《软件安全》实验报告

姓名：梁婧涵 学号：2112155 班级：1120

实验名称：格式化字符串漏洞

实验要求：

以第四章示例4-7代码，完成任意地址的数据获取，观察任意地址Release模式和Debug模式的差异，并进行总结。

#include <stdio.h>

int main(int argc,char \*argv[])

{

char str[200];

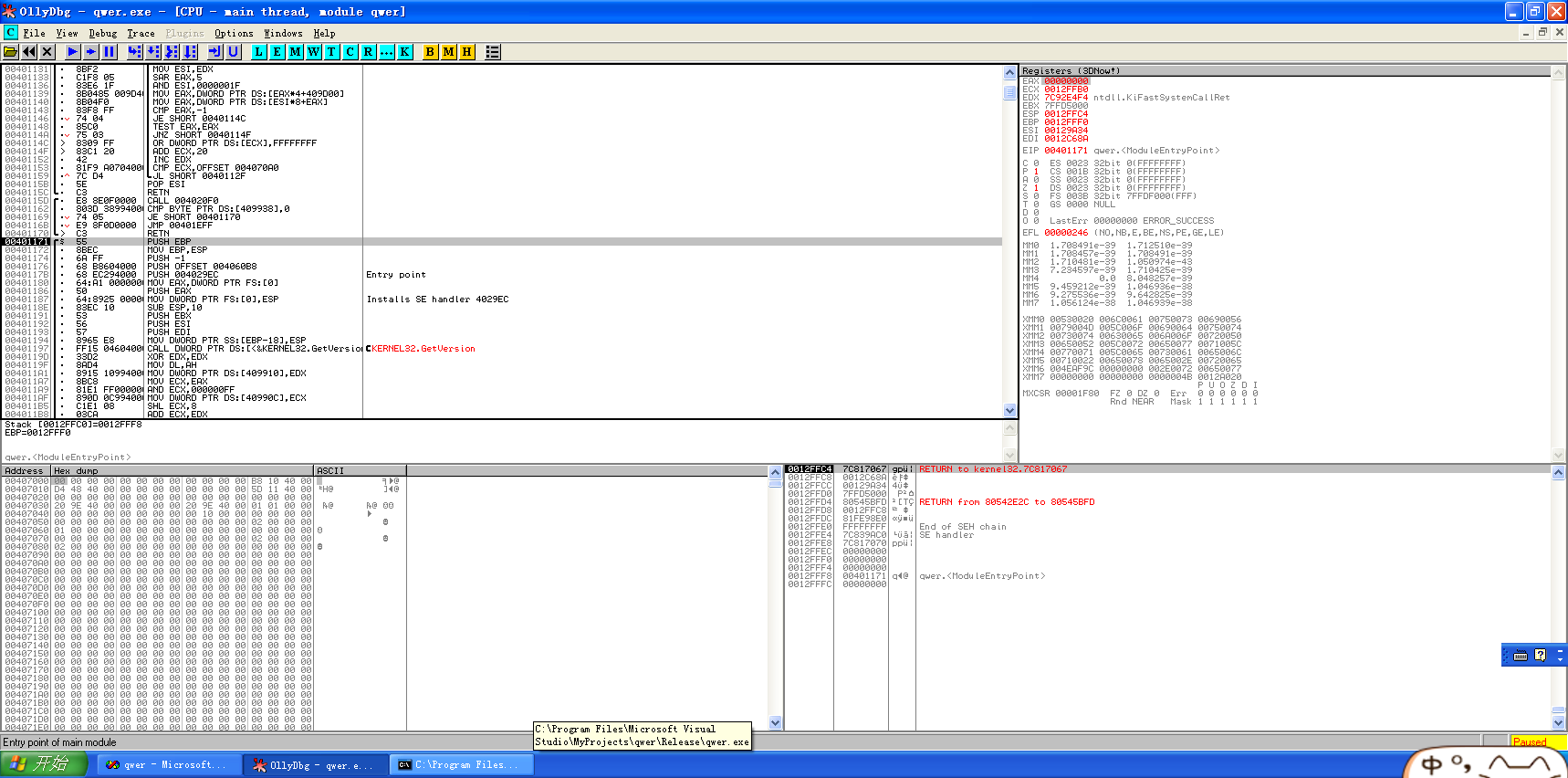
fgets(str,200,stdin);

printf(str);

