

# Installation Guide

For

PwnDroid: Introduction to Source Code  
Review & Dynamic Analysis

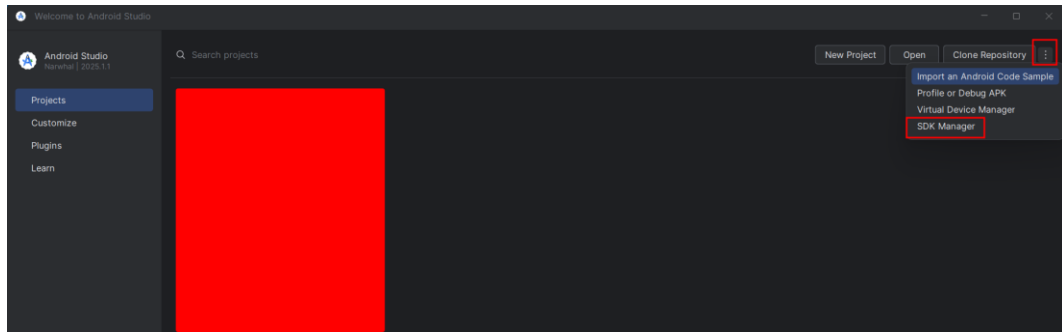
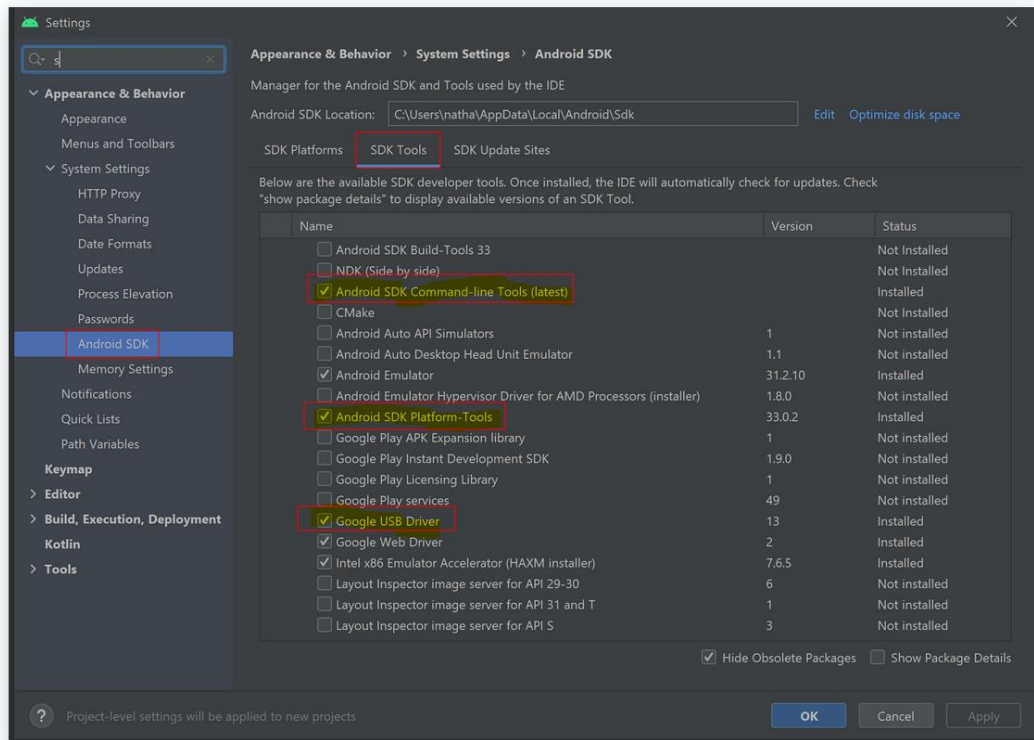
# 1 Table of Contents

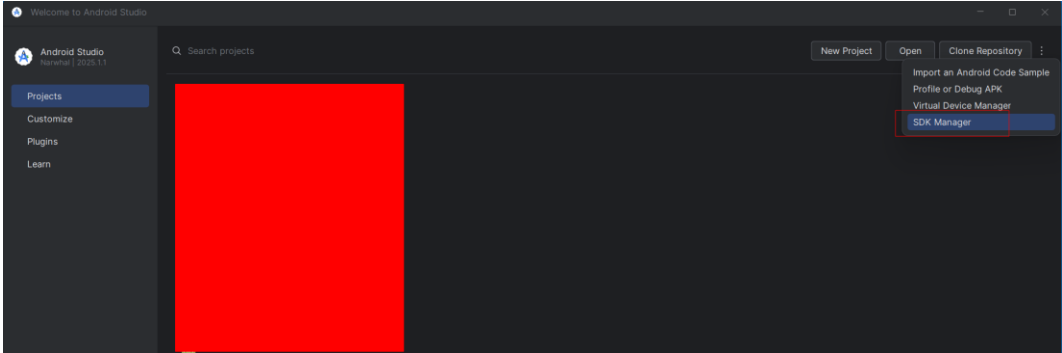
2	Git Repo .....	3
3	Android Studio + ADB + SDK.....	4
4	Download RootAVD .....	7
5	Creating and Rooting Android Virtual Device (AVD).....	8
6	JADX-GUI.....	24

