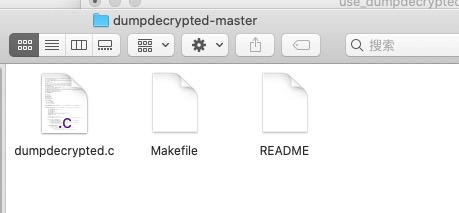
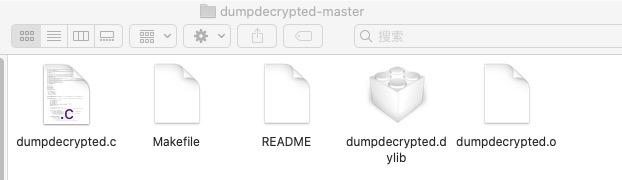
1.去官网下载脱壳工具 <https://github.com/stefanesser/dumpdecrypted>

2.将文件拖拽到桌面，cd到这个dumpdecrypted-master 文件夹下 ，执行make命令

3.将生成的dumpdecrypted.dylib这个库拖进已越狱的手机的/var/root路径下

4.利用MAC上安装的开发证书给动态库签名 ldid -S dumpdecrypted.dylib

5.利用SSH登录iphone, 打开微信程序，利用 ps -A | grep WeChat.app 查看微信的安装路径

假如是/var/containers/Bundle/Application/EB29BBE6-2F89-467F-A1B1-E0FFFCF3AF75/WeChat.app/WeChat

然后执行砸壳命令 DYLD\_INSERT\_LIBRARIES=dumpdecrypted.dylib /var/containers/Bundle/Application/EB29BBE6-2F89-467F-A1B1-E0FFFCF3AF75/WeChat.app/WeChat

6.利用爱思助手将iphone路径下的/var/root/WeChat.decrypted 文件导出到桌面

7. Cd 回到桌面，利用 otool -l WeChat.decrypted |grep cry 查看是不是脱壳成功

8.最后通过 class-dump -H WeChat.decrypted -o wechatHeaders 导出头文件

wechatHeaders 是自己创建的文件夹，用来存放头文件的