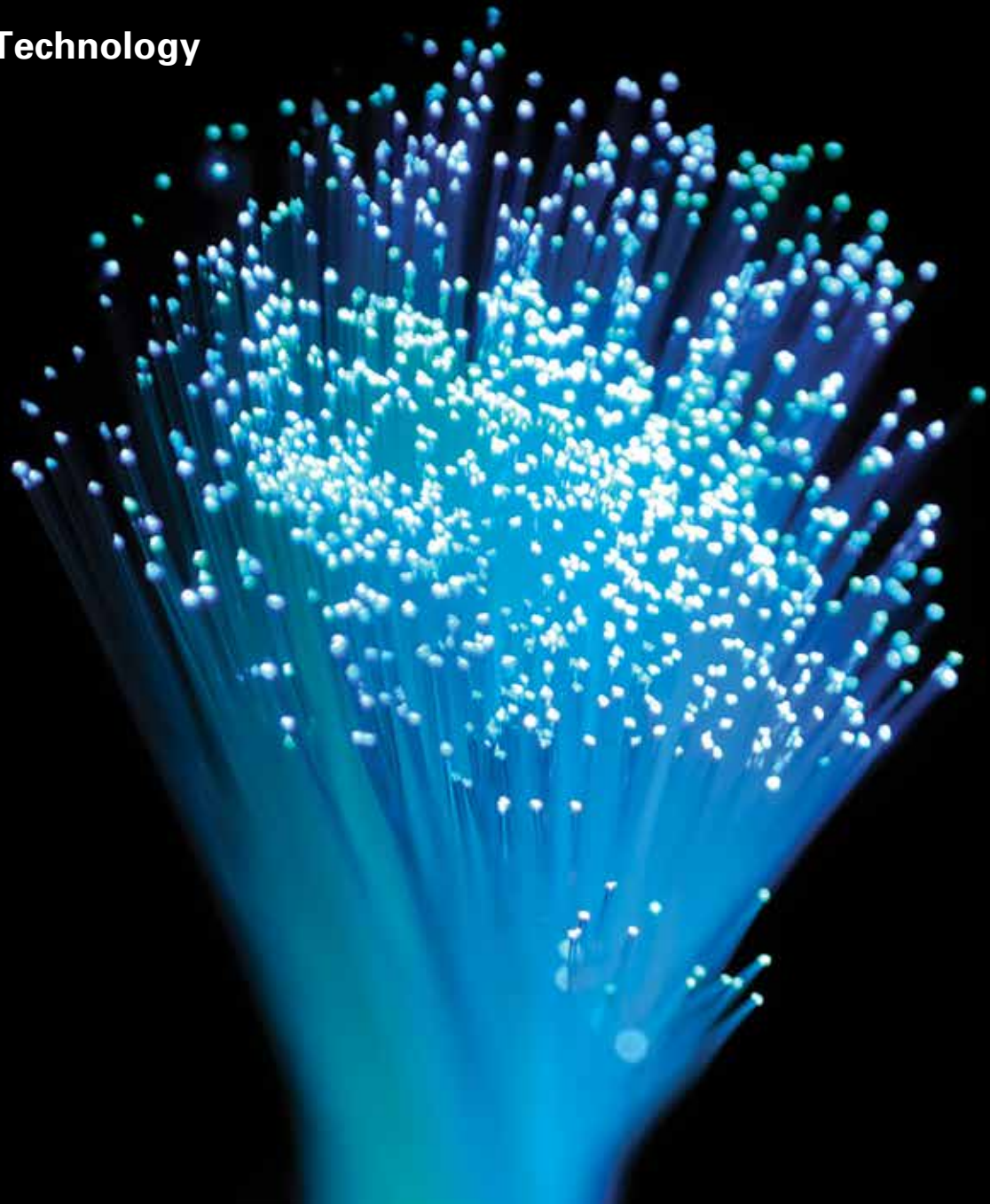




Digital Forensics

Forensic Technology



2017

kpmg.com/ae
kpmg.com/om

Contents

Technology and the 'Big Data' challenge 3

Digital Forensics 6

eDiscovery 8

Data Analytics 10

Technology and the 'Big Data' challenge

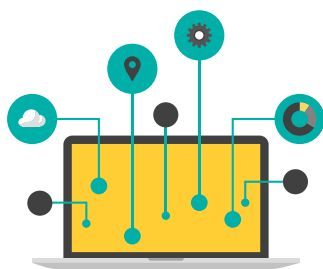
The amount of digital data created and managed by companies is growing exponentially. As a result, organizations face a variety of complex issues with digital data.

