本科生实验报告

实验课程:_____操作系统_____

实验名称:_____编译内核_____

专业名称:_____计算机科学与技术_____

学生姓名:_____凌国明_____

学生学号:_____21307077_____

实验地点:_____教室_____

实验成绩:_____

报告时间:_____2023.03.06_____

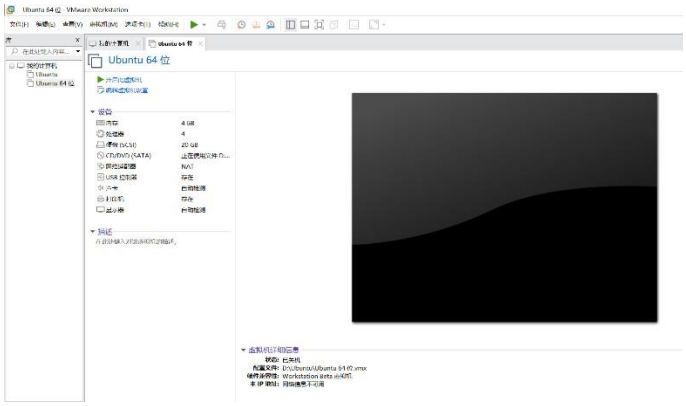
1. 实验要求

在本次实验中，同学们会熟悉现有 Linux 内核的编译过程和启动过程， 并在自行编译内核的基础上构建简单应用并启动。同时，同学们会利用精简的 Busybox 工具集构建简单的 OS， 熟悉现代操作系统的构建过程。 此外，同学们会熟悉编译环境、相关工具集，并能够实现内核远程调试。具体内容如下。

1. 搭建 OS 内核开发环境包括：代码编辑环境、编译环境、运行环境、调试环境等。
2. 下载并编译 i386（32 位）内核，并利用 qemu 启动内核。
3. 熟悉制作 initramfs 的方法。
4. 编写简单应用程序随内核启动运行。
5. 编译 i386 版本的 Busybox，随内核启动，构建简单的 OS。
6. 开启远程调试功能，进行调试跟踪代码运行。
7. 撰写实验报告。

