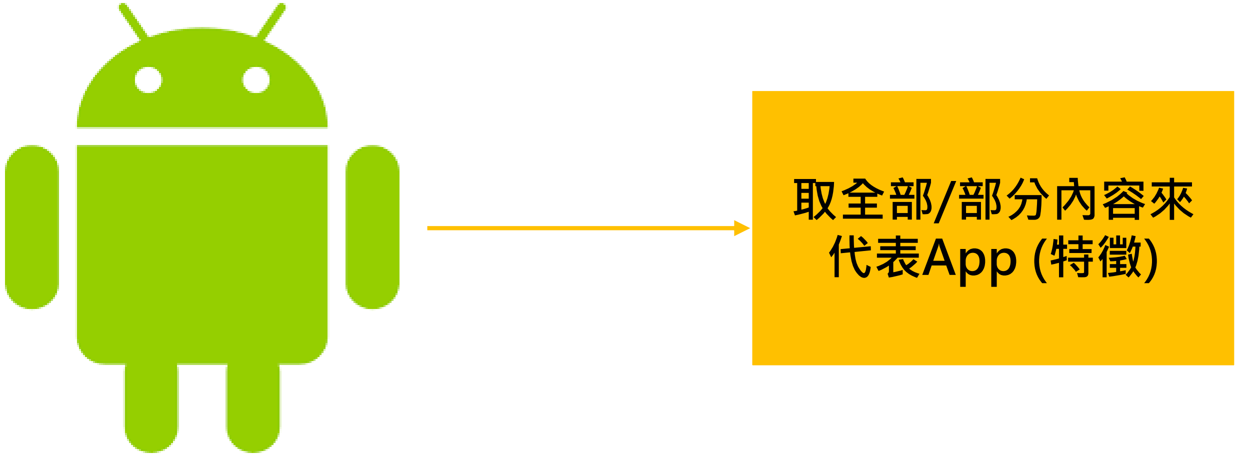
HW10

Android Malware Classification - Feature



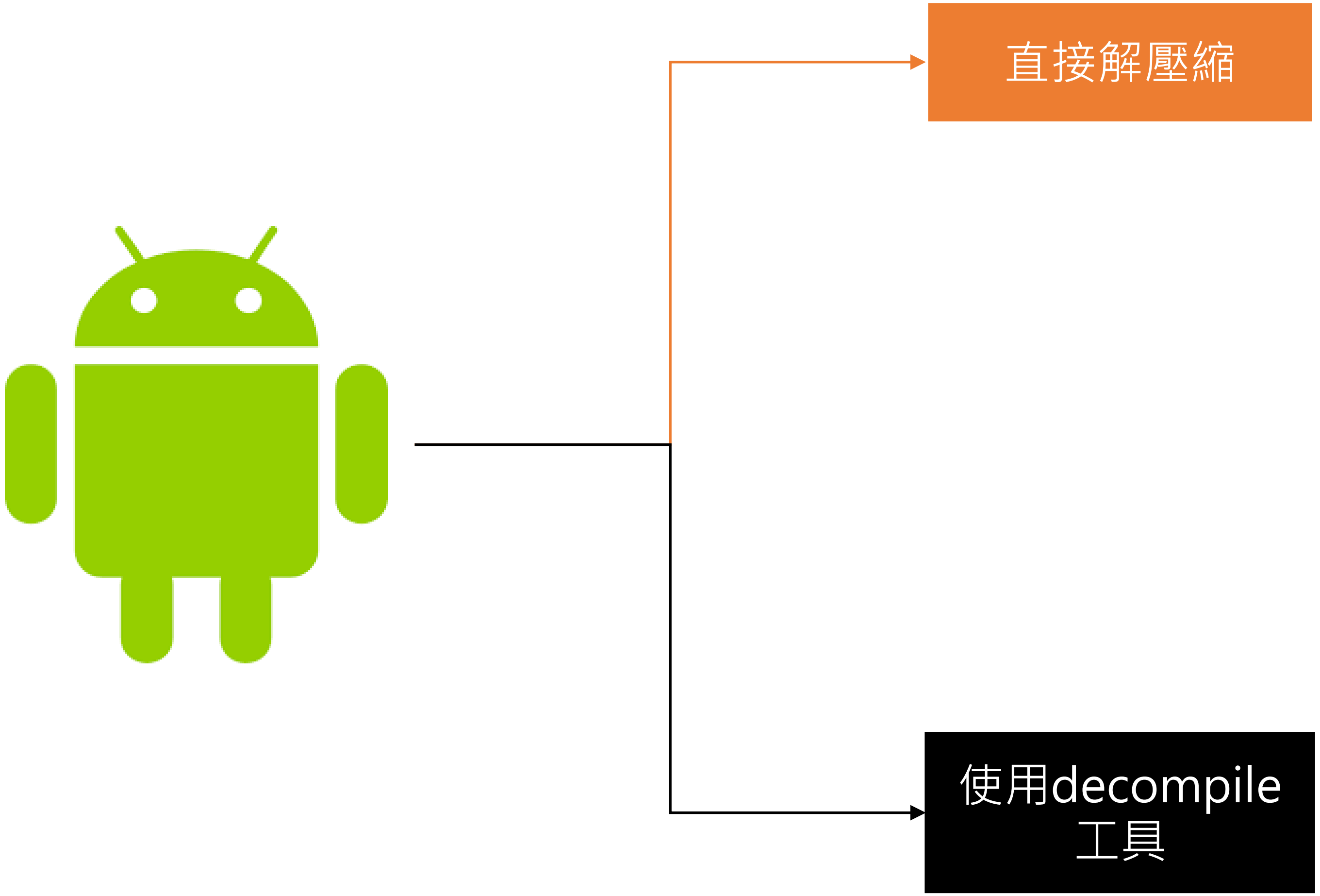
取全部/部分內容來代表App (特徵)

