

Glossaire numérique et téléphonique de l'informatique légale

Reproduction interdite. Citation d'articles autorisée avec mention de la source.

Glossaire numérique et téléphonique de l'informatique légale
Copyright © LERTI 2010, – Version 4.33 – 03/11/2010.

.amr Extension de nom de fichiers audio.

.avi Extension de nom de fichiers vidéo.

.bin Extension, non propriétaire, de nom de fichiers, pouvant concerner des fichiers binaires (en particulier en langage machine), mais aussi des fichiers divers (audio, MIME, Macintosh ou Micrografx). En contexte pénal, surtout si elle est simultanée à celle de fichiers .hex, la présence de fichiers .bin est souvent l'indice d'une activité de carding (voir ce terme).

.bmp Bitmap. Extension de nom de fichiers d'images.

.csv Carriage Value Separator. Extension de nom de fichiers de bases de données en mode texte dont les champs sont séparés par des virgules ou des points-virgules et les enregistrements par des retours chariots. Format universel et non propriétaire.

.doc, docx Extension de nom de fichiers du traitement de texte Microsoft Word.

.emf Enhanced Metafile. Extension de nom de fichiers d'images vectorielles propres à Windows.

.eml Email. Extension de nom de fichiers utilisés par un grand nombre de logiciels de messagerie avec enregistrement sous forme texte d'un seul message par fichier. Définie par les RFC 0822 et 2822. Utilisée notamment par Outlook Express. A ne pas confondre avec Extended ML.

.exe Extension de nom de fichiers exécutables (Dos, Windows).

.gif Graphics Interchange Format. Extension de nom de fichiers d'images.

.hex Hexadécimal. Extension de nom de fichiers exécutables par micro-contrôleurs et notamment ceux qui équipent les puces des cartes bancaires. Voir l'article .bin.

.htm ou .html Hyper Texte Markup Language. Extension de nom de fichiers textes s'affichant sous forme graphique dans les navigateurs Internet.

.jar Extension de nom de fichiers d'archivage de type .zip pour les environnements Java (jar provient de Java et de archive) incorporant un ensemble de métadonnées.

.jpg ou .jpeg Joint Photographic Experts Group. Extension de nom de fichiers d'images.

.mht ou .mhtml Format de fichiers ouvert et non propriétaire permettant d'enregistrer et d'envoyer un fichier HTML au format MIME y compris les images et autres éléments externes de la page HTML.

.mms Extension de nom de fichiers de fichiers de messagerie. Voir MMS.

.mpg ou .mpeg Motion Picture Expert Group. Extension de nom de fichiers vidéos.

.odt Open Document Text. Extension de nom de fichiers texte de la suite Open Office.

.pdf Portable Document Format. Format de documents portables. Extension de nom de fichiers comprenant un langage de description de pages créée par Adobe. L'avantage de ce format est de préserver les polices, les images, les objets graphiques et la mise en forme de tout document source, quelles que soient l'application et la plate-forme utilisées pour le lire et l'imprimer.

.png Portable Network Graphics. Extension de nom de fichiers d'images.

.ppt Extension de nom de fichiers du logiciel de présentation Powerpoint de Microsoft.

.rar Extension propriétaire de nom de fichiers permettant l'archivage par compression d'un ou plusieurs fichiers en un seul.

.rtf Rich Text Format. Extension de nom de fichiers de traitement de textes.

.txt Extension de nom de fichiers textes non mis en page, d'usage très général.

.vgm Extension de nom de fichiers de messagerie.

.wab Windows Address Book. Extension de nom des fichiers du carnet d'adresse Windows. Utilisés notamment par Outlook.

.wmf Windows Metafile. Extension de nom de fichiers d'images vectorielles propres à Windows, apparue début 1990, aujourd'hui remplacés par le format .emf.

.xls Extension de nom de fichiers du tableur Microsoft Excel.

.xml Extended Markup Language. Extension de nom de fichiers comportant un système de balises pour l'affichage ou l'édition.

.zip Extension de nom de fichiers permettant l'archivage par compression d'un ou plusieurs fichiers en un seul.

3G Voir UMTS.

A ≡

ADN Abbreviated Dialling Numbers (ou Speed Dialling Numbers). Répertoire téléphonique propre à la SIM ou à l'USIM. Comprend jusqu'à 250 enregistrements (numéros de téléphones). Le téléphone peut comprendre son propre répertoire, avec un nombre d'enregistrements généralement plus important.

Adresse IP Voir IP.

ADS Alternate Data Stream. Les ADS sont des fichiers cachés, associés à un fichier normal, dans les systèmes de fichiers NTFS. Contrairement aux fichiers "cachés" par l'attribut "hidden", les ADS ne sont pas visibles de l'explorateur ou de la commande "attrib". Leur manipulation cependant très facile peut permettre de dissimuler aisément des données ou de faire exécuter furtivement des programmes malveillants.

ASCII American Standard Code for Information Interchange. Code américain standard pour l'échange d'information. Développé et adopté dans les années soixante du siècle dernier, le premier code ASCII définit une liste de caractères imprimables (96) et de "caractères" non imprimables (32) nécessaires à la représentation et à la communication des premiers et assigne une place à chacun dans une liste de 128 éléments, étendus par la suite à 256 pour inclure notamment les caractères accentués et être codé sur un octet. Quasiement seul système de codage pendant longtemps, le code ASCII a ensuite servi de base à de nombreux autres systèmes de codage, dont le système Unicode en particulier.

ATA Voir IDE.

Avatar Proche du sens étymologique venu de la religion hindoue (mais appliqué à Internet et aux jeux), incarnations – parfaitement virtuelles ici – différentes d'une même personne. "Pseudonyme" conviendrait mieux pour désigner la possibilité de dissimuler ainsi sa véritable identité et surtout sa véritable personnalité.

B ≡

Backdoor Voir Porte dérobée.

Base de registre Registry en anglais. Base de données d'informations système propre au monde Microsoft. Apparue en 1993 avec Windows NT, la base de registre est un système d'informations hiérarchisé contenant de nombreuses données de configuration et de paramétrage tant du système d'exploitation que des logiciels installés. Son interprétation est rendue difficile du fait de la confidentialité des données introduites par chaque éditeur. Elle

recèle néanmoins des informations parfois capitales pour l'investigation numérique.

BIOS Basic Input Output System. Le BIOS enregistre tous les paramètres représentant la configuration matérielle et les différentes options nécessaires au démarrage d'une machine. La date système est enregistrée dans le BIOS (à ne pas confondre avec la date de la ROM).

Bit Représente la plus petite unité possible d'information. Un bit en informatique représente une valeur booléenne ("vrai" ou "faux") du monde représenté.

Bombe logique Programme destiné à exécuter une tâche nuisible lors de la survenance d'un certain événement : date donnée, nombre de mises en marche d'une machine, frappe d'une combinaison donnée de touches par exemple.

Bookmark Marque-page, favori ou signet en français. Repère par lequel on enregistre l'adresse d'une page Web ou un emplacement dans tout type de document, afin de pouvoir y revenir ultérieurement. On les trouve principalement dans les logiciels de traitement de texte et dans les logiciels de navigation internet. L'inscription d'un bookmark relève normalement de l'action volontaire de l'utilisateur d'un ordinateur.

Boot Litt. "botte", au sens "d'être dans la botte" pour qualifier le classement d'entrée dans un grand corps. En informatique : démarrage. Voir "booter", "secteur de boot".

Booter Mise en route initiale d'un ordinateur, avec exécution d'un certain nombre d'opérations de configuration programmées pour cette phase de démarrage.

Botnet Ensemble de machines (dites zombies) exploitées de manière malveillante par un pirate informatique qui en a pris le contrôle à l'insu de ses utilisateurs ou propriétaires afin de diriger une attaque massive (de type DDoS) destinée à paralyser une machine ou un service ou pour envoyer des spams en très grande quantité. Un botnet peut compter plusieurs millions de zombies qui peuvent être mis en action en quelques minutes pour déclencher une action de grande envergure.

