1. 需匹配的关键词命名规则及匹配位置

（注：红色标记为一级分类，蓝色标记为二级分类）

登录信息能否获取：

自由账号：

自有账号 'account' : 11,

账号ID 'account\_id':12,

手机号 'phone\_num' : 13,

第三方账号：

邮箱 'mail' : 14,

微信 'wechat' : 15,

QQ 'qq':16,

微博 'weibo' : 17,

账号基本信息：

账号昵称 'account\_name' : 18,

账号密码 'key' : 19,

关联手机号 'associated\_phone':20,

关联邮箱 'associated\_mail':21,

生日 'birth':22,

其他 'sex': 23,

'work': 23,

'company': 23,

'school': 23,

'current\_location': 23,

'hometown': 23,

'profile': 23,

'pers\_signature': 23,

'[constellation](http://www.youdao.com/w/constellation/" \l "keyfrom=E2Ctranslation)': 23,

'blood\_type': 23,

注册验证码 'register\_code' : 24,

终端信息：

移动终端侧：

手机型号 'phone\_type' : 25,

操作系统 'phone\_os' : 26,

OS语言 'os\_language':27

MAC 'mac' : 28,

IMEI 'imei\_1' : 29

'imei\_2' : 29,

时区设置 'timezone':30,

上网方式 'network\_type' : 31,

应用侧：

APP\_ID 'app\_id':32,

APP语言 'app\_language':33,

APP版本 'app\_ver':34,

身份:

姓名 'name\_chs' : 35,

身份证号 'ID\_num' : 36,

关系：

好有账号 'frend\_id' : 37,

好友昵称 'friend\_name\_chs' : 38,

位置：

GPS 'gps' : 39,

地址（内容） 'addr1\_chs': 40,

'addr2\_chs': 40,

'addr3\_chs': 40,

'addr4\_chs': 40,

时间戳 'timestamp':41,

浏览、发布内容：

格式 'format\_title':42,（标题）

'format\_audio':42,（音频）

'format\_video':42,（视频）

'format\_pic':42,（图片）

'format\_word':42,（文字）

内容 'content1\_chs' : 43,

'content2\_chs' : 43,

'content3\_chs' : 43,

'content4\_chs' : 43,

'content5\_chs' : 43,

内容URL 'con\_url\_essay':44,（文章）

'con\_url\_pic':44,（图片）

'con\_url\_vid':44,（视频）

搜索内容：

是否可获取 'isavailable':45,

关键词（示例） 'keyword1\_chs': 46,

'keyword2\_chs': 46,

'keyword3\_chs': 46,

'keyword4\_chs': 46,

'keyword5\_chs': 46,

WIFI热点：

ID 'wifi\_ID':47,

GPS 'wifi\_GPS':48,

基站：

ID 'basestation\_ID':49,

GPS 'basestation\_GPS':50,

获取方式：

协议：

HTTPs 'HTTPS':51,

GET 'GET':52,

POST 'POST':53,

TCP 'TCP':54,

URL 'URL':55,

编码方式： 'unicode':56,

'url':56,

'gb2312':56,

'md5':56,

'base64':56,

流量方向：

上行 'up': 57,

下行 'down': 58,

附加信息：

报文名称 'export\_name':59,

报文内容 'body': 60,

报文HTTP头 'header': 61,

附加账号昵称：

'wechat\_name\_chs': 62,

'qq\_name\_chs': 62,

'weibo\_name\_chs': 62

1. 流量分析流程说明
2. 利用wireshark进行抓包，并保存为.pcap文件。
3. 在脚本中输入所需匹配的详细信息以及需要导入的.pcap文件。
4. 运行脚本。脚本会将解析后的数据导出到相应的excel中。
5. 最后人工进行筛选，排除一些没有价值的数据。