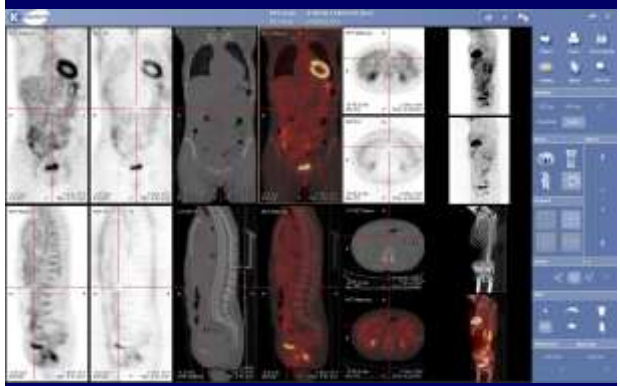
DEFINIZIONE DEI SISTEMI RIS-PACS

- RIS (Radiology Information System) Sistema Informatico Radiologico
  software gestionale della Radiologia
- PACS (Picture Archiving and Communication System)
  Sistema di archiviazione e trasmissione di immagini
  sistema hardware e software dedicato all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali
- HIS (Hospital Information System) Sistema informativo ospedaliero
  sistema che integra gli strumenti informatici utilizzati in ambito sanitario per gestire i flussi amministrativi e clinici di un ospedale

FUNZIONE DEI SISTEMI RIS-PACS



http://upload.wikimedia.org/wikipedia/commons/4/40/Viewer_medecine_nucleaire_keosys.JPG

ATTIVITA' TIPICHE DEI SISTEMI RIS-PACS

- ARCHIVIAZIONE (in formato digitale)
- VISUALIZZAZIONE (in formato digitale) e altri mezzi di output
- ELABORAZIONE (in formato digitale)
- TRASMISSIONE (in formato digitale)

PROCEDURE GESTITE DAI SISTEMI RIS-PACS

- PRENOTAZIONE (in formato digitale)
- ACCETTAZIONE (in formato digitale)
- AQUISIZIONE DIAGNOSTICA (in formato digitale)
- REFERTAZIONE (in formato digitale)
- ALTRE PROCEDURE INTERMEDIE (in formato digitale)

ARCHITETTURA DEI SISTEMI RIS-PACS

http://upload.wikimedia.org/wikipedia/commons/2/28/Workflow_diagram.pn

OGGETTI TRATTATI DAI SISTEMI RIS-PACS

Standard DICOM (*Digital Imaging and COmmunications in Medicine)* definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico quali ad esempio immagini radiologiche. (http://it.wikipedia.org/wiki/DICOM)

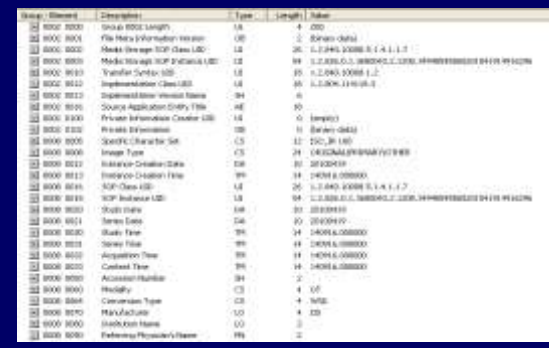
Immagini DICOM

\+

Header
- nome e cognome del paziente
- procedura
- tempi e date di acquisizione
- tipo di scansione
- posizione dell'immagine
- dimensione dell'immagine
- ecc.

OGGETTI TRATTATI DAI SISTEMI RIS-PACS

DICOM HEADER



OGGETTI TRATTATI DAI SISTEMI RIS-PACS

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 RIS-PACS (in formato digitale)
- DATI ESTERNI DEI FILE (in formato digitale)

OGGETTI TRATTATI DAI SISTEMI RIS-PACS

DATI PERSONALI (in formato digitale)

- anagrafiche dei pazienti e degli operatori
- nome
- cognome
- sesso
- luogo e data nascita
- residenza
- codice fiscale
- telefono e e-mail
- paternità e maternità (con relativi dati)
- ...e molti altri dati personali

OGGETTI TRATTATI DAI SISTEMI RIS-PACS

DATI QUANTITATIVI (in formato digitale)

- numero esami effettuati
- frequenza
- medici richiedenti
- quantità e qualità di farmarci usati
- percentuali e statistiche di consumo
- tempi, modi e statistiche di uso delle apparecchiature
- ...e molti altri

OGGETTI TRATTATI DAI SISTEMI RIS-PACS

ALTRI DATI ORGANIZZATIVI, CONTABILI, FISCALI (in formato digitale)

- agende
- rendicontazioni
- cassa
- ...e molti altri

UBICAZIONE DEI DATI DEI SISTEMI RIS-PACS

- ARCHIVI LOCALI (PC, buffer, stampanti, scanner, ecc.)
- ARCHIVI REMOTI (Server HIS, Hosting, Housing, Cloud Computing)
- DISPOSITIVI MOBILI (m-health)
- MEMORIE PORTATILI

I DATI DEI RIS-PACS COME OGGETTO DI TUTELA

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 interrompere 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)

I DATI DEI RIS-PACS COME OGGETTO DI TUTELA

Anche il sistema informatico
è oggetto di tutela penale

- 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.)

