**合同包1**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **技术参数** | 数量 |
| 1 | 在线提取检验设备 | 1.应支持采集Windows系统（最高支持Win11）、WinServer服务器、Linux服务器；  2.应支持案件管理、人员管理、检材管理，卡片式展示和管理方式；  3.应支持一案一策，可配置和预置策略管理，策略内容包含采集范围、核案项、核案线索；  4.应支持基本磁盘/动态磁盘多种文件系统格式的解析；  5.应支持系统痕迹分析，包括USB设备使用记录、应用程序运行痕迹、最近访问记录、回收站删除记录、远程桌面、未分配簇中打印记录等；  6.应支持上网记录分析；  7.应支持即时通讯分析；  8.应支持邮件分析，包括Foxmail、Outlook Express等客户端的邮件内容，并可恢复被删除的邮件信息；  9.应支持账号密码提取：包括Xshell、Xftp、RDP、Wlan、VNC、SecureCRT、Navicat、Foxmail、FileZilla、TeamViewer等；  10.应支持自动搜索最近使用文件:包含常规文件、办公文件、压缩包文件、最近脚本文件等；  11.应支持文件内容搜索；支持关键文件导出；  12.应支持手工截图；采集过程支持屏幕录像；  13.哈希值计算：支持对内存镜像、数据采集、截屏录屏、导出文件等计算哈希值；  14.应支持本机账号痕迹信息检测；  15.应支持现场自动检测Mysql、SqlServer、PostgreSql、mongodb数据库版本信息、保存路径、数据库类型信息的获取；  16.应支持现场自动检测Apache、Nginx、Tomcat以及IIS等网站信息的获取，包括网站服务器类型、网站的配置、网站目录等信息；  17.支持自动搜索最近使用文件:包含常规文件、办公文件、压缩包文件、最近脚本文件等；  18.应支持关键文件自动导出: 网站文件、数据库文件、日志文件、配置文件、防火墙文件等；  19.应支持服务器概览信息汇总: 网站数据库前后关联、操作历史记录、登录用户、服务器端口用途、定时任务等。 | 1套 |
| 2 | APP和URL动静态解析软件 | 1.应用模块集成Android和iOS真实手机运行环境；主控硬件配置采用嵌入式高性能低功耗64位6核处理器；  2.应支持真实手机画面映射到取证操作界面的能力，用鼠标点击映射的手机画面，控制集成手机里APP真实操作，支持操作界面对真实手机的文本输入；  3.应支持导出APP测试记录的离线数据包，用于分发共享查看完整检测过程，支持BCP数据格式导出。支持一键导出检测报告，可选WORD、PDF格式；**（需提供软件实际使用功能截图）**  4.应支持APP应用动态访问URL信息的自定义特征标签标注，并进行标红突出显示标签。集成Android真机监测沙箱，应支持接打电话、收发短信、在3G/4G、WIFI环境下的数据访问、安装/运行/卸载APP能力，支持应对APP对虚拟沙箱（虚拟机）的处置能力；  5.应支持手机APP权限的一键配置开关（自动允许、询问、拒绝），提高APP的检测效率；  6.支持一键预制手机内置诱导信息，包括通讯录、通话记录、短信记录；  7.应支持自动化批量APP的动态检测，每个APP分别输出检测报告，检测报告包括应用基本信息、静态解析信息、动态解析域名信息、第三方调证等信息；**（需提供软件实际使用功能截图）**  8.应支持APP应用进程监控自启动和关联启动，停止应用进程，显示启动应用进程的PID和进程信息；**（需提供软件实际使用功能截图）**  9.应集成IOS真机监测沙箱，支持接打电话、收发短信、在3G/4G、WIFI环境下的数据访问、安装/运行/卸载APP应用能力；  10.应支持IDFA、IDFV、通讯录、日历、提醒事项、传感器数据、运动数据、媒体和音乐、照片、获取定位、相机操作、录音操作、语音识别、TouchID/FaceID、获取WiFi信息等动态行为的采集；**（需提供软件实际使用功能截图）**  11.应支持读写粘贴板、检查权限、蓝牙操作、授权弹窗、监听电话状态等动态行为的检测；**（需提供软件实际使用功能截图）** | 1套 |
| 3 | 手机云取证 | 1．应支持Android、iOS，其中iPhone手机应支持越狱和未越狱设备，Android手机应支持已ROOT和未ROOT设备。  2．应支持备份文件解析，包括iTunes（iPhone）、Android、等平台手机的备份文件。  3．应支持多种应用云数据取证  （1）应支持云备份类。  （2）应支持交易支付类。  （3）应支持银行类：  （4）应支持社交。  （5）应支持出行类。  （6）应支持云盘类。  （7）应支持国外社交类。  （8）应支持短视频类。  （9）应支持生活服务类。  （10）应支持通信运营商类。  （11）应支持快递类。  （12）应支持智能生活及智能安防类。  （13）应支持智能穿戴类。  （14）应支持邮箱类。  （15）应支持数字货币类。  （16）应支持金融借贷类。  （17）应支持视频固定。  4．应支持APP提取密钥。  5．应支持大屏动态实时数据演示：产品处于云数据下载过程中，可点击进入大屏展示，实时展示下载的相关信息，并可点击对应文件进行相关预览。  6．应支持文件与任务的断点续传，可在断电断网等异常中断后的任务和文件断点续传。  7．应支持多检材、多应用、多账号并行云取证。  8．应支持Android系统在取证过程中无需频繁点击授权提示，提高取证效率。  9．应支持手机自动备份取证，减轻用户取证的工作量。  10．应支持获取手机相关设备信息。  11．应支持手机已删除数据的恢复，其中iPhone手机越狱和未越狱均可实现删除数据恢复，Android手机可自动ROOT后进行删除数据恢复，在ROOT失败情况下，也能应支持Android手机解析和恢复QQ、微信、微博等应用程序数据。  12．应支持手机内存镜像的获取和解析。  13．应支持Android手机基于镜像的深度数据恢复。  14．应支持各品牌手机在未root情况下免刷机直接提取进行并自动解密密。  15．应支持iPhone提权取证，突破iOS系统限制，无需越狱，即可绕过备份密码，提取更丰富的手机数据。  16．应支持使用设备自带显卡进行GPU并行运算解密、应支持密钥数据库文件解密、应支持缓存文件解密Android微信多账号数据；应支持各种即时通讯软件语音文件的转码，并在软件内直接播放；应支持部分应用程序删除数据的恢复；应支持部分应用程序密码/秘钥的提取。  17．应支持手机各类解析数据。  18．应支持各类云盘解析。  19．应支持银行类APP的获取解析。  20．应支持其他应用解析等。  21．语音识别，应支持单个或批量语音识别，可将语音文件自动识别成文字内容，且识别结果应支持列表展示与会话展示，解决人工听取语音耗时长的问题。  22．涉案分析，专业定位淹没在海量数据中的关键涉案信息，利用基于机器学习的智能分析，快速聚焦黄、赌、毒、诈骗、涉贷等会话数据，攻克海量数据查找分析难题。  23．照片分析，快速识别手机中所有照片的人脸，并进行分类，种类包括SH、SB、SJ、SM、SK、证件照（身份证、银行卡、护照、驾驶证、行驶证、车牌、营业执照、名片等）、二维码、人物照片等。辅助分析嫌疑人及其关系网人物样貌。新增AI人脸搜索功能，导入目标图片，对检材中的人物照片进行人脸搜索，碰撞匹配，结果展示。  24．汉语机器翻译其他语言功能，冲破语言障碍，实现跨语言办案，从而降低破案门槛。 | 1套 |
| 4 | 天机云链系统 | 1.应支持≥16条公链全量数据：利用区块链技术，根据各公链特点，搭建节点和对公链链上数据解析，形成链上全量数据库，目前支持Bitcoin、Ethereum、BNB Chain、TRON、Polygon、Dogecoin、Litecoin、Bitcoin Cash、Dash、Arbitrum、Optimism、Base、Avalanche、Blast、zkSync共16条主流公链数据，其他公链持续更新中；  2.入库数据≥1280亿条：通过大数据算法对链上数据解析、清洗、入库，已构建链上全量数据库；  3.链上数据秒级入库：通过区块链技术和大户据算法，实现链上数据秒级同步入库，支持全量、最新的链上数据进行资金追踪；  4.≥10亿条标签：包括实体标签（如交易所、钱包）、风险标签、行为标签等，可进行虚拟币地址溯源和身份追踪；标签数据持续更新中；  5.支持≥700万虚拟币的分析：除了BTC、ETH、USDT、USDC等主流币外，还支持公链上其他代币的交易额、交易数据、活跃地址、持仓地址等的分析；  6.自有服务器，保证数据和使用安全：IDC自有运维多台服务器，保证数据的存储和使用安全；  7.多链聚合分析：聚合≥16条主流公链的全量数据，同一个地址在多链上的数据一网打尽；  8.虚拟币地址智能研判；  9.聚合浏览器；  10.地址基础数据分析；  11.地址条件分析；  12.主要交易对手分析；  13.可视化交易对手分析；  14.资金链路智能分析；  15.资金链路流入流出列表分析；  16.比特币地址UTXO分析；  17.地址标签库：；  18.虚拟币交易哈希查询；  19.虚拟币信息查询；  20.ENS查询；  21.法币案件资金穿透；  22.案件管理：支持案件数的统计、案件录入、涉案资金估值、涉案地址管理多维度管理；  23.案件协同：支持案件共享、案件移交、案件分享等，便于协同办案；  24.团队账号：同一团队下，可设置多个账号，并进行案情信息共享；  25.涉案规模估计：通过案件内管理的地址，结合实时币价信息进行涉案规模估计；  26.地址实时监控；  27.协助调证：支持快速通过地址、哈希、自然人信息向交易所、钱包等多组织发起调证、冻结、解冻等申请；  28.智能调证分析：对交易所、钱包等机构调证回来的信息，进行智能调证分析，并形成调证报告  29.交易所资金分析；  30.资产估值：支持历史币价和现价查询，可对涉案代币的资金进行资产估值。 |  |

