# Part 1 PC Bootstrap

## Introduction

This lab is split into three parts. The first part concentrates on getting familiarized with x86 assembly language, the QEMU x86 emulator, and the PC's power-on bootstrap procedure. The second part examines the boot loader for our 6.828 kernel, which resides in the boot directory of the lab tree. Finally, the third part delves into the initial template for our 6.828 kernel itself, named JOS, which resides in the kernel directory.

### Experiment envirment

Hardware:

Memory: 4G

Processor: Intel(R) Core(TM) i5-8250H CPU @ 1.60GHz × 2

OS Type: 64 bit

Disk: 50GB

Software:

OS: Ubuntu 20.04 LTS(x86\_64)

GCC: gcc 9.3.0 #Run gcc -v

Make: GNU Make 4.2.1 #Run make --verison

GDB: GNU gdb 9.1.0 # gdb –v

实际上环境的配置还是比较麻烦的，按照实验页的步骤安装好qemu和gdb后，还需要一些其他的工具链，在配置时我没有记录详细过程，但大抵是参照参考文献的方法进行的，便不再回忆了。

## Part 1: PC Bootstrap

The purpose of the first exercise is to introduce you to x86 assembly language and the PC bootstrap process, and to get you started with QEMU and QEMU/GDB debugging. You will not have to write any code for this part of the lab, but you should go through it anyway for your own understanding and be prepared to answer the questions posed below.

### Exercises 1

Familiarize yourself with the assembly language materials available on [the 6.828 reference page](https://pdos.csail.mit.edu/6.828/2018/reference.html). You don't have to read them now, but you'll almost certainly want to refer to some of this material when reading and writing x86 assembly.

We do recommend reading the section "The Syntax" in [Brennan's Guide to Inline Assembly](http://www.delorie.com/djgpp/doc/brennan/brennan_att_inline_djgpp.html). It gives a good (and quite brief) description of the AT&T assembly syntax we'll be using with the GNU assembler in JOS.

Exercise1就是需要我们对链接中的参考资料有一些了解，没有什么实质性的内容。

### Exercises 2

We will now dive into a bit more detail about how a PC starts up. A PC's physical address space is hard-wired to have the following general layout:

|  |
| --- |
| +------------------+ <- 0xFFFFFFFF (4GB)  | 32-bit |  | memory mapped |  | devices |  | |  /\/\/\/\/\/\/\/\/\/\  /\/\/\/\/\/\/\/\/\/\  | |  | Unused |  | |  +------------------+ <- depends on amount of RAM  | |  | |  | Extended Memory |  | |  | |  +------------------+ <- 0x00100000 (1MB)  | BIOS ROM |  +------------------+ <- 0x000F0000 (960KB)  | 16-bit devices, |  | expansion ROMs |  +------------------+ <- 0x000C0000 (768KB)  | VGA Display |  +------------------+ <- 0x000A0000 (640KB)  | |  | Low Memory |  | |  +------------------+ <- 0x00000000 |

The first PCs, which were based on the 16-bit Intel 8088 processor, were only capable of addressing 1MB of physical memory. The physical address space of an early PC would therefore start at 0x00000000 but end at 0x000FFFFF instead of 0xFFFFFFFF. The 640KB area marked "Low Memory" was the *only* random-access memory (RAM) that an early PC could use; in fact the very earliest PCs only could be configured with 16KB, 32KB, or 64KB of RAM!

The 384KB area from 0x000A0000 through 0x000FFFFF was reserved by the hardware for special uses such as video display buffers and firmware held in non-volatile memory. The most important part of this reserved area is the Basic Input/Output System (BIOS), which occupies the 64KB region from 0x000F0000 through 0x000FFFFF. In early PCs the BIOS was held in true read-only memory (ROM), but current PCs store the BIOS in updateable flash memory. The BIOS is responsible for performing basic system initialization such as activating the video card and checking the amount of memory installed. After performing this initialization, the BIOS loads the operating system from some appropriate location such as floppy disk, hard disk, CD-ROM, or the network, and passes control of the machine to the operating system.

