Digital Forensic Services

Computer forensics is in our DNA and is a particular specialty of KLDiscovery. For many of our experts, it has been their life-long passion and it shows in their work. Our team, equipped with state-of-the-art tools and attuned to the latest technical and legal developments, guarantee that our clients will receive the best service available.

Collections

Without a sound forensic collection, critical electronic evidence may be missed, inadvertently altered or otherwise rendered inadmissible. This can expose your business to legal complications, unreliable evidence, financial loss and/or reputational damage.

KLDiscovery's digital forensics experts understand the importance of their role performing data collections and do not take that obligation lightly. Whether it be for a small matter (collection of data from a single device) or a large corporate investigation (involving multiple custodians and data sources), in-person or remote, KLDiscovery will help determine the most defensible, efficient and cost-effective strategy.

Experts in every time zone.

Each year, KLDiscovery regularly collects data from approximately 150 different countries. As a result, our experts possess deep experience with country-specific discovery laws and customs. With offices across the globe, our data collection experts can be on the ground quickly, wherever your data is located.

Remote Collection Manager (RCMgr®)

KLDiscovery's RCMgr is the most comprehensive self-collection suite in eDiscovery. End-users and IT professionals alike can now easily perform forensically-sound collections of hard drives, loose files and email servers – effortlessly and defensibly.

RCMgr drives arrive pre-configured to collect only the data you have defined. RCMgr logs the entire collection in granular detail, ensuring that our forensics experts can track the process from start to finish. Upon completion of the collection, RCMgr verifies and encrypts the collected data for secure shipment back to our lab.

Packed full of features typically only available to expert on-site collection experts, RCMgr works on your schedule. Have a question at 3:00 a.m.? No problem. All RCMgr devices come with 24/7/365 support from KLDiscovery's certified forensics analysts.

Without a sound forensic collection, critical electronic evidence may be missed, inadvertently altered or otherwise rendered inadmissible.

RCMgr is the most comprehensive self-collection suite in eDiscovery with 24/7/365 staff support.

Investigations

KLDiscovery's digital forensic investigations service provides the expertise and tools needed to extract and analyze digital evidence to support your legal matter.

Wherever electronic equipment is used, there is a potential source of electronic evidence and digital information, including a "bread crumb" trail to illuminate misuse or wrongdoing. Our computer forensics experts help extract critical evidence, recover any data that culprits may have sought to erase or hide, retrieve key data buried in documents and organize data contained in multiple information sources to give our clients the insight and knowledge they need.

A forensic investigation may be undertaken on a wide range of media (if it stores data, it can potentially be investigated). Many of the most commonly encountered locations include hard drives, servers, mobile phones, tablets, cloud storage, back-up media, social media and individual electronic documents (photos, spreadsheets, etc.).

Our forensics experts employ the most modern and standardized techniques to carefully and accurately identify, preserve and extract critical evidence. This includes the implementation of a strict "chain of custody" procedure, audit trail and adherence to all region-specific evidence handling procedures throughout the handling of the data.

While there is no typical forensic investigation, each will have unique characteristics, scenarios we have experience in include:

- Commercial disputes
- IP or data theft cases
- Employment disputes
- External breaches or intrusion
- Computer misuse
- Harassment or bullying
- Fraud
- Criminal investigations

KLDiscovery's computer forensics experts can search for anything and everything, ranging from evidence of usage patterns to listings of deleted files. While what we can search for is limitless, common requests for analysis often include:

- Deleted file recovery
- Internet search and browsing history activity
- Windows registry analysis
- External media activity
- Last accessed, modified or created dates and files
- Webmail recovery
- Evidence of cloud-based storage
- Evidence of wiping utilities or file destruction
- Cross-validation of opposing expert reports
- Password cracking
- Chat, text and other on-demand/mobile communication history

Digital forensics is a complex arena where the use of an independent expert is highly recommended and preparedness is key. Our analysts have extensive experience providing evidence at trial as well as authoring expert reports and affidavits.

Computers and data evolve – so do we.

The tides of innovation and technological advancement reshape the digital world in the blink of an eye. We understand those changes and are constantly evolving to stay ahead of the latest technical and legal developments in compliance and electronic discovery.

SLS KLD US_Digital Forensics Services_Feb 2023

KLDiscovery
9023 Columbine Road
Eden Prairie, MN 55347
952.937.1107
www.kldiscovery.com