**合同包2**

**（一）PC智能分析**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **技术参数** |
| 1 | 要素导入 | 1、支持向导式的自动化分析研判，可导入域名、服务器IP、APK等多种类型的线索。  2、支持批量导入要素信息及要素线索。 |
| 2 | 线索智能扩充 | 1、支持域名线索自动扩充，结合域名DNS解析行为、网站特征等线索特征信息智能扩充，快速串联出同窝点、同开发者的域名、服务器IP线索。  2、支持服务器IP线索自动扩充，结合DNS反向解析行为、IP特征信息等线索特征信息智能扩充，快速串联出同窝点、同开发者的域名、服务器IP线索。  3、支持APK线索智能扩充，基于海量APK数据，结合APK名称、包名、图标、源代码等APK特征信息线索的特征智能扩充，快速串联出同窝点、同开发者的同源APK线索。 |
| 3 | 要素智能快筛 | 支持快速筛查可研判的高价值要素，上传单个或批量要素后，系统自动完成要素线索进行评估并反馈要素是否可研判，协助用户快速筛选出高分析价值的要素。 |
| 4 | 智能研判流程图 | 1、支持查看模型研判过程中的线索流转过程，相关规则命中情况。  2、对线索关联、智能匹配、嫌疑特征筛查、综合嫌疑程度打分等过程综合分析，输出研判小结，能更清晰的掌握研判结果“从哪里来、为什么来”。 |
| 5 | 智能研判图谱 | 支持图谱形式清晰的呈现研判结果，方便用户快速找到可疑节点，梳理线索-“R”的关联关系，快速判断哪些“R”存在可疑行为。 |
| 6 | “R”列表 | 支持查看要素关联“R”列表，包含“R”基础信息、特征标签及命中涉案线索详情，直观判断“R”可疑程度及与要素的关联程度。 |
| 7 | “R”画像 | 1、支持对智能研判发现的“R”进行分析，提供基础属性分析及行为特征分析。  2、支持对智能研判发现的可疑终端或“R”进行刻画，清晰描述“R”终端和“R”信息，完成多维度用户画像，辨别“R”身份。 |
| 8 | 智能研判报告 | 支持自动生成要素研判报告，包含要素基础信息、“R”画像报告、“R”研判信息、智能研判结论等。 |
| 9 | 二次研判 | 1、支持手动添加外部新线索进行要素二次研判。  2、支持添加已解锁“R”画像中的高价值域名、路由等作为二次深挖研判线索。 |
| 10 | 要素详情 | 支持查看要素基础信息、要素关联线索及智能研判结果。 |
| 11 | 多维线索解析 | 基于域名、IP、APK等线索类型，进行多维解析，可挖掘线索间的关联关系，扩充要素线索。 |
| 12 | 版本 | 可查看下载≥300个终端画像和报告。（服务有效期1年，过期无法使用） |

