操作系统研讨课 实验报告

代瀚堃 2019K8009929051

一、实验中遇到的问题

1. 不会连接网卡/QEMU 不会设置

网卡的设置折腾了好长时间，卡死在 InitPhy 侦测速度的地方，虽说是自动侦测，但似乎速度不支持，经过一段时间之后，才摸索出来，基本上是这样：

扩展坞的网卡接到物理机，设置速度为 1Gbps，全双工，或者其他板卡支持的速度和工作模式，然后板卡和扩展坞用网线连起来。

QEMU 需要用 e1000 的脚本来连接，如果需要调试，需要在脚本中加上-s 和-S 选项

2. load_elf 和 alloc_uvm 的时候触发缺页了

原因是提供的 load_elf 函数导入 ELF 是按照 mem_sz 来放置的，但返回的 length 却是 file_sz，按照 file_sz 来分配页框就有可能出错：

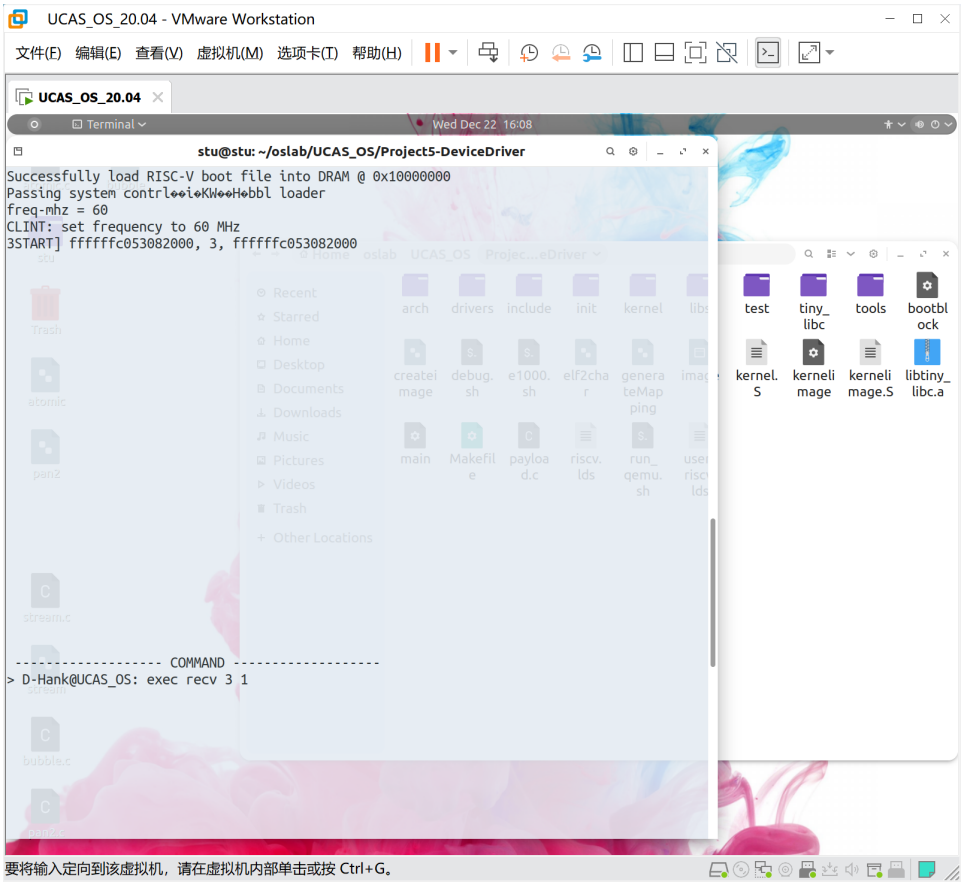
```
while (ph_entry_count--) {
    phdr = (Elf64_Phdr *)ptr_ph_table;

    if (phdr->p_type == PT_LOAD) {
        /* TODO: */
        for (i = 0; i < phdr->p_memsz; i += NORMAL_PAGE_SIZE) {
            if (i < phdr->p_filesz) {
                unsigned char *bytes_of_page =
                    (unsigned char *)prepare_page_for_va(
                        (uintptr_t)(phdr->p_vaddr + i), pgdir);
                memcpy(
                    bytes_of_page,
                    elf_binary + phdr->p_offset + i,
                    MIN(phdr->p_filesz - i, NORMAL_PAGE_SIZE));
                if (phdr->p_filesz - i < NORMAL_PAGE_SIZE) {
                    for (int j =
                             phdr->p_filesz % NORMAL_PAGE_SIZE;
                         j < NORMAL_PAGE_SIZE; ++j) {
                        bytes_of_page[j] = 0;
                    }
                }//rest
            } else {
                long *bytes_of_page =
                    (long *)prepare_page_for_va(
                        (uintptr_t)(phdr->p_vaddr + i), pgdir);
                for (int j = 0;
                     j < NORMAL_PAGE_SIZE / sizeof(long);
                     ++j) {
                    bytes_of_page[j] = 0;
                }
            }
        }
```

