计算机三级辅导:硬盘MBR全面分析计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_AE_A1_E7_AE_97_E6_9C_BA_E4_c98_644177.htm 在分析MBR的结构之前，先有来看看计算机的引导顺序(System Boot Sequence) Step 1. 内部电源打开，初始化，等待一小段时间用来产生稳定的电流。如果主板芯片和CPU收到了不符合规定的电流，将自动产生一个RESET信号。在主板没有收到电源的Power Good信号之前，重复步骤1。 Step 2. 执行BIOS中0FFF0h处的代码。这里只有一条JMP指令，将跳转到真正的BIOS启动程序处。 Step 3. BIOS开始加电自检(Power-On Self Test, POST)，如果出现错误，启动停止。成功的话执行INT 19h(SYSTEM - BOOTSTRAP LOADER) Step 4. BIOS开始寻找显卡，找到的话将执行显卡的BIOS。接着显卡初始化，将显示一段显卡信息，我们开机看到的第一屏就是它。 Step 5. BIOS开始执行所有其他设备的BIOS，包括软驱，硬盘等。 Step 6. BIOS显示启动信息 Step 7. BIOS开始额外的检测。一般有内存检测，如果内存有问题，将显示错误消息。 Step 8. BIOS探测所有的硬件，将显示如硬盘/光区信息等 Step 9. BIOS给出一个已知硬件的列表 Step 10. BIOS按照设置的驱动器顺序找驱动器，如果驱动器存在的话继续找启动扇区，软驱/硬盘的启动扇区都在0柱0头1扇区(cylinder 0, head 0, sector 1) Step 11. 将启动扇区读到内存0000:7c00处，接着INT 19h开始执行0000:7c00处代码 Step 12. 如果找不到驱动器，系统显示错误信息并停止。通常是"No boot device"或"NO ROM BASIC -SYSTEM HALTED" 上面是冷启动的过程，热启动将从步骤8开始 磁盘的启动扇区就是主

引导记录(Master Boot Record)，包括0柱0头1扇区的512个字节，它的任务是完成BIOS到操作系统的交接。 MBR的大体结构: 偏移 内容 0000 MBR程序代码 01BE 分区表 01FE 结束标志 分区表结构 BYTE 1 如果是引导分区，就是80H，如果不是，就是00H 2-4 是该分区的起始扇区号 5 标志字节，比如05表示扩展分区 6-8 该分区的终止扇区号 9-12 该分区已使用的扇区数 13-16 该分区总共占用的扇区数 这是从我的硬盘上提取的MBR（硬盘是Maxtor的金钻20G，netfay的电脑早过时了:P），不同型号的硬盘MBR稍有不同，不过功能都是一样的 0000 33 C0 8E D0 BC 00 7C FB-50 07 50 1F FC BE 1B 7C 3.....|.P.P....| 0010 BF 1B 06 50 57 B9 E5 01-F3 A4 CB BE BE 07 B1 04 ...PW..... 0020 38 2C 7C 09 75 15 83 C6-10 E2 F5 CD 18 8B 14 8B 8,|.u..... 0030 EE 83 C6 10 49 74 16 38-2C 74 F6 BE 10 07 4E AC ....It.8,t....N. 0040 3C 00 74 FA BB 07 00 B4-0E CD 10 EB F2 89 46 25 lt..t...gt..}U 00B0 AA 74 5A 83 EF 05 7F DA-85 F6 75 83 BE 2E 07 EB .tZ.....u..... 00C0 8A 98 91 52 99 03 46 08-13 56 0A E8 12 00 5A EB ...R..F..V....Z. 00D0 D5 4F 74 E4 33 C0 CD 13-EB B8 00 00 80 08 10 16 .Ot.3..... 00E0 56 33 F6 56 56 52 50 06-53 51 BE 10 00 56 8B F4 V3.VVRP.SQ...V.. 00F0 50 52 B8 00 42 8A 56 24-CD 13 5A 58 8D 64 10 72 PR..B.V$..ZX.d.r 0100 0A 40 75 01 42 80 C7 02-E2 F7 F8 5E C3 EB 74 B7 .@u.B.....^..t. 0110 D6 C7 F8 B1 ED CE DE D0-A7 A1 A3 B0 B2 D7 B0 B3 ..... 0120 CC D0 F2 CE DE B7 A8 BC-CC D0 F8 A1 A3 00 BC D3 ..... 0130 D4 D8 B2 D9 D7 F7 CF B5-CD B3 CA B1 B3 F6 CF D6 ..... 0140 B4 ED CE F3 A1 A3 B0 B2-D7 B0 B3 CC D0 F2 CE DE ..... 0150 B7 A8 BC CC D0 F8 A1 A3-00 C8 B1 C9 D9 B2 D9 D7 0160

F7 CF B5 CD B3 00 00 00-00 00 00 00 00 00 00 00 ..... 0170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 0180 00 00 00 8B FC 1E 57 8B-F5 CB 00 00 00 00 00 00 .....W..... 0190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 01A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 01B0 00 00 00 00 00 2C 44 63-B5 D7 B5 D7 00 00 80 01 .....,Dc..... 01C0 01 00 0B FE 7F FD 3F 00-00 00 3F 04 7D 00 00 00 .....?...?.}... 01D0 41 FE 0C FE FF FF 7E 04-7D 00 7D 9B E5 01 00 00 A.....~.}.}..... 01E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 01F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA .....U. 由于程序代码从0000:7C00开始，下面看反编译的结果(经过修改)