DigitalHound 数字取证平台 V3.2.1.0

> **让每一字节都无处遁形** · 国产自研 · 一站式计算机取证工作台
>
> *Every byte tells a story — DigitalHound listens.*

🎯 产品定位

DigitalHound 是一款面向公安、司法、企业合规、应急响应与个人调查场景的 **一站式计算机数字取证平台**。

基于工业级内核 **SleuthKit / libtsk** 深度定制，覆盖从 **磁盘镜像加载** → **文件系统还原** → **工件解析** → **时间线关联** → **AI 研判** → **取证报告** 的完整调查链路，在国内同类产品中同时具备 **商业级功能完备性** 与 **源码级可审计性**。

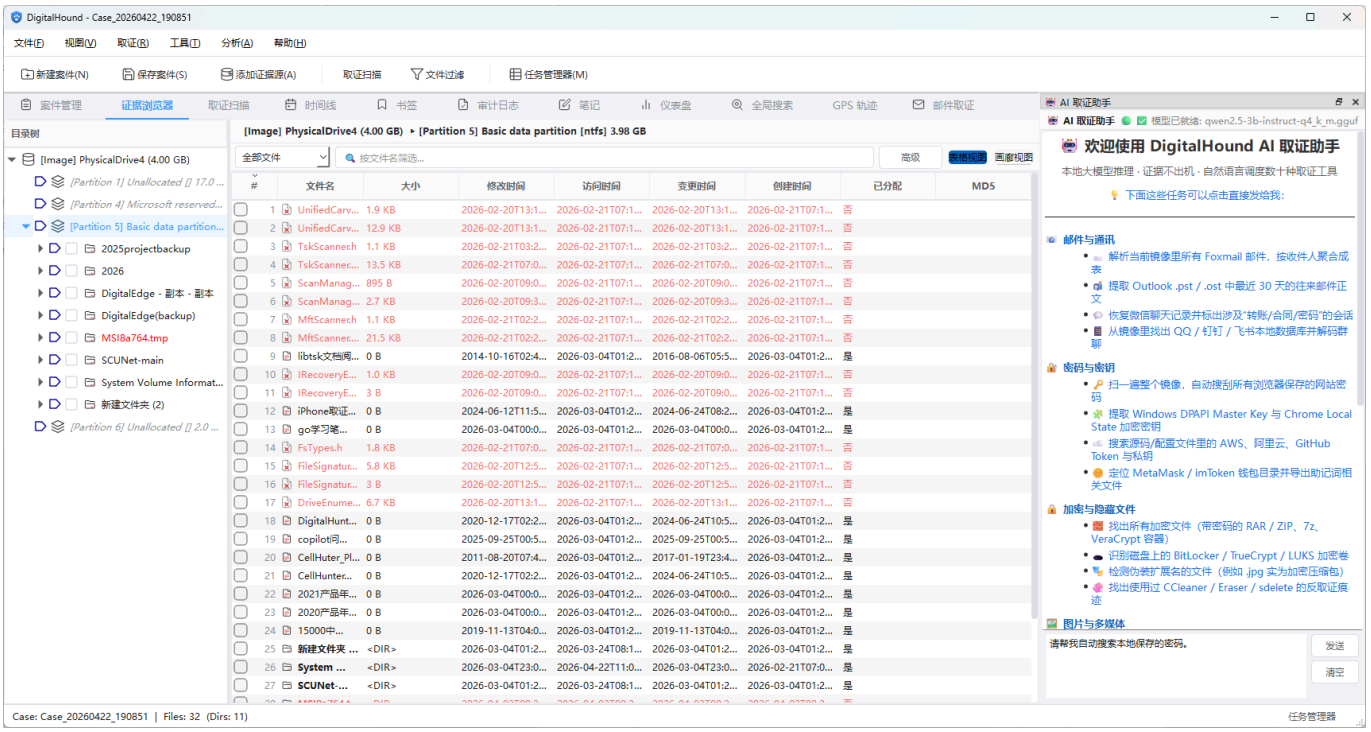
DigitalHound 是一款面向执法机关、企业安全团队与司法鉴定中心的新一代数字取证一体化平台。基于 SleuthKit 深度定制内核，原生支持 E01/DD/VHD 等主流镜像格式，内置 500+ 工件解析器，覆盖浏览器、即时通讯、邮件、注册表、事件日志、Prefetch、USN、跳转列表等全场景痕迹。 平台首创集成本地 AI 大模型——离线运行的取证助手可用自然语言对话式调查证据，20+ 类别的 AI 图像智能分类让海量图片筛查效率提升百倍。从磁盘镜像采集、写保护、关键字搜索、时间线关联分析，到微信/QQ 数据库解密、凭据采集、GPS 轨迹还原、报告导出，DigitalHound 以单机即可完成全流程取证。 中文原生 · 一键取证 · 全离线 · 可庭证。 🎯 功能卖点:

