



## I LEZIONE

### Evoluzione tecnologica negli ultimi 20 anni

- aumento della potenza di calcolo dei computer
- standardizzazione del formato digitale delle informazioni e aumento dell'impiego del trattamento di dati in formato digitale e con sistemi informatici
- diffusione dei sistemi informatici
- diffusione dei sistemi di trasmissione di dati digitali
- sviluppo di reti private LAN e WAN
- sviluppo di reti pubbliche – INTERNET
- diminuzione dei costi dei sistemi informatici e di accesso alle reti

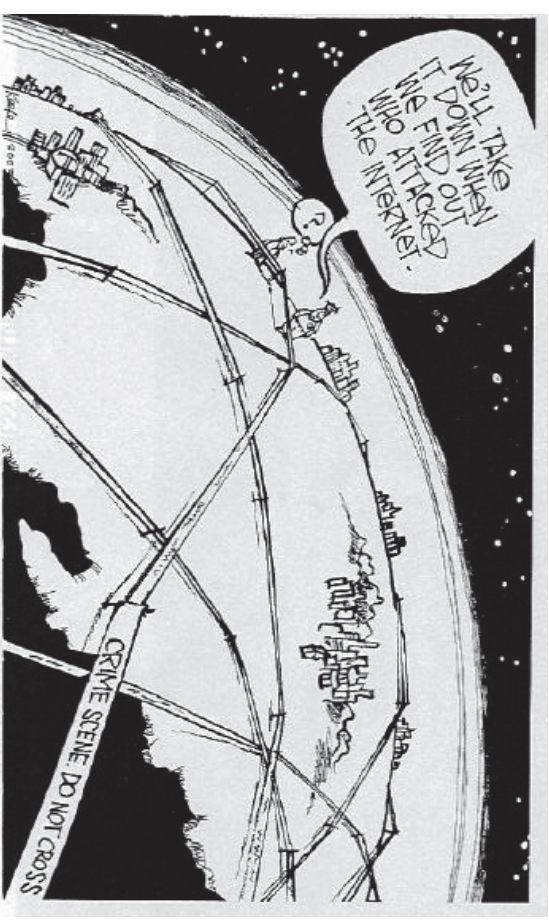
## Nel Cyberspazio senza frontiere...

- aumento delle capacità di elaborazione (legge di Moore)
- diminuzione dei costi dell'informatica
- diffusione della tecnologia
- globalizzazione
- integrazione dei sistemi

## ...a fronte di reati delocalizzati...

- |                              |                                  |
|------------------------------|----------------------------------|
| ● Terrorismo                 | ● Cracking                       |
| ● Pedopornografia            | ● Truffe on line                 |
| ● Discriminazione razziale   | ● Phishing                       |
| ● Violazione della privacy   | ● Spamming                       |
| ● Ingiuria e diffamazione    | ● Frode informatica              |
| ● "Furto" e riuso di dati    | ● Violazioni al diritto d'autore |
| ● Riciclaggio                |                                  |
| ● Estorsioni                 |                                  |
| ● Falso in bilancio          |                                  |
| ● Accessi abusivi            |                                  |
| ● Danneggiamenti informatici |                                  |

## Il Cyberspazio non ha frontiere...



in [http://digitalforensics.champplain.edu/about\\_cdf.html](http://digitalforensics.champplain.edu/about_cdf.html)

## ...difficoltà di ricostruzione dei reati globalizzati...

- ☐ dislocazione dell'autore: da dove
- ☐ indeterminazione degli autori: quanti
- ☐ anonimizzazione dell'autore: chi è, chi sono
- ☐ cronologia degli eventi: quando
- ☐ modalità esecutive: in che modo
  - velocità dell'attività
  - volatilità delle tracce
- ☐ movente: perché
- ☐ reiterazione: quante volte
- ☐ offensività: contro chi

## All'aumento del trattamento di dati con sistemi informatici conseguenze

### l'incremento della domanda di analisi dei dati digitali a fini di investigazione e di giustizia per

- reati informatici in senso stretto
- reati non informatici ma commessi con sistemi informatici
- reati di cui si rinvergono tracce o indizi nei sistemi informatici

alle ore 18

# la Repubblica.it

Ricerca nel sito | Scrivete  
Fai di Repubblica la tua home page | Servizio clienti  
Ultimo aggiornamento LUNEDÌ 09 FEBBRAIO 2004 ore 16.43

