Plan de cours

ÉCOLE POLYTECHNIQUE MONTRÉAL

INF8430 – Investigation numérique en informatique

Département de génie informatique et génie logiciel
Hiver 2023
3 crédits
Triple : 3 / 1,5 / 4,5

Professeur

Prénom et nom :	Sylvain Desharnais
Bureau :	À distance
Téléphone :	Courriel seulement
Courriel :	s.desharnais@polymtl.ca
Disponibilité :	Voir la rubrique « Personnes-ressources » ci-dessous

Description de l'annuaire

Application de techniques et de protocoles d'investigation numériques pour la collecte, l'identification, la description, la sécurisation, l'extraction, l'authentification, l'analyse, l'interprétation et l'explication des données numériques contenues dans des systèmes informatiques et dans des périphériques de stockage. Capture et analyse des données volatiles, notamment des séances actives de réseaux et des processus en cours. Collecte d'informations des navigateurs Web.

Objectifs

À la fin du cours, l'étudiant sera en mesure de/d' :

- gérer les informations sensibles et confidentielles dans les dispositifs de stockage;
- 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.

Après avoir fait les séances de travaux pratiques, l'étudiant sera en mesure de/d' :

- utiliser différentes technologies et protocoles pour la récupération des données d'un système informatique y compris d'un réseau informatique;
- concevoir et développer des protocoles pour faire la collecte de l'information dans des dispositifs de stockage;
- utiliser des logiciels d'investigation numérique.

Méthodes d'enseignement

Le cours comprendra :

- 36 heures d'exposés magistraux (bimodaux L-2710 mercredis 12h45-15h45) au cours desquels l'enseignant présentera le contenu théorique et 3 heures d'exposés (reliés aux travaux de session des étudiants) donnés par les étudiants;
- En cas de problème de santé (ex : COVID), vous serez avisé le plus tôt possible par courriel et l'enseignement se donnera, si possible à distance;
- 21 heures de laboratoires en présence L-4708 (Lundis B1 12h45-15h45) reliés au contenu théorique
- Lectures obligatoires : Seront transmises séparément via le Moodle du cours.

Évaluation

Mode d'évaluation	Quantité	Pondération	Date
Laboratoires	2	20%	Voir section à cet effet ci-dessous
Travail de session	1	30%	
Capsule vidéo	1	10%	
Devoir-maison	1	10%	
Examen final	1	30%	Selon l'horaire qui sera émis par l'École

Important – Note de passage :

La note de passage est une note en double seuil. Pour passer le cours INF8430, vous devrez obtenir au moins **60% sur le cumul** de toutes les activités évaluées ainsi que **50% au global des épreuves par équipe** et **50% au global des épreuves individuelles**. L'étudiant(e) obtenant moins de 20/40 (50%) au global des deux épreuves individuelles verra les notes de ses travaux d'équipe être corrigée à 0% (sans affecter les notes des coéquipiers ayant obtenu au moins 30/60). Tous les étudiant(e)s d'une équipe dont la somme des notes des activités d'équipe est moins de 30/60 (50%) verront les notes de ces épreuves corrigées à 0%.

Personnes-ressources

Le chargé de cours et le chargé de laboratoire.

Le chargé de cours sera disponible pour une rencontre individuelle ou de groupe sur Zoom les **lundis et samedis seulement**. Pour le rencontrer, prière de prendre rendez-vous en écrivant un courriel, au moins 72 heures d'avance, à s.desharnais@polymtl.ca La discussion peut porter sur des points liés à la théorie aussi bien que sur des points liés au travail de session. Lorsque vous demandez un rendez-vous, fournissez heure et date de trois moments où vous êtes disponible (un lundi ou un samedi).

Pour les sujets liés aux laboratoires, veuillez vous adresser directement à la chargée ou au chargé de laboratoire. Marc Dib sera votre chargé de laboratoire et il peut-être contacté au marc-2.dib@polymtl.ca ou via tout autre moyen qu'il indiquera lors de la première séance de laboratoire.

Livres de cours

Notes de cours : « *Notes d'investigation numérique – Version 2023a* », disponible sur le site du cours.

Livre : « *Comprendre l'informatique judiciaire – Tome 1 – Concepts de base* » disponible sur le site du cours.

