4e édition

COLLOQUE

Groupe sur l'Analyse, la Recherche et le Développement en Source Ouverte

Mercredi 29 mai 2019
8 h 00 – 16 h 00

Université de Montréal
Pavillon André-Aisenstadt
2920, chemin de la Tour
Montréal
Salle 1140

En collaboration avec :

éducation permanente umontréal

JLR 30 ans de solutions foncières

COMMISSIONNAIRES
FIABLE · EN TOUT TEMPS · EN TOUT LIEU

CICC Centre international de criminologie comparée 50 ans 1969 2019

Université de Montréal

serene·risc

Remerciements

Le comité organisateur désire remercier les partenaires commerciaux de l'événement pour leur contribution à faire de cet événement un succès !

Partenaire principal

éducation permanente umontréal

Partenaires

JLR 30 ans de solutions foncières

COMMISSIONNAIRES
FIABLE · EN TOUT TEMPS · EN TOUT LIEU

CICC Centre international de criminologie comparée 50 ans 1969-2019

Université de Montréal

serene risc

HORAIRE DE LA JOURNÉE

8h00 à 8h30	**Accueil**	**Salle1140**
8h30 à 9h00	Mot d'accueil et présentation des dignitaires	
9h00-10h00	Médias sociaux et Tribunaux – Marie-Christine Robert	
10h00 à 10h30	**Pause / Réseautage**	
10h30 à 11h30	Les escroqueries par Internet : des cas reportés à la détection de répétitions criminelles - Quentin Rossy	
11h30 à 12h00	Présentation des commanditaires	
12h00-13h30	**Diner**	**Agora Jean-Coutu**

13h30	Ateliers				
	Piste 1 : Médias sociaux (débutant)	**Piste 2 : Tendances (débutant et intermédiaire)**	**Piste 3 : Les outils pour l'obtention d'informations en source ouverte et leur maîtrise (débutant et intermédiaire)**	**Piste 4 : Cryptomonnaie et nouvelle économie (débutant et intermédiaire)**	**Piste 5 : Amenez votre portable (avancé)**
13h30 à 13h55	1 **Facebook comme outil de renseignement policier: analyse de réseau de motards criminels** Élizabeth Mason (salle 1140)		3 **Hunchly : sauvegarde, collecte et analyse de pages Web** Marc-André Audet et Romain Le Grand (salle 1411)	5 **Telegram et Discord: pour une meilleure compréhension des pump and dump effectués sur le marché des cryptomonnaies** Marc-André Loiselle (salle 1409)	7 **DevTools : Vous êtes plus fort que Facebook !** Alain Rioux (salle 1340)
14h00 à 14h25	2 **Description des activités des groupes s'identifiant à Anonymous au Canada: Analyse de la menace grâce à Facebook** Andréanne Bergeron (salle 1140)		4 **L'utilisation du logiciel Gephi pour l'analyse de réseaux** Francis Cossette (salle 1411)	6 **Les cryptomonnaies et le minage sous la loupe de l'AMF** Odrée Blondin et Hélène Guilbault (salle 1409)	8 **DevTools : Vous êtes plus fort que Facebook ! (suite)** Alain Rioux (salle 1340)
14h25 à 14h45	**Pause / Réseautage**				
14h45 à 15h10	9 **La recherche sur les médias sociaux : une introduction** Sébastien Meloche (salle 1207)	11 **La modélisation thématique non-supervisée (LDA) : Comment catégoriser des quantités massives de données textuelles** Maxime Bérubé (salle 1411)	13 **Quelques trucs stupides d'intrusion** Laurent Desaulniers (salle 1140)	15 **La déanonymisation des détenteurs de cryptomonnaies** Mathieu Lavoie (salle 1409)	17 **Buscador : un outil puissant et polyvalent** Philippe Lefebvre (salle 1340)
15h15 à 15h40	10 **Canlii : une source de données sous-utilisée? L'exemple des opérations Mr Big à travers les jurisprudences canadiennes** Francis Fortin (salle 1207)	12 **L'évolution de la réaction sociale en ligne suite à l'attentat de Manchester** Thuc-Uyên Tang (salle 1411)	14 **Investigation et veille sur Internet: au-delà de la maîtrise des outils** Quentin Rossy (salle 1140)	16 **Suivre des paiements de cryptomonnaies à la trace : mission impossible?** David Décary-Hétu (salle 1409)	18 **L'automatisation des recherches en sources ouvertes : un mythe ou réalité?** Sébastien Ruel (salle 1340)
15h45 à 16h00	Quand les social botnets manipulent l'information : Le cas du #Brexit - Valentine Crosset et Mot de la fin				(salle 1140)
16h00	**4 @ 7**				**(Salon Maurice Labbé – 6225, 6e étage)**

