ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Definizione, obiettivi e metodi dell'Informatica forense

Master ICT Law

Lezione #1

Raffaella Brighi
(Alma Human AI – CIRSFID)

Prof.ssa di Informatica giuridica e di Informatica forense
Direttrice del Master
in Trattamento dei dati personali e Privacy Officer

1

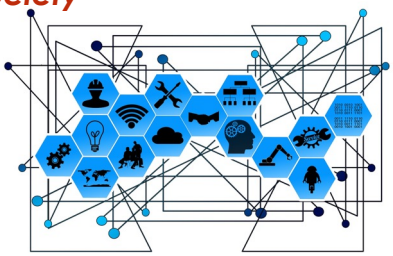
Processi e prove informatiche
Parte I

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

2

Le tracce digitali nella *Data Society*

- Ciascun sistema che tratti dati digitali può essere esaminato a supporto dell'attività investigativa o più in generale per trarne informazioni che, se correttamente acquisite e analizzate, possano essere utilizzate come elemento di prova in un procedimento giudiziario.



Le tracce digitali prodotte dagli strumenti IT sono di diverso tipo:

- alcuni prodotti consapevolmente dalle persone
- altri nascosti generati automaticamente dai sistemi: file generati dalle applicazioni installate, informazioni gestite dal sistema operativo, log dei dispositivi di rete, frammenti di file cancellati ecc.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

3

Processi e prove informatiche

- Investigazioni, indagine, difesa e giudizio in **procedimenti penali** (reati informatici, reati commessi con sistemi informatici, reati comuni cui si rilevano indizi nei sistemi informatici).

- Inoltre:

  Nel **processo civile**, in ambito **giuslavoristico**, in materia di diritto **amministrativo**, ecc.:

  Corporate Digital forensics (investigazioni aziendali)

  Informatica forense sanitaria e **clinical risk managment**

Elemento comune e unificante:

il dato digitalizzato come oggetto di indagine

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

4

EU SOCTA 2021 – Il crimine organizzato in Europa e l'uso della tecnologia

The use of technology is a key feature of serious and organised crime in 2021. Criminals exploit encrypted communications to network among each other, use social media and instant messaging services to reach a larger audience to advertise illegal goods or to spread disinformation. The online environment and online trade provide criminals access to expertise and sophisticated tools enabling criminal activities.

Europol (2021), European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg.

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

5

Le indagini informatiche

- Le indagini informatiche si distinguono da quelle tradizionali per:
  - Dimensione transnazionale
    Problemi di cooperazione giudiziaria che richiedono un aggiornamento degli strumenti per la raccolta trasnazionale delle prove e uno sforzo di armonizzazione degli strumenti investigativi per evitare un far west tecnologico
  - Lesività della riservatezza e della sicurezza dei dati
    Diventano potenzialmente oggetto di analisi tutti quei dati che costituiscono il patrimonio informativo della persona e che coesistono in modo promiscuo negli spazi digitali
  - Tendenza ad assumere un carattere *esplorativo- proattivo* piuttosto che di repressione
  - Necessità di intermediazione dei provider di servizi

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

6

(segue) ostacoli tecnici

- I dati informatici sono facilmente alterabili, manipolabili e difficili da archiviare.
- Sorgenti di dati sempre più ampie ed eterogenee
- Architetture distribuite
- Nuove sofisticate forme di attacco
- Ubiquità dei sistemi di archiviazione
- Le sorgenti digitali possono contenere informazioni parziali, incomplete o ambigue rispetto all'ambiente che, solo combinate con altri dati, diventano elementi di prova in dibattimento.

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

7

(segue) un continuo bilanciamento

Sorge la necessità di conciliare innovazioni scientifiche e rispetto delle regole processuali, nello sforzo continuo di salvaguardare due opposte esigenze:

- l'accertamento del fatto
- la tutela dei diritti fondamentali degli individui coinvolti nell'accertamento

- La prospettiva dell'attività tecnica, in questo contesto, è quella della *utilizzabilità* in dibattimento – a disposizione di tutte le parti processuali per la valutazione di ogni aspetto rilevante – a garanzia dell'esercizio del diritto di difesa e a tutela dei diritti fondamentali dei soggetti coinvolti.
- Tutte le parti coinvolte nel processo devono poter valutare se sono stati seguiti metodi scientifici e appropriati ed essere in grado di eseguire i processi descritti nella documentazione giungendo ai medesimi risultati

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

8

L'Informatica forense

L'informatica forense è la scienza forense che definisce le modalità di individuazione, acquisizione e interpretazione dei dati digitali da dispositivi informatici e reti perché possano essere valutati come prova nel procedimento.

Si tratta di individuare le modalità migliori per acquisire le prove senza alterarle o modificare il sistema informatico su cui si trovano e garantire che le prova acquisite siano identiche a quelle originali.

Si colloca nell'ambito dell'informatica giuridica.

[MAIOLI, C., *Dar voce alle* prove: elementi di informatica forense, in Crimine virtuale, minaccia reale, Franco Angeli, Milano, 2004]

9

Contesto

Informatica forense ≠ sicurezza informatica

IL PRESENTE MATERIALE È RISERVATO AL PERSONALE DELL'UNIVERSITÀ DI BOLOGNA E NON PUÒ ESSERE UTILIZZATO AI TERMINI DI LEGGE DA ALTRE PERSONE O PER FINI NON ISTITUZIONALI

10

Chiarificazione terminologica: dalla computer forensics alla digital forensics

- A seconda dei dispositivo oggetto di analisi o delle modalità di raccolta dei dati l'informatica forense può essere meglio classificata in varie specializzazioni:
  - **Disk forensics:** è la principale e più antica area dell'informatica forense, a cui spesso ci si riferisce con il termine computer forensics. Riguarda l'analisi di supporti informatici di memorizzazione (hard disk, chiavette USB, CD-ROM, ecc.)
  - **Network forensics**: con lo sviluppo delle reti di computer il potere informativo del singolo dispositivo tende a ridursi. La net forensics allarga l'ambito di indagine a sistemi remoti o virtuali seguendo il percorso del dato durante la trasmissione.
  - **Cloud forensics**: ambiente in cui l'elaborazione distribuita dei dati, la mancanza di accesso fisico alle memoria di massa, la coesistenza di dati di soggetti non coinvolti, fa emergere diverse problematiche nel momento in cui si cerca di adottare gli standard

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

11

(segue)

- **Mobile forensics**: ha come oggetto di indagine i dispositivi mobili e si può dividere in SIM CARD forensics(contenuto della SIM), Mobile Handset forensics (contenuto del dispositivo), Memory Card Forensics (cheda di espansione di memoria); Cellsite Forensics (tabulati telefonici)
- **Embedded Forensics**: analisi dei numerosi strumenti digitali che possono contenere tracce utili ai fini di una indagine (Playstation, braccialetti elettronici, scatole nere..)
- ….
- **Social Network Analsys**: applicazione di metodi di acquisizione forense dei dati e delle informazioni rivenienti dalla SNA finalizzata a analisi delle interazioni sociali e identificazione degli individui all'interno della comunità
- **Blockchain Forensics**
- **Artificial Intelligence Forensics**

L'oggetto di studio è sempre la digital evidence

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

12

La Cyber Intelligence

- Fornisce supporto alle decisioni strategiche o operative: raccoglie quanti più dati possibili, li analizza con logiche e criteri ben precisi estraendo informazioni; valuta fonti; formula ipotesi ed elabora risultati
- Tecniche:
  - Discovery Knowledge
  - Big Data Analytics
  - OSINT: Open Source Intelligence
  - Intelligenza artificiale
  - …

Capacità di previsione

Diventano potenzialmente oggetto di analisi tutti quei dati che costituiscono il patrimonio informativo della persona e che coesistono negli spazi digitali

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

13

Gli attori (processuali e non)

- Studiosi di Informatica, Informatica giuridica, procedura penale
- Magistrati e avvocati
- Forze dell'ordine (PG, Guardia di finanza, ecc.)
- Consulenti (esperti informatica forense)
  - Consulente Tecnico del Pubblico Ministero;
  - Consulente Tecnico di Parte dell'imputato/indagato, delle parti civili, delle
  - parti offese;
  - Perito del Giudice;
  - Ausiliario di P.G.
  - Consulente Tecnico d'Ufficio del Giudice;
  - Consulente Tecnico di Parte

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

14

Multidisciplinarietà

- La corretta applicazione delle norme giuridiche impone a ogni operatore forense (magistrati, avvocati, polizia giudiziaria, ma anche a cancellieri, custodi, consulenti, periti, ecc.) l'obbligo di informazione, formazione e aggiornamento in campo informatico, informatico-giuridico e informatico forense.

