Zhipeng Tian
P436
Assignment 3C
4/12/12

1. Trace the call graph of copy mm, invoked from do fork. What does the leaf-level function copy_one_pte do?

```
do_fork()
        copy_mm()
                dup_mm()
                        allocate_mm()
                        mm_init()
                        dup_mmap()
                                anon_vma_fork()
                                arch_dup_mmap()
                                copy_page_range()
                                        copy_pud_range()
                                                copy_pmd_range()
                                                        copy_pte_range()
                                                                copy_one_pte()
```

copy_one_pte() copies the contents of one PTE to a new location and mark the page as read-only, to prevent parent and child process from writing onto the page.

2. In the last assignment, you constructed the call graph of do page fault, which eventually calls do_wp_page (in mm/memory.c). What does this function do?

handle_pte_fault() calls do_wp_page(). handle_pte_fault() is used to handle different types of page fault. It decides whether page fault type it is and choose the different function to handle them. do_wp_page() is the one to determine whether those pages who have page fault need to be duplicated. Basically it breaks COW pages for handle_pte_fault().

3. Which function can you use to check if a given virtual address is in a particular VMA?

We can use find_vma() to find out which VMA covers the given address, and then check whether the returned VMA is the one we are looking for.

4. In one of these low level memory copy functions, you will need to do something special for dumbfork. For that purpose you may need to be able to tell inside this low-level function that the function was called from dumbfork, and not fork (or any other function). For example:

if (in_dumbfork)
// do dumbforky things
else
// do whatever you usually do
How would you achieve this?

To enter the dumbfork mode, we can create a new vm_flags to indicate the dumbfork mode. Then we modify copy_page_range()'s behavior a little bit. As long as it receive our new flag, it calls do_wp_page() directly without hand over to page fault handler. And when do_wp_page() is called, let it copy the page to the new address immediately.

5. Describe the functions in the page-fault handler that are responsible for demand allocation.

do_no_page() is one of the functions doing demand allocation. It called by handle_pte_fault() the first time a page is to be allocated. And it checks whether the page is an anonymous page. If so, it calls do_anonymous_page() to allocate a page. Otherwise, it will call nopage() to allocate a page and insert it into the page table.

do_anonymous_page() is another function handle demand allocation. It allocates a new page for the process if the process accesses a page at first time.