目录

Android逆向：动态调试

- 最新版本：`v1.6.0`
- 更新时间：`20240729`

简介

介绍Android逆向开发期间，如何动态调试安卓程序。包括用AndroidStudio调试apk的smali代码、用LLDB调试安卓程序、用Frida调试安卓程序、编写Xposed模块去调试安卓程序。对于AndroidStudio调试安卓Smali代码，此处以YouTube为例，介绍主要步骤：确保安卓已root、调试工具选择、反编译出smali代码、确保app可调试、调试方式启动app、Android Studio中导入smali代码、给smali加断点、配置Android Studio项目、确保adb可获取进程列表、Android Studio调试app进程；对于LLDB调试安卓，包括下载安卓版lldb-server到电脑、把lldb-server传输下载到安卓手机中、电脑中运行lldb、用lldb连接安卓手机中的lldb-server、最后是开始用lldb调试安卓app进程。对于Firda调试安卓，包括初始化Frida调试环境、Frida调试安卓app，以及贴出几个实例包括LiftFileManager、DisplayDemo等。以及Frida方面的常见的问题和心得。然后是动态调试方面的一些常见问题和心得。以及其他一些分析调试工具，包括Unidbg、AndBug、redexer、Fino等；以及用于辅助调试的adb，比如用adb查看内存映射；最后加上心得和实例和附录的参考资料。

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/android_re_dynamic_debug: Android逆向：动态调试

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

- Android逆向：动态调试 book.crifan.org
- Android逆向：动态调试 crifan.github.io

离线下载阅读

- Android逆向：动态调试 PDF
- Android逆向：动态调试 ePub
- Android逆向：动态调试 Mobi

版权和用途说明

此电子书教程的全部内容，如无特别说明，均为本人原创。其中部分内容参考自网络，均已备注了出处。如发现有侵权，请通过邮箱联系我 `admin 艾特 crifan.com`，我会尽快删除。谢谢合作。

各种技术类教程，仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途，均与本人无关。

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

Android逆向动态调试概览

关于安卓逆向，之前已通过安卓应用的安全和破解进行了一定的介绍。

而安卓逆向期间，除了 `静态分析` 去研究 `反编译的代码` 外，想要了解安卓app的底层机制和逻辑，需要通过 `动态调试` 。

而目前安卓的动态调试的一些主要方法有：

- 用 `Android Studio` 去调试（ `apk` 反编译得到的） `smali` 代码
- 用 `LLDB` 调试安卓app
- 用 `Frida` 调试安卓app
- 给安卓app编写 `XPosed` 插件，去调试hook逻辑
  - 详见：Xposed插件开发 · 安卓逆向调试：XPosed框架

此教程主要就是介绍这方面的详细内容。

安卓逆向动态调试的总体思路

TODO：

【未解决】Android的YouTube逆向：研究request请求api和protobuf相关部分代码

此处介绍安卓逆向的总体思路：

- 找到要hook的点 = 找到核心代码的入口点
  - 对于Android来说，往往是 `java` 中相关的 `基础的类` ， `内置的类`
  - 比如
    - `网络请求` 类
    - `url` 相关的类
      - 比如
        - `new URL`
    - `字符串` 相关的类
      - 可能会用到URL拼接，其内部涉及到 `字符串` 的拼接
      - 比如
        - `append`
        - `getBytes`
        - `String builder`
- 再去动态调试逻辑，hook代码逻辑
  - 相关工具： `Xposed` 、 `frida` 、 `LLDB` 、 `AS` 等
- 期间配合抓包
  - 先要 `抓包` 找相关 `url`
    - 后续才知道要过滤哪些url

找到要hook的点

其中关于找到要hook的点，值得就是：

- java层：找到对应的，实现你要的功能的类
  - 其中切入点，可以从Java基础的类去入手
    - 详见下面的解释
- Native层=C/C++代码= `so` 库文件：找到C/C++的函数

Java基础的内置的类

URL

```
URL myURL = new URL("http://example.com/pages/");
URL page1URL = new URL(myURL, "page1.html");
URL page2URL = new URL(myURL, "page2.html");
```

或：

```
new URL("http", "example.com", "/pages/page1.html");
```

或：

```
//URLDemo.java
import          *;

public class URLDemo {

  public static void main(String[] args) {
    try {
      URL url = new URL("http://www.javatpoint.com/java-tutorial");

      System.out.println("Protocol: " + url.getProtocol());
      System.out.println("Host Name: " + url.getHost());
      System.out.println("Port Number: " + url.getPort());
      System.out.println("File Name: " + url.getFile());
    } catch (Exception e) {
      System.out.println(e);
    }
  }
}
```

或：

```
import          *;

URL url = new URL("/a-guide-to-java-sockets");

URL home = new URL("http://baeldung.com");
URL url = new URL(home, "a-guide-to-java-sockets");
```

或：

```
@Test
public void givenBaseUrl_whenCreatesRelativeUrl_thenCorrect() {
    URL baseUrl = new URL("http://baeldung.com");
    URL relativeUrl = new URL(baseUrl, "a-guide-to-java-sockets");

    assertEquals("http://baeldung.com/a-guide-to-java-sockets",
      relativeUrl.toString());
}
```

或：

```
URL url = new URL(yourUrl, "/api/v1/status.xml");
```

或：

```
URL domain = new URL("http://example.com");
URL url = new URL(domain + "/files/resource.xml");
```

hook插件与开发

TODO：

- 把如何用XPosed写Android的hook插件的帖子整理过来
-
- 【已解决】Android 11的Magisk中安装EdXposed 0.5.2.2结果失败：请先从Magisk Manager中安装Riru Installation failed
- 【已解决】在Android 11中安装EdXposed框架

- Android的Hook插件开发框架
  - XPosed
  - `Cydia Substrate`

用AndroidStudio调试smali详细步骤

TODO：

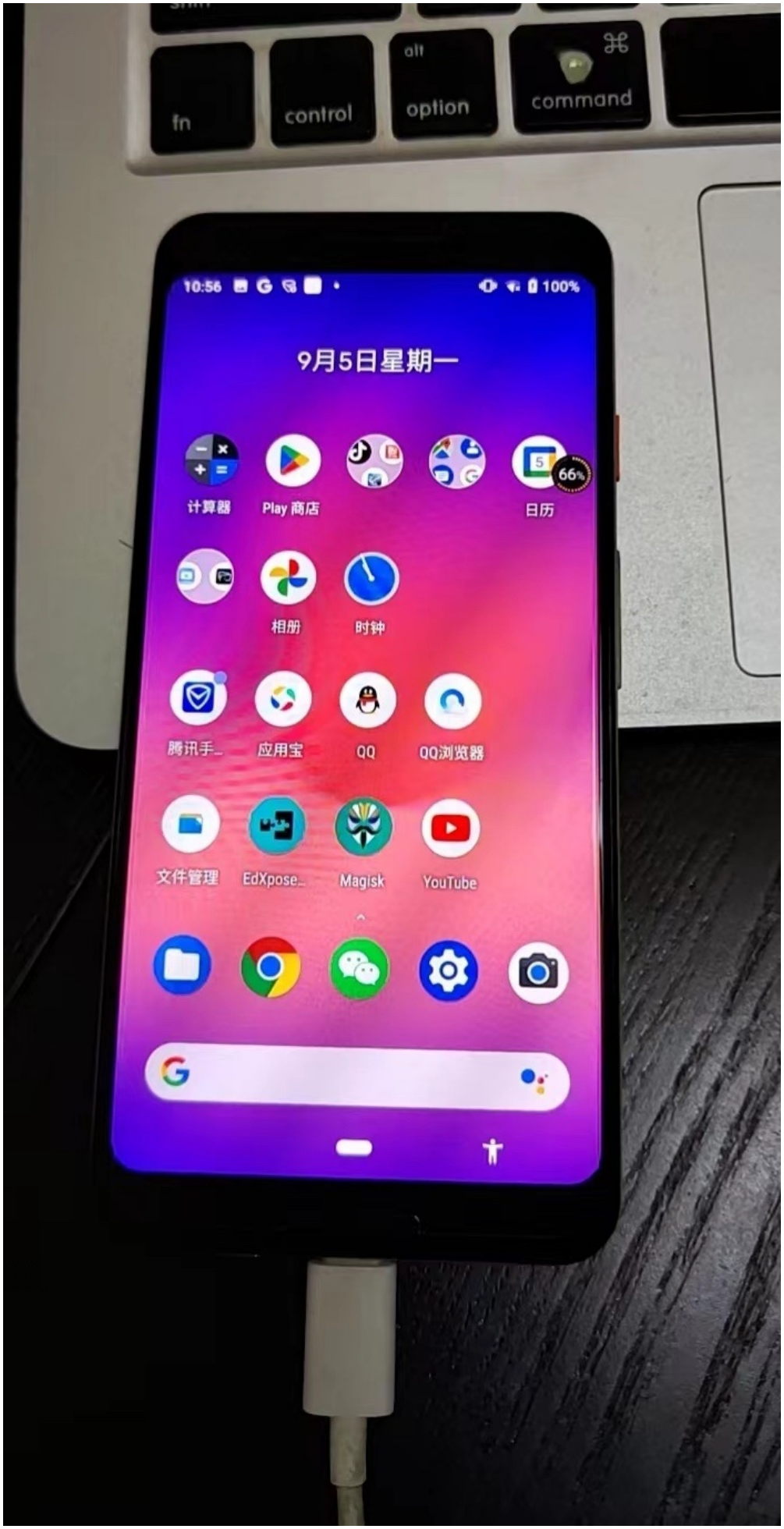
- Smalise
  - 【记录】试用VSCode的smali插件：Smalise

详细步骤

确保安卓已root

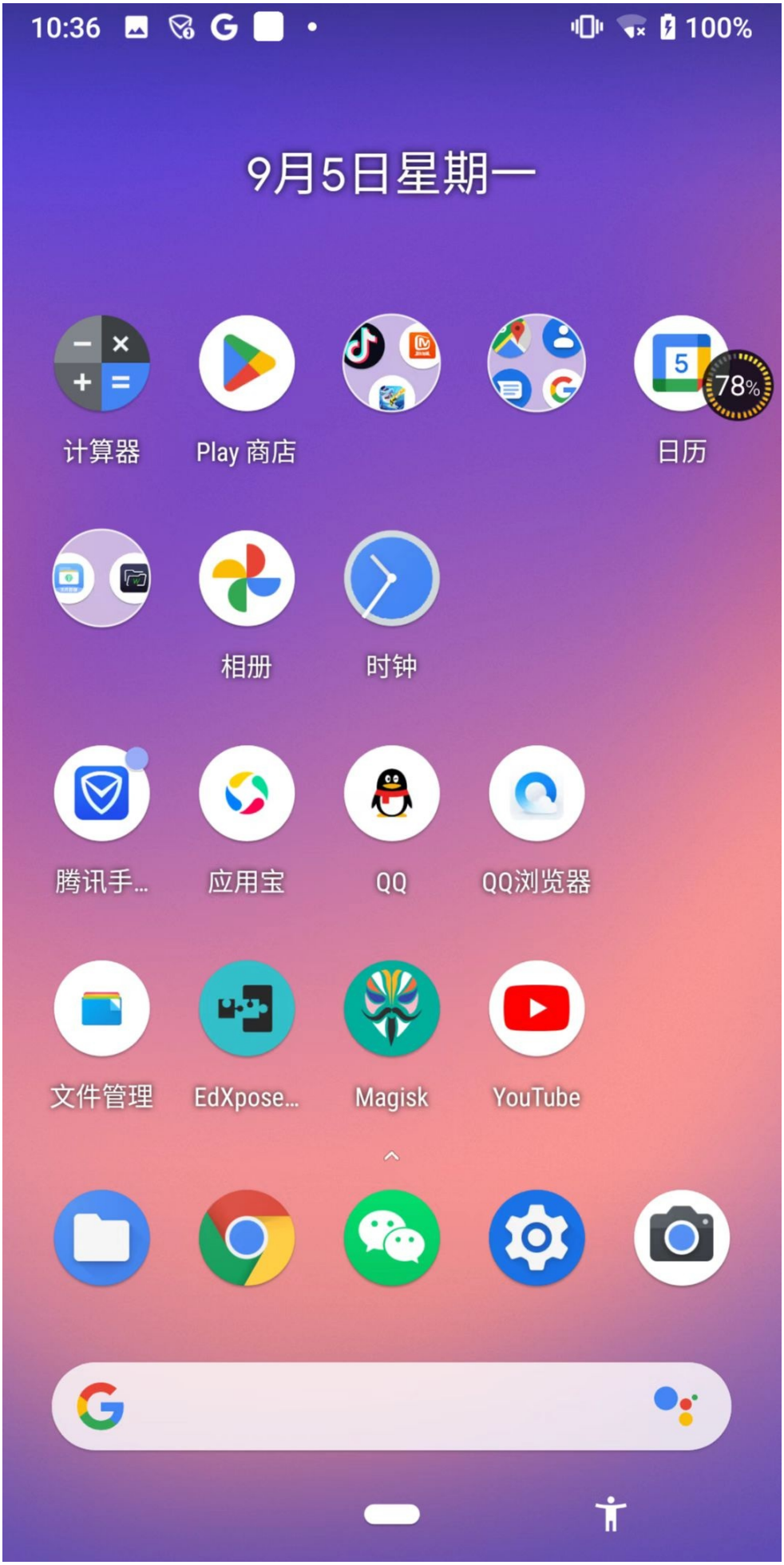
确保安卓设备已root：

此处之前买的二手的`Google Pixel 3`，已root：

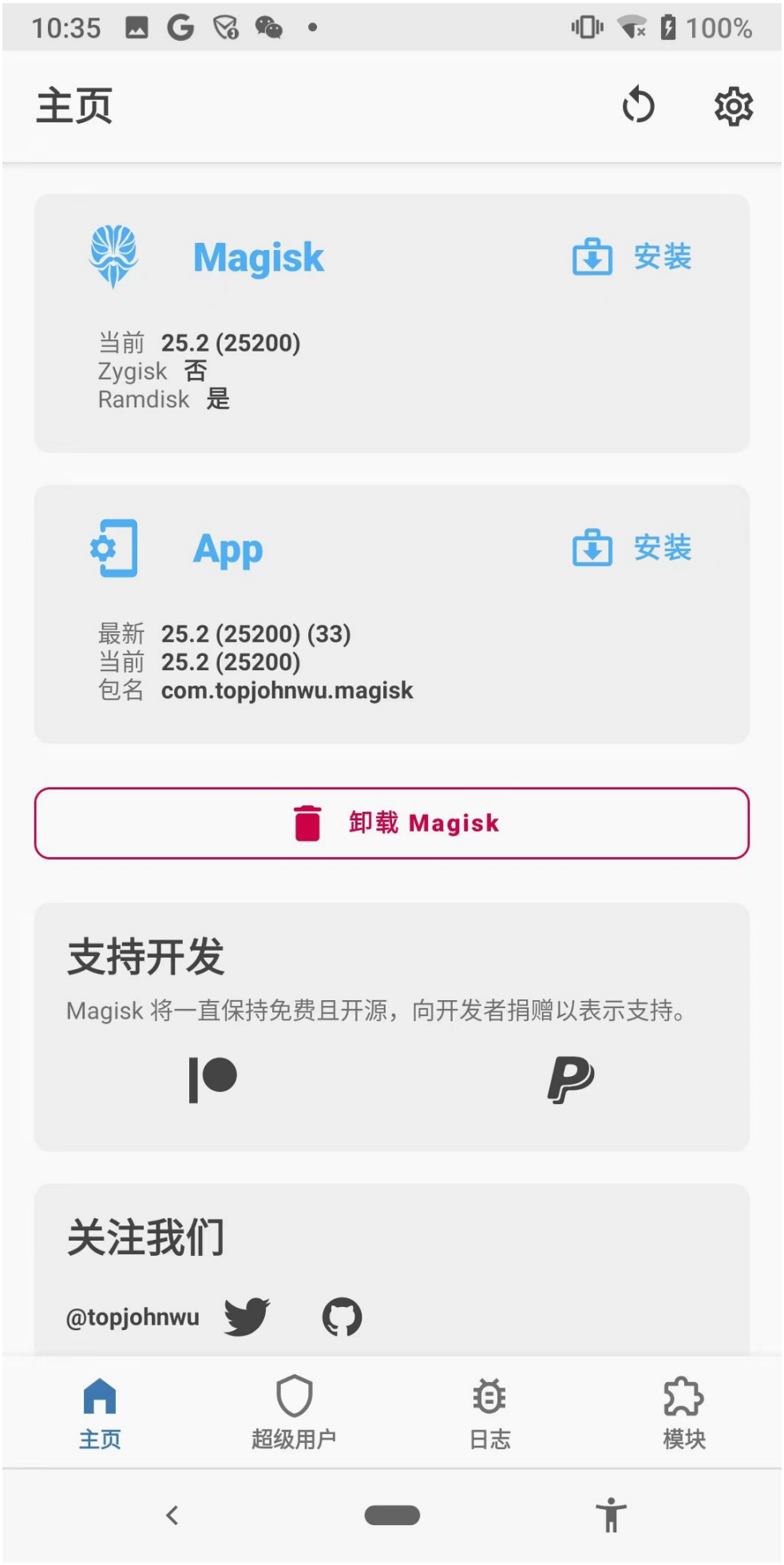

fn
control
alt
option
command
10:56
100%
9月5日星期一
计算器
Play 商店
日历
66%
相册
时钟
腾讯手...
应用宝
QQ
QQ浏览器
文件管理
EdXpose...
Magisk
YouTube

自带安装了：

- `Magisk Manager`
  - 图
    -


10:36
100%
9月5日星期一
计算器
Play 商店
日历
78%
相册
时钟
腾讯手...
应用宝
QQ
QQ浏览器
文件管理
EdXpose...
Magisk
YouTube

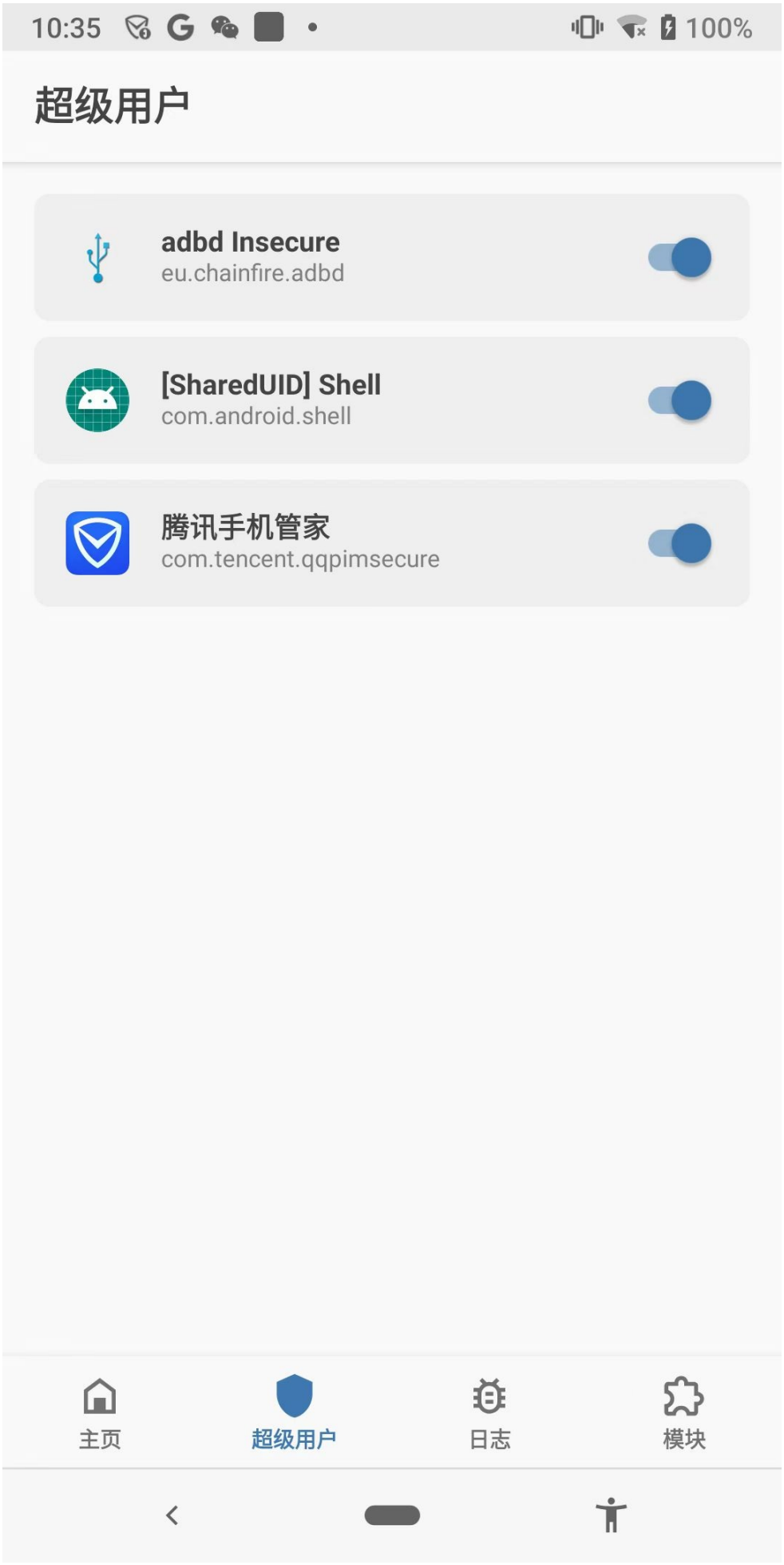
-


10:35
100%
主页
Magisk
安装
当前 25.2 (25200)
Zygisk 否
Ramdisk 是
App
安装
最新 25.2 (25200) (33)
当前 25.2 (25200)
包名 com.topjohnwu.magisk
卸载 Magisk
支持开发
Magisk 将一直保持免费且开源，向开发者捐赠以表示支持。
关注我们
@topjohnwu
主页
超级用户
日志
模块

    - 升级后是：`Magisk`
        - 内部包含：
            - `Magisk`（的框架）
            - `App` = `Manager`：管理配置界面的app

且已给相关app授权了root权限：

- （对应着）`adb shell` 中首次 `su` 后，即可申请 `root权限`，允许后，此处就会出现：
    - `Shell` = `com.android.shell`
        -


10:35
100%
超级用户
adbd Insecure
eu.chainfire.adbd
[SharedUID] Shell
com.android.shell
腾讯手机管家
com.tencent.qqpimsecure
主页
超级用户
日志
模块

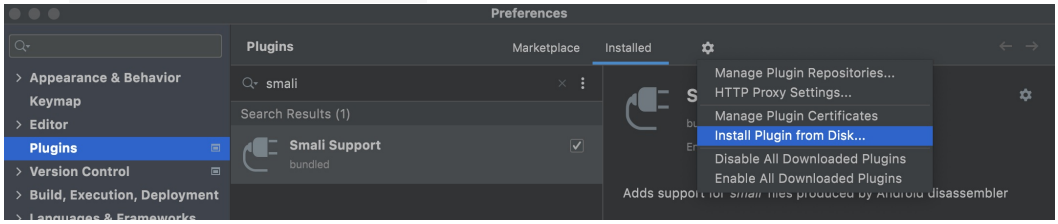
调试工具选择

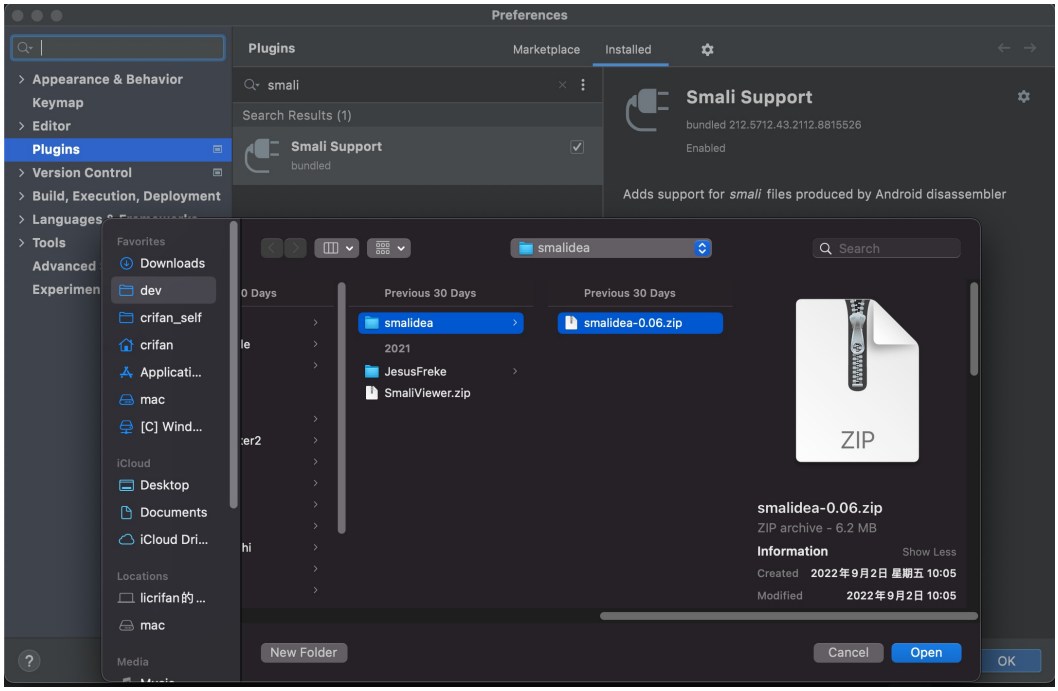
- 调试安卓apk 的工具/环境
  - `Android Studio` + `smalidea` 插件：调试 `smali`
  - `JDB` ：调试 `Smali`
  - `IDA` ：调试 `dex`
  - `Qtrace`

此处选择，相对易用的：

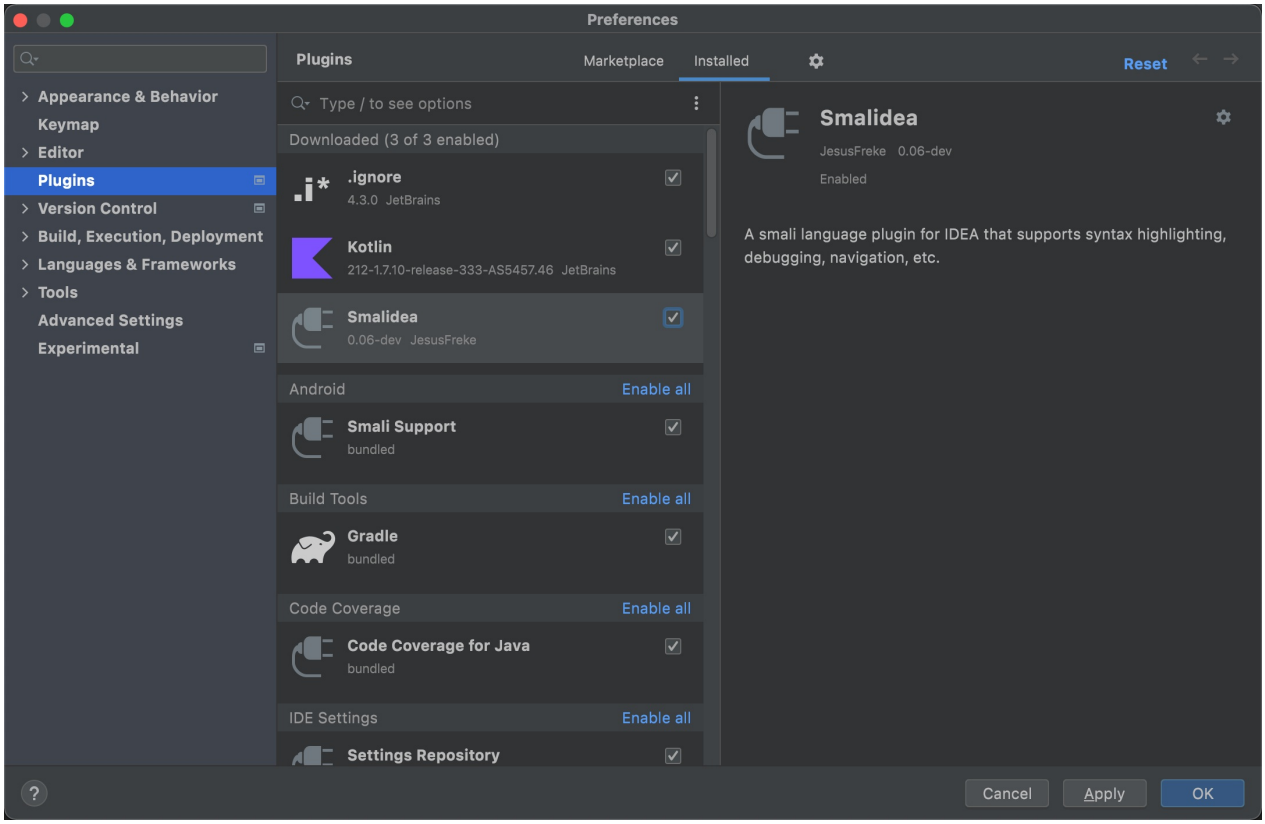
- `Android Studio` + `smalidea` 插件：调试 `smali`

Android Studio中安装smali插件 `smalidea`

- 安装AS插件：`Smalidea`
  - AS中搜索并点击安装 `Smalidea`
  - 手动下载zip从再手动安装
    - 从JesusFreke / smalidea / Downloads — Bitbucket下载插件压缩包文件
      - https://bitbucket.org/JesusFreke/smalidea/downloads/smalidea-0.06.zip
    - 然后AS中 `Install Plugin from Disk`
    - 

    - 

-> 安装后的 `Smalidea` 插件：



反编译出smali

反编译 `apk` ，得到 `smali` 源码

常见反编译工具：

- Apktool
  - 直接1步：apk to smali
- baksmali
  - 要2步：先 apk to dex，再 dex to smali

此处用 `apktool` 去反编译YouTube的apk：

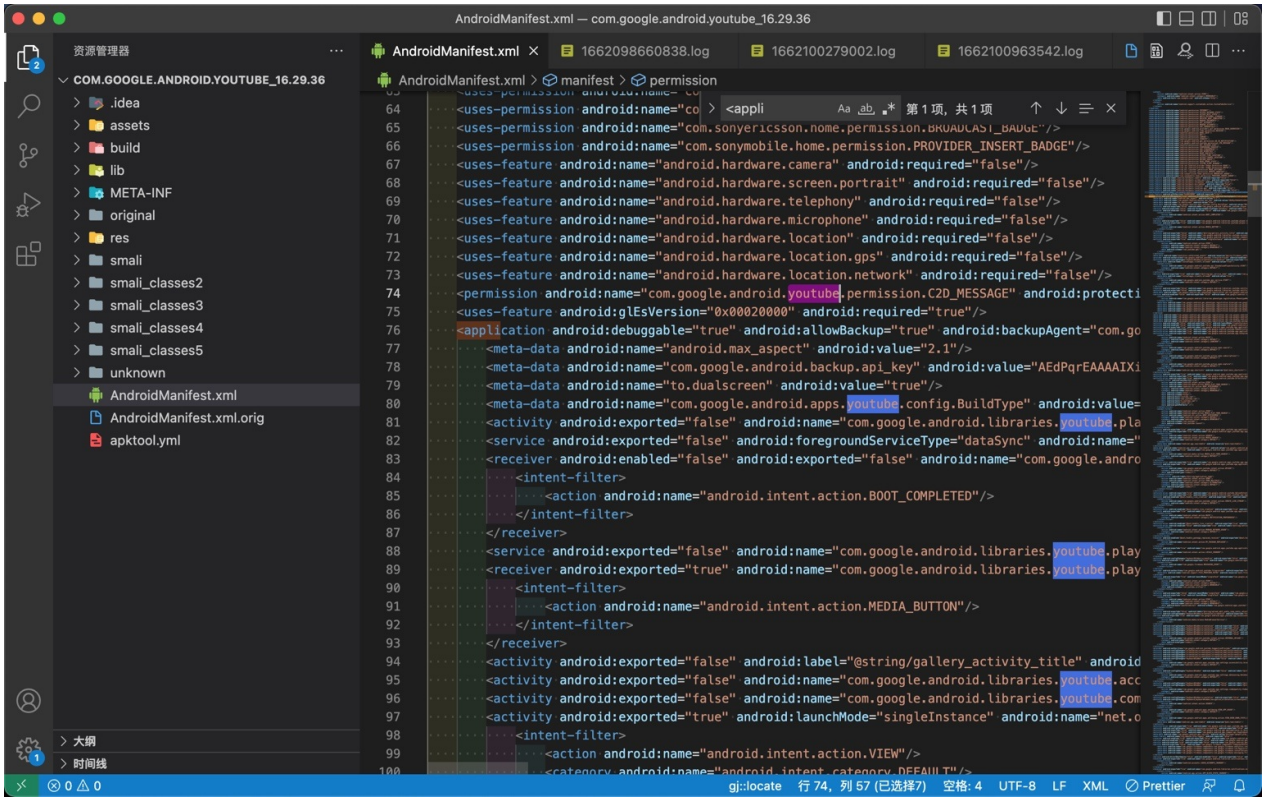
去反编译得到包含 `smali` 源码的目录：

```
apktool d --use-aapt2 ../../apk/16.29.36/com.google.android.youtube_16.29.36.apk
```

如果要指定输出目录，也可以加上 `-o`

```
apktool d --use-aapt2 ../../apk/16.29.36/com.google.android.youtube_16.29.36.apk -o com.google.android.youtube_16.29.36_aapt2
```

输出的目录的内容：



- 一个或多个 `smali` 目录
  - 注：每个 `smali` 目录，对应着 `apk` 内部的 `dex` 文件
- `AndroidManifest.xml`
  - 文本模式的，有 `apk` 核心的配置和参数

app可调试

TODO：

- 【已解决】安卓逆向：如何让YouTube的apk可以被调试
- 【已解决】安卓让apk可调试：修改全局系统属性ro.debuggable
- 【已解决】安卓逆向：用MagiskHide Props Config实现全局apk可调试
- 【未解决】安卓逆向：让apk可调试之通过XPosed插件
- 【未解决】尝试用BDOpener修改ro.debuggable使得apk可调试
- 【已解决】用Magisk插件MagiskHide Props Config去设置ro.debuggable实现全局app可调试
- 【已解决】Google Pixel3安卓手机中MagiskHide Props Config中没有ro.debuggable属性可设置
- 【未解决】安卓逆向：用mprop修改属性ro.debuggable让apk可调试
- 【未解决】安卓逆向：用rootadb的setpropex修改属性ro.debuggable让apk可调试
- 【未解决】mprop提示报错：inject position not found, may be already patched

---

确保app `可调试` = `debuggable`：

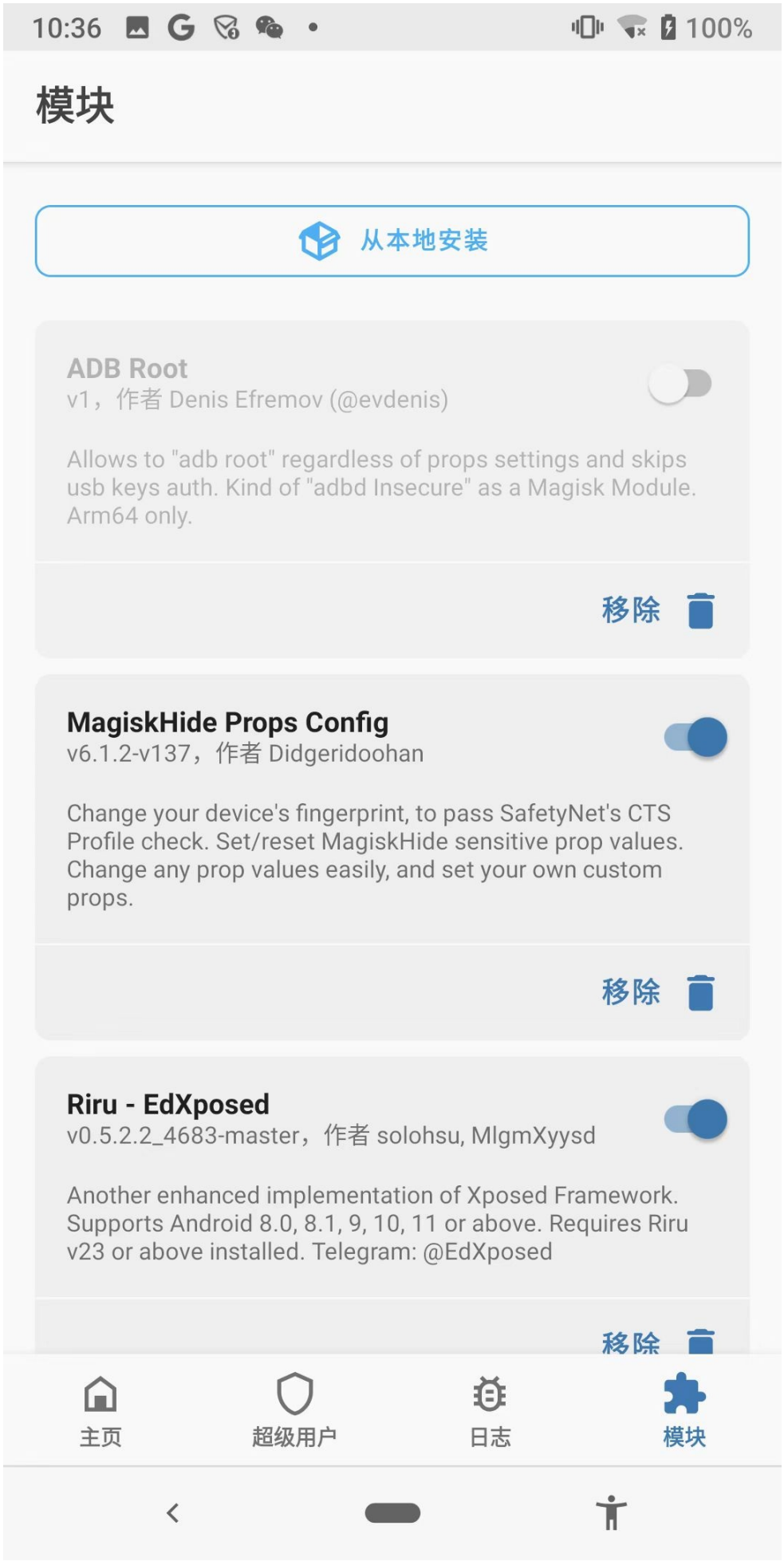
让app可调试，有多种方式：

- 针对 `特定app` 可调试
  - app代码中 `AndroidManifest.xml` 加上 `android:debuggable="true"`
    - 思路：往往是（ `apktool` 等）反编译得到源码，修改后，再重新打包回去
    - 缺点：对于稍微复杂点的apk，往往重新打包的过程中会出错，会很麻烦
- `全局可调`：安卓系统中所有app进程都可调试
  - 实现思路：修改系统全局属性 `ro.debuggable`
  - 具体方法
    - 修改 `boot.img`，重新刷入
      - 说明：比较折腾的一种。不推荐，虽然也可以一劳永逸，但是比较折腾，刷机操作失误还容易变砖
    - `mprop`
      - 已基本失效，放弃
    - `XPosed` 插件
      - `xinstaller`
      - `Xdebuggable`
      - `BuildProp Enhancer`
      - `XDebug`
    - `Magisk`
      - `Magisk`
        - 命令行： `magisk resetprop ro.debuggable 1`
        - 缺点：重启后失效
      - `Magisk` 插件
        - `MagiskHide Props Config`
          - 用 `props` 去修改 `ro.debuggable=1`

