Analyse des données récupérables à partir de disques durs hors-service

Travail de diplôme réalisé en vue de l'obtention du diplôme HES

par :

Cyril CHEVALLEY

Conseiller au travail de diplôme :

(David BILLARD, Professeur HES)

Genève, le 24 février 2012
Haute École de Gestion de Genève (HEG-GE)
Filière informatique de gestion

Déclaration

Ce travail de diplôme est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science HES-SO en Informatique de gestion. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de diplôme, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de diplôme, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 24 février 2012

Cyril CHEVALLEY

Remerciements

Je tiens à remercier toutes les personnes qui m'ont soutenu dans la réalisation de ce travail de Bachelor ainsi que tout au long de mon cursus à la Haute Ecole de Gestion.

Je remercie particulièrement Monsieur David BILLARD, mon directeur de mémoire, pour son suivi et la mise à disposition du matériel nécessaire à l'accomplissement de ce mémoire. Je remercie également Monsieur Matias LOURO, assistant HES, pour sa disponibilité.

Je souhaite également remercier ma famille pour m'avoir soutenu jusqu'au bout et avoir su me motiver.

Sommaire

L'informatique joue un grand rôle dans la vie d'aujourd'hui. Les entreprises ont été amenées à remplacer les documents « papier » par des documents informatisés. Les individus veulent des supports de données d'une plus grande capacité pour stocker leurs photos, musiques et autres documents.

En effet, en dix ans, la capacité de stockage d'un disque dur, d'une carte mémoire ou d'une clé USB a été multipliée par 1000. On est passé d'un disque dur de 500 MB à 500 GB. Plus on a d'espace de stockage disponible plus on a de données sur un même support.

Ce travail a pour but de fournir des statistiques par rapport aux données récupérables à partir de disques durs hors-services, eux-mêmes récupérés dans différents endroits. Il n'est pas nécessaire de récupérer beaucoup de données pour retrouver des documents confidentielles ou personnelles.

Vous pourrez également découvrir le « Computer Forensics[1] » et comment fonctionne les outils d'analyses.

Pour étudier les disques durs récupérés, la méthode McKemmish a été utilisée. Cette méthode comprend les quatre étapes suivantes :

1. Identification
2. Préservation
3. Analyse
4. Présentation

Ce mémoire traite aussi les points importants pour ne pas éparpiller des données sensibles et comment bien se débarrasser des supports de données. Vous trouverez plusieurs solutions efficaces pour y parvenir.

Ce travail apportera aussi une sensibilisation aux dangers que peuvent engendrer le vol ou la perte de données confidentielles et comment s'assurer et se prémunir contre ces risques que ce soit pour vous ou pour votre entreprise.

[1] Correspond en français à informatique légale, cf. Glossaire

Table des matières

Liste des Graphiques

Liste des Figures

Introduction

Le marché de l'informatique et des technologies évolue continuellement très rapidement. Cela implique pour les entreprises de maintenir à jour leurs installations pour toujours être performantes et ne pas se laisser dépasser par la concurrence. Pour les particuliers, cela a moins d'incidence, cependant beaucoup de personnes renouvellent leurs matériel électronique seulement parce qu'un nouveau modèle est sorti sur le marché, et pour acquérir ce nouveau modèle, ces personnes sont amenées à vendre ou à recycler leurs anciens appareils.

C'est pourquoi ces dernières années, on a pu constater une grande évolution au niveau des ventes de matériels électronique d'occasions. Que ce soit dans des magasins spécialisés ou sur Internet via des sites d'enchères ou d'achat direct.

La conséquence est que les gens ne se rendent pas vraiment compte de ce qu'ils laissent comme trace dans ces appareils. En effet, dans la plus part des cas, il y a des informations personnelles et professionnelles qui peuvent être confidentielles ou simplement révéler des détails intimes.

De nos jours, l'informatique et la technologie sont de plus en plus présentes dans nos vies. La plupart des personnes possèdent un ordinateur à leur domicile, utilisent un téléphone portable doté d'un support de stockage, copient des données sur des clés USB, transmettent des emails avec des pièces jointes. Ceci montre qu'une énorme quantité de fichiers se déplacent chaque jour. Cependant si l'on égare sa clé USB, que l'on vende son ordinateur ou bien que l'on se trompe de destinataire dans un email, il est facile qu'une tierce personne puisse prendre possession de vos informations, confidentielles ou non.

C'est pourquoi il faut sensibiliser les gens aux dangers que peuvent apporter le vol d'informations confidentielles ou le vol d'identité, car le risque est important pour les entreprises qui ne veulent pas que des données sensibles tombent dans de mauvaises mains. De plus, la cybercriminalité[2] est très présente de nos jours, du vol d'identité en passant par la vente de données confidentielles à des concurrents.

Comme écrit ci-dessus, on trouve des supports de données dans la plupart des appareils électroniques. Il y en a dans les ordinateurs, portables ou de bureau, les téléphones mobiles, les clés USB, les consoles de jeux vidéo et les tablettes

[2] Notion large qui regroupe « toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique connecté à un réseau». Source : Wikipédia. Cf. Glossaire

électroniques entre autres. Tous ces objets sont susceptibles d'être revendus ou jetés à un moment ou à un autre pour différentes raisons. Mais ce qui est important c'est qu'il faut faire attention avant de s'en débarrasser.

Ce travail de Bachelor vous fournira des statistiques sur les données récupérées à partir de disques durs hors-service et démontrera ainsi l'importance de la façon de se débarrasser de ce genre de matériel.

Ce genre de travail est à même à être effectuer par la police scientifique, c'est pourquoi beaucoup d'allusion à ces derniers sont fait dans ce travail.

1. Principes et fonctionnement d'un disque dur

Je vais commencer par expliquer le fonctionnement d'un disque dur car il faut savoir comment un disque dur stocke les données pour comprendre comment un logiciel peut récupérer ces données.

Un disque dur est constitué de plusieurs plateaux, qui eux possèdent plusieurs pistes. Chaque piste contient des secteurs. La taille d'un secteur est au minimum de 512 octets.

Chaque secteur est composé de différentes informations :

- Le « Gap » : c'est une zone inutilisée qui laisse le temps nécessaire au changement de mode du disque dur (pour passer du mode lecture au mode écriture).
- La zone « Servo » : c'est une zone permettant la synchronisation entre la logique du contrôleur de disque et les données à lire.
- Une zone « En-tête » : elle contient les informations sur prochain secteur et elle permet d'identifier le numéro de secteur suivant.
- Une zone pour les données : c'est là que les données enregistrées sont stockées.
- Une zone « Checksum » : c'est une zone pour détecter et réparer les erreurs.

Ce qu'il faut retenir, c'est qu'un fichier n'est pas stocké sur un seul secteur. En effet, chaque fichier est reparti en bouts et chaque bout est placé dans un secteur. Le disque dur utilise donc un index pour connaître chaque secteur où est réparti le fichier. Cependant une fois les données supprimées, cet index l'est également. C'est pourquoi il est difficile de reconstruire un fichier effacé car il faut retrouver où chaque secteur était stocké.

2. Principe de l'effacement de données

Il faut également connaître et comprendre les différentes techniques d'effacement d'un disque dur car même après avoir effacé les données d'un disque il est possible de retrouver des informations.

1.1 Formatage

Formater signifie préparer le disque dur en installant un système de fichiers précis pour qu'il puisse être compatible avec le système d'exploitation utilisé car chaque système d'exploitation nécessite un système de fichiers différents. C'est pourquoi avant la première utilisation, il faut faire un formatage pour que le disque dur soit reconnu par le système d'exploitation. Il existe deux types de formatages :

1.1.1 Formatage de haut niveau

Le formatage de haut niveau a une incidence sur les informations liées au système d'exploitation. En effet, il ne s'occupe pas de la surface du disque mais d'effacer ou de réécrire l'index ou la table d'allocation.

1.1.2 Formatage de bas niveau

Le formatage de bas niveau est un formatage réalisé lors de sa fabrication. Il n'a aucune incidence sur le système d'exploitation. Un formatage de bas niveau est un peu comme remettre à zéro un disque dur car il initialise la surface du disque et ses pistes.

1.2 Touche Delete

La touche « Delete » est la touche présente sur tous les claviers d'ordinateurs. Elle sert à supprimer un fichier devenu inutile. Lorsque l'on appuie sur cette touche pour supprimer un fichier, ce dernier n'est pas supprimé à 100%. Il est placé dans la corbeille de l'ordinateur. Tant qu'un fichier se trouve dans la corbeille, il est toujours possible de le restaurer, c'est-à-dire de le récupérer si on en a besoin. Donc il est toujours indexé et l'espace utilisé par le fichier sur le disque n'est pas utilisable.

Par contre s'il l'on décide de vider la corbeille, l'espace alloué au fichier supprimé sera cette fois-ci réutilisable. Le fichier n'est plus atteignable par le système car il n'est plus indexé mais il sera toujours présent sur le disque (comme après un formatage de haut niveau). Par contre il occupe toujours les secteurs où il était stocké et donc récupérable via un logiciel spécialisé.

2. Pourquoi trouve-t-on toujours des données ?

Comme expliqué au point précédent, il existe plusieurs possibilités pour effacer des données d'un disque dur et elles ne sont pas toutes la même incidence sur le disque.

Le formatage ne supprime que l'index d'un fichier donc les données sont toujours présentes sur le disque mais ce dernier ne sait plus sur quels secteurs, il est donc dans l'impossibilité de lire ce fichier. Par contre, un programme spécialisé dans la récupération de donnée peut avec plus ou moins de succès reconstruire le fichier grâce aux informations que possède un secteur tel que la zone « En-tête » qui informe si c'est le début ou la fin du fichier et quels sont les secteurs suivants.

Comme décrit au point 1.1.1, lors d'un formatage de haut niveau, seul l'index ou la table d'allocation est effacé. C'est-à-dire que les données sont toujours présentes sur le disque dur mais plus indexé donc le système ne sait plus reconstruire le fichier pour le lire. Grâce à un logiciel spécialisé qui se sert d'un puissant algorithme, il arrive à reconstruire le fichier.

Figure 1 – Recherche de données
Source : www.tech2date.com

Evidemment il peut arriver que ce ne soit pas le cas. Premièrement car on a continué de travailler sur le disque et donc enregistré de nouveau fichier. Ces nouveaux fichiers sont alors stockés sur le disque dans différents secteurs. Si un de ces derniers contenaient une partie d'un fichier effacé, il sera dès lors très difficile pour un logiciel de reconstruire le fichier. Cependant certains programmes récupèrent le fichier mais il est illisible par le programme de lecture (par exemple Microsoft Word pour lire un fichier « doc »). Nous nous apercevrons dans la partie « Statistiques » qu'en effet beaucoup de fichier sont récupérés mais peu sont lisibles. Cela vient du fait que certains secteurs de fichiers ont été remplacés par d'autres.

Il existe tout de même des logiciels spécifiques capables de remplacer la partie manquante du fichier pour que les parties récupérées puissent quand même être visibles. Par contre ce travail ne traite en aucun cas ce sujet-là.

3. Recherche et récupération de matériel à analyser

3.1 Récupération du matériel pour le travail de diplôme

3.1.1 Auprès d'entreprises de recyclage

Pour pouvoir effectuer des analyses de disques durs dans des conditions réelles il me fallait donc trouver des disques durs hors-service. Les conditions réelles sont nécessaires pour que les statistiques des données récupérées ne soient pas faussées.

Donc ma première idée était de demander des disques durs auprès d'entreprises de recyclages de matériel informatique. J'ai réussi à trouver trois entreprises qui s'occupent de recycler des disques durs.

La première entreprise est Réalise, une entreprise d'insertion, qui récupère du matériel informatique pour le remettre en état de marche et ainsi le revendre d'occasion. Cependant lors de ma visite dans leurs bureaux le 2 novembre 2011, les responsables m'ont indiqué qu'aucun matériel fournit par des clients ne pouvait être fournis à une tierce personne par soucis de confidentialité vis-à-vis de leurs clients. Malgré une proposition de clause de confidentialité de ma part, je n'ai eu aucun succès.

La deuxième entreprise à laquelle j'ai pensé est l'espace de récupération du Nant de Châtillon. Ici aussi j'ai également été confronté à un problème car le tri des matériaux est très strict et tout matériel entré, ne peut ressortir. Malgré que je m'attende un résultat identique, j'ai quand même décidé de me rendre dans les centres de voirie de plusieurs communes genevoises pour essayer de récupérer des disques durs. Je leur ai également demandé si je pouvais emprunter du matériel et le ramener après analyse, mais par soucis que le matériel ne finisse pas à nouveau dans la rue, les centres de voirie ne laissent non plus rien ressortir.

La troisième entreprise de recyclage de matériel informatique est Katana. C'est une entreprise genevoise qui fournit un service de destruction de disques durs. J'ai découvert cette entreprise grâce à un article du journal L'Express parue le 23 novembre 2011. Seulement c'est une entreprise de destruction qui offre une garantie de 100% de réussite à leurs clients donc impossible de récolter du matériel à analyser.

