**Amlogic新设备制作u-boot和dtb操作说明**

文档整理自flippy大佬（https://github.com/unifreq）网络指导制作uboot的教程。

如果想更好破解Amlogic电视盒子固件的话，需要先分析原厂安卓系统的uboot和dtb，以及分区布局。

# 第一步、获取安卓固件分区布局

要用adb（下载地址：https://github.com/ophub/kernel/releases/download/tools/adb.tar.gz）连到安卓固件里查看，主要是关心哪些区域是安全的，哪些是要保留的。当然如果能生成可用的主线uboot的话就不存在这个问题了。

最大的3个分区：cache,system,data一般是安全的。

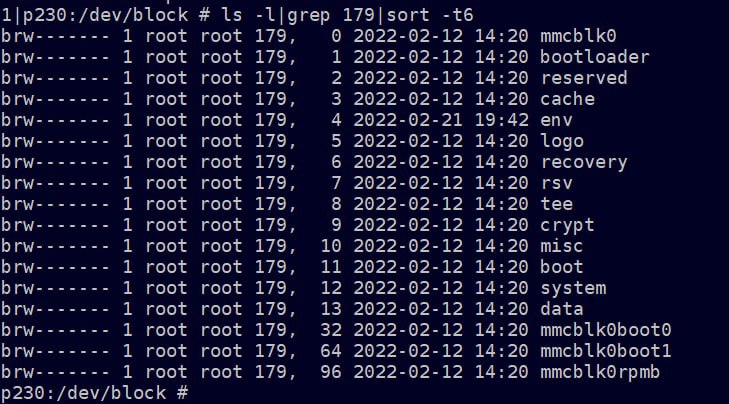
adb connect 192.168.1.111

adb shell

先查看分区情况：

cd /dev/block

ls -l|grep 179|sort -t6



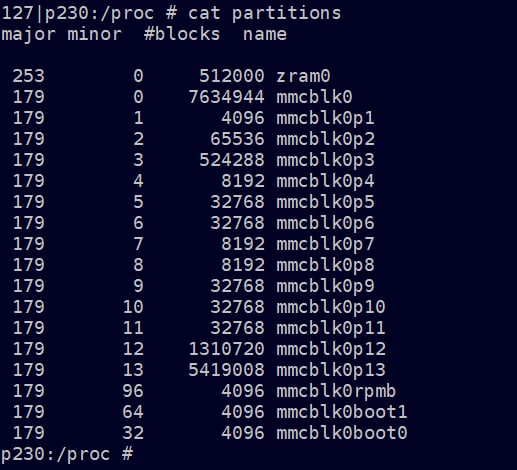
