Digital Forensics e Laboratorio (9 CFU)

Prof. Sebastiano Battiato
Prof. Luca Guarnera

6 Marzo 2024 - A.A. 2023/2024

Corso di Laurea in Informatica
Università di Catania
Dipartimento di Matematica e Informatica

Obiettivi Formativi (1/2)

Il corso mira a favorire l'acquisizione di conoscenze e competenze all'avanguardia in materia di **Digital (e Image/Video 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.

Obiettivi Formativi (2/2)

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.

DF come professione?

- 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.

5

Digital Forensics vs Computer Security

The Cyber Security major's job is to secure down systems and prevent hackers from gaining access while the Digital Forensics majors have the job of figuring out exactly what happened when the other failed.

VS

Digital Forensics

6

Legge n° 48 del 18 marzo 2008

- L'entrata in vigore della legge n° 48 del 18 marzo 2008 ha di fatto sancito l'introduzione dei **principi fondanti** della **computer forensics** all'interno del nostro ordinamento, prevedendo importanti aspetti legati alla gestione delle **digital evidence** che, per loro natura, presentano caratteristiche di estrema volatilità e fragilità.

- Il legislatore nell'introdurre i nuovi principi per l'assunzione delle prove informatiche, non ha indicato nel dettaglio le modalità esecutorie da applicare ma ha focalizzato l'attenzione su due basilari aspetti, sicuramente più vincolati al risultato finale che non al metodo da utilizzare, ovvero la **corretta procedura di copia dei dati utili alle indagini e la loro integrità e non alterabilità in sede di acquisizione.**

Edizione 23/24

Utilizzo software **AMPED 5 e AUTHENTICATE** - http://ampedsoftware.com/it/ -

Utilizzo software ***LegalEye*** *(*https://www.legaleye.cloud/public *)*

Utilizzo software PC-Crash – BOSCH Car Forensics

Collaborazione con lo SpinOFF Universitario iCTLab (www.ictlab.srl)

Tutorato per approfondimenti e laboratorio

Seminari professionisti esterni:

Dott. ZANGARA Ignazio - Università degli Studi di Catania (Aspetti Giuridici)

Seminario IISFA , Seminari FF.OO (To be confirmed)

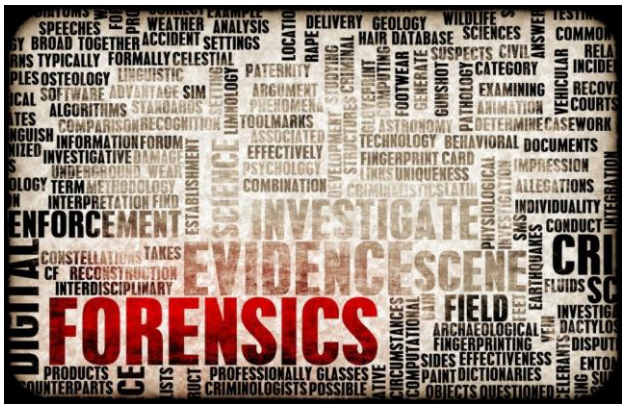
Interventi di professionisti esterni (con eventuali demo):

Formazione Continua

- Syllabus integrato con Certificazione CIFI (work in progress in collaborazione con IISFA)

Forensic Science

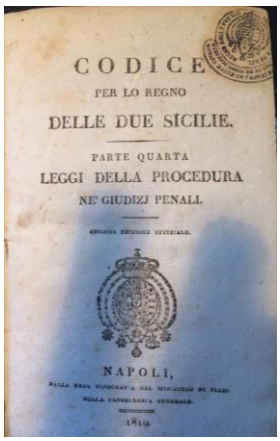
Forensic science (often shortened to forensics) is the practical application of science to matters of the law. Use of **scientific methods** for gaining probative facts (from **physical/analog** or **digital evidences**)

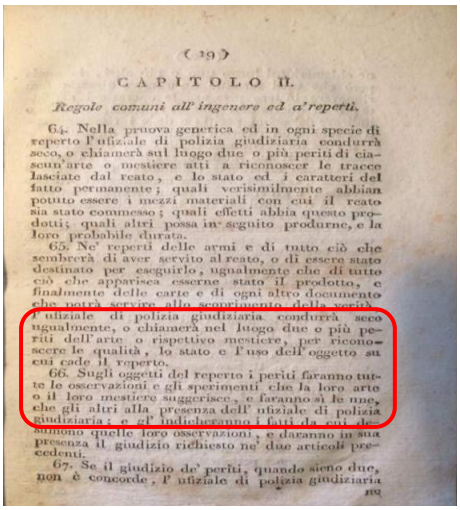


Dalla “prova” alla “prova scientifica”

Quando la **prova** verte su un fatto governato da leggi scientifiche e/o tecniche specialistiche per le quali è necessario ricorrere ad un **esperto**, si parla di **prova scientifica**

Forensics ante litteram





(19)

CAPITOLO II.

