Ruolo e prospettive dell'Informatica Forense

Cesare Maioli

CIRSFID e Facoltà di Giurisprudenza
Università di Bologna

Catania, 19 marzo 2012

Introduzione

- I **dati digitali** sono le entità di base su cui operano i sistemi informatici come applicazioni software, email, feed, il web
- L'economia globale è sempre più dipendente dall'**elaborazione** di informazioni digitali e dalla loro **trasmissione** attraverso le reti telematiche
- Le autorità procedenti *(law enforcer)* nell'ambito della loro attività d'indagine, si avvalgono sempre più di tali dati che, una volta correttamente **acquisiti** e **analizzati** potranno, da soli o in combinato alle tradizionali modalità investigative, assumere **valore di prova** contribuendo significativamente all'identificazione e persecuzione dell'autore materiale dell'illecito

Reati che coinvolgono le TIC

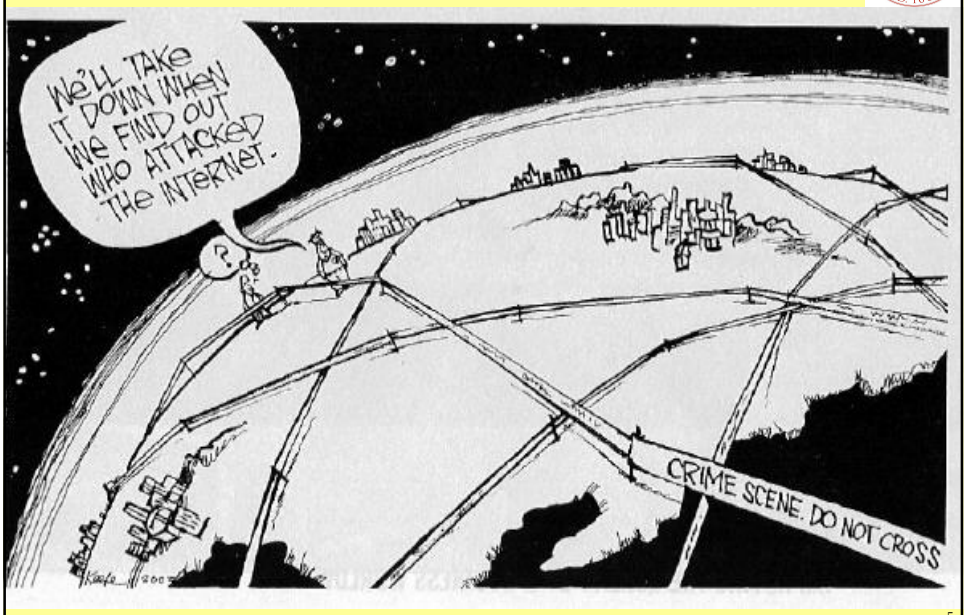
- **Reati tradizionali o comuni** in cui il computer assume la qualità di **strumento del reato**; ad esempio frodi o falsificazioni e, più in generale, qualsiasi utilizzo di informazioni con modalità pregiudizievoli e malevole
- **Reati relativi a contenuti** (*content-related offences*) in cui si utilizzano le TIC (Tecnologie dell'Informazione e della Comunicazione) per facilitare la **distribuzione** di **materiali illegali o illeciti**; ad esempio violazioni dei diritti d'autore e la pornografia minorile
- **Reati di danneggiamento** volti a danneggiare **l'integrità delle componenti tecnologiche** dei sistemi TIC; ad esempio la distribuzione di *virus*

Il trattamento di dati informatici a fini processuali

Il ricorso all'**Informatica Forense** può rendersi **necessario** nei procedimenti aventi ad oggetto:

- **reati informatici** propriamente detti ex L. n°547/93, L. n°48/08
- **reati** commessi con **l'impiego di sistemi informatici**
- dati (o informazioni) aventi **valore di prova o indizio** per reati informatici e non
- strumenti (supporti) di **archiviazione** di dati rilevanti

Il Cyberspazio non ha frontiere...



http://digitalforensics.champlain.edu/about_cdf.html

Nel Cyberspazio senza frontiere...

Difficoltà di ricostruzione dei reati globali

- Dislocazione dell'autore: da dove
- Indeterminatezza degli autori: quanti
- Anonimizzazione dell'autore: chi è, chi sono
- Cronologia degli eventi: quando
- Modalità esecutive: in che modo
  - velocità dell'attività
  - volatilità delle tracce
- Movente: perché
- Reiterazione: quante volte
- Offensività: contro chi

...a fronte di reati senza frontiere...

La criminalità usa la tecnologia informatica che non ha confini

- Terrorismo
- Cracking
- Accesso abusivo
- Danneggiamento informatico
- Pedopornografia
- Discriminazione razziale
- Ingiuria e diffamazione
- Spamming
- Bilanci falsi
- Riciclaggio
- Phishing
- Truffe on line
- Estorsioni
- Violazione della privacy
- Violazioni al diritto d'Autore
- Frode informatica
- "Furto" di dati

Contromisure

- Biometria
- **Infrastruttura pubblica di chiavi**
- Carte con password one-time
- **File crittati**
- Sistemi di prevenzione delle intrusioni
- Sistemi di login e password
- **Crittografia dei dati in transito**
- Sistemi di rilevamento delle intrusioni
- Controlli degli accessi nel server
- Firewall
- Software antivirus

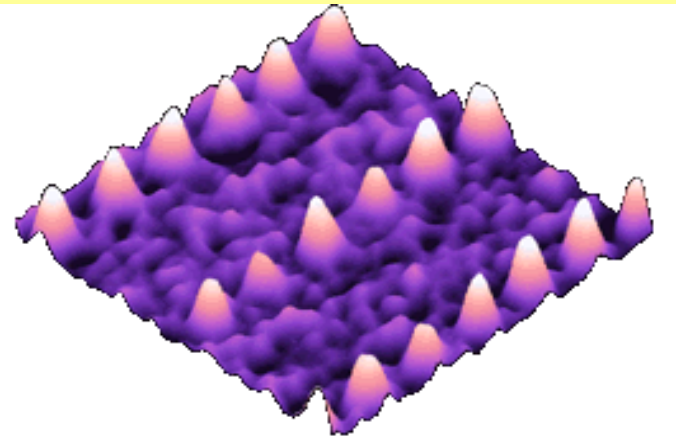
Crescita della domanda di analisi

All'aumento del trattamento di dati con sistemi informatici consegue **l'incremento della domanda di analisi dei dati digitali a fini di investigazione e di giustizia** per

- reati informatici e telematici (es. L. 547/93, L.48/08)
- reati non informatici ma commessi con sistemi informatici
- reati di cui si rinvengono tracce o indizi nei sistemi informatici