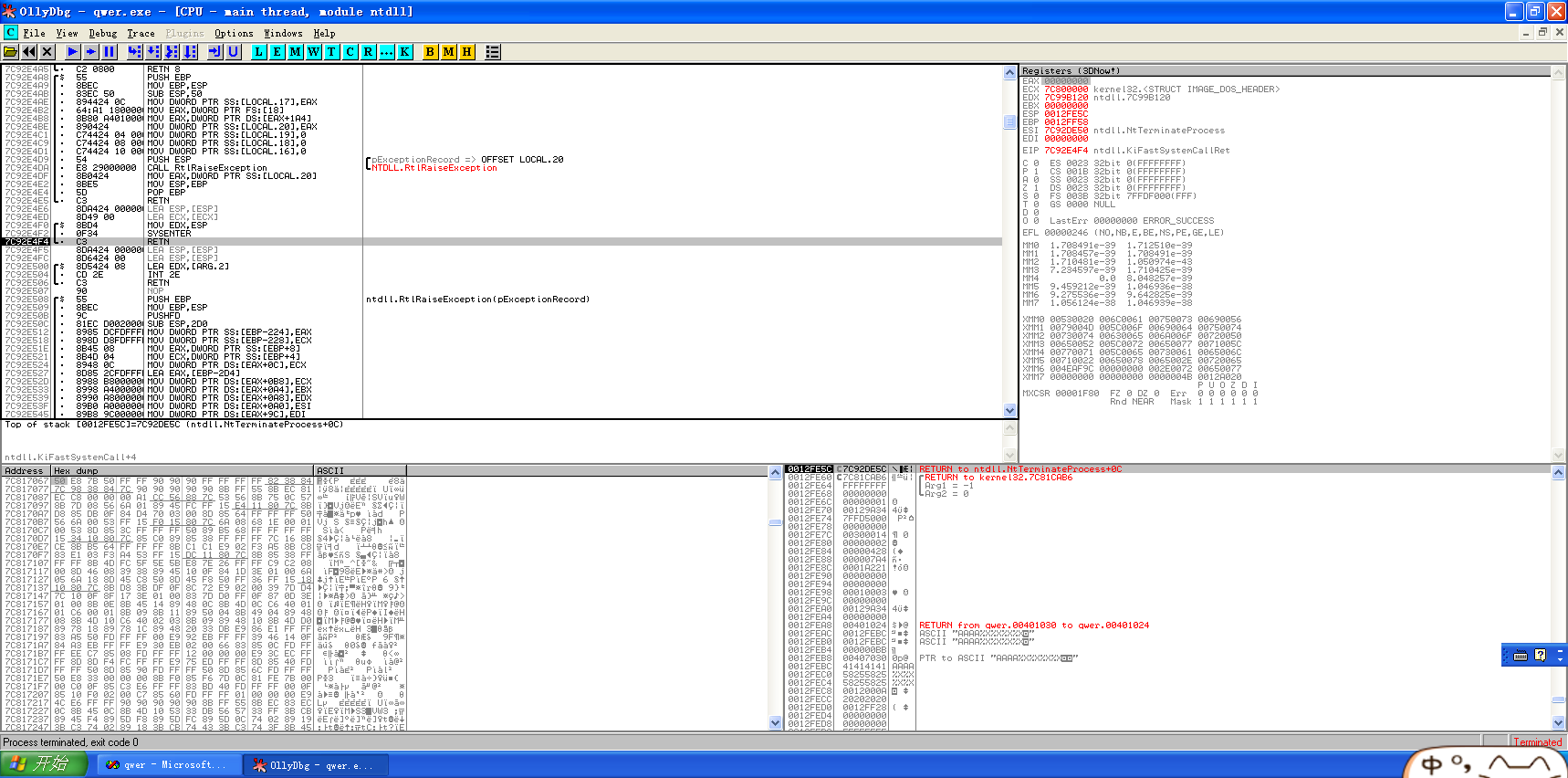
return 0;

