Laboratoire – Forensique volatile

Avertissement : Le texte qui suit a été écrit en 2015 et se rapporte à des artéfacts créés en 2015. Ceci explique certaines incohérences, notamment que l'enquête informatique nous soit confiée dans le courant de l'année actuelle.

1. Situation :

Les protagonistes de notre cas sous investigation sont Robin Des Boies et Zénon Rusalka.

Robin Des Boies est un escroc des temps modernes qui vole aux riches pour donner aux pauvres. Pour lui, tous les coups sont permis, du moment que ce sont les riches qui payent. Des Boies est présentement président de l'AIMÉ, l'**A**ssociation **I**nternationale des **M**alandrins **É**ternels.

Zénon Rusalka est le très connu (mais pas très populaire) président, directeur-général et vice-président du développement des affaires et du développement durable de la Banque des Pauvres de Nouvelle-France.

Le 11 mars 2015, entre 19H00 et 20H00, Zénon Rusalka a reçu un courriel de la part de Robin Des Boies qui contenait des menaces de chantage. Du haut de son arrogance, Rusalka a immédiatement répondu, par courriel, dans sa langue natale : « A*z idő fogja megmondani* ».

Il s'est aussitôt tourné vers le chef de la sécurité de la banque, Morton Kasperovsky. Celui-ci s'est dit choqué de ces menaces à l'endroit de son chef, mais a admis son impuissance devant ce type de problème depuis que Rusalka, dans un élan d'austérité[1] (Rusalka avait alors présenté ceci comme de la « rigueur budgétaire » !), avait éliminé tous les postes d'investigateurs numériques à la banque. De guerre lasse, Rusalka s'en fut chez lui, rongé par une insomnie qu'il réussit à calmer, à 1h00 du matin, avec 250 ml de The Dalmore Rare & Fine Quarante-Cinq Ans Highlands Single Malt (33,000$/750 ml à la SAQ! Il est d'usage d'en humer les nobles vapeurs plutôt que de le boire comme le font les roturiers !).

Le lendemain, Rusalka est arrivé vers 5h00 à la banque. Une surprise l'y attendait. Vers minuit, un coursier masqué avait déposé un paquet dans le tiroir des dépôts de nuit. Ce paquet était adressé à Rusalka et contenait une clé USB et un message écrit en lettres détachées. Le message disait : « Hier, je me suis introduit subrepticement chez Robin et j'ai pris une copie forensique de la mémoire RAM de son ordinateur, de son « pagefile » et de sa base de registre. Ça va vous donner les renseignements nécessaires pour l'attraper et le faire condamner. Signé — Adélard Victor Gérard Comodor »

Il faut savoir que Comodor fait partie de l'AIMÉ et est aspirant au poste de président. C'est par ce coup de Jarnac et non par bonté d'âme qu'il espère dégommer Des Boies en le mettant hors circulation. Méfiant, Rusalka contacte Alfredo d'Avira, capitaine de la police locale, dont la maison est hypothéquée trois fois par la Banque des pauvres de Nouvelle-France, grâce à la duplicité de Rusalka. D'Avira lui conseille de contacter la firme privée d'investigation numérique InvNum Inc. qui a pris le relais. La clé a été remise à Sylvain Desharnais, président de la firme, sans avoir été consultée de quelque façon que ce soit. Sylvain Desharnais l'a imagée de manière forensique et a transféré cette image forensique sur son site web corporatif.

2. Mission :

Votre équipe a été mandatée pour examiner la clé USB et en extraire les informations numériques se rapportant au cas. De plus, vous devrez faire des recommandations sur les poursuites à entreprendre contre Robin Des Boies. À cet égard, vous devez considérer le droit québécois et canadien, aux niveaux civil et criminel. Recommander de poursuivre implique de fournir les preuves nécessaires et les renseignements, les plus précis possibles, demandés par le formulaire. Notamment, en ce qui a trait à l'article de loi, il doit être

[1] Il faut se rappeler qu'au moment d'écrire ce TP, le gouvernement du Québec, mené par les libéraux, procédait à une diminution des dépenses dans l'appareil gouvernemental. Série de coupures décriées comme appauvrissant encore plus les classes pauvre et moyenne des québécois. Les partis de l'opposition appelaient cela de l'austérité mais le gouvernement disait que c'était de la rigueur!

précis jusqu'à la disposition pertinente.

3. **Exécution :**

   a. Introduction : Pour les fins de cette mission, votre chef d'équipe est :

      i. INF8430 : Chargé(e) de laboratoire ;

      ii. IFT3002 : Chargé de cours ;

      iii. 8SEC202 : Chargé de cours.

