# Linux数据采集程序的详细文档说明

## app.py入口程序

1. app.py,， WiFi信息扫描，主要为开启网卡获取目标的网口信息。
2. /api/whichwlan接口，choosewlan方法，调用terminal.getallwifiname里的changewifishell，改变shell命令里的网卡名字；表现的功能为选择网卡
3. /api/startcollect，startcollect方法，调用wifilist.startwifiserver里的start和killshell方法，同时用两个线程启动两个方法，start执行本地shell命令，killshell结束shell命令，然后采集log中的wifi信息，存入本地的mongodb数据库
4. /api/handshake，collecthandshake方法，调用wifilist.getwifihandshake的starthandshake和wifilist.routeattack的start，同时用两个线程启动这两个方法，starthandshake为获取wifihandshake包，并采集log分析是否真的采集到有密码信息的握手包，start为使用路由泛洪攻击，并采集log分析是否攻击成功， 若是采集了带有密码信息的握手包那就将握手包移动到下载文件夹
5. /api/download/<wifi>，download方法，主要作用是客户端下载已经采集的握手包，一个文件下载的接口
6. /api/shutdown，shutdownwifi方法，调用wifilist.wifiswitch的stopwifi方法，作用为关闭所有有关wifi扫描的程序和线程，关闭虚拟网卡，还回网卡的名字

## wfi.py入口程序

1. wifi.py，获取网卡信息，选择网卡开启伪造的AP，并收集接入热点的收集信息
2. /api/allwlan，getallwlan方法，调用terminal中的getallwifiname方法，表现为执行iwconfig命令获取系统识别的所有的网卡信息
3. /api/whichwlan,wlanname方法，调用terminal.getallwifiname中的rename方法，修改系统中所有有关AP的配置文件，以及执行开启AP的shell命令的网卡名字，客户端表现为选择网卡
4. /api/wificonf，wificonf方法，调用terminal.getallwifiname中的changewificonf方法，配置伪造AP的wifi名字和wifi密码
5. /api/start,start方法调用terminal.switch的startallshell方法，和terminal.gethostapdfield的startcollect方法， 具体表现为，开启虚拟的APwifi，并且分析产生的log采集有用的字段存入本地的mongo数据库
6. /api/shutdown，stop方法调用terminal.switch中的shutdownshell的方法，表现为停止AP，kill所有与AP有关的进程
7. /api/mobiinfo,querymobidata方法我查询本地mongodb中采集的手机信息

## 文件介绍及主要py文件

1. Attack：routeattack.py,主要功能是开启定向路由的泛洪攻击，攻击指定的wifi目标，使所有连接此wifi的设备全部掉线；stopattack.py，停止路由的泛洪攻击
2. Homebak：运行设备home文件夹所有shell文件，和文件夹的备份，用于在新设备快速搭建环境
3. Mongodatabak:本地mongodb数据的备份，确保执行功能测试和单元测试时有原始数据
4. Pubfunc:公用函数，存放一些单元测试脚本，和一些常用的函数方法的定式
5. Script、shelldic都是些脚本文件和一些log文件，用于本地开发和功能调试
6. Terminal主要存放扫描wifi信息和获取handshake握手包的功能
7. Wifilist主要存放伪造AP，和搜集手机信息的功能