

# 目录

前言	1.1
安卓root概览	1.2
安卓模拟器root	1.3
安卓手机root	1.4
root流程	1.4.1
BL解锁	1.4.1.1
fastboot mode	1.4.1.2
root相关工具	1.4.2
TWRP	1.4.2.1
Magisk	1.4.2.2
root相关	1.5
A/B槽位	1.5.1
OPPO R11s	1.5.2
root心得	1.6
附录	1.7
参考资料	1.7.1

# Android逆向：开启root

- 最新版本: v0.6
- 更新时间: 20221030

## 简介

总结安卓逆向期间涉及的给安卓root。先是概览；然后是分别介绍安卓模拟器和安卓真机的root；之后详细介绍安卓真机的root的流程，包括Bootloader解锁、fastboot mode等，和涉及到的工具：TWRP、Magisk等；以及相关知识和设备：A/B槽位、OPPO R11s的root；然后整理root心得。

## 源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

### HonKit源码

- [crifan/android\\_re\\_enable\\_root: Android逆向：开启root](#)

### 如何使用此HonKit源码去生成发布为电子书

详见：[crifan/honkit\\_template: demo how to use crifan honkit template and demo](#)

### 在线浏览

- [Android逆向：开启root book.crifan.org](#)
- [Android逆向：开启root crifan.github.io](#)

### 离线下载阅读

- [Android逆向：开启root PDF](#)
- [Android逆向：开启root ePUB](#)
- [Android逆向：开启root Mobi](#)

## 版权和用途说明

此电子书教程的全部内容，如无特别说明，均为本人原创。其中部分内容参考自网络，均已备注了出处。如发现有侵权，请通过邮箱联系我 admin 艾特 crifan.com，我会尽快删除。谢谢合作。

各种技术类教程，仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途，均与本人无关。

## 鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 crifan 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

## 更多其他电子书

本人 crifan 还写了其他 150+ 本电子书教程，感兴趣可移步至：

[crifan/crifan\\_ebook\\_readme: Crifan的电子书的使用说明](#)

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2022-10-30 18:03:22

# 安卓root概览

[Android逆向](#)期间，往往前提是需要：一个root的安卓手机。

就会涉及到，如何给安卓手机root。

此处介绍Android的root的相关内容。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2022-10-30 17:19:45

