

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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

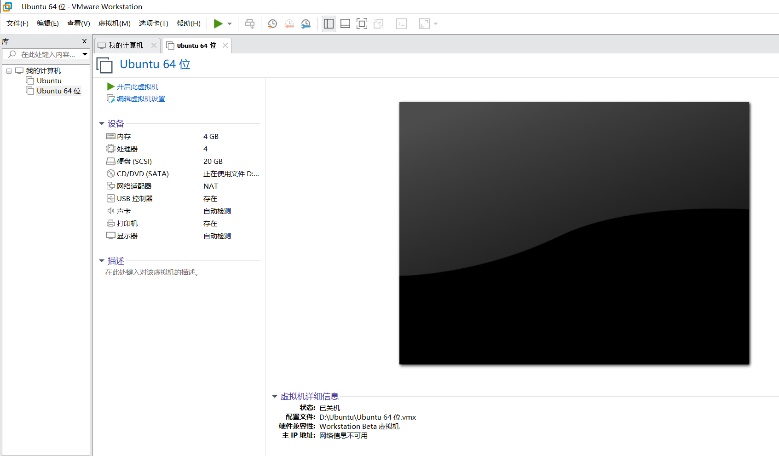
实验成绩:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

报告时间:\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023.03.06\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

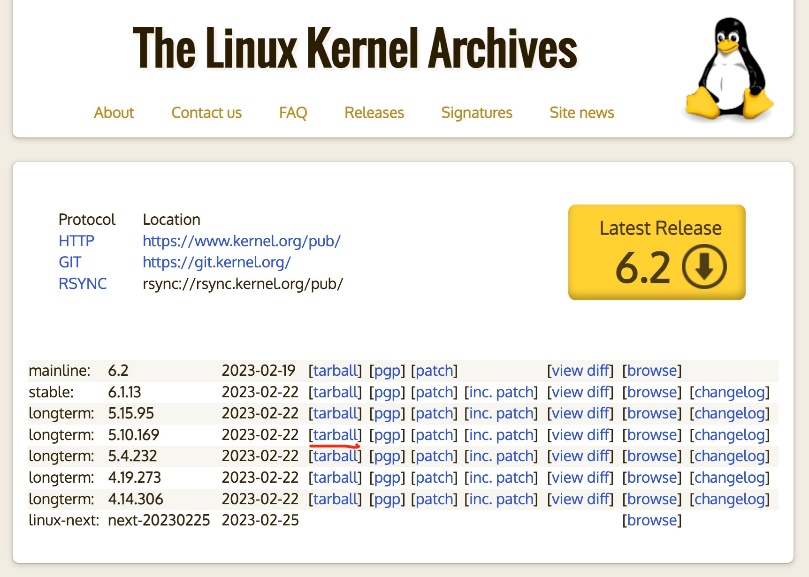
1. **实验要求**

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。

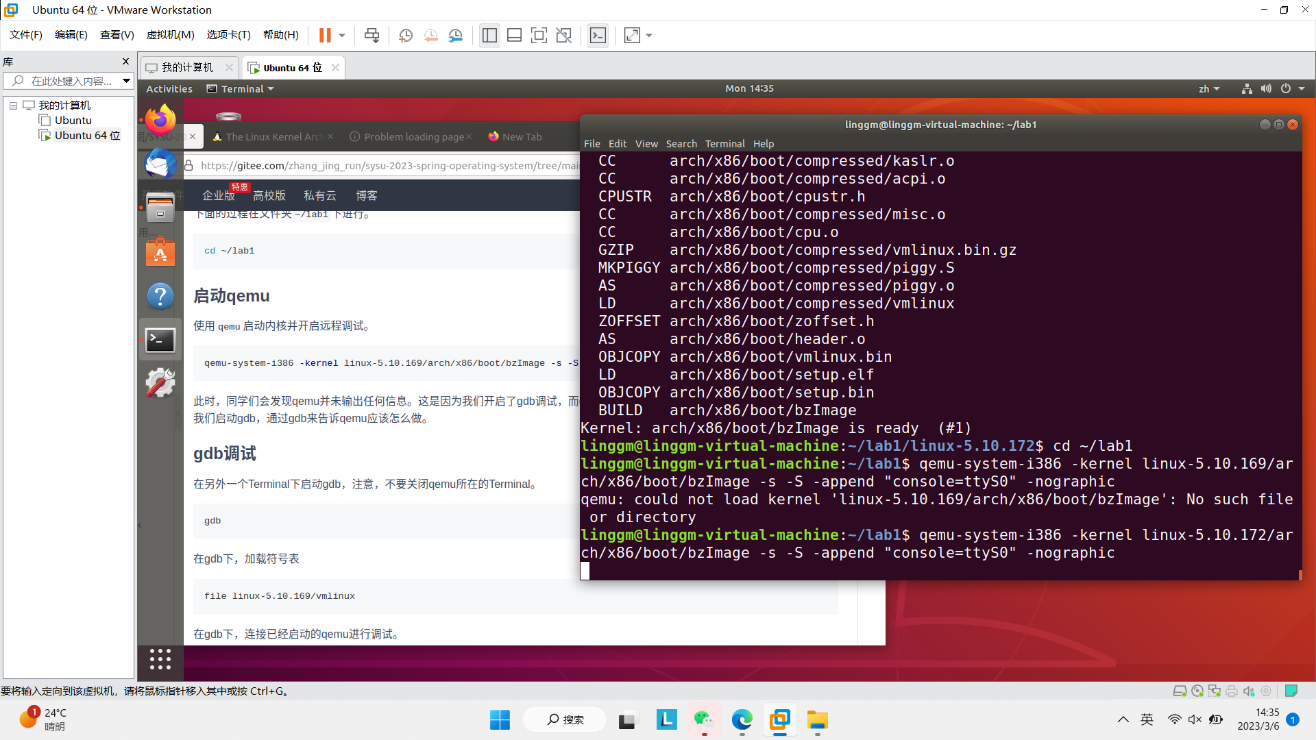
1. 搭建OS内核开发环境包括：代码编辑环境、编译环境、运行环境、调试环境等。
2. 下载并编译i386（32位）内核，并利用qemu启动内核。
3. 熟悉制作initramfs的方法。
4. 编写简单应用程序随内核启动运行。
5. 编译i386版本的Busybox，随内核启动，构建简单的OS。
6. 开启远程调试功能，进行调试跟踪代码运行。
7. 撰写实验报告。
8. **实验过程**
9. 环境配置，下载Vmware，安装Ubuntu虚拟机，换源。



