**美亚柏科DC-8811 取证魔方.V3**



**硬件配置**

●配置电容触控显示屏尺寸不低于11.6英寸，分辨率不低于1920\*1080

●配置CPU不低于Intel 酷睿i7-7820eq，内存不低于32GB DDR4，SSD系统盘不低于480GB；

●主要I/O接口：2个SATA/SAS只读接口、1个IDE只读接口、2个SATA/SAS读写接口、1个USB3.0只读接口，4个USB3.0读写口，1个USB3.1 Type-C接口，万兆网口和千兆网口，HDMI显示接口

●配置WIFI模块

●外观尺寸：336\*326\*77mm

●预装Win7 64位WES版本操作系统；

**智能取证**

● 采用大尺寸触控方式，取证分析工作所见即可得；

● 支持自定义取证流程，可固定常用取证方案，一键完成取证工作；

● 支持检材录入及案件管理功能。

1. **硬盘复制**

* 硬盘复制功能支持一对一、一对二、二对二复制，并提供SATA/SAS免接线直插式只读接口；
* 支持IDE、SATA、SAS、USB等接口硬盘的高速复制，SAS硬盘最高复制速度可达50GB/min；
* 支持对异常扇区磁盘(如坏扇区)的多次尝试复制功能，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。
* 支持对目标计算机进行不拆机硬盘复制；
* 支持断点续传功能，可在出现临时停止或异常中断后从断点处继续执行复制操作；
* 支持在硬盘复制或镜像时进行关键词搜索，并可将结果直接导入内置取证分析软件进行分析；
* 支持自动识别HPA隐藏区域，并可进行复制、镜像等操作；
* 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，E01镜像复制时可设置压缩率、存放路径等参数；
* 支持将硬盘镜像文件直接还原到硬盘；
* 并行工作能力，即在硬盘复制的同时支持对数据进行取证分析以及仿真分析.

1. **取证分析**

* 具有自动取证、索引搜索功能，可以实现自动调查分析操作、导出并打印报告
* 支持Windows系统（最高支持Win10）、Mac OS X系统（最高支持Mac10.13）和Linux系统取证
* 支持对多个磁盘或镜像的并行数据分析和关键词搜索
* 支持在未分配簇、PageFile.sys、Hiberfil.sys等位置进行取证分析
* 支持MD5、SHA-1、SHA-256等多种哈希值计算

**文件系统加载和恢复能力**

* 支持基本磁盘/动态磁盘、MBR磁盘/GPT磁盘、LDM/LVM/LVM2磁盘、磁盘阵列重组，支持FAT12、FAT16、FAT32、exFAT、NTFS、CDFS、UDF、Ext2/3/4、HFSX/HFS+ UFS、ReiserFS、XFS、NILFS2、ReFS、VMFS、ZFS、JFS、JFS2、APFS、F2FS、BTRFS、 QNX4FS、QNX6FS、JFFS2以及手机上的YAFFS2、ROFS、黑莓BlackBerryFS等多种文件系统格式的解析
* 支持E01、Ex01、L01、DD、IMG、001、ISO、DMG、VMDK、VHD、AFF、Lx01、GHO、VDI、DVD、HDD、HDS、VHDX、QCOW2等镜像文件的加载和分析
* 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
* 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

**复合磁盘结构解析能力**

* 支持LDM/LVM/LVM2磁盘结构
* 支持Linux的MDADM软RAID解析
* 支持win10的 Windows Storage Spaces存储空间解析
* 支持macOS的Fusion Drive融合磁盘解析
* 支持macOS的RAID0解析
* 支持JBOD、RAID0、RAID1、RAID5常规左同步、RAID5常规右同步、RAID5常规左异步、RAID5常规右异步的RAID磁盘组加载
* 提供RAID自盘组自动计算磁盘序列功能，可提供最符合条件的RAID类型建议

