

智能与效率

电子数据取证技术在AI时代的新发展

弘连网络 曹长健



目录

01.

公司简介



02.

阶段成果



03.

持续推进





核心产品

数据哨兵远程计算机调查平台 (ZY600)

证易数据哨兵是一款对企业内部计算机进行**事前预防、事中监控、事后调查取证**的专业电子数据调查平台，适用于内部审计、法律合规、风险管理、人力资源、内部控制等部门进行**内部监察与反舞弊工作使用**。

平台在不影响目标计算机工作的前提下，根据调查分析需求，**支持查看目标计算机的使用痕迹、浏览器记录、即时通讯记录、文件操作记录、密码 / 密钥等信息，并支持桌面监控和策略监控。**

核心功能

- 事前预防** • 实时桌面监控 • 离线假屏监控 • 文件操作行为监控 • 邮件收发行为监控
- 事中监控** • 定时监控策略 • 定时计算机快照 • 定时内存快照 • 违规行为预警
- 事后调查取证** • 索引快照对比 • 应用数据分析 • 文件内容搜索 • 文件溯源

应用场景

商业秘密泄露

技术资料、软件代码、专利、客户信息、营销方案等商业秘密泄露事件调查。

反舞弊反欺诈

内部腐败、资产挪用、财务报表造假、逃税逃汇等舞弊行为。

违规行为

合规调查、内部投诉核实调查。

保密评估

员工及管理层在职/离职审查、保密核查。

平台亮点

1 客户端隐蔽

远程静默推送安装,高效内存调用,不影响目标计算机正常工作,调查完成后自动卸载。

3 调查迅速

B/S架构,无需调查员安装任何工具,提供快照、全量分析等多种方案选择。

2 专业合规

按照取证执法部门标准严格要求设计开发,全量操作日志记录保存,业内领先电子数据取证技术支撑。

4 快捷部署

单域控、多域控、跨网络、异地网络环境均可快速部署,具有专业数据备份容灾机制。



核心产品--弘连电子数据存证平台



弘连电子数据存证平台是一款采用分布式存储技术、基于加密证书数字签名和可信时间戳，面向政府行业建设的**在线电子数据取证、存证、出证**服务平台。

平台现提供**在线存证、浏览器存证、云手机存证**三种存证方式，覆盖99%以上的网页存证场景以及80%以上手机页面存证场景。平台支持包含部门管理、用户管理、取证文书生成等各类业务功能。

平台遵循司法部《**电子数据存证技术规范**》（SF/T 0076-2020）要求，同时获得《**信息安全技术网络安全等级保护 基本要求**》（GB/T 22239-2019）等保认证。确保平台在存证流程规范性、数据安全性上都达到行业领先水平。