Bus On appelle bus un ensemble de liaisons physiques pouvant prendre des formes diverses (circuits, câbles) destinées à la communication entre les éléments composant un système informatique. Trois bus internes se retrouvent dans tout ordinateur : le bus de données, le bus des adresses et le bus des commandes. L'USB (Universal Serial Bus) est un bus d'entrées-sorties qui permet de relier un vaste ensemble de composants (scanner, appareil photos, clés USB) à un ordinateur.

C ≡

Cache, cacher Lors de la navigation sur Internet à l'aide d'un navigateur (Internet Explorer, Firefox par exemple), le système d'exploitation conserve une copie des objets importés, et en particulier des images, afin d'éviter de retourner chercher ces objets sur Internet lors d'une prochaine consultation d'un même site et d'accélérer ainsi les accès. Dans ce sens "cacher" ne signifie pas "dissimuler". Au contraire, la liste exhaustive des fichiers "cachés" est présente dans des fichiers de log ("index.dat" pour Internet Explorer). Notons toutefois que les spécifications de mise en cache ne sont pas publiées. Il en résulte, du point de vue de l'investigation informatique légale, que la preuve négative ne peut être retenue.

Carding Terme utilisé par les fabricants de fausses cartes, notamment bancaires, pour désigner leur activité, et, par extension, tout ce qui s'y rattache. Ne signifie évidemment pas l'activité textile de cardage !

Carte mémoire Mémoire flash (de type NAND) sur support individualisé destinée à étendre une mémoire interne (cas des téléphones portables en particulier). Du fait de leur petite – voire très petite – taille, ces cartes sont propices à l'échange et à la dissimulation de données. Les différentes cartes disponibles sont les CompactFlash (CF), SmartMedia cards (SM), xD cards, Multi media Cards (MMC), Secure Digital (SD), Mini SD, Micro SD, Secure Digital High Capacity (SDHC), Solid State Disk (SSD), MemoryStick et MemoryStick M2.

Carving Procédure de restauration de données effacées basée sur les signatures de début et fin de fichiers. En général fonction intégrée dans les logiciels d'investigation informatique. Dit aussi Salvage.

ccTLD Country Code Top Level Domain. TLD (voir ce terme) attribué à un pays donné (.fr pour la France par exemple).

Chat Voir tchat.

Cheval de Troie Comme le Cheval de Virgile (Timeo danaos et donae ferentes ...) un Cheval de Troie fait autre chose que ce qu'il est supposé devoir faire, par exemple ouvrir une porte dérobée qui permet des intrusions silencieuses dans un système informatique. Il ne se réplique pas de

lui-même et à ce titre ne peut pas être considéré comme un virus au sens strict.

Clef Luhn Algorithme très simple qui permet de vérifier la validité d'une suite de chiffres. Utilisé dans de nombreux domaines, notamment dans les cartes bancaires.

Cluster Un cluster (grappe en français) est un regroupement de secteurs angulaires d'une même piste circulaire, ou, le plus souvent d'un même cylindre. Ce regroupement est destiné à accélérer l'accès aux informations.

Code ASCII Voir ASCII.

CompactFlash (CF) Carte mémoire de type flash (voir l'article "Carte mémoire").

Connexion Voir "Hits".

Cookie Littéralement : gâteau sec. Du point de vue informatique, désigne un petit fichier déposé sur l'ordinateur de l'internaute qui consulte un site Internet. Le dépôt des cookies peut répondre à des objectifs techniques comme l'identification d'une machine pour le temps d'une transaction. Il correspond souvent à l'objectif commercial de connaître et d'enregistrer le comportement d'un internaute. Les cookies peuvent être interdits et/ou supprimés par l'utilisateur.

Copie pure et parfaite Une copie est pure quand son empreinte numérique est identique à celle - confirmée - de l'information numérique dont elle est la copie; elle est en outre parfaite quand l'information numérique originale n'a pas été modifiée par l'opération de copie.

Copie-image Copie bit à bit intégrale de l'information numérique présente sur un support d'informations, y compris espaces non utilisés, espaces non alloués et queues de clusters, effectuée à l'aide d'un logiciel spécifique. Réalisée dans le cadre d'une investigation numérique légale, une copie-image doit être pure et parfaite ; dans le cas contraire, le rapport d'investigation explique les raisons de l'impureté ou de l'imperfection. (Angl. approché : Forensic Copy).

Cylindre Un disque dur comprend plusieurs plateaux. Un cylindre regroupe les pistes circulaires de chaque plateau situées à même distance du centre du disque.

D ≡

Date de la ROM Chaque carte mère comporte une puce de mémoire permanente de type ROM qui mémorise les données du BIOS. Cette puce comprend un champ qui indique la date de fabrication de la ROM. Cette date peut être tenue pour la "date de naissance" d'une carte mère et donc souvent d'un ordinateur.

Date système La date système est celle enregistrée dans le BIOS d'une machine. Cette date sert à dater toutes les opérations effectuées sur cette machine. Sur les machines de type PC, sa fiabilité est relative, d'une part car elle connaît une dérive avec le temps, d'autre part parce que l'utilisateur peut facilement la modifier.

Dates des fichiers et répertoires Les systèmes d'exploitation enregistrent diverses dates concernant les répertoires et les fichiers. Ces dates dépendent des systèmes de fichiers et des systèmes d'exploitation : ainsi, on peut trouver une date de création, une date de dernière modification, une date de dernier accès ou encore une date de dernière modification des propriétés. Toutes ces dates présentent une fiabilité relative : elles peuvent provenir d'une date système fautive et peuvent être modifiées a posteriori. Ces dates peuvent être modifiées lors de simples opérations de copie – quand elles sont réalisées entre système de fichiers différents par exemple –. Les dates modifiées volontairement peuvent parfois être décelées, soit en raison d'incohérences, soit parce que certains fichiers enregistrent de manière interne l'une ou l'autre des dates mentionnées ci-dessus. Toutes ces dates doivent être interprétées avec beaucoup de précautions.

dc3dd Voir dd.

dcfdd Voir dd.

DCO Device Configuration Overlays. Zone d'un disque rendue inaccessible par le fabricant ou le distributeur afin de donner à ce disque une taille inférieure à sa capacité réelle, dans un but commercial. Cette zone peut être utilisée pour cacher de l'information, à l'aide de logiciels spéciaux. Voir HPA.

dd disk dump. Utilitaire venu du monde Unix permettant de réaliser des copie-image de fichiers ou de disques. Reposant sur cette commande, plusieurs utilitaires dont dcfdd et dc3dd ont été développés spécialement pour l'investigation informatique légale.

Débrider, débridage Voir Jailbreak.

Déni de service Désigne le fait qu'une machine ne peut plus assurer un service (messagerie, serveur Web par exemple) en raison du trop grand nombre de requêtes qui lui est adressé. Un déni de service est souvent provoqué de manière intentionnelle dans le but de nuire. On distingue alors les attaques de type PING-Flood (envoi de requête PING), SYN-Flood (envoi de paquets de synchronisation sans phase d'acquittement), de type ACK-Flood (par envoi de paquets de type ACK en grand nombre).

Déni de service distribué Désigne le fait qu'un ensemble de machines sont mobilisées pour participer en même temps à une attaque par déni de service (voir Botnet).