Whilst data analytics helps with structured data (such as data in a financial database), it is unstructured data (such as emails, office documents and media files) that makes up most of an enterprise's data volumes* and these volumes are growing at three times the rate of structured data!

Consider that when searching for answers in fraud, compliance, regulatory and litigation matters, only a fraction of this seemingly impenetrable unstructured data mountain is target-rich. The time and cost implications of sifting through this data mountain result in either

significant costs or ignoring/overlooking the relevant data altogether. This is why Technology is so important.

Our industry-leading technologies have been devised to allow our Forensic team and clients to find, recover and utilize this data in a speedy and cost-effective manner. Using analytics tools and best of breed software, we cut through the mass of data to identify relevant information and in turn establish the facts, whether in large international litigation or arbitration cases, investigations or regulatory and compliance matters.



MESA Hub

Our advanced facility, based in Dubai, acts as a hub for our Middle East South Asia (MESA) member firms. This ensures that data stays within the region. Adopting the model of having MESA-wide Forensic Technology professionals located across the region, as opposed to a centralized team, gives our clients a competitive advantage. A local team means that we are on the ground faster and supporting you as you manage the review process, without language or cultural concerns affecting the process.

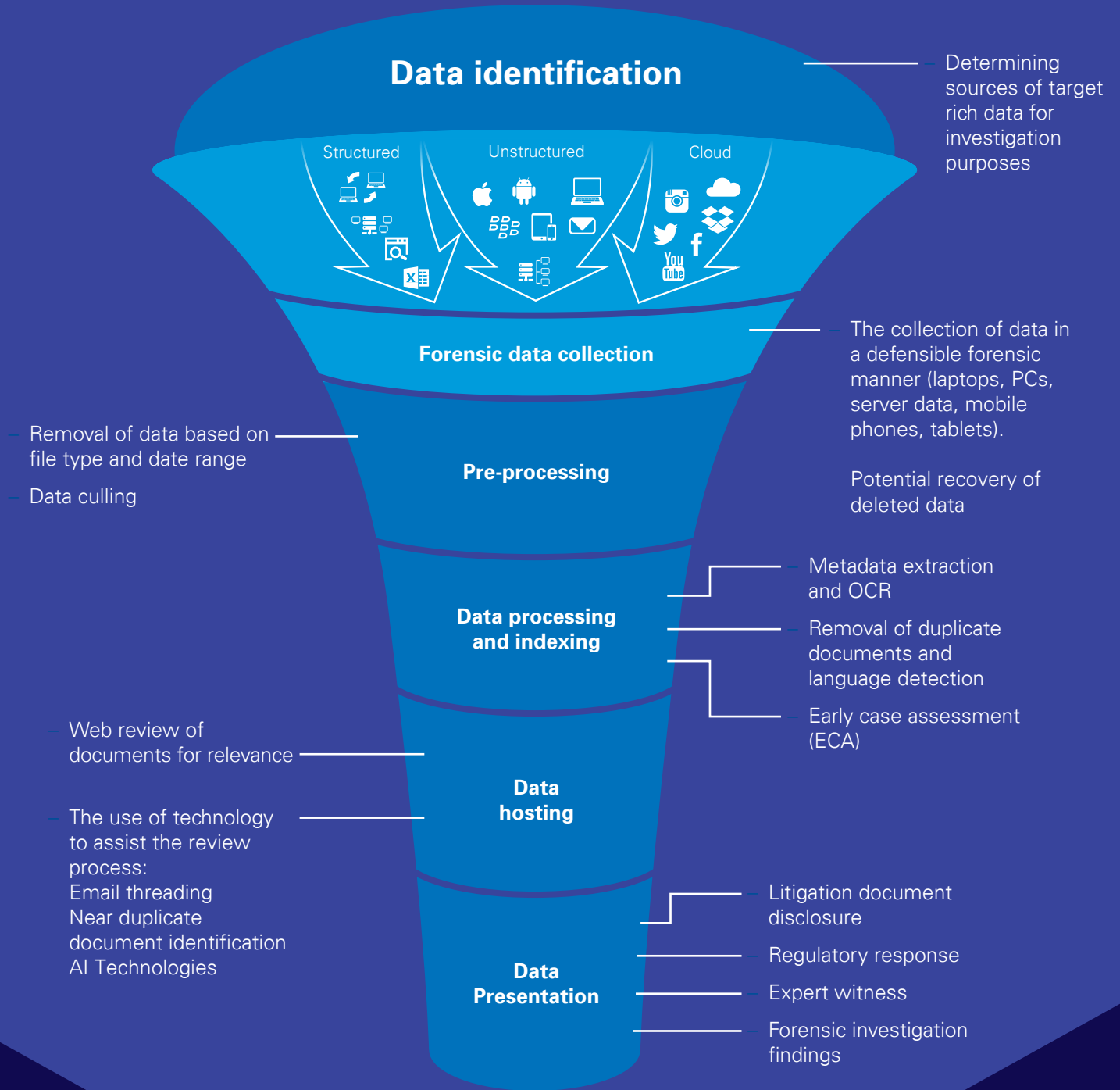


Our solutions and capabilities

Our Forensic Technology facility has been designed to give KPMG's clients a leading technology offering now and into the future. With several highly secure sub-networks, we offer the full range of Forensic Technology Services locally, namely:

- Digital Forensic Network that can analyze all types of computers, servers and mobile devices. This includes recovering deleted or hidden data, system logs, browser histories, and data misappropriation via USB or cloud storage.
- eDiscovery Network that can securely accommodate hundreds of external reviewers, such as investigators or attorneys, so as to conduct on-line document review.
- Cryptography Network that can unlock password-protected files, ensuring hidden information is revealed and our clients are not locked out of crucial information.
- Investigative Data Analytics Network that can identify fraudulent entries and other financial misstatements in the books of account.

