Énoncé de travail – Stratégies de fouille

Avertissement : Cet exposé a été écrit en 2014 et réédité à l'hiver 2023. Il se peut donc qu'il y ait des incohérences dans la narration des événements, notamment le fait que l'enquête nous ait été confiée si longtemps après les événements.

1) **Scénario :**

L'AIMÉ (Association Internationale des Malandrins Éternels) est un regroupement de malfaiteurs de tous acabits. Avec eux, nul sentiment si ce n'est pour eux-mêmes. Récemment, la police de Montréal a identifié un de leur membre en la personne de Glaude Parisakys. Violent, d'une stupide méchanceté mais d'une grande intelligence, celui-ci a été maintes fois arrêté mais jamais condamné. Il n'en fallait pas plus pour que l'escouade de lutte contre les sempiternels criminels mette en mandate une équipe d'écoute électronique pour espionner Parisakys et une autre pour le filer (les deux équipes relevant de la capitaine Marianne Fitzwalter). La semaine passée, alors que Parisakys dinait au restaurant kiribatien « Leps Koubatim », il a été rejoint par un homme qui s'est assis à sa table sans commander de repas. La conversation a vite tourné au vinaigre et l'homme s'est levé en criant à qui voulait l'entendre que Parisakys avait tabassé son fils alors que celui-ci arpentait le campus de l'Université de l'IA (Île d'Anticosti). Les deux hommes ont commencé à se bousculer et à s'échanger mornifles et taloches. Deux policiers en uniformes, par hasard assis au fond de la salle, ont assisté à l'échauffourée et ont pu intervenir rapidement. Après avoir mis les deux hommes en état d'arrestation, ils furent rapidement amenés au poste de police et l'équipe de filature… les y a filés.

Lorsque l'équipe de filature est arrivée au poste, Parisakys était déjà en voie d'être libéré (il a un excellent avocat : 24/7, service en 15 minutes ou c'est gratuit[1]) sous promesse de comparaître. Mais dans sa rage, il partit en oubliant de récupérer le contenu de ses poches[2]. Fitzwalter s'est alors enquis du contenu des poches du suspect et les policiers en uniforme ont indiqué que Parisakys cachait des barrettes USB dans la doublure de son manteau. Fitzwalter a immédiatement demandé et obtenu un mandat de perquisition téléphonique pour saisir ces barrettes USB. Apprenant que l'investigateur numérique de la police locale ne pouvait pas effectuer l'examen des barrettes avant 2 ans, elle a demandé et obtenu la permission de faire appel à la firme privée InvNum Inc. Elle a alors contacté le président de ce cabinet de détectives, Sylvain Desharnais, et lui a demandé son assistance.

2) **Renseignements de la capitaine Fitzwalter :**

Marianne nous fournit les renseignements ci-dessous, renseignements provenant de la filature ou de l'écoute électronique :

a) Parisakys est un maniaque de sécurité informatique. Il se fait une copie de tous ses fichiers importants sur d'autres médias informatiques. Fitzwalter pense que la clé USB sert de support pour ces sauvegardes ;
b) Il a programmé un logiciel qu'il a appelé « Riboflavine ». Ce logiciel lui sert de « portefeuille » où il range ses fichiers considérés importants. Ce logiciel créé des fichiers dont l'extension est « rib ». Un fichier .rib commence par une entête dont on ne connaît pas la nature. On y trouve ensuite un fichier encastré dans sa forme non-chiffrée. Un jour où Parisakys se sentait nostalgique, il a montré à un de ses collaborateur un fichier qu'il conservait depuis des années et qui se rapportait à un crime commis il y a plusieurs années, en lui disant : « Si la police voyait cette photo, elle me créerait de sérieux ennuis »;
c) Il garde aussi des photos, moins compromettantes mais tout de même probantes, du même type de crime que celui gardé dans le fichier .rib ;
d) Il a aussi programmé un autre logiciel de chiffrement 2048 bits qu'il a intitulé « Signaturé ». Signaturé produit des fichiers dont la signature est 1CAFE90000536F46, suivi de plus ou moins près (mais on ne sait où exactement) de la taille du fichier. Jusqu'à maintenant, l'algorithme utilisé par l'application Signaturé et le mot de passe pour l'activer, restent inconnus ;