}

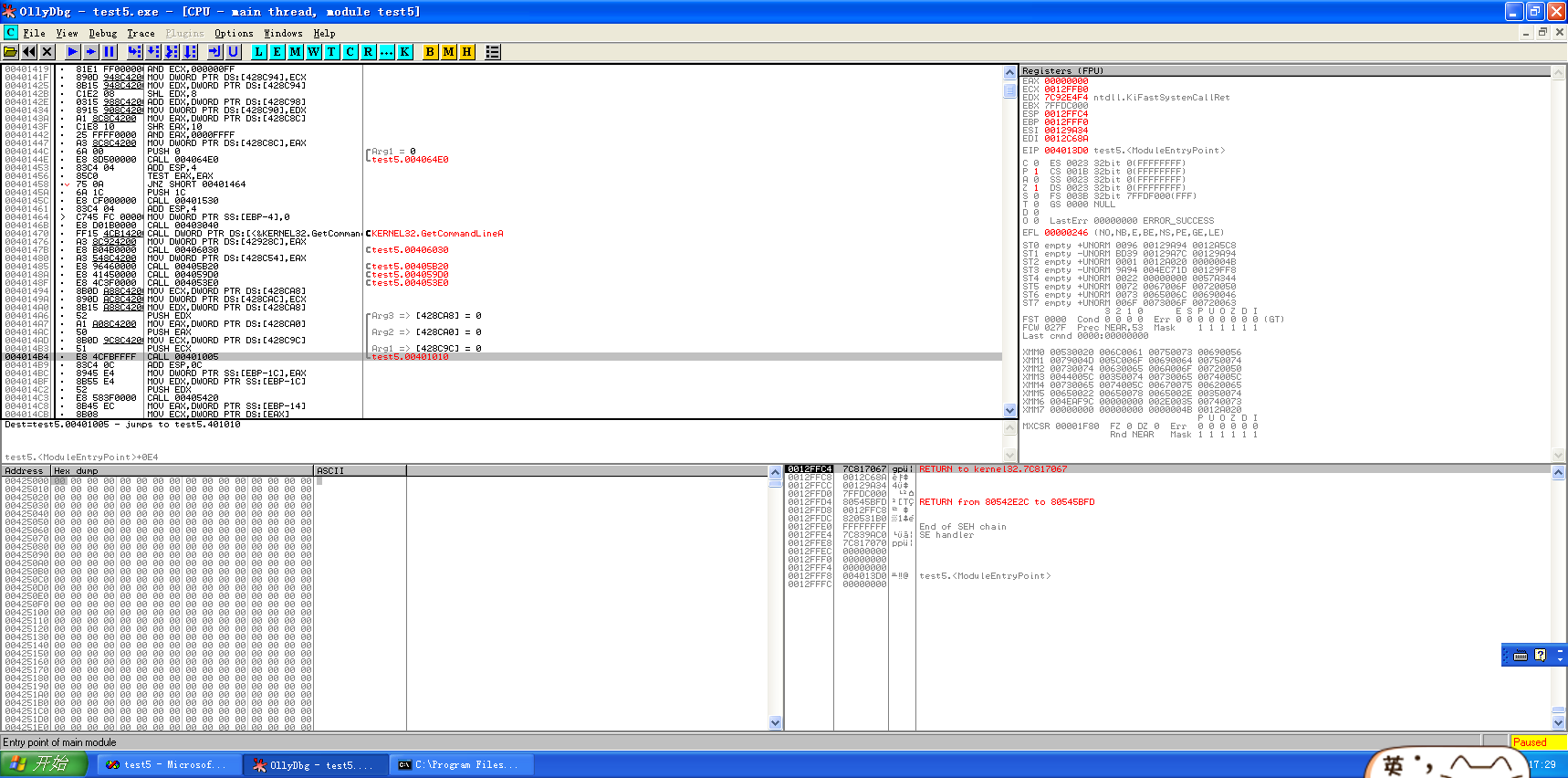
实验过程：

1. 这段代码实现了从标准输入读取字符串并将打印到标准输出。由于没有对输入的字符串进行任何处理或验证，因此可以通过输入恶意数据来访问任意地址的数据。
2. 在Release模式下，编译器会进行优化，例如删除未使用的代码和变量，以及使用更高效的代码生成技术。