

相当于在第二步的过程中，内核会在3环进程的栈中的上面放上Frame结构(用来之后的恢复原来的执行，3环进程的状态信息)之后调用3环的Signal Handler。之后进入到3环,执行3环定义的信号处理函数Signal Handler函数，该函数用来处理信号/(异常)，本质也就是修改之前0环放在栈上面的frame结构（之前3环进程的状态信息），修改完成之后，就直接ret的时候会调用rt\_sigreturn函数，此时会再次进入0环，调用该函数，而该函数的实现就是将进程栈中的值pop放入到寄存器中。

