

**本科实验报告**

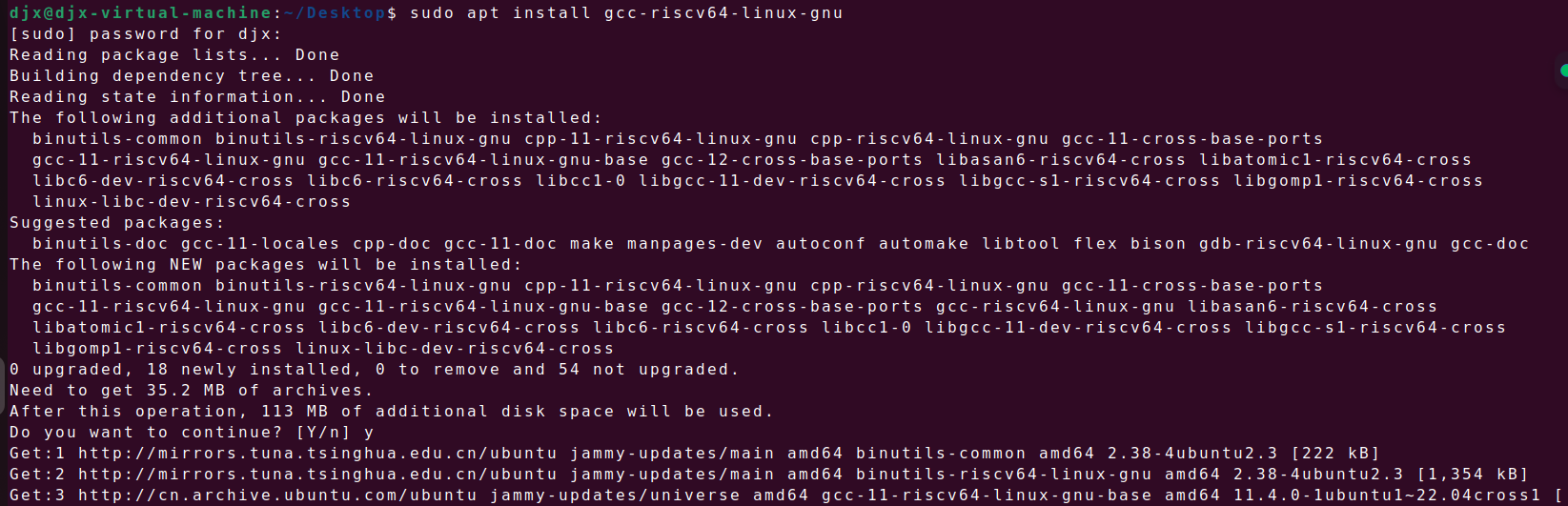
|  |  |
| --- | --- |
| 课程名称： | 操作系统 |
| 姓 名： | 董佳鑫 |
| 学 院： | 计算机学院 |
| 系： | 计算机系 |
| 专 业： | 计算机科学与技术 |
| 学 号： | 3210102181 |
| 指导教师： | 寿黎但 |

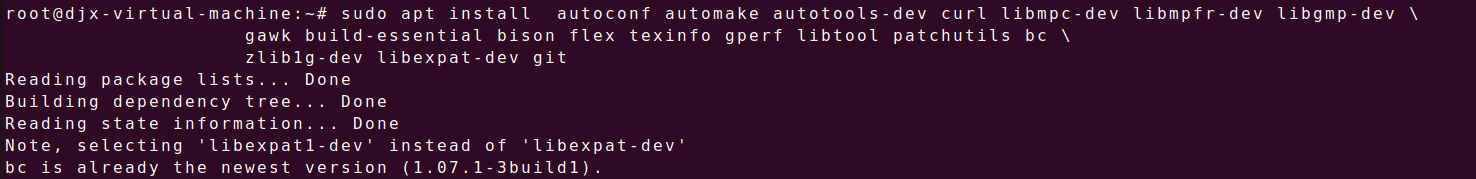
# Lab 0: GDB & QEMU 调试64位 RISC-V LINUX

实验过程和操作步骤

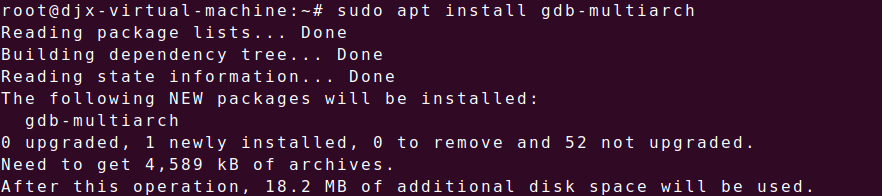
我使用的是基于VMware的ubantu系统，所有命令都在该Linux系统终端执行。

