UNIVERSITÀ DEGLI STUDI DI CAMERINO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Corso di Laurea Specialistica in Informatica (classe 23/s)

Dipartimento di Matematica e Informatica

POLCAT
UN FRAMEWORK PER L'INDAGINE FORENSE

Tesi di Laurea sperimentale
in
Reti di Elaboratori 2

Laureando

Dott. Gabriele Vitali

Relatori:

Ing. Alberto Polzonetti

Dott. Fausto Marcantoni

ANNO ACCADEMICO 2006 / 2007

"L'esperienza è l'insegnante più severo
perché prima ti fa l'esame
e poi ti spiega la lezione."

INDICE

INTRODUZIONE

Il Digital Forensics, e con esso la disciplina dell'Informatica Forense, sono dottrine sempre più emergenti nella società dell'Information Communication Tecnology, in particolare tra le Forze di Polizia di Stato. Le macro-aree che si possono individuare sono relative al repertamento sulla scena del crimine, i metodi di analisi dei dati contenuti nelle memorie digitali, lo studio e l'osservazione delle informazioni sulle reti, il trattamento dei circuiti elettronici digitali a scopo di indagine ed il reporting legale o di alto livello per la lotta al crimine informatico. Nel corso delle attività d'indagine da parte della Polizia Giudiziaria, siano queste di iniziativa propria o delegate, si pone il problema pratico inerente la ricerca, l'individuazione ed il repertamento dei sistemi high tech e dei dati digitali in essi contenuti con l'obiettivo principale di farne sicure fonti di prova.

Nasce in questo modo, come già è avvenuto in altri paesi, la necessità di avere una serie di strumenti, di standard, formalizzazioni, linee guida, best pratice, procedure e corsi di formazione (sia di base che avanzati), indirizzati a contrastare efficacemente le azioni criminose compiute attraverso l'uso delle tecnologie informatiche e mirate al raggiungimento di un'elevata interoperabilità anche in campo internazionale. L'importanza di avere tanto gli strumenti quanto il personale tecnico altamente qualificati sono da ricercare nell'esigenza di sapere "cosa fare e cosa non fare", "come fare e come non fare".

Per quanto concerne gli stumenti forensi, il mercato dell'ICT offre una vasta gamma di prodotti, sia Closed che Open Source. I software open source consentono un ampio riconoscimento della

tecnologia dei sistemi, l'analisi della logica di funzionamento e la verifica dei processi a cui i dati sono sottoposti, ma non offrono tools integrati in un'unica interfaccia grafica, compatibilità con applicativi sviluppati per differenti sistemi operativi e compilazione reportistica. I software closed source offrono interfacce user friendly, tools integrati, ma non dispongono di larga compatibilità verso le differenti tecnologie e aderenza agli standard qualitativi perché le implementazioni sono arbitrarie e in formati chiusi.

L'obiettivo di questo lavoro, perciò, è quello di riuscire a realizzare un Framework Open Source che sia di supporto a tutte le attività di indagine forense, rispettando quelli che sono gli standard di qualità per la produzione sicura del software, e che sia in grado di interoperare con gli altri prodotti utilizzati dalle polizie internazionali.

Nel primo capitolo sono state descritte le fasi dell'attività di digital forensic, partendo da una descrizione generale del dominio applicativo, proseguendo con le caratteristiche più rilevanti e inerenti la computer forensic e concludendo con la stesura di buone regole per compiere i repertamenti.

Nel secondo capitolo l'attenzione si è concentrata più sullo stato dell'arte della digital forensic in italia, ovvero su quelle che sono le norme previste dalla "macchina giuridica" e su quali sono le problematiche connesse all'attività forense, partendo da una descrizione dei reati più comuni e concludendo con alcune considerazioni riguardo l'uso di prodotti Open Source piuttosto che Closed Source.

Il terzo capitolo pone la base di partenza per lo sviluppo del framework forense, fornendo quelli che saranno i vincoli da rispettare e le problematiche da risolvere limitatamente alle

esigenze della Polizia Postale di Ancona. In tale capitolo si descrivono le funzionalità, il livello di conoscenza e le modalità di funzionamento del software applicativo PolCat, attualmente utilizzato per svolgere le attività di indagine forense.

Nel quarto capitolo viene indicato come si intende risolvere il problema, partendo da alcune considerazioni sui vantaggi che derivano dall'uso di un Framework in ambito forense, proseguendo con la presentazione e definizione di un insieme di parametri di qualità forniti dagli standard ISO 17799 e ISO 27001 [wik08].
Si introduce altresì una nuova metodologia di sviluppo CLASP (Comprehensive, Lightweight Application Security Process) [owa07,owa08b] del Progetto OWASP (Open Web Application Security Project)[owa08a] basata sul principio della suddivisione di ruoli e attività e della gestione della continuità operativa e delle comunicazioni, per la reingegnerizzazione e realizzazione di software standardizzato e certificato.

Capitolo 1

L'ATTIVITÀ FORENSE

1.1. PREMESSA

Il termine "forense" deriva dal latino "forensem" (aggettivo formato su forum): del foro, attinente al foro, legale. Aggiunto di legista, che tratta le cause, che esercita la professione di curiale e si riferisce a qualcosa, oppure relativo a, o utilizzati in un tribunale di diritto.
Al giorno d'oggi, ma comunque da parecchio tempo, con il termine forense ci si riferisce quasi sempre a un metodo per ottenere le prove da utilizzare in un tribunale di diritto e per giungere alla risoluzione di attività criminali [Tor07].
La scienze forense è spesso denominata soltanto forense, ed è l'applicazione pratica di diverse scienze giuridiche per risolvere questioni relative a presunti reati commessi su sistemi proprietari e che può includere una azione civile o penale.
L'uso del termine "forense" al posto di "scienza forense" è oggi, in realtà, un termine globalmente accettato considerando che il termine "forense" è effettivamente un sinonimo di "legale" o "relativo ai tribunali", dal significato della radice latina.
Dato che adesso il termine è strettamente associato con il campo scientifico-criminale, molti dizionari equipararano la parola "forense" con "scienze forensi" [NTW07].
Le scienze forensi si estendono ad una vasta gamma di sotto-scienze e sono quelle che utilizzano le tecniche delle scienze naturali per ottenere elementi di prova penale pertinenti.
Le specialità delle scienze forensi includono:

- Forensic Accounting - l'acquisizione, l'interpretazione e lo studio delle prove relative alla contabilità.
- Digital Forensics (nota anche come Computer forensic) - il recupero, la ricostruzione e l'interpretazione dei contenuti digitali (cioè le immagini, PDF, messaggi e-mail, ecc), memorizzati in un computer, da utilizzare come prova.
- Forensic Document Examination - la ricostruzione, lo studio e l'interpretazione del documento-prova fisico, come ad esempio l'analisi della grafia o il printmaking.
- Forensic Economics - l'acquisizione, lo studio e l'interpretazione degli elementi di prova relativi al danno economico, che comprende la determinazione di perdite e di guadagni, il valore di business di profitto e la perdita, la perdita dell'avviamento, la gestione dei lavoratori e i futuri costi di spese mediche, etc etc.
- Forensic Engineering - la ricostruzione, lo studio e l'interpretazione dei danni relativi alla struttura o alla meccanica di disposiviti, edifici, etc etc.
- Forensic Linguistics - lo studio e l'interpretazione del linguaggio per utilizzarlo come elemento di prova.
- Forensic Origin and Cause - lo studio, l'interpretazione e l'identificazione di un incendio per l'esplicito proposito di determinarne la causa di origine e d'accensione dello stesso (cioè i casi d'incendio doloso).
- Forensic Photography - l'arte-scienza di ricostruire, di interpretare e di produrre una accurata fotografia di un delitto per il beneficio del giudice.
- Forensic Psychology and Psychiatry - lo studio, la valutazione e l'individuazione di malattie mentali e del comportamento umano, allo scopo di ottenere elementi di prova legale.

- Forensic Anthropology - è la pratica dell'antropologia fisica, applicata a una situazione giuridica – solitamente riguarda l'identificazione e il recupero di resti umani (ossa).
- Criminalistics science – (criminologia) è l'applicazione della combinazione di elementi di prova (cioè le impronte digitali, le impronte lasciate da calzature e le tracce dei pneumatici), degli indizi e delle sostanze di controllo.
- Criminalistics science - comprende elementi di prova raccolti da una vasta gamma di scienze forensi per determinare le risposte alle questioni relative alla valutazione e comparazione delle indagini penali. Queste prove sono in genere acquisite in un laboratorio specializzato.
- Forensic Biology - comprende le analisi del DNA e le analisi sierologiche dei fluidi corporei (fisiologia) ai fini dell'individuazione e di identificazione.
- Forensic Entomology - aiuta a determinare l'ora e il luogo della morte e può spesso determinare se l'organismo in fase di esame è stato spostato dopo la morte.
- Forensic Geology - è l'applicazione delle prove trovate nel suolo e nei minerali, ed applicate ad una causa legale.
- Forensic Odontology - è lo studio dei denti, in particolare, dell'unicità dell'impronta dentale.
- Forensic Pathology - combina le dicipline della medicina e della patologia, applicato ad un legale inchiesta, per determinare la causa delle lesioni o della morte.
- Forensic Toxicology - è lo studio, la valutazione e l'identificazione degli effetti dei veleni, dei prodotti chimici, o delle droghe nel o sul corpo umano.

Come abbiamo visto, la scienza forense ricopre una vasta gamma di settori, in particolare tutti quelli dove sia ipotizzabile la possibilità di commettere un reato giuridico. Pertanto lo scopo di questa tesi è quello di presentare più in dettaglio il settore della Digital Forensic,

descrivendone il dominio applicativo, la normativa a riguardo e le tecniche di ricerca e di analisi dei dati nell'attività investigativa della Polizia Giudiziaria.

1.2. CENNI STORICI

La disciplina ha origine in ambienti giuridici di common law ad alta evoluzione tecnologica come gli Stati Uniti (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) 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. In Italia, oltre a nuclei nei corpi di polizia, (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.) vi sono aziende di servizi di sicurezza

informatica che fra le altre cose forniscono anche servizi di post incident analysis di informatica forense, atti a fornire un servizio di prevenzione di futuri attacchi o malfunzionamenti per evitare la perdita di dati rilevanti [Tre02].

1.3. LA DIGITAL FORENSICS

Il Digital Forensics è un campo fortemente emergente tra le Forze di Polizia, i Militari, i Servizi Segreti e qualsiasi organizzazione pubblica o privata che si trova a gestire sistemi di comunicazione high tech al suo interno. Il Digital Forensic raccoglie sempre crescenti fette di mercato ed il business che si sta creando attorno ad esso lo rende appetibile a studi di alto livello sia in campo universitario che privato.
Nel "lontano" 2001 il primo Digital Forensic Research Workshop [DFRW01] segnò le linee guida per la determinazione della scienza del Digital Forensics ed in particolare, nel report della riunione si può leggere quanto segue:

"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."

che nella nostra lingua italiana corrisponde a:

"La digital forensic science è 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

Come si può vedere l'accezione della definizione è sbilanciata nel senso "criminale" eppure oggi gli strumenti ed i risultati del DF si applicano estensivamente anche a settori non penali (si direbbe in Italia). Ad esempio all'interno di aziende o organizzazioni che si trovano a gestire estesi sistemi di comunicazione digitali e che vogliono mantenerne il controllo conformemente a determinate direttive interne. Questo ha allargato sempre più gli studi di questa materia ma soprattutto ne ha ingigantito gli aspetti commerciali.
Altra osservazione riguarda il fatto che il Digital Forensic non si limita alle memorie di massa e/o alle reti di computer ma abbraccia qualsiasi sistema digitale: dai PC, agli iPod, agli smartphone fino ai sistemi di riconoscimento automatico di voci ed immagini, ecc.. In questo senso è una materia scientifica di immense proporzioni che richiede, allo specialista un'enorme preparazione tecnica.
Nel contempo lo sviluppo del DF ha spinto la nascita dell'Anti-Forensics o Counter-Forensics, una parte del DF che si occupa specificamente di come impedire agli strumenti ed alle metodologie del DF di operare correttamente con risultati completi.
Non si può parlare però di Digital Forensic senza sconfinare nel campo della sicurezza informatica. Di fatto sicurezza informatica e digital forensics sono due faccie della stessa medaglia perché con la prima si vanno a gestire quelle che sono le procedure per la sicurezza delle informazioni, mentre con la seconda si vanno a utilizzare gli strumenti informatici per cercare di ricostruire un reato informatico. 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. Se cerchiamo invece nel panorama italiano troviamo che, ad esempio, Denis Frati [Fra06] più sinteticamente la definisce nel modo seguente:

"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)

Andrea Ghilardini invece [Ghi02] rilascia in una sua intervista la seguente dichiarazione

"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 specialità degli informatici forensi è quella di esaminare media digitali e sistemi tecnologici al fine di estrarre gli elementi probatori necessari a dimostrare o confutare il presunto reato commesso.
Se invece andiamo a sondare l'ambiente giuridico troviamo che la scienza forense è, in senso lato, la scienza che studia il valore processuale di determinati accadimenti ai fini della costituzione di fonti di prova, mentre per computer 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 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 si parla tanto di digital forensics quanto di computer forensics, tando di prova quanto di valore del dato, ma tutti nella sostanza esprimono gli 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 di digital forensic.

1.3.1. L'informatica forense

Oltre alla digital e alla computer forensic appena introdotte, possiamo aggiungere concetti simili ma che estendono in un certo senso il significato dei temi appena citati; in letteratura [Atz06], [For01] vanno sotto il nome di informatica forense ovvero le procedure e 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. 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:

- 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,
- analizzare i dati senza alterarli.

In sintesi, lo scopo principale dell'informatica forense è quello 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*.

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.

1.4. LA CATENA DI CUSTODIA

Quando un oggetto fisico, oppure un dato digitale, diviene "reperto" di natura forense è qualcosa di più dell'oggetto o del dato stesso e quel qualcosa in più che lo accompagnerà sempre da lì in avanti è la sua storia tecnico/legale [Mat07a], [Mat07d].
In Italia il termine "catena di custodia" non è molto impiegato in ambito forense proprio perchè richiama inequivocabilmente il più famoso anglosassone "Chain of Custody", che significa:

"*lista dettagliata di cosa si è fatto dei dati originali una volta raccolti..."*

A questo proposito bisogna tornare indietro ad un altro concetto: la "scena del crimine", ossia il luogo dove è avvenuto un fatto che viola la legge penale italiana e quindi ne definisce il reato. Sulla scena del crimine, a seguito del processo denominato sopralluogo vengono estratti informazioni ed oggetti di interesse ai fini della risoluzione del caso per poi essere catalogati ed eventualmente sigillati. Si dice quindi che avviene un sequestro (Artt. 253, 254 C.P.P.) e gli oggetti individuati e prelevati vengono denominati corpi del reato.
La catena di custodia deve necessariamente nascere dal sopralluogo e dal relativo sequestro. In particolare vi è l'obbligo di verbalizzare sia le attività del sopralluogo che quelle di sequestro (libro II° del C.P.P.) annettendo l'ovvia autorizzazione dell'ufficiale procedente. I

primi elementi della catena di custodia "italiana" sono quindi i verbali di sopralluogo e sequestro.
Quando si decide di sottoporre dei corpi di reato ad analisi in un centro scientifico o quando si decide che degli specialisti scientifico forensi devono intervenire sulla scena del crimine, interviene un'analisi e ricerca sistematica e strutturata di elementi utili ai fini probatori e delle indagini. Da tale ricerca ed analisi vengono estrapolati i reperti ed i referti. I primi possono essere corpi di reato o parti di essi che divengono oggetto di analisi mentre i secondi sono documenti che evidenziano cosa l'analisi scientifica ha potuto dedurre riguardo i reperti e come sono avvenute tali deduzioni (includono quindi i chiari riferimenti alle basi tecnico/scientifiche di esse).
Un classico e banalissimo esempio consiste nell'avere come corpo del reato sequestrato un PC il quale nel verbale appare descritto come "...case tower di colore... con lettore di DVD, ecc." mentre ad una prima analisi si scopre che nel DVD drive un supporto DVD rimasto dentro durante il sequestro e non verbalizzato (la porta del drive si apre solo se il PC è attivo o se si usano particolari stratagemmi meccanici). La domanda ora è cos'è il DVD ritrovato nel drive? non è sicuramente un corpo di reato perchè non appare nel verbale di sequestro ma l'autorità giudiziaria deve essere avvisata della sua presenza in quanto conviene sicuramente sottoporlo ad analisi (si tratta sicuramente di un reperto interessante dato che si trova nel PC sequestrato).
In definitiva tutti gli elementi di utilità che si individuano sulla scena del crimine sono potenzialmente reperti da analizzare e dal momento della loro individuazione arricchiranno la loro esistenza di due classi di informazioni:

- la serie di verbali che ne definisce il passaggio di mano fino all'archiviazione, distruzione o restituzione a legittimo proprietario;

- l'insieme degli elementi indiziari o probatori che possono essere determinati in via scientifica e/o deduttiva da essi (la serie dei referti e delle discussioni dibattimentali correlate).

Dal punto di vista informatico arriva ovviamente il concetto di informazione digitale a complicare ulteriormente le cose. Si può dire che l'informazione digitale estratta da una qualsiasi memoria digitale è un reperto? e cosa dire per i pacchetti di dati intercettati su una rete di computer? tali elementi possono essere sottoposti sicuramente ad analisi scientifico/forense ma sono altamente immateriali e come tali fortemente correlati, per la loro esistenza, ad un verbale che la attesti inequivocabilmente. Se ad esempio si interviene sulla scena del crimine e si preleva un dato digitale copiandolo è lecito parlare di sequestro o di acquisizione di informazioni come nel caso delle intercettazioni? se è sequestro qual'è il corpo del reato? il supporto su cui si trova copiato il dato? e la catena di custodia di tali informazioni deve riguardare il supporto o i dati? Domande lecite che, data la delicatezza dell'argomento in questione, non trovano facili risposte. A tale scopo risulta utile l'utilizzo di strumenti di firma digitale o, come effetivamente succede nella realtà, predisporre dei 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.

1.5. LE FASI DELL'ATTIVITÀ DI DIGITAL FORENSIC

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.
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 (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) 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. Prima di fornire nel dettaglio le attività che

un tecnico forense esegue, forniamo una breve presentazione delle stesse mediante l'ausilio di un diagramma di flusso:

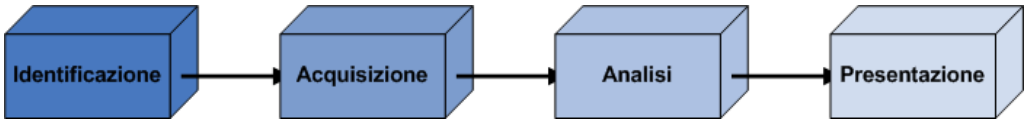

Figura 1: le fasi dell'attività forense

Anche se il processo descritto evidenzia un flusso diretto in avanti e senza possibilità di ritorno è da considerare comunque la possibilità di eseguire il backup di alcuni passaggi di tanto in tanto, questo perché:

- durante la fase di acquisizione si potrebbe scoprire di aver bisogno includere più fonti di dati, costringendoci al ridimensionamento del piano di Acquisizione;
- Durante l'analisi si potrebbe scoprire che alcune informazioni fanno riferimento a fonti di dati non acquisiti;
- Durante la presentazione i dati potrebbero essere messi in discussione con domande che richiedono di eseguire ulteriori analisi al fine di fornire risposte più soddisfacenti.

