 概述：一个跨平台（交叉编译）开发工具套装，用于不用XCode的情况下，开发iOS程序
        - a cross-platform suite of development tools for managing, developing, and deploying iOS software without the use of Xcode
    - 用途：
        - 主要用于越狱后的iOS的扩展插件的开发
            - It is an important tool for people building extensions (tweaks) for jailbroken iOS; many extension developers use Theos.
            - Theos is a little tool which helps you with all the application creation and compilation.
    - 包含组件
        - project templating system：NIC
            - creates ready-to-build empty projects for varying purposes
        - robust build system driven by GNU Make
            - capable of directly creating .deb packages for distribution in Cydia
        - Logos, a built-in preprocessor-based library of directives = an Objective-C preprocessor
            - designed to make MobileSubstrate extension development easy
    - 其他说明
        - Theos is primarily used for jailbreak-centric iOS development (such as MobileSubstrate extensions, PreferenceLoader bundles, and applications intended for distribution in Cydia), but can be used for other types of projects as well.
        - This can be helpful for someone wishing to develop an iPhone SDK-based application without using Mac OS X or Xcode to do so, as Theos can be used on Linux and iOS as well
    - 资料
        - GitHub
            - theos/theos: A cross-platform suite of tools for building and deploying software for iOS and other platforms. (github.com)
                - https://github.com/theos/theos.git
            - Wiki
                - 主页
                    - Home · theos/theos Wiki (github.com)
                - 安装
                    - Installation · theos/theos Wiki (github.com)
        - iphonedev.wiki

        - Theos - iPhone Development Wiki
- Logify
    - 是什么：Theos的一个模块
    - 功能：
        - 输入：`.h` 头文件
        - 输出：`.xm` 文件
            - `.xm` = MobileSubstrate扩展
            - 输出log日志：当被调用时
    - 目的：帮助hook开发者调试和查看哪些函数被调用了
    - 用法举例
        - logify.pl SomeClassHeader.h > tweak.xm
- NIC=New Instance Creator
    - 叫法：
        - 你也可以称其为：Nicolas
    - 是什么：It provides a way to create projects (“instances”) based on templates.
        - Theos comes with a handful of useful templates and others are available from various developers in the community.
    - 文档
        - New Instance Creator (NIC) · Theos
        - NIC - iPhone Development Wiki