Denial of service (DoS) Voir déni de service

Distributed denial of service (DDoS) Voir déni de service distribué

Données accessibles S'agissant de la description et de la qualification des scellés, les catégories de l'investigation informatique légale ne correspondent pas au statut juridique de scellés "ouverts" ou "fermés" issu du monde physique non numérique. Les données numériques d'un scellé sont qualifiées d'"accessibles" quant il est possible de les lire, de les modifier ou de les supprimer sans porter atteinte au statut juridique qui est leur est attribué. Un téléphone portable resté assemblé dans un sachet transparent est typiquement un scellé juridiquement "fermé" mais de "données accessibles". Le rapport de garde décrit le statut des scellés en entrée au laboratoire. Les scellés sont toujours restitués par le Lerti "données inaccessibles" : ainsi les téléphones sont décomposés entre leurs divers composants (boîtier, carte SIM, batterie, carte mémoire) dans des sachets de scellés compartimentés par thermosoudage.

Données non accessibles Voir l'article "Données accessibles".

Données Toute information présentée sous forme numérique, quel que soit sa nature ou son sens. Ces données peuvent représenter un texte, un dessin, une image, un son, un ensemble structuré d'informations... Data en anglais. Les données numériques sont toujours associées à des métadonnées.

DoS Abréviation de Denial of Service. Voir ce mot.

Dump Verbe décrivant l'opération consistant à copier la totalité d'une mémoire (vive en particulier), généralement sur un support permanent, et substantif relatant le résultat de cette opération.

E ≡

Ecart-type Instrument statistique permettant de mesurer la dispersion d'une série de valeurs autour de la moyenne (c'est la racine carrée de la moyenne des carrés des écarts à la moyenne d'une distribution normale en statistiques descriptives).

EEPROM Electrically-Erasable Programmable Read-Only Memory (mémoire en lecture seule effaçable électriquement). Composant de stockage d'informations non volatiles utilisé dans les ordinateurs et d'autres équipements (cartes à puces, console de jeux vidéo ...). Une EEPROM peut être programmée et effacée plusieurs milliers de fois et lue à l'infini. Les mémoires Flash sont une variété d'EEPROM.

Empreinte numérique Empreinte digitale d'une information numérique produite par un algorithme mathématique appliqué à cette information (disque physique ou logique, fichier). Cet algorithme – par essence à sens unique – est tel qu'il est impossible de changer l'information numérique sans en changer la valeur de l'empreinte. Autrement dit, si l'empreinte numérique d'un fichier n'a pas changé alors ce fichier n'a pas été modifié et réciproquement. Pour être certaine, l'empreinte numérique doit être calculée de deux manières indépendantes (pour les disques durs en particulier). Parfois désigné par "valeur de hachage". (Angl. : Hash Value).

EXIF Exchangeable image file format. Spécification de format de fichier pour les images utilisées par les appareils photographiques numériques. Il a été établi par le Japan Electronic Industry Development Association (JEIDA). Cette spécification repose sur des formats existants tels que JPEG, TIFF et autres, en y ajoutant des balises de métadonnées. Ces métadonnées comportent la date, l'heure et les réglages de l'appareil de prise de vue ainsi que la localisation par GPS du lieu de prise de vue pour les appareils disposant de cette fonctionnalité (comme l'iPhone 3G de Apple).

EXT2, EXT3 Systèmes de fichiers utilisés par Linux.

Extension de nom de fichiers Les fichiers sont en général désignés par un nom suivi d'un point et d'une extension finale, par exemple "image.jpg".

F ≡

FAT, FAT32 Systèmes de fichiers utilisés par les systèmes d'exploitation DOS et Windows.

Faux virus Hoax en anglais. Catégorie assez particulière de virus reposant sur la crédulité et l'absence de formation des usagers des systèmes informatiques. Ces faux virus fonctionnent sur le mode antique de la chaîne : en prévenant de ne pas ouvrir un soit disant mail intitulé "Bonjour" par exemple et surtout en proposant de prévenir tous vos amis des risques catastrophiques de ce mail, un faux virus génère un tel trafic sur un réseau informatique qu'il peut l'engorger complètement. On pourrait considérer qu'il s'agit d'un canular si le but recherché n'était pas de nuire.

Favori Voir Bookmark.

Fichier d'images Fichier dont le contenu est représentable graphiquement sous forme d'une image.

Firmware Logiciel (micro logiciel est la traduction recommandée) embarqué dans un composant matériel qu'il pilote (lecteur de DVD par exemple). Intégré généralement dans une EEPROM, le firmware peut souvent être mis à jour par un utilisateur averti, à partir de nouvelles versions mises à disposition du public sur le site du fabricant.

Flash Voir article Mémoire flash.

Formater Opération consistant à délimiter les pistes et les secteurs d'un disque et à établir le système d'adressage. Le formatage détruit en apparence toutes les informations, mais ces dernières peuvent généralement être retrouvées avec des outils appropriés, sauf si le formatage s'est accompagné d'une procédure spéciale de suppression effective des données.

G ≡

Go Unité de mesure usuelle en informatique. Un "Go" est un giga octets, soit 1024 Mo ou encore 1 073 741 824 octets. Un Go "commercial" ou normalisé ne fait que un milliard d'octets.

GPRS General Packet Radio Service.

Grep Commande en ligne venue du monde Unix, permettant de filtrer des fichiers sur des chaînes de caractères ou des expressions dites régulières. Cette commande peut être associée à d'autres dans un "pipe" (tuyau de commandes) de manière à en chaîner plusieurs (plusieurs grep notamment) de manière particulièrement souple et efficace.

GSM Global System for Mobiles. Système de téléphonie cellulaire mis en place par la Conférence des Administrations Européennes des Postes et Télécommunications et largement répandu dans le monde (sauf Etats-Unis, qui utilisent le standard IS41 et où la diffusion du GSM est restreinte).

H ≡

Hiberfil.sys Nom donné dans les systèmes d'exploitation Windows au fichier d'hibernation. Ce fichier est créé lorsqu'un ordinateur est mis en veille prolongée, afin de permettre un redémarrage rapide du système dans l'état où il se trouvait au moment de l'extinction. Pour cela, le système effectue une copie complète de la mémoire vive. Précieux recueil d'information pour l'investigation numérique car le fichier d'hibernation peut comprendre des informations autrement inaccessibles (mots de passe en clair par exemple).

Hits Tous les journaux de log, qu'ils soient ceux des machines des usagers ou ceux des serveurs, enregistrent les connexions Internet, notamment lors des visites de sites répondant au protocole http. Chaque requête est enregistrée de manière singulière, avec des informations diverses, qui comprennent par exemple l'heure. Ces requêtes singulières sont les "Hits", que l'on peut traduire par "connexion". Ce mot prend alors un sens très différent du sens courant. En effet, pour remplir une page "Web", il faut autant de requêtes ou "hits" qu'il y a d'images, de textes et d'éléments divers. Tandis que le public pense avoir établi une seule "connexion" avec tel site, le journal de log enregistre de nombreux "hits" et l'informaticien voit de nombreuses "connexions".

Hoax Voir Faux virus.

HPA Host Protected Area. Zone cachée d'un disque dur, inaccessible aux logiciels courants. Cette zone peut toutefois être utilisée en faisant appel à des logiciels spéciaux, facilement accessibles et gratuits. La HPA peut constituer une "cachette" d'autant plus sûre que tous les logiciels d'investigation ne savent pas la lire. Voir également DCO.

HPLMN Home PLMN (voir ce sigle). Intervalle de temps pendant lequel un téléphone recherche son propre réseau.

HTTP Hyper Text Transfer Protocol. Il s'agit d'un des principaux protocoles de l'Internet, dont l'objectif est de permettre l'affichage de pages par l'intermédiaire d'un navigateur et de mettre en relation des objets (pages, images, sons, ...) situés dans l'ensemble de l'espace adressable par ce protocole, connu sous le nom de "web".

I ≡

ICCID ou ICC Integrated Circuit Card Identifier. Numéro de série d'une carte SIM. Imprimé sur la carte et présent en mémoire. Seul identifiant d'une carte SIM accessible sans code PIN. Il comprend l'identifiant SIM (89), un code pays (33 pour la France), un code opérateur et un numéro de série, soit 19 ou 20 chiffres au total. Défini par la recommandation E118 du CCITT, maintenant ITU-T.

