POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Plan de cours

CF140 – ACQUISITION ET ANALYSE DE PREUVE NUMÉRIQUE

Programme des certificats
Automne 2023
3 Crédits
3-0-6
www.moodle.polymtl.ca

Chargés de cours

Nom	**Alexandre Girouard**
Courriel	alexandre-2.girouard@polymtl.ca

Nom	**Juan Miguel Munizaga**
Courriel	juan-miguel.munizaga@polymtl.ca

Nom	**Nadine Paoliello**
Courriel	n.paoliello@polymtl.ca

Description du cours

Enquête privée vs enquête de l'État. Recherche, préservation et saisie de la preuve numérique. Types d'autorisation judiciaire et aspects légaux. Rédaction et obtention d'autorisations judiciaires. Planification de l'exécution de l'autorisation judiciaire. Filet de protection et mesures de sécurité personnelle. Exécution de l'autorisation judiciaire. Équipement d'opération en informatique judiciaire. Accès au lieu de perquisition, évaluation des lieux et exécution de la perquisition électronique, examen des médias, protection logique et physique lors de l'examen, saisie des médias et des données numériques, protection des effets saisis et départ des lieux. Remise en opération et rétroaction. Laboratoire d'informatique judiciaire et matériel opérationnel Acquisition et traitement de la preuve. Appréciation de la preuve numérique. Calendrier des procédures judiciaires. Divulgation et présentation de la preuve numérique au tribunal. Numérisation de la preuve documentaire papier. Palais de justice de l'ère numérique.

COURS PREALABLES	COURS COREQUIS	COURS SUBSEQUENTS
CF110	-	-

Objectifs d'apprentissage

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

- décrire les étapes de préparation et d'exécution d'une perquisition en informatique judiciaire ;
- planifier une intervention en informatique judiciaire lors de l'exécution d'une autorisation judiciaire en tenant compte des informations qui lui sont fournies ;
- décrire les différents éléments d'un filet de protection s'appliquant à une situation donnée ;
- choisir les principaux éléments matériels et logiciels requis par une intervention en informatique judiciaire ;
- décrire les étapes de l'expertise en informatique judiciaire qui peuvent apporter assistance à l'enquête principale et aux procédures judiciaires ;
- saisir, protéger, cloner et extraire la preuve.

Matériel requis

Processeur : Intel I5 8e génération ou mieux ou AMD Ryzen 5 Mobile Processor

Disque dur/Stockage : SSD 512Go ou mieux

Mémoire vive : 8Go ou mieux

Carte graphique : Rien de particulier, la carte graphique intégrée suffit

Système d'exploitation : Windows 10 ou 11

Autres : Suite Office de base, Connexion Internet avec une vitesse minimale de 30Mbps

ATTENTION ! les processeurs ARM (M1,M2) d'Apple par exemple créent des problèmes avec les cours et ne sont pas recommandés

À noter que les besoins en bande passante peuvent varier en fonction de la densité de l'expérience multimédia. Cependant, il est fortement recommandé d'avoir une connexion haute vitesse standard (5 Mb/s) afin de profiter pleinement de l'expérience Zoom.

- Webcam.
- Microphone – casque d'écoute (connecteur USB recommandé).

Pour plus de détails, voir les liens suivants :
https://www.polymtl.ca/si/outil-de-visioconference-zoom
https://support.zoom.us/hc/fr/articles/201362023-Zoom-system-requirements-Windows-macOS-Linux#h_d278c327-e03d-4896-b19a-96a8f3c0c69c

Méthodes d'enseignement et d'apprentissage

Cours offert par Internet seulement

L'utilisation de systèmes d'intelligence artificielle (IA) générative (ex : ChatGPT, OpenAI Codex, GitHub Copilot, DALL-E, Midjourney, etc.) **est interdite pendant les évaluations et la rédaction des travaux**, et ce en raison des enjeux suivants :

- La fiabilité des réponses;
- La fraude et le plagiat;
- La confidentialité des données et le respect du droit d'auteur.