此处选择，相对方便操作和效果更好的：

MagiskHide Props Config

- Magisk的插件
  - MagiskHide Props Config
    - 下载
      - https://github.com/Magisk-Modules-Repo/MagiskHidePropsConf/releases
        - https://github.com/Magisk-Modules-Repo/MagiskHidePropsConf/releases/download/v6.1.2/MagiskHidePropsConf-v6.1.2.zip
    - 安装并开启后
      -


10:36
100%
模块
从本地安装
ADB Root
v1，作者 Denis Efremov (@evdenis)
Allows to "adb root" regardless of props settings and skips usb keys auth. Kind of "adbd Insecure" as a Magisk Module. Arm64 only.
移除
MagiskHide Props Config
v6.1.2-v137，作者 Didgeridoohan
Change your device's fingerprint, to pass SafetyNet's CTS Profile check. Set/reset MagiskHide sensitive prop values. Change any prop values easily, and set your own custom props.
移除
Riru - EdXposed
v0.5.2.2_4683-master，作者 solohsu, MlgmXyysd
Another enhanced implementation of Xposed Framework. Supports Android 8.0, 8.1, 9, 10, 11 or above. Requires Riru v23 or above installed. Telegram: @EdXposed
移除
主页
超级用户
日志
模块

安装后，去安卓设备端的命令行（`adb shell` 进去）运行：

```
props
```

根据提示，去（先新增再）修改为：`ro.debuggable=1`

核心的选择是：

- `5` - Add/edit custom props
  - `n` - New custom prop
    - `ro.debuggable`
      - `y` - Yes
        - `1`
          - `y`

最后查看属性，确保修改成功：

```
> adb shell getprop ro.debuggable
1
```

AndroidManifest.xml加debuggable属性

顺带介绍另外一种，虽然不推荐，但是大家常提到的方式：

- app代码中 `AndroidManifest.xml` 加上 `android:debuggable="true"`

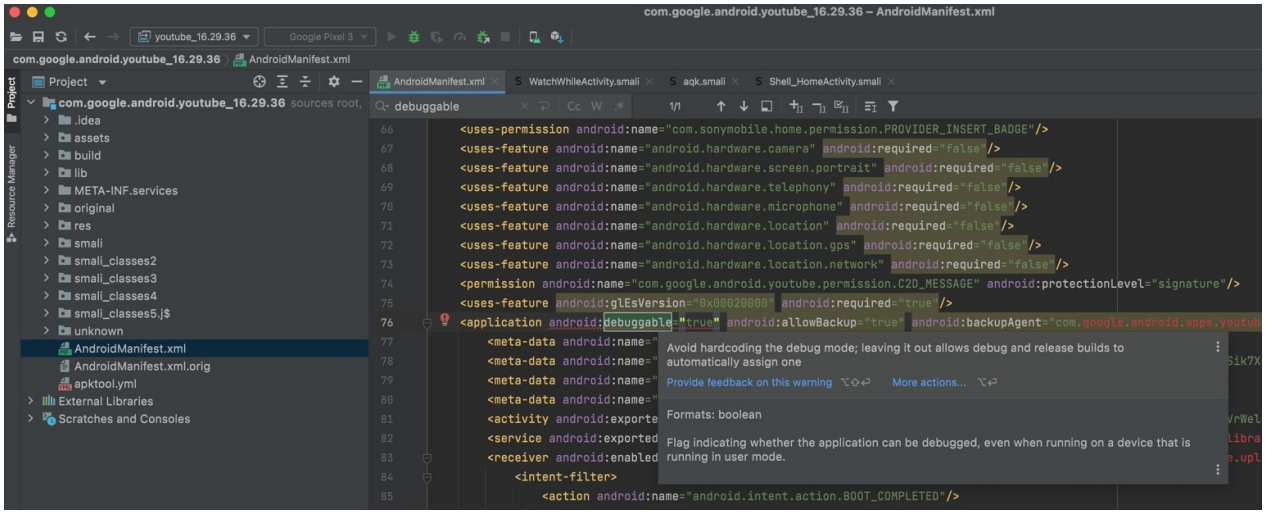
思路：

把apktool反编译后的代码中的

`AndroidManifest.xml`

去修改，加上：

```
android:debuggable "true"
```



然后再用apktool重新打包出apk（有失败的风险）

安装到安卓手机中，成为可调试的app

调试方式启动app

以调试方式启动app：

- 目的：这样启动的app，才可以被调试，方便被调试

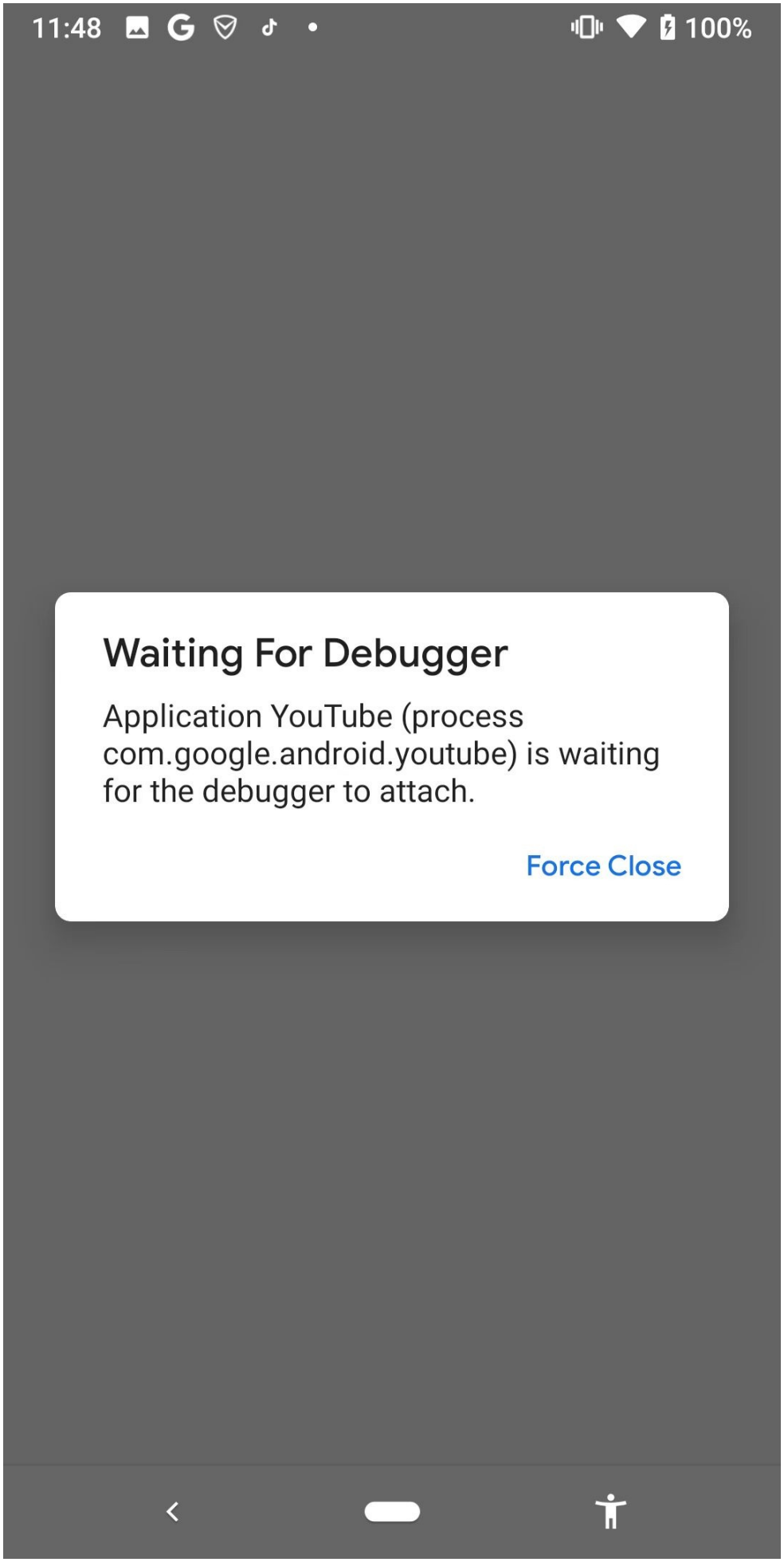
此处以调试方式启动 `YouTube` 的app：

```
adb shell am start -D -n com.google.android.youtube/com.google.android.apps.youtube.app.application.Shell_HomeActivity
```

说明：

- `-D` ：表示 `debug` 模式
- `com.google.android.youtube/com.google.android.apps.youtube.app.application.Shell_HomeActivity`
  - `com.google.android.youtube`
    - app包名=package
  - `com.google.android.apps.youtube.app.application.Shell_HomeActivity`
    - app的主页面=MainActivity

以调试模式启动后的效果：


11:48
100%
Waiting For Debugger
Application YouTube (process com.google.android.youtube) is waiting for the debugger to attach.
Force Close

启动后，app没有立刻正常运行，而是显示 `Waiting For Debugger`

并且：此界面不会消失，直到对应的debugger调试器连接上，开始调试，此界面才消失，才继续开始运行app

说明：

如何获取app的包名

`Youtube` 包名： `com.google.android.youtube`

- 方式1： `pm`

举例：

```
~ adb shell pm list packages -f | grep youtube
package:/data/app/com.google.android.youtube-9Nw_99XIz2jZh7Lyor2SKQ==/base.apk com.goog
le.android.youtube
```

- 方式2： `aapt`

```
 aapt dump badging com.google.android.youtube_16.29.36.apk | grep package
package: name='com.google.android.youtube' versionCode='1522263488' versionName='16.29.
36' compileSdkVersion='31' compileSdkVersionCodename='12'
```

如何获取app的MainActivity

app的首页的 `activity` ，一般被叫做 `MainActivity`

一般情况是： `apktool` 逆向导出的 `xml` 格式的 `AndroidManifest.xml` 中，找到 `android.intent.action.MAIN` 所属于的 `activity` ，就是 `MainActivity`

-》此处YouTube的情况稍微特殊点：

`AndroidManifest.xml`

```
        <activity         exported="true"         name="com.google.android.apps.youtube
.app.application.Shell_HomeActivity"         theme="@style/Theme.YouTube.Launcher"/>
        <activity-alias         exported="true"         name="com.google.android.youtub
e.HomeActivity"         targetActivity="com.google.android.apps.youtube.app.application
.Shell_HomeActivity"/>
        <activity-alias         exported="true"         name="com.google.android.youtub
e.app.application.Shell$HomeActivity"         targetActivity="com.google.android.apps.y
outube.app.application.Shell_HomeActivity"/>
        <activity-alias         exported="true"         name="com.google.android.youtub
e.app.honeycomb.Shell$HomeActivity"         targetActivity="com.google.android.apps.you
tube.app.application.Shell_HomeActivity">
            <intent-filter>
                <action         name="android.intent.action.MAIN"/>
                <category         name="android.intent.category.DEFAULT"/>
                <category         name="android.intent.category.LAUNCHER"/>
```

```
            </intent-filter>
```

找到：

- `android.intent.action.MAIN`

所属的activity是：

- `com.google.android.youtube.app.honeycomb.Shell$HomeActivity`

其是个别名 `alias` ，对应着 `真正的activity` = `MainActivity` 是：

- `com.google.android.apps.youtube.app.application.Shell_HomeActivity`

TODO：

- 【已解决】获取安卓apk应用的app的主界面activity即MainActivity

AS中导入smali代码

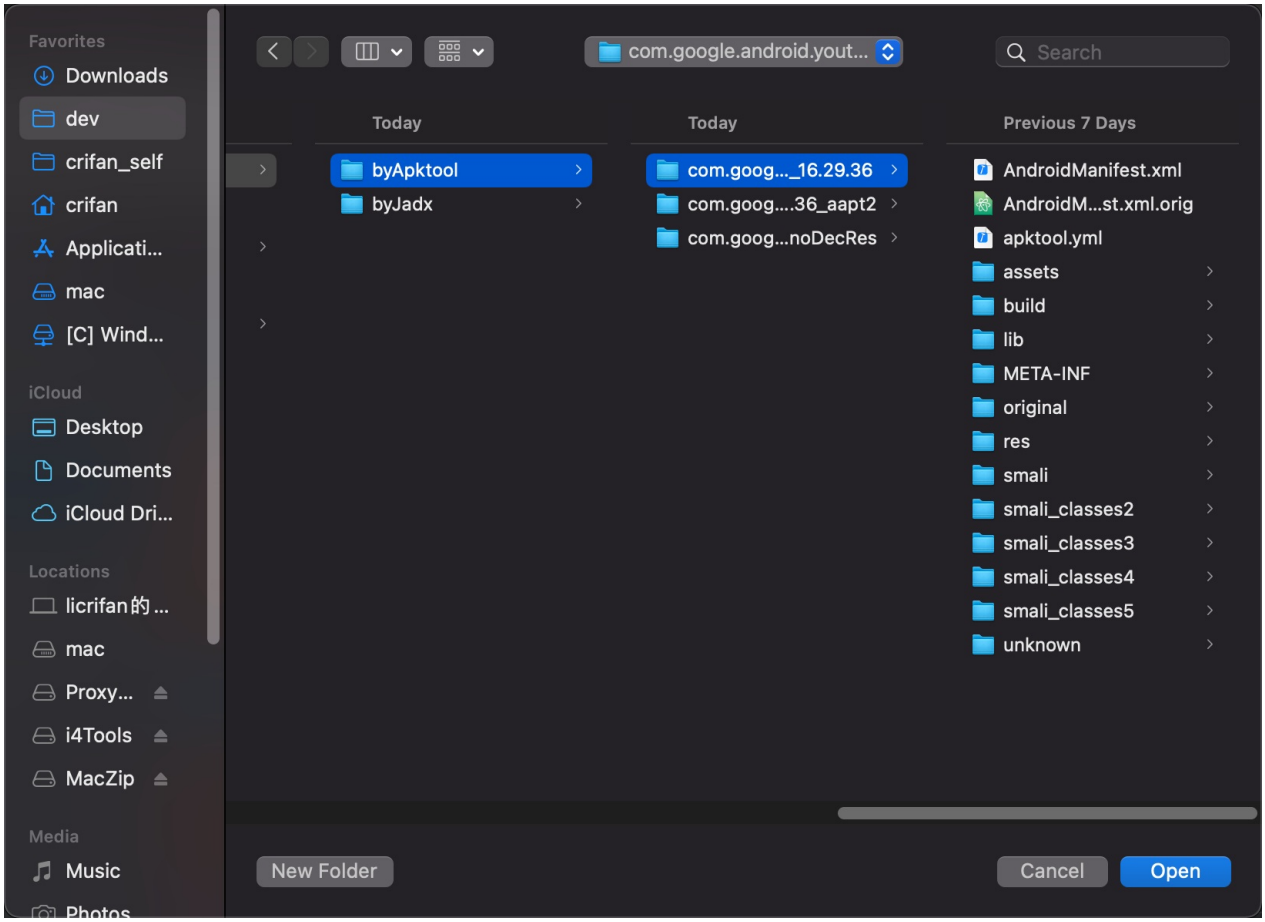
导入带 `smali` 源码的目录到 `Android Studio` 作为新项目：

导入smali的源码：

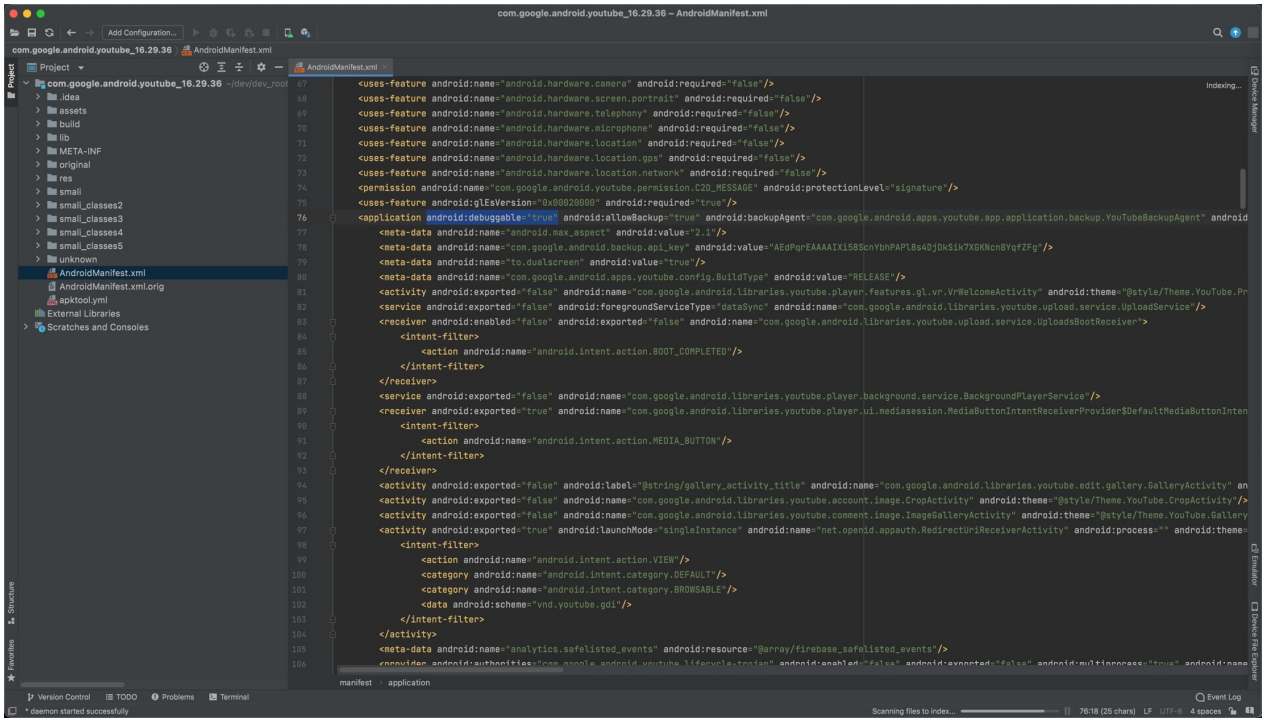
新版 `Android Studio` 的 `Welcome to Android Studio` 欢迎对话框中，点击：

- `Open`

去选择对应的， `Apktool` 反编译后的输出的目录：

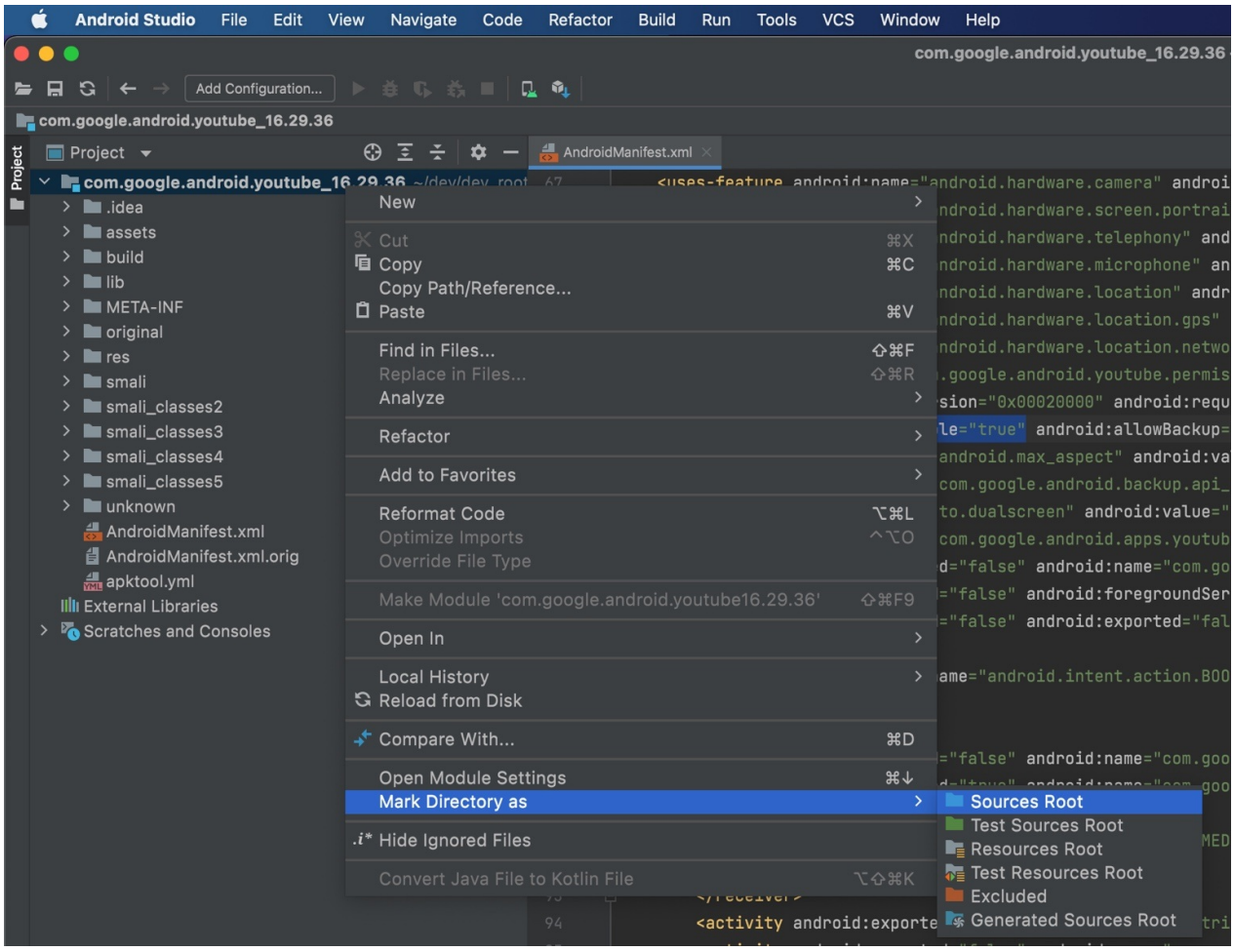


导入后，即可：



然后把根目录设置为**源代码根目录**：

`Mark Directory as Source Root`



注：其实不需要像别人说的：

- 一定要：

    - 只导入smali代码到项目中
    - 只能把smali代码所在目录去mark as source root

而是：

- 只要当前项目中包含了smali代码

即可。

TODO：

- 【已解决】安卓AS调试apk的smali：导入apktool反编译的源码作为项目代码

给smali加断点

给Smali代码加断点：

- 先(重点)是：找到要加断点的地方
- 再去加断点

如何找到要加断点的位置?

要在哪里加断点?

才能实现，app运行时触发到断点而停下来，供自己调试

一般逻辑是：

- 找到最有可能运行到的代码的逻辑对应的地方
  - 入口的 `MainActivity`
    - 前面的：如何获取app的 `MainActivity` ，已经解释过
      - 此处 `YouTube` 就是： `com.google.android.apps.youtube.app.application.Shell_HomeActivity`
  - 或者是你调试时的看到的**顶层页面**

获取顶层页面的activity

```
adb shell dumpsys activity top | grep --color=always ACTIVITY
...
  ACTIVITY com.google.android.youtube/com.google.android.apps.youtube.app.watchwhile.WatchWhileActivity 781cc07 pid=20720
```

-》

- 此处 `YouTube` 的顶层页面是：
  - `com.google.android.apps.youtube.app.watchwhile.WatchWhileActivity`

然后就可以去，此处 `Apktool` 反编译后的， `smali` 的源码所在位置了：

- `com.google.android.youtube_16.29.36`
  - `smali_classes2/com/google/android/apps/youtube/app/application/Shell_HomeActivity.smali`
  - `smali_classes2/com/google/android/apps/youtube/app/watchwhile/WatchWhileActivity.smali`

找到了smali文件位置

给哪些函数打断点?

再说说：具体给哪些函数打断点

-》代码运行才能，才容易触发到断点停下来（我们才好调试）

这部分涉及到安卓的正向开发知识

概述是：

- `onResume`
- `onStart`
- `getLifecycle`
- 等等

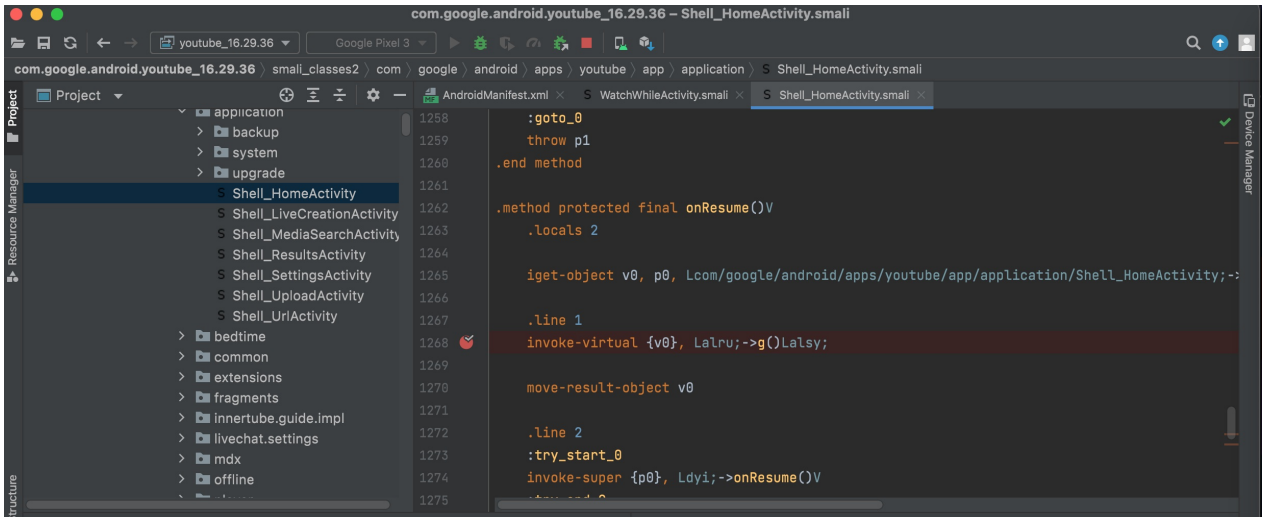
如此，去找：

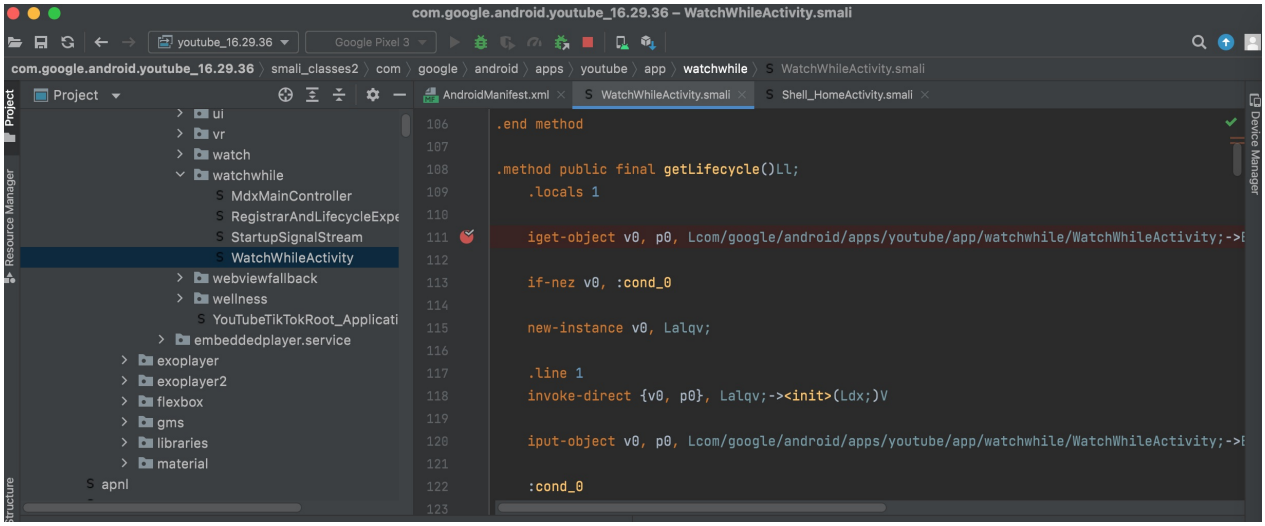
- `com.google.android.youtube_16.29.36`
  - `smali_classes2/com/google/android/apps/youtube/app/application/Shell_HomeActivity.smali`
  - `smali_classes2/com/google/android/apps/youtube/app/watchwhile/WatchWhileActivity.smali`

的

- `onResume`
- `onStart`
- `getLifecycle`

等函数，去打断点：





TODO：

【已解决】Android Studio调试Smali：给YouTube的smali代码加断点

配置AS项目

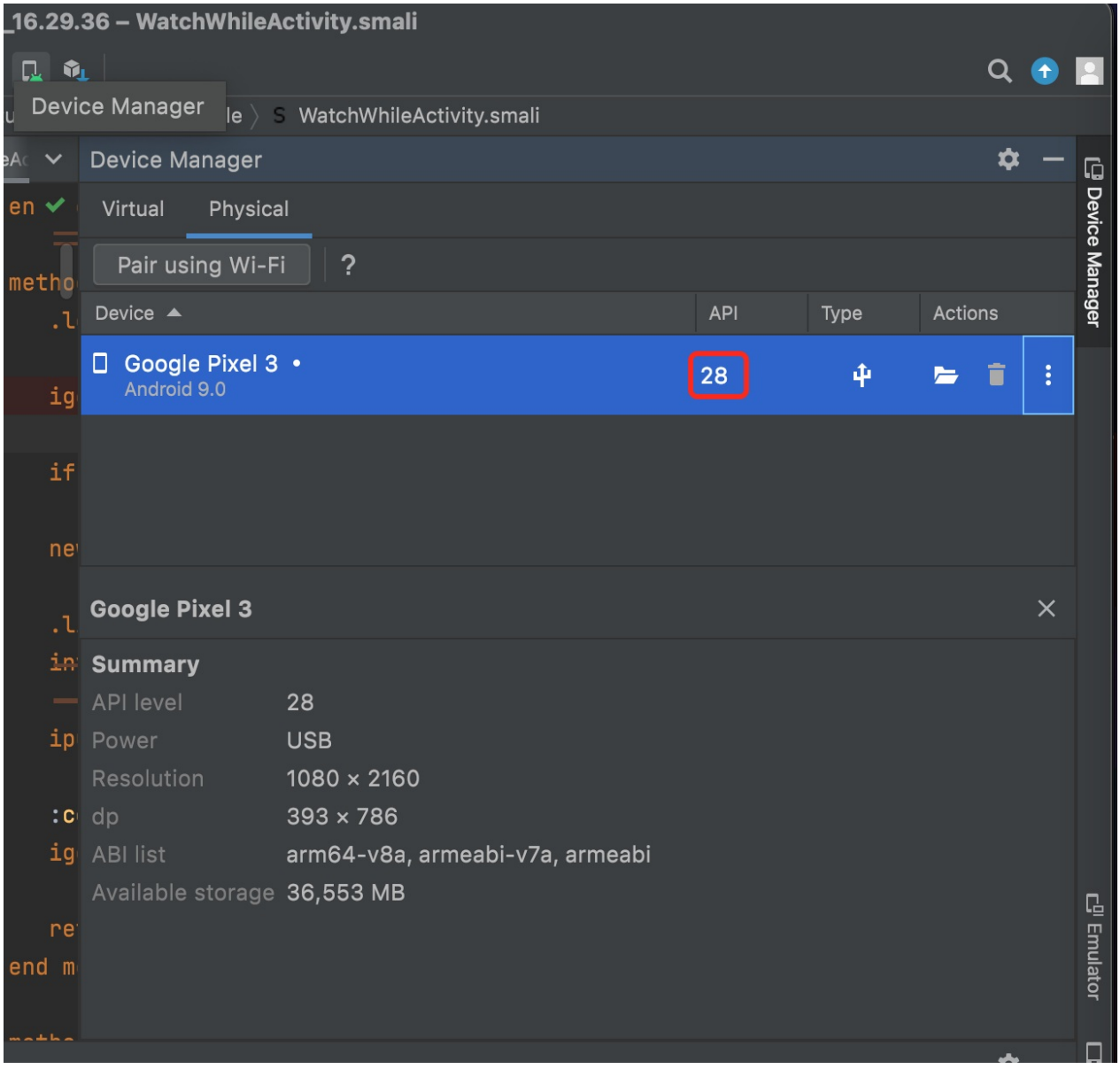
Android Studio项目初始化配置

主要是：

`File` -> `Project Structure` -> `Project Settings` -> `Project SDK`：

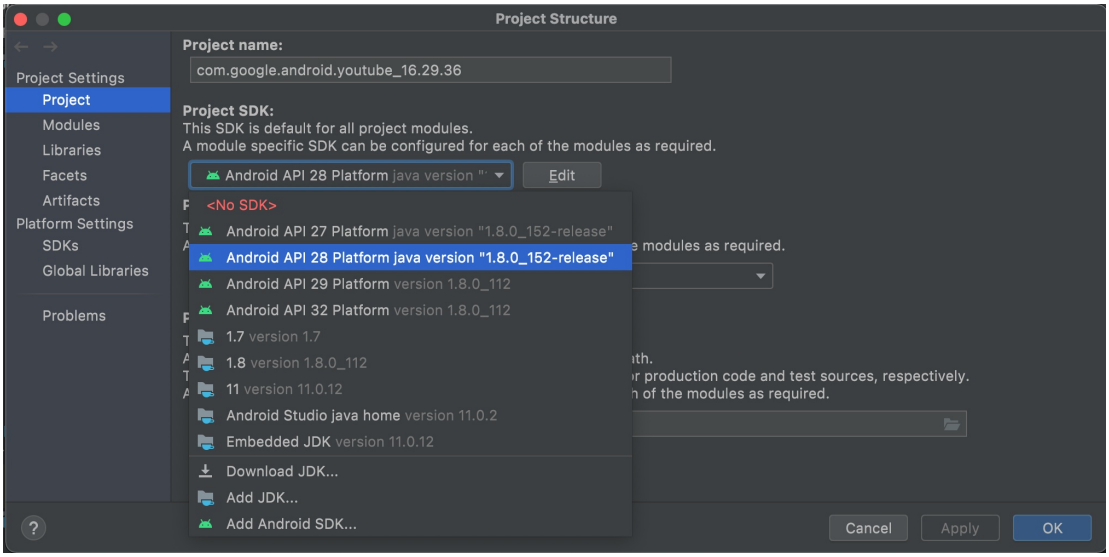
设置为和安卓设备的 `Android API Level` = `sdkVersion` 一致的值：

此处：Android设备是 `Google Pixe 3`，API是 `Android 9` = `Android API 28`



所以设置为：

- `Android API 28 Platform`

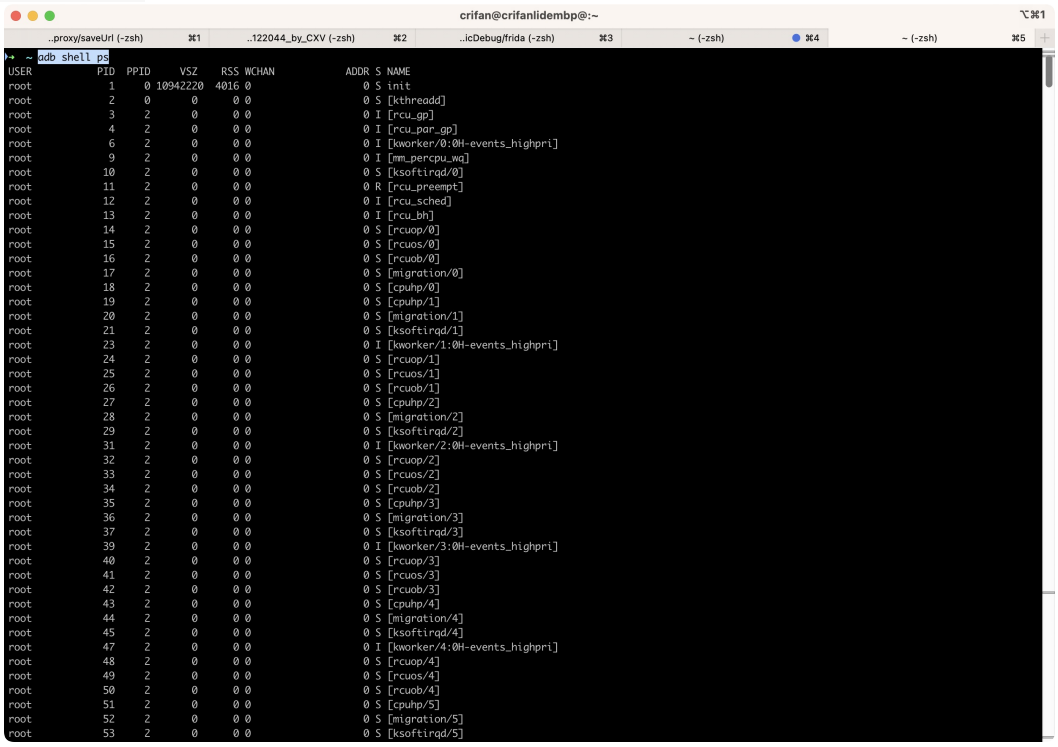


TODO：

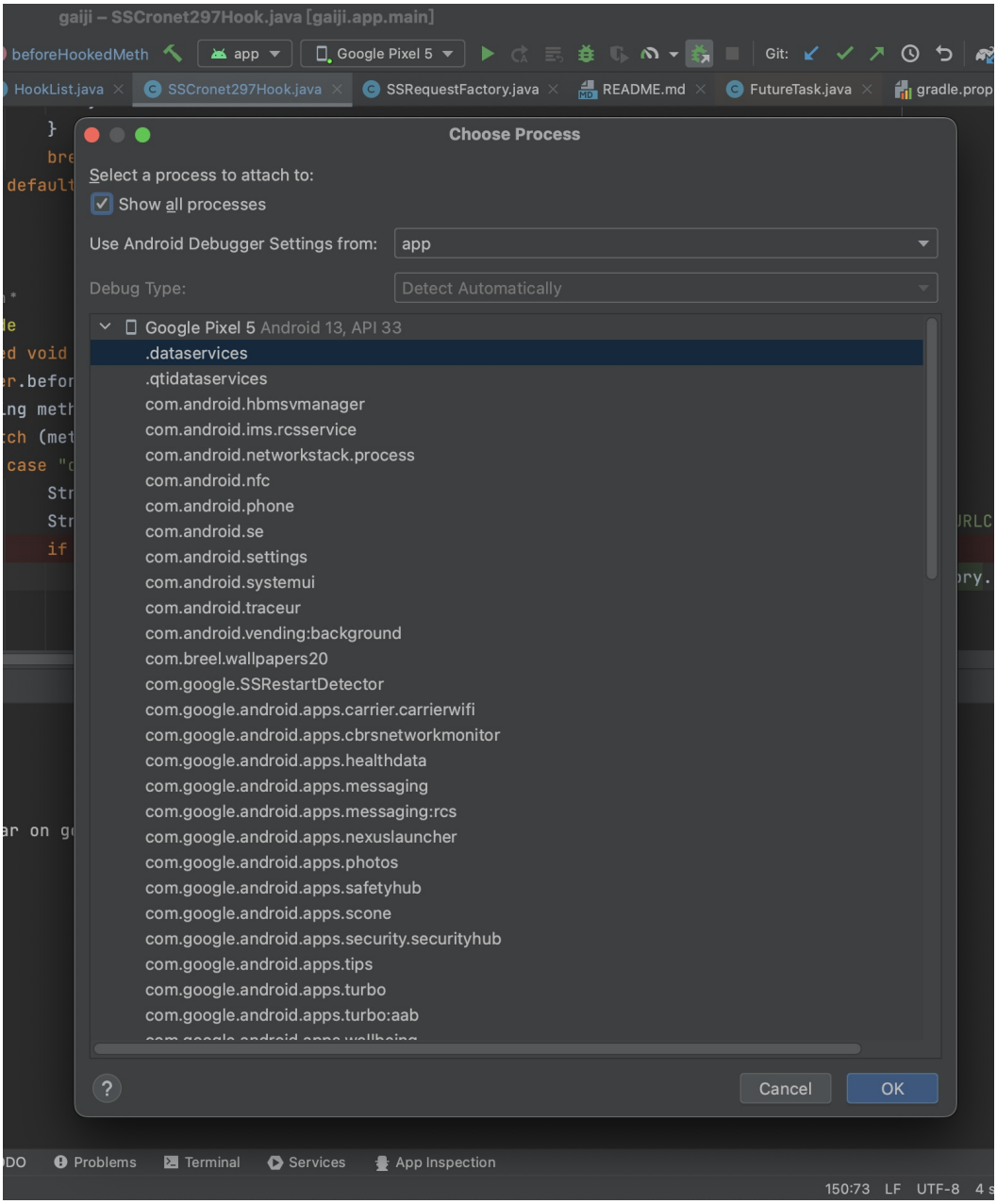
- 【基本解决】安卓AS调试apk的smali：新建和设置远程调试配置
- 【已解决】安卓AS调试apk的smali：初始化配置AS调试环境

