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

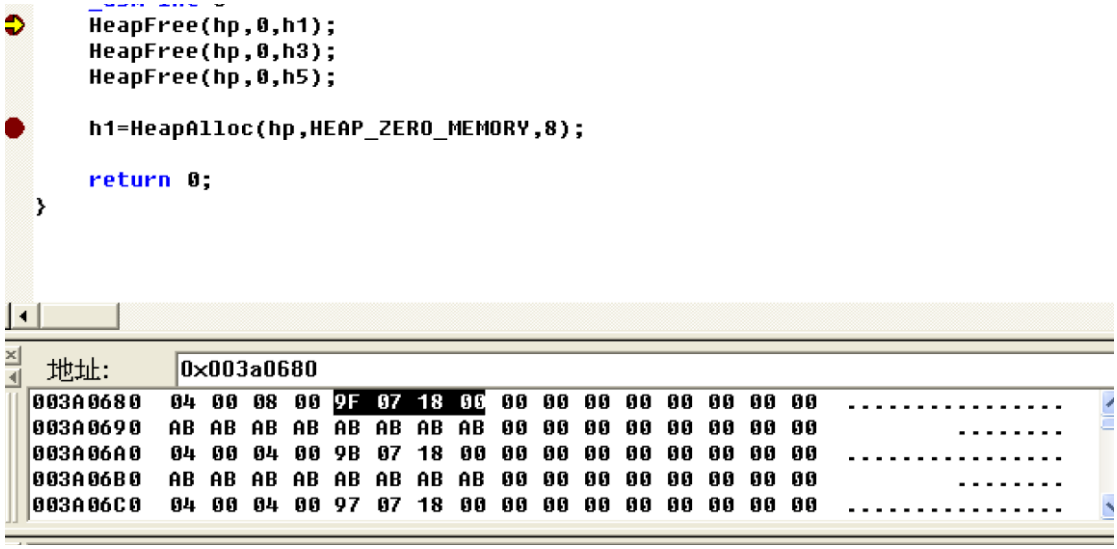
   H2: 0x003a06a8

   H3: 0x003a06c8

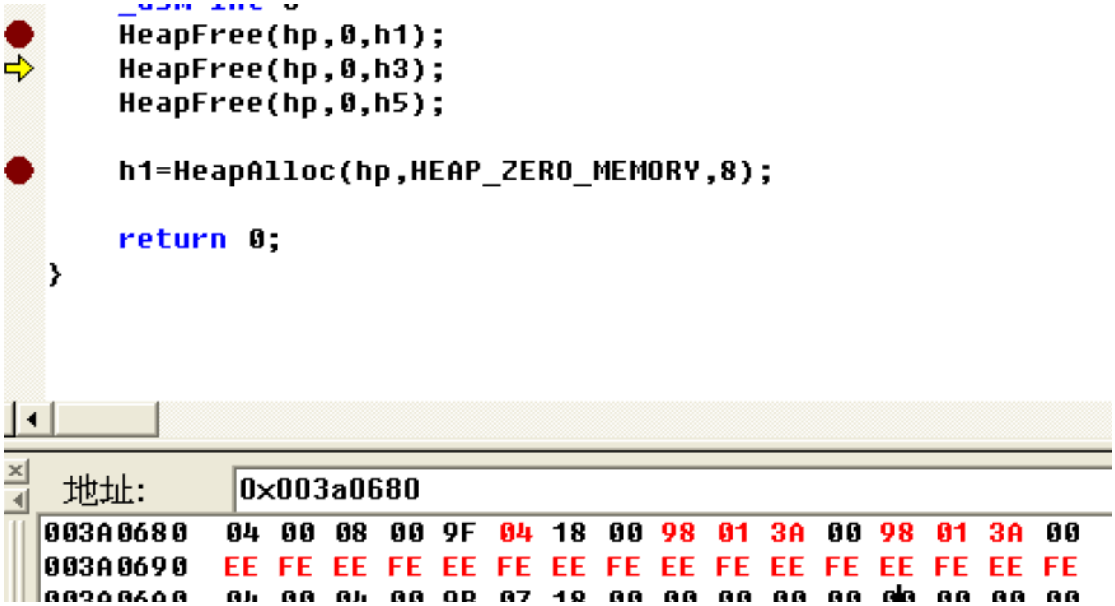
   H4: 0x003a06e8

   H5: 0x003a0708

   H6: 0x003a0728