再查看其他几个位置的情况：

cat /proc/partitions > /data/local/1.txt

cat /proc/ntd > /data/local/2.txt

cat /proc/partitons /data/local/3.txt

再结合 ls -l /dev/block > /data/local/4.txt

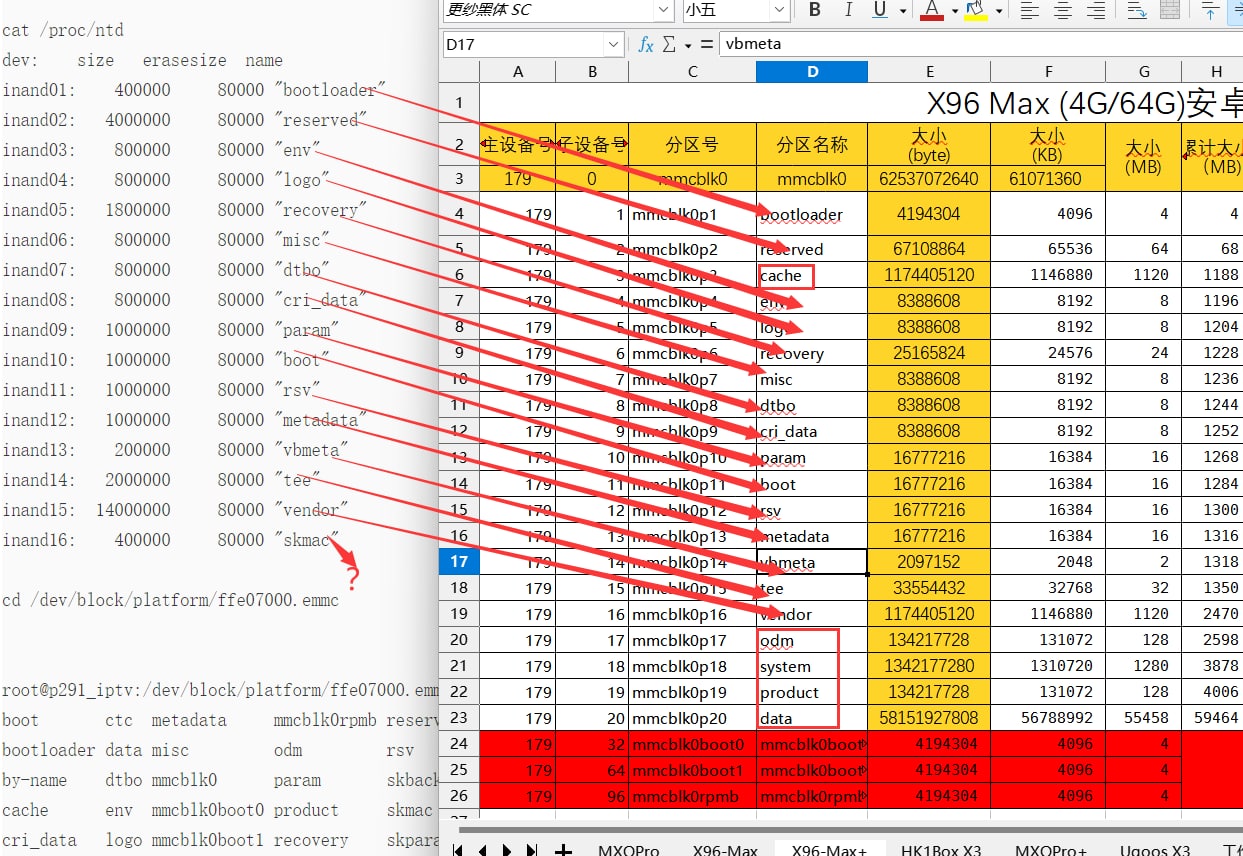


生成上面的几个文件后，在本地window电脑的C盘根目录下创建a文件夹，重新cmd链接adb connect 192.168.1.111 下载文件。

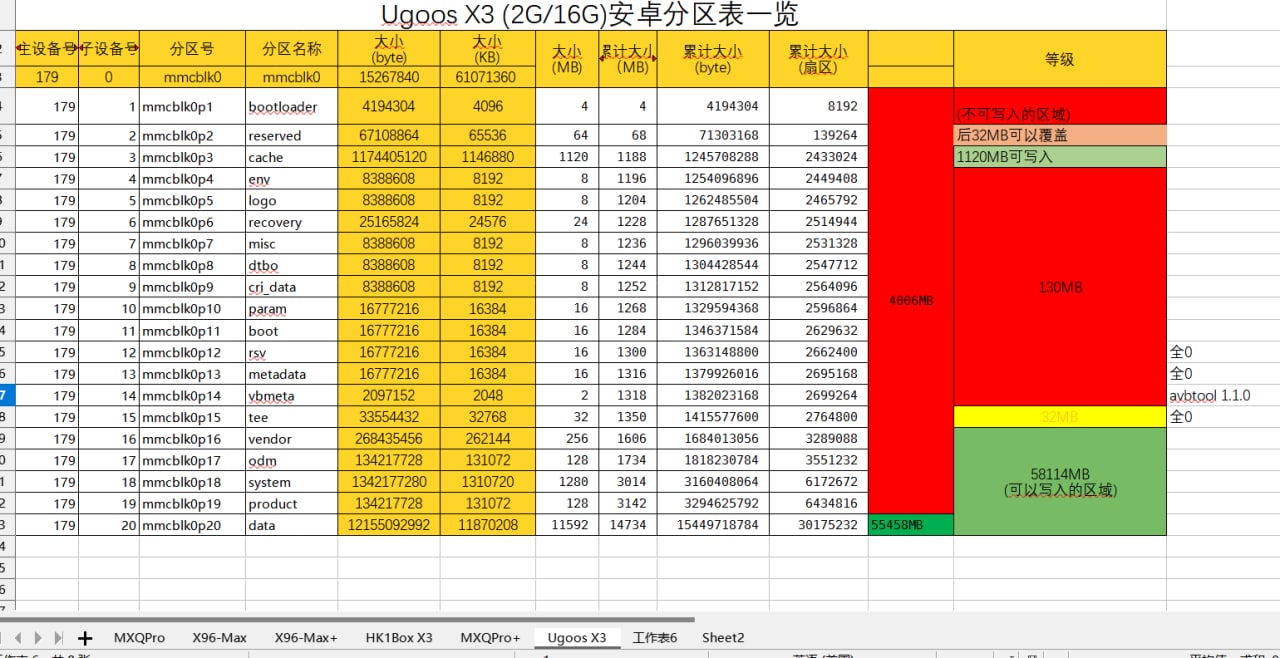
adb pull /data/local/1.txt C:\a

依次下载1234几个文件文件

打开excel，参照现在的模板把得到的几个文件的数据套进去



最后得到一张分区布局表：



# 第二步、提取bootloader和dtb文件

导出dtb命令：

