# 刷机资料整理

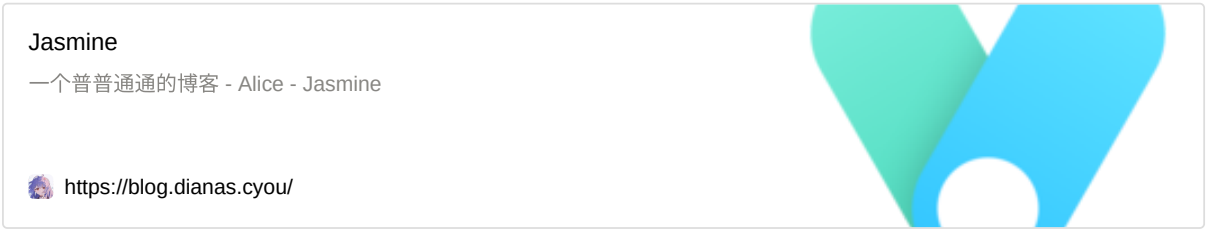
| | |
|---|---|
| Rss文稿 | |
| 关联材料 | |
| 建立日 | @July 30, 2022 7:03 PM |
| 状态 | 完毕 🙌 |
| 计划日 | |
| 读书记录 | |
| 课时数 | |
| 课题 | |

💡 **前言**：本教程仅供作者参考，阅读者**需要自己承担因尝试解锁导致的后果**。如果你对自己的动手能力感到怀疑，可以选择付费请人！**这个教程需要一台 WIN7及以上/Linux 的电脑。请先提前阅读一遍教程，而不是一步一步来。最好使用 Win10 ，避免驱动问题**

**大概有几种方法：**rec，fastboot，fastbootd，9008，mtk端口

Android 阵营厂商众多，的确很难保证他们步伐齐一，也就不存在某种一定通行的「通法」能够搞定任一 Android 设备的 `Magisk` 刷入。

本教程由 Sudoskys 引录编辑




## 几种术语[^17]

**双清:** Dalvik/ART Cache Cache 其目的就是清除分区以及数据而已，简称重置手机。

**三清:** Dalvik/ART Cache Cache Data 刷机前基本上必选三清！目的是新系统的兼容性达到最佳。

**四清:** Dalvik/ART Cache Cache Data System 四清针对版本差异过大的！ 重要！四清后不刷入系统无法开机进系统！！只能电脑刷或者储存卡刷，请谨慎！

**五清:** Dalvik/ART Cache Cache Data System Internal Storage（内置储存） 一旦选了这个清除，那手机内置存储上的东西就都没有了！就不能从手机选择卡刷包了！

**六清:** Dalvik/ART Cache Cache Data System.

**底包:**既不是ROM也不是OTA软件包，它是一组低级驱动程序，可帮助操作系统完成其想做的任何事情。 它包括调制解调器，蓝牙，引导程序，DSP等各种内容。支持所有Snapdragon和MTK设备，包括仅限中国的设备。底包就相当于一个纯净版或者内核版的系统包

**MTK**:联发科.MTK和高通是生产手机CPU的厂家。MTK平台和高通平台指的是这两家的操作系统。

**A/B分区**

Android从7.0开始引入新的OTA升级方式，A/B System Updates，这里将其叫做A/B系统。顾名思义，A/B系统就是设备上有A和B两套可以工作的系统（用户数据只有一份，为两套系统共用），简单来讲，可以理解为一套系统分区，另外一套为备份分区。其系统版本可能一样；也可能不一样，其中一个是新版本，另外一个旧版本，通过升级，将旧版本也更新为新版本。当然，设备出厂时这两套系统肯定是一样的。之所以叫套，而不是个，是因为Android系统不是由一个分区组成，其系统包括boot分区的kernel和ramdisk，system和vendor分区的应用程序和库文件，以及userdata分区的数据

A/B系统实现了无缝升级(seamless updates)，有以下特点：出厂时设备上有两套可以正常工作的系统，升级时确保设备上始终有一个可以工作的系统，减少设备变砖的可能性，方便维修和售后。

OTA升级在Android系统的后台进行，所以更新过程中，用户可以正常使用设备，数据更新完成后，仅需要用户重启一次设备进入新系统。如果OTA升级失败，设备可以回退到升级前的旧系统，并且可以尝试再次更新升级。

**VAB架构**

又称虚拟AB分区，出厂安卓11的新机型，几乎都是VAB架构。

安卓分区架构发展史为：onlyA，AB，onlyA动态分区，AB动态分区，VAB架构。 所谓的VAB架构，其实就是AB分区，套上了动态分区，再解决了AB分区的空间占用问题。

刷机时经常会刷写的分区(system,vendor,boot,recovery等等)。userdata分区就是用户分区，格式化data就是格式化的这个分区。需要注意的是，格式化data和清空data，是两个不同的概念，经常会有小白把这两个概念搞混淆。

格式化data就是把userdata的分区进行格式化操作，就像你格式化U盘一样，是格式化操作。

而清空data，是删除data分区的所有文件及文件夹。当你遇到data挂载不上时，你清空data是没有效果的，这个时候，你需要进行格式化data操作，才能挂载data，所以，这两个不要搞混淆了

**通用系统映像(GSI/SGSI)**

https://source.android.google.cn/devices/tech/ota/dynamic_partitions/implement

从Android 9开始，Google更改了要求，所有设备都必须使用[system-as-root]

GSI则由A-only和A/B进行区分刷入

GSI则是一种可以忽略厂商定制的通用刷机包

**动态分区**

Google在Android 10开始引入了动态分区（Dynamic Partitions） 简单来说，就是把原来的system , vendor , product还有odm分区整合到了一起，构成super分区 在刷入设备的时候动态调整system等分区的大小

**什么是GSI**

GSI代表通用系统映像。这是一个文件系统映像，您可以将其刷到设备的系统分区。之所以具有通用性，是因为它使用新的标准化硬件API访问硬件（因此它可以在任何启用treble的设备上运行）。

**字库(分区)**

字库是硬件，就相当于电脑的硬盘。

功能机时代，很多手机程序、控制信息、字库信息是存储在一个专用芯片里面，芯片中主要部分是字库，所以一些售后和维修人员就习惯把这个存储芯片称做字库芯片。不过，到了智能机时代，这个存储芯片的功能已经远远超越了存储字库这么简单，所以它也远不是“字库”所能概括的，更准确的表述应该为eMMC芯片(embedded MultiMediaCard）。

简单来说，“字库”(eMMC芯片)就相当于电脑中的BIOS+硬盘，一方面，它里面固化有手机的启动程序、基本输入输出程序、系统设置信息等等；另一方面，它还起到了存储照片、音乐等文件的作用，也就是我们经常提到的手机xxGB存储空间，而且手机的ROM(系统固件)也在这颗芯片当中，由此可见它对于一部手机的重要性。

与手机一样，“字库”(eMMC芯片)也有相应的分类。

1、原装专用字库，即原厂生产、针对相应型号专门使用的芯片；

2、原装代用字库，同样是由生产，在原装字库货源短缺的情况下，替代原装字库使用的芯片，由于不是专门适用某型号机器的字库芯片，所以在体积上与原装字库存在差异，一般都要稍大一些；

3、其他品牌的字库，例如某芝部分型号的芯片，可以替换原装字库使用。

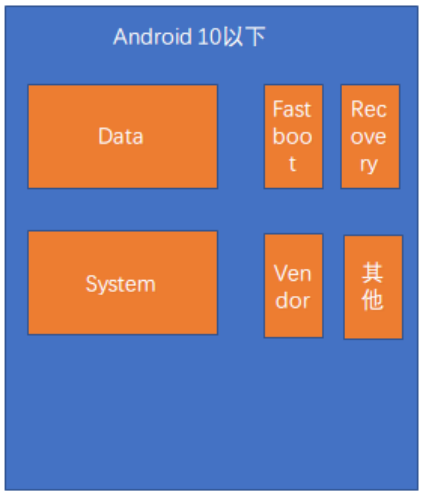
简单来说，字库要是坏了，换主板吧

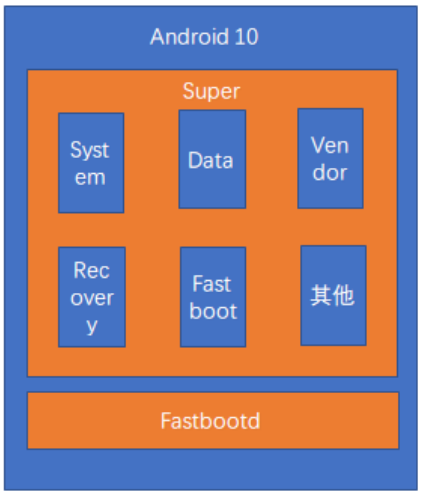
**FastbootD**

据我所知, fastbootd 是用户空间中的 fastboot。

在动态分区手机. `data`, `system`等原来的物理分区, 现在都被放到一个共同的`super`分区下. 这种"虚拟分区"只在用户空间(Android系统里)可见, 也就是说原版fastboot只能识别到整个`super`, 而`super`里的`data`这些却不行.

所以fastbootd 就是动态分区手机的 fastboot(指非动态分区手机的).




What is FastbootD? How to Boot to FastbootD Mode - DroidWin

In this guide, we will make you aware of what exactly is a FastbootD Mode and will list out various methods through which you could boot your device to the FastbootD Mode. When it comes to the various booting modes on an

https://www.droidwin.com/fastbootd-mode/


# 准备设备

本教程用到的工具我**已经打入附带的文件包** [1^]

## 提前注意

安装系统的版本需要是 5.0~12.0 之间 (2022)，同时注意，**解锁BL或救砖都会让你的文件被清空，需要备份**

**注意！**

- 解锁设备将允许修改系统重要组件，并有可能在一定程度上导致设备受损

- 解锁后设备安全性将失去保证
- 解锁后部分对系统安全性依赖高的功能和服务失效
- 解锁后部分系统功能遭到修改后，将影响系统新版本升级
- 解锁后由于刷机导致的硬件故障，售后维修网点可以按非保修处理
- 三星设备解锁后会永久性熔断 KNOX 安全认证
- 大部分手机的版权认证 DRM 等级也会从 L1 下降至 L3、无法通过 Play 商店认证等。

不建议你在主力机上解锁 Bootloader，而且，如果厂商明确表示不能解锁 Bootloader ，请放弃。如果一定要刷机并且报着变砖的觉悟，请使用 MTK方法强解。

## 准备驱动文件

准备你的手机对应的机型的驱动文件，文件包提供 Vivo 和 Oppo 的两种驱动文件[1^]。个人建议下载一个泛用型驱动 universal adb drivers。少数情况下不能识别的话，需要我们用「手机厂商名 + adb driver」的关键词搜索得到相关的下载和安装教程。

安装完驱动请重启。

手机驱动下载|手机驱动大全-FiimeROM

FiimeROM作为一家专业的小米红米原生周边全资源平台，为用户提供MIUI固件，原生ROM，移植ROM和SGSI镜像，Rec下载，驱动下载，玩机教程等的服务，联合众多开发者更新维护开发工具和官改，致力于完善小米原生生态

https://mi.fiime.cn/qudong


**对于非MTK玩家:** 重启后在设备开机状态下连接电脑，打开终端，输入`adb devices`，如果返回了设备名称，说明 adb 配置完成；用 `adb reboot bootloader` 进入 fastboot 界面，键入 `fastboot reboot` 后，若设备重启，说明 fastboot 正常。