When Intel finally "broke the one megabyte barrier" with the 80286 and 80386 processors, which supported 16MB and 4GB physical address spaces respectively, the PC architects nevertheless preserved the original layout for the low 1MB of physical address space in order to ensure backward compatibility with existing software. Modern PCs therefore have a "hole" in physical memory from 0x000A0000 to 0x00100000, dividing RAM into "low" or "conventional memory" (the first 640KB) and "extended memory" (everything else). In addition, some space at the very top of the PC's 32-bit physical address space, above all physical RAM, is now commonly reserved by the BIOS for use by 32-bit PCI devices.

Recent x86 processors can support *more* than 4GB of physical RAM, so RAM can extend further above 0xFFFFFFFF. In this case the BIOS must arrange to leave a *second* hole in the system's RAM at the top of the 32-bit addressable region, to leave room for these 32-bit devices to be mapped. Because of design limitations JOS will use only the first 256MB of a PC's physical memory anyway, so for now we will pretend that all PCs have "only" a 32-bit physical address space. But dealing with complicated physical address spaces and other aspects of hardware organization that evolved over many years is one of the important practical challenges of OS development.

The following line:

[f000:fff0] 0xffff0: ljmp $0xf000,$0xe05b

is GDB's disassembly of the first instruction to be executed. From this output you can conclude a few things:

* The IBM PC starts executing at physical address 0x000ffff0, which is at the very top of the 64KB area reserved for the ROM BIOS.
* The PC starts executing with CS = 0xf000 and IP = 0xfff0.
* The first instruction to be executed is a jmp instruction, which jumps to the segmented address CS = 0xf000 and IP = 0xe05b.

Why does QEMU start like this? This is how Intel designed the 8088 processor, which IBM used in their original PC. Because the BIOS in a PC is "hard-wired" to the physical address range 0x000f0000-0x000fffff, this design ensures that the BIOS always gets control of the machine first after power-up or any system restart - which is crucial because on power-up there *is* no other software anywhere in the machine's RAM that the processor could execute. The QEMU emulator comes with its own BIOS, which it places at this location in the processor's simulated physical address space. On processor reset, the (simulated) processor enters real mode and sets CS to 0xf000 and the IP to 0xfff0, so that execution begins at that (CS:IP) segment address. How does the segmented address 0xf000:fff0 turn into a physical address?

To answer that we need to know a bit about real mode addressing. In real mode (the mode that PC starts off in), address translation works according to the formula: *physical address* = 16 \* *segment* + *offset*. So, when the PC sets CS to 0xf000 and IP to 0xfff0, the physical address referenced is:

16 \* 0xf000 + 0xfff0 # in hex multiplication by 16 is

= 0xf0000 + 0xfff0 # easy--just append a 0.

= 0xffff0

0xffff0 is 16 bytes before the end of the BIOS (0x100000). Therefore we shouldn't be surprised that the first thing that the BIOS does is jmp backwards to an earlier location in the BIOS; after all how much could it accomplish in just 16 bytes?

由于8088CPU中寄存器都是16位，而CPU地址总线是20位的，我们怎么通过16位的寄存器去拼接20位的地址呢？所以我们需要采用下面的方法：把段寄存器中的值左移4位，形成20位段基址，然后和16位段内偏移相加，就得到了真实地址。比如上面的指令中段寄存器的内容为0xf000，所以真实地址为 0xf000<<4+0xe05b = 0xfe05b。

上面讲述了地址的计算方式，IBM PC从物理地址0x000ffff0开始执行，它位于为ROM BIOS保留的64KB区域的最顶端。要执行的第一条指令是一条jmp指令，它跳转到分段地址CS = 0xf000和IP = 0xe05b。

所以问题来了：

Use GDB's si (Step Instruction) command to trace into the ROM BIOS for a few more instructions, and try to guess what it might be doing. You might want to look at Phil Storrs I/O Ports Description, as well as other materials on the 6.828 reference materials page. No need to figure out all the details - just the general idea of what the BIOS is doing first.

Exercise2 需要我们在进入QEMU之后使用 si 来跟踪ROM BIOS中的更多指令，猜测他们在做一些什么，我们可以参考一些资料，不需要弄清楚所有的细节。

所以我们接下来介绍一下前面的代码们：

1. 0xffff0: ljmp $0xf000, $0xe05b

跳转到0xf000:0xe05b.

