

Data Forensics



RESPOND
SERVICE

Improve corporate risk reduction with strategic security and privacy services.

Is the Data Forensics Service right for your company?

- Can you identify the forensic evidence of employee misuse of data or fraud, theft of intellectual property, or a security breach?
- Do you possess the technical knowledge to collect electronic evidence while maintaining acceptable chain of custody management to ensure its acceptance in court?
- Do you need support to enforce the recovery of electronic evidence, or present it in court?

Overview

Digital forensics is the rapid systematic and thorough approach used to find evidence and gather material for the support of criminal and civil actions .

DigitalDefence is prepared to guide your organization through all stages of a case involving electronic data, from responding to the initial incident to your eventual success in arbitration or court.

Benefits of Digital Defence's Data Forensics Service

Our success is based on a variety of factors, including:

- Experience of our investigators – Each forensic specialist has 15 years or more of real-life experience gained in enterprise, military or law enforcement
- Legal experience – Our investigators have presented in court and at arbitration hearings; they understand the legal process, and how their findings play a part in the outcome
- Strong practices – Digital Defence employs a stringent methodology that was developed in consultation with law enforcement and the legal community. We approach every case as if it will be going to court, and will be subject to intense scrutiny. Our practices support this perspective, ensuring that we are fully prepared to represent and defend our findings
- Industry recognition—Our forensic specialists are active members of organizations such as the High Technology Crime Investigation Association (HTCIA) . They also possess industry-recognized certifications such as the Certified Information Systems Security Professional (CISSP), the Certified Computer Examiner (CCE), and vendor-specific designations.
- Thought leadership—Digital Defence forensic specialists are frequently lecturers, present at major security conferences, and teach practical workshops

Who Uses Data Forensics?

- Private individuals— domestic matters such as mistrust, family disputes, divorce, custody; recovery of deleted data or lost data
- Corporations—employee HR issues (e.g.: sexual harassment claims, wrongful dismissal), union issues, internal crime (fraud, embezzlement), corporate sabotage, corporate espionage, verification of data in mergers and acquisitions; employee monitoring
- Government—matters involving private consulting, public defence
- Auditors and accounting firms— investigation of fraud
- Law enforcement and Private Investigators—providing electronic support services; aid in password retrieval, data recovery, employee monitoring, investigation of injury compensation claims
- Legal professionals—support criminal and civil litigation, expert witness services, execution of Anton Piller orders

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss

Over 90% of today's information is created or stored electronically. Have you acquired the evidence to support your case?

Service Description

DigitalDefence offers the following services:

- Pro-Active forensics – There are certain risky events (e.g. terminating an employee with just cause, suspicion of theft of intellectual property) that could place an employer at risk for future litigation from an employee. Digital Defence can acquire copies of employee data prior to the event to minimize your potential liability
- Seizure of data and systems – DigitalDefence is highly skilled in collecting data to be used in formal legal proceedings (criminal, civil) and can also assist in recovering data and systems under an Anton Piller order
- Forensics analysis – DigitalDefence forensic specialists can assist you by finding and analyzing the information that may be used to support legal proceedings. This assistance can include:
 - Providing expert consulting on the forensics and legal processes
 - Creating exact and authenticated copies of hard drives and other electronic media
 - Recovering hidden or deleted files, including password-protected or encrypted data
 - Discovering attempts to conceal, delete, or fabricate electronic evidence
 - Determining user activity, including online activity (websites visited, email and other online communications)
 - Tracing incoming emails (fraud, threats against individuals or organizations)
- Secure asset disposal, including secure deletion of data in accordance with Canadian and international standards
- Analysis of mobile devices – DigitalDefence has developed unique and successful approaches to recovering electronic data from mobile devices, including cell phones, Blackberry devices, and hand-held computers
- Litigation support – As court-qualified experts, DigitalDefence can help litigators to pursue and win their cases by providing consulting and background knowledge, preparing declarations, and providing expert witness testimony

DigitalDefence is provides cutting edge training in digital forensics. Current course offerings include Hands-On Data Forensics for Corporate Investigators, and Workshop in Malware Analysis.

For more information please visit www.digitaldefence.ca



Digital Defence Inc

Toll-Free 866-677-1337 | Tel 905-681-3310
302 - 3310 South Service Road,
Burlington, Ontario L7N 3M6

Disclaimer

© 2010 Digital Defence. All rights reserved.
This document is for informational purposes only.
Digital Defence makes no warranties, express or implied, in this document.