目录

iOS逆向开发

- 最新版本：`v0.6`
- 更新时间：`20221020`

简介

概述如何进行iOS的逆向开发，包括核心流程，即先准备iPhone越狱，再到从app中砸壳出ipa，再到静态分析ipa中二进制，以及动态调试ipa，最后才是相关的iOS逆向开发内容，包括tweak越狱插件开发等内容。

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_reverse_dev: iOS逆向开发

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 book.crifan.org
- iOS逆向开发 crifan.github.io

离线下载阅读

- iOS逆向开发 PDF
- iOS逆向开发 ePub
- iOS逆向开发 Mobi

版权说明

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。

更多其他电子书

本人 `crifan` 还写了其他 `100+` 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

概述

TODO:

把之前已发布的：

GitHub - crifan/prevent_iphone_hacked_ios_security: 防止iPhone被黑：iOS安全

https://github.com/crifan/prevent_iphone_hacked_ios_security

整合进来

iOS逆向概述

为了新手对于iOS逆向开发有个更全面直观的了解，下面先对iOS逆向开发做个总体的概述

iOS逆向领域架构图

此处整理，iOS逆向所涉及到等多个领域的知识，以及每个领域之间的关系，即：

iOS逆向领域架构图

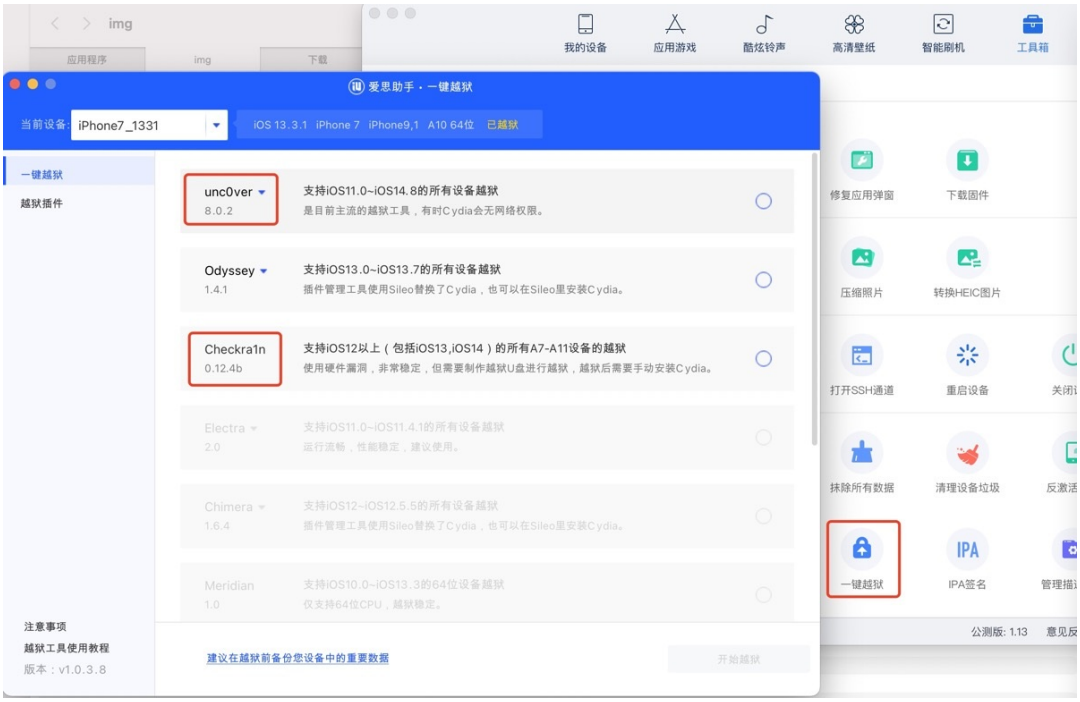
- 在线浏览（支持缩放）
  - iOS逆向开发内容架构图 | ProcessOn免费在线作图
- 离线查看

iOS逆向内容概述

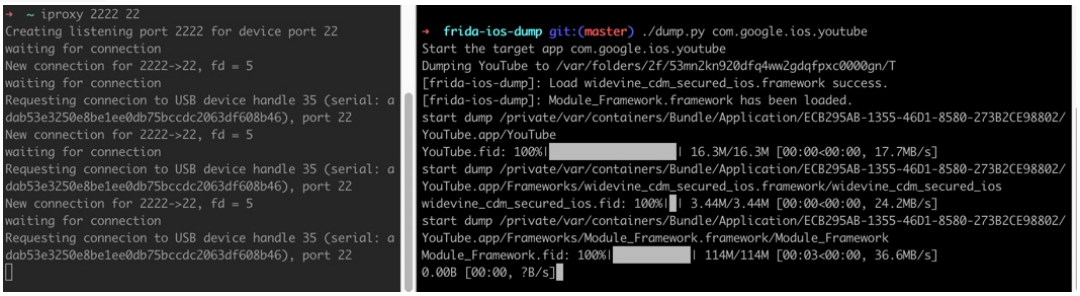
- 先准备越狱iPhone
  - 越狱工具
    - `unc0ver`
      - 自己下载unc0ver到iPhone中
      - 

