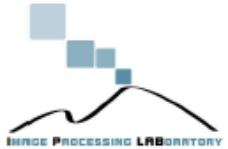


Corso di Laurea in Informatica I Livello

Lezione Inaugurale del Corso di Computer Forensics

Le Nuove Frontiere dell'Investigazione Digitale

Status e Prospettive

19 Marzo 2012 - ore 15,30

Dipartimento di Matematica e Informatica

SALUTI E PRESENTAZIONE DEL CORSO

SEBASTIANO BATTIATO – UNIVERSITÀ DEGLI STUDI DI CATANIA

EUGENIO DONATO CACCAVELLA – UNIVERSITÀ DEGLI STUDI DI BOLOGNA

RELATORI

CESARE MAIOLI – UNIVERSITÀ DEGLI STUDI DI BOLOGNA

Ruolo e prospettive dell'Informatica forense

SALVATORE LO MONACO – FUNZIONARIO NCIS, SIGONELLA

L'Introduzione dell'Investigatore al mondo digitale

MICHELE FERRAZZANO – UNIVERSITÀ DEGLI STUDI DI BOLOGNA

Reati di pedopornografia in ambiente peer to peer: analisi dei file di log per ricostruire attività di scambio tra vari utenti indagati

MODERATORE: GIOVANNI GALLO – UNIVERSITÀ DEGLI STUDI DI CATANIA

Computer Forensics

Corso di Laurea in Informatica

A.A. 2011/2012

Obiettivi Formativi (1/2)

Il corso mira a favorire l'acqusizione di conoscenze e competenze all'avanguardia in materia di **Computer e Image Forensics** e a promuovere il riconoscimento e la graduale regolamentazione delle nuove professionalità legate all'informatica forense.

Il corso esamina gli aspetti tecnologici (e in parte giuridici) attinenti alla prova digitale in ambito forense.

Il coordinamento scientifico del corso è affidato al **prof. Sebastiano Battiato** in collaborazione con il **dott. Donato Eugenio Caccavella.**

Obiettivi Formativi (2/2)

Il corso esamina gli aspetti tecnologici (e in parte giuridici) attinenti alla prova digitale in ambito forense.

- Modalità di investigazione “digitale” alla luce dell'ordinamento giuridico italiano: tecniche di indagine informatica, investigazione difensiva nel campo dei crimini informatici e dei crimini comuni la cui prova sia costituita da dati digitali o veicolati da sistemi informatici.
- Overview dei problemi tecnici, tipicamente informatici, in connessione con le problematiche giuridiche che sottendono a tali tipi di indagini. Ci si soffermerà in particolare sulle ”best-practice” da utilizzare sul campo per acquisizione, conservazione, analisi e produzione dei dati digitali rinvenuti nei computer e dei flussi telematici per la loro utilizzabilità nell'ambito dei vari tipi di processi, istruttori e/o procedimento amministrativi.
- **Image and Video Forensics** e relative tecniche investigative.

Articolazione del Corso

Il corso è articolato in distinti moduli didattici, comprendenti lezioni teoriche, laboratori e seminari di approfondimento su specifici temi tenuti da esperti esterni, per un totale di 48 ore complessive.

Modulo 1 – Tecniche di trattamento dei Reperti Informatici

Modulo 2 – Investigare su Immagini e Video

Le lezioni si terranno nel secondo semestre dell'A.A. 2011-2012, ogni lunedì alle ore 15,00 presso l'Aula 24 del Dipartimento di Matematica ed Informatica

Risultati A.A. 2010/2011

Docenti e Seminari di I ordine:

ATERNO Stefano, BALOSSINO Nello, BATTIATO Sebastiano, CACCAVELLA Donato Eugenio, COSTABILE Gerardo, FERRAZZANO, FLORA Matteo, GAMMAROTA Antonio, JERIAN Martino, LUPARIA Luca, MAZZARACO Giuseppe, NICASTRO Antonio, PERRI Pierluigi

Slides disponibili su:http://www.dmi.unict.it/~battiato/CF1011/CF1011.html

10 Borse di studio a forze dell'ordine e professionisti (supporto di Telefono Arcobaleno) - **150** studenti (non solo di Informatica)

Utilizzo **software AMPED 5** (licenza academy disponibile per tutta la durata del corso)

