Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB6023 Gr. 01
Titre : Forensique numérique avancée et réponse aux incidents
Session : Hiver 2024 Horaire et local
Professeur : Desharnais, Sylvain

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e maîtrisera les concepts théoriques, les méthodologies et processus pour résoudre des problèmes pratiques liés au domaine de la criminalistique numérique et de la réponse aux incidents.

Contenu

Portrait de la cybermenace et de la cybercriminalité. Méthodologies et les processus nécessaires pour détecter les cyber-incidents. Méthodologies d'enquêtes sur les ordinateurs et les réseaux : identification, récupération et évaluation d'éléments de preuves digitaux. Étapes du processus de réponses aux incidents liés à la cybersécurité.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

À la fin du cours, l'étudiant sera en mesure de/d' :
- concevoir des outils d'investigation numérique;
- trouver l'information reliée à un problème de sécurité informatique;
- recueillir des données qui ont été stockées sur des supports numériques;
- concevoir des procédures pour analyser les traces des incidents de sécurité informatique;
- intégrer l'investigation numérique au système de sécurité (défense en profondeur);
- choisir les technologies, les protocoles et les stratégies d'investigation numériques destinés à apporter des preuves numériques;
- identifier les principales menaces pesant sur un réseau informatique;
- intégrer au processus de sécurité les étapes classiques d'une opération d'investigation numérique;
- utiliser une approche éthique à la cueillette de preuves.

Voici certaines compétences complémentaires qui vous seront transmises :
- Capacité à analyser en mode hexadécimal un média ou un fichier;
- Familiarisation avec les logiciels de forensique informatique (FTK et Autopsy SleuthKit);
- Connaissance des sites où chercher des informations de droit canadien et québécois fiables;
- Connaissance de la structure des systèmes de fichiers FAT32 et NTFS;
- Capacité d'analyser une situation d'enquête et de déterminer le meilleur moyen d'en ressortir les preuves nécessaires;
- La capacité de citer ses sources de façon adéquate / selon les normes utilisées au département.

3. Stratégies pédagogiques :

- Cours magistraux donnés en mode non-présentiel (via Zoom)
- Examen de mi-session (en présentiel si la température le permet, sinon à distance via Moodle)
- Examen final (en présentiel si la température le permet, sinon à distance via Moodle)

L'étudiant.e doit avoir une caméra web activée et une session Zoom en cours dans le cas où l'examen se tient à distance.

Les étudiant(e)s qui s'inscrivent à ce cours doivent s'assurer qu'ils ont accès à : un ordinateur (avec un système d'exploitation Windows); une connexion Internet; une caméra web; un microphone; la suite Office 365 (les étudiant(e)s ont un accès gratuit à la suite Office 365 : https://uqo.ca/sti/outils-numeriques).

Le cours utilisera la plateforme Zoom pour les séances de cours. Les étudiant(e)s sont invité(e)s à consulter le Guide d'utilisation de Zoom à l'intention des étudiants, disponible également sur la page Moodle du cours. Site pour soutien de réussite en mode non-présentiel : uqo.ca/etudier-non-presentiel

4. Heures de disponibilité ou modalités pour rendez-vous :

Le chargé de cours sera disponible pour une rencontre individuelle ou de groupe sur Zoom les mardis avant-midi. Pour le rencontrer, prière de prendre rendez-vous en écrivant un courriel (pour cette information, veuillez consulter le site Moodle de ce cours), au moins 72 heures d'avance. La discussion peut porter sur des points liés à la théorie aussi bien que sur des points liés aux travaux pratiques. Lorsque vous demandez un rendez-vous, fournissez heure et date de trois moments disjoints où vous êtes disponible (un mardi avant-midi).

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Présentation du plan de cours, des activités évaluées, introduction et mise en contexte	10 janv. 2024
2	Survol d'une opération d'investigation numérique (Partie 1 – Fondements de l'IN)	17 janv. 2024
3	Aspects techniques – investigation numérique, expressions régulières	24 janv. 2024
4	Stratégies de fouille	31 janv. 2024
5	Analyse de systèmes de fichiers et lecture de données hexadécimales	7 fév. 2024
6	Analyse de systèmes de fichiers et lecture de données hexadécimales	14 fév. 2024
7	Analyse de systèmes de fichiers et lecture de données hexadécimales	21 fév. 2024
8	Forensique volatile et autres forensiques. Pratique d'examen et récapitulation	28 fév. 2024
9	**Semaine d'études**	06 mars 2024
10	**Examen**. Forensique volatile et les autres forensiques	13 mars 2024
11	Survol d'une opération d'investigation numérique (Partie 2 – Saisie éthique)	20 mars 2024
12	Aspects légaux de l'investigation numérique et de la sécurité	27 mars 2024
13	Aspects légaux de l'investigation numérique et de la sécurité	3 avril 2024
14	Réponse aux incidents de sécurité, processus de réponse	10 avril 2024
15	Pratique d'examen, récapitulation et **examen**	17 avril 2024

6. Évaluation du cours :

Cette section renseigne l'étudiante et l'étudiant quant aux différentes évaluations (ex. : travaux et examens) qui auront lieu au cours du trimestre. Voir le tableau des évaluations ci-dessous.

