# 实验报告

**实验一：系统软件启动过程**

****

**姓名：孙东\_\_\_\_\_\_\_**

**学号：2013659\_\_\_\_**

**专业：物联网工程\_**

**时间：2022/10/15\_**

## （一）组员与分工

组员：孙东 韩雪 吴传杰

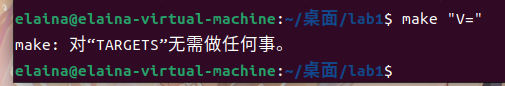
我的分工：对项目整体进行熟悉，能在其他人答不出来时及时补充，保证答辩流畅。同时负责讲解ex5 ex6 challenge。

## （二）代码

https://github.com/JNTMOS/IKUN

## （三）bug+疑问

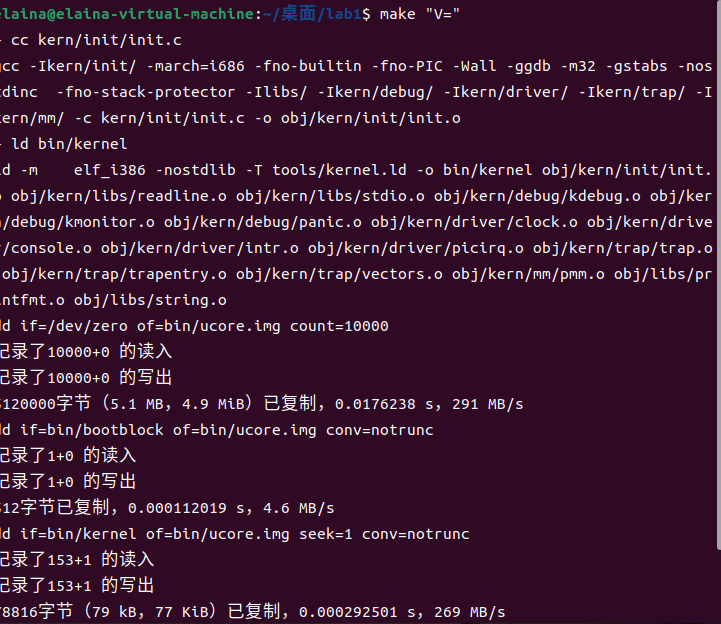
（1）执行exercise1时make “V=”无效的问题



解决方法：

因为已经有obj bin两个文件夹，所以需要先执行make clean再执行make“V=”即可。





（2）\_\_vectors[]无法正确引用问题

在trap.c中声明\_\_vectors[]时必须加上extern，否则将无法引用在vertor.S生成的\_\_vectors[]。

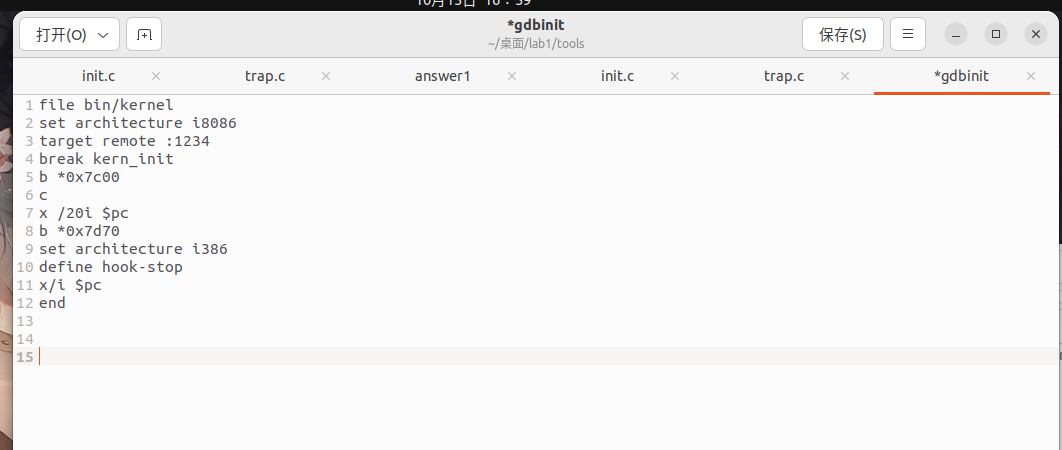


（3）gdbinit无法正常获取汇编代码问题

此bug后面不知为何再也无法复现，故没有截图

大致情况是：现在gdbinit中定义hook\_stop，再make debug进入kernel\_init()后显示的汇编代码对不上实际汇编代码。推测是因为定义在了set architecture i386之前，但重新试一遍没能成功复现。

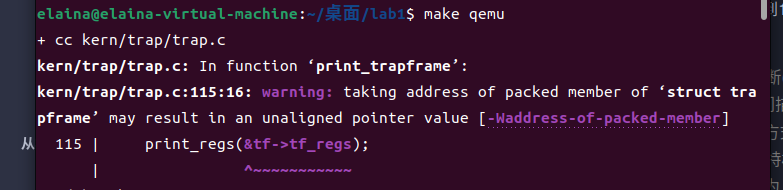
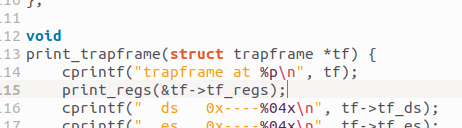
疑问：qemu能否知道set architecture何时生效？

