Introduzione alla Informatica Forense

Cesare Maioli
CIRSFID e Facoltà di Giurisprudenza
Università di Bologna

Treviso, 27 settembre 2013

Indice

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 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

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

Elemento comune e unificante:

il **dato digitalizzato**

come oggetto di indagine

Dati relativi a un documento

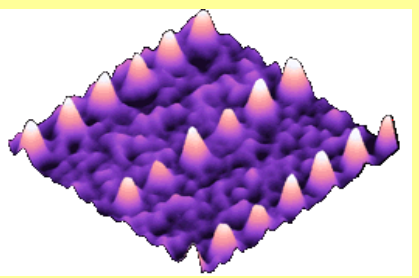
DATI INTERNI

- immagini, elaborazioni (in formato digitale)
- documenti (in formato digitale)
- dati personali (in formato digitale)
- dati sensibili (in formato digitale)
- dati quantitativi (in formato digitale)
- altre informazioni (in formato digitale)

DATI ESTERNI

- dati tecnici del sistema (in formato digitale)
- dati esterni dei file (in formato digitale)

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

Tutela dei dati

I dati sia se organizzati in documenti informatici sia come dati di sistema sono oggetto di tutela penale

- Documenti informatici (art. 491 bis c.p.)
- Falso (materiale e ideologico) in documenti informatici (da 476 al 493 bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis e ter c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o
- Interruzione di un sistema informatico o telematico (art. 615 quinquies c.p.)
- Intercettazione non autorizzata (art. 617 quater, quinquies, sexies c.p.)
- Violazioni della riservatezza dei dati personali (D. Lgs. 196/03)

7

Sistema Informatico e Telematico

(Cass. 2672 / 2006)

Complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di codificazione e decodificazione - dalla registrazione o memorizzazione, per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da ingenerare informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente

8

Tutela del sistema informatico

- Danneggiamento di sistema informatico (art. 635 quater e quinquies c.p.)
- Frode informatica (art. 640 ter c.p.)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)
- Accesso abusivo a sistema informatico (art. 615 ter c.p.)
- Abuso e commercio di codici di accesso (art. 615 quater c.p.)
- Diffusione di virus e malware (art. 615 quinquies c.p.)

9

Ratio dell'Informatica Forense

Quali sono

i principi tecnici da applicare

e le norme giuridiche da attuare

per il corretto trattamento dei dati digitali

a fini processuali ?

10

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

11

Contesto

12

Informatica forense

Tipologie:

- Disk Forensics
- Network Forensics
- Email 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

Fasi principali del trattamento del dato informatico

Identificazione

- Scelta dei dati che possono essere recuperati e ritrovati elettronicamente tramite l'utilizzo di strumenti e suite di Informatica Forense

Acquisizione

- Disponibilità fisica o con strumenti da remoto di computer, dati di log e di traffico e dispositivi esterni di memorizzazione

Analisi

- Ricerca ed individuazione dei dati rilevanti

Valutazione

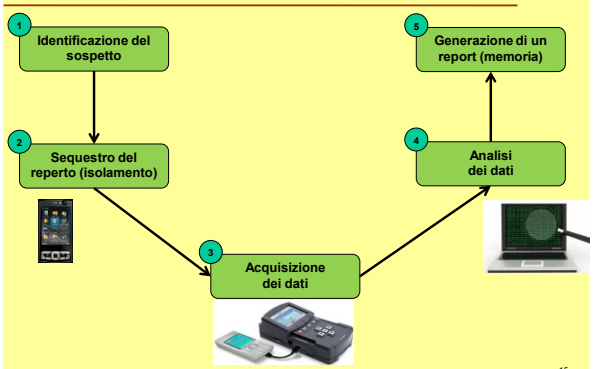
- Valutazione delle informazioni e dei dati che sono stati recuperati al fine di comprenderli, classificarli e determinazione se e come possano essere utilizzati per l'incriminazione o il proscioglimento dell'indagato

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

Fasi del trattamento del dato informatico

Esempio nel caso dei dispositivi mobili



Caratteristiche inerenti la natura fisica del dato

- Necessità di un supporto (hard disk, floppy disk, flash memory, altri)
- Riproducibilità in numero infinito di copie
- Volatilità dei dati
- Modificabilità (quasi) anonima dei dati
- Deteriorabilità dei dati e dei supporti

Esigenze di metodo

- Completezza dell'acquisizione
- Integrità dei dati acquisiti
- Paternità dei dati (o almeno provenienza)
- Esaminabilità dei dati acquisiti
- Verificabilità delle procedure seguite
- Riproducibilità delle operazioni eseguite

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: legge n. 547/93; legge 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

19

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

20

...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
- …

21

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

22

Cornice per la gestione di dati e documenti

Ogni modulo di un sistema informativo è regolamentato da rigorose procedure di gestione documentale nella cornice di

- D. Lgs. n. 82 del Marzo 2005 (Codice dell'Amministrazione Digitale) e D. Lgs. n. 159 del 4 Aprile 2006 (Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'Amministrazione Digitale)
- Conservazione dei documenti
- *Digest e funzioni hash*
- Firma digitale
- Marca temporale

23

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
- Collisione dello **stesso valore** del digest da due **fonti diverse** è impossibile (probabilità una su 10 seguito da 32 zero)

24

Digest e hash function – II
Esempio: MD5

D'accordo	`e3e4a48142318596a3160af3129c4825`
Sono nato a Ravenna	`dc342741a78c07f9d56aac42fe98756b`
<questa presentazione>	`0e6d7d56c4520756f59235b6ae981cdb`
Sono un professore	`870f6dddf00fda887a2d59980ff7ab8e`
Sono un professore.	`b3a82770def09bffaec94072d6ca85d3`

- Stessa Lunghezza: 32 cifre esadecimali (128 bit - 16 byte)
- Valori dipendenti dal contenuto del documento
- Ad una minima variazione dell'input corrisponde una grande variazione nel digest

25

Firma elettroniche e certificati

- **Firme elettronica**: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1, comma 1, lett. q) del D. Lgs. 82/2005)
- Firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata (c.d. asimmetriche), correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici; (art. 1, comma 1, lett. s)
- **Certificato Qualificato**: insieme di informazioni che creano una stretta e affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi a specificati rigidi requisiti e rilasciati da certificatori accreditati

26

Marca temporale e riferimento temporale

- La **marca temporale** consiste in una integrazione della firma digitale, applicata da un certificatore secondo le disposizioni delle regole tecniche, ed è efficace in ogni situazione in cui un **documento deve avere una data certa**, oppure per prolungare nel tempo la validità di un documento informatico, dopo la scadenza del certificato di sottoscrizione
- Il **riferimento temporale** è "*l'informazione, contenente la data e l'ora in cui viene ultimato il processo di conservazione digitale, che viene associata ad uno o più documenti digitali,…. L'operazione di associazione deve rispettare le procedure di sicurezza definite e documentate, a seconda della tipologia dei documenti da conservare, dal soggetto pubblico o privato che intende o è tenuto ad effettuare la conservazione digitale ovvero dal responsabile della conservazione nominato dal soggetto stesso*". Si tratta di una annotazione che **attesta il momento in cui viene chiuso il processo di archiviazione** ed è rilevante solo a questo scopo

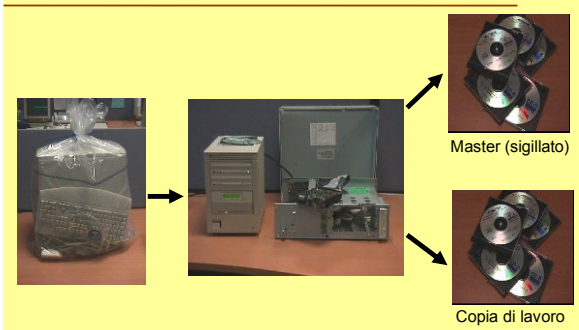
27

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

28

Processo di creazione dell'immagine dei file



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

29

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**

30

Strumenti per la creazione di una copia di un hard disk

31

Una stazione di acquisizione forense

32

Evidenze digitali

- **Qualsiasi informazione, con valore probatorio, che sia memorizzata o trasmessa in formato digitale** (*SWGDE, 1998*)
- 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

33

Tra le modifiche al codice penale introdotte dalla Legge 48/2008

Art. 491 bis

- Soppressione del secondo periodo del comma 1° dell'art 491 bis c.p., contenente la definizione di **documento informatico** quale supporto che contiene dati
- Nuova nozione all'interno del CAD rovescia la definizione precedente definendolo come "*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"
- Rilevanza disciplina sulle **firme elettroniche** come sistema atto a garantire la **paternità dei documenti informatici e requisiti di autenticità e genuinità**. In particolare si veda l'art. 20, comma 1-bis CAD in tema di efficacia probatoria.

34

Capo III: Modifiche al C.p.p. e al dlgs n° 196/2003

- Il raggio d'azione va oltre il settore del **cybercrime**, aprendosi in realtà a qualsiasi attività di indagine sottolineando il ruolo fondamentale della c.d. **digital investigation** nell'odierna prassi giudiziaria.
- Notevole **impatto sulla disciplina generale in tema di prove** soprattutto con riguardo alle garanzie costituzionali e difensive che interessa
- Proprio perché così rilevante, delicata e di "stringente attualità", la materia **avrebbe richiesto un approccio ben più attento**, evitando la loro facile "moltiplicazione" o mera "estensione" ai nuovi fenomeni da regolare

35

Capo III: Modifiche al Codice di procedura penale

- Tecnica emendativa seguita consiste sostanzialmente in un adeguamento attraverso **operazioni di "chirurgia lessicale"** disposizioni processuali già vigenti
- Si vedano gli artt. 8, 9, 11 della legge dove in tema di:
  - **ispezioni e rilievi tecnici** (art 244, 2° comma c.p.p.)
  - **esame di atti, documenti e corrispondenza presso banche** (art 248, 2° comma c.p.p.)
  - **doveri di esibizione e consegna** (art 256, 1° c c.p.p.)
  - **obblighi e modalità di custodia** (art 259, 2° c c.p.p.)
  - **sigilli e vincolo delle cose sequestrate** (art 260,1° e 2° comma c.p.p.)
  - **acquisizione di plichi e corrispondenza** (art 353, 1° e 2° comma c.p.p.)
  - **accertamenti urgenti e sequestro** (art 354, 2° comma c.p.p.)
- Per ciascun istituto il legislatore amplia l'oggetto della norma attraverso l'inserimento di espressioni che rimandano ad attività legate al trattamento di ***"dati, informazioni e programmi informatici"***

36

Capo III: Modifiche al Codice di procedura penale

- Sorge la necessità di assicurare pieno controllo sull'operato degli inquirenti, in particolare la **verifica sulle procedure acquisitive**
- Il legislatore fornisce un "paradigma" sul corretto *modus operandi* da seguirsi nelle operazioni di accesso al *computer* o dispositivo oggetto d'indagine, sottolineando l'importanza alla salvaguardia sull'integrità dei dati che assume, quindi, canone operativo imprescindibile
- Frequente il richiamo alla necessità di adottare ***"misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"***

37

Problemi dell'informatica forense

- Problema dell'identità (*identity*)
- Problema della locazione (*location*)
- Problema dell'integrità (*integrity*)
- Problema della viscosità (*stickiness*)
- Problema del tipo di dati (*data type*)
- Problema della tracciabilità (*traceability*)
- Problema dell'analisi (*analysis*)

38

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

39

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

40

Caso Sostituzione di Persona - I

Massima (Cass V penale, 2013/18826)

L'inserimento, in una chat di incontri personali, del numero di telefono cellulare di un'altra persona, ignara, in associazione a uno pseudonimo (il telematico *nickname*) al fine di danneggiare la stessa persona facendola apparire sessualmente disponibile, integra il reato di sostituzione di persona di cui all'articolo 494 del C. p., nella modalità dell'attribuzione di un falso nome

Considerazione giuridica

- Divieto di interpretazione analogica
- Possibilità di interpretazione estensiva

Ratio decidendi

Leading case; la Cassazione stabilisce che è doveroso procedere a interpretazione estensiva quando un reato 'tradizionale' viene commesso con il mezzo informatico

Casi analoghi

- Aste online
- Alterazione dati account

41

Caso Sostituzione di Persona - II

I profondi e, per certi versi, rivoluzionari cambiamenti che l'evoluzione tecnologica ha prodotto attraverso l'affermarsi delle nuove tecnologie informatiche, … hanno dispiegato i loro effetti anche in materia penale, ponendo molteplici problemi, tra i quali di non poco momento appaiono quelli sottesi a un'attività di interpretazione estensiva che, in assenza di organici interventi legislativi, consenta di adeguare l'ambito di operatività delle tradizionali fattispecie di reato, come quella di cui all'art. 494, c.p, alle nuove forme di aggressione per via telematica dei beni giuridici oggetto di protezione, senza violare i principi della tassatività della fattispecie legale e del divieto di interpretazione analogica delle norme penali. Attività di interpretazione estensiva della norma penale, che, appare opportuno ribadire, lungi dall'essere dall'essere vietata, è invece lecita e, anzi, doverosa, quando sia dato stabilire - attraverso un corretto uso della logica e della tecnica giuridica - che il precetto legislativo abbia un contenuto più ampio di quello che appare dalle espressioni letterali adottate dal legislatore.

