# 全文工具设计文档

1. 功能说明

增加“全文工具”SearchToolkit模块，计划包含目前已知的涉赌，涉黄，涉枪，飞机场4种依赖全文的线索模型。当前先实现涉赌模型，其他模型预留接口。

SearchToolkit模块依赖内网全文集群，现实中有**直连**和**堡垒机跳转**两种连接方式。目前只考虑**堡垒机跳转**模式。用户通过鼠标配置，执行模型，并可以下载结果到本机。业务过程类似侦察兵模块。

1. 业务逻辑
2. 用户选择涉赌模型后，提供堡垒机用户名，密码，堡垒机IP，全文机IP，C2通过SSH协议自动实现堡垒机登陆跳转到全文机，在默认文件夹上传涉赌脚本并远程后台执行。
3. 每个选中模型的每次执行，以“任务”的形式抽象表示，包括“+创建任务”，“查看任务详情”，“删除任务”。每个“任务”用一个唯一ID表示。
4. “任务”在创建后，对应的模型脚本是在服务器上异步执行，每次点击‘任务详情’

C2去服务器获取任务状态后展示相关信息。

1. 持久化信息，用户名->全文工具->任务ID\_模型名称\_状态.bcp，内含堡垒机各种配置信息，按\t分割。
2. 查看任务详情，用linux命令查看进程和结果文件信息来确定任务状态。
3. 交互设计
4. 左侧主面板增加一项“全文工具”，位于“侦察兵”下方。
5. 左侧针对“全文工具”增加一个二级面板，用来承载创建任务，选择模型，配置参数，查看任务详情等用户实际操作。
6. 针对每个任务，增加任务详情子窗口，包括堡垒机用户名，堡垒机密码，堡垒机IP，全文机IP，模型选择，结果下载，服务器上临时存储结果的目录等元素。
7. 每个‘任务’一个元素项，右键菜单：任务详情，任务删除
8. tooltip待设计
9. 说明
10. 整体类似‘侦察兵’的交互和逻辑
11. 待上传到服务器的脚本，用zip压缩，作为资源嵌入到项目中
12. 代码放置于IAOLab\SearchToolkit目录中
13. 对应的ssh工具包，约简单约小越好