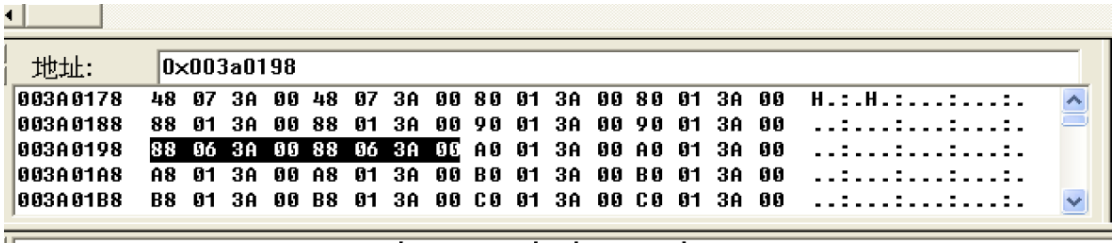


此时按下 F10：

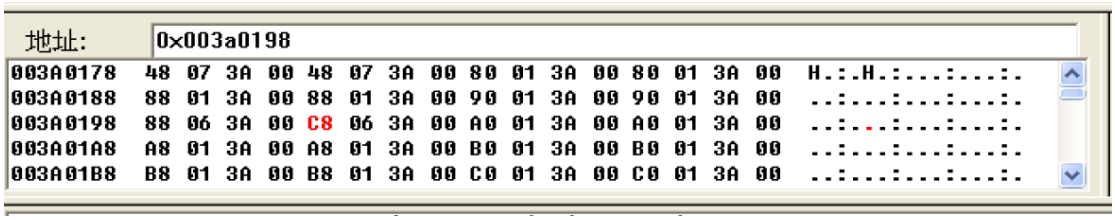


即此时 h1 的 flink，blink 均指向 003a0198（即空闲链表 f2）。

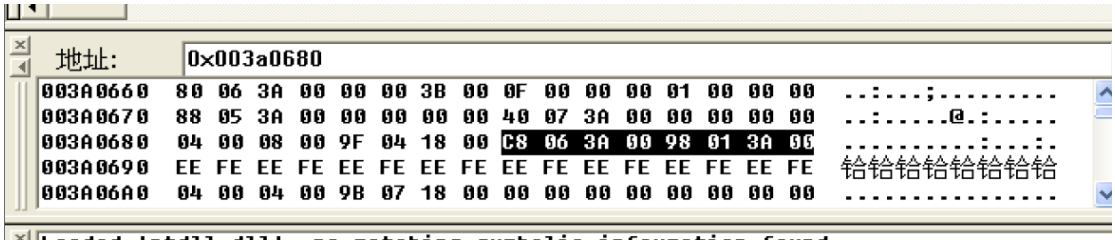
而 f2 的 flink，blink 均指向 003a0688（即 h1 的块身）。