IDE Integrated Drive Electronics. Le standard ATA (Advanced Technology Attachment) est une interface standard permettant la connexion de périphériques de stockage et en particulier les disques durs sur les ordinateurs de type PC. Ce standard ATA a été mis au point en 1994 par l'ANSI. Malgré l'appellation officielle "ATA", ce standard est plus connu sous le terme commercial IDE ou Enhanced IDE (EIDE ou E-IDE). Rétroactivement appelé PATA pour le distinguer du nouveau standard SATA.

IMEI International Mobile Equipment Identity. Numéro de série d'un GSM. Imprimé en général à l'intérieur du téléphone et présent en mémoire. Accessible par *#06#.

IMSI International Mobile Subscriber Identity. Numéro d'identification unique du souscripteur d'une carte SIM. Présent sur la carte SIM, cet identifiant est composé d'un code pays, d'un code opérateur et d'un numéro de client, soit 15 chiffres au total. L'identification du souscripteur correspondant à un IMSI est disponible chez l'opérateur.

Information numérique Toute information présentée de manière digitale et qui peut être divisée entre l'information proprement dite – constituant les données – (texte, dessin, image, son, base de données...) et les informations relatives à cette information proprement dite appelées méta-données (nom de fichier, nom de répertoire, date et heure de création, de modification ou d'édition d'un document, expéditeur d'un email...). La connaissance d'une méta-donnée peut être le moyen de la découverte de l'information proprement dite. Inversement, les méta-données peuvent constituer des preuves numériques (datation d'un événement, expéditeur d'un email...). (Angl. : Digital Information).

Informatique légale Application de techniques et de protocoles d'investigation numérique respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution de type judiciaire, par réquisition, ordonnance ou jugement. Dit aussi investigation numérique légale. (Angl. approché : Forensics).

Investigation numérique légale Voir informatique légale.

Investigation numérique Utilisation de techniques spécialisées dans la collecte, l'identification, la description, la sécurisation, l'extraction, l'authentification, l'analyse, l'interprétation et l'explication de l'information numérique. Ces techniques sont mises en œuvre quand une affaire comporte des questions relatives à l'usage d'un ordinateur et de tout autre support d'information, ainsi qu'à l'examen et l'authentification de données en faisant appel aux techniques d'analyse du fonctionnement des ordinateurs ou à la connaissance des structures de données. L'investigation numérique est une branche spécialisée de l'informatique qui requiert des compétences allant au-delà de celles nécessaires à la maintenance et à la sécurité informatique. (Angl. approché : Computer Forensics).

IP Internet Protocol. Dans la version dite "IPv4", encore largement répandue, les adresses IP sont composées de 4 octets exprimés en décimal séparés par un point, de type 123.123.123.123. Avec la version "IPv6" en cours de déploiement, l'adressage repose sur 16 octets exprimés en hexadécimal. L'espace adressable passe ainsi de 2³² objets (ordinateurs, imprimantes, etc.), soit un peu plus de 4 milliards, à 2¹²⁸, soit un nombre supérieur au nombre d'atomes dans l'univers !

J ≡

Jailbreak Litt. évasion (de prison), "débrider" en langue française. Opération qui consiste à modifier le système d'exploitation d'un matériel électronique pour permettre de passer outre aux restrictions imposées par le constructeur. Les systèmes électroniques les plus concernés sont les téléphones portables (iPhone en particulier), les matériels de la marque Apple (iPad, iPod) et les consoles de jeux (Playstation). Le système débridé peut alors recevoir des applications non autorisées par le constructeur ou être modifié au gré de l'utilisateur qui peut potentiellement accéder à toutes les fonctionnalités du système d'exploitation. Les constructeurs, et en particulier la société Apple, combattent le débridage qui entraîne la perte de la garantie. Le débridage, effectué par l'utilisateur ou réalisé après autorisation de justice lors d'une expertise, donne généralement l'accès à la totalité de la mémoire d'un support électronique.

Journal de log Voir Log.

Journalisation Voir Système de fichier.

K ≡

KAVICHS ou *KAVICHS KAVICHS ou Kavichi's Alternate Data Stream (ADS). Petit fichier de description associé à tout fichier par le logiciel anti-virus Kaspersky.

Keylogger Enregistreur de frappe. Ce type de logiciel permet d'enregistrer la frappe du clavier et, parfois, de réaliser des captures d'écran à intervalles réguliers, évidemment à l'insu de l'utilisateur. Ce type de logiciel espion vise principalement la récupération et la transmission (généralement par mail) des mots de passe et codes d'accès divers. Voir virus-espion.

Ko Unité de mesure usuelle en informatique. Un "Ko" est un kilo octets, soit 1 024 octets. Les constructeurs utilisent souvent des Ko de 1 000 octets (système normalisé), ce qui fait apparaître commercialement des tailles plus grandes, pour les disques par exemple.

L ≡

LBA Voir secteur.

LDN Last Dialed Numbers. Derniers numéros composés. Les 10 derniers numéros composés peuvent être enregistrés sur la carte SIM.

LOCI Location Information. La carte SIM enregistre la localisation du dernier relais sur lequel le téléphone s'est connecté.

Log Un "Journal de log" ou un "Log" retrace toutes les opérations d'un certain type effectuées sur une machine. Ces journaux enregistrent un nombre variable de paramètres et très souvent la date. Ils sont de qualité et d'intérêt variables selon les systèmes d'exploitation (souvent excellents sous Linux et décevants sous Windows). Ils peuvent être activés ou non par les opérateurs-système. Ils sont conservés pendant une durée variable. Ils sont généralement effacés par les auteurs d'intrusions réussies pour supprimer toute trace de ladite intrusion.

Logiciel Un logiciel est un ensemble d'instructions, de programmes et de données permettant de faire effectuer automatiquement des traitements par une machine. Un logiciel s'incarne dans des fichiers contenus dans un support d'information et il est accompagné d'une documentation.

Logiciel applicatif ou "application" Logiciel spécifique ou progiciel destiné à remplir une ou plusieurs fonctions à la demande d'un utilisateur humain avec lequel il communique dans un langage que ce dernier peut manipuler.

Logiciel spécifique ou "spécifique" Logiciel conçu pour répondre au besoin d'un client particulier (par opposition à un progiciel).

Login Nom d'utilisateur (ou identifiant) permettant de se connecter sur un système serveur, en réponse au message dit d'invite. La saisie du login est toujours suivie par celle d'un mot de passe. Le couple login - mot de passe identifie un compte utilisateur d'une machine serveur, généralement attribué par l'administrateur de cette machine, et en aucun cas à la personne physique qui utilise le login et le mot de passe. Seuls les systèmes faisant appel à des mesures biométriques (iris, empreintes digitales) identifient des personnes physiques.

M ≡

Macro-virus Tous les logiciels de bureautique offrent la possibilité d'écrire des macros instructions. Le but de ces dernières est de permettre à l'utilisateur d'automatiser facilement des séquences répétitives d'opérations : imprimer un original sur une imprimante et des copies sur une autre par exemple. Un virus macro (ou macro-virus) est un détournement nuisible de cette programmation. On les rencontre particulièrement dans les outils bureautiques Microsoft : Word, Excel, Powerpoint en particulier.

Malware En anglais, contraction de "malicious" et "software", que l'on peut traduire par "logiciel malveillant". Voir virus.

Master Boot Record Tout premier secteur adressable d'un disque. D'une taille de 512 octets, le Master Boot Record indique comment est partitionné le disque et quelle est la partition de boot. Voir aussi Volume Boot Record.

MBR Voir Master Boot Record.

