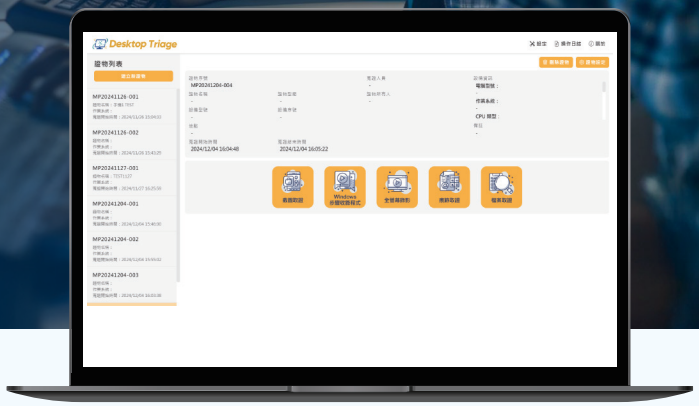
BlockChain Security

chainsecurity.asia

Desktop Triage

Desktop Triage is an easy-to-use digital forensics tool that assists investigators in collecting evidence from suspicious computer devices. It gathers digital evidence from both internal and external devices of the computer and records the evidence collection process to ensure transparency and accountability.



Automatically Screenshots

Automatically capture computer screen images by setting the desired time period and number of screenshots.

Steps Recording

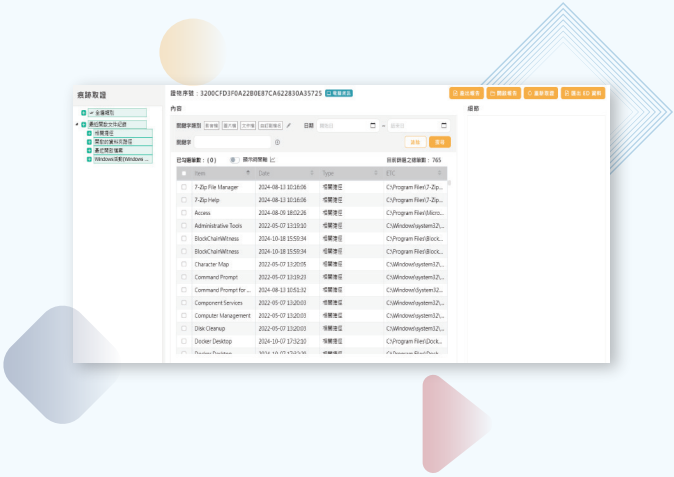
Record the user's activities on the computer with a series of consecutive screenshots.

Artifacts Collection

Extract detailed usage traces from the computer, such as website browsing history, software execution records, and document access logs.

Live Search

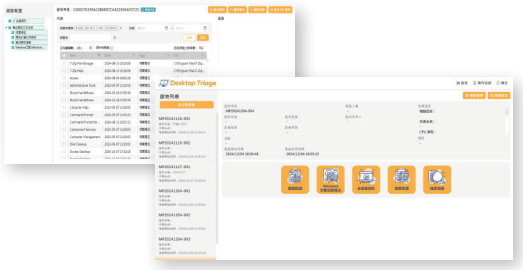
Retrieve all file data from the computer's hard drive or external storage devices.



> This product provides automated screenshot forensics and OCR text recognition on Windows systems. It also records the entire investigation process and generates a detailed evidence collection report to prevent potential disputes during the forensic process.

BCS dedicate ourselves to create client-focus solutions based on innovation, integrity, and sustainability

Desktop Triage



A Precise And Efficient Digital Forensic Tool

Digital Forensics: Securing Critical Evidence from Computers

This product allows for a thorough search of data within a computer, including the internal storage system, external hard drives, web browsing history, and executed software. Investigators can obtain important files and data from the computer as evidence.

Evidence Collection: Transparent and Verifiable Process

The integrity of the evidence collection process directly impacts the effectiveness of the evidence. This product can fully record the entire process during evidence collection, providing a detailed account of all actions taken by the investigator. It generates a visualized evidence collection record, ensuring transparency and accountability in the process, while enhancing the credibility of the digital evidence.

Screenshots Collection

- Take continuous, period, single, or browser screenshots, with manual settings for the number of screenshots and the desired time period.
- Select screenshot files for OCR text recognition and can search for keywords within the screenshots.
- Select screenshot evidence and generate a report, including images, file names, and collection time, etc.
- Record screen activity or steps to produce visual evidence reports of the collecting process.

Steps Recording

- Specifically collects computer usage footprints, including：website browsing history, recent software execution history, recent document history, etc.

About BlockChain Security

Founded in 2018, by industry experts with over 17 years in digital forensics, evidence preservation and information security. We noticed the gap of blockchain adaptations and began our mission to combine two core technologies; blockchain and information security.

chainsecurity.asia service@chainsecurity.asia +886 2 2515-2533