

Zythom

Dans la peau d'un
informaticien expert judiciaire

Tome 6
Yéléna

Dans la peau d'un informaticien expert judiciaire - Tome 6

Zythom

**Dans la peau d'un informaticien
expert judiciaire**

**Tome 6
Yéléna**

"Je jure, d'apporter mon concours à la Justice, d'accomplir ma mission, de faire mon rapport, et de donner mon avis en mon honneur et en ma conscience."

Serment prêté en Cour d'appel par l'expert judiciaire.

Copyright © 2015 by Zythom

All rights reserved.

ISBN 978-1-326-41411-5

*A mon père, que la maladie empêche de lire ce livre d'une traite :
Je t'aime.*

Avant-propos

Tranquillement, le blog <http://zythom.blogspot.com> vient de franchir ses neuf années d'existence. Bien sûr, la frénésie d'écriture du début (200 billets écrits en 2007 !) est retombée, mais j'espère que la qualité du partage est toujours au rendez-vous, en tout cas j'ose le croire... Ecrire pour partager ses expériences, ses émotions ou ses passions n'est pas évident pour un non-professionnel de l'écriture. Se mettre à nu devant les lecteurs potentiels, et aimer cela, est une sensation déroutante et grisante. C'est aussi une démarche de réflexion personnelle qui demande de chercher à mieux se connaître et de vouloir se remettre en cause pour s'améliorer.

L'ouvrage que vous tenez en main, si vous disposez de la version papier (disponible chez www.lulu.com/spotlight/zythom), ou que vous lisez au format électronique – sur liseuse, sur tablette, sur téléphone portable ou sur votre écran d'ordinateur – reprend les meilleurs billets du blog, du moins ceux publiés après le tome 5. Ils sont normalement toujours en ligne, mais le fait de les regrouper ici leur donne une deuxième vie, une autre dimension.

C'est toujours pour moi une agréable surprise de voir le succès de ces textes, et le nombre de lecteurs du blog et des différents tomes de la série « Dans la peau d'un informaticien expert judiciaire ». Je me dois de préciser, chère lectrice et cher lecteur, que mes proches – à qui ces ouvrages sont avant tout destinés – n'ont de cesse de me garder les pieds sur terre et d'éviter que mes chevilles et ma tête ne gonflent trop. Pour l'instant, je pense qu'ils y arrivent...

Bonne lecture et n'hésitez pas à me faire part de vos commentaires en m'écrivant via la page contact de mon blog :
<http://zythom.blogspot.fr/p/contact.html>

Zythom, Arrakis,
Octobre 2015 (avec ma serviette de bain)

Avertissements sérieux

Il convient de préciser que l'expert judiciaire est soumis au secret professionnel et qu'il ne peut faire état des éléments d'information qui ont été recueillis lors de ses opérations et dont la divulgation pourrait porter atteinte à un intérêt légitime. Les dates, lieux, sexes et noms des personnes ont été modifiés dans toutes les anecdotes citées ici.

Les informations délivrées et les opinions exprimées dans cet ouvrage n'engagent que moi et ne sauraient refléter une position officielle, ni de mon employeur, ni des autres experts judiciaires, ni de quelque institution que ce soit.

« Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi. »

Article 10 de la Déclaration des droits de l'homme et du citoyen de 1789

« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi. »

Article 11 de la Déclaration des droits de l'homme et du citoyen de 1789

« L'imprimerie et la librairie sont libres. »

Loi du 29 juillet 1881, article 1er.

Orthographe

« Les rectifications orthographiques du français en 1990 proposent une nouvelle orthographe pour certains mots du français afin de la rendre plus simple ou en supprimer certaines incohérences.

Ces rectifications ont pour origine un rapport du Conseil supérieur français de la langue française, approuvé par l'Académie française et publié dans les « Documents administratifs » du Journal officiel de la République française du 6 décembre 1990. L'orthographe issue est qualifiée de nouvelle (NO), recommandée, rectifiée (OR), révisée, modernisée ou de 1990, par opposition à l'orthographe dite traditionnelle ou ancienne. Le Conseil international de la langue française (CILF), où tous les pays francophones sont représentés, lui a donné un avis favorable. Néanmoins, l'Académie accepte les deux orthographe : « Aucune des deux graphies ne peut être tenue pour fautive » (Journal officiel). »¹

Depuis juin 2008, la nouvelle orthographe est la référence pour l'Éducation Nationale en France².

Dans la mesure de mes capacités et celles de mes relecteurs, j'ai essayé de respecter, dans cet ouvrage, la nouvelle orthographe. Il se peut que, parfois, quelques restes de l'ancienne orthographe se soient égarés. Et certaines habitudes ont la vie dure : j'ai beaucoup de mal à accepter d'enlever les accents circonflexes des mots « coût », « Maître », « connaître »... Alors j'ai décidé de faire un mélange des anciennes et nouvelles orthographe selon mon bon plaisir. J'en demande pardon au lecteur par avance.

¹ Source Wikipédia : https://fr.wikipedia.org/wiki/Rectifications_orthographiques_du_fran%C3%A7ais_en_1990

² Bulletin officiel de l'Éducation nationale hors-série n°3 du 19 juin 2008, p.37

Certaines réactions chimiques n'ont lieu qu'en présence d'un catalyseur, tels les mariages, légalisés par la présence d'un officiel. Quelques équations ne peuvent être résolues que par l'insertion d'une quantité inconnue appelée x . Si vous n'avez pas ce qu'il vous faut pour obtenir un résultat, vous devez ajouter ce dont vous avez besoin. Si vous avez besoin d'une aide extérieure qui n'existe pas, il vous faut l'inventer.

Chaque fois que l'homme s'est trouvé incapable de maîtriser son environnement les mains nues, ledit environnement a été soumis par la force ou l'entêtement par l'Homme plus x . Il en était ainsi depuis le début des Temps : Homme plus outils ou armes.

Mais x n'est pas nécessairement quelque chose de concret ou de solide, quelque chose de mortel ou de visible. Ce pouvait être aussi intangible ou indémontrable que la menace des feux de l'Enfer ou la promesse du Ciel. Ce pouvait être un rêve, une illusion, un mensonge abominable... N'importe quoi, pratiquement.

Eric Frank Russel, "Plus X"

Contre-expertise

Depuis deux ans, j'accepte [les expertises privées commandées par des avocats](#). Il s'agit essentiellement de contre expertises. Les dossiers que je découvre alors sont analysés en profondeur, tant du point de vue procédure, que du point de vue technique. Et parfois, j'ai des surprises...

[Léo Tyrell](#) est informaticien, et comme souvent, la récupération de données est une demande récurrente de son entourage. A force de pratiquer, les différents outils disponibles sur internet n'ont plus aucun secret pour lui. Il est passé Maître dans l'utilisation de [PhotoRec](#), [Recuva](#), [PC Inspector File Recovery](#) et autres [Glary Utilities](#).

Plus il dépanne son entourage, et plus Léo se dit qu'il existe là certainement un marché intéressant. Il décide de créer un site internet présentant ses compétences et ses tarifs. Il s'intéresse également de près à des logiciels beaucoup plus sophistiqués, utilisés par les services d'enquêtes en tout genre : [EnCase Forensic](#), [AccessData Forensic Toolkit](#), [X-Way Forensics](#)...

Un jour, pour une raison qui m'échappe, M. Tyrell est contacté par un juge d'instruction qui souhaite lui confier une mission. Comment le magistrat a-t-il pris connaissance de l'existence de Léo Tyrell, nul ne le sait. Par Internet probablement, ou qui sait, par le bouche à oreille.

C'est pour lui une consécration, une reconnaissance de ses compétences. Il va pouvoir mettre son savoir-faire au service de la justice.

Le magistrat lui explique au téléphone qu'il travaille sur une affaire de diffamations et injures publiques sur des forums de discussions, que des ordinateurs ont été saisis, et qu'il aimerait que ceux-ci soient analysés pour retrouver le ou les auteurs des messages inappropriés. M. Tyrell, trop heureux de la reconnaissance implicite de son savoir-faire, accepte avec enthousiasme.

Il reçoit quelques jours plus tard un courrier officiel du juge d'instruction avec pour mission de :

- Bien vouloir analyser les scellés UN et DEUX du PV n° 1234/5647 du [SDPJ](#) de [Villevieille](#) afin d'en extraire éventuellement des éléments constitutifs de la présente plainte;
- Faire toutes observations utiles à la manifestation de la vérité.

Comme indiqué dans le courrier du magistrat, Léo retourne le récépissé d'acceptation de mission et attend avec impatience de pouvoir récupérer les ordinateurs. Quelques semaines plus tard, il est contacté par un Officier de Police Judiciaire pour prendre rendez-vous et venir chercher les deux scellés.

Une fois en possession des ordinateurs, il brise les scellés et démonte les disques durs à fin d'analyse. Il y trouve des emails de correspondance entre le suspect et le plaignant. Il découvre également des logiciels d'anonymisation et de VPN, utilisés probablement lors des accès aux forums de discussion.

Après quelques semaines de travail, il rend au magistrat un rapport qu'il pense brillant.

A ce stade du récit, je voudrais faire quelques remarques :

- M. Tyrell n'est pas expert judiciaire, car il n'est pas inscrit sur la liste des experts près la Cour d'Appel de sa région. Cela ne pose pas de problème particulier, car un magistrat n'est pas obligé de choisir un expert inscrit sur cette liste (à condition toutefois de motiver ce choix).
- La désignation d'un expert hors liste impose des précautions particulières : il est nécessaire qu'il ait conscience qu'il devra respecter une « déontologie » et les règles de procédure civile visées sous les articles [233 à 248](#), [273 à 281](#) et [282 à 284-1](#) du NCPC.

- Il devra également pouvoir justifier d'une garantie d'assurance suffisante couvrant une éventuelle mise en cause de sa responsabilité civile résultant de la mission.

- Le Code de Procédure Pénale impose la prestation de serment aux personnes non inscrites sur les listes d'experts judiciaire, à défaut par écrit ([article 160](#)). Dans le cas présent, la prestation de serment a eu lieu après l'ouverture des scellés, ce qui me semble curieux.

- L'expert nommé hors liste sera pour le reste soumis aux obligations communes à tous les experts et en particulier à la pratique de la déclaration d'indépendance. (ref [Cour de Cassation](#)).

- Enfin, l'intitulé de la mission couvre ici un champ particulièrement vaste. Sachant que l'expert désigné ne dispose que de quelques éléments du dossier qui lui sont transmis, il importe de contacter le magistrat pour se faire préciser la mission, voire se faire communiquer des pièces essentielles du dossier, comme ici par exemple, la plainte.

Afin d'analyser le travail effectué par M. Tyrell, l'une des parties me contacte et me transmet le rapport pour une contre-expertise privée, entièrement à ses frais et sans garantie de pouvoir être exploitée en justice. Mon travail commence. Il s'agit d'analyser le rapport d'expertise, d'en expliquer le contenu de manière pédagogique, et d'en effectuer la critique objective. Dans cette affaire ([romancée](#) je le rappelle), beaucoup d'approximations ont été faites :

Sur les scellés :

- l'ouverture des scellés a été faite sans aucune précaution (pas de photographie, pas de description des contenus, pas de vérification des numéros de série, pas d'inventaire exhaustif...).

- une liste de logiciels ayant servis à l'analyse des disques durs est bien fournie dans le rapport, mais aucune information n'est donnée sur le mode opératoire de l'utilisation de chaque logiciel.

- à aucun endroit n'est fait mention de bloqueur d'écriture, ni des précautions prises pour éviter de modifier les disques durs des scellés. Aucune somme de contrôle (hash code) n'a été calculée pour prouver la non altération des preuves.

Sur les dates d'accès internet :

- toutes les dates fournies dans le rapport font référence à la date du système d'exploitation. Mais celle-ci est-elle exacte ? L'horloge du BIOS indique-t-elle une heure exacte ? Le système heure d'hiver/heure d'été est-il actif ? Y a-t-il eu altération de la chronologie des fichiers (par manipulation manuelle de l'horloge du système, ce qui n'est pas interdit) ?

- les dates des fichiers n'ont pas été corrélées avec les dates indiquées dans les entêtes des messages emails. Aucune étude n'a été faite pour vérifier auprès des FAI que les accès constatés sur les forums correspondent aux dates fournies.

Sur les moyens techniques :

- le rapport confond compte informatique utilisé sur le PC et personne susceptible d'utiliser le compte (un membre de la famille, un ami...).

- l'un des ordinateurs est de marque Apple. Aucune mention spécifique n'est faite dans le rapport : pas d'indication sur le nom du système d'exploitation installé et sa version, pas d'état d'utilisation d'outils d'investigation spécifique à l'environnement Apple.

- le rapport cite trois logiciels commerciaux d'analyse inforensique fort onéreux. Est-il possible d'en connaître les numéros d'enregistrement de licences ? (c'est un coup bas, mais il permet d'éliminer les guignols utilisant des logiciels crackés pour faire leurs investigations).

Sur le fond du dossier :

Les qualifications d'injure et de diffamation sont des notions juridiques précises que tout le monde ne maîtrise pas nécessairement. A Paris, la 17e chambre du tribunal correctionnel, dite chambre de la presse, est spécialisée dans ce domaine. C'est aussi le prétexte de billets savoureux : <http://www.maitre-eolas.fr/post/2009/02/04/1306-l-etron-et-la-plume...>

Faute d'avoir demandé des précisions sur sa mission, l'expert part au petit bonheur la chance dans l'exploration des données du disque dur, avec des requêtes basées sur des expressions régulières de mots clefs choisis selon l'état d'esprit de l'expert et non pas guidés par une méthode rigoureuse. Les recherches semblent avoir été faites avec comme objectif de trouver des preuves accablant le suspect.

Le plaignant et le suspect étant manifestement en contact, tous les liens prouvant ce contact sont présentés comme étant des preuves de ce contact. La démonstration ressemble fort à une tautologie (100% des gagnants ont tenté leur chance !).

Aucune exploration n'est faite "in vivo", sur une copie du disque dur par exemple, ou dans une machine virtuelle. Ne sont pas cités les logiciels installés, en lien avec le dossier, et utilisés pour accéder aux forums de discussion.

L'utilisation d'un logiciel VPN, et d'une messagerie anonymisée n'implique pas l'intention de mal agir. Chaque internaute a le droit de chercher à protéger sa vie privée.

Conclusions :

Les "experts" voulant jouer aux experts judiciaires risquent eux-aussi la mise en cause de leur compétence devant la justice. A leurs risques et périls. Dans le cas présent, le rapport d'expertise a été écarté.

Enfin, chaque citoyen peut se voir accusé injustement d'un fait dont il est innocent. Beaucoup croient que la découverte de la vérité s'effectue "automatiquement" et "gratuitement" à travers des enquêtes sérieuses menées avec tous les moyens (humains et financiers) d'une justice moderne.

Ils se trompent lourdement.

Game of gones

Ce dimanche, mon fils fêtait son anniversaire avec ses copains. Il nous avait demandé si nous acceptions de les emmener tous dans une salle de jeux portant le doux nom de "[laser game évolution](#)".

Les parents organisant des anniversaires connaissent l'énergie dégagée par la réunion de 9 enfants de 11 ans et les dégâts pouvant en résulter. J'ai le plus grand respect pour les instituteurs, dont le métier et le savoir-faire consistent à empêcher d'atteindre le point de fusion thermonucléaire d'un groupe pouvant aller jusqu'à 30 composants plus ou moins stables.

J'ai donc étudié avec la plus grande attention la requête de mon petit dernier.

Mmmmmm, laser game, qu'est-ce que c'est que ça...

Waaaouuuu, un jeu où l'on enferme les ~~monstres gamins et rôles~~ [gones](#) dans une pièce et où ils peuvent courir partout en se tirant dessus, mais ça a l'air géniaaal !

Et en plus, on se tire dessus avec des pistolets lasers...

Mon rêve ! Il faut que j'y participe aussi !

Et nous voilà donc tous réunis, mes 9 compagnons de jeu et moi, sous le regard un peu ~~embarrassé~~ attendri de mon épouse pour accomplir un rêve d'enfance : un combat au laser... Certes, loin du mythique sabre laser qui a nourri mon adolescence (encore que j'étais plus intéressé par Z6PO et R2D2), mais suffisamment près de mon univers mental mélangeant [Halo](#), Call of Duty et autres jeux où l'on trouve des rayons de la mort, des [armes Tesla](#) et autres [Wunderwaffen](#).

La préparation est très simple : une vidéo nous indique comment ajuster le harnais sur lequel se trouvent les cibles lumineuses et les règles de combat. On utilise le pistolet laser pour viser l'une des 9 cibles du harnais d'un des adversaires (il y a deux couleurs de joueurs, les rouges et les bleus), si l'on "touche" on gagne 100 points et l'adversaire visé en perd 50. En cas de "tir ami" chacun perd 50 points. On ne doit pas "tuer" quelqu'un dans les escaliers.

Si l'on se fait tuer en hauteur, il faut redescendre. On ne doit pas masquer ses cibles. Quand on s'est fait toucher, les lumières sont éteintes pendant 8 secondes avant de pouvoir rejouer. On ne doit pas s'affronter à une distance inférieure à un mètre. Un peu de fumée dans la pièce permet de visualiser les rayons lasers sur toute leur longueur. Les parties durent 20 mn, et à ma grande surprise, les 9 [gones](#) avec lesquels j'ai joué ont parfaitement respecté ces règles.

La stratégie que j'ai choisie s'est avérée plutôt gagnante : il vaut mieux être très mobile et bouger sans arrêt, mort ou vivant, pour rencontrer le plus de cibles possibles. Sniper de temps en temps peut être amusant, surtout assisté d'un spotter. Mais on est vite repéré et encerclé.

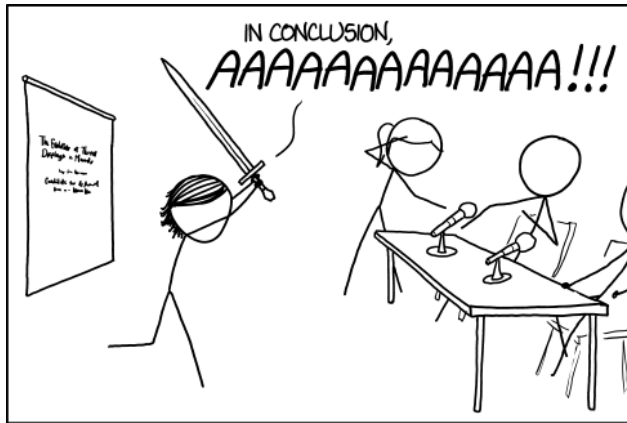
Le jeu en équipe est assez difficile à faire comprendre à des enfants de 11 ans. J'ai donc opté pour la stratégie du [mouvement brownien](#) : chacun court de son côté dans tous les sens et vise la couleur adverse... En fait, je n'en ai parlé à personne et la stratégie s'est mise en place toute seule ;-). Je reconnais qu'il y a eu un peu de confusion lors de la deuxième partie quand les équipes ont été modifiées et qu'un certain nombre d'entre nous ont changé de couleur : il a fallu comprendre qu'il fallait tirer sur une autre couleur que lors de la partie précédente, ce qui, dans un jeu où les tirs réflexes ont une priorité importante, a valu quelques tirs amis malencontreux.

Le décor est assez bien fait : la pièce est dans la pénombre, on se déplace dans un labyrinthe sans réelle possibilité de se cacher. L'une des parties s'est déroulée dans une pièce où se trouvait une voiture sans porte ni coffre ni toit. Les gones ont adoré ! Il y a des tours permettant de se placer au-dessus de la mêlée, mais l'on est vite repéré avec toutes les lumières que l'on a sur soi.

J'ai beaucoup aimé les deux parties que j'ai faites. Un grand dadais de 49 ans qui court partout au milieu de neuf gones, ça ne passe pas vraiment inaperçu...

Un dernier détail : on joue à ce jeu comme on surfe sur internet, sous pseudonyme. Mon fils a choisi "Dark Vador". En bon père, j'ai donc choisi "Luke"... La prochaine fois, je serai [Muad'Dib](#), ou [Ripley](#), ou [T800](#), ou [Dave](#).

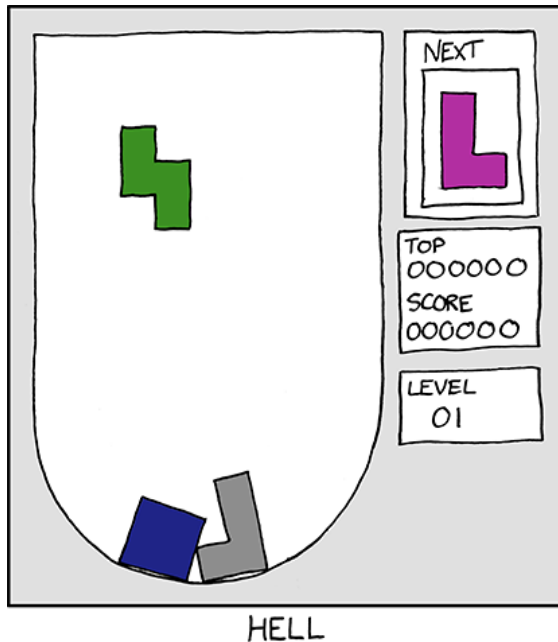
A moins que pour ce "game of gones", je ne choisisse [Jon Snow](#)...



THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

Source image xkcd : <http://xkcd.com/1403/>

La prépa



Source image xkcd : <https://xkcd.com/724/>

Dès le lycée, je savais que l'informatique serait le domaine dans lequel j'allais travailler. Il faut dire aussi qu'à l'époque, je parle de la fin des années 1970, l'informatique commençait à suffisamment se démocratiser pour sortir des entreprises, et tout le monde sentait bien depuis déjà longtemps que le domaine aurait un développement prometteur.

J'avais réussi à suivre la filière scientifique de l'époque (on ne disait pas 1ère ou Terminale "S" en ce temps lointain, mais "C") et j'envisageais avec ambition l'entrée en Classe Préparatoires Aux Grandes Ecoles, les fameuses CPGE ou "classes prépas".

Tous mes professeurs de lycée m'en avaient vanté les mérites, et le métier d'ingénieur semblait correspondre à mes aspirations. Et

pour devenir ingénieur, une seule voie possible, la voie royale : la prépa.

Première étape : obtenir l'inscription dans la meilleure prépa possible. Renseignements pris auprès des profs de maths, les prépas parisiennes avaient la côte. Henri IV, Louis-le-Grand, Janson-de-Sailly, Saint-Louis étaient les noms donnés comme étant les plus prestigieux. Mais, bien que bon élève dans mon lycée de province, mon dossier de candidature ne fut pas retenu. Je me consolais en intégrant ce qui m'était donné comme la meilleure prépa de l'époque dans le Nord de La France : le [lycée Faidherbe de Lille](#).

J'ai toujours aimé les mathématiques et les sciences physiques. J'étais abonné à tout ce qui comptait comme revues scientifiques accessibles au public : Sciences et Avenir, Pour la Science... J'aimais les énigmes, les casse-têtes mathématiques. J'aimais ressentir le frisson des grandes questions scientifiques et techniques : conquête de l'espace, maîtrise de l'énergie, bizarreries de la physique quantique, comportement des objets mathématiques "étranges" comme [les attracteurs](#). L'intelligence artificielle et l'informatique m'attiraient inexorablement...

Deuxième étape :

En septembre 1981, j'entrais comme interne en prépa scientifique, autrement appelée "Math Sup". Je devenais taupin, sans savoir que j'allais vivre les trois années les plus difficiles de ma vie, ni qu'il me faudrait des années pour m'en remettre.

J'ai suivi le chemin royal.

J'ai accepté le formatage mental.

J'ai accepté la mainmise d'adultes qui ne connaissent rien du métier d'ingénieur que j'avais choisi.

J'ai accepté leurs diktats, leurs enseignements, leurs idées.

J'ai creusé la tombe de ma créativité, de mon innocence.

J'ai accepté leur évaluation des individus, des formations.

J'ai appris quelles écoles étaient "les meilleures", quelles formations étaient "pour les élites".

J'ai appris à classer les listes d'écoles et de concours par "valeur".

Un taupin qui réussit, c'est quelqu'un qui apprend beaucoup de choses, vite et bien. C'est quelqu'un qui connaît son cours AVANT d'aller en cours. C'est quelqu'un qui est capable de faire des dizaines et des dizaines d'exercices jusque tard dans la nuit pour obtenir la meilleure note au devoir surveillé ou à l'interrogation orale du lendemain. C'est quelqu'un qui met sa jeunesse entre parenthèse pendant deux, voire trois ans, pour se consacrer corps et âme au gavage de son cerveau.

Pendant deux années complètes, chaque jour de la semaine, chaque semaine de l'année, j'ai absorbé des concepts, des outils, des formules, des réflexes qui n'avaient pour seul but de me permettre de préparer le concours d'entrée des grandes écoles. Chaque concours avait sa propre "réputation" auprès des professeurs, et donc auprès des étudiants. Il y avait les grandes "grandes écoles" et les petites. Nous regardions avec condescendance les écoles qui recrutaient sur dossier, les petites écoles inconnues et les écoles peu "cotées".

Après deux années de travail acharné, j'avais réussi à être pris dans plusieurs écoles d'ingénieurs. Mais mon échelle de valeur, imposée par mes professeurs et par l'esprit sectaire du système prépa, m'imposait de redoubler, de repasser les concours pour obtenir MIEUX, une école plus PRESTIGIEUSE, parce j'en avais la CAPACITE, le POTENTIEL, parce que JE LE VALAIS BIEN.

J'ai donc redoublé, comme un bon tiers de mes camarades, pour avoir mieux, pour aller PLUS HAUT.

Et après cette troisième année de gavage, j'ai réussi à intégrer une école prestigieuse : l'École Nationale de Mécanique de Nantes (ENSM) qui proposait une option informatique qui commençait à avoir une assez bonne réputation. Je tiens à préciser que cette

école s'appelle maintenant École Centrale de Nantes (ECN). Cette école a contribué à faire ce que je suis aujourd'hui.

Bien sûr, je ne renie pas ces trois années de ma jeunesse, ni les choix que j'ai pu faire, ni les amitiés que j'ai pu forger dans ces moments difficiles. Mais je n'ai compris que bien plus tard que j'aurais pu faire autrement, qu'il existait des voies moins royales mais plus humaines. La prépa est un système de sélection poussé jusqu'à l'absurde. Qui décide de ce qu'est une bonne prépa, une bonne école ? Très souvent des personnes qui n'ont aucune idée de ce qu'est le métier d'ingénieur.

J'ai passé les premières années de ma vie professionnelle à désapprendre les comportements élitistes que le système prépa m'avait inculqués. J'ai découvert d'autres diplômes, d'autres compétences, d'autres formations. J'ai rencontré des personnes très intéressantes, très compétentes, très intelligentes dans mon domaine d'expertise, et qui avaient suivi d'autres voies. Des voies plus efficaces, moins destructrices de l'individu. Et j'ai parfois eu du mal à admettre que je m'étais trompé, que j'avais choisi de souffrir pour rien.

Je travaille aujourd'hui dans une école d'ingénieurs qui propose cinq années d'études directement après le bac, sans classe préparatoire intégrée. Le concours d'entrée est un ensemble d'épreuves basées sur le programme du bac S, avec un effort sur la suppression du biais social.

L'école a pour objectif de former le meilleur ingénieur généraliste possible, en s'appuyant sur toutes les disciplines concernées, et dispose de cinq années pleines pour cela. Une fois entré dans l'école, il n'y a pas de concours interne pour passer en année supérieure. Le travail demandé est raisonnable. L'école est une structure privée de type association 1901. Les frais de scolarité sont importants mais couverts en grande partie par les bourses. Nous n'avons pas la chance d'avoir [un mécène](#) pour nous soutenir, mais 30% du budget est amené par les travaux de recherche (R&D appliquée) du personnel et la recherche de subventions de la direction. Mais ce n'est pas l'objet de ce billet.

Quand je vois les compétences acquises par les étudiants que je côtoie, et leurs conditions de travail, je me dis que mes professeurs de terminale m'avaient bien mal renseigné.

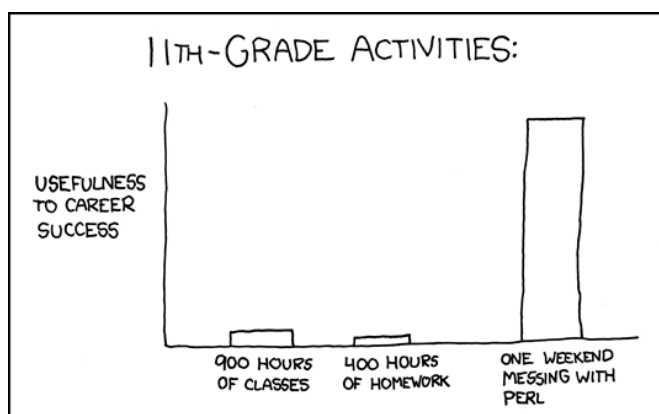
Il existe aujourd'hui un nombre important de formations qui permettent à chacun d'arriver à exprimer le meilleur de lui-même sans sacrifier sa jeunesse. Un bon ingénieur n'est pas nécessairement une éponge à Maths, Physique, Chimie.

Un bon ingénieur est avant tout quelqu'un de passionné.

Un bon professeur est quelqu'un qui sait alimenter cette passion.

Une bonne école est une structure qui arrive à rassembler ces deux catégories de personnes et à les respecter.

Enfin, c'est ce que je me plais à croire.



Source image xkcd : <http://www.xkcd.com/519/>

Un expert judiciaire peut-il être mauvais dans votre domaine ?

Cela fait maintenant plus de 14 années que j'ai prêté le serment de l'expert judiciaire, et donc autant d'années où je suis confronté aux regards des autres sur cette activité, surtout depuis que j'ai ouvert ce blog, en septembre 2006.

Et une question revient souvent de la part de mes interlocuteurs : un expert judiciaire peut-il être mauvais dans son domaine d'expertise, qui se trouve être le vôtre ?

La question n'est pas toujours posée aussi directement. Elle apparaît souvent en filigrane dans certaines critiques que je peux lire sur internet, et dans les questions que l'on me pose sur le processus d'inscription des personnes sur les listes auprès des tribunaux. La question est souvent posée par des spécialistes très compétents dans leur domaine, et qui ont été déçus par une rencontre avec un "expert".

Je pourrais évacuer le problème en répondant : "oui, il y a des experts judiciaires nuls". Je sens déjà la crispation des présidents de compagnies d'experts qui me lisent et la bronca de certains experts judiciaires qui ne portent pas mon blog dans leur cœur (mais qui me lisent quand même ;-).

Mais c'est vrai qu'on me dit qu'il y a des experts judiciaires nuls...

Tout dépend cependant de ce que l'on entend par "nuls". J'ai déjà raconté [ici cette anecdote du DSI](#) d'un grand groupe qui venait d'être inscrit sur la liste des experts judiciaires et qui ne semblait pas connaître grand-chose de l'analyse inforensique d'un disque dur... Effectivement, cette personne serait peu inspirée d'accepter une mission où il aurait à faire une telle analyse technique. Mais peut-on considérer pour autant qu'il soit un expert judiciaire "nul" ? N'a-t-il pas des compétences (que je n'ai pas forcément) sur la gestion d'un grand service informatique, ou plutôt d'un service informatique d'un grand groupe ? N'est-il pas avisé sur les

questions de bonnes pratiques du management d'un système d'information ? Sur son organisation ?

Qui suis-je pour en juger ?

Une des ambiguïtés du terme "expert judiciaire" vient du mot "expert". Prenons tout d'abord sa définition dans [le dictionnaire en ligne de l'académie française](#) :

Expert :

Personne particulièrement qualifiée dont la profession consiste à se prononcer sur l'origine, l'authenticité, la valeur d'un objet d'art ou d'un objet de collection. *Un expert en timbres, en meubles de style, en faïences, en livres anciens. L'expert estime que ce tableau, cet autographe est un faux. Faire appel à un expert pour fixer une mise à prix.*

Par extension : Toute personne qui, connaissant bien un domaine particulier, en a fait sa spécialité. *C'est un expert en architecture médiévale. Plus qu'un connaisseur, c'est un expert.*

Pour autant, je trouve intéressante la page Wikipédia consacrée à l'[Expert](#) :

"L'expert n'est pas simplement celui qui sait, sur un champ délimité de savoir. Son expérience reconnue lui permet d'apporter une réponse argumentée à une demande d'expertise. Il faut le différencier du savant et aussi du spécialiste."

Son expérience reconnue... Mais par qui et comment ?

Un expert doit être différencié du savant et du spécialiste...

La confusion augmente quand on sait qu'un certain nombre de professions utilisent le mot "expert" :

- expert en assurances
- expert-comptable
- expert immobilier
- géomètre-expert

Une recherche du mot "expert" dans [les fiches métiers de pole-emploi](#) retourne 19 résultats...

Finalement, nos anciens auraient peut-être été bien inspirés d'éviter le mot "expert" et de lui préférer le mot "technicien". Mais l'expression "technicien judiciaire" a du paraître moins prestigieuse à certains.

De mon point de vue, l'expert judiciaire est un généraliste de sa spécialité avec une bonne expérience. Il est moins bon qu'un spécialiste pointu (mais il peut le comprendre et échanger avec lui), mais il possède des connaissances plus larges (un minimum de connaissances en droit, une vision large de son domaine d'activité). Il faut également un minimum d'expérience pour pouvoir estimer les bonnes pratiques, les règles de l'art ou les préjudices subis.

La nomenclature qui définit les domaines dans lesquels l'on peut être expert judiciaire a été publiée dans l'arrêté du 10 juin 2005 ([JO du 28/06/2005 texte 12](#) pdf). Concernant l'informatique, il y a plusieurs rubriques, comme par exemple :

- E.1.1. Automatismes
- E.1.2. Internet et multimédia
- E.1.3. Logiciels et matériels
- E.1.4. Systèmes d'information (mise en œuvre)
- E.1.5. Télécommunications et grands réseaux
- F.5.5. Biostatistiques, informatique médicale et technologies de communication
- G.2.5. Documents informatiques

Cette dernière rubrique (Documents informatiques) étant dans la section G : "Médecine légale, criminalistique et sciences criminelles", sous section G.2 : "Investigations scientifiques et techniques"...

Je suis pour ma part inscrit uniquement dans la rubrique "Logiciels et matériels" (ne me demandez pas pourquoi). Tous les informaticiens comprendront que cette rubrique est extraordinairement vaste et couvre tous les aspects de l'informatique.

C'est pour cela que je me sens "généraliste".

Suis-je pour autant bon dans ce domaine ? Je dirais que je me sens tout petit quand je lis par exemple [certaines épreuves d'InsomniHack](#), ou le programme du [SSTIC 2013](#)... Ce qui fait que les spécialistes en sécurité informatique, confronté à une expertise judiciaire, pourraient en déduire que je suis nettement moins bon qu'eux. Pour autant, je suis capable de comprendre leurs explications, voire de les rendre claires. Et c'est justement ce que me demande les magistrats (ou les avocats) : déchiffrer la complexité technique d'un dossier pour qu'ils puissent prendre la décision juridique appropriée.

Je suis un généraliste de l'informatique confronté à des spécialistes. Et comme en médecine, parfois, les spécialistes regardent un peu de haut le médecin généraliste.

Donc, pour répondre à la question qui fait l'objet du billet, oui, un expert judiciaire peut vous sembler mauvais dans votre domaine d'expertise. Mais ce n'est pas ce qu'on lui demande. On lui demande de comprendre vos explications de spécialistes et de répondre clairement et scientifiquement à des questions posées par un magistrat ou un avocat.

Et de donner son avis en son honneur et sa conscience.

L'art de la copie d'écran

Il m'est arrivé, au début de mon activité d'expert judiciaire en informatique, d'assister des huissiers de justice lors de la constitution de preuves, en matière de publication sur internet.

En clair, aider un huissier à faire une copie d'écran.

Puis, avec le temps, les compétences informatiques des huissiers ont fortement augmenté, et il devient rare que l'on me demande de l'aide pour faire une copie d'écran.

Pourtant...

Comme vient de le montrer [une affaire récente](#), une copie d'écran peut être refusée par un tribunal, si elle ne présente pas un caractère probant suffisant.

Extrait [du jugement](#) :

"Attendu que si la preuve d'un fait juridique n'est, en principe, et ainsi qu'en dispose l'article 1348 du code civil, soumise à aucune condition de forme, il demeure néanmoins que lorsqu'il s'agit d'établir la réalité d'une publication sur le réseau internet, la production d'une simple impression sur papier est insuffisante pour établir la réalité de la publication, tant dans son contenu, que dans sa date et dans son caractère public, dès lors que ces faits font l'objet d'une contestation ; qu'en effet, et comme le souligne le défendeur l'impression peut avoir été modifiée ou être issue de la mémoire cache de l'ordinateur utilisé dont il n'est pas justifié que cette mémoire ait été, en l'occurrence, préalablement vidée ;"

A l'intention de mes lecteurs, surtout s'ils sont huissiers, je propose une méthode de copie d'écran d'une page web qui me semble respecter les règles de l'art :

Étape 1 : Choisir un ordinateur "sur" pour établir le constat.

Idéalement, il faut prendre un ordinateur réinstallé "from scratch", à partir d'un template de machine virtuelle par exemple, ou un ordinateur réinitialisé à partir de ses DVD de restauration.

Pour gagner du temps, il est souvent préféré l'utilisation d'une machine ayant déjà servi (le PC du directeur, de l'huissier, du secrétaire...).

[EDIT] Il est possible de booter une machine à partir d'un liveCD pour plus de sécurité (commentaire de KaitoKito).

Étape 2 : Vider le cache local.

Sur l'ordinateur choisi pour effectuer le constat, lancer le navigateur et vider le cache. Cette opération peut être complétée par l'utilisation d'un utilitaire de nettoyage (tel que [CCleaner](#) par exemple, qui existe en version portable sur une [LiberKey](#) par exemple).

Étape 3 : Vérifier les DNS.

Vous allez surfer sur internet, en entrant l'adresse d'un site web. Il faut donc vérifier que sa traduction en adresse IP se fait correctement. Au besoin, il est possible de faire plusieurs essais avec des serveurs DNS différents.

Étape 4 : Afficher la page incriminée.

Saisir l'adresse complète du site web dans le champ approprié du navigateur (et non pas dans un moteur de recherche).

Étape 5 : Imprimer la page.

Une fois la page affichée, en faire l'impression sur une imprimante de confiance. Si l'imprimante n'est pas sûre, faire une comparaison intégrale de l'impression papier. Vérifier que l'adresse complète de la page apparaît sur l'impression : en effet, en cas d'adresse longue, celle-ci est souvent tronquée. Il faut agir sur les paramètres de mise en page d'impression (variables en fonction des imprimantes). La date doit apparaître clairement et il faut vérifier qu'elle est correcte (et mentionner la vérification sur le procès-verbal !).

Notez que cette étape peut être dématérialisée par la création d'un fichier PDF (à l'aide d'une imprimante pdf) ou la sauvegarde de la page complète dans un format approprié.

Je conseille également d'imprimer le code source de la page, contenant beaucoup plus d'informations pouvant être utiles à la manifestation de la vérité.

Étape 6 : Recommencer avec un autre navigateur.

Une clef USB contenant par exemple les logiciels du kit [Liberkey](#), peut accueillir différents navigateurs sans qu'il soit besoin de les installer : Chromium, Firefox, Chrome, Opera, QtWeb...

L'utilisation d'un autre navigateur permet de vérifier les différents comportements qu'une page web peut avoir (code source, plugings...).

Étape 7 : Recommencer avec un autre ordinateur et un autre réseau.

Le plus simple est d'utiliser un smartphone fonctionnant en 3G, et de vérifier que les informations affichées par la page web incriminée sont les mêmes que précédemment.

Voilà. La procédure est complète. Vous avez votre copie d'écran et le PV mentionnant scrupuleusement toutes les opérations effectuées.

Cela suffit-il à constituer une preuve irréfutable ?

La réponse est non.

Si la partie adverse souhaite réellement contester cette procédure, rien de plus simple : il suffit de me contacter pour une contre-expertise.

Exemples :

Étape 1 : Choisir un ordinateur "sûr" pour établir le constat.

Il est extrêmement rare que l'ordinateur utilisé pour faire le constat soit "sur". Le seul moyen d'en être certain est un ordinateur tout neuf sorti de son emballage (et encore ;-). L'hypothèse d'une contamination par un malware ou un virus n'est pas à exclure. D'où la nécessité de faire les constatations avec au moins un autre ordinateur (un smartphone par exemple), ce qui est rarement fait.

Étape 2 : Vider le cache local.

Il n'est pas rare que l'entreprise dispose d'un serveur proxy pouvant faire office de cache. Ce cache a-t-il été neutralisé ?

Étape X : Quelles vérifications ont été faites sur le serveur hébergeant la page web incriminée ? Qui a vérifié s'il n'y a pas eu falsification des codes sources à un moment ou à un autre ? Qui peut assurer que la personne ayant créé les codes sources incriminés est la seule à pouvoir y accéder ?

Je suis sûr que parmi mes lecteurs férus de sécurité informatique, nombreux seront ceux qui trouveront des failles à la procédure que j'ai présentée.

Donc, de nombreuses contestations sont possibles. Elles dépendent des moyens financiers que vous mettrez en œuvre pour vous défendre, de la compétence de votre avocat, et bien sûr, de celle de votre expert judiciaire ;-)

La copie d'écran est un art complexe.

Stockage

La semaine dernière, j'ai reçu un ordinateur sous scellé à fin d'analyse. Pour une fois, il ne s'agit pas de recherche d'images pédopornographiques, mais de retrouver des conversations électroniques.

J'ouvre le scellé, et en extrait le disque dur pour analyse. Le disque dur fait 3To...

Bon, c'est normal, les capacités des disques durs vont en augmentant, mais après vérification, je ne dispose pas de disques durs suffisamment grands, et mon NAS personnel est presque plein. Comment faire une copie pour analyse, sachant qu'il me faut facilement le double de la taille du disque d'origine : pour l'image bit à bit, pour le fonctionnement en VM et pour toutes les données extraites ?

Sachant que le budget de la Justice, déjà exsangue, n'est pas prévu pour m'offrir un joli NAS, et que tout le monde compte sur mon travail d'analyse, rapide, fiable et PAS CHER... il me faut trouver une solution.

Twitter étant mon ami, je lance un tweet SOS à ceux qui me suivent sur le compte @Zythom. Et me voilà en train de tester plusieurs outils gratuits dont je vais un peu vous parler aujourd'hui.

Tout d'abord, il se trouve que je dispose d'un nombre invraisemblable de carcasses d'ordinateurs qui remplissent mon bureau, entre vieilles cartes mères et webcams-qui-ne-marchent-que-sous-XP. J'ai donc cherché dans le lot un vieux PC avec une carte mère acceptant les disques durs SATA. Me voici avec un NEC "Pentium 4" datant du temps où l'on nommait les PC du même nom que leur processeur.

Une fois la poussière priée d'aller sur les objets alentours, je pars en chasse d'un clavier et d'une souris PS2, d'un écran fonctionnel, d'un cordon d'alimentation et d'un câble réseau catégorie 5e au moins.

En regardant bien la carte mère de cette vieille machine, je compte 4 ports SATA et deux ports IDE. Je fouille alors dans mon stock de disques durs dédiés aux expertises, et j'en extrais un vieux disque dur IDE de 40 Go, deux disques SATA de 3To et un disque tout neuf de 4To.

Me voici prêt à tenter de construire un NAS avec ça.

Les followers qui ne dormaient pas au moment où j'ai posé ma question m'ont proposé les produits suivants :

- [Nexenta Community Edition](#)
- [XPEnology](#)
- [OpenMediaVault](#)
- [OpenFiler](#)
- [FreeNAS](#) et
- [NAS4Free](#)

J'ai testé ces produits avec la machine que j'avais assemblée de bric et de broc. Voici mes constatations, et je demande aussitôt aux passionnés de ces produits de me pardonner mon test simpliste (je ne suis pas un labo de tests non plus !) :

- Nexenta CE n'a pas reconnu mes disques durs;
- XPEnology n'a pas fonctionné de manière stable malgré tous mes efforts (je dispose déjà de deux NAS Synology, un vieux DS209j et un DS713+ flambant neuf, donc j'étais motivé);
- OpenMediaVault n'a pas réussi à faire booter ma machine;
- OpenFiler n'a pas reconnu mon disque dur de 4To lors de la configuration SoftRAID;

Le développement de FreeNAS ayant été repris par une société commerciale, j'ai directement testé NAS4Free qui est [la suite du développement du code originel de FreeNAS](#). NAS4Free a reconnu l'ensemble de ma configuration, aucun message d'erreur n'est

apparu lors de la constitution du RAID0 qui a aggloméré tous mes disques durs (sauf celui de 40Go qui sert uniquement pour le système au démarrage).

Mon choix s'est donc arrêté sur NAS4Free.

J'ai donc maintenant un NAS de capacité ~~40To~~ 9 To qui me permet de mener à bien la mission d'expertise qui m'a été confiée. L'accès aux disques est rapide, l'incorporation dans mon réseau privé très simple, le partage des données entre machines Linux ou Windows est simple à paramétrer. Bref, une solution que je recommande à tous ceux qui ont un besoin rapide de stockage pour pas trop cher.

Seuls inconvénients : la consommation et le bruit, légèrement supérieurs à ceux de mon NAS perso Synology DS713+ sur lequel s'appuie toute la famille.