DATE LIMITE d'abandon de cours sans mention d'échec : 26 février 2024.

Veuillez noter : Pour chaque activité évaluée, un énoncé sera remis quelques jours avant le début de la période consacrée à celui-ci. En plus de l'énoncé, vous recevrez les fichiers avec lesquels vous devrez travailler et un briefing vous sera donné à ce sujet. Pour les examens, l'énoncé est intégré à la question. Avant chaque examen, il y aura une séance où l'enseignant résoudra des problèmes similaires à ceux que vous aurez à l'examen.

ChatGPT et autres outils génératifs : Les solutions requises pour les TP et dans les examens se prêtent mal à l'utilisation des outils génératifs. Vous devez traiter les résultats de cette utilisation comme une citation dans le texte et dans la médiagraphie.

Activité évaluée	Mode et date-heure buttoir	%age de la note finale
TP – Stratégies de fouille	En équipe, remise avant le 14 février à 19h00, Moodle	25%
Examen intra (en présentiel si la température le permet, sinon à distance avec caméra web allumée et en session Zoom)	Individuel, le 28 février de 10h00 à 11h30	25%
Travail de session – Trois articles sur un sujet lié au cours (autorisation préalable du sujet par l'enseignant)	En équipe, remise avant le 3 avril à 19h00, Moodle	25%
Examen final (en présentiel si la température le permet, sinon à distance avec caméra web allumée et en session Zoom)	Individuel, le 17 avril de 10h00 à 11h30	25%

La qualité de la langue

Travaux pratiques : Les rapports relatifs aux travaux pratiques doivent être rédigés dans un français intelligible et exempt d'anglicismes. Pour vous aider au niveau des anglicismes, veuillez consulter le site de l'Office de la langue française du Québec au https://www.oqlf.gouv.qc.ca/accueil.aspx . Tout terme accepté comme étant du bon français par cet organisme sera considéré comme correct au niveau de la correction. Les trois ouvrages de de Villers cité dans la bibliographie (section 16 ci-dessous) viennent compléter le site de l'OQLF pour les corrections. 10% de la note des travaux pratiques se rapporte à la qualité du français. Tout travail pratique dont le niveau est si défectueux qu'il devient un obstacle à une correction efficace sera retourné à l'équipe pour qu'il soit redressé dans un délai
de 48 heures. L'équipe perdra alors les 10% du français, même si la copie redressée est dans un français convenable. Si la copie est retournée sans retouche ou très peu de retouches, la copie sera corrigée de la meilleure façon possible et le correcteur accordera seulement 50% de la note issue de cette correction.
Examens : La rédaction d'examen se faisant avec une contrainte de temps, on ne peut exiger des étudiant(e)s le même niveau de français que pour les travaux pratiques. En revanche, une réponse incohérente ou inintelligible ne peut déboucher sur la certitude que la matière a été bien comprise. La qualité du français utilisé par l'élève lors de l'examen doit donc être tel que le correcteur puisse évaluer efficacement cette compréhension de la matière.

Règles de présentation des travaux

Le numéro de l'équipe et les noms des équipiers doivent apparaître en page 1 de tout rapport remis. Les rapports relatifs aux travaux pratiques doivent utiliser le formulaire mis à la disposition des équipes. Les réponses demandées peuvent varier en longueur, allant d'un seul mot à plusieurs lignes. Chaque question doit être répondue indépendamment des autres questions. Les réponses doivent être aussi concises mais aussi précises que possible. Les réponses inutilement longues ne seront pas corrigées car il n'appartient pas au correcteur de choisir les éléments utiles de la réponse parmi les éléments inutiles.

Règles concernant les retards dans la remise des travaux

Les dates des remises des rapports des travaux pratiques sont connues dès le début de la session. Il appartient donc à l'étudiant(e) de planifier correctement la quantité de travail à mettre sur le travail pratique ainsi que le moment où appliquer cet effort. Lorsqu'un travail est remis après la date d'échéance, l'équipe perd 5% pour chaque heure de retard. La remise est considérée en retard lorsque l'heure est commencée (donc : un retard d'une minute est considéré comme une heure de retard). Si l'équipe sait que la remise ne fera pas en temps, elle peut prendre entente avec l'enseignant et convenir d'un nouveau moment pour la remise et de la pénalité qui résultera du retard. Le délai convenu et la pénalité doivent être raisonnables compte tenu des circonstances.

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude. L'utilisation d'un logiciel de médiagraphie comme Zotéro est fortement suggérée.
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)
- Politique sur la liberté académique

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

Notes d'investigation numérique, Sylvain Desharnais, disponibles sur le site Moodle du cours.
Desharnais, S. (2010). Comprendre l'informatique judiciaire. Publié à l'origine chez Guérin, maintenant libre de droit sur Moodle.
de Villers, M.-É. (2021). Multidictionnaire de la langue française (7e éd). Québec Amérique.
Villers, M.-É. de. (1993). La grammaire en tableaux. Québec/Amérique.
Villers, M.-E. de et Desnoyers, A. (2003). La nouvelle grammaire en tableaux et un recueil de conjugaison les modèles pour conjuguer tous les verbes d'usage courant. Québec Amérique.

9. Page Web du cours :

https://moodle.uqo.ca