2.5 Digital Forensic Services

Digital forensics, which includes computer forensics is the process of forensically acquiring and analyzing a wide variety of digital media sources. This may include laptops, desktop, external hard drives, external media storage devices, email, internet history, network folders, and a wide variety of log sources. It includes the collection, preservation, analysis and if required, court presentation of digital-related evidence.

Digital evidence is very fragile and can easily be altered or lost if the collection process is not initiated at the onset of an investigation. Evidence can be a critical component of cyber incident response, internal investigations, criminal and civil proceedings (which include fraud, sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal confidential information).

We are commonly engaged as part of corporate investigations, where the allegations are likely to lead to Code of Conduct, Arbitration, Statutory or Criminal allegations. This may include a comprehensive review of email (e-Discovery) which may involve the acquisitions and analysis of large volumes of email. Our investigators are experience in cases where the email (and attachments) exceed 1,000,000 records. We continue to enjoy a strong relationship with the legal community in support of litigation matters. (see e-Discovery Services)

Used as an important component within cyber incident response, digital forensics is utilized to perform root cause analysis, mitigation of the event and identification of recommendations to prevent event reoccurrence. C.S.I. Services has performed digital forensics as part of incident response within IT and ICS/SCADA (OT) environments using distinctly different methodologies. While it is true that digital forensics can provide a wealth of information, it remains only a small part of our entire investigative toolset as part of any investigation – with experience remaining our greatest asset!

Used within Criminal, Federal and corporate Code of Conduct cases, C.S.I. Services can present complex computer evidence in a judicial (or quasi-judicial) proceeding. We bring expert witness qualifications and extensive experience in expert testimony. We have presented digital forensics evidence in civil and criminal courts in Canada and the United States.

We utilize a number of different forensic software and hardware tools depending on the investigation type and requirements. Our hardware and software tools are extensive, and enable acquisition of electronic evidence from virtually any form of storage media. Sample of types of investigations/services:

- Fraud, theft, or exfiltration of intellectual or confidential property
- Human Resources (HR) investigations, including Code of Conduct allegations, harassment, and inappropriate use of computers
- Support for Internal Audit and Legal investigations
- Email, chat history, internet history, keyword searching
- File metadata extraction and analysis
- Investigation of potential hacking/computer intrusion

- Cellphone/smartphone mobile analysis
- Consulting and assistance in the execution of Anton Pillar orders
- Years of experience utilizing forensics within OT/SCADA QA and Production networks (continual validation of methodology, focusing on maximizing "availability" often in support of Incident Response)
- Providing detailed forensic reporting and expert court testimony

Examples (partial) of data sources include:

- Computers (laptops/desktops)
- Servers (Windows/Unix/Linux) – local and remote
- External hard drives (USB, loose hard drives)
- External media (USB, SD/microSD cards, other flash media)
- Servers – Windows, Unix, Linux (on-site or remote)
- Cellphones, smartphones, tablets
- Server-side sources of information
- Cloud-based storage
- Email – acquisition, analysis and analytics
- Analysis of malware and workstation/network "indicators of compromise"

In today's "connected universe", C.S.I. Services has extensive experience in conducting open-source investigations across a vast array of public and "dark web" sites. While it is true that not all information is easily accessible, our range of tools is capable of searching across a wide variety of legal data sources and provide a graphic visualization of a subject's online activities and postings.