



Cybercrimes.it

Computer Forensics & Crimine Informatico

Denis Frati

# La Prova Informatica nel Processo Penale

Aspetti tecnici e giuridici

Traccia per l'intervento al convegno "La Prova Informatica nel Processo Penale – Aspetti tecnici e giuridici", venerdì 4 maggio 2007, Tribunale di Ivrea.

Seminari di Diritto Penale dell'Informatica, organizzati da Osservatorio Centro Studi Informatica Giuridica di Ivrea e Camera Penale Vittorio Chiusano – Piemonte Occidentale e Valle d'Aosta

### **Prefazione:**

Riguardo i vari aspetti della computer forensics e dell'indagine digitale, in generale, esiste in rete una voluminosa documentazione redatta da preparatissimi professionisti della materia informatica e giuridica, professionisti che spesso hanno approfondito le due tematiche sino a diventare profondi conoscitori di entrambe.

Grazie ai frequenti contatti intrattenuti a livello personale con periti privati e colleghi, cercherò di trattare questi argomenti dal punto di vista della "manovalanza", di chi lavora direttamente sui supporti e sui dati, cercando di evidenziare ai vostri occhi le problematiche con cui si scontra l'analista forense, CTP o investigatore che sia.

Si può comunque anticipare che gran parte di questi problemi è dovuto all'assenza di una qualunque normativa che disciplini metodiche, procedure, strumenti da usarsi nelle analisi forensi alla ricerca di prove digitali.

Va tuttavia notato come, in risposta all'esigenza di standard operativi a cui assoggettare tutte le parti coinvolte nei procedimenti in cui sono coinvolti media digitali, stiano nascendo gruppi di lavoro (composti da magistrati, investigatori, avvocati e periti) con la finalità di elaborare, attraverso le esperienze maturate nei vari campi, delle linee guida che consentano di operare nel rispetto della legge, linee guida, o best practices (secondo la terminologia anglosassone) da trasformare poi in norme di legge.

### **Intervento:**

L'evoluzione tecnologica e la sua esponenziale diffusione hanno portato i dispositivi digitali ad essere strumenti di reati comuni e non solo di reati informatici, come avveniva in prevalenza all'inizio degli anni 80 con la diffusione delle Bulletin Board e la loro trasformazione in Internet.

Sempre più frequentemente troviamo dispositivi digitali quali telefoni cellulari, iPod, palmari, gps, fotocamere e videocamere digitali, chiavette usb, laptop, ecc...sulla scena del crimine e/o direttamente utilizzati dall'autore e/o dalla vittima dello stesso.

Questi dispositivi, potendo fornire indicazioni utili ai fini dell'indagine, andranno sempre analizzati al fine di individuare la "prova".

Ma cosa si intende in ambito giuridico/informatico con il termine "prova digitale"?

L'argomento non è di semplice dibattito. Nel mese di marzo è stato presentato a Bruxelles il Progetto Europeo sull'Ammissibilità della Prova Elettronica nei Tribunali.

Tale progetto ha la finalità di comparare la definizione di prova elettronica e l'uso che ne viene fatto nei tribunali dei Paesi aderenti all'UE, al fine di proporre un codice comune a riguardo.

Al momento nel panorama italiano i più sembrano accettare la seguente definizione:

"Qualsiasi informazione, con valore probatorio, che sia o memorizzata o trasmessa in un formato digitale" (Scientific Working Group on Digital Evidence, 1998).

Formato digitale significa che il dato digitale, qualunque sia il supporto che lo contiene, è interpretabile da dispositivi elettronico/digitali in grado di comprendere, a livello base, un unico linguaggio, il codice binario, fatto di uno (1) e zero (0).

Tali dati, nella loro forma minima, il bit, sono memorizzati su supporti di memorizzazione di tipo magnetico, o magneto/ottico, quindi per loro natura modificabili, anche inavvertitamente. A livello più pratico, meno accademico, potremo dire, per esempio, che attraverso un hard disk, preso in carico dalla PG a seguito di perquisizione e sequestro (fonti di prova), si viene in possesso della prova, i dati in esso contenuti, da cui si potranno poi estrarre, se individuati, files/dati di rilevanza ai fini dell'indagine, che costituiranno gli elementi di prova. Quali caratteristiche deve possedere la prova affinché abbia valore probatorio, sia quindi utilizzabile in dibattimento (citando le slide "L'intrinseca fragilità delle tracce digitali" Prof. M. Monga, Milano 23-11-2006 ):

- autenticità
- integrità
- veracità
- completezza
- legalità.