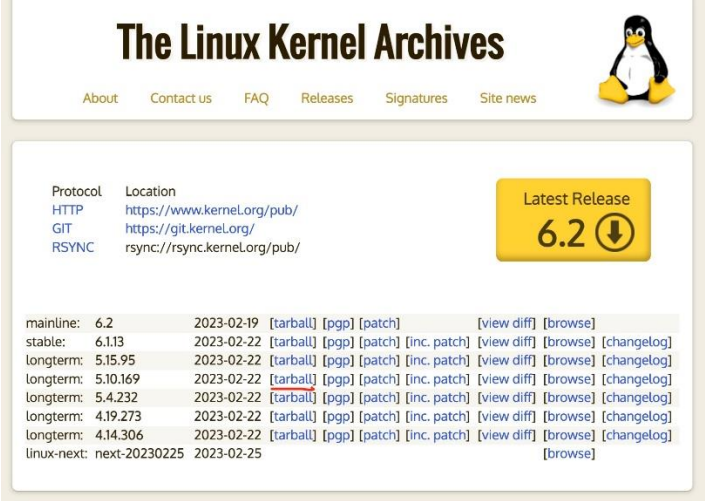
2. 实验过程

1） 环境配置，下载 Vmware，安装 Ubuntu 虚拟机，换源。

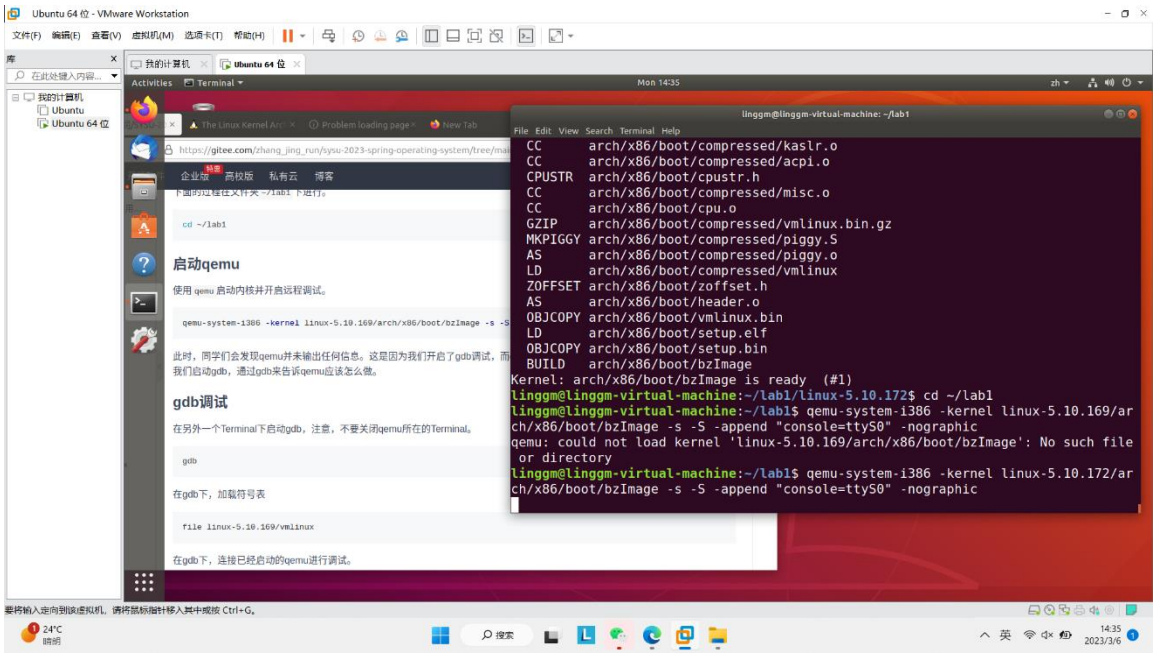


2）配置 C/C++环境，安装其他工具

3）下载了 Linux5.10.172，并编译 Linux 内核

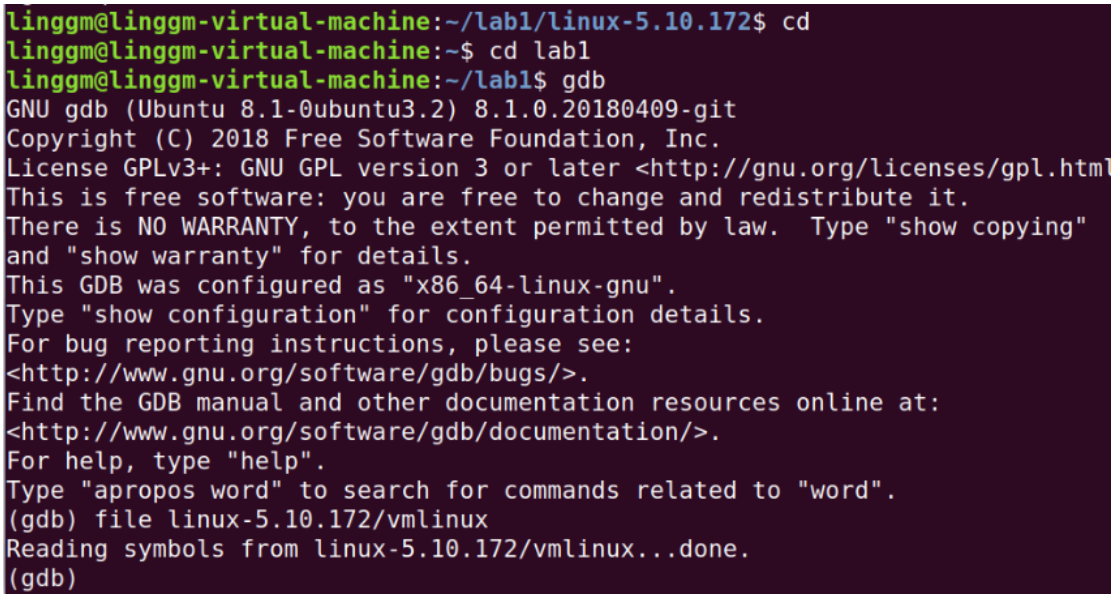


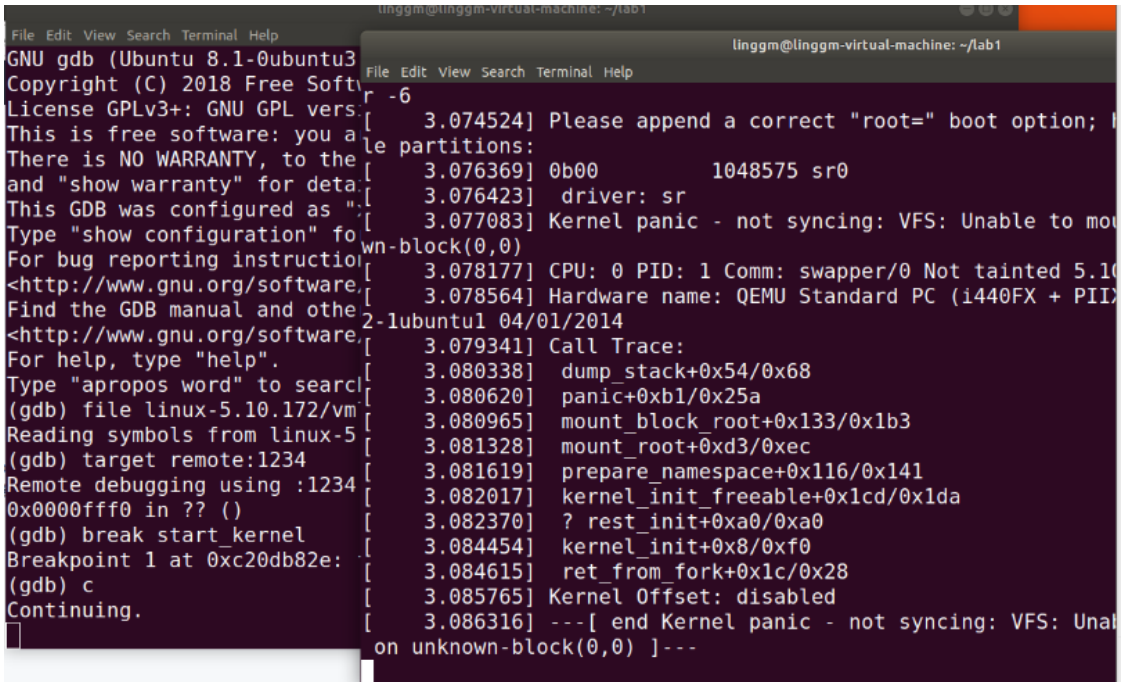
4）启动内核并调试，使用 qemu 启动内核，开启远程调试



