1. **IDA Python脚本编写**

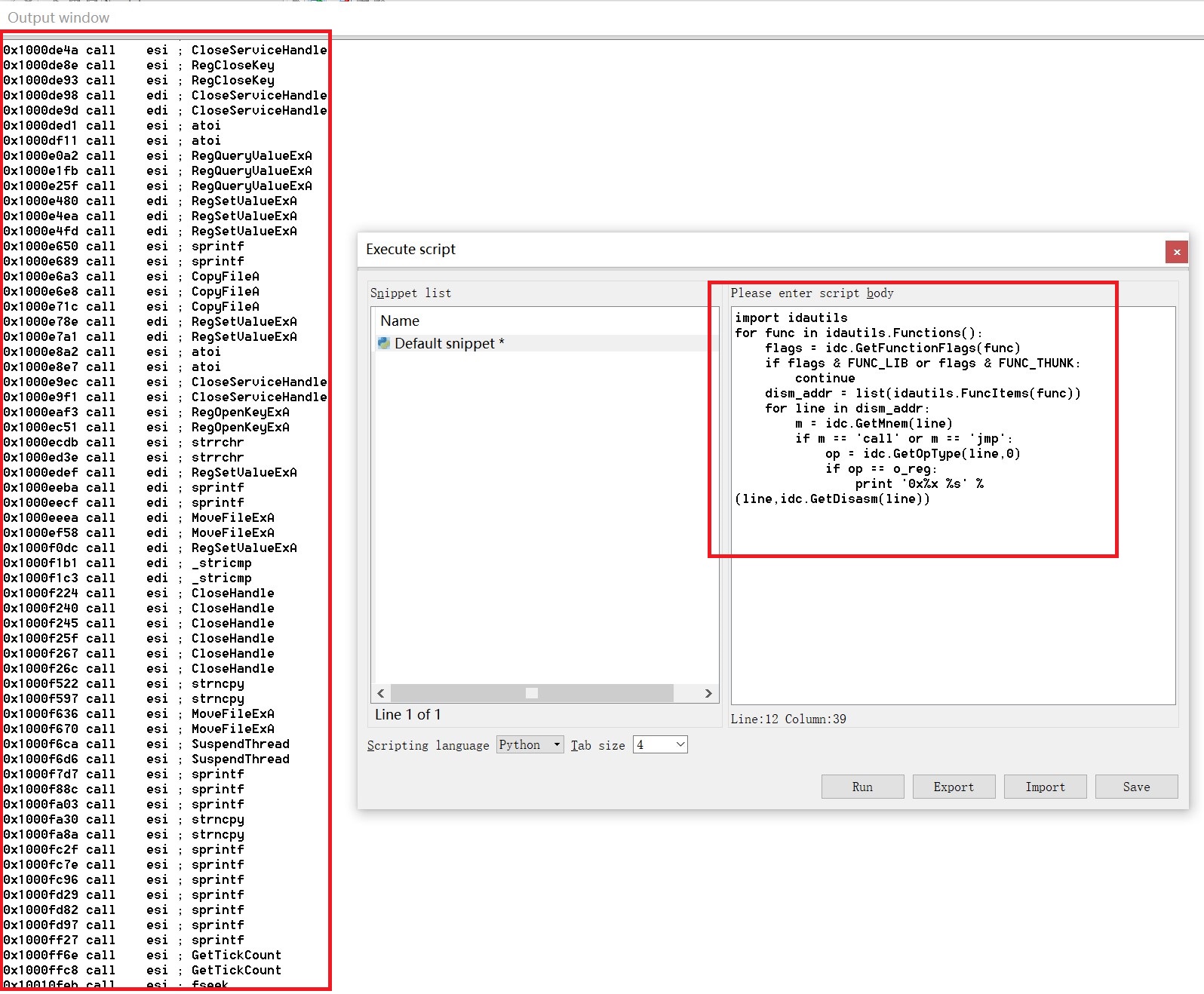
**功能：**

遍历所有函数，排除库函数或简单跳转函数，当反汇编的助记符为call或者jmp且操作数为寄存器类型时，输出该行反汇编指令

**代码：**

1. **import idautils**
2. **for func in idautils.Functions():**
3. **flags = idc.GetFunctionFlags(func)**
4. **if flags & FUNC\_LIB or flags & FUNC\_THUNK:**
5. **continue**
6. **dism\_addr = list(idautils.FuncItems(func))**
7. **for line in dism\_addr:**
8. **m = idc.GetMnem(line)**
9. **if m == 'call' or m == 'jmp':**
10. **op = idc.GetOpType(line,0)**
11. **if op == o\_reg:**
12. **print '0x%x %s' % (line,idc.GetDisasm(line))**

**执行结果：**

****

给出参考链接：[参考](https://blog.csdn.net/sxr\_\_nc/article/details/116566985?ops\_request\_misc=&request\_id=&biz\_id=102&utm\_term=idapython&utm\_medium=distribute.pc\_search\_result.none-task-blog-2~all~sobaiduweb~default-0-116566985.142^v63^js\_top,201^v3^control,213^v1^t3\_esquery\_v2&spm=1018.2226.3001.4187)