Digital Forensics

Laboratorio – 3 CFU

Luca Guarnera, Ph.D.

RTDa – Dipartimento di Matematica e Informatica

Università di Catania

luca.guarnera@unict.it

https://www.dmi.unict.it/lguarnera/

Università di Catania

IMAGE PROCESSING LABORATORY

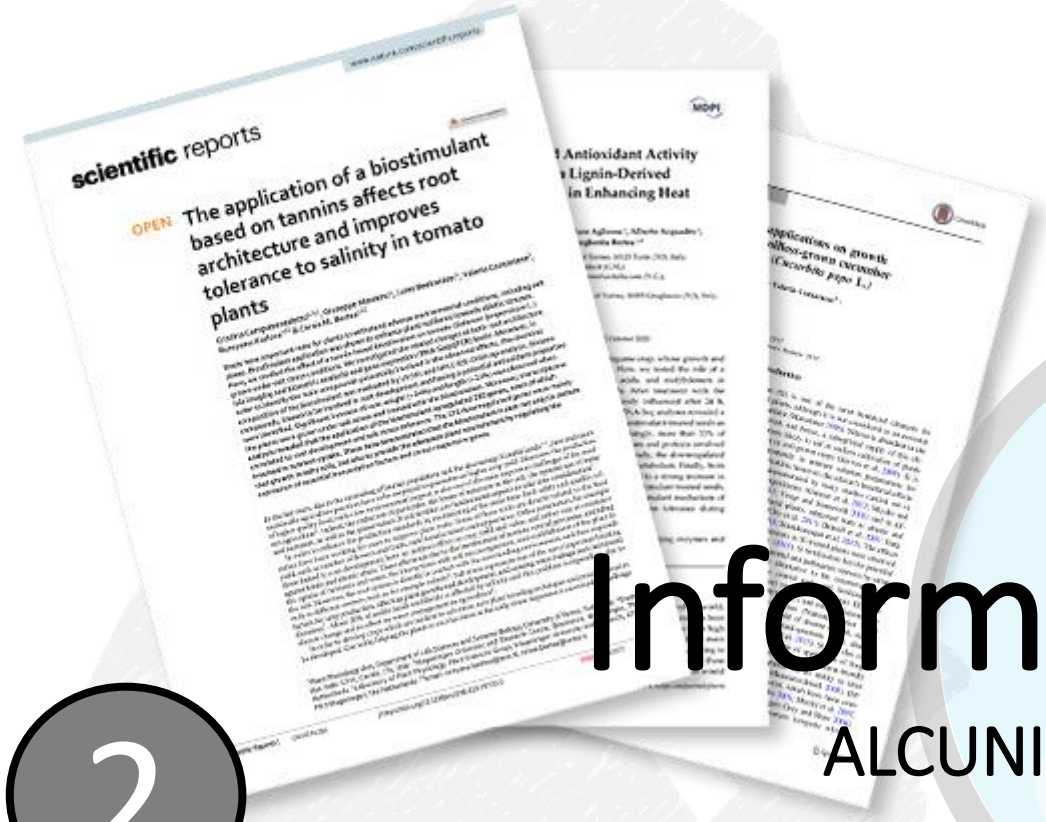
Alcune Info …

- Stanza 311 (secondo piano, Blocco 1)
- Ricevimento:
  - Martedi dalle 11 alle 13
  - Oppure fissiamo un appuntamento via email: luca.guarnera@unict.it

Laboratorio di Digital Forensics – Programma

- Autenticazione sulle Immagini Digitali
- Amped Five
- Amped Authenticate
- Caine
- Strumenti 3D
  - 3D Zephyr
  - Structure Sensor
  - …

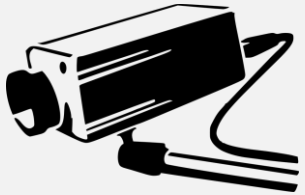
https://forms.gle/JVe2D7yRTtBaBiQW8



Informatica Forense

ALCUNI CONTESTI APPLICATIVI

2



Università di Catania

Luca Guarnera
luca.guarnera@unict.it

Digital Forensics

Information Technology Law

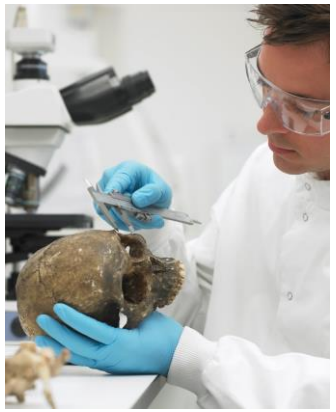
Università di Catania

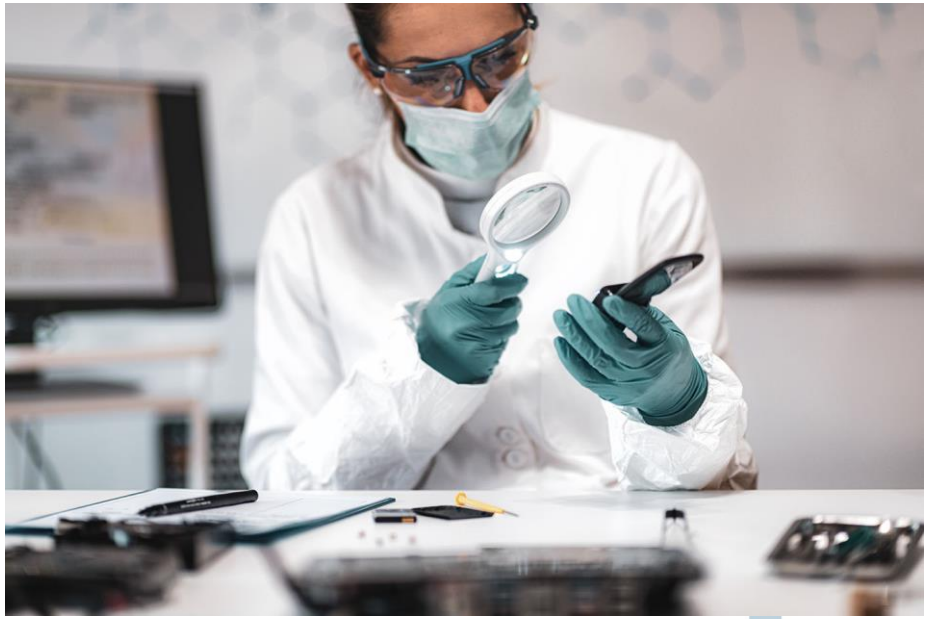
Luca Guarnera
luca.guarnera@unict.it

IMAGE PROCESSING LABORATORY

Forensic Science

(sometimes shortened to Forensics) is the application of technical and scientific methods to the justice, investigation and evidence discovery domain.





Digital Forensics History

1

The first notion of digital forensics came in the **1970s**, when the ***Federal Rules (US)*** regulations began talking about **DIGITAL EVIDENCE**

2

The **DIGITAL FORENSICS INVESTIGATIONS** started in the mid-to-late 1980s, when federal agents began to study how to find digital evidence in computers

3

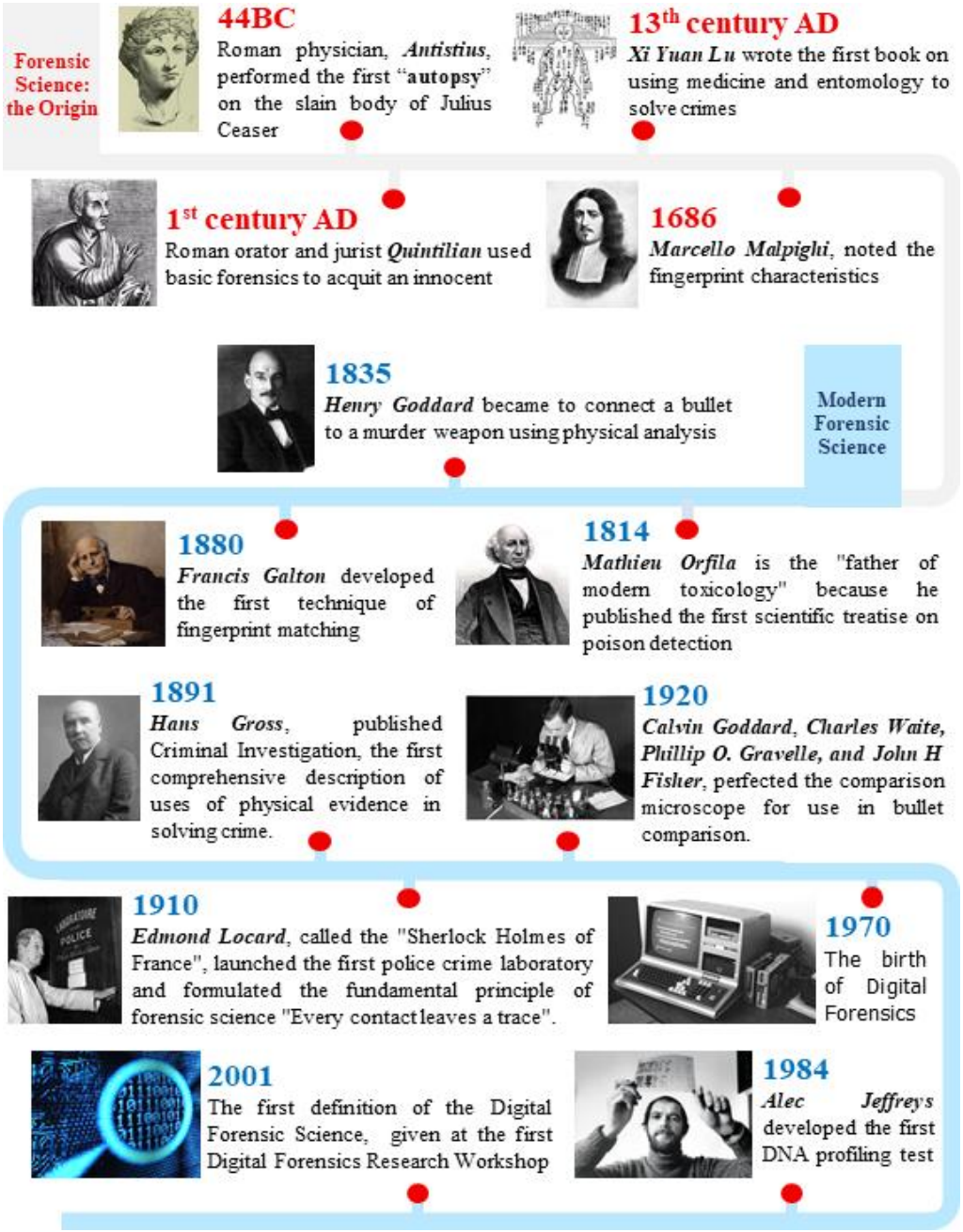
The **first research groups** in the area of Forensic Science started around **2000 and 2001**

4

The first definition of the Digital Forensic Science was given at the first Digital Forensics Research Workshop (DFRWS), in 2001

The use of scientifically derived and proven methods toward the **preservation**, **collection**, **validation**, **identification**, **analysis**, **interpretation**, **documentation** and **presentation** of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations

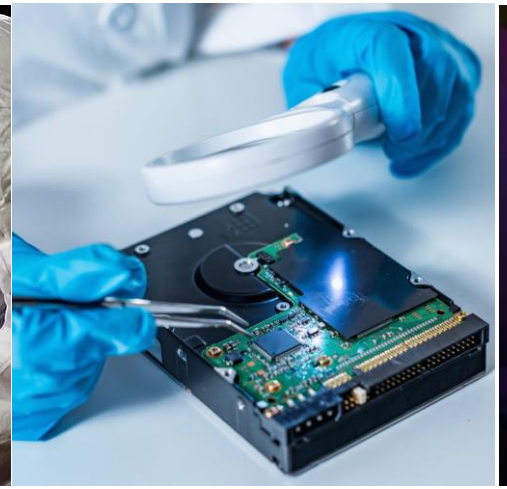
Ma c’è molto di più sulle origini delle Scienze Forensi



Forensic Science

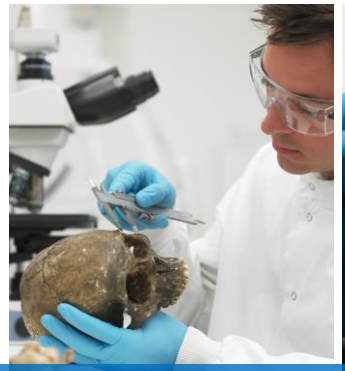
Uno dei campi della Forensics Science che sta avendo molti risultati è la **Digital Forensics**

- **Anni '70**: **prima nozione** di Digital Forensics
- **Anni '80**: **alla ricerca di prove digitali**.
- **Anni '90**: si **afferma la Digital Forensics**:
  - ***è un campo con problemi e possibilità abbastanza grandi da giustificare un'indagine***.



Forensic Science

(sometimes shortened to Forensics) is the application of technical and scientific methods to the justice, investigation and evidence discovery domain.



DIGITAL FORENSICS

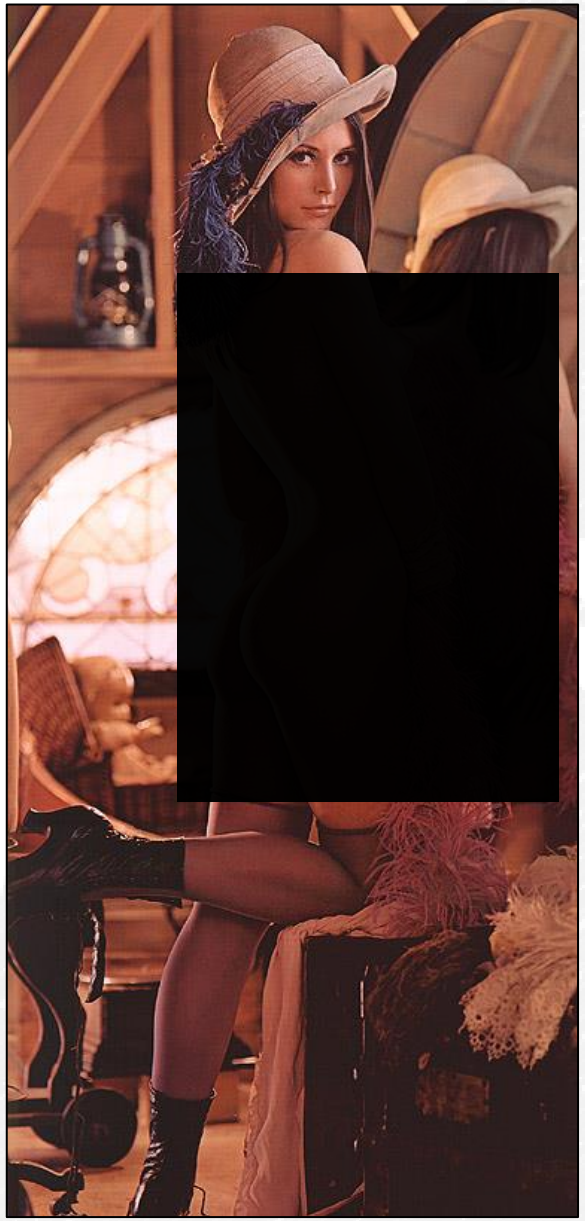
The first definition of the Digital Forensic Science was given at the first Digital Forensics Research Workshop (DFRWS), in 2001

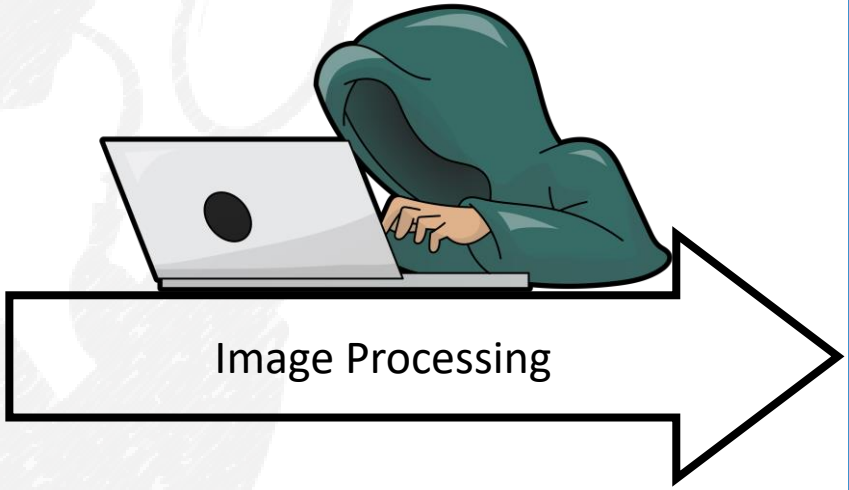
*"The use of scientifically derived and proven methods toward the **preservation**, **collection**, **validation**, **identification**, **analysis**, **interpretation**, **documentation** and **presentation** of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"*

Image Forensics

Cosa possiamo dire di questa immagine?

Cosa possiamo dire di questa immagine?





Autentica?
Integra?

Cosa possiamo dire di questa immagine?

Cosa possiamo dire di questa immagine?

Authenticity VS Integrity

First and foremost: **Authenticity is not Integrity**

AUTHENTICITY ≠ INTEGRITY

Image is an accurate representation of the original event

Information is unaltered from the time of acquisition until its final disposition

Operation	Authenticity	Integrity
JPEG compression/Re-saving	OK	NO
Upload & Download Facebook	OK	NO
Image processing operations	NO (?)	NO
Recapture of a fake image	NO	OK
Staging	NO	OK

Image Forgery

Splicing

an object is inserted into the image

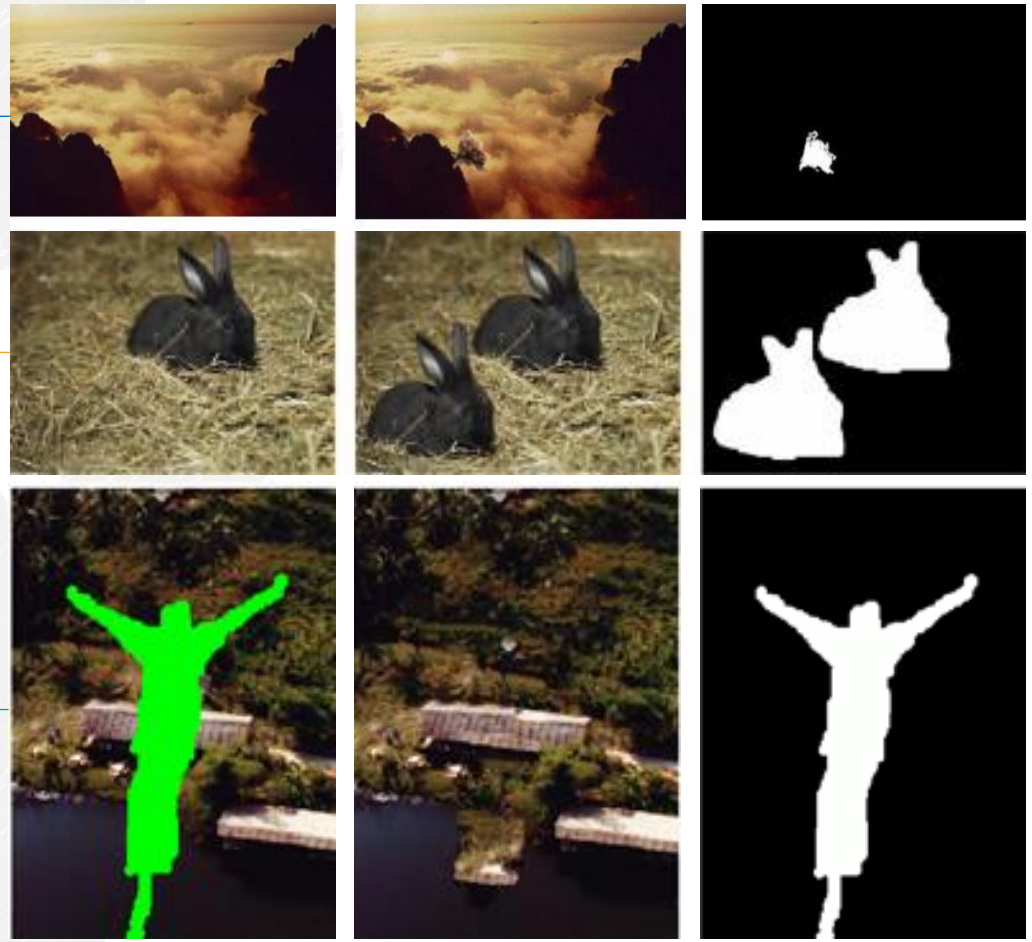
Copy-move

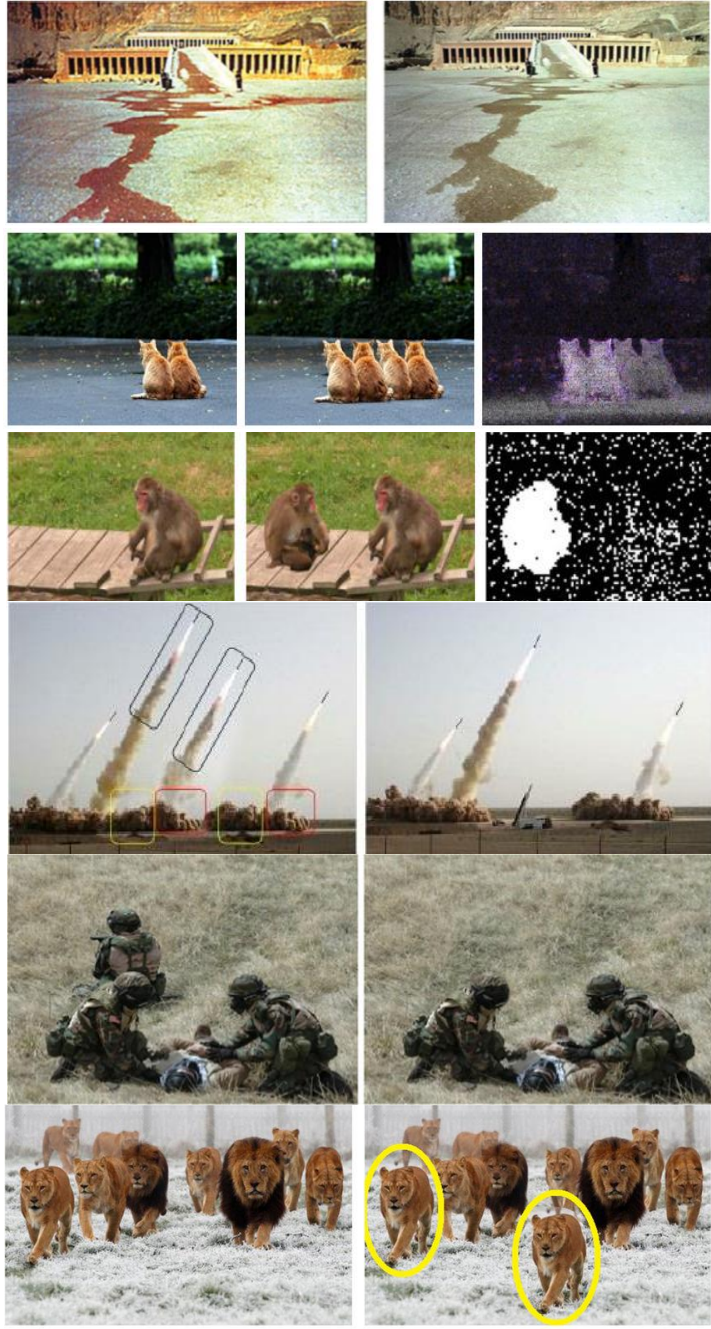
cloning of an object in the same image

In-painting

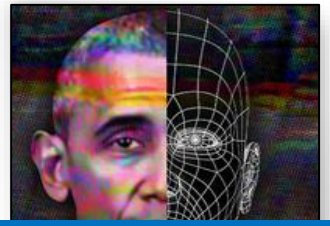
Removing an object by covering the missing area with the background

