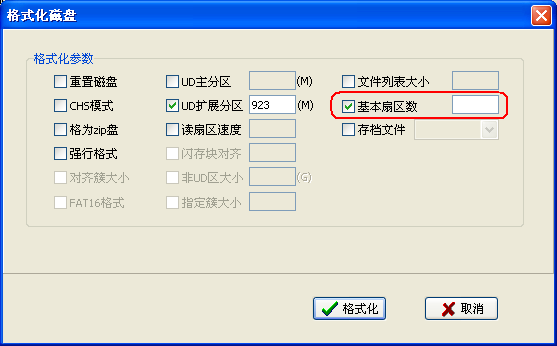
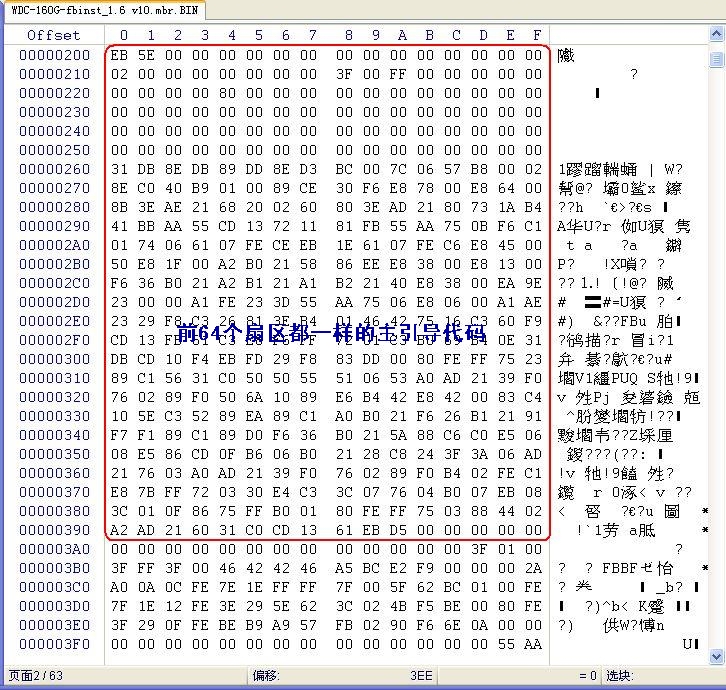
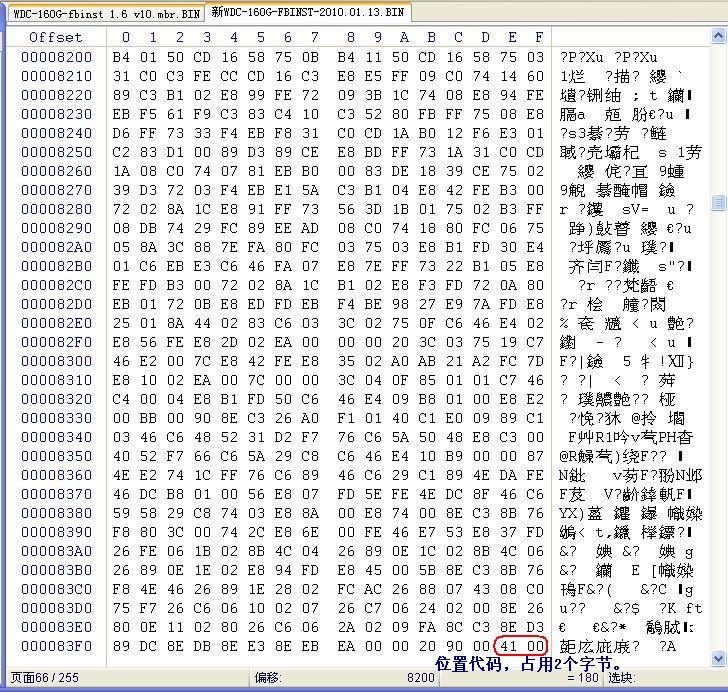
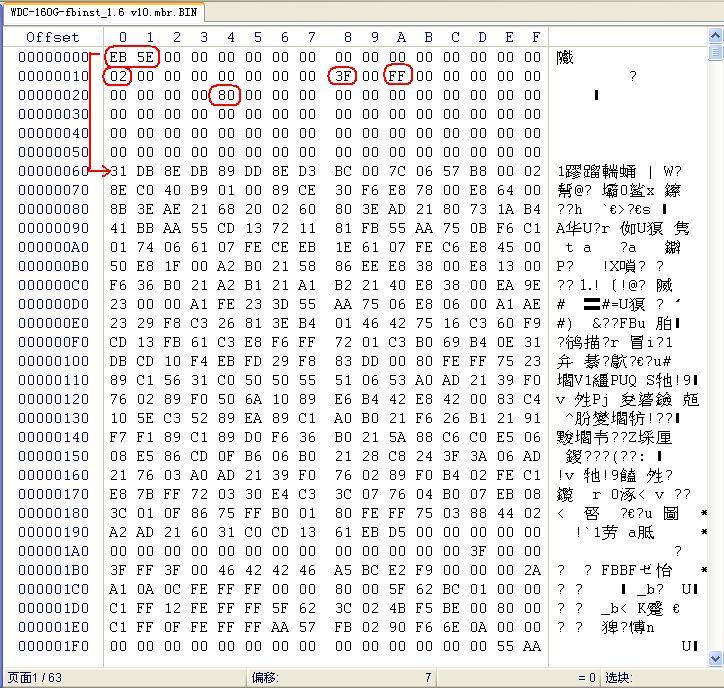
fbinst启动U盘解读（MBR层面）