可获取全部进程列表

此处要确保：

- 可以查看到全部进程列表
  - adb shell中
    - `adb shell ps` 能输出全部进程列表
      - 

  - `Android Studio` 中
    - `Attach Debugger to Android Process` 的 `Choose Process` 中，（勾选了 `Show all processes` 后）

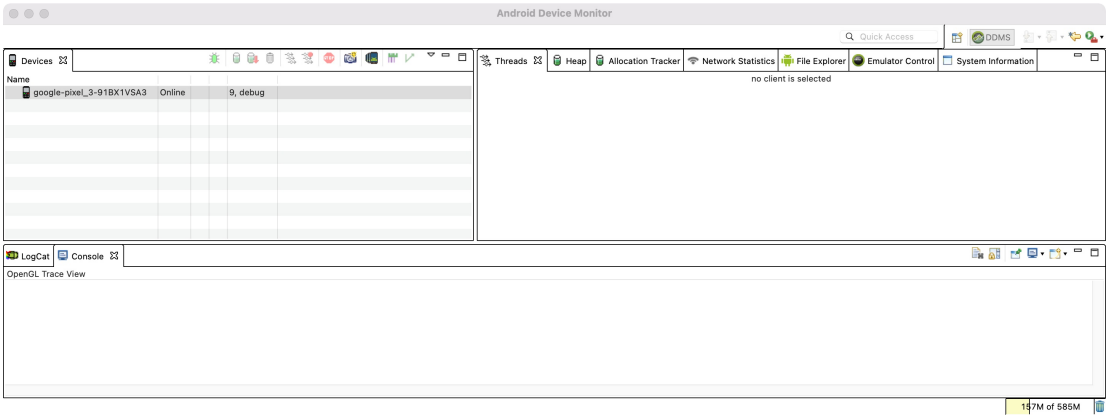


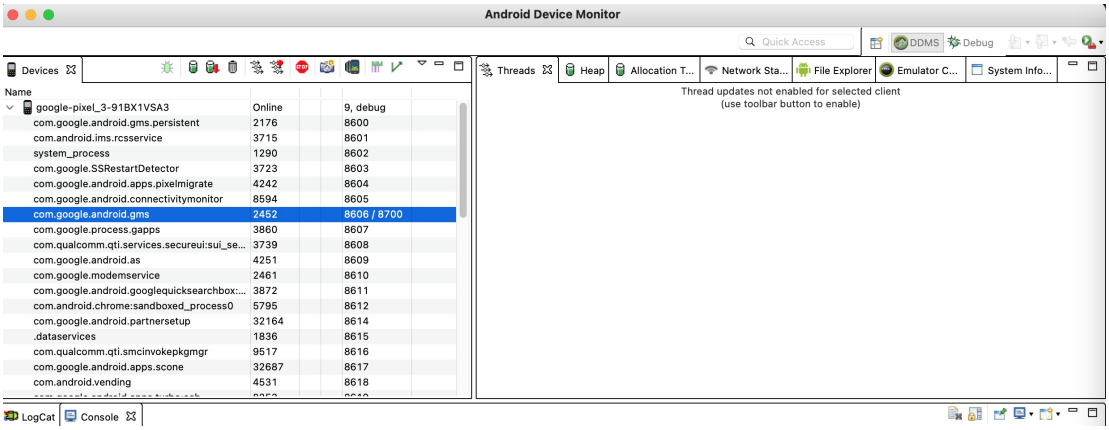
否则如果不满足上述条件，则后续无法顺利调试。

之前遇到的各种情况

此处记录和整理，之前遇到的各种情况：

- adb没有root权限
  - 现象：`adb shell` 的子命令，包括 `ps`，无法直接运行（要么报错，要么没权限，要么没返回结果）
    - 相应的，`adb shell ps`，也无法列出全部进程的列表
  - 解决办法：
    - 是Magisk的插件 `ADB Root` 的问题，关闭 `ADB Root`，就解决问题了。
- 没有开启app可调试
  - 现象：`adb shell getprop ro.debuggable` 输出 `0`
  - 解决办法：

        - 参考：app可调试，用Magisk的插件 `MagiskHide Props Config` ，去新增设置 `ro.debuggable = 1`
    - 效果：开启了app可调试权限：
        - `adb shell getprop ro.debuggable` 输出 `1`
- `Android Device Monitor` (注：已废弃 `DDMS`)，中看不到进程列表
    - 现象
        - 

    - 原因：adb没有权限
    - 解决办法：
        - 用Magisk给adb授予root权限
    - 效果
        - 

AS调试app进程

TODO：

- 查看参数变量值
  - 【已解决】Android Studio调试Smali代码：如何查看函数的局部变量临时变量的值
  - 【已解决】Android Studio调试Smali代码：如何查看函数的全部参数的值
  - 【已解决】Android 11的Google Pixel3中AS调试YouTube的Smali代码
  - 【已解决】Android Studio调试smali代码：查看变量值出错internal error

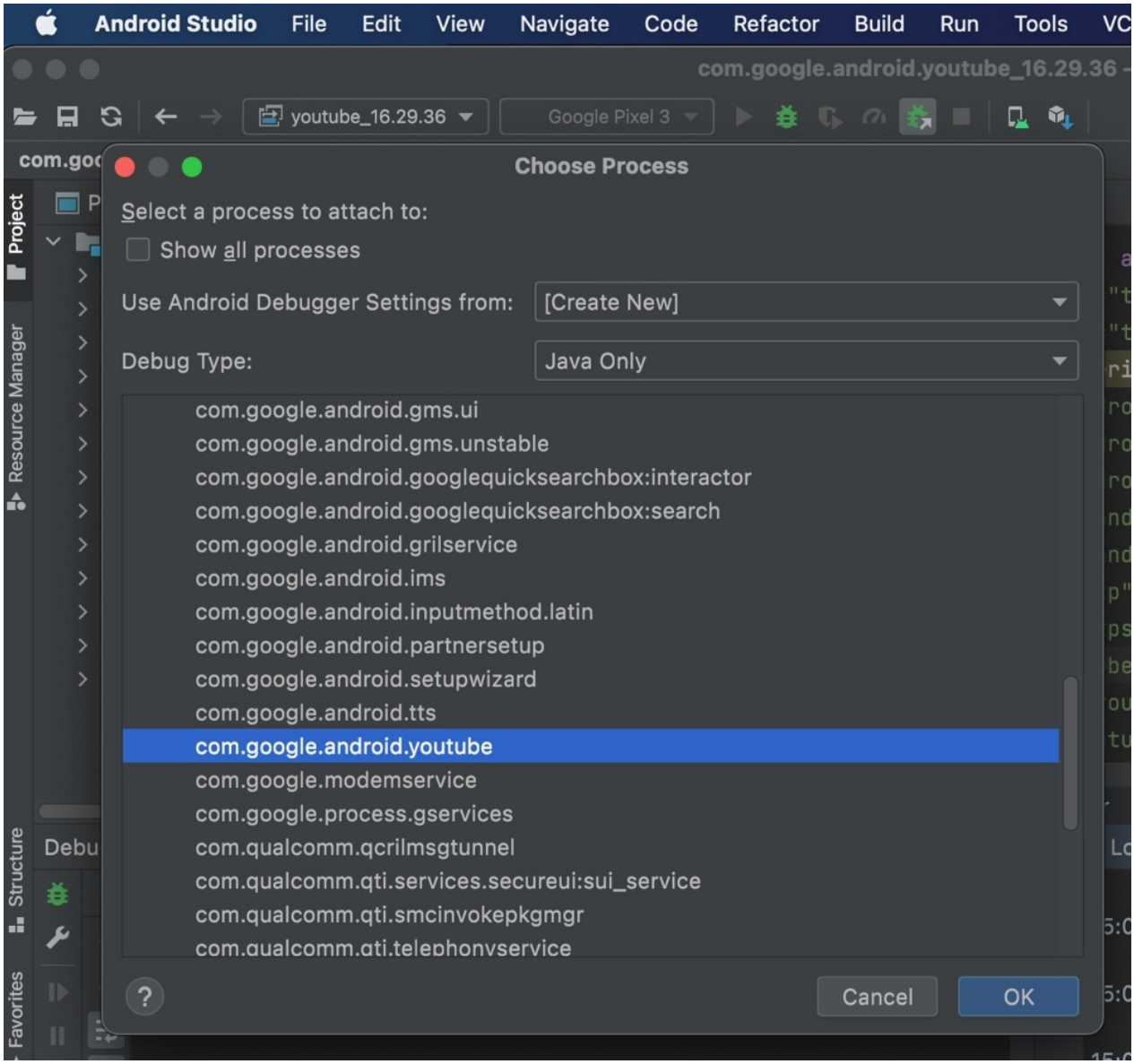
Android Studio中调试设备端的app进程

- `Attach Debugger to Android Process`
  -

进入`Choose Process`弹框页面

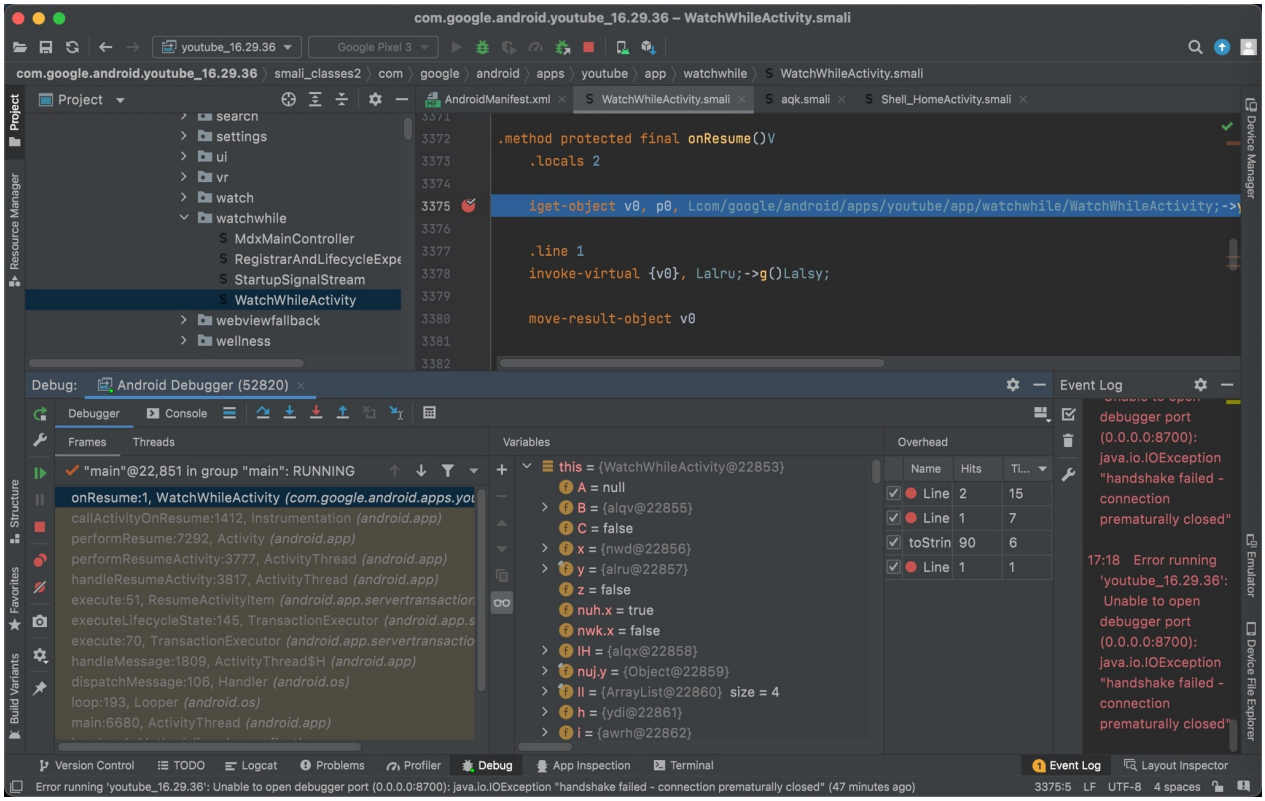
正常会显示出安卓设备，且会列出设备中可调试的众多进程

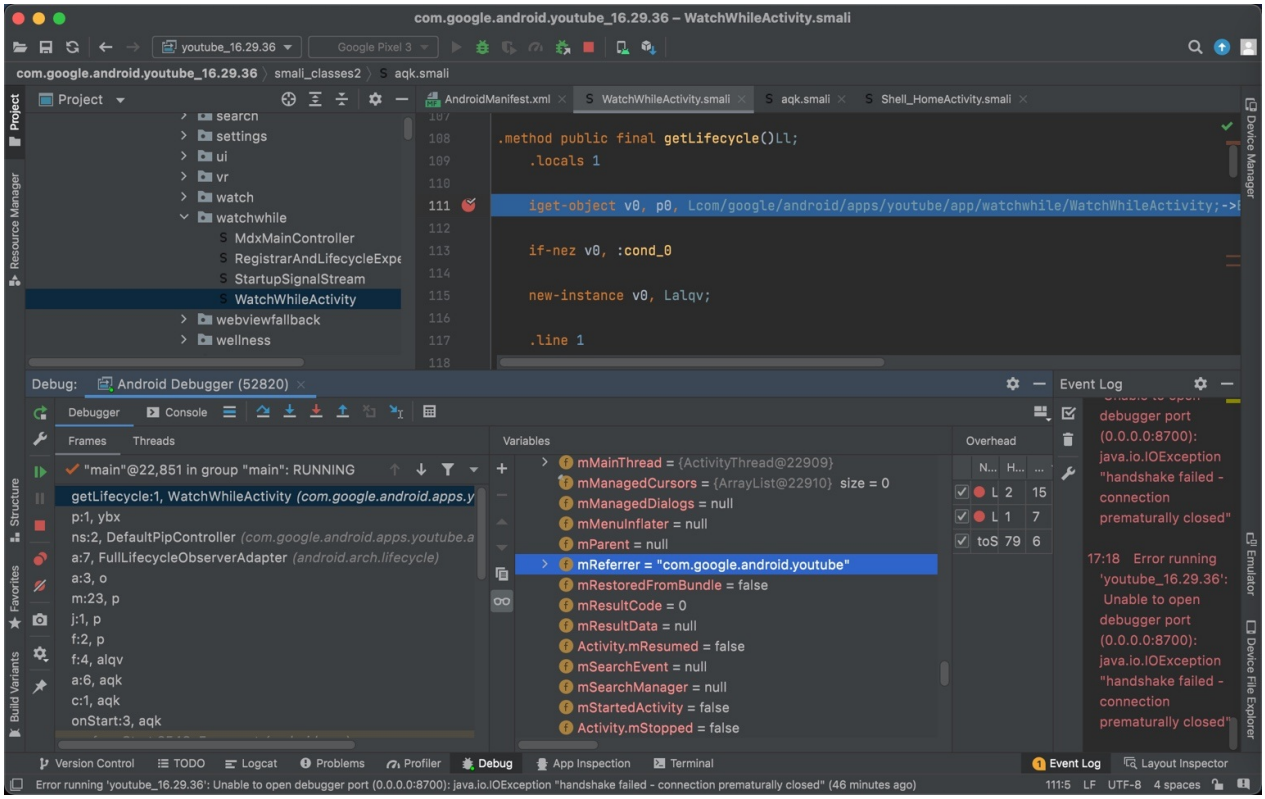
选择对应的要调试（此处是`YouTube`）的进程：



即可顺利启动调试

并触发之前加的断点了：





如果没启动或断点没生效，则重新点击调试

有时候，至少此处经常发生：点击了一次 `Attach Debugger to Android Process` + `OK`，虽然启动了YouTube，但是无法调试进程

所以经常需要再去重新点击一次 `Attach Debugger to Android Process` + `OK`，然后就可以正常调试，触发断点了

但是其实感觉是：没有真正挂上安卓手机中YouTube的进程，因为此时YouTube的app端还在正常运行

感觉是此处调试环境还是有点问题的，有空再去深究原因。

TODO：

- 【基本解决】安卓AS调试apk的smali：新建和设置远程调试配置
- 【已解决】安卓AS调试apk的smali：初始化配置AS调试环境
- 【未解决】用Android Studio调试YouTube的smali代码：request请求发送相关的位置
- 【未解决】用root的安卓手机OPPO R11s去配合Android Studio调试YouTube的Smali代码
- 【已解决】安卓YouTube逆向：搭建安卓apk动态调试环境

调试Smali实例

此处介绍安卓AndroidStudio去调试Smali代码的实例。

调试安卓Youtube的smali

此处贴出，`Android Studio` 动态调试 `YouTube` 的 `Smali` 的完整的项目代码：

crifan/AndroidYouTubeDynamicDebug: 安卓逆向动态调试YouTube (github.com)

供参考。

调试Smali心得

AndroidStudio调试Smali代码

TODO：

- smali断点不生效
  - 【未解决】再次出现AS调试Google Pixel3中的YouTube的问题：Smali断点不生效
  - 【记录】Android 11的Google Pixel3中确认adb shell是否工作正常
  - 【未解决】尝试解决Android Studio中smali断点不生效：调试相关设置
  - 【未解决】尝试解决Android Studio中smali断点不生效：smali文件类型File type
  - 【未解决】尝试解决Android Studio中smali断点不生效：卸载重装smalidea插件
  - 【未解决】尝试解决Android Studio中smali断点不生效：故意打开ADM的DDMS有冲突多试试
  - 【未解决】尝试解决Android Studio中smali断点不生效：Android Studio中adb相关设置
  - 【未解决】尝试解决Android Studio中smali断点不生效：用DDMS和monitor配合试试
  - 【未解决】尝试解决Android Studio中smali断点不生效：USB数据线和端口相关
  - 【未解决】Android Studio调试Smali：通过Remote JVM Debug的attach to remote VM的调试按钮去调试
  - 【已解决】Android Device Monitor的DDMS中看不到app包名进程的名称都是问号
  - 【未解决】尝试解决Android Studio中smali断点不生效：JDWP进程相关
  - 【未解决】尝试解决Android Studio中smali断点不生效：Smali插件相关

安卓逆向期间，折腾Android Studio去调试smali代码，其实更麻烦的不在于搞懂本身的流程，而在于：

找到一个好用的调试设备：已root好的，可以顺利调试的安卓手机

因为期间遇到Google Pixel 3的adb异常，导致adb shell各种命令无法正常运行，包括adb的ps无法正常获取进程列表

从而导致后续调试时AS中看不到进程，折腾了很长时间，才确认，就是adb方面的问题导致的。

解决了该问题了，AS中能attach到进程，后续就顺利多了。

并且另外Google Pixel 3本身不稳定，导致虽然开始能调试，但是后来出现开发者选项崩溃的问题，无法进入设置了。对于正常安卓逆向开发，也有很大影响。

总之：还是要找个靠谱的root后的安卓手机，才能保证后续安卓逆向的顺利。

如何调试Smali代码逻辑

TODO：

- 【记录】用Android Studio调试YouTube的smali代码：smali/anwu.smali
- 【记录】用Android Studio调试YouTube的smali代码：smali_classes2/azfv.smali
- 【记录】用Android Studio调试YouTube的smali代码：smali/anuh.smali
- 【记录】用Android Studio调试YouTube的smali代码：smali_classes2的WatchWhileActivity.smali
-

- 【记录】用AS调试YouTube的Smali代码：调试相关业务逻辑
- 【未解决】给AS调试YouTube的Smali代码：加url过滤
- 【已解决】Xposed如何hook混淆后的安卓应用中的类名和函数名

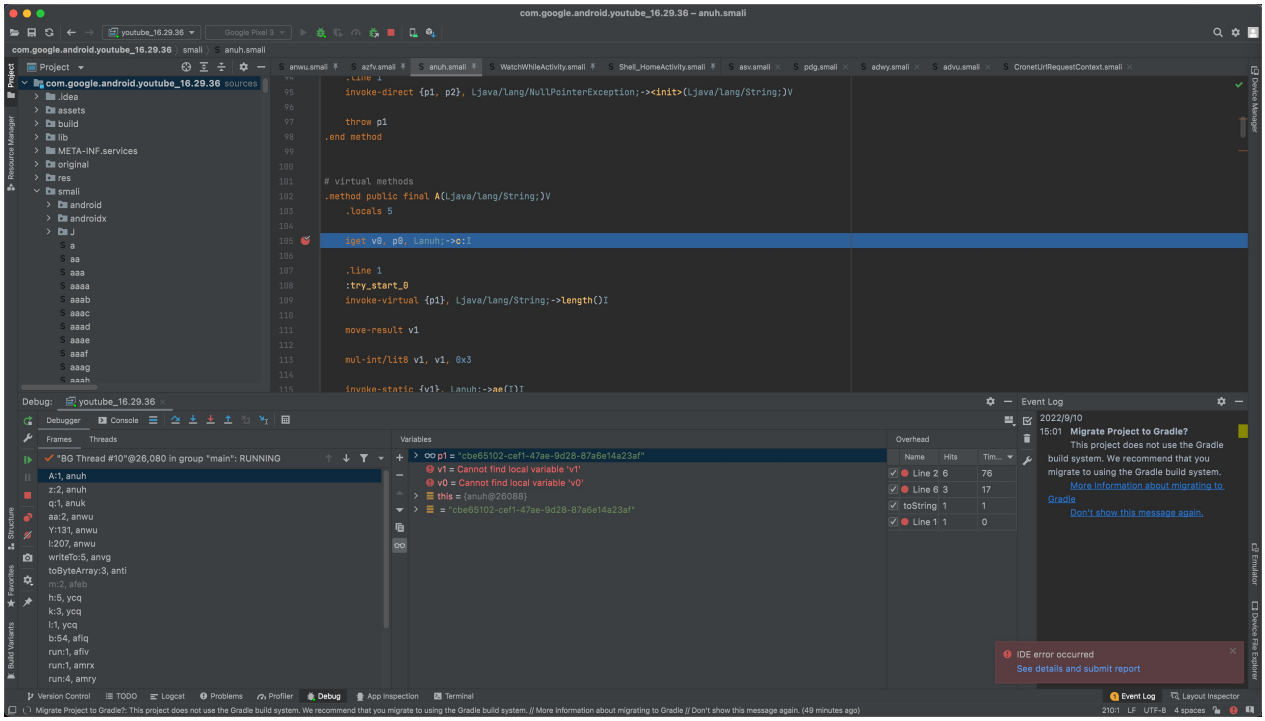
调试Smali常见问题

用AS去调试Smali期间，时不时的遇到一些错误，整理如下：

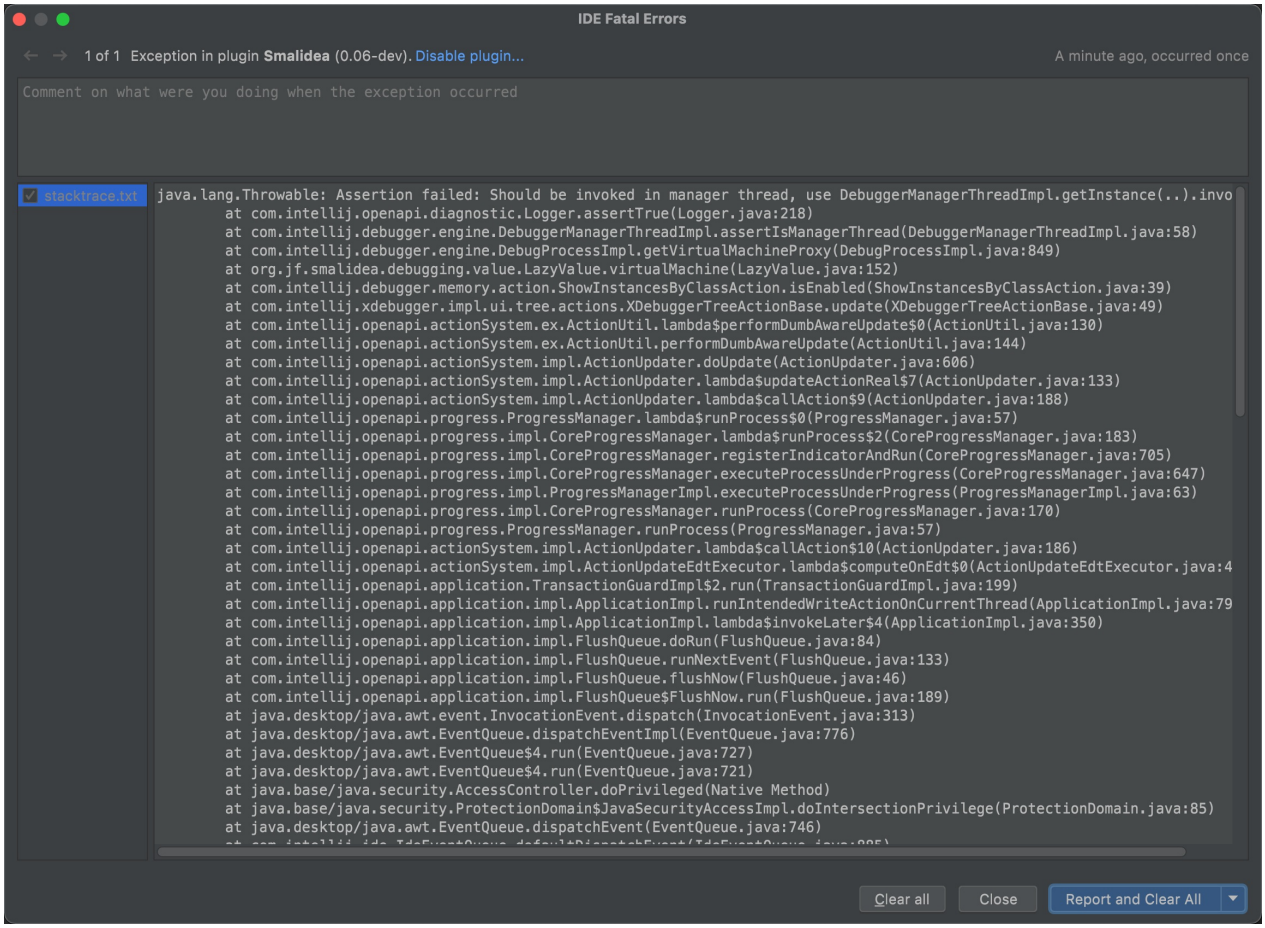
IDE error occurred See details and submit report

- 现象：AS中用Smalidea插件调试smali代码期间，突然的出现报错

```
IDE error occurred
See details and submit report
```



点击 `See details and submit report` ，看到详情：




```
Exception in plugin Smalidea

java.lang.Throwable: Assertion failed: Should be invoked in manager thread, use Debugge
rManagerThreadImpl.getInstance(..).invoke...
    at com.intellij.openapi.diagnostic.Logger.assertTrue(Logger.java:218)
    at com.intellij.debugger.engine.DebuggerManagerThreadImpl.assertIsManagerThread(Deb
uggerManagerThreadImpl.java:58)
    at com.intellij.debugger.engine.DebugProcessImpl.getVirtualMachineProxy(DebugProces
sImpl.java:849)
    at org.jf.smalidea.debugging.value.LazyValue.virtualMachine(LazyValue.java:152)
    at com.intellij.debugger.memory.action.ShowInstancesByClassAction.isEnabled(ShowIns
tancesByClassAction.java:39)
    at com.intellij.xdebugger.impl.ui.tree.actions.XDebuggerTreeActionBase.update(XDebu
ggerTreeActionBase.java:49)
    at com.intellij.openapi.actionSystem.ex.ActionUtil.lambda$performDumbAwareUpdate$0(
ActionUtil.java:130)
    at com.intellij.openapi.actionSystem.ex.ActionUtil.performDumbAwareUpdate(ActionUti
l.java:144)
    at com.intellij.openapi.actionSystem.impl.ActionUpdater.doUpdate(ActionUpdater.java
:606)
    at com.intellij.openapi.actionSystem.impl.ActionUpdater.lambda$updateActionReal$7(A
ctionUpdater.java:133)
    at com.intellij.openapi.actionSystem.impl.ActionUpdater.lambda$callAction$9(ActionU
pdater.java:188)
    at com.intellij.openapi.progress.ProgressManager.lambda$runProcess$0(ProgressManage
r.java:57)
    at com.intellij.openapi.progress.impl.CoreProgressManager.lambda$runProcess$2(CoreP
rogressManager.java:183)
```

```
    at com.intellij.openapi.progress.impl.CoreProgressManager.registerIndicatorAndRun(C
oreProgressManager.java:705)
    at com.intellij.openapi.progress.impl.CoreProgressManager.executeProcessUnderProgre
ss(CoreProgressManager.java:647)
    at com.intellij.openapi.progress.impl.ProgressManagerImpl.executeProcessUnderProgre
ss(ProgressManagerImpl.java:63)
    at com.intellij.openapi.progress.impl.CoreProgressManager.runProcess(CoreProgressMa
nager.java:170)
    at com.intellij.openapi.progress.ProgressManager.runProcess(ProgressManager.java:57)

    at com.intellij.openapi.actionSystem.impl.ActionUpdater.lambda$callAction$10(Action
Updater.java:186)
    at com.intellij.openapi.actionSystem.impl.ActionUpdateEdtExecutor.lambda$computeOnE
dt$0(ActionUpdateEdtExecutor.java:45)
    at com.intellij.openapi.application.TransactionGuardImpl$2.run(TransactionGuardImpl
.java:199)
    at com.intellij.openapi.application.impl.ApplicationImpl.runIntendedWriteActionOnCu
rrentThread(ApplicationImpl.java:794)
    at com.intellij.openapi.application.impl.ApplicationImpl.lambda$invokeLater$4(Appli
cationImpl.java:350)
    at com.intellij.openapi.application.impl.FlushQueue.doRun(FlushQueue.java:84)
    at com.intellij.openapi.application.impl.FlushQueue.runNextEvent(FlushQueue.java:133
)
    at com.intellij.openapi.application.impl.FlushQueue.flushNow(FlushQueue.java:46)
    at com.intellij.openapi.application.impl.FlushQueue$FlushNow.run(FlushQueue.java:189
)
    at java.desktop/java.awt.event.InvocationEvent.dispatch(InvocationEvent.java:313)
    at java.desktop/java.awt.EventQueue.dispatchEventImpl(EventQueue.java:776)
    at java.desktop/java.awt.EventQueue$4.run(EventQueue.java:727)
    at java.desktop/java.awt.EventQueue$4.run(EventQueue.java:721)
    at java.base/java.security.AccessController.doPrivileged(Native Method)
    at java.base/java.security.ProtectionDomain$JavaSecurityAccessImpl.doIntersectionPr
ivilege(ProtectionDomain.java:85)
    at java.desktop/java.awt.EventQueue.dispatchEvent(EventQueue.java:746)
    at com.intellij.ide.IdeEventQueue.defaultDispatchEvent(IdeEventQueue.java:885)
    at com.intellij.ide.IdeEventQueue._dispatchEvent(IdeEventQueue.java:754)
    at com.intellij.ide.IdeEventQueue.lambda$dispatchEvent$6(IdeEventQueue.java:441)
    at com.intellij.openapi.progress.impl.CoreProgressManager.computePrioritized(CorePr
ogressManager.java:825)
    at com.intellij.ide.IdeEventQueue.lambda$dispatchEvent$7(IdeEventQueue.java:440)
    at com.intellij.openapi.application.impl.ApplicationImpl.runIntendedWriteActionOnCu
rrentThread(ApplicationImpl.java:794)
    at com.intellij.ide.IdeEventQueue.dispatchEvent(IdeEventQueue.java:486)
    at com.intellij.openapi.actionSystem.impl.Utils.lambda$expandActionGroupImpl$1(Util
s.java:166)
    at com.intellij.openapi.actionSystem.impl.Utils.runLoopAndWaitForFuture(Utils.java:
530)
    at com.intellij.openapi.actionSystem.impl.Utils.expandActionGroupImpl(Utils.java:159
)
    at com.intellij.openapi.actionSystem.impl.Utils.fillMenu(Utils.java:244)
    at com.intellij.openapi.actionSystem.impl.ActionPopupMenuImpl$MyMenu.lambda$updateC
hildren$1(ActionPopupMenuImpl.java:180)
    at com.intellij.util.TimeoutUtil.run(TimeoutUtil.java:104)
    at com.intellij.openapi.actionSystem.impl.ActionPopupMenuImpl$MyMenu.lambda$updateC
hildren$3(ActionPopupMenuImpl.java:179)
    at com.intellij.openapi.actionSystem.impl.Utils.performWithRetries(Utils.java:570)
```

```
    at com.intellij.openapi.actionSystem.impl.ActionPopupMenuImpl$MyMenu.updateChildren(
ActionPopupMenuImpl.java:178)
    at com.intellij.openapi.actionSystem.impl.ActionPopupMenuImpl$MyMenu.show(ActionPop
upMenuImpl.java:138)
    at com.intellij.ui.PopupHandler$2.invokePopup(PopupHandler.java:130)
    at com.intellij.ui.PopupHandler.mousePressed(PopupHandler.java:48)
    at java.desktop/java.awt.AWTEventMulticaster.mousePressed(AWTEventMulticaster.java:
288)
    at java.desktop/java.awt.AWTEventMulticaster.mousePressed(AWTEventMulticaster.java:
287)
    at java.desktop/java.awt.AWTEventMulticaster.mousePressed(AWTEventMulticaster.java:
287)
    at java.desktop/java.awt.AWTEventMulticaster.mousePressed(AWTEventMulticaster.java:
287)
    at java.desktop/java.awt.AWTEventMulticaster.mousePressed(AWTEventMulticaster.java:
287)
    at java.desktop/java.awt.Component.processMouseEvent(Component.java:6649)
    at java.desktop/javax.swing.JComponent.processMouseEvent(JComponent.java:3345)
    at com.intellij.ui.treeStructure.Tree.processMouseEvent(Tree.java:394)
    at com.intellij.ide.dnd.aware.DnDAwareTree.processMouseEvent(DnDAwareTree.java:44)
    at java.desktop/java.awt.Component.processEvent(Component.java:6417)
    at java.desktop/java.awt.Container.processEvent(Container.java:2263)
    at java.desktop/java.awt.Component.dispatchEventImpl(Component.java:5027)
    at java.desktop/java.awt.Container.dispatchEventImpl(Container.java:2321)
    at java.desktop/java.awt.Component.dispatchEvent(Component.java:4859)
    at java.desktop/java.awt.LightweightDispatcher.retargetMouseEvent(Container.java:49
18)
    at java.desktop/java.awt.LightweightDispatcher.processMouseEvent(Container.java:4544
)
    at java.desktop/java.awt.LightweightDispatcher.dispatchEvent(Container.java:4488)
    at java.desktop/java.awt.Container.dispatchEventImpl(Container.java:2307)
    at java.desktop/java.awt.Window.dispatchEventImpl(Window.java:2784)
    at java.desktop/java.awt.Component.dispatchEvent(Component.java:4859)
    at java.desktop/java.awt.EventQueue.dispatchEventImpl(EventQueue.java:778)
    at java.desktop/java.awt.EventQueue$4.run(EventQueue.java:727)
    at java.desktop/java.awt.EventQueue$4.run(EventQueue.java:721)
    at java.base/java.security.AccessController.doPrivileged(Native Method)
    at java.base/java.security.ProtectionDomain$JavaSecurityAccessImpl.doIntersectionPr
ivilege(ProtectionDomain.java:85)
    at java.base/java.security.ProtectionDomain$JavaSecurityAccessImpl.doIntersectionPr
ivilege(ProtectionDomain.java:95)
    at java.desktop/java.awt.EventQueue$5.run(EventQueue.java:751)
    at java.desktop/java.awt.EventQueue$5.run(EventQueue.java:749)
    at java.base/java.security.AccessController.doPrivileged(Native Method)
    at java.base/java.security.ProtectionDomain$JavaSecurityAccessImpl.doIntersectionPr
ivilege(ProtectionDomain.java:85)
    at java.desktop/java.awt.EventQueue.dispatchEvent(EventQueue.java:748)
    at com.intellij.ide.IdeEventQueue.defaultDispatchEvent(IdeEventQueue.java:885)
    at com.intellij.ide.IdeEventQueue.dispatchMouseEvent(IdeEventQueue.java:814)
    at com.intellij.ide.IdeEventQueue._dispatchEvent(IdeEventQueue.java:751)
    at com.intellij.ide.IdeEventQueue.lambda$dispatchEvent$6(IdeEventQueue.java:441)
    at com.intellij.openapi.progress.impl.CoreProgressManager.computePrioritized(CorePr
ogressManager.java:825)
    at com.intellij.ide.IdeEventQueue.lambda$dispatchEvent$7(IdeEventQueue.java:440)
    at com.intellij.openapi.application.impl.ApplicationImpl.runIntendedWriteActionOnCu
rrentThread(ApplicationImpl.java:794)
```

```
    at com.intellij.ide.IdeEventQueue.dispatchEvent(IdeEventQueue.java:492)
    at java.desktop/java.awt.EventDispatchThread.pumpOneEventForFilters(EventDispatchTh
read.java:203)
    at java.desktop/java.awt.EventDispatchThread.pumpEventsForFilter(EventDispatchThrea
d.java:124)
    at java.desktop/java.awt.EventDispatchThread.pumpEventsForHierarchy(EventDispatchTh
read.java:113)
    at java.desktop/java.awt.EventDispatchThread.pumpEvents(EventDispatchThread.java:109
)
    at java.desktop/java.awt.EventDispatchThread.pumpEvents(EventDispatchThread.java:101
)
    at java.desktop/java.awt.EventDispatchThread.run(EventDispatchThread.java:90)
```

