Dati a prova di contestazione. Arriva la videoforensics

Dott. Antonmarco Catania
Direttore Divisione di Videoforensics presso la GSG International
Perito per sicurezza presso la Cam.Com. Milano

Sta prendendo sempre più spazio la scienza che si occupa di tutte le forme di trattamento dei bit informatici per essere valutati in un'aula di tribunale

"Buon giorno, sono il Comandante della Polizia locale. Questa notte è accaduto un furto. Le telecamere ne hanno ripreso l'autore e forse si può riconoscere la targa dell'auto. E' possibile salvare il filmato su un CD? Si riescono anche a schiarire i fotogrammi per leggere meglio la targa?"

L'installatore si precipita dal cliente, armato del manuale di istruzione e di software di controllo remoto – si fare prima a scaricare il video via rete… poi forse il masterizzatore non funziona - e salva il filmato in Avi… così è leggibile da tutti.

Ha agito correttamente il Comandate a demandare all'installatore l'estrazione dei dati con una telefonata?

L'operazione di acquisizione del reperto è stata effettuata correttamente? Cosa accade se, dopo qualche giorno, l'HD viene riscritto e rimane solo la copia effettuata dall'installatore? E se questo, "smanettando con Paint o similari, ricostruisce un numero di targa, ha agito correttamente? Sono utilizzabili le prove così raccolte in un'aula di tribunale?

La Videoforensics prova a dare qualche risposta a queste domande.

La Videoforensics, in relazione alla quale in Italia non esiste alcuna normativa specifica, può essere considerata una branchia della Digital Forensics, la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici.

Una Legge che riveste una grande importanza al riguardo è la n.48/2008, che per quanto attiene alle questioni poste, disciplina il trattamento delle prove informatiche.

Nel nostro laboratorio di Videoforesics, per primi in Italia (e non solo) abbiamo iniziato a studiare la videosorveglianza, nell'ottica di poterne conseguire delle prove utili ed utilizzabili nel dibattimento di un'aula di giustizia.

Iniziamo a dire che il risultato della videosorveglianza è un Dato Digitale – una sequenza di numeri binari - all'interno della

quale è contenuta un'Informazione Digitale attinente ad un'indagine – la foto di un viso, un filmato di un'auto,…
E' evidente la differenza tra Dato Digitale e Informazione Digitale, così come risulta evidente che ciò che bisogna preservare è quindi il Dato Digitale mentre ciò che bisogna studiare è l'Informazione Digitale.
Il legislatore impone la cura assoluta nel repertare la prova e nel conservarla assolutamente integra.
Ma nel caso della videosorveglianza quale è la prova che bisogna preservare? La stampa del viso incriminato, il cd su cui è stato salvato il filmato o l'hard disk?
La prova, nel processo penale, proof, è il risultato della conoscenza conseguita attraverso gli accertamenti effettuati sul mezzo di prova, evidence.
Quando si tratta di computer forensics, il mezzo di prova, cioè l'evidence che contiene le informazioni, connesse con l'indagine, è il dato digitale.
Il reperto da acquisire è quindi il dato digitale, cioè la sequenza di uni e zeri che possono contenere informazioni attinenti all'indagine – non l'HD in quanto tale.
E' chiaro che il dato digitale è un reperto immateriale che sussiste in quanto sussiste il mezzo che lo contiene. L'immaterialità del

Dott. Antonmarco Catania
Direttore Divisione di Videoforensics presso la GSG International
Perito per sicurezza presso la Cam.Com. Milano

dato informatico è stata riconosciuta dallo stesso legislatore il quale, tra i computer crimes, non ha previsto il reato di furto, limitandosi alla mera duplicazione abusiva.
Analogamente per quanto avviene per le impronte digitali, per cui, a seguito alla fase irripetibile del rilievo, si arriva a generare una foto sulla quale vengono poi svolti tutti i possibili accertamenti, così, in relazione alla prova digitale, è indispensabile effettuare una copia assolutamente genuina e secondo l'art. 48 legge 18 marzo 2008, preservarla affinché siano possibili successivi accertamenti ripetibili.
Una prova digitale non genuina può costituire una prova illegittimamente acquisita ai sensi dell'art. 191 c.p.p. e quindi inutilizzabile.
Effettuare una copia genuina di un dato digitale al fine di farlo divenire un reperto sul quale poter fare accertamenti ripetibili che portino ad acquisire conoscenza, che abbia nesso con il caso in questione, significa generare una copia identica del dato digitale.
L'identicità viene tipicamente garantita da fatto che applicando una determinata funzione al dato digitale, oggetto dell'indagine, quale potrebbe essere il contenuto di un hard disk, si ottenga uno ed un solo valore, detto hash. Ad esempio, se utilizziamo come funzione l'MD5, si ha che:
hash = MD5(dato-digitale)
Se si applica tale funzione al contenuto di due HD e si ottengono due risultati diversi, allora il dato digitale contenuto nel primo HD non corrisponde con quello contenuto nel secondo HD.
L'acquisizione del reperto è quindi l'attività volta alla copia (clonazione o duplicazione che dir si voglia) dei dati presenti sul supporto di memoria, o in transito su una rete. Rappresenta, forse, la fase più delicata perché se svolta da personale non dovutamente formato può portare alla distruzione di dati potenzialmente rilevanti o all'invalidazione del supporto e/o dei dati in esso contenuti.
L'acquisizione è un atto irripetibile che deve essere svolto quindi seguendo procedure di "best practices", da personale competente, che fa uso di tools hardware e software specifici.
La fase di acquisizione del reperto deve risultare assolutamente accurata, in modo da salvaguardare l'integrità del reperto.
Quando si acquisisce un dato informatico ed in particolare quando si acquisiscono registrazioni video, un'attenzione particolare è necessaria prestarla inoltre alla ricostruzione