Authentic image | Tampered Image | Ground-truth mask



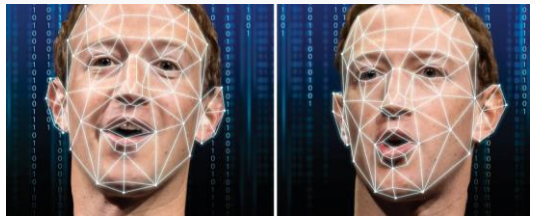


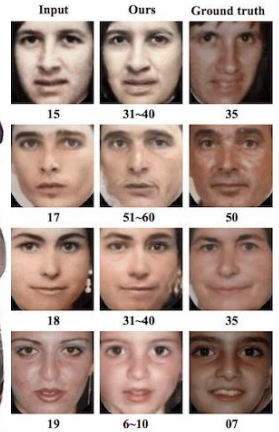
Deepfakes

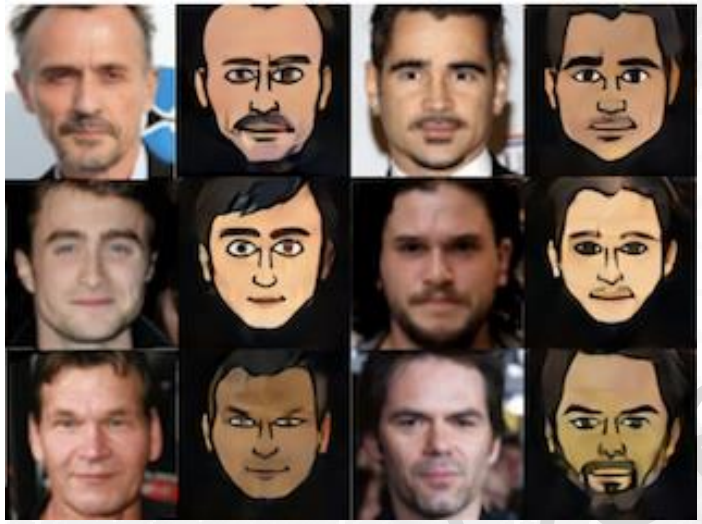


Deepfakes refers to all those multimedia contents synthetically altered or created by exploiting machine learning generative models

"[…] In autumn 2017, an **anonymous Reddit user** under the pseudonym "**deepfakes**" posted several **porn videos on the Internet** […]".





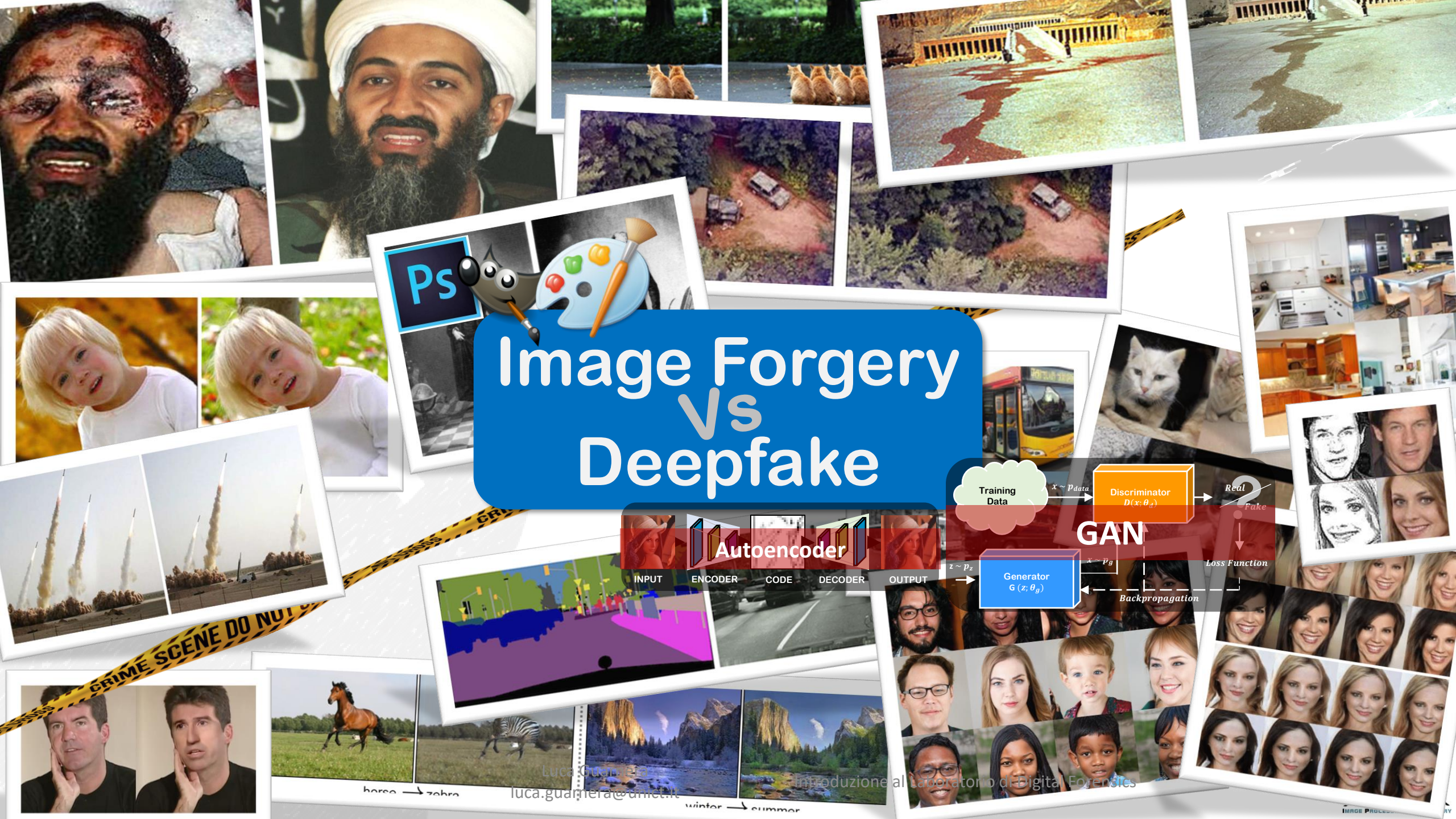


horse → zebra

winter → summer

thispersondoesnotexist.com

Image Forgery Vs Deepfake



Original Image **Forgery**

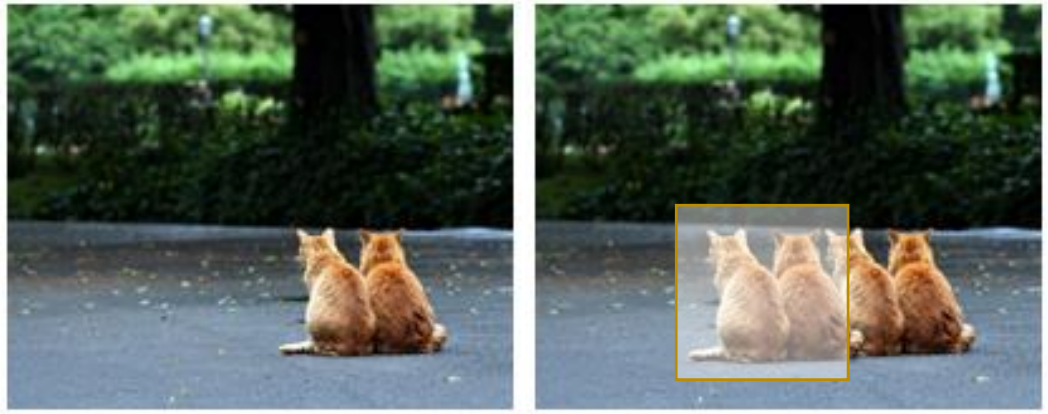
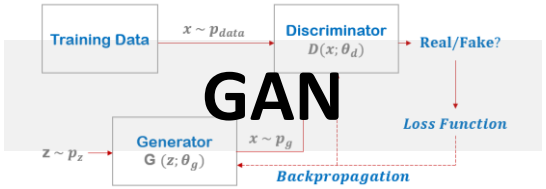


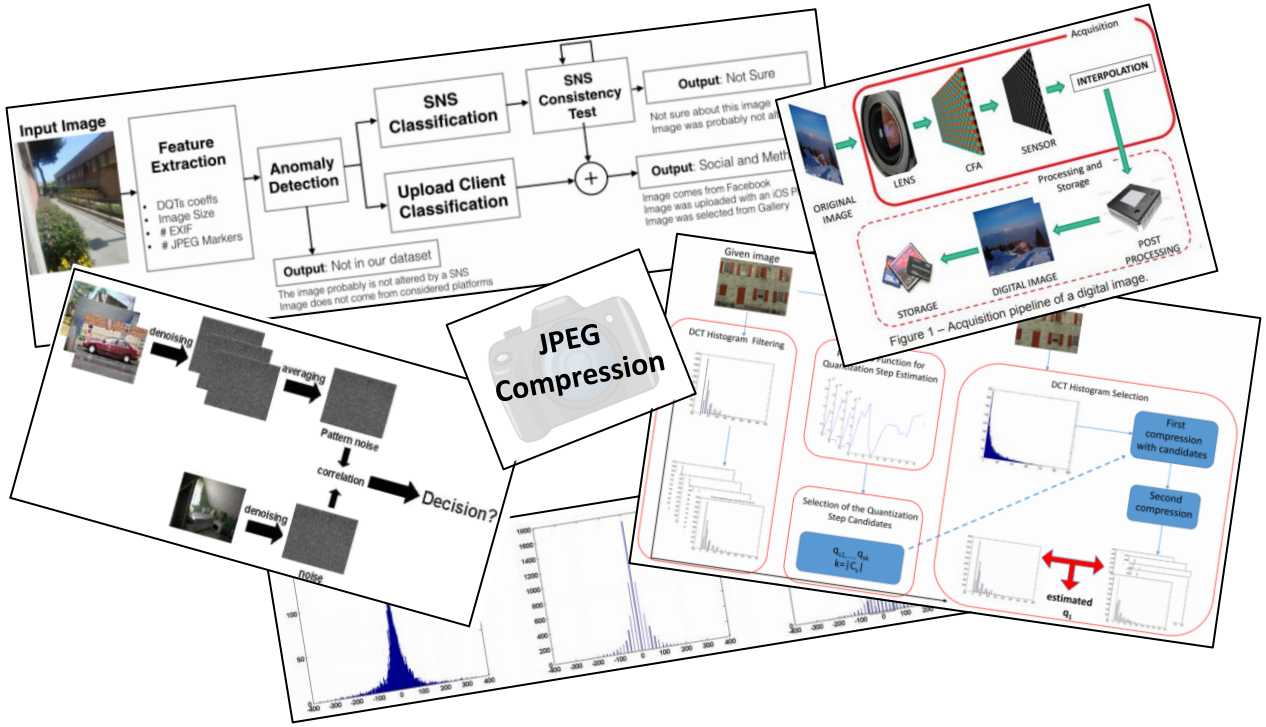
Image Forgery

Vs

DeepFake



Forgery Detection Methods



Deepfake Detection Methods

Digital Forensics Expert

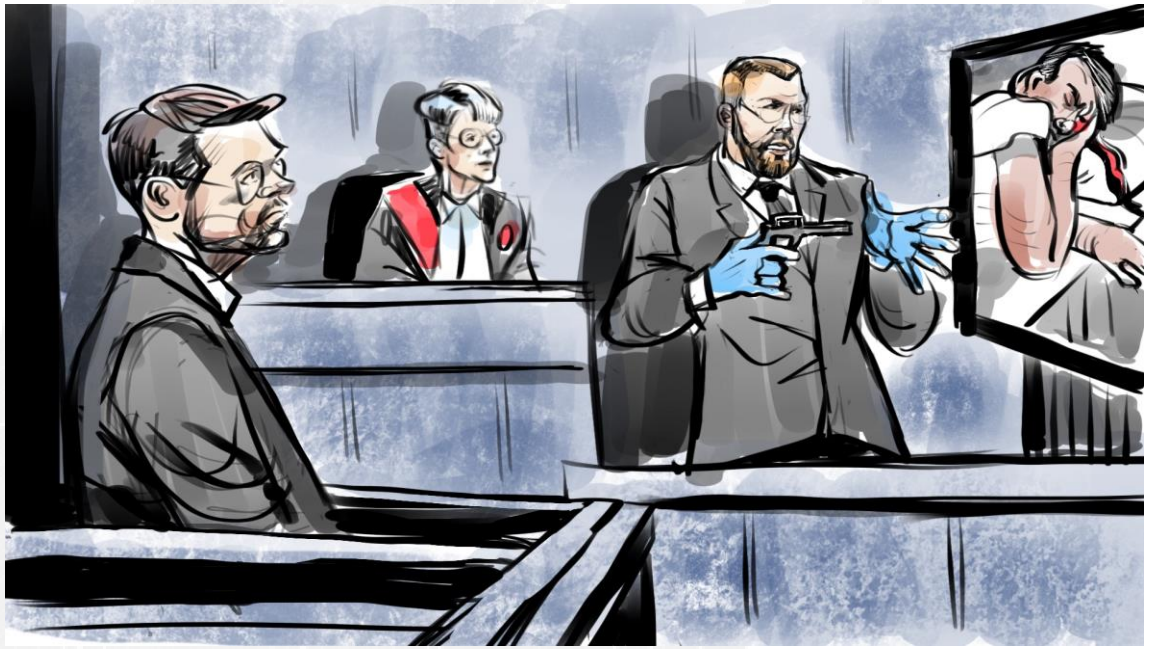
Digital Forensics Expert

- L'informatico forense deve avere conoscenze **tecnico** e **giuridico**
- Le attività sono dirette a qualsiasi attrezzatura elettronica con potenzialità di memorizzazione dei dati: **Cellulari**, **smartphone**, **sistemi di domotica**, **autoveicoli** e **tanto altro**.

Data l'eterogeneità dei supporti investigabili, si preferisce denominare questa figura professionale, **Digital Forensic Expert**.

Digital Forensics Expert

- Non basta saper **scovare**, **analizzare** e **conservare** una fonte di prova, bisogna anche saperla **spiegare** / **presentare** / **illustrare** renderla comprensibile agli addetti ai lavori.
- Bisogna comprendere che la fonte di prova informatica, comunque, è immersa in un quadro probatorio complessivo.



Dato digitale

Il dato digitalizzato come oggetto di indagine

ICT: Tipologie di Reato

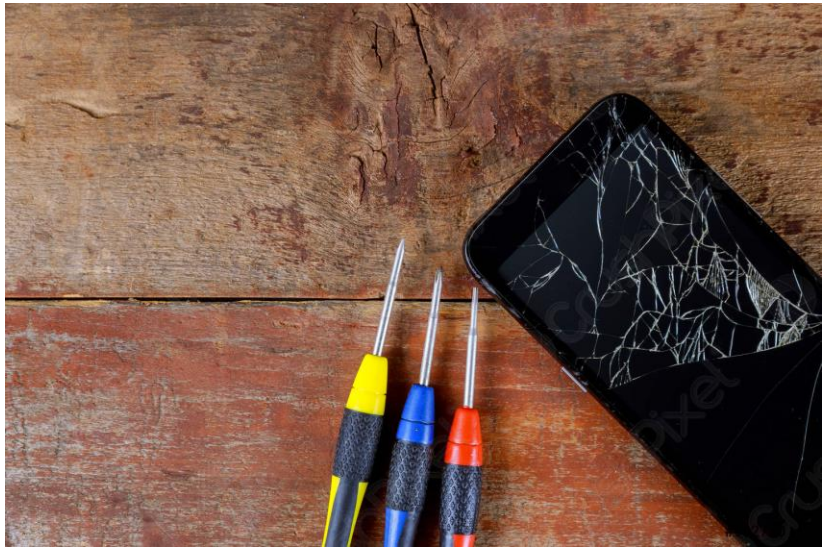
Reati tradizionali o comuni
computer come strumento

Reati relativi a contenuti
es. distribuzione di materiale illegali o illeciti

Reati di danneggiamento
es. distribuzione di virus

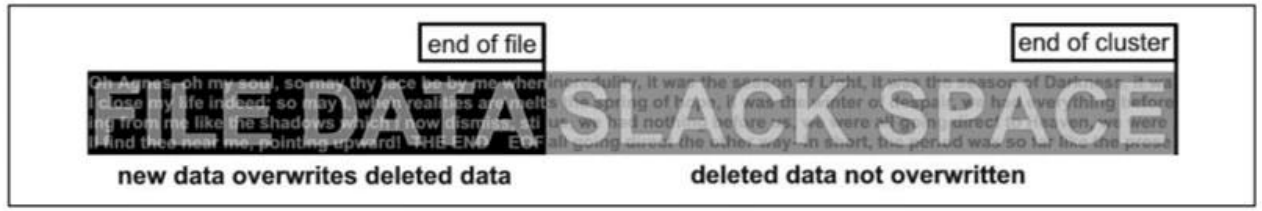
Limiti dell’Informatica Forense

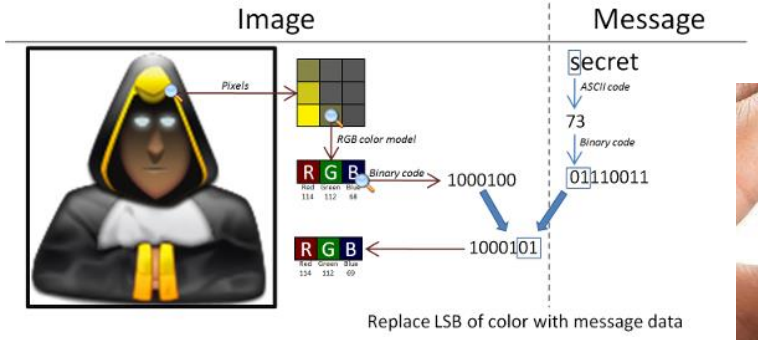
- **Estrema facilità di alterazione dei reperti**
- **Facile creazione ad arte di elementi probatori**
- **Difficile riconducibilità dei reperti ai veri autori**
- **Necessità di trovare riscontri (in maniera quasi paranoica)**



Main Goal

- Protect the suspect system
- Discover all files
- Recover deleted files
- Reveal contents of hidden files
- Access protected or encrypted files
- Use steganalysis to identify hidden data
- Analyze data in unallocated and slack space
- …
- Provide an opinion of the system layout
- Provide expert testimony or consultation





Chain of Custody

- **Procedure di custodia a catena**
  - Tenere un registro delle prove che indichi quando le prove sono state ricevute e sequestrate e dove si trovano.
  - Registrare le date di rilascio degli oggetti a chiunque
  - Limitare l'accesso alle prove
  - Collocare il disco rigido originale in un armadietto delle prove
  - Eseguire tutte le analisi forensi su una copia speculare, mai sui dati originali.

Il Reperto informatico: le 5 fasi

- Identificazione
- Acquisizione
- **Analisi**
- Valutazione
- Presentazione

Modalità operative

- Vengono generate più copie: una **master** e alcune di lavoro per tutte le parti processuali coinvolte
- Imaging consente di restituire i dispostivi originali al proprietario che così può continuare nel suo lavoro su quella risorsa
- Le immagini sono ampiamente accettate nei tribunali come rappresentazioni dei dispositivi originali

Devono essere messe in atto delle procedure atte a verificare l'autenticità e l'integrità dei dati dopo il processo di acquisizione e la generazione di successive copie.

A tal fine si utilizzano i digest ottenute tramite apposite funzioni Hash

Funzioni Hash

Il **digest** di un file (che è una successione di bit) è una stringa di simboli di **lunghezza predefinita** generata dalla applicazione di una **funzione di hash** sul file stesso

DPCM 8 febbraio 1999: *"**l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash**"*

Non è possibile dal digest risalire al testo originale

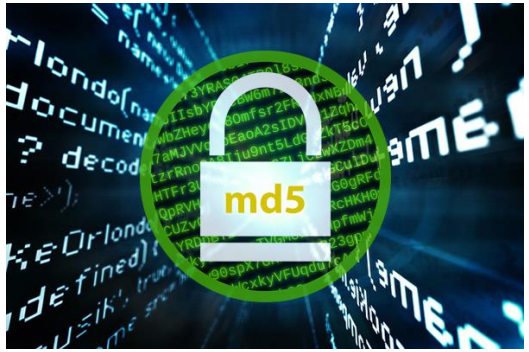
Collisioni dello **stesso valore** del digest da due **fonti diverse sono quindi pressochè impossibili**

Funzioni Hash

Nel linguaggio tecnico, la funzione hash è una **funzione** non **iniettiva** (e quindi non invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione. Nelle **applicazioni crittografiche** si chiede, per esempio, che la funzione hash abbia le seguenti proprietà:

- **resistenza alla preimmagine**: sia computazionalmente intrattabile la ricerca di una stringa in input che dia un hash uguale a un dato hash;
- **resistenza alla seconda preimmagine**: sia computazionalmente intrattabile la ricerca di una stringa in input che dia un hash uguale a quello di una data stringa;
- **resistenza alle collisioni**: sia computazionalmente intrattabile la ricerca di una coppia di stringhe in input che diano lo stesso hash.

