

- 科大讯飞AI学习机破解安装第三方应用教程

- 第三方应用安装（又称：升级软件法）

- 思路
    - 实践

- 第一步：确认cpu的厂商
    - 第1.1步（通过UI猜安卓版本）：看平板右上角的状态栏，如果像一样，那就是安卓12，如果是其他样子的，那就是安卓9
    - 第二步：修改得到apk
    - 第三步：在平板上实施“调虎离山”之计，并做到

- 自此，第三方应用安装的教程结束！完结撒花~

- 2024.2.13更新：有一种基于修改system分区以达到自动开启adb的方法，我放在了“AI学习机高阶教程（Experimental | 未完工警告）”中的“修改system分区以达到连接电脑自动打开adb”部分
  - 2024.2.20更新：新研发出一种基于修改system分区以达到root的方法（已在展讯机型测试通过）
  - 2024.2.24更新：如果你是新版本的展讯机型，你可以直接去root然后配合上“修改system分区……adb部分”强开adb，上方的教程留给未更新的老机型

- AI学习机高阶教程（Experimental | 未完工警告）

- 修改system分区以达到连接电脑自动打开adb（T10, v1.07.7实践成功，2024.2.12）

- 获取学习机的root（即刷入Magisk）

- 解锁bootloader（最重要的一集）
    - 进入download
    - 提取分区（重要：提取完请手动将system镜像复制一份，防止出意外状况后无法恢复至原来状态）
    - 修改system
    - 修改bootanim.rc（路径为system/system/etc/init/bootanim.rc），在最后面加上这么几行：
    - 取消挂载system.img：
    - 刷入system：
    - 最后效果

- 附录：一些资源及其使用方法/作用

- SPD\_Driver
    - Research Download
    - spd\_dump及CVE-2022-38694\_unlock\_bootloader项目

# 科大讯飞AI学习机破解安装第三方应用教程

- 本项目欢迎各位读者开issue，本项目秉承公益的原则，故禁止倒卖！被骗的欢迎开issue来提供骗子个人信息！
- 如果看不了图片，你可以去下载WattToolkit，里面有“Github加速”功能；或者你也可以把这个项目克隆到本地，然后下个VScode，Vscode中下一个OfficeViewer插件就能看了

## 第三方应用安装（又称：升级软件法）

### 思路

- 制作可以打开隐藏的activity的apk（包名得是应用商店可下载的软件的包名，且将版本号更改为9999999999），然后拿钉钉、QQ、微信等聊天软件传上去，进行“更新”，后面通过这个途径达到开启adb的效果。

### 实践

#### 第一步：确认cpu的厂商

打开平板上的“设置”app，点到“我的设备”，看到“处理器”一栏，一般这里会显示“Unisoc”“Qualcomm”等字样，那你就完成了第一步，且证明了该设备系统版本为安卓9