Figure 2 – Katana Logo
Source : www.katana.ch

3.1.2 Auprès d'entreprises

Vu les résultats de mes recherches auprès d'entreprises de recyclage de matériel informatique, j'ai décidé de faire du démarchage directement auprès d'entreprises pour savoir s'ils étaient d'accord de me donner ou prêter des disques durs hors-service.

J'ai donc expliqué ma demande et le sujet de mon travail de diplôme à plusieurs de mes contacts dans diverses entreprises, et j'ai réussi à me procurer six disques durs.

3.1.3 Dans la rue

Comme vous l'aurez déjà remarqué dans nos rues, beaucoup de personnes y déposent leurs déchets lors de déménagement ou tout simplement pour se débarrasser de choses encombrantes. On y trouve souvent du matériel informatique. C'est pourquoi je me suis dit qu'il fallait que j'y porte attention. J'ai également demandé à mon entourage de regarder et me dire s'ils voyaient des ordinateurs dans la rue. Cette démarche a porté ses fruits puisque grâce à cela j'ai réussi à récupérer quatre autres disques durs.

3.1.4 Total

Portant le total à dix disques durs, une durée de deux mois à quand même été nécessaire pour les regrouper.

3.2 Récupération du matériel lors d'investigation

Lors d'investigation menée par la police scientifique, d'autres types de matériel peuvent être récupérés. Car de nos jours la plus part des appareils électroniques possèdent un disque dur ou un espace de stockage. C'est pourquoi il faut être attentif à ne rien oublier car des données sensibles ou importantes peuvent être récupérées sur le type de matériel suivant :

- Ordinateur
- CD-ROM
- DVD-ROM
- Disquette
- Clé USB
- Téléphone portable / Smartphone
- Carte mémoire
- Lecteur MP3
- Console de jeux vidéo
- Imprimante
- Appareil d'interconnexion

4. Mise en place des ressources nécessaires

4.1 Installation de mon espace de travail

Après avoir récupéré les disques durs, il faut faire une copie-image[3] du disque dur sur un disque dur vierge. C'est pourquoi il me fallait un disque dur vierge qui m'a été fourni généreusement par Monsieur David BILLARD. Par la suite, il m'a fallu un deuxième disque dur que j'ai demandé à Monsieur Gérard INEICHEN, responsable du centre informatique de la HEG.

Monsieur BILLARD et la HEG m'ont permis de travailler et d'utiliser le matériel à disposition dans une salle de l'école pour que je puisse effectuer mon travail de diplôme avec les meilleurs outils possibles. Un des outils nécessaires à mon travail est le duplicateur de disque dur.

Image MASSter Solo III Forensics :

Cet appareil est destiné à dupliquer des disques durs. Il a été mis à disposition par Monsieur David BILLARD. Il est nécessaire pour faire une copie-image d'un

[3] Terme adapté de l'anglais « forensic copy », l'expression « *copie-image* » représente une copie bit à bit intégrale de *l'information numérique* présente sur un *support d'information*, y compris espaces non utilisés, espaces non alloués et queues de clusters, effectuée à l'aide d'un logiciel spécifique. Source : Wikipédia. Cf. Glossaire

disque dur récupéré sur un disque dur vierge pour éviter de travailler directement sur le disque dur récupéré car si on effectue une mauvaise opération par exemple en supprimant des données qui seraient impossibles à récupérer, il suffit de refaire une copie. Cette machine duplique exactement le disque dur dans l'état où il est. Elle copie aussi l'espace libre. Elle duplique la mémoire bit par bit.

4.2 Logiciels de récupération de données

Les logiciels présentés ci-dessous seront utilisés dans le but d'analyser les disques durs récupérés et ainsi trouver les données toujours disponibles ou les données effacées.

4.2.1 FTK Imager

Forensic Toolkit Imager est un logiciel développé par la société Access Data. C'est un logiciel d'analyse forensique[4] gratuit. La version que j'ai utilisée est la 3.1.0.

Ce logiciel permet de monter une copie-image et ainsi pouvoir regarder son contenu actuel. Il offre également la possibilité de pouvoir retrouver des données effacées mais seulement si le disque n'a pas été formaté.

Il est disponible à l'adresse suivante :
http://accessdata.com/support/adownloads

4.2.2 RescuePRO

RescuePRO est un logiciel développé par San Disk. Il permet de récupérer des données depuis différents supports de données tels que clé USB, carte mémoire, disque dur mais également copie-image ce qui est très important dans mon cas.

Lors d'un achat de carte mémoire SD, j'ai eu droit à une licence gratuite d'une année car ce logiciel est normalement disponible pour $ 40.00. J'ai utilisé la version 3.5.0. Une version d'essai est disponible à l'adresse ci-dessous mais permet seulement d'analyser et d'afficher les données :

http://www.lc-tech.com/rescuepro/

[4] Applique une démarche scientifique et des méthodes techniques dans l'étude des traces qui prennent leur origine dans une activité criminelle, ou litigieuse en matière civile, réglementaire ou administrative. Source : Wikipédia. Cf. Glossaire

4.2.3 X-Ways Forensics

X-Ways Forensics est un logiciel développé par X-Ways Software Technology. C'est un outil à la pointe de la technologie forensique. Il est spécialement utilisé par les experts en informatique judiciaire. Il permet de récupérer des données très rapidement.

Figure 3 - X-Ways Logo
Source : www.riskdrivesion.com

J'ai utilisé la version 13.0 qui a été mise à disposition par Monsieur David BILLARD.

Ce logiciel n'est pas disponible en téléchargement. Il est, comme mentionnée ci-dessus, réservé aux spécialistes.

4.2.4 Recuva

J'ai également décidé d'utiliser ce logiciel car lorsque l'on tape sur « Google » : Logiciel de récupération de données, c'est parmi de nombreux logiciels gratuits celui qui ressort le plus. C'est pourquoi j'ai pensé que les statistiques seraient plus intéressantes avec un logiciel qu'un utilisateur lambda est susceptible d'utiliser lorsqu'il veut récupérer un fichier effacé.

Figure 4 - Recuva Logo
Source : baltagy.blogspot.com

Recuva est un logiciel développé par Piriform Ltd. C'est un logiciel gratuit de récupération de données. J'ai utilisé la version 1.42.

Il est disponible gratuitement à l'adresse suivante :

http://www.piriform.com/recuva

4.2.5 Net Analysis

Net Analysis est un logiciel développé par Digital Detective. Ce programme est destiné à analyser l'historique de la navigation Internet. Pour cela, il faut, auparavant, avoir récupérer des fichiers spécifiques où sont stockées les données de navigation. Je vous fournirai plus de détails dans le chapitre dédié à ce sujet.

Ce logiciel n'est pas disponible gratuitement, cependant une version démo est téléchargeable. La version démo (30 jours) rempli entièrement les exigences pour effectuer ce travail. J'ai utilisé la version 1.53.

Disponible à l'adresse ci-dessous :

http://www.digital-detective.co.uk/downloads.asp

5. Procédure forensique

Pour ce travail j'ai choisi d'utiliser le modèle McKemmish qui m'a été enseignée durant mon cursus à la HEG par Monsieur David BILLARD. Ce modèle est utilisé par les experts en informatique légale[5].

Il y a quatre étapes :

1. Identification
2. Préservation
3. Analyse
4. Présentation

Chaque étape est décrite ci-dessous :

5.1 Identification

Dans la première étape, il s'agit d'identifier le matériel saisi qui peut contenir des indices et des preuves numériques[6]. Dans mon cas, il s'agit d'identifier les disques durs récupérés.

Voici la liste des disques durs récupéré :

Nom de copie : FIRSTEC1

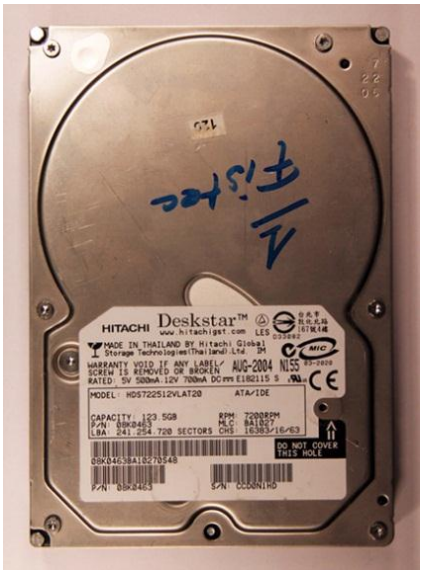
Marque : HITACHI

Modèle : HDS722512VLAT20

Numéro de série : CCD0N1HD

Capacité : 123.5 GB

Technologie : IDE



[5] On désigne par informatique légale ou investigation numérique légale l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques. Source : Wikipédia. Cf. Glossaire

[6] Représente toute *information numérique pouvant être utilisée comme preuve dans une affaire de type judiciaire.* Source : Wikipédia. Cf. Glossaire

Nom de copie : FIRSTEC2

Marque : SAMSUNG

Modèle : SHD-30560A

Numéro de série : J1QF723405

Capacité : 560 MB

Technologie : IDE

Nom de copie : FIRSTEC3

Marque : WESTERN DIGITAL

Modèle : WD400

Numéro de série : WMAC51058061

Capacité : 40.0 GB

Technologie : IDE

Nom de copie : DIPLOME

Marque : SAMSUNG

Modèle : SV0322A

Numéro de série : J46JB15653A

Capacité : 3.2 GB

Technologie : IDE

Nom de copie : DISKKEY

Marque : HITACHI

Modèle : IC25N040ATCS04-0

Numéro de série : NDDJUBV4B

Capacité : 40.0 GB

Technologie : IDE

Nom de copie : DISK6

Marque : HITACHI

Modèle : HDS728080PLAT20

Numéro de série : S2RWS70D

Capacité : 82.3 GB

Technologie : IDE

Nom de copie : DISK7

Marque : Maxtor

Modèle : 90871U2

Numéro de série : E20PJBWC

Capacité : 8.4 GB

Technologie : IDE

Nom de copie : DISK8

Marque : Maxtor

Modèle : DiamondMax Plus 9

Numéro de série : Y2B14YME

Capacité : 80.0 GB

Technologie : IDE

Nom de copie : DISK9

Marque : Seagate

Modèle : Barracuda 7200.7

Numéro de série : 5JVC3JB6

Capacité : 80.0 GB

Technologie : IDE

Nom de copie : DISK10

Marque : Maxtor

Modèle : D740X-6L

Numéro de série : VQ20A011-01-B

Capacité : 20.0 GB

Technologie : IDE

5.2 Préservation

La préservation est la deuxième étape de la méthode. Le but est de faire une copie du support de données sur un support vierge. Cela permet de garder intacte le support original et ainsi en cas de besoin pouvoir le copier une seconde fois pour que l'analyse soit toujours la même. Il ne faut en aucun cas que la preuve ne soit corrompue, c'est-à-dire qu'elle subisse des modifications après la saisie.

Il faut donc au préalable faire une copie du disque dur. Pour ce travail, j'ai utilisé l'appareil appelé « duplicateur de disque dur », l'Image MASSter Solo III Forensics, présenté au point 4.1

Pour réaliser cette opération, nous avons besoin d'un disque dur vierge qui accueillera la copie. Le terme utilisé pour nommer ce disque est « Evidence Drive ». Il est branché sur le duplicateur de disque dur. Ensuite, il faut brancher le disque que nous souhaitons copier, appelé « Suspect Drive », au duplicateur. Ce dernier est lui relié à une alimentation externe.

La copie une fois copiée le « Evidence Drive » est protégée en écriture, c'est-à-dire qu'aucune donnée ne peut être écrite, modifiée ou supprimée. Cela évite toute mauvaise manipulation qui modifierait la preuve numérique.

Effectuer cette copie, permet de s'assurer qu'une preuve qui peut être trouvée lors de l'analyse, peut être retrouvée par une autre personne si la cours de justice demande une contre-expertise.

Les deux disques durs « Evidence Drive » utilisés pour recevoir les copies des dix disques « Suspect Drive » sont :

Nom de copie :	EVIDENCE DRIVE 1
Marque :	SAMSUNG
Modèle :	HD502HJ
Numéro de série :	S20BJA0ZA41299
Capacité :	500.0 GB
Technologie :	SATA
Contient :	FIRSTEC1, FIRSTEC2, FIRSTEC3, DISK6, DISK7, DISK8, DISK10, DIPLOME

Nom de copie :	EVIDENCE DRIVE 2
Marque :	Seagate
Modèle :	Barracuda 7200.9
Numéro de série :	5LSGE8JC
Capacité :	160.0 GB
Technologie :	SATA
Contient :	DISK9, DISKKEY

Une fois les branchements effectués, nous allumons l'appareil. Après mise en marche, nous vérifions les informations du disque dur en cliquant sur « Drive Info ». Cela nous permet de nous assurer que le disque dur est bien reconnu par la machine.

Nous pouvons maintenant lancer la copie du disque et cliquant sur « Run ». L'appareil va nous demander de confirmer la copie de « Suspect Drive to Evidence Drive ». C'est effectivement ce que nous voulons donc on valide. Ensuite on va devoir donner un nom à la copie du disque car le disque « Evidence Drive » peut contenir plusieurs copies d'autres disques durs.

