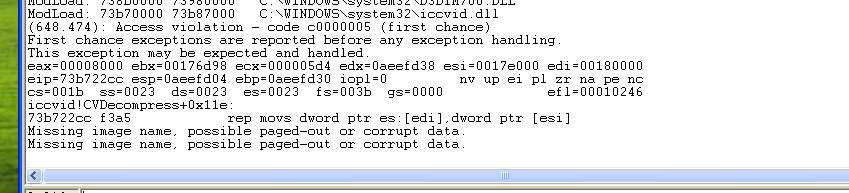
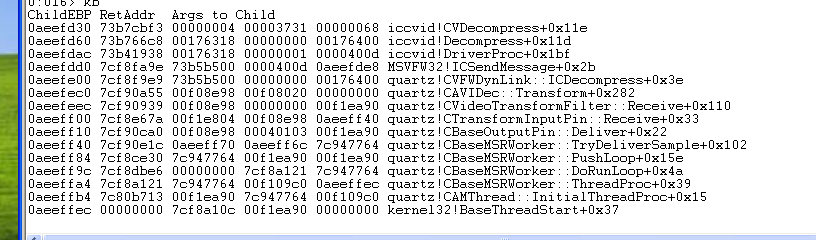
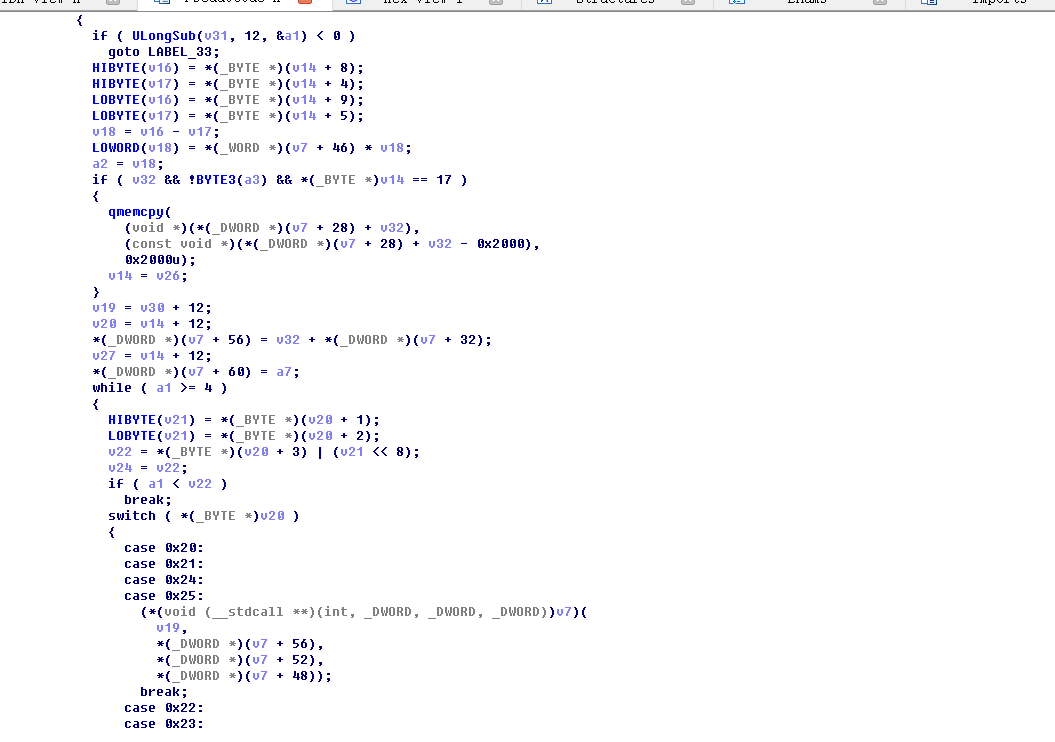
CVE-2010-2553

Windbg运行程序放入poc，程序断下



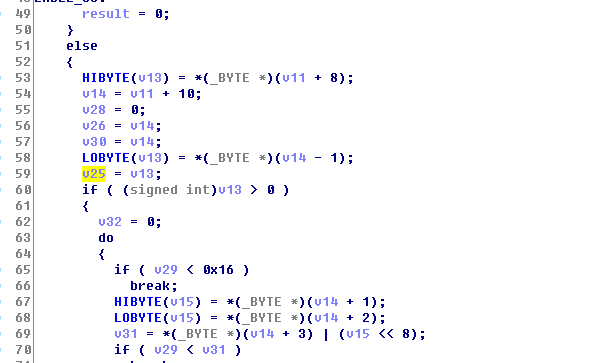
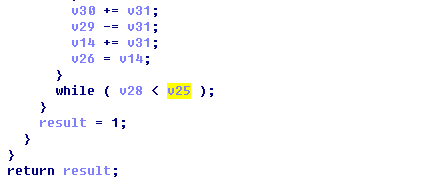


