Accuracy
in excellent company

An allegation has been made in your company, but does it warrant investigation? How should you go about it? Are bad actors destroying evidence? Can a document search find evidence that has been deliberately concealed?

Accuracy Forensic View is a bespoke Relativity application that turns these investigation challenges into advantages. It makes use of forensic images to find what bad actors may be hiding, finds signs of avoidance efforts and uses those traces to focus on who is concealing what evidence. Accuracy Forensic View kick-starts investigations and uncovers the truth, including immediately:

- Revealing missing documents and devices
- Uncovering any formatting, wiping and encryption
- Rebuilding mailboxes, user profiles and PCs

Accuracy Forensic View's analytics are based on years of experience in digital investigation techniques. Combining this smart approach with Relativity's power provides investigators and reviewers with the tools necessary to reveal the truth, all the while saving both time and money.

ACCURACY FORENSICS

INVESTIGATIONS

FORENSIC ACCOUNTING

DISCOVERY

CORPORATE INTELLIGENCE

WEBSITE:
discovery.accuracy.com

CONTACT:
discovery@accuracy.com

Accuracy Forensic View

Using guilty behaviour to assess new INVESTIGATIONS and REDUCE COSTS

WHAT ARE THEY TRYING TO HIDE?

Experience shows that many subjects of an investigation undertake a course of behaviour that reveals their mens rea (guilty mind). These guilty acts can be used to flag both suspicious employees and relevant evidence, which can in turn help to confirm whether an allegation is founded and sometimes even quickly crack the case. Just like a detective reading the body language of a suspect, cyber analysis of computer activity can wave a large red flag – alerting anyone who is looking.

ACCELERATING THE INVESTIGATION

An investigation requiring a document review can take weeks, months or even years to complete. Being able to immediately identify hot documents that have been destroyed by the main suspect(s) is extremely powerful. It gives the lead investigators the option to confront and "flip" the individual(s) involved, making it possible to quickly and efficiently get to the heart of the matter. In some cases, this initial effort may be sufficient to resolve the matter and close the investigation.

IS THERE REALLY AN ISSUE?

It is often a tough decision to initiate an investigation. Is this just a malicious complaint by a disgruntled employee? Is the cost and disruption necessary? Being able to quickly find signs of evidence destruction or concealment can be crucial to the decision-maker's thought process.

REDUCING TIME AND COST

Our initial red flag analysis can focus the work on the individuals with something to hide and can "seed" the document review with the hot documents that they were concealing. This can dramatically reduce the scale of the document review, especially if artificial intelligence and concept clustering are used to extrapolate the related population from the initial hot documents.

LETTING THE SUSPECTS DO THE HARD WORK FOR YOU

Almost every investigation includes at least one red flag relating to missing evidence or data destruction. Deletion of files or data is the most common red flag – users typically delete important evidence on the day that they find out about the investigation and then again on the day before the forensic data collection is performed. By comparing backups of mailboxes taken before and after an investigation becomes public, we can exploit the users' own efforts to hide evidence to reveal what is important. Another good place to start is recovering the history of a user's access to files that are no longer present, deleted, password protected or stored off-system, for example, on missing USB sticks.

Investigation red flags

Examples of the types of analysis

- Missing files and emails
- Missing devices and data sources
- Wiping and encryption
- PC system integrity issues
- User profile integrity issues
- Outlook email integrity issues