DWord Shoot软件破解实验

姓名： 汤清云 学号： 2013536

实验目的：

* 在VC6.0中使用IDE逐步调试
* 观察堆管理结构
* 记录Unlink节点的双向空闲链表的状态变化
* 了解堆溢出漏洞下的Dword Shoot攻击

实验报告：

1. 逐步调试如下

初始地址：

Hp:0x003a0000

H1: 0x003a0688

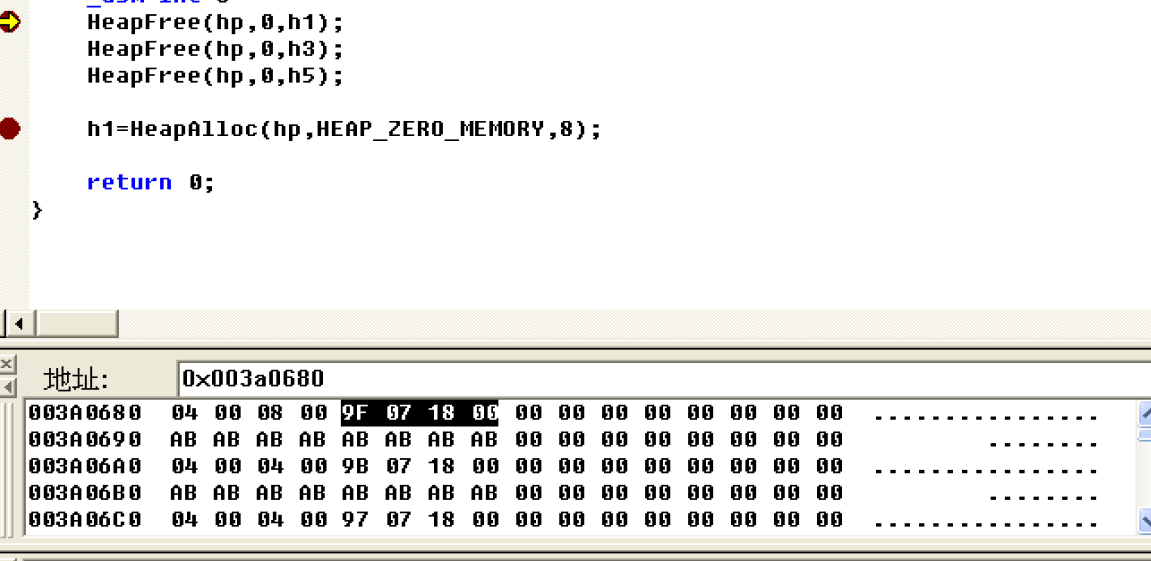
H2: 0x003a06a8

H3: 0x003a06c8

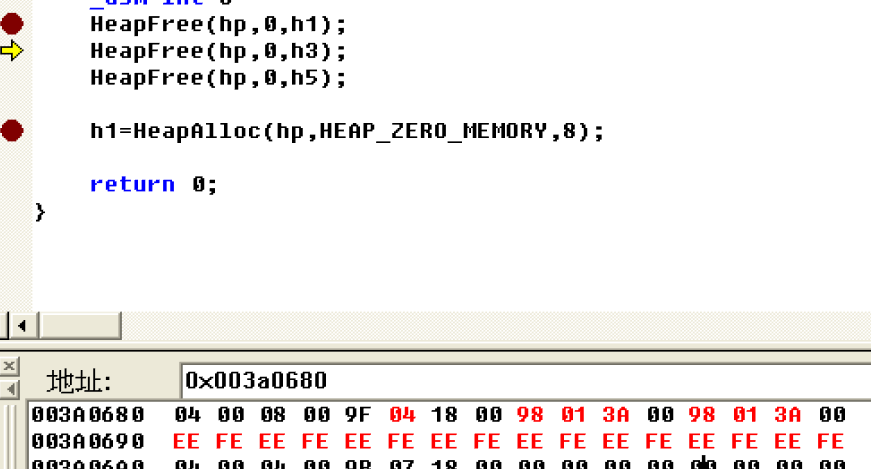
H4: 0x003a06e8

H5: 0x003a0708

H6: 0x003a0728

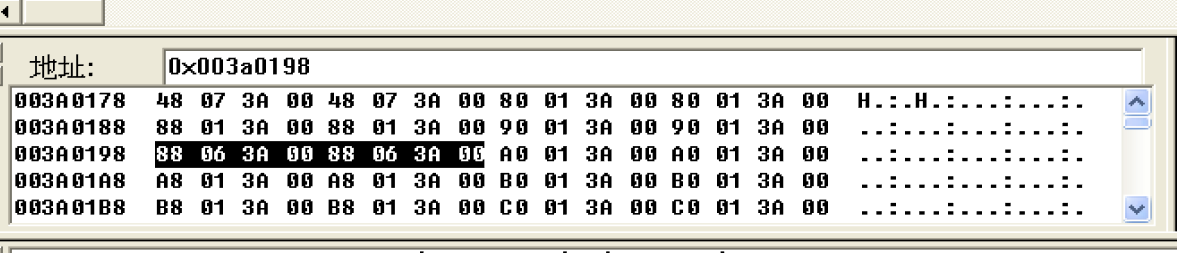


此时按下F10：

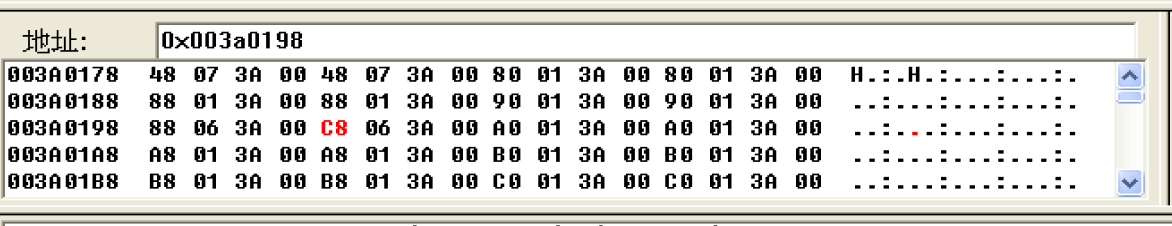