MD5 (signature) Association d'un nombre de très grande taille à un fichier, une partition ou un disque, de telle sorte que le changement d'un seul bit du fichier ou du disque produise une signature totalement différente. Permet ainsi de signer de manière absolument certaine un objet informatique, signature qui constitue son empreinte numérique. Ce nombre est de taille 256¹⁶, soit environ 3,4 suivi de 38 nombres décimaux, toujours représenté en hexadécimal sous forme d'un nombre de 16 octets. Le calcul du MD5 a été éventé en 2005. En conséquence, le Lerti utilise SHA-1 (voir ce terme).

Mémoire flash Type de mémoire de masse à semi-conducteurs réinscriptibles – comparables sur ce point à la mémoire vive –, mais dont les données persistent lors de la mise hors tension, comme pour les disques durs. Inventées au cours des années 80, elles n'ont connu leur développement que bien plus tard. De très nombreux supports d'informations font aujourd'hui appel à

ce type de mémoire que l'on rencontre dans les téléphones portables, les appareils photographiques, les PDA, les clés USB, les GPS, les consoles de jeux, les systèmes embarqués et, depuis 2008, dans certains ordinateurs portables. La question se pose de savoir si ces mémoires remplaceront un jour les disques durs, en raison du nombre limité d'écritures qu'elles supportent, – au mieux un million à l'heure actuelle–. Ce sont des EEPROM dont il existe deux types : les mémoires NAND et NOR (voir ces termes).

MemoryStick (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

MemoryStick M2 (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

Meta-données Informations relatives aux données numériques (nom de fichier, nom de répertoire, date et heure de création, de modification ou d'édition d'un document, d'une photographie, d'un email ...). Les meta-données peuvent constituer des preuves numériques à forte valeur probante dans la mesure où elles ne sont généralement pas accessibles à l'utilisateur et ne sont pas toujours modifiées lors de la copie ou le déplacement de la donnée proprement dite.

MFT Master File Table. Fichier contenant la liste des fichiers d'un système NTFS avec leurs attributs. Les tous petits fichiers (700 à 800 octets) sont directement enregistrés dans la MFT. Sauf action volontaire d'effacement, la MFT garde la trace de tous les fichiers qui ont figuré sur la partition.

Micro SD (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

MIME Multipurpose Internet Mail Extensions. Standard Internet qui étend le format de données des courriels pour supporter des textes en différents codages de caractères autres que l'ASCII, des contenus non textuels, des contenus multiples, et des informations d'en-tête en d'autres codages que l'ASCII. Les courriels étant généralement envoyés via le protocole SMTP au format MIME, ces courriels sont souvent appelés courriels SMTP/MIME.

Mini SD (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

MMS Multimedia Messaging Service. Extension des SMS aux sons et aux images.

Mo Unité de mesure usuelle en informatique. Un "Mo" est un mega octets, soit 1 024 kilo octets ou encore 1 048 576 octets. Un "Mo" commercial ou normalisé représente un million d'octets.

MRU Most Recently Used. Liste des derniers fichiers ou objets utilisés. Sous Windows enregistrements de la base de registre par type de fichiers.

MSISDN Mobile Station International Subscriber Directory Number. Numéro de téléphone de l'utilisateur. Figure de manière optionnelle dans la carte SIM.

Multi Media Cards (MMC) (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

MVNO Mobile Virtual Network Operators. Opérateurs dépourvus d'infrastructures techniques de télécommunications, louant du temps de connexion en gros aux opérateurs hôtes pour le revendre au détail aux usagers. Sept en France lors de leur lancement en 2005, ils sont plusieurs dizaines à l'heure actuelle. Les MVNO gèrent la facturation et sont propriétaires des cartes SIM de leurs clients.

N ≡

NAND Type de mémoires flash permettant le stockage économique de grandes quantités d'informations avec un accès séquentiel. On les trouve dans de nombreux supports récents comme les cartes mémoires.

Navigateur Logiciel permettant d'interpréter les fichiers "Web" et d'envoyer des requêtes sur les sites. Les principaux navigateurs (Browsers en anglais) sont Internet Explorer, Firefox, Netscape, Mozilla et Opéra. Ces logiciels gardent dans des fichiers "caches" la trace des connexions réalisées à des fins techniques (pour accélérer les affichages ultérieurs) et non à des fins d'enquêtes judiciaires. Le plus utilisé, Internet Explorer, ne publie pas les règles de mise en cache. Si les connexions enregistrées peuvent être tenues pour certaines, rien n'indique que toutes les connexions soient enregistrées.

NOR Type de mémoires flash qui se caractérisent par un accès direct aux cellules individuelles permettant d'héberger des programmes exécutables. On les rencontre notamment dans les téléphones portables.

NTFS Système de fichiers utilisé par Windows NT et systèmes postérieurs (Windows 2000, Windows XP).

O ≡

Octet Unité de mesure informatique. Un octet est égal à 8 bits.

OLE "Object Linking and Embedding" soit litt. "objet lié et incorporé". Protocole mis au point par Microsoft permettant à des applications utilisant des formats différents de dialoguer entre-elles (un tableau de chiffres dans un traitement de texte peut être ainsi mis à jour dynamiquement par la feuille de calcul d'un tableur).

Opérateurs téléphoniques Société offrant les services du GSM et/ou de l'UMTS. Trois en France : Orange, SFR et Bouygues.

Ordinateur zombie Voir zombie

P ≡

P2P Voir Peer to Peer.

Pagefile.sys Nom donné dans les systèmes d'exploitation Windows au fichier de pagination, encore nommé fichier d'échange ou de swap (voir ce mot).

Partition Un disque dur est découpé en disques logiques qui apparaissent comme autant de volumes séparés. Sous Windows, ces volumes sont intitulés "C:", "D:", etc. jusqu'à "Z:". Ces mêmes désignations peuvent toutefois s'appliquer à des disques physiquement différents.

Peer to Peer Litt. "de pair à pair". Typologie de réseau dans lequel tous les postes connectés sont à la fois serveurs et clients, sans serveur ni administration centrale. Très utilisé pour les échanges de fichiers contrefaits (Films, logiciels, musique, livres, etc.). Les plus connus sont Kazaa, eMule, eDonkey. De nouvelles générations de logiciels peer to peer ont fait leur apparition en 2005 avec cryptage des échanges et masquage des adresses.

PIC Programmable Intelligent Computer ou Peripheral Interface Controller (contrôleur d'interface périphérique). Famille de microcontrôleurs de la société Microchip dérivés du PIC1650 et développés à l'origine par la division microélectronique de General Instruments. Un microcontrôleur est une unité de traitement de l'information de type microprocesseur à laquelle on a ajouté des périphériques internes permettant de réaliser des montages sans nécessiter l'ajout de composants externes. Les PIC intègrent mémoire de programme, mémoire de données, ports d'entrée-sortie, et même horloge. Certains modèles disposent de toute l'électronique nécessaire à la connexion sur port USB.

PIN Personal Identification Number. Code à quatre chiffres permettant l'accès à la SIM. Blocage après trois essais infructueux. Le déblocage de la carte SIM impose le recours au code PUK, que les opérateurs téléphoniques doivent communiquer quand ils en sont requis par ordonnance ou réquisition judiciaire.

Piste Un disque est découpé en pistes circulaires qui délimitent des portions adressables de chaque secteur angulaire logiquement mis en place lors du formatage du disque. Les disques actuels sont généralement découpés en plusieurs milliers de pistes.

Pixel Un pixel est le point élémentaire d'affichage sur un écran.

PLMN Public Land Mobile Network. Réseau GSM dans un territoire donné.

Plug-in Extension qui complète un logiciel hôte pour lui conférer des fonctionnalités nouvelles ou pour l'adapter à un environnement particulier. Le nom provient de la métaphore de la prise électrique : comme elle, un *plug-in* se branche sur un logiciel principal. Le *plug-in* est souvent réalisé par des informaticiens sans relation avec les auteurs du logiciel principal. Un *plug-in* ne peut fonctionner seul.