42

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

43

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**

44

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 (per es. intercettazioni, dati di traffico): a ciò consegue un diverso regime giuridico di trattamento

45

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

46

Esempio: risoluzione di un indirizzo IP

- Chi effettua l'indagine può risolvere un indirizzo IP di un utente mediante:
  - Identificazione dell'indirizzo IP (da log; ma può essere anonimizzato)
  - Individuazione del *Service Provider* per l'accesso in archivi di registri autorizzati (da registri; ma la gestione dei dati può essere inaccurata)
  - Contatto del titolare dell'indirizzo IP; problemi con indirizzi dinamici, luoghi pubblici, reti wireless insicure
  - 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 registrazioni
- Importante sul punto è la disciplina in tema di **conservazione dei dati** da parte dei *Service Provider* (**data retention**)

47

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
  - 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

48

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

Acquisizione pagina web

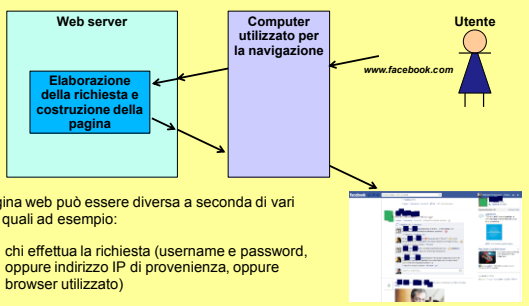
Quando una pagina web viene presentato come prova spesso si assiste (in ordine di frequenza) all'esibizione di:

- Pagine web stampate su carta (così come vengono visualizzate)
- Codice html della pagina web (fatto da persone più accorte)
- Pagine web stampate su carta certificate da un notaio

Nessuna di queste metodologie è idonea. Anche quando c'è l'intervento del notaio che non è in grado di attestare la reale provenienza dei dati

Per presentare una pagina web occorre avvalersi di un consulente tecnico che provvede all'acquisizione dei dati e alla documentazione della provenienza dei dati

Richiesta di una pagina web



La pagina web può essere diversa a seconda di vari fattori, quali ad esempio:

- chi effettua la richiesta (username e password, oppure indirizzo IP di provenienza, oppure browser utilizzato)
- quando viene fatta la richiesta
- parametri passati durante la richiesta

Verifiche nell'acquisizione pagina web

- Una pagina web si compone di tanti oggetti
  - Il testo della pagina
  - Le immagini
  - I video
  - …
- Ogni oggetto può provenire da fonti diverse
  - Dalla stampa della pagina non si capisce
  - Si può capire dal codice sorgente
- Occorre inoltre verificare l'effettiva sorgente dei dati
  - Necessario catturare il traffico di rete generato per l'ottenimento della pagina web
- Occorre fornire garanzie temporali
- È un'operazione tecnica, non può esser fatta da un giurista

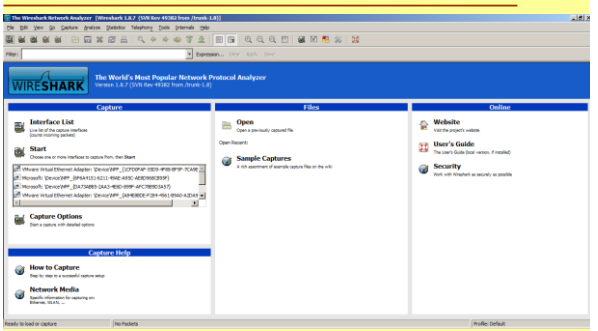
Acquisizione pagina web

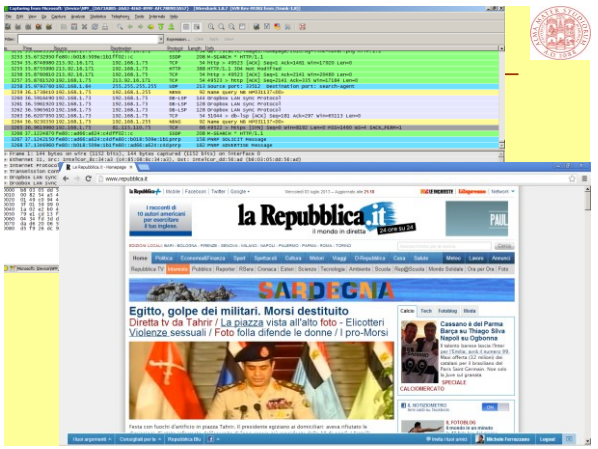
Corretta metodologia di acquisizione:

- Registrazione del traffico di rete
- Consultazione della pagina web da acquisire
- Consultazione di una pagina web con tempo di riferimento (es. quotidiano online)
- Salvataggio di tutte le pagine web visitate e del traffico di rete
- Applicazione di firma digitale e marca temporale in tutti i dati sopra citati
- *Facoltativo: registrazione del video dello schermo durante le operazioni*

La stampa su carta diventa una mera rappresentazione, tutti i dati vanno presentati su supporto informatico

Esempio di software per l'intercettazione del traffico telematico generato





Strumenti software per l'analisi forense

Software commerciali

- **Encase** di Guidance Software
- **Forensic Tool Kit (FTK)** 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

Distribuzioni Linux

- Helix di E-fence
- DEFT
- CAINE

56

Toolkit

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

57

Funzionalità dei toolkit

- 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

58

Evidenze presenti sul dispositivo mobile

- Elementi di prova possono essere trovate in molte locazioni dell'apparecchio e della rete
  - Fotografie e video
  - Liste di Contatti
  - Storico delle chiamate
  - Messaggi (SMS, MMS, altri)
  - Agende, rubriche, calendari
  - Informazioni GPS e reti WiFi utilizzate
  - Navigazione web
  - Note (testuali e audio)
  - Chat
  - Email e allegati ad email
  - Vocabolario T9
- Necessari strumenti (hardware e software) per l'acquisizione dei dati

59

Caso pratico: morte per incidente stradale

Fatto

- Una persona esce di casa la sera 3 maggio 2012 verso le 23:30 per una commissione. Il coniuge denuncia la scomparsa la mattina del 4 maggio 2012. Viene ritrovata morta in una scarpata la mattina del 5 maggio all'interno dell'auto
- Si cerca di capire cosa possa essere accaduto analizzando lo smartphone della vittima rinvenuto nell'auto

Esiti dell'analisi forense sullo smartphone

- Nessun elemento utile tra chiamate e SMS
- Alle 2:23 del 4 maggio è transitata molto vicino alla propria abitazione
- Lo smartphone memorizza la connessione alla rete wireless

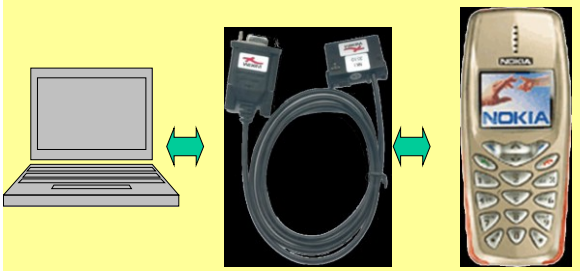
#	BSSID	SSID	Security mode	Last Connected	Deleted?
1		Apple Demo			
2		Apple Store			
3	F8:1E:DF:49:43:D4	Network di Pippo	WPA2 Personal	02/05/2012 13:45:16	
4	00:23:CD:D4:59:0B	Alice-123456		04/05/2012 02:23:43	

60

Acquisizione di evidenze presenti sul dispositivo mobile - I

Esempio di acquisizione con Cellebrite UFED

Acquisizione di evidenze presenti sul dispositivo mobile - II



Esempio di acquisizione con software e computer

Trattamento del reperto informatico mobile

Raccolta e gestione di evidenze

- La prima cosa da fare con i telefoni cellulari è di isolarli dalla rete
  - Rischio cancellazione da postazione remota e connessa
  - Rischio di sovrascrittura contenuti (in chiaro e cancellati) in caso di ricezione di chiamate, messaggi o email
- Per isolare il telefonino si utilizzano contenitori che bloccano i segnali radio (es.: scatole di Faraday, fogli di alluminio)

(http://www.paraben.com/)

Consulenza tecnica in una Procura del nord Italia - I

Antefatto: gli organi inquirenti, Polizia giudiziaria e consulente 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

Consulenza tecnica in una Procura del nord Italia - 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 (…)"

Consulenza tecnica recente della Procura di Lecce

- Accusa di tentata concussione
- Sequestro di un server dell'università
- Sul server sono presenti mail, contatti, messaggi, file di terzi

È consentito violare la privacy di terzi mediate un sequestro massivo e indistinto del contento del server?

- Modalità di effettuazione del sequestro selettiva

L'indagato ha diritto alla tutela della privacy rispetto alle indagini?