Mais si le dernier reste allumé en permanence toute l'année, le NAS4Free ne reste allumé que le temps d'une expertise, c'est-à-dire... quelques nuits ;-)

Ma prochaine étape sera de faire l'achat que quelques cartes PCI multiports SATA pour augmenter la capacité de mon NAS improvisé. Je dois pouvoir atteindre les 16 disques durs de 4To, soit 64To !

Ensuite, pour passer à 180To, je testerai le pod de stockage Backblaze que [Korben m'a fait découvrir](#).

De quoi voir venir ;-)

Expérience sur l'anonymat

Lorsque j'ai décidé d'ouvrir ce blog en 2006, j'ai pris comme pseudonyme "Zythom" car je voulais séparer mes activités IRL et numérique. Je considérais l'utilisation d'un pseudonyme comme allant de soi dans l'univers numérique.

Dès que j'ai commencé à avoir des lecteurs, je me suis trouvé devant le problème classique de la modération ou pas des commentaires. Après avoir hésité un peu, j'ai fait le choix de modérer les commentaires pour garder le contrôle du contenu du blog. Ce faisant, je sais que mon statut juridique est plus risqué, puisque j'autorise la publication du commentaire. Mais c'est mon choix et je l'assume jusqu'à présent.

Pour compenser un peu, parmi les différents paramètres de la configuration du blog, j'ai choisi d'autoriser la soumission de commentaires anonymes. Cela me semble logique, même si cela encourage quelques personnes à abuser de cette possibilité.

Mais je souhaitais pouvoir aller plus loin dans l'anonymat que je pouvais offrir à mes éventuels correspondants, aussi, en juin 2010, j'ai ajouté à la [page contact](#) de mon blog [un formulaire PrivacyBox](#) permettant à tout internaute qui le désire de me contacter d'une manière complètement anonyme, sans que je ne puisse avoir de moyens de connaître son identité réelle. Les messages que je reçois via ce formulaire sont de plus automatiquement chiffrés avec ma clef publique OpenPGP.

Maintenant que le service de PrivacyBox va fermer, il est temps pour moi de faire un petit bilan de cette expérience.

Donner la possibilité à des personnes de vous écrire sans contrainte d'identité lève un certain nombre de barrières : la parole est plus libre, plus directe. Des choses peuvent être dites sans fard, sans le vernis de la politesse et la retenue de l'éducation. J'ai ainsi reçu des courriers d'encouragements et de soutiens de personnes qui souhaitaient rester anonymes.

J'ai aussi reçu des messages d'insultes, de menaces, de critiques...

Mais j'ai également reçu par ce biais des messages qui m'ont interrogé. Je me souviens en particulier de cette personne qui m'expliquait ses penchants pour les jeunes enfants et qui était tombé sur mon blog parce que j'y parle (souvent) de mes dossiers de recherches d'images pédopornographiques. Cette personne me livrait ses tourments et m'expliquait comment elle surmontait le passage à l'acte en consommant des ouvrages interdits en France mais autorisés au Japon (des mangas spécialisés dans les dessins pornographiques mettant en scène des enfants). J'ai reçu en quelques jours plusieurs messages très crus de sa part sur le sujet, sans pouvoir y répondre puisque la personne n'a pas souhaité me laisser le moyen de la contacter, et pour cause.

J'ai reçu également quelques demandes pour des interventions dans des dossiers, des questions sur le piratage, sur les techniques de contournement ou sur les moyens mis en œuvre par la Justice pour lutter contre telle ou telle fraude. J'y ai répondu dans la mesure de mes capacités et lorsque l'utilisateur me laissait une adresse email pour cela.

J'ai reçu en tout une centaine de messages.

J'ai ainsi été spectateur d'une liberté totale d'expression, sans inhibition.

J'en ai appris beaucoup sur la nature humaine.

J'en ai appris aussi sur moi-même, sur mes propres rouages.

J'ai mené cette expérience pour aller jusqu'au bout de l'anonymat.

Je suis désolé que le service de PrivacyBox ferme.

En tout cas, j'ai eu moins peur en lisant ces emails anonymes, qu'en lisant les commentaires que l'on trouve sous les articles de certains journaux en ligne...

Un hacker expert judiciaire

Note : Dans ce billet, j'utilise évidemment la définition initiale (et normale) du mot "hacker", c'est-à-dire (via [Wikipédia](#)) : "Un hacker est quelqu'un qui aime comprendre le fonctionnement d'un mécanisme, afin de pouvoir le bidouiller pour le détourner de son fonctionnement originel. Appliqué à l'informatique, un hacker sait où et comment bidouiller un programme ou matériel électronique pour effectuer des tâches autres que celles prévues par ses concepteurs."

Aussi loin que je puisse remonter le fil de mes souvenirs, j'ai toujours été un hacker. Un hacker de l'ombre, anonyme et discret. Mais toute mon énergie est tournée vers le hacking, en particulier informatique.

Quels sont mes hacks favoris ? J'aime bien démonter les systèmes pour comprendre comment ils fonctionnent. Je viole systématiquement les garanties de tous les matériels que j'achète, uniquement pour voir l'agencement intérieur et comprendre le fonctionnement du produit. J'admire souvent l'intelligence des ingénieurs et des techniciens qui ont réussi à mettre au point tel sous-système particulièrement astucieux. Je remplace parfois une pièce par une autre, plus performante, pour rendre le produit plus efficace, mieux adapté. J'en reçois une joie intense quand cela fonctionne.

C'est un état d'esprit très pratique quand on est expert judiciaire, c'est-à-dire inscrit sur une liste de référence auprès de sa Cour d'Appel de rattachement. Quand les magistrats me confient un scellé, ils n'imaginent pas nécessairement les trésors de savoir-faire qu'il faut pour pouvoir les démonter correctement sans connaître a priori le modèle, pour éviter tous les pièges parfois tendus par les fabricants (vous savez, LA vis cachée sous une étiquette sous la batterie...). Je fabrique parfois mes propres outils (par exemple [un tournevis à partir d'une brosse à dent](#)) pour ne pas abîmer les plastiques des machines qui me sont confiées (on n'attaque pas le démontage d'un Mac au burin et au marteau !).

Je suis un hacker car j'aime comprendre le fonctionnement interne d'un système informatique, que ce soit un ordinateur, un ensemble d'ordinateurs ou un réseau informatique.

J'aime bien détourner l'usage initial d'un objet, pour le transformer, l'adapter ou le recycler. Oh, ce n'est jamais extraordinaire, car je n'ai pas l'âme, l'intelligence ou la patience d'un inventeur. Mes créations sont banales aux yeux des spécialistes, mais elles sont uniques à mes propres yeux.

Je [construis un NAS](#) avec une vieille carte mère, des adaptateurs SATA, des disques durs et une vieille unité centrale. Je remplace le processeur par un moins consommateur d'énergie. Je supprime le ventilateur, tout en underclockant le processeur dans le BIOS, pour baisser le bruit de fonctionnement.

Je transforme une salle de TP informatique en cluster de calcul, le temps d'une après-midi, en bootant sur un liveCD. J'y affiche en temps réel le calcul d'une image de synthèse en utilisant [une version parallélisée de PovRay](#). Chaque machine calcule 1/20e de l'image et l'ordinateur du prof (le 21e pc de la salle) assemble en direct le résultat des calculs. C'est magique. La salle est hackée.

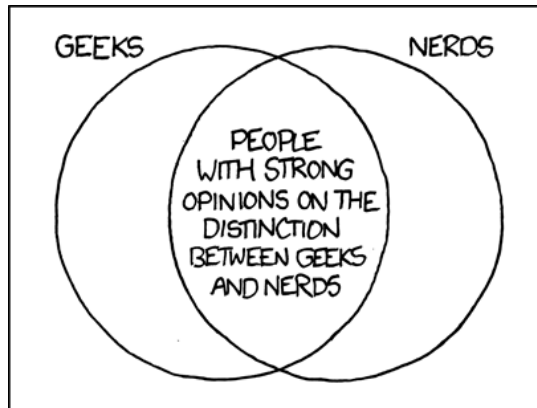
Je démonte un disque dur externe USB pour en récupérer la carte et pouvoir ainsi transformer rapidement n'importe quel disque dur interne en disque externe. Le boîtier est hacké. Je bricole une alimentation de télévision pour l'utiliser sur un ordinateur portable dont le chargeur est en panne. L'alim est hackée. Je récupère toutes les vis, tous les câbles, tous les adaptateurs de mes vieux ordinateurs, parce que cela peut toujours servir (et d'ailleurs, cela me sert souvent). Les vis sont hackées. Euh, là non en fait...

Cela fait-il de moi un **Hacker**, intronisé parmi les plus grands Hackers internationaux ? Non, bien sûr. Je suis un tout petit hacker de province.

Certains diront même que je ne suis pas un vrai hacker. Car un vrai hacker est un rebelle qui ne peut pas être expert judiciaire. A ceux-là, je rappelle que tout le monde peut bidouiller. Alors, pourquoi pas un expert judiciaire ?

Et pour mes enfants, je suis le plus grand hacker expert judiciaire du monde !

Double d'un côté un peu [nerd](#) et [Otaku](#)...



Source image xkcd : <https://xkcd.com/747/>

Lettre à mes 16 ans

Salut à toi, Zythom.

Je suis ton futur toi, ton toi plus vieux. J'ai 49 ans.

Je sais, c'est vieux, surtout quand on a que 16 ans...

Bon, je ne voudrais pas spoiler ton avenir (regarde dans le dictionnaire Harrap's ça veut dire, le volume Anglais -> Français), mais je reviens vers toi pour te rassurer et te donner quelques conseils.

16 ans, c'est super, mais la suite c'est pas mal non plus. Tu vas voir, ça va même aller en s'améliorant. Pour le lycée, ne change rien. Continue de marcher dans le système, de sourire aux profs, même aux casse-couilles.

J'aime bien ton idée de "plutôt que de faire exploser le système en s'y opposant, il vaut mieux essayer de s'y adapter et de le changer de l'intérieur". Ça ne marche pas, mais au moins ça permet d'éviter de s'en prendre plein la tronche, et de rester marqué.

A propos de marques, les boutons d'acnés, n'y touche pas trop, tu en auras jusqu'à la fin de tes jours. That's life.

Les filles, c'est super. Soit patient et ne change rien. Les filles aiment les voyous, mais les femmes aiment les mecs bien. La moto, c'est cool : change juste de casque, parce que l'intégral sur une 125, c'est un peu trop. Mais bon.

Le club d'informatique que tu as créé avec deux potes à lunettes (ne te moque JAMAIS des mecs à lunettes, tu comprends, JAMAIS), c'est super. Continue à jouer avec l'[IBM 5100](#) qu'un parent d'élève vous a prêté. Travaille tes algorithmes, fais fonctionner tes méninges. Par contre, arrête de trop d'occuper à faire rentrer tout ça dans la mémoire de ta [TI57](#), la mémoire, c'est le truc qui va exploser à ne plus savoir quoi en faire. Travaille sur papier et voit GRAND. Genre une mémoire quasi infinie.

Pour ton avenir professionnel, continue à t'inquiéter. Tu deviendras le plus grand procrastinateur de l'univers, mais à chaque fois que tu en auras besoin, tu passeras le cap. Sache quand même que tu vas en baver dur pendant quelques années, mais qu'après tu ne comprendras même pas pourquoi on te paye tellement tu aimeras ton métier. Tu verras même que parfois on ne te payera pas, ou mal. Et tu t'en ficheras, enfin presque.

Côté famille, soit cool. Les études, c'est bien. Ceux qui autour de toi s'éclatent en boîte tous les week-ends au lieu de bosser leur bac vont galérer pas mal ensuite. Toi, tu vas ramer pendant cinq ans, mais après tu vas t'éclater pendant 50 ans. Un bon truc, ce serait de convaincre tout ce petit monde de mettre un peu d'argent dans [une petite société américaine](#) toute jeune et toute petite, située à Albuquerque. Genre 1000 Francs par tête de pipe. Fais-moi confiance.

Un truc moche quand même : la clope. Si tu peux arrêter tout de suite, ça t'évitera quelques tensions par la suite. Et quoique tu en penses, on ne trouvera pas de solution pour le cancer "quand tu en auras besoin". Ça, c'est tout faux. Et parles-en à tes proches aussi...

Arrête aussi le baby et les flippers. Ça mène à rien. De toutes façons, tu seras jamais très bon et c'est pas dans tes moyens. Par contre, continue les jeux d'arcade : Pac-Man et Space Invaders. Tu te feras un peu moins éclater après ~~à CoD~~. A propos, je te signale qu'il y a une position dans Pac-Man où les fantômes [ne peuvent pas venir t'éclater](#). Et si tu pouvais mettre de côté la console Pong, plutôt que ta TI57, ça me fera plaisir 30 ans plus tard en déballant les vieux cartons...

Ah, et concernant [Wattrelos](#), ne te bile pas, tu n'y feras pas de vieux os. Mais tu arriveras à regretter le Nord, si si. Si, je te dis ! Du brun !

Allez courage.

Je te laisse, j'ai mon moi de 70 ans qui m'envoie un [holo](#).

Mon père

Mon père est né avant la 2^{de} guerre mondiale. Parisien pendant l'occupation, il est envoyé en province pour manger correctement. Il fait ainsi sa première communion à Bayeux, le 5 juin 1944, soit un jour avant le débarquement des troupes alliées. Bayeux fut l'une des premières villes libérées de France métropolitaine. Il me raconte encore aujourd'hui comment, avec d'autres enfants de tous âges, il demandait aux GI qui ont traversé Bayeux tout au long des semaines qui ont suivies, des barres de chocolat et des chewing-gums.

Enfant jovial et un peu turbulent, mon père m'a toujours fait rire en racontant les bêtises qu'il a pu faire à l'école, les blagues de potache, les explosions en cours de chimie... Cela l'a empêché d'avoir le baccalauréat, mais grâce à la [Capacité en Droit](#), il a pu devenir instituteur, puis directeur d'école primaire.

Mon père aime la vie, et aime aussi l'animation des jeunes. Il sera membre du [Bon Conseil](#) à Paris, puis y deviendra animateur. Il racontera plus tard à son fils passionné (moi) les parties de cache-cache à 40 gamins toute une après-midi dans le métropolitain. 40 gamins (chacun avec un ticket) répartis en deux équipes, qui doivent se chercher dans un périmètre délimité par plusieurs lignes de métro... Il a vécu une partie de son enfance à [la caserne Babylone](#), dans le 7^e à Paris, son père étant garde républicain, en charge de la surveillance de l'Élysée.

Mon père a été appelé en Algérie française pour faire son service militaire. Il y a rencontré une jeune et jolie jeune femme qui devint sa femme (et qui devint ensuite ma mère). Il me raconte cette anecdote d'avoir été consigné dans ses quartiers (interdiction de sortir de la caserne) au motif d'avoir "tenu la main de sa fiancée pour l'aider à descendre du tram". Le motif avait fait le tour de la caserne pour le plus grand plaisir des hommes de troupe...

Il épousera ma mère et s'installera dans le quartier populaire de Bab El Oued à Alger, elle et lui exerçant le même métier : instituteur. Ils y vivront pendant toute la guerre d'Algérie perdant à ja-

mais leurs jeunesses dans ce gâchis colonialiste. Ils rentreront en métropole dans les derniers. Fonctionnaires ayant abandonné leurs postes, ils ne devront leur salut qu'au fait que tous les fonctionnaires aient abandonné leurs postes en même temps, prenant d'assaut les bateaux pour sauver leurs vies. Ils ne trouveront un poste d'enseignant que dans le Nord de la France. Je vous laisse deviner comment ma mère se souvient de son arrivée en France métropolitaine pendant [l'hiver 1962-1963](#) après avoir connu la douceur du climat méditerranéen...

Courageusement, ils (re)construisent leur vie et éduquent leurs enfants en les entourant d'affection, en nous donnant le bonheur et la joie d'une jeunesse qu'ils auraient voulu avoir. Leur histoire commune est difficile à raconter séparément, tant leur couple semble avoir été, jusqu'à encore aujourd'hui, solide comme un roc.

Aussi loin que mes souvenirs remontent, mon père a été directeur d'école. Nous vivions d'ailleurs DANS l'école, puisque nous occupions le logement de fonction prévu pour le directeur. Cette maison, très grande avec des plafonds très hauts (4,20m !) et des pièces difficiles à chauffer, avait la particularité d'avoir des murs en briques recouvertes de [torchis](#). J'en parle un peu [dans ce billet](#) « Je me souviens de mon enfance », tome 5. Pas très pratique pour planter un clou...

Il a été un directeur d'école très aimé par ses élèves. Il leur a consacré sa vie, se levant à 6h tous les jours pour se coucher à 23h. Les parents d'élèves, souvent d'origine très modeste, le respectaient pour son humanité, même si [certains lui faisaient quelques misères](#). Tout en gardant son humeur joviale, il travaillait dur (ma mère également), donnant beaucoup à ses élèves, croyant à l'ascenseur social, et ajoutait à ses heures normales des cours du soir destinés aux adultes analphabètes.

Lors de la cérémonie de remise de ses palmes académiques, j'étais un grand adolescent ému qui écoutait son père faire un magnifique discours rempli de blagues et de citations.

Quand il a pris sa retraite, bien méritée, il a continué à aller, plusieurs fois par an, dans son ancienne école de [Wattrelos](#) où il fut directeur si longtemps. Il y retourne pour faire chanter les élèves, avec l'accord des instituteurs. Il a continué 26 ans après son départ en retraite, jusqu'à aujourd'hui où la fatigue de son âge se fait sentir et l'oblige à renoncer.

Quand ma fille aînée est entrée en primaire (et nous habitons à l'autre bout de la France, plus près du soleil qui leur a tant manqué), il est allé voir le directeur de l'école primaire de mon grand village, s'est présenté et lui a proposé de faire chanter les enfants des classes. Un peu surpris au départ, tous les enseignants ont accepté et apprécié ce moment magique qu'il leur propose une ou deux fois par an depuis plus de 10 ans. Les enfants l'adorent. Son surnom : "le papy chanteur" !

Cette année sera la dernière de sa tournée des deux écoles : il commence à fatiguer. Je le soupçonne aussi d'avoir cherché dans les yeux de ses propres petits enfants (qui tous les trois ont fait la même école primaire) la fierté qu'ils avaient de pouvoir dire à leurs copains : le papy chanteur, c'est MON papy ! Mais maintenant, mon petit dernier quitte l'école primaire pour la 6e...

Mon père a eu et a toujours une belle vie bien remplie. Il s'est mis à l'informatique depuis deux ans, motivé par ma mère et avec l'aide de leur mairie qui propose des cours pour seniors. Nous leur avons offert un beau "tout en un" avec grand écran tactile et ils participent à une réunion Skype tri-partie chaque week-end, avec ma sœur, eux et moi.

J'ai toujours été réservé dans mes déclarations d'affection envers mon père. Un truc fréquent semble-t-il dans les relations enfants-parents. Comme je sais qu'il lira ce billet (avec l'aide technique de ma mère) depuis son Nord adoptif, je profite de cette fête des pères à distance pour lui dire, du bas de mes 49 ans :

"Papa, je t'aime !"

Les innocents

Lorsqu'un enquêteur me confie un scellé, celui-ci est bien entendu accompagné d'une mission, comme par exemple : "fournir tous les éléments en rapport avec les faits". Ce type de mission présente une particularité redoutable : il est impossible de prévoir le temps que l'on va mettre pour analyser le contenu du scellé...

Prenons un exemple. Je suis contacté par téléphone par un enquêteur, en général un gendarme ou un policier. Celui-ci évoque quelques éléments de son dossier en rapport avec la mission qu'il compte me confier. Souvent l'enquêteur me demande conseil sur la rédaction exacte de la mission, pour ne pas faire de bourde (exemple de bourde : "imprimer sur papier toutes les images retrouvées". Je DOIS effectuer la mission, même s'il y a 20 000 images !).

L'enquêteur aime également être précis sur les termes techniques qu'il va utiliser pour décrire la mission, surtout dans un domaine qu'il ne maîtrise pas forcément. Encore que dans le domaine de l'informatique, gendarmes, policiers et magistrats ont énormément progressé ces dernières années. Je trouve de moins en moins de scellés sans disque dur... Et de plus en plus de scellés avec leurs périphériques USB !

Mais je n'arrive quasiment jamais à avoir une réponse à cette question simple : quelle est la taille du ou des disques durs.

Prenons un exemple plus précis : l'enquêteur m'explique que le propriétaire de l'ordinateur est soupçonné d'échanger des images pédopornographiques. Son ordinateur a été placé sous scellé et ma mission, si je l'accepte, est la suivante (vous remarquerez qu'en fait, il y a plusieurs missions) :

- réceptionner le scellé et le briser
- faire une copie des données numériques présentes sur les disques durs présents dans le scellé
- rechercher toutes traces d'images pédopornographiques

- rechercher tous les échanges effectués en rapport avec ces images (emails, sites internet, chat, etc.)
- fournir tous les éléments en rapport avec les faits
- placer sur cédérom ou dvd tous les éléments trouvés, en deux exemplaires
- reconstituer le scellé et rédiger un rapport.

En général, l'enquêteur arrive assez vite sur ce qu'il a en tête depuis le début de la conversation : "acceptez-vous la mission ?".

A ce stade, j'essaye d'en savoir un peu plus : système d'exploitation, taille des disques durs... En général sans succès. J'essaye aussi de négocier la livraison du scellé à mon domicile (souvent possible, mais de moins en moins).

Mais avant tout cela, il me faut accepter la mission et établir un devis, qui doit aussi être accepté par le magistrat qui supervise l'enquête pour que l'expertise démarre. Autant vous dire que le devis est parfaitement pifométrique au nez doigt mouillé. Dans l'affaire qui m'intéresse, j'ai estimé l'analyse à environ 20 heures de travail, parce que je suis un grand naïf et que je me refuse à établir des devis plus réalistes...

Après prise de rendez-vous et dépôt d'une demi-journée de congés payés, le jour J, à l'heure H prévue, l'enquêteur est à ma porte, avec le scellé. Il vérifie mon identité ~~avec un lecteur d'empreinte rétinienne~~ en me demandant mon nom, et je signe les papiers d'acceptation de mission et de réception du scellé.

Il ne me reste plus qu'à jeter le scellé sur un mur pour le briser, et ma première mission est terminée. Je plaisante. J'ouvre le scellé en coupant le cordon de l'étiquette jaunie par le temps (ce type d'étiquette date probablement du milieu du siècle dernier) attachée subtilement autour de l'ordinateur. Sache, jeune [padawan](#) enquêteur, que je m'amuse beaucoup à essayer d'accéder à l'ordinateur SANS briser le scellé. Seul un Chevalier Jedi sait emmailloter correctement un scellé pour que PERSONNE ne puisse l'ouvrir sans le briser.

On s'amuse comme on peut.

C'est à ce moment-là, dans l'affaire en question, que je me suis rendu compte que le scellé contenait un disque dur de 3 To...

Bien bien bien. Je m'équipe comme il faut d'un nouveau NAS pour absorber l'image du disque dur, plus toutes les données extraites. Soit environ 6 To. Rien que ce travail-là m'a pris un mois. Entre réglages, tests divers, hésitations, mesures de performances, le temps s'écoule très vite le soir et les week-ends (n'oubliez pas que le reste du temps j'ai un vrai métier).

Je procède, la main tremblante, à la copie du disque dur. Tout est fait pour qu'il ne tombe pas en panne à ce moment-là : ventilateur, onduleur, encens et divers rites liés [à ma foi](#). La copie a duré 48h pendant lesquelles j'ai très mal dormi.

Voici venu le temps de l'exploration préalable de la copie du disque dur. C'est un moment que j'aime bien : en effet, [au cœur des ténèbres, j'aime l'odeur du napalm au petit matin](#)... Je me promène l'air de rien sur le disque dur pour regarder à qui j'ai affaire.

Ce disque dur avait l'air d'appartenir à quelqu'un de normal.

Mince.

Je procède alors à la récupération de toutes les images présentes sur le disque dur, effacées ou non. Me voici à la tête de dizaine de milliers d'images. Pendant des jours (en fait des nuits), je trie, je regarde, je cherche des images pédopornographiques : rien !

Je vérifie la présence de logiciels de chiffrement, de stéganographie. J'étudie en profondeur la base de registre qui garde trace de... tout en fait : clefs et disques durs USB installés et branchés, logiciels installés, supprimés, etc. Rien d'intéressant !

Je lis tous les documents doc, pdf, txt, cvs, odt, le contenu des zip, 7z, rar, etc. Nénio !

Je cherche tous les fichiers de grandes tailles, je vérifie la présence de containers TrueCrypt ou équivalent. Niente !

Je dresse la liste de tous les logiciels de communication présents (il y en a beaucoup) : Skype, Windows Live, Outlook, Firefox, Chrome, Internet Explorer... Pour chacun, je dis bien POUR CHACUN, il me faut étudier leurs traces, les messages échangés, leurs bases de données, souvent chiffrées d'une manière propriétaire.

Je commence par les outils de messagerie : déchiffrement des bases, analyse des échanges. Patiemment, outils après outils, avec l'aide des sites spécialisés en inforensique, avec les outils développés par la communauté, je cherche des échanges entre pédopornographes, des éléments en rapport avec les faits. Nichts !

L'enquêteur m'appelle de temps en temps pour ~~me presser~~ connaître l'état d'avancement de mes investigations. Je le tiens au courant. Si je trouve quelque chose, j'ai sa ligne directe et un forfait illimité.

J'attaque ensuite les historiques de navigation. Entre les différents comptes des utilisateurs de l'ordinateur, et les fichiers effacés, je me suis retrouvé avec 800 000 fichiers à analyser ! Cookies, URL, données des caches... Un confrère m'a orienté vers un logiciel que je ne connaissais pas : [NetAnalysis](#). Test de la version d'essai, achat à mes frais de la licence, attente de la réception du dongle. Une fois le dongle reçu, j'analyse les données, je reconstitue les pages consultées à partir des données en cache, y compris les caches effacés. Un mois passe. Nada !

L'utilisation de l'ordinateur semble normale : du surf sur des sites pornographiques ([internet, c'est pour le porno](#)), des photos de

famille, des films d'amateur, de la musique, des accès Youtube, le bon coin, Meetic. Rien d'anormal. Dim !

Je suis dans le cas de figure où l'on creuse partout sans savoir ce que l'on cherche réellement comme cadavre, dans une affaire où il n'y a pas de corps... Il faut me rendre à l'évidence, j'ai affaire à un innocent !

Mince.

Enfin.

300 heures de travail, à la recherche de preuves ignobles, la peur au ventre de tomber sur des images immondes, pour finalement me dire que l'ordinateur semble normal. Que son propriétaire est normal. Que ses utilisateurs sont normaux.

Soulagement.

Je n'ai pas pu m'empêcher néanmoins d'avoir un petit pincement au cœur quand j'ai rédigé ma note de frais et honoraires dans laquelle je mentionne 20 heures de travail. Mais j'ai travaillé pour la France, j'ai blanchi un innocent, je dispose de deux NAS performants et d'une clim pour mon bureau, j'ai appris à me servir d'un logiciel efficace acheté à mes frais. J'ai occupé mes soirées et mes week-ends.

Je suis heureux.

Mais ce sont quand même les innocents qui demandent le plus d'efforts.

Les défis des potes

Comme beaucoup de personnes, j'ai perdu des proches à cause de la maladie. J'ai ainsi perdu ma tante, ma grand-mère et ma belle-sœur, toutes les trois mortes d'un cancer. J'aimais ces personnes et elles me manquent beaucoup.

Avec un groupe d'amis, nous nous retrouvons, depuis plus de vingt ans, pour faire la fête, des randonnées, des activités sportives et des visites, dans différentes régions de France. Les enfants de chacun sont venus grossir la troupe, ce qui fait qu'il n'est pas rare qu'on soit une quarantaine de personnes à ~~hurler~~ chanter, danser, boire et s'amuser dans un gîte loué pour l'occasion. Et comme les enfants deviennent ~~enfin~~ grands, nous allons même pouvoir enfin reprendre nos chansons paillardes...

Et depuis que l'une d'entre nous est partie, mangée par le crabe, nous lui dédions toutes nos activités sportives, en général sous la forme d'un défi.

Le prochain défi, ce sont [les 24h du Mans vélo](#)...

Notre première participation à cette épreuve d'endurance de 24h remonte à l'année dernière. J'en avais parlé [dans ce billet](#) « Vu de ma selle », tome 5. D'ailleurs, quand je relis le billet, je me demande pourquoi j'ai accepté de recommencer... même si je l'avais inscrit comme [résolution n°6](#) pour l'année 2013 !

Évidemment, comme l'année dernière, je n'ai rien fait comme préparation physique. Je continue simplement à faire mon trajet quotidien boulot-dodo en vélo, ce qui me paraît nettement insuffisant. J'ai beau faire de l'aviron de temps en temps, mon objectif d'un IMC à 25 est loin d'être atteint et s'est même éloigné assez fortement pendant ces dernières vacances. Et je me suis fait un tour de rein pas plus tard que samedi dernier en déménageant ma grande fille...

C'est mal parti.

Pourtant, j'attends avec impatience ce week-end qui promet d'être infernal.

Parce que c'est chouette de retrouver ses amis et sa famille.

Parce qu'il faut se lancer des défis de temps en temps.

Parce qu'il faut [manger-bouger](#).

Parce qu'on a la chance de pouvoir le faire.

Ce week-end, je vais donner mon maximum en pensant à mes douleurs et en maudissant mes amis. Je vais faire 87,885 km, soit 21 tours du circuit Bugatti, en 4 séries (5+5+5+6, oui notre coach pense que je vais être meilleurs sur la dernière série !) en relais dans une équipe de huit personnes. Je vais faire fonctionner certains des 650 muscles dont je ne soupçonne pas encore l'existence. Je vais haïr cette selle incompatible avec mon postérieur douillet. Je vais anathématiser les vélocipédistes et abominer l'objet de leur adoration.

Mais surtout, je penserai à toi Manu.

L'ANSSI et le test Google

Je fais partie des premières générations d'étudiants de lycéens à avoir été autorisées à utiliser une calculatrice électronique au baccalauréat. J'ai donc connu les deux systèmes : la règle à calcul et les [tables de logarithmes](#) versus la calculatrice électronique. Autant vous dire que j'ai choisi mon camp immédiatement !

Et pourtant, je me souviens des querelles sans fin opposant les "pour" et les "contre", avec en ligne de mire la disparition des capacités intellectuelles des générations futures. Au passage, si je constate effectivement une baisse des aptitudes au calcul mental de mes étudiants, je me permets de constater une hausse très nette de leurs compétences dans bons nombres de domaines utiles au métier de l'ingénieur (mais j'y reviendrai).

Les professeurs de l'époque ont dû s'adapter au monde nouveau qui s'imposait à eux. Ils ont dû revoir les problèmes qu'ils donnaient à leurs élèves, parfois depuis plusieurs décennies. En effet, certains problèmes devenaient ridiculement faciles dès lors que l'on disposait de ce magnifique instrument de calcul. J'appelais ces problèmes "les tests calculatrices". Certains professeurs ont mis plus de temps à s'adapter, ce qui m'a permis d'avoir parfois des notes inespérées, en particulier en chimie. Je me souviens de ces vieux professeurs qui nous grommelaient "comment ferez-vous pour calculer vos logarithmes si la calculatrice tombe en panne"...

Il faut savoir accepter le progrès, s'adapter et accepter que certaines compétences deviennent obsolètes. L'utilisation des tables de logarithmes en fait partie.

L'accès facile à internet pour tous les étudiants, partout et tout le temps grâce aux téléphones mobiles, a changé la donne pour beaucoup d'enseignants et révolutionne la manière d'appréhender beaucoup de problèmes. Est-il nécessaire d'apprendre par cœur telle ou telle somme d'information quand elle est facilement accessible ? Quel type de savoir faut-il enseigner : la connaissance qu'une information existe, savoir la retrouver ou la connaissance en elle-même ? Chaque professeur répond à ce type de question

selon sa pratique et son savoir-faire. Mais cela donne parfois lieu à ce que j'appelle "des tests Google", c'est-à-dire des tests où les réponses se trouvent facilement avec un moteur de recherche.

Je suis personnellement en plein questionnement sur mon devenir professionnel : je fais ma petite crise de la cinquantaine et, malgré un travail que j'aime et qui me propose encore beaucoup de défis, j'ai du mal à admettre que je ne pourrai plus jamais changer d'emploi dans les 15 années à venir, si je ne le fais pas maintenant. Je suis donc en train de répondre à des annonces et de passer des entretiens. Vu mon profil et mon expérience d'expert judiciaire, je recherche un poste dans l'[analyse inforensique](#). Au passage, je remercie les lecteurs de ce blog et tous les twittos qui ont relayé l'information.

Et parmi les ~~milliers~~ ~~centaines~~ ~~dizaines~~ quelques offres sur ce créneau visibles sur le marché, j'ai répondu à une annonce de l'[ANSSI](#). L'Agence Nationale de la Sécurité des Systèmes d'Information regroupe en effet de nombreux spécialistes de l'investigation numérique, dont quelques-uns que j'ai pu rencontrer au SSTIC. C'est donc avec une vraie envie de travailler avec ces personnes que je me suis rendu à l'entretien d'embauche qui m'a été proposé.

J'ai accepté de ne pas dévoiler le contenu de cet entretien, aussi je ne vous donnerai pas de détails sur son déroulement, rien sur la confiscation de mes téléphones à l'accueil, je n'aborderai pas la difficulté de trouver l'adresse, ni la climatisation en panne.

Un point m'a néanmoins surpris : les recruteurs m'ont fait passer ce que j'appelle un "test Google". Appelé "test technique", il s'agit d'un long formulaire comportant de nombreuses questions techniques sur tous les aspects de l'inforensique. Toutes les réponses de ce test se trouvent facilement sur Google. Sauf que je n'avais pas accès à internet...

Le problème est que je travaille depuis de nombreuses années avec un accès internet (depuis 1990 en fait), et que j'ai pris l'habitude

d'intégrer cet outil dans ma manière de travailler. A cinquante ans, je n'apprends plus par cœur les paramètres des commandes UNIX que je n'utilise que de temps en temps. Je n'apprends plus par cœur les définitions des concepts que je manipule. Lorsque j'ai besoin de construire une [expression rationnelle](#), je le fais avec l'aide d'internet. Quand j'ai un doute sur l'orthographe d'un mot, je le googlise.

Bref, j'utilise internet comme une gigantesque encyclopédie. Et de la même manière qu'avec la calculatrice, j'ai oublié la manière de "calculer les logarithmes avec les tables", j'ai placé un certain nombre de mes connaissances "dans le nuage"... Pas toutes bien sûr, mais celles qu'il me semble inutile d'encombrer mon esprit. Pareillement, je ne retiens aucun numéro de téléphone ni rendez-vous : une partie de ma vie est dans mon téléphone...

Je sais, c'est mal pour exercer sa mémoire. J'ai longtemps un peu lutté contre cette fainéantise, mais mon naturel a pris le dessus. Pourquoi faire cet effort, quand tant d'autres efforts sont à faire !

Ce qui fait que je me suis trouvé ridicule à ne pas savoir répondre à certaines questions du formulaire ANSSI, telle que "quelle est la différence entre un processus et un thread". Ne riez pas.

Pourtant, je suis persuadé que la mesure des connaissances, que ce soit pour évaluer un étudiant ou un candidat à l'embauche, doit être autre chose qu'un "test Google". J'aurais préféré qu'on ait un peu plus confiance en ma capacité à apprendre, à m'adapter. J'aurais préféré qu'on regarde un peu plus mon parcours, mes réalisations, mes succès et mes échecs.

J'aurais préféré qu'on ne me dise pas "bossez un peu plus l'inforsique des systèmes live et revenez dans deux ans". Même si c'est vrai.

Dans deux ans, j'aurai des lunettes Google et je réussirai tous les tests Google !

Dans deux ans, j'aurai peut-être réussi à travailler avec les meilleurs de l'ANSSI !

Mais dans deux ans, j'aurai 52 ans.



Source image xkcd "Tar" : <http://xkcd.com/1168/>

L'incendie

Samedi 17 août. C'est mon avant dernier jour de vacances et je suis en train de ~~me faire un tour de rein~~ déménager ma fille aînée à 200 km de chez moi. Il est midi et demi, je reçois un coup de fil du gardien de l'école : un incendie s'est déclaré dans les locaux...

Le téléphone a cette faculté de pouvoir vous faire voyager instantanément d'un point à un autre du globe. Me voici donc d'un seul coup au travail en train de gérer un cas d'urgence, avec dans les mains une boîte de rangement d'étudiante en médecine pleine d'os de tailles diverses...

J'arrive à établir rapidement la chronologie : à 11h55 le disjoncteur général de l'établissement s'est enflammé, dans un local technique hors des locaux, ce qui a déclenché l'alarme incendie. La centrale du système de sécurité incendie a aussitôt envoyé un message au gardien de l'école et à la société de gardiennage. 11h56, le gardien constate un dégagement de fumée dans le local technique désigné par le système de sécurité incendie et appelle aussitôt les pompiers.

Quelques minutes plus tard, ceux-ci sont sur place et appellent les agents d'ERDF pour qu'ils sécurisent le local Très Haute Tension (15 000 v). L'incendie s'est entre temps éteint de lui-même. L'ensemble du quartier est privé d'électricité.

C'est à ce moment-là, vers 12h30, que le gardien m'appelle sur mon lieu de vacances pour rendre compte de l'incident. Nous sommes samedi, l'école doit ouvrir lundi ses portes aux étudiants, aux chercheurs et au personnel. Plus précisément, nous sommes samedi 17 août, c'est-à-dire en plein pont de la semaine du 15 août... La semaine où le moins de gens travaillent dans les entreprises en France. Bien bien bien.

Je suis responsable informatique ET technique, c'est-à-dire que j'ai en charge le bon fonctionnement technique des locaux et des appareils de l'établissement. Le bon fonctionnement, aujourd'hui, cela signifie également son alimentation correcte en électricité :

pour les ordinateurs, pour les serveurs, pour les actifs réseaux, pour les imprimantes, pour les téléphones, pour la centrale de sécurité incendie, pour les portes coulissantes, pour les systèmes d'ouverture par badge... Bref, pour tout.

Mais à distance, je ne peux pas faire grand-chose. Je demande donc au gardien de me tenir au courant de l'évolution des événements. Je raccroche. Une demi-heure se passe, il me rappelle : les agents d'ERDF ont isolé l'école dont les équipements électriques Très Haute Tension sont hors service et rétabli le courant pour le reste du quartier. A charge pour moi de les recontacter dès que les réparations seront effectuées, puisque le matériel incendié appartient à l'école qui bénéficie d'un tarif vert. Les pompiers sont partis, les agents d'ERDF également, l'école est sans électricité, le gardien est tout seul... Bien bien bien.

Premier bilan : il n'y a pas de blessé, l'incendie a fait des dégâts très localisés, l'école n'a pas d'électricité, le Plan de Continuité d'Activité de la salle serveurs a bien fonctionné : notre groupe électrogène a démarré dès la coupure de courant, alimentant ainsi les onduleurs qui maintiennent la salle serveurs et les accès internet sous tension. Le temps que la cuve de gazole se vide...

L'école a des liens très forts avec les collectivités locales : ville, communauté d'agglomération, conseil général, région... J'ai dans mon téléphone mobile plusieurs numéros de cellules d'urgence de ces entités. J'appelle un premier numéro, pas de réponse, un deuxième, pas de réponse, un troisième qui sonne, sonne, sonne dans le vide, et miracle, une personne décroche. Je suis à la cellule d'urgence du conseil général. J'explique mon cas à la personne, qui visiblement utilise un talkie-walkie (!). Là, très calmement, il m'explique qu'il dispose d'une liste de personnes à contacter et qu'il va les appeler. Je laisse mes coordonnées et je raccroche.

J'ai le cœur qui bat très fort.

Peu de gens s'en rendent compte, mais on demande souvent l'impossible aux services supports. Ma mission est de faire fonction-

ner l'école, quelles que soient les difficultés. Les étudiants comptent sur moi, les chercheurs comptent sur moi, les enseignants comptent sur moi, les personnels administratifs comptent sur moi... Mais pour l'instant, tout le monde est en vacances, et personne ne se doute du problème qui se pose à moi : comment alimenter l'école en électricité au plus vite, en cette fin de semaine du 15 août !

Quelques minutes après, le téléphone sonne. Un technicien du conseil général est sur place, avec son chef de service et constate les dégâts et le problème. Il me propose de contacter une entreprise qui dispose de GROS groupes électrogènes et de voir s'ils peuvent être disponibles pour lundi matin. Il me donne leurs coordonnées, ainsi que celles d'une entreprise de transport susceptible de pouvoir les livrer. Le cœur battant (et les mains dans les cartons de déménagement), j'appelle l'entreprise, qui répond, qui dispose de deux groupes électrogènes de forte puissance et qui me les réserve. J'appelle l'entreprise de transport, qui répond et qui accepte de livrer les deux groupes. J'apprendrai ensuite que c'est le patron en personne et son fils qui se sont chargés de la livraison lundi 19 août, en pleine quinzaine de fermeture de l'entreprise...

J'envoie alors un SMS à mon chef pour lui résumer la situation et le tenir au courant des problèmes et des solutions mises en œuvre. J'ai conscience d'avoir de la chance.

J'ai passé un mauvais dimanche (mais meilleur que celui du gardien dans l'école sans électricité).

Lundi, le personnel et les étudiants découvraient une école sans électricité, et les vertus du rangement de bureau au retour de vacances. La salle serveurs fonctionnait toujours, alimenté par notre groupe électrogène de secours. Lundi, les deux groupes électrogènes étaient livrés, installés, raccordés et démarrés. Lundi soir, l'école disposait d'un des bienfaits du XXe siècle : l'électricité.

Tout le monde poussait un ouf de soulagement.

Sauf moi.

Combien de temps cela allait tenir ?

Quelle est l'autonomie des cuves des groupes électrogènes ?

Combien de temps pour effectuer les réparations du disjoncteur THT ?

A quel prix ?

Bref, la reprise était compliquée.

Le constructeur a été contacté pour savoir s'il disposait de pièces de rechange sur du matériel vieux de 20 ans. Réponse : non, mais j'ai du neuf si vous changez tout. Après avis d'ERDF qui impose une remise aux normes de tout le matériel en cas d'incident de ce type, la décision de tout changer a été prise. Rendez-vous a été pris avec le constructeur pour obtenir à prix raisonnable le matériel miraculeusement en stock (sinon temps d'attente = 12 semaines, usine fermée en août), et rendez-vous a été pris avec les différentes entreprises (livraison, démontage, installation, raccordement), dont ERDF qui a été exemplaire sur ce problème.

Deux jours et demi plus tard, l'un des deux groupes tombait en panne d'essence (à 2h30 du matin) suite à la panne d'une pompe de transfert du gazole. 1000 litres consommés en 2,5 jours, soit 400 litres par jour et par groupe, soit 800 litres de gazole par jour pour les deux groupes... Mon cœur et [mon plan RSE](#) en étaient malades.

Le dimanche 25 août, un imbécile stoppait l'un des groupes en appuyant sur l'arrêt "coup de poing", à 8h du matin...

Le lundi 26 août, un représentant des habitants du quartier venait me faire part du mécontentement du voisinage suite aux nuisances sonores des groupes électrogènes. Je rédige alors une lettre d'explication que je suis allé placarder dans les halls des immeubles alentour.

Lundi après-midi les travaux de démontage commençaient.

Le mercredi 28 août, toutes les entreprises devant intervenir sur les réparations du local technique THT avaient terminé. Le courant garanti EDF était rétabli, 11 jours après l'incendie.

Je profite de ce blog, même si j'écris ici sous pseudonyme, pour féliciter toutes les personnes d'astreinte, dans tous les services de France et de Navarre, dans les collectivités comme dans les entreprises privées, pour leur dévouement et leur efficacité. Et bravo aussi aux services supports en général !

Il reste maintenant aux assurances à intervenir, mais cela, c'est un autre problème.

Je me souviendrai de mon retour de vacances 2013.

Je suis trop faible

Je suis fasciné par son regard d'une infinie tristesse, malgré son sourire forcé. Le visage de cette petite fille est rempli, dévoré par ses deux grands yeux marron. J'ai son visage sur des dizaines de photos, prises sous des angles différents. Elle regarde parfois l'objectif, parfois dans le vide. Le plus dur, c'est quand ses yeux plongent dans les miens.

Sur chaque photo d'elle, un sexe d'homme. Près de son visage, dans sa bouche ou dans ses mains. Sans être médecin, je lui donne cinq ou six ans. Je suis en pleine expertise judiciaire sur des photos pédopornographiques.

Je suis seul dans mon bureau, chez moi, porte fermée, avec interdiction donnée à mes enfants de me déranger. Je les entends passer près de ma fenêtre en riant. Il fait beau, c'est un beau week-end de printemps.

Nouvelle photo, toujours d'elle. Ses grands yeux m'obsèdent. Son petit corps nu semble si fragile qu'on a envie de la protéger, de traverser l'écran pour empêcher cet homme de l'approcher, de lui faire du mal, de la violer. Mais je suis impuissant à agir, je ne peux que regarder et prendre des notes pour mon rapport.

J'ai honte de ma faiblesse, de mes réactions, de ma sensiblerie. Tant de personnes travaillent dans des conditions difficiles : médecins, pompiers, gendarmes, policiers... Mais ils se soutiennent, se parlent, échangent, évacuent par des mots les horreurs qu'ils côtoient.

Moi, je suis seul. Je n'ai pas de formation pour gérer ce que je ressens, ce que je vois. Je suis un simple informaticien qui aide la justice. Je n'ai que ce blog.