8h00 Accueil (Salle 1140, Pavillon André-Aisenstadt)

8h30 Mots d'accueil et présentation des dignitaires

Francis Fortin, Professeur adjoint, École de criminologie de l'Université de Montréal

Dignitaires:

Martin Desbiens-Côté, commandant, Section des Crimes technologiques, Service spécialisé en enquêtes criminelles, Direction des enquêtes criminelles, Service de police de la Ville de Montréal

Patrick Daoust, analyste en renseignement criminel, Gendarmerie royale du Canada

9h00 Médias sociaux et Tribunaux

Revue jurisprudentielle en matière de médias sociaux. Très populaires, les Facebook, Instagram, Pinterest et YouTube de ce monde, sont de véritables mines d'or d'informations. À la fois outils d'enquête et « scènes de crime » les médias sociaux font partie intégrante du quotidien d'une grande partie de la population et par conséquent, également du paysage judiciaire. Se retrouvant ainsi de plus en plus devant les tribunaux, comment toutes ces informations provenant de sources dites « ouvertes » sont-elles accueillies par ces derniers ? Constituant une opportunité unique, l'utilisation de ces sites accessibles apporte également son lot de défis, notamment pour que ces éléments de preuve soient acceptés par la cour. Réalité du web 2.0 et maintenant du web 3.0, les médias sociaux ont été au cœur de nombreuses décisions dans les dernières années, offrant ainsi un portrait de plus en plus clair de ce qui est maintenant possible d'obtenir avec ces outils numériques.

Marie-Christine Robert, Avocate, Ministère de la Justice du Québec

10h00 Pause / Réseautage

10h30 Conférences (Salle 1140)

Les escroqueries par Internet : des cas reportés à la détection de répétitions criminelles

Si les escroqueries commises à l'encontre de personnes sont séculaires, la diversité et la complexité intrinsèque des schémas de tromperie déployés en ligne semblent complexifier leur analyse et leur classification. De surcroît, les escroqueries par Internet sont bien souvent associées à d'autres formes d'activités criminelles en ligne, telles que le vol de données et d'identités, ainsi que le blanchiment des biens soustraits. Le cœur de la présentation porte ainsi sur la nature des activités frauduleuses, les manières de les analyser et de les classifier, ainsi que sur les enjeux liés à l'évaluation de leur ampleur. Dans un second temps, la détection de répétitions criminelles au sein des cas reportés aux autorités de Suisse romande sera présentée afin de discuter des enjeux de production de renseignement criminel opérationnel par la reconstruction de séries et la détection des espaces de rencontres virtuels qui concentrent les phénomènes.

Quentin Rossy, Professeur, École des Sciences Criminelles, Université de Lausanne

11h30 Présentations des commanditaires
Faculté de l'éducation permanente, JLR et Commissionnaires

12h00 Dîner (Agora Jean-Coutu)

13h30 Ateliers en après-midi – première partie

Piste 1 Médias sociaux (débutant) (Salle 1140)

13h30 (1) Facebook comme outil de renseignement policier: analyse de réseau de motards criminels

