Installation Guide

For

PwnDroid: Introduction to Source Code Review & Dynamic Analysis

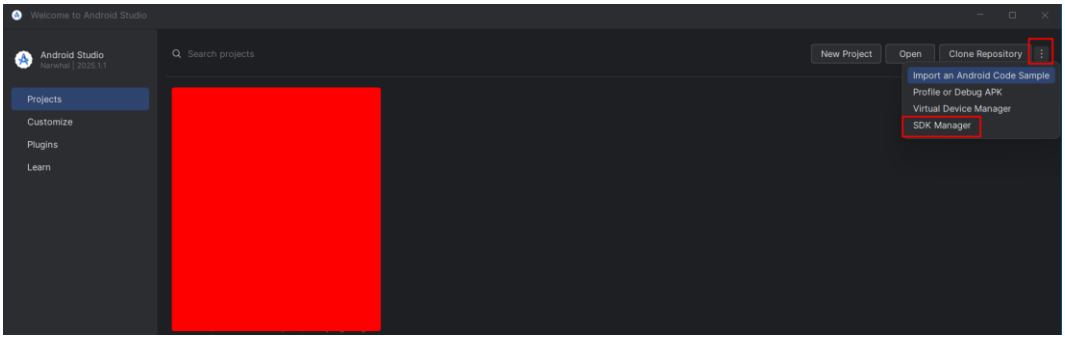
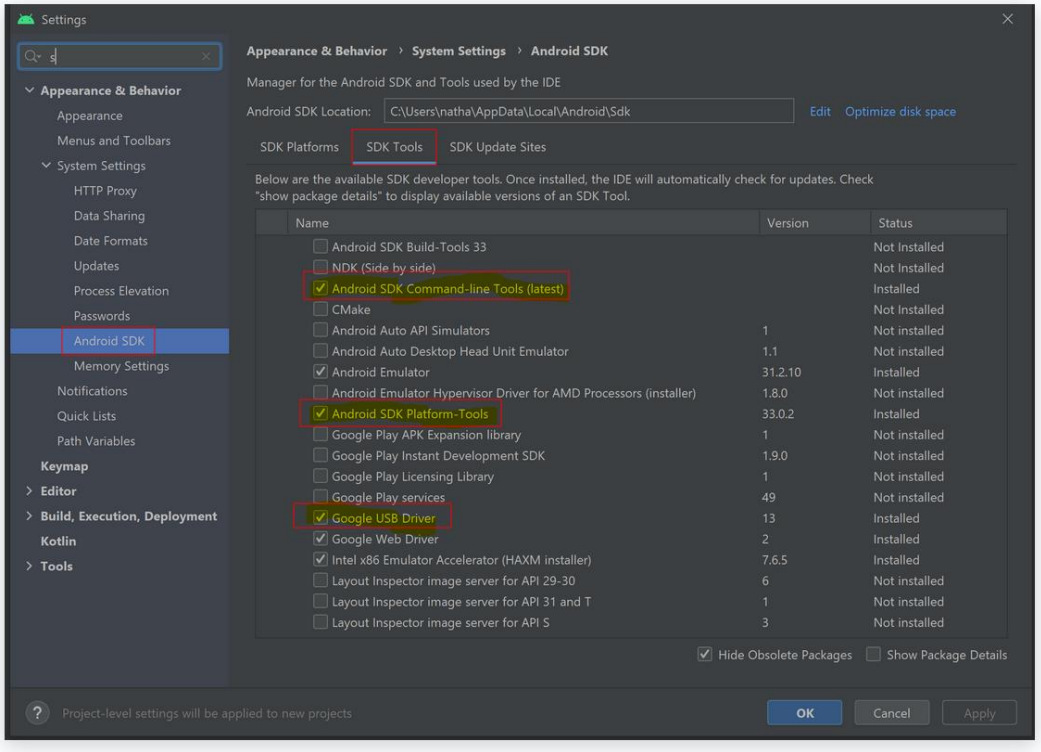
1 Table of Contents

2 Git Repo 3
3 Android Studio + ADB + SDK 4
4 Download RootAVD 7
5 Creating and Rooting Android Virtual Device (AVD) 8
6 JADX-GUI 24

2 Git Repo

1	git clone https://github.com/QiaoNPC/CSLU_PwnDroid_Workshop cd CSLU_PwnDroid_Workshop pip install -r requirements.txt
2	You can proceed to install the lab APKs

3 Android Studio + ADB + SDK

1	Install Android Studio
2	Click on 3 DOTS and SDK Manager 
3	Download these 3 modules, your UI may be different from mine, but find the words that I highlighted 
4	Then follow the following steps

Step 4: Once installed, set the platform-tools file into the path.

- In your search bar, type environment and click “Edit the system environment variables”.
- Click “Environment Variables”.
- Under “User variables,” click “New”.
- Set the variable name to “~~Android~~”. → path
- For the variable value, you need to find where your platform tools are located on your hard drive. In general, when installed with Android Studio, it will live here: C:\Users{Your username}\AppData\Local\Android\Sdk\platform-tools

  Note: You need to turn on the view hidden files function to access app data.
- Once you have verified the location of your platform tools, click “OK”.

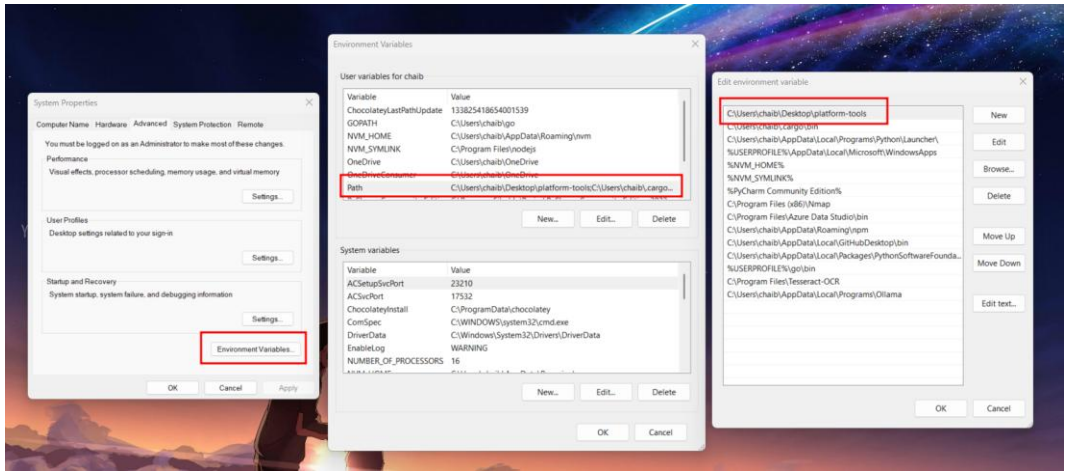
Step 5: Now, verify that the path is working correctly:

```
run command line > Windows key + R > cmd > enter
```

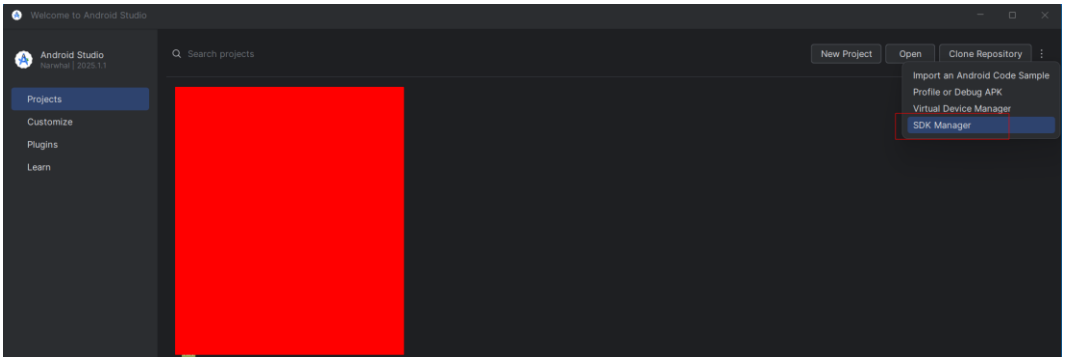
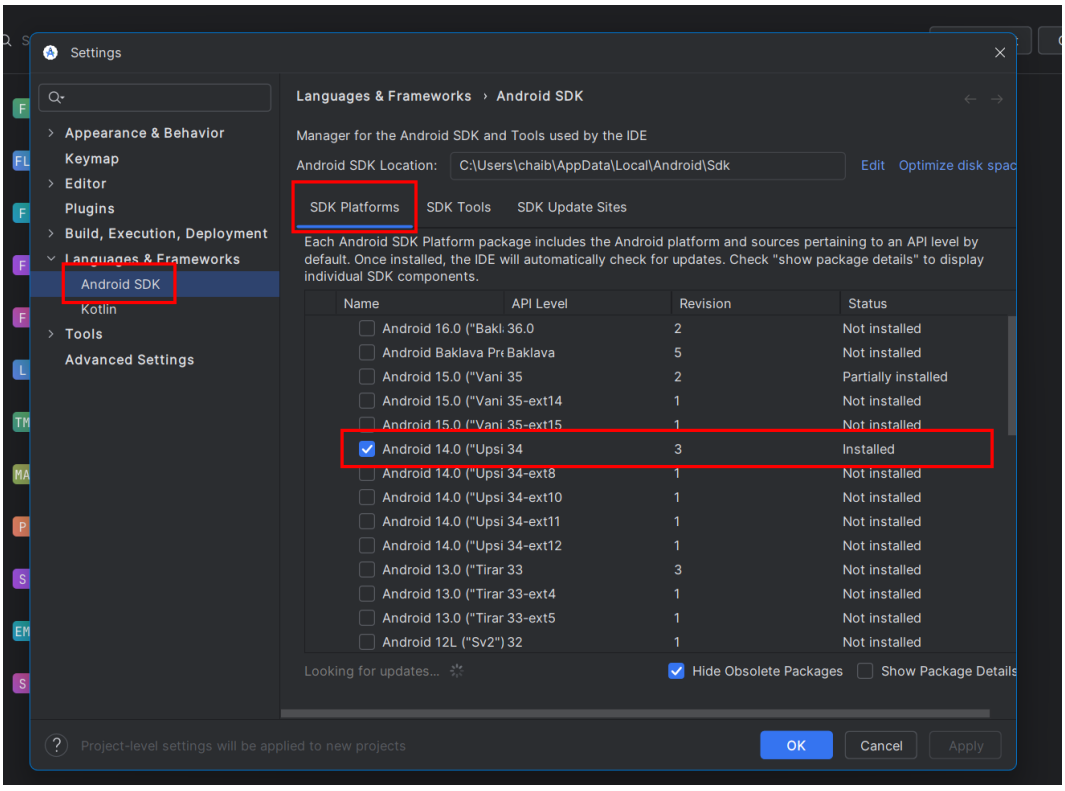
Step 6: Type “adb devices”, and then press enter. If pathed correctly, you will see a list of connected devices. You are now ready to use adb to troubleshoot your devices.

