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 :	Microsoft Teams
Session :	Hiver 2024
Date de début :	11 janvier 2024
Date de fin :	25 avril 2024
Date limite d'abandon :	15 mars
Rencontres synchrones via la MS Teams:	Tous les jeudis de 18h30 à 21h20
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 visant à découvrir, collecter, conserver et présenter la preuve numérique tout en assurant la sécurité informatique dans la perspective du développement logiciel et des données.

Objectifs du microprogramme

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

- maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure;
- savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale;
- savoir dresser et exécuter un plan d'intervention en cas d'incident et de brèche de données, de manière à trouver le meilleur compromis entre la minimisation des dommages et l'interruption des activités de l'organisation.

Charge de travail

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

Enseignement magistral	30 heures
Atelier (s)	3 heures
Présentations (assister et prestation)	7 heures
Évaluation	5 heures
Travaux	50 heures
Lectures	40 heures
TOTAL	135 heures

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 MS Teams et les forums de discussion. Toutes les ressources et les consignes sont disponibles sur le site Moodle du cours: https://moodle.usherbrooke.ca/course/view.php?id=28238

Prendre note que la maîtrise de l'anglais est requise pour certaines lectures et pour les conférences qui peuvent se dérouler en anglais.

4. Déroulement du cours

Séance 1 – 11 janvier 2024 – Introduction et présentation du plan de cours
Séance 2 – 18 janvier 2024 – Introduction aux concepts de droit pénal et criminel*
Séance 3 – 25 janvier 2024 – Sources des besoins liés à la criminalistique*
Séance 4 – 01 février 2024 – L'événement – Atelier*
Séance 5 – 08 février 2024 – Les préalables à la criminalistique*
Séance 6 – 15 février 2024 – Le processus d'enquête en criminalistique : L'identification*
Séance 7 – 22 février 2024 – Le processus d'enquête en criminalistique : La cueillette*
Séance 8 – 29 février 2024 – Intra (15%) - Conférence*
Relâche – 07 mars 2024 – Aucun cours
Séance 9 – 14 mars 2024 – Le processus d'enquête en criminalistique : L'examen*
Séance 10 – 21 mars 2024 – Le processus d'enquête en criminalistique : L'analyse*
Séance 11 – 28 mars 2024 – Le processus d'enquête en criminalistique : La présentation*
Séance 12 – 04 avril 2024 – La preuve numérique en matière criminelle et pénale*
Séance 13 – 11 avril 2024 – Enjeux liés à la capture de la preuve et sa conservation en TI*
Séance 14 – 18 avril 2024 – Révision de la matière - Conférence*
Séance 15 – 25 avril 2024 – Examen final (30%)

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

5. Échéancier des présentations

Séances	Dates	Thèmes (à titre indicatif)
6	15 février 2024	Différences entre criminalistique et sécurité des TI
7	22 février 2024	Outils de détection d'incidents de sécurité et vulnérabilités
9	14 mars 2024	Outils de capture de la preuve technologique
10	21 mars 2024	Outils de gestion des dossiers d'enquête
11	28 mars 2024	Utilisation de preuves numériques dans un procès – Exemples
13	11 avril 2024	Enjeux de criminalistique ailleurs dans le monde

Selon le nombre de participants au cours, les présentations seront individuelles ou en équipe.

6. Évaluation des apprentissages

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

Compétence mobilisée	Capacité à exprimer avec synthèse une problématique de sécurité TI
Description	Présentations de 15 minutes au groupe de la problématique analysée.
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 qui sera déterminé lors des premières séances.
Date de remise	À déterminer lors des premières séances.

Université de Sherbrooke

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 directement et d'environ 300 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	10 % de la note finale. La pondération individuelle sera répartie proportionnellement selon le nombre de conférences que nous serons en mesure de tenir.
Date de remise	Au plus tard, le dimanche suivant la conférence avant 23h59. La ou les dates restent à déterminer selon la disponibilité des conférenciers.

Évaluation No 3: Compte rendu de présentations

Compétence mobilisée:	Capacité à comprendre les concepts présentés par ses collègues, d'en synthétiser l'essence pour en exprimer les différents enjeux
Description	Directement sur la plateforme Moodle, le compte rendu devra d'abord positionner la ou les présentations dans leurs contextes. Puis, devront être indiqués les différents concepts, enjeux ou constats qui seront présentés. Sans répéter les éléments présentés, les étudiants énuméreront les constats ou observations qu'ils retiennent. Ensuite, les personnes étudiantes devront comparer les présentations entre elles afin d'en identifier les principales forces et faiblesses. Enfin, les étudiants devront formuler une critique ou appréciation qui permettra aux présentateurs de s'améliorer.
Critères d'évaluation	Grille d'évaluation sur Moodle.
Notation	5 % de la note finale. Chaque compte rendu compte pour 2,5%. Au choix, lorsque l'équipe ne présente pas l'un des thèmes.
Date de remise	Au plus tard, le dimanche suivant la présentation avant 23h59.

