TechnoScope
by satw 1/19

La tecnica sulla scena del crimine

Ah, ecco! – Scienza forense digitale

Nella scienza forense digitale vengono raccolte e analizzate – come suggerisce il nome stesso – le tracce e le prove digitali per ricostruire la dinamica del reato. In teoria ogni reato lascia tracce dietro di sé. Il ladro ha cercato sul suo smartphone la sua destinazione su Google Maps? L'assassino aveva già minacciato prima la sua vittima via e-mail? O è il reato stesso che è stato perpetrato online, ad esempio una truffa finanziaria? I messaggi inviati e ricevuti vengono archiviati nei cloud, le foto caricate possono contenere dati sulla posizione, se il GPS era acceso, e il tragitto dello smartphone può essere ricostruito in base alle celle telefoniche agganciate.

Affinché le prove digitali possano reggere in tribunale, l'intera procedura di repertamento e analisi delle prove deve essere documentata in maniera completa – come avviene in tutti gli altri rami della scienza forense.

Come si procede?

Repertamento dei dispositivi informatici: Tutti i dispositivi presenti sulla scena del crimine, ad esempio hard disk, chiavette USB, telefoni cellulari, scanner, telecamere di sorveglianza, eccetera, vengono repertati e, se possibile, viene recuperata la password delle persone coinvolte. Altrimenti, contrariamente a quanto succede spesso nei film, decodificare la password può essere una procedura lunga e difficile. I telefoni cellulari vengono spenti subito, infilati in una cosiddetta «custodia Faraday» o messi in modalità aereo, onde evitare qualunque connessione alla rete che potrebbe alterare i dati presenti sul cellulare. I monitor dei computer vengono fotografati, per «congelare» la situazione al momento. Una decisione importante che va presa subito riguarda il computer, se lasciarlo acceso oppure spegnerlo. Se rimane acceso, è possibile seguire in tempo reale l'attività criminale, senza contare il fatto che in questo modo non si mette neanche a rischio il futuro accesso ai dati nel caso in cui il disco rigido sia criptato. Per contro, spegnendo il computer si può impedire la cancellazione dei dati.

Analisi dei dati: I dati digitali vengono trasferiti su un supporto dati in maniera da evitare che l'originale venga danneggiato inavvertitamente e prevenire quindi un'eventuale «contaminazione dei dati». In questo caso si può utilizzare un write blocker, ovvero un dispositivo che garantisce che i dati non vengano alterati. Con specifici software è possibile accedere anche ai dati nascosti o parzialmente cancellati. Inoltre gli investigatori raccolgono anche le informazioni da internet, ad esempio dalle chat, dai siti visitati e dalle e-mail, in modo da poter ricostruire tutte le attività criminali. È probabile che le analisi vengano affidate a consulenti esterni in possesso del know-how e delle conoscenze informatiche necessarie. Dopo aver repertato i dati, i dispositivi vengono analizzati per ricercare eventuali tracce di DNA, impronte digitali o altri tipi di tracce.

Colophon
Accademia svizzera delle scienze tecniche SATW
www.satw.ch/it
Gennaio 2019