Photo suivante. Cela fait maintenant trois heures que mon cerveau absorbe ces images, que je les inventorie. Je fais une pause, je ferme les yeux. Pourquoi est-ce que je n'arrive pas à contenir mes

larmes ? Je suis un homme, je dois savoir gérer mes émotions. Je laisse la crise passer. Je suis un homme, rien de ce qui est humain, je crois, ne m'est étranger ([Térence](#)).

Je suis un faible.

Je reprends mes investigations, un peu apathique. Rien ne m'oblige à passer autant de temps sur chaque photo. J'accélère la visualisation. D'autres filles, d'autres visages, d'autres âges, d'autres hommes, tant de positions.

Il est tard, la nuit est avancée. Je termine mon rapport, je rédige les annexes, grave les DVD. Pour faciliter la lecture du rapport papier par les OPJ, greffiers et magistrats, j'évite les illustrations, je les repousse en fin de rapport, en annexe.

J'ai choisi quelques photos parmi les plus marquantes.

J'ai choisi celles où cette enfant regarde l'appareil photo avec ses grands yeux tristes, avec dans la bouche ce sexe aussi grand que sa tête.

J'ai encore cette image dans la tête.

Il faut que j'arrive à gérer mes émotions.

Les autres experts y arrivent bien.

Je suis trop faible.

Cracker les mots de passe

Quand j'étais jeune responsable informatique, dans les années 1990, il existait une "tradition" chez les administrateurs réseaux de l'époque : le test des mots de passe des utilisateurs pour vérifier la sécurité du réseau informatique que l'on gérait.

C'est ainsi que j'ai découvert le logiciel "[crack](#)", librement distribué et partagé sur internet par les administrateurs réseaux.

C'est aussi à cette époque que j'ai compris l'intérêt de partager des connaissances utiles pour ceux qui souhaitent se protéger, partant du principe que ces connaissances étaient déjà dans les mains de ceux qui veulent attaquer.

Voici donc un billet sur les outils que j'utilise aujourd'hui dans les analyses que j'ai à mener, soit dans le cadre judiciaire, soit dans le cadre professionnel (quel admin n'a pas déjà eu à contourner un mot de passe root, ou un mot de passe BIOS). J'espère qu'il pourra être utile aux experts judiciaires débutants en la matière, ou à tous ceux qui veulent tester leur réseau informatique personnel ou professionnel.

Dernier point : il n'est pas inutile de rappeler que toute utilisation illégale de ce type d'outils entraîne votre responsabilité juridique. Si vous cherchez à intercepter le mot de passe de votre patron, ou faire une bonne blague à votre collègue, passez votre chemin. Si vous êtes administrateur réseau, vérifiez avant vos tests que vous avez l'approbation et le soutien de votre hiérarchie, ce qui ne coule pas de source. Enfin, chers parents, ou chers enfants, la récupération des mots de passe des membres de votre famille pour s'en servir à leur insu est réprimandée par la loi.

Bref, ce qui est mal est mal, ce qui est illégal est illégal...

[S'il n'était mort il serait encore en vie.](#)

Note à mes lecteurs issus ou nageant déjà dans l'univers de la sécurité informatique, ne vous attendez pas à des découvertes techniques incroyables dans ce qui va suivre, considérez ce billet comme une initiation au B.A.BA pour mes lecteurs "mékeskidis" (© Maître Eolas) ou les simples curieux.

0) L'outil magique, celui qui impressionne les amis : [Ophcrack](#)

Rendez-vous sur le site de [téléchargement d'Ophcrack](#), récupérez le liveCD qui va bien (Vista/7 par exemple), gravez le et bootez votre machine Windows 7. Regardez et admirez, c'est plug and play.

Ophcrack fonctionne très bien également sur des machines virtuelles, par exemples des images disques créées par la commande "dd" et [transformées en VM par liveView](#).

Pour les plus motivés d'entre vous, il existe des "tables arc en ciel" en téléchargement plus ou moins libre sur internet, permettant d'améliorer les performances de récupération des mots de passe. Attention, ces tables peuvent faire plusieurs gigaoctets. Vous pouvez également les faire vous même (par exemple avec [Rainbow-Crack](#)) : prévoir un ordinateur TRES puissant et plusieurs mois de calculs...

Ophcrack est un outil précieux lors des perquisitions, où l'on rencontre souvent du matériel sous Windows XP ou Windows 7.

Conseil aux administrateurs réseaux débutants : bloquez très vite le mode "boot sur CD" de tous les postes que vous administrez...

1) L'ancêtre, celui qui fera de vous un barbu : [crack](#)

Crack est un logiciel de recherche de mot de passe par création de combinaisons de mots courants stockés dans des fichiers. Je dois à ce logiciel ma plus belle collection de "dictionnaires", le mot étant à prendre ici au sens de "liste de mots" (sans définition). J'ai des dictionnaires de mots dans un grand nombre de langues, des dictionnaires de mots écrits en phonétique, des règles de codage/décodage en langage SMS (t1t1 pour tintin), etc. J'ai également récupéré, quand ils ont été disponibles sur internet, tous les fichiers de mots de passe (parfois plusieurs millions) d'utilisateurs...

Comme indiqué en préambule, c'est le premier programme que j'ai utilisé dans le contexte d'analyse de la sécurité de mon réseau, pour tester la validité des mots de passe choisis par les étudiants. Je précise que je suis barbu avec modération. 20% des mots de passe utilisés par les étudiants ont été trouvés en moins de 5 mn, 80% en moins d'une heure. J'ai affiché dans le couloir du laboratoire informatique la liste des mots de passe par ordre de découverte (sans le nom du compte associé), avec obligation pour chaque étudiant de changer leur mot de passe... Toute une époque ;-)

Crack est un programme conçu pour UNIX et fonctionnant sous UNIX. La rubrique ["Troll" de la FAQ](#) est instructive à ce sujet. Ceux qui ont un peu plus de temps, liront avec délice [les emails les plus curieux](#) envoyés au développeur de crack.

C'est un programme pédagogique, qui peut encore être utile, même si je dois avouer ne pas m'en être servi depuis longtemps.

2) La référence : [John l'éventreur](#)

[John The Ripper](#), ou JTR, est l'une des références dans l'univers des briseurs de mots de passe. Bien qu'un peu ancien maintenant, ce logiciel a su évoluer pour utiliser différentes méthodes d'approche.

Il a surtout l'avantage de fonctionner dans beaucoup d'environnements : Windows, Linux, Mac OS, etc. C'est encore un logiciel basé sur des dictionnaires.

Je raconte [dans ce billet](#) (« Assistance à Huissier », tome 5), une petite anecdote liée à la présence de ce logiciel sur le poste de travail d'un salarié avec le mot de passe du patron dans un fichier texte...

3) L'attaque à distance multi-protocoles : [Hydra](#)

Si vous devez auditer un ensemble de postes, de serveurs, de protocoles, de services, de trucs à distance, ou tout simplement un ordinateur allumé ciblé, le tout sans bouger de votre poste d'analyse, voici le produit qu'il vous faut : [THC-Hydra](#).

Je reporte ici la description du produit extraite [de ce manuel en français](#) : THC Hydra est un crackeur de mot de passe réseau supportant les protocoles suivants : TELNET, FTP, HTTP-GET, HTTP-HEAD, HTTPS-GET, HTTP-HEAD, HTTP-PROXY, HTTP-PROXY-NTLM, HTTP-FORM-GET HTTP-FORM-POST, HTTPS-FORM-GET, HTTPS-FORM-POSTLDAP2, LDAP3, SMB, SMBNT, MS-SQL, MYSQL, POSTGRES, POP3-NTLM, IMAP, IMAP-NTLM, NNTP, PCNFS, ICQ, SAP/R3, Cisco auth, Cisco enable, SMTP-AUTH, SMTP-AUTH-NTLM, SSH2, SNMP, CVS, Cisco AAA, REXEC, SOCKS5, VNC, POP3, VMware-Auth, NCP, Firebird.

Le logiciel possède deux modes de fonctionnement : l'attaque par dictionnaires ou [par force brute](#). A ce propos, ne pas oublier les

fonctionnalités moins connues du couteau suisse des réseaux : nmap et [ses possibilités d'attaque par force brute](#).

4) Le mot de passe BIOS oublié : [PC CMOS Cleaner](#)

Toute la description est dans le titre. Là encore, un liveCD à télécharger pour booter ensuite dessus. Rapide, efficace, mais modifie le scellé ce qui est interdit.

Sinon, la vieille méthode dite de "la pile BIOS à enlever" marche toujours, mais il faut savoir la trouver, surtout sur les ordinateurs portables. Encore une fois, interdit dans le cas d'un scellé.

5) Efficace mais long : les emails

La meilleure de toutes les solutions est un constat simple que je fais souvent : la grande majorité des gens n'utilisent qu'un ou deux mots de passe, pour tous les systèmes d'authentification qu'ils rencontrent.

Il est donc très probable que l'utilisateur de l'ordinateur analysé ait choisi son mot de passe "habituel" pour s'enregistrer sur un site quelconque de téléchargement de démos, d'achats en ligne ou de webmail. Parmi tous les sites en question, il n'est pas rare que le mot de passe utilisé lors de la procédure d'inscription soit envoyé EN CLAIR dans l'email de confirmation de création du compte.

Il suffit donc d'analyser les correspondances emails (Outlook, Thunderbird, traces logs des différents navigateurs, etc.) pour retrouver un ensemble d'emails du type "votre mot de passe est bien ZorroDu69, merci de conserver cet email" (oui, merci). Quand vous listez ensuite tous les mots de passe ainsi trouvés, le nombre dépasse rarement 3 ou 4. Il ne reste plus qu'à les tester sur le compte ciblé pour trouver le bon.

C'est l'application d'une des bases de [l'ingénierie sociale](#)...

Conclusion

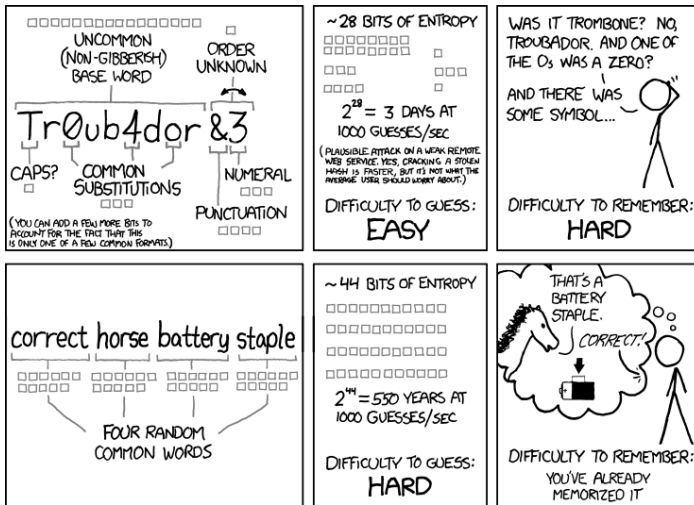
L'amoureux de la vie privée que je suis commencera par un conseil sur les mots de passe : choisissez-les de manière à ce qu'ils ne puissent pas apparaître dans une liste de mots de passe, et suffisamment longs pour qu'ils résistent à une attaque [par force brute](#). Je donne souvent l'exemple des premières lettres des mots d'une chanson ou d'un poème, en mélangeant majuscules et minuscules, ex : [LsLdvdL.BmCdULm](#), auxquelles vous ajoutez quelques chiffres (en majuscule, non, je plaisante), ex : [LsLd-vdL1844BmCdULm1896](#). C'est beau, c'est long, ~~c'est bon~~, c'est difficile à deviner quand on vous regarde taper sur le clavier (sauf si vous chantonnez).

Mais attention, ce n'est pas inviolable (cf. point n°0 sur Ophcrack et le boot sur cédérom).

Ensuite, un conseil encore plus pénible : choisissez un mot de passe très différent pour chaque compte informatique. Dix comptes, dix mots de passe. 50 comptes, 50 mots de passe. Un mot de passe pour Twitter, un autre pour Facebook, un autre pour Gmail, etc. Évidemment, la nature humaine est ainsi faite que la mémorisation parfaite de tous ces mots de passe devient un tantinet compliquée. Je vous recommande donc le logiciel [KeePass](#) pour stocker de façon sécurisée tous vos mots de passe. Ce logiciel est même certifié par l'[ANSSI](#), c'est dire. Il peut également générer des mots de passe très long aléatoirement, avec la possibilité de faire des copier/coller, ce qui revient à ne même pas connaître le mot de passe que vous utilisez.

Du coup, vous n'avez à retenir vraiment qu'un seul mot de passe, jamais mis par écrit : celui de l'accès à KeePass. De plus, ce logiciel est à double authentification (présence d'un fichier à choisir + mot de passe). Vous pouvez même placer KeePass sur le Cloud pour pouvoir y accéder de partout !

Cracker des mots de passe est une activité assez amusante, un petit défi technique accessible à tous. Il est par contre plus difficile pour certains étudiants de garder à l'esprit que tout ce savoir technique doit servir du bon côté de la Force. Quoi qu'il en soit : [sit vis vo-biscum](#) !



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source image xkcd : <https://xkcd.com/936/>

Courir contre soi-même

J'ai eu une enfance sportive : mes parents m'ont encouragé à la pratique du sport, et j'ai répondu à leurs attentes, même si ma curiosité naturelle m'a amené à "papillonner" d'un sport à l'autre. Avec le recul, je pense que ce qui m'intéressait beaucoup, c'était surtout la progression. Dès qu'il fallait faire beaucoup beaucoup d'efforts pour une progression minime, le sport concerné m'intéressait beaucoup beaucoup moins.

J'ai donc pratiqué le foot, la natation, le tennis, le ski et la voile avant mes 18 ans, puis l'aviron et le handball pendant mes années d'étudiants, et enfin la spéléologie, le badminton et le squash pendant mes années parisiennes.

Que s'est-il passé ensuite ?

Le travail, les enfants, le confort et le poil dans la main ont fait que je suis resté sur des acquis physiques que je pensais éternels. Quelques petites alertes m'ont fait changer d'avis : une sortie spéléo dans un gouffre un peu "sportif" duquel j'ai bien cru ne jamais sortir, un essoufflement persistant à la montée des escaliers, une sainte horreur de tout ce qui ressemble de près ou de loin à un effort d'endurance... J'ai donc pris la décision qu'il fallait prendre dans ce cas-là : j'ai arrêté tout effort sportif... Exit donc la spéléo, les sports de raquettes, et aussi tout ce qui ressemblait à une compétition. Et pour asseoir cette décision dans la durée sans regret, rapport à l'essoufflement, j'ai pris l'ascenseur.

Dix années ont passé, heureuses et pleines d'occupations. Mon activité professionnelle m'amène à me bouger un peu, essentiellement à pousser sur les bras pour déplacer mon fauteuil à cinq roulettes. J'aime les bons repas et les bonnes bouteilles. Ce qui devait arriver donc arriva : je me suis encroûté.

Heureusement, les enfants, La Femme et les potes sont là pour me faire bouger un peu ! Tout a pourtant commencé par une décision que j'ai prise tout seul, et à laquelle mes proches ne croyaient pas un instant : aller au travail tous les jours en vélo, quelque soit le temps. Je me tiens depuis plus de deux ans à cette décision, que

j'explique un peu [dans ce billet](#) « Le vélo », tome 4. J'en ai même fait [ici le bilan un an après](#) (« Le vélo, un an après », tome 5).

Ensuite, j'ai décidé de reprendre l'aviron, une fois par semaine, dans un club très éloigné de celui avec lequel j'avais découvert ce sport : je suis inscrit en loisir, ce qui n'empêche pas les ampoules.

Enfin, mes potes me poussent à travers des défis qui m'apparaissent extrêmes : les 24h du Mans vélos l'année dernière (« [Vue de ma selle](#) », tome 5) et cette année (« [Les défis des potes](#) », tome 6 ci-avant). Et ce week-end, le marathon de Jersey par équipe.

Si, dans cette longue introduction, vous avez zappé un élément important pour comprendre la suite du billet, je le rappelle ici : je ne suis pas un grand fan des compétitions d'endurance. Et pourtant, MES POTES M'ONT FAIT PARTICIPER A UN MARATHON CE WEEK-END !!!

Le principe du marathon par équipe est très simple : vous courez sur le même parcours que les marathoniens (42,195 km), mais en effectuant des relais. Chaque membre de l'équipe court un bout du marathon et passe un témoin au suivant. Nous étions cinq dans l'équipe, et j'avais à courir la distance extraordinaire de 7,2 km...

C'était donc ce week-end. Samedi matin, départ pour l'île de Jersey.

Pourquoi Jersey ?

Question posée au coach de notre équipe, et beau-frère par la même occasion. Réponse : "parce qu'il y a un marathon, que je n'y étais jamais allé et que les organisateurs proposent à la fois un marathon classique et un marathon par équipe idéal pour un défi des potes".

Samedi, tourisme sur cette île magnifique, si anglaise et pourtant très française. Je vous passe les détails : paysages magnifiques,

gens accueillants, histoire très riche, châteaux forts, campagne anglaise et vaches typiques.

Dimanche, nous voici sur la ligne de départ. J'encourage avec enthousiasme la première relayeuse de mon équipe (qui en plus est mon épouse...), avant d'aller prendre le bus qui m'emmène à mon point de relais : je suis 4e coureur de l'équipe.

Une fois sur place, je m'hydrate, je me concentre... et je sens monter une certaine anxiété. C'est une chose de courir pour soi, c'est autre chose de courir pour une équipe. Vais-je savoir donner le meilleur de moi-même ? Et si je pars trop vite ? Vais-je être le boulet de mon équipe ? Je regarde tous les coureurs autour de moi, et je vois beaucoup de jeunes, beaucoup de sportifs, beaucoup d'équipements, et très peu de boulet-like. D'après nos savants calculs, ma relayeuse devrait arriver vers midi pour me transmettre le témoin. Après, bah, ce sera à moi de jouer...

Midi arrive, j'ai le cœur qui bat à 100 à l'heure. Je n'ai qu'une seule envie, c'est de me mettre à courir. Les dernières minutes semblent plus longues que les autres. J'ai vu passer un bon nombre de marathoniens (la course individuelle se fait en même temps que la course par équipe, le départ des individuels se faisant simplement 1/2h avant). Je suis admiratif de l'aisance et du style de la plupart des personnes qui sont passées. Mais plus que les autres, j'admire ceux pour qui c'est dur. Je me dis que ceux qui souffrent vraiment sont plus méritant que ceux pour qui c'est "facile". J'applaudis chaque participant.

Midi 5, ma relayeuse arrive, je suis chaud-bouillant. Elle me donne le bracelet-témoin et je m'élançe. C'est à moi de donner. Les 5 premières minutes sont magnifiques, je cours sans effort, emporté par l'adrénaline. Le parcours est sinueux, avec quelques montées, quelques descentes, des virages parmi les arbres. Je rattrape quelques personnes, la plupart courant depuis plus de trois heures, mais aussi quelques relayeurs qui viennent juste de partir comme moi.

Mais très vite mon corps commence à résister. Les muscles envoient des signaux d'alarme au cerveau : "QU'EST CE QUI SE PASSE ? ? ?". Je cours pour une cause : la lutte contre le cancer. Mais mon corps ne le sait pas. Chaque pas, chaque mètre, chaque [verge anglaise](#) est une lutte contre une envie de s'arrêter, de se mettre à marcher. Au bout d'un quart d'heure, je suis à bout de souffle. Je suis parti trop vite. Mon cœur d'informaticien va exploser. Mes poumons, plus habitués aux rythmes des sports de ma console Wii, crient AU SECOURS. Et cette petite voix lancinante dans ma tête qui se fait de plus en plus pressante : "et si tu marchais un petit peu, juste pour reprendre des forces ?".

Une demi-heure s'est écoulée. Le soleil tape fort, je transpire beaucoup. Soudain, je comprends que de mettre un bandana pour éviter la transpiration dans les yeux n'est pas forcément une bonne idée. J'étouffe. Je suis une cocotte-minute. J'enlève le bandana. Cela va un peu mieux. A chaque carrefour, un groupe de personne de l'organisation m'encourage en applaudissant et en criant "Well done ! Come on !". C'est fou le bien que cela peut faire. Je leur réponds en français un "Merci ! Merci beaucoup !" qui les fait rire. J'entends parfois en retour un "bienvenue !" ou "bonjour !". Le public nous encourage également. Je cours depuis 1/2h et j'ai l'impression que ça fait une éternité.

Les panneaux indicateurs sont en miles. J'ai vu passer le panneau des 17 miles. J'ai vu aussi celui des 19 miles. Des repères pour les marathoniens individuels... Mais à chaque fois, je suis incapable de répondre à la seule question qui m'intéresse : combien me reste-t-il à faire avant le prochain relais...

Une table de ravitaillement se profile. Un homme au milieu du chemin tient des bouteilles : deux bouteilles d'eau dans une main et deux bouteilles de Gatorade colorées dans l'autre. Je lui crie "orange" et il me tend un Gatorade à l'orange. Je ne savais pas que c'était a priori réservé aux marathoniens individuels. J'aime le sucre, on ne se change pas et les mauvais taux de ma dernière analyse sanguine sont le cadet de mes soucis. J'arrive encore à respirer, à boire maladroitement et à courir. Je me refuse à abandonner la bouteille au bord du chemin, malgré les centaines de cadavres déjà présents. Je trouve une poubelle ad hoc quelques centaines de

mètres plus loin. Je suis très fier de moi. Petite victoire sur moi-même.

La voix dans ma tête hurle de plus en plus fort : "MAIS ARRÊTE DONC DE COURIR ET MARCHE". Une grande ligne droite me permet de voir qu'il reste encore beaucoup à courir. Mon moral baisse. La ligne droite est en fait une montée. Mon moral baisse encore. Un coureur me double comme une fusée. Mon moral baisse et je me mets à marcher. Un mètre, deux mètres, dix mètres.

Il paraît qu'au bout d'un certain temps d'efforts, le corps du coureur à pied sécrète des substances euphorisantes qui concourent au plaisir du sportif. Soit je n'arrive pas à attendre assez longtemps, soit mon bonheur habituel est tel que je suis déjà saturé d'euphorie, soit mon corps ne sait pas sécréter ce type de produit car j'ai plutôt le sentiment d'une souffrance qui augmente avec le temps d'efforts !!!

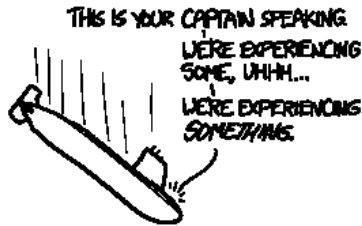
Pour moi, courir, c'est surtout courir contre soi-même. Après dix mètres de marche, j'arrive à redonner l'impulsion mentale nécessaire pour reprendre un rythme de course, quel qu'il soit. Je suis un boulet, je suis une brêle, je suis un mauvais, mais purée, ces 7,2 km, je les ferai en courant !

Je double un marcheur. Je l'entends se ressaisir et reprendre la course. Il me double. Je le redouble un peu plus loin quand il s'est remis à marcher. Le jeu se répète encore. Je regarde ma montre : cela fait 45mn que je cours au maximum de mes possibilités. L'arrivée doit être proche. J'accélère. Je suis en vrac, j'ai mal partout. Le temps s'étire. J'entends le haut-parleur qui annonce aux relayeurs le numéro du coureur qui arrive. J'accélère. J'entends mon numéro. Je vois ma prochaine relayeuse. Je lui tends le bracelet. C'est fini. Je m'assois dans l'herbe et je cherche mon souffle. 7,2 km en 49 mn...

J'ai probablement été le boulet de mon équipe de filles, mais nous avons fait chacun notre premier marathon à cinq en 4h30 et notre classement général n'est pas ridicule.

Maintenant, deux jours après cette aventure, j'ai les deux jambes dures comme du bois. Le manque d'entraînement sans doute ;-)

Pour moi, courir, c'est avant tout courir contre soi-même.



Source image what-if.xkcd :
<http://what-if.xkcd.com/138/>

Conversation entre un libraire et un expert judiciaire

Il m'arrive d'être contacté par email par un internaute qui m'interpelle sur un point et, parfois, une conversation épistolaire s'amorce, donnant lieu à des échanges intéressants. Ce fut le cas avec [Hoper](#), et cela donne ce billet à quatre mains, publié simultanément sur nos blogs respectifs.

[Hoper](#) :

Bonjour Zythom,

Je vais commencer par me présenter à minima. Informaticien, [un peu blogueur](#), et un peu "énervé" quand il s'agit de défendre nos libertés, j'ai découvert votre blog en 2011. Je vous lis encore à l'occasion, et j'aurai quelques questions sur votre activité.

Par exemple la personne qui avait "défacé" votre blog vous reprochait de ne pas être suffisamment du côté de la "justice". Vous êtes-vous déjà demandé si, au contraire, vous ne le seriez pas déjà un peu trop ? Je m'explique.

Nous vivons une époque merveilleuse où tous les citoyens sont surveillés en permanence (prism, affaires des journalistes sur écoute, etc.) et où les lanceurs d'alertes concernant la surveillance excessive (et illégale) mise en place par nos gouvernements "démocratiques" sont traqués comme des terroristes.

Pendant ce temps Vous fouillez dans la vie privée des gens. A la requête d'un juge certes, mais tout de même. Tout le monde est manipulable... Ça ne vous met pas mal à l'aise ?

[Zythom](#) :

Bonjour Hoper,

Je vais me présenter rapidement pour les lecteurs de votre blog : je suis ingénieur en informatique, je travaille comme directeur informatique et technique dans une grande école d'ingénieurs où je sévissais auparavant comme enseignant-chercheur, et j'exerce en parallèle l'activité d'expert judiciaire en informatique. Je raconte ma vie sur mon blog perso : "[Zythom - blog d'un informaticien expert judiciaire](#)". Je vais essayer de répondre correctement à vos questions...

Lorsqu'un crime est commis, et qu'un ordinateur est trouvé sur place, il me semble normal de saisir l'ordinateur et de l'examiner. Pour l'expert judiciaire qui sera affecté à cette tâche, "examiner" signifie répondre à un ensemble de questions posées par un magistrat instructeur. Souvent, surtout quand il s'agit de chercher des preuves photographiques, cela nécessite de plonger dans la vie privée des utilisateurs de cet ordinateur.

En modifiant les éléments d'identification des affaires dans lesquelles j'interviens, en "romançant" pour reprendre le mot du procureur dans [l'Affaire Zythom](#), je parle souvent sur mon blog de mes interventions dans la vie privée des gens. Par exemple, dans les billets "[Une vie privée](#)", "[Je cherche la vérité](#)", "[Emilie 4 ans](#)" ou "[Ad nauseam](#)". Je concluais d'ailleurs ce dernier billet ainsi :

Quand j'ai un doute, ou que je me sens mal à l'aise, je ne dois pas me contenter de dire : je mets en annexe, les autres feront le tri. Il faut décider ce qui relève de la mission. Il faut décider ce qui relève de la dénonciation de crime.

Le reste, c'est la vie privée.

Et parfois, c'est dur de faire les choix, quand on sait qu'on peut briser une vie.

Mais briser la vie de qui ? Celle de l'utilisateur du disque dur ? Celle de sa prochaine victime s'il y en a une ? La mienne ?

Ce qui montre que j'ai parfaitement conscience des risques que j'affronte.

Mais j'assume pleinement cette responsabilité. J'ai choisi de prêter le serment suivant : "*Je jure d'apporter mon concours à la Justice, d'accomplir ma mission, de faire mon rapport, et de donner mon avis en mon honneur et en ma conscience.*" et j'entends bien y rester fidèle.

Puis-je être l'objet d'une tentative de manipulation ?

Ma réponse est simple : oui, tout le temps.

Je vais développer un peu.

Nous vivons dans une société où chacun est libre de déposer une plainte et de demander l'action de la justice. Certains abusent de cette possibilité pour, par exemple, déstabiliser un concurrent, chercher à obtenir des informations commerciales confidentielles, etc. L'expert judiciaire peut se retrouver au milieu de conflits violents, par exemple entre deux entreprises qui veulent se détruire mutuellement. Chaque partie cherche à obtenir de l'expert un rapport favorable à sa cause.

L'expert judiciaire doit résister à des tentatives d'intimidation, voire même à des attaques physiques. Je décris [dans ce billet](#) (« L'expert judiciaire ou le collaborateur biodégradé », tome 4) une agression dans un dossier qui a entraîné la ruine de l'expert judiciaire !

Vous le voyez, l'expert judiciaire n'a pas tous les pouvoirs. Son action est encadrée par la loi, et son rôle consiste à donner un avis sous la forme d'un rapport. Et le magistrat n'est pas tenu de suivre cet avis. Les avocats peuvent également "attaquer" le rapport de l'expert, avant son dépôt (par la rédaction de dires), ou après son dépôt en demandant une contre-expertise. Je pratique d'ailleurs beaucoup ce genre d'activité en lien avec des avocats, ou des associations, pour les aider à rédiger des dires. J'en parle dans ce billet intitulé "[Contre-expertise](#)" (cf. tome 6 ci-avant). Je vous invite à le (re)lire et j'en reporte ici la conclusion :

Enfin, chaque citoyen peut se voir accusé injustement d'un fait dont il est innocent. Beaucoup croient que la découverte de la vérité s'effectue "automatiquement" et "gratuitement" à travers des enquêtes sérieuses menées avec tous les moyens (humains et financiers) d'une justice moderne. Ils se trompent lourdement.

Sur le chiffrage des données, j'ai toujours encouragé mon prochain à l'utiliser pour protéger sa vie privée, soit avec des VPN ("[Vie privée, vie publique](#)", "[Fournisseurs de VPN](#)", ou "[SSTIC](#)

[OpenVPN Synology Freebox et iPhone](#)"), soit avec des [containers TrueCrypt](#).

[Hoper](#) :

"Lorsqu'un crime est commis, et qu'un ordinateur est trouvé sur place, il me semble normal de saisir l'ordinateur et de l'examiner."

Pour moi les choses sont loin d'être aussi simples.

Je m'interroge justement sur ce sujet. Pardonnez je vous prie ma totale méconnaissance du droit (je serai bien en peine d'expliquer la différence entre un crime et un délit par exemple, tout en sachant qu'elle est fondamentale légalement parlant).

Je m'interroge donc, sur ce qui peut autoriser un juge à demander l'analyse d'un équipement informatique. Quels sont les actes suffisamment graves pour justifier une telle intrusion dans la vie privée ? Sachant que, sauf erreur de ma part, Lopsi 2 autorise une intrusion à distance dans des cas aussi bénins que l'assistance aux sans papier, je me dis que, quelle que soit la faute commise, un juge pourrait décider de saisir mon matériel informatique.

Est-ce le cas ?

[Zythom](#) :

Je ne suis pas juriste, je ne peux pas prétendre connaître la bonne réponse à cette question, mais l'action des magistrats est encadrée par la loi. Ils ne peuvent pas faire ce qu'ils veulent et, de plus, les décisions qu'ils prennent peuvent être contestées, avec l'aide d'un avocat qui vous assistera dans la défense de vos intérêts.

Pour une réponse plus pertinente, il faudrait poser la question à un magistrat, ou au moins à un juriste.

[Hoper](#) :

Autre question, même si cela tourne un peu autour du même sujet. Êtes-vous d'accord avec **toutes** les lois françaises ?

Si vos conclusions d'expert conduisaient un jour à inculper une personne pour quelque chose que vous ne condamneriez pas vous personnellement... (ou alors une beaucoup plus lourdement que vous ne l'auriez fait) Cela ne vous poserait pas un problème ?

En résumé, je trouve qu'humainement et moralement parlant, vous prenez beaucoup de risques pour une justice qui semble (vue de loin hein) de moins en moins "juste". Vous ne le faite pas pour l'argent. Pas non plus pour vos pairs qui vous attaquent en justice, tentant de limiter de façon totalement inadmissible votre liberté d'expression.

Alors... pourquoi ?

Zythom :

Il m'arrive d'avoir dans un dossier une faiblesse humaine : ma sensibilité, mon "opinion", mes préjugés s'imposent à moi et brouillent mon avis (je rappelle que je ne "juge" pas une personne, je donne un avis technique en réponse à des questions qui me sont posées).

Heureusement, la méthode scientifique est là pour m'aider à garder la tête froide et à me défaire de ce type de réflexes primaires.

Un expert judiciaire est là pour donner un avis scientifique sur un point technique. Son opinion politique, ses préjugés sur le comportement de telle ou telle partie à la cause n'importent pas. Il en va de même pour les magistrats.

Et de même que la science peut se tromper, l'expert judiciaire peut également se tromper. J'ai alors à faire face à ma conscience. D'où la référence à ce concept dans le serment de l'expert judiciaire : *"donner mon avis en mon honneur et en ma conscience."*

Je ne suis pas d'accord avec toutes les lois françaises. J'ai en détestation le concept même de copyright et j'ai un avis très critique sur

la HADOPI (soit ironique comme dans ces deux billets [ici](#) et [là](#), soit plus technique comme dans [ce billet](#), intitulé « Le rapport Znaty sur Hadopi et TMG », tome 5).

Alors pourquoi est-ce que je souhaite mettre mes compétences techniques à la disposition de la justice ? Je pense qu'il faut d'abord préciser un point : il y a d'un côté les lois, votées par les hommes et femmes politiques que les citoyens ont élus, et d'un autre les magistrats qui constituent l'un des éléments clefs de l'institution judiciaire. Je me méfie comme de la peste du mot "justice" qui a plusieurs sens, et je vous invite à lire sur ce point l'[excellent article de Wikipédia](#), dont voici un extrait :

"La justice est un idéal souvent jugé fondamental pour la [vie sociale](#) et la [civilisation](#). En tant qu'institution, sans lien nécessaire avec la notion, elle est jugée fondamentale pour faire respecter les lois de l'autorité en place, légitime ou pas. La justice est censée punir quiconque ne respectant pas une loi au sein de sa société avec une sanction ayant pour but de lui apprendre la loi et parfois de contribuer à la réparation des torts faits à autrui, au patrimoine privé ou commun ou à l'environnement."

Si une mission me pose un problème de conscience, j'ai la possibilité de la refuser. Pour l'instant, ce n'est jamais arrivé.

Je ne travaille effectivement pas pour la justice (en tant qu'institution) pour l'argent, ni pour mes pairs. Je travaille pour l'institution judiciaire parce que cela me rapproche de l'univers de ma femme qui est avocate.

Et cela me paraît une excellente raison ;-)

[Hoper](#) :

Dans plusieurs billets, vous semblez avoir des doutes sur vos activités. Je ne parle pas seulement de la gêne que vous décrivez lors des perquisitions, mais de l'activité en général.

Je cite :

"Après tant de coups, après tant de désillusions, je me suis rendu compte que les seuls dossiers qui pouvaient avoir mérité d'avoir eu envie de devenir expert judiciaire étaient les énigmes posées par les scellés que l'on me confie dans les instructions. Et comme la plupart du temps, il s'agissait de recherche d'images ou de films pédopornographiques, je me dis que je suis un con."

C'est tout de même assez fort comme paragraphe...

Pouvez-vous développer ? Car ici, en substance, on comprend "Tout ce que j'ai fait n'a pas servi à grand-chose d'autre que de me fournir des défis techniques à relever.

Avouez qu'il y a alors de quoi se poser des questions.

Zythom :

C'est un peu la raison d'être de mon blog : l'écriture me permet de travailler sur mes frustrations, sur mes angoisses et sur mes faiblesses. Et parfois, cela donne une phrase un peu désabusée.

Travailler pour l'institution judiciaire, c'est mettre ses compétences au service de la justice. Mais c'est aussi découvrir un univers très contraint, très attaqué et très peu soutenu, avec des moyens financiers d'un autre âge. C'est dur de voir que l'idéal que l'on peut avoir sur la Justice n'est pas soutenu par les élus, ni par le justiciable.

Enfin, il m'a fallu aussi un certain temps pour digérer le fait que, non, l'expert judiciaire n'est pas accueilli à bras ouvert par une institution reconnaissante de son implication citoyenne, non, tous les experts judiciaires ne sont pas compétents, non, l'amour de la technique n'est pas suffisant pour être un bon expert judiciaire, etc.

Quand j'ai commencé l'activité d'expert judiciaire, je voulais aider la justice à découvrir la vérité. Maintenant, je suis plus intéressé par les défis techniques, tout en sachant que cela aide à découvrir

la vérité. C'est gagnant/gagnant. Mais parfois, quand le dossier est difficile à digérer, en particulier en matière pédopornographique, j'ai plus de mal.

L'écriture sur le blog m'aide beaucoup, et bien entendu le soutien de mes proches.

Hoper :

Vous indiquez que vous avez la possibilité de refuser une mission qui vous semblerait vraiment contraire à vos principes.

C'est une très bonne chose en théorie. Mais avez-vous réellement tous les éléments pour faire un choix éclairé dans la pratique ?

D'après les exemples que vous donnez, on a plutôt l'impression que vous n'avez qu'une connaissance très limitée du contexte de la mission proposée, peu ou pas d'éléments techniques, et que l'on vous demande généralement de donner une réponse "la toute de suite maintenant".

Ne pensez-vous pas, dans ces conditions, qu'il serait possible de regretter un jour d'avoir accepté une mission ? Pas parce qu'elle vous prendrait plus de temps que prévu, ni parce qu'elle nécessiterait des compétences spécifiques, mais bien parce qu'elle vous poserait un problème éthique ?

Zythom :

Vous avez la possibilité de refuser une mission dès votre désignation par un magistrat. Personne ne peut vous obliger à accepter une mission, sauf cas exceptionnel que je n'ai jamais connu.

Une fois votre mission acceptée, si des événements qui vous étaient inconnus posent un problème éthique, il est toujours possible de se déporter, en expliquant les raisons aux parties et au magistrat. Le plus tôt est le mieux, surtout si des frais importants doivent être engagés. Le cas s'est présenté plusieurs fois pour moi quand je me suis rendu compte que j'avais été en relation

client/fournisseur avec un participant à la première réunion d'expertise, et que ce fait pouvait mettre en cause mon impartialité.

Hoper :

Concernant le chiffrement, vous encouragez donc son utilisation afin que chacun puisse protéger sa vie privée. Vous le faite en sachant qu'un chiffrement correctement implémenté vous empêcherai de remplir une mission qui vous aurait été confiée.

N'y aurait-il pas, dans cette attitude, une sorte de contradiction ?

Zythom :

Il n'y a pas de contradiction à être pour la défense de la vie privée, et être amené à devoir entrer dans la vie privée des gens.

Imaginez un policier qui encourage à s'équiper de portes blindées pour empêcher les cambriolages, alors qu'il doit lui-même forcer des portes dans le cadre d'enquêtes criminelles (par exemple).

Hoper :

Quand je m'interroge sur le respect de la vie privée, vous me répondez :

L'expert doit se limiter à la mission qui lui a été confié. Tout ce qui n'entre pas dans le cadre de cette mission doit être écarté.

C'est très bien mais que faire si, a contrario, la mission donnée est trop limitée ?

Exemple : "Trouver toutes les images pédopornographiques présentes sur cette machine"... En oubliant de vous demander d'en chercher la provenance ! (téléchargement effectué par l'utilisateur ou "piratage" etc.)

Si les questions qui vont ont été posées ne sont pas assez nombreuses, il y a le risque d'aboutir à un mauvais jugement non ?

[Zythom](#) :

Oui. C'est pour cela qu'il arrive souvent que le magistrat, ou l'enquêteur, me contacte pour discuter avec moi des missions, avant leur rédaction définitive.

Si ce n'est pas le cas, et si les missions sont imprécises, il est toujours possible de contacter le magistrat après coup pour se faire préciser un point obscur. Il est malheureusement difficile d'arriver à joindre un magistrat, et quand on y arrive, il vaut mieux aussi que ce soit pour une bonne raison (il n'est pas là pour vous expliquer un point de procédure).

Mais si l'affaire n'est pas claire, que les parties sont de mauvaises fois, que l'expert n'est pas très bon, que les missions sont imprécises et que le magistrat s'appuie un peu trop sur son rapport pour prendre sa décision, alors oui, cela peut aboutir à de mauvais jugements. C'est je crois, l'origine du proverbe : "*Un mauvais arrangement vaut mieux qu'un bon procès*".

Heureusement, c'est rare, car les experts sont de mieux en mieux formés aux procédures juridiques, et les avocats, enquêteurs et magistrats de plus en plus compétents en matière informatique.

[Hoper](#) :

Concernant les erreurs, manipulations etc., vous me rappelez très justement que l'on peut demander (qui paye ! ?) une contre-expertise. Bien. Mais ce nouvel expert devra-t-il répondre exactement aux mêmes questions, ou sa mission peut-elle être élargie (cf. exemple ci-dessus) ?

[Zythom](#) :

Quand vous n'êtes pas content d'une expertise, il vous est possible d'en demander une autre au magistrat. C'est la contre-expertise. Si la demande n'est pas solidement argumentée, le magistrat va la refuser pour éviter les dépenses inutiles, car en général toutes ces expertises sont payées par l'une des parties qui fait l'avance (elle sera remboursée si elle "gagne" le procès, par la partie perdante, je simplifie). Si la demande est acceptée, la mission peut être élargie, si le magistrat le décide ainsi.

Sinon, vous pouvez toujours demander une expertise privée, à vos frais, pour venir critiquer scientifiquement le rapport de l'expert judiciaire. Je me suis d'ailleurs fait une spécialité en la matière, puisque je traite aujourd'hui plus d'expertises de ce type que d'expertise judiciaire. Mais tout cela à un coût, que l'État ne prend pas en charge.

[Hoper](#) :

A propos des experts maintenant. Vous expliquez vous même ne pas réellement savoir comment ils sont choisis, comment leur compétences sont validées etc. Soyons optimistes, et partons du principe qu'une très grande majorité d'experts sont effectivement très compétents dans leur domaine d'expertise. Il reste forcément des cas isolés, des personnes qui n'auraient pas eu être inscrite sur les listes.

J'imagine qu'après plusieurs échecs (conclusions remises en cause par des contre expertises justement), la question de leur "suppression" doit se poser ? Ça arrive souvent ? Sait-on pourquoi une personne n'est plus sur la liste ?

[Zythom](#) :

Auparavant, le seul moyen de faire sortir un mauvais expert des listes était une procédure de radiation, procédure plutôt infamante. Aujourd'hui, puisqu'il faut demander tous les cinq ans sa réinscription sur la liste, beaucoup d'experts disparaissent des listes, soit parce qu'ils ne redemandent pas leur inscription, soit parce que leur demande de réinscription est refusée. C'est plus discret et moins infamant. Mais la procédure de radiation existe toujours.

[Hoper](#) :

Que se passe-t-il si un expert judiciaire tombe sur une difficulté technique qu'il n'arrive pas à résoudre seul. A-t-il le droit de "faire appel à un ami" ? Je suppose que le secret de l'instruction l'en empêche ? Même si il s'agit de demander l'aide d'un autre expert judiciaire ?

[Zythom](#) :

L'expert termine toujours son rapport par une phrase affirmant qu'il a rempli seul et en personne sa mission. Donc il n'a pas le droit de faire intervenir de son proche chef une autre personne dans la procédure. Mais il lui est possible de se documenter auprès de tierces personnes, sans livrer le détail du dossier. Il n'est pas interdit de poser une question purement technique sur une liste de diffusion, ou sur Twitter. Cela m'arrive souvent. On ne peut pas tout savoir, mais on doit savoir qu'on ne sait pas tout ;-)

Si par contre, je dois faire intervenir une société dans l'analyse d'un disque dur parce que celui-ci ne fonctionne plus, je dois demander auparavant l'autorisation du magistrat qui m'a désigné. Le rôle de l'expert judiciaire est bien encadré.

[Hoper](#) :

Le fonctionnement de la justice en France est quelque chose de très mal connu par l'écrasante majorité de la population (moi le premier). Inconnue et répressive, il est logique que l'administration judiciaire fasse "peur". D'où l'importance des blogs (le vôtre, celui de Maître Eolas et de beaucoup d'autres). Merci beaucoup pour le temps passé à nous éclairer sur ces sujets.

[Zythom](#) :

Merci Hoper pour cet échange qui aborde des questions intéressantes qui me sont souvent posées lors des différentes rencontres que j'ai pu avoir IRL avec des internautes, mais que je n'avais jamais abordées ici. Et merci aussi pour le temps passé.

Le tri

Me voilà encore une fois devant un ordinateur que je dois analyser. Les informations transmises par l'Officier de Police Judiciaire me disent qu'une lointaine autorité a signalé à Interpol que l'ordinateur aurait servi à télécharger des images pédopornographiques.

Moi, je ne suis qu'un tout petit maillon de la chaîne : je n'ai pas saisi l'ordinateur, je ne connais pas son contexte de connexion à internet, j'ai simplement une unité centrale saisie pas loin de chez moi et posée sur mon bureau, avec pour mission de dire si elle contient des images pédopornographiques et si possible comment elles sont arrivées là...

Bien, bien, bien.

Je prends des photos du scellé, comme j'ai vu faire dans les séries américaines. J'ouvre le scellé, je dépose l'unité centrale sur mon bureau. Elle sent la cigarette. Je prends des photos, puis j'ouvre l'unité centrale avec un tournevis, proprement pour ne pas laisser de marques. Je prends des photos de l'intérieur, puis j'enlève le disque dur. Enfin, je prends en photo le disque dur, je note ses caractéristiques, son modèle, son numéro de série. J'en fais une copie numérique bit à bit en priant pour qu'il ne rende pas l'âme à ce moment-là... Je dormirai mal cette nuit-là.

Le lendemain, je m'assure que la copie s'est bien passée, je remonte le disque dur dans l'unité centrale, je prends des photos, je range le scellé. Le vrai travail d'investigation peut commencer.