      - 运行unc0ver去越狱
    - `checkra1n`
      - Mac中运行checkra1n，根据操作提示去越狱

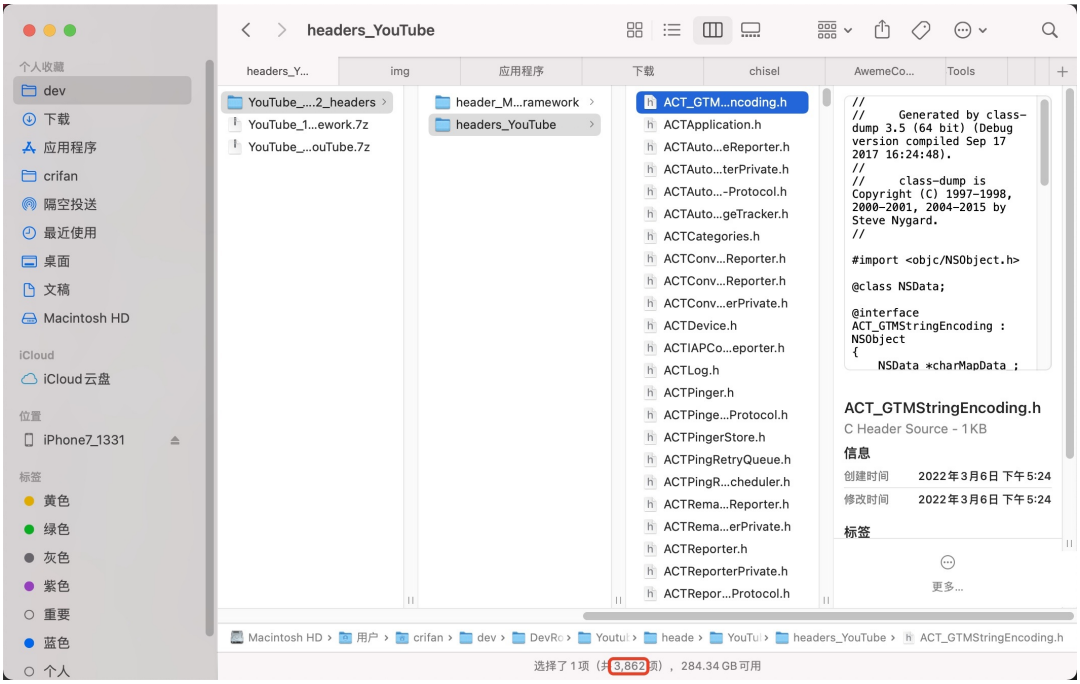
- 也可以借助于 `爱思助手` 的 `一键越狱` 去越狱
  - 底层也是用unc0ver、checkra1n等工具



  - 包括准备好常用越狱插件开发工具，比如
    - `Filza`：文件管理
    - `OpenSSH`：ssh连接操作iPhone
    - `AFC2`：允许通过USB操作iPhone
    - `iCleaner Pro`：临时禁止或启用插件
    - `AppSync Unified`：免签名安装app
    - 等等
- 再从AppStore安装的正版app中砸壳出ipa

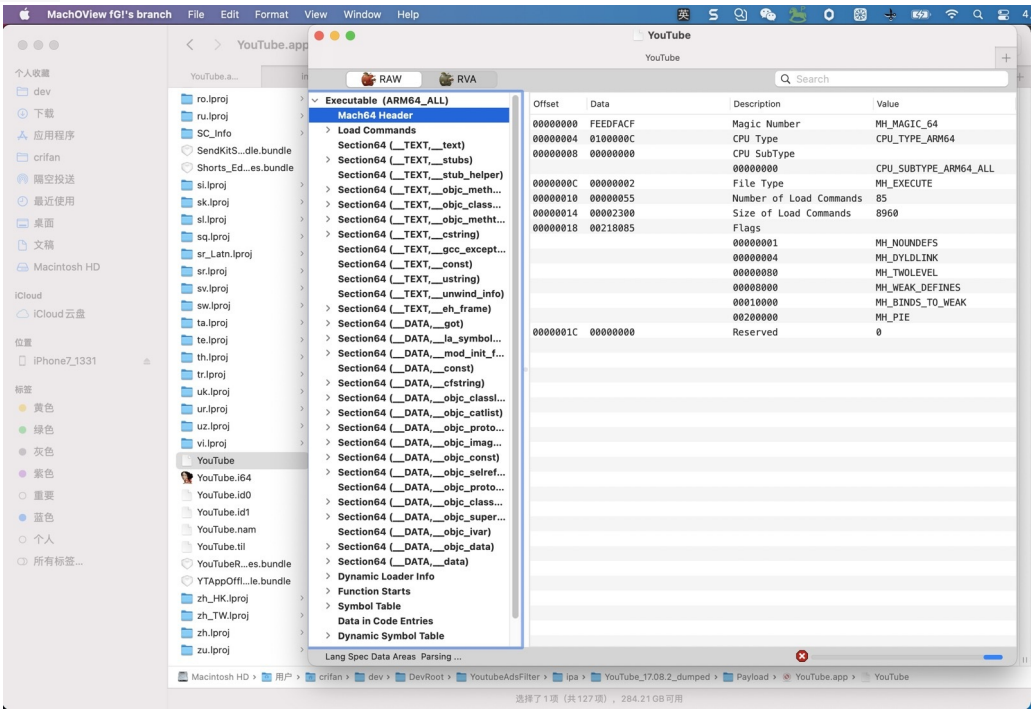
-
  - 常用工具
    - `frida-ios-dump`
      - 