3. get_kva_of 函数实现有问题

P4 中这个函数返回的是 4KB 对齐的地址，但我们在为用户拷贝数据时，用这个 4KB 对齐的地址拼上 offset 域显然不太合适，所以应该实现在 get_kva_of 内

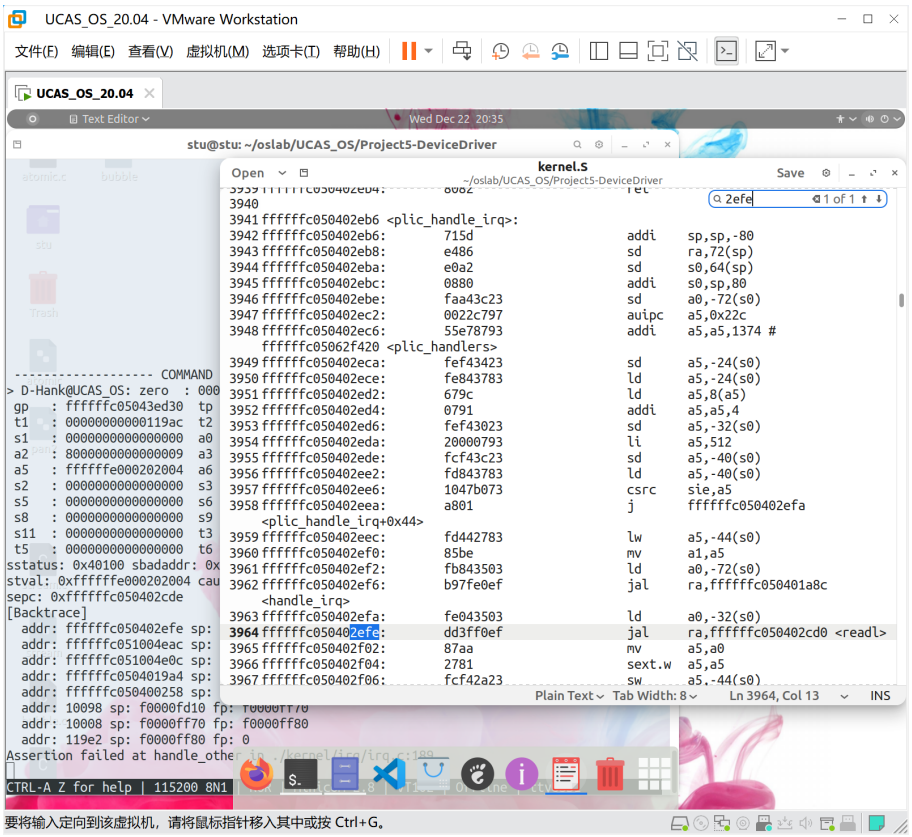
因为这个 bug 并没有触发例外，而是在用户态打印 recv 的包时才有问题，在板子上很难调试，只能一点一点打印，发现 frLength 和 addr 地址重合：



且看上去都像是对齐的地址，而内核态打印出的 recv 信息又没有错，这明显是 get_kva_of 出了问题

4. io_map 没有配置好

一开始尝试在 IO 时切换到初始页表，但最后在网卡中断解除阻塞时还是缺页了：



看来应该是调用 plic_handle_irq 的时候没有把页表切回来。。。

但事实上只需要在用户进程的 pg_dir 中把第 384 项配置成初始 IO 的那几个页框就行

二、还有待解决的问题

1. do_kill 和 do_exec 时没有检查 net_send_queue 和 net_recv_queue，虽然目前还没有出问题