

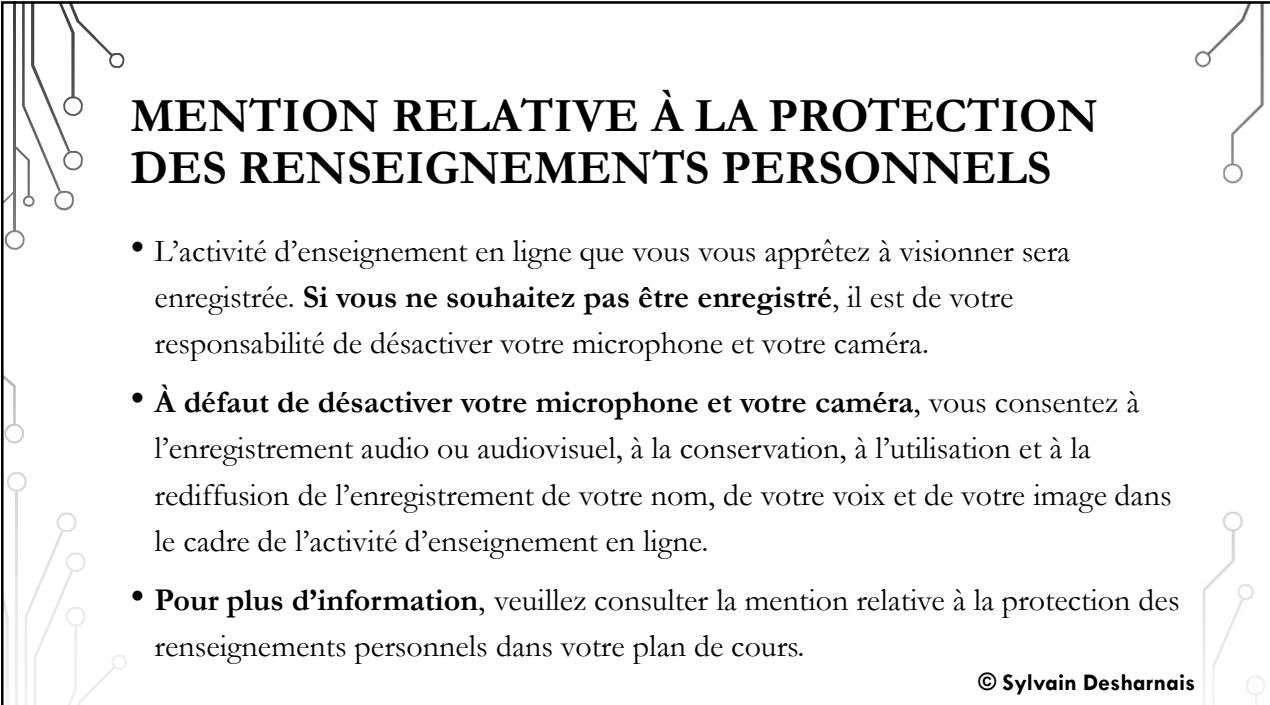
INVESTIGATION NUMÉRIQUE

PLAN DU COURS, VISITE MOODLE, BRIEFING LAB, APPROCHES ET STRATÉGIES DE FOUILLE

Un commencement est un moment d'une délicatesse extrême.
Dune (la version David Lynch)

© Sylvain Desharnais

1



MENTION RELATIVE À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

- L'activité d'enseignement en ligne que vous vous apprêtez à visionner sera enregistrée. **Si vous ne souhaitez pas être enregistré**, il est de votre responsabilité de désactiver votre microphone et votre caméra.
- **À défaut de désactiver votre microphone et votre caméra**, vous consentez à l'enregistrement audio ou audiovisuel, à la conservation, à l'utilisation et à la rediffusion de l'enregistrement de votre nom, de votre voix et de votre image dans le cadre de l'activité d'enseignement en ligne.
- **Pour plus d'information**, veuillez consulter la mention relative à la protection des renseignements personnels dans votre plan de cours.

