l'informaticien Hany Farid, du Darmouth College, aux États-Unis, a ainsi montré qu'une photo de groupe avait été créée en rassemblant des personnes de différentes photos : le reflet de l'éclairage dans les yeux des participants ne concordait pas avec leur position dans la scène.

À la pointe de la recherche en informatique judiciaire, des systèmes automatiques visent à assister l'enquêteur dans son raisonnement, en détectant des éléments qui sortent de l'ordinaire, qui sont étranges ou incohérents. De tels éléments peuvent être la trace d'événements intéressants pour l'enquête ou révéler que les preuves ont été falsifiées. À terme, ces systèmes de raisonnement automatique seront probablement la seule façon pour les enquêteurs de faire face aux données de plus en plus nombreuses et diverses. Cependant, les techniques ne progressent que lentement. Des systèmes détectant des incohérences d'horodatage ont par exemple été élaborés (un fichier ne peut pas être supprimé avant d'avoir été créé), mais leur application est compliquée par de multiples paramètres (tel le passage à l'heure d'été ou d'hiver).

Des mémoires qui augmentent plus vite que la vitesse de calcul

L'informatique judiciaire est confrontée à de grands défis, qui risquent de s'accroître dans les années à venir. Les ordinateurs d'aujourd'hui ont en moyenne 1 000 fois plus de mémoire que ceux du début des années 1990, mais ils ne sont que 100 fois plus rapides ; il y a donc moins de puissance de calcul disponible pour traiter chaque octet de mémoire. En outre, le nombre de cas nécessitant la collecte d'éléments numériques augmente bien plus vite que le nombre d'enquêteurs capables de les examiner. Et les indices numériques sont maintenant utilisés par les enquêteurs pour élucider des crimes, tandis que par le passé, ils servaient surtout lors du procès.

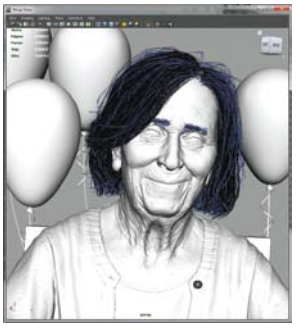
Autre difficulté, les téléphones portables peuvent être équipés de programmes d'autodestruction qui effacent leurs données quand ils reçoivent un texto particulier. Pour parer à cette éventualité, on les stocke dans une boîte métallique nommée cage de Faraday, qui bloque les ondes radio. La mémoire de nombreux téléphones portables s'effaçant si on les laisse éteints trop longtemps, les cages de Faraday doivent être équipées de prises électriques et de chargeurs. Elles ne suffisent pas toujours : sur certains téléphones, des appels automatiques au domicile sont programmés et les données s'effacent quand ils n'aboutissent pas ; sur d'autres, des algorithmes de cryptage trop puissants pour être déchiffrés par la police scientifique sont utilisés.

Le travail des enquêteurs est encore compliqué par l'émergence des techniques de stockage de données sur Internet. Le téléphone peut ne contenir aucune donnée du suspect et n'être qu'un outil pour accéder à un serveur. L'expert qui analyse l'appareil n'est pas nécessairement autorisé à utiliser les informations qu'il trouve pour accéder aux données stockées à distance. Pire, ces données ont parfois été effacées après la saisie par un collaborateur du suspect.

Outre ces questions techniques, le plus grand défi auquel est confrontée l'informatique judiciaire aujourd'hui est le manque d'experts qualifiés. Leur recrutement est bien plus compliqué que dans d'autres domaines, car ils doivent avoir une vaste connaissance des systèmes informatiques, des programmes et des formats de données, présents comme passés. En d'autres termes, ils doivent être généralistes dans une société qui privilégie de plus en plus la spécialisation.

Une approche intéressante consiste à appliquer les outils de l'informatique judiciaire à d'autres domaines, afin de stimuler la recherche et d'élargir la base des utilisateurs. Ils sont déjà utilisés par les professionnels de la sécurité, qui s'en servent pour analyser les intrusions dans les réseaux et bloquer les accès exploités par les pirates, ou par les entreprises de récupération de données, qui reconstituent des fichiers endommagés ou supprimés par erreur. D'autres applications sont possibles, consistant par exemple à vérifier qu'on n'a pas laissé involontairement des informations professionnelles ou personnelles sur un système informatique.

Quoi qu'il en soit, les spécialistes de l'informatique judiciaire seront confrontés à des volumes de données et une complexité des systèmes toujours plus grands. Les détectives numériques sont engagés dans une course aux armements non seulement avec les criminels, mais aussi avec les développeurs des systèmes informatiques. ■



© Dan Roarty/ www.danroarty.com

3. LES IMAGES DE SYNTHÈSE et les retouches numériques de photographies sont devenues si réalistes que des techniques élaborées sont nécessaires pour les reconnaître. Le personnage ci-dessus est factice *(en haut, une étape préliminaire de son élaboration)*.

BIBLIOGRAPHIE

R. Brown, **Reconstructing corrupt DEFLATEd files,** *Digital Investigation*, vol. 8, pp. S125-S131, 2011.

S. Garfinkel, **Every last byte,** *Journal of Digital Forensics, Security and Law*, vol. 6, pp. 7-8, 2011.

R. Walls *et al.*, **Effective digital forensics research is investigator-centric,** *Proceedings of the Sixth USENIX Workshop on Hot Topics in Security*, pp. 1-7, 2011.

S. Garfinkel *et al.*, **Using purpose-built functions and block hashes to enable small block and subfile forensics,** *Digital Investigation*, vol. 7, pp. S13-S23, 2010.