

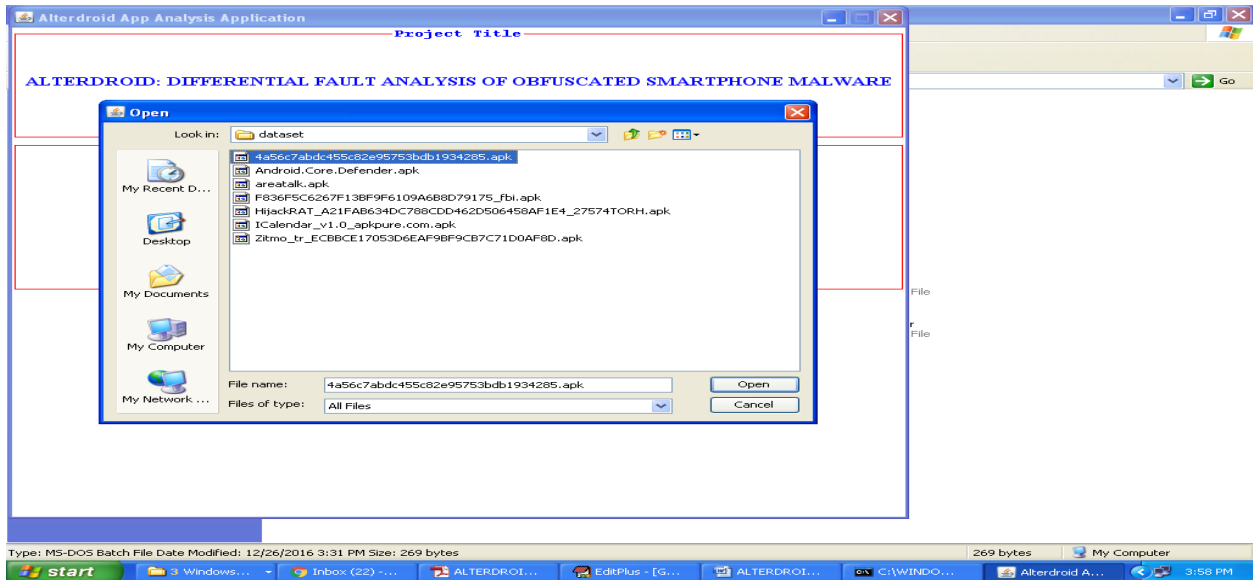
ALTERDROID: Differential Fault Analysis of Obfuscated Smartphone Malware