    - `Clutch`
    - `dumpdecrypted`
    - `bfinject`
- 接着才是逆向开发
  - 主要分两类
    - 静态分析
    - 动态调试
  - 下面分别详细解释：
- 静态分析
  - 从脱壳ipa解压得到app包
    - 用class-dump导出头文件



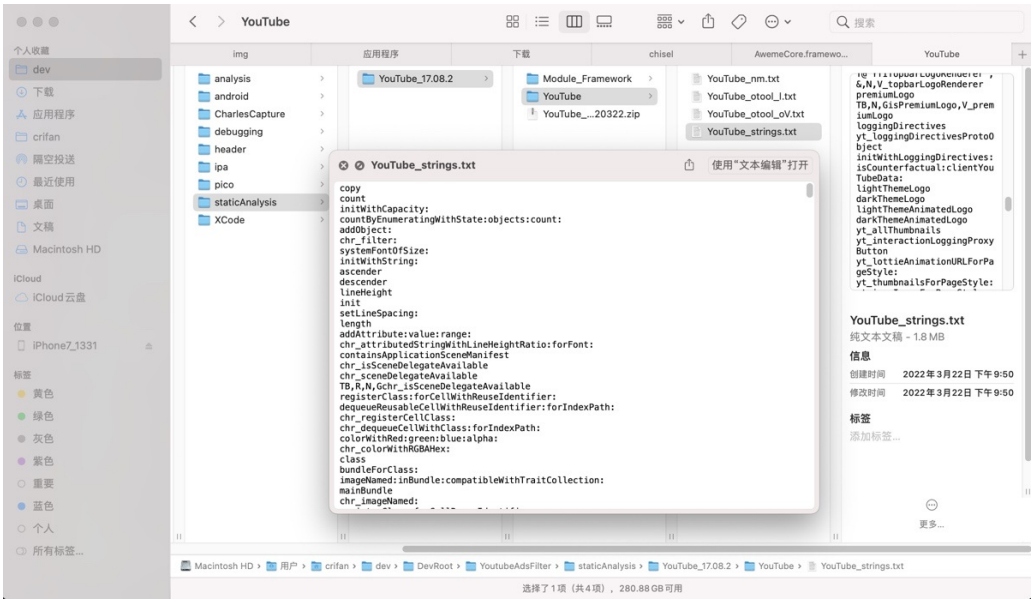
- 以搞懂包含哪些类

- 查看二进制信息
  - `MachOView`