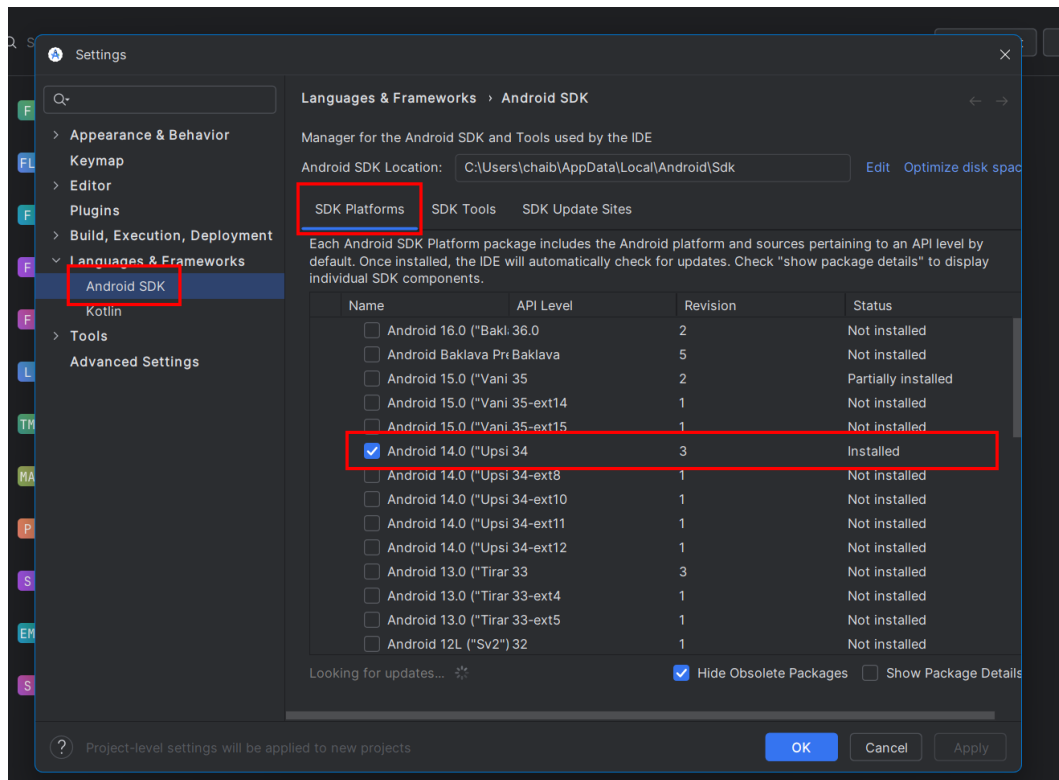
## 2 Git Repo

1	git clone <a href="https://github.com/QiaoNPC/CSLU_PwnDroid_Workshop">https://github.com/QiaoNPC/CSLU_PwnDroid_Workshop</a> 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 <a href="#">Android Studio</a>																																																												
2	<p>Click on 3 DOTS and SDK Manager</p> 																																																												
3	<p>Download these 3 modules, your UI may be different from mine, but find the words that I highlighted</p>  <table><tr><th>Name</th><th>Version</th><th>Status</th></tr><tr><td><input type="checkbox"/> Android SDK Build-Tools 33</td><td></td><td>Not Installed</td></tr><tr><td><input type="checkbox"/> NDK (Side by side)</td><td></td><td>Not Installed</td></tr><tr><td><input checked="" type="checkbox"/> Android SDK Command-line Tools (latest)</td><td></td><td>Installed</td></tr><tr><td><input type="checkbox"/> CMake</td><td></td><td>Not Installed</td></tr><tr><td><input type="checkbox"/> Android Auto API Simulators</td><td>1</td><td>Not installed</td></tr><tr><td><input type="checkbox"/> Android Auto Desktop Head Unit Emulator</td><td>1.1</td><td>Not installed</td></tr><tr><td><input checked="" type="checkbox"/> Android Emulator</td><td>31.2.10</td><td>Installed</td></tr><tr><td><input type="checkbox"/> Android Emulator Hypervisor Driver for AMD Processors (installer)</td><td>1.8.0</td><td>Not installed</td></tr><tr><td><input checked="" type="checkbox"/> Android SDK Platform-Tools</td><td>33.0.2</td><td>Installed</td></tr><tr><td><input type="checkbox"/> Google Play APK Expansion library</td><td>1</td><td>Not installed</td></tr><tr><td><input type="checkbox"/> Google Play Instant Development SDK</td><td>1.9.0</td><td>Not installed</td></tr><tr><td><input type="checkbox"/> Google Play Licensing Library</td><td>1</td><td>Not installed</td></tr><tr><td><input type="checkbox"/> Google Play services</td><td>49</td><td>Not installed</td></tr><tr><td><input checked="" type="checkbox"/> Google USB Driver</td><td>13</td><td>Installed</td></tr><tr><td><input checked="" type="checkbox"/> Google Web Driver</td><td>2</td><td>Installed</td></tr><tr><td><input checked="" type="checkbox"/> Intel x86 Emulator Accelerator (HAXM installer)</td><td>7.6.5</td><td>Installed</td></tr><tr><td><input type="checkbox"/> Layout Inspector image server for API 29-30</td><td>6</td><td>Not installed</td></tr><tr><td><input type="checkbox"/> Layout Inspector image server for API 31 and T</td><td>1</td><td>Not installed</td></tr><tr><td><input type="checkbox"/> Layout Inspector image server for API S</td><td>3</td><td>Not installed</td></tr></table>	Name	Version	Status	<input type="checkbox"/> Android SDK Build-Tools 33		Not Installed	<input type="checkbox"/> NDK (Side by side)		Not Installed	<input checked="" type="checkbox"/> Android SDK Command-line Tools (latest)		Installed	<input type="checkbox"/> CMake		Not Installed	<input type="checkbox"/> Android Auto API Simulators	1	Not installed	<input type="checkbox"/> Android Auto Desktop Head Unit Emulator	1.1	Not installed	<input checked="" type="checkbox"/> Android Emulator	31.2.10	Installed	<input type="checkbox"/> Android Emulator Hypervisor Driver for AMD Processors (installer)	1.8.0	Not installed	<input checked="" type="checkbox"/> Android SDK Platform-Tools	33.0.2	Installed	<input type="checkbox"/> Google Play APK Expansion library	1	Not installed	<input type="checkbox"/> Google Play Instant Development SDK	1.9.0	Not installed	<input type="checkbox"/> Google Play Licensing Library	1	Not installed	<input type="checkbox"/> Google Play services	49	Not installed	<input checked="" type="checkbox"/> Google USB Driver	13	Installed	<input checked="" type="checkbox"/> Google Web Driver	2	Installed	<input checked="" type="checkbox"/> Intel x86 Emulator Accelerator (HAXM installer)	7.6.5	Installed	<input type="checkbox"/> Layout Inspector image server for API 29-30	6	Not installed	<input type="checkbox"/> Layout Inspector image server for API 31 and T	1	Not installed	<input type="checkbox"/> Layout Inspector image server for API S	3	Not installed
Name	Version	Status																																																											
<input type="checkbox"/> Android SDK Build-Tools 33		Not Installed																																																											
<input type="checkbox"/> NDK (Side by side)		Not Installed																																																											
<input checked="" type="checkbox"/> Android SDK Command-line Tools (latest)		Installed																																																											
<input type="checkbox"/> CMake		Not Installed																																																											
<input type="checkbox"/> Android Auto API Simulators	1	Not installed																																																											
<input type="checkbox"/> Android Auto Desktop Head Unit Emulator	1.1	Not installed																																																											
<input checked="" type="checkbox"/> Android Emulator	31.2.10	Installed																																																											
<input type="checkbox"/> Android Emulator Hypervisor Driver for AMD Processors (installer)	1.8.0	Not installed																																																											
<input checked="" type="checkbox"/> Android SDK Platform-Tools	33.0.2	Installed																																																											
<input type="checkbox"/> Google Play APK Expansion library	1	Not installed																																																											
<input type="checkbox"/> Google Play Instant Development SDK	1.9.0	Not installed																																																											
<input type="checkbox"/> Google Play Licensing Library	1	Not installed																																																											
<input type="checkbox"/> Google Play services	49	Not installed																																																											
<input checked="" type="checkbox"/> Google USB Driver	13	Installed																																																											
<input checked="" type="checkbox"/> Google Web Driver	2	Installed																																																											
<input checked="" type="checkbox"/> Intel x86 Emulator Accelerator (HAXM installer)	7.6.5	Installed																																																											
<input type="checkbox"/> Layout Inspector image server for API 29-30	6	Not installed																																																											
<input type="checkbox"/> Layout Inspector image server for API 31 and T	1	Not installed																																																											
<input type="checkbox"/> Layout Inspector image server for API S	3	Not installed																																																											
4	Then follow the following steps																																																												

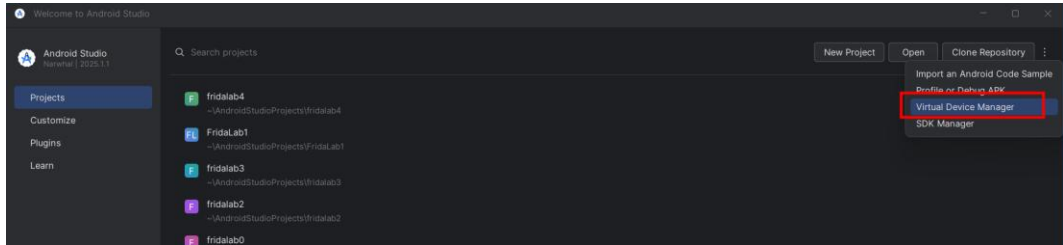
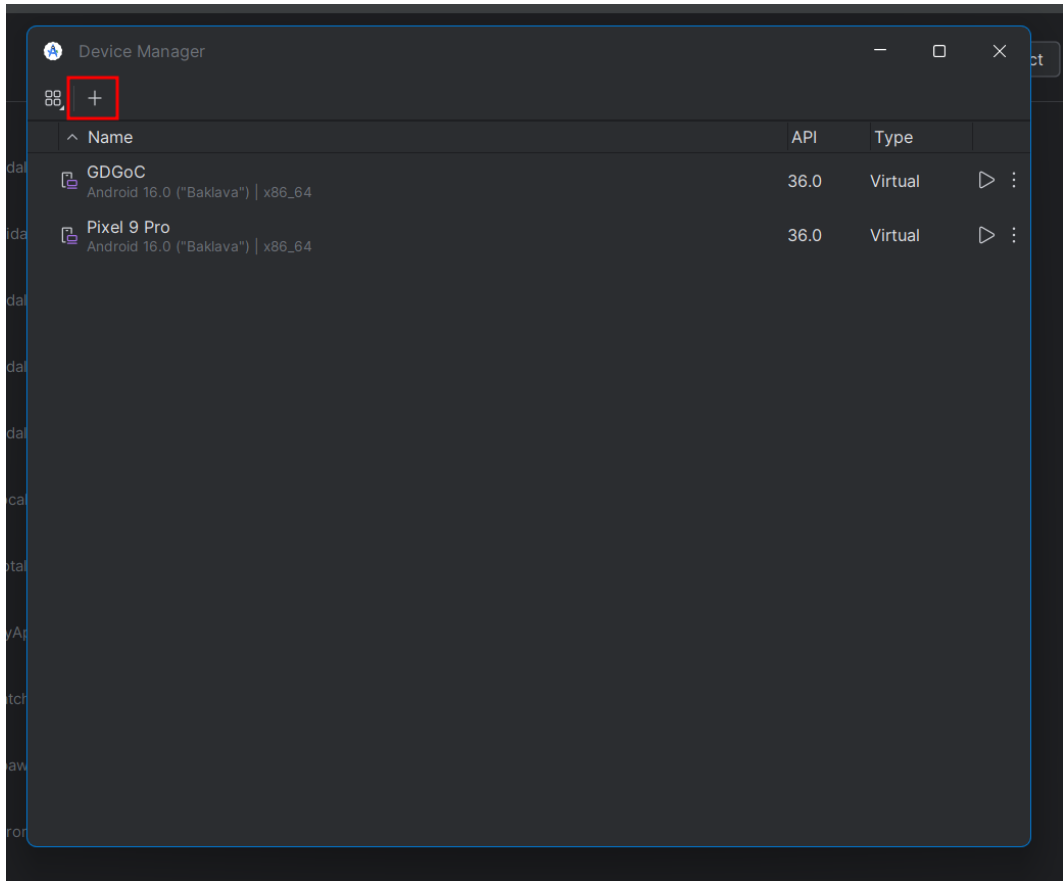
	<p>Step 4: Once installed, set the platform-tools file into the path.</p> <ul style="list-style-type: none"> <li>→ → In your search bar, type environment and click "Edit the system environment variables".</li> <li>→ Click "Environment Variables".</li> <li>→ Under "User variables," click "New".</li> <li>→ Set the variable name to "Android".</li> <li>→ 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</li> </ul> <p><b>Note:</b> You need to turn on the view hidden files function to access app data.</p> <ul style="list-style-type: none"> <li>→ Once you have verified the location of your platform tools, click "OK".</li> </ul> <p><b>Step 5:</b> Now, verify that the path is working correctly:</p> <div style="background-color: #2e3436; color: #eeeeec; padding: 5px; border: 1px solid #2e3436;"> <pre>run command line &gt; Windows key + R &gt; cmd &gt; enter</pre> </div> <p><b>Step 6:</b> 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.</p> <p>Reference: <a href="https://help.esper.io/hc/en-us/articles/12657625935761-Installing-the-Android-Debug-Bridge-ADB-Tool">https://help.esper.io/hc/en-us/articles/12657625935761-Installing-the-Android-Debug-Bridge-ADB-Tool</a></p>
5	<p>Click on SDK Manager</p> 
6	<p>Install the one highlighted here</p>