Data management funnel

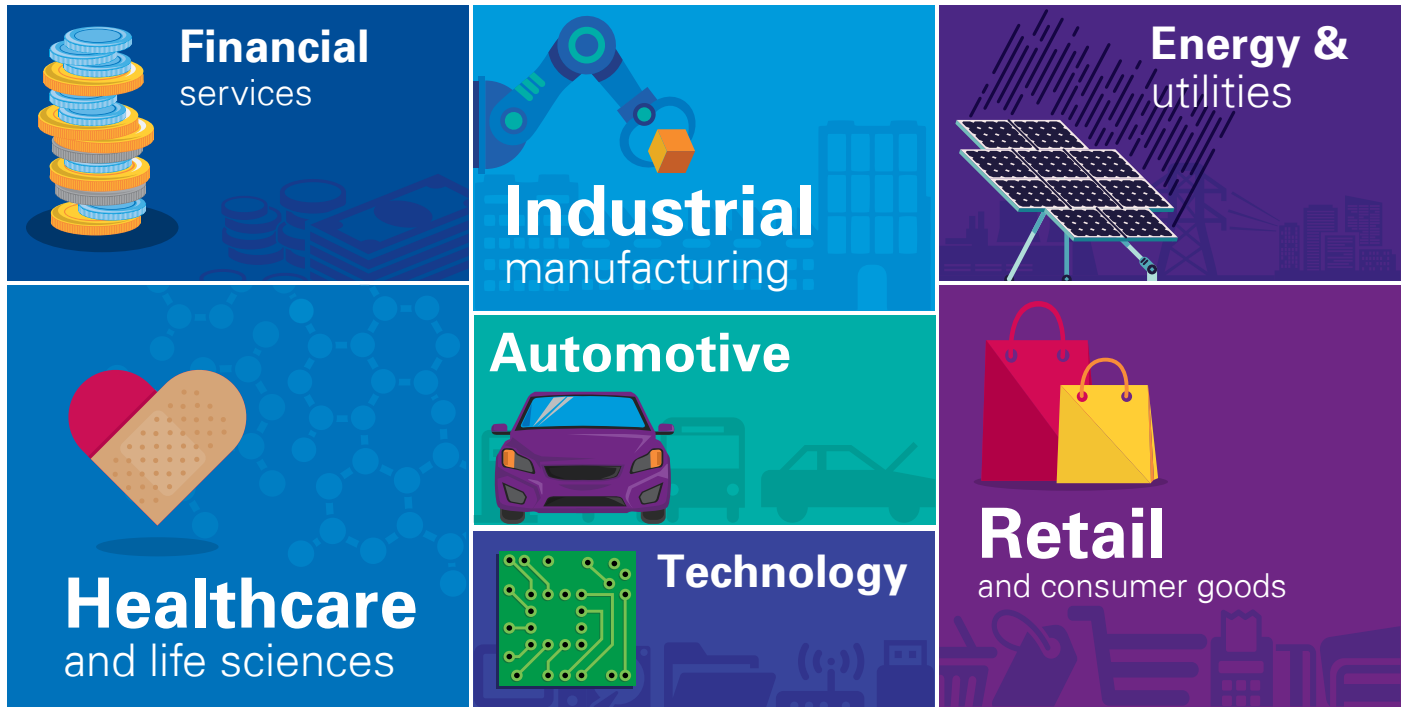


Data volume decreases

Data relevance decreases

Industry experience

We work with many of the world's leading organizations across a multitude of industries. Our professionals perpetually study and understand the industry landscape and the relationship between the various functional areas such as IT, compliance, legal and regulatory. Understanding the unique complexity and challenges that our clients face in their respective industries allows us to assist them in a meaningful way and helps us tailor an approach that will enable an effective and efficient (eDiscovery) implementation.



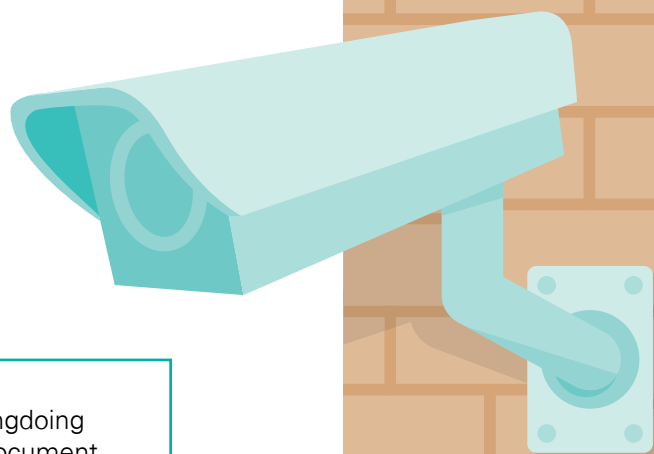
Global presence

KPMG's vast network means that we service our clients with a global delivery model. Our Forensic Technology teams are fully integrated and assist clients from all over the world in managing their respective business challenges.



By maintaining a global presence, KPMG is able to leverage the experience of colleagues through subject matter expertise and cultural knowledge in any respective geographical region. With our extensive global presence, we are well-positioned to support our clients and their projects.

Digital Forensics



Case Studies



Fictitious Document - HR Investigation

KPMG was engaged to investigate the alleged wrongdoing of an employee suspected of submitting a forged document with the intention to defraud our client. Our team of Digital Forensic Experts was able to recover metadata evidence from the electronic document to substantiate the allegation, as well as identify another employee who colluded & assisted in the creation of the fictitious document. With the help of our report, our client was able to prove the wrongdoing and initiate disciplinary actions against both employees.



Mobile Phone Examination – Procurement Fraud

KPMG was requested to examine a potential trade secret violation involving a senior Procurement Officer who was suspected of leaking sensitive and confidential bid-related information to a vendor, by taking pictures using his mobile phone. After a thorough investigation, our Computer Forensic team was able to recover the incriminating (deleted) pictures and corresponding WhatsApp conversation from the mobile phone. Using these as evidence, our client was able to initiate disciplinary action against employee.