即此时h1的flink，blink均指向003a0198（即空闲链表f2）。

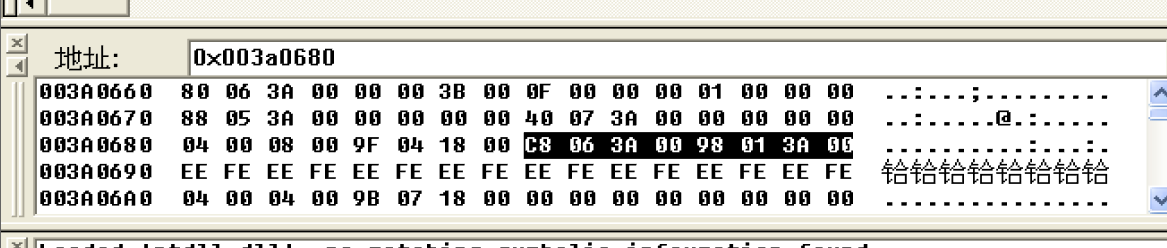
而f2的flink，blink均指向003a0688（即h1的块身）。



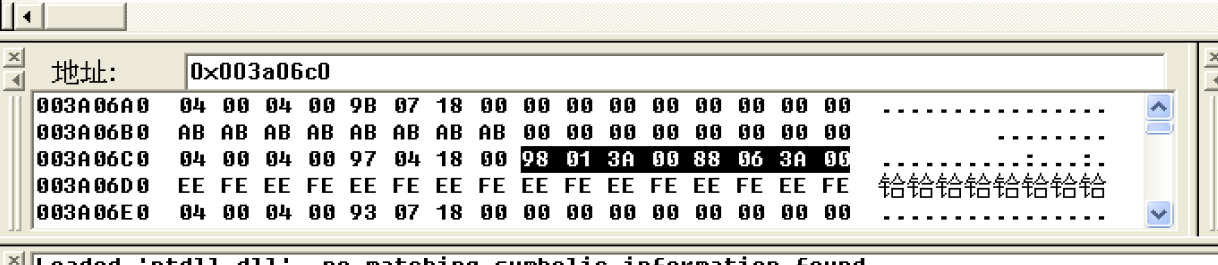
此时再次按下F10：



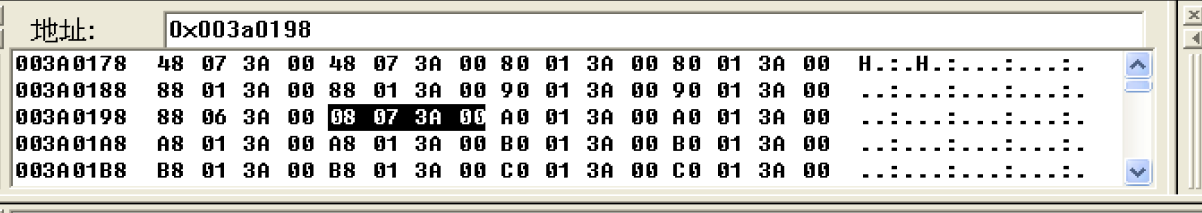
F2的link变为003a06c8（h3的地址）



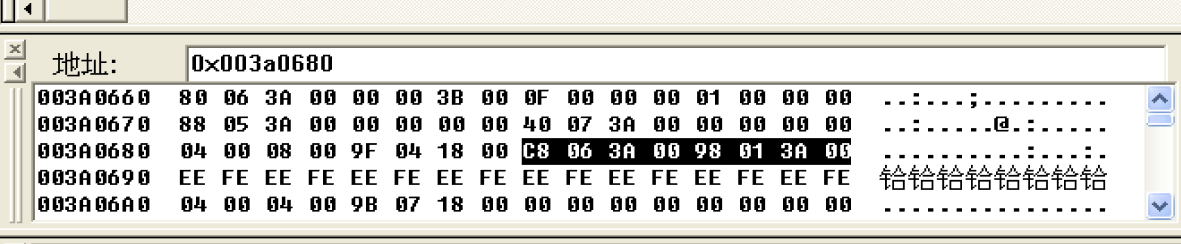
H1的flink变为003a06c8（h3的地址）



此时h3的flink，blink也分别指向f2和h1，再次按下F10：

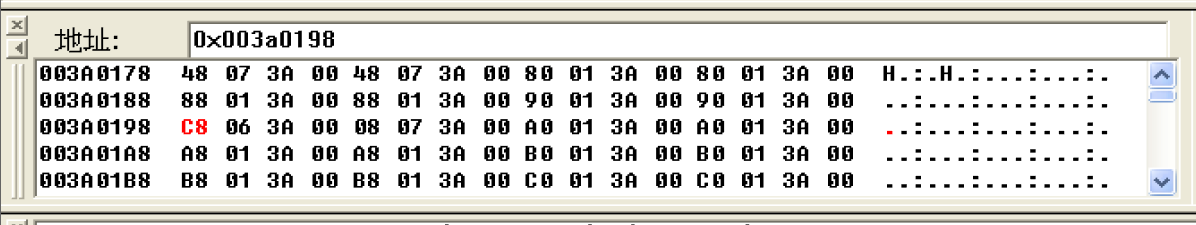


F2变为003a0708（h5）