* APK智能研判系统

**1.建设内容**

本系统要求“平台+服务”的模式，提供大数据分析展示与案情研判系统。项目交付后，提供为期12个月的平台维护、模型迭代服务、系统操作培训、产品升级培训服务、问题响应服务等内容。系统功能包括：

1. 具备目标筛查能力

提供多种基础筛查模型进行数据筛查与展示。

1. 具备实人转换及支付查询

提供实人要素互译实现对异常金融数据的关联穿透和智能识别。

1. 具备数据关联分析能力
2. 具备可视化展示能力
3. 具备数据导出功能

**2.服务要求**

2.1系统维护的要求：质保期为12个月，质保期内提供相关软件产品免费主动升级服务。

2.2系统培训的要求：项目交付后，服务提供单位需要派驻技术人员到现场提供一段时间的系统培训。

2.3采购人在本次招标需求之外的新增功能研发需求，由中标人与招标单位在合同中另行约定相应的开发量及相关费用等事宜。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **指标项** | **功能要求** | | **服务次数** |
| **一** | **智能研判系统** | | | |
|  | 全息查询 | 设备查询-设备信息 | | ≥30000次/年 |
|  | 设备查询-设备特征 | | ≥30000次/年 |
|  | 设备查询-历史WIFI/IP | | ≥30000次/年 |
|  | 设备查询-轨迹走势 | | ≥30000次/年 |
|  | 设备查询-APP特征 | | ≥30000次/年 |
|  | 设备查询-社交账号 | | ≥10次/年 |
|  | ★设备查询-行为推测 | | ≥30000次/年 |
|  | WiFi查询 | | ≥10000次/年 |
|  | IP查询 | | ≥10000次/年 |
|  | APP查询 | | 不限次 |
|  | 经纬度分析 | | ≥5000次/年 |
|  | ★基站查询 | | ≥5000次/年 |
|  | 分析研判 | APP分析 | | ≥5000次/年 |
|  | ★APP同源拓展 | | 不限次 |
|  | 群体画像 | | ≥5000次/年 |
|  | APK解析 | | 不限次 |
|  | 零号设备分析 | | ≥3000次/年 |
|  | 聚集地分析 | | ≥300次/年 |
|  | WiFi碰撞 | | ≥2000次/年 |
|  | IP碰撞 | | ≥2000次/年 |
|  | WiFi/IP批量碰撞 | | ≥2000次/年 |
|  | 智能分析 | ★APP智能深度分析 | | ≥100次/年 |
|  | ★可视化智能研判 | | ≥100次/年 |
|  | ★窝点智能分析 | | ≥100次/年 |
|  | 实人档案支付洞察 | 实人要素互译 | | ≥40000 次/年 |
|  | 银行卡属性分析 | | ≥40000 次/年 |
|  | 线下交易洞察 | | ≥40000 次/年 |
|  | 转账洞察（YSF) | | ≥40000 次/年 |
|  | 全网交易洞察 | | ≥40000 次/年 |
|  | 支付智能分析 | ★涉诈卡分析 | | ≥10000 次/年 |
|  | ★涉案人员资金研判分析 | | ≥10000 次/年 |
|  | 日志中心 | 我的日志 | 查询日志、查询明细。 | / |
|  | 售后服务 | 售后服务 | 提供7\*24小时线上售后服务，根据要求提供售后服务。 | / |
|  | 更新升级：支持在线升级，免费提供数据服务更新升级，保证所提供软件服务系统为最新版本。 | / |
|  | 使用账号 | | 全模块使用账号 | ≥2个 |
| 其他要求 | | | | |
| 1.★要求引入的用户移动智能终端数据源覆盖终端设备数量≥100亿，总月活用户数量需达14亿。  2.要求“pg”设备轨迹信息≥300万。 | | | | |

