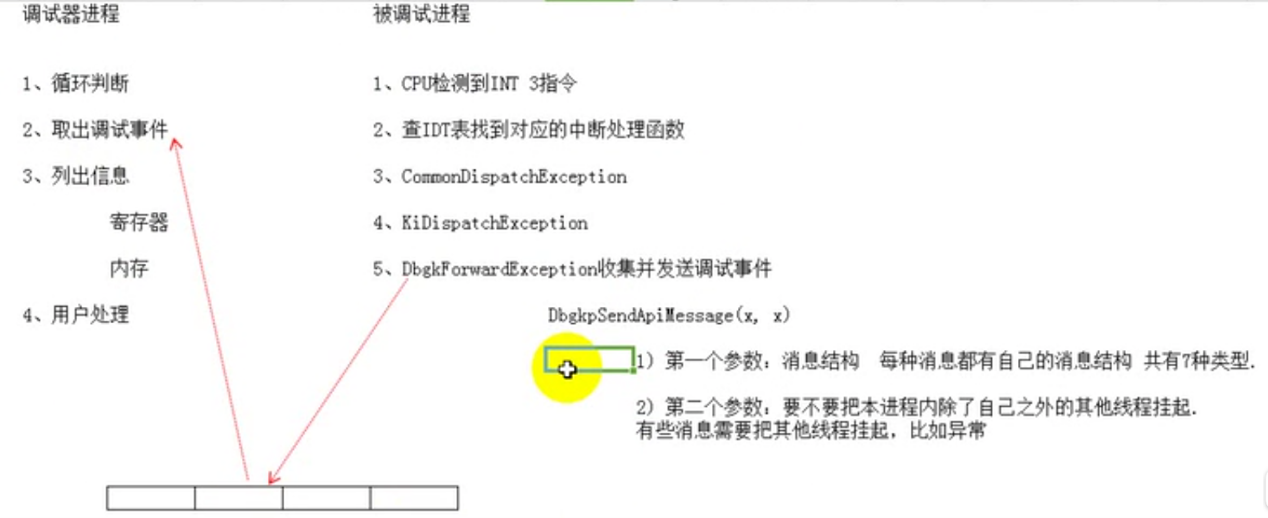
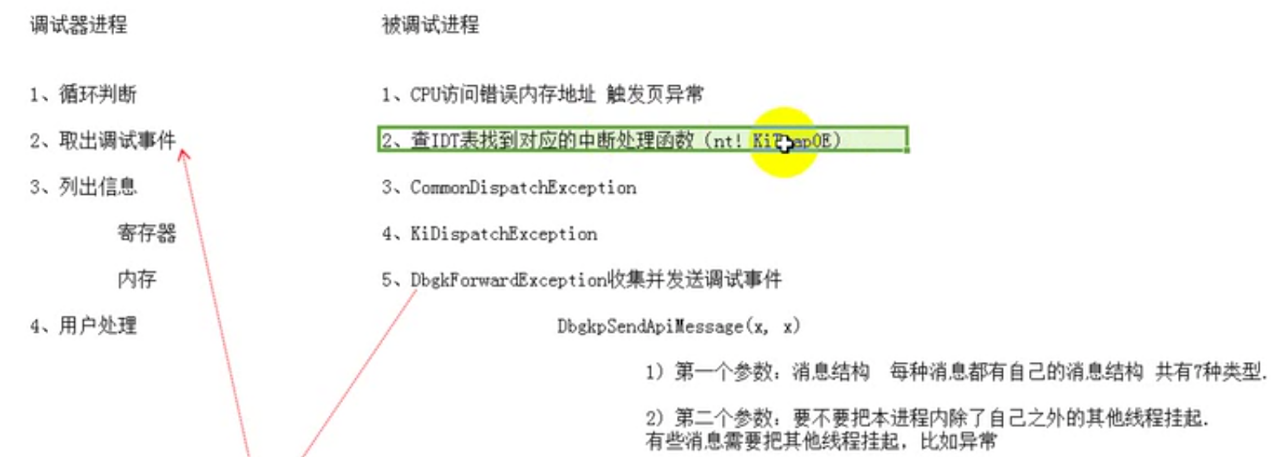


软件断点：



先调试器进程，通过Debug\_Object对象，来向被调试进程写入int 0x3，当程序指定到这之后，会触发异常，查询IDT，保存trap\_frame等等，之后向Debug\_Object对象中发送调试事件，之后调试器进程循环取出调试事件，先根据调试事件来分类，判断是异常，之后根据异常的种类分，再之后，就是将原来的内容写入到int 0x3位置，再。。。。。

内存断点：



可以在进程刚创建的事件中，使用修改被调试物理页的p或者R/W属性，之后进程运行之后，会触发异常，再之后就是发送事件给Debug\_Object对象，调试器进程取出事件，现根据事件进行分类，判断出是异常事件，之后根据Exception->errrorcode来分来判断是那种异常，之后就是根据Exception\_Record中的ExceptionInformation[0]来判断是哪种R还是W问题，之后ExceptionInformation[1]存放问题的地址，之后再修改会原来的页属性。。。。。