© Sylvain Desharnais

2

JE SUIS...

- B.Sc.Ed.phys, B.A.A, certificat cyber enquête, M.Sc. Informatique (sujet) et bientôt en écriture de thèse Doctorat en Informatique cognitive (sujet);
- Enquêteur régional en informatique (Formation, procédures opérationnelles et dotation matérielle) – Revenu Canada – Qc, Atlantique, Nord Ontario 13 ans;
- Investigateur numérique privé – 7 ans – Opérations fermées nov. 2020;
- Enseigne investigation numérique: ULaval 2011+, Poly 2014+, UQAC 2023+

© Sylvain Desharnais

3

PLAN DE COURS

- Visite détaillée du site Moodle du cours:
 - Sections
 - Nouvelles versions de documents en cours de session transmises via Forum Moodle
- Agenda bref
- Plan de cours (Voir diapositive suivante)

© Sylvain Desharnais

4

ÉVALUATION – TRIPLE SEUIL

Mode d'évaluation	Qté	Pondération	Type	Date de remise
Laboratoires B1	2	2 * 10%	Éq.	6 mars et 19 avril à 19h00
Travail de session	1	30%	Éq.	29 mars à 19h00
Capsule vidéo	1	10%	Éq.	10 avril à 19h00
Devoir-maison	1	10%	Indiv.	11 avril à 19h00
Examen final	1	30%	Indiv.	Déterminé par registraire

- Épreuves par équipe: minimum 50%
- Épreuves individuelles: minimum 50%
- Au global des deux types d'épreuve: minimum 60%

© Sylvain Desharnais

5

CONSTITUTION DES ÉQUIPES

- 4 par équipe
- Équipes déjà formées: Envoyez-moi un courriel dès maintenant
- Ceux sans équipe – Faites-vous connaître via le forum
- Date limite pour me transmettre les noms: 18 janvier 2023 à 19h00
- **Passé ce délai**, je forme des équipes à partir de ceux qui restent
- **Attention**: Si mésentente dans l'équipe, vous m'en parlez et vite

© Sylvain Desharnais

6

DOLÉANCES SUR CORRECTION

- Généralement, les travaux corrigés sont retournés dans la semaine suivant la date-heure buttoir pour la remise de ceux-ci;
- Une fois que je vous ai envoyé votre copie corrigée d'une activité évaluée, vous aurez une semaine pour soumettre vos doléances par courriel;

© Sylvain Desharnais

7

DOLÉANCES SUR CORRECTION

- Doléances ne mentionnant pas les sujets suivants seront **rejetés**:
 - Prénom et nom
 - Item **exact** pour lequel vous soumettez des doléances
 - Pourquoi la correction faite est incorrecte
 - **Combien de points méritez-vous en plus**
- Lorsque vous me faites part de vos doléances, faites attention au ton du courriel;

© Sylvain Desharnais

8

LABS, TRAVAIL DE SESSION, CAPSULE

- Laboratoires:
 - Briefing la semaine d'avant (lecture commentée de l'énoncé et du formulaire)
 - Production du rapport: Voir les dates-buttoir au plan de cours
 - Critères de correction: mentionnés dans l'énoncé → Prière de vous en servir
- Travail de session:
 - Briefing au 2^{ième} cours (lecture commentée de l'énoncé)
 - Création d'une capsule
 - Sujets et constitution des équipes avant date-buttoir
 - ATTENTION: Étapes intermédiaires et rencontres → Voir le plan de cours

© Sylvain Desharnais

9

EXAMEN

- Sera à distance
- 2h30
- Droit à toute documentation
- Faire les exercices du manuel vous place en meilleure position pour mieux réussir l'examen
- N'inclut plus l'étude de cas R-OCICE qui fait l'objet d'un devoir maison de fin de session
- Corrigé rapidement, retour via Moodle

© Sylvain Desharnais

10

QUESTIONS À L'EXAMEN FINAL

Au final il y a **toujours** une question (avec ou sans sous-question) sur les sujets suivants. Les pourcentages indiqués sont approximatifs et peuvent varier:

- Interprétation d'une entrée \$MFT 20-25%
- Droit et procédures opérationnelles 10%
- Stratégies de fouille 10-15%
- Interprétation aperçu FAT32 15-20%
- Interprétation d'un matriciel 10%
- Sujets divers 5-10%

© Sylvain Desharnais

11

DEVOIR MAISON: ANALYSE R-OCICE

- Étude de cas portant sur le processus éthique d'une saisie de preuve
- Réponses individuelles mais lecture et réflexion peuvent être faites en groupe
- Implique quatre documents:
 - Étude de cas – Formulaire dédié à l'analyse R-OCICE
 - Étude de cas – Briefing
 - Courriel individuel – Décision à motiver
 - Étude de cas – Observations sur le site opérationnel
- Documents transmis via Moodle au moment approprié

© Sylvain Desharnais

12

NORMES DE RÉDACTION

- Voir Moodle du cours, Section A: A05, A06, A07
- En français impeccable (10% des points) → Logiciel de correction et ami compétent
- Vous devez citer d'où vous tirez vos idées pour:
 - Rendre justice aux auteurs autres que vous-mêmes;
 - Me démontrer que vous avez fait de la recherche documentaire (%age des points)
- Citations en italique, entre guillemets français et référencé dans la médiagraphie
- Attention: paraphraser, utiliser Google Translation et copier-coller = plagier
- Respect des normes et des termes des énoncés → %age des points

© Sylvain Desharnais

13

PÉNALITÉS DE RETARD

- Retard pénalité de 5% de la note attribuée par heure de retard entamée
- Il est de la responsabilité des coéquipiers de s'assurer que le travail est remis à temps
- Morale 1:

**Il vaut donc mieux soumettre un travail incomplet ou imparfait
à temps que de remettre le travail en retard**

- Morale 2:

On fait confiance (à ses coéquipiers)...
mais on vérifie

© Sylvain Desharnais

14

MATÉRIEL FORTEMENT SUGGÉRÉ

- Par équipe – 2 environnements forensiques (premier laboratoire):
 - Une machine virtuelle Linux Paladin
- ET
- Une machine virtuelle Windows 10

© Sylvain Desharnais

15

AU DÉBUT DE CHAQUE COURS, JE...

- Présente un cas de jurisprudence (Entre 10 et 15 cas de jurisprudence en tout dont un deviendra une question d'examen)
- Section administrative: rappel d'échéance, briefing et autres sujets

© Sylvain Desharnais

16

CAPSULES VIDÉO

- Écouter les capsules HIN1 à HIN15 d'ici 10 jours
- Téléchargez du site du cours l'item « G02 - Artéfacts - Systèmes de fichiers et stratégies de fouille - Stratj01 » pour reproduire ce que vous voyez pendant le clip
- Apportez FTK Imager et l'image forensique au cours de la semaine prochaine
- Écouter les autres capsules pour fin de janvier

© Sylvain Desharnais

17

CLIPS VIDÉO

- Sur site du cours – Section V

- Sujets:

- HIN01 - Interface 4_31
- HIN02 - Monter un artéfact 6_28
- HIN03 Image Mounting 6_21
- HIN04 Création d'une image forensique 6_32
- HIN05 Mémoires et protégés 6_26
- HIN06 Diverses exportations 4_27
- HIN07 Custom Content 6_04

- Sujets:

- HIN08 Fonctionnalités diverses 5_30
- HIN09 Se déplacer dans le volet DI 6_24
- HIN10 Trouver et désencastrer 5_16
- HIN11 Interpréteurs hexadécimaux 5_31
- HIN12 Authentification 6_01
- HIN13 Cloner 5_38
- HIN14 Aseptiser 4_58
- HIN15 Restaurer 5_08

- 86 minutes à écouter

Écouter le clip, réécouter en faisant l'exercice, faire l'exercice seul plusieurs fois

© Sylvain Desharnais

18