      La supervision vise à vous permettre de mener à bien cette mission. Vous aurez à votre disposition l'image de la clé USB reçue par Monsieur Rusalka. Afin de bien vous acquitter de cette tâche, vous devez remplir le formulaire qui vous est fourni par le site web d'InvNum Inc. (i.e. : le site web du cours).

   b. Précisions :

      i. Une mémoire RAM, c'est un fouillis de données morcelées en segments de longueur uniforme, segments qui sont sauvegardés sans ordre apparent (le segment #1 peut être sauvegardé dans des secteurs ayant des numéros plus élevés que les secteurs où est sauvegardé le segment #2, par exemple).

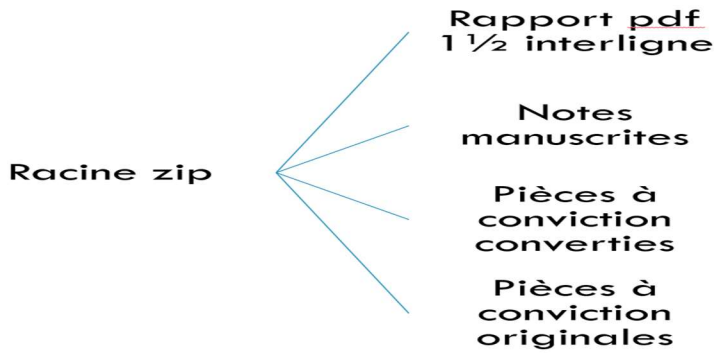
      ii. Une mémoire RAM de 256 Mo, c'est comme 6 boîtes d'archive, pleines à craquer de feuilles format lettre imprimées recto verso sans retour de charriot. Même avec les meilleures intentions, ce ne serait pas possible de tout examiner dans le délai qui vous est imparti.

      iii. On ne vous demande donc **PAS** de sortir 100% des indices présents dans la RAM, la mémoire tampon et la base de registre. On vous demande de fournir environ une **vingtaine** d'indices (en tout et partout et au total de toutes les questions) qui vous permettraient d'affirmer sous serment que vous avez des motifs raisonnables de croire que Des Boies a commis une entorse.

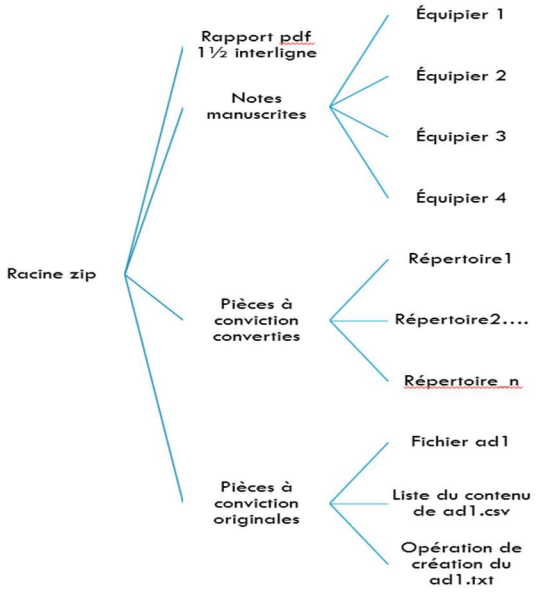
      iv. Pourquoi des motifs raisonnables de **croire** et non des motifs raisonnables de **soupçonner** ni des motifs de **soupçon** ? Parce que des motifs raisonnables de croire permettront à un policier d'obtenir un mandat de perquisition ou à un particulier d'obtenir une ordonnance Anton Piller ou encore d'intenter directement une poursuite civile.

      v. **Mais attention!** Vous ne devez pas vous contenter d'utiliser seulement les extrants de Memoryze/Redline et de Volatility. Vous devez appliquer d'autres techniques apprises en cours de session, utiliser d'autres logiciels, certains familiers et d'autres que nous avons survolés le temps d'un clin d'œil. DONC : ne vous contentez pas d'utiliser seulement deux logiciels.