Non importa se ci avviciniamo al mondo della digital forensic tramite una o più fonti di dati, non importa quali siano tali fonti di dati o se saranno o meno utilizzate. Vi è una base, inerente al processo di computer forensic, che è pienamente descritta con le 4 fasi appena presentate:

- Identificazione
- Acquisizione
- Analisi
- Presentazione

1.5.1. Il processo di identificazione

Il primo e fondamentale passo nel digital forensic è determinare dove cercare la prova digitale nel senso di stabilire quale apparato è in grado almeno teoricamente di memorizzare informazioni digitali attendibili ed inerenti il caso in studio per poi capire in quale stato dovrebbe essere repertato e/o analizzato. Il repertamento fisico è la fase nella quale l'apparato digitale viene sigillato per la successiva analisi di laboratorio. Si noti la distinzione tra esso ed il repertamento dati che si riconduce sommariamente ad una copia certificata di dati di interesse. Sebbene molti pensino che questa attività si limiti al repertamento ed analisi dei personal computer nella realtà esso si estende ad una grande varietà di sistemi elettronici digitali. La valutazione di quale tra i sistemi digitali presenti nell'area di competenza debba essere repertato per la successiva analisi non risulta immediata. Telefoni cellulari, organiser(s), smart-card(s), palmtop, intere reti di computer, ecc. potrebbero in molti casi risultare utili ed il riconoscimento del loro stato (attivi, spenti, batteria scarica, connessi, ecc.) sicuramente influisce sulla decisione di acquisirli e sulla modalità per farlo. L'esempio ormai classico del provider di servizi Internet per utenti comuni che nei suoi server mantiene informazioni utili a delle indagini ha portato, in questi ultimi dieci anni, a sequestrare e bloccare fisicamente interi apparati (commettendo peraltro diversi illeciti) mentre il repertamento avrebbe dovuto limitarsi esclusivamente alle informazioni di interesse presenti nelle memorie di massa. Tale esempio è uno dei più importanti riscontri dei problemi legati ad un errato processo di identificazione.

1.5.2. Il processo di acquisizione

Per l'acquisizione delle prove da un sistema informatico il modo migliore sarebbe quello di poter accedere al sistema con il ruolo di amministratore, 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. Per una corretta documentazione del processo di acquisizione delle prove non si esclude la possibilità di filmare addirittura tutta la fase di individuazione e di acquisizione 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.

Una nota molto importante deve essere riportata in relazione al tipo di acquisizione dei dati di una memoria di massa o di una device digitale in genere. Si possono distinguere infatti almeno tre livelli di copia:

- copia di livello fisico: o bitstream copy, in cui il contenuto dell'unità fisica viene letto sequenzialmente (la sequenza è stabilita dall'indirizzamento fisico, in genere gestito dal controller dell'unità di memoria) caricando la minima quantità di memoria di volta in volta indirizzabile (ad es. negli hard disk il settore fisico, nelle ROM il byte, ecc.) per poi registrarla nella stessa sequenza su di un comune file binario (immagine fisica dell'unità);
- copia di basso livello del file system: o cluster-copy, in cui il contenuto di una partizione logica (strutturatasi a seguito di una formattazione correlata ad un preciso file system) viene letto sequenzialmente caricando la minima quantità di memoria che il file system consente di indirizzare di volta in volta (ad es. il cluster in FATxx) per poi registrarla nella stessa sequenza su di un comune file binario (immagine di basso livello del file system);
- copia del file system: in cui parte o tutto il contenuto di alto livello di una partizione logica (strutturatasi a seguito di una formattazione correlata ad un preciso file system), ivi intendendo i contenuti di file e directory evidenti (non cancellati), viene sottoposto a backup su di un file (file di backup) di particolare formato (dipendente dal tool impiegato).

1.5.3. Il processo di analisi

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 evidenziato in, l'analisi forense deve rispettare le seguenti regole:

- Minimo trattamento dei dati di partenza: il caso ideale è ovviamente quello in cui si riesce a svolgere una copia completa e certificata dei dati utili. In tale situazione infatti l'oggetto di analisi è la copia e quindi la probabilità di alterazione dei dati in origine è praticamente nulla. Purtroppo esistono dei casi particolari nei quali non è possibile svolgere copie complete e quindi bisogna operare direttamente sul reperto originale. In questo frangente è necessario svolgere tutte quelle operazioni minime indispensabili a scopo forense che garantiscano la minima alterazione possibile del sistema in studio.
- Logging delle attività: tutte le attività svolte durante l'analisi forense devono essere accuratamente registrate in un log o meglio ancora in un report ricco di particolari che consentano, nel migliore dei casi, di ripetere tutte le azioni svolte ma comunque sempre di evidenziare se siano state avviate alterazioni dei dati originali (magari indispensabili al fine di ottenere le prove digitali cercate). In particolare di ogni alterazione bisogna sottolineare chi la origina, in cosa consiste ed a quali limiti si estende, se è avvenuta a livello logico o fisico, lo stato preesistente (qualora rilevabile), le motivazioni del cambiamento, etc.
- Ammissibilità legale dei risultati: le prove digitali che si ottengono devono provenire da una procedura tecnica che rispetta appieno le locali leggi.

Un problema comune nel settore del digital forensic è la necessità di prendere in considerazione tutti i dati disponibili per l'attività. Questo vincolo non è sempre di banale soddisfazione. Uno dei casi più evidenti è quello del time-stamping di file, e-mail, log(s), ecc.,

ipotizzando l'analisi di un PC, l'analisi di date ed orari dipende ovviamente dallo stato dell'orologio interno e quindi, più in generale, del BIOS, da cui la semplice copia dell'hard disk non porta tutte le informazioni necessarie. Un altro caso interessante è quello in cui la configurazione interna del computer analizzato è di un qualche interesse ai fini dell'indagine, ecc., la scelta quindi del cosa considerare come dato per l'analisi si deve lasciare al singolo caso.

1.5.4. Il processo di presentazione

Le citate attività tecniche (identificazione, acquisizione ed analisi del sistema informatico) trovano, nel settore informatico forense, sfogo unico e sostanziale nell'esposizione dibattimentale e quindi un errore espositivo e/o formale può vanificare mesi di analisi ed invalidare anche prove digitali molto evidenti.

Le presentazioni delle prove digitali (in genere tramite relazioni tecniche e discussioni) vengono preparate basandosi su aspetti sociali e psicologici, informatici e legali imponendo la costituzione di un gruppo di lavoro interdisciplinare il più delle volte difficile da integrare causa le evidenti differenze degli approcci professionali nei singoli settori.

L'ideale è scindere il più possibile le considerazioni di tipo legale da quelle di natura prettamente tecnica. Ciò consente agli operatori di muoversi più liberamente svincolandosi da condizionamenti relativi ai risultati della loro attività di analisi. Questo se lo scopo, eticamente corretto, è la ricerca della "verita" e non la verifica di un'ipotesi accusatoria o difensiva.

Una valida e completa relazione tecnica di un'attività forense dovrebbe contenere: la sintesi dei principi scientifici accademicamente riconosciuti su cui l'analisi ed il repertamento si basano, la catena di custodia dei reperti (generalmente formata dai verbali che ne testimoniano prelievi, trasferimenti e luoghi di permanenza) e la loro accurata descrizione, le specifiche richieste

dell'Autorità Giudiziaria con annesse le necessarie e precise autorizzazioni della Procura competente, la descrizione delle operazioni tecniche svolte in laboratorio e l'esito finale.
Di dette parti, le richieste dell'autorità giudiziaria e l'esito finale rappresentano gli elementi chiave che vengono presi in considerazione da avvocati, giudici e pubblici ministeri al fine di trarre conclusioni di ordine legale. Tutte le altre vengono riportate in maniera da rendere agevole lo studio e l'eventuale ripetizione delle analisi da parte di ulteriori organi tecnici forensi.
In particolare, l'esito finale deve avere le seguenti caratteristiche:

- sintetico: dato che non necessita di riportare eccessivi particolari tecnici dell'analisi ma solo ciò che interessa dal punto di vista giuridico.
- semplificato: colui che legge e valuta l'esito è di principio un fruitore inesperto nel settore informatico e quindi, nell'ipotesi che sia possibile, bisogna eliminare terminologie non consuete e spiegare a livello elementare quanto rilevato.
- asettico: non deve contenere giudizi personali dell'operatore né tanto meno valutazioni legali sulle informazioni rilevate a meno che tali considerazioni non siano state espressamente richieste.

La relazione tecnica è quindi, assieme ad altri elementi provenienti dalle indagini classiche, la base per il dibattimento e non dovrebbe suggerire considerazioni di tipo legale che invece sono da formarsi in tale frangente processuale.

1.6. IL KIT DELL'INFORMATICO FORENSE

Utilizzare una metodologia e gli strumenti corretti 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 [Sca07]. 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.

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.

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:

- va accuratamente verificato lo stato di ogni supporto magnetico;
- vanno ispezionati quaderni, fondi di tastiera e monitor per individuare eventuali password;
- va ricostruita (tracing) l'attività di un accesso abusivo dalla rete, 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);
- vanno individuati virus e altro software malevolo, dove per codice malevolo 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);

- 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, 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;
- va effettuato un accurato inventario delle attrezzature ispezionate;
- è opportuno ripetere due volte le analisi per avere certezza della meticolosità delle operazioni eseguite.

Le operazioni da compiere non sono poche e richiedono la massima attenzione da parte di qualsiasi operatore sia stato chiamato ad eseguirle, pena la nullità dell'elemento probatorio in seduta dibattimentale.

Capitolo 2

STATO DELL'ARTE DELLA COMPUTER FORENSIC

2.1. I REATI INFORMATICI

Le tipologie di reato in Internet sono di svariati tipi: si pensi al messaggio offensivo inviato per posta elettronica, alla diffusione di immagini diffamatorie o pedopornografiche, o al download di risorse protette dal diritto d'autore [Viz06]. L'identificazione dell'autore di un reato online è resa problematica da molteplici fattori: in un sistema, quale Internet, non controllato da alcuna autorità sovranazionale che consente agli utenti un assoluto anonimato, dove i dati si diffondono con rapidità elevatissima oltre i confini nazionali, e dove cancellare le tracce è relativamente semplice, identificare il responsabile di un reato è un'operazione davvero complessa che difficilmente viene eseguita con successo [Cos06].
Pertanto un reato informatico è un fenomeno criminale che si caratterizza per l'abuso della tecnologia informatica. Tutti i reati informatici sono accomunati da:

- L'utilizzo della tecnologia informatica per compiere l'abuso;
- L'utilizzo dell'elaboratore nella realizzazione del fatto.

L'esigenza di punire i crimini informatici, emerse già alla fine degli anni '80, tanto che, il 13 Settembre 1989, il Consiglio d'Europa ha emanato una 'Raccomandazione sulla Criminalità Informatica' dove

venivano discusse le condotte informatiche abusive. I reati vennero divisi in due liste: facevano parte della prima lista detta 'lista minima' quelle condotte che gli Stati sono invitati a perseguire penalmente quali:

- La frode informatica che consiste nell'alterare un procedimento di elaborazione di dati con lo scopo di procurarsi un ingiusto profitto;
- Il falso in documenti informatici;
- Il danneggiamento di dati e programmi;
- Il sabotaggio informatico;
- L'accesso abusivo associato alla violazione delle misure di sicurezza del sistema;
- L'intercettazione non autorizzata;
- La riproduzione non autorizzata di programmi protetti;
- La riproduzione non autorizzata di topografie.

Facevano invece parte della seconda lista detta 'lista facoltativa' condotte 'solo eventualmente' da incriminare, quali:

- L'alterazione di dati o programmi non autorizzata sempre che non costituisca un danneggiamento;
- Lo spionaggio informatico inteso come la divulgazione di informazioni legate al segreto industriale o commerciale;
- L'utilizzo non autorizzato di un elaboratore o di una rete di elaboratori;
- L'utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto.

Successivamente, in occasione del XV Congresso dell'Associazione Internazionale di Diritto Penale (AIDP) del 1990, emerse la necessità di incriminare non solo i reati previsti dalla lista minima ma anche le condotte descritte nella lista facoltativa. Le varie legislazioni

informatiche che hanno seguito il XV Congresso dell'AIDP hanno tenuto conto delle indicazioni date dall'associazione e nel Settembre 1994 il Consiglio d'Europa ha aggiornato la precedente Raccomandazione ampliando le condotte perseguibili penalmente, inserendo:

- Il commercio di codici d'accesso ottenuti illegalmente;
- La diffusione di virus e malware.

2.2. IL PANORAMA NORMATIVO ITALIANO

Il legislatore ha scelto di collocare i nuovi reati informatici accanto alle figure di reato già esistenti. Tra queste evidenziamo:

- La Frode Informatica. Viene associata alla frode 'tradizionale' con la differenza che viene realizzata per mezzo di uno strumento informatico. La legge 547 del 1993 aggiunge al Codice Penale l'art 640-ter per punire chiunque cerchi di ottenere un arricchimento interferendo abusivamente nell'elaborazione dei dati. Non viene identificato come frode informatica l'indebito utilizzo di carte di pagamento magnetiche che è invece disciplinato dall'art. 12 della legge 197 del 5 Luglio 1991.
- La Falsificazione di Documenti Informatici. I documenti informatici sono equiparati a tutti gli effetti ai documenti tradizionali e l'art. 491-bis c.p. prevede l'applicabilità delle disposizioni sulla falsità in atti pubblici e privati. La falsificazione in comunicazioni informatiche ricalca invece il delitto di falsità in scrittura privata (art. 485 c.p.).
- Le Aggressioni all'Integrità dei Dati. La legge 547 del 1993 amplia le precedenti disposizioni in materia e integra al

Codice Penale l'art. 635-bis sul danneggiamento dei sistemi informatici e telematici, l'art. 615-quinquies sulla diffusione di virus e malware, l'art. 392 sulla violenza sulle cose (a tal proposito la legge 547 del 1993 precisa le situazioni dove le aggressioni riguardano beni informatici) ed infine l'art. 420 sul reato di attentato ad impianti di pubblica utilità.

- Le Aggressioni alla Riservatezza dei Dati e delle Comunicazioni Informatiche. Riguardo le forme di intrusione nella sfera privata altrui si incriminano l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), la detenzione e diffusione abusiva di codici d'accesso (art. 615-quater c.p.) la rivelazione del contenuto di documenti segreti (art. 621 c.p.) includendo i documenti protetti contenuti su supporti informatici.

Circa le aggressioni alle comunicazioni informatiche viene ampliato il concetto di corrispondenza contenuto nel quarto comma dell'art. 616 c.p. che ingloba anche la corrispondenza informatica e telematica e punisce l'intercettazione e l'interruzione di comunicazioni informatiche (art. 617-quater c.p.) e l'installazione di apparecchiature atte ad intercettare o impedire comunicazioni informatiche (art. 617-quinquies), qualora tali condotte non siano esplicitamente autorizzate.

2.3. ANALISI DI ALCUNI TIPI DI REATO

L'elenco dei reati perseguibili penalmente, o comunque che possono essere considerati tali, sono diversi e ciascuno ha le sue proprie caratteristiche. Il fattore comune, tuttavia, è dato dall'utilizzo delle sempre nuove tecnologie immesse sul mercato e dal diffondersi continuo di strumenti di diffusione dell'informazione come ad esempio gruppi di discussione, blog e forum. Anche in questo caso è ovvio come si stia parlando delle due facce della stessa medaglia.
Di seguito riportiamo alcuni esempi di tipologia di reato che sono oggetto di studio e di analisi da parte della Polizia Postale.

2.3.1. Opere pirata e diritto d'autore

Nei casi di pirateria, viene punita l'appropriazione indebita dell'idea originale. Gli oggetti che si intende tutelare sono di diversi tipi. Nell'ambito informatico troviamo:

- Le Topografie: con qualche anno di ritardo rispetto ai termini previsti dalla direttiva europea, la legge 70 del 21 Febbraio 1989 tutela le topografie di prodotti a semiconduttori ovvero i tracciati incisi sulle piastrine di silicio. A tal proposito non sono previste sanzioni penali per le violazioni dei diritti nonostante la Raccomandazione del 13 Settembre 1989 del Consiglio d'Europa le preveda.
- I Software: con la modifica della legge 633 del 22 Aprile 1941 sul diritto d'autore, i programmi per elaboratore vengono inclusi tra le opere di ingegno. In seguito alla Direttiva CEE del 14 Maggio 1991 recepita dal Dlgs 518 del 29 Dicembre

1992, si vuole prevenire la duplicazione e la vendita dei programmi a fine di lucro (art. 171-bis 1.a.). La sanzione pecuniaria prevista viene successivamente aggravata dal Dlgs 205 del 15 Marzo 1996.

- I sistemi informativi e le basi di dati: il Dlgs 169 del 6 Maggio 1999 riconosce i diritti di esclusiva al creatore del database (artt 64-quinquies e sexies) e il diritto di tutela al 'costitutore' del database, ovvero a colui che effettua investimenti in termini di tempo e denaro per raccogliere e inserire materiale nel database, con il fine di salvaguardare il valore patrimoniale dell'investimento.
- Le Opere Fonografiche e Videografiche: gli abusi di duplicazione e distribuzione, vengono disciplinati dalla legge 406 del 29 Luglio 1981, mentre le opere cinematografiche destinate al circuito cinematografico e televisivo sono tutelate dalla legge 400 del 20 Luglio 1985.

2.3.2. La frode informatica

La frode informatica o altresì detta frode elettronica, in generale consiste nel penetrare attraverso un pc all'interno di server che gestiscono servizi con lo scopo di ottenere tali servizi gratuitamente, oppure, sempre utilizzando il server al quale si è avuto accesso, clonare account di ignari utilizzatori del servizio.
Le frodi elettroniche presuppongono anche l'utilizzo del POS (Point of Sales che letteralmente significa punto vendita), un apparato elettronico di trasmissione dati che collega i singoli esercenti con la società emettitrice, e consistono proprio nell'abuso di alcune sue specifiche proprietà, come la capacità di leggere, memorizzare e trasmettere i dati delle carte di credito (e dei titolari) contenute nella banda magnetica. Esistono due specifiche operazioni illegali eseguite in presenza di un POS:

- intercettazione dei dati, mediante apparati elettronici (vampiri o sniffer), durante l'operazione di trasmissione degli stessi per l'autorizzazione all'acquisto. L'intercettazione è finalizzata a reperire dati di carte utilizzabili per ricodificare le bande di carte rubate o false. Viene realizzata mediante un computer e appositi collegamenti che catturano i dati in uscita dal POS dell' esercente (con la sua complicità o sua insaputa);
- dirottamento dei dati durante la loro trasmissione per l'accredito. Il dirottamento presuppone la cattura, da parte di un computer collegato alla linea telefonica, dei dati riguardanti lo scarico del logo e la falsificazione delle coordinate di accredito del negoziante, per dirottare gli importi su un altro conto cotrollato dall'autore del crimine).

La frode informatica costituisce reato con fattispecie e pene distinte da quello di frode, di recente istituzione, introdotta dalla legge n. 547/1993 e disciplinata dall'art. 640 ter del c.p. Il delitto di frode informatica è commesso da "chiunque", alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. Le condotte fraudolenti poste in essere attraverso tale reato sono tre:

- la prima consiste nell'alterazione del funzionamento del sistema informatico o telematico, ossia in una modifica del regolare svolgimento di un processo di elaborazione o di trasmissione dati; l'alterazione provoca i suoi effetti materiali sul sistema informatico o telematico;
- la seconda coincide con l'intervento, senza diritto, con qualsiasi modalità, su dati, informazioni o programmi contenuti nel sistema, e pertanto ogni forma di interferenza

diversa dall'alterazione del funzionamento del sistema. L'intervento senza diritto ha per oggetto i dati, le informazioni o i programmi. Solitamente questa seconda condotta rappresenta la modalità attraverso cui viene realizzata la alterazione del sistema informatico;

- la terza coincide con l'intervento sulle informazioni, ovvero sulle correlazioni fra i dati contenuti in un elaboratore o in un sistema.