1. 配置C/C++环境，安装其他工具
2. 下载了Linux5.10.172，并编译Linux内核

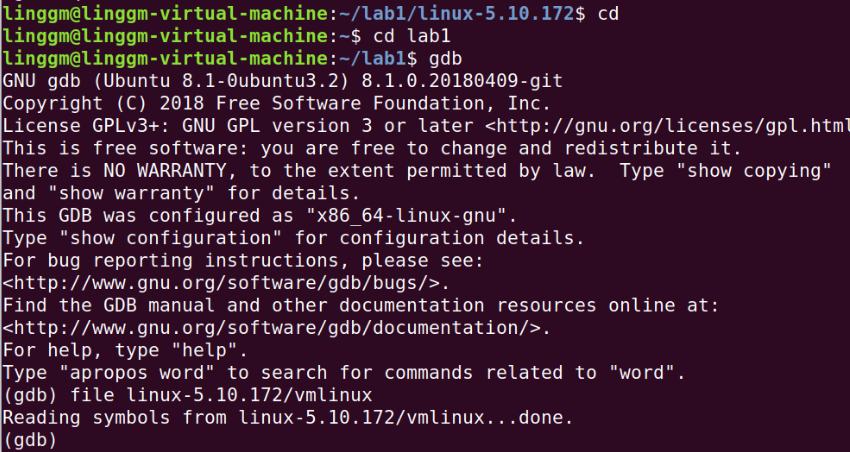


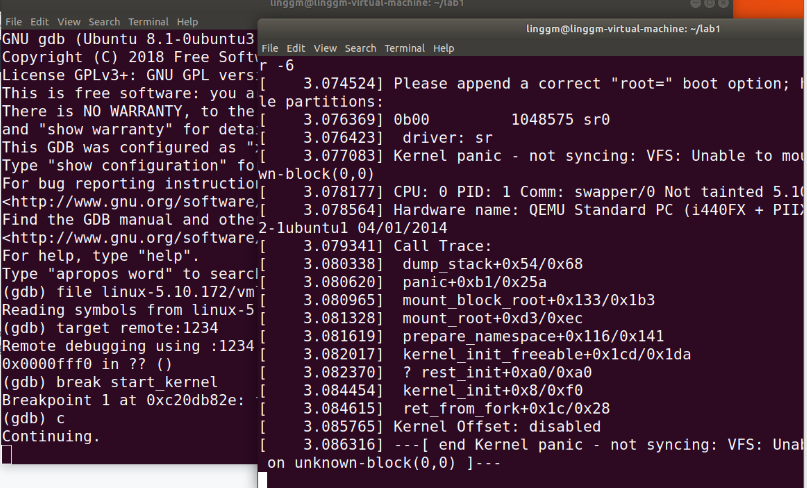
1. 启动内核并调试，使用qemu启动内核，开启远程调试



1. 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



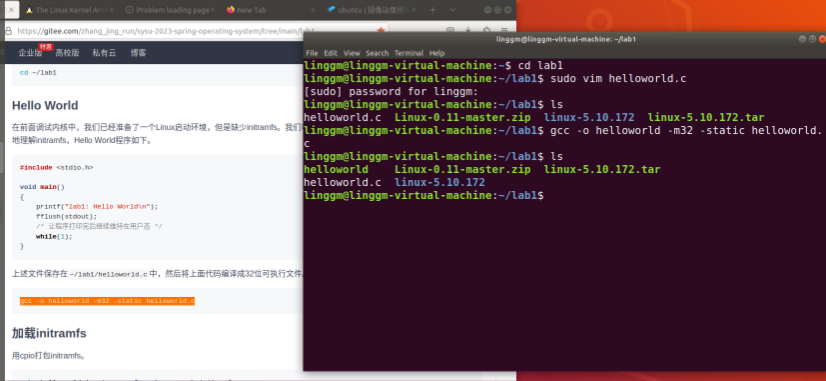


1. 制作Initramfs

* Hello World

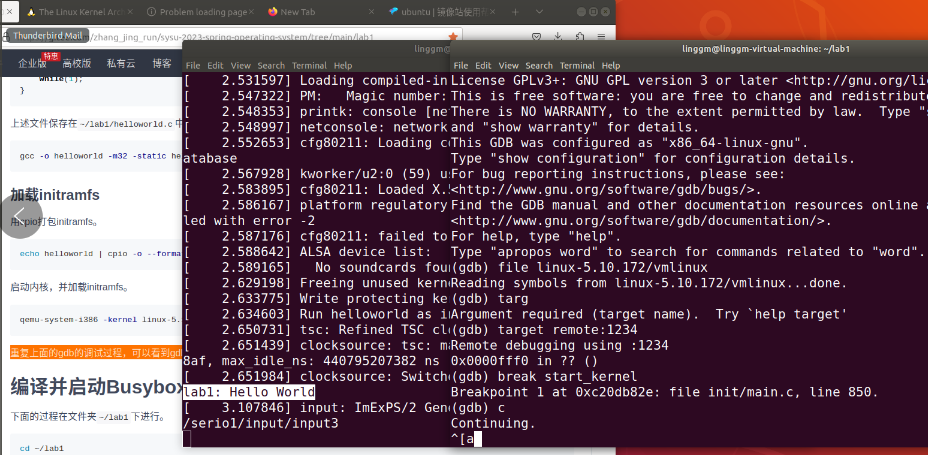
用vim写一个HelloWorld.c程序，利用gcc工具将这段代码编译成32位可执行文件

