

UNIVERSITÀ DEGLI STUDI DI CAMERINO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Corso di Laurea Specialistica in Informatica

Dipartimento di Matematica e Informatica



Metodi e Modelli nella Digital Forensics in Italia: Ipotesi di uno strumento di mapping

*Tesi di Laurea Sperimentale
in
Reti di Elaboratori*

Laureando:

Maurizio Torcasio

Relatore:

Dott. Fausto Marcantoni

Correlatore

Dott. Andrea Lazzari

Anno Accademico 2006 / 2007

In memoria

Cristian Torcasio

♠ 13/09/2007

Abstract

Facendo una semplice indagine su come ci si stia muovendo in Italia nell'ambito della ricerca delle prove informatiche, le cosiddette “digital evidence”, si può notare che siamo ancora in un settore molto giovane alla ricerca di linee guida generali e condivise.

Però al proliferare di corsi universitari sulle indagini forensi con contenuto informatico giuridico, di tools per l'analisi forense, di una qualche apertura da parte della magistratura al riconoscimento delle prove digitali in ambito processuale, spesso non corrisponde un'effettiva ricaduta omogenea di competenze nell'ambito effettivo di chi si occupa di indagini e/o sicurezza.

Proprio di questi giorni il furto con destrezza dell'hard disk di un giudice a Napoli all'interno del tribunale contenente almeno 3 anni di informazioni riservate e di dati sulle indagini ancora in corso, ci fa capire come non sia ancora presente una consapevolezza dell'importanza di proteggere le informazioni. Come invece sia evidente la mancanza di una cultura della sicurezza attiva delle informazioni sensibili ai fini della sicurezza dello Stato: le cosiddette “informazioni classificate”. Come pure manca una consapevolezza nella necessità di gestire l'accesso sicuro ai luoghi (tribunali), effettuare copie di sicurezza (backup) e della cifratura dei dati sensibili (crittografia). Tutto ciò contrariamente a quanto succede ad esempio nei principali paesi anglofoni (America[10][11][12][23], UK [13][9], Australia[24][15]) dove le stesse istituzioni producono documenti di riferimento per la gestione dell'informatica forense [11] e della sicurezza.

Questo lavoro vuole essere il punto di partenza per la creazione di una mappatura aperta ma condivisa sui vari ambiti della digital forensics e sui vari soggetti che gravitano in questo settore, dagli universitari, alle varie forze di polizia, dai giudici ai criminali con i loro profili. L'obiettivo è quello di fornire una base di discussione

condivisa che consenta di tracciare linee guida per i protagonisti della digital forensics al fine di realizzare una prima procedura, oramai necessaria, al fine di gestire i problemi di interpretabilità giuridica della norma rispetto alle attuali best-practice per giungere ad una check-list riconosciuta a tutti i livelli di competenza.

Parole chiave: cyber network computer digital forensics

Indice Generale	4
Ringraziamenti	6
Premessa	7
Capitolo 1: Introduzione	8
1.1 Ma cos'è la Digital Forensics?	11
1.2 L'Ipotesi di Mappa	15
1.3 Domini implicati nella Digital Forensics	17
Capitolo 2: Quali sono le procedure adottate all'estero?	18
2.1 Cosa propongono le aziende private di consulenza	19
2.2 Cosa fanno le istituzioni: il caso inglese	22
2.3 Cosa fanno le istituzioni: il caso americano	25
Capitolo 3: Cosa succede in Italia	28
3.1 Lo stato dell'arte	28
3.2 Le leggi	31
Capitolo 4: Le mappe	34
4.1 La mappa principale: Digital Forensics	36
4.1.1 Definizione di Digital Forensics	36
4.1.2 Oggetto della Digital Forensics	36
4.1.3 Domini coinvolti dalla Digital Forensics	37
4.1.4 Le categorie della Digital Forensics	37
4.1.5 Principi fondamentali	38
4.1.6 La mappa della Digital Forensics	39
4.2 La prova digitale	40
4.2.1 Cosa si intende per prova digitale	40
4.2.2 Valore probatorio di una prova digitale	40
4.2.3 Cosa da alla prova digitale valore probatorio	41
4.2.4 Procedure di ottenimento della prova digitale	41
4.2.5 Problemi aperti.	41
4.3. La Giurisprudenza	43
4.3.1 La mappa della giurisprudenza	43
4.3.2 Reati	43
4.3.3 La Procedure del c.p.p e quelle operative	44

4.3.4 I Soggetti coinvolti	44
4.4. La tecnologia	45
4.4.1 L'Hardware	46
4.4.1.1 Small Scale Digital Device	47
4.4.1.2 Storage Device	48
4.4.1.3 Obscure Device	49
4.4.1.4 Network Device	50
4.4.2 Software	51
4.4.2.1 I Sistemi Operativi	51
4.4.2.2 Strumenti (Software) di analisi	52
4.4.2.3 Tipologie di File System	53
Capitolo 5: Questioni aperte	54
Capitolo 6: Conclusioni	55
Glossario	56
Allegato A: Mappa di Brinson ad albero	61
Allegato B: Mappa di Brinson grafica	63
Bibliografia, Riferimenti, Weblografia	64

Ringraziamenti

In primis ringrazio mia moglie Antonella perchéè mia moglie e mi sopporta assecondando da sempre la mia passione informatica e mio figlio Andrea, che ho coinvolto suo malgrado nella stesura delle mappe, e anche se “soffre” in questo periodo la mia latitanza di padre, non me lo fa pesare.

Ringrazio il direttore del corso di Informatica dott. Flavio Corradini per la sua disponibilità ad ascoltare le mie proposte di tesi, indirizzandomi e consigliandomi.

Ringrazio il mio relatore, dott. Fausto Marcantoni, per aver accettato senza riserve la mia proposta di tesi fornendomi il necessario supporto scientifico e il dott. Andrea Lazzari mio correlatore che mi ha costantemente seguito nello sviluppo della tesi, dandomi preziosi consigli.

Inoltre ringrazio l'avv. Marco Vitali del Foro di Pesaro, collega e amico per la supervisione degli aspetti giuridici e con lui il maresciallo Lorenzetti della Polizia Giudiziaria di Pesaro.

Infine ringrazio gli ispettori Paolo Silvestri e Raffaello Desiati della PolPost di Bolzano che mi hanno permesso di conoscere le procedure adottate dalla polizia delle poste e telecomunicazioni, confermandomi che sull'argomento c'è molto interesse, oltre alla necessità di avere delle linee guida condivise.

Premessa

L'obiettivo di questa tesi è quello di creare una base di discussione basata su mappe mentali che porti alla creazione di una serie di mappe condivise sulle procedure di cyber/network/computer/digital forensics in Italia

Capitolo 1

Introduzione

Si dice che il computer e l'informatica siano ormai parte della vita di tutti noi. Tecnicamente sarebbe più preciso parlare di tecnologie di comunicazione e trasmissione dell'informazione, le cosiddette ICT (Information and Communication Technology).

Purtroppo fanno anche sempre più parte del lato oscuro della vita, quello legato ai reati. Si sente sempre più spesso che persone siano state truffate o peggio derubate dei loro soldi attraverso l'uso delle tecnologie informatiche, ai più oscure e bizzarre.

I giornalisti tendono come sempre ad enfatizzare utilizzando parole ad effetto come hacker, pirata informatico, cyber crime, ecc. per poter etichettare meglio cose che non conoscono a pieno.

Ci sono poi coloro che commettono altri tipi di reati, dove lo strumento informatico è solo un nuovo mezzo, tecnologicamente evoluto, per poter soddisfare le loro necessità bestiali, i pedofili.

Oppure l'uso delle tecnologie dette web 2.0, tanto per citare, Youtube, dove è di "moda" inviare filmati su gesta criminali, che vanno dal bullismo a scuola alla gara in moto in autostrada a 200 all'ora, allo stupro dell'adolescente da parte del branco.

Infine c'è chi usa la tecnologia informatica a fini terroristici, o mafiosi.

L'elenco ovviamente non finisce qui, ma questi sono i casi attualmente più eclatanti.

Tutto questo porta da parte delle forze di contrasto alla criminalità, cioè potere

legislativo, giuridico, esecutivo a trovarsi spesso in ritardo nella formazione tecnologica, fino a casi paradossali [25], portando così alla perdita di opportunità nella ricerca e scoperta di prove certe da poter utilizzare in sede di giudizio.

Nasce, come già è avvenuto in altri paesi, la necessità di avere una serie di strumenti, di standard [16], di formalizzazioni [17], linee guida, best practice, procedure, corsi di formazione di base e avanzata [15] al fine di contrastare efficacemente le azioni criminose compiute attraverso l'uso delle tecnologie informatiche, come anche di persone tecnicamente preparate in quel settore dell'informatica che viene da alcuni chiamato computer forensics e da altri digital forensics.

1.1 Ma cos'è la digital forensics?

Se partiamo dall'inizio abbiamo una prima definizione già presente in "DFRWS TECHNICAL REPORT: "A Road Map for Digital Forensic Research" Report From the First Digital Forensic Research Workshop (DFRWS) [18] ma coniata da Brian Carrier, che in [19] intanto la eleva a scienza tant'è che la chiama Digital Forensics Science e che definisce così:

Digital Forensic Science

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

L'uso di metodi derivati e verificati scientificamente per la conservazione, l'accumulazione, la convalida, l'identificazione, l'analisi, l'interpretazione, la documentazione e la presentazione di prove digitali derivate dalle fonti digitali allo scopo di facilitare o permettere la ricostruzione degli eventi criminali, o contribuire a prevenire le azioni non autorizzate che potrebbero essere pericolose e potenzialmente distruttive rispetto alle operazioni pianificate [N.d.A in un sistema informativo].

Nell'ultima periodo si parla implicitamente anche di sicurezza "*helping to anticipate*

unauthorized action.....”.

Di fatto sicurezza informatica e digital forensics sono due facce della stessa medaglia. Cioè la gestione della sicurezza delle informazioni e le loro implicazioni legali. Quindi è possibile affermare che la sicurezza informatica ha come obiettivo la prevenzione della manipolazione non autorizzata dell'informazione, la digital forensics ha come obiettivo l'evidenziazione del dato digitale rilevante ai fini giuridici.

Diciamo anche che questa definizione è quella che condivido. Se cerchiamo invece in Italia troviamo che ad esempio, Denis Frati [20] più sinteticamente la definisce così:

*“La digital forensics è la scienza che consente,
attraverso l'uso di specifiche metodologie e tools,
l'individuazione, la conservazione e l'analisi delle prove digitali.*

Dove per prova digitale intende:

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

Mentre Andrea Ghilardini [21] dice in una sua intervista

*“La Computer Forensics è la disciplina che si occupa della preservazione,
dell'identificazione, dello studio, della documentazione di computer, o sistemi
informativi in generale, al fine di evidenziare l'esistenza di prove nello svolgimento*

dell'attività investigativa». Tradotto nella vita di tutti i giorni, significa che la nostra specialità [N.d.A. quella di informatici forensi...] è quella di esaminare media digitali e sistemi tecnologici al fine di estrarre le evidenze [N.d.A. prove] richieste per dimostrare o confutare il quesito che ci è stato posto.”

Se invece ci rivolgiamo ad esperto di scienze giuridiche come il Prof. Giovanni Ziccardi [22] che afferma:

“Scienza forense

- E' lato sensu la scienza che studia il valore processuale di determinati accadimenti ai fini della costituzione di fonti di prova.*

e poi che

“Per computer forensics si intende quella scienza che studia il valore che un dato correlato a un sistema informatico o telematico può avere in ambito giuridico, o legale che dir si voglia (Ziccardi, 2006, definizione volutamente estremamente restrittiva).”

Dove il valore è inteso come

- la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice e delle partiprocessuali in ordine alla genuinità, non ripudiabilità, imputabilità e integrità del dato stesso e dei fatti dallo stesso dimostrati.”*

Come si può notare l'uno parla di digital forensics e l'altro di computer forensics, di prova e di valore del dato, ma tutti nella sostanza parlano degli stessi concetti utilizzando però aggettivi diversi. Da questo appare già evidente come sia complesso già in fase di nomenclatura avere una idea chiara e condivisa sull'argomento.

1.2 L'Ipotesi di Mappa

Ho quindi ipotizzato che fosse necessario prima di tutto definire una base di conoscenza comune sulla quale poi sviluppare e approfondire i vari argomenti.

