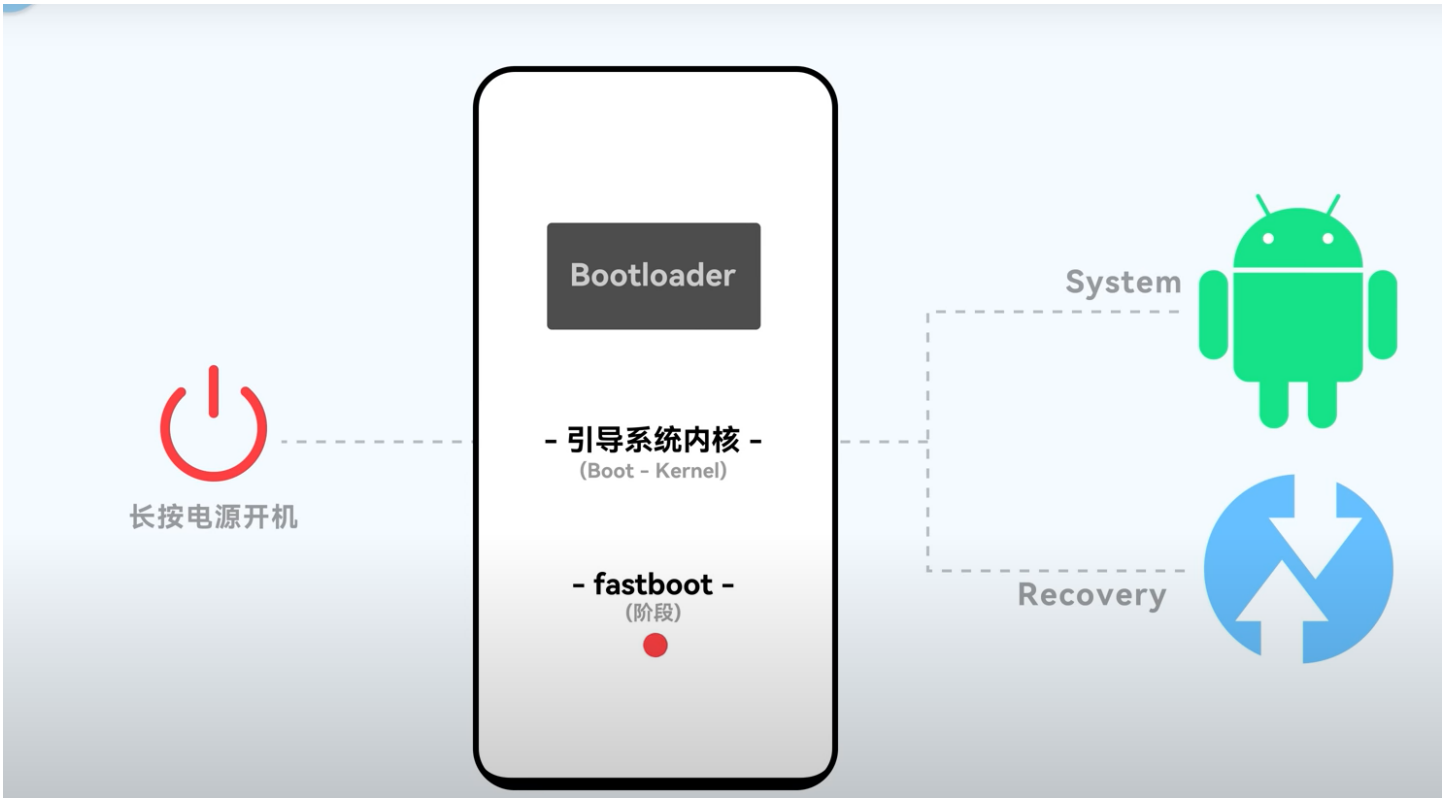