Evidence Tampering – Timeline Analysis

The below case study is a testimony to our independence whilst conducting sensitive & complex investigations.

One of our clients accused an employee of tampering with a highly sensitive digital evidence file when the latter was in his custody. Following an investigation into this incident, KPMG was appointed by the General Counsel to submit a fact-finding report. Our team, made up of Digital Forensic investigators, went through millions of system and log files to reconstruct the timeline surrounding the event, thus enabling a better understanding of the actions which led to metadata change in evidence file.

Having identified the root cause of the incident, KPMG released a report stating that the tampering was purely accidental and not a result of any not a result of malicious intent. Our team further proved that neither the accused nor any other user had logged into the system to tamper with this sensitive file on the identified day of the incident. This fact-finding report, submitted by KPMG, enabled the General Counsel to make an informed and impartial decision.

KPMG’s extensive industry knowledge and commitment to providing excellent service is at the core of our Evidence Collection Service offering. Over the years, KPMG has accumulated experience across different industry organizations’ IT landscape and systems, providing a valuable holistic approach to Forensic Collections. Along with our experience implementing a variety of workflows, our global presence allows us to support any global organization while using local resources.

KPMG uses a combination of industry-leading forensic collection technology and internally developed solutions customized for the Investigative, Legal and Compliance global community.

As well as providing Forensic Collection and Preservation services, we have gathered significant experience in metadata analysis of digital evidence from multiple electronic sources (PCs, Laptops, Servers, Network Shares, Tablets, Mobile Phones, etc.).

Our bespoke solutions include:



We currently have the capability to non-intrusively collect data in the event of non-cooperation from users. By working with our client’s corporate IT team, we can gain access to a user’s laptop/desktop and without requiring any physical access to his/her laptop/desktop.

eDiscovery



Case Studies



Dispute Investigation – Key Evidence Gathering and Document Review

KPMG was engaged to identify potential data sources for a client involved in a long running dispute after the IT function had been replaced and the Senior Management and the Legal team were both unaware of where “potentially relevant” data was residing. Without this knowledge, our client was in a precarious position legally. An Identification and Data Mapping exercise had to be undertaken. The laptops and external drives of 25 custodians as well as server data was analyzed and considered to be critical to our client. We forensically collected the data and assisted our client’s legal team in its review. Key documents, once thought lost, had been found which in turn enabled our client to establish crucial facts and strengthen their case.



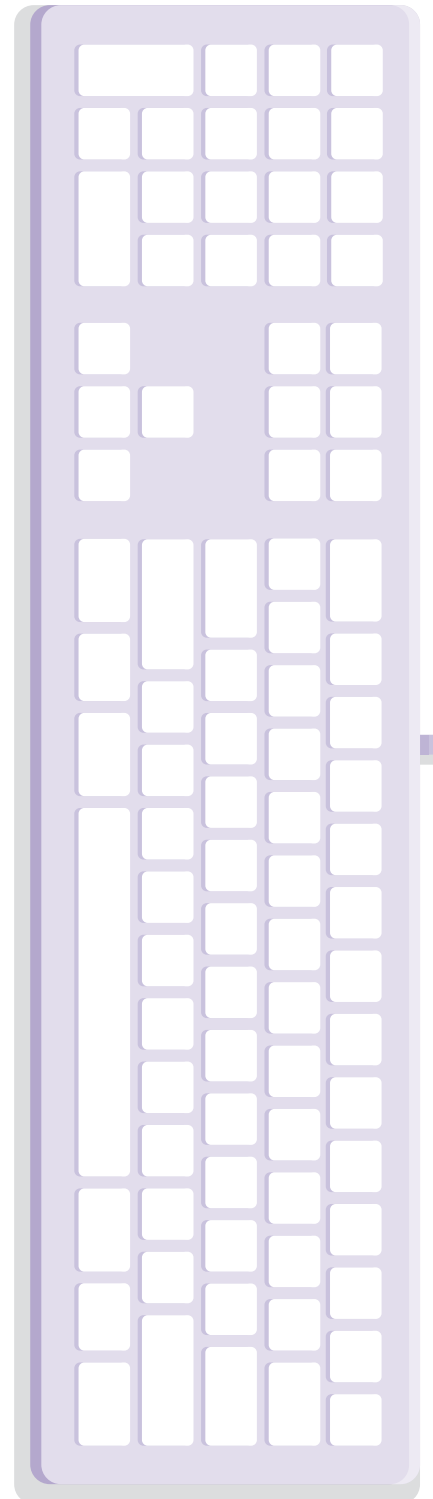
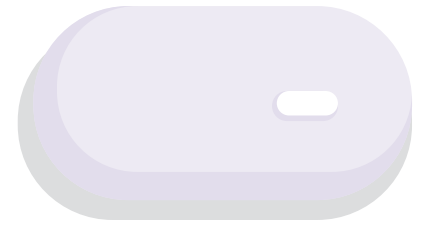
Dawn Raid – Internal Investigation