想取什麼內容當特徵都可以

1. Permission
2. API call
3. Op code
4. Intent
5. Inter-Component Communication
6. System call
7. Network usage
8. Dex file
9. Entire apk

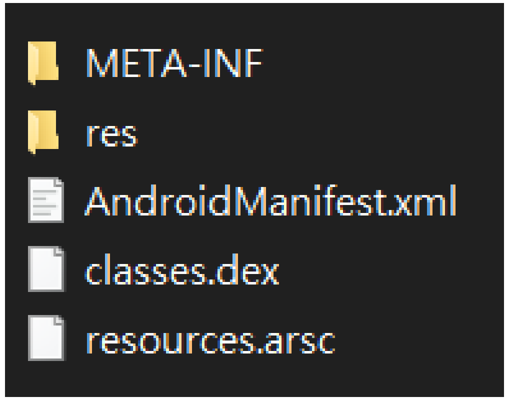
…, etc.

Android Malware Classification - Feature

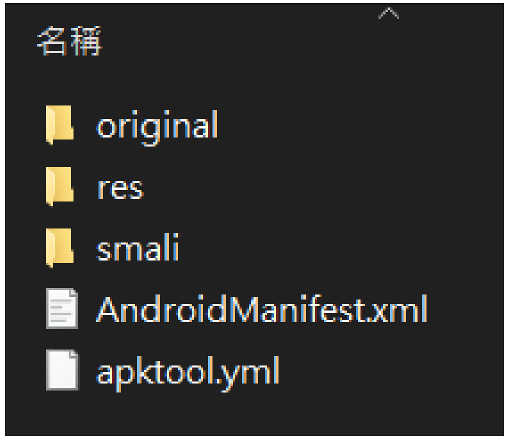


直接解壓縮

使用decompile 工具



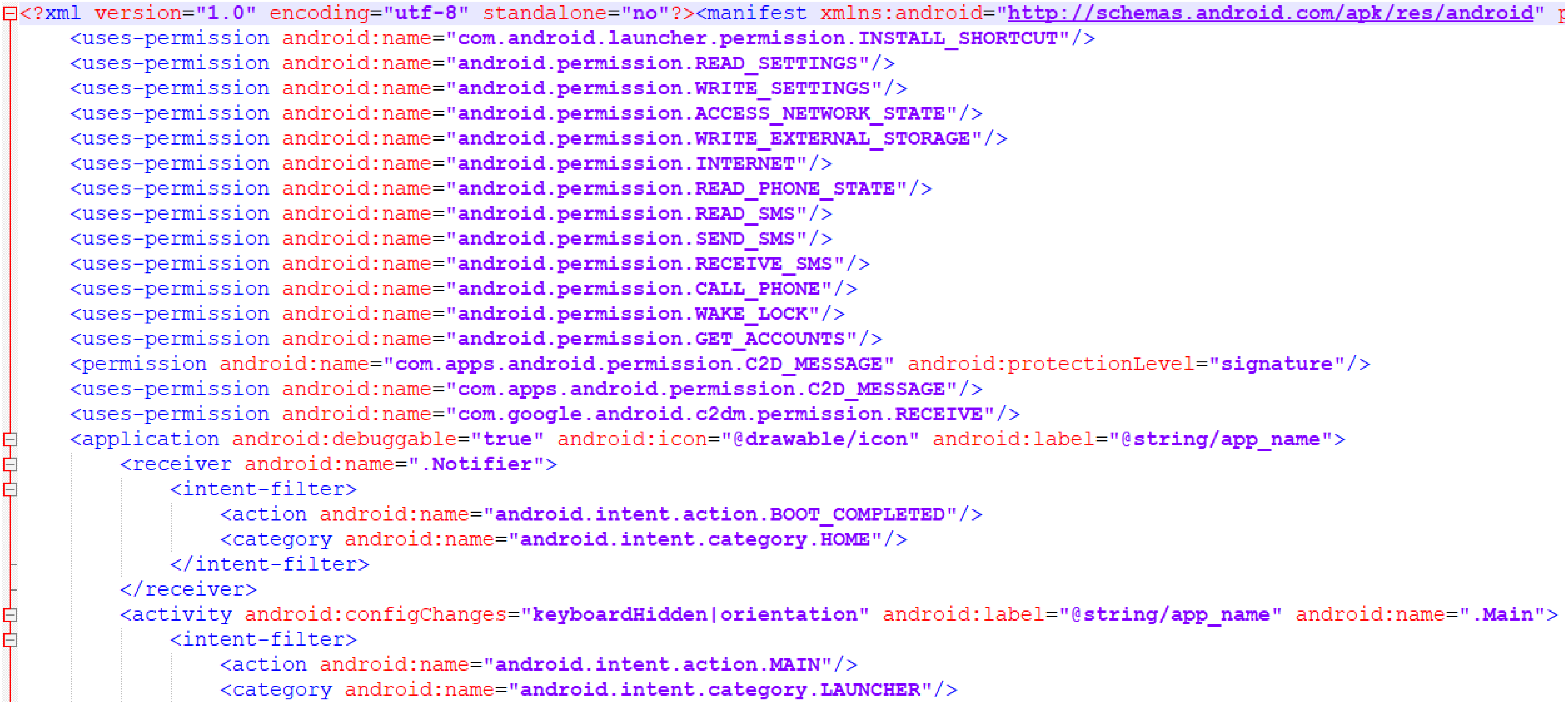
- META-INF
- res
- AndroidManifest.xml
- classes.dex
- resources.arsc