Regole comuni all' ingenere ed a' reperti.

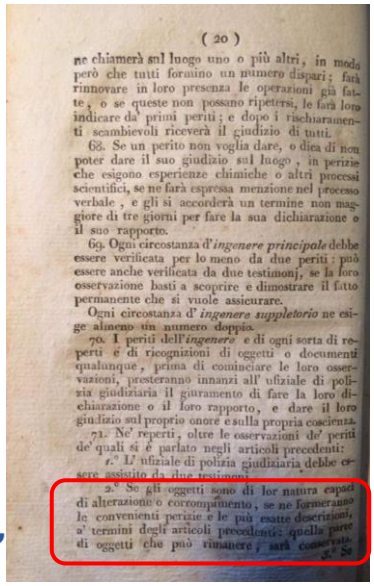
64. Nella pruova generica ed in ogni specie di reperto l' ufiziale di polizia giudiziaria condurrà seco, o chiamerà sul luogo due o più periti di ciascun' arte o mestiere atti a riconoscer le tracce lasciate dal reato, e lo stato ed i caratteri del fatto permanente; quali verisimilmente abbian potuto essere i mezzi materiali con cui il reato sia stato commesso; quali effetti abbia questo prodotti; quali altri possa in seguito produrne, e la loro probabile durata.

65. Ne' reperti delle armi e di tutto ciò che sembrerà di aver servito al reato, o di essere stato destinato per eseguirlo, ugualmente che di tutto ciò che apparisca esserne stato il prodotto, e finalmente delle carte e di ogni altro documento che potrà servire alla scoperta della verità l' ufiziale di polizia giudiziaria condurrà seco ugualmente, o chiamerà nel luogo due o più periti dell' arte o rispettivo mestiere, per riconoscere le qualità, lo stato e l' uso dell' oggetto su cui cade il reperto.

66. Sugli oggetti del reperto i periti faranno tutte le osservazioni e gli sperimenti che la loro arte o il loro mestiere suggerisce, e faranno sì le une, che gli altri alla presenza dell' ufiziale di polizia giudiziaria; e gl' indicheranno i fatti da cui desumono quelle loro osservazioni, e daranno in sua presenza il giudizio richiesto ne' due articoli precedenti.

67. Se il giudizio de' periti, quando sieno due, non è concorde, l' ufiziale di polizia giudiziaria

Forensics ante litteram (2)



(20)

ne chiamerà sul luogo uno o più altri, in modo però che tutti formino un numero dispari; farà rinnovare in loro presenza le operazioni già fatte, o se queste non possano ripetersi, le farà loro indicare da' primi periti; e dopo i rischiaramenti scambievoli riceverà il giudizio di tutti.

68. Se un perito non voglia dare, o dica di non poter dare il suo giudizio sul luogo, in perizie che esigono esperienze chimiche o altri processi scientifici, se ne farà espressa menzione nel processo verbale, e gli si accorderà un termine non maggiore di tre giorni per fare la sua dichiarazione o il suo rapporto.

69. Ogni circostanza d'*ingenere principale* debbe essere verificata per lo meno da due periti: può essere anche verificata da due testimonj, se la loro osservazione basti a scoprire e dimostrare il fatto permanente che si vuole assicurare.

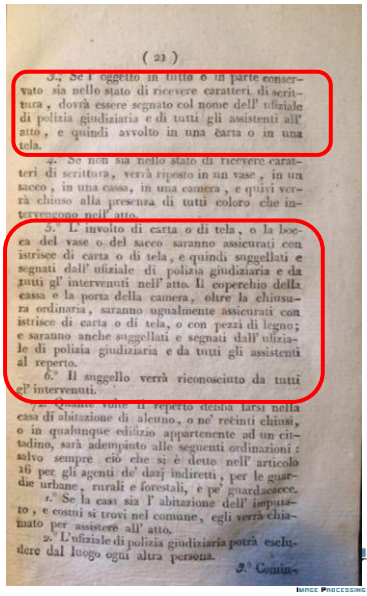
Ogni circostanza d'*ingenere suppletorio* ne esige almeno un numero doppio.

