Ruolo e prospettive dell'informatica forense

Michele Ferrazzano

michele.ferrazzano@unibo.it

Agenda

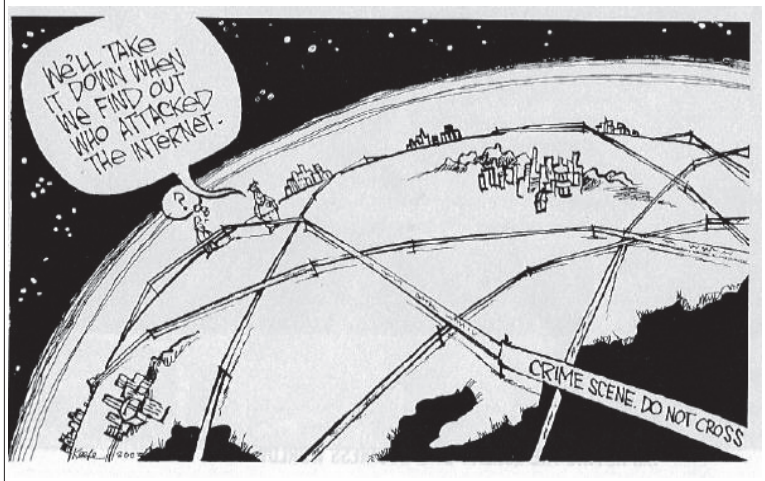
- In che mondo viviamo?
- Definizioni
- Problematiche operative
- Tendenze
- Prospettive

Utenti Internet nel mondo
agg. 30 giugno 2012

Aree geografiche	Popolazione mondiale (2012)	Utenti Internet (2000)	Utenti Internet (2012)	Diffusione	Incremento 2000-2012	Rapporti tra aree geografiche
Africa	1,073,380,925	4,514,400	**167,335,676**	15.6 %	3,606.7 %	7.0 %
Asia	3,922,066,987	114,304,000	**1,076,681,059**	27.5 %	841.9 %	44.8 %
Europa	820,918,446	105,096,093	**518,512,109**	63.2 %	393.4 %	21.5 %
Medio Oriente	223,608,203	3,284,800	**90,000,455**	40.2 %	2,639.9 %	3.7 %
Nord America	348,280,154	108,096,800	**273,785,413**	78.6 %	153.3 %	11.4 %
Sud e centro America	593,688,638	18,068,919	**254,915,745**	42.9 %	1,310.8 %	10.6 %
Oceania	35,903,569	7,620,480	**24,287,919**	67.6 %	218.7 %	1.0 %
TOTALE	**7,017,846,922**	**360,985,492**	**2,405,518,376**	**34.3 %**	**566.4 %**	**100.0 %**

http://www.internetworldstats.com/stats.htm

Problema: il cyberspazio non ha frontiere



Problema: il cyberspazio non ha frontiere

- 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

Problema: il cyberspazio non ha frontiere

- Dimensione internazionale del fenomeno
  - 1989 - Consiglio d'Europa: primo elenco di reati informatici per le legislature nazionali su cui intraprendere una azione uniforme di contrasto
  - 1999 - G8: principi sull'accesso transnazionale a dati memorizzati
    - Dopo l'11 settembre 2001 adottò una Raccomandazione sul crimine transnazionale su alcuni tipi di reati informatici
  - 2001 - Consiglio d'Europa: Convenzione sul Cybercrime
    - Paesi europei e altri non facenti parte dell'UE (USA, Canada, Giappone…)

Problema: il cyberspazio non ha frontiere Convenzione sul Cybercrime

- Budapest, 23 novembre 2001
  - *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185*
- 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

Problema: il cyberspazio non ha frontiere Convenzione sul Cybercrime: ratifica

- Alcuni Paesi europei (Belgio, Germania, Italia, Spagna) hanno inserito i reati informatici nelle norme del proprio Codice Penale
- Altri Stati (Cipro, India, Sri Lanka, Regno Unito, Romania e Portogallo) hanno inserito i crimini informatici in leggi apposite come "Computer Crime Act"
- Entrambi gli approcci sono ritenuti adeguati per implementare completamente la Convenzione