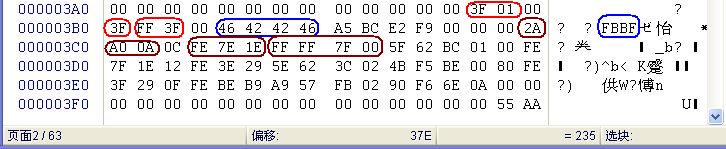
**一、使用简介**  
我们知道：  
由于种种复杂原因，不同BIOS对U盘CHS/LBA参数处理结果不尽相同，导致同一个U盘，在一台机器上BOOT成功，在另一台机器上就可能BOOT失败。   
  
【早期硬盘也有类似问题，但最后通过多个工业标准，已经解决。而USB是万能接口，且有关标准未得到厂商统一遵守，问题更复杂】  
  
现在开源社区的bean提出了巧妙构思，开发出fbinst，基本解决了BIOS下的CHS/LBA参数适应调整问题，使U盘BOOT成功率大大提高。(除非碰上了极度变态的主板和BIOS)。   
——fbinst的巧妙构思  
预留8M(1-16064扇区)隐藏区，在每个扇区固定位置都写入该扇区在WIN下的LBA值，并在1-63扇区都写入boot code。BIOS启动时，通过boot code读取预先写入的LBA值，并与BIOS识别的LBA值进行比较，找出差距，倒推出当前BIOS对U盘的识别和访问情况，根据这个情况来调整纠正对U盘的访问。   
——fbinst隐藏区空闲空间的利用  
fbinst对付BOOT兼容性问题的开发已经完成，目前新版本的开发重点已转向隐藏区的利用。由于8M隐藏区的每个扇区记录LBA时只用了几个字节，且boot code占据空间也不是很大，所以大量扇区空间是空闲的。在这个区域里可以嵌入：   
  
1。不同版本的grub4dos   
  
2。grub2   
  
3。ntldr   
  
4。1.44M/2.88M启动盘映像   
  
5。微型Linux   
  
现在的 fbinst 版本已经可以支持大的隐藏区了，可以装入WinPE或其他DOS工具，用grldr加载引导之。下面有详细说明。  
  
**二、MBR结构解析：**  
【1】主引导代码：  
**1.高明之一：**几乎所有写入U盘的其他类主引导记录的都是占用一个扇区（占用0号扇区，如 HDD+,ZIP+，NT5,NT6 等等），而 fbinst 却是在前64个扇区的主引导代码都一样(稍微差异下面解释)，BIOS在启动时只是读出一个扇区，但是它可能不是u盘的0扇区，因此引导代码要占多个扇区。以前的测试证明，63个就基本够了，最大只需要255。  
不过我的一个U盘启动电脑时，基本扇区数设置为20000才成功启动，否则跳过U盘直接启动本机系统了。  
  