## 准备设备

Win7 或以上电脑一台，能传输文件的数据线一条（最好是原装线），电脑下载解压 ADB 命令行，退出所有手机助手类软件，找的Recovery放电脑上，如果是 img 文件则可以直接使用，如果是压缩包则解压找出 img 或者 payload 解包。

手机确保已经解锁BL锁。另外电脑建议装一下 ADB 驱动

上述工具已经打入附带文件包。

## 准备 ADB/Fastboot

adb 和 fastboot 是我们针对 Android 设备进行高级调试和安装的工具。

如果你已经安装了 choco 或 homebrew 等包管理工具的话，Windows 输入 `choco install adb universal adb-drivers -y`，Mac 输入 `brew install android-platform-tools` 能最方便的完成 adb 和 fastboot 的配置。Windows 用户可以参照 Windows 操作系统下的 ADB 环境配置 这篇文章；macOS 用户可以尝试 此脚本 或是参考 使用 Mac 为 Android 手机刷原生系统 进行手动配置。最

后最最不济，可以尝试在 Google 开发者页面 下载对应 adb 包，解压后在对应的目录下执行指令亦可，或者是尝试 WebADB 或 adb 在线执行器 这样的在线 adb 工具，比较考验浏览器的兼容性。

## 准备深度测试或申请解锁BL（可选）

> BL 是 bootloader 的简称 就是 开机引导程序 ，Bootloader 锁，主要是在引导过程中对系统签名，内核签名及 Recovery 签名进行检验，如果签名不一致，即终止引导。

在开发者选项中打开「OEM 解锁」（除了少部分流入我国市场的国外运营商有锁机外，此选项基本都可供用户开启。）

**解bl锁会清除手机（恢复出厂设置）所有数据，记得提前备份好。**

不同的手机解锁方式不同，你甚至可以去线下店让服务人员解锁。或者从自己的社区中获取本机型的解锁信息。部分手机解锁很麻烦，比如华为，想要解锁只能去淘宝买解锁码，而且当你刷回官方 ROM 时，会自动加锁。当然，华为的解锁码是和硬件相关的，买到解锁码把它记下，下次进 FASTBOOOT 输入`fastboot oem unlock 解锁码`就可以了。

而对于小米手机，可以通过这个地址 申请解锁 下载工具，然后打开手机设置，进入关于手机–>系统版本点10下，在`设备解锁状态`中绑定账号和设备，进入`Fastboot`模式(关机后，同时按住开机键和音量下键)，打开刚才下载的工具，点击`解锁`后系统会恢复出厂系统并解锁。也可以通过OEM解锁

**如果你的设备不能进行官方解锁，在下面可以尝试 MTK强解 。**

注：一些古董机型是没有BL锁的，比如红米Note。

**附上小米解锁教程。**

小米社区

https://web.vip.miui.com/page/info/mio/mio/detail?postId=28646781&boardId=5415551&isComment=&isRecommend=0&app_version=dev.211029&ref=share

## 备份完整分区[15^]

这里的分区就是字库。

什么是备份完整字库？我们说的64GB，128GB，256GB等等，这个就是说的主板的储存容量，也就是字库。某个分区的数据损坏，好听的说法是分区数据坏了，难听的说法是字库损坏了。

所以，解锁bl后第一件事，就是备份完整字库，以防不测。有人会说，不是有9008吗？有必要备份完整字库吗？有必要。

原因：假如一个手机所有分区加起来有100个，9008大概会刷写30个左右，剩下的70个不会刷写。

那么这个70个当中有某个分区数据损坏了，9008是无法救砖的，必须返厂，用工厂售后（非卖手机的那种售后）的工厂包，方可救砖。当然，如果这个工厂包，没有刷写完100个分区的话，基本上也是无法救砖的。

备份文件下载链接 pan.baidu.com/s/1Yp3ljJWWvKMdpUpSUkt_Sw 提取码:vo15

**高通机型备份字库**

安装个MT管理器，使用root权限执行【高通字库备份.sh】即可。备份的文件在/sdcard/Rannki目录中。

**高通机型还原字库**

提前把之前备份好的Rannki文件夹，复制到 `/sdcard/Rannki`，安装个MT管理器，使用root权限执行【高通字库还原.sh】即可。

**MTK 机型备份字库**

安装个MT管理器，使用root权限执行【MTK字库备份.sh】即可。备份的文件在/sdcard/Rannki目录中。

**MTK 机型还原字库**

提前把之前备份好的Rannki文件夹，复制到 `/sdcard/Rannki`，安装个MT管理器，使用root权限执行【MTK 字库还原.sh】即可。

字库备份还原，解决的不只是基带问题，

是：除硬盘物理损坏外的所有问题，解决率为100%。

以上如何防止掉基带教程由酷安 Rannki 原创

▼ 详细叙述

**UFS闪存手机**

主板一般被分成了6个硬盘，即**sda，sdb，sdc，sdd，sde，sdf。**

所以，主板设备代码分别是：`/dev/block/sda，/dev/block/sde，/dev/block/sdc，/dev/block/sdd，/dev/block/sde，/dev/block/sdf`

备份分区的代码举例：`dd if=/dev/block/sda1 of=/sdcard/1.img,dd if=/dev/block/sda2 of=/sdcard/2.img` 等等等等.....

还原分区的代码举例：`dd if=/sdcard/1.img of=/dev/block/sda1,dd if=/sdcard/2.img of=/dev/block/sda2` 等等等等.....

**Emmc闪存手机**

主板设备代码：**/dev/block/mmcblk0**

备份分区的代码举例：`dd if=/dev/block/mmcblk0p1 of=/sdcard/1.img,dd if=/dev/block/mmcblk0p2 of=/sdcard/2.img` 等等等等.....

还原分区的代码举例：`dd if=/sdcard/1.img of=/dev/block/mmcblk0p1,dd if=/sdcard/2.img of=/dev/block/mmcblk0p2` 等等等等.....

当然，像 system 分区， vendor 分区，userdata 分区，super 分区，这些分区就没必要进行备份还原了。

查看分区信息的命令：

先安装busybox的面具模块：链接: `pan.baidu.com/s/1hFQr0nvXprzcz2gyQxtFzQ` 提取码: `y61r`

然后终端命令：`busybox fdisk /dev/block/sda` 回车，然后再输入p回车，就可以看到sda这块硬盘的所有分区信息了。adb,adc,add,ade,adf

同理,emmc闪存手机的命令是：busybox fdisk /dev/block/mmcblk0回车，再输入p回车，就能看到所有分区信息了。

> 如果你的手机已经出现问题，且没有备份完整字库……去售后换主板，或者找个同机型的，用他的完整备份字库刷入，当然我并不确定是否成功，因为会不会黑砖，这是个待验证的问题。而且最好别全部使用别人的手机的全字库备份，就算不黑砖，也会大概率出现bl永久锁定，永久无法再次解锁bl了，只能换主板）

## 刷入镜像

线必须是原装线或者质量靠谱的线，否则会出现 `USB Error` ！

如果你没有使用 MTK ，请通过`adb devices`命令确认已经连上手机。

### 准备 Magisk

Magisk 是一个强大的 Android 框架，是一个通用的第三方 systemless 接口，通过这样的方式实现一些较强大的功能。

你可以从 Github 或者 文件包 [1^] 下载它，推荐去 Github 下载，越新越好。

**安装Magisk Manager APP后如果它显示`Ramdisk`为"是"，那么你才可以进行下面的操作。**

> Tips：极少数小米设备存在检测设备信息错误的问题，Ramdisk 虽然显示为「否」，但实际上是需要修改 boot.img。

### 准备修补的img

官方 ROM 的压缩包，例如 Google、小米、Moto，由厂商发布，可从固定的发布页面、机型论坛等获取相关链接。一些厂商同时提供了 OTA 包和全量包，我们优先下载全量包，解压后即可获得 boot.img，也就是我们所需要的 boot 分区的镜像文件。请去官网或者其他平台下载**符合**你的**机型和型号**的rom包！

如果你使用的是第三方开发者制作的 ROM，也同样需要下载系统全量包解压获取，而部分开发者也会单独释出 boot.img 为玩家提供便利。如果你比较幸运，在论坛中有人分享了自己修改好的镜像，可以直接获取进行刷写。

使用ZIP解压工具解压完整的ROM卡刷包（最新MIUI系统安装包），找到`boot.img`和`vbmeta.img`两个文件，复制出来备用。

**如果没有，你可以使用 MTK 进行提取（请见MTK工具强解小节，注意解锁Bootloader后才可以提取）。**

准备好 boot.img 后，打开打开`Magisk Manager`APP，点击`Magisk`后边的`安装`，选择安装方式为`选择并修改一个文件`，从电脑端复制`boot.img`文件到手机并选中该文件，点击`开始`，仔细阅读修改结果并从结果中复制patch后的文件（一般在`Download`文件夹下，文件名类似`magisk_patched-24100_gk0te.img`）到电脑。

> ⚠️ **你所用到的镜像(提取OR修改)都要留存副本！否则变砖警告！**

# 刷入镜像可选方法

> ⚠️ 阅读者**需要自己承担因尝试 Root 导致的后果**。如果你对自己的动手能力感到怀疑，可以请人！

## 面具 Ramdisk 为「否」的机型？

Ramdisk 是系统中的一个小分区，Ramdisk 告诉系统接下来要加载哪些东西。Magisk 的目的是修改 Ramdsik，把自己加进开机需要加载的系统组件中。App 中 Ramdisk 的值为「否」时，表示需要修改的 Ramdisk 被放在了 recovery.img 中，我们需要提取并修改 recovery.img。

1. 下载当前系统的全量包，如果你使用了第三方 Recovery，那么 recovery.img 就是这个第三方的镜像。提取 recovery.img **或者** MTK 中执行 `python mtk r recovery recovery.img`，备份，然后传到手机上
2. 修改镜像：打开面具，在选择修补文件后，会多出一个「Recovery Mode」的选项。记得勾选
3. 刷入镜像：使用的命令是 `fastboot flash recovery <修改后的 recovery.img 路径>` **或者** `python mtk w recovery <修改后的 recovery.img 路径>`

这几步完成后，重启手机。和修改 boot.img 不同的是，我们需要立即按下设备进入 Recovery 的组合键，这样才能挂载 Magisk 。这是因为我们是通过修改 recovery.img 的方式挂载 Magisk 的，只有在按下组合键的情况下，设备才会启动 recovery 分区，从而实现 Magisk 的挂载。

按下组合键后，设备不会进入 Recovery 模式，而是会闪屏过后直接进入一个有 Magisk 的系统。每一次重启都要这样做才能挂载 Magisk。进入系统后就没有特别需要注意的问题了。

而想要进入真正的 Recovery ，我们需要在按下组合键后的闪屏界面长按音量 + 键。

# 简单介绍

## 底层刷机

底层刷机，顾名思义，这是一种从底层刷写手机字库的方式，与正常的程序相比，这种方式更为彻底，无视所有软件层面的权限，例如BL锁。可以将其理解为往单片机的Flash里烧写程序。