- 原因：Smalidea插件的bug
- 解决办法：暂无

lldb调试安卓

此处介绍如何用LLDB去调试安卓app（进程）。

Mac中：下载安卓版lldb-server

从网上下载lldb-server到Mac

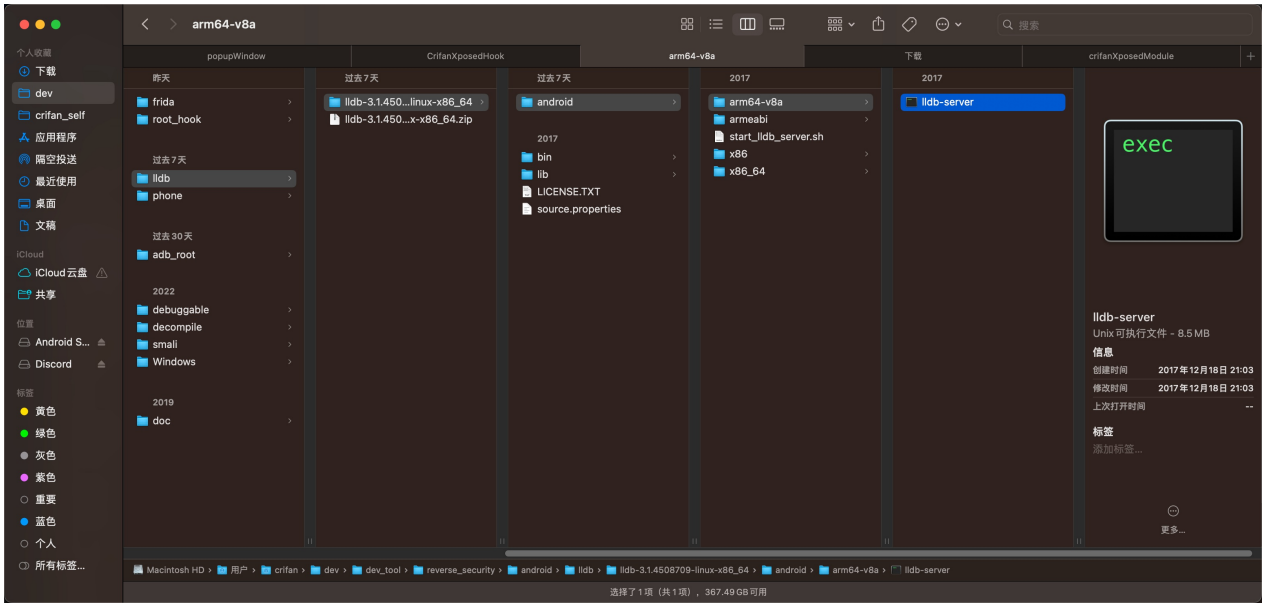
Android SDK Offline: Android NDK LLDB Direct Download

->

https://dl.google.com/android/repository/lldb-3.1.4508709-darwin-x86_64.zip

下载得到 `lldb-3.1.4508709-darwin-x86_64.zip` ，解压后得到：

`lldb-3.1.4508709-linux-x86_64/android/arm64-v8a/lldb-server`



确认文件类型是ARM64的：

```
➜  arm64-v8a ll
total 16568
-rwxr-xr-x@ 1 crifan  staff   8.1M 12 18  2017 lldb-server

➜  arm64-v8a file lldb-server
lldb-server: ELF 64-bit LSB shared object, ARM aarch64, version 1 (SYSV), dynamically l
inked, interpreter /system/bin/linker64, BuildID[sha1]=16479c73b494c432c5f171db2bb68f29
e033f157, stripped
```

Mac中：把lldb-server下载到安卓手机中

从Mac下载lldb-server到此处安卓手机Pixel5中：

```
adb push lldb-3.1.4508709-linux-x86_64/android/arm64-v8a/lldb-server /data/local/tmp
```

注：

- 此处安卓手机正常默认情况下，已有路径：`/data/local/tmp`
  - 专门供开发相关用途使用
- adb shell中可以确认

```
blueline:/data/local/tmp/ # ls -lh
total 4.0M
-rwxrwxrwx 1 shell shell 8.0M 2017-12-18 21:03 lldb-server
```

  - 此处确保有 `可执行权限 = x`
    - 如果没有，则要去加上

```
chmod +x lldb-server
```

安卓手机中：运行lldb-server

```
./lldb-server platform --server --listen unix-abstract:///data/local/tmp/dev/lldb_debug
.sock &
```

注：

- 此处可以通过ps查看到进程的确在运行

  ```
  blueline:/data/local/tmp/dev/lldb # ps -A | grep lldb
  root          27860   7054 10779208   4628 __skb_wait_for_more_packets 0 S lldb-serv
  er
  ```

- 参数含义
  - 概述
    - COMMANDS
      - `v[ersion]`
        - Prints lldb-server version and exits
      - `g[dbserver]`
        - Runs the server using the gdb-remote protocol. LLDB can afterwards connect to the server using gdb-remote command
      - `p[latform]`
        - Runs the platform server. LLDB can afterwards connect to the server using platform select, followed by platform connect
    - PLATFORM COMMAND
      - 语法

        ```
        lldb-server p[latform] [options] -server -listen [[host]:port]
        ```

      - CONNECTION
        - `--server`
          - Run in server mode, handling multiple connections. If this is not specified, lldb-server will accept only one connection and exit when it is finished
        - `--listen <host>:<port>`
          - Hostname and port to listen on. Obligatory. If port is zero, a random port will be used
        - `--socket-file <path>`
          - `Write the listening socket port number to the specified file`
  - 详解
    - lldb-server – Server for LLDB Debugging Sessions — The LLDB Debugger

Mac中：用lldb客户端去连接lldb-server

- 进入=启动=运行 lldb

```
lldb
```

- 设置要连接的类型是：远端的安卓手机

```
platform select remote-android
```

  - 输出举例

```
(lldb) platform select remote-android
  Platform: remote-android
Connected: no
```

- 连接安卓（中的lldb-server）

```
platform connect unix-abstract-connect:///data/local/tmp/dev/lldb_debug.sock
```

  - 输出举例

```
(lldb) platform connect unix-abstract-connect:///data/local/tmp/dev/lldb_debug.
sock
  Platform: remote-android
    Triple: aarch64-unknown-linux-android
OS Version: 30 (4.9.248-gc4689af91bc5-ab7425221)
  Hostname: localhost
Connected: yes
WorkingDir: /data/local/tmp/dev/lldb
    Kernel: #0 SMP PREEMPT Fri Jun 4 06:01:28 UTC 2021
```

注：

- 可以用 `platform list` 查看全部的支持的类型有哪些

```
(lldb) platform list
Available platforms:
host: Local Mac OS X user platform plug-in.
remote-linux: Remote Linux user platform plug-in.
remote-android: Remote Android user platform plug-in.
remote-freebsd: Remote FreeBSD user platform plug-in.
remote-gdb-server: A platform that uses the GDB remote protocol as the communicatio
n transport.
darwin: Darwin platform plug-in.
remote-ios: Remote iOS platform plug-in.
remote-macosx: Remote Mac OS X user platform plug-in.
ios-simulator: iPhone simulator platform plug-in.
tvos-simulator: tvOS simulator platform plug-in.
watchos-simulator: Apple Watch simulator platform plug-in.
darwin-kernel: Darwin Kernel platform plug-in.
remote-tvos: Remote Apple TV platform plug-in.
```

```
remote-watchos: Remote Apple Watch platform plug-in.
remote-bridgeos: Remote BridgeOS platform plug-in.
host: Local Mac OS X user platform plug-in.
remote-netbsd: Remote NetBSD user platform plug-in.
remote-openbsd: Remote OpenBSD user platform plug-in.
qemu-user: Platform for debugging binaries under user mode qemu
remote-windows: Remote Windows user platform plug-in.
```

- 连接前后，都可以去查看和验证实际状态（是否是希望的已连接）

  ```
  platform status
  ```

  - 举例
    - 连接前

      ```
      (lldb) platform status
        Platform: remote-android
      Connected: no
      ```

    - 连接后

      ```
      (lldb) platform status
        Platform: remote-android
          Triple: aarch64-unknown-linux-android
      OS Version: 30 (4.9.248-gc4689af91bc5-ab7425221)
        Hostname: localhost
      Connected: yes
      WorkingDir: /data/local/tmp/dev/lldb
          Kernel: #0 SMP PREEMPT Fri Jun 4 06:01:28 UTC 2021
      ```

Mac中：用lldb调试安卓app进程

- 背景
  - 被测安卓的app
    - app名称：`Lift File Manager`
    - 包名：`com.lift.filemanager.android`
    - 主页面
      - 

然后可以用lldb去调试安卓app（进程）了：

```
process attach -p 24058
```

- 说明
  - `attach`：当前用挂载模式（而不是spawn模式）
  - `-p 24058`
    - `-p` == `--pid`：进程的PID
    - `24058`：当前安卓app的（主）进程的PID

输出举例

- 命令行输出：

```
(lldb) process attach -p 24058
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/8B041FC2-79D5
-1089-00E4-8324BAFA5142/app_process64 No LZMA support found for reading .gnu_debugdata
section
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/1DEC5134-A095
-22F9-C83C-48DAE0AEC3BE/libandroid_runtime.so No LZMA support found for reading .gnu_de
bugdata section
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/52A96623-E462
-0961-84C4-425671CC1C5D/libbinder.so No LZMA support found for reading .gnu_debugdata s
ection
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/ED5D3D46-2F5F
-F1ED-D424-A588996F33C8/libcutils.so No LZMA support found for reading .gnu_debugdata s
ection
...
...
...
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/68482D47-6551
-C4A4-AE65-B2B4FC4E6ABA/libGLESv2_adreno.so No LZMA support found for reading .gnu_debu
gdata section
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/7A027C1B-6689
-FB13-BC4C-DDF60D309D9F/libllvm-glnext.so No LZMA support found for reading .gnu_debugd
ata section
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/28A702E7-CF8C
-5CCC-2481-D2DD8B341E1B/libcompiler_rt.so No LZMA support found for reading .gnu_debugd
ata section
warning: (aarch64) /Users/crifan/.lldb/module_cache/remote-android/.cache/11A028BE-C11F
-BD95-B235-8593B25A1887/libwebviewchromium_loader.so No LZMA support found for reading
.gnu_debugdata section
Process 24058 stopped
* thread #1, name = 'er.android:sist', stop reason = signal SIGSTOP
    frame #0: 0x000000707075bf38 libc.so`__epoll_pwait + 8
libc.so`__epoll_pwait:
->  0x707075bf38 <+8 :  cmn    x0, #0x1, lsl #12         ; =0x1000
    0x707075bf3c <+12 : cneg   x0, x0, hi
    0x707075bf40 <+16 : b.hi   0x707075a820              ; __set_errno_internal
    0x707075bf44 <+20 : ret
  thread #2, name = 'Signal Catcher', stop reason = signal SIGSTOP
    frame #0: 0x000000707075b978 libc.so`__rt_sigtimedwait + 8
libc.so`__rt_sigtimedwait:
->  0x707075b978 <+8 :  cmn    x0, #0x1, lsl #12         ; =0x1000
    0x707075b97c <+12 : cneg   x0, x0, hi
    0x707075b980 <+16 : b.hi   0x707075a820              ; __set_errno_internal
    0x707075b984 <+20 : ret
  thread #3, name = 'perfetto_hprof_', stop reason = signal SIGSTOP
    frame #0: 0x000000707075acf4 libc.so`read + 4
libc.so`read:
->  0x707075acf4 <+4 :  svc    #0
    0x707075acf8 <+8 :  cmn    x0, #0x1, lsl #12         ; =0x1000
    0x707075acfc <+12 : cneg   x0, x0, hi
    0x707075ad00 <+16 : b.hi   0x707075a820              ; __set_errno_internal
...
...
...
```

```
  thread #21, name = 'queued-work-loo', stop reason = signal SIGSTOP
    frame #0: 0x000000707075bf38 libc.so`__epoll_pwait + 8
libc.so`__epoll_pwait:
->  0x707075bf38 <+8> :  cmn    x0, #0x1, lsl #12         ; =0x1000
    0x707075bf3c <+12> : cneg   x0, x0, hi
    0x707075bf40 <+16> : b.hi   0x707075a820              ; __set_errno_internal
    0x707075bf44 <+20> : ret
Target 0: (app_process64) stopped.
Executable module set to "/Users/crifan/.lldb/module_cache/remote-android/.cache/8B041FC2-79D5-1089-00E4-8324BAFA5142/app_process64".
Architecture set to: aarch64-unknown-linux-android.
(lldb)
```

- 截图
  -

-

常见问题

error Connection shut down by remote side while waiting for reply to initial handshake packet

- 现象：lldb去连接安卓中lldb-server时报错：

```
(lldb) platform connect unix-abstract-connect:///data/local/tmp/dev/lldb/lldb_debug.sock
error: Connection shut down by remote side while waiting for reply to initial handshake packet
```

- 原因：此处Android 13已开启了SELinux，导致无法连接
- 解决办法：去关于SELinux
  - 有2种方式
    - 永久关闭：需要修改Android源码，重新编译ROM或boot.img
      - 此处暂时没条件，暂时放弃此路
    - 临时关闭：通过参数设置关闭
      - 具体命令

```
adb shell setenforce 0
```

        - 或：
          - 先 `adb shell` 进入shell，再 `su` 切换成root用户，再用 `setenforce 0` 去关闭 `SELinux`
        - （之前和之后都可以）用 `getenforce` 去确认=查看当前SELinux状态
          - `Enforcing`：SELinux已开启

```
1redfin:/data/local/tmp/dev/lldb # getenforce
Enforcing
```

          - `Permissive`：SELinux已关闭

```
redfin:/data/local/tmp/dev/lldb # getenforce
Permissive
```

心得

如何查看安卓app的进程的PID

有多种方式查看到，（当前正在运行的）安卓app的进程的PID：

- Mac中

```
frida-ps -Uai
```

  - 其中可以看到自己已安装的安卓的app的详情：进程PID、app名称、包名
    - 举例

```
➜  LiftFileManager_jadx_AlarmManager frida-ps -Uai | grep lift
24058   Lift File Manager  com.lift.filemanager.android
```

      - 可以看到要测试的app的：
        - 进程PID：`24058`
        - app名称：`Lift File Manager`
        - 包名：`com.lift.filemanager.android`

- （安卓手机的）adb的shell中

```
ps -A | grep yourAndroidAppName
```

  - 举例

```
redfin:/ # ps -A | grep lift
u0_a243       24058 1008 33543564 207388 do_epoll_wait      0 S com.lift.filema
nager.android
u0_a243       xxxx  1008 14793148 119908 do_epoll_wait      0 S com.lift.filema
nager.android:sist
u0_a243       xxxx  1008 14754236 139864 do_epoll_wait      0 S com.lift.filema
nager.android:dae
u0_a243       xxxx  1008 14734752 109496 do_epoll_wait      0 S com.lift.filema
nager.android:lift
```

    - LiftFileManager的主进程PID是：`24058`

如何用lldb调试程序

之后就是，如何用lldb调试的具体效果了。

举例：

去看看加载的image：

```
(lldb) image list -o -f
(lldb) image list -o -f
[  0] 0x0000006524034000 /Users/crifan/.lldb/module_cache/remote-android/.cache/8B041FC
2-79D5-1089-00E4-8324BAFA5142/app_process64
[  1] 0x0000007075ae9000 [vdso](0x0000007075ae9000)
[  2] 0x0000007075aea000 /Users/crifan/.lldb/module_cache/remote-android/.cache/0714FD9
0-1698-1186-FE9E-FC2187186124/linker64
[  3] 0x00000070728d6000 /Users/crifan/.lldb/module_cache/remote-android/.cache/1DEC513
4-A095-22F9-C83C-48DAE0AEC3BE/libandroid_runtime.so
[  4] 0x000000706fe94000 /Users/crifan/.lldb/module_cache/remote-android/.cache/52A9662
```

```
3-E462-0961-84C4-425671CC1C5D/libbinder.so
[  5] 0x0000007044c000 /Users/crifan/.lldb/module_cache/remote-android/.cache/ED5D3D4
6-2F5F-F1ED-D424-A588996F33C8/libcutils.so
[  6] 0x0000007070e09000 /Users/crifan/.lldb/module_cache/remote-android/.cache/CE1E7F5
F-3909-217B-2745-8673575C5CBE/libhidlbase.so
[  7] 0x0000007070f9e000 /Users/crifan/.lldb/module_cache/remote-android/.cache/661D436
6-5D5E-C814-EC19-1E5D951FE16A/liblog.so
[  8] 0x0000007073549000 /Users/crifan/.lldb/module_cache/remote-android/.cache/5D6AF74
1-2421-1886-D954-D61C96514A46/libutils.so
[  9] 0x000000706f681000 /Users/crifan/.lldb/module_cache/remote-android/.cache/584DB18
9-C827-EFEF-DD92-857A7E567C38/libwilhelm.so
[ 10] 0x0000007072800000 /Users/crifan/.lldb/module_cache/remote-android/.cache/0258740
B-928B-138C-E564-C516FD6B9141/libc++.so
[ 11] 0x000000706706c0000 /Users/crifan/.lldb/module_cache/remote-android/.cache/49090AE
5-9E6A-E37F-8BEA-E53C551820AD/libc.so
[ 12] 0x000000706f703000 /Users/crifan/.lldb/module_cache/remote-android/.cache/1B99BAD
0-6575-7949-B4B5-3A0C1FD55A0D/libm.so
[ 13] 0x000000706f956000 /Users/crifan/.lldb/module_cache/remote-android/.cache/316B312
0-5B8A-84EF-BC6D-1492C06AEEB8/libdl.so
[ 14] 0x0000007072482000 /Users/crifan/.lldb/module_cache/remote-android/.cache/01A12DD
5-2243-73ED-CC3A-74506F64A9C9/libbase.so
...
[265] 0x0000006dc2241000 /Users/crifan/.lldb/module_cache/remote-android/.cache/7A027C1
B-6689-FB13-BC4C-DDF60D309D9F/libllvm-glnext.so
[266] 0x0000006dc1e86000 /Users/crifan/.lldb/module_cache/remote-android/.cache/EF21915
6-ADF1-D883-C02F-44E4C1FC04B2/libGLESv1_CM_adreno.so
[267] 0x0000006dc1e69000 /Users/crifan/.lldb/module_cache/remote-android/.cache/FFCCE96
5-AAA2-1D95-77F2-CF1708C764B7/eglSubDriverAndroid.so
[268] 0x0000006dc1d8b000 /Users/crifan/.lldb/module_cache/remote-android/.cache/28A702E
7-CF8C-5CCC-2481-D2DD8B341E1B/libcompiler_rt.so
[269] 0x0000006dc1d42000 /Users/crifan/.lldb/module_cache/remote-android/.cache/11A028B
E-C11F-BD95-B235-8593B25A1887/libwebviewchromium_loader.so
[270]                   JIT(0x99dda8b0)(0x0000000099dda8b0)
[271]                   JIT(0x99dda350)(0x0000000099dda350)
[272]                   JIT(0x99dda010)(0x0000000099dda010)
...
[338]                   JIT(0x95dd2cd0)(0x0000000095dd2cd0)
[339]                   JIT(0x95dd28d0)(0x0000000095dd28d0)
[340]                   JIT(0x95dd2450)(0x0000000095dd2450)
(lldb)
```

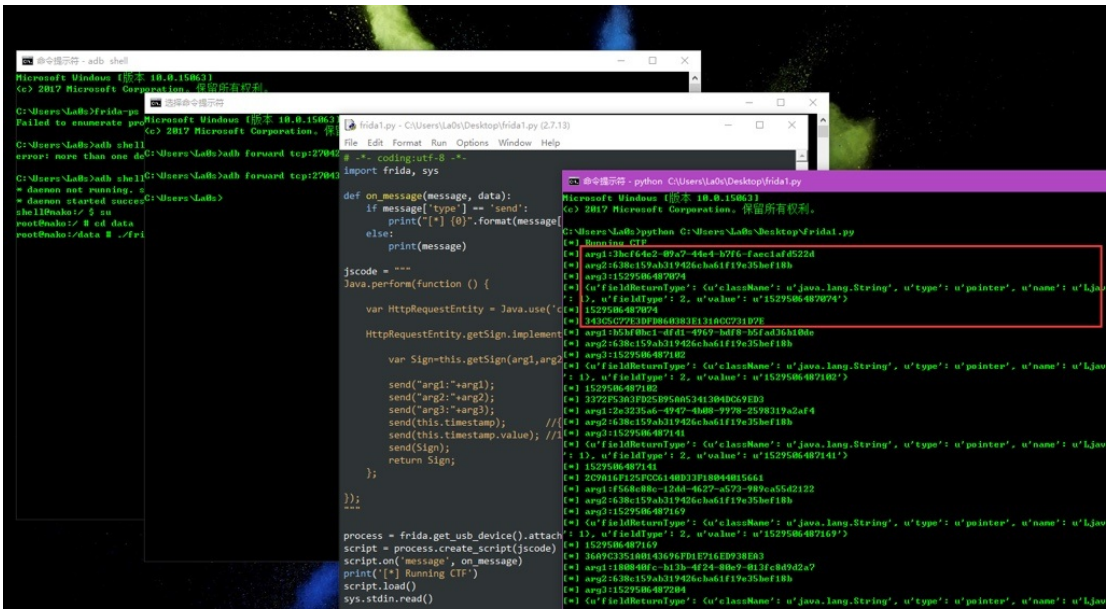
- 截图

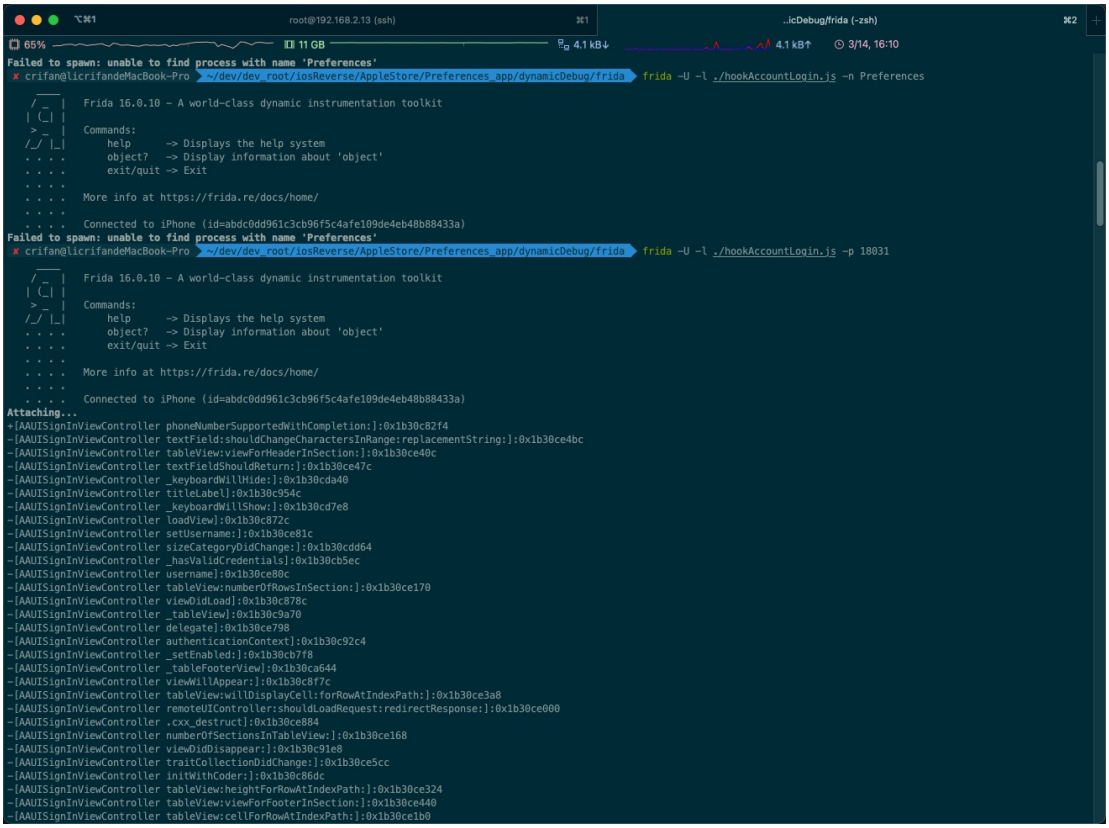
-
-

其他更多关于LLDB的用法，详见独立子教程：

主流调试器：LLDB

Frida调试安卓

- `Frida`
  - 概述
    - **iOS逆向**和**Android逆向**中常用的动态调试工具之一
    - 用于动态调试程序逻辑，实现各种调试功能
    - 核心使用逻辑是 `frida+js脚本` ，或 `frida-trace` 追踪函数执行过程
      - 以及高级的 `Frida` 的 `Stalker` 追踪函数实际运行过程等等
  - 主页
    - 官网
      - https://frida.re/
    - Github
      - https://github.com/frida/frida
- 截图
  - Windows
    - 
  - Mac



- 详解
  - 独立子教程
    - 逆向调试利器：Frida

初始化Frida开发环境

- 概述
  - 电脑端安装 `frida` （和 `frida-tools` ），移动端安装 `frida` （的**server**）
    - Mac中逆向iOS
      - Mac：安装 `frida` （ `pip3 install frida` ）和安装 `frida-tools` （ `pip3 install frida-tools` ）
      - iOS（iPhone）：包管理器（ `Sileo` / `Cydia` ）中（通过软件源： `https://build.frida.re` ）安装 `frida` 的插件
    - Mac中逆向Android
      - Mac：安装 `frida` （ `pip3 install frida` ）和安装 `frida-tools` （ `pip3 install frida-tools` ）
      - Android： `Magisk` 中安装MagiskFrida插件
        - 注：Frida官网的Android版 `frida-server` 有问题，所以换装第三方可用版本
- 详见
  - 安装和升级 · 逆向调试利器：Frida (crifan.org)

Frida调试安卓app

用 `frida` 或 `frida-trace` 等工具去调试安卓应用：

找到安卓应用的包名或PID

```
frida-ps -Uai
```

找到此处的要调试的应用：

- 19384 DisplayDemo com.example.displaydemo
  - =>
    - app名：DisplayDemo
    - 包名：com.example.displaydemo
    - PID：19384

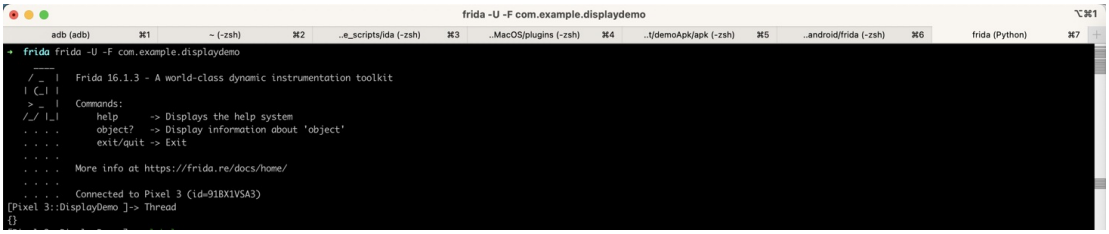
用 `frida` 或 `frida-trace` 去调试

此处手动点击DisplayDemo这个app，确保在前台运行，然后去hook调试：

- frida

  ```
  frida -U -F com.example.displaydemo
  ```

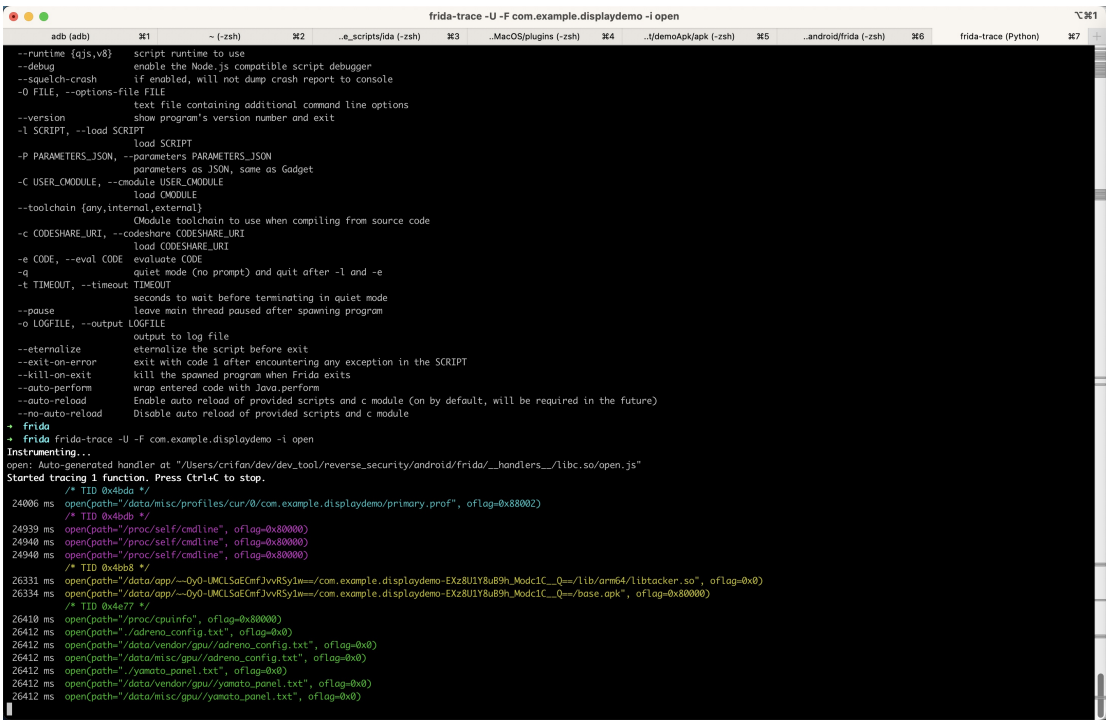
  - 效果

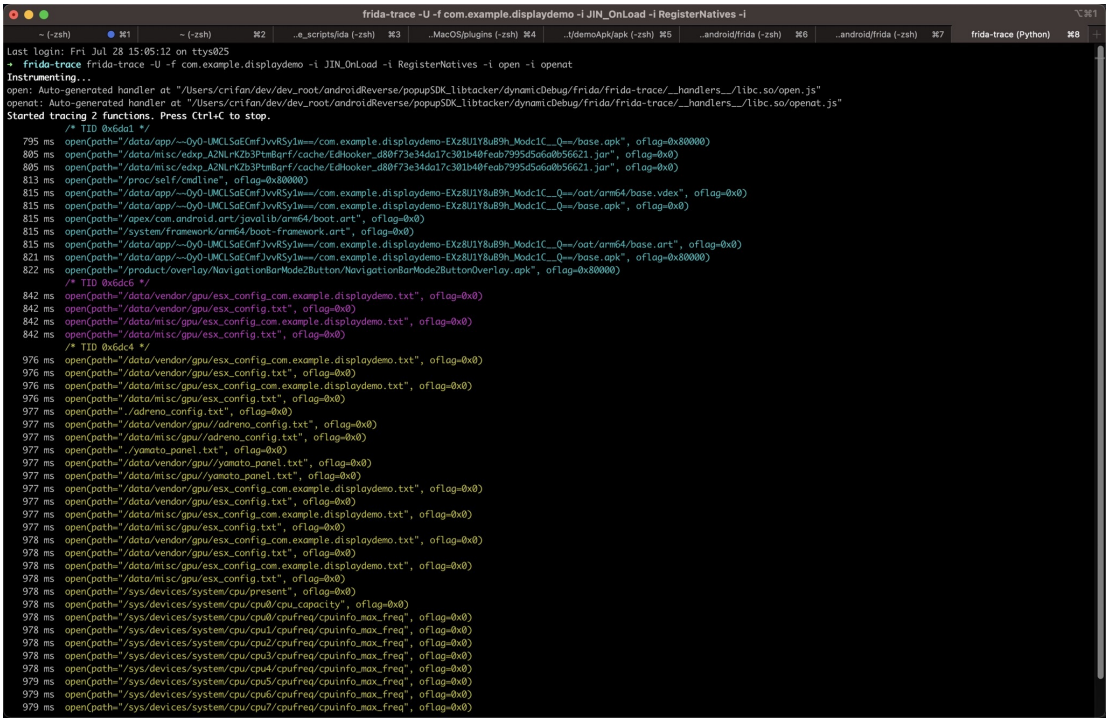
    

- frida-trace

  ```
  frida-trace -U -F com.example.displaydemo -i open
  frida-trace -U -f com.example.displaydemo -i JIN_OnLoad -i RegisterNatives -i open
  -i openat
  ```

