Android 逆向工程筆記

# 工具簡介

## 基本工具

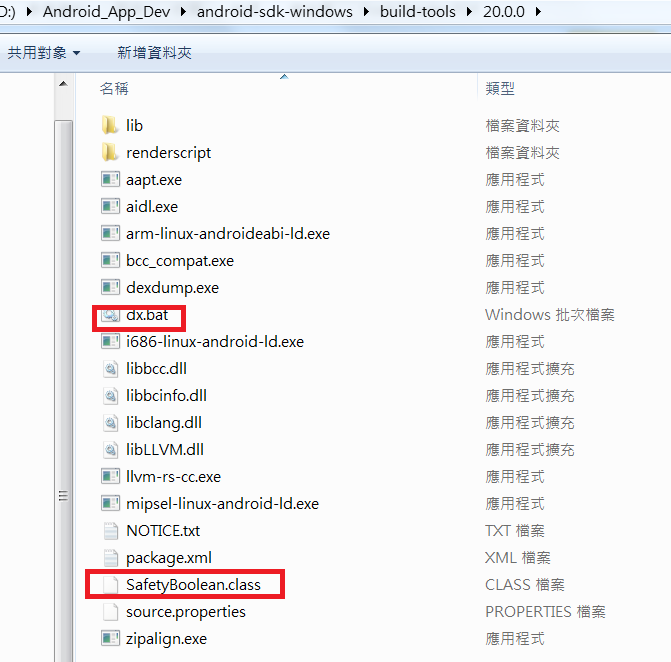
1. apktool: <https://ibotpeaches.github.io/Apktool/>
2. jd-gui: <http://java-decompiler.github.io/>
3. dex2jar: <https://sourceforge.net/projects/dex2jar/>
4. dedexer: <http://dedexer.sourceforge.net/>

## SDK 工具

1. dx: <sdk-path>\build-tools\<sdk-version>
2. aapt: <sdk-path>\build-tools\<sdk-version>
3. dexdump: <sdk-path>\build-tools\<sdk-version>

