# Résumé d’un cas d’étude

Ce qui suit est une traduction, un peu modifiée, d’un document dans « Forensic Examination of Digital Evidence: A Guide for Law Enforcement. » US Dept. of Justice, 2004

<https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>

Consulter l’original pour beaucoup plus d’informations.

(Un vieux cas -1999, mais intéressant et utile à étudier car très bien documenté – malgré les changements technologiques, les principes et les idées de base restent les mêmes)

**Historique**. Un citoyen concerné a contacté la police au sujet de biens possiblement volés.

Il avait trouvé une annonce de vente moto qui l’intéressait. Cette annonce proposait un Honda moto pour un prix bas, donc il a contacté le vendeur. Après avoir rencontré le vendeur, il a été saisi par le suspect que la moto ait été volée. Il a contacté la police qui a alerté l'Unité Vol Auto. L'unité a mené une opération d'infiltration (sting operation) pour acheter la moto. Les agents d'infiltration ont rencontré le suspect, qui, après avoir reçu le paiement, leur a fourni avec le véhicule, le titre de véhicule, la carte d'immatriculation et la carte d'assurance. Bien que les documents fournis par le suspect semblaient être authentiques, Il a été déterminé qu’ils étaient des excellentes contrefaçons. Le suspect a été arrêté et le véhicule qu'il conduisait a été fouillé. Pendant la recherche, un ordinateur portable a été saisi. L'enquêteur de vol d'automobile a contacté le laboratoire de forensique informatique pour examiner l'ordinateur saisi. L'enquêteur a obtenu un mandat de perquisition pour analyser l'ordinateur et rechercher les matériaux utilisés dans les contrefaçons ainsi que d'autres éléments de preuve en rapport avec les accusations de vol de voitures.

**Objectif:** Déterminer si le suspect a utilisé l'ordinateur portable comme un instrument dans les crimes de : vol d'automobiles, fraude, contrefaçon, utilisation de faux documents, possession de titres contrefaits de véhicules ou pour le stockage de données relatives à ces crimes.

**Type d'ordinateur:** Gateway Solo® 9100 ordinateur portable.

**Système d'exploitation:** Microsoft®Windows® 98.

**Chefs d’accusation:** Vol d’auto, fraude, contrefaçon, utilisation de faux documents et possession de titres de véhicules contrefaits.

**Agent du cas:** Enquêteur de vol d’auto

**Lieu de l'examen:** Computer Forensic Laboratory.

**Outils utilisés:** Guidance Software ™ EnCase®, DIGIT ©, Jasc Software ™ Quick View Plus®, et

AccessData ™ Password Recovery Tool Kit ™.

**Traitement**

**Évaluation**

**1**. La documentation fournie par l'enquêteur a été examinée.

a. L'autorité légale a été établie par un mandat de perquisition obtenu spécifiquement pour l’examen de l'ordinateur dans un environnement de laboratoire.

b. La chaîne de traçabilité a été dûment documentée sur les formulaires ministériels appropriés.

c. La demande de service et un résumé détaillé expliquant l'enquête, fournissant de mots clés, ainsi que des informations sur le suspect, le véhicule volé, les documents contrefaits, et la publicité sur Internet. L'enquêteur a également fourni des photocopies des documents contrefaits.

**2**. L'enquêteur d’informatique judiciaire a rencontré l'agent du cas et discuté des possibilités d'enquête additionnelles et des preuves potentielles recherchées dans l'enquête.

**3.** L’acquisition des éléments de preuve a été complétée.

a. Les éléments de preuve ont été marqués et photographiés.

b. Un fichier a été créé et l'information du cas a été enregistrée dans la base de données du laboratoire.

c. L'ordinateur a été stocké dans un local sûr de propriété du laboratoire.

**4.** L'affaire a été confiée à un enquêteur d’informatique judiciaire.

**Création d’images** (Imaging)

**1.** L'ordinateur portable a été examiné et photographié.

a. Le matériel a été examiné et documenté.

b. Un disque de démarrage contrôlé a été placé dans le lecteur de disquette de l'ordinateur. L'ordinateur était sous tension et le programme de configuration du BIOS a été saisi. Les informations BIOS ont été documentées et l'heure du système a été comparée à une source de temps fiable et documenté. La séquence de démarrage a été vérifiée et documentée; le système était déjà prêt à démarrer à partir du lecteur de disquette.

c. L'ordinateur portable a été mis hors tension sans apporter de modifications au BIOS.