第1.1步（通过UI猜安卓版本）：看平板右上角的状态栏，如果像是其他样子的，那就是安卓9



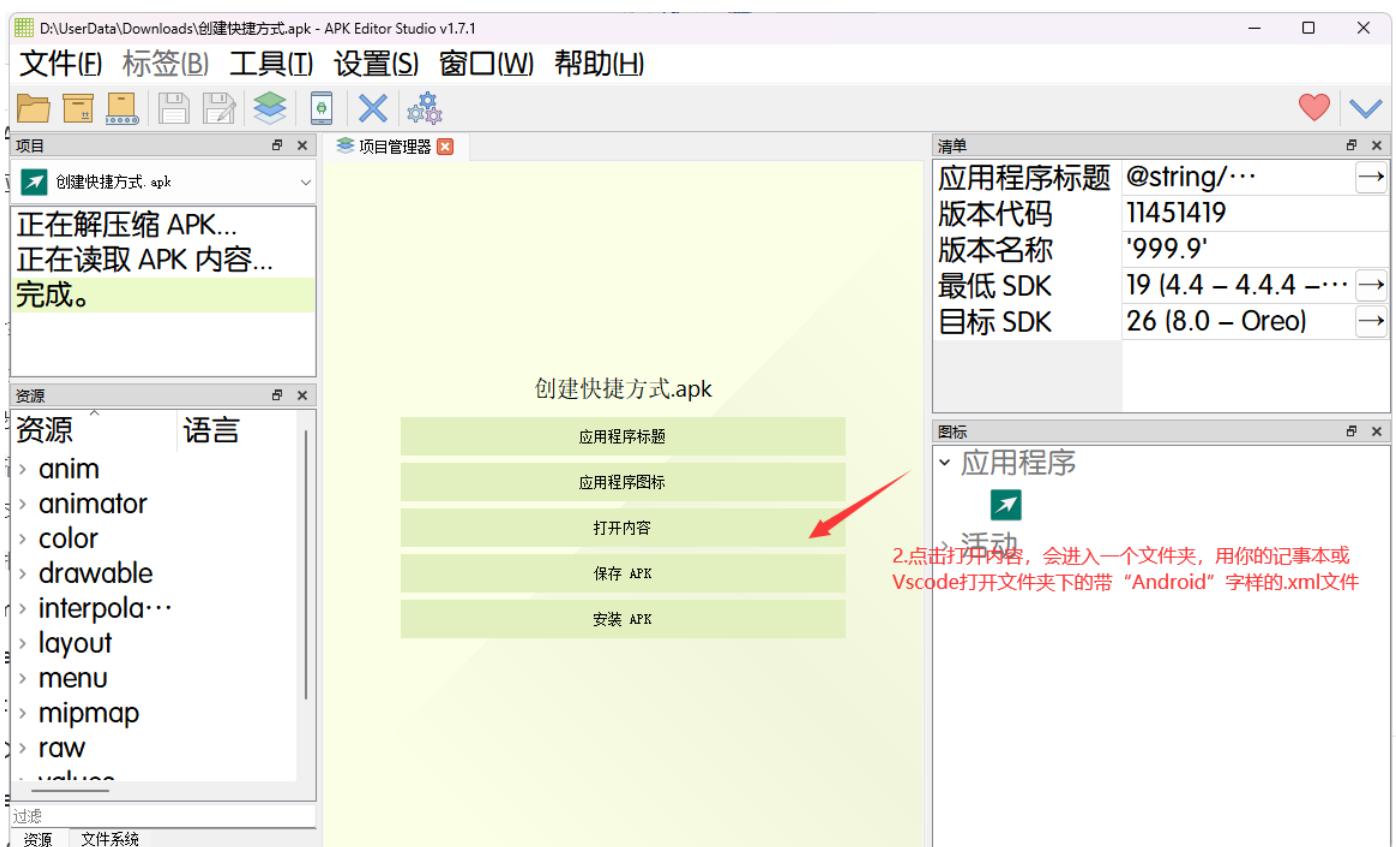
