

# Enterprise Security Digital Forensic Specialist - 22820

---

## Primary Focus

Under the direction of the Chief Security Officer, Enterprise Security, the Digital Forensic Analyst works closely with enterprise security personnel and legal counsel to plan, conduct and process all manner of digital collections relating to internal and external investigations, e-discovery matters and security incident response.

## Responsibilities

Actively participate in investigations, e-discovery and incident response, working as part of teams that may include any or all of enterprise security personnel, legal counsel, IT, records management personnel and members of the eDiscovery Response Team.

Utilize Enbridge's forensic and other tools to carry out digital preservation, collection and processing in a manner consistent with Enbridge's protocols, maintaining chain of custody throughout, including, among other responsibilities:

- Working with Legal Counsel on litigation hold notices and responses.
- Identifying targeted custodians and data sources.
- Leveraging information obtained as part of identification and preservation processes.
- Determining and carrying out appropriate collection strategy per source.
- Maintaining integrity of collected information.
- Evaluating risks, costs and timings of collection approach, liaising with legal counsel in support of discussions with regulators and opposing counsel.
- Processing collected data into desired processed end state, ready for review by legal counsel, security and compliance personnel.
- Supporting early case assessment, performing targeted, high-level review of what has been indexed/collected and custodian and subject matter experts interviews.
- Assessing potential volume of relevant data sources.
- Culling and filtering to reduce volume of export / review set.
- Supporting the accurate and efficient document review and analysis.
- Exporting production sets to electronic or other media.
- Creating custom load files of production set based on agreed upon production specifications.

## Qualifications

The ideal candidate should have a minimum of 5 years of experience in some of the following fields:

- Case experience in digital forensic investigations
- Experience in litigation support, technological investigations and eDiscovery

- Experience with the following technologies:

All EnCase suite of products (Forensic, Enterprise, eDiscovery and Cybersecurity), Litigation support tools for eDiscovery (i.e.: Summation, Relativity, EDRM), Fluent in Database query and script development (MS-SQL, Oracle), Computer Operating systems (Windows XP, Windows Server, Windows 7, Linux, Unix, Mac OS X), Computer File systems (NTFS, EXT3, EXT4, HFS+), EnCE, CISSP, CISM or GIAC certification highly desired, other technical certifications in addition would be an asset.

In addition, the ideal candidate would possess:

- Exceptional Customer service
- Completed undergraduate degree with outstanding academic credentials in Computer Science, MIS, or other related technical education
- Strong interpersonal skills and ability to work as a team
- Ability to elaborate innovative solutions
- Strong analytical and problem solving skills
- Strong interpersonal, negotiation, consensus building, and leadership skills
- Ability to work independently with minimum supervision
- Well organized to handle multiple concurrent tasks
- Excellent documentation and communication skills
- Knowledge of information security best practices (ISO17799/27001, NIST, etc)
- Knowledge of regulatory and legislative influences on information security (e.g. PIPEDA, Sarbanes-Oxley)
- Possess or able to obtain Canadian Government Secret Level Security Clearance.

### **Other Information**

Enbridge, where energy meets people was named one of Canada's Top 100 Employers and Alberta's Top 55 Employers for 2012.

Enbridge is an equal opportunity employer.

Final candidates for this position will be required to undergo a security screening, including a criminal records check.