Realizzazione di software **open source** per l'Image Forensics realizzato come plugins di ImageJ disponibile qui: **http://svg.dmi.unict.it/iplab/imagej/index.htm**

Add-on moduli per il software EmuleForensics

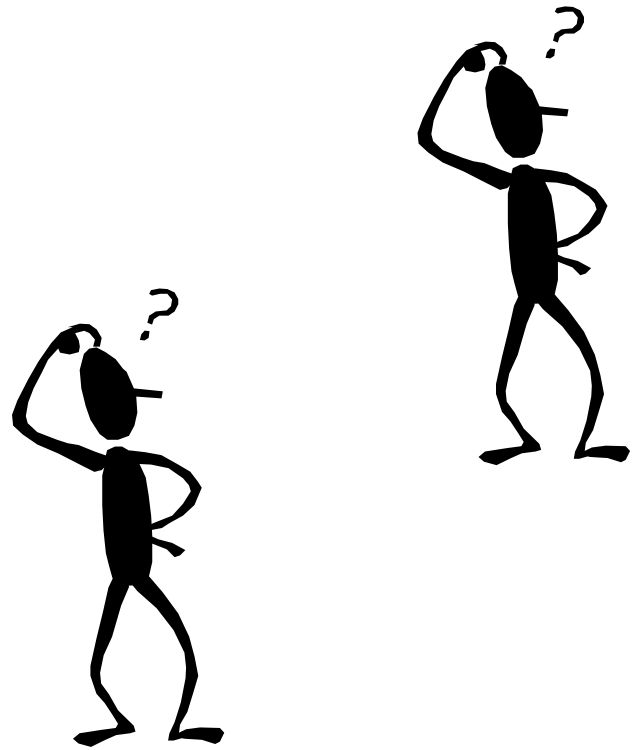
Novità A.A. 2011-2012

- Videoripresa di tutte le lezioni a cura del GTUG Catania (a breve un canale su YouTube)
- Modulo ***Image and Video Forensics*** SHARED tramited FAD nell'ambito di un progetto di formazione del Tribunale di Milano in collaborazione con il CILEA ed il Comune di Milano, rivolto alla P.G. del distretto di Milano.
- Sessioni di laboratorio (presso il laboratorio IPLAB aula 146) con l'utilizzo di toolkit (HW/SW) forensi da utilizzarsi su casi reali in collaborazione con il NIT di Siracusa.
- Acquisto Licenze Academy FTK
- Supporto per gli esterni (forze dell'ordine, professionisti) di libri di testo sull'elaborazione delle immagini

Ringraziamenti e Collaborazioni

CIRSFID

Modalità d'esame



Prove in Itinere con esonero.

Laboratorio (?)

Prova scritta

Progetto SW (opzionale) da concordare con il docente.

Utility

Slides e Materiale Vario:

www.dmi.unict.it/~battiato/CF1112/CF1112.html

Forum

E-mail:

battiato@dmi.unict.it

Ricevimento:

(Consultare il web)

