《漏洞利用及渗透测试基础》实验报告

姓名：申宗尚 学号：2213924 班级：信息安全

**实验名称：**

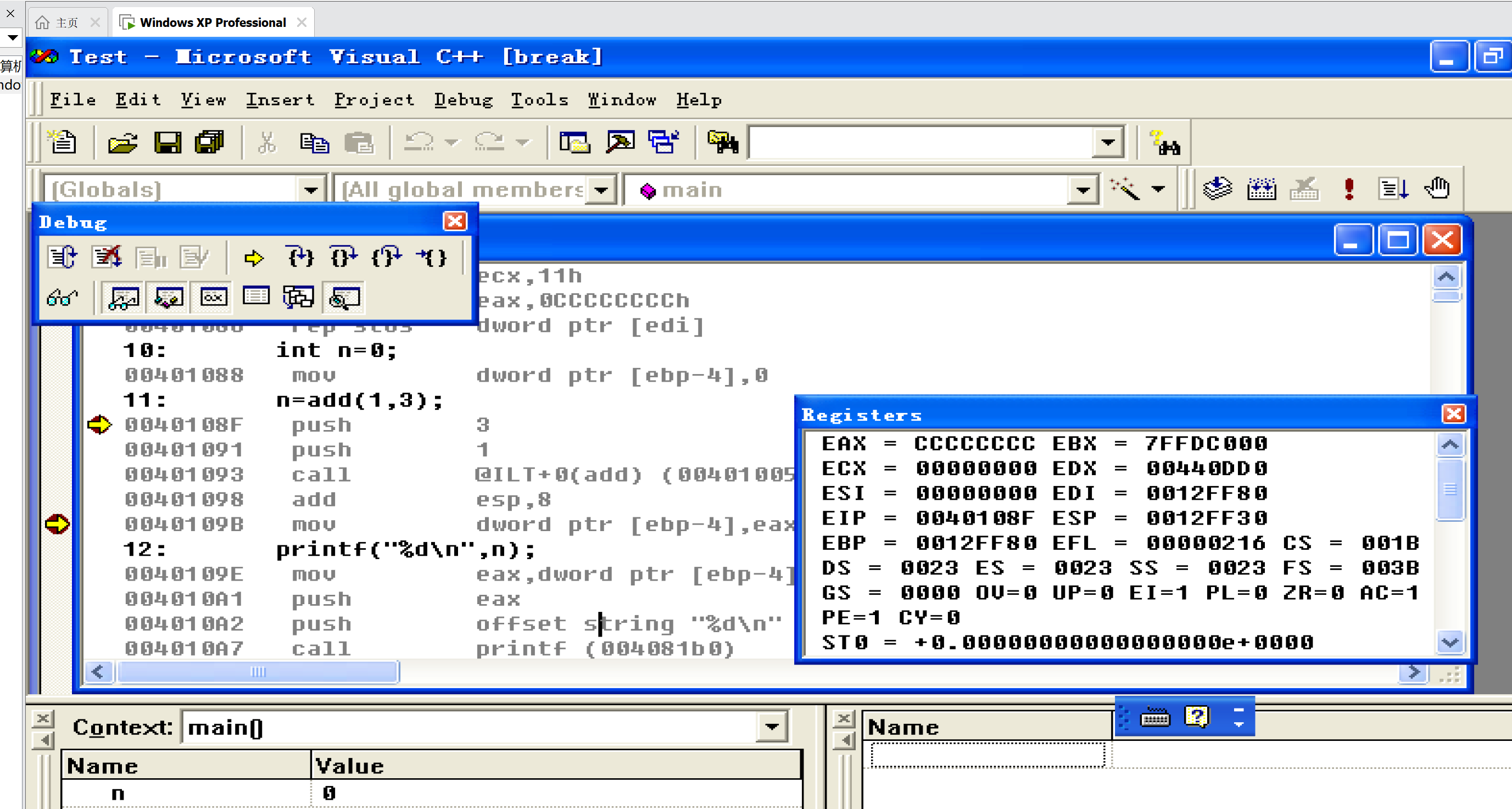
IDE反汇编实验

**实验要求：**