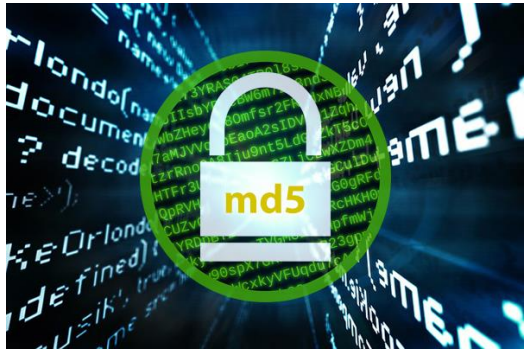
MD5



- L'acronimo **MD5** (***M**essage **D**igest algorithm **5***) indica un algoritmo crittografico di hashing realizzato da Ronald Rivest nel 1991 e standardizzato con la RFC 1321.

- Questo tipo di codifica prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a **128 bit.** La codifica avviene molto velocemente e l'output (noto anche come "MD5 Checksum" o "MD5 Hash") restituito è tale per cui è altamente improbabile ottenere con due diverse stringhe in input uno stesso valore hash in output.

MD5



- Ad oggi sono disponibili molte risorse online che hanno buone probabilità di riuscire a decriptare parole comuni codificate.

- A oggi, la disponibilità di algoritmi efficienti capaci di generare stringhe che collidono (ossia che producono in output lo stesso valore di hash) in un tempo ragionevole ha reso MD5 sfavorito rispetto ad altri algoritmi di hashing, sebbene la sua diffusione sia a tutt'oggi molto estesa (basti pensare che il controllo di integrità più frequente su file si basa proprio su MD5).

SHA (Secure Hash Algorithm)

- Con il termine SHA si indica una famiglia di cinque diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA) e pubblicate dal NIST come standard federale dal governo degli USA (FIPS PUB 180-4).

- Gli algoritmi della famiglia sono denominati SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512: le ultime 4 varianti sono spesso indicate genericamente come SHA-2, per distinguerle dal primo. Il primo produce un digest del messaggio di soli 160 bit, mentre gli altri producono digest di lunghezza in bit pari al numero indicato nella loro sigla (SHA-256 produce un digest di 256 bit).

- L'SHA-1 è il più diffuso algoritmo della famiglia SHA ed è utilizzato in numerose applicazioni e protocolli.

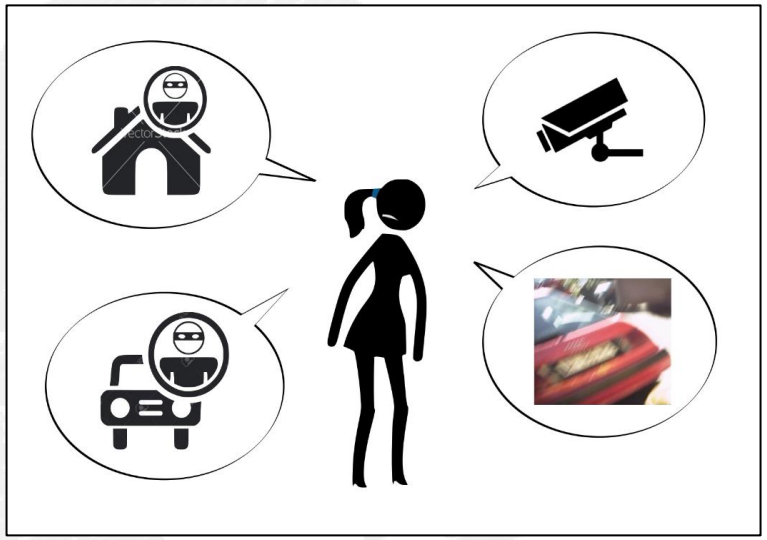
Cosa faremo nel Laboratorio di Digital Forensics?

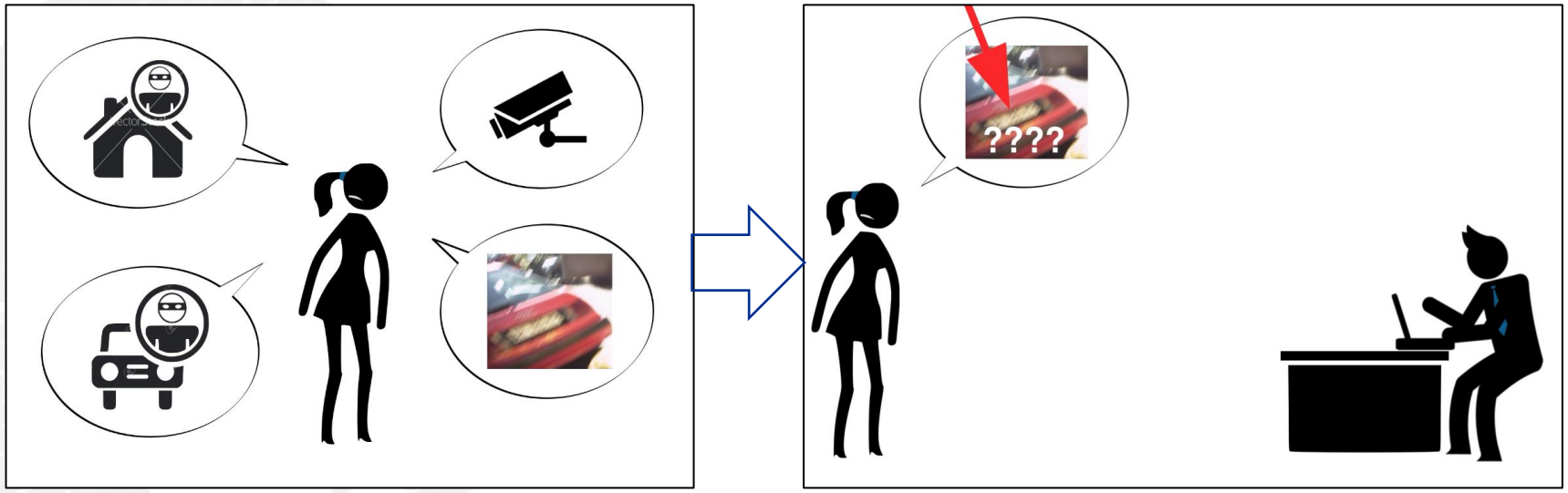
Utilizzeremo vari strumenti …

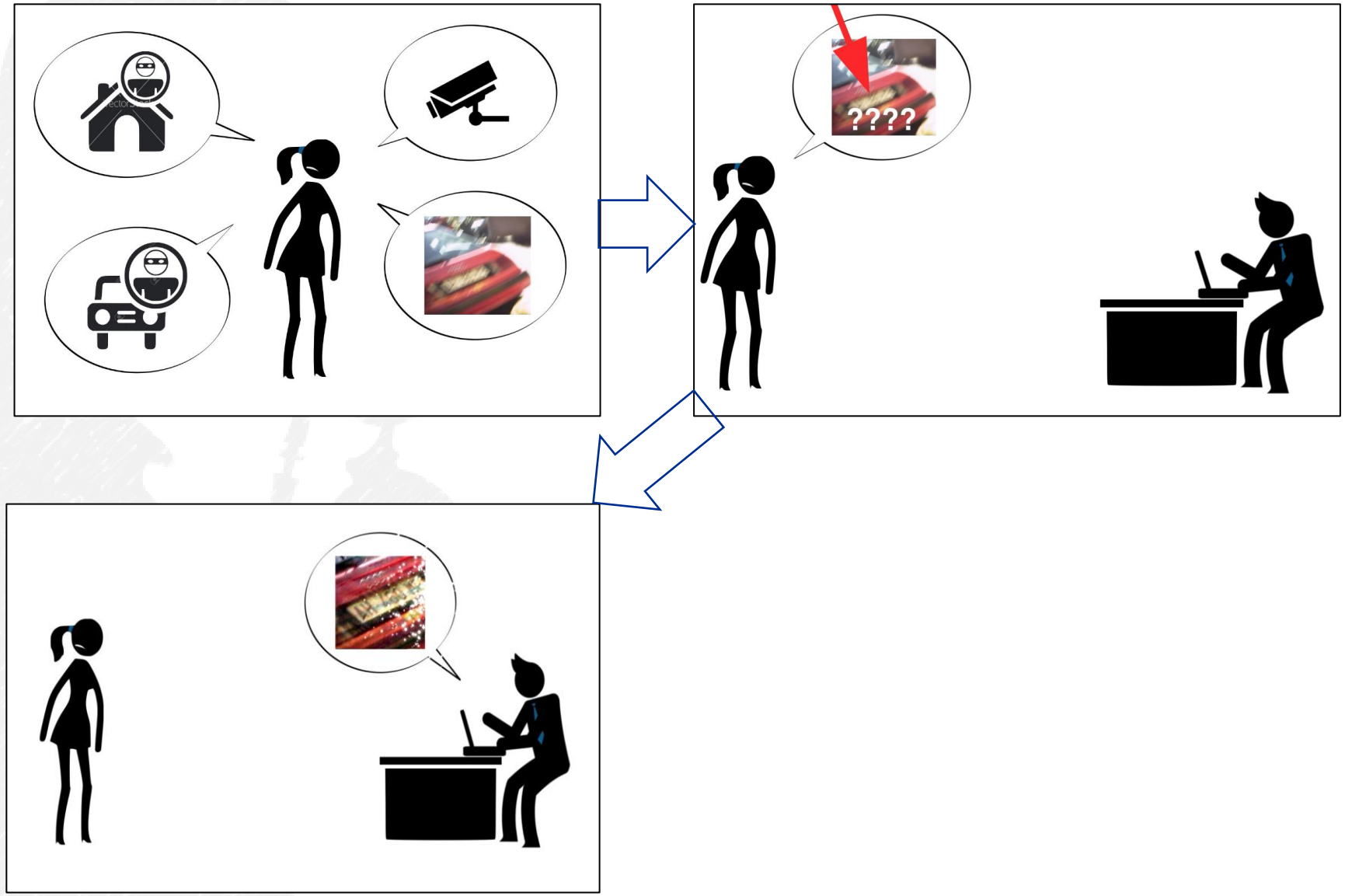
AMPED FIVE

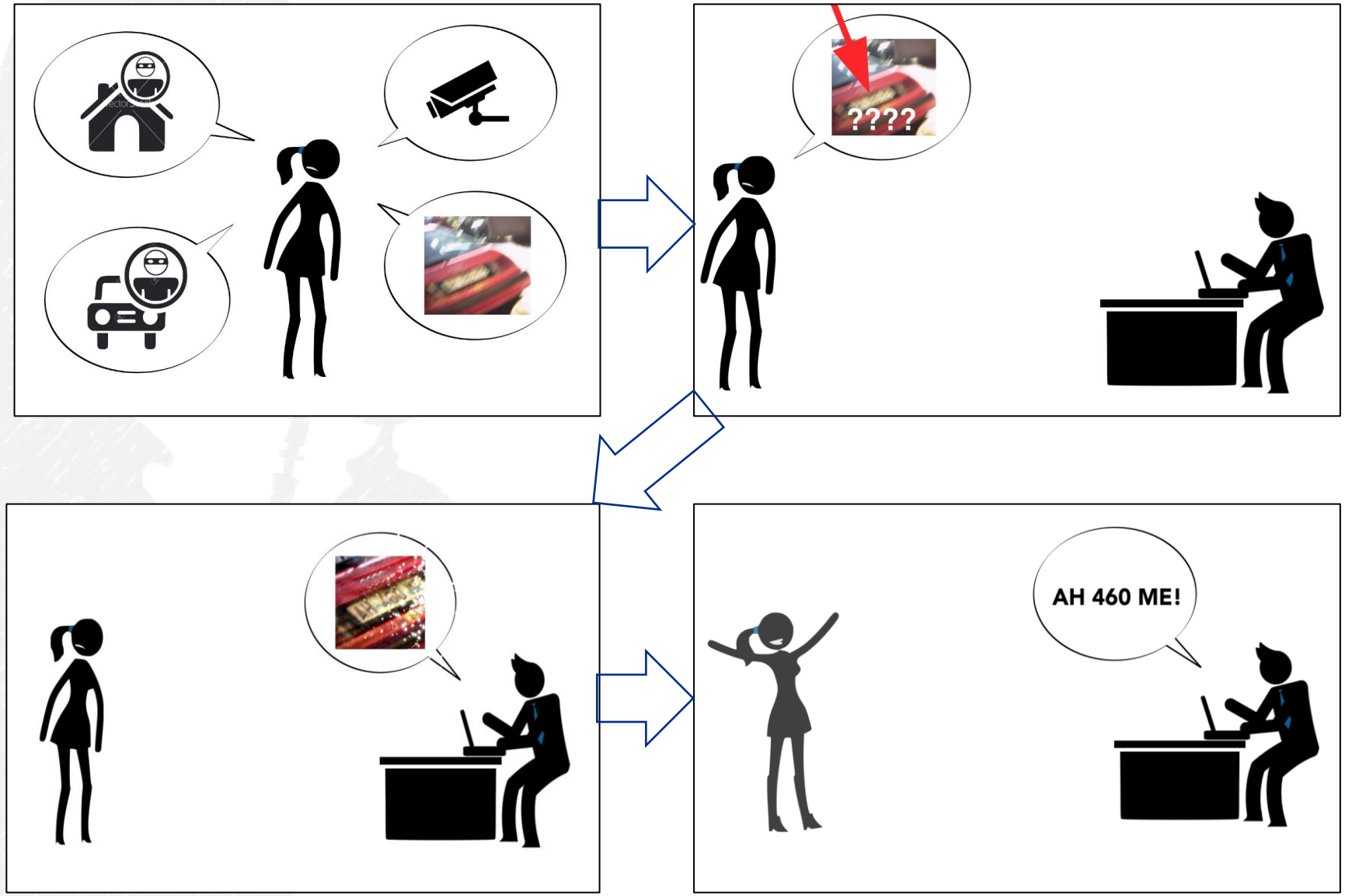
AMPED AUTHENTICATE

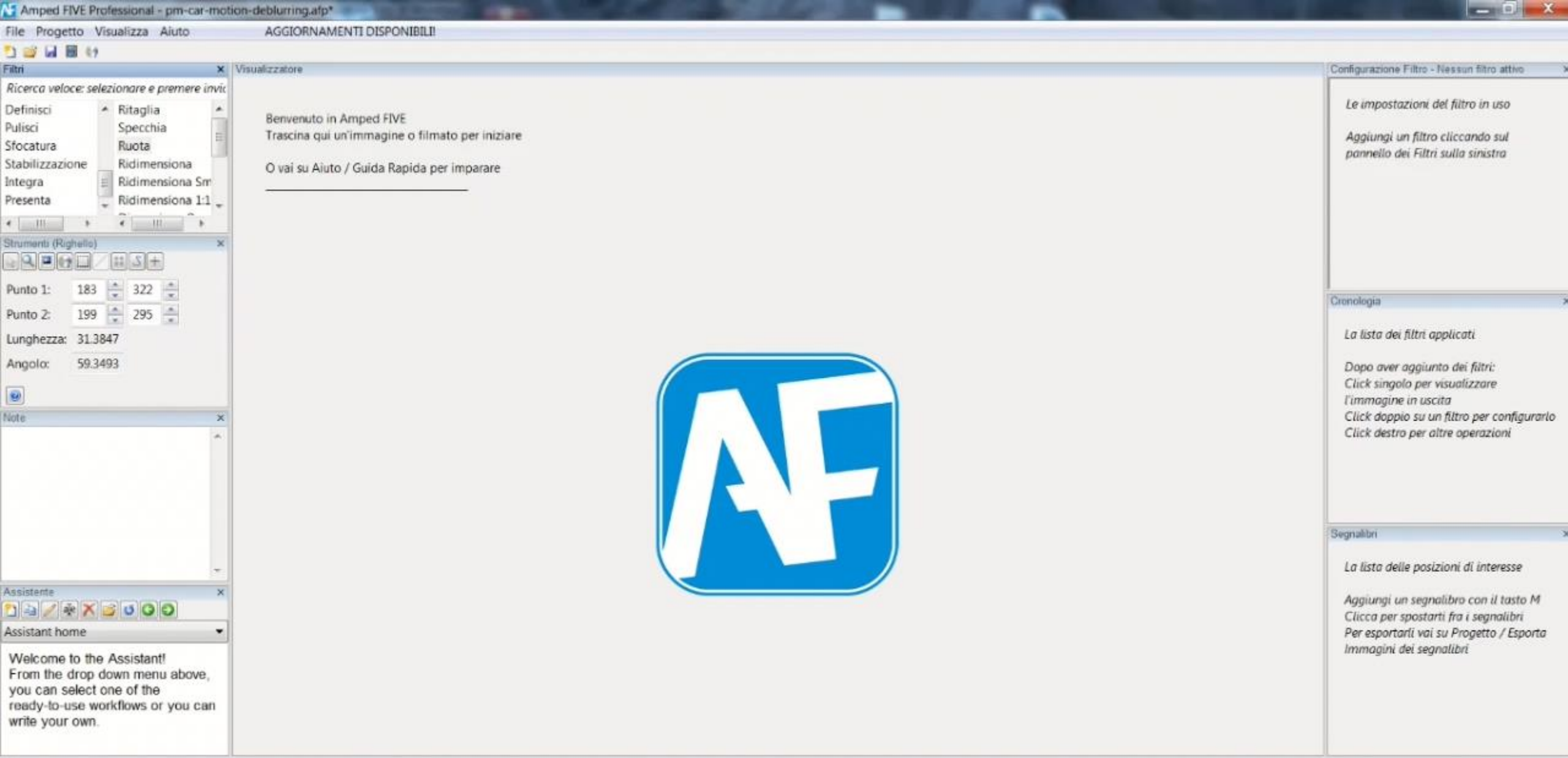
Amped Five








????
AH 460 ME!

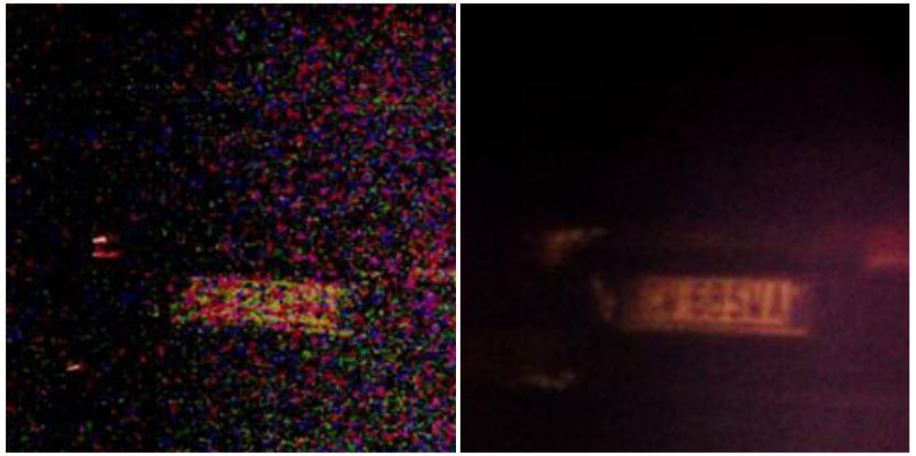

Amped FIVE Professional - pm-car-motion-deblurring.afp*
File Progetto Visualizza Aiuto
AGGIORNAMENTI DISPONIBILI!
Filtri
Ricerca veloce: selezionare e premere invio
Definisci
Pulisci
Sfocatura
Stabilizzazione
Integra
Presenta
Ritaglia
Specchia
Ruota
Ridimensiona
Ridimensiona Sm
Ridimensiona 1:1
Strumenti (Righello)
Punto 1: 183 322
Punto 2: 199 295
Lunghezza: 31.3847
Angolo: 59.3493
Note
Assistente
Assistant home
Welcome to the Assistant!
From the drop down menu above, you can select one of the ready-to-use workflows or you can write your own.
Visualizzatore
Benvenuto in Amped FIVE
Trascina qui un'immagine o filmato per iniziare
O vai su Aiuto / Guida Rapida per imparare
Configurazione Filtro - Nessun filtro attivo
Le impostazioni del filtro in uso
Aggiungi un filtro cliccando sul pannello dei Filtri sulla sinistra
Cronologia
La lista dei filtri applicati
Dopo aver aggiunto dei filtri:
Click singolo per visualizzare l'immagine in uscita
Click doppio su un filtro per configurarlo
Click destro per altre operazioni
Segnalibri
La lista delle posizioni di interesse
Aggiungi un segnalibro con il tasto M
Clicca per spostarti fra i segnalibri
Per esportarli vai su Progetto / Esporta Immagini dei segnalibri
Lettore
0
00:00:00.0
Ciclo
1
Fotogrammi
Velocità: 1.0x
Velocità
00:01
01:22
Pronto

Amped Five

Correzione della prospettiva di una scena

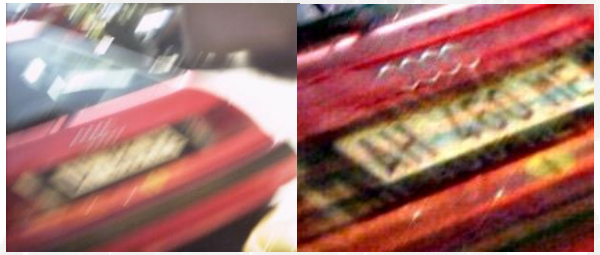
Correzione sfocatura da movimento

Miglioramento di filmato buio

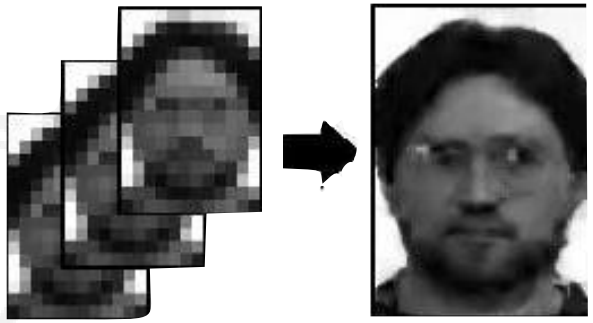


Luca Guarnera
luca.guarnera@unict.it

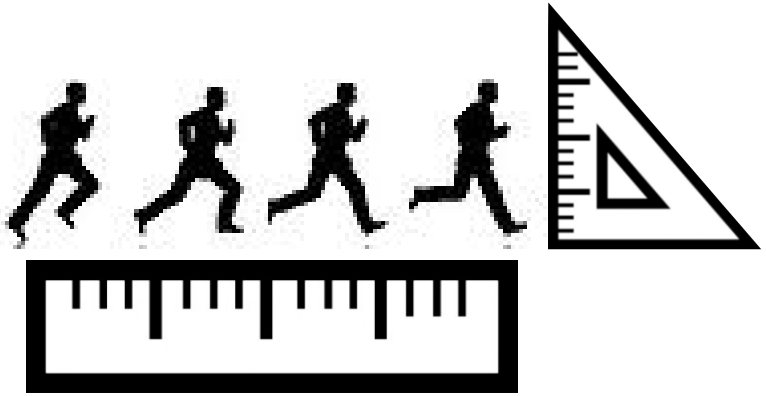
Digital Forensics



Driving Plate Reconstruction



Face Reconstruction



Biometric Analysis

Anti - Tampering

Image Enhancement

DVR Analysis

Amped Authenticate: Forensic Image and Video Authentication

Video Esempio:

- https://youtu.be/-bmN1dY5zXI

AMPED AUTHENTICATE

Dispositivi di Memorizzazione

Dispositivi di Memorizzazione

La memorizzazione nei dispositivi digitali avviene a diversi livelli:

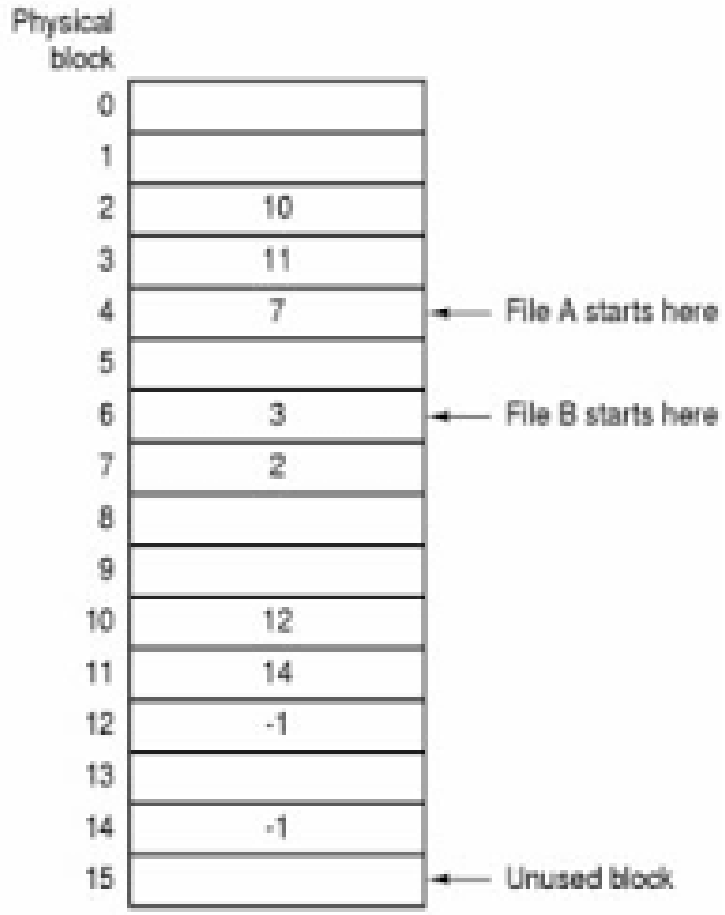
- livello **fisico**, come le particelle magnetiche e le incisioni creati dal laser
- livello **logico**, in termini di partizioni, dispositivi, tracce e settori

Le modalità con cui un dispositivo gestisce i dati a livello logico ha implicazioni dirette su qualunque analisi forense

Dispositivi di Memorizzazione

- I diversi file system utilizzano lo spazio sui dispositivi di memorizzazione in maniera **dissimile** l'uno dall'altro; servono dunque tecniche di analisi diverse per esaminare i dati memorizzati da essi

- Nei diversi file system i dati non sono necessariamente memorizzati in posizioni continue ma sono **frammentati** in blocchi che sono logicamente associati tra loro tramite informazioni di indirizzamento



Cancellazione dei dati

La cancellazione di dati dai supporti digitali può presentarsi in forme diverse:

- Se effettuata da una applicazione standard rimuove solamente l'indirizzo dell'informazione associata a ogni blocco di dati, che logicamente connette i vari blocchi che costituiscono i contenuti dei file
- I file che sono cancellati vengono rinominati in un'altra directory (ad es. Cestino, unused space)

I dati rimangono sul supporto, e sono recuperabili parzialmente, fintanto che non siano completamente sovrascritti da nuovi dati o cancellati tramite appositi strumenti (e.g. **software di wiping**). La rappresentazione fisica residua dei dati cancellati viene detta permanenza dei dati, ed è una delle cause del problema della cosiddetta «viscosità»

Software & Resources

- https://compute-forensics.com/top-ten-free-computer-forensic-software/
- https://www.toddington.com/resources/?utm_content=buffer72706&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer
- https://www.ictsecuritymagazine.com/articoli/digital-forensics-costo-zero/
- http://resources.infosecinstitute.com/computer-forensics-tools/#gref
- https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

Caine & Autopsy

Un esempio di recupero di file cancellati tramite l’uso del S.O. Caine e il software Autopsy

Università di Catania

Caine O.S.

- **Caine** (Computer Aided INvestigative Environment) è una distribuzione Linux che offre un completo ambiente di tools e software adatti per l'esperto forense.

- Caine si pone come obbiettivo di Fornire un completo supporto all'operatore durante le fasi della investigazione digitale: **Preservazione**, **acquisizione**, **esaminazione** ed **analisi**.

Caine

- La novità di CAINE 9.0 è che tutti i dispositivi sono (inizialmente) in modalità **Read-only**
  - Questo nuovo metodo di blocco della scrittura assicura che tutti i dischi vengano effettivamente preservati dalle operazioni di scrittura accidentale
- È possibile utilizzare i tool con una GUI chiamata **BlockON / OFF**.
  - Se si ha bisogno di scrivere un disco, si può sbloccare con BlockOn / Off o usare "Mounter" cambiando la policy in **writable mode**.
- È possibile usare CAINE da remoto.

Tanti tools

- **Stegdetect**
  - ottimo tool steganografico per scoprire le informazioni nascoste nelle immagini
- **Ophcrack**
  - per l’exploit delle password
- **Fundl**
  - per recuperare tutti i files cancellati in un hd
- **AIR** (Automated Image Restore)
  - utiliy avanzata per la creazione di immagini di supporti di memoria

Tools

- **Exif**
  - un software che permette di estrarre i metadati EXIF dalle fotografie digitali.
- **DvdDisaster**
  - recupero di dati da supporti ottici danneggiati.
- **Wipe**
  - software per cancellare file in modo che non siano più recuperabili.
- **Fundl**
  - software per il recupero rapido dei dati cancellati.
- **Ophcrack**
  - cracking delle password di Windows utilizzando le rainbow tables.

Tools

- **Stegbreak**
  - estrazione dei dati nascosti in file JPG mediante steganografia.
- **GtkHash**
  - calcolo dell’ hash di un file mediante diversi algoritmi.
- **Pasco**
  - analisi avanzata della cache di Internet Explorer.
- **Photorec**
  - software per il recupero dei files cancellati mediante tecniche di data carving.

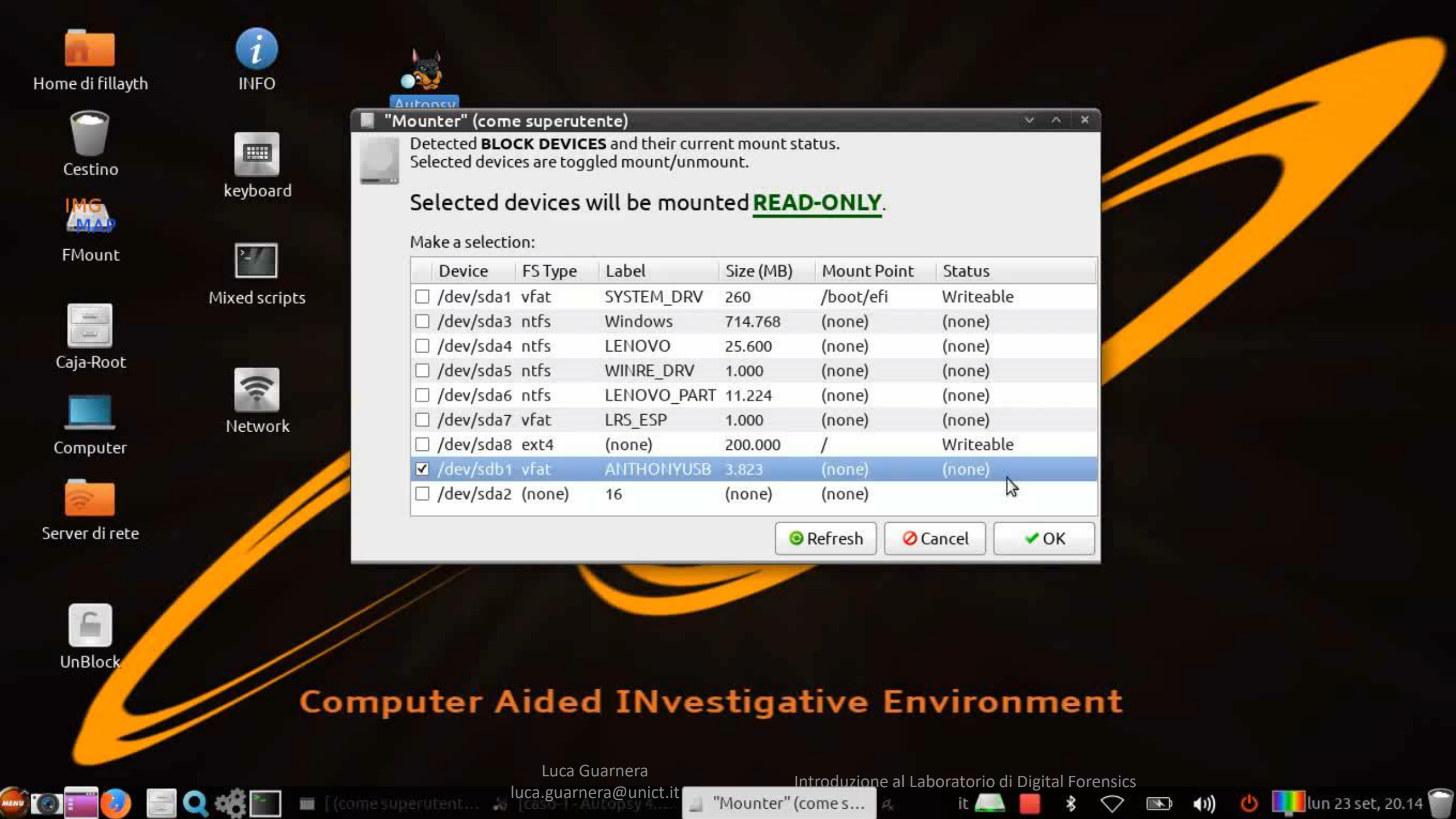
Tools

- **Guymager**
  - creazione di immagini dei supporti di memoria; meno complesso rispetto ad AIR.

- **Autopsy**
  - software per eseguire analisi su file e eventualmente recuperare quelli cancellati

Autopsy (SleuthKit)

Autopsy® è una piattaforma di digital forensics e un'interfaccia grafica per The Sleuth Kit® e altri strumenti forensi digitali. Viene utilizzato dalle forze dell'ordine, dai militari e dagli esaminatori aziendali per indagare su ciò che è accaduto su un computer, uno smartphone e su qualsiasi altro dispositivo di normale utilizzo.


Home di fillayth
INFO
Cestino
keyboard
FMount
Mixed scripts
Caja-Root
Network
Computer
Server di rete
UnBlock
"Mounter" (come superutente)
Detected BLOCK DEVICES and their current mount status.
Selected devices are toggled mount/unmount.
Selected devices will be mounted READ-ONLY.
Make a selection:
Device FS Type Label Size (MB) Mount Point Status
/dev/sda1 vfat SYSTEM_DRV 260 /boot/efi Writeable
/dev/sda3 ntfs Windows 714.768 (none) (none)
/dev/sda4 ntfs LENOVO 25.600 (none) (none)
/dev/sda5 ntfs WINRE_DRV 1.000 (none) (none)
/dev/sda6 ntfs LENOVO_PART 11.224 (none) (none)
/dev/sda7 vfat LRS_ESP 1.000 (none) (none)
/dev/sda8 ext4 (none) 200.000 / Writeable
/dev/sdb1 vfat ANTHONYUSB 3.823 (none) (none)
/dev/sda2 (none) 16 (none) (none)
Refresh
Cancel
OK
Computer Aided INvestigative Environment
"Mounter" (come s...
lun 23 set, 20.14

Il Digital forensics Expert è in grado di recuperare dati cancellati in «qualsiasi» dispositivio di memoria…

Avete mai venduto uno smatphone?

Video (Le Iene): http://www.video.mediaset.it/video/iene/puntata/376449/viviani-recupero-dati-cellulare.html

Nuove Tecnologie a supporto delle investigazioni digitali

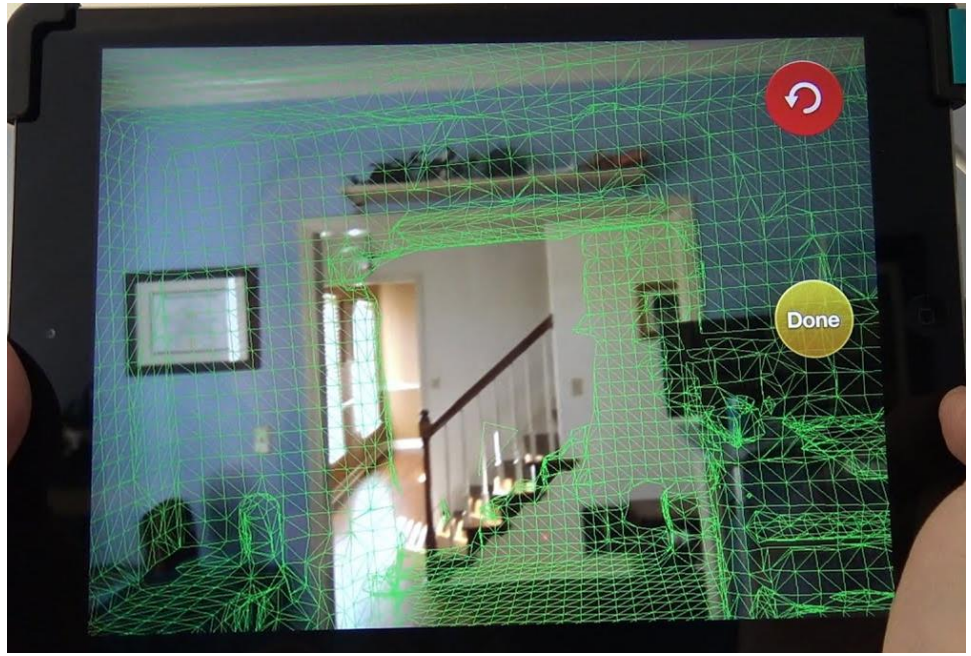
Strumenti 3D (PARTE 1)

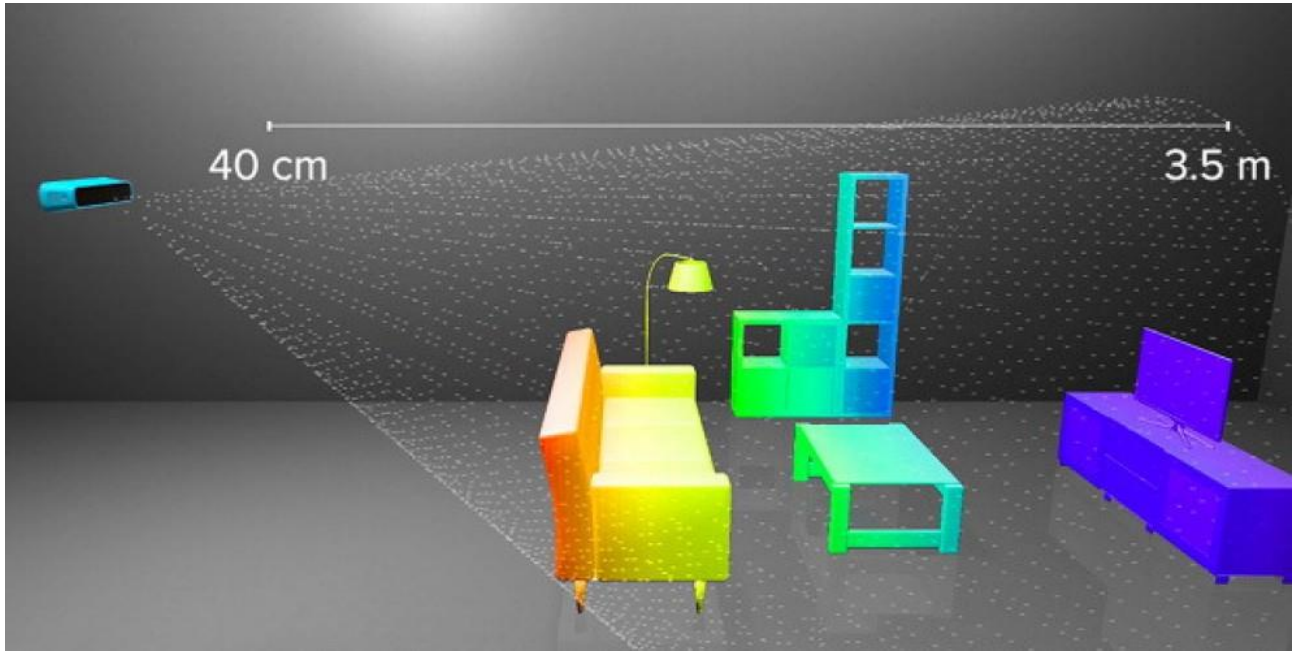
Structure Sensor

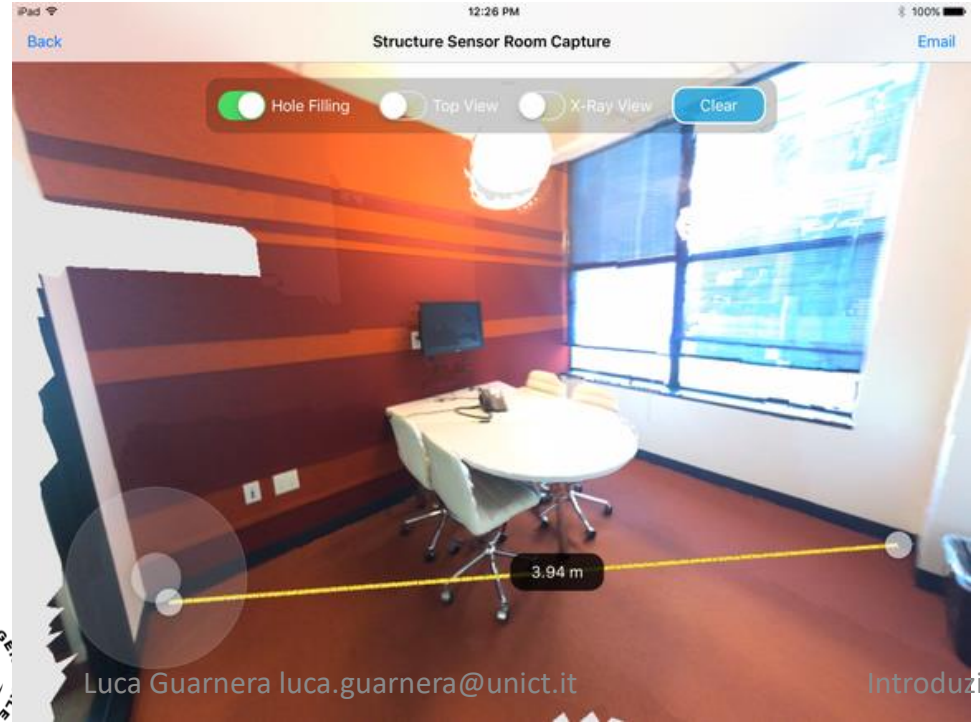
Strumento che consente di catturare oggetti in 3D applicato all'iPad.

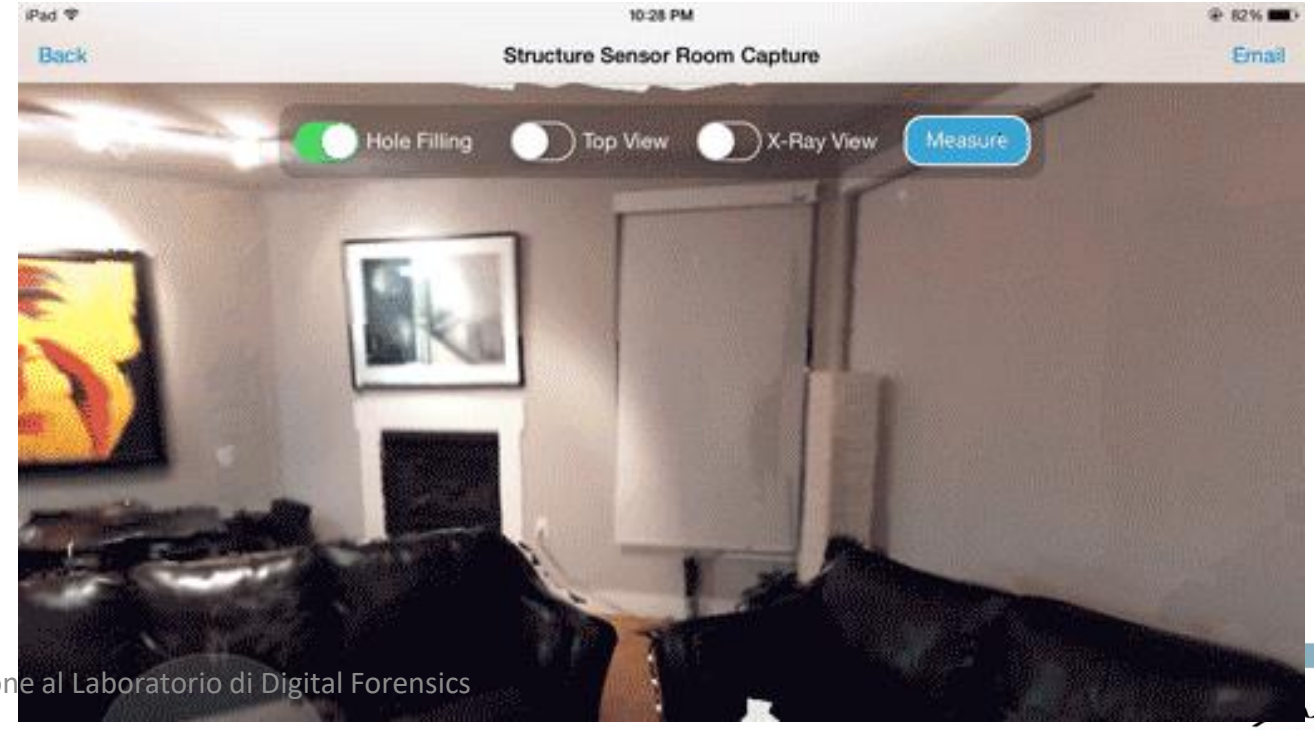
+

=


Done


40 cm
3.5 m


iPad
12:26 PM
100%
Back
Structure Sensor Room Capture
Email
Hole Filling
Top View
X-Ray View
Clear
3.94 m


iPad
10:28 PM
82%
Back
Structure Sensor Room Capture
Email
Hole Filling
Top View
X-Ray View
Measure

3D is better…

Notte dei Ricercatori 2018

Università di Catania
Dipartimento di Matematica e Informatica

Una nuova scena del crimine

Scena del crimine

Università di Catania

IMAGE PROCESSING LABORATORY

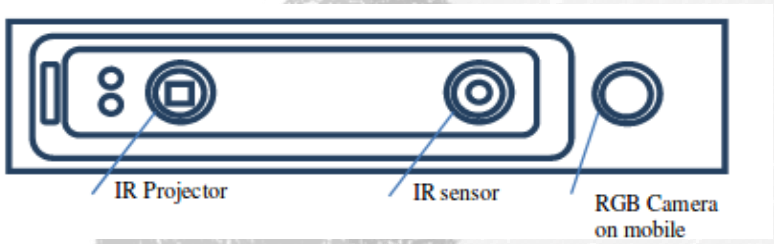
Notte dei Ricercatori 2018

Università di Catania

Dipartimento di Matematica e Informatica

Structure Sensor

By Occipital (2014)



Università di Catania

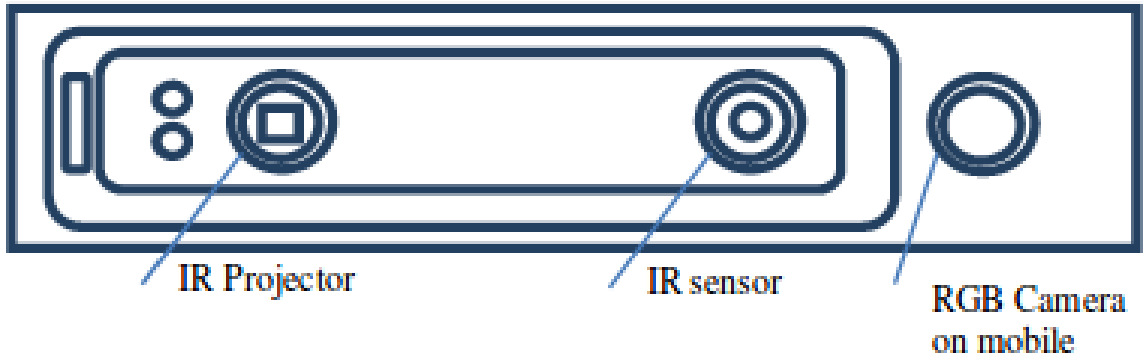
Image Processing Laboratory

Overview

E’ uno scanner che consiste in un piccolo sensore che appartiene alla categoria dello “**active scanner**”

- Sfrutta la luce strutturata a infrarossi al fine di creare una mappa 3D della scena o oggetto scansionato.

