

Clearwell Digital Investigations Solution

THE BENEFITS:

SOLVE DIGITAL INVESTIGATIONS 10 TIMES FASTER

Information technology and security professionals at enterprises and governmental agencies have realized immediate and significant results using the Clearwell Digital Investigation Solution. The solution's benefits include:

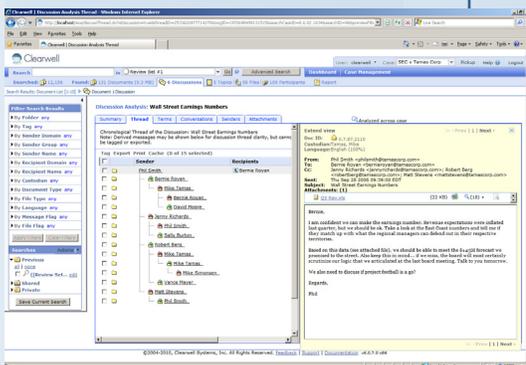
- Solve digital investigations quickly and accurately
- Easily collect suspect data from relevant data sources
- Rapidly identify all the participants involved in an investigation
- Quickly deliver all the evidence to internal sponsors online
- Eliminate the manual review of thousands of false positives

The Challenge: More digital investigations, more email and documents, but no more time.

Information technology and security teams face tremendous pressure along every dimension. The number of digital investigations continues to grow, as does the amount of electronically stored information requiring analysis. Deadlines are increasingly aggressive, raising the urgency around finding all the evidence and accurately determining who knew what, and when. Moreover, controlling costs remains a pressing concern, preventing teams from adding more people to cope with the ever-increasing workload.

In seeking to meet these demands, information security teams have relied on traditional technologies and workflows. These manual workflows often involve investigators collecting data across the enterprise using multiple tools, applying simple keyword search techniques and reviewing gigabytes of data document by document. Because of this, today's digital investigation process is onerous and time-consuming, requiring a large number of manual steps and significant re-work which, in turn, costs millions of dollars and leaves the organization vulnerable to substantial risk and financial exposure.

The Solution: The Clearwell Digital Investigation Solution



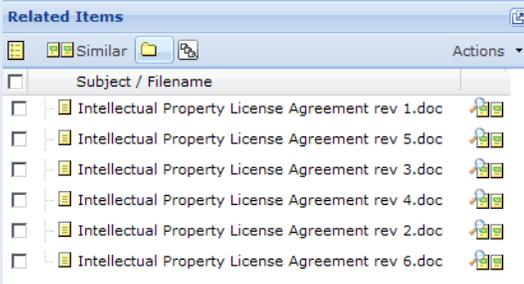
Discussion Threads

Automatically links emails into threads allowing investigators to rapidly traverse the life span of an email

The Clearwell Digital Investigation Solution is designed to streamline the digital investigation process, helping investigators handle more investigations in less time while improving the accuracy of the results. The solution forensically collects electronic files from across the organization, automatically analyzes the data, and enables investigators to rapidly identify all evidence and suspects involved in a digital or government investigation. Key capabilities of the Clearwell Digital Investigation Solution include:

Analyze emails, attachments, and documents in minutes: Clearwell is operational quickly, allowing investigators to begin their e-discovery process sooner and understand the context of the investigation across the collected data set. As a single application for the entire e-discovery lifecycle, Clearwell provides the capability to collect from all critical enterprise data sources, process data immediately, and begin analysis without moving data between multiple standalone tools. As a result, investigators gain earlier access to the evidence, providing visibility to understand the issue and quickly conclude investigations.

Rapidly collect data in a defensible manner: Clearwell's collection capability allows information technology and security teams to easily collect suspect data from multiple critical data sources including email servers, employee computers, file servers, SharePoint™, and applications in the cloud. During the collection process, Clearwell verifies the integrity of the data before and after collection, ensuring data is forensically sound and providing a defensible audit trail that can be used to document chain of custody.



Find Similar

Enables investigators to quickly understand the scope of an idea across the collected evidence

"Clearwell has clearly made the existing resources more efficient in performing their work and enabled them to handle more than we have a right to ask of them. With Clearwell my team is twice as productive as it was before."

JONATHAN CHOW
CHIEF INFORMATION SECURITY OFFICER
NBC UNIVERSAL



Clearwell Systems, Inc.
441 Logue Avenue
Mountain View, CA 94043
650.526.0600 tel
650.526.0699 fax
www.clearwellsystems.com

Determine exactly who knew what, and when: Clearwell's Discussion Thread feature links together all related messages including all replies, forwards, CC's and BCC's, and provides a chronological thread of the entire discussion. By walking the thread, investigators can quickly determine who knew what, and when, as well as identify all the participants, all emails, and all attachments related to their particular investigation.

Quickly discover the most relevant evidence: Employing linguistic analysis techniques, Clearwell suggests keywords and topics that are present in the data, providing investigators with a conceptual overview during the early stages of the investigation. Clearwell's Find Similar feature allows investigators to easily identify and view all items with similar content to the document under review, revealing the scope of an idea across the entire case.

Maximum investigation flexibility through advanced search capabilities: Clearwell allows investigators to search for specific phrases, dates, header information, user groups, locations, tags, and comments. Clearwell provides the flexibility to include text variations such as plurals and alternative verb forms in search results, and also provides exact matching via literal search. Power users can leverage advanced features such as wildcard, fuzzy, proximity, and Boolean searches.

Increase investigator productivity: Clearwell's rapid tagging capabilities allow investigators to easily categorize, track, and manage all emails, discussions, attachments, and documents for each case. Investigation teams can apply status codes, critical notes, and assign email and documents for review to any member of the investigation or sponsoring team. The solution's secure, role-based access enables teams to lock down investigators or sponsors to specific evidence associated with a particular case or set of cases.

Rapidly find all instances of critical evidence: Once a critical piece of evidence is discovered during an investigation, Clearwell can perform a reverse lookup across the entire case dataset to find the trail of evidence for a specific item throughout the case. Within seconds, this analysis identifies all those in possession of the evidence, as well as the location where all instances of the evidence exists.

Prove process integrity: Clearwell tracks every action taken by each investigator (e.g. login, logout, all searches and query terms, results, tags, print jobs, export jobs, and more) providing a full reproducible audit trail. Clearwell can automatically produce activity reports for any investigator and for any investigation across any time frame.

Produce proof and deliver results to internal sponsors: Clearwell provides a complete set of reports, documenting the relevant terms have been searched and resulting emails, attachments, and documents have been produced in a way that is defensible for potential downstream litigation. Once investigators have identified relevant evidence, internal or business sponsors can log in to the system to perform additional analysis, review, and redaction of documents.

To schedule a demonstration, contact a Clearwell sales representative at sales@clearwellsystems.com, or call us at **877.727.9909**.