Devant l'échec du mégaprocès SharQc en 2015, qui a mené à la libération sans accusations d'une majorité des motards arrêtés dans le cadre de l'opération du même nom effectuée en 2009, les organisations policières ont tout intérêt à procéder à une remise en question de leurs stratégies face à la lutte contre les motards criminels. L'objectif de la présente recherche était de déterminer l'apport des données virtuelles de Facebook pour le renseignement policier sur les motards criminels en adoptant une approche comparative. Pour ce faire, deux réseaux des membres du groupe de motards criminel ciblé ont été construits, le premier à partir des données policières et le second à partir des données Facebook. L'analyse s'est scindée en deux : la première partie compare les mesures de centralité des membres du groupe de motards criminels ciblé des deux réseaux (policier et Facebook), tandis que la seconde partie examine l'évolution des deux réseaux dans le temps. Les résultats ont démontré que les données Facebook étaient contemporaines, dynamiques et de qualité, constituant donc un apport considérable pour le renseignement policier. Les organisations policières maximiseraient son utilité en ayant recours à Facebook en parallèle aux données policières.

Élizabeth Mason, Analyste, Service de police de Repentigny

14h00 (2) Description des activités des groupes s'identifiant à Anonymous au Canada: Analyse de la menace grâce à Facebook

Au cours des dernières années, les chercheurs ont observé l'émergence de communautés présentes sur des sites Web permettant les interactions sociales, dont le groupe Anonymous. Dans la littérature, les avis sont partagés quant à la vraie nature de ce groupe. Certains mentionnent que ce sont des délinquants anarchistes, d'autres affirment qu'il s'agit d'une simple communauté en ligne partageant les mêmes idéologies, et d'autres encore pensent que le groupe représente un mouvement social émergeant. Considérant qu'il est difficile de donner un portrait précis de ce qu'est le mouvement Anonymous et que très peu de connaissances sont disponibles jusqu'à ce jour quant à sa dynamique, la présente recherche vise à décrire les communautés en ligne s'identifiant à Anonymous au Canada, et ce, en tenant compte qu'il est possible que le mouvement soit différent d'une région à l'autre et d'un sous-groupe à l'autre. En analysant les publications Facebook de différentes pages s'identifiant à Anonymous au Canada, nous avons étudié les types et les thèmes des publications les plus populaires. Il en ressort principalement que les groupes dénoncent beaucoup de situations, mais prennent très peu de moyens concrets pour agir.

Andréanne Bergeron, Doctorante, École de Criminologie, Université de Montréal

Piste 3 : Les outils pour l'obtention d'informations en source ouverte et leur maîtrise (intermédiaire) (Salle 1411)

13h30 (3) Hunchly : sauvegarde, collecte et analyse de pages Web

Hunchly est un outil spécialement conçu pour sauvegarder et analyser les pages Web visitées. Plusieurs fonctionnalités du logiciel facilitent le processus de collecte d'informations. Par exemple : historique des pages Web visitées, extraction automatisée et personnalisée de contenus (adresses courriel, identifiants de médias sociaux, mots-clés, analytiques), annotation des pages visitées, exportation des données brutes et intégration dans d'autres outils (par exemple Maltego), etc. Le logiciel enregistre le contenu brut (code source HTML, javascript, images) des pages visitées. Ainsi, une page pourra être reproduite telle qu'elle était lors de sa consultation. Le stockage des informations collectées et son traitement sont effectués localement. Aucun lien avec des plateformes infonuagiques n'est nécessaire. Cette présentation vise à faire découvrir les fonctionnalités clés du logiciel et démontrer comment il peut faciliter la collecte d'informations. Des démonstrations du logiciel sont prévues.

Marc-André Audet, Programmeur-analyste, Service de police de la Ville de Montréal
Romain Le Grand, Agent de recherche, Service de police de la Ville de Montréal

14h00 (4) L'utilisation du logiciel Gephi pour l'analyse de réseaux

L'utilisation de banques de données massives est de plus en plus commune. Les logiciels d'analyse de réseau sont très utiles pour analyser rapidement de telles bases de données et ainsi représenter les liens qui unissent les entités.

Francis Cossette, Analyste stratégique, Service de police de Québec

Piste 4 : Cryptomonnaie et nouvelle économie (débutant) (Salle 1409)

13h30 (5) Telegram et Discord: pour une meilleure compréhension des pump and dump effectués sur le marché des cryptomonnaies

La présentation vise les groupes de manipulateurs sur Telegram et Discord qui commettent des manipulations financières de style pump and dump sur le marché des cryptomonnaies. Il est possible de recenser et de comprendre des stratagèmes de manipulation de cryptomonnaies à partir de réseaux sociaux comme Telegram et Discord.