底层刷机模式常用于使用卡刷（Recovery下以及一系列使用ADB刷机方式的统称）或者线刷（Bootloader下使用Bootloader命令刷机的方式）刷成砖后救砖的场景下。按照主流处理器，高通为9008刷机模式，MTK为MTK PreLoader模式，海思麒麟为eRecovery模式（类rec操作）和eDownload模式。

> 底层刷机教程
>
> 底层刷机，顾名思义，这是一种从底层刷写手机字库的方式，与正常的程序相比，这种方式更为彻底，无视所有软件层面的权限，例如BL锁。可以将其理解为往单片机的Flash里烧写程序。 ...
>
> https://wiki.pchelper666.com/%E5%BA%95%E5%B1%82%E5%88%B7%E6%9C%BA%E6%95%99%E7%A8%8B

## OTA

**这是升级，谈不上刷机**

OTA 意思就是**增量升级**，就是在原先系统的基础上增加新功能，也许是给手机打个补丁，也许是对性能的优化。**手机要活着能进系统且未修改才能用**。OTA 不会删除资料和系统的设定。备份资料放的位置要问官方，但通常不需要知道位置，内建备份也有还原功能，还能选择要还原的东西，还原的时候有问题的部分可以选择略过。

有些档案用 patch 的方式处理了, 有些用覆盖的方式 (要看做这个 OTA 包的人怎么做), 所以, 如果有档案与预期的不同 (通常是 root 后会删除或修改档案), OTA 会失败。

你也可以解 OTA 的包进行修补获取Root权限。

## 软刷

软件刷就是刷机大师，刷机精灵等的第三方刷机软件刷，现在已经绝迹了；

## 厂刷

寄回厂子……

## 卡刷线刷

刷机可以自由选择ROM版本，所谓卡刷就是 Rcovery 模式刷机，线刷是 Fastboot 模式刷机。

区别卡刷包 和线刷包最明显的区别是 (卡刷包的文件内容）里有 **Recovery 文件，而**（线刷包的文件内容）里有 FLASH 文件，如果你注意到上方路径，从文件名可以看到线刷包文件名里有“FASTBOOT” 。

### 线刷

线刷是用 Fastboot，一般都是直接刷镜像，由 uboot 以直接写入闪存的办法把镜像直接写到闪存对应的位置（或者说分区）。

线刷时备份资料可以使用PC端的程式来管理，出问题的话三清之后再选择性恢复，再不行就全部设定和资料重头来过。线刷 要有电脑, 执行特定的程式. (通常就算手机挂到都进不去 Recovery 也能刷)

所以线刷包实际一般就是包含了 Fastboot 程序和各个系统镜像以及一个可执行的脚本的包，用户直接运行那个脚本，脚本调用 Fastboot 来刷。

## 卡刷 /第三方 REC

一般是在 recovery 里进行的，有直接刷镜像的比如 kernel 部分，但像 system 都是挂载 system 分区后再个别的更新里面的文件（差分或者直接覆盖），而不是像线刷那样把整个 system 镜像重刷一次。如果是通过打二进制补丁差分更新的话（绝大部分官方 OTA 包的做法），就要求被更新的文件和出厂时一样，否则就会失败，这是 OTA 失败的原因。优点是比较简单快捷，非常适合不会刷机的新手。

具体卡刷应该分两种, 一种是**小的更新包** (作法与 OTA 一样, 当然结果也一样), 另一种是完整的系统包, 这种通常是把系统的 partition 重新 format 再把资料放上去. (不会动到使用者资料的分区)。

卡刷可以用手机直接下载卡刷包，更名Update.zip后进入recovery刷机，刷后资料还会在，但是通常不做资料清除的话很容易发生问题，严重的就是一直出现系统错误，轻的则是偶尔出现闪退。

所以基本上刷完机最好进Recovery三清，刷前做三清也行，重点就是该清的要清一清，不然问题很多。接着要还原备份的时候如果系统本差异太大最好不要还原系统设定和App之类的资料，还原一些使用者data就好。卡刷需要存储空间，一般能进 recovery 就能刷。

卡刷包有比较复杂些的目录结构，除了用来更新的文件外，也包括一个可执行文件和脚本，但这两个脚本是给recovery来用的，而不是用户。

**什么是第三方REC？？**

> 👉 Recovery 就像电脑的PE，可以清楚数据，恢复初始化状态也可以刷写系统。可是官方的recovery只能刷官方签名的系统，而不能刷第三方系统，所以就有人做 Recovery 去代替官方 (即第三方Recovery) 的，这样就能随心所欲的刷非官方的ROM了。像是所有的官改包，第三方是配的包，国际版的包以及原生系统，都是用第三方REC刷入。

可以说，有了第三方REC，是你刷机的出发点，想刷什么都可以（当然刷的东西兼容你的设备）有了它，你就可以各种不同的系统，开始真正的刷机之路。但是，大部分的第三方REC不支持OTA升级，也就是说，每次你收到系统更新的时候，都必须要下载完整包更新。

第三方Recovery有很多种，最常用的是 `TWRP` ，还有很多基于 `TWRP` 修改的种类，比如 `橙狐Recovery` ， `SHRP` ， `PBRP` ， `奇兔Recovery` 等等。

可以去 TWRP 官网搜索，或者在 TWRP 官方APP下载，但是速度可能不是很好。

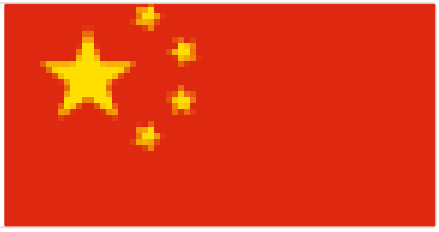
> Devices
>
> This is the Team Win website and the official home of TWRP! Here you will find the list of officially supported devices and instructions for installing TWRP on those devices.
>
> https://twrp.me/Devices/

也可以去橙狐官网找。

OrangeFox Recovery Downloads

OrangeFox Recovery is one of the most popular custom recoveries in android ecosystem, with amazing additional features that are not present in other recoveries. We support a host of devices

https://orangefox.download/zh-CN



如果以上途径都找不到，可以去酷安找你机型的话题，在话题内搜索关键词：`TWRP，rec，橙狐，oringe，pbrp，沥青，shrp。`

## 第三方 Recovery

有的Recovery作者附带了刷入脚本，这样的直接运行脚本按着走就行了，这里讲一下通用方法。

手机关机，**长按 音量减键 + 电源键** 进入 `FASTBOOT` 模式。用数据线把手机和电脑连接起来。以 `OrangeFox` 为示例。在上述步骤的下载后会得到一个压缩包，打开该压缩包，解压其中的 `recovery.img` 到任意一个位置。 压缩包是为了在有第三方 Recovery 的情况下刷入/更新 OrangeFox ，但是我们目前并没有，所以我们需要解压其中的 `recovery.img` 来使用 `fastboot` 刷入。如果你选择使用 LR.Team 定制版 TWRP，可以选择一键刷入版，就不会有下一步复杂的操作。

然后打开终端，输入 `fastboot flash recovery 上一步解压的 recovery.img 的文件地址` （或者 `.\fastboot` ？） **这一步需要配置好 ADB 环境。**

不出意外，会输出：

```
sending recovery OKAY（传输Recovery）
writing recovery OKAY（刷入Recovery）
finished.
```

**执行完毕后长按 音量加键 + 电源键**，出第一屏即一秒左右可松手，进入 `Recovery` 模式。当然你也可以使用 `fastboot reboot recovery` 来进入 `Recovery` 模式。

一般情况下，会出现一个英文界面，从上往下依次写着 `Mount` `Dectypt` ，这是让你解密 Data 。输入你的锁屏密码即可，**记得输入完后点击右下角的勾**。

解密DATA分区后，才能刷入第三方ROM，可以理解为是对官方系统的保护.

解密DATA会格式化数据，解密完成后，DATA被清空，当然也包括内置卡上也空了。**所以一定先备份好手机上的一切重要资料，包括手机存储/内置卡/外置卡上重要数据！**

经过十秒左右秒钟的解密后，不出意外会显示欢迎界面，点击屏幕下方勾即可。然后就是挂载 `System` 的界面，滑动下方滑块即可。

最后就进入了主界面。

💡 如果你是卡刷官方包后，不做任何操作是肯定会恢复官方recovery的，关于如何防止恢复官方recovery办法。进入Recovery后，不是特别老的机型，一般都需要做一下防覆盖，否则重启进系统后刷的Recovery会被官方Recovery覆盖。最常用的办法是卡刷完官方ROM包后刷个Magisk.zip就OK了。如果你并不想ROOT但是又不想恢复官方recovery，可以再卡刷完ROM后。签名boot、当然有的TWRP高级里没有签名boot功能，但是一般情况下都会有防止覆盖TWRP功能，这俩个功能实现原理不一样，但是它俩都可以防止恢复官方recovery (资料来自搞机助手，非常感谢).（如果你不想使用Magisk，可以试试 OrangeFox 的防止还原 Recovery 的功能，在 `设置` –> `OTA` 下。

> 橙狐改简体中文：点击底部的 `Menu` –> 右上角的齿轮图标 –> `Regional` –> 点击 `Language` 下的 `English` ，选择 `Chinese Simplified` 。

[^13]

💡 给手机刷入 Recovery 其实也不需要电脑，用另一部手机借助 Termux 也是同样可以的。在 Termux 配置好 ADB 环境后，照上述步骤刷入即可。安装 Termux 的那部手机无需 ROOT。

**特殊情况说明**

**新款联发科机型必须关闭AVB2.0校验**

否则任何对系统的修改都会导致卡在Fastboot。涉及的机型包括但不限于红米6，6A，9，9A，红米Note8Pro，红米10X4G，5G，红米K30U，小米Play，以及之后的联发科机型。至于AVB2.0怎么关闭，不同机型不同安卓版本方法不用，可以在TWRP里找这个功能，或者找刷过的大佬问方法。

**红米3S进入Recovery模式的方法是长按三键**

**附上 Redmi Note 7 Pro教程**

如何在 Redmi Note 7 Pro 上刷机？

拿到手机后干什么？刷机！ 如果你的设备出现损坏，我不会对你的设备负责！ 如果你的设备出现损坏，我不会对你的设备负责！ 如果你的设备出现损坏，我不会对你的设备负责！ 刷机前请先看看最下面的乱七八糟的问题（ 由

https://blog.linioi.com/posts/11/

**相关Recovery下载**

小米Recovery下载|Recovery大全-FiimeROM

FiimeROM作为一家专业的小米红米原生周边全资源平台，为用户提供MIUI固件，原生ROM，移植ROM和SGSI镜像，Rec下载，驱动下载，玩机教程等的服务，联合众多开发者更新维护开发工具和官改，致力于完善小米原生生态体验。

https://mi.fiime.cn/Recovery

Devices

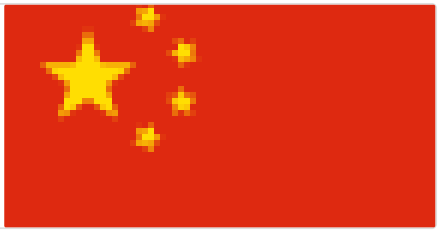
This is the Team Win website and the official home of TWRP! Here you will find the list of officially supported devices and instructions for installing TWRP on those devices.

