其他协议解析字段

|  |  |  |  |
| --- | --- | --- | --- |
| 协议类别 | | 协议名称 | 解析字段内容 |
| 邮件协议 | | SMTP方式发邮件 | 1、用户ID及密码 |
| 2、发送账号和接收账号 |
| 3、发送主题和内容 |
| 4、附件(可下载) |
| POP3方式收邮件 | 1、用户ID及密码 |
| 2、发送账号和接收账号 |
| 3、邮件主题和内容 |
| 163邮箱 | 发件人、收件人、标题、内容、附件 |
| QQ邮箱 | 发件人、收件人、标题、内容 |
| 126邮箱 | 发件人、收件人、标题、内容、附件 |
| yeah邮箱 | 发件人、收件人、标题、内容、附件 |
| 139邮箱 | 发件人、收件人、标题、内容、附件 |
| 搜狐邮箱 | 发件人、收件人、标题、内容、附件 |
| 新浪邮箱 | 发件人、收件人、标题、内容、附件 |
| 21cn邮箱 | 发件人、收件人、标题、内容、附件 |
| HTTP协议 | | HTTP上传 | 1.访问的url以及服务器的ip、mac 2.一些赌博、邮箱等网站的用户名和密码 3、客户端信息（系统、浏览器等版本信息）、cookie等信息 |
| WEB地址访问跟踪 | 1、访问网站URL |
| 2、访问内容 |
| 3、客户端信息（系统、浏览器等版本信息）、cookie等信息 |
| HTTPS协议 | | HTTPS证书信息 | 国家、公司，可下载证书 |
| FTP协议 | | FTP | 用户名、密码、操作行为 |
| TELNET协议 | | TELNET | 服务器名称 |
| VPN协议 | | VPN连接 | 服务器ip、用户名、类型 |
| 远程终端 | | remote | 使用定位 |
| ssh | 使用定位 |
| 终端服务 | 使用定位 |
| 流媒体协议 | | RTSP | 下载文件名 |
| 搜索引擎 | | 百度搜索 | 搜索类型、关键词 |
| GOOGLE搜索 | 搜索类型、关键词 |
| BING搜索 | 搜索类型、关键词 |
| SOGOU搜索 | 搜索类型、关键词 |
| 有道搜索 | 搜索类型、关键词 |
| 中搜 | 搜索类型、关键词 |
| 中华网搜索 | 搜索类型、关键词 |
| 360好搜 | 搜索类型、关键词 |
| 爱问搜索 | 搜索类型、关键词 |
| 微博协议 | | QQ微博 | 通行证、信息传送方式（发帖、转帖、跟帖）、信息内容 |
| 新浪微博 | 通行证、发帖、评论 |
| 文件传输 | | 迅雷 | 本机（内网）MAC、本机IP、登陆状态 |
| QQ传输文件 | 发件人、文件名称 |
| 电骡 | 操作内容 |
| 突网工具 | | 无界访问跟踪 | 使用定位和版本信息 |
| 自由门访问跟踪 | 使用定位 |
|
| 通讯录 | | 飞信通讯录 | 昵称、电话号码 |
| 遇见 | 昵称、电话号码 |
| 彩云通讯录 | 昵称、电话号码 |
| 新浪微博通讯录 | 昵称、电话号码 |
| 网络游戏 | | 联众游戏 | 可以获取到账号和聊天信息 |
| 完美游戏 | 用户名 |
| 传奇 | 用户名、密码 |
| 证券股票 | | 同花顺 | 用户名和用户状态 |
| 手机阅读 | | 搜狐新闻 | 登录账号、评论内容，登录平台、登录时间、操作类型 |
| 腾讯新闻 | 登录账号、评论内容，登录平台、登录时间、操作类型 |
| 网易新闻 | 登录账号、评论内容，登录平台、登录时间、操作类型 |
| 手机地图 | | 高德导航 | 经纬度 |
| 高德免费导航 | 经纬度 |
| 搜狗地图 | 查询内容 |
| 图吧导航 | 经纬度 |
| 翼周边 | 经纬度 |
| 手机软件 | | 百度音乐 | 账号 |
| 酷我音乐 | 账号 |
| PPTV | 账号、密码 |
| 优酷 | 账号、IMEI |
| 网络购物 | | 拍拍 | 收件人姓名、收货人电话、收货地址、添加地址 |
| 凡客 | 收件人姓名、收货人电话、收货地址、添加地址 |
| 聚美优品购物 | 账号、收件人姓名、收货人电话、收货地址 |
| 京东 | 账号、收件人姓名、收货人电话、收货地址 |
| 肯德基 | 收件人姓名、收货人电话、收货地址 |
| 当当 | 用户名、密码 |
