Materiale rieditato nell'articolo:
Introduzione all'informatica forense, in *La sicurezza preventiva dell'informazione e della comunicazione*, P. Pozzi (a cura), FrancoAngeli, 2004

Dar voce alle prove: elementi di Informatica forense

Cesare Maioli
Università di Bologna
maioli@cirfid.unibo.it

1. Informatica forense

In un caso presentato agli studenti di un master in informatica giuridica[1], si sono illustrate le tecniche realmente adottate dagli organi inquirenti, dalla Polizia giudiziaria e dal perito del Pubblico ministero, per altro cultore di materia giuridica all'università, che a fronte di un documento Word, ritrovato circa due anni dopo il presunto crimine su un personal computer di una segreteria di un ente pubblico, aperto a molti utenti e privo di effettive misure di sicurezza, hanno attribuito alla data di creazione memorizzata insieme al documento valore di prova essenziale su cui basare la richiesta di imputazione di alcuni informatici che operavano in quell'ente. Nella vicenda erano coinvolte primarie società di informatica dalle enormi cognizioni e potenzialità.

Gli studenti hanno prontamente osservato che la data rilevata da quel tipo di registrazione è completamente inaffidabile[2] e soprattutto che l'attendibilità dei contenuti, le modalità di prelievo dei *file* indiziati avrebbero dovuto essere molto più tempestive e soprattutto avvallate da garanzie derivanti dall'apposizione della firma digitale[3]. Studenti più evoluti hanno discusso della necessità di *time-stamping*, in aggiunta alla firma digitale, e posto quesiti sul tipo di software con cui vengono, in ogni caso, rilevati i dati da un computer. Questo per valutare l'opportunità di utilizzare codice *open-source* che garantisca la completa trasparenza, indipendenza e verificabilità dalle tecnologie delle operazioni di rilevazione delle prove[4].

Il caso che è relativo a un'imputazione penale in una grande città del Nord da parte di una Procura ben organizzata e di buona fama, in una causa certamente non sotto gli occhi dei mezzi di comunicazione, non è isolato: la preparazione e le attese di giovani laureati in giurisprudenza sulle modalità di indagine in procedimenti in cui l'informatica ha un ruolo centrale, qui per la valutazione delle prove, paiono essere al di sopra della preparazione e dei comportamenti degli inquirenti. Riteniamo che l'esempio introduca con efficacia alcuni temi di **Informatica forense,** la disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova [7]. Gli scopi dell'informatica forense sono di conservare, identificare, acquisire, documentare e interpretare i dati presenti su un computer. A livello generale si tratta di individuare le modalità migliori per ([5]e [9]):

- acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano,
- garantire che le prove acquisite su altro supporto siano identiche a quelle originarie,

---

[1] Master in Informatica giuridica e diritto dell'informatica dell'Università di Bologna (www.cirfid.unibo.it/master).

[2] Almeno dal 1995, finanche i manuali introduttivi di Windows 95 e 98 riportano questa informazione; in [11] si ha un inquadramento più generale.

[3] La prova dell'integrità e dell'autenticità può essere fornita tramite l'uso di sistemi crittografici e di firma digitale; per ogni singolo file o per l'intero hard disk viene calcolato un valore numerico, che funziona come una specie di impronta digitale. Confrontando questo valore prima e dopo l'analisi, si può dimostrare che non sono state introdotte modifiche e che la prova è autentica, perché modificando anche un solo bit, l'intero valore viene calcolato in maniera totalmente diversa. Se questo procedimento viene effettuato alla presenza di testimoni e accuratamente documentato, non ci sono ragioni per contestare l'integrità e la veridicità della prova.

[4] Nonostante alcuni importanti studiosi osservino che il valore giuridico da attribuire a documenti generati da software di informatica forense che sono licenziati secondo un modello proprietario (per tutti [8]) sia nullo, riteniamo che dalla competenza e dall'esperienza dell'informatico forense derivi la consapevolezza di poter esprimere, in scienza e coscienza, valutazioni da trasmettere alle autorità inquirenti in base ai quesiti formulatigli indipendentemente dal tipo di licenza del software utilizzato.

- analizzare i dati senza alterarli.

In sintesi, di “dare voce alle prove”.