https://twrp.me/Devices/

OrangeFox Recovery Downloads

OrangeFox Recovery is one of the most popular custom recoveries in android ecosystem, with amazing additional features that are not present in other recoveries. We support a host of devices

https://orangefox.download/zh-CN



## 高通9008刷机

**理论上高通处理器都可以用这个方法**

**用这个方法必须要满足两个最基本条件**

1.能找到 QPST 专用刷机包

2.确认手机能进9008端口

💡 高通 QPST 线刷其实就是利用高通芯片自带的9008端口，将手机系统内的所有分区的镜像文件，直接刷写手机。这个刷机方式比 REC卡刷 和 fastboot 线刷，更底层、高效、强大。这种方式，不需要进入手机的任何分区，就可以直接刷写手机固件。

> 高通的 QPST线刷模式，因联机之后端口名字叫Qualcomm HS-USB QDLoader 9008 (COMx)而得名。该模式下，用户可通过QPST及其衍生工具（本质为QPST命令行调用）直接对手机的Flash芯片进行读写操作，而不需要解锁Bootloader。常见刷机工具有QPST，MiFlash（Pro）等工具，刷机包中一般会有一个分区表xml文件。以及一个eif文件。XML文件命名一般为Rawprogram（数字）.XML和Patch（数字）.XML,EIF文件一般命名为prog_存储芯片类型（比如UFS和EMMC）*firehose*(SOC型号，比如MSM8998或者SDM855)_（内存类型，一般是DDR）.eif，只要带有这两个文件的，一般都是高通支持9008的刷机包。 进入9008模式，高通略为麻烦。MSM8994及以前的SoC，可以通过Fastboot命令直接进入9008模式：
>
> `adb reboot edl`

---

此方案无需改线，无需触点短接等操作，需要电脑进行操作

我们将手机的变砖分为四个程度

1. 能亮屏，按键有反应 开机卡住 连接USB电脑有反应
2. 黑屏 ，按键有反应 连接电脑有反应
3. 屏幕不亮 按键无反应 连接电脑有反应
4. 砖头什么样 手机什么样---黑砖

**首先去下载高通的线刷工具，一般下载最新版本的即可。**

`https://qpsttool.com/category/download`

运行该线刷工具，需要电脑识别到端口9008，在电脑设备管理器中可以找到，如果没有反应需要电脑安装9008的驱动。

`https://www.aliyundrive.com/s/KTLkyyjTsDB`

接着需要下载官方固刷包进行刷入就可以了

### 刷包成功后出现的几种情况

1.数据线自动断开链接，手机充电灯亮起-----刷写成功

2.无反应！------换包刷写，或试另一种刷写方式

> 💡 按住手机上下音量+电源调试手机进入9008模式，其次电脑识别到9008端口

## 联发科深刷：MTK 刷入/强解

联发科的底层刷机模式没有高通那么麻烦。该模式在 MTK 内部被称为 MTK in-house developed loader。MTK 的该模式与高通略有不同，该模式具有帮助系统寻找Uboot的功能。该模式除了具有启动功能之外，还具有下载功能。首先还是需要明确的是mtk芯片都有一个boot rom，如果没有这个rom，那么程序是无法被下载到 Nand Flash中的，然后此时的Flash上是为空的，没有任何数据的。系统在上电之后它会检测是启动模式还是下载模式，如果是下载模式，它会初始化一个usb的串口，将Preloader加载到内部的SRAM中，跳转到Preloader中去执行，初始化好Flash和外部RAM之后，依次将preloader、lk、kernel、android下载到nand flash中去。刷机工具是SP Flash Tools ，需要验证的对应的DA文件，或者 MTKclinet

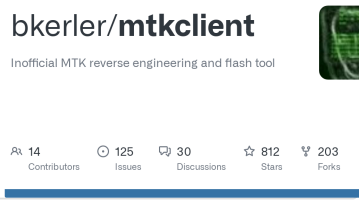
### 准备 MTK 工具/工具箱

> 💡 **解释**：MTk 工具依赖安卓的一种漏洞来实现 Root ，提取 boot.img，在使用前请关注你的社区（酷安等）。工具箱的使用都有说明，请自行咨询或查阅资料。

GitHub - bkerler/mtkclient: Inofficial MTK reverse engineering and flash tool

Just some mtk tool for exploitation, reading/writing flash and doing crazy stuff. For windows, you need to install the stock mtk port and the usbdk driver (see instructions below). For linux, a patched kernel is only needed when using old kamakiri (see

https://github.com/bkerler/mtkclient




MTK 提供不同平台的版本，但是因为依赖 Python，所以你需要从文件包或从 Download Python | Python.org 安装Python（**确保安装时勾选 ADD PYTHON to PATH**），并使用 `pip config set global.index-url https://pypi.tuna.tsinghua.edu.cn/simple` 配置国内镜像源。

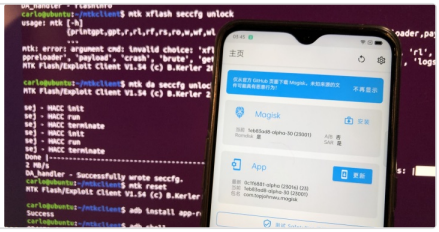
**天玑920 以后的设备不受此方法支持！（天玑1200仍旧支持）**

这里以Windows系统为演示系统。乌班图看这里

真我\OPPO 解锁BL、ROOT教程

虚拟机环境安装Ubuntu 20.04 下载链接： https:// releases.ubuntu.com/20.

https://zhuanlan.zhihu.com/p/452973221



## 初始化

在 mtkclient-main 文件夹下右键打开命令行
执行 `python setup.py install`

🛠️ 下面每执行一次命令，都需要重复关机状态下 “插上USB同时按住音量加减及开机键，待到看到命令行变成这个后就松手”步骤。 **一定不要输错命令！！！！！！！**

## 备份 Root 前手机全部分区

`python mtk rl out`
自救命令，使用mtkclient写入备份的镜像
`python mtk wl out`

**这个步骤如果备份用户数据会耗费8小时，你可以备份到userdata时中断并删除 usedata.img。**

**然后将项目目录下的out文件夹复制出来，防止后续覆盖**

## 强解 Bootloader

如果你OEM已经解锁且BI也已经解锁的，请跳过这步。

如果你没有获取到深度测试或者官方解锁的，可以用 `python mtk da seccfg unlock` 尝试解锁，风险自担，**这一步会清除你手机的全部数据，请注意**

强解后请重置手机，输入 `python mtk reset` （**如果是MTK 可以不清除设备所有数据**）重置。完毕后长按开机键开机，开机第一屏会有提示，按一下开机键即可解决，因为重置过手机，所以第一次开机时间会有点长，耐心等待即可。待到开机后，设置中打开开发者选项就可以看到OEM解锁

选项变灰，出现一行小字引导加载程序已解锁。开机前会有一段英文提示，即为解锁成功（可以用 `fastboot oem lks` 验证，返回 0 代表解锁成功）

附：重新锁回使用 `python mtk da seccfg lock` ，谨慎使用。

### 提取boot与vbmeta

```
python mtk r boot,vbmeta boot.img,vbmeta.img
```

手机关机，待到关机完成，插上USB同时按住音量加减及开机键待到看到命令行提取的数字闪动后，请松手。

提取完毕后，boot与vbmeta 的镜像文件会在目录中，然后**请备份它们到一个其他的文件夹**

**按照上文【准备修补的img】小节准备修补后的镜像，注意一定要使用最新版本的面具，会解决很多问题。**

### Root 手机

使用如下命令，提取手机中的 boot 和 vbmeta.img 镜像

```
python mtk r boot,vbmeta boot.img,vbmeta.img
```

有的手机没有 vbmeta 分区，会有提示，没关系。
**准备修补后的镜像**，重命名为 `boot.patched` ，放入项目根目录

> 🛠️ 个别如遇无法开机等问题，可尝试保持boot镜像中的vbmeta,此选项在最新版面具中已支持。

执行命令刷入，重启手机，安装面具即可发现root成功

```
python mtk w boot,vbmeta boot.patched,vbmeta.img.empty
```

### 备份 Root 后的手机

使用如下命令备份手机全部镜像，以便可以在手机变砖时进行自救。

```
python mtk rl out
```

自救命令，使用mtkclient写入备份的镜像

```
python mtk wl out
```

**这个步骤如果备份用户数据会耗费8小时，你可以备份到userdata时中断并删除 usedata.img。**

**然后将项目目录下的out文件夹复制出来，防止后续覆盖，还有就是一定不要输错命令！！！！！！！**

> 🛠️ 如果在解锁中遇到问题请先去 https://github.com/bkerler/mtkclient/issues ，搜索遇到的问题，如果是新的bug欢迎向作者反馈。需注明机型和提供相应的preloader。还有就是花钱请人救砖。

## Fastboot刷入镜像/卡刷

卡刷是最值得推荐的，过程也不复杂，只要刷机过程保持电量充足，刷机包正确，刷机过程不对手机进行操作，一般都是能成功刷入的。

1. 无需第三方 **Recovery**
2. 不影响系统升级（完整包升级）

复制修改镜像后的完整路径（**在 Windows 中，选中文件 > Shift + 右键，会多出「复制为路径」命令**），在终端中输入：

```
## 手机重启到 Bootloader
adb reboot bootloader
## 如果 Ramdisk 为 yes
fastboot flash boot <修改后的 boot.img 路径>
 ## 刷入完成后重启
fastboot reboot
```

如果想要谨慎一点，比如说修改的镜像文件是从网上下载的，想先试试看能否正常启动，则可以用命令：`fastboot boot`。这样顺利启动系统后即可暂时拥有 Magisk ，不过重启后就会失效。

文件包中有Han.GJZS-v2.12.1附带了很多工具，可以使用ADB和FastBoot（不懂不要用）

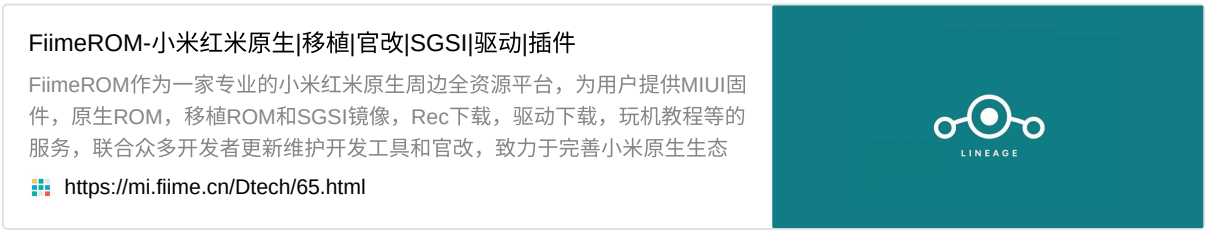
## 升级系统时 Magisk 的保留

目前各大品牌的旗舰手机均采用A/B架构（即同时有两套系统共存、其中一个作为备份、共用一份用户数据）。这就为我们升级系统提供了极大的便利。当我们安装更新后，在重启手机以前，新的系统将作为备份系统存在，这时我们可以利用现有系统仍保留的root权限修改备份系统的分区，刷入 Magisk 。

安装了 Magisk 后记得关掉系统的自动更新。有更新的时候，写点卸载 Magisk > 还原原厂镜像，不重启。就能正常进行 OTA。A/B 分区的设备可以保留 Magisk 更新
https://sspai.com/post/53075