Reference: https://help.esper.io/hc/en-us/articles/12657625935761-Installing-the-Android-Debug-Bridge-ADB-Tool

My configuration looks like this



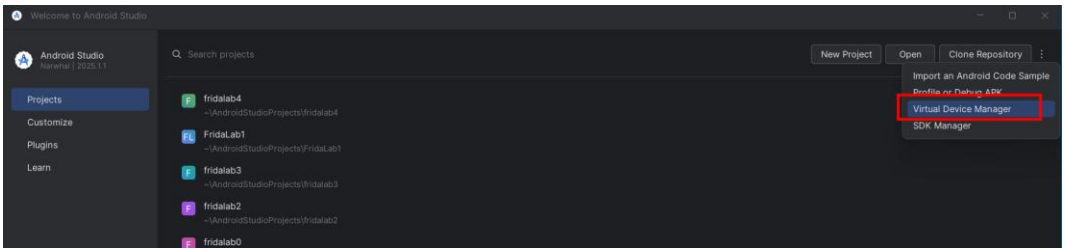
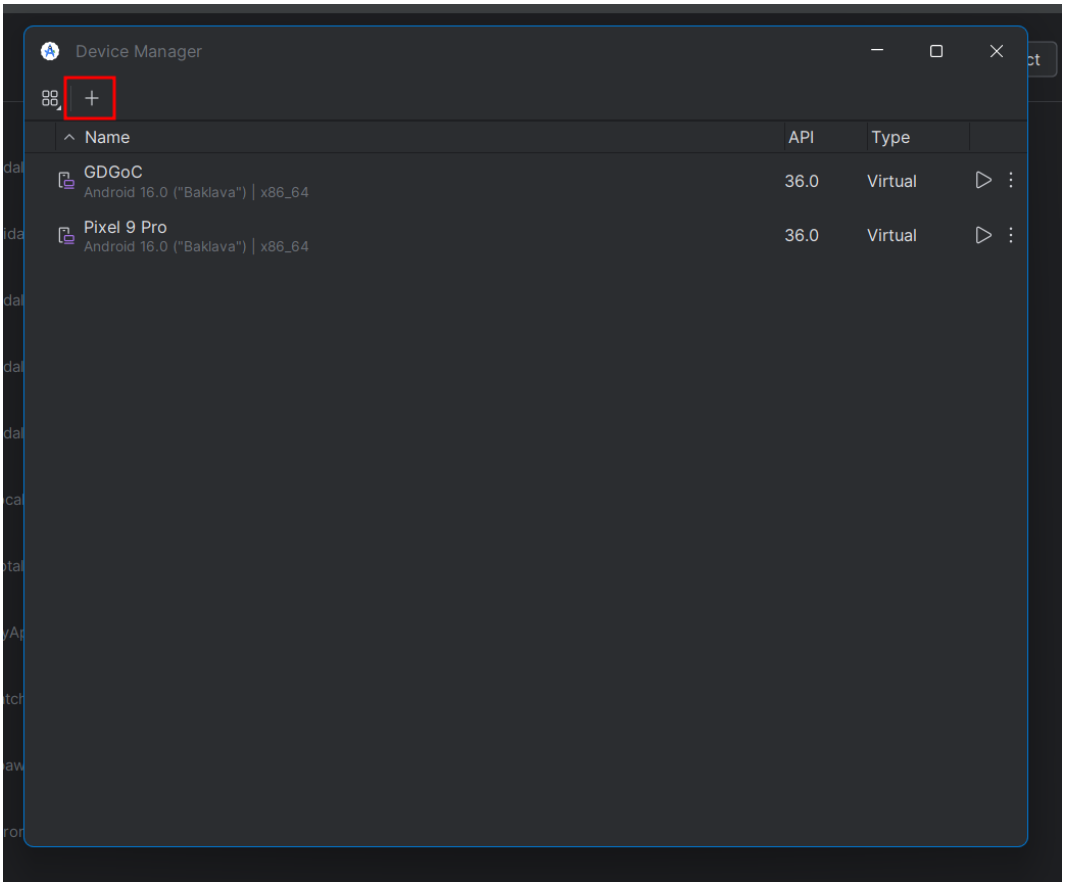
5	Click on SDK Manager