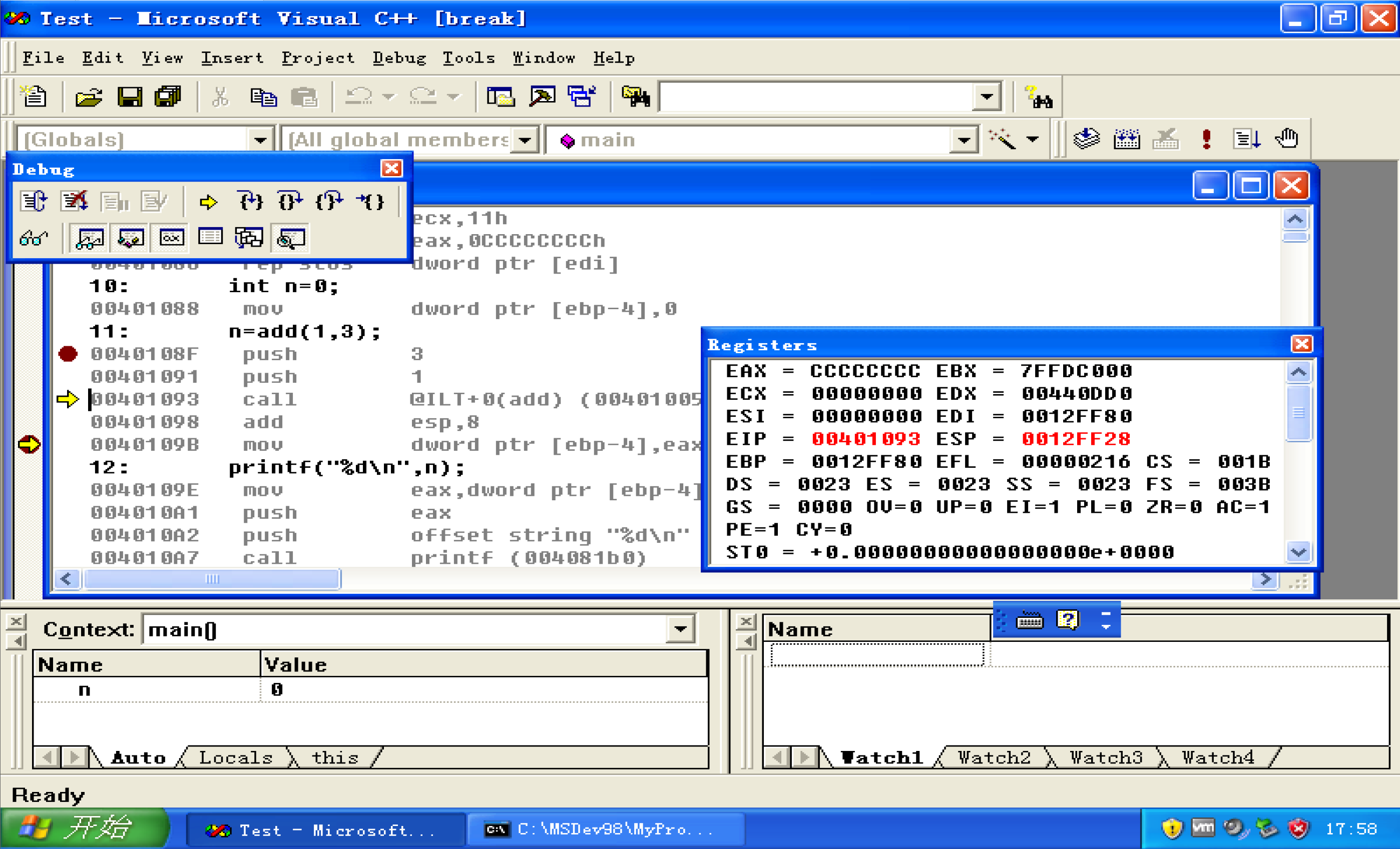
根据第二章示例2-1，在XP环境下进行VC6反汇编调试，熟悉函数调用、栈帧切换、CALL和RET指令等汇编语言实现，将call语句执行过程中的EIP变化、ESP、EBP变化等状态进行记录，解释变化的主要原因。