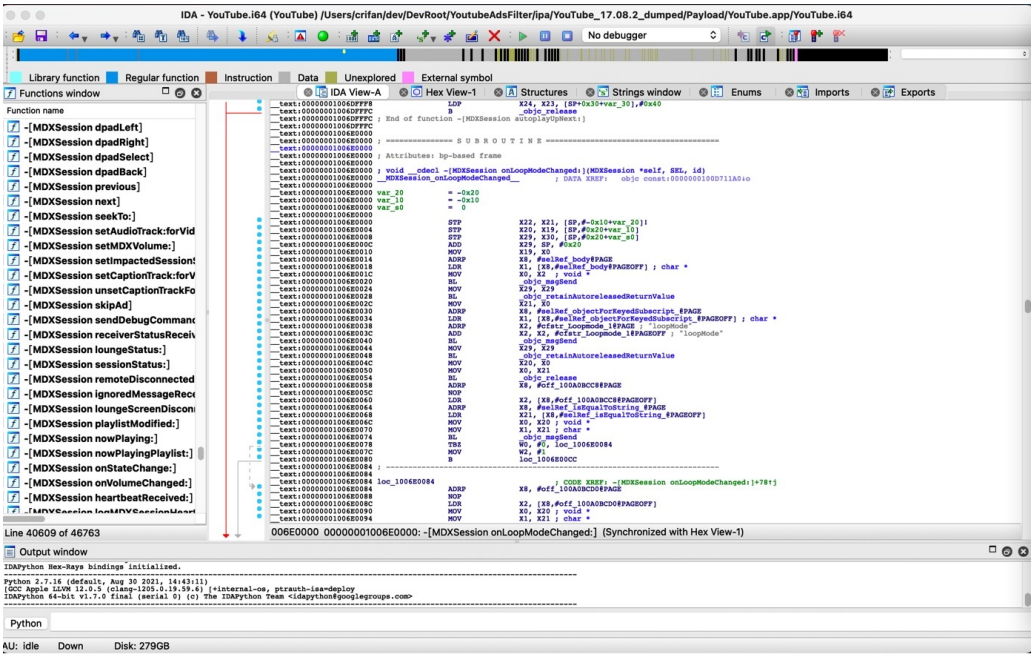
  - `jtool2`
  - `rabin2`

- 导出字符串等资源
  - `strings`

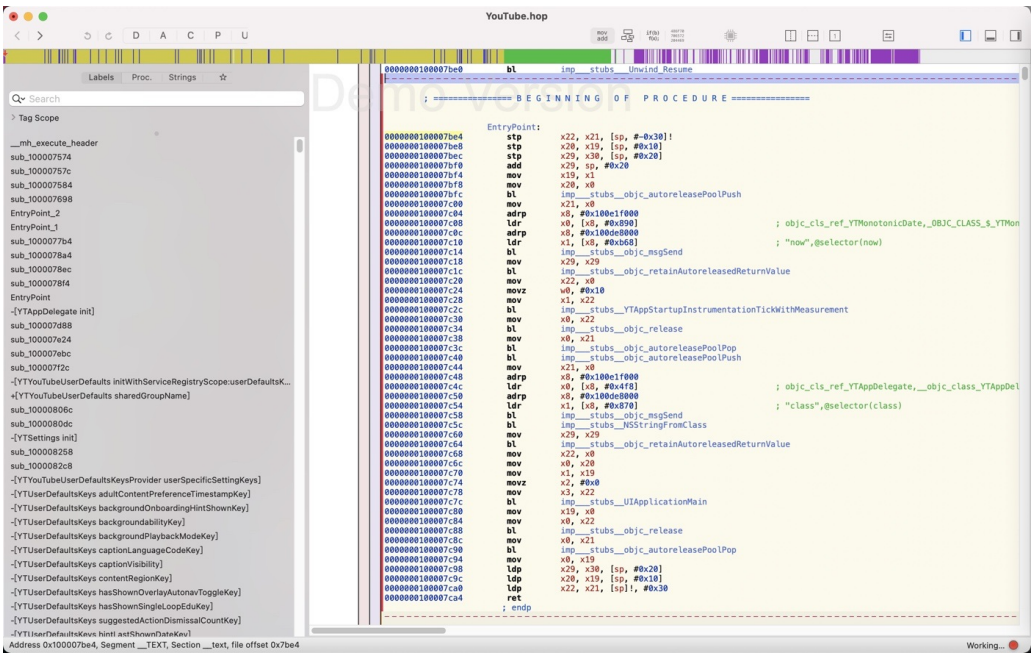


- `nm`
- `otool`
- `jtool2`
- `rabin2`

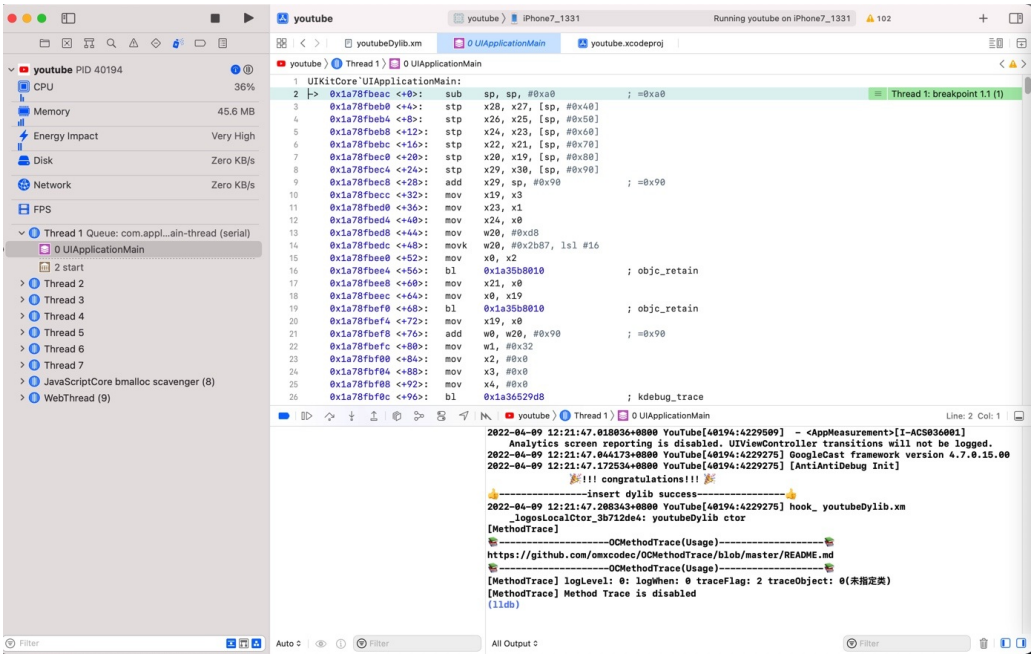
- 分析代码逻辑
  - IDA：Functions、Strings、Imports、F5伪代码等好用的功能模块



