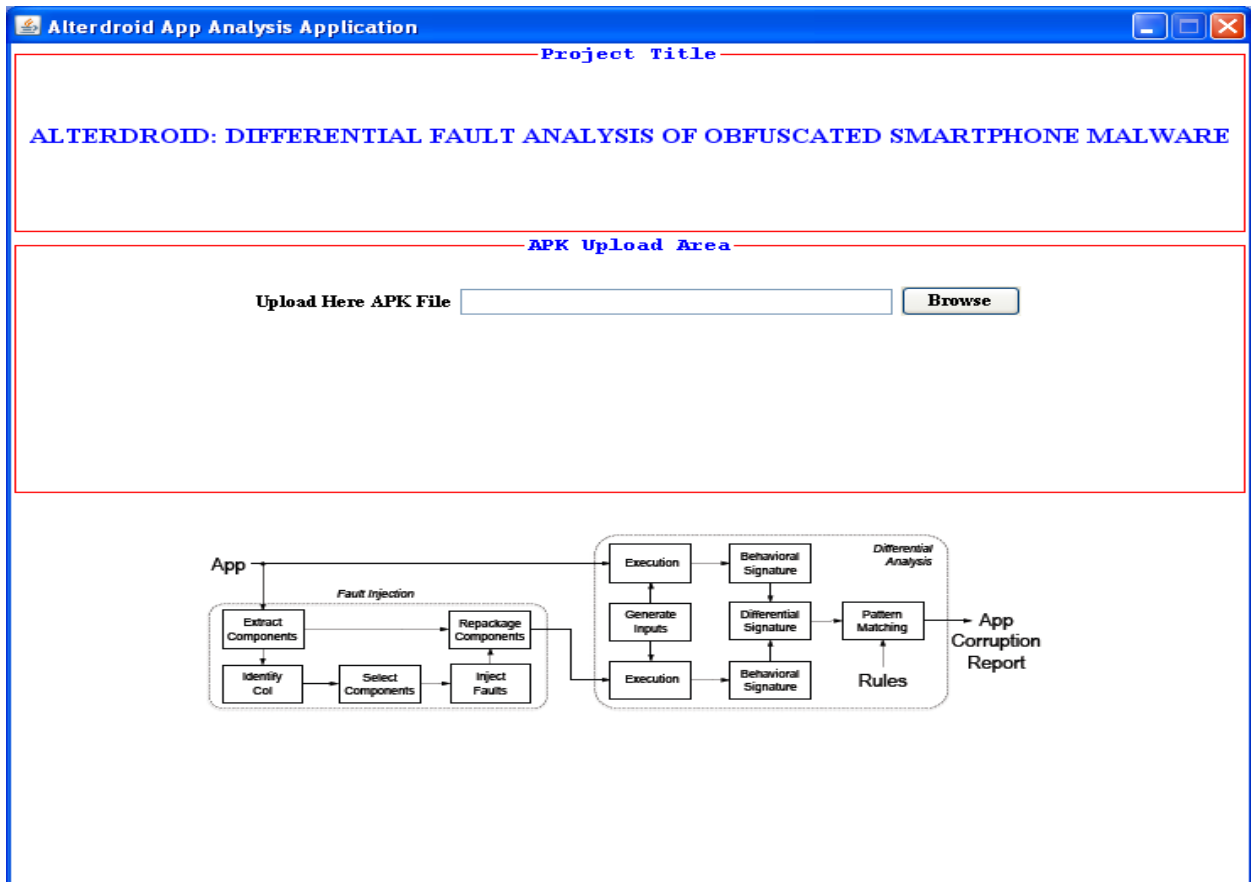
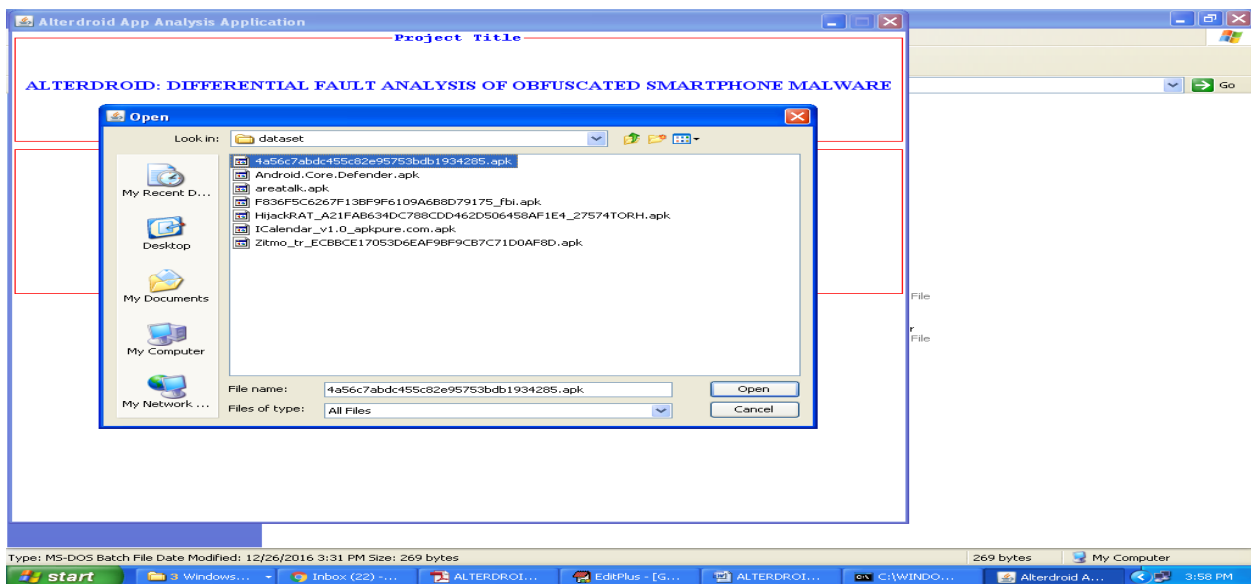