Marc-André Loiselle, candidat à la maîtrise, École de Criminologie, Université de Montréal

14h00 (6) Les cryptomonnaies et le minage sous la loupe de l'AMF

Alors que les organismes de réglementation des marchés financiers mettent régulièrement en garde le public quant aux risques que représentent les monnaies virtuelles, leur utilisation est devenue de plus en plus courante depuis les dernières années. Malgré les allégations à l'effet contraire, plusieurs activités liées à l'écsystème des cryptomonnaies s'avèrent des offres de valeurs mobilières. L'objectif de cette conférence est de présenter le type de dossier ainsi que les nouveaux défis et enjeux rencontrés dans le cadre de nos enquêtes relatives aux cryptomonnaies.

Odrée Blondin, Autorité des marchés financiers
Hélène Guilbault, Autorité des marchés financiers

Piste 5 : Amenez votre portable (avancé) (Salle 1340)

13h30 (7 et 8) DevTools : Vous êtes plus fort que Facebook !

Les outils de développement (DevTools), qu'on retrouve sur les navigateurs récents tels que Google Chrome, peuvent s'avérer fort utiles pour manipuler une page Web. Que ce soit pour retirer, modifier ou extraire des données, ces outils vous permettent de prendre facilement le contrôle des pages Web que vous visitez. Cette présentation vous montrera comment, avec un peu de Javascript et d'aspirine, vous pouvez maîtriser le code de Facebook et de bien d'autres sites Web. Et pour réutiliser ou partager votre code, apprenez à faire un petit signapplet (bookmarklet) ou mieux, une extension de navigateur. Cette présentation s'adresse à un public qui aime les défis. Il sera question de programmation Javascript, de DOM (Document Object Model) et d'autres sujets.

Alain Rioux, Enquêteur, Sûreté du Québec

14h25 Pause

14h45 Ateliers en après-midi – deuxième partie

Piste 1 : Médias sociaux (débutant) (Salle 1207)

14h45 (9) La recherche sur les médias sociaux : une introduction

Comme vous le savez déjà, les sources ouvertes sont un atout majeur dans les enquêtes policières. Cependant, il est important de considérer les risques associés à ce type de recherche. Il ne faut pas oublier que les policiers et analystes ne sont pas les seuls à utiliser cette source de renseignement. L'atelier qui suit offre une introduction aux bonnes conduites à avoir lorsqu'on enquête des sujets d'intérêt dans les sources ouvertes, mais aussi sur l'utilisation des médias sociaux d'un point de vue personnel. On abordera entre autres le concept de l'anonymat, la trace numérique et les particularités de certains médias sociaux. Suite à cet atelier, les participants seront comment bien préparer leurs recherches en sources ouvertes et éviter de compromettre leur sécurité par une exposition en ligne.

Sébastien Meloche, Gendarmerie Royale du Canada

15h15 (10) Canlii : une source de données sous-utilisée? L'exemple des opérations Mr Big à travers les jurisprudences canadiennes

Au Canada, la plupart des décisions ayant fait l'objet d'un jugement écrit sont ajoutées à la banque de données de Canlii. Il s'agit d'une vaste banque de données qui peut être recherchée et analysée grâce aux outils de recherche avancée et un API (application programming interface). Dans un premier temps, cette présentation vise à présenter les fonctionnalités et la pertinence d'utiliser Canlii pour la recherche académique et juridique. Dans un deuxième temps, nous utiliserons un échantillon de 34 jugements rendus par divers tribunaux canadiens disponibles publiquement sur Canlii, afin d'examiner et découper les étapes des opérations policières de type Mr Big au moyen d'une analyse documentaire. Une synthèse des connaissances et des implications pour les agences d'application de la loi sera présentée.