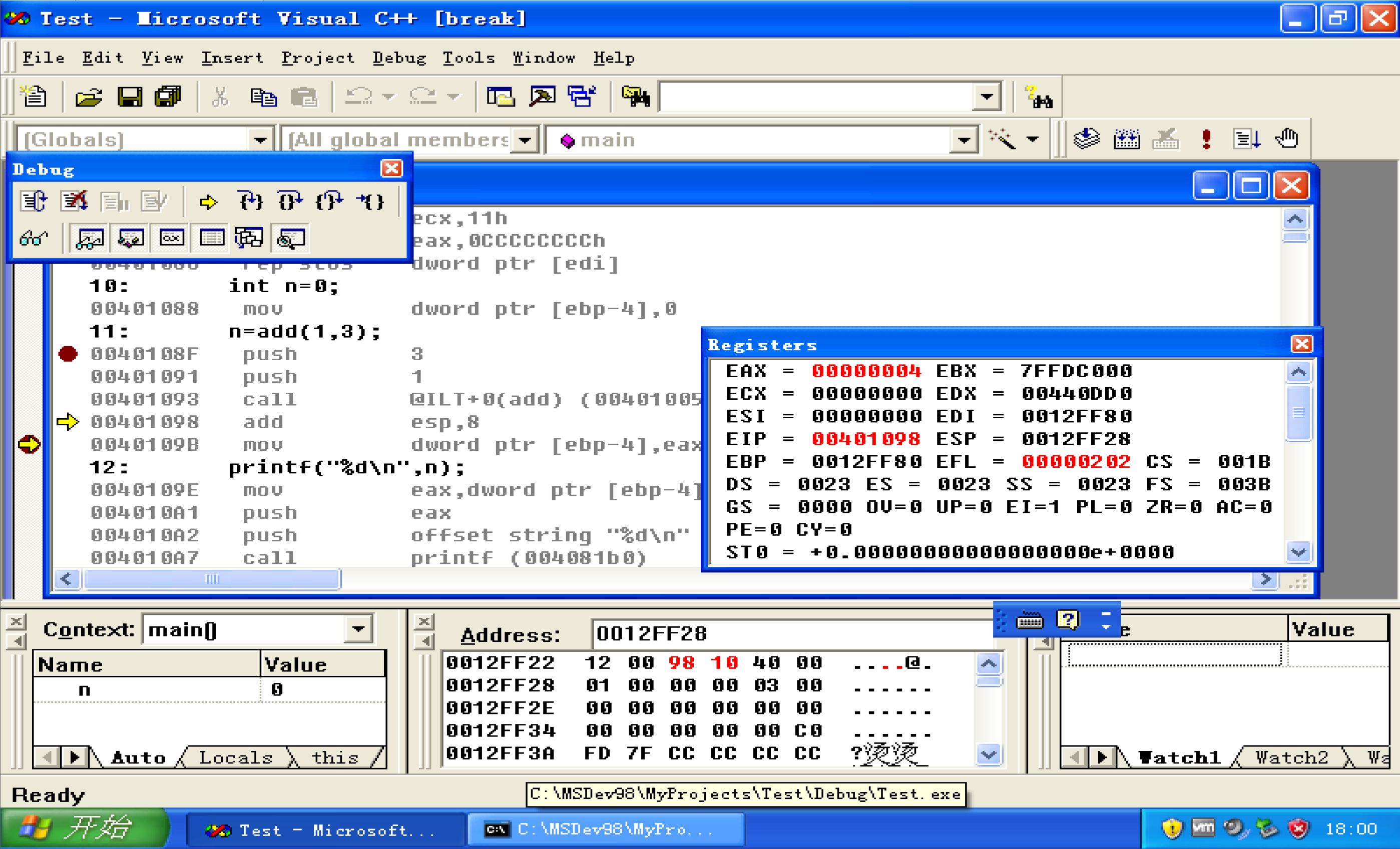
**实验过程：**

1. 进入VC反汇编



2. 观察add函数调用前后语句



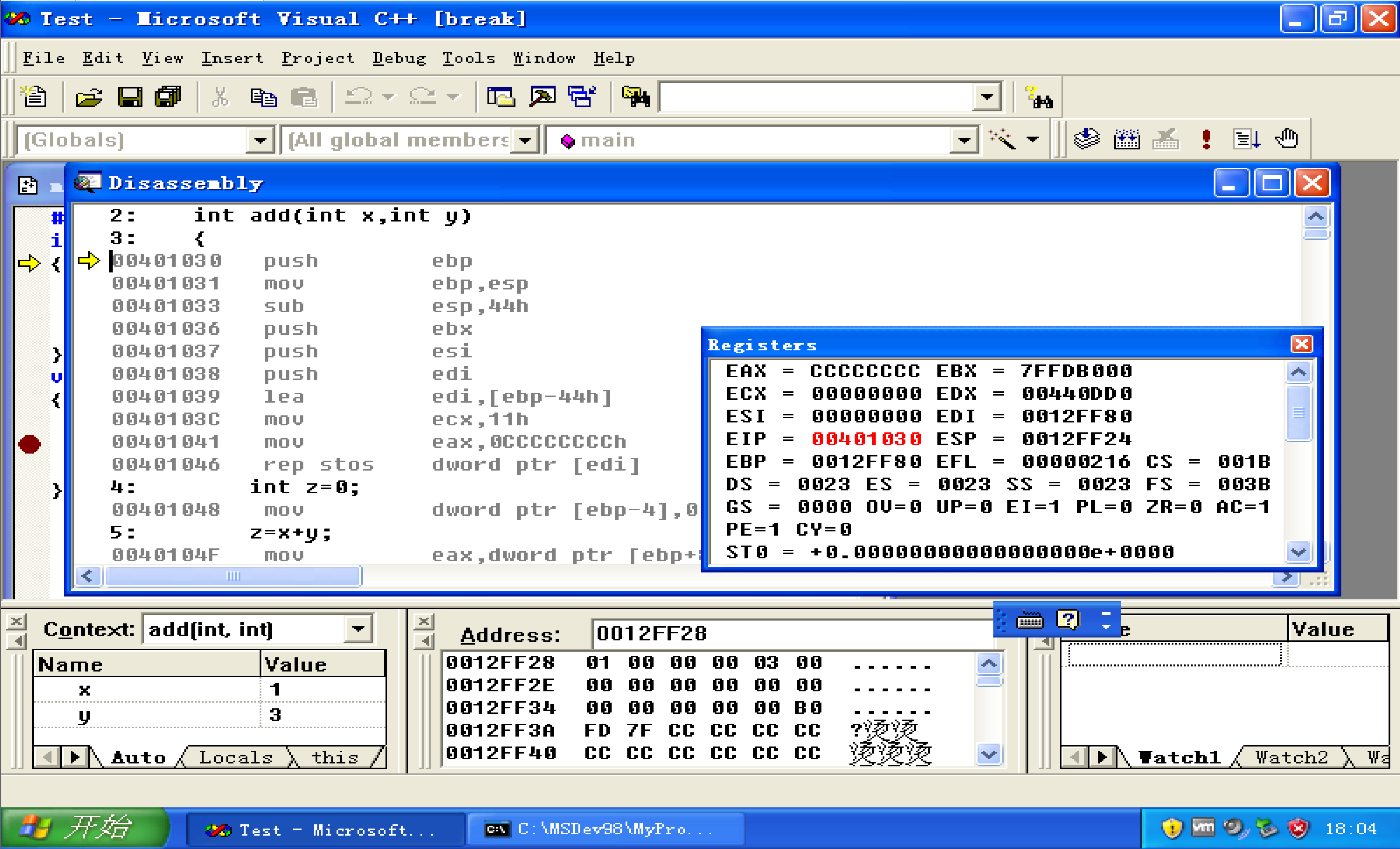


Call指令执行前，通过从右往左传递参数，将参数3，1依次推入栈内，随后进行函数调用。

Call指令执行后，eax寄存器变为00000004，EIP变为下一步add指令的地址。

最后将eax（即add函数的返回结果）储存至变量n的存储地址

3. add函数内部栈帧切换等关键汇编代码



在add函数内部，先将ebp（main函数栈帧地址）存入栈顶，再将栈顶指针esp值赋给ebp，成为add函数新的栈帧底部，再将esp进行-44h的操作，预留出新的栈空间，随后进行栈内部空间的初始化、清零操作。

在进行完运算后，将原本存入的main函数栈帧取出，并给ebp赋值，从而切换栈，再更改EIP位置，使其进行完函数调用后接着运行主函数下一条代码。

**心得体会：**

通过实验，掌握了RET指令的用法：RET指令实际就是执行了Pop EIP

同时，对于程序中函数的调用底层逻辑、栈空间切换有了更深层的认识，（为何函数调用耗费空间、时间，因为会有很多栈的操作和空间的初始化、清零操作），因此在实际中，除了经常用到的复杂操作，应该以性能为主，尽量写在主函数中。