  - 效果

- 

- 

示例

此处贴出一些，用Frida去调试安卓应用的，相关实例演示。

LiftFileManager

用 `frida` 加 `js` 脚本去调试 `com.lift.filemanager.android` = `LiftFileManager`：

命令

```
frida -U -f com.lift.filemanager.android -l hook_LiftFileManager.js
```

js脚本代码

- `hook_LiftFileManager.js`

```
/**
 * Update: 20230808
 * Usage:
 *  frida -U -f com.lift.filemanager.android -l hook_LiftFileManager.js
 */

function processJniOnLoad(libraryName) {
  const funcSym = "JNI_OnLoad";
  const funcPtr = Module.findExportByName(libraryName, funcSym);
  console.log("funcSym=" + funcSym + ", funcPtr=" + funcPtr);

  console.log("[+] Hooking " + funcSym + "() @ " + funcPtr + "...");
  // jint JNI_OnLoad(JavaVM *vm, void *reserved);
  var funcHook = Interceptor.attach(funcPtr, {
      onEnter: function (args) {
          const vm = args[0];
          const reserved = args[1];
          console.log("[+] " + funcSym + "(" + vm + ", " + reserved + ") called");
      },
      onLeave: function (retval) {
        console.log("[+]\t= " + retval);
      }
  });
}

function processNativeFunc(libraryName, nativeFuncName) {
  const nativeFuncPtr = Module.findExportByName(libraryName, nativeFuncName);
  console.log("nativeFuncName=" + nativeFuncName + ", nativeFuncPtr=" + nativeFuncPtr);
  var nativeFuncHook = Interceptor.attach(nativeFuncPtr, {
    onEnter: function (args) {
      const args0 = args[0];
      console.log(nativeFuncName + " [+] args0=" + args0);
    },
    onLeave: function (retval) {
      console.log("[+]\t= " + retval);
    }
  });
}
```

```
// hook normal C function
function hookCFunc(){

  // int execlp(const char *path, const char *arg0, ..., NULL);
  Interceptor.attach(Module.findExportByName(null, "execlp"), {
    onEnter: function (args) {
      var path = Memory.readCString(args[0]);
      var arg0 = Memory.readCString(args[1]);
      var arg1 = Memory.readCString(args[2]);
      console.log("execlp: path=" + path + ", arg0=" + arg0 + ", arg1=" + arg1);
    },
    onLeave: function (args) {
    }
  });

  // int execv(const char *pathname, char *const argv[]);
  Interceptor.attach(Module.findExportByName(null, "execv"), {
    onEnter: function (args) {
      var pathname = Memory.readCString(args[0]);
      var argv = args[1];
      console.log("execv: pathname=" + pathname + ", argv=" + argv);
    },
    onLeave: function (args) {
    }
  });

  // int pthread_create(pthread_t *thread, const pthread_attr_t *attr, void *(*start_ro
utine)(void*), void *arg);
  Interceptor.attach(Module.findExportByName(null, "pthread_create"), {
    onEnter: function (args) {
      var thread = args[0];
      var attr = args[1];
      var start_routine = args[2];
      var arg = args[3];
      console.log("pthread_create: thread=" + thread + ", attr=" + attr + ", start_rout
ine=" + start_routine + ", arg=" + arg);
    },
    onLeave: function (retNewPid) {
      console.log("\t pthread_create retNewPid= " + retNewPid);
    }
  });

  // int clone(int (*fn)(void *_Nullable), void *stack, int flags, void *_Nullable arg,
 ...  /* pid_t *_Nullable parent_tid, void *_Nullable tls, pid_t *_Nullable child_tid *
/ );
  Interceptor.attach(Module.findExportByName(null, "clone"), {
    onEnter: function (args) {
      var fn = args[0];
      var stack = args[1];
      var flags = args[2];
      var arg = args[3];
      console.log("clone: fn=" + fn + ", stack=" + stack + ", flags=" + flags + ", arg="
 + arg);
    },
    onLeave: function (retval) {
```

```
    }
  });

  // pid_t fork(void);
  Interceptor.attach(Module.findExportByName(null, "fork"), {
    onEnter: function (args) {
      console.log("fork called");
    },
    onLeave: function (retval) {
      console.log("\t fork retval= " + retval);
    }
  });

  // int posix_spawn(pid_t *pid, const char *path, const posix_spawn_file_actions_t *fi
le_actions, const posix_spawnattr_t *attrp, char *const argv[], char *const envp[]);
  Interceptor.attach(Module.findExportByName(null, "posix_spawn"), {
    onEnter: function (args) {
      var pid = args[0];
      var path = Memory.readCString(args[1]);
      var file_actions = args[2];
      var attrp = args[3];
      var argv = args[4];
      var envp = args[5];
      console.log("posix_spawn: pid=" + pid + ", path=" + path + ", file_actions=" + fi
le_actions + ", attrp=" + attrp + ", argv=" + argv + ", envp=" + envp);
    },
    onLeave: function (retval) {
    }
  });

  // int posix_spawnp(pid_t *pid, const char *file, const posix_spawn_file_actions_t *f
ile_actions, const posix_spawnattr_t *attrp, char *const argv[], char *const envp[]);
  Interceptor.attach(Module.findExportByName(null, "posix_spawnp"), {
    onEnter: function (args) {
      var pid = args[0];
      var file = Memory.readCString(args[1]);
      var file_actions = args[2];
      var attrp = args[3];
      var argv = args[4];
      var envp = args[5];
      console.log("posix_spawnp: pid=" + pid + ", file=" + file + ", file_actions=" + f
ile_actions + ", attrp=" + attrp + ", argv=" + argv + ", envp=" + envp);
    },
    onLeave: function (retval) {
    }
  });

  // int sigaction(int signum, const struct sigaction *_Nullable restrict act, struct s
igaction *_Nullable restrict oldact);
  Interceptor.attach(Module.findExportByName(null, "sigaction"), {
    onEnter: function (args) {
      var signum = args[0];
      var actP = args[1];
      var oldactP = args[2];
      console.log("sigaction: signum=" + signum + ", actP=" + actP + ", oldactP=" + old
actP);
```

```
  },
  onLeave: function (args) {
  }
});

// int remove(const char *path);
Interceptor.attach(Module.findExportByName(null, "remove"), {
  onEnter: function (args) {
    var path = Memory.readCString(args[0]);
    console.log("remove: path=" + path);
  },
  onLeave: function (args) {
  }
});

// FILE *fopen(const char *restrict pathname, const char *restrict mode);
Interceptor.attach(Module.findExportByName(null, "fopen"), {
  onEnter: function (args) {
    var pathname = Memory.readCString(args[0]);
    var mode = Memory.readCString(args[1]);
    console.log("fopen: pathname=" + pathname + ", mode=" + mode);
  },
  onLeave: function (args) {
  }
});

// int open(const char *pathname, int flags, mode_t mode);
Interceptor.attach(Module.findExportByName(null, "open"), {
  onEnter: function (args) {
    var path = Memory.readCString(args[0]);
    var oflags = args[1];
    console.log("open: path=" + path + ", oflags=" + oflags);
  },
  onLeave: function (retFd) {
    console.log("\t open retFd=" + retFd);
  }
});

// int flock(int fd, int operation);
Interceptor.attach(Module.findExportByName(null, "flock"), {
  onEnter: function (args) {
    var fd = args[0];
    var operation = args[1];
    console.log("flock: fd=" + fd + ", operation=" + operation);
  },
  onLeave: function (retval) {
  }
});

// int killpg(int pgrp, int sig);
Interceptor.attach(Module.findExportByName(null, "killpg"), {
  onEnter: function (args) {
    var pgrp = args[0];
    var sig = args[1];
    console.log("killpg: pgrp=" + pgrp + ", sig=" + sig);
  },
```

```
    onLeave: function (args) {
    }
  });

  // // ssize_t read(int fd, void buf[.count], size_t count);
  // Interceptor.attach(Module.findExportByName(null, "read"), {
  //   onEnter: function (args) {
  //     var fd = args[0];
  //     var buf = args[1];
  //     var count = args[2];
  //     console.log("read: fd=" + fd + ", buf=" + buf + ", count=" + count);
  //   },
  //   onLeave: function (args) {
  //   }
  // });

  // ssize_t pread(int fildes, void *buf, size_t nbyte, off_t offset);
  Interceptor.attach(Module.findExportByName(null, "pread"), {
    onEnter: function (args) {
      var fildes = args[0];
      var buf = args[1];
      var nbyte = args[2];
      var offset = args[3];
      console.log("pread: fildes=" + fildes + ", buf=" + buf + ", nbyte=" + nbyte + ",
offset=" + offset);
    },
    onLeave: function (args) {
    }
  });

  // // ssize_t write(int fildes, const void *buf, size_t nbyte);
  // Interceptor.attach(Module.findExportByName(null, "write"), {
  //   onEnter: function (args) {
  //     var fildes = args[0];
  //     var buf = args[1];
  //     var nbyte = args[2];
  //     console.log("write: fildes=" + fildes + ", buf=" + buf + ", nbyte=" + nbyte);
  //   },
  //   onLeave: function (args) {
  //   }
  // });

  // ssize_t pwrite(int fildes, const void *buf, size_t nbyte, off_t offset);
  Interceptor.attach(Module.findExportByName(null, "pwrite"), {
    onEnter: function (args) {
      var fildes = args[0];
      var buf = args[1];
      var nbyte = args[2];
      var offset = args[3];
      console.log("pwrite: fildes=" + fildes + ", buf=" + buf + ", nbyte=" + nbyte + ",
 offset=" + offset);
    },
    onLeave: function (args) {
    }
  });
```

```
// int close(int fd);
Interceptor.attach(Module.findExportByName(null, "close"), {
  onEnter: function (args) {
    var fd = args[0];
    console.log("close: fd=" + fd);
  },
  onLeave: function (retval) {
  }
});

// int pipe(int pipefd[2]);
Interceptor.attach(Module.findExportByName(null, "pipe"), {
  onEnter: function (args) {
    var pipefdArray = args[0];
    console.log("pipe: pipefdArray=" + pipefdArray);
  },
  onLeave: function (retval) {
  }
});

const KnownStrLis = [
  "",
  "CurrencyMap/US/0/",
  "CurrencyMap/CN/0/",
  "CurrencyMap/CN/",
  "CurrencyMap/",
  "CurrencyMap",
  "CN",
  "US",
  "/",
  "0",
  "id",
  "zh_CN_#HANS",
  "zh_Hans_CN",
  "zh",
  "Hans",
  "HANS",
]

// char *strcpy(char *restrict dst, const char *restrict src);
Interceptor.attach(Module.findExportByName(null, "strcpy"), {
  onEnter: function (args) {
    var dst = Memory.readCString(args[0]);
    var src = Memory.readCString(args[1]);
    if ( KnownStrLis.includes(src)) {
      console.log("strcpy: dst=" + dst + ", src=" + src);
    }
  },
  onLeave: function (args) {
  }
});

// char *strncpy(char *dest, const char *src, size_t count);
Interceptor.attach(Module.findExportByName(null, "strncpy"), {
  onEnter: function (args) {
    var dest = Memory.readCString(args[0]);
```

```
    var src = Memory.readCString(args[1]);
    var count = args[2];
    console.log("strncpy: dest=" + dest + ", src=" + src + ", count=" + count);
  },
  onLeave: function (args) {
  }
});

// char *strcat(char *restrict dst, const char *restrict src);
Interceptor.attach(Module.findExportByName(null, "strcat"), {
  onEnter: function (args) {
    var dst = Memory.readCString(args[0]);
    var src = Memory.readCString(args[1]);
    console.log("strcat: dst=" + dst + ", src=" + src);
  },
  onLeave: function (args) {
  }
});

// // pid_t getpid(void);
// Interceptor.attach(Module.findExportByName(null, "getpid"), {
//   onEnter: function (args) {
//     // console.log("getpid called");
//   },
//   onLeave: function (retPid) {
//     console.log("\t getpid retPid=" + retPid);
//   }
// });

// pid_t getppid(void);
Interceptor.attach(Module.findExportByName(null, "getppid"), {
  onEnter: function (args) {
    console.log("getppid called");
  },
  onLeave: function (retval) {
    console.log("\t getppid retval=" + retval);
  }
});

// pid_t setsid(void);
Interceptor.attach(Module.findExportByName(null, "setsid"), {
  onEnter: function (args) {
    console.log("setsid called");
  },
  onLeave: function (retval) {
    console.log("\t setsid retval=" + retval);
  }
});

// void *dlopen(const char *filename, int flags);
Interceptor.attach(Module.findExportByName(null, "dlopen"), {
  onEnter: function (args) {
    var filename = Memory.readCString(args[0]);
    var flags = args[1];
    console.log("dlopen: filename=" + filename + ", flags=" + flags);
  },
```

```
    onLeave: function (args) {
    }
  });

}

function waitForLibLoading(libraryName) {
  var isLibLoaded = false;

  hookCFunc();

  Interceptor.attach(Module.findExportByName(null, "android_dlopen_ext"), {
      onEnter: function (args) {
          var libPath = Memory.readCString(args[0]);
          var flags = args[1];
          var info = args[2];
          console.log("android_dlopen_ext: libPath=" + libPath + ", flags=" + flags + "
, info=" + info);
          if (libPath.includes(libraryName)) {
            console.log("[+] Loading library " + libPath + "...");
            isLibLoaded = true;
          }
      },
      onLeave: function (args) {
          if (isLibLoaded) {
            processJniOnLoad(libraryName);

            // public static native void display(Application application);
            const nativeFuncName = "Java_com_aSIIoEMUzSX_fukjRx_Nzilsxr_DYphTcg"
            processNativeFunc(libraryName, nativeFuncName);

            isLibLoaded = false;
          }
      }
  });
}

Java.perform(function() {
  const libraryName = "libRehADGd.so";
  waitForLibLoading(libraryName);
});
```