RILEVANZA DEI DATI DEI SISTEMI RIS-PACS

- I RIS-PACS producono e gestiscono enormi quantità di dati digitali
  - rappresentazioni (immagini, rielaborazioni, suoni, testi, ecc.)
  - dati interni (dati personali, amministrativi, contabili, statistici, ecc.)
  - dati esterni (dati di sistema, cronologici, ubicazione, ecc.)
- Dati, interni ed esterni ai file sono contenute
  - in documenti informatici (art. 234 c.p.p)
  - nei file relativi ai documenti (dati esterni di sistema)
  - nei file del sistema informatico (file di log, file manager, ecc.)
- I dati digitali forniscono enormi quantità di informazioni utili …

RILEVANZA DEI DATI TRATTATI DAI SISTEMI RIS-PACS

- IN AMBITO PROPRIAMENTE SANITARIO
  - clinico
  - amministrativo
  - contabile
  - statistico
- IN AMBITO GIUDIZIARIO
  - giudizi contabili (ad es. per responsabilità erariale)
  - giudizi amministrativi (ad es. per legittimità atti amministrativi)
  - giudizi civili (ad es. per responsabilità contrattuale, risarcimento danni, ecc.)
  - giudizi penali (ad es. per responsabilità professionale, malpractice, maltrattamento dati personali, ecc.)

I SISTEMI RIS-PACS COME REPOSITORY DI DOCUMENTI INFORMATICI

- Sistema di documentazione di fatti processualmente rilevanti
  - dati personali
  - data e ora dell'esame
  - caratteristiche fisiche
  - condizioni fisiche
  - informazioni amministrative
  - modalità di pagamento

- Mezzo di prova di fatti processualmente rilevanti

RILEVANZA GIURIDICA DEI DOCUMENTI INFORMATICI GENERATI DAI SISTEMI RIS-PACS

- per il DIRITTO SOSTANZIALE
- per il DIRITTO PROCESSUALE
  - PENALE
  - CIVILE
  - AMMINISTATIVO
  - CONTABILE

QUALI SONO

I PRINCIPI TECNICI DA APPLICARE

E LE NORME GIURIDICHE DA ATTUARE

PER IL CORRETTO TRATTAMENTO DEI DATI DIGITALI PRODOTTI DAI SISTEMI RIS-PACS

A FINI PROCESSUALI ?

Informatica Forense

è la scienza che studia le tecniche, metodologie e procedure e strumenti per l'individuazione, estrazione, conservazione, protezione, analisi, documentazione, interpretazione ed ogni altra forma di trattamento dei dati in formato digitale, rilevanti a fini probatori in un processo

Nel Cyberspazio senza frontiere fisiche...

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

...I reati e gli altri fatti processualmente rilevanti vanno ricostruiti partendo dai dati digitali

- ubicazione dell'autore: **da dove**
- identificazione dell'autore: **chi è, chi sono**
- individuazione degli autori: **quanti**
- cronologia degli eventi: **quando**
- modalità esecutive: **in che modo**
  - velocità dell'attività
  - volatilità delle tracce
- movente: **perchè**
- effetti: **danni**
- reiterazione: **quante volte**
- offensività: **contro chi**

MEZZI DI PROVA AD OGGETTO INFORMATICO

DOCUMENTI. = rappresentazione di un fatto incorporata in una base materiale

Art. 234 C.p.p. (Prova documentale) È consentita l'acquisizione di **scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.**

2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita **copia**.

3. È vietata l'acquisizione di documenti (191) che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti (195[7], 203, 240).

MEZZI DI PROVA AD OGGETTO INFORMATICO

DOCUMENTI. = rappresentazione di un fatto incorporata in una base materiale

il documento comprende 4 elementi (Tonini):

- il **fatto rappresentato** = fatti, persone, cose, pensieri

- la **rappresentazione** = modo con cui un fatto è reso conoscibile: immagini, parole, suoni

- l'**incorporamento** = operazione di fissazione della rappresentazione sulla base materiale: scrittura, fotografia, fonografia, cinematografia, **registrazione magnetica**

- la **base materiale** = supporto che consente di fissare la rappresentazione (carta, pellicola, supporto magnetico)

MEZZI DI PROVA AD OGGETTO INFORMATICO

DOCUMENTI. = rappresentazione di un fatto incorporata in una base materiale

Art. 234 (Prova documentale) È consentita l'acquisizione di ... **documenti che rappresentano fatti, persone o cose mediante ... qualsiasi altro mezzo.**

Rientrano in tale *genus*:

- file di testo
- file di sistema
- le fotografie digitali
- i filmati digitali
- le fotografie estratte da filmati digitali
- le registrazioni magnetico-digitali

2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita **copia**.
3. (... Divieto...)