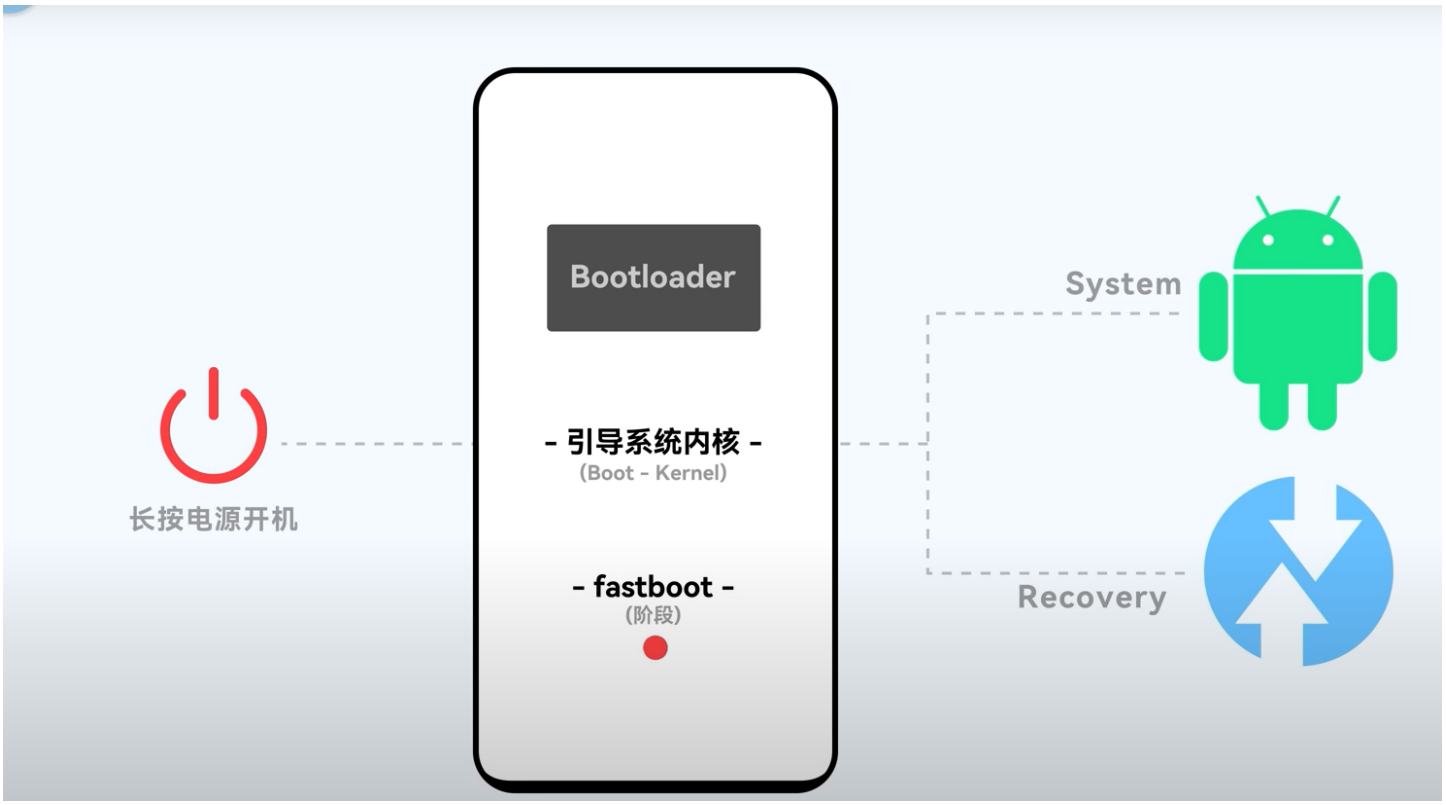
刷机相关的词汇解释