（三）数据清洗分析系统

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **技术参数** |
| 1 | 数据智能清洗 | 1、支持单批次选择1000个以上的文件一键导入，支持xlsx、xls、pdf、txt、csv、et、ett、dat、wps、html等文件格式，支持单表、单表多个sheet表、多表、文件夹、多重文件夹的一键批量导入。支持拖动文件或文件夹至导入页面直接进行导入（**提供软件功能截图**）。  2、支持单批次导入多种类型数据的混合导入，软件智能区分多种类型的数据分类入库。  3、支持rar、zip压缩文件自动解压并导入，支持加密文件密码验证。  4、支持的超大型文件导入，单个大于4G，数据量超1000万以上文件在10分钟以内导入（**提供软件性能截图**）。  5、智能解析各类数据，支持内网线上调取和外网线下机构调取数据的直接导入。  6、在数据导入界面能够显示每一个文件的大小、识别状态、数据数量、导入率，识别率等，可双击任一行查看该文件的导入详情。支持查看已导入、未导入数据的详情。  7、数据导入自动清洗识别（**提供软件功能截图**）。  8、数据导入的过程中智能补充数据缺失值，如姓名、账号等。  9、未识别文件支持自定义模板导入，后续同类数据可以智能识别导入。也可以批量将未识别的文件下载至本地。支持将自定义模板导出分享给其他用户导入应用。  10、支持自定义数据储存资源库，当遇到资源库中没有的数据类型时，可自己创建数据资源表结构用于存储同类数据，创建完成会自动存储清洗模板，再次导入同类数据可以智能识别，自动导入。  11、支持对已导入的数据进行管理，可删除单个文件及文件夹，支持一键全字段去重及自选字段去重。  12、对已导入的数据提供数据概览，包括各类调单主体数量、各类数据的数据量以及数据清洗后的存储资源表等。 |
| 案件管理 | 1、采用案件管理的方式对不同的案事件进行区分管理，支持案件的新建、编辑、删除。新建案件及编辑案件时可编辑案件名称、案件类型、案件说明。  2、支持一键将案件数据分类打包导出。  3、支持一键将案件整体打包为特定格式数据文件导出；导出的数据文件支持其他用户导入到本软件中使用。 |
| 通用分析 | 满足各类数据分析。 |
| 账单分析 | 对各类账单智能分析。 |
| 通用功能 | 对各类清洗排序。 |
| 零代码可视化自主建模 | 当系统内置模型不满足用户分析需求时，软件提供零代码可视化自主建模功能，用户可以根据自己的想法和思路，无需写SQL语句，全程采用拖拽点选、以流程设计的模式建设适合具体个案的分析模型。  1、拖拽式操作：对数据表进行操作时，支持用鼠标从资源列表中拖拽某一或某几张数据表到建模区。  2、条件过滤：支持在拖拽出的数据表上进行任意字段的条件过滤，也可以在数据预览区字段名称上右键点击后快速设置过滤条件。可实现多数据表间过滤条件的互相引用，当被引用的条件做更改时，其它引用此条件处也随之更改。  3、数据排序：对于预览区数据表，支持对任意字段的快捷升降序排序；也可右键点击字段名称对每个字段单独设置排序方式，实现多字段的组合排序。  