GSM-Support ul. Dobrego Pasterza 102/5, 31-416 Krak·w
mobile +48 608107455, NIP 8133358609 REGON: 181081334
www.gsm-support.net

Internet Evidence Finder

Designed for forensic examiners and trained investigators in law enforcement & government, as well as IT security personnel in corporations who are conducting full forensic examinations of Windows and Mac computers.

- Windows and Mac OSX file system support
- Primarily used in a forensic lab environment
- Native image support for E01, Ex01, L01, Lx01, AD1, dd and dmg format
- Search live and deleted artifacts on hard drive and live RAM captures

Powerful Search Capabilities: Search 260+ Windows and Mac Internet artifacts and recover more data from more locations.

- Recover data from social networking communications, instant messenger chats, cloud-based artifacts, P2P file sharing apps, mobile backups, webmail, web browser history, pictures and videos
- Proprietary carving technique recovers more data from unallocated space & RAM
- Searches entire logical or physical drives: E01, Ex01, L01, Lx01, AD1, dd and dmg images
- Searches Files including the pagefile.sys, hiberfil.sys, and more
- Volume shadow and zip archives copies can be analyzed as standalone sources of evidence
- Ability to search multiple drives, images, file & folders in a single search
- The Artifacts Supported page has all the specific details for Windows and Mac artifact support

Find Evidence Quickly: Get immediate search results so you can start working with the data right away.

- Use ñQuick Searchò preset to see whatõs there and focus the investigation
- Review results in real-time without having to wait for search to complete
- Target search by artifact type, keyword and location on hard drive
- Multi-threaded support for multi-core processors improving search speed

Standardized Reporting: Flexible reporting and categorization to narrow down evidence quickly.

- Rebuild web pages in their original format on the date they were visited
- Parsed search queries for user keyword searches on major search engines
- Web history categorization - dating, cloud, classified, chat and social media sites, malware sites, pornographic sites, or create your own custom categories
- Search, filter, and bookmark important evidence
- Export report in html, pdf, excel, csv, and tab-delimited formats

- Share ñPortable Case Folderò with other investigators and stakeholders
- View results in a visual graphical timeline format
- Display chat searches visually like they would appear in the original application

Trusted By Industry Leaders: Used by leading law enforcement, government, and businesses around the globe.

- Developed by a former police officer & forensic examiner
- Validated by DOD Cyber Crime Center
- Validated by the National Institute of Justice
- Trusted by thousands of organizations in over 90 countries

Adheres to Industry Standards: Maintain the integrity of the case and chain of custody.

- Integrity of file metadata maintained- no data is altered
- IEF provides the file offset/physical location of data to manually verify all results
- Be confident in the results when testifying in court

Simple to Use: Get to key evidence with only 3 clicks of the mouse.

- Single search for over 250 Internet artifacts, no need to run multiple scripts
- Start working on your case immediately; no complicated setup
- Just ñset itò and ñforget itò while you work on other things
- No extensive training needed

Visualization

- With IEF Timeline, view evidence in a graphical chronological timeline
- Use drill downs to isolate webmail, chat messages, social media browser history and more during a specific time-frame
- Use IEF Timeline to zero-in on specific dates in time, or spikes in a suspectûs online activity
- Timeline supports .tln and log2timeline.csv files
- Plot geo-tagged artifacts on World Map tool in IEF Report Viewer (or export to KML file for analysis with Google Earth)

Analyze Recovered Pictures: IEF includes features intended to assist law enforcement with identification and categorization of pictures recovered by an IEF search.

- Refine search results by skin tone & body part detection
- Hashing of Recovered Pictures ï PhotoDNA, MD5 and SHA-1 hashes are provided for picture files recovered by IEF
- Access to the PhotoDNA feature is available at no additional cost for qualified Law Enforcement Customers. Request PhotoDNA Access
- Import Project Vic or custom hash databases to automate the identification and categorization of picture files
- Export pictures from the IEF report viewer for customers using third party picture analysis software (for example C4All)

Comparison Chart

- ief01
- 2edytowany

É 2022 www.gsm-support.net