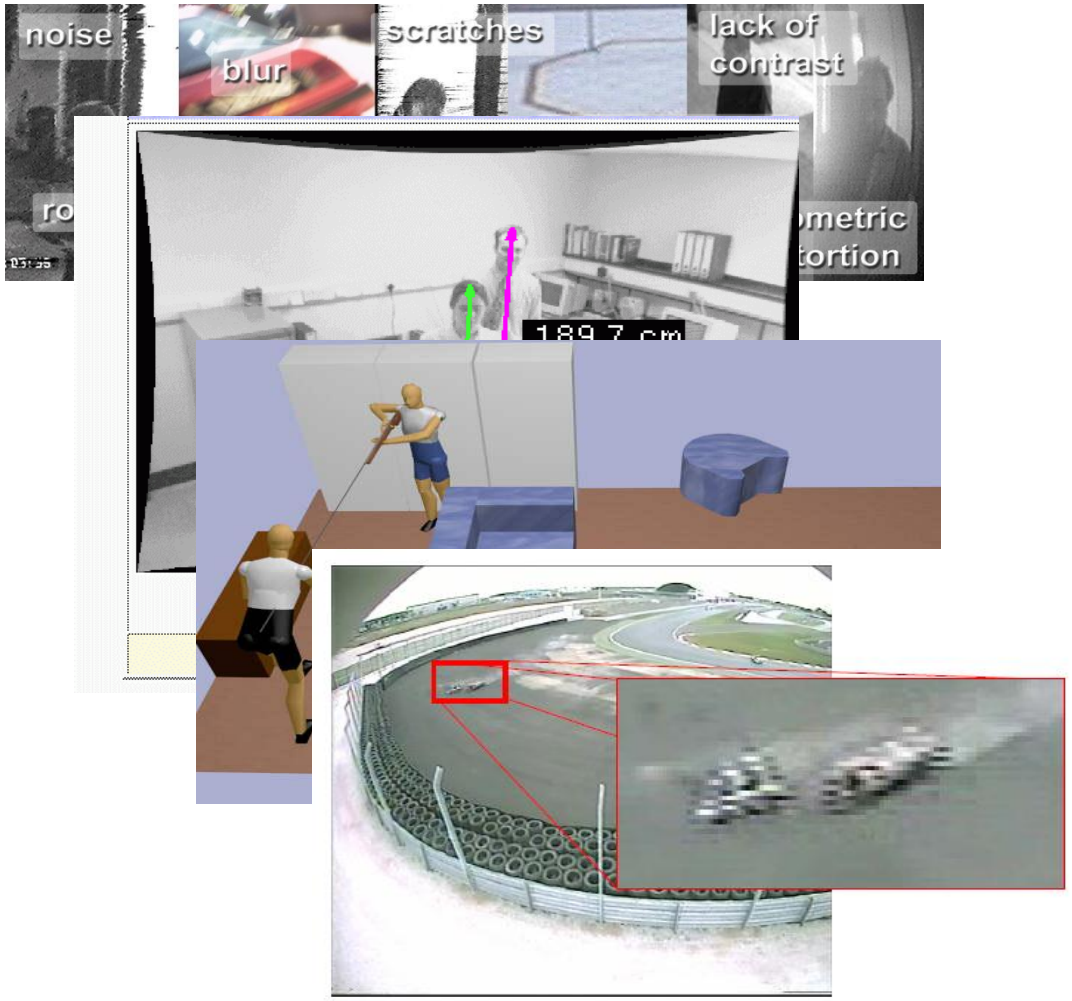
Image and Video Forensics

Image (Video) Forensics

"Forensic Image (Video) analysis is the application of IMAGE SCIENCE and DOMAIN EXPERTISE to interpret the content of an image or the image itself in legal matters" (SWGIT – www.fbi.gov)

Esempi..

- Image Reconstruction
- Self Embedding
- Video Analysis
- 3D Reconstruction
- Steganography
- Image Forgery Identification
- Image Source Identification

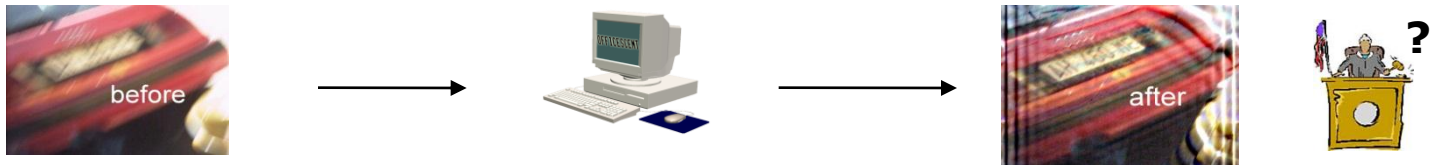


Implicazioni in ambito “forense”

Il dato digitale è per sua natura molto sensibile a manipolazioni. Risulta semplice (ed economico) da manipolare.

Diverse le problematiche in ambito investigativo/forense da gestire:

- Che differenza c'è fra **miglioramento** o **manipolazione** dell'immagine? Quali elaborazioni sono ammissibili?
- **Digital Forgery** (qual è l'originale? qual è l'elaborato?)