5）第 4 步完成后 qemu 没有输出任何信息，这是因为开启了 gdb 调试，qemu 需等待 gdb 的 c 指令才能继续执行。

第五步是进行 gdb 调试：新开一个终端，启动 gdb，此时不应关闭原有终端，先加载符号表，然后连接 qemu 进行调试，设置断点后，输入 c 运行 qemu



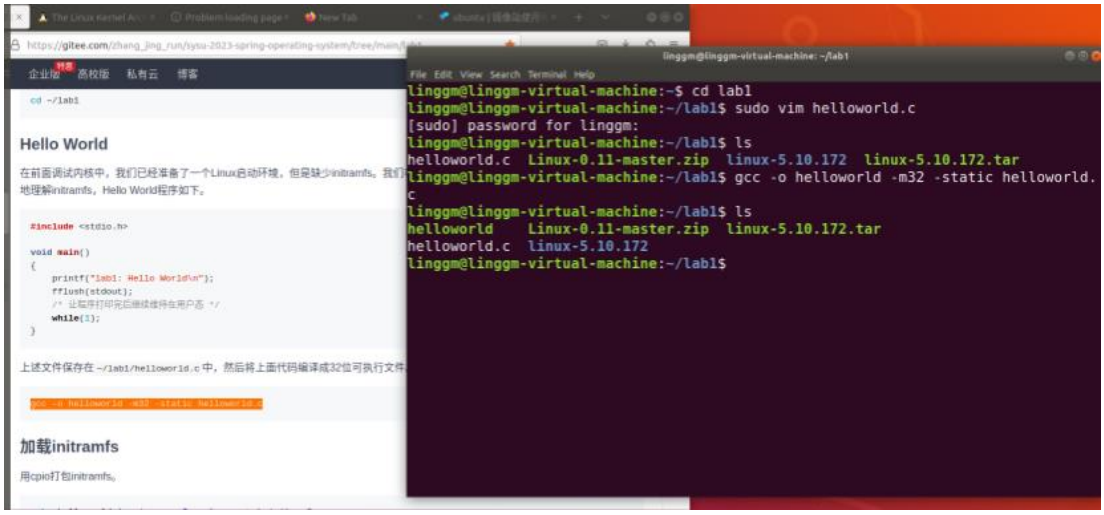


6）制作 Initramfs

- Hello World

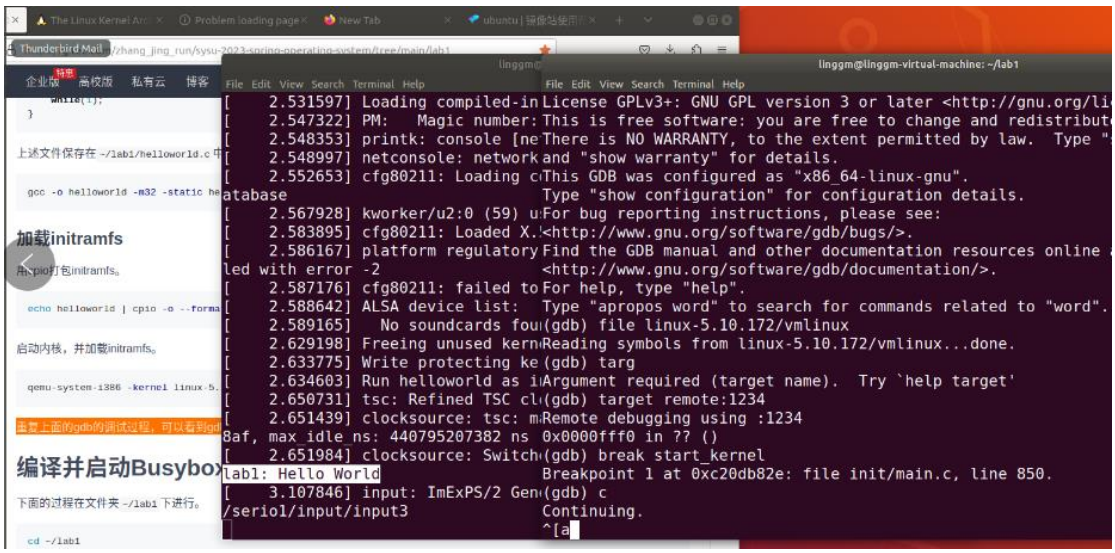
  用 vim 写一个 HelloWorld.c 程序，利用 gcc 工具将这段代码编译成 32 位可执行文件

