

Introduzione

Corso di Informatica giuridica (corso propedeutico)

Facoltà di Giurisprudenza – LIUC

L'informatica forense

(Computer Forensics - CF)

- E' la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico per essere **valutato in un processo giuridico** e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici...

Tratto da www.wikipedia.org

La prova informatica/1

- Una *prova* serve per ricostruire la verità dei fatti
 - Nel mondo fisico una prova si vede, si tocca, si percepisce con i sensi
- ...e una *prova informatica*?
 - Nel mondo digitale una prova è solo una astrazione logica (es. un file).
 - Un file può essere copiato (esistere su diversi supporti)
 - Non può essere rubato (se lo copio non sottraggo niente al proprietario)
 - Può essere alterato (particella di materiale magnetico che cambia il suo orientamento)
 - Se risiede sulla RAM essa viene modificata e sovrascritta in continuazione dal SO

La prova informatica/2

- Perché una prova sia ammessa in un processo, deve essere idonea a dimostrare i fatti ai quali si riferisce
- ...e una *prova informatica*?
 - Affinchè sia ammessa in sede processuale dovrà possedere requisiti di ***integrità*** e ***non ripudiabilità***

Le fasi

- Individuazione e isolamento delle prove
- Acquisizione dei dati
- Analisi
- Ricostruzione degli eventi
- Raccolta e conservazione delle fonti di prova

I problemi attuali della CF

- Mancanza di uno standard e di tecniche di indagine consolidate

L'informatica forense

(Computer Forensics - CF)

- E' la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei **sistemi informatici**

