AHA – La forensique numérique

En forensique numérique, comme son nom l'indique, des traces et des preuves numériques sont collectées et analysées pour comprendre un délit. En théorie, tout acte délictuel peut laisser des traces numériques. Le cambrioleur a-t-il utilisé son smartphone pour rechercher sa destination sur Google Maps? L'assassin a-t-il menacé sa victime au préalable par e-mail? Le délit a-t-il été commis en ligne, p. ex. dans le cas d'une fraude financière? Les messages envoyés et reçus sont sauvegardés sur des clouds, les photos téléchargées peuvent contenir des données de localisation si le GPS a été activé et le trajet d'un smartphone peut être retracé à l'aide des cellules radio contactées.

Pour que les preuves numériques soient valables devant un tribunal, le processus de conservation et d'analyse des preuves doit être entièrement documenté de la même façon que dans les autres domaines de la criminalistique.

Comment procéder?

Sécuriser les appareils: Sur la scène de crime, tous les appareils numériques tels que les disques durs, les memory sticks USB, les téléphones mobiles, les scanners, les caméras de surveillance etc., sont sécurisés et, si possible, les mots de passe des personnes impliquées sont récupérés. Contrairement à ce que l'on voit souvent au cinéma, le craquage des mots de passe peut s'avérer laborieux.

Les téléphones mobiles sont directement éteints, placés dans un sac Faraday ou réglés sur le mode avion afin d'éviter toute connexion avec le réseau qui permettrait de modifier les données existantes. Les écrans d'ordinateurs sont photographiés afin de sauvegarder l'état actuel. Une décision importante doit alors être prise sans tarder: faut-il laisser l'ordinateur allumé ou l'éteindre? Le laisser allumé permet de suivre les activités criminelles en cours et de ne pas compromettre l'accès ultérieur aux données suite à un chiffrement du disque dur. L'éteindre permet d'empêcher la suppression des données.

Analyser les données: Les données numériques sont transférées sur un nouveau support afin de ne pas endommager l'original par inadvertance et d'éviter toute « contamination des données ». Un «Write Blocker» garantit l'impossibilité de modifier les données tandis que des logiciels spécifiques permettent d'accéder aux données cachées et partiellement supprimées. De plus, des informations sont collectées à partir d'Internet, p. ex. des chats, des sites Web consultés ou des e-mails, afin de mieux cerner les activités criminelles. Il peut s'avérer nécessaire que des spécialistes externes effectuent l'analyse car celle-ci requiert des connaissances et des compétences précises en termes de programmation. Une fois les données sauvegardées, les appareils sont analysés afin de déceler l'ADN, les empreintes digitales et les autres traces éventuelles.

Impressum
Académie suisse des sciences techniques SATW
www.satw.ch/fr
Janvier 2019