Format des travaux

Les devoirs et travaux sont remis via le site Moodle du cours selon les spécifications. Aucun document imprimé ne sera accepté. Le fichier contenant le travail remis doit être en format PDF, à l'exception du DE03 et le TP01 qui seront sous format Moodle Quiz. Le travail remis doit répondre aux exigences énoncées dans l'énoncé du travail à faire.

Remise des travaux

Les devoirs et travaux sont à remettre avant l'heure et le jour indiqués comme étant la date de remise. Tout retard dans la remise des travaux sera sanctionné. Pour chaque jour de retard, la pénalité est de 10 %, l'heure où le travail a été reçu sur Moodle faisant office de cachet.

Critères d'évaluation du travail de session

Les critères d'évaluation pour chaque travail demandé sont précisés dans l'énoncé du document de description du travail.

Personnes-ressources

Support aux étudiants : certificats@polymtl.ca
Support technique : support.certificat@polymtl.ca
Support Zoom : support.certificat@polymtl.ca
Service aux étudiants – Soutien à la réussite : https://www.polymtl.ca/soutien/
Soutien aux étudiants en situation de handicap : https://www.polymtl.ca/soutien/accueil-des-etudiants

Documentation

Aucun achat de livre. La documentation est fournie sur Moodle.

Programme du cours

Semaine / cours	Chargé de cours	Chargé de TP	Thèmes	TD, labo, TP	Lectures/ Exercices préparatoires	Évaluation
Cours 1 : 31 août	N.P.	J.M	Présentations. Plan de cours. Introduction. Définitions et concepts en informatique judiciaire.	Diapo & vidéo	Chapitre 1	
Cours 2 : 7 sept.	J.M.	A.G.	▪ Enquêtes privées vs enquête de l'État. ▪ Aspects légaux des autorisations judiciaires. ▪ Obtention d'autorisation judiciaire. ▪ Type d'autorisations judiciaires. ▪ Étude de cas.	Diapo & vidéo	Chapitre 2	
Cours 3 : 14 sept.	A.G.	N.P.	▪ Procédures judiciaires privées ou civiles. ▪ Infrastructures dédiées et obligations judiciaires. ▪ Opérations non gouvernementales.	Diapo & vidéo	Chapitre 2	*Remise DE01*
Cours 4 : 21 sept.	N.P.	J.M	▪ Demande d'assistance. ▪ Déclenchement de l'enquête, processus d'enquête, cyberenquête, sauvegarde de données. ▪ Autorisations judiciaires : rédaction, résultats et validation.	Diapo & vidéo	Chapitre 2	
Cours 5 : 28 sept.	J.M.	A.G.	▪ Mandat de perquisition et repérage des artéfacts. ▪ Équipement d'opération en informatique judiciaire. ▪ Planification de la perquisition : physique et électronique.	Diapo & vidéo	Chapitre 3	

Semaine / cours	Chargé de cours	Chargé de TP	Thèmes	TD, labo, TP	Lectures/ Exercices préparatoires	Évaluation
Cours 6 : 5 oct.	A.G.	N.P.	▪ Entrée sur le site opérationnel et fouille. ▪ Processus analytique de saisie. ▪ Processus décisionnel et mesures de sécurité personnelle. ▪ Examen des dispositifs électroniques et examen des médias non installés.	Diapo & vidéo	Chapitre 4	*Remise DE02*
12 octobre	**Semaine de relâche**					
Cours 7 : 19 oct.	N.P.	J.M.	▪ Saisie des pièces à conviction vs réalisation des copies judiciaires. ▪ Pré expertise et protection des pièces à conviction. Prévisionnement de la preuve recherchée. ▪ Départ du site opérationnel, remise en activité, post-opération, mise en attente. ▪ Rétroaction. Acquisition judiciaire et sauvegarde des données. ▪ Exercices d'application d'informatique judiciaire.	Diapo & vidéo	Chapitre 5	*Remise DE03*
Cours 8 : 26 oct.	J.M	A.G.	▪ Matériel opérationnel. Intervention sur dispositifs électroniques actifs. ▪ Importance des données volatiles.	Diapo & vidéo	Chapitre 6	
Cours 9 : 2 nov.	A.G.	N.P.	**Laboratoire avec machines virtuelles, Logiciel XWAYS :** ▪ Récupération des données, recherches et fouille des copies judiciaires. ▪ Processus analytique. Analyse judiciaire.	**Laboratoire** Présence en mode synchrone	Travail sur VM	*Remise DE04*

