#实验⼀： 内容

⽬标： 熟悉开发操作系统的环境和⼯具， 熟悉Linux 内核的编译、 加载运⾏的过程， 熟悉下qemu模拟器的使⽤⽅法。

##1.完成Linux内核编译；

具体内容参⻅实验指导；

##2.完成initramfs的制作过程

具体内容参⻅实验指导；

##3.完成内核的装载和启动过程

具体内容参⻅实验指导；

##4.完成Busybox的编译、 启动过程

具体内容参⻅实验指导；

##5.完成Busybox的远程调试

具体内容参加实验指导， 可以尝试gdb的多种功能；

##6.完成Linux 0.11内核的编译、 启动和调试

下载Linux 0.11内核代码

注意从课程提供的地址下载， 否在linux 0.11内核不能编译， 因为早期的linux内核需要低版本的gcc编译器；

编译32位版本的linux 0.11内核

找到Makeﬁle， 查看⾥⾯的内容， 通过make⼯具进⾏编译； 另外， 因为需要调试， 所以需要在gcc编译命令中添加 -g参数， 产 ⽣内核的符号表； 编译32位版本的内核， 需要添加-m 32参数；

使⽤qemu-system-i386加载、 启动内核

qemu-system-i386 -m 16 -boot a -fda Image -hda hdc-0.11.img -s -S

进⼊Linux 0.11操作系统， 熟悉该操作系统的命令

⽐如查看⽬录结构， 运⾏简单的shell命令如ls、 ping等；

利⽤gdb进⾏调试远程调试

i. 启动gdb；

ii. 加载linux 0.11的符号表 （⼀般位于tools/system）；

iii. target remote:1234远程连接qemu调试；

iv. 设置源码⽬录： directory linux 0.11的源码路径;

v. 设置汇编代码的形式： set disassembly-ﬂavor intel

vi. 在关键位置设置断点如在地址0x7c00、 内核⼊⼝函数 （main） 等 （可以参考linux 0.11 源码中的bootsect.S中的⼀些关键 地址和寄存器）；

vii. 观察 0x7DFE和0x7DFF地址的内容；

熟悉linux 0.11操作系统与主机操作系统之间的⽂件交换

i. 关闭qemu模拟器；

ii. 找到hdc-0.11.img硬盘镜像⽂件， 这是linux 0.11操作系统启动后的根⽂件系统， 相当于在 qemu 虚拟机⾥ 装载的硬盘；

iii. 先⽤fdisk命令查 看磁盘的分区情况以及⽂件类型(minix): ﬁdsk hdc-0.11.img;

iv. 创建本地挂载⽬录 mkdir hdc;



v. 显式磁盘空间

df -h

vi. 挂载linux 0.11硬盘镜像

sudo mount -t minix -o loop,oﬀset=512 hdc-0.11.img

hdc (注意是hdc的完整路径)

vii. 查看是否挂载成功

df -h （是否出现挂载的hdc路径）

h. 查看挂载后的hdc⽬录结构

ll hdc

i. 在hdc中创建⽂件

进⼊hdc的usr⽬录 cd hdc/usr

sudo touch hello.txt

sudo vim hello.txt （编辑⽂件）

j. 卸载⽂件系统hdc

sudo unmount /dev/loop (查看具体的loop设备)

df -h （查看是否已经卸载）

重新⽤qemu启动linux 0.11

观察/usr⽬录下是否有hello.txt⽂件