L'alterazione può ricadere sia sul programma, facendo compiere al computer operazioni in modo diverso da quelle programmate (ad esempio cambiando la funzione dei tasti di addizione e/o di sottrazione), così come può avere ad oggetto le informazioni contenute nel sistema informatico.
Nella storia dell'informatica, e più specificamente in quella di Internet, è capitato che gli autori di questo genere di frode venissero assunti da parte delle stesse società alle quali avevano arrecato danno, allo scopo di usare le conoscenze del trasgressore per migliorare i sistemi di sicurezza interni dell'azienda. Non è definibile hacker chi si introduce in un sistema per danneggiarlo o per provocare il mal funzionamento con l'intenzione di trarne un ingiusto profitto, poiché tale tipologia di comportamento è in netto contrasto con la filosofia dell'hacking. Nel caso di acquisti o operazioni attraverso la rete Internet, le truffe possibili sono effettuate dai cosiddetti "pirati informatici" (coloro che acquistano i numeri della carta attraverso un'intrusione telematica). Una delle prime frodi informatiche è stata la sottrazione di fondi attuata con la così detta "tecnica del salame". Il bersaglio ideale era una banca perché movimenta migliaia di conti al giorno. Questa frode avveniva agendo sugli arrotondamenti che quotidianamente venivano operati su ogni movimento di fondi.

2.3.2.1. Un esempio di frode informatica: il phishing

Al giorno d'oggi è in forte aumento, quasi esponenziale si potrebbe dire, la truffa on line, nata in Spagna e Portogallo, chiamata "phishing". Si tratta di una nuova forma di spamming, che potrebbe avere come conseguenza il furto del numero di carta di credito o di password, informazioni relative a un account o altre informazioni personali. Tale truffa solitamente ha come campo di azione le banche e l'e-commerce.

Il phishing è un tipo di frode ideato allo scopo di rubare l'identità di un utente. Quando viene attuato, una persona malintenzionata cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali convincendo l'utente a fornirgliele con falsi pretesti. Il phishing viene generalmente attuato tramite posta indesiderata o finestre a comparsa.

Il phishing viene messo in atto da un utente malintenzionato che invia milioni di false e-mail che sembrano provenire da siti Web noti o fidati come il sito della propria banca o della società di emissione della carta di credito. Arriva dunque nella propria casella di posta elettronica un'e-mail che sembra provenire dalla banca e vi dice che c'è un imprecisato problema al sistema di "home bancking". Vi invita pertanto ad aprire la home page della banca con cui avete il conto corrente gestito via web e di cliccare sul link indicato nella mail. Subito dopo aver cliccato sul link vi si apre una finestra (pop-up) su cui digitare la "user-id" e la "password" di accesso all'home bancking. Dopo pochi secondi, in generale, appare un altro pop-up che vi informa che per assenza di collegamento non è possibile la connessione. I messaggi di posta elettronica e i siti Web in cui l'utente viene spesso indirizzato per loro tramite sembrano sufficientemente ufficiali da trarre in inganno molte persone sulla

loro autenticità. Ritenendo queste e-mail attendibili, gli utenti troppo spesso rispondono ingenuamente a richieste di numeri di carta di credito, password, informazioni su account ed altre informazioni personali. Queste imitazioni sono spesso chiamate siti Web ingannevoli ("spoofed"). Una volta all'interno di uno di questi siti falsificati, è possibile immettere involontariamente informazioni ancora più personali che verranno poi trasmesse direttamente all'autore del sito che le utilizzerà per acquistare prodotti, richiedere una nuova carta di credito o sottrarre l'identità dell'utente.

Oltre agli estremi del reato di frode informatica, di cui all'art. 640 ter del codice penale, il phishing integra l'ipotesi delittuosa della truffa. Il reato di frode informatica, come ha ricordato più volte la giurisprudenza della Cassazione (v., in particolare Cass. sez. IV, 4 ottobre 1999, n. 3056) ha la medesima struttura, e quindi i medesimi elementi costitutivi, della truffa, dalla quale si distingue solamente perché l'attività fraudolenta dell'agente investe non la persona, bensì il sistema informatico (significativa è la mancanza del requisito della "induzione in errore" nello schema legale della frode informatica, presente invece nella truffa). Di talché il phishing da un lato, induce in errore la persona che fornisce inconsapevolmente i propri dati al phisher, dall'altro lato la sua azione investe il sistema informatico dell'istituto creditizio poiché interviene sine titulo all'interno dello stesso.

Il reato di frode informatica presenta numerose analogie con quello di truffa: identico trattamento sanzionatorio (da sei mesi a tre anni unitamente alla multa da 51 a 1032 euro), e analoga suddivisione fra un'ipotesi delittuosa semplice ed una aggravata dagli stessi elementi previsti dal secondo comma dell'art. 640, e analogo simmetrico richiamo alla procedibilità a querela nell'ipotesi semplice legato procedibilità officiosa nell'ipotesi aggravata.

Inoltre anche il trattamento sanzionatorio previsto per l'ipotesi aggravata della frode informatica è identico rispetto a quello previsto dall'art. 640 c.p. per la truffa aggravata, ovvero della

reclusione da uno a cinque anni e della multa da trecendonove a millecinquecento euro. Queste circostanze ci consentono di replicare anche per la frode informatica le considerazioni di natura processuale spese per la truffa, aggiungendo che esiste anche la possibilità giuridica del cumulo fra i due reati, anzi che nella maggior parte dei casi il phishing costituisce un'attività criminale che viola le prescrizioni previste da entrambe le norme incriminatici.
La Polizia postale, per contravvenire a questo fenomeno, ha comunque inviato una circolare all'ABI (Associazione Bancaria Italiana) invitando le banche ad avvertire i propri clienti di non digitare i codici personali nel caso dovessero ricevere questo tipo di e-mail.
Il fenomeno del phishing che in realtà non coinvolge solo le banche ma in generale le varie aziende che si occupano di e-business è oggi considerato la parte dello spam più in crescita in tutto il mondo e colpisce sia le aziende che i consumatori.
Proprio per questi motivi Microsoft, e-Bay e Visa hanno deciso di dar vita al Phish Report Network: una sorta di database che raccoglie le informazioni utili per identificare le e-mail truffaldine che arrivano agli utenti di tutto il mondo e che consentirà di stilare una lista nera dei siti del phishing a cui sono stati attribuiti molti tentativi di truffa.
In questo contesto, si inseriscono le operazioni di acquisizione e di analisi del traffico di rete effettuate dalla polizia postale e che vanno sotto il nome di network forensic. Lo scopo di tale attività è quello di ricercare e identificare, se non direttamente le persone responsabili, l'origine di questo tipo di reato.

2.3.2.2. Un esempio di frode informatica: il typosquatting

Il typosquatting è una forma evoluta di cybersquatting e consiste nel registrare un nome di dominio molto simile a quello utilizzato da

un'altra società, con un duplice obiettivo: intercettare una parte del traffico indirizzato al sito ufficiale e intercettare il maggior numero possibile di e-mail inviate a indirizzi della società presa di mira.
Spesso gli utenti commettono un errore digitando l'indirizzo Internet di un sito Web; se il nome di dominio del typosquatter è sufficientemente simile, ha buone possibilità di intercettare questo tipo di traffico che viene, così, "autodirottato".
Ovviamente, se il sito è poco visitato, il fenomeno interessa una piccola percentuale di utenti; nel caso di siti con un traffico molto elevato, però, la percentuale può crescere, fino a raggiungere le migliaia di visitatori al giorno.
Il pirata, in questo modo, può veicolare messaggi pubblicitari o proporre prodotti e servizi forniti da società concorrenti o complementari alla società-vittima. Il segreto di questa tattica risiede nella capacità di individuare un indirizzo di typosquatting basato sugli errori di digitazione più frequentemente commessi dagli utenti.
In altre parole, se questo sito in oggetto si chiama www.pcalsicuro.com, secondo il typosquatting qualcuno potrebbe registrare il dominio "www.pcaslicuro.com" e utilizzarlo per trasmettere del malware. Si tratta, in altre parole, di avvicinarsi il più possibile all'indirizzo del sito originale di cui si vuole simulare l'URL in modo tale che un utente, digitando frettolosamente, si possa ritrovare su una pagina infetta.
Risulta interessante vedere come questi truffatori si siano dati da fare registrando molti domini tra i quali:

www.corrire.it, www.ilmessagero.it, www.messagero.it,
www.tutttogratis.it, www.reppublica.it, www.googler.it,
www.googlie.it, hotmaill.it, liberol.it, www.quattoruote.it,
www.unfi.it, wwwgenialloyd.it, wwwilmessaggero.it, www.ispsel.it,
www.googlew.it, www.juvenus.it, wwwhwupgrade.it,
www.corriete.it, www.uninib.it, www.unpi.it, www.freonline.it,

www.pagineialle.it, nirgilio.it, www.asnsa.it, www.repubblica.it, tuttoratis.it, www.sbobba.it, www.egazzetta.it, libvero.it, www.alitala.it, wwwadr.it.

In effetti, la mera attività di typosquatting non dovrebbe essere illegale, perché si tratta della registrazione di un nome di dominio come altri. Al massimo, il problema potrebbe arrivare se la società il cui dominio è stato "copiato" volesse acquistare anche i domini simili al suo e di conseguenza si entrerebbe in un affare privato. In questo caso, però, l'attività di typosquatting è legata ad un'azione di diffusione di malware.

Nell'ottobre del 2001, Marc Schneider ha pubblicato i risultati di una ricerca condotta sul campo. Qualche tempo prima, aveva registrato il nome di dominio "jptmail.com", molto vicino al noto "hotmail.com".

I due caratteri diversi, "j" e "p", sulla tastiera sono situati immediatamente alla destra della "h" e della "o" dell'indirizzo originale.

In realtà, questo indirizzo non era stato ben concepito, essendo necessario che vengano fatti ben due errori di digitazione consecutivi, cosa che avviene piuttosto raramente.

Nonostante tutto, però, è riuscito a dirottare, in un anno, ben 3.000 visitatori.

Si calcola che un indirizzo con un solo errore di digitazione potrebbe dirottarne fino a dieci volte di più.

Il procedimento seguito per intercettare parte delle e-mail indirizzate alla società vittima consiste nell'attivare i propri server MX (che sono i nomi dei server di posta elettronica) e indicare che si vuole ricevere tutte le e-mail spedite a xxx@proprionome.xx, senza far puntare il nome di dominio su un sito.

In altre parole, se una libreria online registra il nome di dominio "amzon.com" e recupera tutte le mail inviate a xxx@amzon.com o sales@amzon.com, potrà facilmente intercettare una parte della

clientela di Amazon, offrendo i propri prodotti agli utenti che hanno richiesto informazioni, commettendo un piccolo errore di digitazione. Nel caso citato da Marc Schneider, xxx@jptmail.com aveva ricevuto circa 300 messaggi in nove giorni, potenzialmente 9.000 al mese.
La strategia dei typosquatters è fondamentalmente basata su questi punti: concentrarsi su siti con un forte traffico, registrare numerose varianti del nome invertendo le lettere o sostituendone alcune, oppure depositare dei nomi che sono varianti fonetiche di quelli originali.

2.3.3. Il reato di pedofilia e scambio di materiale pedo-pornografico

I gruppi di lavoro costituiti all'interno della Polizia Postale si occupano anche di contrastare le attività [BSDRI05] di sfruttamento dei minori al fine di produrre, diffondere, commercializzare e pubblicizzare materiale pedo-pornografico su Internet. Effettuano un monitoraggio continuo degli spazi web impropriamente utilizzati per promuovere la pedofilia nonché per attrarre minori a fini di adescamento degli stessi. Tale impegno, posto in essere per contrastare un fenomeno che negli ultimi tempi ha destato notevole allarme sociale, viene coordinato anche con l'attività di associazioni non governative, quali l'ECPAT (End Child Prostitution, Pornography And Trafficking), il Telefono Azzurro ed il Telefono Arcobaleno, e semplici cittadini che segnalano costantemente situazioni potenzialmente rilevanti sotto il profilo penale. A tal fine viene svolto un continuo servizio di monitoraggio di Internet, finalizzato all'individuazione di siti a carattere pedo-pornografico, che vengono censiti e catalogati mediante un data-base presente al Servizio Polizia Postale e delle Comunicazioni, consultato per evitare duplicazioni di indagini. Nel corso di tali servizi si individuano, inoltre, i soggetti presenti su canali "chat" e "bbs" al fine di

reprimere le condotte delittuose tramite l'effettuazione dell'attività di contrasto prevista dall'art.14 L.269/98, che viene coordinata dal Servizio centrale per una migliore ottimizzazione delle forze e delle notizie.

2.4. ALCUNE CONSIDERAZIONI

Nonostante la normativa italiana in materia sia una delle più recenti, l'informatica avanza molto più velocemente di quanto possano fare le leggi. A complicare una situazione già complessa si aggiungono:

- la difficoltà che si riscontra nell'identificazione della persona che ha commesso il reato una volta identificato il sistema informatico utilizzato per commettere il reato
- la possibilità di essere vittime di criminali informatici che attaccano da stati con ordinamenti diversi dal nostro
- la possibilità di celare con facilità l'identità del criminale dietro quella di altre persone innocenti
- la carenza di sentenze a riguardo

Ci si trova pertanto molto spesso di a dei vuoti normativi a cui è davvero difficile porre rimedio.

2.5. PROBLEMATICHE CONNESSE ALL'ATTIVITÀ FORENSE

Tra le problematiche di carattere tecnico che si presentano più di frequente all'attenzione di chi opera l'analisi di sistemi informatici è opportuno evidenziarne le più frequenti, che saranno esposte, per quanto possibile, con criteri cronologici, simulando una serie di eventi che tipicamente si presentano in successione, nel corso dell'attività in esame [PGDC07], [Sav03].

- Presenza di password sul BIOS e necessità di superarle. La difficoltà può essere spesso superata, specialmente nelle operazione che riguardano computers portatili, procurandosi, su siti internet dedicati, le password generiche (così dette di default, predefinite) che di solito il costruttore riserva per poter accedere al BIOS, quando opera per l'assistenza ai prodotti della sua azienda. In certe circostanze, però, si rende impossibile accedere al BIOS e pertanto si procede alla delicata operazione di smontaggio del disco rigido presente nel computer e di istallazione in un altro sistema dedicato all'analisi. In tal modo, la password sarà aggirata e sarà possibile accedere ai dati contenuti nel disco. In casi estremi è possibile rimuovere la batteria tampone, presente sulla scheda madre, che permette di conservare, a sistema spento, i dati presenti nel BIOS. Detta pratica deve essere, se possibile, evitata poiché, in tal caso però, insieme alla password, andranno persi i dati presenti nel BIOS, tra i quali i riferimenti cronologici del sistema.
- Lunghezza delle operazioni di calcolo del checksum o hash (MD5 o SHA1) del supporto originale e della sua copia. La possibilità di dar corso alla detta operazione va valutata di

volta in volta, in relazione ai tempi dell'indagine ed alla necessità di utilizzare sistemi di garanzia di inalterabilità della prova alternativi a quelli tradizionali.

- Difficoltà di visualizzare file dei più diversi formati. Opportune ricerche sulla rete internet permettono spesso di reperire idonei programmi di visualizzazione. In alcuni casi, i file (proprietari) sono leggibili solo a mezzo dei programmi attraverso i quali sono stati creati, non essendo visualizzabili attraverso il programma utilizzato per l'analisi o altro visualizzatore. In tal caso, quando non è possibile disporre del programma originale, è opportuno uscire dal programma di analisi ed utilizzare una copia del disco in esame, per riavviare il sistema originale, di modo che il file sarà visualizzato dal programma che lo ha creato, se era presente nel sistema oggetto di analisi. In estrema ratio, è possibile aprire il file non intelligibile con un editor esadecimale (es. hexedit) che mostrerà bit per bit il contenuto del file.
- Difficoltà di rilevare file e file-system crittografati e/o steganografati. Fermo restando il problema di visualizzare i detti file, senza possedere la chiave di decodifica, è opportuno perlomeno dare atto della loro presenza, utilizzando idonei programmi (es. stegdetect) atti a rilevare quelli steganografati. Per i file crittografati vi è unicamente la possibilità di operare per esclusione. Al fine di accedere al contenuto di files protetti da password è possibile utilizzare appositi programmi di vario genere. È però opportuno che l'uso di detti programmi sia specificatamente autorizzato dal Pubblico Ministero, analogamente a quanto avviene per la rimozione di ostacoli fissi in sede di perquisizione locale.
- Difficoltà di procedere all'esame di nuovi supporti informatici, come le console di videogiochi (es. Xbox della Microsoft, dotata di disco rigido), penne USB, lettori ibridi musicali e di dati, telefoni cellulari di nuova generazione, fotocamere

digitali, "memory card" (schede di memoria), etc. etc. che possono essere utilizzati per immagazzinare informazioni digitali. Aldilà delle problematiche già esposte relative all'utilizzo di specifiche apparecchiature, per quel che riguarda i programmi, alcuni operatori della Polizia Postale e delle Comunicazioni, hanno approntato una metodologia efficace, basata principalmente sull'utilizzo di programmi "open source", per l'acquisizione con atto ripetibile e la successiva analisi dei dati contenuti in questi nuovi supporti informatici.

- Particolari difficoltà si possono talvolta incontrare quando si effettua l'esame di materiale sequestrato da altri Uffici di Polizia. La difficoltà più frequente consegue al fatto che gli hard disk sequestrati possono essere configurati in modo tale da rendere impossibile l' estrapolazione delle evidenze informatiche in quanto, per rendere funzionanti tali supporti, è necessario che siano installati simultaneamente (configurazione RAID), su un computer dotato di un controller di disco rigido identico a quello installato nel computer dal quale i dati sono stati prelevati. Il problema può essere aggirato riproducendo la situazione originaria ed effettuando l'acquisizione delle fonti di prova tramite il software in dotazione. Nei casi sopraccitati è evidente che una maggiore collaborazione tra gli uffici interessati, fin dalla fase iniziale delle attività di polizia giudiziaria, eviterebbe all'origine il problema (una possibile soluzione è creare un simulatore di controller RAID).
- Problemi di non poco conto si possono avere durante l'acquisizione di un disco rigido sequestrato effettuata con il programma ENCASE, poiché si possono verificare una lunga e vasta serie di errori, dovuti spesso allo stato deprecabile del supporto in osservazione. Solo avviando in modalità di sola lettura il predetto disco, con l'uso del sistema operativo GNU/Linux, è possibile acquisire la parte di dati utili alle

indagini e visionarli successivamente con il programma ENCASE.

- Ulteriori difficoltà possono emergere quando si interviene durante un'analisi immediata in sede di perquisizione, nei sistemi a computer spento. In tal caso occorre valutare, prima di tutto, i tempi operativi in relazione ai dati da ricercare e quindi si sceglie il software più idoneo a disposizione degli operatori (GNU/Linux, Encase, etc. etc):
    - esame mediante avvio del computer a mezzo di sistema operativo GNU/Linux, residente su un floppy disk oppure CD-ROM ed uso della sola memoria RAM come area di lavoro e conseguente verifica del contenuto del disco fisso, con montaggio delle partizioni in sola lettura;
    - esame mediante il programma Encase attraverso una connessione di rete o direttamente utilizzando un dispositivo write protect e conseguente utilizzo della funzione anteprima "preview" per verificare il contenuto del disco fisso.
- Anche nel caso dell'analisi di sistemi "live" cioè accesi, il problema fondamentale è l'eventuale mancanza di strumenti adeguati. In special modo sono necessarie apparecchiature per:
    - la masterizzazione dei dati utili alle indagini, reperiti mediante l'ispezione sul posto;
    - l'acquisizione diretta sul posto dei dischi rigidi contenenti elementi utili.

