《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

**实验名称：**

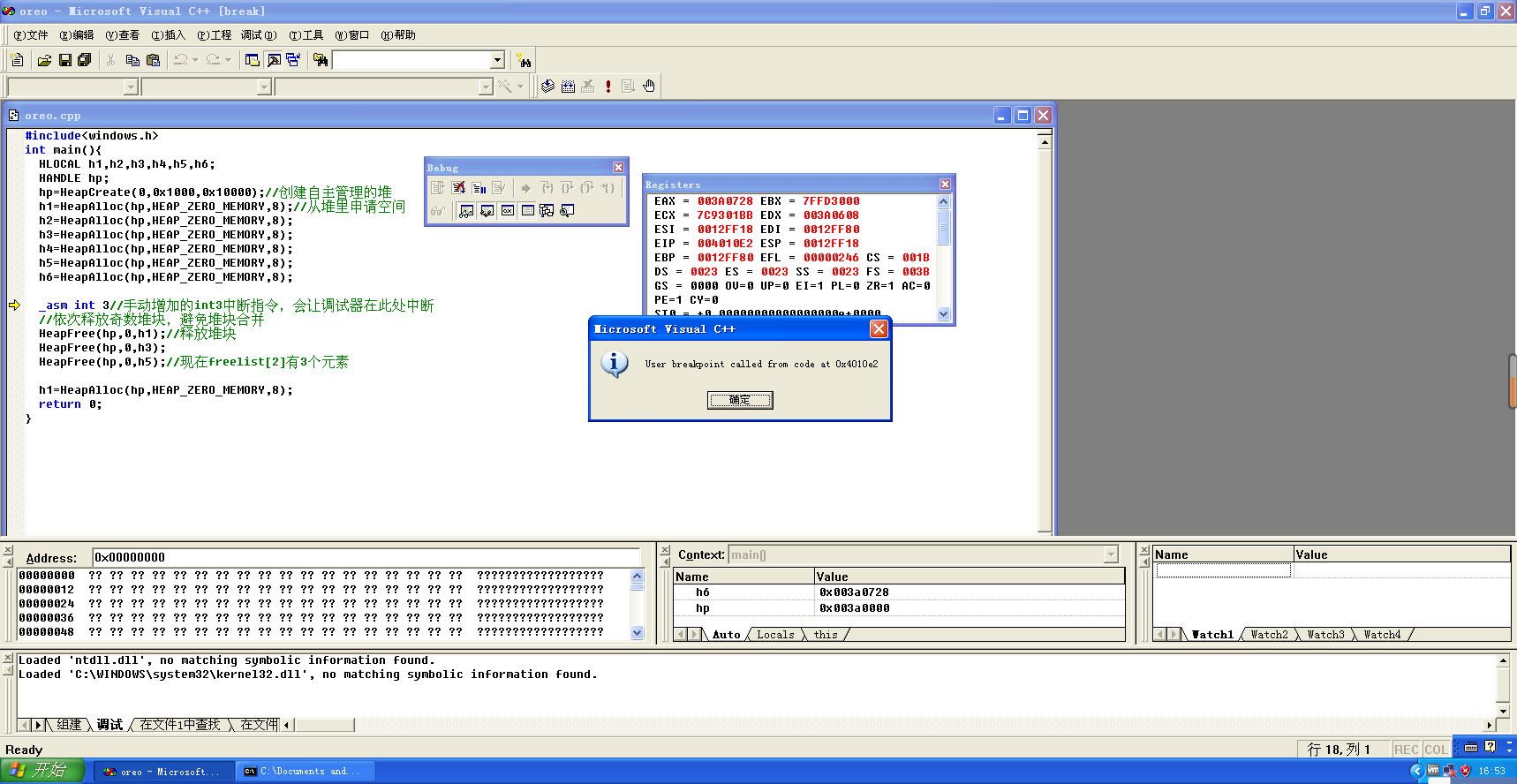
堆溢出Dword Shoot演示实验

**实验要求：**

以第四章示例4-4代码为准，在VC IDE中进行调试，观察堆管理结构，记录Unlink节点时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。