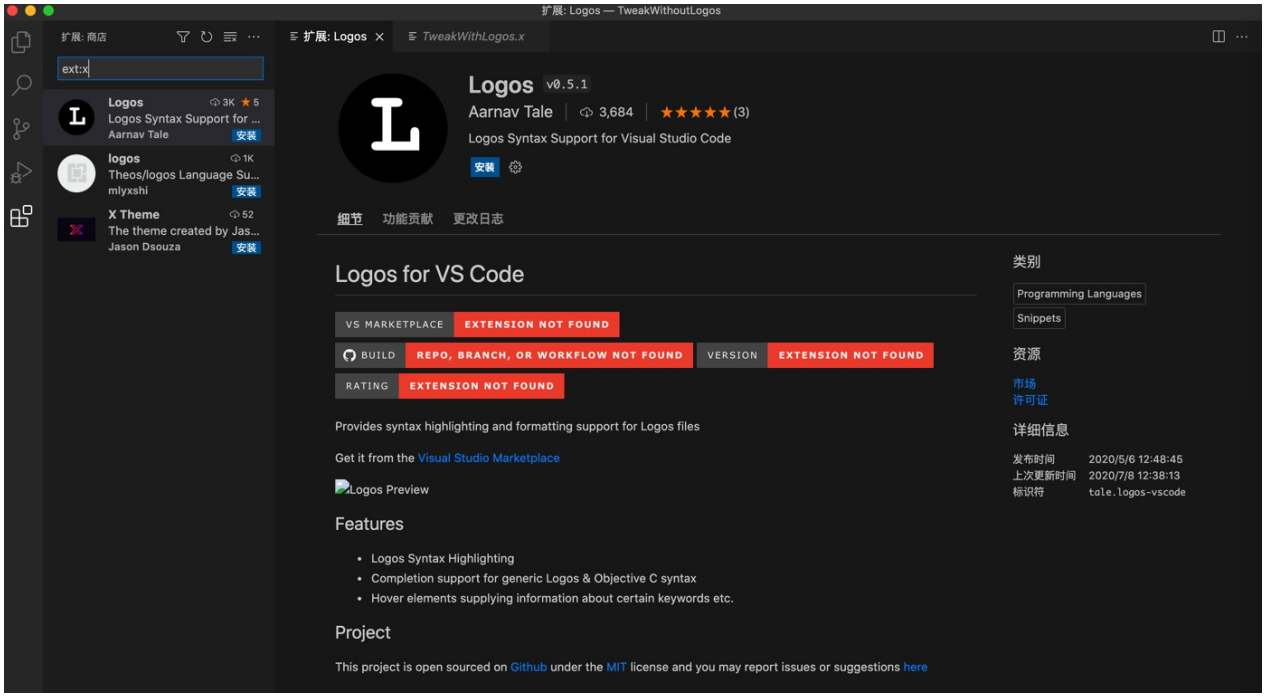
其他相关

Logos的语法高亮

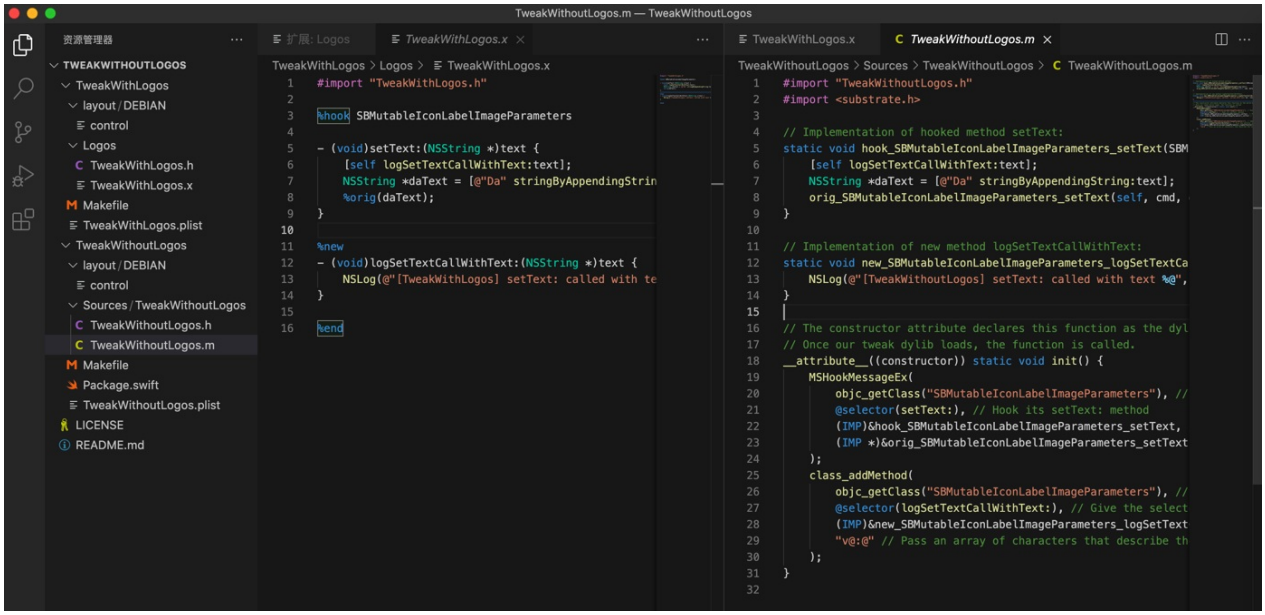
VSCode支持Logos语法高亮：

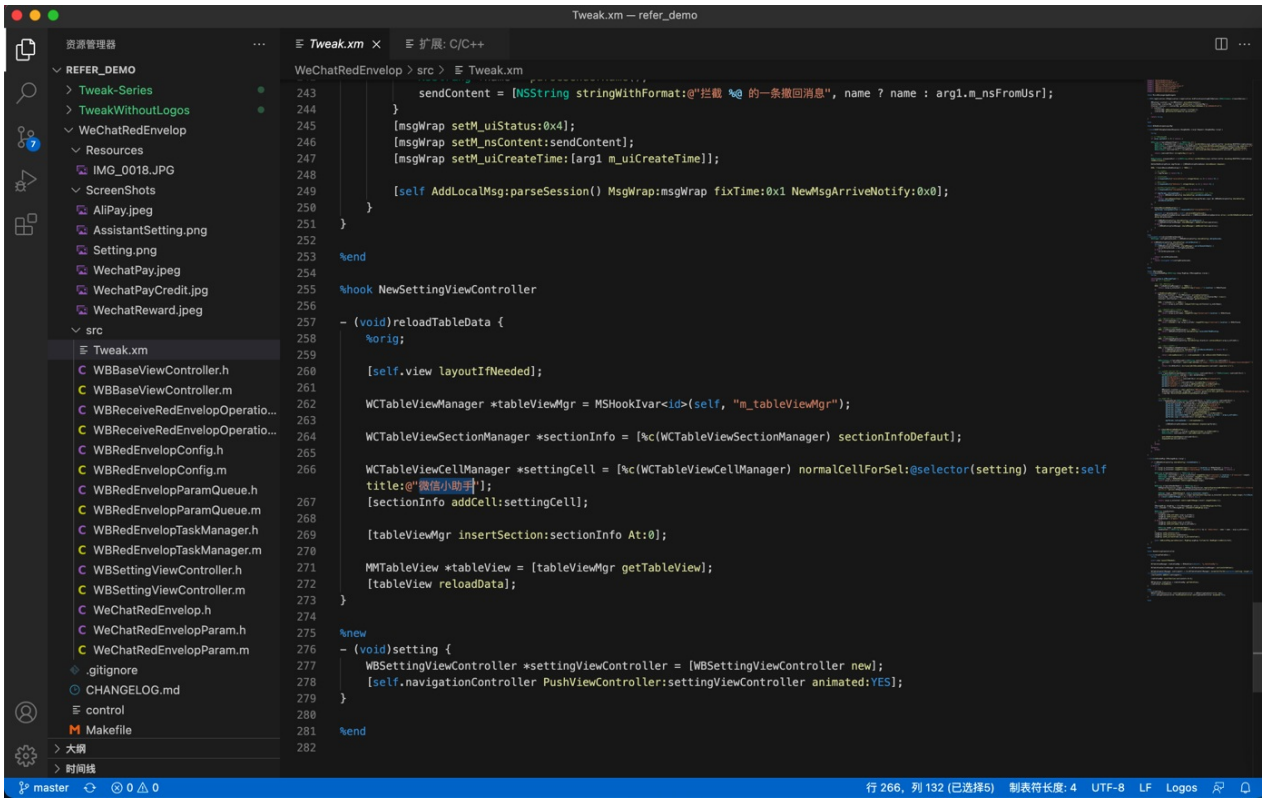
打开 `logos` 的 `.x` 文件，去搜Logos，可以找到插件：

`Logos Syntax Support for Visual Studio Code`



安装后，即可支持Logos的语法高亮：





搭建Theos环境

TODO：

- 【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

---

前提

- `Mac`
  - `Homebrew`
  - `XCode`
    - XCode是必须的，因为 `Command Line Tools` 是不够用的。而 `Xcode` 包含了所有Apple平台的所有工具（链）
  - 必要的工具
    - `ldid`
    - `xz`

```
brew install ldid xz
```

