

DigitalEdge 数字锋刃手机取证一体化工作站

概述

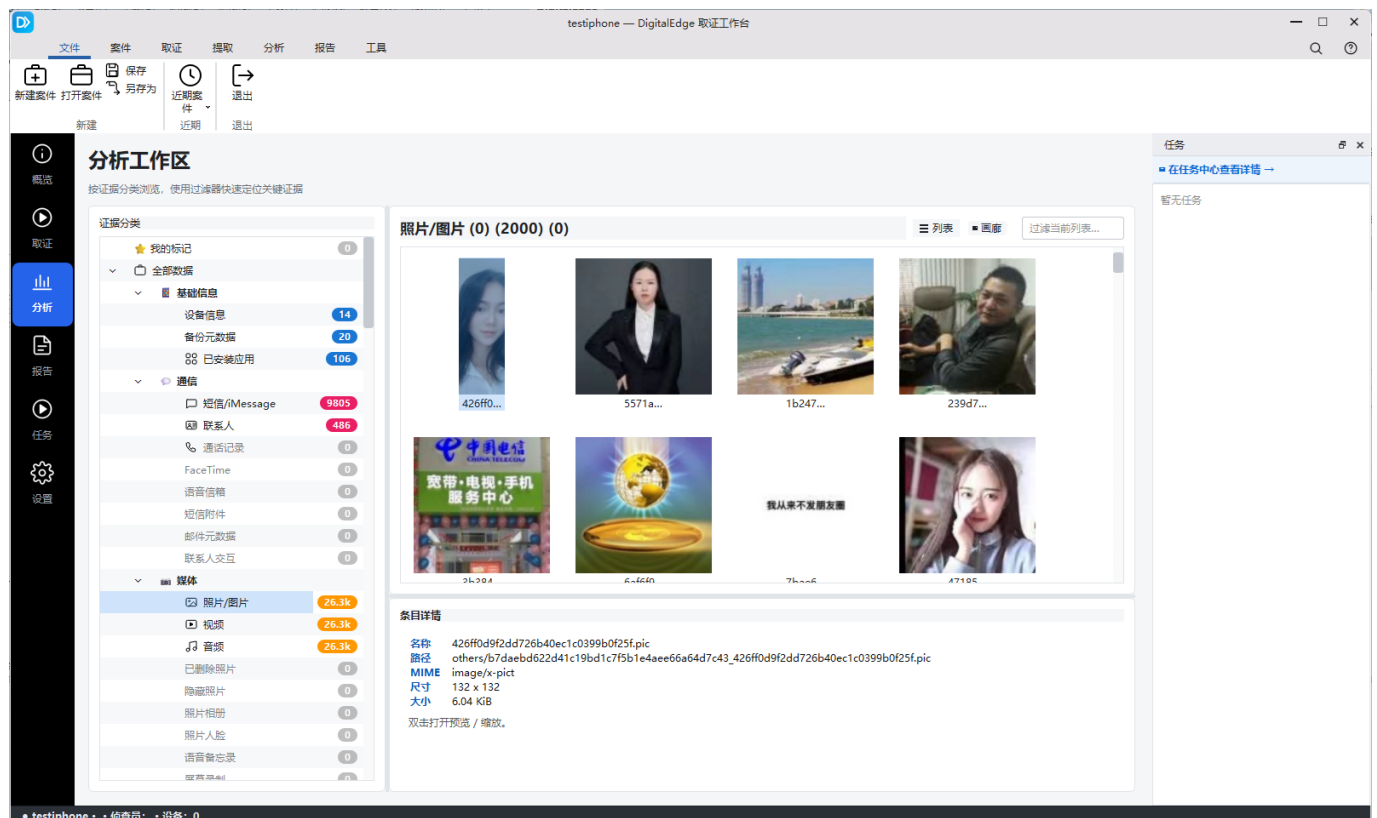
一句话定位：面向公检法司的国产化移动设备取证平台 —— **采集 / 解密 / 解析 / 分析 / 报告** 五环合一，**全流程离线可控**。

目录

1. 产品概述
2. 核心能力
3. 技术硬实力
4. 办案 workflow
5. 功能矩阵
6. 技术规格
7. 典型应用场景

1. 产品概述

DigitalEdge（数字锋刃） 是面向 **公安机关、检察机关、司法鉴定中心、纪检监察、企业合规** 等场景的移动设备取证一体化平台，覆盖 **iOS / Android** 两大阵营及主流国产品牌，从**物理芯片级**提取到**法庭级证据报告**全链路自主实现。