  gcc -o helloworld -m32 -static helloworld.c



- 加载 initramfs

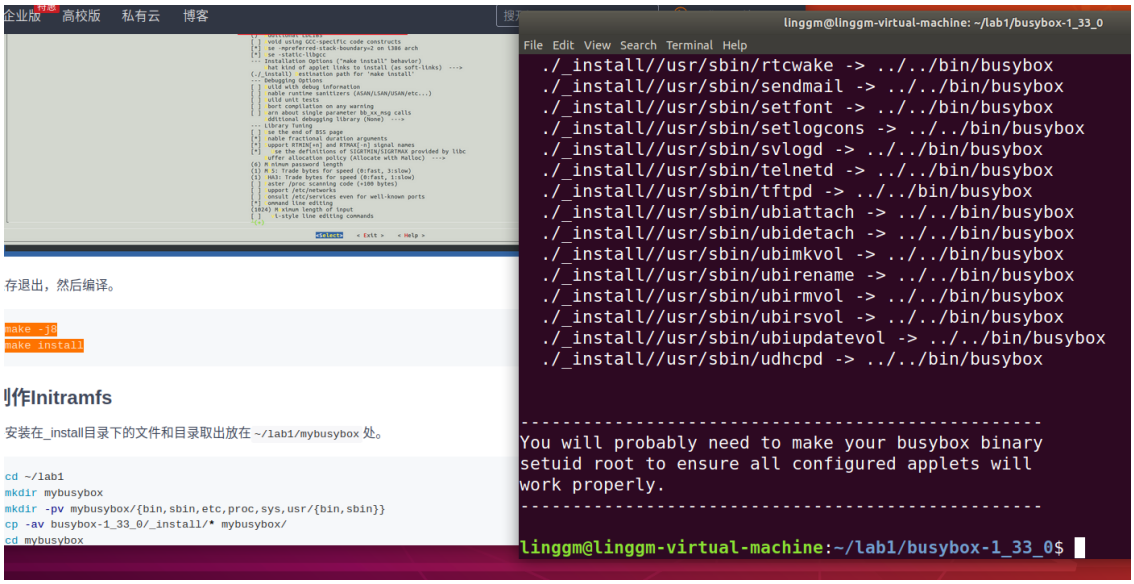
  用 cpio 打包 initramfs，启动内核并加载 initramfs



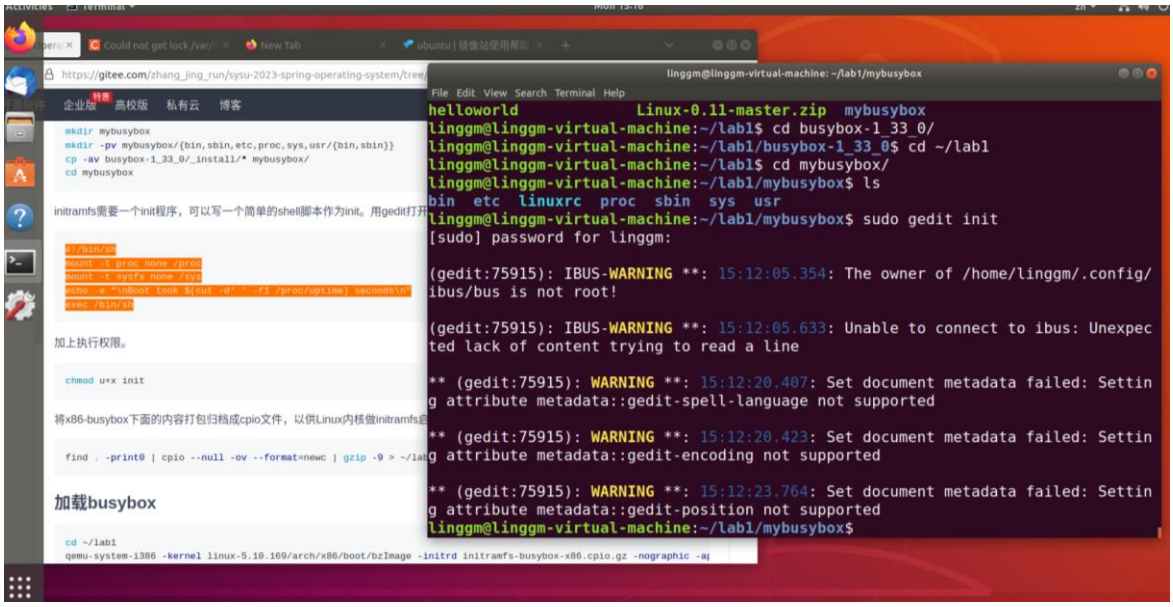
可以看到，按如上步骤，helloworld 程序得以运行。

7）编译并启动 busybox

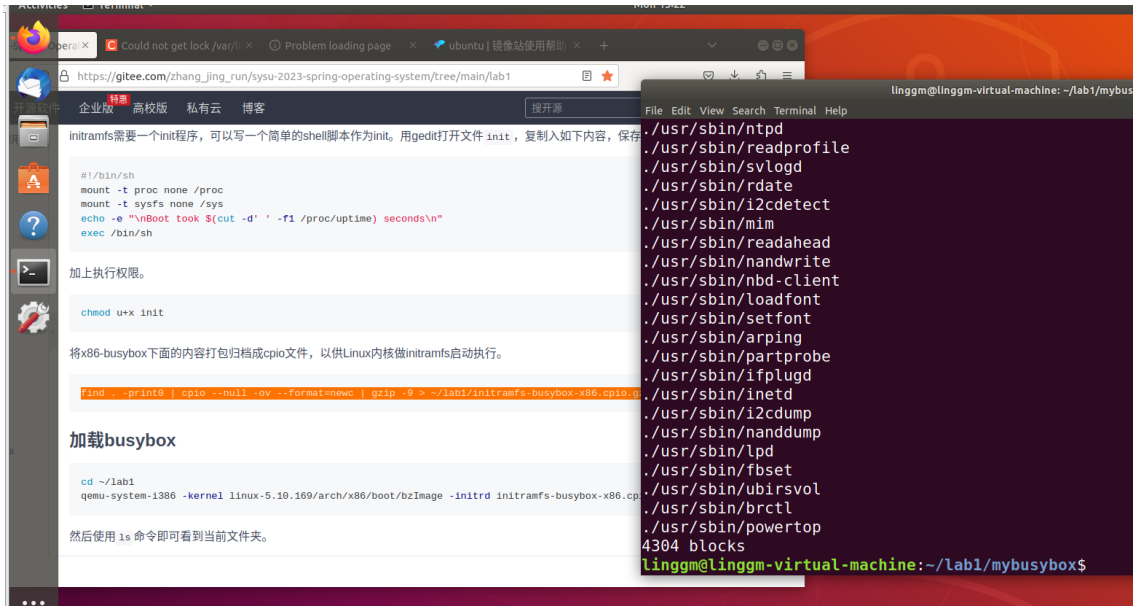
- 下载，解压，编译

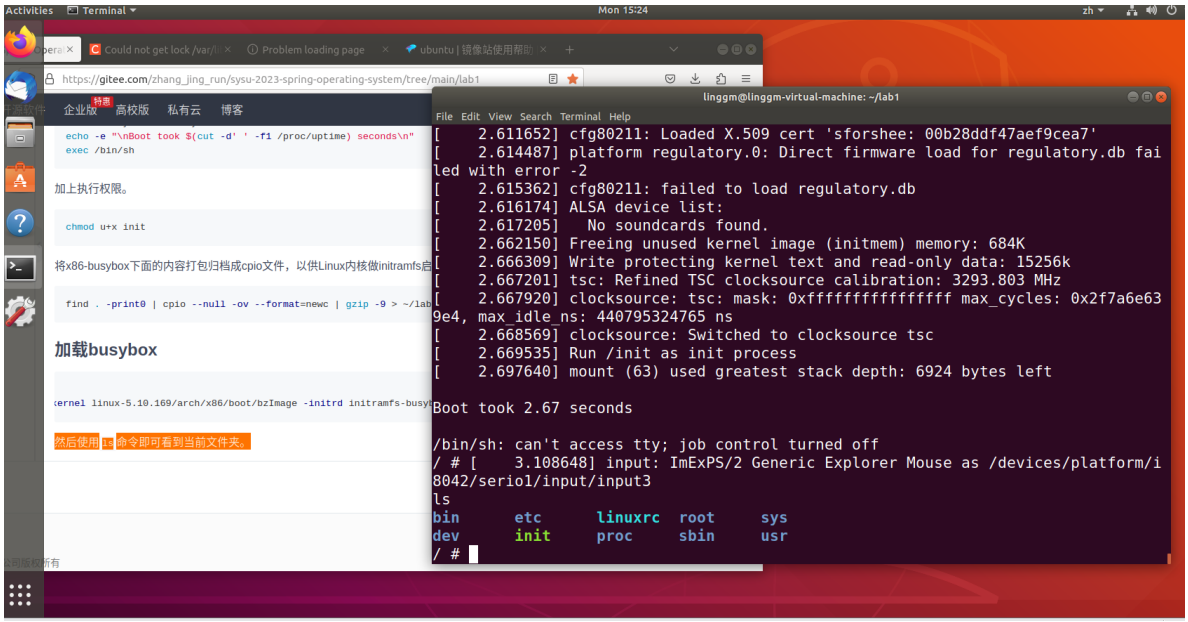


- 制作 initramfs