[1] Il s'agit de la firme Paul Malandrin et associés dont le site web montre, en caractères absolument minuscules, la restriction suivante : 24/7, service en 15 minutes ou c'est gratuit, sauf en dehors de la région métropolitaine, exception faites de la ville d'Ottawa excluant la zone de 10 hectares entourant la brasserie Duke of Spade mais incluant la rue Banks de 17h00 à 23h30 du lundi au vendredi du côté sud de la rue…

[2] Lorsqu'une personne en état d'arrestation est amenée au poste, on lui enlève automatiquement tout ce qu'il a dans les poches et on les place temporairement sous séquestre. S'il est libéré, ces effets lui sont remis. S'il est transféré dans une prison, les affaires personnelles sont remises à la prison, qui se chargera de les lui remettre au moment de sa libération.

e) Parisakys entretient des relations avec une organisation altermondialiste appelée les « Frères de l'Eau », organisation menée par une certaine Frija. La rumeur veut que cette organisation veuille installer une antenne au Québec afin de nous conscientiser sur notre gaspillage éhonté de l'eau potable alors que d'autres humains en manque cruellement. Compte tenu de la personnalité de Parisakys et de ses antécédents, une telle association n'est fort probablement pas dictée par la pitié des pauvres assoiffés, mais plutôt par sa boulimie financière ;

f) Présentement, Parisakys œuvre dans le domaine du vol et de la falsification de cartes de crédit et de la possession de carte de crédit volée, fabriquée ou falsifiée. Il a affirmé à un collaborateur qu'il stockait des données de carte de crédit sur son ordinateur ;

3) **Travaux préalables** :

a) Révisez les clips vidéo portant sur l'utilisation de FTK Imager et Autopsy SleuthKit;
b) Révisez les procédures permettant d'appliquer les stratégies de fouille;
c) Les preuves à recueillir sont celles indiquées dans le « Formulaire de réponse au TP » (TP pour « Travail Policier »).

4) **Directives spéciales** :

a) Le seul fichier que vous remettrez sera un fichier zip. Voir au numéro 6 ci-dessous pour des directives précises sur la structure de ce fichier;
b) Notes manuscrites : Vous **devez prendre des notes manuscrites et les fournir** dans le fichier zip contenant vos preuves. La qualité et la quantité de ces notes sera évalué en fonction de ce qui est qualifié de « bonnes notes » dans les « Notes d'investigation numérique ». À cet effet, chaque membre de l'équipe doit se conformer aux principes énoncés dans la section 2420-5 « Documenter »;
c) Rapport : Les questions auxquelles vous devez répondre sont celles indiquées dans le « Formulaire de réponse au TP ». Une fois le formulaire rempli, il doit être converti en document à 1½ interligne et imprimé en pdf avant d'être placé dans le fichier zip qui sera remis par le biais du site du cours;
d) Pièces à conviction originales : Dans le même fichier zip, vous placerez une image ad1 (conteneur spécialisé FTK Imager) contenant toutes les pièces à conviction pertinentes et seulement celles pertinentes. L'utilisation du ad1 fera qu'à tous moments on pourra accéder aux preuves originales;
e) Pièces à conviction accessibles : Dans le même fichier zip, vous placerez les pièces à conviction extraites du ad1. La norme pour ces pièces est de pouvoir y accéder par le biais d'un double clic sur un ordinateur où est installé un système d'exploitation Windows 10 et une suite Microsoft Office 360. L'objectif est de permettre au procureur et à la défense d'accéder aux preuves sans avoir à passer par FTK Imager;
f) Vous devez mettre en place et exécuter les procédures pertinentes dans la situation;
g) Si une pièce à conviction ne vous est pas demandée, vous ne devez pas la fournir. Toute équipe n'obéissant pas à cette règle sera pénalisée.

