**应用：**BI TY (BInary Type)

**用途：**推导二进制代码中变量的类型

**Windows下使用方法：**

注：此工具依赖于IDA Pro 和 python3，需提前安装依赖项

1、安装python3.5.2，IDA Pro和PyQt5-5.6-gpl-Py3.5-Qt5.6.0-x32-2，并下载BInary Type项目文件

将代码克隆到本地之后：“运行前必装组件”中的两个安装程序先安装。

**BInary Type Git地址：** git@bitbucket.org:zhiwu/binary-type.git **（必须）**

**IDA Pro 下载地址：** [**http://pan.baidu.com/s/1bp7rOpp**](http://pan.baidu.com/s/1bp7rOpp) **（必须）**

**python3.5.2下载地址：** [**https://www.python.org/downloads/**](https://www.python.org/downloads/) **（必须）**

PyQt5下载地址： <https://riverbankcomputing.com/software/pyqt/download5> （非必须）

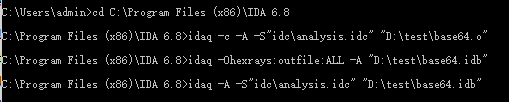
2、命令行执行IDA Pro分析二进制文件（需要在IDA的目录下）

**依次执行： idaq -c -A -S"idc\analysis.idc" "D:\test\base64.exe"**

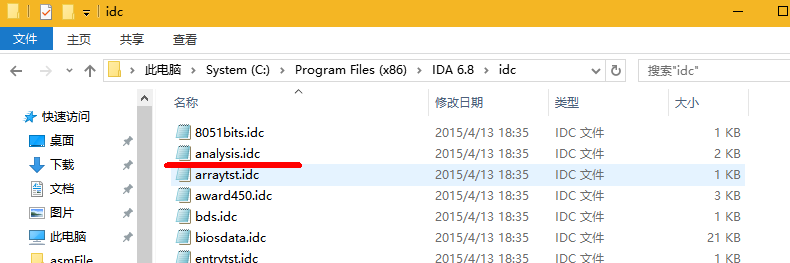
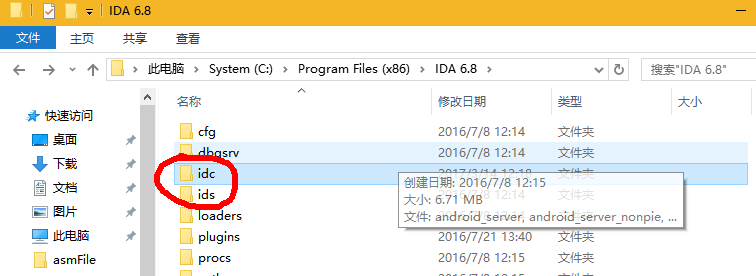
**idaq -Ohexrays:outfile:ALL -A " D:\test\base64.idb "**

**idaq -A -S"idc\analysis.idc" " D:\test\base64.idb "**

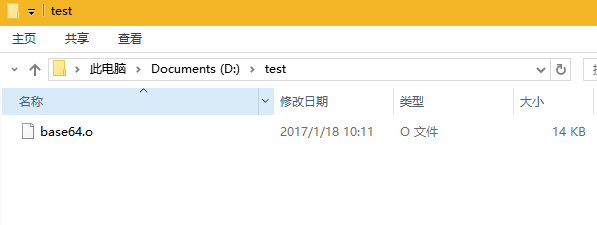
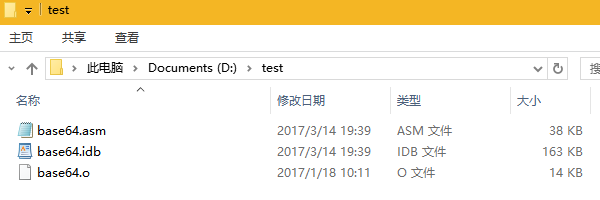
(注意：-S后面没有空格，-A表示让ida自动运行，不需要人工干预。也就是在处理的过程中不会弹出交互窗口，但是如果从来没有使用过ida那么许可协议的窗口无论你是否使用这个参数都将会显示。-c 参数会删除所有与参数中指定的文件相关的数据库，并且生成一个新的数据库。-S 参数用于指定ida在分析完数据之后执行的idc脚本，该选项和参数之间没有空格，并且搜索目录为ida目录下的idc文件夹。)