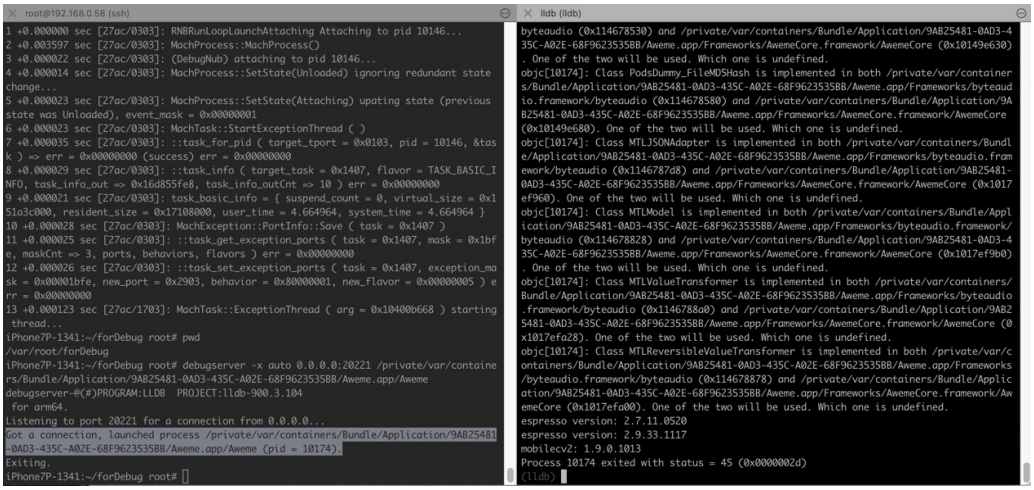
  - Hopper



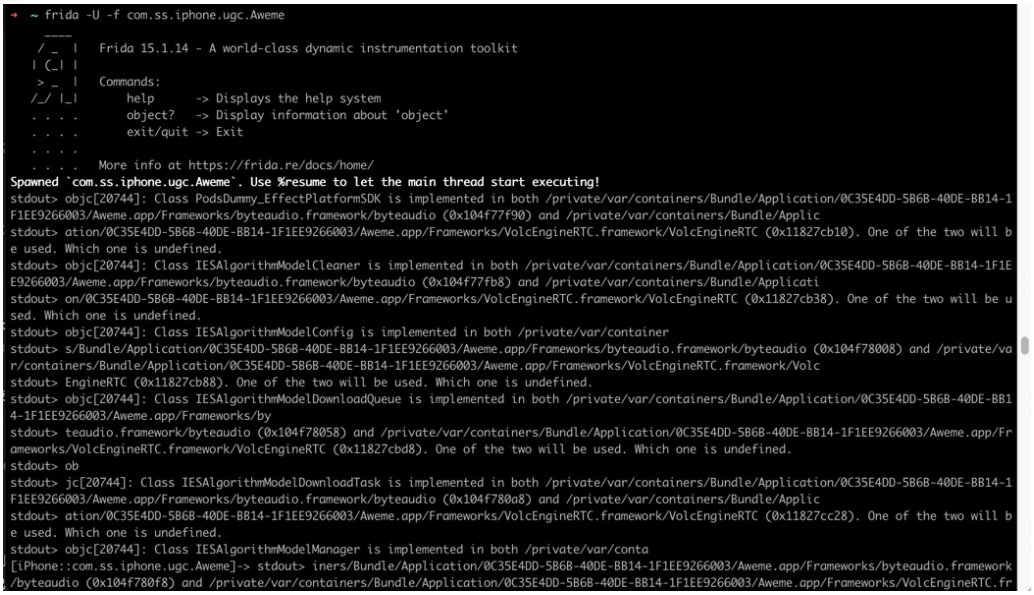
- 动态调试
  - 用各种调试方式和工具去调试app的逻辑
    - 常用调试方式
      - 图形界面：`XCode` + `MonkeyDev`



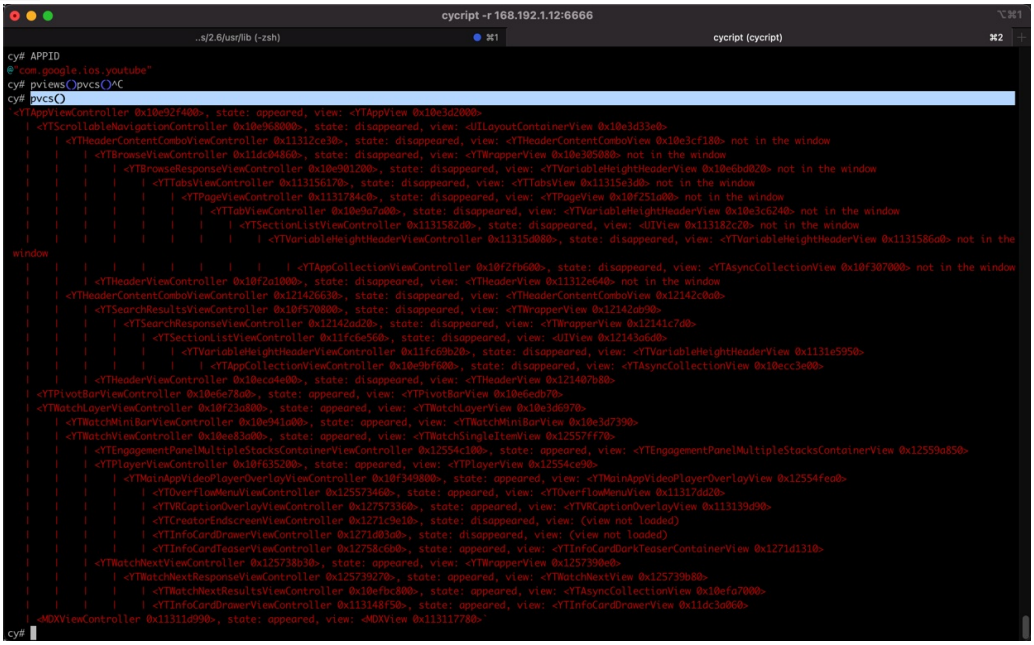
      - XCode内部也有 `lldb`
    - 命令行：`debugserver` + `lldb`