Porte dérobée Backdoor en anglais. Moyen non documenté d'accès à un dispositif informatique ou implémenté par un programme malicieux (Cheval de Troie par exemple). Peut avoir été mis en place par le constructeur afin de se réserver un moyen d'action. Généralement destiné à l'espionnage d'une machine ou à son détournement pour des fins illicites : envoi massif de mails, organisation d'un denial of service par exemple.

Preuve numérique Toute information numérique pouvant être utilisée comme preuve dans une affaire de type judiciaire. La collecte de l'information numérique peut provenir de l'exploitation de supports d'information, de l'enregistrement et de l'analyse de trafic de réseaux (informatiques, téléphoniques ...) ou de l'examen de copies numériques (copies-image, copies de fichiers ...). Les copies-écran d'informations numériques ne sont pas des preuves numériques au sens de la présente définition, mais elles peuvent servir de point de départ pour la recherche ultérieure de preuves numériques. (Angl. : Digital Evidence).

Progiciel Logiciel conçu pour répondre au besoin d'un marché (par opposition à un logiciel spécifique).

Pthc Pre-teen hard core. Abréviation utilisée pour désigner les fichiers pédopornographiques où sont représentés des pré adolescents dans des situations pornographiques manifestes. Voir les entrées Ptsc, Yo.

Ptsc Pre-teen soft core. Abréviation utilisée pour désigner les fichiers pédo-pornographiques où sont représentés des pré adolescents dans des situations érotiques. Voir les entrées Pthc, Yo

PUK Personal Identification Number Unblocking Key. Code à huit chiffres qui permet le déblocage d'une carte SIM après blocage de l'accès par PIN. Numéro obtenu auprès de l'opérateur, avec l'ICCID de la carte SIM, sur réquisition ou ordonnance.

Q =

Queue de cluster Un fichier n'occupe généralement pas l'intégralité d'un cluster. La place qui reste entre la fin du fichier et la fin du cluster constitue la queue de cluster. Cet emplacement peut contenir de l'information provenant d'un précédent fichier ou de la mémoire vive. Les outils appropriés permettent de lire les queues de clusters, où peuvent se trouver des informations très anciennes.

R =

Raid Redundant Array of Inexpensive Disk ou Grappe redondante de disques durs bon marché. Ensemble de techniques permettant de répartir les données sur plusieurs disques durs afin de se prémunir de la défaillance de l'un d'eux, d'améliorer les performances d'un ensemble ou de combiner ces avantages. Les principales techniques sont le Raid 0 (agrégation par bandes de plusieurs disques pour améliorer les temps d'accès), le Raid 1 (mise en miroir de deux disques) et Raid 5 (agrégation par bandes d'au moins trois disques, avec redondance et parité répartie).

Rapport de garde Rapport ou procès-verbal établi lors de la saisie ou de la réception d'une information numérique et de son support, comportant toute information sur le détenteur antérieur (propriétaire, usager, gardien), les lieux et conditions d'acquisition (saisie, transmission), la nature du support d'information (description physique avec photographie, numéro de série), la description éventuelle de l'information numérique (méta-données, structure des données, empreinte numérique), la situation d'accès aux données (accessibles ou non), la présence de sceau (avec identification), le libellé de l'étiquette d'accompagnement, les dates d'ouverture et de fermeture du support, la mention des modifications éventuelles (suppression de mot de passe) et l'état de restitution du support (scellé, accessibilité aux données, étiquette) avec photographie. Beaucoup de progrès restent à faire en France à ce sujet où le terme même de "rapport de garde" est quasiment inconnu. (Angl. approché : Chain of Custody).

Rapport d'investigation Enregistrement des étapes d'une investigation numérique permettant de garantir qu'une preuve numérique est issue de manière irrévocable d'une information numérique. Ce rapport décrit comment l'information numérique originale a été préservée, donne son empreinte numérique, décrit les moyens logiciels et matériels de blocage en écriture utilisés, décrit les opérations réalisées et les logiciels mis en œuvre, expose les éventuels incidents rencontrés et notamment les modifications de l'information numérique analysée, énonce les preuves réunies et donne les numéros de série des supports d'information utilisés pour leur enregistrement. Ce rapport est un rapport judiciaire si et seulement s'il est produit à la demande d'une institution de type judiciaire et s'il est associé à un rapport de garde. (Angl. approché : Chain of Evidence).

Recherche sur disque La recherche est effectuée sur l'intégralité du disque, c'est-à-dire à la fois sur les fichiers et sur les secteurs non alloués et sur les queues de clusters. Cette recherche permet de retrouver des informations que l'utilisateur a cru effacer, si elles n'ont pas été recouvertes par de nouvelles depuis l'effacement.

Recherche sur fichiers La recherche s'effectue sur les fichiers existants, tels qu'ils peuvent apparaître dans l'explorateur de Windows par exemple.

Répertoire Regroupement de fichiers ou de sous-répertoires sous un même intitulé.

Requête Interrogation élémentaire d'une base de données ou d'un serveur web. Une requête retourne une réponse qui peut être une donnée ou un objet quelconque (image, texte, sons, autre).

Reset Terme anglais que l'on peut traduire par "remise à zéro", "redémarrage" ou encore "réinitialisation". Opération effectuée en général à la suite du blocage d'un système informatique sans autre issue. Peut, dans certains cas, être le moyen d'obtenir une réponse d'identification d'un système informatique, comme pour les cartes à puces.

Roaming Possibilité de passer d'un point d'accès à un autre entre opérateurs différents, sans interruption de communication, en France ou à l'étranger.

S =

Salvage Voir Carving.

Samba Le logiciel Samba permet de "voir" une partition montée sur une machine Linux depuis un explorateur Windows comme s'il s'agissait d'une partition Windows, sur laquelle toutes les opérations habituelles peuvent être effectuées (si elles sont autorisées) : copier, détruire, écrire et renommer des fichiers et des répertoires.

SATA Le bus Serial ATA (S-ATA ou SATA) est un bus série permettant la connexion de périphériques de stockage haut débit sur les ordinateurs. Le standard Serial ATA est apparu en février 2003 afin de pallier les limitations de la norme ATA (plus connue sous le nom "IDE" et appelée rétroactivement Parallel ATA), qui utilise un mode de transmission en parallèle.

SCSI Small Computer Serial Interface. Interface permettant la connexion de plusieurs périphériques de types différents sur un ordinateur par l'intermédiaire d'une carte, appelée contrôleur SCSI. Concerne notamment les disques durs utilisés sur les serveurs. En déclin rapide avec le développement du bus SATA.

Secteur de boot Tout premier secteur d'un disque, en anglais "Master boot record", composé des 512 premiers octets de tout disque. Donne la table de partition du disque et indique quelle est la partition de boot active.

Secteur non alloué Un secteur non alloué est un secteur du disque disponible pour recevoir un fichier ou une partie de fichier. Ce secteur peut avoir contenu des informations qu'il conserve jusqu'à recouvrement par un nouveau fichier. Tant qu'il n'est pas alloué à nouveau, les informations contenues dans ce secteur peuvent être lues par des outils appropriés.

Secteur Un disque est découpé en secteurs angulaires qui délimitent des portions adressables de chaque piste circulaire logiquement mise en place lors du formatage du disque. Les secteurs des premiers disques étaient repérés par un numéro de cylindre, de tête et de secteur par piste. Le mode d'adressage actuel est l'adressage LBA (Logical Block Addressing). Ce mode repose sur un numéro unique qui identifie un secteur donné.

Secure Digital (SD) (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

Secure Digital High Capacity (SDHC) (CF) Carte mémoire de haute capacité de type flash (voir l'article Carte mémoire).