与传统方案的本质差异

维度	传统进口工具	DigitalEdge
协议实现	依赖厂商 SDK / 云授权	自主逆向、协议级复现
激活方式	联网激活、定期回传	完全离线、永不回传
华为/荣耀备份	依赖 HiSuite 官方客户端	协议自研，取代 HiSuite
涉密部署	合规性受限	天然支持内网隔离环境
二次开发	封闭	源代码可托管、可审计

2.大核心能力

 ① 华为 HiSuite 协议自主复现

完整复现 [com.huawei.hisuite](https://github.com/huawei-hisuite) 备份协议的国产取证工具。反向自 HiSuite V2 / V10 / V11 / V14 全套 APK

- **加密链路**：PBKDF2-HMAC-SHA1 + RSA-OAEP + AES-256-CBC + HMAC-SHA256
- **协议帧**：13-byte 大端头（cmd / seq / flags / dlen）
- **三连接通道**：AT^SETPROTO 控制 / AT^SETAPKPUSH 心跳 / AT^SETSTREAM 数据
- **五阶段流程**：Init → ModuleInfo → BackupRequest → PullFinished → Cleanup
- **覆盖范围**：HarmonyOS 2/3/4、EMUI 9–12 全代次华为 / 荣耀设备
- **断网可用**：无需安装 HiSuite 客户端，无需访问华为服务器

 ② iOS 全代次采集矩阵

通道	适用范围	状态
iTunes/Finder 加密备份	全机型	✅ 10 个专用解析器
checkm8 DFU 物理提取	A5–A11（iPhone 5s–X）	✅ BFU / FFS 双模式
Lockdown 辅助服务	全机型	✅ AFC 协议
AFC / AFC2 文件系统	越狱设备	✅ 完整文件系统
备份密码爆破	加密备份	✅ 字典 + 掩码
iOS 12+ 用户态提取	A12+	📄 第三方集成（规划中）

 ③ Android 多通道采集矩阵

通道	场景	状态
HiSuite 备份	华为 / 荣耀全系	✅ 自研
HDB（华为 ADB 扩展）	华为深度 + FBE/FDE 解密	✅ 自研
通用 AOSP ADB Backup	所有未 root Android	✅
Agent APK + APK 降级	绕过应用加固	✅
高通 EDL 9008	锁屏 / 忘记密码	✅