- D'altro canto ogni informatico forense, oltre ad una profonda preparazione tecnica, deve conoscere con precisione il quadro giuridico delle sue attività e quindi i principi di diritto sostanziale, di diritto processuale ed in particolare il regime dei mezzi di prova e di ricerca della prova, per evitare errori talvolta irrimediabili.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

15

Prove informatiche e cattiva scienza
Parte II

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

16

Scienza e verità

- Nel novero delle scienze forensi si comprendono oggi molte discipline, ognuna delle quali con metodi e paradigmi differenti: con **differenti tecniche**, differenti **gradi di affidabilità**, differenti **livelli di errore** e diverso **grado di accettazione** da parte della comunità scientifica.
- A fronte dell'eterogeneità delle discipline impiegate, accade però che molte delle tecniche utilizzate non siano basate su un corpo di conoscenze che riconosce le limitazioni alla base dei principi scientifici.
- Alcune di queste possono non avere una base di ricerca ben sviluppata o non sono sviluppate all'interno del dominio della *scienza*.

Quale scienza è utilizzabile nel processo?
Esiste solo una scienza buona o anche una scienza cattiva?
[Taruffo, 2009]

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

17

Lo scienziato forense

- Il giudice, al momento del processo, si trova ad accertare fatti la cui conoscenza presenta caratteristiche di natura scientifica, per le quali è costretto a farsi coadiuvare da esperti delle varie scienze. Le prove scientifiche vengono spesso presentate da un testimone esperto (expert witness)
- Gli scienziati forensi hanno a che fare con la raccolta, la conservazione e l'analisi delle prove scientifiche nel corso di un'indagine. Mentre alcuni scienziati forensi si spostano sul scena del crimine per raccogliere le prove, altri svolgono un ruolo puramente di laboratorio, per le analisi sugli oggetti portati loro
- Oltre al loro ruolo di laboratorio, gli scienziati forensi testimoniano come esperti (expert witnesses), in casi penali e civili, e possono lavorare sia per l'accusa sia per la difesa
- A causa della loro posizione, gli scienziati forensi dovrebbero mantenere un alto livello di integrità e rigorosi orientamenti etici per quanto riguarda il loro lavoro

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

18

L'ingresso della prova informatica nel processo

- L'ingresso della prova scientifica nel processo ha sempre rappresentato motivi di acceso dibattito 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.
- Stranamente questo non è accaduto per la c.d prova informatica che è entrata nei processi dalla porta principale come se fosse già uno strumento consolidato.
- Questo probabilmente avviene per la confidenza e una certa superficialità che oggi tutti abbiamo verso l'impiego delle nuove tecnologie in ogni ambito della nostra vita.
- Tuttavia **l'informatica non sfugge dalla fallibilità di tutte le altre discipline scientifiche.** L'elevata connotazione specialistica, insieme alla facilità di manipolazione e alterazione dei dati, espone al rischio di introduzione della *junck science*

- *«I bit sotto tortura confessano qualunque cosa»*

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

19

Appartengono a un passato recente…

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

- [Monti, 2003]

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

20

Tipici problemi

- Raccolta di dati effettuata con imperizia
  - System administrator e tecnici che aiutano gli investigatori e che hanno scarsa sensibilità forense
- Distruzione delle prove da parte dei primi intervenuti sul luogo del crimine
  - Forze di polizia non sensibili alla necessità di mantenere l'integrità del dato possono danneggiare i dati e lasciare che i dati vengano eliminati dai male intenzionati

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

21

Casi rappresentativi

Casi sulla rilevanza dell'adozione o meno di tecniche per la corretta acquisizione dei dati:

- Caso Vierika (Trib. Di Bologna, 2005; Corte d'appello 2008)
  - accesso abusivo a sistema informatico e telematico e danneggiamento con diffusione di virus (615 ter e quinquies c.p.)
  - sequestro del materiale detenuto dal provider effettuato, per delega, da tecnici del provider (pagine web e file di log)
  - indagini e copie di file sul computer sequestrato effettuate con software dell'indagato (privo di licenza) sul computer dell'indagato
  - competenze dichiarate (senza ironia) da personale inquirente: "ho l'ECDL"
- Caso Garlasco (sentenza del Tribunale di Vigevano)
  - Ricognizione del materiale (nessun accertamento tecnico) in luogo di procedure che meglio si sarebbero sposate al caso concreto quali **l'ispezione, la perquisizione, il sequestro**
  - Conseguenze: **compromissione prove**
    - su 56.000 file, 39.000 erano stati acceduti
    - 1.500 file erano stati modificati
    - 500 file creati
  - Alterazione del supporto informatico

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

22

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 ?

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

23

Verso un approccio integrato

- Convergenza verso una base normativa sovranazionale e riformulazione delle norme processuali tenendo conto delle innovazioni tecnologiche
- Un approccio epistemologico più attento alle fasi precedenti al processo e al contesto di riferimento
- Protocolli operativi aggiornati e testati, standard metodologici rigorosi in tutte le fasi del processo (norme ISO, best practices, linee guida)
- Istituzione di centri specializzati per la gestione delle prove informatiche
- Formazione interdisciplinare

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

24

Il dato informatico a uso forense
Parte III

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

25

Proprietà del dato informatico

- Alcune caratteristiche fisiche

Codifica binaria
Volatilità
Facilità di alterazione
Impossibilità di individuare alterazioni
Perfetta replicabilità

- Da cui derivano difficoltà/problematiche legate a

Interpretazione
Attendibilità
Paternità

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

26

Il concetto di informazione

- L'informazione non esiste senza un supporto fisico.
- Ogni supporto ha le sue proprie caratteristiche.
- La stessa informazione può essere scritta su supporti differenti.
- Uno stesso supporto può portare informazioni differenti.
- L'informazione richiede un supporto fisico ma non coincide con esso (entità logiche vs entità fisica)
- L'insieme delle regole con cui si stabiliscono le corrispondenze che consentono di leggere informazioni da un supporto e di scrivere informazione su un supporto si chiama *linguaggio*.

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

27

Livelli di rappresentazione dell'informazione

Livello sintattico: combinazione dei simboli a prescindere dal loro significato. Dipende dalle caratteristiche fisiche del supporto (oggettiva)

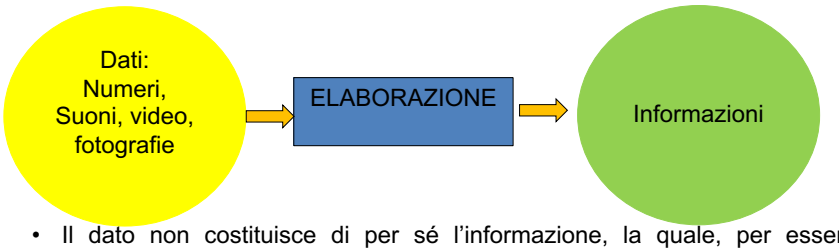
Livello semantico: corrispondenza tra segni e significato (se il destinatario è in grado di associare ai segni un senso)

Livello pragmatico: interpretazione/comprensione dell'informazione (valore)

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

28

Il dato e l'informazione



- Il dato non costituisce di per sé l'informazione, la quale, per essere desunta, necessita di un'ulteriore attività che si rapporti al dato.
- Quando sappiamo cosa rappresenta un certo dato allora abbiamo l'informazione
- L'elaborazione di più dati consente di ottenere una o più informazioni, che vengono a loro volta utilizzate per raggiungere altri scopi. Per esempio, il dato numerico 20 non ha alcun significato da solo, ma ne assume uno se viene associato al fattore "età".

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

29

Il calcolatore e la codifica dell'informazione (1)

- Dati e istruzioni devono essere memorizzati in un formato adatto a un elaboratore automatico.
- Gli attuali calcolatori impiegano per la memorizzazioni dei dati e delle istruzioni dispostivi, detti bitstabili, in grado di assumere stabilmente una configurazione scelta tra due differenti (es. presenza o assenza di tensione elettrica): un alfabeto di questo genere è detto **alfabeto binario**.
- A ciascuno dei due stati è associata una cifra binaria, detta **bit.**
- Il BIT:
  - Può avere solo valore 0 e 1
  - È l'unità elementare di informazione memorizzabile in un elaboratore
  - Il suo valore corrisponde a un possibile stato di un dispositivo bitstabile
    - 1 = Tensione alta e 0 = Tensione bassa; ecc.

