CNEJITA: journée technique du 21/06/2011

Jean-Arnaud Causse, Toulouse

LES OUTILS DE L'EXPERT
LES MOYENS GRADUELS D'ÉQUIPEMENT

LES OUTILS DE L'EXPERT

- Préambule
- L'expertise au Civil
- L'expertise au Pénal
  - L'expertise des supports numériques courants
  - L'expertise des téléphones mobiles / des smartphones
  - L'expertise des supports exotiques
- L'assistance à Huissier

PRÉAMBULE

- Cette présentation est basée sur ma propre expérience
- Cette présentation n'est pas une présentation exhaustive, ni une formation à tel ou tel outils
- Cette présentation a pour seul but de favoriser un échange entre nous

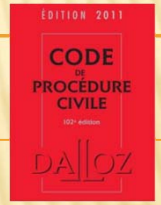
Avant de mutualiser nos outils,

mutualisons nos expériences

Au passage: un merci à Internet, à la mail-list et aux J.T. CNEJITA,

à vous tous et aux autres …

L'EXPERTISE AU CIVIL



- article 146 du Code de Procédure Civile

  « En aucun cas, une mesure d'instruction ne peut être ordonnée en vue de suppléer la carence de la partie dans l'administration de la preuve »

- L'outillage prérequis est faible : bureautique, …
- Les moyens spécifiques doivent être fournis par les parties
- Et ceci à titre de vérification et non d'investigation
- Comme toujours, les généralités souffrent d'exceptions

L'EXPERTISE AU CIVIL

L 'expertise au civil

et particulièrement avec des entreprises de taille respectable

→ Un tsunami de papier

à croire que l'argumentation se mesure

à la hauteur des piles de pièces annexes

- Numérisation des pièces transmises par les parties
  - Les (jeunes) avocats s'y mettent rapidement — diminution des coûts
  - La numérisation des documents papier nécessite un matériel adapté et efficace — chargeur automatique
  - Le gain est évident en place, en archivage, en vacances …

L'EXPERTISE AU PÉNAL

Elles sont les plus mal payées

Et pourtant elles nécessitent les outils les plus onéreux

- Trois gammes de prix
  - La 2CV : elle va au bout du monde pour pas cher et si on a le temps

0 – 200 €

POUR COMMENCER MAIS CHRONOPHAGE

  - La Familiale : elle est pratique et confortable pour un prix abordable

300 – 1000 €

UN BON COMPROMIS

  - La Ferrari : tout le monde en rêve, mais son entretien coûte cher

2000 – 5000 €

DIFFICILE À AMORTIR SEUL

LES SUPPORTS NUMÉRIQUES COURANTS

- Les systèmes d'exploitation cibles
- Le clonage
- La récupération des fichiers effacés
- La recherche / le tri d'image et vidéo
- L'analyse des traces Internet (surf / emails / IM)
- Le reste

LES SYSTÈMES CIBLES

- Le podium

	Part des visites* par Famille de Sytème d'Exploitation *Indicateur moyen par site*					
	nov.-09	*déc.-09*	*janv.-10*	*févr.-10*	*mars-10*	*avr.-10*
Microsoft	93.0%	92.5%	92.4%	92.4%	92.3%	**91.9%**
Windows XP	62.5%	59.6%	58.4%	57.9%	57.3%	**55.6%**
Windows Vista	25.0%	25.4%	24.5%	23.5%	22.6%	**22.4%**
Windows 7	3.3%	5.7%	7.7%	9.2%	10.6%	**12.3%**
Apple	5.9%	6.3%	6.4%	6.4%	6.4%	**6.8%**
Mac Os X Intel	4.7%	4.9%	5.1%	5.1%	5.1%	**5.3%**
OS iPhone (iPhone, iPod, iPad)	0.5%	0.7%	0.7%	0.7%	0.8%	**0.9%**
Mac Os X PPC	0.7%	0.6%	0.6%	0.6%	0.5%	**0.5%**
Linux	0.8%	0.8%	0.9%	0.8%	0.8%	**0.9%**
Autres OS	0.3%	0.4%	0.4%	0.4%	0.4%	0.4%
TOTAL	100%	100%	100%	100%	100%	**100%**

* Visites effectuées dans le pays, sur les sites audités par une solution AT Internet, dont le trafic est généré principalement depuis le même pays.
** En moyenne pour 1 site, en moyenne sur 23 pays européens (Voir méthodologie).

- Les autres (ex: AS400) : si cela intéresse quelqu'un dans la salle ?

