



Forensic Technology

In a nutshell

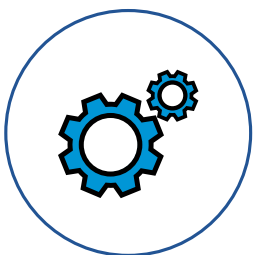
We provide a variety of technical Forensic services to clients in all industries. Our core services can be summarized as follows:

Incident Response: A prompt and appropriate response is required in the event of a cyber-attack. KPMG can help investigate such incidents, conduct a root cause analysis, mitigate your damage and loss, secure your digital trails forensically and restore your normal business operations.

Digital Forensics: Identification, preservation, and analysis of computing and storage devices support your investigations in a forensically sound and defensible way. KPMG is your reliable partner and can represent you in front of authorities, counterparty, or court.

E-Discovery: Using an internationally recognized process, KPMG can locate the relevant documents within a large volume of data, sift through them efficiently and make them available in a suitable format.

Forensic Data Analytics: KPMG's specialists can assist you with the systematic investigation and evaluation of all kinds of datasets as well as with forensic plausibility checks using standardized test scenarios. We can also run tests specific to your industry, company or process to enhance the outcome of an analysis.



Client issues

- Data theft or data loss
- Investigations related to disputes, regulatory or internal reviews where a high amount of information needs to be analyzed quickly and efficiently
- Cyber incidents, such as ransomware attacks, spear phishing, etc.
- Suspicion of fraudulent transactions, anomalies in financial data and other possible misappropriation of funds that require a forensic data analysis

Main sectors & clients

Our clients come from all industries, such as financial services, government & public sector, energy & construction, technology & manufacturing, transportation, pharma & life sciences, not-for-profit organizations, consumer goods & retail, and law firms.



Our approach

- Identification of evidence: We identify the areas where electronic clues and evidence can be found. We focus on all available data storage media.
- Preservation of evidence: We secure all evidence in order to preserve its integrity and map the digital footprint so it is admissible as evidence in court. This can be carried out either remotely from our CYBERLAB® laboratory as well as directly at our clients' premises.
- Analysis of evidence: Using powerful systems and tools, we analyze the secured data in our laboratory according to case-specific requirements. Sometimes, we already perform an initial analysis on site.
- Presentation of evidence: The secured evidence, initially available only in electronic form, is processed in accordance with formal legal requirements and presented in such a way that it can be used in court



Benefits we bring

- We offer guidance and consulting in crisis management during the initial stages of an incident or investigation.
- Our specialists are experienced professionals in Forensic Technology covering a wide range of topics (Digital Forensics, Incident Response, e-Discovery, Forensic Data Analytics etc.) thus allowing us to provide you with a holistic solution to your problem.
- Our tools allow us to analyze structured and unstructured data efficiently and cost-effectively in order to provide you with the necessary evidence and information. We also provide comprehensive and deep insight into your data while maintaining a high quality standard.
- We support you and coordinate the initial measures for the detection of, and the appropriate response to suspected or confirmed cyber incidents by setting up an Incident Response Hotline.
- We can handle all conventional, legacy and new media types (including smartphones, tablets, and social media) and can adapt to your needs in order to detect and respond to (possible) incidents.
- Our mobile appliances provide the possibility to perform all processing and analysis at your premises.
- We offer secure data hosting facilities in Switzerland with the latest, state-of-the-art technology.



How we have helped our clients in the past

The client, an insurance broker, suspected that a former employee had collected relevant client files, data and other information during his employment. Furthermore, the client suspected that the employee collaborated with a competing insurance broker and therefore systematically approached clients in order to lure them away. KPMG's Forensic Technology team was entrusted to identify and collect digital forensic evidence in order to confirm that the employee leaked this information and therefore infringed confidentiality provisions. On the basis of the discovered evidence further legal proceedings were initiated.

Why KPMG Forensic?

We have a specialized and diverse team that has worked on a variety of projects throughout the years. It is equipped with a sophisticated infrastructure and the latest, state-of-the-art technologies – such as Artificial Intelligence, Machine Learning, or Technology Assisted Review.

We are supported by over 40 accredited Forensic practices worldwide, giving us leverage if the complexity and nature of a case requires a multidisciplinary, extraterritorial approach. The coordination is carried out discreetly by your personal contact according to your needs.

Contacts

KPMG AG

Räffelstrasse 28
PO BOX
8036 Zurich

Esplanade de Pont-Rouge 6
PO Box 1571
1211 Geneva 26

Jakob Ogrodnik

Senior Manager
Head of Forensic Technology
Zurich

+41 58 249 79 68
jogrodnik@kpmg.com

Hedi Radhouane

Manager
Forensic Technology
Zurich

+41 58 249 64 54
hradhouane@kpmg.com

[kpmg.ch/ftech](https://www.kpmg.ch/ftech)

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. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2020 KPMG AG, a Swiss corporation, is a subsidiary of KPMG Holding AG, which is a member of the KPMG global organization of independent firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.