Semaine / cours	Chargé de cours	Chargé de TP	Thèmes	TD, labo, TP	Lectures/ Exercices préparatoires	Évaluation
Cours 10 : 9 nov.	N.P.	J.M.	▪ Aspects physiques des médias de stockage numérique.	Diapo & vidéo	Chapitre 7	
Cours 11 : 16 nov.	J.M.	A.G.	▪ Introduction à l'informatique judiciaire sur les systèmes d'exploitation des appareils mobiles. ▪ Procédures judiciaires, étapes, obligations et déroulement.	Diapo & vidéo	Chapitre 8	
Cours 12 : 23 nov.	A.G.	N.P.	▪ Calendrier des preuves et étapes des procédures judiciaires. Divulgation de la preuve. Protection des médias électroniques. ▪ Présentation du dossier de cour. ▪ Logiciels de présentation, numérisation, cour électronique.	Diapo & vidéo	Chapitre 9	*Remise DE05* *Remise TP01*
Cours 13[1] : 30 nov.	N.P.	J.M.	▪ Révision ; ▪ Filet de protection et mesures de sécurité personnelle ; ▪ Protection logique et physique des médias (avant, durant et après) ; ▪ Calendrier de preuves et étapes du processus judiciaire ; Logiciels, etc.	Diapo & vidéo	Chapitre 10	
7 décembre	**Journée sans cours ni examen**					
Cours 14 : ***14 déc.***	A.G.	N.P.	***Examen final.***[2]	**Présence obligatoire**	Chapitre 1 à 10	***EF01***

[1] Dernière séance pour procéder à l'évaluation de l'enseignement par les étudiants. Voir la section « *Améliorer votre enseignement* » de la page suivante : https://www.polymtl.ca/appui-pedagogique/nos-services

[2] Durée maximum : 2 h 30 ; le/les chargé(s) de cours sera/seront disponible(s).

Évaluation

NATURE		NOMBRE	MODE DE RÉALISATION		PONDÉRATION	DATE
Devoir 1	(DE01)	1	Numérique :	document PDF à être remis dans la boîte de remise sur MoodleExamen (activité « Devoirs »).	5 %	14 septembre 2023 23h59
Devoir 2	(DE02)	1			10 %	5 octobre 2023 23h59
Devoir 3	(DE03)	1	Informatique :	en ligne, sans aucune restriction, par activité « Test » MoodleExamen	10 %	19 octobre 2023 23h59
Devoir 4	(DE04)	1	Numérique :	document PDF à être remis dans la boîte de remise sur MoodleExamen (activité « Devoirs »).	10 %	2 novembre 2023 23h59
Devoir 5	(DE05)	1			10 %	23 novembre 2023 23h59
Travail pratique	(TP01)	1	Informatique :	en ligne, sans aucune restriction, par activité « Test » MoodleExamen	15 %	23 novembre 2023 23h59
Examen final	(EF01)	1	Informatisé :	en ligne et à distance, à livre ouvert, sans aucune restriction, par activité « Test » MoodleExamen et surveillance avec *Zoom*.	40 %	14 décembre

* Qualité Requise des Diplômé.es

Charge de travail

Présence en cours : 12 périodes de 3 h + contrôle périodique & examen final = 42 h
Travail personnel : étude personnelle : lecture et étude 36 h ; heures dédiées au projet 17 h ; préparation aux tests et à l'examen final 40 h = 93 h
Total : 135 h

*** Cette information est donnée à titre indicatif seulement. Certaines personnes peuvent avoir besoin d'investir plus ou moins de temps.