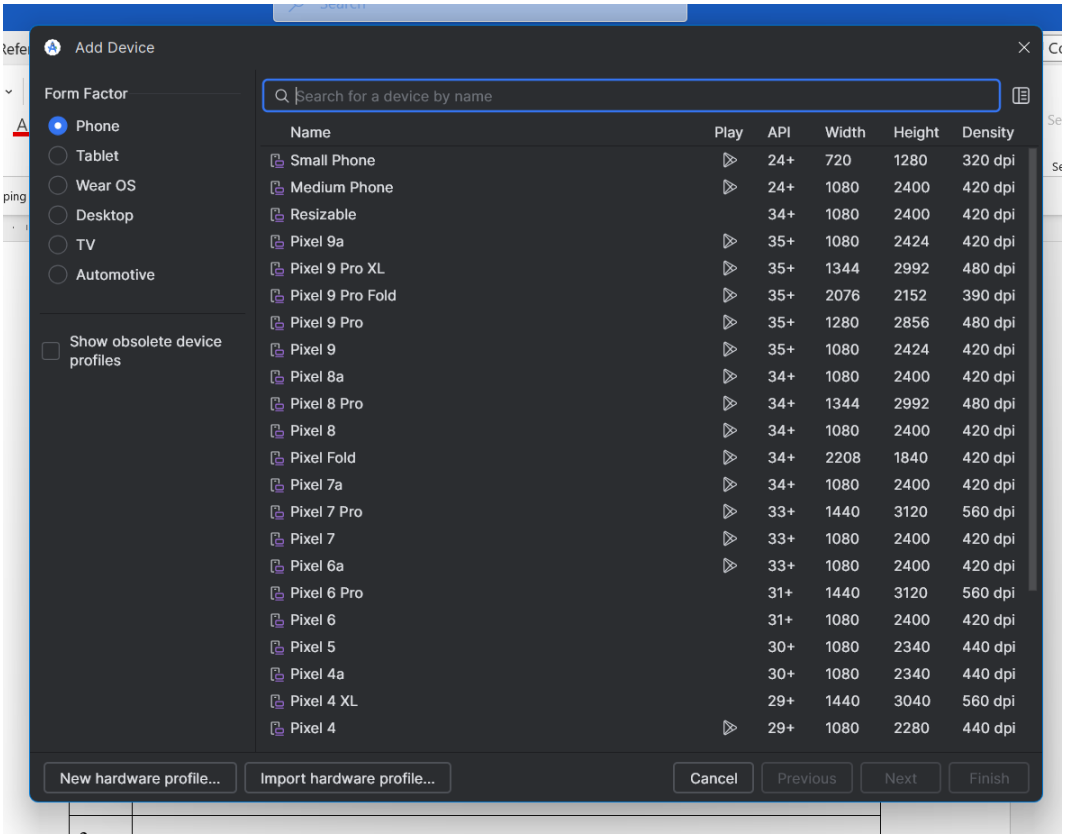
	
6	Install the one highlighted here 

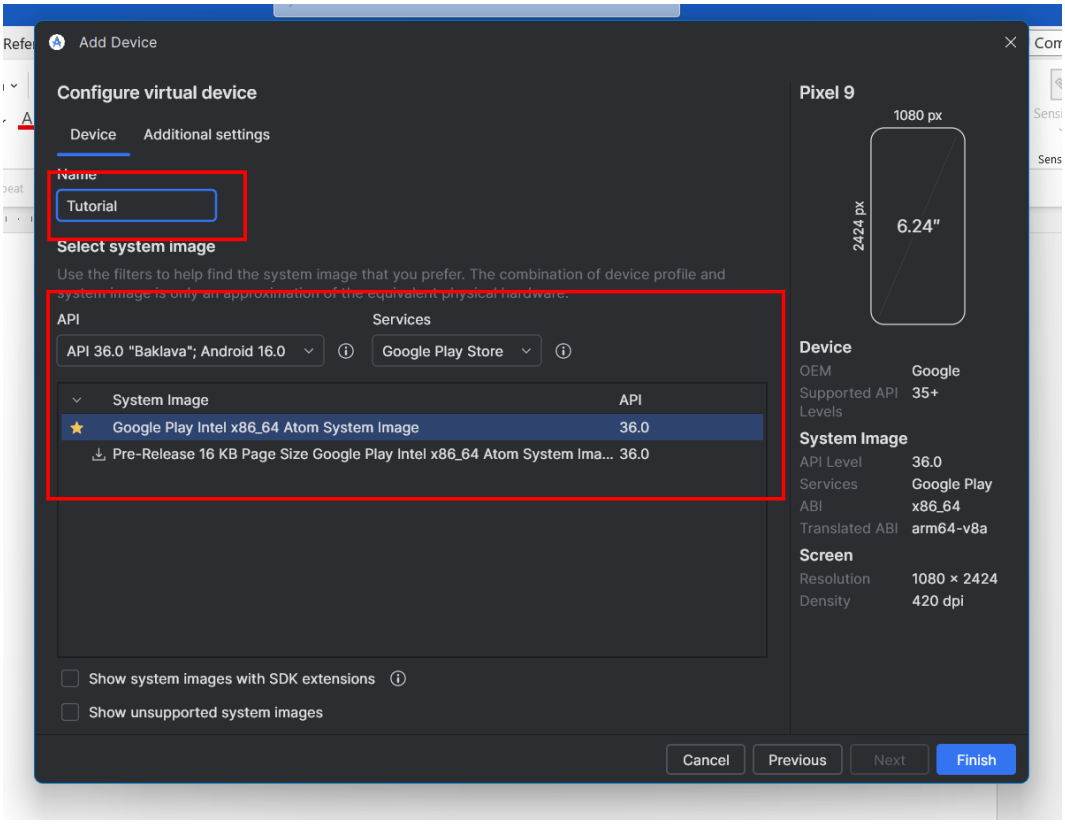
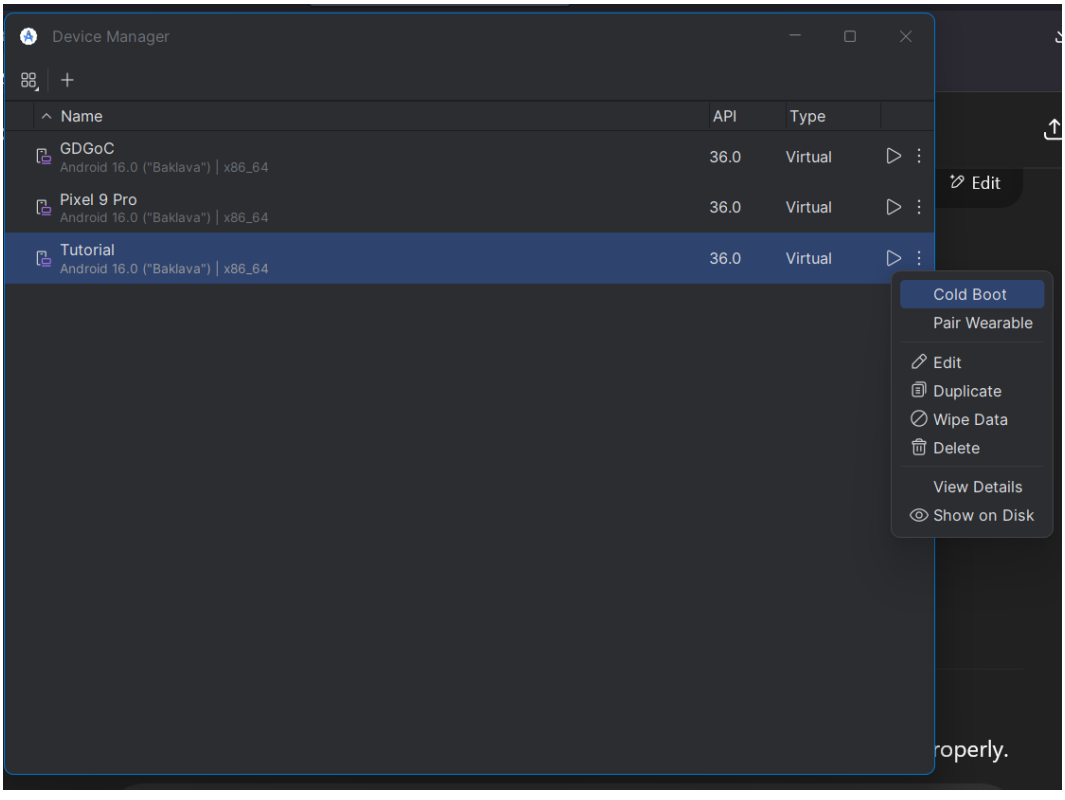
4 Download RootAVD

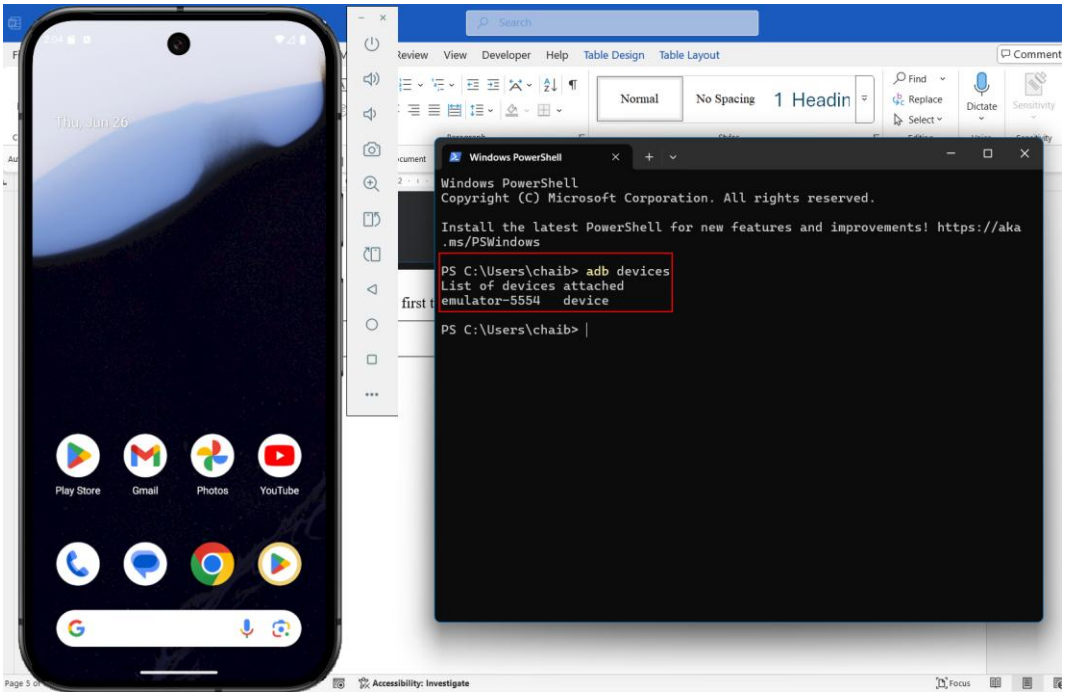
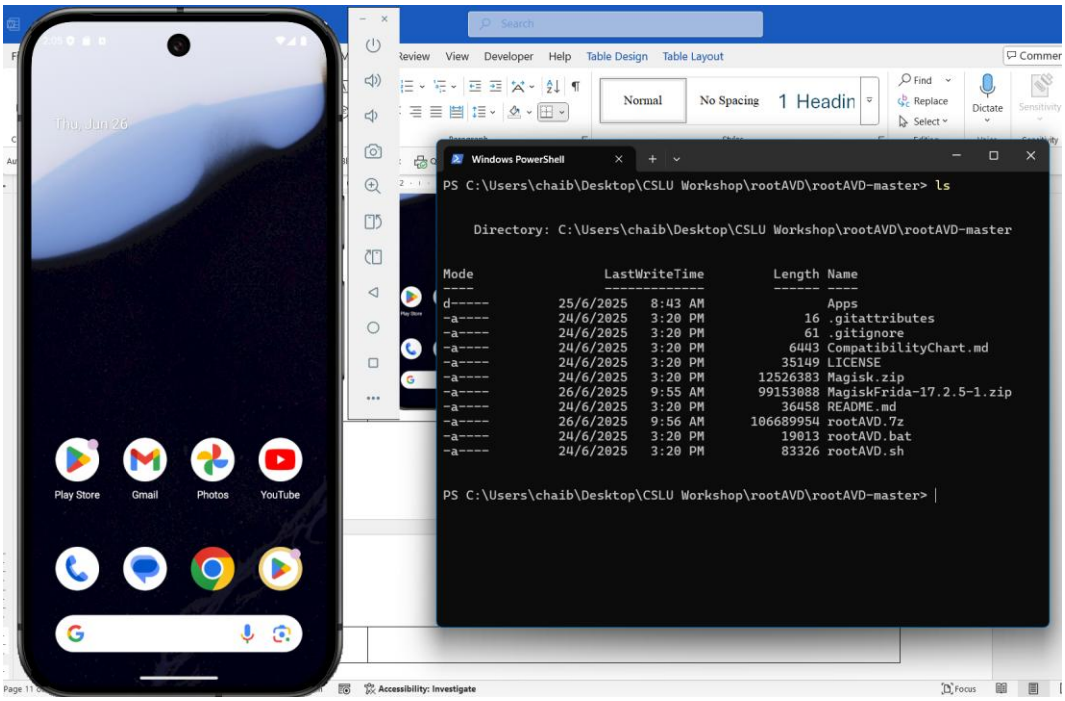
1	Install RootAVD