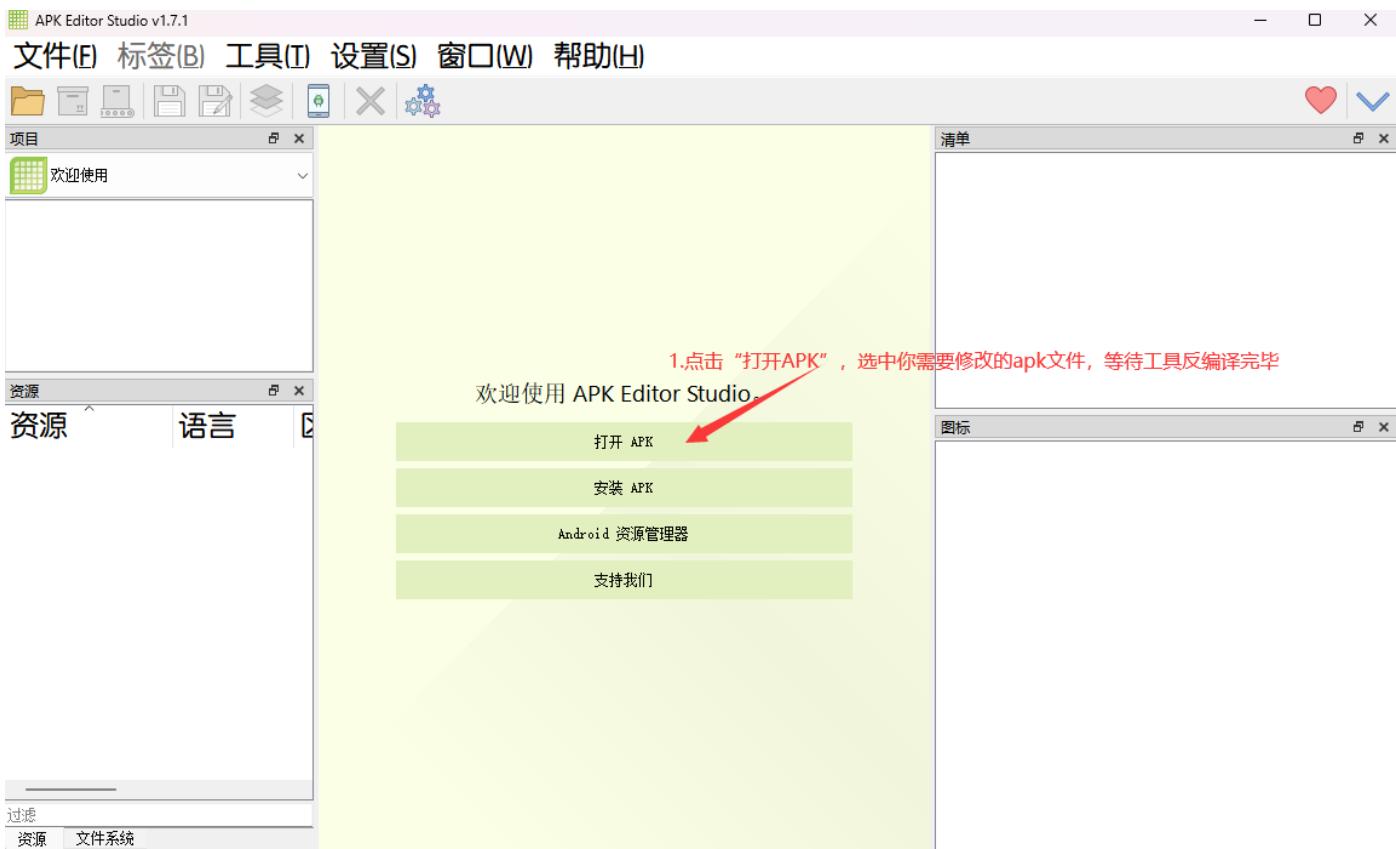
一样，那就是安卓12，如

