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 2026 Horaire et local (*non-présentiel – à distance*)
Professeur : Sylvain Desharnais

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 l'investigation numérique et de la réponse aux incidents.

Contenu
Méthodologies d'enquêtes sur les ordinateurs et les réseaux : identification, récupération, préservation et évaluation d'éléments de preuves digitaux. Portrait de la cybermenace et de la cybercriminalité. Méthodologies et les processus nécessaires pour détecter les cyber-incidents. 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);
- Bonne connaissance en droit canadien et québécois;
- 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 en mode non-présentiel (voir hyperlien sur le site Moodle du cours);
- Travaux pratiques;
- Séances de préparation aux examens;
- Examen de mi-session (en non-présentiel);
- Examen final (en non-présentiel).

- 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 11.** La version pro est fortement suggérée);
- Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours;
- L'enseignant est disponible pour vous répondre en moins de 48 heures par courriel ou pour vous rencontrer via Zoom (voir hyperlien sur le site Moodle du cours);
- Le manuel du cours intitulé « Notes d'investigation numérique » (**NIN**), les documents, les diapositives des présentations et le matériel nécessaire au cours sont disponibles sur le site Moodle du cours.
- L'utilisation d'un logiciel de médiagraphie comme Zotéro est fortement suggérée.

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

Communication par courriel (sylvain.desharnais@uqo.ca). Réponse en moins de 48 heures. Pour prendre rendez-vous pour une rencontre Zoom, envoyez un courriel énonçant trois moments non-contigus dans au moins 2 journées différentes. Je suis généralement disponible de 9h00 à 18h00 sauf les mercredis et les jeudis AM.

5. Plan détaillé du cours sur 15 semaines :

Important : Les lectures et les visionnements de capsules indiquées ci-dessous sont à faire avant d'arriver au cours. Les chapitres indiqués sont les chapitres du manuel du cours « Notes d'investigation numériques ».

Semaine	Thèmes	Dates
1	Présentation du plan de cours, des activités évaluées, introduction et mise en contexte Briefing – laboratoire Zéro – Environnements forensiques. Lire : Chap 2000 et 2100	15 jan. 2026
2	Survol d'une opération d'investigation numérique (IN). Fondements de l'IN. Aspects techniques. Lire : Ch. 2400 et 2420. Écouter : V102 et V104	22 jan. 2026
3	Aspects techniques de l'IN. Stratégies de fouille – expressions régulières. Lire : Ch. 2430 et 2500. Écouter : HIN01, HIN02, HIN16, HIN21	29 jan. 2026
4	Stratégies de fouille. Lire : Ch. 2430. Écouter: HIN03, HIN04, HIN20, V110	5 fév. 2026
5	Systèmes de fichiers FAT32. Lire : Ch. 2600 – Intro et FAT32. Écouter : HIN05 à HIN11 (inclusivement) et V108	12 fév. 2026
6	Systèmes de fichiers NTFS. Lire : Ch. 2600 – NTFS et matriciels. Écouter : HIN12 à HIN15, HIN17 et V109	19 fév. 2026
7	Systèmes de fichiers NTFS. Lire : Ch. 2600 – NTFS et matriciels. Écouter : HIN12 à HIN15, HIN17 et V109	26 fév. 2026
8	**Semaine d'études**	2 au 6 mars 2026
9	**Examen de mi-session**	**12 mars 2026**
10	Forensique volatile et autres forensiques. Lire : Ch. 2410 et 2440 à 2470. Écouter : V106 et V107.	19 mars 2026
11	Aspects légaux de l'IN et de la sécurité. Lire : Ch. 2200 et 2300. Faire un survol du document « Articles de loi.pdf ». Écouter : V101 et V105	26 mars 2026
12	Aspects légaux de l'IN et de la sécurité. Lire : Ch. 2200 et 2300.	2 avril 2026
13	Survol d'une opération d'investigation numérique. Saisie éthique. Lire : Ch. 2400 et 2420	9 avril 2026
14	Survol d'une opération d'investigation numérique. Saisie éthique. Lire : Ch. 2400 et 2420 Réponse aux incidents de sécurité, processus de réponse. Lire : Ch. 2830 Biais cognitifs. Renseignements d'origine source ouverte. Lire : Ch. 2810 et 2820	16 avril 2026
15	**Examen final**	**23 avril 2026**

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 : 5 mars 2026
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 – Cas Parisakys	En équipe. Remise avant le 26 fév. à 23h00, Moodle	15%
TP2 – Stratégies de fouille – Cas Des Boies	En équipe. Remise avant le 26 mars. à 23h00, Moodle	15%
Examen intra	Individuel, le 12 mars de 8h45 à 11h15	20%
Travail de session	En équipe. Remise avant le 9 avr. à 23h00, Moodle	20%
Examen final	Individuel, le 23 avril de 8h45 à 11h15	30%

La qualité de la langue dans les 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 (voir la section des références ci-dessous) viennent compléter le site de l'OQLF. 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, ni que le correcteur comprendra votre réponse. La qualité du français utilisé par l'étudiant(e) lors de l'examen doit donc être telle que le correcteur puisse évaluer efficacement cette compréhension de la matière.

Règles de présentation des travaux
Comme les travaux donnent lieu à un rapport sur un formulaire préparé par l'enseignant, vous n'insèrerez pas de page-titre ni de table des matières dans votre rapport pour les cas Parisakys et Des Boies. Le numéro de l'équipe et les noms des équipiers doivent apparaître en page 1 du rapport. 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. Les réponses doivent être aussi concises mais aussi complètes 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
- 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 v2026a. Voir le site Moodle du cours.
- Ne pas acheter : Computer Forensics – Investigation Procedures and Response
- Ne pas acheter : File System Forensic Analysis, Brian Carrier, chez Addison-Wesley
- Ne pas acheter : de Villers, Marie-Éva, chez Québec Amérique :
    - Multidictionnaire de la langue française (7e éd);
    - Multidictionnaire des difficultés de la langue française;
    - La grammaire en tableaux
    - La nouvelle grammaire en tableaux et un recueil de conjugaison

9. Page Web du cours :

https://moodle.uqo.ca