- 加载 busybox

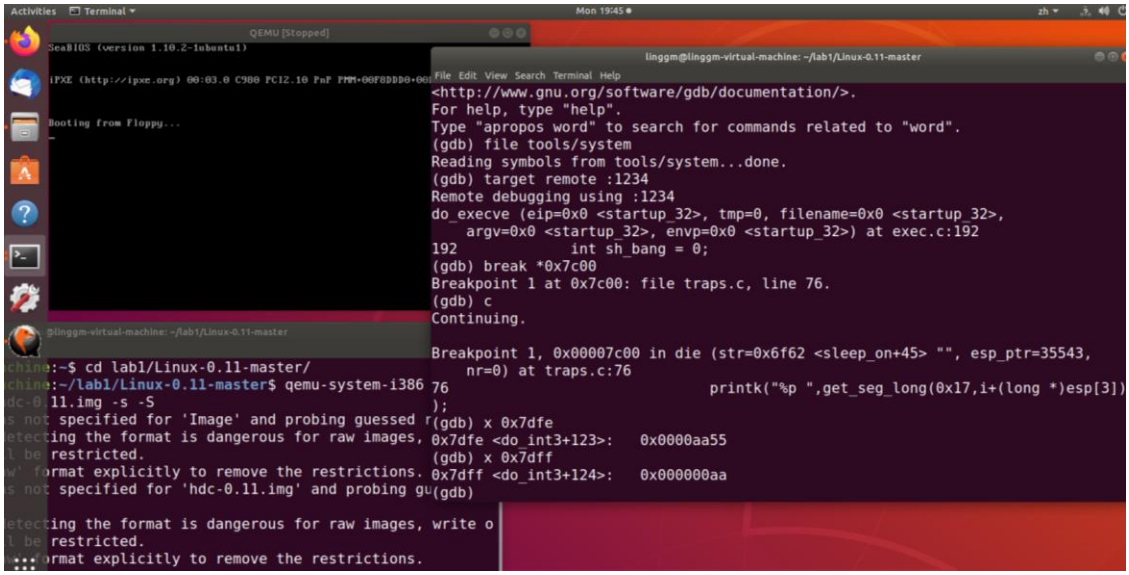




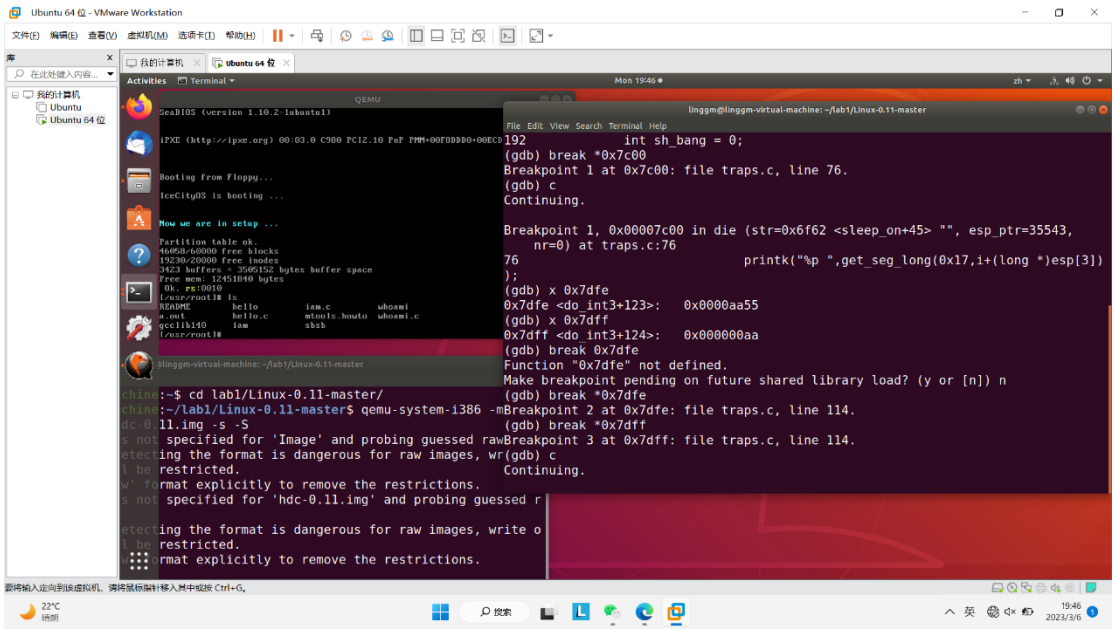
8）下载 Linux0.11 内核并编译，注意修改 Makefile

```
RAMDISK =  #-DRAMDISK=512

# This is a basic Makefile for setting the g
include Makefile.header

LDFLAGS += -Ttext 0 -e startup_32
CFLAGS  += $(RAMDISK) -Iinclude -g -m32
CPP     += -Iinclude
```