Implicazioni

- Valgono gli stessi principi generali della **digital forensics** per la trattazione dei reperti digitali
  - Preservazione dell'originale
  - Acquisizione integra e non ripudiabile
  - Utilizzo di copie di lavoro
  - Documentazione e ripetibilità
- In generale, ogni manipolazione tende ad evidenziare particolari presenti, non a cambiare i contenuti dell'immagine

Fantasy

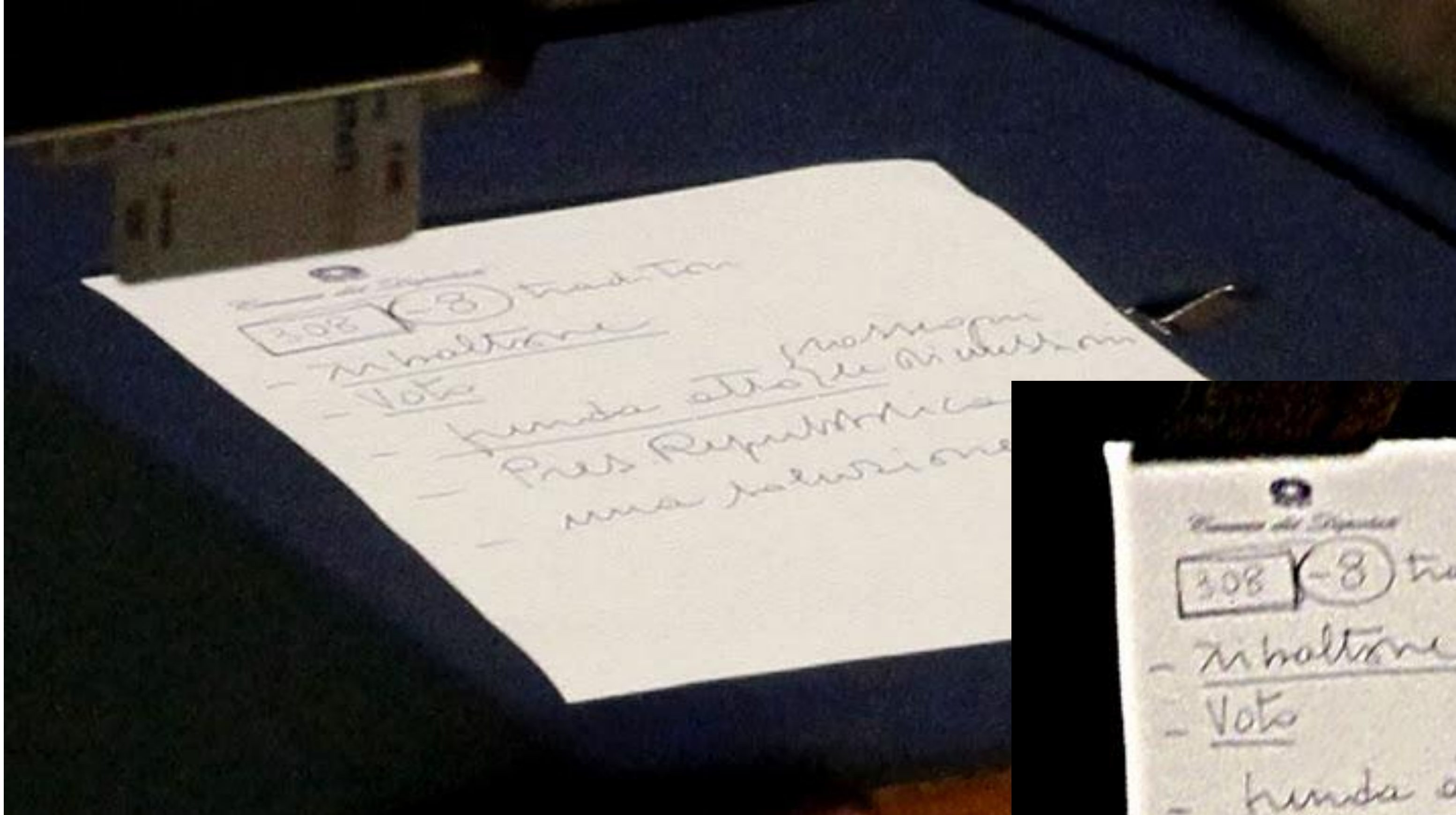
- Avete visto come si ingrandiscono le foto in film come Blade Runner o in serie come CSI e RIS?