En réserve à la bibliothèque :
Desharnais, Sylvain. 2010. « *Comprendre l'informatique judiciaire - Tome 1 - Concepts de base* ». Montréal : Guérin, éditeurs ltée, 288 p. ISBN : 9782760172302.
Carrier, Brian. 2005. « *File system forensic analysis* ». Toronto : Addison-Wesley, 569 p. ISBN : 0321268172.

Matériel devant être fourni par l'étudiant

Selon le projet de session, l'équipe peut avoir à fournir du matériel et de l'équipement.

Obligatoire : Chaque équipe de travail en laboratoire devra créer lors du premier laboratoire **deux** machines virtuelles permettant d'exécuter des procédures typiques en forensique informatique. L'équipe devra s'assurer que ces machines restent à leur disposition tout au long de la session. Il y aura une machine virtuelle Linux « Paladin » et une autre qui sera un Windows. Pour pouvoir réaliser cette dernière, l'un des co-équipiers devra être inscrit au programme de logiciels gratuits de l'École.

Programme du cours

Voici l'ordre dans lequel les sujets seront traités. Il se peut que les derniers sujets ne soient pas traités si le temps vient à manquer.

- Plan de cours, incluant les moyens d'évaluation, les travaux à faire et les délais de remise;
- Rédaction, recherche documentaire, clips vidéo à écouter;
- Formation des équipes de travail de laboratoire et de session;
- Approches et stratégies de fouille et d'examen d'un média numérique;
- Expressions régulières;
- Systèmes de fichiers FAT32, NTFS;
- Mémoire RAM, assistants numériques personnels;
- Fondements de l'investigation numérique, faits et circonstances d'une cueillette;
- Notions de droit;
- Procédures opérationnelles;
- Infonuagique, données massives, anti forensique, forensiques mobile et furtive.

Épreuves évaluées

Introduction : énoncés, données et briefings :

- À l'exception de l'examen final, toutes les épreuves évaluées font l'objet d'un énoncé de travail;
- Les énoncés de travail sont rendus disponibles sur le site Moodle du cours au moment approprié;
- Chaque énoncé indique les objectifs globaux, le contexte, le travail à faire, la forme et la nature du rapport à soumettre ainsi que les critères globaux de correction qui seront utilisés pour corriger l'épreuve;
- Les données nécessaires à la réalisation des épreuves évaluées sont mises à la disposition des étudiant(e)s via le site Moodle du cours;
- Avant le début d'une épreuve évaluée, l'enseignant donne un briefing sur l'épreuve en question;
- Les étudiant(e)s doivent lire l'énoncé avant le briefing.

Dates de début et de remise des travaux relatifs aux épreuves évaluées :

Activité	Sujet	Débutera le	Remise des travaux	%age
Lab. non évalué	Environnements forensiques	9 janvier 2023	Aucun rapport à remettre	0%
Laboratoire	Stratégies de fouille	6 février 2023	6 mars 2023 à 19h00	10%
Travail de session	Déterminé par équipe	23 janvier 2023	29 mars 2023 à 19h00	30%
Capsule vidéo	Même que travail de session	23 janvier 2023	10 avril 2023 à 19h00	10%
Devoir maison	Procédé analytique de saisie	5 avril 2023	11 avril 2023 à 19h00	10%
Laboratoire	Forensique volatile	13 mars 2023	19 avril 2023 à 19h00	10%
Examen	Examen final	Déterminé par registraire	Déterminé par registraire	30%

Important – Pénalités pour retard :

Afin de permettre une rétroaction efficace, les travaux doivent être remis au plus tard avant la date-heure buttoir indiquée dans le tableau ci-dessus, sous peine d'une pénalité de **5% par heure de retard entamée**.

Activités pendant les laboratoires :

Les activités des laboratoires seront les suivantes :

- 9 janvier : Création d'environnements forensiques;
- 23 janvier : Travail sur le projet de session. Marc Dib vous prodiguera des conseils utiles;
- 6 et 20 février : Laboratoire sur la stratégie de fouille;
- 13 mars et 17 avril : Laboratoire sur la forensique volatile;
- 27 mars : Travail sur le projet de session et la capsule vidéo. Marc Dib vous conseillera sur la finalisation de votre projet et vous expliquera quelles erreurs ne doivent pas être faites dans la réalisation de votre capsule.