Innanzitutto l'idea di utilizzare come strumento di analisi una mappa mi è venuta dalla lettura di un recente articolo di Brinson [1] dove viene proposta una struttura gerarchica ad albero che viene definita essere una ontologia "minore" o con la "o minuscola" derivata dalla definizione data da Tomas Gruber [2]

What's Ontology?

"Short answer: An ontology is a specification of a conceptualization."

ma meglio definita sempre da Gruber [3] [4].

La struttura della mappa proposta da Brinson tiene conto della situazione giuridica, militare ed universitaria americana che è chiaramente diversa dalla nostra.

Appare quindi evidente, e questo è un primo proposito di questa tesi, che è necessario riformulare la mappa, primo, per tener conto della complessa realtà Italiana, secondo, perché è carente in alcuni aspetti.

Riportiamo di seguito nella pagina successiva la mappa di Ashley Brinson, secondo una struttura ad albero limitatamente ai primi 3 livelli.

- **Cyber Forensics**
 - Technology
 - Hardware
 - Large Scale Digital Device
 - Small Scale Digital Device
 - Computers
 - Storage Device
 - Obscure Device
 - Software
 - Analysis Tools
 - Operating System
 - File System
 - Profession
 - Law
 - Enforcement
 - Courts
 - Academia
 - Research
 - Education
 - Military
 - Offensive
 - Defensive
 - Private Sector
 - Consulting
 - Industry

La versione estesa si trova nell'allegato A in forma gerarchica testuale e nell'allegato B in forma di mappa grafica. Anche qui è possibile notare che l'uso dell'aggettivo *cyber* al posto di *digital* vuole essere una forzata differenziazione, legata più al concetto narrativo-giornalistico-giuridico di *cyber-crime*, che porta solo ad una inutile complicazione nella nomenclatura, anche se già questa prima suddivisione, limitata ai primi tre livelli, è abbastanza condivisibile.

1.3 Domini implicati nella Digital Forensics

Questa mappa ha come primo vantaggio la possibilità di consentire di estrapolare quali sono i domini principali che vengono coinvolti in una indagine con contenuto informatico. Nella figura di seguito riportata vediamo, a differenza della precedente rappresentazione ad albero, come i domini mappati non siano totalmente disgiunti ne abbiano solo punti di contatto ma anche intersezioni pronunciate. Si può notare anche come il dominio legislativo sia quello con maggiori intersezioni.

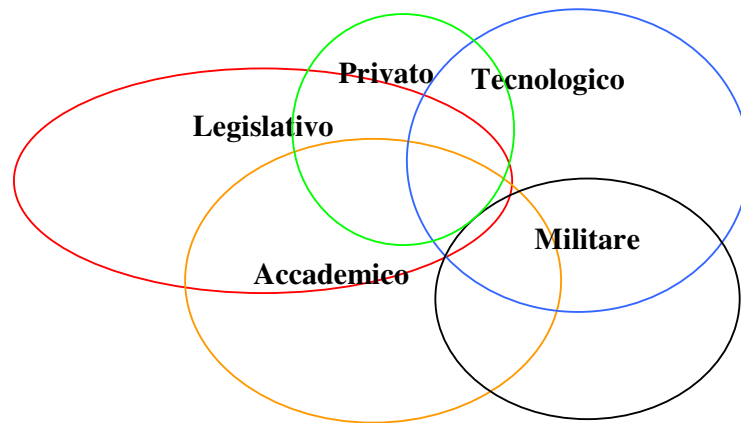


Fig. 1 Domini della Digital Forensics

L'aspetto problematico e cruciale sta nei punti di contatto e intersezione tra i vari domini. Cioè quando competenze diverse e professionisti specializzati entrano a contatto tra loro, dando luogo a problemi di incomprensione, di procedure non scientificamente formalizzate, di protocolli non condivisi.

Capitolo 2

Quali sono le procedure adottate all'estero?

Ovviamente non è possibile in questa sede sviluppare un discorso completo su tutte le procedure o best practice utilizzate al di fuori dell'Italia.

Prenderemo quindi in esame quelle considerate più aggiornate sul piano tecnico e legislativo (sottolineo che la legge non è quella italiana), senza tralasciare però lo sviluppo storico delle stesse.

Quest'analisi è peraltro importante perché ci da una serie di informazioni utili allo scopo di chiarire meglio perché certe soluzioni debbano o possano essere adottate o meno in Italia.

2.1 Cosa propongono le aziende private di consulenza

Potremmo partire ad esempio da quanto già Joan E. Feldman, fondatore della forensics.com, proponeva nel 2001 [5], cioè “le 10 cose più importanti da fare per collezionare prove elettroniche” (notare ancora l’uso di elettronico al posto di digitale) dove risulta interessante oltre all’elencazione delle 10 azioni da fare, l’approccio mediante check-list.

In particolare nelle fasi iniziali dell’indagine in cui è necessario scrivere su un apposito documento se e quali computer sono presenti in un ipotetico luogo del possibile reato, cioè la cosiddetta *Check-list for System Discovery* dove si consiglia di verificare i seguenti punti:

Check-list for System Discovery	
	Descrivere l’aspetto dei sistemi computerizzati, includendo il numero e il tipo di computer, e il tipo di sistema operativo e di sw applicativo utilizzato. Quando si chiede in merito ad ogni tipologia di sw installato, assicurarsi di chiedere nome dell’autore del sw, nome del programma, versione del programma
	La struttura di ogni sistema di posta elettronica, incluso il sw utilizzato, il numero degli utenti, la posizione dei file di posta, e l’uso delle password
	La struttura di ogni rete, inclusa la configurazione dei server di rete e delle workstation, e la marca e il numero di versione del sistema operativo di rete in uso
	Lo specifico sw utilizzato. Questo include applicativi sw per la gestione di cose quali calendari, project management, gestione utenti, elaborazione testi, gestione di database. Sono anche inclusi programmi specifici per l’industria, programmi proprietari, sw per la crittografia, programmi di utilità. Quando si domanda in merito al sw verificare quando è stato installato e quando è stato aggiornato
	L’elenco del personale responsabile delle operazioni in corso, di quelle di mantenimento, di espansione e manutenzione della rete
	L’elenco del personale responsabile della amministrazione del sistema di posta elettronica
	L’elenco del personale responsabile del mantenimento delle informazioni elaborate (record) del modo in cui tali informazioni (record) sono organizzate e recuperate
	I processi di archiviazione e recupero dei supporti di backup sia interni che esterni
	Le procedure usate dagli utenti di sistema per loggarsi sul computer e sulla rete. Questo comprende l’uso di password, audit trails, ed altre misure di sicurezza usate per identificare la data di creazione modifica o eventualmente

	di accesso
	Se e come l'accesso a particolari files è controllato. Informazioni come quelle di una access control list identificano quali utenti hanno avuto accesso a quei files
	Come i file condivisi sono strutturati e identificati nel sistema
	Routines per archiviare e differenti tipi di dati

Proseguendo è necessario annotare anche nella *Check list dei supporti elettronici*, ma sarebbe meglio dire dei *supporti digitali*, cosa viene effettivamente recuperato

Check list dei supporti elettronici	
Data files	
	Office desktop computer/workstation
	Notebook computer
	Home computer
	Computer del personale di segreteria /dello staff/ degli assistenti
	Palmtop
	Network file servers/mainframe/mini-computer
Backup tapes	
	System-wide backups (mensile/settimanale/incrementale)
	Disaster recovery backups (memorizzati esternamente)
	Backups personali o ad hoc (occhio ai dischetti a ad altri supporti portatili)
Altri supporti	
	Archivi su nastro
	Supporti rimovibili/sostituibili
	Floppy disk ed altri supporti portatili (CD, ZIP)

Infine tenere traccia, etichettandoli in modo univoco, nella cosiddetta "*Check list dell'esame dei supporti elettronici*" ogni evento particolare che si produce durante l'analisi dei supporti trovati

Check list dell'esame dei supporti elettronici	
	Assegnare un unico numero per ogni supporto digitale
	Proteggere dalla scrittura tutti i supporti
	Testare tutti i supporti sui virus. Memorizzare ogni virus trovato e notificare immediatamente la parte prodotta
	Stampare la lista delle directory di ogni supporto. Assicurarsi di stampare anche il numero del supporto

	Verificare la mancanza di virus e di dati sui supporti utilizzati per le copie dei dati (ogni copia deve essere fatta su un supporto distinto, dedicata solo ad un singolo caso)
	Recupera i dati di ogni supporto (floppy disk) in un file con un nome che corrisponde al numero assegnato al supporto
	Verificare che tutti i file nell'elenco delle directory appaia nella copia
	Metti in luogo sicuro i supporti originali
	Quando stampi un particolare documento, inserisci una intestazione o piè di pagina con l'indicazione del percorso completo del documento stampato (es: Disk 123\corr\pistolafumante.txt)

Concetto ripreso e aggiornato sempre da Feldman [6] "Ten Steps to Successful Computer-Based Discovery" che sinteticamente riportiamo di seguito.

1. Inviare una lettera (N.d.A.: ufficiale) di conservazione delle prove.
2. Includere nel documento definizioni, istruzioni, e domande specifiche sui dati digitali scoperti
3. Prendete un 30(b),(6) (N.d.A. modulo ufficiale) per la deposizione del personale impiegato ai sistemi informativi.
4. Raccogliere i nastri di backup
5. Raccogliere CD-ROM, (N.d.A.: e DVD) "Zip" Drive, e altri supporti rimovibili
6. Chiedere ogni testimonianza sul computer in uso
7. Fare la copia immagine
8. Proteggere in scrittura e dai virus tutti i media
9. Preservare la catena di custodia
10. Assumere un esperto

Ovviamente l'ultimo punto è un chiaro invito all'utilizzo dei servizi della società di Feldman, visto che non dice mai chiaramente come ad esempio devono essere preservate le prove o come fare una copia immagine, ma il decalogo è interessante perchè consente di avere un filo conduttore sulle principali cose da fare anche se con pochi approfondimenti scientifici.

2.2 Cosa fanno le istituzioni: il caso Inglese

Prendendo il documento prodotto dalla ACPO 'Association of Chief Police Officers' Inglese, "Good Practice Guide for Computer-Based Electronic Evidence" [13] vediamo come il documento si focalizzi sull'importanza della validità delle prove sul piano legale e specifichi chiaramente a chi si rivolge il documento oltre a specificare il fatto che l'obiettivo è quello di fornire una guida a coloro che si trovano a dover reperire prove informatiche senza invalidarle, così come si fa, ad esempio con le impronte digitali o con la ricerca del DNA.

Infatti il documento inizia indicando quali persone possono trarre beneficio dalle best practice indicate e cioè:

1. **Personale che per lavoro frequenta la criminalità e/o le scene di un crimine o ha contatto con una vittima / testimone / sospetto** che deve:

garantire il sequestro e il trasporto di attrezzature sulle scene di ricerca al fine di recuperare prove elettroniche all'interno di computer, nonché l'individuazione delle informazioni necessarie per indagare sulla criminalità che sfrutta l'alta tecnologia.

2. **Gli investigatori** che devono:

pianificare e gestire l'identificazione, la presentazione e la memorizzazione di prove elettroniche reperite all'interno di computer.

3. **Personale e/o Staff di recupero delle prove** (N.d.A. Analisti) che deve occuparsi di:

recupero e la riproduzione delle prove elettroniche reperite all'interno di computer sequestrati (N.d.A. dagli investigatori) da parte di personale preparato appositamente a tale funzione e che ha avuto una formazione specifica nella definizione di prove valide (N.d.A. in base ai principi giuridici del paese in cui è commesso il reato) in un tribunale. Coloro i quali non abbiano ricevuto tale

formazione e che non sono in grado di adeguarsi a tali principi non dovrebbero fare parte di questa categoria di persone

4. **Consulenze esterne (come) testimoni (leggasi periti) (di parte):** Si deve operare: La selezione e la gestione delle persone che possono assistere a contribuire al recupero, l'identificazione e la Interpretazione di prove elettroniche reperite all'interno di computer

Lo stesso documento di seguito propone i 4 principi fondamentali che per la loro importanza andiamo ad elencare:

Principio 1: Nessuna azione deve essere presa dalle forze della legge o dai loro agenti che possano cambiare lo stato dei dati su un computer o sui supporti di memorizzazione digitali che possano portare al loro rigetto in sede di dibattimento in Corte.

Principio 2: Nel caso in cui una persona trovi necessario accedere ai dati originali memorizzati su un computer o su supporti di memorizzazione digitali, quella persona deve essere competente a farlo e deve essere in grado di dare prova di ciò giustificando la rilevanza e le implicazioni della sue azioni.