不支持的话，只能按文章的方法 OTA 之后重新刷一次 Magisk。

附：**AB分区保留面具升级系统**




### 具体步骤

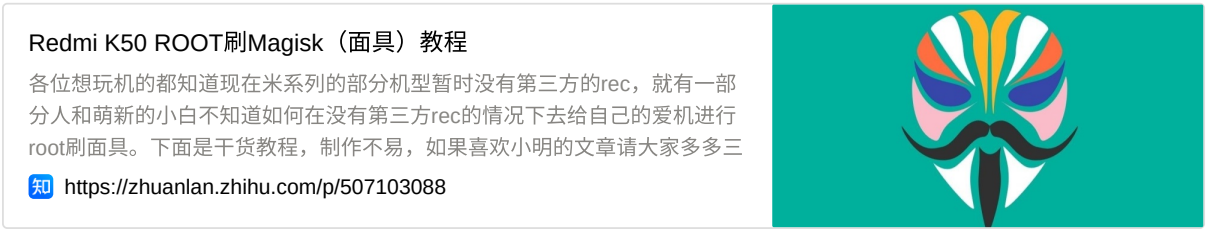
关闭系统自动更新。设置-系统-开发者选项。

下载更新并安装更新。此时会提示检测到root需要下载全量包，为正常现象。

待其安装好后，千万！千万！千万！不要重启，否则你Magisk就没了，又得重装一遍。

这时候打开Magisk Manager。卸载-还原原厂镜像。安装-安装-安装到未使用的槽位（OTA后）。

接着按提示重启即可。重启完成后系统应该是新系统，Magisk应该还在。




## Magisk 面具

> Magisk 工作机制是「拦截」，Magisk通过挂载一个与系统文件相隔离的文件系统来加载自定义内容，为系统分区打开了一个通往平行世界的入口，所有改动在那个世界（Magisk 分区）里发生，在必要的时候却又可以被认为是（从系统分区的角度而言）没有发生过。Magisk 可以被看作是一种文件系统，这种文件系统通过巧妙的实现方式避开了对系统文件的直接修改

确认 Root 没有问题后，再打开 Magisk App 中选择**安装 > 直接安装**，来「永久」写入 Magisk。

系统更新时想要保留 Magisk 的，重新打包刷入一次是最为通用稳妥的办法。

**刷入Magisk后进行OTA系统更新**

见上文

### 系统分区解锁

现在几乎所有手机都不能动 system.

需要安装模块才能修改 system.

### 隐藏 root

本节内容部分都是 @MiaoHan 的 酷安专栏内容。

Riru 已经停止维护，所以本节只讲 Zygisk

**ROOT目前主流的检测方法**

1、检查常用目录是否存在su

2、使用which命令查看是否存在su

3、主动申请root权限

4、执行busybox

5、访问私有目录，如/data目录，查看读写权限

6、读取build.prop中关键属性，如ro.build.tags和ro.build.type

7、检查市面主流的模拟器

8、检测frida、xposed等Hook框架的特征

### 开启 Zygisk 的面具

如果你现在用的阿尔法(Alpha)版面具，开了 MagiskHide 功能，要先关闭 MagiskHide 功能，然后开启Zygisk才能用本期教程的方案。

**不管哪一个版本，只开启Zygisk，不要开启遵守排除列表！**

开启Zygisk后要重启手机，Zygisk才能生效。

**如果**你每次打开面具，它都会提示“检测到不属于Magisk的su文件”，**如果没提示这个，你不要试图安装“隐藏系统root”模块。**

对于这种情况，你一定要安装一个名为“隐藏系统root”的面具模块，文件包里有，或者删除system\xbin目录下一个名为“su”的文件。我建议你安装模块，不建议你删除su文件。因为个别系统System只读，删不掉此文件。个别系统删掉开机也会自动恢复。

> 刷了这个“隐藏系统root”模块，会导致Momo提示找到Magisk，但是影响不大，更不会影响隐藏root。我个人建议，如果不是强迫症，建议不要在意这个了。如果你是MIUI开发版系统，比较在意Momo的提示，想让Momo不提示找到Magisk，那么你需要重刷一遍当前开发版系统(重刷系统这一步是为了关闭系统自带的root)。重刷完不要打开系统自带的root，不能用面具接管系统root的方式刷面具，你应该用第三方recovery或者修补boot的方式刷入面具。

### 停用隐藏应用列表

隐藏应用列表完全没有隐藏root的作用。

银行类金融类游戏类应用，检测设备环境的优先级永远是先检测root，然后再检测应用列表或者不检测应用列表。大部分应用都不检测应用列表。

### 以Shamiko为核心的隐藏root方案

面具启用随机包名+开启Zygisk+遵守排除列表(不能开)+安装“SHamiko”模块+配置排除列表(排除列表)+安装“隐藏系统root”模块(**特定用户安装，没有提示不要**)→若无效→停用或移除部分面具模块

### 面具随机包名

面具设置里，找到“隐藏Magisk应用”选项点开，会跳出一个对话框。这个对话框里已经有默认名称“Settings”，你可以把它删掉并输入你喜欢的名字。比如我输入MiaoHan，点确定就不用管它了，它最后会自动跳转到新生成的面具界面里。期间无论跳转什么界面，你只需要点确定或者允许就行了。面具随机包名成功后，会看到原来的面具消失，桌面出现新生成的面具“MiaoHan”。如果随机包名失败或者“隐藏Magisk应用”一直转圈圈，那么你需要使用代理隧道。

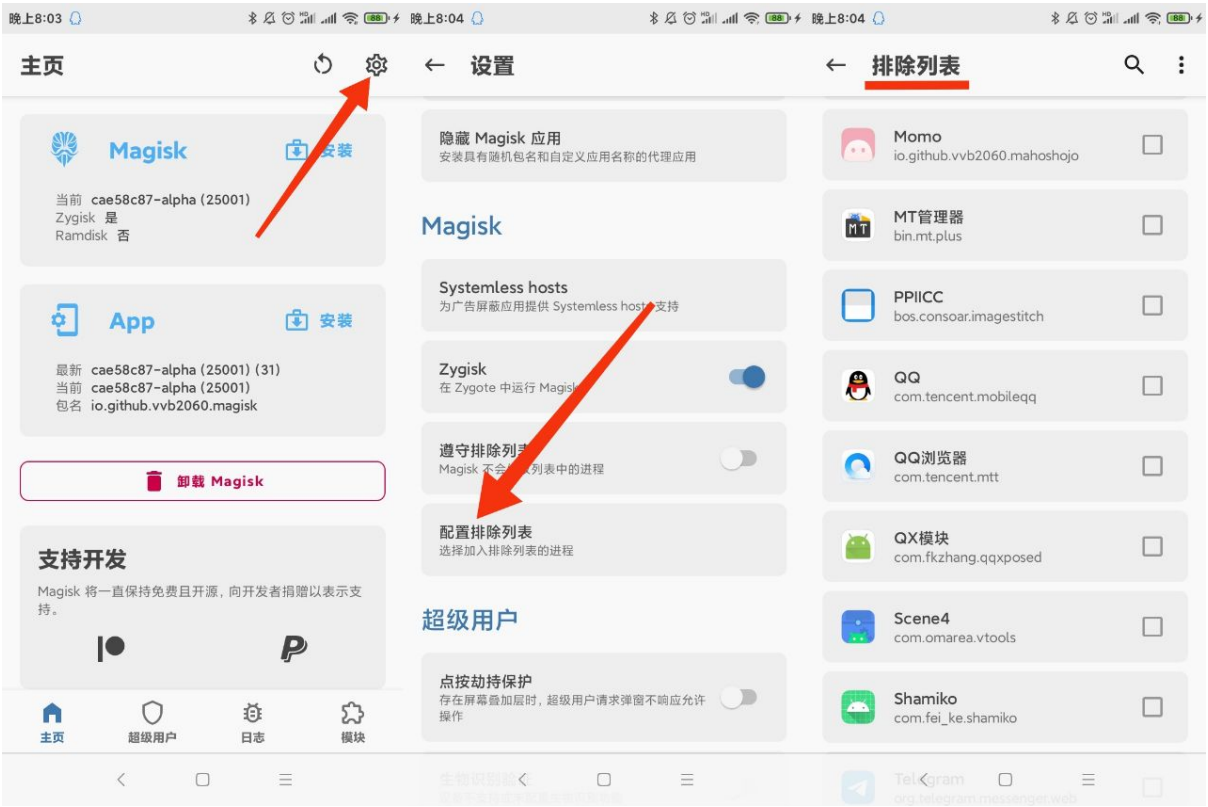
> 如果面具随机包名后，出现 “ 还原Magisk 应用”的提示，重启一下手机就好了。**不用点安装，只需重启一遍手机。**

### SHamiko

一个面具模块，可以在面具开启Zygisk的情况下，实现类似于MagiskHide的隐藏root效果，可以对应用隐藏Magisk、Zygisk本身和二进制文件“su”。你可以把它简单理解为，就是隐藏root的模块。

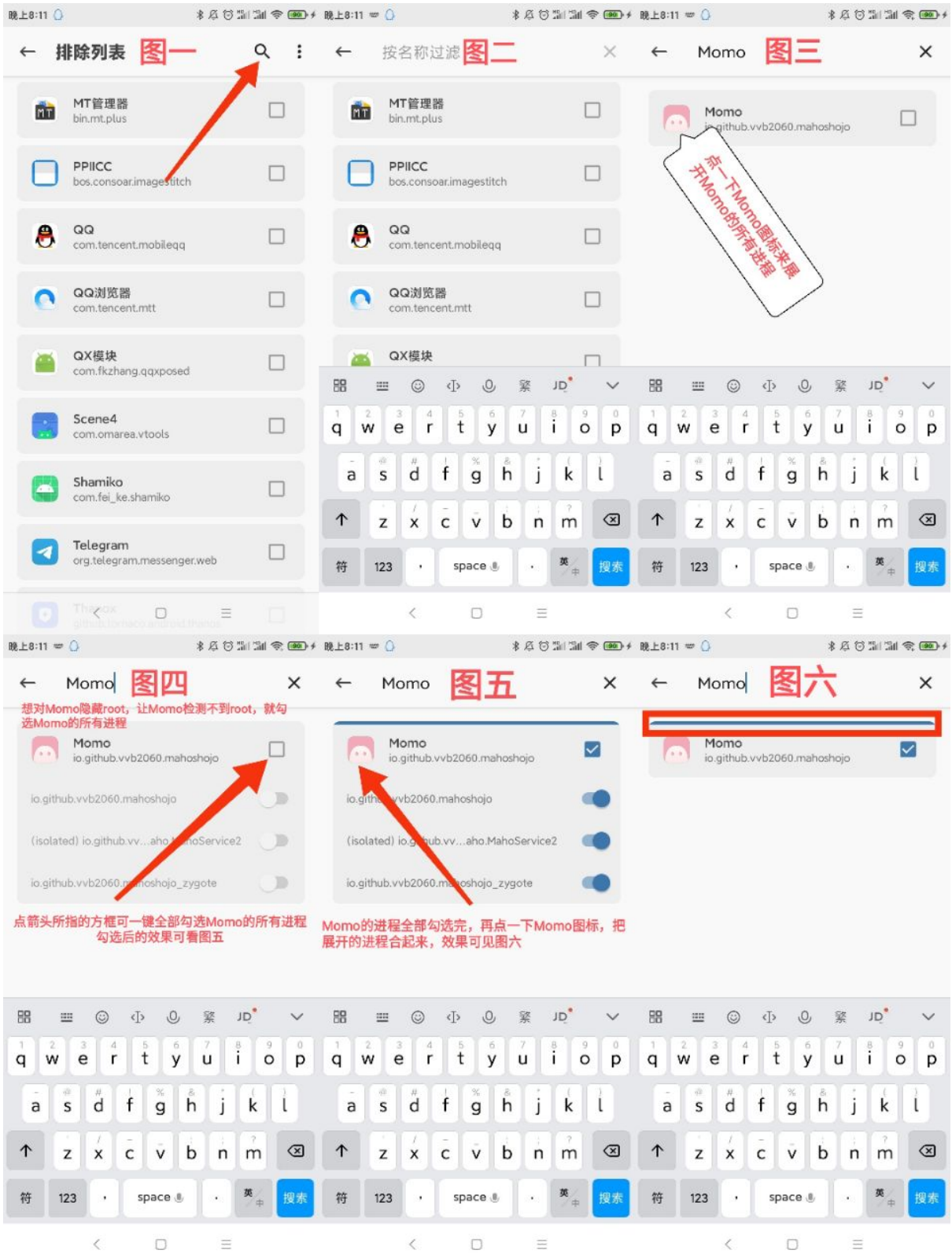
### 安装 Momo APP检查情况

打开面具，右上角点击齿轮进入面具设置界面。在面具设置界面下滑找到配置排除列表选项，点配置排除列表选项进入排除列表界面。在“Shamiko”模块的加持下，理论上你在排除列表勾选哪个应用，哪个应用就检测不到root。




