## FL-2000 取证航母一体化智能取证工作站系统.V2S

### 技术参数

一、资质及其他要求：

1.★产品需为国内自主研发，且具有自主知识产权，无软件潜在泄密风险；（须提供软件著作权证书作为佐证）

2.★产品需具有部级测机构出具的检验报告及省级软件测评中心出具的测试报告（须提供对应的报告证明复印件）；

二、硬件配置要求

1.需配置不低于23.8英寸的触控显示器；

2.需配置不少于2个34英寸以上的宽屏高清显示器；

3.需配置不低于7英寸的触控显示屏，可用于案件信息显示和硬盘擦除控制等；

4.需配置主频不低于3.0GHz、内核数不低于24核、线程数不低于32线程的CPU；

5.需配置不低于128GB DDR5高速内存；

6.需配置不低于12GB显存的独立显卡；

7.需配置不低于2TB的固态硬盘作为系统盘；

8.★需配置不低于8TB\*4组RAID5阵列的数据存储盘；（需提供软件界面截图）

9.需配置不少于 4个SATA/SAS硬盘只读仓和4个SATA/SAS硬盘读写仓（可灵活切换到只读）；

10.需配置不少于2路的SATA硬盘仓用于硬盘擦除和不少于2路的USB3.0接口用于USB存储介质擦除；

11.需配置不少于8路直通功能的手机取证USB3.0接口；

12.需配置不少于4个USB3.0读写接口；

13.需配置不少于2个220V电源接口、4路5V/2.1A USB充电口、1个无线快充、1个RJ45千兆网络接口、1个电话接口；

14.★需配置银行卡取证接口（IC芯片、磁条、NFC三种银行卡）、身份证取证接口、三合一SIM卡取证接口；（需提供软件界面截图及实物照片）

15.需配置蓝光刻录光驱；

16.需配置不少于1个500万像素广角摄像头和不少于1个1300万像素自动对焦的高拍仪摄像头；

17.★需配置不少于一个支持3.5/2.5吋的sata硬盘扩展仓；（需提供实物照片）

18.需支持有线（HDMI接口）和无线投屏；

19.预装windows10神州网信政府版操作系统；

三、技术条款要求：

（一）主要功能：

1.需提供录屏录像功能，配置广角摄像头可以对取证区域进行录像，同时支持取证日志审计；

2.需支持自定义取证流程，可以接入存储介质后一键完成介质预检、数据固定、取证分析、系统仿真和融合分析等取证工作，并自动生成取证报告；

3.★需提供语音交互功能，支持语音知识问答和语音操作取证；（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

4.需支持语音识别，支持单个或批量语音识别；

5.需支持维汉翻译，支持普通维文、拉丁维文-汉语机器翻译功能；

6.★需支持对手机和计算机取证结果进行融合分析。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

（二）多路硬盘复制

1)需支持不少于4路高速硬盘复制同时工作

2)需支持不少于4路读写与8路只读的切换，实现8路同时镜像

3)需支持对异常扇区磁盘多次尝试复制功能，多次尝试复制失败后系统自动跳过异常扇区继续进行复制操作。

4)需支持对复制和DD镜像时，进行断点续传功能

5)需支持自动识别HPA、DCO隐藏区域

6)需具备高性能的镜像功能，支持 MD5，SHA1，SHA-256等格式的校验，支持DD镜像、E01镜像、AFF镜像文件制作功能，存放路径

（三）仿真系统

1)需支持对Windows系统的用户操作痕迹进行时间线播放

2)需支持对Windows、MAC 操作系统系统信息、易丢失数据等不少于2种关键数据获取

3)需支持Windows、MAC、Linux、ESXi等不少于4种操作系统登录密码的绕过功能

4)需支持HFS、apfs等不少于2种加密磁盘进行仿真

5)需支持tgz,xb格式的仿真取证

6) 需支持对全盘镜像或分区镜像（dd,e01,qcow3等）不少于3种格式的仿真取证以及镜像中的分区、操作系统及用户等重要信息直接查看

7)需支持不少于对物理磁盘和镜像文件2种介质存储方式的仿真取证；

8)需支持对Windows、Mac OS、Linux等操作系统进行仿真取证

9)需支持同时进行不少于8个数据源以及多镜像仿真

10)需支持对GPT格式大容量磁盘的识别和仿真

11)需支持Windows系统仿真失败时的高级修复

12)需支持全自动仿真，可一键完成磁盘或镜像的仿真

13)需支持历史仿真记录、环境配置（内存、共享目录、虚拟机、网卡等）等查看

（四）计算机取证

1)需支持FAT32、exFAT、NTFS、ReFS、CDFS、UDF、HFSX/HFS+、APFS、EXT4、BTRFS等不少于10种主流文件系统格式的解析

2)需支持E01、Ex01、L01、DD、001、ISO、VMDK、VHD、AFF、GHO、HDD、VHDX等镜像文件的加载和分析

3)需支持RAID自盘组自动计算磁盘序列，并推荐适配RAID类型建议；需支持JBOD、RAID0、RAID1、RAID5、RAID6、RAID F1阵列重组

4)★需支持macOS的RAID0解析、Fusion Drive融合磁盘解析、APFS Fusion融合磁盘解析（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