Principio 3: Deve essere creata e preservata una traccia o una memoria di tutti i processi applicati sulle prove elettroniche reperite all'interno di computer. Ciò deve consentire a terze parti di essere in grado di esaminare quei processi a raggiungere gli stessi risultati.

Principio 4: La persona incaricata dell'indagine ha la totale responsabilità di assicurare che la legge e tutti questi principi siano rispettati.

Nello stesso documento troviamo anche alcune importanti definizioni e puntualizzazioni in merito a diversi aspetti che non sempre sono ben compresi da parte di coloro che operano nei vari domini sopra citati provocando la nascita di problemi di comprensione, valutazione e validità probatoria delle prove recuperate in fase di indagine. Riporto pertanto alla voce glossario alcune definizioni utili alla comprensione.

Inoltre si evidenzia che un aspetto importante da tenere sempre presente in un'analisi digitale forense è la natura delle prove elettroniche ricavate dal computer: Le prove elettroniche ricavate dal computer sono le informazioni e i dati aventi valore investigativo che sono memorizzate o trasmesse da un computer.

In quanto tale, questa prova è prova latente nello stesso senso che sono prove latenti le impronte digitali o il DNA.

Nel suo stato naturale, noi non possiamo vedere cosa è contenuto nell'oggetto fisico contenente la nostra prova. Servono software ed equipaggiamenti specifici per rendere le prove disponibili. Inoltre la prova elettronica è per sua natura, fragile. Possono essere alterate, danneggiate, o distrutte a seguito di manipolazioni o analisi improprie. Proprio per queste ragioni, devono essere prese tutte le precauzioni necessarie per documentare, collezionare, preservare ed esaminare questo tipo di prove. Un errore nel processo di documentazione può renderle inutilizzabili o far giungere a conclusioni inesatte o parziali

2.3 Cosa fanno le istituzioni: il caso americano

Le istituzioni americane, forti delle elevate competenze tecniche disponibili, delle esperienze sul campo, e di una legislazione differente, hanno oramai da anni, fornito alle forze di polizia gli strumenti legislativi e le linee guida per il trattamento ottimale delle prove informatiche (così come di ogni altro tipo di prova).

La produzione regolare di testi di riferimento, forniti in particolar modo dal Dipartimento di Giustizia Americano che già nel 1999 forniva un primo documento [7] e che dal 2001 con [10] "Electronic Crime Scene Investigation: A Guide for First Responders" ha fornito un'ottima base di riferimento per la persecuzione dei crimini informatici. Bisogna anche dire che la produzione di testi è impressionante per quantità e qualità basta andare nel sito della U.S. Department of Justice [8] per rendersi conto dell'interessante quantità di documenti siano stati prodotti a beneficio sia delle forze di polizia sia delle corti di giustizia americane.

Interessante, in questo caso [10], risulta la tabella di corrispondenza tra azione criminosa e reato commesso che consente la possibilità di relazionare i casi tipici di reato con gli aspetti legali.

Altro elemento importante [11] è l'insieme di worksheet (schede riepilogative) per la raccolta delle informazioni reperite dall'analisi su quanto recuperato sulla scena del crimine e la loro classificazione.

In particolare l'"*Hard Drive Evidence Worksheet*" dove indicare tutti i dati che riguardano le informazioni sui dischi recuperati durante l'indagine. Dai dati sulle etichette dei dischi stessi ai parametri tecnici, quali Capacità, Cilindri, Testine, Settori, Partizioni, ecc. dei dischi fissi, recuperati attraverso l'analisi tramite software specifici quali Fdisk, Partition Table, SafeBack, EnCase, e altri. Vanno poi indicate anche le copie immagine e/o di backup recuperate e la modalità con cui è

fatta la copia, la piattaforma operativa, cioè il Sistema Operativo utilizzato e il sw di analisi utilizzato per ottenere l'informazione, l'elenco delle utilities usate in aggiunta a quelle di base disponibili.

Per finire la voce delle "Analysis Milestone" per ricordare all'analista cosa deve andare a verificare sul sistema. Per il dettaglio si rimanda alle pagine 46 e 47. Il secondo worksheet "Removable Media Worksheet" riguarda invece i media rimovibili dove vengono indicati tipologie e quantità. Per il dettaglio si rimanda alle pagg. 48/49 dello stesso testo.

Continuare nell'analisi delle proposte presenti nei documenti prodotti dal Dipartimento di Giustizia Americano sarebbe da solo argomento di sviluppo non di una ma di una serie di ricerche di tesi e non è l'obiettivo di questa tesi. Però è doveroso citare almeno i documenti più importanti e i loro contenuti più interessanti. Quindi citiamo "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors" [23] che è una guida su come le forze dell'ordine e i procuratori debbano procedere nella presentazione di prove digitali in una corte di giustizia focalizzandosi su aspetti quali problematiche di ricerca e di sequestro, integrità, scoperta, e divulgazione di prove digitali, principi per la preparazione delle prove in tribunale, presentazione della prova digitale, in particolare come affrontare i casi di pedo-pornografia.

Proseguiamo citando recentissimo [26] "Investigations Involving the Internet and Computer Networks" che si focalizza ovviamente sulle modalità di indagine nelle reti di calcolatori. Tale guida approfondisce in particolar modo come rintracciare un Indirizzo Internet, come affrontare le indagini che riguardano E-Mail, siti Web. Come svolgere le indagini sui servizi basati sul social software, quali i servizi di

messengeria istantanea (chat, IRC) le reti di condivisione di file P2P, bulletin boards, e newsgroup, infine le metodologie usate negli attacchi in rete di Network Intrusion tipo Denial of Service. Il documento si conclude esponendo anche gli aspetti legali di tali tipologie di indagini.

Concludiamo questa carrellata parlando di un breve ma interessante documento [28] “Addressing shortFalls in Forensic Science Education” che fa il punto sul processo di formazione nelle scienze forensi in America ed evidenzia la necessità di avere, come afferma questa ricerca, un base comune di percorsi formativi che permettano di avere una ricaduta omogenea nella formazione degli esperti in scienze forensi. Cita il precedente documento già redatto sempre dalla NIJ [29] “Education and Training in Forensic Science - A Guide for Forensic Science Laboratories, Educational Institutions, and Students”

Capitolo 3

Cosa succede in Italia

3.1 Lo stato dell'arte

Nell'ambito italiano siamo in una situazione di grande fermento. Infatti, ci si stà muovendo, soprattutto in ambito accademico, in particolare quello giuridico e quello informatico, principalmente nella definizione di procedure atte a fornire certificazioni, specializzazioni, competenze specifiche ai vari protagonisti del settore che operano per scelta (periti forensi) o per obbligo di lavoro (forze di polizia e magistratura). Una disamina qui di queste proposte, principalmente di corsi richiederebbe troppo tempo e non è un obiettivo di questa tesi.

Però a parte queste eccezioni istituzionali, che non forniscono ancora un protocollo operativo condiviso, anche se il progetto L.E.F.T. pare vada in questa direzione, il panorama italiano è più che altro centrato sulle abilità dei singoli, che forniscono i loro servizi sulla base della loro eterogenea esperienza.

Questo porta ad una mancanza di uniformità nelle procedure di acquisizione di prove digitali, come pure nella trattazione dell'ammissibilità delle stesse in sede dibattimentale. A dire il vero questo è reso difficile anche dalla varietà di apparecchiature informatiche oramai in commercio. Il che vuol dire avere competenze tecniche elevate e molto specialistiche, che non sempre sono riscontrabili in un unico soggetto.

Fare il punto sullo stato dell'arte è quindi cosa alquanto ardua.

Già Luca Chirizzi nell'introduzione del suo libro [31] lamenta come *“La lacuna generata dall'inesistenza di un simile protocollo fa sì che i soggetti demandati ad occuparsi dell'investigazione, della difesa, e del giudizio debbano, di volta in volta, affidarsi alle proprie capacità professionali”* [32]

Occorre quindi fare in modo che i due principali domini individuati nelle mappe (informatico e giuridico) della digital forensics, *“...scienza interdisciplinare ad alto rischio di contraddizione..”*, come intesa da Dario Scalea [33] trovino un linguaggio comune che permetta la corretta valutazione delle prove.

Si tratta in sostanza di “scoprire” o meglio “inventare” una Stele di Rosetta che consenta ai due mondi, quello informatico e quello giuridico di comunicare per conoscersi meglio e ridurre al minimo il rischio di commettere errori in sede di giudizio.

Se quindi è ormai condiviso dalla maggior parte della comunità scientifica che i passi logici del processo seguito da un digital forenser, come nella proposta di Denis Frati [34] possono essere così sintetizzati:

1. Identificazione
2. Conservazione
3. Acquisizione
4. Analisi
5. Presentazione

dal punto di vista di chi deve investigare, nel rispetto della legge, deve invece tener conto che si parla di:

1. Perquisizione ed eventuale
2. Sequestro
3. Acquisizione
4. Analisi
5. Presentazione (documentazione dei risultati)

Ancora Luca Ghirizzi riesce abilmente nel suo testo [31] a fornire una guida dove i passi sopra elencati vengono analizzati in particolare tenendo conto la legislazione vigente. Fino a spingersi a proporre un Flow-Chart, non esaustivo, delle varie fasi.

Approccio diverso è quello di Andrea Ghirardini, oramai noto perito forense, che nel suo recentissimo libro [35] ha ovviamente un approccio più tecnico e centrato sugli strumenti informatici di acquisizione e soprattutto analisi che il perito forense può utilizzare. Infatti i contenuti principali del testo sono: indagini forensi in campo informatico - Il panorama giuridico italiano - Acquisizione del dato: sequestro, intercettazione e duplicazione - Il laboratorio del computer forenser - L'analisi di media, partizioni e volumi - Investigare su un file system - Tool e programmi di analisi, investigare con Helix Knoppix - Metodologia di analisi generale - Analisi di un sistema Windows, Mac OS X e Linux - Analisi dei file di log - Network Forensics - Analisi di supporti rimovibili e media non convenzionali.

Esistono poi blog e siti che trattano di computer forensics, tenuti e aggiornati da diversi protagonisti della computer forensics italiana, citiamo non in ordine di importanza e senza pretesa di esaustività: Andrea Ghirardini [36], Stefano Fratepietro [37], Giovanni Bassetti [38], progetto L.E.F.T. [39], Investigazione e Sicurezza [40] Progetto IRItaly [41][42], Denis Frati [43]. IISFA [44], Marco Mattiucci [45], Giovanni Ziccardi[46]

3.2 Le Leggi

Le leggi italiane sono e devono essere alla base del lavoro dei digital forenser, delle forze di polizia, degli avvocati, dei pubblici ministeri, e ovviamente dei giudici.

Quindi la loro conoscenza è *condicio sine qua non* per la corretta attività del digital forenser.

Nella nostra realtà non esiste un impianto legislativo specifico per la digital forensics ma di recente la ricostruzione probatoria dei fatti di reato è sempre più spesso affidata ai risultati della cosiddetta “*prova scientifica*” conseguita tramite operazioni svolte da periti o consulenti tecnici o reparti speciali delle forze di polizia. Test genetici del DNA, esami biologici, analisi chimiche e tossicologiche, esami psicologici, ricostruzioni e simulazioni della scena del crimine e delle dinamiche che vi si sono svolte, metodi spettrografici per il riconoscimento vocale (voice-print), stilometria, sono tutti esempi delle cosiddette “*prove scientifiche*” che vengono oramai accettate in qualsiasi tribunale, come dimostrano recenti fatti di cronaca (Delitto di Garlasco, Delitto di Perugia, Caso Cogne, ecc.).

Nel caso della digital forensics si parla più specificatamente di *prova digitale* (digital evidence).

Una definizione di prova digitale, lo ribadiamo, è la seguente

“Qualsiasi informazione, con valore probatorio,
che sia o memorizzata o trasmessa in un formato digitale”

(Scientific Working Group on Digital Evidence, 1998).

L'impianto normativo americano, che peraltro ci viene proposto dalla abbondante e recente produzione cinematografica, vedi i vari serial tv CSI, NCIS, Numb3rs, ecc. ci fa presupporre una estrema “*dimestichezza*” nell'accettare, riconoscere, validare, usare la prova digitale nel dibattito processuale, basata peraltro sui due pilastri della giurisprudenza nord-americana noti come “*Frye test*” e “*Daubert test*”.

In Italia invece il dibattito sull'ammissibilità di tale prova in sede di giudizio è ancora una questione aperta che porta spesso ad ampi contrasti tra le varie componenti del dibattito. Invero i settori accademici della giurisprudenza più attenti ed aggiornati sul piano informatico vanno nella direzione di ricercare come e quali tipologie di prove digitali è possibile ammettere e quali no.