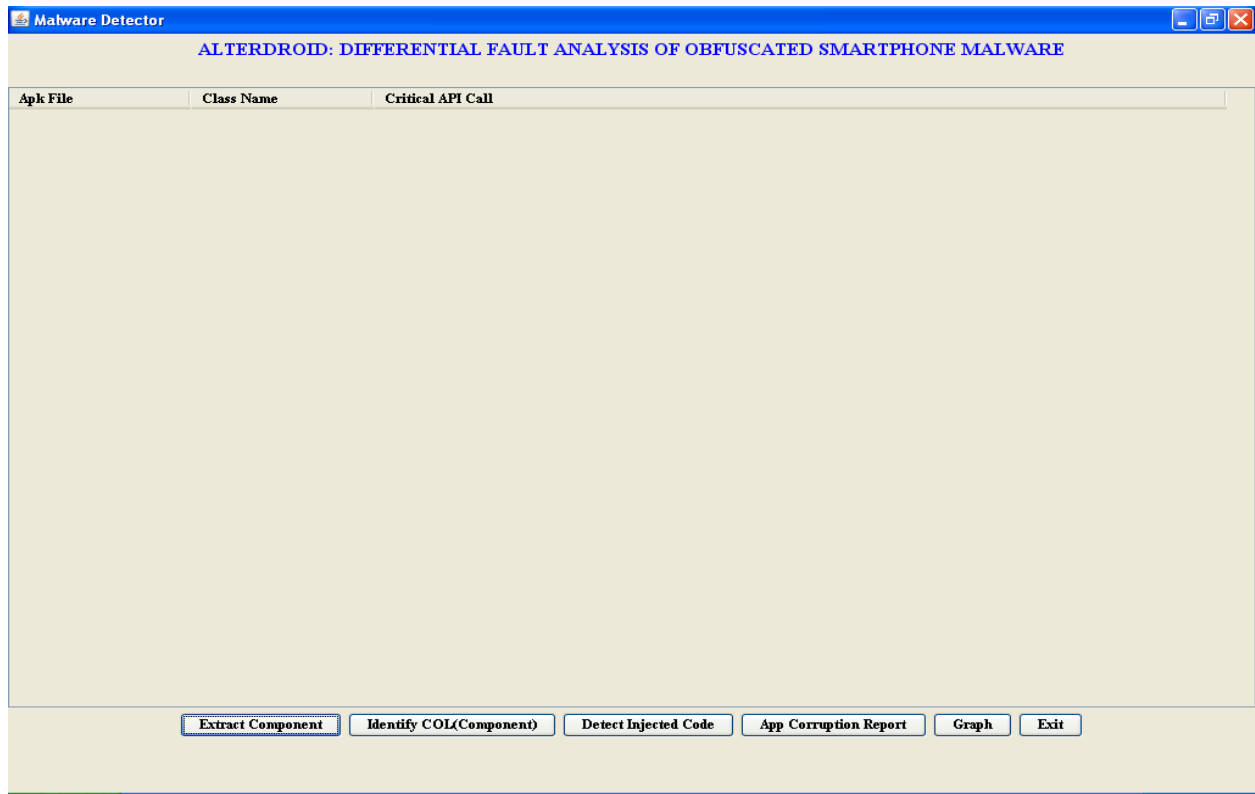
ALTERDROID: Differential Fault Analysis of Obfuscated Smartphone Malware