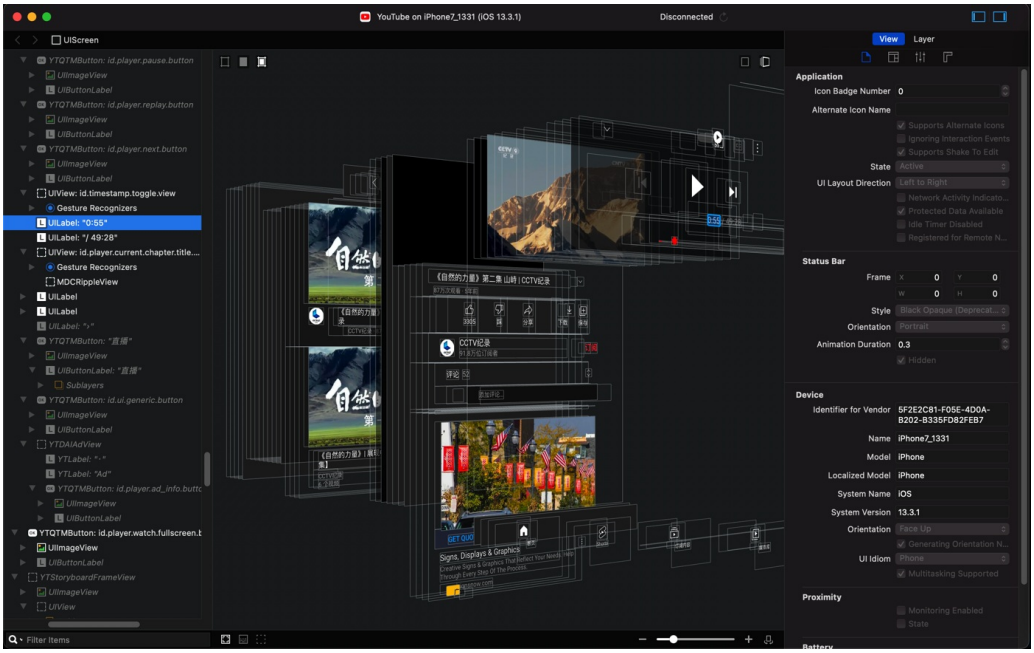
- 常用逆向工具
  - `Frida`： hook对应函数，调试输入参数和返回值