4、字段设置隐藏或可见：支持管理员在后台设置任意字段的隐藏。也可在预览区右键点击字段名称设置任意字段的隐藏， 还可双击任意一行数据通过弹出的菜单来批量设置字段的隐藏/显示。  5、字段位置任意调整：支持采用鼠标拖拽的方式对字段的位置/顺序进行任意调整。  6、扩展字段：支持对数据表中某一字段通过特定函数提取其隐含信息扩展为新的字段，对扩展出的新字段可进行重命名，可扩展的字段包括时间类，车牌类、身份证类、字符类、运算类、数值类等。  7、统计功能：统计支持分组统计、交叉表统计和图表统计。分组统计可以选择字段做分组，支持统计数量、合计、平均值、最大值、最小值、信息拼接等；交叉表统计支持自由设置行和列；图表统计支持饼状图、柱状图、折线图、雷达图显示，图表可下载。  8、数据上下钻：分组统计之后自动生成一个数据链接指向源表，可以双击某一行记录上钻查看详细信息；也可选择某一字段添加数据链接，自定义需链接的数据表，上下钻该字段在其它数据表中的关联信息。  9、自碰撞：支持在条件过滤、扩展字段、统计筛选之后，或直接在原数据表上，设置碰撞条件进行自碰撞。  10、多表碰撞：支持两张数据表之间通过选择碰撞方式及碰撞条件，生成新的结果表，支持碰撞后的结果表和其它数据表的再次碰撞。  11、碰撞方式选择：支持碰撞的方式选择，可以选择内连接、左连接、右连接、左排除、右排除、全连接、数据合并共七种碰撞连接方式。  12、碰撞条件选择：支持对碰撞条件的选择，包括对做条件的字段选择、对条件符号的选择，其中条件符号包括等于、大于等于、小于等于、大于、小于、不等于、加、减、时间差（秒、分、小时、天）、收付差以及自定义函数的编写。  13、数据表导出：支持把碰撞筛选出结果表和原始数据表以Excel表格形式导出，可选择要导出的行数、选择导出浏览数据或原始数据。  14、数据表碰撞建模保存发布：数据筛选、建模碰撞结束后，可以对建模区里的模型进行保存/发布。保存支持保存为草稿、另存草稿；发布支持发布给指定人、指定群组或发布给所有人，可对模型进行应用名称、模型分类、应用描述进行编辑。已发布的模型可进行修改、删除、重命名、取消发布等操作。  15、模型的导出/导入：支持把已建好的模型导出为文件，在相同的平台下可将该文件导入，即可重现模型的建模步骤，进行相应的查看、修改、删除等操作。  16、模型定时执行：已建的模型可保存为定时任务，执行频率可按每天、每周、每月（可选执行的时分）或间隔时/分/秒选择，模型即可自动根据设定的时间/频率执行。  **以上自主建模功能参数提供经国家认证或认定有资质的检验检测机构颁发的检测报告进行佐证，未提供不得分。** |
| 软件性能 | 1、数据导入：导入数据结果为100万级的响应时间≤150s。  2、分组统计：对数据表（1000万级、无索引）进行分组统计的响应时间≤2s。  3、数据关联碰撞：对2个数据表（分别含1000万条及1万条、无索引）进行关联碰撞的响应时间≤35s。  **以上性能参数提供经国家认证或认定有资质的检验检测机构颁发的检测报告进行佐证。** |
|  | 说明 | 提供加密狗≥1个，单机支持不低于1000万数据量的分析。 |