**加密数据解密能力**

* 支持EFS离线解密
* 支持BitLocker离线解密(支持最新Win10 XTS-AES新加密算法)
* 支持FileVault2离线解密
* 支持VeraCrypt离线解密
* 支持Luks离线解密
* 支持对苹果系统APFS下的FileVault2加解密数据解密及APFS文件系统加密数据解密
* 支持TrueCrypt加密文件/分区的自动检测和加载解密
* 支持Virtual Box虚拟机加密虚拟磁盘解密功能
* 支持KVM虚拟机加密虚拟磁盘解密功能
* 支持iTunesBackup备份解析以及加密备份的解密功能

**文件系统其它功能**

* 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的解析功能
* 支持磁盘/镜像检材类型数据源重置功能
* 支持卷影副本解析，并可查看文件的历史版本
* 支持NTFS文件溯源分析、涉案分析等分析功能
* 支持NTFS安全属性等高级属性解析功能

**取证能力**

* 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、用户最近访问记录、回收站删除记录、远程桌面、未分配簇中打印记录等
* 支持上网记录分析，包括IE、Chrome、Firefox、360、傲游、Opera、腾讯TT、世界之窗、搜狗、Microsoft Edge、2345浏览器、Yandex等浏览器的用户网页浏览记录
* 支持即时通讯分析，包括QQ、微信、阿里旺旺、钉钉、Skype、RTX、MSN、飞信、京东咚咚、网易泡泡、新浪UC、雅虎、YY语音、ICQ、Line、Pidgin、AIM、Miranda、Adium、ooVoo、飞秋等应用的聊天记录、好友信息、群组信息的解析
* 在联网及获取绑定手机的情况下，支持解析电脑版微信聊天记录、好友信息、群组信息；微信登陆状态下可在线解析无需手机；支持从内存镜像中获取微信密钥进行离线解析
* 支持手机微信备份文件解析，可解析备份在电脑上的微信信息
* 支持QQ解析，在未保存密码的情况下，也可能解析出聊天记录的内容；支持绕过QQ绑定的手机设备锁，在有绑定手机的情况下也可以直接输入登陆密码进行解密
* 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
* 支持邮件分析，包括Foxmail、Outlook Express、Office Outlook、EML、MSG、DreamMail、Win10邮件客户端、Thunderbird、网易闪电邮、邮箱大师、IBM Lotus Notes、Becky! Mail、MacMail、MacEntourage等客户端的邮件内容，并可恢复被删除的邮件信息
* 可提取Foxmail、DreamMail、Thunderbird、网易闪电邮、Office Outlook、UC、QQ、阿里旺旺、飞信、SKYPE、MSN、RTX、飞秋、营销QQ、GigaTribe、Becky! Mail等密码或密钥
* 支持密码/密钥检索功能，包含BitLocker、FileVault2、WiFi密钥的自动检索
* 支持输入法分析，包括百度拼音 、搜狗拼音、搜狗五笔、QQ拼音、Linux Sun拼音输入法等输入法应用的输入记录
* 支持云存储应用分析，包括iCloud、金山快盘、OneDrive云盘、腾讯微云、360云盘等
* 支持Mac内置应用、Mac打印信息、Mac无线连接、Mac蓝牙、Mac远程连接记录等的解析
* 支持快速搜索并定位反取证软件、加密文件等功能，支持对文件进行分类，并支持对视频文件进行分帧查看，提高调查速度
* 支持照片Exif信息提取和分析
* 支持下载工具分析，包括迅雷、网际快车、电驴、超级旋风、比特彗星、FileZilla、BitTorrent等下载软件的下载记录信息
* 支持快速搜索并解析Windows日志、Apache日志和IIS日志信息
* 支持注册表被删除键名、键值的恢复，并能显示最后写入时间

**搜索能力**

* 支持索引搜索，对设备进行索引后，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
* 支持关键词快速搜索，支持正则表达式

**报告能力**

* 支持自动生成报告，方便后续浏览与整理
* 支持自定义报告，取证大师的摘录功能可以将数据片段、文本信息、文件信息、取证结果或其它类型的数据添加到摘录视图中，并可将摘录数据生成报告以自定义模板形式导出