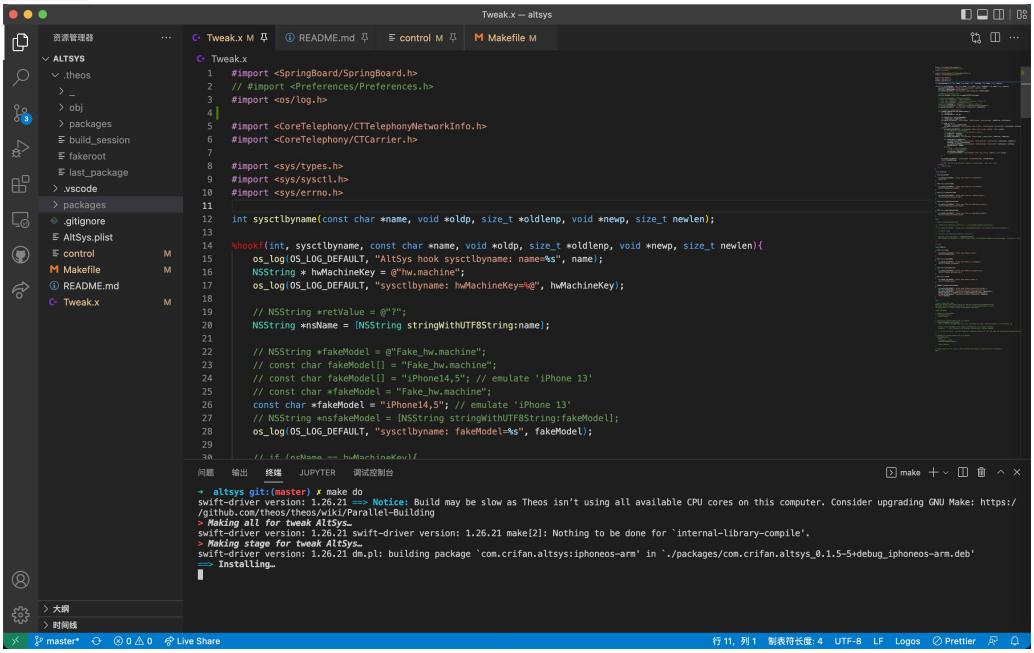
  - `Cycript`： 查看页面元素的类和属性、实时修改各种值



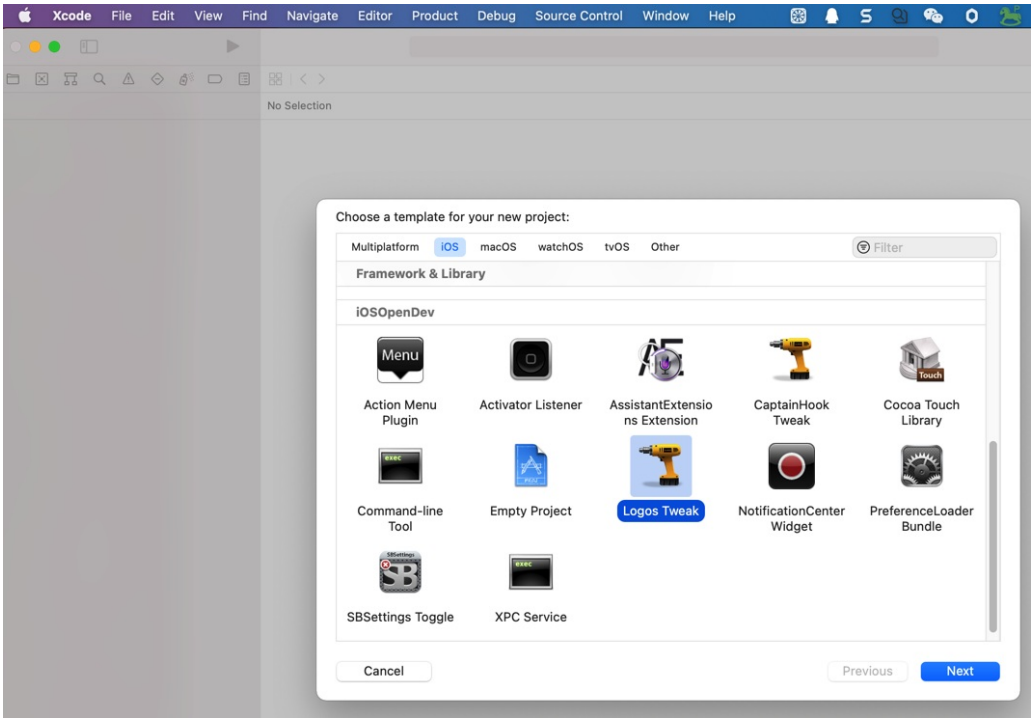
  - `Reveal`： 查看UI页面详细属性



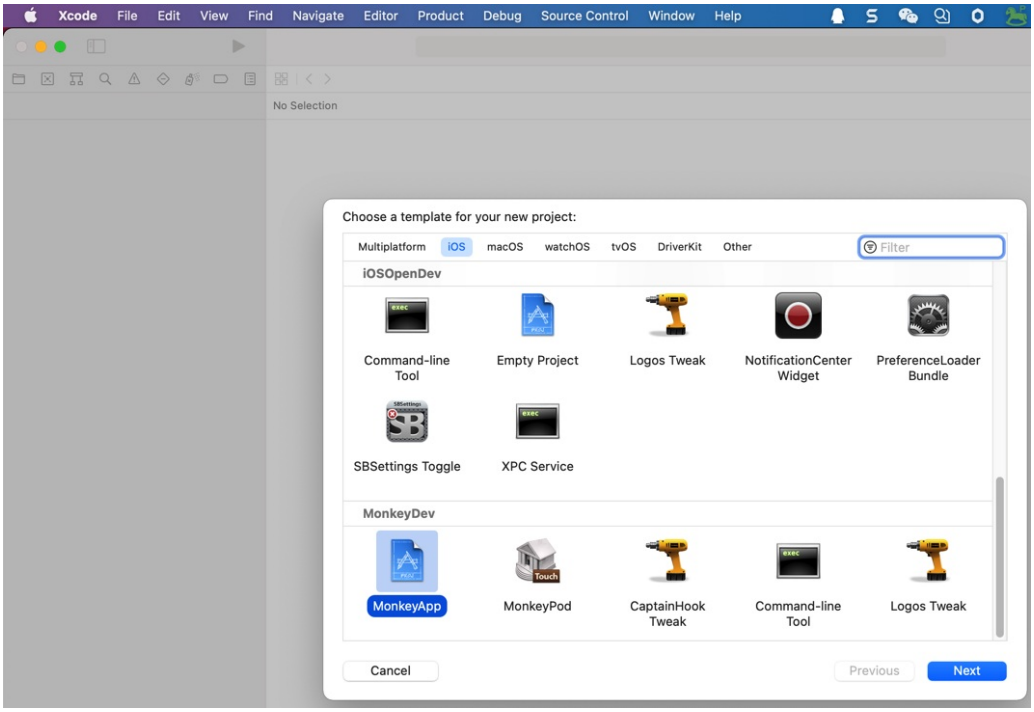
- 目的：搞懂我们所关心的app内部相关逻辑
  - 用于后续去写hook代码去修改成我们要的逻辑和值
- 最后才是：Tweak插件开发
  - 常见插件开发框架
    - 基于 `CydiaSubstrate`
      - `Theos` / `Logos`
    - `fishhook`
    - `CaptainHook`
  - 具体开发方式
    - 命令行
      - `Theos` / `Logos`：写hook源码.xm，基于Makefile去编译