Francis Fortin, Professeur adjoint, École de criminologie, Université de Montréal

Piste 2 : Tendances (intermédiaire) (Salle 1411)

14h45 (11) La modélisation thématique non-supervisée (LDA) : Comment catégoriser des quantités massives de données textuelles

À l'ère des nouvelles technologies de l'information et de la communication, il est de plus en plus fréquent d'être confronté à des quantités massives de données textuelles, et ce, dans de multiples domaines. Bien que très riches et hautement intéressantes, ces données nécessitent généralement d'importantes ressources afin de les analyser. Afin de surmonter les défis associés à l'analyse de quantités massive de données textuelles, cette présentation fera la démonstration détaillée des étapes à suivre pour la réalisation d'une modélisation par Allocation Dirichlet Latente (LDA) avec le module Gensim de Python. Il y sera notamment question de la préparation des données textuelles, de leurs prétraitements aux fins d'analyse, de l'identification de bigramme et trigramme significatifs, de la représentation graphique des principaux thèmes identifiés dans les documents analysés, ainsi que des limites associées à cette méthodologie.

Maxime Bérubé, Chercheur postdoctoral, Université Concordia

15h15 (12) L'évolution de la réaction sociale en ligne suite à l'attentat de Manchester

L'attentat de Manchester, qui est survenu le 22 mai 2017, a suscité de nombreuses réactions en ligne, notamment sur Twitter. Cette étude a comme objectif d'analyser l'évolution de la réaction sociale en ligne et de décrire ses différentes phases. À l'aide d'outils d'analyse, une quantité colossale de tweets ont été analysés chaque heure après l'attentat afin d'identifier les tendances à la suite de l'événement.

Thuc-Uyên Tang, Candidate à la maîtrise, Université de Montréal

Piste 3 : Les outils pour l'obtention d'informations ouvertes et leur maitrise (débutant) (Salle 1140)

14h45 (13) Quelques trucs stupides d'intrusion

Pour beaucoup de gens, les tests de sécurité requièrent beaucoup de connaissances techniques alors qu'il existe beaucoup de trucs simples qui permettent de rapidement cloner des cartes d'accès, voler des mots de passe via Wifi, voler des clés et compromettre des entreprises. L'objectif de cette présentation est de présenter l'état d'esprit de l'attaquant et comment la créativité est utile à des fins d'intrusion. À la fin de la conférence, l'audience devrait être en mesure de réaliser l'ensemble des tests présentés.

Laurent Desaulniers, Chef d'équipe en test d'intrusion, GoSecure

15h15 (14) Investigation et veille sur Internet : au-delà de la maîtrise des outils

Cet atelier ambitionne de mettre en lumière et discuter les enjeux méthodologiques de la recherche de données en sources ouvertes sur Internet dans une perspective d'exploitation opérationnelle dans un environnement policier. La discussion portera sur le processus de recherche en lui-même et abordera quelques questions clés qui jalonnent toute investigation en ligne : (1) que cherche-t-on et pourquoi ?, où chercher et comment évaluer l'étendue du champ d'investigation ?, (3) comme fixer la fin d'une investigation en ligne ?, (4) comment préserver les traces internétiques détectées ?, et (5) comment intégrer ces données dans un processus de continuité de la preuve ? L'atelier présentera les enjeux au travers d'exemples d'enquêtes réelles, de quelques études empiriques exploratoires et pistes de solutions méthodologiques. Les questions sont posées, la discussion est lancée !

Quentin Rossy, Professeur, École des Sciences Criminelles, Université de Lausanne

Piste 4 Cryptomonnaie et nouvelle économie (intermédiaire) (Salle 1409)

14h45 (15) La déanonymisation des détenteurs de cryptomonnaies

Les cryptomonnaies ont été inventées pour permettre des échanges financiers internationaux, instantanés et surtout anonymes. Les cryptomonnaies publient dans la plupart des cas des listes des transactions, mais n'associent ces transactions qu'à des identifiants anonymes. Au cours des dernières années, de multiples techniques ont été conçues pour diminuer, voire éliminer complètement l'anonymat des détenteurs de cryptomonnaies. Cette présentation aura pour objectif de passer en revue ces différentes techniques pour expliquer leurs forces et leurs faiblesses. Cette présentation nous permettra également de présenter l'outil BitCluster tant dans sa forme gratuite que commerciale qui mise sur ces techniques pour permettre de rapidement déanonymiser, de façon partielle, les détenteurs de cryptomonnaies.

