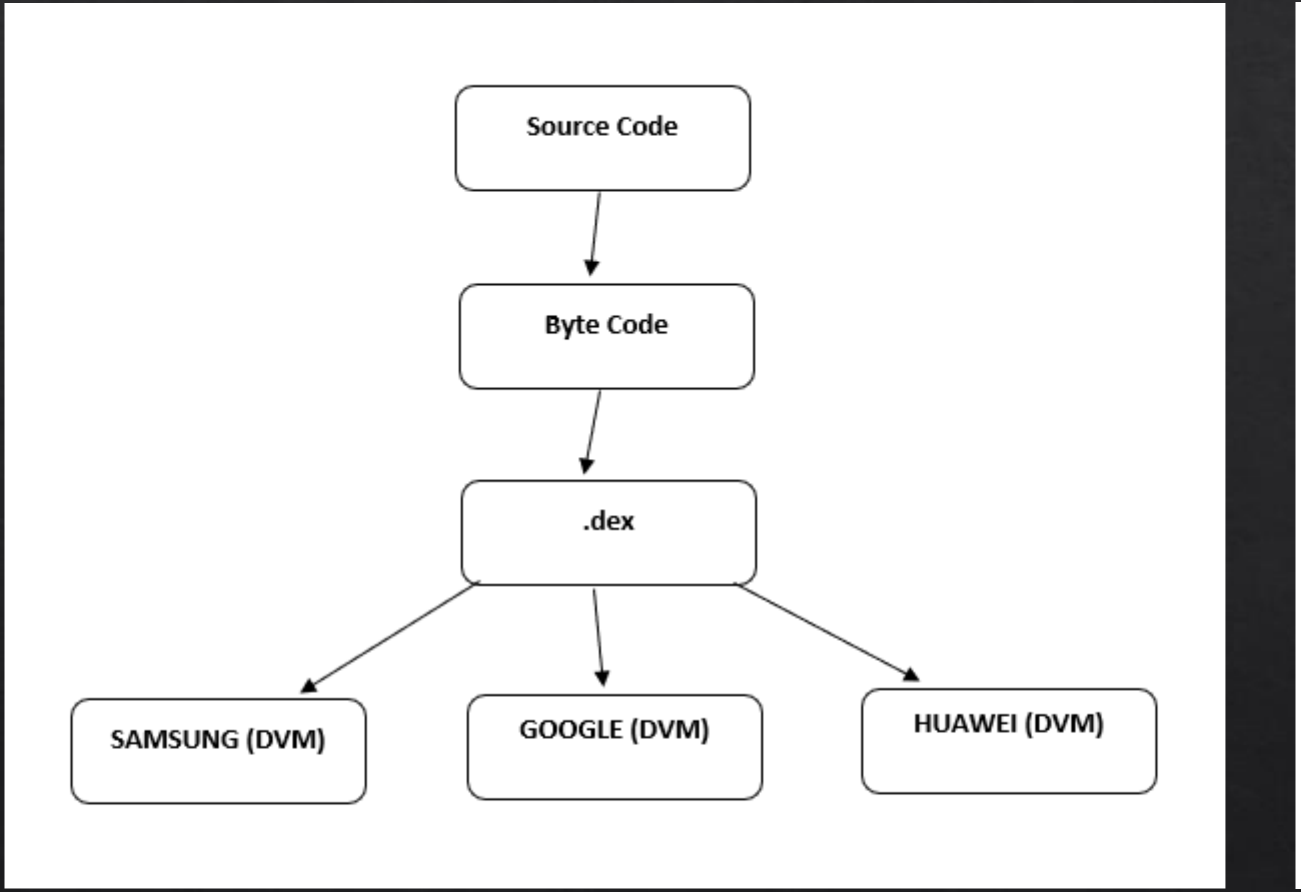
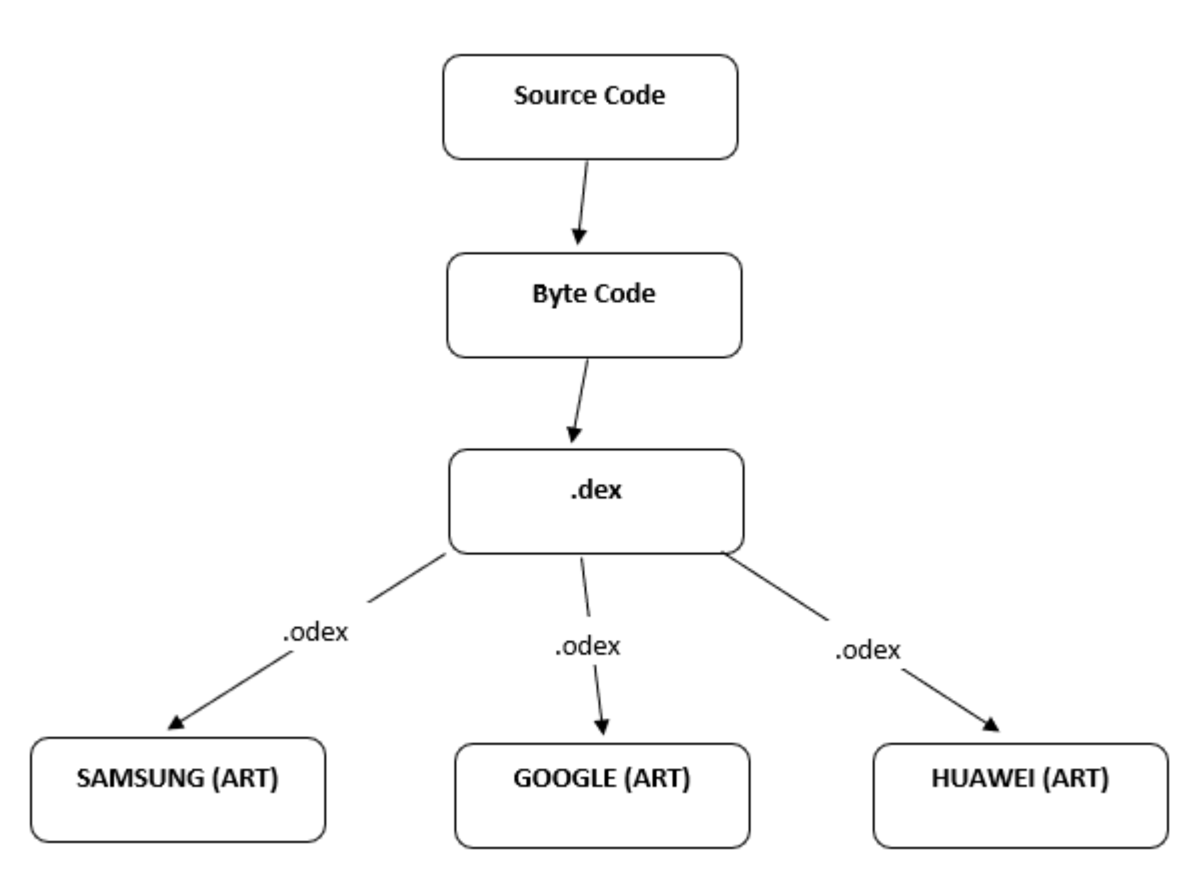
Old Android compilation process