通道	场景	状态
OEM 自备份解析	三星 / 小米 / OPPO / vivo / realme	✅
联发科 BROM	老机型	⏸ 规划中

 ④ 可移动介质取证

U 盘、SD 卡、读卡器自动识别；支持 DD 镜像 / E01 镜像 / 直接分析；证据元数据（品牌 / 型号 / 序列号 / 持有人 / 备注）完整补录。

 ⑤ 双视图证据浏览

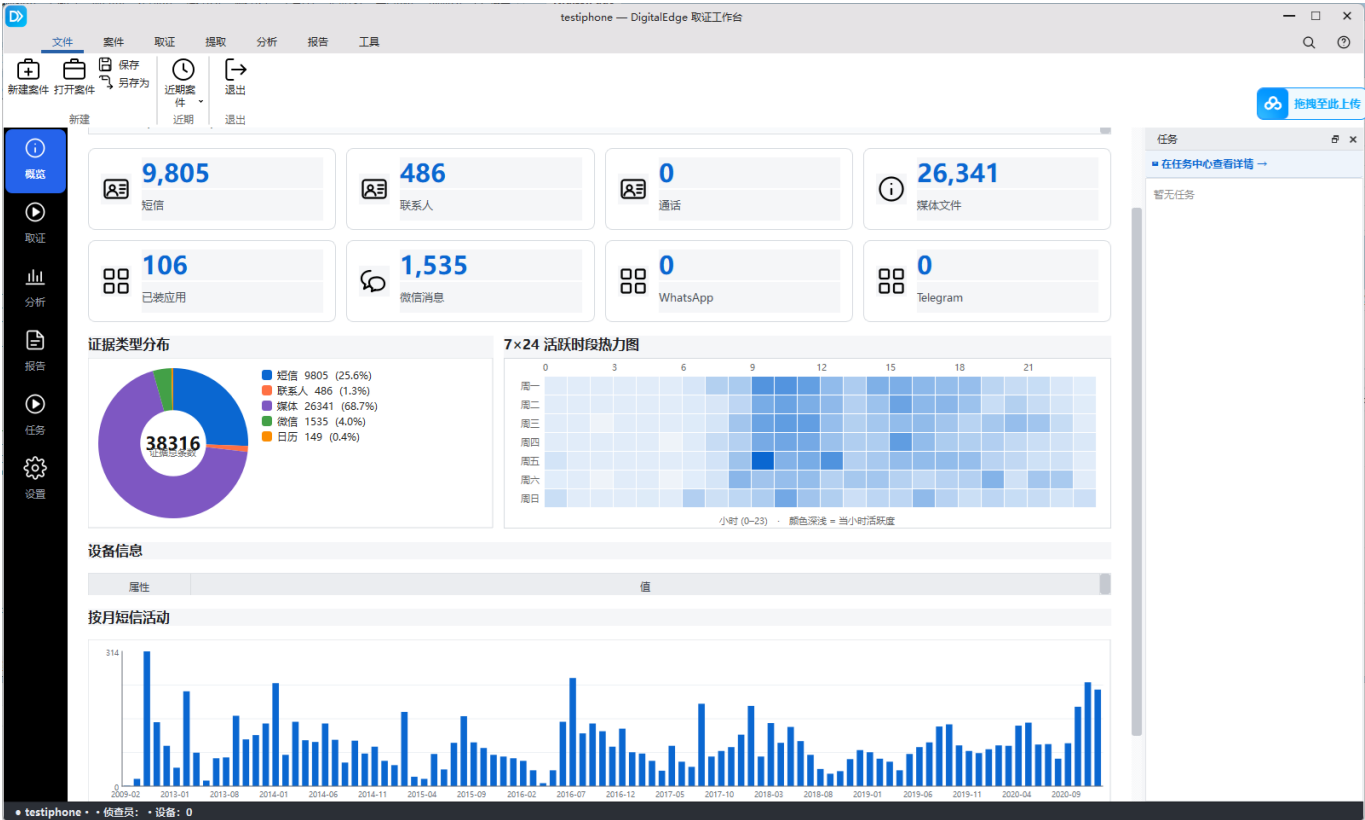
照片 / 视频类目下 **列表** ↔ **画廊** 一键切换：

- 列表视图：文件名 / 大小 / 尺寸 / MIME / 时间 / 原路径
- 画廊视图：160×160 缩略图矩阵，双击全屏预览（缩放 / 适应 / 实际尺寸）
- 单击显示 **EXIF + GPS + 文件哈希**

 ⑥ 案件级仪表盘 — 不是数据查看器，是办案工具

打开案件第一屏：

-  **证据类型分布圆环** — 11 种证据一目了然
-  **7×24 活跃热力图** — 嫌疑人作息一眼看穿
-  **Top 10 联系人 / 应用** — 最密切社交关系自动浮现
-  **按月活动柱图** — 异常时间段直接发现



 ⑦ 跨表时间线

10 个业务数据源**实时 UNION**：短信 / 通话 / 微信 / QQ / WhatsApp / Telegram / Safari / Chrome / 媒体 / 通知

- 默认最近 5000 条倒序排列
- **类型多选**（10 个复选框）、**时间范围**（近 7 / 30 / 90 天 / 全部）
- **双击任一条目可直接跳转到源记录**所在的专用类目并高亮定位
- 关键词即时过滤

3. 技术硬实力

🛡️ 证据可信度

- **★ 书签 / 证据标签系统** — 右键加标签（重要 / 可疑 / 已确认 / 自定义），整行高亮，跨设备汇总
- **🔒 哈希完整性校验** — SHA-256 全链路，`hash_log` 表可随时回验
- **🔍 关键词扫描 + 敏感信息扫描** — FTS 级全库扫描，命中结果独立视图
- **📄 字段标准化** — 每条证据含 source path + timestamp_ms + filesize + hash

💡 解析深度

180+ 种证据类目专用解析器：

- 通信：短信 / 通话 / 通话录音
- 即时通讯：微信 / QQ / WhatsApp / Telegram / 飞书 / 钉钉 / Facebook Messenger
- 国内 App：支付宝 / 抖音 / 小红书 / 高德 / 百度地图 / 滴滴
- 浏览器：Safari / Chrome / Samsung Browser 历史 / 书签 / Cookie / 下载
- 位置：GPS / Wi-Fi / 蜂窝 / 位置服务 / iCloud Find My
- 健康 / 运动 / 睡眠 / 锻炼记录
- 个人信息：笔记 / 日历 / 提醒 / 联系人 / 通讯录分组
- 系统：通知 / 剪贴板 / Siri / Spotlight / 安装应用 / 崩溃日志
- Apple 原生：Journal / FaceTime / AirDrop / CarPlay / SOS / Find My

