Faculté des sciences
Centre de formation en technologies de l'information

UNIVERSITÉ DE SHERBROOKE

1. Identification et Renseignements Généraux

Titre du cours :	INF807 – Criminalistique en sécurité TI
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet réaction
Cours préalables ou concomitants :	INF804 - Sécurité des logiciels (suggéré)
Lieu du cours :	Moodle
Session :	Hiver 2020
Date de début :	9 janvier 2020
Date de fin :	16 avril 2020
Date limite d'abandon :	16 mars 2020
Rencontres synchrones AdobeConnect :	Tous les jeudis à partir du 9 janvier 2020 18h00 à 21h00
Personne(s)-ressource(s) :	Michel Céré
Courriel(s) :	michel.cere@usherbrooke.ca

2. Mise en contexte

Description officielle du cours

Cible(s) de formation :

À la fin de cette activité pédagogique, l'étudiante ou l'étudiant sera capable :

1. Comprendre la criminalistique, son importance dans les organisations ainsi que la gouvernance et les bonnes pratiques auxquelles elle peut recourir.
2. Connaître les principes de base du droit criminel canadien et les crimes liés aux technologies.
3. Évaluer si les règles de sécurité minimale en matière de criminalistique sont présentes et suffisantes.
4. Comprendre les différentes étapes d'une enquête lors d'un incident de sécurité.
5. Connaître les règles et mécanismes de conservation de la preuve numérique en droit criminel canadien.
6. Connaître les mécanismes d'utilisation de la preuve numérique et du témoignage d'un expert dans le cadre d'un procès criminel.
7. Connaître différents enjeux liés à la capture et la conservation de la preuve en TI.

Contenu :

Les incidents en matière de sécurité informatique sont monnaie courante à tel point que les organisations ne se demandent plus si elles vont subir une attaque informatique, mais quand. En effet, peu importe la façon dont une organisation tente de se prémunir contre une attaque

informatique, force est de constater que nul n'est à l'abri d'une faille de sécurité. Lorsque l'incident se produit, les actions des différents intervenants peuvent être critiques quant à l'obtention de preuves et à leur conservation en vue d'une part de déterminer la cause de l'incident et d'autre part, d'en gérer les conséquences.

Place du cours dans le programme

INF807 est un cours obligatoire dans le programme. Il présente les aspects liés à la sécurité visant à conserver découvrir la preuve, a sécurité informatique dans la perspective du développement logiciel et des données.

Objectifs du microprogramme

Le Microprogramme en sécurité informatique - volet prévention permet à l'étudiante ou à l'étudiant de :

- maîtriser les tenants et aboutissants de la sécurité informatique contemporaine;
- maîtriser la nature des surfaces d'attaque exposées par une infrastructure de TI;
- savoir concevoir, mettre en oeuvre et documenter une stratégie efficace pour protéger et défendre ces surfaces d'attaque, en tenant compte d'un budget de ressources donné;
- pouvoir critiquer une telle stratégie telle que mise en place dans une organisation, de manière à en corriger les faiblesses.

Charge de travail

Les 3 crédits équivalent à 135 heures, réparties de la façon suivante :

Enseignement magistral	30 heures
Atelier (s)	6 heures
Présentations (assister et prestation)	3 heures
Évaluation	6 heures
Travaux	50 heures
Lectures	40 heures
TOTAL	135 heures

Particularités

3. Considérations Méthodologiques

Approches méthodologique et pédagogique

Le cours INF807 privilégie une diversité de méthodes pédagogiques, dont la pratique réflexive, les groupes de discussion, l'apprentissage par problèmes, la méthode des cas et l'apprentissage par projet. Il est attendu que chaque individu participant au cours s'engage de manière active et régulière en intervenant dans les séances AdobeConnect et les forums de

discussion.
Puisqu'il s'agit d'un cours en ligne, toutes les ressources et les consignes sont disponibles sur Moodle 2: http://www.usherbrooke.ca/moodle2-cours/.

