Platform	Santoku
Tool	Androguard 3.3.5
Dependency	Python 2.7
Google Drive Folder Details : **APK_decompilation**	Contains the decompiled .java files of the .apk, Generated using Dex2Jar and read using JD-GUI.
Google Drive Folder Details : **Andromal1-analysis**	Contains the static analysis of the malicious .apk using Androguard commands. Resulting analysis such as permissions, activities, main process (driver function), reflection code and so on are saved in separate .txt files.
Google Drive File Details : **VM-LoG_Santoku-2019-10-28-11-35-22_log**	VM log while analyzing the malware. (Non trivial info)
Google Drive File Details : **SHA256.txt**	SHA256 of the malicious apk
Google Drive File Details : **Android_Malware_VirusShareDetails.txt**	Screenshot with the details from VirusShare
Google Drive Folder Details: **Demo Screenshots**	Sample output of androguard analysis of the malicious apk
Notes:	1. Santoku seems to be an unstable platform for malware analysis. 2. The default python and androguard versions in Santoku are old and has limited capability. 3. Latest androguard version is compatible with python3 but Santoku crashed every time, while switching the androguard installation to python3. Hence, some analysis results (e.g: generating call graphs) could not be generated. 4. As a next step, installed Lubuntu and would launch Santoku from within Lubuntu and perform the analysis.