

FTK 3



What's New in Forensic Toolkit?

Reengineered Components for Improved Performance

Redesigned Database Layer: The FTK GUI is 10xs more responsive across the board, even on machines with only 4GB of RAM.

Redesigned Processing Engine:

- Leverages the same battle-tested FTK components
- Faster more efficient processing
- Cancel/Pause/Resume functionality
- Better real-time processing status
- CPU resource throttling
- New email notification upon processing completion

Distributed Processing:

- Every copy of FTK of comes with 4 workers, allowing you to leverage CPU resources from up to 4 computers. (3 distributed workers and 1 worker on the main FTK examiner system)

NOTE: Multiple FTK licenses cannot share common processing workers or a common Oracle database. If you are interested in having multiple examiners share common workers and a central database, please ask us about AccessData Lab.

- Leverage legacy hardware to reduce processing time

Completely Reengineered dtSearch Integration:

- Search results populate very fast, even with large result sets.
- We've changed the way results are stored and way results are displayed.

Enhanced Analysis

Built-in optical character recognition:

- Index and search image files (e.g. TIFFs and PDFs).

Native Encryption Support:

- Encrypt, decrypt and process encrypted evidence archives.

New Macintosh Capabilities:

- Process B-Trees attributes for metadata
- PLIST support
- SQLite database support
- Apple DMG and DD_DMG disk image support
- Crack Sparse Images or Sparse Bundles
- JSON file support

Dramatically Enhanced Graphics Tab:

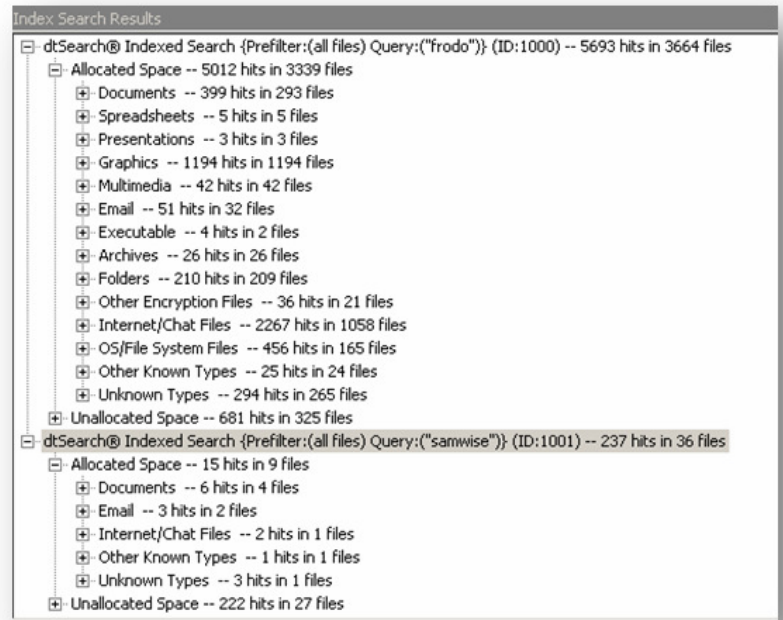
- Image thumbnails are now stored in batches in the case folder, enabling faster image retrieval and reduced backup time.
- Fewer refreshes and less delay as you scroll quickly through pages of graphics.
- New icon for corrupted images vs. loading images.

Additional Encryption Support:

- Supports popular encryption technologies, such as Credant, SafeBoot, Utimaco, EFS, PGP, Guardian Edge, Sophos Enterprise and S/MIME.

Explicit Image Detection Integration (Available as an Add-on):

- Automated detection and identification of graphic images by analyzing visual features in the image to assess its actual visual content.
- All images are given a score based on their projected potential to be pornographic, in order to streamline the process of identifying evidentiary images.



Index search results are displayed by category.

Acquisition and Restoration

Secure Remote Device Mounting: Remotely connect to a single target machine and mount devices (physical devices, logical volumes or memory) locally on the examiner's machine. This enables examiners to use FTK, Imager or a third-party utility to forensically analyze live data on the remote devices from their examiner systems.

Live Device Acquisition:

- Perform network-based, secure, single-system forensic acquisition of physical devices, logical volumes and RAM.
 - Image the full range of system memory
 - Image entire physical device or devices
 - Image an entire volume or volumes
- The agent can be quickly deployed and does not require installation of any kind.
- No painful authentication/authorization process is required.

Evidence File Restoration: Quickly restore your forensic image to media for simple interaction and better contextual understanding, distribution or processing with other tools.

Analysis of Live Data

RAM Dump Analysis:

- Enumerate all running processes, including those hidden by rootkits, and display associated DLLs, network sockets and handles in context, from 32- and 64-bit Windows machines.
 - **For each process it will display:** Name | Path | Start Time | Working Directory | Command Line | ProcessID | ParentID | MD5 | SHA1 | Fuzzy Hash | Size | Windows Title
 - **For each DLL:** Name | Path | Process Name | ProcessID | ParentID |
 - **For Network Socket:** Port | Protocol | Local Address | Remote Address | Remote Port | Process Name | ProcessID
 - **For Open Handles:** Handle Type | Path | Access Mask | ProcessID
- Dump a process and associated DLLs for further analysis in third-party tools.
- Memory string search allows you to identify hits in memory and automatically map them back to a given process, DLL or piece of unallocated and dump the corresponding item. **COMING SOON!**
- Process RAM captures for additional forensic artifacts, such as passwords, html pages, .lnk files and MS Office documents.

Reporting and Case Management

Define Column Settings Per Bookmark in Your Reports: Define unique column settings that apply to a specific bookmark.

Processing Exception & Case Info Report: FTK 3 now provides clear reporting on what files could not be processed or indexed. In addition, the report displays version, name of evidence and case processing preferences per evidence item, including dtSearch options, as well as overall processing time.

Define Registry Supplemental Reports (RSR) During Pre-processing or Additional Analysis:

- Choose from a set of pre-defined Summary RSR templates, which are automatically made available in the Reporting Wizard
- Access our library of RSR reports online <http://www.accessdata.com/rsr.html>
- Create your own

Export MSGs from All Supported Email Types: Currently supported email types are: Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, EML (Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, etc.), Netscape, AOL and RFC 833

CSV Support: You now have the option to automatically create a CSV of the processed files that can be imported into Excel or a database application

Case Portability: You can easily store and transfer an entire case on separate physical media without doing a full case backup.

Enhanced User Administration: Administrators can now change user names, roles, passwords and delete users.

Optimize Performance with Dynamic Modification of Memory Allocation

Database Memory Adjuster: Depending on data set size, the ability for results in the GUI to come back quickly is a result of hardware and memory allocation for the database. Oradjuster enables examiners to dynamically modify memory allocation between processing and analysis to further improve processing and review performance. It will automatically free up memory resources utilized by the database upon the closure of FTK.

