

## Analytic & Forensic Technology



---

Deloitte's international network of member firms and affiliates operates computer forensics labs across the globe, giving our professionals unparalleled access to industry leading facilities and expertise.

### Who we are

The Analytic & Forensic Technology ('AFT') practice of Deloitte in the Cayman Islands collects, organises, catalogues, and provides data for review by attorneys, accountants, and analysts. We provide computer forensics, electronic discovery, and data management/analysis services for clients involved in complex litigation, inquiries and investigations.

Our AFT professionals use leading software tools and methodologies to analyse and decipher electronic evidence, including files and data that may have been deleted or hidden from conventional detection.

As an example, Deloitte AFT professionals can :

- Recover data previously 'deleted' by the user
- Pinpoint data anomalies that might reveal potential fraudulent or criminal activity
- Precisely search and retrieve relevant information from electronic documents and data
- Detect patterns of e-mail correspondence to understand who's sending what to whom and what they are saying.

Deloitte's international network of member firms and affiliates operates computer forensics labs across the globe, giving our professionals unparalleled access to industry leading facilities and expertise.

We can help our clients with the following interconnected multidisciplinary skill sets which support the primary techniques of electronic data recovery, preservation, analysis and presentation.

## Computer Forensics

Our professionals can work with the client to navigate IT systems for evidence of malfeasance such as information deletion, policy violation or unauthorised access. A wealth of information may be recoverable from computer hard drives and backup tapes, including active, deleted, lost or encrypted files, or file fragments. Even files that were created but never saved may be recovered.

An electronic data investigation typically begins with capturing data from a computer by producing a duplicate image of the hard drive containing all resident data, including files that users may have deleted long before. This image is then preserved in a locked, fireproof safe for evidentiary and chain of custody purposes.

Our computer forensics professionals can then search a copy of the image for e-mails, documents, spreadsheet files, web downloads and other electronic data that may have been deleted or encrypted, or may exist only in fragments. Searches can be based on key words identified during an investigation or by a relevant date or time period. Such bits and pieces of information, when recovered and presented in an evidential manner, can have tremendous value in an investigation. Computer forensics may also be used to compare hard copy documents with their electronic counterparts to determine if the document has been altered.

## Electronic Discovery

In a complex business dispute, litigation or regulatory investigation, all companies face one certainty: the discovery process. Whether you're a litigation attorney at a law firm or in-house counsel at a corporation, responding to a discovery request involves a myriad of complex requirements for proper data collection, processing, hosting, review and production. The number of responsive documents can range from hundreds to millions, and each responsive, non-privileged document must be produced in an efficient, secure, easily accessible manner.

Our e-Discovery solutions help counsel and companies control the costs and mitigate the risks associated with the discovery process by:

- Maintaining chain-of-custody records and tracking activity to address authenticity of data and process concerns
- Providing experienced teams to recommend and implement solutions that fit the case at hand (and not a 'one size fits all' solution)
- Coordinating discovery efforts including documentation for process reproducibility and transparent reporting
- Applying sophisticated techniques and use of software designed to meet the specific and unique requirements for each project
- Maintaining data security protocols and preservation of meta-data
- Providing hosted environments for storage and access to discovery documents

## Data Analytics

Most of our electronic data analysis focuses on the underlying business transactional data contained in a forensic investigation. We take a systematic approach to data analysis that begins with assisting the client in locating, scoping, acquiring, testing and verifying data to identify and detect anomalies within data that could indicate potential wrongdoing.

Our industry standard and proprietary data analysis tools combine the principles of data matching, pattern recognition and data forensics along with our extensive experience in providing forensic accounting services. We can identify potential anomalies and relationships that may indicate fraudulent behaviour; our technology solutions can combine data from many disparate sources within an organisation, for instance, general ledger, payables, receivables, HR, or loan and derivative books, and compare it to fraud profiles and external reference databases. In the past, data inquiries have generally been reactive and relatively 'low tech,' usually requiring a tip off or a catastrophe to prompt the inquiry. Now, through the use of visual data mining techniques and targeted approaches, our professionals can electronically perform the data analysis. These technologies can make large-scale proactive pattern detection a reality.

## Contact

**Stuart Sybersma**  
Partner  
+1 (345) 814 3337  
ssybersma@deloitte.com

**Chris Rowland**  
Director  
+1 (345) 814 3304  
cmrowland@deloitte.com

**Nick Kedney**  
Senior Manager  
+1 (345) 814 2281  
nkedney@deloitte.com