RILEVANZA DEI DATI DIGITALI A FINI PROCESSUALI

aumento della domanda di analisi dei dati digitali a fini di indagine e di investigazione difensiva per:

- reati informatici e telematici propriamente detti (ad es. ex L. 547/93)
- reati comuni a condotta libera, commessi con l'impiego di sistemi informatici e telematici
- dati aventi valore di prova o indizio per qualunque tipo di reato, rinvenibili in sistemi informatici, telematici e di archiviazione

Comune denominatore:
Il dato digitalizzato come oggetto di indagine

INDAGINE SUI DATI DEI RIS-PACS

http://upload.wikimedia.org/wikipedia/commons/2/28/Workflow_diagram.pn

Caratteristiche inerenti la natura fisica (?) del dato

- necessità di un supporto (hard disk, floppy disk, flash memory, ecc.)
- riproducibilità in numero infinito di copie
- volatilità dei dati
- modificabilità (quasi) anonima dei dati
- deteriorabilità dei dati e dei supporti

Esigenze di rigore tecnico e metodologico

- 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

Principi per la corretta gestione del reperto informatico

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

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

Catena di custodia: 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 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

Esigenze di ordine giuridico

Il fine dell'attività tecnica è consentire
la disponibilità per tutte le parti processuali

per l'utilizzabilità nel procedimento penale
(ma anche in processi di altro tipo)
dei dati,
informazioni,
rappresentazioni digitali
dei dati accessori di sistema e/o esterni

integri e completi

al fine della valutazione di ogni fatto giuridicamente rilevante,

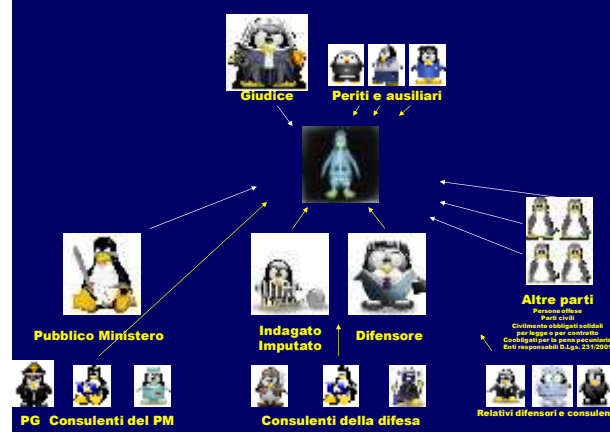
sostanziale e/o processuale

Una corretta prassi di Informatica Forense favorisce simultaneamente tutte le parti del processo e persegue il Giusto Processo (art. 111 Costituzione)

- Polizia Giudiziaria (efficienza e buon andamento della PA)
- Pubblico Ministero (esercizio dell'azione penale)
- indagato-imputato (rispetto del diritto di difesa)
- persona offesa – parte civile (domande civili)
- altre parti del processo
- Giudice (giudizio)

in ogni stato e grado del procedimento

I DATI RIS-PACS INTERESSANO A TUTTE LE PARTI DEL PROCESSO



LEGGE 4 APRILE 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)

Capo III
MODIFICHE AL
CODICE DI PROCEDURA PENALE
E AL
CODICE DI CUI AL DECRETO LEGISLATIVO
30 GIUGNO 2003, N. 196

Modif.ta da L. 24 luglio 2008 n. 125, di conv. con modif. del D. L. 23 maggio 2008 n. 92 (in G.U. n. 122, 26 maggio 2008, S.G.) – Misure urgenti in materia di sicurezza pubblica (**c.d. "Pacchetto sicurezza"**)

LEGGE 4 APRILE 2008 N. 48

Art. 14 *(Entrata in vigore)*

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

Legge 18 marzo 2008 n. 48
Pubblicata in G.U. del 4 aprile 2008

ENTRATA IN VIGORE IL 5 APRILE 2008

Legge 48/2008: le modifiche al codice penale

491 bis. (1) (Documenti informatici). Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, **avente efficacia probatoria (2)** si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. [**SOPPRESSO:** *A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.*]

(1) Articolo aggiunto dall'art. 3 della L. 23 dicembre 1993, n. 547, recante modificazioni e integrazioni alle norme del codice penale e di procedura in tema di criminalità informatica.