输出

截图

- （之前某次的）截图

-
-

-

log日志

```
➜  frida frida -U -f com.lift.filemanager.android -l hook_LiftFileManager.js
     ____
    / _  |   Frida 16.1.3 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Pixel 3 (id 91BX1VSA3)
Spawned `com.lift.filemanager.android`. Resuming main thread
[Pixel 3::com.lift.filemanager.android ]-> open: path /data/app/~~gJRGEMcdzVg-RT9VfCj4AA==/com.lift.filemanager.android-viAUZmvMdgKc2Zy2M8FibQ==/base.apk, oflags 0x80000
open: path /data/misc/edxp_A2NLrKZb3PtmBqrf/cache/EdHooker_d80f73e34da17c301b40feab7995d5a6a0b56621.jar, oflags 0x0
open: path /data/misc/edxp_A2NLrKZb3PtmBqrf/cache/EdHooker_d80f73e34da17c301b40feab7995d5a6a0b56621.jar, oflags 0x0
open: path /proc/self/cmdline, oflags 0x80000
open: path /data/app/~~gJRGEMcdzVg-RT9VfCj4AA==/com.lift.filemanager.android-viAUZmvMdgKc2Zy2M8FibQ==/base.apk, oflags 0x80000
open: path /product/overlay/NavigationBarMode2Button/NavigationBarMode2ButtonOverlay.apk, oflags 0x80000
pthread_create: thread 0x7fe513f228, attr 0x7fe513f260, start_routine 0x6ddf1e6b3c, arg 0x6f4f35ffc0
clone: fn 0x707076fd0c, stack 0x6d6daf4cc0, flags 0x3d0f00, arg 0x6d6daf4cc0
pthread_create: thread 0x7fe513f258, attr 0x7fe513f290, start_routine 0x6ddf1e6b3c, arg 0x6f4f35ffc0
clone: fn 0x707076fd0c, stack 0x6d6daf4cc0, flags 0x3d0f00, arg 0x6d6daf4cc0
```

```
pthread_create: thread 0x7fe513f2a8, attr 0x7fe513f2e0, start_routine 0x6ddf1e6b3c, arg
0x6f4f35c820
clone: fn 0x707076fd0c, stack 0x6d6c9eacc0, flags 0x3d0f00, arg 0x6d6c9eacc0
pthread_create: thread 0x6d6c9ea3c8, attr 0x6d6c9ea400, start_routine 0x6ddf1e6b3c, arg
0x6f4f361b90
clone: fn 0x707076fd0c, stack 0x6d6b8e0cc0, flags 0x3d0f00, arg 0x6d6b8e0cc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/frc_1:565703110738:an
droid:37ec4862ed1c78d044af8b_firebase_settings.xml, oflags 0x0
pthread_create: thread 0x7fe513f1e8, attr 0x7fe513f220, start_routine 0x6ddf1e6b3c, arg
0x6f4f365330
clone: fn 0x707076fd0c, stack 0x6d6a7d6cc0, flags 0x3d0f00, arg 0x6d6a7d6cc0
pthread_create: thread 0x6d6c9ea388, attr 0x6d6c9ea3c0, start_routine 0x6ddf1e6b3c, arg
0x6f4f366f00
clone: fn 0x707076fd0c, stack 0x6d6a8e0cc0, flags 0x3d0f00, arg 0x6d6a8e0cc0
pthread_create: thread 0x6d6c9ea388, attr 0x6d6c9ea3c0, start_routine 0x6ddf1e6b3c, arg
0x6f4f363760
clone: fn 0x707076fd0c, stack 0x6d6a6cccc0, flags 0x3d0f00, arg 0x6d6a6cccc0
pthread_create: thread 0x6d6c9ea388, attr 0x6d6c9ea3c0, start_routine 0x6ddf1e6b3c, arg
0x6f4f36c270
clone: fn 0x707076fd0c, stack 0x6d6a5c2cc0, flags 0x3d0f00, arg 0x6d6a5c2cc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.google.firebase.c
rashlytics.xml, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/frc_1:565703110738:android:3
7ec4862ed1c78d044af8b_firebase_defaults.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/frc_1:565703110738:android:3
7ec4862ed1c78d044af8b_firebase_fetch.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/frc_1:565703110738:android:3
7ec4862ed1c78d044af8b_firebase_activate.json, oflags 0x0
pthread_create: thread 0x7fe513f258, attr 0x7fe513f290, start_routine 0x6ddf1e6b3c, arg
0x6f4f36de40
pthread_create: thread 0x6d6daf4348, attr 0x6d6daf4380, start_routine 0x6ddf1e6b3c, arg
0x6f4f361b90
clone: fn 0x707076fd0c, stack 0x6d6b6e0cc0, flags 0x3d0f00, arg 0x6d6b6e0cc0
clone: fn 0x707076fd0c, stack 0x6d6b5d6cc0, flags 0x3d0f00, arg 0x6d6b5d6cc0
open: path /proc/6929/timerslack_ns, oflags 0x88241
android_dlopen_ext: libPath /data/user_de/0/com.google.android.gms/app_chimera/m/000000
47/oat/arm64/DynamiteLoader.odex, flags 0x2, info 0x6d6daf3b58
open: path /proc/6930/timerslack_ns, oflags 0x88241
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000047/oat/arm64/Dyna
miteLoader.vdex, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/.com.google.firebase.crashly
tics.files.v2:com.lift.filemanager.android/com.crashlytics.settings.json, oflags 0x0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000047/DynamiteLoader
.apk, oflags 0x0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000047/DynamiteLoader
.apk, oflags 0x0
open: path /apex/com.android.art/javalib/arm64/boot.art, oflags 0x0
open: path /system/framework/arm64/boot-framework.art, oflags 0x0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000047/oat/arm64/Dyna
miteLoader.art, oflags 0x0
pthread_create: thread 0x7fe513f1e8, attr 0x7fe513f220, start_routine 0x6ddf1e6b3c, arg
0x6f4f36a6a0
clone: fn 0x707076fd0c, stack 0x6d6b3bccc0, flags 0x3d0f00, arg 0x6d6b3bccc0
open: path /proc/6931/timerslack_ns, oflags 0x88241
pthread_create: thread 0x7fe513f1f8, attr 0x7fe513f230, start_routine 0x6ddf1e6b3c, arg
0x6f4f368ad0
```

```
clone: fn 0x707076fd0c, stack 0x6d6b2b2cc0, flags 0x3d0f00, arg 0x6d6b2b2cc0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
pthread_create: thread 0x6d6b2b2408, attr 0x6d6b2b2440, start_routine 0x6ddf1e6b3c, arg
0x6f4f3715e0
clone: fn 0x707076fd0c, stack 0x6d6b1a8cc0, flags 0x3d0f00, arg 0x6d6b1a8cc0
pthread_create: thread 0x6d6b2b2598, attr 0x6d6b2b25d0, start_routine 0x6ddf1e6b3c, arg
0x6f4f36fa10
clone: fn 0x707076fd0c, stack 0x6d6b09ecc0, flags 0x3d0f00, arg 0x6d6b09ecc0
open: path /proc/6933/timerslack_ns, oflags 0x88241
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
pthread_create: thread 0x7fe513f0f8, attr 0x7fe513f130, start_routine 0x6ddf1e6b3c, arg
0x6f4f374d80
clone: fn 0x707076fd0c, stack 0x6d6af94cc0, flags 0x3d0f00, arg 0x6d6af94cc0
pthread_create: thread 0x7fe513f508, attr 0x7fe513f540, start_routine 0x6ddf1e6b3c, arg
0x6f4f3731b0
clone: fn 0x707076fd0c, stack 0x6d6ae8acc0, flags 0x3d0f00, arg 0x6d6ae8acc0
open: path /proc/meminfo, oflags 0x0
pthread_create: thread 0x6d6ae8a3b8, attr 0x6d6ae8a3f0, start_routine 0x6ddf1e6b3c, arg
0x6f4f376950
clone: fn 0x707076fd0c, stack 0x6d6ad80cc0, flags 0x3d0f00, arg 0x6d6ad80cc0
open: path /data/app/~~H9XVwTH8sAvVL5p5cBHHzw==/com.google.android.gms-EalbGkD7CDLYvLNB
ylKTSQ==/base.apk, oflags 0x80000
pthread_create: thread 0x7fe513f808, attr 0x7fe513f840, start_routine 0x6ddf1e6b3c, arg
0x6f4f378520
clone: fn 0x707076fd0c, stack 0x6d6ac76cc0, flags 0x3d0f00, arg 0x6d6ac76cc0
open: path /data/user/0/com.lift.filemanager.android/databases/com.google.android.datat
ransport.events, oflags 0xa0042
open: path /data/app/~~H9XVwTH8sAvVL5p5cBHHzw==/com.google.android.gms-EalbGkD7CDLYvLNB
ylKTSQ==/split_config.xxhdpi.apk, oflags 0x80000
open: path /data/app/~~H9XVwTH8sAvVL5p5cBHHzw==/com.google.android.gms-EalbGkD7CDLYvLNB
ylKTSQ==/split_config.zh.apk, oflags 0x80000
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/FirebaseHeartBeatW0RF
RkFVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.xml, oflags 0x0
pthread_create: thread 0x7fe513f3a8, attr 0x7fe513f3e0, start_routine 0x6ddf1e6b3c, arg
0x6f4f37a0f0
clone: fn 0x707076fd0c, stack 0x6d6ad80cc0, flags 0x3d0f00, arg 0x6d6ad80cc0
open: path /data/user/0/com.lift.filemanager.android/files/.com.google.firebase.crashly
tics.files.v2:com.lift.filemanager.android/open-sessions/64D0B857022700011AB6F3CB35D4C1
92/report, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/files/.com.google.firebase.crashly
tics.files.v2:com.lift.filemanager.android/open-sessions/64D0B857022700011AB6F3CB35D4C1
92/start-time, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/files/.com.google.firebase.crashly
tics.files.v2:com.lift.filemanager.android/initialization_marker, oflags 0xc2
android_dlopen_ext: libPath /system/framework/oat/arm64/org.apache.http.legacy.odex, fl
ags 0x2, info 0x6d6ac749a8
open: path /data/user/0/com.lift.filemanager.android/no_backup/androidx.work.workdb, of
lags 0xa0042
pthread_create: thread 0x7fe513f558, attr 0x7fe513f590, start_routine 0x6ddf1e6b3c, arg
0x6f4f376950
```

```
clone: fn 0x707076fd0c, stack 0x6d6a7d6cc0, flags 0x3d0f00, arg 0x6d6a7d6cc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.facebook.sdk.appE
ventPreferences.xml, oflags 0x0
android_dlopen_ext: libPath /data/user_de/0/com.google.android.gms/app_chimera/m/000000
4c/oat/arm64/MeasurementDynamite.odex, flags 0x2, info 0x6d6daf3838
open: path /system/framework/oat/arm64/org.apache.http.legacy.vdex, oflags 0x0
open: path /system/framework/org.apache.http.legacy.jar, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/no_backup/androidx.work.workdb-wal
, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/no_backup/androidx.work.workdb-shm
, oflags 0x80042
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/0000004c/oat/arm64/Meas
urementDynamite.vdex, oflags 0x0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/0000004c/MeasurementDyn
amite.apk, oflags 0x0
open: path /system/framework/org.apache.http.legacy.jar, oflags 0x0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/0000004c/MeasurementDyn
amite.apk, oflags 0x0
open: path /apex/com.android.art/javalib/arm64/boot.art, oflags 0x0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/0000004c/MeasurementDyn
amite.apk, oflags 0x80000
open: path /system/framework/arm64/boot-framework.art, oflags 0x0
open: path /system/framework/oat/arm64/org.apache.http.legacy.art, oflags 0x0
pthread_create: thread 0x7fe513f558, attr 0x7fe513f590, start_routine 0x6ddf1e6b3c, arg
0x6f4f376950
clone: fn 0x707076fd0c, stack 0x6d6a7d6cc0, flags 0x3d0f00, arg 0x6d6a7d6cc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.facebook.sdk.USER
_SETTINGS.xml, oflags 0x0
android_dlopen_ext: libPath /system/framework/oat/arm64/com.android.media.remotedisplay
.odex, flags 0x2, info 0x6d6ac749a8
open: path /data/user/0/com.lift.filemanager.android/no_backup/androidx.work.workdb, of
lags 0xa0042
pthread_create: thread 0x7fe513f5f8, attr 0x7fe513f630, start_routine 0x6ddf1e6b3c, arg
0x6f4f376950
clone: fn 0x707076fd0c, stack 0x6d6b8e0cc0, flags 0x3d0f00, arg 0x6d6b8e0cc0
open: path /data/user/0/com.lift.filemanager.android/no_backup/androidx.work.workdb-wal
, oflags 0xa0042
open: path /system/framework/oat/arm64/com.android.media.remotedisplay.vdex, oflags 0x0
open: path /system/framework/com.android.media.remotedisplay.jar, oflags 0x0
open: path /system/framework/com.android.media.remotedisplay.jar, oflags 0x0
open: path /apex/com.android.art/javalib/arm64/boot.art, oflags 0x0
open: path /system/framework/arm64/boot-framework.art, oflags 0x0
open: path /system/framework/oat/arm64/com.android.media.remotedisplay.art, oflags 0x0
pthread_create: thread 0x6d6b8e01c8, attr 0x6d6b8e0200, start_routine 0x6ddf1e6b3c, arg
0x6f4f37bcc0
clone: fn 0x707076fd0c, stack 0x6d6a7d6cc0, flags 0x3d0f00, arg 0x6d6a7d6cc0
pthread_create: thread 0x7fe513f508, attr 0x7fe513f540, start_routine 0x6ddf1e6b3c, arg
0x6f4f381030
clone: fn 0x707076fd0c, stack 0x6d5ccb2cc0, flags 0x3d0f00, arg 0x6d5ccb2cc0
open: path /dev/urandom, oflags 0x80000
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.facebook.internal
.preferences.APP_GATEKEEPERS.xml, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/no_backup/androidx.work.workdb-wal
, oflags 0xa0042
android_dlopen_ext: libPath /system/framework/oat/arm64/com.android.location.provider.o
dex, flags 0x2, info 0x6d6ac749a8
```

```
pthread_create: thread 0x7fe513f5f8, attr 0x7fe513f630, start_routine 0x6ddf1e6b3c, arg
0x6f4f381030
clone: fn 0x707076fd0c, stack 0x6d6a7d6cc0, flags 0x3d0f00, arg 0x6d6a7d6cc0
pthread_create: thread 0x7fe513f658, attr 0x7fe513f690, start_routine 0x6ddf1e6b3c, arg
0x6f4f37bcc0
clone: fn 0x707076fd0c, stack 0x6d5ccb2cc0, flags 0x3d0f00, arg 0x6d5ccb2cc0
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f37d890
clone: fn 0x707076fd0c, stack 0x6d5aac4cc0, flags 0x3d0f00, arg 0x6d5aac4cc0
pthread_create: thread 0x6d5ccb24d8, attr 0x6d5ccb2510, start_routine 0x6ddf1e6b3c, arg
0x6f4f382c00
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f387f70
clone: fn 0x707076fd0c, stack 0x6d597bacc0, flags 0x3d0f00, arg 0x6d597bacc0
clone: fn 0x707076fd0c, stack 0x6d598c4cc0, flags 0x3d0f00, arg 0x6d598c4cc0
pthread_create: thread 0x7fe513f6b8, attr 0x7fe513f6f0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3863a0
clone: fn 0x707076fd0c, stack 0x6d566b0cc0, flags 0x3d0f00, arg 0x6d566b0cc0
open: path /system/framework/oat/arm64/com.android.location.provider.vdex, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.facebook.internal
.preferences.APP_SETTINGS.xml, oflags 0x0
open: path /system/framework/com.android.location.provider.jar, oflags 0x0
pthread_create: thread 0x6d566b03b8, attr 0x6d566b03f0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3847d0
open: path /system/framework/com.android.location.provider.jar, oflags 0x0
clone: fn 0x707076fd0c, stack 0x6d555a6cc0, flags 0x3d0f00, arg 0x6d555a6cc0
pthread_create: thread 0x6d6ad805b8, attr 0x6d6ad805f0, start_routine 0x6ddf1e6b3c, arg
0x6f4f38d2e0
pthread_create: thread 0x7fe513f758, attr 0x7fe513f790, start_routine 0x6ddf1e6b3c, arg
0x6f4f38eeb0
open: path /apex/com.android.art/javalib/arm64/boot.art, oflags 0x0
open: path /system/framework/arm64/boot-framework.art, oflags 0x0
open: path /system/framework/oat/arm64/com.android.location.provider.art, oflags 0x0
clone: fn 0x707076fd0c, stack 0x6d54392cc0, flags 0x3d0f00, arg 0x6d54392cc0
clone: fn 0x707076fd0c, stack 0x6d5449ccc0, flags 0x3d0f00, arg 0x6d5449ccc0
pthread_create: thread 0x6d566b0418, attr 0x6d566b0450, start_routine 0x6ddf1e6b3c, arg
0x6f4f390a80
clone: fn 0x707076fd0c, stack 0x6d598c4cc0, flags 0x3d0f00, arg 0x6d598c4cc0
open: path /data/user/0/com.lift.filemanager.android/files/AppEventsLogger.persistedeve
nts, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/LifeSharedPrefers.xml
, oflags 0x0
android_dlopen_ext: libPath /data/app/~~H9XVwTH8sAvVL5p5cBHHzw== /com.google.android.gms
-EalbGkD7CDLYvLNBylKTSQ== /oat/arm64/base.odex, flags 0x2, info 0x6d6ac74b18
open: path /data/app/~~H9XVwTH8sAvVL5p5cBHHzw== /com.google.android.gms-EalbGkD7CDLYvLNB
ylKTSQ== /oat/arm64/base.vdex, oflags 0x0
open: path /data/app/~~H9XVwTH8sAvVL5p5cBHHzw== /com.google.android.gms-EalbGkD7CDLYvLNB
ylKTSQ== /base.apk, oflags 0x0
open: path /data/app/~~H9XVwTH8sAvVL5p5cBHHzw== /com.google.android.gms-EalbGkD7CDLYvLNB
ylKTSQ== /base.apk, oflags 0x0
open: path /apex/com.android.art/javalib/arm64/boot.art, oflags 0x0
open: path /system/framework/arm64/boot-framework.art, oflags 0x0
open: path /data/app/~~H9XVwTH8sAvVL5p5cBHHzw== /com.google.android.gms-EalbGkD7CDLYvLNB
ylKTSQ== /oat/arm64/base.art, oflags 0x0
pthread_create: thread 0x6d6ac764c8, attr 0x6d6ac76500, start_routine 0x6ddf1e6b3c, arg
0x6f4f38eeb0
```

```
clone: fn 0x707076fd0c, stack 0x6d533d0cc0, flags 0x3d0f00, arg 0x6d533d0cc0
open: path /data/user/0/com.google.android.gms/shared_prefs/google_ads_flags.xml, oflags
 0x0
open: path /data/app/~~RbAu5LfZALdcOdiK1xs1uA== /com.google.android.trichromelibrary_579
016631-9HB7aC3CI8mFFZlcY5ZSvA== /base.apk, oflags 0x0
pthread_create: thread 0x6d6daf3148, attr 0x6d6daf3180, start_routine 0x6ddf1e6b3c, arg
0x6f4f389b40
android_dlopen_ext: libPath /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.web
view-bGRQSGrklU6ssg_JAwBwSQ== /oat/arm64/base.odex, flags 0x2, info 0x7fe513d088
clone: fn 0x707076fd0c, stack 0x6d457b6cc0, flags 0x3d0f00, arg 0x6d457b6cc0
open: path /proc/6959/timerslack_ns, oflags 0x88241
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /oat/arm64/base.vdex, oflags 0x0
pthread_create: thread 0x6d6b8e0048, attr 0x6d6b8e0080, start_routine 0x6ddf1e6b3c, arg
0x6f4f38b710
clone: fn 0x707076fd0c, stack 0x6d533d0cc0, flags 0x3d0f00, arg 0x6d533d0cc0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /base.apk, oflags 0x0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /base.apk, oflags 0x0
open: path /apex/com.android.art/javalib/arm64/boot.art, oflags 0x0
open: path /system/framework/arm64/boot-framework.art, oflags 0x0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /oat/arm64/base.art, oflags 0x0
android_dlopen_ext: libPath /data/user_de/0/com.google.android.gms/app_chimera/m/000000
32/oat/arm64/dl-AdsFdrDynamite.integ_232400000100000.odex, flags 0x2, info 0x6d6ac75908
pthread_create: thread 0x6d457b5398, attr 0x6d457b53d0, start_routine 0x6ddf1e6b3c, arg
0x6f4f38eeb0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000032/oat/arm64/dl-A
dsFdrDynamite.integ_232400000100000.vdex, oflags 0x0
clone: fn 0x707076fd0c, stack 0x6d435c7cc0, flags 0x3d0f00, arg 0x6d435c7cc0
open: path /proc/6961/timerslack_ns, oflags 0x88241
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.google.android.gm
s.measurement.prefs.xml, oflags 0x0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /base.apk, oflags 0x80000
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000032/dl-AdsFdrDynam
ite.integ_232400000100000.apk, oflags 0x0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /split_config.zh.apk, oflags 0x80000
open: path /data/app/~~RbAu5LfZALdcOdiK1xs1uA== /com.google.android.trichromelibrary_579
016631-9HB7aC3CI8mFFZlcY5ZSvA== /base.apk, oflags 0x80000
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000032/dl-AdsFdrDynam
ite.integ_232400000100000.apk, oflags 0x0
open: path /apex/com.android.art/javalib/arm64/boot.art, oflags 0x0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /base.apk, oflags 0x80000
open: path /system/framework/arm64/boot-framework.art, oflags 0x0
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000032/oat/arm64/dl-A
dsFdrDynamite.integ_232400000100000.art, oflags 0x0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /split_config.zh.apk, oflags 0x80000
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw== /com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ== /split_weblayer.apk, oflags 0x80000
open: path /data/app/~~RbAu5LfZALdcOdiK1xs1uA== /com.google.android.trichromelibrary_579
016631-9HB7aC3CI8mFFZlcY5ZSvA== /base.apk, oflags 0x80000
```

```
android_dlopen_ext: libPath libmonochrome.so, flags 0x2, info 0x7fe513ec70
open: path /data/user_de/0/com.google.android.gms/app_chimera/m/00000032/dl-AdsFdrDynam
ite.integ_232400000100000.apk, oflags 0x80000
pthread_create: thread 0x6d457b5718, attr 0x6d457b5750, start_routine 0x6ddf1e6b3c, arg
0x6f4f392650
clone: fn 0x707076fd0c, stack 0x6d4308fcc0, flags 0x3d0f00, arg 0x6d4308fcc0
open: path /proc/6962/timerslack_ns, oflags 0x88241
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
pthread_create: thread 0x7fe513ddb8, attr 0x7fe513ddf0, start_routine 0x6ddf1e6b3c, arg
0x6f4f382c00
clone: fn 0x707076fd0c, stack 0x6d6ac76cc0, flags 0x3d0f00, arg 0x6d6ac76cc0
pthread_create: thread 0x7fe513dac8, attr 0x7fe513db00, start_routine 0x6ddf1e6b3c, arg
0x6f4f38eeb0
clone: fn 0x707076fd0c, stack 0x6d6ac76cc0, flags 0x3d0f00, arg 0x6d6ac76cc0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ==/lib/arm64/libmonochrome.so, oflags 0x0
open: path /proc/6964/timerslack_ns, oflags 0x88241
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ==/base.apk, oflags 0x80000
android_dlopen_ext: libPath /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.web
view-bGRQSGrklU6ssg_JAwBwSQ==/base.apk!/lib/arm64-v8a/libmonochrome.so, flags 0x2, info
0x7fe513d860
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ==/lib/arm64/libwebviewchromium_plat_support.so, oflags 0x0
open: path /data/app/~~RbAu5LfZALdcOdiK1xs1uA==/com.google.android.trichromelibrary_579
016631-9HB7aC3CI8mFFZlcY5ZSvA==/base.apk, oflags 0x80000
open: path /system/lib64/libwebviewchromium_plat_support.so, oflags 0x0
android_dlopen_ext: libPath /system/lib64/libwebviewchromium_plat_support.so, flags 0x2
, info 0x7fe513d9b0
pthread_create: thread 0x7fe513dbd8, attr 0x7fe513dc10, start_routine 0x6ddf1e6b3c, arg
0x6f4f382c00
```

```
clone: fn 0x707076fd0c, stack 0x6d43e7ecc0, flags 0x3d0f00, arg 0x6d43e7ecc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/WebViewChromiumPrefs.
xml, oflags 0x0
pthread_create: thread 0x7fe513ddf8, attr 0x7fe513de30, start_routine 0x6ddf1e6b3c, arg
0x6f4f382c00
clone: fn 0x707076fd0c, stack 0x6d43e7ecc0, flags 0x3d0f00, arg 0x6d43e7ecc0
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ==/base.apk, oflags 0x80000
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ==/split_config.zh.apk, oflags 0x80000
open: path /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.webview-bGRQSGrklU6s
sg_JAwBwSQ==/split_weblayer.apk, oflags 0x80000
open: path /product/overlay/NavigationBarMode2Button/NavigationBarMode2ButtonOverlay.ap
k, oflags 0x80000
open: path /proc/meminfo, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/app_webview/webview_data.lock, ofl
ags 0x42
pthread_create: thread 0x7fe513e008, attr 0x7fe513e040, start_routine 0x6ddf1e6b3c, arg
0x6f4f378520
clone: fn 0x707076fd0c, stack 0x6d43e7ecc0, flags 0x3d0f00, arg 0x6d43e7ecc0
pthread_create: thread 0x7fe513e988, attr 0x7fe513e9c0, start_routine 0x6ddf1e6b3c, arg
0x6f4f394220
clone: fn 0x707076fd0c, stack 0x6d43d74cc0, flags 0x3d0f00, arg 0x6d43d74cc0
open: path /proc/6968/timerslack_ns, oflags 0x88241
pthread_create: thread 0x6d43d744f8, attr 0x6d43d74530, start_routine 0x6ddf1e6b3c, arg
0x6f4f382c00
clone: fn 0x707076fd0c, stack 0x6d416fbcc0, flags 0x3d0f00, arg 0x6d416fbcc0
open: path /proc/self/stat, oflags 0x80000
open: path /proc/6969/timerslack_ns, oflags 0x88241
open: path /proc/cpuinfo, oflags 0x80000
dlopen: filename /data/app/~~ebf6Ooj8iz0WmmF2AEomWw==/com.google.android.webview-bGRQSG
rklU6ssg_JAwBwSQ==/base.apk /lib/arm64-v8a/libmonochrome.so, flags 0x5
sigaction: signum 0x6, actP 0x7fe513e408, oldactP 0x2002c40a8
sigaction: signum 0x7, actP 0x7fe513e408, oldactP 0x2002c40c8
sigaction: signum 0x8, actP 0x7fe513e408, oldactP 0x2002c40e8
sigaction: signum 0x4, actP 0x7fe513e408, oldactP 0x2002c4068
sigaction: signum 0xb, actP 0x7fe513e408, oldactP 0x2002c4148
sigaction: signum 0x1f, actP 0x7fe513e408, oldactP 0x2002c43c8
sigaction: signum 0x5, actP 0x7fe513e408, oldactP 0x2002c4088
open: path /data/user/0/com.lift.filemanager.android/app_webview/pref_store, oflags 0x8
0000
open: path /proc/cpuinfo, oflags 0x0
open: path /proc/cpuinfo, oflags 0x0
open: path /sys/devices/system/cpu/present, oflags 0x0
open: path /sys/devices/system/cpu/possible, oflags 0x0
dlopen: filename libc.so, flags 0x2
open: path /data/user/0/com.lift.filemanager.android/app_webview/BrowserMetrics/Browser
Metrics-64D0B857-1AB6.pma, oflags 0x2
pthread_create: thread 0x7fe513e598, attr 0x7fe513e6e0, start_routine 0x6d83f30904, arg
0x2003b7ea0
clone: fn 0x707076fd0c, stack 0x6d41187cc0, flags 0x3d0f00, arg 0x6d41187cc0
pthread_create: thread 0x7fe513e408, attr 0x7fe513e550, start_routine 0x6d83f30904, arg
0x2003b7da0
clone: fn 0x707076fd0c, stack 0x6d41089cc0, flags 0x3d0f00, arg 0x6d41089cc0
pthread_create: thread 0x6d41089758, attr 0x6d410898a0, start_routine 0x6d83f30904, arg
0x2003b7a60
```

```
clone: fn 0x707076fd0c, stack 0x6d3be70cc0, flags 0x3d0f00, arg 0x6d3be70cc0
open: path /proc/6838/stat, oflags 0x80000
pthread_create: thread 0x6d3be70758, attr 0x6d3be708a0, start_routine 0x6d83f30904, arg
0x2003b77a0
clone: fn 0x707076fd0c, stack 0x6d3ad42cc0, flags 0x3d0f00, arg 0x6d3ad42cc0
open: path /proc/6838/stat, oflags 0x80000
open: path /proc/6838/task/6838/stat, oflags 0x80000
open: path /proc/6838/task/6848/stat, oflags 0x80000
open: path /proc/6838/task/6849/stat, oflags 0x80000
open: path /proc/6838/task/6851/stat, oflags 0x80000
open: path /proc/6838/task/6852/stat, oflags 0x80000
open: path /proc/6838/task/6853/stat, oflags 0x80000
open: path /proc/6838/task/6854/stat, oflags 0x80000
pthread_create: thread 0x6d3ad42758, attr 0x6d3ad428a0, start_routine 0x6d83f30904, arg
0x2003b7620
open: path /proc/6838/task/6855/stat, oflags 0x80000
clone: fn 0x707076fd0c, stack 0x6d39c14cc0, flags 0x3d0f00, arg 0x6d39c14cc0
open: path /proc/6838/task/6892/stat, oflags 0x80000
open: path /proc/6838/task/6893/stat, oflags 0x80000
open: path /proc/6838/task/6894/stat, oflags 0x80000
open: path /proc/6838/task/6895/stat, oflags 0x80000
open: path /proc/6838/task/6896/stat, oflags 0x80000
open: path /proc/6838/task/6897/stat, oflags 0x80000
open: path /proc/6838/task/6898/stat, oflags 0x80000
open: path /proc/6838/task/6899/stat, oflags 0x80000
open: path /proc/6838/task/6900/stat, oflags 0x80000
open: path /proc/6838/task/6901/stat, oflags 0x80000
open: path /proc/6838/task/6917/stat, oflags 0x80000
open: path /proc/6838/task/6918/stat, oflags 0x80000
open: path /proc/6838/task/6919/stat, oflags 0x80000
open: path /proc/6838/task/6920/stat, oflags 0x80000
open: path /proc/6838/task/6922/stat, oflags 0x80000
open: path /proc/6838/task/6923/stat, oflags 0x80000
open: path /proc/6838/task/6926/stat, oflags 0x80000
open: path /proc/6838/task/6927/stat, oflags 0x80000
open: path /proc/6838/task/6928/stat, oflags 0x80000
open: path /proc/6838/task/6929/stat, oflags 0x80000
open: path /proc/6838/task/6930/stat, oflags 0x80000
open: path /proc/6838/task/6931/stat, oflags 0x80000
open: path /proc/6838/task/6932/stat, oflags 0x80000
open: path /proc/6838/task/6933/stat, oflags 0x80000
pthread_create: thread 0x7fe513e558, attr 0x7fe513e6a0, start_routine 0x6d83f30904, arg
0x2003b7600
clone: fn 0x707076fd0c, stack 0x6d38b0dcc0, flags 0x3d0f00, arg 0x6d38b0dcc0
open: path /proc/6838/task/6934/stat, oflags 0x80000
open: path /proc/6838/task/6935/stat, oflags 0x80000
open: path /proc/6838/task/6936/stat, oflags 0x80000
open: path /proc/6838/task/6939/stat, oflags 0x80000
open: path /proc/6838/task/6942/stat, oflags 0x80000
open: path /proc/6838/task/6945/stat, oflags 0x80000
open: path /proc/6838/task/6946/stat, oflags 0x80000
open: path /proc/6838/task/6947/stat, oflags 0x80000
open: path /proc/6838/task/6948/stat, oflags 0x80000
pthread_create: thread 0x7fe513e578, attr 0x7fe513e6c0, start_routine 0x6d83f30904, arg
0x2003b72e0
open: path /proc/6838/task/6950/stat, oflags 0x80000
```

```
clone: fn 0x707076fd0c, stack 0x6d37a06cc0, flags 0x3d0f00, arg 0x6d37a06cc0
open: path /proc/6838/task/6951/stat, oflags 0x80000
open: path /proc/6838/task/6953/stat, oflags 0x80000
open: path /proc/6838/task/6954/stat, oflags 0x80000
open: path /proc/6838/task/6959/stat, oflags 0x80000
open: path /proc/6838/task/6960/stat, oflags 0x80000
open: path /proc/6838/task/6962/stat, oflags 0x80000
open: path /proc/6838/task/6964/stat, oflags 0x80000
open: path /proc/6838/task/6967/stat, oflags 0x80000
open: path /proc/6838/task/6968/stat, oflags 0x80000
open: path /proc/6838/task/6969/stat, oflags 0x80000
open: path /proc/6838/task/6990/stat, oflags 0x80000
open: path /proc/6838/task/6991/stat, oflags 0x80000
open: path /proc/6838/task/6992/stat, oflags 0x80000
open: path /sys/devices/system/cpu/cpu0/regs/identification/midr_el1, oflags 0x0
open: path /proc/6838/task/6993/stat, oflags 0x80000
open: path /proc/6838/task/6994/stat, oflags 0x80000
open: path /proc/6838/task/6995/stat, oflags 0x80000
open: path /proc/6838/task/6996/stat, oflags 0x80000
open: path /sys/devices/system/cpu/cpu1/regs/identification/midr_el1, oflags 0x0
open: path /sys/devices/system/cpu/cpu2/regs/identification/midr_el1, oflags 0x0
open: path /sys/devices/system/cpu/cpu3/regs/identification/midr_el1, oflags 0x0
open: path /sys/devices/system/cpu/cpu4/regs/identification/midr_el1, oflags 0x0
open: path /sys/devices/system/cpu/cpu5/regs/identification/midr_el1, oflags 0x0
open: path /sys/devices/system/cpu/cpu6/regs/identification/midr_el1, oflags 0x0
open: path /sys/devices/system/cpu/cpu7/regs/identification/midr_el1, oflags 0x0
open: path /sys/devices/system/cpu/cpu8/regs/identification/midr_el1, oflags 0x0
dlopen: filename libandroid.so, flags 0x2
dlopen: filename libmediandk.so, flags 0x2
dlopen: filename libandroid.so, flags 0x2
pthread_create: thread 0x7fe513e988, attr 0x7fe513ead0, start_routine 0x6d83f30904, arg
0x6a0001ce40
clone: fn 0x707076fd0c, stack 0x6d368ffcc0, flags 0x3d0f00, arg 0x6d368ffcc0
open: path /system/etc/hosts, oflags 0x80000
pthread_create: thread 0x7fe513e958, attr 0x7fe513eaa0, start_routine 0x6d83f30904, arg
0x6a0001cdc0
clone: fn 0x707076fd0c, stack 0x6d357f8cc0, flags 0x3d0f00, arg 0x6d357f8cc0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/font_unique_name_tab
le.pb, oflags 0x0
dlopen: filename libandroid.so, flags 0x2
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Preferences, o
flags 0x80000
pthread_create: thread 0x7fe513e748, attr 0x7fe513e890, start_routine 0x6d83f30904, arg
0x6a0001d8a0
clone: fn 0x707076fd0c, stack 0x6d34698cc0, flags 0x3d0f00, arg 0x6d34698cc0
open: path /data/data/com.lift.filemanager.android/app_webview/Default/Web Data, oflags
0xa8042
pthread_create: thread 0x7fe513dc68, attr 0x7fe513ddb0, start_routine 0x6d83f30904, arg
0x6a0001f680
clone: fn 0x707076fd0c, stack 0x6d33561cc0, flags 0x3d0f00, arg 0x6d33561cc0
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Local Storage/
leveldb/LOG, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Local Storage/
leveldb/LOCK, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Local Storage/
leveldb/CURRENT, oflags 0x0
```

```
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Local Storage/
leveldb/MANIFEST-000001, oflags 0x0
pthread_create: thread 0x7fe513e0b8, attr 0x7fe513e200, start_routine 0x6d83f30904, arg
0x6a0013fae0
clone: fn 0x707076fd0c, stack 0x6d32442cc0, flags 0x3d0f00, arg 0x6d32442cc0
pthread_create: thread 0x7fe513e0b8, attr 0x7fe513e200, start_routine 0x6d83f30904, arg
0x6a0013fb60
clone: fn 0x707076fd0c, stack 0x6d3133bcc0, flags 0x3d0f00, arg 0x6d3133bcc0
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Local Storage/
leveldb/MANIFEST-000001, oflags 0x401
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Local Storage/
leveldb/000003.log, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Local Storage/
leveldb/000003.log, oflags 0x401
pthread_create: thread 0x7fe513e478, attr 0x7fe513e5c0, start_routine 0x6d83f30904, arg
0x6a0013eb40
clone: fn 0x707076fd0c, stack 0x6d30234cc0, flags 0x3d0f00, arg 0x6d30234cc0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/wasm/index, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/js/index, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/wasm/index, oflags 0xc1
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/js/index, oflags 0xc1
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/wasm/index-dir/the-real-index, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/js/index-dir/the-real-index, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/wasm/index-dir/temp-index, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ode Cache/js/index-dir/temp-index, oflags 0x241
pthread_create: thread 0x7fe513ed08, attr 0x7fe513ed40, start_routine 0x6ddf1e6b3c, arg
0x6f4f39e900
clone: fn 0x707076fd0c, stack 0x6d2f12dcc0, flags 0x3d0f00, arg 0x6d2f12dcc0
pthread_create: thread 0x7fe513e618, attr 0x7fe513e650, start_routine 0x6ddf1e6b3c, arg
0x6f4f399590
clone: fn 0x707076fd0c, stack 0x6d2dfeacc0, flags 0x3d0f00, arg 0x6d2dfeacc0
pthread_create: thread 0x7fe513e848, attr 0x7fe513e990, start_routine 0x6d83f30904, arg
0x6a0013d820
clone: fn 0x707076fd0c, stack 0x6d2dfcacc0, flags 0x3d0f00, arg 0x6d2dfcacc0
pthread_create: thread 0x7fe513e048, attr 0x7fe513e080, start_routine 0x6ddf1e6b3c, arg
0x6f4f39cd30
clone: fn 0x707076fd0c, stack 0x6d2dec3cc0, flags 0x3d0f00, arg 0x6d2dec3cc0
open: path /data/user/0/com.lift.filemanager.android/files/frc_1:565703110738:android:3
7ec4862ed1c78d044af8b_firebase_defaults.json, oflags 0x241
pthread_create: thread 0x6d6a6cc4c8, attr 0x6d6a6cc500, start_routine 0x6ddf1e6b3c, arg
0x6f4f3a04d0
clone: fn 0x707076fd0c, stack 0x6d2dd80cc0, flags 0x3d0f00, arg 0x6d2dd80cc0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
```

```
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3a20a0
clone: fn 0x707076fd0c, stack 0x6d2dc6dcc0, flags 0x3d0f00, arg 0x6d2dc6dcc0
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3a3c70
clone: fn 0x707076fd0c, stack 0x6d2db63cc0, flags 0x3d0f00, arg 0x6d2db63cc0
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3a7410
clone: fn 0x707076fd0c, stack 0x6d2da59cc0, flags 0x3d0f00, arg 0x6d2da59cc0
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3a8fe0
clone: fn 0x707076fd0c, stack 0x6d2d94fcc0, flags 0x3d0f00, arg 0x6d2d94fcc0
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3aabb0
clone: fn 0x707076fd0c, stack 0x6d2d833cc0, flags 0x3d0f00, arg 0x6d2d833cc0
pthread_create: thread 0x7fe513f678, attr 0x7fe513f6b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3ac780
clone: fn 0x707076fd0c, stack 0x6d2d729cc0, flags 0x3d0f00, arg 0x6d2d729cc0
pthread_create: thread 0x6d2db63448, attr 0x6d2db63480, start_routine 0x6ddf1e6b3c, arg
0x6f4f399590
open: path /data/app/~~gJRGEMcdzVg-RT9VfCj4AA==/com.lift.filemanager.android-viAUZmvMdg
Kc2Zy2M8FibQ==/lib/arm64/libobjectbox-jni.so, oflags 0x0
android_dlopen_ext: libPath /data/app/~~gJRGEMcdzVg-RT9VfCj4AA==/com.lift.filemanager.a
ndroid-viAUZmvMdgKc2Zy2M8FibQ==/lib/arm64/libobjectbox-jni.so, flags 0x2, info 0x7fe513
e700
clone: fn 0x707076fd0c, stack 0x6d2d5cbcc0, flags 0x3d0f00, arg 0x6d2d5cbcc0
open: path /data/data/com.lift.filemanager.android/files/objectbox/objectbox/lock.mdb,
oflags 0x80042
open: path /data/data/com.lift.filemanager.android/files/objectbox/objectbox/data.mdb,
oflags 0x42
open: path /data/data/com.lift.filemanager.android/files/objectbox/objectbox/data.mdb,
oflags 0x81001
open: path /data/data/com.lift.filemanager.android/files/objectbox/objectbox/lock.mdb,
oflags 0x80042
open: path /data/data/com.lift.filemanager.android/files/objectbox/objectbox/data.mdb,
oflags 0x42
open: path /data/data/com.lift.filemanager.android/files/objectbox/objectbox/data.mdb,
oflags 0x81001
pthread_create: thread 0x6d39c14758, attr 0x6d39c148a0, start_routine 0x6d83f30904, arg
0x6a0013d0a0
pthread_create: thread 0x7fe5143d18, attr 0x7fe5143e60, start_routine 0x6d83f30904, arg
0x6a0013eb20
clone: fn 0x707076fd0c, stack 0x6ce2ca4cc0, flags 0x3d0f00, arg 0x6ce2ca4cc0
clone: fn 0x707076fd0c, stack 0x6d2d045cc0, flags 0x3d0f00, arg 0x6d2d045cc0
pthread_create: thread 0x7fe5144dd8, attr 0x7fe5144de0, start_routine 0x707355dbf8, arg
0x6dff42da20
```

```
clone: fn 0x707076fd0c, stack 0x6ce0ba6cc0, flags 0x3d0f00, arg 0x6ce0ba6cc0
pthread_create: thread 0x7fe5144f40, attr 0x0, start_routine 0x706f43972c, arg 0x6def34
cd10
clone: fn 0x707076fd0c, stack 0x6ce0aa8cc0, flags 0x3d0f00, arg 0x6ce0aa8cc0
pthread_create: thread 0x6ce0ba6ab8, attr 0x0, start_routine 0x7071af09a0, arg 0x6def34
7190
clone: fn 0x707076fd0c, stack 0x6ce0aa8cc0, flags 0x3d0f00, arg 0x6ce0aa8cc0
open: path /data/vendor/gpu/esx_config_com.lift.filemanager.android.txt, oflags 0x0
open: path /data/vendor/gpu/esx_config.txt, oflags 0x0
open: path /data/misc/gpu/esx_config_com.lift.filemanager.android.txt, oflags 0x0
open: path /data/misc/gpu/esx_config.txt, oflags 0x0
pthread_create: thread 0x7fe51448a8, attr 0x7fe51448e0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3aff20
clone: fn 0x707076fd0c, stack 0x6ce0aa8cc0, flags 0x3d0f00, arg 0x6ce0aa8cc0
pthread_create: thread 0x6ce0aa83a8, attr 0x6ce0aa83e0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3ae350
clone: fn 0x707076fd0c, stack 0x6ce099ecc0, flags 0x3d0f00, arg 0x6ce099ecc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.lift.filemanager.
android_preferences.xml, oflags 0x0
pthread_create: thread 0x7fe51443c8, attr 0x7fe5144400, start_routine 0x6ddf1e6b3c, arg
0x6f4f3ae350
clone: fn 0x707076fd0c, stack 0x6cdffcdcc0, flags 0x3d0f00, arg 0x6cdffcdcc0
pthread_create: thread 0x6cdffcd3f8, attr 0x6cdffcd430, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b1af0
clone: fn 0x707076fd0c, stack 0x6cdfec3cc0, flags 0x3d0f00, arg 0x6cdfec3cc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/admob.xml, oflags 0x0
pthread_create: thread 0x7fe5143858, attr 0x7fe5143890, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b1af0
clone: fn 0x707076fd0c, stack 0x6cdfec3cc0, flags 0x3d0f00, arg 0x6cdfec3cc0
pthread_create: thread 0x6cdffcd488, attr 0x6cdffcd4c0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b5290
clone: fn 0x707076fd0c, stack 0x6cdfdb9cc0, flags 0x3d0f00, arg 0x6cdfdb9cc0
pthread_create: thread 0x7fe51442e8, attr 0x7fe5144320, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b8a30
clone: fn 0x707076fd0c, stack 0x6cdfcafcc0, flags 0x3d0f00, arg 0x6cdfcafcc0
open: path /data/user/0/com.google.android.gms/shared_prefs/admob_user_agent.xml, oflags
 0x0
pthread_create: thread 0x7fe5144368, attr 0x7fe51443a0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b8a30
clone: fn 0x707076fd0c, stack 0x6cdfcafcc0, flags 0x3d0f00, arg 0x6cdfcafcc0
pthread_create: thread 0x7fe5144768, attr 0x7fe51447a0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3ba600
clone: fn 0x707076fd0c, stack 0x6cdfcafcc0, flags 0x3d0f00, arg 0x6cdfcafcc0
pthread_create: thread 0x7fe5144898, attr 0x7fe51448d0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b6e60
clone: fn 0x707076fd0c, stack 0x6cdfba5cc0, flags 0x3d0f00, arg 0x6cdfba5cc0
pthread_create: thread 0x6cdffcd578, attr 0x6cdffcd5b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3bc1d0
clone: fn 0x707076fd0c, stack 0x6cd99aacc0, flags 0x3d0f00, arg 0x6cd99aacc0
pthread_create: thread 0x7fe5144898, attr 0x7fe51448d0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3bf970
clone: fn 0x707076fd0c, stack 0x6cd98a0cc0, flags 0x3d0f00, arg 0x6cd98a0cc0
pthread_create: thread 0x6cdffcd4f8, attr 0x6cdffcd530, start_routine 0x6ddf1e6b3c, arg
0x6f4f3bdda0
clone: fn 0x707076fd0c, stack 0x6cd6796cc0, flags 0x3d0f00, arg 0x6cd6796cc0
pthread_create: thread 0x6cdffcd3b8, attr 0x6cdffcd3f0, start_routine 0x6ddf1e6b3c, arg
```

```
0x6f4f3c3110
clone: fn=0x707076fd0c, stack=0x6cd568ccc0, flags=0x3d0f00, arg=0x6cd568ccc0
pthread_create: thread=0x6cd568c3b8, attr=0x6cd568c3f0, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3c1540
clone: fn=0x707076fd0c, stack=0x6cd4582cc0, flags=0x3d0f00, arg=0x6cd4582cc0
pthread_create: thread=0x7fe5142008, attr=0x7fe5142150, start_routine=0x6d83f30904, arg=
0x6a0012bca0
clone: fn=0x707076fd0c, stack=0x6cd4542cc0, flags=0x3d0f00, arg=0x6cd4542cc0
pthread_create: thread=0x6cd45428b8, attr=0x6cd4542a00, start_routine=0x6d83f30904, arg=
0x6a0012afe0
clone: fn=0x707076fd0c, stack=0x6cd4444cc0, flags=0x3d0f00, arg=0x6cd4444cc0
dlopen: filename=libGLESv2.so, flags=0x1
dlopen: filename=libEGL.so, flags=0x1
dlopen: filename=libEGL_adreno.so, flags=0x2
pthread_create: thread=0x7fe51449b8, attr=0x7fe51449f0, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3c8480
clone: fn=0x707076fd0c, stack=0x6cd42bdcc0, flags=0x3d0f00, arg=0x6cd42bdcc0
open: path=/data/user/0/com.lift.filemanager.android/files/frc_1:565703110738:android:3
7ec4862ed1c78d044af8b_firebase_defaults.json, oflags=0x241
android_dlopen_ext: libPath=/vendor/lib64/hw/gralloc.sdm845.so, flags=0x2, info=0x6cd45
3e048
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/vendor/gpu/esx_config_com.lift.filemanager.android.txt, oflags=0x0
open: path=/data/vendor/gpu/esx_config.txt, oflags=0x0
open: path=/data/misc/gpu/esx_config_com.lift.filemanager.android.txt, oflags=0x0
open: path=/data/misc/gpu/esx_config.txt, oflags=0x0
pthread_create: thread=0x7fe5144c58, attr=0x7fe5144c90, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3ca050
clone: fn=0x707076fd0c, stack=0x6cd40fccc0, flags=0x3d0f00, arg=0x6cd40fccc0
open: path=./adreno_config.txt, oflags=0x0
open: path=/data/vendor/gpu//adreno_config.txt, oflags=0x0
open: path=/data/misc/gpu//adreno_config.txt, oflags=0x0
pthread_create: thread=0x6ce0aa7b08, attr=0x6ce0aa7b40, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3cd7f0
clone: fn=0x707076fd0c, stack=0x6cd3ff2cc0, flags=0x3d0f00, arg=0x6cd3ff2cc0
open: path=./yamato_panel.txt, oflags=0x0
open: path=/data/vendor/gpu//yamato_panel.txt, oflags=0x0
open: path=/data/misc/gpu//yamato_panel.txt, oflags=0x0
open: path=/data/vendor/gpu/esx_config_com.lift.filemanager.android.txt, oflags=0x0
open: path=/data/vendor/gpu/esx_config.txt, oflags=0x0
open: path=/data/misc/gpu/esx_config_com.lift.filemanager.android.txt, oflags=0x0
```

```
open: path /data/misc/gpu/esx_config.txt, oflags 0x0
open: path /data/vendor/gpu/esx_config_com.lift.filemanager.android.txt, oflags 0x0
open: path /data/vendor/gpu/esx_config.txt, oflags 0x0
open: path /data/misc/gpu/esx_config_com.lift.filemanager.android.txt, oflags 0x0
open: path /data/misc/gpu/esx_config.txt, oflags 0x0
open: path /sys/devices/system/cpu/present, oflags 0x0
open: path /sys/devices/system/cpu/cpu0/cpu_capacity, oflags 0x0
open: path /sys/devices/system/cpu/cpu0/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/devices/system/cpu/cpu1/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/devices/system/cpu/cpu2/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/devices/system/cpu/cpu3/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/devices/system/cpu/cpu4/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/devices/system/cpu/cpu5/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/devices/system/cpu/cpu6/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/devices/system/cpu/cpu7/cpufreq/cpuinfo_max_freq, oflags 0x0
open: path /sys/class/kgsl/kgsl-3d0/gpu_model, oflags 0x0
dlopen: filename libGLESv2_adreno.so, flags 0x2
dlopen: filename libGLESv1_CM_adreno.so, flags 0x2
open: path /data/data/com.lift.filemanager.android/app_webview/Default/Cookies, oflags
0xa8042
open: path /data/data/com.lift.filemanager.android/app_webview/Default/Cookies, oflags
0x0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/index, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/index-dir/the-real-index, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/3804ac0efe04121c_0, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/3804ac0efe04121c_1, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/3804ac0efe04121c_s, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/LOCK, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/LOG, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/LOCK, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/LOCK, oflags 0x42
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/MANIFEST-000001, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e, oflags 0x0
open: path /data/user_de/0/com.lift.filemanager.android/code_cache/com.android.skia.sha
ders_cache, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/000001.dbtmp, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/CURRENT, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/MANIFEST-000001, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/MANIFEST-000001, oflags 0x401
```

```
open: path /data/user/0/com.lift.filemanager.android/app_webview/Default/Session Storag
e/000003.log, oflags 0x241
android_dlopen_ext: libPath /vendor/lib64/hw/android.hardware.graphics.mapper@2.0-impl-
qti-display.so, flags 0x1, info 0x6ce0ba5fc8
dlopen: filename libadreno_utils.so, flags 0x2
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/.com.google.Chrome.s
yx3nP, oflags 0xc2
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/.com.google.Chrome.s
yx3nP, oflags 0x242
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.lift.filemanager.
android_preferences.xml, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.google.android.gm
s.measurement.prefs.xml, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/app_webview/.com.google.Chrome.glO
OwN, oflags 0xc2
open: path /data/user/0/com.lift.filemanager.android/files/AppEventsLogger.persistedeve
nts, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/.com.google.firebase.crashly
tics.files.v2:com.lift.filemanager.android/open-sessions/64D0B857022700011AB6F3CB35D4C1
92/userlog.tmp, oflags 0x42
pthread_create: thread 0x6d3be6fbe8, attr 0x6d3be6fc20, start_routine 0x6ddf1e6b3c, arg
0x6f4f3cbc20
clone: fn 0x707076fd0c, stack 0x6cd3ae1cc0, flags 0x3d0f00, arg 0x6cd3ae1cc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/AwOriginVisitLoggerPr
efs.xml, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/.com.google.firebase.crashly
tics.files.v2:com.lift.filemanager.android/open-sessions/64D0B857022700011AB6F3CB35D4C1
92/userlog, oflags 0x42
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
pthread_create: thread 0x6d598c3368, attr 0x6d598c33a0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3cbc20
clone: fn 0x707076fd0c, stack 0x6cd3997cc0, flags 0x3d0f00, arg 0x6cd3997cc0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
```

```
ocal.db, oflags=0xa0042
open: path=/data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags=0xa0042
pthread_create: thread=0x6d38b0c3b8, attr=0x6d38b0c3f0, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3cbc20
clone: fn=0x707076fd0c, stack=0x6cd3957cc0, flags=0x3d0f00, arg=0x6cd3957cc0
open: path=/data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fbf7ad96532b1f6f_0, oflags=0x2
open: path=/data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fbf7ad96532b1f6f_1, oflags=0x2
open: path=/data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fbf7ad96532b1f6f_s, oflags=0x2
open: path=/data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags=0xa0042
pthread_create: thread=0x7fe5144238, attr=0x7fe5144270, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3d6300
clone: fn=0x707076fd0c, stack=0x6cd37edcc0, flags=0x3d0f00, arg=0x6cd37edcc0
pthread_create: thread=0x6d2f12d308, attr=0x6d2f12d340, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3d7ed0
clone: fn=0x707076fd0c, stack=0x6cd36e3cc0, flags=0x3d0f00, arg=0x6cd36e3cc0
open: path=/data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/47dd006ca3dbb334_0, oflags=0xc2
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
open: path=/data/misc/keychain/pubkey_blacklist.txt, oflags=0x0
open: path=/data/misc/keychain/serial_blacklist.txt, oflags=0x0
open: path=/system/etc/security/cacerts/f013ecaf.0, oflags=0x0
open: path=/system/etc/security/cacerts/f013ecaf.0, oflags=0x0
pthread_create: thread=0x7fe5144f08, attr=0x7fe5144f40, start_routine=0x6ddf1e6b3c, arg=
0x6f4f3d2b60
clone: fn=0x707076fd0c, stack=0x6cd35a0cc0, flags=0x3d0f00, arg=0x6cd35a0cc0
pthread_create: thread=0x6dcb829768, attr=0x6dcb829770, start_routine=0x707355dbf8, arg=
0x6dff40a9b0
clone: fn=0x707076fd0c, stack=0x6d435c7cc0, flags=0x3d0f00, arg=0x6d435c7cc0
open: path=/data/user/0/com.lift.filemanager.android/app_webview/BrowserMetrics-spare.p
ma.tmp, oflags=0x242
open: path=/data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags=0xa0042
open: path=/data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags=0x4
2
open: path=/data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags=0x0
```

```
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/app_webview/.com.google.Chrome.XGS
wvA, oflags 0xc2
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
pthread_create: thread 0x6ce0ba6ab8, attr 0x0, start_routine 0x7071af09a0, arg 0x6def33
c0b0
clone: fn 0x707076fd0c, stack 0x6dcf04bcc0, flags 0x3d0f00, arg 0x6dcf04bcc0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
pthread_create: thread 0x7fe5143638, attr 0x7fe5143670, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b6e60
clone: fn 0x707076fd0c, stack 0x6dcee9fcc0, flags 0x3d0f00, arg 0x6dcee9fcc0
pthread_create: thread 0x6cdfdb9428, attr 0x6cdfdb9460, start_routine 0x6ddf1e6b3c, arg
0x6f4f33ef50
clone: fn 0x707076fd0c, stack 0x6dcdd95cc0, flags 0x3d0f00, arg 0x6dcdd95cc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/pcvmspf.xml, oflags 0
x0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.lift.filemanager.
android_preferences.xml, oflags 0x241
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/com.google.android.gm
s.measurement.prefs.xml, oflags 0x241
pthread_create: thread 0x6cdfdb9438, attr 0x6cdfdb9470, start_routine 0x6ddf1e6b3c, arg
0x6f4f3ca050
clone: fn 0x707076fd0c, stack 0x6dcdd95cc0, flags 0x3d0f00, arg 0x6dcdd95cc0
pthread_create: thread 0x6dcdd955c8, attr 0x6dcdd95600, start_routine 0x6ddf1e6b3c, arg
0x6f4f3bf970
clone: fn 0x707076fd0c, stack 0x6dccc8bcc0, flags 0x3d0f00, arg 0x6dccc8bcc0
pthread_create: thread 0x6cdfdb9278, attr 0x6cdfdb92b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3bc1d0
clone: fn 0x707076fd0c, stack 0x6dccb81cc0, flags 0x3d0f00, arg 0x6dccb81cc0
pthread_create: thread 0x7fe5143418, attr 0x7fe5143450, start_routine 0x6ddf1e6b3c, arg
0x6f4f33ef50
clone: fn 0x707076fd0c, stack 0x6dcca77cc0, flags 0x3d0f00, arg 0x6dcca77cc0
pthread_create: thread 0x6cdfdb9278, attr 0x6cdfdb92b0, start_routine 0x6ddf1e6b3c, arg
```

```
0x6f4f33b7b0
clone: fn 0x707076fd0c, stack 0x6dcc96dcc0, flags 0x3d0f00, arg 0x6dcc96dcc0
open: path /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7BC3562A445BE6E17C
D85D775DF427D4C01AD8/pcam.jar, oflags 0x0
pthread_create: thread 0x7fe5143318, attr 0x7fe5143350, start_routine 0x6ddf1e6b3c, arg
0x6f4f3b8a30
clone: fn 0x707076fd0c, stack 0x6dcc7cccc0, flags 0x3d0f00, arg 0x6dcc7cccc0
pthread_create: thread 0x7fe5143318, attr 0x7fe5143350, start_routine 0x6ddf1e6b3c, arg
0x6f4f340b20
open: path /proc/7411/timerslack_ns, oflags 0x88241
open: path /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7BC3562A445BE6E17C
D85D775DF427D4C01AD8/pcam.jar, oflags 0x0
clone: fn 0x707076fd0c, stack 0x6dcc6c2cc0, flags 0x3d0f00, arg 0x6dcc6c2cc0
pthread_create: thread 0x7fe5143318, attr 0x7fe5143350, start_routine 0x6ddf1e6b3c, arg
0x6f4f338010
clone: fn 0x707076fd0c, stack 0x6dcc5afcc0, flags 0x3d0f00, arg 0x6dcc5afcc0
open: path /proc/7412/timerslack_ns, oflags 0x88241
pthread_create: thread 0x7fe5143318, attr 0x7fe5143350, start_routine 0x6ddf1e6b3c, arg
0x6f4f3863a0
open: path /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7BC3562A445BE6E17C
D85D775DF427D4C01AD8/pcam.jar, oflags 0x0
open: path /proc/7413/timerslack_ns, oflags 0x88241
clone: fn 0x707076fd0c, stack 0x6dcc46ccc0, flags 0x3d0f00, arg 0x6dcc46ccc0
pthread_create: thread 0x7fe5143318, attr 0x7fe5143350, start_routine 0x6ddf1e6b3c, arg
0x6f4f37d890
open: path /data/user/0/com.lift.filemanager.android/cache/volley/-1207530946-547165462
, oflags 0x0
clone: fn 0x707076fd0c, stack 0x6d5aac4cc0, flags 0x3d0f00, arg 0x6d5aac4cc0
open: path /proc/7415/timerslack_ns, oflags 0x88241
open: path /proc/7414/timerslack_ns, oflags 0x88241
pthread_create: thread 0x7fe5143728, attr 0x7fe5143760, start_routine 0x6ddf1e6b3c, arg
0x6f4f3dd240
open: path /data/user/0/com.lift.filemanager.android/cache/volley/715414548-394311354,
oflags 0x0
clone: fn 0x707076fd0c, stack 0x6d587bacc0, flags 0x3d0f00, arg 0x6d587bacc0
open: path /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7BC3562A445BE6E17C
D85D775DF427D4C01AD8/oat/pcam.jar.cur.prof, oflags 0xc2
open: path /data/user/0/com.lift.filemanager.android/cache/volley/-1727183717-967741021
, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7BC3562A445BE6E17C
D85D775DF427D4C01AD8/pcbc, oflags 0x0
pthread_create: thread 0x7fe5143668, attr 0x7fe51436a0, start_routine 0x6ddf1e6b3c, arg
0x6f4f387f70
clone: fn 0x707076fd0c, stack 0x6d556b0cc0, flags 0x3d0f00, arg 0x6d556b0cc0
pthread_create: thread 0x7fe5143668, attr 0x7fe51436a0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3d2b60
clone: fn 0x707076fd0c, stack 0x6d431a4cc0, flags 0x3d0f00, arg 0x6d431a4cc0
pthread_create: thread 0x7fe5143608, attr 0x7fe5143640, start_routine 0x6ddf1e6b3c, arg
0x6f4f3dee10
clone: fn 0x707076fd0c, stack 0x6cd99aacc0, flags 0x3d0f00, arg 0x6cd99aacc0
open: path /data/app/~~gJRGEMcdzVg-RT9VfCj4AA==/com.lift.filemanager.android-viAUZmvMdg
Kc2Zy2M8FibQ==/base.apk, oflags 0x80000
pthread_create: thread 0x7fe5143668, attr 0x7fe51436a0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3db670
clone: fn 0x707076fd0c, stack 0x6cd98a0cc0, flags 0x3d0f00, arg 0x6cd98a0cc0
open: path /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7BC3562A445BE6E17C
```

```
D85D775DF427D4C01AD8/pcam.jar, oflags 0x80000
pthread_create: thread 0x7fe51436a8, attr 0x7fe51436e0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3e25b0
clone: fn 0x707076fd0c, stack 0x6cd40fccc0, flags 0x3d0f00, arg 0x6cd40fccc0
pthread_create: thread 0x6cd98a02b8, attr 0x6cd98a02f0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3e5d50
clone: fn 0x707076fd0c, stack 0x6cc4000cc0, flags 0x3d0f00, arg 0x6cc4000cc0
pthread_create: thread 0x6cd40fc348, attr 0x6cd40fc380, start_routine 0x6ddf1e6b3c, arg
0x6f4f3e09e0
clone: fn 0x707076fd0c, stack 0x6cc2ef6cc0, flags 0x3d0f00, arg 0x6cc2ef6cc0
pthread_create: thread 0x7fe5143668, attr 0x7fe51436a0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3e4180
clone: fn 0x707076fd0c, stack 0x6cc1deccc0, flags 0x3d0f00, arg 0x6cc1deccc0
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/paid_storage_sp.xml,
oflags 0x0
pthread_create: thread 0x7fe51435d8, attr 0x7fe5143610, start_routine 0x6ddf1e6b3c, arg
0x6f4f3eb0c0
clone: fn 0x707076fd0c, stack 0x6cc0ce2cc0, flags 0x3d0f00, arg 0x6cc0ce2cc0
android_dlopen_ext: libPath /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7
BC3562A445BE6E17CD85D775DF427D4C01AD8/pcam.jar /libd36668F50D9B1.so, flags 0x2, info 0x
6cdfdb8030
pthread_create: thread 0x7fe5143738, attr 0x7fe5143770, start_routine 0x6ddf1e6b3c, arg
0x6f4f3e7920
clone: fn 0x707076fd0c, stack 0x6cc0bd8cc0, flags 0x3d0f00, arg 0x6cc0bd8cc0
pthread_create: thread 0x6cc0ce2418, attr 0x6cc0ce2450, start_routine 0x6ddf1e6b3c, arg
0x6f4f3ecc90
clone: fn 0x707076fd0c, stack 0x6cbfacecc0, flags 0x3d0f00, arg 0x6cbfacecc0
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fb0a44f3e240ce58_0, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fb0a44f3e240ce58_1, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fb0a44f3e240ce58_s, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/shared_prefs/admob.xml, oflags 0x2
41
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fbf7ad96532b1f6f_0, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fbf7ad96532b1f6f_1, oflags 0x2
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/fbf7ad96532b1f6f_s, oflags 0x2
open: path /proc/self/cmdline, oflags 0x80000
open: path /proc/self/cmdline, oflags 0x80000
open: path /proc/self/cmdline, oflags 0x80000
pthread_create: thread 0x6cc0ce1ec8, attr 0x6cc0ce1f00, start_routine 0x6ddf1e6b3c, arg
0x6f4f3ee860
clone: fn 0x707076fd0c, stack 0x6d81d3dcc0, flags 0x3d0f00, arg 0x6d81d3dcc0
pthread_create: thread 0x6cc1dec478, attr 0x6cc1dec4b0, start_routine 0x6ddf1e6b3c, arg
0x6f4f3f2000
clone: fn 0x707076fd0c, stack 0x6d81c33cc0, flags 0x3d0f00, arg 0x6d81c33cc0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
```

```
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
pthread_create: thread 0x7fe5143408, attr 0x7fe5143440, start_routine 0x6ddf1e6b3c, arg
0x6f4f3f3bd0
clone: fn 0x707076fd0c, stack 0x6d81929cc0, flags 0x3d0f00, arg 0x6d81929cc0
pthread_create: thread 0x6d556b0348, attr 0x6d556b0380, start_routine 0x6ddf1e6b3c, arg
0x6f4f3f0430
pthread_create: thread 0x7fe5143328, attr 0x7fe5143360, start_routine 0x6ddf1e6b3c, arg
0x6f4f3f57a0
clone: fn 0x707076fd0c, stack 0x6d8181fcc0, flags 0x3d0f00, arg 0x6d8181fcc0
clone: fn 0x707076fd0c, stack 0x6d81715cc0, flags 0x3d0f00, arg 0x6d81715cc0
pthread_create: thread 0x7fe51432c8, attr 0x7fe5143300, start_routine 0x6ddf1e6b3c, arg
0x6f4f3f7370
clone: fn 0x707076fd0c, stack 0x6d81b29cc0, flags 0x3d0f00, arg 0x6d81b29cc0
pthread_create: thread 0x6cd99aa418, attr 0x6cd99aa450, start_routine 0x6ddf1e6b3c, arg
0x6f4f3fc6e0
clone: fn 0x707076fd0c, stack 0x6d8160bcc0, flags 0x3d0f00, arg 0x6d8160bcc0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
pthread_create: thread 0x6d8181f418, attr 0x6d8181f450, start_routine 0x6ddf1e6b3c, arg
0x6f4f3f8f40
clone: fn 0x707076fd0c, stack 0x6d81501cc0, flags 0x3d0f00, arg 0x6d81501cc0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
pthread_create: thread 0x6cd99aa418, attr 0x6cd99aa450, start_routine 0x6ddf1e6b3c, arg
0x6f4f403620
clone: fn 0x707076fd0c, stack 0x6d813f7cc0, flags 0x3d0f00, arg 0x6d813f7cc0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
```

```
ocal.db, oflags 0xa0042
pthread_create: thread 0x6cdffcd418, attr=0x6cdffcd450, start_routine 0x6ddf1e6b3c, arg=
0x6f4f3fe2b0
clone: fn 0x707076fd0c, stack 0x6d810edcc0, flags=0x3d0f00, arg 0x6d810edcc0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
pthread_create: thread 0x6d435c7768, attr=0x6d435c7770, start_routine 0x707355dbf8, arg=
0x6dff43b5e0
clone: fn 0x707076fd0c, stack 0x6d812edcc0, flags=0x3d0f00, arg 0x6d812edcc0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
```

```
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/files/generatefid.lock, oflags 0x4
2
open: path /data/user/0/com.lift.filemanager.android/files/PersistedInstallation.W0RFRk
FVTFRd+MTo1NjU3MDMxMTA3Mzg6YW5kcm9pZDozN2VjNDg2MmVkMWM3OGQwNDRhZjhi.json, oflags 0x0
open: path /data/user/0/com.lift.filemanager.android/databases/google_app_measurement_l
ocal.db, oflags 0xa0042
open: path /data/user/0/com.lift.filemanager.android/app_webview/.com.google.Chrome.AIY
A7r, oflags 0xc2
open: path /dev/urandom, oflags 0x80000
open: path /data/user/0/com.lift.filemanager.android/cache/WebView/Default/HTTP Cache/C
ache_Data/index-dir/temp-index, oflags 0x241
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]-> pthread_create: thread 0x6dcb829768, attr 0x
6dcb829770, start_routine 0x707355dbf8, arg 0x6dff411640
clone: fn 0x707076fd0c, stack 0x6d81b29cc0, flags 0x3d0f00, arg 0x6d81b29cc0
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]-> open: path /data/misc/profiles/cur/0/com.lif
t.filemanager.android/primary.prof, oflags 0x88002
open: path /data/user/0/com.lift.filemanager.android/app_pccache/5/AC7BC3562A445BE6E17C
D85D775DF427D4C01AD8/oat/pcam.jar.cur.prof, oflags 0x88002
[Pixel 3::com.lift.filemanager.android ]->
[Pixel 3::com.lift.filemanager.android ]-> open: path /data/user/0/com.lift.filemanager
.android/files/AppEventsLogger.persistedevents, oflags 0x0
```