**2.** EnCase® a été utilisé pour créer un fichier contenant une image du disque dur de l’ordinateur

a. L'ordinateur portable a été connecté à un ordinateur de laboratoire à travers un câble direct, qui a connecté les ports parallèles des ordinateurs.

b. L'ordinateur portable a été démarré avec un démarrage contrôlé et EnCase® a été lancé en mode serveur.

c. L'ordinateur de laboratoire, équipé d'un lecteur magnéto-optique pour le stockage de fichiers, a démarré avec une disquette de démarrage contrôlé. EnCase® a été amorcé en mode serveur et les fichiers contenant des preuves ont été acquis et écrits sur des disques magnéto-optiques.

d. Lorsque le processus d'imagerie a été achevé, les ordinateurs ont été éteints.

i. L'ordinateur portable a été retourné au local du laboratoire.

ii. Les disques magnéto-optiques contenant les fichiers EnCase® ont été protégés en écriture et soumis comme preuves.

**Analyse**

**1.** Un ordinateur de laboratoire a été préparé avec Windows® 98, EnCase® pour Windows, et autres logiciels d’informatique légale.

**2**. Les fichiers de preuve EnCase® de l'ordinateur portable ont été copiés dans le disque dur de l'ordinateur du laboratoire.

**3.** Un nouveau dossier EnCase® a été ouvert et les fichiers de preuves de l'ordinateur portable

ont été examinés utilisant EnCase.

a. Les fichiers supprimés ont été récupérés par EnCase®.

b. Les données des fichiers, y compris les noms de fichiers, les dates et heures, la taille physique et logique, et chemin complet, ont été enregistrées.

c. Des recherches utilisant les mots-clés fournis par l’enquêteur ont été effectuées. Tous les résultats ont été examinés.

d. Les fichiers graphiques ont été ouverts et consultés.

e. Les fichiers HTML ont été ouverts et consultés.

f. Les fichiers de données ont été ouverts et consultés; deux fichiers protégés par mot de passe et cryptés ont été localisés.

g. L’espace non alloué a été fouillé.

h. Les fichiers de valeur probante ou d’intérêt pour l’enquête ont été copiés sur un CD.

**4.** L’espace non-alloué a été copié des fichiers de preuve EnCase® sur un disque dur nettoyé selon les recommandations du Département de la Défense (DoD 5200.28-STD). Le logiciel DIGIT © a ensuite été utilisé pour découper des images de l'espace non alloué. Un total de 8,476 images ont été extraites.

**5.** Les fichiers protégés par mot de passe ont été copiés sur une disquette de 1,44 MB. L’outil Password Recovery AccessData ™ a été exécuté sur les fichiers et les mots de passe ont été récupérés pour les deux fichiers. Les dossiers ont été ouverts utilisant les mots de passe et visualisés.

**Résultats**

L'analyse de l'ordinateur portable a abouti à la récupération de 176 fichiers de valeur de preuve ou d'enquête. Les fichiers récupérés sont:

**1.** 59 fichiers de documents, y compris les documents contenant le nom du suspect et informations personnelles; texte inclus dans les documents contrefaits; chèques numérisés de salaires, d’entreprises, et chèques certifiés; texte décrivant des objets volés; et un texte décrivant la moto récupérée.

**2.** 38 fichiers graphiques y compris des fichiers d'images à haute résolution représentant des chèques de salaires et d'entreprise ainsi que des chèques certifiés; monnaie des Etats-Unis; titres de véhicules; cartes d'immatriculation et permis de conduire modèles de la Géorgie et d'autres États; cartes d'assurance de diverses entreprises; et chèques certifiés contrefaits payables à une société d'informatique allant de 25 000 $ à 40 000 $ pour l'achat d'ordinateurs portables. La plupart des graphiques ont été analysées.