> 🧠 本地 AI 取证助手：离线大模型对话式调查。
> 🖼️ AI 图像智能分类：20+ 类别（武器/毒品/证件/车牌/CSAM 等）
> 💾 SleuthKit 深度定制内核：E01 / DD / VHD / RAW，支持孤立与已删除文件
> 🔐 写保护 + 实时响应采集：现场一键活检
> 🔑 凭据采集：19 种类型（浏览器/WiFi/SSH/DPAPI/KeePass/加密钱包等）
> 💬 即时通讯解密：微信/QQ 通过模拟登录获取密钥（无需内存扫描）
> 🌏 GPS 轨迹可视化：内嵌 Leaflet 地图 + KML 导出
> 🗓️ 时间线关联分析：自动聚类发现可疑时段
> 🗂️ 统一案件数据库：SQLite 存储，支持 TB 级证据
> 📑 多格式报告：HTML / PDF / CSV 一键导出
> 🌐 全离线 · 中文原生 · 无云依赖

> **姊妹产品**：`DigitalImager`（免费磁盘镜像制作工具，类似 FTK Imager）

⭐ 核心亮点

#	能力	说明
1	🔬 **工业级取证内核**	以源码方式深度集成 SleuthKit libtsk / libewf / libvhdi / libvmdk / libqcow / libpff，非 DLL 包装，可定制每一处细节
2	🧩 **70+ 工件解析器**	覆盖 Windows / macOS / Linux 三大系统的注册表、EVTX、浏览器、聊天、云盘、持久化等海量痕迹
3	🤖 **本地 AI 取证助手**	内置本地大模型推理（.gguf），自然语言调度取证工具，**证据不出机**
4	🕐 **时间线关联引擎**	跨模块聚合事件，支持 2 分钟窗口关联簇与异常活动段识别
5	🔐 **密钥与密文攻坚**	已规划 DPAPI 解密链、Telegram Desktop 离线解密、微信/QQ 模拟登录取密钥
6	🗄️ **SQLite 统一案件库**	对标 Autopsy / Magnet AXIOM，所有结果结构化入库，支持复查与二次分析
7	🌐 **多语言界面**	原生支持简体中文 / English / 日本語 / 한국어 四语言实时切换


