

The proof is out there.

Find it, with **Internet Evidence Finder (IEF)** - The industry leading solution in recovering Internet-related evidence left behind on computers.

Internet Evidence Finder (IEF) is a digital forensics solution that can search a hard drive, live RAM captures, or files for Internet-related evidence. IEF was designed with digital forensics examiners/investigators in mind. IEF is also used by IT security professionals, litigation support personnel, incident response teams, cyber security specialists and corporate investigators.

IEF can recover evidence left behind within social networking artifacts, instant messaging chat histories, popular webmail applications, web browsing history, and peer-to-peer file sharing applications.

PRODUCT FEATURES

Recovery of more types of Internet-related evidence

- Social Networking Artifacts:
 - Facebook, Google+, Twitter, Myspace, Bebo
- Instant Messenger Chat History:
 - Skype, ICQ, Yahoo, GoogleTalk, MSN, AOL, mIRC, etc.
- Browser History:
 - Internet Explorer, Chrome, Safari, Firefox
- Webmail:
 - Gmail, Yahoo, Hotmail
- P2P applications:
 - Ares, eMule, Shareaza, Limewire, Gigatribe, Torrent

Finding more relevant & accurate evidence

- Patent pending data recovery process
- Single search for more than 50 artifacts
- Customize your search by selecting artifacts and locations to search

Simplified Workflow

- Automated check for disk encryption with Triage Edition
- Native image mounting
- Live RAM captures with Triage Edition

Rich & Comprehensive Reporting

- Locations of each recovered artifact displayed for easy validation
- Filter, sort, search, and bookmark recovered artifacts

Searching in more places

- Entire Logical or Physical Drives
 - .E01/dd images supported
- Unallocated space / deleted data
- Selected Files
 - Including live RAM captures, network PCAP files, the pagefile.sys / hiberfil.sys files, and more
- Entire user-selected folders and sub-folders
- Other important areas on a hard drive where evidence may be found



“We wanted a product that didn’t just recover browser artefacts but also addressed the importance of data from social networking tools and chat utilities.”

*Detective Constable Matt Johnstone, Fife Police Headquarters
Fife, Scotland*

“Using search terms can only get you so far when you’re faced with mounds of data to parse through. I found IEF to be a huge value, in depth, relevant tool to nearly every exam.”

*Det. Stephen Payne, Oregon State Police
Oregon, United States*

IEF Standard Edition: Setting the bar in digital forensics

IEF software comes on a USB dongle and can be installed on as many computers as necessary. The dongle holds the license key. Simply plug the USB dongle into the computer on which you’re running IEF and install the software. This dongle approach allows the flexibility to use IEF on different workstations but it can only run on a single computer at a time.

IEF Triage Edition: Take the power of IEF into the field

The Triage Edition offers all the functionality of the Standard Edition. In addition; with Triage you get the following:

- Automated check for disk encryption
- Built-in live RAM capture
- Built-in drive imaging
- Mount and search volume shadow copies
- Ability to save all results on the dongle

KEY BENEFITS



ROBUST SEARCH & DEPENDABLE RESULTS

IEF can recover more types of digital evidence than any other solution, which makes it more likely to uncover critical evidence. You can do a single search and find all Internet related evidence without having to try keywords, manually carve data, or run individual scripts. It’s the closest thing to a “Find All Evidence” button.

With our patent-pending technology, IEF finds more forms of Internet artifacts and filters out false positives. IEF is able to recover evidence from not only deleted data, but also live RAM captures, which often hold vital evidence.



ACCELERATE INVESTIGATIONS & REDUCE CASE BACKLOG

With the ever-growing hard drive capacities and the explosive growth in both case loads and complexity, organizations and agencies of all kinds require an accurate and comprehensive solution for recovering data. IEF is a rapid automated solution that saves a tremendous amount of time and allows you to work on other parts of the investigation while it’s searching. It’s as straightforward as hitting search and coming back to a comprehensive report to review the results.



USER FRIENDLY

Both experienced and new forensic examiners/investigators find the IEF user interface flexible, intuitive and easy to use. Because its reporting options are as impressive as its analytical capabilities, producing professional reports for both internal or external audiences is equally simple and straightforward. Time is of the essence and that is why there is no complex configuration or setup.



THE GOLD STANDARD IN DIGITAL ARTIFACT RECOVERY

IEF is considered the defacto standard for the recovery of digital evidence and is used by thousands of the most prestigious national security agencies, law enforcement teams, and corporations around the world.



COURT ADMISSIBLE

The reporting feature that’s built into IEF provides the information examiners require to manually verify all results.

JADsoftware Inc.

Waterloo Research & Technology Park
295 Hagey Boulevard, N2L 6R5,
Waterloo, Ontario, Canada

Phone: 519-342-0195

Fax: 519-772-3908

Email: sales@jadsoftware.com

Web: www.jadsoftware.com