Caratteristiche



- Il sensore può acquisire oggetti fino a 12 metri.
- Ha una precisione di 0,5 mm che peggiora quando la distanza dai sensori e il volume di scansione sono aumentati.
- Poiché questo scanner utilizza la luce strutturata a infrarossi, non funziona bene se utilizzato in presenza dell'espozione del sole.

Le modalità di utilizzo

- Nella **prima modalità**, acquisiamo ed elaboriamo la **mash** di un oggetto per produrre il **modello 3D** finale.

- La **seconda modalità** consente di connettere l'iPad a un computer di uso generale utilizzando due software: **Structure** e **Skanect**.

Le modalità di utilizzo

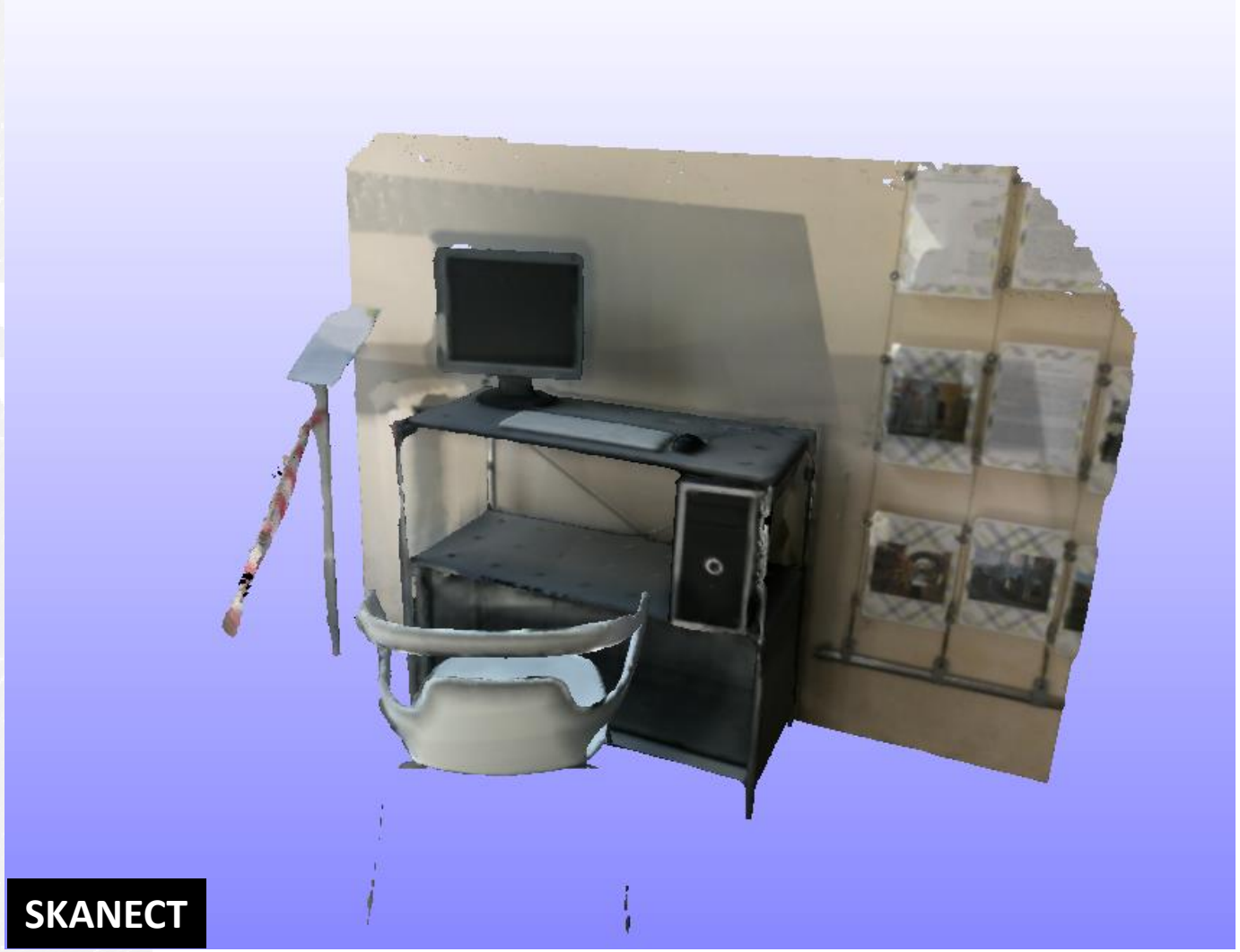


IMAGE PROCESSING LABORATORY

UNIVERSITÀ degli STUDI di CATANIA

lab

Notte dei Ricercatori

Università di Catania

Dipartimento di Matematica e Informatica

3D FLOW ZEPHYR

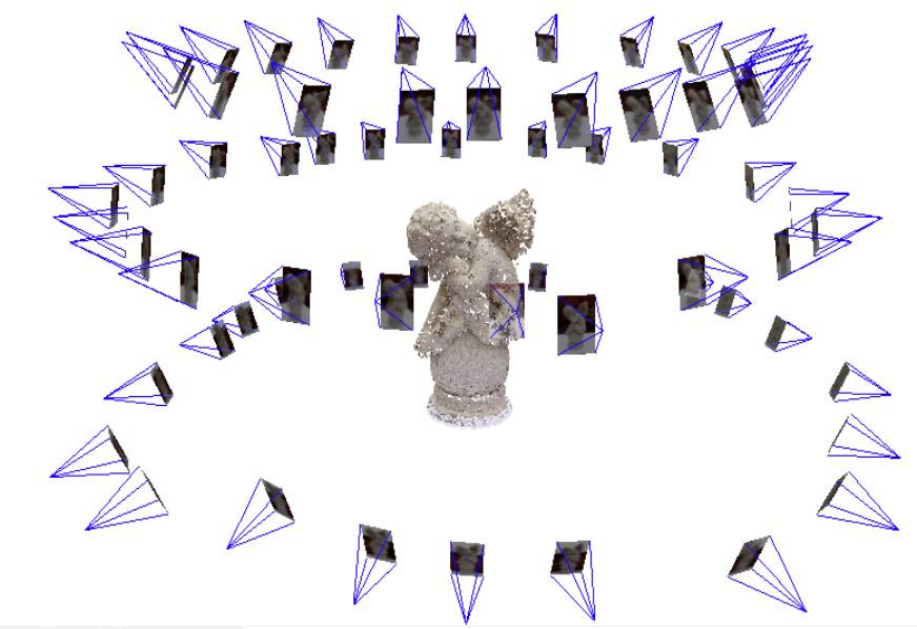
Ricostruzione modelli 3D dalla realtà acquisita

Universi
di Catan

IMAGE PROCESSING LABORATORY

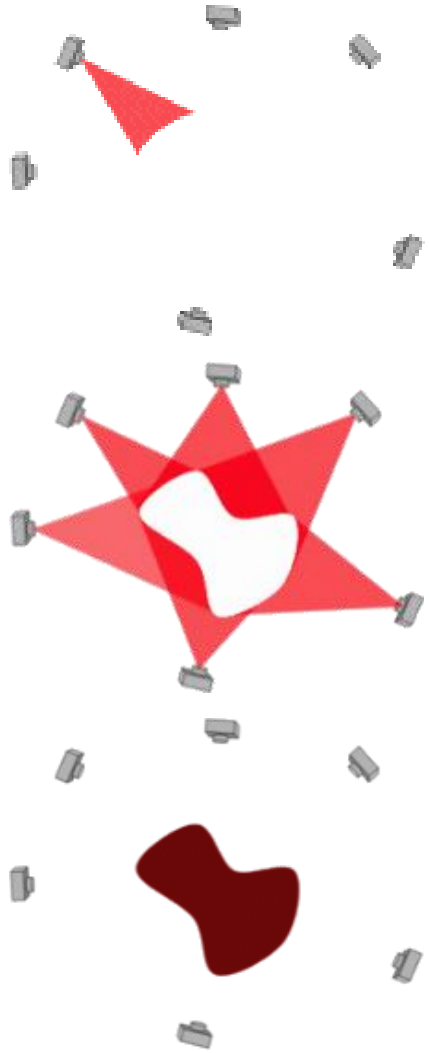
Overview

- 3DF Zephyr è un software operante nel campo della **Computer Vision** e **dell'Image Processing**. Esso utilizza particolari aspetti della fotogrammetria per la **ricostruzione in 3D** della realtà osservata.



Pipeline

1. Acquisizione dataset
2. Structure from motion
3. Multiview stereo
4. Mesh extraction
5. Texture mapping

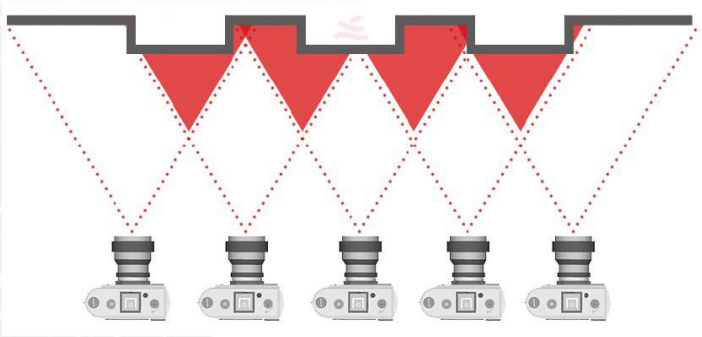


Acquisizione dataset

- È fondamentale che il dataset venga acquisito rispettando determinati criteri di qualità.

Modalità di rilievo

- Le modalità di rilievo sono svariate e particolari di caso in caso.
- È bene sottolineare come vi sia la possibilità di acquisire il dataset della scena sia tramite fotografie che tramite video.

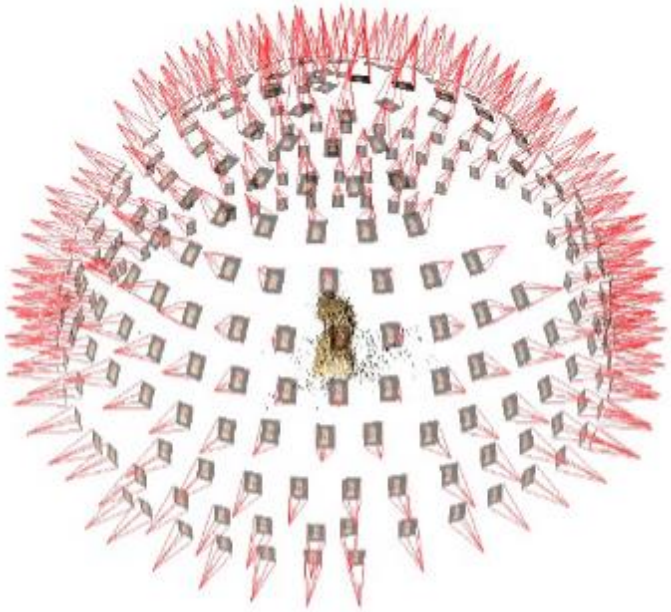


Ripresa fotografica ad assi paralleli

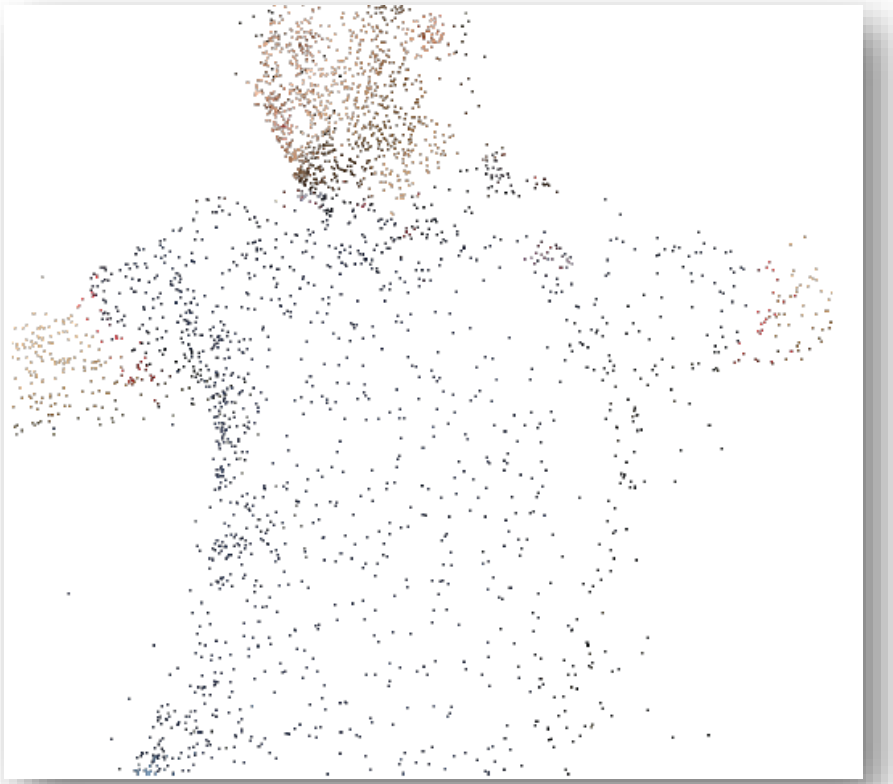
Ripresa fotografica ad assi convergenti

Structure from Motion

Il software estrae le posizioni e gli orientamenti delle fotocamere al momento dello scatto della foto. Questo particolare procedimento viene gestito dall'algoritmo proprietario che prende il nome di **SAMANTHA**.

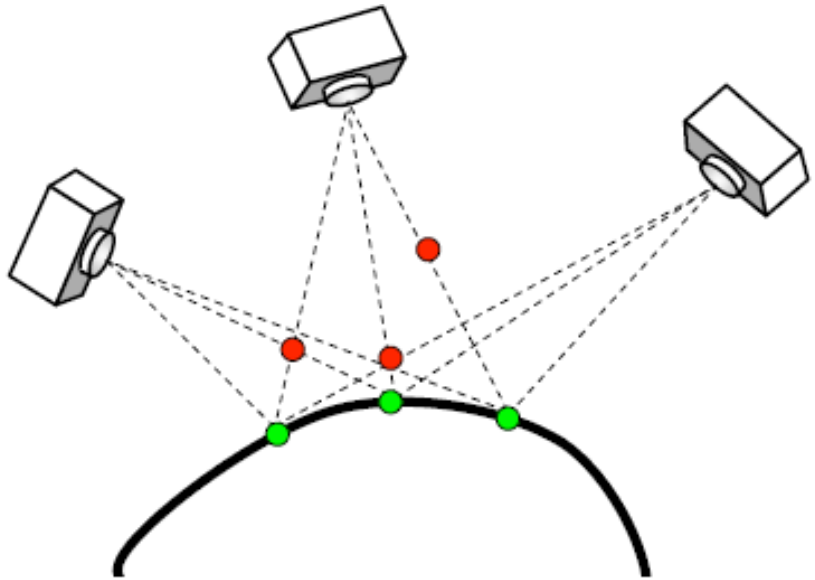


In questa fase viene a creare una nuvola di punti sparsa in cui verranno posizionati ed orientati tutti gli scatti.

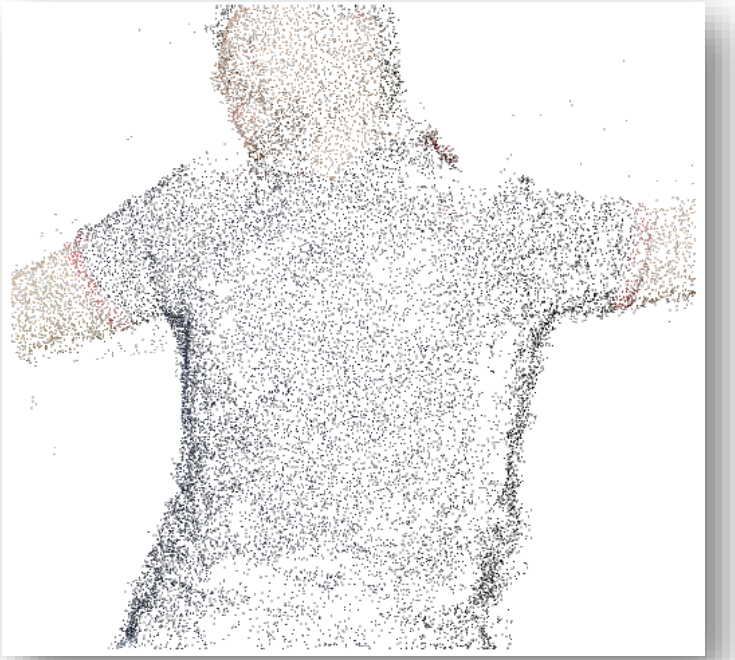


Multiview Stereo

In questa fase verrà calcolata la mappa di profondità della scena acquisita. Tale processo è gestito dall'algoritmo proprietario **STASIA**.



Tramite la mappa di profondità ottenuta in questa fase si è in grado di ricavare una **nuvola di punti densa**.



Mesh extraction

- In questa fase verrà estratta la **mesh poligonale** che rispecchia la scena catturata.

Texture mapping

- E’ spesso preferibile, invece, avere delle **mesh texturizzate** che rispecchino maggiormente i dettagli della realtà. Per tale motivo, ogni poligono che compone la mesh viene texturizzato con le porzioni di immagini su cui esso viene individuato.

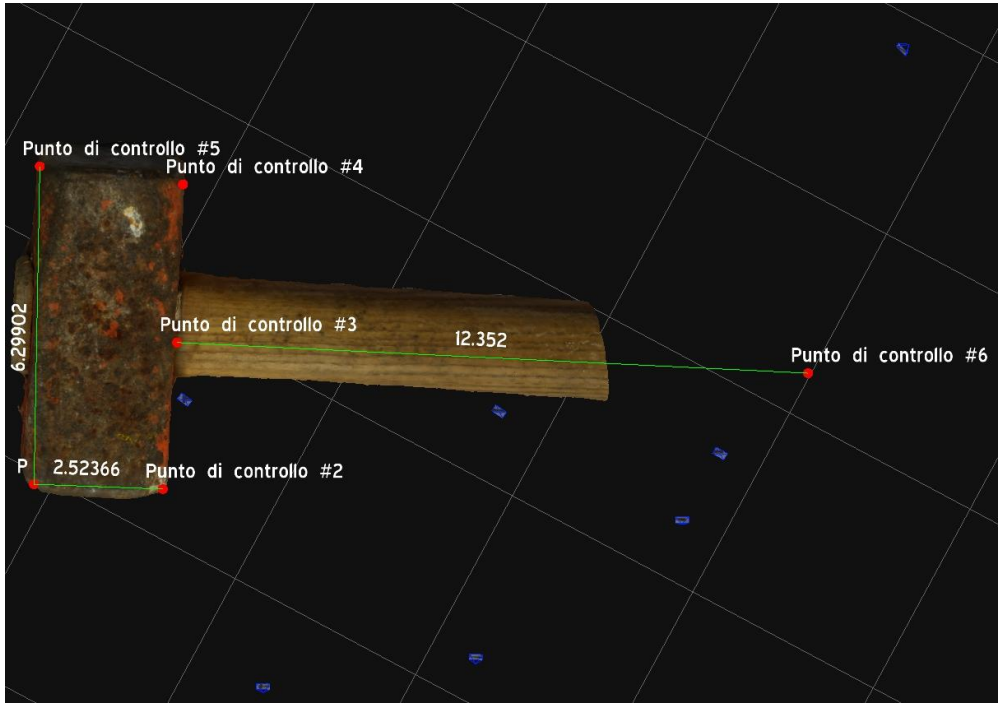
Ulteriori risorse

MULTI-ICP

3DF Zephyr supporta la gestione avanzata di dati provenienti da laser scanner grazie al cosiddetto **Multi-ICP** (Iterative Closest Point), un algoritmo studiato per minimizzare la distanza tra due nuvole di punti. È possibile, quindi, unire una nuvola di punti fotogrammetrica ad una nuvola laser.