(2) Articolo così modificato dall'art. 3 della L. 48/2008, recante 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

Legge 48/2008: le modifiche al codice di procedura penale

- Mezzi di ricerca della prova
  - Ispezioni (art. 244 c.p.p.)
  - Perquisizioni (art. 247 c.p.p.)
    - Richiesta di consegna (art. 248 c.p.p)
  - Sequestro di corrispondenza telematica (art. 254 c.p.p.)
  - Sequestro di dati informatici di traffico (art. 254 c.p.p.)
    - Dovere di esibizione (art. 254 c.p.p.)
    - Custodia delle cose sequestrate (art. 259 c.p.p.)
    - Sigillo elettronico o informatico e copia dei dati (art. 260 c.p.p.)
- Attività a iniziativa della P.G.
  - Perquisizioni (art. 352 c.p.p.)
  - Corrispondenza telematica (art. 352 c.p.p.)
  - Accertamenti urgenti e sequestro (art. 354 c.p.p.)
- Conservazione dati di traffico (art. 132 D. Lgs. 30 giugno 2003, n. 196)
- Competenza

Legge 48/2008: le modifiche al codice di procedura penale

ISPEZIONI

244. (Casi e forme delle ispezioni). 1. L'ispezione delle persone, dei luoghi e delle cose (103) è disposta con decreto motivato (125[3]) quando occorre accertare le tracce e gli altri effetti materiali del reato.

2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (359, 364), **anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.**

(1) Articolo così modificato dall'art. 8 della L. 48/2008, recante 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

Legge 48/2008: le modifiche al codice di procedura penale

PERQUISIZIONI

247. (Casi e forme delle perquisizioni). 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato (253[2]) o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato (60, 61) o dell'evaso, è disposta perquisizione locale (352).

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. (1)

2. La perquisizione è disposta con decreto motivato (125[3]).

3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria (57) delegati con lo stesso decreto (370) (2).

(1) Articolo così modificato dall'art. 8, c.2, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita` informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

(2) Cfr. l'art. 68 comma 2 Cost. nonché, per i reati di cui all'art. 90 Cost., l'art. 7, L. 5 giugno 1989, n. 219

Legge 48/2008: le modifiche al codice di procedura penale

COSA SI INTENDE PER:

- ***…ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione…***
  - *cracking* di P.G. delle misure di sicurezza ?
  - l'accesso e la perquisizione modificano *ex se* i dati (esterni) ?
  - come impedire l'alterazione (differente da immodificabilità) ?
  - la verificabilità dell'alterazione o meno presuppone o impone l'adozione di *tools open source* ?

Legge 48/2008: le modifiche al codice di procedura penale

RICHIESTA DI CONSEGNA

248. (Richiesta di consegna). 1. Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini.

2. Per rintracciare le cose da sottoporre a sequestro (253 ss.) o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria (57) da questa delegati (370) possono esaminare [SOSTITUIRE: *atti, documenti e corrispondenza presso banche* CON] **presso banche atti, documenti e corrispondenza nonchè dati, informazioni e programmi informatici**. In caso di rifiuto, l'autorità giudiziaria procede a perquisizione (255). (1)

(1) Articolo così modificato dall'art. 8, c.3, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita` informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Legge 48/2008: le modifiche al codice di procedura penale

SEQUESTRO DI CORRISPONDENZA TELEMATICA

254. (Sequestro di corrispondenza). [SOSTITUIRE: *1. Negli uffici postali o telegrafici è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa o che comunque possono avere relazione con il reato.* CON]

1. **Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.**
2. Quando al sequestro procede un ufficiale di polizia giudiziaria (57), questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli **o alterarli** e senza prendere altrimenti conoscenza del loro contenuto (353).
3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati (103[6]) (1).

(1) Articolo così modificato dall'art. 8, c. 4, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Legge 48/2008: le modifiche al codice di procedura penale

SEQUESTRO DI DATI INFORMATICI DI TRAFFICO

Art. 254-bis. – (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). **– 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.** (1).

(1) Articolo così modificato dall'art. 8, c. 5, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Legge 48/2008: le modifiche al codice di procedura penale

COSA SI INTENDE PER:

- … **fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione …**
  - sono i c.d. dati esterni, dati di handover, GPS ?
- … **la loro acquisizione avvenga mediante copia di essi su adeguato supporto…**
  - con quali procedure tecniche di acquisizione ?
  - quando il supporto può considerarsi "adeguato" ?

Legge 48/2008: le modifiche al codice di procedura penale

COSA SI INTENDE PER:

- **…con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.**
  - quale tipo di copia ?
  - con quali *tools* ?
  - le copie di dati – se tra loro conformi (hash) – diventano originali;
    - rectius "originari" ?
    - time stamping ?
  - come si assicura l'immodificabilità ?
  - con quale procedura ?
    - Ex art. 359, 360 (117 disp. att. c.p.p.), 392, 233 c.p.p., altro ?
  - con quali garanzie difensive ?

Legge 48/2008: le modifiche al codice di procedura penale

ALCUNE IMPLICAZIONI

- Art. 257 c.p.p. – Riesame del decreto di sequestro
  - imputato – sequestratario - quella che avrebbe diritto alla restituzione
  - riesame per restrizione mediante selezione dei dati ?
  - quali metodi di selezione dei dati ?

Legge 48/2008: le modifiche al codice di procedura penale

256. (Dovere di esibizione e segreti). 1. Le persone indicate negli artt. 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, **nonchè i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto,** e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreti di Stato (202) ovvero di segreto inerente al loro ufficio o professione (200).