Comune denominatore:
il dato digitalizzato come oggetto di indagine

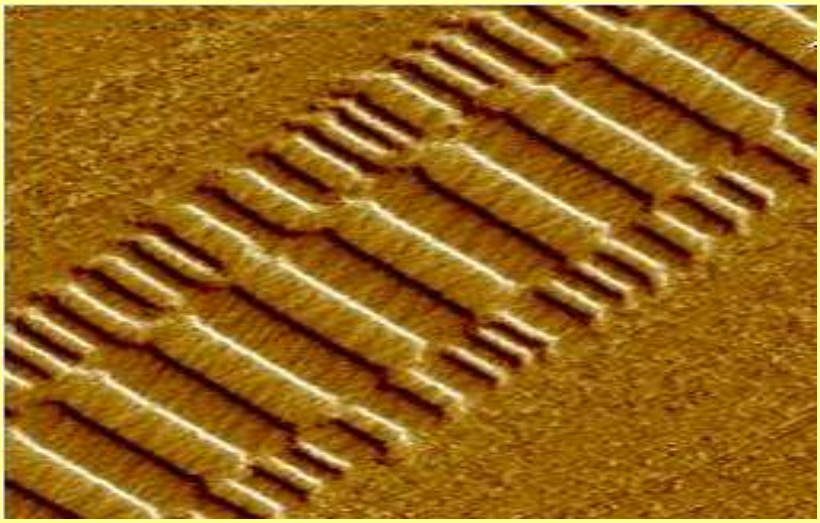
Bit magnetici scritti con una sonda MFM (Magnetic Force Microscope)



I bit sono di dimensione di circa 180 nm (nanometro; 180 miliardesimi di metro cioè milionesimi di millimetro) distanziati di cerca 370 nm, dando origine quindi a una densità di cerca 5 Gbits/pollice cioè 5 miliardi di bit per 2.3 cm

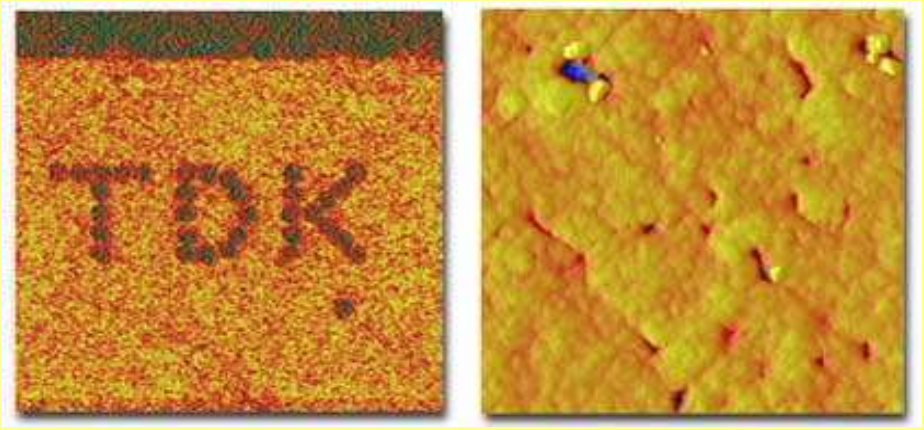
http://www.veeco.com/library/nanotheater.php

Hard Disk- II



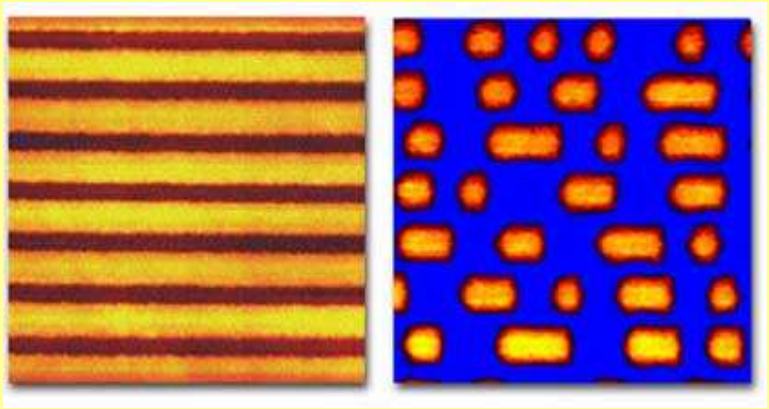
http://www.veeco.com/library/nanotheater.php

Bit scritti su una superficie ferroelettrica



http://www.veeco.com/library/nanotheater.php

Bit su DVD – RW



http://www.veeco.com/library/nanotheater.php

Definizione e obiettivi dell'Informatica Forense

L'Informatica forense è la disciplina avente ad oggetto lo studio delle attività di **individuazione**, **conservazione, protezione, estrazione, documentazione** ed ogni altra forma di trattamento ed **interpretazione** del **dato digitale** memorizzato su supporto informatico, al fine di essere valutato come **prova** nel processo

Corso di Informatica Forense: obiettivi

- Il corso esamina gli **aspetti giuridici e tecnologici** attinenti alla prova digitale.
- Muovendo dalla **computer forensics** internazionale si analizzano le modalità di indagine informatica alla luce dell'ordinamento giuridico italiano: tecniche di indagine scientifica, indagine informatica, investigazione difensiva nonché le indagini su sistemi di telefonia fissa e mobile.
- Si fornisce un quadro dei **problemi tecnici tipicamente informatici** in correlazione alle **problematiche giuridiche sottese** a tali tipi di indagini, *in primis* la corretta applicazione del diritto penale sostanziale e processuale.
- L'attenzione si sofferma sull'analisi delle norme rilevanti per le tecniche di acquisizione, conservazione, analisi e produzione dei dati digitali rinvenuti nei computer e dei flussi telematici, per la loro **utilizzabilità nell'ambito dei vari tipi di processi** (civile, penale, tributario, amministrativo, contabile) nonché in altri tipi di istruttoria e procedimento amministrativo sia della Pubblica Amministrazione che delle autorità indipendenti (Banca d'Italia, Consob, Privacy, Antitrust, Telecomunicazioni).

Informatica Forense - *Parte tecnologica*

1. Procedimenti e strumenti tecnici e organizzativi per l'informatica forense
2. Computer come **macchine del tempo**
3. **Archeologia informatica**
4. Metodi di duplicazione e riproduzione dei dati
5. Analisi dei dischi e delle memorie; livelli di volatilità
6. Analisi di dispositivi mobili; integrazione con la telefonia e con sistemi multimediali
7. Sistemi operativi e file system
8. **Geologia informatica**
9. Raccolta di reperti dai dispositivi
10. Protocolli di rete e analisi del traffico
11. Attacchi alle reti; investigazioni su Internet, router, collegamenti
12. Analisi di strumenti di malware
13. **Redazione di rapporti** solidi per l'analisi giudiziaria
14. Complementi sui casi (VoiceOverIP, Phone Forensics, elementi di steganografia, cloud computing)

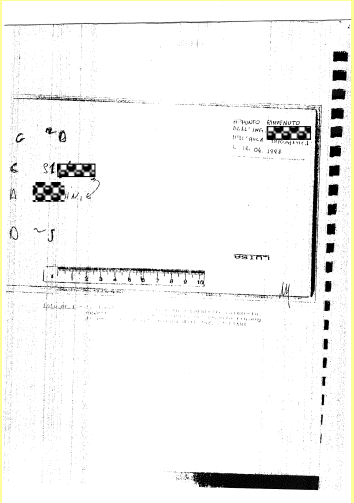
Informatica Forense - *Parte giuridica*

1. Evoluzione tecnologica e nuove forme di criminalità
2. Le esperienze internazionali di computer forensics
3. L'esperienza italiana: dalla Computer Forensics all'Informatica Forense
5. **Modelli processuali penali ed informatica forense**
6. Norme rilevanti per l'informatica forense
7. L'indagine penale in materia informatica
8. Le investigazioni difensive in materia informatica
9. La legislazione speciale in materia informatica
10. **Indagini informatiche** e criminologia informatica
11. Indagini, investigazioni e trattamento dei dati personali
12. Consulenti e periti in materia informatica
13. Casi di cronaca
14. **Il problema delle indagini e della giurisdizione sovranazionale**
15. La Convenzione su Cybercrimine e i recepimenti nazionali
16. L'informatica forense per gli altri tipi di processo (e-Discovery)