| 淘宝 | 账号 |
| 团800 | 用户名、密码 |
| 论坛贴吧 | | 百度贴吧 | 手机版：贴吧名称、发帖内容、url、IMEI |
| 电脑版：贴吧名称、发帖内容、url |
| 猫扑 | 用户名、密码、发帖内容 |
| 手机聊天 | | 微信 | 微信内部ID、上线信息 |
| 陌陌 | 接收者、聊天内容 |
| 音视频协议 | | QQ音频 | 音频文件 |
| 即时通讯 | | 腾讯QQ定位 | qq上下线以及心跳信息 |
| 易信 | 手机号、用户名，在线状态 |
| 飞信 | 用户名、聊天内容 |
| MSN | 系统消息 |
| 网易泡泡 | 用户名 |
| 淘宝旺旺 | 用户名 |
| 新浪UC | 聊天内容 |
| skype | 使用定位 |
| 出行信息 | | 滴滴打车 | 经纬度、手机号、上网账号、上线、叫车 |
| 快的打车 | 经纬度、手机号、上网账号、上线、叫车 |
| 滴滴专车 | 手机号、IMEI、司机上线 |
| 易到专车 | 手机号、IMEI、司机上线 |
| 携程（网页版） | 班车次、票价、起点、终点、姓名、身份证、出发时间、类型（飞机票、火车票、汽车票） |
| 同程（网页版） | 班车次、票价、起点、终点、姓名、身份证、出发时间、类型（火车票、汽车票）（未解析火车票） |
| 同程（安卓） | 班车次、票价、起点、终点、姓名、身份证、出发时间、类型（火车票  班车次、终点、电话、出发时间（飞机票） |
| 途牛（网页版） | 票价、起点、终点、姓名、身份证、出发时间、类型：飞机票  类型：火车票(火车票信息不全) |
| 途牛（安卓） | 票价、起点、终点、姓名、身份证、出发时间、类型：飞机票  （未解析火车票、汽车票） |
| 网络电话 | | KC | 登陆账号 |
| 微微 | 可以获取到音频通话并下载收听，还原到KC中 |
| 4G | 登陆账号、可以获取到音频通话并下载收听，还原到KC中 |
| 云呼 | 可以获取到音频通话并下载收听，还原到KC中 |
| 97call | 可以获取到音频通话并下载收听（专用播放器）登陆账号 |
| 中华通 | 可以获取到音频通话并下载收听，还原在爱聊中 |
| 有信 | 可以获取到音频通话并下载收听，还原到KC中 |
| 阿里通 | 可以获取到音频通话并下载收听，还原在爱聊中 |
| 爱聊 | 可以获取到音频通话并下载收听 |
| TALKBOX | 账号、密码、音频 |
| 进程扫描 | 手机设备信息 | 支付宝 | 手机型号、来源软件、操作系统、操作系统版本号 |
| 腾讯视频 | 手机型号、来源软件、操作系统、操作系统版本号 |
| 优酷 | 手机型号、来源软件、操作系统、操作系统版本号 |
| 电脑设备信息 | 360安全卫士 | 唯一设备识别码、安装软件、系统名称 |
| 手机定位信息 | 墨迹天气 | 安装软件、手机IMEI、经纬度 |
| 百姓网 | 安装软件、手机IMEI、经纬度 |
| 赶集生活 | 经度，纬度，IMEI |
| 百度糯米 | 经度，纬度，IMEI |
| 丁丁优惠 | 经度，纬度，IMEI |
| Go桌面 | 经度，纬度 |
| 面包旅行 | 经度，纬度 |
| 糯米网 | 经度，纬度 |
| 前程无忧 | 经度，纬度 |
| 美团 | 经度，纬度 |
| 58同程 | 经度，纬度 |
| 大众点评 | 经度，纬度 |
| 运行软件 | Skout | 来源软件、操作系统、状态 |
| 安装软件 | 豌豆荚 | 软件名称、安装商店、平台、状态 |
| 魅族商店 | 软件名称、安装商店、平台、状态 |
| 小米商店 | 软件名称、安装商店、平台、状态 |
| 联想商店 | 软件名称、安装商店、平台、状态 |
| 数据库 | | SQLSERVER | 用户名、实例名称 |
| 涉恐软件 | | telegram | 使用定位 |
| viber | 使用定位 |
| oovoo | 使用定位 |
| path | 登陆状态 |
| 蜂加 | 登陆状态 |
| ROUNDS | 登陆状态 |
| 赛风 | 登陆状态 |
| fqrouter | 用户名、密码、登陆状态 |
| puff | 用户名、密码、登陆状态 |
| vpngate | 用户名、密码、登陆状态 |
| wallproxy | 用户名、密码、登陆状态 |