  Quando si interviene su dei sistemi live o accesi la procedura si complica, in quanto l'intervento deve garantire l'inalterabilità delle condizioni in cui si trova il sistema oggetto di indagine. In questi casi, è indispensabile utilizzare degli strumenti software previamente costruiti o validamente reperiti.

Non poche difficoltà si possono incontrare negli interventi presso le strutture pubbliche e private, il cui sistema informatico è costituito da apparecchiature complesse, spesso dotate di sistema operativo proprietario. L'organizzazione dei dati in tal caso è ordinariamente gestita da programmi non commerciali e progettati per funzionare solo su apposite piattaforme tecnologiche. Tali macchine, di norma, lavorano a ciclo continuo, per cui risulta improponibile procedere ad un eventuale spegnimento, che procurerebbe danni grandemente ulteriori, rispetto all'interesse perseguito. In detta situazione, l'unico modo per estrapolare i dati necessari per le indagini, è quello di servirsi dell'ausilio sia materiale sia tecnico degli amministratori del sistema, all'uopo nominati ausiliari di Polizia Giudiziaria, in base all'ex art. 348 c.p.p. comma 4, che risultano spesso gli unici in grado di gestire il complesso sistema informatico.

A seguito di interventi in occasione di rapine e truffe, per l'acquisizione delle immagini e dei filmati registrati dalle telecamere dei sistemi di sicurezza, notevoli difficoltà hanno riguardato la presenza di sistemi hardware e software di tipo proprietario, talché le immagini ed i filmati non sono facilmente acquisibili, anche perché ordinariamente i relativi sistemi non sono predisposti per il riversamento dei dati su supporti esterni. Le soluzioni adottate, per ridurre i tempi di utilizzo dei detti dati, possono essere le seguenti: in alcuni casi gli operatori di polizia possono effettuare una connessione di rete tra computer portatile e la macchina che gestisce il sistema di sicurezza, acquisendo l'intera registrazione; in altri casi la società, che gestisce l'impianto di sicurezza, può fornire il software idoneo a connettersi con il server dove sono contenute le registrazioni; in altri casi è invece possibile eseguire e acquisire la copia del disco contenuto nel server.

2.6. OPEN VS CLOSED SOURCE

L'eterna "lotta" tra il software aperto e il software proprietario, non poteva non intaccare il settore della digital forensic. In quest ambito, infatti, gli strumenti software utilizzati per l'analisi dovrebbero essere o licenziati (che corrisponde anche ad una "garanzia di funzionamento") o , se sono distribuiti gratuitamente, non essere provento di cracking/pirateria perché oltre ad essere illecito l'utilizzo, non possono garantire che il cracking non comporti modifiche alle informazioni o dei malfunzionamenti al sistema [Car03], [EHP06].
Tra le motivazioni che possono indurre a scegliere l'open source piuttosto che il closed source troviamo le seguenti:

- Trasparenza: gli strumenti sono conosciuti, documentabili e verificabili anche dalla controparte.
- Disponibilità: non occorre acquistare software specifici (e costosi) per svolgere o controllare un'attività.
- Varietà: esistono soluzioni e supporto per una miriade di situazioni, anche improbabili (ad esempio per i file system).
- Adattabilità: i sorgenti sono modificabili per ogni esigenza specifica.
- Flessibilità: il paradigma Unix secondo il quale "tutto è visto come un file" permette di gestire uniformemente anche situazioni nuove.
- Modalità "read-only": linux è per sua natura poco invasivo e ha comunque supporto nativo per la modalità di sola lettura.
- Aderenza agli standard: spesso i software commerciali usano implementazioni arbitrarie e formati chiusi.

Tuttavia, la netta divisione tra i due filoni è riassunta nei due punti seguenti.

- **Open Source** I software open source offrono ampio riconoscimento del file system, ma non offrono tools integrati in un'unica interfaccia grafica, compatibilità degli applicativi sviluppati per differenti sistemi operativi, compilazione reportistica. E' possibile analizzare i processi logici a cui sono sottoposti i dati.
- **Closed Source** I software closed source offrono interfaccia user friendly, tools integrati (editor esadecimale, player, password cracker, hashing, log attività, ecc...), compilazione reportistica, ma non dispongono di larga compatibilità verso i file system non nativi. Non consentono l'analisi della logica di funzionamento e la verifica dei processi a cui i dati sono sottoposti.

Il motivo per il quale in questo campo, si approccia una tecnologia Open Source è che sicuramente si hanno ben chiare in mente le operazioni che dovremo compiere; siamo in grado di effettuare in buona percentuale un'attività forense e nel caso in cui qualcosa non dovesse andare per il verso giusto, sappiamo dove mettere le mani senza andare a confutare tutti quei principi sui quali si basa questa attività. Analizzando il tipo di strumenti messi a disposizione dall'informatica contemporanea, conoscendo l'evoluzione avuta negl'ultimi anni dall'Informatica Forense, vorrei dire che quasi tutti gli strumenti (software ed hardware) utilizzabili oggi sono di derivazione Open Source. Le licenze sotto le quali vengono rilasciati alcuni software, infatti, danno la possibilità di utilizzare il loro codice sorgente a patto che, se migliorato, se ne rilasci una copia dei miglioramenti aderendo alla licenza originale; ma chi impedisce il programmatore di turno di "studiare" il codice di questo genere di software, coglierne idee e spunti elaborativi e quindi confezionare

prodotti Closed Source? Con questo non si asserisce che gli "inventori" esistono solo nel mondo delle licenze in filosofia Open.
Fin'ora abbiamo analizzato le motivazioni che ci possono spingere a scegliere un prodotto realizzato e rilasciato secondo una delle tante licenze, che popolano il mondo dell'Open Source, dobbiamo però anche sottolineare come nel mondo del commerciale vi siano molte più possibilità di trovare la soluzione al nostro problema, soluzioni che possiamo definire dirette o indirette. Le soluzioni dirette sono tutte quelle soluzioni a piccoli problemi hardware, software, di applicazione etc. etc. che un buon centro assistenza permette di risolvere senza grosse difficoltà o che nella peggiore delle ipotesi fornisce l'alternativa alla metodologia seguita; alcuni centri assistenza si avvalgono infatti di esperti non solo in quel campo di nostro interesse, questo mette a disposizione del cliente un team che difficilmente si potrebbe permettere. Le soluzioni indirette, invece, sono l'insieme dei meccanismi che legano il software Closed Source di turno alle certificazioni ed alle garanzie importanti in quel settore; grazie ad una certificazione rilasciata dalla software-house ove si esplicita che il proprio prodotto esegue le operazioni secondo le normative vigenti oppure ancora, che il loro software ha superato tutti i test relativi al perfetto funzionamento, che il loro software è stato acquistato ed utilizzato da figure importanti nel campo delle applicazioni e si fornisce in questo modo all'utilizzatore il passaggio segreto verso la tranquillità. Chiunque infatti se interrogato sulla validità delle operazioni compiute risponderebbe non con spiegazioni ma con certificazioni.
In effetti quello che ci viene offerto dall'Open Source e quello che ci viene offerto dal Closed Source sono entrambi necessari al buon compimento dell'attività di Digital Forensic. Resta comunque il fatto che qualsiasi sia lo strumento utilizzato, il giusto collante (che rende unico questo genere di attività) è la professionalità di chi lo utilizza. Una giusta conoscenza di tecniche, tecnologie, metodologie ed un aggiornamento continuo permettono la realizzazione di un'attività di

analisi raramente minata da errori. Diventa necessaria un'attività di formazione, dove soggetti esperti nel settore, mettono a disposizione il loro know-how per meglio delineare il profilo professionale dell'esperto di settore.
Unire le due filosofie (Open Source e Closed Source) non vuol dire tradire qualcuno, bensì aumentare la propria capacità risolutiva (perché fondamentalmente qualsiasi processo informatico è composto dalla risoluzione di microproblemi) diminuendo le energie impiegate.

2.6.1. Alcuni strumenti per l'attività di Digital Forensic

Il software che ad oggi è quello più utilizzato per l'analisi delle tracce informatiche è EnCase, destinato all'uso professionale ed investigativo da numerose agenzie e forze dell'ordine in tutto il mondo e considerato in linea con gli standard internazionali, infatti EnCase® Forensics è il tool più utilizzato nelle procedure di investigazione informatica da parte di organizzazioni governative e forze dell'ordine a livello mondiale. Tra le sue caratteristiche principali troviamo una evoluzione del supporto per l'analisi di e-mail, nei formati PST, DBX, AOL , MBOX e web-mail (Yahoo, Hotmail e Netscape), la possibilità di navigazione delle pagine HTML presenti nella cache ed accesso dettagliato ai log di navigazione, con un supporto migliorato per i browser che stanno rapidamente crescendo di popolarità, come Mozilla Firefox, Opera e Apple Safari, l'aggiunta del tool "Linen" (Linux for EnCase), per acquisizione e ricerca in ambiente Linux e un motore di acquisizione potenziato nel caso particolare di drive con settori danneggiati
Ma le critiche più frequenti mosse ad EnCase riguardano la scelta della Guidance Software di non rendere visibile il codice sorgente del programma. Infatti al fine di garantire la completa trasparenza,

indipendenza e verificabilità delle tecnologie delle operazione di rilevazione delle prove sarebbe opportuno utilizzare un software con codice open-source. Altre critiche mosse nei riguardi di questo software derivano dalle seguenti considerazioni:

- Il numero di file system supportati è ancora limitato; EnCase supporta i file system più comuni trascurandone molti altri, come ad esempio: reiser, ext3, jfs, ufs, hfs, hfs+, veritas.
- La varietà di formati dei file di evidence riconosciuti da EnCase è piuttosto limitata, esistono altri tool decisamente più potenti che riescono ad ovviare a questo problema.
- In aggiunta alla firma digitale, al fine di migliorare l'autenticità delle prove fornite attraverso l'utilizzo del software, si è molto discusso sulla necessità di utilizzare un ulteriore strumento di validazione, il time-stamping.
- Il costo del software è abbastanza eccessivo. In alternativa ad EnCase esistono software meno "famosi" capaci di supportare la maggior parte delle operazioni di computer forensic, ad un prezzo decisamente più competitivo.

Iritaly (Incident Response Italy): nasce nel 2003 [Fra07], presso il Polo Didattico e di Ricerche di Crema il progetto IRItaly, sviluppato sotto la direzione del Prof. Dario Forte. La versione base, destinata all'acquisizione delle immagini dei sistemi da analizzare, dispone di tutti gli strumenti, diventati ormai standard in questi tipi di distrubuzioni, si va quindi da ddflcd, una versione migliorata del classico comando dd, alla sua GUI (interfaccia grafica) denominata AIR (nello screenshot). IRItaly Livecd versione base può vantare la presenza tra i propri tool anche del recentissimo Aimage per l'acquisizione di immagini forensi secondo il nuovo standard Advanced Forensic Format. E' inoltre disponibile il tool TcpDum per l'acquisizione del traffico di rete.

F.I.R.E (Forensic and Incident Response Environment)
Progetto nato nel 2002 è giunto attualmente alla versione 0.3.5. A detta di molti utenti la distribuzione non si distingue per usabilità, sebbene sia stata ricercata una buona compatibilità garantendo, oltre alla modalità grafica gestita da FluxBox, anche la possibilità di operare via shell con comodi menù. F.I.R.E. Dispone di GUI per Windows e di binari statici per Windows, Linux e solaris. I tools accessibili attraverso il menù grafico coprono la virus e rootkit detection, acquisizione e analisi di network e media. Sicuramente di una distribuzione leggera ed essenziale.

Helix vede la luce nel febbraio 2003 [Efe05] in seno alla Efense Inc., azienda impegnata nell'informatica forense e nel primo intervento a seguito di incidenti informatici.
La distribuzione basata su Knoppix, attualmente alla versione 1.7 07032006, si distingue per un desktop, basato sul window manager Xfce, assai curato. Tutti i tools sono implementati nel ricco menù, dove l'utente ha solo l'imbarazzo della scelta. Se tale ricchezza di software ne fanno da una parte quasi una distribuzione live per l'utente normale, dall'altro la rendono piuttosto pesante, andando ad incidere pesantemente sulle risorse di RAM e CPU delle macchine ospiti. Inoltre la compatibilità con periferiche audio e video non è assoluta e anche l'installazione su hard disk non è priva di rischi. E' al momento l'unica distribuzione ad implementare i programmi Writer, Calc e Impress della suite OpenOffice 2 consentendo l'immediata visione dei più comuni files realizzati con Microsoft Office. Si differenzia inoltre da altre versioni per l'assenza di strumenti per la cattura del traffico di rete e l'auditing delle vulnerabilità. Il Bootable Cd contiene una GUI per l'ambiente Windows, i binari statici per Linux e Solaris e una copiosa documentazione.

PHLAK (Professional Hacker's Linuk Assault Kit) e' l'unica distribuzione in esame ad essere basata su Morphix, distribuzione Linux estremamente modulare. L'ambiente desktop è anche in questo caso il leggero Xfce, o in alternativa FluxBox. La distribuzione riconosce con facilità anche le schede audio e video di portatili datati, garantendo una buona compatibilità, è inoltre possibile installarla con facilità sull'hard disk, riconoscendo sistemi operativi già installati, senza alcun problema al boot. Phlak dispone di tools per la computer e la network forensic, che sono però in minima parte avviabili via menù grafico, avendo gli sviluppatori preferito il lancio per linea di comando.

BackTrack è' la nuova distribuzione sostenuta e sviluppata da Remoteexploit.org, l'unica tra quelle prese in esame basata su Slackware. Nasce dalla fusione di Auditor e Whax, due distribuzioni volte all'IT security. L'ambiente desktop è KDE, dal cui menù si può avviare tutti i numerosi tools. L'ambiente grafico deve essere avviato su richiesta dell'utente, con il comando "startx", dopo la fase di boot. Tuttavia la distribuzione non presenta una perfetta compatibilità con l'hardware disponibile.

Consigliare l'uso di un software Closed Source è cosa abbastanza semplice, per i motivi descritti; consigliarne uno Open Source è una sfida dalla quale dobbiamo imparare tanto, innanzi tutto se siamo in grado di attendere alle aspettative di chi ci chiede di effettuare un'attività di acquisizione o di analisi; inoltre si possono imparare nuove metodologie oppure possiamo scoprire che vi sono mille modi diversi per risolvere i problemi posti.

Capitolo 3

PERCHÉ POLCAT

3.1. PREMESSA

In questo capitolo tratteremo l'analisi del software PolCat che la Polizia Postale di Ancona attualmente utilizza per svolgere le loro attività di indagine.
Il suo nome, PolCat, deriva oltre che dal sostantivo Polizia dal nome del comando Linux Cat. Infatti era questo il comando che inizialmente veniva utilizzato per effettuare la clonazione di un disco. PolCat nasce nel maggio 2002. In realtà si trattava di un precursore dell'attuale applicativo in dotazione e le sue dimensioni erano talmente ristrette da poter essere contenuto in un floppy disk. Ovviamente, come per il software odierno, Polcat offriva soltanto gli strumenti necessari per acquisire i dati (clonare un disco o produrre un file di evidence).
Esso è stato pensato prima di tutto come strumento per reperire dati da dispositivi portatili, onde evitare di smontarli e comprometterne così o il funzionamento o il contenuto.
Negli anni successivi, dato che GNU/Linux supportava un numero maggiore di hardware rispetto a MS-DOS, si è pensato di estendere le capacità di acquisizione dati anche a dispositivi come USB, PCMCIA, dischi SATA, etc. etc.
Inizialmente è nato con interfaccia a linea di comando e questo richiedeva una maggiore conoscenza del sistema da parte degli agenti e per fare in modo che potesse essere facilmente utilizzato da tutti gli addetti del settore, si è pensato di aggiungere un'interfaccia

abbastanza amichevole così da facilitare le normali opearazioni di clonazione o di evidence.

Lo scopo di questo capitolo, quindi, è quello di documentare il livello di conoscenza e le modalità di funzionamento dell'applicativo PolCat attualmente in uso. In particolare verranno riassunte le funzionalità di questo tool (la descrizione dettagliata e completa è riportata nella documentazione prodotta sino ad oggi) per poi passare ad una analisi più approfondita del codice (riportata sempre nel documento allegato) in modo da avere una base di partenza per il processo di reingegnerizzazione del prodotto e giungere alla produzione di un software pubblico e certificato di parleremo nel prossimo capitolo. In questo contesto, per software pubblico si intende un prodotto sviluppato in filosofia open source, questo per ovviare ai tanti problemi che derivano dall'uso di applicativi chiusi (come EnCase) e che abbiamo trattato precedentemente, mentre invece per software certificato si intende un prodotto che, per il suo sviluppo, ha rispettato le linee guida dello standard ISO 27001 di cui parlemo in seguito. Il risultato di queste analisi è stato il frutto di test cosiddetti "monkey proof" (letteralmente "a prova di scimmia") eseguiti utilizzando PolCat su ambienti sia virtuali che reali.

3.2. L'ANALISI DEL PASSATO

PolCat è un'applicazione cosiddetta "live" che poggia cioè su sistemi operativi Linux e che non necessita di alcuna installazione su disco fisso ma viene caricata automaticamente all'avvio del PC (salvo un ordine non corretto dei dispositivi di boot). E' pertanto necessario che la macchina sulla quale operare sia dotata di supporto di lettura ottica a livello hardware e impostare, tra le opzioni disponibili nell'elenco di boot del bios, l'unità di lettura ottica come principale di

modo che possa caricarsi automaticamente all'avvio del sistema. La figura seguente mostra l'avvio dell'applicazione.

Figura 2: scheramta di avvio di PolCat

Questo strumento di attività forense è in grado di effettuare solamente una delle 4 fasi presentate nel primo capitolo: l'acquisizione dei dati. In aggiunta tuttavia sono state inserite alcune funzioni che potrebbero essere comunque utili per la fase di indentificazione e durante tutto il procedimento della catena di custodia dell'attività di digital forensic. Nei prossimi paragrafi, presentiamo un riassunto di quelle che sono le funzionalità dell'applicativo in questione.

3.2.1. Come lavora PolCat

PolCat è in grado di operare in due modalità differenti ma che conducono agli stessi risultati:

- modiltà RESCUE: è la modalità riservata agli utenti esperti dei sistemi operativi Unix Based perché lavora "a riga di comando". In questa modalità tutte le operazioni forensi sono effettuate digitando manualmente i comandi sul prompt;

tralasciamo volutamente questa parte proprio perché richiede specifiche competenze di utilizzo.

- modalità NORMALE, si presenta all'operatore sotto forma di una serie di interfacce grafice in successione, mediante le quali è possibile scegliere quale operazione si vuol eseguire. E' proprio su quest'ultima modalità che sono state svolte tutte le analisi del caso, ed è proprio quest'ultima che andremo a riportare in questa parte del lavoro.

La prima richiesta che l'applicativo fa all'operatore, dopo essere stato avviato, è di impostare la data e l'ora di sistema. Questa operazione si rende necessaria al fine di poter documentare in maniera dettagliata tutte le fasi inerenti l'acquisizione dei dati. La figura che segue mostra l'interfaccia di comunicazione con l'operatore.

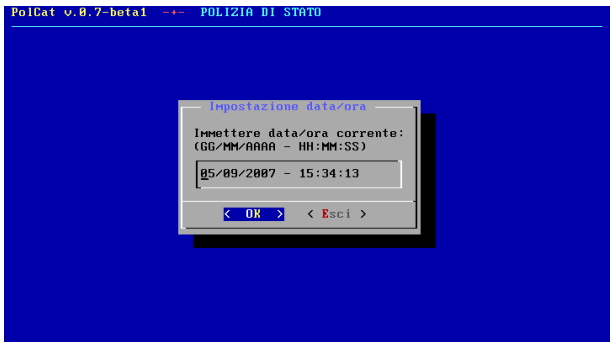

Figura 3: impostazione data e ora

In realtà, data e ora vengono impostate automaticamente con gli stessi valori dell'ora di sistema della macchina su cui si opera. Una volta che l'ora è stata settata, possiamo cominciare ad usare l'applicativo secondo le nostre necessità.