建议在面具排除列表勾选应用(即对应用隐藏root)后，最好检查一下应用是否在后台运行。如果是在后台运行，你最好结束一下，再打开应用。如果不是在后台运行，你就可以直接打开应用。**注意彻底结束进程**

当面具排除列表勾选Momo后，打开Momo可以看到Momo已经不再提示找到可执行程序“su”、Magisk、Zygisk，说明“Shamiko”模块配合面具排除列表隐藏root是有效的。接下来我们如法炮制，在排除列表勾选那些检测到root后无法运行或者闪退的应用，比如银行类、金融类、游戏类应用。这样它们就检测不到root，也就可以正常运行了。下一部分(第七部分)我会再演示一遍对ZFB隐藏root，即排除列表勾选ZFB的步骤。




> 到了这一步可能有的朋友会有疑问，怎么我排除列表勾选了Momo的所有进程，Momo还是提示找到Magisk？找到二进制文件“su”？找到Zygisk？出现这种情况，一般是因为你安装的面具模块导致的。如果你不解决Momo的这

> 些提示，大概率银行类金融类游戏类应用你还是打不开，所以你应该跳过第八部分看我第十部分的内容——停用面具模块。

### 用排除列表对 ZFB 隐藏root

玩机的朋友可能会知道，当root后ZFB可能会无法刷脸，归根结底还是因为ZFB检测到了root。我们需要对ZFB隐藏root，相关步骤如下：

进入面具排除列表，然后右上角搜索找到ZFB，点击ZFB图标把它展开如图四，这里面显示的一条条都是ZFB的进程。当我们勾选ZFB的所有进程，ZFB就检测不到root了，也就是对ZFB隐藏root了。不用一个个点，展开后点ZFB右边的方框即可全部勾选这些进程。把这些进程全部勾选后，如图六，可以看到ZFB上面的进度条全满。这个进度条表示里面的进程有没有全部勾选，如果没有全部勾选，进度条就不会全满。就像图七图八进度条不全满，里面的进程就没有全部勾选，这样是不行的。必须全部勾选里面的进程，才能完全隐藏root。

非必需操作：排除列表勾选完ZFB后，退出面具。然后长按桌面的ZFB图标，ZFB图标上会出现“应用信息”四个字，点“应用信息”进入“应用信息”界面。如果你是显示图一那样，你就直接去打开ZFB，也不用点“结束运行”。如果你是显示图二那样，就点一下“结束运行”，然后再去打开ZFB。

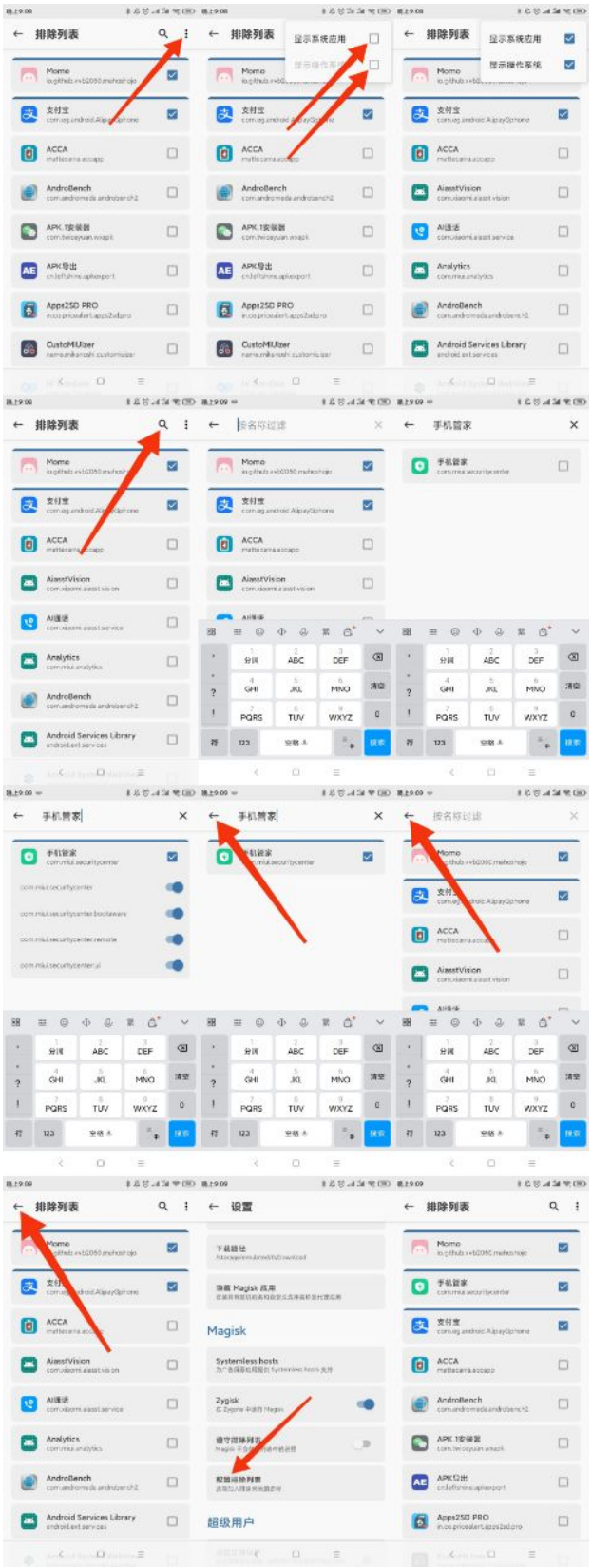
好了，不出意外的话，当排除列表勾选ZFB后，打开ZFB就会发现刷脸功能又可以使用了。

### 排除列表对手机管家隐藏root(MIUI系统专属)

如果你是MIUI系统的用户，对ZFB或者薇信以及其他金融类应用隐藏root后，用它们ZF时可能会弹出以下提醒。

当看到以上提醒，一些朋友可能会觉得，你这方案不行啊。SHamiko模块生效了，也在排除列表勾选了ZFB所有进程，居然还会提示手机已被root。其实这真不是ZFB检测到了root，而是MIUI系统的系统应用“手机管家”检测到了root，发出的弹窗提醒。至于为什么会弹窗这个，因为你排除列表没勾选手机管家啊！

进入面具排除列表，然后右上角搜索手机管家，大概率都会搜索不到，主要是方法不对，以下教大家查找手机管家的正确方法。




## 停用面具模块

适用场景：

也安装了“Shamiko”模块，并且“Shamiko”模块也生效了(显示笑脸)，排除列表也勾选了Momo的所

有进程，打开Momo还是提示找到Magisk，或者找到二进制文件“su”，或者找到Zygisk。进而打开银行类金融类游戏类应用提示root无法运行，或者功能不正常。

原因分析：这种情况不是因为“Shamiko”模块失效了，而是你们装了太多系统优化类面具模块。部分系统优化类面具模块，让你们手机不再纯净，破坏了系统的完整性，让设备处于被修改的状态。进而导致“Shamiko”模块隐藏失效，Momo从而找到以下三个提示。而我从来不用系统优化类面具模块，只用寥寥可数的几个模块(还不是系统优化类)，所以可以很容易的过掉Momo以下三个提示。

### Momo找到Magisk或者找到二进制文件“su”或者找到Zygisk的解决方法

**Momo提示找到Magisk解决方法**

> 安装了“Shamiko”模块，并且“Shamiko”模块也生效了(显示笑脸)，排除列表也勾选了Momo的所有进程，打开Momo还是提示找到Magisk。

#### 解决方法

(1)去面具模块界面，检查有没有安装“隐藏系统root”模块。如果是安装了“隐藏系统root”模块，那就不要解决Momo提示找到Magisk了。因为就是这个模块，导致Momo提示找到Magisk。但是你又不能停用这个模块，停用它你就更加隐藏不了root。

关于“隐藏系统root”这个模块的作用，我发现许多人对这个模块的作用存在很大误解。

如果你每次打开面具时，它都会提示“检测到不属于Magisk的su文件”，那么你需要安装这个“隐藏系统root”模块，如果你打开面具没提示这个，就不能安装也不要安装。

(2)去面具模块界面，检查有没有安装“隐藏系统root”模块。如果没安装这个模块，那说明是其他模块导致Momo提示找到Magisk。

怎么排查是哪个面具模块引起Momo找到Magisk呢？我建议停用除“SHamiko”以外的所有模块，即“SHamiko”模块你不要停用，其余模块全部停用。PS:停用的面具模块，主要包括字体模块、桌面模块、调节音质、优化触控、停用温控、开启高刷、调整扬声器马达、开启快充等等这一类优化模块。

停用后重启手机打开Momo再看看，如果停用面具模块解决了Momo找到Magisk的问题，那么我建议大家重新启用面具模块时，一个一个或者两个两个来启用。每启用一个或者两个，就重启下手机打开Momo再看看。直到Momo再次提示找到Magisk，就可以知道是哪个模块引起的了。知道是哪个模块引起的，就把哪个模块移除不用就行了。

**Momo提示找到二进制文件“su”解决方法**

> 安装了“Shamiko”模块，并且“Shamiko”模块也生效了(显示笑脸)，排除列表也勾选了Momo的所有进程，特定用户也安装了“隐藏系统root”模块，打开Momo还是提示找到二进制文件“su”。

#### 解决方法

我建议停用除“SHamiko”以外的所有模块，即“SHamiko”模块你不要停用，剩余模块全部停用。如果你是安装了“隐藏系统root”模块的特定用户，那么你就停用除“隐藏系统root、SHamiko”以外的所有模块。即这两个SHamiko模块和隐藏系统root模块你不要停用，剩余模块全部停用。