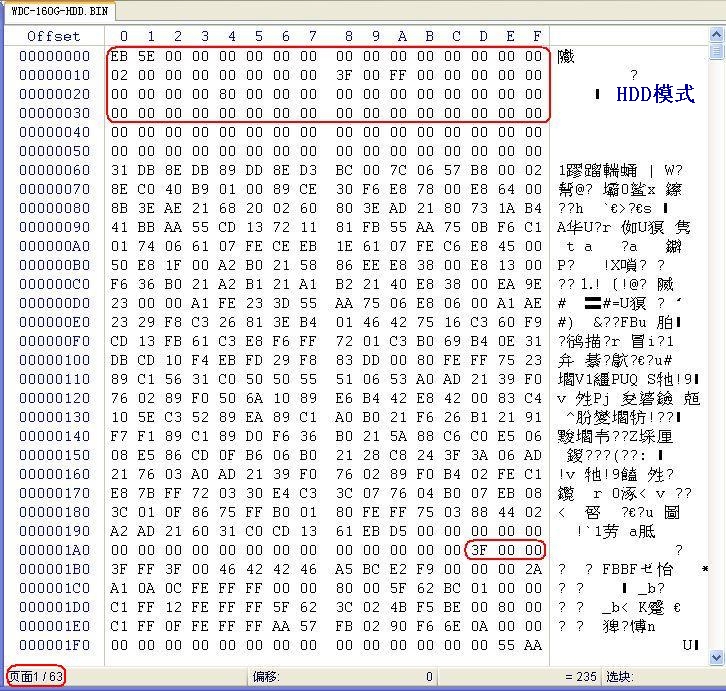
**2.高明之二：**c、h、s（磁头、柱面、扇区）的检测需要更多的空间，至少需要一个柱面（约8M），在主数据区的每个扇区尾部都有该扇区位置代码（占用2个字节），BIOS一读便知此位置。除了位置代码外的其他部分空间就浪费了，因此才把它作为主数据区,从fbinst 1.6版开始最大30M，其间文件不连续（因为每个扇区尾部的绝对扇区地址占用2个字节）。其后再增加的存储启动和维护文件的空间称为扩展数据区，无尾部的绝对扇区地址，其间文件连续。  
最小的主数据区必须包含64个主引导代码和fbinst菜单和文件列表。（但是需手动修改）  
如下图：  
  
  