gcc -o helloworld -m32 -static helloworld.c



* 加载initramfs

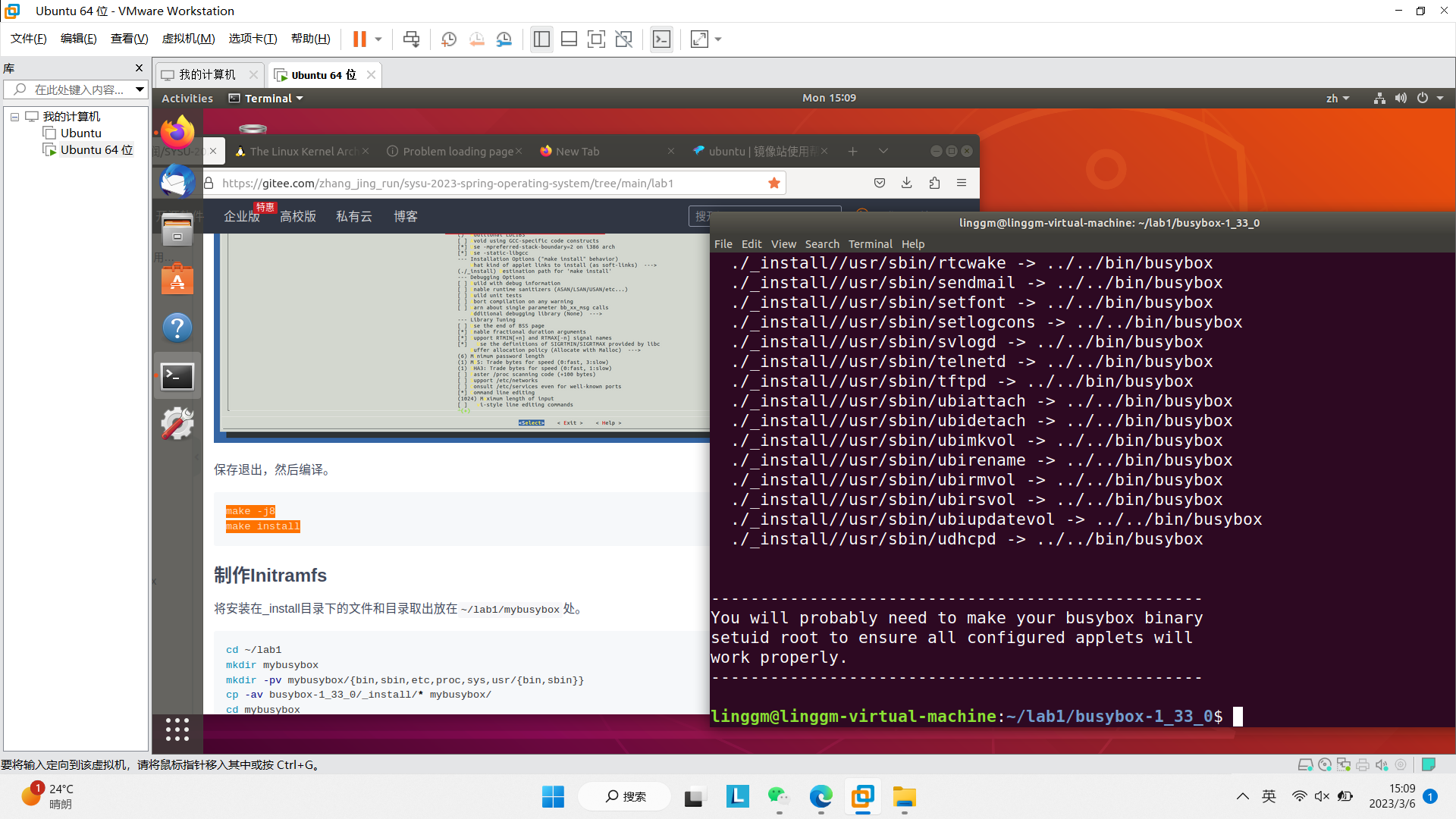
用cpio打包initramfs，启动内核并加载initramfs



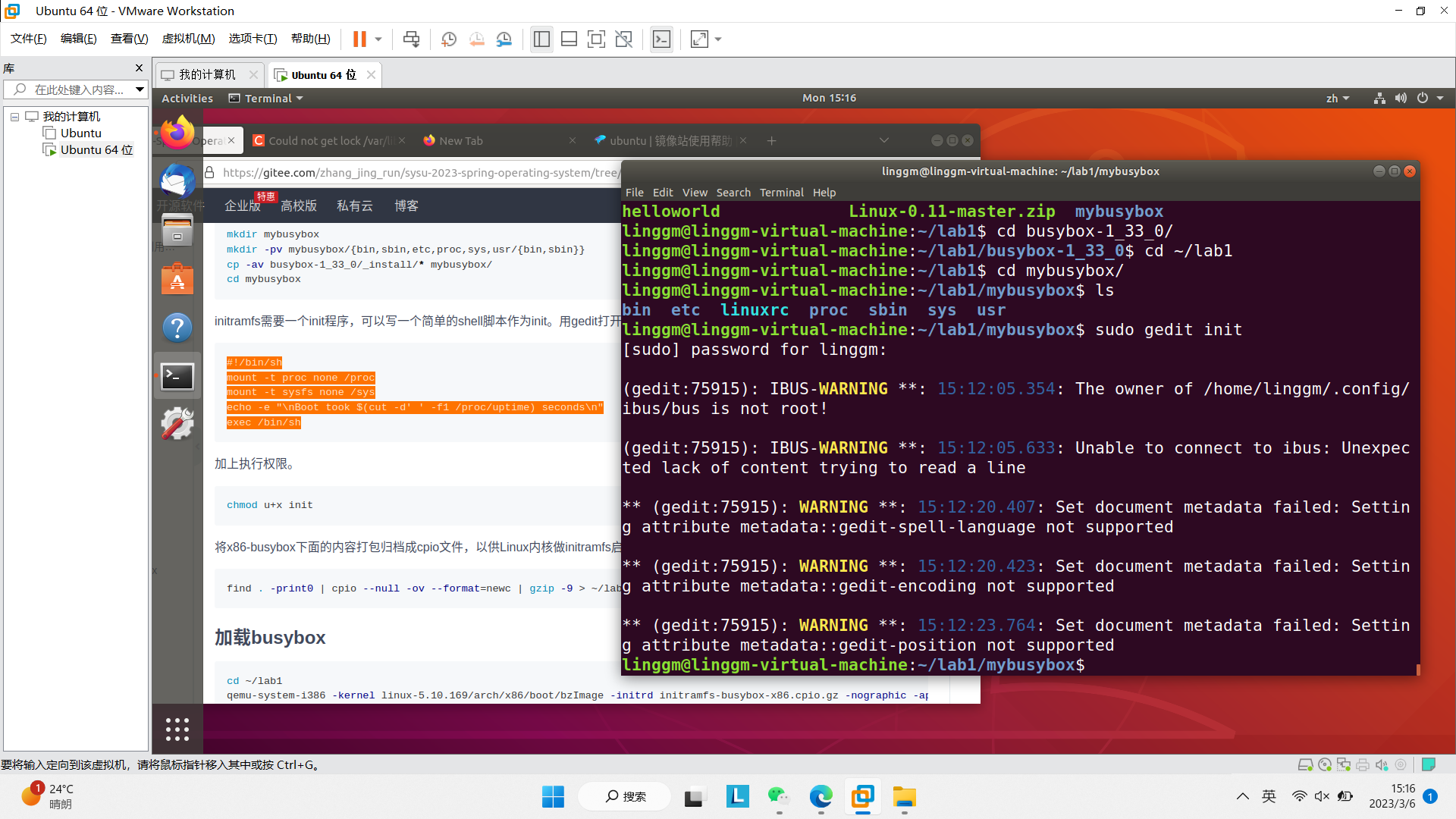
可以看到，按如上步骤，helloworld程序得以运行。