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

30

Il calcolatore e la codifica dell'informazione (2)

- Due fasi:
  - l'entità informazionale viene trasformata in un'altra entità informazione in alfabeto binario
  - L'entità di informazione in binario viene scritta sul supporto fisico (es. sequenza di lampadine)
- Un bit permette di distinguere tra loro solo due entità informative (o elementi, possibilità) rappresentate dai valori 0 e 1 (SI/NO, Vero/falso, M/F)
- Per codificare un numero superiore di elementi è necessario utilizzare sequenze di bit. In questo modo aumentano le possibili combinazioni.
  - Es. 2 bit danno 4 combinazioni di stati: 00, 01, 10, 11
- **Il numero di bit utilizzati determina il numero di simboli disponibili per la rappresentazione dei valori**

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

31

Il calcolatore e la codifica dell'informazione (3)

- Dati numerici, testi, immagini, suoni e qualsiasi tipologia di dato possono essere scritti in forma binaria stabilendo una corrispondenza tra cifre binarie e ciò che rappresentano: ovvero una *codifica*.
- E' necessario adottare una *codifica* per ogni tipo di dato:
  - Numeri in base decimale (1234676980)
  - le 26 lettere maiuscole e minuscole (a,b,c, …. A, B, C,…)
  - Il simboli di interpunzione (:,.+-*=)
  - Immagini in bianco e nero o a colori
  - Audio e video
- Una codifica si dice **standard** quando consiste in un accordo preventivo che stabilisce una volta per tutte l'associazione tra caratteri e simboli (cioè sequenze di bit)
- ASCII (8 bit), oggi Unicode (4 byte, di cui 1 byte compatibile con ASCI UTF-8)

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

32

Codice ASCII per la rappresentazione di caratteri alfanumerici

Binario	Oct	Dec	Hex	Glifo	Binario	Oct	Dec	Hex	Glifo	Binario	Oct	Dec	Hex	Glifo
010 0000	040	32	20	Spazio	100 0000	100	64	40	@	110 0000	140	96	60	`
010 0001	041	33	21	!	100 0001	101	65	41	A	110 0001	141	97	61	a
010 0010	042	34	22	"	100 0010	102	66	42	B	110 0010	142	98	62	b
010 0011	043	35	23	#	100 0011	103	67	43	C	110 0011	143	99	63	c
010 0100	044	36	24	$	100 0100	104	68	44	D	110 0100	144	100	64	d
010 0101	045	37	25	%	100 0101	105	69	45	E	110 0101	145	101	65	e
010 0110	046	38	26	&	100 0110	106	70	46	F	110 0110	146	102	66	f
010 0111	047	39	27	'	100 0111	107	71	47	G	110 0111	147	103	67	g
010 1000	050	40	28	(	100 1000	110	72	48	H	110 1000	150	104	68	h
010 1001	051	41	29	)	100 1001	111	73	49	I	110 1001	151	105	69	i
010 1010	052	42	2A	*	100 1010	112	74	4A	J	110 1010	152	106	6A	j
010 1011	053	43	2B	+	100 1011	113	75	4B	K	110 1011	153	107	6B	k
010 1100	054	44	2C	,	100 1100	114	76	4C	L	110 1100	154	108	6C	l
010 1101	055	45	2D	-	100 1101	115	77	4D	M	110 1101	155	109	6D	m
010 1110	056	46	2E	.	100 1110	116	78	4E	N	110 1110	156	110	6E	n
010 1111	057	47	2F	/	100 1111	117	79	4F	O	110 1111	157	111	6F	o
011 0000	060	48	30	0	101 0000	120	80	50	P	111 0000	160	112	70	p
011 0001	061	49	31	1	101 0001	121	81	51	Q	111 0001	161	113	71	q
011 0010	062	50	32	2	101 0010	122	82	52	R	111 0010	162	114	72	r
011 0011	063	51	33	3	101 0011	123	83	53	S	111 0011	163	115	73	s
011 0100	064	52	34	4	101 0100	124	84	54	T	111 0100	164	116	74	t
011 0101	065	53	35	5	101 0101	125	85	55	U	111 0101	165	117	75	u

33

Codifica di immagini

- Anche le immagini vengono codificate come una sequenza di bit
- Il passaggio da un'immagine a una sequenza binaria prende il nome di digitalizzazione
- Un'immagine viene vista come un insieme di punti (pixel) giacenti su una griglia bidimensionale
- Ad ogni punto viene associata un insieme di bit che ne codificano il colore o la tonalità di grigio (per bianco e nero)
- Risoluzione: numero di punti rappresentati per unità di superficie

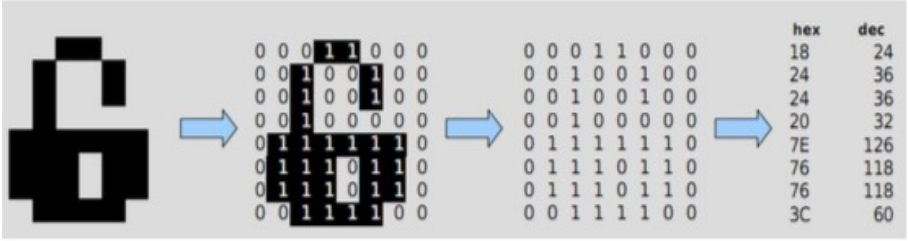
ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

34

[Cfr. Di Ruscio, *http://www.di.univaq.it/diruscio/infIntro/Lezione4.pdf*]

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

35



[Cfr. Di Ruscio, *http://www.di.univaq.it/diruscio/infIntro/Lezione4.pdf*]

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

36

Codifica di suoni

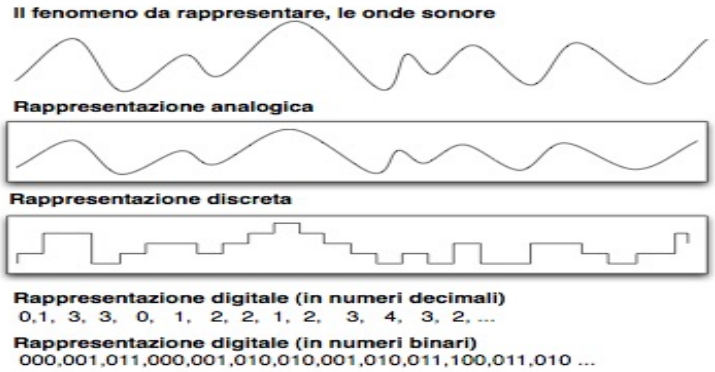


Figura 2.16: *Rappresentazioni analogiche e digitali*

Per digitalizzare un'informazione continua dobbiamo convertire i dati in bit. Occorre campionare il segnale, ovvero misurarne il valore a intervalli regolari

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

37

0100000101001111

- Numero in base 10 **16719**
- Numero in base 16 **414F**
- Testo ASCII **AO**
- Pixel bianchi e neri

I bit possono rappresentare qualsiasi tipo di informazione

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

38

Proprietà del dato informatico (1)

I bit forniscono informazioni solo se correttamente interpretati

i dati non sono fruibili se non se ne conosce il *senso*

dati generati da software non più attuali diventino illeggibili; lo stesso accade a causa della rapida obsolescenza a cui è soggetto l'hardware o anche a causa del deterioramento (rottura, perdita) dei dispositivi stessi.

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

39

Attendibilità del dato informatico

Consideriamo la seguente sequenza di bit

01100100 01110100 01101000 01101010

e poi la seguente sequenza di bit

01000011 01101001 01100001 01101111

Non è possibile accertare:
- eventuali modifiche apportate in precedenza a singoli bit
- numero di modifiche intervenute
- autore della modifica
- epoca dell'ultima modifica e delle eventuali modifiche precedenti

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

40

Esempi

- Alterazione dei metadati
- Alterazione contenuto

- Messaggi falsi https://ifaketextmessage.com

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

41

Esempio: post diffamatori su Facebook

Come può essere provata l'avvenuta diffamazione on line?

Cosa occorre provare?

- Il contenuto e le date
- La riconducibilità al presunto autore
- Quale pubblico ha avuto accesso al contenuto diffamatorio

Come?