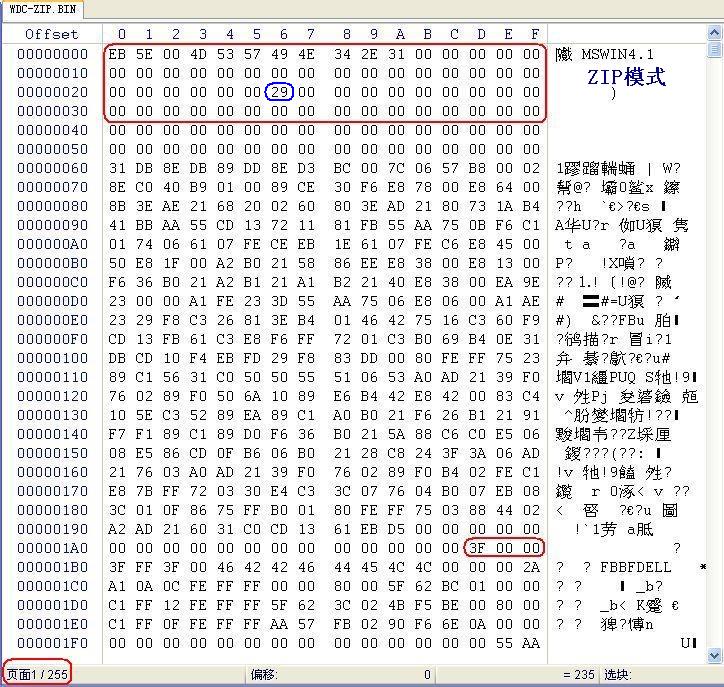


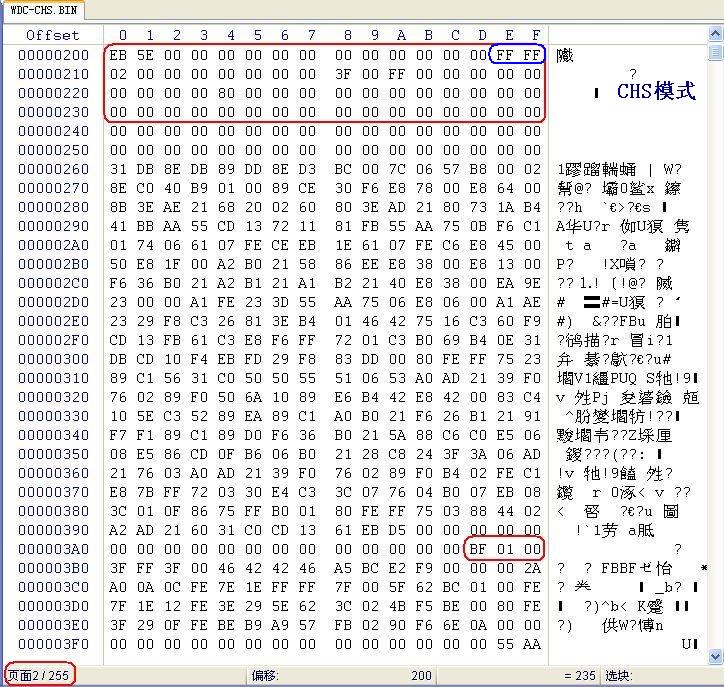
【2】MBR细解，如图示：  
下图中是HDD模式的MBR，偏移00处是跳转指令，EB5E及跳转至偏移0x60处执行，偏移18处表示每磁道扇区数为63（3F），偏移1A处表示磁头数255（FF）  
  


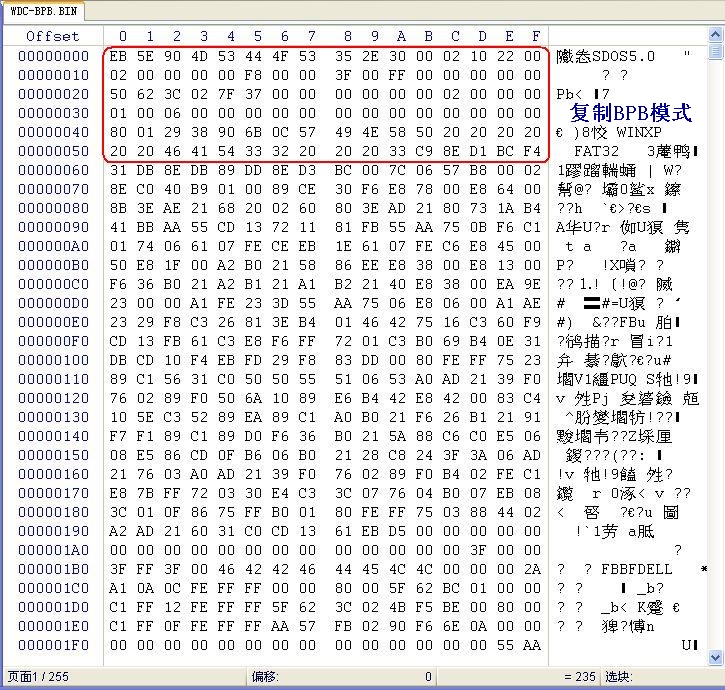
【3】分区表细解：[**高明之三**]  
  