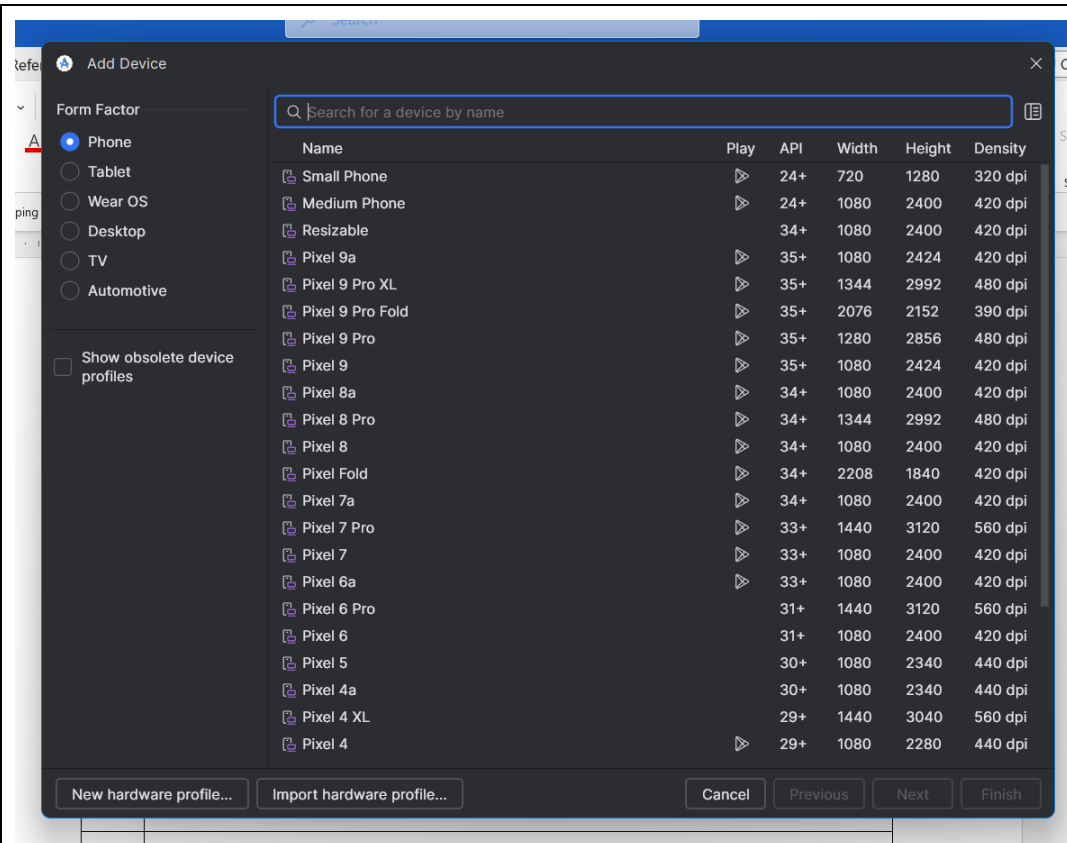
## 4 Download RootAVD

1	Install <a href="#">RootAVD</a>
---	---------------------------------

## 5 Creating and Rooting Android Virtual Device (AVD)

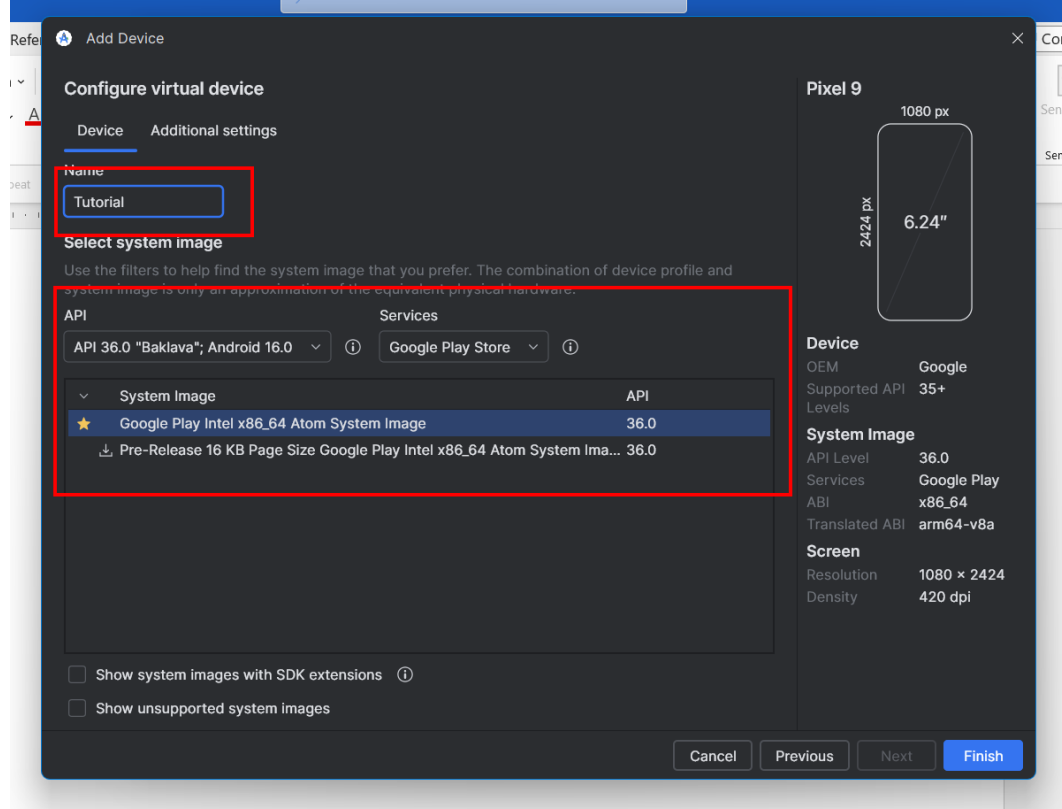
1	<p>Click on Virtual Device Manager</p> 									
2	<p>Click add</p>  <table><tr><th>Name</th><th>API</th><th>Type</th></tr><tr><td>GDGoC Android 16.0 ("Baklava")   x86_64</td><td>36.0</td><td>Virtual</td></tr><tr><td>Pixel 9 Pro Android 16.0 ("Baklava")   x86_64</td><td>36.0</td><td>Virtual</td></tr></table>	Name	API	Type	GDGoC Android 16.0 ("Baklava")   x86_64	36.0	Virtual	Pixel 9 Pro Android 16.0 ("Baklava")   x86_64	36.0	Virtual
Name	API	Type								
GDGoC Android 16.0 ("Baklava")   x86_64	36.0	Virtual								
Pixel 9 Pro Android 16.0 ("Baklava")   x86_64	36.0	Virtual								
3	<p>Choose any phone you like</p>									



