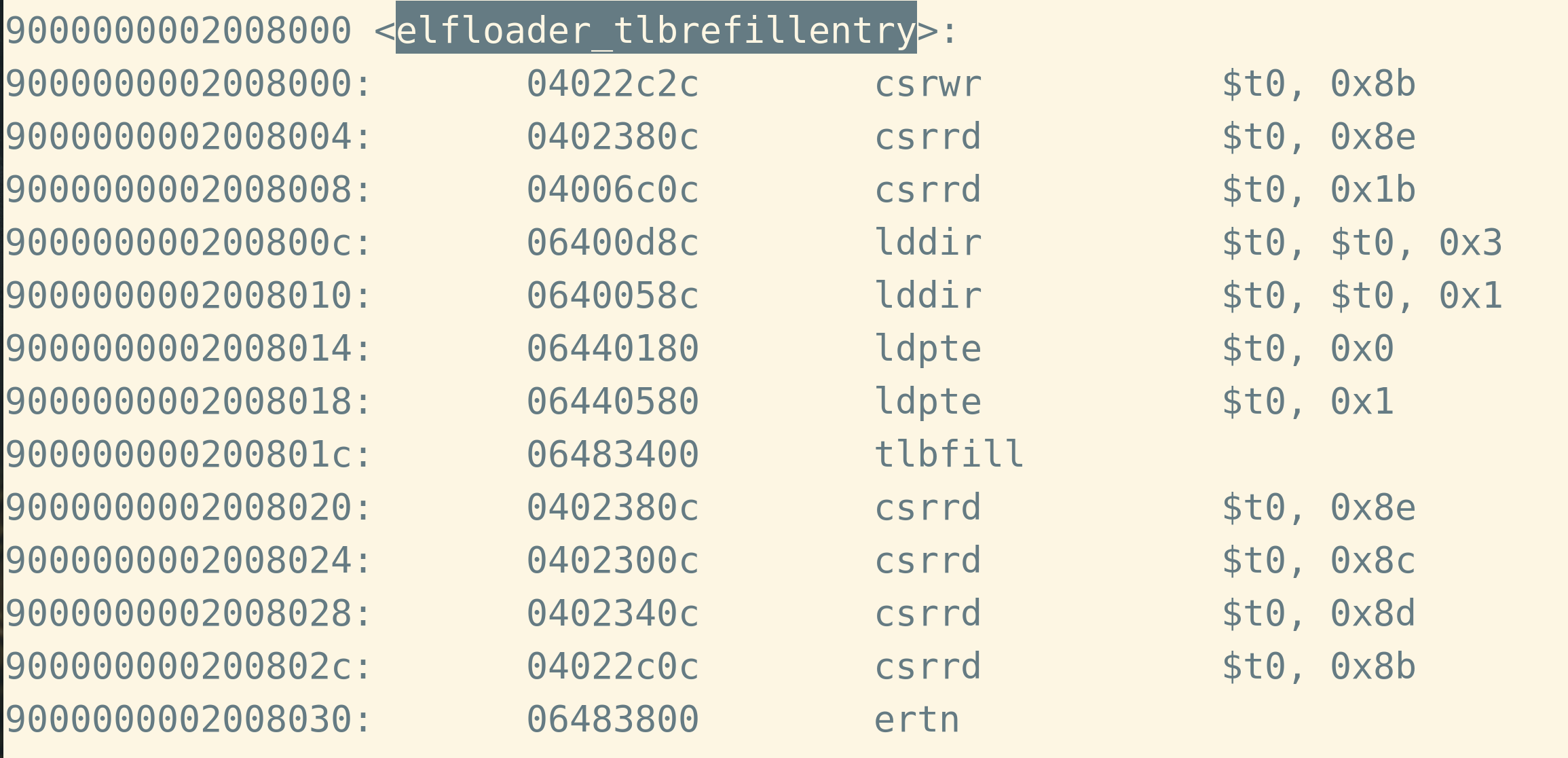
内核使用64G大页发现的问题。

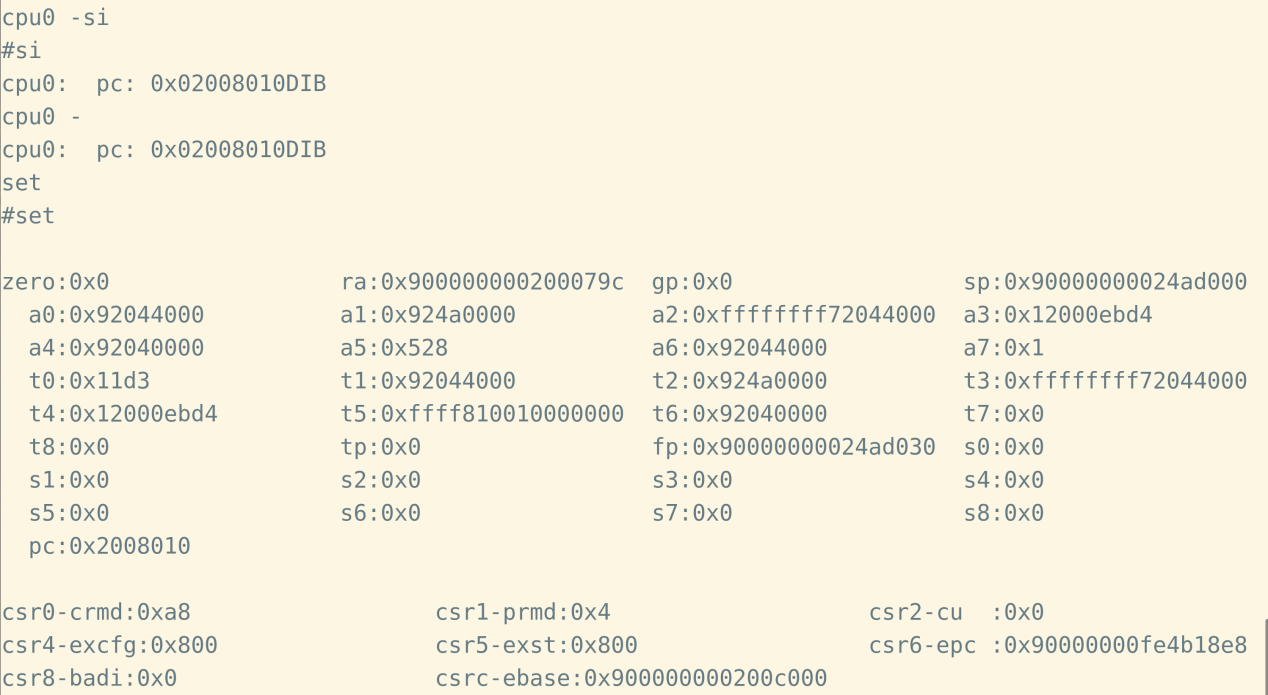
* 问题一：进入内核的虚拟地址0xffff 8100 9000 0000，触发tlb refill，tlb refill代码:

handle\_tlb\_refill:

