



- [Home](#)
- [Products](#)
 - [Forensics](#)
 - [FTK](#)
 - [MPE+](#)
 - [AD Lab](#)
 - [AD Enterprise](#)
 - [SilentRunner Mobile](#)
 - [Decryption](#)
 - [Triage](#)
 - [Live Response](#)
 - [eDiscovery & Litigation Support](#)
 - [AD eDiscovery](#)
 - [AD ECA](#)
 - [AD Summation iBlaze](#)
 - [AD Summation Enterprise](#)
 - [AD Summation CaseVantage](#)
 - [WebBlaze](#)
 - [Discovery Cracker](#)
 - [Cyber Security / Incident Response](#)
 - [CIRT](#)
 - [AD Enterprise](#)
 - [SilentRunner Sentinel](#)
- [Services](#)
 - [Forensics](#)
 - [Discovery Planning](#)
 - [eDiscovery Collection](#)
 - [Processing/Review Prep](#)
 - [Cloud Review/Case Mgt.](#)
 - [Augmented Attorney Review](#)
 - [Auto Doc Production](#)
 - [eServe](#)
 - [Data Storage](#)
- [Training](#)
 - [Courses](#)
 - [Course Syllabi](#)
 - [Certifications](#)
 - [Customized Training](#)
 - [Summation Specialized Training](#)
 - [Training Calendar](#)
 - [AD Training Partners](#)

- [Academic Program](#)
 - [AD Academic: Computer Forensics](#)
 - [AD Academic: Summation](#)
 - [Forensic Academic Partners](#)
 - [Summation Academic Partners](#)
- [Summ It Up](#)
- [News](#)
 - [Press Releases](#)
 - [Articles](#)
 - [Events](#)
- [Support](#)
 - [AD Downloads](#)
 - [AD Summation Downloads](#)
 - [Previous Releases](#)
 - [Discussion Forum](#)
 - [Contact Support](#)
 - [General Inquires / Sales](#)
 - [Technical / Customer Support](#)
 - [Knowledge Base](#)
 - [Court Reporter Information](#)
- [Company](#)
 - [Contact Us](#)
 - [General Inquires / Sales](#)
 - [Technical / Customer Support](#)
 - [Overview](#)
 - [Resellers](#)
 - [Corporate Resellers](#)
 - [Summation Resellers](#)
 - [US Federal Resellers](#)
 - [Management](#)
 - [Career Opportunities](#)
- [Technology Partners](#)
 - [FTK](#)
 - [MPE+](#)
 - [AD Lab](#)
 - [AD Enterprise](#)
 - [SilentRunner Mobile](#)
 - [Decryption](#)
 - [Triage](#)
 - [Live Response](#)
-



Feeling Encased?

Replace your traditional computer forensics tools
with FTK for just \$840!

[LEARN MORE >](#)

THE INDUSTRY-STANDARD COMPUTER FORENSICS SOFTWARE USED BY GOVERNMENT AGENCIES & LAW ENFORCEMENT AROUND THE WORLD



Forensic Toolkit® (FTK®) is recognized around the world as the standard in computer forensics software. This court-validated digital investigations platform delivers cutting-edge computer forensic analysis, [decryption and password cracking software](#) all within an intuitive and customizable interface. FTK 3 is built for speed, analytics and enterprise-class scalability. Known for its intuitive interface, email analysis, customizable data views and stability, FTK lays the framework for seamless expansion, so your computer forensics solution can grow with your organization's needs.

Forensic Toolkit 3 is now the most advanced computer forensics software available, providing functionality that normally only organizations with tens of thousands of dollars could afford. However, we are committed to making our technology available to all investigators and analysts, whether they are in law enforcement, education, a government agency, a Fortune 500 corporation, or performing digital investigations as a computer forensics service provider.

“FTK 3 is superb, and the Mac features are something that can't be found in any other Windows analysis tool.”

– Ryan R. Kubasiak

Apple Certified Technical Coordinator, Apple Certified Support Professional

GCFA, CCE, ACE, EnCE, CEECS

<http://www.appleexaminer.com>

PRODUCT DETAILS:

An Integrated Computer Forensics Solution

- Create images, analyze the registry, conduct an investigation, decrypt files, crack passwords, identify steganography, and build a report all with a single solution.
- [Recover passwords](#) from 100+ applications; harness idle CPUs across the network to decrypt files and perform robust dictionary attacks.
- KFF hash library with 45 million hashes.

Enterprise-class Architecture

- Supports large and complex datasets.
- Never lose work due to a crash, because the FTK components are compartmentalized. (Example: If the GUI crashes, the Workers continue to process data.)
- Ability to back up and archive cases.
- Every copy of FTK 3 includes a total of 4 Workers to enable distributed processing – 1 on the examiner machine and 3 distributed.
 - **NOTE:** If you are interested in having multiple examiners share common workers and a central database, please contact your sales representative to inquire about [AccessData Lab](#).
 - [Distributed Processing](#) requires powerful hardware and networking technology. Processing evidence is very disk IO intensive and requires fast drives. In addition, the machine that runs the Processing Manager must be the fastest computer (CPU) speed in the processing group. Finally, for peak performance you will need the fastest networking technology available to you. For details on configuring distributed processing, please see the following documents:
 - [Configuring Distributed Processing with FTK 3](#)
 - [FTK 3 System Specifications Guide](#)
- The solution easily expands to incorporate [Lab](#) capabilities, such as the ability to leverage a centralized database infrastructure and shared distributed processing farm, as well as collaborative forensic analysis, central case/task management and Web review. This is of particular value to government and law enforcement computer forensics labs.