可以看到iccvid中发生溢出

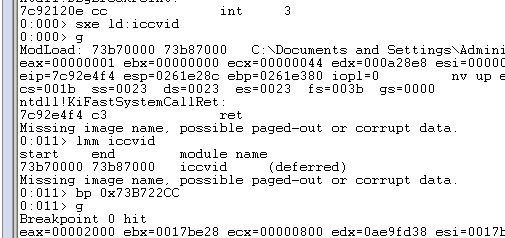


Ida打开跳到指定地址

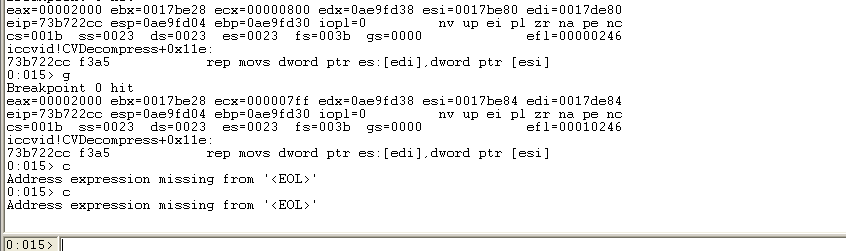
可以看到qemecpy函数将前一个地址的0x2000复制到后一个地址



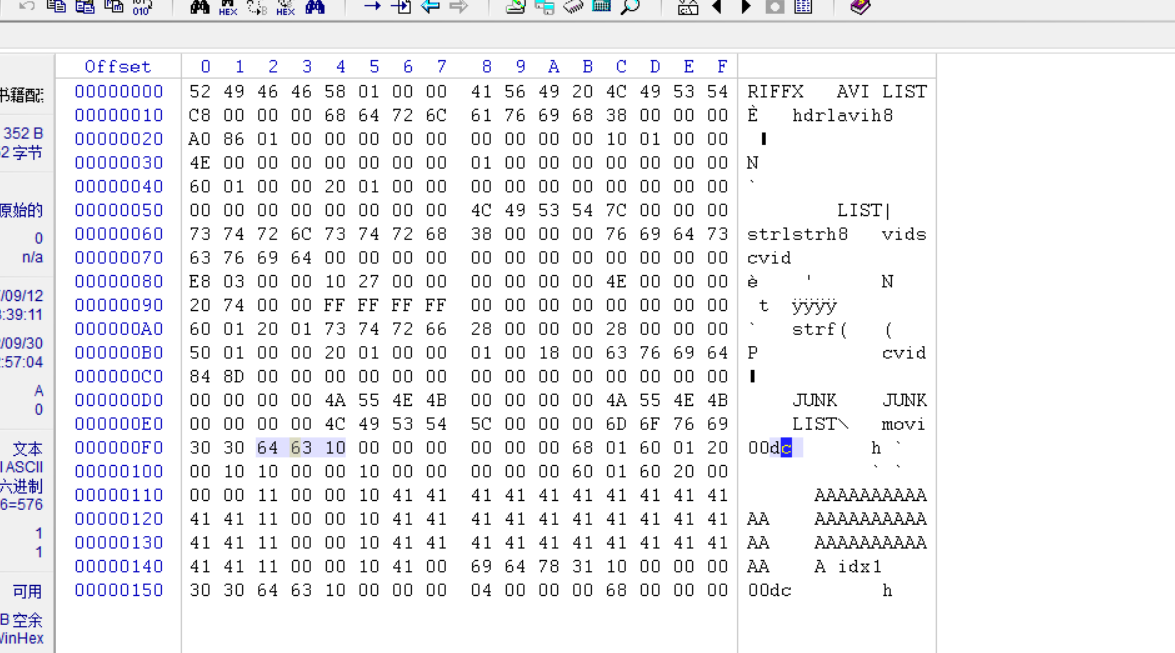
可以看到序号从0到v25



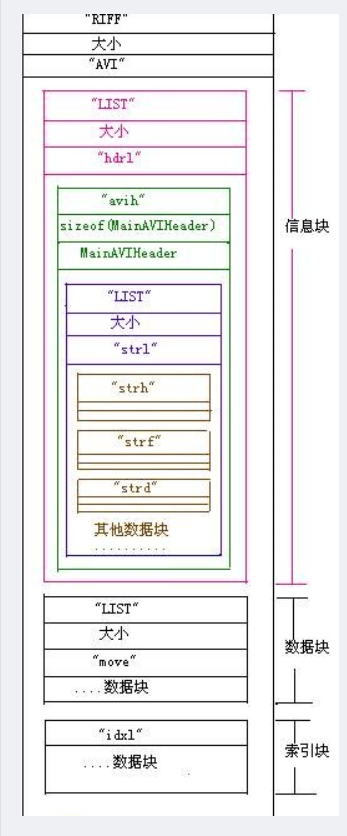
再次windbg打开加载符号iccvid



可以看到第三次发生crash

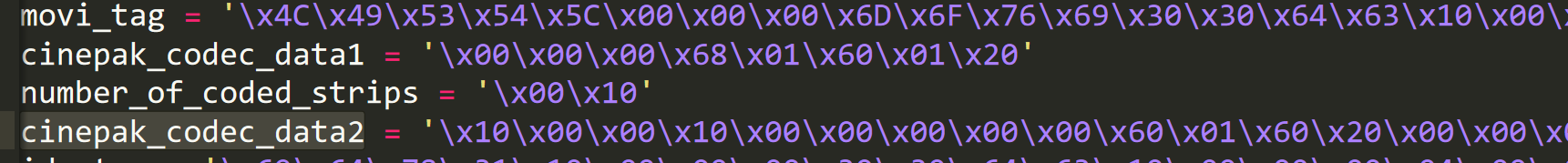


这是poc格式

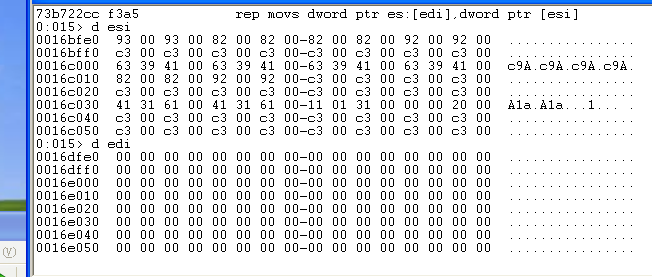


**movi列表**

dc表示压缩格式视频



Data为数据内容



可以看到内存数值如下解码后的情况