根据实验指导手册，首先安装编译内核所需要的交叉编译工具链和用于构建程序的软件包，以及启动 riscv64 平台上的内核的模拟器 qemu和GDB调试器。

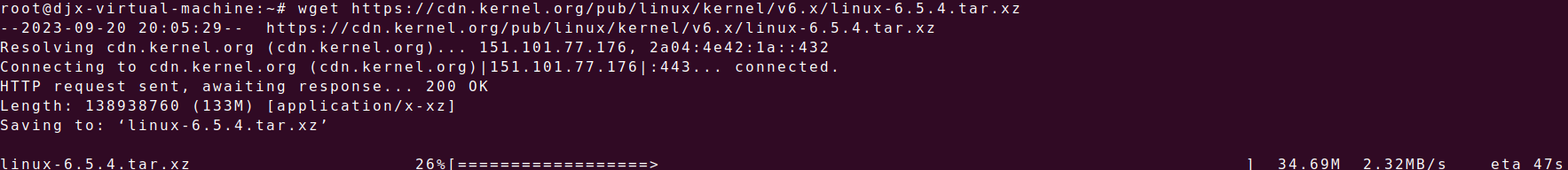




06dfece7424f5972f225f37a23be39b



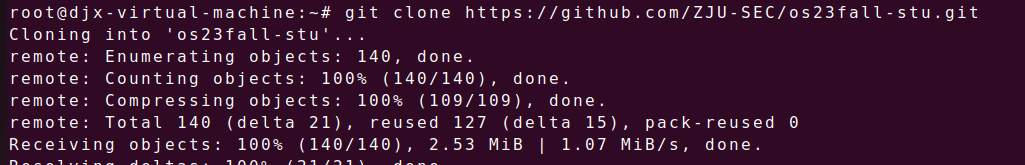
在下载好所需的实验环境后，接下来下载Linux内核源码，这里使用wget命令进行下载。