DisplayDemo

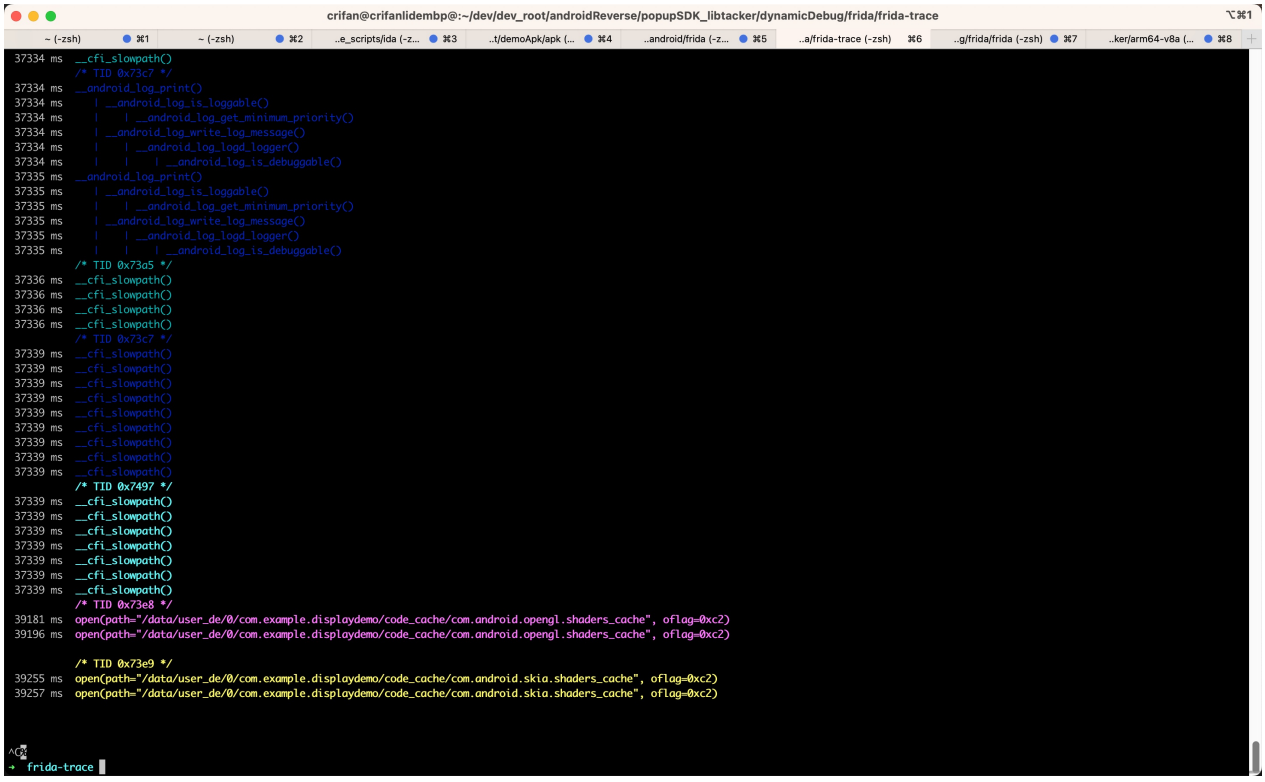
用 `frida-trace` 调试安卓app： `com.example.displaydemo`

命令

```
frida-trace -U -f com.example.displaydemo -I libdl.so -I liblog.so -I libtacker.so -i open -i openat -i dlopen
```

输出

截图



log日志

```
frida-trace -U -f com.example.displaydemo -I libdl.so -I liblog.so -I libtacker.so -i open -i openat -i dlopen

...

__android_log_buf_write: Loaded handler at "/Users/crifan/dev/dev_root/androidReverse/popupSDK_libtacker/dynamicDebug/frida/frida-trace/__handlers__/liblog.so/__android_log_buf_write.js"
__android_log_is_debuggable: Loaded handler at "/Users/crifan/dev/dev_root/androidReverse/popupSDK_libtacker/dynamicDebug/frida/frida-trace/__handlers__/liblog.so/__android_l
```

```
og_is_debuggable.js"
android_openEventTagMap: Loaded handler at "/Users/crifan/dev/dev_root/androidReverse/p
opupSDK_libtacker/dynamicDebug/frida/frida-trace/__handlers__/liblog.so/android_openEve
ntTagMap.js"
open: Loaded handler at "/Users/crifan/dev/dev_root/androidReverse/popupSDK_libtacker/d
ynamicDebug/frida/frida-trace/__handlers__/libc.so/open.js"
openat: Loaded handler at "/Users/crifan/dev/dev_root/androidReverse/popupSDK_libtacker
/dynamicDebug/frida/frida-trace/__handlers__/libc.so/openat.js"
Started tracing 82 functions. Press Ctrl+C to stop.
           /* TID 0x73a5 */
   628 ms  dlsym(handle 0x28d2598c92f4b5bd, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   641 ms  dlsym(handle 0x28d2598c92f4b5bd, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   642 ms  dlsym(handle 0x18091f93b592f005, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   642 ms  dlsym(handle 0x18091f93b592f005, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   642 ms  dlsym(handle 0xf61d9d184f5bd255, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   642 ms  dlsym(handle 0xf61d9d184f5bd255, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   642 ms  dlsym(handle 0xf93963b9819f875f, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   642 ms  dlsym(handle 0xf93963b9819f875f, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   642 ms  dlsym(handle 0xb6965c803b1ea0bf, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   642 ms  dlsym(handle 0xb6965c803b1ea0bf, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   642 ms  dlsym(handle 0xf33483d7107b39b5, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   642 ms  dlsym(handle 0xf33483d7107b39b5, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   642 ms  dlsym(handle 0x49a6c69ccf1943e5, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   642 ms  dlsym(handle 0x49a6c69ccf1943e5, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   643 ms  dlsym(handle 0x12b477e61386e20d, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   643 ms  dlsym(handle 0x12b477e61386e20d, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0__JI")
   643 ms  dlsym(handle 0x3cb81b9cf29f00eb, symbol="Java_sun_nio_fs_UnixNativeDispatche
r_access0")
   646 ms  __android_log_buf_write()
   646 ms      __android_log_is_loggable()
   646 ms          __android_log_get_minimum_priority()
   646 ms      __android_log_write_log_message()
   646 ms          __android_log_logd_logger()
   646 ms              __android_log_is_debuggable()
   647 ms  __android_log_buf_write()
   647 ms      __android_log_is_loggable()
   647 ms          __android_log_get_minimum_priority()
   647 ms      __android_log_write_log_message()
   647 ms          __android_log_logd_logger()
   647 ms              __android_log_is_debuggable()
```

```
⋮
1 ms                    __android_log_is_debuggable()
  651 ms  open(path "/data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8
U1Y8uB9h_Modc1C__Q==/base.apk", oflag 0x80000)
  657 ms  __android_log_buf_write()
⋮
  676 ms  open(path "/proc/self/cmdline", oflag 0x80000)
  679 ms  dl_iterate_phdr()
  679 ms  android_dlopen_ext()
  681 ms  dlsym(handle 0x6c3b15dbd25a16d1, symbol "oatdata")
  681 ms  dlsym(handle 0x6c3b15dbd25a16d1, symbol "oatlastword")
  681 ms  dlsym(handle 0x6c3b15dbd25a16d1, symbol "oatdatabimgrelro")
  681 ms  dlerror()
  681 ms  dlsym(handle 0x6c3b15dbd25a16d1, symbol "oatbss")
  681 ms  dlerror()
  681 ms  dlsym(handle 0x6c3b15dbd25a16d1, symbol "oatdex")
  681 ms  dlsym(handle 0x6c3b15dbd25a16d1, symbol "oatdexlastword")
  681 ms  dl_iterate_phdr()
  681 ms  open(path "/data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8
U1Y8uB9h_Modc1C__Q==/oat/arm64/base.vdex", oflag 0x0)
  683 ms  open(path "/data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8
U1Y8uB9h_Modc1C__Q==/base.apk", oflag 0x0)
  684 ms  open(path "/apex/com.android.art/javalib/arm64/boot.art", oflag 0x0)
  684 ms  open(path "/system/framework/arm64/boot-framework.art", oflag 0x0)
  684 ms  open(path "/data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8
U1Y8uB9h_Modc1C__Q==/oat/arm64/base.art", oflag 0x0)
  702 ms  __android_log_buf_write()
  702 ms    __android_log_is_loggable()
  702 ms      __android_log_get_minimum_priority()
  702 ms    __android_log_write_log_message()
  702 ms      __android_log_logd_logger()
  702 ms        __android_log_is_debuggable()
  703 ms  __android_log_buf_write()
  703 ms    __android_log_is_loggable()
  703 ms      __android_log_get_minimum_priority()
  703 ms    __android_log_write_log_message()
  703 ms      __android_log_logd_logger()
  703 ms        __android_log_is_debuggable()
  704 ms  open(path "/data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8
U1Y8uB9h_Modc1C__Q==/base.apk", oflag 0x80000)
  705 ms  open(path "/product/overlay/NavigationBarMode2Button/NavigationBarMode2Butto
nOverlay.apk", oflag 0x80000)
  712 ms  __android_log_buf_write()
  712 ms    __android_log_is_loggable()
  712 ms      __android_log_get_minimum_priority()
  712 ms    __android_log_write_log_message()
  712 ms      __android_log_logd_logger()
  712 ms        __android_log_is_debuggable()
  713 ms  __android_log_buf_write()
  713 ms    __android_log_is_loggable()
  713 ms      __android_log_get_minimum_priority()
  713 ms    __android_log_write_log_message()
  713 ms      __android_log_logd_logger()
  713 ms        __android_log_is_debuggable()
  718 ms  __android_log_is_loggable()
  718 ms    __android_log_get_minimum_priority()
```

```
            /* TID 0x73cb */
   739 ms  dlsym(handle 0x8473cc9900a85ecd, symbol="InitEsxProfile")
   739 ms  open(path "/data/vendor/gpu/esx_config_com.example.displaydemo.txt", oflag 0
x0)
   739 ms  open(path "/data/vendor/gpu/esx_config.txt", oflag 0x0)
   739 ms  open(path "/data/misc/gpu/esx_config_com.example.displaydemo.txt", oflag 0x0)

   739 ms  open(path "/data/misc/gpu/esx_config.txt", oflag 0x0)
            /* TID 0x73a5 */
   752 ms  __android_log_buf_write()
   753 ms      __android_log_is_loggable()
   753 ms          __android_log_get_minimum_priority()
   753 ms      __android_log_write_log_message()
   753 ms          __android_log_logd_logger()
   753 ms              __android_log_is_debuggable()
   769 ms  __cfi_slowpath()
   769 ms  __cfi_slowpath()
   783 ms  __cfi_slowpath()
. . .
   964 ms  dladdr(addr 0x6dc20f4b08, info 0x6d6dbfc760)
   964 ms  __android_log_print()
   964 ms      __android_log_is_loggable()
   964 ms          __android_log_get_minimum_priority()
   964 ms      __android_log_write_log_message()
   964 ms          __android_log_logd_logger()
   964 ms              __android_log_is_debuggable()
   965 ms  android_dlopen_ext()
   965 ms  dlsym(handle 0xf4f687c6329daa95, symbol="HMI")
   966 ms  open(path "/data/vendor/gpu/esx_config_com.example.displaydemo.txt", oflag 0
x0)
   966 ms  open(path "/data/vendor/gpu/esx_config.txt", oflag 0x0)
   966 ms  open(path "/data/misc/gpu/esx_config_com.example.displaydemo.txt", oflag 0x0)

   966 ms  open(path "/data/misc/gpu/esx_config.txt", oflag 0x0)
   966 ms  open(path "./adreno_config.txt", oflag 0x0)
   966 ms  open(path "/data/vendor/gpu//adreno_config.txt", oflag 0x0)
   966 ms  open(path "/data/misc/gpu//adreno_config.txt", oflag 0x0)
   966 ms  open(path "./yamato_panel.txt", oflag 0x0)
   966 ms  open(path "/data/vendor/gpu//yamato_panel.txt", oflag 0x0)
   966 ms  open(path "/data/misc/gpu//yamato_panel.txt", oflag 0x0)
   966 ms  open(path "/data/vendor/gpu/esx_config_com.example.displaydemo.txt", oflag 0
x0)
   966 ms  open(path "/data/vendor/gpu/esx_config.txt", oflag 0x0)
   966 ms  open(path "/data/misc/gpu/esx_config_com.example.displaydemo.txt", oflag 0x0)

   967 ms  open(path "/data/misc/gpu/esx_config.txt", oflag 0x0)
   967 ms  __android_log_print()
   967 ms      __android_log_is_loggable()
   967 ms          __android_log_get_minimum_priority()
   967 ms      __android_log_write_log_message()
   967 ms          __android_log_logd_logger()
   967 ms              __android_log_is_debuggable()
   967 ms  open(path "/data/vendor/gpu/esx_config_com.example.displaydemo.txt", oflag 0
x0)
   967 ms  open(path "/data/vendor/gpu/esx_config.txt", oflag 0x0)
   967 ms  open(path "/data/misc/gpu/esx_config_com.example.displaydemo.txt", oflag 0x0)
```

```
967 ms  open(path "/data/misc/gpu/esx_config.txt", oflag 0x0)
968 ms  open(path "/sys/devices/system/cpu/present", oflag 0x0)
968 ms  open(path "/sys/devices/system/cpu/cpu0/cpu_capacity", oflag 0x0)
968 ms  open(path "/sys/devices/system/cpu/cpu0/cpufreq/cpuinfo_max_freq", oflag 0x0)

968 ms  open(path "/sys/devices/system/cpu/cpu1/cpufreq/cpuinfo_max_freq", oflag 0x0)

968 ms  open(path "/sys/devices/system/cpu/cpu2/cpufreq/cpuinfo_max_freq", oflag 0x0)

968 ms  open(path "/sys/devices/system/cpu/cpu3/cpufreq/cpuinfo_max_freq", oflag 0x0)

968 ms  open(path "/sys/devices/system/cpu/cpu4/cpufreq/cpuinfo_max_freq", oflag 0x0)

968 ms  open(path "/sys/devices/system/cpu/cpu5/cpufreq/cpuinfo_max_freq", oflag 0x0)

968 ms  open(path "/sys/devices/system/cpu/cpu6/cpufreq/cpuinfo_max_freq", oflag 0x0)

968 ms  open(path "/sys/devices/system/cpu/cpu7/cpufreq/cpuinfo_max_freq", oflag 0x0)

969 ms  open(path "/sys/class/kgsl/kgsl-3d0/gpu_model", oflag 0x0)
969 ms  __android_log_print()
969 ms      __android_log_is_loggable()
969 ms          __android_log_get_minimum_priority()
969 ms      __android_log_write_log_message()
969 ms          __android_log_logd_logger()
969 ms              __android_log_is_debuggable()
969 ms  __android_log_print()
969 ms      __android_log_is_loggable()
969 ms          __android_log_get_minimum_priority()
969 ms      __android_log_write_log_message()
969 ms          __android_log_logd_logger()
969 ms              __android_log_is_debuggable()
969 ms  dlopen(path "libEGL_adreno.so", mode 0x2)
970 ms  dlsym(handle 0xf9e57fda79bd3c09, symbol "eglSetBlobCacheFuncsANDROID")
971 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glGetStringi")
971 ms  dlsym(handle 0x231259e63d1aef61, symbol "glGetStringi")
971 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glGetStringi")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glGetStringi")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glMemoryBarrier")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glMemoryBarrier")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glBindVertexArray")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glBindVertexArray")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glDeleteVertexArrays")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glDeleteVertexArrays")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glGenVertexArrays")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glGenVertexArrays")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glPatchParameteri")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glPatchParameteri")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glBindFragDataLocationEXT")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glBindFragDataLocationEXT")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glBindFragDataLocationIndexedEXT")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glBindFragDataLocationIndexedEXT")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glBlendBarrierKHR")
972 ms  dlsym(handle 0x231259e63d1aef61, symbol "glBlendBarrierKHR")
972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol "glDrawArraysInstanced")
```

```
    972 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDrawArraysInstanced")
    972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDrawElementsInstanced")
    972 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDrawElementsInstanced")
    972 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDrawBuffers")
    972 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDrawBuffers")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glReadBuffer")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glReadBuffer")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDrawArraysIndirect")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDrawArraysIndirect")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDrawElementsIndirect")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDrawElementsIndirect")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDrawRangeElements")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDrawRangeElements")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetMultisamplefv")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetMultisamplefv")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetTexLevelParameteriv")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetTexLevelParameteriv")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glTexBuffer")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glTexBuffer")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glTexBufferRange")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glTexBufferRange")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glTexStorage2D")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glTexStorage2D")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDiscardFramebufferEXT")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDiscardFramebufferEXT")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glEndTilingQCOM")
    973 ms  dlsym(handle 0x231259e63d1aef61, symbol="glEndTilingQCOM")
    973 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glStartTilingQCOM")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glStartTilingQCOM")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glVertexAttribDivisor")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glVertexAttribDivisor")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glVertexAttribIPointer")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glVertexAttribIPointer")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glBlitFramebuffer")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glBlitFramebuffer")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glRenderbufferStorageMultisample")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glRenderbufferStorageMultisample")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glFramebufferTexture2DMultisampleEX
T")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glFramebufferTexture2DMultisampleEX
T")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glRenderbufferStorageMultisampleEXT"
)
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glRenderbufferStorageMultisampleEXT"
)
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glUnmapBuffer")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glUnmapBuffer")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glFlushMappedBufferRange")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glFlushMappedBufferRange")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glMapBufferRange")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glMapBufferRange")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glInsertEventMarkerEXT")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glInsertEventMarkerEXT")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glPopGroupMarkerEXT")
    974 ms  dlsym(handle 0x231259e63d1aef61, symbol="glPopGroupMarkerEXT")
    974 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glPushGroupMarkerEXT")
```

```
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glPushGroupMarkerEXT")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetProgramResourceLocation")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetProgramResourceLocation")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDebugMessageCallbackKHR")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDebugMessageCallbackKHR")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDebugMessageControlKHR")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDebugMessageControlKHR")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDebugMessageInsertKHR")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDebugMessageInsertKHR")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetDebugMessageLogKHR")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetDebugMessageLogKHR")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glObjectLabelKHR")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glObjectLabelKHR")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glPopDebugGroupKHR")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glPopDebugGroupKHR")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glPushDebugGroupKHR")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glPushDebugGroupKHR")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glClientWaitSync")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glClientWaitSync")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDeleteSync")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDeleteSync")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glFenceSync")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glFenceSync")
975 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glIsSync")
975 ms  dlsym(handle 0x231259e63d1aef61, symbol="glIsSync")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glWaitSync")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glWaitSync")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetInternalformativ")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetInternalformativ")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetProgramBinary")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetProgramBinary")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glProgramBinary")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glProgramBinary")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glProgramParameteri")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glProgramParameteri")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glBindSampler")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glBindSampler")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDeleteSamplers")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDeleteSamplers")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGenSamplers")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGenSamplers")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glSamplerParameteri")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glSamplerParameteri")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glSamplerParameteriv")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glSamplerParameteriv")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glBeginQuery")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glBeginQuery")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glDeleteQueries")
976 ms  dlsym(handle 0x231259e63d1aef61, symbol="glDeleteQueries")
976 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glEndQuery")
977 ms  dlsym(handle 0x231259e63d1aef61, symbol="glEndQuery")
977 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGenQueries")
977 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGenQueries")
977 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetQueryObjectuiv")
977 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetQueryObjectuiv")
977 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glGetQueryiv")
```

```
   977 ms  dlsym(handle 0x231259e63d1aef61, symbol="glGetQueryiv")
   977 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glInvalidateFramebuffer")
   977 ms  dlsym(handle 0x231259e63d1aef61, symbol="glInvalidateFramebuffer")
   977 ms  dlsym(handle 0x5dae32eb4dcc0329, symbol="glInvalidateSubFramebuffer")
   977 ms  dlsym(handle 0x231259e63d1aef61, symbol="glInvalidateSubFramebuffer")
   977 ms  open(path "/data/user_de/0/com.example.displaydemo/code_cache/com.android.sk
ia.shaders_cache", oflag 0x0)
   990 ms  __android_log_print()
   990 ms      __android_log_is_loggable()
   990 ms          __android_log_get_minimum_priority()
   990 ms      __android_log_write_log_message()
   990 ms          __android_log_logd_logger()
   990 ms              __android_log_is_debuggable()
   990 ms  __android_log_print()
   990 ms      __android_log_is_loggable()
   990 ms          __android_log_get_minimum_priority()
   990 ms      __android_log_write_log_message()
   990 ms          __android_log_logd_logger()
   990 ms              __android_log_is_debuggable()
   990 ms  dlerror()
   990 ms  android_dlopen_ext()
   991 ms  dlsym(handle 0x32a24e38d5386b55, symbol="HIDL_FETCH_IMapper")
   991 ms  __android_log_is_loggable()
   991 ms      __android_log_get_minimum_priority()
   991 ms  dlopen(path "libadreno_utils.so", mode 0x2)
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="compute_aligned_width_and_height")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="compute_fmt_aligned_width_and_heigh
t")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="compute_surface_padding")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="compute_compressedfmt_aligned_width
_and_height")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="isUBWCSupportedByGpu")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="get_gpu_pixel_alignment")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="adreno_get_metadata_blob_size")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="adreno_init_memory_layout")
   992 ms  dlsym(handle 0xf1188f74383613ef, symbol="adreno_get_aligned_gpu_buffer_size")

   992 ms  __cfi_slowpath()
           /* TID 0x73cc */
  1406 ms  __cfi_slowpath()
  1407 ms  __cfi_slowpath()
  1407 ms  __cfi_slowpath()
  1407 ms  __cfi_slowpath()
  1407 ms  __cfi_slowpath()

...

           /* TID 0x73a5 */
 35028 ms  __cfi_slowpath()
 35028 ms  __cfi_slowpath()
 35035 ms  __android_log_buf_write()
 35036 ms      __android_log_is_loggable()
⋮ ⋮ ⋮
           /* TID 0x73c9 */
 35113 ms  open(path "/data/user_de/0/com.example.displaydemo/code_cache/com.android.op
engl.shaders_cache", oflag 0x0)
```

```
 36036 ms  open(path "/proc/self/cmdline", oflag=0x80000)
 36037 ms  open(path "/proc/self/cmdline", oflag=0x80000)
 36037 ms  open(path "/proc/self/cmdline", oflag=0x80000)
           /* TID 0x73a5 */
⋮
 36345 ms  __cfi_slowpath()
 37083 ms  open(path "/data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8
U1Y8uB9h_Modc1C__Q==/lib/arm64/libtacker.so", oflag=0x0)
 37085 ms  open(path "/data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8
U1Y8uB9h_Modc1C__Q==/base.apk", oflag=0x80000)
 37086 ms  android_dlopen_ext()
 37094 ms  dlsym(handle 0x2bb94aab7ee5d9eb, symbol="JNI_OnLoad")
 37097 ms  __android_log_print()
 37097 ms      __android_log_is_loggable()
 37097 ms          __android_log_get_minimum_priority()
 37097 ms      __android_log_write_log_message()
 37097 ms          __android_log_logd_logger()
 37097 ms              __android_log_is_debuggable()
 37099 ms  dlerror()
 37100 ms  android_dlopen_ext()
 37111 ms      dlsym(handle 0x0, symbol="android_get_exported_namespace")
 37111 ms      dlopen(path "libRS_internal.so", mode=0x1)
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocation1DData")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocation1DRead")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocation2DData")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocation2DRead")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocation3DData")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocation3DRead")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationAdapterCreate")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationAdapterOffset")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationCopy2DRange")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationCopy3DRange")
 37141 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationCopyToBitmap")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationCreateFromBitmap")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationCreateStrided")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationCreateTyped")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationCubeCreateFromBitm
ap")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationElementData")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationElementRead")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationGenerateMipmaps")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationGetPointer")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationGetSurface")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsaAllocationGetType")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationIoReceive")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationIoSend")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationRead")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationResize1D")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationSetSurface")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationSyncAll")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationSetupBufferQueue")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAllocationShareBufferQueue")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsAssignName")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsClosureCreate")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsClosureSetArg")
 37142 ms      dlsym(handle 0xb510c3446c65bd65, symbol="rsClosureSetGlobal")
```

```
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextCreateVendor")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextDeinitToClient")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextDestroy")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextDump")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextFinish")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextGetMessage")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextInitToClient")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextPeekMessage")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextSendMessage")
37142 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextSetPriority")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsContextSetCacheDir")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsElementCreate2")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsElementCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsaElementGetNativeData")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsaElementGetSubElements")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsaGetName")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsInvokeClosureCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsObjDestroy")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsSamplerCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptBindAllocation")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptCCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptFieldIDCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptForEachMulti")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptGetVarV")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptGroup2Create")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptGroupCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptGroupExecute")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptGroupSetInput")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptGroupSetOutput")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptIntrinsicCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptInvoke")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptInvokeIDCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptInvokeV")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptKernelIDCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptReduce")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetTimeZone")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetVarD")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetVarF")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetVarI")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetVarJ")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetVarObj")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetVarVE")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsScriptSetVarV")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsTypeCreate")
37143 ms       | dlsym(handle 0xb510c3446c65bd65, symbol="rsaTypeGetNativeData")
37144 ms  dlsym(handle 0xdd4f837609790777, symbol="HIDL_FETCH_IDevice")
...
          /* TID 0x748b */
37148 ms  dlopen(path "libRSDriver_adreno.so", mode=0x1)
37169 ms  dlerror()
37169 ms  dlsym(handle 0xd30b16fb5b2b6c41, symbol="rsdHalQueryVersion")
37169 ms  dlsym(handle 0xd30b16fb5b2b6c41, symbol="rsdHalQueryHal")
37169 ms  dlsym(handle 0xd30b16fb5b2b6c41, symbol="rsdHalInit")
37169 ms  dlsym(handle 0xd30b16fb5b2b6c41, symbol="rsdHalAbort")
37169 ms  open(path "/proc/cpuinfo", oflag=0x80000)
37170 ms  open(path "./adreno_config.txt", oflag=0x0)
```

```
 37170 ms  open(path "/data/vendor/gpu//adreno_config.txt", oflag 0x0)
 37170 ms  open(path "/data/misc/gpu//adreno_config.txt", oflag 0x0)
 37170 ms  open(path "./yamato_panel.txt", oflag 0x0)
 37171 ms  open(path "/data/vendor/gpu//yamato_panel.txt", oflag 0x0)
 37171 ms  open(path "/data/misc/gpu//yamato_panel.txt", oflag 0x0)
 37172 ms  __cfi_slowpath()
 37180 ms  dlopen(path "libllvm-qcom.so", mode 0x2)
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_create_llvm_instance")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_destroy_llvm_instance")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_compile_source")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_link_program")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_get_error_code")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_get_build_log")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_query_handle_type")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_handle_to_executable")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_free_handle")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_disassemble")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_free_assembly")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_program_get_ddl_data")
 37256 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_handle_from_binary")
 37257 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_handle_create_binary")
 37257 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_program_free_binary")
 37257 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_interpret_printf_buffer"
)
 37257 ms  dlsym(handle 0x2dd005fbeae03129, symbol "cl_compiler_query_version_string")
 37264 ms  __cfi_slowpath()
 37265 ms  __cfi_slowpath()
 37265 ms  __cfi_slowpath()
 37265 ms  __cfi_slowpath()
 37265 ms  dlopen(path "libqti-perfd-client.so", mode 0x2)
...
 37266 ms  __cfi_slowpath()
 37266 ms  dlopen(path "librs_adreno_sha1.so", mode 0x2)
 37269 ms  dlsym(handle 0xe42754d5434639f, symbol "libllvm_qcom_so_SHA1")
 37269 ms  dlsym(handle 0xe42754d5434639f, symbol "libCB_so_SHA1")
 37269 ms  dlsym(handle 0xe42754d5434639f, symbol "libgsl_so_SHA1")
 37269 ms  dlsym(handle 0xe42754d5434639f, symbol "librs_adreno_so_SHA1")
 37269 ms  dlsym(handle 0xe42754d5434639f, symbol "libRSDriver_adreno_so_SHA1")
 37269 ms  dlclose(handle 0xe42754d5434639f)
 37269 ms  __cfi_slowpath()
 37270 ms  __android_log_print()
 37270 ms      __android_log_is_loggable()
 37270 ms          __android_log_get_minimum_priority()
 37270 ms      __android_log_write_log_message()
 37270 ms          __android_log_logd_logger()
 37270 ms              __android_log_is_debuggable()
           /* TID 0x73a5 */
 37270 ms  dlopen(path "libRSCacheDir.so", mode 0x1)
 37272 ms  dlsym(handle 0xaaa10682b389f92b, symbol "rsQueryCacheDir")
...
 37339 ms  __cfi_slowpath()
           /* TID 0x73e8 */
 39181 ms  open(path "/data/user_de/0/com.example.displaydemo/code_cache/com.android.op
engl.shaders_cache", oflag 0xc2)
 39196 ms  open(path "/data/user_de/0/com.example.displaydemo/code_cache/com.android.op
engl.shaders_cache", oflag 0xc2)
```

```
          /* TID 0x73e9 */
 30255 ms  open(path: "/data/user_de/0/com.example.displaydemo/code_cache/com.android.sk
ia.shaders_cache", oflag: 0xc2)
 30257 ms  open(path: "/data/user_de/0/com.example.displaydemo/code_cache/com.android.sk
ia.shaders_cache", oflag: 0xc2)
```

常见问题

Failed to spawn timeout was reached

- 现象

```
➜  frida frida-trace -U -f com.example.displaydemo -i JIN_OnLoad -i RegisterNatives
Spawning `com.example.displaydemo`...

Failed to spawn: timeout was reached
```

- 原因：偶发的bug
- 解决办法
  - 多试试几次
  - 重启安卓手机
  - 杀掉frida-server后，手动重启几次
    - 注：此处由于之前是Magisk安装的插件MagiskFrida，好像是：
      - 发现frida-server被杀掉后，会自动重启frida-server

心得

Frida的js脚本中过滤字符串参数

- 背景

想要在 `Interceptor.attach` 的 `onEnter` 中，实现参入参数的过滤=判断，去实现，当满足某些条件，才打印（或不打印）某些日志之类的需求

- 核心逻辑：用 `someJsStrList.includes(inputParaStr)` 去判断即可
- 示例代码

```
const KnownStrList = [
  "CurrencyMap/US/0/",
  "CurrencyMap/CN/0/",
  "CurrencyMap/CN/",
  "CurrencyMap/",
  "CurrencyMap",
  "CN",
  "US",
  "/",
  "0",
  "id",
  "zh_CN_#HANS",
  "zh_Hans_CN",
  "zh",
  "Hans",
  "HANS",
]

// char *strcpy(char *restrict dst, const char *restrict src);
Interceptor.attach(Module.findExportByName(null, "strcpy"), {
  onEnter: function (args) {
    var dst = Memory.readCString(args[0]);
    var src = Memory.readCString(args[1]);
    if ( KnownStrList.includes(src)) {
      console.log("strcpy: dst=" + dst + ", src=" + src);
    }
  },
  onLeave: function (args) {
  }
});
```

Frida去hook安卓JNI函数JIN_OnLoad却hook不到无输出

- 现象

此处，要调试的安卓app：

- DisplayDemo

    - 内部的so库：`libtacker.so`
        - 加载方式：`System.loadLibrary("tacker");`

-》可能是此处特殊的加载方式，导致了：

frida-trace无法去hook到，libtacker.so的加载，也就无法找到其内部的函数JNI_OnLoad了

所以frida-trace无法hook此处的JNI_OnLoad，无输出。

- 解决办法

手动写frida的js脚本，去

```
  const funcSym = "JNI_OnLoad";
  const funcPtr = Module.findExportByName(libraryName, "libtacker.so");
```

- 完整代码：
    - `hook_libtacker_JNI_Onload.js`

```
/**
 * frida -U -f com.example.displaydemo -l hook_libtacker_JNI_Onload.js
 */

function processJniOnLoad(libraryName) {
  const funcSym = "JNI_OnLoad";
  const funcPtr = Module.findExportByName(libraryName, funcSym);

  console.log("[+] Hooking " + funcSym + "() @ " + funcPtr + "...");
  // jint JNI_OnLoad(JavaVM *vm, void *reserved);
  var funcHook = Interceptor.attach(funcPtr, {
      onEnter: function (args) {
          const vm = args[0];
          const reserved = args[1];
          console.log("[+] " + funcSym + "(" + vm + ", " + reserved + ") called");
      },
      onLeave: function (retval) {
          console.log("[+]\t= " + retval);
      }
  });
}

function waitForLibLoading(libraryName) {
  var isLibLoaded = false;

  Interceptor.attach(Module.findExportByName(null, "android_dlopen_ext"), {
      onEnter: function (args) {
          var libraryPath = Memory.readCString(args[0]);
          if (libraryPath.includes(libraryName)) {
              console.log("[+] Loading library " + libraryPath + "...");
              isLibLoaded = true;
          }
      },
      onLeave: function (args) {
          if (isLibLoaded) {
```

```
                processJniOnLoad(libraryName);
                isLibLoaded = false;
            }
        }
    });
}

Java.perform(function() {
    const libraryName = "libtacker.so";
    waitForLibLoading(libraryName);
});
```

（此处点击Jump跳转页面后）即可hook到JNI_OnLoad函数的执行：

=> 输出：

- 截图


frida-trace frida-trace -U -f com.example.displaydemo -i dlopen
Instrumenting...
dlopen: Auto-generated handler at "/Users/crifan/dev/dev_root/androidReverse/popupSDK_libtacker/dynamicDebug/frida/frida-trace/__handlers_
Started tracing 1 function. Press Ctrl+C to stop.
/* TID 0x78f8 */
506 ms dlopen(path="libEGL_adreno.so", mode=0x2)
521 ms dlopen(path="libadreno_utils.so", mode=0x2)
/* TID 0x78d5 */
7651 ms dlopen(path="libRS_internal.so", mode=0x1)
/* TID 0x7950 */
7657 ms dlopen(path="libRSDriver_adreno.so", mode=0x1)
7663 ms dlopen(path="libllvm-qcom.so", mode=0x2)
7668 ms dlopen(path="libqti-perfd-client.so", mode=0x2)
7669 ms dlopen(path="librs_adreno_sha1.so", mode=0x2)
/* TID 0x78d5 */
7671 ms dlopen(path="libRSCacheDir.so", mode=0x1)
^C
frida-trace frida -U -f com.example.displaydemo -l hook_libtacker_JNI_Onload.js
frida-trace cd ..
frida cd frida
frida ll
total 8
-rw-r--r--@ 1 crifan staff 1.3K 7 28 22:30 hook_libtacker_JNI_Onload.js
frida frida -U -f com.example.displaydemo -l hook_libtacker_JNI_Onload.js
Frida 16.1.3 - A world-class dynamic instrumentation toolkit
Commands:
help -> Displays the help system
object? -> Display information about 'object'
exit/quit -> Exit
More info at https://frida.re/docs/home/
Connected to Pixel 3 (id=91BX1VSA3)
Spawned `com.example.displaydemo`. Resuming main thread!
[Pixel 3::com.example.displaydemo]-> %resume
[Pixel 3::com.example.displaydemo]-> [+] Loading library /data/app/~~OyO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8U1Y8u89h_Modc1C__Q==/
[+] Hooking JNI_OnLoad() @ 0x6dd0349438...
[+] JNI_OnLoad(0x6eaf3380d0, 0x0) called
[+] = 0x10006
测试页面
option
command

- log日志

```
➜  frida frida -U -f com.example.displaydemo -l hook_libtacker_JNI_Onload.js
     ____
    / _  |   Frida 16.1.3 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Pixel 3 (id=91BX1VSA3)
Spawned `com.example.displaydemo`. Resuming main thread!
[Pixel 3::com.example.displaydemo ]-> %resume
[Pixel 3::com.example.displaydemo ]-> [+] Loading library /data/app/~~0yO-UMCLSaECmfJvvRSy1w==/com.example.displaydemo-EXz8U1Y8uB9h_Modc1C__Q==/base.apk /lib/arm64-v8a/libtacker.so...
[+] Hooking JNI_OnLoad() @ 0x6dd0349438...
[+] JNI_OnLoad(0x6eaf3380d0, 0x0) called
[+]     = 0x10006
```

模拟代码运行

Unidbg

- Unidbg
  - Github
    - https://github.com/zhkl0228/unidbg
      - Allows you to emulate an Android native library, and an experimental iOS emulation
  - 概述
    - unidbg是unicorn的一个实现，它可以让你在电脑上跑arm的可执行文件或共享库文件
    - unidbg是一个基于 `unicorn` 的逆向工具，可以在PC端直接调用Android（的apk中）和iOS（的ipa中）的 `so` 动态库文件（中的native函数方法）
  - 背景
    - 目前很多 App 的加密签名算法都在so文件中，强行逆向so的话可能会消耗大量时间和资源
  - 规避方式
    - 用 xposed 采用 hook 的方法从程序计算签名
      - 缺点：需要模拟器或者真机运行这个应用，使用效率不高
    - 用过 jtype 启动JVM，然后通过 native 对so文件进行调用
      - 缺点：因为每次都需要启动JVM，所以效率也不高
    - unidbg
      - 原理：通过在 app 中找到对应的 JNI 接口，然后用 unicorn 引擎直接调用 so 文件
      - 优点：不需要运行 app，也无需逆向 so 文件，所以效率相对要高不少
  - 底层依赖于：Unicorn
    - 详见
      - CPU模拟利器：Unicorn

安卓的Hook框架

TODO：

- hook框架
  - 【整理】安卓hook框架：Sandhook

- 安卓的Hook框架
  - Xposed（系列）
  - Cydia Substrate

Xposed框架

- 概述
  - Xposed/EdXposed/LSPosed系列框架
    - 可以安装插件实现各种功能
    - 也可以自己自己写Xposed插件，实现特定功能
      - 理论上也可以动态调试Xposed插件
- 详解：安卓逆向调试：XPosed框架

CydiaSubstrate

- 主页
  - CydiaSubstrate
- 下载
  - com.saurik.substrate.apk
- 功能
  - 和 `Xposed` 类似的框架，用来安装各种插件，实现各种功能。
    - 比如可以：
      - 安装绕过 `ssl` 检测的插件，用来破解 `ssl pinning`
        - 关于安卓的app中的https：
          - app内部启用了：
            - `SSL Pinning` = `ssl certificate pinning` = `certificate pinning`
              - = `ssl证书绑定` =证书绑定`
      - 此处也可以用来安装相关插件，导出安卓的dex文件
- 特点
  - Hook底层方法非常方便
    - 对so中的方法hook操作非常便捷
- 截图