MISURAZIONI

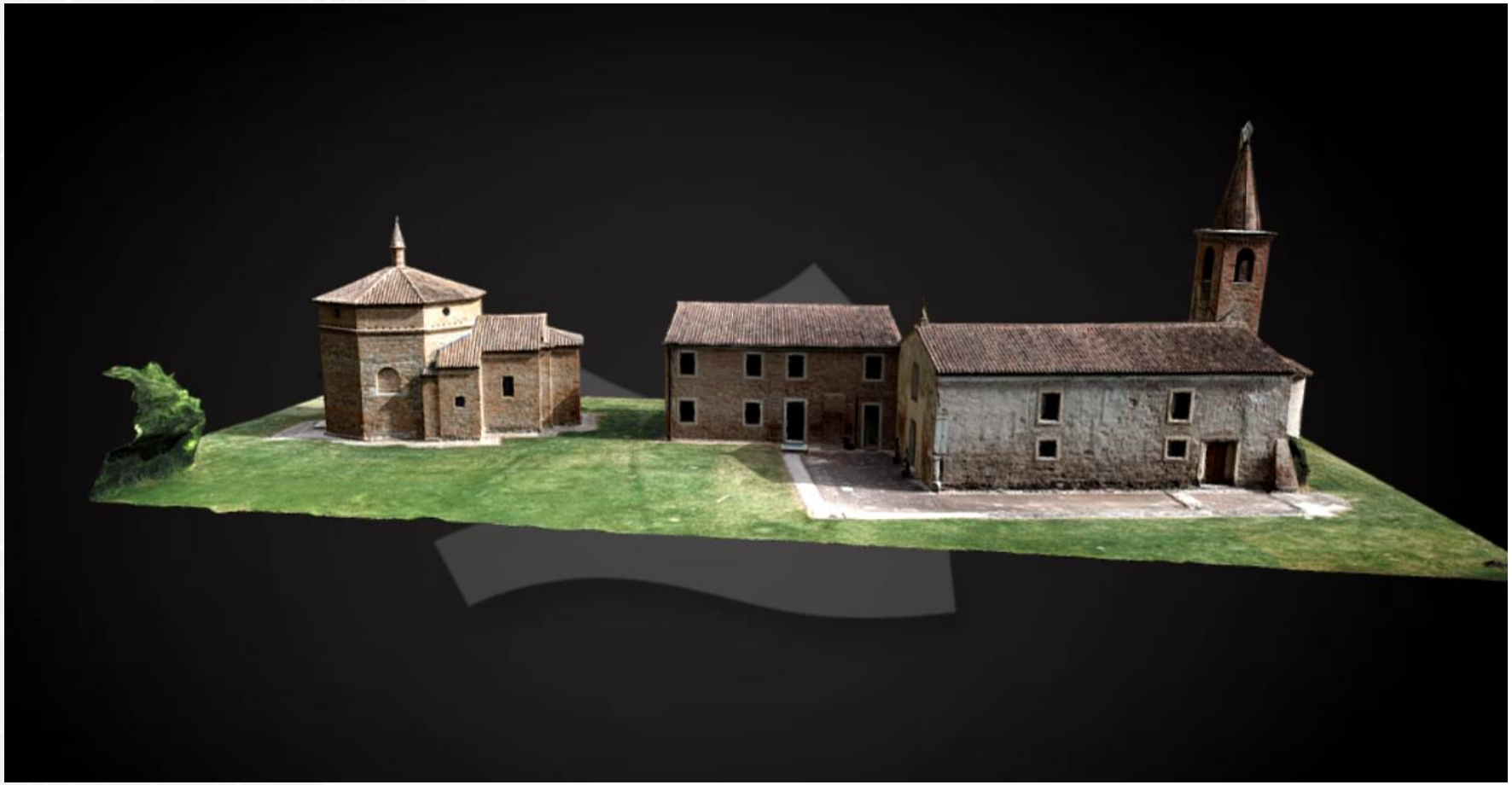
E' possibile, inoltre, eseguire rapide misurazioni in 3D. Queste vengono eseguite sulla base di alcuni punti e distanze di controllo definiti manualmente dall'operatore.



Alcuni risultati

- Foto raccolte: 33
- Dispositivo di acquisizione: LG Electronics LG-H815 (LG G4)

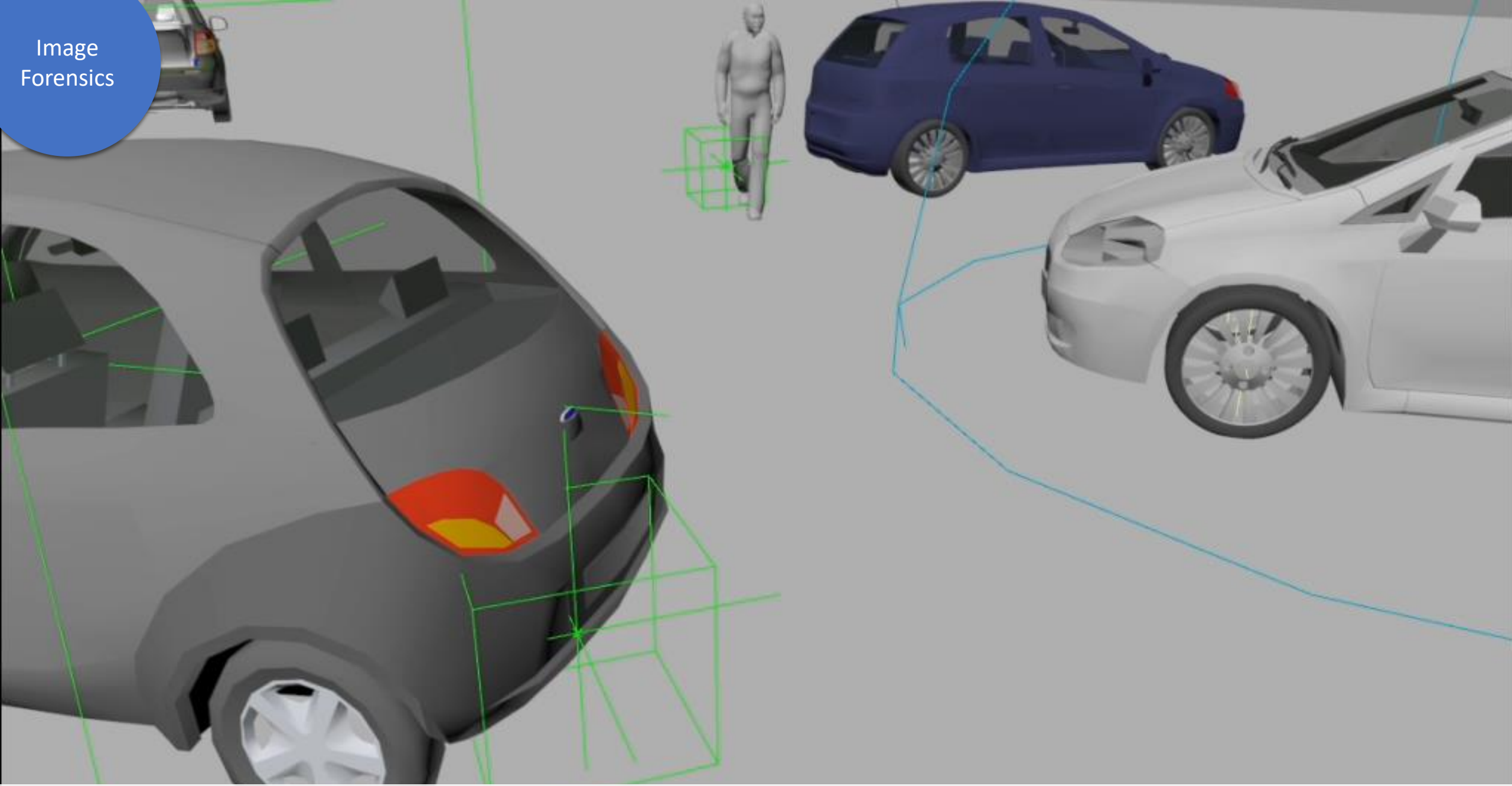
Alcuni risultati



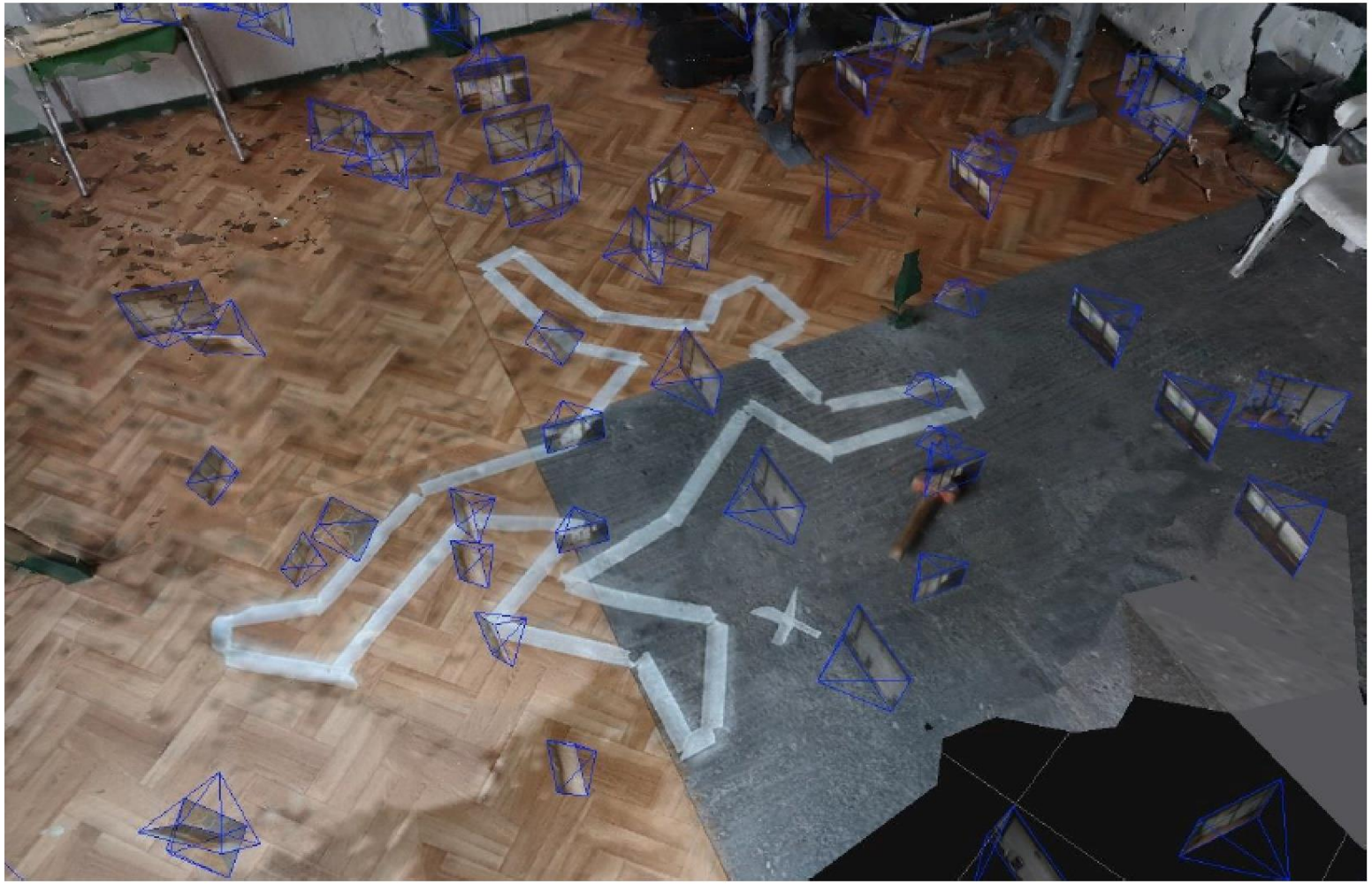
Fonte: 3dflow.net

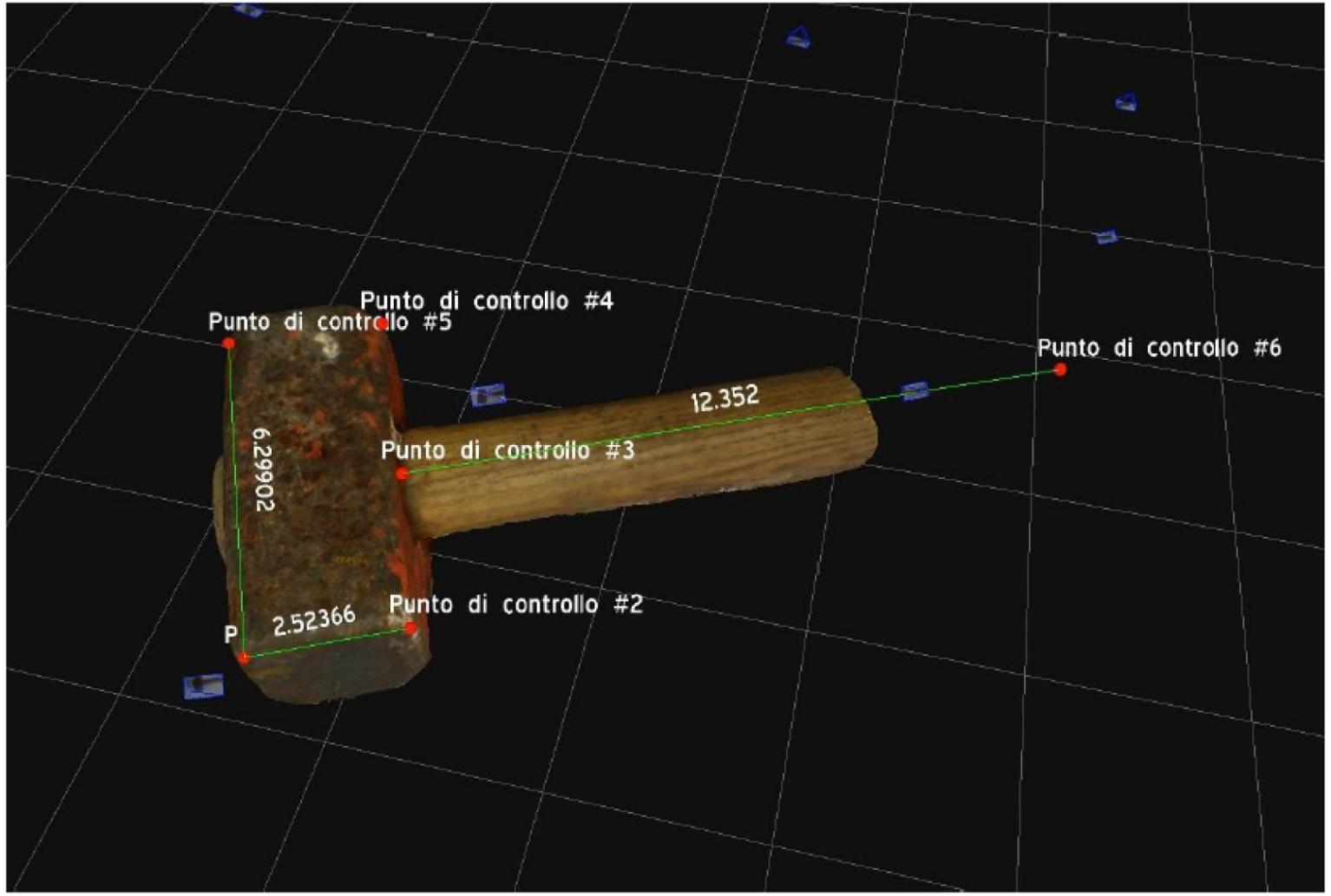
Nuove Tecnologie a supporto delle investigazioni digitali

Strumenti 3D (PARTE 2)



Altri Stumenti per la ricostruzione 3D

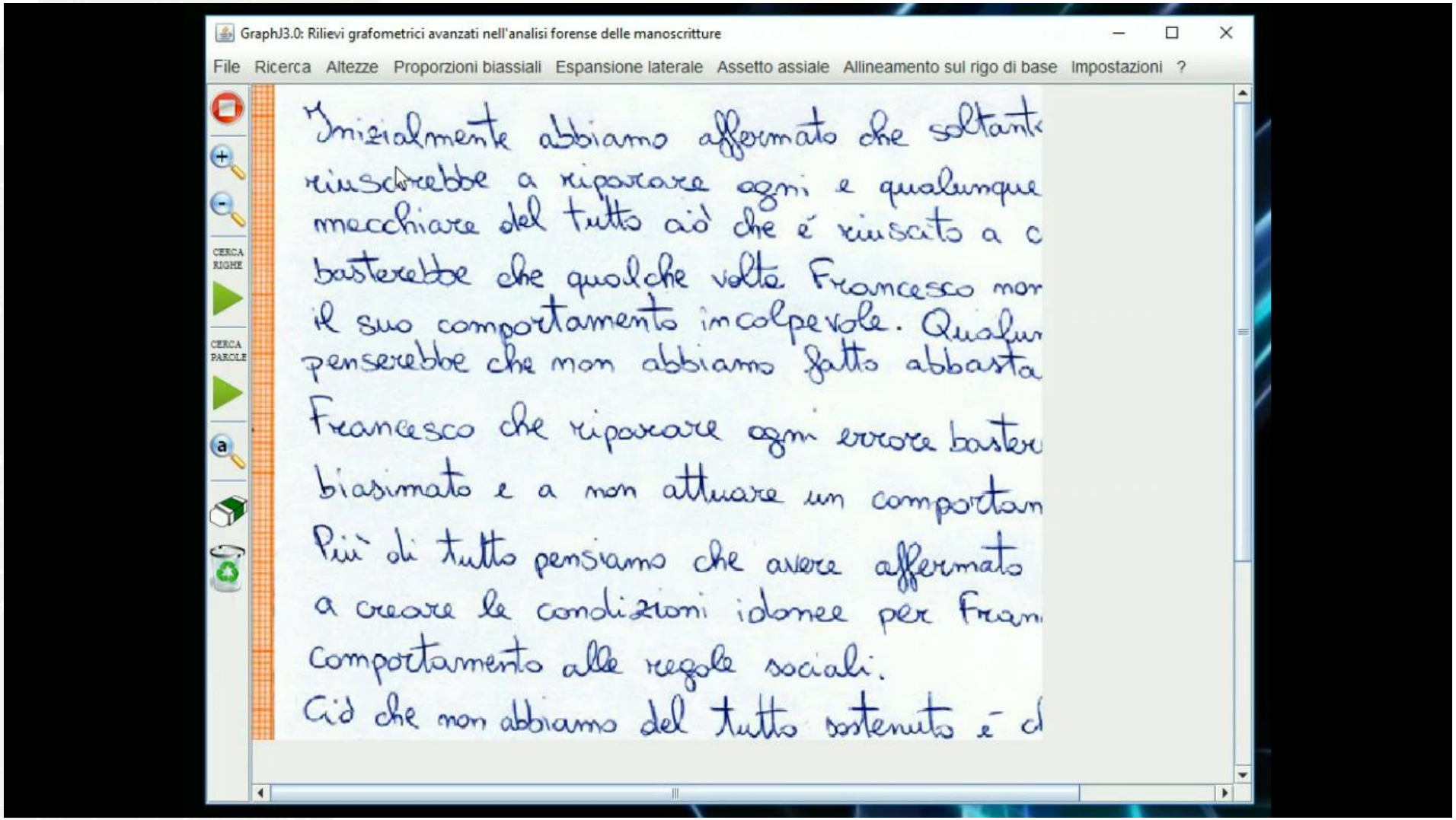



Punto di controllo #4
Punto di controllo #5
Punto di controllo #6
12.352
6.29902
Punto di controllo #3
Punto di controllo #2
2.52366
P

Nuove Tecnologie a supporto delle investigazioni digitali

Analisi forense delle manoscritture

GraphJ: Analisi Manoscritture

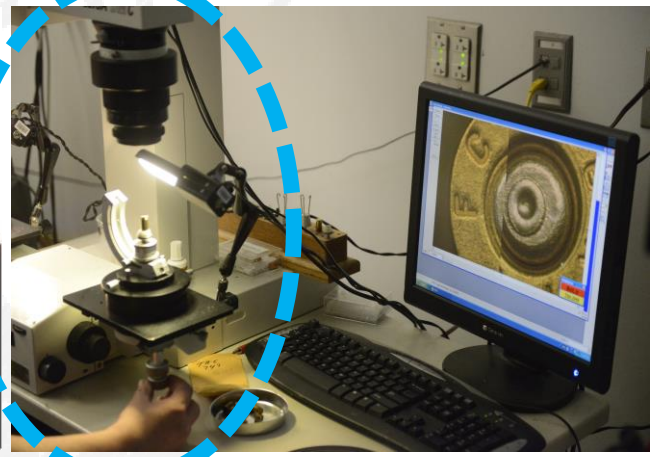


Nuove Tecnologie a supporto delle investigazioni digitali

Balistica Forense delle armi da fuoco

Forensic firearm ballistics

Forensic firearm ballistics is the science of examining the characteristics of **firearms**, **cartridges**, and/or **bullets** found at a crime scene.



- Ballistic Forensics Specialists are tasked with tying this evidence to crime suspects.
- Comparison Microscope

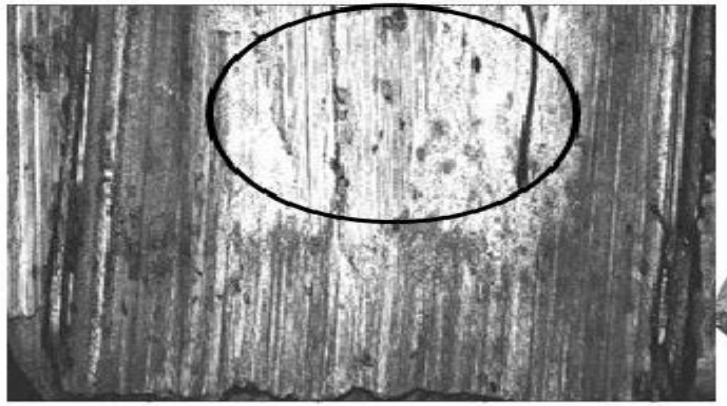
The Father of Modern Forensics Ballistics

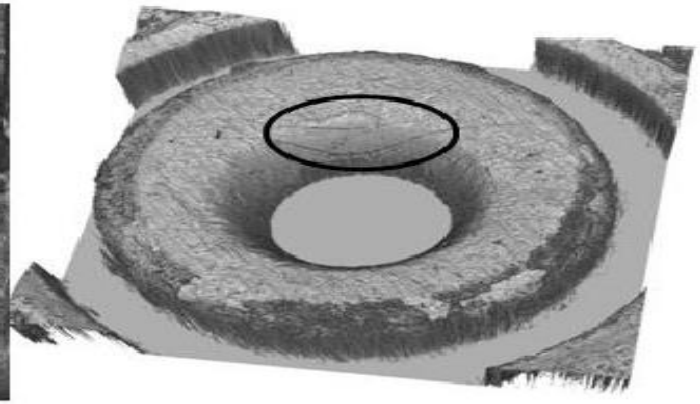
- In **1925**, **Major Calvin H. Goddard** wrote an article for the Army Ordnance titled ***Forensic Ballistics***.
- In **April 1925**, Major Goddard established the **Bureau of Forensic Ballistics** in New York City with **C. E. Waite, Philip O. Gravelle**, and **John H. Fisher**.

