

AccessData Forensics



BUILD A SOLUTION TO
MEET YOUR SPECIFIC NEEDS
WITH FLEXIBILITY,
SCALABILITY AND EASE OF USE



AccessData[®]

A Pioneer in Digital Investigations Since 1987

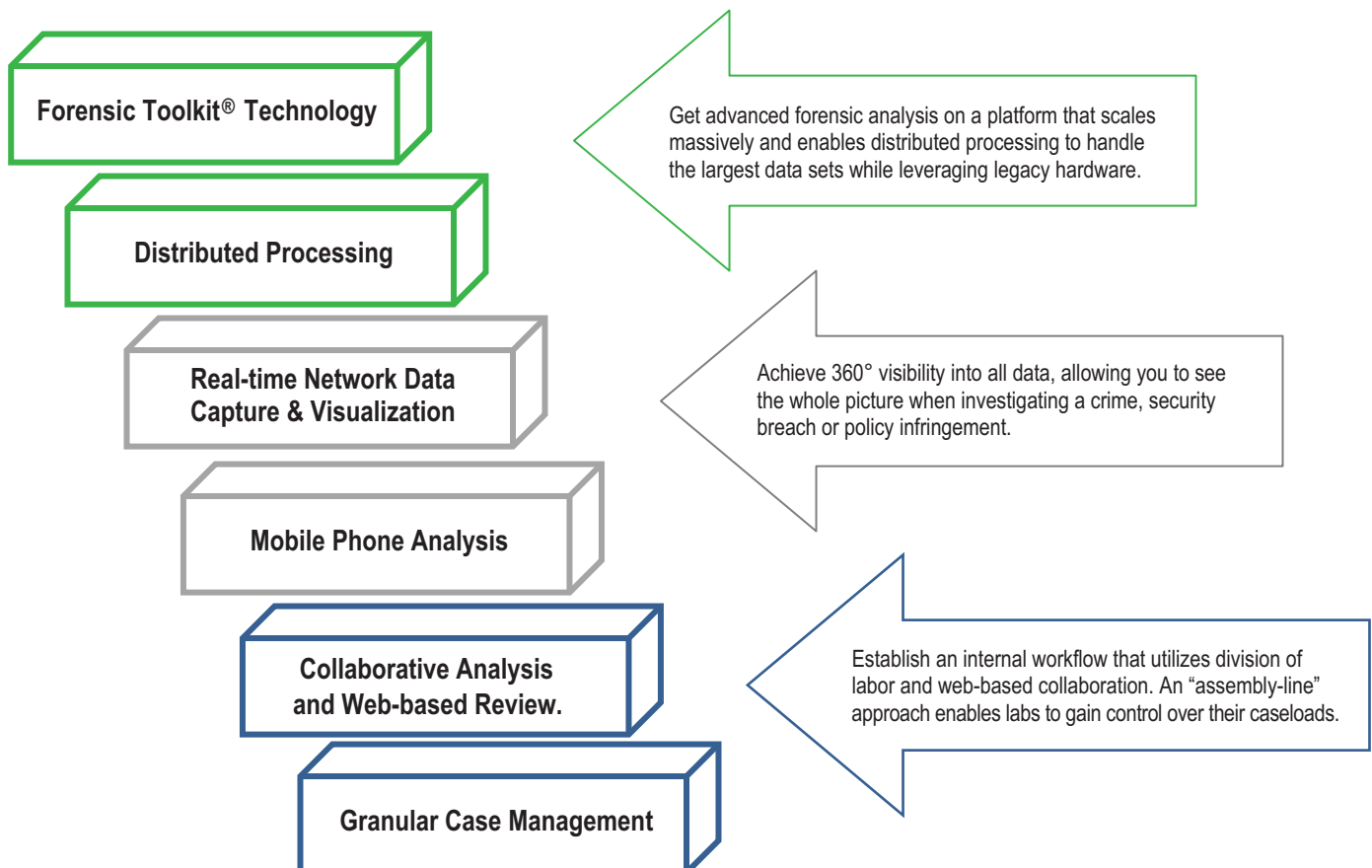


Introducing a New Era in Digital Forensic Investigations...