权限

- 第三方软件权限（低）
  - 比如，每次app启动都会向用户请求读取信息，当然流氓软件你不同意，APP直接不让你启动

- 用户权限（中）
  - 基本的增删改查，安装app，卸载app，设置登陆密码，搜索浏览本地文件等
- Root权限（超级用户，最高）
  - 至高无上的权限

分区

- Boot分区
  - 启动和引导文件
    - Kernel（内核）
    - Ramdisk（虚拟内存）
- System分区
  - 系统分区
    - 操作系统和预装的软件
- Data分区
  - 用户数据，包括应用，音视频，图片，文档，系统设置等
- Cache
  - 缓存
- Recovery
  - 恢复和更新其他分区的内容

Android7.0以后分为A，B区（Boot，System）
A区：日常使用的分区
B区：备用分区

...后续还可能会改变

Bootloader锁

Bootloader中文名称为“启动加载”。在嵌入式操作系统中，BootLoader是在操作系统内核运行之前运行，它可以初始化硬件设备、建立内存空间映射图，从而将系统的软硬件环境带到一个合适状态，以便为最终调用操作系统内核准备好正确的环境。

Bootloader引导启动时检测即将被启动的东西（recovery.img / boot.img）的签名是否是厂商的，如果不是的话就拒绝启动。

Recovery

Recovery是Android手机备份功能，指的是一种可以对安卓机内部的数据或系统进行修改的模式（类似于windows PE或DOS）。在这个模式下可以，对已有的系统进行备份或升级，也可以在此恢复出厂设置。

刷入第三方的Recovery，将获得更多的功能，并且可以刷入第三方rom，官方自带则不行。

进入recovery的方法：

1、将手机完全关机后，按住音量键下（上）+电源键，进入bootloader界面；

2、按音量键将光标移动到recovery那一行；

3、按电源键，之后手机会自动重启进入recovery模式。

其中音量键为光标选择键，可以用来移动光标，电源键则是确认键。

主界面

reboot system now：重启手机（刷机完毕选择此项就能重新启动系统）

apply SDcard：update.zip：安装存储卡中的update.zip升级包（你可以把刷机包命名为update.zip然后用这个选项直接升级）

wipe data/factory reset：清除用户数据并恢复出厂设置（刷机前必须执行的选项）

wipe cache partition：清除系统缓存（刷机前执行）（系统出问题也可尝试此选项，一般能够解决）

install zip from SDcard：从SDcard上安装zip升级包（可以执行任意名称的zip升级包，不限制升级包名称）

backup and restore：备份和还原系统（作用和原理如同电脑上的Ghost一键备份和还原）

mounts and storage：挂载和存储选项（详细功能见下面的解释）

advanced：高级设置

Fastboot

Fastboot，英语翻译意思是快速启动。在安卓手机中fastboot是一种比recovery更底层的刷机模式（俗称引导模式）。就是使用USB数据线连接手机的一种刷机模式。相对于某些系统（如iOS）卡刷来说，线刷更可靠，安全。

准备工具

1. fastboot工具(安卓工具箱中有提供)
2. 自己手机能用的boot.img、recovery.img文件。

具体步骤

一、手机进入fastboot模式并用数据线连接电脑，安装好相关驱动程序。

二、解压下载好的fastboot工具，如解压到D:/fastboot/。

三、将准备好的boot.img、recovery.img文件文件也放到D:/fastboot/中。

四、打开命令行工具cmd，执行如下命令进入到fastboot所在目录中

d: 回车

cd fastboot 回车

fastboot devices 回车

如果它列出了你的手机，如HT*******，说明手机连接好了

执行以下命令刷入boot与recovery：

fastboot flash recovery recovery.img 回车

等待OKAY （这里是刷新recovery）

fastboot flash boot boot.img 回车

等待OKAY （这里是刷新boot）

双清/三清/四清

双清就是清除Data、Cache两个分区，这个操作会导致你在系统刷好后安装的普通APP通通被清空，但并不会清空sdcard中的数据（也就是你日常存文件的那个目录），相当于恢复出厂设置。

三清就是在双清的基础上把Dalvik Cache也给清了，某些特定场景下可以解决程序崩溃的问题。

四清通常指的是在三清的基础上连System分区也给清了，这会导致你的系统彻底消失，类似于在电脑上把系统盘格式化了一样，通常并不需要进行这个操作。

boot.img

boot.img是Android系统启动所必须加载的文件。简单的说，boot.img包含两部分，分别为kernel 和 ramdisk。

twrp.img

TWRP实际上就是替换了原机自带Recovery的第三方程序

常用的命名

adb命令

```
adb devices                          显示设备信息
adb install 123.apk                  安装一个软件
adb uninstall -k 123.apk             删除一个软件
adb shell                            进入shell环境
adb push c:/1.txt /sdcard/sdir/      向设备推送文件
adb pull /sdcard/1.txt C:/           从设备取回文件
adb reboot bootloader/recovery       使手机重启进入BL或RE
adb reboot recovery
```

fastboot命令

```
# 进入fastboot
adb  reboot  fastboot
# 刷入第三方的recovery，分区
fastboot flash recovery recovery.img
# 重启手机
adb reboot
# 重启到Recovery界面
adb reboot recovery
# 重启到bootloader界面
adb reboot bootloader
# 擦除分区
fastboot erase 分区名
比如：清除system分区 fastboot erase system
```