Forensics Examination of Firearms

Weapon serial numbers

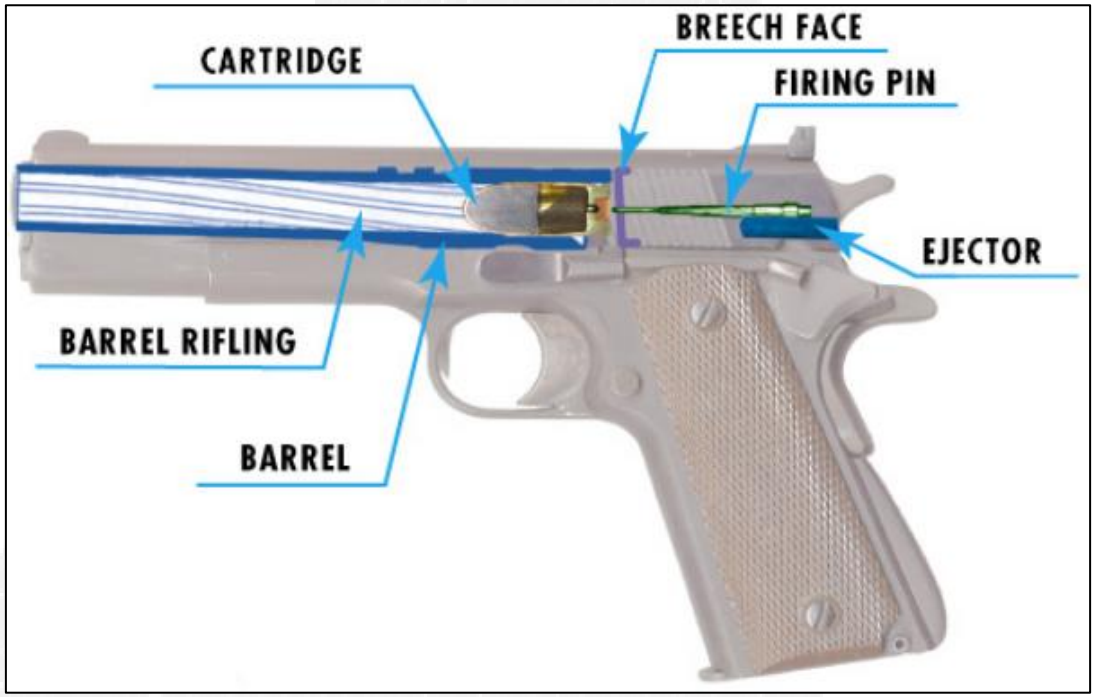
Fingerprints on the weapon's surface

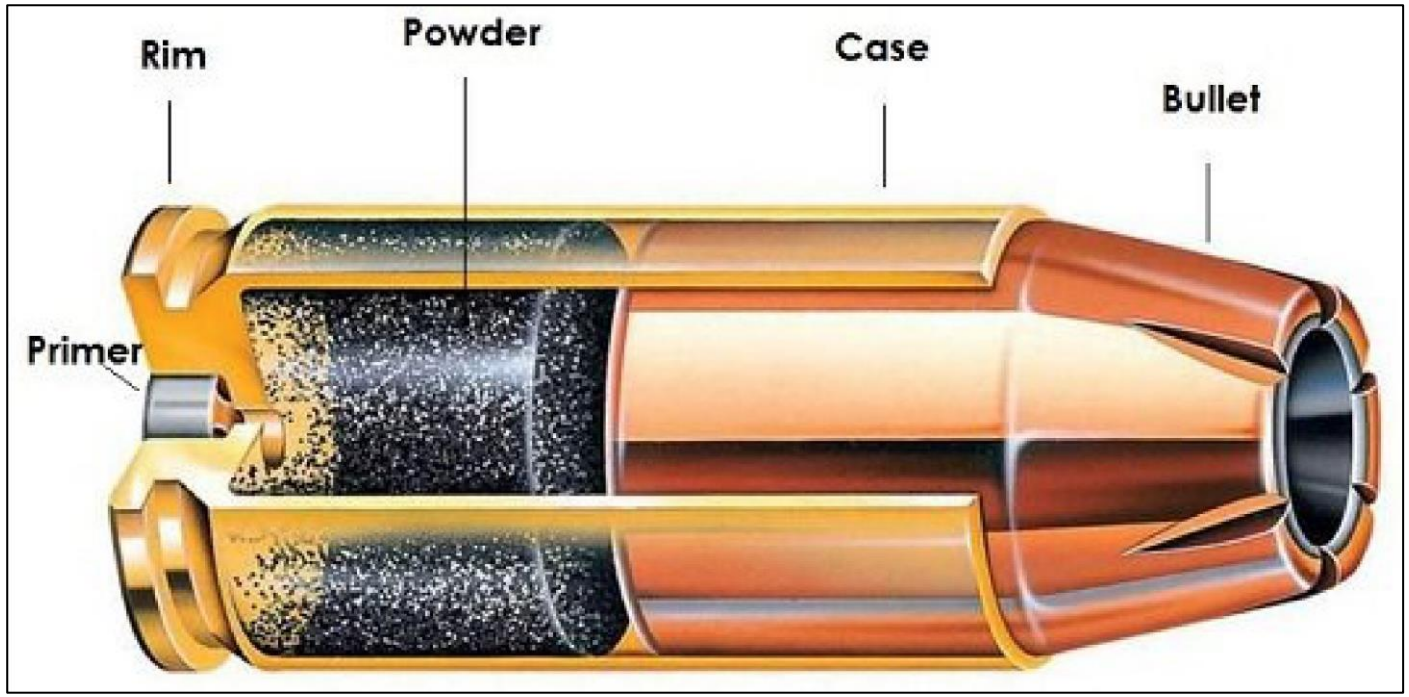




Ballistic striations

Firearm and Cartridge components





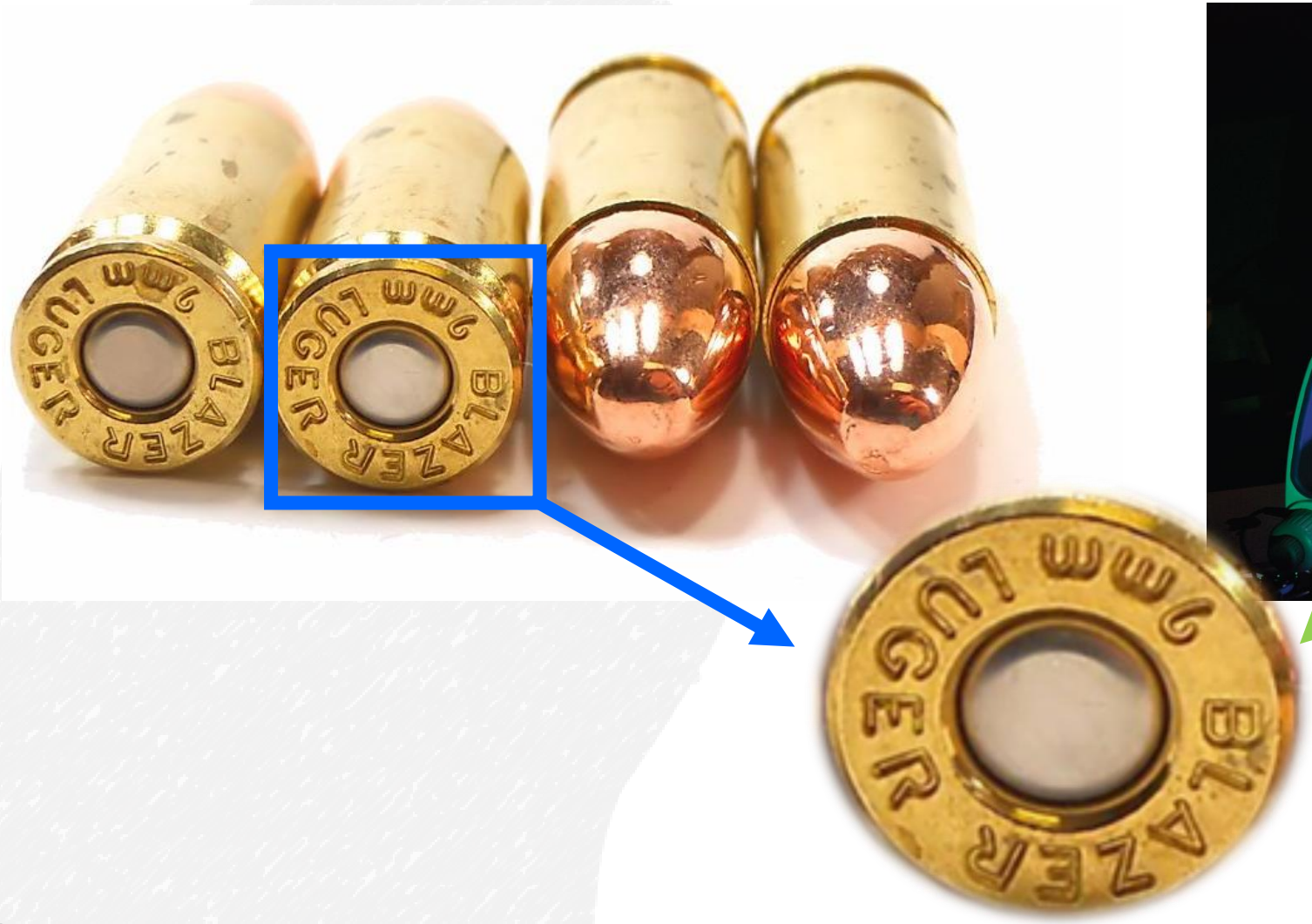
Weapon firing process

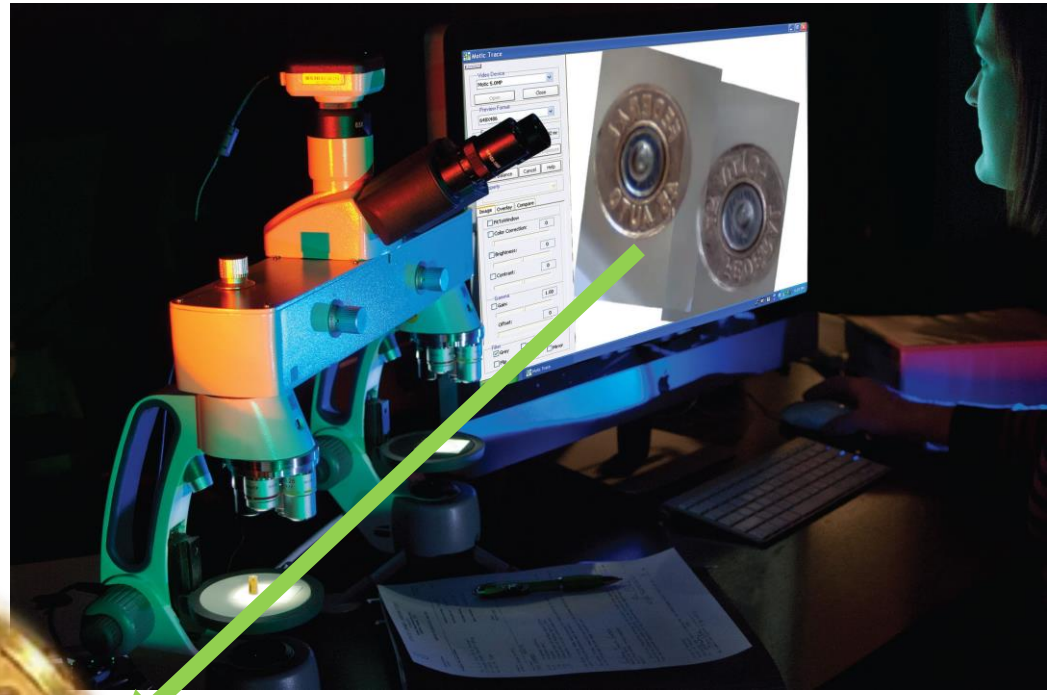
The weapon loading

The shot

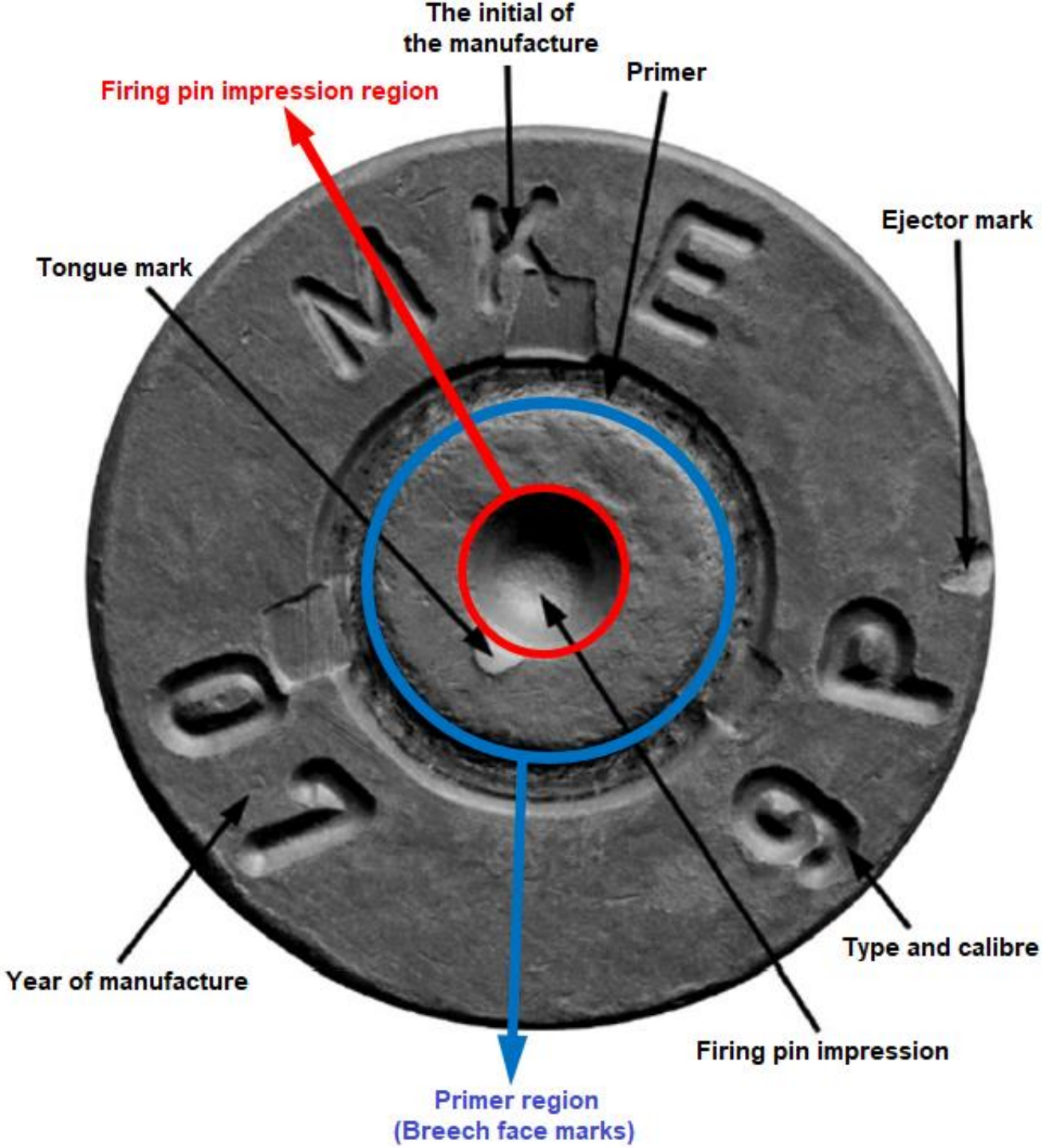
The cartridge ejection

Cartridge Analysis





Head of cartridge case and characteristics

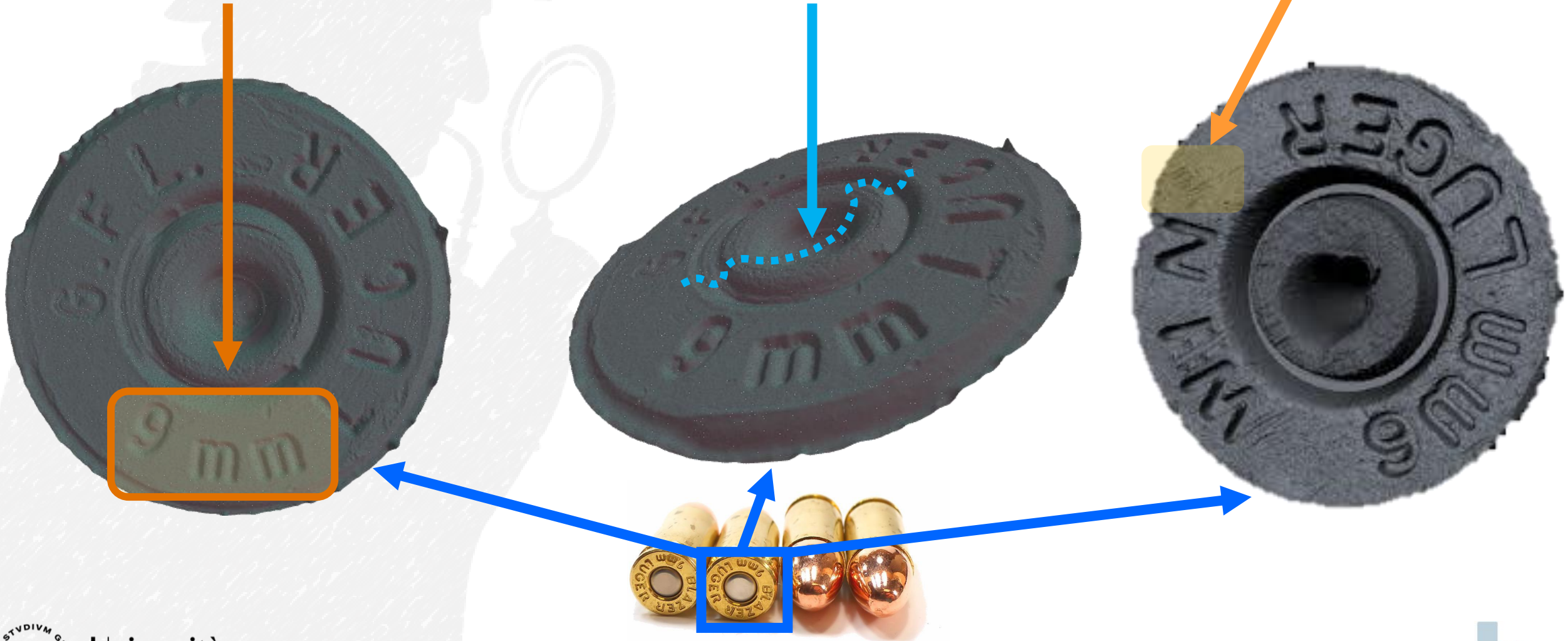


Cartridge Characteristics

Caliber of the bullet

Lands and **grooves**

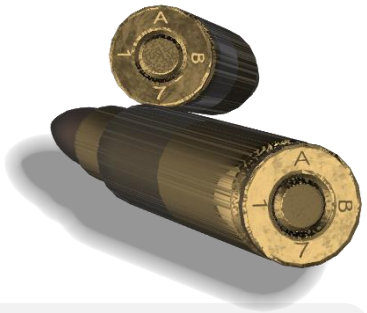
Streaks orientation



Luca Guarnera
luca.guarnera@unict.it

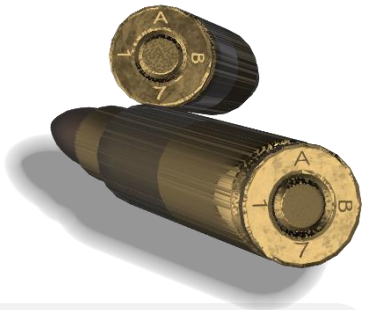
Università di Catania

Forensic Question



The cartridges found in a crime scene are compared to the cartridges fired by the suspect's gun.

Forensic Question



How do we obtain the projectiles and/or cartridge cases from the suspect's weapon without any further deformation caused by the impact with other objects?