Investigators today need much more than a disparate bag of tools to get the job done. Case loads and case complexity are increasing at an explosive rate, due to legal requirements, eDiscovery demands, technically savvy criminals, increasing data sets and a slew of other factors. In addition, there are a number of non-forensic players in an investigation who must review the case data in a timely manner, including Human Resources representatives, legal departments, members of the District Attorney's office and so on. The landscape has changed in such a way that a simple computer forensic tool just doesn't cut it anymore. The practice of juggling products to achieve the level of analysis required, then hand delivering case data for review does not scale to meet the demands of an ever-growing case load.

This is why AccessData has designed a suite of forensic investigation technologies that fit together seamlessly, wrapped in a single, easy-to-use interface. By integrating capabilities, such as mobile phone analysis, distributed processing, division of labor and web-based task management into the Forensic Toolkit platform, you can work more cases faster. Simply choose the enhanced capabilities you need, and build the solution that's right for your organization. Over time, if your needs grow, you can build on to your existing components to stay ahead of the curve. The technologies discussed herein are the most stable, most integrated and most flexible forensic solution available, delivering the power to handle the largest data sets with speed, accuracy and efficiency. The result is a more effective investigative process that saves you time... and ultimately, money.

BUILDING AN EFFECTIVE, EFFICIENT FORENSICS SOLUTION...



Forensic Toolkit® 3.X

A Foundation Built for Speed, Analytics and Enterprise-class Scalability...

Forensic Toolkit (FTK) 3.X enables a new approach to digital investigations with enterprise-class architecture and an embedded Oracle database that scales massively to handle the largest data sets and caseloads. Every copy of FTK 3 comes with a total of 4 workers (1 worker on the examiner machine and 3 distributed workers) to enable distributed processing and dramatically reduce processing and indexing time. Unlike other solutions, its database-driven, compartmentalized architecture virtually eliminates the crashing and lost work associated with memory-based technology. It includes AccessData's cutting-edge cracking and decryption technology, and delivers some of the most advanced features available in computer forensics solutions today. Furthermore, this leading forensic platform lays the framework for seamless expansion, so your solution can grow with your organization's needs.

Benefits of the FTK® Architecture:

Integrated Solution: Create an image, view the registry, conduct an investigation, decrypt files, crack passwords, and build a report with a single solution.

Distributed Processing: Every copy of FTK comes with 4 workers—3 distributed and 1 on the examiner machine.

Handle Massive Data Sets without the Crashes: The embedded Oracle database scales massively, and due to FTK's architecture, if the GUI crashes, the workers continue to process data.

Enterprise Architecture Allows for Expansion: The solution can be easily expanded to include collaboration, case management and increased distributed processing capabilities.

Get to Relevant Data Faster: The overview tab automatically categorizes data into different groups by status, extension and type.

Advanced Functionality:

Market-Leading Cracking and Decryption Technology of PRTK® and DNA®: Support for 100+ data types.

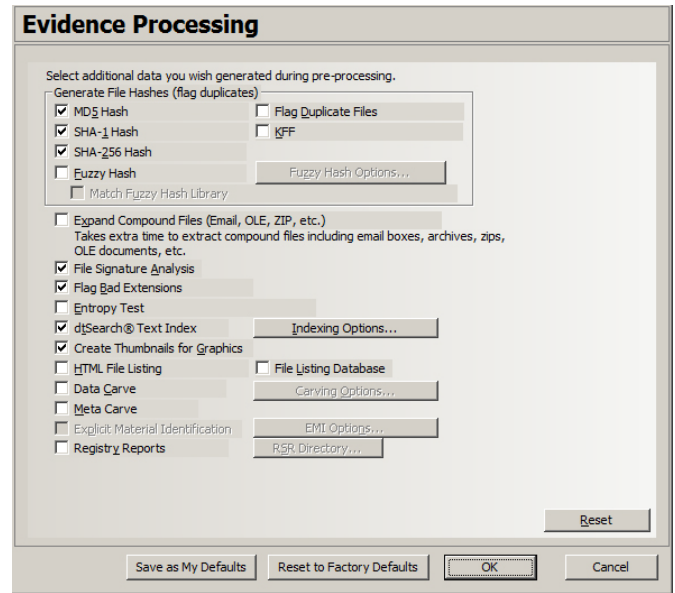
Unicode and Code Page Support

Customizable Interface: View data in 100s of different ways with dockable windows, user-definable tabs, the ability to rearrange metadata columns and the ability to resize gallery view graphics in a separate window.