4. Déroulement du cours

Séance 1 - 9 janvier 2020

Introduction et présentation du plan de cours

Petite histoire de la cybercriminalité

Contexte: statistiques sur le nombre de données potentiellement créées par jour, fraudes, violations de politiques, espionnage, etc.

Définitions conceptuelles (science de la criminalistique, criminalistique numérique (digitale), etc.

Gouvernance en criminalistique numérique (digitale)

La criminalistique numérique (digitale) dans les organisations

- Ce qu'est la criminalistique numérique (digitale), pourquoi c'est important, etc.
- Organisme de renforcement des lois
- Entreprises, sociétés, etc.
- Gouvernements, agences, etc.
- Firmes de consultants

Séance 2 - 16 janvier 2020

Concepts de droit pénal et criminel
Fardeau de la preuve
Exemples d'infractions et crimes liés aux technologies
Les droits fondamentaux et l'impact sur la preuve

Séance 3 - 23 janvier 2020

ATELIER 1: Scénario d'incident - Comment réagissent-ils et jusqu'où? Quand croient-ils avoir terminé?

L'événement
Prise de décision
Escalade
Communication
Documentation

Séance 4 - 30 janvier 2020

Rappel sur les règles de sécurité qui doit être présente.
Les fondations

- ISO 27001

- Les laboratoires d'enquêtes (ISO 17025)
- Gestion des incidents (ISO 27035)
- Cryptographie
- Disponibilité, intégrité et confidentialité
- Relève / conformité

Mettre en place une organisation de criminalistique numérique (digitale);

- Besoin de la criminalistique;
- Structure de criminalistique;
- Interactions avec les autres structures organisationnelles;
- Politiques, etc;
- Standards, guides de bonnes pratiques, etc.

Séance 5 - 6 février 2020

TP1 : Types d'incidents de sécurité et vulnérabilités : Exemples récents
Thèmes sur les failles : Matérielles / Humaines / Logicielles / Fournisseurs / Externes / etc.
Thèmes sur les vulnérabilités : Potentielles / Théoriques ou futures / Actuelles / etc.

SLA / Conformité / Légal
ODPRD - GDPR
Gestion de crise
Post événement
La gestion de l'incident
Impacts
Analyse
Quelques solutions technologiques de support à la criminalistique

Séance 6 - 13 février 2020

Principes et processus d'enquêtes (ISO 27043)

Séance 7 - 20 février 2020

TP2 : Capture de la preuve technologique
Thèmes : Base de données / iOS / Android / Windows / Linux / MacOS / Cloud / IoT (Internet of Things) / Web / etc.

Recherche de preuve numérique (ISO 27050)

Séance 8 - INTRA - 27 février 2020

Séance 9 - 5 mars 2020

TP3 : La gestion de crise : Exemples récents
Thèmes : Gestion d'une crise liée à un incident de sécurité majeur et récent.

Séance 10 - 12 mars 2020

Identification, acquisition et préservation des évidences digitales (ISO 27037)

Séance 11 - 19 mars 2020

TP4 : Utilisation de preuves numériques dans un procès
Thèmes : Procès en cours ou passé, civil ou criminel, canadien ou américains / etc.

Analyse et interprétation des évidences digitales (ISO 27042)

Séance 12 - 26 mars 2020

Guide sur la conformité des méthodes d'enquêtes (ISO 27041)

Séance 13 - 2 avril 2020

TP5 : Enjeux liés à la preuve numérique (ex. : Cryptographie / Réseaux / Cloud / Juridiction / Outils / etc.)
Thèmes : Capture / Analyse et interprétation / Conservation / Communication

Administration de la preuve numérique en matière pénale et criminelle au Canada

L'utilisation de la preuve numérique et le témoignage d'un expert dans le cadre d'un procès criminel

Séance 14 - 9 avril 2020

Enjeux liés à la capture de la preuve et sa conservation en TI.
Par exemple:

- Cryptographie
- Réseaux
- Nuages
- Juridiction
- Outils

Séance 15 - Examen final - 16 avril 2020

5. ÉVALUATION DES APPRENTISSAGES

Évaluation No 1: TPs

Compétence mobilisée	Capacité à exprimer avec synthèse une problématique de sécurité TI
Description	Présentations au groupe de la problématique à traiter et traiter lors du projet. Des temps maximums de 5 et de 15 minutes sont alloués.