1. 0xfe05b: cmpl $0x0, $cs:0x6ac8
2. 0xfe062: jne 0xfd2e1

0x0与cs:0x6ac8这个位置的数字进行比较，如果不相等就跳到0xfd2e1, 指令决定了这是一次reboot还是resume。如果不相等说明这是一次resume，跳转到resume程序的入口地址。具体位置和BIOS有关，可以查看s[tackoverflow上相关问题](https://stackoverflow.com/questions/59479227/why-bios-need-to-compare-a-value-in-seemly-randomized-address-to-zero-in-the-s).

4. 0xfe066: xor %dx, %dx

5. 0xfe068: mov %dx %ss

6. 0xfe06a: mov $0x7000, %esp

7. 0xfe070: mov $0xf34d2, %edx

8. 0xfe076: jmp 0xfd15c

9. 0xfd15c: mov %eax, %ecx

首先看地址说明没有跳转，这是一次reboot。接着清零%dx寄存器。设置栈的段地址为0x0000，偏移量0x7000。跳转到0xfd15c继续执行.

10. 0xfd15f: cli

关闭中断指令，因为启动不能被中断.

11. [0xfd160] 0xfd160: cld

设置方向标志位为0，表明串操作方向是从低地址到高地址.

12. 0xfd161: mov $0x8f, %eax

13. 0xfd167: out %al, $0x70

14. 0xfd169: in $0x71, %al

这三个操作中涉及到两个新的指令out, in。这两个操作是用于操作IO端口的。

　 CPU与外部设备通讯时，通常是通过访问，修改设备控制器中的寄存器来实现的。那么这些位于设备控制器当中的寄存器也叫做IO端口。为了方便管理，80x86CPU采用IO端口单独编址的方式，即所有设备的端口都被命名到一个IO端口地址空间中。这个空间是独立于内存地址空间的。所以必须采用和访问内存的指令不一样的指令来访问端口。

　 所以这里引入in，out操作：

　 in %al, PortAddress 向端口地址为PortAddress的端口写入值，值为al寄存器中的值

　　out PortAddres,%al 把端口地址为PortAddress的端口中的值读入寄存器al中

　 标准规定端口操作必须要用al寄存器作为缓冲。

那么这三条命令就是要操作端口0x70，0x71，它们对应的是什么设备呢？根据下面的链接中所提供的清单：http://bochs.sourceforge.net/techspec/PORTS.LST

我们知道了，0x70端口和0x71端口是用于控制系统中一个叫做CMOS的设备，这个设备是一个低功耗的存储设备，它可以用于在计算机关闭时存储一些信息，它是由独立的电池供电的。这个链接有详细介绍http://wiki.osdev.org/CMOS

这个CMOS中可以控制跟PC相关的多个功能，其中最重要的就是时钟设备（Real Time Clock）的 ，它还可以控制是否响应不可屏蔽中断NMI(Non-Maskable Interrupt)。

操作CMOS存储器中的内容需要两个端口，一个是0x70另一个就是0x71。其中0x70可以叫做索引寄存器，这个8位寄存器的最高位是不可屏蔽中断(NMI)使能位。如果你把这个位置1，则NMI不会被响应。低7位用于指定CMOS存储器中的存储单元地址，所以如果你想访问第1号存储单元，并且在访问时，我要使能NMI，那么你就应该向端口0x70里面送入0b10000001 = 0x81。

即mov $0x81, %al

out %al, 0x70

　 然后对于这个地址单元的操作，比如读或者写就可以由0x71端口完成，比如你现在想从1号存储单元里面读出它的值，在完成上面的两条指令后，就可以输入这条指令

　　in $0x71, %al

再回到我们的系统，这三条指令可以看出，它首先关闭了NMI中断，并且要访问存储单元0xF的值，并且把值读到al中，但是在后面我们发现这个值并没有被利用，所以可以认为这三条指令是用来关闭NMI中断的.

15. 0xfd16b: in $0x92, %al

16. 0xfd16d: or $0x2, %al

17. 0xfd16f: out %al, $0x92

这三条指令依然在控制外设。同样查询后得知0x92端口对应的是PS/2 system control port A，第一位置1使A20地址线被激活，用于测试可用的地址空间.

18. 0xfd171: lidtw %cs:0x6ab8

19. 0xfd177: lgdtw %cs:0x6a74

这两条指令分别用来加载0xf6ab8开始的6个字节到中断描述符表寄存器（IDTR）中和加载0xf6a74开始的6个字节到全局描述符表寄存器（GDTR）中.

20. 0xfd17d: mov %cr0, %eax

21. 0xfd180: or $0x1, %eax

22. 0xfd184: mov %eax, %cr0

这三条指令将CR0寄存器的最低位置为1，代表着启动保护模式.

23. 0xfd187: ljmpl $0x8, $0xfd18f

一个长跳转结束保护模式.

其实很多地方还是不太理解的，不过先把搜集到的资料和自己的理解整合在这里就是了。

## Part 2: The Boot Loader

于PC来说，软盘，硬盘都可以被划分为一个个大小为512字节的区域，叫做扇区。一个扇区是一次磁盘操作的最小粒度。每一次读取或者写入操作都必须是一个或多个扇区。如果一个磁盘是可以被用来启动操作系统的，就把这个磁盘的第一个扇区叫做启动扇区。这一部分介绍的boot loader程序就位于这个启动扇区之中。当BIOS找到一个可以启动的软盘或硬盘后，它就会把这512字节的启动扇区加载到内存地址0x7c00~0x7dff这个区域内。然后使用jmp指令将CS:IP设置为0000:7c00，并将控制权传递给引导加载程序。像BIOS加载地址一样，这些地址是相当任意的-但它们对于PC是固定的和标准化的。

对于6.828，我们将采用传统的硬盘启动机制，这就意味着我们的boot loader程序的大小必须小于512字节。整个boot loader是由一个汇编文件，boot/boot.S，以及一个C语言文件，boot/main.c。Boot loader必须完成两个主要的功能。

1. 首先，boot loader要把处理器从实模式转换为32bit的保护模式，因为只有在这种模式下软件可以访问超过1MB空间的内容。

2. 然后，boot loader可以通过使用x86的特定的IO指令，直接访问IDE磁盘设备寄存器，从磁盘中读取内核。

对于boot loader来说，有一个文件很重要，obj/boot/boot.asm。这个文件是我们真实运行的boot loader程序的反汇编版本。所以我们可以把它和它的源代码即boot.S以及main.c比较一下。

### Exercise 3

Take a look at the [lab tools guide](https://pdos.csail.mit.edu/6.828/2018/labguide.html), especially the section on GDB commands. Even if you're familiar with GDB, this includes some esoteric GDB commands that are useful for OS work.

Set a breakpoint at address 0x7c00, which is where the boot sector will be loaded. Continue execution until that breakpoint. Trace through the code in boot/boot.S, using the source code and the disassembly file obj/boot/boot.asm to keep track of where you are. Also use the x/i command in GDB to disassemble sequences of instructions in the boot loader, and compare the original boot loader source code with both the disassembly in obj/boot/boot.asm and GDB.

Trace into bootmain() in boot/main.c, and then into readsect(). Identify the exact assembly instructions that correspond to each of the statements in readsect(). Trace through the rest of readsect() and back out into bootmain(), and identify the begin and end of the for loop that reads the remaining sectors of the kernel from the disk. Find out what code will run when the loop is finished, set a breakpoint there, and continue to that breakpoint. Then step through the remainder of the boot loader.

Be able to answer the following questions:

* At what point does the processor start executing 32-bit code? What exactly causes the switch from 16- to 32-bit mode?
* What is the *last* instruction of the boot loader executed, and what is the *first* instruction of the kernel it just loaded?
* *Where* is the first instruction of the kernel?
* How does the boot loader decide how many sectors it must read in order to fetch the entire kernel from disk? Where does it find this information?