名稱

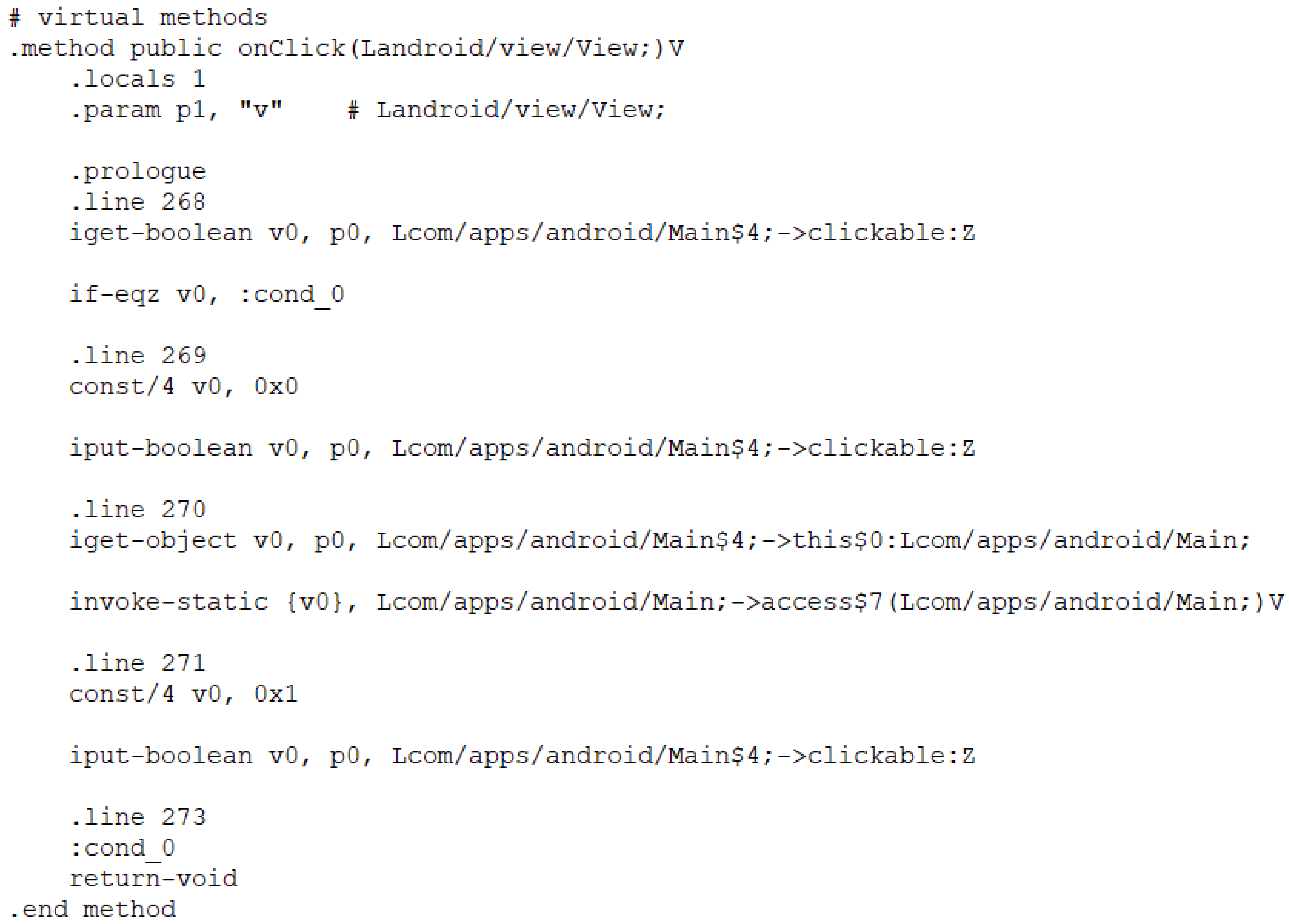
- original
- res
- smali
- AndroidManifest.xml
- apktool.yml

AndroidManifest.xml



```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" p
    <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
    <uses-permission android:name="android.permission.READ_SETTINGS"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <permission android:name="com.apps.android.permission.C2D_MESSAGE" android:protectionLevel="signature"/>
    <uses-permission android:name="com.apps.android.permission.C2D_MESSAGE"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <application android:debuggable="true" android:icon="@drawable/icon" android:label="@string/app_name">
        <receiver android:name=".Notifier">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED"/>
                <category android:name="android.intent.category.HOME"/>
            </intent-filter>
        </receiver>
        <activity android:configChanges="keyboardHidden|orientation" android:label="@string/app_name" android:name=".Main">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
```

