

Computer and Cyber Forensics Services



Deloitte understands that our clients face many different types of computer forensic matters. To help them address these potential challenges, our Computer and Cyber Forensics (Computer Forensics) practice offers a full range of services across the forensic, discovery and investigative lifecycles. Our experienced teams of specialists have extensive technical and investigative knowledge and we have a global network of over 200 computer forensic examiners in 35 countries to assist with investigations.

Our Computer Forensics practice has experience well beyond data collection. We bring value to our clients across numerous technical areas including cyber incident response, mobile device discovery and examinations, expert witness services and forensic investigations.

Cyber incident response

The rapidly evolving landscape of cybercrime and data breaches continues to pose major problems for many organizations in today's digital world. Despite traditional defense mechanisms such as firewalls, it is often difficult for organizations to defend their systems against the latest threats or adversaries.

Once a cyber incident is identified and confirmed, the race is on to eradicate the adversary from the system, understand the systems that have been attacked and the data that has been exposed and exfiltrated from the organization. Deloitte's cyber incident response team strives to provide timely and actionable information in these crisis situations. Through our blend of people, methodology and technology, we can provide rapid reporting and an understanding of the systems attacked to help triage the data at risk.

Our core services include:

- Compromise Investigation
- Damage Assessment
- Remediation

Our broad array of services can help to address various aspects of the cyber threat, while assisting your organization through proactive education on current threats, process improvements and risk mitigation.

Mobile device discovery and examinations

Mobile devices have made a tremendous impact on the way everyday business is conducted. With increased usage of these devices in many organizations, the scope of discovery has expanded to include associated data types such as photos, voice files, text messages and application data. Additionally, detailed forensic review of the devices may allow an organization to have a broader understanding of a device's usage and attribute activities to the device's user. While the complexity of investigating mobile devices continues to rise, so does the need to investigate this media because these devices often contain critical data that may not be found in other repositories.

Deloitte brings significant experience to support mobile device management and eDiscovery solutions. In particular, we have helped many companies navigate large mobile device litigation holds, assisted with creating appropriate discovery work flows, preserved thousands of mobile devices, provided forensic analysis and reporting of devices, performed data extraction and produced mobile device data into standard review formats. Our focus is not only on collection of the mobile device, but also collecting and integrating the cellular provider records into the matter.

We have collected over 9,000 mobile devices varying over 300 different makes and models. Our teams of specialists forensically collect mobile devices using industry standard tools and protocols that are tested and verified. In addition, Deloitte has created applications to enhance the discovery capabilities beyond the use of traditional forensic tools, helping to integrate mobile device metadata and message or conversation family relationships into document review tools.

Our core services:

- Data collection & preservation
- Internal & incident response
- Forensic analysis & data analytics

Our innovations:

- DEParT — A Deloitte tool that prepares data by separating messages into component parts with message threading and other document review analytic capabilities for loading directly into document review platforms
- Relativity Mobile Device Analytics

Expert witness services

Computer forensic expert witnesses are typically engaged by outside counsel and in-house counsel may have little control over the expert witness that is hired, often resulting in inconsistent experiences that may lead to an increased level of risk for the organization.

Frequent turnover of witnesses may mean an inefficient use of internal IT resources that might have to repeatedly provide duplicate information to various new parties. Rate structures and hours expended may vary, making it difficult to quantify the value of the services. The Deloitte difference comes from leveraging both computer forensic analytics and specialized data analytic tools to assist with promptly identifying issues potentially relevant to the matter.

Deloitte considers our computer forensic expert witness services as more than a transactional or one-off experience. We strive to add value through continuing education, process improvement and risk mitigation. By building long-term relationships with our clients, we are able to understand their organization and IT infrastructure and can reduce time spent repeatedly reviewing the same information. Further, we seek fee arrangements that incentivize our efficiency, while maintaining the requisite independence required of an expert witness.

Data collection

Effectively identifying and preserving data and documents to meet demands can be difficult. As such, responding efficiently, concisely and accurately to court-dictated discovery or investigatory requests can raise risks. These risks can be addressed through defensible preservation methodologies and processes to help mitigate not only the risks, but also potentially reduce overall costs.

Deloitte offers data collection services across a wide range of data sources and devices. Our teams use industry standard forensic software and hardware to improve drive acquisition speed, and multiple options for write blocking to help maintain the integrity of each collection. Our professionals follow industry standard Chain of Custody (CoC) guidelines. The collection methodologies and CoC documentation are designed to meet requirements for court acceptance.

The Deloitte difference:

- Forensic specialists. Our diverse teams bring specialized technical and business knowledge. We have witnesses that have testified in court, arbitration, regulatory and other proceedings globally.
- Industry focused. Deloitte leverages in-depth knowledge of industry sectors based on years of experience working closely with our clients.
- Global reach. We are able to draw from the experience of 200,000 professionals within the network of the Deloitte Touche Tohmatsu Limited member firms and their affiliates. This access enables us to address a wide range of cross-border issues impacting people, process and technology.

Our experience with data collection ranges from matters involving tens of thousands of data sources down to matters involving the collection of one data source. The data collection processes used by Deloitte can be scaled to the needs of the matter.

Some tools we use include:

- Hard drive and loose media acquisitions
- Network acquisitions
- Mobile device acquisitions
- Archived media collections (Backup Tape)
- Cloud based repositories (i.e. Gmail, Facebook, Office 365, etc.)

In addition, Deloitte is able to assist organizations with the development of a forensics collection work flow, collections auditing and staff augmentation needs as it relates to collections. Assisted self-collection using pre-configured devices (to collect certain folders, files types, etc.) and other remote collection services are also available as needed.

Contact

Matt Larson
Principal
Deloitte Financial Advisory
Services LLP
+1 404 220 1637
malarson@deloitte.com

Mike Weil
Director
Deloitte Financial Advisory
Services LLP
+1 312 486 0207
miweil@deloitte.com

As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.