Examen type INF8430

Sujet 1 : Stratégies de fouille {1 question, 2 stratégies détaillées demandées, 7 items par stratégie, pour 20 points}

Situation : Vous avez la charge de l'examen des médias numériques saisis lors d'opérations d'investigation numérique.

Mission : Veuillez établir la stratégie d'examen que vous emploierez pour découvrir les preuves demandées dans la section « Briefing » ci-dessous. Précision : Vous ne devez pas vous contenter de nommer les éléments de votre stratégie. Vous devez expliquer comment vous l'appliquerez. Par exemple, si une de vos stratégies implique l'utilisation d'une donnée préexistante, vous devez aussi dire comment vous obtiendrez ou avez obtenu cette donnée. Vous devez dire quel outil vous utiliserez pour l'appliquer et qu'est-ce que votre stratégie trouvera (selon vous) qui constituera une des occurrences recherchées.

Exécution : Vous avez 2 semaines pour commencer à obtenir des résultats. Ceci pour permettre à l'enquêteur au dossier d'investiguer avant le moment de la prolongation de rétention des effets saisis.

Administration et logistique : Vous avez à votre disposition l'ensemble des ressources de votre laboratoire (qui est bien équipé et moderne sans être de dernier cri), mais vous avez un budget limité.

Briefing : Insérez ici n'importe quel exercice du numéro 3 de l'annexe F (page 246-247) du manuel du cours « Notes d'investigation numérique ».

Modèle de réponse fourni à l'examen

Stratégie principale:

Famille de stratégie et stratégie (tel qu'écrits dans le manuel du cours)
Donnée-source (intrant que vous utiliserez dans la stratégie - Nature, description et provenance)
Outil utilisé pour appliquer la stratégie
Cible (sur quel artefacts appliquerez-vous la stratégie)
Méthode d'application (description sommaire de comment vous vous y prendrez pour produire le résultat escompté)
Résultats escomptés (description sommaire de l'extrant que vous espérez obtenir suite à l'application de la stratégie)
Utilisation projetée (En quoi l'extrant vous sera-t-il utile pour démontrer la culpabilité du suspect)

Stratégie « plan B »:

Famille de stratégie et stratégie (tel qu'écrits dans le manuel du cours)
Donnée-source (intrant que vous utiliserez dans la stratégie - Nature, description et provenance)
Outil utilisé pour appliquer la stratégie
Cible (sur quel artefacts appliquerez-vous la stratégie)
Méthode d'application (description sommaire de comment vous vous y prendrez pour produire le résultat escompté)
Résultats escomptés (description sommaire de l'extrant que vous espérez obtenir suite à l'application de la stratégie)
Utilisation projetée (En quoi l'extrant vous sera-t-il utile pour démontrer la culpabilité du suspect)

Sujet 2 : Interprétation d'une entrée $MFT {1 question en 6 sous-questions et 3 sous-sous-questions totalisant 20 points}

Situation : Le fichier intitulé « MFT » (« MFT.pdf » pour ceux utilisant les aperçus d'écran) présente une série d'entrées $MFT.

Mission : À la rubrique « Assignation » ci-dessous, je vous assigne une entrée $MFT de laquelle vous devez extraire les renseignements vous permettant de répondre aux questions spécifiées dans la section « Sous-questions ». Les décalages sont calculés à partir du début du fichier.

Exécution : Les décalages et les tailles de fichiers doivent être écrits en **hexadécimales**. Les numéros de grappe et le nombre de grappes consécutives doivent être en **décimales**. Si vous citez un nombre qui se trouve dans l'aperçu, dites à quels décalages (n'oubliez pas de donner le point de référence fixe) ce nombre se trouve. Lorsque vous écrivez un nombre dans votre réponse, vous devez préciser si le nombre est écrit en hexadécimale (notation : 0x…).

Précision : Cette question vaut au total 20 points. Le pointage de chaque sous-question apparaît entre accolades.

Assignation : Insérez ici n'importe quel exercice des numéros 37 à 49 de l'annexe F (page 259-267) du manuel du cours « Notes d'investigation numérique ».

