

**汇编语言和逆向技术实验报告**

**实验七：Reverse Engineering Challenge**

****

学 院 网络空间安全学院

专 业 信息安全

学 号 2212046

姓 名 王昱

班 级 信息安全班

1. **实验目的**
   1. 熟悉静态反汇编工具IDA Freeware；
   2. 熟悉反汇编代码的逆向分析过程；
   3. 掌握反汇编语言中的数学计算、数据结构、条件判断、分支结构的识别和逆向分析
2. **实验原理**
3. 通过IDA Freeware可以得到二进制代码的反汇编代码，如图1和图2所示。

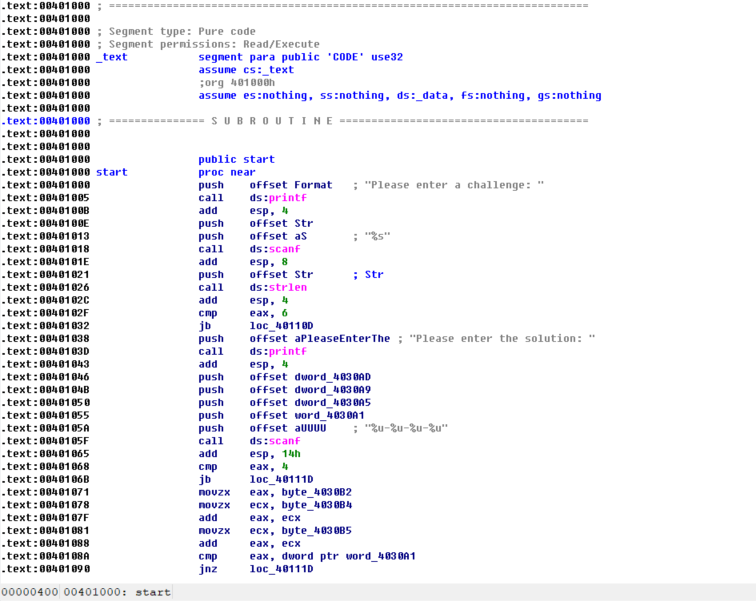


图 1 challenge.exe的反汇编代码

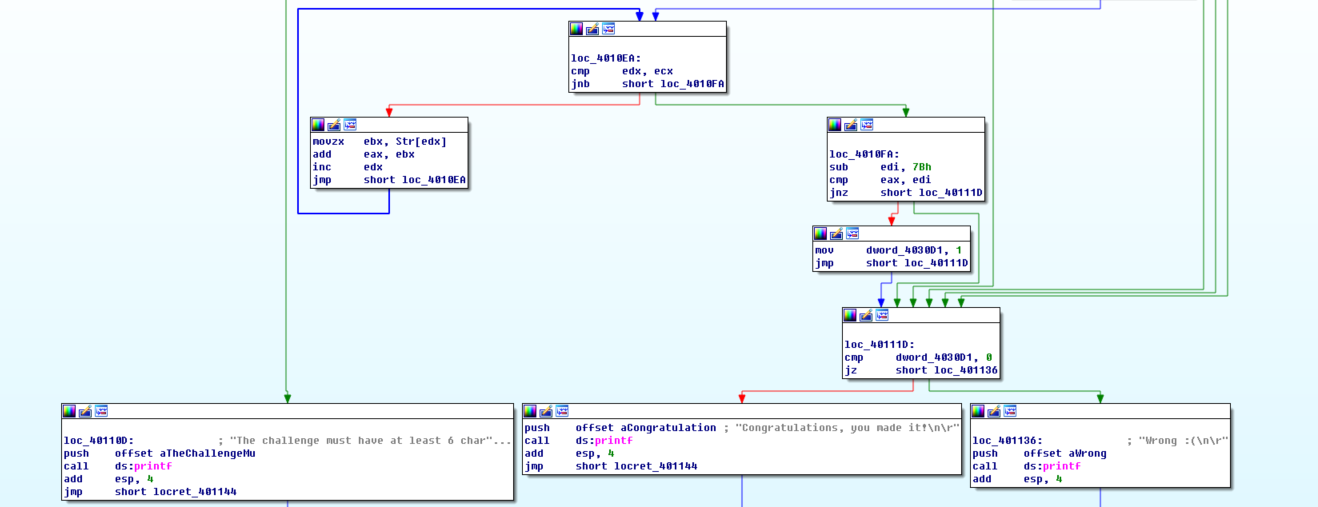