Critères d'évaluation	Grille d'évaluation dans Moodle Un verbatim à haut niveau devra être déposé avant le début de la séance sur Moodle.
Notation	10 % de la note finale par TP pour un total de 50%
Date de remise	06 février 2020, 18h00 20 février 2020, 18h00 05 mars 2020, 18h00 19 mars 2020, 18h00 02 avril 2020, 18h00

Évaluation No 2: Participation à l'atelier

Compétence mobilisée:	L'ensemble de la matière vue durant le cours
Description	L'étudiant démontre son intérêt et son évolution par sa participation lors de l'atelier qui aura lieu dans un endroit à déterminer.
Critères d'évaluation	Participation lors de l'atelier.
Notation	5 % de la note finale
Date de remise	N/A

Évaluation No 3: Examen intra

Compétence mobilisée	L'ensemble de la matière vue durant le cours
Description	Sous la forme d'un quiz contenant 1 question à développement (10 pts) et 10 questions à choix multiples (1 pt chacune), démontrer la compréhension des principaux concepts en sécurité de l'information et de la cybersécurité. Il s'agit d'un examen d'une heure à faire sur la plateforme Moodle
Critères d'évaluation	Parmi les critères: • Justesse et complétude de la réponse • Richesse des éléments fournis
Notation	20 % de la note finale
Date de remise	27 février 2020, de 18h00 à 21h00

Évaluation No 4: Examen final

Compétence mobilisée:	L'ensemble de la matière vue durant le cours
Description	Sous la forme d'un quiz contenant 2 questions à développement

	(10 pts) et 25 questions à choix multiple (25 pts), démontrer la compréhension de la matière vue dans le cours. Il s'agit d'un examen de trois heures à faire sur la plateforme Moodle.
Critères d'évaluation	Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.
Notation	25 % de la note finale
Date de remise	16 avril 2020, de 18h00 à 21h00

6. Règlements et autres

Promotion de la qualité de la langue

Pour promouvoir la qualité du français, les fautes d'orthographe, de lexique et de syntaxe sont prises en considération. Dans tous les travaux, elles seront comptabilisées comme suit : 0,25 pour chaque faute jusqu'à concurrence de 10 % de la note maximale pour chaque objet d'évaluation.
Vous êtes fortement encouragés à effectuer une relecture attentive des travaux avant leur remise officielle et à utiliser les outils de correction disponibles.

Présentation des travaux

Les travaux doivent obligatoirement être soumis sur le site Moodle 2 du cours à la date d'échéance prévue.
Les fichiers électroniques doivent obligatoirement être soumis en format PDF pour faciliter l'insertion de commentaires.
L'intitulé du fichier doit comprendre le numéro du travail, votre nom et votre prénom (exemple: pour le travail 1: Travail1_Nom_Prénom.docx).

