中兴远航 30s 小白向解锁 bl+ 解锁 root 流程

一周前刚从🐟上购入 6+128 的全新远航 30s（套娃机，名字还叫 vikk v16 plus），非常感谢大佬！让我立刻就能 root 远航 30s。大佬的解锁教程位于 github 链接，但我作为菜狗中间还是踩了不少坑，所以打算补充完善一下大佬的教程，以小白向的流程发布（这或许也是中兴系第一个展锐处理器小白解锁教程 hhhh）

前提前提：

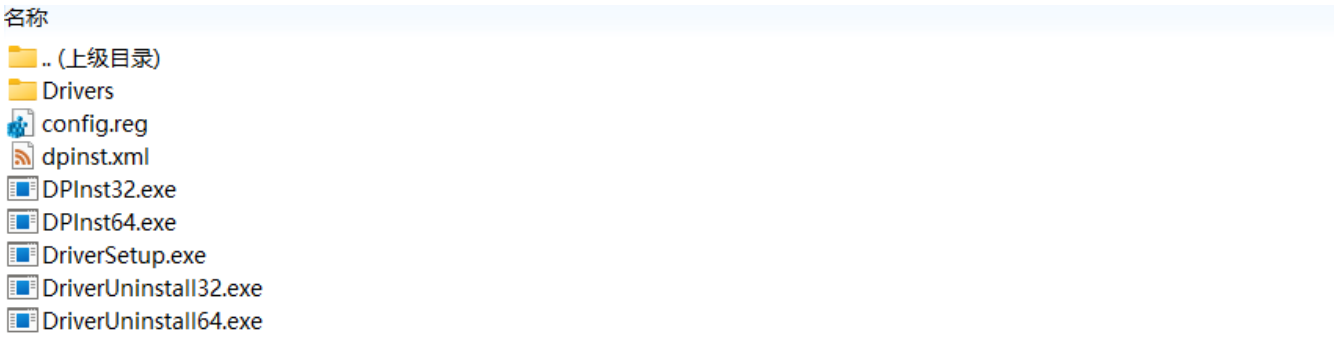
请确保手机电量充足！！至少在 80% 以上供你折腾！

学会并可以执行 adb 命令，如果不会的话去百度吧。

学会并可以执行 cmd 命令，你最好已经学会在 windows 终端中执行 cmd 命令。

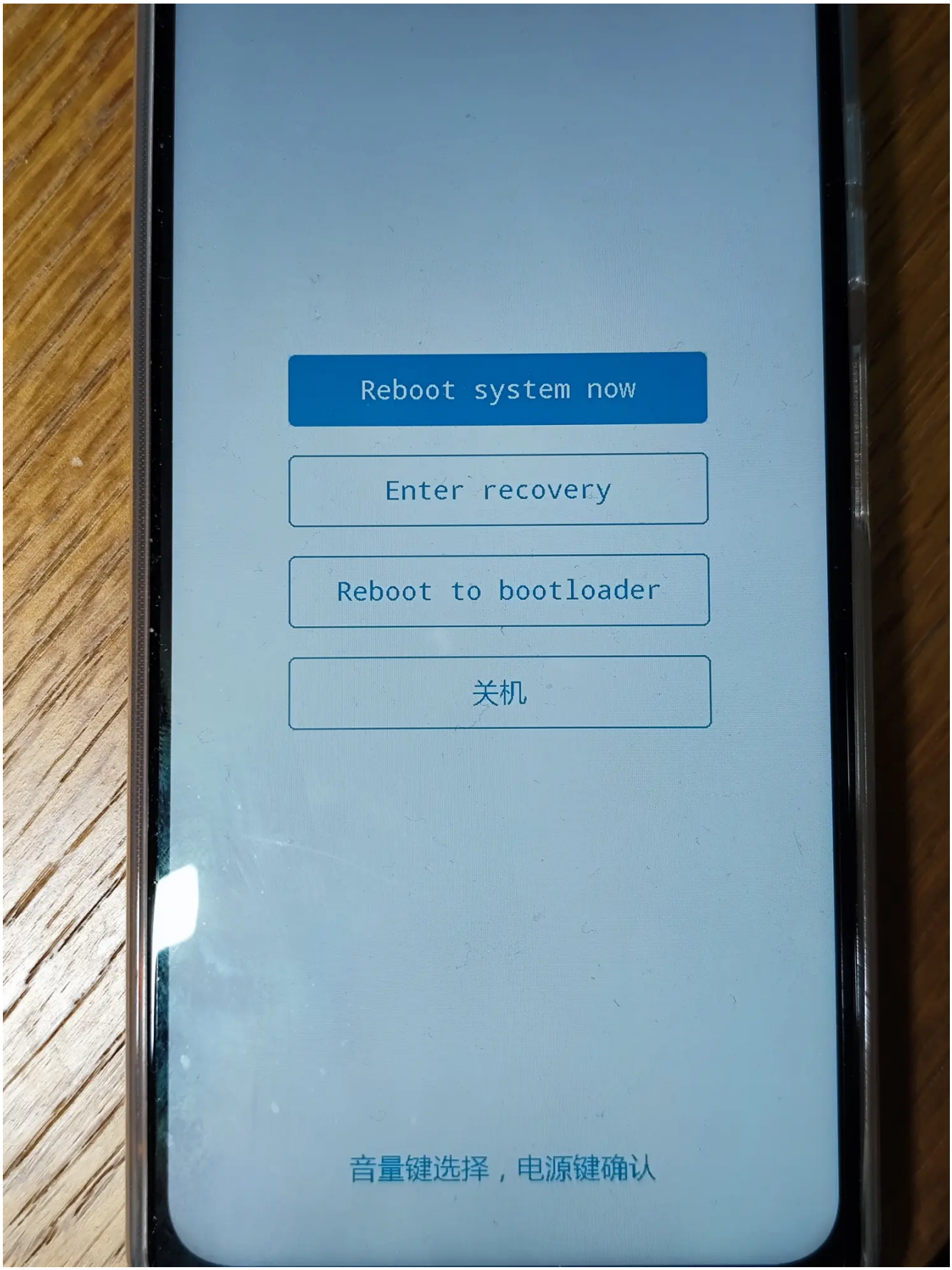
bl 解锁步骤：

1. 下载并解压 windows 端展锐驱动 SPD_Driver_R4.20.4201.zip，找到你的系统对应版本文件夹，然后找到 DriverSetup.exe 以及 DPInst64.exe 安装（linux 端及驱动安装失败的，请参考大佬的 github 链接）



2. 下载解锁脚本，可以去大佬的网盘下载网盘链接，我也上传了蓝奏云蓝奏云链接。关闭杀毒软件然后解压
3. 手机关机，数据线连接电脑
4. 找到 unlock_emmc.bat，使用管理员权限打开，其会等待 30s

5. 长按手机音量减 + 电源键，手机会进入下载模式（电脑应该会听到有设备连接的声音），此时手机黑屏是正常情况
6. 脚本会自动运行，根据脚本提示运行脚本，脚本会运行多次。如果是等待 10s 就等待；如果显示 pause，当你听到手机再次连接电脑之后，回车跳过 pause【请抓紧时间，不要让手机脱离黑屏状态】。
7. 脚本会自动备份 boota.img/bootb.img，该过程非常缓慢，耐心等待（emmc 是这样的）
8. 解锁完成之后手机会进入一个蓝白色界面（如下图所示，此为 fastbootd 界面）



，请手动进入 recovery 模式，并且清除数据，recovery 界面如下图所示



9. 清除完成数据即可开机，此时手机左上角显示如下小字，即为 bl 解锁成功。

“INFO: LOCK FLAG IS : UNLOCK!!!”

