Android Security Lab

Goal: try to find a secret hidden in an Android app

Step 1: Static analysis

- Download jadx (with jre)
    - Unzip
    - Launch jadx.exe
- Copy app1.apk
- Open app1.apk with jadx
    - Find MainActivity in Resources section
    - Find package name thanks to R class

- Browse through the Source code files and try to understand
    - The root detection protection
    - The encryption logic
    - The main application logic

- What would be needed to retrieve the secret ?

Step 2: Dynamic analysis

- Install Android Studio
  - Including Android Virtual Device
- New project / No activity
  - Accept default parameters
- From Tools menu
  - Device Manager
  - Start existing Device (called Pixel) or create a new one WITHOUT Google Play
  - Emulator will launch slowly in the bottom right corner

- Download Frida server
  - Choose Frida server Android x86 64 (to match the architecture of the Pixel virtual device you stared in Android studio)
  - Unzip the file and rename it frida-server
  - Use Device File Explorer in Android Studio (bottom right instead of Emulator)
  - Drag and drop unzipped frida-server file to data/local/tmp folder

- Find adb path
  - Android Studio, Tools menu then SDK Manager
  - Android SDK Location text box: copy paste this path
  - In a terminal, go this path
  - Then subfolder platform-tools
  - Check with command adb version
- Start Frida server
  - adb shell
  - su (to become root)
  - ./data/local/tmp/frida-server &

- Install Frida client on your laptop
  - Check if you have pip3 installed: pip3 –version
    - If not, install latest version of Python
    - Find out where pip3 binary has been installed and go to the corresponding folder
  - pip3 install frida-tools

- See how to write Frida hooking scripts thanks to those examples
  - hooking scripts are in .js files
  - Hook application with
    `frida -U -l your_script.js -f <package_name>`
    where package_name has been found in Step 1

- Display the secret