2. Quando la dichiarazione concerne un segreto di ufficio o professionale (200), l'autorità giudiziaria, se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti, i documenti o le cose indicati nel comma 1, provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro (1).

3. Quando la dichiarazione concerne un segreto di Stato, l'autorità giudiziaria ne informa il presidente del Consiglio dei Ministri, chiedendo che ne sia data conferma. Qualora il segreto sia confermato e la prova sia essenziale per la definizione del processo, il giudice dichiara non doversi procedere per l'esistenza di un segreto di Stato.

4. Qualora, entro sessanta giorni dalla notificazione della richiesta, il Presidente del Consiglio dei Ministri non dia conferma del segreto, l'autorità giudiziaria dispone il sequestro.

5. Si applica la disposizione dell'art. 204.

(1) Gli artt. 12 e 16 della L. 24 ottobre 1977, n. 801, recante norme sull'ordinamento dei Servizi segreti e la disciplina del segreto di Stato così dispongono:

«12. Sono coperti dal segreto di Stato gli atti, i documenti, le notizie, le attività e ogni altra cosa la cui diffusione sia idonea a recar danno alla integrità dello Stato democratico, anche in relazione ad accordi internazionali, alla difesa delle istituzioni poste dalla Costituzione a suo fondamento, al libero esercizio delle funzioni degli organi costituzionali, alla indipendenza dello Stato rispetto agli altri Stati e alle relazioni con essi, alla preparazione e alla difesa militare dello Stato.

«In nessun caso possono essere oggetto di segreto di Stato fatti eversivi dell'ordine costituzionale».

«16. Di ogni caso di conferma dell'opposizione del segreto di Stato a' sensi dell'art. 352 c.p.p.

(*) Il Presidente del Consiglio dei Ministri è tenuto a dare comunicazione, indicandone con sintetica motivazione le ragioni essenziali, al Comitato parlamentare di cui all'art. 11 della presente legge, il Comitato parlamentare, qualora ritenga a maggioranza assoluta dei suoi componenti infondata l'opposizione del segreto, ne riferisce a ciascuna delle Camere per le conseguenti valutazioni politiche».

(*) Ora, ai sensi dell'art. 208 coord., art. 202.

(2) Articolo così modificato dall'art. 8, c. 6, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio

Legge 48/2008: le modifiche al codice di procedura penale

IN CASO DI DOVERE DI ESIBIZIONE
E OBBLIGO DI CONSEGNA,
SU CHI GRAVA L'OBBLIGO DI EFFETTUARE

"copia su adeguato supporto"

"adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" ?

- obbligo per le persone indicate nell'art. 200 e 201 c.p.p. ?
- obbligo per l'A.G. procedente ?
- obbligo per la P.G. ?

Legge 48/2008: le modifiche al codice di procedura penale

CUSTODIA DELLE COSE SEQUESTRATE

259. (Custodia delle cose sequestrate) (1).

1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell'art. 120 (att. 813, 82; reg. 10, 11).
2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Al custode può essere imposta una cauzione. **Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria.** Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale (135), nella cancelleria o nella segreteria.

(1) Articolo così modificato dall'art. 8, c. 7, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Legge 48/2008: le modifiche al codice di procedura penale

ALCUNE IMPLICAZIONI

- Art. 259 c.p.p. – Custodia delle cose sequestrate
  - i dati sono "cose" ?
  - custodia dei dati, informazioni, programmi, o dei supporti ?
  - quando il supporto può considerarsi adeguato ?
  - custodia in cancelleria, segreteria ?
  - (se non è possibile o opportuno) custodia in luogo diverso, custode ?
  - è una forma di trattamento di dati (anche sensibili) che dà luogo a responsabilità ex art. 2050 c.c. ?
  - obbligo di adozione delle misure di sicurezza ex All. B) D. Lgs. 196/03) ?
  - necessità dell'All. C) D. Lgs. 196/03 - Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia (ex artt. 46 e 53 Cod.; termine ex art. 181, 3° c., scaduto il 30 giugno 2004)

Legge 48/2008: le modifiche al codice di procedura penale

SIGILLO ELETTRONICO O INFORMATICO E COPIA DEI DATI

260. (Apposizione dei sigilli alle cose sequestrate. Cose deperibili). 1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste (126) ovvero, in relazione alla natura delle cose, con altro mezzo, **anche di carattere elettronico o informatico,** idoneo a indicare il vincolo imposto a fini di giustizia (349 c.p.).

2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'art. 259. **Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.**

3. Se si tratta di cose che possono alterarsi, l'autorità giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione (att. 83).

(1) Articolo così modificato dall'art. 8, c. 8, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Legge 48/2008: le modifiche al codice di procedura penale

PERQUISIZIONI

352. (Perquisizioni) (1). 1. Nella flagranza del reato (382) o nel caso di evasione (385 c.p.), gli ufficiali di polizia giudiziaria (57) procedono a perquisizione personale o locale (247 ss.; coord. 225) quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso (103, 356; att. 113; 609 c.p.).

