Cybercriminalité: mythe ou réalité?

Lancement de la saison scientifique du Centre International de criminologie comparée (CICC)

Jeudi 2 février 2017

De l'enquête traditionnelle à l'enquête virtuelle: *le profil du cyberenquêteur*

Par **Frédérick Gaudreau**

Étudiant au DESS en sécurité intérieure, École de criminologie

Chargé de cours à l'UQTR et à l'École Polytechnique de Montréal

Capitaine, chef du Service des enquêtes sur la criminalité contre l'État à la Sûreté du Québec

UQTR Savoir. Surprendre.

SÛRETÉ DU QUÉBEC POLICE SERVICE INTÉGRITÉ JUSTICE

POLYTECHNIQUE MONTRÉAL LE GÉNIE EN PREMIÈRE CLASSE

Background « Cyber »

http://www.dnaindia.com/

Métier de cyberenquêteur: cadre de compétence

http://www.dnaindia.com/

Modèles et techniques d'enquête

- Il existe plusieurs modèles et techniques d'enquête au sujet de l'investigation et de la recherche de trace numérique
- Ces modèles peuvent s'appliquer aux agences d'application de la loi mais également au domaine de la maintenance informatique, de la cyber sécurité et de l'audit (CIARDHUAIN, 2004)
- De nombreux auteurs se sont penchés sur la question dont S.Lapointe (1999); M.Goodman (2001); E.Casey (2011); R & S. Bryant (2014); B. Nelson, A. Phillips & C. Steuart (2016)
- **Mais au fait, qu'est-ce qui a vraiment changé dans le monde des enquêtes?**

Compétences recherchées
Enquêteur - Police

- Détenir la capacité de :
  1. Initier des enquêtes;
  2. Préparer un plan d'enquête;
  3. Procéder à l'enquête;
  4. Participer aux procédures judicaires;
  5. Établir et maintenir des liens de coopération avec le public et les partenaires impliqués dans les événements de son secteur d'activité;
  6. Maintenir à jour ses connaissances.

Modèle de la Sûreté du Québec

Compétences recherchées
Enquêteur - Informatique judiciaire

- Être familier avec les différentes formes de TIC (FAIRTLOUGH, 2015)
- Connaitre les méthodes d'extraction des données numériques (FAIRTLOUGH, 2015)
- Détenir les certifications pertinentes au domaine de l'informatique judiciaire (NELSON et al., 2016)
- Être familier avec les prérequis et les conditions pour agir et être reconnu à titre de témoin expert (CASEY, 2011)
- Critères pour être déclaré expert devant les tribunaux au Canada: *Pertinence; nécessité d'aider le Juge des faits; absence et qualification de toute autre règle d'exclusion.* (R. c. Mohan [1994] 2 R.C.S. 9.)

Formation requise pour devenir et/ou exercer le métier de *cyberenquêteur*

Formations

- Formation d'enquêteur:
  - Multiples écoles de formation reconnues par le Bureau de la sécurité privée
  - Programmes collégiaux et universitaires (ex: Bacc sécurité police UdeM)
  - École de criminologie UdeM
  - École nationale de police du Québec (ENPQ) – EXCLUSIVITÉ AUX POLICIERS
- Formation d'enquêteur spécialisé en informatique judiciaire:
  - Collège Canadien de police (CCP) – EXCLUSIVITÉ AUX AGENTS DE LA PAIX
  - Certifications…
- Formation spécifique au domaine « *cyber* »:
  - Exemples : École Polytechnique de Montréal et son programme de certificats en cyber enquête; cyber fraude et cyber sécurité; Programme en criminalistique UQTR (Trace numérique)

Certifications (Clarke, 2010; Casey, 2011; Nelson et al, 2016)

- Associations:
  - International Association of Computer Investigative Specialists (IACIS)
    - Certified Forensic Computer Examiner (CFCE)
  - ISC Certified Cyber Forensic Professional (CCFP)
  - High Tech Crime Network (HTCN) (4 certifications)
- Fournisseurs de produits forensic:
  - EnCase Certified Examiner Certification
  - AccessData Certified Examiner
- Autres:
  - SysAdmin Audit Network Security (SANS)
  - A+ ; N+; CISSP; CEH; etc.

Formations et certifications : applicables aux cyberenquêtes?

- La forte majorité des programmes académiques actuels sont souvent mal adaptés aux réalités du travail spécialisé de cyberenquêteur;
- On enseigne aux étudiants en informatique les connaissances requises pour assurer le bon fonctionnement et la bonne utilisation d'un système, d'un outil ou d'un produit;
- L'enquêteur, pour faire efficacement son travail, doit connaitre l'ensemble des aspects techniques inhérents aux conséquences de l'utilisation de ces produits sur les systèmes avec lesquels ils interagissent;
- Ces aspects techniques sont rarement enseignés, faute d'utilité en milieu corporatif;
- Également, les technologies changent rapidement, et une connaissance n’est généralement valide que jusqu’à ce que le produit à laquelle elle réfère soit mis à jour.

Profil *idéal* du cyberenquêteur: utopie?

http://usa.kaspersky.com

Profil *idéal* ?

- Méthode : sondage informel auprès de *cyberenquêteurs* d'expérience (policiers et civils)
- 2 hypothèses :
  - **Être un cyberenquêteur accompli c'est d'avoir d'abord des compétences en informatique et ensuite d'apprendre le métier d'enquêteur**
  - **Être un cyberenquêteur accompli c'est d'être d'abord un policier et/ou un enquêteur et d'ensuite aller se faire former et se spécialiser en informatique**

Sommaire des réponses

- Le critère principal de sélection devrait être l'expérience policière (patrouille et enquête générale)
- Le métier d'enquêteur ne s'apprend pas assis derrière un bureau et ne s'achète pas, il faut sortir sur le terrain
- Il est difficile, voir impossible, de former quelqu'un avec une vision « police », malgré ses connaissances avancées en informatique
- Un bon cyberenquêteur devrait avoir une expertise supérieure à la moyenne au niveau informatique
- Les connaissances et les compétences au niveau informatique peuvent et doivent se développer au fil du temps via des formations et de la R&D

Exigences

Transition

Enquêteur

- Capacité d'apprentissage, autonomie, pensée structurée;
- Jouer et naviguer souvent dans le gris, rarement dans le blanc ou noir;
- Les relations interpersonnelles sont primordiales (approches des gens, collègues, partenaires);
- Compréhension de la « joute » et de la culture judiciaire;
- Bonne gestion des tâches, des priorités, et de la notion de profit vs investissement d'une démarche d'enquête;
- Capacité à prendre une décision, avoir du flair ou de l'intuition (que l'on voit ça comme inné, ou acquis, ça existe concrètement)

Spécialiste en informatique judiciaire

- Connaissance des fonctions de base des logiciels et des plateformes;
- Connaissance des sources d'informations techniques et technologiques en cas de besoins;
- Apprentissage des particularités de la preuve numérique: volatilité, fragilité, emplacement;
- Compréhension du fonctionnement du web et des systèmes de fichiers

Réflexion

CBS Television Studios

- Personne ne peut prétendre être un *expert* sur tous les aspects de l'informatique (FAIRTLOUGH, 2015)
- Peut-on prétendre être un *cyberenquêteur* chevronné et accompli devant tous les types de crimes?

Merci de votre attention!

Frédérick Gaudreau

fregaud@gmail.com