PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5570 di Venerdì 01 marzo 2024

Raccolta, gestione e conservazione delle prove digitali

Le prove digitali sono un prezioso strumento di indagine, che deve però essere gestito correttamente. Una raccolta, gestione e conservazione non corretta di queste prove può portare ad una perdita di credibilità giudiziaria.

Nessuno dubita del fatto che oggi, sulla scena del crimine non vengono solo raccolte tracce fisiche, ma anche tracce di origine digitale. Il National Institute of Justice, negli Stati Uniti, definisce la "Digital evidence" come un'informazione archiviata o trasmessa in forma binaria, che può essere utilizzata durante il dibattimento giudiziario. Una raccolta, gestione e conservazione non corretta di queste prove può portare ad una perdita di credibilità giudiziaria.

Le prove digitali costituiscono un'informazione che può essere archiviata o trasmessa in forma binaria e che può essere presentata in giudizio; queste informazioni digitali possono essere trovate su un hard disk di un computer, su uno smartphone, su una chiavetta USB e su altri strumenti informatici. Queste prove digitali frequentemente sono associate al crimine elettronico, a pornografia infantile o a frodi legate all'utilizzo improprio delle carte di credito.

Negli ultimi decenni questa tipologia di prove è cresciuta in modo esponenziale e può essere utilizzata per perseguire vari tipi di crimini, non necessariamente di origine elettronica. Ad esempio, i messaggi di posta elettronica di un individuo sospettato o i dati presenti su uno smartphone possono contenere informazioni critiche afferenti a specifiche indagini.

È ormai famoso il caso, avvenuto nel 2005, in cui l'analisi dei contenuti di un floppy disk consentì agli investigatori di individuare un serial killer che era riuscito a eludere l'arresto, da parte della polizia, fino dal 1974 e che nel frattempo aveva ucciso almeno 10 persone!

Chi scrive appare talvolta in giudizio, come consulente della magistratura o di parte, e nella sua deposizione fa' frequente riferimento a prove di origine digitale.

Il fatto che spesso la magistratura inquirente o giudicante non abbia una conoscenza approfondita sulle modalità di raccolta, gestione e conservazione di queste prove fa sì che un abile avvocato possa avanzare perplessità sulla credibilità di questi elementi probatori.

Ecco la ragione per la quale raccomando ai lettori di leggere con attenzione il documento allegato, che dà preziose indicazioni sulle modalità con cui è possibile conferire un elevato grado di credibilità a prove digitali, in grado di annullare lo spazio per possibili contestazioni da parte della controparte.

Per dare un'idea della potenziale complessità della raccolta e dell'analisi di evidenze digitali, si pensi ad esempio ad un investigatore che deve esaminare del materiale digitale, che si ritiene possa essere collegato a attività di pornografia infantile. L'investigatore deve, per lunghe ore, osservare centinaia di video, estratti dal computer sequestrato.

L'analista, in particolare, deve vedere se è presente nelle immagini un essere umano e se questo essere umano è un adulto od un bambino. È bene ricordare che oggi sono disponibili applicativi di intelligenza artificiale che possono, almeno in parte, automatizzare questo esame e alleviare il compito dell'esperto informatico.

Ecco perché può essere di grande aiuto un applicativo, sviluppato con il supporto del National Institute of Justice, negli Stati Uniti, e l'Università di Purdue, che viene battezzato dall'acronimo FileTSAR - File Toolkit for Selective Analysis Reconstruction

Anche l'Università di Rhode Island ha sviluppato un altro applicativo, chiamato DeepPatrol, che usa tecniche di intelligenza artificiale per analizzare rapidamente grandi quantità di dati.

Ma non basta.

È anche disponibile un applicativo digitale, liberamente disponibile presso Yahoo, chiamato OpenNSFW, che permette di rilevare in modo automatico la presenza di possibili scene pornografiche in riprese filmate.

Questo applicativo analizza le immagini e attribuisce un punteggio alla probabilità che queste immagini facciano riferimento a scene pornografiche. Il punteggio è variabile fra zero e uno ed un punteggio di 0,8 indica una elevata probabilità che l'immagine sia pornografica.

Un altro applicativo estremamente interessante analizza la possibile età del soggetto ripreso, anche in questo caso utilizzando tecniche di intelligenza artificiale. È così possibile mettere in evidenza immagini pornografiche, ove sono presenti immagini di bambini o minori.

Resta inteso che l'analisi di queste immagini rappresenta comunque un aspetto non unico nell'intero processo di cattura e conservazione delle immagini. Occorre adottare dei protocolli estremamente garantistici, che possano garantire come le immagini catturate siano esattamente le stesse presenti sul supporto informatico, da cui sono state estratte, e che successive manipolazioni non abbiano compromesso in modo irreversibile le immagini stesse.

Negli Stati Uniti, ma anche in Italia, ho avuto notizia del fatto che i magistrati giudicanti possano chiedere che una immagine, artificialmente migliorata dall'esperto che la presenta, possa essere riportata all'immagine originale, in modo da poter seguire passo passo il processo di trattamento dell'immagine, che porta a presentare alla corte un'immagine più facilmente comprensibile, rispetto all'originale.

Improving the collection of digital evidence (pdf)

Adalberto Biasiotti