Les données du disque dur se présentent de plusieurs façons :

- bien rangées dans des ensembles qu'on appelle "des fichiers"
- en vrac partout ailleurs sur le disque dur.

Les fichiers non effacés sont accessibles via les tables d'allocation des fichiers. Les fichiers effacés sont, pour certains, encore accessibles via ces mêmes tables (qui se comportent comme des index

de livres). La majorité de ces fichiers proviennent des mécanismes de mise en cache des navigateurs. Quelques-uns viennent de la suppression de fichiers choisis par l'utilisateur. Puis il y a les "paquets de données" éparpillés sur le disque dur, référencés nulle part (la référence a été définitivement effacée). Ces paquets contiennent des traces de fichiers ayant un jour été "cohérents". On trouve de tout dans ces paquets, des bouts d'images, des bouts de téléchargements, des bouts de conversations, des bouts de fichiers systèmes, etc.

Une fois récupéré l'ensemble de toutes ces données (effacées, pas effacées, en fichiers ou en bout de fichiers), je me retrouve face à un Everest de données qu'il me faut trier. Je vous parle ici d'un tas de cinq cents mille fichiers.

Cinq cents mille.

Première étape : éliminer les fichiers "communs", ceux qui appartiennent de façon certaine au système d'exploitation ou aux applications connues. Pour cela, je vous recommande la "[National Software Reference Library](#)" qui contient plusieurs bases de données intéressantes.

Mais ensuite, il faut tout regarder.

Je commence par les plus gros fichiers : je tombe alors sur des films qu'il faut que je visionne. Je me tape en accéléré et par morceaux tous les grands blockbusters des cinq dernières années... Je regarde toutes les bases de données présentes sur le disque dur, et en particulier la base de registres, les fichiers logs du système et les bases de données des différentes applications. La plupart de ces bases sont codées en binaire de manière propriétaire par les éditeurs concernés. J'analyse chaque base : applications de messagerie, logiciel d'échange de données, chat, etc. J'obtiens la liste des connexions effectuées, les fichiers téléchargés, les données échangées...

Je continue mon tri.

Viennent ensuite les archives ZIP, 7Z et autres dont j'extrais les fichiers. 15 archives résistent et me demandent un mot de passe... que je cracke pour tomber sur du porno banal. [Internet, c'est pour le porno.](#)

Je continue mon tri.

Je regroupe toutes les images dans un ensemble de répertoires (Windows n'aime pas les répertoires contenant trop de fichiers). Je passe des soirées entières, pendant plusieurs semaines, à les regarder : mariages, soirées, vacances d'un côté, et tout le contenu porno des caches des navigateurs utilisés...

Je continue mon tri.

Il me reste quelques fichiers qui résistent à mon classement. Chacun représente un défi qu'il me faut relever. Surtout que pour l'instant, je n'ai rien trouvé de pédopornographique. J'ouvre les fichiers avec un éditeur hexadécimal. Je regarde leurs empreintes numériques, leur contenu. Je pense aux différents défis lancés par les conférences sur la sécurité informatique. Je me sens nul. Ici les fichiers illisibles sont simplement des images ou des fichiers word avec des entêtes corrompus.

Tout cela pour rien. Enfin, pas vraiment. Cela prouve l'innocence de l'utilisateur du PC, ce qui n'est pas rien. Pour moi, cet ordinateur est clean du point de vue de mes missions. Sur mon rapport j'indique que je n'ai trouvé aucune donnée pédopornographique. Je n'écris pas qu'il n'y en a pas. J'écris que je n'en ai pas trouvées. Ni trace d'un téléchargement qui pourrait laisser supposer la présence de telles données.

Et encore une fois, la fin de ce long tri ennuyeux me rend heureux : ma mission est terminée, et elle se termine bien. Il ne reste plus qu'à expliquer ma note de frais et honoraires, maintenant. Mais ça, c'est une autre histoire...

GERME

Depuis trois ans, je suis une formation au management. Comme beaucoup d'ingénieurs, j'ai toujours privilégié la connaissance et la compétence technique au détriment des autres qualités que doit avoir un bon "chef d'équipe". Le travail en équipe et l'animation d'équipe ne m'ont pas été enseignés lors de ma formation initiale maintenant lointaine. Et après 30 ans d'immersion dans la technique, il était temps de retourner à l'école, pour corriger ce que j'avais pu apprendre "sur le tas". Le management en fait partie.

Je suis allé voir la personne en charge des ressources humaines dans mon entreprise et elle m'a conseillé de prendre contact avec une animatrice de ce formidable organisme [qui s'appelle GERME](#).

Késako ?

GERME est une association loi 1901 qui est née d'une initiative de membres et d'animateurs de l'Association Progrès du Management (APM) en 1992 qui ont souhaité une approche de perfectionnement au management des entreprises pour leurs cadres de direction. L'association GERME a finalement été créée fin 1997 et constitue le réseau de référence pour les managers qui veulent développer et mettre en œuvre de nouvelles compétences en management. L'acronyme GERME signifie d'ailleurs Groupes d'Entraînement et de Réflexion au Management des Entreprises.

Les managers adhérents à GERME progressent et se développent par la formation, les mises en situation et le partage d'expériences au sein de groupes présents sur tout le territoire français, les Antilles et la Belgique. Chaque groupe compte de 15 à 20 cadres de direction qui se réunissent 8 fois par an pour suivre un cycle de formation, pilotés par des animateurs formés à la pédagogie GERME.

C'est pour moi l'occasion de prendre un peu de recul par rapport à la pression du travail, à l'urgence des problèmes que je rencontre au quotidien dans mon entreprise. C'est surtout pour moi un lieu

d'échanges en confiance. En effet, quoi de mieux que de rencontrer des personnes d'autres entreprises, ayant des responsabilités similaires, mais dans des métiers très différents, et de pouvoir se confier à eux, de pouvoir parler de ses propres faiblesses, erreurs et défauts en étant écouté sans se sentir jugé.

Une fois par mois, sur 8 mois sélectionnés judicieusement pour que tout le monde puisse participer, je rencontre des personnes qui sont devenues pour moi des camarades de galère, que je connais maintenant mieux que leurs collègues de boulot, et nous suivons une journée de formation animée par un conférencier sélectionné par le réseau GERME, sur un thème que nous avons collectivement choisi. Les thèmes se regroupent dans 4 axes pédagogiques : le manager et le monde, le manager et son entreprise, le manager et son équipe, et enfin le manager lui-même...

Pour vous donner une idée, voici quelques-unes des formations que j'ai suivies depuis 2011 :

- Comment gérer les personnalités difficiles ?
- Comment motiver son équipe ?
- Comprendre et manager la génération Y
- Anticiper et accompagner le changement
- L'attitude intérieure positive
- Prendre la parole en public et rester zen
- L'intelligence émotionnelle
- Comment mieux gérer son stress ?
- Humour et management
- Conduire le changement
- Décrypter la gestuelle pour rendre plus efficace sa communication
- La communication de crise, quelles relations avec la presse ?
- L'art de la répartie : comment réagir en toute situation ?
- Équilibre vie professionnelle vie privée

A chaque fois, le conférencier anime la journée en alternant présentation, mise en situation, exercices pratiques, échanges entre apprenants, etc.

Cela permet de recevoir des connaissances en provenance d'un professionnel expérimenté, de pouvoir les discuter et se les approprier, et surtout de confronter "entre nous" les expériences - bonnes ou mauvaises - des uns et des autres. Qui n'a pas eu à gérer une réunion houleuse, une personne qui réagit de manière désagréable, des problèmes d'ego ou un conflit au sein de son équipe de travail ?

J'apprends beaucoup sur moi-même au cours de ces formations. Elles ont contribué - j'espère - à améliorer mon contact avec les autres, que ce soit dans mon univers professionnel où l'on est parfois prompt à critiquer l'interface chaise-clavier, dans ma gestion des réunions d'expertise où l'écoute est importante ainsi que la bonne gestion de crise, ou dans ma tâche de conseiller municipal, je pense en particulier à l'animation des réunions publiques.

Les valeurs GERME, sur lesquelles travaillent tous les adhérents, sont les suivantes : Progrès, Respect, Ouverture, Confiance, Humilité et Ensemble (PROCHE). Elles illustrent bien le mode de fonctionnement du groupe GERME auquel j'appartiens. Elles permettent de développer et mettre en œuvre de nouvelles compétences en management. Elles permettent d'apprendre à se connaître pour accepter ses limites et renforcer ses points forts.

En septembre 2013, il y avait 87 groupes GERME réunissant 1310 adhérents. Les groupes accueillent des cadres de direction associés à la réflexion et aux décisions stratégiques : cadres en responsabilité d'équipes, cadres en responsabilité transversales et parfois des dirigeants de TPE. Les adhérents sont accueillis dans un groupe en veillant à la diversité des fonctions et à la non-concurrence des entreprises représentées. Vous trouverez plus d'informations sur le site de l'association : <http://www.germe.com> N'hésitez pas à entrer en contact avec un animateur proche de vous ou directement avec l'équipe d'accueil de l'association. Les formations sont prises en charge par votre entreprise.

J'avais beaucoup d'idées reçues sur le management, principalement par méconnaissance. J'imaginai que certaines personnes avaient une sorte de qualité naturelle innée de "leader" charismatique, ou d'autres l'insupportable comportement de "petits chefs". Je pensais que les cours de management consistaient en un ensemble de "trucs" pour manipuler les gens et en augmenter la productivité. J'avoue être allé un peu à reculons aux premières formations, moi le scientifique pur cru.

Au final, j'apprends à être plus ouvert, responsable, engagé, en constant perfectionnement, capable de comprendre mon environnement avec du recul, acteur et diffuseur de progrès au sein de mon entreprise, et acteur du changement.

Mes collègues ont constaté le changement. J'ai pu apprécier mon évolution dans la conduite des réunions d'expertise judiciaire. Même les étudiants sentent que j'ai changé en mieux. Même mes enfants...

Il me reste à mettre tout cela en pratique avec les élections municipales qui s'annoncent...

J'en parlerai sûrement ici.



Ma petite entreprise

J'ai décidé de créer ma propre entreprise.

Ouaip, rien que ça.

J'ai un métier qui me fait vivre, qui me passionne et qui me demande chaque jour d'être au top. Mais l'activité d'expert judiciaire en informatique, que je mène en parallèle, m'a fait découvrir un univers qui m'intéresse beaucoup, et pas uniquement parce que mon épouse est avocate. Seulement voilà, les expertises judiciaires, c'est bien, mais vu comment évolue le budget de la justice, les magistrats ordonnent de moins en moins d'expertises, et les Officiers de Police Judiciaire sont de plus en plus compétents pour mener les investigations techniques dans leurs affaires.

Pour autant, avec la complexité croissante de l'informatique, et la tendance à la judiciarisation de la société, le nombre de litiges techniques va augmenter. Le budget de la justice étant de plus en plus contraint, l'expertise judiciaire sera de plus en plus cruciale, et décisive, d'autant plus qu'elle sera rarement suivie d'une contre-expertise. Il est donc important que chaque partie soit accompagnée tout au long de l'expertise, mais également après, par un expert privé.

En 2010, j'ai décidé de tester un peu [l'activité d'expert freelance](#). Il se trouve que depuis cette période, mon chiffre d'affaire concernant cette activité n'a fait qu'augmenter, au point de dépasser cette année celui de mes activités d'expert judiciaire. Je donne un exemple d'expertise freelance dans ce billet intitulé "[Contre-expertise](#)" (cf. tome 6 ci-avant).

Il est temps maintenant de structurer cette activité, et en particulier de déterminer précisément les services que je peux proposer et les faire connaître au public approprié. Ce blog perso sera l'un de mes outils de communication. Je compte sur vous pour en parler autour de vous ;-)

Les services que je propose :

1) Assistance technique pendant les réunions d'expertise judiciaire.

En complément de l'avocat qui est l'expert en droit qui s'assurera que vos intérêts sont bien défendus d'un point de vue juridique, et qui établira la stratégie juridique, il est souvent intéressant de s'adjoindre les conseils d'un expert technique qui connaît et comprend parfaitement les problèmes informatiques mis en jeu, mais aussi les procédures d'expertises judiciaires et leurs pièges. L'expert judiciaire en charge des réunions d'expertise est souvent très content d'avoir à faire à des personnes qui parlent le même langage que lui et en comprennent toutes les subtilités. Je jouerai le rôle de facilitateur entre mon client et l'expert judiciaire, au mieux des intérêts de mon client.

2) Assistance dans la rédaction des dires.

Il existe de plus en plus d'avocats parfaitement compétents en matière informatique, mais ils sont encore trop peu nombreux. L'art de l'avocat est d'assurer la bonne défense *juridique* de son client, et pour compléter cela, certains n'hésitent pas à faire appel à un expert *technique* pour étudier tous les éléments techniques laissés éventuellement en suspend par l'expert judiciaire. L'expert judiciaire est seul devant toutes les parties, et il doit être soutenu dans sa recherche de la vérité par un débat contradictoire qui a lieu avant le dépôt de son rapport, et en particulier par l'analyse de son pré-rapport. Il faut éviter les zones d'ombre et souvent plusieurs experts valent mieux qu'un pour éclairer un dossier dans toutes ses dimensions. Il ne s'agit pas d'attaquer l'expert judiciaire pour le faire trébucher, mais de lui permettre d'être exhaustif dans l'accomplissement de ses missions, *avant* la remise de son rapport définitif.

3) Analyse critique d'un rapport d'expertise judiciaire.

Les différentes réunions d'expertise ont eu lieu, le pré-rapport a été discuté avec des dires et leurs réponses, et le rapport définitif a été remis au magistrat. Et ce rapport vous est très défavorable, d'une manière qui vous semble excessive. Votre avocat sait que l'affaire est mal engagée et souhaite mettre toutes les chances de votre côté. Il n'est plus alors question de peser le pour ou le contre

sur la question de savoir s'il faut engager des frais pour se faire assister par un expert technique pendant les phases précédentes. La défense est aux abois, il faut faire analyser le rapport d'expertise judiciaire, non plus sous l'angle du droit, mais sous l'angle purement technique. C'est le type de service qui m'est le plus demandé, et en général en urgence.

Si l'expert judiciaire est compétent, ce qui est le plus souvent le cas, je ne peux que faire l'éloge de son travail et vous aider à faire le deuil de vos prétentions.

Mais parfois, comme le rappelle Madame Marie-Claude MARTIN, vice-présidente du TGI de Paris, qui a publié dans la revue "[Experts](#)" (numéro 73 de décembre 2006), un excellent article intitulé "la personnalité de l'expert" :

"[...] plusieurs comportements sont susceptibles d'être observés :

- "*L'expert sans problème*" : Je lis la mission, elle rentre parfaitement dans mes attributions, je l'accepte.

- "*L'expert aventureux, ou téméraire, ou intéressé*" : La mission ne paraît pas relever de ma compétence, mais elle m'intéresse ; je prendrai un sapiteur ultérieurement [...]

- "*L'expert optimiste qui dit toujours oui*" : Je suis surchargé, je prends quand même cette mission, je me ferai aider au besoin par l'équipe qui m'entoure [...].

- "*L'expert stressé qui ne sait pas dire non*" : Je suis surchargé, mais si je dis non, je ne serai plus désigné et je vais rapidement me trouver sans mission.

Il y a donc des cas où le travail d'expertise peut ne pas avoir été parfait. Dans ces cas, je crois sincèrement que les avocats devraient s'adjoindre les services d'un expert privé.

Le public ciblé :

Les avocats constituent le public privilégié des services de que je propose. Je n'accepte une mission que si elle est validée/proposée par un avocat. Le travail en direct avec une partie, sans la caution juridique d'un avocat ne m'intéresse pas : chacun son métier, je ne peux pas vous guider dans les arcanes des procédures juridiques,

ni même vous conseiller dans ce domaine. Mon domaine à moi, c'est l'informatique.

Travailler avec un avocat, c'est pour moi la garantie de pouvoir me concentrer sur la partie purement technique. Dans la plupart des dossiers que j'ai déjà eue à traiter, l'avocat m'a surpris par la finesse de la compréhension qu'il avait des problèmes techniques soulevés. Mais tous les avocats ne sont pas aussi compétents en informatique que [Maître Eolas](#), ou [Maître Iteanu](#), ou [Maître Bensoussan](#). Il est souvent profitable pour le client de former un binôme avocat-expert performant. C'est ce que je vous propose.

Procédure de travail

Je travaille depuis plusieurs années avec des avocats aux six coins de la France.

J'aime les choses simples et efficaces : si vous n'êtes pas avocat, contactez d'abord votre avocat et discutez de votre affaire avec lui. Proposez-lui mes services et s'il estime en avoir besoin, dites-lui de me contacter. Si vous êtes avocat, contactez-moi par le biais [du formulaire contact de mon blog](#). Si vous savez utiliser une clef publique OpenPGP, la mienne se trouve sous le formulaire. Décrivez-moi le contexte de l'affaire. Je garantis une prise de contact rapide pour discuter des détails à suivre, des délais et du coût estimatif.

Le coût :

Je parlais des coûts des expertises privées quand je lançais timidement cette activité en 2010, [dans ce billet](#) : « Une expertise privée, combien ça coûte ? », tome 3. Je dois reconnaître que les tarifs ont évolué. Il faut maintenant [me contacter](#) pour les connaître.

En janvier 2013, j'ai publié un billet intitulé "[Pourquoi les experts judiciaires sont-ils si chers](#)". Je vais reprendre ici la blague que j'avais alors citée pour illustrer la réponse à cette question :

C'est l'histoire d'un ingénieur qui a un don exceptionnel pour réparer tout ce qui est mécanique. Après toute une carrière de bons et loyaux services, il part à la retraite, heureux.

Un jour, son ancienne entreprise le recontacte pour un problème apparemment insoluble sur l'une de leur machines à plusieurs millions d'euros. Ils ont tout essayé pour la refaire fonctionner et malgré tous leurs efforts, rien n'a marché. En désespoir de cause, ils l'appellent, lui qui tant de fois par le passé a réussi à résoudre ce genre de problème.

A contre cœur, l'ingénieur à la retraite accepte de se pencher sur le problème. Il passe une journée entière à étudier et analyser l'énorme machine. A la fin de la journée, avec une craie, il marque d'une petite croix un petit composant de la machine et dit "Votre problème est là..."

L'entreprise remplace alors le composant en question, et la machine se remet à marcher à merveille.

Quelques jours plus tard, l'entreprise reçoit une facture de 10 000 euros de l'ingénieur. La jugeant un peu élevée, elle demande une facture détaillée, et l'ingénieur répond alors brièvement :

- Une croix à la craie : 1 €
- Pour savoir où la mettre : 9 999 €.

La société paya la facture et l'ingénieur repartit dans sa retraite heureuse.

Je ne suis pas encore à la retraite, mais je SUIS cet expert qui sait où tracer la croix à la craie dans votre (pré)rapport d'expertise défavorable.

Et si le rapport d'expertise est parfait ET défavorable, je ne peux plus rien pour vous. Je vous le dirai en première lecture et il ne vous en coûtera rien.

Mais réagissez bien, réagissez vite !

Contactez-moi avant qu'il ne soit trop tard;-)

Ensemble, avec Vous et pour Tous, continuons !

Je parle assez peu de mon activité de conseiller municipal sur ce blog, alors qu'elle occupe de plus en plus de mon temps libre, surtout en ce moment avec la préparation des élections municipales de 2014.

J'ai toujours été intéressé par les événements de ma commune. Je suis lecteur assidu du journal communal et j'assistais épisodiquement à différentes manifestations plus ou moins folkloriques.

Jusqu'au jour où un voisin qui travaillait à la mairie m'a incité à assister à un conseil municipal. Tout à mon ignorance, je lui ai répondu "Ah bon, c'est public ?"... Et dès le mois suivant, je me retrouvais assis dans les rangs du public, enfin du public, plutôt à côté d'un tondu et d'un pelé, assistant à [mon premier conseil municipal](#).

Depuis, le virus ne m'a pas quitté, et quand il a fallu trouver des bénévoles pour aider à tenir les bureaux de votes supplémentaires (la population de la commune est en forte croissance), un conseiller de l'époque m'a foncé dessus en me disant : "puisque je vois que vous êtes toujours dans les rangs du public, je vous propose de m'aider à tenir le bureau de vote".

Tenir un bureau de vote, c'est être au cœur de la vie de notre démocratie. Mais c'est aussi de longues heures d'attente comblées par des discussions sur tous les sujets du moment. Ce qui fait que lors des dernières élections municipales, le candidat principal [est venu me trouver pour compléter sa liste](#). Je me suis donc retrouvé antépénultième sur sa liste (lire [ce billet](#) : « Antépénultième », tome 2). Normalement, je n'aurais pas dû être élu. Sauf qu'il n'y a pas eu d'autres listes face à nous...

Cette fois, pour les élections de 2014, c'est avec un bilan de 5 années de travail comme conseiller municipal que je m'apprête à participer à l'ensemble de la campagne électorale. C'est une découverte pour moi.

Tout d'abord, le maire sortant ne se représente pas, ayant passé plus de 30 ans à gérer sa commune et atteint un âge respectable. Il sait qu'il faut passer la main et ne pas faire le mandat de trop. Il passe le relais à son 1er adjoint qui est, me semble-t-il, très bien préparé à son futur rôle de 1er magistrat de la commune (s'il est élu). Il a donc fallu constituer une liste avec tous les conseillers qui souhaitent repartir pour 5 années de travail, et compléter la liste (car tous ne souhaitent pas repartir) avec des "petits" nouveaux.

Ma commune fait environ 5500 habitants et jouxte une ville très dynamique. La campagne municipale qui s'annonce, avec le départ du maire historique local, sera à l'image de la commune : dynamique ! C'est-à-dire qu'il y aura plusieurs listes qui vont s'affronter, et un futur conseil municipal avec une opposition, ce qui est une bonne chose.

Pour l'instant, sauf dans les grandes villes où les monstres politiques sont déjà en action, notre équipe (et celles de nos futurs concurrents) travaille discrètement et construit le programme. C'est une phase intéressante où de nombreuses idées sont exprimées, ce qui est très important surtout dans une liste quasi apolitique. Comme la liste est constituée majoritairement de conseillers sortants, nous partons des projets en cours et du bilan pour nous projeter sur l'avenir de la commune, ses difficultés et ses atouts.

Parallèlement au programme, il faut s'intéresser également à la "tactique" de campagne : quand présenter la liste au public, quand commencer les premières réunions publiques et sur quels thèmes du programme, quel slogan choisir, quelles affiches imprimer. Il faut également écrire les courriers, préparer le site internet, décider des outils technologiques, etc. Sachant que dans notre cas, il n'y a pas de conseiller en communication et que toutes les dépenses se font sur notre argent personnel.

J'assiste également aux manœuvres des listes adverses, aux tentatives d'espionnage, de débauchage de membres de la liste. J'ai ainsi

été approché pour faire partie d'une autre liste, ce que j'ai refusé poliment. C'est le bal des hypocrites ;-)

Tant que ce n'est pas le [bal de ardents](#)...

Chaque mois nous nous réunissons avec des tâches à faire, des sujets à trancher, des discussions à avoir. A chacun son travail, même si parfois, cela tient un peu de la "bricole". Moi, par exemple, je m'occupe du site internet... Je sais réserver des noms de domaine (check), je sais choisir des hébergeurs (check) et gérer les boîtes aux lettres du domaine (check), mais quant au choix du design du site, c'est une autre histoire... J'en suis à tester différents modèles tous prêts pour me faciliter la tâche !

Et début 2014 commencera la saison du combat politique : les réunions publiques et les confrontations d'idées ! Pour un timide compulsif comme moi, additionné d'une once d'agoraphobie, la période s'annonce difficile. Pensez-y avant d'envoyer une tomate sur l'orateur ;-)

Ensuite la liste sera déposée officiellement, avec une alternance stricte homme/femme. A ce moment-là, je saurai en quelle position je suis, et je verrai si j'ai une chance d'être élu, puis d'être adjoint ou simple conseiller.

Une chose me rend plus fort que bon nombre de mes concurrents : je n'ai aucune ambition. Si je ne suis pas élu, je serai ravi d'être dans l'opposition, même assis dans les rangs du public. La critique, c'est bien aussi. Et puis, c'est plus facile ;-)

Si je suis élu ET adjoint, je pourrai peut-être célébrer avec fierté le premier [mariage homo](#) de la commune ! Si je suis élu, je ferai en sorte que [nul vote électronique](#) ne vienne semer le doute dans notre démocratie locale. Si je suis élu, j'essaierai d'accueillir chaque nouvelle personne qui s'installe sur la commune [comme il se doit](#). Si je suis élu, je continuerai à lutter contre [l'insolence des riches](#). Si je ne suis pas élu, je continuerai quand même à consacrer un peu de temps [pour les moins chanceux d'entre nous](#) (lire aussi [ce bil-](#)

[let](#) : « La banque alimentaire », tome 2). Si je suis élu, j'espère pouvoir enfin [aller serrer la main des gens du voyage](#).

N'oubliez pas d'inciter les jeunes à s'inscrire sur les listes électorales avant le 31 décembre, et dites-leur de voter ! En attendant, je serai toujours ému par [les réactions des gens dans un bureau de vote](#) (lire aussi [ce billet](#) : « De l'autre côté du bureau », tome 3).

Quand je serai plus vieux, j'enlèverai mon béret devant l'urne de vote.

Votez pour moi !



Hôpital en mer

Le bateau file bon train sur la mer déchaînée. Nos voiles sont gonflées et [la gîte](#) est forte malgré [la grand-voile arisée](#). Le vent souffle fort et aucun autre voilier n'est sur l'eau. L'apprentissage de la voile doit se faire aussi dans de rudes conditions, et ce stage à [l'école des Glénans](#) ne fait pas exception.

Je vous parle des années 1980, une époque où nulle électronique n'avait sa place à bord des voiliers de cette école de voile prestigieuse (en dehors d'un récepteur radio pour prendre la météo). Nous mesurions la vitesse du bateau avec une planche lestée reliée à un bout à nœuds ([un loch](#)), la profondeur d'eau sous la quille [avec un plomb](#) et la force du vent avec [la forme des vagues](#). Les téléphones portables n'existent pas encore...

La mer est blanche de l'écume des vagues emportée par le vent. Il fait "vent frais" disent les marins. Nous sommes emmitouflés dans nos cirés jaunes, éclaboussés par les embruns. Nous avançons vent arrière, surfant sur les vagues en formation. C'est un moment d'émotions fortes, partagé par tout l'équipage.

Hélas, le barreur fait une faute. Une vague mal négociée déstabilise le bateau qui fait une embardée. Par vent arrière, la [bôme](#) est presque perpendiculaire au bateau. Elle hésite entre bâbord et tribord. Le moindre déséquilibre et elle change de côté. Cette manœuvre s'appelle [l'empannage](#). Mal maîtrisée, les conséquences peuvent être dramatiques : la bôme traverse brutalement le bateau en balayant tout sur son passage.

Dans notre cas, la bôme n'a percuté personne. Mais [l'écoute](#), qui relie la bôme au pont du bateau, a attrapé la tête d'un équipier et l'a brutalement projeté sur le coin de la cabine... Le choc sur la boîte crânienne a fait un bruit terrifiant et il reste inanimé sur le pont, ballotté par les vagues pendant qu'on reprend le contrôle du bateau.

Nous sommes deux penchés au-dessus de lui. Il est inconscient. Avec précaution, nous essayons de voir s'il a une blessure apparente. Nous découvrons du sang qui s'écoule de son oreille. J'ai 18 ans, mais je sais que ce symptôme ne présage rien de bon.

A ce moment-là, je me rends compte que nous sommes loin de tout, même si nous naviguons à vue des côtes, entre [l'île d'Houat](#) et Belle-Île. Je descends dans la cabine jusqu'à la table à carte. Je regarde la position approximative où nous nous trouvons, le point ayant été fait peu de temps auparavant. Il y a sur une carte marine pleine d'informations qui sont indiquées : [les amers](#) pour faire le point, la nature des fonds marins, le nom des ports... et, je m'en rends compte à ce moment-là, les hôpitaux !

Il y a un hôpital à Le Palais sur Belle-Île ! Je remonte annoncer la nouvelle à mon chef de bord qui, aussitôt, demande à l'équipage d'effectuer les manœuvres ad-hoc pour mettre le cap sur Le Palais. Je le remplace au chevet de mon camarade blessé. Je me place à genoux au-dessus de lui et cale sa tête sur mes cuisses pour essayer d'amortir le choc des vagues.

Le temps nous semble infiniment long. Belle-Île s'approche lentement de nous. Nous sommes tous très tendus, attentifs à faire fonctionner le bateau au plus vite. Mes cuisses me font mal à force de rester dans cette position. Je me sens inutile à l'avance du bateau et indispensable à empêcher l'impensable.

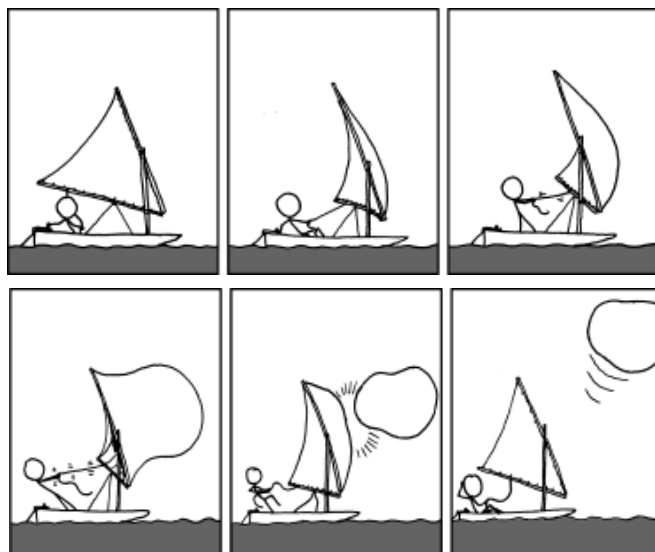
Nous entrons dans le port à pleine vitesse. Notre bateau, comme la grande majorité des bateaux de l'école de voile des Glénans de l'époque, n'a pas de moteur, pas même un moteur d'annexe. D'habitude, nous rentrons dans un port très doucement, propulsé par notre seule voile d'avant (en général [un foc](#)), après quelques lavoiments plus ou moins rassurants pour les propriétaires des bateaux amarrés. Cette fois-ci, nous arrivons toutes voiles dehors, à pleine vitesse, droit vers le quai principal.

Je revois encore le membre d'équipage debout à la proue et faisant office de [brigadier avant](#), lorsqu'il a bondi sur le quai et couru jus-

qu'au premier passant venu. Il l'a attrapé par le col et lui a hurlé dessus : "OÙ EST L'HÔPITAL ? OÙ EST L'HÔPITAL ?". Aujourd'hui, on parlerait d'agression caractérisée... Le pauvre ère lui a indiqué une direction dans laquelle s'est engouffrée mon camarade d'infortune. Un quart d'heure après, une ambulance venait chercher notre blessé. Nous étions tous hagards en la regardant l'emmener aux urgences.

Ce n'est que quelques jours plus tard que nous avons appris qu'il avait une fracture du crâne, et qu'il s'en sortirait sans séquelle.

Depuis ce jour, j'évite toujours de me trouver entre les écoutes et la cabine d'un bateau, surtout par vent arrière.



Source image xkcd : <https://xkcd.com/976/>

Journées réseaux 2013

Quelques jours après mon retour des "journées réseaux" ([JRES](#)) 2013 qui se sont tenues à Montpellier, voici le temps de faire un petit bilan de cette expérience.

Cela fait plusieurs années que je souhaite participer à cette manifestation qui regroupe une grande partie de la communauté des informaticiens travaillant dans les établissements d'enseignement supérieur et/ou dans la recherche, c'est-à-dire ma communauté professionnelle.

Et le hasard a fait que cette année, les organisateurs m'ont contacté via ce blog pour m'inviter à faire une présentation en séance plénière sur le thème de l'expertise judiciaire. Autant dire que je ne pouvais pas dire non...

Les premiers contacts ont été pris il y a longtemps ([janvier 2013](#)), et l'idée de parler devant mes pairs sous le pseudonyme Zythom était attrayante. Mais plus les mois passaient et plus la pression montait : ma présentation de généraliste de l'informatique allait-elle intéresser l'assemblée de spécialistes présente dans la salle ? Comment serait perçu mon souhait de participer à cette conférence sous pseudonyme ? Quel regard mes pairs allaient-ils porter sur moi ? Comment les quelques lecteurs du blog présents dans l'assistance allaient-ils réagir ?

Bref, plus le temps passait et plus je pétochais...

L'organisation des JRES 2013 s'est avérée impeccable du point de vue de l'invité que j'étais : une personne s'est attachée à s'assurer que je franchissais correctement les jalons, et me relançait avec patience quand je tardais sur la remise d'un livrable, notice de présentation, visuels de la présentation, détails pratiques sur le transport, l'hébergement, etc.

Et le premier jour de la conférence est arrivé : je me suis retrouvé assis dans la grande salle de l'opéra de Montpellier, avec 1500 per-

sonnes ! C'est vraiment à ce moment-là que j'ai senti la peur me nouer les tripes : j'allais devoir parler deux jours plus tard dans cette même salle, devant ce public de spécialistes des réseaux...

Il faut dire que la salle est très impressionnante.

Voici la photo prise depuis la scène avec mon smartphone, quelques minutes avant ma présentation :



Photo Zythom

Autant vous dire que j'étais dans mes petits souliers...

La veille, j'ai séché l'après-midi de présentations pour travailler et répéter ma présentation une dizaine de fois. J'ai quitté le "social event" du mercredi soir car j'étais encore trop stressé, ce qui fait que je n'ai pas pu profiter de la fête organisée pour les 10 ans des JRES.

Le mercredi matin, j'ai présenté à la salle de preview (la salle réservée aux orateurs pour permettre de soumettre une nouvelle ver-

sion de leur présentation), la énième version encore modifiée de mes visuels. Puis je me suis réfugié dans un coin du palais des congrès pour écouter un peu de musique pour me détendre contre cette angoisse grandissante difficile à contrôler, et c'est là que j'ai eu l'idée de relire la "[Litanie contre la peur](#)" des sœurs du Bene Gesserit de [l'univers de Dune](#). Cela ne marche pas du tout sur moi, mais je me suis dit que cela ferait une bonne introduction à mon intervention... Pour ceux qui n'ont pas lu l'ouvrage de Frank Herbert, voici le mantra :

*Je ne connaîtrai pas la peur car la peur tue l'esprit.
La peur est la petite mort qui conduit à l'oblitération totale.
J'affronterai ma peur.
Je lui permettrai de passer sur moi, au travers de moi.
Et lorsqu'elle sera passée, je tournerai mon œil intérieur sur son chemin.
Et là où elle sera passée, il n'y aura plus rien.
Rien que moi.*

Si vous voulez voir un Zythom très tendu et stressé, voici l'intégralité de ma présentation en vidéo (avec en bonus track à 43' la prière des RSSI ;-): <https://youtu.be/NEgy7ZO9s30>

Ce que je garderai comme souvenir de ces journées réseaux, c'est une super organisation, un grand stress de mon côté, des présentations de qualité où j'ai appris beaucoup de choses, et des rencontres très agréables avec [@bortzmeyer](#), [@folle](#), [@Jehane_fr](#), [@BoeufNoix](#) et plein d'autres lecteurs du blog. C'est très intimidant de discuter en présentiel avec chacune de ces personnes !

J'espère pouvoir aller dans deux ans aux JRES 2015, mais cette fois comme simple participant...

Réponse de la cour d'appel

C'est la période où les cours d'appel envoient aux candidats à l'inscription sur les listes d'experts judiciaires la réponse tant attendue. Je le sais, car je reçois beaucoup de courriers de lecteurs se posant beaucoup de questions sur leur avenir judiciaire...

Alors, résumons un peu la situation : vous avez constitué un dossier de candidature que vous avez déposé avant le 1er mars. Vous avez peut-être été reçu en entretien par un magistrat qui vous a questionné sur vos capacités. Un policier ou un gendarme a mené une enquête de bonne moralité en questionnant vos voisins (ou votre conjoint). Les magistrats de la cour d'appel se sont réunis pour décider s'ils pouvaient vous inscrire sur la liste des experts judiciaires. Un greffier a rédigé leur réponse que vous tenez dans vos mains tremblantes.

Cas n°1 : Vous n'avez pas été accepté à l'inscription sur la liste des experts judiciaires. Votre déception est à la hauteur du temps d'attente qu'aurait mis les tribunaux à vous rembourser vos frais d'expertises. Le choc est aussi sec que le ton du courrier que vous relisez incrédule...

Extrait du courrier que j'ai reçu le 11 décembre 1997 :

Monsieur,

J'ai l'honneur de vous notifier, conformément aux dispositions de l'article 18 du décret n°74-1184 du 31 décembre 1974, relatif aux experts judiciaires, que votre candidature n'a pas été retenue pour l'année 1998 par le cour d'appel de [Tandaloor], réunie en assemblée générale le 24 octobre 1997.

Je puis vous indiquer que les décisions prises pour l'établissement des listes d'experts, ne peuvent donner lieu qu'à un recours devant la cour de cassation.

Je vous prie d'agréer, Monsieur, l'expression de ma considération distinguée.

Remarquez au passage qu'il a fallu un mois et demi pour rédiger ce courrier, ce qui donne une idée du temps judiciaire des sous-effectifs déjà à cette époque, courrier que je me permets de mettre en regard du courrier type que je reçois quand je un de mes étudiants postule à une offre d'emploi :

Monsieur,

Après analyse de votre candidature, et malgré la qualité de celle-ci, nous sommes au regret de vous informer que nous ne pouvons pas retenir votre dossier pour le poste de DSI du projet Mars 2014 (H/F) (Référence DTC2014) au sein de la société VoyageSansRetour. En effet, d'autres candidats ont un profil plus proche de celui recherché pour ce poste.

Nous vous remercions de la confiance que vous avez témoignée à VoyageSansRetour et nous vous prions d'agréer, Monsieur, nos sincères salutations.

Une fois passé l'amère déception (sisi, je vous assure, ça va passer), vous vous demandez ce qui a pu aveugler l'assemblée générale des magistrats de la cour d'appel et l'empêcher d'accepter de vous inscrire sur leur prestigieuse liste des experts judiciaires. Je vous donne quelques pistes :

- Vous vous êtes trompé de cour d'appel pour le dépôt de votre dossier de candidature. Vérifiez sur [Google](#) (ou mieux sur [Duckduckgo](#)), surtout si vous êtes en région parisienne. Etre inscrit sur la liste, ça se mérite...

- Votre candidature est excellente, mais les magistrats disposent d'assez d'experts excellents sur leur liste.

- C'est votre première candidature et les magistrats testent votre motivation (légende urbaine ?).

- Vous n'avez pas assez d'expérience car vous êtes encore étudiant et les magistrats pensent qu'il vous faut vous aguerrir un peu dans cette jungle impitoyable où s'affrontent les 16-70 ans et qu'on appelle le monde du travail. Et je ne parle même pas des stagiaires de troisième...

- Vous avez trop d'expérience ou celle-ci est trop ancienne à 69 ans en tant que retraité de l'aviation de chasse.

- Vous n'avez pas été nommé comme expert judiciaire dans des affaires d'envergure nationale ou internationale où vous auriez pu briller par votre excellence (je prends le cas où vous postuliez pour une inscription sur la liste des experts près la cour de cassation).

- Vous n'êtes pas assez qualifié (bruit du ciel qui vous tombe sur la tête).

Je n'ai qu'un seul conseil à vous donner : **retentez l'année prochaine** (avant le 1er mars), sauf si vous êtes étudiant auquel cas il faudra passer vos examens et attendre ~~dix ans~~ un peu pour acquérir de l'expérience. Si vous n'êtes pas pris la deuxième fois, laissez passer quelques années et retentez.

Cas n°2 : Vous êtes accepté !!!!! \0/ \0/ \0/ \0/ \0/

Votre cœur bat à 200 pulsations par minute, et malgré les recommandations répétées de votre cardiologue, vous sautez de joie sur les différents murs de votre habitation, vous embrassez votre belle-mère, vous installez [Gentoo Linux](#) sur la tablette que vous avez reçue à Noël...

Mais passées ces dix secondes de joie incommensurable, un poids terrible s'abat sur vos épaules : serez-vous à la hauteur ? Vous errez dans votre quartier portant une lanterne et cherchant l'humanité, vous maigrissez et vos amis ne vous reconnaissent plus, vous doutez de tout, même de Gentoo...

Vous relisez encore une fois le courrier reçu pour essayer d'en déchiffrer le contenu caché au-delà du premier paragraphe.

Voici celui que j'ai reçu le 17 décembre 1998 :

Monsieur,

J'ai l'honneur de vous aviser de votre inscription sur la liste d'experts judiciaires de la cour d'appel de [\[Tandaloor\]](#) pour l'année 1999, sous la rubrique :

informatique

Vous trouverez en annexe, pour faciliter l'exécution des missions qui vous seront confiées, une notice résumant les principales obligations de l'expert judiciaire.

Je vous serais obligé de bien vouloir vous présenter le lundi 11 janvier 1999 au siège de la cour d'appel de [\[Tandaloor\]](#), dans la grande salle d'audience ([porte 101](#)) afin de rencontrer les chefs de cour préalablement à votre prestation de serment qui aura lieu à 14h dans cette même salle.

Je vous prie d'agréer, Monsieur, l'expression de ma considération distinguée.

Ressaisissez-vous !

Voici quelques conseils (et réponses aux questions que l'on me pose le plus souvent) :

- N'achetez aucun matériel, ni bloqueur, ni PC surpuissant, ni microscope électronique, ni salle blanche, ni matériel Apple. Investissez dans une tenue sobre mais solennelle, pour votre prestation de serment, et répétez cent fois devant un miroir et la main sur le cœur : "*je le jure*".

- Recherchez les coordonnées de la compagnie *pluridisciplinaire* de votre cour d'appel. Contactez les, prenez rendez-vous avec son président, préparez toutes les questions que vous vous posez et votre carnet de chèques : inscription à la compagnie, à la revue [Experts](#), à l'assurance indispensable en responsabilité civile (prix défiant toute concurrence en tant que membre de la compagnie). Inutile de contacter à ce stade une compagnie spécialisée, qui de toute façon n'accepte en son sein et en général que des experts inscrits obligatoirement dans une compagnie pluridisciplinaire.

- Parmi les questions, revient souvent les aspects administratifs et comptables... Ma réponse : ça dépend de votre emploi principal. Pour ma part, je suis salarié. J'ai choisi le statut d'autoentrepreneur (qui n'existait pas en 1999, je vous passe les détails historiques sordides). Pour la comptabilité, adressez-vous ~~à votre femme~~ à votre compagnie. **Surtout ne demandez rien à l'administration !** Personne ne comprend le statut des experts judiciaires, j'ai toujours eu des discussions où je me rendais compte que j'en savais plus sur le sujet que mon interlocuteur. Les seuls interlocu-

teurs valables sont vos futurs confrères de votre compagnie pluridisciplinaire et/ou les cahiers de la revue [Experts](#). Même les textes de loi sont parfois obscurs ou sans décret d'application.

- La formation obligatoire. En tant que nouvel inscrit, vous êtes en période probatoire (inscription sur la liste pour une période de deux ans seulement, au lieu de cinq pour les experts aguerris). Vous devez suivre une formation (en général de cinq jours). Renseignez-vous auprès de votre compagnie pluridisciplinaire. Cela n'existait pas en 1999 et je me suis formé directement auprès de mon épouse avocate qui a réussi à me faire entrer dans le crâne la différence entre civil et pénal, le sens profond des mots "warrant", "verus dominus", "usucapion", "Urssaf", "quéérable", "léonin", "forclusion", "exécution provisoire", "contradictoire", "incompétence du juge" ainsi que le sens des [différentes abréviations](#) "OPJ", "JI", "Urssaf", "T.com.", "TGI", "SAS", "COJ", "Bull.", "Cass.civ.II", etc. Cette formation vous permettra normalement de pouvoir reconnaître les différentes personnes auxquelles vous allez avoir à faire, pour éviter de dire "bonjour Maître" à l'avocat général... Une (re)lecture de l'intégrale du blog de [Maître Eolas](#) est nécessaire, et au moins de ce billet : « Apprenons à les reconnaître » sur <http://www.maitre-eolas.fr/post/2007/08/26/705-apprenons-les-reconnatre>

- Achetez quelques ouvrages dans votre librairie préférée. Les parisiens ou les provinciaux en visite à Paris peuvent s'approvisionner chez Gibert Jeune "Droit, Économie, Gestion", 6 place Saint Michel. Sinon une recherche "expert judiciaire" sur [Amazon.fr](#) donne de très bons résultats ;-)

- Soyez patient. Il est possible que vous ne soyez pas désigné du tout pendant les deux années de probation... C'est dommage, mais c'est comme ça. J'ai eu des années avec 10 affaires et des années avec... zéro.

- Prévenez votre employeur de votre bonne fortune et assurez-vous que vous pourrez vous absenter de temps en temps (en général une journée) en posant des jours de congés.

- L'inscription sur une liste d'entraide entre experts judiciaires me semble être une bonne idée. Je vous recommande chaudement celle mise en place par le [LERTI](#) pour les experts en informatique, et qui regroupe des personnes de qualité qui n'hésitent pas à donner un bon conseil ou le bon tuyau quand on est dans la peine (par exemple : quel est le fax du service juridique de tel FAI...)