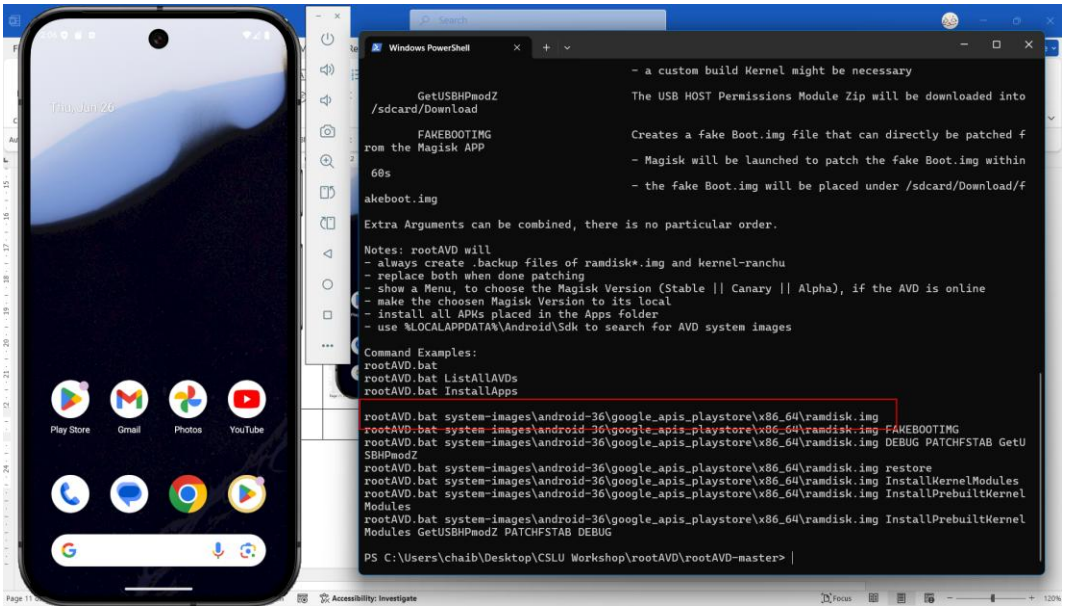
5 Creating and Rooting Android Virtual Device (AVD)

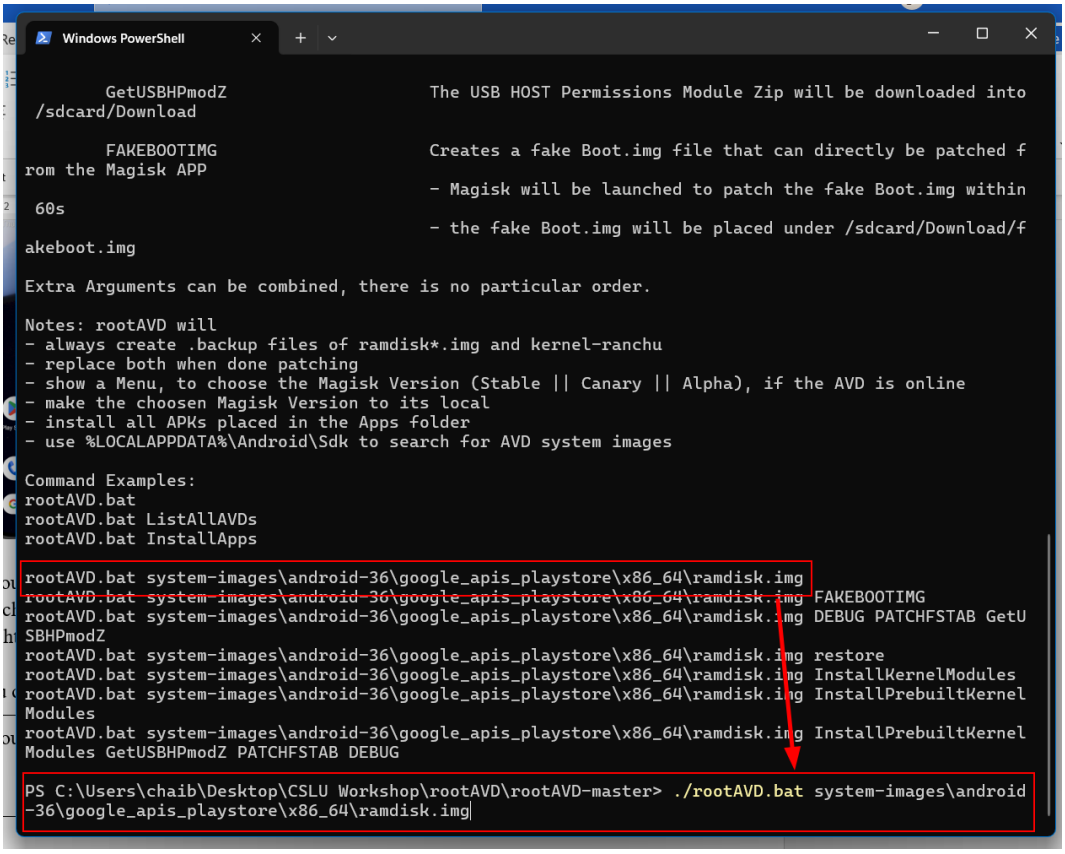
1	Click on Virtual Device Manager 
2	Click add 
3	Choose any phone you like

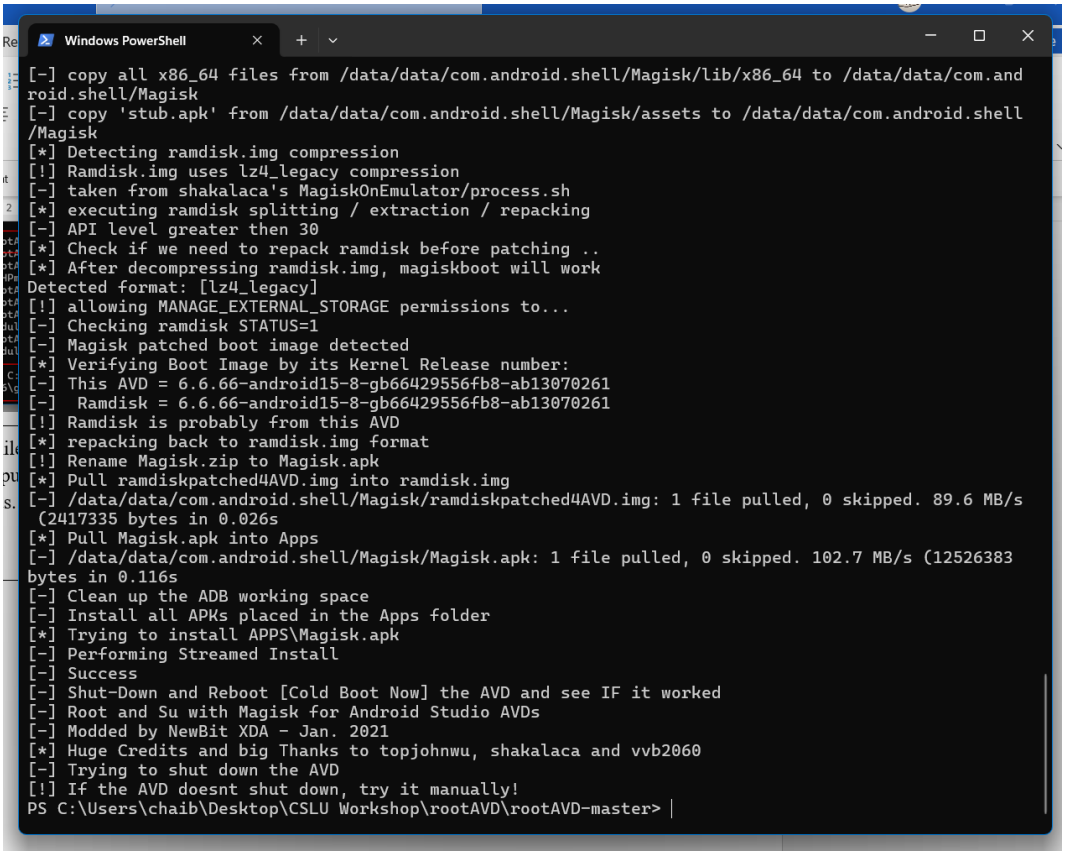
	
4	Choose a name and select the API, it is recommended to select the same API as me because I have tested and used this with no issues. KEEP IN MIND OF THE API YOU INSTALLED, IF ITS 36, REMEMBER THIS NUMBER. VERY IMPORTANT