70. I periti dell'*ingenere* e di ogni sorta di reperti e di ricognizioni di oggetti o documenti qualunque, prima di cominciare le loro osservazioni, presteranno innanzi all' ufiziale di polizia giudiziaria il giuramento di fare la loro dichiarazione o il loro rapporto, e dare il loro giudizio sul proprio onore e sulla propria coscienza.

71. Ne' reperti, oltre le osservazioni de' periti de' quali si è parlato negli articoli precedenti:

1.° L' ufiziale di polizia giudiziaria debbe essere assistito da due testimoni.

2.° Se gli oggetti sono di lor natura capaci di alterazione o corrompimento, se ne formeranno le convenienti perizie e le più esatte descrizioni, a' termini degli articoli precedenti: quella parte di oggetti che può rimanere, sarà conservata.



(21)

3.° Se l' oggetto in tutto o in parte conservato sia nello stato di ricevere caratteri di scrittura, dovrà essere segnato col nome dell' ufiziale di polizia giudiziaria e di tutti gli assistenti all' atto, e quindi avvolto in una carta o in una tela.

4.° Se non sia nello stato di ricevere caratteri di scrittura, verrà riposto in un vase, in un sacco, in una cassa, in una camera, e quivi verrà chiuso alla presenza di tutti coloro che intervengono nell' atto.

5.° L' involto di carta o di tela, o la bocca del vase o del sacco saranno assicurati con istrisce di carta o di tela, e quindi suggellati e segnati dall' ufiziale di polizia giudiziaria e da tutti gl' intervenuti nell' atto. Il coperchio della cassa e la porta della camera, oltre la chiusura ordinaria, saranno ugualmente assicurati con istrisce di carta o di tela, o con pezzi di legno; e saranno anche suggellati e segnati dall' ufiziale di polizia giudiziaria e da tutti gli assistenti al reperto.

6.° Il suggello verrà riconosciuto da tutti gl' intervenuti.

7.° Quante volte il reperto debba farsi nella casa di abitazione di alcuno, o ne' recinti chiusi, o in qualunque edifizio appartenente ad un cittadino, sarà adempiuto alle seguenti ordinazioni: salvo sempre ciò che si è detto nell' articolo 16 per gli agenti de' dazj indiretti, per le guardie urbane, rurali e forestali, e pe' guardacacce.

1.° Se la casa sia l' abitazione dell' imputato, e costui si trovi nel comune, egli verrà chiamato per assistere all' atto.

2.° L'ufiziale di polizia giudiziaria potrà escludere dal luogo ogni altra persona.

3.° Comin-

IMAGE PROCESSING LABORATORY

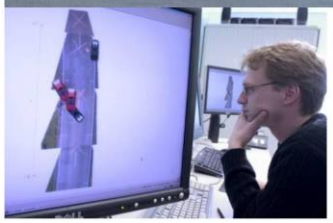
23

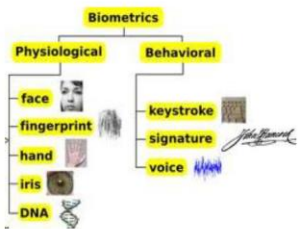
Casework: Chip cards, Electronic devices
Computers, Networks, phones, cell site analysis

Digital Forensics

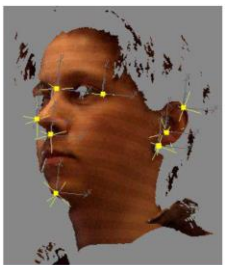
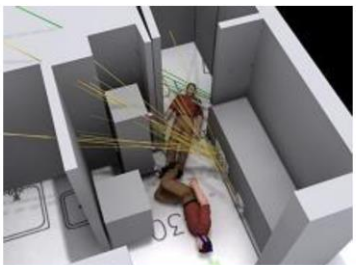
IMAGE PROCESSING LABORATORY

24




Biometrics
Physiological
Behavioral
face
fingerprint
hand
iris
DNA
keystroke
signature
voice



Storia della Digital Forensics

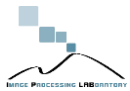
La **Forensic Science** è l'applicazione di metodi tecnici e scientifici per il settore della **giustizia**, **investigazione** e **scoperta di prove**.

