Étude de cas – Posinc

Faits ou observations pendant la perquisition

Résidence de Jean Saies

Voici les observations faites et les faits constatés pendant votre perquisition chez Jean Saies :

- À votre arrivée sur les lieux, à 8h00, Jean Saies est déjà au bureau. On vous donne l'ordre d'attendre que celui-ci vienne ouvrir la porte, ce qu'il fait vers 09h10;
- L'appartement où il habite est minuscule et le seul endroit où il y a des papiers, c'est dans une boîte d'archive dont la fouille prend environ 20 minutes;
- Son appartement est divisé en cinq : salle de bain, cuisinette, deux chambres à coucher et un salon qui sert de bureau;
- Près de la fenêtre, face à l'entreprise Posinc sise de l'autre côté de la rue, se trouve un bureau sur lequel se trouvent deux ordinateurs portatifs dont l'un est affublé d'un auto-collant « Posinc – De wyn yn jo seilen! ». Vous demandez à Jean Saies ce que signifie ces mots. Il hausse les épaules en affirmant qu'il ne sait pas et que c'est un ami originaire d'Europe qui lui a donné cet auto-collant;
- Vous demandez à Jean si cet ordinateur portatif est celui qui appartient à Posinc et il dit que c'est le cas;
- Vous prenez une photo de l'auto-collant et Jean s'en dit outré, criant à l'intrusion dans sa vie privée;
- Vous demandez les mots de passe des ordinateurs et il refuse de vous donner quoi que ce soit;
- Dans le tiroir du bureau, vous trouvez une clé USB de 1 Mo, une clé USB de 128 Mo, une clé USB de 256 Go;
- La clé de 1 Mo comporte un logo disant « Ménard & associés » et une étiquette disant « Testament – Jean Saies ». Vous lui demandez s'il s'agit bien de son testament et il répond que c'est le cas et il tente, sans succès, de s'emparer de la clé;
- Vous demandez à Jean Saies à qui appartient l'autre ordinateur portatif et il dit que ça lui appartient en personne et qu'il s'en sert uniquement pour naviguer sur Internet;
- Vous demandez à Jean ce que contiennent les deux dernières clé USB et il répond que ça ne contient rien d'intéressant;
- L'équipe de fouille physique trouve un cellulaire Samsung Galaxy A8 sur le dessus de la table de nuit de Jean Saies;
- Vous demandez à Jean si ce cellulaire lui appartient. Il répond que la compagnie lui a acheté ce cellulaire mais qu'il l'utilise rarement;
- Dans la deuxième chambre à coucher, vous repérez une ardoise tactile (une « tablette ») Microsoft Surface Pro. Il déclare que c'est l'appareil personnel de son fils et qu'il ne s'en sert jamais;
- Jean affirme que vous n'avez pas le droit de fouiller cet appareil puisqu'il appartient à son fils;
- Vous demandez à Jean où est son fils et il dit, un peu agressif « Il travaille, LUI! Pas comme d'autres qui empêchent les travailleurs honnêtes de travailler! »
- Vous lui demandez s'il est possible de lui parler et il répond, excédé « Fichez-lui la paix. Y'a rien à voir avec ce que vous cherchez! »
- Jean quitte ensuite les lieux en grommelant des insultes peu discrètes;
- Dans une boîte rangée dans le placard de la chambre du fils, l'équipe de fouille trouve un disque externe sans-fil My Passport;
- Vous contactez votre collègue affecté à la fouille des ordinateurs chez Posinc, de l'autre côté de la rue. Vous lui dites que Jean Saies n'a pas voulu vous donner le mot de passe de l'ordinateur portatif et il vous donne le mot de passe administrateur de Posinc « Soleil123 »;
- Vous commencez l'examen de la clé USB 1 Mo et elle contient un seul document docx dont le contenu est effectivement un testament du dénommé Jean Saies. Vous fermez le fichier et remettez la clé où vous l'avez trouvée;