- Enfin, l'abonnement à ce flux RSS : <http://zythom.blogspot.com/feeds/posts/default> me semble indispensable ;-)

Bienvenue dans cette confrérie que forment les experts judiciaires. N'écoutez pas les vieux cons (dont je suis) et soyez indépendants mais avec politesse. Cela s'appelle la confraternité. Et surtout, n'oubliez pas que vous n'êtes pas juge, que vous donnez un avis technique basé sur une méthode scientifique et que la science est le domaine du doute et de la remise en cause. Ne dites pas "M. Truc a ouvert ce fichier à 14h", mais "le compte informatique de M. Truc a servi pour l'ouverture de ce fichier à 14h, heure relevée dans les métadonnées de l'ordinateur, dont le BIOS indique (au moment de l'expertise) qu'il existe un décalage de X minutes et dont le système d'exploitation indique (au moment de l'expertise) qu'il ne suit pas l'heure d'été". Écrivez vos rapports d'expertise d'une main tremblante en pensant [à l'éternel voyage de la science et au professeur Tardieu](#). Pensez également aux personnes qui se sont faites une spécialité des ~~torpillages~~ [critiques des rapports d'expertises](#). La qualité de votre travail est à ce prix.

"Voilà ce qui me paraît être la vérité", dit le savant.

"Voilà la certitude", traduit la foule ignorante, oublieuse de "l'éternel voyage" de la science.

Bon voyage, et si vous avez des enfants, pensez à fermer la porte de votre bureau [pendant certaines expertises](#)...

Conséquences des agissements de la NSA sur les expertises judiciaires

Depuis plusieurs mois, les informations révélées par Edward Snowden secouent l'univers de la sécurité informatique. Car, s'il s'agit du plus grand scandale de surveillance électronique occidental éclatant au grand jour, il s'agit aussi du plus grand fiasco de la sécurité informatique de tous les temps.

Avec tous les spécialistes pointus en sécurité informatique, tous les audits effectués sur les différents matériels, toutes les alertes récurrentes sur les espions chinois et russes, personne (parmi les gens pouvant parler librement) n'a rien remarqué, personne n'a su où regarder, personne ne s'est rendu compte de la collecte massive d'informations avant qu'Edward Snowden ne livre les documents de la NSA.

Bien sûr, certains journalistes, comme ceux travaillant chez [Reflets](#), avaient commencé à lancer des alertes en recoupant des informations et des données techniques, mais la prise de conscience collective a été plus que tardive.

Quand je lis chez Korben, dans ce billet : « Qu'allons-nous encore tolérer des Etats-Unis et de la NSA ? » (cf. <http://korben.info/quallons-nous-encore-tolerer-des-etats-unis-et-de-la-nsa.html>), que les Etats-Unis disposent depuis 1997 d'un service d'informaticiens offensifs (TAO) qui se sont infiltrés dans 258 systèmes informatiques de 89 pays, ma première pensée est pour toutes les expertises judiciaires que j'ai menée depuis, avec une seule question à l'esprit : ai-je pu affirmer dans l'un de mes rapports d'expertise judiciaire quelque chose qui pourrait avoir été le fait d'une action d'une telle équipe ? Ai-je pu charger un innocent d'un élément qu'il aurait pu ne pas commettre ? Ai-je moi-même été piégé dans mes investigations, quand tant de personnes se sont faites roulées ?

J'ai alors relu tous les rapports que j'ai rédigé depuis 1999, avec en tête l'action de la NSA, l'existence de cette équipe de hackers d'état et la guerre électronique en cours, avec l'ampleur qu'on lui connaît

maintenant. J'ai vérifié mes conclusions et j'ai pu constater avec soulagement que j'avais toujours pris les précautions élémentaires dans l'analyse des preuves sur lesquelles j'ai eu à travailler. En partie ~~à cause~~ grâce à l'existence de longue date des malwares et virus toujours plus sophistiqués qui obligent l'expert judiciaire à toujours émettre des réserves quand on lui demande, par exemple, si tel ou tel compte informatique a servi au téléchargement d'images pédopornographiques, puisqu'un tel téléchargement peut être effectué, par exemple, par un malware à l'insu de l'utilisateur de l'ordinateur.

Oui, mais ai-je été assez pédagogique dans mes avertissements ? Ai-je moi-même réellement cru que je pouvais me trouver face à un ordinateur sciemment piraté ? N'ai-je pas haussé les épaules en me disant qu'il était peu probable que l'ordinateur de M. Toutlemonde que j'avais sous scellé devant moi ai été la cible d'un groupe de hackers chinois, russes ou même américains ou français ?

J'espère avoir été clair dans mes rapports sur l'existence de ces risques.

Pourtant, je ressens un malaise. A chaque fois que j'ai été confronté à un ordinateur infecté de malware et/ou de virus, je l'ai signalé noir sur blanc dans mon rapport, en indiquant la nature des malwares trouvés. Mais qu'en est-il des backdoors logicielles inconnues à l'époque et que l'on découvre aujourd'hui ? Qu'en est-il des logiciels implantés puis effacés correctement, avec nettoyage parfait des traces ? Je ne peux être certain de rien. Je me sens [comme le professeur Tardieu](#).

Oh, certes, j'ai toujours été scientifique dans mes approches du problème qui m'était présenté. J'ai été factuel, méticuleux et consciencieux. Je n'ai pas écrit "M. Truc a stocké des images pédopornographiques sur son ordinateur", mais "Je constate la présence d'images pédopornographiques sur l'ordinateur appartenant à M. Truc". J'ai toujours indiqué que les téléchargements effectués avec le compte informatique de M. Truc pouvaient être le fait d'une

autre personne utilisant son compte, voire d'un logiciel agissant à l'insu de M. Truc.

Maintenant que tous les mois [des routeurs montrent leurs faiblesses](#) et qu'il est clair que tous les pays espionnent tous les citoyens de la planète, que les forces de l'ordre mènent des actions hors du contrôle de la justice de leur pays, il est facile de critiquer la naïveté des informaticiens et plus globalement la naïveté des citoyens (et de leurs élus).

Mon problème est d'expliquer aux magistrats, aux avocats et aux policiers qu'un ordinateur est devenu une passoire, que le réseau est devenu une passoire, que les sites web sont devenus des passoires... Il va falloir vivre dans ce monde, mais avant que tous ne comprennent que les preuves numériques sont de moins en moins fiables, des innocents risquent d'être poursuivis et condamnés.

C'est aux experts judiciaires en informatique d'en faire prendre conscience rapidement aux acteurs de la justice.

Quant à la vie privée, je ferai parler la NSA à travers la bouche du Colonel Nathan R. Jessup (Jack Nicholson dans "Des hommes d'honneur"), en modifiant à peine quelques paroles de la scène d'anthologie du film :

Nous vivons dans un monde qui a des murs, et ces murs doivent être gardés par des hommes en arme. Qui va s'en charger ? Vous ?

Je suis investi de responsabilités qui sont pour vous totalement insondables. Vous pleurez ~~Santiago~~ votre vie privée et vous maudissez ~~les Marines~~ la NSA.

C'est un luxe que vous vous offrez. Vous avez le luxe d'ignorer ce que moi je sais trop bien. La mort ~~de Santiago~~ de la vie privée, bien que tragique, a probablement sauvé des vies. Et mon existence, bien que grotesque et incompréhensible pour vous, sauve des vies.

Vous ne voulez pas la vérité parce qu'au tréfonds de votre vie frileuse de tout petit bourgeois vous ~~ME~~ voulez sur ce mur, vous avez besoin de moi sur ce mur.

Notre devise c'est "Honneur Code Loyauté". Pour nous ces mots sont la poutre maîtresse d'une vie passée à défendre des bastions. Chez vous ces mots finissent en gag.

Je n'ai ni le temps ni le désir de m'expliquer devant un homme qui peut se lever et dormir sous la couverture d'une liberté que moi je protège et qui critiquera après coup ma façon de la protéger.

J'aurai préféré que vous me disiez merci et que vous passiez votre chemin ou alors je vous suggère de prendre une arme et de vous mettre en sentinelle postée.

Colonel Nathan R. Jessup (Jack Nicholson)

La vie privée est morte depuis longtemps, et je crains que le Colonel Nathan R. Jessup n'ait finalement gagné, contrairement à ce qui se passe dans le film. Le seul moyen de lutter contre lui est le chiffrement à tout va, [de gré à gré](#).

Mais j'attends toujours de tomber sur un disque dur chiffré par M. Toutlemonde, disque placé dans un ordinateur équipé d'un système d'exploitation sécurisé, ordinateur branché sur un réseau chiffré, sûr et décentralisé, réseau où se trouveront des serveurs respectueux de la vie privée, et reliant des utilisateurs attentifs au respect de leurs données personnelles.

Ce jour-là, je vous promets d'ouvrir une bouteille et de trinquer à la protection de la vie privée, et cela même si cette protection complexifie (un peu) la lutte contre les activités criminelles de quelques-uns.

Je sens que je ne suis pas prêt de me saouler sur ce coup-là...

Le petit blogueur et l'ANSSI

En discutant avec les personnes du stand de l'ANSSI aux JRES2013, je me suis rendu compte que mon billet intitulé "[L'ANSSI et le test Google](#)" avait fait grincer quelques dents... Cela m'a désolé car ce n'était vraiment pas le but. En relisant le billet, je me suis dit que je n'avais pas été très clair et que l'autodérision dont j'avais essayé de faire preuve n'était pas bien passée et que n'était resté que le dénigrement d'un processus de recrutement.

Voici donc quelques points que j'aimerais clarifier :

L'ANSSI, [Agence Nationale de la Sécurité des Systèmes d'Information](#), est une structure ~~gouvernementale~~ étatique chargée d'assurer la sécurité et la défense des systèmes d'information de l'état et des sociétés stratégiques françaises. Vous trouverez tous les détails de son fonctionnement et de son histoire [sur son site](#), ou sur [la page Wikipédia qui lui est consacrée](#).

N'étant ni spécialiste de la sécurité, ni DSI dans un établissement sensible ou stratégique, je n'ai entendu parler de l'ANSSI que lorsque j'ai été invité au [SSTIC 2012](#) (où je me suis fait [déchirer mon blog](#), merci de me le rappeler..) pour parler de l'activité d'expert judiciaire.

J'ai alors découvert l'existence de l'ANSSI, son mode de fonctionnement et pu discuter avec des personnes passionnantes, toutes très compétentes dans leur spécialité. Pour dire les choses autrement, l'ANSSI regroupe un nombre impressionnant des spécialistes de la sécurité informatique, et est la seule structure française à recruter de manière importante dans ce domaine.

C'est pourquoi, j'ai voulu voir si un profil comme le mien pouvait les intéresser, sachant que MOI j'étais très intéressé par leur profil. Hélas, mes compétences ne correspondaient pas au poste pour lequel j'ai postulé. J'ai donc logiquement pris une veste. Fin de l'histoire.

Le billet "[L'ANSSI et le test Google](#)" raconte tout cela, mais avec comme sujet principal une moquerie de ma part sur les tests mesurant les compétences. Il faut dire que je travaille depuis 25 ans dans des établissements d'enseignement supérieur et que les méthodes et pratiques d'enseignement et d'éducation (ce que l'on appelle "[la pédagogie](#)") sont au cœur de mes préoccupations. Et comme tout enseignant, j'ai des idées bien arrêtées sur ce sujet. Je ne vais pas réécrire le billet...

Mais alors que je ne faisais qu'écrire une moquerie dans un billet de petit blog, j'oubliais un point très important : les employés de l'ANSSI sont tenus à la plus grande discrétion. Ils ne disposent pas d'une liberté qui m'est chère : la liberté d'expression. Ou plutôt, ils en disposent, mais avec un fort encouragement à la discrétion. C'est comme cela. Je rappelle que l'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale, et que si chacun à l'ANSSI pouvait raconter sa vie dans un blog, tout cela ne ferait pas très sérieux (mais serait certainement très intéressant)...

[Certains de mes confrères experts judiciaires me rappellent parfois que mon blog "ne fait pas très sérieux", voire "est la honte de l'expertise judiciaire", ou encore "mais qui est le CON qui tient ce blog ?". Seulement voilà, c'est mon petit coin d'internet, ma manière de profiter de cet espace de liberté. Je n'oblige personne à me lire et je rappelle qu'on est toujours le CON de quelqu'un. Je souffre du fait que les ordres des avocats ont encouragé ceux-ci à ouvrir des blogs, mais que les compagnies d'experts n'ont rien fait sur le sujet. C'est tellement XXème siècle...]

Ce n'est jamais intelligent de lancer une pique (une pichenette ?) contre des personnes qui ne peuvent pas répondre. Je travaille suffisamment avec les gendarmes pour comprendre cela.

Je voudrais donc m'adresser aux personnes de l'ANSSI qui ont trouvé mon billet désagréable et faire remonter un commentaire que j'avais écrit sous le billet : "*oui, je suis déçu car j'aurais bien voulu travailler avec les roxors de l'ANSSI*".

Ma consolation : je suis sur la photo présentant [le directeur général de l'ANSSI](#) sur la page Wikipédia d'icelle ;-)

Et pour les autres, souvenez-vous : tout s'arrange autour d'une binouze, surtout au SSTIC.

I 
ANSSI

L'admin réseau, cet enquêteur inconnu

Nous venons de terminer une migration de notre infrastructure d'accès à internet. Nous sommes passés d'un réseau de collecte à un autre, réseaux de collecte nous permettant d'avoir accès à un point d'entrée du réseau RENATER, FAI officiel des établissements d'enseignement supérieur et de recherche.

Concrètement, pour moi, il s'agit d'acheter un appareil électronique qu'on appelle un routeur, le déballer et le visser dans une armoire pleine d'appareils similaires (en fait des switches), attendre qu'un prestataire approprié vienne configurer cet appareil, et le jour J, au top conjoint donné par un informaticien de RENATER et du réseau de collecte, déconnecter le câble branché sur A pour le mettre sur B. Voilà, voilà.

Oui, mais non.

Jeudi, quand j'ai changé le câble de prises, l'accès à internet a été coupé, mais n'est pas revenu aussitôt le câble rebranché. 1000 personnes ont vu leurs cheveux se dresser sur leurs têtes : plus d'internet (en fait, je les ai rassurés aussitôt, plus d'accès à internet, merci pour lui).

Bah, j'étais prévenu, on ne change pas un chemin d'accès d'un claquement de câble dans une prise. Les plus studieux d'entre vous iront lire cette présentation du changement de routage de manière dynamique avec BGP : <http://www.linux-france.org/prj/edu/archinet/systeme/ch69.html>. Disons pour résumer qu'un expert de ces problématiques s'occupe de tout au NOC (Network Operation Center) de RENATER.

Premier problème : l'ancien réseau de collecte A annonce la route vers mon établissement avec la priorité maximale. Difficile pour le nouveau réseau de collecte de faire mieux et de devenir prioritaire. La migration s'annonce difficile, surtout que la personne en charge de BGP chez A est... en congés aujourd'hui. Je vais finir par croire que A est fâché de ne pas avoir remporté l'appel d'offre et met quelques freins à la migration vers B.

Vendredi, le problème est réglé, je bascule tout l'établissement vers le nouveau réseau de collecte B. Le trafic passe dans les deux sens. Voilà, voilà.

Oui, mais non.

Le trafic ne passe pas. Retour arrière. Sauf que le réseau de collecte A voit d'un mauvais œil les alertes sur sa plate-forme de supervision "un coup je m'en vais", "un coup je reviens", surtout en cette période où plus de 40 établissements font plus ou moins la même chose. Ces choses-là se règlent au téléphone, mais ce n'est pas le meilleur moment. Pourtant, je reste calme, cela ne sert à rien d'énerver tout le monde avec mon stress. Autre réunion téléphonique, avec RENATER et le nouveau réseau de collecte B cette fois. Tout le monde me dit que tout est ok de leurs côtés et que les problèmes viennent de chez moi.

C'est là que débute une véritable enquête.

Nous mettons en place en salle serveurs un tableau de papier sur lequel nous listons tous les problèmes rencontrés : perte partiel de l'accès internet (merci le loadbalancing avec une simple LiveBox), sites webs ok mais deux serveurs DNS sur quatre injoignables, accès aux services web internes aléatoires, envois des emails intermittents, etc.

La tension est palpable mais j'avais pris les devants en prévenant tous les clients que nous allions vivre une migration importante et qu'il risquait d'y avoir des perturbations dans La Force. Nous sommes concentrés sur la résolution du problème.

Tout est remis en cause. Et quand je dis tout, je veux vraiment dire tout : câbles, prises, virtualisation des passerelles, virtualisation des switches, les VLAN, les switches physiques, l'apparition d'une boucle sur le réseau réel, sur les réseaux virtuels. Les admins réseaux se sont transformés en enquêteurs suspicieux de tout ce qu'ils ont mis en place. Et pour chaque idée, un test est effectué.

Le vendredi soir arrive, la nuit et l'heure tardive n'y change rien. Je rentre chez moi le cœur gros. Le samedi est consacré à mon fils et son tournoi de ping-pong. Mais mon esprit est ailleurs : qu'est-ce que j'ai pu rater pour que notre migration se soit mal passée ?

Le week-end sera court : je décide de travailler tout le dimanche sur le problème. Me voilà donc seul dans cette maudite salle serveurs à faire différents tests. Je reboote les équipements les uns après les autres, y compris les serveurs de virtualisation après avoir migré les différentes machines virtuelles. Et soudain : EUREKA ! Le port du switch sur lequel est branchée la passerelle n'est pas correctement tagué. Je corrige la configuration, je branche la passerelle et j'ai enfin un accès internet correct. Je suis aux anges. Je préviens mon équipe par SMS, je [tweete avec allégresse](#) et [finesse](#), et je rentre le cœur léger.

Mais lundi matin, en arrivant à mon bureau, patatra. Mon équipe me dit que rien ne marche. Nous reprenons toute notre enquête. Elle durera 14h.

14h à refaire toutes les hypothèses, à reprendre toutes les pannes possibles, à passer des coups de fil pour s'entendre dire "non, non, le problème vient de votre côté". A un moment, nous nous sommes retrouvés avec tout notre réseau débranché, une passerelle physique construite de bric et de broc avec un PC et deux cartes réseaux et un live cdérom [pfsense](#), le tout branché sur un switch HP récupéré et reconfiguré avec les VLAN ad hoc pour l'occasion... A 23h, je lâche le coup, exténué. Je ferme mon bureau avec le moral au plus bas. Pour la petite histoire, je monte sur mon vélo pour rentrer, et je découvre que la roue arrière est déboîtée. Je cherche dans l'école des outils pour essayer de réparer. Mon moral descend encore d'un cran. Sale journée.

Deux points positifs quand même : j'ai réussi à remettre la roue de mon vélo (j'aurai réussi au moins à réparer une chose ce jour-là). Et j'ai réussi à reproduire le problème sur commande : lorsque la passerelle est branchée seule sur le nouveau routeur du nouveau réseau de collecte, j'arrive à surfer sur internet à partir d'un poste

(le seul ayant cette machine comme passerelle). MAIS si j'ouvre plusieurs pages dans plusieurs onglets, au bout d'une dizaine d'onglets, la passerelle n'accède plus à internet. Si j'attends environ une minute, elle retrouve ses esprits et accède de nouveau à internet. A n'y rien comprendre.

J'ai très peu dormi cette nuit-là. Cinq jours que nous sommes quasiment coupés d'internet. Quelques personnes disposent d'un accès via la LiveBox du [PRA](#). Nos serveurs web principaux sont sains et saufs (hébergés à l'extérieur en prévision de la migration). Mais beaucoup des outils du SI sont en temps normal accessibles aux étudiants et à leurs parents, et leur inaccessibilité commence à peser sur l'organisation.

Une part importante de mon métier est de penser à des plans B. J'ai d'ailleurs développé [un sens aigu du film d'horreur permanent](#). Seulement voilà, dans le cas présent, j'arrive au bout du bout des idées possibles de tests à imaginer, de pannes possibles, de vérifications à effectuer...

Mais la nuit porte conseil. Je me réveille avec en tête l'hypothèse que le nouveau routeur, bien que configuré correctement (configuration plusieurs fois vérifiée), PEUT présenter un dysfonctionnement en cas de sollicitation. C'est mon dernier espoir. Problème : je ne connais pas ce nouvel équipement qui se configure en ligne de commande, et la documentation fait 300 pages. Je décide de prendre l'option "appel à un ami".

Nous sommes mardi matin. Je téléphone à un expert du nouveau réseau de collecte pour lui demander de venir m'aider en salle serveurs. Après quelques négociations, il me propose de tout faire depuis son bureau, si je lui ouvre un accès ssh à notre passerelle. Pendant une heure, nous ferons des tests avec lui. Jusqu'au moment où je l'entends dire au téléphone : "tiens, ça me donne une idée". Cela faisait 24h que je n'avais pas entendu cette phrase.

Quelques minutes après notre problème était résolu.

Rien ne clochait de notre côté. Ni sur notre réseau, ni sur notre passerelle, ni sur nos DNS, ni sur notre routeur. Le problème venait de leur côté à EUX. Le port sur lequel est branchée la fibre optique venant de notre routeur était auparavant utilisé pour gérer des échanges entre une adresse IP unique et une adresse IP unique (une connexion entre serveurs proxys appairés). Il avait été configuré pour résister à une attaque DDOS, c'est-à-dire qu'il refusait de fonctionner s'il détectait un comportement anormal. Or, son branchement sur notre routeur a entraîné une discussion entre l'IP de notre routeur et un grand nombre d'adresses IP, ce qui a été détecté comme une anomalie, et donc une mise "OFF" pendant une minute.

Cela explique que dimanche, alors que j'étais seul à surfer, et que je n'avais pas pensé à ouvrir 20 onglets dans mon navigateur, tout fonctionnait. Mais lundi, dès que le personnel et les étudiants ont commencé à vouloir surfer, le système se coupait "quasiment" en permanence.

L'enquête est terminée. La fin a été comme souvent heureuse, grâce à l'entraide des différents admins réseaux, même si le réflexe initial de chacun est d'avoir confiance en SON système et de rejeter la faute sur le système de l'autre.

La morale est sauvée : celui par qui le problème est arrivé, est celui qui l'a résolu. Je lui ai promis de boire ensemble une bouteille de champagne. L'erreur de configuration était subtile, mais sa perspicacité lui a permis de la débusquer.

Et grâce à lui, nous avons révisé en profondeur nos configurations...

L'erreur et l'expertise judiciaire

La hantise de l'expert judiciaire est de commettre une erreur. Je cite souvent [l'histoire du professeur Tardieu](#) qui a probablement fait condamner nombre d'innocents. Et pourtant il ne s'était toujours prononcé qu'à coup -qu'il croyait- sûr.

Au-delà des ignorances des futures avancées de la science, toujours en mouvement, l'expert judiciaire reste humain et est donc faillible à ce titre. Il peut commettre des erreurs et celles-ci peuvent avoir un impact considérable sur la suite du processus judiciaire.

Je suis tombé par hasard sur cette page de www.kitetoa.com où se trouvent deux rapports d'experts judiciaires qui vont illustrer mon propos.

L'affaire concerne [un informaticien poursuivi pour contrefaçon](#). Le premier expert judiciaire intervenant dans cette affaire est contacté par un magistrat qui lui demande de venir étudier le dossier au palais et de répondre à plusieurs questions. La démarche est particulière puisque le magistrat ne demande pas à l'expert judiciaire de mener des investigations techniques sur les scellés (qui existent pourtant dans cette affaire), mais d'étudier un dossier papier et de donner son avis dessus. L'expert a accepté sa mission, et à mon avis, son erreur réside dans cette acceptation.

Extrait [du rapport du 1er expert judiciaire](#) :

Page 3

1) Lecture des éléments du dossier en la présence de Madame le Juge H.

Nous, Monsieur R., avons procédé à la consultation du dossier No du Parquet [42], no d'instruction [101], afin de répondre à la mission confiée.

Ensuite, pour chacune des questions posées, l'expert judiciaire commencera sa réponse par "A la lecture des faits exposés dans les éléments de la procédure nous pouvons répondre..."

Un deuxième expert judiciaire s'est penché, en appel semble-t-il, sur le travail de son confrère. Voici son analyse :

Extraits [du rapport du 2e expert judiciaire](#) :

Page 5

Les investigations judiciaires ont été confiées à l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication ([OCLCTIC](#)).

Au cours de ses investigations, l'OCLCTIC a placé sous scellé deux éléments techniques : le scellé numéro "UN" (cote D 74), qui correspond à la copie de l'espace d'hébergement alloué au site internet de "G.", et le scellé numéro "R-UN" (cote D 60), qui correspond au fichier "VGNaked.zip", téléchargé à partir du site internet "www.g.....net".

Une mission d'expertise technique a été confiée à Monsieur R., dont le rapport précise que la mission a été réalisée sur l'unique fondement de la "lecture des éléments du dossier en la présence de Madame le Juge H."

Ce seul et unique fondement des travaux d'expertise est confirmé par la phrase : "A la lecture des faits exposés dans les éléments de la procédure", qui introduit chacun des trois paragraphes de conclusion du rapport de Monsieur R.

Sur ce seul et unique fondement des travaux d'expertise, le rapport de Monsieur R. conclut par l'affirmative sur l'ensemble des faits reprochés à Monsieur G., c'est-à-dire sur la modification et l'adaptation du logiciel ViGuard, sur la mise à disposition, gratuite ou onéreuse, d'un logiciel ViGuard créé à partir des éléments permettant la suppression ou la neutralisation du logiciel ViGuard.

[..]

Page 16

Le scellé numéro "UN", correspondant à la copie de l'espace d'hébergement alloué au site internet de "G.3, n'a fait l'objet d'aucune expertise technique.

Il est donc techniquement impossible de caractériser et de fonder les éléments techniques d'une infraction à propos de ce scellé.

Le scellé numéro "R-UN", correspondant au fichier "VGNaked.zip", téléchargé à partir du site internet "www.g.....net", n'a fait l'objet d'aucune expertise technique.

Il est donc techniquement impossible de caractériser et de fonder les éléments techniques d'une infraction à propos de ce scellé.

Pages 17-18

[...]

Ces éléments informatiques n'ont pas été analysés par l'expert désigné.

[...]

Cela signifie que les éléments techniques placés sous scellé par l'OCLCTIC, essentiels à la compréhension du dossier et indispensables à la qualification de l'infraction éventuelle, n'ont pas été analysés au cours de l'expertise technique réalisée par Monsieur R.

Cela signifie également que Monsieur R., au mépris des règles expertales fondamentales, a émis ses conclusions sans avoir procédé à aucune analyse des éléments techniques contenus au sein des scellés.

Comment, dans ces conditions, Monsieur R. peut-il affirmer et conclure être en présence "d'un cas avéré de modification et de réassemblage de tout ou partie de logiciel", sans qu'aucune analyse des éléments informatiques que sont le logiciel original et le logiciel modifié ait été réalisé, sans que soient décrits la méthode et les outils du désassemblage et du réassemblage, et sans que soient précisées la nature et l'ampleur des modifications ?

De même, comment, dans ces conditions, Monsieur R. peut-il affirmer et conclure à "la distribution gratuite de logiciels tirés du source du logiciel ViGuard", sans avoir eu accès au code source du logiciel ViGuard, sans avoir analysé la nature et le contenu du ou des fichiers mis en cause, et sans

avoir vérifié et analysé les conditions de la mise à disposition du ou des fichiers mis en cause ?

Enfin, comment, dans ces conditions, Monsieur R. peut-il affirmer et conclure que Monsieur G. "diffuse bien tous les éléments, comportements, logiciels, extraits de code et informations permettant la neutralisation du produit ViGuard", sans présenter la liste et le contenu de ces éléments, comportements, logiciels, etc., sans avoir défini, ni comment, ni en quoi, le logiciel ViGuard pouvait être neutralisé par ces éléments, et sans avoir procédé à aucun test protocolaire démontrant que l'ensemble de ces éléments permet effectivement (condition nécessaire et suffisante) de neutraliser le logiciel ViGuard ?

Dans ces conditions, les conclusions du rapport d'expertise de Monsieur R. sont donc d'un point de vue technique totalement infondées et injustifiées, et par voie de conséquence, ne peuvent en aucun cas être retenues pour caractériser ou fonder une infraction.

[...]

La charge est dure et sans appel. Qui a dit que les experts se soutiennent les uns les autres... Remarquez au passage que l'analyse du deuxième expert suit rigoureusement [les règles de déontologie des experts judiciaires](#) : "l'expert qui remet une note ou des observations écrites sur les travaux d'un confrère, doit le faire dans une forme courtoise, à l'exclusion de toute critique blessante et inutile. Son avis ne peut comporter que des appréciations techniques et scientifiques".

Ce que je cherche à mettre en avant est qu'il est toujours possible de corriger l'erreur d'un expert judiciaire, à condition de le faire le plus tôt possible. Si l'expertise judiciaire est contradictoire, faites-vous accompagner de votre propre expert (un expert peut mener une expertise privée à vos côtés et s'assurer que son confrère respecte les règles de l'art en matière d'expertise judiciaire). Parlez-en avec votre avocat.

Lorsqu'un expert judiciaire adresse son pré-rapport aux parties, celles-ci peuvent émettre des remarques, en général sous forme de questions à l'expert. Ce sont "les dires à expert". Faites-vous aider

par un expert qui saura faire préciser un point ou lever un doute.
Parlez-en avec votre avocat.

Lorsque le rapport est définitif, les choses sont plus compliquées, mais l'affaire n'est pas encore jugée. Il vous est possible de demander un rapport d'expertise privée qui analyse de façon critique le rapport déposé. Parlez-en avec votre avocat. Même chose si vous faites appel.

L'erreur est de croire que tout s'arrange tout seul et que les magistrats verront facilement les défauts éventuels d'un rapport d'expertise, surtout sur les points très techniques. L'erreur est de croire que la dépense est inutile, ou que la justice est gratuite. L'erreur est de se laisser faire sans mettre toutes les chances de son côté.

Pour l'expert, l'erreur sera de croire qu'il faut accepter toutes les missions demandées par le magistrat, sous prétexte que ce dernier est garant de la procédure.

Pour l'avocat, l'erreur est de penser qu'il pourra seul détecter les failles techniques d'un rapport d'expertise. Il est expert en droit, rarement en technique.

Bien entendu, je prêche pour ma paroisse...



Source image : <http://www.says-it.com/churchsigns/sign05.php>

Porte à porte

Depuis six ans, je suis conseiller municipal dans ma commune. J'ai déjà raconté sur ce blog comment j'en suis arrivé à siéger au conseil municipal. Je vais résumer en quelques phrases.

Je me suis toujours intéressé aux projets de ma commune. C'est une petite ville tranquille de 5500 habitants. Aussi, quand mon nouveau voisin m'a indiqué travailler pour la commune et qu'il m'a indiqué que le conseil municipal avait lieu le lendemain soir (de notre conversation), et qu'il était public, j'ai dit pourquoi pas. Ensuite, une fois par mois, j'ai assisté à chaque conseil municipal dans le nombreux public de trois personnes.

Quand le nombre de bureaux de vote de la commune a augmenté, du fait de l'augmentation de la population, une des adjointes est venue me voir, aussitôt le conseil municipal terminé, pour me demander si j'acceptais de l'aider à tenir un des nouveaux bureaux de vote. J'ai dit pourquoi pas. Ensuite, à chaque élection, j'ai participé à la tenue du bureau et au dépouillement.

Quand le maire a constitué sa liste, il y a six ans, il m'a contacté pour savoir si j'acceptais d'y apparaître, en antépénultième position. J'ai précisé que je n'étais adhérent à aucun parti, il m'a dit que cela ne posait aucun problème. J'ai dit pourquoi pas. Comme notre liste était la seule à se présenter, j'ai été élu avec tous les autres membres de la liste.

Depuis, je participe à la vie de la commune en prenant part aux décisions du conseil municipal (une fois par mois) et en travaillant au sein de plusieurs commissions (communication-culture, voirie-espaces verts, impôts).

Et six années ont passé. Nous voilà en train de mener campagne pour notre ré-élection. C'est ma première participation à une campagne électorale complète. Nous nous sommes réunis plusieurs fois pour échanger et préparer notre programme. Il a fallu trouver un slogan, préparer les affiches et tracts, créer le site web, le

compte Twitter, la page Facebook, planifier des réunions publiques...

Puis est venu le temps du porte à porte.

C'est une vraie découverte pour moi.

Et une difficulté...

Je suis quelqu'un d'un peu renfermé. Je ne m'approche pas facilement des gens, j'ai toujours l'impression de déranger. J'étais un très mauvais dragueur, car j'avais toujours l'impression que la fille avec qui j'essayais de démarrer une conversation voyait écrit en gros sur mon front mes véritables intentions (SEXE en lettres clignotantes)... Donc, quand je m'approche de quelqu'un avec mon tract pour essayer d'engager la conversation, je sens sur mon front clignoter le message "VOTEZ POUR NOUS", et ça me met mal à l'aise.

Heureusement, nous avons fait du porte à porte à plusieurs. L'idée était qu'un "ancien" soit accompagné par un "nouveau", c'est-à-dire qu'un membre de l'actuel conseil municipal soit accompagné d'une personne non encore élue (tous les membres actuels du conseil municipal ne se représentent pas, ce qui fait que notre liste compte des "nouveaux"). Je suis donc considéré comme "anciens" et j'étais accompagné d'un nouveau, qui se trouve être un commercial de profession. Autant vous dire que c'est lui qui m'a appris à faire du porte à porte...

Tout d'abord, ne pas faire du porte à porte trop tôt le matin (8h le dimanche matin me semble une grosse erreur). Nous avons plutôt choisi de frapper aux portes l'après-midi, samedi et dimanche.

Ne pas se tenir trop près de la porte, pour ne pas indisposer les personnes.

Se présenter, sourire, expliquer la démarche, donner les éléments clefs du message et les dates de réunion.

Ne pas insister.

Durant deux week-ends, j'ai donc écumé mon quartier avec mes collègues-assistants-mais-en-fait-c'était-moi-leur-assistant. J'ai été surpris du bon accueil général que les gens nous ont fait. Plusieurs nous ont même invité à entrer pour nous réchauffer, ou nous mettre à l'abri de la pluie. Sur 200 personnes rencontrées, une seule a été agressive en dénigrant l'action de la municipalité et des politiques en général. Toutes les autres ont été bienveillantes et (relativement) à l'écoute.

A chacun nous demandions s'il avait une remarque à nous faire, un ou plusieurs problèmes à remonter. Nous avons pris des notes de chaque point indiqué. La plupart du temps, il s'agit d'un problème de voirie ou de stationnement. Souvent les gens ne comprennent pas que la place de parking publique située devant chez eux ne leur est pas réservée. La plupart des points sont des problèmes de voisinage. Il faut expliquer que la commune ne peut pas tout, et qu'il faut se parler entre voisins. Il faut surtout écouter les gens exposer leurs problèmes. Certains sont bénins, d'autres sont terribles. Tous sont importants.

"Les poubelles sont sorties trop tôt par mes voisins. Du coup, les chiens viennent fouiller dedans, les renversent et ça met des cochonneries partout !". Nous prenons note, rappelons qu'il faut en parler avec les voisins. Il nous faudra aussi rappeler à tout le monde les horaires de passage du ramassage des ordures, prévoir des emplacements adaptés là où les poubelles sont renversées, discuter avec leurs propriétaires...

Une femme âgée élevant seule son enfant aveugle et handicapé moteur nous a fait part de son inquiétude sur ce qui va se passer après sa disparition. Comme elle vient de s'installer sur la commune, personne n'était au courant de sa situation, situation qu'elle gère parfaitement d'ailleurs, seule depuis 40 ans... Nous sommes restés avec elle une demi-heure à l'écouter raconter son histoire, tranche de vie extraordinaire.

Un homme s'inquiète de la construction imminente d'un lotissement. Il ne pourra plus profiter du lever de soleil sur le champ en face de chez lui. Son impasse va devenir une rue. Sa vie va changer. Il faut écouter à défaut de pouvoir convaincre.

Une dame nous parle des mauvaises herbes qui poussent dans la rue. "Avant, la commune était plus propre". Nous lui expliquons que les jardiniers communaux passent plus souvent, mais avec un produit moins toxique, et moins efficace. La protection des nappes phréatiques commence par des changements d'habitude, et la commune doit montrer l'exemple. Pas facile de convaincre.

La Poste du centre-ville a été fermée, sous prétexte qu'il y a déjà un bureau de poste dans la zone commerciale. Vu de Paris, deux Postes dans la même commune, ça faisait vraiment trop riche. Les personnes âgées nous font sentir qu'elles aimaient bien aller à la Poste à pied...

"Les gens roulent trop vite, mettez (ma) rue en sens unique, ce sera moins dangereux." Nous expliquons qu'une rue en sens unique incite les gens à rouler encore plus vite. Incrédulité...

Je constate un vrai problème de communication entre la commune et ses administrés. Beaucoup de gens ne se déplacent plus maintenant à la mairie. Les habitudes ont changé. Quasiment aucun des affichages légaux (en mairie) ne sont lus. Il faut amener l'information aux administrés, et le bulletin mensuel que nous éditions ne suffit plus. Il faudra améliorer cela.

Le porte à porte, une expérience de vie.
Surtout pour un informaticien un peu ours.

On verra si nous sommes réélus...

En tout cas, on ne manquera pas de travail !

Création d'entreprise

En 2010, je réfléchissais [au développement d'une activité de conseils](#), pour finalement faire le saut en 2013 avec la création de [ma petite entreprise](#).

Un vieux rêve d'étudiant... Concrètement, c'est un peu plus compliqué.

1) Le choix de la structure.

En bon ingénieur de base, j'ai une idée un peu déformée de ce qu'est réellement une entreprise, même si j'y travaille. Disons que "de mon temps", ce concept n'était pas enseigné sur les bancs, ni du lycée, ni des classes prépas, ni des écoles d'ingénieurs, ni des laboratoires de recherche...

Je me suis donc retourné vers mon épouse, et je lui ai posé LA question : "mais finalement, c'est quoi une entreprise ?"... Après quelques aspirines et questions plus ou moins saugrenues, j'ai fini par comprendre que si je voulais vendre mes services, il fallait que je crée la structure juridique appropriée, avec toutes les déclarations qui vont avec.

Comme je suis tout seul, que je propose une activité de service aux avocats, la structure qui nous a semblé la plus adaptée est celle de l'auto-entrepreneur. C'est d'ailleurs celle que je conseille aux experts judiciaires qui viennent de prêter serment. C'est aussi très simple du point de vue formalités : il suffit d'aller sur le site [lauto-entrepreneur.fr](#) et de suivre le mode d'emploi (avec un dictionnaire).

J'ai un avantage sur le commun des mortels : mon épouse a tout fait pour moi !

J'essaye de retenir les rôles des différents organismes : unions de recouvrement des cotisations de sécurité sociale et d'allocations familiales, impôts, organismes collecteurs de taxes, assurances,

retraites... Mais rien n'y fait, je suis étrangement hermétique à cet univers. C'est l'intérêt d'être deux !

2) L'offre de base.

Comme je l'expliquais [dans mon billet](#) intitulé « Ma petite entreprise » (tome 6 ci-avant), je propose mes services aux avocats selon trois axes :

- assistance technique pendant les réunions d'expertise judiciaire;
- assistance dans la rédaction des dires;
- analyse critique d'un rapport d'expertise judiciaire.

Si le premier axe est assez classique, les deux autres sont basés sur un travail à distance permettant de faire baisser les coûts d'une expertise privée. Surtout que je pratique des tarifs "de lancement d'activité" : je reçois les documents de manière sécurisée, j'en fais l'analyse préalable, j'établis un devis précis, et s'il est accepté, je démarre mon travail aussitôt. Je peux être très réactif, ce qui est apprécié par les avocats qui courent souvent contre la montre.

3) La publicité.

Comment faire connaître mes propositions de service à l'ensemble des avocats de France ?

Tout d'abord, j'ai choisi d'en parler sur ce blog, ce qui m'a paru assez naturel. C'est un blog personnel, que je tiens [depuis 2006](#), et sur lequel je parle de tous les sujets qui me tiennent à cœur. Et celui-ci en est un. Je n'ai pas à me justifier sur mes choix éditorialistes, surtout qu'un seul clic suffit pour qu'un lecteur quitte un billet vers des cieux qu'il juge plus intéressants. Ce blog n'est plus un blog de moine [comme en 2007](#).

J'accepte donc des missions par l'intermédiaire de [ma page contact](#), dès lors qu'elles sont proposées par un avocat.

Mais ce n'est pas suffisant, et pas assez professionnel.

Très vite, il m'a fallu créer un site internet dédié à mon activité d'autoentrepreneur. Seulement voilà, développeur web, c'est un métier. Autant j'ai su trouver un nom à mon entreprise (qui soit parlant, joli, qui sonne bien, facile à retenir, et non utilisé...) et acheter le nom de domaine, autant je galère à fabriquer LE site qui me satisfait.

Pour l'instant, j'ai un site de base chez Gandi, inclus dans l'achat du nom de domaine, mais limité en nombre de pages, et surtout ne permettant pas l'utilisation des outils statistiques de Google (il faut passer à l'offre payante). J'ai donc décidé de développer un autre site sur une plate-forme gratuite que je connais bien : Blogger. J'entends déjà rire les développeurs professionnels... mais pour l'instant, je ne m'en sors pas trop mal, même si le résultat n'est pas encore à la hauteur de mes espérances.

Le moment le plus WTF a été quand il a fallu faire une séance photos pour illustrer le site. Me voici donc habillé en costume d'expertise, poudré pour ne pas luire comme un ostensor (© [Charles Beaudelaire](#)), et souriant maladroitement devant l'objectif amateur de mon épouse amatrice... Sur les 30 photos, seules deux ont survécu au choix impitoyable de mon fan club familial pour se retrouver sur le site. Je me demande quand même s'il ne va pas falloir passer par une agence de professionnels. On verra quand le chiffre d'affaire aura décollé.

Un point intéressant est ma découverte de l'univers des Google Adwords, avec toutes les techniques marketings associées : campagnes de publicité, ciblage, emplacement, conversion, analyses de performances, listes de mots clés, réseau de contenu, remarketing... Autant de concepts qui me sont encore étrangers et qu'il va me falloir maîtriser. Je pense que je ferai un billet dédié à ce vaste sujet, ou du moins à la découverte que j'en ferai.

Je vais également contacter mon réseau de connaissances et d'amis. Comme je n'ai pas la fibre commerciale, je pense privilégier le contact épistolaire individuel. Je présenterai mon projet de

services et ma demande d'aide promotionnelle (du type : "parlez-en autour de vous"). Il me faut faire un beau papier à entête et me réentraîner à tenir une plume...

4) Le développement.

Je n'en suis pas là. Je n'ai pas beaucoup de temps à consacrer à cette activité parallèle à mon vrai métier qui me passionne aussi. Il y a aussi la vie de la commune avec les élections qui approchent, les expertises judiciaires demandées par les magistrats qui sont prioritaires, et la vie de famille avec des enfants qui grandissent trop vite !

Mais si j'ai créé cette structure, c'est pour la développer. J'ai un âge où plus personne ne viendra me chercher pour me débaucher, et où mes compétences techniques vont probablement stagner. Il faut maintenant que je vende mon expérience à ceux qui sauront le mieux en profiter.

Difficile défi, surtout pour un mauvais vendeur !

Le pédophile

J'aime bien télécharger des films de toutes sortes sur internet. Des films piratés pour la plupart, et beaucoup de films pornos. A force d'essais et d'erreurs, j'ai appris pas mal de trucs pour trouver les films qui m'intéressent. Sur les forums, les gens discutent des différents outils qui leur permettent d'échanger des programmes gratuits, des œuvres du domaine public, des photos qu'ils ont prises pendant leurs vacances. J'aime bien Shareaza que j'utilise depuis longtemps. C'est un logiciel P2P qui permet de partager tout et n'importe quoi, et surtout de trouver ce que l'on recherche.

Moi, ce que j'aime, c'est télécharger tous les morceaux de musique à la mode, enfin à la mode de ma jeunesse, c'est-à-dire la Vraie Musique. J'ai tous les tubes des chanteurs que j'aime, mais dont les DVD sont trop chers pour moi. C'est pareil pour tous les films de cinéma que je n'irai pas voir en salle parce que c'est trop cher. Enfin, c'est cher mais aussi c'est un peu la honte d'aller voir un film porno ou de le louer... Alors je télécharge en masse, tous les films pornos que je trouve avec Shareaza.

Quand j'y repense, je me rends compte que mes goûts ont évolué. Avant, j'allais sur YouPorn, avec son rangement bien pratique en catégories. J'ai testé un peu tous les genres : amateur, couples, hairy, mature, voyeur, 3D, etc. Mais très vite, ma catégorie préférée a été "teen". Toutes ces actrices en tenue d'écolière, ou avec des couettes... j'ai trouvé ça très "stimulant". Alors, avec mon programme Shareaza, j'ai recherché parmi tous les films pornos que je pouvais télécharger, ceux plus orientés sur les jeunes filles.

Puis de "teens", je suis passé à "preteens".

Puis de "preteens", je suis passé à "pre teen hard core", les fameuses "pthc". Les noms des fichiers vidéos sont évocateurs : "Allan -4yo pthc pedo", "David & Helen -10yo"... Je ne parle pas anglais, mais j'ai très vite trouvé les bons mots clefs pour télécharger les films qui m'intéressent. Mon ordinateur est allumé 24h/24 et je télécharge en permanence. J'ai plus de 10 000 films maintenant.

J'ai été surpris quand la police est venue m'interroger. Je croyais que les réseaux P2P étaient protégés et qu'on ne pouvait pas savoir qui téléchargeait... Et puis dans la masse des gens qui téléchargent, je pensais passer inaperçu. Il paraît que mon adresse IP a été "flashée" en Russie lors du téléchargement d'un fichier surveillé. Le signalement à Interpol a amené la police jusqu'à chez moi et mon matériel a été saisi. Interpol, sans blague !