自2022年上线以来，平台为广大用户有效地解决了各类场景下的“**自证难题**”，显著提升了电子证据证明力，强化公信力。



在线存证



浏览器存证



云手机存证



存证规范



等保认证

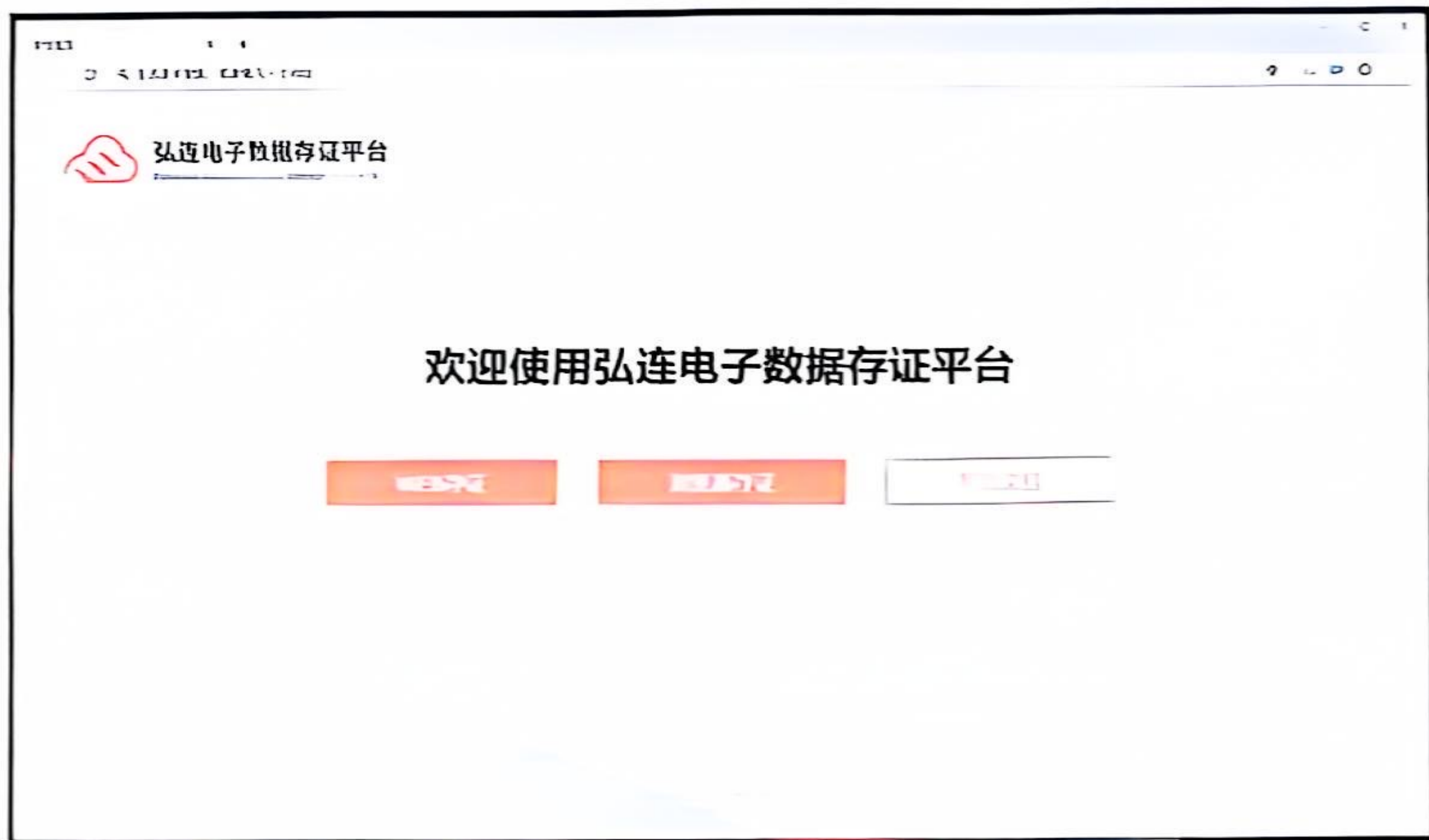
浏览器存证



弘连网络
FORENSIX.CN



证易科技



专业存证浏览器，提供录像、
代理等多种功能

存证浏览器



自动识别当前网页标题和地址，
一键快速存证，自动检测本地
环境

自动检测识别



满足99%网页存证场景，例如：
部分需要账号登录的页面等

所见即所得

传统数据分析方式的局限