1. 编译并启动busybox

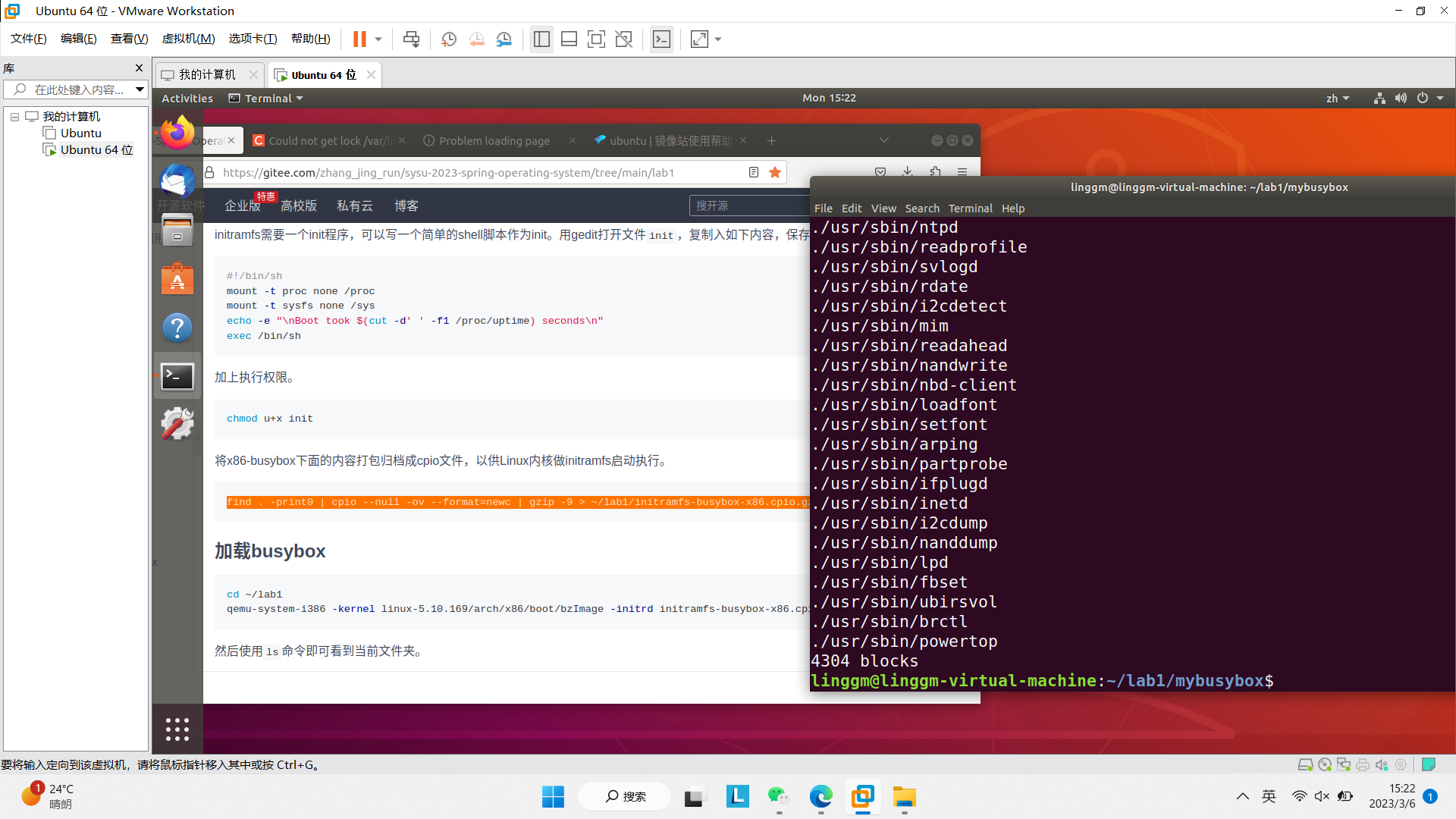
* 下载，解压，编译

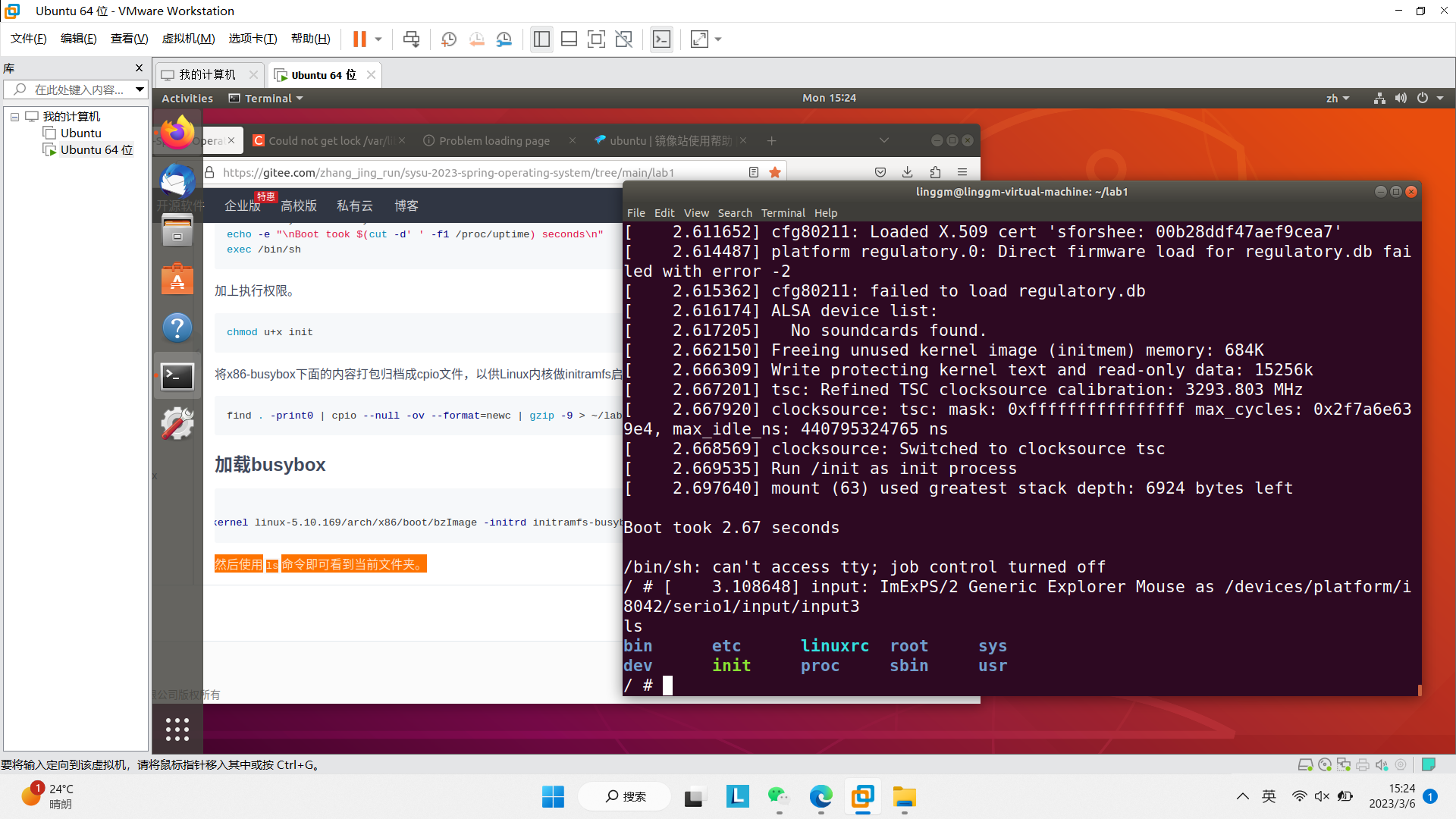


* 制作initramfs

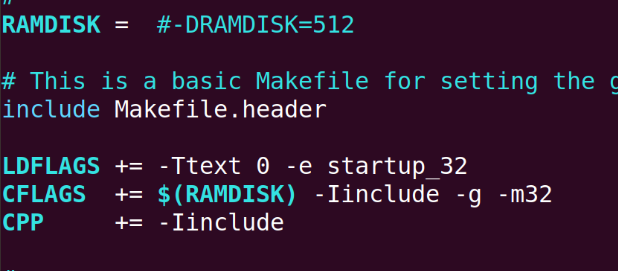


* 加载busybox