Molto interessante appare il documento [45] *“Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale”* del dott. Giovanni Canzio Consigliere della Corte Suprema di Cassazione.

Egli afferma che l'impianto normativo italiano del processo penale è

- *“verosimilmente meglio attrezzato, rispetto alla tradizionale cultura anglo-americana, per far fronte alla crescente complessità dei metodi della scienza e della tecnologia applicati nell'accertamento dei fatti”*

ed ancora

- *“specifiche norme del codice di rito regolano l'ammissibilità della prova a richiesta delle parti sulla base dei criteri fondamentali della rilevanza e delle non manifesta superfluità (art. 190 e 495 c.p.p.)*

- *il procedimento acquisitivo degli elementi probatori (di tipo tecnico-scientifico) non è concentrato temporalmente ma è progressivamente scandito attraverso le varie fasi del processo, sì che il grado di incertezza del risultato probatorio tende a ridursi;*

- *l'oralità e l'immediatezza del contraddittorio per la prova sono temperate dall'ammissibilità di relazioni scritte degli esperti (art. 227.5 e 501.2 c.p.p.) e di memorie scritte delle parti e dei difensori (art. 121.1 c.p.p.);*

- *il giudice della ammissione della prova e della ricostruzione probatoria del fatto è unico e professionale;*

- è riservato al giudice un significativo spazio di integrazione probatoria ex officio (artt. 190.2, 195.2, 441.5 e 507 c.p.p.), con particolare riguardo alla perizia ed alla nomina degli esperti, scelti tra persone fornite di particolare competenza tecnica e scientifica nella specifica disciplina (artt. 221, 224 e 508 c.p.p.);

- il libero convincimento del giudice è condizionato dall'obbligo di razionale giustificazione delle scelte decisorie secondo il modello normativo della motivazione in fatto (artt. 192.1 e 2, 546.1 lett. e c.p.p.)”.

Il documento continua parlando delle cosiddette “prove atipiche” o non disciplinate dalla legge,

“I cui limiti sono peraltro enunciati puntualmente dall’art. 189 del c.p.p., norma cardine questa, per assicurare l’opportuna flessibilità del sistema processuale in materia di prova scientifica”.

Non vogliamo qui peraltro fare un’elencazione di articoli del codice e rimandiamo alle mappe per una puntuale disamina degli articoli del Codice Penale e delle leggi che ritengo siano fondamentali nella pratica della digital forensics.

Capitolo 4


Le Mappe


Le mappe da me realizzate vengono proposte, senza pretesa di completezza o di assoluta inamovibilità, per consentire una base di conoscenza condivisa, al fine di strutturare un eventuale percorso di ricerca, formativo, di sperimentazione, normativo, tecnologico e con lo scopo comunque di fornire un quadro il più ampio possibile sulla digital forensics in Italia.

Il mio intento è quello di aprire una piattaforma web dove le mappe siano condivisibili a chi voglia fornire il suo contributo di miglioramento delle stesse.

Il programma per la loro realizzazione è il sw Open Source Freemind, del quale ho utilizzato l'ultima versione stabile, la 0.8.0. Informazioni sul programma e la sua versione scaricabile possono essere trovate in <http://freemind.sourceforge.net/>. Queste mappe saranno visibili su www.mauriziotorcasio.it alla voce mappe della digital forensics, in formato html.

Appare ovvio che non sia necessario qui riportare tutte le mappe prodotte, anche perché si prestano meglio ad un uso dinamico e ipertestuale che qui non è possibile replicare. Mi limito quindi a riportare solo a quelle che ritengo sia qui importante sottolineare. Infatti diversi sono gli aspetti tecnici, procedurali, legali che sarebbero degni di ulteriori approfondimenti, obiettivo che si vuole stimolare con la pubblicazione delle mappe su web.

Ho voluto lasciare in inglese la mappa di Brinson per differenziarla dalle mie. Le parti che non sono considerate accettabili o utilizzabili in Italia sono state contrassegnate con una  rossa molto evidente.

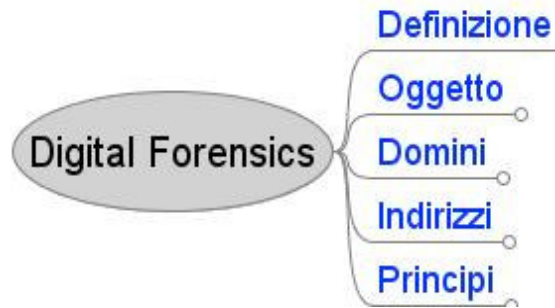
Le parti aggiunte nella suddetta mappa sono contrassegnate con una freccia verso destra di colore azzurro .

Dalle mappe inoltre si evince che ogni terminazione chiusa da un pallino contiene un sotto livello di definizioni, oppure linka (freccia rossa) o ad un'altra mappa relativa allo specifico concetto o anche ad un collegamento ipertestuale ad una pagina web o ad un documento specifico.

Di seguito riportiamo alcune delle mappe ritenute più significative.

4.1 La mappa principale: Digital Forensics

La mappa principale è quella che ha come soggetto appunto la Digital Forensics.



Come si può notare in questa mappa ho evidenziato 5 aspetti principali che la riguardano. Vale a dire

4.1.1 Definizione di Digital Forensics



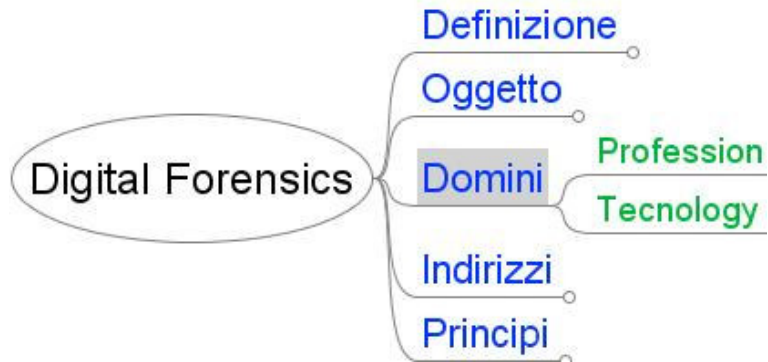
4.1.2 Oggetto della Digital Forensics: la freccia rossa indica che c'è collegamento ad una sotto-mappa specifica per definire il concetto di prova digitale



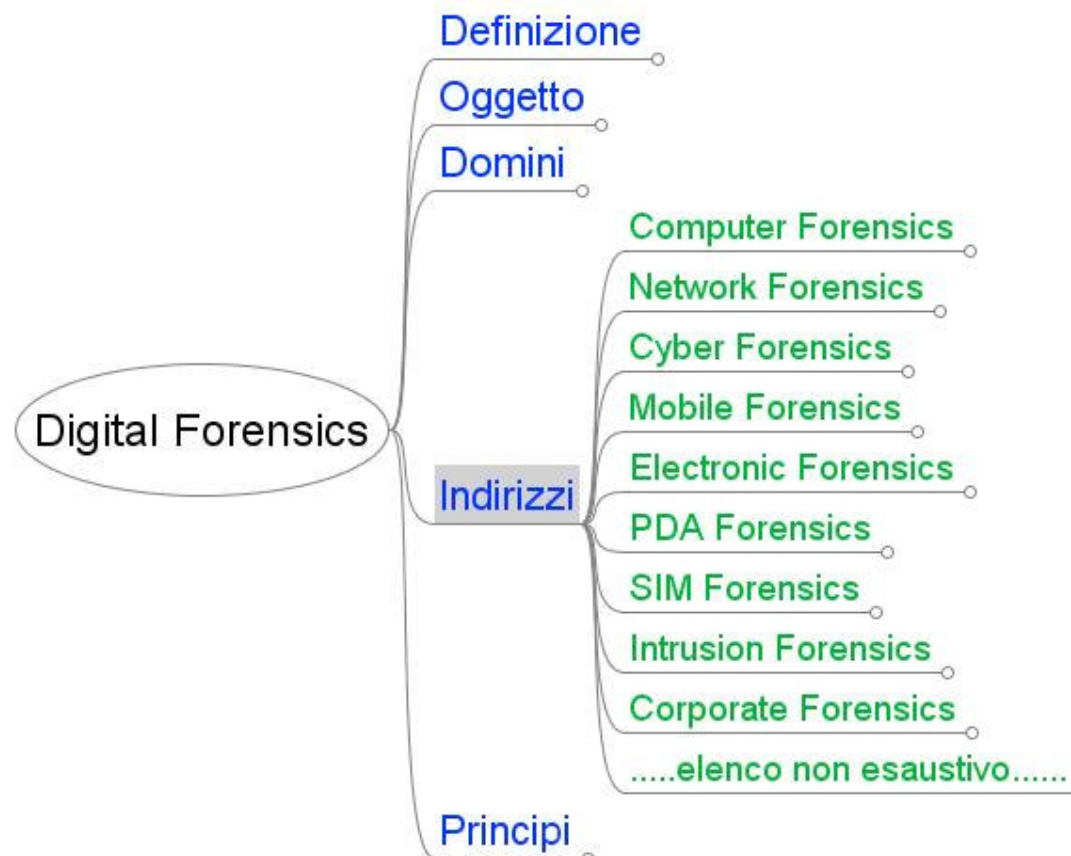
4.1.3 Domini coinvolti dalla Digital Forensics

Questa mappa è stata rielaborata da quella di Brinson sulla base però del concetto

di dominio.