图 2 challenge.exe的反汇编代码的图形化显示

1. 不修改二进制代码，分析汇编代码的计算过程、条件判断、分支结构等信息，逆向推理出程序的正确输入数据，完成逆向分析挑战。

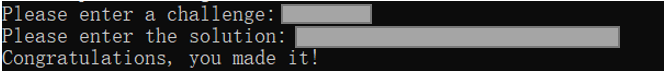
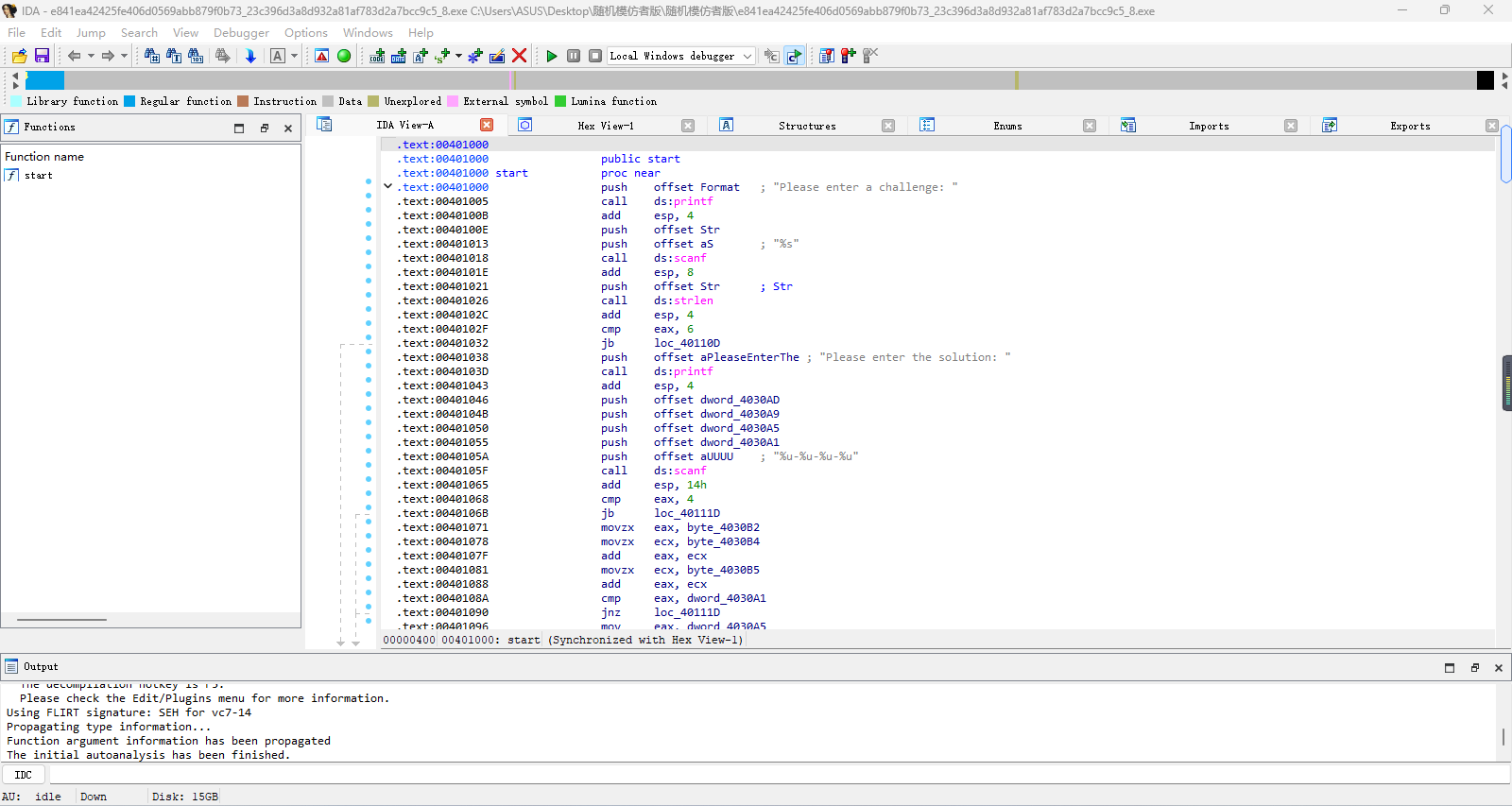
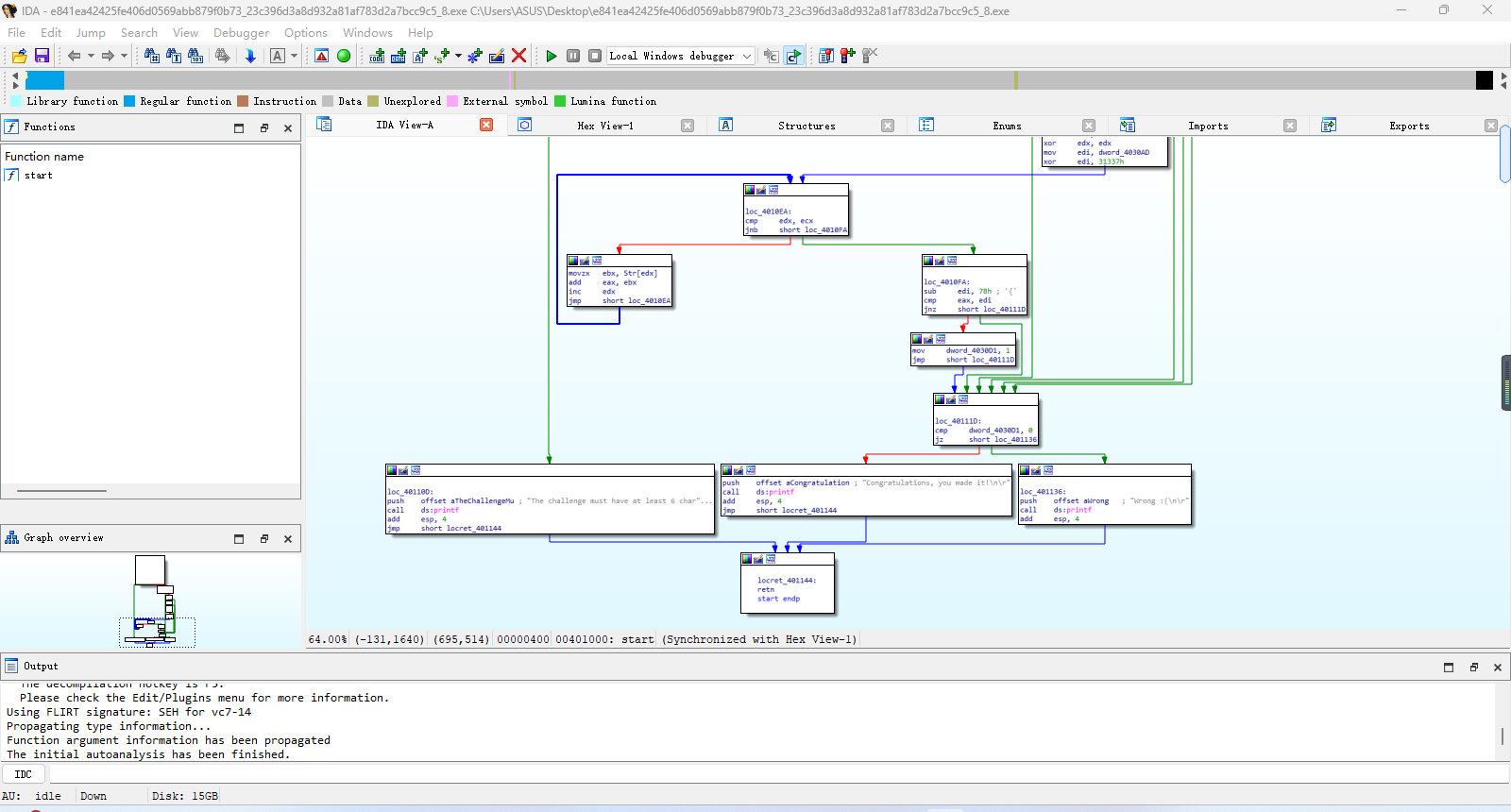


