

221220076

第一次实验报告

个人信息

姓名：落华栋

学号：221220076

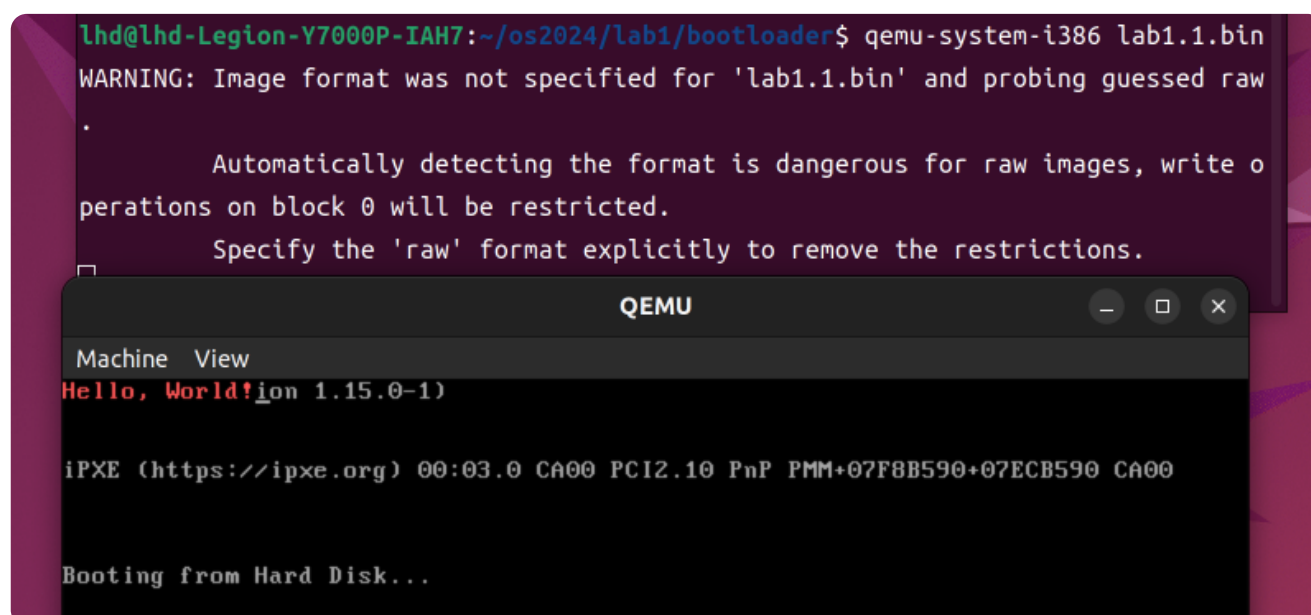
邮箱：221220076@smail.nju.edu.cn

实验进度

完成了全部三个任务：即在实模式、保护模式以及加载磁盘中的程序并运行

实验结果

在实模式下打印



```
lhd@lhd-Legion-Y7000P-IAH7:~/os2024/lab1/bootloader$ qemu-system-i386 lab1.1.bin
WARNING: Image format was not specified for 'lab1.1.bin' and probing guessed raw
.
    Automatically detecting the format is dangerous for raw images, write o
perations on block 0 will be restricted.
    Specify the 'raw' format explicitly to remove the restrictions.
[
QEMU
Machine  View
Hello, World!ion 1.15.0-1)

iPXE (https://ipxe.org) 00:03.0 CA00 PCI2.10 PnP PMM+07F8B590+07ECB590 CA00

Booting from Hard Disk...
```

在保护模式下打印

```
lhd@lhd-Legion-Y7000P-IAH7:~/os2024/lab1$ make play os.img
qemu-system-i386 os.img
WARNING: Image format was not specified for 'os.img' and probing guessed raw.
        Automatically detecting the format is dangerous for raw images, write
operations on block 0 will be restricted.
        Specify the 'raw' format explicitly to remove the restrictions.

QEMU

Machine  View
Hello, World!ion 1.15.0-1)

iPXE (https://ipxe.org) 00:03.0 CA00 PCI2.10 PnP PMM+07F8B590+07ECB590 CA00

Booting from Hard Disk...
```

在保护模式下加载程序打印"Hello, World"

```
lhd@lhd-Legion-Y7000P-IAH7:~/os2024/lab1$ make play os.img
Ma qemu-system-i386 os.img
WARNING: Image format was not specified for 'os.img' and probing guessed raw.
        Automatically detecting the format is dangerous for raw images, write
operations on block 0 will be restricted.
        Specify the 'raw' format explicitly to remove the restrictions.

QEMU

Machine  View
SeaBIOS (version 1.15.0-1)

iPXE (https://ipxe.org) 00:03.0 CA00 PCI2.10 PnP PMM+07F8B590+07ECB590 CA00
Hello, World!

Booting from Hard Disk...
```

修改的代码

实模式下

参照了已给出的代码，故不再赘述

保护模式

修改了 `start.s`，首先将16位的汇编指令修改为32位，然后补充了关中断、启动A20总线、设置CR0的PE位为1，之后填充了GDT表项，然后设置了 `displaystr` 和 `nextchar` 函数。

保护模式下加载用户程序

首先删除了 `start.s` 里的 `displaystr` 和 `nextchar` 函数，因为在 `app.s` 里已经完成了这两个函数。然后修改了 `boot.c` 里的 `void bootMain(void)`。

一些实验过程中解决的问题

code16和code32是用来做什么的

code16和code32分别用来告诉编译器将代码编译为实模式下16位 `Thumb` 代码和保护模式下32位 `ARM` 代码的

查找地址：<https://zhuanlan.zhihu.com/p/138658372>

为什么加载GDT的时候要减一

原因是因为GDT界限相当于GDT字节大小减一。