Ma tecnicamente parlando, come si perviene alla prova digitale, in modo da rispondere alle specifiche appena elencate?

Attraverso le procedure specifiche dei vari indirizzi della digital forensics (computer, network, mobile, ecc...).

Soffermandoci sulla computer forensics essa può essere definita come quella disciplina dedicata al trattamento delle prove digitali secondo fasi ben definite:

- 1) identificazione
- 2) preservazione
- 3) acquisizione
- 4) analisi
- 5) presentazione

Analizzandoli nello specifico:

L'identificazione: è quell'attività volta ad identificare attraverso l'analisi esterna dei dispositivi in esame, la loro interrogazione a livello logico e all'hashing, al riconoscimento univoco ed inequivocabile di dispositivi, supporti e dati.

Con dispositivi digitali la cui capacità di memorizzare dati aumenta costantemente, come le funzionalità rese disponibili dagli stessi (fotografare, riprodurre audio e video, navigare in Internet, ...) risulta sempre più difficile individuare da quali dispositivi si possa realmente reperire prove, "dati digitali", utili a fini investigativi.

Si corre il rischio di sottoporre ad analisi, per loro natura complesse e lunghe, dispositivi di nessun rilievo ai fini dell'indagine.

L'identificazione deve essere certa ed univoca, non è pensabile l'identificazione generica di supporti di memorizzazione che non permetta di collegare in modo incontestabile un dato al supporto dal quale è stato estratto.

Va tuttavia notato che il processo di identificazione non è limitato al solo supporto (l'hard disk, il cd, la chiave usb, ecc...) in cui la prova, intesa come insieme di dati è contenuto, ma anche sullo stesso insieme di dati e sui singoli elementi di prova, gli eventuali file o blocchi di bit, che dalla prova saranno estratti.

Appare quindi evidente che l'identificazione non è un processo a se stante, ma che ricorre successivamente anche nelle fasi di acquisizione e analisi, come vedremo successivamente.

Se ipotizziamo di procedere al sequestro di 1000 cd, dovrà essere possibile dare contezza dei supporti magneto/ottici presi in carico dalla Polizia Giudiziaria e di quelli sui quali si è svolta l'analisi, se questa avviene a campione.

Questo semplice esempio è già indicativo dell'assenza di metodiche standardizzate, non solo tra le parti coinvolte nel processo, ma tra le stesse forze di polizia.

Non esiste infatti un identico procedere, c'è chi sostiene che:

- la PG ha sicuramente operato al meglio;
- si dovrebbe registrare sul verbale di sequestro i seriali di tutti i supporti;
- si dovrebbe procedere, con incidente probatorio, davanti alle parti al sequestro dei supporti, sigillandoli, lasciando al perito/analista\_investigatore la successiva documentazione della presa in carico dei campioni e della loro acquisizione secondo le best practices.

Se poniamo attenzione a quanto vediamo nei TG, facendo riferimento alle immagini trasmesse nei servizi relativi al caso Telecom/Tiger\_team, era possibile notare come i case dei pc sequestrati dalla Polizia Giudiziaria mostrassero tutti i sigilli!

Successivamente si sarà proceduto a documentare che dal case con numero seriale 1234 è stato estratto l'hard disk marca X, con tali caratteristiche tecniche è seriale 09876.

Preservazione: come l'identificazione, anche la preservazione non è un passaggio a se stante, ma che anzi si fonde indissolubilmente con i passaggi di acquisizione ed analisi.

La prova va preservata, tecnicamente, attraverso l'utilizzo di dispositivi/software write blocker, attraverso la sua duplicazione ed attraverso l'analisi delle sole copie forensi.

La prova viene preservata documentando le attività su di essa svolte, e sulle copie che rappresentano anch'esse prove, ed i passaggi di mano in mano.

Quest'ultima attività si concretizza nella chain of custody, la catena di custodia, documento atto a documentare, perdonate il giro di parole, quando, come e da chi la prova viene acquisita e custodita, anche in tempi successivi.

A livello di PG non esiste un documento definibile "catena di custodia". La chain of custody sarà piuttosto rappresentata dagli atti interni al fascicolo che documenteranno il sequestro della prova, l'eventuale consegna al perito e ripresa in carico dalla PG, il deposito della stessa all'ufficio prove di reato del tribunale, ecc...

L'acquisizione: è 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.