这可能导致在调试过程中可用的信息减少，因此可能更难观察和理解程序的行为。此外，由于优化的存在，可能会对实验结果产生影响。

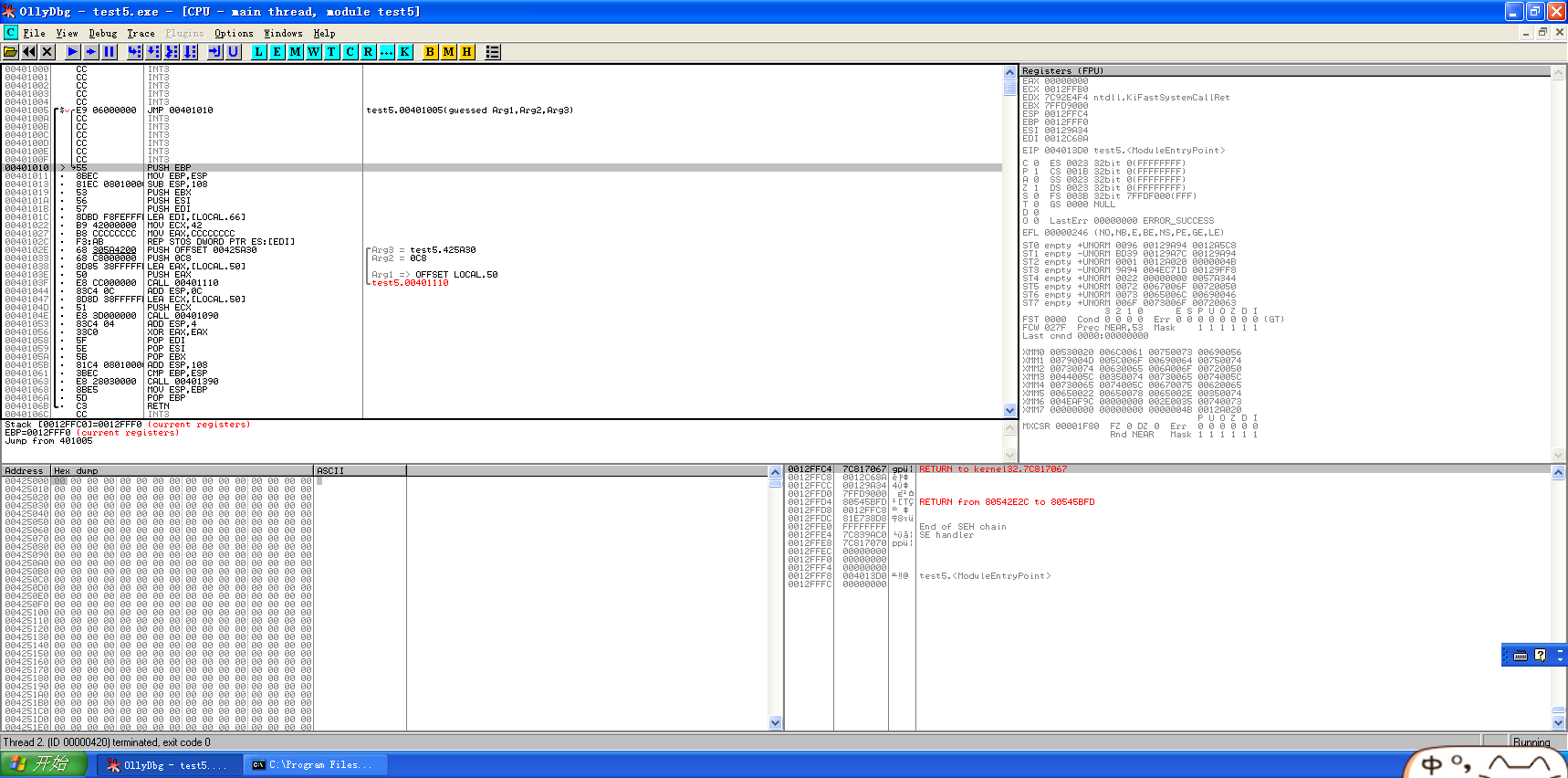
发现sub抬高了0C8（200字节），简洁，三个push，把esp复制到eax0012FEBC（要输的字符串地址），输入“AAAA%X%X%X%X”