Une fois toutes les informations récoltées, le duplicateur va :

1. Mettre en marche les disques durs
2. Identifier les disques durs
3. Copier le « Suspect Drive » sur le « Evidence Drive »

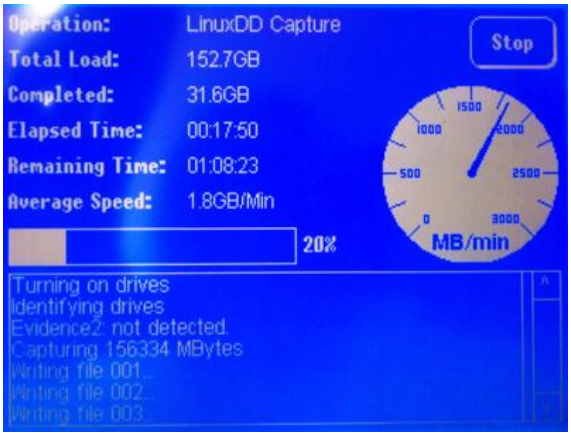


Figure 5 - Image MASSter Solo III Forensics

Lors de cette étape, on peut observer différentes informations telles que :

- L'opération qui est en train d'être effectuée
- La taille du disque à copier « Total Load »
- Les nombres de données déjà copiées « Completed »
- Le temps écoulé « Elapsed Time »
- Le temps restant « Remaining Time »
- La vitesse moyenne de copie « Average Speed »
- Le pourcentage effectué

Il faut répéter cette opération pour chaque disque dur que vous voulez copier. J'ai donc réalisé cette étape dix fois.

La durée de la copie d'un disque dépend de sa capacité et de la vitesse à laquelle il peut travailler. Un disque récent sera plus rapide à copier qu'un disque ancien. Pour les dix disques que j'ai copiés, le temps moyen de copie est d'environ deux heures par disque.

Une fois les copies terminées, il faut brancher le disque dur qui contient les copies c'est-à-dire « Evidence Drive » sur un ordinateur pour pouvoir l'analyser.

Le temps moyen de copie d'un disque de 120 GB est d'environ deux heures.

5.3 Analyse

La troisième étape consiste à analyser chaque disque dur avec différentes méthodes et à l'aide de plusieurs logiciels. Un expert en informatique légale utilisera cette phase pour trouver des preuves numériques contre un suspect. Dans mon cas, cette étape me permet de réunir les fichiers récupérables sur les disques afin d'établir des statistiques selon le type de fic hier et son contenu.

Figure 6 – Preuve numérique
Source : www.howtobecomealocksmith.org

5.3.1 Récupération de données

5.3.1.1 Sans logiciel

L'analyse la plus simple est de vérifier si le disque dur contient encore des données accessibles via l'explorateur Windows (données non-supprimées). Il faut quand même utiliser un logiciel pour cette étape car l'explorateur Windows ne sait pas lire une copie-image d'un disque dur. Il faut donc monter la copie-image à l'aide d'un logiciel approprié. J'ai utilisé le programme "FTK Imager". Lorsque la copie-image est montée, elle apparait comme un disque dur qui serait connecté à l'ordinateur alors qu'il est que virtuel.

5.3.1.2 FTK Imager

Le premier logiciel dont je me suis servi pour analyser est FKT Imager. Ce logiciel permet de retrouver des données qui auraient été effacées, seulement si le support de données n'a pas été formaté. Ce programme est capable de lire une image de disque dur comme si c'était un vrai disque dur.

Voilà comment fonctionne le programme :

Pour commencer il faut monter l'image : « File » puis « Image Mounting ». Il faut sélectionner une image en cliquant sur « … » puis sur « Mount » pour valider. Ensuite pour afficher le disque : « File » puis « Add Evidence Item… ». On sélectionne « Physical Drive » puis on sélectionne le disque dur que l'on vient de monter et « Finish ».

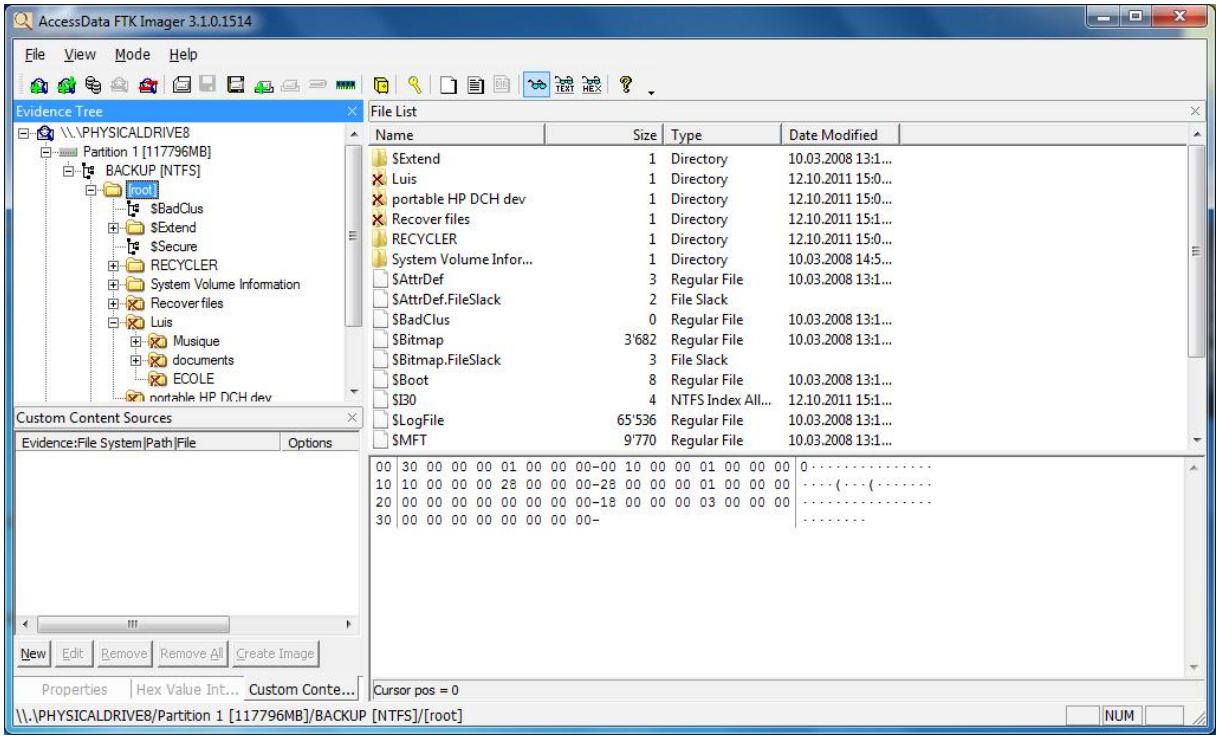


Figure 7 – Capture d'écran de FTK Imager

5.3.1.3 RescuePRO

Le deuxième programme est RescuePRO. Logiciel très simple d'utilisation, il est capable de lire une copie-image de disque dur. Il suffit de sélectionner le type de données que l'on désire retrouver et de choisir sur quel support. Ensuite le programme fait le reste.

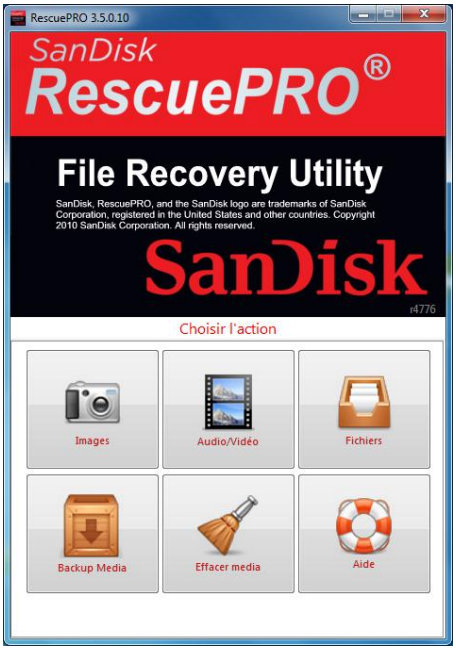


Figure 8

Capture d'écran de RescuePRO 1

Pour mon analyse j'ai choisi de récupérer tous types de fichiers car je désirais retrouver des documents en plus des images et fichiers audio et vidéo. Donc on sélectionne « Fichiers », puis on choisit « Fichier d'Images Media ». Une fois l'image sélectionnée, on clique sur « Commence ».

Temps de récupération par disque varie entre 2 et 180 minutes.
Le temps moyen est d'environ une heure

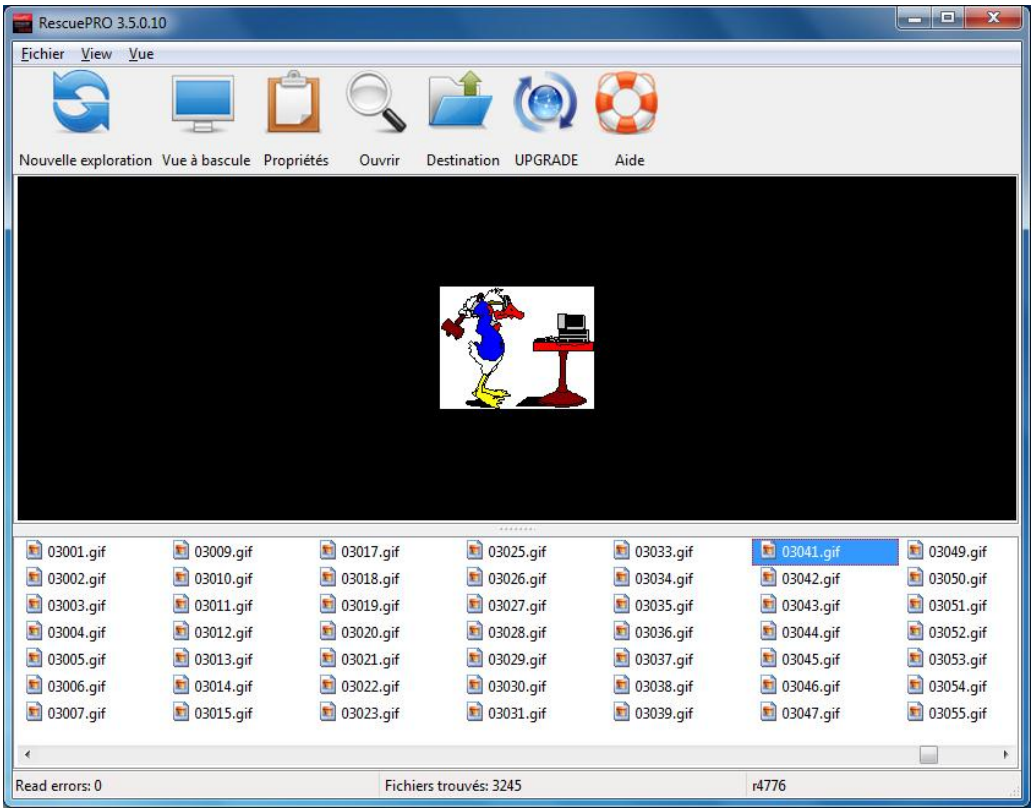


Figure 9 – Capture d'écran de RescuePRO 2

5.3.1.4 Recuva

Logiciel également très simple d'utilisation, il est destiné au grand public désireux de retrouver des fichiers effacés par mégarde. Comme pour le programme précédent, on sélectionne le type de données à rechercher et sur quel support.

Par contre ce logiciel n'est pas capable de lire une copie-image. Il faut donc monter la copie-image grâce à FTK Imager. On sélectionne le type de documents que l'on désire récupérer. Il n'est pas possible de choisir deux types en même temps. Il faut donc répéter l'étape de récupération autant de fois qu'il y a de types de données à récupérer. On choisit par exemple « Images » puis on clique sur « Suivant ». On sélectionne « Dans un emplacement spécifique » et on choisit le disque virtuel qu'on a monté auparavant. Pour un meilleur résultat, je conseille d'activer la checkbox « Activer l'analyse approfondie » puis « Démarrer.

Le temps de récupération par disque varie entre 5 et 180 minutes. Le temps moyen est d'un peu plus d'une heure.