U盘第1、2扇区分区表位置对比：  
1扇区  

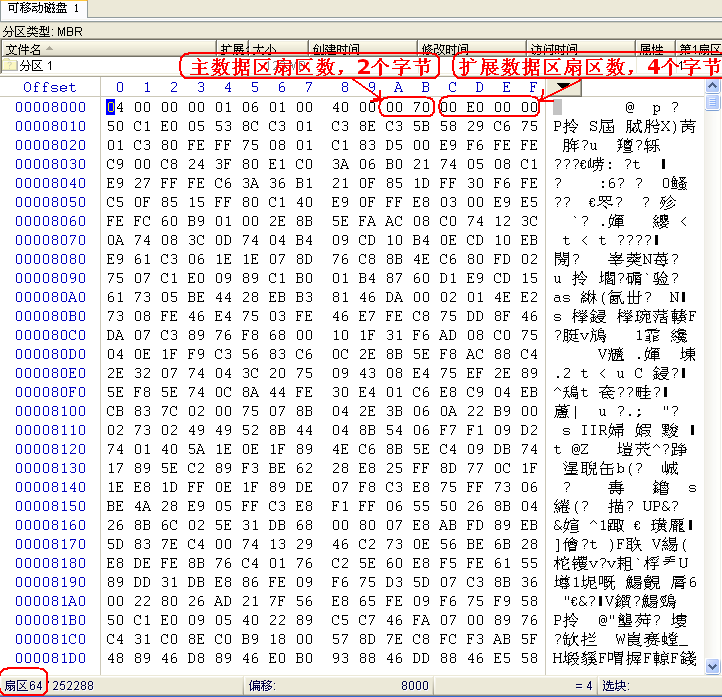

2扇区  


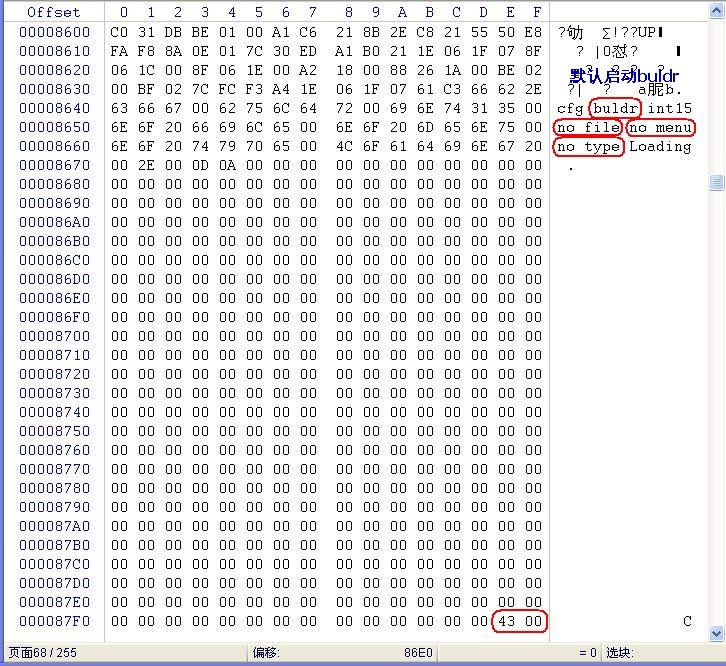
天涯海角1216的理解：  
比如上面第一分区起始位置扇区为 8388608（16进制为00 00 80 00），表示距离第一分区有8388608个扇区，如果此时BIOS读入的是第8号扇区，而此处分区表显示8388600（fbinst 将MBR以后扇区的分区表递减），即距离第一分区有8388600个扇区，且是第8号扇区，BIOS便回读至0号扇区（MBR中有 B9 01 00字符，意思是读入0号扇区），便可以非常准确地知道该扇区位置以及分区表详细信息。（其他分区的分区表也是递减，方法类似）  
  
  
**三、各种模式对比：【高明之四】**  
  
  


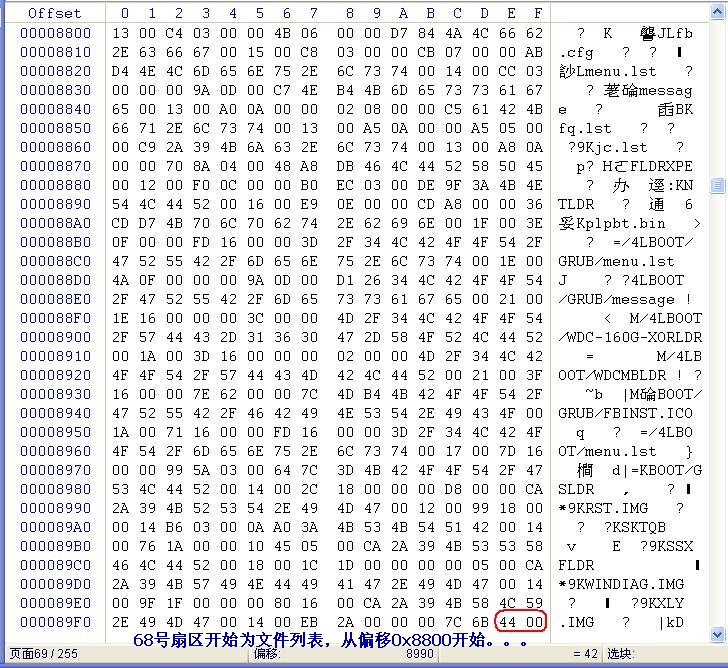






**四、辅助代码细解：【高明之五-UD区**】  
  
fbinst 1.6辅助代码为第65-67号扇区，此为67号扇区。（这个是默认 fbinst 格式化基本扇区数为64的，否则依次增加）  
  
主数据区（包括0扇区和fbinst菜单以及文件列表）和扩展数据区大小设定位置。（64号扇区起始处）  
  
  