#### 第二步：修改得到apk

准备文件：

- [APK Editor Studio\(\)](#)
- 创建快捷方式.app(这里的是洋葱学园改版，你需要将它包名改为你需要的)
- 展讯特有的adb/下载模式驱动
- [adb工具下载及环境配置（一看就会）](#)

然后，打开APK Editor Studio



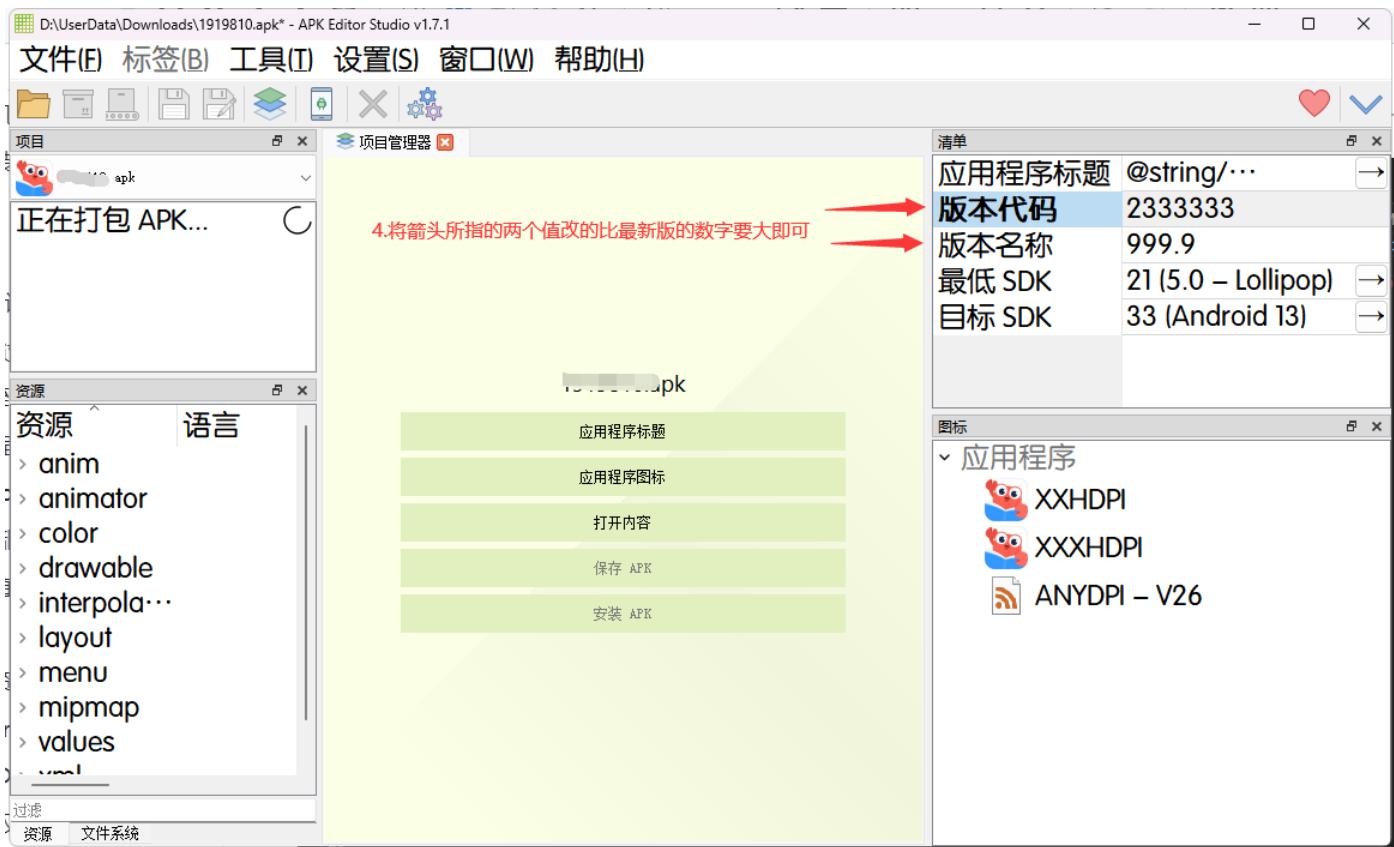
```
1.md  AndroidManifest.xml
C: > Users > Administrator > AppData > Local > Temp > apk-editor-studio > apk > {e83a6935-fb35-4a36-be15-4102f2b7bd8b} > AndroidManifest.xml
1   <versionCode="9" package="com.yangcong345.android.phone" platformBuildVersionCode="117" platformBuildVersionName="1.17">
2       3.在这个xml文件的第一行中有个package="<包名>"的东西，你将双括号中的包名改成你自己那里那个可以替换的软件的包名
3
4
5
6   <name" android:largeHeap="true" android:supportsRtl="true" android:theme="@style/ThemeApp">
7     v4.content.FileProvider">
8
9
10
11
12
13
14
15
16
17
18
19
20   <:theme="@android:style/Theme.Translucent.NoTitleBar"/>
21   <:theme="@android:style/Theme.Translucent.NoTitleBar"/>
22   <:theme="@android:style/Theme.Translucent.NoTitleBar"/>
23
24
25
```

自此，准备工具的制备告一段落，你需要点“保存apk”来保存你来之不易的成果。

第三步：在平板上实施“调虎离山”之计，并做到

3.1：通过某种方式将你的劳动成果从电脑上传到平板上（QQ、微信、钉钉，甚至是USB传输也行），打开下载好的apk文件，此时正常会弹出软件更新，点击继续，然后直接返回桌面，长按被替换的软件并卸载，卸载之后会看到之前的应用更新，一路无脑安装即可，打开创建快捷方式后右上角菜单把三个方框勾上

3.2.1（“设置-我的设备”中看到自己是“Qualcomm”的情况）：在“打开快捷方式”app中搜索“搜索建议”，点右边绿色的“详情”按钮，点“打开”然后如下图操作



然后点几次"版本号"就能打开开发者，进而打开"USB 调试"

3.2.2 ("设置-我的设备"中看到自己是"Unisoc"的情况)：在步骤3.1完成后直接在"打开快捷方式"中向下翻到***EngineerMode***那一项(包名为**com.sprd.engineermode**)，然后点"活动列表"，点开最顶上那一个的"详情"，然后点"打开"，切换到"DEBUG&LOG"选项卡，向下滑找到"USB Debug"并打开该选项

到这里，你已经成功开启了**adb**，可以进入下一个步骤了！加油，达瓦里氏，胜利就在眼前！

3.3 安装adb驱动和爱玩机工具箱，并授予工具箱MDM权限，来实现软件安装的本地化、自主可控化

下载：[爱玩机工具箱\(com.byyoung.setting\) - S-22.0.8.1 - 应用 - 酷安 \(coolapk.com\)](#)

[Download SPD Driver R4.20.4201 \(UniSoc Driver\) \(androiddatashost.com\)](#)

你在第二部准备工作还下了一个压缩包 (.zip) 文件，你需要把它解压到一个目录。然后将下载的爱玩机工具箱移到那个解压的目录中，并在上方的地址栏输入"cmd",能打开一个窗口，你需要输入如下内容

```
adb install <apk文件路径 (我更建议你打个空格，然后直接将apk文件拖进来，windows会自动识别路径) >
```