Current Android compilation process



What’s an APK?

- Stands for Android Package
- It’s the .exe equivalent of Android OS
- It’s a ZIP file so you can simply run UNZIP command to extract the contents of this file
- Contains all of the source code, resources and other important files that helps to run an app
- Key components of an APK file are:
  - AndroidManifest.XML
  - Classes.dex
  - resources.arsc
  - res
  - META-INF

APK internals

AndroidManifest.xml

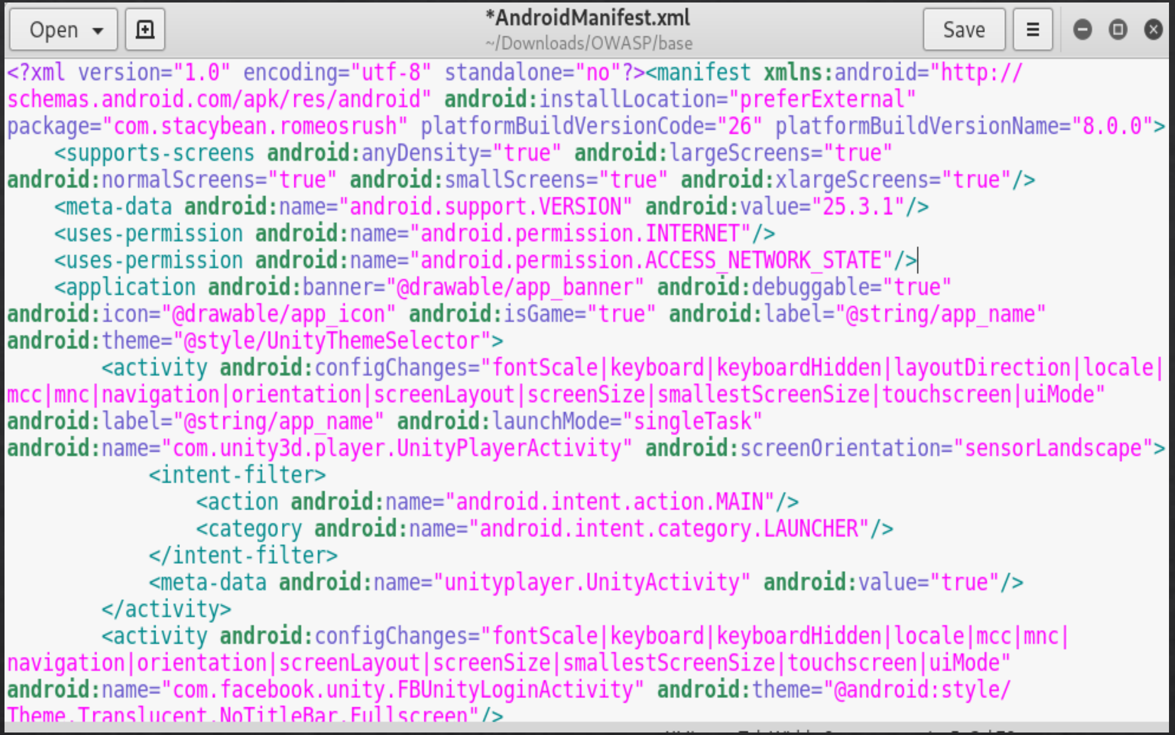
- It provides information that a device needs in order to run the app
- Permissions that an application has
- List all of the activities, services, broadcast receivers etc.