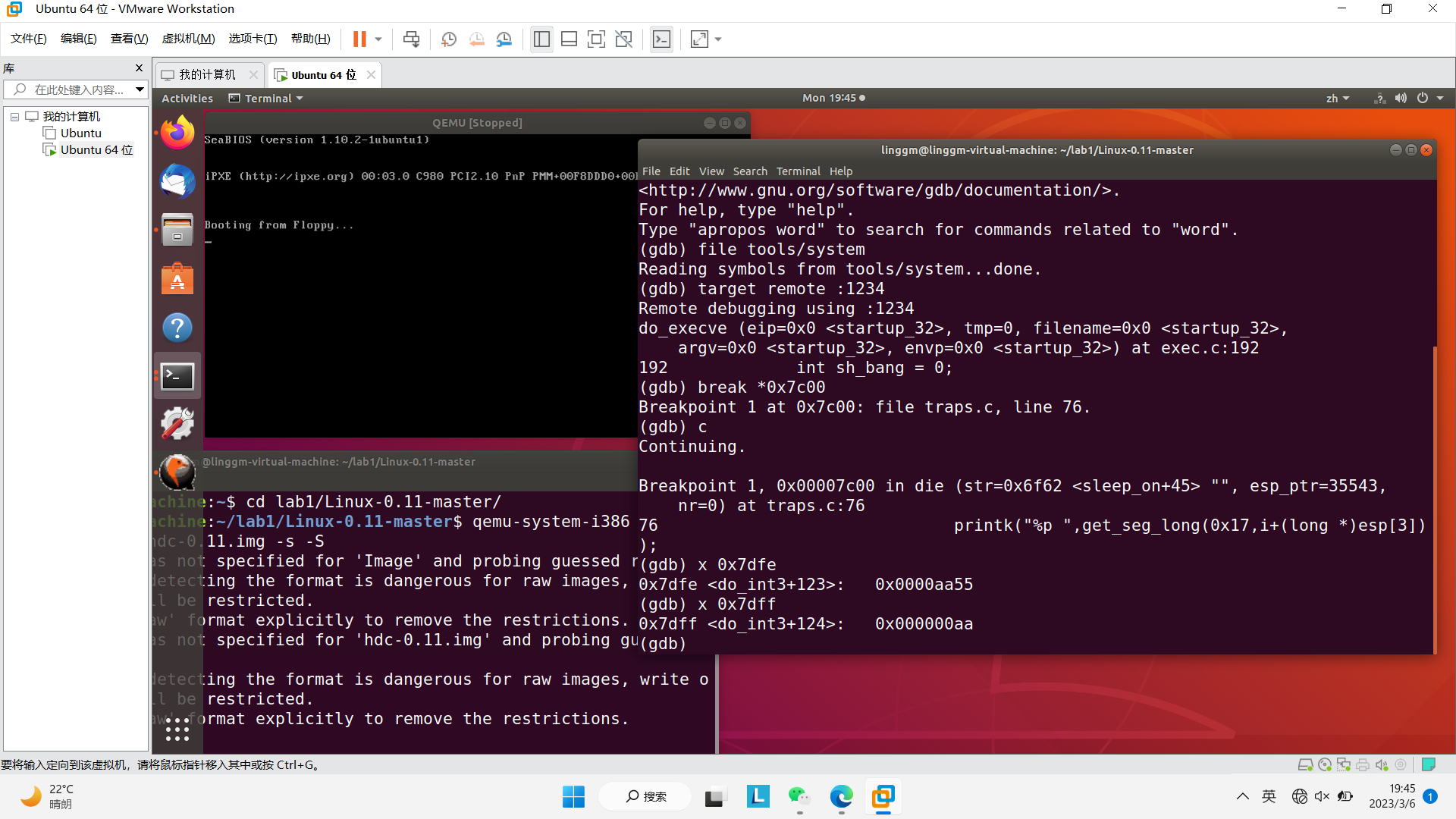




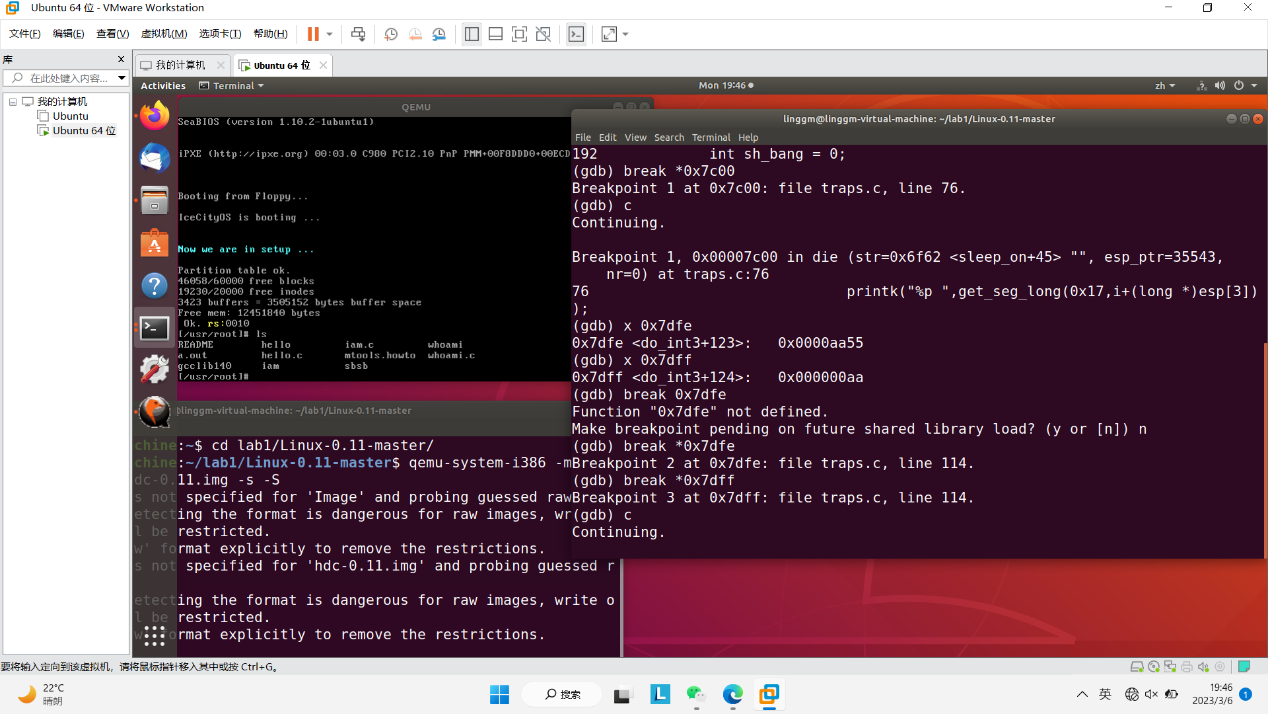
1. 下载Linux0.11内核并编译，注意修改Makefile



1. 使用qemu-system-i386加载，启动内核



1. 使用gdb进行远程调试

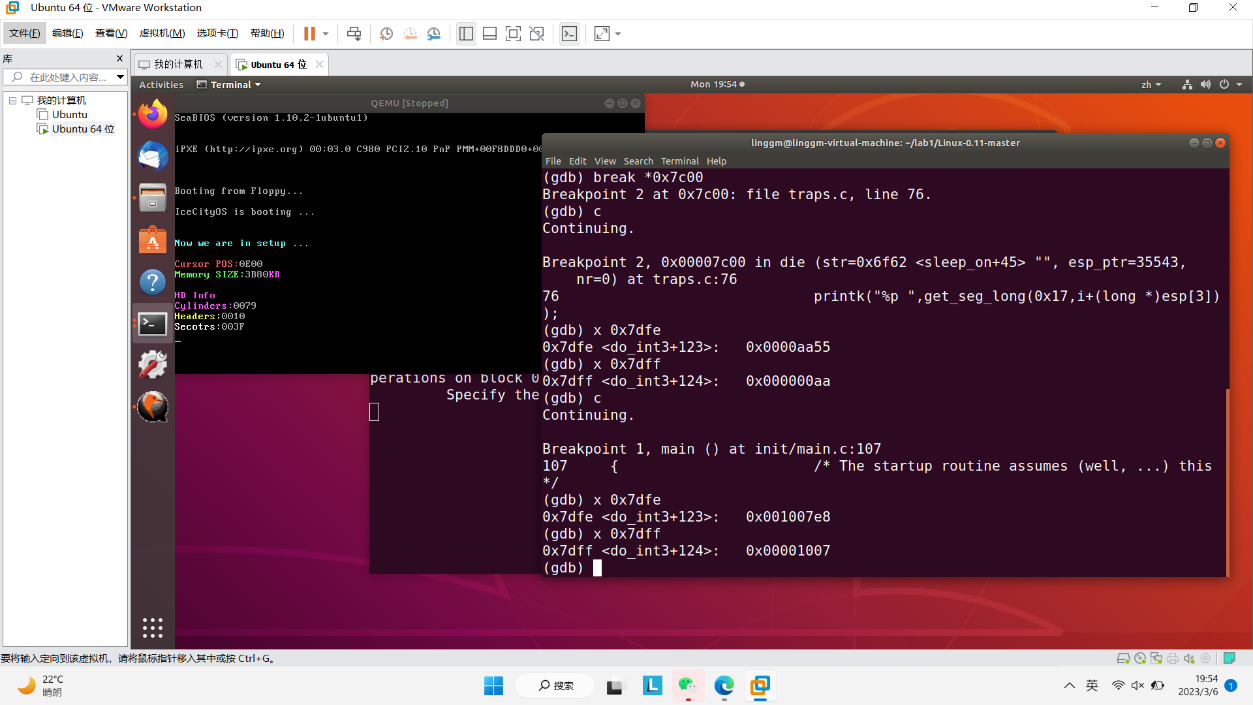