然后，点开平板上的“爱玩机工具箱”app，你需要进到“权限中心”，并照着应用提示，启用最下面的“高级设备管理员（带防卸载）”即可。后面，你可以在“导航——应用相关——应用安装器”中自行启用“激活此安装器”，本篇不过多赘述。

建议在破解后删除“系统更新”应用，命令如下：

```
adb shell pm uninstall -k --user 0 com.iflytek.study.ota
```

这样是为了防止KDXF官方后续对该方法完全的封杀

自此，第三方应用安装的教程结束！完结撒花~

**2024.2.13更新：**有一种基于修改**system**分区以达到自动开启**adb**的方法，我放在了["AI学习机高阶教程（Experimental | 未完工警告）"](#)中的“修改**system**分区以达到连接电脑自动打开**adb**”部分

**2024.2.20更新：**新研发出一种基于修改**system**分区以达到**root**的方法（已在展讯机型测试通过）

**2024.2.24更新：**如果你是新版本的展讯机型，你可以直接去**root**然后配合上“修改**system**分区……**adb**部分”强开**adb**，上方的教程留给未更新的老机型

# AI学习机高阶教程（Experimental | 未完工警告）

Warning: 下列操作较为危险，有几率导致平板变砖，三思而行（我们现在暂时还没有出刷机包，救不回来，官方刷机费一次要60大洋）

## 修改**system**分区以达到连接电脑自动打开**adb**（T10, v1.07.7实践成功，**2024.2.12**）

1.先去下载spd\_dump程序和任意ud710设备的fdl1/2文件并安装驱动（这些东西详见[附录：一些资源及其使用方法/作用](#),fdl1/2我用的天翼一号2021的，可以在CVE-2022-38694\_unlock\_bootloader项目Release中找到，你下载压缩包就ok） 2.你需要解压这个压缩包然后在解压目录下打开cmd，并输入：

```
spd_dump fdl <fdl1路径, 将文件拖拽到命令行即可自动生成> 0x5500 fdl <fdl2路径, 将文件拖拽到命令行即可自动生成> 0x9efffe00 exec partition_list partition.xml ##得到当前机型分区表
```

打开你备份的分区表文件partition.xml，看到**system**这一栏，后面**size**里的数字就是你需要的（注：这个提取出的分区表的单位为**MB**，所以你写命令时要在数字后加**M**），然后你需要重进下载模式，输入：

```
spd_dump fdl <fdl1路径, 将文件拖拽到命令行即可自动生成> 0x5500 fdl <fdl2路径, 将文件拖拽到命令行即可自动生成> 0x9efffe00 exec read_part system 0 <分区大小, 比如100M> system.img reset ##提取system分区并保存到system.img, 在操作完成后让设备自动重启
```

你得到**system**镜像后，需要再额外复制一份，将其命名为**system\_bak.img**（防止设备成砖卡启动后无法救砖）

自此，你就得到了两份**system**，你需要使用7zip打开**system.img**，将"system"目录下的"build.prop"文件复制到**system.img**所在的目录，并使用记事本/Vscode之类的编辑器打开**build.prop**，在文件末尾加上以下4行：

```
persist.service.adb.enable=1  
service.adb.tcp.port=5555  
persist.sys.usb.config=diag,adb,mtp  
ro.sys.usb.default.config=diag,adb,mtp
```

做完这一切，保存并退出

然后下个WSL，然后在WSL终端切换到当前目录，执行以下命令

```
mkdir system  
sudo mount -o rw system.img system  
sudo rm system/system/build.prop  
sudo cp build.prop system/system/build.prop  
umount system.img
```

到这，你就改完system了，将其刷回设备上的system分区即可，你需要在cmd中运行如下命令以执行此操作：

```
spd_dump fd1 <fd11路径, 将文件拖拽到命令行即可自动生成> 0x5500 fd1 <fd12路径, 将文件拖拽  
到命令行即可自动生成> 0x9efffe00 exec write_part system system.img reset
```

大概过个半小时吧，平板就开机了，最后的效果是你一插入数据线，就会有“已连接到USB调试”的通知，这就说明你成功了

Enjoy！

## 获取学习机的root（即刷入Magisk）

为何要把root部分拿出来讲呢？因为这学习机的boot无法patch（原因是没有ramdisk）

system分区植入法目前已成功实践，rec法因为avb的原因无法正常启动，所以下文只讲system分区植入magisk法

- 大概思路：将magisk安装到安卓system分区，可以参考[某酷安大佬写的方案（Magisk system root部分）](#)