Lors du procès, j'ai pu lire le rapport de l'expert judiciaire qui a analysé le contenu de mon disque dur. J'ai pu voir le regard crispé des greffiers et magistrats du tribunal quand ils ont regardé quelques-unes des copies d'écran, et la liste des noms de fichiers. Mon avocat a tout fait pour éviter qu'on projette des extraits de films pendant l'audience. J'ai pu constater le dégoût dans les yeux de mes proches. Il paraît que je suis un pédophile, moi qui n'ai jamais touché un enfant.

Je suis en prison maintenant, mais je lis dans le journal [que je ne suis pas le seul à faire la même chose](#).

C'est si facile. A portée de quelques clics.

Mes lecteurs habituels le savent bien, je romance mes histoires pour ne pas divulguer d'informations sur les dossiers sur lesquels j'interviens, avec l'autorisation de la compagnie d'expert judiciaire de la cour d'appel à laquelle j'appartiens (relire les billets de l'[affaire Zythom](#) (tome 2), en particulier celui sur [la décision de la compagnie](#)). Ce billet est donc une "romance".

Souvent, j'écris mes textes à la première personne, parce que c'est mon blog. Ici, je voulais surprendre quelques lecteurs en écrivant le billet du point de vue du pédophile. Je me demande combien se sont fait prendre, et à partir de quelle phrase ils ont compris. Les auteurs débutants se posent toujours de drôles de questions...

J'ai écrit ce texte en réaction à tout ceux qui me disent qu'ils surfent depuis longtemps sur internet et qu'ils n'ont jamais rencontré de contenus pédopornographiques, que les médias en font trop, que la police devrait faire autre chose que de traquer les internautes, que le gouvernement utilise ce faux prétexte pour censurer la liberté d'échanger des contenus numériques... S'il est évident que des forces financières sont à la manœuvre pour éviter le naufrage de leur modèle économique, il n'est pas possible de nier que nos autoroutes de l'information ne transportent pas que des marchandises légales. S'il y a beaucoup à dire sur tous ces sujets (ce qui n'est pas l'objet de ce billet), je suis personnellement confronté aux images et films échangés par les pédophiles. J'en souffre, mais je continue, parce que je suis fier d'être un petit maillon de la chaîne des gens qui luttent contre ces pratiques.

On ne peut pas nier leurs existences.

Je souffre autant de plonger dans la pédopornographie, que d'entendre dire par les uns qu'elle n'existe pas ou peu, et par les autres qu'elle justifie l'ajout de nouvelles lois avec le prétexte de "civiliser" internet.

Les pédophiles existent.

Internet facilite leurs échanges.

Les lois actuelles suffisent amplement.

Il faut simplement donner les moyens à la justice.

AMHA.

Le petit garçon qui est en moi

En lisant ce billet de l'astronaute Alexander Gerst :

<https://spacetux.org/cpamoa/2014/03/lethargie-technique-ou-ce-que-nous-pouvons-apprendre-des-ecoliers/> sur le blog d'Anne @Cpamoa, je me suis posé la question "quelle part y a-t-il encore en moi des rêves du petit garçon que j'ai été"...

Enfant, je me nourrissais des exploits des astronautes américains. La conquête de l'espace ouvrait des horizons infinis. J'étais persuadé aller dans l'espace avant la fin du (20e) siècle. Je rêvais d'impesanteur et de chute libre dans un ascenseur. Je rêvais de marcher sur Mars.

L'astrophysique regorgeait de mystères qui me fascinaient. Je regardais plein d'espoir des formules incompréhensibles dans l'encyclopédie Universalis de mes parents. Je rêvais de courbure d'espace et d'écoulement du temps.

Je dévorais tous les articles scientifiques des revues dont j'attendais l'arrivée dans la boîte aux lettres avec impatience. Les [Tokamaks](#) n'avaient pas de secret pour moi. J'en avais même fait le sujet d'un exposé devant ma classe de seconde qui me laisse le souvenir d'un silence gêné et d'un professeur prompt à passer à l'exposé suivant... Je rêvais des bienfaits d'une énergie abondante et non polluante.

J'étais fasciné par la programmation des petits calculateurs qui apparaissaient ça et là. Les progrès rapides de la puissance de calcul et des capacités de stockage me laissaient entrevoir l'arrivée proche d'une intelligence artificielle dont j'essayais d'imaginer les conséquences sur la vie de tous les jours. Je connaissais tout sur la programmation de ma petite calculette, et mes idoles s'appelaient [SHRDLU](#) et [Lisp](#). Je rêvais d'interroger un [Multivac](#) ou un [HAL 9000](#). Mes héros sont alors [Ada Lovelace](#) et [Alan Turing](#).

Je passais mon temps à construire [des automates cellulaires](#)...

Je construisais des vaisseaux spatiaux avec mes pièces de [Meccano](#).

La science était ma religion, le progrès scientifique ne s'arrêterait jamais et améliorerait le monde.

Aucun de ces rêves d'enfant n'est devenu réalité.

Il ne reste en moi que l'amertume de leur disparition.

On ne devrait jamais grandir.

L'informatique et les divorces difficiles

Je suis souvent contacté, en tant que blogueur - expert judiciaire, par des internautes qui me demandent ce qu'ils doivent faire pour prouver telle ou telle malversation de leur futur ex-conjoint sur leur matériel informatique...

La situation est en général la suivante : un couple est en procédure de divorce, le climat est très conflictuel, et au milieu trône... un ordinateur. Non que le couple se dispute la garde de la machine (encore que certains courriels que j'ai reçus montre un certain attachement parfois et en général à du matériel "Pomme"), mais plutôt que l'un accuse l'autre d'avoir piégé l'ordinateur et de collecter illégalement un certain nombre de données.

Comment constituer un dossier de preuves permettant d'accabler l'adversaire afin de lui faire rendre gorge et de le mettre minable plus bas que terre ?

Tel est en substance la question qui m'est posée à travers ce blog. Et comme j'accepte volontiers les consultations gratuites, mais que je souhaite optimiser mes réponses sur ce thème, j'en profite pour écrire mes quelques conseils sous la forme d'un billet, ce qui me permettra d'adresser à mes interlocuteurs un simple lien plutôt qu'un copié/collé...

Exemple : Daenerys et Cersei, qui vivaient ensemble avant de gagner récemment le droit de divorcer, se livrent toutes les deux une bataille terrible, avec coup bas, dénigrement et stratégies de haine meurtrière. Daenerys accuse Cersei d'avoir installé sur son ordinateur personnel un keylogger lui permettant d'avoir eu accès à tous ces mots de passe, et de surveiller à distance toute sa correspondance. Il faut dire que Cersei est plutôt calée en informatique, la preuve, c'est elle qui a configuré le Facebook de Daenerys.

La guerre fait rage.

Heureusement, être blogueur a ses petits avantages : je suis contacté par Daenerys qui me ~~confond avec Drogo~~ demande de l'aide... Elle se retrouve sans le sou, nomade errant d'un appartement à un autre, avec pour seules richesses ~~des oeufs pas frais~~ un ordinateur MacBook Pro 15" *sous les pixels la puissance* ©, un iPad *Air qui peut le plus pèse le moins* © et un iPhone 5s 64Go *toujours plus loin* ©. Et une seule idée : comment faire payer le plus possible Cersei pour cette infamie, *elle va morfler cette salope* © !

Savez-vous quelles sont les professions qui voient les gens toujours sous leur plus mauvais côté ? Les proctologues et les avocats spécialisés dans les divorces... Et les avocats qui me lisent savent que la colère d'un conjoint cela peut prendre des proportions extrêmes...

Oui, mais comment faire mordre la poussière à son adversaire ?

Comment prouver sa faute ?

Comment expliquer au juge que l'autre c'est le mal et que la surveillance de ma vie privée ne relève pas ici des prérogatives de la NSA ?

Comment démonter le disque dur pour l'analyser sans risque ?

Comment le copier sans compromettre les preuves ?

Comment établir les preuves de manière irréfutables ?

De même qu'un bon avocat sait calmer la colère de son client et essaye toujours de le guider vers la procédure de divorce la moins conflictuelle possible, dans l'intérêt de tous, un bon expert saura guider son client vers le meilleur conseil technique, dans l'intérêt de tous.

Première chose à faire : éteindre son ordinateur et le ranger proprement à l'abri de l'humidité et des chocs. Le plus tôt sera le mieux. Oui, je sais, c'est un cadeau de votre amant auquel vous tenez beaucoup. Oui, c'est une machine hors de prix à laquelle vous attachez beaucoup d'importance.

Mais n'y touchez plus ! Investissez dans un nouvel ordinateur, ce ne sera que le début d'une longue série de dépenses.

Ensuite, réinitialisez tous vos mots de passe (de toutes manières, vous n'en avez qu'un ou deux, pas vrai ?). Faites-le pour tous vos comptes.

Et réinitialisez vos téléphones (tant pis pour vos contacts, de toutes manières, avec le divorce, beaucoup de contacts vont disparaître...) et réinitialisez vos tablettes à leurs configurations d'origine. Recréez des comptes emails, recréez des comptes iTunes, recréez des comptes Ubuntu... Bref, recommencez une nouvelle vie numérique.

Puis contactez votre avocat, Maître Tyrion, pour lui demander conseil sur les suites à donner au piratage de votre ordinateur. Si vous êtes sûr que celui-ci a été perverti par votre maintenant-ennemi-juré.

Et parmi les moyens de constitution de preuve, il y aura l'analyse réalisée par un expert judiciaire en informatique.

Je précise ici : PAS l'analyse faite par un ami qui s'y connaît, la preuve, il travaille comme informaticien dans une grosse boîte. Non : une analyse de ce type doit être faite par une personne assermentée et habituée à procéder à une analyse inforensique de matériel informatique confié par la justice. Vous ne demanderiez pas à un ami de faire un constat d'huissier, non ?

L'expert judiciaire n'est pas nécessairement le meilleur technicien du monde, ou le plus grand spécialiste en sécurité informatique, mais c'est une personne expérimentée et habilitée par la justice à intervenir pour établir un rapport sur les faits et rassembler de manière scientifique les preuves avérées qu'il aura constatées.

J'oubliais : [cette analyse aura un coût](#). Mais Daenerys est prête à tout pour se venger, non ?

La justice française ayant l'un des budgets honteusement les plus faibles d'Europe, il faudra probablement quelques ~~années~~ mois avant qu'un expert ne soit désigné pour procéder à l'analyse de l'ordinateur incriminé. L'expert judiciaire analysera ensuite les centaines de gigabits du disque dur. Si vous êtes sous Windows, ce sera simple mais long. Si vous êtes sous GNU/Linux ou MacOS, ce sera plus compliqué car mieux protégé. N'oubliez pas de lui fournir les différents mots de passe utilisés à l'époque.

Puis viendra la contre-expertise, le procès, l'appel du procès, la cassation.

Donc, si vous êtes sûr que votre ex-conjoint a piégé votre ordinateur et que vous en avez subi un préjudice terrible, oui, cela en vaut la peine. Mais n'oubliez pas qu'un grand avocat [a dit récemment](#) : "La justice, c'est une administration à laquelle on a donné le nom d'une vertu. Ça n'est rien d'autre que cela. Elle a les qualités et les défauts d'une administration. Moi, je ne voudrais pas avoir à faire à la justice."

Une autre manière de faire consiste à se poser et à réfléchir. Le jeu en vaut-il la chandelle ? Mon conjoint m'a certes joué un mauvais tour en espionnant toutes mes correspondances, mais n'est-il pas plus simple de tourner la page ? Cela mérite-t-il que j'y consacre toute cette énergie et tout cet argent ?

L'expertise judiciaire informatique peut être la bombe atomique de votre divorce. Mais un simple reset est parfois la meilleure solution - et le meilleur conseil d'ami.

Le témoin

Il arrive qu'on demande à l'expert judiciaire de venir témoigner lors d'un procès. Un de mes confrères à bien voulu me faire l'honneur de raconter son expérience sur mon blog [dans ce billet](#) (« Les Assises », tome 5).

Cela ne m'était jamais arrivé, jusqu'à cette semaine.

Je dois dire que je n'étais pas pressé de vivre cette expérience (mais suffisamment curieux quand même pour souhaiter le faire au moins une fois dans ma vie).

J'ai reçu il y a quelques mois l'email suivant :

Bonjour Monsieur l'expert,

Je vous informe que je vais vous citer comme témoin dans le dossier X dans lequel vous m'avez adressé un rapport d'expertise privée particulièrement clair et précis.

Vous allez recevoir une convocation pour une audience qui aura lieu le 1er avril (ce n'est pas une plaisanterie) au TGI de Vulcain.

Je vous remercie de me dire si vous acceptez de venir témoigner, afin que je lance la procédure.

Je vous prie d'accepter, Monsieur l'expert, mes salutations respectueuses,

Signé : Maître Spock

Enfin, ce moment tant craint était arrivé : participer à un procès, devant une cour, dans un tribunal, en public, devant tout le monde, comme dans les séries ! J'en parle aussitôt à mon épouse qui me répond d'un air entendu : "~~J'espère que tu seras indemnisé vas-y ça me fera des vacances~~".

Je réponds donc "oui" à Maître Spock et quelques jours plus tard, un huissier de justice sonne à ma porte pour me remettre en main propre une citation comme témoin pour l'audience du 1er avril (je ne m'en remets pas) d'un tribunal situé à l'autre bout de la ~~galaxie~~ France...

Je note le rendez-vous dans mon agenda ~~de ministre~~, je pose un jour de congé auprès de mon employeur pour cette date, je déplace les rendez-vous déjà programmés.

Le temps passe.

La date s'approchant, je prends mes billets de train et j'achète les tickets de métropolitain nécessaires à mon transport jusqu'au tribunal. Le week-end précédent, je me plonge dans le rapport que j'avais déposé dans ce dossier, j'apprends par cœur les faits, les dates et tous les éléments techniques du rapport, les annexes, les ~~critiques~~ remarques de la partie adverse sur mon travail, les éléments de procédure... Bref, je passe un bon week-end (qui en plus est celui du second tour des élections municipales où j'ai tenu un bureau de vote et soit dit en passant fêté ~~ma~~ la victoire de ma liste et ma brillante élection). Bref je bosse à fond le dossier. Plus le jour approche et plus je sens une boule d'angoisse se former. Mon épouse me rassure : "tu vas ~~en chier~~ y arriver, tu es le meilleur".

Le jour J, je prends le train le matin très tôt pour traverser la France, tellement tôt que, malgré 4 heures de train, j'arrive devant le tribunal avec deux heures d'avance. J'en profite pour repérer les lieux, trouver la salle d'audience, me présenter au greffe, me faire expliquer un peu la procédure : "bah, vous allez prêter serment, puis ~~vous faire cuisiner~~ répondre aux questions". Je trompe mon stress en allant me glisser dans le public (peu nombreux) d'un procès d'assises qui se tenait dans la salle voisine (véridique). Une histoire de cambriolage par des pieds nickelés, de coups de couteaux, de séquestration, de vol... On se détend comme on peut.

Un quart d'heure avant l'audience, Maître Spock arrive et m'explique comment il voit les choses : "vous allez être isolé dans la salle des témoins, puis l'huissier viendra vous chercher, vous prêterez serment, puis je vous poserai quelques questions, puis la cour vous posera aussi quelques questions, ainsi que la partie adverse". Devant mon visage transpirant, il ajoute : "mais ne vous inquiétez pas, rien de compliqué. Soyez vous-même et répondez sans trop entrer dans les détails techniques".

Ok.

Donc l'inconnu total.

Je ne sais pas quand on va venir me chercher.

Je n'assiste pas aux débats.

Je ne connais pas les questions qui vont m'être posées.

Je ne sais pas où je vais poser mon sac, mon manteau, mon pull, mon écharpe (je suis en chemise car je transpire déjà 10L d'adrénaline).

Je ne sais pas qui est qui dans la salle (Président, procureur, avocats, parties). Je ne connais que deux personnes : Maître Spock et l'innocent qu'il défend.

Ah si, je sais une chose : la presse judiciaire est là.

Ok, ok.

Mon cœur bat la chamade.

[minute historique : *autrefois afin de parlementer ou lors d'une reddition, on émettait un signal avec un tambour ou une trompette ; on appelait cela battre la chamade, [source Wikipédia](#)*]

Me voici en train d'attendre dans la salle des témoins (en fait dans la salle des pas perdus, le tribunal ne disposant pas de salle pour isoler les témoins).

Comme d'habitude, je constate avec un étonnement tout scientifique, que si l'on note t le temps d'attente, mon niveau de stress augmente proportionnellement à t , alors que mon encéphalogramme varie en $1/t$...

Je fais alors la seule chose que je sais faire dans ces cas-là : je récite la litanie contre la peur des sœurs du [Bene Gesserit](#) :

Je ne connaîtrai pas la peur car la peur tue l'esprit.

La peur est la petite mort qui conduit à l'oblitération totale.

J'affronterai ma peur.

Je lui permettrai de passer sur moi, au travers de moi.

Et lorsqu'elle sera passée, je tournerai mon œil intérieur sur son chemin.

Et là où elle sera passée, il n'y aura plus rien.

Rien que moi.

J'appelle [mes followers Twitter](#) à l'aide. Ils me remontent le moral.

Les minutes passent.

Je ne sais pas si mon affaire passe en premier (il y a plusieurs affaires convoquées à la même heure).

Les minutes semblent être des heures.

Des personnes entrent dans la salle d'audience : des personnes en robes noires, des personnes à l'air sombre, des personnes angoissées, des personnes avec des blocs notes, des avocats rigolards, un policier...

Les minutes deviennent une heure.

Je sursaute à chaque sortie d'une personne dont je suis persuadé qu'elle vient me chercher. Je n'ai pas hâte d'entrer dans l'arène, j'ai envie qu'on m'oublie, je suis pressé d'en finir, j'ai hâte d'entrer dans l'arène.

Les minutes deviennent deux heures.

J'entends quelques bribes de mots en provenance de la salle, je reconnais la voix de stentor de Maître Spock. Je sens que je vais bientôt être appelé.

Je regarde sur internet l'origine du mot "stentor" [minute culturelle : dans la mythologie grecque, Stentor (en grec ancien Στέντωρ / Sténtór) est le crieur de l'armée des Grecs lors de la guerre de Troie. Son nom vient du verbe στέννω / sténein qui signifie « gémir profondément et bruyamment, mugir ». Il reste dans l'expression populaire « avoir une voix de Stentor » qui, dès l'Antiquité, signifie avoir une voix très puissante, retentissante et parfaitement audible. Les scholiastes d'Homère précisent que Stentor est d'origine thrace, qu'il est le premier à se servir d'une conque comme trompette de guerre

et qu'il est mis à mort après avoir été vaincu par le dieu Hermès dans une joute vocale. Source [Wikipédia](#)

J'en profite également pour relire le serment des témoins : "Je jure de parler sans haine et sans crainte, de dire toute la vérité, rien que la vérité." (source [Wikipédia : liste des serments](#)).

Je relis la litanie contre la peur.

(normalement, si j'ai réussi mon exercice d'écriture de billet, vous êtes là maintenant chaud bouillant comme je pouvais l'être).

Quand, soudain, l'huissier audiencier sort de la salle et
(roulement de tambours)
(sonneries de trompettes)
(mon cœur s'arrête)
(je me lève, au ralenti, style "Matrix")

Ah, tiens, non, ce n'est pas l'huissier audiencier, c'est Maître Spock.

Maître Spock :

"Bonjour Monsieur l'expert, je suis désolé, mais l'affaire est reportée".

(silence)

Ah, ok.

"Mais elle est reportée à une date ultérieure que je vous communiquerai dès que j'en aurai connaissance".

(re silence)

Oui. Bien sûr.

"Je suis désolé"

(silence encore)

Oui, moi aussi.

Nous sommes sortis du tribunal pour aller prendre un verre avec la presse judiciaire. Après quelques bières, mon sang contenait à nouveau quelques globules rouges. Les discussions portaient sur le futur nouveau gouvernement. Fidèle à ma longue habitude des réunions publiques (c'est-à-dire lorsque je participe à un groupe de plus de deux personnes), je suis resté dans un coin à écouter et à boire les paroles des célébrités présentes.

Bilan :

Points négatifs :

- un procès auquel je ne pouvais pas assister (puisque cité comme témoin)
- 8h de transport (TGV, métro, RER)
- 2h d'attente car arrivé en avance
- 2h d'attente en salle des pas perdus faisant office de salle des témoins
- une journée de congés perdue
- je ne sais pas si je serai remboursé (car je n'ai pas été appelé à la barre)
- ce billet de blog qui est frustrant pour tout le monde

Points positifs :

- j'ai servi la justice et tenté de participer à la défense d'un innocent
- j'ai révisé la litanie contre la peur
- j'ai serré la main (deux fois) de [Pascale Robert Diard](#) et pris un verre avec elle.

That just made my day.

La motivation d'un élu local

En septembre 2006, j'annonçais [dans ce billet](#) (« 1er conseil municipal », tome 1), ma première participation (dans le public !) à un conseil municipal de ma commune. J'ai ensuite participé [à la tenue d'un bureau de vote](#). Et un jour, on m'a demandé [si j'acceptais d'essayer de devenir conseiller municipal](#).

Et en 2008, [j'ai été élu \(brillamment\) conseiller municipal](#).

Sur ce blog, j'ai raconté un peu quelques-unes des facettes de mon activité de conseiller :

- l'élection du maire ([Habemus Papam](#), tome 2)
- la participation aux commissions ([Fluctuat nec mergitur](#), tome 2)
- les élections sénatoriales de 2008 ([Un train de sénateur](#), tome 2)
- les actions caritatives ([La banque alimentaire](#), tome 2 et [Merci](#), tome 4)
- les collections de panneaux de limitation de vitesse ([Les anciens et la vitesse](#), tome 2)
- les élections européennes de 2009 ([Journal d'un bureau de vote](#), tome 3)
- les discussions en conseil municipal ([Bio, nature et pollution](#), tome 3)
- les élections régionales de 2010 ([De l'autre côté du bureau](#), tome 3)
- l'accueil des gens du voyage ([Au nom de la commune](#), tome 4)
- la décision contestée ([L'insolence des riches](#), tome 4)
- l'archaïsme salutaire ([Vous ne pourrez pas vérifier](#), tome 5)

Jusqu'au jour où il a bien fallu se représenter devant les électeurs ([Ensemble, avec Vous et pour Tous, continuons](#)) et chercher à les convaincre de voter pour nous ([Porte à porte](#)).

Maintenant que les élections municipales de 2014 sont terminées, et que je suis réélu pour six ans, le travail continue.

Mes motivations ont-elles changées ?

En 2006, j'avais 42 ans, [l'âge magique](#). J'étais curieux de savoir ce qu'il se passait sur ma commune. J'avais envie de connaître ses développements, son avenir, ses potins.

En 2008, j'avais envie de donner mon avis, même s'il n'était [pas toujours suivi](#).

En 2014 (à 50 ans donc), j'ai envie de vraiment faire avancer certains dossiers qui me tiennent à cœur. C'est pour cela que j'ai proposé au Maire de me confier tous les dossiers en rapport avec le numérique. Il a accepté de me nommer "conseiller délégué au développement du numérique". Je vais pouvoir travailler aux propositions d'évolutions de la commune dans ce domaine, les présenter en commission, puis ensuite au conseil municipal.

Mes objectifs sont les suivants :

- améliorer la communication élus-citoyens, mairie-citoyens et élus-mairie (listes de diffusion, panneaux d'affichage numérique, espaces numériques de travail, réseaux sociaux, textos, etc.)
- encourager l'utilisation maximale des logiciels open source
- promouvoir l'open data
- préparer l'arrivée (un jour ?) de la fibre jusqu'à l'habitant ([FTTH](#)) par la pose de fourreaux sur tous les travaux de voirie et lors de tous les aménagements de lotissements
- encourager la formation numérique des aînées
- faciliter la circulation de l'information
- permettre les réunions à distance grâce aux visioconférences logicielles
- dématérialiser les documents dès que c'est utile...

J'ai quelques idées qui paraissent farfelues au premier abord : filmer le conseil municipal et mettre en ligne les vidéos sur une chaîne YouTube communale, créer un festival numérique, une page Facebook pour la mairie, un atelier GNU/Linux, un atelier d'échange de clefs GPG...

Les idées ne manquent pas, la motivation non plus.

Il reste à prendre en compte les aspects légaux, administratifs, les habitudes, les avis des autres, les aspects financiers, l'inertie générale, la peur du changement, la peur de l'inconnu...

Maintenant qu'un grand nombre de citoyens disposent d'un ordinateur dans leur téléphone, cela devrait être plus facile car l'informatique fait moins peur.

Il suffit juste de ne pas oublier ceux qui n'y ont pas accès.

Il ne faut pas non plus oublier ceux qui ont des handicaps (visuels, auditifs, etc.).

Il ne faut laisser personne sur le côté.

Yapuka...

Les géants

Parfois, je me rends compte à quel point je peux être pitoyable, à mes yeux tout au moins. Pour beaucoup de lecteurs (à ce que je comprends de certains emails que je reçois), je suis une sorte de héros hypercompétent capable de tout faire en informatique. C'est très loin d'être le cas : je suis nul en sécurité informatique, je suis nul en développement informatique moderne, je ne capte rien en téléphonie mobile, [je ne connais pas la différence entre un processus et un thread](#), je ne dispose pas d'outils extraordinaires, ni de connaissances incroyables...

J'ai déjà expliqué tout cela en images dans le billet "[expert judiciaire, ce qu'on pense que je fais](#)".

La justice n'ayant aucun moyen technique à m'offrir, les services de l'état (police ou gendarmerie) ne fournissant aucun logiciel ni matériel aux experts judiciaires hors de leur rang, je me débrouille comme je peux. En voici un exemple.

Un scellé m'est remis pour analyse, avec comme mission principale de relever la présence éventuelle d'images ou de films pédopornographiques. Après la copie du disque dur, me voici à analyser tous les fichiers encore présents, entiers ou sous forme de traces dans les recoins du disque dur.

A un moment de mes observations manuelles, je note la présence du logiciel [Shareaza](#). Je n'ai bien évidemment rien contre le partage P2P, technologie parfaitement légale, mais dans le cas que l'on m'a confié, je m'intéresse de près au contenu partagé.

N'ayant pas la chance de disposer d'un logiciel de type [P2P Marshal](#), me voilà avec sur les bras des dizaines de fichiers avec des noms longs comme un jour sans pain et des extensions ".partial" et ".sd".

Les fichiers ".partial" contiennent les données en cours de téléchargement (ou de partage) et les fichiers ".sd" contiennent des

données de gestion des téléchargements. Une ouverture de ces fichiers .sd avec [Notepad++](#) montre une partie en clair contenant le nom du fichier en cours de téléchargement. Intéressant ! Je trouve dans la plupart des fichiers .sd des noms contenant des références pédopornographiques. Je note tout cela dans mon rapport.

J'installe sur un ordinateur monté pour l'occasion (une machine virtuelle en fait) le logiciel Shareaza que je récupère sur internet dans la même (ancienne) version que celle trouvée sur l'ordinateur placé sous scellé. Je télécharge quelques vidéos et documents mis en partage de manière légale par des internautes, et j'observe le comportement des différents fichiers .part et .sd lors des différentes manipulations.

A un moment, je réalise que, comme la plupart des fichiers .part nommés dans les fichiers .sd contiennent des vidéos, il me suffit de renommer les fichiers en question avec l'extension correspondant au type de vidéos qu'ils sont censés contenir : j'ajoute .avi/.mpg/.mov au choix après l'extension .partial et j'essaye d'ouvrir la vidéo avec [VLC](#).

VLC est un logiciel fantastique qui a entre autre la capacité de lire des vidéos incomplètes, avec des pans entiers manquants.

Bingo, j'arrive à lire toutes les vidéos (ou presque), dont celles de nature pédopornographique. Je passe encore un week-end pénible, [à classer les vidéos](#), à en extraire des images choisies pour le rapport et à les graver sur un DVD annexé au rapport.

Rien d'autre qu'un travail fastidieux, loin de l'image d'Épinal de l'expert omniscient et omnipotent, enfermé dans mon bureau pour éviter que mes enfants ne voient leur père regarder des images pédophiles sur ses écrans.

Je l'ai déjà écrit moult fois ici même : [je suis nul](#) et [je suis faible](#).

"Nous sommes des nains juchés sur des épaules de géants. Nous voyons ainsi davantage et plus loin qu'eux, non parce que notre vue est plus aiguë ou notre taille plus haute, mais parce qu'ils nous portent en l'air et nous élèvent de toute leur hauteur gigantesque."
(Bernard de Chartres, XIIe siècle)

Évidemment, les géants représentent nos prédécesseurs, mais aussi le savoir accumulé dans les livres ou sur internet. C'est aussi l'expérience de nos collaborateurs, les conseils de nos aînés, les avis de nos confrères.

Merci à tous les géants.



42 ans

Nous avons tous des êtres chers qui disparaissent trop tôt. Je ne suis pas épargné par la grande faucheuse qui tranche autour de moi. Cette peine intime, je la garde pour mes proches et pour moi.

Pourtant, tous les 27 avril sur ce blog, je parle du geste désespéré d'un de mes étudiants qui a mis fin à ses jours en pleine jeunesse. J'étais jeune maître de conférences et il avait brillamment effectué son stage avec moi. Il s'était enthousiasmé pour les réseaux de neurones avec lesquels je jouais.

C'était il y a longtemps, il y a 22 ans.

Dans sa lettre d'adieu à ses parents, il a écrit qu'un des rares bons moments qu'il avait passé dans les derniers mois de sa courte vie était avec moi, pendant son stage. Cet aveu m'a toujours déchiré le cœur.

Avec en plus le regret de n'avoir pas vu son mal vivre, alors que nous étions complices de travail.

Il aurait fêté aujourd'hui son anniversaire.

Bon anniversaire Stéphane, tu es toujours dans mon cœur et tu as toujours vingt ans.

Réseaux de neurones 2

Ce billet est la suite [de celui-ci](#) (« Réseaux de neurones 1 », tome 5) qu'il est préférable de lire avant mais c'est vous qui voyez.

Après quelques heures passées sur l'apprentissage du langage Go, je me suis résolu à revenir à mes fondamentaux : le langage C. Cela fait 20 ans que je n'ai pas codé sérieusement, et j'ai eu peur de perdre trop de temps à m'initier à un nouveau langage. Ce qui suit va faire sourire tous les développeurs actuels et définitivement me décrédibiliser auprès d'eux...

Il y a 20 ans, j'étais chercheur et je programmais sur une station de calcul [Apollo](#), dans un environnement de développement équivalent à vi (sous [Domain/OS](#)). J'appelais quelques routines graphiques de base, à une époque où l'environnement graphique informatique était en pleine révolution. Mes langages favoris étaient le [langage OCCAM](#) et le langage C.

Lorsque de chercheur, je suis devenu professeur en école d'ingénieurs, j'ai enseigné le langage C. La mode était alors au Turbo C de Borland. Mon enseignement n'incluait pas la partie graphique. Mes étudiants se contentaient très bien des tableaux de pointeurs de fonctions de structures doublement chaînées, et des envois de données sur le réseau.

Me voici donc aujourd'hui (enfin, il y a quelques mois), à me demander ce qui pouvait être utilisé comme [IDE](#) aujourd'hui, avec tous les progrès informatiques. Je me suis dit qu'un environnement multiplateformes pourrait être intéressant, pour profiter du meilleur des univers Windows ou GNU/Linux.

J'ai choisi [Code::Blocks](#).

Me voici donc en train de compiler quelques programmes simples trouvés sur les différents sites d'initiation à cet IDE. Je redécouvre alors la joie de compiler un code source, d'[éditer les liens](#) avec les

bibliothèques standards, et de voir les premiers "Hello world" à l'écran. J'ai eu une petite pensée pour [Dennis MacAlistair Ritchie](#)...

Très vite, je me suis retrouvé à écrire quelques procédures de calcul concernant les réseaux de neurones. J'ai créé mon premier réseau, mes premières structures, mes premiers malloc (et à chaque malloc son free correspondant ;-).

Comme 20 ans auparavant, j'ai vite trouvé l'affichage standard limité : il me fallait tracer des courbes, des nuages de points, des évolutions de critères en cours de [minimisation](#). Il me fallait appeler quelques fonctions graphiques...

Et là... Grosse déception !

En 20 ans de foisonnement d'interfaces graphiques et d'amélioration de processeurs spécialisés, aucune bibliothèque graphique SIMPLE n'a l'air de s'être imposée. Un truc du genre : j'ouvre une fenêtre, je dessine un pixel dedans quand je veux et basta. Si je suis sous Windows, ça m'ouvre une fenêtre Windows, si je suis sous GNU/Linux, et bien ça m'ouvre une fenêtre GNU/Linux... Bon, j'avoue que je n'ai pas beaucoup cherché, et je compte un peu sur vous pour me montrer la voie si je me suis fourvoyé.

J'ai choisi la [bibliothèque graphique SDL](#) parce que pas mal de sites ont l'air de dire que c'est très bien pour s'initier. Ça tombe bien, parce que je ne souhaite pas devenir un professionnel du graphisme, je veux juste dessiner quelques courbes.

Ce qui m'a un peu surpris, c'est de devoir "bidouiller"

Code::Blocks pour que mes premiers programmes utilisant SDL puissent fonctionner (je n'ai pas conservé les messages d'erreur, mais j'ai ramé). Heureusement, pas mal de monde utilise le combo Code::Blocks + SDL et la communauté publie des tutos bien faits.

Me voici donc en train de faire mes premières courbes. Bon, mes programmes sont devenus beaucoup moins lisibles maintenant que je les ai truffés d'appels à des routines graphiques plus ou moins claires, mais j'ai compris les bases du truc. Jusqu'au jour où j'ai voulu tracer une courbe dans une nouvelle fenêtre... En effet, SDL ne permet pas d'ouvrir plusieurs fenêtres. Mais heureusement SDL2 peut le faire ! Sauf qu'il faut tout réécrire car les concepts graphiques n'ont rien à voir. Je me suis donc tapé [le guide de migration SDL1.2 vers SDL2.0](#) dans la même journée que l'apprentissage de SDL1.2. Je râle, je râle, mais je remercie tous les développeurs qui consacrent leur vie à créer tous ces outils (et les manuels qui vont avec). Je sais maintenant manipuler (un peu) les pointeurs de fenêtres et de [Renderer](#).

Comme SDL2 est sortie en août 2013, j'ai un peu galéré à trouver comment adapter Code::Blocks pour faire fonctionner mes premiers programmes SDL2 (mais j'ai trouvé !). Et j'ai pleuré des larmes de joie quand j'ai vu mes premières courbes tracées dans deux fenêtres séparées.

J'ai ensuite pu attaquer les choses sérieuses avec la mise au point des routines d'optimisation. J'en ai déjà expliqué une partie [dans ce billet](#) (« Minimisation », tome 4). Mes premiers programmes ont consisté à mettre au point les routines suivantes :

- calcul du gradient par rétropropagation de l'erreur
- méthode d'optimisation par descente de gradient à pas constant
- amélioration de la méthode précédente avec calcul économique d'un pas variable (méthode de Wolfe et Powell)
- amélioration de la méthode précédente avec calcul itératif de l'inverse du Hessien (méthode de Broyden, Fletcher, Goldfarb et Shanno).

Je suis toujours bluffé par l'accélération foudroyante des méthodes quasi-newtoniennes pour s'approcher du minimum de la fonction.

J'en suis là aujourd'hui.

J'ai un programme illisible qui fonctionne malgré tout parfaitement : je peux créer un réseau de neurones complètement connecté qui peut apprendre virtuellement n'importe quel ensemble d'apprentissage, dès lors que celui-ci est constitué d'un nombre fini de couples {entrées connues, sorties désirées}. Je suis à la recherche d'un problème pas trop complexe, en évitant si possible tous les problèmes de classification (type mémorisations de visage ou reconnaissance de caractères). J'aimerais plutôt un problème de modélisation, comme par exemple la prédiction des éruptions du "[Old Faithful](#)" (si quelqu'un a des données récentes sur ce geysier, avec températures, pression, etc.).

Il me faut du temps pour rendre mes routines plus lisibles, pour sauvegarder les coefficients calculés, pour tester d'autres environnements, pour créer un tableur Excel et OpenOffice, pour trouver un problème intéressant à ma portée...

Il me faut aussi comprendre comment faire pour exploiter toute la mémoire de ma machine. Je n'arrive pas encore à créer des matrices de grandes tailles (du genre 10000x10000 réels double précision). Je suis pour l'instant limité à un réseau d'au maximum 50 neurones et 1224 connexions.

Mais 50 neurones, c'est déjà beaucoup ;-)

Expert près la Cour Administrative d'Appel

Pour la première fois, les Cours Administratives d'Appel sont tenues de mettre en place un tableau des experts. Si vous souhaitez postuler pour y être inscrit, il faut déposer la demande d'inscription avant le 15 septembre prochain. Je vous recommande d'anticiper cette date le plus possible pour éviter le rejet inéluctable de votre demande en cas de dossier incomplet.

Mais avant, revoyons tout cela tranquillement.

Qu'est-ce que donc que la justice administrative ?

N'ayant jamais étudié le droit, je fais partie des Mékeskidi en la matière. Heureusement, il y a d'excellents sites qui expliqueront tout cela mieux que moi, à commencer par celui de Maître Eolas :

- le grand divorce de 1790 : la séparation des autorités administratives et judiciaires : <http://www.maitre-eolas.fr/post/2007/07/13/665-le-grand-divorce-de-1790-la-separation-des-autorites-administratives-et-judiciaires>
- L'autre justice : <http://www.maitre-eolas.fr/post/2007/07/16/666-l-autre-justice>
- L'autre Justice (2) : <http://www.maitre-eolas.fr/post/2007/07/18/670-l-autre-justice-2>

Pour ceux qui ont le tort de ne pas lire ces trois billets, voici un raccourci :

Il existe en France deux juridictions séparées : l'ordre administratif et l'ordre judiciaire. L'existence de ces deux ordres de juridictions distincts est en France le produit de l'histoire, fruit de la volonté d'empêcher le juge judiciaire de s'immiscer dans les questions de l'administration (source [Wikipédia](#)).

Tenant compte des déboires qu'ont connus les Rois de France avec les parlements et craignant d'être entravés à leur tour dans leur action, les révolutionnaires construisent un système visant à empêcher les magistrats d'influer sur la vie politique et législative.

Du juge, ils n'attendent que la stricte application de la loi, émanation de la souveraineté populaire, qui ne souffre ni interprétation,

ni détournement -interdiction leur est faite de prendre des décisions de règlement, et obligation leur est faite d'en référer au législateur pour interpréter la loi. Mais avant tout, les révolutionnaires interdisent aux juridictions judiciaires d'exercer leur contrôle sur les différends susceptibles de naître entre les administrés et l'administration.

Dès lors, sont créés deux ordres distincts : un ordre administratif, chargé du contentieux administratif opposant les citoyens à l'administration, et un ordre judiciaire, chargé de régler les conflits entre personnes privées et de sanctionner les infractions à la loi. (source justice.gouv.fr)

Et les experts dans tout cela ?

Attention, en parlant d'"experts", il faut bien préciser le mot, tant la notion est floue et prête à confusion dans la langue française. Les tribunaux de l'ordre judiciaire, lorsqu'ils ont besoin de l'aide d'un technicien pour juger une affaire, font appel à des personnes inscrites sur une liste tenue par chaque Cour d'Appel. Les personnes inscrites sur ces listes sont appelés "experts judiciaires".

Jusqu'au 31 décembre 2013, un seul article du code de justice administrative faisait référence à l'établissement des tableaux d'experts : "*chaque année, le président procède, s'il y a lieu, à l'établissement du tableau des experts près la juridiction qu'il préside*". Depuis le 1er janvier 2014, cet article est remplacé et les Cours Administratives d'Appel doivent mettre en place une liste expertale.

Expert administratif ?

Quel sera le titre donné à ces "nouveaux" experts, je ne sais pas. Le [décret n°2013-730 du 13 août 2013](#) portant modification du code de justice administrative, ne parle en effet (dans son [chapitre IV](#)) que "d'un tableau des experts auprès de la cour et des tribunaux administratifs du ressort". Mais les associations qui regroupent les personnes inscrites sur ce type de liste ont trouvé un terme : au lieu "d'expert judiciaire", il faudrait maintenant parler "d'expert de justice". Toutes les associations ont donc changé leurs noms (ou sont en train de le faire), ce que vous pouvez constater dans votre moteur de recherche favori en tapant les mots clefs "compagnie" "expert" "judiciaire" (exemple [ici avec mon moteur préféré](#)).

Pour ma part, je trouve tout cela un peu confus, puisque l'inscription à une association d'experts n'est pas obligatoire, et qu'il y aura des experts judiciaires non administratifs, des experts administratifs non judiciaires et des experts judiciaires et administratifs... J'attends d'y voir plus clair avec un texte de loi. En attendant, je parlerai d'expert administratif, ou d'expert près une cour administrative d'appel.

Il est à noter qu'aucune procédure n'a été créée (à ma connaissance) pour le tableau des experts près le Conseil d'État, qui est le pendant de la Cour de Cassation.

La procédure d'inscription

Le président de la cour administrative d'appel procède aux inscriptions, après avis d'une commission composée des présidents des tribunaux administratifs du ressort et d'experts en nombre au moins égal au tiers de ses membres. Il arrête les inscriptions en fonction des besoins des juridictions dans les différents domaines d'activité dans lesquels les juridictions administratives peuvent avoir recours à une expertise. Ces domaines d'activité sont recensés dans [une nomenclature arrêtée par le vice-président du Conseil d'Etat](#).

Vous noterez la ressemblance avec la nomenclature utilisée par l'ordre judiciaire.

Voici quelques rubriques pouvant intéresser un informaticien :

E. — INDUSTRIES

E.1. Électronique et informatique.

E.1.1. Automatismes.

E.1.2. Internet et multimédia.

E.1.3. Logiciels et matériels.

E.1.4. Systèmes d'information (mise en œuvre).

E.1.5. Télécommunications et grands réseaux.

F. — SANTÉ

F.5. Biologie médicale et pharmacie.

F.5.5. Biostatistiques, informatique médicale et technologies de communication.

G. — MÉDECINE LÉGALE, CRIMINALISTIQUE ET SCIENCES CRIMINELLES

G.2. Investigations scientifiques et techniques.

G.2.5. Documents informatiques.

Si vous travaillez dans un service informatique :

G.3. Armes. — Munitions. — Balistique.

G.3.1. Balistique.

G.3.2. Chimie des résidus de tir.

G.3.3. Explosifs.

G.3.4. Munitions.

G.3.5. Technique des armes.

sans oublier

H.1. Interprétariat.

H.1.3. Langue française et dialectes.

H.3. Langue des signes et langage parlé complété.

(rhooo, je plaisante...)

Les conditions pour être inscrit au tableau des experts administratifs

Pour être inscrit, l'expert doit satisfaire à cinq conditions définies à l'article R. 221-11 du code de justice administrative :

- Justifier d'une qualification et avoir exercé une activité professionnelle, pendant une durée de dix années consécutives au moins, dans le ou les domaines de compétence au titre desquels l'inscription est demandée, y compris les qualifications acquises ou les activités exercées dans un État membre de l'Union européenne autre que la France ;
- Ne pas avoir cessé d'exercer cette activité depuis plus de deux ans avant la date de la demande d'inscription ou de réinscription ;
- Ne pas avoir fait l'objet d'une condamnation pénale ou d'une sanction disciplinaire pour des faits incompatibles avec l'exercice d'une mission d'expertise ;
- Justifier du suivi d'une formation à l'expertise ;
- Avoir un établissement professionnel ou sa résidence dans le ressort de la cour administrative d'appel.

Les experts déjà inscrits sur les listes d'experts judiciaires sont réputés satisfaire, à l'issue de la période probatoire, aux conditions énoncées aux quatre premiers points.

Comment s'inscrire ?

Le dossier de demande d'inscription doit être adressé au président de la cour administrative d'appel avant le 15 septembre (il serait folie de l'envoyer le 14 septembre !). La première inscription est faite pour une durée probatoire de trois ans à l'issue de laquelle l'expert peut demander sa réinscription pour une période de cinq ans (art. R.221-12).

Le président de la cour administrative d'appel prend l'avis d'une commission présidée par lui-même et composée des présidents des tribunaux administratifs du ressort de la cour et d'experts inscrits au tableau de la cour (au moins deux experts sans que leur nombre puisse excéder le tiers des membres de la commission) (art. R.221-10). La commission tient compte des besoins des juri-

dictions du ressort (art. R.221-14). La décision de refus d'inscription ou de réinscription d'un candidat doit être motivée (art. R.221-15). Les décisions de refus d'inscription ou de réinscription d'un candidat, de retrait ou de radiation d'un expert du tableau peuvent être contestées. Elles sont examinées par une autre cour administrative d'appel (art. R.221-19).

Les experts inscrits au tableau d'une cour administrative d'appel doivent adresser à la fin de chaque année civile un état des missions qui leur ont été confiées, des rapports déposés et des missions en cours ainsi que des formations suivies au cours de l'année (art. R.221-16).

Il est important de noter l'importance de la partie du document suivante :

« *Les organismes de droit public ou privé intervenant dans mon domaine d'activité avec lesquels j'entretiens des liens directs ou indirects sont les suivants :* » où le candidat doit mentionner les organismes de droit public (État, collectivités territoriales, établissements publics tels que CHU, etc.) ainsi que les organismes de droit privé (sociétés de droit commercial, compagnies d'assurances, laboratoires privés, associations, etc.) avec lesquels il entretient des relations qui ne sont pas occasionnelles, sous quelque forme que ce soit.