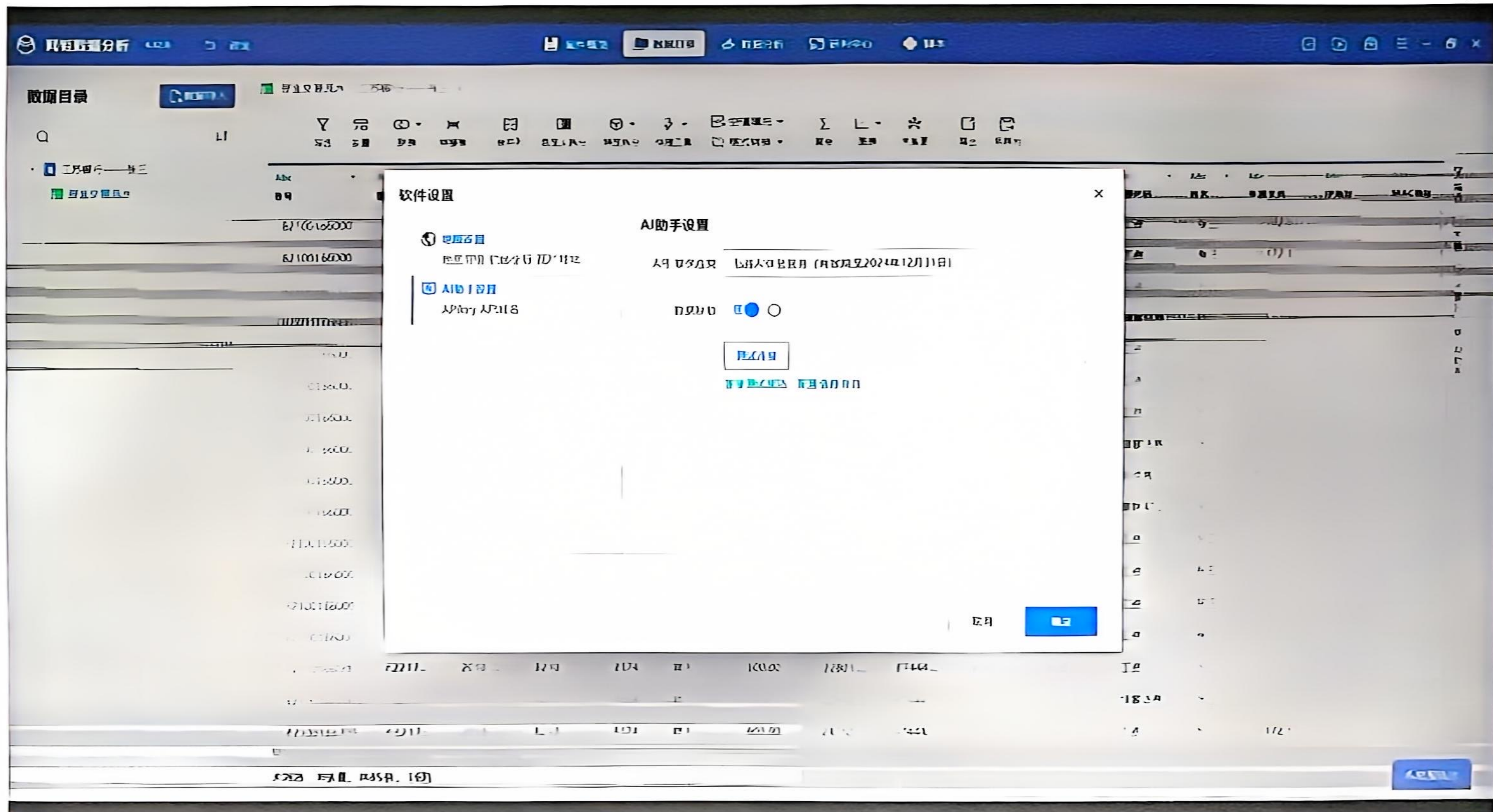
1. **分析维度受限**: 预设的模型和功能限制了分析的灵活性和深度。
2. **扩展性不足**: 数据量增长往往导致成本线性上升。
3. **使用门槛高**: 复杂的界面和专业术语对非技术用户不友好。
4. **人工效率低**: 人工审查大量数据耗时耗力, 容易出错。

大模型在取证数据分析中的挑战

1. **数据隐私保护**: 本地模型性能有限, 在线模型存在数据安全隐患。
2. **上下文限制**: 上下文窗口限制了有效信息的传递和处理。
3. **计算准确性**: 无法保证复杂计算结果的绝对准确性。