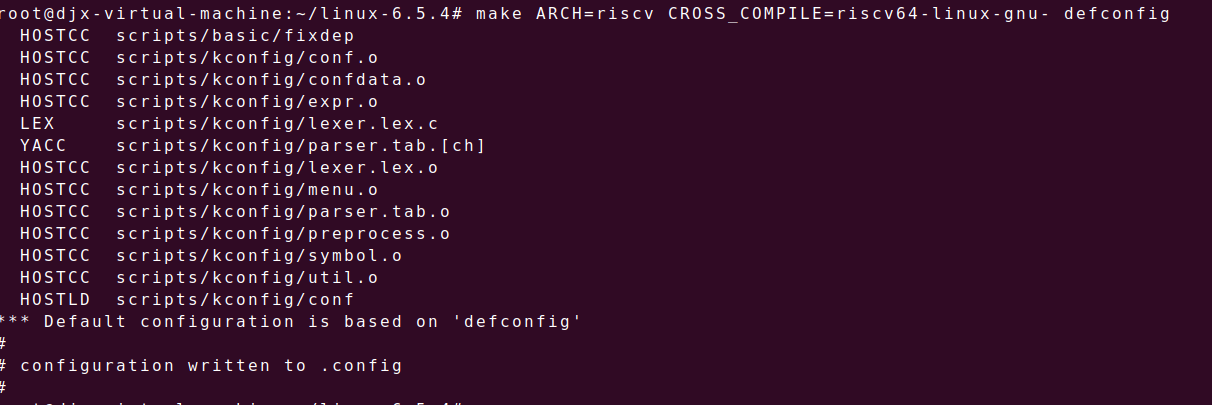
下载完成以后将xz文件进行解压，使用tar命令。

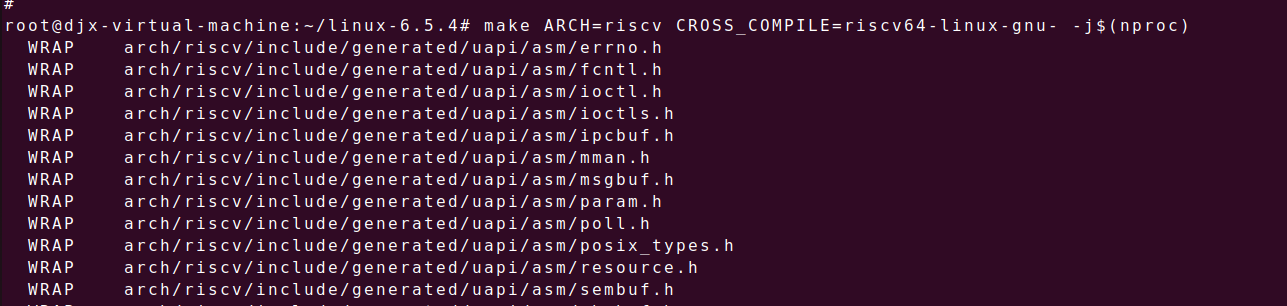
fbda4b0f76049f0fc91a0a489e67240

然后使用git命令将仓库克隆到Linux本地。

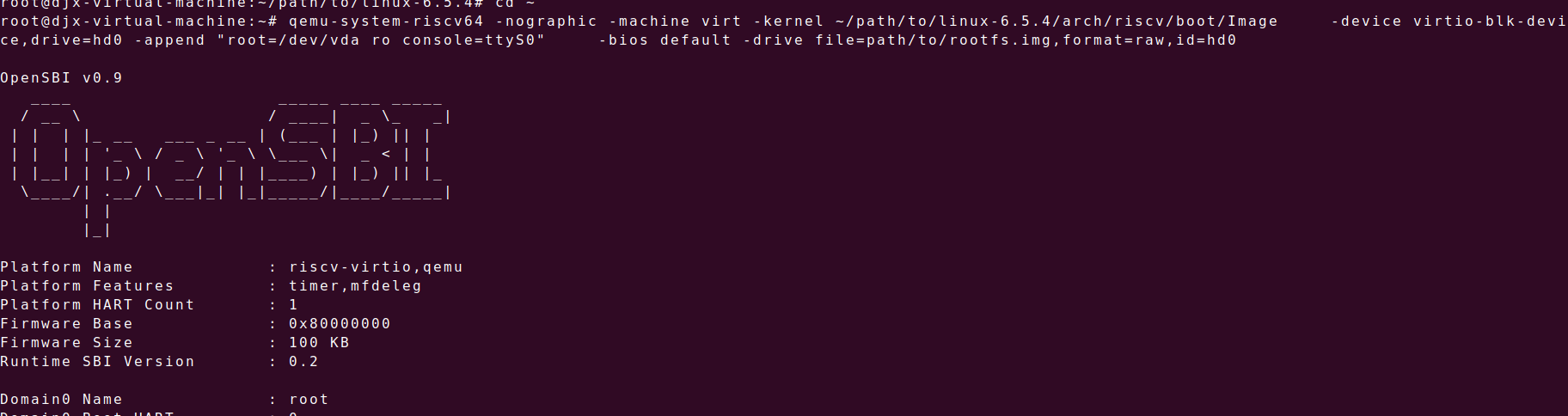


成功将根文件系统的镜像克隆到本地后，然后进入刚才下载好的Linux内核目录内，执行make命令进行编译。





编译完成后，我们使用qemu运行内核，可以看到Linux内核正常运行，证明编译正确。