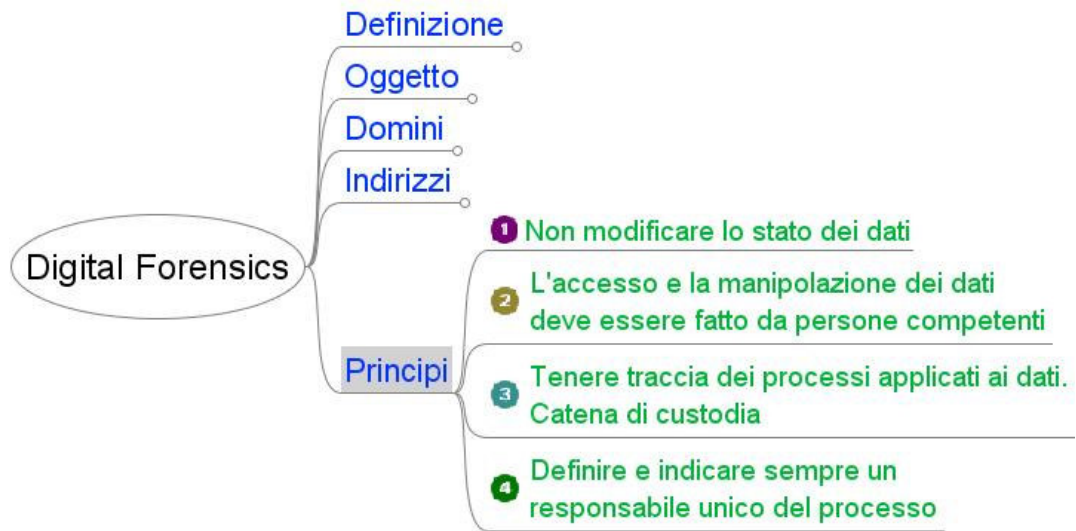


4.1.4 Le categorie della Digital Forensics

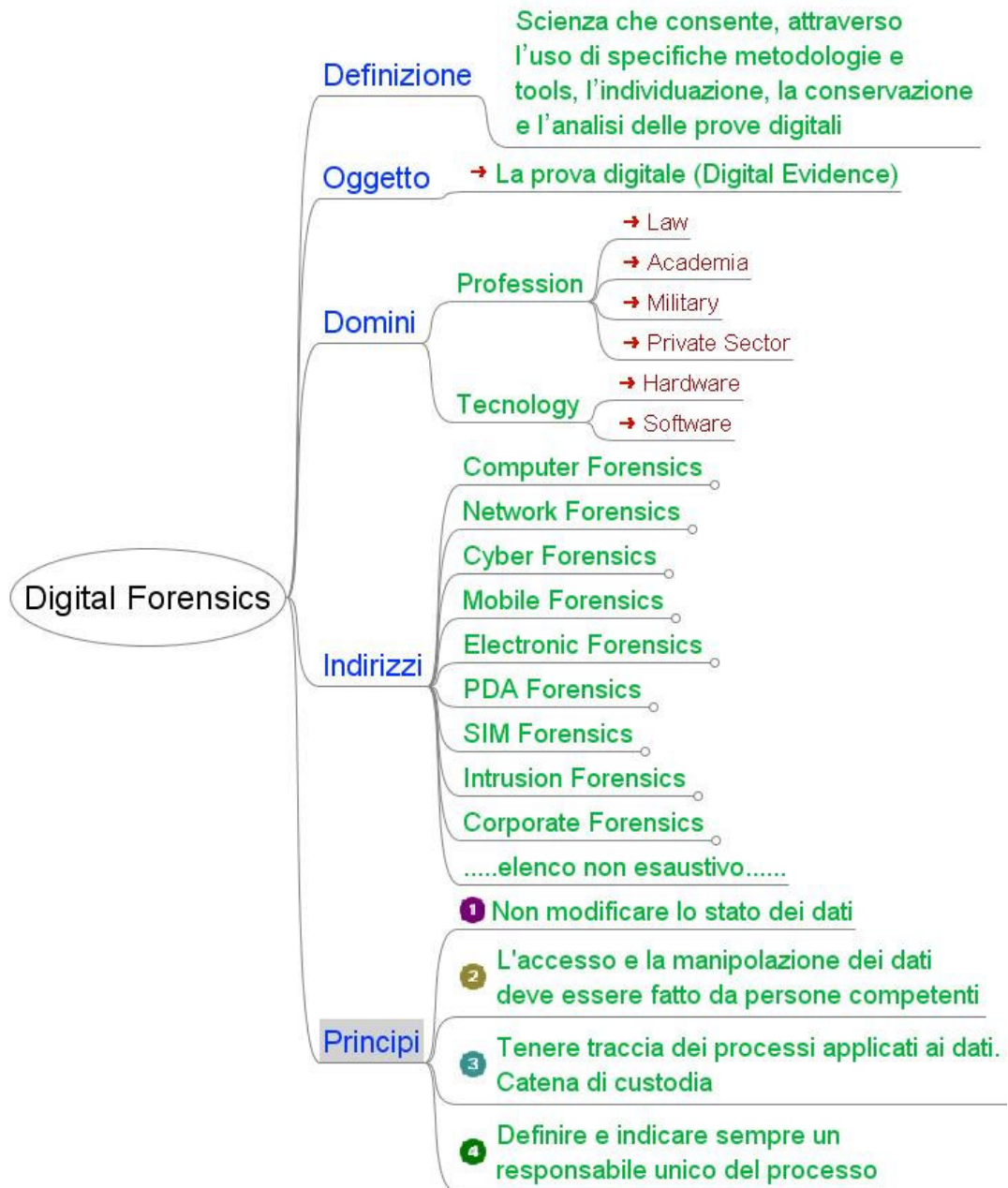


4.1.5 Principi fondamentali

Su di essi si deve basare l'attività di chi affronti problematiche inerenti alla Digital Forensics. Ovvero colui che potremmo definire essere il Digital Forenser

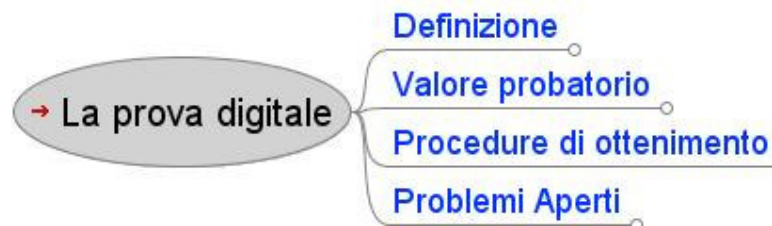


4.1.6 La mappa della Digital Forensics completamente esplosa è la seguente:



4.2 La prova digitale

Notevole importanza assume la sotto-mappa relativa alla cosiddetta prova digitale, che è appunto l'oggetto della Digital Forensics, che visualizziamo di seguito.



Tale mappa evidenzia 4 aspetti fondamentali:

4.2.1 Cosa si intende per prova digitale



4.2.2 Valore probatorio di una prova digitale.



4.2.3 Cosa da alla prova digitale valore probatorio in sede di giudizio



4.2.4 Procedure di ottenimento della prova digitale.

Con quali procedure è possibile ottenerla per poterla usare senza rischio di rigetto in giudizio



4.2.5 Problemi aperti.



Sicuramente appare importante evidenziare che ci sono ancora delle problematiche aperte su come ammettere in un dibattimento le prove digitali ottenute utilizzando vari strumenti di cui non sempre il giudice è in grado di comprendere appieno le

caratteristiche e le modalità procedurali di acquisizione della stessa. Peraltro di questo abbiamo già parlato nel capitolo delle leggi.

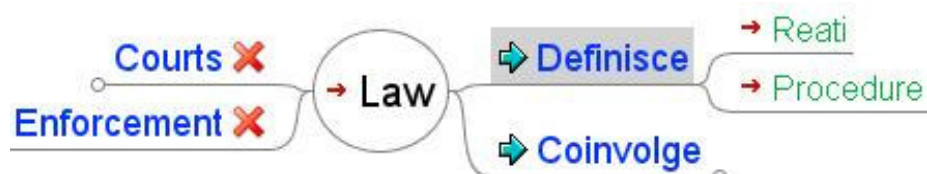
4.3. La Giurisprudenza

Degna di nota sicuramente è la mappa relativa alla giurisprudenza (LAW) che intesa da Brinson principalmente come un sottoinsieme delle professioni, viene da me considerata come uno dei sotto-domini che sono coinvolti nella scienza della Digital Forensics.

Gli aspetti evidenziati come Courts ed Enforcement non riguardano il panorama giuridico italiano e sono quindi stati segnati come non utilizzabili, ma non sono stati eliminati dalla mappa per completezza.

4.3.1 La mappa della Giurisprudenza

La mappa è la seguente



4.3.2 Reati

Sono stati invece aggiunti gli aspetti relativi a cosa si occupa la legge in particolare quella penale, in Italia. Avremo quindi la sotto-mappa dei reati



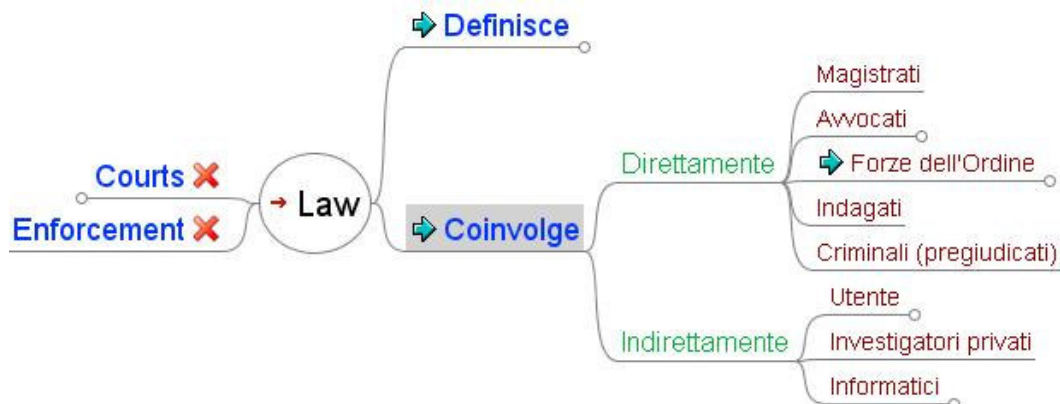
4.3.3 La Procedure del c.p.p e quelle operative

Ecco la sotto-mappa delle procedure adottate in Italia per la persecuzione dei reati e degli articoli del c.p.p. più utilizzati in merito



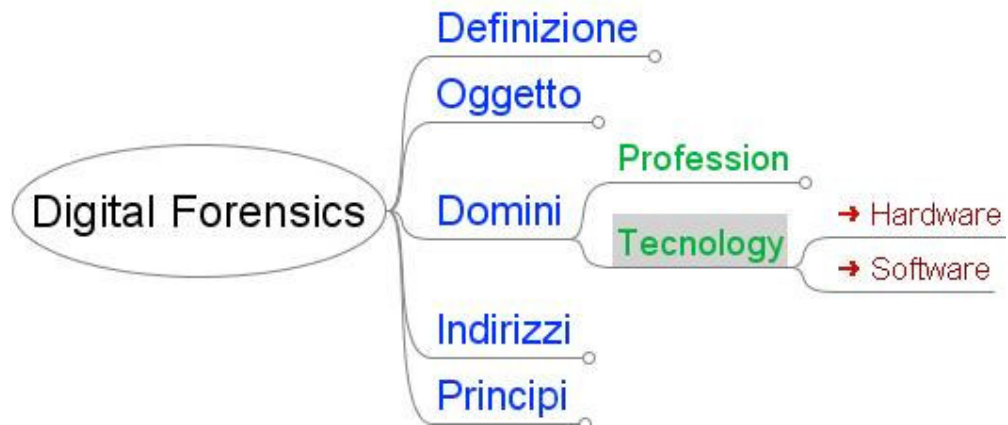
4.3.4 I Soggetti coinvolti

Ho poi voluto indicare, con una scelta del tutto personale, quali sono i soggetti coinvolti, direttamente perché vi operano nel bene o nel male, e indirettamente, perché chiamati in causa nel caso di indagini, che riguardano contenuti digitali.



4.4 La Tecnologia

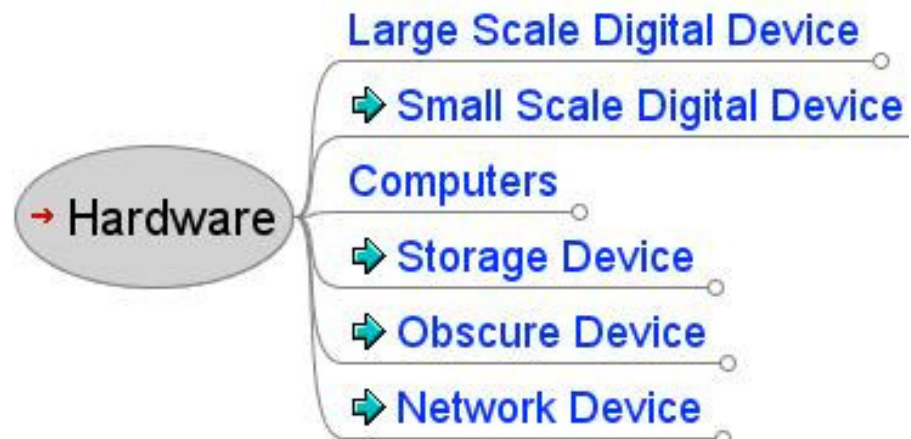
Proseguiamo la panoramica sulle mappe visualizzando il dominio che coinvolge la tecnologia nella Digital Forensics, suddivisa in Hardware e Software,.



In particolare nel caso dell'Hardware Brinson, traslascia stranamente tutta la componentistica relativa alle reti di comunicazione, alle flash card, e a tutta una serie di vari device che comunque posseggono memorie che potenzialmente possono contenere prove digitali.

4.4.1 L'Hardware

La mappa è la seguente



Esplodiamo le parti modificate per visualizzare i componenti che sono stati aggiornati.