9）使用 qemu-system-i386 加载，启动内核



10） 使用 gdb 进行远程调试

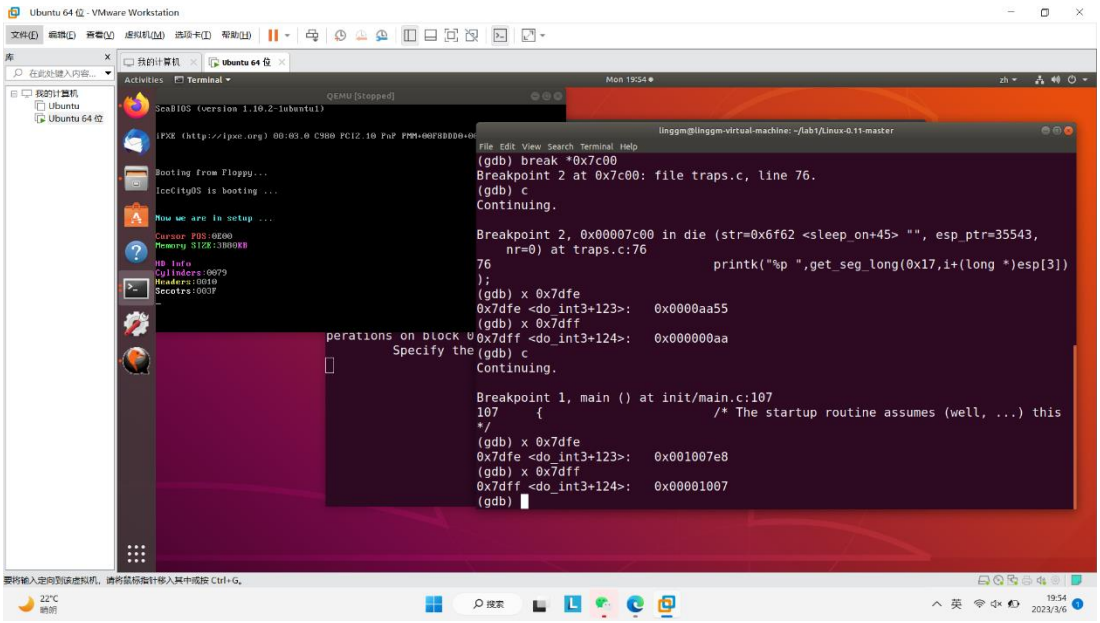


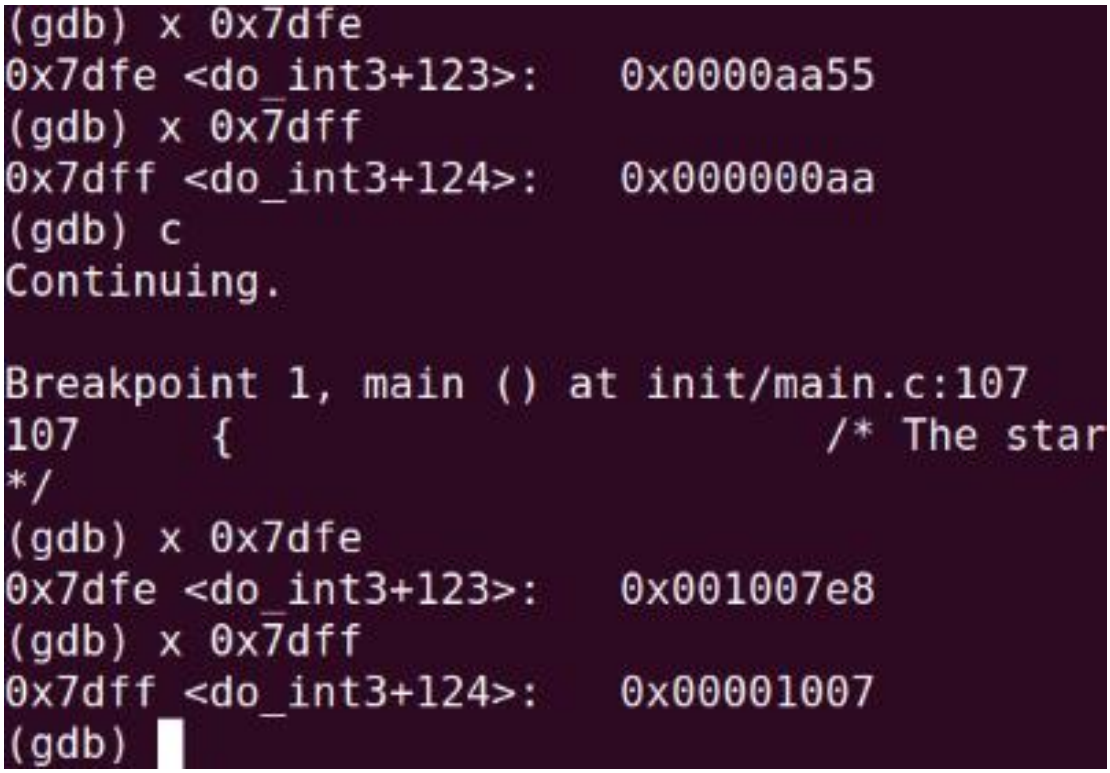
先 file/tools/system 加载符号表

再 target remote :1234 连接 qemu

再 set disassembly-flavor intel

然后 break 设置断点，最后输入 c 运行