cat /dev/dtb >/data/local/mybox.dtb

导出bootloader命令：

dd if=/dev/block/bootloader of=/data/local/bootloader.bin

导出gpio命令：

cat /sys/kernel/debug/gpio >/data/local/mybox\_gpio.txt

导出的三个文件下载到本地电脑：

adb pull /data/local/mybox.dtb C:\a

依次把dtb、bootloader和gpio的几个文件都下载到本地电脑。

# 第三步、生成acs.bin文件

原厂uboot需要固件最前面4MB

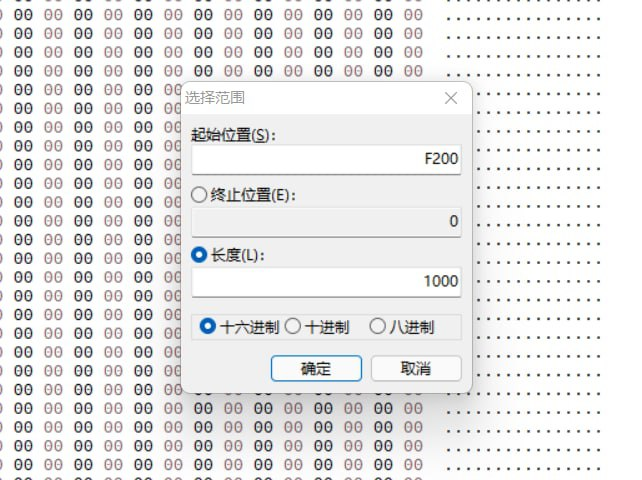
原厂dtb也可以从原厂固件中提取，但有些机型锁过bl的话就提不出来。需要反编译成dtc，再和主线的dts去做对比分析。

如果有主线uboot，4MB后面全都可以使用，如果用原厂uboot的话就要跳过不安全的区域。主线uboot最重要的是acs.bin，用于初始化内存的部分，在uboot的某个位置，要提取出来。