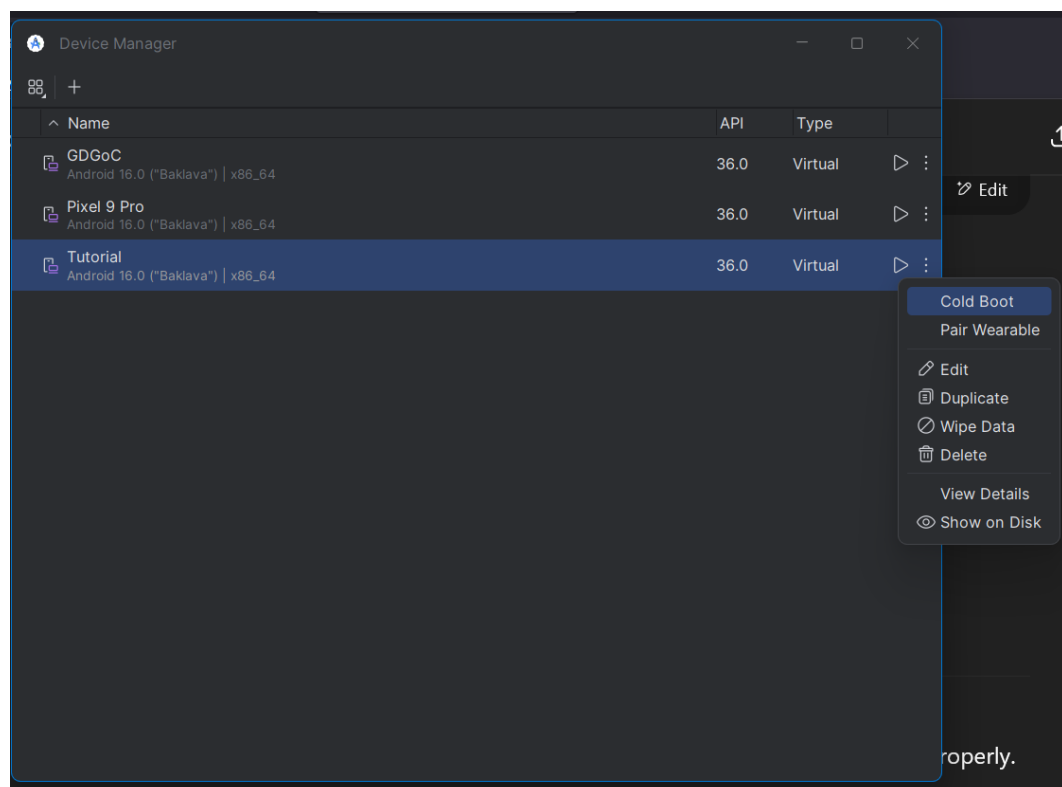


4

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**



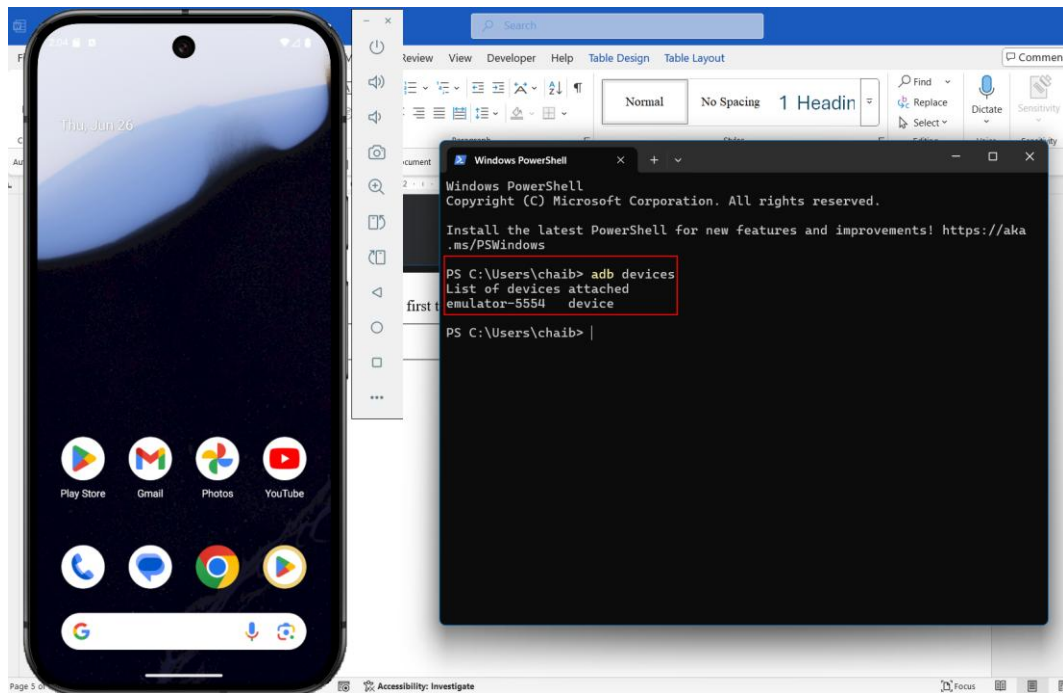
Once created, cold boot the device



The first time running the device, it will take some time to load

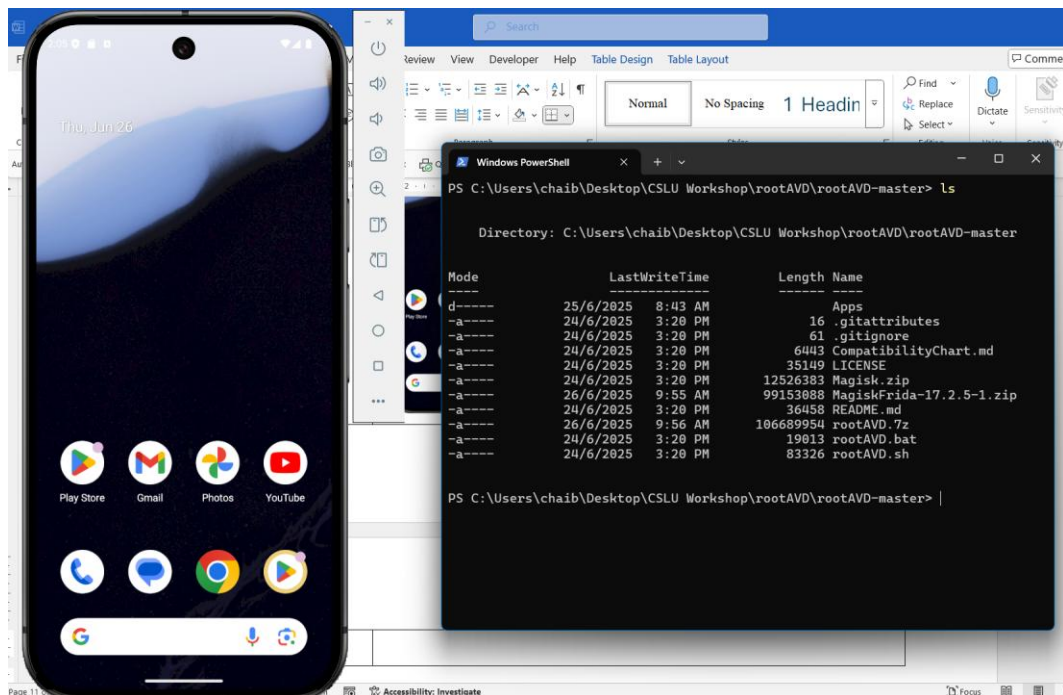
6

If you downloaded ADB correctly, you will be able to see your device in ADB once it loads



7

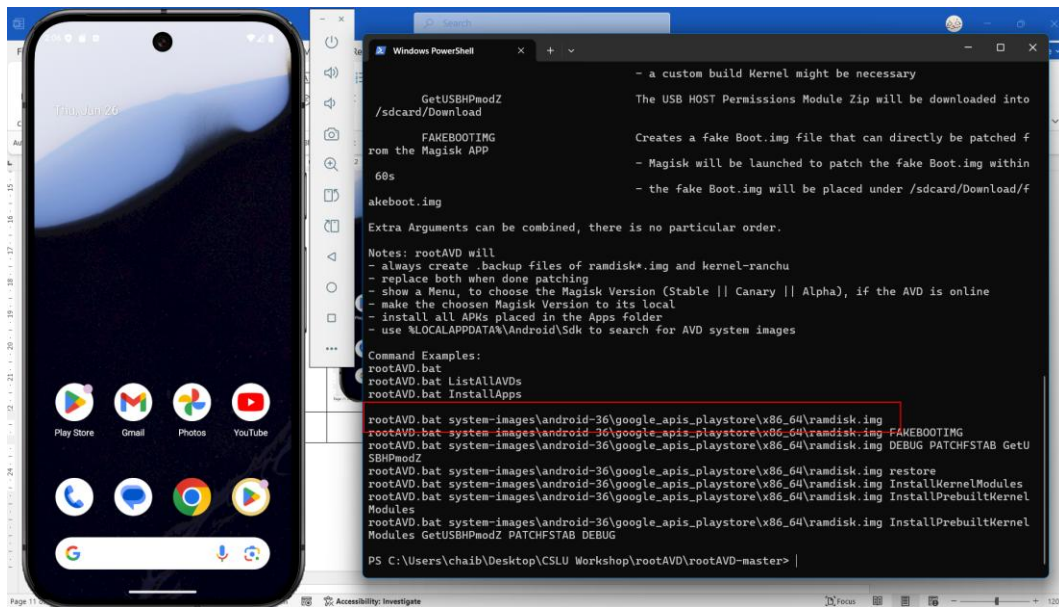
Proceed to where you had your RootAVD installed



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

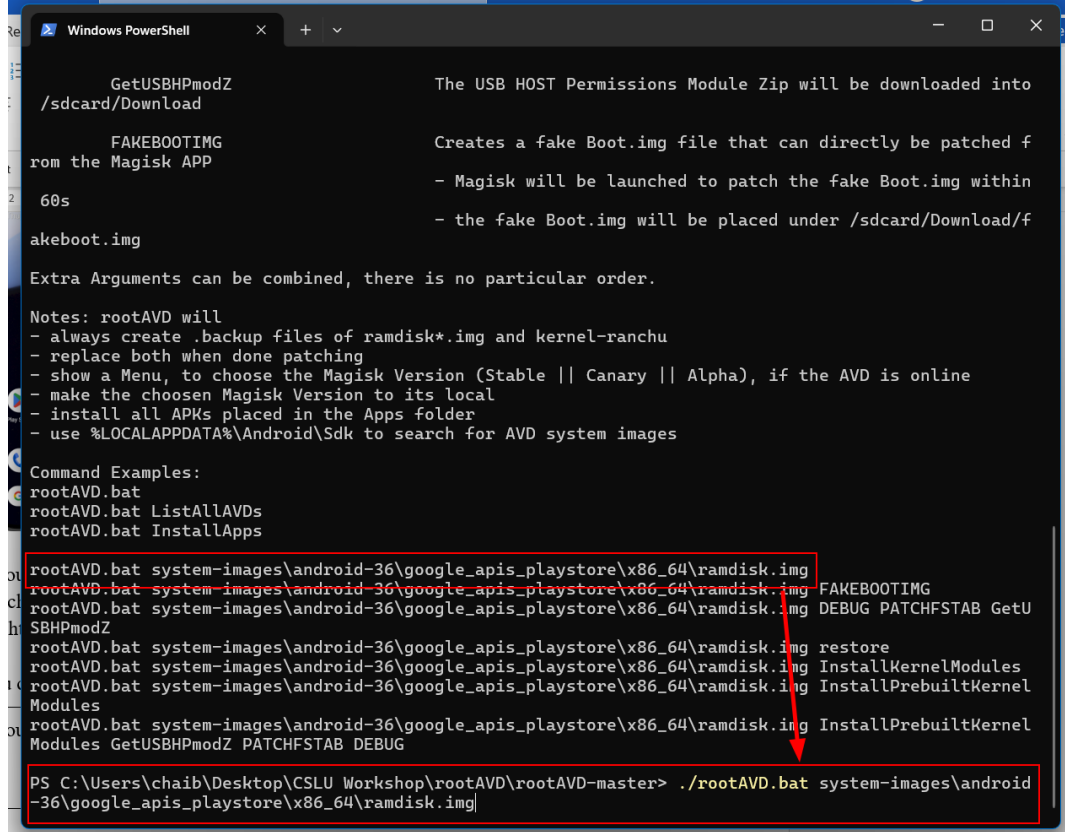


If you read closely in the highlighted line, you will be able to see android-36, matching the number you see earlier. If you don't see android-36, same like me, it might mean you installed another version.