Classes.dex

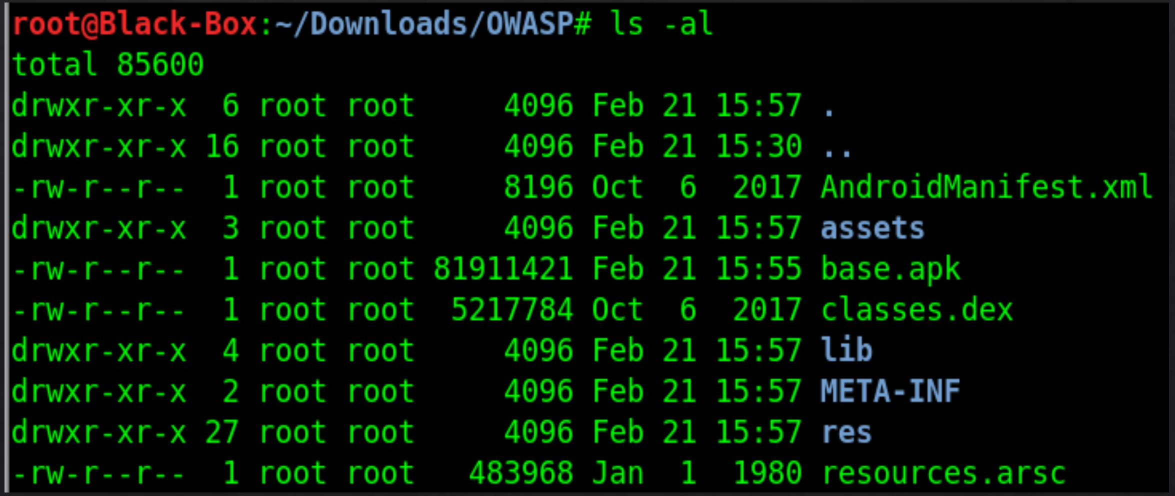
- It contains Java bytecode in DEX (Dalvik Exchange) format

res

- It contains device configuration, Bitmaps and Layouts



```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://
schemas.android.com/apk/res/android" android:installLocation="preferExternal"
package="com.stacybean.romeosrush" platformBuildVersionCode="26" platformBuildVersionName="8.0.0">
    <supports-screens android:anyDensity="true" android:largeScreens="true"
android:normalScreens="true" android:smallScreens="true" android:xlargeScreens="true"/>
    <meta-data android:name="android.support.VERSION" android:value="25.3.1"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <application android:banner="@drawable/app_banner" android:debuggable="true"
android:icon="@drawable/app_icon" android:isGame="true" android:label="@string/app_name"
android:theme="@style/UnityThemeSelector">
        <activity android:configChanges="fontScale|keyboard|keyboardHidden|layoutDirection|locale|
mcc|mnc|navigation|orientation|screenLayout|screenSize|smallestScreenSize|touchscreen|uiMode"
android:label="@string/app_name" android:launchMode="singleTask"
android:name="com.unity3d.player.UnityPlayerActivity" android:screenOrientation="sensorLandscape">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
            <meta-data android:name="unityplayer.UnityActivity" android:value="true"/>
        </activity>
        <activity android:configChanges="fontScale|keyboard|keyboardHidden|locale|mcc|mnc|
navigation|orientation|screenLayout|screenSize|smallestScreenSize|touchscreen|uiMode"
android:name="com.facebook.unity.FBUnityLoginActivity" android:theme="@android:style/
Theme.Translucent.NoTitleBar.Fullscreen"/>
```



```
root@Black-Box:~/Downloads/OWASP# ls -al
total 85600
drwxr-xr-x  6 root root     4096 Feb 21 15:57 .
drwxr-xr-x 16 root root     4096 Feb 21 15:30 ..
-rw-r--r--  1 root root     8196 Oct  6  2017 AndroidManifest.xml
drwxr-xr-x  3 root root     4096 Feb 21 15:57 assets
-rw-r--r--  1 root root 81911421 Feb 21 15:55 base.apk
-rw-r--r--  1 root root  5217784 Oct  6  2017 classes.dex
drwxr-xr-x  4 root root     4096 Feb 21 15:57 lib
drwxr-xr-x  2 root root     4096 Feb 21 15:57 META-INF
drwxr-xr-x 27 root root     4096 Feb 21 15:57 res
-rw-r--r--  1 root root   483968 Jan  1  1980 resources.arsc
```

resources.arsc

- **Contains compiled resources in a binary format**
- **May also include images, strings, or other data used by an app**

META-INF

This folder contains the manifest information and other metadata about the java package carried by the jar file.