- Vous voulez examiner l'ordinateur portatif corporatif. À cette fin, vous ouvrez physiquement l'appareil et vous en retirez le « disque dur » : un Samsung NVMe avec une interface PM980a de 256 Go pour lequel vous n'avez pas d'adaptateur;
- Vous tentez un démarrage avec une clé USB Paladin et celle-ci réussit. Vous créez une image forensique du disque et vous la placez sur un disque USB portatif aseptisé que vous avez apporté;
- Pendant que l'image forensique se créée, vous fouillez l'ordinateur portatif personnel;
- Vous en ouvrez le capot et son disque dur est un SATA-SSD de 120 Go. Vous le retirez de l'appareil et vous le branchez sur votre ordinateur portatif de fouille, par le biais d'un adaptateur SATA-USB et après avoir protégé le port USB contre l'écriture;
- Il s'agit d'un Windows 10 version Famille qui ne comporte que deux utilisateurs (à l'exception des utilisateurs par défaut de Microsoft, dont le compte d'administrateur) : Jacques et JeanSaies;
- Vous commencez à examiner le répertoire JeanSaies;
- Il contient à peine une demi-dizaine de documents relatifs à Posinc, tous d'une importance secondaire;
- Il contient aussi une centaine de jpg parmi lesquels vous ne trouvez rien qui se rapporte à l'investigation en cours;
- En examinant le disque, vous réalisez que Jacques Viens est camionneur pour TRIMI;
- Dans le répertoire « Jacques » il y a un sous-répertoire « Doctorat »;
- D'après les documents présents dans ce répertoire, vous comprenez que le métier de camionneur de Jacques Viens n'est pas sa seule occupation. Il prépare présentement une thèse sur l'actualisation rétrograde inversée des anti-paiements rédhibitoires versés de façon postdatée aux grossistes en jouets;
- Un autre document indique que la date de dépôt de sa thèse est dans 2 semaines de la date d'aujourd'hui;
- Un des logiciels parmi ceux utilisés récemment par Jacques est le logiciel de statistiques R;
- Il y a une multitude de bases de données dans le répertoire de Jacques
- Un autre sous-répertoire de Jacques est le répertoire « Voyages aux States ». Vous constatez que Jacques tient un compte très serré de tous ses voyages aux États-Unis, incluant la portion de ces voyages parcourue au Canada;
- Un autre sous-répertoire (Mes Photos) contient 2783 photos en format jpg, prises avec un appareil Canon IXUS 275 HS (avec fonctionnalités GPS et Wi-Fi, fonctionnalités qui sont apparemment activées si l'on en croit votre examen des intradonnées);
- Les fouilleurs physiques n'ont pas trouvé d'appareil photo lors de la fouille;
- Le répertoire « Mes Photos » contient des photos de paysages, dont certains sont célèbres : Vieux-Québec, Oratoire St-Joseph, chutes Niagara, Vallée de Napa, Grand Canyon…
- Vous choisissez au hasard une trentaine de photos sur les 2783 et vous ne trouvez aucune photo de nature personnelle;
- En dehors de ces répertoires, il n'y a rien qui vaille la peine d'être mentionné;
- Le cellulaire n'est protégé par aucune fonctionnalité de protection (mot de passe, dessin, empreinte digitale, reconnaissance faciale ou oculaire);
- Vous constatez que l'écran du cellulaire est fracassé au point de ne pas pouvoir voir 80% de l'écran;
- Vous le connectez sur votre laptop de perquisition et vous en visualisez le contenu avec CellSpy Pro;
- Le système d'exploitation du Samsung est un Android #XYZ Drumstick;
- Vous consultez le carnet d'adresse;
- Ce carnet d'adresse contient les noms de personnes clairement associées à Posinc;
- Dans ce carnet, vous voyez la mention « Mon Fils » et vous notez que le fils porte le nom de Jacques Viens;
- Le dernier appel fait avec ce téléphone date d'il y a peu, le 11 mars 20XX à 17h33;
- L'appel a été placé auprès de l'identifiant « Camion 7718 »;
- Dans un des répertoires utilisateur, vous trouvez une série de fichiers audio dont les noms s'apparentent à une date-heure. Vous faites jouer celui intitulé 20XX0311_1733;

