高手揭密开发简单“ 操作系统 ”全过程 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/266/2021_2022__E9_AB_98_E6_89_8B_E6_8F_AD_E5_c100_266165.htm [什么？] 很多文章中把写一个引导程序称作是开发一个最简单的操作系统，其实这是非常片面的，引导程序算不上操作系统，虽然此程序可以运行在裸机上。所谓引导程序，直观的说就是在系统加电启动时BIOS第一个执行的程序。 引导程序要想发挥作用，让机器识别，就必须安置在一个特别的位置，这个位置就是磁盘的第一个扇区（0面0磁道1扇区，备注：没有0扇区），而一个包含引导程序的扇区叫作引导扇区。 一个合法的引导扇区（1）通常包含512个字节（当然喽，一个扇区通常本来就是512个字节），（2）并且以0xAA55这样一个占用两个字节的数据结尾作为标志符。（备注：0x前缀说明这是一个十六进制数）。 也就是如果把引导扇区看成一个字符数组的BootSector[]话（因为一个字符，即char，刚好为一个字节），那么这个数组就拥有512个元素，如果用C语言申明的话即为 char BootSector[512]. 接着，一个合法的引导扇区必须以0xAA55结束，即 BootSector[510] = 0x55. BootSector[511] = 0xAA. 除了结束标志必须符合上面的要求之外，中间虽然还有510字节的空间，但执行代码可以少于510字节，用无意义字符（通常用0x0）填充剩余空间即可。 [过程] PC是通过BIOS来启动机器的，当PC机加电之后BIOS启动相应的程序完成机器的自检，然后就寻找可以引导的驱动器，即大家通常所说的启动盘。在 BIOS中可以设置从哪个盘启动，但通常总要检查硬盘，所以当BIOS检查完前面的启动设备之后，如

果没有发现任何引导程序，那么就会开始检查主硬盘，即C盘。如果此时在C盘上找到了合法的引导扇区，那么就会将引导扇区的内容（共512字节）装载到内存0x0000:07C00处。此时BIOS把控制权限交给这段引导程序。 那么，接下来，引导程序通常会简单的执行一些指令，比如输出一段文字，显示一个启动界面等等，但最重要的，引导程序将会启动一个更大的程序，然后把权限交给他，这通常就是我们所说的操作系统内核。额外补充一句，目前对操作系统的定义有不少，但笔者比较赞成的观点如下： 从形式上看，操作系统是：从计算机启动到结束的过程中始终在运行的程序。而这通常就是我们所说的操作系统内核。从功能上看，操作系统：管理和维护所有的硬件、软件、数据资源，并为上层应用或服务提供一个抽象的接口。从某种层面上看，第二中定义更接近于虚拟机。（闲话一段^_^） [如何] 现在，已经了解了这些基本的概念，那么，如何动手制作这样的引导扇区呢？这个过程十分简单， （1）首先按照要求写一个合法的引导程序（通常用汇编，机器码也可以，呵呵）；（2）然后将其通过汇编程序，如NASM汇编成二进制文件；（3）最后，将这个二进制文件写入到目标盘的第一个扇区。 跟我做:-P] 上面说的很简单吧？那好，现在我们来写一个吧！ 第一步：写代码 . 文件名：boot.asm . 代码如下，注意，汇编中通常用“ . ”来表示注释内容 . 此段代码参考《自己动手写操作系统》（于渊） . . 初始化函数 org 07c00h . 告诉编译器将此段程序加载 . 到内存0x0000:07C00处 mov ax, cs mov ds, ax mov es, ax call PrintStr . 调用屏幕打印函数 jmp $ . 无限循环 PrintStr: . 屏幕打印函数 mov ax, HelloWorld . 将字符串拷贝到ax mov bp, ax .

es:bp = 串地址 mov cx, 24 . cx = 串长度 mov ax, 01301h . ah = 13, al = 01h mov bx, 000ch . 页号为0（bh = 0） 黑底红字（bl = 0ch , 高亮） mov dl, 0 int 10h . 10h号中断 ret HelloWorld: db "Welcome to Lees OS *_*" . 字符串负值 times 510-($-$$) db 0 . 用0x0填充剩余的空间使生成 . 的二进制代码刚好为512字节 dw 0xaa55 . 结束标志 . 整个程序结束！很短吧 