La particolarità di PolCat risiede nell'aver organizzato in maniera gerarchica le sue funzionalità.

Quest'ultime possono essere rappresentate sia per livelli di astrazione (che ha permesso di analizzare le funzioni in base al proprio grado di utilizzo) sia mediante una struttura ad albero (che

permette di esprimere la complessità di una specifica operazione come sequenza delle interazioni da effettuare).
Quelle riportate di seguito (e che sono state rappresentate sotto forma di struttura ad albero) sono tutte le funzioni che l'applicativo mette a disposizione:

- **Menu Opzioni**
  - **Tools**
    - Firmware
    - Visualizza
    - Wiping
      - Floppy
      - Disco
      - Partizione
    - Hashing
      - Floppy
      - Disco
      - Partizione
      - CD-Rom
    - Restore
    - Data e Ora
    - Console
  - **Acquisizione**
    - Dischi
      - Clonazione
      - Evidence
    - Rete
      - Server
      - Client
  - **Uscire**

Di seguito verranno riportate e corredate con alcune immagini tutte le funzioni precedentemente elencate, focalizzando l'attenzione sulle corrette fasi da eseguire e sul corretto funzionamento.
Per quanto concerne l'approccio che abbiamo definito "a livelli", invece, abbiamo potuto identificare i seguenti:

- **1° livello:** è il livello generale e comune per tutte le operazioni. In genere coincide con le funzioni legate alle fasi di avvio dell'applicazione, al settagio dei parametri del tempo, all'uscita dall'applicazione e alla scelta dei menù.
- **2° livello:** è il livello caratterizzato dall'insieme delle funzioni relativo ai menù del primo livello più le funzioni per ritornare al livello precedente. Questo livello è composto dalle seguenti interfacce:
  - Interfaccia Tool: raccoglie tutte le funzioni degli strumenti che PolCat mette a disposizione e che sono:
    - firmware_menu
    - visualizza_menu
    - wiping_menu
    - hashing_menu
    - restore_start
    - tempo
    - shell
  - Interfaccia Acquisizione: raccoglie tutte le funzioni che permettono un'acquisizione discriminata secondo tipologia:
    - Dischi
    - Rete
- **3° livello:** è il livello in cui si trovano le funzioni individuate all'interno di quelle presenti nel livello precedente. Tra queste riportiamo le più importanti e trasversali alla maggiorparte delle funzioni come:

- Interfaccia di selezione dei dispositivi hardware che sono sorgenti di file
- Interfaccia di selezione dei dispositivi di destinazione delle acquisizioni o dei risultati dati dai tool utilizzati
- Interfaccia per l'inserimento delle informazioni relative all'operatore e per l'inserimento di alcune noti utili per il processo di catena di custodia
- Interfaccia per il salvataggio dei report o per la stampa su supporto cartaceo

Di seguito, mostriamo il diagramma delle interfacce grafiche relative ai primi due livelli:

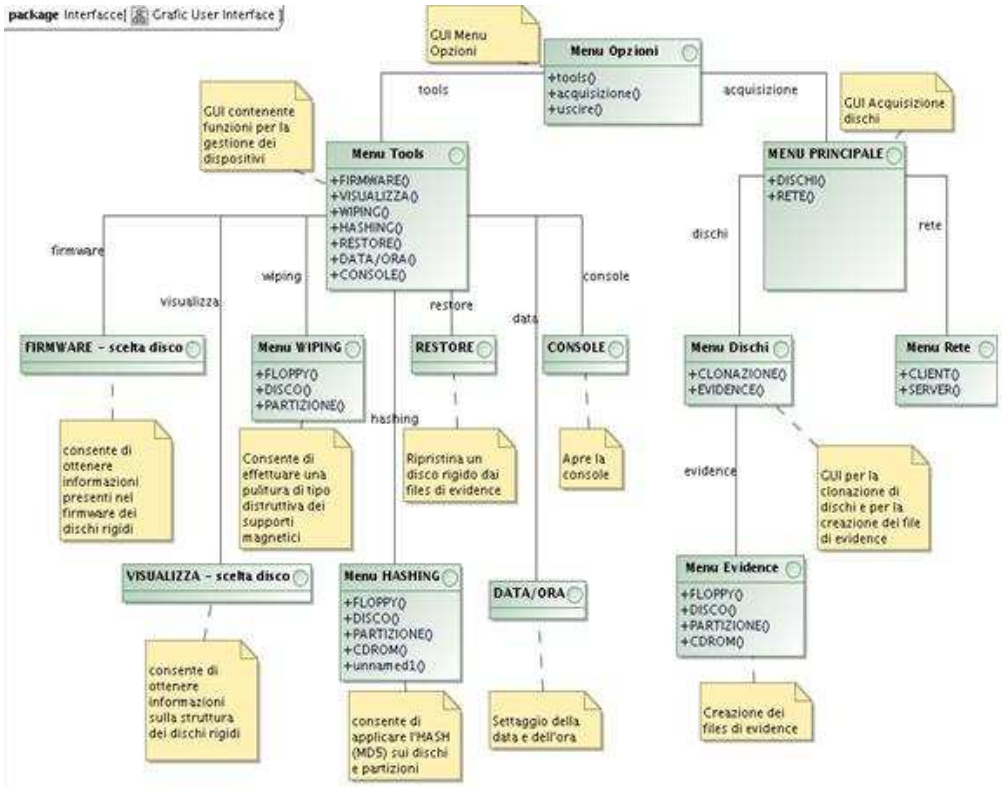

Figura 4: diagramma delle classi delle funzioni

3.2.2. Descrizione delle funzionalità

Come si può vedere dalla figura seguente (rappresentata dal 1° livello di astrazione), i gruppi principali di funzioni sono racchiusi in due macro-gruppi:

- TOOLS: gruppo che contiene tutte le funzioni per la gestione dei dischi;
- ACQUISIZIONE: gruppo che contiene tutte le funzioni per l'acquisizione dei dati dai dischi.

La terza voce presente nel menù è il comando che consente di chiudere l'applicazione e arrestare il sistema.

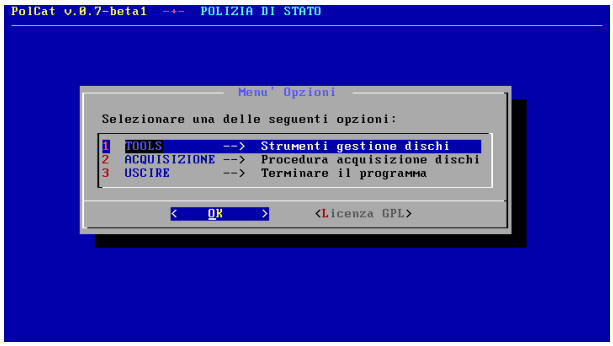

Figura 5: menù principale di PolCat

Tra i tools messi a disposione abbiamo i seguenti (vedi figura sottostante) e il cui significato è riportato nelle pagine seguenti.

Figura 6: menù degli strumenti

3.2.2.1. Firmware

Come si può dedurre sia dal nome, sia dalla breve descrizione che appare evidenziando la scelta, questa opzione restituisce le informazioni relative ai dischi presenti sulla macchina su cui si sta svolgendo l'acquisizione. I dati fanno riferimento al modello del disco, al seriale, alla divisione in settori, etc. etc.

Figura 7: rapporto operazione di firmware

E' possibile recuperare le informazioni del firmware di tutti i dispositivi presenti, o in alternativa, selezionarne solo alcuni. I dati così recuperati possono essere corredati con delle note (che all'occorenza potranno essere lasciate vuote) e sucessivamente andranno a popolare il rapporto del firmware. A questo punto, il rapporto potrà essere stampato o salvato su un supporto di memoria di massa come ad esempio un floppy disk.

3.2.2.2. Visualizza

A differenza del Firmware, questa opzione restituisce maggiori dettagli riguardo un disco selezionato, in particolare il tipo file system presente sul disco (Fat, Fat 32, NTFS, ext3, etc. etc).

Figura 8: informazioni del dispositivo

Non è possibile in questo caso inserire le note ma si può comunque stampare o salvare su floppy disk il report generato.

3.2.2.3. Wiping

Letteralmente significa "pulizia a fondo". E in realtà questa opzione consente di cancellare (definitivamente) i file contenuti su un dispositivo di memoria di massa presente sulla macchina. Dall'analisi svolta infatti si è visto che è possibilie cancellare, a scelta, uno dei seguenti dispositivi: floppy, disco o partizione. Una volta selezionato il supporto da pulire, viene richiesto il numero totale di sovrascritture da eseguire.

Figura 9: numero di sovrascritture

Quando il processo di wiping termina con successo si torna al menù principale dei tools.

3.2.2.4. Hashing

Questa opzione consente di calcolare il message digest (md5) dei dati dei dispositivi presenti sulla macchina. L'MD5 è un algoritmo che prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit (ovvero con lunghezza fissa di 32 valori esadecimali, indipendentemente dalla stringa di input) che può essere usata per calcolare la firma digitale dell'input. La codifica avviene molto velocemente e si presuppone che l'output (noto anche come "MD5 Checksum" o "MD5 Hash") restituito sia univoco (ovvero si ritiene che sia impossibile, o meglio, che sia altamente improbabile ottenere con due diverse stringhe in input una stessa firma digitale in output) e che non ci sia possibilità, se non per tentativi, di risalire alla stringa di input partendo dalla stringa di output (la gamma di possibili valori in output è pari a 1632). PolCat consente di calcolare l'hash di:

- Floppy disk
- Hard disk
- Partizioni
- CD-Rom

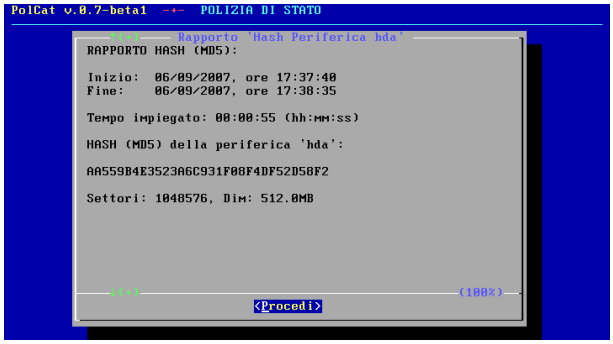

Figura 10: rapporto del calcolo dell'hash

Una volta che l'hash è stato calcolato, può essere stampato oppure salvato su un dispositivo di memoria di massa. E' proprio grazie a questo valore che è possibile stabilire se i dati acquisiti siano stati o meno alterati (in riferimento alla prima acquisizione ovviamente).

3.2.2.5. Restore

L'opzione di restore tenta il ripristino del contenuto di un disco rigido, o di una sua partizione, su un altro dispositivo di memoria di massa. Per poter effettuare il ripristino di un disco o di una partizione occorre avere a disposizione una cartella contenente il file di evidence da ripristinare.

Figura 11: scelta della partizione da ripristinare

Questo file infatti contiene tutti i dati che erano presenti sul disco e che erano stati precedentemente acquisiti.

3.2.2.6. Data/Ora

Questa opzione consente di modificare la data e l'ora impostate all'avvio dell'applicazione.

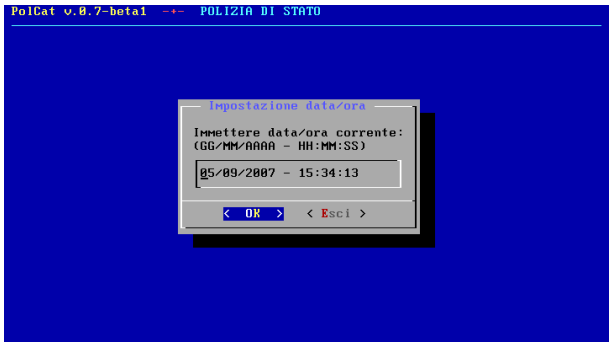

Figura 12: cambio data/ora

3.2.2.7. Console

L'opzione console consente di richiamare la modalità rescue, in modo da poter operare con l'interfaccia a riga di comando. Ricordiamo in questo caso che è richiesta una specifica conoscenza dei comandi e del sistema operativo.

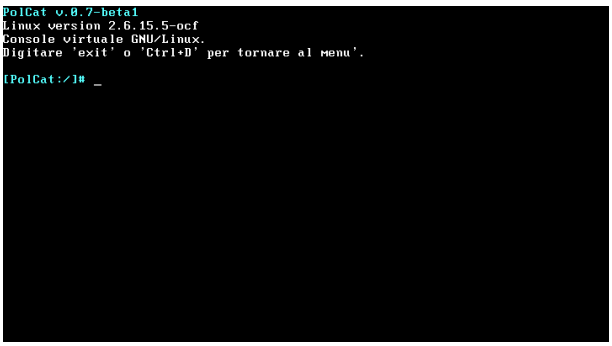

Figura 13: interfaccia a riga di comando

3.2.2.8. Acquisizione Disco

L'acquisizione dei dischi è una delle due voci selezionabili dal gruppo di opzioni presenti nel gruppo Acquisizione. Tale funzionalità fornisce all'utente la possibilità di effettuare una CLONAZIONE diretta dei dischi oppure generare un file di EVIDENCE. Com'è possibile dedurre dal significato dei termini, la clonazione esegue una duplicazione bit a bit di un hard disk mentre l'evidence restituisce l'effettiva prova digitale sulla quale andare ad operare con gli strumenti di analisi. Il motivo per cui PolCat dà la possibilità di clonare un hard dick è da ricercare nelle problematiche legate alla fase di individuazione: se ad esempio non è possibile lavorare direttamente su un disco, è preferibile prima clonarlo, inserire la procedura agli atti (nel rispetto della catena di custodia) e lavorare successivamente sul file di evidence.

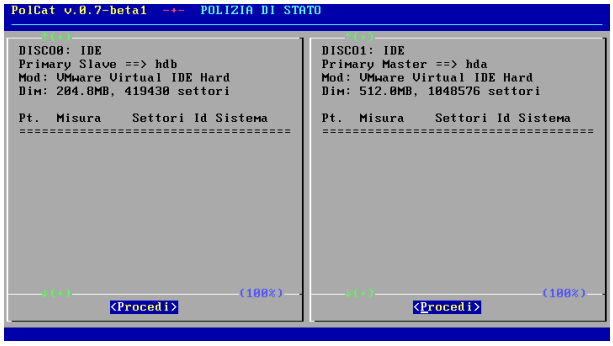

Figura 14: clonazione - informazioni sui dischi

La garanzia di una corretta clonazione è data dalla corrispondenza del calcolo dell'hash prima e dopo la clonazione (funzionalità prevista nell'iter operativo)

Figura 15: rapporto della clonazione

L'unico vincolo richiesto dalla clonazione è che il disco di destinazione sia più grande del disco sorgente.
Per quello che riguarda l'opzione di evidence invece, si ha la possibilità di acquisire i dati tra i seguenti dispositivi di memoria di massa:

- Floppy disk
- Hard disk
- Partizioni
- CD-Rom

Una volta selezionata la sorgente, occorre specificare il disco di destinazione del file di evidence (da riutilizzare in seguito per l'analisi dei dati). Anche in questo caso, per una corretta gestione di tutto il processo e della catena di custodia, si chiederà di nominare il file e inserire tutti i dati relativi a questa operazione (opratore, note e ufficio).

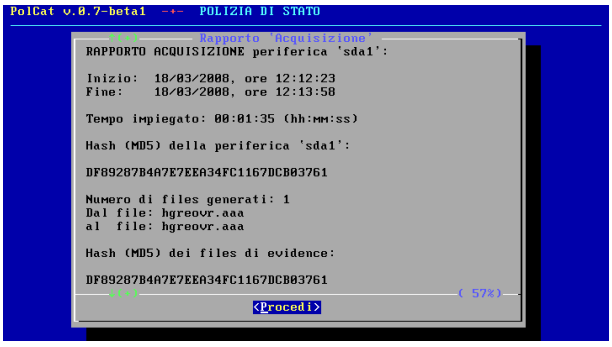

Figura 16: rapporto dell'acquisizione - hash

Figura 17: rapporto finale dell'acquisizione

Una corretta acquisizione è garantira dalla possibilità di clalcolare Hash di origine e Hash di destinazione, così come mostra il report generato dal compitento dell'operazione.

3.2.2.9. Acquisizione Rete

Questa opzione non è da confondere con il settore della Network Forensic. Ricordiamo che quest'ultima lavora solamente sul traffico di rete alla ricerca di possibili tracce che possano identificare coloro che commettono i reati di cui abbiamo parlato nella relativa sezione.
In PolCat invece l'acquisizione di rete è una funzionalià che è stata inserita sempre per ovviare alle problematiche che si possono verificare in fase identificazione degli elementi probatori.
Con l'acquisizione di rete è sufficiente per tanto impostre il computer sorgente come server, e il computer destinatario come client e i dati fluiranno attraverso il collegamento stabilito.

Figura 18: acquisizione da rete - client

Tramite rete è possibile fare la clonazione di un disco o generare un file di evidence, così come abbiamo visto per l'acquisizione dei dischi. Oltretutto, c'è la possibilità di scegliere tra differenti algoritmi di hash, sia lato client che lato server per garantire che le operazioni svolte non abbiano prodotto danni ai dati acquisiti.

3.3. PROBLEMATICHE CONNESSE ALL'ACQUISIZIONE PER LA POLIZIA POSTALE DI ANCONA

Nei paragrafi precedenti abbiamo esposto quelle che sono le difficoltà che si possono incontrare in tutte le fasi dell'attività forense. Ricordiamo che in questa sezione del lavoro stiamo descrivendo le operazioni che PolCat può compiere, ed esse sono solamente operazioni di acquisizione di dati dai supporti magnetici (direttamente da disco o anche da rete in modalità client/server) .
Pertanto, relativamente alle operazioni di acquisizione, la Polizia Postale di Ancona pone la risoluzione delle seguenti questioni [PGDC07]:

- Diminuire la lunghezza delle operazioni per il calcolo del checksum o dell' hash (MD5 o SHA1) del supporto originale e

della sua eventuale copia tramite la riscrittura di algoritmi più efficaci.

- Problemi di non poco conto si possono avere durante l'acquisizione di un disco rigido sequestrato effettuata con il programma ENCASE, poiché si possono verificare una lunga e vasta serie di errori, dovuti spesso allo stato deprecabile del supporto in osservazione.
- Necessità di visualizzare e acquisire file nei più diversi formati soprattuto i file di evidence generati dal programma EnCase. In alcuni casi, i file (proprietari) sono leggibili solo a mezzo dei programmi attraverso i quali sono stati creati. In tal caso, quando non è possibile disporre del programma originale, è opportuno uscire dal programma di analisi ed utilizzare una copia del disco in esame, per poter riavviare il sistema originale, di modo che il file sarà visualizzato e può essere utilizzato per le normali operazioni.
- Possibilità di aprire il file non intelligibile con un editor esadecimale (es. hexedit) che può mostrare bit per bit il contenuto del file.
- Difficoltà di rilevare file e file-system crittografati e/o steganografati. Fermo restando il problema di visualizzare i detti file, senza possedere la chiave di decodifica, è opportuno perlomeno dare atto della loro presenza, utilizzando idonei programmi (es. stegdetect) atti a rilevare quelli steganografati. Per i file crittografati vi è unicamente la possibilità di operare per esclusione. Al fine di accedere al contenuto di files protetti da password è possibile utilizzare appositi programmi di vario genere.
- Difficoltà di procedere all'esame di nuovi supporti informatici, come le console di videogiochi (es. Xbox della Microsoft, dotata di disco rigido), penne USB, lettori ibridi musicali e di dati, telefoni cellulari di nuova generazione, fotocamere digitali, "memory card" (schede di memoria), etc. etc. che

possono essere utilizzati per immagazzinare informazioni digitali.