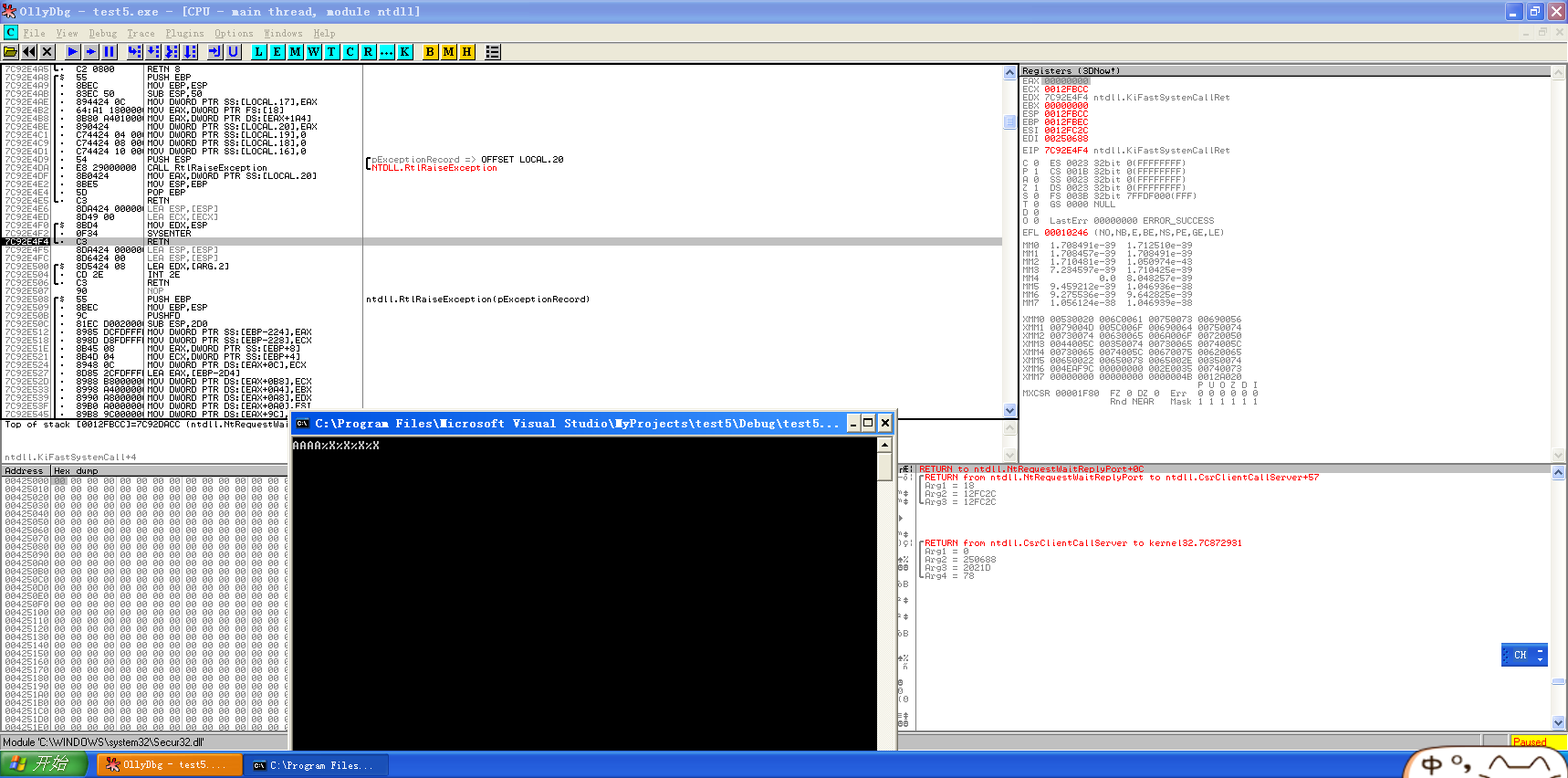
1. 在Debug模式下，编译器通常不会进行优化，因此生成的代码可能更容易理解和调试。此外，Debug模式下会添加一些额外的信息，例如符号表和调试符号，以帮助调试器定位代码中的问题。