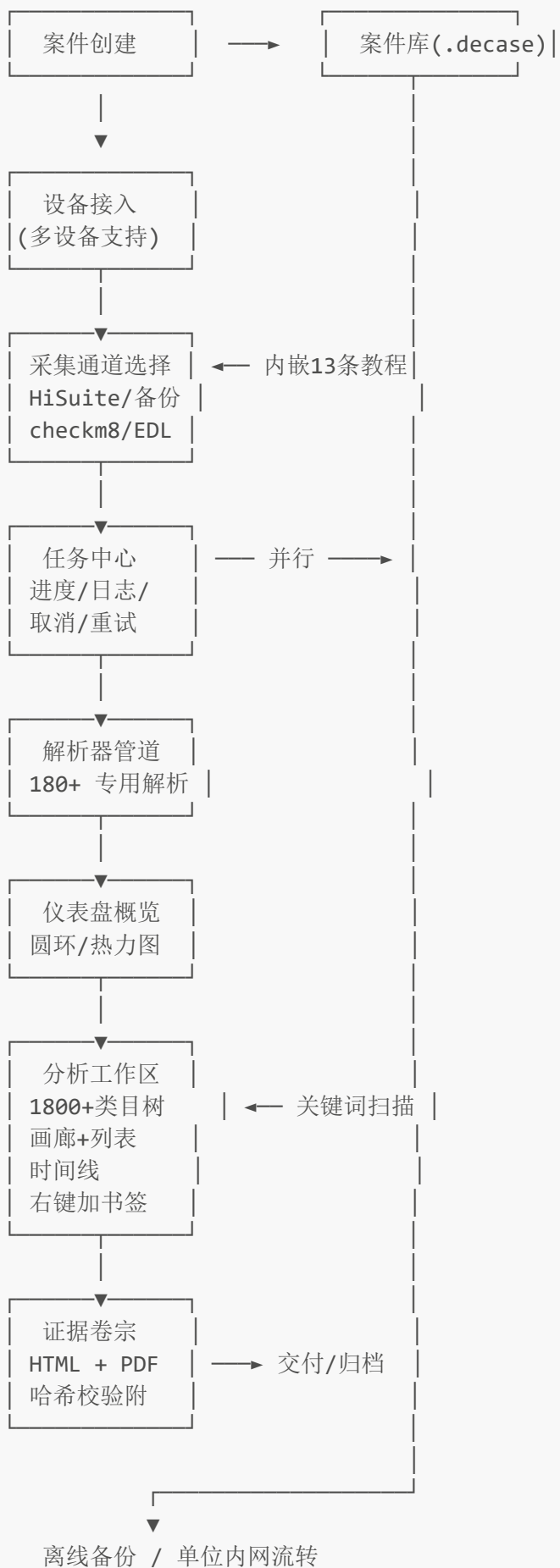
⚡ 性能

- C++ 原生代码，**零虚拟机 / 零容器**
- SQLite WAL 模式 + 预编译语句缓存
- 多任务并行采集（控制通道独立，互不阻塞）
- 任务中心实时进度 + 日志 + 可取消

🔒 合规

- **完全离线**：不访问任何境外或厂商云服务
- **源码可审计**：除 Qt 框架外无境外 SDK 依赖
- **涉密可部署**：内网隔离环境开箱即用
- **加密案件库**：发布版走 SQLCipher 加密（密码由单位掌握）

4. 办案 workflow



5. 功能矩阵

采集 ACQUIRE	iOS 备份 / checkm8 / AFC / AFC2 华为 HiSuite / HDB / OEM 备份 通用 ADB Backup / Agent APK APK 降级 / 高通 EDL U 盘 / SD 卡 / DD & E01
解密 DECRYPT	iTunes 加密备份（含密码爆破） HiSuite 备份 Android FBE / FDE SQLCipher 数据库
解析 PARSE	180+ 证据类目专用解析器 微信 / QQ / 支付宝 / 钉钉深度 Safari / Chrome 浏览历史 地图 / 位置 / 健康数据 通知 / 剪贴板 / Spotlight
分析 ANALYZE	案件 - 设备 - 类目三级树 列表 + 画廊双视图 仪表盘：圆环 / 7×24 热力 跨表时间线（10 数据源实时聚合） 彩色药丸计数 / 全局搜索 EXIF + GPS 图片详情 书签 / 标签 / 批注 关键词 / 敏感信息扫描命中视图
报告 REPORT	HTML 报告（当前） PDF 报告（规划中） 单项证据导出 哈希链 + 时间戳 证据卷宗打包