Per chiarire queste problematiche è necessario ed inevitabile procedere per esempi:

- trovandosi a dover acquisire i dati immagazzinati su un computer acceso, la sola azione di spegnerlo seguendo la procedura standard potrebbe portare all'avvio di programmi e/o procedure che, in chiusura di sessione, sono stati deputati dall'utente, o dal sistema operativo stesso, alla cancellazione di dati importanti, le cronologie dei files aperti dai diversi player, di internet, lo svuotamento dei file di swap e di spool di stampa, motivo per il quale si consiglia di staccare brutalmente il collegamento alla presa di corrente del dispositivo, causandone lo spegnimento immediato.  
E' anche vero che esistono casi (incident response e specifiche scene del crimine)

nei quali l'analisi di un sistema accesso offra “prove” rilevanti, si pensi ai dati contenuti nella RAM.

E' altresì vero che l'analisi di un sistema accesso porta inevitabilmente alla modifica dello stesso (terminazione o avviamento di nuovi processi o connessioni, cambiamento dei time-stamp, ecc...), rendendo il reperimento delle prove in contraddittorio non ripetibile.

- trovandosi a dover acquisire i dati immagazzinati in un sistema spento è essenziale che non si proceda con l'accessione standard dello stesso. L'avvio del sistema operativo, oltre a poter causare la cancellazione di file e/o partizioni di swap, comporterebbe come minimo il cambiamento dei metadati relativi alla creazione/accesso/modifica dei files di sistema.

E' quindi evidente che tale tipologia di analisi va ponderata caso per caso da personale all'uopo formato.

E' interessante notare come, differentemente da quanto avviene da noi, negli USA, consci di tali problematiche, il Dipartimento della Giustizia abbia pubblicato un paper (“Forensic Examination of Digital Evidence: a guide for law enforcement” - U.S. Departmente of Justice) in cui vengono spiegate le corrette procedure di acquisizione al fine di non causare modifiche nella fonte di prova.

Al fine di rendere l'utilizzo della prova valido in dibattimento e mantenere la fattibilità dell'incidente probatorio (evento richiesto ai fini della validità) è indispensabile non lavorare sulla prova originale, ma utilizzare copie identiche validate utilizzando algoritmi di hashing, al fine di garantirne l'assoluta equivalenza.

La tipicità di queste copie è di essere identiche in toto all'insieme di bit contenuti originariamente sul supporto, si parla quindi di “bit stream image”, ossia di un immagine generata attraverso il flusso costante (stream) di bit, tale da poter riprodurre l'esistenza di file cancellati, parti di essi, spazi (settori) vuoti, ecc..

La realizzazione di immagini forensi viene eseguita attraverso l'uso di tools ( open e closed source) considerati, a livello internazionale, capaci di garantire l'identità della copia con l'originale.

Identità che va comunque verificata e di cui discuteremo tra poco.

Vale la pena far notare, ai fini di illustrare nuovamente la fragilità della prova digitale, come durante l'acquisizione della copia, in caso vengano incontrati errori sul supporto originale, il software preposto alla copia, inserisca in corrispondenza dei settori danneggiati (o comunque non leggibili) una serie di dati specificati dall'operatore, questo al fine di evitare la presenza di dati spuri, non derivanti dalla copia, ma preesistenti sul supporto su cui si realizza la copia.

Facendo riferimento al tool “dd” nativo del S.O. Linux, se si imposta una dimensione dei blocchi di bit da trasferire, in fase di copia dei dati, eccessiva, si rischia, incontrando un singolo settore danneggiato (usualmente 512 bytes), di perdere anche dati non direttamente interessati dall'errore

```
#dd if=dispositivo_sorgente of=dispositivo_destinazione conv=noerror, sync bs=512
```

in questo caso trasferendo blocchi di dati della dimensione di 512 bytes, in caso di errore su

un settore, nel disco di destinazione si avrà un solo settore “azzerato”.  
Se per velocizzare la copia dessimo una dimensione di 4 Mbytes

```
#dd if=dispositivo_sorgente of=dispositivo_destinazione conv=noerror, sync bs=4096
```

in caso di errore su un solo settore, andremmo incontro alla perdita dei successivi 3,5 Mbyte (approssimativamente), in cui sul dispositivo originale potrebbero esservi immagazzinati dati rilevanti ai fini processuali.

Dimostrazione di come, pur usando una metodologia corretta ed un tool corretto, ai fini forensi, l'utilizzo di un parametro mal valutato possa portare alla perdita dell'identità con l'originale, la prova digitale (la sua copia) viene alterata.