Android-OpenDebug

- 主页
  - iSECPartners/Android-OpenDebug: Make any application debuggable
- 功能
  - 是一个 `Cydia Substrate` 的插件
    - 所以前提是要先安装 `Cydia Substrate`
  - 可以使得任何一个安卓程序可以被调试
    - 就有了分析和破解的可能
- 下载
  - Android-OpenDebug APK下载
- 安装
  - `adb install Android-OpenDebug.apk`
  - 或直接安装apk

Introspy-Android

- 主页
  - GitHub
    - iSECPartners/Introspy-Android: Security profiling for blackbox Android
  - 网站
    - Introspy-Android
- 功能
  - 帮助分析安卓app运行期间的行为
    - 以便于找到可能存在的安全问题
- 提示
  - 是个 `Cydia Substrate` 插件
    - 所以前提是先安装 `Cydia Substrate`

adb辅助调试

adb查看进程内存映射

- 查看进程的内存映射real layout of process segment

```
/proc/ pid /maps
```

举例：

查看安卓app：`AIO File Manager`=包名：`com.manager.files.super.cleaner`的进程的内存映射

```
adb shell
```

后：

查看确认进程PID：

```
blueline:/storage/emulated/0/dev # ps -A | grep clean
u0_a256       14868   1025 2051980  61568 SyS_epoll_wait      0 S com.manager.files.sup
er.cleaner
```

查看到AIO File Manager的PID是：14868

再去切换到root权限：

```
su
```

然后才能看到maps映射：

```
cat /proc/14868/maps
```

输出结果：

```
blueline:/sdcard/dev $ cat /proc/14868/map
map_files/  maps
```

详细结果：

```
blueline:/storage/emulated/0/dev # cat /proc/14868/maps
12c00000-52c00000 rw-p 00000000 00:00 0                                  [anon:dalvik-m
ain space (region space)]
6faeb000-6fcc8000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
apex/com.android.art/javalib/boot.art]
6fcc8000-6fd0b000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
apex/com.android.art/javalib/boot-core-libart.art]
6fd0b000-6fda9000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
apex/com.android.art/javalib/boot-core-icu4j.art]
6fda9000-6fdd2000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
apex/com.android.art/javalib/boot-okhttp.art]
```

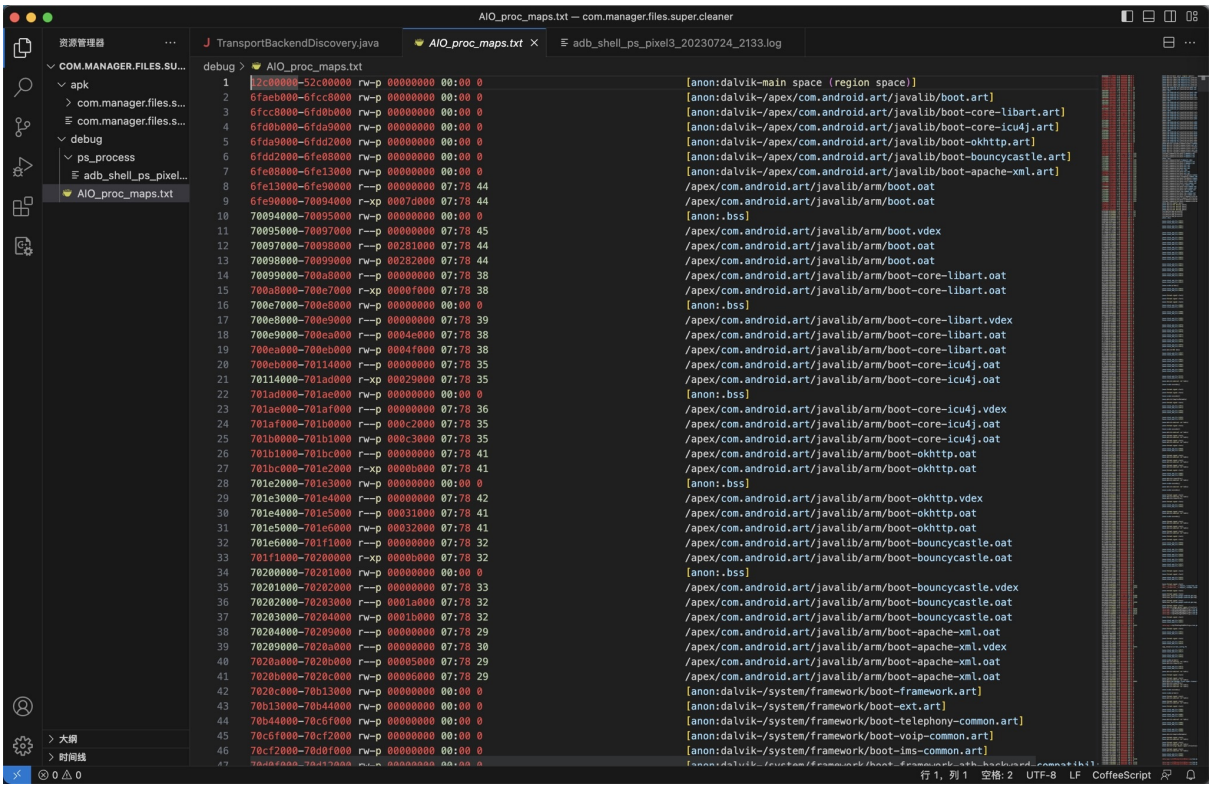
```
6fdd2000-6fe08000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
apex/com.android.art/javalib/boot-bouncycastle.art]
6fe08000-6fe13000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
apex/com.android.art/javalib/boot-apache-xml.art]
6fe13000-6fe90000 r--p 00000000 07:78 44                                 /apex/com.andr
oid.art/javalib/arm/boot.oat
6fe90000-70094000 r-xp 0007d000 07:78 44                                 /apex/com.andr
oid.art/javalib/arm/boot.oat
70094000-70095000 rw-p 00000000 00:00 0                                  [anon:.bss]
70095000-70097000 r--p 00000000 07:78 45                                 /apex/com.andr
oid.art/javalib/arm/boot.vdex
70097000-70098000 r--p 00281000 07:78 44                                 /apex/com.andr
oid.art/javalib/arm/boot.oat
70098000-70099000 rw-p 00282000 07:78 44                                 /apex/com.andr
oid.art/javalib/arm/boot.oat
70099000-700a8000 r--p 00000000 07:78 38                                 /apex/com.andr
oid.art/javalib/arm/boot-core-libart.oat
700a8000-700e7000 r-xp 0000f000 07:78 38                                 /apex/com.andr
oid.art/javalib/arm/boot-core-libart.oat
700e7000-700e8000 rw-p 00000000 00:00 0                                  [anon:.bss]
700e8000-700e9000 r--p 00000000 07:78 39                                 /apex/com.andr
oid.art/javalib/arm/boot-core-libart.vdex
700e9000-700ea000 r--p 0004e000 07:78 38                                 /apex/com.andr
oid.art/javalib/arm/boot-core-libart.oat
700ea000-700eb000 rw-p 0004f000 07:78 38                                 /apex/com.andr
oid.art/javalib/arm/boot-core-libart.oat
700eb000-70114000 r--p 00000000 07:78 35                                 /apex/com.andr
oid.art/javalib/arm/boot-core-icu4j.oat
70114000-701ad000 r-xp 00029000 07:78 35                                 /apex/com.andr
oid.art/javalib/arm/boot-core-icu4j.oat
701ad000-701ae000 rw-p 00000000 00:00 0                                  [anon:.bss]
701ae000-701af000 r--p 00000000 07:78 36                                 /apex/com.andr
oid.art/javalib/arm/boot-core-icu4j.vdex
701af000-701b0000 r--p 000c2000 07:78 35                                 /apex/com.andr
oid.art/javalib/arm/boot-core-icu4j.oat
701b0000-701b1000 rw-p 000c3000 07:78 35                                 /apex/com.andr
oid.art/javalib/arm/boot-core-icu4j.oat
701b1000-701bc000 r--p 00000000 07:78 41                                 /apex/com.andr
oid.art/javalib/arm/boot-okhttp.oat
701bc000-701e2000 r-xp 0000b000 07:78 41                                 /apex/com.andr
oid.art/javalib/arm/boot-okhttp.oat
701e2000-701e3000 rw-p 00000000 00:00 0                                  [anon:.bss]
701e3000-701e4000 r--p 00000000 07:78 42                                 /apex/com.andr
oid.art/javalib/arm/boot-okhttp.vdex
701e4000-701e5000 r--p 00031000 07:78 41                                 /apex/com.andr
oid.art/javalib/arm/boot-okhttp.oat
701e5000-701e6000 rw-p 00032000 07:78 41                                 /apex/com.andr
oid.art/javalib/arm/boot-okhttp.oat
701e6000-701f1000 r--p 00000000 07:78 32                                 /apex/com.andr
oid.art/javalib/arm/boot-bouncycastle.oat
701f1000-70200000 r-xp 0000b000 07:78 32                                 /apex/com.andr
oid.art/javalib/arm/boot-bouncycastle.oat
70200000-70201000 rw-p 00000000 00:00 0                                  [anon:.bss]
70201000-70202000 r--p 00000000 07:78 33                                 /apex/com.andr
oid.art/javalib/arm/boot-bouncycastle.vdex
70202000-70203000 r--p 0001a000 07:78 32                                 /apex/com.andr
```

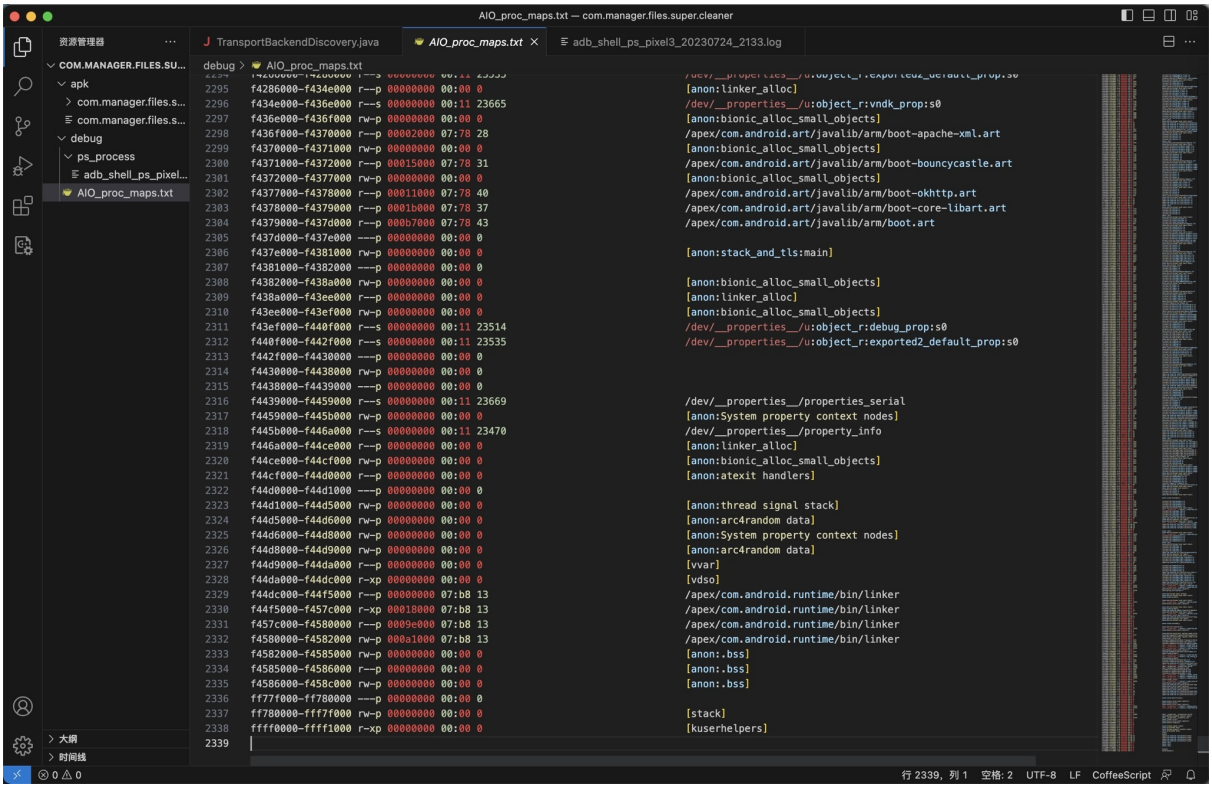
```
oid.art/javalib/arm/boot-bouncycastle.oat
70203000-70204000 rw-p 0001b000 07:78 32                                 /apex/com.andr
oid.art/javalib/arm/boot-bouncycastle.oat
70204000-70209000 r--p 00000000 07:78 29                                 /apex/com.andr
oid.art/javalib/arm/boot-apache-xml.oat
70209000-7020a000 r--p 00000000 07:78 30                                 /apex/com.andr
oid.art/javalib/arm/boot-apache-xml.vdex
7020a000-7020b000 r--p 00005000 07:78 29                                 /apex/com.andr
oid.art/javalib/arm/boot-apache-xml.oat
7020b000-7020c000 rw-p 00006000 07:78 29                                 /apex/com.andr
oid.art/javalib/arm/boot-apache-xml.oat
7020c000-70b13000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
system/framework/boot-framework.art]
70b13000-70b44000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
system/framework/boot-ext.art]
70b44000-70c6f000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
system/framework/boot-telephony-common.art]
70c6f000-70cf2000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
system/framework/boot-voip-common.art]
70cf2000-70d0f000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
system/framework/boot-ims-common.art]
70d0f000-70d12000 rw-p 00000000 00:00 0                                  [anon:dalvik-/
system/framework/boot-framework-atb-backward-compatibility.art]
70d12000-70f01000 r--p 00000000 fd:04 1225                               /system/framew
ork/arm/boot-framework.oat
70f01000-71613000 r-xp 001ef000 fd:04 1225                               /system/framew
ork/arm/boot-framework.oat
71613000-71615000 r--p 00901000 fd:04 1225                               /system/framew
ork/arm/boot-framework.oat
71615000-71616000 rw-p 00000000 00:00 0                                  [anon:.bss]
71616000-71620000 r--p 00000000 fd:04 1258                               /system/framew
ork/boot-framework.vdex
71620000-71621000 r--p 00903000 fd:04 1225                               /system/framew
ork/arm/boot-framework.oat
71621000-71622000 rw-p 00904000 fd:04 1225                               /system/framew
ork/arm/boot-framework.oat
71622000-71627000 r--p 00000000 fd:04 1219                               /system/framew
ork/arm/boot-ext.oat
71627000-71638000 r-xp 00005000 fd:04 1219                               /system/framew
ork/arm/boot-ext.oat
71638000-71639000 r--p 00016000 fd:04 1219                               /system/framew
ork/arm/boot-ext.oat
71639000-7163a000 r--p 00000000 fd:04 1256                               /system/framew
ork/boot-ext.vdex
7163a000-7163b000 r--p 00017000 fd:04 1219                               /system/framew
ork/arm/boot-ext.oat
7163b000-7163c000 rw-p 00018000 fd:04 1219                               /system/framew
ork/arm/boot-ext.oat
7163c000-71644000 r--p 00000000 fd:04 1231                               /system/framew
ork/arm/boot-telephony-common.oat
71644000-71645000 r--p 00000000 fd:04 1260                               /system/framew
ork/boot-telephony-common.vdex
71645000-71646000 r--p 00008000 fd:04 1231                               /system/framew
ork/arm/boot-telephony-common.oat
71646000-71647000 rw-p 00009000 fd:04 1231                               /system/framew
ork/arm/boot-telephony-common.oat
```

```
71647000-7164c000 r--p 00000000 fd:04 1234                               /system/framew
ork/arm/boot-voip-common.oat
7164c000-7164d000 r-xp 00005000 fd:04 1234                               /system/framew
ork/arm/boot-voip-common.oat
7164d000-7164e000 r--p 00000000 fd:04 1261                               /system/framew
ork/boot-voip-common.vdex
7164e000-7164f000 r--p 00006000 fd:04 1234                               /system/framew
ork/arm/boot-voip-common.oat
7164f000-71650000 rw-p 00007000 fd:04 1234                               /system/framew
ork/arm/boot-voip-common.oat
71650000-71652000 r--p 00000000 fd:04 1228                               /system/framew
ork/arm/boot-ims-common.oat
71652000-71653000 r--p 00000000 fd:04 1259                               /system/framew
ork/boot-ims-common.vdex
71653000-71654000 r--p 00002000 fd:04 1228                               /system/framew
ork/arm/boot-ims-common.oat
71654000-71655000 rw-p 00003000 fd:04 1228                               /system/framew
ork/arm/boot-ims-common.oat
71655000-71657000 r--p 00000000 fd:04 1222                               /system/framew
ork/arm/boot-framework-atb-backward-compatibility.oat
71657000-71658000 r--p 00000000 fd:04 1257                               /system/framew
ork/boot-framework-atb-backward-compatibility.vdex
71658000-71659000 r--p 00002000 fd:04 1222                               /system/framew
ork/arm/boot-framework-atb-backward-compatibility.oat
71659000-7165a000 rw-p 00003000 fd:04 1222                               /system/framew
ork/arm/boot-framework-atb-backward-compatibility.oat
7165a000-719bd000 rw-p 00000000 00:00 0                                  [anon:dalvik-z
ygote space]
719bd000-719bf000 rw-p 00000000 00:00 0                                  [anon:dalvik-n
on moving space]
719bf000-719cc000 rw-p 00000000 00:00 0                                  [anon:dalvik-n
on moving space]
719cc000-74e5b000 ---p 00000000 00:00 0                                  [anon:dalvik-n
on moving space]
74e5b000-7565a000 rw-p 00000000 00:00 0                                  [anon:dalvik-n
on moving space]
b1562000-b1564000 r--p 00000000 fd:04 176                                /system/bin/ap
p_process32
b1564000-b1568000 r-xp 00001000 fd:04 176                                /system/bin/ap
p_process32
...
...
...


f4226000-f4246000 r--s 00000000 00:11 23653                              /dev/__propert
ies__/u:object_r:vendor_socket_hook_prop:s0
f4246000-f4266000 r--s 00000000 00:11 23566                              /dev/__propert
ies__/u:object_r:heapprofd_prop:s0
f4266000-f4286000 r--s 00000000 00:11 23535                              /dev/__propert
ies__/u:object_r:exported2_default_prop:s0
f4286000-f434e000 r--p 00000000 00:00 0                                  [anon:linker_a
lloc]
f434e000-f436e000 r--s 00000000 00:11 23665                              /dev/__propert
ies__/u:object_r:vndk_prop:s0
f436e000-f436f000 rw-p 00000000 00:00 0                                  [anon:bionic_a
```

```
lloc_small_objects]
f436f000-f4370000 r--p 00002000 07:78 28                                 /apex/com.andr
oid.art/javalib/arm/boot-apache-xml.art
f4370000-f4371000 rw-p 00000000 00:00 0                                  [anon:bionic_a
lloc_small_objects]
f4371000-f4372000 r--p 00015000 07:78 31                                 /apex/com.andr
oid.art/javalib/arm/boot-bouncycastle.art
f4372000-f4377000 rw-p 00000000 00:00 0                                  [anon:bionic_a
lloc_small_objects]
f4377000-f4378000 r--p 00011000 07:78 40                                 /apex/com.andr
oid.art/javalib/arm/boot-okhttp.art
f4378000-f4379000 r--p 0001b000 07:78 37                                 /apex/com.andr
oid.art/javalib/arm/boot-core-libart.art
f4379000-f437d000 r--p 000b7000 07:78 43                                 /apex/com.andr
oid.art/javalib/arm/boot.art
f437d000-f437e000 ---p 00000000 00:00 0
f437e000-f4381000 rw-p 00000000 00:00 0                                  [anon:stack_an
d_tls:main]
f4381000-f4382000 ---p 00000000 00:00 0
f4382000-f438a000 rw-p 00000000 00:00 0                                  [anon:bionic_a
lloc_small_objects]
f438a000-f43ee000 r--p 00000000 00:00 0                                  [anon:linker_a
lloc]
f43ee000-f43ef000 rw-p 00000000 00:00 0                                  [anon:bionic_a
lloc_small_objects]
f43ef000-f440f000 r--s 00000000 00:11 23514                              /dev/__propert
ies__/u:object_r:debug_prop:s0
f440f000-f442f000 r--s 00000000 00:11 23535                              /dev/__propert
ies__/u:object_r:exported2_default_prop:s0
f442f000-f4430000 ---p 00000000 00:00 0
f4430000-f4438000 rw-p 00000000 00:00 0
f4438000-f4439000 ---p 00000000 00:00 0
f4439000-f4459000 r--s 00000000 00:11 23669                              /dev/__propert
ies__/properties_serial
f4459000-f445b000 rw-p 00000000 00:00 0                                  [anon:System p
roperty context nodes]
f445b000-f446a000 r--s 00000000 00:11 23470                              /dev/__propert
ies__/property_info
f446a000-f44ce000 r--p 00000000 00:00 0                                  [anon:linker_a
lloc]
f44ce000-f44cf000 rw-p 00000000 00:00 0                                  [anon:bionic_a
lloc_small_objects]
f44cf000-f44d0000 r--p 00000000 00:00 0                                  [anon:atexit h
andlers]
f44d0000-f44d1000 ---p 00000000 00:00 0
f44d1000-f44d5000 rw-p 00000000 00:00 0                                  [anon:thread s
ignal stack]
f44d5000-f44d6000 rw-p 00000000 00:00 0                                  [anon:arc4rand
om data]
f44d6000-f44d8000 rw-p 00000000 00:00 0                                  [anon:System p
roperty context nodes]
f44d8000-f44d9000 rw-p 00000000 00:00 0                                  [anon:arc4rand
om data]
f44d9000-f44da000 r--p 00000000 00:00 0                                  [vvar]
f44da000-f44dc000 r-xp 00000000 00:00 0                                  [vdso]
f44dc000-f44f5000 r--p 00000000 07:b8 13                                 /apex/com.andr
```

```
oid.runtime/bin/linker
f44f5000-f457c000 r-xp 00018000 07:b8 13                                 /apex/com.andr
oid.runtime/bin/linker
f457c000-f4580000 r--p 0009e000 07:b8 13                                 /apex/com.andr
oid.runtime/bin/linker
f4580000-f4582000 rw-p 000a1000 07:b8 13                                 /apex/com.andr
oid.runtime/bin/linker
f4582000-f4585000 rw-p 00000000 00:00 0                                  [anon:.bss]
f4585000-f4586000 r--p 00000000 00:00 0                                  [anon:.bss]
f4586000-f458c000 rw-p 00000000 00:00 0                                  [anon:.bss]
ff77f000-ff780000 ---p 00000000 00:00 0
ff780000-ff7f7000 rw-p 00000000 00:00 0                                  [stack]
ffff0000-ffff1000 r-xp 00000000 00:00 0                                  [kuserhelpers]
```

- 

- 

内存映射信息的解读

想要搞懂：

- 内存对齐
- 哪个是stack

等具体含义。

Understanding ELF using readelf and objdump (studylib.net)

```
[1] 0039d000-003b2000 r-xp 00000000 16:41 1080084 /lib/ld-2.3.3.so
[2] 003b2000-003b3000 r--p 00014000 16:41 1080084 /lib/ld-2.3.3.so
[3] 003b3000-003b4000 rw-p 00015000 16:41 1080084 /lib/ld-2.3.3.so
[4] 003b6000-004cb000 r-xp 00000000 16:41 1080085 /lib/tls/libc-2.3.3.so
[5] 004cb000-004cd000 r--p 00115000 16:41 1080085 /lib/tls/libc-2.3.3.so
[6] 004cd000-004cf000 rw-p 00117000 16:41 1080085 /lib/tls/libc-2.3.3.so
[7] 004cf000-004d1000 rw-p 004cf000 00:00 0
[8] 08048000-08049000 r-xp 00000000 16:06 66970 /tmp/test
[9] 08049000-0804a000 rw-p 00000000 16:06 66970 /tmp/test
[10] b7fec000-b7fed000 rw-p b7fec000 00:00 0
[11] bffeb000-c0000000 rw-p bffeb000 00:00 0
[12] ffffe000-fffff000 ---p 00000000 00:00 0
```

其中：

- VMA# 11
  - `[11] bffeb000-c0000000 rw-p bffeb000 00:00 0`

是：

- stack
  - usually, the kernel allocate several pages dynamically and map to the highest virtual address possible in user space to form stack area.

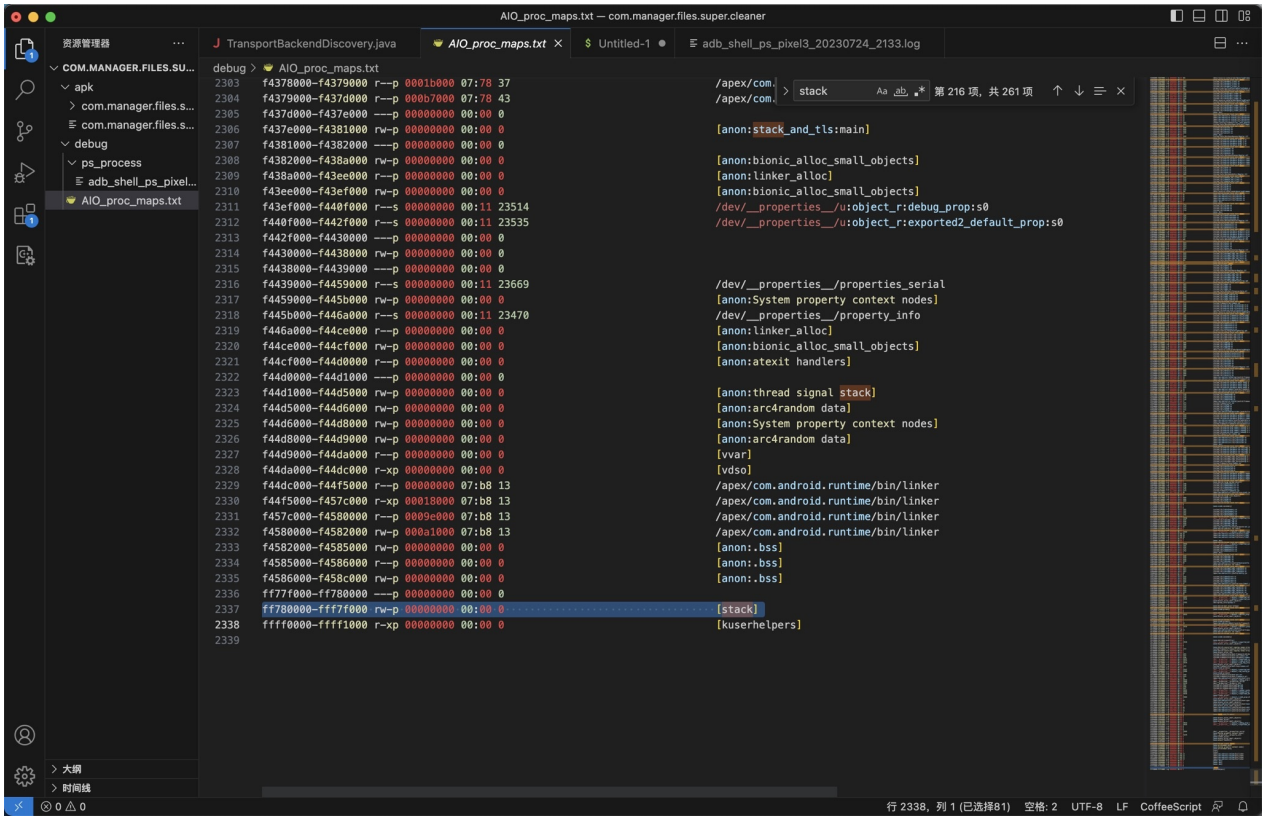
-> 此处去搜stack，还真有多个stack这样的：

```
e6ded000-e6df1000 rw-p 00000000 00:00 0                                  [anon:thread s
ignal stack]

e84d3000-e86d3000 rw-p 00000000 00:00 0                                  [anon:dalvik-r
b copying gc mark stack]
e86d3000-e96d3000 rw-p 00000000 00:00 0                                  [anon:dalvik-c
oncurrent copying gc mark stack]
e96d3000-e9ed4000 rw-p 00000000 00:00 0                                  [anon:dalvik-l
ive stack]
e9ed4000-ea6d5000 rw-p 00000000 00:00 0                                  [anon:dalvik-a
llocation stack]

ebbc0000-ebdc0000 rw-p 00000000 00:00 0                                  [anon:dalvik-r
b copying gc mark stack]

f2282000-f228e000 rw-p 00000000 00:00 0                                  [anon:dalvik-t
hread local mark stack]
...
```

倒数最后一个：

```
ff780000-fff7f000 rw-p 00000000 00:00 0                                  [stack]
```

整个名字就是Stack：



是我们希望的，要找的

- Simply speaking, each process address space isdivid ed into two part (this assume Intel compatible 32 bit processor): user space and kernel space. User space is in 0x00000000-0xc0000000 range, while kernel space starts on 0xc0000000 onward

->

- 每个进程的（Intel 的32位处理器的）地址空间都被分为2部分
  - 用户空间
    - 范围：`0x00000000-0xc0000000`
      - 所以上述test的地址空间的，最高位置(地址范围 `bffeb000-c0000000`),分配给了stack
        - `[11] bffeb000-c0000000 rw-p bffeb000 00:00 0`
  - 内核空间
    - 范围：0xc0000000-...

其他相关解释：

Executable and Linkable Format (ELF) (netmeister.org)

```
0000000000400000      8K r-x--  a.out
0000000000601000      4K rw---  a.out
0000003433e00000    112K r-x--  /lib64/ld-2.5.so
0000003433401b000      4K r----  /lib64/ld-2.5.so
0000003433401c000      4K rw---  /lib64/ld-2.5.so
0000003434200000   1336K r-x--  /lib64/libc-2.5.so      <-- The first "LOAD" segment, wh
ich contains .text and .rodata sections
0000003434434e000   2044K -----  /lib64/libc-2.5.so      <-- "Hole"
0000003434454d000     16K r----  /lib64/libc-2.5.so      <-- Relocation (GNU_RELRO) info
 -+---- The second "LOAD" segment
```

```
0000003434551000      4K rw---  /lib64/libc-2.5.so      <-- .got.plt .data sections
 -+
0000003434552000     20K rw---    [ anon ]             <-- The remaining zero-filled se
ctions (e.g. .bss)
0000003434e00000     88K r-x--  /lib64/libpthread-2.5.so     <-- The first "LOAD" segme
nt, which contains .text and .rodata sections
0000003434e16000   2044K -----  /lib64/libpthread-2.5.so     <-- "Hole"
0000003435015000      4K r----  /lib64/libpthread-2.5.so     <-- Relocation (GNU_RELRO)
 info  -+---- The second "LOAD" segment
0000003435016000      4K rw---  /lib64/libpthread-2.5.so     <-- .got.plt .data section
s      -+
0000003435017000     16K rw---    [ anon ]                  <-- The remaining zero-fil
led sections (e.g. .bss)
00002aaaaaaab000      4K rw---    [ anon ]
00002aaaaaac6000     12K rw---    [ anon ]
00007fffffffea000     84K rw---    [ stack ]
ffffffffff600000   8192K -----    [ anon ]
 total            14000K
```

供参考。

其他工具

此处整理和安卓逆向的动态调试有关的，其他的分析和调试方面的工具。

AndBug

- 主页
  - swdunlop/AndBug: Android Debugging Library
- 作用
  - 在没有源代码的情况下，调试android上的java程序
- 功能
  - 支持断点、call stack查看、查看class、method等信息
- 截图
  -

redexer

- 主页
  - plum-umd/redexer: The Redexer binary instrumentation framework for Dalvik bytecode
  - The Redexer Dalvik bytecode instrumentation platform
- 文档
  - Tutorial: using redexer to implement logging in Android apps
- 功能
  - Dalvik 字节码（用于安卓APP）分析框架
  - 它是一套基于OCaml的实用工具
    - 帮助程序员解析、操作Dalvik虚拟机
- 作者
  - Redexer由来自马里兰大学帕克分校的PLUM组织开发完成
  - 主要作者是：Jinseong Jeon，Kristopher Micinski以及Jeff Foster

Fino

- `Fino = FINO`
- 主页
  - sysdream/fino: Android small footprint inspection tool
- 功能
  - An Android Dynamic Analysis Tool
- 特点
  - 资源占用少

附录

下面列出相关参考资料。

参考资料

- 【未解决】Mac中用LLDB调试DisplayDemo安卓app中的libtacker.so
- 【已解决】安卓逆向：lldb调试安卓app
- 【已解决】Mac中下载和安装lldb-server到安卓手机Pixel3
- 【已解决】已root的Android13的Pixel5中：用lldb调试安卓
- 【已解决】Mac中lldb连接安卓中lldb-server报错：error Connection shut down by remote side while waiting for reply to initial handshake packet
- 【记录】用lldb去调试安卓app：LiftFileManager
- 【已解决】Mac中给安卓手机Pixel3中初始化Frida调试环境
- 【已解决】安卓手机Pixel3中运行frida-server
- 【已解决】安卓手机Pixel3中adb shell中chmod无效
- 【部分解决】Mac中运行adb root卡死restarting adbd as root
- 【已解决】Mac中调试Pixel3中frida报错：Failed to enumerate processes connection closed
- 【已解决】Mac中用frida去调试安卓手机Pixel3中的安卓app
- 【已解决】尝试解决Android的frida不可用问题：MagiskFrida
- 【已解决】安卓逆向：Pixel3中初始化frida调试安卓apk的环境
- 【未解决】安卓逆向：用frida去hook调试JNI_OnLoad
- 【记录】用frida-trace调试DisplayDemo中更多的函数调用
- 【已解决】frida-trace去hook安卓应用报错：Failed to spawn timeout was reached
- 【已解决】安卓逆向DisplayDemo：用Frida去hook调试dlopen
- 【未解决】安卓逆向DisplayDemo：用Frida去hook调试android_dlopen_ext
- 【未解决】安卓逆向LiftFileManager：用frida去hook调试
- 【未解决】安卓逆向：用frida去hook调试RegisterNatives
- 【已解决】安卓逆向LiftFileManager：用frida调试lcodecorex/KeepAlive相关底层C函数
- 【记录】安卓逆向LiftFileManager：分析frida调试lcodecorex/KeepAlive的结果
- 【已解决】安卓逆向LiftFileManager：用frida调试flock及结果分析
- 【未解决】安卓逆向LiftFileManager：用frida调试pthread_create并分析结果
- 【未解决】安卓逆向LiftFileManager：用frida调试创建进程的Linux的C函数
- 【未解决】Mac中安装frida
- 【已解决】Frida去hook安卓JNI函数JIN_OnLoad却hook不到无输出
- 【已解决】安卓逆向DisplayDemo：用frida+js脚本去hook函数JIN_OnLoad
- 【已解决】Frida调试安卓进程：字符串参数判断过滤
- 【未解决】尝试解决Android Studio中smali断点不生效：smalidea插件问题
- 【未解决】尝试解决Android Studio中smali断点不生效：卸载重装smalidea插件
- 【记录】Android Studio调试smali：IDE出错Exception in plugin Smalidea
- 【记录】安卓手机中查看进程内存映射
- 【已解决】Android Studio和DDMS中看不到安卓设备中的所有进程
- 【已解决】Mac中运行adb shell无需su超级用户即可正常运行输出结果
- 【未解决】Android Studio调试报错：Unable to open debugger port localhost handshake failed connection prematurally closed
- 【未解决】Android Studio中smali断点不生效无法触发断点
-
- crifan/AndroidYouTubeDynamicDebug: 安卓逆向动态调试YouTube (github.com)

- 主流调试器：LLDB
- Xposed插件开发 · 安卓逆向调试：XPosed框架
- CPU模拟利器：Unicorn
-
- lldb-server – Server for LLDB Debugging Sessions — The LLDB Debugger
- Android SDK Offline: Android NDK LLDB Direct Download
- 内容相对最完整
  - 安卓逆向*13 --- AndroidStudio* + *Smalidea* 动态调试 *smali* 代码【*APK*可调试】、*gradle* 配置擒贼先擒王的博客-CSDN博客_smalidea
- DDMS adb 调试 端口 映射 关系
  - Android调试系列—使用android studio调试smali代码 - Gordon0918 - 博客园 (cnblogs.com)
- Android Studio 动态调试 apk 反编译出的 smali 代码 - yhjoker - 博客园 (cnblogs.com)
- Android逆向破解：使用Android Studio调试反编译后的smali代码 - 简书 (jianshu.com)
- Android逆向 | AndroidStudio的两种动态调试技巧 - 腾讯云开发者社区-腾讯云 (tencent.com)
- 超详细的android so库的逆向调试 - 掘金 (juejin.cn)
- 学习笔记： Android studio 调试smali_深秋黄金甲的博客-CSDN博客_androidstudio smali
- Android Studio 3.6 调试 smali的全过程 - 腾讯云开发者社区-腾讯云 (tencent.com)
- Smali动态调试之Android Studio - Blog - teisyogun (bushrose.github.io)
- 基于Android studio动态调试smali全过程 - 简书 (jianshu.com)
- Android逆向笔记-使用Android Studio调试Smali代码（方式一）_IT1995的博客-CSDN博客
- android 动态调试 - 简书 (jianshu.com)
- Android Applications Reversing 101 (evilsocket.net)
- 安卓逆向-从环境搭建到动态调试apk - FreeBuf网络安全行业门户
- 安卓逆向分析中常用动态调试方法总结*Denny_Chen*的博客-CSDN博客_安卓动态调试
- Android逆向破解：使用Android Studio调试反编译后的smali代码 - 简书 (jianshu.com)
- Android Studio 动态调试 apk 反编译出的 smali 代码 - yhjoker - 博客园 (cnblogs.com)
- [免费专栏] Android安全之Android Studion 动态调试APK的两种方法菠萝橙留香的博客-CSDN博客_安卓apk调试
- [原创]修改Nexus5的boot.img - 打开系统调试-Android安全-看雪论坛-安全社区|安全招聘|bbs.pediy.com
- unidbg调用so生成xgorgon - SegmentFault 思否
- unidbg调用so文件 - SegmentFault 思否
- 菜鸡诈尸水贴之unidbg学习笔记 - 『移动安全区』 - 吾爱破解 - LCG - LSG |安卓破解|病毒分析|www.52pojie.cn
- Android逆向之旅---Hook神器家族的Frida工具使用详解 - Android应用安全防护和逆向分析-----作者 - CSDN博客
- 浅谈 android hook 技术 - Android - 掘金
- 使用Frida框架进行hook | La0s
- Android逆向之旅-Hook神器家族的Frida工具使用详解 - 云+社区 - 腾讯云
- hookmaster/frida-all-in-one: 《FRIDA操作手册》by @hluwa @r0ysue
- 详解Hook框架frida，让你在逆向工作中效率成倍提升 - 知乎
- Android Hook工具之Frida 基础使用 - 简书
- Understanding ELF using readelf and objdump (studylib.net)
- Executable and Linkable Format (ELF) (netmeister.org)
-