停用后重启手机打开Momo再看看，如果停用面具模块解决了Momo找到二进制文件“su”的问题，那么我建议大家重新启用面具模块时，一个一个或者两个两个来启用。每启用一个或者两个，就重启下手机打开Momo再看看。直到Momo再次提示找到二进制文件“su”，就可以知道是哪个模块引起的了。知道是哪个模块引起的，就把哪个模块移除不用就行了。

**Momo提示找到Zygisk的解决方法**

> 安装了“Shamiko”模块，并且“Shamiko”模块也生效了(显示笑脸)，排除列表也勾选了Momo的所有进程，打开Momo还是提示找到Zygisk。

#### 解决方法

如果你隐藏应用列表的生效应用里选择了Momo，那么你应该取消对Momo的隐藏。Momo不会检测应用列表，你对Momo隐藏应用列表反而会导致Momo检测到Zygisk。

如果隐藏应用列表生效应用里没选择Momo，Momo还是提示发现Zygisk。那么一般可能是因为面具版本太低或者Shamiko版本太低，总之发现Zygisk这个不太好解决。有时候你升级Momo版本，(升级后的Momo)就有可能发现Zygisk；或者你升级面具版本，也有可能导致Momo发现Zygisk。

> 0.5.2版本的Shamiko模块是配合25.1以上版本的面具，才能对Momo隐藏Zygisk。想让Momo检测不到Zygisk，你可以升级面具版本到最新25.2。

启用“Shamiko”白名单模式后，你手机里安装的所有应用(也包括系统应用)都检测不到root了。你不用再像第(一)期教程中的那样，想对哪个应用隐藏root，还必须得在面具排除列表勾选哪个应用才行。启用白名单模式后，你可以跟排除列表繁琐的勾选步骤说再见了，不用再去配置排除列表了。

## “Shamiko”白名单模式

#### 需要注意的事项

既然SHamiko白名单模式比黑名单模式有优势，那是不是可以不加分辨的启用白名单模式呢？还真不是这样的，在决定使用白名单模式前，我建议你知道一些注意事项：

⑴白名单模式存在一些较为严重的Bug

部分机型启用“Shamiko”白名单模式后，打开一些应用会闪退，并且部分应用自带的浏览器打不开网页。还有就是，开启白名单模式会造成手机性能的损耗，不过这点感知不强。

⑵新安装应用无法获取root权限

有些酷友不明白这句话的意思，我给大家详细解释一下：首先打开面具，进入超级用户界面，可以看到你授权过root的应用。当你启用“Shamiko”白名单模式后，也只有超级用户界面的应用能获取root了。你新安装的(需要root的)应用，以及你之前你没打开过(需要root)的应用，都获取不了root。我举个例子：比如你启用“Shamiko”白名单模式后，安装搞机助手(搞机助手需要root才能运行)，那么搞机助手就会获取不了root，进而无法运行。

#### “Shamiko”白名单模式的隐藏root方案

> 面具启用随机包名+开启Zygisk+遵守排除列表(不能开)+安装“SHamiko”模块+启用“Shamiko”白名单模式+安装“隐藏系统root”模块(特定用户安装)→若无效→停用或移除部分面具模块

“ Shamiko”白名单模式跟黑名单模式一样，也需要关闭遵守排除列表，“Shamiko”模块才能生效。

关于特定用户的安装“隐藏系统root”模块还是得再讲一下。如果你每次打开面具，它都会提示“检测到不属于Magisk的su文件”，那么你一定要安装一个名叫“隐藏系统root”的面具模块。如果没提示这个，你不能安装，也没必要安装。

PS：这个“隐藏系统root”模块文件包里就有，下载后在面具里刷入即可。刷完记得重启手机

**启用“SHamiko”白名单模式的方法**

既然要启用“Shamiko”白名单模式，首先要学会判断当前“Shamiko”模块是处于哪种模式？如何判断呢？我们要看“Shamiko”的模块描述。首先我们打开面具进入模块界面，可以看到“Shamiko”笑脸正在工作。如果“Shamiko”的模块描述里显示的是“blacklist mode”，说明“Shamiko”处于黑名单模式，正在以黑名单模式运行；如果“Shamiko”的模块描述里显示的是“whitelist mode”，说明“Shamiko”处于白名单模式，正在以白名单模式运行。

正常情况下，你的“Shamiko”模块描述里都应该显示“blacklist mode”，因为这是“Shamiko”模块的默认工作方式。

**如何切换为“Shamiko”白名单模式呢？**

有以下两种方法：

⑴安装一个名叫“Shamiko”的软件

这是个APP应用，我置顶评论的链接里就有下载。这是咱们酷安某位大佬开发的软件，我不知道是哪个大佬开发的，如果有知道的兄弟麻烦告诉我下。这个软件可以一键开启和关闭“Shamiko”黑名单模式，非常的方便，使用方法也很简单。

首先确保“Shamiko”模块处于黑名单模式，然后下载和安装这个“Shamiko”软件。安装后打开，会有超级用户弹窗提示“Shamiko”软件要申请root权限，你点允许。给完“Shamiko”软件root权限后，打开中间那个“whitelist mode”选项，“Shamiko”模块就切换为白名单模式了。这时你进面具里，就会发现“Shamiko”模块已经处于“whitelist mode(白名单模式)”了，甚至不用重启手机，立即生效。切换回“blacklist mode(黑名单模式)”也很简单，关闭“whitelist mode”选项就行了。切换回也是不用重启手机，立即生效。

PS：无论“Shamiko”模块是从黑名单模式切换为白名单模式，还是从白名单模式切换回黑名单模式。用这个“Shamiko”软件切换后无论关机还是重启，都会一直有效哦。还有这个“Shamiko”软件也不用保持后台运行，用完你可以在最近任务卡片里划掉它。

⑵用MT管理器新建“whitelist”空文件

首先确保“Shamiko”模块处于黑名单模式，打开MT管理器，点左上角三条横杠，进根目录。此时MT管理器若申请root权限你要点允许，否则无法访问根目录下的文件夹。给MT管理器root权限后，按/data/adb/shamiko的路径点进去， 在shamiko文件夹里建一个名为whitelist文件。文件名不好记，大家复制粘贴就好了。当文件建完也不用重启，“Shamiko”就启用了“whitelist mode(白名

单模式)”。切换回“blacklist mode(黑名单模式)”也很简单，用MT管理器删除whitelist文件就行了。切换回也是不用重启手机，立即生效。

PS：大家还记得我这篇教程第二部分讲的内容吗？当你开启“Shamiko”白名单模式后，你新安装的(需要root的)应用，以及你之前你没打开过(需要root)的应用，都获取不了root。当你现在“Shamiko”处于白名单模式，遇到新安装的应用申请不了root时，你可以先关闭白名单模式。关闭后白名单模式后，在黑名单模式下打开所需要root的应用，让它申请一遍root。然后再用“Shamiko”软件或者MT管理器打开“Shamiko”白名单模式。

#### 测试“Shamiko”白名单模式隐藏root效果

当我们启用“Shamiko”模块白名单模式后，如何判断它有没有隐藏root的效果呢？还是需要用上我们强大的“Momo”APP了。PS：Momo是一个检测设备是否root的应用！如果打开Momo，Momo提示找到可执行程序“su”、Magisk、Zygisk说明检测到了root；如果打开Momo，Momo没有提示找到可执行程序“su”、Magisk、Zygisk说明隐藏root有效或者未root。

如果你是从“Shamiko”黑名单模式切换为白名单模式的，我建议先去排除列表取消对Momo的勾选，再打开Momo看看检测结果。因为这样做，有助于判断“Shamiko”白名单模式是否有效隐藏root。当你排除列表取消对Momo的勾选，再次打开Momo，Momo依旧没有提示找到可执行程序“su”、Magisk、Zygisk说明白名单模式隐藏root是有效的。

当确定“Shamiko”白名单模式隐藏root有效后，我们可以打开任何因为root打不开的银行类、金融类、游戏类应用。记住，你现在是白名单模式了，不需要用排除列表勾选了。若你切换回黑名单模式，一定要在排除列表勾选要隐藏root的应用。

#### 如果隐藏无效就停用面具模块

适用场景：
也安装了“Shamiko”模块，并且“Shamiko”模块也生效了(显示笑脸)，模块描述里也显示的是“whitelist mode(白名单模式)”，打开Momo还是提示找到Magisk，或者找到二进制文件“su”，或者找到Zygisk。进而打开银行类金融类游戏类应用提示root无法运行，或者功能不正常。

原因分析：这种情况不是因为“Shamiko”模块白名单模式失效了，而是你们装了太多系统优化类面具模块。部分系统优化类面具模块，让你们手机不再纯净，破坏了系统的完整性，让设备处于被修改的状态。进而导致“Shamiko”模块隐藏失效，Momo从而找到以下三个提示。而我从来不用系统优化类面具模块，只用寥寥可数的几个模块(还不是系统优化类)，所以可以很容易的过掉Momo以下三个提示。

# 小米刷原生

刷机有风险 如果不会刷还请不要刷

## 刷底包

首先要解锁手机BL锁 。

解锁完下载MIUI系统底包 必须要和类原生安卓版本一样 安卓9=安卓9 安卓10=安卓10请前往官网或者mi.fiime.cn下载相对应的系统底包，然后参考上面的教程刷第三方REC。

刷完第三方rec会自动进入 进去之后把下载好的底包移动到手机里面进入清除 把按钮滑到右边 双清完再刷系统点击安装 选择下载好的底包 有个滑动按钮 滑到右边就开始刷了 记住 钩子不要勾

### 通用教程

刷完底包后请不要清除任何东西

请直接刷完底包接着刷原生ROM包

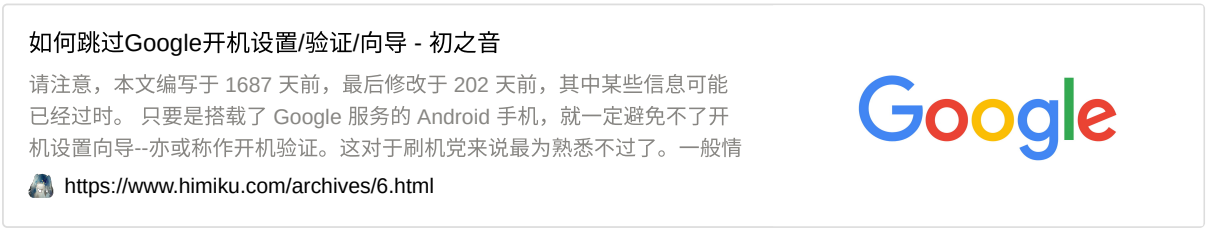
刷完，返回主页面 。

进入清除 格式化Data分区 。输入yes 三清就可以重启手机了。

**注意:如果不格式化DATA可能导致卡开机动画且无法连接电脑读盘**

三清:Dalvik/ART CacheCacheData刷机前基本上必选三清！目的是新系统的兼容性达到最佳。

进入系统如果有谷歌验证的话 过不了，建议格frp锁。




> 或者刷入https://mi.fiime.cn 的跳过包？

> 💡 第三方rec需要选择和安卓版本一样的包如果无限重启REC 请尝试刷入一次

## 突发救砖

1. 刷机包与手机自带的BOOT版本不匹配，这个时候只需要从ROM包里提取boot.img文件单刷，然后再重新刷机就好了。
2. 刷完后卡在第一屏或重启，可以进 RECOVERY 里面，双WIPE (**清除手机数据) 之后再刷机就可以解决问题**，一些ROM包会提示不用WIPE，但如果你出现上述情况，也可以双WIPE试试。
3. 如果你实在不行了，那么准备好保存好的原始 boot.img 和 vbmeta.img 刷入。