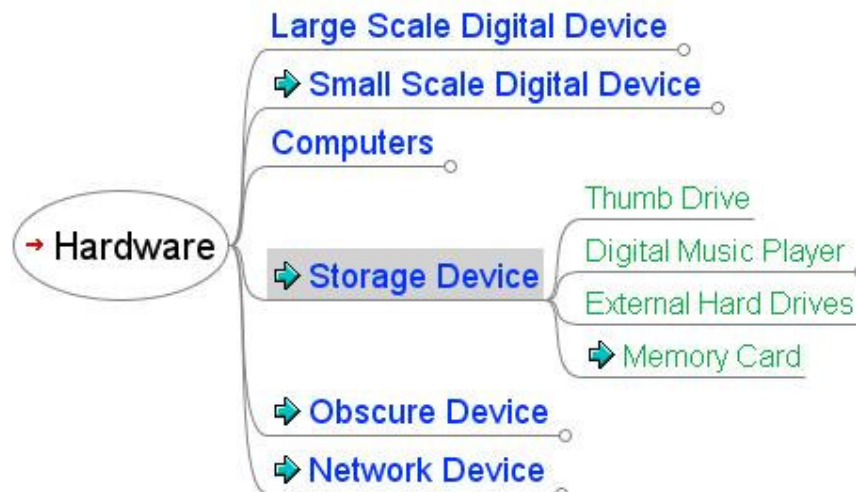
4.4.1.1 Small Scale Digital Device

Nel caso delle SSDD non vengono menzionati quegli oggetti classificati come electronic organizer, che con le loro informazioni di agenda e contatti sono a volte molto utili per poter tracciare la rete di relazioni che l'indagato e/o la vittima aveva con l'ambiente in cui viveva



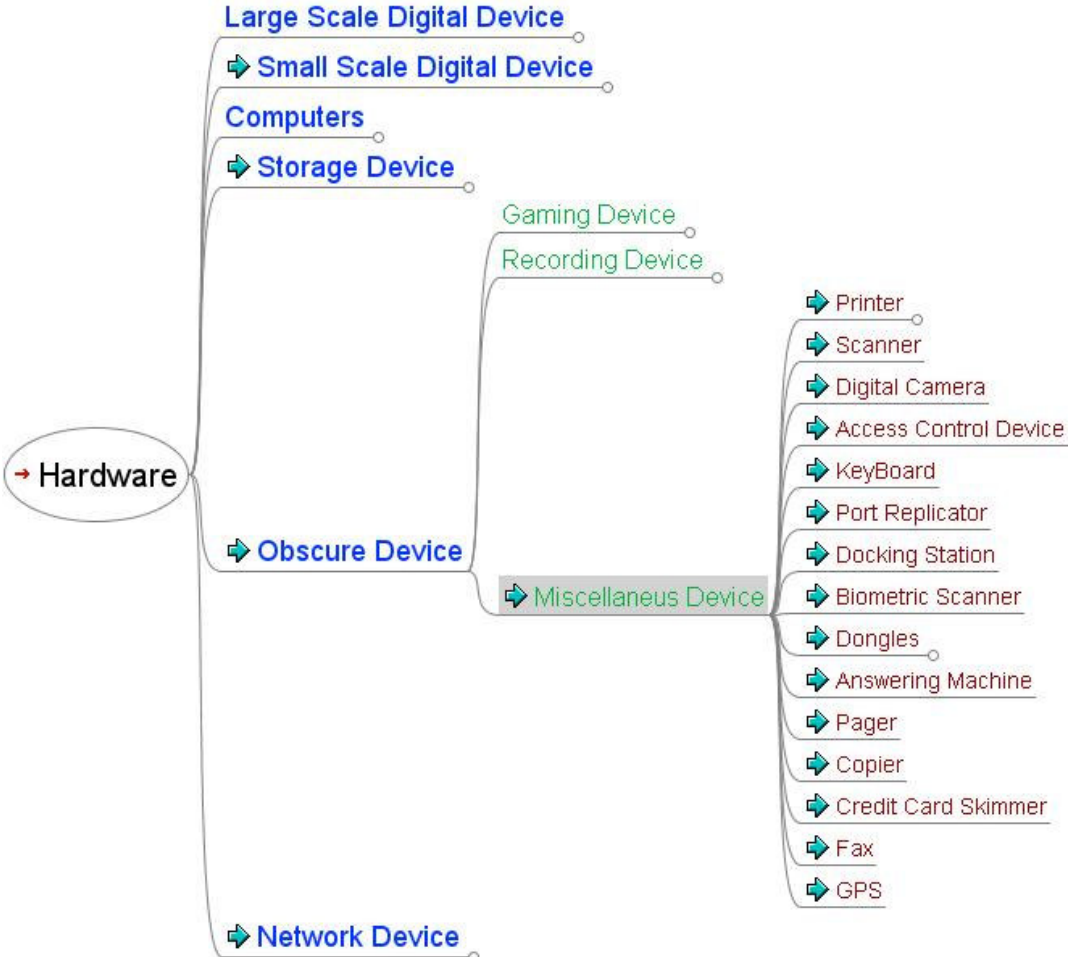
4.4.1.2 Storage Device

L'avvento negli ultimi due anni di quelle che sono chiamate Memory Card, che con capacità sempre maggiori possono essere una fonte enorme di prove, in quanto utilizzate sempre più come espansioni di memoria agili, maneggevoli e occultabili per le loro ridotte dimensioni, in quei componenti elettronici che sono di uso comune come telefonini cellulari, digital camera, videocamere digitali, gaming device, musical player, GPS, ecc.



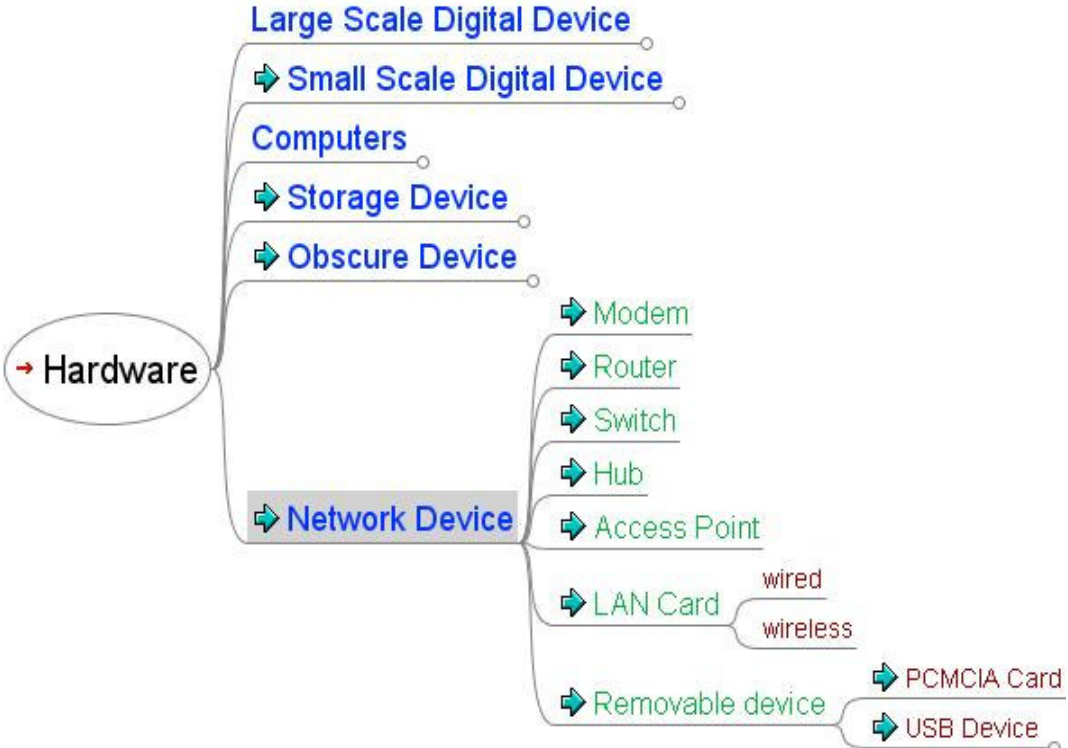
4.4.1.3 Obscure Device

Mantenendo la nomenclatura di Obscure Device, anche per la loro poca evidenza o presenza negli ambiti delle indagini esplodiamo il ramo dei device che sono di difficile inserimento in categorie distinte come quelle evidenziate nella mappa.



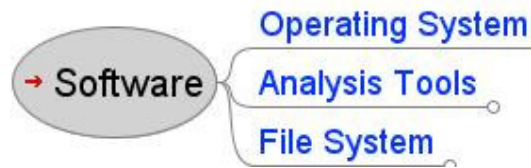
4.4.1.4 Network Device

Infine, anche se Brinson non li cita per nulla, sono oramai di prioritaria importanza la categoria dei Network Device, che risultano essere una grossa fonte di informazioni soprattutto nel caso di network e cyber forensics



4.4.2 Software

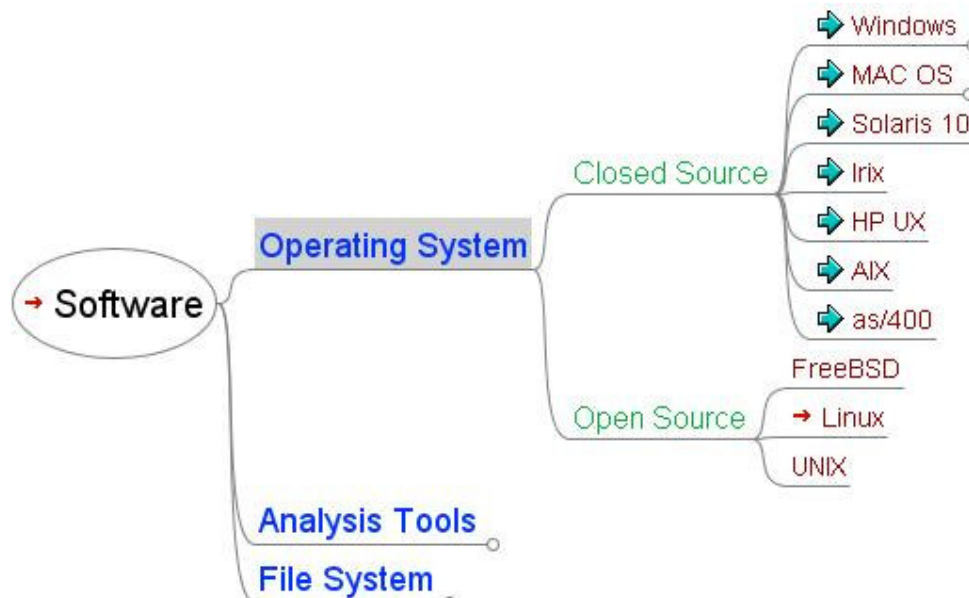
L'altra fondamentale categoria che andiamo a esplicitare è quella del Software



Si osserva che per il digital forensier è necessario possedere adeguate competenze negli ambiti indicati. Ma occorre sottolineare che conoscere bene i Sistemi Operativi su cui si opera e i loro File System come pure gli strumenti necessari per l'analisi dei dati digitali, non può essere disgiunto da una appropriata strategia nella ricerca ed estrazione delle informazioni oggetto di indagine.

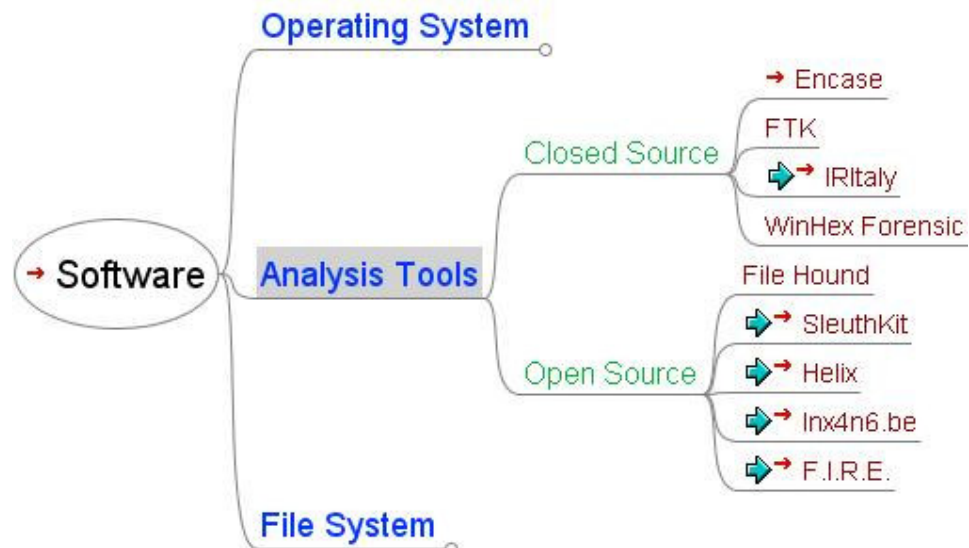
4.4.2.1 I Sistemi Operativi

I Sistemi Operativi vengono ovviamente suddivisi tra Open Source e Closed Source (detti anche S.O. proprietari). La mappa ne evidenzia le famiglie più note e di maggior diffusione.