L’informatica forense comprende le attività di verifica dei supporti di memorizzazione dei dati e delle componenti informatiche, delle immagini, audio e video generate da computer, dei contenuti di archivi e basi dati e delle azioni svolte nelle reti telematiche.

Importanti aspetti della disciplina riguardano, a un livello di maggior dettaglio, il ruolo della progettazione e mantenimento di una *catena di custodia* e gli argomenti principali da prendere in esame quando si presentano prove in sede processuale.

Il sistema informatico oggetto dell’indagine può essere un personal computer o un server isolato, nel qual caso si parla di *computer forensics*, ovvero può trattarsi di almeno due elaboratori connessi tra loro; in tal caso si parla di *network forensics*.

La disciplina ha origine in ambienti giuridici di *common law* ad alta evoluzione tecnologica come gli Stati Uniti[5] e la Gran Bretagna e ha visto sorgere numerose agenzie specializzate che non solo fornisco servizi di informatica forense ma offrono anche formazione e in qualche caso vendono il *computer forensics tool kit*, valigetta virtuale analoga a quella che l’anatomo-patologo usa per acquisire materiali da utilizzare nelle perizie di medicina legale.

Un data significativa nell’evoluzione della materia è il 1994 allorché il Dipartimento della Giustizia degli Stati Uniti ha pubblicato un insieme di linee guida, il cui ultimo aggiornamento è del 2002, che per accuratezza, autorevolezza ed esaustività hanno fissato uno standard e sono divenute un basilare riferimento per studi e atti successivi [3]. In Italia, oltre a nuclei nei corpi di polizia[6], vi sono aziende di servizi di sicurezza informatica che fra le altre cose forniscono anche servizi di *post incident analysis* di informatica forense.

L’informatica forense agisce **dopo** che un sistema informatico è stato violato per esaminare i reperti informatici in modo esaustivo, completo, accurato, incontaminato e documentato. Il reperto informatico, per la sua natura digitale, è riproducibile e quindi l’esame può e deve avvenire su una copia onde evitare alterazioni, inquinamenti e contraffazioni dell’originale. Un sistema sicuro non può quindi essere fonte di reperti informatici e, per il loro reperimento, si arriva a dover talora utilizzare tecniche di *hacking*.

L’informatica forense serve dopo che sono state utilizzati gli strumenti di risposta a un incidente, allorché intervengono gli organi inquirenti. Come noto, si valuta che alcune centinaia di attacchi avvengano ogni giorno, al mondo, verso sistemi informatici. Essi possono essere portati da un attaccante che, tramite la conoscenza di punti vulnerabili di un obiettivo cerca di penetrare in un sistema informatico ovvero da un programma che automaticamente cerca di individuare i punti deboli di un sistema e penetrarvi. Si genera così l’*incidente informatico* (l’ordinamento giuridico italiano prevede casi nei quali il suo trattamento segua alla querela di parte e casi nei quali si procede d’ufficio). L’azienda di norma si occupa dell’incidente dapprima seguendo le politiche interne di sicurezza e rivolgendosi successivamente agli organi investigativi. Si osserva che da alcuni anni i rischi derivanti da crimini informatici coinvolgono sempre più anche le medie e piccole imprese e non solo le multinazionali e i grandi istituti bancari [4].

2. Gestione delle prove

Se si analizza in dettaglio un qualsiasi personal computer si possono conoscere attività, gusti, pensiero di chi l’utilizza; l’analisi dei sistemi è dunque utile per condurre indagini e per acquisire prove inerenti a eventi legati alla vita del suo utilizzatore.

[5] La data di nascita della Computer forensics è il 1984, quando il laboratorio scientifico dell’FBI e altre agenzie investigative americane iniziarono a sviluppare programmi da utilizzare nell’esame dei dati presenti nei computer. Nello stesso anno, per rispondere alla crescente richiesta di investigazioni in ambito informatico, fu creato, all’interno dell’FBI, il Computer Analysis and Response Team (CART) con il compito fondamentale di procedere nei casi in cui si rende necessaria l’analisi di un computer.

[6] Significativi passi iniziali sono rappresentati dalla creazione, nel 1996, del Nucleo Operativo di Polizia delle Telecomunicazioni, e dalla istituizione, nel 1998, del Servizio di Polizia Postale e delle Telecomunicazioni, all’interno del quale sono confluite le risorse del citato Nucleo e della Divisione della Polizia Postale.

