Cirrus — Cloud Forensics Data Extraction Platform

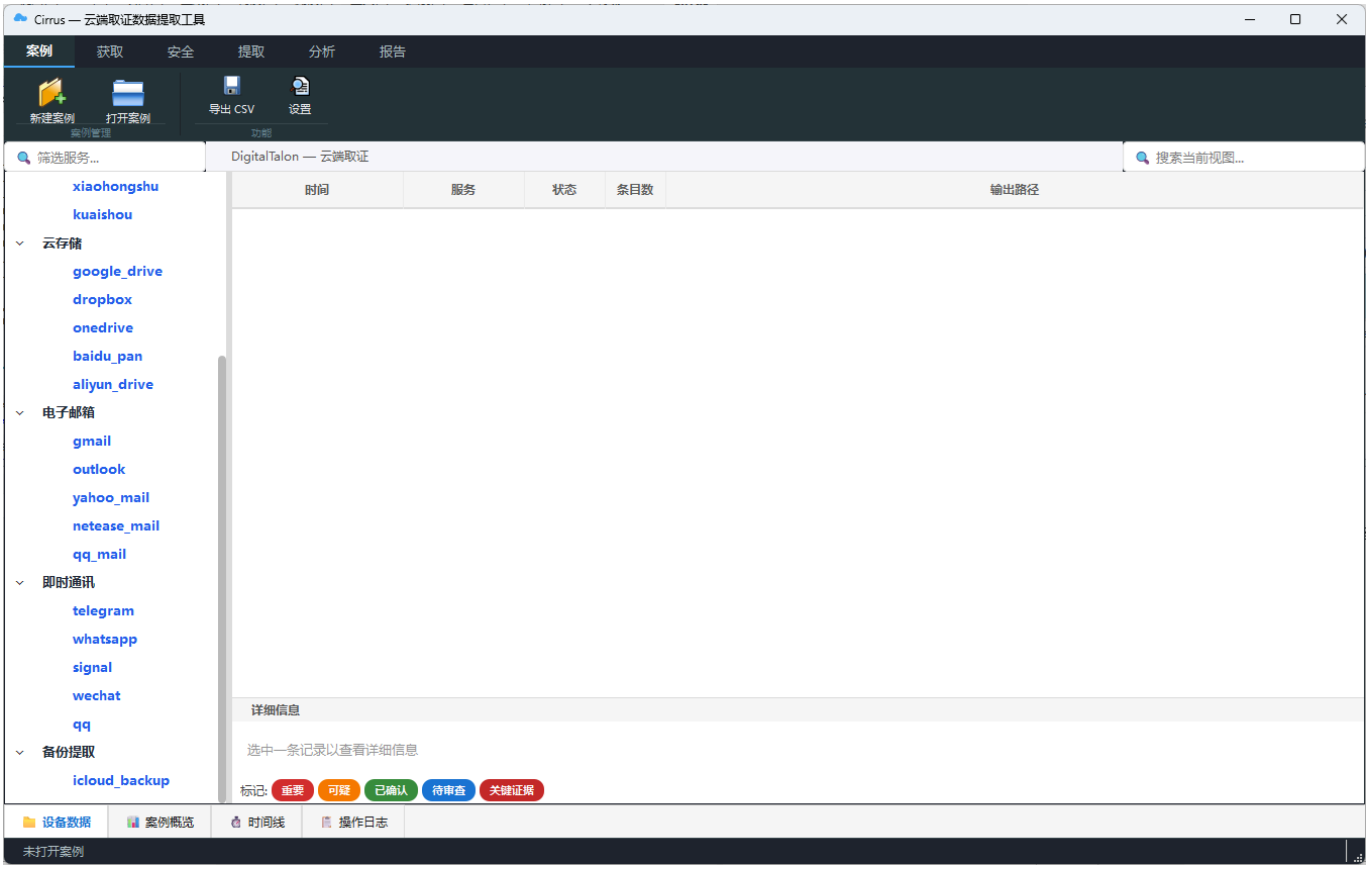
Product overview and technical highlights

1. Product positioning

Cirrus is a desktop platform for **cloud and online-account data extraction and analysis** in digital forensics workflows. It runs in **GUI** or **CLI** mode so investigators can work interactively in the lab or automate batch jobs in scripted pipelines.

The platform covers **five categories** and **26 cloud services**: social media, cloud storage, email, instant messaging, and device backups. Built-in **chain-of-custody** handling, audit logging, and cross-service **timeline** tools help teams preserve defensible evidence and review extracted data in one place.

Built with **Qt 6** on Windows (x64), Cirrus integrates with local browsers and OS credential stores while talking to remote services over HTTPS using session cookies, OAuth tokens, IMAP, or local application data where applicable.



2. Core capability matrix

2.1 Data extraction (26 extractors)

Category	Supported platforms	Count
Social media	Facebook, Instagram, Twitter/X, Snapchat, LINE, Weibo, Douyin, Bilibili, Xiaohongshu, Kuaishou	10
Cloud storage	Google Drive, Dropbox, OneDrive, Baidu Netdisk, Aliyun Drive	5
Email	Gmail, Outlook, Yahoo Mail, NetEase Mail (163/126/yeah.net), QQ Mail	5
Instant messaging	Telegram, WhatsApp, Signal, WeChat, QQ	5
Device backup	iCloud Backup	1

Each service is implemented as a pluggable **extractor** behind a common interface: authenticate with supplied credentials, pull data into a case folder, and emit structured JSON (and related files) suitable for review and reporting.