	
5	Once created, cold boot the device  The first time running the device, it will take some time to load

6	If you downloaded ADB correctly, you will be able to see your device in ADB once it loads 
7	Proceed to where you had your RootAVD installed 
8	Run the following command: **./rootAVD.bat** You will be able to see the following large output, but keep in mind of the highlighted line that I show

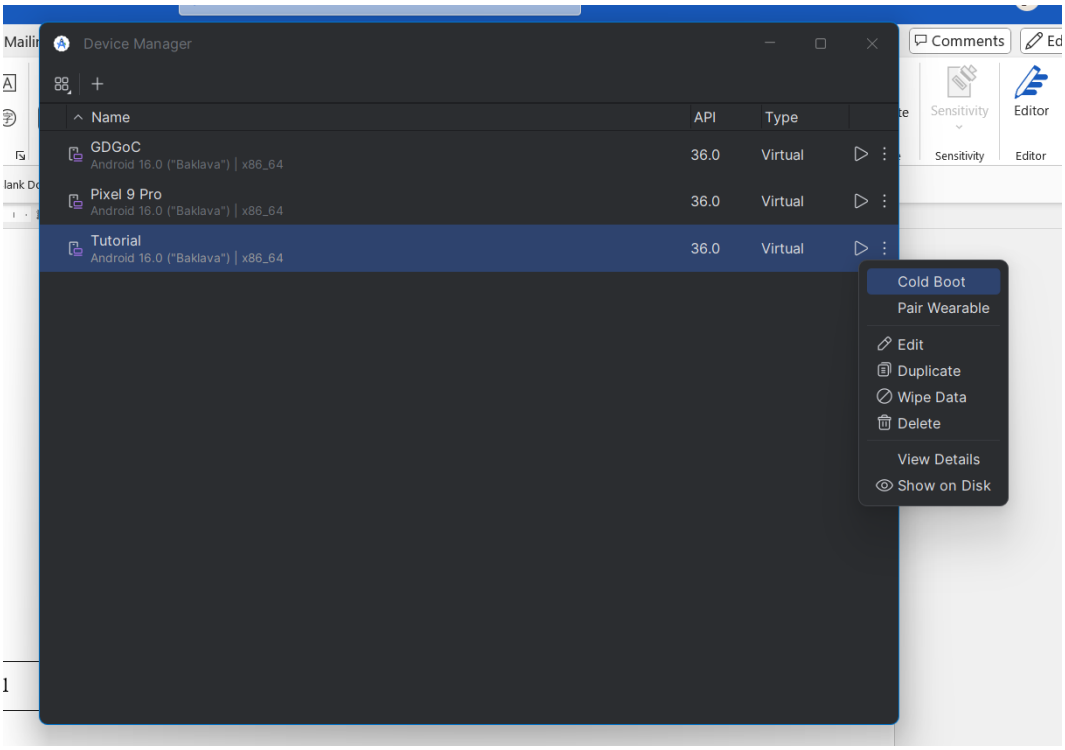
	 If you read closely in the highlighted line, you will be able to see android-36, matching the number you see earlier. If you don't see android-36, same like me, it might mean you installed another version. You can use **./rootAVD.bat ListAllAVDs** to list it
9	If you see 36 like me above, copy n paste the highlighted line and run it

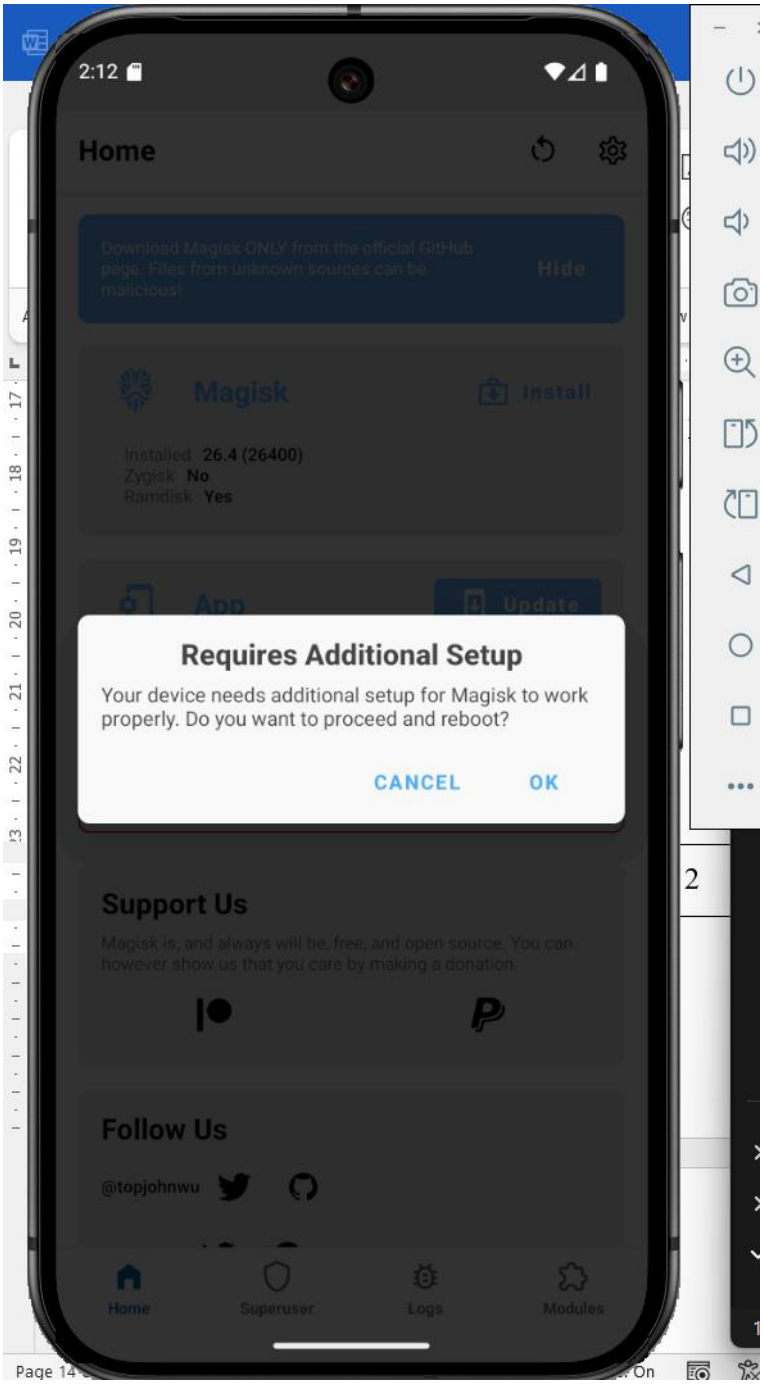
	
10	While it is running, don't click anything, it should end by itself with the following output, and your phone will AUTOMATICALLY shut itself down 10 seconds after it ends. If it doesn't, shut down manually.