5)需支持Linux下的LVM解析；需支持Linux的MDADM软RAID解析

6)需支持Windows LDM动态磁盘解析；需支持Windows storage Spaces存储空间解析

7)需支持EFS、BitLocker、TrueCrypt、VeraCrypt、Luks、FileVault2的离线解密；需支持APFS文件系统加密数据离线解密

8)需支持证据文件镜像挂载成本地磁盘功能；支持检材中虚拟磁盘镜像解析；支持磁盘/镜像检材类型数据源重置功能

9)需支持正则表达式；支持建立索引搜索，对文件名和内容可实现秒级搜索响应；支持对Office复合文件和PDF文件的搜索

10)需支持Bitlocker、TrueCrypt、VeraCrypt内存秘钥搜索及解密

11)需支持Virtual Box、QEMU(KVM)、VMware虚拟磁盘解密

12)需支持iTunesBackup备份解析以及加密备份的解密功能

13)需支持简单删除文件恢复、格式化后的文件恢复、被删除的磁盘分区恢复、根据文件头尾特征对被删除文件进行恢复

14)需支持windows、mac、UOS、银河麒麟系统的系统痕迹分析、USB设备使用记录、应用程序运行痕迹、用户最近访问记录、回收站删除记录、远程桌面、用户痕迹分析

15)需支持浏览器类应用程序解析，包括但不限于IE、Chrome、Firefox、360、傲游、Opera、腾讯TT、世界之窗、搜狗、Microsoft Edge、2345浏览器、Yandex

16)需支持邮箱类应用程序解析，包括但不限于Foxmail、邮箱大师、Office Outlook

17)需支持输入法应用程序解析，包括但不限于百度拼音 、搜狗拼音、搜狗五笔、QQ拼音

18)需支持云存储应用的解析，包括但不限于百度云盘、iCloud、腾讯微云等

★19)需支持至少一款隐写软件的解析（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

20)需支持即时通讯类应用程序解析，包括但不限于QQ、微信、钉钉、telegram

21)需支持快速搜索并定位反取证软件、加密文件等功能，需支持对文件进行分类，并需支持对视频文件进行分帧查看，提高调查速度；

22)需支持网络下载工具的下载记录，包括但不限于迅雷、网际快车、电驴、超级旋风 、比特彗星、FileZilla、BitTorrent

23)在联网状态下，电脑端QQ、微信登陆状态下，无需手机可在线解析支持微信、QQ、钉钉的聊天记录、好友信息、群组信息，并支持删除记录的恢复；支持内存镜像中获取QQ、微信的密钥进行离线解析

24)需支持手机登陆QQ的情况下在电脑端通过二维码扫描进行解密的功能

25)QQ有设备锁情况下支持绕过

26)需支持手机登录微信情况下在电脑端通过二维码扫描进行解密的功能

27)需支持手机微信备份文件的自动查找及解析

28)需支持对即时通讯中的语音进行转换，包括不限于将维文转化成汉文、语音转文字等，提升可阅读性

29)需支持用户自主编程、编程方式简单可视化、可调试、可拓展，满足个性化需求

30)★需提供丰富的人工智能能力给用户调用，提升编程效率，包括但不限于OCR、图片分类、人脸检测等（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

31)需支持将取证结果的重点信息进行标注、归类并按照实际需求自定义模版形式导出

32)需支持照片Exif信息提取和分析

33)需支持卷影副本解析，并可查看文件的历史版本

34)需支持文件签名分析，快速查找可疑签名文件；并根据文件签名等特征信息，在未分配簇、Pagefile.sys、Hiberfil.sys等位置进行文件签名恢复

35)需支持在未分配簇、PageFile.sys、Hiberfil.sys 等位置进行取证分析

36)需支持NTFS文件溯源分析、涉案分析等分析功能

37)支持MD5、SHA-1、SHA-256等多种哈希值计算

38)需支持工具集功能，需提供动态取证、密钥获取、内存镜像解析、镜像挂载工具、银行卡采集、哈希计算等应用

（五）手机取证

1、手机支持能力

1)需支持Android、iOS、鸿蒙手机取证

2)需支持手机备份文件解析

3)需支持手机镜像制作及解析。

2、手机解锁及提权

1)需支持华为、三星、vivo、小米、oppo、魅族等主流品牌手机的密码破解、ROOT权限获取及高级备份。

2)需超级ADB技术，支持手机在未ROOT情况下免刷机直接提取镜像进行并自动解密。

3)需支持iOS系统破解4位开机密码。

4)需提供iPhone提权服务，突破iOS系统（支持iOS10.0-16.1.2版本）限制，无需越狱，即可绕过备份密码，提取更丰富的手机数据，其中iOS14.0-15.4.1（iPhoneXS以上机型）支持免联网免签名一键快速提权。