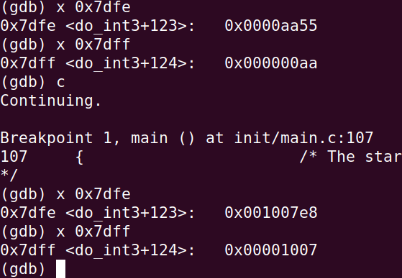
先file/tools/system加载符号表

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

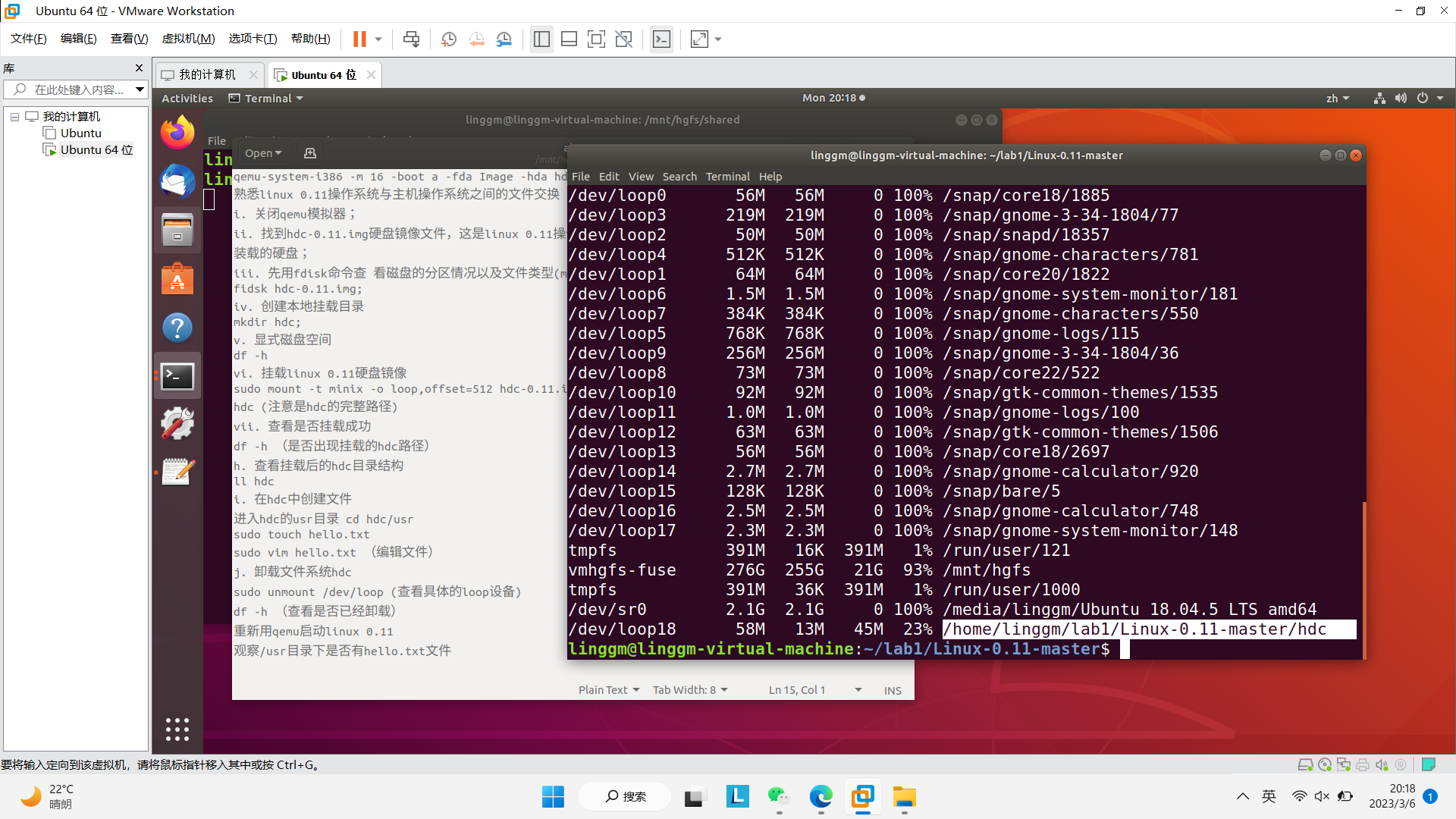




0x7DFE 和 0x7DFF 的不同阶段的内容如上图

