**AX-OFS Online Forensic System**

Product Introduction

The AX-OFS (Online Forensic System) is a **Windows-centric live forensic analysis platform** engineered for real-time extraction of volatile data, system artifacts, and user activity traces. Specializing in **physical memory acquisition**, **password decryption**, and **HTML report automation**, it empowers law enforcement, cybersecurity teams, and auditors to capture critical evidence from active systems with court-admissible integrity.
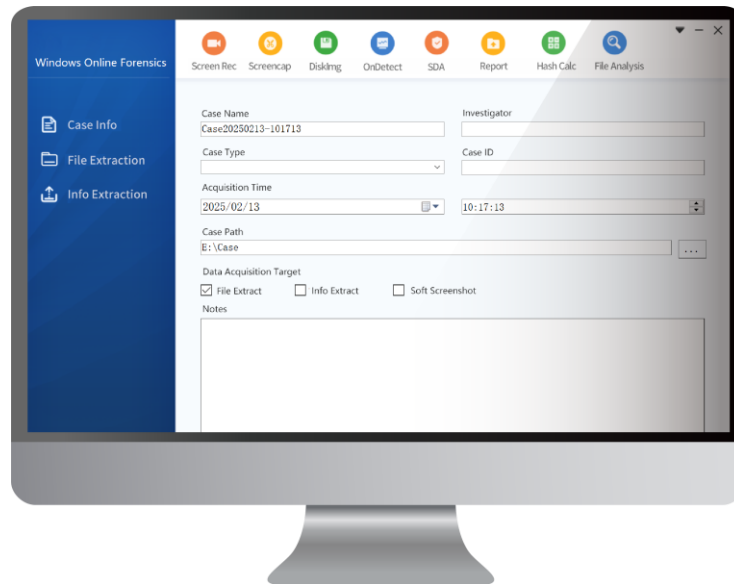
Key Features

1. Comprehensive Data Extraction

- **Multi-mode Extraction**:
    - Target files, deleted files, keyword-based files, size/time-filtered data.
    - Extract Windows event logs, USB flash disk usage records, scheduled tasks, and registry hives.
- **Browser & App Forensics**:
    - Parse 15+ browsers (Chrome, Firefox, Safari, etc.) for history, cookies, and cached passwords.
    - Decrypt **WeChat/QQ memory snapshots**, DingTalk/BatChat logs, and email clients (Outlook, Foxmail).
- **Password Recovery**:
    - Extract system passwords, **Chrome/FireFox protected storage**, VPN/RDP credentials, and encrypted wallet files.

2. Forensic Imaging & Verification

- **Disk Imaging**:
    - Generate DD/E01 images with **on-the-fly MD5/SHA256 hashing**.
- **Memory Acquisition**:
    - Capture RAM dumps for malware analysis (e.g., ransomware encryption keys).

3. Operational Flexibility

- **Auxiliary Drive Licensing**:
    - Deploy time-limited **secondary disk** for multi-system investigations.

- **Online/Offline Modes**:
  - Air-gapped imaging or live-system extraction with zero footprint.
- **Preview & Selective Extraction**:
  - Screen files pre-recovery (e.g., filter encrypted/compressed files).

4. Reporting & Compliance
- **HTML Reports**:
  - Generate timeline-based, court-ready reports with evidence summaries.
- **Regulatory Adherence**:
  - Align with **ISO 27037** and **NIST SP 800-86** standards for forensic integrity.

Technical Highlights
- **Real-time Decryption Engine**: Bypass **memory-resident encryption** for WeChat, QQ, and enterprise apps.
- **Hash-Validated Workflow**: Ensure evidence integrity via **MD5/SHA256** during extraction.
- **Multi-threaded Processing**: Accelerate data capture by 40% vs. legacy tools.

Use Cases
- **Corporate Investigations**: Uncover insider data leaks via WeChat/QQ chat logs or USB usage trails.
- **Incident Response**: Identify live malware/rootkits through RAM analysis and process snapshots.
- **Law Enforcement**: Recover deleted browser histories, encrypted emails, or VPN credentials.

Why AX-OFS?
- **Precision**: Combine **file carving** and **keyword contextualization** to minimize false positives.
- **Speed**: Image 1TB disks in <4 hours with parallel thread optimization.
- **Adaptability**: Support Windows 7 through Windows 11 23H2.

Ansion Intelligence
Innovating Digital Forensics Solutions for Justice and Enterprise

Ansion Intelligence

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.