- Non poche difficoltà si possono incontrare negli interventi presso le strutture pubbliche e private, il cui sistema informatico è costituito da apparecchiature complesse, spesso dotate di sistema operativo proprietario. L'organizzazione dei dati in tal caso è ordinariamente gestita da programmi non commerciali e progettati per funzionare solo su apposite piattaforme tecnologiche. Tali macchine, di norma, lavorano a ciclo continuo, per cui risulta improponibile procedere ad un eventuale spegnimento, che procurerebbe danni grandemente ulteriori, rispetto all'interesse perseguito.

Le soluzioni a tali problematiche possono essere fornite da una nuova riscrittura del codice di PolCat laddove, a seguito di un'attenta fase di reverse engineering delle funzioni dell'applicativo, si renda necessario oppure ampliare le funzionalità già presenti con moduli particolari per specifiche operazioni.

Capitolo 4

DISPOSIZIONI PER IL NUOVO FRAMEWORK

4.1. L'ESIGENZA DI UN FRAMEWORK

Nell'ambito generale della produzione del software, un framework è una struttura di supporto su cui un software può essere organizzato e progettato [DFRW01].

Alla base di un framework c'è sempre una serie di librerie di codice utilizzabili con uno o più linguaggi di programmazione e spesso corredate da una serie di strumenti di supporto allo sviluppo del software, come ad esempio un IDE (ambiente di programmazione integrato in un'applicazione), un debugger (strumento per la localizzazione e rimozione di eventuali errori), o altri strumenti ideati per aumentare la velocità di sviluppo del prodotto finito.

Lo scopo di un framework, pertanto, è quello di far risparmiare allo sviluppatore la riscrittura di codice già steso in precedenza per compiti simili o specifici, circostanza che si presenta sempre più spesso man mano che le interfacce utente sono diventate sempre più complesse, o più in generale man mano che è aumentata la quantità di software con funzionalità secondarie simili.

Un esempio a riguardo potrebbe essere il tipo di interazione con l'utente offerta da un menu a tendina; quest'ultima sarà sempre la stessa indipendentemente dall'applicazione cui il menu appartiene (o almeno questo è ciò che l'utente si aspetta).

In casi come questo un framework che permetta di aggiungere la funzionalità di una finestra con un menu a tendina soltanto con poche righe di codice sorgente a carico del programmatore, o magari permettendogli di disegnare comodamente il tutto in un ambiente di sviluppo, permetterà al programmatore di concentrarsi sulle vere funzionalità dell'applicazione, senza doversi fare carico di scrivere codice "di contorno".

Il termine inglese framework quindi può essere tradotto come "intelaiatura" o "struttura", ed è appunto la sua funzione (come a sottolineare che al programmatore rimane solo da creare il contenuto vero e proprio dell'applicazione.

Un framework solitamente è definito da un insieme di librerie o di classi (secondo che si faccia riferimento alla programmazione degli anni 80 o al nuovo paradigma di programmazione ad oggetti) e dalle relazioni tra esse, mentre una libreria software è un insieme di funzioni di uso comune, predisposte per essere collegate ad un programma applicativo. Il collegamento può essere statico o dinamico, nel qual caso si parla di Dynamic-link library.

Lo scopo delle librerie software è quello di fornire una vasta collezione di funzioni di base pronte per l'uso, evitando al programmatore di dover scrivere ogni volta le stesse funzioni di uso generale. Ad esempio molti linguaggi di programmazione hanno una libreria di funzioni matematiche, che offrono numerose funzioni come l'elevamento a potenza, il calcolo dei logaritmi e così via.

Ogni linguaggio di programmazione possiede la sua collezione di librerie, le quali vengono distinte in librerie standardizzate e librerie non standardizzate. La differenza tra librerie standard e non standard influisce in maniera determinante sulla portabilità di un programma software fra sistemi operativi diversi e piattaforme hardware diverse. I programmi che fanno uso solo di funzioni di librerie standard hanno generalmente un grado di portabilità maggiore. Il termine italiano viene da un'errata traduzione dell'inglese library, che vuol dire biblioteca, ma oramai libreria è

entrata a tal punto nel vocabolario dei professionisti del settore che sarebbe troppo difficile e lungo far accettare il termine corretto.
Scrivere un framework perciò significa fornire un'implementazione di librerie o di classi astratte in modo da avere un punto di partenza altamente indipendete da ciò che effettivamente il programmatore andrà a svilupparci sopra. L'insieme delle funzioni o delle classi concrete, definite ereditando il framework, eredita le relazioni già esistente tra le stesse; ottenendo in questo modo un insieme di funzioni e/o classi concrete con un insieme di relazioni tra classi.
Lo scopo di questa tesi perciò è quello di fornire gli strumenti necessari per la scrittura di un framework che sia:

- **di supporto alle attività di digital forensic**: cioè che metta a disposizione degli sviluppatori un insieme di librerie di base che eseguano quelle che sono le operazioni viste in precedenza;
- **pubblico**: cioè le librerie sono scritte nel rispetto della filosofia Open Source la quale ha come obiettivo quello di diffondere il codice sorgente al fine di apportare ulteriori aggiornamenti e miglioramenti oltre al vantaggio legato all’assenza di costi di acquisto;
- **certificato**: cioè un prodotto di qualità che, per il suo sviluppo, abbia rispettato e seguito le linee guida degli standard riguardanti il Sistema di Gestione della Sicurezza delle Informazioni (di cui parleremo in questo capitolo) riportate nelle normative BS7799 e ISO27001 e le linee guida riportata dal progetto OWASP (Open Web Application Security Project) con la metodoligia CLASP (Comprehensive, Lightweight Application Security Process).

4.2. GLI STANDARD QUALITATIVI NELLA COMPUTER FORENSIC

In quest'ultima parte del lavoro ci occuperemo di descrivere quali sono queste linee guida degli standard di modo che possano essere seguite ed applicate alle fasi di riscrittura del framework in oggetto. Occorre tuttavia precisare che esistono già diverse associazioni che si occupano di standardizzare quelle che sono le usuali operazioni di digital forensic. Tra queste segnaliamo:

- La ACPO (Association of Chief Police Officer) della National High Tech Crime Unit, la quale ha sviluppato la "ACPO guide" [ACPO02], il cui scopo è quello di fornire regole per l'acquisizione, l'analisi e la presentazione delle prove digitali in dibattimento. Tale documentazione non vuole presentarsi come lo standard su cui basare ogni rilevazione, in quanto la non conformità a questa guida non deve essere considerata come fonte di rigetto nella prova, ma vuole essere solamente una sorta di vademecum utile per una corretta procedura di un'indagine forense.
- L'IOCE (Internazional Organization of Computer Evidence) viene fondata nel 1995 per offrire un forum di discussione dove scambiare proprie opinioni ed esperienze sul crimine informatico e informatica forense, ed ha revisionato la guida ACPO durante la conferenza IHCFC nel 1999.
- Lo IACIS (International Association of Computer Investigative Specialist) è un'organizzazione di volontari no-profit composta da professionisti delle forze di polizia dedicati all'istruzione nel campo dell'informatica forense.

I principi e le considerazioni che sono stati evidenziati da queste associazioni possono essere sintetizzati nelle quattro regole fondamentali per l'ammissibilità di una prova in sede dibattimentale e sono anche fonte di raccolta dei requisiti essenziali per lo sviluppo del framework.
I principi sono i seguenti:

- minima manipolazione dell'originale e, quando possibile, conservazione della prova in luogo sicuro e protetto;
- documentare scrupolosamente ogni minimo cambiamento della prova durante l'esame;
- conformità alle regole della prova, assicurare che il procedimento sia conforme ad uno standard;
- non manipolare la prova oltre i limiti delle proprie capacità tecniche e professionali.

4.3. GLI STANDARD QUALITATIVI NELLA PRODUZIONE DEL SOFTWARE

Per qualità del software si intende la misura in cui un prodotto software soddisfa un certo numero di aspettative rispetto sia al suo funzionamento sia alla sua struttura interna. Gran parte della ricerca nel campo dell'ingegneria del software è dedicata, direttamente o indirettamente, al tema della qualità. In particolare, si è cercato di stabilire chiaramente cosa si intenda per qualità del software, definendo un insieme di parametri di significativi, realizzando tecniche per misurare tali parametri rispetto a un dato sistema software e sviluppando tecnologie (per esempio linguaggi di programmazione) e metodologie (per esempio di analisi e di progettazione) che facilitino la realizzazione di software di qualità.

Tradizionalmente, i parametri (o i fattori) rispetto a cui si può misurare o definire la qualità del software vengono classificati in due famiglie:

- **parametri esterni**: si riferiscono alla qualità del software così come è percepita dai suoi utenti, e includono correttezza, affidabilità, robustezza, efficienza, usabilità.
- **parametri interni**: si riferiscono alla qualità del software così come è percepita dagli sviluppatori, e includono verificabilità, manutenibilità, riparabilità, evolvibilità, riusabilità, portabilità, leggibilità, modularità.

Non raramente esiste una correlazione fra questi due aspetti, come a dire che "il software scritto male tende anche a funzionare male".
Per questo motivo, quando si cerca di realizzare un prodotto o un sistema software è importante svolgere una serie di passi e seguire una sorta di percorso che aiuti ad ottenere risultati di alta qualità e anche nei tempi prefissati.

4.3.1. La metodologia CLASP del progetto OWASP

Il progetto OWASP (Open Web Application Security Project) [OWA07], [OWA08a] nasce dalla volontà di un gruppo di volontari che produce tools, standard e documentazione open-source di qualità professionale, libera da license e orientata alla sicurezza delle applicazioni web. Gli obiettivi di OWASP sono quelli di:

- diffondere la cultura dello sviluppo di applicativi web "sicuri",
- contribuire alla sensibilizzazione sia dei professionisti che delle aziende verso le problematiche di Web Security, attraverso la circolazione di idee, articoli, best-practice e tool,

- promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza di qualsiasi realtà (anche italiana).

Tra le molteplici aree tematiche e i progetti di cui occupa questa organizzazione no-profit (OWASP Guide, OWASP PenTest Checklist, Top Ten Web Application Vulnerability, .NET project, Live CD project) vi è il CLASP Project (ISO 17799 & Web Security nella versione italiana del progetto), un programma che si prefigge di diffondere le linee guida da adottare in tutte le fasi del ciclo di vita del software.
CLASP (Comprehensive Lightweight Application Security Process) [OWA08b]fornisce un approcchio strutturato e ben organizzato su come come muoversi in sicurezza riguardo le fasi iniziali del ciclo di vita dello sviluppo di software, quando possibile.
CLASP in realtà è un insieme di elementi di processi che possono essere integrati in qualsiasi processo di sviluppo software ed è stato sviluppato per essere efficace e facile da utilizzare.
Necessita di un approccio prescrittivo come input, con l'obiettivo di documentare quelle che sono le attività si dovrebbero portare a compimento, e restituisce una vasta serie di risposte che rendono di ragionevole attuazione tali attività.

4.3.2. Lo standard ISO 17799 e la certificazione ISO 27001

Le informazioni sono patrimonio vitale per la vita di ogni organizzazione. Proteggerle e assicurarne la continua implementazione significa disporre di una fonte di conoscenza che è anche vantaggio competitivo e servizio di utilità inestimabile.
Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) gestito secondo la norma BS7779 [Asn03], [TWT05] del 1995 e le

linee guida ISO 17799 del 2000 permette di introdurre e mantenere nel tempo in modo sistematico i processi che determinano e definiscono ruoli, responsabilità e procedure per raggiungere gli obiettivi del SGSI [DiP06], [DNV08].

Gli standard di sicurezza informatica sono dunque metodologie che permettono alle organizzazioni di attuare tecniche di sicurezza finalizzate a minimizzare la quantità e la pericolosità delle minacce alla sicurezza informatica. Le guide contenute nei documenti che descrivono questi standard offrono indicazioni generali e misure tecniche di dettaglio, che, se bene applicate, possono contribuire a mettere in opera un sistema di sicurezza informatica efficace [SIN05].

Uno degli standard di sicurezza più ampiamente usati oggi è l'ISO 17799 del 1995. Questo standard deriva dallo standard BS 7799:1 pubblicato dal BSI (British Standards Institute) a cui fa seguito il BS 7799:2 che recentemente è stato pubblicato come ISO 27001 ed è certificabile, mentre l'ISO 17799 viene definito come manuale pratico (Security Code of Practice) privo di valore normativo, vale a dire una delle tante metodologie adottabili per soddisfare i requisiti della norma ISO 27001. La certificazione ISO/IEC 27001 serve a dimostrare che il Sistema di Gestione della Sicurezza delle Informazioni rispetta i requisiti espressi dallo standard, testimoniando che sono state adottate le necessarie precauzioni per proteggere i dati sensibili da accessi e modifiche non autorizzati.

Lo standard utilizza un approccio basato su processi per definire, implementare, operare, monitorare, revisionare, mantenere e migliorare il Sistema di Gestione della Sicurezza delle Informazioni di una organizzazione (SGSI).

4.3.3. I principi di base

Dall'analisi condotta sulla norma ISO 17799 e sulla metodologia CLASP si può asserire che la sicurezza dell'informazione è caratterizzata da 3 elementi chiave: integrità, riservatezza e disponibilità.
Al fine di procedere ad un corretto sviluppo di un software, ed in particolare del framework PolCat, possiamo basarci sui seguenti principi base:

- politiche di sicurezza (Security Policy): forniscono le direttive di gestione ed il supporto per le informazioni di sicurezza.
- sicurezza organizzativa (Security Organization): controllo della sicurezza delle informazioni in seno all'azienda; mantenere la sicurezza e la facilità dei processi organizzativi delle informazioni anche quando accedono le terze parti; monitorare la sicurezza delle informazioni quando la responsabilità dell'elaborazione dell'informazione è stata conferita in outsource.
- controllo e classificazione dei beni (Asset Classification and Control): mantenere la protezione dell'assetto organizzativo e garantire che l'assetto delle informazioni riceva un appropriato livello di protezione.
- sicurezza del personale (Personnel Security): ridurre i rischi di errore, di furto, di frode o di abuso da parte degli operatori; accertarsi che gli utenti siano informati delle possibili minacce e preoccupazioni sulla sicurezza delle informazioni e siano dotati a sostenere la politica della società sulla sicurezza nel corso del loro lavoro normale; minimizzare i danni dagli avvenimenti e dalle disfunzioni di sicurezza ed imparare da tali avvenimenti.

- sicurezza fisica e ambientale (Physical and Environmental Security): impedire l'accesso, il danneggiamento e l'interferenza dei non autorizzati all'interno del flusso delle informazioni del business; impedire perdita, danni o l'assetto del sistema e l'interruzione delle attività economiche; impedire la manomissione o il furto delle informazioni.
- gestione di comunicazioni e operazioni (Communications and Operations Management): accertarsi del corretto funzionamento e facilità di elaborazione dell'informazione; minimizzare il rischio di guasti dei sistemi; proteggere l'integrità dei software e delle informazioni; mantenere l'integrità e la validità dei processi di elaborazione dell'informazione e della comunicazione; garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture a supporto; prevenire danni ai beni e le interruzioni alle attività economiche; impedire perdita, modifica o abuso delle informazioni scambiate fra le organizzazioni.
- controllo di accesso (Access Control): per controllare l'accesso alle informazioni; per impedire l'accesso non autorizzato ai sistemi d'informazione; per accertare la protezione dei servizi in rete; per impedire l'accesso non autorizzato nel calcolatore; per rilevare le attività non autorizzate; per accertarsi sulla sicurezza delle informazioni quando sono utilizzate le postazioni mobili rete e tele rete.
- sviluppo e manutenzione di sistemi (System Development and Maintenance): accertare che la sicurezza sia stata costruita all'interno delle operazioni di sistema; per impedire la perdita, la modifica o il cattivo utilizzo dei dati dell'utente all'interno dei sistemi di applicazione; per proteggere riservatezza, autenticità e l'integrità delle informazioni; per accertarsi che le attività di progetto e supporto alle attività siano condotte in

modo sicuro e per mantenere la sicurezza del software e dei dati di sistema.

- gestione continuità operativa (Business Continuity Management): neutralizzare le interruzioni alle attività economiche ed ai processi critici degli affari, dagli effetti dei guasti.
- adeguatezza (Compliance): evitare di non rispettare le leggi civili, penali e qualsiasi altro requisito di sicurezza; per elevare l'efficacia e minimizzare l'interferenza da/per il processo di verifica del sistema.

4.4. DA POLCAT A POLCAT.LIB

Il documento che è stato prodotto fino ad oggi, e di cui si è parlato nel precedente capitolo, è stato prodotto seguendo e cercando di rispettare quanto più possibilie i principi appena esposti. La fase iniziale di tutto il processo di riscrittura è stata caratterizzata dall'individuazione dei ruoli, e delle relative responsabilità, basati sulla metodologia CLASP. La successiva redazione del documento è stata il frutto di costanti incontri tra le figure previste da CLASP in modo da poter tenere sempre aggiornato lo stato di avanzamento dei lavori e presentare tempestivamente le problematiche emergenti. Sono state eseguite, di conseguenza, le seguenti fasi:

- Reverse Engineering: orientata alla ricerca di tutte le funzioni presenti e del loro corretto funzionamento;
- Raccolta e analisi dei requisiti: orientata alla ricerca delle parti da sostituire, ampliare o implementare ex novo in base anche a quelle che sono le richieste della Polizia Postale di Ancona.

4.4.1. Reverse Engineering

La produzione del documento di analisi di PolCat ci ha permesso di sviscerare tutti quelli che sono i problemi funzionali dell'applicatico mettendo in pratica quello che in gergo tecnico va sotto il nome di Reverse Engineering. Per studiare le caratteristiche di ciascuna funzione è stato adottato il seguente template di analisi:

Nome:	Nome della funzione
id:	identificativo della funzione (la prima cifra identifica il livello, le altre identificano la funzione chiamante)
Input:	parametri passati alla funzione;
Output:	funzionalità definita;
Funzioni richiamate:	funzioni che vengono utilizzate al suo interno;
Righe di codice:	numero di righe di codice utilizzate per definire la funzione;
Cosa fa:	Una breve sintesi su ciò che fa la funzione;
Bug/miglioramenti:	Descrizione dei bug incontrati e dei possibili miglioramenti da apportare alla funzione;
Note:	Note generiche sulla funzione;
Funzioni di sistema utilizzate:	Elenco delle funzioni di sistema utilizzate;

Figura 19: template per l'analisi delle funzioni

che è stato applicato a tutte e 106 le funzioni attualmente implementate. Per ognuna delle funzioni è stato anche riportato un diagramma a stati di finiti atto a descriverne il comportamento,

inteso come parametri passati in input, sottochiamate ad altre funzioni o a funzioni di stistema, valori restiuiti in output.