Nel caso di reati informatici il sistema informatico può essere una sorta di arma del delitto o il bene colpito da azioni delittuose; in entrambi i casi l'analisi di immagini dei contenuti delle aree di memorizzazione (*hard disc* e altro), delle aree in cui il sistema operativo memorizza il flusso dei lavori e degli accessi (*log file* e simili), delle aree di memorizzazione temporanea dei dati e dei programmi (memoria *read-only* e *buffer*) può portare all'individuazione di elementi utili alle indagini, indizi o prove.
Da questo segue che l'informatica forense non solo è significativa laddove si verifichino reati informatici ma anche e soprattutto in molte situazioni in campo fiscale, commerciale[7] e, per quanto consta alla nostra esperienza peritale, conferme di alibi, contenzioso del personale con la direzione, rapporti tra un cliente e un istituto di credito, rapporti tra cliente e gestore di servizi di commercio elettronico.
Per l'acquisizione delle prove da un sistema informatico il modo migliore è quello di poter accedere al sistema con il ruolo di amministratore di sistema, senza togliere la corrente elettrica, in modo da poter consultare anche la memoria Ram che viene "cancellata" in caso di spegnimento. In generale, andrà deciso caso per caso se accedere alla macchina accesa o togliere direttamente la tensione in modo da ottenere il più possibile una fotografia del sistema così come era: infatti eseguire uno spegnimento classico comporta sicuramente la cancellazione e l'alterazione di molti dati. Ne emerge la necessità che le autorizzazioni da parte degli Uffici che coordinano le indagini siano da trasmettere in tempi strettissimi a chi effettua materialmente le indagini.
Non meno importante risulta la gestione degli elementi di prova acquisiti, il loro trasporto e archiviazione per evitare che le stesse vengano alterate o comunque possa essere in discussione la loro integrità. A tale scopo risulta utile l'utilizzo di strumenti di firma digitale o la predisposizione di verbali che documenti dall'inizio del procedimento la vita e la custodia delle prove acquisite. La *catena di custodia* permette di garantire che non si sono prodotte alterazioni ai dati dal momento del loro sequestro al momento del dibattimento e per tutte le fasi dell'iter processuale.
Infine, per una corretta documentazione del processo di acquisizione delle prove va attentamente verbalizzata o addirittura filmata tutta la fase di analisi e di ricerca di esse in modo da poter giustificare con chiarezza ogni singola operazione eseguita.
Per quanto riguarda l'autenticazione delle prove va dimostrato che essa è stata eseguita senza modificare o in qualche modo turbare il sistema e le prove stesse vanno autenticate e verificate temporalmente con opportuni programmi di utilità in modo da poter facilmente dimostrare in sede di giudizio che le operazione di riproduzione delle prove è stata eseguita nei modi e nei tempi indicati.
Per l'analisi delle prove occorre rispettare due principi: i dati oggetto dell'analisi non devono venire alterati e, senza entrare qui in dettagli di geometria dei dischi e dei supporti magnetici, un'analisi dettagliata non dovrà essere eseguita solo all'interno dei *file* ma anche nei settori del supporto magnetico lasciati liberi (*slack space*, aree non allocate e aree di *swap* del sistema operativo) che contengono comunque dati registrati e cancellati in precedenza ovvero dati che qualcuno desidera "nascondere".
Come in altri settori forensi, anche nel campo informatico risulta comodo e utile predisporre una lista delle azioni che devono essere eseguite e documentare puntualmente le attività e i compiti svolti in relazione a ciascuna di esse. Il principio di fondo è quello di non dare nulla per scontato e quindi, adattando alla situazione italiana alcune linee guida autorevoli ([2] e [7]):

- va accuratamente verificato lo stato di ogni supporto magnetico,
- vanno ispezionati quaderni, fondi di tastiera e monitor per individuare eventuali *password*,

[7] In Italia dottrina e giurisprudenza relative a temi di informatica forense sono presenti per: riciclaggio di denaro e reati tributari, omicidio intenzionale, frodi alle assicurazioni, uso per scopo personale delle attrezzature informatiche del datore di lavoro, decriptazione di dati, violazione del diritto d'autore, abusi sessuali, distruzione di dati o accesso abusivo e conseguente estrazione non autorizzata di dati, alterazione di dati od uso improprio di programmi, detenzione e distribuzione di materiale pornografico, uso improprio della posta elettronica, diffamazione, contratti a oggetto informatico.