- L'un des interlocuteurs, selon toute vraisemblance, est Jean Saies;
- Celui-ci donne instruction à son correspondant de faire un détour par le 305, chemin Sainte-Julie à Saint-Clet pour ramasser du stock à convoyer jusqu'à Napa et à remettre à la « bande de cinglés de la diète »;
- Il y a une centaine de conversations en tout;
- Il y a beaucoup de photos personnelles de Jean Saies avec une femme et un enfant d'une dizaine d'années dans toutes sortes de situations de la vie quotidienne;
- Certaines photos montrent la femme couchée dans un cercueil;
- Il y a beaucoup de photos du même enfant à tous âges;
- La clé USB 256 Go contient une base de données chiffrée avec un logiciel, présent sur la clé, programmé pour stocker des mots de passe;
- Vous essayez différents mots de passe, sans succès. Frustré, vous inscrivez de façon distraite ce qu'il y a d'écrit sur l'étiquette de l'ordinateur portatif corporatif « De wyn yn jo seilen! » et la base de données s'ouvre;
- Toutes les entrées sont constituées de mots (apparemment un surnom) suivi de chiffres et de ce qui semble un numéro de téléphone, style « Mal Léché 925.50 45.3592722 -74.2448667 450-555-1234 »
- La clé contient aussi des feuilles de travail Excel protégées par un mot de passe. Vous tentez le coup avec le mot de passe découvert pour la base de données, sans succès;
- Vous ouvrez un des fichiers Excel avec 7-zip et vous le déconstruisez afin de lire les données du document.xml;
- Vous y trouvez des adresses de Toronto, Macao et Monaco, mais partielles, sauf une, à Dublin;
- Vous allez sur Google Street View pour voir ce qu'il y a à cette adresse et vous constatez qu'il s'agit d'une banque;
- Vous fouillez le fichier xml de Excel à l'aide des mots-clés TRIMI, Posinc et Tariss, mais le fichier ne contient aucune de ces occurrences;
- La clé n'a rien de spécial en termes de spécifications. Elle est d'un type qu'on peut facilement trouver dans un magasin d'électronique;
- Vous pensez que pour accéder aux informations des autres feuilles Excel, ça va vous prendre au moins 4 heures encore;
- La clé contient des fichiers dont l'extension est pbz;
- La clé contient aussi des vidéos et des photos de Jean et son fils lors d'événements importants comme sa graduation, une compétition de natation où il gagne la médaille d'or, etc…
- Faire un clone forensique de la clé prendrait 270 minutes;
- Vous en êtes là lorsque l'image forensique de l'ordinateur portatif corporatif indique la fin de la procédure;
- Vous ouvrez l'image forensique de l'ordinateur portatif corporatif et vous constatez que la partition principale est chiffrée avec BitLocker. Vous donnez le mot de passe « admin » qui vous a été fourni par votre collègue et ça vous donne accès au contenu;
- Le répertoire C:\Users\JeanSaies\Documents contient des documents dont le contenu correspond à ce qui est recherché dans le cadre de la perquisition;
- Certains fichiers datent d'il y a 2 ans et d'autres datent d'hier;
- Bien que la plupart des fichiers contenant des données soit dans le répertoire utilisateur de Jean Saies, certains fichiers de données sont dans des répertoires désignés par défaut par des logiciels lors de leur installation;
- C'est le cas d'une centaine de fichiers ayant une extension pbz. Leur contenu semble compressé ou codé. Vous tentez différentes procédures pour y avoir accès. Vous réussissez à y accéder, mais pour chaque fichier, la procédure dure 20 minutes;
- Le contenu des fichiers pbz est relié aux affaires de Posinc pour la période sous enquête;

- Vous réalisez que l'extension pbz est lié au logiciel « PlusssBizard ». Vous téléphonez au fabriquant pour en avoir une copie de courtoisie et il vous dit qu'il n'en met pas à la disposition des autorités gouvernementales et que ce sera 500$ pour une seule licence;
- Il vous signale que le fait d'avoir une copie du logiciel ne donne pas forcément accès aux données car le logiciel doit d'abord reconnaître l'environnement installé avant d'ouvrir un fichier créé dans cet environnement;
- Vous lui demandez s'il lui est possible (pour ce fabriquant) de garantir l'accès aux données, s'il peut « bidouiller » les bases de données de manière à contourner les restrictions du logiciel. Il répond que oui, mais que c'est une journée de travail complète, ce qui coûtera au-delà de 2 000 $;
- D'autres fichiers sont dispersés un peu partout sur le disque dur et il vous est difficile de déterminer les répertoires contenant de l'information pertinente au mandat de ceux qui ne le sont pas;
- Certains fichiers sont dans un répertoire dont l'accès semble interdit, même à l'administrateur de la compagnie;
- Certains des logiciels installés sur l'ordinateur portatif corporatif permettent à Jean Saies de se connecter sur les logiciels d'expédition et réception de TRIMI, de la division alimentaire et de la division Électronique;
- Une base de données fait état de transactions obscures et douteuses datant d'il y a 10 ans;
- La liste des contacts Outlook de Jean Saies contient les noms de plusieurs (mais pas tous) chauffeurs de TRIMI et de plusieurs employés des quais d'expédition/réception de Shawinigan, Laval, La Prairie et Napa;
- Vous n'avez trouvé aucun indice quant à des instances de diète ésotérique.