Modèle de réponse fourni à l'examen

Veuillez répondre aux sous-questions suivantes en utilisant le modèle de réponse proposé.

a) De quel fichier cet aperçu d'écran est-il tiré? {0,5 point}

b) Est-ce que ces données sont des paradonnées ou des intradonnées? {0,5 point}

c) À quel fichier ces métadonnées se rapportent-elles? {1 point}

d) À quel décalage (« offset ») se trouve l'attribut $80? Exprimez le décalage en hexadécimale et selon l'échelle située à gauche de l'aperçu d'écran {2 points}

e) Dans l'attribut $80, donnez le décalage, en hexadécimale de la donnée qui vous indique où se trouve la trame de données {2 points}

f) Interprétez la trame de données en faisant ressortir {14 points} :

   i. les nombres hexadécimaux composant chaque segment;

   ii. le numéro, en décimale, de la première grappe de chaque segment du fichier; et

   iii. le nombre, en décimale, de grappes consécutives de chaque segment

Sujet 3 : Interprétation d'une entrée FAT32 {1 question en 7 sous-questions, totalisant 20 points}

Assignation : Je vous assigne le fichier dont le segment court débute au décalage **Utilisez l'application FAT32.exe du site Moodle (item G05)**.

Situation : Je vous fournis deux fichiers intitulés « FAT32_10 » et « Racine32_10 » (« FAT32_10.pdf » et « Racine32_10.pdf » pour ceux qui veulent utiliser des aperçus d'écran). FAT32_10 et Racine 32_10 proviennent de la même clé USB de 128 Mo, formatée en une seule partition FAT32. À la rubrique « **Assignation** » ci-dessus, je vous indique à quel décalage débute le segment court d'une entrée FAT32 (segment d'une longueur de 32 octets). Ce segment court (court, donc long de 32 octets) fait partie de l'entrée FAT32 d'un fichier stocké sur la partition FAT32 mentionnée au début du présent paragraphe.

Mission : Je vous demande d'extraire de l'entrée qui vous est assignée les renseignements nécessaires vous permettant de répondre aux sous-questions précisées à la section « Sous-questions » ci-dessous.

Exécution : Si vous citez un nombre qui se trouve dans l'aperçu (pdf), dites à quel décalage ce nombre se trouve. Si vous citez un nombre qui se trouve dans les fichiers FAT32_10 ou Racine32_10, fournissez un décalage exprimé en **hexadécimale**. Les autres données (taille, numéro de grappe, etc.) doivent être écrites en **décimales**, sauf spécification contraire.

Précisions : Veuillez utiliser le modèle de réponse que vous trouverez ci-dessous. Lorsque vous écrivez un nombre dans votre réponse, vous devez **impérativement** préciser si le nombre est écrit en hexadécimale (notation : 0x…) ou en décimale (0d…). Lorsque vous citez un décalage, vous devez **impérativement** utiliser soit la méthode « décalages-début-fin » ou la méthode « décalage-début-et-longueur ». Vous pouvez fournir des explications avec votre réponse et si votre réponse est incorrecte ou incomplète, je tiendrai compte des explications lors de la correction. Veuillez toutefois noter que pour valoir des points, ces explications doivent être accompagnées de la réponse, même si cette dernière est erronée.

Modèle de réponse fourni à l'examen

a) Est-ce que les métadonnées de ce fichier sont des paradonnées ou des intradonnées? **{1 point}**

b) Quel est le titre (nom long au complet) de ce fichier, incluant l'extension de fichier? **{2 points}**

c) Quelle est la taille logique, en octets, de ce fichier? **{2 points}** À quel décalage (« offset ») **exact** avez-vous vu cette information? **{1 point}**

d) Est-ce que ce fichier a été effacé par l'utilisateur ou non et dites à quoi voyez-vous cela? **{2 points}**

e) Combien de grappes sont nécessaires pour stocker ce fichier? **{2 points}**

f) Dans quelles grappes retrouve-t-on les différents segments de ce fichier? Pour répondre, vous devez partir du répertoire racine avec une certaine donnée et continuer et terminer votre réponse à l'aide de la table d'allocation des fichiers. **{6 points}**

g) Quelle est la taille physique de ce fichier? **{2 points}** À quel décalage (« offset ») **exact** avez-vous vu cette information? Exprimez le décalage selon l'échelle située à gauche de l'aperçu d'écran ou, si vous utilisez le fichier source, exprimez-le en hexadécimale. **{1 point}**

h) Quel est le nom du volume où réside la partition FAT32? **{1 point}**

Sujet 4 : Familiarisation au droit canadien et québécois {1 question valant 10 points, réponse doit comporter 6 items, vaut pour 20 points}