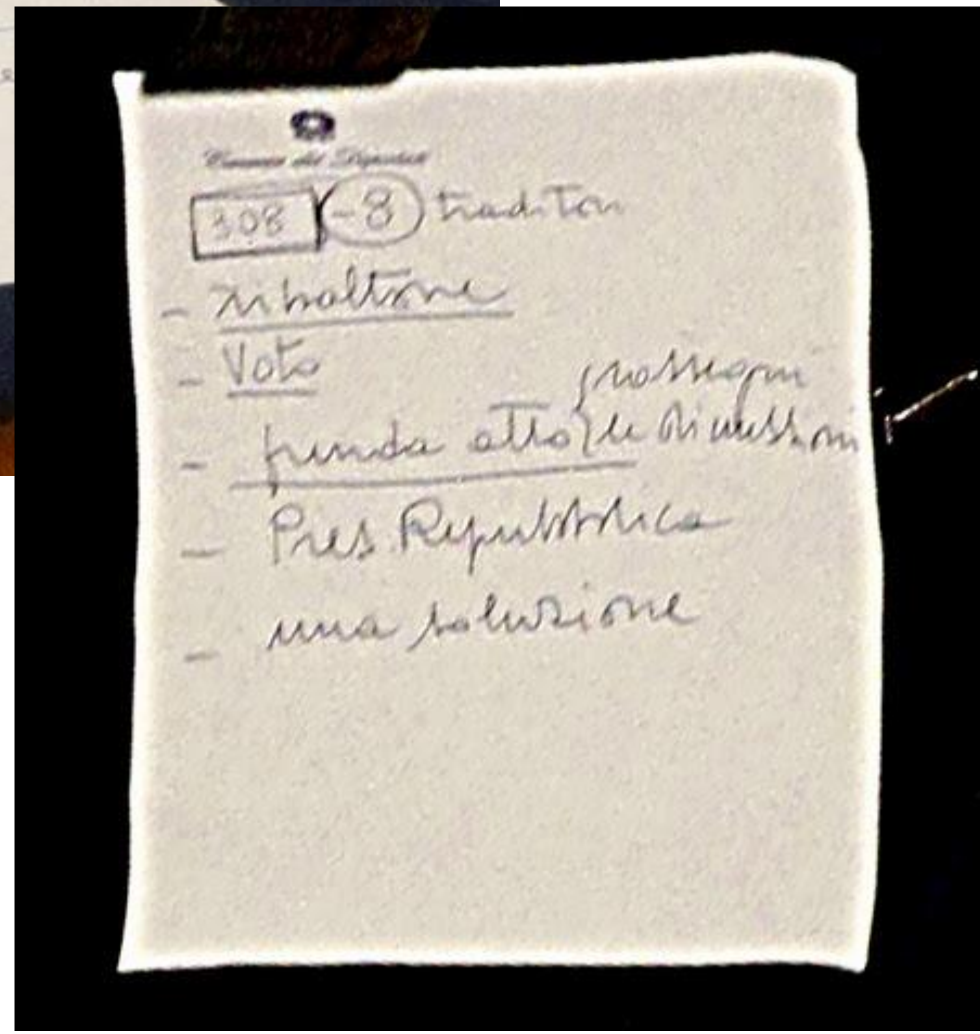
CSI

Fantasy

- Non si possono "creare" informazioni che non ci sono…
- Si possono però enfatizzare informazioni che non si vedono, ……ma ci sono