## 安卓模拟器root

Android逆向期间，如果要逆向的app，可以在安卓模拟器中正常安装和运行，那么，其实使用模拟器去折腾，也是一个比较好的选择，因为：

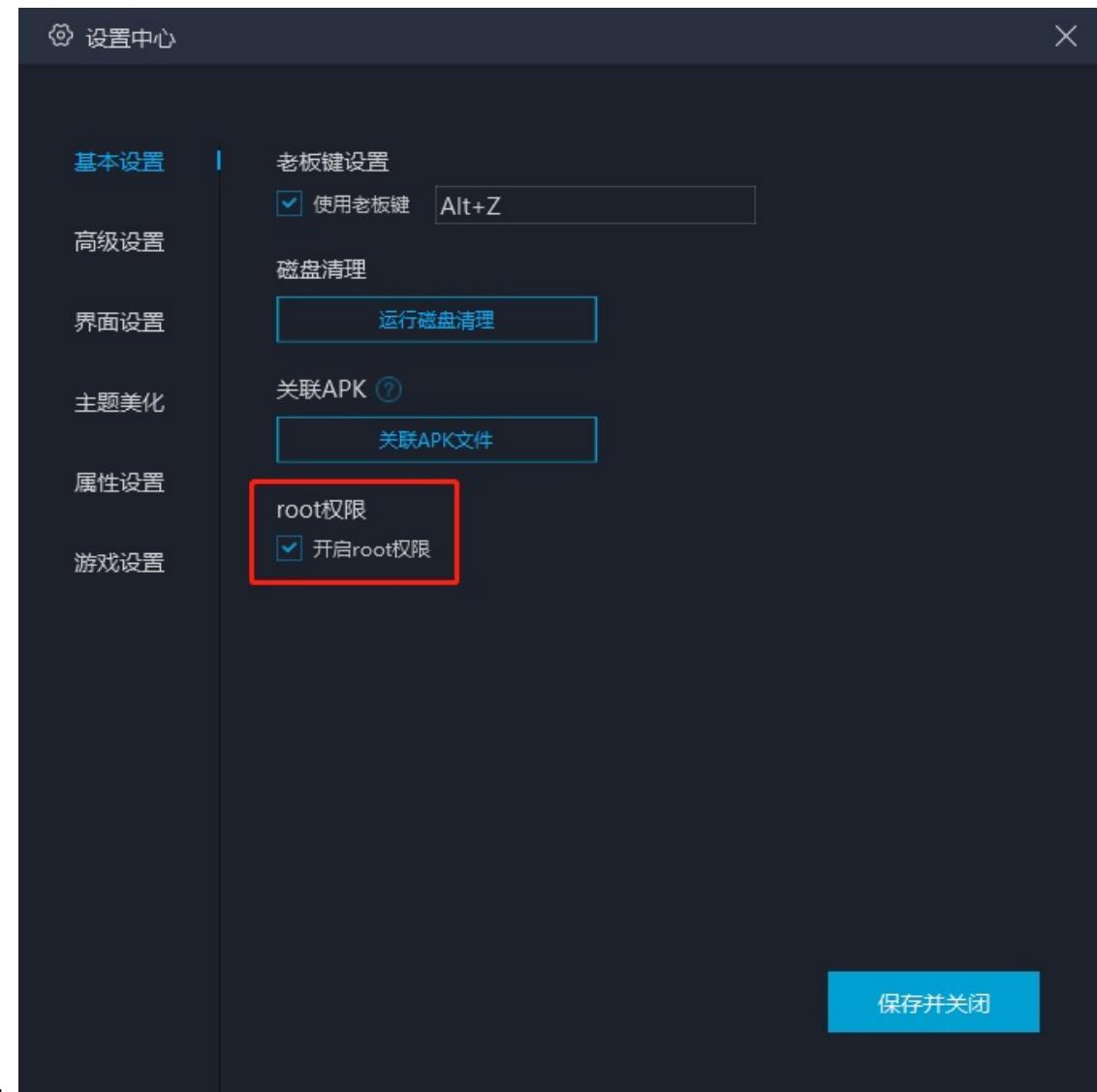
安卓的root权限，对于多数安卓模拟器来说，都能很方便的支持，毕竟基本上就是一个参数的开启的事情。

目前已知的，相对还算好用的安卓模拟器，且支持root的有：

- [夜神Nox](#)

◦

- 网易Mumu
  - <https://mumu.163.com/>



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook 最后更新: 2022-10-30 17:35:42

# 安卓手机root

给安卓手机=安卓真机，去root：

- 早期：是个简单的事情
- 现在：往往，是个复杂、麻烦的事情

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook 最后更新：2022-10-30 17:36:56

## root流程

TODO:

- 【已解决】给Android 11的Google Pixel3去开启root权限
  - 【未解决】如何给OPPO R11s开通root权限
  - 【记录】root安卓手机OPPO R11s的root环境初始化
-

## BL解锁

TODO:

- 【未解决】如何给OPPO R11s去Bootloader解锁
- 

- BL解锁 = Bootloader解锁

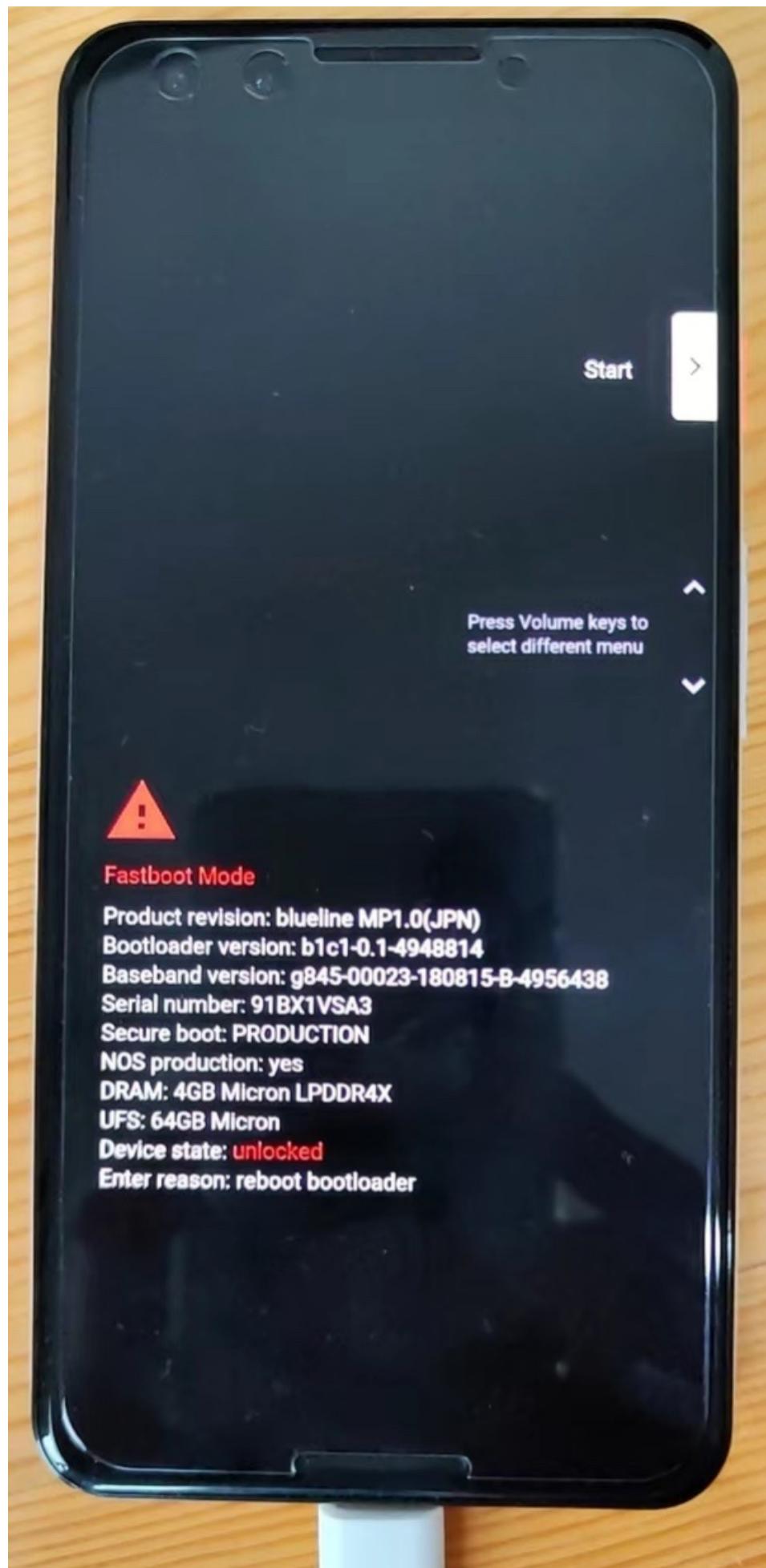
crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-10-30 17:56:34

## fastboot mode

TODO:

- 【已解决】安卓手机什么是fastboot mode
  - 【未解决】Android 8.1的OPPO R11s无法进入bootloader的fastboot mode
- 

- fastboot mode
  - = 刷机模式 = bootloader mode = download mode = 下载模式
  - 长什么样
    - Google Pixel 3
    -