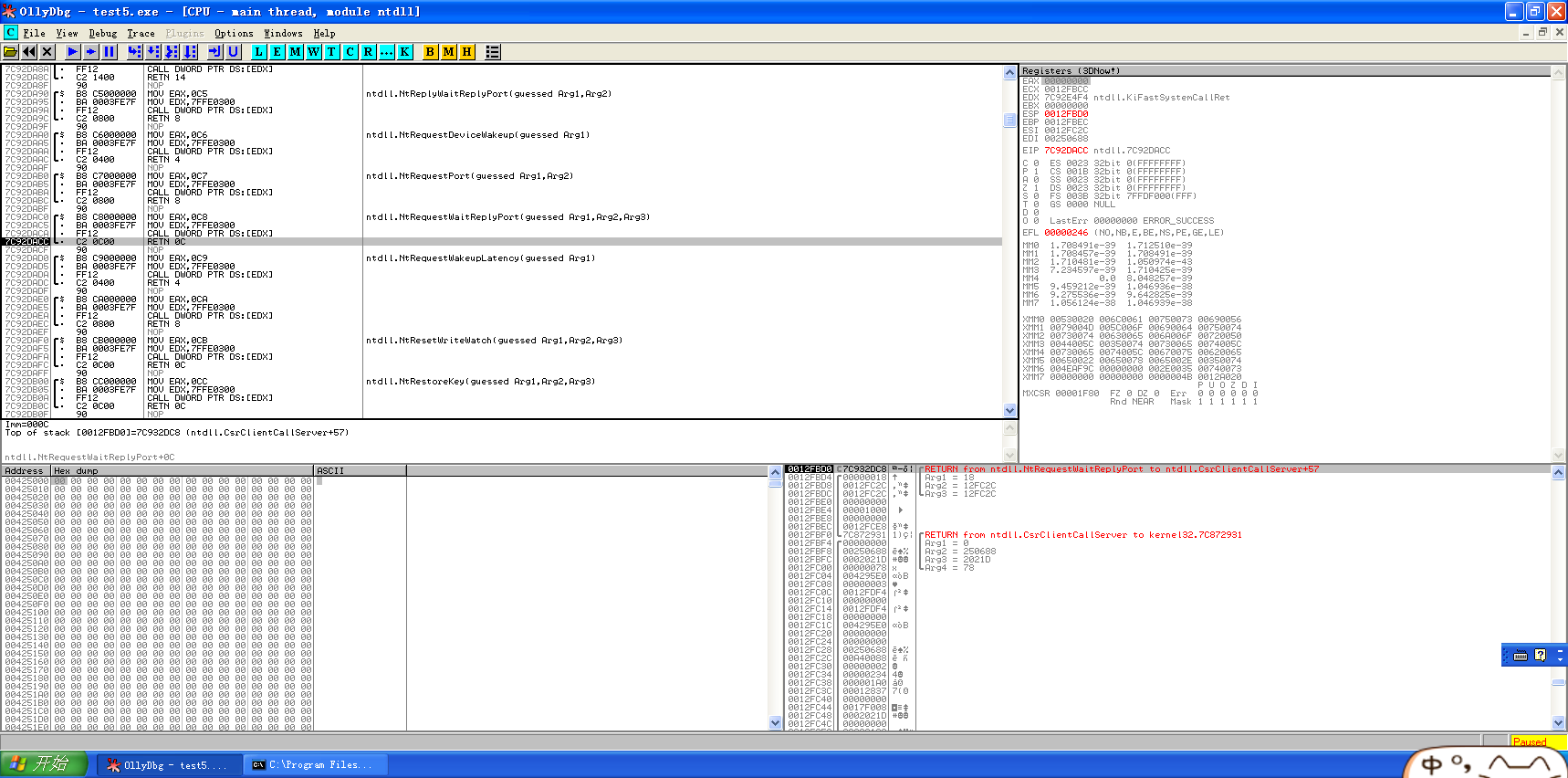


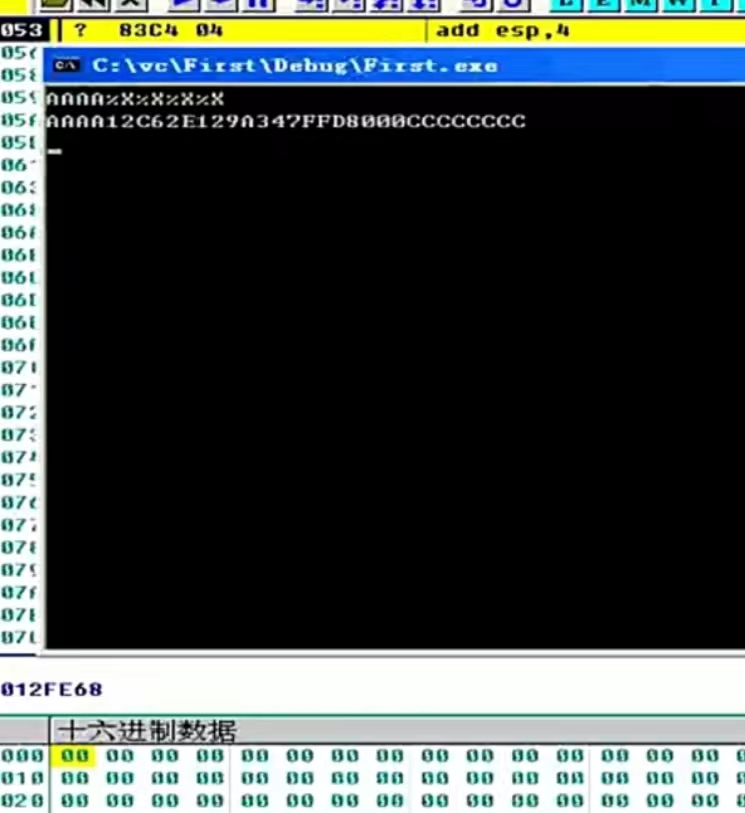
找到主函数，进入



Debug模式push ebp，三个push在栈顶部，通过ecx和eax将108初始化，lea求地址，edp-0C8是字符串地址。



F8

字符数组的起始地址，参数入栈“AAAA%X%X%X%X”运行得到

心得体会：

通过输入特定的字符串来访问程序的不同部分，例如栈、堆和全局变量。我们可以在不同的模式下运行程序并观察其输出或使用调试器来查看内存中的数据。我们可以比较不同模式程序的行为和输出，并总结它们之间的差异和影响。

通过这个实验，我深刻认识到了代码中的安全问题和潜在漏洞。尽管这个程序只是一个简单的输入输出程序，但是由于没有进行任何输入验证和处理，可以轻松通过输入特定字符串来访问任意地址的数据，从而导致程序崩溃或被攻击者利用。同时，我也认识到了代码的优化和调试堆程序行为的影响。在Debug模式下，程序会添加额外的信息，这有助于我们理解和调试程序，但是可能导致程序运行速度较慢。而在Release模式下，程序会进行优化，这可以提高程序的运行速度，但是可能会降低调试和观察程序行为的能力。