

AccessData Lab



STREAMLINED INVESTIGATIONS
THROUGH COLLABORATION
AND CASE MANAGEMENT



AccessData[®]
A Pioneer in Digital Investigations Since 1987



Conquer your caseload through division of labor, collaborative analysis, centralized case management and Web-based review...

Computer forensics units throughout the world are inundated with ever-growing caseloads and increasingly massive data sets. AccessData (AD) Lab was developed specifically to help forensics labs gain control over their caseloads by enabling examiners to work more cases faster. The traditional model, in which one examiner works a case from beginning to end is not always the most efficient approach. Now that most forensics labs are overwhelmed with work and limited by budgetary constraints, finding a solution that amplifies existing resources while increasing efficiency has become a top priority.

AccessData Lab is a centralized investigative platform that enables division of labor, collaborative analysis, centralized case management and Web-based review, thereby dramatically streamlining the investigative process. Furthermore, AD Lab enables distributed processing, allowing you to utilize additional hardware to dramatically increase your processing speed.

Multiple Examiners Can Work Collaboratively on a Case

With AD Lab, multiple investigators are able to work on a case simultaneously, each focusing on their respective strengths. For example, an analyst particularly adept at email investigations could focus on email, while other investigators focus their attention on graphics or Internet artifacts. With this “divide and conquer” approach, high priority cases can be turned around at speeds that no single investigator could achieve.

Individual Examiners Can Work a Case from Beginning to End Using a Shared Investigative Platform

While this platform enables collaboration, examiners are still able to work an entire case from beginning to end on their own workstations. However, all case data is stored in a centralized location, and if desired, an examiner can give permission to a colleague or non-technical personnel to view and comment on his or her case.

Examiners and Non-technical Parties Can Review and Comment on Case Data via the Web-based Interface

AccessData Lab allows both forensic examiners and those without any computer forensics training to review and comment on data through a secure Web interface. This enables both computer forensics colleagues and non-technical players, such as attorneys, human resources personnel and outside experts to participate in the investigative process without delay, regardless of their locations.

Managers Can Assign Tasks and Monitor Progress via the Central Management Console

For the lab manager, AD Lab offers an easy-to-use, centralized Web portal from which to manage the lab’s case work. Using an extremely simple interface, the manager is able to assign cases and tasks to investigators and track the progress of individual investigations. Granular role-based permissions allow you to control who is able to view specific data sets (i.e. create review groups) — for both the FTK users and the Web reviewers. For example, Forensic Examiner A can only view email, while Attorney Web Reviewer B can only view files that have been labeled “Responsive”.

The screenshot shows a web-based task management interface. At the top right, it says "Welcome Administrator" with links for "Home" and "Logout". Below that are buttons for "+ New Task Assignment" and "Refresh Tasks". The main content is a table with columns: Task Name, Assignee, Status, Due Date, Progress, Priority, and Notes. The table lists several tasks, including "Create Report", "Review Assigned Data", "Review Email", and "Update Status", each with an assigned person, status, due date, progress bar, priority, and notes.

Task	Task Name	Assignee	Status	Due Date	Progress	Priority	Notes
Task: Create Report	Create Report	jpeterson	Assigned	10/31/2009	80%	Medium	Create a report on the evidence in this case.
Task: Review Assigned Data	Review Assigned Data	mhudson	Assigned	10/13/2009	0%	Low	Review the data for any responsive files. Label them, create a production set, and export into an AD1.
Task: Review Email	Review Email	jperschon	Assigned	10/22/2009	50%	High	We suspect there are credit card numbers in the email. Utilize the email threading tab to find them.
Task: Update Status	Update Status	adorais	Assigned	10/13/2009	0%	Low	Check the Status on this, please.

Assign tasks and track progress via a central management console.

The benefits of a centralized investigative platform...

Collaborative Analysis

- By utilizing an “assembly line,” division-of-labor approach, the investigation process is streamlined and cases can be brought to completion more efficiently.
- Control who can see which data in a given case or across cases. You can apply these restrictions to both the FTK users and those viewing data via the Web Review Console.
- Examiners can see each other’s results in real time.
- Non-technical users can easily support the investigative process, because FTK users and Web Review users can collaborate on a case at the same time.

Advanced Technology: Review and Analytics

- Email discussion threading allows you to view an entire discussion in chronological order, including all replies, carbon copies and forwards, so you can easily determine who was involved and what was being communicated.
- Advanced tagging/labeling options for custom and bulk tagging with annotation pop ups and 3 way (include/exclude/neutral) label filters lets you quickly toggle between coded and un-coded documents.
- Leverage sophisticated searching capabilities, with relevancy ranking, hit highlighting in files, emails and attachments, and Search History reporting.
 - Boolean, Proximity, Stemming, Related Words, Phonic, Wildcard, Synonym, Concept and Fuzzy with sensitivity slider.

Using AccessData Lab for eDiscovery

Deduplicate across the matter or within custodian/evidence groups.

Export responsive-only documents and email (reduced PST or NSF) in native format or as an AD1 forensic archive, organized by custodian or as a single instance, with options to preserve the original folder structure.