Et après ?

Je suis en train de constituer mon dossier. Je suis toujours enthousiaste à l'idée de mettre mes compétences au service de la justice. Mes contacts au sein de la magistrature administrative sont dubitatifs sur l'idée d'avoir besoin d'un expert en informatique. Cela m'étonne : n'y aurait-il pas de litiges entre les citoyens et l'administration en France où l'informatique serait partie prenante ?

On verra bien si mon dossier est retenu. Si non, tant pis, je retenterai une deuxième fois (comme pour celui d'expert judiciaire).

Je ne manquerai pas de vous tenir au courant du suivi.

Je vous prie de croire, chère lectrice, cher lecteur, à l'expression de mes salutations distinguées.

Zythom

Réseaux de neurones 3

Ce billet fait partie [d'une série](#) (« Réseaux de neurones 1 », tome 5 et « Réseaux de neurones 2 », tome 6 ci-avant) qu'il vaut mieux avoir lu avant, mais c'est vous qui voyez.

[Nous avons vu](#) que pour jouer avec un neurone, il fallait calculer son potentiel (la somme pondérée des sorties des neurones qui lui sont connectés), puis sa sortie grâce à sa fonction d'activation. Je n'en ai pas encore parlé, mais pour pouvoir modifier les coefficients du réseau, il faut aussi connaître la dérivée de la fonction d'activation du neurone. Idem pour la variable "erreur" dont je parlerai un peu plus tard, pendant la phase d'apprentissage du réseau.

Si vous êtes étudiant et que vous souhaitez travailler sérieusement sur les réseaux de neurones, je vous conseille d'étudier attentivement le code source d'une bibliothèque telle que [FANN](#) qu'un lecteur m'a recommandé et qui a l'air très bien. Dans mon cas, je suis partisan d'un travail artisanal qui permet de mieux comprendre les différents mécanismes en jeu. Et puis, j'aime bien le blog de Libon : [fabriqué à mains nues](#), alors...

Pour moi, un neurone, en langage C, c'est donc cela :

```
typedef struct neur
{
    double sortie;           /* état du neurone i */
    double (*pfonct_activ)(double); /* fonction d'activation */
    double potentiel;       /* potentiel du neurone */
    double (*pfonct_deriv)(double); /* fonction dérivée */
    double err;             /* erreur */
} NEUR;
```

Avec cette déclaration, un réseau de neurones peut être le simple tableau suivant : `NEUR* neurone[NBMAXNEUR]`; où `NBMAXNEUR` est une constante indiquant le nombre total de neurones (y compris les entrées du réseau).

La création d'un réseau se fera alors de manière dynamique avec un petit programme du type :

```
for (i=0; i<NEMAXNEUR; i++)
{
    neurone[i]=(NEUR*)malloc(sizeof(NEUR));
    if (neurone[i]==NULL)
    {
        fprintf(stderr,"Allocation neurone numéro %ld impossible \n",i);
        exit(EXIT_FAILURE);
    };
};
```

Note à moi-même pour plus tard : ne pas oublier un appel à "free()" pour chaque appel à "malloc()".

Parmi tous les réseaux de neurones possibles, j'ai choisi de travailler avec un réseau complètement connecté à une seule sortie. Il s'agit du type de réseau possédant le plus de liens possibles entre les neurones.

Il est assez facile à construire :

- le 1er neurone est relié à toutes les entrées du réseau
- le neurone suivant est relié à toutes les entrées du réseau, et à la sortie du premier neurone,
- le Nème neurone est relié à toutes les entrées du réseau, et à la sortie de tous les neurones précédents,
- la sortie du réseau est la sortie du dernier neurone.

Je vous ai fait un petit dessin qui montre ce type de réseau :

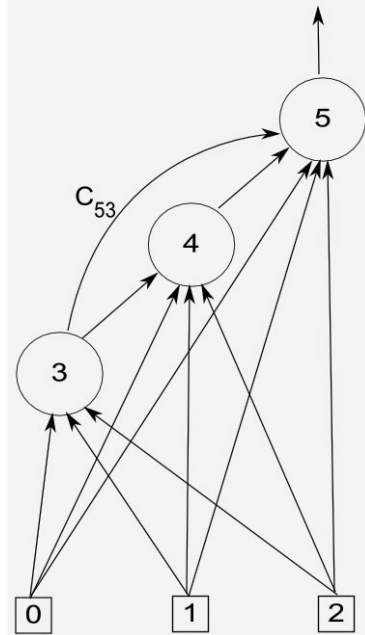


Figure 1 : Réseau complètement connecté avec 3 entrées, 3 neurones et une sortie

Dans un réseau de neurones, le cœur du problème, ce qu'il faut rechercher, ce sont les coefficients des liens reliant les neurones entre eux. Le coefficient reliant le neurone j vers le neurone i s'appelle C_{ij} . Par exemple, sur la figure 1, le coefficient reliant 3 à 5 s'appelle C_{53} (attention au sens).

Pour faire très simple, et suivre la notation utilisée, j'ai choisi une matrice pour stocker les coefficients C_{ij} : double coef[NBMAXNEUR][NBMAXNEUR];

où NBMAXNEUR contient le nombre d'entrées et le nombre de neurones (soit 6 sur la figure ci-dessus). Ainsi, le coefficient C_{53} est stocké dans coef[5][3]. Ma matrice aura beaucoup de zéros, mais je privilégie la simplicité.

La propagation de l'information au sein du réseau se fait donc de la manière suivante :

```
for (i=NBENTREES; i<NBMAXNEUR; i++)
{
    pot=0.0;
    for (j=0; j<i; j++)
    {
        pot=pot+coef[i][j]*neurone[j]->sortie;
    };
    neurone[i]->potentiel=pot;
    neurone[i]->sortie=(neurone[i]->pfonct_activ)(pot);
};
```

La sortie du réseau est donc `neurone[NBMAXNEUR-1]->sortie`

Les entrées du réseau sont considérées comme des neurones particuliers très simples (pas de liens vers eux, pas de fonction d'activation, potentiel égal à l'entrée).

Le prochain billet sera consacré à l'apprentissage d'un tel réseau de neurones (ie : au calcul des coefficients du réseau). On révisera aussi un peu les fonctions. Il vaut mieux aller doucement.

Points de vue

Nous sommes plusieurs hommes en costume ou en uniforme dans la pièce, sous le regard stressé du locataire des lieux qui assiste à notre perquisition.

Quelques minutes auparavant, nous avons sonné à 6h05 à la porte du logement, comme demandé par notre ordre de mission. J'assiste les forces de l'ordre, l'huissier et le serrurier. Je n'en mène pas large.

L'homme nous a ouvert la porte un peu hagard. Il était déjà debout et en train de se préparer pour aller travailler. Sa femme est en robe de chambre, se demande ce qu'il se passe, qui peut frapper à la porte à cette heure, et nous dit de ne pas faire de bruit pour ne pas réveiller les enfants.

Chacun observe la scène de son propre point de vue. L'huissier explique l'intervention à l'homme qui vient d'ouvrir la porte, les policiers sont en attente, légèrement en retrait. Le serrurier et moi sommes derrière ce rideau humain en train de découvrir la violence psychologique de ce type d'intervention. L'homme qui ouvre la porte écarquille les yeux et écoute les griefs qui lui sont reprochés. Sa femme qui est derrière lui est en colère mais pense à ses enfants qui dorment...

Je suis maintenant dans une pièce encombrée de matériel informatique : plusieurs ordinateurs fixes, des ordinateurs portables, des téléphones, des switchs, des câbles... Sans bruit, les policiers ouvrent les armoires, les tiroirs, les placards, pendant que l'huissier prend des notes. La liste du matériel à analyser s'allonge, me dis-je. Le serrurier s'ennuie dans un coin.

J'entends un enfant qui pleure et sa maman qui lui parle pour le rassurer. Quelques minutes après, je le vois entrer dans le bureau où nous sommes. Il me regarde. De son point de vue, je suis un étranger qui est dans le bureau de son papa en train de fouiller ses affaires.

Je l'ai lu quelque part, les enfants voient le monde plus grand qu'il n'est, plus impressionnant. Pour leur parler, il est conseillé de se mettre à leur hauteur. Face à cet enfant apeuré, mais suffisamment courageux pour affronter un groupe d'inconnus, je m'assois sur les talons et met mon regard au niveau du sien. Je lui parle avec ma voix la plus douce possible en essayant d'y gommer toute la tension que je ressens. Je le rassure sur nos intentions, je reprends les arguments utilisés par sa mère. Il repart prendre son petit déjeuner.

Pendant notre échange de moins d'une minute, tout le monde s'est arrêté de parler et de travailler, pour nous regarder et nous écouter. Les policiers ont hoché la tête en voyant le "petit d'homme" partir la tête haute. Le père a hoché la tête. La mère, toujours en colère, m'a foudroyé du regard. Question de point de vue.

Avant de me relever, je perçois sous le plan de travail du bureau, un petit [NAS](#) qui est jusqu'à présent passé inaperçu à la fouille du bureau. J'ai pu le signaler à l'huissier qui l'a ajouté à ses notes, et a allongé ma liste des choses à analyser. Il n'était visible qu'accroupi devant le bureau. Question de point de vue.

--oOo--

Il y a plusieurs façons de réagir à cette anecdote :

- il y a le lecteur qui privilégiera le point de vue "intrusion dans la vie privée".

Le réflexe est alors de se mettre du côté de la famille, de se demander si c'est bien normal de pouvoir entrer chez les gens comme cela. La maison doit être sanctuarisée. C'est un point de vue que je partage aussi.

- il y a celui qui se demandera comment mieux planquer ses données.

Cacher ses données privées pour les protéger devrait être un réflexe chez tout le monde. Les solutions ne manquent pas : externalisation chez un tiers de confiance, répartition dans plusieurs pièces, chiffrement, etc. Les données privées doivent répondre à des niveaux d'accès contrôlés : le monde extérieur, les amis, les enfants, le conjoint... Et il faut bien sur prévoir le cas où le monde extérieur s'invite à l'intérieur. C'est mon point de vue.

- il y a celui qui se placera du côté de la loi, du côté de la force publique, du côté de la société, du côté des victimes de cet homme.

Cet homme est suspecté d'avoir commis des actes criminels odieux. Il est facile de le voir comme un monstre, comme un danger pour les autres. Et si c'était mes enfants qui avaient été les victimes de ses actes ? Je partage ce point de vue.

- il y a celui qui se placera du côté de l'expert.

Comment un homme de science réagit-il lorsqu'il est sorti de sa tour d'ivoire pour être plongé dans le quotidien d'un huissier, d'un policier ? Est-il formé, est-il prêt ? Doit-il assister en simple spectateur et refuser d'être acteur ? Doit-il tout accepter, ou tout laisser faire ? [L'expérience de Milgram](#) est passée par là...

- il y a le point de vue du policier, de l'huissier, du magistrat, de l'informaticien, de l'avocat, mais aussi du comptable, de l'instituteur, de l'ancienne victime, du politique, du médecin, de la secrétaire... J'écoute souvent ses points de vue lorsque je discute avec ces personnes. Je partage souvent leurs vues.

Prêter ses connaissances au service de la justice, c'est aussi remettre en cause ses positions, ses opinions, son point de vue. C'est faire du doute un élément de méthodologie scientifique. Les choses sont toujours plus compliquées qu'elles n'en ont l'air. Le café du commerce est un monde en noir et blanc sans nuances de gris ni couleurs.

Enfin, c'est mon point de vue.

Et le vôtre ?

Ils avaient

Je travaille dans une école d'ingénieurs qui recrute des terminales S bientôt fraîchement titulaires du baccalauréat. Leurs dossiers d'inscription portent pour la plupart comme année de naissance, l'année 1996... Ils ont à peine 18 ans aujourd'hui.

Ils sont nés en même temps que la brebis Dolly, premier mammifère cloné de l'histoire ([5 juillet 1996](#)). La même année les Spice Girls sortaient leur tube [Wannabe](#). Bill Clinton préside les États-Unis, Boris Eltsine la fédération de Russie et Jacques Chirac la France.

1996, c'est l'année de la création de l'[April](#). C'est aussi l'année où les informaticiens commencent à se faire entendre sur le problème [du codage des dates](#) avec le prochain passage de 99 à 00. Cette même année sort [Tomb Raider](#) sur DOS, PlayStation, [Sega Saturn](#) et Macintosh.

Ils avaient à peine un an quand l'Angleterre a restitué Hong-Kong à la Chine (1er juillet 1997), quand la princesse Diana s'est tuée dans un accident de voiture à Paris (31 août 1997) et à la mort de Mère Thérèse (5 sept 1997).

Ils avaient aussi un an lors de la sortie de [Titanic](#).

Ils avaient deux ans lors de la sortie de l'[iMac](#) qui colora l'informatique en même temps que sortait [Windows 98](#), et que l'obscur société [Google naissait dans un garage](#). Ils ne s'en souviennent pas, mais leurs parents les portaient fièrement au dessus de la foule lors de la fête de la victoire de la France contre le Brésil, 3-0.

Ils avaient 2 ans lorsque l'[euro](#) a remplacé l'[ECU](#), 5 ans quand il a remplacé le [franc français](#). Autant dire qu'ils n'ont jamais connu d'autre monnaie que l'euro.

Ils avaient 4 ans lors du changement de siècle et de millénaire, lors de la création de [Wikipédia](#).

Ils avaient 5 ans lors des attaques du 11 septembre 2001 que j'espère ils n'ont pas vu en direct à la télévision (pour ma part j'étais en TP d'informatique et nous regardions les images en direct sur internet).

[Altavista](#) régnait en maître sur les moteurs de recherche.

Ils avaient 6 ans lorsque la navette spatiale Columbia s'est désintégrée lors de son retour sur Terre ([1er fév 2003](#)).

Ils avaient 7 ans lors de la naissance de [Facebook](#) (4 fév 2004), 10 ans quand ils auraient pu commencer à s'en servir (26 sept 2006), mais il fallait avoir au moins 13 ans...

Ils avaient 8 ans à la naissance d'[Ubuntu](#) (20 oct 2004) et au lancement de [YouTube](#) (14 fév 2005), 9 ans à l'arrivée au pouvoir d'Angela Merkel (22 nov 2005) et 10 ans lors du premier [tweet](#) (21 mars 2006).

Ils avaient 12 ans lors de l'élection de [Barack Hussein Obama II](#). Autant dire que pour eux, un président des États-Unis, c'est grand, noir et cool.

Ils avaient 13 ans lors du vote de la loi Hadopi qui a rendu le partage non marchand illégal.

Ils ont toujours connu la téléphonie mobile et n'ont pour la plupart jamais vu un téléphone à cadran rotatif (et ne sauraient pas s'en servir...). iOS et Android n'ont aucun secret pour eux.

Ils ont tout juste 18 ans aujourd'hui.

Pour eux, je serai le vieux con qui les appelle "[Monsieur](#)" ou "[Madame](#)"...

Bienvenue à eux :-)

L'interrogatoire

L'homme qui est en face de moi est souriant. Il m'inspire confiance et coopère complètement avec moi, malgré le stress.

Il faut dire que ce n'est jamais très agréable de se retrouver avec, dans son bureau, un expert judiciaire, son patron, un huissier de justice et un représentant syndical...

Pour lui, tout cela n'était pas prévu.

Je lui pose des questions sur son métier d'informaticien, sur l'entreprise dans laquelle il travaille, sur ses responsabilités. Je lui pose quelques questions techniques pour lui montrer que je partage avec lui un intérêt et des compétences similaires. Nous sommes du même monde, ce monde informatique que peu d'utilisateurs comprennent vraiment...

Il est à lui tout seul le service informatique : il gère le réseau, le serveur, la hotline, les commandes, les réparations, les interventions. L'entreprise n'est pas bien grande, mais il en est l'homme clef pour la partie informatique/réseau/télécom.

Je lui pose LA question : "avez-vous utilisé le mot de passe de votre patron pour vous connecter sur son compte et accéder à des données confidentielles ?"

Il me regarde et sa réponse est limpide : "Non. Je n'ai pas accédé au compte informatique de mon patron." Son regard est franc, un bon rapport de confiance s'est établi entre nous, il est jeune, il manque encore un peu d'expérience, je le crois.

Je demande au patron l'autorisation d'avoir accès aux différents ordinateurs utilisés par son informaticien. Il y a un ordinateur de travail posé sur un bureau encombré de câbles, de post-it, de figurines de Star Wars. Je passe une heure entouré de tout ce petit monde à regarder son contenu, à expliquer à l'huissier ce que je

fais, ce que je vois. Je contourne le répertoire marqué "privé", bien que l'ordinateur soit strictement professionnel.

Il faut dire que nous sommes en pleine période "[arrêt Nikon](#)" et que beaucoup de discussions ont lieu sur la cybersurveillance. Tout ce que je sais, c'est que pour qu'une fouille soit possible, qu'elle concerne une armoire personnelle ou un support dématérialisé, elle doit avoir un fondement textuel, ou être justifiée par des circonstances exceptionnelles et des impératifs de sécurité, ou être contradictoire, et respecter le principe de proportionnalité. Je ne suis pas un fin juriste, mais je n'ouvre les répertoires privés qu'en dernier recours... Les photos des enfants et de la famille qui trône autour sur les écrans suffisent déjà à me mettre mal à l'aise.

L'ordinateur fixe semble clean, je ne trouve rien de suspect. Je demande à l'informaticien s'il dispose d'un ordinateur portable pour son travail. Il me répond que oui, qu'il est dans sa sacoche. Le patron fait quelques commentaires sur le prix de ce joujou qui, à l'époque, coûte plusieurs fois le prix d'un ordinateur fixe.

J'interroge l'informaticien sur l'utilisation de cet ordinateur portable. Il m'explique que cela facilite ses interventions sur les actifs du réseau, ou à distance lorsqu'un problème survient et qu'il est chez lui. Il est très fier de m'indiquer qu'il dispose d'une ligne ADSL, chose plutôt rare à l'époque. Nous échangeons sur le sujet quelques commentaires techniques, le courant passe bien entre nous. Je compatis à sa situation embarrassante de premier suspect aux yeux de son patron.

Il me fournit facilement les mots de passe d'accès aux machines, aux applications. Il est serein et répond facilement à mes questions. Une heure se passe encore, et je ne trouve rien de particulier sur son ordinateur portable.

Je prends dans ma mallette un liveCD ([HELIX](#), distribution gratuite à l'époque. Aujourd'hui j'utilise [DEFT](#)) pour démarrer son portable sans modifier son disque dur. Je lance quelques outils d'investigation.

Je vois son regard intéressé de connaisseur. J'explique ce que je fais pour que l'huissier puisse rédiger son rapport. Je sens l'attention de l'assistance remonter un peu après ces deux heures plutôt soporifiques.

Je demande au patron son mot de passe. Un peu surpris, celui-ci me le donne. Je le note, et l'huissier aussi. Je fais une recherche du mot de passe en clair avec une [expression rationnelle](#) simple.

Et là, bingo. Je trouve le mot de passe du patron en clair. Stocké dans un fichier effacé.

Je lève les yeux, je regarde l'homme assis à côté de moi. Sans un mot. Son visage jovial se transforme. Son regard se durcit. J'y vois de la haine. La métamorphose est tellement rapide que je reste stupéfait. Personne autour de nous n'a encore compris ce qu'il vient de se passer.

J'explique à voix haute ce que je viens de trouver : un fichier effacé contenant le mot de passe en clair du patron. Une analyse rapide montre la présence du logiciel [John The Ripper](#).

Je me suis fait balader depuis le début.

Le contact amical que j'avais établi était une illusion.

L'innocent vient de devenir coupable.

La suite de l'enquête montrera le piratage du compte du patron, les accès aux données confidentielles et leurs modifications.

Je ne suis pas fait pour mener correctement un interrogatoire : j'ai trop d'empathie. Mais jamais je n'oublierai la transformation de son visage et l'étincelle de haine que j'ai vue dans son regard ce jour-là.

Petit guide de survie à l'expertise informatique

J'ai beaucoup apprécié le billet du blog "[Eclat\(e\) d'une jeune avocate](#)" intitulé "[Petit guide de survie à l'expertise construction \(part I\)](#)". J'y ai retrouvé certaines situations que j'ai pu vivre en expertise, ou dont ma femme (avocate) me parle quand elle est elle-même en expertise.

Sans nécessairement écrire le billet croisé dont je n'ai pas le talent, je me suis dit "tiens, ça, c'est une bonne idée de billet". Voici le résultat.

Sachez à titre liminaire que toutes les situations ci-après exposées reposent sur des faits réels que j'ai vécus ©.

Une expertise judiciaire, du point de vue de l'expert judiciaire, ça commence par la lecture des missions envoyées par le magistrat. Ces missions sont souvent écrites à l'origine par l'avocat d'une des parties, en général celle qui demande l'expertise. L'avocat ayant lui-même retranscrit ce que son client lui a demandé, ledit client ayant essayé de traduire ce que son service informatique lui a remonté comme problème. Ceux qui connaissent le jeu du "[téléphone arabe](#)" peuvent imaginer facilement le résultat final. Prévoir donc un coup de fil au magistrat, à l'avocat, au client et au responsable informatique pour avoir une explication de texte avant d'accepter les missions demandées.

Puis vient le moment palpitant consistant à faire coïncider les agendas pour organiser la première réunion. L'usage veut que l'expert appelle en premier les avocats, puis les parties. Dans la pratique, il est conseillé d'appeler en premier le chef d'entreprise du lieu où se trouve le matériel à expertiser, afin de savoir s'il existe une salle de réunion assez grande pour loger tout le monde, et si l'entreprise n'est pas en plein inventaire, ou en congés (ou en liquidation !), à la date retenue par les avocats. Ensuite, muni de trente créneaux pour les six mois à venir, vous pouvez commencer à contacter les avocats... pardon, les secrétariats des cabinets d'avocat. Prévoir de vous munir du numéro de référence du dossier donné par le cabinet d'avocat appelé, du numéro de référence

du dossier donné par le greffe du tribunal, du nom de l'entreprise, etc. Commencer toujours sa première phrase par "Bonjour, je suis M. Zythom, expert judiciaire (à prononcer distinctement), je souhaite parler à Maître Bâ, pour organiser une première réunion d'expertise, dans le dossier "Entreprise GrosClient", le tout avec une voix caverneuse et assurée, pour franchir le barrage du secrétariat.

Une fois des dates communes trouvées entre les agendas des avocats et le vôtre, entamer la ronde des agendas des parties. Au passage, s'assurer que l'avocat contacté est toujours mandaté par le client, et en profiter pour relever les prénom et nom du gérant de l'entreprise. Prévoir un deuxième tour avec les avocats si aucune date ne s'avère satisfaire tout le monde. Ne me parlez pas de [doodle](#), personne ne semble connaître son existence dans cet univers parallèle au mien.

Prévoir un coup de fil au greffe du tribunal pour lui indiquer que la date fixée pour le dépôt du rapport pose un léger problème, étant entendu que l'échéance de six mois initialement inscrite dans les missions, correspond en fait à la date arrachée pour la première réunion. Obtenir une prolongation de mission.

Adresser un courrier recommandé avec avis de réception aux parties et à leurs avocats pour leur indiquer les date, heure et lieu de réunion. Fournir les coordonnées GPS aux avocats parisiens, et vérifier que l'heure de début de réunion est compatible avec les différents trains des parties concernées, ou les distances en voiture fournies par Google maps ou Mappy (ajouter 30mn pour les horaires indiqués par iPhone Plans...)

Ne pas oublier de demander aux parties de fournir **une copie** des pièces du dossier afin de pouvoir s'assurer que le déchiffrement des missions est compatible avec les pièces. Interdire l'envoi par fax, certains secrétariats n'hésitant pas à vous refaxer les 90 pages déjà envoyées sous prétexte qu'une page n'est pas passée. Demander un numérotage des pages. Remettre toutes les pièces en ordre, certains secrétariat ayant eu du mal avec l'agrafeuse, voire avec le recto/verso du photocopieur qui vient de changer.

Chaque partie vous enverra toutes ses pièces, identifiée avec un numéro différent. Il vous faudra tout classer selon votre choix, et apposer votre propre numérotation, avec bordereau récapitulatif reprenant tous les numéros utilisés par les parties.

Certains cabinets facétieux vous enverront leur dossier **en original**. Prévoir la demande de récupération en début de réunion. Faire des copies à vos frais...

Quand la date fatidique s'approche, ne pas hésiter à envoyer un petit email aux parties pour leur rappeler l'échéance imminente. Ne pas répondre aux supplices de déplacement de la date, même celles assorties des menaces les plus explicites du genre "si vous ne déplacez pas cette réunion, je demande votre récusation" (!), ou "je ne pourrai pas être présent car j'ai un dossier "TresGros-Client". Tenir bon. Repenser à l'énergie qu'il a fallu pour coordonner les agendas. Penser au ton froid du greffe quand vous avez demandé une prolongation de date de dépôt du rapport.

Le jour de la réunion, il faut arriver en avance pour repérer les lieux. Rien n'est plus ridicule qu'un expert perdu dans la campagne en train de chercher le lieu de la réunion qu'il a organisée. Arriver la veille est une option. Arriver deux jours avant est un manque de confiance en son GPS.

Venir habillé "en dimanche" est un signe de compétence. Il faut éviter les T-Shirts geeks, les baskets ou les chemises hawaïennes. Un expert judiciaire en informatique est avant tout un expert judiciaire, un sachant, un savant, une personne comprise de ses seuls semblables. L'habit fait le moine, il faut assortir la cravate, la veste, la chemise, le pantalon, les chaussettes et les chaussures. Ne pas hésiter à demander conseil à son épouse. Ne pas tenir compte des remarques étonnées des enfants qui prennent leur petit déjeuner. Une avocate m'a fait remarquer une fois, sur un ton dubitatif, que j'étais en chemisette. Il faut savoir que dans certains milieux autorisés, les chemisettes sont combattues et leurs porteurs exposés [sur l'escalier des gémonies](#).

Entrer le premier dans la salle de réunion et choisir soigneusement sa place, souvent repérable par l'unique fauteuil en cuir présent dans la salle. Ne pas tenir compte du soulèvement de sourcil du PDG de l'entreprise quand il entrera dans la salle de réunion, légèrement en retard.

Refuser tout café/croissant/~~petit pain au chocolat~~ qui pourrait vous être proposés, en précisant bien "je ne peux pas accepter de collation qui ne soit pas proposée en présence des tous les participants, et en leur absence, du fait de l'obligation du contradictoire". La double négation et le sens obscur de la phrase assoit votre prestige auprès de la secrétaire qui vous accueille.

L'heure de la réunion étant arrivé, ne pas céder aux appels désespérés de l'avocat(e) perdu(e) dans la campagne et qui voudrait que vous veniez la chercher dans un village homonyme mais situé à 300 km du lieu de réunion. Commencer la réunion à l'heure pile, chaque région ayant son soi-disant quart d'heure qui ne sert qu'à justifier l'impossibilité chronique de certains à arriver à l'heure.

Expliquer le rôle de l'expert judiciaire. Rappeler qu'il n'est pas expert en droit, afin de valoriser aux yeux de leurs clients les avocats présents. Lire les missions à voix haute, ce qui permet aux experts en droit de se rappeler le dossier, lu en diagonal dans le train.

Enfin, le cœur du problème technique peut être abordé. C'est le moment où les clients, chauffés à blanc depuis tant de mois (d'années ?), se jettent des SCUD et sortent des tranchées... D'où l'importance de la présence des avocats qui jouent un rôle actif pour ~~jeter de l'huile sur le feu traduire~~ modérer les propos de leurs clients.

Au bout de deux ou trois heures de réunion, tout le monde se calme petit à petit et les sachants peuvent commencer à s'exprimer. C'est alors le début du règne des informaticiens, le temps des sigles et des remarques rigolotes des avocats : "heu, Monsieur l'ex-

pert, ERP c'est bien Établissement Recevant du Public, éclairez moi ?"

Le repas est pour moi un moment solitaire. Il se limite à un paquet de biscuits avalé rapidement pendant que je classe mes notes, numérote les pièces étudiées, et commence à rédiger les premières réponses aux questions du magistrat.

L'après-midi est consacré à la somnolence des avocats et des PDG présents. Les informaticiens se complaisent dans des discussions précises sur les concepts qui leur sont chers. Parfois, un avocat appuie les dires de son client avec une intervention brève et prudente. Un bon expert sait laisser de la place à chacun pour que tout le monde "fasse le job".

Après une phase d'écoute active, vient ensuite le temps des premières prises de position. Il faut donner un avis. L'expert prend position. La tension remonte.

En fin de réunion, prendre date immédiatement, en présence de toutes les parties, pour une prochaine réunion. Non seulement cela économise tous les courriers RAR, mais aussi tout le temps perdu à contacter tout le monde plusieurs fois... Gare à ceux qui sont partis en avance.

Une fois la réunion terminée, féliciter tout le monde pour la bonne tenue de la réunion, même si les SCUD volaient bas et en nombre.

Dès le soir, relire ses notes et les mettre au propre, écouter son dictaphone, noter les phrases clefs, les moments forts, les remarques pertinentes.

Dès le lendemain, commencer son pré-rapport. Ecrire aux avocats pour donner une date limite de réception des pièces complémentaires demandées en réunion.

Recharger l'encre du fax.

Préparer la réunion suivante.

Donner une date limite pour les dire.

Recevoir des dire volumineux le jour d'expiration du délai.

Modifier en profondeur son rapport pour prendre en compte les dire.

Recevoir des dire tardifs hors délai.

Pleurer.

Recevoir des dire après le dépôt du rapport auprès du greffe.

Pleurer.

Recevoir un courrier incendiaire parce qu'on n'a pas pris en compte les dire hors délai.

Pleurer.

Assister à l'audience où son rapport est discuté par les parties.

Pleurer chaudement.

Recevoir un compliment du magistrat qui trouve votre rapport clair et complet.

Être en joie.

Recevoir sa note de frais et honoraire.

Payer avec : la facture de l'encre du fax, le remboursement des traites de la Ferrari, le dernier Call of Duty...

Et le soir, au coin du feu, discuter avec ma femme du sens caché du dernier texte modifiant le déroulement de la procédure expertale : ♥

PSES 2014

Chaque année depuis maintenant 5 ans, Pas Sage en Seine (PSES) propose un cycle de conférences, de talks, de rencontres, avec des bidouilleurs, des "gens du réseau", des artistes, des hacktivistes, des entrepreneurs, des journalistes, des curieux...

Depuis ma lointaine province, j'entendais parler de cette manifestation, sans pour autant avoir pu m'y rendre. Cette année, l'un des organisateurs, Skhaen, m'a contacté pour m'inviter à faire une présentation de mon activité d'expert judiciaire, avec comme sujet "Vous n'avez vraiment rien à cacher ?".

J'ai eu plaisir à venir et à rencontrer un tas de gens sympathiques et curieux qui ont suivi ma présentation avec bienveillance. Pour ceux qui n'ont pas pu venir à Numa y assister, les organisateurs l'ont mis en ligne.

Mon seul regret : ne pas avoir pu assister aux 4 jours de conférences...Surtout qu'il y avait du beau monde : Manhack, Stéphane Bortzmeyer, Kitetoa, Maître Eolas, et bien d'autres !

Encore bravo aux organisateurs pour le travail fourni et les résultats obtenus.

Merci à Skhaen pour l'invitation et l'accueil.

A quand une casquette PSES ?

;-)

Récupération de données

J'ai déjà fait part ici même plusieurs fois des techniques que j'utilise pour récupérer des données dans le cadre de mes expertises judiciaires.

Je vous propose aujourd'hui une méthode assez simple qui m'a permis de récupérer tout un ensemble d'images, de films et de musiques d'un ami bien en peine de voir son disque dur tomber en panne. Lisez bien l'ensemble du billet avant de commencer, entraînez-vous sur un vieux disque, essayez de comprendre les différents paramètres de chaque commande pour les adapter à votre cas. Je ne suis pas responsable des problèmes que vous allez générer... (mais je compatis ;-)

Conditions :

Vous êtes rendu destinataire d'un disque dur illisible, mais qui semble fonctionner correctement : vous pouvez le brancher sur un ordinateur, vous l'entendez démarrer sans bruit suspect, sans odeur particulière, mais le système d'exploitation ne le voit pas, ne le détecte pas ou ne retrouve aucune donnée.

Matériels :

J'utilise deux ordinateurs. Le premier sera celui dans lequel sera placé le disque dur illisible. Vous devez être capable de le faire démarrer sur CD, DVD ou clef USB. Le deuxième ordinateur est sous Windows et dispose de suffisamment d'espace disque pour pouvoir stocker une image du disque que vous allez récupérer. Les deux ordinateurs sont branchés sur le même réseau.

Logiciels :

- le [distribution DEFT](#) que vous placerez sur CD, DVD ou clef USB

- le [logiciel PhotoRec](#) que vous téléchargerez en choisissant la bonne version de Windows (32 ou 64 bits).

- un répertoire appelé "partage" sur l'ordinateur Windows et configuré de manière à être accessible en écriture avec le compte windows "zythom"

Procédure :

- Placez le disque dur illisible dans le premier ordinateur

- Bootez le sur la distribution DEFT

- Puis tapez les commandes :

```
#mkdir /root/tempo
```

(création d'un répertoire provisoire en mémoire vive dans /root)

```
#mount -t cifs -o username=zythom /root/tempo  
192.168.0.1/partage
```

où 192.168.0.1 est l'adresse IP de l'ordinateur Windows.

- Tapez ensuite la commande :

```
#dd_rescue /dev/sda /root/tempo/image.dd
```

où "/dev/sda" doit être le device correspondant à votre disque dur illisible (à adapter selon votre configuration).

- Patientez quelques minutes ou quelques heures (ou quelques jours), en fonction de la taille de votre disque dur.

- Quand la commande est terminée, vous pouvez éteindre l'ordinateur n°1. Vous devez disposer d'une image bit à bit du disque dur illisible sur votre ordinateur n°2, celui sous Windows, dans le répertoire "partage", sous le nom "image.dd". Cette image peut être exploitée par différents logiciels pour y récupérer les données, en particulier photorec.

- Sur l'ordinateur n°2, dans une fenêtre de lignes de commandes, tapez la commande : photorec image.dd
- Suivez les indications du logiciel PhotoRec et laissez-le extraire toutes les données qu'il reconnaît.
- Envoyez ensuite vos dons au créateur du logiciel, par exemple en regardant les dates et origines [de vos pièces de la zone euro](#) ;-)

Si ma technique ne fonctionne pas, parlez-en avec un informaticien et ne vous découragez pas : il y a plein d'autres méthodes permettant de récupérer les données. Seul conseil valable dans tous les cas : n'utilisez plus le disque dur, vous risquez d'effacer définitivement les données que vous essayez de récupérer.

Bon courage.

Questionnaire de Proust

L'histoire du questionnaire de Proust est à lire ici :

https://fr.wikipedia.org/wiki/Questionnaire_de_Proust

Je me suis essayé à l'exercice (pas si facile), en voici le résultat :

Ma vertu préférée : la Science ([vertu spéculative](#)).

La qualité que je préfère chez un homme : la compétence.

La qualité que je préfère chez une femme : [la compétence](#).

Ce que j'apprécie le plus chez mes amis : qu'ils s'intéressent à moi.

Mon principal défaut : l'égoïsme.

Mon occupation préférée : apprendre.

Mon rêve de bonheur : explorer les gouffres de la planète Mars.

Quel serait mon plus grand malheur ? : la mort de mes proches.

Ce que je voudrais être : l'inventeur de l'intelligence artificielle.

Le pays où je désirerais vivre : [Cocagne](#).

La couleur que je préfère : 470 nm.

La fleur que j'aime : la fleur du [Persea americana](#).

L'oiseau que je préfère : Deepo, la mouette à béton de [John Diefool](#).

Mes auteurs favoris en prose : [Frank Herbert](#), [Isaac Asimov](#), [Arthur Charles Clarke](#), [Alfred Elton van Vogt](#).

Mes poètes préférés : [Stéphane Mallarmé](#), en particulier [ce sonnet](#) aux rimes en x-or.

Mes héros dans la fiction : [Muad'Dib](#), [Elijah Baley](#), [Gosseyn](#).

Mes héroïnes favorites dans la fiction : [Susan Calvin](#), [Ellen Ripley](#), [Leeloo](#).

Mes compositeurs préférés : [Mozart](#), [John Williams](#).

Mes peintres favoris : [Banksy](#), [Boulet](#).

Mes héros dans la vie réelle : [M. et Mme Michu](#).

Mes héroïnes dans l'histoire : [Hypatie d'Alexandrie](#), [Augusta Ada King-Byron](#).

Mes noms favoris : Zythom (mais j'ai d'autres pseudonymes ;-)

Ce que je déteste par-dessus tout : mon [côté obscur](#).

Personnages historiques que je méprise le plus : j'essaye de ne mépriser personne.

Le fait militaire que j'admire le plus : la [bataille de Camerone](#).

La réforme que j'estime le plus : la [réforme clithénienne](#).

Le don de la nature que je voudrais avoir : la fermeté de ma jeunesse.

Comment j'aimerais mourir : rapidement.

État d'esprit actuel : concentré.

Fautes qui m'inspirent le plus d'indulgence : les fautes de goût.

Ma devise : [Nunc est bibendum](#).

Evolution professionnelle

A l'approche des 50 ans, l'année dernière, j'ai décidé de vérifier mon employabilité. Selon l'Organisation internationale du travail (et [Wikipédia](#)), l'employabilité est "*l'aptitude de chacun à trouver et conserver un emploi, à progresser au travail et à s'adapter au changement tout au long de la vie professionnelle*". Pour moi, cela consistait à vérifier, bien qu'aimant mon entreprise, mon chef, mes collègues, mes étudiants et mon travail, si je pouvais trouver une entreprise qui voudrait m'aider à développer mes aptitudes dans l'univers de [l'inforsique](#).

J'ai donc pris mon courage à deux mains, mis à jour mon CV et j'ai cherché sur le marché du travail l'entreprise idéale et le poste associé. J'ai cherché du côté clair de la Force (les petites annonces du marché ouvert de l'emploi, les candidatures spontanées) mais aussi de son côté obscur (le réseau, les amis, les relations, ~~la NSA~~, tout pour accéder au marché caché de l'emploi).

Pour ne rien regretter, j'ai ciblé large : mobilité sur toute la France y compris Paris, aucune prétention salariale a priori, pas de préférence grosse entreprise ou PME ou TPE, privé, public, CDI ou CDD, prêt à démarrer comme un débutant, comme un senior, comme un expert. J'ai des compétences d'encadrement, je sais travailler en équipe, je respecte les règles établies. Bref, le salarié (presque) idéal.

J'ai donc appliqué les règles de recherche d'emploi que je préconise auprès de mes étudiants ([lire ce billet où je les explique](#) : « Recrutement des jeunes », tome 4).

Le blog m'a bien aidé, Twitter également (un retweet de Maître Eolas, c'est 3000 personnes qui viennent sur le blog !) et j'ai pu ainsi décrocher plusieurs entretiens d'embauche. Certains se sont bien passés, [d'autres moins bien](#).

Tout bourgeois veut bâtir comme les grands seigneurs,

Tout prince a des ambassadeurs,

Tout marquis veut avoir des pages.

Et il m'est arrivé ce que je pensais dès le départ : aucune proposition n'a abouti.

Il y a plusieurs explications à cela :

- je suis nul
- j'ai plus de 45 ans
- je ne sais pas me vendre
- mes compétences n'intéressent personne
- la crise
- je n'ai pas de réseau
- je suis nul
- c'est la faute à internet
- les entreprises n'ont pas su voir mon énorme potentiel
- mes enfants ont tout fait pour ne pas déménager
- je suis nul.

Ok, donc, comme [Rocky Balboa](#), je vais devoir m'entraîner dans un coin tout seul pour affûter mes muscles et JE REVIENDRAI (heu, non, ça c'est [Arnold](#)). C'est d'ailleurs ce que m'a conseillé sérieusement le responsable de mon entretien à l'ANSSI : "vous devriez vous entraîner sur l'analyse de systèmes live et revenir dans deux ans".

Putain DEUX ans !

Je n'intégrerai donc pas les équipes de cette agence gouvernementale, et je le regrette. J'aurais aimé travailler avec des jeunes et brillants ingénieurs sur des sujets très techniques toujours en pointe. J'aurais aimé pouvoir relever ce challenge. Mais, comme pour mes tentatives de voyages dans l'espace (lire cette série de billets : <http://zythom.blogspot.fr/search/label/Mars>, surtout [celui-ci](#) : « Espace, frontière de l'infini », tome 2), il faut savoir se faire une raison : j'ai une capacité à changer d'emploi nulle.

Maintenant, positivons :

- j'ai un boulot
- j'aime mon boulot
- mon entreprise est performante sur un marché porteur
- mon entreprise apprécie mon travail
- j'ai un travail dynamique, prenant et passionnant
- j'ai des perspectives de progrès et d'amélioration
- j'habite un coin de paradis
- j'ai une bonne santé
- j'ai une famille formidable
- le chiffrement RSA [n'a pas encore été cracké.](#)

Un lecteur avisé pourrait objecter : "mais pourquoi diable avez-vous eu envie de chercher un autre emploi ?" Ma réponse est imparable : "parce que".

Parce que je voulais voir ce que je valais encore sur le marché du travail.

Parce que je suis effrayé à l'idée d'avoir passé 20 ans dans la même entreprise.

Parce que je suis effrayé à l'idée de passer les 15 prochaines années dans la même entreprise.

Un lecteur avisé pourrait objecter : "qu'importe le flacon pourvu qu'on ait l'ivresse". Certes. C'est d'ailleurs ce que je me dis aussi. Bien obligé.

Alors j'ai pris une décision :

Puisque j'aime mon entreprise, plutôt que de changer d'environnement, je vais essayer d'améliorer mes compétences dans toutes les activités que je mène actuellement, et sortir de ma zone de confort. Professionnellement, il faut que j'améliore mes compétences de manager et que je favorise la progression de mes collaborateurs. Côté expertises, il faut que je développe mon activité d'ex-

pertises privées et [que j'apprenne à me vendre](#). Côté vie publique, il faut que j'essaye de m'impliquer plus encore dans la vie de la commune.

Selon le Ministère français chargé de l'emploi (et toujours [Wikipédia](#)), l'employabilité est "*la capacité d'évoluer de façon autonome à l'intérieur du marché du travail, de façon à réaliser, de manière durable, par l'emploi, le potentiel qu'on a en soi*".

Conclusions :

De ses échecs, il faut savoir apprendre. Et se relever.

Et ne pas attendre qu'on vienne vous offrir le poste idéal.

Il faut le créer soi-même.

Et savourer sa chance d'avoir un métier qu'on aime.

C'est dans les vieux pots qu'on fait la meilleure soupe.

Putain 15 ans !

Pépites du passé

La ligne de téléphone n'est pas utilisée, la maison est calme, je peux tenter une connexion à internet. Je suis déjà détenteur d'une adresse email professionnelle, de par mon métier d'enseignant-chercheur, mais j'ai également une adresse email *personnelle*. Nous sommes à la fin des années 1990.

Je ne suis pas encore fixé sur mon fournisseur d'accès à internet : il faut dire que le choix est pléthorique, entre [LibertySurf](#), [Free-Surf](#), [Free](#) et les autres. Je surveille de près ma consommation téléphonique pour éviter son explosion : en effet, les unités téléphoniques sont à ajouter au coût d'accès à internet. Heureusement, mon [Minitel](#) trône fièrement à côté du téléphone dans la salle à manger, et ses services payants m'ont déjà habitué à l'usage du chronomètre.

En ce moment, je teste [Oreka](#) qui m'offre 18 heures d'accès à internet gratuitement, communications incluses. Je me suis vite habitué à la bannière publicitaire que mon cerveau n'interprète même plus.

Je suis l'heureux propriétaire d'un [USRobotics Sportster Fax Modem 14,4k](#) flambant neuf qui trône à côté de mon ordinateur, dans un fouillis de câbles que l'on ne voit jamais sur les publicités informatiques.

A chaque fois que je l'allume, je pense aux ouvrages d'un de mes auteurs de Science-Fiction favori : [Isaac Asimov](#) et son entreprise [US Robots, inc.](#) J'aime sa séquence sonore de connexion, difficile à décrire, mais parfaitement reconnaissable à l'oreille. Je connais la signification de chaque voyant que je regarde clignoter en attendant avec impatience l'établissement de la connexion.

Je relève les emails de ma boîte [Mygale.org](#) ainsi que ceux de ma femme. Grâce à son informaticien de mari, elle a été la première avocate de son barreau à disposer d'une boîte email, ce qui lui a

valu un article clin d'œil intitulé "la femme araignée" dans le journal des jeunes avocats. J'espère qu'elle l'a gardé...

Je m'occupe des différents sites perso que je fais vivre chez différents hébergeurs : sur Mygale.org bien sûr, mais aussi sur [Chez.com](#) et [GeoCities](#). Il faut dire que l'édition des pages HTML est maintenant grandement facilitée par la suite logiciel [Netscape Communicator](#). Je suis un virtuose de la mise en page et du mélange *multimédia* : des images gif animées avec du son et du texte...

