VIVO IQOO PRO 5G 刷机成功记录（理论上 IQOO pro 也适用）

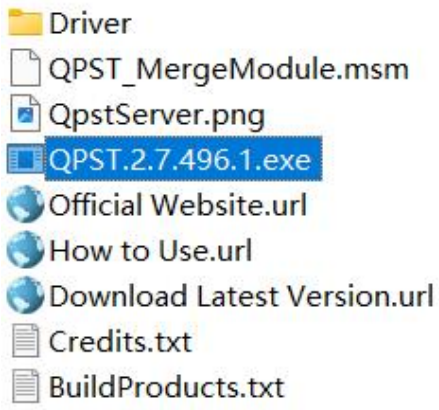
拆机 9008 降级

一、电脑环境准备：

9008 驱动：vivo_usb_driver.exe
QPST_2.7.496
viQOO 工具箱 V2.1.3
9008 刷机包

1.安装驱动 vivo_usb_driver.exe，安装到默认位置，以前装过其他 9008 驱动可以跳过此步骤

2. 安装 QPST_2.7.496，解压 QPST_2.7.496(包含 QFIL).zip，解压后路径不要有中文，解压完成后运行 QPST.2.7.496.1.exe 安装，安装到默认位置不要更改



3. 解压 viQOO 工具箱 V2.1.3.7z，解压后路径不要有中文。
4. 解压 9008 刷机包：Vivo_iQOO Pro 5G_PD1916-8.11.2_9008 线刷-使用 QFIL.zipVivo_iQOO Pro 5G_PD1916-8.11.2_9008 线刷-使用 QFIL.zip，解压后路径不要有中文

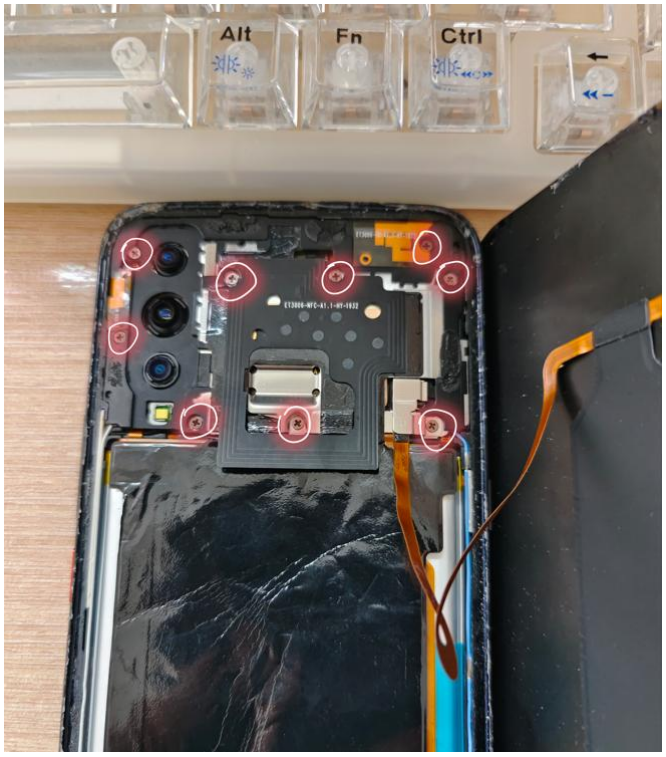
二、手机拆机准备

成功解锁版本截图：

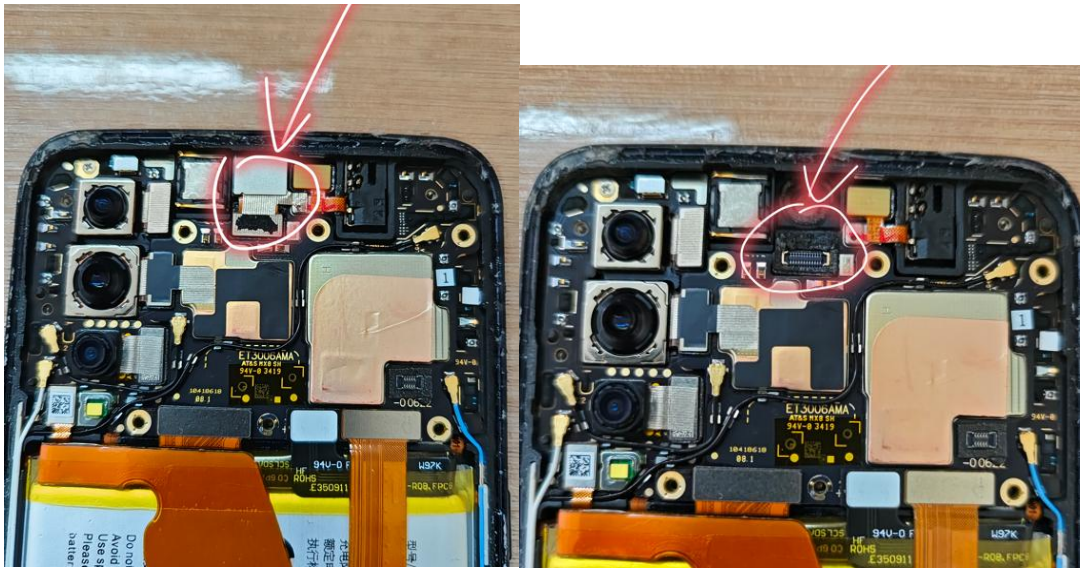
如果你的版本低于 8.11.2，可以尝试一下用 fastboot 线刷包里的 8.11.2 直接升级（我的手机直接用线刷包升级会失败，因此无法验证这个包能否成功解锁）