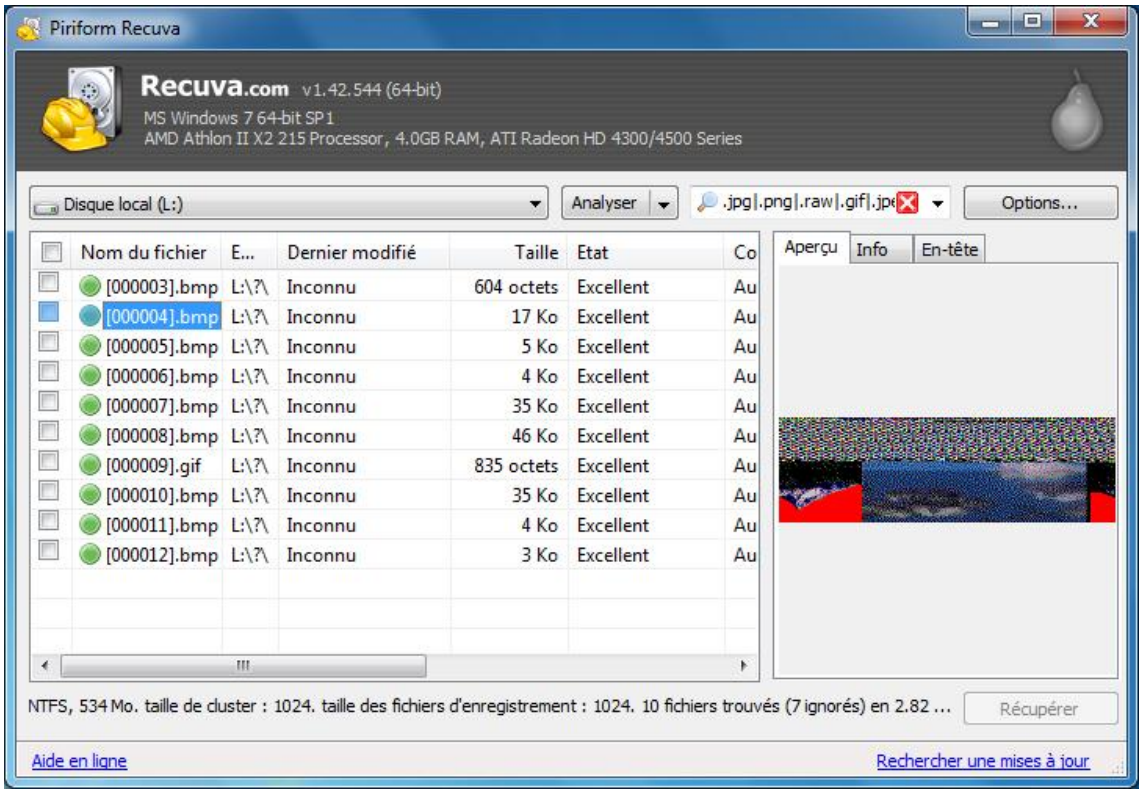


Figure 10 – Capture d'écran de Recuva

5.3.1.5 X-Ways Forensics

Ce dernier logiciel est plus compliqué d'utilisation car il offre beaucoup plus de possibilités à son utilisateur, il est uniquement destiné aux spécialistes du métier d'expert en informatique légale. Ce programme est aussi capable de travailler sur la mémoire virtuelle.

Pour commencer il faut créer un nouveau cas. Pour cela cliquer sur « File » dans la fenêtre « Case Data », puis « Create New Case ». On donne un nom au cas et on valide avec « OK ». Une fois le nouveau cas créé, on sélectionne à nouveau « File » dans la fenêtre « Case Data » puis on va ajouter une image d'un disque pour l'analyser, « Add Image… ». On sélectionne l'image et on valide avec « Ouvrir ». Pour que l'on puisse analyser tout le disque, il faut ajouter toutes les partitions : on clique sur « Access » puis « Add All Partitions To Case ». Pour lancer l'analyse il faut cliquer sur « Specialist » dans la barre des menus. Puis sur « Refine Volume Snapshot… ». Ici on lui indique qu'on désire faire une nouvelle capture des données en validant la checkbox « Take new one ».

Le temps de récupération varie entre 5 et 40 minutes. Le temps moyen est de 20 minutes. Il est nettement le plus rapide.

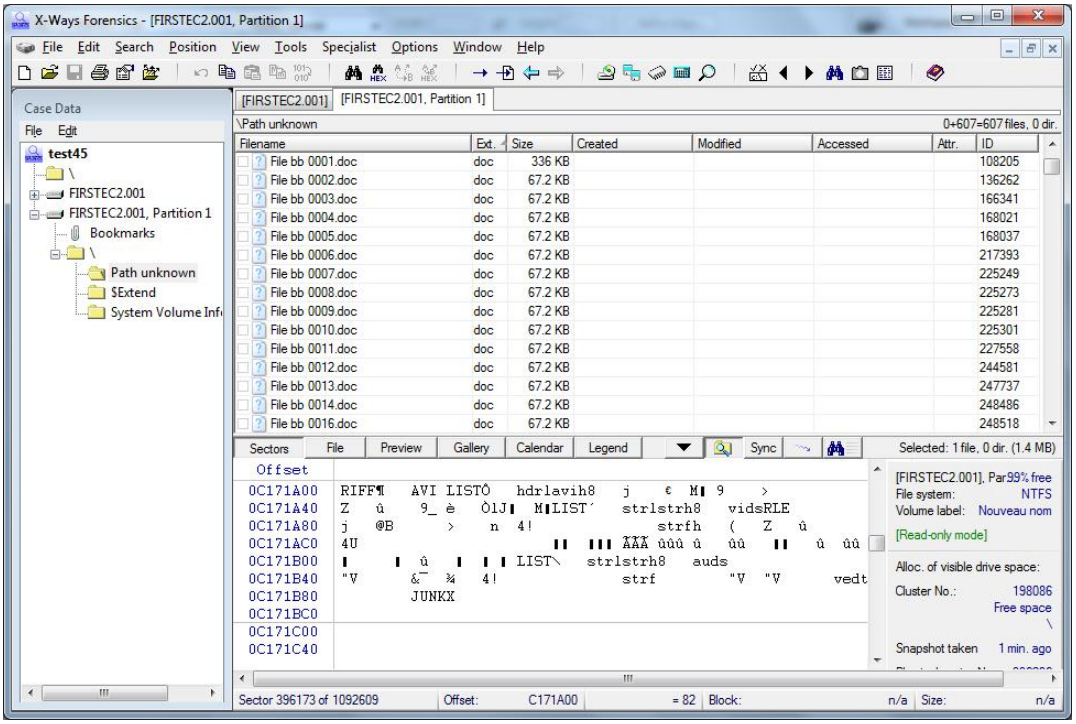


Figure 11 – Capture d'écran de X-Ways Forensics

On lui indique également qu'il doit effectuer une recherche approfondi en validant « Particularly thorough file system structure search » et aussi « File header signature search » pour qu'il recherche les signatures des en-têtes de fichier.

Une fois validé, on doit choisir le type de fichier que l'on désire rechercher. Ici il est possible d'en sélectionner plusieurs. On peut également définir une taille maximum des fichiers à retrouver. On valide avec « OK » et la recherche est lancée ! Les fichiers récupérés apparaitront dans le dossier « Path unknown ».

5.3.1.6 Net Analysis

Grâce à ce logiciel, on peut analyser les données de navigation Internet effectuées par l'utilisateur. Les principales données que l'on peut récolter avec ce programme sont :

- Les sites fréquentés par l'utilisateur
- Les cookies[7]

Pour pouvoir afficher ces informations dans le logiciel, il faut récupérer des fichiers nommés « index.dat ». Il suffit ensuite d'ouvrir le fichier désiré dans le programme.

[7] En informatique, un cookie est défini par le protocole de communication HTTP comme étant une suite d'informations envoyée par un serveur HTTP à un client HTTP. Source : Wikipédia Cf. Glossaire

5.3.2 Trie des données

5.3.2.1 Quels types de fichiers sont importants ou sensibles ?

Premièrement il faut faire un choix des fichiers à analyser. C'est-à-dire faire une sélection de types de fichiers à étudier tels que les documents Microsoft Office, les images, les emails, les fichiers Internet, etc.

On pourrait répondre tous car lorsqu'une personne vole l'identité d'une autre, elle a besoin de connaître un maximum de chose à propos de la personne dont l'identité a été volée pour pouvoir paraitre crédible.

Sinon sans parler de vol d'identité les fichiers les plus sensibles sont :

- Emails
- Documents confidentiels
- Photos
- Cookies/fichiers Internet
- Fichiers audio

Ces fichiers sont sensibles car ce sont des documents personnels ou professionnels qui ne sont pas destinés à être publiés ou même consultés par une tierce personne.

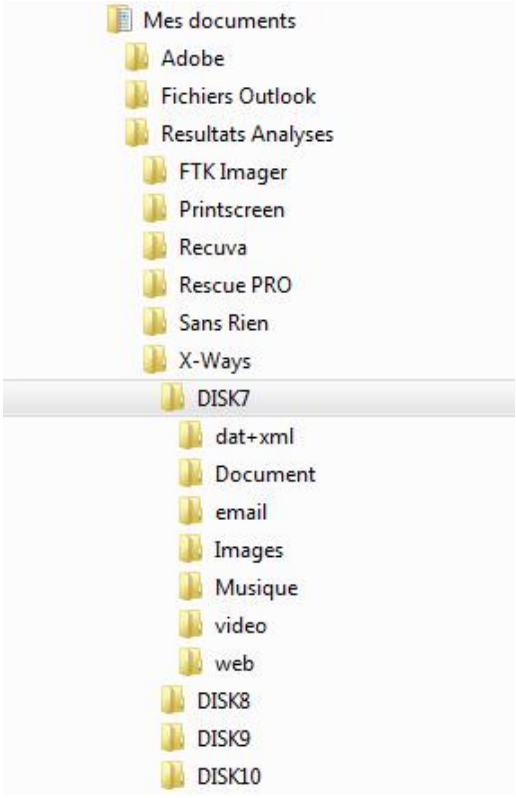


Figure 12
Hiérarchie pour le tri des données

Comme expliqué au point précédent, certains logiciels proposent de retrouver des types de fichiers bien précis ce qui évite de devoir trier une multitude de répertoires. Tous ne proposent pas ce service, il faut donc commencer par trier les différents types de fichiers un par un. Grâce à l'explorateur Windows, on peut trier un dossier par types de fichiers. Il suffit ainsi de ne garder que les fichiers dont le type nous intéresse.

5.3.2.2 Différencier données professionnelles et personnelles

Ce point a nécessité beaucoup de temps car sur chaque disque dur analysé, une importante quantité de fichiers a été récupérées. Donc pour pouvoir différencier données les données professionnelles des données personnelles, il faut étudier fichier par fichier.

Images

Pour analyser des images, j'ai déjà commencé par afficher les photos en tant que grandes icônes dans le dossier. Ainsi on arrive à voir quels fichiers sont lisibles et lesquels ne le sont pas. Ensuite lorsque l'on a séparé les fichiers lisibles des illisibles, on peut définir si l'image est d'origine personnelle ou professionnelle. Pour décider qu'une photo était de type professionnel ou personnel, c'est avant tout une déduction en rapport à ce qui est représenté sur l'image.

Musique

Pour savoir si un fichier audio est lisible, il suffit de le lire avec un lecteur de musique. Pour tester une grande quantité, j'ai chargé la totalité des fichiers retrouvés (par disque) dans Windows Media Player. Dès qu'un fichier est illisible, le programme affiche un message d'erreur. Il suffit de lire chaque fichier en avance rapide pour connaître quels fichiers sont lisibles et lesquels ne le sont pas.

Pour différencier fichier professionnel et personnel, il suffit d'écouter les intro de chaque morceau et définir s'il s'agit de musique ou d'un enregistrement professionnel.

Vidéos

Comme pour les images, pour savoir si un fichier est lisible ou non, on peut commencer par les afficher en tant que grandes icônes. Si un aperçu est disponible cela signifie généralement que le fichier est bon. Cependant j'ai également essayé de lire les vidéos car très peu de fichiers de ce type ont été retrouvés. Comme pour les images, le choix "professionnel" ou "personnel" reste intuitif.

Documents

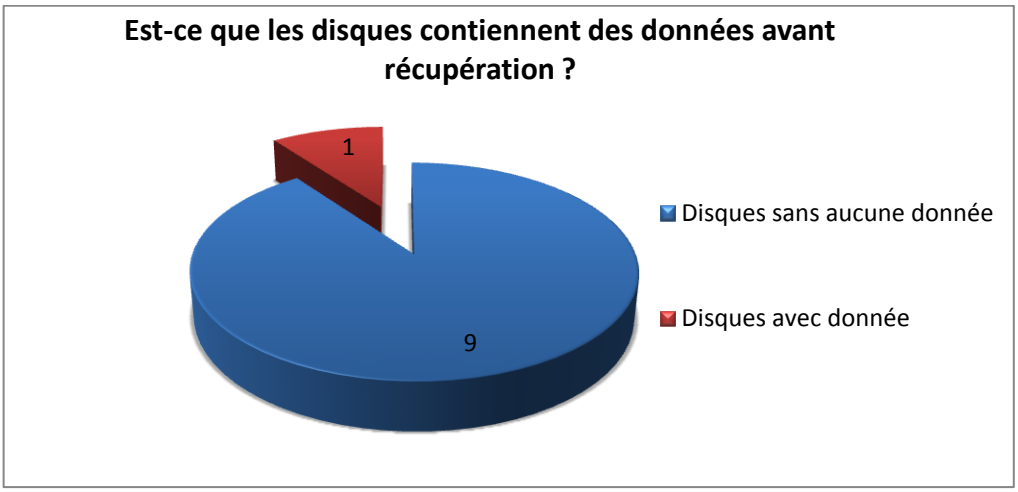
Cela devient plus ardu d'analyser les documents (MS Office ou PDF) car on n'a pas forcément un aperçu du document pour premièrement savoir s'il est lisible. La seule solution est d'ouvrir les fichiers et ainsi valider leur lecture puis définir de quels types (professionnel ou personnel) sont les données contenues. De plus, on ne peut pas ouvrir tous les fichiers d'un coup car la mémoire de l'ordinateur ne supporterait pas. Il faut donc prendre son mal en patience et étudier les fichiers les uns après les autres.