- *MANIFEST.MF: It contains various information used by the java run-time environment when loading the jar file, such as which is the main class to be run from the jar file, version of package, build number, creator of the package, security policies/permissions of java applets and the list of file names in the jar along with their SHA1 digests, etc.*
- *CERT.SF: This contains the list of all files along with their SHA-1 digest.*
- *CERT.RSA: This contains the signed contents of the CERT.SF file along with the certificate chain of the public key used for signing the contents.*

Enough..Let’s Reverse Engineer an app

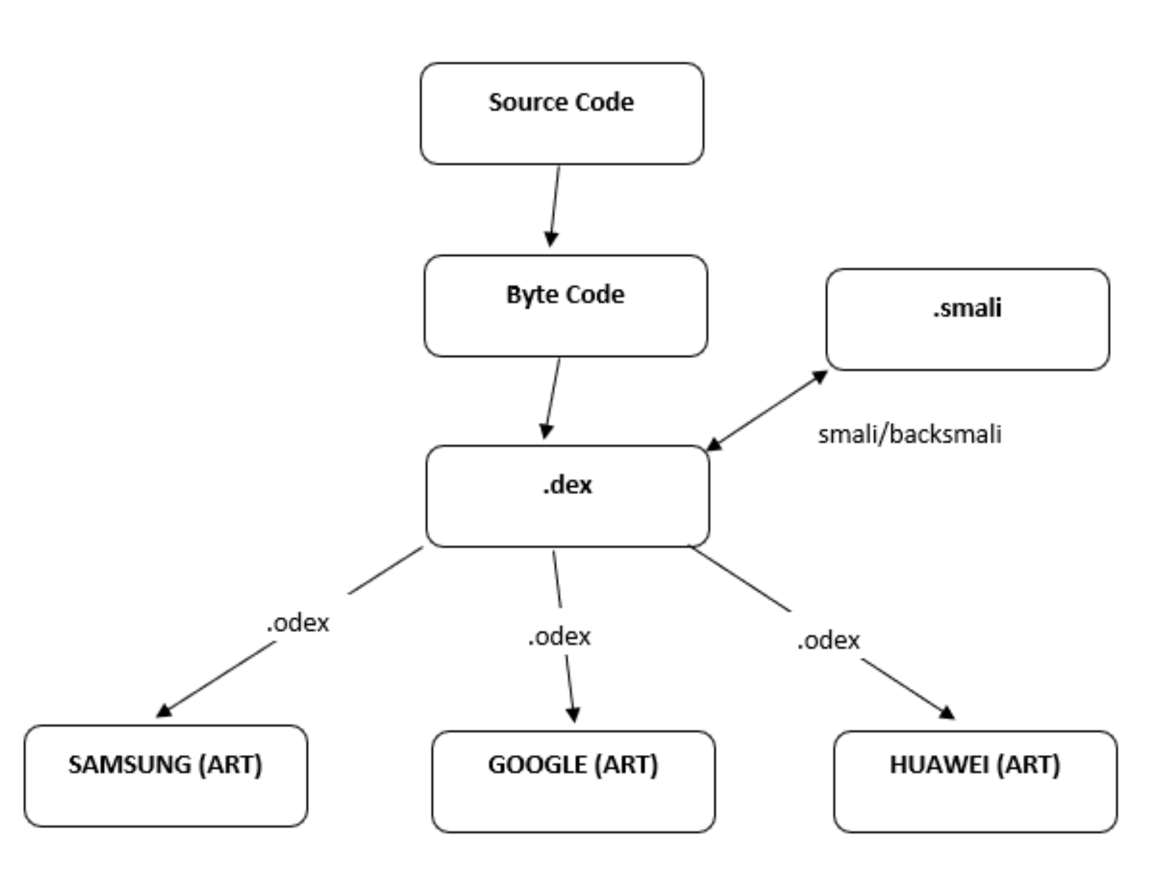
BUT WAIT…..We need tools ☹