Reati che coinvolgono le Tecnologie dell'Informazione e della Comunicazione *(alcuni esempi)*

- 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

Reati che coinvolgono le Tecnologie dell'Informazione e della Comunicazione

- Reati di danneggiamento volti a danneggiare l'integrità delle componenti tecnologiche dei sistemi TIC
  - Es.: danneggiamento informatico, distribuzione di virus
- Reati tradizionali o comuni in cui il computer assume la qualità di strumento del reato o di strumento per facilitare la distribuzione di materiali illeciti
  - Es.: frodi, falsificazioni, violazioni dei diritti d'autore, la pornografia minorile
- Reati non informatici. Alcuni dati utili alle indagini sono contenuti in dispositivi digitali
  - Es.: omicidio, stupro

Trattamento di dati informatici a fini processuali

- Il ricorso all'Informatica Forense può rendersi necessario nei procedimenti aventi ad oggetto:
  - Reati informatici propriamente detti
  - Reati commessi con l'impiego di sistemi informatici
  - Strumenti di archiviazione di dati rilevanti

Comune denominatore

DATO DIGITALIZZATO COME OGGETTO DI INDAGINE

Reati che coinvolgono le TIC - Norme di riferimento

- Legge 23 dicembre 1993, n. 547
  - Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica
- Legge 18 marzo 2008, n. 48
  - Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Problema: il cyberspazio non ha frontiere Convenzione sul Cybercrime: ratifica

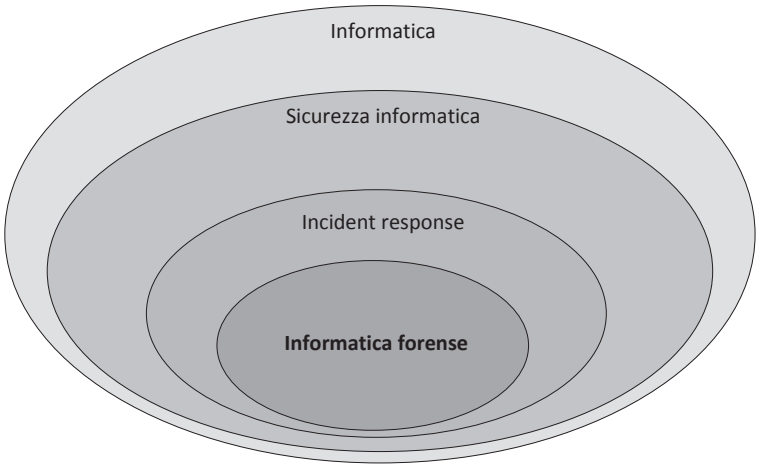
- Legge 48/2008
  - Modifica alcuni dei reati informatici contenuti nel codice penale ("diffusione di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico o telematico" di cui all'art. 615quinquies c.p.)
  - Introduce nuovi reati ("falsa dichiarazione o 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
  - Alcune imprecisioni e refusi (dati *vs.* informazioni, pacco trasmesso per via telmatica…)

Definizioni

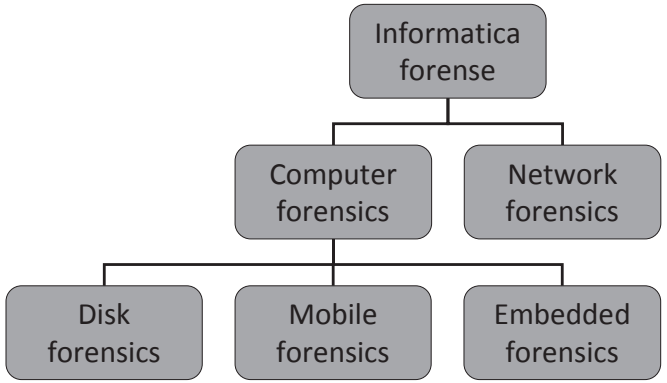
Informatica forense

- **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**

Informatica forense *vs.* Sicurezza informatica



Informatica forense
Classificazione



Informatica forense
Fasi principali

- **Identificazione**
  - Ricerca del luogo in cui si presume sia memorizzato il dato informatico di interesse
- **Acquisizione e conservazione**
  - Disponibilità fisica o con strumenti da remoto di computer, dati di log e di traffico e dispositivi esterni di memorizzazione
- **Analisi**
  - 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