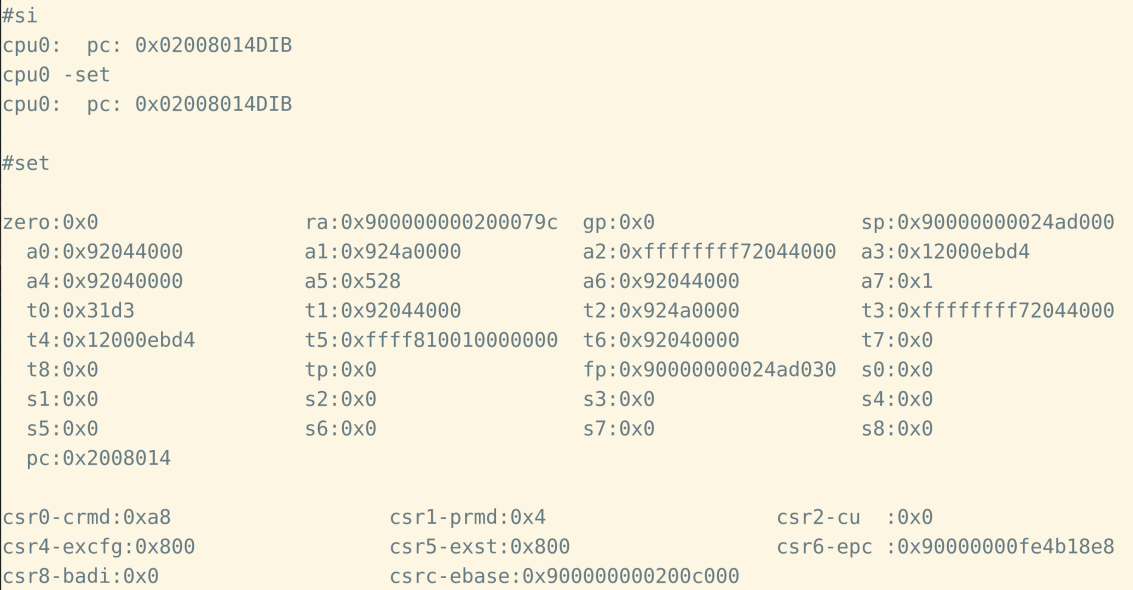


其中红色框仅为debug用，非红色框是refill代码。

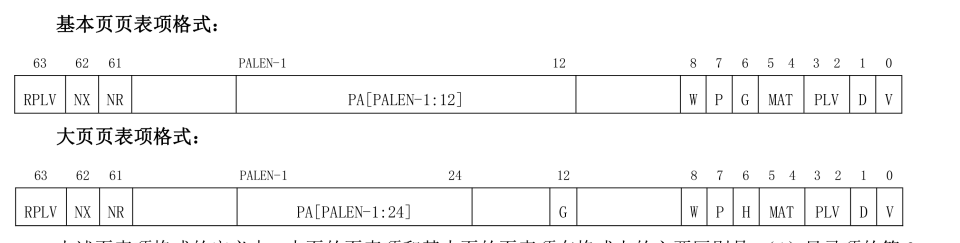
第一次执行lddir(0x9000 0000 0200 800c处指令)，t0值是0x11d3



