

OS LAB1 REPORT

1811363 洪一帆

具体负责部分的文档内容可以查看[result.md](#)

以下是文档截图

练习2及4的相关报告

1811363 洪一帆

练习2 - BIOS的启动及debug

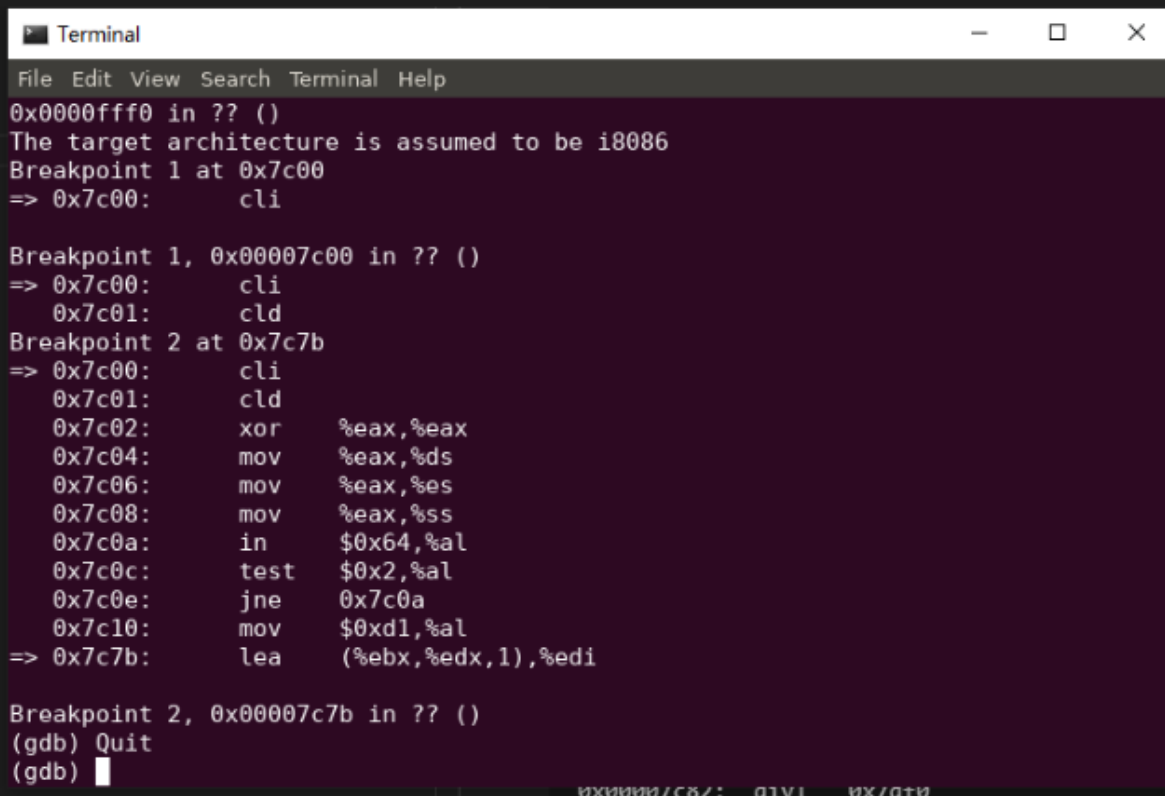
BIOS实际上是被固化在计算机 ROM（只读存储器）芯片上的一个特殊的软件，为上层软件提供最底层的、最直接的硬件控制与支持。

1. 断点的设置：

在lab1init中输入：

```
b *0x7c00
continue
x /2i $pc
b *0x00007c7b
x /10i $pc
continue
```

在0x7c00处设置断点。此地址是bootloader入口点地址，即boot/bootasm.S的start地址处。0x00007c7b是BootLoader中的一个位置，可以在结果中看到它的上下文。



```
Terminal
File Edit View Search Terminal Help
0x0000ffff in ?? ()
The target architecture is assumed to be i8086
Breakpoint 1 at 0x7c00
=> 0x7c00:      cli

Breakpoint 1, 0x00007c00 in ?? ()
=> 0x7c00:      cli
0x7c01:      cld
Breakpoint 2 at 0x7c7b
=> 0x7c00:      cli
0x7c01:      cld
0x7c02:      xor     %eax,%eax
0x7c04:      mov     %eax,%ds
0x7c06:      mov     %eax,%es
0x7c08:      mov     %eax,%ss
0x7c0a:      in      $0x64,%al
0x7c0c:      test    $0x2,%al
0x7c0e:      jne     0x7c0a
0x7c10:      mov     $0xd1,%al
=> 0x7c7b:      lea     (%ebx,%edx,1),%edi

Breakpoint 2, 0x00007c7b in ?? ()
(gdb) Quit
(gdb) █
```

运行结果log

问题合集

wsl无法打开Makefile中的调试工具，是因为无法调用TERMINAL:=xfce4-terminal：

解决：

- 安装虚拟机Ubuntu，但是因为系统自动更新导致之前的包版本不匹配。reinstall直接把系统给整崩了（好像是删除包的时候出现太多错误系统直接中断了）。心态炸了。。。。
- 通过wsl安装可视化界面gnome-terminal：但是装好后忘记改terminal参数然后一直报错。太蠢了。。

```
# TERMINAL :=xfce4-terminal  
TERMINAL :=gnome-terminal
```

无法进行Ubuntu和window之间剪切板的交互

只能通过截图来展示结果。

没有能够很好地理解BIOS启动过程中CS寄存器的值

一开电，启动的是实模式，早期是为了向下兼容。

CS为F000H，EIP为FFF0H。将地址相加，得到BIOS的起始地址应该是1 EFF0H。

但是文档里面说应该是FFFF FFF0H。感到很困惑。

解决：

- 更多地查阅和理解：CS有一个shadow register，其值为FFFF，和EIP相加和得到正确的结果。
- **理论结合实践**
可以从log中看到起始地址确实为FFFF FFF0H，并且执行了一个长跳转。
- 为什么要设置一个shadow register这样的机制--是为了更好地向前兼容。

写在最后

为了准备展示发现好麻烦啊，真的需要很仔细地去理解查阅各个知识点。但是确实收获了很多。