Atitit ios反编译 attilax总结

##### **iOS app可以“有条件”地被反编译**

首先，告诉大家一个不幸的消息，上架至App Store的app，被apple加密了。所以标题才是“有条件”才能进行反编译，令人欣喜的是，在debug下产生的ipa或者是release下的ipa包或者是渠道包（各种应用市场能下的ipa包）都能直接反编译。

##### **脱掉App Store给“二级制文件”穿上的外衣**

当然，引言已经说了，道高一尺魔高一丈，就算是被apple加密的ipa，其实也是可以反编译的，只不过相对麻烦罢了。  
来来来，给你们几个工具，就可以解掉apple的加密了

* clutch
* dumpdecrypted
* gdb
* AppCrackr

由于AppCrackr被很多开发者吐槽，这个傻瓜式的解密会严重导致盗版泛滥，所以这个工具已经很不好用了。

##### **如何利用工具去反编译**

这里会介绍两个工具****class-dump****和****Hopper Disassembler****

现在仅讨论代码层面的反编译

1、反编译工具

（1）class-dump

主要用来反编译一个库文件或者app的方法名、属性等声明（即.h文件，强大的是反编译出来的.h不仅仅包含头文件中的声明，.m中的function方法名称也同样能够反编译出来）。class-dump的安装在前文中有详细描述，这里不再赘述。

（2）IDA

主要用来反编译库文件的实现（当然方法声明同样能够反编译出来，用class-dump主要是更加形象，有针对性），这个反编译工具非常强大能够将函数的实现及逻辑关系、流程统统显示出来，弊端就是反编译出来的内容为汇编语言，需要一定汇编基础的才能看懂。比较头疼。

（3）Hopper Disassembler

与IDA功能相似，主要功能都是反编译查看方法的实现，这个软件的功能相对于IDA来说，可读性要强很多，反编译出来的内容类似于汇编与OC的运行时的结合体，相对比较容易看出方法的具体实现。

笔者个人比较喜欢用1和3来完成反编译过程。

各个软件的下载地址：

（1）class-dump

[http://stevenygard.com/projects/class-dump](http://stevenygard.com/projects/class-dump" \t "http://blog.csdn.net/cjh965063777/article/details/_blank)

（2） IDA

[https://www.hex-rays.com/products/ida/support/download\_demo.shtml](https://www.hex-rays.com/products/ida/support/download_demo.shtml" \t "http://blog.csdn.net/cjh965063777/article/details/_blank)

（3）Hopper

手把手教你反编译别人的app - 简书.html

关于iOS开发中反编译的那些事儿 - 小白的专栏 - 博客频道 - CSDN.NET.html