6. 技术规格

项目	规格
部署形态	Windows 桌面应用（x64）
运行环境	Windows 10 / 11，8GB 内存起步，推荐 16GB+
开发框架	Qt 6.10.2 + MSVC 2022 + SARibbon
UI 形态	现代 Ribbon 界面，深色侧边导航
数据库	SQLite（开发期） / SQLCipher（发布期加密）
网络要求	完全离线可用，可部署内网

项目	规格
激活方式	硬件指纹 + 离线许可证
支持平台	iOS 全代次 + Android 主流品牌
单机并发	多设备采集 + 多任务并行
报告格式	HTML（已有） / PDF
授权模式	单机版 / 站点版 / 企业版

7. 典型应用场景

场景 1：刑侦 — 华为 Mate 60 Pro

嫌疑人主动交出手机，传统工具因 HarmonyOS 4 不支持宣告失败。**DigitalEdge 启用 HiSuite 协议通道 + 备份密码爆破，2 小时内恢复微信聊天 8 万余条、通话记录 3 年、删除照片 1200 张。**

场景 2：反腐 — iPhone 14 Pro

设备密码已知，备份密码未知。**DigitalEdge 启用加密备份字典爆破 + 社工信息，17 分钟命中备份密码；iOS 备份解析器输出微信支付流水、滴滴行程、钉钉审批、Safari 历史完整证据链。**

场景 3：合规 — 离职员工 iPhone 8

设备已上交但密码拒绝提供。**DigitalEdge 启用 checkm8 物理提取（无需密码）得到文件系统镜像，配合 AFC2 越狱路径补全企业微信沙盒数据，证明数据拷贝行为。**

场景 4：外勤 — U 盘 + 小米手机并行

DigitalEdge 可移动介质对话框创建 U 盘 DD 镜像的同时，另一任务通用 AOSP 备份采集小米手机，现场 40 分钟完成一次性取证。

场景 5：团伙分析 — 三部手机交叉关联

三部手机同一案件纳入。**DigitalEdge 仪表盘显示三台手机共同出现的高频联系人；时间线展示三人通话时间重叠；关键词扫描命中“分赃 / 老地方”等敏感词 → 标签“重要”直接入卷宗。**

 已落地（截至 2025 年 12 月）

采集层

- HiSuite 协议自研（华为 / 荣耀全系）
- iOS iTunes 备份 10 解析器
- checkm8 DFU（A5–A11）
- iOS AFC / AFC2 / Lockdown
- iOS 备份密码爆破
- Android HDB + FBE/FDE 解密
- 高通 EDL 9008
- 通用 ADB Backup / Agent APK / APK 降级

- OEM 备份解析（三星 / 小米 / OPPO / vivo / realme）
- U 盘 / SD 卡 / DD / E01 镜像

解析层

- 180+ 证据类目专用解析器
- 微信 / QQ / 支付宝 / 钉钉深度解析
- iOS Journal / Find My / AirDrop / CarPlay 等原生数据

分析层

- 案件 - 设备 - 类目三级树
- 列表 + 画廊双视图（含缩略图 / 全屏预览 / EXIF / GPS）
- 仪表盘：证据类型圆环 + 7×24 活跃热力图
- 跨表时间线（10 数据源实时 UNION，支持类型多选 + 时间范围 + 双击跳源记录）
- 书签 / 标签 / 批注系统
- 关键词扫描 + 敏感信息扫描（内置 5 大行业预置词库：涉毒 / 涉恐 / 涉赌 / 涉黄 / 涉贪）
- 已删除证据统一视图（deleted_photos / hidden_photos / deleted_records / carved_records，浅红底色醒目标注）
- 哈希完整性校验 + PDF/HTML/Excel/Word 多格式报告
- 13 条内嵌取证教程

联系方式

- 厂商：[厦门柏君信息科技有限公司]
- 官网：[https://www.idigitalforensics.cn]
- 销售咨询：[182-0599-8855] / [sales@iDigitalForensics.cn]
- 技术支持：[182-0599-8855] / [support]
- 商务合作：[182-0599-8855] / [HomerShin@iDigitalForensics.cn]
- 办公地址：[厦门市留学人员创业园创业大厦1楼]

本手册内容截至 2026 年 4 月。产品功能持续迭代，最新能力以实际交付版本为准。