第二次执行lddir(0x9000 0000 0200 8010处指令)后，t0值是0x31d3。

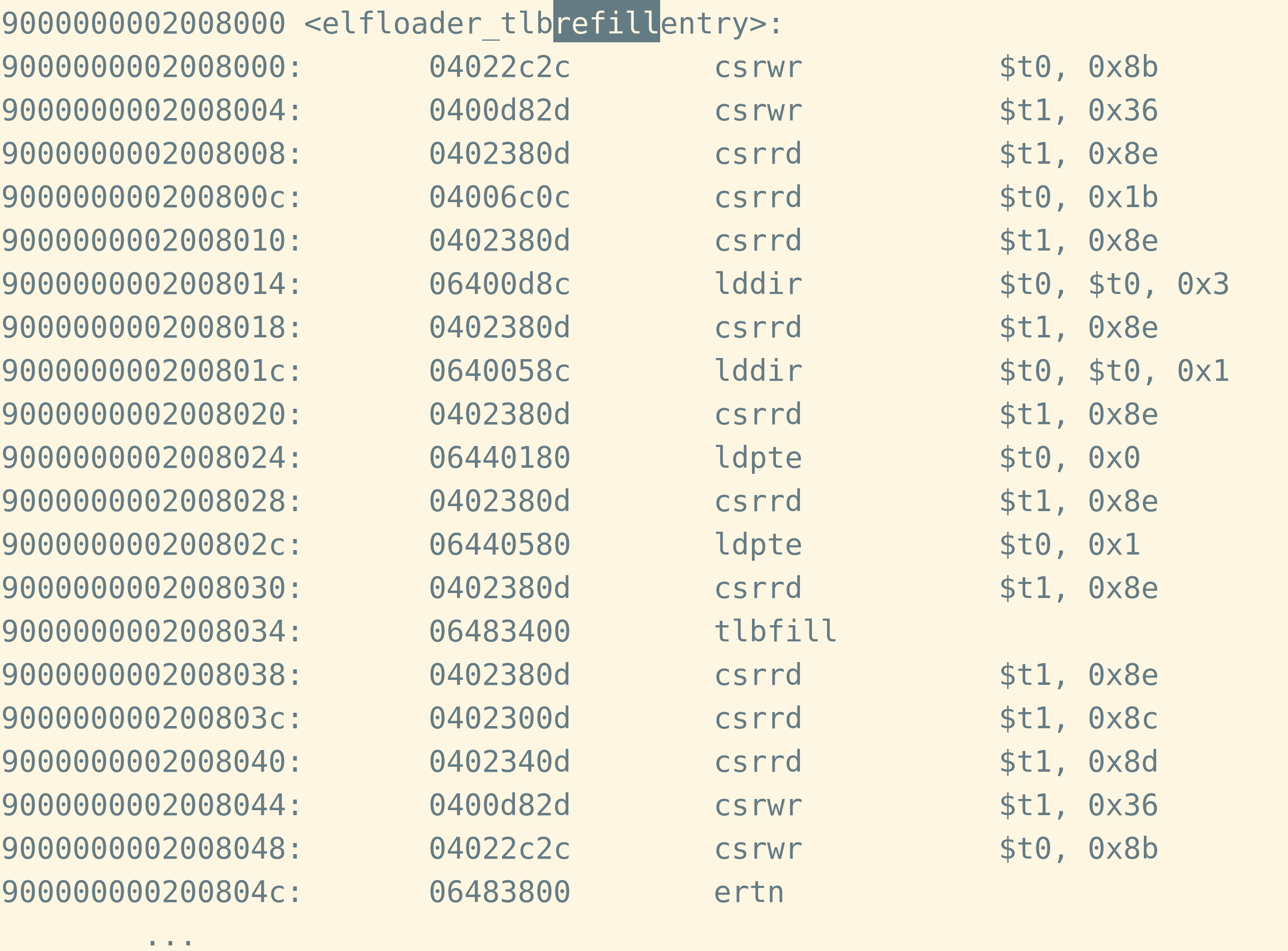


按照手册，页表项bit6是Huge位，第一次执行lddir指令后t0里已经是大页页表项，bit6=1，再执行lddir，t0的值不应该改变，但变成了0x31d3。