5) **Règles du jeu** :

a) Jouez le jeu ! Votre rapport sera meilleur si vous vous placez dans la peau d'un investigateur numérique en train de vraiment effectuer le travail;
b) Le présent exercice est programmé pour vous permettre d'appliquer les connaissances acquises lors du cours et de mener **vraiment** l'enquête, dans un contexte s'en approchant le plus possible. Bien que ça puisse être tentant, vous devez éviter de recourir à des logiciels autres que ceux ayant fait l'objet d'une installation lors du laboratoire sur les environnements forensiques. Le TP a été créé de façon à ce qu'il soit entièrement faisable avec ces applications;
c) Toute question relative à la technique ou aux procédures d'enquête ou au droit s'appliquant dans le contexte du cas Parisakys devra être acheminée à la personne suivante :
   i) Pour INF-8430 : votre chargé(e) de laboratoire;
   ii) Pour IFT-3002 : votre enseignant;
   iii) Pour 8SEC202 : votre enseignant;
d) Cette personne-ressource se chargera de faire liaison avec Marianne Fitzwalter, as de l'enquête, MBA et Ph.D. en criminologie. Celle-ci veut que vous tiriez de la barrette USB un maximum d'informations. Toutefois, aucune information ne sera donnée par cette personne-ressource quant aux preuves qui s'y trouve. Lorsqu'on examine forensiquement un média, c'est vraiment très très très rare que ton patron connaisse d'avance ce qui s'y trouve : il faut se débrouiller avec un budget restreint, les moyens du bord, beaucoup de patience dans la recherche et une certaine dose d'intuition!

e) L'échange d'informations entre équipe est permis. **MAIS** : vos notes et le contenu de votre formulaire doivent être le fruit de **votre** travail d'équipe et doivent démontrer que vous avez effectué le travail. Si vous posez des questions ou échangez des informations avec des collègues ou avec votre personne-ressource, **ceci doit apparaître dans vos notes manuscrites**;

f) **Important** : Pour votre gouverne, toutes les pièces à conviction importantes ont été piégées. Le contenu de l'« Image02.E01 » de la clé ressemble à celui de l'« Image03.E01 ». Mais ce n'est qu'une apparence (pour vous en convaincre, faite l'empreinte numérique de ces deux fichiers E01). Vous devez donc fournir les pièces à conviction provenant de **VOTRE** image.

g) **Toutes les équipes reçoivent comme mission de trouver les preuves pour le vol et la falsification de cartes de crédit et la possession de carte de crédit volée, fabriquée ou falsifiée ainsi que le crime commis à l'endroit du fils de l'homme ayant eu une altercation avec Parisakys au restaurant, de même que le (ou les) crime(s) ai(en)t été commis par Parisakys ou par ses comparses**.

h) **En plus de cette mission commune**, vous recevez une mission particulière à votre équipe. Vous devez enquêter sur le crime qui vous est révélé par le fichier encastré dans le fichier .rib. Vous devrez, ultimement, fournir le fichier désencastré du .rib ainsi que tout autre fichier montrant ce même crime. À l'égard de ce crime (et de ce crime seulement), vous devrez suggérer à Fitzwalter **un** article de loi en vertu duquel Parisakys doit être poursuivi par le procureur et dire pourquoi vous choisissez cet article. Pour vous aider, consultez le document « Articles de loi » que vous trouverez sur le site du cours.

i) D'un point de vue éthique, il est impossible d'utiliser des photographies illustrant réellement les crimes. Par exemple, on ne peut pas utiliser la photo d'une personne commettant un meurtre ou la photo d'un cadavre pour illustrer qu'un meurtre est commis par notre « suspect » car ceci irait contre les valeurs académiques québécoises ou risquerait, à bon droit, de heurter la sensibilité de certaines personnes.

