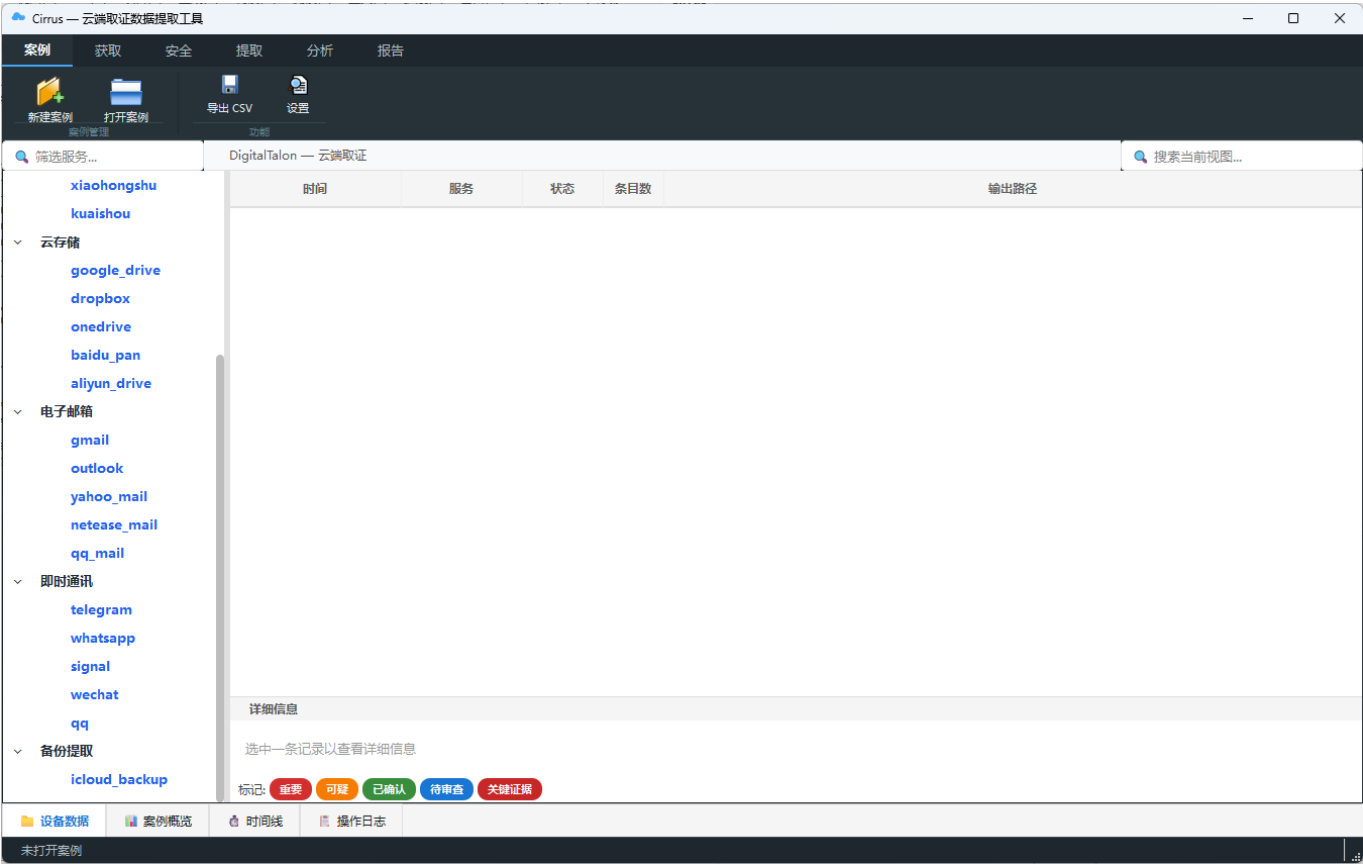


Cirrus — 云端取证数据提取平台

功能概述与技术优势

一、产品定位

Cirrus（卷积云取证）是一款面向电子数据取证场景的**云端数据提取与分析平台**，支持 GUI 与 CLI 双模式运行。平台覆盖社交媒体、云存储、电子邮箱、即时通讯、设备备份等五大类共 **26 个云服务**的数据提取，同时提供完整的证据链保全、时间线聚合与分析功能。



二、核心功能矩阵

2.1 数据提取（26 个提取器）

分类	支持平台	数量
社交媒体	Facebook、Instagram、Twitter/X、Snapchat、LINE、微博、抖音、哔哩哔哩、小红书、快手	10
云存储	Google Drive、Dropbox、OneDrive、百度网盘、阿里云盘	5
电子邮箱	Gmail、Outlook、Yahoo Mail、网易邮箱(163/126/yeah.net)、QQ 邮箱	5

分类	支持平台	数量
即时通讯	Telegram、WhatsApp、Signal、微信、QQ	5
设备备份	iCloud Backup	1

2.2 凭据采集

来源	技术手段
Chrome / Edge	SQLite 读取 + DPAPI / AES-256-GCM 解密
Firefox	logins.json + cookies.sqlite 解析
macOS 钥匙串	.keychain-db 导入
手动输入	OAuth Token、Session Cookie、IMAP 授权码等
自动发现	扫描本机所有浏览器配置文件，一键导入

2.3 证据保全

- 所有提取文件自动计算 **SHA-256** 哈希
- 每步操作记录到带时间戳的审计日志
- 支持一键**完整性校验**，检测文件是否被篡改或丢失
- 导出 **JSON / HTML** 格式证据报告

2.4 分析功能

功能	描述
跨服务时间线	聚合所有提取数据，按时间排序生成统一时间线
全文搜索	对案件目录下全部 JSON 数据进行关键词检索
关键词监控	预设关键词列表，自动扫描匹配并高亮
案件仪表盘	统计各服务数据量、提取状态概览
邮件专用查看器	邮箱分组展示、正文渲染、附件管理、CSV 导出

2.5 用户界面

- **Ribbon 风格工具栏** — 六页签（案例/获取/安全/提取/分析/报告），操作一目了然
- **底部多视图切换** — 设备数据、案例概览、时间线、操作日志
- **证据标记系统** — 重要、可疑、已确认、待审查、关键证据 五级标记
- **拖放导入** — 直接将凭据文件拖入窗口即可识别并导入
- **启动画面** — SVG 渲染的品牌启动画面