Situation : Le cas exposé dans la section « Énoncé » ci-dessous est un résumé tiré de cas de jurisprudence. Comme c'est un résumé, il manque forcément des détails. L'objectif de la question est de me donner votre perception professionnelle de la situation et non de voir si vous pouvez en venir à la même conclusion que le juge des faits.

Mission : Pour chaque item de la section « Renseignements demandés », fournissez le renseignement demandé.

Exécution : Vous devez **impérativement** utiliser le format du modèle de réponse fournit ci-dessous dans la section « Modèle de réponse » ci-dessous. L'accusation doit concerner la personne désignée à la rubrique **« Accusé »** ci-dessous. L'article choisi doit être l'un des articles mentionnés à la rubrique **« Alternatives** » ci-dessous.

Énoncé : Insérez ici n'importe quel exercice du numéro 9 de l'annexe F (pages 224-240) du manuel du cours « Notes d'investigation numérique ».

Accusé : Dans le doute, accusez-les tous!!

Alternatives : À l'examen, des alternatives vous seront fournies sous cette forme. Exemple : 21 (Participant à une infraction), 24 (Tentative), 83.01 (Terrorisme), 244 (Décharger une arme à feu), 320.13 (Conduite dangereuse), 445 (Tuer ou blesser des animaux)

Précision : Tous les cas sont des cas criminels. La formulation de l'accusation doit reprendre le contenu de l'article codifiant que ce comportement est un crime. Vous devez alors créer un amalgame des mots de l'article et des mots provenant de l'énoncé. Fournir la bonne formulation de l'accusation est plus important que d'avoir le même article ou le même verdict que le juge des faits. Pour les exemples de preuve, soyez le plus spécifique possible afin que le correcteur puisse comprendre que vous avez compris la relation entre une preuve, un vecteur de preuve (Actus reus ou mens rea) et une accusation. Si aucune preuve n'est exigible pour un vecteur de preuve, inscrire « S/O ». **ATTENTION** : Vous ne devez donner qu'un seul article et une seule accusation.

Renseignements demandés :

- Nom de la loi
- Article précis
- Libellé du titre de l'article de loi
- Formulation de l'accusation
- Élément(s) à prouver
- Exemple de preuve de mens rea
- Exemple de preuve d'actus reus

Modèle de réponse fourni à l'examen

a) Nom de la loi: Code criminel du Canada
b) Article précis, c'est-à-dire précis jusqu'à la disposition pertinente que vous évoquez
c) Libellé du titre de l'article de loi (Le titre indiqué dans le document "Articles de loi.pdf"
d) Formulation de l'accusation: Constituez un amalgame entre le texte de l'article de loi et l'énoncé
e) Exemple de preuve de mens rea: Pas ce que vous voulez prouver mais la preuve que vous soumettrez
f) Exemple de preuve d'actus reus: Pas ce que vous voulez prouver mais la preuve que vous soumettrez

Sujet 6 : Interprétation d'un matriciel {1 question valant 10 points}

Assignation : Je vous assigne le segment aux décalages suivants **Insérez ici n'importe quel exercice provenant du numéro 50 du manuel du cours « Notes d'investigation numérique » pages 266-269**

Situation : Vous examinez un média formaté NTFS. Je vous fournis le fichier intitulé « Matriciels2023 » (« Matriciels2023.pdf » pour ceux voulant utiliser les aperçus d'écran) contenant un matriciel $BITMAP.

Mission : À la rubrique « Assignation » ci-dessus, je vous assigne un intervalle à interpréter dans ce matriciel $BITMAP. Interprétez le segment de matriciel de la zone qui vous est assignée. Vous devez **impérativement** donner les numéros de toutes les grappes occupées et de toutes les grappes disponibles et éviter les formulations du style « Tous ceux que je ne désigne pas comme occupés sont disponibles ». Les décalages sont calculés à partir du début du fichier Matriciels2023.