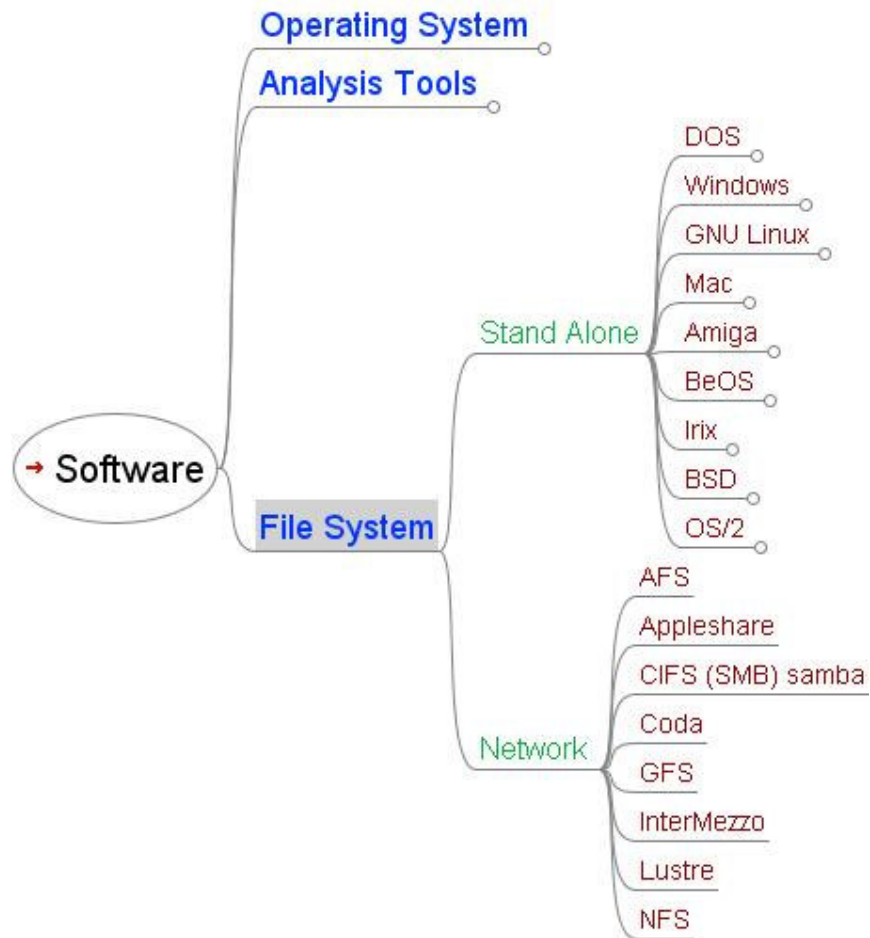
4.4.2.2 Strumenti (Software) di analisi.

Anche in questa mappa si evidenziano gli strumenti di analisi che incontrano attualmente il maggior apprezzamento e la maggior diffusione suddivisi sempre tra Open e Closed Source.



4.4.2.3 Tipologie di File System

Questo è forse l'ambito più complesso per un digital forenser anche se i File System più diffusi si riducono a poche unità.



Capitolo 5

Questioni aperte

Questa tesi non ha la pretesa di fornire una risposta a tutte le situazioni di indagine digitale forense ma vuole essere solo un punto di partenza di un cammino che potrà svolgersi in più direzioni a volte parallele a volte convergenti. Tra le tante questioni aperte alle quali non si è data risposta c'è ne una che forse non appare così evidente ma che diventa importante da considerare nel momento in cui un digital forenser va ad operare secondo una procedura personale o condivisa. Bisogna infatti considerare che l'indagato possa aver operato con tecniche cosiddette di antifoensics, mediate da chi si occupa di sicurezza delle informazioni. Tra tali tecniche portiamo ad esempio quelle come i metodi di crittografia dei documenti ritenuti importanti, i metodi di steganografia che consentono di "nascondere" informazioni digitali dentro altre informazioni digitali. L'elenco sarebbe lungo e mi limito qui a segnalare un interessante articolo [48].

Capitolo 6

Conclusioni

Lo sviluppo di questa tesi si è rivelato molto impegnativo sia nella fase di ricerca del materiale da analizzare sia nella fase di sintesi e implementazione dell'ipotesi di poter creare una base di conoscenza condivisa svolta attraverso le mappe prodotte e la stesura di questo documento di tesi.

Posso quindi ritenermi in parte completamente soddisfatto dal risultato conseguito, tenuto conto sia dell'argomento affrontato sia della mia età, dopo ben 20 anni dalla mia prima laurea.

Peraltro la mia ricerca mi ha portato a verificare che sono molti gli aspetti, anche complessi che varrebbe la pena di approfondire con una ulteriore ricerca.

Questo settore come quello, che possiamo considerare complementare, della sicurezza informatica mi affascina molto, anche se non sempre, per impegni di lavoro, riesco ad aggiornarmi come vorrei.

Credo e spero che il risultato raggiunto sia una buona base di partenza o comunque un filo conduttore per chi, come i soggetti indicati nelle mappe, voglia approfondire l'argomento della Digital Forensics.

Conto a questo punto di proseguire nella mia ricerca, approfondendo quelli che per me sono gli argomenti di maggiore interesse.

Ringrazio anche chi direttamente o indirettamente, dentro e fuori l'Università di Camerino ha contribuito, in modo più o meno consapevole, allo sviluppo di questa tesi e non è stato citato all'inizio.

Glossario

Access token: In Windows NT, an internal security card that is generated when users log on. It contains the security IDs (SIDs) for the user and all the groups to which the user belongs. A copy of the access token is assigned to every process launched by the user.

Acquisition: A process by which digital evidence is duplicated, copied, or imaged.

Analysis: To look at the results of an examination for its significance and probative value to the case.

BIOS: Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports.

Buffer: An area of memory, often referred to as a “cache,” used to speed up access to devices. It is used for temporary storage of data read from or waiting to be sent to a device such as a hard disk, CD-ROM, printer, or tape drive.

CMOS: Complementary metal oxide semiconductor. A type of chip used to store BIOS configuration information.

Compressed file: A file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed. Most common compression utilities are PKZIP with an extension of .zip.

Cookies: Small text files stored on a computer while the user is browsing the Internet. These little pieces of data store information such as e-mail identification, passwords, and history of pages the user visited A

Copy: An accurate reproduction of information contained on an original physical item, independent of the electronic storage device (e.g., logical file copy). Maintains contents, but attributes may change during the reproduction.

CPU: Central processing unit. The computational and control unit of a computer. Located inside a computer, it is the “brain” that performs all arithmetic, logic, and control functions in a computer.

Deleted files: If a subject knows there are incriminating files on the computer, he or she may delete them in an effort to eliminate the evidence. Many computer users think that this actually eliminates the information. However, depending on how the files are deleted, in many instances a forensic examiner is able to recover all or part of the original data.

Digital evidence: Information stored or transmitted in binary form that may be relied on in court.

Docking station: A device to which a laptop or notebook computer can be attached

for use as a desktop computer, usually having a connector for externally connected devices such as hard drives, scanners, keyboards, monitors, and printers.

Dongle: Also called a hardware key, a dongle is a copy protection device supplied with software that plugs into a computer port, often the parallel port on a PC. The software sends a code to that port and the key responds by reading out its serial number, which verifies its presence to the program. The key hinders software duplication because each copy of the program is tied to a unique number, which is difficult to obtain, and the key has to be programmed with that number.

DSL: Digital subscriber line. Protocols designed to allow highspeed data communication over the existing telephone lines between end-users and telephone companies.

Duplicate: An accurate digital reproduction of all data contained on a digital storage device (e.g., hard drive, CD-ROM, flash memory, floppy disk, Zip®, Jaz®). Maintains contents and attributes (e.g., bit stream, bit copy, and sector dump).

Duplicate digital evidence: A duplicate is an accurate digital reproduction of all data objects contained on the original physical item.

Electromagnetic fields: The field of force associated with electric charge in motion having both electric and magnetic components and containing a definite amount of electromagnetic energy. Examples of devices that produce electromagnetic fields include speakers and radio transmitters frequently found in the trunk of the patrol car.

Electromagnetic interference: An electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment.

Electronic device: A device that operates on principles governing the behavior of electrons. which include computer systems, scanners, printers, etc.

Electronic evidence: Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device.

Encryption: Any procedure used in cryptography to convert plain text into cipher text in order to prevent anyone but the intended recipient from reading that data.

Examination: Technical review that makes the evidence visible and suitable for analysis; tests performed on the evidence to determine the presence or absence of specific data.

File name anomaly: Header/extension mismatch; file name inconsistent with the content of the file.

File slack: Space between the logical end of the file and the end of the last allocation unit for that file.

File structure: How an application program stores the contents of a file.

File system: The way the operating system keeps track of the files on the drive.

First responder: The initial responding law enforcement officer and/or other public safety official arriving at the scene.

Forensically clean: Digital media that are completely wiped of nonessential and residual data, scanned for viruses, and verified before use.

Hashing: The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

Hidden data: Many computer systems include an option to protect information from the casual user by hiding it. A cursory examination may not display hidden files, directories, or partitions to the untrained viewer. A forensic examination will document the presence of this type of information.

Host protected area: An area that can be defined on IDE drives that meets the technical specifications as defined by ATA4 and later. If a Max Address has been set that is less than a Native Max Address, then a host protected area is present.

IDE: Integrated drive electronics. A type of data communications interface generally associated with storage devices.

Image: An accurate digital representation of all data contained on a digital storage device (e.g., hard drive, CD-ROM, flash memory, floppy disk, Zip®, Jaz®). Maintains contents and attributes, but may include metadata such as CRCs, hash value, and audit information.

ISDN: Integrated services digital network. A high-speed digital telephone line for high-speed network communications.

ISP: Internet service provider. An organization that provides access to the Internet. Small Internet service providers provide service via modem and ISDN, while the larger ones also offer private line hookups (e.g., T1, fractional T1).

Latent: Present, although not visible, but capable of becoming visible.

MAC address: Media access control address. A unique identifying number built (or “burned”) into a network interface card by the manufacturer.

Modem: A device used by computers to communicate over telephone lines. It is recognized by connection to a phone line.

Network: A group of computers connected to one another to share information and resources.

Networked system: A computer connected to a network.

ORB: A high-capacity removable hard disk system. ORB drives use magnetoresistive (MR) read/write head technology.

Original electronic evidence: Physical items and those data objects that are associated with those items at the time of seizure.

Password-protected files: Many software programs include the ability to protect a file using a password. One type of password protection is sometimes called “access denial.” If this feature is used, the data will be present on the disk in the normal manner, but the software program will not open or display the file without the user entering the password. In many cases, forensic examiners are able to bypass this feature.

Preservation Order: A document ordering a person or company to preserve potential evidence.

Proprietary software: Software that is owned by an individual or company and that requires the purchase of a license.

Peripheral devices: An auxiliary device such as a printer, modem, or data storage system that works in conjunction with a computer.

Phreaking: Telephone hacking.

Port: An interface by which a computer communicates with another device or system. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

Port replicator: A device containing common PC ports such as serial, parallel, and network ports that plugs into a notebook computer. A port replicator is similar to a docking station but docking stations normally provide capability for additional expansion boards.

Printer spool files: Print jobs that are not printed directly are stored in spool files on disk.

Removable media: Items (e.g., floppy disks, CDs, DVDs, cartridges, tape) that store data and can be easily removed.

SCSI: Small Computer System Interface. A type of data communications interface.

Screen saver: A utility program that prevents a monitor from being etched by an unchanging image. It also can provide access control.

Seizure disk: A specially prepared floppy disk designed to protect the computer system from accidental alteration of data.

Server: A computer that provides some service for other computers connected to it via a network.

Sleep mode: Power conservation status that suspends the hard drive and monitor

resulting in a blank screen to conserve energy, sometimes referred to as suspend mode.

Stand-alone computer: A computer not connected to a network or other computer.

Steganography: The art and science of communicating in a way that hides the existence of the communication. It is used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

System administrator: The individual who has legitimate supervisory rights over a computer system. The administrator maintains the highest access to the system. Also can be known as **sysop, sysadmin, and system operator**.

Temporary and swap files: Many computers use operating systems and applications that store data temporarily on the hard drive. These files, which are generally hidden and inaccessible, may contain information that the investigator finds useful.

Unallocated space: Allocation units not assigned to active files within a file system.

Volatile memory: Memory that loses its content when power is turned off or lost.

Write protection: Hardware or software methods of preventing data from being written to a disk or other medium i.e **write blocker**.