La plupart des fichiers professionnels possèdent un logo de l'entreprise, une mise en page spécifique et des titres que l'on ne retrouve pas dans des documents personnels comme par exemple « Processus de validation » ou "plan d'opération" etc. Il est donc relativement facile d'établir qu'il s'agit bien de données professionnelles.

5.4 Présentation

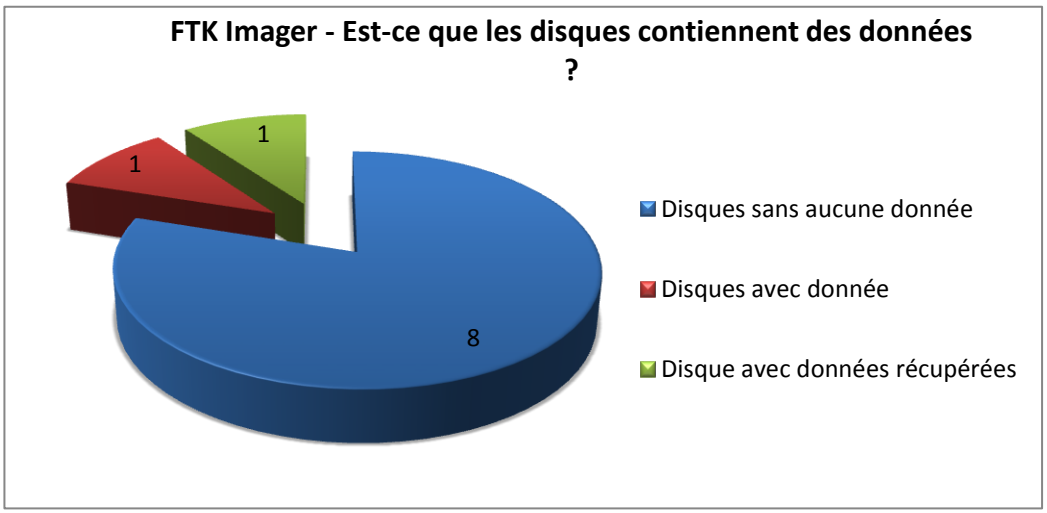
Cette quatrième et dernière étape permet de présenter les résultats de l'analyse afin qu'elles soient compréhensibles par des personnes non-spécialistes.

Sur ce graphique, on remarque que 9 disques sur 10 ne possèdent aucune donnée stockée. Cela signifie que les données ont au moins été effacées d'une manière simple (formatage ou touche « delete »). Seulement 5 images étaient stockées sur le disque « DISK10 ». Ces images sont de type personnel.



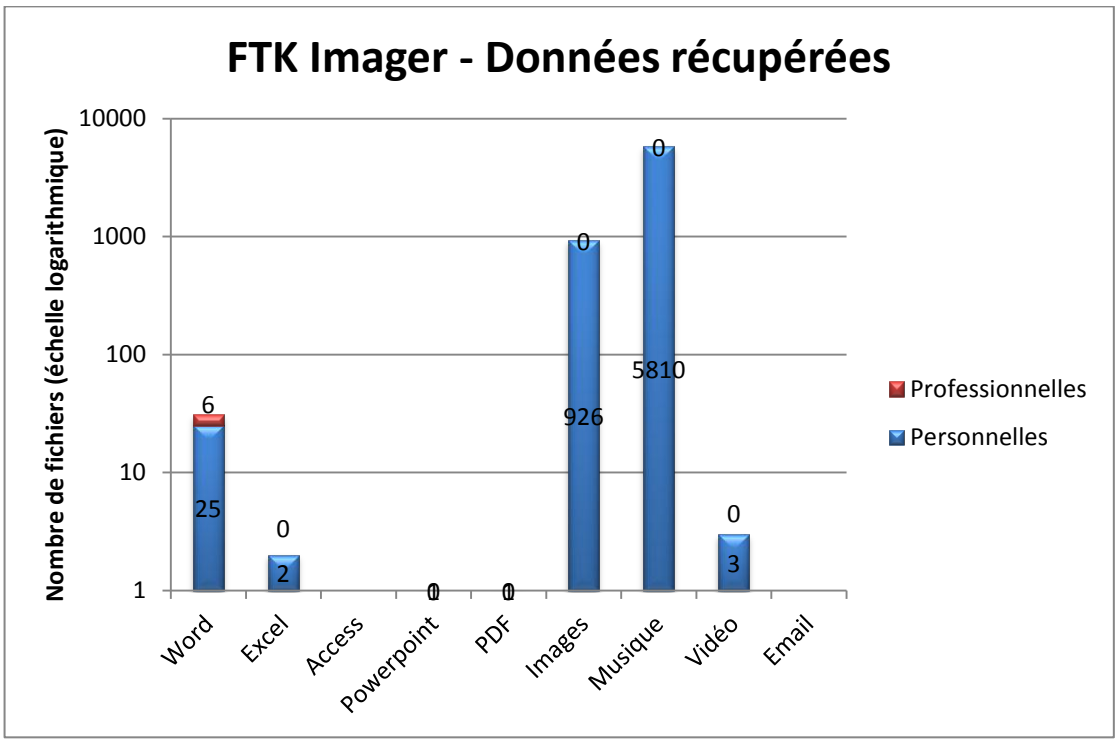
Graphique 1 - Est-ce que les disques contiennent des données avant récupération ?

Sur ce graphique, on remarque qu'en plus des données du disque « DISK10 », on retrouve avec FTK Imager des données sur un autre disque. Cela signifie que les données ont été supprimées avec la touche « Delete » car le programme ne retrouve pas de donnée après formatage. Je suppose donc que 8 disques sur 10 ont été formatés.



Graphique 2 – FTK Imager – Est-ce que les disques contiennent des données ?

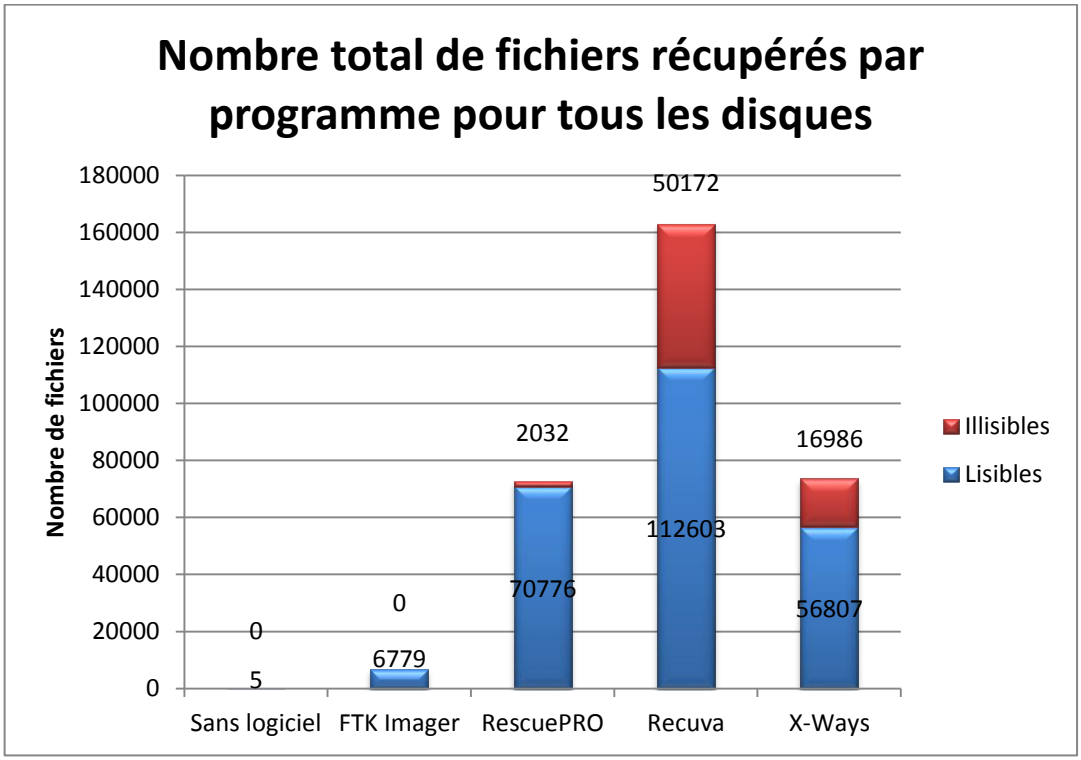
Voici plus de détails sur les données récupérées avec FTK Imager sur le seul disque où se trouvaient des fichiers :



Graphique 3 – FKT Imager – Données récupérées

La totalité des fichiers récupérés sont lisibles. On remarque que seulement 4 documents « Word » sont des données professionnelles, le reste étant personnelles. Au niveau des données personnelles, la plus part des documents sont des lettres de motivation, des curriculums vitae. Par contre le « PDF » récupéré est une déclaration fiscale. Sinon les images et la musique retrouvées sont des fichiers personnels. Les dates de modification des fichiers vont de 2004 à 2007.

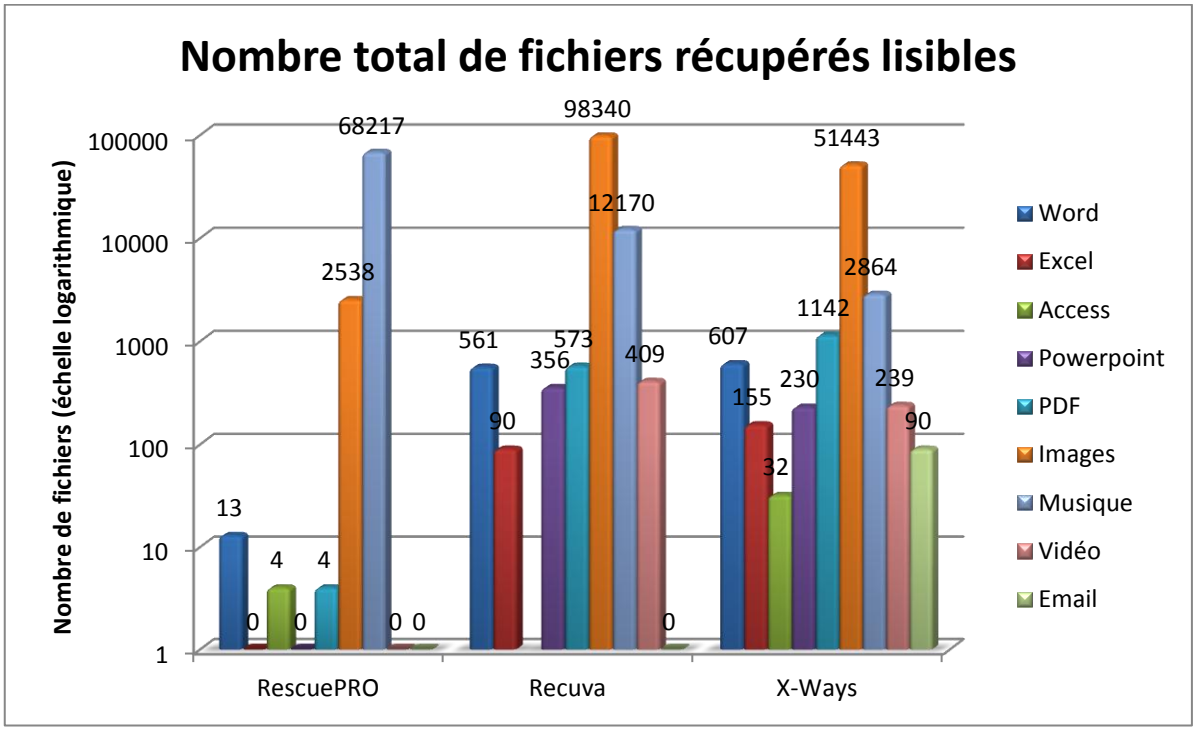
Ce graphique représente la totalité des fichiers récupérés (lisibles et illisibles), regroupés par logiciels utilisés (pour tous les disques). On remarque que pour chaque logiciel, environ 70% des fichiers sont lisibles. Cela démontre les bonnes performances des programmes utilisés.



Graphique 4 – Nombre total de fichiers récupérés par programme pour tous les disques

Ce graphique représente chaque type de fichiers lisibles récupérés par logiciel. On remarque que la majorité des fichiers récupérés sont des images et de la musique. Cela se traduit par le fait que la plus part des personnes stocke leurs photos numériques sur leurs ordinateurs et téléchargent aussi beaucoup de musique par Internet. De plus, beaucoup d'images proviennent de la navigation Internet.

Je constate que le nombre de musique récupéré avec X-Ways (2864) est inférieur au nombre de fichiers musicaux retrouvés avec FTK Imager (5810). J'aurais plutôt imaginé retrouver au minimum le même nombre de pistes audio mais ce n'est pas le cas.