Answers:

* 答: 可以阅读boot.s文件知道在如图所示的ljmp $PROT\_MODE\_CSEG, $protcseg:

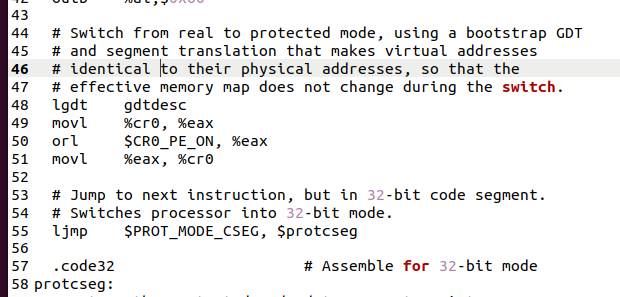


图3.1

* 答:boot loader执行的最后一条语句是bootmain子程序中的最后一条语句

" ((void (\*)(void)) (ELFHDR->e\_entry))(); ",

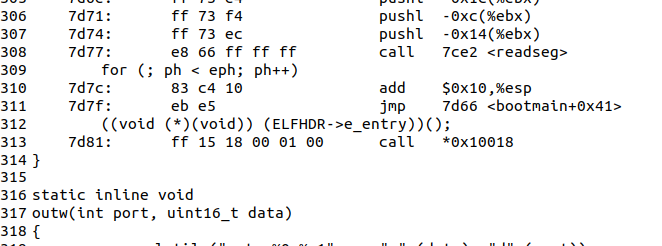


图3.2

* 答:即跳转到操作系统内核程序的起始指令处。 这个第一条指令位于/kern/entry.S文件中，第一句 movw $0x1234, 0x472.

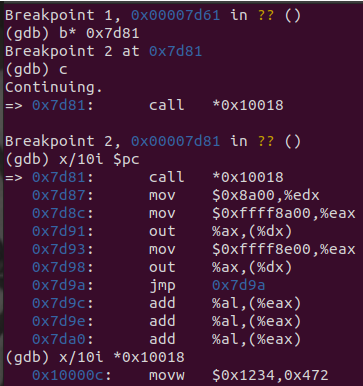


图3.3

这个就是先在obj/boot/boot.asm中找到0x7d81位置会执行bootmain最后一条语句(如图3.2)，先设置断点然后执行到这里，再进入,看到0x10018开始后面的第一条语句。

* 答：首先关于操作系统一共有多少个段，每个段又有多少个扇区的信息位于操作系统文件中的Program Header Table中。这个表中的每个表项分别对应操作系统的一个段。并且每个表项的内容包括这个段的大小，段起始地址偏移等等信息。所以如果我们能够找到这个表，那么就能够通过表项所提供的信息来确定内核占用多少个扇区。

那么关于这个表存放在哪里的信息，则是存放在操作系统内核映像文件的ELF头部信息中。

### Exercise 4

Read about programming with pointers in C. The best reference for the C language is *The C Programming Language* by Brian Kernighan and Dennis Ritchie (known as 'K&R'). We recommend that students purchase this book (here is an [Amazon Link](http://www.amazon.com/C-Programming-Language-2nd/dp/0131103628/sr=8-1/qid=1157812738/ref=pd_bbs_1/104-1502762-1803102?ie=UTF8&s=books)) or find one of [MIT's 7 copies](http://library.mit.edu/F/AI9Y4SJ2L5ELEE2TAQUAAR44XV5RTTQHE47P9MKP5GQDLR9A8X-10422?func=item-global&doc_library=MIT01&doc_number=000355242&year=&volume=&sub_library=).

Read 5.1 (Pointers and Addresses) through 5.5 (Character Pointers and Functions) in K&R. Then download the code for [pointers.c](https://pdos.csail.mit.edu/6.828/2018/labs/lab1/pointers.c), run it, and make sure you understand where all of the printed values come from. In particular, make sure you understand where the pointer addresses in printed lines 1 and 6 come from, how all the values in printed lines 2 through 4 get there, and why the values printed in line 5 are seemingly corrupted.

There are other references on pointers in C (e.g., [A tutorial by Ted Jensen](https://pdos.csail.mit.edu/6.828/2018/readings/pointers.pdf) that cites K&R heavily), though not as strongly recommended.

*Warning:* Unless you are already thoroughly versed in C, do not skip or even skim this reading exercise. If you do not really understand pointers in C, you will suffer untold pain and misery in subsequent labs, and then eventually come to understand them the hard way. Trust us; you don't want to find out what "the hard way" is.