****

（4）ex6函数警告

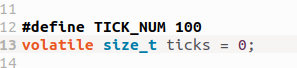
取trapframe地址会导致获得未对齐的指针

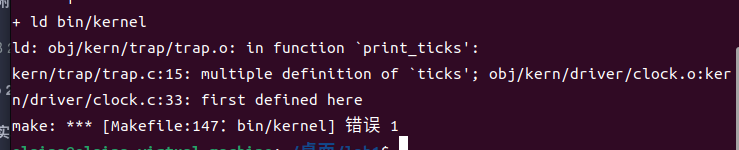
暂时不知道如何解决



（5）ticks重名错误

Ticks重定义错误，已在clock中定义。



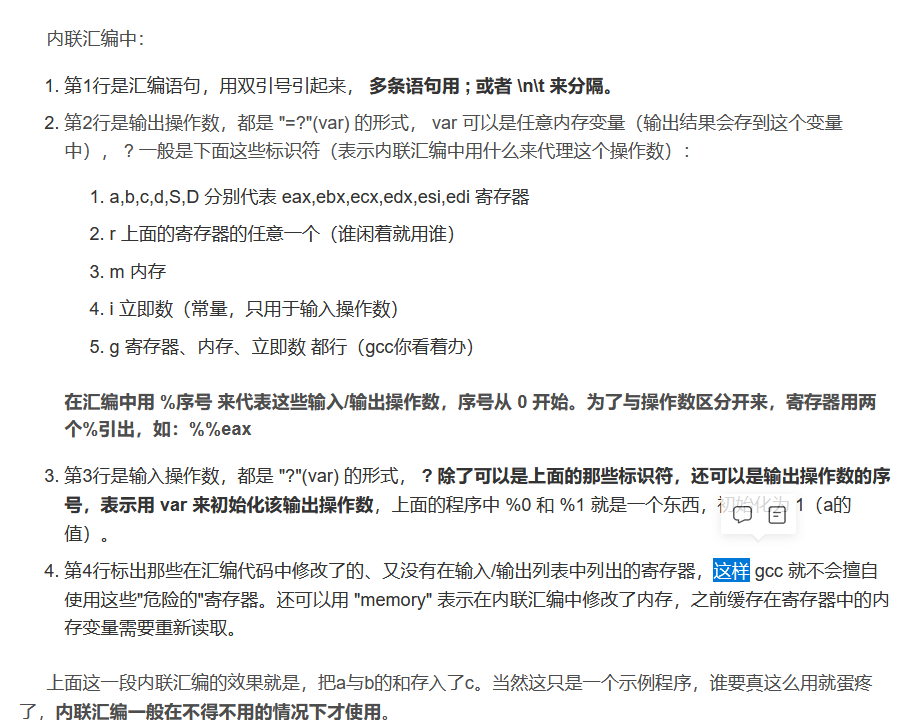


解决方法：不能重名，改成tick即可。

（6）gcc内联汇编（疑问）

写过VC++中的\_\_asm，但不熟悉GCC的asm函数。



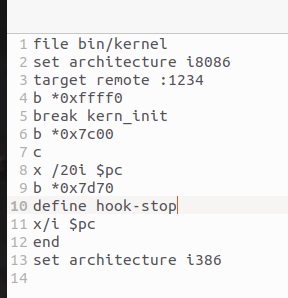


解决方法：上网学习

（7）Volatile



（8）b \*0xffff0不生效问题



当以下指令存在时：

b \*0x7c00

c

x /20i $pc

将不会停在0xffff0而是直接停在0x7c00，目前没找到根本的解决方法，只能选择其一。

（8）make grade之后再进行make qemu会进入kernel monitor状态，代码功能无法正常使用。

解决方法: make clean一遍就能用了，但是再次make grade还是会出问题，不知道为什么，可能是make grade破坏了源文件某些代码。

PS：希望下个实验别出这个问题，当时没找到解决方案去找老师答辩给我吓坏了，幸好make grade能跑。

## （四）吐槽

（1）看的资料有些没有老师讲解看起来很吃力

（2）有些语法不熟悉还有函数不熟悉，如GCC的内联汇编格式和我们学的就不太一样，coding需要的某些函数参数不明，还查不到资料。

（3）参考书的图片不能放大，且有些句子不是很通顺。

（4）第一个实验不太熟悉实验程序结构和相关工具使用，入手较难。

（5）challenge相关的资料较为难懂且感觉不够完整，challenge的提示少，答案都不能完全看懂QAQ（菜菜呜呜）

（6）汇编好难，特别是内联汇编，只懂一点mips 和简单的x86。（汇编不是必修）