- **Anni '70**: **prima nozione** di Digital Forensics
- **Anni '80**: **alla ricerca di prove digitali**.
- **Anni '90**: si **afferma la Digital Forensics**:

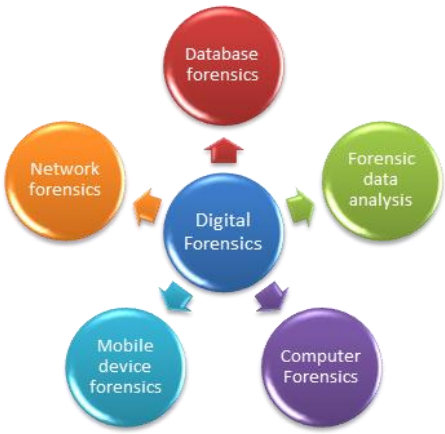
.

The first **Digital Forensics Research Workshop** (DFRWS) was held in Utica, NY in August 2001.

Digital Forensic Science
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.

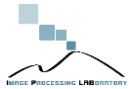


29



- **Source identification**
- **Integrity verification/tampering detection**

Techniques from multimedia forensics merely provide a way to test for the authenticity and source of digital sensor data. In this sense is not about analyzing the **semantics** of digital or digitized media objects.



30

Modalità d'esame

Prove in Itinere con esonero (modalità da definire) dalla prova scritta

Laboratorio e/o prove opzionali (punti bonus)

Prova scritta (max 26)

Progetto (opzionale)

1) Relazione tecnica di approfondimento da concordare con il docente.
2) Relazione di Consulenza Tecnica
3) Sviluppo di tool

Utility

Slides e Materiale Vario su Teams - **Codice 2jc74j2**

Per le lezioni - Canale FAD dedicato (YouTube *ComputerForensicsCT*)

E-mail: battiato@dmi.unict.it

Ricevimento:

Consultare il web/Canale TEAMS: Codice **9knyk3e**

Risorse

34

Referenze (1)

CyberForensics e Indagini Digitali – Manuale tecnico-giuridico e casi pratici

di S. Aterno, F. Cajani, G. Costabile, D. Curtotti

G. Giappichelli Editore
ISBN 978-8892116757

35


Ringraziamenti
e Collaborazioni
ENFSI
EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTES
LEGAL EYE
DIGITAL PROOF KEEPER
IISFA
ASSOCIAZIONE ITALIANA DIGITAL FORENSICS
AMPED SOFTWARE
Authenticate
Amped FIVE
Digital Forensics
IMAGE PROCESSING LABORATORY

36


POLICE LINE DO
IFOSS
International Forensics Summer School
ETHICAL AND LEGAL CHALLENGES IN AI-DRIVEN FORENSIC SCIENCE
JULY 14-20, 2024
Watch a preview!
School Directors
PROF. SEBASTIANO BATTIATO, PH.D.
University of Catania
PROF. DONATELLA CURTOTTI, PH.D.
University of Foggia
PROF. GIOVANNI ZICCARDI, PH.D.
University of Milan
Social Network
IFOSS
@ifoss_official
@ifoss_official
IFOSS
School location
The school will take place at Sampieri, Sicily
https://www.hotelbaiasamuele.it/en/
www.ifoss.it
info@ifoss.it

37

IFOSS 2024 - (Some) Speakers

ALESSANDRO TRIVILINI
Scuola universitaria professionale della svizzera italiana (SUPSI)

NELLO CRISTIANINI
University di Bath

STEFANO MARRONE
University of Naples Federico II

MATTEO FLORA
The Fool

PROF. DR. DIDIER MEUWLY
University of Twente

GIOVANNI TESSITORE – SENIOR FORENSIC SCIENTIST
Ministero dell'Interno

DR. FABIO BRUNO
Head of DFL at INTERPOL-GCI, Singapore

MARTIN DRAHANSKÝ
Faculty of Information Technology, Brno University of Technology

IFOSS International Forensics Summer School
New Edition 2024!
Email: info@ifoss.it web site: www.ifoss.it

38

IFOSS International Forensics Summer School

2022 EDITION here the video recap

ORGANIZERS

ENDORSERS

SPONSORS

IMAGE PROCESSING LABORATORY

39

Video (Le Iene - 2013)

http://www.video.mediaset.it/video/iene/puntata/376449/viviani-recupero-dati-cellulare.html