这个就是让你阅读一下pointers.c然后理解为什么会有这样的结果，这个其实并不难，在此复制一下其他人文档的结果:（非要说的话第三个和第五个最值得看一下吧）

首先程序声明了3个重要的数组，指针

int型数组--int a[4];    int类型指针--int \*b = malloc(16);     int类型指针--int \*c;

打印的第一句：

　　printf("1: a = %p, b = %p, c = %p\n", a, b, c);

其中：

　　a输出的是数组a的首地址，0xbfb4bf84。

　　b输出的是指针b所指向的操作系统分配给它的空间的起始地址，0x8886008

　　c输出的是未定义的指针变量c的值，0xb75d8255

打印第二句之前，完成的操作：

　　c = a;  让c指针和a指向同一个内存地址，0xbfb4bf84;

　 for(i = 0; i<4; i++) a[i] = 100+i;   这个操作会让数组a的四个单元的值变为，100,101,102,103。

　 c[0] = 200;   由于c和a指向同一个地方，c[0] = a[0] = 200;

　 printf("2: a[0] = %d, a[1] = %d, a[2] = %d, a[3] = %d,", a[0], a[1], a[2], a[3]);　所以打印第二句，第一个元素的值会是200.

打印第三句之前，完成操作：

　　c[1] = 300;

　　\*(c+2) = 301;

3[c] = 302;

分别代表访问数组中的值的三种不同的方法。由于c和a相同，所以它们也是在修改数组a的值。把a[1], a[2]，a[3]全都被改变。printf("3: a[0] = %d, a[1] = %d, a[2] = %d, a[3] = %d,", a[0], a[1], a[2], a[3]);

打印第四句前，完成操作：c = c+1;

将指针c指向数组中下一个单元，即a[1]

　　\*c = 400

　　修改a[1]值为400

　　printf("4: a[0] = %d, a[1] = %d, a[2] = %d, a[3] = %d,", a[0], a[1], a[2], a[3]);

打印第五句前，完成操作

　　 c = (int \*)((char \*)c + 1);

先把c强制转换为char类型指针，然后指针加1，此时c的数值应该也加1，由于之前c指向a数组中1号元素的起始地址，1号元素起始地址为0xbfb4bf88，之后加1，变为0xbfb4bf89。然后再把c强制转换回int类型指针，

此时c所操作的地址为0xbfb4bf89~0xbfb4bf8c。

　　\*c = 500

　　把地址地址为0xbfb4bf89~0xbfb4bf8c的值换为500，此时会影响原来数组a的1,2号元素。原来一号元素在内存中存放在地址0xbfb4bf88~0xbfb4bf8b处，存放的值为400，十六进制为0x00000190

　　 0xbfb4bf88  0xbfb4bf89  0xbfb4bf8a  0xbfb4bf8b

　　　 90                 01                 00                00

　　 原来二号元素在内存中存放在地址0xbfb4bf8c~0xbfb4bf8f处，存放的值为301，十六进制为0x0000012D。

　　 0xbfb4bf8c  0xbfb4bf8d  0xbfb4bf8e  0xbfb4bf8f

　　　 2D                 01                 00                00

　 而现在c操作的地址为0xbfb4bf89~0xbfb4bf8c，并赋值500，十六进制为0x000001F4，所以内存单元变为

　 0xbfb4bf88  0xbfb4bf89  0xbfb4bf8a  0xbfb4bf8b

　　 90                 F4                 01                00

　 0xbfb4bf8c  0xbfb4bf8d  0xbfb4bf8e  0xbfb4bf8f

　　　00                 01                 00                00

　 所以此时a[1]的值变为0x0001F490 = 128144, a[2]的值变为0x00000100 = 256.