Unsurpassed Email Processing and Analysis: Automatically break out email and attachments with support for 11+ different email formats.

Advanced Data Carving Engine: Specify criteria, such as file size, data type and pixel size to reduce the amount of irrelevant data carved.

Powerful, Wizard-Driven Reporting Engine: Export detailed reports in more than 7 different formats, including PDF, HTML, RTF and XML.



Pre-processing Refinement : Exclude irrelevant data as you load it, greatly reducing processing time.

Acquisition & Analysis of Live Data with FTK® ...

RAM Dump Analysis

- Enumerate all running processes, including those hidden by rootkits, and display associated DLLs, network sockets and handles in context, from 32-bit windows machines.
- 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.
- Process RAM captures for additional forensic artifacts, such as passwords, html pages, .lnk files and MS Office docs.

Live Device Acquisition

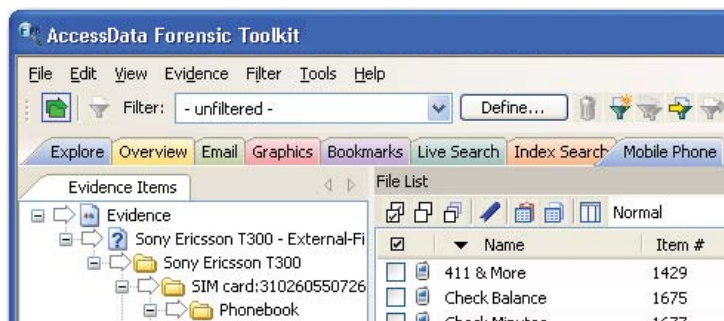
- Perform network-based, secure, single-system forensic acquisition of physical devices, logical volumes and RAM.
 - Image the full range of system memory
 - Image entire physical device or devices
 - Image an entire volume or volumes
- The agent can be quickly deployed and does not require installation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

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.

FTK® Mobile Phone Examiner

Add Integrated Mobile Phone Analysis to your FTK Solution.

- Supports 600+ phones with more on the way.
- Correlate mobile phone data with computer evidence and data from other phones.
- Analyze multiple phones within the same interface.
- Acquire phone data in a forensically sound container without altering mobile phone data.
- Analyze phonebook, last dialed numbers, missed calls, received calls, SMS messages, multimedia messages, photos, files, phone details, calendar, notes, tasks and more.
- Direct SIM analysis through SIM reader.
- Read deleted messages from the SIM card, when possible.
- Generate reports that include both computer evidence and mobile phone evidence.
- Includes SIM reader and USB communication cables and drivers

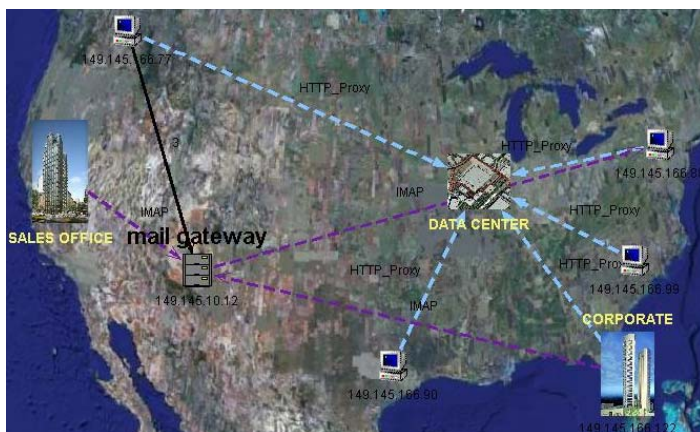


When plugged into FTK, a separate Mobile Phone tab appears in the interface. The solution detects any connected mobile phone devices and prompts you to select the devices you wish to acquire.

SilentRunner™ Sentinel™

Get a 360-degree view into all data by achieving real-time network data capture and advanced visualization.

