**[[教程福利]](https://www.52pojie.cn/forum.php?mod=forumdisplay&fid=66&filter=typeid&typeid=346) 红米K40实操提取boot获得面具root权限超细教程+工具（教程适用一切安卓11手机）**

***红米K40出厂安卓11系统，目前没有REC。那么想要ROOT权限怎么办呢。下面我来详细解说其中一种方法***

***教程方法理论上适用所有安卓11手机，***

***必须有电脑，必须要电脑***

***首先解BL锁是前提，（目前任何手机需要ROOT都是需要解BL吧）***

***然后需要下载一个完整的卡刷包，手机目前处于什么版本就下什么版本的完整包（任意版本都是一样的操作方法），小米直接在miui版本右上角点击下载最新完整包即可***

***然后就是电脑下载python-3.9.2-amd64，也可自己百度下（64位毒盘链接：[https://pan.baidu.com/s/1ARNFU5rXB82sAEjmwo2aYw](https://pan.baidu.com/s/1ARNFU5rXB82sAEjmwo2aYw%22%20%5Ct%20%22_blank) 提取码：8880  ）下完安装，这是运行环境而已。***

***然后下载payload\_dumper-win64（毒盘链接：[https://pan.baidu.com/s/1aIX\_hQUpCIgsIFaqgDAtog](https://pan.baidu.com/s/1aIX_hQUpCIgsIFaqgDAtog%22%20%5Ct%20%22_blank) 提取码：8880 ）下好解压到桌面就行***

**---------------------------------------------------------------------------------**

**准备开整**

**1.将卡刷包传到电脑解压好得到payload.bin**



**2.将这个bin拷贝到这个目录下**



**3.打开payload运行程序**



**4.打开出来一个窗口自动解包等待完成（速度看电脑配置，可以不用等待全部完成。不懂的就等完成后再操作）**



**5.完成后打开这个目录解出来得所有文件都在这里了**



**6.将解出来boot文件传到手机内存**



**7.手机下载最新版得面具打开**



**8.选择刚才放进来得boot文件，点开始修补**



**9.修补好的boot文件会被重新命名并显示目录**



**10.打开手机看到boot文件**



**10.（①下载adb工具并解压好。有的可以忽略这一步毒盘链接：[https://pan.baidu.com/s/16jrAFmJqf0At51usVbRyKA](https://pan.baidu.com/s/16jrAFmJqf0At51usVbRyKA%22%20%5Ct%20%22_blank) 提取码：8880 ）**

**11.将这个修补好的boot文件改名再传到电脑上并放到这个目录（adb目录里面）**



**12.打开adb-cmd输入fastboot flash boot boot.img回车会自动弹出另一个窗口（注意有空格，建议直接复制）**



**13.新窗口会提示连接手机，手机开机进入fastboot模式并且链接电脑，识别到手机后自动刷入并窗口自动消失**



**14.回到这个窗口输入fastboot reboot回车来重启手机（注意空格，建议直接复制）**



**开机后打开面具已经有root权限了**

 

***现在的手机基本都是安卓11了，分区也是所谓的AB分区了，暂时没REC的！***

***教程理论是适用所有一切安卓11的已解BL想要获取ROOT权限的手机***