Informatica forense

Componente tecnica

Componente giuridica

Informatica forense
Competenze parte tecnica

- Procedimenti e strumenti tecnici e organizzativi
- Computer come macchine del tempo
- Archeologia informatica
- Metodi di duplicazione e riproduzione dei dati
- Analisi dei dischi e delle memorie; livelli di volatilità
- Analisi di dispositivi mobili; integrazione con la telefonia e con sistemi multimediali
- Sistemi operativi e file system
- Geologia informatica
- Raccolta di reperti dai dispositivi
- Protocolli di rete e analisi del traffico
- Investigazioni sulle reti
- Complementi sui casi (VoiceOverIP, Phone Forensics, elementi di steganografia, cloud computing)
- **Redazione di rapporti solidi per l'analisi giudiziaria**

Informatica forense
Competenze parte giuridica

- Terminologia
  - Prova *vs.* fonte di prova
  - Consulente tecnico *vs.* perito
- Norme rilevanti per l'informatica forense
  - La Convenzione su Cybercrime e i recepimenti nazionali

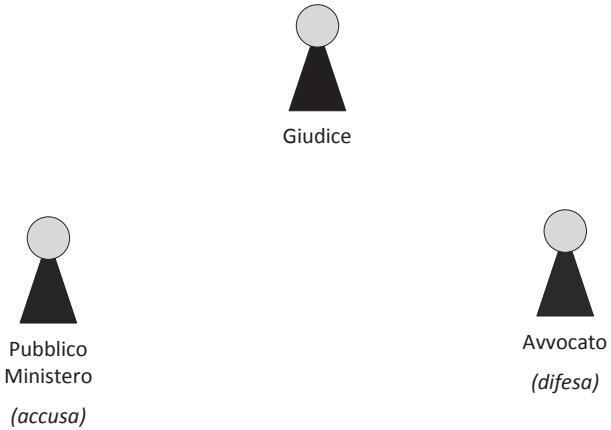
- Evoluzione tecnologica e nuove forme di criminalità
- Le esperienze internazionali e italiana di computer forensics
- Modelli processuali penali ed informatica forense
- Indagini in materia informatica
- Il problema delle indagini e della giurisdizione sovranazionale
- Consulenti e periti in materia informatica
- Casi di cronaca
- L'informatica forense per gli altri tipi di processo (e-Discovery)

Prova *vs.* fonte di prova

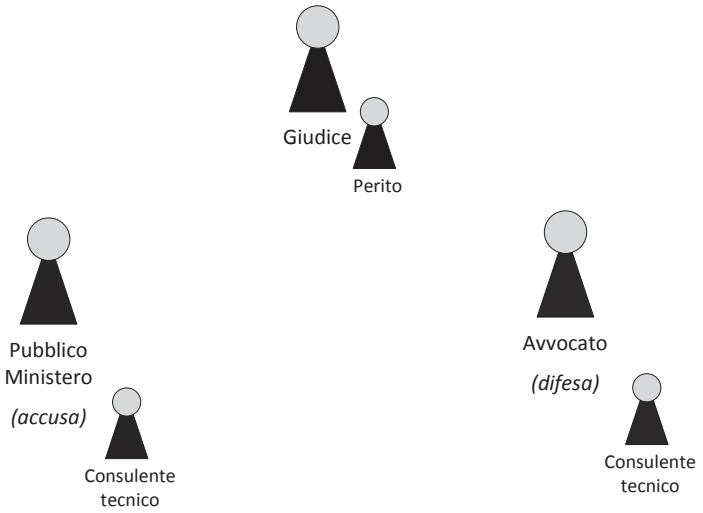
- *Qualunque strumento, metodo, persona, cosa o circostanza che possa fornire informazioni utili per risolvere l'incertezza intorno alla verità o falsità degli enunciati fattuali* (Taruffo)

- Nel diritto processuale penale più che di "prova" in senso lato si parla di "fonte di prova", consistente in "*tutto ciò che è idoneo a fornire risultati apprezzabili per la decisione del giudice*" (Tonini)