When investigating a crime, security incident or malicious employee activity, investigators and analysts know they should leave no stone unturned. Yet, it is impossible to get the whole picture when using only a stand-alone forensic tool. SilentRunner Sentinel operates like a surveillance camera, passively monitoring real-time network activity and delivering dynamic, graphical visualization of communication flows. This allows you to swiftly uncover break-in attempts, weaknesses, abnormal usage, policy violations, misuse and anomalies. Furthermore, Sentinel can play back events from thousands of communications, enabling you to validate and deeply analyze criminal activity, system threats and security breaches. This level of visibility greatly enhances your ability to identify offenders and track their activity, determine root cause, and mitigate the recurrence of a security incident. With appliance-based collectors, pre-loaded on Dell R900 servers, SilentRunner Sentinel is now a plug and play solution, with easy deployment and configuration.



Visualize nodal communications and expose patterns or hidden data relationships.

- Use with FTK or AD Enterprise to achieve a 360-degree view into all data — host-based static data, RAM and network traffic data.
- Capture network traffic at full gigabit network line speeds.
- Advanced visualization graphically illustrates nodal communications and data propagation.
- Forensically record and analyze unlimited amounts of network data.
- On-demand incident playback allows you to replay events exactly as they occurred.
- Web-interface allows you to navigate through the data from any perspective and provides centralized command and control of the collection engines.
- Monitors 1,500+ services and protocols out of the box.
- Red Hat Linux-based collection platform—much more stable OS and a guarantee of complete packet captures.
- Integration with Oracle 11g means powerful processing and indexing, and faster insertions and extractions of data.
- Improved query speed for VOIP, email and web-based reporting.
- Dynamic protocol/service identification means collections are no longer port-based. They're dynamically identified by the packet information.
- Schedule tcp dump captures along with immediate hashing of the output files to ensure forensic integrity, which is useful for lawful interception at ISPs.

AccessData® Lab and Lab Lite

Work more cases — faster.

A single investigator working a case from beginning to end on a single computer will never gain control over an ever-growing case load. AccessData technology allows you to take a new approach. We offer two powerful solutions, delivering critical capabilities that will allow you to work more cases faster. Increased processing speeds, division of labor with seamless collaboration, and an easy way to manage your staff and monitor productivity will allow you to achieve a more efficient work environment and greater control over your case load — all without having to hire additional resources.

FUNCTIONALITY	AD LAB LITE	AD LAB
Distributed Processing	INCREASED	INCREASED
Investigator Collaboration	UNLIMITED	UNLIMITED
Case and Task Management	YES	YES
Role-based Permissions to Control Access & Activity	YES AT THE CASE LEVEL	YES AT THE DATA LEVEL
Web Review & Analysis	NO	UNLIMITED

What Does This Functionality Mean For You?

Centralized Investigative Platform: Using the Lab platform, organizations can centralize their investigative infrastructure. Instead of all the processing, indexing and storage of data occurring on an single examiner machine, each examiner can leverage a shared infrastructure that can include a centralized Oracle database(s) and a distributed processing farm. This is where all of the case data is processed, indexed and stored. Access to each case is still controlled by the lab manager or the examiner in charge of a specific case, but the actual hardware infrastructure, where all the work takes place, is centralized. While this lab platform enables real-time collaboration, a single analyst is still able to work an entire case from beginning to end on his or her machine. Each analyst has an investigative workstation that shares a single Oracle infrastructure, comprised of one or more databases. Examiners can authenticate and easily connect to other examiners' databases to view and support each other's cases in a collaborative manner.

Distributed Processing: Get to the analysis phase faster by leveraging additional hardware to greatly reduce processing time.

Investigator Collaboration: Investigators no longer need to play the jack-of-all-trades game. Lab managers can leverage the core competencies of their investigators by assigning tasks aligned with their skill sets. Through division of labor, an investigator particularly adept at email analysis can focus on email, while another skilled in the analysis of Internet artifacts can focus on that area of the investigation.

Case and Task Management: Easily assign cases and specific tasks to investigators and monitor progress via an easy-to-use web interface. Notify investigators when new tasks have been assigned to them and allow examiners to update their status and progress.

