Task:

Mr. John sent us his mobile for analysis saying that he can’t access his photos and documents anymore. Your job is to find out what happened and help Mr. John recover his files.

Requirements:

1. Script (bash/PowerShell/python) to get the applications installed close to a given timestamp and filter them based on permission (use androguard for apk parsing).
2. Script that receives as arguments path to broken file from the mobile and recovers them.

Some hints to guide you to the process:

1. Search for broken files on the phone, /sdcard/Download or /sdcard/DCIM.
2. Try to find out when the files were last modified and try to link this with apps installation time (**adb shell pm dump <pkgname> | grep firstInstallTime**).
3. If you discover some “interesting” apps, pull the apk (**adb shell pm path <pkgname>** & **adb pull <resulted\_path>**) and try to look at the code to see what it is doing.
4. Also look on /sdcard for artifacts like keys, password etc that could be linked to the encryption process.

SCRIPTS:

pm (package manager) – list packages -f -3(third party) -i(unde a fost instalata)

-d disabled

Pm dump package name – first install time

Dumpsys alarm / jobscheduler / activity / device\_policy / package / accesbility

Cpuinfo / meminfo / usagestats / account / wifi / dumpstate

logcat