Mode d'enseignement à distance

L'enseignement et l'encadrement du cours sont en mode synchrone & asynchrone. Les séances seront enregistrées et disponibles pendant la durée du trimestre en entier.

Mention relative à la protection des renseignements personnels : enregistrement des activités d'enseignement en ligne en mode synchrone

Les activités d'enseignement en ligne en mode synchrone seront enregistrées afin de permettre aux personnes étudiantes ne pouvant pas assister en temps réel au cours d'avoir accès à l'activité d'enseignement. L'enregistrement sera ensuite rendu disponible sur Moodle aux seules personnes étudiantes inscrites à ce cours au présent trimestre.

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 à ce cours au présent trimestre 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, RLRQ c A-2.1.

L'enregistrement sera retiré de Moodle à la fin de la session et sera détruit dans les 30 jours après la fin de la session.

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 : droit 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 ;
- diffuser ou vendre les vidéos.

Fraude : règlement et sanctions

Les étudiantes et les étudiants doivent adopter une attitude professionnelle exemplaire. L'article 8 des règlements des études au certificat présente la position de Polytechnique Montréal à l'égard de la fraude sur la base du principe de tolérance zéro. Voici quelques éléments tirés du règlement en vigueur.

Par fraude, on entend toute forme de plagiat, de tricherie ou tout autre moyen illicite utilisé par une étudiante ou un étudiant pour obtenir un résultat d'évaluation non mérité ou pour influencer une décision relative à un dossier académique.

À titre d'exemple, constituent 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 ;
- le non respect des consignes lors d'un contrôle, d'un examen, d'un travail ou de toute autre activité faisant l'objet d'une évaluation;
- la sollicitation, l'offre ou l'échange d'information pendant un contrôle ou un examen;
- la falsification de résultats d'une évaluation ou de tout document en faisant partie;
- la possession ou l'utilisation pendant un contrôle ou un examen de tout document, matériel ou équipement non autorisé y compris la copie d'examen d'une autre personne étudiante.

Selon la gravité de l'infraction et l'existence de circonstances atténuantes ou aggravantes, l'étudiante ou l'étudiant peut se voir imposer une sanction correspondant à, entre autres, l'attribution de la cote 0 pour l'examen, le travail ou toute autre activité faisant l'objet d'une évaluation qui est en cause, l'attribution de la note F pour le cours en cause, l'attribution de la note F à tous les cours suivis au trimestre.

Dans le cas d'un travail en équipe, les étudiantes et les étudiants d'une même équipe de travail tel que reconnu par l'enseignant sont solidaires du matériel produit au nom de l'équipe. Si un membre de l'équipe produit et remet un travail au nom de l'équipe et qu'il s'avère que ce travail est frauduleux tous les membres de l'équipe sont susceptibles de recevoir une sanction à moins qu'il soit démontré sans ambiguïté que l'infraction est le fait d'un ou de quelques membres de l'équipe en particulier.

Ressources et services pour les étudiantes et étudiants

Le Service aux étudiants (SEP) est constitué de professionnels qualifiés et d'une Escouade étudiante, dédiés à favoriser votre bien-être et votre réussite à Polytechnique Montréal, autant sur le plan académique, personnel que social. Que ce soit sous la forme de rencontres individuelles, d'ateliers pratiques ou de programmes tels que le tutorat et le mentorat, les services offerts vous aideront à vous épanouir à votre plein potentiel durant vos études à Polytechnique Montréal. N'hésitez pas à les contacter. Vous avez tout à y gagner !

Le Bureau d'intervention et de prévention des conflits et de la violence (BIPCV), vous accueille, vous guide et vous soutient en matière de violence à caractère sexuel, harcèlement ou tout enjeu relatif au respect des personnes. Le BIPCV est un bureau indépendant, assurant un service respectant la confidentialité et une écoute sans jugement. Contactez-les : bipcv@polymtl.ca 514 340 4711 Poste 5151.