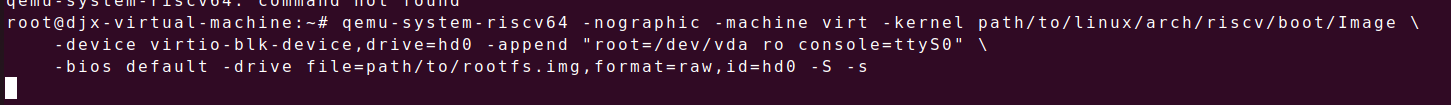
下一步，我们打开两个Linux终端，在第一个终端执行命令：

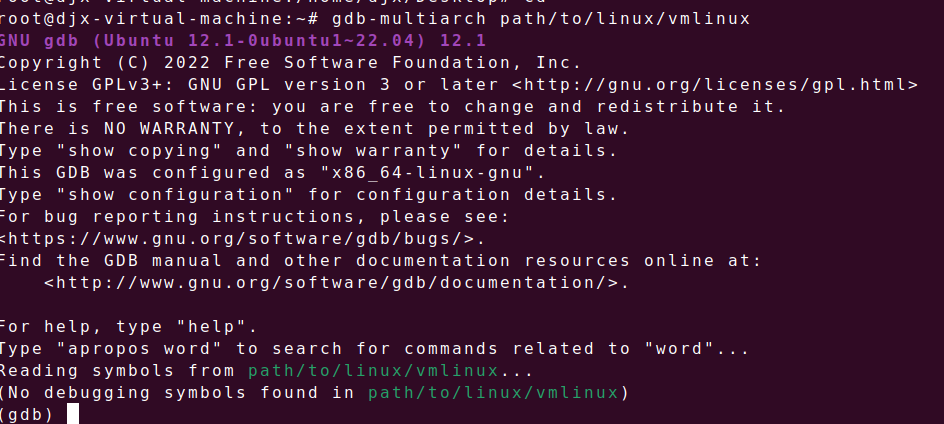
qemu-system-riscv64 -nographic -machine virt -kernel path/to/linux/arch/riscv/boot/Image \ -device virtio-blk-device,drive=hd0 -append "root=/dev/vda ro console=ttyS0" \ -bios default -drive file=path/to/rootfs.img,format=raw,id=hd0 -S -s