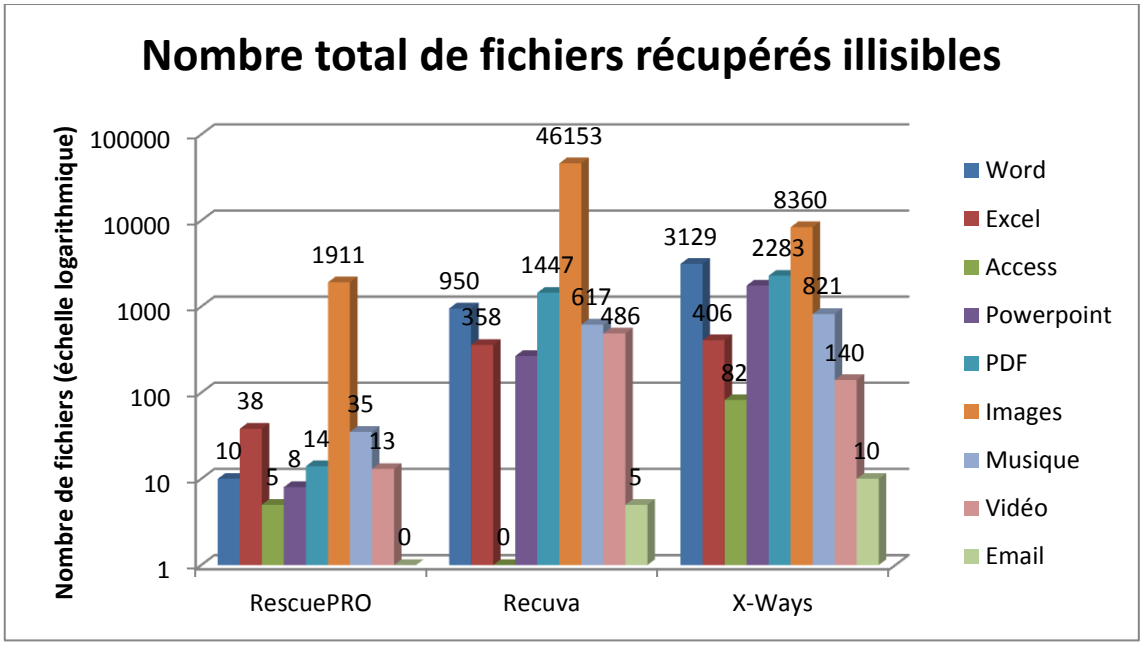


Graphique 5 – Nombre total de fichiers récupérés lisibles

Ce graphique représente chaque type de fichiers illisibles récupérés par logiciel. On remarque qu'avec RescuePRO, on récupère plus de fichiers illisibles que lisibles.

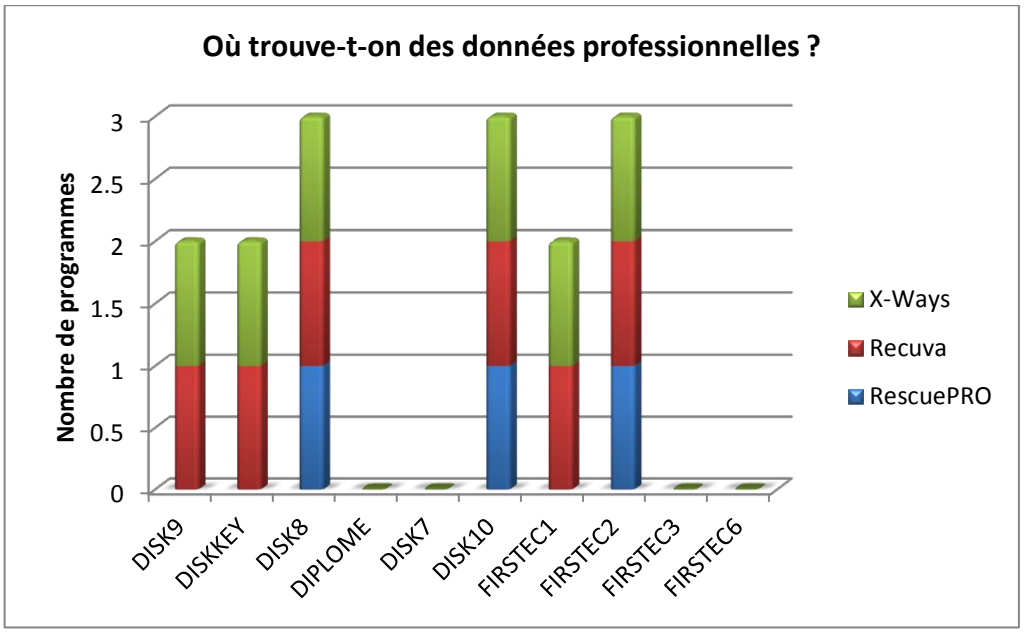
La totalité des emails retrouvée est très faible. Ma supposition est que de nos jours la plus part des entreprises utilisent les emails sur le réseau interne et ne sont donc pas sauvegardés sur le disque dur de la machine. De plus, les messageries emails permettent la sauvegarde en ligne de ce genre de documents.

Très peu de vidéos ont été récupérées. Je suppose que, premièrement, cela vient du fait que peu d'entreprises travaillent avec des vidéos et deuxièmement que généralement ce genre de fichier est très volumineux. En effet, plus le fichier est volumineux plus il sera difficile de le reconstituer car il est découpé en un nombre trop important de bouts. Cela se confirme en analysant tous types de fichiers que ceux de plus petite taille sont quasiment tous lisibles alors que les plus volumineux le sont moins.



Graphique 6 – Nombre total de fichiers récupérés illisibles

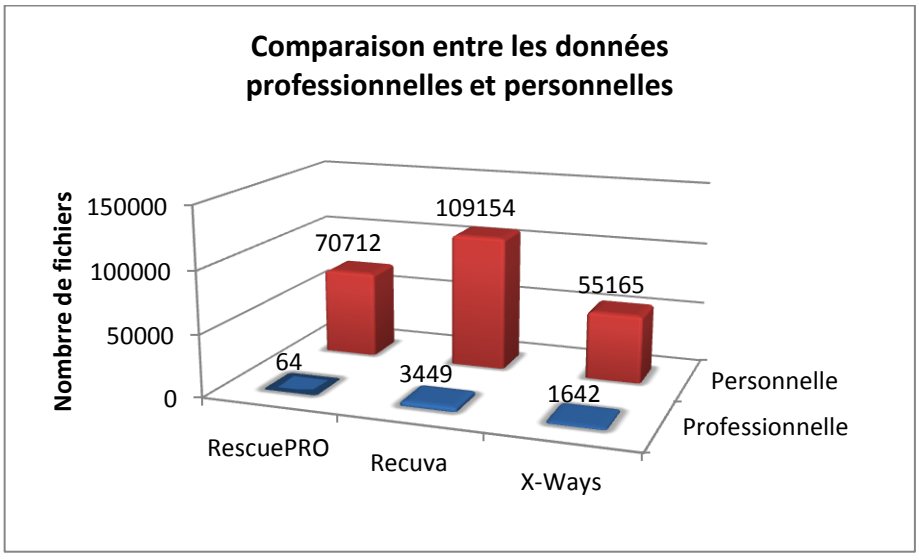
Après l'analyse des fichiers lisibles de chaque disque, je peux affirmer que seulement 4 disques ne possèdent pas au moins un fichier professionnel. Voici un graphique pour illustrer mes propos.



Graphique 7 – Où trouve-t-on des données professionnelles ?

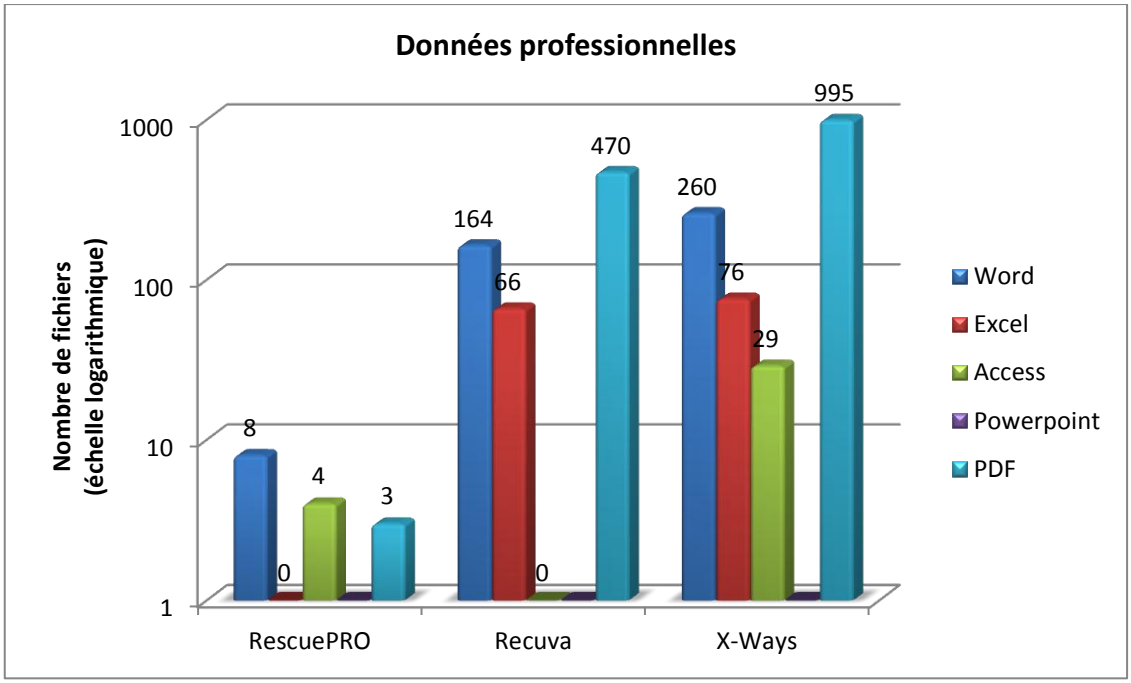
Par contre sur chaque disque et avec chaque programme, on retrouve au moins un fichier personnel. Aucun disque était complet vide.

Sur ce graphique on remarque la grande différence entre le nombre de fichiers personnels et professionnels. Selon moi, ceci vient surtout du fait que plus de la moitié des disques récupérés ne doivent pas provenir d'entreprises. Je suis sûr que au minimum 4 proviennent d'entreprises. De plus, beaucoup de personnes utilisent l'ordinateur du travail à des fins personnelles.



Graphique 8 – Comparaison entre les données professionnelles et personnelles

Ce graphique représente uniquement les données professionnelles récupérées sur tous les disques séparé par programme. On remarque que le programme le plus performant au niveau de la récupération de documents est X-Ways. Ce résultat n'est pas étonnant sachant que c'est un logiciel développé pour les experts en informatique légale. En comparaison avec le programme Recuva, à part au niveau des fichiers Access, les différences sont minimes. Cependant lors de la lecture de ces fichiers, j'ai remarqué que beaucoup de fichier PDF avaient exactement le même contenu.



Graphique 9 – Données professionnelles

Voici une liste de documents professionnels récupérés :

- Contrats
- Courriers
- Commandes
- Résultats de tests
- Business Plan
- Procédures
- Processus
- Plan de circuits imprimés
- Procès-verbaux
- Rapports
- Plan qualité
- Devis

Avec X-Ways, j'ai pu récupérer des fichiers datant de 1998 mais un seul était lisible. Cependant les autres ont quand même un nom de fichier qui permet de deviner leurs contenus.

Ces analyses démontrent bien le fait que l'on retrouve beaucoup de fichiers professionnels et que ces derniers ne devraient pas pouvoir être récupéré par une tierce personne car ce sont des documents officiels et confidentiels.

Il en va de même pour les données personnelles. Effectivement, j'ai retrouvé des fichiers personnels, si c'était les miens, je n'aimerais pas qu'ils puissent être récupérés par un individu quelconque.

Voici une liste d'exemples de documents récupérés :

- Déclarations fiscales
- Photos de vacances
- Photos avec plaques de voiture
- Curriculum vitae
- Lettres de motivation
- Bulletins scolaire
- Diplômes
- Bulletins de commandes
- Documents scolaire

Avec un fichier de chaque type énuméré ci-dessus, un cybercriminel peut récolter beaucoup d'informations sur vous et ainsi les utiliser à votre insu, voir contre vous.

