

1. 字符串，特征字

根据程序运行中出现的特征字词进行搜索，从而获取定位到程序的相关位置之中。此前该方法使用较多，当前一般很难找到需要的关键词，有时需要对特征字段进行拆分搜索，才能获得一些进展。

2. 关键 api 的监控

通过挂钩关键的系统 api，获取程序运行时的数据，进而分析程序行为，从程序行为入手逼近关键点。该方法比较难，需要对 Android 函数和编程相当熟悉才能使用。

3. 挂钩解密函数

使用 Xposed 或者 Cydia 之类的 Hook 框架，编写 Hook 代码，对需要的函数设置钩子，动态 dump 出需要的信息。

4. Monitor

1) DDMS

Android Log 信息，是 Android 程序运行过程中产生的一些运行信息。这些信息可能是由目标程序产生的，也可能是系统运行过程中，由系统进程产生的。能够提供非常多的信息，遇到问题，先去分析 log。

2) Thread

跟踪程序运行中的各个 Thread 的调用和运行类

3) Method Trace

进程函数调用跟踪，一般会跟踪到很多的 Trace 函数，比较复杂，需要花费很多的时间去分析 Trace 数据

startMethodTracing() --- stopMethodTracing()

5. 插入 Log 信息

对自己关注的地方，手动插入打印 log 信息的函数，自动打印出程序运行时的参数。

6. 动态调试

功能强大，熟悉了之后对程序分析非常有用。