在第二个终端执行命令：

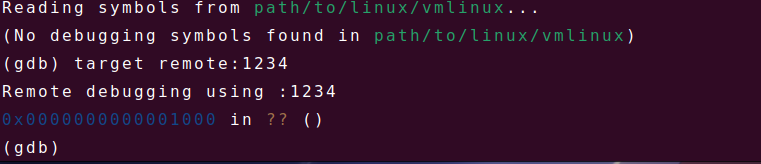
gdb-multiarch path/to/linux/vmlinux

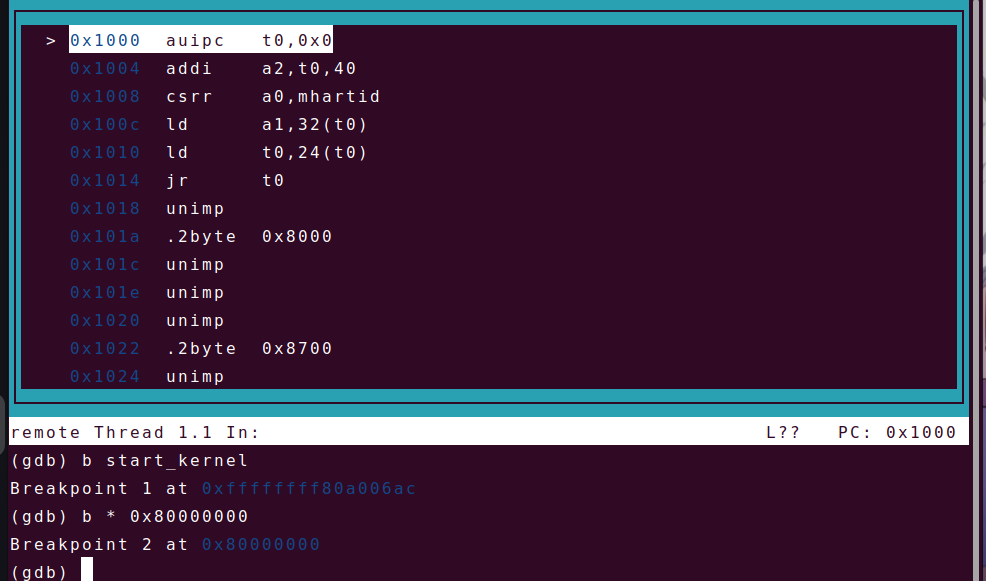
然后我们就可以在第二个终端内进行GDB调试。

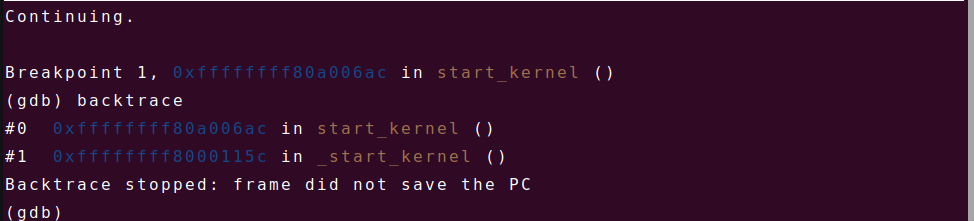


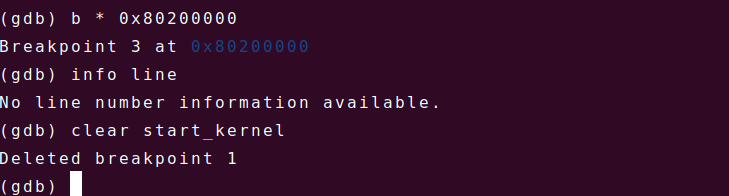


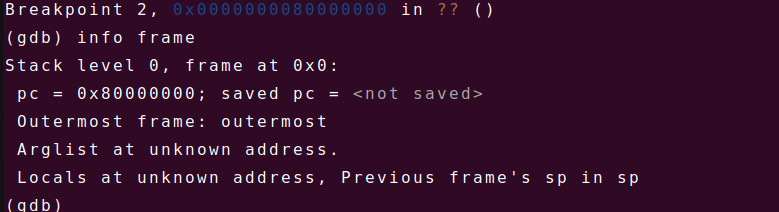
进入GDB程序后，先使用target remote :1234来连接qemu，然后在GDB内尝试各种指令，比如使用layout asm查看汇编源代码，使用break设置断点，使用continue执行到断点，使用next进行单步执行，以及使用finish命令结束当前函数……等等，下面展示部分操作结果。