设置theos的环境变量

先确认自己的shell是啥：

```
➜  iOS_Tweak echo $SHELL
/bin/zsh
```

此处是： `zsh` ，所以去编辑 `zsh` 的启动脚本：

```
vi ~/.zshrc
```

加上：

```
export THEOS /opt/theos
export PATH $THEOS/bin:$PATH
```

说明：

- 安装位置的选择
  - 为了后续兼容其他相关开发工具，比如iOSOpenDev
  - 最好安装到默认的=大家常用的位置
    - `/opt/theos`
  - 最好不要放在其他位置
    - 比如我之前就放在自己的某个目录
      - `/Users/crifan/dev/DevSrc/iOS_Tweak/theos`
    - 否则容易导致各种错误
- 如果后续需要，可以把IP的环境变量也加上

```
export THEOS_DEVICE_IP 192.168.31.43
```

  - 注：其中的 `192.168.31.43` 是你的调试的目标设备iPhone的WiFi的IP地址

下载theos代码

```
cd /opt/theos
git clone --recursive https://github.com/theos/theos.git $THEOS
```

常见问题

xcrun error invalid active developer path

macOS升级后

```
git clone
```

出错：`xcrun: error: invalid active developer path`

解决办法：

```
xcode-select --install
```

会弹框，点击安装，开始安装`xcode-select`。等安装完毕，即可。

下载私有框架=下载sdk

注：`XCode 7.3`之后，就不再提供，后续开发tweak时（可能）需要链接使用的私有框架private Framework了

所以要单独下载：

```
curl -LO https://github.com/theos/sdks/archive/master.zip
TMP=$(mktemp -d)
unzip master.zip -d $TMP
mv $TMP/sdks-master/*.sdk $THEOS/sdks
rm -r master.zip $TMP
```