Screen shots

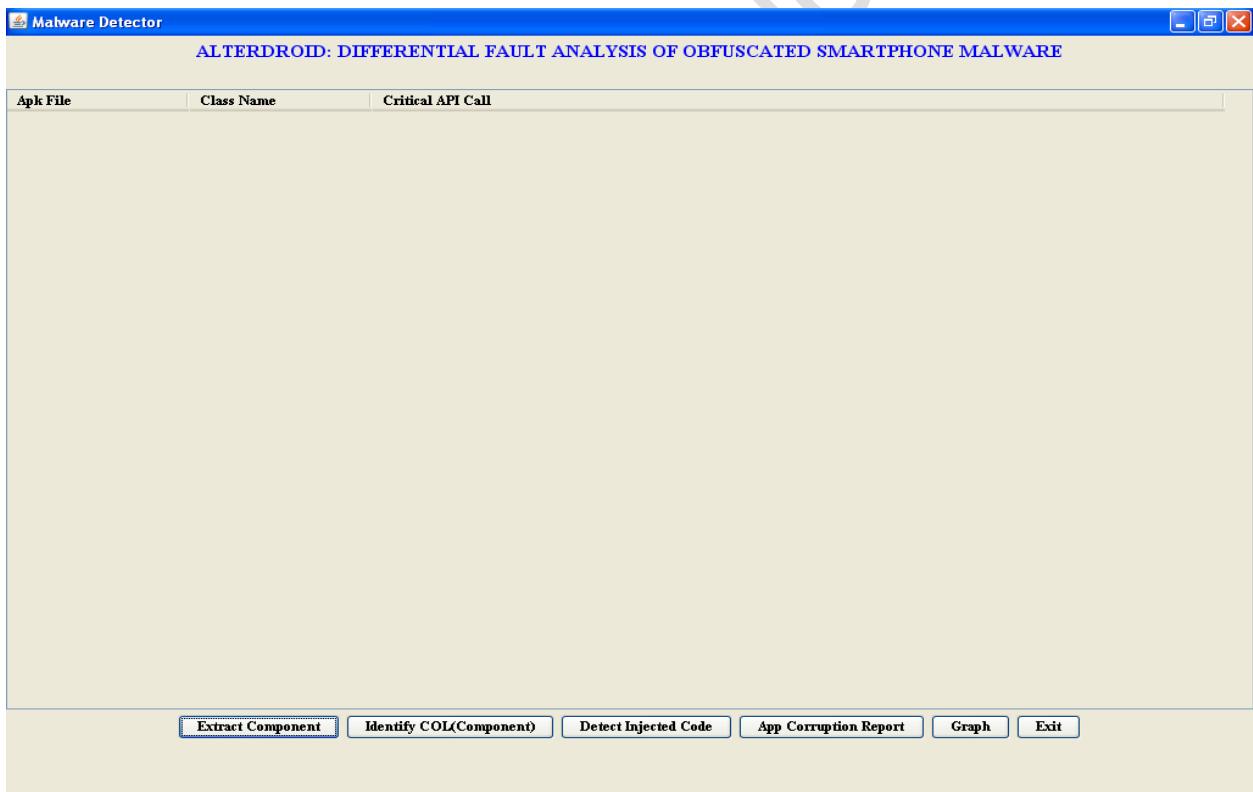
The screenshot shows the 'Alterdroid App Analysis Application' window. The 'Project Title' field contains the text 'ALTERDROID: DIFFERENTIAL FAULT ANALYSIS OF OBFUSCATED SMARTPHONE MALWARE'. Below this is the 'APK Upload Area' with a text input field labeled 'Upload Here APK File' and a 'Browse' button. At the bottom of the window is a flowchart illustrating the analysis process:

```
graph TD
    App[App] --> EC[Extract Components]
    EC --> IC[Identify Col]
    IC --> SC[Select Components]
    SC --> IF[Inject Faults]
    IF --> RC[Repackage Components]
    RC --> EC
    RC --> E1[Execution]
    RC --> E2[Execution]
    E1 --> BS1[Behavioral Signature]
    E2 --> BS2[Behavioral Signature]
    BS1 --> DI[Differential Signature]
    BS2 --> DI
    DI --> PM[Pattern Matching]
    Rules[Rules] --> PM
    PM --> ACR[App Corruption Report]
```

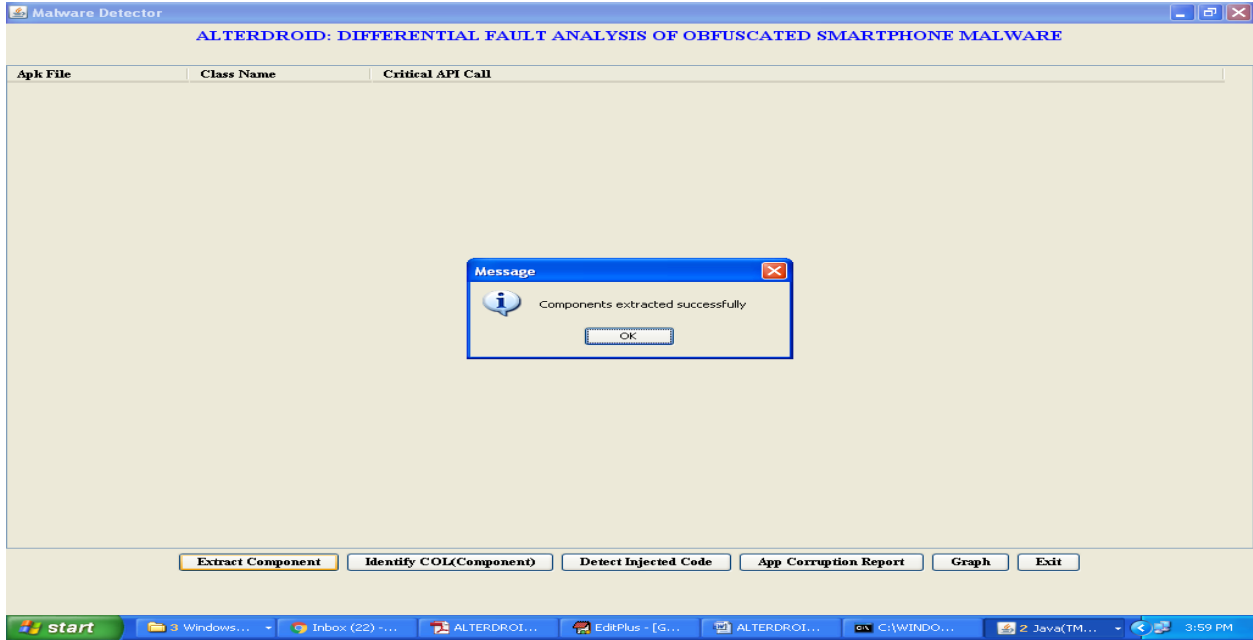
Now click on browse button to upload apk file from 'dataset' folder.