- va ricostruita (*tracing*) l'attività di un accesso abusivo dalla rete[8],
- vanno individuati virus e altro software malevolo[9],
- va ricostruita la successione dei compiti e delle azioni,
- vanno confrontati tra loro gli indizi,
- va individuato il ruolo che assume il sistema oggetto della indagine,
- va considerato il ruolo delle persone che utilizzano il sistema per individuare eventuali individui indiziati, informati dei fatti o in grado di rivelare la *password*[10],
- va effettuato un accurato inventario delle attrezzature ispezionate,
- è opportuno ripetere due volte le analisi per avere certezza della meticolosità delle operazioni eseguite.

3. La valigetta dell'informatico forense

Utilizzare una metodologia corretta non significa solo non perdere prove, ma significa anche mantenere la credibilità dei dati raccolti. In una qualunque indagine, una delle prime attività solitamente compiute è quella di isolare la scena del crimine, per evitare l'accesso alle persone non autorizzate, ricercare impronte digitali, effettuare una descrizione accurata dell'ambiente unitamente a fotografie e filmati.[11]

Il luogo deve essere attentamente controllato per cercare appunti, diari, note dai quali si possano eventualmente ricavare password o chiavi di cifratura.

In caso di sequestro delle attrezzature la macchina e i dischi devono essere opportunamente imballati e conservati e devono essere apposte etichette e sigilli. Deve essere indicato chi ha raccolto le prove, come le ha raccolte, dove, come sono conservate e protette, chi ne ha preso possesso, quando e perché.

Devono essere osservate opportune cautele affinché le prove non siano maneggiate da personale non autorizzato e siano conservate in luoghi sicuri e adeguatamente presidiati. L'obiettivo non è solo quello di proteggere l'integrità della prova ma di evitare che la mancanza di una custodia appropriata sia eccepita nel processo.

Ogni attività deve essere documentata. I rapporti devono essere esaustivi: le scoperte fatte, gli strumenti utilizzati (quale software, incluso il riferimento alla versione), la metodologia usata per analizzare i dati vanno indicati e va altresì fornita una spiegazione di quello che è stato fatto, del perché, del chi e del tempo impiegato.

---

[8] A tal fine è necessaria un'approfondita conoscenza dei protocolli di rete e dei server di posta elettronica in modo da poter individuare il punto di partenza dei dati e dei messaggi stessi. In questa attività si dimostrano particolarmente utili i sistemi di IDS (Introduction Detective System).

[9] Per codice malevolo [5] si intende il software che è utilizzato per ottenere e mantenere un potere o un vantaggio non autorizzato su un'altra persona; modalità tipiche del suo utilizzo riportate in letteratura comprendono: accesso remoto, raccolta dati, sabotaggio, blocco di un servizio (*denial of service*), intrusione in un sistema, furto di risorse informative, circonvenzione dei meccanismi di controllo degli accessi, necessità di riconoscimento di stato sociale, autosoddisfazione (l'*hacker* buono).

[10] L'analisi comportamentale e la ingegneria sociale di solito consentono di affinare la ricerca delle persone colpevoli di reati. La seconda fa riferimento principalmente alle modalità con cui password e simili informazioni riservate vengono carpite da persone ignare e non coinvolte nel reato; la prima consente di effettuare una correlazione tra i dati acquisiti e le modalità di azione di una persona sospetta. I suoi passi tipici vanno dalla definizione di un insieme di sospetti alla comprensione dei possibili motivi di comportamento doloso, per poi effettuare le interviste alle persone interessate e gli interrogatori ai sospetti, comprendere eventuali errori compiuti da chi gestisce la sicurezza.

[11] Nel caso di un reato informatico, la descrizione della scena del crimine dovrebbe comprendere, oltre alla foto dell'ambiente in generale, una fotografia dello stato delle connessioni presenti sul retro del computer e, se il computer è acceso, dell'immagine presente sullo schermo, dei numeri seriali e delle altre caratteristiche identificative. Le linee guida statunitensi sono talora estremamente dettagliate e attente, per esempio

- avvertono che nella ricerca delle impronte digitali sul computer non va usata la polvere di alluminio che è un conduttore di elettricità e potrebbe alterare le magnetizzazioni,
- suggeriscono i formati delle etichette che servono a identificare ogni possibile fonte di prova e i dati da includere: il numero del caso, una breve descrizione, la firma, la data e l'ora in cui la prova è stata raccolta.