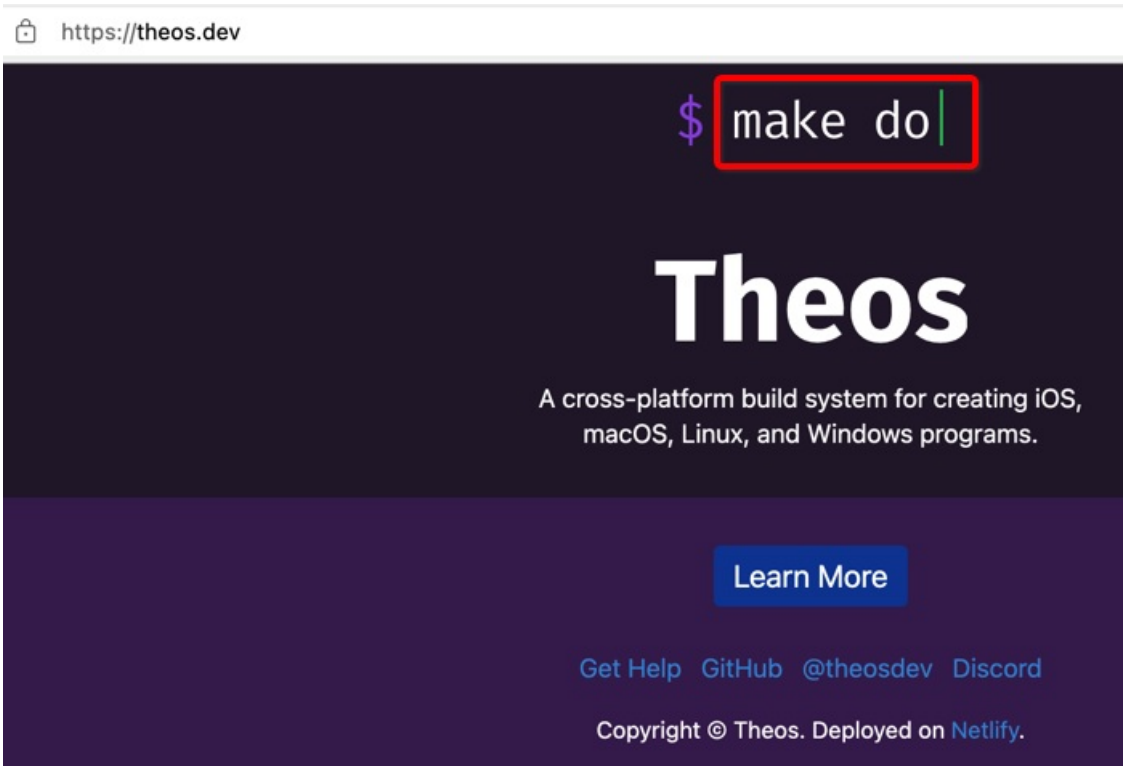
编译运行调试

最后是，编译运行调试：

```
make do
```

注：

- 最新的`make do` == 之前的：`make package install`
  - 新官网（https://theos.dev/）中也有显示



说明：

- 新版theos已内置 `CydiaSubstrate` （ `CydiaSubstrate.framework` ），无需运行 `bootstrap.sh` 或从 `iPhone` 中拷贝了
- 新版theos也无需： `dpkg-deb` 、 `brew install dpkg` 了

相关资料

- Logos - iPhone Development Wiki

官网资料：

- Installation · theos/theos Wiki (github.com)
- Installation macOS · theos/theos Wiki (github.com)
- Features · theos/theos Wiki (github.com)
- NIC · theos/theos Wiki (github.com)

有价值资料：

- Theos - iPhone Development Wiki
- Theos/Setup - iPhone Development Wiki (iphonedevwiki.net)
- NIC - iPhone Development Wiki
- iOS逆向工程之插件开发 | 李峰峰博客 (imlifengfeng.github.io)
- iOS 越狱的Tweak开发 - 简书 (jianshu.com)

其他一些Logos示例代码：

- https://github.com/EamonTracey/TweakWithoutLogos.git
- https://github.com/ZaneH/Tweak-Series.git
- 给锁屏界面画一个红色背景框：
  - Tweak-Series/redrectangle at master · ZaneH/Tweak-Series (github.com)
- ZaneH/Tweak-Series: Repo for YouTube series (github.com)
- Wechatredenvelop (awesomeopensource.com)
  - iOS微信抢红包Tweak安装教程 - Swiftyper
- buginux/WeChatRedEnvelop: iOS版微信抢红包Tweak (github.com)
- https://github.com/kasumar/TweakForWeChatRedEnvelop.git
- Wechatpri (awesomeopensource.com)

iOSOpenDev

- 概述
  - 常用 `iOSOpenDev` 去开发iOS越狱插件
- 详解
  - 详见独立教程：
    - iOS逆向开发：iOSOpenDev开发插件

MonkeyDev

- `MonkeyDev`
  - 概述
    - iOSOpenDev的升级版，可以用来开发越狱插件，也可以用于动态调试ipa
      - Github
        - https://github.com/AloneMonkey/MonkeyDev
  - 详解
    - iOS逆向开发：MonkeyDev调试

插件开发心得

TODO：

- 【已解决】iOS中如何去hook CDStruct类型的变量
- 【已解决】iOS的Logos的Tweak代码中调用self报错：Receiver type for instance message is a forward declaration
- 【未解决】Logos中iOS代码报错：Expected expression
- 【无需解决】Xcode编译iOS的hook代码报错：Expected expression
- 【已解决】Xcode中xm源码中无法看到和添加断点
- 【已解决】Xcode中以源码方式打开xm后缀的文件
- 经验心得=优化
  - 【已解决】研究YouTube逻辑：log日志打印优化每隔几次才输出
- iOS开发
  - 【已解决】iOS的ObjC代码中如何判断对象是否是某个类的实例
  - 【已解决】iOS的ObjC中判断字符串是否包含某个子字符串
  - 【已解决】Mac中用gem安装Cocoapods报错：ERROR SSL verification error at depth 0 ok 0 Unable to download data from https://ruby.taobao.org/
  - 【已解决】搞懂iOS中ObjC的setter函数定义