**联动能力**

* 支持将取证结果直接导出到数据逻辑关系分析软件中进行分析
* 支持直连或单向数据传输线形式将取证结果上传到蛛网中进行数据碰撞
* 支持案件关联到蛛网进行案件相关的关联碰撞
* 支持与取证信息网络查询联动，QQ/飞信/阿里旺旺/SKYPE等密钥可以直接推送到极光进行破解

**其他能力**

* 支持动态取证功能（工具集内），获取计算机系统运行状态下的动态信息，包括系统进程、各种通讯及网络服务帐号和密码、上网记录及网络连接信息等
* 支持工具集功能，提供动态取证、QQ密钥获取、内存镜像解析、内存镜像制作、镜像挂载工具、FileVault2密钥获取工具、人脸识别、银行卡采集、\*\*利剑、哈希计算等应用
* 支持按时间线方式浏览文件和取证结果
* 支持在线情况下即时通讯内容的维文转汉文翻译、语音转文字等功能
* 支持案例概览功能
* 支持自定义脚本功能

1. **操作系统仿真**

●支持对物理磁盘和镜像文件两种介质存储方式的仿真取证；

● 支持对Windows操作系统（最新支持Windows10，支持微软账户破解）的80多个版本进行仿真取证；

● 支持对Mac OS操作系统（最新支持10.14，支持加密磁盘仿真）的20多个版本进行仿真取证；

● 支持对Linux（最新支持Ubuntu 19.04）的20多个版本进行仿真取证；

★ 支持同时进行多个数据源以及多镜像仿真；

※ 支持Windows、MAC、Linux操作系统登录密码的绕过功能；

★ 支持apfs加密磁盘进行仿真；

★ 支持对全盘镜像或分区镜像（DD镜像、E01镜像、云镜像等）的仿真取证；

● 支持对GPT格式大容量磁盘的识别和仿真；

● 支持Windows系统仿真失败时的高级修复；

● 支持对全盘镜像或分区镜像（DD镜像、E01镜像等）的仿真取证，可直接查看DD、E01等镜像中的分区、操作系统及用户等重要信息；

● 支持全自动仿真，可一键完成磁盘或镜像的仿真；

● 支持对Windows 操作系统获取信息不少于：系统信息、易失数据、账号密码、上网痕迹、用户痕迹等五大类重要数据；

● 支持对Windows系统的用户操作痕迹进行时间线播放；

1. **手机采集**

* 支持Android、iOS智能手机系统。
* 支持获取手机通讯簿、短信及通话记录信息。
* 支持获取手机媒体文件，包括音频文件、视频文件等。
* 支持提取SIM卡上的通讯录、短息、通话记录。
* 支持iPhone和Android手机已删除数据的恢复，包括已删除的电话簿、短信、通话记录、日程表等信息。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。
* **支持QQ、微信等软件信息的解析。 (提供GAB检测报告佐证)**

1. **视频采集**

* 提供网络视频采集功能，可支持多台录像机设备同时进行视频采集。**(提供GAB检测报告佐证)**
* 提供硬盘视频采集功能，可安全、快速从硬盘获取视频数据。
* 提供删除视频恢复功能，可自动恢复已删除视频文件。
* 内置离线地图，可方便在地图上进行标注及案件研判工作。
* 内置通用播放器，支持播放超过500种格式的视频文件。
* 支持在下载前进行视频搜索、预播放，提升现场采集效率。

1. **计算机在线快速采集**

* 获取目标计算机的内存镜像。
* 支持密码绕过及离线取证。
* 获取系统信息、易失数据、账号及密码、邮件等信息。
* 支持在数据采集过程中进行屏幕截图、录制。
* 支持内存镜像、屏幕录制和采集数据的MD5值计算。
* 支持以幻灯片方式播放用户的使用痕迹。
* 支持对采集的磁盘分区目录无痕浏览、搜索。
* 支持将采集的数据导出或上传至蛛网服务器。
* 支持采集策略调整，提供精灵数据管理工具。