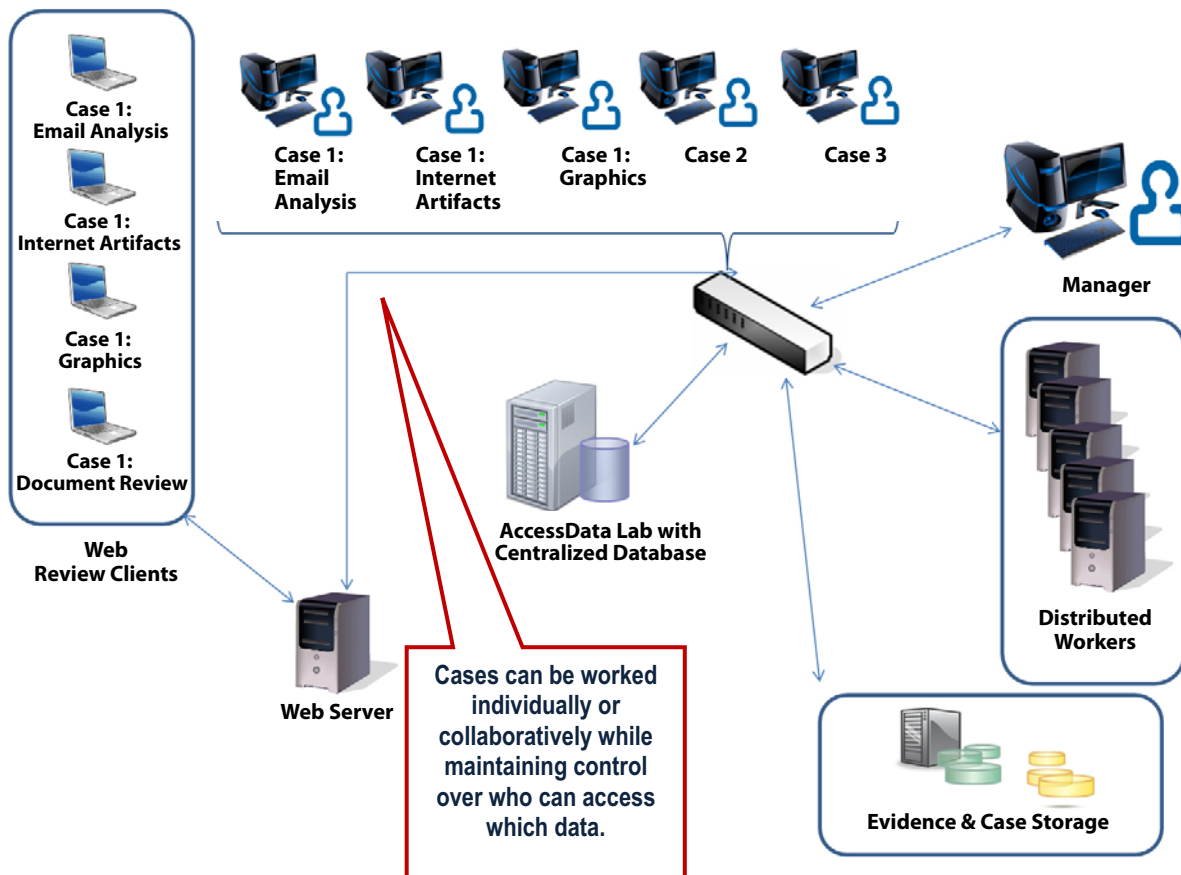
Generate load files for export to popular third-party review tools, including Concordance, EDRM XML, Summation, iCONNECT and Introspect.

AD Lab enables detailed production reporting, such as transparent search reports, processing exception reports, production and exclusion reports.

Enterprise-class Architecture

- Take an enterprise approach to controlling data with a centralized investigative platform, instead of each examiner storing data on his or her individual machine.
- Creating a collaborative environment with a shared infrastructure amplifies existing resources, allowing analysts of all skill levels to work more effectively, while saving time and money.
- Utilize a distributed processing farm to greatly reduce processing time.
- Leveraging a computer forensic solution that handles larger data sets than any other tool on the market.
- AD Lab leverages your existing AccessData investment, so you can build upon what you already own.

HOW IT WORKS:



Solution Highlights:

Manage multiple cases and multiple examiners...

- Examiners in **distributed labs** can **work together** on the same case.
- **Assign tasks** to multiple analysts and **monitor progress**.
- **Role-based case access** controls who can view which cases.

Collaborative analysis streamlines the investigative process...

- Collaborate on the same case at the same time, utilizing a **division-of-labor** approach.
- Examiners can each work their own cases, sharing a **centralized infrastructure** for storage and processing.
- **View each others'** cases to support each other throughout an investigation.
- Examiners using FTK and non-technical Web Review users can **work a case at the same time**.
- **Web Review Console** delivers advanced analytics and is easy to use.
 - o Email discussion threading
 - o Sophisticated searching capabilities: Fuzzy, Stemming, Related Words, Phonic, Wildcard, Proximity and Concept
 - o Search hit highlighting in files, emails and attachments
 - o Search relevancy ranking
 - o Advanced tagging/labeling options
 - o Bookmark items into categories and include comments
 - o Split screen support
 - o And more...

Enterprise-class, centralized architecture for ease of use and efficiency...

- Oracle database enables **simultaneous collaboration**.
- Centralized processing, indexing and data storage.
- Examiners can leverage a **distributed processing farm**.
- Fully leverage the **cutting-edge analysis** capabilities of Forensic Toolkit® technology.
 - o **Customizable** interface
 - o Advanced data modeling
 - o Unsurpassed **email analysis**
 - o **Memory** search and analysis
 - o **Wizard-driven** processing, searching and reporting
 - o And more...

The screenshot displays the Silverlight Web Review interface. On the left, a file explorer shows a directory structure with folders like 'Archives', 'Colton', 'Documents and Settings', 'Levels', 'Program Files', 'WINDOWS', 'Share', and 'Stuff'. The main area shows a list of files with columns for Position, Labels, Object Name, and Extension. A search bar at the top allows for 'Simple Search...'. A text viewer on the right shows a document titled 'Before the storm' with text about a tornado in the Salt Lake Valley. A red callout box points to the interface with the text: 'Silverlight Web review interface makes it easy for both computer forensics examiners and non-technical personnel to view and comment on evidence, regardless of their locations.'