“WARNING: LOCK FLAG IS : UNLOCK, SKIP VERIFY!!! ”

10. 第一次开机时间较长（卡在 myos 界面），请耐心等待。如果 15min 后仍卡第二屏（myos），重刷系统完整包（见附录）

解 bl 常见问题：

1. 解锁完成之后卡第一屏（厂商 logo）并且无限重启

说明没有清除数据，建议重刷系统完整包（见附录）

2. 脚本提示无法写入

如果是无法写入 uboot，可以在脚本最后

将 spd_dump exec_addr 0x65012f48 fdl fdl1-dl.bin 0x65000800 fdl fdl2-dl.bin 0xb4fffe00 exec write_part splloader %spl_bak% write_part uboot_a %uboot_a_bak% write_part uboot_b %uboot_b_bak% erase_part misc write_part misc misc-fastbootd.bin read_part boot_a 0 64m boota.img read_part boot_b 0 64m bootb.img reset

修改为

spd_dump exec_addr 0x65012f48 fdl fdl1-dl.bin 0x65000800 fdl fdl2-dl.bin 0xb4fffe00 exec write_part splloader %spl_bak% erase_part uboot_a write_part uboot_a %uboot_a_bak% erase_part uboot_b write_part uboot_b %uboot_b_bak% erase_part misc write_part misc misc-fastbootd.bin read_part boot_a 0 64m boota.img read_part boot_b 0 64m bootb.img reset

[就是在 write 之前先 erase 这个 part，以确保可以写入]

3. 脚本卡在读取 boot.img

emmc 是这样的，时间很长。如果等不了，或者你是 11 系统无需备份 boot 的话，可以删除读取 boot 部分。即将脚本最后改为

spd_dump exec_addr 0x65012f48 fdl fdl1-dl.bin 0x65000800 fdl fdl2-dl.bin 0xb4fffe00 exec write_part splloader %spl_bak% write_part uboot_a %uboot_a_bak%

write_part uboot_b %uboot_b_bak% erase_part misc write_part misc misc-fastbootd.bin reset

4. 解锁完成之后卡第二屏（MyOS）

进 fastbootd 重刷系统完整包（见附录）

root 解锁步骤：

1. 首先确保你的手机系统为最新的 11.5.11 系统（MyOS11.5.11_7531N_UNI_H），如果不是的话（例如 vikk 系统，例如 06 系统，03 系统），请重刷系统完整包（见附录）并 ota 更新至 11 系统
2. 下载大佬制作好的远航 30s，11 系统版本 boot（boot 已经修补 magisk 并签名）。下载链接：https://wwi.lanzoup.com/inhZc1qps6ah
3. 进入 fastbootd 模式（蓝白界面），使用 fastboot enhance 刷写 boot2309-27000.img，你是 a 槽位的系统就刷 boot_a 分区，你是 b 槽位的系统就刷 boot_b 分区。
4. 如果你是 ota 到 11 版本的系统，它会提示存在 system_a/b_cow 分区，是否强行刷入，强行刷入 boot 分区即可。
5. 清除数据并重启手机，第一次开机时间较长，请耐心等待。
6. 开机完成后下载 magisk27 版本，下载链接 https://mrzzoxo.lanzoui.com/ivf891nh5zsf，打开后提示修复 magisk 环境，等他自动修复并重启即可。
7. 可以通过 adb shell 命令进入 shell，输入 su 测试是否 root 成功。

刷 root 常见问题：

1. 我的系统版本不是 11.5.11，且无法 ota 升级到该版本

1.1 如果是版本号大于 11 的（5g+4g 版本），请自行修补 boot 并签名（详见大佬 github：https://github.com/TomKing062/CVE-2022-38694_unlock_bootloader/wiki/Magisk#magisk-systemless-mode），这需要一定计算机基础。