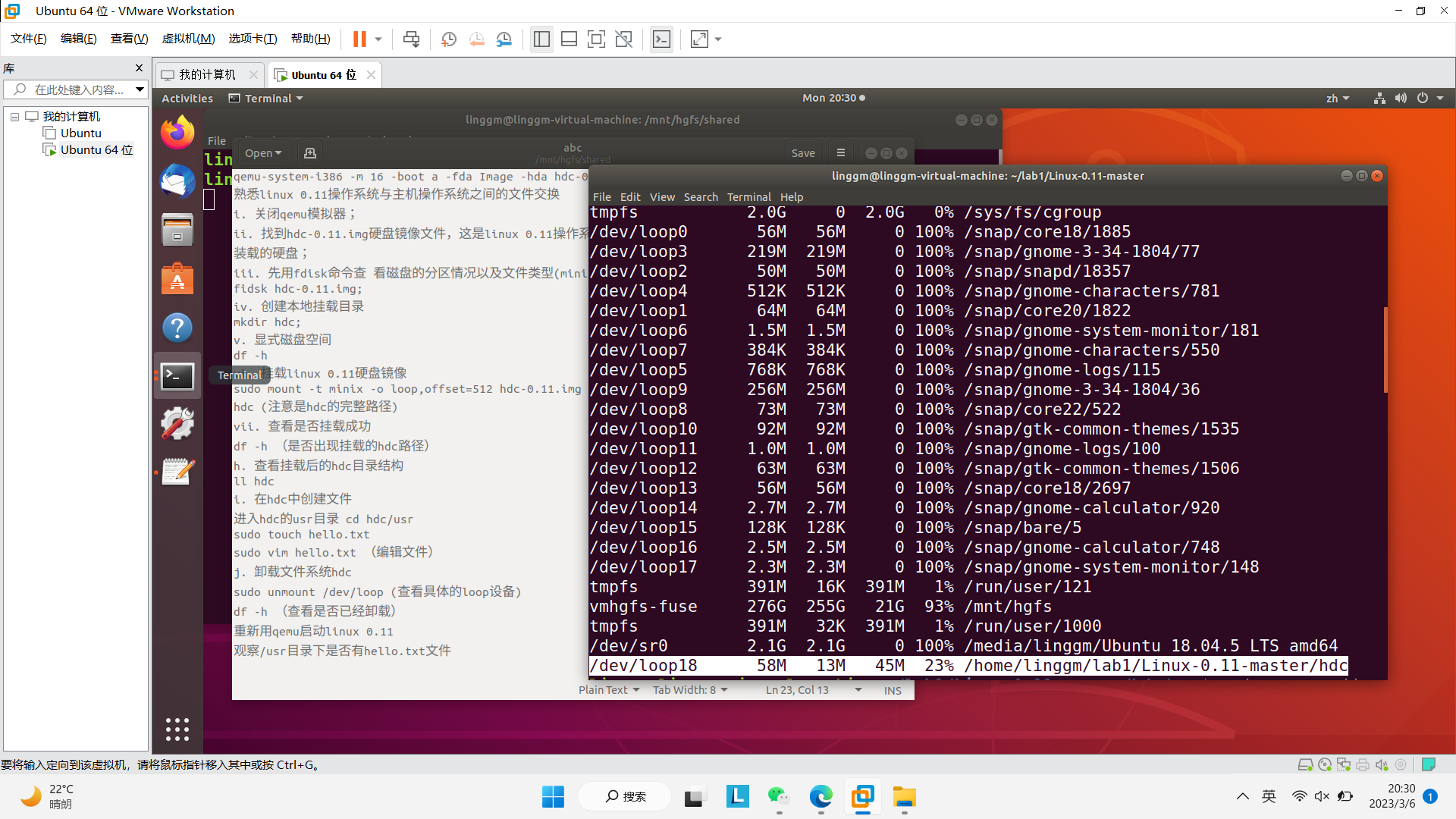
1. 熟悉Linux0.11操作系统与主机操作系统的文件交换

* 关闭qemu，找到硬盘镜像文件，创建本地挂载目录

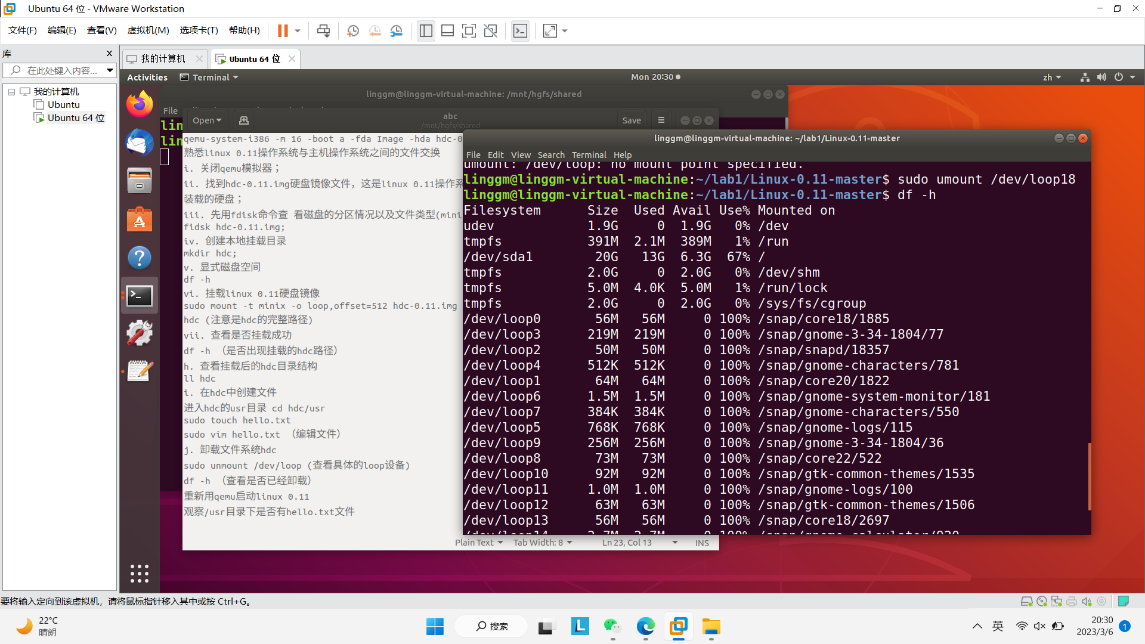


Loop18中有hdc的路径，挂载成功

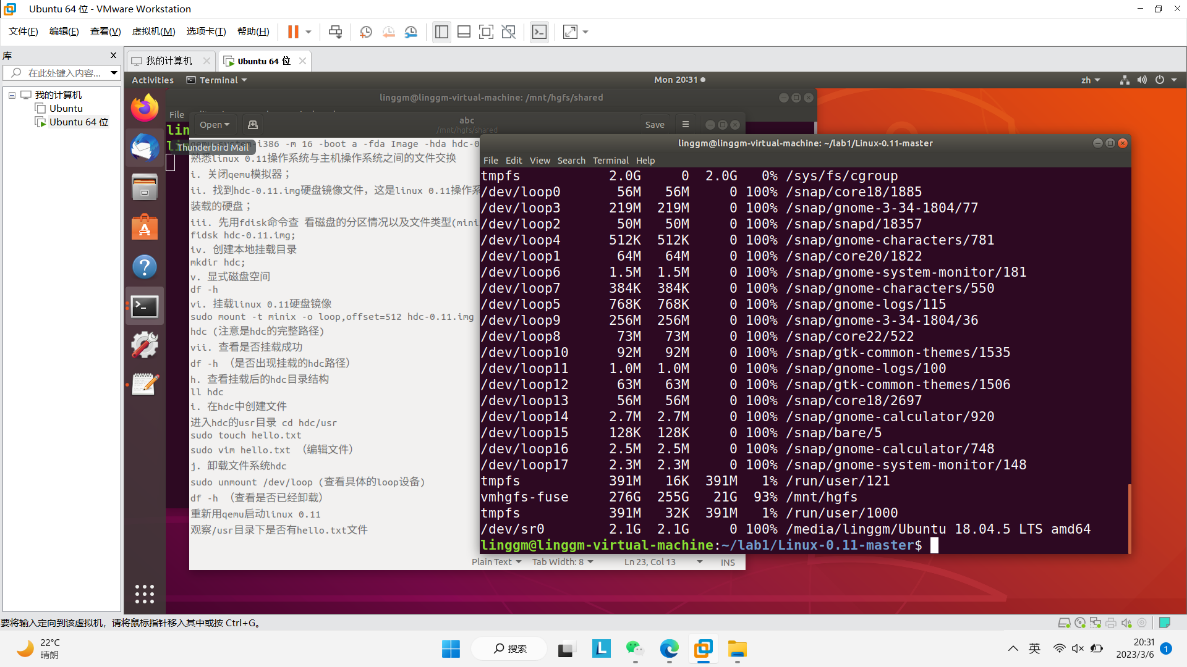
* 在hdc/src中创建hello.txt文件