Je repense aujourd'hui à tout cela parce qu'en rangeant l'IM-MENSE bazar qu'est mon bureau, je suis tombé sur mon vieux modem USB. Un jour, quand j'arriverai à la couche géologique contenant les données de mes vieux sites perso psychédéliques, je ferai pleurer vos yeux. En attendant, je pose sur ce blog un billet de souvenirs pour me rappeler de ces pépites qui ont illuminées ce pas-si-lointain passé. Ne croyez pas pour autant ceux qui pensent que c'était mieux avant. [L'âge d'or de l'informatique est devant nous](#) (cf. « L'âge d'or est devant nous... », tome 1).

*Sed fugit interea [tempus fugit](#) irreparabile,
dum singula amore capti circumvectamur*

(Mais en attendant, il fuit : le temps fuit sans retour, tandis que nous errons, prisonniers de notre amour du détail.)

Septieme ciel

Je regarde par la fenêtre de l'avion et la tension monte...

Je n'ai à mon compteur que six sauts, mais le prochain, le septième, est le premier que je vais faire entièrement seul... Je suis monté dans l'avion avec une certaine appréhension, les autres camarades de stage qui m'accompagnent effectuant leur sixième saut sont eux accompagnés de leur moniteur.

Dans l'avion, chacun est silencieux, concentré sur les figures imposées comme exercice pour son saut. Les moniteurs se font des signes entre eux, amusés par notre enthousiasme et notre inexpérience. Chaque stagiaire est dans sa bulle. La mienne grossit, grossit à mesure que l'avion prend de la hauteur. Le stress monte également, ce qui me surprend car les autres sauts ne m'avaient pas fait peur. Mais cette fois, je suis seul, sans moniteur pour me demander si tout va bien, pour me faire vérifier mon équipement encore une fois dans l'avion, pour me déstresser par un geste ou un sourire moqueur.

Je vérifie mon équipement : la poignée permettant de sortir l'extracteur de la voile est bien en place, les deux poignées de la terrible procédure de sécurité sont bien là (largage de la voile principale et ouverture de la voile de secours), les sangles sont bien mises...

[Note : le mot "parachute" désigne l'ensemble complet : sac + voile principale + voile de secours + sangles, poignées et dispositifs divers]

Je regarde l'aiguille de l'altimètre tourner lentement : 2500m, 3000m, 3500m, 4000m... Quand elle indique 4200m, le pilote secoue une grosse clochette et l'un des moniteurs ouvre la porte. Le vacarme ambiant augmente d'un cran. Je suis le premier qui doit sauter, je suis assis à même le sol de la cabine exiguë qui peine à loger les 9 parachutistes.

Je me lève tant bien que mal, chacun me laissant une petite place pour me permettre de bouger.

Pendant la montée, j'ai décidé du type de sortie que j'allais faire : un roulé-boulé arrière qui démarre dos au vide. J'ai également repensé à toutes les péripéties qui me sont arrivées tout au long de ces quatre derniers jours, pendant ma formation [PAC](#) :

- Lors du 1er saut, j'attendais je ne sais quel signe pour ouvrir ma voile, la main sur la poignée de l'extracteur... L'un des moniteurs a saisi ma main (et la poignée avec) et tiré dessus pour me faire ouvrir la voile !

- Autant la voile s'était ouverte en douceur pour mon 1er saut, autant elle a "claqué" lors du 2e saut. Je suis secoué comme un pantin désarticulé pendant son ouverture. Je ne m'y attendais pas du tout !

- Pour le 3e saut, le moniteur qui nous guide du sol pendant toute la descente sous voile (chaque élève dispose d'une oreillette radio) s'emmêle dans les couleurs des voiles et je prends pour moi un ordre impératif de faire demi-tour, alors que je ne suis plus qu'à 50m du sol. Me voilà donc vent arrière pour me poser. Trop tard pour changer de direction, je me pose en courant, avec une belle gamelle à la clef et une dizaine de mètres à brouter de l'herbe !

- Les conditions météo ont changé en altitude, et voilà qu'il fait -5°C à 4200m... Je n'avais pas vraiment prévu cela : je n'ai pas de gants, pas de pull. Y fait frette !

- Je n'ai pas réussi l'exercice du 4e saut consistant à rester en chute libre volontairement sur le dos pendant quelques secondes... Je suis tellement cambré que je me retourne immédiatement. A moins que ce ne soit mon (léger) ventre qui décale mon centre de gravité ;-)

- Le roulé-boulé avant [du 5e saut](#) était correct. Mais lorsque j'ai ouvert les bras, je me suis retrouvé sur le dos ! Du coup, je me suis cambré pour me retourner, mais le retournement a été plus brutal que prévu et je me suis désarticulé (voir vidéo).

- Pendant l'exercice consistant à faire un 360° à plat, à droite, puis à gauche, j'ai les deux coudes trop bas. Du coup, je n'arrive pas bien à tourner. Il me faut un peu de temps pour comprendre, mais à 200 km/h, le temps manque. Priorité au contrôle de l'altimètre et à l'ouverture de la voile !

- Lors du 6e saut (et dernier saut accompagné), après le roulé-boulé arrière et les deux séries de tonneaux de l'exercice, une fois stabilisé, j'ai perdu mes surlunettes ! Ce qui veut dire que mes lunettes de vue étaient exposées directement au vent relatif de la chute libre à 200 km/h. Elles sont restées par miracle sur mes yeux. Le moniteur a apprécié que je ne m'en occupe pas plus que ça et que je me concentre sur ma stabilité, mon altimètre et mon ouverture de voile. Néanmoins, juste avant que la voile ne me secoue comme un prunier, j'ai sauvé mes lunettes en mettant les deux mains sur les yeux !

--oOo--

Je suis maintenant seul pour sauter de l'avion. Je tiens la barre à deux mains.

Je me lance un "go" dans la tête, lâche la barre qui me retient à l'avion, lance la tête en arrière, attrape mes deux genoux avec les mains et commence une série de 4 pirouettes arrières dans le vide.

Je me mets sagement à plat et stabilise comme je peux ma position. Je teste quelques mouvements des bras et des jambes et analyse leurs impacts sur ma position.

Je regarde mon altimètre toutes les cinq secondes.

A partir de 2000m, je ne le quitte plus des yeux, en révisant mentalement la procédure de sécurité à faire si la voile ne s'ouvre pas.

A 1700m, je sors l'extracteur et déclenche l'ouverture de la voile.

A 1500m, la voile est correctement déployée, je pousse un cri sauvage de joie et prend les commandes. Les six minutes suivantes sont une formalité : je profite de la vue, je fais quelques 360° sous voile, je me rends tranquillement vers mon point de rendez-vous de 300m, je fais mon approche finale et je me pose en douceur (sur les fesses, c'est ma technique ;-)

Je savoure le plaisir intense que je viens de vivre. Je vous laisse deviner la définition la plus appropriée de l'expression "[septième ciel](#)" qui s'applique à ce que je ressens après ce septième saut.

J'ai [une pensée pour Sid](#) et je le remercie de m'avoir encouragé à faire cette formation.

Puis je range mon parachute et rentre à pied au hangar, avec des étoiles plein les yeux et la musique de "[Top Gun](#)" dans la tête ;-)

Le disque dur

Le disque dur est posé devant moi sur le bureau. Je l'observe quelques instants en silence. Je viens de passer plusieurs heures à l'extraire d'un ordinateur particulièrement résistant au démontage. Je ne voulais pas faire de rayures avec mes tournevis, aussi ai-je du en fabriquer des souples avec de vieilles brosses à dents...

J'ai maintenant devant moi un disque dur tout à fait banal (et un tas de vis que j'ai mis de côté pour le remontage). Je le regarde fixement, faisant une petite pause dans cette expertise judiciaire solitaire. Comme tous les disques durs non SSD, c'est une merveille de mécanique. Pendant son fonctionnement, les têtes de lecture flottent sur un coussin d'air à quelques nanomètres des plateaux, ce qui ne laisse pas de me surprendre.

Le premier défi, qui consiste à essayer de faire démarrer l'ordinateur sur cédérom sans toucher au disque dur, a échoué. Mes différents "boot cd" n'ont pas réussi à reconnaître les différents éléments de l'ordinateur, en particulier la carte réseau. En tout cas, pas suffisamment pour me permettre de cloner le disque dur en un temps "raisonnable", et avec la garantie de ne PAS modifier les données inscrites dessus. Préservation de la preuve, garantie d'une expertise ultérieure donnant les mêmes résultats, responsabilité de l'expert, etc.

Le deuxième défi a donc été de réussir à extraire le disque dur du cocon constitué par cette magnifique carcasse aluminium, mince et fragile, sans vis apparente, clipsée de manière invisible. Difficile défi. Heureusement, internet est une source d'informations telle que j'ai pu trouver un site de passionnés ayant déjà entrepris le démontage de ce modèle ET partageant cette expérience. Avec précaution, j'ai entrepris de suivre leurs conseils, et pas à pas, malgré quelques petites différences liées certainement à une évolution du modèle, j'ai réussi à extraire le disque dur.

Le voilà posé sur mon bureau.

Je le prends en photo, je note le numéro de série et les diverses caractéristiques du disque. Je le prends délicatement entre les doigts pour le brancher sur mon ordinateur d'acquisition.

Je mets ce dernier sous tension. Quelques gouttes de sueurs perlent sur mon front : le moment est critique. Le disque dur fonctionne-t-il ? Les plateaux tournent-ils ? Les têtes de lecture vont-elles accéder correctement aux données stockées sur la couche ferromagnétique ? Y a-t-il un bruit suspect ?

Malgré toute mon expérience, mon cœur bat plus vite.

Apparemment tout va bien. Je lance la copie bit à bit du disque dur. Celle-ci va durer une douzaine d'heure. Je m'assure une nième fois que mon système de stockage est suffisant pour recevoir la copie, qu'aucune coupure programmée n'arrêtera le transfert, que la pièce est assez aérée pour évacuer la chaleur (mon bureau est minuscule). Je pars me coucher, un peu inquiet. Le lendemain, avant de partir travailler, je vérifie que la copie suit son cours, qu'elle avance correctement, que le disque dur ne chauffe pas trop. J'ai hâte d'être à ce soir pour pouvoir enfin éteindre le disque dur original.

Dans un coin de mon bureau trône l'ordinateur éventré, entouré de ses vis et clips soigneusement identifiés. Ma journée de travail est terminée, je peux commencer mon activité d'expert judiciaire. Je m'assure que les hashes de la copie et celui du disque dur d'origine sont cohérents, que ma copie numérique est bien sauvegardée et en sécurité. Je commence le remontage du disque dur dans l'ordinateur.

Puis, enfin, vient le défi principal : la recherche des informations que l'on m'a demandée de faire. Celles-ci sont peut-être cachées quelques parts, dans un fichier ou dans un container chiffré. Celles-ci sont peut-être dans la zone non allouée, dans des fragments d'anciens fichiers. Celles-ci n'existent peut-être pas. Mais ça, je ne le saurais que dans quelques jours ou quelques semaines.

J'aborde avec effroi ce dernier défi...

Expert ou Huissier

Je suis souvent sollicité pour mener à bien des constatations concernant du matériel informatique en tant qu'expert judiciaire. Je suis alors obligé d'expliquer à mon interlocuteur qu'à mon avis il est préférable pour lui de passer par un huissier de justice s'il souhaite que les constatations soient opposables à une partie adverse.

Quelques explications me semblent nécessaires.

Un expert judiciaire est une personne inscrite sur une liste ad hoc d'une cour d'appel ou de la cour de cassation. Cette personne n'est en "mission judiciaire" que lorsqu'elle est sollicitée par un magistrat. Le reste du temps, c'est une personne normale, sans "super pouvoir" particulier.

Il est possible (et relativement fréquent) que cette personne soit contactée par un particulier ou une entreprise parce que son nom apparaît sur la liste de la cour d'appel (ou celle plus prestigieuse de la cour de cassation). Mais dans ce cas, l'intervention se fait à titre personnel, sans mission officielle demandée par un magistrat. On parle alors de mission privée.

Lorsque j'établis un rapport d'expertise privée, celui-ci n'a pas la même valeur que le rapport que je rédige dans une mission d'expertise judiciaire.

Lorsque je rédige un rapport d'expertise judiciaire au pénal, à la demande d'un juge d'instruction par exemple, je travaille seul. Les questions qui me sont posées sont très factuelles : y a-t-il présence de telle ou telle information sur le disque dur de l'ordinateur, l'ordinateur a-t-il été utilisé pour visiter tel ou tel site internet et si oui à quel moment, etc.

Dans tous les autres cas "officiels" (civil, tribunal de commerce, etc.), l'expertise judiciaire doit être menée en présence des parties concernées, d'une manière dite "contradictoire". Les questions qui me sont posées par le magistrat sont exposées aux parties, les ré-

ponses que j'y apporte sont critiquées, débattues ou défendues par les parties présentes. Les questions posées demandent un "avis" de l'expert, par exemple sur l'évaluation des montants financiers des préjudices subis par les désordres informatiques constatés.

Il arrive, et c'est l'objet de ce billet, qu'une partie souhaite préparer son dossier au mieux avant d'aller au procès, ou simplement pour impressionner son adversaire. Elle fait alors appel à un expert judiciaire, parce que le poids de la fonction compte, ainsi que les mots de son titre : "expert" et "judiciaire". Mais le magistrat ne s'y trompe pas : la parole d'une personne missionnée par une partie (pour des missions choisies par elle et directement payée par elle) n'a pas le même poids que celle d'un expert en mission judiciaire, quand bien même il s'agisse de la même personne.

Le rapport rédigé par un expert [n'est pas un acte authentique](#). Dans le code civil français, [un acte authentique](#) est "*celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.*" Ainsi, les notaires, les officiers d'état civil, les huissiers de justice peuvent rédiger des actes authentiques.

Jusqu'en 2010, les constats d'huissier n'avaient que *la valeur de simples renseignements* ([cf. article 1 de la loi en vigueur en 2007](#)), mais [depuis 2010](#), le texte a été corrigé : "*Ils peuvent, commis par justice ou à la requête de particuliers, effectuer des constatations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter. Sauf en matière pénale où elles ont valeur de simples renseignements, ces constatations font foi jusqu'à preuve contraire.*"

C'est pourquoi il me semble préférable de faire faire les constatations techniques par un huissier de justice, plutôt que par un expert judiciaire en mission privée.

Bien sûr, se pose alors la question : les huissiers de justice sont-ils tous compétents en matière informatique ? A l'évidence, comme pour toute profession non informatique, la réponse est non. Mais alors comment faire ?

Il existe des huissiers de justice qui se sont faits une spécialité en matière informatique. Ceux-là sont compétents, dans la mesure de leur compréhension de la technique informatique qu'ils maîtrisent. Pour eux, serveurs mandataires, caches de navigation, serveurs DNS n'ont plus de secrets. Pour autant, qu'en est-il des serveurs mandataires transparents ou des DNS menteurs ? Pour la cour d'appel de Paris, seul [le respect des préconisations jurisprudentielles compte...](#)

Mon conseil, donc :

- si les aspects techniques sont relativement simples (et que vous les maîtrisez suffisamment), faites appel uniquement à un huissier de justice compétent (sur les conseils de votre avocat bien sûr, puisqu'il saura vous trouver un huissier).
- si vous pensez que la complexité technique est élevée, faites appel à un huissier de justice compétent ET un expert judiciaire.

C'est le prix à payer pour mettre toutes les chances de son côté.

AMHA.

La recette

Les litiges entre un prestataire informatique et son client peuvent trouver naissance dans des détails de méthodologie qui prennent toute leur importance quand il faut répartir les responsabilités.

Et souvent, c'est la mission de l'expert judiciaire.

Dans cette affaire, que je romance à titre d'exemple, le contrat est clair : le prestataire s'engage à développer un site web "*avec une gestion rigoureuse et transparente en sept étapes*" :

- *Lancement du projet*
- *Spécifications fonctionnelles et techniques*
- *Conception graphique du site*
- *Prototypage*
- *Réalisation du site*
- *Tests d'intégration et de qualification*
- *Mise en production et lancement du site*

La brochure annexée au contrat de prestation détaille chaque étape, les mérites et le savoir-faire du prestataire.

Le problème ici est que le client n'a pas été satisfait du résultat de son prestataire et refuse de payer le solde de la facture, alors que le site web est en ligne et fonctionnel. Le ton est monté, les courriers en recommandé échangés, puis l'affaire s'est retrouvée devant la justice qui a désigné un expert judiciaire pour tirer les choses au clair...

Et me voilà en charge du dossier.

Il est facile d'imaginer un mauvais client qui, quoiqu'il arrive, ne sera jamais satisfait de la prestation qu'il trouve très chère pour un résultat qui sera toujours insuffisant à ses yeux.

Il est tout aussi facile d'imaginer un prestataire qui vend très cher une prestation basique à un client ignorant des choses techniques, certaines affaires récentes mettent même en avant des sommes considérables englouties dans des développements web où les difficultés techniques sont sans rapport avec les montants facturés...

Cette différence de connaissances entre un prestataire et son client se traduit par des obligations pour le prestataire. Elles sont principalement de deux types : l'obligation de conseil et l'obligation de renseignement.

D'après le « Lamy informatique et réseaux » (en sa version 2010, si quelqu'un veut me sponsoriser pour la version la plus récente, je suis preneur. M. Lamy si vous me lisez...), l'obligation de conseil du professionnel informatique s'inscrit dans une obligation plus large qui est l'obligation d'information. Cette dernière suppose, outre l'obligation de conseil, une obligation de renseignement et une obligation de mise en garde.

Par exemple, certains fournisseurs n'hésitent pas à insérer dans leurs contrats informatiques une clause stipulant que :

« Le client est conscient que le projet informatique qui va être développé entre les parties au sein de son entreprise est complexe et qu'il est susceptible de remettre profondément en cause son organisation et ses méthodes de travail, ainsi que la qualification du personnel et suppose une collaboration étroite entre les parties, un dialogue permanent dans un esprit de confiance et de respect mutuel. »

Le prestataire doit donc, pour se dégager de toute responsabilité, attirer l'attention du client sur les contraintes d'utilisation du système, les exigences de l'environnement du système et de toutes les difficultés éventuelles auxquelles le client pourra faire face durant les phases de démarrage et d'utilisation du système.

Le devoir de conseil est renforcé lorsque le client est profane ou peu expérimenté, ainsi que le rappelait déjà la Cour d'Appel de Paris en 1983 : *« (...) ce devoir étant d'autant plus rigoureux que les clients sont mal informés en la matière ».*

C'est particulièrement flagrant lors du déroulement de la procédure de recette.

Lors des débats, le prestataire a affirmé que « *la mise en ligne du site vaut quasiment (sic) pour acceptation de la recette, puisque le site devient dès lors visible au public* », puis ensuite que « *le site est en ligne et fonctionne, il est donc officieusement (sic) en phase de maintenance* »

Je ne suis pas de cet avis, car s'il est en effet courant de mettre un site internet en ligne alors qu'il est toujours en phase de développement, pour la simple raison qu'il faut faire des tests "grandeurs natures", l'usage est de mettre les codes sources du site sur un serveur dit "de pré-production", avec une adresse web provisoire, commençant par exemple par www4, et paramétré pour ne pas être indexé automatiquement par les moteurs de recherche, pour éviter qu'il ne soit utilisé par les internautes. Le site est donc en ligne pour subir des tests en condition réelle de fonctionnement, avec comme objectif de faire valider le travail par le client. Le fait qu'il soit en ligne et qu'il "fonctionne", ne signifie pas non plus qu'il est en phase de maintenance. Il manque la recette par le client.

L'obligation de réception qui pèse sur le client est la contrepartie de l'obligation de délivrance qui pèse sur le prestataire informatique. Cette obligation de réception existe dans tous les contrats informatiques, qu'ils aient pour objet la vente ou le louage d'un matériel, d'un système informatique, la fourniture d'un logiciel ou d'une prestation informatique. Elle est importante notamment du fait que son exécution conditionne généralement ensuite le paiement du prix (CA Paris, 13 mai 1981, Sté ICL c/ Sté provencale de surveillance, Juris-Data, n°22752), qui est une des obligations majeures du client.

Pour satisfaire à son obligation de réception, le client met généralement en œuvre une procédure convenue à l'avance avec son co-contractant que l'on dénomme « procédure de recette ». Les mo-

alités de sa mise en œuvre par le client varie cependant suivant les contrats et la nature des livrables.

Lorsqu'il s'agit d'effectuer la recette d'un matériel informatique, le client doit généralement établir un procès-verbal de réception qui atteste que le matériel livré paraît conforme à ce qui avait été commandé. Les choses deviennent plus complexes lorsqu'il s'agit pour le client de prononcer la recette d'un logiciel spécifique. Il est alors usuellement pratiqué un processus de recette en deux étapes successives : une recette provisoire, suivie d'une recette définitive.

La recette provisoire correspond à la phase initiale de vérification du livrable à satisfaire aux spécifications du contrat (la recette provisoire d'un site web est en général effectuée en ligne sur le serveur de pré-production), tandis que la recette définitive, qui intervient ultérieurement, permet de vérifier le bon fonctionnement du logiciel ou du système en service régulier (c'est-à-dire, comme dans la terminologie des marchés publics, dans des conditions proches de l'activité opérationnelle, et, en l'espèce, en ligne, sur le site définitif de production).

Toute difficulté considérée par le client comme affectant l'aptitude du logiciel ou du système doit faire l'objet d'une réserve accompagnée de fiches d'anomalies remises au prestataire (voir not. Bitan H., *Contrats informatiques*, Litec, 2002, n°21). Si les anomalies constatées sont particulièrement bloquantes (c'est-à-dire qu'elles empêchent toute mise en œuvre suffisante du logiciel ou du système durant la phase de recette définitive), le client peut aussi surseoir à prononcer la recette provisoire tant que ces anomalies ne sont pas corrigées.

On voit donc bien que la simple mise en ligne d'un site web et son accès (supposé) au public, ne peuvent pas suffire à justifier l'acceptation de la recette du site (et encore moins tacitement).

Il importe donc que le prononcé de cette recette soit mûrement réfléchi. En cas de difficultés techniques particulières ou d'un niveau d'anomalie trop important, il est prudent pour le client de

refuser de prononcer la recette définitive et de réclamer une nouvelle période de tests de validité, voire de réclamer après deux recettes manquées, la réécriture de tout ou partie de l'application, sous peine de demander la résiliation du contrat aux torts du fournisseur.

Je vois trop souvent des dossiers où le client fait une confiance aveugle à son prestataire en refusant de réfléchir sur les aspects pourtant basiques relevant d'une [gestion de projet](#) informatique. Certes le prestataire est un sachant technique, mais le client doit prendre sa part dans la gestion de projet, et une bonne procédure de recette en fait partie. Ce que ne peut ignorer le prestataire.

Pour des raisons évidentes de confidentialité, je ne peux pas vous dire quelle était, à mes yeux, la répartition des responsabilités dans ce dossier, mais j'espère vous avoir fait réfléchir sur l'importance de la gestion de projet (des deux côtés de la barrière), sur la procédure de recette en particulier, et enfin sur le rôle d'un expert judiciaire en informatique.

Quot homines, tot sententiae

Autant d'hommes, autant d'opinions

Térence, Le Phormion, v. 454

Yéléna

Encore une expertise où je regarde, encore et encore, des photos de petites filles violées. Je les trie par thème de torture, par catégorie d'âge supposé, par poses pornographiques.

Et il y a cette petite fille qui revient souvent. Je l'ai appelé Yéléna.

Le décor est sordide : des pièces sombres à l'ameublement minimaliste, avec des papiers peints d'un autre temps. Les fenêtres sont sales, le matelas du lit est bosselé, les meubles abîmés. Parfois sur les photos, j'aperçois un texte en alphabet cyrillique qui me fait imaginer que tu es peut-être russe, ou bulgare, ou serbe, enfin slave quoi. D'où le prénom que je t'ai donné, Yéléna.

Depuis le temps que je trie ce type de photos, d'une expertise judiciaire à une autre, je t'ai croisée plusieurs fois, toi et ton regard triste au sourire forcé. Dans le meilleur des cas, tu es en mini bikini moulant, prenant des poses de strip clubs. Dans les pires, tu manipules des sexes d'hommes bien trop grands pour ton corps.

Et ces photos tournent, tournent, reviennent et repartent, d'un serveur à un autre, détournant cette magnifique liberté d'échange offerte par internet. Et plutôt que de lutter plus efficacement contre les tortionnaires, les politiciens prennent le prétexte de la présence de tes photos pour restreindre les libertés de tous au profit d'un petit nombre, avec des lois scélérates.

Mais de tout cela, tu n'en as cure, et je le comprends.

Le flicage d'internet, c'est en ton nom, mais ce n'est pas pour toi.

Mon rôle se limite à découvrir la trace de la présence de tes photos et films sur le disque dur d'un internaute, qui sera ensuite probablement condamné pour possession d'images pédopornographiques. Je sais aussi que des policiers traquent les pédophiles, les réseaux assouvissant leurs penchants, ceux qui prennent les pho-

tos, ceux qui vendent les corps de fillettes de ton âge. Avec un certain succès. Le droit à l'oubli, ce n'est pas pour toi.

Lors de mes premières missions en recherche d'images pédopornographiques, j'étais un jeune papa découvrant les joies et l'amour de ses enfants. La vision de ces photos et de ces films me touchait profondément. J'ai souvent raconté sur ce blog ces moments douloureux, parce que pour moi, c'était une façon d'évacuer toute l'horreur que je ressentais.

J'ai souvent pleuré en silence devant mon écran.

Je serrais plus fort mes enfants le soir en les couchant, et je ne pouvais pas m'empêcher de penser à toi, de temps en temps. Qu'es-tu devenue ? Quel âge as-tu maintenant ? As-tu survécu à cette enfance infernale ?

Bien sûr, je ne le saurai jamais.

Je continue à apporter mon aide aux enquêteurs, je fais ma petite part du labeur, avec un constat qui me fait peur : aujourd'hui, quand je regarde tes photos, Yéléna, je ne ressens plus rien. Je ne pleure plus devant mon écran. Je me suis endurci, insensibilisé. Je les trie par thème de torture, par catégorie d'âge supposé, par poses pornographiques.

Et il y a cette petite fille qui revient souvent. Je t'ai appelé Yéléna.

Cela signifie, en russe, "éclat du soleil".

Mélanges

J'ai plusieurs activités que je mène en parallèle : ma vie professionnelle de responsable informatique et technique, une activité d'expert judiciaire, un mandat de conseiller municipal (délégué au développement numérique de la commune), des missions de conseils auprès des avocats, une vie familiale, une identité numérique et une vie personnelle (et sportive)...

Tous ces univers sont relativement étanches et indépendants.

J'ai des collègues de travail dont je suis relativement proches, j'ai de très bonnes relations avec des confrères experts judiciaires, je m'entends très bien avec mes colistiers de la commune (même avec certains de l'opposition, c'est dire ma bonne composition), j'ai une vie familiale riche et grisante, des copains...

Mais je ne suis pas quelqu'un de très bavard (sauf quand on me lance sur mes marottes ;-)) et en dehors de ma proche famille, je n'ai pas d'ami, [au sens que Montaigne donnait à ce terme](#) (Par "ami", j'entends "quelqu'un qui peut traverser la France en cas de coup dur", pas un lien Facebook)

Finalement, je me sens assez seul, et ce blog me permet de tromper ce sentiment par l'écriture, en parlant de moi (oui, je sais, ce blog perso est [TRES égocentré](#)).

Pourtant, je peine à expliquer à la plupart des personnes que je rencontre, l'intérêt des interactions issues du monde virtuel. Probablement parce que le mot "virtuel" n'est pas approprié. Un blog, un compte Twitter, une page Facebook, cela permet de générer des interactions sociales, des échanges d'idées, des piques, des blagues, des nouvelles sur tous les sujets, avec des vrais gens qui vivent dans le vrai monde réel.

Les outils numériques me permettent d'échanger avec un nombre très important de personnes, sans avoir à aller boire un coup au café, sans m'abrutir devant le journal télévisé, sans attendre la pro-

chaîne réunion familiale. Cela m'ouvre sur le monde, moi qui suis un peu autiste.

Quand je retrouve les copains avec qui j'ai fait mes études, j'ai du mal à leur faire comprendre l'intérêt des blogs. J'ai beau leur expliquer que ce blog m'a permis de rencontrer des gens formidables, de discuter avec des internautes par réseaux interposés, de participer à des conférences, de progresser dans mon savoir-faire et dans mes opinions, je sens une certaine résistance de leur part...

Twitter est un outil plus compliqué à expliquer, car derrière la simplicité du concept se cache des interactions et des codes plus complexes. C'est un outil également très chronophage, que j'utilise avec parcimonie, car j'ai le souhait de lire TOUTE ma ligne de temps, c'est-à-dire TOUS les tweets des personnes que je suis. Je suis aussi le roi du retweete et je tweete souvent des liens d'articles de blogs que j'aime bien. Je suis assez pauvre en création personnelle (du coup vous pouvez me suivre sans crainte d'être floodé, enfin pas souvent ;-)

Ma personnalité se transforme, au gré des passages d'un type d'interactions à un autre. Je suis sérieux dans mon travail, en charge d'une équipe, d'un groupe d'étudiants ou d'un projet. Je sais décider, trancher, avancer, tel un petit Salomon de Prisunic (©Desproges). Alors que dans ma vie publique de conseiller municipal, je suis beaucoup plus hésitant, à l'écoute, prêts à changer d'avis. Et sous mon identité numérique, je m'épanche volontiers sur mes sentiments, mes doutes, mes souffrances, ce que je ne fais jamais dans mon univers professionnel.

Je souffre d'un [trouble dissociatif de l'identité](#) : j'ai plusieurs personnalités qui se mélangent, et chacune se complait dans un univers particulier. C'est assez étrange. Je peux assister à un événement très privé et me faire la réflexion, tout à fait hors de propos, "tiens, ça ferait un bon sujet de blog". Je peux me rendre compte en réunion d'expertise que le problème évoqué pourrait tout à fait concerner le système informatique de ma société. En faisant la fête avec mes copains, j'ai parfois envie d'en faire profiter mes followers sur Twitter.

Mes copains sont bienveillants envers moi, les internautes qui me lisent aussi, pour la plupart. Mes collègues, les étudiants, les magistrats, les clients me trouvent compétent, enfin certains. Ma famille et ceux qui me côtoient de près, me trouvent un peu étrange, comme un grand gamin. Tous ces mondes se mélangent et s'interpénètrent, comme une [surface de Boy](#).

Je m'enrichis de ces différences et, quand "les autres" m'effraient un peu, le filtre de l'écran me rassure un peu. Je suis un enfant qui ne veut pas mûrir.

Je crois que j'abuse aussi parfois des mélanges.
Mais c'est un abus fort commun et très plaisant.

Professionnaliser son adresse email

En développant mon activité de consultant auprès des avocats, je me suis rendu compte que, dans mon fichier "prospects avocats", la majorité des emails se terminaient en "wanadoo.fr", "gmail.com" ou "yahoo.fr"...

Bien entendu, cela fait sourire tous les informaticiens, pour qui, en général, ces noms de domaine ne font pas très "pro". Mais la réalité nous rattrape toujours, et force est bien de constater que beaucoup de personnes trouvent assez compliqué ce que nous, informaticiens, trouvons relativement évident, comme par exemple qu'il vaut mieux prendre une adresse email indépendante du fournisseur d'accès à internet. Comme ça, si vous changez de fournisseur d'accès, vous n'êtes pas obligé de prévenir tous vos clients : vous pouvez garder la même adresse email.

Je vais donc essayer de détailler à mes lecteurs non avertis une méthode permettant de se doter d'une adresse email professionnelle personnalisée, à moindre frais et en toute simplicité, à condition de bien suivre le mode d'emploi.

Bien entendu, toutes les professions sont concernées : que vous soyez avocat, huissier, géomètre ou charpentier, la procédure est la même.

Ah, oui, j'oubliais : le coût.

Environ 15 euros (par an).

Avant d'entrer dans le vif du sujet, je voudrais présenter quelques définitions, comme dans tout bon cours qui se respecte :

- Fournisseur d'accès à internet.

Un fournisseur d'accès à Internet (FAI), est un organisme (généralement une entreprise mais parfois aussi une association) offrant une connexion à Internet, un réseau informatique mondial. Le terme en anglais désignant un FAI est Internet Service Provider (ISP) ou Internet Access Provider (IAP).

Orange, Free, French Data Network (FDN) sont des exemples de fournisseurs d'accès à internet. RPVA n'est pas un fournisseur d'accès à internet.

- [adresse email](#).

Une adresse électronique, adresse e-mail ou adresse courriel est une [chaîne de caractères](#) permettant de recevoir du [courrier électronique](#) dans une [boîte aux lettres informatique](#).

C'est cette chaîne de caractères que je vous propose de personnaliser. Elle est constituée des trois éléments suivants, dans cet ordre :

- une *partie locale*, identifiant généralement une personne (lucas, Jean.Dupont, joe123) ou un nom de service (info, vente, postmaster) ;
- le caractère séparateur @ ([arobase](#)), signifiant *at* (« à » ou « chez ») en [anglais](#) ;
- un [nom de domaine](#) identifiant généralement l'entreprise hébergeant la boîte électronique (exemple.net, exemple.com, exemple.org).

- [boîte aux lettres informatique](#).

Une [boîte aux lettres](#), ou [boîte de réception](#), ou BAL (abrégié de « [boîte aux lettres](#) »), ou [inbox](#) en anglais, est un espace dédié à un [utilisateur](#), où sont stockés (...) les courriels qui lui parviennent, en attendant qu'il les lise.

Vous pouvez avoir plusieurs adresses emails qui dirigent les emails vers une seule boîte aux lettres. Vous pouvez avoir une seule adresse email qui envoie les emails vers plusieurs boîtes aux lettres. Email, adresse email et boîte aux lettres sont trois choses différentes.

- [client de messagerie](#).

Un [client de messagerie](#) est un [logiciel](#) qui sert à lire et envoyer des [courriers électroniques](#). Ce sont en général des [clients lourds](#) mais il existe aussi des [applications Web](#) (les [webmails](#)) qui offrent les mêmes fonctionnalités. La

caractéristique essentielle de tous ces logiciels est de permettre d'accéder à la boîte de [courriers électroniques](#) d'un utilisateur.

Outlook ou Thunderbird sont des exemples de clients de messagerie. Les webmails permettent, eux, d'être accessibles avec un simple navigateur internet (Firefox, Chrome, Internet Explorer...).

Maintenant que le décor est planté, passons à la pratique.

Je m'appelle Maître Yoda, je suis avocat, et pour me joindre, je voudrais que mes clients écrivent à maitre-yoda@jedi-associes.fr

Je voudrais leur répondre avec cette adresse email.

Etape 1 : acquérir un nom de domaine

Parmi tous les sites proposant ce service, j'ai un faible pour [Gandi.net](#). C'est une longue histoire d'amour entre nous et, malgré tout le temps passé, je suis encore satisfait de leurs services.

Sur la page d'accueil : www.gandi.net se trouve une fenêtre permettant de savoir si le nom de domaine "jedi-associes.fr" est libre ou si quelqu'un l'a déjà loué. A la date d'écriture de ce billet, le domaine est libre et coûte 12 € HT par an.

Attention de bien choisir son nom de domaine. Il y a des règles à respecter (nom de marques, etc.), et il engagera ensuite votre réputation.

Une fois le nom de domaine sélectionné, vous pouvez passer à la caisse pour finaliser votre commande. Attention, il vous faut alors créer un compte sur le site de Gandi. La procédure est simple, je

ne vais pas la détailler ici. Lisez bien les informations affichées et renseignez correctement les champs.

L'ironie de la démarche est qu'il faut indiquer une adresse email valide pour pouvoir créer un compte Gandi. Mais vous disposez bien d'une adresse email valide, non ? L'important est de se souvenir de l'adresse email mentionnée. Je vous recommande de noter tout cela sur un cahier ad hoc, que vous pourrez consulter si dans quelques temps vous devez retrouver cette information.

Vous voilà donc l'heureux propriétaire du nom de domaine "jedi-associes.fr"

Etape 2 : créer sa boîte aux lettres

Dans l'interface de Gandi "Services/Domaines", sélectionnez votre nom de domaine, puis cliquez sur "Boîtes mail : 0/5 **Gérer**". Ensuite, cliquez sur "Service Gandi Mail : Inactif **activer**"

Vous pouvez maintenant créer jusqu'à 5 boîtes aux lettres distinctes (sans frais supplémentaire). Pour cela, il vous suffit de cliquer sur le bouton "**créer**" situé sous la liste (vide) des boîtes mail, puis de remplir le formulaire :

- Dans le champ "Compte", mettez "maitre-yoda" (sans les guillemets).
- Dans les champs "Mot de passe" et "Confirmation du mot de passe", mettez un bon mot de passe qui protégera l'accès à vos emails. Évitez de choisir un mot de passe que vous utilisez déjà par ailleurs. Pour plus d'informations sur le choix des mots de passe, je vous recommande la conclusion de mon billet "[Cracker les mots de passe](#)" (tome 6 ci-avant).

Les autres champs sont facultatifs, mais je vous recommande de remplir celui correspondant à "Email secondaire" pour ne pas perdre d'emails en cas de dépassement de quota.

Votre boîte aux lettres sera créée en quelques minutes.

Etape 3 : tester son email et l'accès à sa boîte aux lettres

Pour accéder à votre nouvelle boîte aux lettres, il vous suffit de vous rendre sur <https://webmail.gandi.net/> et d'y entrer votre login (dans mon exemple, le login est "maitre-yoda@jedi-associes.fr" sans les guillemets) et votre mot de passe. Vous accédez ainsi à l'interface de gestion de vos emails, dans laquelle vous allez pouvoir lire et écrire des emails sous l'identité maitre-yoda@jedi-associes.fr

Demandez à un ami de vous écrire (à maitre-yoda@jedi-associes.fr) et lisez son email dans votre interface de gestion. Répondez-lui et vérifiez avec lui qu'il a bien reçu votre réponse.

Si tout est ok, c'est terminé. Il ne vous reste plus qu'à diffuser cette adresse email autour de vous et à relever vos emails régulièrement.

Pour aller plus loin

Vous voilà propriétaire de votre propre nom de domaine, et vous avez créé une boîte aux lettres et une adresse email personnalisée. Vous lisez et envoyez des emails à partir de votre interface de gestion.

Vous pouvez créer jusqu'à 1000 "redirections mails" vers votre boîte aux lettres. Une "redirection mail" est, dans la terminologie Gandi, une adresse email. Vous pouvez donc avoir plusieurs adresses emails différentes qui dirigeront tous les emails qui leur seront envoyés vers votre unique boîte aux lettres. Cela permet de

disposer d'un grand nombre d'adresses emails personnalisées, sans pour autant devoir aller relever un nombre équivalent de boîtes aux lettres.

Vous pouvez aussi créer 4 autres boîtes aux lettres (pour vos associés et/ou vos secrétaires).

Vous pouvez également ne créer aucune boîte aux lettres et n'utiliser qu'une "redirection mail" vers une boîte aux lettres existante (celle que vous avez l'habitude d'utiliser). Mais il faudra alors configurer votre client de messagerie pour qu'il puisse également écrire avec votre nouvelle adresse email.

Vous pouvez également chiffrer vos emails pour protéger leur contenu et vous assurer qu'ils ne seront lus que par vos correspondants. Si vous ne chiffrez pas vos emails, n'oubliez pas qu'ils peuvent être facilement lus par un intermédiaire indélicat, un peu comme une carte postale sans enveloppe.

Votre nom de domaine peut servir à autre chose qu'à envoyer ou lire des emails : il peut également personnaliser votre site web, accessible par exemple à l'adresse www.jedi-associes.fr

N'oubliez pas non plus de sauvegarder les emails importants, de surveiller votre quota de stockage et de renouveler chaque année le paiement de votre nom de domaine.

Mais tout cela, c'est une autre histoire.

N'hésitez pas à me contacter si vous rencontrez des difficultés.

La dématérialisation des échanges

La revue "Experts" a eu la bonne idée de mettre en ligne, accessible à tous, un compte rendu d'une table ronde consacrée à la dématérialisation des échanges en expertise judiciaire.

L'article est lisible ici: <http://www.revue-experts.com/la-dematerialisation-des-echanges-en-expertise-judiciaire.html>.

Quelques extraits :

« Opalexe est une usine à gaz, très compliquée et déstructurée. »
L'assertion ne vient pas de la concurrence, mais de l'avocat Me Lebon, qui présentait le désormais très consensuel RPVA (Réseau privé virtuel des avocats). « Opalexe est un premier pas, mais doit être amélioré en simplicité. Il doit pouvoir se greffer au système existant, le RPVJ (Réseau privé virtuel de la justice) ».

« Depuis des années on nous demande à la [CEACAP](#) de ne pas parler de notre plate-forme à l'extérieur. Pour ne pas faire concurrence à Opalexe, dont on devait attendre qu'il accomplisse le travail. Ne voyant rien venir de probant, nous avons décidé de nous lancer », introduit Patrick Jeandot, président de la CEACAP, avant de présenter l'outil dématérialiseur [NdZ : [NetExplorer](#)] de sa compagnie, « d'une grande simplicité. »

« Les cartes à puce que vous [NdZ : la [CNCEJ](#)] nous proposez font déjà partie du siècle dernier. »

L'avocat Me Lebon tranche de son côté plutôt « contre » les deux systèmes, parlant de solutions existantes bien plus simples que ces plates-formes. Une messagerie électronique sécurisée ne suffirait-elle pas ? « Si vous arrivez déjà à cela, ce serait énorme. À être trop ambitieux, on prend le risque d'échouer. Un espace de travail collaboratif qui convienne à tous demeure très compliqué à construire. Vos plates-formes forcent tout le monde à penser de la même façon. »

Pour ma part, je penche pour l'utilisation coordonnée du logiciel [GPG](#) déjà accessible à tous, et l'organisation de [key signing parties](#).

Outre l'aspect convivial (des key signing parties), le fait que ces outils soient éprouvés, gratuits, utilisables dans tous les environnements informatiques, par tous (experts, magistrats, parties, etc.) et sur toutes les messageries existantes, me fait penser qu'un pas important serait franchi en toute simplicité. La formation pourrait être effectuée par les associations ou les entreprises ayant mises sur ce type d'outils... ou par les experts judiciaires en informatique ;-)

La création d'une paire de clefs publique/privée et sa gestion (révocation, protection, échange...) devraient être enseignées dès le collège. Nos échanges électroniques - et notre vie privée - en serait grandement sécurisés.

Remerciements

Cet ouvrage n'existerait pas sans ma famille qui me soutient, ni les lecteurs du blog qui me suivent. Qu'ils soient tous ici chaudement remerciés.

Je ne vous oublie pas, vous, lecteur qui a réussi à finir cet ouvrage. J'espère que quelques-uns des textes vous ont plus et qu'ils vous ont donné l'envie de les lire en direct sur le blog, ou de lire les autres tomes. Merci de soutenir ma thérapie par l'écriture.

J'ai une pensée particulière pour mon épouse qui continue à me soutenir dans ma démarche, malgré les ennuis causés par le blog (pour plus d'informations, voir le tome 2 « L'affaire Zythom » et le tome 5 « Pwned »). Elle est d'autant plus méritante qu'elle ne partage pas mon envie de mise à nu sur le blog... Il n'est pas toujours facile d'être marié à un blogueur informaticien expert judiciaire !

Je n'oublie pas non plus Maître Eolas qui m'a soutenu dans les temps difficiles, et qui m'a encouragé à continuer le blog. Qu'il reçoive ici ma reconnaissance et mes remerciements respectueux.

Enfin, je voudrais remercier tous les blogueurs qui m'ont mis dans leurs listes de liens. J'aime cette manière de montrer que l'on apprécie les récits des autres, célèbres et inconnus, et le partage que cela induit. C'est l'un des charmes de la blogosphère ;-)

Merci à vous tous.

Zythom, depuis mon bureau de Tatooine,
Octobre 2015 (sans ma serviette).

Table des matières

Avant-propos	4
Avertissements sérieux	5
Orthographe	6
Contre-expertise	8
Game of gones	14
La prépa	17
Un expert judiciaire peut-il être mauvais dans votre domaine ?	22
L'art de la copie d'écran	26
Stockage	30
Expérience sur l'anonymat	33
Un hacker expert judiciaire	35
Lettre à mes 16 ans	38
Mon père	40
Les innocents	43
Les défis des potes	48
L'ANSSI et le test Google	50
L'incendie	54
Je suis trop faible	59
Cracker les mots de passe	61
Courir contre soi-même	68
Conversation entre un libraire et un expert judiciaire	74
Le tri	86
GERME	89
Ma petite entreprise	93
Ensemble, avec Vous et pour Tous, continuons !	98
Hôpital en mer	102
Journées réseaux 2013	105
Réponse de la cour d'appel	108
Conséquences des agissements de la NSA sur les expertises...	114
Le petit blogueur et l'ANSSI	118
L'admin réseau, cet enquêteur inconnu	121
L'erreur et l'expertise judiciaire	126
Porte à porte	131
Création d'entreprise	135
Le pédophile	139
Le petit garçon qui est en moi	142
L'informatique et les divorces difficiles	144
Le témoin	148
La motivation d'un élu local	154
Les géants	157
42 ans	160
Réseaux de neurones 2	161
Expert près la Cour Administrative d'Appel	165
Réseaux de neurones 3	171
Points de vue	175
Ils avaient	178

L'interrogatoire	180
Petit guide de survie à l'expertise informatique	183
PSES 2014	189
Récupération de données	190
Questionnaire de Proust	193
Evolution professionnelle	195
Pépites du passé	199
Septieme ciel	201
Le disque dur	205
Expert ou Huissier	207
La recette	210
Yéléna	215
Mélanges	217
Professionnaliser son adresse email	220
La dématérialisation des échanges	226
Remerciements	228

