Project 4

Consider the Android malware archive at the following link (disable the antimalware before executing malware analysis): https://mega.nz/file/RINQzQKT#KDnuXqL1jmpF0Qrb8Vo2V_jbrJLBsUL6N3Wy2z4Sg_Y

The archive contains malware belonging to three different families: fakebank, overlay, reddrop.

The objective of the project is: choose one malware family and write a report on the analysis of the different samples of the selected family (the archive contains 4 samples for each family). The idea is to find the malicious payload in the different samples of the selected family.

The report must include the following sections:
1) Antimalware analysis: by submitting the samples to the tools web VirusTotal and Jotty;

2) Static analysis: by using bytecodeviewer (https://github.com/Konloch/bytecode-viewer) to highlight interesting snippet of code (include and discuss such code in the report); by using MobSF framework (https://github.com/MobSF/Mobile-Security-Framework-MobSF) to extract automatically features from the code interesting for malware analysis.

3) Dynamic analysis: use MobSF to execute the application in a controlled environment (a simulator) and observe the beahvior of the application.