LE CLONAGE

mission du Juge d'Instruction:

« Procéder à une copie par tous moyens techniques appropriés de nature à garantir une reproduction à l'identique, intègre et infalsifiable, du contenu des supports de données informatiques renfermés dans les scellés examinés »

L'accès au disque dur / La recopie / Le calcul du Hashcode

- gratuit :
  - suite forensic : DEFT / Helix montage readonly Linux
  - outil de copie forensic : dcfldd / ddrescue / guymager / FTK Imager / ...
- payant et plus confortable :
  - bloqueur en écriture électronique (débit)
  - logiciel de blocage ? 
- plus rapide, mais plus cher :
  - duplicateur

TABLEAU

Intelligent Computer Solutions

wiebeTECH
A Brand of CRU-DataPort

L'accès au clone

- gratuit : FTK Imager / P2 Explorer
  Liveview et la virtualisation (cette après-midi)
  Les outils « forensics » pour leurs propres besoins

LA RÉCUPÉRATION DES FICHIERS EFFACÉS

- La récupération « traditionnelle »
  - gratuit :
    - Recuva / Undelete Plus Portable / …
  - payant :
    - GetDataBack / Ontrack EasyRecovery / R-Studio / Stellar Phoenix / …

- Le file carving
  - gratuit :
    - PhotoRec / Scalpel / Foremost
  - payant :
    - X-Ways / FTK / Encase

LA RECHERCHE / LE TRI D'IMAGE / VIDÉO

- Le file carving (cf. slide précédent)
- L'extraction des images insérées : thumbnail / .doc .ppt .pdf ...
  - gratuit : ?
  - payant : X-Ways / FTK / Encase
- Le tri « skin color » (pédopornographie)
  - gratuit : ?
  - payant : X-Ways / FTK / Encase (?)
- La recherche dans des bases de référence (pédopornographie)
  - gratuit : ?
  - payant : FTK / Encase (?)

LES TRACES INTERNET / LES EMAILS

- Historique / Cache / Messagerie instantanée
  - gratuit :
    - Pasco, Galleta, Nirsoft, Index.dat, PhotoRec
  - payant :
    - X-Ways Trace (n'est plus mis à jour)
    - NetAnalysis
    - CacheBack
    - Paraben Chat Examiner
    - Internet Evidence Finder (à une longueur d'avance)
- Email (recherche / récupération / conversion / lecture)
  - gratuit :
    - Nirsoft, les Mailer
  - payant :
    - ABC Amber (arrêté ?), Emailchemy, Stellar Phoenix
    - Paraben E-Mail Examiner
    - FTK , Encase

NirSoft

IEF

Outlook Express

Stellar DATA RECOVERY

Emailchemy the email alchemist

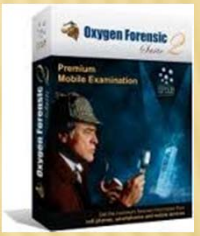
paraben corporation

LE RESTE

- L'analyse de l'activité
  - gratuit: Nirsoft / Sleuth Kit et une multitude d'autres outils
  - payant: X-Ways / FTK / Encase
- La recherche par mot clé
  - gratuit: Nirsoft SearchMyFiles / Sleuth Kit
  - payant: recherche multicritère X-Ways / FTK / Encase
- Les casseurs de mots de passe (rarement utile ?)
  - gratuit mais limité: OphCrack
  - de nombreux produits payants: OphCrack / Passware / FTK ...
  - des solutions hardware onéreuses
- Les logiciels de compta ou métier
  - Les versions démos
  - Le démarrage de la machine avec un clone
- La virtualisation présentation de cette après-midi

LES TÉLÉPHONES MOBILES

- Les logiciels
  - gratuit: les suites constructeurs 
  - payant: MobilEdit / Oxygen Forensic / Paraben Lantern (Iphone / MacOS)
  - onéreux (hardware): XRY-XACT / Cellebrite



LES MISES À JOURS SONT PRIMORDIALES

LES TÉLÉPHONES MOBILES

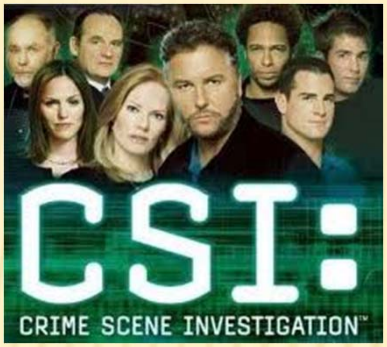
- Le matériel
  - gratuit: faut pas rêver
  - payant, mais pas très cher:
    - lecteur carte SIM
    - câble data au coup par coup — Ebay: clone pas cher peu robuste
    - kit alimentation de voyage / chargeur universel
    - brouilleur GSM WIFI — interdit au particulier
  - onéreux: valise MobilEdit / XRY-XACT / Cellebrite

LES SUPPORTS EXOTIQUES

- GSM
- Système de vidéosurveillance
- Pointeuse
- Carte bleue

LES ASSISTANCES À HUISSIER

Les avocats et huissiers ont tendance à croire que nous sommes :



Les outils de l'expertise pénale peuvent être utiles (ex: recherche par mots clés)
mais cloner un disque de 2To sur place pendant un constat ne dure pas 30 secondes

Attention au démontage d'une machine - sauf si l'ordonnance le prévoit explicitement

CNEJITA: journée technique du 21/06/2011

Jean-Arnaud Causse, Toulouse

FIN

LES OUTILS DE L'EXPERT
LES MOYENS GRADUELS D'ÉQUIPEMENT