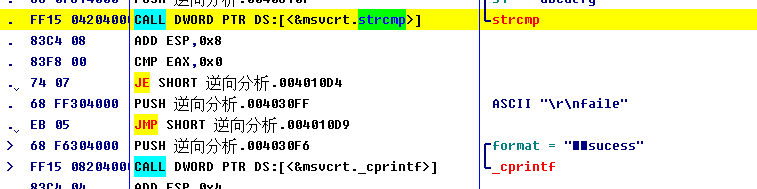
1. 分析出分支结构



If（strcmp(str1 , str2) == 0）

{  
 push (“成功”)

}

Else

{

Push (“失败”)

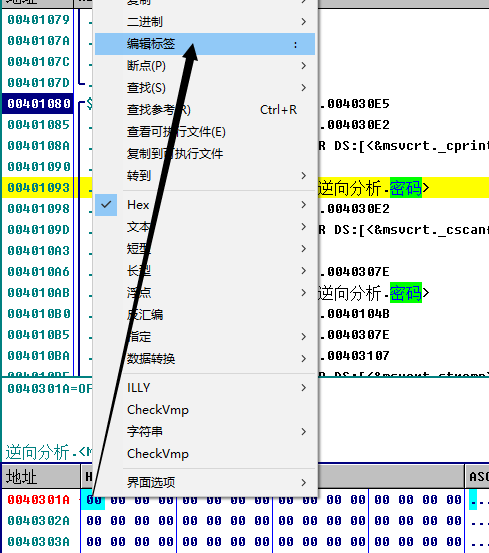
}

Call printf

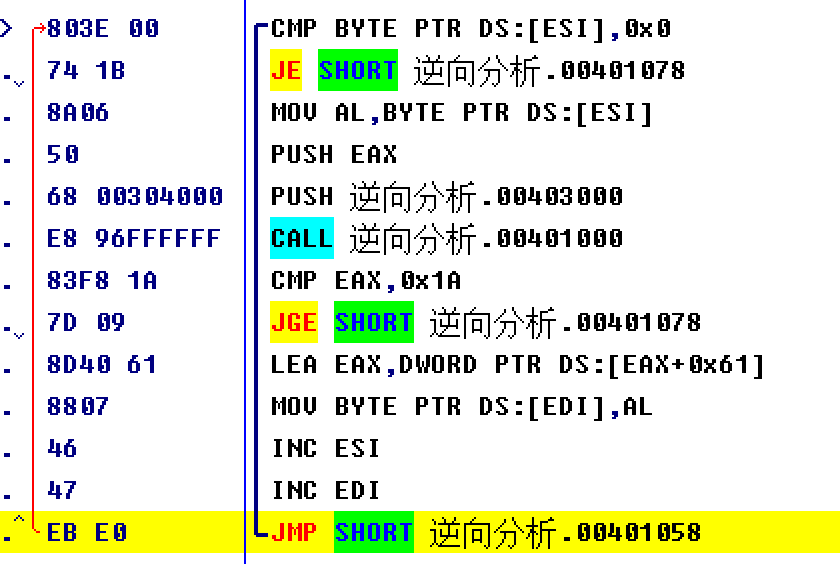
Add esp , 4

* 给全局变量添加标签

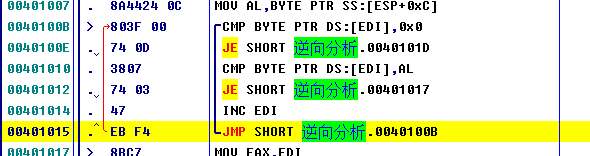




1. 分析出循环结构



总结出一个特征： 凡是向上跳转的，而且距离不是很远的，都是一个循环结构



1. 分析出有多个函数



