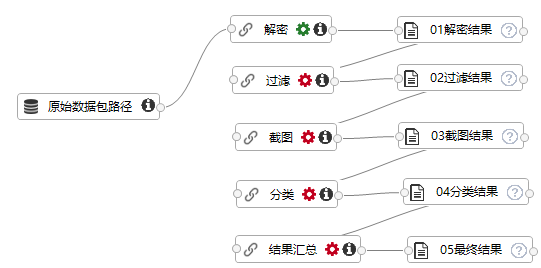
# 取证脚本模型化设计文档

## 取证脚本模型界面设计

1、取证脚本模型界面设计：



若解密数据包所在路径：

D:\work\rawData\130200\_queryResult\_db\_20210129093508\_ 20210129102345.tgz

脚本基本参数格式：

python 脚本名称 输入路径 输出路径

解密脚本参数设置:

|  |
| --- |
| 不指定输出路径(*默认路径为输入文件同级目录下01解密*):  python step1\_decrypt.py D:\work\rawData （默认输出路径*D:\work\rawData\01解密）* |
| 指定输出路径:  python step1\_decrypt.py D:\work\rawData E:\01result |

过滤脚本参数设置：

|  |
| --- |
| 不指定输出路径(*默认路径为输入文件同级目录下02过滤*):  python step2\_filter.py D:\work\rawData\01解密 （默认输出路径*D:\work\rawData\02过滤）* |
| 指定输出路径:  python step2\_filter.py D:\work\rawData\01解密 E:\02result |

截图脚本参数设置：

|  |
| --- |
| 不指定输出路径(*默认路径为输入文件同级目录下03截图*):  python step3\_screen\_capture.py D:\work\rawData\02过滤 （默认输出路径*D:\work\rawData\03截图）* |
| 指定输出路径:  python step3\_screen\_capture.py D:\work\rawData\02过滤 E:\03result |

分类脚本参数设置：

|  |
| --- |
| 不指定输出路径(*默认路径为输入文件同级目录下04分类*):  python step4\_ classify.py D:\work\rawData\03截图 （默认输出路径*D:\work\rawData\04分类）* |
| 指定输出路径:  python step4\_ classify.py D:\work\rawData\03截图 E:\04result |

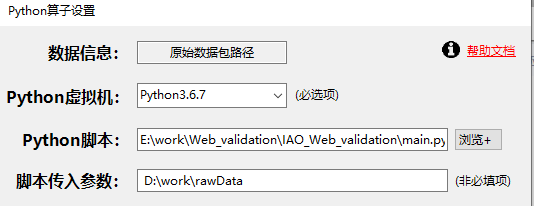
最终脚本参数设置：

|  |
| --- |
| 不指定输出路径(*默认路径为输入文件同级目录下05最终结果*):  python step5\_ finnaly.py D:\work\rawData （默认输出路径*D:\work\rawData\05最终结果）* |
| 指定输出路径:  python step5\_ finnaly.py D:\work\rawData E:\05result |

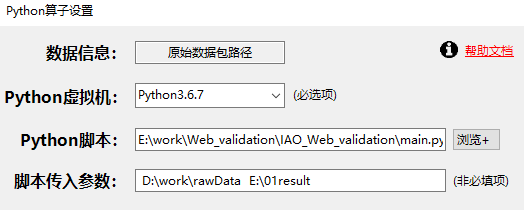
*备注：任一脚本运行结束，不仅在对应目录生成结果，也会刷新结果算子内容为结果所在路径。*

2、具体“解密”python算子内容设计：

默认输出路径：



指定输出路径:



## python脚本简化目标

* 去掉python3.7.6的依赖环境，只要是Python3都支持
* 去掉对谷歌浏览器的依赖