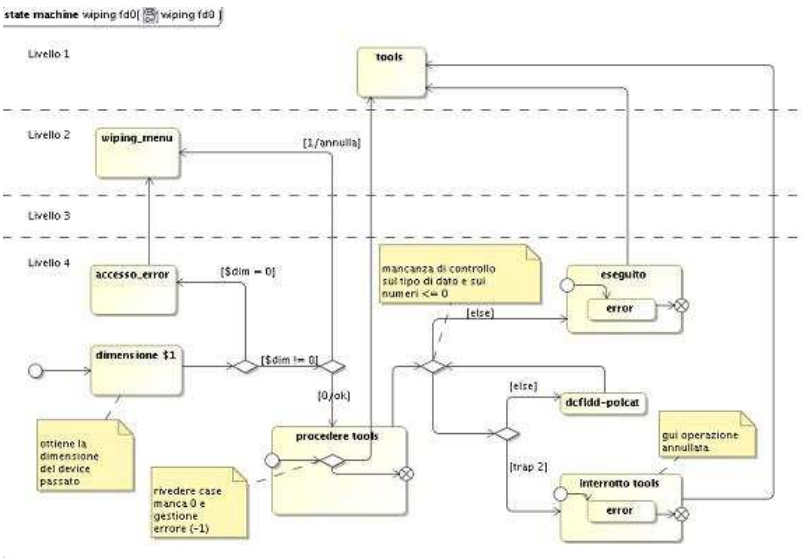

Figura 20: diagramma di stato per la funzione wiping

Le problematiche che abbiamo evidenziato, e che saranno quindi le questioni da risolvere nel prossimo futuro, sono state molteplici e di caratteristiche sia tecniche che funzionali. Per quanto riguarda le prime abbiamo riscontrato una forte dipenedenza di alcune funzioni con il kernel del sistema operativo ed occorrerà pertanto astrarre le funzioni fino a renderle indipendenti dalla piattaforma sottostante contribuendo allo stesso tempo rendere il nuovo framework più portabile e interoperabile. Oltre a quanto detto, PolCat non è in grado di acquisire file di evidence da programmi proprietari come EnCase e dunque occorrerrà inserire una nuova sezione di codice capace di farlo. Per quanto riguarda le seconde abbiamo riscontrato che alcune funzioni possono entrare in loop infiniti e non restituisco i corretti valori quano viene chiusa la procedura.

4.4.2. Analisi dei requisiti

Per quanto concerne l'analisi dei requisiti sono stati utilizzati i digrammi Use-Case del linguaggio di modellazione UML. In UML, gli Use Case Diagram (UCD o diagrammi dei casi d'uso) sono diagrammi dedicati alla descrizione delle funzioni o servizi offerti da un sistema, così come sono percepiti e utilizzati dagli attori che interagiscono col sistema stesso. Sono impiegati soprattutto nel contesto della Use Case View (vista dei casi d'uso) di un modello, e in tal caso si possono considerare come uno strumento di rappresentazione dei requisiti funzionali di un sistema. Tuttavia, non è impossibile ipotizzare l'uso degli UCD in altri contesti; durante la progettazione, per esempio, potrebbero essere usati per modellare i servizi offerti da un determinato modulo o sottosistema ad altri moduli o sottosistemi. In molti modelli di processo software basati su UML, la Use Case View e gli Use Case Diagram che essa contiene rappresentano la vista più importante, attorno a cui si sviluppano tutte le altre attività del ciclo di vita del softwareQuesti diagrammi consentono di descrivere i possibili usi che un utente qualsiasi può seguravere è stato utilizzato il linguaggio di modellazione.

4.4.2.1. Avvio dell'applicazione

Il diagramma use case che descrive l'avvio del framework è il seguente:

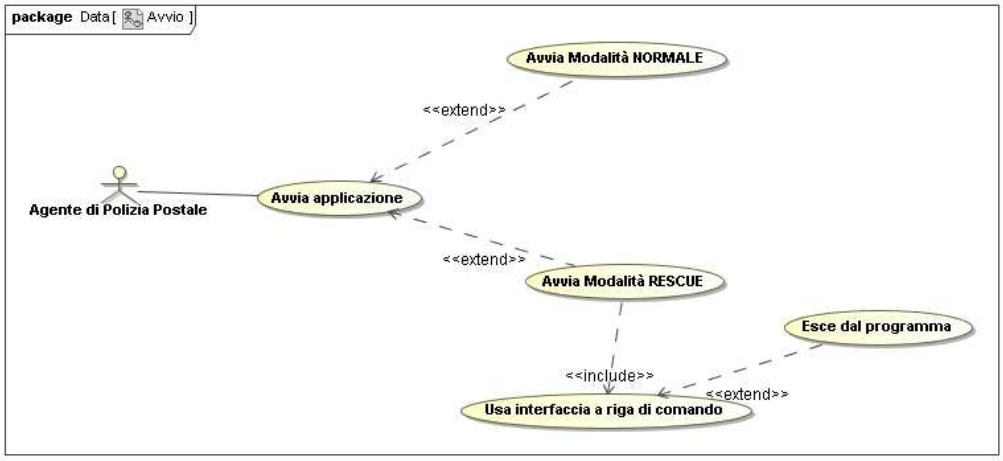

Figura 21: diagramma use-case per la fase di avvio

Come si può vedere anche per il nuovo applicativo verrà data la possibilità di operare in due differenti modalità: una, la più semplice, è la modalità NORMALE, la quale mette a disposizione un'interfaccia (shell) grafica user friendly per poter interagire in maniera semplice e veloce basata su menù richiamabili con tastierino numerico e/o con le frecce direzionali. In questo modo l'operatore inesperto può tranquillamente eseguire una clonazione, ad esempio, semplicemente come una sequenza numerica; l'altra, per gli utenti esperti del settore, è la modalità rescue, con la quale si vanno a compiere le operazioni direttamente da riga di comando. In questo caso sarebbe opportuno ripensare ad una shell i cui comandi siano facili da richiamare e semplici da utilizzare.

4.4.2.2. Avvio modalità NORMALE

Dato che la modalità RESCUE richiede una profonda conoscenza del sistema operativo ne tralasciamo il comportamento. Discutiamo invece di seguito la modalità NORMALE così come mostrata dal relativo diagramma USE CASE:

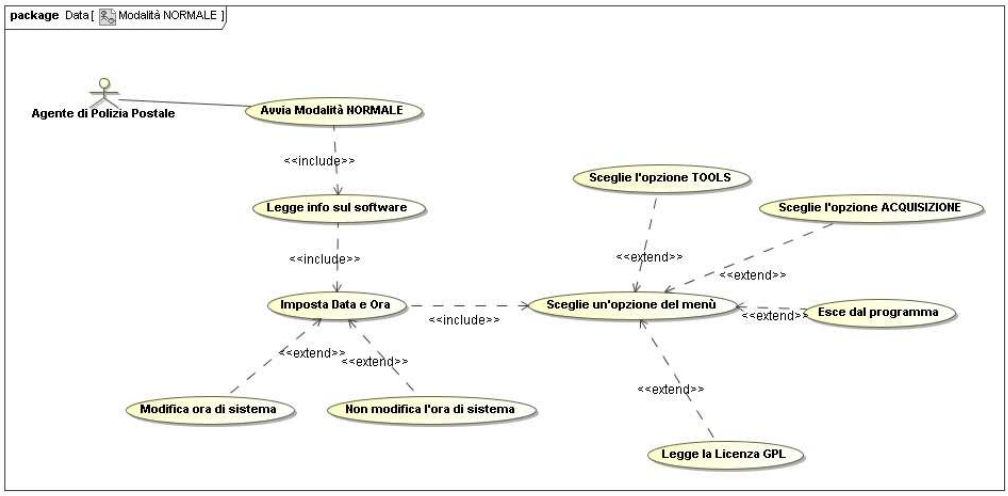

Figura 22: diagramma use case per la modalità NORMALE

Una volta scelto questo tipo di avvio, dovranno essere mostrate le informazioni sul software. Una volta lette, l'operatore (Agente di Polizia Postale nel diagramma) dovrà necessariamente impostare la data e l'ora che serviranno per documentare le operazioni effettuate. E' previsto che l'ora possa essere presa automaticamente dal sistema ma qual'ora questa non sia corretta, occorrerà impostarla senza errori. Solo quando le informazioni temporali saranno state impostate, sarà possibilie accedere al menù principale dal quale sarà possibile compiere le acqusizioni, utilizzare gli strumenti forniti oppure leggere le informazioni della GNU GPL (General Public License) che è una licenza per software libero. Il testo della GNU GPL è disponibile per chiunque riceva una copia di un software coperto da questa licenza. Gli utenti che accettano le sue condizioni hanno la possibilità di modificare il software, di copiarlo e

ridistribuirlo con o senza modifiche, sia gratuitamente sia a pagamento. Quest'ultimo punto distingue la GNU GPL dalle licenze che proibiscono la ridistribuzione commerciale.

4.4.2.3. Acquisizione disco e rete

L'acquisizione dei dischi è descritta dal diagramma che segue:

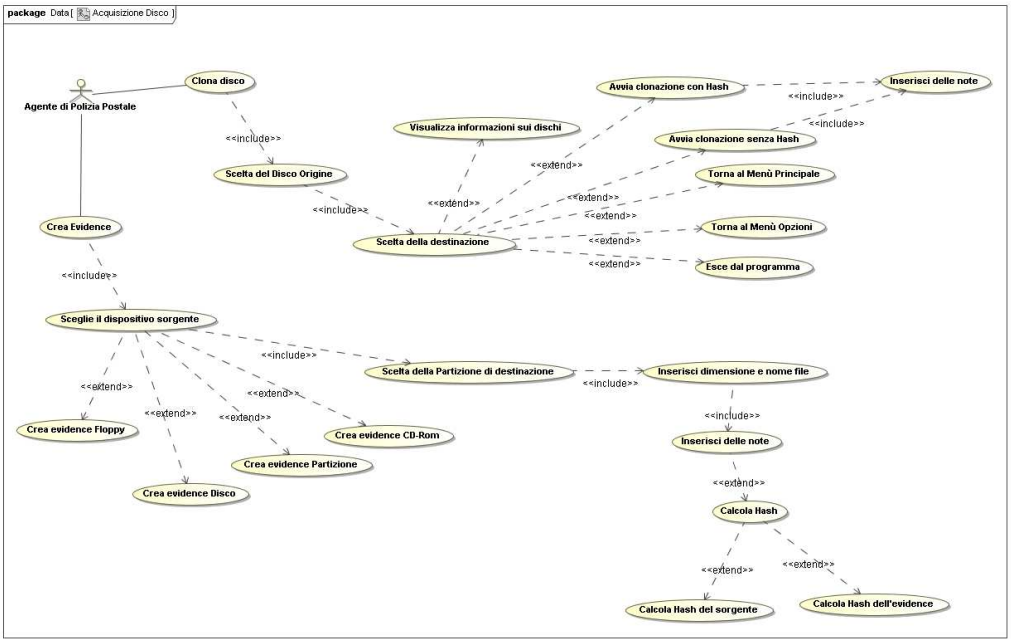

Figura 23: diagramma use case per l'acquisizione e clonazione

L'operatore avrà sempre la possibilità di sceglie se clonare un disco (soluzione al problema di non poter sequestrare fisicamente l'hardware) oppure creare un file di evidence nel caso in caso in cui si può operare direttamente sulla macchina. Com'è possibile dedurre dal significato dei termini, la clonazione esegue una duplicazione bit a bit di un hard disk mentre l'evidence restituisce l'effettiva prova digitale sulla quale andare ad operare con gli strumenti di analisi.
Per quanto riguarda la clonazione si dovranno ovviamente rispettare la selezione del disco (o partizione) sorgente e successivamente scegliere un dispositivo di sestinazione per la copia. Il calcolo dell'hash (sia sull'origine che sulla destinazione) dovraà essere fatto

con nuovi algoritmi, più veloci rispetto a quelli precedentemente usati così da soddisfare il requisito di velocità di acquisizione di una prova informatica. Tutta l'operazione di clonazione deve essere per quanto possibile commentata e pertanto è previsto di inserire uno spazio adibito all'inserimento delle note e di tutto quanto può essere utile questo punto di dovrà provvedere al calcolo.
Per quanto riguarda l'evidence invece, occerrà introdurre il codice necessario per l'individuazione e l'acquisizione, oltre agli usuali supporti di memorizzazzione, anche dei dispositivi di memorizzazione su USB e Compact Flash, che non sono attualmente presviste.
Le stesse osservazioni si possono dire per quanto riguarda la modalità di acquisizione tramite rete (in modalità client server) mostrata dal diagramma che segue:

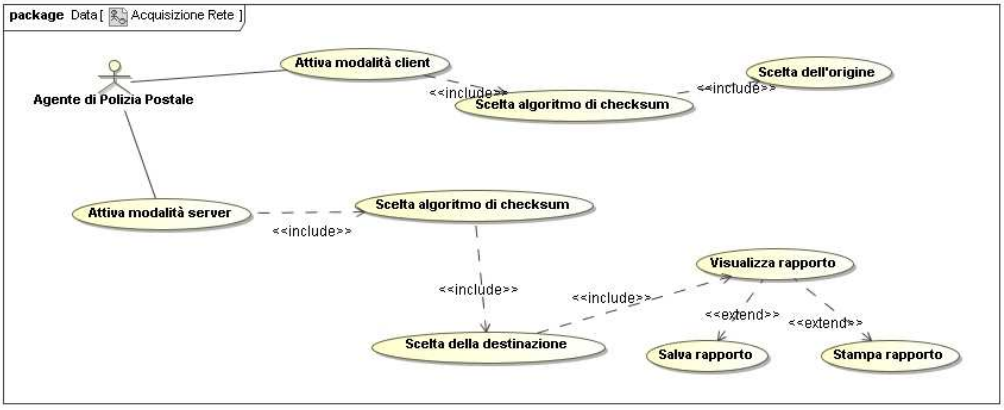

Figura 24: diagramma use-case per l'acquisizione da rete

Comunque, anche se non è stato inserito nei diagrammi, è da prevedere l'uso dello strumento di firma digitale, unito alla marcatura temporale, per garantire una ulteriore validità dei dati acquisiti (sia con la clonazione che con l'evidence). Il servizio di marcatura temporale di un documento informatico, consiste nella generazione, da parte di una Terza Parte Fidata, di una firma digitale del documento (anche aggiuntiva rispetto a quella del sottoscrittore) cui è associata l'informazione relativa ad una data e ad un'ora certa. Un file marcato temporalmente ha estensione .m7m

e al suo interno contiene il documento del quale si è chiesta la validazione temporale e la marca emessa dall'Ente Certificatore. Ma se da un lato può essere utile per la veridicità delle informazioni, dall'altro può essere un problema dato che può complicare la procedura di acquisizione.

4.4.2.4. TOOLS

L'alternativa all'acquisizione è rappresentata dalla scelta dei tools. Questi strumenti sono stati previsti al fine di poter effettuare altre operazioni (oltre all'acquisizione) che siano comunque utili ai fini forensi. Il diagramma che segue ne descrive i casi d'uso nel caso della scelta dell'opzione TOOLS dal menù principale:

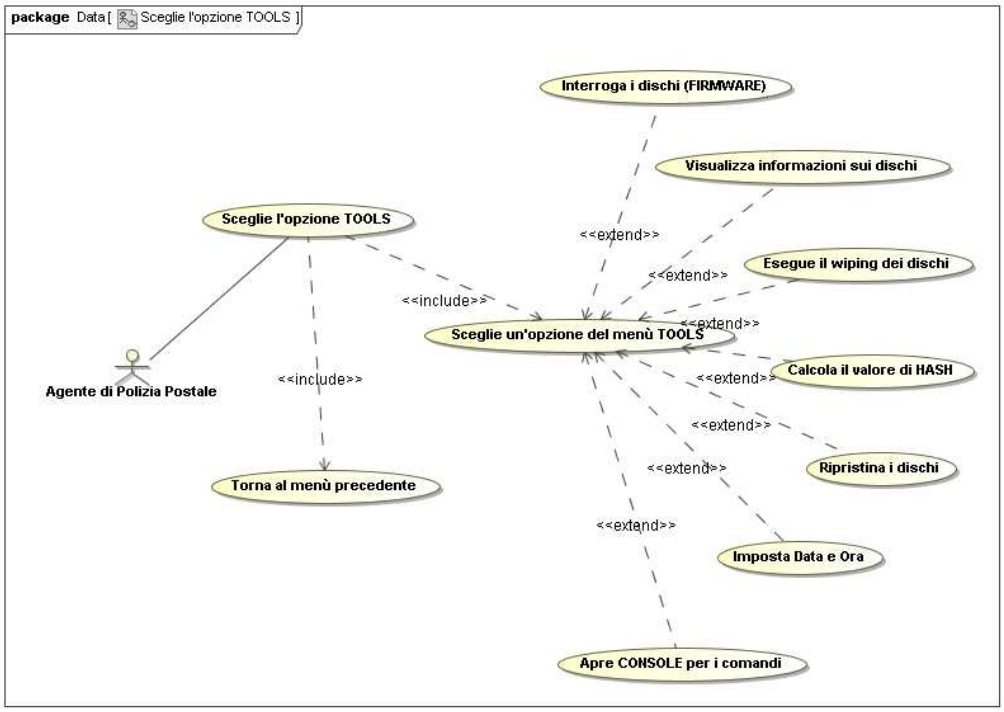

Figura 25: diagramma use-case per l'opzione TOOLS

Ritroviamo in questo caso, tutte le operazioni che abbiamo precedentemente descritto.

4.4.2.5. Firmware

Per quanto concerne l'acquisizione delle informazioni sul firmware degli hard disk, abbiamo osserveto che, nel rispetto di quelle che sono le specifiche proposte dalla Polizia Postale di Ancona, questo strumento dovrà essere integrato per dara la possibilità di acquisire il firmware anche di altri dispositivi, come lettori ottici, supporti magnetici esterni (come dispositivi USB), Compact Flash e floppy disk. Il diagramma che segue ne descrive il funzionamento:

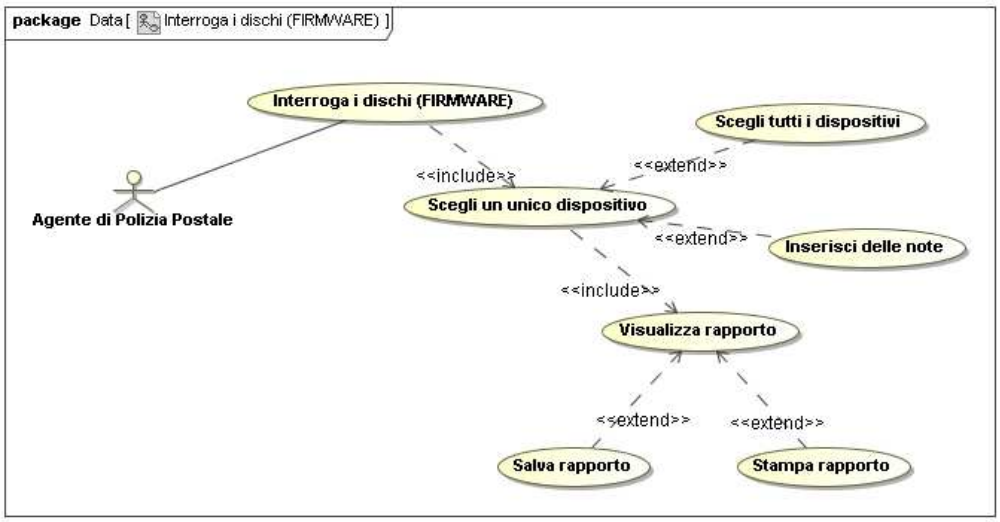

Figura 26: diagramma use-case per lo strumento firmware

4.4.2.6. Visualizza

A differenza del Firmware, questa opzione restituisce maggiori dettagli riguardo un dispositivo selezionato. Anche in questo caso si dovranno aggingere le parti di codice necessarie per il riconoscimento di altri supporti di memorizzazione. (il diagramma dei casi d'uso è simile a quello visto per il firmware).