SHA-1 (signature) Association d'un nombre de très grande taille à un fichier, une partition ou un disque, de telle sorte que le changement d'un seul bit du fichier ou du disque produise une valeur totalement différente. Cette valeur constitue l'empreinte numérique de l'objet ainsi signé. Permet de signer de manière absolument certaine un objet informatique. Dans la version SHA-1, ce nombre est de taille 256*20, soit environ 1,4 suivi de 48 nombres décimaux, toujours représenté en hexadécimal sous forme d'un nombre de 20 octets. Les versions ultérieures de SHA-1 sont déjà définies : SHA-256 ou SHA-512 par exemple.

Signature MD5, SHA-1 Voir MD5, SHA-1.

Signet Voir Bookmark.

SIM Subscriber Identity Module. Carte délivrée par un opérateur téléphonique et destinée à être insérée dans un GSM. Le GSM et la carte SIM constituent deux entités indépendantes disposant d'informations qui leur sont propres. Voir USIM.

Slack Espace compris entre la fin logique d'un fichier et la fin d'un secteur physique du disque, dans lequel on trouve des résidus d'anciens fichiers ou de la mémoire vive. Voir l'article queue de cluster.

SMART Self-Monitoring, Analysis and Reporting Technology. Technologie d'analyse prédictive de panne de disques durs, mise en place par IBM en 1992. Cette technologie a été implémentée dans la quasi-totalité des disques IDE et SCSI à partir de 1995. Elle a été étendue ensuite aux disques SATA. SMART enregistre la "vie" du disque : nombre d'heures de fonctionnement, nombre de mises en marche, fréquence des incidents, température de fonctionnement ... Ces informations ne peuvent pas être modifiées par l'utilisateur. Les informations SMART sont totalement indépendantes des données utilisateur. Elles peuvent s'avérer précieuses pour l'investigation. Malheureusement, faute d'une normalisation, chaque constructeur donne des informations différentes, ce qui peut être source d'erreurs et de confusions (ainsi, le "Power On Hours" est exprimé en ... secondes, minutes ou heures selon les disques). La fiabilité des informations SMART est donc sujette à caution.

SmartMedia cards (SM) (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

SMS Short Message Service. La carte SIM enregistre les 20 derniers SMS reçus. Les SMS "effacés" de la carte SIM par l'utilisateur peuvent être retrouvés tant qu'ils n'ont pas été recouverts par de nouveaux messages. Dans les téléphones récents, les SMS sont généralement enregistrés en très

grand nombre dans le téléphone. La possibilité de récupérer les messages effacés dépend beaucoup du modèle de téléphone.

SMTP Simple Mail Transfer Protocol. Litt. "Protocole simple de transfert de courrier". L'un des plus anciens protocoles de l'Internet, peu modifié depuis son origine. Ce protocole de communication est utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique. Très largement répandu dans tout l'Internet. Voir l'article MIME.

Solid State Drive (SSD) (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

Spam Courriel envoyé massivement à des destinataires qui ne l'ont pas demandé. C'est par l'envoi de fichiers attachés à des spams que sont propagés de nombreux malwares.

SPN Service Provider Name. Nom de fournisseur de service. Peut être affiché sur l'écran du téléphone.

Spyware Voir virus-espion.

SQL Structured Query Language ou langage structuré de requêtes. Langage (ou pseudo-langage) informatique standard et normalisé permettant d'interroger et de modifier pratiquement toute base de données relationnelle. Devenu quasiment universel aujourd'hui.

SSH Secure Shell. Protocole de communication sécurisé par une authentification des usagers et des transferts de fichiers cryptés.

Support d'information Tout dispositif permettant la transmission ou l'enregistrement de l'information numérique comprenant notamment les disques durs, les disques amovibles, les assistants personnels (PDA), les clés USB, les téléphones portables et leurs cartes SIM, les mémoires flash (appareils photographiques notamment), les routeurs, serveurs, dispositifs embarqués ("boîtes noires") et autres appareils pour les réseaux, les cartes à puce ou à pistes (bancaires ou non). (Angl. : Data Carrier).

Swap Littéralement "échange". Système d'échange entre la mémoire vive et une partition ou un fichier – dits de swap – sur le disque dur afin de disposer d'une copie de la mémoire sur disque, y compris de parties qui, excédant la capacité de la mémoire, sont mises en attente sur le disque. Précieux recueil d'information pour l'investigation numérique car le fichier de swap peut comprendre des informations autrement inaccessibles (mots de passe en clair par exemple).

System Volume Information Apparue avec Windows 95 la "base de registres" ("registry" en anglais) concentre de nombreuses informations techniques et notamment les configurations de démarrage ou encore la trace des dispositifs qui ont été connectés à un ordinateur, avec leur description assez précise (disque dur externe avec marque et modèle par exemple). Cette base de registres figure dans le répertoire "System Volume Information" avec plusieurs milliers d'autres fichiers installés par divers logiciels. Seul l'intitulé du répertoire est visible de l'utilisateur. Ni son contenu ni son accès ne lui sont accessibles.

Système de fichiers Désigne la manière d'organiser les données sur un disque dur. Les principaux systèmes de fichiers sont FAT, FAT32, NTFS sous Windows, EXT2 et EXT3 sous Linux. Un système de fichier contient une table d'allocation décrivant l'ensemble des fichiers contenu dans une partition, avec divers attributs, qui varient selon les différents systèmes de fichiers. Ces attributs comprennent toujours au moins diverses dates, auxquelles s'ajoutent des attributs relatifs à la nature du fichier et à son propriétaire. Les systèmes de fichiers les plus évolués (NTFS, EXT3) sont journalisés, c'est-à-dire qu'ils enregistrent toutes les opérations effectuées sur tous les fichiers. Justifiée par des raisons techniques, la journalisation est d'une aide précieuse en matière d'investigation informatique légale.

Système d'exploitation Operating System (OS) en anglais. Le système d'exploitation d'un ordinateur, – mais aussi de tout autre appareil informatique comportant un processeur (téléphone, GPS) – est un ensemble de programmes permettant la mise en œuvre du matériel. Il constitue une couche intermédiaire entre les composants matériels et les logiciels applicatifs. Il permet aussi aux utilisateurs humains – avec des degrés différents de complexité, du mode "ligne de commande", réservé aux informaticiens, au mode graphique, universel – de manipuler des données. De très nombreux systèmes d'exploitation ont vu le jour, depuis ceux des grandes machines des débuts de l'informatique à ceux des téléphones portables d'aujourd'hui. Pour les ordinateurs de bureaux ou serveurs actuels, les principaux systèmes d'exploitation sont les systèmes Windows et Linux.

T ≡

Tchat De l'anglais "to chat", litt. "bavarder", trad. fr de l'argot "tchatcher". Désigne les systèmes permettant de discuter en temps réel avec une ou plusieurs personnes sur un réseau comme l'Internet. Le tchat peut se pratiquer à partir d'un protocole qui lui est consacré (IRC ou Internet Relay

Chat) au sein de "chat rooms" qui mettent en relation plusieurs personnes simultanément ou par des messageries instantanées comme MSN qui mettent en relation deux personnes, avec possibilité d'extension à d'autres. Les intervenants se présentent généralement masqués par des pseudonymes ou des avatars.

Temps réel Un système informatique fonctionnant en temps réel est conçu de telle manière que toute donnée nouvelle est immédiatement prise en compte et traitée de sorte que les états de sortie du système intègrent cette donnée nouvelle. Pendant un temps confinés à la conduite des processus industriels, les systèmes temps réels sont aujourd'hui très largement répandus (réservation trains, avions, etc.). Cependant les impératifs de temps de réponse sont très différents selon les domaines concernés, pouvant aller de la microseconde à plus d'une heure.

Thumb Litt "pouce", en français "vignette" ou "miniature". Désigne une image de petit format permettant d'afficher rapidement une représentation d'une image de grande taille.