图 3 逆向分析，完成挑战

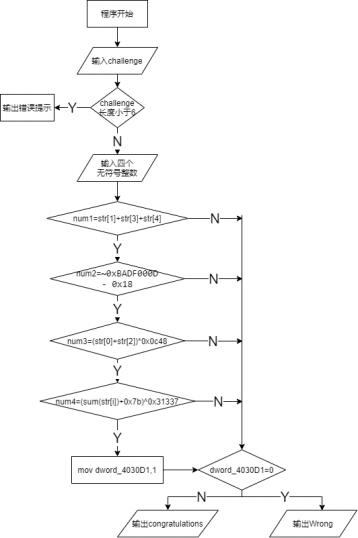
1. **实验过程**

（一）使用IDA Freeware，获得二进制代码的反汇编代码，提供截图



（二）逆向分析二进制代码的计算过程、数据结构、条件判断、分支结构等信息，记录逆向分析的详细过程。

整体的流程图如下：

：

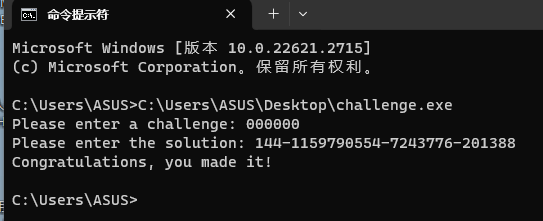
(1)由第一个判断模块知道，A1的值和eax 相同。要让 A1 和 eax 一样，就要让 str 的第 2，4，5 个字的 ASCII 码加起来等于 A1。这是根据 cmp eax, A1 和 jz loc\_4011D0 这两条指令判断的。eax的值是B2,B4,B5三个字符的ASCIl 码值相加。因此，对于每一个不同的str输入，可以通过计算字符串第2、3、4位字符对应的ASCII码值从而得到A1的值。

(2)由第二个判断模块可得，A5 的值不会因为 str 的不同而变化，它是一个固定的数。根据 cmp A5, 0BADFO0ODh 和 jnz loc\_4011D0 这两条指令，要算出 A5 的值，就要先把cmp 的源操作数 0BADFO0ODh 取反，然后再减去 18h。因为得到的数值是由A5+18h得到的，因此要得到A5需要将这个数值再-18h，就得到了固定的A5的值。

(3)由第三个模块可得，根据 mov eax, A9，div C48h，movzx eax, byte ptr [esp]，imul eax, [esp+8]，cmp eax, edx 和 jnz loc\_4011D0 这六条指令，要让 A9 除以 C48h 的余数和 str 的第 1 个字和第 3 个字的 ASCII 码的乘积一样，就要让 A9 满足一个方程。被除的寄存器是eax，首先先将A9赋值给eax，然后divC48h后，再把str的第一个字的ASCII码赋值给eax，再乘上str字符串的第三个字符对应的ASCll码，最终得到的eax和除法得到的结果相等。因此对应方程A9/0C48h==ASCll(1)\*ASCll(3)由此可以计算出A9的值。

(4)最后一个模块，根据 mov eax, [esp+10h]，mov ecx, eax，xor eax, eax，xor edx, edx，mov dl, [esp+edx]，add eax, edx，inc edx，loop loc\_4011A0，cmp edi, eax，xor edi, AD，xor edi, 31337h 和 jz loc\_4011D0 这十二条指令可得，要让 edi 和 str 的每一个字的 ASCII 码的和一样，就要让 AD 和 31337h 的异或结果和 edi 的初始值的异或结果等于 str 的每一个字的ASCII 码的和。

(三)运行程序，根据提示输入字符串和逆向挑战的结果，获得“Congratulations，you made it！”输出。



1. **实验结论及心得体会**

**在本次实验中，通过对实验程序的逆向分析提升了对IDA的熟练程度深入了解了关于IDA的基本操作，在此过程中我提升了对逆向技术的理解，也有了许多感悟。**