附录

下面列出相关参考资料。

参考资料

- 【已解决】Mac中初始化和安装Theos开发环境
- 【已解决】用theos开发越狱iOS改机扩展插件
- 【整理】iOS越狱扩展插件开发工具：Theos
- 【整理】iOS越狱Theos开发插件相关参考代码
- 【已解决】Mac中git clone报错：xcrun error invalid active developer path
- 【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】iOS中Cydia Substrate
- 【未解决】iOS越狱检测手段：__RESTRICT
- 【整理】iOS越狱后的app：Substitute
- 【已解决】Substitute相关动态库包含哪些API接口函数
-
- MidnightTeam/substitute: A free runtime modification library. (github.com)
- Package: Substitute • com.ex.substitute • Bingn... (ios-repo-updates.com)
- comex/substitute: A free runtime modification library. (github.com)
- FAQ | Cydia Substrate
- Getting Started
- Blocking Code Injection on iOS and OS X (pewpewthespells.com)
- Frida • A world-class dynamic instrumentation framework
- Tutorial Creating tweaks without Logos directly from Xcode : jailbreakdevelopers (reddit.com)
- steipete/Aspects: Delightful, simple library for aspect oriented programming in Objective-C and Swift.
- theos/theos: A cross-platform suite of tools for building and deploying software for iOS and other platforms. (github.com)
- Home · theos/theos Wiki (github.com)
- Installation · theos/theos Wiki (github.com)
- Theos - iPhone Development Wiki
- iOS Tweak进阶 – 六阿哥博客 (6ag.cn)
- theos/sdks: Patched sdks that include private framework tbds (github.com)
- http://joedj.net/ldid
- iosre/iOSAppReverseEngineering: The world’s 1st book of very detailed iOS App reverse engineering skills :) (github.com)
- https://github.com/iosre/iOSAppReverseEngineering/blob/master/iOSAppReverseEngineering.pdf
- New to Jailbreak Tweak Development, Where Do I Start? : jailbreakdevelopers (reddit.com)
- [Tutorial] Developing a simple CydiaSubstrate tweak : jailbreak (reddit.com)
- Developing an iOS 12 substrate tweak – KaplanDevBlog (wordpress.com)
- Tweak development for iOS jailbreak(Others-Community) (titanwolf.org)
- [Guide/Tutorial] How to make your first MobileSubstrate Tweak using THEOS and no prior
- Objective-C knowledge! : jailbreak (reddit.com)
- Theos - iPhone Development Wiki
- Theos/Setup - iPhone Development Wiki (iphonedevwiki.net)
- iOS Tweak Development Series - YouTube
- https://www.youtube.com/playlist?list=PLFWEDfSyl7h9JFTfKD4qBdh_5OjZ1DdAw
- Installing Theos - iOS Tweak Development Part 1 - YouTube
- iOS Tutorial - CydiaSubstrate tweak (sodocumentation.net)
- Wechat_tweak (awesomeopensource.com)
- iOS 越狱的Tweak开发 - 简书 (jianshu.com)
- Theos - iPhone Development Wiki
- objective c - is there anywhere where I could start MobileSubstrate tweaks programming? - Stack Overflow

- theiostream/theos-ref: Theos Docs! (because there never was a chapter 2) (github.com)
- Theos - iPhone Development Wiki
- Logos - iPhone Development Wiki
- Logify - iPhone Development Wiki
- theos/theos: A cross-platform suite of tools for building and deploying software for iOS and other platforms. (github.com)
- [Tutorial] TweakWithoutLogos | A brief tweak development guide without Logos : jailbreak (reddit.com)
- xcode - Git is not working after macOS Update (xcrun: error: invalid active developer path (/Library/Developer/CommandLineTools) - Stack Overflow