1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

2. (…)

(1) Articolo così modificato dall'art. 9 della L. 48/2008, recante 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

Legge 48/2008: le modifiche al codice di procedura penale

352. (Perquisizioni) (1). *(Continua)*

2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare (293) o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata (656) per uno dei delitti previsti dall'art. 380 ovvero al fermo di una persona indiziata di delitto (384), gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.
3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'art. 251 quando il ritardo potrebbe pregiudicarne l'esito.
4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute (2572, lett. d). Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.

(1) Articolo così modificato dall'art. 9 della L. 48/2008, recante 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

Legge 48/2008: le modifiche al codice di procedura penale

ACCERTAMENTI URGENTI E SEQUESTRO

354. (Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro). 1. Gli ufficiali e gli agenti di polizia giudiziaria (57) curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero. **In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.**

2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente ovvero non ha ancora assunto la direzione delle indagini (1), gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti (253, 356; att. 113) (2) (3).

3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale (245, 357, 2, lett. e); att. 113).

(1) Articolo cosi modificato dall'art. 9, c. 3, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita` informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

INDAGINE SUI DATI DEI RIS-PACS

GLI STRUMENTI DI ACQUISIZIONE DEI DATI DIGITALI

- acquisizione dei dati digitali mediante copia
- su adeguato supporto
- con una procedura che assicuri
  - la conformità della copia dei dati acquisiti a quelli originali
  - l'immodificabilità
- custodia e/o conservazione dati originari

GLI STRUMENTI DI ACQUISIZIONE DEI DATI DIGITALI

L. 4 aprile 2008 n. 48

- la *bit strem image*
- su supporti ottici
- calcolo hash – firma digitale
- marca temporale

GLI STRUMENTI DI ACQUISIZIONE DEI DATI DIGITALI

- la *bit strem image (o copia forense) acquisizione e copia bit a bit su un altro dispositivo di memorizzazione di*
  DATI RIS-PACS
  - *un file*
  - *un gruppo di file*
  - *contenuto di un intero supporto*

Supporti di memorizzazione

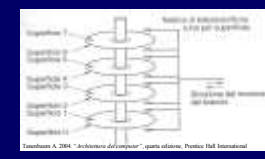
- Elettronico
  - Schede di memoria, USB Pendrive…
- Magnetico
  - DAT, Floppy disk, Hard disk…
- Ottico
  - CD, CD-RW, DVD, DVD-RW, Blu-ray, HD DVD…

Memorie elettroniche

- Nelle memorie elettroniche il dato è rappresentato dalla presenza o meno di una carica di elettroni

Supporti magnetici

- Un disco magnetico si compone di uno o più piatti di alluminio con un rivestimento magnetizzabile



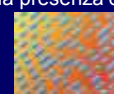
Tanenbaum A. 2004. "*Architettura dei computer*", quarta edizione, Prentice Hall International

- La testina è sospesa appena sopra la superficie (nei floppy disk è a contatto)
- Scrittura: la corrente attraversa la testina e la superficie sottostante viene magnetizzata
- Lettura: la testina passa sopra un'area magnetizzata, viene indotta una corrente nella testina e ciò permette di leggere i bit memorizzati in precedenza

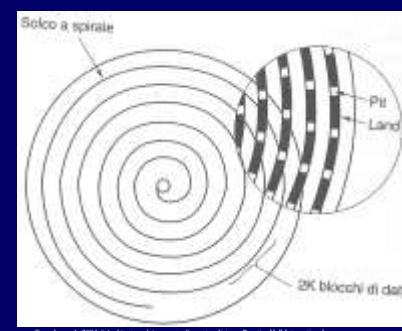
Supporti ottici

- Rispetto ai supporti magnetici, i supporti ottici offrono densità di memorizzazione maggiore

- Lettura e scrittura regolati da raggi laser
  - Scrittura: un laser a raggi infrarossi ad alta potenza brucia minuscoli fori (meno di 0,8 micron per i CD, 0,4 micron per i DVD). Le depressioni si chiamano pit, le aree non bruciate land
  - Lettura: un laser a raggi infrarossi a bassa potenza invia un fascio luminoso verso il supporto. I pit sono delle cunette, i land delle superfici piatte, quindi riflettono in modo diverso il raggio
- La vicinanza pit/land o land/pit identifica il bit 1, la presenza di soli land il bit 0

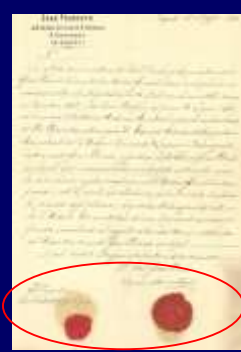


Supporti ottici
schema del Compact Disc



Tanenbaum A. 2004. "*Architettura dei computer*", quarta edizione, Prentice Hall International

Sigillo classico



Sigillo elettronico

???