You can use **./rootAVD.bat ListAllAVDs** to list it

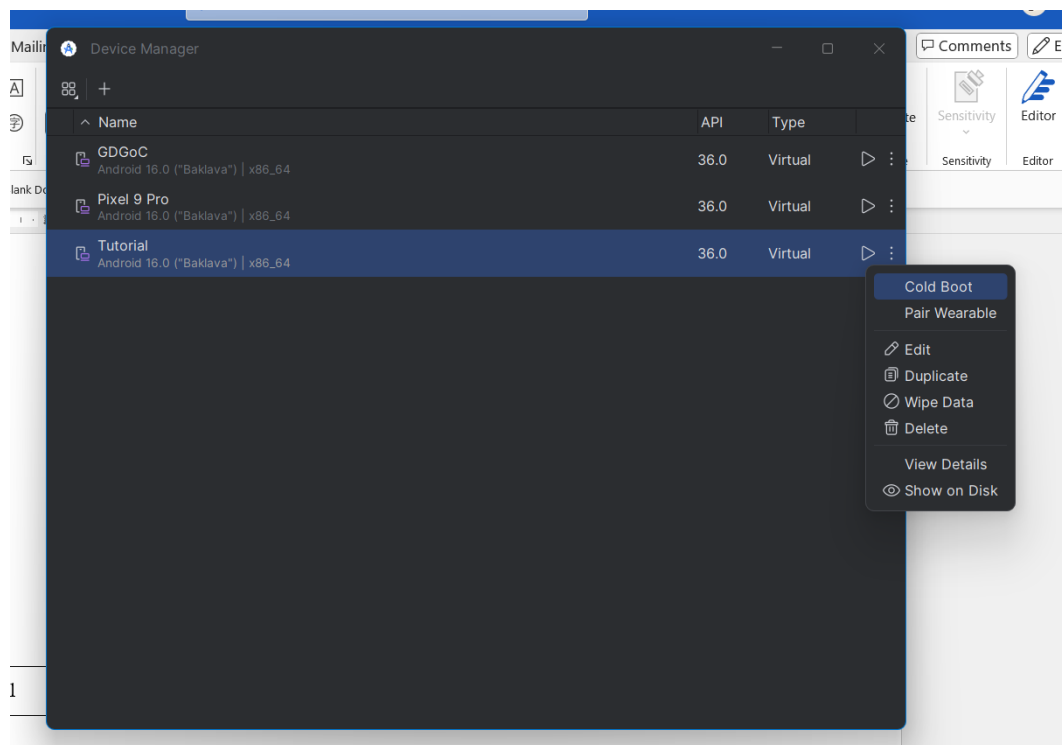
9

If you see 36 like me above, copy n paste the highlighted line and run it

	 <pre> GetUSBHPmodZ           The USB HOST Permissions Module Zip will be downloaded into /sdcard/Download  FAKEBOOTIMG           Creates a fake Boot.img file that can directly be patched f rom the Magisk APP 60s                   - Magisk will be launched to patch the fake Boot.img within akeboot.img           - the fake Boot.img will be placed under /sdcard/Download/f  Extra Arguments can be combined, there is no particular order.  Notes: rootAVD will - always create .backup files of ramdisk*.img and kernel-ranchu - replace both when done patching - show a Menu, to choose the Magisk Version (Stable    Canary    Alpha), if the AVD is online - make the choosen Magisk Version to its local - install all APKs placed in the Apps folder - use %LOCALAPPDATA%\Android\Sdk to search for AVD system images  Command Examples: rootAVD.bat rootAVD.bat ListAllAVDs rootAVD.bat InstallApps  rootAVD.bat system-images\android-36\google_apis_playstore\x86_64\ramdisk.img rootAVD.bat system-images\android-36\google_apis_playstore\x86_64\ramdisk.img FAKEBOOTIMG rootAVD.bat system-images\android-36\google_apis_playstore\x86_64\ramdisk.img DEBUG PATCHFSTAB GetU SBHPmodZ rootAVD.bat system-images\android-36\google_apis_playstore\x86_64\ramdisk.img restore rootAVD.bat system-images\android-36\google_apis_playstore\x86_64\ramdisk.img InstallKernelModules rootAVD.bat system-images\android-36\google_apis_playstore\x86_64\ramdisk.img InstallPrebuiltKernel Modules rootAVD.bat system-images\android-36\google_apis_playstore\x86_64\ramdisk.img InstallPrebuiltKernel Modules GetUSBHPmodZ PATCHFSTAB DEBUG  PS C:\Users\chaib\Desktop\CSLU Workshop\rootAVD\rootAVD-master&gt; ./rootAVD.bat system-images\android -36\google_apis_playstore\x86_64\ramdisk.img </pre>
10	<p>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.</p>

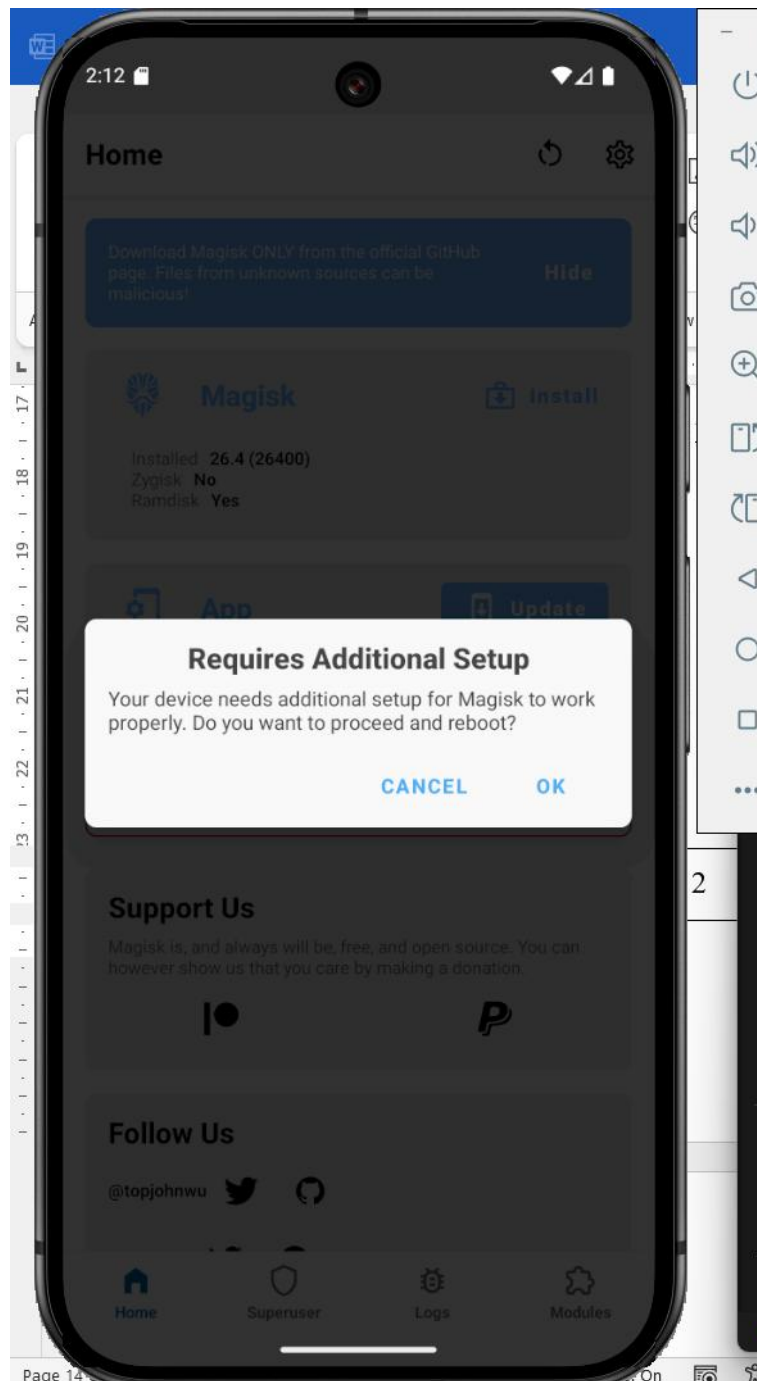
```
Windows PowerShell
[-] copy all x86_64 files from /data/data/com.android.shell/Magisk/lib/x86_64 to /data/data/com.and
roid.shell/Magisk
[-] copy 'stub.apk' from /data/data/com.android.shell/Magisk/assets to /data/data/com.android.shell
/Magisk
[*] Detecting ramdisk.img compression
[!] Ramdisk.img uses lz4_legacy compression
[-] taken from shakalaca's MagiskOnEmulator/process.sh
[*] executing ramdisk splitting / extraction / repacking
[-] API level greater then 30
[*] Check if we need to repack ramdisk before patching ..
[*] After decompressing ramdisk.img, magiskboot will work
Detected format: [lz4_legacy]
[!] allowing MANAGE_EXTERNAL_STORAGE permissions to...
[-] Checking ramdisk STATUS=1
[-] Magisk patched boot image detected
[*] Verifying Boot Image by its Kernel Release number:
[-] This AVD = 6.6.66-android15-8-gb66429556fb8-ab13070261
[-] Ramdisk = 6.6.66-android15-8-gb66429556fb8-ab13070261
[!] Ramdisk is probably from this AVD
[*] repacking back to ramdisk.img format
[!] Rename Magisk.zip to Magisk.apk
[*] Pull ramdiskpatched4AVD.img into ramdisk.img
[-] /data/data/com.android.shell/Magisk/ramdiskpatched4AVD.img: 1 file pulled, 0 skipped. 89.6 MB/s
(2417335 bytes in 0.026s
[*] Pull Magisk.apk into Apps
[-] /data/data/com.android.shell/Magisk/Magisk.apk: 1 file pulled, 0 skipped. 102.7 MB/s (12526383
bytes in 0.116s
[-] Clean up the ADB working space
[-] Install all APKs placed in the Apps folder
[*] Trying to install APPS\Magisk.apk
[-] Performing Streamed Install
[-] Success
[-] Shut-Down and Reboot [Cold Boot Now] the AVD and see IF it worked
[-] Root and Su with Magisk for Android Studio AVDs
[-] Modded by NewBit XDA - Jan. 2021
[*] Huge Credits and big Thanks to topjohnwu, shakalaca and vvb2060
[-] Trying to shut down the AVD
[!] If the AVD doesnt shut down, try it manually!
PS C:\Users\chaib\Desktop\CSLU Workshop\rootAVD\rootAVD-master> |
```

