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 2022
Date de début :	06 janvier 2022
Date de fin :	22 avril 2022
Date limite d'abandon :	
Rencontres synchrones AdobeConnect :	Tous les jeudis à partir du 06 janvier 2022 18h30 à 21h30
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 œuvre 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 - 06 janvier 2022 - Introduction et présentation du plan de cours
Séance 2 - 13 janvier 2022 - Introduction aux concepts de droit pénal et criminel*
Séance 3 - 20 janvier 2022 - Sources des besoins liés à la criminalistique*
Séance 4 - 27 janvier 2022 - L'événement – Atelier*
Séance 5 - 03 février 2022 - Les préalables à la criminalistique*
Séance 6 - 10 février 2022 - Le processus d'enquête en criminalistique : L'identification*
TP-Présentations sur le thème « La gestion de crise : Exemples récents »
Séance 7 - 17 février 2022 - Le processus d'enquête en criminalistique : La cueillette*
TP-Présentations sur le thème « Capture de la preuve technologique »
Séance 8 - 24 février 2022 - Intra (15%) - Conférence*
Séance 9 - 03 mars 2022 - Le processus d'enquête en criminalistique : L'examen*
TP-Présentations sur le thème « Types d'incidents de sécurité et vulnérabilités »
Séance 10 - 10 mars 2022 - Le processus d'enquête en criminalistique : L'analyse*
TP-Présentations: « Outils de gestion des évidences digitales ou de la conformité »
Séance 11 - 17 mars 2022 - Le processus d'enquête en criminalistique : La présentation*
TP-Présentations sur le thème : « Utilisation de preuves numériques dans un procès »
Séance 12 - 24 mars 2022 - La preuve numérique en matière criminelle et pénale*
Séance 13 - 31 mars 2022 - Enjeux liés à la capture de la preuve et sa conservation en TI*
TP-Présentations sur le thème « Enjeux liés à la preuve numérique »
Séance 14 - 7 avril 2022 - Présentations
TP-Présentations obligatoire pour tous comptant pour deux (2) présentations sur le thème « Applicabilité des concepts de criminalistique dans le cadre de vos environnements professionnels » Pour les groupes ayant moins de 10 participants.
Séance 15 - 14 avril 2022 - Examen final

***PRENDRE NOTE :** Sauf pour l'intra et l'examen final, l'ordre et le contenu des séances peut être appelés à changer selon la disponibilité des conférenciers.

5. ÉVALUATION DES APPRENTISSAGES

Évaluation No 1: Présentations individuelles ou de groupe selon le nombre d'inscription.

Compétence mobilisée	Capacité à exprimer avec synthèse une problématique de sécurité TI
Description	Présentations d'environ 10 minutes au groupe de la problématique analysée. La durée sera précisée sur Moodle peu après le début de la session.
Critères d'évaluation	Grille d'évaluation sur Moodle Un verbatim à haut niveau devra être déposé avant le début de la séance sur Moodle.
Notation	40 % de la note finale. La pondération sera répartie proportionnellement selon le nombre de présentations que le groupe sera en mesure de faire pendant la session et qui sera déterminé lors des premières séances.
Date de remise	À déterminer lors des premières séances.

Évaluation No 2: Compte rendu de conférences

Compétence mobilisée:	Capacité à comprendre les concepts présentés lors de la conférence et d'en synthétiser l'essence pour en exprimer les différents enjeux
Description	Sur la plateforme Moodle ou sinon sous la forme d'un écrit dans un format PDF d'environ 250 mots, le compte rendu devra d'abord positionner la conférence dans son contexte. Puis, devront être indiqués les différents concepts, enjeux ou constats qui seront présentés. Sans répéter les éléments présentés lors de la conférence, les étudiants énuméreront les constats ou observations qu'ils retiennent. Enfin, les étudiants devront formuler une critique ou appréciation qui permettra aux conférencières ou conférenciers d'améliorer leurs présentations.
Critères d'évaluation	Grille d'évaluation sur Moodle.
Notation	20 % de la note finale. La pondération individuelle sera répartie proportionnellement selon le nombre de conférence que nous serons en mesure de tenir.
Date de remise	Avant la prochaine séance qui suit la présentation. La ou les dates restent à déterminer selon la disponibilité des conférenciers et selon le choix des présentations.

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	15 % de la note finale
Date de remise	24 février 2022, de 18h30 à 19h30

Évaluation No 4: Examen final

Compétence mobilisée:	L'ensemble de la matière vue durant le cours
Description	Sous la forme d'un questionnaire à compléter chez soi ou encore par le biais d'un examen sur la plateforme Moodle visant à démontrer la compréhension de la matière vue dans le cours. Il s'agit d'un travail ou 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, les détails seront disponibles sur Moodle dans le courant de la session.
Notation	30 % de la note finale
Date de remise	À déterminer pendant la session ou lors de la dernière séance.

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.
Sauf s'il est demandé de compléter directement sur la plateforme Moodle, la remise des fichiers électroniques doivent obligatoirement être soumis en format PDF.
L'intitulé du fichier doit comprendre le sigle du cours, la date de remise, votre nom et votre prénom.
(exemple: pour le travail 1: INF807_2022-01-10_Nom_Prénom.pdf).
S'il s'agit d'un travail de groupe, la nomenclature du fichier doit comprendre le sigle du cours, a date de présentation, le numéro de groupe sur Moodle ainsi que le nom de famille des membres du groupes
(Exemple : INF807_2022-01-10_Gr1_Nomdefamille1_Nomdefamille2_Nomdefamille3.pdf)

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.

