**服务器取证分析设备**

**主要功能参数：**

1. Linux（CentOS、Redhat、Ubuntu、Debian等）系统
2. 支持多种连接验证方式，包括密码、私钥和加密私钥连接，并支持用户身份登录并提权，实现禁止 root 帐号远程登陆服务器的提取固定
3. 支持远程终端操作，提供命令行操作窗口，可一键获取服务器信息（包括基本信息、日志、网络、网站及 Docker 数据）并生成 HTML 报告，同时支持对一键获取内容进行预设
4. 支持 Mysql、MongoDB、PostgreSQL、SQLServer 数据库提取分析，包括直连远程主机数据库、查看远程数据库数据表基本情况、对数据库进行备份导出、内置数据库管理软件对关系型数据库和非关系型数据库进行管理
5. 支持查看远程主机网络通信状态和定制获取数据包，并在新建案件时挂载 Socks5 代理，可隐藏投递源 IP 地址
6. 支持案件隔离模式，每个案件可对应不同的树形拓扑网络，并支持同时跨多层子网堡垒机及下属设备
7. 支持以本机作为根节点，一键连接目标主机投放 Agent，网络通信层支持正向连接、反向连接和代理连接，一键部署私有代理服务器和支持本机勘验功能
8. 支持对多台服务器设备同时取证，使用案件概览页面路由表可随时切换控制表内所有设备
9. 支持 UDP 内网穿透代理模式(直连加密流量不过代理服务器，可绕过部分防火墙针对TCP通信的限制
10. 支持将任意内网层级远程服务器网络服务端口或该服务器任意局域网 IP 端口转发至本地空闲端口
11. 支持 Agent 端一键部署 Socks5 服务，可配合端口映射将Socks5服务映射到本地，在多服务器复杂内网情况下横向投递Agent或对内网其他服务器进行移动，且提取时隐藏源 IP 地址为该堡垒机IP地址。

### **数据提取**

1. 支持 磁盘镜像（DD、E01 、zip格式）和文件目录压缩（zip格式）上传至 OSS
2. 支持磁盘镜像过程中因断网导致的任务中断，自动重新构建通信链路，恢复网络即可续传
3. 支持远程镜像或文件下载时，缓存到中间跳板服务器磁盘中，或通过中间跳板服务器上传至OSS
4. 支持阿里云、腾讯云和华为云 OSS 镜像在同区域桶（bucket）自动识别内网传输，内网传输速度可达云同区域最高速度，选定 OSS 任务后，即使关闭软件（未勾选销毁 Agent），OSS 镜像任务仍可在待取证服务器后台继续运行

### **数据解析**

1. 支持 Docker 容器自动提取分析，包括基本信息、镜像列表、容器列表、卷列表、网络列表、登录信息等
2. 支持网站数据自动提取分析，包括但不限于 Apache、Nginx、Tomcat 以及 IIS，远程主机网站配置情况、服务器配置、日志、数据文件显示及一键获取、宝塔/小皮面板深度解析等
3. 支持自动提取服务器日志，包括但不限于登录日志、文件访问日志、历史命令日志、系统日志、应用日志、安全日志、内核日志等
4. 支持查看当前系统所启用的网络端口、协议类型、远程服务器 IP、端口及所对应的进程等信息
5. 支持基本信息自动提取分析，包括系统概况、系统磁盘使用情况、内存使用情况、用户列表、进程列表、系统启动项、IP 地址等
6. 支持网络信息自动提取分析，包括防火墙规则、DNS 缓存、网卡列表、网络连接、网络服务、 ARP 缓存等
7. 支持管理员日志自动提取分析，包括查询服务器所有有效用户、发现服务器隐藏账户、提取相应操作系统用户登录密码等
8. 支持广播执行脚本功能，可同时对多服务器发送并执行bat脚本、 shell 脚本
9. 支持广播方式进行全文关键词搜索，可同时对多服务器磁盘上的文件进行内容关键词搜索。