

关于 adb 的一些常用命令

在做 APP 安全测试时 (Android 端), 除了业务逻辑, 会经常要用到一些 adb 命令, 在此记录一下。

adb 下载地址: <https://adbshell.com/downloads>

一些思路小记

1、提取 apk 文件

1. 获取当前屏幕上正在运行的 APP 的包名和类名 (获取包名)

```
adb shell dumpsys window | grep mCurrentFocus
```

2. 获取某个应用的 apk 路径

```
adb shell pm path <pkg>
```

3. 让 adb 获得 root 权限

```
adb root
```

4. 提取 apk 文件到本地

```
adb pull <apk-path> <local-path>
```

如提取到当前目录 (./也可以省略不写)

```
adb pull /system/priv-app/Settings/Settings.apk ./
```

2、查看 logcat 日志信息

首推 Android Device Monitor , 很好用 (界面化工具), 可进行日志筛选、查找、导出等。

Tips: Android Device Monitor 已在 Android Studio 3.1 及以上版本中弃用, 可自行下载 [Android SDK 工具包](#)。

Android Device Monitor 启动脚本路径

<android-sdk-path>\tools\monitor.bat

另外就是通过命令来看了。

2.1 查看指定包名的 logcat 日志

打印指定包名的 logcat 日志

adb logcat | findstr <pkg>

输出到本地文件, 按 CTRL+C 停止。

adb logcat | findstr pkg > <path/file-name>

2.2 查看指定进程号的 logcat 日志

根据包名、服务名查找 PID

adb shell ps | grep <关键字, 可以是包名, 服务名等>

查看指定进程号的 logcat 日志

adb logcat --pid=<PID>

2.3 打印从某个时间点开始的系统日志

打印从某个时间点开始的系统日志

adb logcat -T "月-日 00:00:00.000" > <path/file-name>

如从 6 月 10 日 12 点这个时间点开始打印 logcat 日志

adb logcat -T "06-10 12:00:00.000" > logcat-06101200.txt

Android logcat 命令详解

<https://www.cnblogs.com/jianxu/p/5468839.html>

使用 `adb logcat` 命令显示 Android 设备上的 Log 日志

<https://blog.csdn.net/wenzhi20102321/article/details/81058196>

3、启动 APP 的方法

3.1 直接点击屏幕上的 APP 应用图标

3.2 借助 frida 强制重启 APP（使用于某些场景，如 无法点击 APP 图标）

`frida -U --no-pause -f <pkg>` # 只需知道包名即可，不需要知道类名

3.3 使用 adb 命令启动 APP

adb 启动应用程序命令

`adb shell am start -n <pkg>/<activity-name>`

`adb shell am start -n <pkg>/MainActivity`

参 考

Android 自动化之-ADB 与 ADB shell 常用命令

<https://cloud.tencent.com/developer/article/1543286>

ADB—查看设备信息

<https://www.jianshu.com/p/811741a2ad97>