- La stampa del messaggio contenente le frasi diffamatorie può bastare processualmente a dimostrare l'avvenuta diffamazione online e l'autore della diffamazione?
- È attendibile la copia conforme di una pagina web fatta da un notaio?

- ➢ Cristallizzare il contenuto del messaggio per impedirne l'alterazione
- ➢ Stabilire un collegamento forense adeguato tra elemento informativo e identità fisica

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

42

Proprietà del dato informatico (2)

Presa una sequenza di bit non è possibile accertare:

- Eventuali modifiche apportante in precedenza al singolo bit
- Numero di modifiche intervenute
- Autore della modifica
- Epoca dell'ultima modifica e delle eventuali modifiche precedenti

Gravi ripercussioni sui profili riguardanti l'**integrità** e la **paternità** del dato

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

43

Proprietà del dato informatico (3)

I dati possono essere **riprodotti e replicati infinite volte**, copiando la sequenza di bit (perfetta riproducibilità).

La copia digitale è IDENTICA all'originale.

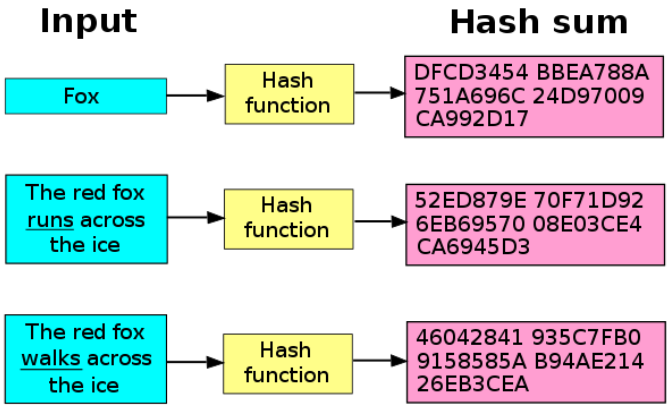
- *Esempio: si veda la differenza tra copia di documento informatico e duplicato di documento informatico (ai sensi di art. 23 bis CAD)*
- *Funzione di Hash per garantire l'integrità*

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

44

La funzione di Hash

- Sono algoritmi che associano **unidirezionalmente** una stringa di lunghezza arbitraria con una stringa di bit di lunghezza fissa.



ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

45

Proprietà della funzione di hash

- Dato un messaggio, la funzione restituisce sempre lo stesso hash
- E' sempre possibile calcolare l'hash in modo veloce, indipendentemente dal contenuto del messaggio stesso
- Non deve essere possibile generare un messaggio a partire dal suo hash
- Un cambiamento in un messaggio porta alla generazione di un nuovo hash scorrelato da quello del messaggio di partenza
- E' estremamente difficile trovare due messaggi che generino lo stesso hash

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

46

Organizzazione logica e fisica dei dati informatici

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

47

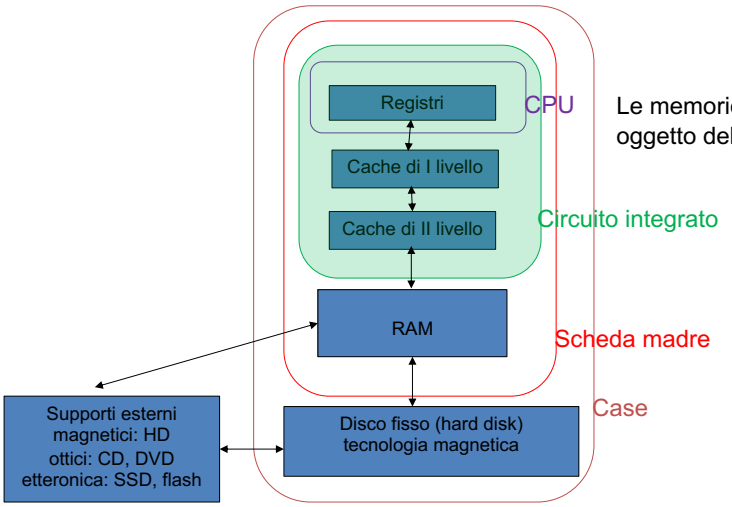
L'organizzazione dei dati: dati volatili e dati persistenti

- I dati possono essere:
  - memorizzati nella **memoria centrale** e quindi "**volatili**". La memoria centrale agisce come supporto alla CPU, cui deve fornire dati e istruzioni a alta velocità
  - memorizzati nelle **memorie di massa** (cd-rom, floppy, hard-disk, nastri, ecc..), cioè archiviati. In questo caso i dati si dicono persistenti (o permanenti) e sono accessibili anche dopo lo spegnimento del calcolatore
- La registrazione dei dati su tali memorie ha
  - un aspetto ***logico***: come il sistema operativo e le applicazioni organizzano le informazioni
  - un aspetto ***fisico***: come i dati sono materialmente disposti nei supporti fisici

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

48

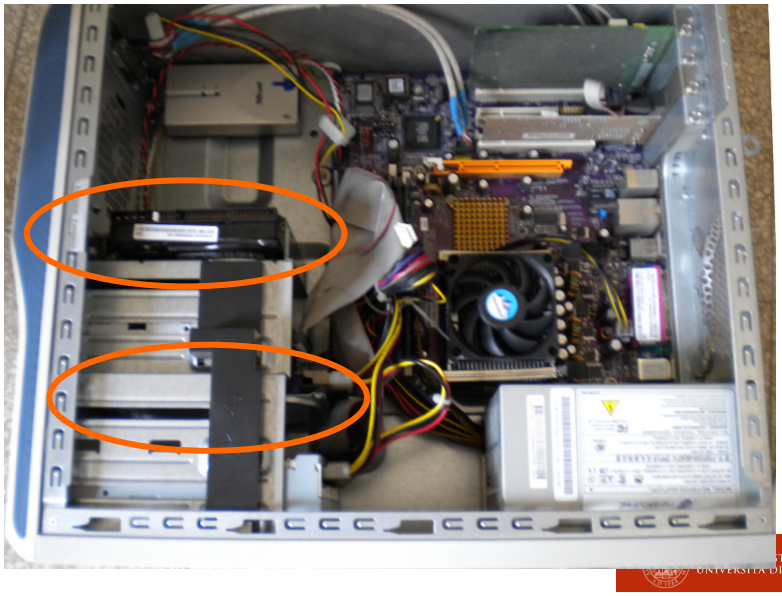
Organizzazione fisica
gerarchia della memoria



Le memorie volatili sono oggetto della *live* forensics

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

49



50

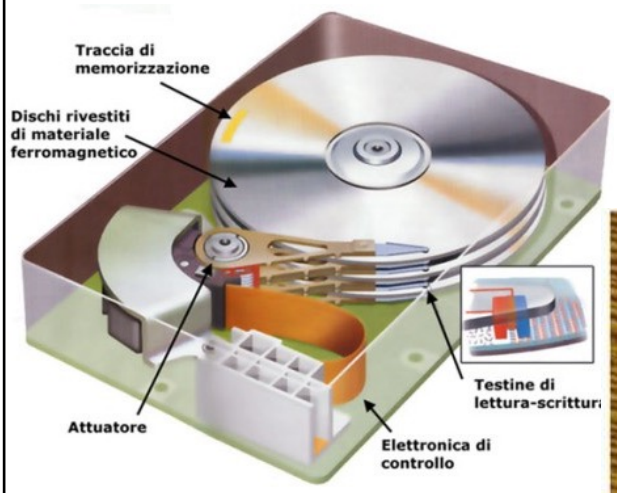
Tipi di supporti di memorizzazione

- **Supporti magnetici**
  - Hard disk magnetico (HDD), floppy disk
- **Supporti elettronici**
  - Unità a stato solido (SSD), chiavette USB
- **Supporti ottici**
  - DVD, CD

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

51

Hard disk magnetico

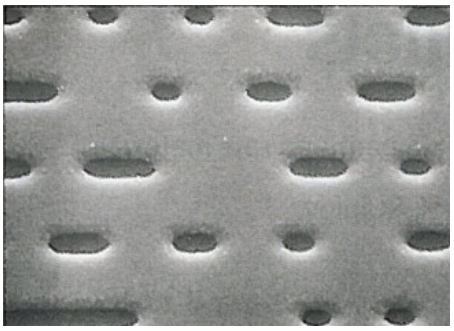


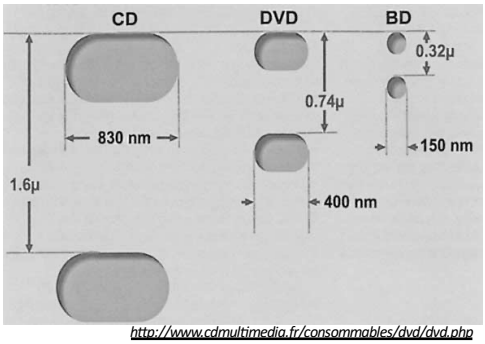
http://tekw.org/wp-content/uploads/2012/09/scheletro-hard-disk.jpg

http://www.asmicro.com/Applications/Scanning-Probe-Materials-Analysis.htm

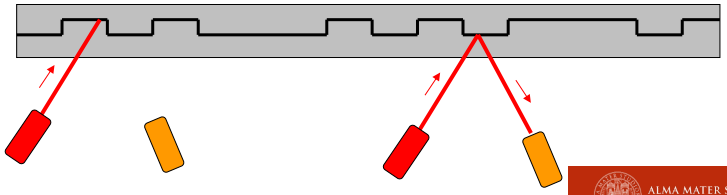
UNIVERSITÀ DI BOLOGNA

52





http://www.cdmultimedia.fr/consommables/dvd/dvd.php



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

53

Fungus eats CD

Spores bore holes in compact disks, rendering them useless.