Caso 1 - I: Danno a apparecchiature della PA

Oggetto: **manoscritto con passaggi**

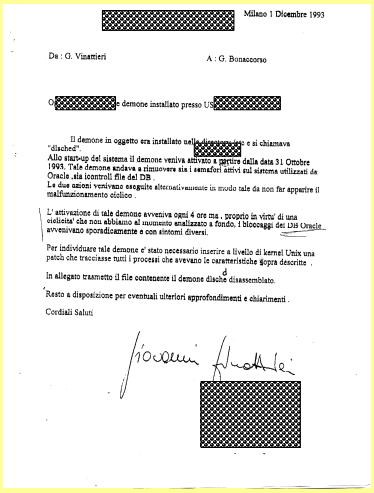
Tecnica di verifica: perizia calligrafica comparativa



Caso 1 – II: démoni nel 1993

Oggetto: fax + **descrizione demone** + fotocopia con 3 pezzi di **listato**

Tecnica di verifica: nessuna



[redacted] Milano 1 Dicembre 1993

Da : G. Vinattieri A : G. Bonaccorso

O [redacted] demone installato presso US[redacted]

Il demone in oggetto era installato nell[redacted] e si chiamava "disched".
Allo start-up del sistema il demone veniva attivato a partire dalla data 31 Ottobre 1993. Tale demone andava a rimuovere sia i semafori attivi sul sistema utilizzati da Oracle ,sia i controll file del DB .
Le due azioni venivano eseguite alternativamente in modo tale da non far apparire il malfunzionamento ciclico .

L' attivazione di tale demone avveniva ogni 4 ore ma , proprio in virtu' di una ciclicita' che non abbiamo al momento analizzato a fondo, I bloccaggi dei DB Oracle avvenivano sporadicamente e con sintomi diversi.

Per individuare tale demone e' stato necessario inserire a livello di kernel Unix una patch che tracciasse tutti I processi che avevano le caratteristiche sopra descritte .

In allegato trasmetto il file contenente il demone dische disassemblato.

Resto a disposizione per eventuali ulteriori approfondimenti e chiarimenti .

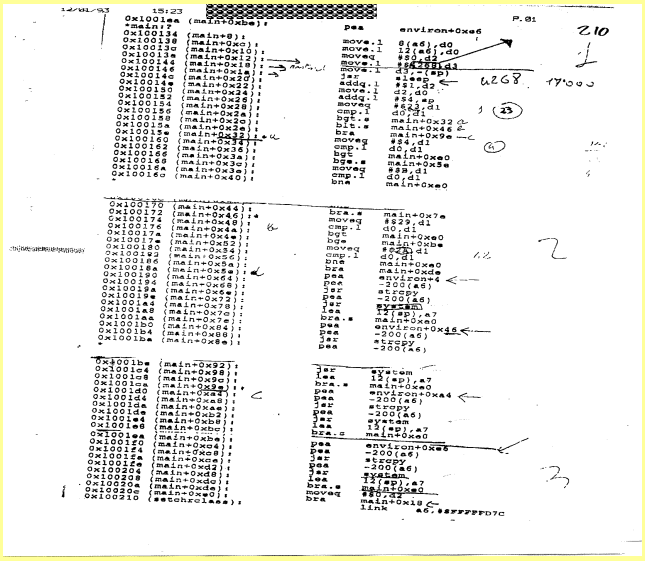
Cordiali Saluti

[redacted]

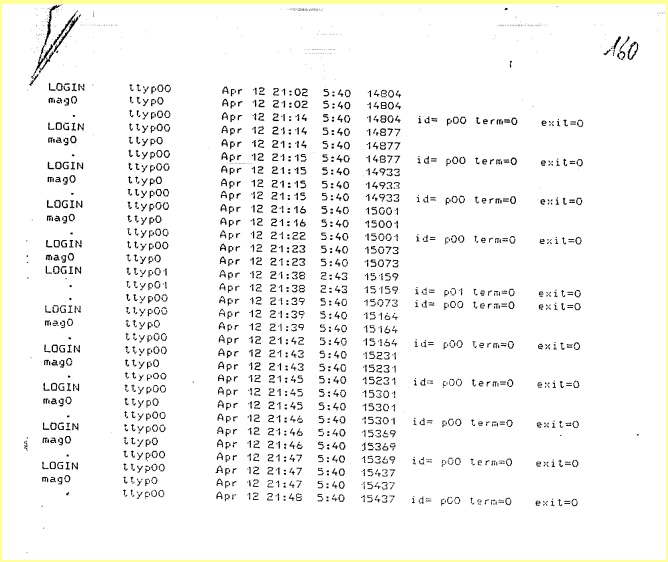
Caso 1 – III: tre listati incollati

Oggetto: tre **listati di comandi unix**

Tecnica di verifica: nessuna



Caso 1 – IV: Esempio di prova per la PG



160

LOGIN	ttyp00	Apr	12	21:02	5:40	14804		
mag0	ttyp0	Apr	12	21:02	5:40	14804		
.	ttyp00	Apr	12	21:14	5:40	14804	id= p00 term=0	exit=0
LOGIN	ttyp00	Apr	12	21:14	5:40	14877		
mag0	ttyp0	Apr	12	21:14	5:40	14877		
.	ttyp00	Apr	12	21:15	5:40	14877	id= p00 term=0	exit=0
LOGIN	ttyp00	Apr	12	21:15	5:40	14933		
mag0	ttyp0	Apr	12	21:15	5:40	14933	id= p00 term=0	exit=0
.	ttyp00	Apr	12	21:16	5:40	15001		
LOGIN	ttyp00	Apr	12	21:16	5:40	15001		
mag0	ttyp0	Apr	12	21:22	5:40	15001	id= p00 term=0	exit=0
.	ttyp00	Apr	12	21:23	5:40	15073		
LOGIN	ttyp00	Apr	12	21:23	5:40	15073		
mag0	ttyp0	Apr	12	21:38	2:43	15159		
LOGIN	ttyp01	Apr	12	21:38	2:43	15159	id= p01 term=0	exit=0
.	ttyp01	Apr	12	21:39	5:40	15073	id= p00 term=0	exit=0
.	ttyp00	Apr	12	21:39	5:40	15164		
LOGIN	ttyp00	Apr	12	21:39	5:40	15164		
mag0	ttyp0	Apr	12	21:42	5:40	15164	id= p00 term=0	exit=0
.	ttyp00	Apr	12	21:43	5:40	15231		
LOGIN	ttyp00	Apr	12	21:43	5:40	15231		
mag0	ttyp0	Apr	12	21:45	5:40	15231	id= p00 term=0	exit=0
.	ttyp00	Apr	12	21:45	5:40	15301		
LOGIN	ttyp00	Apr	12	21:45	5:40	15301		
mag0	ttyp0	Apr	12	21:46	5:40	15301	id= p00 term=0	exit=0
.	ttyp00	Apr	12	21:46	5:40	15369		
LOGIN	ttyp00	Apr	12	21:46	5:40	15369		
mag0	ttyp0	Apr	12	21:47	5:40	15369	id= p00 term=0	exit=0
.	ttyp00	Apr	12	21:47	5:40	15437		
LOGIN	ttyp00	Apr	12	21:47	5:40	15437		
mag0	ttyp0	Apr	12	21:48	5:40	15437	id= p00 term=0	exit=0
.	ttyp00							

Caso 2: Consulenza tecnica in una procura italiana - I

- Antefatto: gli organi inquirenti, Polizia giudiziaria e perito del Pubblico ministero, per altro cultore di materia giuridica* all'università, a fronte di un documento Word - **ritrovato circa due anni dopo il presunto crimine** su un personal computer di una segreteria di un ente pubblico, privo di misure di sicurezza - hanno **attribuito alla data di creazione memorizzata insieme al documento valore di prova**.

