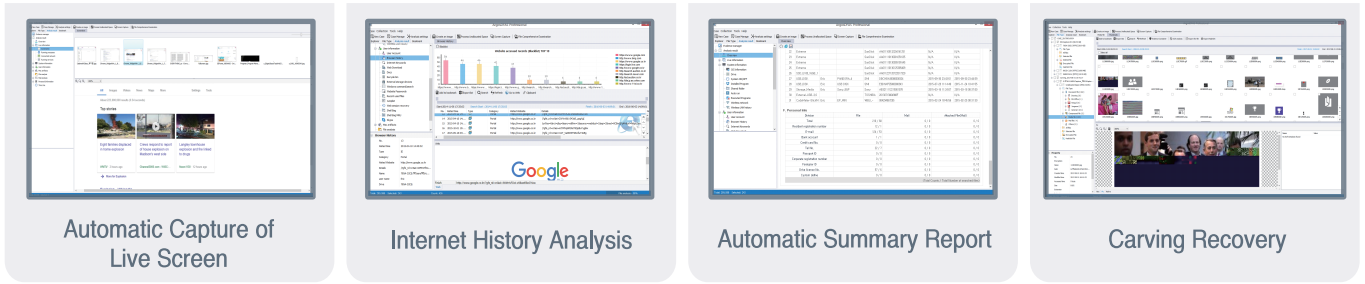


Features



Evidence Acquisition

- Disk imaging: Supports disk imaging on a live system (Does not require hard disk detachment)
- Evidence file acquisition: Logically acquires images of files to maintain their integrity as evidence



Analytical Features

- System information analysis: Automatically analyzes system information and system usage patterns
- User behavior information analysis: Automatically analyzes traces of user behaviors
- File and local mail analysis: Enables multiple keyword analysis and regular pattern analysis
- OCR analysis: Allows text extraction from image files and keyword searches of images



Expeditious Response

- Live memory acquisition: Acquires volatile information when system is on (Live Memory Capture)
- Initial response: Analyzes process, service and network information of the live system
- Automatic reports: Creates automated, summarized reports of basic analysis results
- Bookmark: Enables bookmarking for main information and supports creation of customized reports



Data Carving and Complete Analysis

- Deleted file identification: Enables expeditious identification of deleted files
- Data carving: Provides intensive data carving for files without metadata
- Bad signature analysis: Identifies arbitrarily modified filename extensions

Use Case