della timeline, annotando la data e l'ora – compresa di secondi – del sistema, confrontandola immediatamente con l'ora reale.
Pochi secondi di differenza impressi sulle immagini possono sostenere o meno un alibi!
Meglio sarebbe poi, durante l'acquisizione di un reperto, filmare tutte le operazioni.
La Videoforensics si occupa anche di come ricercare un evento all'interno di una registrazione di giorni o settimane. In questo caso, vengono in aiuto gli strumenti di videoanalitics, utilizzati, in questo caso, non per generare allarmi, bensì per ricercare "particolari comportamenti".
Una volta che si è in possesso di un filmato attinente all'indagine, è necessario autenticarlo, dare cioè una risposta al dubbio che questo non sia stato modificato – o artatamente generato – prima di essere acquisito come reperto.
Fino a quando la ricerca viene effettuata su sistemi noti, dotati ad esempio di watermarking, correttamente programmati, la risposta è piuttosto semplice. In realtà, la maggioranza delle indagini è effettuata su sistemi non standard, manufatti in ogni parte del mondo!
In questo caso la questione risulta essere decisamente più complessa e molto spesso di tratta di svolgere vere e proprie indagini scientifiche.
Disponendo allora del mezzo di prova, l'evidence, si vuole quindi disporre una vera e propria prova - proof - Chi è quell'uomo? A chi appartiene quell'auto che sembrerebbe avere quella targa?
Il parametro di cui bisogna tenere conto in questo ambito – e retroattivamente già in fase di progettazione di un sistema di videosorveglianza - sono allora i Pixel x Metro disponibili in una determinata immagine.
Possiamo dire che con 30 pixel per metro riconosciamo del movimento in un'area, con 130 pixel per metro possiamo riconoscere qualcuno già noto, con 200 pixel per metro identifichiamo una persona.
Ma se la quantità di pixel disponibili non sono sufficienti ad un riconoscimento di un volto o di una targa, è possibile elaborare l'immagine senza che venga definita un'elaborazione non utilizzabile in un processo?
Il dato digitale è certamente mutato a seguito di una elaborazione digitale, ma quando si può dire che l'informazione digitale contenuta è stata migliorata piuttosto che non manipolata?
Si può dire che un'immagine non è stata manipolata quando si preserva l'immagine originale, si fa riferimento ad algoritmi di sharpening, smoothing, edge detection, interpolazione e filtraggio di frequenze riconosciuti dalla comunità scientifica, si documenta la sequenza degli algoritmi applicati, essendo così in grado di riprodurre in ogni momento la sequenza di operazioni che ha portato ad un determinato risultato.
Con il nuovo processo penale, l'attività di indagine può essere svolta, oltre che dalle forze dell'ordine, anche dalle parti che possono avvalersi di consulenti tecnici, in particolare di quelli iscritti negli albi specifici presso camere di commercio e tribunali. GSG International, istituendo un laboratorio di indagini di Videoforensics, si è posta ancora una volta all'avanguardia nella qualificazione della proposta in un mercato della sicurezza che deve elevare a tutti i livelli la professionalità della propria offerta.
La divisione di Videoforesics della GSG International è nata così dotandosi di tutti gli strumenti e le competenze necessarie a dare una risposta alla domanda di supporto in questo ambito, attraverso servizi di consulenza specifica, acquisizione dei reperti, perizie di autenticità, ricerca eventi, enhancement delle immagini, ricerca targhe e consulenze tecniche di parta (CTP) ed oggi annovera tra i suoi clienti, Procure, Forze dell'ordine, Polizie Locali ma anche importanti Studi Legali.

Sul portale della Rivista Antifurto www.spaziosecurity.it, sezione Riviste On Line, potrà scaricare e consultare il PDF di questo articolo