Voici également un aperçu de ce que peut donner l'analyse d'un fichier « index.dat » avec le programme Net Analysis :

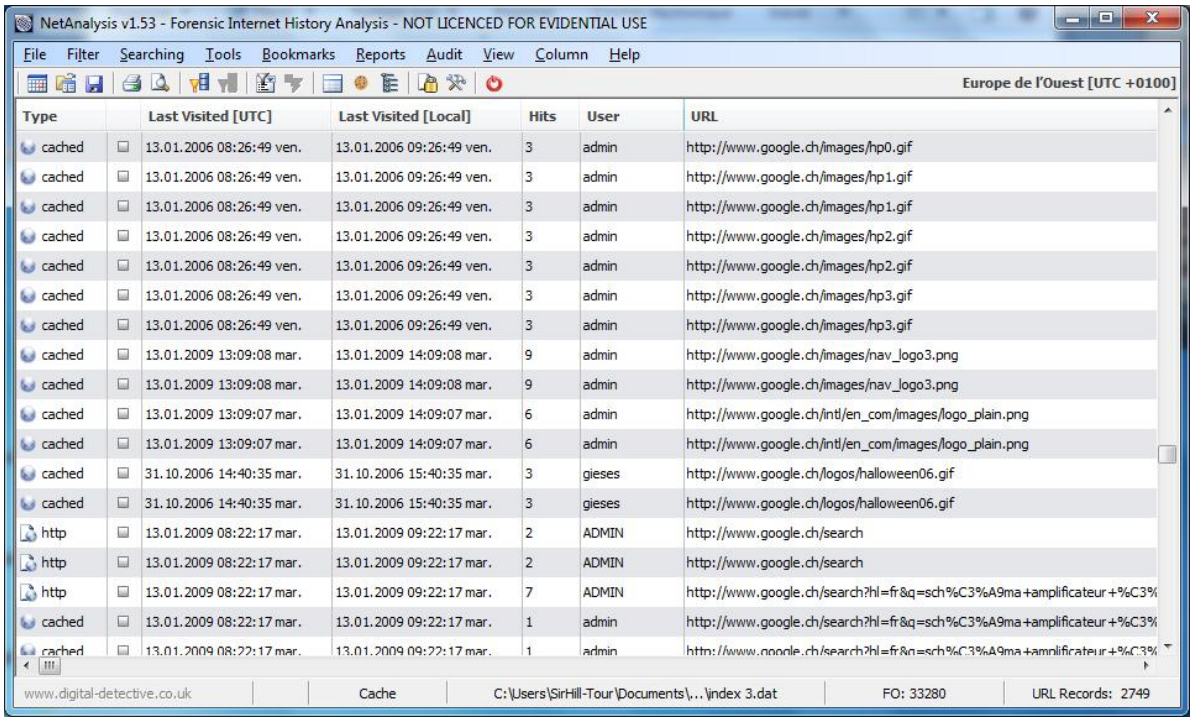


Figure 13 – Capture d'écran de Net Analysis

6. Etude pour connaître les habitudes des gens par rapport au recyclage des disques durs

Pour connaître les habitudes des gens et des entreprises, j'ai pris l'initiative de démarcher auprès d'eux pour savoir quel était leurs façons de procéder lorsqu'ils désirent recycler leur matériel informatique.

6.1 Auprès de particuliers

Concernant les particuliers, j'ai créé un questionnaire en ligne pour savoir comment les gens s'y prennent pour se débarrasser de leurs disques durs. Ce questionnaire m'a aussi permis de me faire une idée sur les connaissances des gens par rapport à la récupération de données.

Près de cinquante-deux personnes ont répondu à mon questionnaire. Il s'agit de personnes âgées entre 18 et 65 ans. Après analyse des résultats, environ 65% des personnes interrogées, pensent qu'il n'est pas possible de récupérer des données après les avoir effacées ou supprimées. Par contre parmi les gens qui estiment qu'il est possible de récupérer des données, plus de 70% penseraient à

installer un programme pour tenter de les retrouver. Les 30% restants disent que c'est une solution trop coûteuse. Personne ne ferait appelle à une entreprise spécialisée. En effet cette dernière solution est plutôt réservée pour récupérer des documents très importants.

Quatre personnes ont déjà essayé de récupérer par elles-mêmes un fichier. 100% des personnes qui disent que récupérer des données est possible, pensent qu'il est possible de le faire sur un ordinateur. Les possibilités qui reviennent également sont la clé USB et l'appareil photo. Par contre personne ne supposent qu'il est possible de récupérer des données sur un autre type de support.

Je remarque donc qu'un faible pourcentage des personnes interrogées connaît la possibilité de récupérer un fichier effacé. Ce qui est plus frappant encore, c'est que les personnes qui connaissent cette option, travaillent dans un milieu où la technologie est très présente. Donc je suppose que les connaissances de ces personnes viennent de leurs milieux professionnels. Il faut donc travailler dans un domaine technologique pour savoir récupérer des données.

Concernant la question du recyclage d'ordinateur, 20% des personnes font un formatage et une réinstallation du système d'exploitation avant de s'en débarrasser ou de le donner. Environ 10% des personnes sondées donnent leur ordinateur sans effectuer la moindre suppression de données, ce qui est à mon avis un pourcentage très élevé car il reste des données personnelles et confidentielles. De plus, 70% des sondés ne font qu'une suppression des données à l'aide de la touche « delete » et seulement environ 30% d'entre eux pensent à vider la corbeille.

Les entreprises dont les employés travaillent avec des ordinateurs devraient vraiment effectuer une sensibilisation auprès de leurs employés car je trouve les résultats ci-dessus inquiétant par rapport à la protection des données. Car les personnes qui désirent s'attaquer au vol de données savent comment s'y prendre pour parvenir à leur fin.

6.2 Auprès d'entreprises

Pour les entreprises, il a été plus difficile d'obtenir des réponses à l'aide d'un questionnaire. C'est pourquoi j'ai récolté les réponses par téléphone. J'ai commencé par interroger des entreprises où j'avais un contact à l'interne. Quinze entreprises ont eu l'amabilité de me répondre.

Il s'avère que la plus part des entreprises possédant un service informatique détruisent, elles-mêmes, physiquement, le matériel. Certaines sociétés stockent les disques hors-services pour toujours savoir où ils sont. Pour les plus petites entreprises qui ne possèdent pas de personnel chargé de s'occuper de l'informatique, elles les stockent également ou elles les renvoient au fournisseur en échange d'un neuf.

Je remarque que les entreprises font nettement plus attention à leurs données que les particuliers.

6.3 Auprès d'entreprises sous-traitantes

De plus en plus d'entreprises font appellent à des sociétés externes pour s'occuper de leur service informatique. C'est-à-dire gérer le réseau informatique, le parc informatique comprenant les ordinateurs, serveurs et imprimantes. Donc il est important de comprendre comment fonctionne une entreprise de solutions informatique vis-à-vis des disques durs hors-service.

Pour le savoir, j'ai donc pris contact avec Monsieur Elio KARRER, partenaire technique pour la société InterHyve Systems. Grâce à cet entretien, j'ai pu obtenir les informations suivantes :

- Chaque disque dur hors-service est premièrement effacé avec un formatage de bas niveau et ensuite détruit physiquement par leurs soins. Il m'a également renseigné sur le fait que les sociétés pour lesquelles il change les disques durs n'ont pas de consignes particulières concernant ces derniers, mais il les informe comme quoi les disques vont être détruits par précaution.
- Lors de cet entretien j'ai également eu la confirmation que de plus en plus d'employés demandent un accès à leur boite email à la maison, tout comme les intranet disponible via une connexion sécurisée ce qui amène donc des données sensibles en dehors de la société. Ce qui nous amènera au point 9 pour parler de sensibilisation.

6.4 Auprès d'entreprises spécialisées

J'ai trouvé deux entreprises spécialisés qui ont été décrites au point 5, qui sont Réalise et Katana.

Après discussion avec ces dernières, chacune a des méthodes différentes car leurs objectifs ne sont pas les mêmes. Pour Réalise, l'objectif est de réutiliser le matériel, tandis que pour Katana c'est la destruction du matériel.

6.4.1 Réalise

Lors de ma seconde visite chez Réalise le 25 janvier 2012, j'ai eu l'opportunité de visiter les locaux et ainsi de voir comment fonctionne une entreprise de recyclage de matériel informatique. Un employé m'a montré et expliquer les différentes étapes de leur processus concernant les disques durs.

La première étape est de séparer le matériel contenu dans les ordinateurs. Il faut ensuite vérifier l'état de marche du disque dur. S'il fonctionne, on peut alors commencer à effacer les données. Leur méthode est d'utiliser un logiciel appelé Darik's Boot and Nuke, plus connu sous le nom de DBAN. Ce logiciel permet d'effacer les données en écrivant des suites de données aléatoires dans les secteurs du disque afin de remplacer les données encore présentes. Ensuite il utilise un logiciel qui vérifie qu'il ne reste plus aucune donnée. Si c'est le cas, le disque est prêt à être monté dans un ordinateur destiné à la revente. Sinon il recommence l'étape précédente jusqu'à qu'il n'y ait plus aucune donnée.

6.4.2 Katana

J'ai rendu visite à Katana lors d'un rendez-vous fixé le 15 février 2012 avec le co-directeur Monsieur Siddik APAYDIN.

Il m'a présenté les différentes options possibles de destruction de disque dur que la société offre à sa clientèle.

Il est possible de demander qu'un broyage du disque ou bien de faire le service complet, c'est-à-dire de passer par les trois étapes qui sont :

1. Démagnétisation
2. Perçage
3. Broyage

La première étape consiste à démagnétiser le disque à l'aide d'un puissant aimant. Ceci efface les données contenu sur le disque. La deuxième partie est le perçage du disque et la dernière phase est le broyage complet du disque.

Katana offre ce service à l'aide d'un minibus équipé du matériel nécessaire aux trois étapes. Le bus se déplace directement chez le client et effectue la destruction devant le client pour qu'il soit bien sûr de l'efficacité du service.

La plupart de leurs clients sont des entreprises mais peuvent également être des particuliers. Katana ne fait pas de publicité ciblée mais comme la société possède déjà des clients par rapport à l'autre service qu'elle propose, c'est-à-dire la destruction de documents papiers, elle leur propose et les sensibilise face au risque que consiste le recyclage de disque dur. Monsieur APAYDIN m'a confirmé que les entreprises clientes qui possèdent un service informatique sont très attentives à la perte de données et donc sont très attirées par ce nouveau service, disponible depuis 2011.

Le prix pour une destruction basique (broyage) de vingt-cinq disques équivaut environ à CHF 250.-.

Nous pouvons résumer la philosophie de Katana par une phrase présente sur leur site Internet :

« Chez Katana, nous pensons que seule la suppression de type physique est la plus radicale puisque la donnée cesse d'être. »
Source : http://www.katana.ch/services-et-destruction/disques-durs

7. Comment faire pour détruire son disque dur ou s'en débarrasser ou le vendre ?

J'ai étudié plusieurs options pour se débarrasser de son disque dur proprement. Vous trouverez ici des solutions gratuites ou payantes, pour entreprises ou particuliers.

7.1 Solution simple et gratuite

7.1.1 Retour en magasin

Ramener votre ordinateur ou votre support de données au magasin où l'appareil a été acheté est une des solutions les plus simples. Aucune manipulation n'est nécessaire. La plus part des grands magasins offrent dorénavant ce service.

Il existe même certaines enseignes qui rachètent vos anciens appareils, s'ils ne sont pas démodés. Pour être sûr que le matériel soit bien recyclé, j'ai été me renseigner auprès de la FNAC qui offre ce service. Le matériel récupéré est effectivement destiné au recyclage et ne sera pas revendu. Donc sans risque. Les magasins garantissent généralement une élimination du matériel selon les normes techniques et écologiques.

Voici deux magasins qui proposent ce service :

- FNAC : http://www.fnac.ch/reprise/
- Media Markt : https://shop.mediamarkt.ch/fr/services/reparation/

7.1.2 Centre de voirie

On peut aussi ramener son ordinateur dans le centre de voirie de sa commune ou à l'espace de récupération de Châtillon qui recyclera gratuitement votre matériel. Aucun matériel qui est entré dans un centre de tri ne peut ressortir. C'est donc une bonne solution, cependant elle ne peut être garantie à 100%.

- Centre de tri de Châtillon : http://www.bernex.ch/?q=node/102

7.1.3 Réalise

La dernière possibilité gratuite est de ramener votre ordinateur à l'entreprise Réalise qui s'occupera de revendre votre ordinateur s'il n'est pas trop ancien. Ce qui est important de savoir c'est que cette société nettoiera le disque dur et s'assurera qu'il ne contient plus aucune donnée utilisable.

Ce service est destiné aux particuliers et aux entreprises. Par contre sous différentes conditions. Réalise se déplace pour enlever le matériel à partir de vingt ordinateurs. Sinon vous avez la possibilité de ramener vos ordinateurs directement sur place.

Vous trouverez plus d'informations sur leur site Internet :
http://www.realise.ch/pages/informatique/repriseinformatique.html

7.2 Solution payante

Comme pour les solutions gratuites, il existe également plusieurs possibilités destinées aux particuliers et aux entreprises.

7.2.1 Vendre son ordinateur

On peut vendre son ordinateur, soit à des magasins d'occasions ou sur Internet. Par contre si vous optez pour cette solution, je conseille grandement de changer le disque dur ou d'opter d'effacer les données de votre disque selon la procédure ci-dessous. J'ai décidé de placer cette issue dans les solutions payantes car un disque dur coûte environ une centaine de francs. Une des possibilités est de changer son ancien disque dur contre un nouveau. Cette solution est sans risque mais on pourrait aussi vendre son ordinateur sans changer le disque dur mais un utilisateur lambda ne sait pas forcément effacer les données selon la procédure décrite au point 7.3.

7.2.2 Katana

Comme expliqué précédemment, Katana offre un service de destruction de disque dur. Il est principalement destiné aux entreprises. En effet, cette société se déplace avec leur minibus pour un minimum de CHF 250.- qui équivaut à environ deux-cents-cinquante disques durs. Je conseille cette solution aux entreprises désireuses d'avoir une garantie de 100%.