Tecniche di Trattamento dei Reperti Informatici Parte 1

Prof. Sebastiano Battiato

A.A. 2021/2022

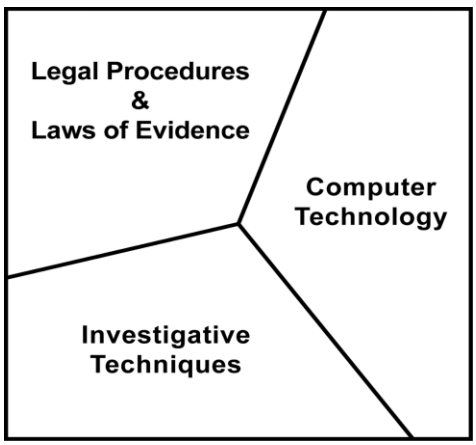
Corso di Laurea in Informatica
Università di Catania
Dipartimento di Matematica e Informatica

Informatica Forense

L'Informatica forense è la disciplina avente ad oggetto lo studio delle attività di **individuazione**, **conservazione**, **protezione**, **estrazione**, **documentazione** ed ogni altra forma di trattamento ed interpretazione del dato digitale memorizzato su supporto informatico, al fine di essere valutato come prova nel processo.

Informatica forense studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (memorie, hard disk, dischetti, nastri, cartaceo, etc.), nonché l'analisi forense di ogni sistema informatico e telematico (computer, rete di computer, ed ogni altro dispositivo per il trattamento di dati in formato digitale), l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione, l'analisi ed esame del sistema informatico e telematico.

Computer Forensics Skills



Dato Digitale

Il dato digitalizzato come oggetto di indagine

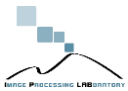
I dati

Rappresentano le entità di base su cui operano i sistemi informatici come **applicazioni software**, **email**, **feed**, il **web**, …

Le autorità procedenti (**law enforcer**) nell'ambito della loro attività d'indagine, si avvalgono sempre più di tali dati che, una volta correttamente acquisiti e analizzati possono assumere valore di prova contribuendo significativamente all'identificazione e persecuzione dell'autore materiale dell'illecito

ICT: Tipologie di Reato

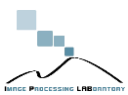
- **Reati tradizionali o comuni**
  computer come strumento
- **Reati relativi a contenuti**
  es. distribuzione di materiale illegali o illeciti
- **Reati di danneggiamento**
  es. distribuzione di virus



Dati Informatici in ambito forense

Può rendersi necessario nei procedimenti aventi ad oggetto:

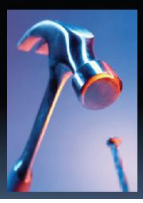
- **Reati informatici**
- **Reati commessi con l'ausilio di strumenti informatici**
- dati (o informazioni) aventi **valore di prova o indizio** per reati informatici e non
- strumenti (supporti) di **archiviazione** di dati rilevanti



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)**

Bisogna avere un approccio metodologico….perché?
Il destino di chi esegue l'accertamento tecnico…



Solo supportando la attività di accertamento con un rigoroso percorso metodologico il tecnico, il "chiodo" il consulente tecnico potrà confermare le proprie conclusioni attraverso la prova di resistenza "giudiziaria"

Ancora sulle competenze

- **Parte Tecnica**:

  Duplicazione dati e Analisi, Ricostruzione Timeline, Archeologia Informatica, Reti e Protocolli; Redazione di rapporti tecnici **solidi**

- **Parte giuridica**

  Terminologia, Norme, Problematica di giurisdizione, Consulenti e periti

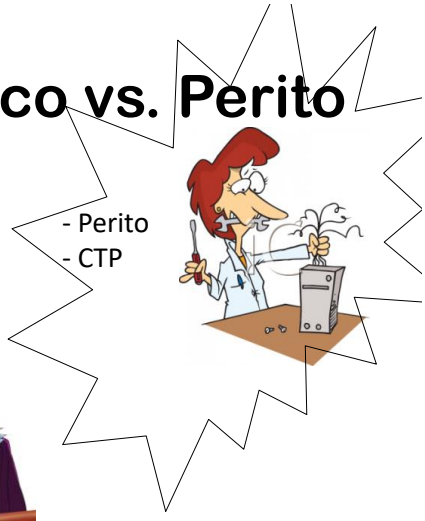
Consulente Tecnico vs. Perito

Giudice

Difesa

Accusa (Pubblico Ministero-Prosecutor)

Consulente Tecnico vs. Perito



Giudice

Difesa

Accusa (Pubblico Ministero-Prosecutor)

Digital Forensics (in pratica)

Tecniche e strategie basate sulla intangibile e spesso volatile natura dei dati digitali, specialmente in ambienti di **rete** o nella **live** forensics.