j) En conséquence, nous allons utiliser un code :

Une photo de :	**Signifie ce crime :**		**Une photo de :**	**Signifie ce crime :**
Mouche domestique	Possession de pornographie infantile		Motocyclette	Méfait concernant des données
Cochon/porc/truie	Harcèlement criminel		Chaise	Traite des personnes
Voilier	Incitation publique à la haine		Serpent	Vol de services de télécommunication
Escargot	Utilisation non autorisée d'ordinateur		Moulin à coudre	Extorsion
Ours	Intimidation		Sofa	Diffamation
Dauphin	Fraude		Vache	Leurre d'enfant
Vampire	Terrorisme			

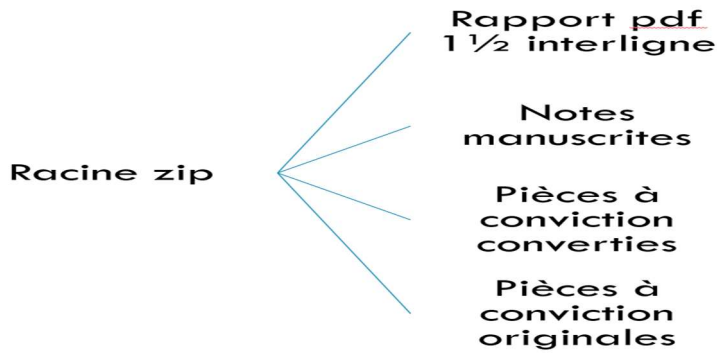
Par exemple : Si votre fichier désencastré du fichier .rib est un fichier représentant un cochon, c'est que vous avez été assigné à une investigation à propos de harcèlement criminel et toutes les photos de cochon, de truie, de porcelet ou de porc deviennent des pièces à conviction démontrant du harcèlement criminel et toutes les autres photos ne sont plus que des photos d'ordre général (une photo de moto n'est plus alors qu'une photo de moto, un photo d'ours n'est plus alors qu'une photo d'ours… etc.)

6) **Structure du fichier zip** : Pour des raisons de commodité, vous ne remettrez qu'un seul fichier qui sera un fichier zip. L'organisation de ce fichier doit être la suivante :

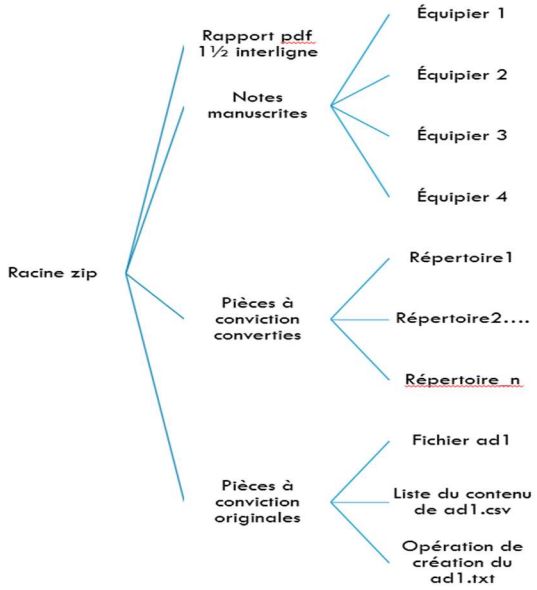
a) À la racine, on retrouve les éléments suivants :
   i) Le formulaire de réponse à ce laboratoire (formulaire rempli, bien sûr!) et converti en pdf à 1½ interligne;
   ii) Le fichier ad1 contenant les preuves trouvées dans l'image forensique bit-à-bit;
   iii) Le dossier « Notes manuscrites des investigateurs numériques »;
   iv) Le dossier « Pièces à conviction »;