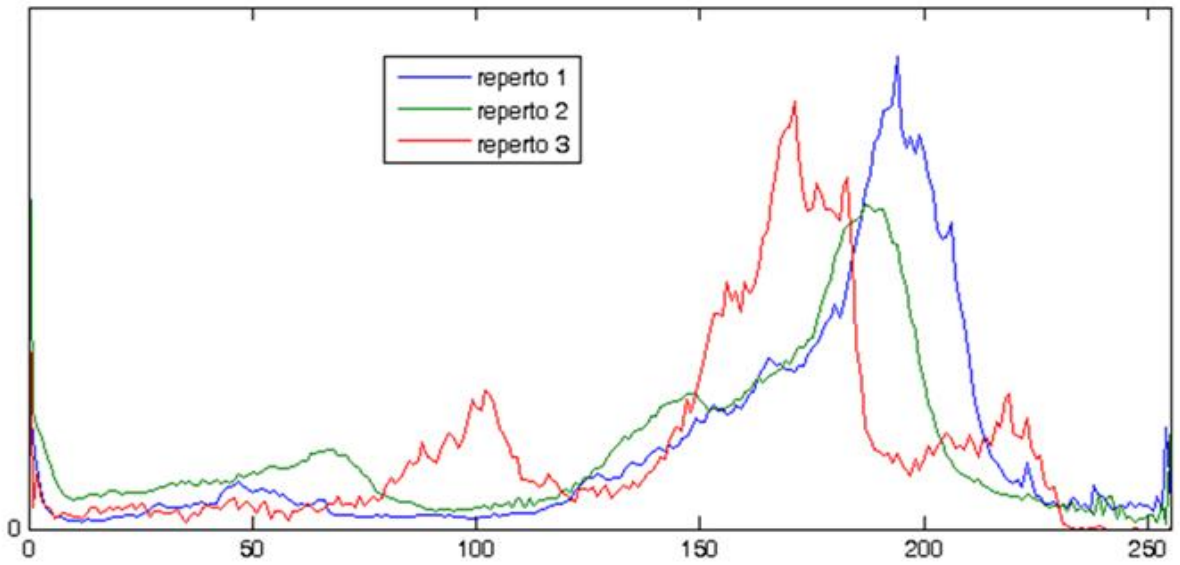
Correzione Prospettica

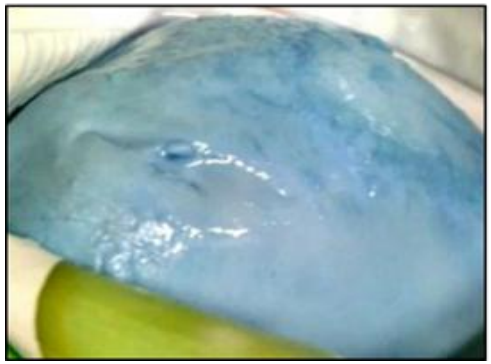


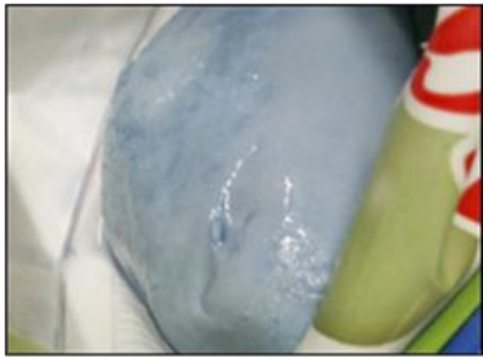

308
-8
Voto
Pres. Repubblica
una soluzione

(source Interpol)

Contraffazione di Immagini Digitali sulla Rete: il caso della "Mozzarella Blu"


reperto 1
reperto 2
reperto 3
0
0
50
100
150
200
250





Le tecniche di Image (video) Forensic costituiscono sicuramente un ulteriore strumento di indagine a disposizione degli investigatori per poter estrarre ed inferire, utili informazioni dalle immagini (e dai video) digitali anche nel caso di dispositivi mobili.

Per essere in grado di recuperare o di inferire delle evidenze di prova è comunque necessaria una adeguata competenza specifica che richiede uno studio sistematico dei **fondamenti della teoria dell'elaborazione delle immagini e dei video digitali**.

I software esistenti agevolano il lavoro degli investigatori ma non riescono per forza di cose ad automatizzare in maniera sistematica ed efficiente tali operazioni e richiedono l'ausilio di professionisti esperti.

Investigare su Immagini e Video

- Fondamenti di elaborazione delle immagini e dei video digitali
- La compressione dei dati
- Contraffazioni: casi famosi e non. Tecniche avanzate per l'identificazione delle contraffazioni: pixel-based, format-based, camera-based, physically-based, geometric based.
- Advanced Content Analysis
- Tip&tricks – Demo in laboratorio
- Overview dei principali software di riferimento (es. Amped5)
- Casi di studio reali (G8 di Genova, il delitto di Garlasco, Cogne, Erba, Google vs Vividown) e simulazioni di laboratorio

Victim Identification: R&D project

- How many victims? How proceed?
- Victim (e.g., child) Identification through advanced technology:
  - **Unsupervised Face Detection/Recognition**
  - **Face Aging (and estimation)**
  - **Face Crowling**
    - **on large Scale data sets**
    - **on Web**