1. AI助手设置

网钜AI数据分析的实践





证易科技

12

网钜AI数据分析的实践



弘连网络
FORENSIX.CN



证易科技

账号	户名	交易日期	凭证代码	交易日期	出入账科目	交易金额	交易金额	交易余额	期末余额
821...	622176...	2003-0...	8210	8174	存入	600.00	600.00	87444...	0.00
821...	622176...	2003-0...	8210	8174	存入	600.00	1200.00	87444...	0.00
821...	622176...	2003-0...	8210	8174	存入	600.00	1800.00	87444...	82100...
821...	622176...	2003-0...	8210	8664	存入	0.87	1800.87	87444...	...
821...	622176...	2003-0...	8210	8174	存入	600.00	2400.87	87444...	0.00
821...	622176...	2003-1...	8210	8174	存入	600.00	2000.87	87444...	0.00
821...	622176...	2003-1...	8210	8174	存入	600.00	2600.87	87444...	0.00
821...	622176...	2003-1...	8210	8664	存入	2.71	2602.26	87444...	0.00
821...	622176...	2003-1...	8601	7702	转出	2.00	1101.26	87444...	0.00
821...	622176...	2003-1...	8601	7702	转出	2000.00	1102.26	87444...	0.00
821...	622176...	2010-0...	8210	8174	存入	600.00	1701.26	87444...	0.00
821...	622176...	2010-0...	8210	8174	存入	600.00	2201.26	87444...	0.00
821...	622176...	2010-0...	8210	8174	存入	16000.00	16201.26	87444...	0.00
821...	622176...	2010-0...	8210	8174	存入	7000.00	22201.26	87444...	0.00
821...	622176...	2010-0...	8210	8174	存入	600.00	22801.26	87444...	0.00
821...	622176...	2010-0...	8210	8664	存入	10.87	22812.22	87444...	0.00
821...	622176...	2010-0...	8210	8174	存入	600.00	24712.22	87444...	0.00