Powerful Processing and Speed

- The GUI is [10 times more responsive](#).
- [Distributed Processing](#) allows you to leverage up to 3 additional computers to dramatically reduce processing time and tackle massive data sets.
- True multi-processor and multi-threading support that takes advantage of hardware advancements.

- Wizard-driven processing ensures no data is missed.
 - Cancel/Pause/Resume functionality
 - Enhanced real-time processing status
 - CPU resource throttling
 - New email notification upon processing completion
- Pre- and post-processing refinement allows you to control how images are processed.
- Advanced data carving engine allows you to carve allocated and unallocated data and specify criteria, such as file size, data type and pixel size to reduce the amount of irrelevant data carved while increasing overall thoroughness.
- Optimized dtSearch integration delivers fast indexing and fast search results.

The Most Advanced Analytics

- The ONLY commercial computer forensics software product that supports both 32-bit and 64-bit Windows machines.
- RAM Dump Analysis
 - Enumerate all running processes, including those hidden by rootkits, and display associated DLLs, network sockets and handles in context.
 - **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 space and dump the corresponding item.
 - Process RAM captures for additional forensic artifacts, such as passwords, html pages, .lnk files and MS Office documents.
- Powerful index search engine and a proper full-feature regular expression engine for binary searches.
- Broad file system, compound file and email support.
 - 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
 - Process and analyze DMG (compressed and uncompressed), Ext4, exFAT, VxFS (Veritas File System), Microsoft VHD (Microsoft Virtual Hard Disk), and Blackberry IPD backup files.
 - Create and process Advanced Forensic Format (AFF) images.
- Supports popular encryption technologies, such as Credant, SafeBoot, Utimaco, EFS, PGP, Guardian Edge, Sophos Enterprise and S/MIME.
- Automatically identify potentially pornographic images, using the Explicit Image Detection (EID) add-on.
- Comprehensive support for [* Apple® Computers](#)
 - Process B-Trees attributes for metadata
 - PLIST support
 - SQLite database support
 - Apple DMG and DD_DMG disk image support
 - JSON file support

Preview, Acquisition and Analysis of LIVE DATA

- Perform network-based, secure, single-system forensic acquisition of physical devices, logical volumes and RAM.
 - The agent is easy to deploy.
 - Doesn't require a cumbersome installation and authentication process.
- Secure Remote Device Mounting

Intuitive Interface and Rich Functionality

- Easy-to-understand and easy-to-use GUI with pre-defined and customizable data views, advanced digital evidence filtering, dockable windows and automated data categorization.
- Multiple data views allow users to analyze files in a number of different ways, such as native, hex, text and filtered.
- Full Unicode and Code Page support.
- Create detailed reports and output them into native format, HTML, PDF, XML, RTF, and more – with links back to the original evidence.
- Define Registry Supplemental Reports (RSR) during pre-processing or additional analysis.
- Clear reporting on what files could not be processed or indexed with the Processing Exception/Case Info report.
- Create a CSV of the processed files that can be imported into Excel or a database application.
- Export MSGs for all supported email types.
- Evidence File Restoration allows you to quickly restore your forensic image to media for simple interaction and better contextual understanding, distribution or processing with other tools.

* Apple and Mac are trademarks of Apple Inc., registered in the U.S. and other countries.

Contact

[Request Information](#)

BROCHURES

- [AD Forensics Brochure](#)
- [FTK Data Sheet](#)
- [AD Enterprise Appliance](#)
- [Explicit Image Detection](#)
- [Laci Peterson Case Study](#)
- [AD Legal Brief](#)
- [MORE >](#)

- [LEGAL JOURNAL: The Rules of Evidence and AccessData Technology](#)
- [The Importance of Memory Search and Analysis](#)
- [MORE >](#)

- [FTK 3.2: Image Restoration](#)
- [FTK 3.2: Global Features](#)
- [FTK 3.2: Enhanced Processing and Interface Options](#)
- [FTK 3.2: Mounting Image Files](#)
- [Native Encrypted Evidence Support](#)
- [Optical Character Recognition](#)
- [Custom File ID and Carving](#)
- [Memory Analysis](#)
- [UI Performance](#)
- [Mac® Computer Analysis](#)
- [Live, Remote Data Acquisition](#)
- [Explicit Image Detection](#)
- [MORE >](#)



[Go To Top »](#)

© 2011 AccessData Group, LLC. All Rights Reserved.

[Contact Us](#) / [Support](#) / [Feedback](#) / [Sitemap](#)

Products

- [Forensic Toolkit](#)
- [AD Enterprise](#)
- [AD eDiscovery](#)
- [AD Summation iBlaze](#)
- [AD Summation Enterprise](#)
- [AD Summation CaseVantage](#)
- [CIRT](#)
- [SilentRunner Sentinel](#)
- [AD Lab](#)
- [Mobile Phone Examiner Plus](#)
- [Distributed Network Attack](#)
- [Password Recovery Toolkit](#)

Support

- [AD Downloads](#)
- [Previous Releases](#)
- [Discussion Forum](#)
- [Technical Papers](#)

Resource Library

- [Brochures](#)
- [White Papers](#)
- [Webinars](#)

Training

- [AccessData Bootcamp](#)
- [AccessData Forensics](#)
- [Windows Forensics 7](#)
- [FTK 3 Transition Day](#)
- [Applied Decryption](#)
- [Internet Forensics](#)
- [Windows Forensics – XP](#)
- [Windows Forensics – Vista](#)
- [Windows Forensics – Registry](#)
- [Mobile Forensics 101](#)
- [Mobile Forensics 202](#)
- [Mobile Forensics 303](#)

- [MORE](#)

Contact Us

- [Americas/Asia Pacific](#)
- [Europe/Middle East/Africa](#)
- [Summation Software Support](#)
- [eDiscovery/Litigation Support Services](#)
- [Discovery Cracker Support](#)