Vous trouverez plus d'informations sur ce service sur le site Internet de la société : http://www.katana.ch/services-et-destruction/disques-durs

7.3 Guidelines pour effacer les données d'un disque

Voici une petite procédure pour effacer correctement ses données. Cette solution n'offre pas de garantie à 100% mais il devient plus difficile de retrouver des données.

Pour assurer la suppression efficace des données, il faut connecter le disque dur sur un autre ordinateur et utiliser un programme qui écrit des suites de données aléatoires dans les secteurs du disque afin de remplacer les données encore présentes.

Cette technique est destiné aux utilisateurs avancés car ce genre de logiciel ne se manipule pas via une interface simple d'utilisation et nécessite de bonnes connaissances en informatique.

Il existe deux logiciels libres :

- Eraser : http://eraser.heidi.ie/download.php
- Darik's Boot and Nuke : http://www.dban.org/download

8. Sensibilisation

8.1 Pourquoi sensibiliser ?

Il faut sensibiliser les gens pour éviter que des données dites sensibles ou confidentielles terminent entre les mains de personnes mal intentionnées. En effet de plus en plus d'entreprises font l'objet d'attaques cybercriminelles, pas forcément en récupérant des données depuis des disques durs hors-service mais avec des virus ou des malveillances. Mais le vol de données est souvent un risque négligé par les entreprises.

8.2 Politique de sécurité

Les grandes entreprises qui possèdent des données sensibles font signer à leurs employés une charte informatique avec comme consignes de ne pas utiliser de clé USB, de ne pas envoyer d'email avec pièce jointe à des destinataires en dehors de l'entreprise. Ces consignes sont là pour éviter que trop de données transitent par d'autres disques durs. Lors de téléphones auprès des entreprises pour connaître leurs façons de se débarrasser des disques durs, je leur ai également demandé s'ils utilisaient des chartes. Mon constat est que les multinationales utilisent ce genre d'outil pour contrer les malveillances mais encore beaucoup de PME ne le font pas.

Je pense que lorsque des employés travaillent avec des données confidentielles, la première chose à imposer par l'employeur devrait être une charte informatique. C'est la première protection à mettre en place contre la perte de données. De plus, beaucoup de ces consignes ne sont pas respectées c'est pourquoi les entreprises devraient sensibiliser leurs employés.

Comme le confirme cet article du journal l'Express *(http://lentreprise.lexpress.fr/solutions-business/vol-de-donnees-les-pme-ne-sont-pas-a-l-abri_30692.html)*, peu de sensibilisation est effectuée par les PME car elles ne possèdent pas les moyens financiers d'avoir une personne chargée de sensibiliser le personnel.

8.3 Sensibilisation des employées par les employeurs

Par contre, l'entreprise peut quand même effectuer un minimum de sensibilisation auprès de ses employés en renouvelant la charte informatique chaque année, avec des affiches et flyers disposés dans des endroits stratégiques du bâtiment.

Malgré une charte informatique, encore beaucoup d'employés emportent des données confidentielles à la maison pour peaufiner leur travail. Cependant lorsqu'un employé se débarrasse de son ordinateur personnel, le disque dur de ce dernier contiendra toujours une trace des données de l'entreprise.

Donc si une personne mal intentionnée récupère un ordinateur, avec peu de moyen, elle peut facilement le démonter et retirer le disque dur pour ensuite récupérer les données qu'il contient. Il pourra ainsi s'en servir à des fins malhonnêtes.

C'est pourquoi les entreprises devraient sensibiliser leurs personnels par rapport à ce problème et leur apprendre à recycler leur matériel informatique personnel.

Pour les grandes entreprises, il est facile de faire parvenir un flyer avec plusieurs possibilités de recyclage ou une procédure pour effacer correctement le disque dur et ainsi éviter les risques de vol de données.

J'ai discuté de cette possibilité avec Monsieur Elio KARRER et il était de mon avis que c'est une solution que peuvent envisager les sociétés désireuses de protéger leurs données.

Chaque employé ne possède pas un ordinateur portable mis à disposition par l'entreprise, par contre il aura toujours des données professionnelles sur son ordinateur personnel. C'est pourquoi il est intéressant pour les entreprises de sensibiliser leurs employés au recyclage de disque dur.

9. Cybercriminalité

La récupération de données sert à combattre la cybercriminalité. En effet, les experts en informatique légale en collaboration avec la police scientifique se chargent lors d'analyses de supports de données entre autres, de trouver une preuve afin d'établir la culpabilité d'un suspect.

La cybercriminalité est un risque pour le grand public et le monde professionnel. Pour les cybercriminels, le grand public est un facteur clé car il ne se soucie pas des données qui sont en sa possession sur des supports de données et comment quelqu'un pourrait les voler. C'est pourquoi ils sont des cibles plus faciles que les entreprises. Car ces dernières font plus attention à ce problème qu'est la cybercriminalité en essayant de minimiser l'accès aux données via l'extérieur.

En se débarrassant de ses disques durs on réduit déjà le risque de vol de données. Les sociétés s'exposent tous les jours aux risques suivant :

9.1 Vol d'identité

Il existe plusieurs cas possibles de vol d'identité. Il se peut que quelqu'un utilise vos données bancaires ou utilise votre adresse pour facturer des commandes. Il est possible aussi qu'une personne s'approprie votre identité sur les réseaux sociaux. Il s'agit d'usurpation d'identité.

Il est devenu facile de s'approprier l'identité d'une autre personne car Internet ne reconnait pas qui est derrière l'ordinateur. C'est la même chose pour les adresses emails. L'adresse a beau avoir votre nom, en aucun cas Internet ne peut vérifier que c'est bien vous qui l'utilisé.

9.2 Intrusions dans le système de l'entreprise

Il y a différents types d'intrusion. Il peut s'agir de virus qui a envoie des informations via Internet ou d'une personne qui a pris le contrôle d'un ordinateur. Il y a plusieurs façons de s'en apercevoir :

- Vitesse d'exécution de l'ordinateur très lente
- La souris bouge toute seule
- Connexions réseaux ralenties

Les cybercriminels utilisent surtout ces techniques pour voler des données confidentielles.

9.3 Arnaque via email

De plus en plus de personnes reçoivent des emails de la part de société se faisant passer pour une autre. Exemple :

L'email demande de remplir le numéro de carte de crédit pour payer la facture l'abonnement téléphonique alors que l'email ne provient pas de l'opérateur mais d'un site ressemblant fortement au vrai.

Il est également possible de recevoir un email d'un site de réseaux sociaux qui demande de changer de mot de passe mais il s'avère que c'était également une copie du site officiel.

Vous avez donc où entrer vos coordonnées de carte de crédit ou mot de passe à des sites piratés.

Conclusion

Savoir récupérer des fichiers à partir de disques durs ou autre type de support de données n'est pas seulement un outil utilisé par les personnes ayant malencontreusement supprimé des données, mais aussi par les cybercriminels, par la police scientifique et les experts en informatique légale. Effectivement, en ce 21^{e} siècle, la plupart de nos informations professionnelles ou personnelles, que ce soit de la musique, des photos, des vidéos ou autres documents, sont stockées dans un ordinateur ou sur un support informatique quelconque tel que disque dur, clé USB ou téléphone portable.

La récupération des données est indispensable après une suppression involontaire dans le cadre d'une utilisation professionnelle ou domestique, ou dans une affaire criminelle lorsque la police fait une saisie de matériel suspect, il faut dans ce cas un expert en analyse pour trouver toutes les données possibles présentes ou ayant été présentes sur un disque dur.

Ce que je retire comme enseignement de ce travail c'est que pour une entreprise, il devient de plus en plus difficile de garantir la confidentialité des données qui se trouvent dans leur système informatique en cas de renouvellement du matériel de stockage.

De nos jours, la plus parts des données que possèdent une entreprise sont stockées informatiquement alors qu'auparavant ces données étaient sur papier. Lorsque l'on voulait jeter ces données, il fallait s'assurer de les passer à la déchiqueteuse. Mais même avec cette solution, une personne avec du temps et de la patience pouvait reconstituer le document. Donc l'informatique n'a pas résolu le problème du vol de données, car plus le support est performant, plus les possibilités de piratage sont grandes.

Ce travail de Bachelor m'a permis de confirmer que les données informatiques engendrent des risques majeurs pour les entreprises. Les dommages sont plus conséquents avec l'avancée de la technologie car une plus grande masse de données est stockée informatiquement que l'étaient les données « papier » et la gestion du recyclage de ces supports, une fois ceux-ci devenus obsolètes, demande des connaissances avancées et beaucoup de rigueur dans les procédures d'élimination.

J’ai constaté que malgré les diverses méthodes utilisées pour supprimer des données, on peut toujours les récupérer avec plus ou moins de succès suivant le logiciel utilisé et le temps consacré à cette tâche.

En conclusion : la manière la plus efficace pour effacer toutes traces de données est la destruction physique du support comme le fait la maison Katana.

Du côté de mon expérience professionnelle, ce travail m’a confirmé mon attrait pour la manipulation de matériel informatique ainsi que pour la sensibilisation des entreprises au niveau de la sécurité. Il est possible que j’envisage dans un futur proche de continuer une formation dans le domaine de la politique de sécurité des systèmes d’informations.

Glossaire

Cookie : En informatique, un cookie est défini par le protocole de communication HTTP comme étant une suite d'informations envoyée par un serveur HTTP à un client HTTP.
Source : http://fr.wikipedia.org/wiki/Cookie_(informatique)

Copie-image : Terme adapté de l'anglais « forensic copy », l'expression « *copie-image* » représente une copie bit à bit intégrale de *l'information numérique* présente sur un *support d'information*, y compris espaces non utilisés, espaces non alloués et queues de clusters, effectuée à l'aide d'un logiciel spécifique.
Source : http://fr.wikipedia.org/wiki/Informatique_légale

Cybercriminalité : La cybercriminalité est une notion large qui regroupe « toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau».
Source : http://fr.wikipedia.org/wiki/Cybercrime

Forensique : La *science forensique*, ou la *forensique*, applique une démarche scientifique et des méthodes techniques dans l'étude des traces qui prennent leur origine dans une activité criminelle, ou litigieuse en matière civile, réglementaire ou administrative. Elle aide la justice à se déterminer sur les causes et les circonstances de cette activité.
Source : http://www.criminologie.com/article/science-forensique

Informatique légale : On désigne par informatique légale ou investigation numérique légale l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution de type judiciaire par réquisition, ordonnance ou jugement. On peut donc également la définir comme l'ensemble des connaissances et méthodes qui permettent de collecter, conserver et analyser des preuves issues de supports numériques en vue de les produire dans le cadre d'une action en justice.
Source : http://fr.wikipedia.org/wiki/Informatique_légale

Preuve numérique : Terme adapté de l'anglais « digital evidence », l'expression « *preuve numérique* » représente toute *information numérique pouvant être utilisée comme preuve dans une affaire de type judiciaire. La collecte de* l'information numérique *peut provenir de l'exploitation de* supports d'information*, de l'enregistrement et de l'analyse de trafic de réseaux (*informatiques*,* téléphoniques *…) ou de l'examen de copies numériques (*copies-images*, copies de fichiers …).*
Source : http://fr.wikipedia.org/wiki/Informatique_légale

Bibliographie

Livres :

Carvey, Harlan. Outils d'analyse forensique sous Windows. *Pearson*. 2010.

Volonino, Linda. Analdua, Reynaldo. Godwin, Jana. Computer Forensics – Principles and Practices. *Pearson/Prentice Hall*. 2007.

Zdziarski, Jonathan. iPhone Forensics. *O'Reilly*. 2008.

Support de cours :

Billard, David. Gestion des risques et forensics v2.0. 2011.

Articles :

Wenger, Jean-Luc. Ils vident les poubelles informatiques. *L'Express – L'Impartial*. 2011
http://www.katana.ch/sites/default/files/Press_4_23-11.pdf

Beuze, Jean-François. Vol de données : les PME ne sont pas à l'abri. *L'Express*. 2011
http://lentreprise.lexpress.fr/solutions-business/vol-de-donnees-les-pme-ne-sont-pas-a-l-abri_30692.html

Vivien, Marc. Explosion des arnaques sur internet. *GHI*. 2011.
http://www.ghi.ch/node/5441

Sites Internet :

Disque dur. *Wikipédia*. 2012.
http://fr.wikipedia.org/wiki/Disque_dur

Informatique légale. *Wikipédia*. 2012.
http://fr.wikipedia.org/wiki/Informatique_légale

Suppression de fichier. *Wikipédia*. 2011.
http://fr.wikipedia.org/wiki/Suppression_de_fichier

Récupération de données. 2012.
http://fr.wikipedia.org/wiki/Récupération_de_données

Cookie. *Wikipédia*. 2012
http://fr.wikipedia.org/wiki/Cookie_(informatique)

Formatage. *Wikipédia*. 2011
http://fr.wikipedia.org/wiki/Formatage

Ribaux, Olivier. Margot, Pierre. Science forensique, Criminologie.com – Dictionnaire de criminologie en ligne.
http://www.criminologie.com/article/science-forensique