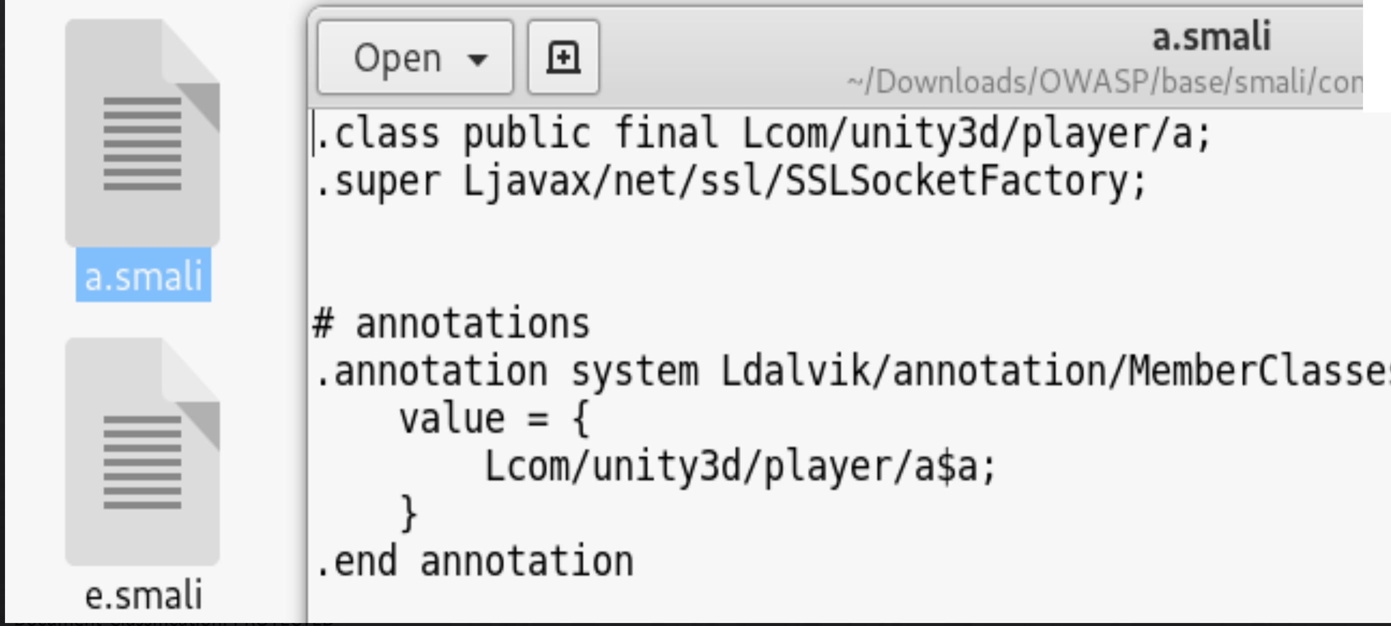
Here you go:

- A working Android Phone (you can get away with an Emulator)
- Of course an APK file
- APKTOOL – Disassemble and builds APK files
- d2j-dex2jar – Turns an APK into JAR file
- jADX – Similar to dex2jar but allows string/symbol search
- JD-GUI – To view the JAR file
- Android-Studio – IDE environment for Android apps
- adb – Android SDK tool to install/uninstall APKs on mobiles and an Emulator
- Sign or Jarsigner – To sign an app

SMALI

- Assembly language that gets compiled into .dex format
- You should use smali to patch your applications
- Smali/Baksmali is an assembler/disassembler for the dex format used by dalvik, Android's Java VM implementation.