Xavier Bosch

The pits: fungal attack wipes CD data.

© *Photodisc*

Computers get viruses. Code gets bugs. Now CDs get fungus. Researchers in Spain have discovered a fungus that eats holes in compact discs, corrupting the information stored in them.

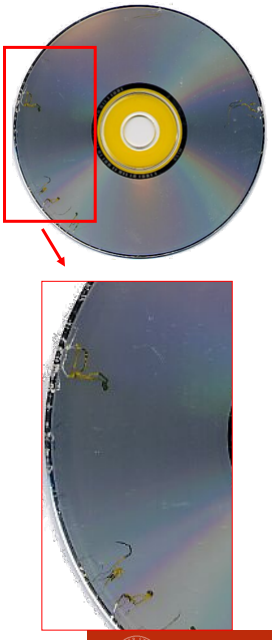
After visiting Belize in Central America, Victor Cardenes of Madrid's National Museum of Natural Sciences (MNCN), found one of his CDs discoloured, transparent and unreadable.

The disk's aluminium and polycarbonate layers were riddled with fungus, Cardenes and his colleagues have discovered.

The team has isolated and cultured what they believe to be Geotrichum candidum. Usually, this fungus lives on plants and animals. Occasionally it infects the human respiratory tract. DNA analysis is pending.

Burrowing in like worms from the side of the disk, "the fungus destroyed crucial information pits", says team-member Javier Garcia-Guinea. Pits in a CD's aluminium and polycarbonate sandwich store binary data, which is read by a laser.

Some fungi are known to live on plastics and polymers, but this is the first report of a CD being eaten by a fungus. The researchers believe that the spores probably entered the CD in Belize.



http://www.nature.com/news/2001/[illegible].html

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

54

L'organizzazione logica dei dati: *file* e *file system*

- Il **file system** è un componente del **sistema operativo** deputato a gestire in modo efficiente la memoria di massa, con l'obiettivo di presentare all'utente nel modo più semplice possibile l'organizzazione logica dei dati e le operazioni su essi:
  - Recupero di dati precedentemente memorizzati
  - Cancellazione/eliminazione di dati
  - Modifica/aggiornamento di dati
  - Copia di dati da una unità all'altra
- I dati contenuti nelle memorie di massa vengono strutturati e gestiti in modo efficiente mediante la loro organizzazione in ***file,*** contenitori logici identificati da un nome per facilitare le operazioni dell'utente.
- Il file è il livello più basso dell'organizzazione logica dei dati.
- I file sono collocati in contenitori logici chiamati cartelle o directory secondo una struttura a albero

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

55

L'organizzazione logica dei dati: *file* e *file system*

- Il file è il livello più basso dell'organizzazione logica dei dati.
- I file sono collocati in contenitori logici chiamati cartelle o directory secondo una struttura a albero
- Tramite il file system ciascun utente può organizzarsi una zona di memoria di massa e garantire che i suoi file siano protetti da accessi esterni o anche condivisi con più utenti.
- In sistemi che prevedono la condivisione di risorse da parte di più utenti, il s.o. introduce meccanismi di protezione e politiche di risoluzione di eventuali conflitti d'uso - **Gestione degli utenti** (controllo degli accessi).
- **Il file system conserva oltre ai dati altre importanti informazioni: la struttura stessa del file system, informazioni sui file (**dati di creazione, accesso modifica del file, politiche di accesso, dimensione, localizzazione)

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

56

L'organizzazione logica dei dati: *file* e *file system*

- A livello di file system non vi è un binomio indissolubile tra dato e file
- Modalità logiche di organizzazione dei dati da parte delle applicazioni:
  - strutturata: insieme di schede dotate della medesima struttura per memorizzare e gestire dati dello stesso tipo (es. tabelle, rubrica telefonica). Strumenti: file strutturati, foglio di calcolo, marcatura (XML) e ontologie informatiche, database, mail boxes, ecc.
  - non strutturata: sequenze non strutturate di caratteri alfanumerici (es. testi). Strumenti: wordprocessor, Information retrieval
- Milioni di record di dababase server o la posta elettronica in formato mbox possono essere contenuti in pochi file o di contro lo stesso dato (un filmato o un backup) può essere spezzettato in più file.
- Il dato descritto a livello di file system è un file non necessariamente coincidente con il dato prodotto dall'applicazione.

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

57

L'organizzazione fisica dei dati

- I dati sulla memoria di massa vengono gestiti in blocchi di piccole dimensione (cluster).
- Il cluster è l'unità minima che il file system può allocare: talvolta coincide con un settore fisico dell'HD talvolta occupa più settori.
- I file di grandi dimensioni vengono spezzettati su più cluster; i file di dimensione minore di un cluster occuperà comunque tutto il cluster

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

58

[M. Ferrazzano]

59

Principali file system

- **File Allocation Table (FAT)**
  - Microsoft Windows, dispositivi portatili
- **New Technology File System (NTFS)**
  - Microsoft Windows
- **Hierarchical File System (HFS)**
  - Apple Macintosh
- **Third Extended File System (EXT3)**
  - Linux
- **Universal Disc Format (UDF)**
  - Dispositivi ottici (CD, DVD)

- Si differenziano per logica di funzionamento, dimensione dei cluster, *journaling* (registro delle operazioni che ha la funzione di evitare situazioni di incoenrenza) ecc.

60

File system: allocazione dei file

Indice

...

Settori

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

...

61

File system: allocazione dei file

Indice

A												

...

Settori

AAAAA1AAAAA	AAAAA2AAAAA	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

...

62

File system: allocazione dei file

Indice

A	B											

...

Settori

AAAAA1AAAAA	AAAAA2AAAAA	3	4	5
6	7	8	9	10
11	12	13	BBBBB14BBBBB	BBBBB15BBBBB
BBBBB16BBBBB	BBBBB17	18	19	20

...

63

File system: allocazione dei file

Indice

A	B											

...

Settori

AAAAA1AAAAA	AAAAA2AAAAA	3	4	5
6	7	8	9	10
11	12	13	BBBBB14BBBBB	BBBBB15BBBBB
BBBBB16BBBBB	BBBBB17	18	19	20

...

64

File system: allocazione dei file

Indice

A	B	C										

...

Settori

CCCCCCCCCCCC	CCCC 2 AAAAAA	3	4	5
6	7	8	9	10
11	12	13	BBBBBBBBBBBB	BBBBBBBBBBBB
BBBBBBBBBBBB	BBBBBB 17	18	19	20

...

65

File system: allocazione dei file

Indice

A	B	C										

...