Censure:

- la data rilevata da quel tipo di registrazione è completamente **inaffidabile**
- l'attendibilità dei contenuti e la modalità di prelievo avrebbero dovuto essere molto più tempestive
- **mancanza** di garanzie derivanti dall'apposizione di una **firma digitale**, **timbro temporale (*time-stamping*)**, caratteristiche del **tipo di software** utilizzato per l'acquisizione e analisi del dato

Caso 2: Consulenza tecnica in una procura italiana - II

* “ (…) la particolarità dell’oggetto in questione – la cui completa valutazione richiederebbe talvolta conoscenze tecniche specifiche – e la continua evoluzione dei servizi informatici disponibili sul mercato non sempre rendono agevole percepire appieno alcuni aspetti rilevanti nella risposta al quesito posto...***Poiché chi scrive non è in possesso di cognizioni specifiche della materia*** che consentano di entrare approfonditamente in dette tematiche (…)”

Anno 2001

Caso 3: anni dopo…Sentenza di Garlasco

- Ricognizione del materiale (nessun accertamento tecnico) in luogo di procedure che meglio si sarebbero sposate al caso concreto quali **l’ispezione, la perquisizione, il sequestro**
- Conseguenze: **compromissione prove**
  - su 56.000 file, 39.000 erano stati acceduti
  - 1.500 file erano stati modificati
  - 500 file creati
- Alterazione del supporto informatico
- Esame dei metadati non veritiero

Caso 4 - Processo penale per diffusione di virus

Caso*Vierika*, giudice monocratico, Bologna, 2004 :

- **sequestro** del materiale detenuto dal provider effettuato, **per delega**, da tecnici del provider (pagine web e file di log)
- **indagini** e copie di file sul computer sequestrato effettuate con **software dell'indagato** (privo di licenza) sul computer dell'indagato
- competenze dichiarate (senza ironia) da personale inquirente: **"ho l'ECDL"**

Tendenze in atto fino al 2007-2008 (?) - I

Attualmente nei processi è molto frequente che il Pubblico Ministero chieda che **vengano considerate "prove"**:

- log di server inviati via fax dal provider
- stampe di *homepage*, sessioni di *chat*, *e-mail* senza firma digitale
- contenuti di supporti di memorizzazione utilizzati dagli accertatori prima di apporre i sigilli
- contenuti di supporti sequestrati senza i dovuti sigilli
- "perizie" d'ufficio predisposte da "consulenti" privi di formazione specifica nel settore della *digital evidence* e, in qualche caso, nemmeno laureati o laureati in materie non tecniche
- relazioni di servizio sui contenuti di un sito remoto predisposte da agenti e ufficiali di polizia giudiziaria privi di competenze specifiche, es. ECDL
- identificazione di un soggetto solo tramite *user-id* e intestazione della eventuale utenza telefonica impiegata per il collegamento alla rete

(Andrea Monti)

Tendenze in atto fino al 2007-2008 - II

L'ingresso della **prova scientifica** nel processo ha sempre rappresentato motivo di accesi dibattiti a livello dottrinale e processuale: si pensi ad esempio al test del DNA soggetta a un lungo periodo di stretta "osservazione" e di analisi critica da parte di illustri scienziati

È importante sottolineare come, stranamente, questo non accada per la cd ***digital evidence***, che entra nei processi dalla porta principale come se fosse già uno strumento consolidato

Questo atteggiamento di totale fiducia da parte degli inquirenti e dei giudicanti, si risolve di fatto in un **atteggiamento di superficialità** che deve portare necessariamente ad un ripensamento

Prova scientifica « *nuova* »

- Strumenti tecnico scientifici ad elevata specializzazione non oggetto di una condivisa e consolidata esperienza nell'uso giudiziario devono essere al centro di analisi
- due aspetti devono **trovare un punto di sutura**:
  - epistemologia scientifica e giudiziaria
  - congegni procedurali a trasfonderla nella ricostruzione processuale di un fatto

in quanto «*le tradizionali categorie concettuali sedimentatesi con gli studi e gli enunciati giurisprudenziali sugli istituti della perizia e della consulenza tecnica sono in grado di dare* ***apporti di assai scarso rilievo*** »

(Dominoni O., *La prova penale scientifica*, Giuffrè, 2005)

Tecniche investigative

Le tecniche d'indagine possono essere suddivise in

- **Tecniche sotto copertura**: intercettazioni, appostamenti e sorveglianza ambientale, solitamente impiegate nelle prime fasi delle investigazioni per la raccolta di informazioni e di evidenze o nell'ambito di attività dirette alla prevenzione
- **Tecniche coercitive**, come perquisizioni e sequestri, utilizzate soprattutto per raccogliere elementi di prova una volta identificate le risorse TIC interessate

Entrambe sono coinvolte nella **lotta al cybercrimine**

Informatica forense - I

- *Digital forensics, forensic computing, cyber-forensics* sono basate sulla intangibile e spesso volatile **natura dei dati digitali**, specialmente in ambienti di rete o nella *live forensics*
- Processo di applicazione di tecniche scientifiche e analitiche alle reti di computer, a dispositivi digitali e ai *file* per scoprire o recuperare evidenze ammissibili nel procedimento penale
- La tecnologia rende il processo d'investigazione e raccolta dei dati a fini probatori estremamente **vulnerabile** per i diritti delle parti interessate (in particolare la difesa tecnica) e soggetto al rischio di malfunzionamenti tecnici, danneggiamenti o contraffazioni.
- La **carenza di preparazione** adeguata inasprisce queste difficoltà
- La **pratica operativa** si è sviluppata in seguito ai diversi scenari offerti dai casi concreti anche in maniera casuale e tramite espedienti

Informatica forense - II

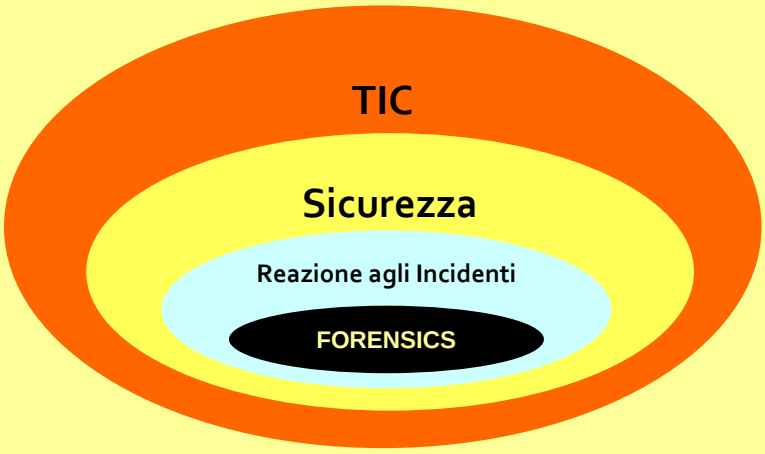
- Riguarda lo studio dei processi tesi all'identificazione, estrazione, documentazione, conservazione e interpretazione di sistemi digitali all'interno dei quali possono essere custodite evidenze o elementi di prova

- **Tipologie:**
  - Disk Forensics
  - Network Forensics
  - Email Forensics
  - Image Forensics
  - Internet Forensics
  - Portable Device Forensics (e.g. flash cards, PDAs, Blackberries, email, pagers, cell phones, IM devices)

- L'insieme dei processi e delle tecniche utilizzate vengono definite "pratiche migliori" (***best practice***).