Gli articoli, le news e il parere  
degli esperti online

Deutsch Bank

Internet

L'Europa a partire da 19 euro

Home | Politica | Cronaca

Economia

Esteri

Sport

Hi-tech

Spettacoli & Cultura

Motori

Week-in

Dossier | Blog

Lavoro & concorsi

Tutte le offerte di lavoro

Borse di studio

Vai

I servizi di Repubblica.it

> Repubblica.it via SMS

> I-mode

> Umts

> Gprs

> Elenco telefonico

> Verifica immobiliare

Repubblica in edicola

Leggi il giornale

Katweb

Scegli il sito

Cerca con Google

ECONOMIA

La giornata a Collechio di Fausto Tonna e Giancarlo Bocchi

In un file nascosto i conti aziendali senza trucchi

**Il contabile: "Datemi un pc"**

Senza me e i miei collaboratori di quei numeri

non capirete niente, non andrete da nessuna parte

di MARCO MENSURATI e PIER FRANCESCO FEDRIZZI

COLLECCHIO - LO

psicodramma comincia alle

dieci del mattino. I due

irrompono sulla scena

situando dallo sfondo

immenso e gelido della

piantua padana a bordo di

due automobili col

lampeggiante. Sono Fausto

Tonna, l'ex direttore

finanziario dell'impero, l'"alter

Fausto Tonna a Collechio

è in edicola  
il telefono  
con Repubblica

Invia questo articolo

Stampa questo articolo

La Gfr perquisisce

Nexta e Morgan Stanley

Protesta dei bond people

in Banca d'Italia

Parmalat, dai conti

spunta il buco del calcio

Trenonti su Fazio

"Nulla di personale"

# la Repubblica.it

Ricerca nel sito | Scrivete  
Fai di Repubblica la tua home page | Servizio clienti  
Ultimo aggiornamento VENERDÌ 09 MAGGIO 2003 ore 10.39

3 libri a 1,50 euro

Homepage | Politica

Cronaca

Economia

Esteri

Sport

Scienza & Tecnologia

Spettacoli & Cultura

Repubblica sul cellulare

Modeste via SMS

Umts

Repubblica in edicola

Leggi il giornale

Katweb

Scegli il sito

Cerca con Google

Vai

CRONACA

Nemmeno gli esperti americani riescono a violare le protezioni

che impediscono l'accesso al "covo telematico" di Galesi e Luce

**L'Fbi non "legge" i palmari delle**

**Br**

**sepolti nei Pc i segreti dei**

**terroristi**

di CLAUDIA FUSANI

ROMA - Nemmeno l'Fbi, riesco

a "leggere" i segreti nascosti

nelle memorie dei computer

palmari delle Br. Il segreto

industriale e, forse, il timore di

ingenti perdite in borsa sono

gli ostacoli che impediscono di

accedere alle memorie segrete

dei tre computer palmari

sequestrati ai brigatisti Nadia

Luce e Mario Galesi.

Paradosicamente, una

"memoria segreta" è la "lista"

sta diventando la principale

alleata della nuova lotta

armata. Le indagini seguono il

Repubblica  
PRESENTA

Invia questo articolo

L'Fbi non riesce

leggere

nei palmari dei

brigatisti

PARLAREMO

Luce rivendica omicidi

di Galesi e C. Antonic

Luce, ordinanza

di custodia per

omicidio d'Antonio

Luce in via Salara

il giorno prima

del delitto

Luce indagata

Luce indagata

Luce indagata

"portatemi il computer che era al primo piano"

"no, non è questo, mi serve il mio"

"recuperate quel file lì"

Bilancio reale

Bilancio del comparto estero

Bilancio Bonlat

Bilancio aziende di famiglia

Bilancio pubblicato

"senza di noi qui non andate da nessuna parte"

nei casi come quello Parmalat,

tutte le parti del procedimento potrebbero essere

pregiudicate da una cattiva gestione dei dati informatici

Esempi di prove per la PG:

oggetto: fax + descrizione demone + fotocopia  
con 3 pezzi di listato  
tecnica di verifica: nessuna

1/3

FRONTESPIZIO FACSIMILE

Per favore, consegnare le seguenti pag. : 1°, 2°, 3°

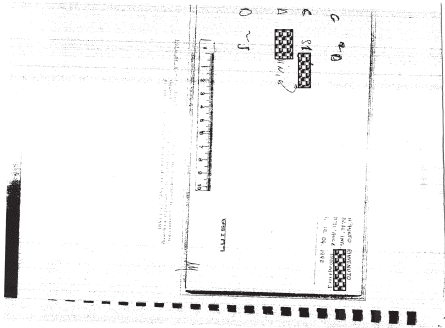
NUMERO FACSIMILE : [REDACTED]

DATA : 2/11/13

NUMERO FACSIMILE : [REDACTED]