Smali files

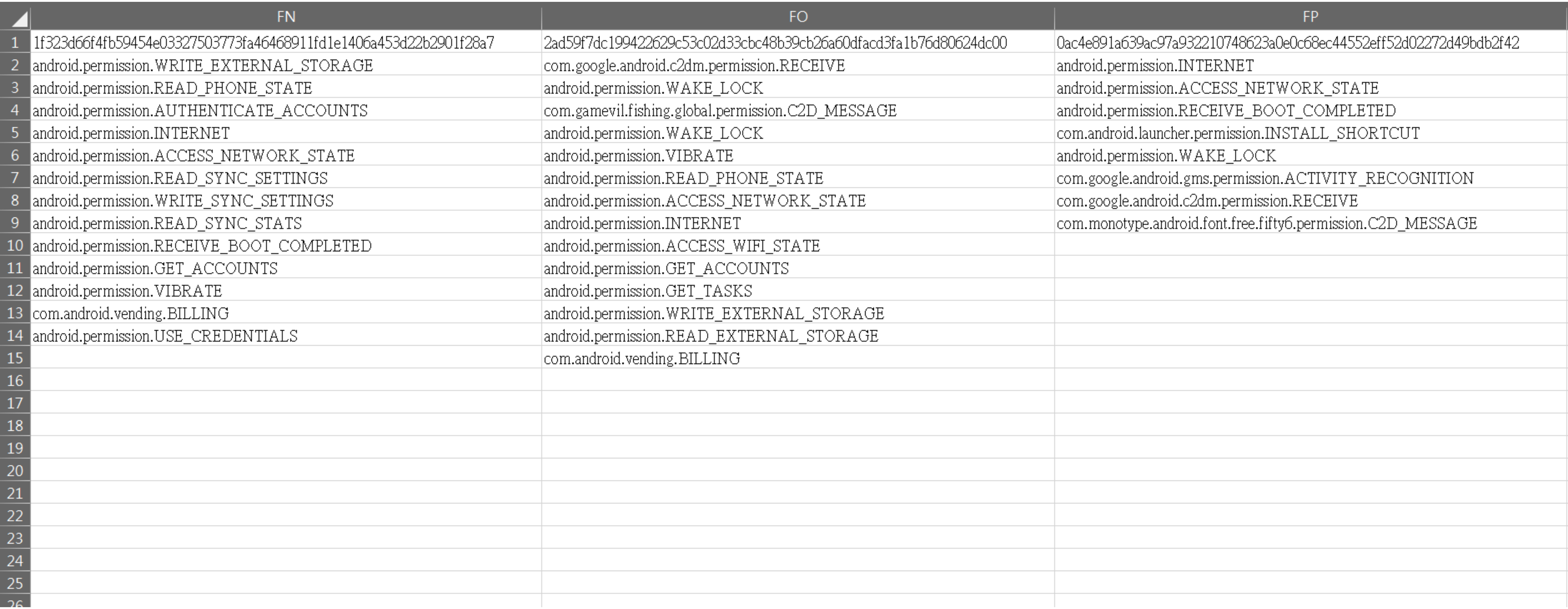


```
# virtual methods
.method public onClick(Landroid/view/View;)V
    .locals 1
    .param p1, "v"    # Landroid/view/View;

    .prologue
    .line 268
    iget-boolean v0, p0, Lcom/apps/android/Main$4;->clickable:Z

    if-eqz v0, :cond_0

    .line 269
    const/4 v0, 0x0

    iput-boolean v0, p0, Lcom/apps/android/Main$4;->clickable:Z

    .line 270
    iget-object v0, p0, Lcom/apps/android/Main$4;->this$0:Lcom/apps/android/Main;

    invoke-static {v0}, Lcom/apps/android/Main;->access$7(Lcom/apps/android/Main;)V

    .line 271
    const/4 v0, 0x1

    iput-boolean v0, p0, Lcom/apps/android/Main$4;->clickable:Z

    .line 273
    :cond_0
    return-void
.end method
```

取特徵

1. **Decompile工具 - APKTool**
   - `apktool d xxx.apk`
   - Windows / linux / macOS