- **Informatica Forense non vuol dire sicurezza informatica**

Contesto



Fasi principali

- **Acquisizione**
  - Disponibilità fisica o con strumenti da remoto di computer, dati di log e di traffico e dispositivi esterni di memorizzazione
- **Identificazione**
  - Scelta dei dati che possono essere recuperati e ritrovati elettronicamente tramite l'utilizzo di strumenti e suite di Informatica Forense
- **Valutazione**
  - Valutazione delle informazioni e dei dati che sono stati recuperati al fine di comprenderli, classificarli e determinazione se e come possano essere utilizzati per l'incriminazione o il proscioglimento dell'indagato
- **Presentazione**
  - Raccolta e descrizione degli elementi scoperti in un linguaggio e modo comprensibile a giuristi, personale non tecnico, e considerabile come elemento di prova secondo le leggi in vigore

Evidenze elettroniche

- Electronic (digital) evidence is **information generated, stored or transmitted using electronic devices** that may be relied upon in court *(IOCE, 2000)*
- **Qualsiasi informazione, con valore probatorio, che sia memorizzata o trasmessa in formato digitale** *(SWGDE, 1998)*
- A livello legislativo **non esiste una definizione** di prova elettronica o prova digitale in alcuno Stato europeo *(AEEC, 2006)*

Evidenze digitali

- L'aspetto caratteristico dei reperti virtuali delle evidenze è dato dalla **volatilità**, dalle **infinite possibilità di riproduzione** mediante procedure rapide e con assoluta rapidità, dalla **necessaria interpretazione** ai fini intellegibili
- Le **alterazioni** possono intervenire per cause legate alle **attività ordinarie del computer** o da un **uso incauto degli operatori**: è difficile determinare quali siano i cambiamenti effettuati con la conseguente impossibilità di ristabilire la situazione *ex-ante*
- L'esame di evidenze digitali può richiedere molto tempo; quindi chi effettua le indagini è di solito **accurato e cauto** quando raccoglie gli elementi di prova. Solitamente una copia primitiva, 'originale', intatta è prodotta per il successivo esame e i dispositivi sono restituiti alle loro applicazioni

Problema dell'identità (*identity*)

- Stabilire un collegamento forense adeguato tra **elemento informativo** e **identità virtuale** di una persona
- Stabilire un collegamento forense adeguato tra **identità virtuale** e **persona reale**

Problema della locazione (*location*)

- Identificare la **localizzazione fisica** di un sospettato
- Considerare le **implicazioni giurisdizionali** legate alla transnazionalità del fenomeno
- **Distinguere tra dati statici e dati in transito**: la corretta distinzione legale tra la perquisizione di un sistema informatico, il sequestro di dati in esso memorizzati, e l'intercettazione di dati nel corso della trasmissione permette di delinearne i confini e chiarire la portata applicativa delle norme di riferimento

Problema dell'integrità (*integrity*)

- Il **processo di acquisizione** dei dati forensi è una sfida tecnica significativa per chi effettua le indagini considerato l'alto **rischio di modificabilità** degli originali e dei metadati minando *ab origine* il valore probatorio del materiale acquisito (ad esempio data e ora)
- Le modalità con cui tali operazioni vengono condotte creano ulteriori problemi rappresentati dalla **mancanza di procedure uniformi** e dal **diverso trattamento** delle *digital evidence* da parte delle legislazioni

Problema della viscosità (*stickiness)*

- **Molte copie** degli stessi file sono generate durante i processi di trasmissione
- Le modalità con cui i dati sono mantenuti o rimossi dai dispostivi elettronici e magnetici di memorizzazione
- In generale la viscosità dei dati è un elemento a **favore degli investigatori**
- Viceversa, la percezione che i dati provenienti da fonti TIC siano soggetti al rischio di alterazione può essere di aiuto per l'accusato, laddove possano essere sollevati dubbi sull'esistenza stessa e/o il loro **valore forense**

Problema del tipo di dati (*data type*)

- Gli **elementi di prova digitale** comprendono:
  - il contenuto di una trasmissione
  - gli attributi o metadati dell'attività di comunicazione
  - il diritto alla privacy degli utenti delle reti
  - la gestione di una risorsa informatica
- **La fonte** di base di qualsiasi informazione digitale è data dalla sua rappresentazione attraverso la **codifica binaria**
- Le leggi trattano i differenti tipi di dati forensi in maniera diversa (ad es. intercettazioni, dati di traffico):a ciò consegue un diverso regime giuridico di trattamento

Problema della tracciabilità (*traceability*)

- **Fonti molteplici**
  - dati che l' indagato ha utilizzato o a lui riconducibili a seguito della sua attività
  - dati creati a seguito dell'utilizzo di un sistema di comunicazione da parte di un sospettato
  - i contenuti delle attività di comunicazione di una persona
- **Identificazione della fonte e della destinazione** facendo riferimento a identificazioni univoche
- Se il dispositivo si trova in un ambiente promiscuo dove può essere utilizzato da più persone, risulta problematico verificare quale sia concretamente la persona fisica che abbia **utilizzato quel dispositivo** o **avuto accesso** tramite credenziali di riconoscimento a un orario determinato

Esempio: risoluzione di un indirizzo IP

- Chi effettua l'indagine può risolvere un indirizzo IP di un utente mediante:
  1. Identificazione dell'indirizzo IP (da log; ma può essere anonimizzato)
  2. Individuazione del *Service Provider* per l'accesso in archivi di registri autorizzati (da registri; ma la gestione dei dati può essere inaccurata)
  3. Contatto del titolare dell'indirizzo IP; problemi con indirizzi dinamici, luoghi pubblici, reti wireless insicure
  4. Acquisizione dei dati personali
- L'abilità di risalire da un indirizzo IP **al soggetto che concretamente pone in essere la navigazione** dipendente da input che provengono da più entità e dall'esistenza di vari log e/o registrazioni
- Importante sul punto è la disciplina in tema **di conservazione dei dati** da parte dei *Service Provider*(***data retention***)

Esempio: temi di network forensics

- La crescita della criminalità informatica che si basa su reti ha sollevato alcune questioni nuove e difficili date **dalla necessità di bilanciamento** fra:
  - Esigenze repressive e d'indagine da parte delle forze dell'ordine
  - Il diritto alla privacy degli utilizzatori delle reti
- Gli interessi dei ***Communication Service Provider*** nelle ipotesi di obblighi di collaborazione con le autorità in termini di :
  - raccolta dei dati trasmessi dagli indagati
  - cessione dei dati generati da attività di sospettati o indagati sui *Service Provider*
  - tutela degli stessi circa il *privilege against self-incrimination*
- La **provenienza** e la **raccolta** di dati forensi avviene da:
  - dati provenienti dal sospettato, ottenuti con modalità di copertura, attraverso varie modalità di ispezione
  - dati ottenuti da un *Communication Service Provider*
  - dati provenienti dal sospettato, ottenuti con modalità coercitive, attraverso operazioni di perquisizione e sequestro