3、手机数据提取和恢复

5)突破Android手机权限限制，需支持OPPO、华为、魅族、小米等手机自动备份取证，在取证过程中无需频繁点击授权提示，提升用户体验，提高取证效率。

6)需支持获取手机基本信息

7)需支持提取SIM卡记录。

8)需支持手机已删除数据的恢复

9)需支持深度恢复微信、短信等删除数据

10)需支持Android手机最近删除文件恢复、需支持Android手机缩略图恢复

11)需支持IOS加密备份的keychain解析

12)需支持Android、iPhone、鸿蒙手机各类文档的分类取证

13)需支持提取应用多账号数据、密钥、附件，恢复删除数据。

14)★需支持微信公众号文章缓存页面重组（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

15)需支持手机即时通讯类、社区交友类（微博类）、电子邮箱类、浏览器类（上网日志）、出行软件类（行程记录类）、电子商务类、手机助手类（第三方安全、手机优化管理类）、车载导航记录、视听软件类、网盘类、银行类、证券金融类、输入法类、物流快递类、文件管理类（文件传输及文本编辑和阅读类）、突网工具类（翻墙类）、区块链类、运动健康类等共计超800款应用数据获取解析。

16)需支持手机Wi-Fi、蓝牙连接记录的提取，支持手机GPS、Wi-Fi、基站、照片位置信息及部分应用程序位置信息的提取。

17)需支持手机APK静态行为分析，支持提取权限、开发者、服务器地址等信息，取代繁琐的手工分析。

4、拓展工具

1)★针对手机APP种类广、版本多、迭代快等特点，用户可自定义编写Python程序，实现对新APP数据的快速提取，并支持将提取结果合并到案例数据中。同时可通过小程序共享平台发布或下载各类拓展功能。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

2)需提供超过30款自主知识产权的手机取证工具集，包含各类工具工具，解决手机取证过程遇到的各种疑难问题。

（六）融合分析

1)需支持完成手机、计算机取证后自动融合分析

2) ★需支持人物画像分析：分析机主身份属性，包括姓名、身份证、住址、手机号码、虚拟身份（QQ、微信、E-mail等）、银行卡号、车辆、毕业学校、加入组群等基本属性。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

3) ★需支持社会关系分析（分析对象<=5）：分析机主的社会关系，找出主要关系人，以及加入群组的情况；分析群聊话题和高频词，可分析敏感群共同群成员；根据聊天内容类型快速过滤分析对象。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

4)★需支持时空分析：以时间、空间及行为等多维度分析机主的事件，使用时间轴、地图结合详情的形式，刻画机主的轨迹事件。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

5)需支持经济行为分析：通过对银行短信、支付宝、微信账单数据的分析，刻画机主与好友间的资金往来情况。

6)需支持行为习惯分析：刻画分析对象行为倾向，包括通联、上网、出行行为。

7)★需支持视频图像分析：利用AI图片技术，进行人脸照片、证件照、银行卡、二维码类图片识别，人脸照片通过出现、合影行为分析机主以及对象的亲密关系，支持以图搜图的能力。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

8)需支持多人关系分析（分析对象<=5）：通过分析同个案件内的多个持有人手机数据，刻画出机主间存在的通联、轨迹、文件、身份、设备等多维度关联关系，支持同人分析。

9)需支持身份挖掘：可提取和分类展示人名、地名、手机号、身份证号、车牌号、银行卡号、快递单号等特殊身份标识及其来源。

10)需支持涉嫌分析：找出文本和多媒体中匹配设定的“黄赌毒骗贷模型”、“置信度”条件范围内的通联内容列表或涉案类型占比情况；支持查看命中的涉案通联的上下文。

11)★需支持文件追踪：对分析的案例数据进行全库的敏感文件比对碰撞，一步步溯源，找出文件在案例中最早出现的详情；支持相似图片追踪。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

12)★需支持高频词分析：对分析的案例中出现文本聊天内容快速分析、查看、导出全案件文本聊天中的高频词汇及详情信息。（需提供软件界面截图及参数响应情况对应的检测报告复印件，并标明对应的检测项）

13)需支持全文检索：可在检索条件设置完成后，从所选分析对象数据中模糊匹配出包含关键词的各类数据。