Thumbcache_xxx.db Base de donnée jouant le même rôle que les fichiers Thumbs.db (voir ce terme) mais pour les systèmes d'exploitation Windows Vista et Seven. Cette base se décline sous quatre formats ou xxx prend les valeurs 32, 96, 256 et 1024. Ces valeurs varient en fonction de la taille des vignettes générées. A la différence des fichiers Thumbs.db, la base de donnée est centralisée.

Thumbs.db Base de données des images, vidéos et divers fichiers présents dans un répertoire, propre aux systèmes d'exploitation Microsoft depuis Windows XP. Cette base de données comprend une "miniature" des images ou des vidéos et plusieurs meta-données (nom et datation des fichiers d'images notamment). Le fait de supprimer les images ou vidéos proprement dites ne supprime pas le fichier "Thumbs.db" ni n'en retire les vignettes associées. Si l'utilisateur ne régénère pas la base de données par demande d'affichage en mode "miniature" il est possible de savoir quelles images figuraient dans un répertoire donné avant suppression. Le fichier "thumbs.db" est considéré comme un fichier système et à ce titre est caché de l'utilisateur.

TLD ou gTLD Top Level Domain ou General Top Level Domain. Partie la plus à droite d'un nom de domaine. Désigne le sommet de la hiérarchie des noms de domaine. Par exemple dans www.societe.com, ".com" constitue le TLD. On distingue les TLD mondiaux, attribués par les divers "Registres" agréés par l'ICANN (Internet Corporation for Assigned Names and Numbers) et les ccTLD qui correspondent aux différents pays du monde (fr pour la France).

Traces Informations retrouvées sur un support informatique et en particulier sur un disque dur, y compris dans les secteurs non alloués ou dans les queues de clusters. Ces traces se présentent le plus souvent sous forme de bribes. Quand elles concernent des images, il est parfois possible d'en reconstituer une partie.

Trojan horse Voir Cheval de Troie.

U ≡

UMTS Universal Mobile Telecommunication System. Successeur du GSM, dit aussi téléphone de 3^e génération (3G).

Unicode Norme informatique, développée par le Consortium Unicode, qui vise à donner à tout caractère de n'importe quel système d'écriture de n'importe quelle langue un nom et un identifiant numérique, et ce de manière unifiée, quelle que soit la plate-forme informatique ou le logiciel. Ce codage vise à se substituer à tous les codes existants et d'en finir avec les problèmes liés au transcodage. Le prix à payer est une dimension du code beaucoup plus importante, qui demande jusqu'à 4 octets pour un caractère dans la variante UTF-32.

URL Uniform Resource Locator. Format universel de nommage permettant de désigner toute ressource disponible par l'Internet. Ce format comprend au moins le nom du protocole (HTTP, FTP, mailto par exemple), l'adresse du serveur (généralement désigné par un nom de domaine) et le chemin d'accès à la ressource. Il peut comprendre d'autres informations comme le numéro de port.

USIM Universal Subscriber Identity Module. Equivalent de la SIM pour l'UMTS. La carte USIM comprend les mêmes fonctionnalités que la carte SIM avec des capacités augmentées et une meilleure authentification.

UTC Coordinated Universal Time ou Temps Universel Coordonné. Succède au temps GMT (Greenwich Mean Time) comme référence mondiale depuis les années quatre-vingt, en raison de l'imprécision – limitée à quelques millisecondes – de la durée de rotation de la terre. L'heure de n'importe quel fuseau horaire s'exprime avec un décalage positif ou négatif par rapport à l'heure UTC. Cette dernière doit cependant être examinée avec soin en raison du décalage introduit dans certains pays par la saison (été ou hiver).

V ≡

Valeur de hachage Voir empreinte numérique.

VBR Voir Volume Boot Record.

Vers Type de virus qui se copie d'ordinateur en ordinateur pour y effectuer une action malicieuse, généralement recueillir des mots de passe ou d'autres informations confidentielles et les renvoyer à une adresse donnée.

Virtualisation Ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner sur une même machine plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes. Les outils de virtualisation servent à faire fonctionner des "serveurs privés virtuels" ou encore des "environnements virtuels". On peut ainsi faire exécuter des programmes conçus pour fonctionner sous Linux sur un ordinateur fonctionnant sous Windows, ou le contraire. Le plus célèbre outil de virtualisation est actuellement VMWare.

Virus du MBR Virus modifiant le master boot record, par exemple pour empêcher l'ordinateur de charger le système d'exploitation.

Virus furtif Virus ayant la propriété de se cacher lorsque l'ordinateur ou l'utilisateur accède au fichier infecté. Si l'on tente de savoir si le fichier est infecté, le virus le saura et offrira à l'antivirus et à l'utilisateur une version non infectée du fichier.

Virus polymorphe Un virus polymorphe inclut des instructions permettant de rendre chaque infection différente de la précédente. Ce changement constant rend la détection de ce type de virus compliqué. Le code change afin de tromper l'antivirus, qui recherche une signature précise. Beaucoup de virus polymorphes sont aussi encryptés. Le virus encryptera son code et ne le décryptera que lorsqu'il doit infecter un nouveau fichier, le rendant encore plus difficile à détecter.

Virus Un virus est un bout de programme informatique conçu pour se reproduire par lui-même et destiné à porter atteinte ou à espionner un système informatique. Un virus s'intègre en général à un programme exécutable à l'insu de l'utilisateur. On distingue plusieurs familles de virus ou de programmes ayant des effets similaires. Nous pouvons distinguer les vers, les virus de la zone d'amorce (ou MBR), les macro-virus, les virus polymorphes, les virus furtifs, les virus espions. Proches des virus, les chevaux de Troie ne présentent pas la possibilité de s'auto reproduire. Ils faut distinguer tous ces virus des faux-virus ou "hoax", mais qui sont tels qu'ils deviennent – du fait du comportement des usagers – de "vrais" virus. Le terme de "malware" tend à regrouper aujourd'hui l'ensemble des logiciels et programmes malveillants. Voir tous ces termes.

Virus-espion Virus destinés à recueillir des informations, généralement – mais non exclusivement – lors de la frappe de données (keyloggers) comme par exemple les mots de passe, les mots-clés soumis aux moteurs de recherche, achats en ligne (numéro de carte bancaire). Angl. Spyware.

Volume Boot Record Tout premier secteur adressable d'une partition. D'une taille de 512 octets, le Volume Boot Record contient toutes les informations propres à la partition. Si la partition est bootable, donne toutes les informations pour ce faire.

W ≡

WAP Wireless Application Protocol.

Warez Issu du suffixe "ware" de software, freeware ou shareware, le warez désigne l'ensemble des logiciels habituellement payants qui sont rendus disponibles en version complète par piratage. Le "z" vient de la terminaison originale "wares" ("wairz" en anglais). Ces warez circulent sur Internet via les réseaux peer-to-peer, les FTPs ou les newsgroups.

Webmail Logiciel de messagerie déporté chez un hébergeur fournissant ce service, accessible par l'intermédiaire d'une interface Web. De ce fait, les messages émis ou reçus sont stockés sur les machines de l'hébergeur et non sur celle de l'utilisateur. Des traces des messages lus ou composés depuis la machine de l'utilisateur peuvent parfois être retrouvées, mais à l'état de bribes plus difficilement exploitables que les mails provenant de messageries résidentes.

X Y Z ≡

xD cards (CF) Carte mémoire de type flash (voir l'article Carte mémoire).

Yo Years old. Désigne l'âge des enfants figurant sur les photographies ou films pédo-pornographiques, 9 Yo pour 9 ans par exemple.

Zombie Ordinateur dont un pirate a pris le contrôle pour l'utiliser le moment venu dans le cadre d'une attaque de type DoS ou d'un botnet. Voir ce terme.

Zone Identifier Le Service Pack 2 pour XP introduit une nouvelle fonctionnalité de sécurité, le "Zone Identifier", qui associe une "zone de sécurité" à certains fichiers. Lors de l'ouverture des fichiers marqués en "zone sensible", une alerte est adressée à l'utilisateur.