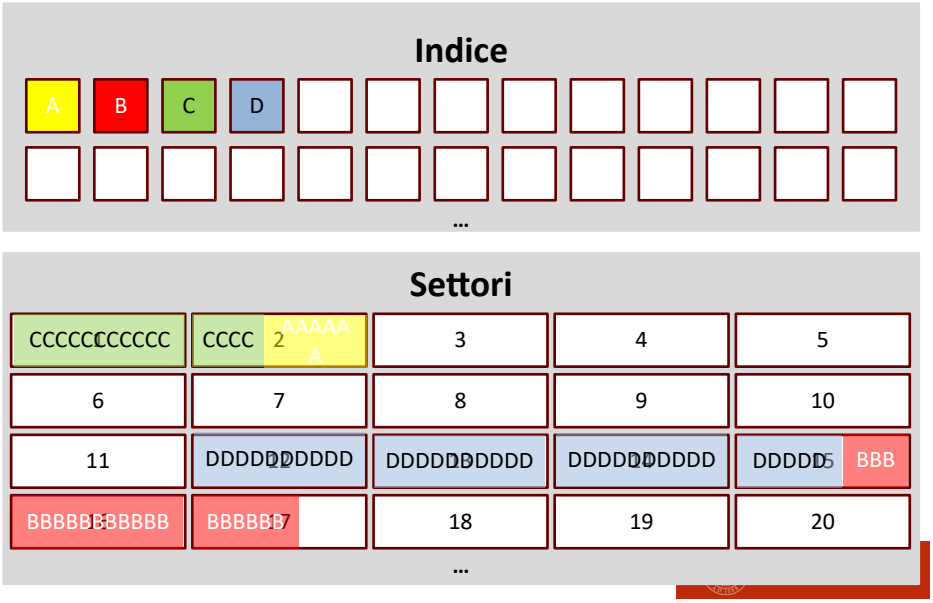
Settori

CCCCCCCCCCCC	CCCC 2 AAAAAA	3	4	5
6	7	8	9	10
11	12	13	BBBBBBBBBBBB	BBBBBBBBBBBB
BBBBBBBBBBBB	BBBBBB 17	18	19	20

...