Durante tutta le fasi di lavorazione forense, deve sempre essere garantito, non solo che la copia sia identica all'originale, ma anche e soprattutto, che l'originale non subisca alcuna modifica.

A tal fine ogni attività fatta sulla prova originale deve prevedere l'utilizzo di write-blocker, ossia dispositivi hardware e/o tools software che impediscano di apportare qualsiasi cambiamento sulla prova originale.

Se pur esistano tools software, quali il comando “mount” in ambiente linux, che funzionino quali write-blocker virtuali, impedendo di fatto qualsiasi azione in scrittura sui dati originali, i puristi vorrebbero in ogni caso l'utilizzo di un write-blocker hardware che salvaguardi l'originale, interponendosi fisicamente tra la forensic workstation e il device sorgente, impedendo scritture su i dati in esso contenuti.

Anche questo punto (write blocker hardware obbligatori si/no) è piuttosto dibattuto.

Non vi è alcuna regolamentazione a riguardo e sebbene anni di utilizzo e sperimentazione con i write blocker software, dimostrino che questi funzionino correttamente, il loro solo utilizzo può venir messo in discussione. Ci si dovrebbe domandare se, forse, più che la funzionalità del tool non si mette in discussione la sua modalità di utilizzo da parte dell'operatore.

Come si garantisce l'identità della copia con l'originale? Attraverso gli HASH, firme digitali di uno specifico insieme di dati.

In presenza dell'identità degli hash di due insiemi di dati (per es. dati contenuti in un hard disk e loro copia) si assume di essere di essere davanti a due insiemi di dati identici.

Ma cos'è un hash?

Gli algoritmi di hash sono processi logico-matematici (funzioni), sottoponendo ai quali un input (insieme di dati) di dimensione arbitraria, si ottiene in output una stringa di lunghezza fissa, per esempio 128 bit (32 caratteri in codifica esadecimale).

Gli algoritmi di hash sono definiti funzioni one-way, ad un solo senso, infatti, data la stringa in output non è possibile risalire ai dati che l'hanno originata.

Appare evidente che data la lunghezza fissa della stringa di output e dato il numero fisso di possibili caratteri che ogni “cifra” può assumere, il numero di possibili combinazioni è limitato, un numero finito. Ciò avviene a fronte di un numero infinito di possibili output!

Appare quindi evidente che esiste la probabilità statistica di incorrere in due hash identici partendo da due input differenti, evento definito “collisione”.

Tale problema è discusso in particolare relativamente all'algoritmo MD5 che, sebbene rappresenti l'algoritmo più utilizzato in campo forense, nel 2005 fu portato a collisione (cit.

Magg. RACIS Carabinieri Marco Mattiucci - [www.marcomattiucci.it](http://www.marcomattiucci.it)) da un gruppo di ricerca cinese.

Sebbene a livello accademico sia stata dimostrata la possibilità di collisioni con l'algoritmo MD5, fino ad ora il più utilizzato, è bene specificare che ciò si è concretizzato solo nella possibilità di creare, dato a priori un hash, due file differenti che sottoposti all'algoritmo avrebbero dato quello stesso risultato.

La proof of concept accademica non indica assolutamente la possibilità di modificare un file mantenendone l'hash inalterato! Infatti, una variazione, anche di un solo bit, della copia rispetto all'originale, comporterebbe due hash differenti.

L'utilizzabilità dell'algoritmo di hash MD5 in campo forense, rimane comunque valida, considerando che la possibilità di incorrere in due masse di dati differenti (i contenuti di due diversi hard disk, per esempio) che possano generare lo stesso hash MD5 (collisione) è una su 4 mila miliardi (circa) !!

Tuttavia, gli algoritmi soggetti a collisioni sarebbero, preferibilmente, da abbandonare, in relazione alle dimensioni che le moderne memorie di massa stanno raggiungendo. Dimensioni tali da poter contenere una tale quantità di dati da rendere statisticamente possibile il verificarsi di una collisione.

Pensare che l'acquisizione di una prova possa concludersi con la presa in carico, fisicamente parlando, e con la realizzazione dell'immagine validata a fini forensi è restrittivo. Tutta l'attività messa in essere andrebbe documentata al fine di garantire l'esame degli eventi succedutesi, ed andrebbe allargata non al solo supporto fisico, su cui reperire l'insieme di dati, prova digitale, ma all'intero sistema in esame.

Al fine di poter inserire le attività informatiche svolte con il sistema in esame in un corretto panorama temporale è importantissimo che chi opera l'acquisizione fisica e/o digitale documenti date e orario del sistema stesso.