## 範例

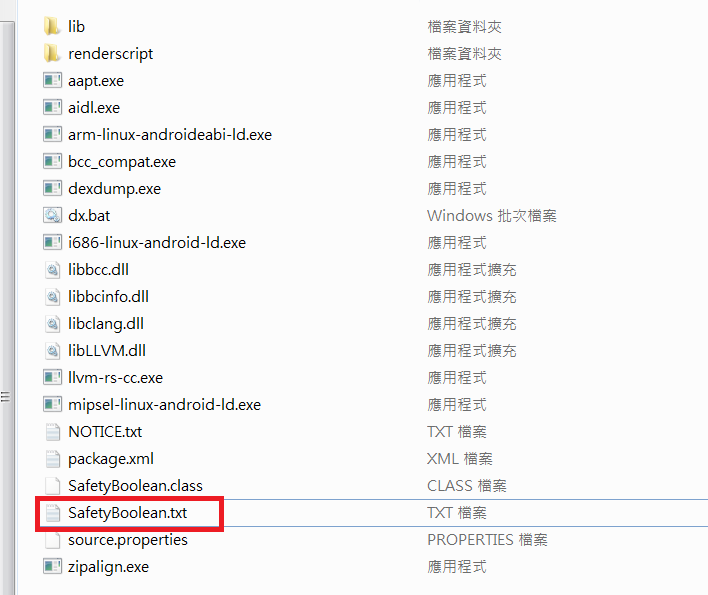
1. Dump class file



打開cmd並且下以下指令



之後就會產生一個dump file



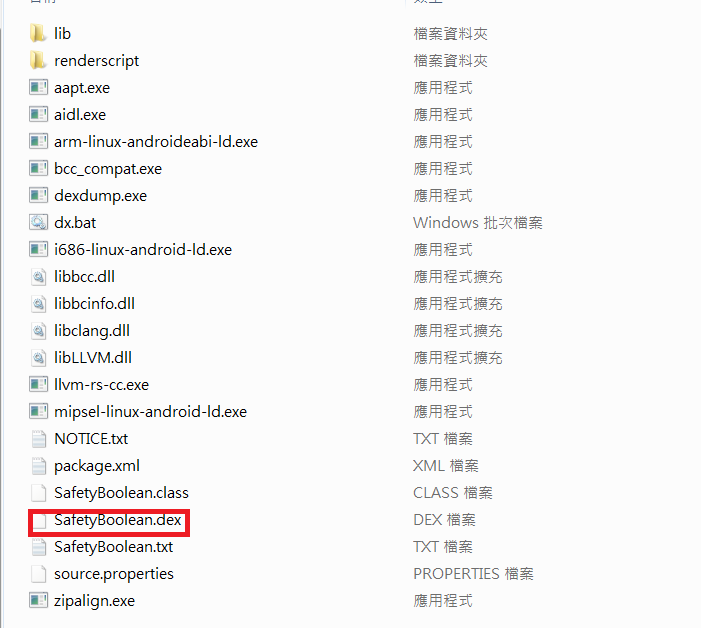
1. Dump dex to file

Class to dex file

打開cmd並且下以下指令



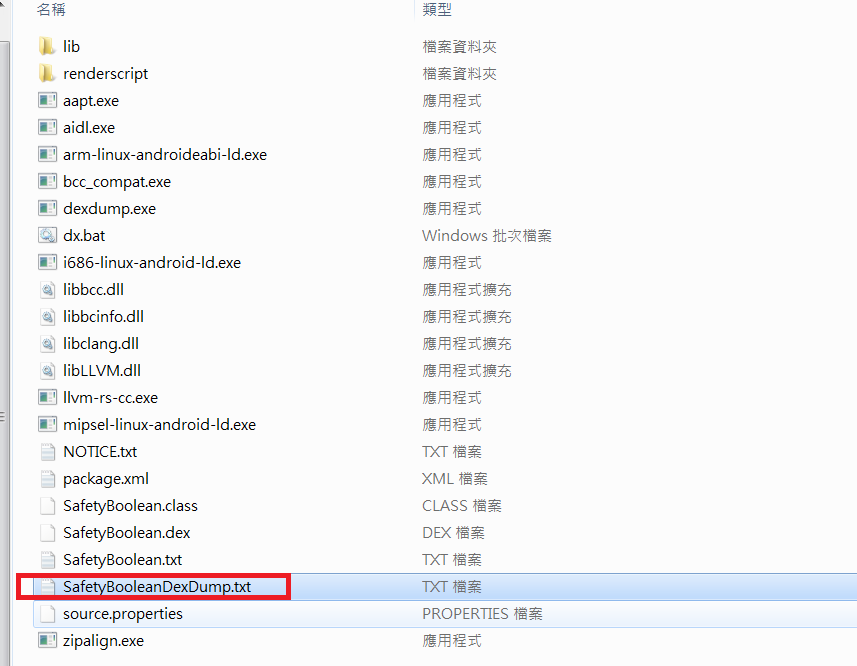
之後就會產生一個DEX file



Dex to file

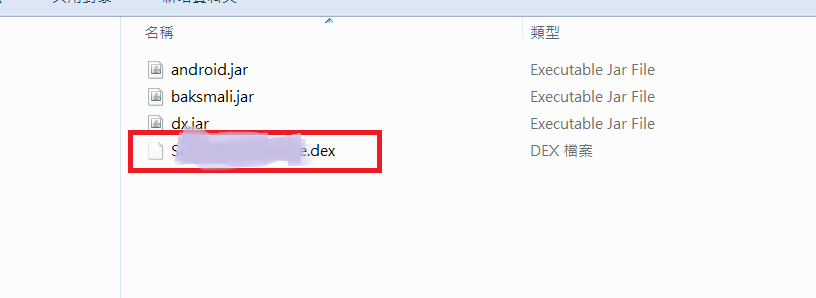


之後就會產生一個DEX dump file



1. Java convert to smali file

把dex file 放到AndroidDumpTool\lib



打開cmd並且下以下指令

java -jar baksmali.jar -o 資料夾名稱 dex file



產生 smali file

Ps: baksmali 可以下載 <https://github.com/fourbrother/java2smali>

附件



參考網站

<http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html>

<http://huli.logdown.com/posts/661513-android-apk-decompile>

<https://codertw.com/android-%E9%96%8B%E7%99%BC/354008/>

<http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html>

<https://docs.oracle.com/javase/specs/jvms/se7/html/jvms-6.html#jvms-6.5>

<https://github.com/fourbrother/java2smali>

<https://r8.googlesource.com/?format=HTML>

<http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html>

# Adb 指令

1. 在沒有root手機的情況下讀取Data目錄下的檔

|  |
| --- |
| **After android 8.0**  使用adb命令時的錯誤  如果直接使用adb命令會產生以下錯誤:  127|shell@android:/ $ cd /data  cd /data  shell@android:/data $ ls  ls  opendir failed, Permission denied  你是沒有許可權的。  正確使用adb讀取data目錄下的檔方式  shell@android:/data $ run-as com.your.package  run-as com.your.package  shell@android:/data/data/com.your.package $ cd /data/data/com.your.package  cd /data/data/com.your.package  shell@android:/data/data/com.your.package $ ls  ls  cache  databases  lib  shared\_prefs  shell@android:/data/data/com.your.package $ cd databases  cd databases  shell@android:/data/data/com.your.package/databases $ ls  yourpackagename.db  $ cat preferences.db > /mnt/sdcard/yourpackagename.db  將你要訪問的package目錄下的db檔拷貝到sdcard中，這樣就可以正常訪問了！  ---------------------  作者：Snowball  來源：CSDN  原文：https://blog.csdn.net/yangzl2008/article/details/8498196  版權聲明：本文為博主原創文章，轉載請附上博文連結！ |