“idc\analysis.idc” 表示脚本文件，原地址在IDA根目录下的idc文件夹里：

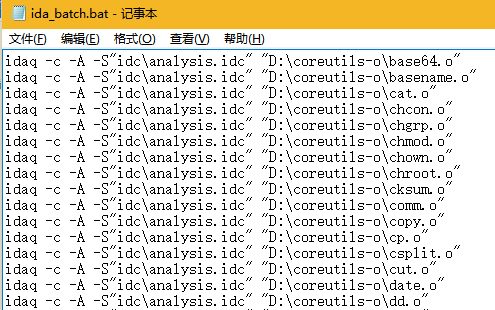


"D:\test\base64.o" 是表示二进制文件的地址，根据实际情况改变

执行完该命令行后，二进制文件的同目录下就可以得到.asm文件

此处可以自行编写ida\_batch.bat文件进行批处理，例如如下文件：

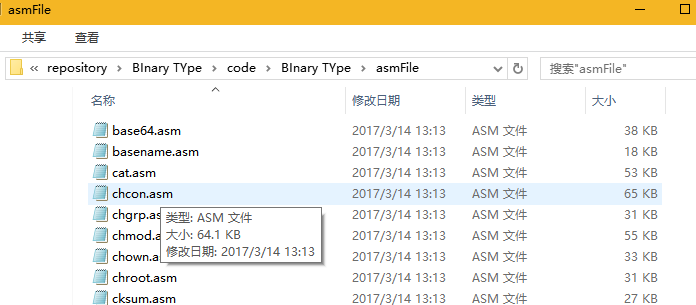




批处理执行完后将.asm文件拷贝到Binary Type/asmFile文件夹中即可。

3、BITY的预处理（将.asm中的函数片段提取出来）

将需要分析的.asm 文件放到BITY的asmFile文件夹下

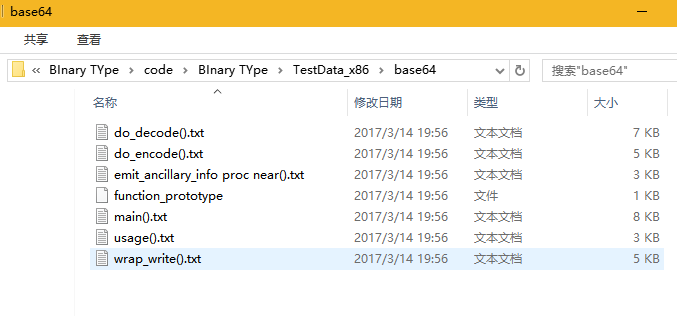
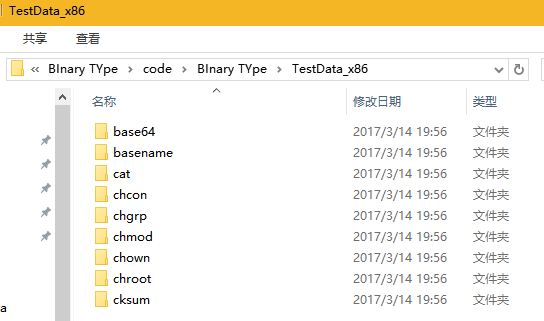


命令行下切换到BITY的目录，然后执行python SplitIDAasm.py



(如果遇到编码问题，只需要用记事本将.asm文件打开，另存为utf-8格式即可)

执行完后TestData目录下回出现若干个文件夹，每个文件夹中存放着按函数分割的汇编代码



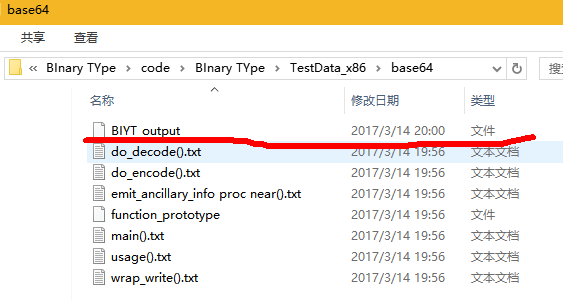
4、执行分析

命令行下执行python Predict\_SVM\_Model.py

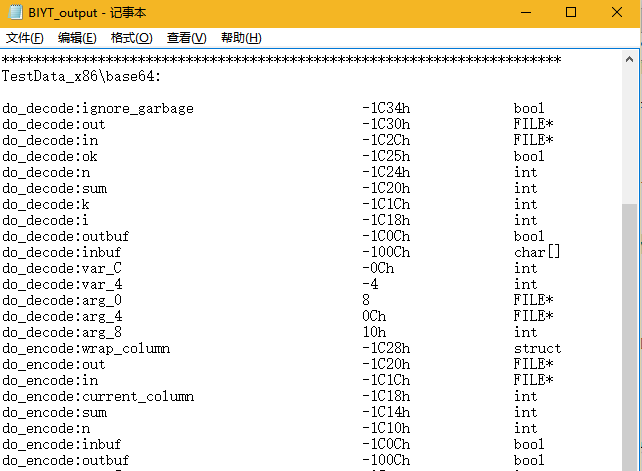


(如果遇到编码问题，只需要用记事本将.asm文件打开，另存为utf-8格式即可)

待提示结束后，再查看TestData目录，多了一个BITY\_output文件，用记事本打开即为分析结果



5、查看TestData目录，多了一个BITY\_output文件，用记事本打开即为分析结果，如图所示：



第一列是“函数名：变量名”，第二列是在栈中的偏移量，第三列是推导出来的类型

**BITY项目组成说明：**

asmFile/ 从IDA中得到.asm文件，放到该文件夹中

TestData/ 执行SplitIDAasm.py后，经过分割的.asm文件即可用于分析（分析样本）

TrainData/ 一些训练样本

SaveData / 无须理会，存放程序需要的一些中间文件

FileToVector.py 将一个汇编代码文件中的每个变量用一个向量的形式表示

Train\_SVM\_Model.py 训练SVM模型

SplitIDAasm.py 分割asmFile中的.asm文件

Predict\_SVM\_Model.py 分析TestData中的数据

Sketchy\_Predict\_SVM\_Model.py 不用管

svm.py LibSVM工具包

svmutil.py LibSVM工具包

libsvm.dll LibSVM动态库

libsvm.so.2 LibSVM动态库

Normalization.py 归一化程序

TransformDwarfFile.py 提取DwarfFile中的debug信息

TransformExplorerFile.py 可将https://gcc.godbolt.org/上经过x86 CL 19 RC编译的二进制码转为BITY可接受的文件

GUI\_Predict.py 一个简单的图形界面的输入，保存代码，点击预测按钮进行预测