Se consideriamo che i time-stamp applicati dal sistema ai files, in seguito ad attività di creazione/modifica/accesso, sono legate a data/ora di sistema appare evidente che la mancata trasmissione di tali informazioni all'esaminatore potrà comportare una non corretta interpretazione degli eventi, ci si potrebbe così trovare, per esempio, nell'impossibilità di dimostrare che l'accusato, in un ben specifico momento non stava utilizzando il sistema, con tutte le conseguenze del caso.

Per quanto tutto ciò appaia scontato e ovvio, la realtà non ha nulla a che vedere con le discussioni accademiche e le check list presenti nella manualistica.

L'analista forense (perito o investigatore che sia) si trova nella condizione di dover prendere in consegna supporti contenenti dati/prove senza poter avere alcuna informazione sulle modalità con le quali il dispositivo è stato acquisito fisicamente.

L'esigenza di una regolamentazione della disciplina è tanto stringente quanto l'impossibilità degli enti preposti all'indagine digitale di rifiutarsi di operare, come forse sarebbe corretto, su tutte quelle prove le cui modalità di acquisizione non sono documentabili e rispondenti a standard tecnici incontestabili in sede dibattimentale.

L'analisi: rappresenta uno step delicato, anch'esso per nulla codificato. Al momento attuale l'unica limitazione esistente sulle procedure e i tools da utilizzarsi e che essi non apportino modifiche alla prova e che quanto fatto sia sempre documentabile.

L'analista forense può trarre giovamento dall'esistenza di alcune basilari linee guida da seguirsi (analizzare i file cancellati, lo spazio di swap, lo slack space, ecc...) per altro sempre

da relazionarsi a cosa si cerca, documentando la propria attività, magari con sistemi di login. Lo stesso non può invece dirsi per il software, i programmi, o tools che dir si voglia, utilizzati nell'analisi.

Esistono sostanzialmente due tipi di software, quelli open source e quelli closed source, dove con il termine "source" (sorgente) si intende il codice, nel senso di listati di istruzioni logiche.

Per il software open source, come indica il termine stesso, il codice sorgente è disponibile, può essere visionato, è quindi possibile, disponendo delle dovute nozioni tecniche, analizzare il codice e comprendere quali procedimenti logici esso opera sui dati che gli si dà in input.

Tale analisi può portare alla messa in discussione delle operazioni realizzate dal codice e ciò è garanzia della sua correttezza di funzionamento.

Esempio piuttosto classico di ciò è il sistema operativo GNU/Linux e gran parte dei tools utilizzabili con esso.

Per il software closed source avviene il contrario.

L'utente disporrà di un applicativo già compilato, trasformato quindi da linguaggio di medio/alto livello (interpretabile dall'uomo) in codice macchina non interpretabile dall'analista, il cui esame non può quindi dirci nulla (o comunque molto poco) riguardo i passaggi logico/matematici a cui sottopone i dati ricevuti in input (esempi più noti EnCase, FTK, WinHex Forensic).

Proprio su questa (im)possibilità di verificare la correttezza delle opzioni compiute del software verte una delle maggiori diatribe.

Tralasciando il discorso economico (usualmente i sistemi basati su GNU/Linux sono gratuiti, al contrario dei software proprietari che possono arrivare a costare svariate migliaia di euro), uno dei maggiori problemi per chi opera nella forensic è se l'utilizzo di un tool sia o no ammissibile per attività di analisi.

Se per la fase di acquisizione si sono avute indicazioni abbastanza precise proprio dell'esame delle copie di sistemi realizzate con i vari tools disponibili, lo stesso non può dirsi per l'analisi.

L'ipotesi più volte discussa di un ente che certifichi la validità o meno di un software per usi forensi è quanto mai complessa, valutando anche che un tool che operi nel rispetto della normativa del paese Blu può, magari, non farlo rispetto a quella del paese Rosso.

La difficoltà di stabilire chi e come debba valutare l'utilizzabilità dei tools per usi forensi lascia gli operatori e gli enti da cui dipendono in una situazione che ci porta a mutare, potremmo dire quasi passivamente, le scelte fatte nel panorama statunitense/nord\_europeo. Va tuttavia notato come negli USA vi sia chi contesta davanti alla corte l'utilizzo di tool proprietari, il cui codice non è disponibile per essere esaminato.

La sostanziale differenza tra i software open e closed source (prezzo a parte), sta principalmente nell'usabilità e nell'integrazione di tools differenti.