* 卸载文件系统hdc



卸载前如上图

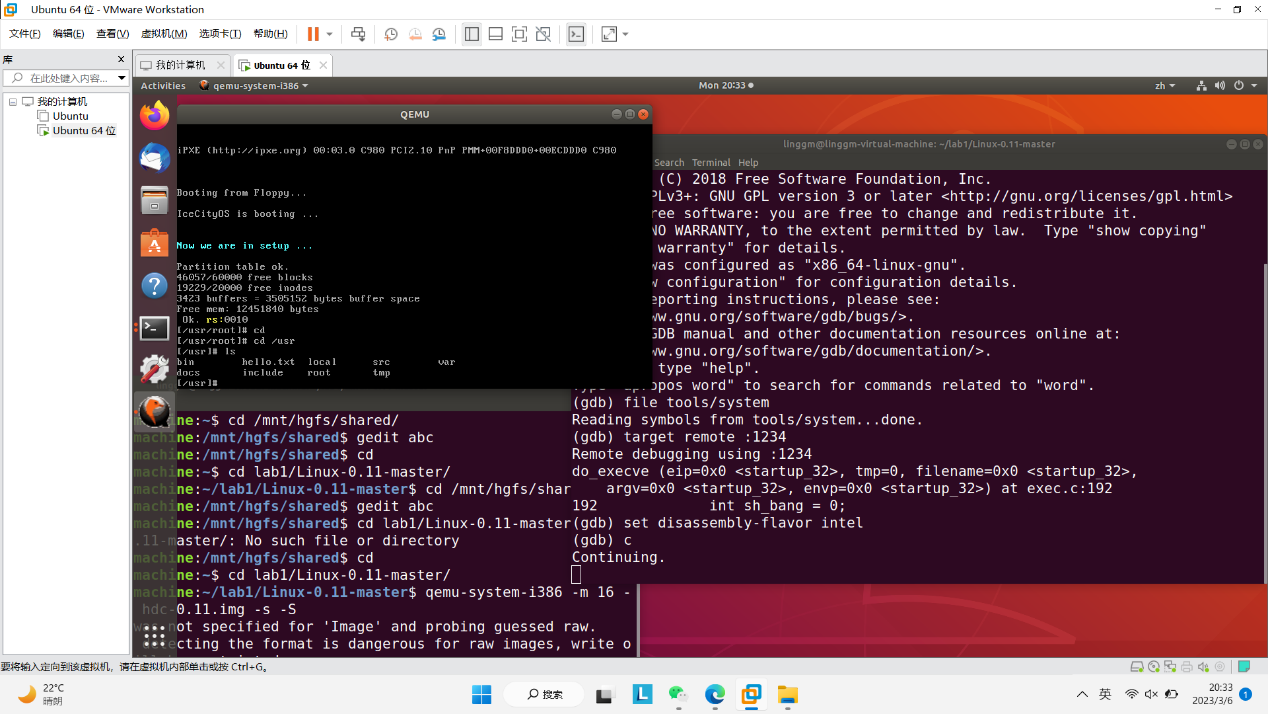


输入卸载指令

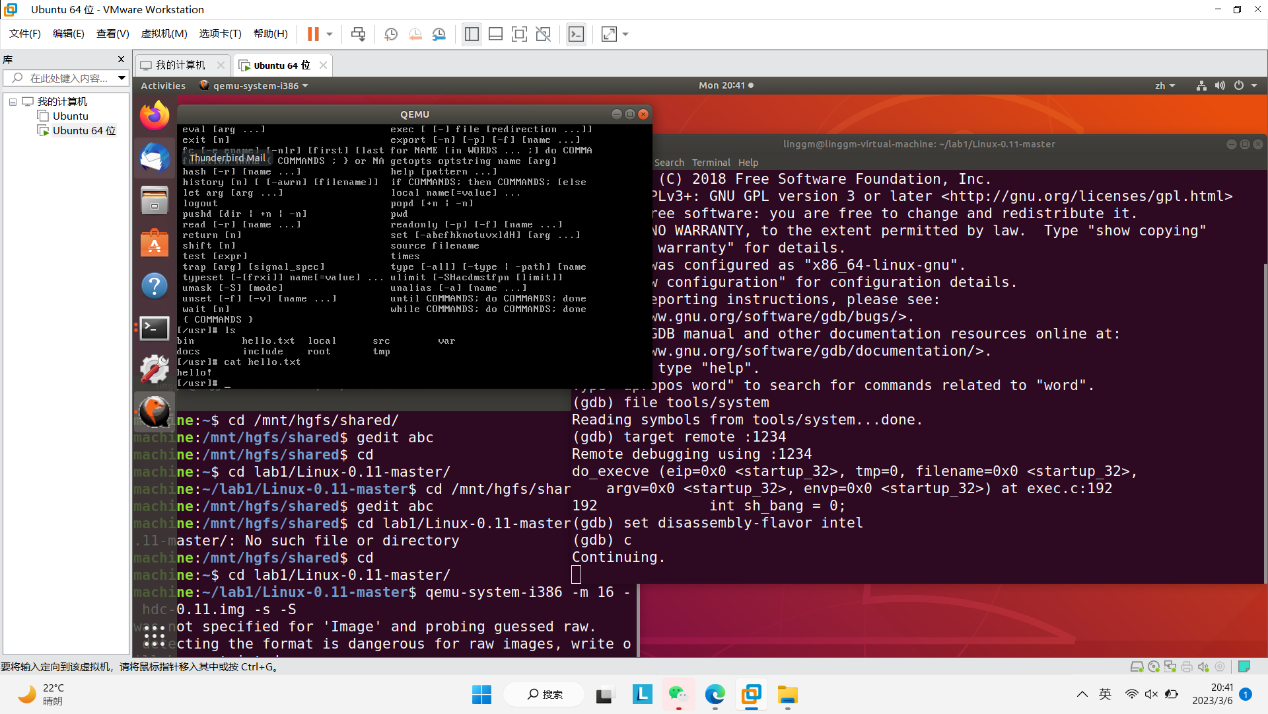


卸载后，有hdc路径的loop18消失

* 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