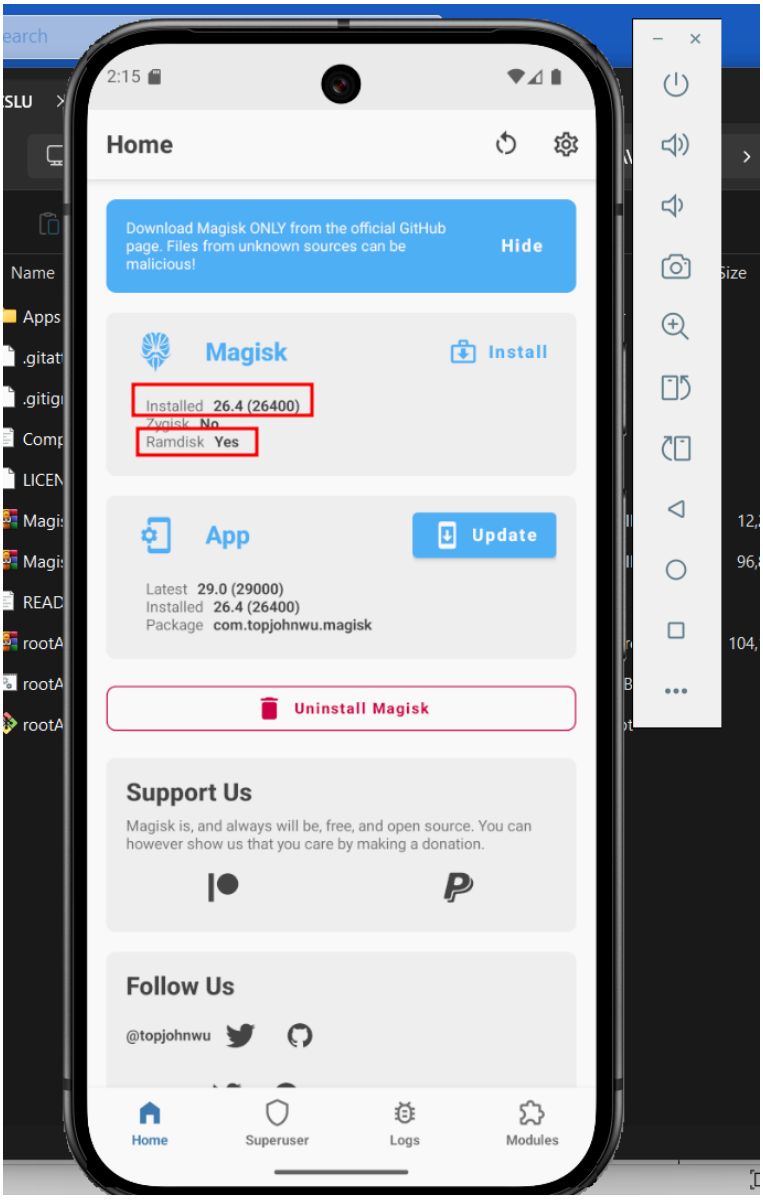


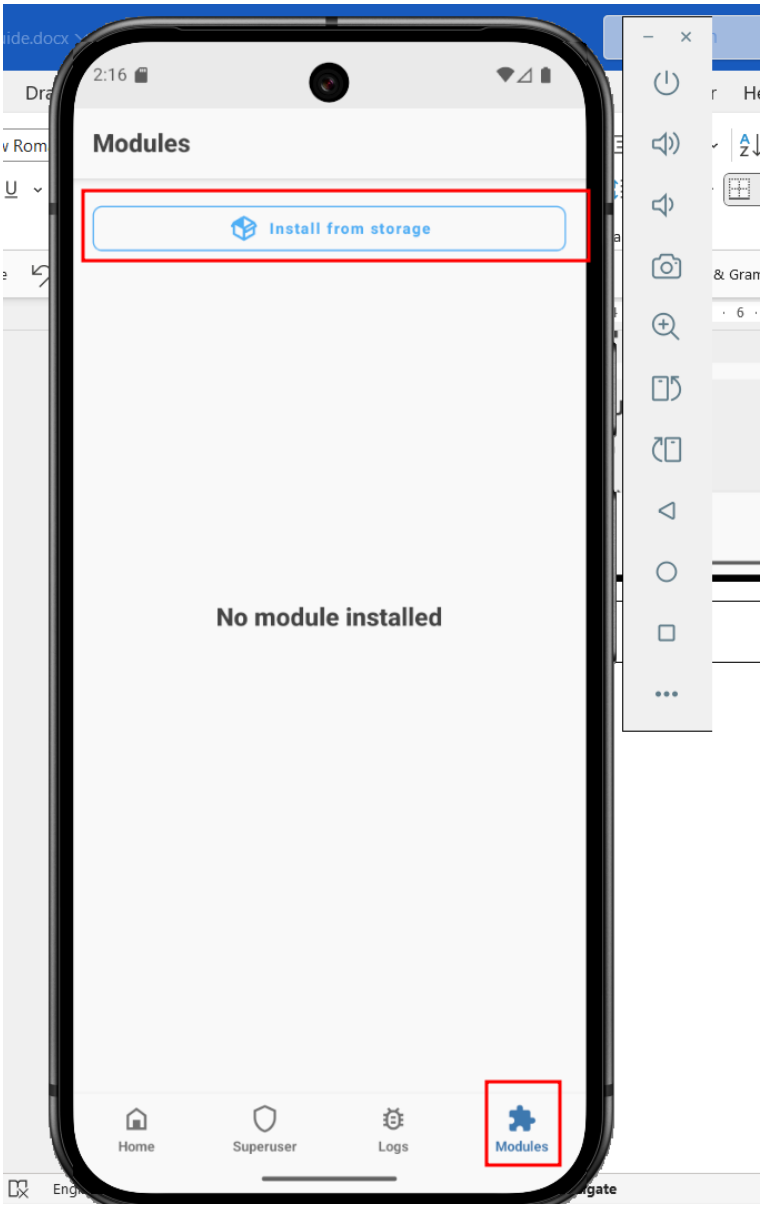
11

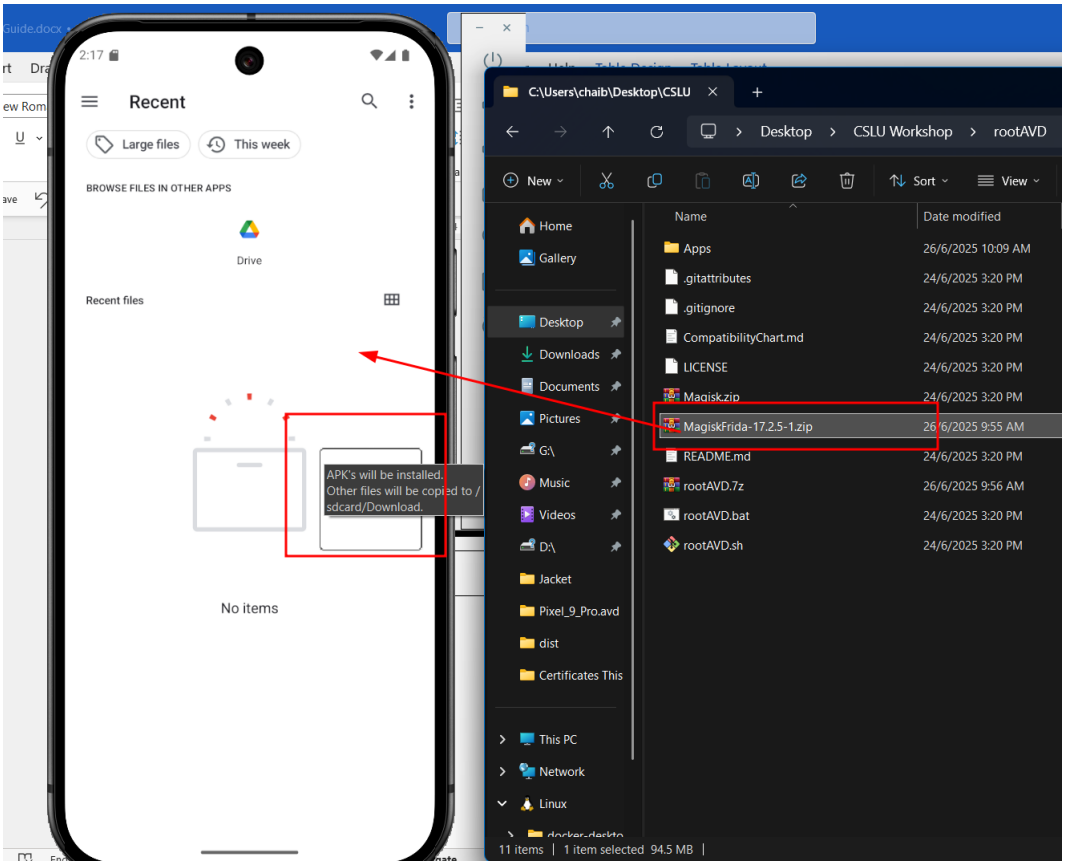
To restart, click coldboot again

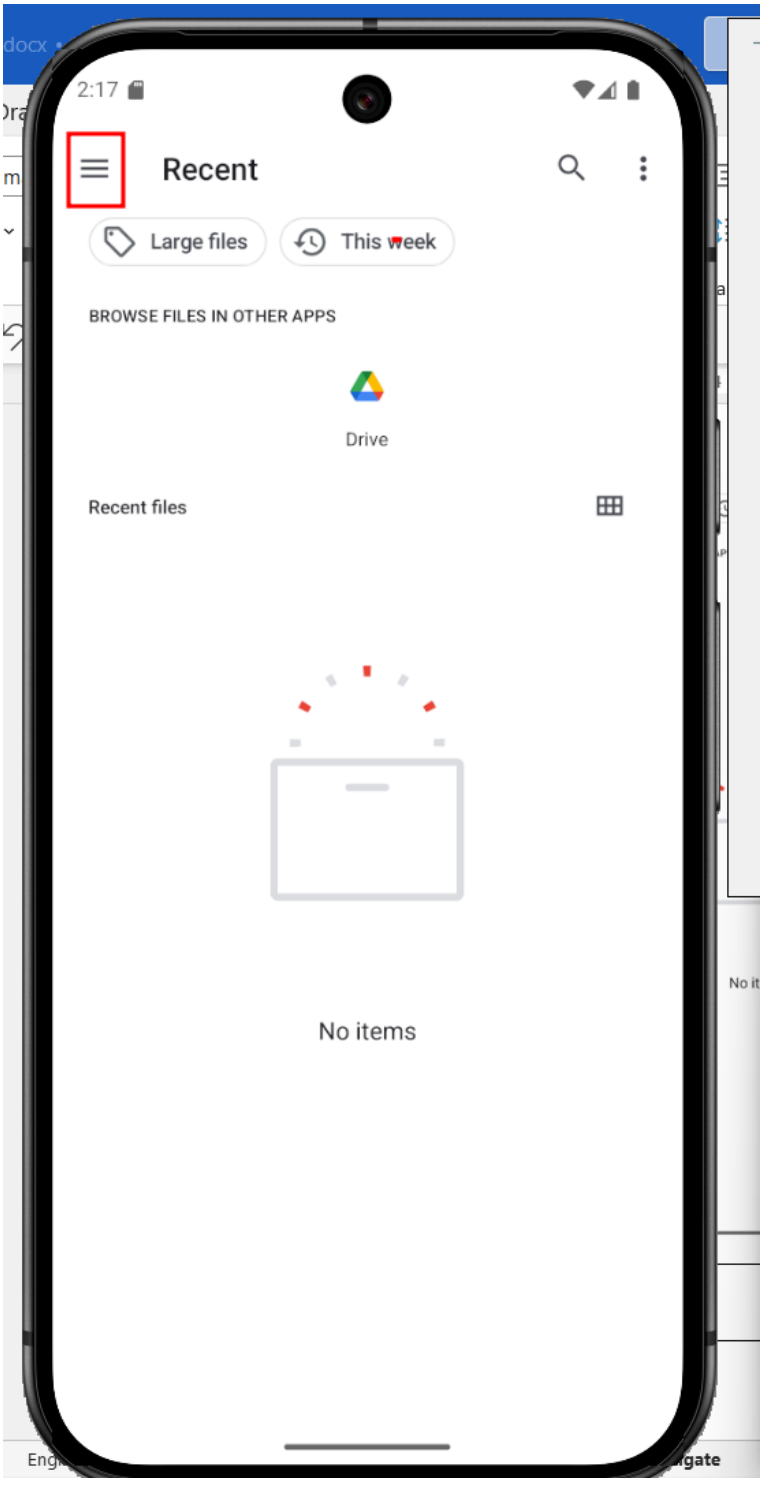


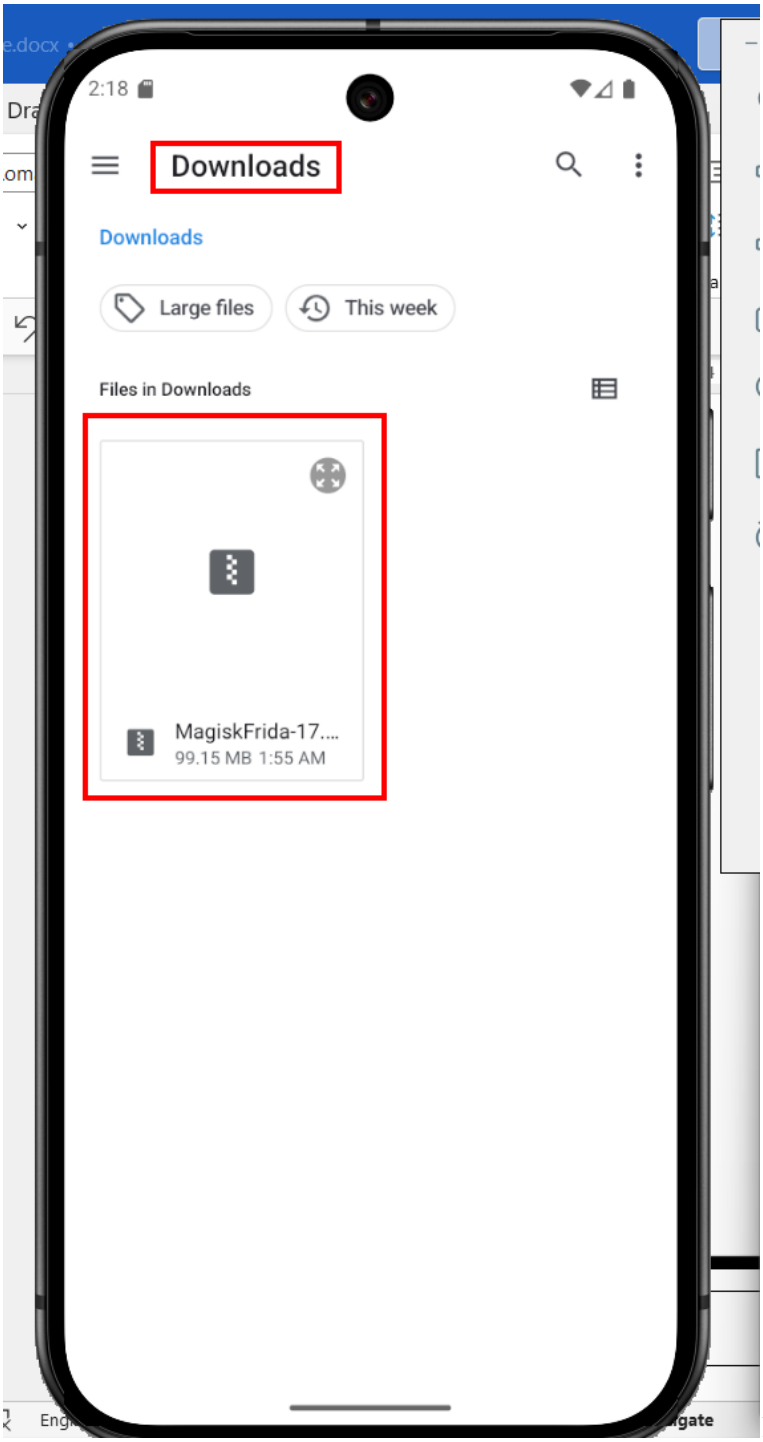
12	Once started, open Magisk. If you are opening Magisk for the first time, it will ask you to restart the phone, just click Yes. It will restart automatically, don't do anything. 
13	If you see the same output as me, then your AVD is rooted properly