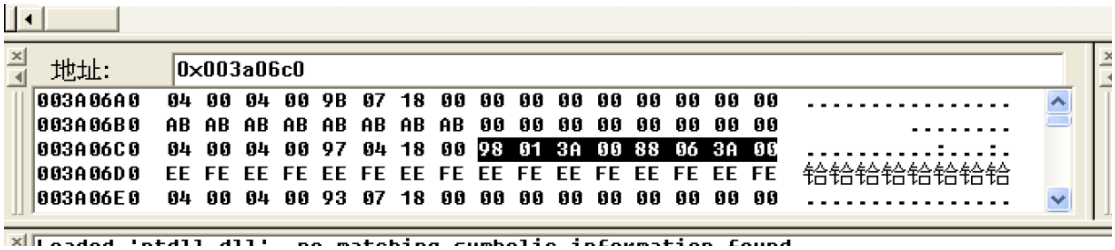
此时再次按下 F10：



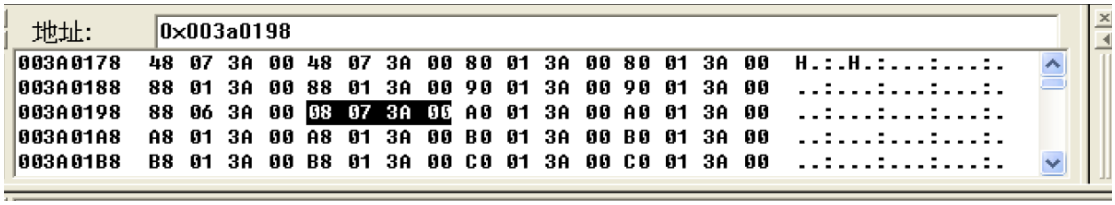
F2 的 link 变为 003a06c8（h3 的地址）



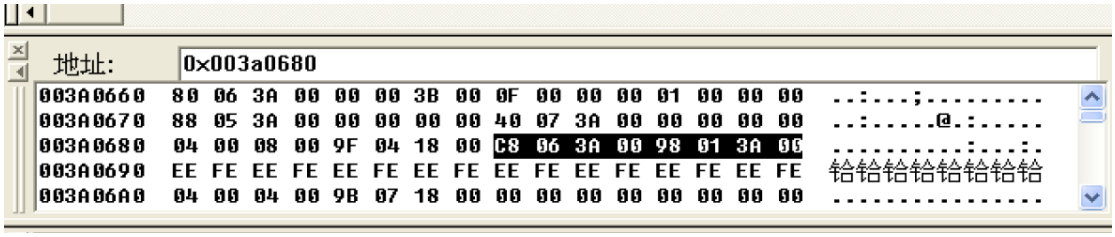
H1 的 flink 变为 003a06c8（h3 的地址）



此时 h3 的 flink，blink 也分别指向 f2 和 h1，再次按下 F10：



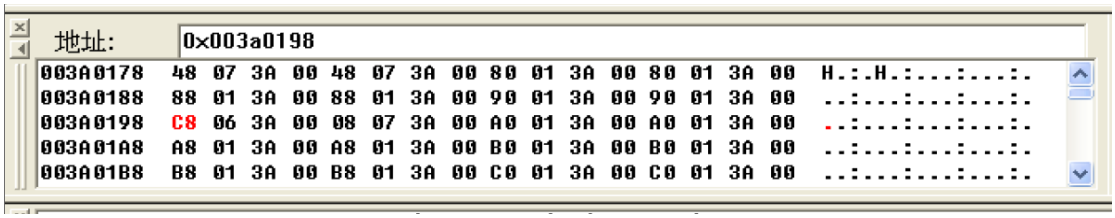
F2 变为 003a0708（h5）



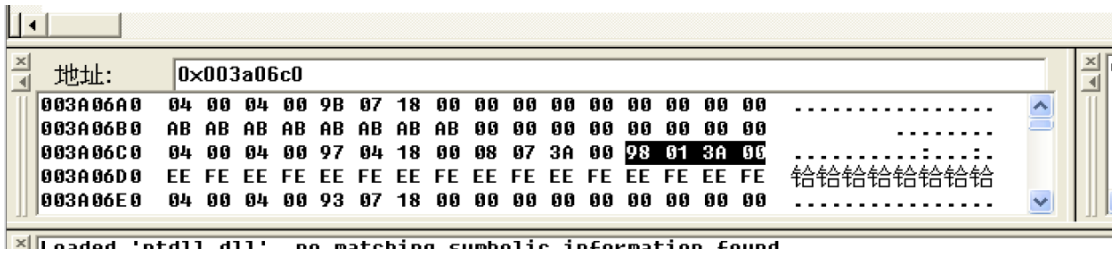
F2 指向 h5，h5 的 flink 指向 f2，blink 指向 h3，h3 的 flink 指向 h5，blink 指

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：

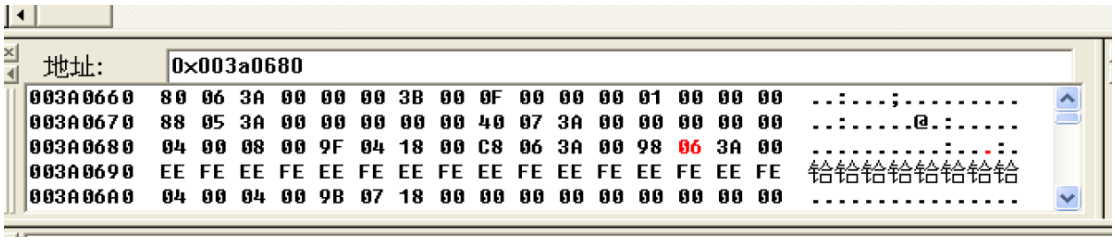


F2 指向了 003a06c8（h3 块身），说明 h1 被摘走，再去查看 h3 的 blink，变化为指向 f2：

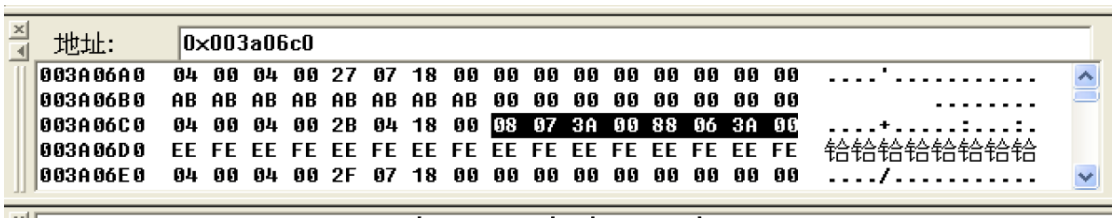


即：（front）f2—h5—h3（back）

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。