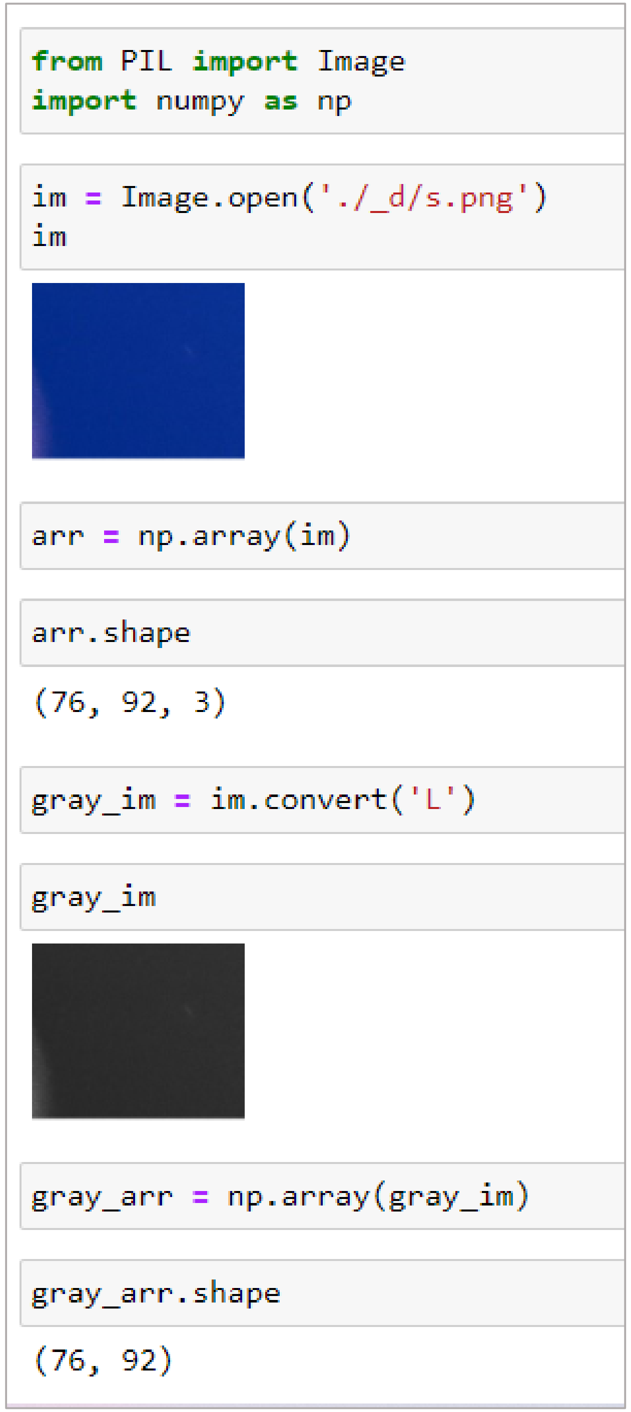
2. **假如要取permission** (以下兩種方式)
   1) 用apktool decompile後寫python去parse xml
   2) 直接用android靜態分析工具 (e.g. AndroGuard等)