大模型驱动的数据分析优势

- 灵活多维度分析

帮助用户完成低智力高算力的重复性工作。

- 智能任务拆解

AI能自动将复杂查询拆分为可执行步骤。

- 自然语言交互

通过对话方式执行指令，大幅降低使用门槛。



传统APK分析的三大挑战

1、技术门槛持续攀升

- 简单的网络抓包难以获取核心服务器信息
- 分析重心向代码层面深度转移
- 专业的源码解读能力难以快速掌握

2、反取证技术不断升级

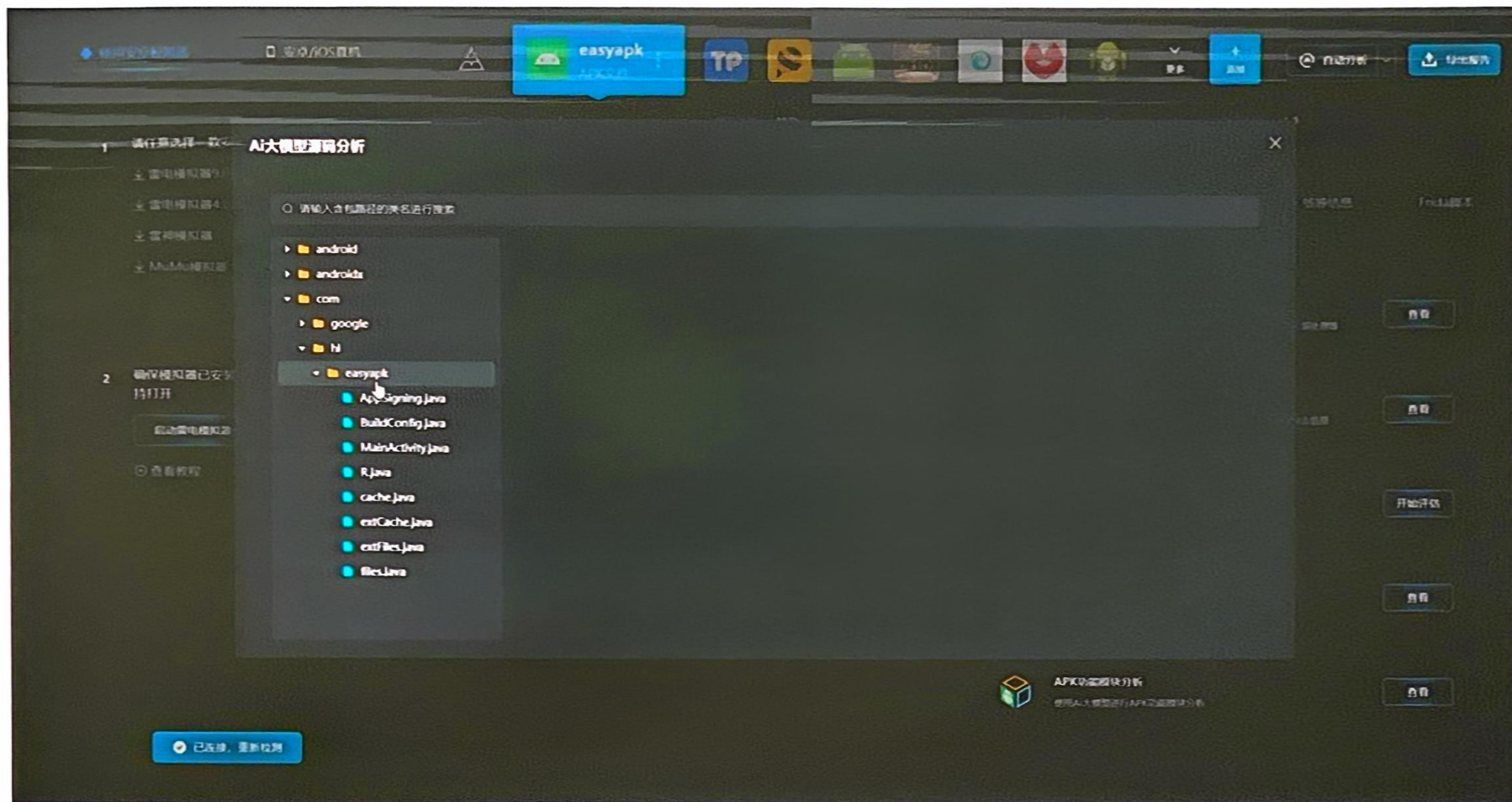
- 恶意应用普遍采用代码混淆
- 大量使用字符串加密技术
- 引入冗余代码干扰分析
- 人工梳理逻辑耗时巨大、效率低下

3、证据获取难度加大

- 代码上下文关联难以快速理解，关键逻辑难以识别
- 关键线索往往被巧妙隐藏



代码分析



传统图片分析的痛点

➤ 海量数据处理：

随着数字化的飞速发展，电子数据呈指数级增长。办案人员面临着处理和分析庞大数据量的挑战，这是一项极其耗时且复杂的任务。

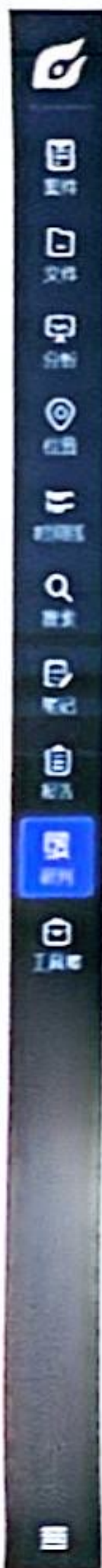
➤ 人工筛选效率低：

传统图片分析严重依赖人工筛选。大量图片需逐一查看，不仅耗时长，还容易造成分析人员疲劳，降低工作效率和准确性，尤其在复杂案件中更为明显。

➤ 隐藏信息易遗漏：

图片中往往包含复杂的隐藏信息。仅凭人工查看，很容易忽视这些潜在的关键线索，导致重要证据的遗漏，影响案件的全面分析。

AI赋能图片智能搜索



系统管理

图片分析

搜索 分享 打印 删除 刷新

全部

图片搜索

输入图片描述或图片中的文字

人脸

查看全部 >



证件/文本图片



截图/拍摄图片



其它



图片分类：采用深度学习算法，能够自动对图片进行快速分类。

AI赋能图片智能搜索

通过融合AI技术，火眼成功解决了传统图片分析中的诸多痛点。这不仅大幅提升了取证效率，更让分析人员能够将精力集中于案件的关键环节。

单机AI服务