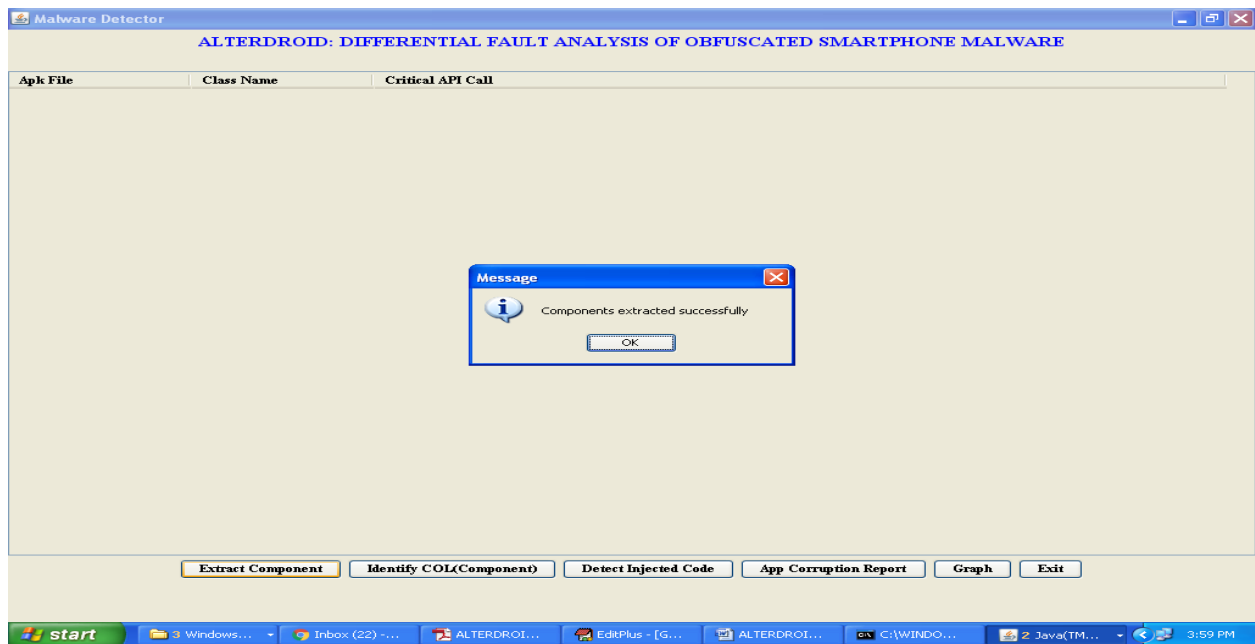
Now click on browse button to upload apk file from 'dataset' folder.



