



|  |  |  |
| --- | --- | --- |
| **序号** | **产品型号** | **产品描述及参数** |
| 1 | 盘古石计算机取证分析系统  P-9800 | 主要功能参数：  1.案件管理：支持保存到单一案件文件，支持离线浏览案件，支持数据校验，当数据源改变时，提示用户重新选择数据源；  2.设备加载支持逻辑卷、物理硬盘、镜像（E01、DD、aff、iso、vmdk、img等）、文件集合对象、动态磁盘、磁盘阵列等。可选择不解析文件系统加载，支持定义磁盘结束扇区；  3.支持BitLocker、TrueCrypt加密分区或磁盘解密加载。BitLocker支持通过输入用户密码、恢复密钥或密钥文件对加密分区或磁盘解密；TrueCrypt支持通过输入用户密码或密钥文件对加密分区或磁盘解析；  4.支持磁盘或镜像文件中的dd镜像和vmdk镜像的直接右键挂载，无需导出即可直接挂载分析，挂载完毕后显示在资源目录树下，可直接通过文件系统查看；  5.支持文件系统包括：ntfs, fat12/16/32, exfat, ext2/3, hfs/hfs+, ISO9660, udf，可以对以下文件系统恢复ntfs, ntfs目录索引，fat12/16/32, exfat；  6.支持Windows/macOS/Linux系统基本信息、时区信息、服务信息、硬件信息、用户信息、开机启动项、无线网络及密码信息、回收站删除记录、最近运行的程序、最近打开的文档、网络配置信息、共享信息、安装软件、USB设备使用信息的获取；  7.支持无线连接记录分析和删除恢复；  8.支持快捷方式分析，包括快捷方式指向源文件所在位置，快捷方式创建时间等；  9.支持文档工具编辑记录分析，Office 2013编辑记录分析，WPS编辑记录分析，福昕编辑记录分析，Adobe Acrobat Reader编辑记录分析。  10.支持VPN数据分析，操作系统自带VPN配置数据的分析，GreenVPN的服务器配置数据分析。  11.上网记录分析支持浏览器包括：IE、Chrome、FireFox、360SE、Opera、Safari、QQ、世界之窗、Microsoft Edge等主流浏览器；支持书签收藏夹、缓存、Cookies、历史记录、搜索记录、下载记录的获取；Chrome支持密码的获取；  12.支持Microsoft Edge、世界之窗等浏览器记录解析和删除恢复、支持腾讯微云等网盘应用数据的分析。  13.支持WEB服务器日志类型数据解析，包括Apache日志分析，IIS日志分析。  14.即时通讯分析支持QQ、微信、千牛、移动飞信、阿里旺旺、新浪UC、SKYPE、MSN、Yahoo、ICQ、ooVoo、AIM、Pidgin、Miranda IM、MySpace、YY、Adium等记录解析，包括账号信息、好友列表、群组列表、好友聊天记录和群组聊天记录等；  15.支持QQ聊天记录中语音文件直接播放，语音转化文字功能；  16.支持QQ2009-2013版本客户端的聊天记录解析，支持本地无密码暴力破解QQ及远程验证两种方式，支持QQ聊天记录的删除恢复功能；  17.支持最新QQ9.x版本客户端的聊天记录解析及恢复。  18.支持在线获取密钥解析QQ、微信、千牛、旺旺等即时通讯应用，包括账号、好友、群组、群成员、聊天记录等信息；  19.邮件分析支持常用Foxmail、Outlook Express、Outlook(Win/Mac)、ThunderBird、Mac OS等邮件客户端，支持126、163、QQ、sina等Web邮箱，支持Outlook邮件客户端的删除恢复，支持加密pst文件的解析。解析内容包括收件箱、草稿箱、发件箱、回收站等；  20.支持卷影像拷贝解析，支持对系统不同还原点进行解析，可解析系统痕迹和用户痕迹等，包括文件系统的浏览；  21.识别常见的反取证软件，包括文件销毁工具、破网工具、文件隐藏工具等；  22.支持肤色识别，快速定位色情图片和视频。同时支持对视频进行自定义分帧，提高识别效率。  23.过滤功能支持多层次多种组合的过滤功能，过滤支持正则表达式。同时支持自定义过滤表达式，支持去重功能；  24.数据恢复：支持文件特征恢复、目录恢复、分区恢复等多种恢复形式；  25.可自动生成报告，取证人员可自定义标签、书签等自定义报告内容，方便后续浏览与整理； |