- In informatica, lo strumento disponibile è la firma digitale
  - Crittografia
  - Chiave privata
  - Chiave pubblica
  - Hash
- Necessità di hardware aggiuntivo
  - Smart card + Lettore di smart card
  - USBkey

Hash
impronta univoca del documento

- Hash: stringa di bit ottenuta applicando una funzione matematica a file o supporti in input di qualsiasi tipo e lunghezza
- La funzione hash:
  - è fissa: ogni algoritmo definisce una precisa lunghezza della stringa (ad esempio, MD5 produce 32 caratteri esadecimali)
  - è difficilmente reversibile: non è possibile risalire al documento originario partendo dall' impronta hash
  - sintetizza il flusso originario di bit in modo univoco: a due file che differiscono anche di un solo carattere o spazio (quindi almeno in un bit) corrispondono due impronte diverse

Hash
Esempio di calcolo dell'MD5

Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura

49A889C77E9C9AE3FDE05396EDCA59E5

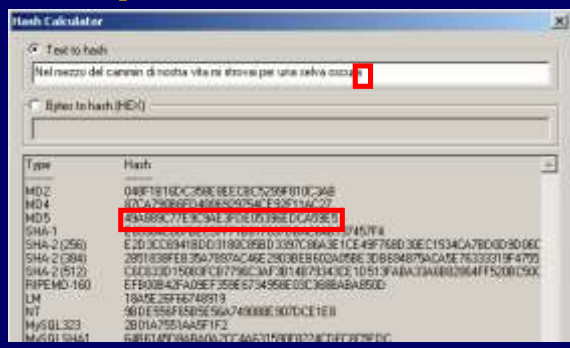
Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura.

21CB4CCEDED46771CF91C4A43EE79732

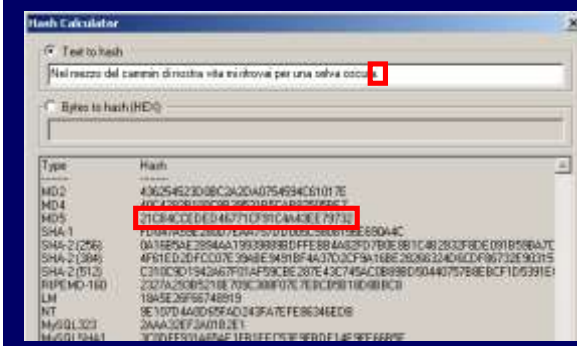
nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura

A84AD79D8952556C9301AA847D436914

Hash
Esempio di calcolo dell'MD5



Hash
Esempio di calcolo dell'MD5



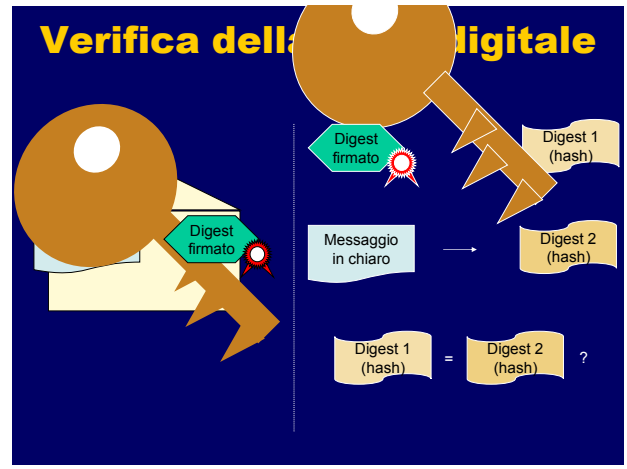
Generazione della firma digitale

- Viene prodotta l'impronta del documento da firmare, utilizzando la funzione di hash
- Si genera la firma digitale cifrando, con la chiave privata del sottoscrittore, l'impronta precedentemente prodotta
- Viene creata la busta elettronica, contenente
  - il documento informatico originario da firmare
  - la firma digitale
  - il certificato della chiave pubblica

Generazione della firma digitale

Verifica della firma digitale

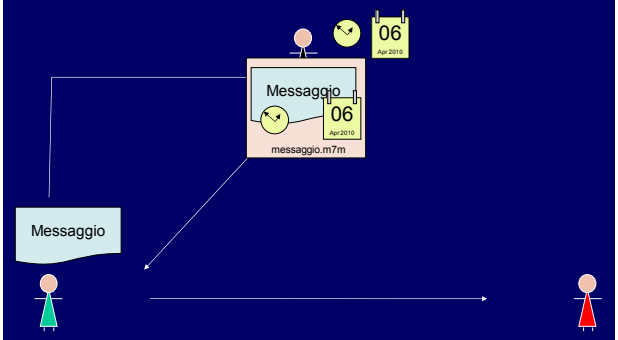
- Si decifra la firma digitale con la chiave pubblica del mittente, contenuta nel certificato allegato; si ottiene così l'impronta in precedenza generata dal mittente del documento
  - l'esito positivo di questa operazione assicura l'autenticità dell'origine dei dati
- Si genera l'impronta hash del documento informatico ricevuto utilizzando la stessa funzione di hash precedentemente utilizzata dal mittente
  - Le due impronte vengono confrontate.
  - L'uguaglianza tra esse dà garanzia di integrità



