Note d'information 04

Terminologie

Version	Date	Auteur	Statut
1.20	25/09/2007	PV	Adopté

Destinataires

- Tous publics

Préambule

La présente note d'information vise à fixer la terminologie et à préciser le sens des concepts de l'informatique légale (ou investigation numérique légale)*, branche de l'informatique destinée à répondre aux besoins de la Justice. Cette terminologie s'inspire des travaux de* l'Anti-Cartel Enforcement Manuel, Chapter 3 : Digital Evidence Gathering, April 2006, *avec lesquels elle est en parfaite cohérence. Il s'agit toutefois d'une adaptation à la situation française et non d'une traduction.*

Informatique légale (ou investigation numérique 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. *(Angl. approché : Forensics)*

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)*

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)*

Preuve numérique

Toute *information numérique* pouvant être utilisée comme preuve dans une affaire de type judicaire. 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 (informatique, téléphoniques …) ou de l'examen de copies numériques (*copies-images*, 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)*

Support d'information

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

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)*

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. *(Angl. approché : Chain of Custody)*

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 – doit être tel qu'il soit impossible (en pratique) de changer *l'information numérique* sans 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)*

Copie-image

Copie bit à bit intégrale de *l'information numérique* présente sur un *support d'information*, y compris espaces non utilisés, espaces non alloués et queues de clusters, effectuée à l'aide d'un logiciel spécifique. 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)*

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 cette *information numérique* originale n'a pas été modifiée par l'opération de copie.