　 打印第六句前，完成操作：

　　b = (int \*)a + 1;

　 这步操作会把b的值加1，由于b现在是int类型指针，所以数值上b的值增加4，所以b的值变为 0xbfb4bf84 + 0x4 = 0xbfb4bf88

　　c = (int \*)((char \*)a+1);

　 这步还是先把a转换为char型指针，然后加1，此时加1会让数值上只增加1，所以c的值变为 0xbfb4bf84 + 0x1 = 0xbfb4bf85

### Exercise 5

对于6.828，可以将ELF可执行文件视为带有加载信息的标头，然后是几个程序段，每个程序段都是要在指定地址加载到内存中的连续代码或数据块。引导加载程序不会修改代码或数据；它将其加载到内存中并开始执行它。

ELF二进制文件以一个定长的ELF头开始，后面是边长的程序头，每个程序头列举了需要载入的程序节。ELF头和程序头的定义详情可见inc/elf.h. （以下我们来回忆ICS中讲的不多但很重要的编译链接那一章）  
我们主要关心以下程序节：

* .text程序的可执行指令
* .rodata 只读数据，比如C编译器生成的ASCII字符串常量。
* .data 数据节包括了程序已经初始化的数据，比如初始化了的全局变量。

在.data节之后是.bss节，它为未初始化的全局变量保留空间。链接器只为.bss记录了地址和大小，需要链接器或者程序自身来为这一节做零初始化。  
在.text节中我们特别关心“VMA”（链接地址）和“LMA”（加载地址）。加载地址顾名思义指这一节应当被加载到内存中的位置。而链接地址则是这一程序节开始执行的**期望位置**。比如链接最重要的一步就是符号重定位。汇编代码中有一些常量在一开始编译生成可重定位目标文件的时候，其值是不确定的，因为编译器并不知道，最后这些程序（数据）的位置；只有在链接过程中，我们知道了程序开始执行的期望位置，然后链接器会对这些常量进行替换。在此基础上我们就可以做Exercise 5了。补充以下两个命令：

objdump -h obj/boot/boot.out #Used to check sections

objdump -x obj/kern/kernel #Used to inspect program headers

下面是问题:

Trace through the first few instructions of the boot loader again and identify the first instruction that would "break" or otherwise do the wrong thing if you were to get the boot loader's link address wrong. Then change the link address in boot/Makefrag to something wrong, run **make clean**, recompile the lab with **make**, and trace into the boot loader again to see what happens. Don't forget to change the link address back and **make clean** again afterward!

Exercise 5 要求修改boot/Makefrag中-Ttext后面的链接地址，重新编译lab，查看什么地方会出错。我们运行就会发现第一个用到链接时常量的指令lgdt gdtdesc会出错。  
除了节中的信息外，ELF头中的e\_entry域也十分重要，它是程序入口的链接地址，即程序的.text节从内存的什么地址开始执行，可以通过运行以下命令查看e\_entry:

objdump -f obj/kern/kernel

回答：

这道题希望我们能够去修改boot loader的链接地址，在lab 1中，作者引入了两个概念，一个是链接地址，一个是加载地址。链接地址可以理解为通过编译器链接器处理形成的可执行程序中指令的地址，即逻辑地址。加载地址则是可执行文件真正被装入内存后运行的地址，即物理地址。

那么在boot loader中，由于在boot loader运行时还没有任何的分段处理机制，或分页处理机制，所以boot loader可执行程序中的链接地址就应该等于加载地址。在lab中作者说，BIOS默认把boot loader加载到0x7C00内存地址处，所以就要求boot loader的链接地址也要在0x7C00处。boot loader地址的设定是在boot/Makefrag中完成的，所以根据题目的要求，我们需要改动这个文件的值。

首先按照题目要求，在lab目录下输入make clean，清除掉之前编译出来的内核可执行文件，在清除之前你可以先把 obj/boot/boot.asm文件拷贝出来，之后可以用来比较。然后打开这个boot/Makefrag文件，我们会发现下列语句：

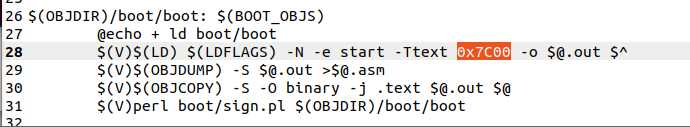


图5.1

其中的-Ttext 0x7C00，就是指定链接地址，我们可以把它修改为0x7E00，然后保存退出。

然后在lab下输入make，重新编译内核，首先查看一下obj/boot/boot.asm，并且和之前的那个obj/boot/boot.asm文件做比较。下图是新编译出来的boot.asm：