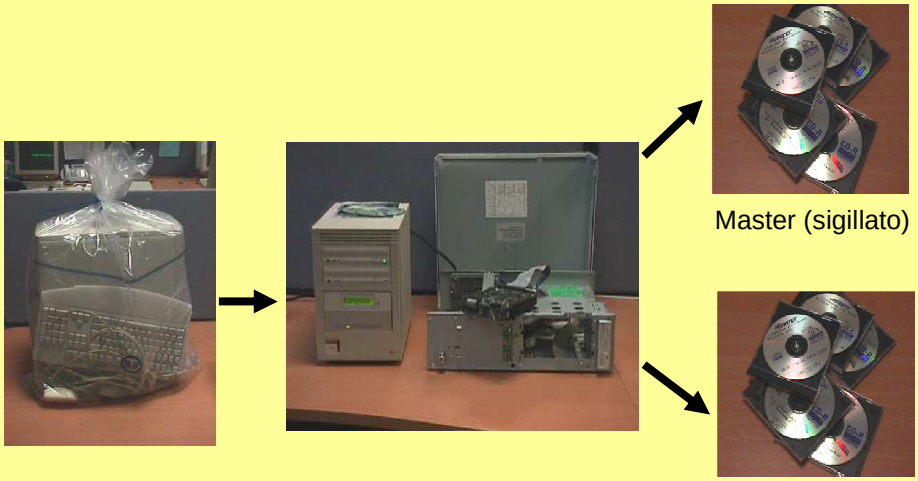
Problema dell'analisi (*analysis*)

- Il volume e la natura dei dati che devono essere trattati durante le indagini può essere proibitivo
- I supporti di memorizzazione sono in grado di contenere enormi **quantità di dati** e i sistemi di comunicazione di trasmettere **smisurati flussi di bit** (bit-stream di dati)
- Ottenere e memorizzare questi dati è di norma facile e diretto
- L'abilità di accedere, gestire e analizzare i dati e la successiva **presentazione dei risultati in tribunale** presenta problemi legati a meccanismi di protezione, rispetto dei limiti di spesa e di tempo richiesti dalla legge

Imaging - I

- Per risolvere il problema dell'integrità chi effettua le indagini deve poter ottenere i dati in modo **completo** con **interferenze minime** sui dati originali sotto esame
- Tali dati possono essere stampati e copiati, anche se questo porta a variazioni nei meta-dati associati, con la possibilità di creare vulnerabilità
- Pertanto la **tecnica più utilizzata** per ottenere dati forense è quella dell'**imaging**
- Una immagine bit-stream di un dispositivo di memorizzazione digitale, ad es. hard disk o smart card, viene acquisita e creata in modo non invasivo includendovi le parti non occupate da dati di interesse

Processo di creazione dell'immagine dei file



Master (sigillato)

Copia di lavoro

Ian Pomfret, *Computer Forensics, British Telecom, 2001*

Imaging - II

- Il processo genera alcuni dati, come la **funzione hash di crittazione,** che possono essere richiesti successivamente per verificare **l'autenticità** e l' **integrità** dei dati dopo il processo di acquisizione e la generazione di successive copie
- Vengono generate più copie: una master e alcune di lavoro per tutte le parti processuali coinvolte
- Imaging consente di **restituire i dispostivi originali** al proprietario che così può continuare nel suo lavoro su quella risorsa
- Le immagini sono ampiamente accettate nei tribunali **come rappresentazioni** dei **dispostivi originali**

Esempio: digest e hash function - I

- Il **digest** di un file (che è una successione di bit) è una stringa di simboli di **lunghezza predefinita** generata dalla applicazione di una **funzione di hash** sul file stesso
- DPCM 8 febbraio 1999: *"l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash"*
- Non è possibile dal digest risalire a testo originale
- Collisioni dello **stesso valore** del digest da due **fonti diverse è impossibile**

Esempio: digest e hash function - II

D'accordo
efcc61c1c03db8d8ea8569545c073c814a0ed755
Sono nato a Ravenna
fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25
<questa presentazione>
0e6d7d56c4520756f59235b6ae981cdb5f9820a0
Sono un professore
ea0ae29b3b2c20fc018aaca45c3746a057b893e7
Sono un professore.
01f1d8abd9c2e6130870842055d97d315dff1ea3

- Stessa Lunghezza: 40 digit (160 bit - 8 byte)
- Valori dipendenti dal contenuto del documento

Volume dei dati

La torre è alta 190 metri.

La stampa dei contenuti di **6 Giga byte** genera una pila più alta della torre !

Un libro di 300 pagine occupa circa 650 Kilo Byte

10 Giga byte contengono circa 15.250 libri

Ian Pomfret, *Computer Forensics, British Telecom, 2001*

Capienza dei supporti

- I **tempi medi di copia** sono di circa due gigabyte al minuto: si impiegano quindi circa otto ore a effettuare una copia bit-stream di un hard disk della capienza di un terabyte

Da una perizia:

"(…)Le attività che il perito e i suoi collaboratori, a partire dalle 16.35, svolgono relativamente al collo 2 sono le seguenti:
✓si predispongono le apparecchiature e si rendono disponibili hd1 e hd2;
✓si **calcola l'impronta md5** del collo 2 alle ore 17.05;
✓si **copia il contenuto** dell'hard disk del collo 2 su hd1 dalle 17.15 alle 17.33 (vedasi foto 48, 49);
✓si **verifica l'impronta md5** alle 17.47;
✓si copia il contenuto dell'hard disk del collo 2 su hd2 dalle 17.50 alle 18.07;
✓si verifica l'impronta md5 alle 18.14.

L'impronta md5 del collo 2 è 491b392e2a9ce11cf60e35016fd80d8c (…)"

Complessità computazionale: Tea Party o dei matrimoni stabili

Problema: far sedere gli ospiti a una tavola rotonda, in modo che ciascuno abbia ai suoi lati una persona che gradisce

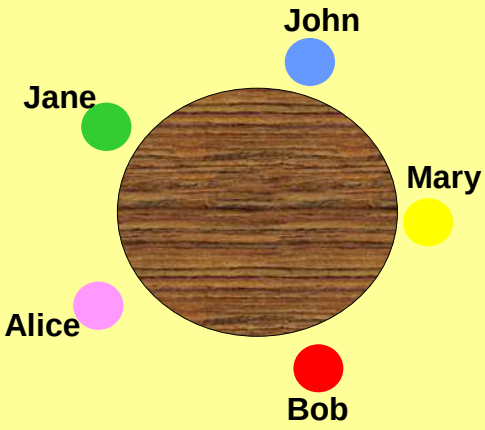
Tabella delle preferenze:

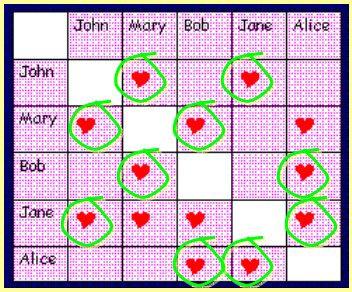
	John	Mary	Bob	Jane	Alice
John		♥		♥	
Mary	♥		♥		♥
Bob		♥			♥
Jane	♥	♥	♥		♥
Alice			♥	♥	