1. Android adb bugreport工具分析和使用

|  |
| --- |
| **Before android 8.0**  adb bugreport > [file path] ps: Suggestion use the sdk version before android 8.0    **After android 8.0**  adb bugreport  adb pull [bug report zip file] [dest\_file\_path]    **異常1**  這裡我出現一個異常：當前SDK最新版本為7.0(25)，而我的手機系統版本為5.0，所以使用命令列：**adb bugreport > report.txt**時出現了如下異常：  **Failed to get bugreportz version, which is only available on devices running Android 7.0 or later.**  這是由於SDK版本太新了，既然手機系統不能升級，那就只好把SDK降級，  其實這裡只是使用了plantform下的adb命令，所以從新下載**platform-tools**即可。  我下載和手機系統版本一致的platform-tools，然後解壓。使用新下載的platform-tools的adb命令執行adb bugreport > out.txt時提示沒有設備。  **異常2**  又使用**adb devices**查看列表仍然沒有。重啟adb也沒用效果。  因為我的是Mac設備，所以命令列執行system\_profiler SPUSBDataType時會顯示一系列外接設備資訊，找到你的Android設備，複製Vendor ID。  進入你下載的低版本**platform-tools**資料夾下，修改或創建**adb\_usb.ini**檔，把剛才複製的Vendor ID粘貼到這裡。再次執行**adb devices**就可以查看到設備清單了。然後再次執行adb bugreport > out.txt就會產生一個設備耗能統計資訊檔。  **注意**  匯出電量統計資料是一個持續輸出的過程，就是說如果你不手動停止，那會一直統計。所以看到檔中已經寫入內容後就可以CTRL+C了。  **Bugreport 分析**  Reference: <https://blog.csdn.net/createchance/article/details/51954142> |

1. 利用adb shell來觀看device中的process和thread

|  |
| --- |
| **Before android 8.0**  Open the command line and check adb connection status by adb devices  Process   * adb shell * ps     Thread   * Get the specified pid by ps command * Ps –t [pid]     **After android 8.0**  Open the command line and check adb connection status by adb devices  Process   * adb shell * ps -A     Thread   * adb shell * ps -A * get user name from process list * ps -AT | grep [user name]     Type the commend ps –help    Reference: <https://blog.csdn.net/RadianceBlau/article/details/77855149> |