刷机流程

基础操作

https://twrp.me/

1.打开手机的开发者模式

提前下载一个ADB工具

2.解锁bootloader

解锁bootloader(bl锁)的风险和可行性
小米（官方申请），oneplus（直接命令,进入fastboot，fastboot oem unlock），samsung，sony，moto解锁教学
难解锁的机型：
华为，荣耀，oppo，realme，vivo

推荐：
小米，oneplus

注意：
非必要不解锁，解锁可能带来如下的风险：

1. 失去厂家保修
2. 失去一些原生功能
3. 清除系统数据
4. 会存在一些安全问题，密码泄露，个人信息泄露等

3.申请root权限和开始刷机

方法1: Recovery卡刷：TWRP(可玩性高，但麻烦)

找手机厂商
https://twrp.me/Devices/

找机型
https://twrp.me/Devices/LG/

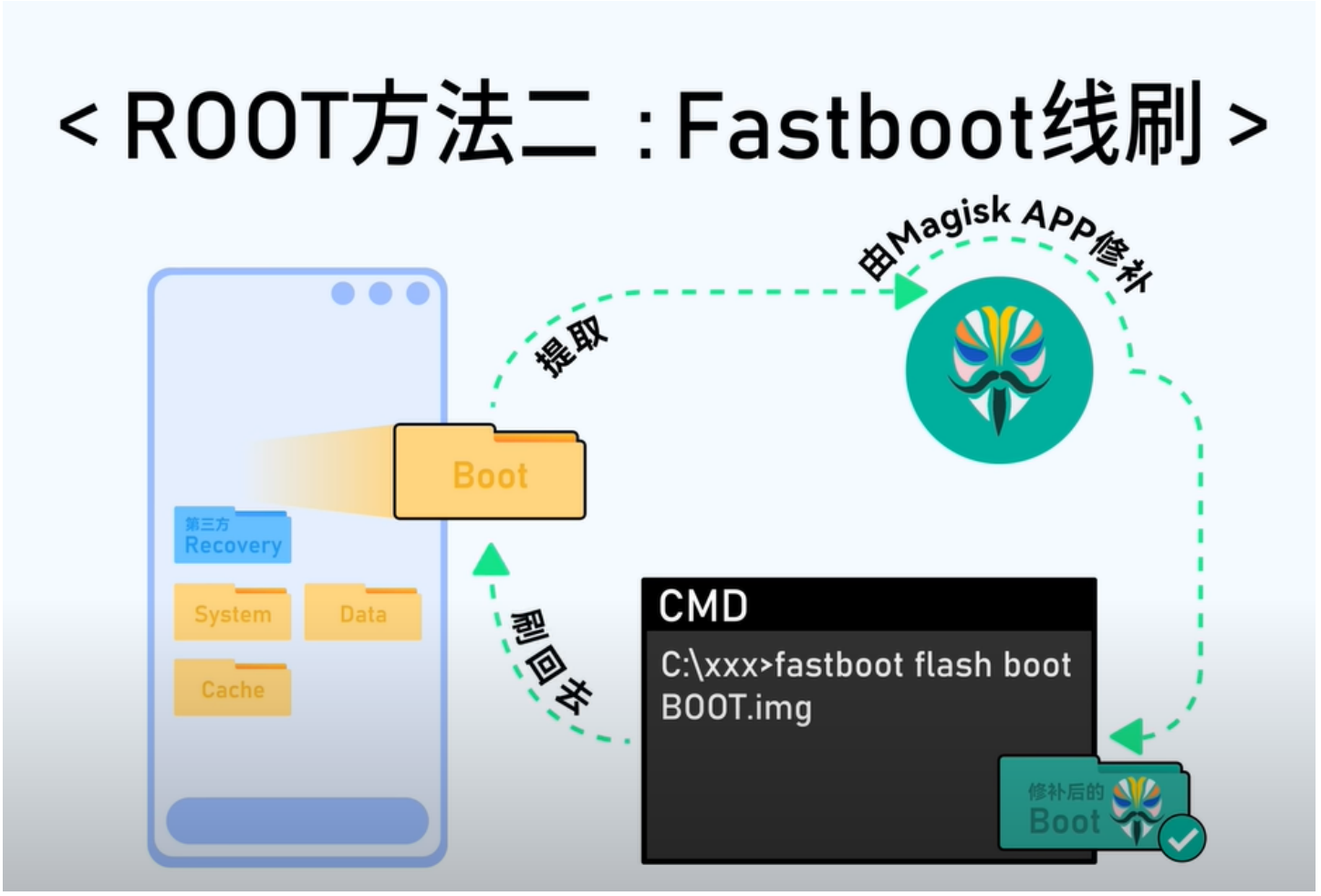
找img包
https://dl.twrp.me/hammerhead/
刷入第三方Recovery：
然后将手机设置到 `fastboot` 模式，使用 `fastboot` 命令将镜像刷进去。

```
$ fastboot flash recovery twrp-3.2.3-0-bullhead.img
```