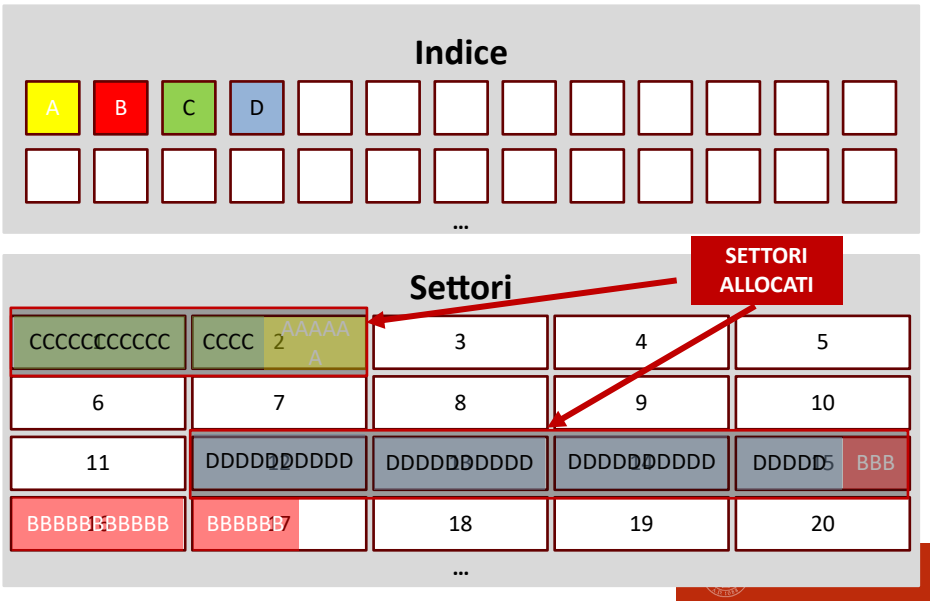
66

File system: allocazione dei file

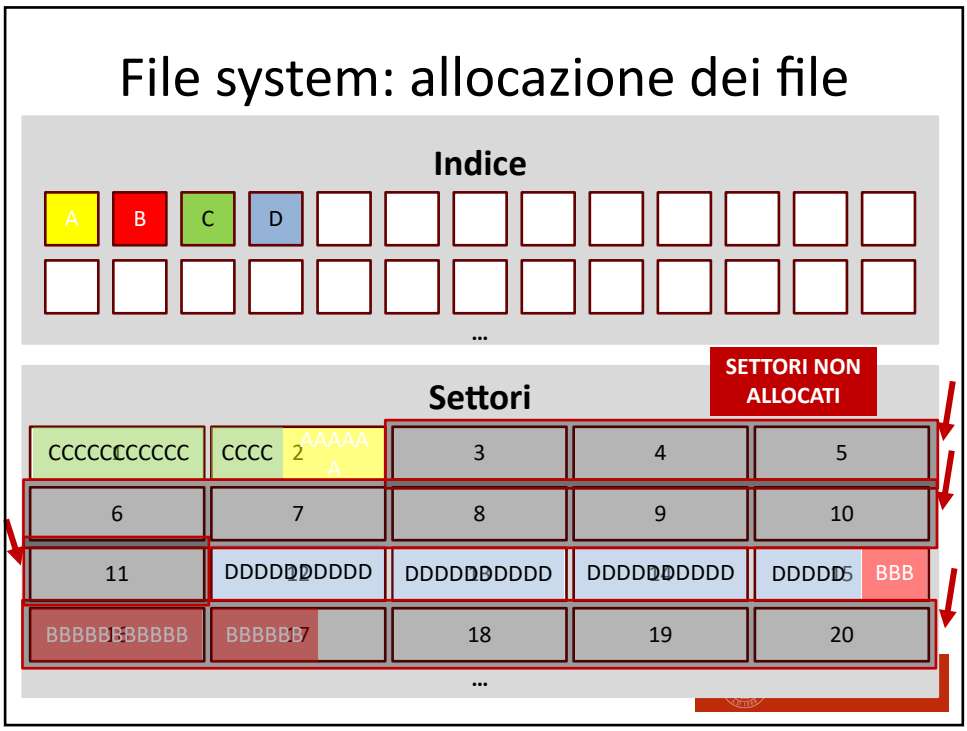


67

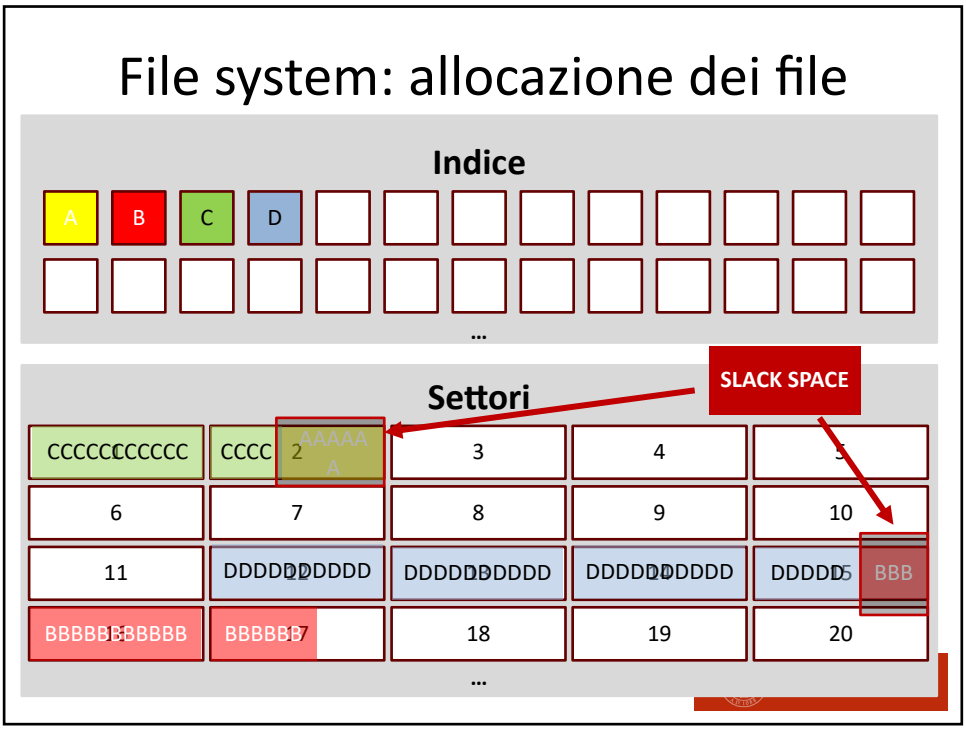
File system: allocazione dei file



68

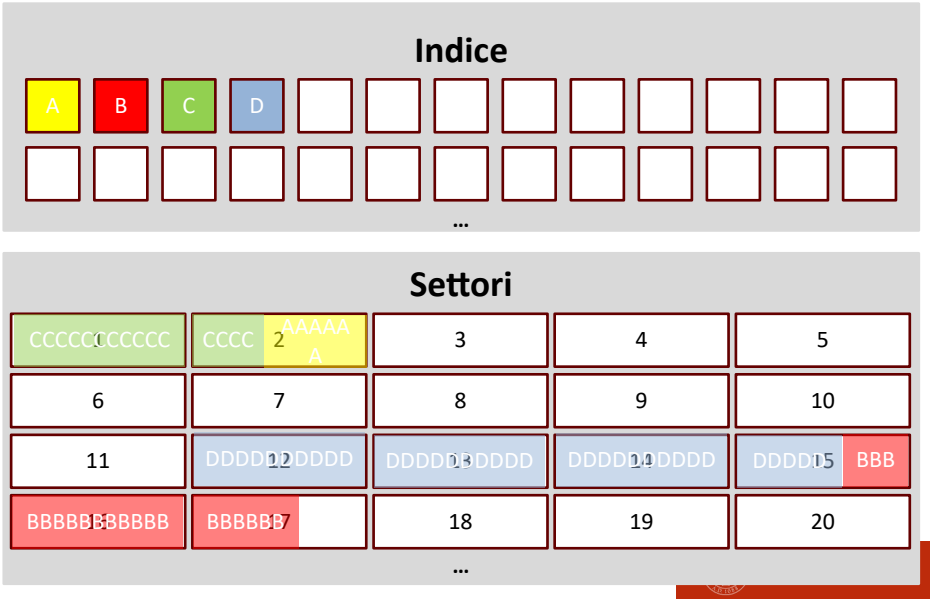

File system: allocazione dei file
Indice
A
B
C
D
...
Settori
SETTORI NON ALLOCATI
CCCCCCCCCCCC
CCCC
2
AAAAAA
3
4
5
6
7
8
9
10
11
DDDDDDDDDDDD
DDDDDDDDDDDD
DDDDDDDDDDDD
DDDDDD
BBB
BBBBBBBBBBBB
BBBBBB
17
18
19
20
...

69


File system: allocazione dei file
Indice
A
B
C
D
...
Settori
SLACK SPACE
CCCCCCCCCCCC
CCCC
2
AAAAAA
3
4
5
6
7
8
9
10
11
DDDDDDDDDDDD
DDDDDDDDDDDD
DDDDDDDDDDDD
DDDDDD
BBB
BBBBBBBBBBBB
BBBBBB
17
18
19
20
...

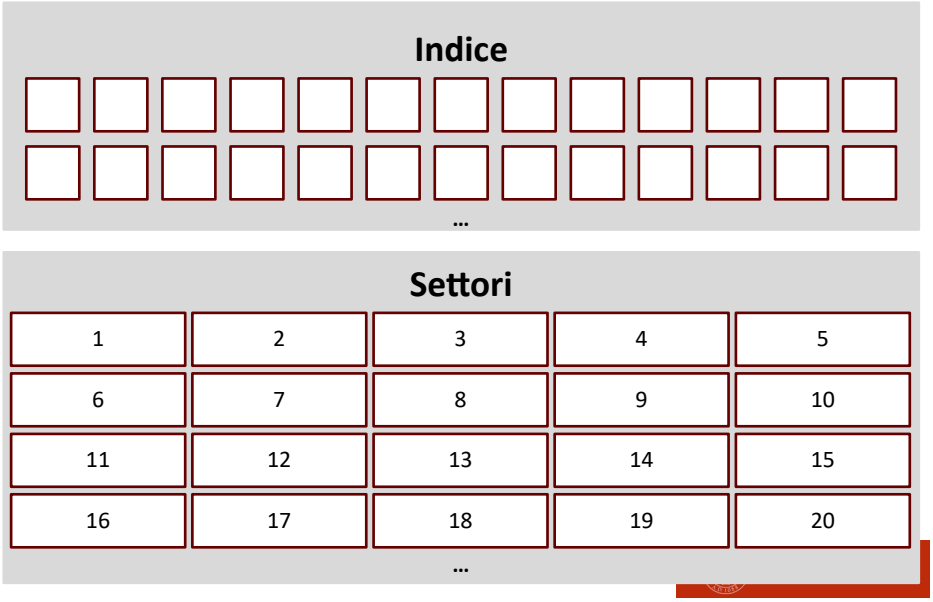
70

File system: formattazione



71

File system: formattazione dopo wiping



72

Proprietà del dato informatico (4)

La cancellazione dei dati è spesso solo apparente

il dato può essere recuperato con software specifici (*data carving*)

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

73

Prova!

- KillDisk https://www.killdisk.com/eraser.html
- Disk Drill: https://www.cleverfiles.com/it/
- Wondershare Recoverit: https://www.wondershare.net/

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

74

Dati e metadati

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

75

Dati e metadati

- La produzione di prove che nascono in digitale unicamente in formato cartaceo comporta la perdita di informazioni rilevanti non presenti nel contenuto del documento: i *metadati*

- Metadati (dati esterni): informazioni sui dati
  - Metadati di sistema
  - Metadati di applicazione

Visibili e invisibili, Metadati temporali, revisioni,

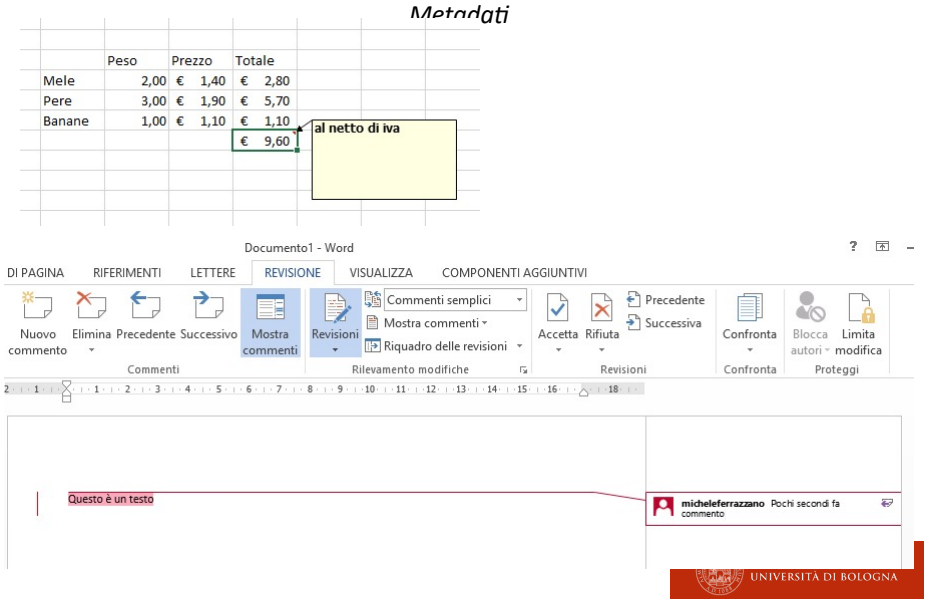
Esempi: nome utente, data creazione, data ultimo accesso, data di ultima modifica, formato e dimensione del file