## root工具

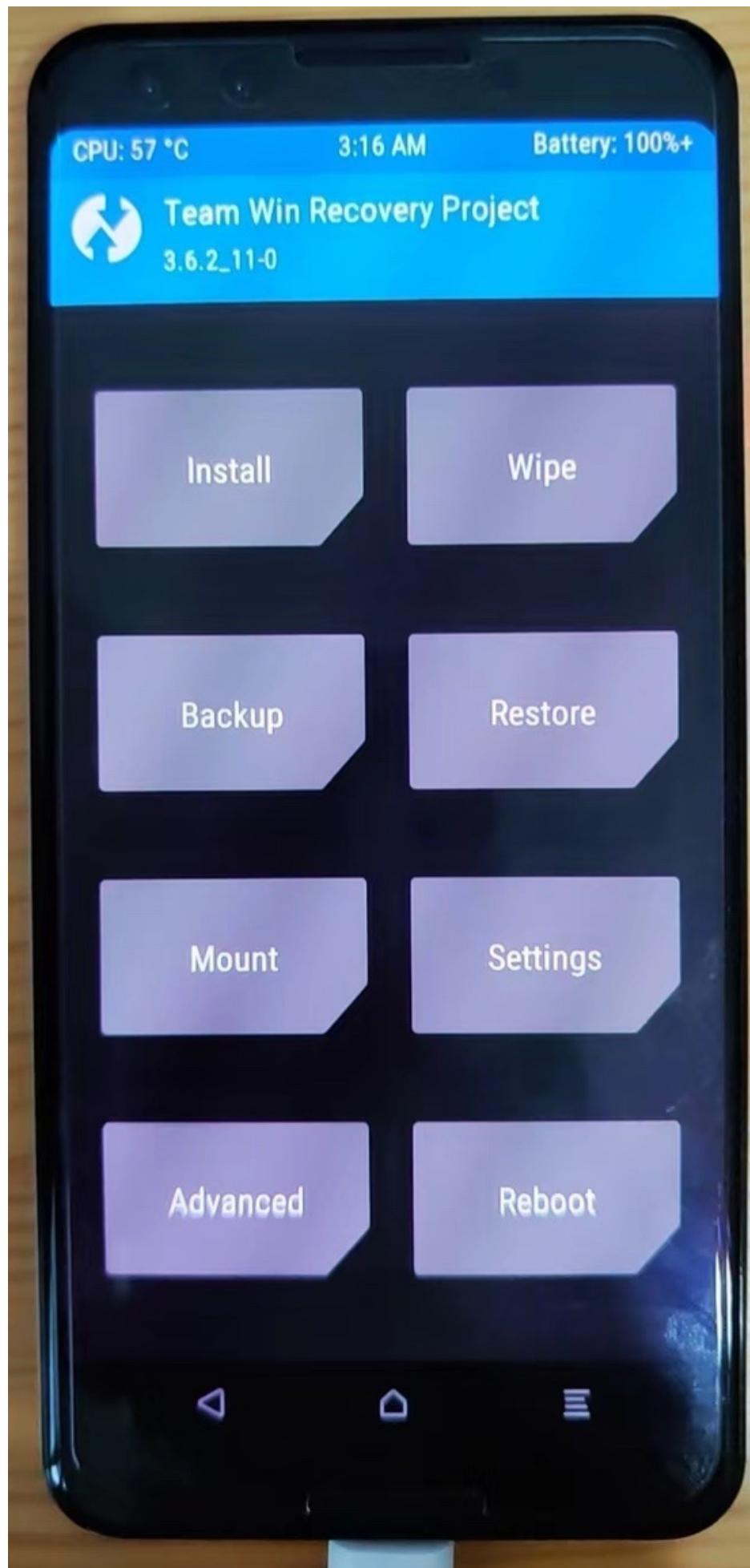
crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-10-30 15:40:12

## TWRP

TODO:

- 【已解决】给Android 11的Google Pixel3去刷第三方Recovery: TWRP
  - 【已解决】Google Pixel3如何进入TWRP
  - 【记录】Google Pixel3中的TWRP界面和功能
  - 【未解决】给OPPO R11s开启root权限: 用TWRP的Recovery刷Magisk
  - 【未解决】给OPPO R11s刷第三方Recovery: TWRP
  - 【记录】OPPO R11s重启后进入奇兔刷机Recovery模式TWRP
- 

- TWRP
  -





# Magisk

TODO:

- 【未解决】给OPPO R11s开启root权限：用非TWRP的Recovery模式安装刷入Magisk
  - 【总结】Magisk Manager使用心得：root超级用户权限管理
  - 【整理】安卓root工具：Magisk
  - 【已解决】OPPO R11s中安装Magisk并给boot.img打补丁
  - 【已解决】Magisk中安装中去Patch启动镜像boot.img
  - 【记录】已root的Google Pixel3中的Magisk相关信息
  - 【记录】OPPO R11s中Magisk Manager初始化和配置参数
  - 【记录】root安卓手机OPPO R11s中升级Magisk Manager
  - 【已解决】OPPO R11s中Magisk Manager升级后提示：不支持的Magisk版本
  - 【整理】Google Pixel3中的Magisk Manager使用心得
  - 【记录】手动下载和升级Magisk到最新版本
  - 【记录】Magisk Manager版本升级
  - 【未解决】Magisk Manager模块从本地安装无法识别选择apk文件
- 

- Magisk
  - 新版： v21

11:49 G P 34%

# 主页

仅从官方 GitHub 页面下载 Magisk。未知来源的文件可能具有恶意行为！[不再显示](#)

 **Magisk**  [更新](#)

当前 **21.0 (21000)** A/B 是  
Ramdisk 是 SAR 是

 **App**  [更新](#)

最新 **25.2 (25200) (33)**  
当前 **23.0 (23000)**  
包名 **com.topjohnwu.magisk**

 [测试 SafetyNet 证明](#)

 [卸载 Magisk](#)