Deve essere applicato un sistema di verifica e di registrazione dei procedimenti usati, che renda possibile la ripetizione da parte di terze parti.
Di norma, si ha l'accortezza anche di conservare una copia del software usato perché solitamente i programmi vengono aggiornati di frequente, mentre i processi durano anni.

Con la crescita di complessità ed estensione dei sistemi informatici, la ricerca di prove al loro interno tramite programmi di utilità forniti dai principali costruttori o realizzati autonomamente appare sempre più difficile: sono state così prodotti sistemi digitali dedicati e appositamente progettati come strumento di ausilio all'indagine di informatica forense.
Dal punto di vista del metodo, un'indagine di informatica forense non avviene mai sul sistema informatico originale ma, per motivi pratici e legali, tutte le volte possibili vengono effettuate copie dei dati e dei sistemi su cui lavorare in un secondo tempo.
Gli strumenti di indagine appartengono a due famiglie: sistemi che eseguono alcune funzioni specializzate e stazioni di lavoro per l'informatica forense; i primi comprendono software di visualizzazione di *file* testo nei vari formati[12], software di visualizzazione di *file* immagini nei vari formati[13], programmi tradizionali che esaminano singolarmente i settori di un disco senza alterarli[14], programmi che consentono di ricercare parti di testo in enormi archivi dove sono memorizzati *file* in vari formati[15], programmi che consentono di avere copia dell'immagine intera dei contenuti di un disco[16]. Per i secondi si tratta di sistemi che raccolgono, copiano e analizzano i dati e costituiscono propriamente i *computer forensics tool kit*.
Alcuni di questi sono specializzati per i sistemi Windows NT, altri per Unix o Linux; esistono almeno due importanti sistemi che mettono a disposizione tutte le funzionalità necessarie per una analisi di informatica forense onnicomprensiva[17].
Le funzionalità che caratterizzano tali strumenti sono tipicamente le seguenti:
- possibilità di eseguire ricerca velocemente sull'intero supporto magnetico (non solo all'interno dei *file* ma anche sulla superficie non utilizzata dei dischi),
- possibilità di produrre copie dei dischi a basso livello (copia settore per settore),
- utilizzabilità su più tipi di *file system*,
- possibilità di combinare in modi diversi i risultati delle ricerche eseguite,
- analisi dei dati secondo varie modalità di codifica (per esempio ASCII ed esadecimale),
- recupero automatico di eventuali *file* apparentemente cancellati,
- stampa e riproduzione, previa scelta dei parametri, delle prove ai sensi dei principi processuali di *civil law* (per esempio dei codici di procedura civile e penale).

4. La didattica dell'informatica forense

Sono numerosi i corsi esistenti negli Stati Uniti e in altri Paesi europei tenuti soprattutto dalle case produttrici di software e stazioni di lavoro commerciali; corsi per il personale interno sono svolti anche in ambito delle organizzazioni statali di polizia e di *intelligence*. Le associazioni professionali degli operatori giuridici e degli avvocati da tempo prevedono corsi di base.
In Italia cominciano a sorgere iniziative a livello accademico spesso come tema derivato o collaterale a corsi relativi alla sicurezza dei sistemi; in campo giuridico vi sono importanti studi che esaminano l'evoluzione del concetto di documento, in una prospettiva di influenza della tecnologia sul diritto (per esempio [10]) e corsi di nuova attivazione sui crimini informatici e su argomenti di

[12] Per esempio, Quick View Plus per i sistemi Windows e Conversion Plus per i Macintosh.
[13] Per esempio, Thumbplus.
[14] Per esempio, Unerase di Norton.
[15] Per esempio, dtSearch.
[16] Essi includono *slack space*, aree non allocate e *file di swap*; per esempio, SafeBack, SnapBack, Ghost, dd di Unix.
[17] New Technology Incorporated composto da molti strumenti collaudati che utilizza un'interfaccia a comandi testuali ed Encase che ha un'interfaccia grafica.