Délits relatifs aux études

Le terme « délit » désigne toute infraction ou toute tentative de commettre une infraction, ainsi que toute participation à une infraction ou à une tentative de commettre une infraction, par une personne assujettie à une règle qui lui est applicable en raison de son statut.
Outre la contravention à toute règle applicable à la personne assujettie en vertu d'une source autre que le Règlement des études (Règlement 2575-009), l'Université considère trois (3) types de délits : les délits relatifs aux études, les délits relatifs à l'Université ou aux membres de la communauté universitaire et les délits relatifs aux activités de stage. Ces délits sont présentés aux articles suivants :
Un délit relatif aux études désigne tout acte trompeur ou toute tentative de commettre un tel acte, quant au rendement scolaire ou une exigence relative à une activité pédagogique, à un programme d'études ou à un parcours libre. Sont notamment considérés comme un délit relatif aux études les faits suivants :

a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne ou des passages ou idées tirés de l'œuvre d'autrui (ce qui inclut notamment le fait de ne pas indiquer la source d'une production, d'un passage ou d'une idée tirés de l'œuvre d'autrui);

b) commettre un auto-plagiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);
c) usurper l'identité d'une autre personne ou procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
d) fournir ou obtenir toute aide non autorisée, qu'elle soit collective ou individuelle, pour une production faisant l'objet d'une évaluation;
e) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique.[1]

Respect des délais

Tout défaut de remplir les exigences d'évaluation prévues au plan de l'activité pédagogique, par exemple pour une production attendue ou un examen, entraîne la **valeur zéro (0)**, à moins que les raisons et les preuves fournies par l'étudiante ou l'étudiant n'aient été acceptées par la faculté ou le centre universitaire de formation.

L'étudiante ou l'étudiant doit **justifier par écrit** son défaut de se soumettre à une évaluation auprès de la faculté ou du centre universitaire de formation. Cette justification doit être **déposée dans le respect du délai** déterminé au règlement complémentaire de la faculté ou du centre universitaire de formation.

Le cas échéant, la faculté ou le centre universitaire de formation peut accorder un délai pour la présentation d'une production, soumettre l'étudiante ou l'étudiant à un examen supplémentaire, apporter des modifications aux exigences de stage ou ne pas tenir compte de cet élément d'évaluation dans l'attribution de la note finale.[2]

7. Notation

Comment une cote est évaluée au CeFTI ?

L'attribution d'une cote au CeFTI n'a rien du hasard. Les enseignants doivent identifier les frontières de cote en fonction d'un modèle basé sur la loi de probabilité de Laplace-Gauss. Voici les règles d'attribution en vigueur au CeFTI.

1. Identification d'une moyenne cible pour l'activité par la direction

- Début de programme : [2,6..3,0]
- Milieu de programme : [2,9..3,3]
- Fin de programme : [3.2..3,7]

2. L'enseignant propose des coupures en conformité avec le règlement des études de l'Université, https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

- A+, A, A- : Excellent
- B+, B, B- : Très bien
- C+, C, C- : Bien
- D+, D : Passable
- E : Échec

[1] Extrait du Règlement des études 2017-2018
[2] Extrait du Règlement des études 2017-2018

3. Les cotes sont transmises à la direction du CeFTI avant d'être officialisées.

L'avantage d'un tel système est la transposition du rendement de l'étudiant en fonction du groupe dans lequel il évolue. L'évaluation reste équitable entre les cohortes. L'enseignant a la liberté de proposer une répartition qui déroge de la règle, lorsqu'il juge avoir un groupe particulier.

Ce processus a été discuté et approuvé par le comité de programme au CeFTI le 25 mai 2017.

RÉVISION D'UNE NOTE

L'Université reconnaît à toute étudiante ou étudiant le droit à une révision de la note finale sous forme de lettre qui lui est attribuée pour une activité pédagogique ou le test institutionnel de français (TIF), à la condition qu'elle ou qu'il en fasse la demande au moyen du formulaire institutionnel au plus tard vingt (20) jours ouvrables après que la note confirmée par la faculté ou le centre universitaire de formation apparaît à son dossier.[3]

8. RÉFÉRENCES BIBLIOGRAPHIQUES

OBLIGATOIRE(S)

Aucun

OPTIONNELLE(S)

Årnes, A. (dir.) (2018). *Digital forensics: an academic introduction*. Hoboken, NJ : John Wiley & Sons Inc.

