**AX-CFS Computer Forensic System**

Product Introduction

The AX-CFS (Computer Forensic System) is a **cross-platform, automated forensic analysis platform** designed for comprehensive investigation of computers and storage media. Combining **Windows, macOS, and Linux analysis modules**, it enables rapid extraction and analysis of system metadata, user activity traces, file artifacts, browser histories, emails, chat logs, and application data. Ideal for law enforcement, corporate audits, and cybersecurity teams, it delivers court-admissible results with forensic precision.
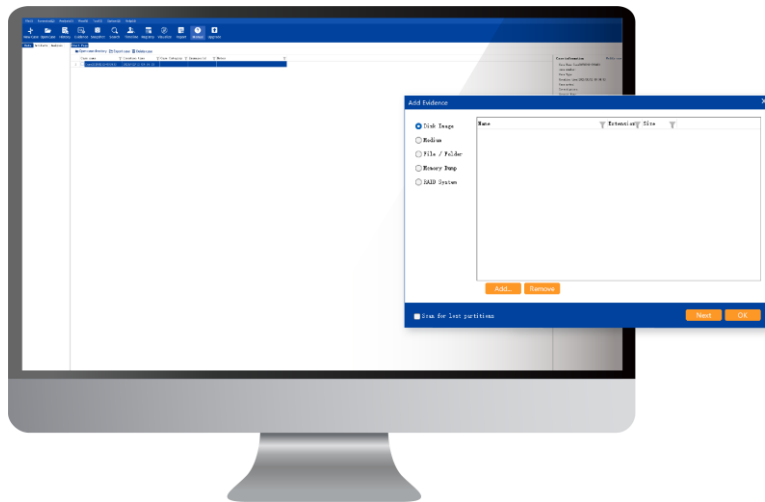
Key Features

1. Cross-Platform & Multi-Format Support

- **Disk Image Compatibility**: DD, E01, VMDK, VHD, QCOW2, and 10+ formats.
- **File Systems**: NTFS, APFS, Ext2/3/4, HFS+, FAT/exFAT, XFS.
- **Operating Systems**: Full support for Windows, macOS, and Linux.

2. Advanced Data Extraction & Analysis

- **Browser Forensics**:
  - Parse history, cookies, downloads, and cached data from **Chrome, Firefox, Safari, Edge, QQ Browser**, and 15+ others.
- **Email & Chat Analysis**:
  - Decrypt and analyze Outlook (PST/OST), Foxmail, Lotus Notes, WeChat, QQ, Skype, and enterprise communication tools.
- **Metadata Insights**:
  - Extract Office document authorship, creation/modification times, and hidden metadata.
  - Recover SQLite databases (e.g., encrypted WhatsApp/Signal chats) with password cracking.

3. Memory & Mobile Integration

- **Volatile Data Capture**:
  - Extract RAM dumps, including QQ chat logs, bank account details, and ID card information.
- **Mobile Backup Parsing**:
  - Analyze iTunes, 360 Mobile Assistant, and Android backup files (e.g., WeChat

memory images).

4. AI-Driven Analytics
- **User Behavior Reconstruction**:
  - Visualize timelines (web browsing, file operations, chats) via **bar charts, line graphs, and heatmaps**.
  - Map geographic data from emails, photos, and GPS logs.
- **Sensitive Data Detection**:
  - Auto-flag bank accounts, IDs, phone numbers, and custom keywords using regex/wildcards.

5. Forensic Tools & Reporting
- **Registry Analysis**:
  - Auto-load Windows registry hives; export HTML reports with editable templates.
- **Hex & Time Decoding**:
  - Decode hex data with **26 templates** (timestamps, encoded strings).
  - Convert timestamps across **21 formats** (Unix, Windows, macOS).
- **Compliance Reporting**:
  - Export interactive HTML/Word reports with evidence summaries, charts, and CSV exports.

Technical Highlights
- **Automated Workflows**: AI-driven parsing for large datasets (e.g., 1M+ files).
- **Live Forensics**: Capture volatile data (RAM, encryption keys) from active systems.
- **Modular Design**: Integrate third-party tools (e.g., X-Ways, Autopsy) via API.

Use Cases
- **Law Enforcement**: Uncover financial fraud via transaction trails or recover deleted chat evidence.
- **Corporate Compliance**: Audit employee devices for IP theft or policy violations.
- **Incident Response**: Identify malware persistence in registry entries or system logs.

Why AX-CFS?
- **Depth**: From **memory forensics** to **encrypted SQLite databases**, no layer is overlooked.
- **Speed**: Process terabytes of data 3x faster than traditional tools.
- **Compliance**: Meets **ISO 27037**, **NIST SP 800-86**, and **GDPR** standards.

Ansion Intelligence
Innovating Digital Forensics Solutions for Justice and Enterprise

---

Ansion Intelligence is a leading provider of cutting-edge digital forensics products and technical services, dedicated to empowering judicial authorities and enterprises with reliable solutions for electronic evidence collection, analysis, and management.