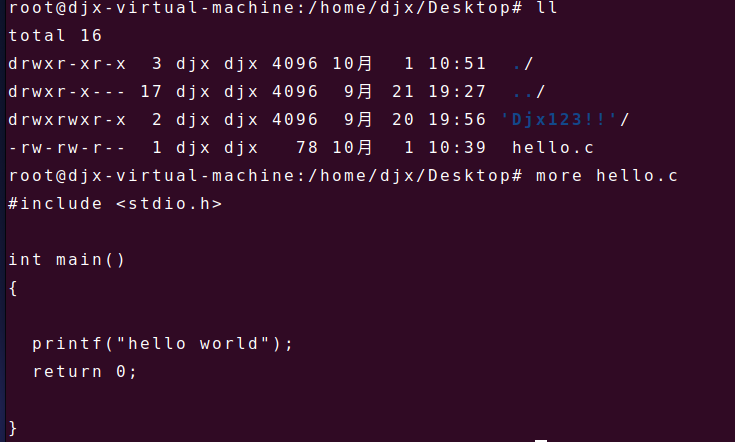


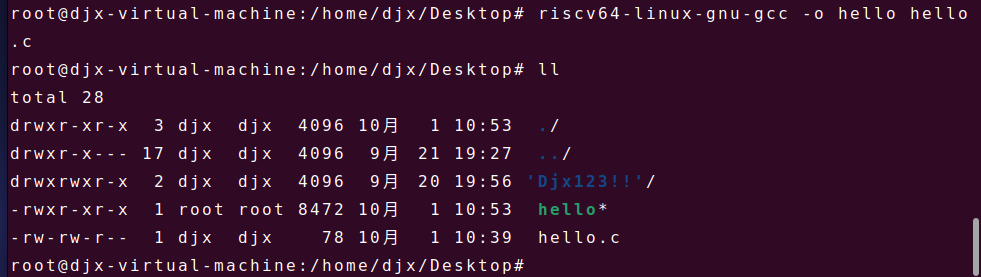




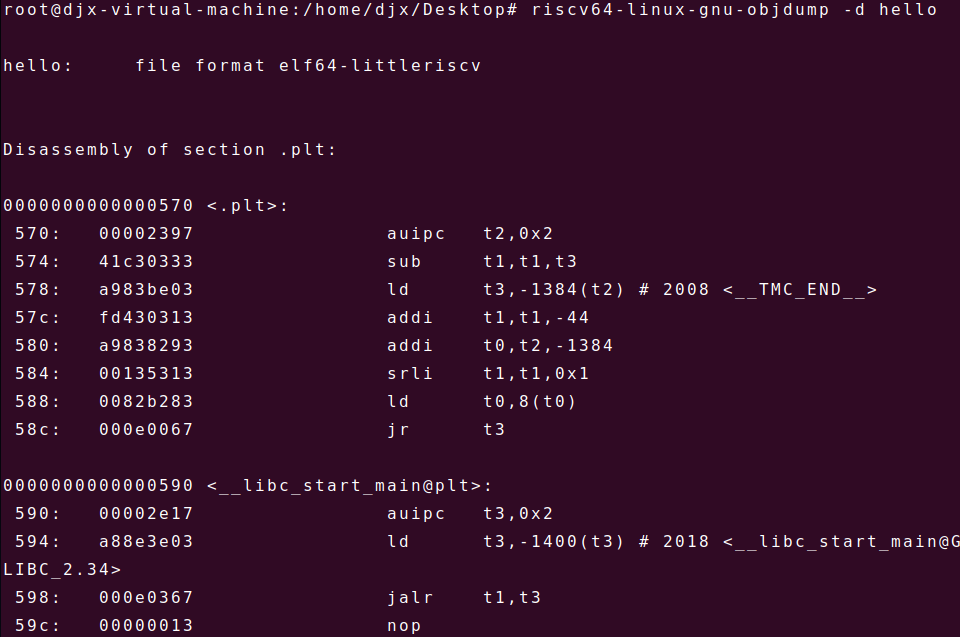
思考题