如果版本高于 8.11.2 或低版本直接升级失败，就需要拆机进 9008

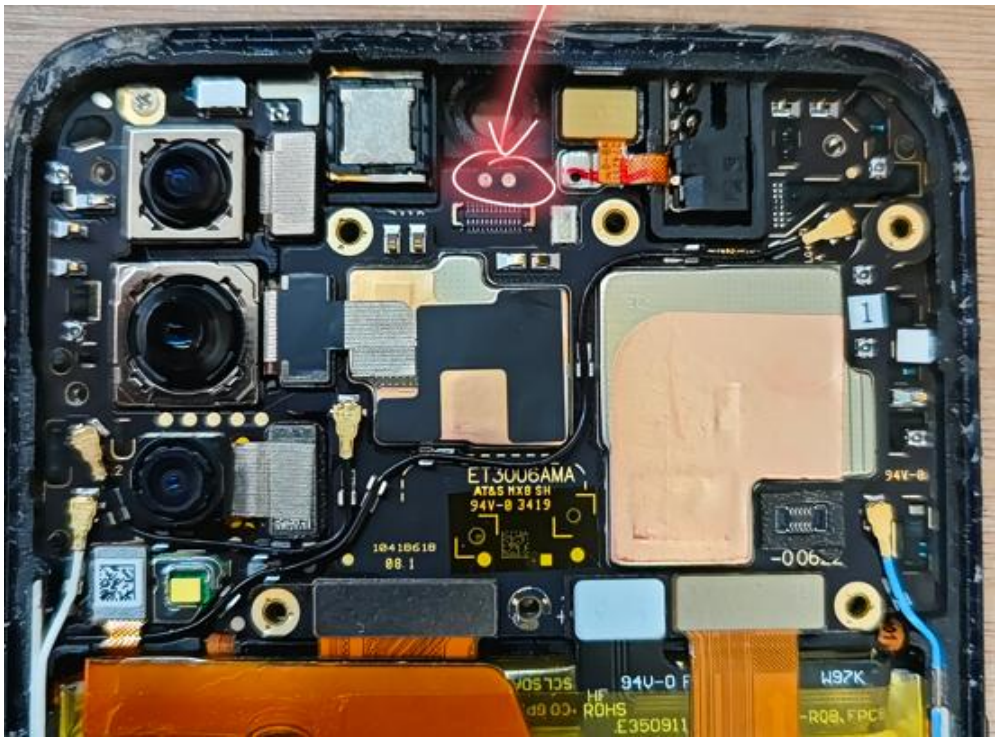
1. 关机后取出 sim 卡槽，用吹风机热风吹后盖，插入拆机片或其他稍硬的卡片沿着后壳划一圈。打开后盖后拧下 9 颗螺丝移除背板



2. 断开前摄排线取下前摄，并小心撕下缓冲泡棉



3. 图上的两个触点就是 9008 调试点位。关机状态下用镊子短接这两个点位，再插上数据线，电脑的设备管理器-端口里就能看到 9008 设备



三、使用 QFIL 刷机

前面安装好 QPST 后就能在安装路径中找到 QFIL，默认安装路径：C:\Program Files (x86)\Qualcomm\QPST\bin，找到里面的 QFIL.exe，右键以管理员身份运行

