Computer forensics: la raccolta

Business Diritto e Informatica

di Emanuele Florindi - Un percorso guidato tra le varie fase delle indagini che conducono al processo per reato informatico. Una definizione di computer forensics e l'avvio delle intercettazioni

Redazione
Pubblicato il 12 giu 2009

Perugia – Nelle scorse settimane l'Avv. Florindi ha illustrato le modalità di avvio delle indagini, fino al momento dell'emissione del cosiddetto "avviso di garanzia", nonché l'avvio della perquisizione con le diverse modalità di raccolta delle prove. La trattazione riprende tracciando una panoramica sulle differenti possibilità che si presentano agli investigatori in questa fase.

Cloni e copie

Proprio in merito all'acquisizione si ha il principale confronto tra differenti correnti: una prima che vede nell'analisi un accertamento irripetibile ed una seconda che, invece, lo considera ripetibile.

La differenza non è soltanto terminologica, ma ha pesanti ricadute in sede processuale: l'accertamento ripetibile, infatti, può sì essere compiuto senza dare alcuna comunicazione alle parti ma, di contro, la difesa potrà sempre richiedere, in sede dibattimentale, che l'accertamento venga ripetuto alla presenza delle parti e di un perito nominato dal Giudice.

L'accertamento non ripetibile, invece, parte dal presupposto che la cosa sia soggetta a modifica e prevede che il PM dia avviso alla persona offesa ed alla persona sottoposta alle indagini del luogo, del giorno e dell'ora previsti per il conferimento dell'incarico affinché questi possano partecipare con propri consulenti. Prima dell'inizio delle operazioni l'indagato può formulare riserva di incidente probatorio e, in tal caso, si procederà alle operazioni in tale sede.

Non vi è dubbio che tale pratica sembri offrire le maggiori garanzie difensive, ma vi sono almeno due elementi che bisogna tenere in considerazione: in primo luogo si tratta di un accertamento **tecnicamente** ripetibile (salvo grossolani errori del consulente), quindi non è tecnicamente possibile parlare di accertamento non ripetibile. In secondo luogo l'utilizzo di un simile strumento, laddove si proceda contro ignoti, rappresenterebbe una grave lesione al diritto alla difesa per il soggetto che, successivamente iscritto nel registro degli indagati, non soltanto non avrebbe alcuna possibilità di ottenere una nuova analisi del supporto in sede di dibattimento, ma ben potrebbe trovarsi di fronte ad un reperto ormai alterato: la valutazione dell'accertamento come non ripetibile, consentirebbe di effettuare anche operazioni in grado di provocare modifiche (per esempio l'avvio della macchina da analizzare senza alcuna cautela).

Proprio per tali ragioni è preferibile, a mio avviso, procedere con la formula dell'accertamento ripetibile fermo restando il fatto che, in presenza di errori o attività che apportino modifiche alla struttura del reperto, lo stesso dovrebbe essere considerato "inquinato" e le risultanze in esso contenute non più genuine né utilizzabili in dibattimento.

Dunque, per garantire la ripetibilità dell'analisi (vero principio cardine della computer forensics), è necessario operare sempre su di una copia del supporto sequestrato. Naturalmente non è sufficiente un semplice ghost del disco rigido, ma è necessario che si tratti di una perfetta duplicazione (in gergo si parla spesso di clonare un hard disk) che, a differenza della mera copia, consentirà di operare su un hard disk praticamente identico all'originale, consentendo, quindi, l'analisi anche di eventuali aree apparentemente vuote.

In commercio esistono numerosi prodotti, hardware e software, in grado di clonare un hard disk garantendo la non alterazione dell'originale e l'esatta corrispondenza originale-copia. Si può trattare di prodotti software commerciali (Encase, ForensicToolkit), open source (dd, aimage, dcfldd, AFF) oppure di apparecchi hardware (hardcopy, diskjokey, i vari prodotti Logicube). Più economici i prodotti software (soprattutto quelli open source), più sicuri gli apparecchi hardware, ormai realizzare la copia garantendo la ripetibilità dell'accertamento non dovrebbe più rappresentare un problema.

È poi buona norma procedere all'acquisizione della firma digitale dell'intero supporto acquisito, con un'operazione detta hashing a senso unico. L'operazione viene tipicamente compiuta utilizzando un algoritmo di classe MD5 che, generando un'impronta della lunghezza di 128 bit (16 byte), costituisce un riferimento certo alla traccia originale, pur non consentendone la ricostruzione.

l'hard disk con un dispositivo che inibisca la scrittura sullo stesso (write block) o, in alternativa, utilizzare un apparato hardware per effettuare una copia precisa dell'hard disk ed avviare la macchina utilizzando tala copia. L'alternativa più valida è però quella di avviare la macchina in modalità virtuale, per esempio utilizzando VmWare, dopo aver effettuato una copia del disco rigido.

In merito a quest'ultimo punto, si consideri che numerosi software di crittografia o di steganografia consentono di impostare un meccanismo di protezione che danneggia il file protetto in caso di errori nell'inserimento della password (oppure inserendo un'apposita password): quindi, errori di digitazione in sede di ispezione potrebbero portare alla cancellazione delle tracce del reato. Allo stesso modo un floppy (o un CD) lasciato nel lettore potrebbero avviare una procedura di cancellazione dell'intero hard disk. Quindi: l'avvio del sistema con il disco originale installato e collegato è decisamente sconsigliato!

Avv. Emanuele Florindi
http://www.accademiascienzeforensi.it
http://www.telediritto.it

La trattazione dell'Avv. Florindi si concluderà la prossima settimana con una trattazione delle possibili metodologie di interpretazione delle prove fin qui acquisite nel corso dell'indagine.