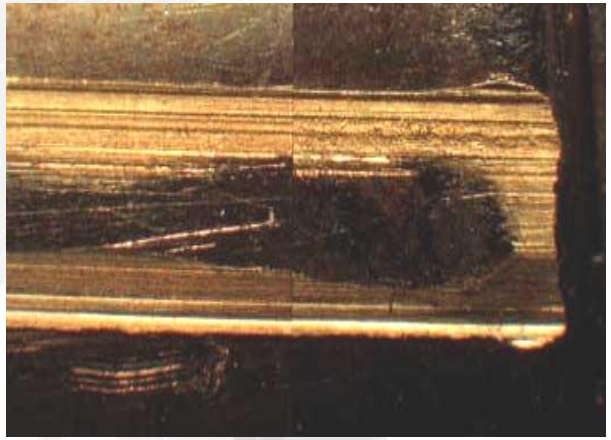
https://www.youtube.com/watch?v=tzm_yyl13yo

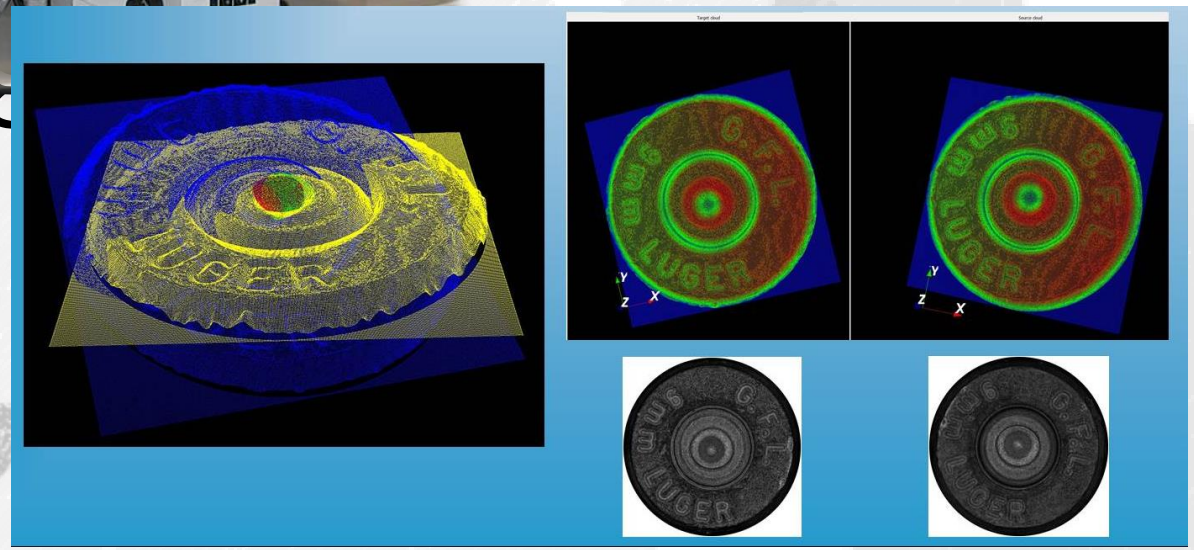
Examining the Individual Characteristics of a Bullet

- To compare individual striations, examiners have to obtain a known sample using the **seized weapon**.
- This is done by firing the weapon into a **soft target** and recovering the slug.
- Known bullet exemplars are created by firing the weapon into a **water tank**.

https://www.youtube.com/watch?v=TcyEWT2O550

Balis Di



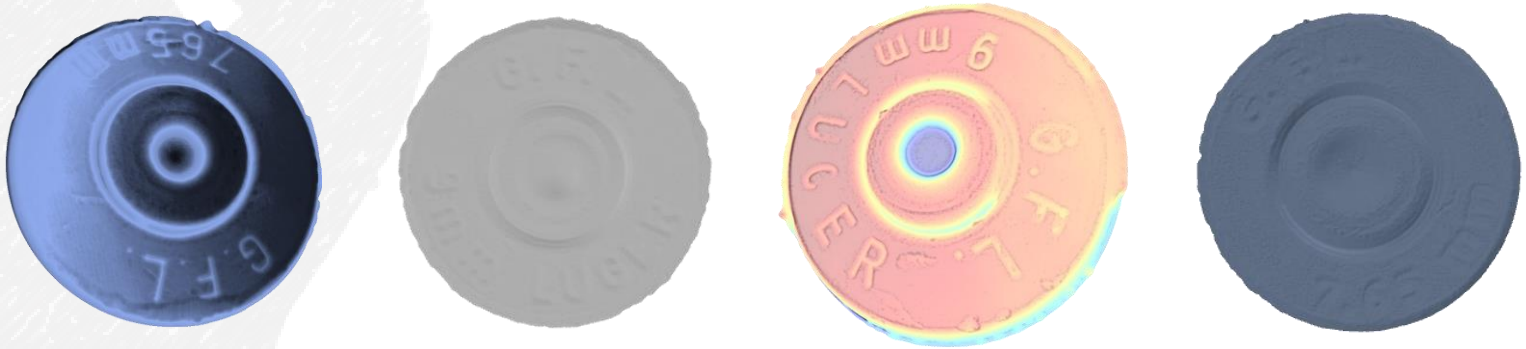


3D Forensic Ballistics Comparison

Luca Guarnera luca.guarnera@unict.it

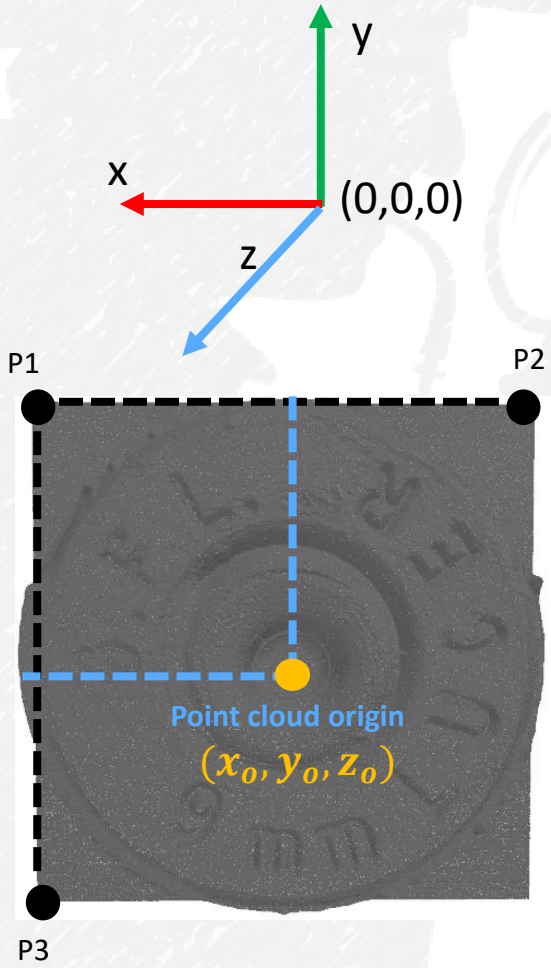
Software and Instruments

RIS DATASET



Preprocessing: RIS dataset

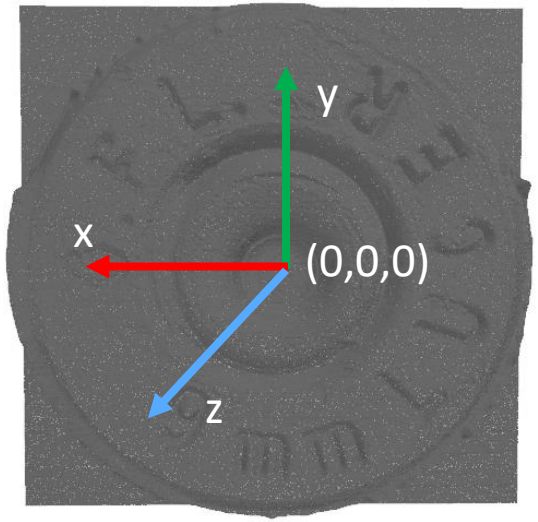
Set the origin of the point cloud



1) Corner detector (**P1, P2,P3**)
2) Point cloud origin
3) Projection of points

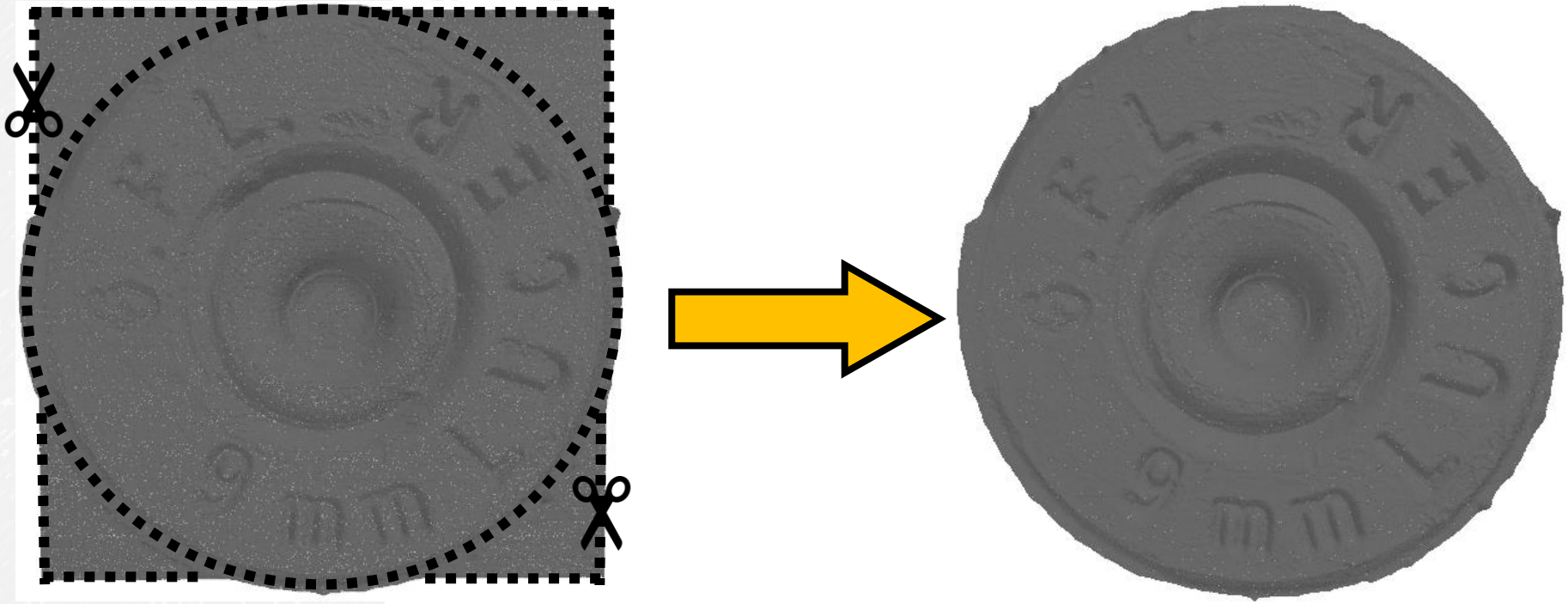
$$\forall\ (x, y, z) \in PC \rightarrow \begin{cases} x = x - x_0 \\ y = y - y_0 \\ z = z - z_0 \end{cases}$$

$$with\ z_0 = 0$$

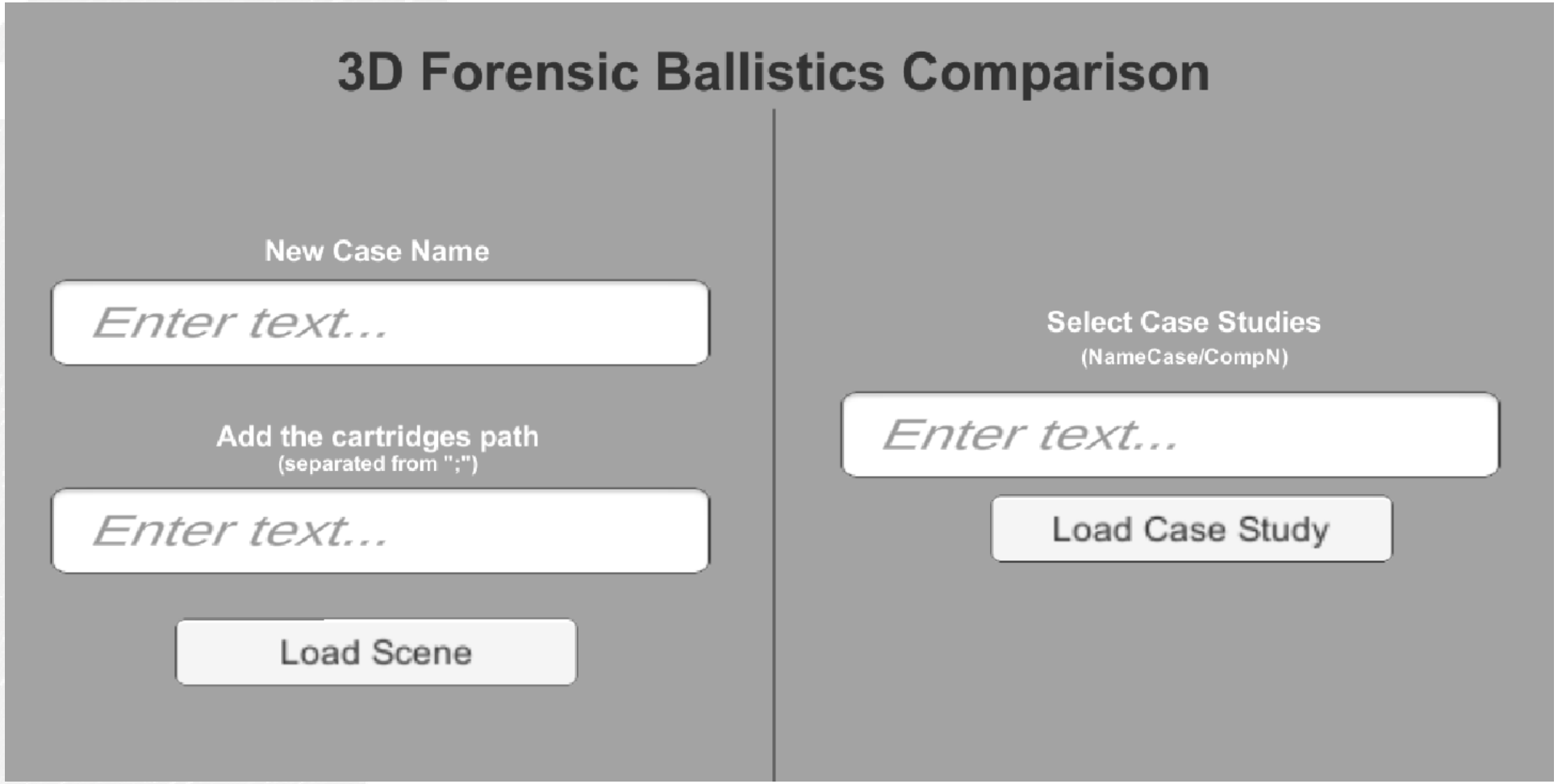


Preprocessing: RIS dataset

Removal of the square



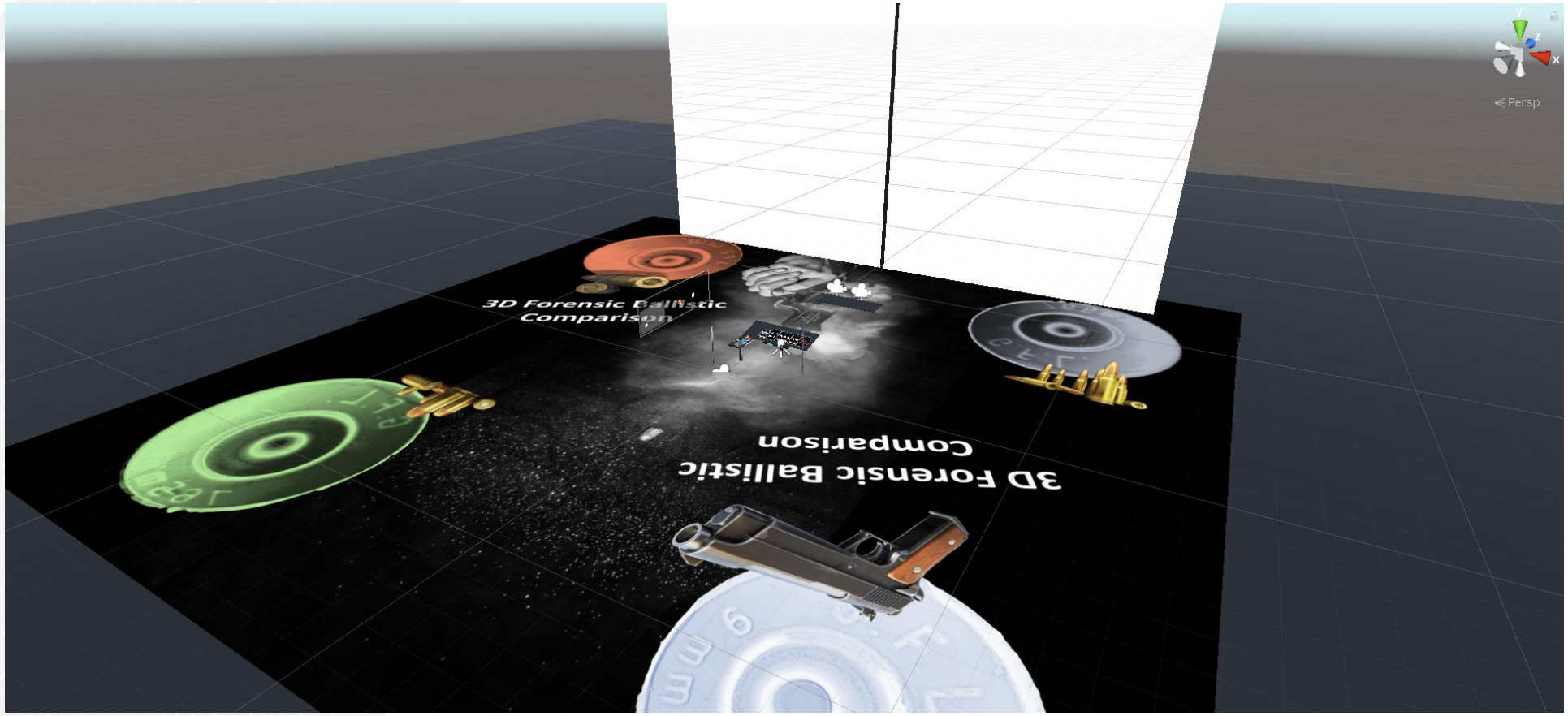
GUI

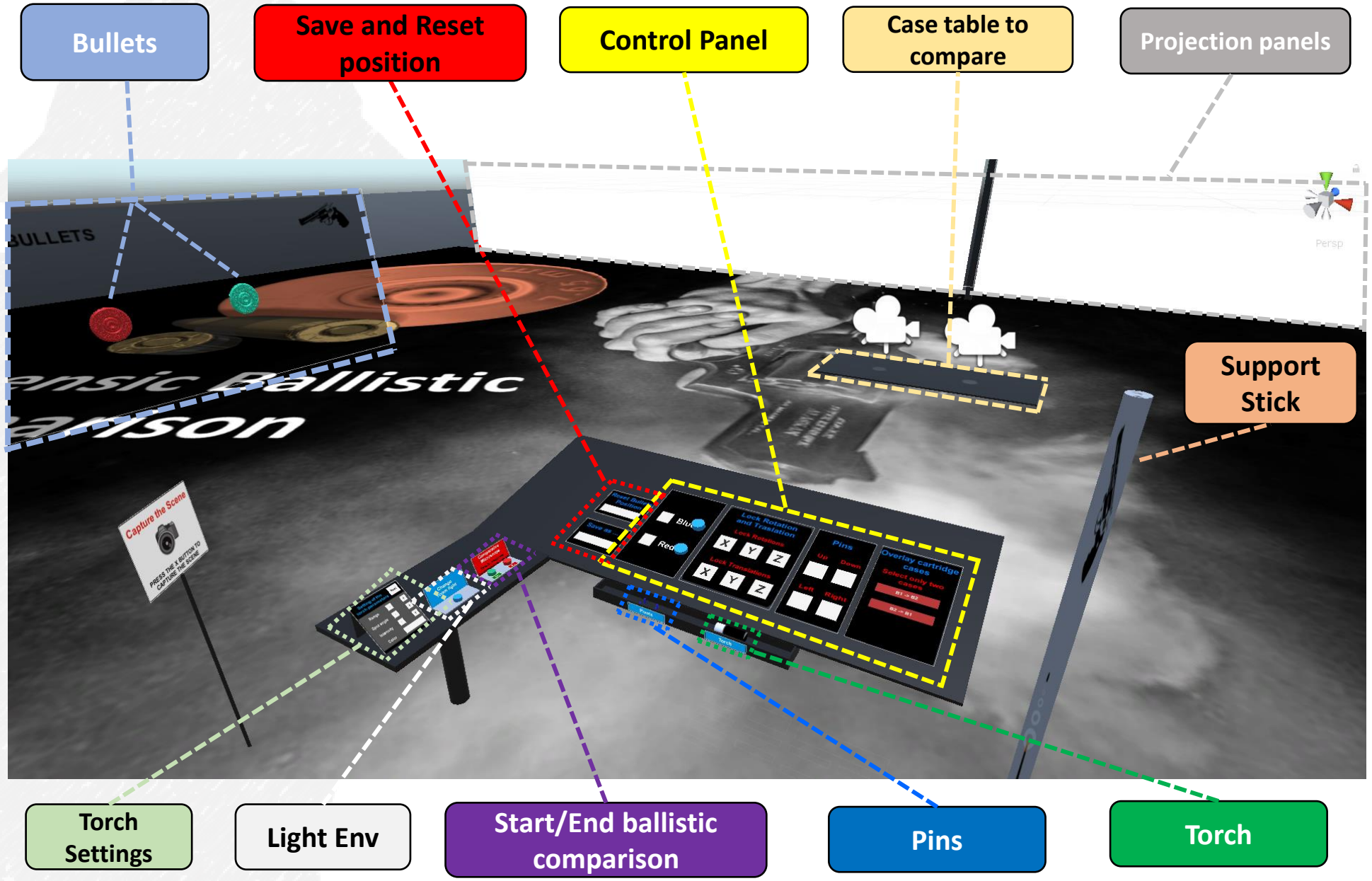

3D Forensic Ballistics Comparison
New Case Name
Enter text...
Add the cartridges path
(separated from ";")
Enter text...
Load Scene
Select Case Studies
(NameCase/CompN)
Enter text...
Load Case Study

GUI

3D Forensic Ballistic
Comparison
Set room position
Press button A to set the
position of the environment
Persp

GUI


3D Forensic Ballistic
Comparison
3D Forensic Ballistic
Comparison
Persp


Bullets
Save and Reset position
Control Panel
Case table to compare
Projection panels
Support Stick
Torch Settings
Light Env
Start/End ballistic comparison
Pins
Torch
BULLETS
Capture the Scene
Lock Rotation and Traslation
Lock Rotations
Lock Translations
Pins
Overlay cartridge cases
Select only two cases
Persp

DEMO - 3D Forensic Ballistics Comparison

https://iplab.dmi.unict.it/mfs/Forensic-Firearms-Ballistics-VR/

Assessing Forensic Ballistics Three-Dimensionally through Graphical Reconstruction and Immersive Observation

Luca Guarnera[1], Oliver Giudice[2], Salvatore Livatino[3], Antonino Barbaro Paratore[4], Angelo Salici[5], Sebastiano Battiato[1]

[1] Dipartimento di Matematica e Informatica, University of Catania, Viale Andrea Doria, 6, Catania, 95126, Italy - *luca.guarnera@unict.it, battiato@dmi.unict.it*

[2] Applied Research Team, IT Department, Banca dâ€™Italia, Rome, Italy - *giudice@dmi.unict.it*

[3] School of Physics, Engineering and Computer Science, University of Hertfordshire, Hatfield, AL10 9AB, UK - *s.livatino@herts.ac.uk*

[4] iCTLab Spinoff of University of Catania, Viale Andrea Doria, 6, Catania, 95126, Italy - *antonino.paratore@ictlab.srl*

[5] Carabinieri Scientific Investigations Department of Messina, Via Monsignor Dâ€™Arrigo, 5, Messina, 98122, Italy - *angelo.salici@carabinieri.it*

Digital Forensics

Laboratorio – 3 CFU

Luca Guarnera, Ph.D.

RTDa – Dipartimento di Matematica e Informatica

Università di Catania

luca.guarnera@unict.it

https://www.dmi.unict.it/lguarnera/

Università di Catania

IMAGE PROCESSING LABORATORY