* Canada, Dubois, A. et Schneider, P. (2019). *Code criminel et lois connexes annotés 2020.*

Choo, K.-K. R. et Dehghantanha, A. (dir.) (2017). *Contemporary digital forensic investigations of cloud and mobile applications. Syngress advanced topics in information security. Amsterdam* ; Boston ; Heidelberg ; London ; New York ; Oxford ; Paris ; San Diego ; San Francisco ; Singapore ; Sydney ; Tokyo : Elsevier : Syngress.

Cichonski, P., Millar, T., Grance, T. et Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology (No. NIST SP 800-61r2) (p. NIST SP 800-61r2)*. National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-61r2

Computer Crimes and Digital Investigations (2016). (Second Edition.). Oxford, New York : Oxford University Press.

Future Law: Emerging Technology, Regulation and Ethics (s.d.).Future Law (First Edition.). Oxford, New York : Oxford University Press.

* Gautrais, V. (2018). *La preuve technologique.*

Gogolin, G. (2013). *Digital forensics explained*. Boca Raton, FL : CRC Press.

Grama, J. L. (2015). *Legal issues in information security. Jones & Bartlett Learning information systems security & assurance series (Second edition.)*. Burlington, MA : Jones & Bartlett Learning.

Information Technology Law: The Law and Society (2019). (Fourth Edition.). Oxford, New York : Oxford University Press.

[3] Extrait du Règlement des études 2017-2018 (https://www.usherbrooke.ca/registraire/fileadmin/sites/registraire/documents/Reglement_des_etudes/reglement_2017_09_05.pdf)

Johansen, G. (2017). *Digital forensics and incident response: a practical guide to deploying digital forensic techniques in response to cyber security incidents.*
Johnson, L. (2014). *Computer incident response and forensics team management: conducting a successful incident response*. Amsterdam ; Boston : Elsevier, Syngress.
* Manarin, B. (2017). *Forensic evidence in context: cases, materials and commentaries*. Toronto, ON : Thomson / Carswell.
* Patenaude, P. (2003). *L'expertise en preuve pénale: les sciences et techniques modernes d'enquête, de surveillance et d'identification*. Cowansville, QC : Éditions Y. Blais.
* Popa, C. (2017). *The Canadian cyberfraud handbook: a professional reference: how to keep up with the evolution of deceptive practices and reduce the erosion of online trust*. Toronto, Ontario : Thomson Reuters Canada Limited.
Sachowski, J. (2016). *Implementing digital forensic readiness: from reactive to proactive process.* Amsterdam : Syngress.
Salhany, R. E. et Salhany, R. E. (2013). *The practical guide to evidence in criminal cases.*
Sammons, J. (2014). *The basics of digital forensics: the primer for getting started in digital forensics (2nd edition.)*. Waltham, MA : Elsevier.
Sammons, J. (dir.) (2015). *Digital forensics: threatscape and best practices*. Waltham, MA : Syngress is an imprint of Elsevier.
Sammons, J. et Daniel, L. (2017). *Digital forensics trial graphics: teaching the jury through effective use of visuals*. London, United Kingdom ; San Diego, California : Academic Press.
* Scanlan, D. M. (2011). *Digital evidence in criminal law. Aurora, Ont : Canada Law Book*.
Shavers, B. (2013). *Placing the suspect behind the keyboard: using digital forensics and investigative techniques to identify cybercrime suspects*. Waltham, MA : Syngress is an imprint of Elsevier.
Shavers, B. et Bair, J. (2016). *Hiding behind the keyboard: uncovering covert communication methods with forensic analysis*. Amsterdam : Boston : Elsevier.
* Smyth, S. M. (2015). Cybercrime in Canadian Criminal law (Second edition.). Toronto, Ontario : Carswell.
Watson, D. (2013). *Digital forensics processing and procedures: meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements*. Amsterdam : Elsevier.

* Références canadiennes.