b) Dans le dossier « Pièces à conviction », il y a deux sous-répertoires :
   i) Pièces à conviction originales : Ce sous-dossier contient le fichier ad1 et ses deux fichiers accessoires d'information (contenu du ad1 et description de la création). Le ad1 contient les artéfacts extraits de l'image forensique bit-à-bit E01. Un fichier ad1 permet de protéger l'intégrité des fichiers qui y sont déposés car il est en lecture seule.;
   ii) Pièces à conviction converties : Le procureur ne dispose pas des logiciels d'investigation numérique. Il dispose en fait d'une simple suite bureautique. Il peut donc, par défaut, lire des fichiers comme, notamment, docx, pdf, jpg… Si une suite bureautique standard n'est pas en mesure d'ouvrir un fichier contenant une preuve, vous devez la convertir afin que le procureur puisse consulter ce fichier. Ce sous-répertoire doit reproduire la structure du fichier ad1 des « Pièces à conviction originales ». Bref, la structure doit correspondre à ce que le procureur verrait s'il regardait l'original avec un explorateur de fichier

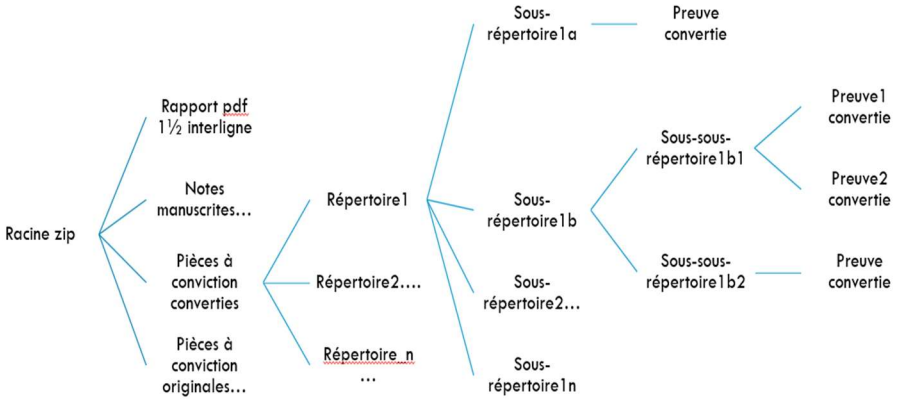
c) La structure du fichier .zip ressemblera donc à ce qui suit :



- Plus en détail :

