高通进9008的方法大全

高通的9008其实有其专有名称，叫做EmergencyDownloadMode(**EDL**)，这个模式是真正的紧急下载模式，也就是什么都启动不了的情况，还有另外一种伪9008，在某些情况下也会表现为9006端口，这种情况其实是sbl1成功启动，但是加载lk(appsboot)失败，一般手机会进入Dload模式，也就是所谓的**磁盘模式**，表现为手机连接电脑会出现一个看得到手机完整分区内容的硬盘设备。

另外说一下高通的刷机协议，高通的刷机工具主要就是QPST套件，这个套件是跟着高通从最早高通进入移动处理器市场到现在高通成为处理器霸主的整个过程的，我们可以根据QPST看到高通刷机协议的变化。

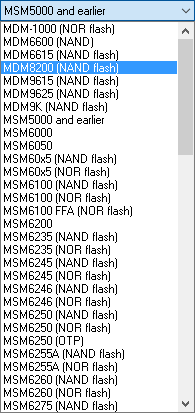
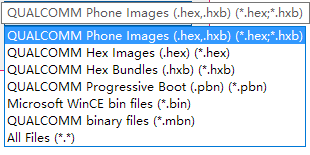


QPST Server

1. 远古时期：SoftwareDownload.exe

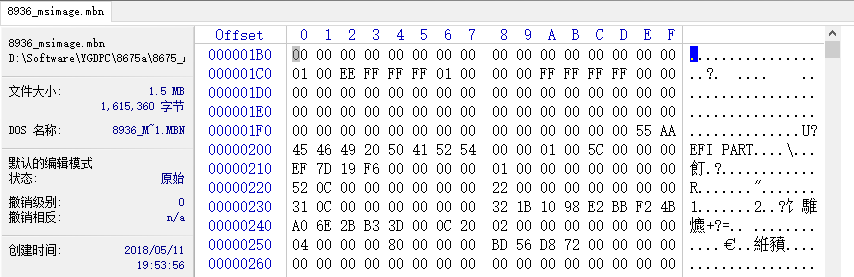


这个是最早期的高通刷机工具，尽管我是没有机会用这个工具刷过机，不过应该伴随了高通很长一段时间。这里我们可以看到，高通在相当早期的一些产品，并且很早开始高通就支持mbn作为二进制可执行文件后缀了，所以我们现在刷机包里都是mbn格式的文件也不奇怪了。现在这个工具的唯一作用就是你用来备份和还原NV数据了，使用频率其实还是挺高的。

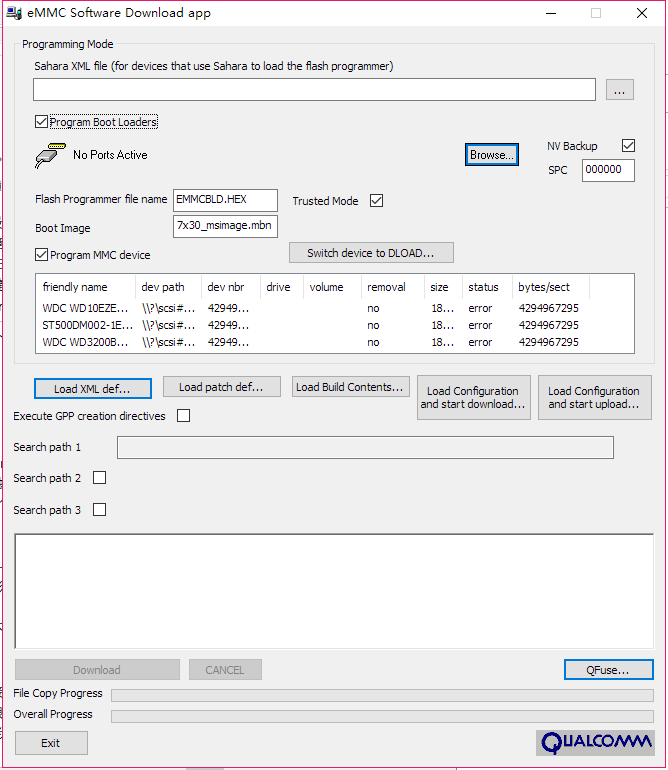


1. 第二代刷机工具：emmc\_download.exe，最新版里面叫做emmcswdownload.exe

这个是笔者用的第一个高通刷机工具，从名字上我们可以看出这个和上代工具的区别来，这时候emmc开始流行，使用nand/nor flash的手机开始被逐步淘汰，高通也跟进了一个新的刷机工具版本。这个工具所使用的是一种称作Sahara的刷机协议，是高通设计实现的，Sahara刷机协议一个比较突出的特点就是刷机的时候先用一个MPRG<platform\_code>.hex和一个<platform\_code>\_msimage.mbn文件，前者应该是一个配置文件，用来初始化早期协议将后者写入到emmc中，然后我们使用十六进制工具打开<platform\_code>\_msimage.mbn，可以发现其头部拥有一个GPT分区表。



这里进一步分析会发现其实这就是一个磁盘镜像文件，内部有手机最小系统+Flash+USB系统启动的必须分区文件，sbl1,rpm,tz,DDR，当我们将这个镜像成功刷入emmc之后，手机就可以开机进入最小磁盘系统，然后我们就有了在电脑上直接操纵手机磁盘的权限，然后高通还准备了一套专门用于向手机磁盘一键式写入分区的脚本，也就是我们经常见到的rawprogram<N>.xml和patch<N>.xml了，有这个脚本烧写程序才知道该把哪个分区对应写入到磁盘的哪个区域，哪个文件该怎样打补丁，还是挺高级的，不愧是大公司的作品。



1. Sahara协议之后
2. 手机故障自动进9008

这种情况一般是开机自检没有通过，可能的原因有sbl1加载失败，pmic/rpm/tz初始化失败，或者是其他硬件故障比如字库爆了，读取不了以上任何分区，就会触发主板固化代码进9008。我们可以利用的地方在于我们可以用某种手段擦除掉上述某个分区，也就可以达到进9008的目的。

1. 通过主板测试点GPIO下拉进9008,

这种方法代价有点大，因为需要拆开手机，在现在一体机with卡扣+黑胶+无螺丝设计组合越来越流行的今天，代价更不是一般的大，拆机一般无法完美复原，影响使用体验。

需要的话，需要拆开手机，在主板上找测试点一个一个接到电源地试试能不能触发9008模式，可以的话就好，不行就凉。

1. 工程线方法

这种方法的适用度比较低，因为这个入口是高通在sb1中设计的Debug接口，当检测到数据线的data+接地时，系统自动进入9008模式，如果厂商对刷机权限限制比较死的话，一般不会开放这个接口，目前已知有这个接口的机型就是小米多数老机型和酷派的一些老机型，像索尼、LG、HTC这种国际大厂一般是锁死了的。

1. 厂商预留的组合键进9008

这个也限于厂商开放度比较高才有效，比如努比亚、乐视的部分机型是可以通过音量加减+开机键直接进入Dload模式的。

1. 通过reboot命令进入edl

这里有几个不同的分支方法

1. reboot edl
2. reboot dload
3. adb reboot edl
4. adb reboot dload
5. fastboot reboot emergency

最后这个需要使用新版的fastboot工具，建议从Android sdk中获取。

1. fastboot oem edl
2. fastboot oem dload

6、其他玄学方法【本人暂时还没发现其他方法】