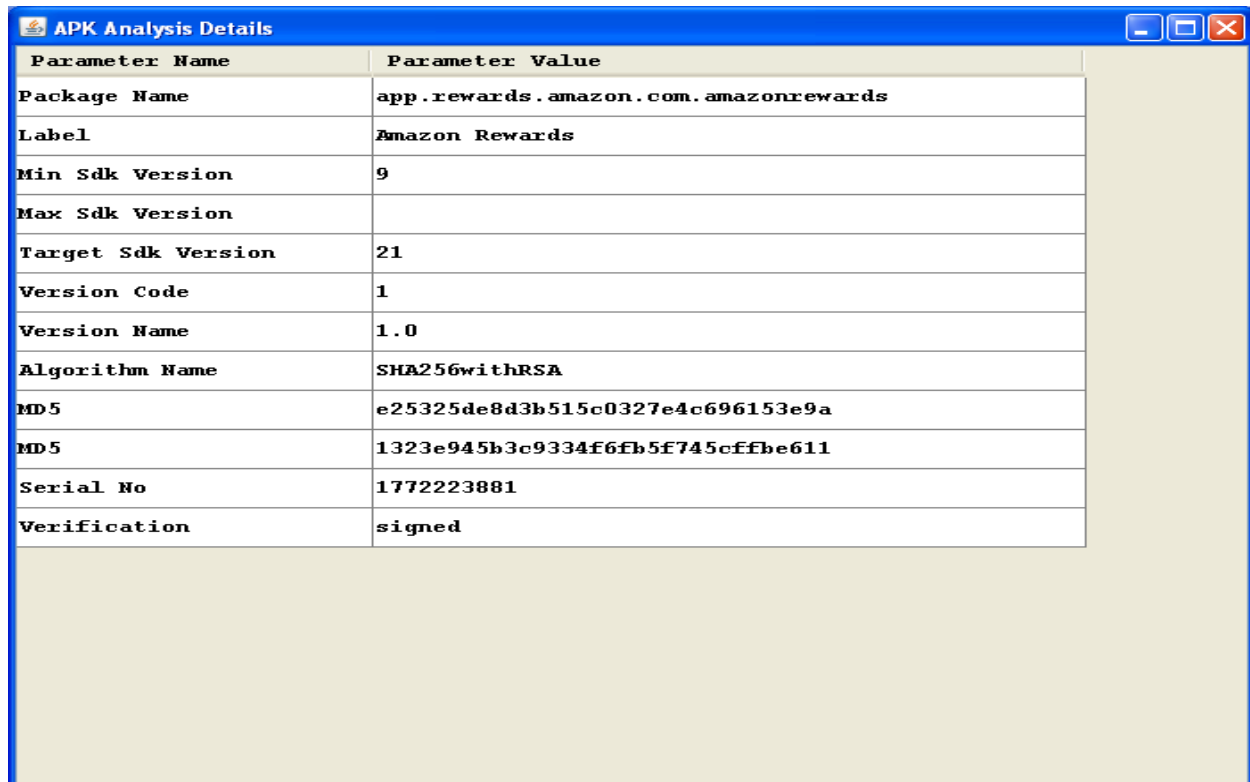
After uploading we will get below screen