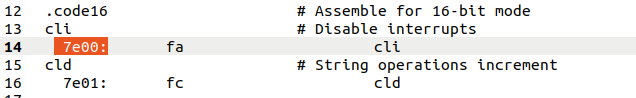


图5.2

然后我们还是按照原来的方式，调试一下内核：

由于BIOS会把boot loader程序默认装入到0x7c00处，所以我们还是再0x7C00处设置断点，并且运行到那里，结果发现如下：

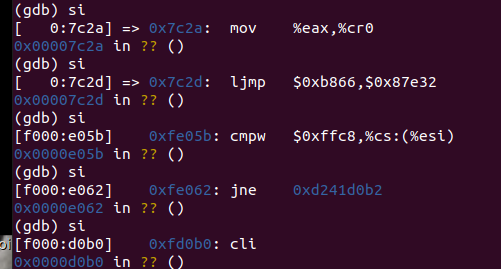


图5.3

在7c2d之后就开始跳到不对的地方了，因为一开始把7c00变成7e00导致本来应该是7c32这里是7e32了。

### Exercise 6

Besides the section information, there is one more field in the ELF header that is important to us, named e\_entry. This field holds the link address of the *entry point* in the program: the memory address in the program's text section at which the program should begin executing. You can see the entry point:

athena% **objdump -f obj/kern/kernel**

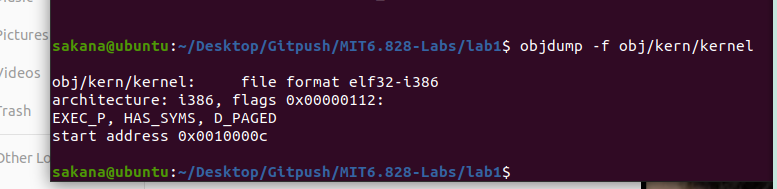


图6.1

所以这个0x10000c是kernel入口点。

下面是问题:

We can examine memory using GDB's **x** command. The [GDB manual](https://sourceware.org/gdb/current/onlinedocs/gdb/Memory.html) has full details, but for now, it is enough to know that the command **x/*N*x *ADDR*** prints *N* words of memory at *ADDR*. (Note that both 'x's in the command are lowercase.) *Warning*: The size of a word is not a universal standard. In GNU assembly, a word is two bytes (the 'w' in xorw, which stands for word, means 2 bytes).

Reset the machine (exit QEMU/GDB and start them again). Examine the 8 words of memory at 0x00100000 at the point the BIOS enters the boot loader, and then again at the point the boot loader enters the kernel. Why are they different? What is there at the second breakpoint? (You do not really need to use QEMU to answer this question. Just think.)

Exercise 6 要求分别在BIOS进入boot loader和boot loader进入kernel的地方，检查从内存地址0x00100000开始的8个word。回答以下两个问题：

* 为什么他们不一样？
* 在第二个断点停下来的时候，在该位置的是什么内容？

答:

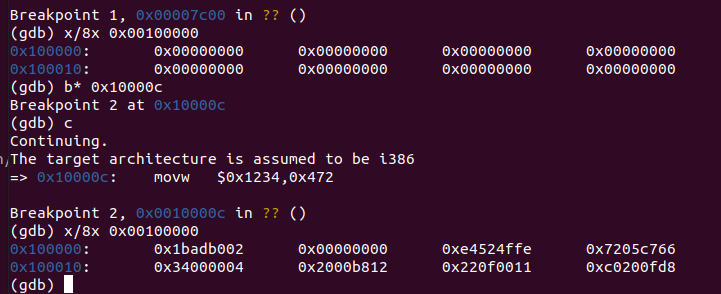


图6.2  
为什么会产生这种变化，因为bootmain函数在最后会把内核的各个程序段送入到内存地址0x00100000处，所以这里现在存放的就是内核的某一个段的内容，由于程序入口地址是0x0010000C，正好位于这个段中，所以可以推测，这里面存放的应该是指令段，即.text段的内容。  
当BIOS进入bootloader时，因为此时工作在实模式，0x10000以上的内存根本无法访问，所以内存中的内容应该为空。 bootloader进入kernel时，程序地址0x100000处加载的操作系统的代码。