After uploading we will get below screen



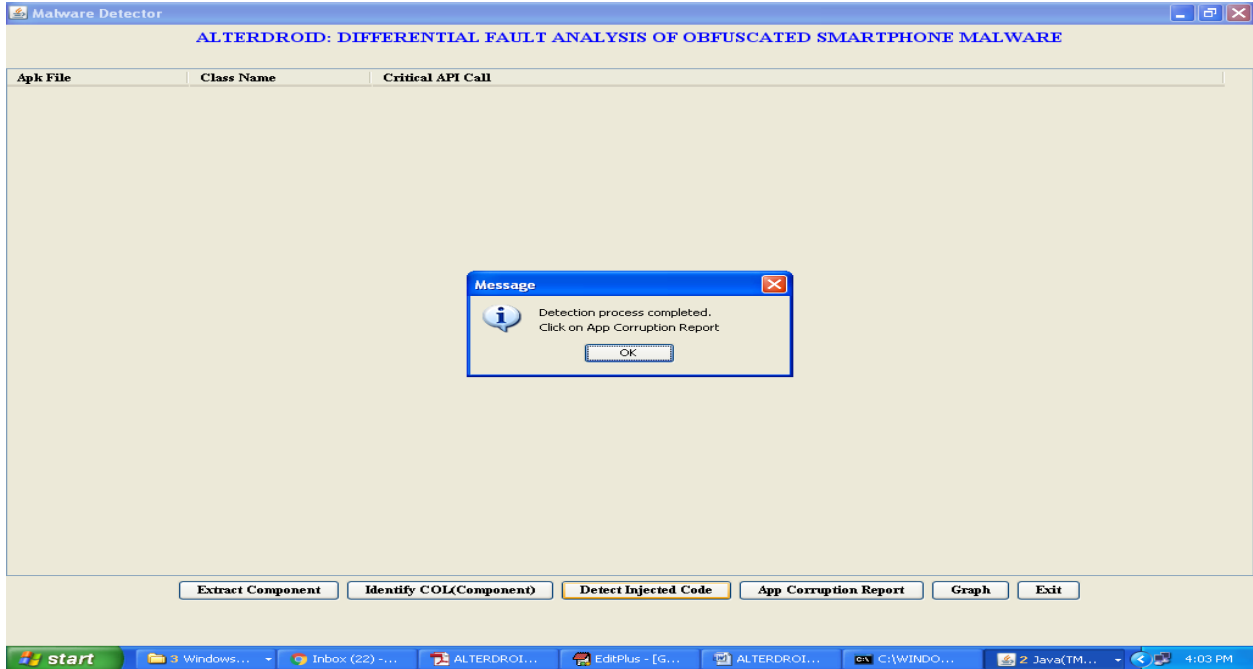
Now click on 'Extract Component' button to extract all apk details and components