## 支持开发

Magisk 将一直保持免费且开源，向开发者捐赠以表示支持。

@topjohnwu

@diareuse <  > 

- 最新版： v25

■

5:12 ① G ⚡ 🔋

主页 

 **Magisk**  安装

当前 无法获取  
Zygisk 否  
Ramdisk 是

 **App**  安装

最新 25.2 (25200) (33)  
当前 25.2 (25200)  
包名 com.topjohnwu.magisk

## 支持开发

Magisk 将一直保持免费且开源，向开发者捐赠以表示支持。

## 关注我们

@topjohnwu  

@vvb2060  

 **主页**  **超级用户**  **日志**  **模块**

<  >



## 新版Magisk中没有模块的在线搜索了

TODO:

- 【未解决】新版Magisk中没有在线搜索安装模块了

## Zygisk

TODO:

- 【已解决】Magisk中的：Zygisk

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2022-10-30 17:52:39

## root相关

TODO:

- 【未解决】安卓逆向：尝试用adbd-insecure给adb的shell增加root权限
  - 【已解决】安卓设备Google Pixel3中获取root权限使得su不报错Permission denied
  - 【记录】adb没有root权限就无法正常工作的相关现象
  - 【已解决】adb root报错：adbd cannot run as root in production builds
  - 【未解决】adb shell中root和su都没有权限修改Download目录下的apk文件的权限属性
  - 【未解决】root的安卓手机Google Pixel3不稳定
- 

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-10-30 17:18:30

## A/B槽位

TODO:

- 【已解决】Magisk版本升级选项：安装到未使用的槽位（OTA后）

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2022-10-30 17:16:24

## OPPO R11s

TODO:

- 【未解决】用EDL模式和高通芯片烧录工具去烧录OPPO R11s的ROM
  - 【已解决】安卓手机EDL模式
  - 【未解决】用Windows电脑试试奇兔刷机能否给OPPO R11s解锁或刷入TWRP的Recovery
  - 【记录】OPPO R11s重启后进入了ColorOS自带Recovery模式
  - 【未解决】寻找可用的免授权的OPPO R11s的下载烧录工具
- 

## OPPO R11s的ROM

TODO:

- 【已解决】从OPPO R11s的ozip导出的zip中提取boot.img文件

## OPPO R11s的root

像 OPPO R11s，如果不小心，重新安装了官方的rom，则就丢失了 Bootloader 的解锁

-» 就没法重新刷TWRP等第三方工具了，就没法正常继续root了

-» 只能想办法再去重新解锁：

要么寄回卖家重新帮你解锁

要自己弄：就涉及到手机中的芯片，比如高通的，相关刷机工具。

主要是烧录数据到Flash中的相关一套工具

而这些工具往往是需要签名授权验证的才能用的

一般不太容易找到免费的下载，而可能要找别人网上解锁，是要收费的

自己之前找了相关工具，但是后来还没精力继续尝试，所以暂时不确定：网上是否能找到，完全的免费的高通的刷固件的工具。

另外，期间涉到的OPPO的官网ROM，倒是可以找到免费的。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2022-10-30 17:54:06

## root心得

关于安卓的root心得：

- 安卓root
  - 安卓模拟器：一般都很简单
    - 一般的模拟器都支持直接开启root
  - 安卓手机
    - 很早之前：很容易
      - 尤其是 Android < 4.0的时代
      - 随便去买个手机，都能用普通的root工具（root精灵、一键root等）成功root
    - 后来：不容易
      - 多数手机想要解锁，都要官网申请，通过后，才能继续root，否则无法root
      - 比如：小米的
    - 现在：也不容易
      - 一般的手机，都不给root，也是要申请root才可以
      - 但是好像据说有些手机，已经被破解了，淘宝上可以花钱找人在线root
        - 猜测：估计就是在线解锁BL，然后继续root的？

## 结论

- 现在如何root
  - 如果本身要破解的安卓app，能正常安装和运行在安卓模拟器：那么可以考虑用安卓模拟器，比如网易的mumu、夜神Nox等
  - 如果只能用真机：
    - 去淘宝上买个别人root好的二手安卓手机
    - 或者：自己买新的安卓手机，自己想办法搞定 BL解锁，然后再 root

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2022-10-30 17:41:50

## 附录

下面列出相关参考资料。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-10-30 15:33:31

## 参考资料

- [打开“共享文件夹”提示没有ROOT权限MuMu模拟器安卓模拟器](#)
- [Root开关功能\\_夜神安卓模拟器新手帮助页](#)
- 

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-10-30 17:27:00