#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；
具体内容参见实验指导；
##2.完成initramfs的制作过程
具体内容参见实验指导；
##3.完成内核的装载和启动过程
具体内容参见实验指导；
##4.完成Busybox的编译、启动过程
具体内容参见实验指导；
##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