Android Analysis

Folder Name	Description
MalwareData | ---malware.zip ----DataDump.tar.gz	Contains androidmanifest.xml and classes.dex files of the malware Datadump contains the actual code extracted using **androdd** tool present in *androguard.*
Screenshots	Contains images of the terminal while running various adnroguard commands
ManiTreeDetails.txt	I found this opensource tool that gives an analysis of apk permissions categorized as per risk levels (high,medium high, etc)
completeapkinfo.txt	All the files, permissions and activity list of the apk
malware.gexf	Gephi compatible format that has call graphs. I wasn't able to get Gephi working under Santoku. I also tried another tool yED that didn't help either.
graph.xgmml	A graph file readable by Cystoscape tool - an open source network graph tool. I will add screenshots for this later.

Overall, I used the following tools:

1. Apkinfo -> to extract completeapkinfo.txt
2. Androdd -> for DataDump.tar.gz
3. Androxml-> to parse the AndroidManifest.xml as Output.xml in a readable form
4. Androxgmml -> to generate the graph.xgmml (a graph file) readable in Cytoscape tool.
5. Androgexf -> to generate malware.gexf file, which can be opened in Gephi but I wasn't able to install Gephi on Santoku. Hence, I used Androxgmml tool as an alternative.
6. Manitree -> Open sources tool that categorizes permissions based on risk level. (Link here)