（或者在 windows 的开始菜单里搜索 QFIL 并以管理员身份运行）

1. 第一次打开要进行设置，Configuration > firehose configuration

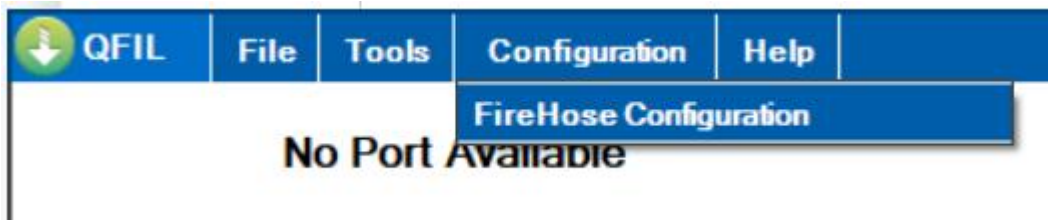
Download Protocol 选 0-Sahara

Device Type 选 ufs

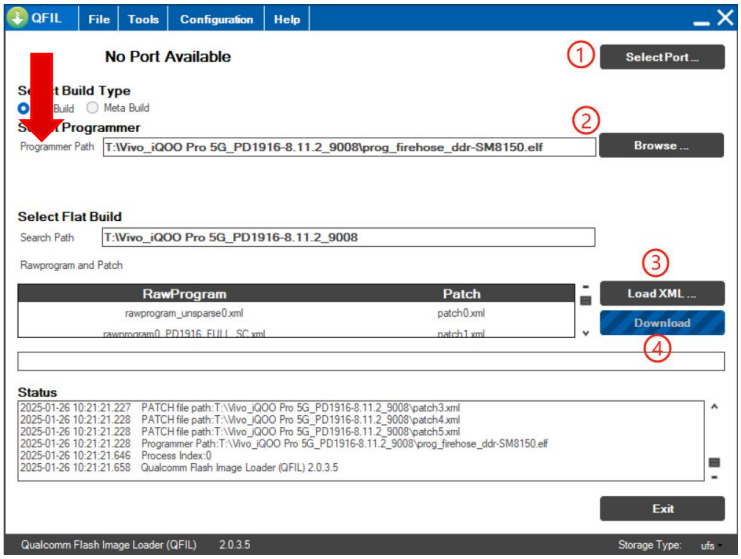
Validation Mode 选 0-No Validation

勾选 Reset After Download

点击 ok 保存，关闭软件重启生效



2. 重启软件后选择 Flat Build，点击 Select Port 选择 9008 端口
点击 Browse 选择解压后的 9008 文件夹内的 prog_firehose_ddr-SM8150.elf
点击 Load XML 选择解压后的 9008 文件夹内的（多选）rawprogram_unsparse0.xml，rawprogram0_PD1916*_FULL_SC.xml（*代表手机目前版本号中的字母，8+256 为 D,12+128 直接选择 rawprogram0_PD1916_FULL_SC.xml，如果不确定版本可以开机后看下设置里的软件版本号），rawprogram1.xml，rawprogram2.xml，rawprogram3.xml，rawprogram4.xml
选择好提交一次后会再弹出一个选择框，选中所有 patch xml 文件：patch0.xml ~ patch5.xml
全部选好后点击 Download，等待下方进度条走完刷机成功，刷好后手机会自动开机



四、解锁 bl

手机刷好 8.11.2 版本后去设置进入开发者模式，打开 OEM 解锁和 usb 调试，退出 vivo 账号，关闭查找手机

以管理员身份运行 viQOO 工具箱的“1.启动工具箱.bat”，选择 1.解锁 bl

解锁方案选择 1.新版高通 xda 方案

```
=------------------------------------------------------------=

                          解锁BL锁

=------------------------------------------------------------=


- 确定要解锁BL锁么？解锁刷机可能造成以下影响：
  手机数据被清空
  手机系统损坏无法开机
  基带丢失
  失去保修
  光学指纹失效（可以售后校准恢复）
  指纹支付不可用（好像可以通过模块修复）
  ...
  自愿承担以上风险，请输入1按Enter继续，否则直接按Enter返回主菜单
1
- 解锁BL锁会清空手机内所有数据 ！！！
  请确认数据已自行备份到手机之外！
  请退出其他手机管理和刷机软件，然后按任意键开始...

- 请选择解锁方案：
  1.新版高通xda方案：如果你的设备是高通处理器且是近两年的新机，可
    以尝试此方案。
  2.MTKClient强解：如果你的设备是联发科处理器，可以尝试此方案。
  3.老机型旧版指令解锁：如果你的设备是六七年前的老机器（官方系统安
    卓5或5.1），可以尝试此方案。
  4.9008修改分区解锁：此方案已知适用于vivoX7系列，X9系列，Y66i。
  输入序号按Enter键继续：
```