Marca temporale

- La procedura di marcatura temporale serve ad attestare l'esistenza di un documento informatico rispetto ad una data certa
- Tale procedura, che deve essere resa disponibile ai propri titolari di firma digitale da ogni certificatore, prevede la generazione di una marca temporale che fornisce un riferimento temporale opponibile ai terzi atto a dimostrare l'esistenza di un documento informatico in un dato momento.
  - Necessaria partecipazione di una terza parte fidata
    - Time Stamping Authority (TSA)
  - Un file marcato temporalmente ha estensione .m7m (ad es. simulazione.txt.m7m) e include:
    - Documento del quale si è chiesta la validazione temporale
    - Marca temporale emessa dall'Ente Certificatore

Marca temporale



Sigillo elettronico

Gli strumenti informatici che realizzano il concetto di sigillo elettronico sono:

✓ **HASH**

✓ **FIRMA DIGITALE**

✓ **MARCA TEMPORALE**

Sigillo elettronico

Strumenti informatici che attualmente realizzano le modalità introdotte dalla L. 48/08 (Rat. Convenzione di Budapest):

✓ **SUPPORTI OTTICI** (CD, DVD… non riscrivibili)

✓ **HASH**

✓ **FIRMA DIGITALE**

✓ **MARCA TEMPORALE**

Sigillo elettronico (un po' meno elettronico)

E se non abbiamo a disposizione la firma digitale e la marca temporale?

PIANO B

- ✓ **COPIA FILE**
- ✓ **HASH stampato su carta**
- ✓ **TIMBRO e FIRMA AUTOGRAFA del procedente**

Software per l'analisi forense dei dati digitali

Digital Evidence & Forensics Toolkit

Open Source Software
Gratuito
Manuali in italiano

http://www.deftlinux.net

Esigenze di ordine giuridico

Il fine dell'attività tecnica è consentire
la disponibilità per tutte le parti processuali

per l'utilizzabilità nel procedimento penale (in senso lato)

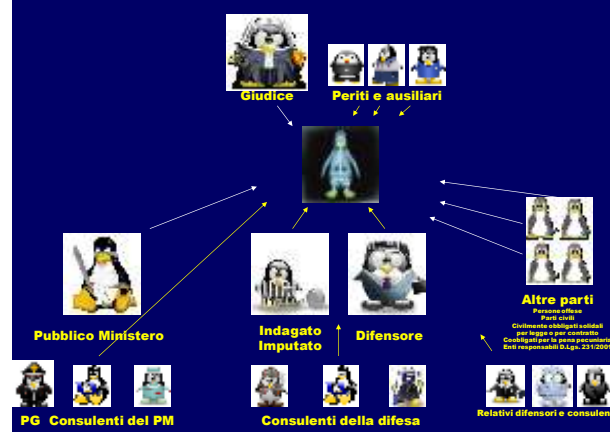
dei dati,
informazioni,
rappresentazioni digitali
dei dati accessori di sistema e/o esterni

integri e completi

al fine della valutazione di ogni fatto giuridicamente rilevante,

sostanziale e/o processuale

I DATI RIS-PACS INTERESSANO A TUTTE LE PARTI DEL PROCESSO



NUOVE FRONTIERE DELL'IF SUI RIS-PACS

Formazione complementare
dei TSRM su
normativa, tecniche, procedure e tools
di Informatica Forense
sui dati RIS-PACS

INFORMATICA FORENSE
SUI
DATI RIS-PACS IN
CLOUD COMPUTING

INFORMATICA FORENSE
SUI DATI RIS-PACS
CON IL
CLOUD COMPUTING

VI RINGRAZIO PER L'ATTENZIONE

avvocato@gammarota.it

Si ringrazia il Dott. Michele Ferrazzano dell'Università di Bologna (www.informaticaforense.it) per aver amichevolmente consentito l'adattamento e l'uso dei suoi lucidi sugli strumenti tecnici per l'attuazione della L. 48/08

E' vietata ogni riproduzione di questa presentazione senza preventivo consenso dell'autore

Questa presentazione è dedicata al personale ed ai tecnici di radiologia medica del Policlinico Ospedale S. Orsola-Malpighi di Bologna, perchè sanno prendersi cura dei bambini del reparto di Pediatria "G. Gozzadini" di Bologna non solo con grande professionalità, ma soprattutto con dolci sorrisi ed inesauribile pazienza.

http://www.xraythai.com/webboard/index.php?action=vthread&forum=13&topic=4478

WWW.AGEOP.ORG

Gradite donazioni per la Casa Siepelunga
Associazione Genitori Ematologia Oncologia Pediatrica
A.G.E.O.P. RICERCA ONLUS
UNICREDIT BANCA: IT16Y0200802483000101054378