总结下来就四步：①解锁板子的bootloader（这一步已经做到能纯Windows环境下进行了），②提取system分区并进行修改，③将修改好的文件放回分区并刷回板子中以root

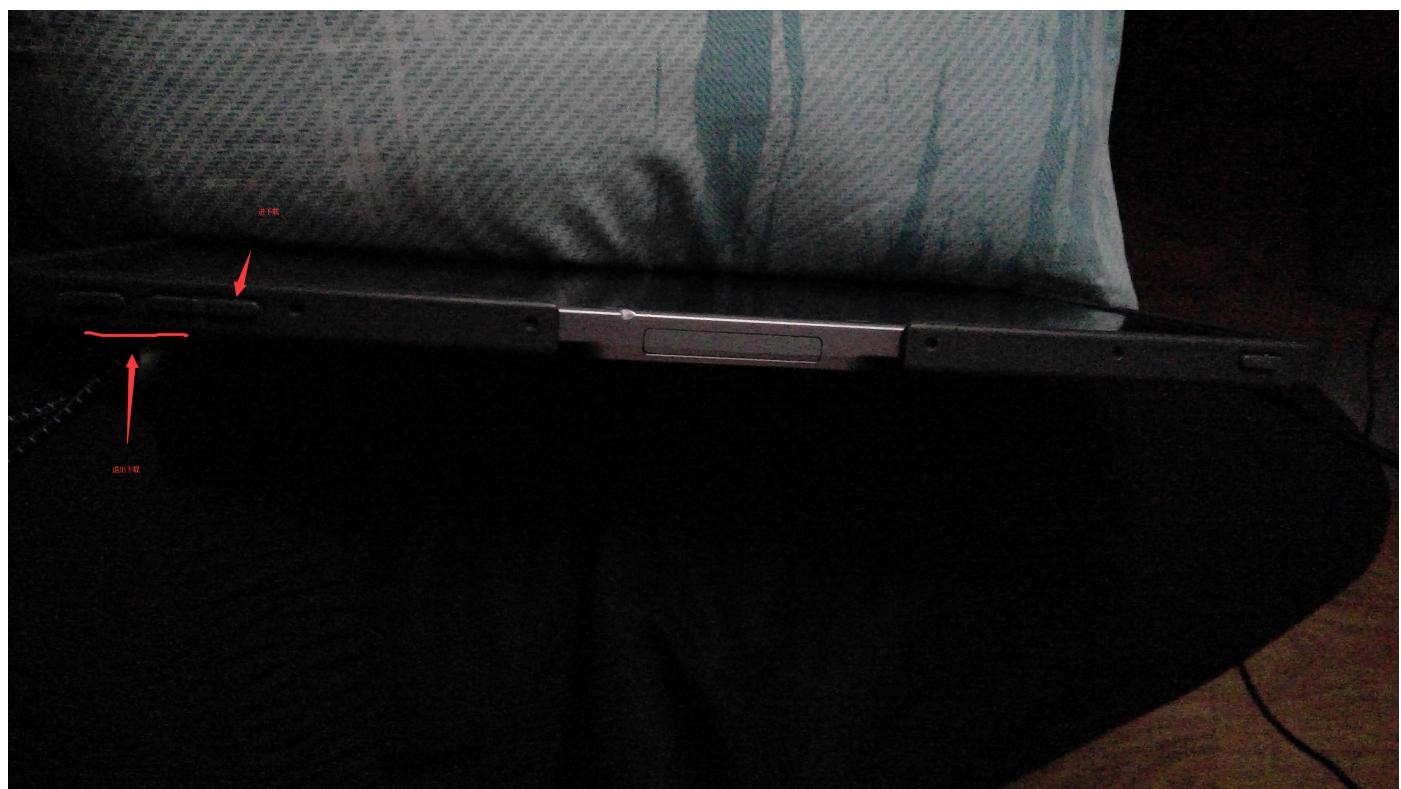
# 解锁bootloader（最重要的一集）

- 文件: <https://pan.baidu.com/s/1CS0MZdqh0nN3Xb8FstRhkA?pwd=hhef&at=1708756671115#list/path=%2F>
- 使用物理按键进入REC（提示：与Jingpad A1进入rec的方式一致），然后使用电源键+音量加的按键组合调出菜单，用音量上选择第二项，然后使用电源键进入fastboot模式，在下载下来的文件的解压目录的地址栏输入cmd，在打开的窗口中输入 fastboot devices 得到一串字母加数字，这就是你机器的序列号，在另一台安卓设备上安装“文件”中的apk，输入你得到的序列号，完事会生成一个叫signature.bin的文件，你需要将这个文件拷到当前目录(即：你cmd在的目录)
- 使用 fastboot flashing unlock\_bootloader signature.bin 的命令，进行设备解锁，然后按下音量下键，确认解锁即可，然后bootloader会进行格机
- 恭喜你，成功解锁bootloader