4.4.2.7. Wiping

Il wiping consente di cancellare (definitivamente) i file contenuti su un dispositivo di memoria di massa collegato alla macchina sulla quale si sta operando una acquisizione. Tale strumento deve essere utilizzato precedentemente alle operazioni di clonazione o di acquisizione perché consente di preparare il disco che riceverà i dati. Una puliza non correttamente eseguita, può essere la causa di una eventuale corruzione dei dati. Il diagramma che segue ne descrive il comportamento:

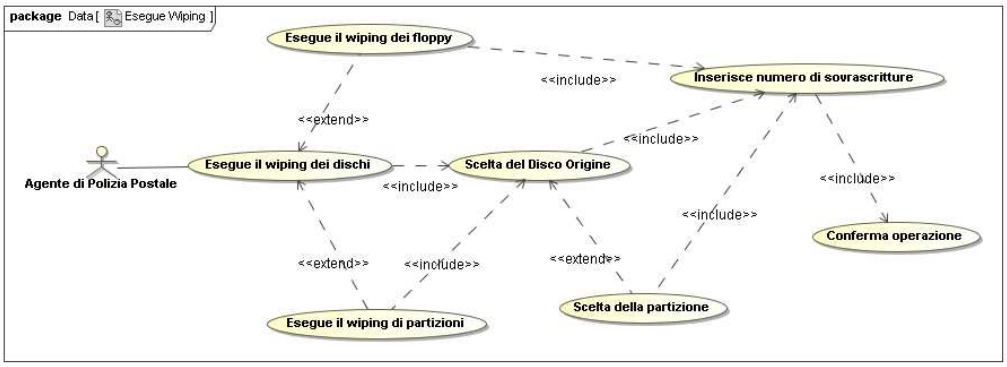

Figura 27: diagramma use-case per lo strumento wiping

E' da notare tuttavia che il wiping si utilizza più per cancellare le tracce piuttosto che per prepare i dispositivi. Diversi sono i metodi e gli algoritimi utilizzati per compiere questa procedura ma sono il numero di sequenze alternate di 0 e di 1 scritte sull'hard disk più l'ultima combinazione casuale a garantirne l'effetto.

4.4.2.8. Hashing

Lo strumento per il calcolo dell'hash è di fondamentale importanza per qualsiasi framework forense. Questa opzione ci consente di calcolare il message digest (md5) dei dati dei dispositivi presenti sulla macchina. L'MD5 (acronimo di Message Digest algorithm 5) è un algoritmo per la crittografia dei dati a senso unico. Oltre a MD5 esistono altri algoritmi per il calcolo dell'hash, tra cui il più famoso è SHA-1. SHA sta per Secure Hash Algorithm e può contare su 5 varianti che differiscono tra loro sulla base del numero di bit che produce come output (i cinque algoritmi sono chiamati SHA-1, SHA-224, SHA-256, SHA-384, e SHA-512). La sicurezza di SHA però, è stata intaccata dai crittoanalisti ed è per questo motivo che sono state scritte le versioni successive.
Tuttavia, indipendentemente dall'algoritmo di hash utilizzato, i casi d'uso per la funzionalità di hash sono descritte dal diagramma seguente:

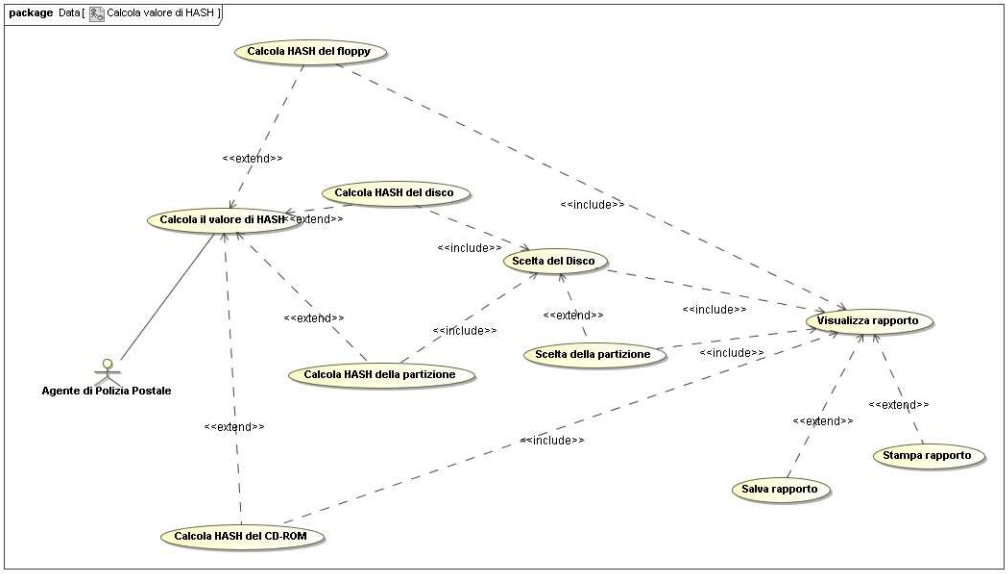

Figura 28: diagramma use-case per lo strumento hashing

Oltre a consetire il calcolo sui dispositivi come floppy disk, hard disk, partizioni e cd-rom, occorreà inserire la possibilità di calcolare l'hash su altri dispositivi id memoria di massa (compact flash e supporti usb).

4.4.2.9. Restore

L'opzione di restore consente il ripristino del contenuto di un disco rigido, o di una sua partizione, su un altro dispositivo di memoria di massa. Ciò che occorre implementare per questa funzionalità, è la possibilità di ripristinare anche file di evidence prodotti da altri strumenti (come EnCase ad esempio) in modo da poter proseguire con l'analisi dei dati. Questo significa che il framework dovrà essere in grado di riconoscere il formato Expert Witness (EWF), che è alla base dei formati immagine creati da EnCase e il formato per l'Advanced Forensic Format. Quest'ultimo, in particolare, è un formato immagine sviluppato per essere estensibile ed aperto. La sua struttura dei dati è documentata ed il formato consiste in un gruppo di coppie nome-valore, chiamati segmenti.

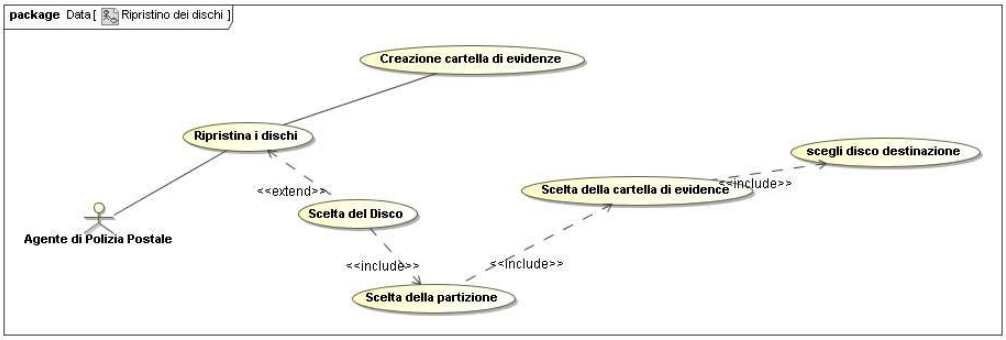

Figura 29: diagramma use-case per lo strumento restore

Indipendentemente dal formato da ripristinare, è necessario avere a disposizione una cartella contenente il file di evidence per poter effettuare il ripristino di un disco o di una partizione. Questo file

infatti contiene tutti i dati che erano presenti sul disco e che erano stati precedentemente acquisiti.

Le funzioni che abbiamo descritto precedentemente sono quelle sulle quali si andrà a lavorare. Sono state volutamente tralasciate le funzionalità di Data / Ora e Console perché il loro utilizzo è e resterà lo stesso descritto in precedenza.

CONCLUSIONI

Quella della digital forensic, e in particolare il computer forensic, è divenuta una realtà in cui tecniche e tecnologie per la ricerca, l'individuazione e il repertamento delle informazioni sono in continua e sistematica evoluzione. Non da meno lo sono i reati informatici che, parallelamente alla disciplina forense, progrediscono in maniera proporzionale rispetto alle novità tecnologiche introdotte sul mercato, le quali rappresentano il fattor comune di tutte le diverse tipologie di illecito riconosciute dalla legge.

Per questi motivi la corretta gestione dei processi dell'attività forense, unita ad una attento management della catena di custodia delle prove digitali, sono la base di partenza per compiere una valida indagine da parte delle Polizie Postali e delle Telecomunicazioni.

In ogni caso le problematiche connesse all'attività forense non sono da attribuire alla mancanza di normative in materia penale in quanto, come si è potuto riscontrare nel secondo capitolo di questo lavoro, sono state oggetto di studio fin dal lontatno 1993. Non sono altresì da attribuire alla mancanza di personale tecnico e qualificato, ma derivano dalla carenza di una serie di strumenti, di standard, di formalizzazioni, di linee guida e di best pratice indirizzati alla ricerca di soluzioni che mirino al raggiungimento di un'elevata interoperabilità.

Con questo lavoro di tesi si è cercato di soddisfare i seguenti obiettvi principali: da un lato la realizzazione Open Source del nuovo Framework PolCat, per l'attività di digital forensic, che sia in grado di fornire uno specifico supporto per la risoluzione delle

problematiche connesse al processo di acquisizione dei dati e di validazione dei files di evidence prodotti; dall'altro lato quello di produrre un software che, per il suo sviluppo, abbia rispettato e seguito le linee guida degli standard riguardanti il Sistema di Gestione della Sicurezza delle Informazioni riportate nella ISO 27001 e nelle linee guida della metodologia CLASP del progetto OWASP (Open Web Application Security Project) al fine di ottenere una certificazione di qualità. La certificazione di un prodotto costituisce una forma di garanzia per chi intende usufruirne, in quanto soddisfa tutte le richieste che sono state fatte dal committente.

Nonostante tutto, il valore giuridico da conferire alle prove generate dagli strumenti di digital forensic, non sono da attribuire ai software prodotti secondo questa metodologia, ma derivano dalla competenza e dall'esperienza dell'informatico forense in quanto ha la consapevolezza di poter esprimere, in scienza e coscienza, valutazioni da trasmettere alle autorità inquirenti indipendentemente dal tipo di software utilizzato.

BIBLIOGRAFIA

[ACPO02]: ACPO – Association of Chief Police Officers, Good Practice Guide for Computer-Based Electronic Evidence, 7Safe Information Security, 2002

[Asn03]: Asnaghi V., "BS7799 e Contratti ICT - Seminario CLUSIT sulla sicurezza nei contratti ICT", 2003, http://www.clusit.it/evento_sia/vasnaghi_16_06_03.pdf

[Atz06]: Atzori M., "Informatica Giudiziaria e Forense - Campi di applicazione", 2006, http://www.digitalforensic.it/menu/applicazioni.html

[BSDRI05]: Bruzzone R., Strano M., De Marco F., Rossi A., Innamorati M., "Spider software di supporto alle indagini sulla pedopornografia sul web", in Conferenza internazionale su strumenti, procedure, standard operativi e ricerca accademica (inerente aspetti tecnici e psicologici) nel settore delle investigazioni su Internet con speciale riferimento alla pedo-pornografia, Raggruppamento Carabinieri Investigazioni Scientifiche, Roma, 2005

[Car03]: Carrier B., "The Open Source Digital Forensics site", 2003, http://www.opensourceforensics.org/

[Cos06]: Costabile G., "Scena Criminis, Documento Informatico e formazione della prova penale - Reati informatici e attività di indagine - Lo stato dell'arte e prospettive di riforma", 2006, http://www.altalex.com/index.php?idnot=7429

[DFRW01]: Digital Forensic Research Workshop, "A Road Map for Digital Forensic Research", 2001, http://dfrws.org/2001/dfrws-rm-final.pdf

[DiP06]: Di Paola S. "Gestione del Processo di Sviluppo", 2006, http://www.sicurinfo.it/informazioni/Files/246/Owasp_Fitec_DiPaola.pdf

[DNV08]: Det Norske Veritas (DNV),"Certificazione Sistemi di Gestione", 2008, http://www.dnv.it/certificazione/sistemidigestione/BS7799/27001/index.asp

[Efe05]: e-fense.com, "the helix live cd", 2005, http://www.e-fense.com/helix/docs.php

[EHP06]: Ethical Hacking, Penetration Testing & Computer Security, "Ten best security live-cd distros pen-test forensics recovery", 2006, http://www.darknet.org.uk/2006/03/10-best-security-live-cd-distros-pen-test-forensics-recovery/

[For01]: Forte D., Le attività informatiche a supporto delle indagini giudiziarie – Il Diritto dell'Er@ di Internet, Mucchi, Modena, 2001;

[Fra06]: Fraticelli C., L'Hacking, il gioco tra guardie e ladri e la computer forensic, 2006, http://www.avvocati.it/formazione/Laculturadelleregole.pdf

[Gal06]: Galdieri P., "Reati informatici e responsabilità delle persone giuridiche: l'Europa chiede una riforma - Reati informatici e attività di indagine - Lo stato dell'arte e prospettive di riforma", 2006, http://www.convegnovarenna.giuristitelematici.it/relazioni/galdieri.pdf

[Ghi02]: Ghirardini A., "Introduzione alla Computer Forensics", 2002, http://www.sikurezza.org/webbit02/computer-forensics.pdf

[Gue06]: Guerrieri L., "Forensic in Open Source, c'è da fidarsi?", 2006, http://www.forlex.it/index.php?option=com_content&task=view&id=23&Itemid=1

[Hof03]: Hofherr M., "Forensics, Intrusion Detection, Security Technology", 2003, http://www.forinsect.de/forensics/forensics-tools.html

[IAT04]: Induction, Awareness and Training Zone, "Induction To ISO 17799 / BS7799", 2004, http://www.induction.to/bs7799/

[ISO05]: ISO - International Organization for Standardization, "ISO/IEC 27001:2005", 2005, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[Kor01]: Kornblum J., "Open Source in Computer Forensics", 2001, http://jessekornblum.com/research/presentations/open-source-in-computer-forensics.pdf

[Mat05]: Mattiucci M. (Mag. CC), e altri, "Investigazioni Tecniche: mezzi e problematiche", in: Conferenza internazionale su strumenti, procedure, standard operativi e ricerca accademica (inerente aspetti tecnici e psicologici) nel settore delle investigazioni su Internet con speciale riferimento alla pedo-pornografia, Raggruppamento Carabinieri Investigazioni Scientifiche, Roma, 2005

[Mat06]: Mattiucci M. (Mag. CC), "I Crimini ad Alta Tecnologia e l'Arma dei Carabinieri", 2006, http://www.marcomattiucci.it/pisa2006.pdf

[Mat07a]: Mattiucci M. (Mag. CC), "Il Digital Forensics", 2007, http://www.marcomattiucci.it/htc.php

[Mat07b]: Mattiucci M. (Mag. CC), "L'assurdo di copia ed originale per i dati digitali", 2007, http://www.marcomattiucci.it/copy.html

[Mat07c]: Mattiucci M. (Mag. CC), "Repertamento di sistemi High Tech", 2007, http://www.marcomattiucci.it/reper.html

[Mat07d]: Mattiucci M. (Mag. CC), "La catena di custodia (Chain of Custody)", 2007, http://www.marcomattiucci.it/chainofcustody.html

[Mat07e]: Mattiucci M. (Mag. CC), "La Hash MD5 - collisioni e probabilità", 2007, http://www.marcomattiucci.it/md5.html

[Mat07f]: Mattiucci M. (Mag. CC), "Computer Forensic", 2007, http://www.marcomattiucci.it/computerforensicarea.html

[Mon06]: Monga M., "L'intrinseca fragilità delle tracce digitali", 2006, http://www.avanzata.it/left/traccedigitali.pdf

[NTW07]: News technology's world - information and services for tecnological world, "Analisi Forense", 2007, http://www.newstechnology.eu/web/content/view/94/6/lang,it/

[OWA07]: Owasp, "OWASP CLASP v1.2" , Copyright: © 2007 OWASP Creative Commons Attribution-NonCommercial-ShareAlike 2.0 Lingua: English Paese: Regno Unito, http://www.lulu.com/content/1401307

[OWA08a]: Open Web Application Security Project, "Welcome to OWASP the free and open application security community", 2008, http://www.owasp.org/index.php/Main_Page

[OWA08b]: OWASP, "Category:OWASP CLASP Project", 2008, http://www.owasp.org/index.php/Category:OWASP_CLASP_Project

[Per04]: Perri P., "Sicurezza informatica aziendale e definizione delle diverse responsabilità degli organici aziendali", 2004, http://www.avanzata.it/slides/pierpolicy.pdf

[Pes06]: Pesce E., "Analisi Forense", 2006, http://www.enricopesce.it/2006/06/02/analisi-forense/

[PGDC07]: Pierlorenzi M. (1° Dir P. di S.), Grilli A. (V.Q.A. P. di S.), Deidda A. (V. Sov. P. di S.), Capriotti R. (Ag. Sc. P. di S.), Elementi di Comupter Forensics – Ricerca ed analisi della prova informatica nell'attività investigativa della polizia giudiziaria, Ancona, Linfa Educational, 2007;

[Ros07]: Rosiello A., "Network Forensic : strumenti avanzati per l'analisi del traffico di rete e la prevenzioni di eventi critici.", 2007, http://www.dinets.it/ictsecurityday2007/doc/Rosiello.pdf

[Sav03]: Savastano R., "Computer Forensic – Problematiche e Metodologie di Audit", Associazione Italiana Information System Auditors, 2003, http://www.aiea.it/pdf/sessioni%20di%20studio%20e%20di%20formazione/2003/Milano%205%20giugno%202003%20%20Computer%20Forensic.pdf

[Sca07]: Scalea D., "Computer Forensics - Metodologia, Eziologia ed Etica", 2007, http://www.cybercrimes.it/whitepapers.html

[Sca07]: Fratis D., "Iritaly live-cd: informatica forense all'italiana", 2007, http://www.cybercrimes.it/whitepapers.html

[SIN05]: SINCERT, Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione e Ispezione, "Sicurezza delle Informazioni, 2005, http://www.sincert.it/documentisincert.asp?id=179

[SLO03]: Studio Legale online, "Diritto dell'informatica", 2003, http://www.studiolegale-online.net/diritto_informatica_08.php

[Tor07]: Torcasio M., "Metodi e Modelli nella Digital Forensics in Italia: Ipotesi di uno strumento di mapping - Tesi di Laurea Sperimentale", 2007

[Tre02]: Trefiletti F., "Storia e attività della Polizia Postale", 2002, http://www.domainday.it/dd_2002/interventi/Fabiola%20Treffiletti_STORIA%20E%20ATTIVITA'%20DELLA%20POLIZIA%20POSTALE.doc

[TWT05]: The Window To, "The BS7799 Security Guide", 2005, http://www.thewindow.to/bs7799/

[Viz06]: Vizzarro D., "I reati informatici nell'ordinamento italiano", 2006, http://www.danilovizzarro.it/papers/I%20Reati%20Informatici%20nell%27Ordinamento%20Italiano.pdf

[Wik08]: Wikipedia l'enciclopedia libera, "Standard di sicurezza informatica", 2008, http://it.wikipedia.org/wiki/Standard_di_sicurezza_informatica

[Zic06a]: Ziccardi G., "Computer Forensics", 2006, http://www.avanzata.it/slides/lezione17.pdf

[Zic06b]: Ziccardi G., Introduzione al rapporto tra scienza forense e tecnologie informatiche e telematiche, 2006, http://www.avanzata.it/left/primoincontroleft.pdf

[Zic06c]: Ziccardi G., "Internet, sicurezza e libertà personali nell'epoca dell'emergenza terrorismo: alcune Riflessioni", 2006, http://www.avanzata.it/articoli/antigone2006.pdf

[Zic06d]: Ziccardi G., "Informazioni libere e protette", 2006, http://www.avanzata.it/slides/introlibert.pdf

[Zic06e]: Ziccardi G., "La brevettabilità del software", 2006, http://www.avanzata.it/slides/slidesbrevetti.pdf