XCTF csaw2013reversing2

原创

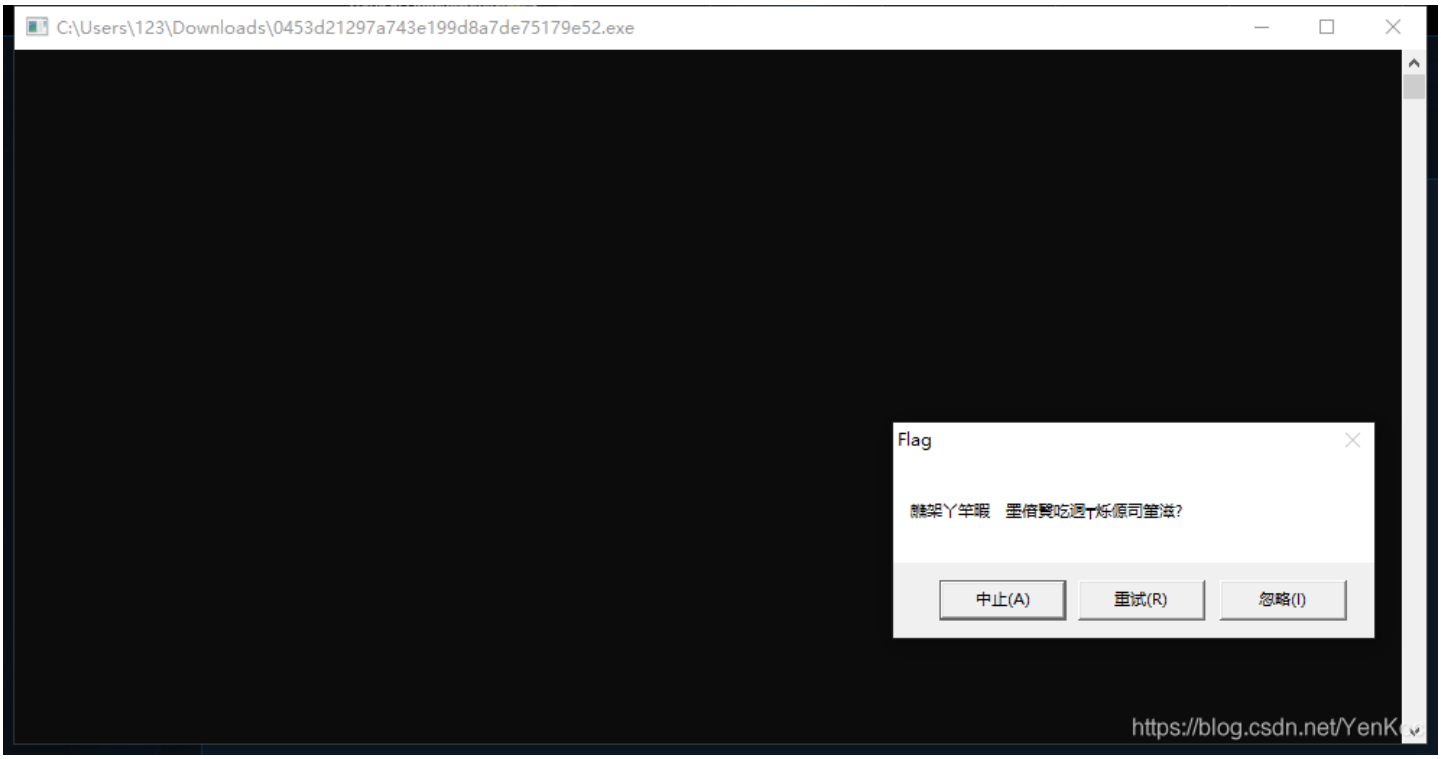
YenKoc 于 2020-01-28 23:20:38 发布

分类专栏： XCTF

本文链接：https://blog.csdn.net/YenKoc/article/details/104103487

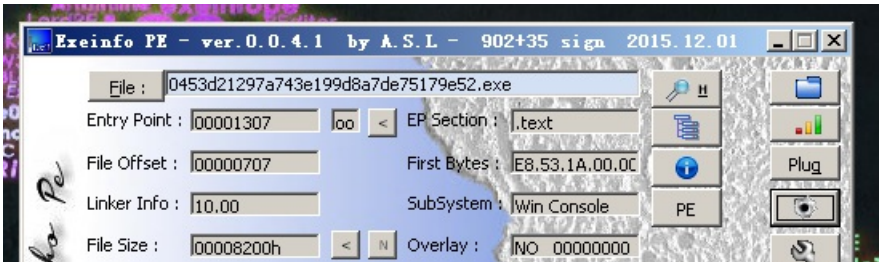
> 题目描述：听说运行就能拿到Flag，不过菜鸡运行的结果不知道为什么是乱码

一.先运行看看。



果然乱码。

二.查壳



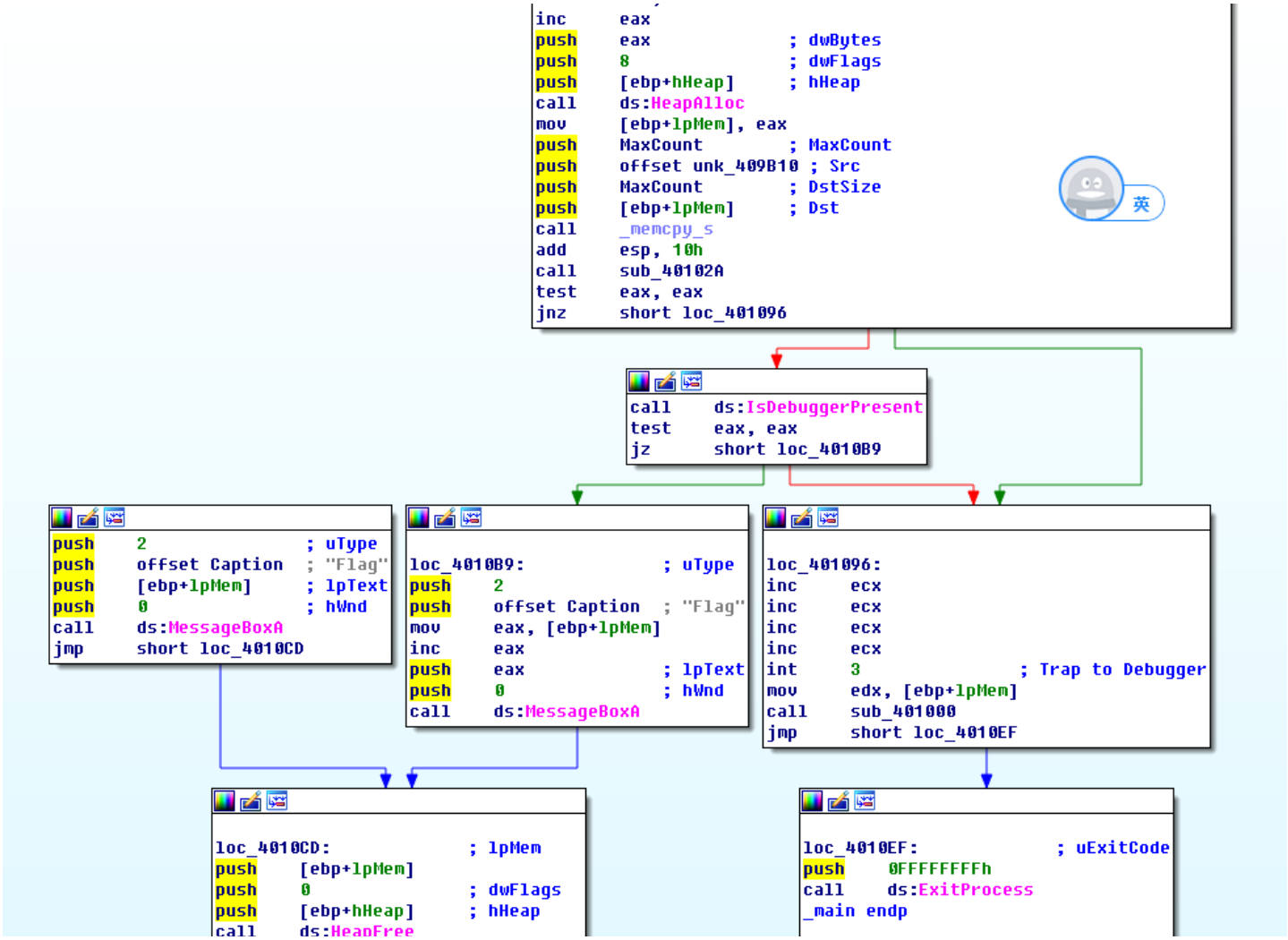
三.是pe文件，可以拖入od和ida进行动态和静态分析。

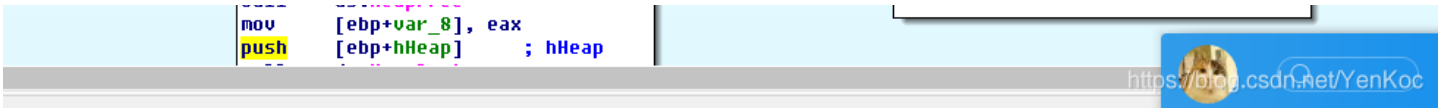
1.对主函数进行反编译一下。