**3.** 63 fichiers HTML, y compris Hotmail® et Yahoo® e-mail et petites annonces pour la moto récupérée, d'autres véhicules, et plusieurs marques d'ordinateurs portables; textes de courriel, y compris les courriels entre le suspect et le citoyen concerné concernant la vente de la moto récupéré; et courriels entre le suspect et une société d’ordinateurs concernant l'achat d'ordinateurs portables.

**4.** 14 fichiers graphiques récupérés dans l’espace non-alloué représentant différents stades d’achèvement d’images numérisées de monnaie américaine.

**5.** Deux documents protégés et cryptés par mot de passe.

a. un document WordPerfect contenant une liste de renseignements personnels sur plusieurs individus y compris les noms, adresses, dates de naissance, carte de crédit et les numéros de compte bancaire et les dates d'expiration, la vérification des informations de compte et d'autres informations. Mot de passe [nomoresecrets].

b. un document Microsoft®Word contenant des informations de titre de véhicule pour la motocyclette récupérée. Mot de passe [HELLO].

**Documentation**

**1.** Rapport d'expertise - Toutes les actions, les processus et les résultats ont été décrits dans un rapport forensique détaillé, qui est gardé dans le laboratoire.

**2.** Rapport de la police - L'agent de cas a été pourvu d'un rapport de police décrivant les éléments de preuve examinés, les techniques utilisées et les résultats.

**3.** Produit de travail - Un disque compact contenant des fichiers et des données de fichiers de valeur probante ou d'intérêt d'enquête a été créée. L'original a été stocké dans le laboratoire.

Des copies ont été fournies à l'agent chargé du dossier et au procureur.

**Et encore …**

Sur la base de l'information révélée par l'analyse de l'ordinateur, plusieurs nouvelles avenues d’enquête ont été ouvertes.

✔En contact avec les personnes énumérées dans le document WordPerfect protégé par mot de passe, les enquêteurs ont appris que elles avaient toutes été volées dans la même ville pendant l’été précédent par un individu correspondant à la description du suspect.

✔La société informatique a révélé que les chèques contrefaits trouvés sur l'ordinateur suspect avaient été acceptés pour l'achat d'ordinateurs et que des ordinateurs ont été envoyés à lui et ont fait l'objet d'une enquête en cours. Les numéros de modèle et les numéros de série fournis par la société informatique correspondent à plusieurs des petites annonces Hotmail® et Yahoo® trouvés sur l'ordinateur du suspect.

✔ Plusieurs des chèques contrefaits trouvés sur l'ordinateur du suspect étaient déjà objets d'enquêtes en cours.

✔Des information récupérés concernant d'autres véhicules ont conduit à la récupération d’autres véhicules volés.

✔Les informations spécifiques recherchées dans le mandat de perquisition concernant la vente de la moto et les documents contrefaits ont été récupérés à partir de l'ordinateur du suspect.

(40 heures de travail en total - les documents cités ci-haut donnent les détails de temps pour chaque tâche).

**Conclusion**

Les chefs d’accusation contre le suspect ont été élargis. Le suspect a plaidé coupable en cour et il a été condamné.

**Point de réflexion :**

Identifier les véritables « cybercrimes » dans ce cas.

**Note sur la récupération des fichiers.**

Comme usagers, nous avons accès seulement aux fichiers atteignables utilisant l’explorateur fourni par les systèmes d’exploitation, inclus l’explorateur de la corbeille. Mais le disque pourra contenir d’autres vieilles données, souvent fragmentaires et éparpillées, qui ne sont pas atteignables utilisant les méthodes ordinaires. Ces données sont des résidus de fichiers temporaires ou de fichiers que l’usager a voulu effacer de manière définitive. C’est ‘l’espace non-alloué’ mentionné ci-dessus. Il est appelé comme ça car du point de vue du système d’exploitation cet espace est vide et réutilisable. Des outils forensiques, comme EnCase mentionné ci-dessus, permettent d’analyser un disque secteur par secteur. Ces outils peuvent être capables de reconstituer des fichiers fragmentaires et de les ‘recoudre’. Dans la Toile on peut trouver des démonstrations de ces outils, p.ex. chercher ‘forensic data recovery tools’, ‘EnCase’ etc.