Consulente tecnico *vs.* perito



Consulente tecnico *vs.* perito



Problematiche operative

Problematiche operative
Esempio: risoluzione di un indirizzo IP

- Identificazione dell'indirizzo IP
  - Può essere "rubato", anonimizzato
- Individuazione del Service Provider per l'accesso in archivi di registri autorizzati
  - Da registri; ma la gestione dei dati può essere poco accurata
- Contatto del titolare dell'indirizzo IP
  - Problemi con indirizzi dinamici, luoghi pubblici, reti wireless insicure
- Acquisizione dei dati personali

- Importante sul punto è la disciplina in tema di conservazione dei dati (*data retention*) da parte degli ISP

Problematiche operative
Collegare il dato informatico ad una persona

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

- Stabilire un collegamento adeguato tra identità virtuale e persona reale

Problematiche operative
Identificare il luogo fisico

- 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

Problematiche operative
Integrità

- L'acquisizione è il momento critico
  - Rischio di modificare irreparabilmente i dati originali
    - Es.: alterazione dei metadati
- 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

Problematiche operative
Viscosità

- Molte copie degli stessi file sono generate durante i processi
  - "Processo" inteso come "programma sw in esecuzione"
- In generale la viscosità dei dati è un elemento a favore degli investigatori, ma se non c'è omogeneità crea problemi

Problematiche operative
Tracciabilità

- 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
  - 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

Problematiche operative
Volume dei dati (stampa)

- *"Dottore, mi stampi tutto, grazie"*
- *"Dove possono parcheggiare i TIR"*

- 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*

Problematiche operative
Volume dei dati (copia forense)

- *"Copi quel file e ce ne andiamo"*

- Tempi di copia: massimo 5 GB al minuto circa
  - 1000 TB = 200 minuti = 3 ore e mezza circa

- Tempi medi di copia: 2 GB al minuto circa
  - 1000 TB = 500 minuti = 8 ore circa

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

Tendenze

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**: perquisizioni e sequestri; utilizzate soprattutto per raccogliere elementi di prova una volta identificate le risorse TIC interessate

- Entrambe sono coinvolte nella lotta al cybercrime

Tendenze in atto fino ad alcuni anni fa *(talvolta, ancora oggi)*

- 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, soggetto a un lungo periodo di stretta "osservazione" e di analisi critica da parte di illustri scienziati
- Questo non accade per la prova digitale
  - Entra nei processi in maniera approssimativa o come se fosse già uno strumento consolidato

Tendenze in atto fino ad alcuni anni fa *(talvolta, ancora oggi)*

- Log di server inviati via fax dal provider
- Stampe di pagine web, sessioni di chat, e-mail
  - O in formato digitale, senza firma digitale
- Accesso ai dati contenuti nei supporti di memorizzazione senza opportune accortezze
- Sequestro di supporti di memorizzazione senza opportuna applicazione di sigilli
- Perizie e consulenze assegnate a persone senza opportuna qualifica
  - "ho l'ECDL"
- Collegamento diretto tra indirizzo IP e intestatario utenza telefonica

Caso Vierika

- Caso Vierika, 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 da personale inquirente:

"ho l'ECDL"

Casi di omicidio - Alibi informatici

- 2007
  - Raffaele Sollecito consegna il suo notebook per dimostrare alibi
    - Visione film
  - Alberto Stasi consegna il suo notebook per dimostrare alibi
    - Scrittura tesi

Caso Garlasco

- Ricognizione del materiale (nessun accertamento tecnico) in luogo di procedure che meglio si sarebbero sposate al caso concreto quali ispezione, perquisizione, 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

Prospettive

Prospettive

- Crescita delle indagini su violazioni; chi effettua gli attacchi è in una posizione sempre più avvantaggiata rispetto a chi mantiene i dati
- Impreparazione e scarse risorse per forze che indagano
- Necessità di qualificazione tecnica e giuridica nel settore specifico delle indagini informatiche
- Troppi dati da analizzare
- Ritardo dalla produzione legislativa

Prospettive

- 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 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
- 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