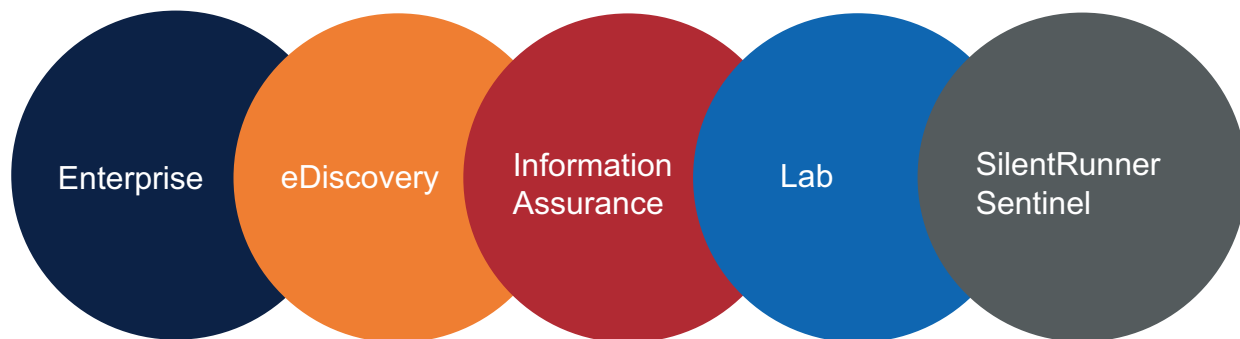
Role-based Permissions: Ensure security by leveraging the role-based security function that comes with Lab Lite and AD Lab. With Lab Lite role-based security controls access on the case level, while AD Lab can control access on a more granular basis, at the data level.

Web Review & Analysis: With AD Lab, cases can be reviewed by parties who do not have FTK or Enterprise. This allows every player in an investigation to utilize a single solution to perform their respective tasks. Non-forensic parties in the investigative process, such as lawyers and human resources representatives, can review case data, bookmark items and make comments



The Web review interface makes it easy for all parties involved in an investigation to review and comment on the data, even those with no forensic tool training.

THE ACCESSDATA® PLATFORM FAMILY OF PRODUCTS



Build an investigative solution to meet your organization's specific needs. This enterprise-class collection of products is designed to allow you to expand your investigative capabilities as your needs grow and evolve. The following enterprise building blocks work together to deliver visibility into all data, unmatched investigative reach and the utmost efficiency.

AccessData Enterprise

- ✓ No scripts — all functionality is in the GUI.
- ✓ True Auto Save/Recovery functionality.
- ✓ Forensically acquire RAM and devices.
- ✓ Schedule bulk acquisitions of RAM and devices.
- ✓ Integrated Incident Response Console — correlate processes, sockets and ports in a single view across nodes.
- ✓ Live memory search and analysis.
- ✓ Right click process kill functionality.
- ✓ Wizard-driven processing, filtering and reporting.
- ✓ Computers “Check In” automatically, enabling capture and analysis of data from machines, no matter where they are.

AccessData Information Assurance (coming soon)

Enhances identification of compromised hosts, enables large-scale data auditing and secure remediation.

- ✓ Proactively identify changes to machines across time.
- ✓ Pinpoint the source and extent of a security incident, whether a data leak or malware outbreak.
- ✓ Generate rich reporting on the state of nodes, identifying unknown and unauthorized processes.
- ✓ Perform large-scale data audits, mapping where data lives, who owns it and what it is.
- ✓ Perform secure file collection and remediation, and replace expired or privileged data with stub documents pointing to an alternate location.

AccessData eDiscovery

A complete turnkey solution for internal litigation preparedness.

- ✓ Web-based review platform delivers cutting-edge analytics and collaborative review of ESI.
- ✓ Advanced early case assessment capabilities.
- ✓ Enables sophisticated searching methodologies.
- ✓ Forensically collect data from workstations, laptops, network shares, email servers, databases and more than 30 structured data repositories.
- ✓ Rich reporting with strong chain of custody support.
- ✓ Automated processing and deduplication.
- ✓ Load file creation.
- ✓ Rich workflow with integrated matter and custodian management.

SilentRunner™ Sentinel™

Visibility into network traffic to complete the investigative picture and properly remediate security breaches, data theft and policy violations.

- ✓ Capture network traffic at full gigabit network line speeds.
- ✓ Works with AD Enterprise to deliver 360-degree view into all data — host-based static data, RAM and network traffic data.
- ✓ Advanced visualization graphically illustrates nodal communications and data propagation.
- ✓ On-demand incident playback allows you to replay events exactly as they occurred.
- ✓ Forensically record and analyze massive amounts of network data.
- ✓ Monitors more than 1,500 services and protocols out of the box.
- ✓ Dramatically improve your ability to identify perpetrators and determine root cause.