```
int __cdecl __noreturn main(int argc, const char **argv, const char **envp)
{
  int v3; // ecx@1
  LPVOID lpMem; // [sp+8h] [bp-Ch]@1
  HANDLE hHeap; // [sp+10h] [bp-4h]@1

  hHeap = HeapCreate(0x40000u, 0, 0);
  lpMem = HeapAlloc(hHeap, 8u, MaxCount + 1);
  memcpy_s(lpMem, MaxCount, &unk_409B10, MaxCount);
  if ( sub_40102A() || IsDebuggerPresent() )
  {
    __debugbreak();
    sub_401000(v3 + 4, (int)lpMem);
    ExitProcess(0xFFFFFFFF);
  }
  MessageBoxA(0, (LPCSTR)lpMem + 1, "Flag", 2u);
  HeapFree(hHeap, 0, lpMem);
  HeapDestroy(hHeap);
  ExitProcess(0);
}
```

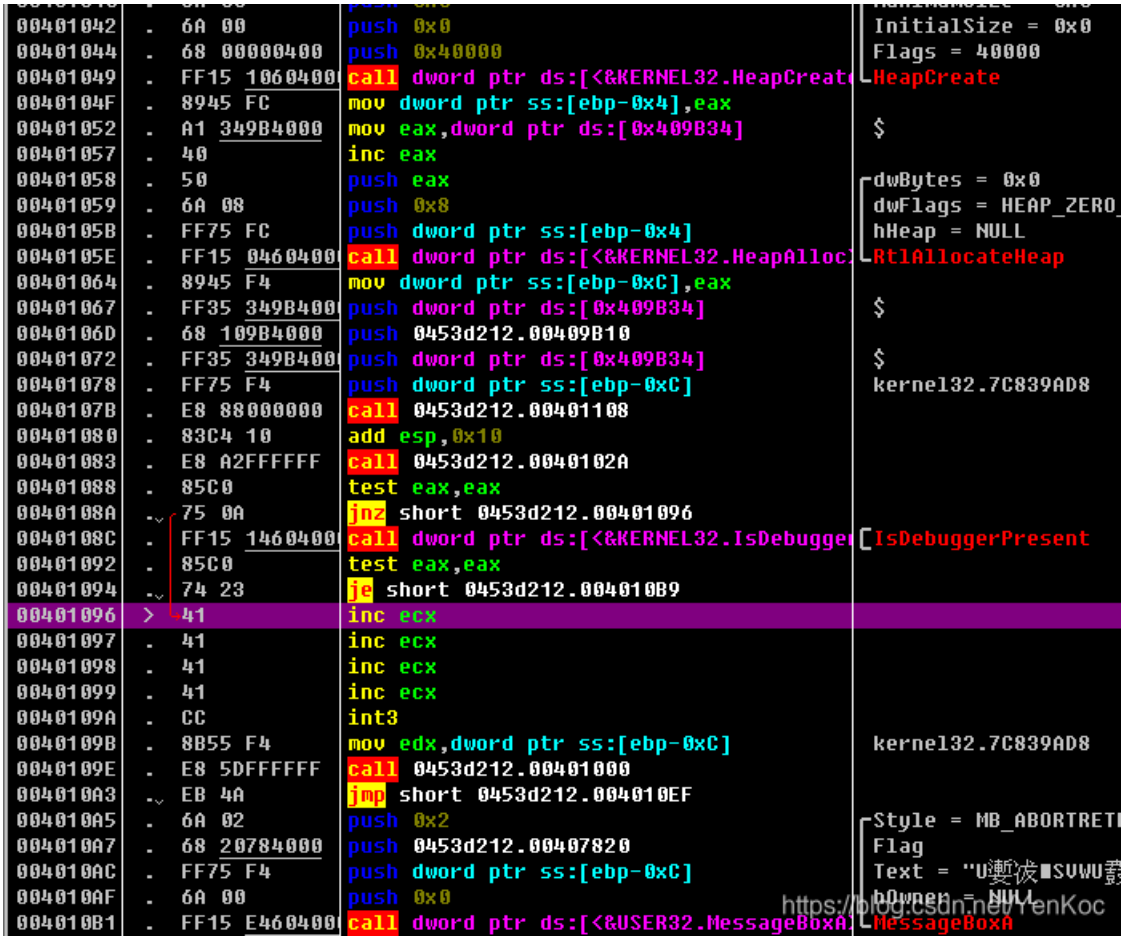

2.这里可以直接看出代码的逻辑和用意，那个if语句可以解码，如果没进入这步，会直接输出乱码的东西，看看汇编，这里已经利用最大资源了，我们来看看汇编是咋样的。





3.结合着伪代码来看，loc_401096是解码的函数，而loc_4010B9是输出窗口的函数，那么我们只要jmp到解码函数，同时到跳到输出窗口，flag不就解码出来了吗。

4.拖入od，中文查找。



修改汇编代码。