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

76

Il dato informatico

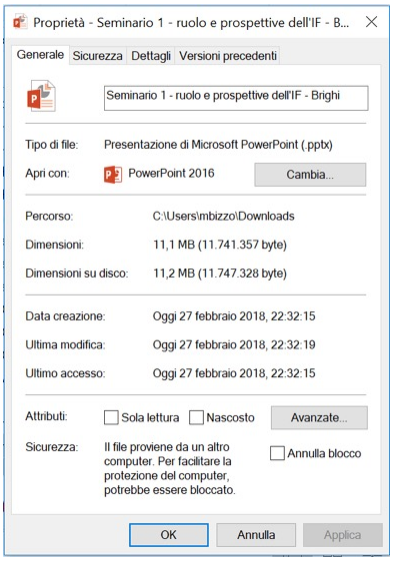
Metadati

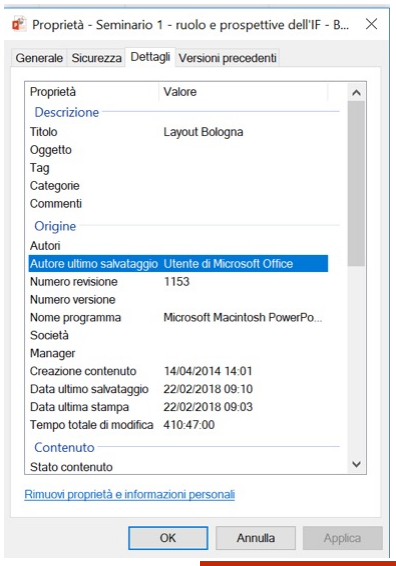


UNIVERSITÀ DI BOLOGNA

77

Metadati





ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

78

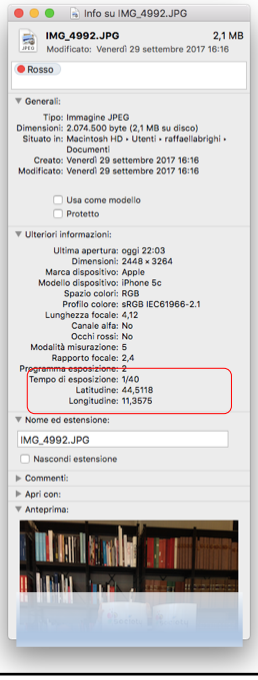
Il dato informatico

Metadati

```
From: "Cleopatra" <cleopatra@egitto.it>
To: "Antonio" <antonio@impero.it>
Subject: Festa di Ballo su Nilo
Date: Sun, 7 sep 2003 13:40:24 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative;
         boundary="----=_NextPart_000_00AB_01C5C873.E7722960"
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1441
This is a multi-part message in MIME format.

------=_NextPart_000_00AB_01C5C873.E7722960
Content-Type: text/plain;
         charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Caro Antonio,

sei invitato alla grande festa i mio onore che si terrà domani alle 20.00

Ti aspetto.

Cleopatra
```

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

79



Metadati

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

80

Riepilogo: caratteristiche del dato informatico

- Prime caratteristiche emerse

Immateriale
Volatilità
Facilità di modifica
Impossibilità di individuare modifiche
Perfetta replicabilità

- Da cui derivano difficoltà / problematiche legate a

Interpretazione
Attendibilità
Paternità

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

81

Il dato informatico: attendibilità?

- Quindi il dato informatico è sempre inattendibile?

- Calcolo dell'hash
- Marca temporale
- Firma digitale

82

L'approccio metodologico dell'informatica forense
Parte IV

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

83

Requisiti della prova informatica

Un corretto approccio metodologico impone di assicurare, in tutte le fasi dell'attività tecnica-organizzativa, i seguenti requisiti per ogni prova informatica:

- Integrità
- Autenticità
- Completezza
- Affidabilità
- Pertinenza
- Sufficienza
- Documentazione

- L'attività si sviluppa secondo un continuo dovere di **documentare ogni fase del procedimento** secondo il paradigma della **chain of custody.**

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

84

Due obiettivi: procedure condivise e skillset del esperto informatico forense

Dal punto di vista dell'informatica forense la garanzia dei requisiti della prova informatica si sostanzia in due direzioni:

(i) l'adesione a standard e alle linee guida di settore che individuino una base condivisibile di procedure operative e modalità di indagine per gli informatici forensi

(ii) Predisposizione di Iter formativi, selettivi e professionalizzanti del Digital forenser

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

85

I principali standard: una overview

Internazionali/generali

- ISO/IEC International Standards (dal 2012);
- Best Practice Manual for the Forensic Examination of Digital Technology (ENFSI, 2015);
- Electronic Evidence Guide (EEG, Council of Europe, 2013);
- Electronic evidence: A basic guide for first responders (ENISA, 2014);
- Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (2019);
- Guidelines on Digital forensics (NIST – National Institute of Standards and Technology, USA, 2014);

Specifiche/di settore

- Good Practice Guide for Computer-Based Electronic Evidence (ACPO - Association of Chief Police Officers, UK, 2012)
- Guidelines on Digital Forensic Procedures for OLAF Staff (2016);
- Circolare 1/2018 della Guardia di finanza - :http://www.gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrasto-alle-evasione-e-alle-frodi-fisca (Volume 2 pag 27 e ess.)

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

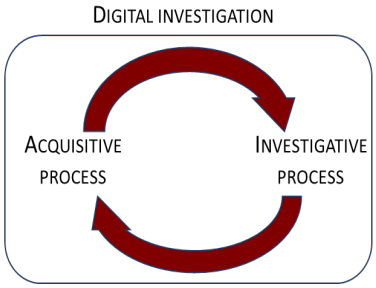
86

LA DIGITAL INVESTIGATION
Standard ISO e buone pratiche

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

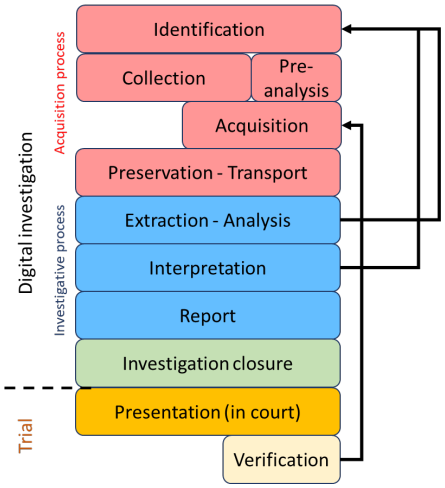
87

Digital investigation: due fasi



Digital investigation

Utilizzo di metodi scientificamente derivati e comprovati per l'identificazione, la raccolta, il trasporto, l'archiviazione, l'analisi, l'interpretazione, la presentazione, la distribuzione, la restituzione e / o la distruzione di prove digitali derivate da fonti digitali, preservando [...] le prove digitali e mantenendo il catena di custodia »(ISO/IEC 27043:2015)



Main steps

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

88

Riferimenti

- BIASIOTTI, EPIFANI, TURCHI (a cura di) Trattamento e scambio della prova digitale in Europa, in "Informatica e diritto" Fascicolo No. 1-2, 2015
- Brighi R., Una governance integrata per nuovi modelli dell'informatica forense, in i-Lex, n. 11-1:2017, www.i-lex.it
- Brighi R. Maioli C., *Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologia in Biasiotti, Epifani, Turchi (a cura di), Trattamento e scambio della prova digitale in Europa , INFORMATICA E DIRITTO, 2015, XXIV, pp. 217 – 234*
- Costantini F. Il «controllo» della prova digitale. Questioni teoretiche, organizzative e operative in Biasiotti, Epifani, Turchi (a cura di), Trattamento e scambio della prova digitale in Europa , INFORMATICA E DIRITTO, 2015, XXIV, pp. 105 – 120
- FERRAZZANO M., Aspetti metodologici, giuridici e tecnici nel trattamento di reperti informatici nei casi di pedopornografia, ARACNE (2018)
- Gammarota, A. *Informatica forense e processo penale: la prova digitale tra innovazioni normativa e incertezze giurisprudenziali*, consultabile all'url: http://amsdottorato.unibo.it/7723, 2016
- Haack S., *Legalizzare l'epistemologia. Prova, probabilità e causa nel diritto*, Egea: Milano, 2015

IL PRESENTE MATERIALE È RISERVATO AL PERSONALE DELL'UNIVERSITÀ DI BOLOGNA E NON PUÒ ESSERE UTILIZZATO AI TERMINI DI LEGGE DA ALTRE PERSONE O PER FINI NON ISTITUZIONALI

Riferimenti

- National Research Council, National Academy of Sciences, Strengthening Forensic Science in the United States: A Path Forward. Washington, DC: National Academies Press, 2009, p. 53
- Maioli C., Dar voce alle prove: elementi di Informatica forense, in Pozzi P., Masotti R., Bozzetti M., (a cura di), Crimine virtuale, minaccia reale, Franco Angeli, Milano, 2004.
- Maioli C., L'insegnamento dell'informatica giuridica: il contributo dell'Università di Bologna, in Peruginelli G., Ragona M., (a cura di), L'informatica giuridica in Italia, Napoli, ESI, 2014.
- MAIOLI C. (a cura), Questioni di informatica forense, Aracne, 2015
- Picotti L. (2011). La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee. *Riv. trim. dir. pen. ec.* 4:827 e ss.
- Torre M. Aspetti giuridici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48 in Biasiotti, Epifani, Turchi (a cura di), Trattamento e scambio della prova digitale in Europa , INFORMATICA E DIRITTO, 2015, XXIV, pp. 65 – 104

IL PRESENTE MATERIALE È RISERVATO AL PERSONALE DELL'UNIVERSITÀ DI BOLOGNA E NON PUÒ ESSERE UTILIZZATO AI TERMINI DI LEGGE DA ALTRE PERSONE O PER FINI NON ISTITUZIONALI