Reverse 250

没加壳，直接 IDA 打开，找到字符串 **flag:{NSCTF_md57e0cad17016b0>?45?f7c>0>4a>1c3a0}**

查看引用找到 `sub_401000()` ，看到有一段 decode 的代码。为了确定逻辑再往上走一层，看到这里：

```
if ( v2 + v1 == 3 )
  result = sub_401000();
else
  result = MessageBoxA(0, "flag:{NSCTF_md57e0cad17016b0>?45?f7c>0>4a>1c3a0}", "Flag", 0);
```

估计和上一题一个尿性，于是无视前边的逻辑直接 decode。回到 decode 的函数如下：

```
int sub_401000()
{
  char *v0; // eax@1
  CHAR Text; // [sp+0h] [bp-38h]@1
  char Dst; // [sp+1h] [bp-37h]@1
  char v4; // [sp+Fh] [bp-29h]@1

  Text = 0;
  memset(&Dst, 0, 0x30u);
  strncpy_s(&Text, 0x31u, "flag:{NSCTF_md57e0cad17016b0>?
45?f7c>0>4a>1c3a0}", 0x30u);
  v0 = &v4;
  // *v4 = "7e0cad17016b0>?45?f7c>0>4a>1c3a0}"
  if ( v4 != 125 )
  {
    do
    {
      *v0 ^= 7u;
      ++v0;
    }
    while ( *v0 != 125 );
  }
  return MessageBoxA(0, &Text, "Flag", 0);
}
```

Python 走起

```
a = "7e0cad17016b0>?45?f7c>0>4a>1c3a0"
out = ""
for i in a:
    out += chr(ord(i)^7)
print out
# 0b7dfc60761e798328a0d9793f96d4f7
```

flag:{NSCTF_md50b7dfc60761e798328a0d9793f96d4f7}

当然也可以根据上一层函数的逻辑通过密码检测。经提醒灰色按钮可以直接用资源编辑器激活（欺负我不熟 Windows T T ）