CLI service identifiers (examples): `google_drive`, `baidu_pan`, `gmail`, `wechat`, `douyin`. Run `Cirrus.exe --cli --list` to print all registered extractors on your build.

2.2 Credential acquisition

Source	Technique
Chrome / Edge	SQLite profile reads + **DPAPI** / **AES-256-GCM** decryption
Firefox	`logins.json` and `cookies.sqlite` parsing
macOS Keychain	`.keychain-db` import
Manual entry	OAuth access tokens, session cookies, IMAP app passwords, and service-specific secrets
Auto-discovery	Scan local browser profiles and import credentials in one step

Credentials can also be **dragged and dropped** onto the main window (e.g. Chrome `Login Data`, `Cookies`, Firefox `logins.json`, keychain exports).

2.3 Evidence preservation

- **SHA-256** hashes computed for extracted artifacts
- **Timestamped audit log** for extraction and import operations
- **Integrity verification** to detect missing or altered files after export
- **Evidence reports** in **JSON** and **HTML** for case documentation

Case output is organized under a configurable case directory, with per-service subfolders and shared report files (e.g. `evidence_report.json`, `timeline.json`).

2.4 Analysis features

Feature	Description
Cross-service timeline	Merge events from all extracted JSON sources into a single chronological timeline
Full-text search	Keyword search across JSON under the active case directory
Keyword monitoring	Predefined keyword lists with automatic scan and highlight
Case dashboard	Overview of services, file counts, sizes, and record estimates
Email viewer	Grouped mailbox view, body rendering, attachment handling, CSV export

2.5 User interface

- **Ribbon-style toolbar** — six tabs: **Case**, **Acquire**, **Security**, **Extract**, **Analyze**, **Report**
- **Multi-pane workspace** — service tree, credentials table, extraction results, and operation log
- **Evidence tagging** — five levels: Important, Suspicious, Confirmed, Pending review, Key evidence
- **Drag-and-drop import** — drop credential files directly into the application window
- **Branded splash screen** — SVG-based startup experience

Traditional menu shortcuts remain available (e.g. **Ctrl+N** new case, **F5** start extraction, **Ctrl+F** search).

---

3. Typical workflow

1. **Create or open a case** — a timestamped folder holds all artifacts and logs.
2. **Import credentials** — browser auto-detect, manual dialog, or drag-and-drop.
3. **Select services** — pick targets in the service tree; filter with the search box.
4. **Extract** — run one service or batch extract; monitor progress and logs.
5. **Analyze** — timeline, full-text search, keyword monitor, or dedicated email viewer.
6. **Report** — export HTML/JSON evidence reports, timeline, logs, or CSV as needed.
7. **Verify** — run integrity checks before handing off media or reports.

---

4. Command-line mode

For automation and headless environments:

```
Cirrus.exe --cli --list
Cirrus.exe --cli --service google_drive --cred credentials.json --output
D:\cases\20260916_001
Cirrus.exe --cli --all --cred credentials.json --output D:\cases\20260916_001
```

The credentials file is JSON compatible with the GUI credential model. On completion, the CLI writes evidence and timeline exports into the output directory, consistent with the GUI case layout.

---

5. Architecture (brief)

Layer	Role
UI (`Cirrus`, dialogs)	Case management, ribbon actions, viewers, settings
Core	`CredentialManager`, `CloudAuthEngine`, `EvidencePreserver`, `BatchExtractor`, `ExtractionWorker`, `TimelineAggregator`
Extractors	One module per cloud service; registered via `ExtractorFactory`
Network	HTTP client helpers, optional proxy and timeout settings

New services are added by implementing `IExtractor` and registering the service key—without changing the main shell.

---

6. System requirements

- **OS:** Windows 10/11 (x64)
- **Runtime:** Qt 6-based build (project targets Qt 6.10.x with MSVC)
- **Network:** HTTPS access to target cloud endpoints; optional HTTP proxy in settings
- **Permissions:** Read access to browser profiles and local app data paths when using local credential or IM backup extraction (e.g. WeChat/QQ data folders)

---

7. Legal and operational notice

Cirrus is intended for **authorized digital forensics, incident response, and compliance** use only. Operators must have ** lawful authority** (consent, warrant, or organizational policy) before accessing accounts or cloud data. Respect platform terms of service and applicable privacy and data-protection laws in your jurisdiction.

---

8. Localization

The desktop UI is available in **Simplified Chinese** (default) and **English**. Choose **Settings** → **Interface** → **Interface language**, then restart the app. CLI: `--lang en` or `--lang zh`. Details: localization-en.md.

9. Related documentation

Document	Language	Description
功能概述.md	Chinese	Feature overview (same product scope)
localization-en.md	English	Language settings and translator workflow

---

Cirrus — cloud forensics data extraction for investigators who need breadth of services, auditable exports, and both interactive and automated workflows.