State-of-the-art Forensic Technology
As it becomes increasingly imperative that information infrastructures and mobile access to data and information are constantly available to businesses, criminal acts and cases of non-compliance pose an ever greater threat.

Targeted electronic attacks on information systems, both by internal and external perpetrators, and fraudulent activities using electronic data processing tools make the headlines almost every day. The diverse use of computers, especially in the area of white-collar crime, places high demands on measures to combat this form of cybercrime.

KPMG Forensic meets these demands with forensic technology and an interdisciplinary team of IT specialists, investigators, auditors and lawyers. With the use of the latest, internationally recognised forensic tools, combined with our many years of experience in the area of computer forensics, we tackle every case with a comprehensive and targeted solution.

**Forensic Technology**

**Our four-phase case process**

1. **Identification of evidence**
   We identify the areas where electronic indications and evidence can be found, taking into account locally available data sources and network structures with external data pools (e.g. cloud services). Our investigations focus on all available data storage media – from laptops to the Unix mainframe, from mobile phones to GPS devices.

2. **Preservation of evidence**
   All evidence must be inventoried and secured to preserve its integrity; the aim is to map the digital footprint in a way that is admissible as evidence in court. This can be carried out either in our CYBERLAB specialist laboratory or directly at our clients’ premises. We locate deleted or hidden files (or fragments) and preserve evidence that the perpetrators believed to be untraceable. Neither the original data nor the systems are compromised or impaired in this process.

3. **Analysis of evidence**
   With the use of powerful systems and tools, we analyse the secured data in our laboratory according to case-specific requirements and put the jigsaw together, enabling differentiated evidence management. In some cases we already perform an initial analysis on site.

4. **Presentation of evidence**
   The secured evidence, initially available only in electronic form, is processed in accordance with formal legal requirements and presented in a way that can be used in court. Our approach and results are always clearly traceable, repeatable and transparent. We can also provide expert witness testimony if required.
We expose computer crime through our IT-supported forensic investigations. The investigations are conducted in a protected laboratory where data is identified and recovered and electronic event sequences are reconstructed. We also test our clients’ current IT security levels in our lab with measures such as ethical hacking and vulnerability assessments of IT systems.

CYBERLAB uses dedicated physical networks that operate independently of the KPMG network. All forensic tools are connected only to this network and are closed to external access, ensuring that highly sensitive client data never leaves the premises or our systems.

By means of special security doors and an airlock, access to CYBERLAB is logged electronically and granted only to a small controlled number of staff. Our server systems are CCTV-monitored and the doors are connected to a separate alarm system.

With these measures, and others that may not be listed here for security reasons, we ensure that our clients’ data is handled confidentially at all times.

Global availability
Our team of experts provides transnational forensic services in line with legal requirements. Thanks to our global structure, we can react rapidly internationally.

How can we help?
- Exposing white-collar crime and misconduct
- Advising on and checking compliance with guidelines and contracts
- Minimising the risk of malicious acts
- Mitigating litigation and regulatory penalties
- Supporting the recovery of lost assets
- Advising on maintaining and restoring your business reputation

Who we are
KPMG Forensic employs more than 2,500 forensic experts in all regions of the world, including IT specialists, auditors, economists, lawyers, valuation consultants, financial advisers, technical experts, integrity and ethics specialists, investigators and former public prosecutors. Our clients benefit from the wealth of experience of our interdisciplinary teams.
What we do?

We offer you fast and discreet support, and answer questions about the extent of damage and necessary measures.

We help you to introduce immediate precautions, set priorities and define an investigation strategy.

We clarify issues in order to identify possible internal and external perpetrators and conduct interviews.

We can also provide comprehensive support in initiating civil proceedings and criminal investigations.

Whether you are an industrial enterprise, service company or law firm, we are ready to provide advice and active support with our state-of-the-art technology and investigative work. Today, government agencies such as public prosecutors and police forces rely on our support.

Contact

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich
kpmg.ch

Philippe Fleury
Partner
Head Forensic
+41 58 249 37 53
pfleury@kpmg.com

Gerben Schreurs
Partner
Forensic
+41 58 249 48 29
gschreurs1@kpmg.com

Jörg Ochsner
Manager
Forensic
+41 58 249 47 89
joergochsner@kpmg.com

© 2016 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss legal entity. All rights reserved.

State-of-the-art Forensic Technology February 2016