**因为未知原因导致安装失败也不要怕，操作中你应该保留了一份原来的镜像，按照最后一步的方法将原来的镜像重新刷回去就能正常开机。**

### 防护策略

- 安装 MM管理器 或 自动神仙救砖 插件
- 备份 Root 后的系统

移除模块重新开机

而如果你因为安装了未知模块而翻车无法顺利进入系统，请先冷静下来：解决此类问题有一个万能的命令`adb wait-for-device shell magisk --remove-modules`，此条指令将会在手机启动过程中生

效。

### MTK恢复

如果移除模块仍然无法开机，刷入系统备份（上文MTK提到了）。

自救命令，使用mtkclient写入备份的镜像

`python mtk wl out`

#### 解压 OTA 包获取其中的 boot.img

Payload 工具已经在工具包中给出

像Google 给出的刷机包，解压其中的 image 包可以直接获得我们想要的各种镜像文件。但部分厂商给出的升级包以及部分第三方 ROM 的刷机包中解压出来只有 payload.bin，无法进一步解压获得我们想要的各种镜像文件。

解压 payload.bin 需要用到特殊的工具，我们可以在 Github 上找到开源的 payload dumper，这是一个基于 python 3 的命令行工具。

以 zip 格式下载源代码，本地解压得到 payload_dumper-master 文件夹，下属两个 py 后缀的 python 文件。将 ROM 的 .zip 包解压缩后，把其中的 payload.bin 文件移送到 payload_dumper-master 中。

```
pip3 install protobuf #安装 protobuf
## 定位到 payload_dumper-master 文件夹
python3 -m pip install protobuf
python3 -m pip install -r requirements.txt
python3 payload_dumper.py payload.bin
```

FiimeROM-小米红米原生|移植|官改|SGSI|驱动|插件

FiimeROM作为一家专业的小米红米原生周边全资源平台，为用户提供MIUI固件，原生ROM，移植ROM和SGSI镜像，Rec下载，驱动下载，玩机教程等的服务，联合众多开发者更新维护开发工具和官改，致力于完善小米原生生态

https://mi.fiime.cn/Dtech/66.html


## 优化资源引用

## 社区

欢迎您

欢迎您

https://fiime.cn/

Magisk

Magisk - The Universal Systemless Interface, to create an altered mask of the system without changing the system itself.

https://forum.xda-developers.com/f/magisk.5903/


AKR社区

AKR, Hack Android! 围绕安卓，为开发者提供学习、分享、发布的交流平台。

https://www.akr-developers.com/


## https://github.com/topjohnwu/Magisk

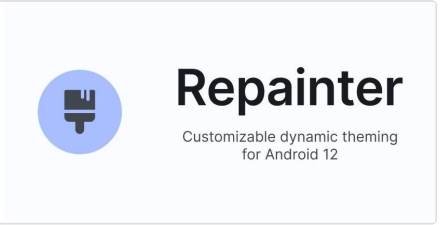
使用任何模块之前请考虑格机风险。模块推荐请自己查社区（酷安等）

## 资源分享

插件仓库-FiimeROM

FiimeROM作为一家专业的小米红米原生周边全资源平台，为用户提供MIUI固件，原生ROM，移植ROM和SGSI镜像，Rec下载，驱动下载，玩机教程等的服务，联合众多开发者更新维护开发工具和官改，致力于完善小米原生生态

https://mi.fiime.cn/libcangku




Magisk 资源分享

想获取更多的玩机资源？那就请来 magisk资源分享 这里看看吧！

https://shuajinet.com/

Magisk仓库模块

Magisk模块仓库（www.52ooooo.com）专注于Magisk模块，Xposed模块收集的模块仓库

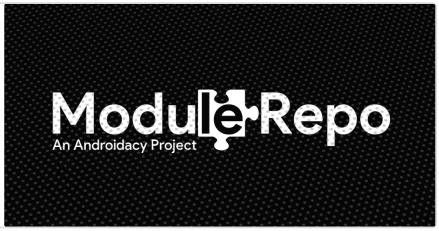
http://tx48.top/

## 社区模块库

Magisk Modules Repository - Androidacy

This is the Androidacy Magisk Modules Repo web app. Search, browser, and download your favorite Magisk modules right here.

https://www.androidacy.com/magisk-modules-repository/?utm_source=old-repo-link&utm_medium=web&utm_campaign=redirects



## https://github.com/LSPosed/LSPosed

> LSPposed是一个模块框架，可以在不接触任何APK的情况下更改系统和应用程序的行为。这意味着模块可以适用于不同的版本甚至ROM，而无需任何更改（只要原始代码没有更改太多）。它也很容易撤消。由于所有更改都在内存中完成，因此您只需停用模块并重新启动即可恢复原始系统。

请使用Zygisk，riru已经停止维护。如果你使用Zygisk，那么Riru就无法使用，这样的话Lsposed也无法使用。不过Lsposed已经推出了Zygisk版本。Zygisk模式下用Shamiko模块的白名单模式，真的是yyds。就是默认全局对所有应用隐藏Root，除了超级用户授权过的应用可以获得Root权限，其他新装软件都完全请求不到和检测到Root。低于安卓9的版本的Miui不要开启Zygisk模式，亲测卡米

MagiskHide没了，Zygisk又是啥？

小米不少机型这几个月都陆续升级到新的安卓12版本，新的系统版本无法继续使用老版本的Magisk，不得不使用alpha版或canary版的Magisk。新的Magisk版本（官方）中已经没有了MagiskHide，现在又来了个Zygisk。 说的都是废话，细的我也不懂。就看下面几条就完事了。 ...

https://www.bilibili.com/read/cv14287396

LSPosed（第三期） - Riru版和Zygisk版安装使用指南【手机改造计划】

各位看官老爷们 大家好 我是搞机半生归来仍是骚年的阿蒲 之前我们聊过LSPosed的使用指南 当时LSPosed还只有Riru版本 如今LSPosed已有Riru和Zygisk两个版本 时光荏苒岁月如梭呀 不知道大家现在更习惯使用哪个版本呢 使用Riru版本的请扣1 使用Zygisk版本的请扣2 闲言少叙 我们直接开始 使用LSPosed的先决条件是我们手机已解锁Bootloader（简称BL）并Root

https://www.bilibili.com/read/cv17028007

GitHub - LSPosed/LSPosed: LSPosed Framework

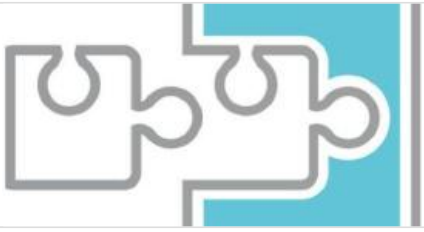
A Riru / Zygisk module trying to provide an ART hooking framework which delivers consistent APIs with the OG Xposed, leveraging LSPlant hooking framework. Xposed is a framework for modules that can change the

https://github.com/LSPosed/LSPosed


Xposed-Modules-Repo

New Xposed Module Repo. Xposed-Modules-Repo has 214 repositories available. Follow their code on GitHub.

https://github.com/Xposed-Modules-Repo



LSPosed

(For developers only) LSPlant is open-sourced and uploaded to maven!!We have extracted our Android Runtime (ART) hook framework into a single, open-sourced library LSPlant (like Sandhook, YAHFA, Epic, and

https://t.me/s/LSPosed

下载模块后，在面具的设置中开启 Zygsik，同时在模块中从本地安装 LSposed。重启设备，桌面就新增 LSPosed 的APP。

## 安全验证^7

Google 那边已经给开发者提供了一个基于 SafetyNet 认证的反盗版功能（anti-piracy feature），开发者如果使用这套机制，那么已经 root、无法通过 SafetyNet 认证的设备就没办法在 Play 商店搜索、下载和更新对应的 App。

SafetyNet 是 Google 移动服务套件的功能，这意味着，只有装有 GMS 并且应用调用了相关接口的情况下，我们才需要通过 SafetyNet 验证。逃避国内应用的 root 检测大部分情况下并不需要通过 SafetyNet 认证，只要使模块和 Magisk 不对这些应用生效即可，无需在意 SafetyNet 结果。

推荐 YASNAC。下载此软件，然后进行一次测试，我们便知道自己的设备是否启用了基于硬件的安全验证。

留意 `evaluationType` 一项的结果，根据前文的解释，若此结果为 `basic`，则意味着没有启用基于硬件的安全验证，若此结果为 `hardware`，则增强安全验证已经启用。

如果选项为 `basic`，我们可以：

• 开启 Zygisk，使用排除列表，将需要的应用添加进排除列表中；依照前面的说法，排除列表中的应用是不受 Magisk 影响的，并且由于系统没有基于硬件的安全验证，此时设备仍然可以通过 SafetyNet；然而**其代价是所有模块在此应用上均无效果**；

Zygisk模式下用Shamiko模块的白名单模式，真的是yyds。就是默认全局对所有应用隐藏Root，除了超级用户授权过的应用可以获得Root权限，其他新装软件都完全请求不到和检测到Root，配置教程请读：

图文分享

https://www.coolapk.com/feed/37950576

附：

https://play.google.com/store/apps/details?id=rikka.safetynetchecker

Shizuku

让你的应用直接使用系统 API

https://shizuku.rikka.app/zh-hans/

## 附录

1^**所需资料打包**<>

2^ **root、刷rec、rom通用教程**<sudo0m.github.io/2022/05/29/root、刷rec、rom通用教程/>

3^Android 玩家必备神器入门：从零开始安装 Magisk - 少数派 (sspai.com)

4^Magisk官方教程<https://topjohnwu.github.io/Magisk/>

5^Magisk官方论坛<https://forum.xda-developers.com/f/magisk.5903/>

6^每个 Android 玩家都不可错过的神器（一）：Magisk 初识与安装 - 少数派 (sspai.com)

7^Android 玩机「神器」的矛盾与新生：Magisk Canary 更新详解 - 少数派 (sspai.com)

8^**Root隐藏教程**：图文分享 - 酷安 (coolapk.com)

9^**酷安MiaoHan 的专栏** https://www.coolapk.com/feed/32286938

10^APKMirror - Free APK Downloads - Free and safe Android APK downloads

11^Clash For Magisk简介 - CFM (adlyq.ml)

12^**小米手機各種刷機方式的疑問?** https://www.mobile01.com/topicdetail.php?f=634&t=3725269

13^**通过 ADB 给手机刷入第三方 Recovery**

14^**小米如何刷入第三方Recovery** https://zhuanlan.zhihu.com/p/428730333

15^ 告诉大家如何防止掉基带问题 https://www.coolapk.com/feed/21305538

16^酷安Rannki原创 https://www.coolapk.com/feed/21305538

17^常识基础 https://mi.fiime.cn/tutorial

18^**刷入原生ROM的通用教程等教程** https://fiime.cn/thread/359

19^**Violet 机型 PE/Plus 刷入教程**

20^**如何在 Redmi Note 7 Pro 上刷机？**

21^https://wiki.pchelper666.com/底层刷机教程

22^**高通9008线刷救黑砖教程** https://www.bilibili.com/read/cv15031395/