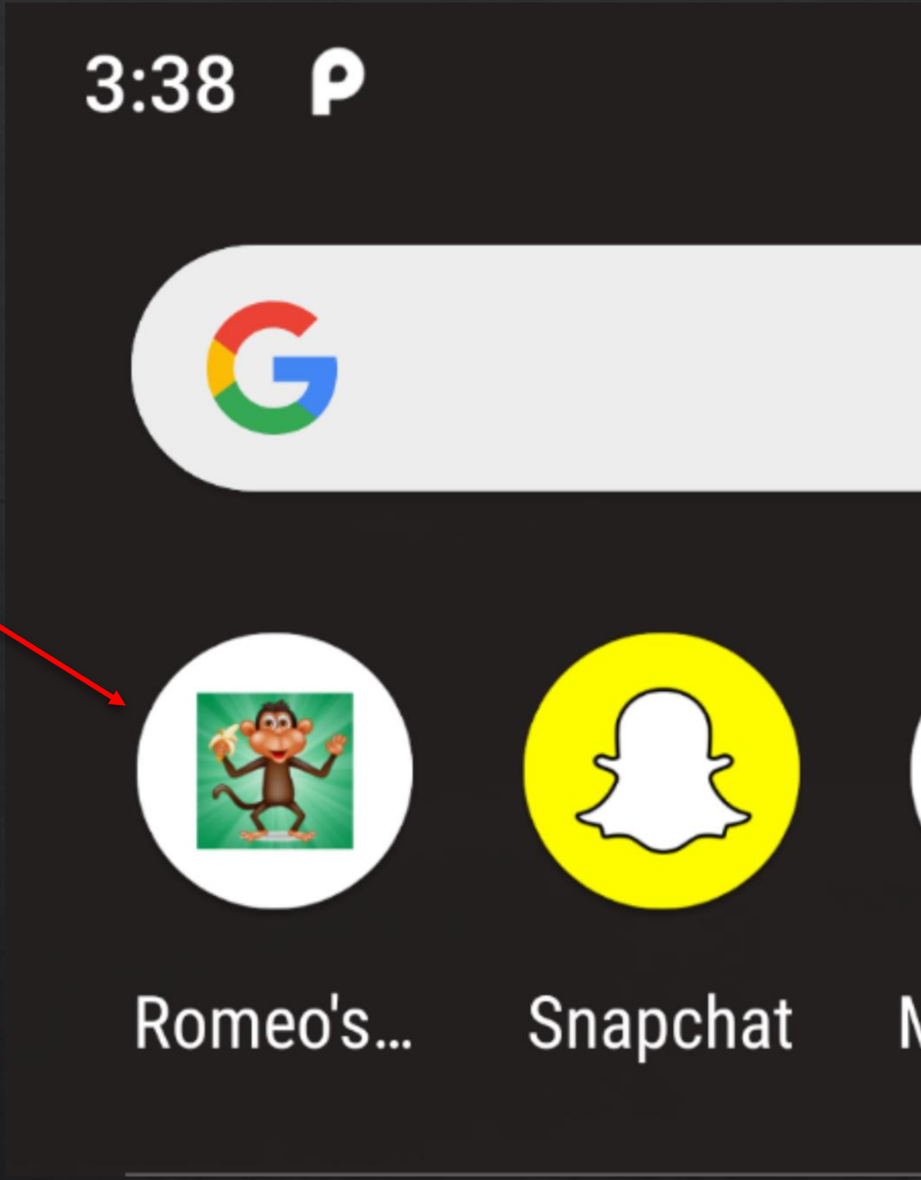




```
.class public final Lcom/unity3d/player/a;
.super Ljavax/net/ssl/SSLSocketFactory;


# annotations
.annotation system Ldalvik/annotation/MemberClasses;
    value = {
        Lcom/unity3d/player/a$a;
    }
.end annotation
```

Special thanks to my friend (Stacy Bean) who let me reverse engineer his app ☺

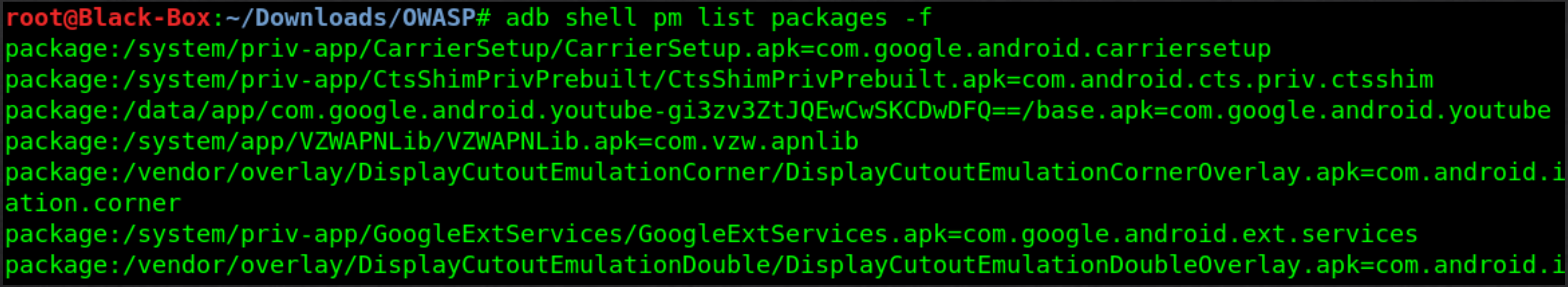


Steps to pull an APK from your mobile :

- Make sure you have developer mode enabled on your mobile phone
- Turn on the USB debugging
- Connect your phone to your laptop and allow your phone’s USB mode to File Transfer
- Run the following commands on your laptop:

To list the installed packages:

