Assignment 1

Name: Elad Sezanayev
ID: 211909940

The feature set that the paper uses is extracted from the proc filesystem of an android emulator at runtime of the application (the apk file).
The feature set is detailed below by categories:
General: Time of execution.
From /proc/stat: user cpu, nice cpu, system cpu, idle cpu, iowait cpu, irq cpu, softirq cpu, steal cpu.
From /proc/[pid]/statm: total program size (on ram, in pages), resident set size, shared pages.
From /proc/[pid]/stat: user space time, kernel space time, wait for children running on user space time, wait for children running on kernel space time, Virtual memory size in bytes, Number of threads, CPU number last executed on, number of minor faults, number of minor faults with childs, number of major faults, number of major faults with childs.
From /proc/net/dev: number of bytes received, number of packets received, number of bytes transmitted, number of packets transmitted.

The type of classifier that I analyze is dynamic.
(By the classifier paper but also by simple logic)

The repository on github: https://github.com/eladsez/AndroidAttack

The video of me running the classifier is attached with this doc.
Note: The classifier results in the video being output into a .pkl with the python pickle tool So it can't be read nicely (because it's in bytes format) but I can print It, and it looks fine.