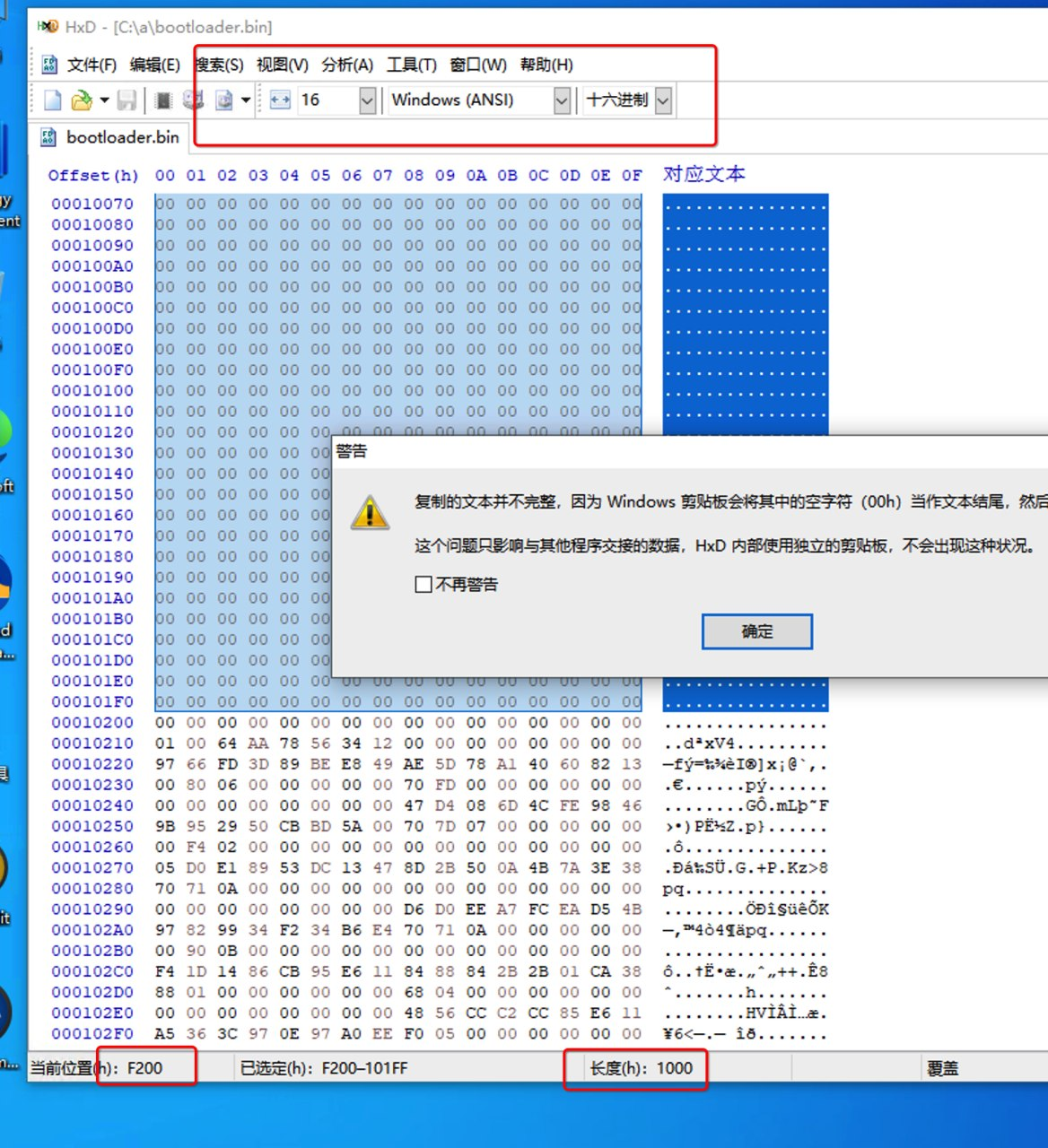
提取acs.bin工具是HxD软件 （下载地址：https://mh-nexus.de/en/downloads.php?product=HxD20）



打开HxD软件，打开上面导出的bootloader文件，右键-选择范围，起始位置F200,长度1000，选十六进制



复制选择的结果，然后新建文件，插入式粘贴，警告忽略，另存为acs.bin



如果是锁了bootloader的话这个区域的代码是是乱码就没用了，上图中很多0这种正常代码就是可以使用的。这个acs.bin在编译主线内核时用。

把这些得到的文件都一起打包发上来：包含bootloader、acs.bin、mybox.dtb、excel，以及过程中的几个导出文件。