When one of our clients grew suspicious that the regional sales team had colluded in inflating sales figures, we were requested to execute a simultaneous forensic collection at numerous locations throughout the Middle East. This was a particularly sensitive case as in addition to HR matters, the client could face more serious actions from regulators due to the potentially misleading health and profitability of the company KPMG Senior Executives met with the client’s legal and IT functions to plan the data acquisition across multiple sites with the main objective to assess potential pitfalls. Having formulated a sound approach, the project was successfully completed and a full legal review could then take place to establish the facts.



Highly Sensitive Data – On-Premise Processing

Our client faced allegations of breaching trade sanctions and as a consequence, had had its assets seized. Since the matter was highly sensitive and had severe business implications, our client understandably had acute concerns regarding possible data leakage. KPMG proceeded with setting up a “mini forensic lab”. The latter was part of our solution to review and analyze the client’s data onsite. A senior KPMG team worked closely with the company’s IT function to forensically gather, preserve, search and review data on-site, behind a firewall. Subsequently, the data size was significantly reduced and only then did then client feel comfortable enough to release the data to defend the allegation.



Organizations increasingly face overwhelming amounts and diverse types of Electronically Stored Information (ESI). This data can result in a variety of complex issues and substantial costs, especially when attempting to comply with global regulatory concerns. The proliferation of enforcement activity, litigation, government requests and investigations has added a significant ever-increasing burden to the enterprise which KPMG is in a position to alleviate. Our data gathering and reviewing skills can also be used to assist companies facing potential internal issues, such as IP theft and HR disputes.

KPMG’s customized and thorough approach combines people, process and technology from the beginning to the end of the eDiscovery lifecycle. This enables clients to cost-effectively tackle today’s complex information landscape and discovery needs, making us one of the most suitable service providers. We guide our clients through the whole process, including:

- 

Identification
- 

Data Handling and Preservation
- 

Collection (PCs, Laptops, Mobile Devices, Network Shares, Servers)
- 

Data Processing and Culling
- 

Analysis, Review and Production
- 

Shutdown and Archive

KPMG understands the importance of innovation and keeps abreast of recent developments in eDiscovery and Forensic Technologies. In addition to proprietary technology solutions, we continually research and evaluate new technologies that provide value to our clients. Fundamentally, KPMG assists clients in discovering the facts underlying their matter expeditiously, while maintaining the defensibility of the process and managing risks in a cost-effective manner.

In the UAE, KPMG has a leading forensic technology data center and laboratory which enables secure analysis, processing and hosting capabilities, harnessing best of breed technologies.

Our services include:



Data Analytics



Case Studies



SEC Regulatory Investigation - Financial restatement

KPMG was appointed by the General Counsel to investigate the confessions of a CEO who alleged that the company's books were inflated to the tune of US\$ 1 Billion. The confession had a significant impact affecting shareholders, investors and the general public. It was one of the largest corporate scandals in the region. In response, our team of Structured Data Analytics experts secured the relevant data stored in various forms within numerous applications in a forensically sound manner, analyzing millions of rows of data to uncover the modus operandi behind this fraud. After our investigation, it became apparent that the revenues had been systematically inflated over a period of 7-8 years by creating fictitious employee IDs, customers, invoices, bank statements and fixed deposits to balance the books. Following the submission of our fact-finding report, the company's books had to be restated to reflect the facts.