	FN	FO	FP
1	1f323d66f4fb59454e03327503773fa46468911fd1e1406a453d22b2901f28a7	2ad59f7dc199422629c53c02d33cbc48b39cb26a60dfacd3fa1b76d80624dc00	0ac4e891a639ac97a932210748623a0e0c68ec44552eff52d02272d49bdb2f42
2	android.permission.WRITE_EXTERNAL_STORAGE	com.google.android.c2dm.permission.RECEIVE	android.permission.INTERNET
3	android.permission.READ_PHONE_STATE	android.permission.WAKE_LOCK	android.permission.ACCESS_NETWORK_STATE
4	android.permission.AUTHENTICATE_ACCOUNTS	com.gamevil.fishing.global.permission.C2D_MESSAGE	android.permission.RECEIVE_BOOT_COMPLETED
5	android.permission.INTERNET	android.permission.WAKE_LOCK	com.android.launcher.permission.INSTALL_SHORTCUT
6	android.permission.ACCESS_NETWORK_STATE	android.permission.VIBRATE	android.permission.WAKE_LOCK
7	android.permission.READ_SYNC_SETTINGS	android.permission.READ_PHONE_STATE	com.google.android.gms.permission.ACTIVITY_RECOGNITION
8	android.permission.WRITE_SYNC_SETTINGS	android.permission.ACCESS_NETWORK_STATE	com.google.android.c2dm.permission.RECEIVE
9	android.permission.READ_SYNC_STATS	android.permission.INTERNET	com.monotype.android.font.free.fifty6.permission.C2D_MESSAGE
10	android.permission.RECEIVE_BOOT_COMPLETED	android.permission.ACCESS_WIFI_STATE	
11	android.permission.GET_ACCOUNTS	android.permission.GET_ACCOUNTS	
12	android.permission.VIBRATE	android.permission.GET_TASKS	
13	com.android.vending.BILLING	android.permission.WRITE_EXTERNAL_STORAGE	
14	android.permission.USE_CREDENTIALS	android.permission.READ_EXTERNAL_STORAGE	
15		com.android.vending.BILLING	
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

CNN

一般圖片的樣子



```
from PIL import Image
import numpy as np
```

```
im = Image.open('./_d/s.png')
im
```

```
arr = np.array(im)
```

```
arr.shape
```

```
(76, 92, 3)
```

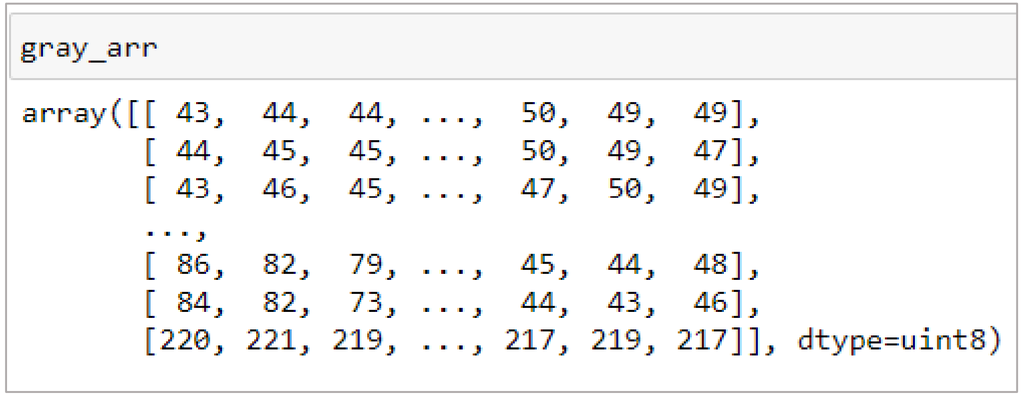
```
gray_im = im.convert('L')
```

```
gray_im
```

```
gray_arr = np.array(gray_im)
```

```
gray_arr.shape
```

```
(76, 92)
```

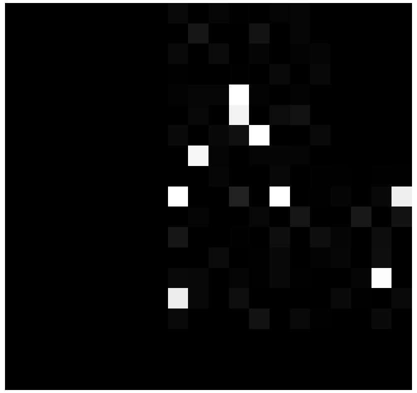


```
gray_arr
```

```
array([[ 43,  44,  44, ...,  50,  49,  49],
       [ 44,  45,  45, ...,  50,  49,  47],
       [ 43,  46,  45, ...,  47,  50,  49],
       ...,
       [ 86,  82,  79, ...,  45,  44,  48],
       [ 84,  82,  73, ...,  44,  43,  46],
       [220, 221, 219, ..., 217, 219, 217]], dtype=uint8)
```

gray_arr為一個灰階圖片，是一個二維陣列。將原本的android特徵排列成像這樣的二維陣列，就變成圖片了。

permission to Img



Dex file to Img