1.2 如果版本号小于 11，请刷系统完整包（参照附录）

2. 刷完 boot 之后卡第一屏

如果你是手动修补的 boot，请根据大佬的 github 进行正确的签名（见问题 1.1 中 github 链接），然后重新刷入签名后的 boot。

如果还是不行 / 其他情况，请刷系统完整包（见附录），确保能开机后再重新刷入 boot

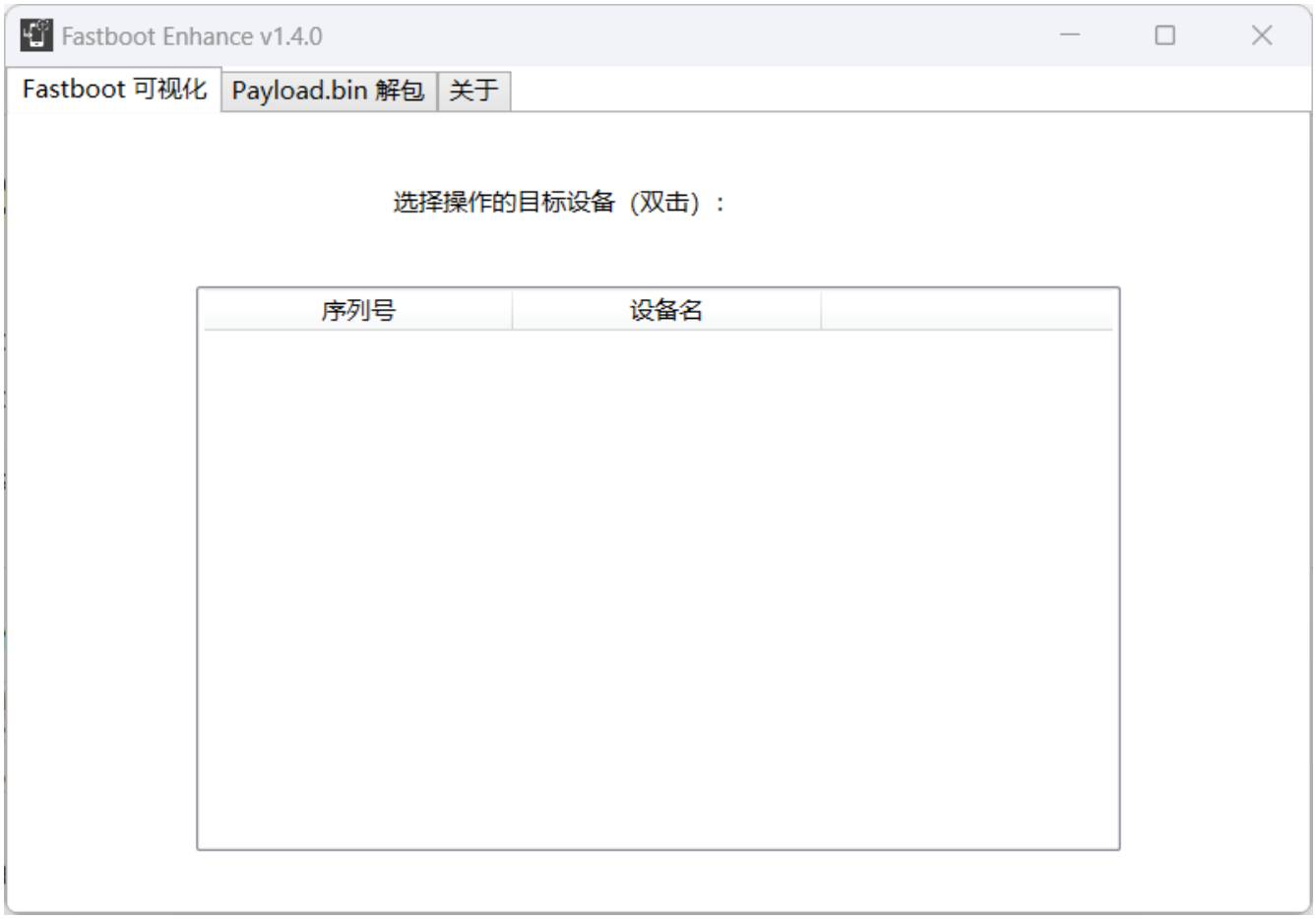
3. 刷 root 卡第二屏（MyOS）超过 15min

system 分区损坏，重刷系统完整包

附录：

附录 1：如何进入 fastbootd 模式？

1. 首先下载 fastboot enhance，github 链接 https://github.com/libxzr/FastbootEnhance/releases，下载里面的 release.zip，打开界面如图