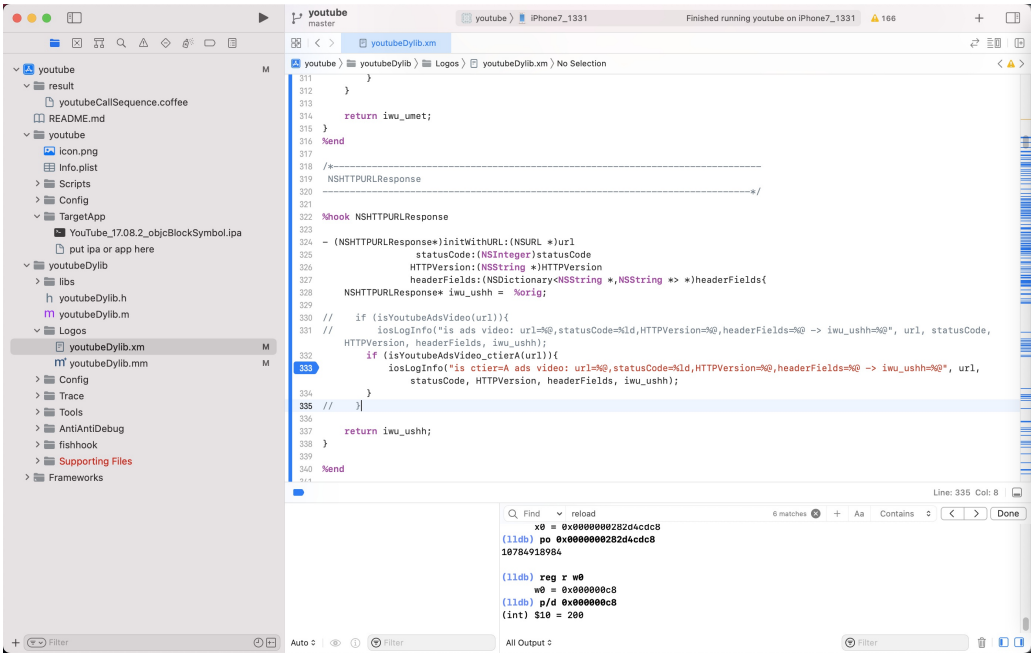


    - 图形界面
      - `iOSOpenDev`：把Logos等开发集成进了XCode
        - 支持Logos、CaptainHook等



- `MonkeyDev`： iOSOpenDev的改进版
  - 支持Logos、CaptainHook等





- 去开发插件=写hook代码
  - 前提：通过静态分析的头文件和动态调试，已知的app内部的类的属性和函数
  - 核心逻辑：去hook对应类的函数和属性
    - 实现对应的效果，比如：
      - 调试：输出函数的输入参数和输出结果
      - 修改逻辑：屏蔽原先逻辑，重写自己想要的逻辑
- 开发出的插件常用于
  - 逆向破解特定app
    - 绕过ssl证书校验，实现Charles抓包https可看到明文数据
    - 修改app原有逻辑，实现特定的功能
      - 支付宝：修改显示的余额
      - 微信：抢红包
      - 抖音：点赞关注
  - 反反调试
  - 反越狱检测

iOS典型逆向开发流程

典型的iOS逆向开发的流程是：

- 先：iPhone越狱
  - 越狱工具
    - unc0ver
    - checkra1n
- 再：逆向破解某iOS的app
  - 对于要研究的某个iOS的app来说，从工作内容角度，主要分：
    - 从AppStore中搜索和安装正版app
    - 去砸壳得到ipa
      - frida-ios-dump
    - 再去研究
      - 静态分析
        - 字符串分析
          - strings
          - nm
          - otool
        - 查看详情
          - MachOView
          - jtool2
          - rabin2
        - 导出头文件
          - class-dump
        - 分析代码逻辑
          - IDA
            - 汇编代码
            - 伪代码
      - 动态调试
        - 命令行方式
          - debugserver + lldb
        - GUI图形界面方式
          - XCode + MonkeyDev
            - lldb
    - 写hook插件
      - 再去调试和验证
        - 如此反复
  - 最后结果：得到一个插件tweak，实现了你要的目的
    - 比如反越狱检测、改机、hook某个app的某些特定功能（比如微信抢红包）等等

iOS逆向的重点和难点

对于iOS逆向开发涉及到众多方面的内容，其中属于重点和难点的是：

- 先搞懂你想要干啥
  - 比如 微信抢红包
- 重点和难点
  - 用静态分析工具和动态调试，共同配合，找出要hook的类
    - 如何用好各种静态分析工具（`otool`、`MachOView`、`IDA Pro`、`Hopper`等），如何进行动态调试（`Xcode`+`MonkeyDev`、`debugserver`+`lldb`、`frida`、`Cycript`、`Reveal`等），从而找到要分析的类和代码运行逻辑等等，才是重点和难点
  - 再去写hook代码，开发出插件，实现对应的功能

子教程

上述所有和iOS逆向开发相关的内容，分别整理到多个独立的子教程以及相关内容：

- 系列
  - 【整理Book】iOS逆向开发：逆向开发流程
  - 【整理Book】iOS逆向开发：iPhone越狱
    - 包括iPhone管理：插件的安装和卸载、文件管理等
  - 【整理Book】iOS逆向开发：越狱插件开发
  - 【整理Book】iOS逆向开发：越狱检测和反越狱检测
  - 【整理Book】iOS逆向开发：抖音逆向
- 相关
  - 【整理Book】iOS逆向心得：Apple苹果相关开发资料 20220527
  - 【整理Book】iOS开发心得
  - 【整理Book】ARM汇编基础知识 20220513
  - 【整理Book】asm汇编开发心得
  - 【整理Book】XCode中lldb 调试心得 开发心得
  - 【整理Book】XCode经验总结：开发心得之调试心得
  - 【整理】XCode经验总结：开发心得之调试心得
  - 【整理Book】IDA Pro使用心得 20220602
  - 【整理Book】iOS逆向心得：Block的相关基础知识

iOS逆向心得

不同app的逆向破解出的难度不同

TODO：

- 【整理】iOS逆向心得：不同app的逆向破解出的难度不同

附录

下面列出相关参考资料。

参考资料

- crifan (Crifan Li)