**Exercise 7.** Use QEMU and GDB to trace into the JOS kernel and stop at the movl %eax, %cr0. Examine memory at 0x00100000 and at 0xf0100000. Now, single step over that instruction using the **stepi** GDB command. Again, examine memory at 0x00100000 and at 0xf0100000. Make sure you understand what just happened.

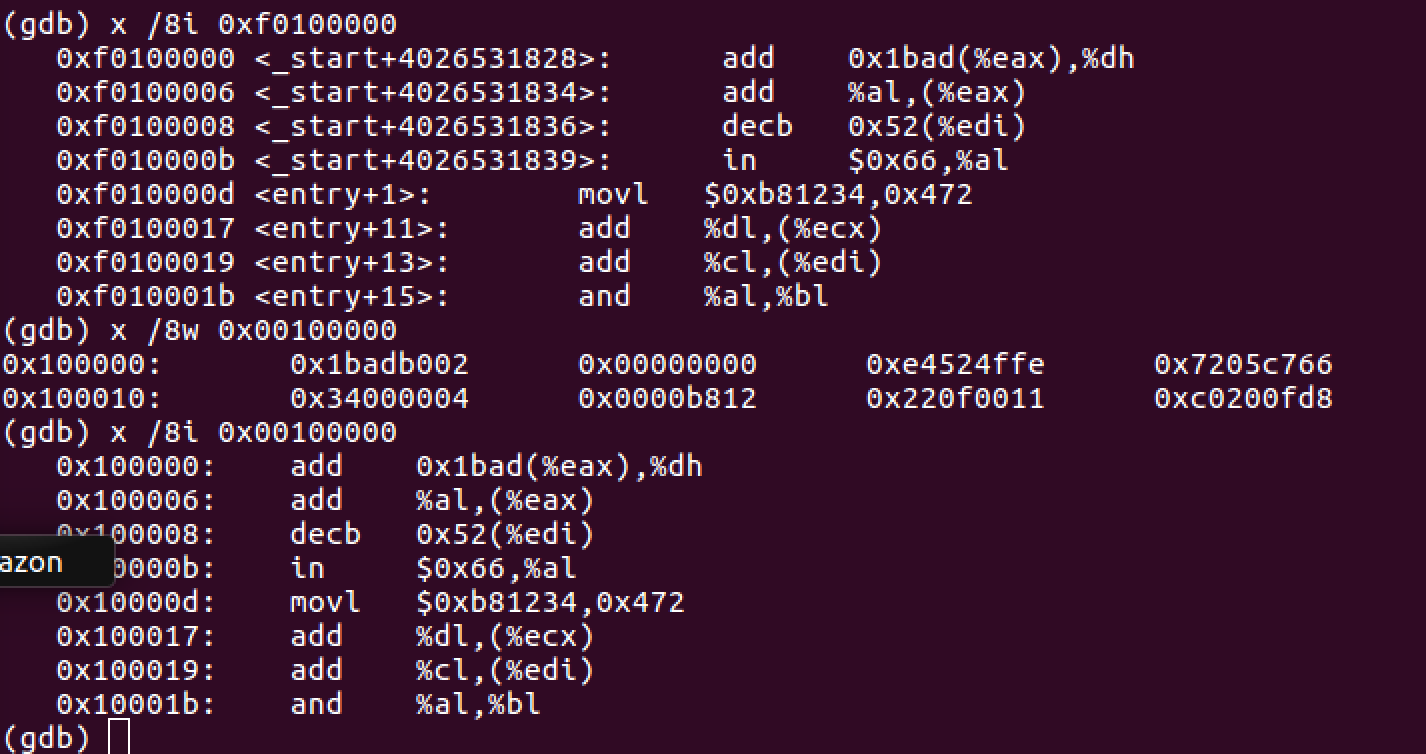
What is the first instruction *after* the new mapping is established that would fail to work properly if the mapping weren't in place? Comment out the movl %eax, %cr0 in kern/entry.S, trace into it, and see if you were right.

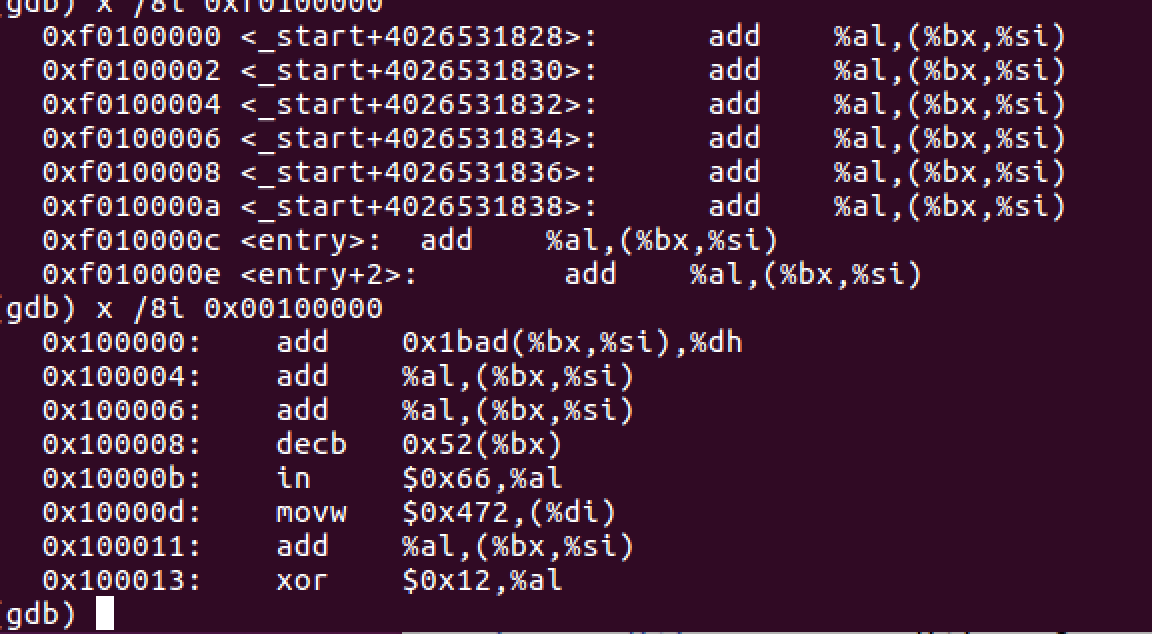
didn’t know where to find the instruction movl %eax, %cr0 by stepping through on gdb, so went to lab/obj/kern/kernel.asm file to see where movl %eax, %cr0 was at.

It’s at f010001a: # Turn on paging…

Jumped to that line in gdb

j \*0xf010001a:





Notes / Vocab: