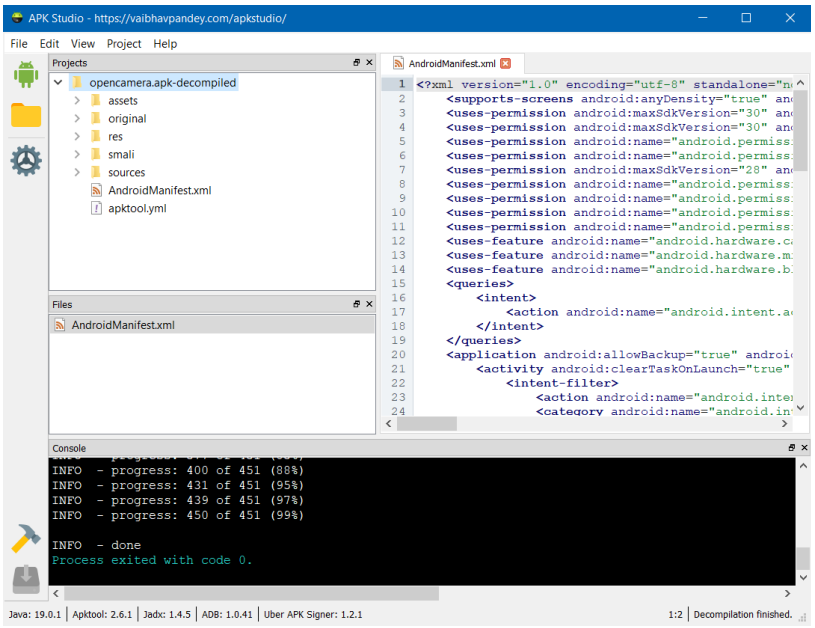
Malicious APK File Creation No. 8

For this assignment I chose to use the Android application OpenCamera, an open source camera app free to download on the Google Play Store. First, I downloaded the OpenCamera apk file from APKMirror, as well as downloading and installing the Android APK Studio software with APKTool to decompile, open, and edit the file. I first disassembled and decompiled the APK file using APKTool, and then I was able to open up the decompiled files in APK Studio. From

```
C:\Users\pro_b>apktool d C:\Users\pro_b\Downloads\opencamera.apk -f
I: Using Apktool 2.6.1 on opencamera.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\pro_b\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

there, I was able to easily view and edit the apk files.



For the malicious files, I created a Trojan horse using two source codes in Java, compiled it from Java to smali and then put the malicious files into the smali folder within the apk. I then also had to modify the AndroidManifest.xml file in order for the malicious files to work correctly within the modified application. I also added in the secret code (“secret code is: ABC123”) in a comment in the first line of the AndroidManifest.xml file. After adding the necessary files and edits, I

repackaged the application into a new apk file. The malicious files don't exactly do anything explicitly malicious, they simply are called to delete some contact information stored on the Android device. They should hopefully allow for the computer to recognize and flag the downloaded apk file as malware.

AndroidManifest.xml

```
1 <!--secret code is: ABC123-->
2 <?xml version="1.0" encoding="utf-8"
3     <supports-screens android:anyDens
4     <uses-permission android:maxSdkVe
5     <uses-permission android:maxSdkVe
6     <uses-permission android:name="ar
7     <uses-permission android:name="ar
8     <uses-permission android:maxSdkVe
```

```
<receiver android:name="edu.uc.cs.androidsecurity.trojan.RunTrojan"/>
    <intent-filter>
        <action android:name="android.trojan.action.BC ACTION"/>
    </intent-filter>
<receiver android:name="edu.uc.cs.androidsecurity.trojan.StartAttack">
    <intent-filter>
        <action android:name="android.intent.action.BOOT COMPLETED"/>
    </intent-filter>
</receiver>
```