To restart, click coldboot again



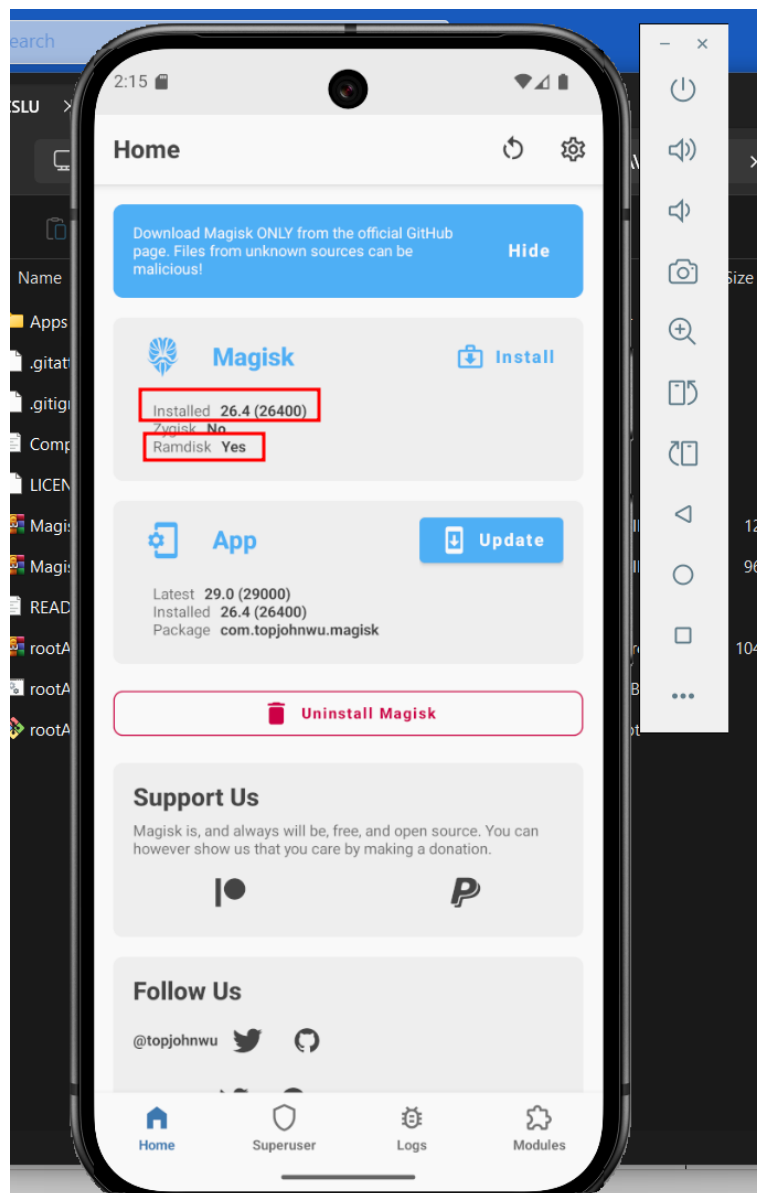
Once started, open Magisk. If you are opening Magisk for the first time, it will ask you to restart the phone, just click Yes. It will restart automatically, don't do anything.

12



13

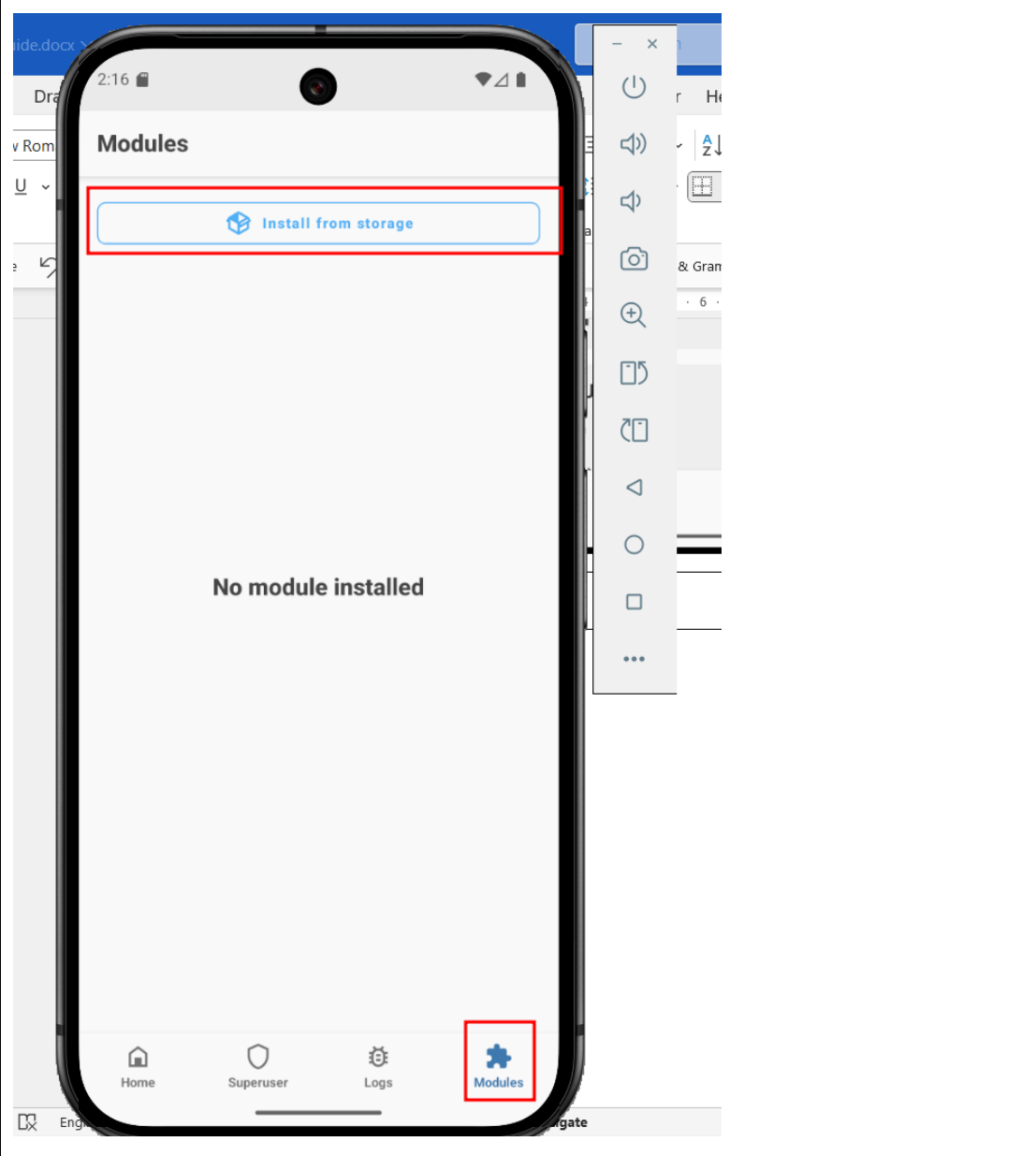
If you see the same output as me, then your AVD is rooted properly