| 2 | 盘古石计算机仿真系统  P-9860 | 主要功能参数：  1.支持将完整磁盘镜像文件和可启动分区镜像文件仿真启动；  2.支持多案件多虚拟机管理，支持虚拟机重构，支持导入虚拟机；  3.支持物理硬盘或者其他存储设备（通过USB、1394等接口连接）；  4.支持以SCSI方式加载虚拟硬盘；  5.支持raw、qcow2、DD、E01格式镜像文件仿真，支持DD或Split DD分卷格式；  6.支持vmdk目录、ESXI虚拟机仿真；  7.支持Windows全系列操作系统；  8.最新支持Win10系统；包括专业版，家庭版，企业版等；  9.支持GPT分区系统的仿真；  10.支持vmware15简体中文版；  11.支持Linux（最新支持Ubuntu18.04）操作系统仿真；  12.支持Mac OS X（最新支持macOS10.13）操作系统仿真；  13.支持原AMD架构操作系统正确仿真；  14.支持提取Windows操作系统的密码Hash或注册表文件，可用于开机密码的明文破解；  15.修复Windows启动蓝屏问题；  16.支持自动解决虚拟机无法启动的故障。用户也可根据需要自定义启动项；  17.支持配置Windows操作系统自启动项；  18.支持绕开Windows操作系统激活机制，对于正常启动需要激活的系统可直接绕过激活机制；  19.支持清除全系列Windows用户登录密码，包括服务器系统的登录密码；  20.支持绕过Linux、Mac OS密码。绕过密码后系统直接获取最高权限，方便取证工作；  21.仿真取证分析时进行的任何操作不会改动原始介质或者镜像文件数据。所有操作均在缓存中进行，重新加载检材后还原到初始状态；  22.自动配置VMWare 和 WinDBG 模拟串口的windows 内核调试； |
| 3 | 盘古石网站取证系统  P-9500 | 主要功能参数：  1.镜像网站，按照原网站结构下载到本地。支持Phpwind、Discuz!等各类论坛，下载后文件以版块、子版块、帖子的方式保存。  2.支持百度贴吧下载，支持微博(新浪微博、腾讯微博、Twitter)、博客（新浪博客、网易博客、百度空间）、社交网络（QQ空间、人人网、Facebook、Google+）。  3.支持网页邮箱（新浪邮箱、网易邮箱、QQ邮箱等）下载。  4.支持淘宝、天猫、1688、微店等购物网站店铺的首页、详情页等页面的固定。  5.支持任意网站的自动登录。  6.支持上述论坛的搜索下载，如搜索某用户的帖子并全部下载。支持论坛按子版块下载。  7.支持任务的增量下载。论坛、博客等可以下载指定时间范围内的内容。  8.支持网页截图，并附有地址栏URL。  9.支持网页链接转换，可在本地浏览整个网页结构。  10.支持下载网页的预览，支持保存为MHT文件。  11.支持任务的断点续传。  12.支持屏幕录像。将网页预览的过程保存为AVI格式。  13.可以获取服务器的IP地址，端口，服务器类型等信息。  14.支持下载层级限制，0表示仅下载当前页面，1表示同时下载当前页面所链接到得页面...以此类推。  15.支持站内/跨站下载，在不跨站的情况下，如果开启渲染必须选项，也将下载显示网页所必须的图片等。  16.支持下载帖子附件的种子文件。  17.下载的同时进行哈希计算，支持MD5、SHA1、SHA256、SHA512。  18.自动为每个板块生成详尽的帖子列表及全站汇总表。  19.任务结束后自动生成勘验报告。 |