Tratto da www.wikipedia.org

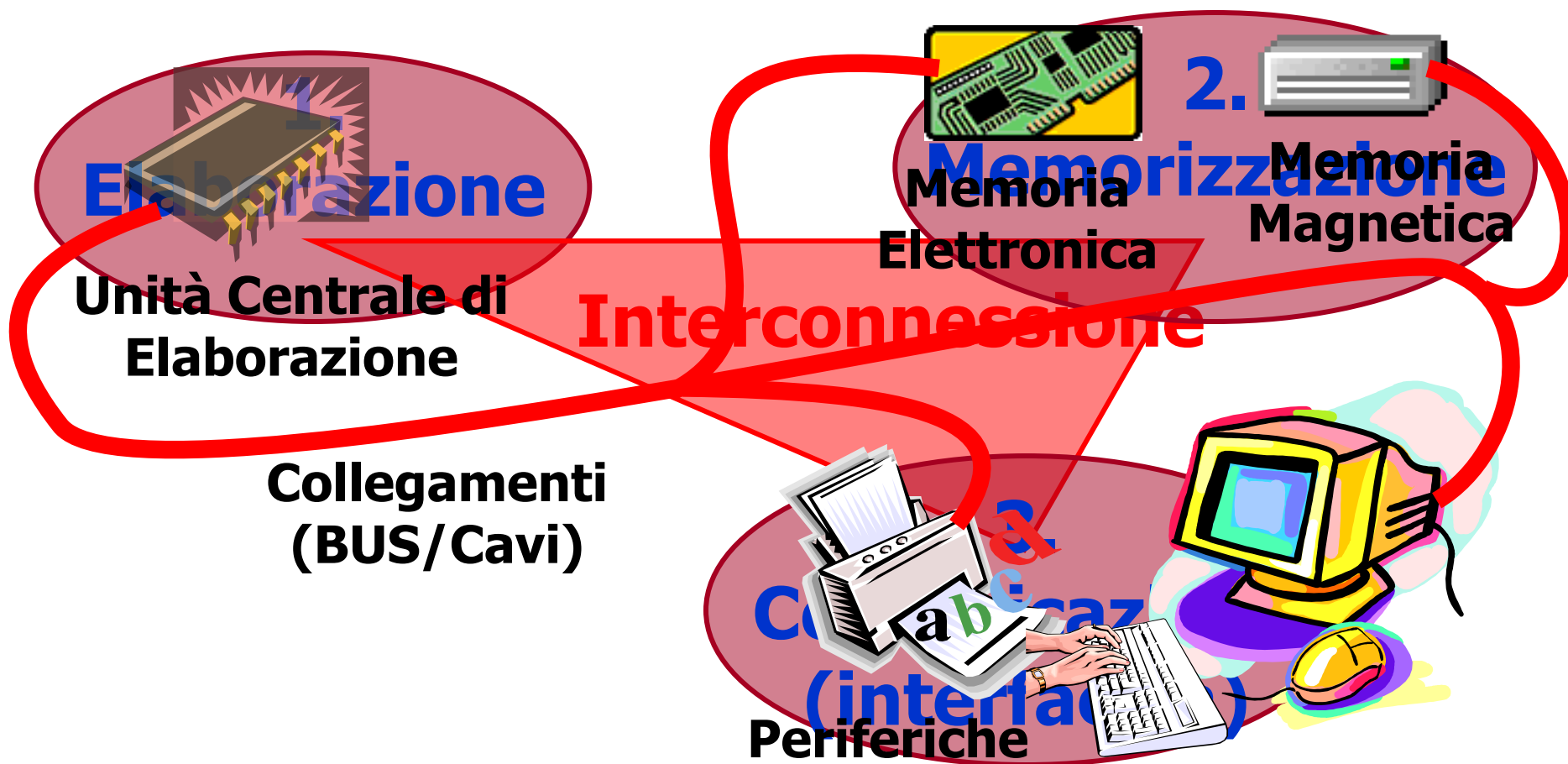
Applicazioni della CF

- Si applica solo ai computer?
 - NO!
- Si applica a **qualsiasi dispositivo tecnologico** che possieda un **sistema di memorizzazione** delle informazioni
 - Macchina fotografica digitale
 - Palmare
 - Console per videogiochi
 - ...