## 进入download

进系统后关机，然后长按音量下+插上数据线即可进入下载

附赠：按键图



提取分区（重要：提取完请手动将system镜像复制一份，防止出意外状况后无法恢复至原来状

态)

```
spd_dump fdl <fdl1> 0x5500 fdl <fdl2> 0x9efffe00 exec read_part system 0 <size>
system.img read_part vendor 0 <size> vendor.img
```

## 修改system

```
mkdir system
sudo mount -o rw system.img system
sudo cp system-root/bin/magisk system/system/bin/magisk
sudo cp system-root/bin/magiskpolicy system/system/bin/magiskpolicy
sudo cp system-root/init/magisk.rc system/system/etc/init/magisk.rc
sudo cp -r system-root/magisk
system/system/etc/init
sudo chmod 0700 -R system/system/etc/init/magisk
sudo chown -R 0 system/system/etc/init/magisk
sudo chcon -R -h u:object_r:system_file:s0 system/system/etc/init/magisk
```

修改bootanim.rc（路径为  
**system/system/etc/init/bootanim.rc**），在最后  
面加上这么几行：

```
on post-fs-data
    start logd
    exec u:r:su:s0 root root -- /system/etc/init/magisk/magiskpolicy --live --
magisk
    exec u:r:magisk:s0 root root -- /system/etc/init/magisk/magiskpolicy --live --
magisk
    exec u:r:update_engine:s0 root root -- /system/etc/init/magisk/magiskpolicy --
live --magisk
    exec u:r:su:s0 root root -- /system/etc/init/magisk/magisk64 --auto-selinux --
setup-sbin /system/etc/init/magisk /sbin
    exec u:r:su:s0 root root -- /sbin/magisk --auto-selinux --post-fs-data

on nonencrypted
    exec u:r:su:s0 root root -- /sbin/magisk --auto-selinux --service

on property:vold.decrypt=trigger_restart_framework
    exec u:r:su:s0 root root -- /sbin/magisk --auto-selinux --service

on property:sys.boot_completed=1
    mkdir /data/adb/magisk 755
```

```
exec u:r:su:s0 root root -- /sbin/magisk --auto-selinux --boot-complete  
on property:init.svc.zygote=restarting  
exec u:r:su:s0 root root -- /sbin/magisk --auto-selinux --zygote-restart  
on property:init.svc.zygote=stopped  
exec u:r:su:s0 root root -- /sbin/magisk --auto-selinux --zygote-restart
```