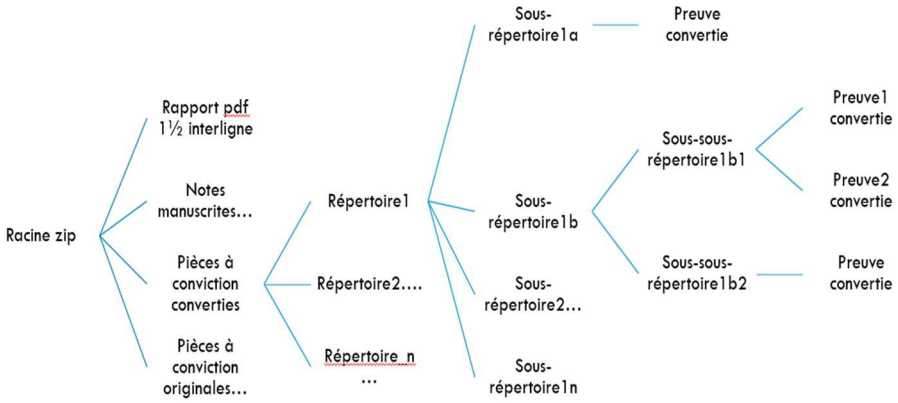
      vi. Si on vous demande de fournir un artéfact précis, il doit être fourni de manière **forensique**. Tous les artefacts demandés ainsi que votre rapport (le formulaire de réponses rempli) et vos notes **manuscrites** doivent être regroupés dans un seul et même fichier, à savoir un seul fichier **zip.** Structure interne sommaire du zip :



- Plus en détail :



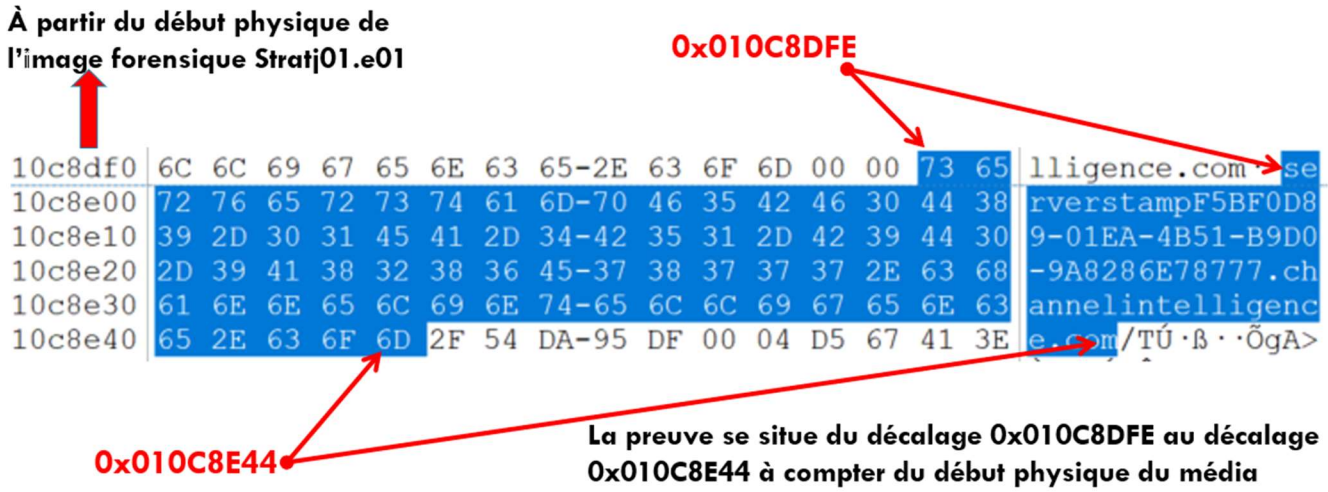
- Et détail pour le seul répertoire « Pièces à conviction converties » :



vii. Vous devrez utiliser FTK Imager pour créer l'image personnalisée .ad1. Les pièces à convictions originales se retrouveront automatiquement avec la structure de répertoire appropriée. Vous devez fournir le ad1, le csv et le txt afférents aux preuves repérées dans un répertoire identifié à cet effet.

- 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[2]; 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.

[2] Le décalage doit être exprimé de façon complète, c'est-à-dire que ce sera un tuple décalage de début – décalage de fin OU décalage de début - longueur



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.

viii. Comme vous êtes investigateurs numériques, vous ne devez pas transgresser ce qui serait la Loi si nous étions en situation réelle. Dans un cas réel, si vous trouviez un mot de passe ou une donnée se rapportant à un individu que notre suspect ou à un crime autre que celui sur lequel vous enquêtez, vous devriez en parler à votre superviseur avant de procéder. Sachez toutefois qu'aucune action ultérieure à l'endroit des membres de l'AIMÉ ne sera autorisée d'ici six (6) mois. Merci de vous conformer aux lois du pays « simulation de cas »...

ix. Vous devez soumettre les notes **manuscrites** (écrites à l'encre bleue, sur une feuille lignée, sur des pages numérotées) de **tous** les membres de l'équipe.