informatica forense legati al diritto penale, all'informatica giuridica e al diritto privato dell'informatica[18]; varie università organizzano cicli di seminari [19].
Alla luce di quanto sta emergendo, riteniamo che un corso di informatica forense nell'ambito del corso di studio di giurisprudenza o di operatore informatico-giuridico, che già comprenda le discipline basiche del diritto (diritto costituzionale, civile, penale, amministrativo, procedure, ecc.) e quelle di base dell'informatica giuridica, debba comprendere i seguenti contenuti: principi di criminologia, modalità di attacco ai sistemi informatici, metodi di accesso ai sistemi informatici e di trasmissione dati, comportamenti dei più diffusi *file system*, struttura degli strumenti di memorizzazione, dei sistemi di compressione, di crittografia e di steganografia, applicazioni internet, prove informatiche (acquisizione, integrità, attendibilità), validazione temporale dei dati (compresa la stima delle date di utilizzo dei *file* utilizzando date riferite ad altri eventi temporalmente confrontabili), strumenti e tecniche di effrazione degli strumenti informatici di sicurezza, prove informatiche (acquisizione, integrità, attendibilità), redazione di atti peritali.
Inoltre, sono state avviate esperienze didattiche in corsi di laurea di base con lezioni istituzionali e cicli di seminari [6], in corsi professionali per le forze di polizia e in scuole master di secondo livello rivolto a laureati. In particolare agli studenti del master, di cui si è accennato in apertura, sono stati forniti elementi su: ingegneria del software, crittografia e firma digitale, privacy, commercio elettronico, oltre ai temi tradizionali [10] di diritto dell'informatica per arrivare a svolgere il modulo di informatica forense che ha compreso: prove civili atipiche, diritto penale dell'informatica, prove e strumenti informatici in campo penale, prove e strumenti informatici in campo civile, mezzi di acquisizione delle prove su computer, mezzi di acquisizione delle prove in rete, *computer crimes* e nuove modalità di indagine, *digital forensics* e informatica forense. Associazioni di operatori del diritto e associazioni di informatici hanno dato origine a vari incontri interdisciplinari dove, spesso partendo da questioni legate alla sicurezza, si è parlato di informatica forense[20].

5. Referenze

[1] Anastasi J., *The new forensics*, Wiley, 2003
[2] Casey E. (editor), *Handbook of Computer Crime Investigation*, Academic Press, 2002
[3] *Federal Guidelines for Searching and Seizing Computer*, US Department of Justice, 1995
[4] Forte D., *Le attività informatiche a supporto delle indagini giudiziarie*, Il Diritto dell'Er@ di Internet, Mucchi, Modena, 2001
[5] Kruse W. G. e J.G. Heiser, *Computer Forensics, Incident Response Essentials*, Addison-Wesley, 2002
[6] Maioli C., *Elementi di Informatica per l'Informatica Giuridica*, Pioda, Roma, 2002
[7] Marcella A. J. e R. Greenfield (editor), *Cyber Forensics*, Auerbach, 2002
[8] Monti A., *Attendibilità dei sistemi di computer forensics*, Ict-Security, n. 9, 2003
[9] *Electronic crime scene investigation: a guide for first responders*, NIJ Guide, Department of Justice, 2001
[10] Pascuzzi, *Il diritto nell'era digitale*, Il Mulino, 2002
[11] Rapetto U. e R. Di Nunzio, *Le nuove guerre*, RCS, 2001
[12] Stephenson P., *Investigating Computer Related Crime*, CRC Press, 2000

[18] Per esempio, Computer crime e cybercrime di L. Picotti (www.jus.unitn.it/faculty/guida/corsi/dir_pen_informatica) , 2003.
[19] All'Università di Bologna si tratta di 24 ore con i seguenti argomenti: la struttura dei supporti di memorizzazione e di comunicazione informatica, le misure di sicurezza, i reati informatici e gli illeciti civili, la natura delle prove informatiche, l'acquisizione delle prove informatiche, le tecnologie per l'acquisizione delle prove informatiche, l'analisi dei dati senza loro alterazione, l'attività della Polizia Giudiziaria e l'attività del Consulente Tecnico nella predisposizione di una perizia, la valutazione delle prove informatiche.
[20] Un esempio recente è il Primo Forum Italiano *Incident response nella sicurezza informatica* del giugno 2003, organizzato a Milano dall'AICA.