I sistemi di analisi forense basati su GNU/Linux, che rappresentano attualmente la scelta open source, non sono altro che un insieme di singoli, validi, tools, per l'appunto a codice aperto, implementati in un sistema a codice aperto (Linux).

Se da una parte il sistema Linux garantisce un'ottima capacità di riconoscimento del filesystem in uso su sistemi diversi, dall'altra non mostra una completa compatibilità tra applicativi operanti su sistemi differenti e nell'interpretazione di dati generati con tali applicativi.

Vi è un'intensa attività di sviluppo che consente da parte la portabilità di alcuni software

open source su sistemi proprietari, quali MS Windows, dall'altra un intenso lavoro di reverse-engineering che permette di comprendere le modalità con cui sistemi operativi e applicativi proprietari operano sui file, consentendo la realizzazione di strumenti che ne permettano comunque un'interpretazione.

I sistemi di analisi closed source, sono applicativi da utilizzarsi principalmente su sistemi operativi Microsoft.

A fronte di un prezzo spesso elevato garantiscono l'integrazione di molti tools in un unico software (tools di cracking delle password, individuazione della steganografia, realizzazione e montaggio delle immagini, player quasi universali), la presenza di un'interfaccia grafica semplice, in grado di mettere a proprio agio l'utente e la presenza di wizard per l'esecuzione di alcune operazioni.

Di contro non consentono, come su detto, l'esame dei passaggi logici effettuati e hanno una minor capacità di lavorare su filesystem differenti.

Dal punto di vista strettamente pratico l'analista forense si scontra con un grande problema: cosa deve cercare ??

Non è purtroppo raro trovarsi davanti ad un supporto di memoria con indicazioni vaghe, o inesistenti so cosa dover ricercare, o sull'evento criminoso oggetto dell'indagine.

Data la sempre maggior quantità di dati presenti nei supporti di memoria è impensabile doversi guardare tutte le immagini, i filmati, ascoltarsi brani audio, leggersi mail e documenti alla ricerca di eventuali ipotesi di reato.

Prendere in consegna un supporto la cui documentazione allegata ci informi unicamente che il titolare dello stesso è indagato, per esempio, per reati contro il patrimonio o associazione a delinquere è un po' poco, anzi proprio nulla.

L'analista necessiterebbe di poter accedere a gran parte del fascicolo relativo al capo d'imputazione, per poter effettuare ricerche in base a specifiche parole, nomi propri, numeri di telefono ecc...

Si rischia altrimenti di vanificare la ricerca degli elementi di prova, sviando l'attenzione dell'analista forense su fatti che, pur essendo sempre reati, possono avere un'importanza irrisoria rispetto al capo d'accusa.

Confrontandomi con periti e colleghi ho notato due differenti approcci all'identificazione degli elementi di prova.

Da una parte c'è chi sostiene l'obbligo di identificare attraverso l'hash ogni dato/file, o almeno ogni dato/file rilevante ai fini dell'indagine, trattato all'interno dell'insieme di dati che costituisce la prova (es. l'immagine acquisita dall'hard disk).

Dall'altra c'è chi sostiene l'esatto opposto, cioè che una volta identificata in maniera univoca la prova, per esempio l'hard disk, attraverso i seriali e gli hash dell'immagine forense dei dati in esso contenuti, sia sufficiente documentare le operazioni effettuate, attraverso la ripetizione delle quali la controparte giungerebbe a rilevare la medesima serie di bit.

Anche a tal riguardo si sente l'esigenza di una regolamentazione, anche al solo fine di tediare giudici tecnicamente (informaticamente parlando) non competenti, con lunghe controversie sul valore esatto dell'hash di un file, prolungando inutilmente i procedimenti con supplementi di perizie, se non rischiando proprio il loro annullamento!

La presentazione: il processo di investigazione della prova digitale si conclude con la sua presentazione all'autorità giudiziari.

In particolare la documentazione da presentarsi dovrà includere:

- informazioni estratte dai dati recuperati, considerando come informazione non il file, per es., di testo, ma l'interpretazione del suo contenuto;
- la correlazione esistente tra informazione digitale e fatto reato;
- descrizione dei procedimenti seguiti durante le fasi di identificazione, preservazione, acquisizione ed analisi;
- i dispositivi ed i software utilizzati;
- i dati estratti/recuperati, presentati su supporto digitale, possibilmente validato con hashing, al fine da prevenire contestazioni relative a possibili successive alterazioni.