Dana .Moshkovitz

Complessità computazionale- II

Una soluzione





Complessità computazionale- III

Per ogni ordinamento degli ospiti attorno alla tavola, occorre verificare il gradimento di ciascuno di essi per i vicini

Quanto tempo è necessario? (caso peggiore)

Ospiti	Passi
n	(n-1)!
5	24
15	87178291200
100	$\approx 9 \cdot 10^{155}$

un computer capace di eseguire 10^{10} istruzioni per secondo, impiegherà circa $3 \cdot 10^{138}$ anni

Dispositivi di memorizzazione

- La memorizzazione nei dispositivi digitali avviene a **diversi livelli**:
  - **livello fisico**, come le particelle magnetiche e le incisioni creati dal laser
  - **livello logico**, in termini di partizioni, dispositivi, tracce e settori
- Le modalità con cui un dispositivo gestisce i dati a livello logico ha implicazioni dirette su qualunque analisi forense
- I **diversi *file system*** utilizzano lo spazio sui dispositivi di memorizzazione in maniera dissimile l'uno dall'altro; servono dunque tecniche di analisi diverse per esaminare i dati memorizzati da essi
- Nei diversi *file system* i dati non sono necessariamente memorizzati in posizioni continue ma sono **frammentati** su più dispositivi, in blocchi che sono logicamente associati tra loro tramite informazioni di indirizzamento

Esempio: dati che nessuno crea intenzionalmente

- File temporanei
- Dati in memorie virtuali e file di swap
- History file dei browser
- History file in Internet
- File temporanei nelle reti telematiche
- Link di collegamento
- File di log
- Metadata
- File di informazioni
- Web based emails

Identificazione e organizzazione dei dati operativi

- Il **software di sistema** e quello applicativo utilizzano il file system per identificare e organizzare i dati su cui operano, in termini di nome dei file, estensioni, cartelle e directory
- Tali informazioni spesso contengono un'ampia varietà di dettagli di interesse forense sugli **attributi dei file**, ad es. grandezza e utilizzo
- I dati di utilizzo, come l'orario e il tipo di operazione che è stata eseguita su un insieme di dati, è una fonte forense di valore ma è altresì molto vulnerabile ad accuse di inaccuratezza, modifiche e interferenze
- Occorre quindi qualche dato corroborante da fonte diversa (ad es. la data memorizzata su una fotografia digitale)

Cancellazione dei dati

- La cancellazione di dati dai supporti digitali può presentarsi in forme diverse:
  - Se effettuata da una **applicazione standard** rimuove solamente l'indirizzo dell'informazione associata a ogni blocco di dati, che logicamente connette i vari blocchi che costituiscono i contenuti dei *file*
  - I *file* che sono cancellati vengono rinominati in un'altra *directory* (ad es. Cestino, *unused space*)
- I dati **rimangono sul supporto**, e **sono recuperabili parzialmente**, fintanto che non siano completamente sovra-scritti da nuovi dati o cancellati tramite appositi strumenti (e.g. software di *wiping*)
- La rappresentazione fisica residua dei dati cancellati viene detta **permanenza dei dati**, ed è una delle cause del **problema della viscosità**

Strumenti software per l'analisi forense

- **Encase** di Guidance Software

- **Forensic Tool Kit** di Access Data Group
- ILook di Perlustro
- Live View di Carnegie Mellon University
- SMART di ASR Data
- Maresware di Mares & Associates
- DataLifter di StepaNet Communications

- Helix di E-fence
- **DEFT**
- CAINE

Tool kit

Due famiglie di strumenti per acquisizione e analisi:

- **Stazioni di lavoro** per l'informatica forense:
  - sistemi integrati hardware e software che raccolgono, copiano e analizzano i dati

- **Sistemi** che eseguono alcune **funzioni specializzate**:
  - software di visualizzazione di file testo nei vari formati
  - software di visualizzazione di file immagini nei vari formati
  - programmi tradizionali che esaminano singolarmente i settori di un disco senza alterarli
  - programmi che consentono di ricercare parti di testo in enormi archivi dove sono memorizzati file in vari formati
  - programmi che consentono di avere copia dell'immagine intera dei contenuti di un disco

Funzionalità dei tool kit

- possibilità di eseguire **ricerca veloce** sull'intero supporto magnetico (non solo all'interno dei *file,* ma anche sulla superficie non utilizzata dei dischi)
- possibilità di produrre copie dei dischi a basso livello **(copia settore per settore)**
- utilizzabilità su più **tipi di *file system***
- possibilità di combinare in modi diversi i risultati delle ricerche eseguite
- analisi dei dati secondo varie **modalità di codifica** (per esempio ASCII ed esadecimale)
- recupero automatico di eventuali **file apparentemente cancellati**
- stampa e riproduzione, previa scelta dei parametri, delle prove

Esempio: raccolta di evidenze

- Eseguire **copie esatte** di tutti i dispositivi e dischi che utilizzano il software
  - Data e ora riportate da ogni file; utilizzabile per la time-line
- **Proteggere il sistema** di eleborazione
  - ✓ Evitare la cancellazione, danneggiamento, virus e corruzione
- **Ritrovare i file**
  - ✓ File normali
  - ✓ File protetti
  - ✓ File nascosti
  - ✓ File crittati
- Reperire tutti i contenuti dei **file nascosti** usati dal sistema operativo e dalle applicazioni
- Accedere ai contenuti dei **file protetti** se si ha l'autorizzazione legale per farlo
- Analizzare i dati
- Utilizzare la consultazione di esperti e di testimoni
- **Stampare** l'analisi di
- ✓ Sistema di elaborazione
- ✓ Tutti I file e dati
- ✓ Valutazioni complessive

Validazione della prova digitale

***Iter* di formazione:**

- **Perquisizione** da parte dell'autorità procedente
- Rispetto della **catena di custodia**
- **Validazione** del dato digitale mediante **funzione di hash**
- **Validazione** degli **strumenti software** impiegati
- **Analisi** del dato digitale
- Cura della **ripetibilità**; garanzia di qualità
- Redazione di un **rapporto coi risultati** dell'indagine
- **Relazione tecnica** e sua illustrazione eventuale

Pratiche migliori per la gestione del reperto informatico

Prossimità dei reperti (***proximity***): vanno raccolti nel tempo più prossimo all'accadere di un evento di interesse

Congelamento (***freezing***) **delle memorie di massa** e di ogni dispositivo di memorizzazione: i contenuti dei dispositivi non devono essere alterati o inquinati

Catena di custodia (*chain of custody*): deve essere garantita la corretta ed ininterrotta continuità nella gestione e custodia del reperto, dal momento in cui viene sequestrato al momento in cui viene prodotto in giudizio

Controllabilità e ripetibilità (*accountability*) di tutte le operazioni compiute sul reperto: consulenti e periti devono essere in grado, leggendo i documenti, di ripetere tutte le operazioni compiute sui reperti

