© Institut médico-légal des Pays-Bas.

2. LES TÉLÉPHONES PORTABLES sont placés dans une cage de Faraday, qui les isole des signaux radio. On minimise ainsi les risques de changement à distance de la mémoire. Celle-ci peut par exemple s'effacer automatiquement après réception d'un texto particulier. En temps normal, la boîte est fermée et l'analyste manipule le téléphone grâce à la caméra interne.

et sauvegardaient tout ce qui se trouvait entre un en-tête et un pied de fichier. Les dispositifs modernes peuvent valider les données qu'ils extraient (par exemple en s'assurant que les octets compris entre un en-tête et un pied caractéristiques d'un fichier JPEG correspondent bien à une photo numérique) et même réassembler les fichiers fragmentés en de multiples morceaux. Ce réassemblage est un défi en raison du nombre de combinaisons de fragments possibles. Il se complique encore quand certains fragments manquent, en particulier quand les données sont compressées.

La compression, très utilisée en informatique, permet d'économiser de la place. L'idée est d'exploiter les redondances : ainsi, quand on compresse la séquence de caractères « tendre tendreté », l'ordinateur remplace la chaîne « tendre » qui apparaît dans « tendreté » par un pointeur vers la première occurrence de cette chaîne. Un texte en anglais se compresse typiquement jusqu'à un sixième de sa taille d'origine.

Un fichier de texte doit être compressé par des algorithmes dits sans perte, qui autorisent une restauration fidèle de l'original quand les données sont décompressées. En revanche, les photographies et les vidéos sont en général compressées par des algorithmes avec perte, qui exploitent les défauts du système de perception humain. Par exemple, quelques dizaines de pixels de couleurs légèrement différentes peuvent être remplacés par un rectangle uniforme. Les économies ainsi réalisées sont énormes. Sans compression, une heure de vidéo plein écran peut occuper 99 gigaoctets, tandis que la même vidéo compressée ne prend plus que 500 mégaoctets, soit environ 200 fois moins.

Il est difficile de récupérer les données quand le fichier compressé est corrompu ou partiellement manquant. Il y a cinq ans, on échouait souvent à reconstituer le moindre élément utile, mais depuis, des progrès notables ont été accomplis.

> La mémoire vive est difficile à analyser car elle change vite, de l'ordre de plusieurs milliards de fois par seconde, et s'efface quand on éteint l'ordinateur.

En 2009, Husrev Sencar, de l'Université TOBB d'économie et de technologie, en Turquie, et Nasir Memon, de l'Institut polytechnique de l'Université de New York, ont développé une technique pour afficher un fragment de photographie au format JPEG même si le début et la fin du fichier sont manquants. En 2011, Ralf Brown, de l'Université Carnegie Mellon, aux États-Unis, s'est intéressé aux fragments de fichiers de texte compressés avec les algorithmes ZIP ou DEFLATE ; il a élaboré une méthode pour les récupérer même quand des informations critiques pour le réassemblage manquent. Cette méthode consiste à balayer les nombreuses façons différentes dont un document peut être décompressé, puis à choisir le résultat le plus probable en fonction de la langue dans laquelle on suppose que le document a été écrit.

La mémoire vive pose des problèmes spécifiques. Elle est difficile à analyser, car son contenu change vite – de l'ordre de plusieurs milliards de fois par seconde – et s'efface quand on éteint l'ordinateur. En outre, la façon dont les programmes stockent l'information dans cette mémoire est rarement fournie par leurs concepteurs et change d'une version à l'autre d'un même programme. Par conséquent, les informaticiens judiciaires doivent décortiquer chaque version pour découvrir son fonctionnement. Ainsi, l'analyse est longue, difficile et incomplète.

Au cours des dernières années, des techniques dites d'analyse syntaxique ou de parsage ont été développées pour étudier la mémoire vive. On dispose aujourd'hui d'outils capables d'indiquer la liste des processus en cours, le contenu du presse-papier ou l'image visible à l'écran de l'ordinateur au moment où cette mémoire a été enregistrée. Outre leur intérêt pour les enquêtes, ces outils servent beaucoup à l'analyse des logiciels malveillants, tels les virus et vers informatiques, ainsi que les actions d'un pirate lors d'une intrusion informatique.

Quand on récupère des photographies ou des vidéos, la question de leur authenticité se pose : ont-elles été retouchées ? De telles pratiques avaient cours bien avant l'arrivée du logiciel *Photoshop*. Par exemple, après son élimination lors d'une purge stalinienne dans les années 1930, Avel Enoukidzé, l'un des principaux dirigeants soviétiques, a été méticuleusement supprimé des photographies officielles par une série d'habiles manipulations des négatifs.

Aujourd'hui, les ordinateurs autorisent des trucages d'une qualité sans précédent et l'élaboration de scènes virtuelles impossibles à distinguer d'enregistrements réels au premier coup d'œil. Néanmoins, grâce aux progrès du traitement d'images, on peut détecter certains artefacts qui indiquent des manipulations. L'examen des reflets lumineux et des ombres révèle parfois qu'une photographie est en fait un assemblage d'images prises dans des environnements physiques légèrement différents. En 2009,