Mathieu Lavoie, Flare Systems

15h15 (16) Suivre des paiements de cryptomonnaies à la trace : mission impossible?

Au cours des 10 dernières années, des milliers de cryptomonnaies ont été lancées incluant Bitcoin, Ethereum, Dash, Zcash pour ne nommer que celles-ci. Bien que la plupart des cryptomonnaies partagent plusieurs caractéristiques comme un blockchain de transactions, il existe des différences plus ou moins subtiles entre les cryptomonnaies qui peuvent faciliter la tâche des enquêteurs ou encore rendre le suivi des paiements de cryptomonnaies complètement impossible, même pour de grandes entités de renseignement étatiques. L'objectif de cette présentation est d'identifier les meilleures techniques pour suivre des paiements de cryptomonnaies. Nous verrons que certaines cryptomonnaies offrent des perspectives d'enquêtes beaucoup plus intéressantes que d'autres. Cette présentation offrira par ailleurs une introduction au fonctionnement des cryptomonnaies pour les personnes qui commencent à s'intéresser au phénomène.

David Décary-Hétu, Professeur adjoint, École de criminologie, Université de Montréal

Piste 5 Amenez votre portable (avancé) (Salle 1340)

14h45 (17) Buscador : un outil puissant et polyvalent

Buscador (qui en espagnol signifie Chercheur), est un système d'exploitation conçu spécifiquement pour l'enquête en ligne à partir des sources ouvertes. Le système d'exploitation basé en Linux, contient les principales applications et des extensions utilisées couramment par les cyberenquêteurs pour notamment l'analyse de profils dans les médias sociaux (Twitter, Instagram), l'analyse de nom de domaine et sous-domaines, le téléchargement et la conversion de vidéos ainsi que l'extraction de métadonnées. L'objectif de cette présentation est de passer en revue ces applications à l'aide d'exemples concrets.

Pour le participant, il est suggéré d'être familier avec l'environnement des machines virtuelles (VMware ou Virtual Box) ainsi que le système d'exploitation Linux.

Philippe Lefebvre, Conseiller renseignement chez Hydro-Québec

15h15 (18) L'automatisation des recherches en sources ouvertes : un mythe ou réalité?

Cette présentation vise à introduire différents modules de recherches en sources ouvertes et démontrer s'ils sont pertinents. Bien que la majorité des recherches en sources ouvertes soient encore effectuées manuellement, plusieurs plateformes et outils maintenant disponibles permettent aux chercheurs et aux analystes d'automatiser certains processus. Cette présentation sous forme de démonstration/discussion vise à sensibiliser, informer et aider les professionnels et les décideurs au sujet de l'automatisation des recherches en sources ouvertes.

Sébastien Ruel, Analyste

15h45 Quand les social botnets manipulent l'information : Le cas du #Brexit (Salle 1140)

Il existe aujourd'hui des botnets investis dans la manipulation de l'information et dans la diffusion de contenus à large échelle. Si le phénomène des botnets n'est pas nouveau, il n'en reste pas moins que l'usage de ces « armées de botnets » dans la propagation de propagande est un phénomène relativement récent et a été en grande partie publicisé à la suite de l'élection présidentielle américaine de 2016. Ces botnets peuvent être relativement simples en se contentant de retweeter du contenu, à plus sophistiqués en cherchant à imiter le comportement humain dans la communication. Cette présentation se basera sur une étude de cas : celle de l'implication de botnets lors du Brexit. Il s'agira de montrer que si les effets de ces logiciels sont aujourd'hui difficiles à évaluer, ils sont néanmoins devenus des moyens puissants pour accroître la portée des messages et créer un faux sentiment de soutien concernant des thématiques qui polarisent et clivent la société.

Valentine Crosset, Doctorante, École de Criminologie, Université de Montréal

16h00 Mot de la fin

16h05 4 @ 7 (Salon Maurice Labbé – 6225, 6e étage)

Suivez le CICC

www.facebook.com/CICCUdeM

www.youtube.com/user/cicctv

www.fr.twitter.com/CICCTweet