2. 如果你是开机状态，那么执行 adb reboot fastboot，然后 fastboot enhance 将可以看到该设备，



双击后重启到 fastbootd 模式。如果你无法正常开机，那么再次执行大佬的 bat 脚本 unlock_emmc.bat，执行结束后将会自动进入 fastbootd 模式

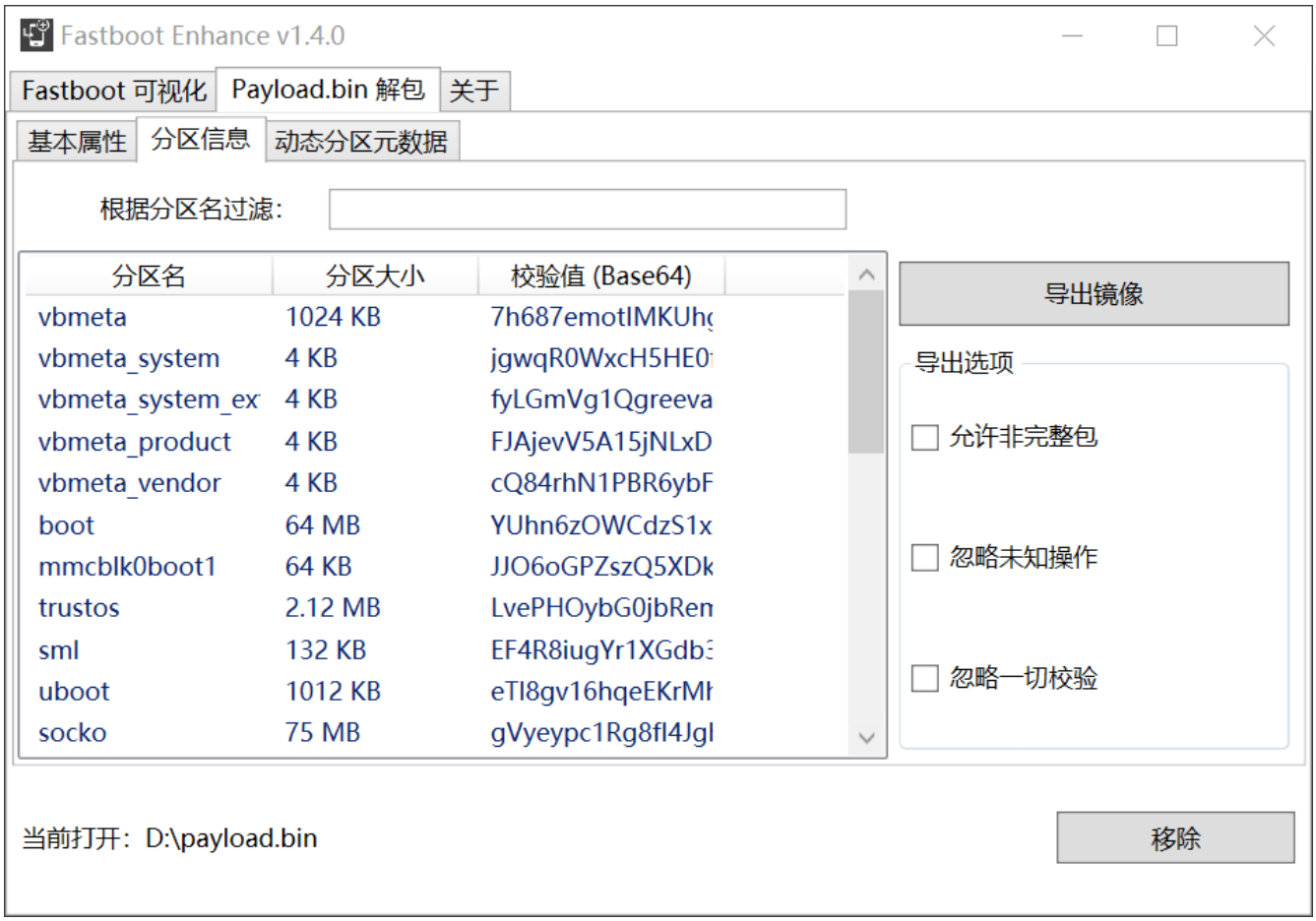
附录 2：如何刷系统完整包（官网 11.5.06 系统）

1. 下载官网 11.5.06 版本的包（如果你的版本号大于 11，说明你是 5g+4g 版本，你需要自己修补 boot ⚠️）下载链接：https://www.ztedevices.com/cn/supports/%e8%bf%9c%e8%88%aa30s/
2. 下载完成之后解压第一层，得到 update.zip, 放置待用
3. 再解压一层，得到 payload.bin，放置待用。
4. 进入 fastbootd 模式（见附录 1），刷写 payload.bin，选择解压出来的 payload.bin 并刷入
5. 从 fastbootd 模式进入 recovery 模式，高级选项里选择 adb 更新系统，然后执行 adb sideload D:\update.zip [这里写你放置 update.zip 的位置]
6. 手机会自动升级，如果升级到 94% 显示升级失败，是正常情况（是个无关紧要的 error），忽略即可。
7. 清除用户数据，重启应该就可以开机了，第一次开机时间较长属于正常情况。