Travail de session :

Le travail de session doit être entrepris très tôt dans la session. Voici les étapes obligatoires :

- Mercredi 25 janvier à 19h00 : Remise par courriel du sujet de votre projet de session;
- Samedi 28 janvier entre 9h00 et 19h00 : Rencontre **obligatoire** avec l'enseignant pour s'assurer de l'orientation de votre projet. Les plages horaires sont aux 45 minutes à compter de 9h00. Veuillez informer l'enseignant tôt de votre choix de plage horaire de rencontre pour votre équipe;
- Mercredi 8 mars à 19h00 : Remise partielle non notée mais corrigée de la partie 1 de votre travail de session. La partie 1 comprend l'introduction, les objectifs, la revue de littérature et la procédure expérimentale;
- Samedi 11 mars entre 9h00 et 19h00 : Rencontre **obligatoire** avec l'enseignant. Rétroaction sur la remise partielle. Survol de ce qui est déjà fait et de ce qui reste à faire. Les plages horaires sont aux 45 minutes à compter de 9h00. Veuillez informer l'enseignant tôt de votre choix de plage horaire de rencontre pour votre équipe;
- Tous les coéquipiers doivent être présent aux rencontres obligatoires. **Les absent(e)s seront pénalisés de 5%**.

Normes de présentation des travaux :

Les travaux sont rédigés en français. Un français impeccable est exigé :

- Vous devez donc vous munir d'un correcteur d'orthographe compétent;
- Vous devez éviter les mots en anglais et les anglicismes. La référence utilisée par les correcteurs est le Grand dictionnaire terminologique de l'Office de la Langue Français du Québec;
- Vous devez éviter les acronymes sauf de très rares exceptions, inévitables. Si vous utilisez un ou plusieurs acronymes, votre rapport doit avoir un tableau par ordre alphabétique d'acronyme donnant la signification de chacun.

Le format, pour tout travail à remettre est :

- pdf;
- Pour le formatage des pages, veuillez utiliser le document « Exigences de rédaction en 0x66F mots ».

Tricherie et autres manœuvres apparentées

- Citer un auteur, c'est rendre à César ce qui lui appartient et démontrer qu'on a fait du travail de recherche. C'est aussi partager notre admiration de chercheur envers un autre chercheur;
- Le règlement de l'École Polytechnique stipule : « *Constitue notamment une fraude : …l'utilisation totale ou partielle, littérale ou déguisée, d'une œuvre d'autrui, y compris tout extrait provenant d'un support électronique, en le faisant passer pour sien ou sans indication de référence à l'occasion d'un examen, d'un travail ou de toute autre activité faisant l'objet d'une évaluation;* … »;
- Ces manœuvres ne seront pas tolérées et le règlement de l'École Polytechnique sera appliqué à la plus stricte lettre.

Mention relative à la protection des renseignements personnels

Les activités d'enseignement en ligne en mode synchrone (bimodale ou à distance) seront enregistrées afin de permettre aux personnes étudiantes ne pouvant pas assister en temps réel au cours, notamment les étudiantes et les étudiants étrangers résidant dans un fuseau horaire différent de celui de Polytechnique Montréal, d'avoir accès à l'activité d'enseignement. L'enregistrement sera ensuite rendu disponible sur Moodle aux seules personnes étudiantes inscrites au cours INF-8430 au trimestre d'hiver 2023.

Si l'étudiante ou l'étudiant active son micro et sa caméra lors de cette activité d'enseignement, il est possible que son nom, son image et sa voix apparaissent sur l'enregistrement. Ces renseignements personnels seront accessibles à la personne enseignante, aux personnes étudiantes inscrites au cours INF-8430 au trimestre d'hiver 2023 et aux employés de Polytechnique affectés à la gestion de Moodle. L'enregistrement sera conservé de façon confidentielle conformément à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

L'enregistrement sera retiré de Moodle au début de la session où le cours INF-8430 se tiendra à nouveau. Si l'étudiante ou l'étudiant ne souhaite pas être enregistré, il est de sa responsabilité de désactiver son microphone et sa caméra.

À défaut de désactiver son microphone et sa caméra, l'étudiante ou l'étudiant consent à l'enregistrement audio ou audiovisuel, à la conservation, à l'utilisation et à la rediffusion de l'enregistrement de son nom, de sa voix et de son image dans le cadre de l'activité d'enseignement en ligne.

Rappel : droits d'auteur

Les activités d'enseignement en ligne sont protégées par les droits d'auteur et le droit à la vie privée dont le droit à l'image. En conséquence, la personne étudiante ne peut pas :

- Partager les vidéos ou des extraits de celles-ci avec une autre personne;
- Enregistrer localement les vidéos;
- Diffuser ou vendre les vidéos.