DigitalHound - Case_20260422_190851
文件(F) 视图(V) 取证(R) 工具(T) 分析(A) 帮助(H)
新建案件(N) 保存案件(S) 添加证据源(A) 取证扫描 文件过滤 任务管理器(M)
案件管理 证据浏览器 取证扫描 时间线 书签 审计日志 笔记 仪表盘 全局搜索 GPS 轨迹 邮件取证
目录树
[Image] PhysicalDrive4 (4.00 GB)
[Partition 1] Unallocated [] 17.0 ...
[Partition 4] Microsoft reserved...
[Partition 5] Basic data partition...
2025projectbackup
2026
DigitalEdge - 副本 - 副本
DigitalEdge(backup)
MSI8a764.tmp
SCUNet-main
System Volume Informat...
新建文件夹 (2)
[Partition 6] Unallocated [] 2.0 ...
[Image] PhysicalDrive4 (4.00 GB) ▸ [Partition 5] Basic data partition [ntfs] 3.98 GB
全部文件
按文件名筛选...
高级
表格视图
画廊视图
文件名 大小 修改时间 访问时间 变更时间 创建时间 已分配 MD5
1 UnifiedCarv... 1.9 KB 2026-02-20T13:1... 2026-02-21T07:1... 2026-02-20T13:1... 2026-02-21T07:1... 否
2 UnifiedCarv... 12.9 KB 2026-02-20T13:1... 2026-02-21T07:1... 2026-02-20T13:1... 2026-02-21T07:1... 否
3 TskScanner.h 1.1 KB 2026-02-21T03:2... 2026-02-21T07:1... 2026-02-21T03:2... 2026-02-21T07:1... 否
4 TskScanner... 13.5 KB 2026-02-21T07:0... 2026-02-21T07:1... 2026-02-21T07:0... 2026-02-21T07:1... 否
5 ScanManag... 895 B 2026-02-20T09:0... 2026-02-21T07:1... 2026-02-20T09:0... 2026-02-21T07:1... 否
6 ScanManag... 2.7 KB 2026-02-20T09:3... 2026-02-21T07:1... 2026-02-20T09:3... 2026-02-21T07:1... 否
7 MftScanner.h 1.1 KB 2026-02-21T02:2... 2026-02-21T07:1... 2026-02-21T02:2... 2026-02-21T07:1... 否
8 MftScanner... 21.5 KB 2026-02-21T02:2... 2026-02-21T07:1... 2026-02-21T02:2... 2026-02-21T07:1... 否
9 libtsk文档阅... 0 B 2014-10-16T02:4... 2026-03-04T01:2... 2016-08-06T05:5... 2026-03-04T01:2... 是
10 IRecoveryE... 1.0 KB 2026-02-20T09:0... 2026-02-21T07:1... 2026-02-20T09:0... 2026-02-21T07:1... 否
11 IRecoveryE... 3 B 2026-02-20T09:0... 2026-02-21T07:1... 2026-02-20T09:0... 2026-02-21T07:1... 否
12 iPhone取证... 0 B 2024-06-12T11:5... 2026-03-04T01:2... 2024-06-24T08:2... 2026-03-04T01:2... 是
13 go学习笔... 0 B 2026-03-04T00:0... 2026-03-04T01:2... 2026-03-04T00:0... 2026-03-04T01:2... 是
14 FsTypes.h 1.8 KB 2026-02-21T07:0... 2026-02-21T07:1... 2026-02-21T07:0... 2026-02-21T07:1... 否
15 FileSignatur... 5.8 KB 2026-02-20T12:5... 2026-02-21T07:1... 2026-02-20T12:5... 2026-02-21T07:1... 否
16 FileSignatur... 3 B 2026-02-20T12:5... 2026-02-21T07:1... 2026-02-20T12:5... 2026-02-21T07:1... 否
17 DriveEnume... 6.7 KB 2026-02-20T13:1... 2026-02-21T07:1... 2026-02-20T13:1... 2026-02-21T07:1... 否
18 DigitalHunt... 0 B 2020-12-17T02:2... 2026-03-04T01:2... 2024-06-24T10:5... 2026-03-04T01:2... 是
19 copilot问... 0 B 2025-09-25T00:5... 2026-03-04T01:2... 2025-09-25T00:5... 2026-03-04T01:2... 是
20 CellHuter_Pl... 0 B 2011-08-20T07:4... 2026-03-04T01:2... 2017-01-19T23:4... 2026-03-04T01:2... 是
21 CellHunter... 0 B 2020-12-17T02:2... 2026-03-04T01:2... 2024-06-24T10:5... 2026-03-04T01:2... 是
22 2021产品年... 0 B 2026-03-04T00:0... 2026-03-04T01:2... 2026-03-04T00:0... 2026-03-04T01:2... 是
23 2020产品年... 0 B 2026-03-04T00:0... 2026-03-04T01:2... 2026-03-04T00:0... 2026-03-04T01:2... 是
24 15000中... 0 B 2019-11-13T04:0... 2026-03-04T01:2... 2019-11-13T04:0... 2026-03-04T01:2... 是
25 新建文件夹 ... <DIR> 2026-03-04T01:2... 2026-03-24T08:1... 2026-03-04T01:2... 2026-03-04T01:2... 是
26 System ... <DIR> 2026-03-04T23:0... 2026-04-22T11:0... 2026-03-04T23:0... 2026-02-21T07:0... 是
27 SCUNet-... <DIR> 2026-03-04T01:2... 2026-03-24T08:1... 2026-03-04T01:2... 2026-03-04T01:2... 是
Case: Case_20260422_190851 | Files: 32 (Dirs: 11)
任务管理器
AI 取证助手
AI 取证助手 模型已就绪: qwen2.5-3b-instruct-q4_k_m.gguf
欢迎使用 DigitalHound AI 取证助手
本地大模型推理 · 证据不出机 · 自然语言调度数十种取证工具
下面这些任务可以点击直接发给我:
邮件与通讯
解析当前镜像里所有 Foxmail 邮件，按收件人聚合成表
提取 Outlook .pst / .ost 中最近 30 天的往来邮件正文
恢复微信聊天记录并标出涉及"转账/合同/密码"的会话
从镜像里找出 QQ / 钉钉 / 飞书本地数据库并解码群聊
密码与密钥
扫一遍整个镜像，自动搜刮所有浏览器保存的网站密码
提取 Windows DPAPI Master Key 与 Chrome Local State 加密密钥
搜索源码/配置文件里的 AWS、阿里云、GitHub Token 与私钥
定位 MetaMask / imToken 钱包目录并导出助记词相关文件
加密与隐藏文件
找出所有加密文件（带密码的 RAR / ZIP、7z、VeraCrypt 容器）
识别磁盘上的 BitLocker / TrueCrypt / LUKS 加密卷
检测伪装扩展名的文件（例如 .jpg 实为加密压缩包）
找出使用过 CCleaner / Eraser / sdelete 的反取证痕迹
图片与多媒体
请帮我自动搜索本地保存的密码。
发送
清空