**实验过程：**

1.VC调试：



2.分析流程：

程序首先创建了大小0x1000的堆区，连续申请了6个大小为8字节（16字节）的堆块；在三次释放后，形成三个16字节的空闲堆块放入空表freelist；再次申请8字节的堆块，则会从freelist中摘取第一个空闲堆块（h1）；如果此时修改h1堆块的指针，则会发生DWORD SHOOT。

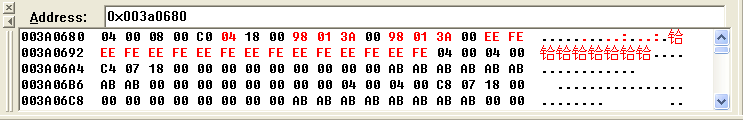
3.记录Unlink节点时的双向空闲链表的状态变化：

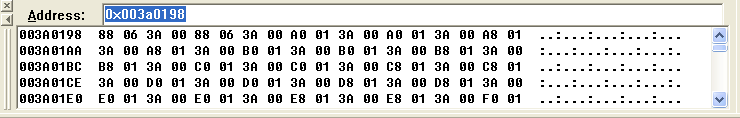
块首：0x003a680

H1：0x003a688

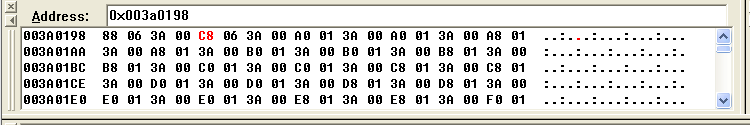
H3：0x003a06c8

H5：0xxx3a0708

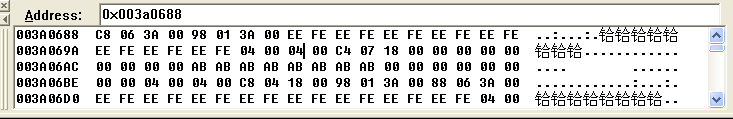
释放H1：  
h1的flink=blink=0x003a0198即freelist。



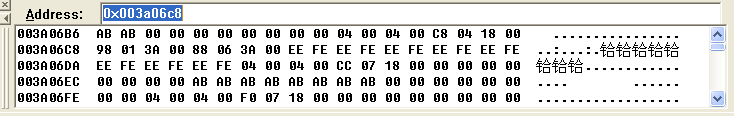
Freelist的flink=blink=0x003a0688即h1。

释放H3：

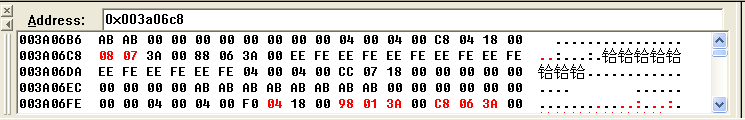
Freelist的blink=0x003a06c8即H3。



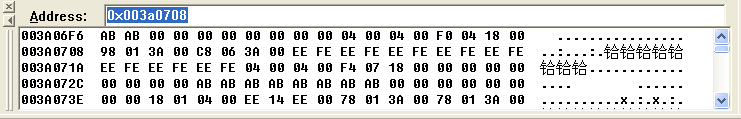
H1的flink=0x003a06c8即H3，blink=0x003a0198



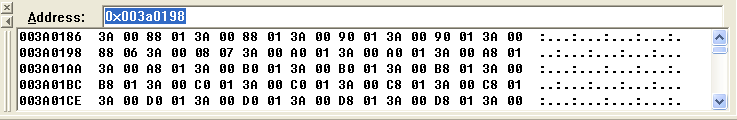
H3的flink=0x003a0198，blink=0x003a0688即H1

释放H5：

H3的flink=0x003a0708即H5



H5的flink=0x003a0198，blink=0x003a06c8即H3



Freelist的blink=0x003a0708即H5

**心得体会：**基于 Dword Shoot 攻击，攻击者甚至可以劫持进程，运行植入的恶意代码。比如，当构造的地址为重要函数调用地址、栈帧中函数返回地址、栈帧中 SEH 的句柄等时，写入的任意数据可能就是恶意代码的入口地址。