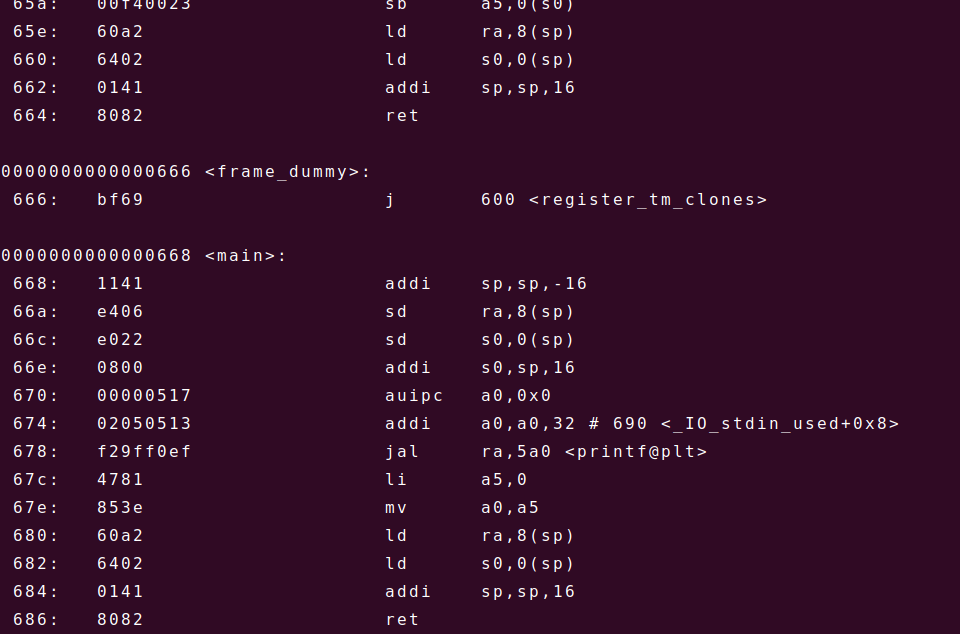
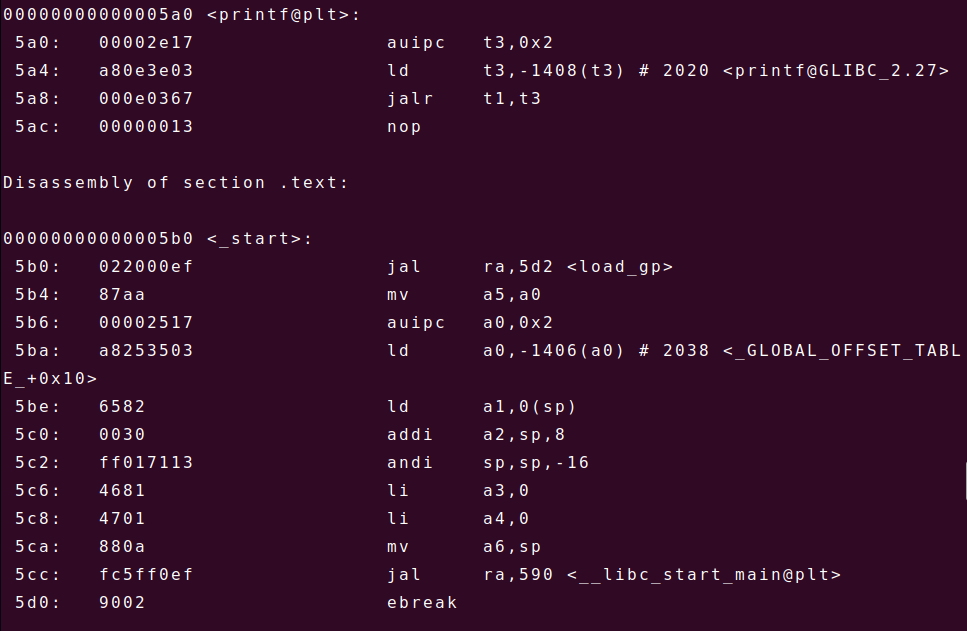
1. 使用 riscv64-linux-gnu-gcc编译一个简单的.c文件，如下图所示。