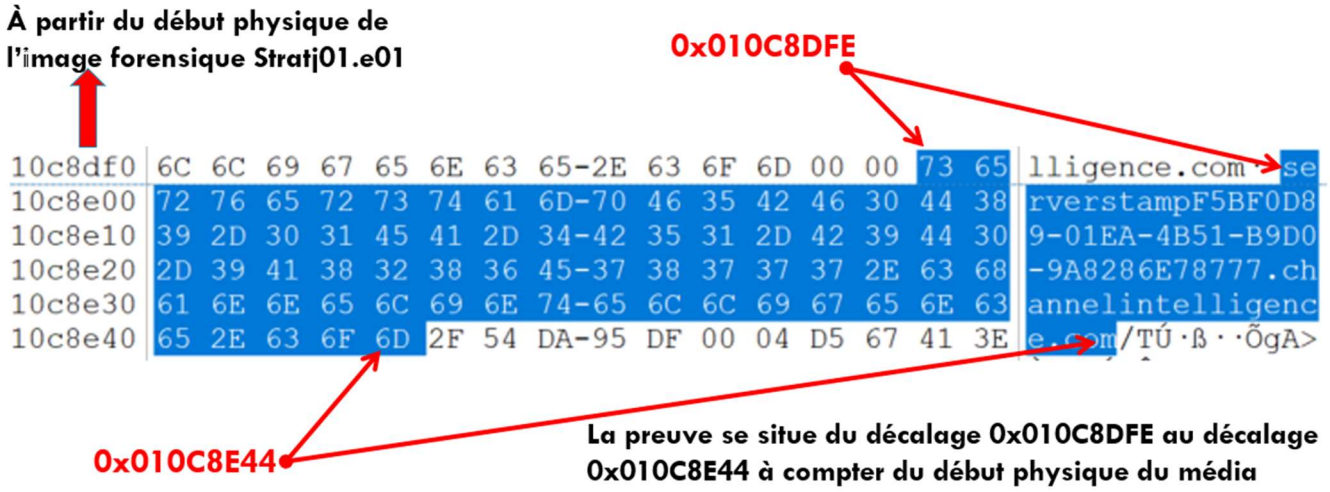


- Et détail pour le seul répertoire « Pièces à conviction converties » :



d) Certaines preuves se trouvent dans des parties non-accessibles d'un fichier ou d'un média pour une personne n'ayant pas de notion de forensique. Exemples : La preuve est dans … 1- la balance d'un fichier ou d'une partition, 2- les intradonnées d'un fichier, 3- le corps d'un fichier impossible à lire avec un ordinateur équipé seulement d'une suite bureautique classique (par exemple : une base de registre ou le contenu d'une mémoire RAM). Dans ces circonstances, on doit utiliser une approche en deux parties pour bien mettre en valeur la preuve. Dans un premier temps, on utilise un éditeur hexadécimal, sélectionner ce qui constitue la preuve et sauvegarder la sélection dans un fichier ayant une extension .brut et un titre évoquant le décalage d'où la preuve est issue. Dans un deuxième temps, on prend un aperçu d'écran de la preuve, avec une extension qui peut être, notamment, .png et un titre évoquant le décalage d'où est issue la preuve. Tous les fichiers .brut sont sauvegardés dans un répertoire réservé à cette fin et tous les .png dans un autre répertoire réservé à cette fin. Le répertoire contenant les fichiers .brut est ensuite monté dans FTK Imager et les

fichiers .brut (et non le répertoire au complet) sont ajoutés à l'image personnalisée .ad1 qui sera placée dans le fichier .zip à remettre. Quant aux aperçus d'écran, ils seront placés dans le sous-répertoire pertinent qui sera remis au procureur. Ci-dessous une illustration de cette procédure en deux parties. N'oubliez pas de faire référence aux .brut et/ou aux .png pertinents dans votre rapport.



Option1: On sélectionne la preuve et on la sauvegarde (« Save Selection », dans un répertoire réservé à cette fin, sous le nom de « 0x010C8DFE_0x010C8E44_débutPhysStratj01.raw ». On insère ensuite le fichier dans le .ad1 final des preuves originales et un aperçu d'écran dans le dossier du procureur.

e) Le fichier contenant les preuves originales est une image personnalisée .ad1 que vous construirez à l'aide du logiciel FTK Imager. Dans le .zip final, veuillez fournir le fichier .ad1 avec ses fichiers afférents .txt et .csv.

7) **Artéfact à examiner** :

a) Les artéfacts se trouvent sur le site du cours et le mot de passe est Bal&Inf+Ift= (Il se peut que pour certains fichiers, le mot de passe soit : Bal&Inf+Ift=5428).

b) Voici les artéfacts qui vous sont assignés :

#Équipe :	1/A	2/B	3/C	4/D	5/E	6/F	7/G	8/H	9/I	10/J	11/K	12/L	13/M
#Image :	4	6	15	11	10	13	14	12	9	8	5	13	7
#Équipe :	14/N	15/O	16/P	17/Q	18/R	19/S	20/T	21/U	22/V	23/W	24/X	25/Y	26/Z
#Image :	5	7	9	14	8	15	10	11	4	15	12	6	13

8) **Barème de correction** :

Le barème de correction se trouve à la page 1 du formulaire de réponse.