[1] Extrait du Règlement des études 2017-2018

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

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]

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

8. RÉFÉRENCES BIBLIOGRAPHIQUES

OBLIGATOIRE(S) Aucun

OPTIONNELLE(S)

- *A Brief History of Cyber Crime (2016, août 17).Florida Tech Online. Site téléaccessible à l'adresse <https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/>. Consulté le 10 décembre 2019.
- *Amelia Thatcher (2017). La cybercriminalité en première ligne. GRC Gazette, 79(3), 17.
- **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.*
- *CSA-ISO/IEC (2013). *Information security incident management* (No. 27035) (p. 55).
- *CAN/CSA-ISO/IEC (2013). *Principes et processus d'investigation sur incident* (No. 27043) (p. 55).
- *CAN/CSA-ISO/IEC (2018a). Electronic discovery — Part 3: *Code of practice for electronic discovery* (No. 27050-3:18).
- *CAN/CSA-ISO/IEC (2018b). *Lignes directrices pour l'analyse et l'interprétation des preuves numériques* (No. 27042:F18).
- *CAN/CSA-ISO/IEC (2018c). *Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques* (No. 27037:F18).
- *CAN/CSA-ISO/IEC (2018d). *Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident* (No. 27041:F18).
- *CSA ISO/IEC (2013). Electronic discovery — Part 2: *Guidance for governance and management of electronic discovery* (No. 27050-2:19).
- 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
- Daniel, L. et Daniel, L. (2012). *Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom*. Waltham, MA : Syngress/Elsevier.
- Deidre Seiden (2017a). *En quête d'éléments de preuve concrets.* GRC Gazette, 79(3), 16.
- Deidre Seiden (2017b). *Interprétation de données par les experts en criminalistique numérique*. GRC Gazette, 79(3), 10-11.
- Deidre Seiden (2017c). *L'union fait la force - Une nouvelle équipe s'attaque à la cybercriminalité*. GRC Gazette, 79(3), 7-9.
- *Digital Forensics Models* (2016, janvier 25).Infosec Resources. Site téléaccessible à l'adresse <https://resources.infosecinstitute.com/digital-forensics-models/>. Consulté le 12 février 2020.
- *Fouilles, saisies et perquisitions de données informatiques* (s.d.). Consulté à l'adresse

(https://www.usherbrooke.ca/registraire/fileadmin/sites/registraire/documents/Reglement_des_etudes/reglement_2017_09_05.pdf)

https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22849/Ellyson_Laura_2018_memoire.pdf?sequence=2&isAllowed=y

- Gautrais, V. (2018). *La preuve technologique.*
- Gouvernement du Canada, G. royale du C. (2014, décembre 16). *Cybercriminalité : survol des incidents et des enjeux au Canada* | Gendarmerie royale du Canada. Site téléaccessible à l'adresse <http://www.rcmp-grc.gc.ca/fr/cybercriminalite-survol-des-incidents-et-des-enjeux-au-canada>. Consulté le 21 novembre 2017.
- ISO/IEC (2014). *Vulnerability disclosure* (No. 29147). Consulté à l'adresse https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip
- ISO/IEC (2015). *Gouvernance du cadre de risque forensique numérique* (No. 30121).
- ISO/IEC 17025 - *Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais* (s.d.)., 8.
- ISO/IEC (2019). Electronic discovery — Part 1: *Overview and concepts* (No. 27050-1). Consulté à l'adresse https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-1:ed-2:v1:en
- Jeffrey Thomson (2017). *Quel est le plus grand défi de la police en matière de cybercriminalité?* GRC Gazette, 79(3), 12-13.
- Joint Task Force Transformation Initiative (2018). *Risk management framework for information systems and organizations:: a system life cycle approach for security and privacy* (No. NIST SP 800-37r2) (p. NIST SP 800-37r2). Gaithersburg, MD : National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-37r2
- Katherine Aldred (2017). *Sur la voie de la « cybercompétence ».* GRC Gazette, 79(3), 4.
- Kissel, R. (s.d.). NIST Special Publication 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, 68.
- Kosseff, J. (2019). *Cybersecurity law* (Second edition.). Hoboken : Wiley.
- Laykin, E. (2013). *Investigative computer forensics: the practical guide for lawyers, accountants, investigators, and business*. Hoboken : John Wiley.
- Pollitt, M. (2010). *A History of Digital Forensics*. In K.-P. Chow et S. Shenoi (dir.), Advances in Digital Forensics VI (Vol. 337, p. 3-15). Berlin, Heidelberg : Springer Berlin Heidelberg. doi:10.1007/978-3-642-15506-2_1
- *Revue de droit criminel: Informatique judiciaire : Guide à l'intention des intervenants en cas d'incident de sécurité informatique* (2011, décembre 10).Consulté à l'adresse http://revuededroitcriminel.blogspot.com/2011/12/informatique-judiciaire-guide.html
- Ross, R., McEvilley, M. et Carrier Oren, J. (2016). Systems Security Engineering: *Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (No. NIST SP 800-160) (p. NIST SP 800-160). National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-160
- Sammons, J. (dir.) (2015). *Digital forensics: threatscape and best practices*. 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.
- Sheetz, M. (2015). *Computer Forensics An Essential Guide for Accountants, Lawyers, and Managers*. Consulté à l'adresse https://www.wiley.com/en-ca/Computer+Forensics%3A+An+Essential+Guide+for+Accountants%2C+Lawyers%2C+and+Managers-p-9781119120278

* Références canadiennes.