Exécution : Les décalages doivent être exprimés en hexadécimale et conformément à la convention de notation exposée lors de ce cours (0x…). Les nombres binaires doivent être écrits conformément à la convention de notation exposée lors de ce cours (0b…). Pour toutes les autres données, utilisez le nombre en décimale. Vous devez utiliser le modèle utilisé dans les réponses aux problèmes exposés dans le livre du cours « Notes d'investigation numérique ». Malheureusement, je ne peux pas ajouter le formulaire tel quel au présent questionnaire. Je suggère toutefois un format de réponse cohérent avec ce qui est utilisé dans les « Notes d'investigation numérique ». Vous devrez donc adapter votre réponse à ce modèle en recopiant les rubriques pertinentes autant de fois que nécessaire.

Précision importante : Les nombres en décimale n'ont pas à être écrits avec l'annotation « 0d… » et tout nombre ne comportant pas d'annotation « 0x… » ni « 0b… » sera considéré comme un nombre décimal au moment de la correction. Si vous manquez d'espace dans l'espace réservé à cet effet, vous pouvez soumettre un fichier avec votre réponse.

Modèle de réponse fourni à l'examen

Plusieurs octets dans le segment:

- Premier octet du segment: décalage 0x
- Dernier octet du segment: décalage 0x
- Première grappe relative à ce segment:
- Dernière grappe relative à ce segment:
- Les octets de ce segment ont pour valeur: 0x
- Ce qui correspond à la valeur binaire: 0b
- Les grappes susmentionnées sont donc:

Un seul octet dans le segment traité:

- Cet octet se trouve au décalage: 0x
- Cet octet a une valeur de: 0x
- Convertit en binaire, ça vaut: 0b
- Les grappes suivantes sont donc occupées:
- Les grappes suivantes sont donc disponibles:

Sujet 5 : Construction d'une expression régulière {1 question valant 15 points}

Situation : Le fichier intitulé « expreg » (pour cette question, il n'y a pas de fichier pdf) contient une dix séries de données ainsi que du remplissage simulant des données chiffrées.

Mission : L'aperçu d'écran ci-dessous est la liste des modèles de souliers de course que je convoite. Vous devez extraire ce qui se trouve dans les champs « Dénivellation » et « Prix », zone encerclée d'un trait noir, et seulement ce champs. Je ne veux rien provenant du champs « Support » et rien provenant du champs « Poids ». L'expression régulière demandée est soit une assertion avant positive ou une assertion arrière positive.

Exécution : 1) Veuillez vous limiter aux données présentes dans le fichier que je vous fournis. 2) Pour les fins de la correction, je copierai votre expression régulière dans mon FTK Imager. Si cette assertion trouve tous les occurrences présentes dans le fichier expreg, je vous donne tous vos points. Si je dois faire des corrections pour que ça fonctionne, j'enlèverai 1 point par correction. 4) Quand je dis « seulement telles données », j'exclus donc les tabulateurs, les espaces et tout autre caractère qui ne font pas partie de la donnée demandée.

Aperçu des données:

Chaussure Course

Marque	Modèle	Support	Dénivellation	Prix	Poids	Couleur
BROOKS	Launch 6	Neutre	10 mm	111.99 $ca	260 gr	Bleu et gris
New Balance	1400v6	Neutre	8 mm	97.49 $ca	237 gr	Indigo et jaune
Nike	Flex Experience Run 9	Ferme	9 mm	66.00 $ca	290 gr	Noir et blanc
Under Armour	Micro G Pursuit BP	Flexible	5 mm	67.50 $ca	217 gr	Noir
Adidas	Energy Falcon	Ultra ferme	15 mm	75.00 $us	333 gr	Rose et rouge
Merrell	Vapor Glove 4	Ultra flexible	6.5 mm	93.75 euro	198 gr	Gris banane
Saucony	Guide ISO 2	Ferme	8 mm	84.99 UKpound	292 gr	Jaune et mauve

Sujet 7 : Questions diverses {5 questions valant chacune 1 point pour un total de 5 points}

Exemple : Que signifie la locution latine « Obiter dictum » et dans quelles circonstances est-elle employée?