附录 2 中的常见问题：

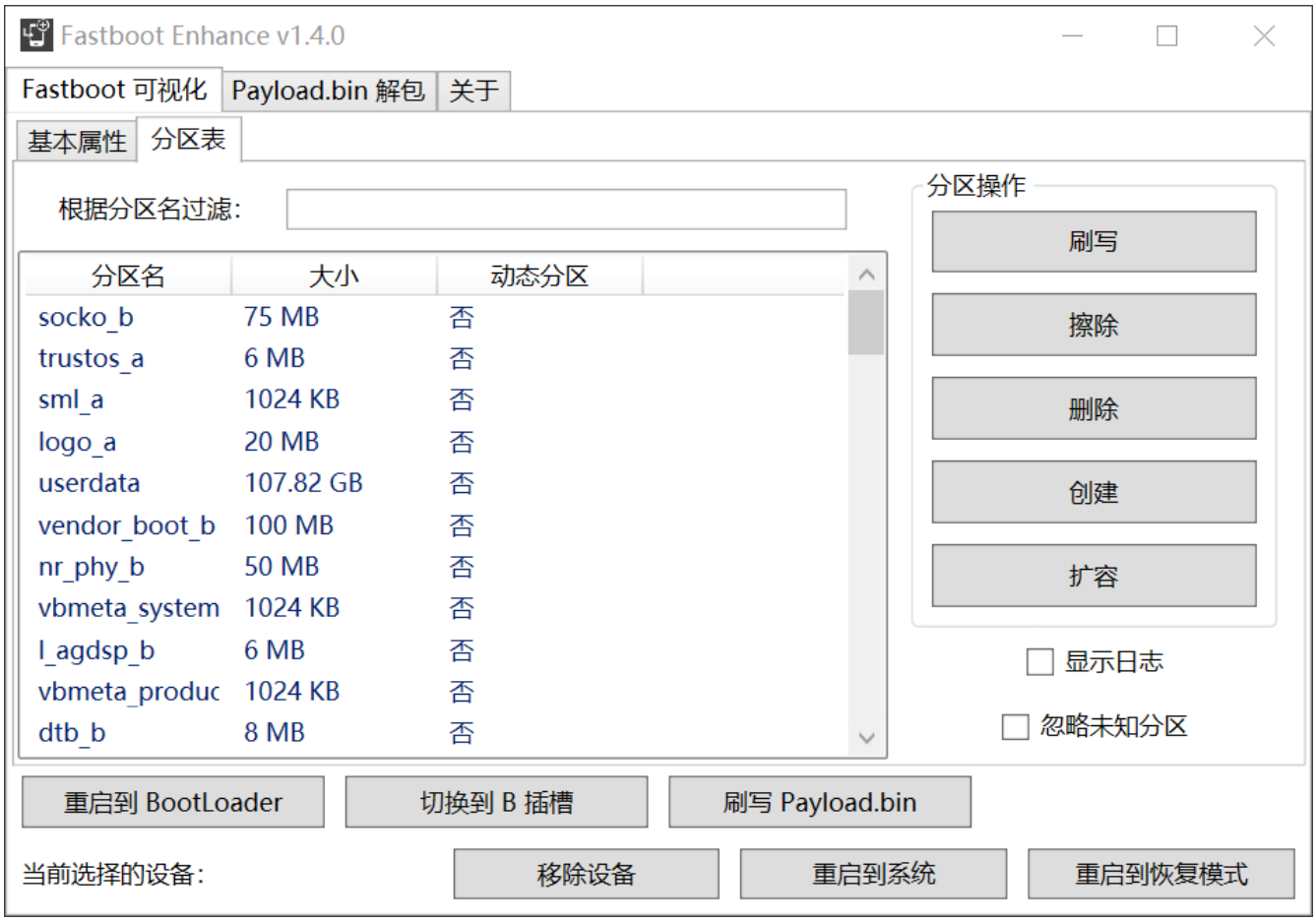
1. recovery 进行 sideload 升级时，升级到 47% 报错

这是因为 recovery 不允许降级，可以通过在 fastbootd 中强刷 boot 解决。重新进入 fastbootd 模式，在 fastboot enhance 中提取 payload.bin 里的 boot.img（下图界面找到 boot 并导出镜像），



用提取的官方 boot.img 刷写你系统槽位所在分区(boot_a/boot_b)。【当然你也可以完整地刷写 payload.bin】基本属性中的当前分区会告诉你系统处于 a 分区还是 b 分区。

在如下图所示的界面中，选中你要刷写的分区 - 分区操作中点击刷写



2. recovery 进行 sideload 升级时，出现其他报错

找到并进入 recovery 升级日志，入口如下图所示



翻到 倒数几页，去看看哪里 error 了。这里仅提供一个问题的解决方法，其他问题请自行根据日志解决

如果是无法挂载系统分区 / 找不到 system 分区。那么进入 fastbootd 模式，删除 system_a,system_b,vendor_a,vendor_b,product_a,product_b,system_ext_a,system_ext_b 分区（有些可能已经没有了，就不管），然后进入 recovery 重新 sideload 刷写 update.zip【不用担心，其会自动重新生成这些系统分区】