刷入magisk：
申请超级用户（root，也可以隐藏）

方法2: Fastboot线刷：要找boot镜像 (简单，可玩性低)

通过命令： `fastboot flash boot boot.img` (没有root，必须自己去官方或者论坛中对应的手机刷机包中找boot.img)



刷包

谷歌的原生系统

根据手机的型号找就行了

https://developers.google.com/android/ota#hammerhead

面具（帮你root的app）

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

老版本的xposed

安装https://repo.xposed.info/module/de.robv.android.xposed.installer

或者

下载Xposed框架：http://dl-xda.xposed.info/framework/sdk23/arm/
我这里是下载最新的v86-sdk23版本。直接刷入

新版本的edxposed，安卓8以后

https://repo.xposed.info/module/org.meowcat.edxposed.manager

小米手机挂载问题

```
# 手机 root 方法参考各手机 root 教程，小米手机在 Windows 电脑下载[解锁工具](//www.miui.com/u
# 以小米手机为例来开启 root 权限后设置 /system 目录为读写
# 以 root 权限执行
adb root
# 解决目录 read only 关键命令行
adb disable-verity
# 重启
adb reboot
# 以 root 权限运行
adb root
# 重新挂载
adb remount
# 设置读写
adb shell mount -o rw,remount /system
```

刷机谷歌pixel手机（版本android8.1.0，系统sailfish）

步骤

注意：刷完机之后，取消账号登录

1. `adb reboot bootloader` 进入Bootloader界面
2. 刷入必要的img文件，执行flash-all
3. 刷入TWRP（和刷入的系统发布年份差不多一致）
4. 安装**https://github.com/ElderDrivers/EdXposed**
5. 安装frida
6. 配置charles（注意android7版本以上，证书不信任问题）
    i. **https://github.com/NVISO-BE/MagiskTrustUserCerts**（必须刷入Magisk）
    ii. re管理器把 `/data/misc/user/0/cacerts-added/` 这个路径下面的文件复制到 `/system/etc/security/cacerts` ，记得挂在读写

附地址

各种玩机地址/工具/命令汇总：**http://wanji.jamcz.com/**

Android SDK（ADB和Fastboot电脑端工具）：**https://developer.android.google.cn/s...**

ADB/Fastboot驱动：**https://cz-jam.lanzouj.com/iZICY02v2k8j**

TWRP：**https://twrp.me/**

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

小米解锁工具：**https://www.miui.com/unlock/index.html**

小米ROM下载：**https://xiaomirom.com/series/**

小米刷机工具：**https://cdn.alsgp0.fds.api.mi-img.com...**

一加ROM下载：**https://www.oneplus.com/cn/support/so...**

三星刷机工具：**https://odindownload.com/**

三星ROM下载：**https://www.sammobile.com/firmwares/**

魅族ROOT链接：**https://mroot.flyme.cn/**

OPPO解锁：**https://www.oppo.cn/thread-397164526-1**

OPPO ROM：**https://www.coloros.com/rom**

Realme解锁：**https://www.realmebbs.com/post-detail**...

Realme刷机工具：**https://www.realmebbs.com/post-detail**...

Realme ROM：**https://www.realme.com/support/softwa**...

索尼解锁：**https://developer.sony.com/develop/op**...

索尼ROM：**https://xperifirm.com/**

MOTO解锁：**https://motorola-global-portal.custhe**...

MOTO ROM：**https://mirrors.lolinet.com/firmware/**...

payload-dumper解包工具：**https://mrzzoxo.lanzouw.com/iR65zpaueyd**

酷安（玩机社区）：**https://www.coolapk.com/**

XDA（海外玩机论坛）：**https://forum.xda-developers.com/**