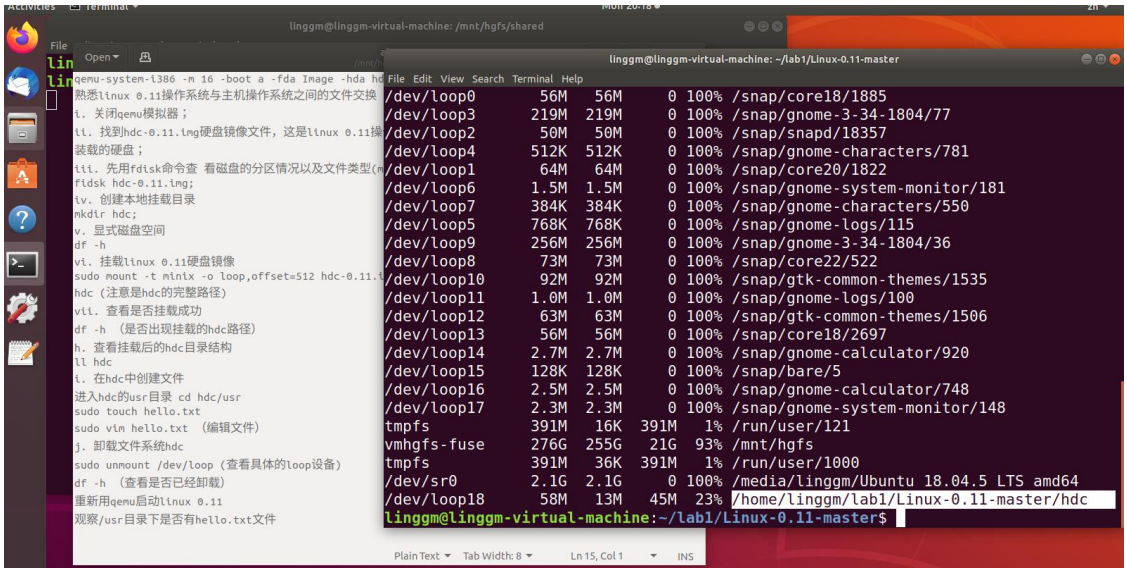




0x7DFE 和 0x7DFF 的不同阶段的内容如上图

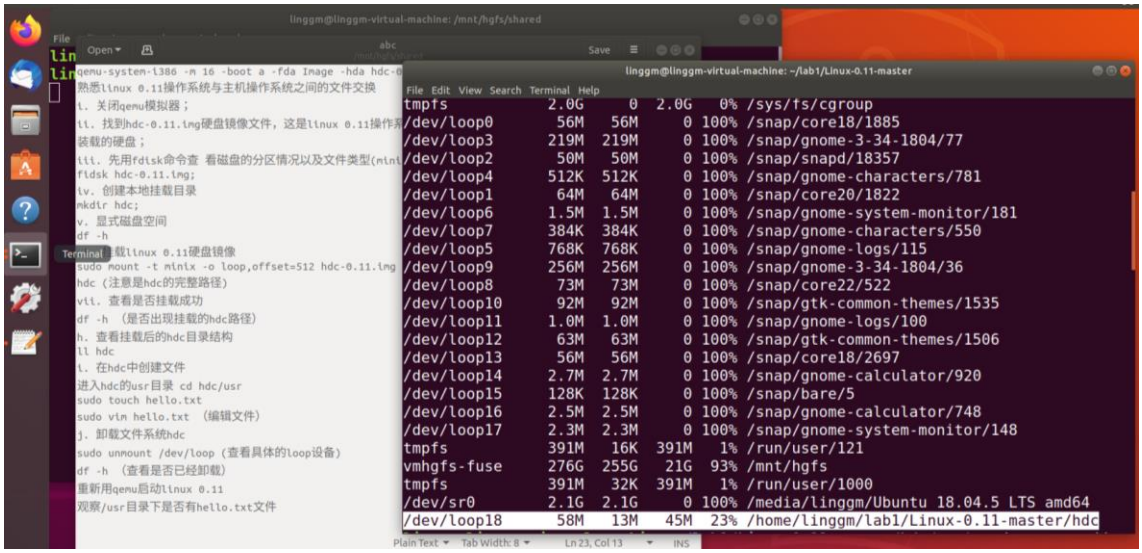
11） 熟悉 Linux0.11 操作系统与主机操作系统的文件交换

- 关闭 qemu，找到硬盘镜像文件，创建本地挂载目录

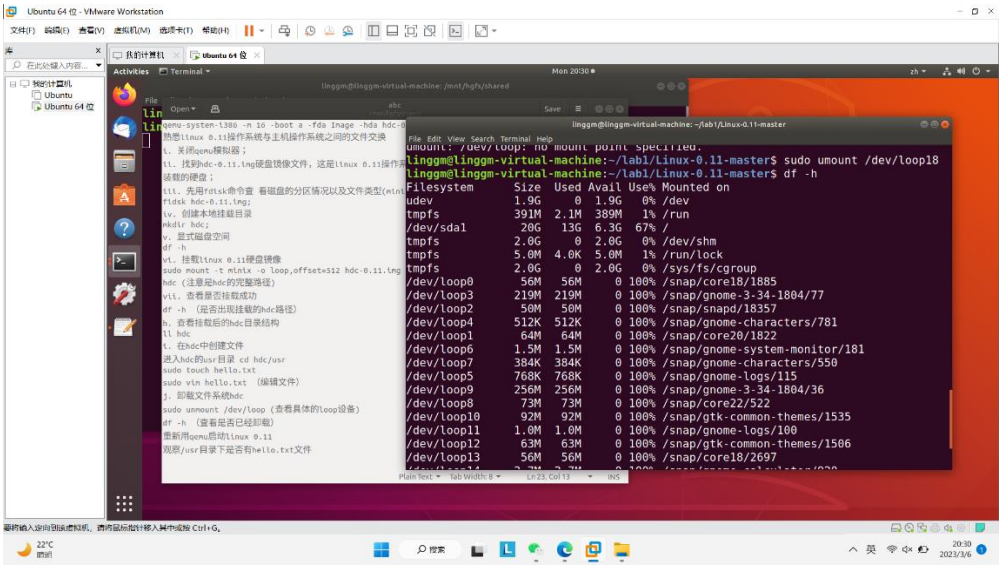


Loop18 中有 hdc 的路径，挂载成功

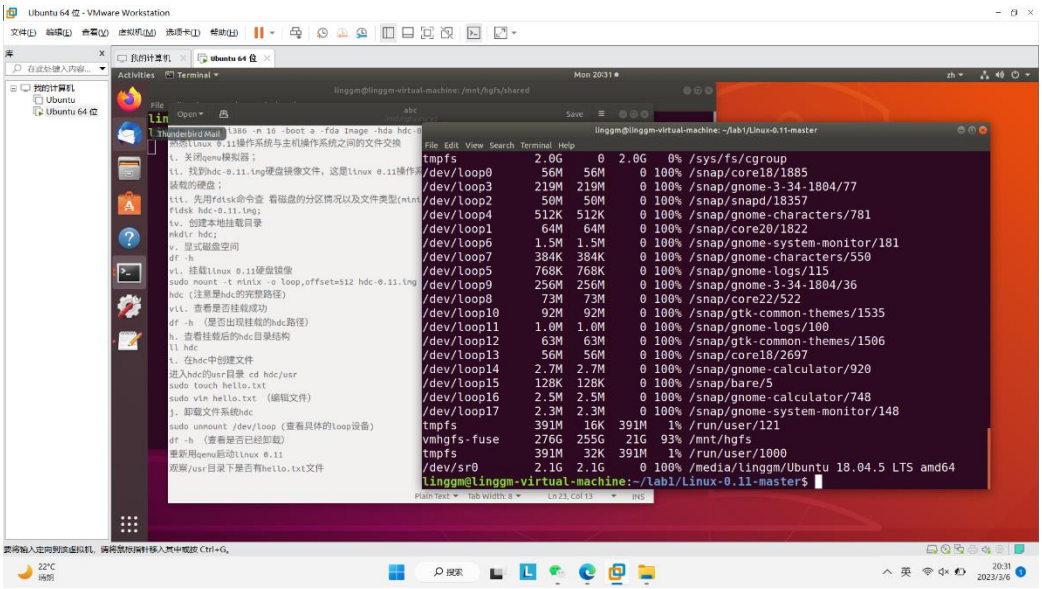