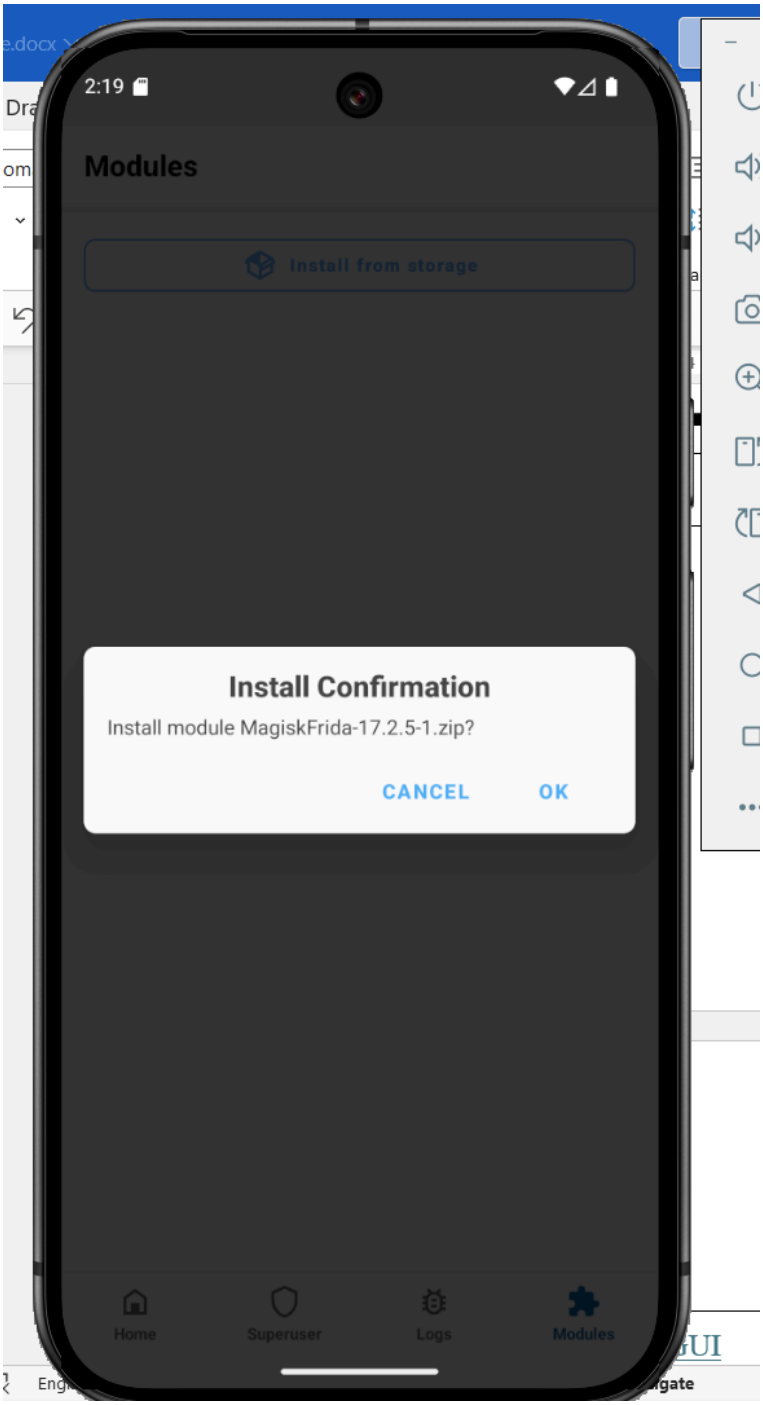
	
14	Click on Modules then Install

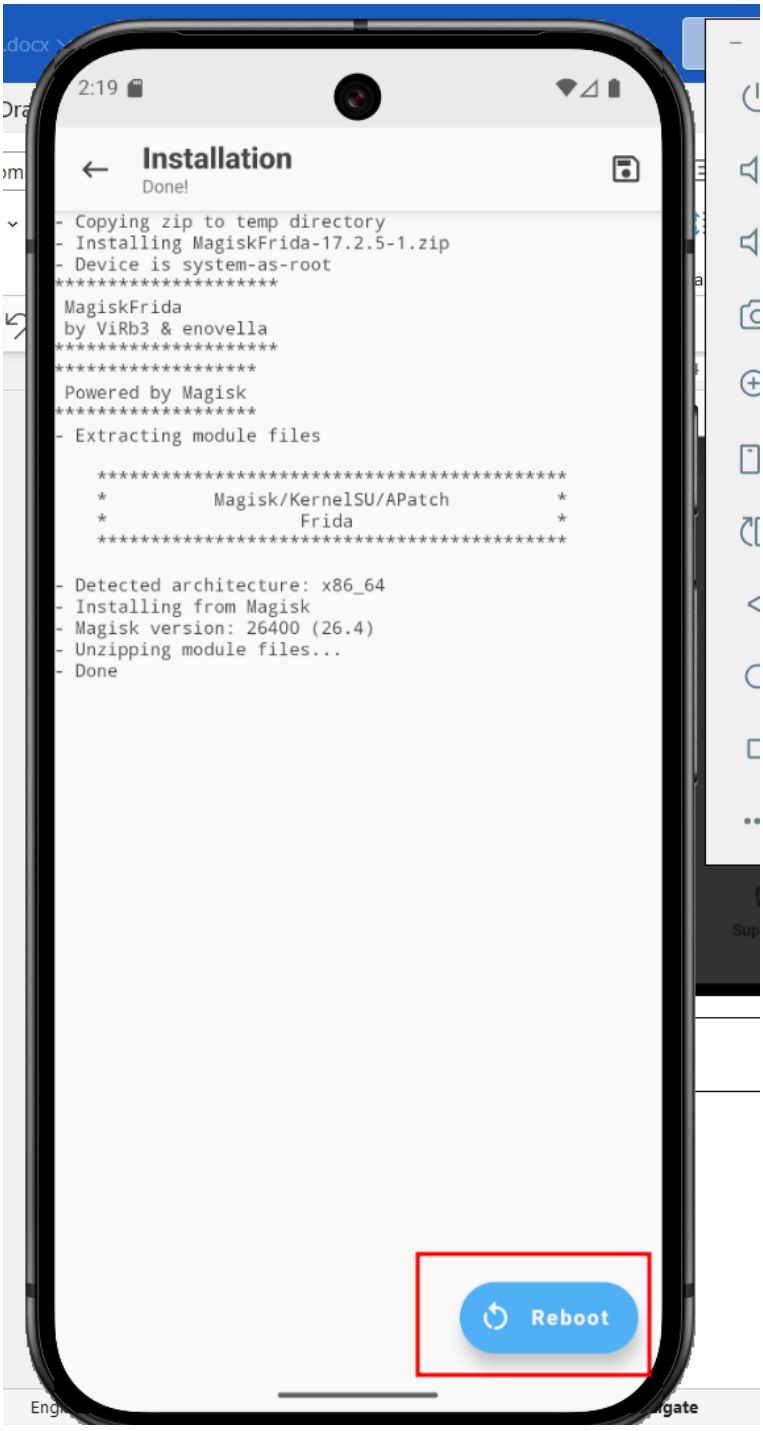
	
15	Drag and drop MagiskFrida zip file into the phone

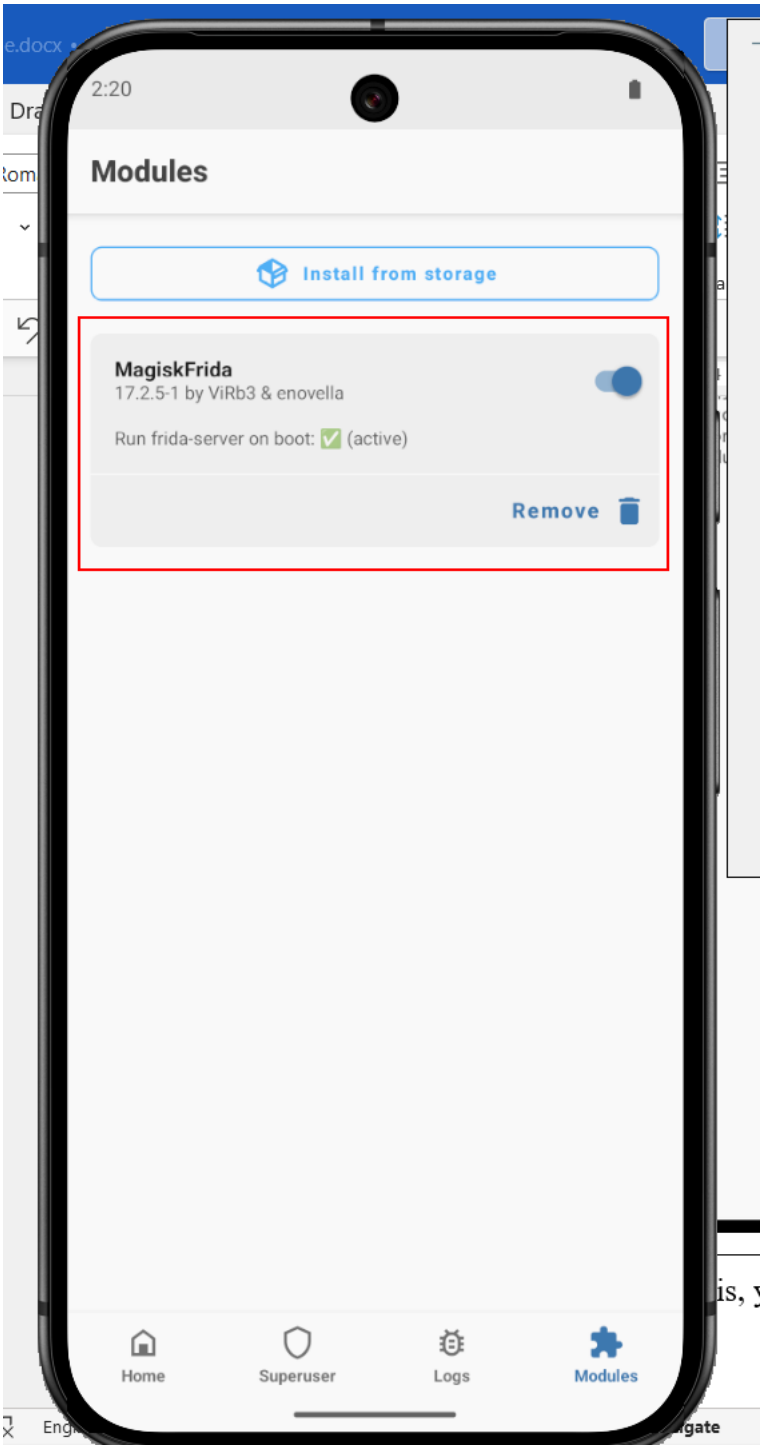
	
16	Click on the Hamburger button and Downloads

	
17	Click on the MagiskFrida file

	 18
18	Install

	 2:19 Modules Install from storage Install Confirmation Install module MagiskFrida-17.2.5-1.zip? CANCEL OK Home Superuser Logs Modules
19	Reboot

	
20	Once you see this, you are set


2:20
Modules
Install from storage
MagiskFrida
17.2.5-1 by ViRb3 & enovella
Run frida-server on boot: ✅ (active)
Remove
Home
Superuser
Logs
Modules

6 JADX-GUI

1	Install JADX-GUI