1. 使用 riscv64-linux-gnu-objdump将1中得到的hello可执行文件进行反汇编，如下图所示。

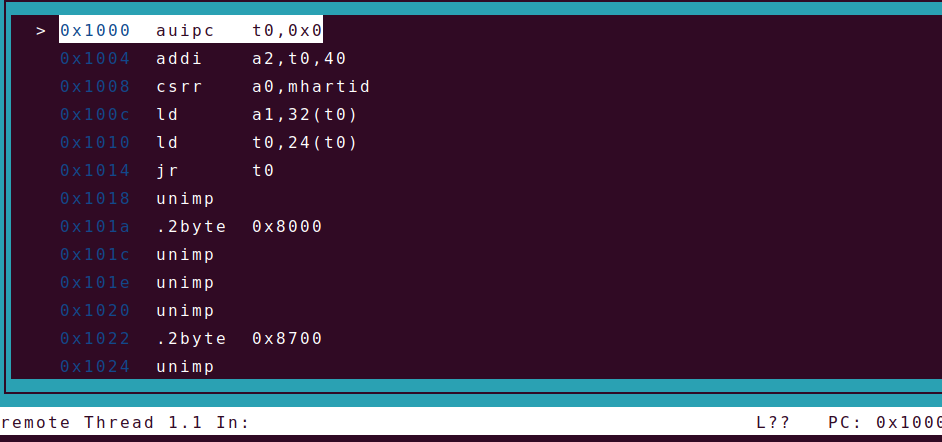




1. 调试Linux

a.在 GDB 中查看汇编代码

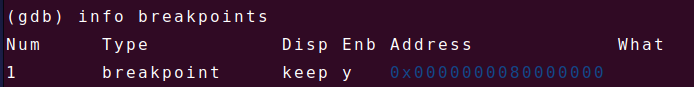




b.在 0x80000000 处下断点



c.查看所有已下的断点



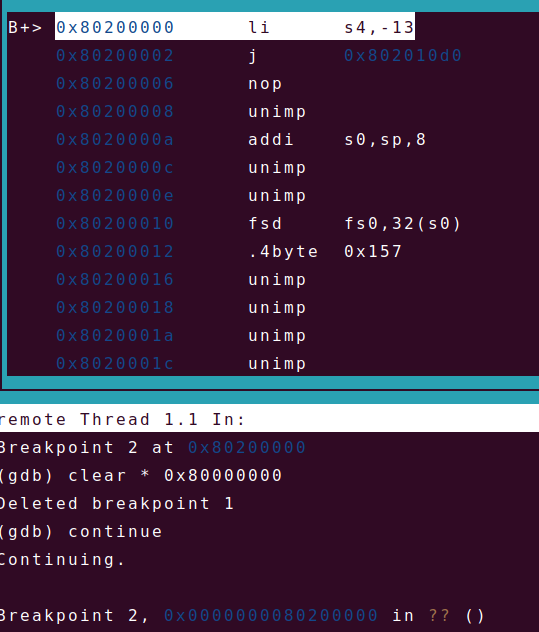
d.在 0x80200000 处下断点



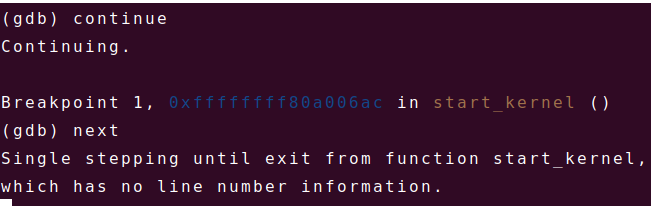
e.清除 0x80000000 处的断点



f.继续运行直到触发 0x80200000 处的断点,使用continue命令，可以看到当前运行到了0x80200000处。



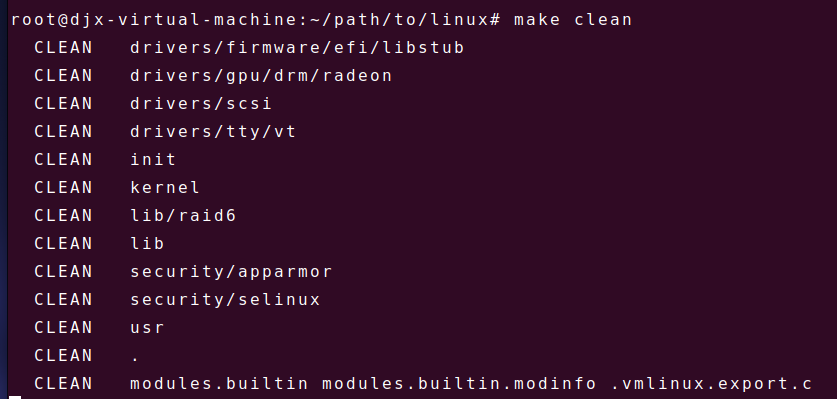
g.单步调试一次



h.退出 QEMU

按下 Ctrl + A，然后松开，接着按下 X，退出qemu。

4.使用 make 工具清除 Linux 的构建产物



5.vmlinux 和 Image 的关系和区别是什么？

在构建Linux内核过程中，vmlinux和image都是Linux内核的构建产物。区别在于，vmlinux是未经压缩的，可执行的内核镜像，包含完整源代码和数据，主要用于调试目的。而image是未压缩的，使用objcopy处理vmlinux后生成的二进制内核映像。通常用于实际的引导启动操作系统。

讨论心得

本次实验较为简单，遇到的问题也比较少。首先是在尝试下载Linux内核源码时，我先试图在Linux图形化界面中，进入浏览器进行下载，发现效率比较低下，后来通过查阅资料学到了wget命令和tar命令，可以在命令行较为高效地下载文件。然后就是关于文件路径问题，实验指导手册给出的只是参考路径，因此不能直接执行命令，需要将其中的路径改为自己Linux系统中对应文件的真实路径才能运行。总体来说，这次实验让我熟悉了Linux命令行的使用以及GDB调试方法，有比较大的收获。