



# Forensic Technology

Using Technology for Investigations and Disputes



# An organisation's IT systems, networks and computers contain vast amounts of data. The Forensic Technology team at BTG Global Risk Partners can turn this data into meaningful and useful information.

Some elements of this information are easily accessed, such as the large number of files often found on a central file server. Others, such as a person's actions on an email system, are less visible and are therefore more difficult to obtain.

Consequently, sourcing information for a particular purpose poses a number of challenges, including ascertaining where it might be hidden, sifting through large amounts of data to find it, or in some cases, discovering if it even exists at all.

In many disputes and investigations, decision-makers are often challenged to find specific information to aid their cause. Whether it is to assess the merits of a matter, determine the extent of an allegation or to comply with legal or regulatory obligations, finding the necessary information can be one of the most challenging aspects of the process.

Our experts have considerable experience in both leading and performing a wide variety of such exercises, large or small, complex or simple. We are able to discover the information you will need to evaluate a situation, undertake an investigation, or respond to a request.

## Our Services

- Electronic disclosure services and consulting
- Computer forensic investigations
- Mobile phone forensic investigations
- Web-review database services
- Electronic fraud pattern analysis
- Data mining and database analysis
- System security assessments

## Our Approach

We use superior experience, methodologies and tools to interrogate a wide range of information and data sources in an auditable, defensible manner. Uniquely, we have experts with specific experience in using the many systems employed in business, rather than just the specialised software used to interrogate data – allowing us to provide greater insight and to build flexibility into the process, as well as to explain what the data 'means'. We can 'translate' your requests into technical processes and explain in plain language what is possible and how it can help you.

In addition, we have acted as experts in a number of matters in courts worldwide, as technical consultants for negotiations on document submissions for governmental requests, and to help prove that document requests in legal matters were burdensome and disproportionate for clients.

## Case Examples

### *Governmental Investigation*

In response to a request from a governmental legislative body, we were asked to conduct a search through the IT assets of a multinational corporation in order to investigate allegations of fraud and bribery for contracts. The client had been accused of improper conduct in the bidding phase for several large governmental contracts and was required to go through a large number of documents to prepare for an inquiry. We helped recover lost data, organise and keyword search it, and present it in an effective fashion for web-review in a matter of a few weeks, which aided the client in successfully challenging the allegations.

### *Fraud Investigation*

We were asked to investigate allegations of director fraud for a company that had gone into administration. The business was very document intensive and more than ten million documents and files existed on its systems. This data had to be reviewed as quickly as possible and the entire process had to be completed in a manner which would ensure that any evidence found would be able to stand up to scrutiny in court if required. Over a terabyte (1,000 gigabytes) of data was processed in the matter of a few days, organised into a database and made searchable by keyword for web-review, whilst IT systems that were used in the day-to-day running of the business were copied, secured and made available for review. Within days, evidence was located that suggested wrongdoing on the part of a former director.

### *Laptop Investigation*

An individual suspected of the theft of banking details claimed that he had not received the details from an accomplice as was suspected, but from an unknown individual on the Internet. Relying on experience in tracing Internet communications, a comprehensive search found no details of such communication, which forced the individual to drop his argument.