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

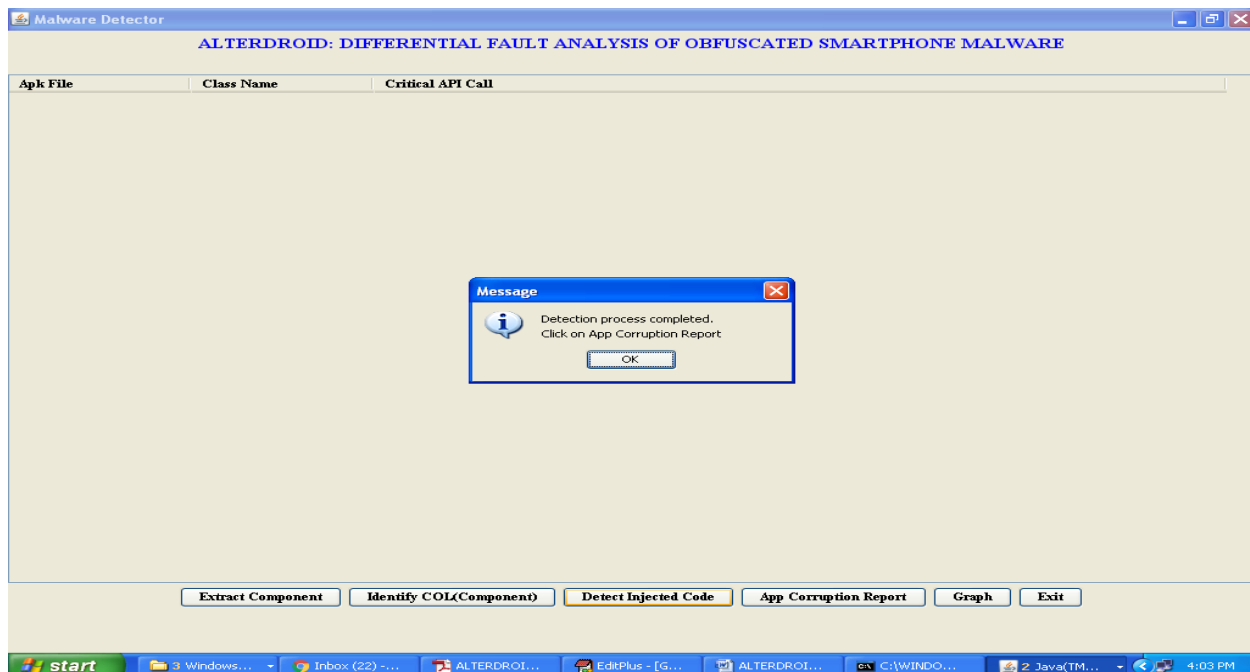


After extracting click on 'Identify COL' button to view detected component details



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



Malware Detector

ALTERDROID: DIFFERENTIAL FAULT ANALYSIS OF OBFUSCATED SMARTPHONE MALWARE

Apk File	Class Name	Critical API Call
----------	------------	-------------------

Message

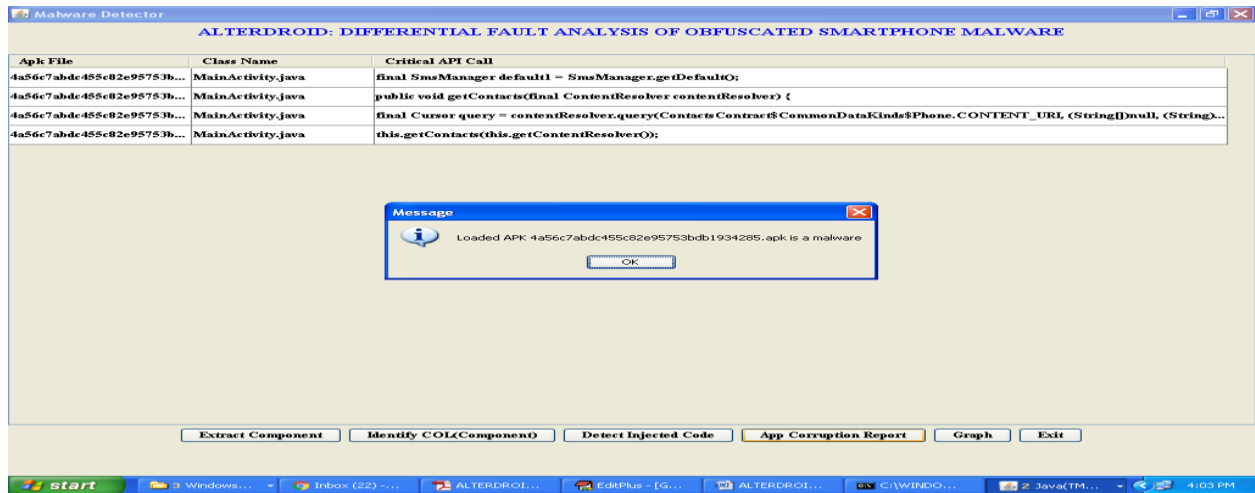
Detection process completed.
Click on App Corruption Report

OK

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

start Windows... Inbox (22) ... ALTERDROI... EditPlus - [G... ALTERDROI... C:\WINDO... Java(TM)... 4:03 PM

Now click on 'App Corruption Report'



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