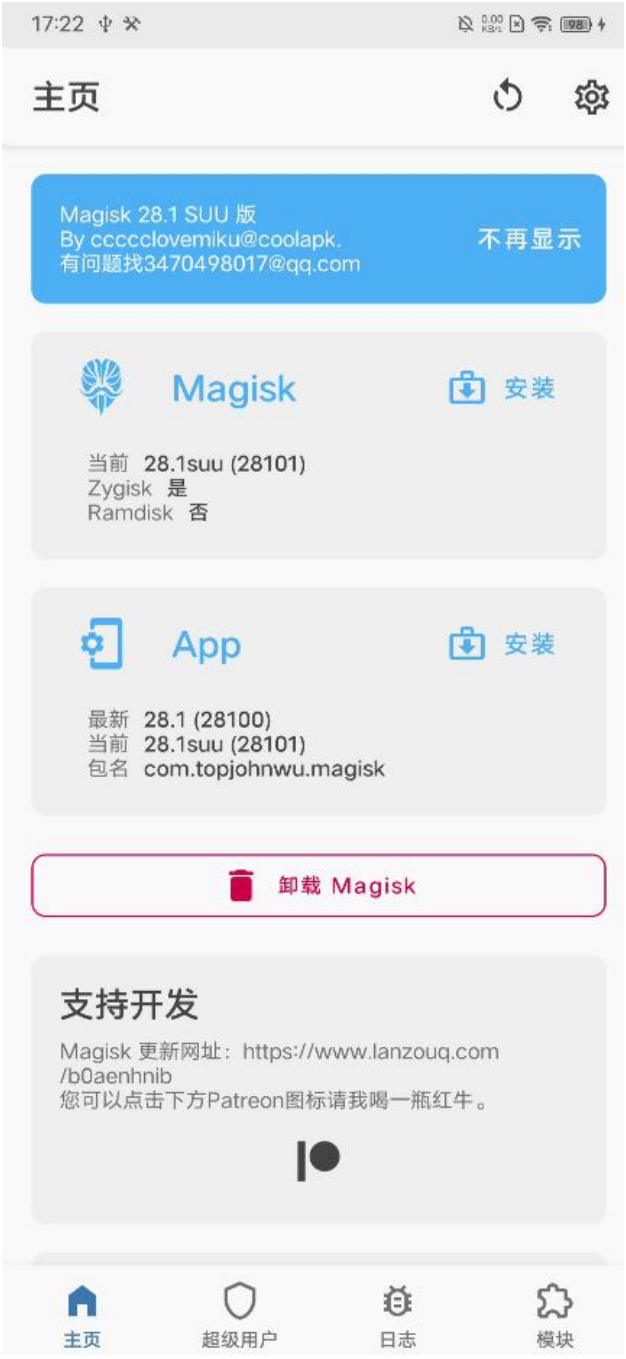
解锁成功后在开机时会有如下提示：

五、获取 root

由于 vivo 屏蔽所有 su 命令，所以普通面具无法正常使用，只能使用 suu 版本面具

suu 版本面具使用自定义的 suu 命令替代 su 命令，会有很多需要 root 权限的应用并没有适配自定义命令导致无法申请权限，不过这个问题可以靠 lsposed 模块或其他方法解决

由酷安的 ccccclovemiku 大佬修改的 suu 版本面具 https://github.com/4accccc/vivo-Magisk-suu
安装好 suu 面具后就和正常装面具流程一样
从 9008 刷机包里复制 boot.img，面具里修补后再传回电脑，手机进 fastboot 后用命令（fastboot flash boot 修补后的文件绝对路径）刷入然后重启
这个机型可玩性小，无法刷其他系统，也建议不要动 recovery，可能会无法开机
刷好面具后如下图，Ramdisk 显示为否，但是实际使用不影响，可能是这个机型特有的问题



然后是常用的过环境检测，Shamiko 只有安装 0.7.5 版本才能在 suu 版本面具下使用，但是 momo 的检测一直过不了，不知道有没有大佬同机型能过完美检测的

最后说下解决大部分应用在 suu 面具下获取 root 的方法：
装好 lsposed 后安装附件里提供的插件
这个模块有内置的修改应用 su 命令的功能

点左上角进入菜单，选择拓展功能，在应用列表中选择要修改的应用，打开总开关和replaceSu+的开关，然后长按 replaceSu+输入自定义 su 命令，改为 suu 保存即可，注意对应应用要在 lsp 的模块中勾选