| 4 | 盘古石现场取证系统  9800H10 | 主要功能参数：  一.离线取证（Offline）  1.现场取证系统的离线取证（Offline）是通过离线的方式启动取证对象计算机，支持Windows、macOS和Linux三大系统计算机的数据取证。  2支持创建dd、e01和aff三种格式的硬盘/卷镜像。支持分片dd镜像和多种压缩率的E01、AFF镜像。创建镜像时，自动识别对象硬盘和证据硬盘，便于取证人员分辩和选择正确的对象硬盘/卷。  3.硬盘克隆是对源盘的完整复制。硬盘克隆支持对证据盘剩余空间的数据擦除，保证证据盘储存的数据与源盘一致，避免数据遭到污染。  4.校验算法丰富，支持MD5、SHA256等多种校验值计算。  5.系统预置数据库、多媒体、图片、文档、应用程序数据库五种类型文件的快速过滤，通过快速过滤提取取证人员关心的数据。过滤条件支持逻辑“与”或“非”多重组合过滤。  6.支持直接分析、提取取证对象计算机硬盘信息、分区信息、系统信息、系统软件和应用程序信息。针对macOS系统，还支持直接分析或提取macOS系统的信息如下：用户信息、共享信息、日志信息（文件导出列表、开关机记录、硬盘信息变更记录、网络信息变更记录用户活动（通讯录、最近使用项）、用户目录下文件列表、加密文件列表、浏览器（Safari、Chrome）、即时通讯（Skype、iMessage、Adium）、电子邮件（mail、Thunderbird）。  二.Windows在线取证  1.Windows在线取证场景不仅支持离线取证（Offline）的所有功能，还支持内存数据取证和系统正在运行的易失数据（账户密码、用户记录和动态网络数据等）取证。  2.系统支持以创建内存镜像的方式获取完整的内存数据。创建内存镜像时，支持创建分片dd镜像和多种压缩率的E01、AFF镜像。获取的内存镜像可以在计算机取证分析系统中进行分析。校验算法丰富，支持MD5、SHA256等多种校验值计算。  3.系统支持直接提取系统、浏览器、电子邮件客户端中保存的、密码输入框中保存的、即时通讯应用账号、拨号/VPN和无线连接记录的账号和密码。  4.系统支持直接提取活动登录会话、当前登录用户、进程信息、进程依赖模块、服务信息、打开文件进程句柄、剪贴板信息、计划任务信息、SAM哈希、自启动项与程序、访问过的快捷方式、运行过的程序列表、用户登录记录、账户密码策略和域信息、%windir%\tasks里的内容、最近打开的文件列表的用户记录数据。  5.系统支持直接提取网络连接列表、TCP/IP端口信息、网络接口信息、混杂模式端口、路由信息、网络文件信息、网络协议统计、共享资源信息、ARP信息、网络会话信息、NETBIOS统计信息、网络活动连接等动态网络数据。  三.macOS在线取证  1.在线状态下直接运行取证程序获取Mac设备硬盘/卷中的数据。支持创建dd、e01和aff三种格式的硬盘/卷镜像。支持分片dd镜像和多种压缩率的E01、AFF镜像。校验算法丰富，支持MD5、SHA256等多种校验值计算。  2.针对加密卷，支持创建解密后卷zip方式获取Mac设备卷中保存的数据。  3.系统根据不同案件类型预置不同的数据提取策略。电子数据取证人员新建案件时选择对应策略，即可完成策略对应数据提取。默认策略可在维护工具中编辑和配置。  四.系统支持截图与录屏取证，便于电子数据取证人员记录取证的所有过程，做到取证过程可追溯。  五.系统的报告页面支持动态生成包含完整取证数据的勘验报告，电子数据取证人员可以对报告内容进行预览，最终可以根据选择内容导出最终版的现场勘验报告。  六.系统分为提取软件和维护软件两个模块，维护软件支持对提取软件的案件管理、策略配置、维护升级和证据盘擦除功能。  1.案件管理支持对系统的取证案件进行管理和导出勘验报告。  2.策略配置支持对案件类型对应的默认提取项进行配置，支持新增案件类型的管理和默认提取项的配置；支持默认文件类型过滤条件的配置。  3.证据盘擦除支持按照简单方式、BMB和DOD方式擦除证据盘中的数据。 |