🧩 工件解析矩阵（480+ 解析器 · 节选）

💼 系统与执行痕迹

- Prefetch 执行历史 · BAM/DAM 后台活动 · AppCompatFlags

- Jump List · RecentDocs · ShellBag · LNK 快捷方式
- IconCache · RecentFileCache · UserAssist · UWP/AppX 清单
- Run MRU · TypedPaths · OpenSaveMRU · WordWheelQuery

🌐 浏览器与网络

- Chrome / Edge / Firefox 历史、下载、书签、Cookie、登录凭据
- TypedURLs · Zone.Identifier(ADS) · 浏览器扩展
- hosts 文件分析 · DNS 客户端日志 · pfirewall.log

💬 通讯与聊天

- Foxmail / Outlook (.pst/.ost) 邮件解析
- 微信 / QQ / 钉钉 / 飞书本地数据库定位
- Telegram Desktop · Discord · Signal · Skype · Teams

☁️ 云盘与远程

- OneDrive · Dropbox · Google Drive 同步元数据
- TeamViewer · AnyDesk · RDP 连接历史与缓存
- VPN 配置（OpenVPN / WireGuard）

🔐 安全与认证

- DPAPI Master Key · Chrome Local State 加密密钥
- Windows 凭据管理器保险柜（.vcrd / Policy.vpol）
- BitLocker 恢复密钥 · WiFi 明文密钥
- SSH known_hosts / authorized_keys / config

🛡 威胁与反取证

- Windows Defender 威胁检测（MPLog / DetectionHistory / 隔离区 / 排除项）
- WMI EventSubscription 持久化检测 · COM 对象劫持
- 日志清除事件检测（Security 1102 / System 104）
- 反取证工具识别（CCleaner / Eraser / sdelete 等）
- 勒索软件指标（勒索信 + 加密扩展名家族识别）

🖼 多媒体与文档

- EXIF 元数据（含 GPS 聚合、地图可视化）
- Thumbnail Cache · Thumbs.db 缩略图
- PE 文件分析（节/导入/导出/签名/版本信息）
- PDF / OOXML / OLE2 文档元数据

📋 事件日志与时间线

- EVTX 全盘扫描 · 按通道/级别/事件 ID 聚合
- System.evtx 关键取证事件（7045 服务安装、1074 关机、104 日志清除）
- Application.evtx 崩溃/挂起（1000/1001/1002）
- Task Scheduler · BITS · Windows Update · PowerShell Transcripts