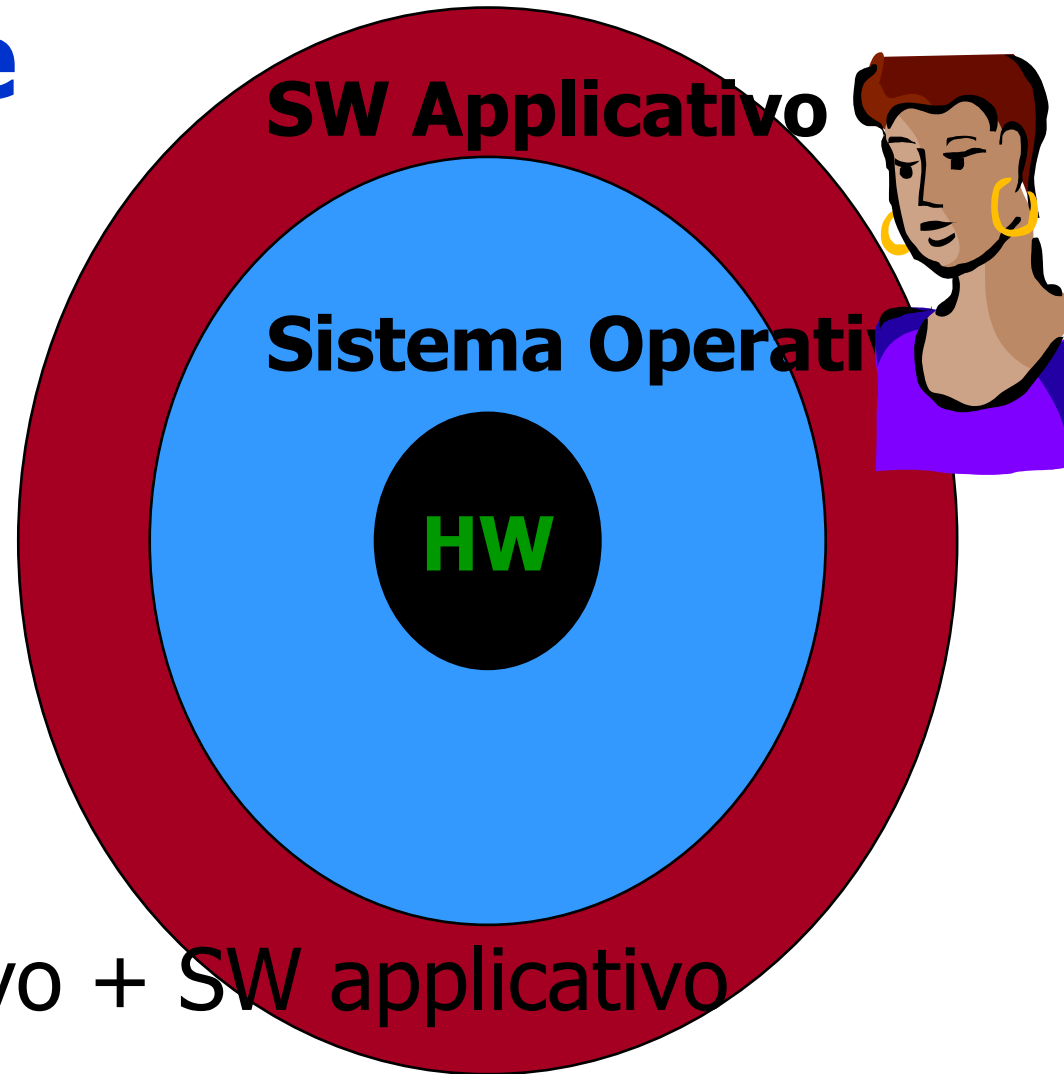
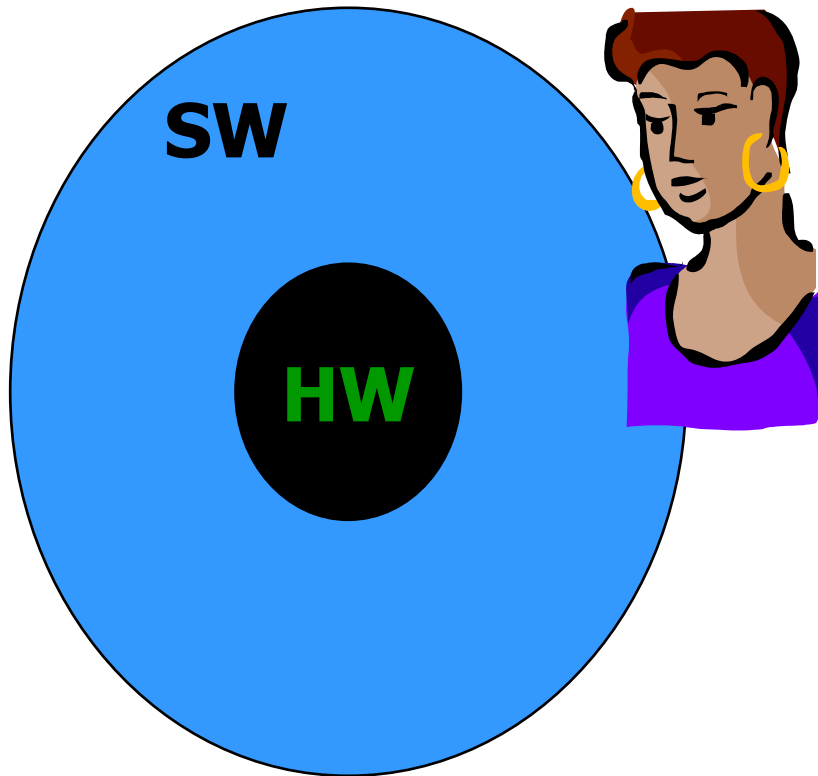
“...sistema di memorizzazione...”

- Cosa significa?
- Cos'è una memoria?
- Ne esistono tipologie diverse?
- Chi scrive i dati al suo interno?
- Come posso leggere i dati memorizzati?
- E quelli cancellati?
-

Il calcolatore: modello architetturale



Il software



➤ SW = Sistema Operativo + SW applicativo

➤ Il S.O. come necessario intermediario

La Network Forensics

- Acquisizione dei dati mediante intercettazione durante il passaggio da un sistema ad un altro
- Consentito dalla legge solo in casi eccezionali
 - Gravi indizi di reato
 - Intercettazione indispensabile alla prosecuzione dell'indagine

Riepilogando...

- Si applica a tutti i dispositivi con capacità di memorizzazione..
- I dati acquisiti per essere validi come prova informatica devono essere integri e non-ripudiabili
- Per garantire tali caratteristiche è necessario adottare una metodologia condivisa