- 在 hdc/src 中创建 hello.txt 文件
- 卸载文件系统 hdc



卸载前如上图

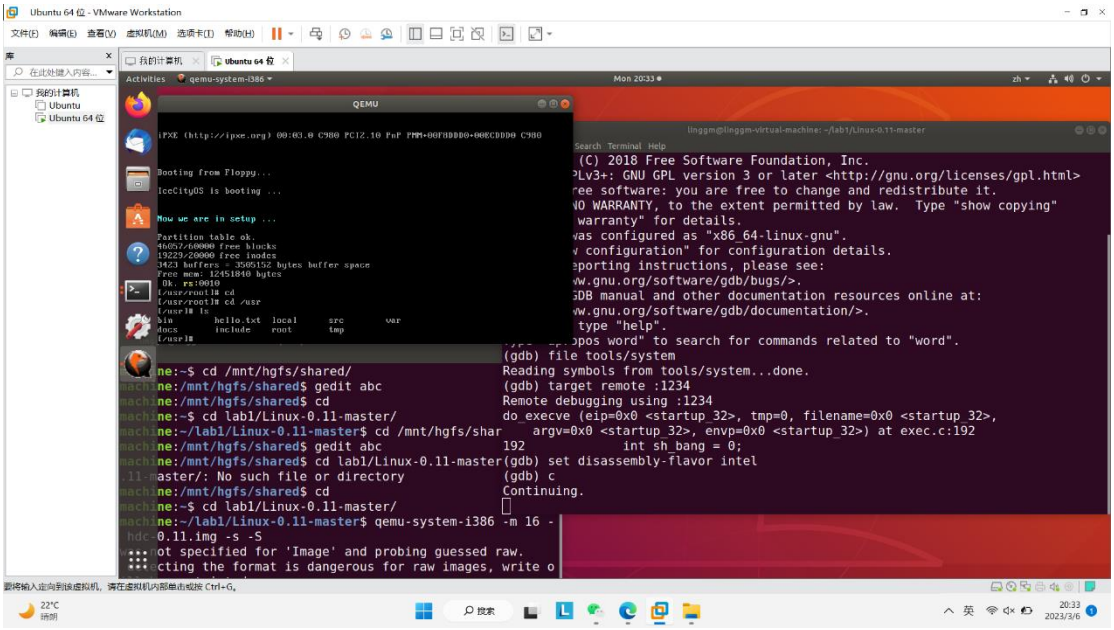


输入卸载指令

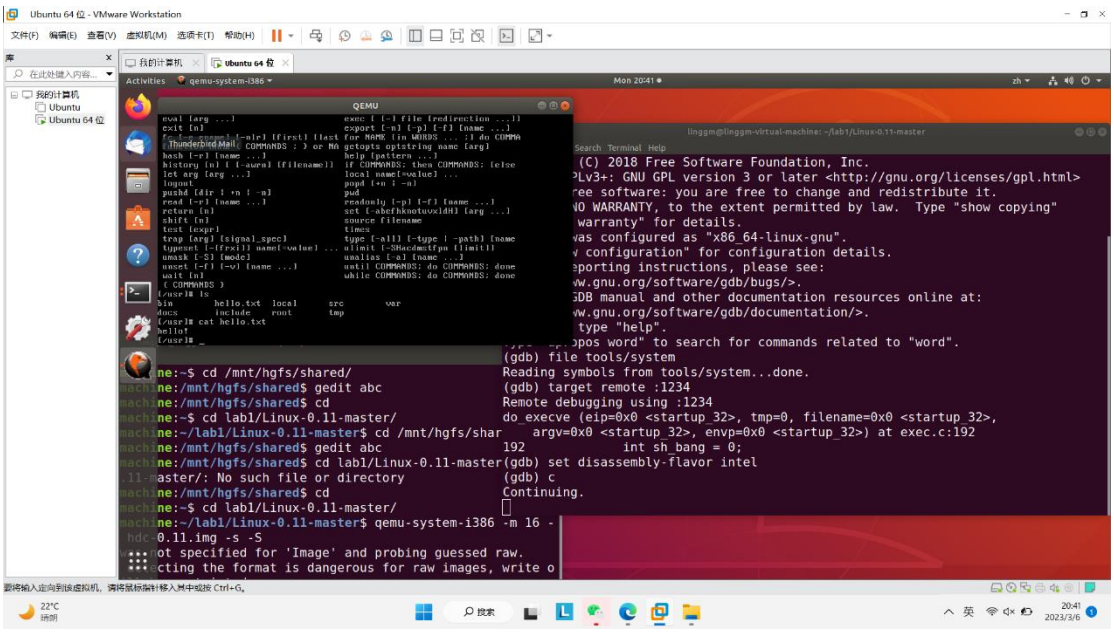


卸载后，有 hdc 路径的 loop18 消失

- 打开 qemu，启动 gdb，打开 qemu 中的 src



发现 src 中确实存在 hello.txt 文件，完成文件交换



在 qemu 中用 cat 指令输出 hello.txt 中的内容，成功