- **时间线关联引擎**：2 分钟窗口聚合 + ≥15 事件/分钟异常段识别

🗑️ 删除与隐藏

- 回收站（$I/$R）恢复 · USN 变更日志解析
- 文件签名异常扫描（扩展名与真实类型不匹配）
- 高熵文件扫描（≥7.99 疑似加密/勒索）
- 加密压缩包识别（ZIP / RAR / 7z）
- 重复文件检测（按哈希聚合，显示浪费空间）

🤖 AI 取证助手

> **核心理念：证据不出机，本地大模型完成研判**

- ✅ **本地推理**：基于 llama.cpp，加载 `.gguf` 模型，全程离线
- ✅ **自然语言调度**：调查员说“找出所有加密压缩包”，AI 自动调用对应解析器
- ✅ **结构化回答**：AI 把原始数据转换为带时间线、标红可疑项的分析报告
- ✅ **可扩展工具集**：通过 `ForensicAiEngine` 注册任意 C++ 工具，让 AI 调用

六大场景示例

分类	示例问题
📧 邮件与通讯	"恢复微信聊天记录并标出涉及转账/合同/密码的会话"
🔐 密码与密钥	"扫一遍整个镜像，自动搜刮所有浏览器保存的网站密码"
🔒 加密与隐藏	"找出所有加密文件（带密码的 RAR / ZIP、7z、VeraCrypt 容器）"
🖼️ 图片与多媒体	"用本地 AI 模型在所有图片中筛出涉黄/涉暴图像并生成清单"
🌐 浏览器与云	"找出访问过的暗网域名（.onion）与可疑交易平台"
🧰 系统线索	"把上述所有痕迹按时间排序，生成一条可导出的案件时间线"

📄 取证报告

- **CSV 分析报告** · 按分类导出记录
- **HTML 交互报告** · 可在浏览器打开、打印、分享
- **PDF 司法级报告** · 含案件概览、证据源、工件记录、书签摘要
- **综合案件报告** · 整合所有扫描结果的汇总文档
- **镜像完整性校验** · MD5/SHA1/SHA256 三重哈希 + 耗时统计

书签系统支持 4 级标签：🔴 **关键证据** / 🟡 **待确认** / 🟢 **已核实** / 🟣 **参考**。

🌍 多语言与国际化

语言	状态
CN 简体中文	✅ 完整翻译（1530 条）

语言	状态
us English	✅ 原生源语言

🔭 其他产品

- 🚧 **DHKeyAcquisition**：模拟 QQ / 微信登录从腾讯服务器获取密钥
- 🚧 **DPAPI 解密链**：打通 Chrome / Edge 密码与 Cookie 的完整解密链路
- 🚧 **Telegram Desktop 离线解密**
- 🚧 **AI 涉黄涉暴图像识别**（本地多模态模型）
- 🚧 **HiSuite USB 协议分析**

💻 技术规格

项	规格
镜像格式	RAW / DD / E01 / Ex01 / VHD / VHDX / VMDK / QCOW / AFF4
文件系统	NTFS / FAT12/16/32 / exFAT / HFS+ / APFS / ext2/3/4 / YAFFS2 / ISO9660
数据库	SQLite（案件库） · ESE（解析 Windows.edb / WebCache / Mail）
AI 推理	llama.cpp · GGUF 本地模型 · OpenAI 兼容 API
部署	免安装便携版 · Windows 10/11 x64

🎁 适用人群

- 🏛️ **公安刑侦 / 网安** — 电子数据勘验、固定证据、庭审材料
- ⚖️ **司法鉴定机构** — 独立第三方电子证据鉴定
- 🏢 **企业内部调查** — 离职审计、知识产权保护、数据泄露溯源
- 🛡️ **应急响应团队** — 勒索软件、APT 入侵、取证即响应
- 🎓 **安全研究与教学** — 可审计的开源级取证平台

DigitalHound · 让每一字节都无处遁形

自研内核 · 本地 AI · 司法级报告 · 开箱即用