ALLEGATO A

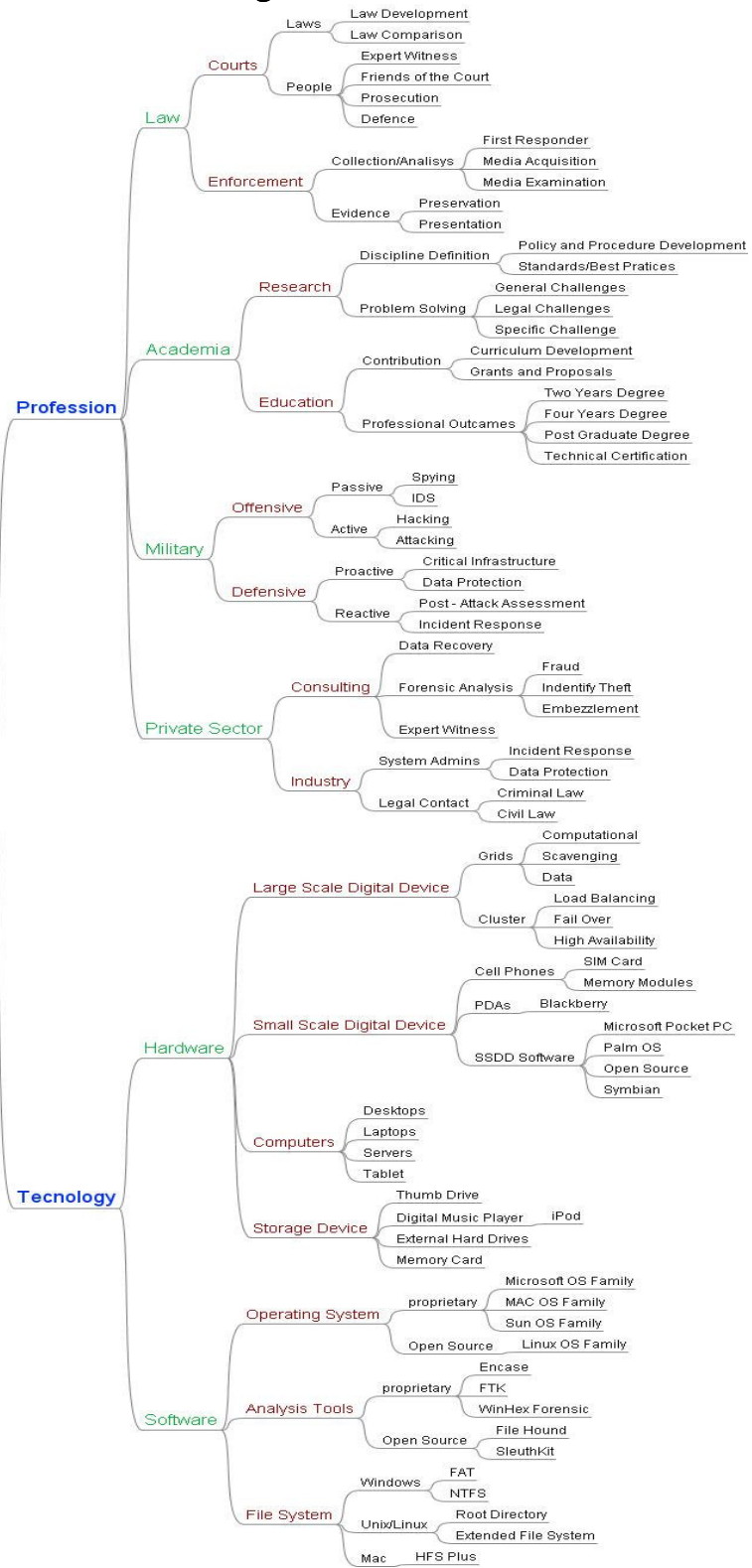
Mappa proposta da Ashley Brinson in formato ad albero gerarchico testuale

- **Cyber Forensics**
 - Technology
 - Hardware
 - Large Scale Digital Device
 - Grids
 - Computational
 - Scavenging
 - Data
 - Clusters
 - Load Balancing
 - Fail-over
 - High Availability
 - Small Scale Digital Device
 - Cell Phones
 - SIM Cards
 - Memory Modules
 - PDAs
 - Blackberry
 - SSDD Software
 - Microsoft Pocket PC
 - Palm OS
 - Open Source
 - Computers
 - Desktops
 - Laptops
 - Servers
 - Tablets
 - Storage Device
 - Tumb drive
 - Digital Music Players
 - iPod
 - External Hard Drive
 - Obscure Device
 - Gaming Device
 - Xbox
 - Playstation
 - Recording Device
 - TiVO
 - DVDR Cable Boxes
 - Software
 - Analisis Tools
 - Proprietary
 - Open Source
 - Operating System
 - Proprietary
 - Microsoft OS Family
 - Mac OS Family
 - Sun OS Family
 - Open Source
 - Linux OS Family
 - File System
 - Windows
 - Fat
 - NTFS
 - Unix/Linux
 - Root Directory
 - Extended File System
 - Mac
 - HFS Plus
 - Profession
 - Law
 - Enforcement
 - Collection/Analysis

- First Responder
- Media Acquisition
- Media Examination
- Evidence
 - Preservation
 - Presentation
- Courts
 - Laws
 - Law Development
 - Law Comparison
 - People
 - Expert Witness
 - Friends of the Court
 - Prosecution
 - Defence
- Academia
 - Research
 - Discipline Definition
 - Policy and Procedure Development
 - Standard Best Practices
 - Problem Solving
 - General Challenges
 - Legal Challenges
 - Specific Challenges
 - Education
 - Contribution
 - Curriculum Development
 - Grants and Proposals
 - Professional Outcomes
 - Two Year Degree
 - Four Year Degree
 - Post Graduate Degree
 - Technical Certification
- Military
 - Offensive
 - Passive
 - Spying
 - IDS
 - Active
 - Hacking
 - Attacking
 - Defensive
 - Proactive
 - Critical Infrastructure
 - Data Protection
 - Reactive
 - Post- Attack Assessment
 - Incident Response
- Private Sector
 - Consulting
 - Data Recovery
 - Forensics Analysis
 - Fraud
 - Identity Theft
 - Embezzlement
 - Expert Witness
 - Industry
 - Systems Admins
 - Incident Response
 - Data Protection
 - Legal Contact
 - Criminal Law and Civil Law

Cyber Forensics

Allegato B



**Bibliografia
Riferimenti
Weblografia**

- [1] Ashley Brinson, Abigail Robinson, Marcus Rogers - "A cyber forensics ontology: Creating e new approach to study cyber forensics.
- [2] Gruber T. "What is an Ontology?" <http://www-ksl.stanford.edu/kst/what-is-an-ontology.html>; 2006
- [3] T. R. Gruber. Toward "principles for the design of ontologies used for knowledge sharing". Presented at the Padua workshop on Formal Ontology, March 1993, later published in International Journal of Human-Computer Studies, Vol. 43, Issues 4-5, November 1995, pp. 907-928 - <http://tomgruber.org/writing/onto-design.pdf>
- [4] T. R. Gruber. A translation approach to portable ontologies. Knowledge Acquisition, 5(2):199-220, 1993 - <http://tomgruber.org/writing/ontologia-kaj-1993.pdf>
- [5] Joan E. Feldman, President Computer Forensics Inc.
"Top Ten Things To Do When Collecting Electronic Evidence"
- [6] Joan E. Feldman, President Computer Forensics Inc
"Ten Steps to Successful Computer-Based Discovery"
- [7] www.ojp.usdoj.gov/nij/topics/forensics/welcome.html
U.S. Department of Justice Office of Justice Programs, National Institute of Justice
Forensic Sciences: Review of Status and Needs
<http://www.ncjrs.gov/pdffiles1/173412.pdf>
- [8] <http://www.ojp.usdoj.gov/nij/topics/forensics/pubs.htm>.
- [9] ACPO NHTCU National Hi-Tech Crime Unit – "Good Practice Guide for Computer-Based Electronic Evidence: Official release version 3.0 - www.acpo.police.uk/policies.asp
- [10] U.S. Department of Justice Office of Justice Programs National Institute of Justice- "Electronic Crime Scene Investigation:A Guide for First Responders" - 2001
- [11] U.S. Department of Justice Office of Justice Programs National Institute of Justice - "Forensic Examination of Digital Evidence: A Guide for Law Enforcement Apr. 2004
- [12] U.S. Department of Justice Federal Bureau of Investigation Laboratory Division - "Handobook of Forensics Services" - 2003
- [13] ACPO E-Crime Working Group -Good Practice Guide for Computer-Based Electronic Evidence: Official release version - www.acpo.police.uk/policies.asp
- [14] - Shayne Sherman - "A digital forensic practitioner's guide to giving evidence in a court of law"- School of Computer and Information Science - Edith Cowan

University, Perth, Western Australia

[15] Helen Armstrong – Philip Russo – “Electronic Forensics Education Needs of Law Enforcement” – Proceedings of the 8° Colloquium for Information System Security Education, West Point, NY June 2004

[16] Matthew Meyers and Marc Rogers - “Computer Forensics: The Need for Standardization and Certification, CERIAS, Purdue University

[17] Ryan Leigland, Axel W. Krings² – “A Formalization of Digital Forensics”
University of Idaho,
ID-IMAG, France

[18] Gary Palmer, “A Road Map for Digital Forensic Research.” Technical Report DTR-T0010-01, DFRWS, November 2001. Report from the First Digital Forensic Research Workshop (DFRWS).

[19] Brian Carrier “Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers” - International Journal of Digital Evidence Winter 2003, Volume 1, Issue 4

[20] <http://www.denisfrati.it/>

[21] <http://www.apogeeonline.com/webzine/2007/07/16/19/200707161901>

[22] <http://www.avanzata.it/left/primoincontroleft.pdf>

[23] U.S. Department of Justice Office of Justice Programs National Institute of Justice - “Forensic Examination of Digital Evidence: A Guide for Law Enforcement Jan. 2007

[24] Tom Wilsdon¹ & Jill Slay² – “Digital Forensics: Exploring Validation, Verification & Certification” - Enterprise Security Management Laboratory, School of Computer & Information Science, University of South Australia

[25] http://web20.excite.it/news/3024/Giudice_inglese_Internet_E_cose

[26] Mattia Monga “Tracce digitali” appunti del corso di informatica giuridica AA 2006/2007 DICo – Università Statale di Milano

[27] U.S. Department of Justice Office of Justice Programs National Institute of Justice Jan '07 “Investigation Involving Internet Computer Networks”

[28] U.S. Department of Justice Office of Justice, Programs National Institute of Justice May '07 “Addressing shortFalls in Forensic Science Education

[29] U.S. Department of Justice Office of Justice Programs National Institute of Justice Jun '04 “Education and Training in Forensic Science - A Guide for Forensic Science Laboratories, Educational Institutions, and Students”

- [30] Cesare Maioli Università di Bologna “Dar voce alle prove: elementi di Informatica forense”
- [31] Luca Chirizzi “Computer Forensic: Il reperimento della fonte di prova informatica” ed. Lauros Robuffo ‘06
- [32] Leo Stilo “Computer forensic: Il volto digitale delle scena criminis necessita di protocolli operativo omogeneei
<http://www.crimine.info/public/crimineinfo/articoli/computer.htm>
- [33] Dario Scalea “Computer Forensics: Metodologia, Eziologia ed Etica”
http://www.cybercrimes.it/papers/cf_metod.pdf
- [34] Denis Frati “La prova informatica nel Processo Penale”
http://www.cybercrimes.it/papers/CSIG_Ivrea_int.pdf
- [35] Andrea Ghirardini – Gabriele Faggioli “Computer Forensics” ed. Apogeo ‘07
- [36] blog di Andrea Ghirardini <http://forensicsbypila.blogspot.com/>
- [37] blog di Stefano Fratepietro <http://steve.yourside.it/it/#>
- [38] sito di Giovanni Bassetti <http://www.nannibassetti.com/>
- [39] sito del L.E.F.T. Legal Electronic Forensics Team, progetto di ricerca (e gruppo di studio) della Cattedra di Informatica Giuridica Avanzata dell'Università degli Studi di Milano <http://www.avanzata.it/left/>
- [40] blog per gli studenti di Scienza per l'investigazione e sicurezza di NARNI
<http://www.2fiorini.it/blog/>
- [41] sito del progetto italiano IRItaly <http://www.iritally-livecd.org/>
- [42] blog del progetto IRItaly <http://iritally.blogspot.com/>
- [43] blog di Denis Frati <http://www.denisfrati.it/>
- [44] sito dell' IISFA Italia, International Information Systems Forensic Association
<http://www.iisfa.it/>
- [45] sito dell'ufficiale dei Carabinieri Marco Mattiucci:
<http://www.marcomattiucci.it/>
- [46] blog del prof. Giovanni Ziccardi <http://www.ziccardi.org/>
- [47] dott. Giovanni Canzio “Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale” Consigliere della Corte Suprema di Cassazione.
- [48] “Anti Forensics: making computer forensics hard” Wendel Guglielmetti Enrique – a.k.a dum_dum

<http://www.intruders.com.br>
<http://ws.hackaholic.org>