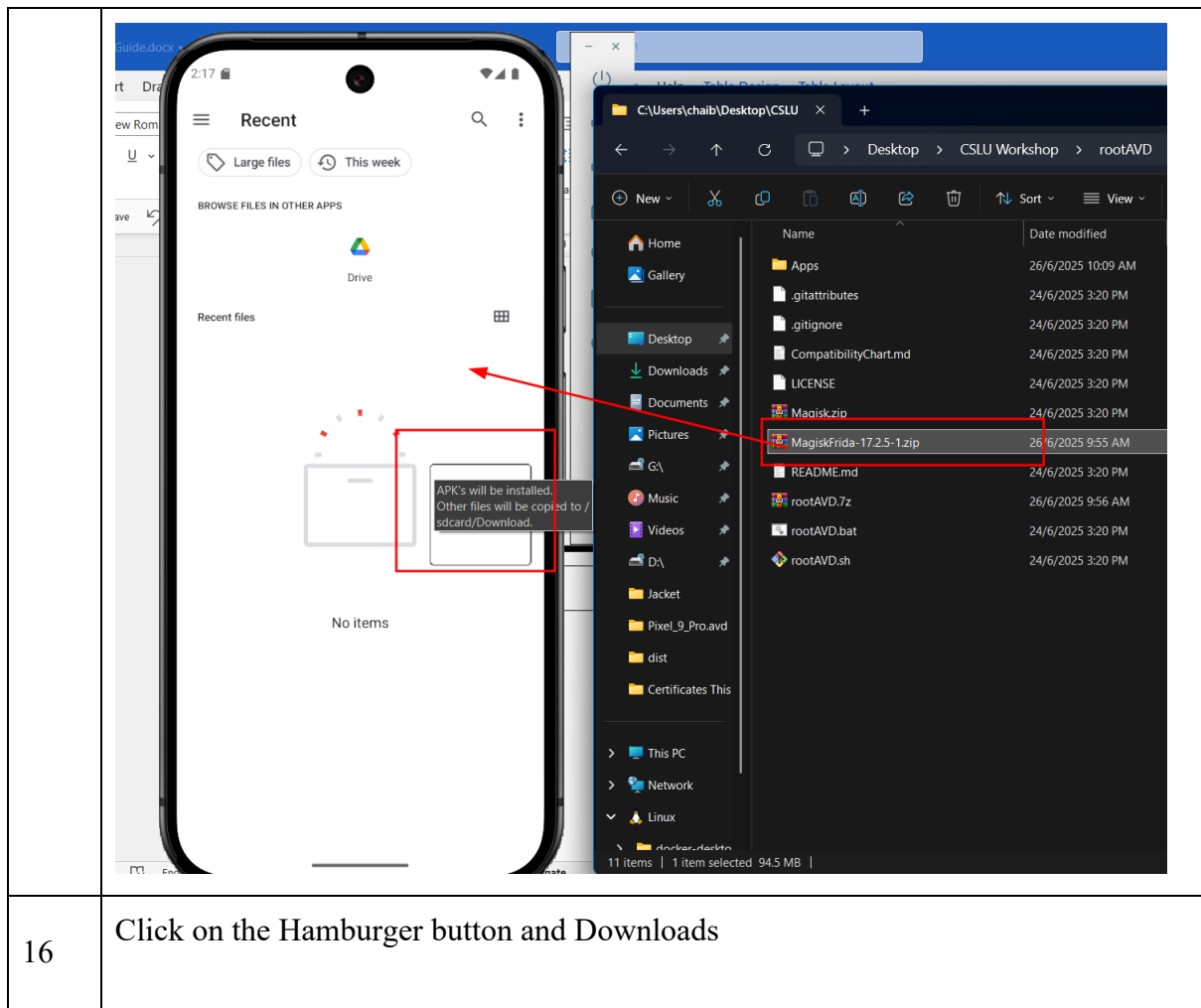


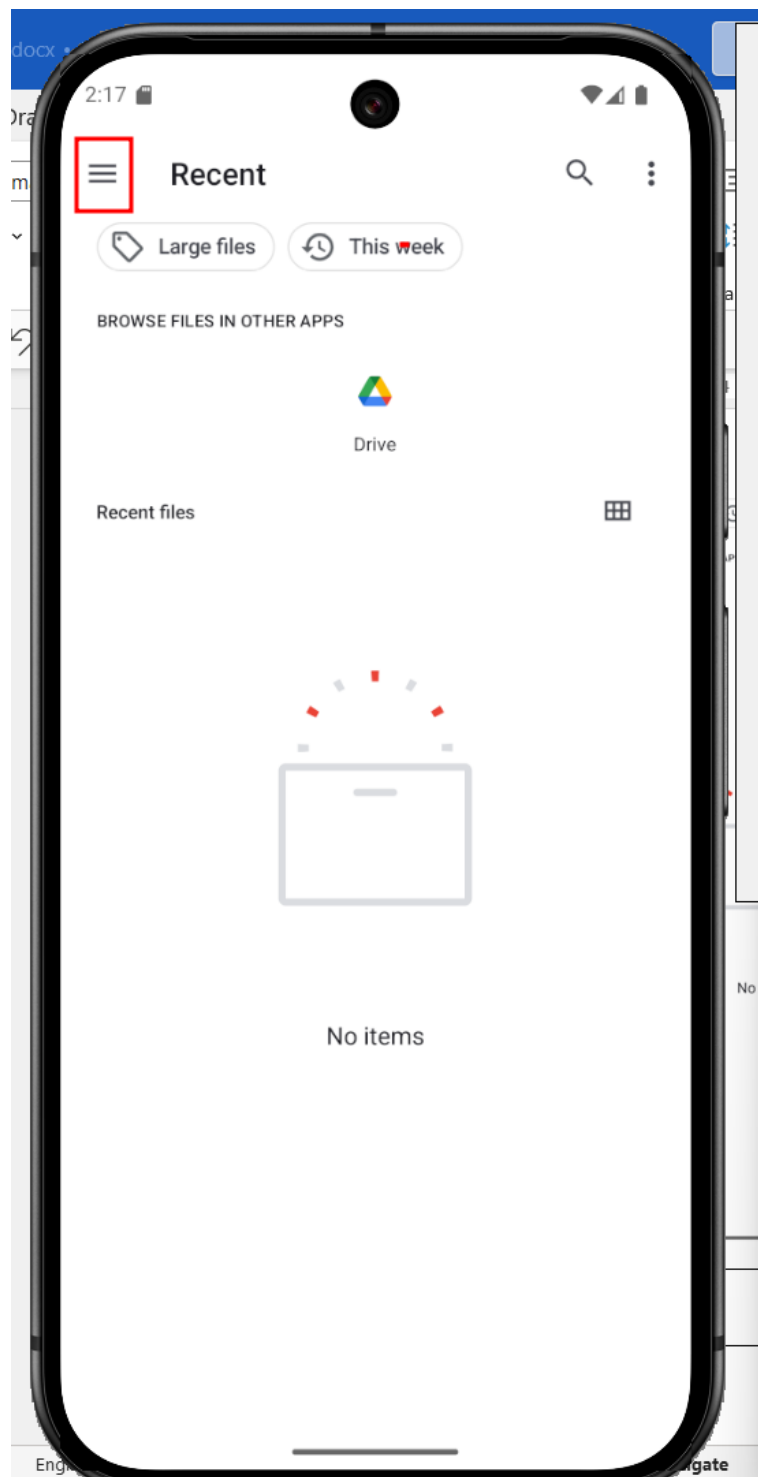
14

Click on Modules then Install



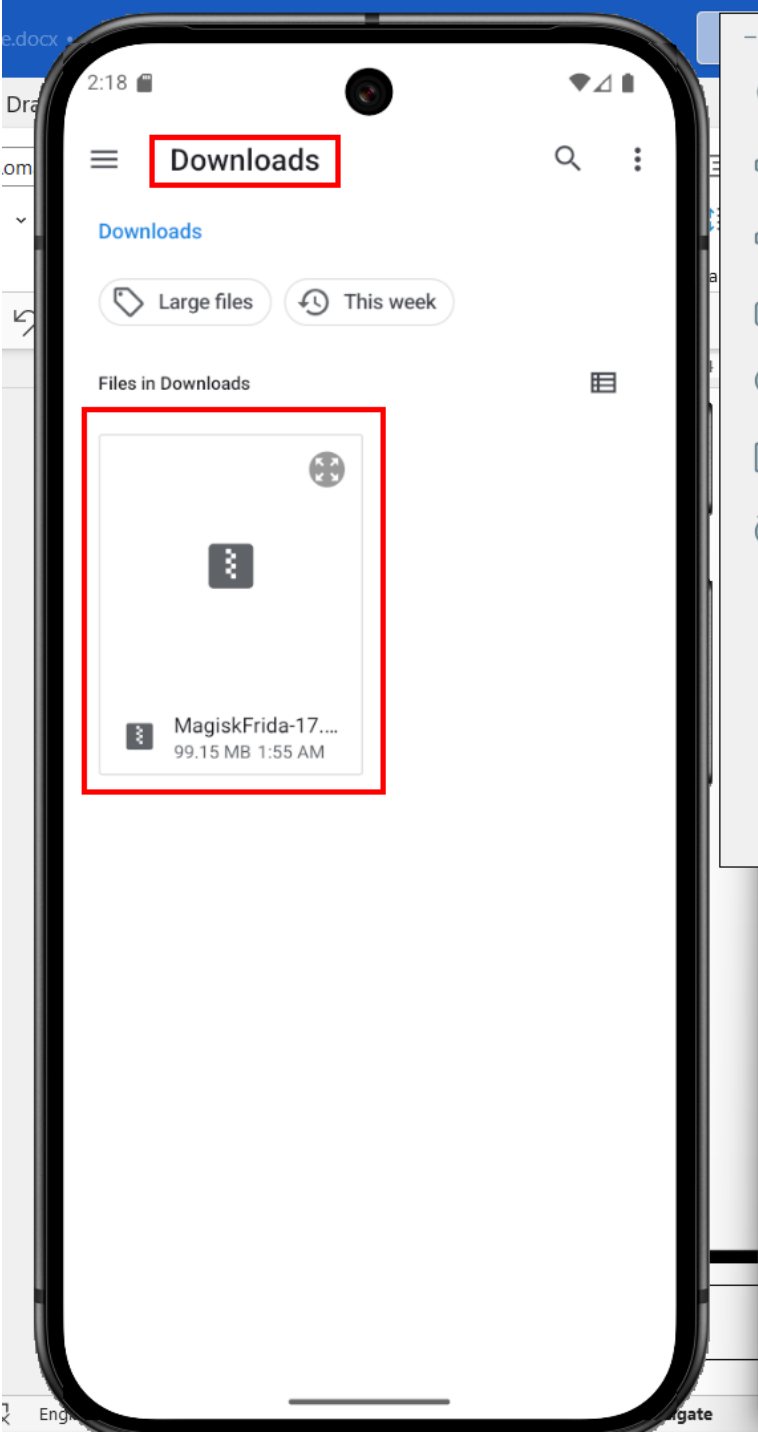
	
15	Drag and drop MagiskFrida zip file into the phone

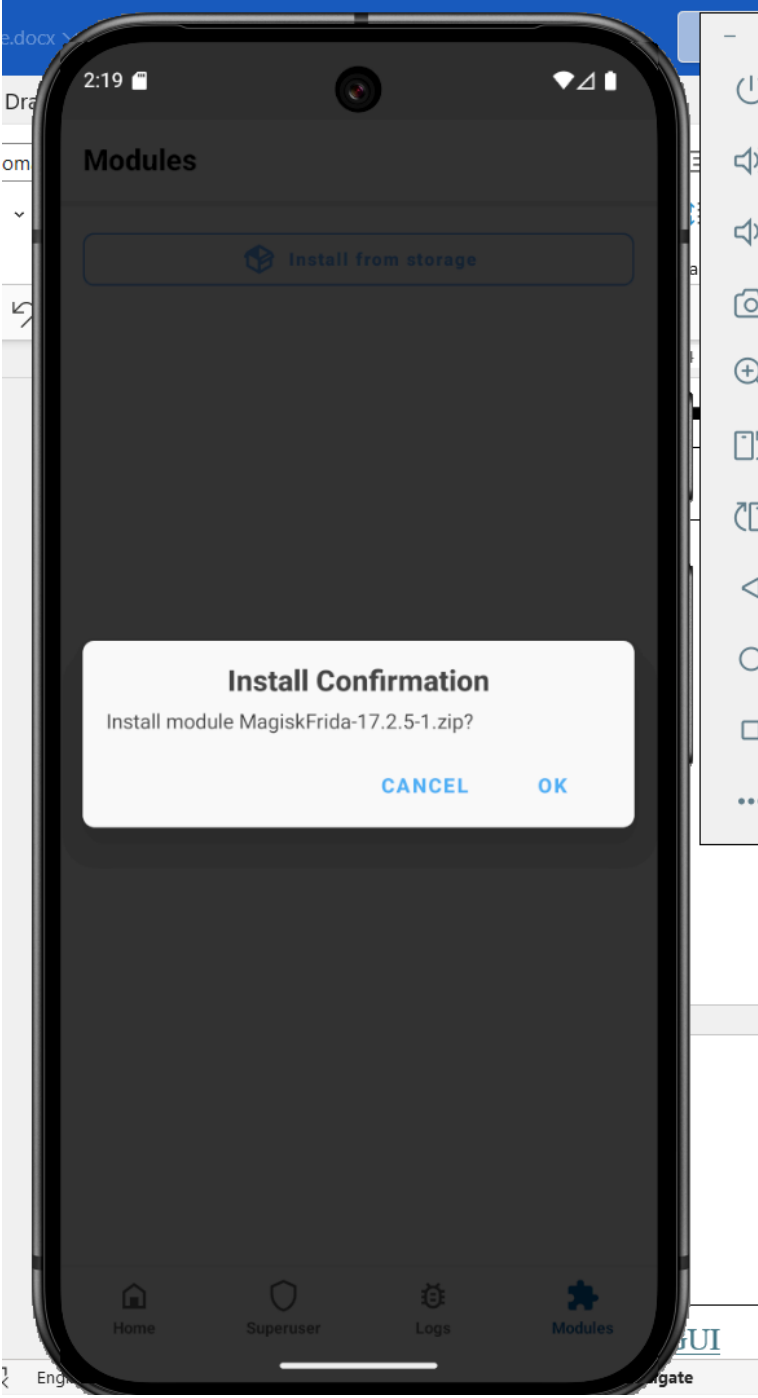


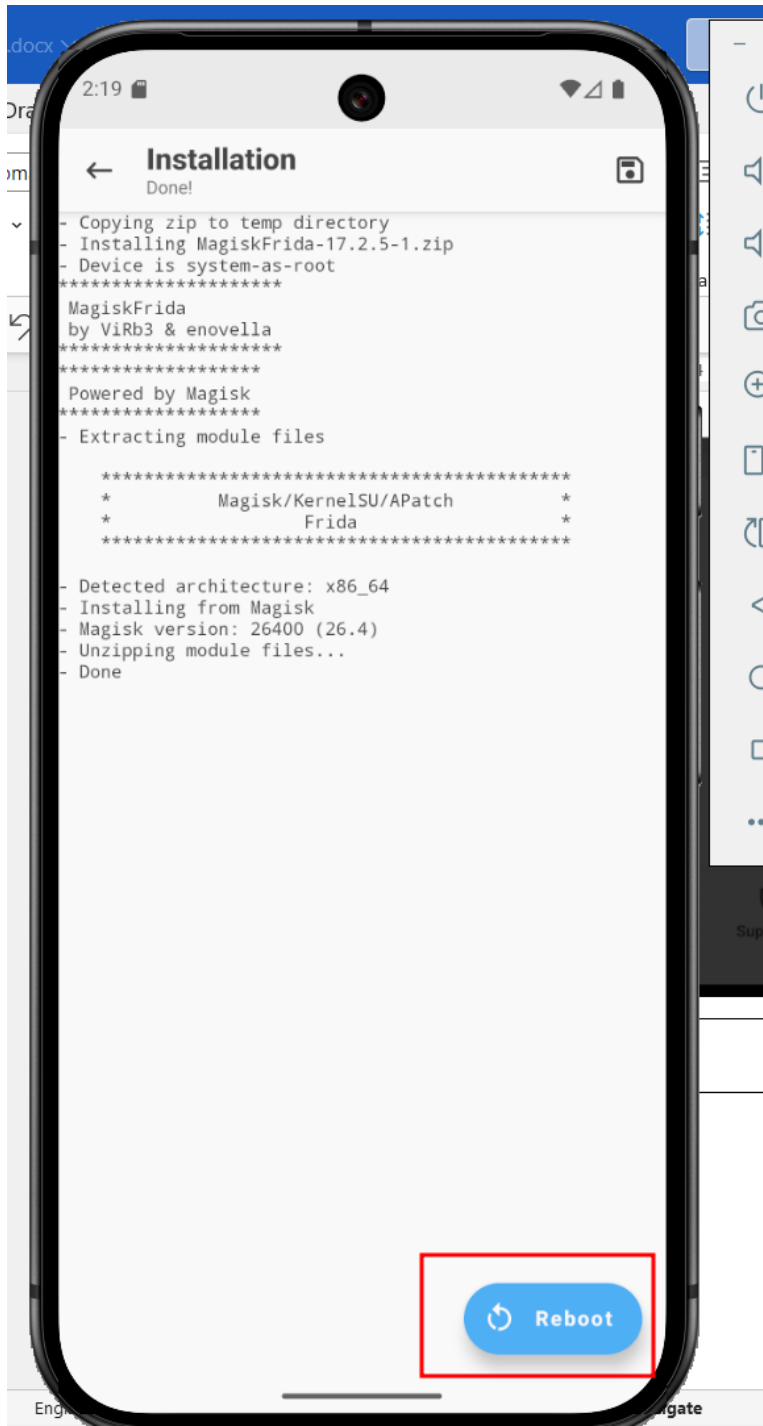


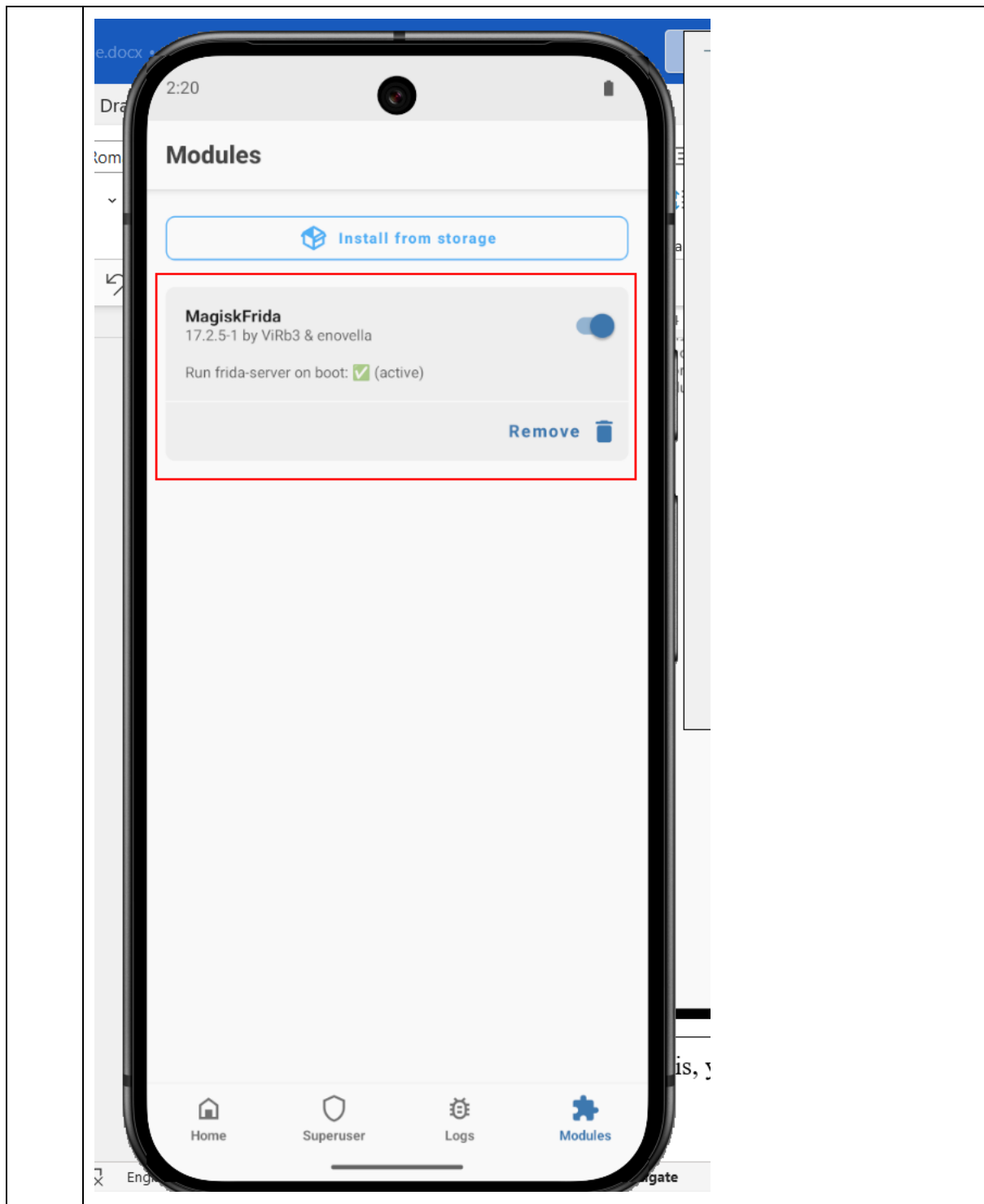
17

Click on the MagiskFrida file

	 <p>2:18</p> <p><b>Downloads</b></p> <p>Downloads</p> <p>Large files This week</p> <p>Files in Downloads</p> <p><b>MagiskFrida-17....</b> 99.15 MB 1:55 AM</p>
18	Install

	 A screenshot of a smartphone screen displaying the Magisk application interface. The screen is dark-themed. At the top, the status bar shows the time 2:19 and battery level. The main header is "Modules". Below it is a button labeled "Install from storage". A white dialog box is centered on the screen with the title "Install Confirmation" and the text "Install module MagiskFrida-17.2.5-1.zip?". At the bottom of the dialog are two buttons: "CANCEL" and "OK". The bottom navigation bar has four icons: Home, Superuser, Logs, and Modules (which is highlighted). <p>19</p> <p>Reboot</p>
--	---

	 <p>The screenshot shows a smartphone screen with the Magisk installation interface. The title bar at the top says "Installation" with a back arrow on the left and a save icon on the right. Below the title, it says "Done!". The main content area displays a list of installation steps in a monospaced font:</p> <ul style="list-style-type: none"><li>- Copying zip to temp directory</li><li>- Installing MagiskFrida-17.2.5-1.zip</li><li>- Device is system-as-root</li><li>*****</li><li>MagiskFrida</li><li>by ViRb3 &amp; enovella</li><li>*****</li><li>Powered by Magisk</li><li>*****</li><li>- Extracting module files</li><li>*****</li><li>*                    Magisk/KernelSU/APatch                    *</li><li>*                                    Frida                                    *</li><li>*****</li><li>- Detected architecture: x86_64</li><li>- Installing from Magisk</li><li>- Magisk version: 26400 (26.4)</li><li>- Unzipping module files...</li><li>- Done</li></ul> <p>At the bottom right of the screen, there is a blue button with a circular arrow icon and the text "Reboot". This button is highlighted with a red rectangular box.</p>
20	Once you see this, you are set



## 6 JADX-GUI

1	Install <a href="#">JADX-GUI</a>
---	----------------------------------