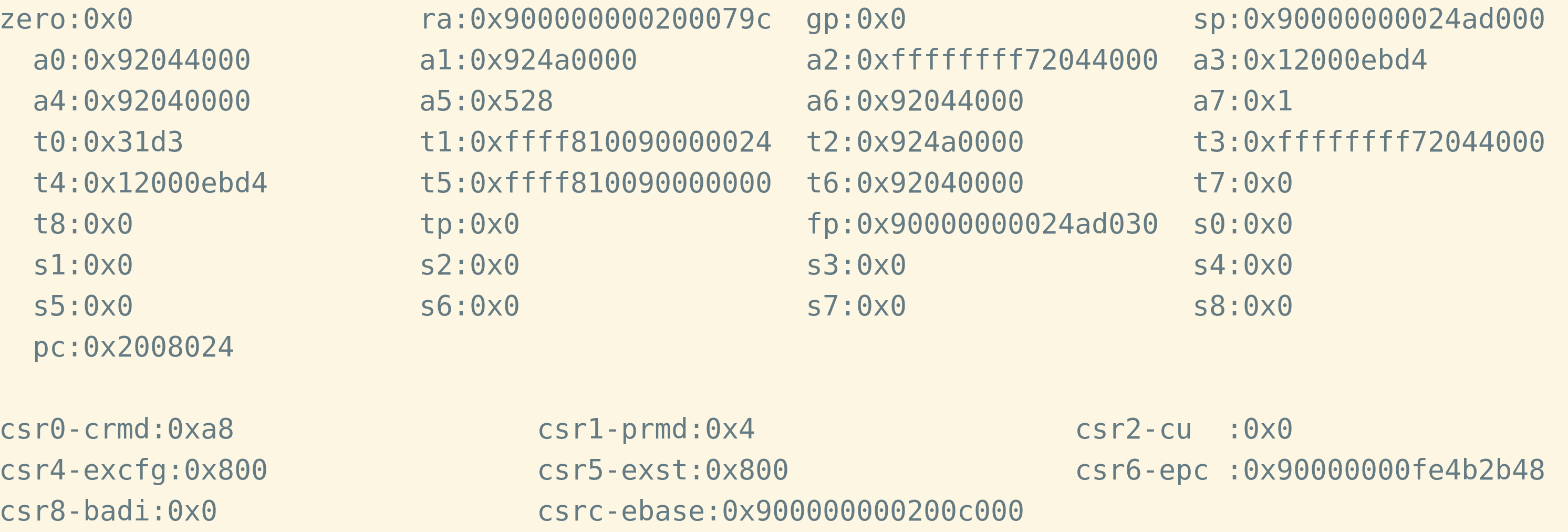


真实机器上页表项格式是否和手册一致？

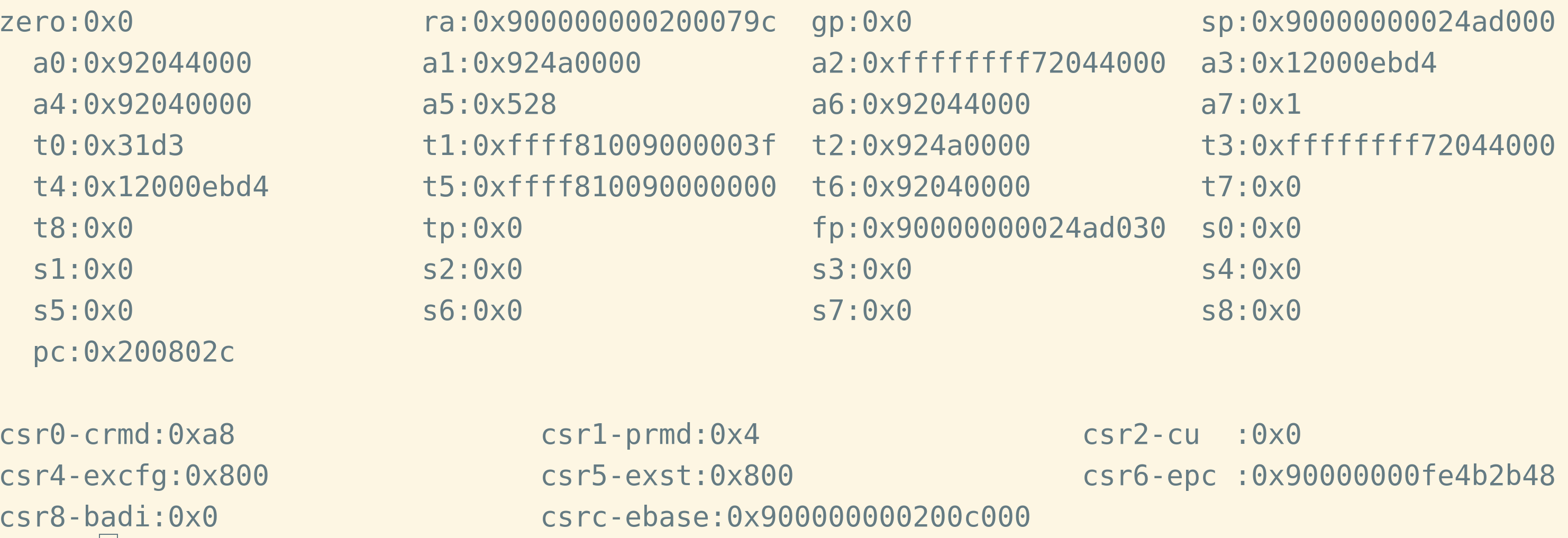
* 问题二：tlbrefill过程中，我添加了debug代码读tlbrehi寄存器到t1中，发现ldpte改变了tlbrehi的ps域。问题在红框代码处。