Université de Sherbrooke

Évaluation No 4: Examen intra

Compétence mobilisée	L'ensemble de la matière vue durant le cours
Description	Sous la forme d'un quiz pouvant contenir des questions à développement, à choix multiples, des mots cachés ou autres formes de questions, cette évaluation vise à 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 2 heures 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	Lors de la 8e séance pendant la période du cours

Évaluation No 5: 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 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 doit obligatoirement être soumise 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 groupe (Exemple : INF807_2022-01-10_Gr1_Nomdefamille1_Nomdefamille2_Nomdefamille3.pdf)

Université de Sherbrooke

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]

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

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]

[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)

8. RÉFÉRENCES BIBLIOGRAPHIQUES

OBLIGATOIRE(S) Aucun

OPTIONNELLE(S) Une liste exhaustive sera disponible sur le site Moodle du cours.

Le cours s'inspire librement des références suivantes :

- **Årnes, A. (dir.) (2018). *Digital forensics: an academic introduction*. Hoboken, NJ : John Wiley & Sons Inc.**
- **Årnes, A. (éd.) (2022). *Cyber Investigations: A Research Based Introduction for Advanced Studies* (First Edition.). Hoboken, NJ : John Wiley & Sons Ltd. Consulté à l'adresse https://onlinelibrary.wiley.com/doi/book/10.1002/9781119582021**

Les références suivantes sont les principales utilisées dans ce cours.

- Canada, Dubois, A. et Schneider, P. (2019). Code criminel et lois connexes annotés 2020.
- Edwards, G. (Financial and cybercrime investigator) (2020). Cybercrime investigators handbook (Vol. 1-1 online resource). Hoboken, New Jersey : John Wiley & Sons, Inc. Consulté à l'adresse https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2251615
- Gehl, R. et Plecas, D. (2017). Introduction to Criminal Investigation: Processes, Practices and Thinking. Justice Institute of British Columbia. Consulté à l'adresse https://pressbooks.bccampus.ca/criminalinvestigation/
- Gottardi, E. V., MacLellan, J. A., Lacy, M., Flumerfelt, R., Greenspan, B. H. et Rondinelli, V. (2022). Qualifying and Challenging Expert Evidence. Criminal law series. Toronto, ON : Emond Publishing.
- Greenspan, B. H., Rondinelli, V., Gourlay, M., Jones, B., Makepeace, J. D., Crisp, G. et Pomerance, R. (éd.) (2021). Modern criminal evidence. Toronto, Canada : Emond.
- Hayes, D. R. (2020). A practical guide to digital forensics investigations (Second edition.). Hoboken N J : Pearson.
- Holt, T. J., Bossler, A. M. et Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics: an introduction (Third edition.). New York, NY : Routledge.
- International Conference on Digital Forensics and Cyber Crime (11th : 2020 : Online), Goel, S. (Of U. of A., SUNY), Gladyshev, P., Johnson, D., Pourzandi, M. et Majumdar, S. (2021). Digital Forensics and Cyber Crime: 11th EAI International Conference, ICDF2C 2020, Boston, MA, USA, October 15-16, 2020, Proceedings. Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (Vol. 1-1 online resource (xii, 249 pages) : illustrations (chiefly color)). Cham, Switzerland : Springer International Publishing AG. Consulté à l'adresse https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2747140
- Nelson, B., Phillips, A. et Steuart, C. (2019). Guide to computer forensics and investigations. Informations security (Sixth edition.). Boston, MA : Cengage. Consulté à l'adresse https://faculty.cengage.com/works/9781337568944
- Shahid Jamal Tubrazy (2016). The Digital Evidence Forensic Laws in Canada and USA: Theories, Concepts and Practices. Createspace Independent Publishing Platform.

- 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
- Stoykova, A. (2022). Standards for Digital Evidence: an inquiry into the opportunities for fair trial safeguards through digital forensics standards in criminal investigations. [Groningen] : University of Groningen. doi:10.33612/diss.222646186
- United States. Secret Service (2021). Preparing for a cyber incident (Vol. 1-1 online resource (1 unnumbered page)). Washington, D.C. : United States Secret Service. Consulté à l'adresse https://purl.fdlp.gov/GPO/gpo173431
- Vincent Gautrais (2018). La preuve technologique (2e édition.). LexisNexis.
- Wade, A. (2019). Digital forensics and investigations: from data to digital evidence. Society Publishing. Consulté à l'adresse http://www.societypublishing.com/book/law/digital-forensics-and-investigation-from-data-to-digital-evidence.html

Les normes et standards suivant seront abordés dans le cadre du cours

- CAN/CSA-ISO/IEC (2013). *Principes et processus d'investigation sur incident* (No. **27043**) (p. 55).
- CAN/CSA-ISO/IEC (2018a). Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident (No. **27041**:F18).
- CAN/CSA-ISO/IEC (2018b). Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques (No. **27037**:F18).
- CAN/CSA-ISO/IEC (2018c). Lignes directrices pour l'analyse et l'interprétation des preuves numériques (No. **27042**:F18).
- CAN/CSA-ISO/IEC (2018d). Electronic discovery — Part 4: Technical Readiness (2021) (No. **27050-4**:2021).
- CSA ISO/IEC (2013). Electronic discovery — Part 2: Guidance for governance and management of electronic discovery (2019) (No. **27050-2**:19).
- CSA ISO/IEC (2020). Electronic discovery — Part 3: Code of practice for electronic discovery (2020) (No. **27050-3**:2020).
- 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 (2019). Electronic discovery — Part 1: Overview and concepts (2021) (No. **27050-1**). Consulté à l'adresse https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-1:ed-2:v1:en