Risultati delle pratiche migliori

- Creazione di una ***bit-stream image***:
  "Congelare" il contenuto del supporto calcolandone il digest (impronta matematica) con un programma di hashing
  Eseguire più di una copia integrale, bit per bit, del supporto su un altro dispositivo di memorizzazione
- Eventuale **dissequestro dei supporti** (diritto di terzi)
- Rispetto ***chain of custody***
- Copie per la difesa e le altre parti del processuali (**diritto di difesa**)
- Copie di riserva

Time-Line

- La capacità di far **corrispondere** gli **eventi temporali** memorizzati dai vari dispositivi da cui si sono ricavati i dati all'orario preciso della loro effettuazione è un elemento critico nelle indagini forensi
- Occorre quindi stabilire **un'accurata cronologia degli eventi** connessi a un'indagine
- Nel caso di reti, le varie componenti registrano gli orari degli eventi; tuttavia la molteplicità delle fonti connessa a possibili inaccuratezze locali rende complicata la ricostruzione
- Il problema è reso più critico dal **contesto transnazionale e dai diversi fusi orari**

Esempio: catena di custodia

- **Identifica** i soggetti che hanno in custodia i reperti digitali
- Consente la conoscenza della **continuità della custodia**
- Prova **l'integrità della gestione** dei reperti raccolti

1. Data e ora del sequestro
2. Luogo e persone da cui si è prelevato
3. Fabbricazione, modello e numero di serie
4. Nome delle persone che hanno raccolto il reperto
5. Descrizione del reperto
6. Nome e firma delle persone che ricevono i reperti
7. Numerazione e classificazione interna del reperto
8. Valori del digest
9. Dati tecnici pertinenti

Tendenze attuali - I

- **Crescita delle indagini su violazioni;** chi effettua gli attacchi è in una posizione sempre più avvantaggiata rispetto a chi mantiene i dati. (es. *malware* di insediamento in sistemi)
- **Modesta preparazione delle forze che indagano;** messa in evidenza anche dalla produzione legislativa
- **Necessità di qualificazione tecnica e giuridica** nel settore specifico delle indagini informatiche
- **Crescita della *e-discovery*,** cioè delle applicazioni in campo del diritto civile**;** elementi di prova nei procedimenti civili, autenticità dei documenti informatici, riduzione di costi

Tendenze attuali - II

- **Troppi dati da analizzare con l'informatica forense;** raccolta selezionata delle informazioni necessarie
- **Mobile Device Forensics e cloud computing;** necessità di robusti metodi di acquisizione e di analisi per cellulari, iPod, PDA; format e accessi non tradizionali
- **Criticità della raccolta e analisi di di dati volatili;** la acquisizione di dati volatili aiuta ad affrontare nuove sfide come la crittografia e la acquisizione di elementi di prova che possono esistere solo per pochi istanti

Iniziative di armonizzazione

Dimensione internazionale del fenomeno: necessità di strumenti condivisi sul piano della protezione

- G8 adottò nel 1999 un insieme di **principi sull'accesso transnazionale a dati memorizzati** e dopo l'11 settembre 2001 adottò una Raccomandazione sul crimine transnazionale su alcuni tipi di reati informatici
- OECD nel 1986 produsse uno studio che presentava le **categorie di reati** che riteneva dovessero costituire una base per i futuri **Cybercrime**
- La Nazioni Unite hanno sempre seguito il contrasto a reati informatici per mezzo di loro agenzie come ITU e Unicef; in due occasioni l'Assemblea Generale ha espresso risoluzioni sui reati informatici: nel 1990 e nel 2001 produsse raccomandazioni relative alla eliminazione di ripari sicuri per incrementare la **cooperazioni fra agenzie investigative internazionali**
- Il Consiglio di Europa nel 1989 stilò il primo elenco di reati informatici per le legislature nazionali su cui intraprendere una azione uniforme di contrasto;nel 2001 ha prodotto la **Convenzione sul Cybercrime** anche con la collaborazione di Stati Uniti, Canada, Giappone e altre nazioni non facenti parte dell'Unione Europea

Convenzione sul Cybercrime

***Ratio* dell'Accordo**:

- Armonizzazione del **diritto penale sostanziale** nell'ottica del *cybercrime*
- Potenziamento delle **procedure processuali** necessarie per l'investigazione e la repressione dei reati commessi tramite sistemi di elaborazione e per la **valorizzazione delle prove informatiche**
- Impostazione di un efficace ed efficiente **sistema di cooperazione internazionale**

Capitoli

1. Utilizzo dei termini
2. Misure da adottare a livello nazionale - profili giuridici sostanziali e procedurali
3. Cooperazione internazionale
4. Clausole finali

Ratifica della Convenzione

- Una volta ratificata, numerosi Paesi europei (e.g. Belgio, Germania, Italia, Spagna) hanno inserito i reati informatici nelle **norme** del proprio **Codice Penale**
- Altri Stati hanno inserito i crimini informatici in leggi apposite come **"Computer Crime Act"**. Si tratta, per esempio, di Cipro, India, Sri Lanka, Regno Unito, Romania e Portogallo
- Entrambi gli approcci sono ritenuti **adeguati per implementare completamente la Convenzione**; tuttavia vi è un vasto accordo che gli Stati del primo gruppo si trovino ad affrontare un maggior numero di problemi per collegare le disposizioni alle norme tradizionali (ad es. frode, contraffazione, intercettazioni illegali)

La Convenzione: diritto sostanziale

Sono **definiti** i seguenti reati: accesso illegale a un sistema informatico , intercettazione illegale, attentato all'integrità dei dati, abuso di apparecchiature informatiche, falso informatico, reati connessi alla pornografia minorile e alla violazione del diritto d'autore

Nel **capitolo II**, Sezione I Diritto penale sostanziale:

- Titolo I fa riferimento **a reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici** e copre, in base agli articoli da 2 a 6: l'accesso illegale ad un sistema informatico; l'intercettazione abusiva; l'attentato all'integrità dei dati (cioè il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione); l'attentato all'integrità di sistema; l'abuso di apparecchiature
- Titolo II si occupa di **reati informatici**, con l'articolo 7 che tipizza il falso informatico e con l'articolo 8 che definisce il reato di frode informatica
- Titolo III si occu73pa di **reati relativi ai contenuti** e definisce i reati relativi alla pornografia infantile
- Titolo IV si occupa di **reati contro la proprietà intellettuale** nell'articolo 10

Legge n. 48 del 2008

Ratifica della Convenzione Cybercrime

- **modifica alcuni dei reati informatici** contenuti nel codice penale (e.g. "diffusione di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico o telematico" di cui all'art. 615quinquies c.p.)
- **introduce nuovi reati** (e.g. "falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri" di cui all'art. 495bis c.p.)
- **modifica il c.p.p. recependo modalità di indagini e di analisi dall'Informatica Forense**

Riferimenti

- Brenner S., *Cybercrime: criminal threats from cyberspace,* Praeger, 2010
- Casey E. (ed.), *Handbook of computer crime investigation: forensic tools and technology*, Academic Press, 2007
- Clough J., *Principles of cybercrime,* Cambridge University Press, 2010
- Lloyd I., *Information technology law*, Oxford University Press, 2011
- Vaciago G*. Digital evidence*, Giappichelli, 2012
- Wall D. S. (ed.), *Crime and deviance in cyberspace*, Aldershot, 2009
- Walden I., *Computer crimes and digital investigations*, Oxford University Press, 2007

http://www.cirsfid.unibo.it/CIRSFID/Centro/AreeDisciplinari/Informatica_Forense.htm