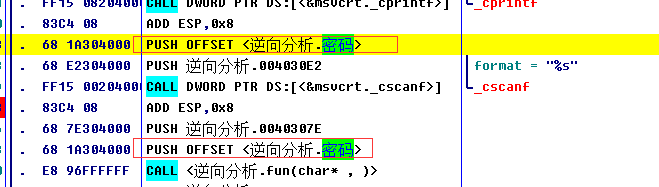


1. 分别分析出函数的调用方式和参数个数

调用方式： Stdcal

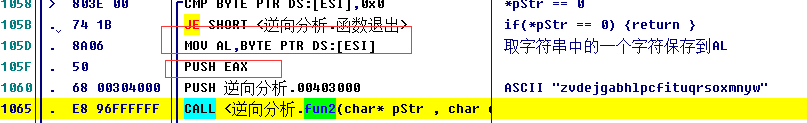
分别都有两个参数（从两个函数内部的ret 8这条汇编得到的信息）

1. 分析出函数的形参的作用
2. 形参的值来自于何处

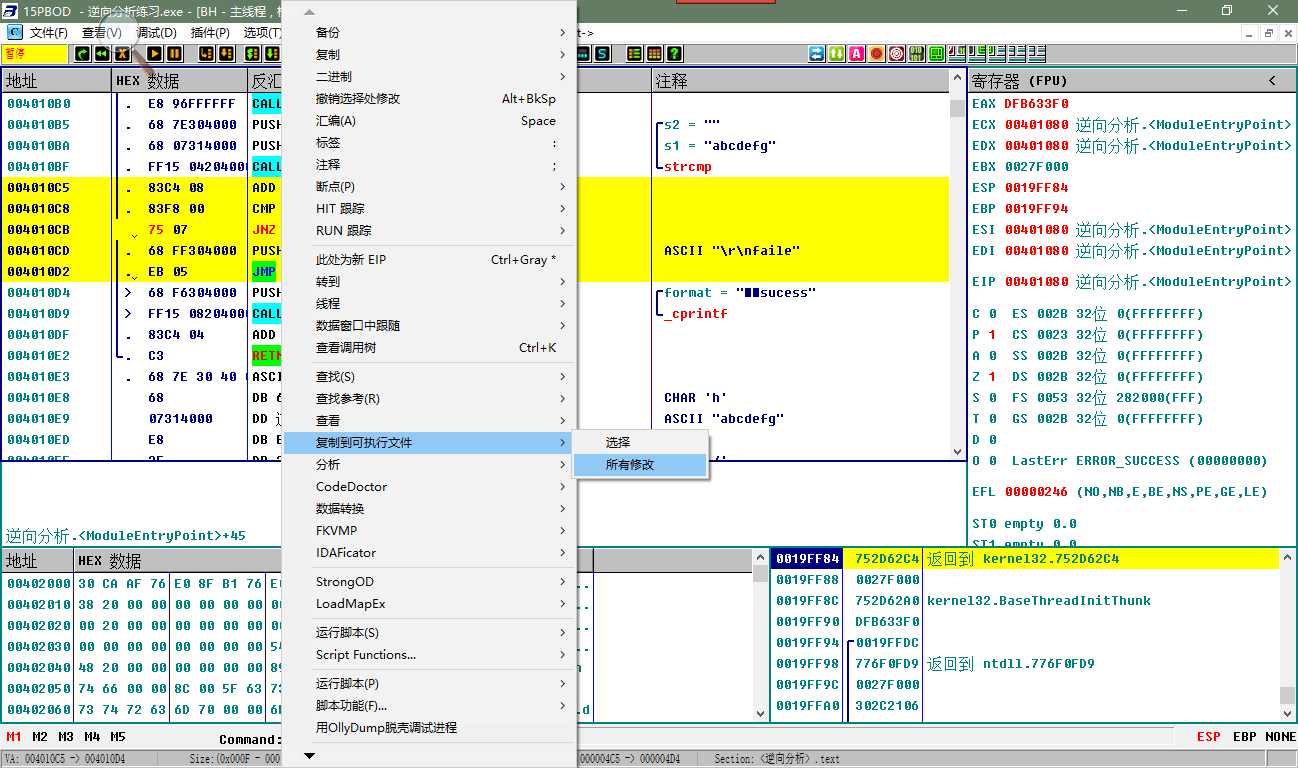


两个函数同时使用了相同全局变量作为参数， 已知其中一个函数是scanf，所以可知这全局变量是一个字符串首地址。

所以可以猜测出，fun函数的第一个参数是一个字符串首地址，而且这个字符串保存的是用户输入的内容



暴力破解，修改文件：

1. 修改关键跳
2. 选中修改的汇编代码
3. 见下图
4. 
5. 保存文件
6. 