- No, la tutela dei suoi dati personali scema rispetto alle esigenze di indagine; i terzi godono della tutela della loro riservatezza

Ne deriva l'obbligo di sequestro selettivo (Legge 48) che le Iso eleggono a prassi migliore

Due ingegneri informatici dell'Università di Lecce rinunciano alla consulenza tecnica dichiarando di non avere le qualifiche per dare seguito alla richiesta di acquisizione di informazioni

67

Ciclo di seminari di Informatica forense

Alma Mater Studiorum - Università di Bologna
Facoltà di Giurisprudenza
Cattedra di Informatica Forense
Cattedra di Informatica Giuridica
Cattedra di ICT Law

CIRSFID - Università di Bologna

CSIG - Centro Studi di Informatica Giuridica

Ciclo di seminari

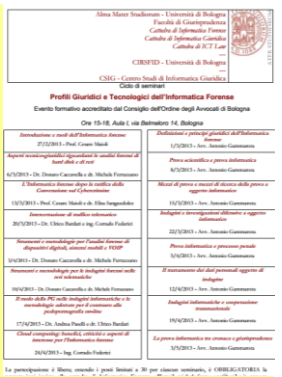
Profili Giuridici e Tecnologici dell'Informatica Forense

Evento formativo accreditato dal Consiglio dell'Ordine degli Avvocati di Bologna

68

Programma del ciclo di seminari

1. **Introduzione e ruoli dell'Informatica forense**
2. **Definizioni e principi giuridici dell'Informatica forense**
3. **Aspetti tecnico-giuridici riguardanti le analisi forensi di hard disk e di reti**
4. **Prova scientifica e prova informatica**
5. **L'Informatica forense dopo la ratifica della Convenzione sul Cybercrimine**
6. **Mezzi di prova e mezzi di ricerca della prova a oggetto informatico**
7. **Intercettazione di traffico telematico**
8. **Indagini e investigazioni difensive a oggetto informatico**
9. **Strumenti e metodologie per l'analisi forense di dispositivi digitali, sistemi mobili e VOIP**
10. **Prova informatica e processo penale**
11. **Strumenti e metodologie per le indagini forensi nelle reti telematiche**
12. **Il trattamento dei dati personali oggetto di indagine**
13. **Il ruolo della PG nelle indagini informatiche e le metodologie adottate per il contrasto alla pedopornografia on-line**
14. **Indagini informatiche e cooperazione transnazionale**
15. **Cloud computing: benefici, criticità e aspetti di interesse per l'informatica forense**
16. **La prova informatica tra cronaca e giurisprudenza**


Alma Mater Studiorum - Università di Bologna
Facoltà di Giurisprudenza
Cattedra di Informatica Forense
Cattedra di Informatica Giuridica
Cattedra di ICT Law

CIRSFID - Università di Bologna

CSIG - Centro Studi di Informatica Giuridica
Ciclo di seminari
Profili Giuridici e Tecnologici dell'Informatica Forense
Evento formativo accreditato dal Consiglio dell'Ordine degli Avvocati di Bologna
Ore 15-18, Aula I, via Belmatoro 14, Bologna

69

Conclusioni

Dato giuridico: modifiche introdotte dalla legge n. 48/2008

Dato tecnico: ISO IEC 27037/2012

Panorama giurisprudenziale mostra la delicatezza del tema:

- Da un lato possibili meccanismi distorsivi degli istituti d'investigazione con connotati informatici
- Dall'altro necessità a una corretta interpretazione delle norme tanto in chiave tecnica quanto in chiave giuridica, mediante lettura costituzionalmente orientata delle norme (art. 111 Cost.)

70

Riferimenti

- Cajani F., *Appunti per una strategia globale di contrasto del cybercrime*, IISFA Memberbook 2011, Experta, 2012
- Corasaniti G., Corrias Lucente G. (a cura), *Cybercrime, responsabilità degli utenti, prova digitale*, Cedam, 2009
- ISO/IEC 27037/2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence, 2012*
- Luparia L. (a cura), *Sistema penale e criminalità informatica*, Giuffrè, 2009
- Maioli C., Sanguedolce E., *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, http://www.altalex.com/index.php?idnot=18096, 2012
- Picotti L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, Diritto penale e processo, 2008
- Sanguedolce E., *Informatica forense e legge 48/2008*, www.bit2law.wordpress.com, 2012
- Vaciago G., *Digital evidence*, Giappichelli, 2012
- Walden I., *Computer crimes and digital investigations*, Oxford University Press, 2007

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

71