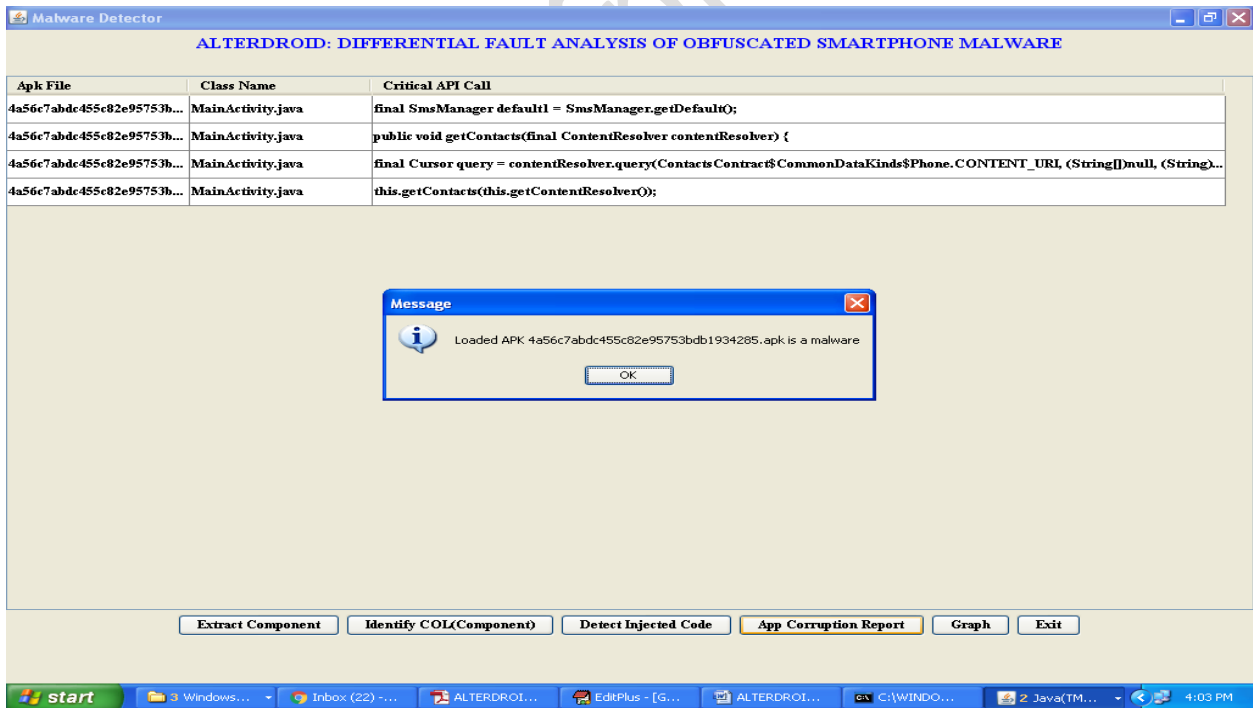
After extracting click on 'Identify COL' button to view detected component details

Parameter Name	Parameter Value
Package Name	app.rewards.amazon.com.amazonrewards
Label	Amazon Rewards
Min Sdk Version	9
Max Sdk Version	
Target Sdk Version	21
Version Code	1
Version Name	1.0
Algorithm Name	SHA256withRSA
MD5	e25325de8d3b515c0327e4c696153e9a
MD5	1323e945b3c9334f6fb5f745cffbe611
Serial No	1772223881
Verification	signed

Now click on 'detect injected code' button to perform detection process



Now click on 'App Corruption Report'



Now click on 'Graph' button to view all components and malware detected components size

Malware Detector

ALTERDROID: DIFFERENTIAL FAULT ANALYSIS OF OBFUSCATED SMARTPHONE MALWARE

Apk File	Class Name	Critical API Call
4a56c7abdc455e82e95753h...	MainActivity.java	final SmsManager default1 = SmsManager.getDefault();
4a56c7abdc455e82e95753h...	MainActivity.java	public void getContacts(final ContentResolver contentResolver) {
4a56c7abdc455e82e95753h...		return null; }
4a56c7abdc455e82e95753h...		

Malware Detection Chart

Component Type	Count
Total Components	45
Malware Components	5

Extract Component Identify COL(Component) Detect Injected Code App Corruption Report Graph Exit

Windows... Inbox (22)... ALTERDROI... EditPlus - [G... ALTERDROI... C:\WINDO... Java(TM)... 4:04 PM

www.takeoffprojects.com