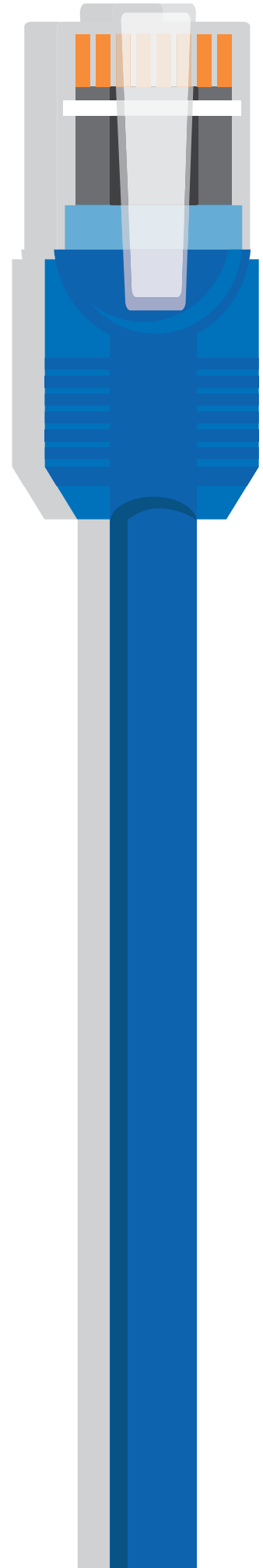
Payment Fraud – HR Investigation

KPMG was requested to review the bank statements of a company after the CEO suspected fraudulent behavior within the HR function. Our team of Structured Data Analytics experts analyzed the company's bank statements and identified several instances where HR had changed bank transfer instructions. The changes in effect meant that the salaries of former and exit employees were being diverted to an illicit bank account in order to extract the funds. As a result of our findings, the client initiated legal and disciplinary actions against the targeted individuals within the HR function.



Procurement Fraud - Link Analysis

KPMG was engaged to investigate a senior employee suspected of abusing their position to influence the procurement process. Our Structured Data Analytics team scrutinized the data available within bank statements and databases and managed to uncover some suspicious patterns. One particularly alarming red flag was the discovery of a senior procurement employee's bank account number which matched that of a vendor's. This triggered further investigation and subsequently led to the senior employee's confession of the fraud. Our client initiated disciplinary action against the said employee for non-disclosure of this procurement relationship.



Data analytics is the extracting and examining of data sets using specialized computer systems and software. Data analytics technologies and techniques are increasingly being used in various industries to enable organizations make better informed business decisions.

Data analytics techniques can effectively uncover critical trends and metrics that would otherwise be lost in a mass of information. This information can then be used to improve and optimize processes and subsequently increase the overall efficiency of a business or system.

Responding to our clients' need to make sense of and translate data into actionable intelligence, KPMG can now provide them with powerful data analytics services and tools. We can identify opportunities to stop fraud, waste, and misappropriation of resources that have a considerable impact on our client's bottom line.

These services are used to support a number of our offerings, including proactive and reactive fraud analysis, fraud risk assessments using risk-ranking methods, and strengthening anti-money laundering (AML) surveillance platforms.

We currently use the advanced tools and technologies to provide Investigative Analytics to the Regulatory, Investigation, and Legal/Compliance communities globally. Our services range from the collection, preservation and analysis of databases, to the intelligent analysis of data to find patterns providing operational insight into a company's activities, entity relationships and any possible hidden relationships between, for instance, employees and vendors.

Our bespoke solutions include:



Contacts us

UAE

Nicholas Cameron

Partner | Forensic

T: +971 4 424 8992

E: nicholascameron@kpmg.com

UAE

Obaid Kasmi

Director | Forensic

T: +971 4 424 8991

E: okazmi1@kpmg.com

www.kpmg.com/ae

www.kpmg.com/om

Follow us on:



@kpmg_lowergulf

kpmg-mesa



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. © 2017 KPMG Lower Gulf Limited and KPMG LLP operating in the UAE, member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International. Designed by The Design Studio UAE

Publication name: Digital Forensics

Publication number: J1203

Publication date: September 2017