从第68号扇区开始为UD内文件列表，下图  
  


**68扇区.jpg** (335.39 KB, 下载次数: 202)

[下载附件](http://bbs.wuyou.com/forum.php?mod=attachment&aid=OTU4OTl8NDU1MjY3NGF8MTQwNDAwNjEwMnwwfDE3MjU3Mg%3D%3D&nothumb=yes)

2010-7-28 09:57 上传

**五、引导过程分析：**  
  
**MBR > UD区 >grldr > PE/IMG/ISO。。。**  
**或**  
**MBR > UD区 >buldr > PE/IMG/ISO。。。**  
  
**fbinst 菜单：**  
1. menu HOTKEY SUBCOMMAND  
启动内核的命令都以menu开始，HOTKEY是对应的热键，子命令有  
  
a) grldr FILENAME  
启动grldr/ntldr文件  
  
b) syslinux FILENAME  
启动ldlinux.bin文件  
  
c) msdos FILENAME  
启动io.sys文件  
   
d) freedos FILENAME  
启动kernel.sys文件  
  
e) chain FILENAME  
加载启动扇区文件  
  
f) linux KERNEL INITRD PARAM  
启动linux内核  
  
2. text STR  
显示一行文字  
  
3. timeout NUM  
设置自动启动的时间  
  
4. default NUM  
设置自动启动的menu项  
  
5. color FG/BG  
设置颜色，前景/背景的格式，颜色值有  
暗色：black, blue, green, cyan, red, magenta, brown, light-gray,   
亮色：dark-gray, light-blue, light-green, light-cyan, light-red, light-magenta, yellow, white  
  
背景只能使用暗色。也可以用normal来表示普通色，它相当于light-gray/black。  
  
**举例：**  
  
timeout 1  
default 0  
color red  
text "fbinst v1.6 menu by bean"  
text "----------[01]----------"  
color green  
text "Press F1> GRLDR"  
menu F1 grldr "grldr"  
color red  
text "----------[02]----------"  
color green  
text "Press F2> WDC-SYSLINUX"  
menu F2 syslinux "ibmlinux.bin"  
color red  
text "----------[03]----------"  
color green  
text "Press F3> MSDOS 7.1"  
menu F3 msdos "io.sys"  
color red  
text "----------[04]----------"  
color green  
text "Press F4> SKTQB"  
menu F4 grldr "SKTQB"  
color red  
text "----------[05]----------"  
color green  
text "Press F5> MaoTao WinPE"  
menu F5 grldr "LDRXPE"  
color red  
text "----------[06]----------"  
color green  
text "Press F6> XORLDR"  
menu F6 chain "XORLDR.MBR"  
color red  
text "----------[07]----------"  
color green  
text "Press F7> BULDR"  
menu F7 grldr "BULDR"  
color red  
text "----------[08]----------"  
color green  
text "Press F8> CJJJP"  
menu F8 grldr "CJJJP"  
color red  
text "----------[09]----------"  
color green  
text "Press F9> NTLDR"  
menu F9 grldr "NTLDR"  
color red  
text "----------[10]----------"  
color green  
text "Press F10 > BOOTMGR"  
menu F10 grldr "BOOTMGR"  
color red  
text "----------[11]----------"  
color green  
text "Press F11 > PLoP Boot Manager"  
menu F11 chain "plpbt.bin"  
color red  
text "----------[12]----------"  
color green  
text "Press F12 > GMYghost.img"  
menu F12 linux "memdisk" "GMYghost.img" "c=142 h=4 s=36 floppy"  
  
也即进入grldr引导后，再加载ISO\IMG\MBR等文件，从而完成你需要的启动过程！  
  
  
**（未完待续，错误之处，请各位批评指正，大家用 winhex 打开磁盘，秘密便真相大白，否则只能跟着别人走。）**