3. 在刷写 payload.bin 时，提示 system 等等分区未知

继续在 fastbootd 中输入 payload.bin，然后删除 system_a,system_b,vendor_a,vendor_b,product_a,product_b,system_ext_a,system_ext_b 分区，然后进入 recovery 中重新刷写 update.zip

修补 boot 中的一个细节【多机型通用 tip】：

如何获得镜像的 fingerprint 以及 osversion?

在大佬的教程第四步 https://github.com/TomKing062/CVE-2022-38694_unlock_bootloader/wiki/Magisk#step-4 中，你需要提供如下的正确信息

Plain Text

```
$FINGERPRINT
$OS_VERSION
```

你可以使用 ./avbtool info_image --image vbmeta.img 命令来获取相关的信息，如果 vbmeta.img 中没有相关信息，可以在 vbmeta_system.img 中获取

仅供学习参考，如果有不对的地方，还请各位大佬多多指教！

（中兴远航 41，畅行 50 与小鲜 50 原理上也可以解锁 bl，有兴趣的大佬可以自主参考 https://github.com/TomKing062/CVE-2022-38694_unlock_bootloader/wiki/AddSupportToModel 进行尝试）

（另：大佬的工具已经支持解锁大量展锐设备 bl，有兴趣的朋友可以去大佬的 github 看看点个 star）