adb shell pm list packages –f



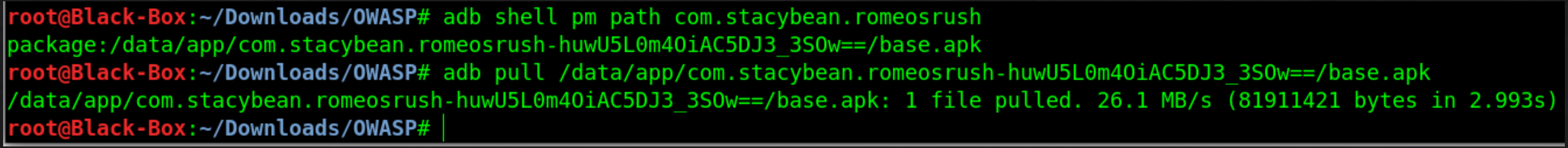
```
root@Black-Box:~/Downloads/OWASP# adb shell pm list packages -f
package:/system/priv-app/CarrierSetup/CarrierSetup.apk=com.google.android.carriersetup
package:/system/priv-app/CtsShimPrivPrebuilt/CtsShimPrivPrebuilt.apk=com.android.cts.priv.ctsshim
package:/data/app/com.google.android.youtube-gi3zv3ZtJQEwCwSKCDwDFQ==/base.apk=com.google.android.youtube
package:/system/app/VZWAPNLib/VZWAPNLib.apk=com.vzw.apnlib
package:/vendor/overlay/DisplayCutoutEmulationCorner/DisplayCutoutEmulationCornerOverlay.apk=com.android.i
ation.corner
package:/system/priv-app/GoogleExtServices/GoogleExtServices.apk=com.google.android.ext.services
package:/vendor/overlay/DisplayCutoutEmulationDouble/DisplayCutoutEmulationDoubleOverlay.apk=com.android.i
```

To find the APK path:

adb shell pm path <name of your package>

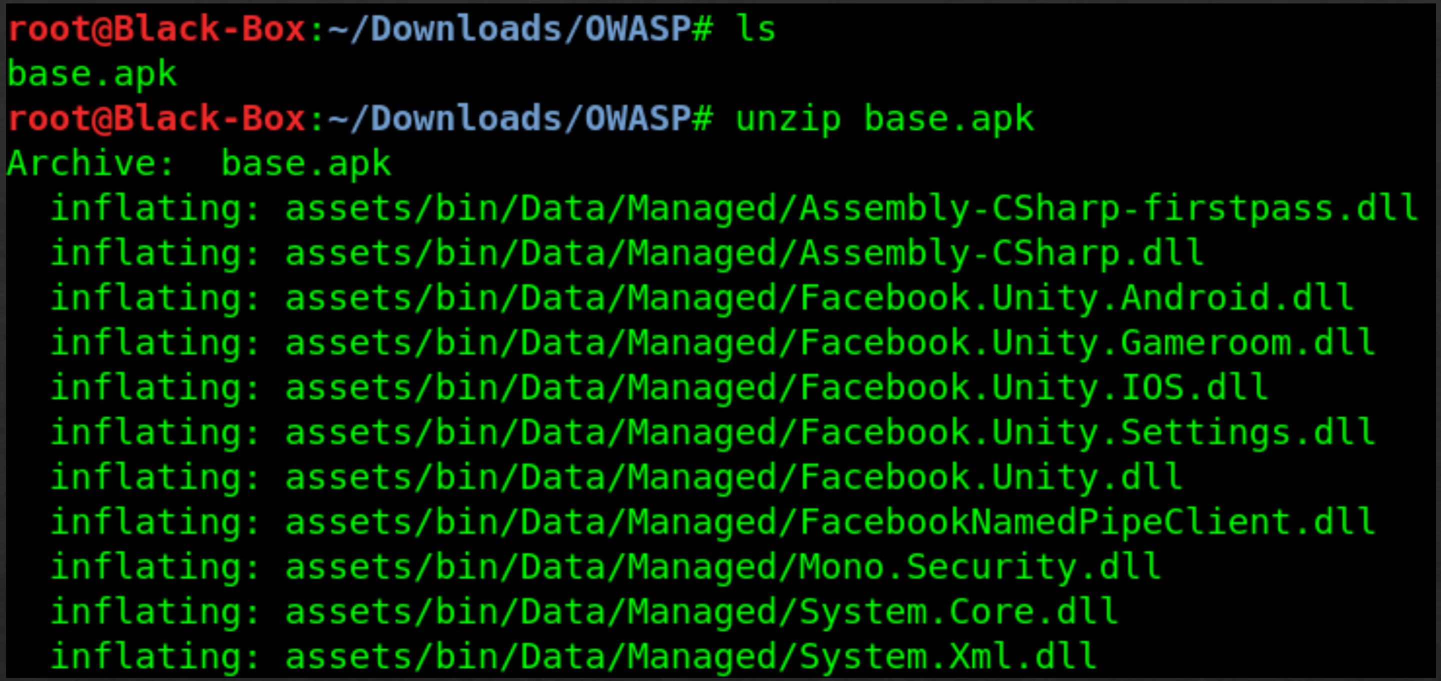
To pull a package and copy it to your laptop:

adb pull /data/app/com.randomname.packagename4I43KfdzneH_QYwRGqYQ==/base.apk /root/Downloads/Test