a. Avertissement avant de commencer : Si des mises en situation sont utilisées, c'est pour vous placer en contexte. De votre côté, vous devez jouer le jeu et faire comme si vous travailliez pour le cabinet InvNum Inc. On s'attend donc à de l'intuition, des remarques pertinentes et de l'implication, comme si vous y étiez.

b. Artefacts à votre disposition :

i. Un conteneur judiciaire personnalisé (« custom content ») FTK Imager contenant l'image de la mémoire vive (RAM) et de la mémoire de débordement (le « pagefile ») de l'ordinateur de Des Boies ;
ii. La base de registre de l'ordinateur de Des Boies ;
iii. Trois photos suspectes que Comodor a placées sur la clé ;
iv. Pour éviter que vous passiez vos trois heures à taper des commandes dans Volatility plutôt que d'analyser, les fichiers txt issus de plusieurs commandes Volatility sont fournis. Ces fichiers sont stockés dans le dossier 04 Résultats. Pour activer ces commandes, un script DOS.bat a été utilisé ;
v. L'analyse Redline déjà faite pour la mémoire vive fournie ;
vi. Le formulaire sur lequel vous devez répondre, puis l'imprimer en pdf et **à interligne et ½** avant de le remettre via le site du cours. Vous êtes priés de ne pas modifier la structure du document, c'est-à-dire que si le numéro 2 est à la page 4 sur le formulaire, il doit apparaître sur la page 4 dans votre rapport ;
vii. Le présent document.

4. **Consigne d'utilisation des artéfacts :**

a) Il y a trois fichiers zip créés à l'aide de 7zip et contenant les artefacts nécessaires à la réalisation du laboratoire de forensique volatile ;

b) Décompressez le contenu des fichiers RobinDesBoies1 et 2 dans le même répertoire, à l'aide d'un logiciel d'archives compétent. À l'aide de FTK Imager, ouvrez captureMemoires.ad1. CaptureMemoires.ad1 indiquera à FTK Imager qu'il doit aussi ouvrir captureMemoires.ad2. Vous n'avez donc pas à ouvrir captureMemoires.ad2 ;

c) Décompressez ensuite le fichier zip #3 dans un répertoire séparé et réservé à cet effet. Ce fichier contient les artefacts autres que les fichiers d'images forensiques. Si vous voulez utiliser des logiciels autres que FTK Imager pour accéder à ces fichiers ou en extraire des preuves, vous devrez vous assurer d'inclure ces preuves dans le ad1 final et indiquer dans votre rapport comment ces preuves ont été obtenues. Pour ceux qui ont écouté les capsules HIN, ça devrait être facile à faire ;

d) MOT DE PASSE : CFIJ=greinarmerki/4712 Attention: sensible à la casse!!!

5. **Rapport :**

a. Formulaire de laboratoire : Vous devez remplir le formulaire de laboratoire, puis l'imprimer en **pdf** à **1½ interligne** avant de l'insérer dans le zip à l'endroit approprié, zip que vous remettrez via le site du cours. Vous êtes priés de ne pas modifier la structure du document « Formulaire », c'est-à-dire que si le numéro 2 est à la page 4 sur le formulaire, il doit apparaître sur la page 4 dans votre rapport ;

b. Pièces à conviction : Vous devez remettre vos pièces à conviction de la façon prescrite ci-haut. Vous serez notamment notés en fonction de la qualité de présentation de vos preuves, originales comme converties, et de vos notes manuscrites. ;

6. **Défi :**

En relevant le défi, vous pouvez augmenter votre note globale, jusqu'à concurrence de 100% de la note totale, mais un maximum de 5 points sont en jeu. Le défi est de révéler une information étonnante ou inusitée (lors de la correction, on fera comme si les étudiants des années passées ne nous avaient jamais révélé d'information étonnante ou inusitée). Aucun indice ne sera donné à cet égard et aucune question à ce sujet ne sera répondue (la question revenant le plus souvent par les années passées étant « Croyez-vous que telle preuve nous vaille des points ? » : vous êtes donc seuls pour nous étonner. Le mode de correction sera le suivant :

a. Nous comparerons les réponses au défi de toutes les équipes et nous les rangerons de la plus étonnante à la moins étonnante ;
b. L'information la plus étonnante recevra une note tenant compte de son originalité, de son utilité à l'enquête et de la quantité et la qualité travail fait pour l'obtenir ;
c. Les réponses suivantes (toujours classées par ordre d'étonnement) recevront une note moins élevée que les réponses précédentes.