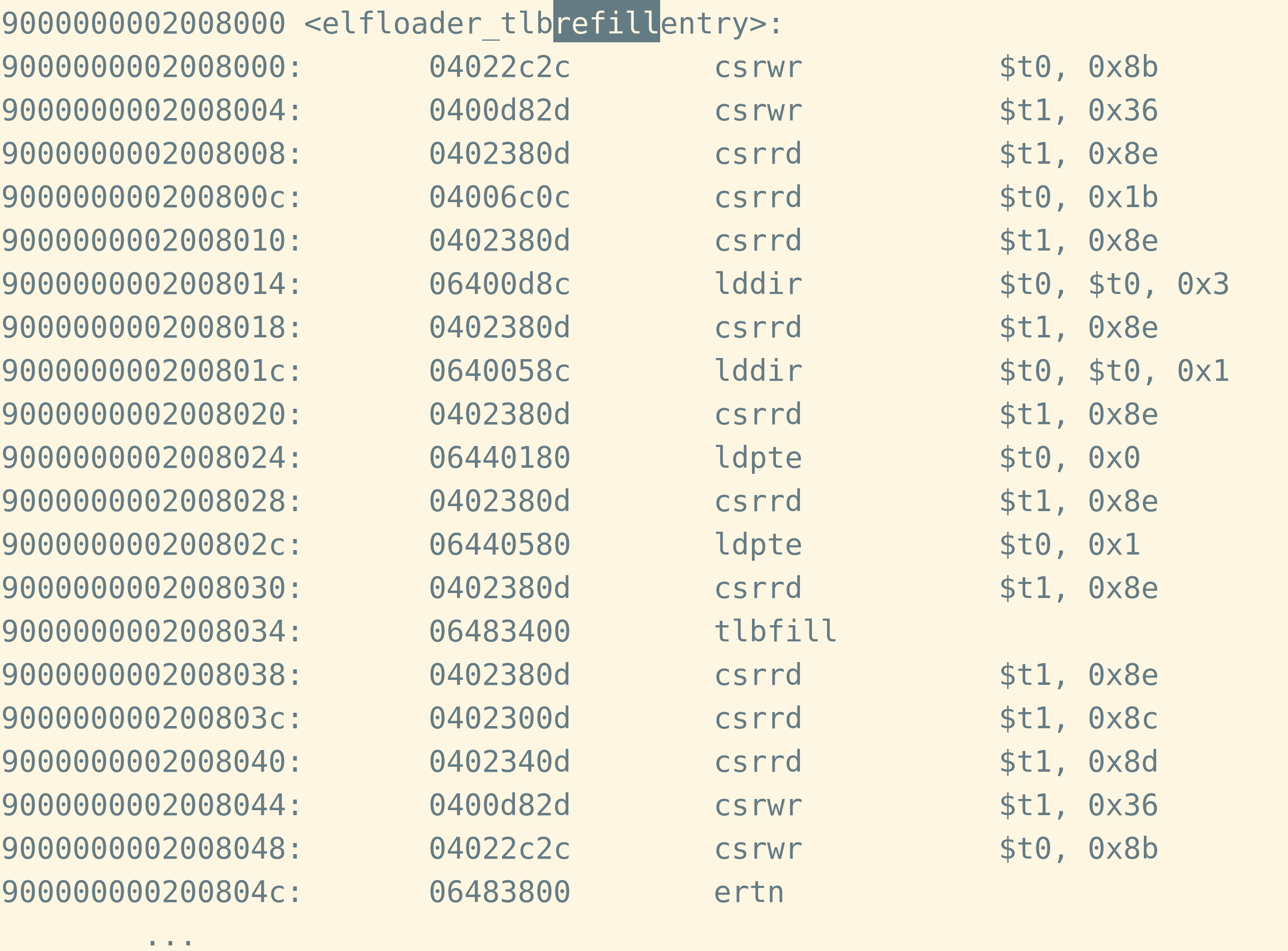
第一条ldpte执行之前(0x9000 0000 0200 8024)，读tlbrehi到t1中，是正确的值(0xffff 8100 9000 0024)。



第一条ldpte执行之后，读tlbrehi到t1中，ps域不再正确，从24变成了3f。



* 问题三：红框处读出tlbrelo0,tlbrelo1，其中tlbrelo1有问题。



0x9000 0000 0200 8038处指令，读出tlbrelo0到t1中，是正常的0x53。

0x9000 0000 0200 803c处指令，读出tlbrelo1到t1中，最高位变成了1，该位对应RPLV，但是我们设置页表的RPLV为0。