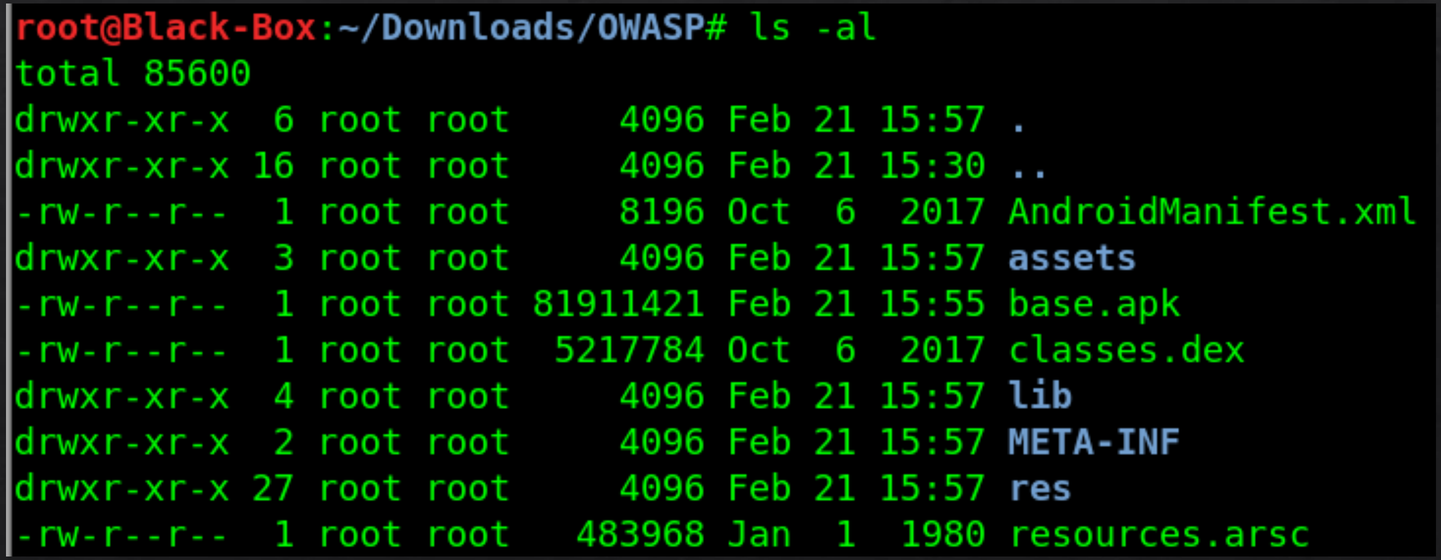
```
root@Black-Box:~/Downloads/OWASP# adb shell pm path com.stacybean.romeosrush
package:/data/app/com.stacybean.romeosrush-huwU5L0m4OiAC5DJ3_3SOw==/base.apk
root@Black-Box:~/Downloads/OWASP# adb pull /data/app/com.stacybean.romeosrush-huwU5L0m4OiAC5DJ3_3SOw==/base.apk
/data/app/com.stacybean.romeosrush-huwU5L0m4OiAC5DJ3_3SOw==/base.apk: 1 file pulled. 26.1 MB/s (81911421 bytes in 2.993s)
root@Black-Box:~/Downloads/OWASP#
```

Listing and Unzipping an APK file →



```
root@Black-Box:~/Downloads/OWASP# ls
base.apk
root@Black-Box:~/Downloads/OWASP# unzip base.apk
Archive:  base.apk
  inflating: assets/bin/Data/Managed/Assembly-CSharp-firstpass.dll
  inflating: assets/bin/Data/Managed/Assembly-CSharp.dll
  inflating: assets/bin/Data/Managed/Facebook.Unity.Android.dll
  inflating: assets/bin/Data/Managed/Facebook.Unity.Gameroom.dll
  inflating: assets/bin/Data/Managed/Facebook.Unity.IOS.dll
  inflating: assets/bin/Data/Managed/Facebook.Unity.Settings.dll
  inflating: assets/bin/Data/Managed/Facebook.Unity.dll
  inflating: assets/bin/Data/Managed/FacebookNamedPipeClient.dll
  inflating: assets/bin/Data/Managed/Mono.Security.dll
  inflating: assets/bin/Data/Managed/System.Core.dll
  inflating: assets/bin/Data/Managed/System.Xml.dll
```

Listing the contents of an Unzipped APK file →



```
root@Black-Box:~/Downloads/OWASP# ls -al
total 85600
drwxr-xr-x  6 root root     4096 Feb 21 15:57 .
drwxr-xr-x 16 root root     4096 Feb 21 15:30 ..
-rw-r--r--  1 root root     8196 Oct  6  2017 AndroidManifest.xml
drwxr-xr-x  3 root root     4096 Feb 21 15:57 assets
-rw-r--r--  1 root root 81911421 Feb 21 15:55 base.apk
-rw-r--r--  1 root root  5217784 Oct  6  2017 classes.dex
drwxr-xr-x  4 root root     4096 Feb 21 15:57 lib
drwxr-xr-x  2 root root     4096 Feb 21 15:57 META-INF
drwxr-xr-x 27 root root     4096 Feb 21 15:57 res
-rw-r--r--  1 root root   483968 Jan  1  1980 resources.arsc
```