Per mancata o errata pressione indicata al [REDACTED]

oggetto: manoscritto con passaggi  
tecnica di verifica: perizia calligrafica comparativa



oggetto: fax + descrizione demone + fotocopia  
con 3 pezzi di listato  
tecnica di verifica: nessuna

2/3

FRONTESPIZIO FACSIMILE

Per favore, consegnare le seguenti pag. : 1°, 2°, 3°

NUMERO FACSIMILE : [REDACTED]

DATA : 2/11/13

NUMERO FACSIMILE : [REDACTED]

Per mancata o errata pressione indicata al [REDACTED]

**oggetto: fax + descrizione demone + fotocopia  
con 3 pezzi di listato  
tecnica di verifica: nessuna**

**3/3**

Comune denominatore: il dato digitalizzato come oggetto di indagine

Nel corso di innumerevoli indagini sono emersi:

### **Limiti culturali degli operatori forensi**

- scarsa cultura informatica tecnica di base
- scarsa cultura di diritto dell'informatica
- carenza di dottrina
- carenza di giurisprudenza

### **Limiti organizzativi ed operativi**

- know how investigativo
- know how difensivo
- poca formazione specifica
- pochissimi laboratori pubblici e privati di analisi dei dati
- a fini investigativi
- taglio dei corsi universitari dedicati all'IF

## **Esempio di prova per la PG**

anche in Italia si è affermata la

## **COMPUTER FORENSICS**

**Il diritto alla prova nel processo accusatorio americano**  
(da Henry Campbell Black, in *Black's Law Dictionary*, West Publishing CO, St. Paul, Minnesota (USA), 1990, voce "Due process of law, Mercone, M., *Diritto Processuale Penale*, Napoli, 2001, p. 44 e ss.);

## Cosa è la Computer Forensics ?

*due process of law* - il giusto processo

### Il diritto alla prova nel processo accusatorio americano

- ***legal and procedural fairness*** – correttezza legale, sostanziale e processuale
- ***timely notice of the charges*** – diritto a conoscere tempestivamente gli elementi di prova e le loro fonti
- ***guiltiness must be proven by legally obtained evidence*** – il diritto alla legalità delle prove di colpevolezza
- ***the verdict must be supported by the evidence legally presented*** – diritto al giudizio *justa alligata et probata*

### Il diritto alla prova nel processo accusatorio americano

- obbligo di rigore nell'acquisizione dei mezzi di prova da esibire in dibattimento
- onere dell'accusa per le prove a carico (o a discarico)
- onere della difesa per le prove a discarico

## Il diritto alla prova nel processo accusatorio americano

- obbligo di rigore nell'acquisizione dei mezzi di prova da esibire in dibattimento
- onere dell'accusa per le prove a carico (o a discarico)
- onere della difesa per le prove a discarico

## Tradizionali oggetti di investigazione scientifica dell'FBI

- oggetti vari (vestiti, auto, armi, ecc.)
- materiale biomedico
- impronte digitali
- sostanze di vario tipo (legno, metalli, liquidi, esplosivi, ecc.)
- fotografie
- suoni
- documenti vari
- documenti cartacei

## Definizioni ed oggetto della Computer Forensics

### *“Computer forensics*

*(...) is the collection of technique and tools used to find evidence in a computer.”*

M. A. CALOYANNIDES, *Computer Forensics and Privacy*, Norwood, MA, 2001

### *“Computer forensics*

*(...) è l'insieme della tecnica e degli strumenti usati per cercare la prova in un computer.”*

***“Computer forensics***

*involves the preservation, identification, extraction and documentation of computer evidence stored as data or magnetically encoded information” (...). “Computer forensics also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disk, diskettes, tapes, etc.) for evidence.”*

J. R. VACCA, *Computer Forensics – Computer Crime Scene Investigation*, Charles River Media, Hingham, Massachusetts, 2002, Intt., XIX

***“Computer forensics***

*concerne la protezione, identificazione, estrazione e documentazione della prova informatica memorizzata come dato o come informazione codificata magneticamente. (...)*

*altresi riguarda l'analisi forense del computer, l'esibizione elettronica, l'esibizione della prova elettronica, l'esibizione digitale, il recupero di dati, l'analisi del computer, mentre l'esame del computer è il processo di esaminare metodicamente i mezzi del computer (hard disk, floppy disk, nastri, etc.) per la prova.”*

***“Computer Forensics***

*(...) deals with the preservation, identification, extraction, and documentation of computer evidence. (...) Like any other forensics science, computer forensics involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing.”*

A.J. MARCELLA – R.S. GREENFIELD, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, USA, Auerbach, 2002:

***“Computer Forensics***

*(...) tratta la conservazione, identificazione, estrazione e documentazione della prova informatica. (...) Come ogni altra scienza, la computer forensics riguarda l'uso di sofisticati strumenti tecnologici e procedure che devono essere seguite per garantire l'esattezza della conservazione della prova e l'esattezza dei risultati riguardanti l'elaborazione della prova informatica.”*

***“Computer forensics***

*(...) involves the preservation, identification, extraction, documentation and interpretation of computer data.”*

W. G. KRUSE II – J. G. HEISER, *Computer Forensics: Incident Response Essentials*, Addison-Wesley, Boston, USA, 2002

***“Computer forensics***

*(...) riguarda la conservazione, identificazione, estrazione, documentazione e interpretazione dei dati del computer”*

**Computer Forensics svolta dall'FBI**

tratto da <http://www.fbi.gov/hq/lab/handbook/forensics.pdf>

**F.B.I. HANDBOOK OF FORENSICS SERVICES**

*Evidence Examinations*

# Oggetto della Computer Forensics

## F.B.I. HANDBOOK OF FORENSICS SERVICES (\*)

### *Evidence Examinations*

- ☐ data seizure (**sequestro di dati**)
- ☐ data duplication (**uplicazione di dati**)
- ☐ data preservation (**conservazione di dati**)
- ☐ data recovery (**recupero dati**)
- ☐ document searches (**ricerca di documenti**)
- ☐ media conversion (**conversione di formati**)
- ☐ expert witness services (**consulenti tecnici**)

(\*) <http://www.fbi.gov/hq/lab/handbook/forensics.pdf>

## F.B.I. HANDBOOK OF FORENSICS SERVICES

**Cancellazione di File di Dati** – I file di dati possono essere recuperati dal computer

**Conversione di formati** – I file di dati possono essere convertiti da un formato ad un altro

**Ricerca per parola chiave** – I file di dati possono essere cercati per parola o frase ed i risultati possono essere registrati

**Password** – Le password possono essere ritrovate e decifrate

*(chi ha inviato i palmari in USA, ha forse letto questa pagina ?)*

## F.B.I. HANDBOOK OF FORENSICS SERVICES

### *Analisi del computer*

**Contenuto** – Gli esami possono stabilire quali tipi di dati sono contenuti in un computer

**Comparazione** – Gli esami possono comparare file di dati per conoscere il contenuto di documenti e file di dati

**Successione** – Gli esami possono determinare tempo e sequenza con la quale i file di dati furono creati

**Estrazione** – I file di dati possono essere estratti dal computer

## F.B.I. HANDBOOK OF FORENSICS SERVICES

**Codice sorgente protetto** – Il codice sorgente può essere analizzato e comparato

**Mezzi di memorizzazione** – I mezzi di memorizzazione usati in macchine da scrivere digitali possono essere esaminati

**Richiesta di ricerca o campo di esame** – Esamina richieste per ricerca o esami in una settimana

## **l'F.B.I. svolge attività di Forensics per conto terzi**

L'FBI mette a disposizione:

- laboratori
- metodologie
- procedure (con alcune limitazioni)

per la resa dei servizi di Forensics a favore di:

- uffici decentrati dell'FBI;
- U.S. Attorneys;
- tribunali militari
- altre agenzie federali, States, county, and municipal law enforcement agencies

## **Fruitori privati di Computer Forensics in USA**

- aziende
- operatori forensi (avvocati, investigatori privati, consulenti)

## **Fruitori pubblici di Computer Forensics in USA**

- U.S. Department of Justice - Federal Bureau of Investigation (FBI)
- Department of Defense
- National Security Agency (NSA)
- Central Intelligence Agency (CIA)
- Altre agenzie governative
- U.S. Postal Service
- States, county, and municipal law enforcement agencies
- operatori forensi (courts, prosecutors, polizia)

**Perché sorgono problemi di metodologia  
del trattamento dei dati informatici  
ad uso probatorio e processuale ?**

### **caratteristiche inerenti la natura fisica del dato**

- ☐ necessità di un supporto (ad es. hard disk, floppy disk, flash memory)
- ☐ riproducibilità in numero infinito di copie
- ☐ volatilità
- ☐ modificabilità (quasi) anonima
- ☐ deteriorabilità

### **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 dei processi eseguiti

### **esigenze di ordine giuridico**

la prospettiva dell'attività tecnica è quella della utilizzabilità in dibattito, a disposizione delle parti processuali al fine della valutazione di ogni aspetto processualmente rilevante

(rinvio al tecnico informatico)