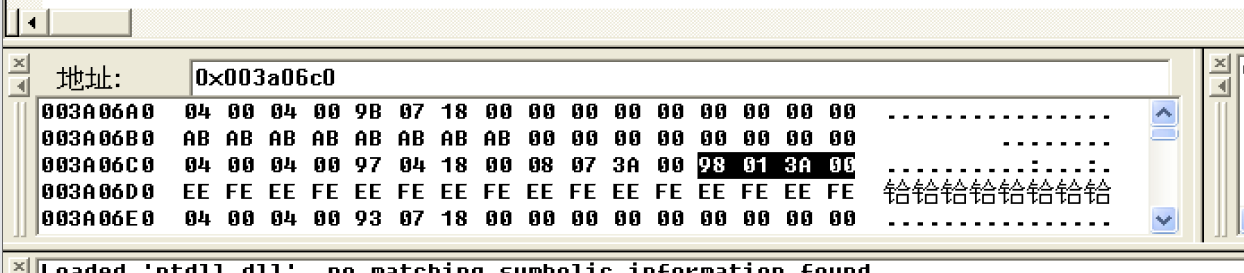


F2指向h5，h5的flink指向f2，blink指向h3，h3的flink指向h5，blink指向h1，h1的flink指向h3，blink指向f2

即：（front）f2—h5—h3—h1（back），不更改代码向下执行：

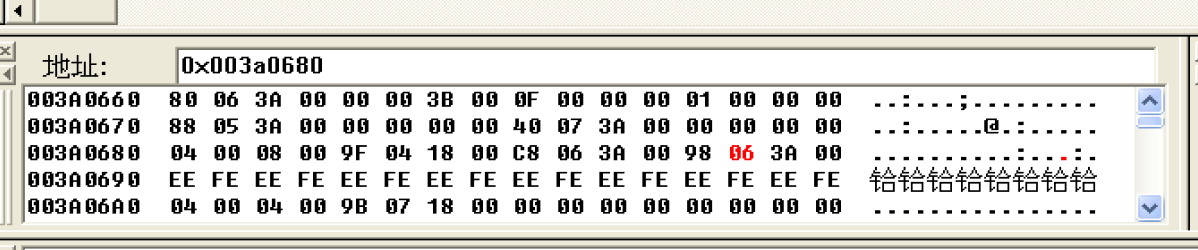


F2指向了003a06c8（h3块身），说明h1被摘走，再去查看h3的blink，变化为指向f2：

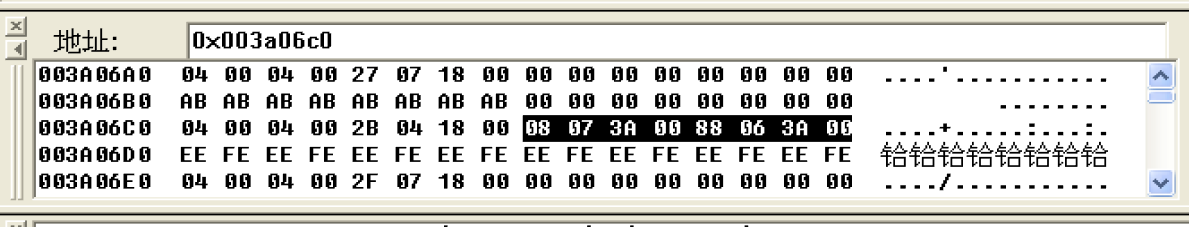


即：（front）f2—h5—h3（back）

若篡改h1的blink为003a0698：



再进行下一步时即发生dword shoot



H3的blink指向了003a0688，即它自身，而非f2，说明发生dword shoot。