## 取消挂载system.img:

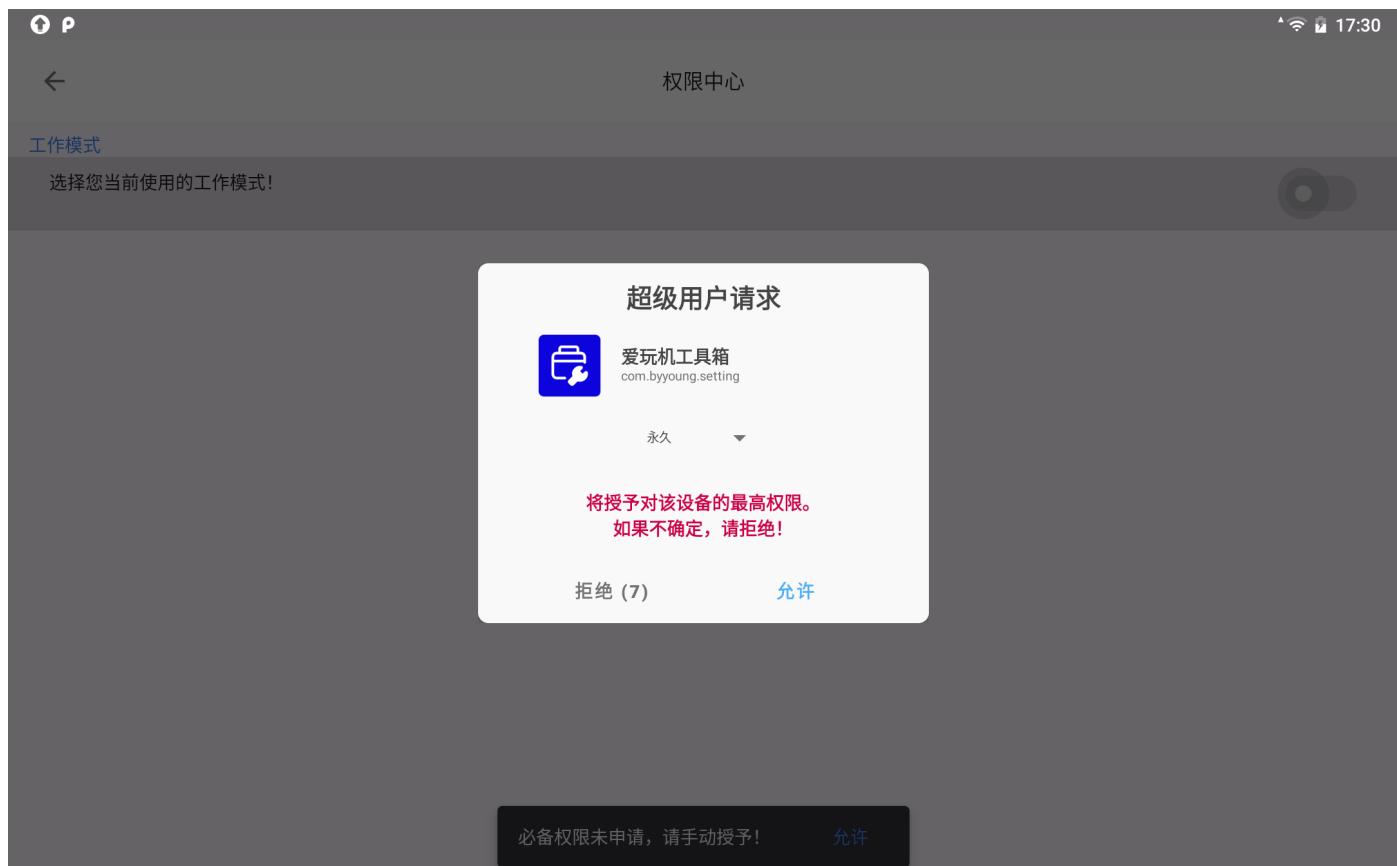
```
sudo umount system.img
```

## 刷入system:

```
spd_dump fdl <fdl1> 0x5500 fdl <fdl2> 0x9efffe00 exec write_part system system.img  
reset
```

此方法理论上通用，祝各位折腾的愉快

## 最后效果



# 附录：一些资源及其使用方法/作用

## **SPD\_Driver**

Link: [Download SPD Driver R4.20.4201 \(UniSoc Driver\) \(androiddatahost.com\)](#)

作用：ADB驱动+展讯下载模式的驱动

使用方法：下载安装即可

注：macOS、Linux不需要安装这个东西

## **Research Download**

Link: [Research Tool - SPD Flash Tool](#)

作用：读取分区、刷入分区（很危险！）

我推荐用R25.20.3901这个版本，因为它比较稳定

用法：使用[ResearchDownload为展讯机型提取镜像 - 哔哩哔哩 \(bilibili.com\)](#)

总之就是你需要pac刷机包才能用

弊端：你必须得先做个包或者先拿同SoC（比如ud710）的fdl才行，还有每次回读操作都太麻烦了，但如果不遵守就有很大可能性会出问题（比如刷砖。售后刷机一次60）

## **spd\_dump及CVE-2022-38694\_unlock\_bootloader项目**

Link: [GitHub - TomKing062/CVE-2022-38694\\_unlock\\_bootloader](#)

作用：提供了第二种进行读写设备分区操作的工具，但它是命令行的；提供了一种强解bootloader的方法（SoC漏洞），研究出来可以搞升级软件法不支持的机型安装软件；可以用这个读取平板的分区表（数据单位为MB）

用法（对于我们学习机而言）

```
spd_dump fdl fdl1.bin 0x5500 fdl fdl2.bin 0x9efffe00 exec
<read_part/write_part/erase_part> <partition_name (分区名称)> 0 <size (分区大小, 是个单位都行, 比如M (MB)、K (KB), 等等)>
```

注: write\_part\erase\_part 不需要写 0 <size> 这一部分