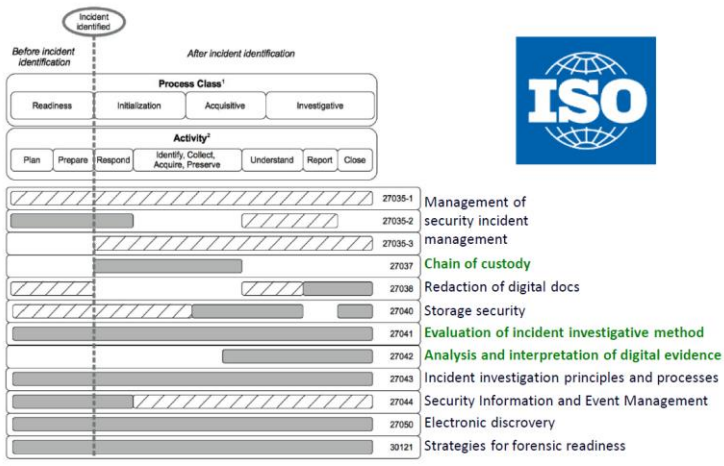
Utilizzo di tecniche **scientifiche** e **analitiche** alle reti di computer, a dispositivi digitali e ai file per scoprire o recuperare evidenze ammissibili nel procedimento penale

Digital Forensics (in pratica)

La tecnologia rende il processo d'investigazione e raccolta dei dati a fini probatori estremamente **vulnerabile** per i diritti delle parti interessate (in particolare la difesa tecnica) e soggetto al rischio di **malfunzionamenti tecnici**, **danneggiamenti** o **contraffazioni**.

L'insieme dei processi e delle tecniche utilizzate vengono definite "pratiche migliori" (**best practices**).

ISO Guidelines

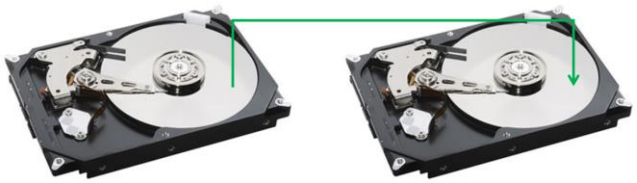


Evidenze digitali

- L'aspetto caratteristico dei reperti virtuali delle evidenze è dato dalla **volatilità**, dalle infinite possibilità di riproduzione mediante procedure rapide e con assoluta rapidità, dalla necessaria interpretazione ai fini intellegibili
- Le alterazioni possono intervenire per cause legate alle attività ordinarie del computer o da un uso incauto degli operatori: è difficile determinare quali siano i cambiamenti effettuati con la conseguente impossibilità di ristabilire la situazione ex-ante

Evidenze digitali

- L'esame di evidenze digitali può richiedere molto tempo; quindi chi effettua le indagini è di solito accurato e cauto quando raccoglie gli elementi di prova.
- Solitamente una **copia primitiva**, '**originale**', intatta è prodotta per il successivo esame e i dispositivi sono restituiti alle loro applicazioni



Data Type

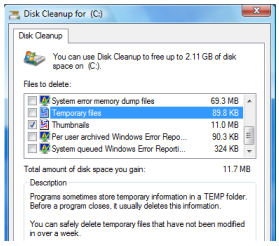
Gli elementi di prova digitale comprendono:
– il contenuto di una trasmissione
– gli attributi o metadati dell'attività di comunicazione
– il diritto alla privacy degli utenti delle reti
– la gestione di una risorsa informatica

- La fonte di qualsiasi informazione digitale è data dalla sua rappresentazione attraverso la codifica binaria

- Le leggi trattano i differenti tipi di dati forensi in maniera diversa (ad es. intercettazioni, dati di traffico): a ciò consegue un diverso regime giuridico di trattamento

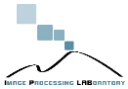
Ancora sui dati (tmp file)

- Dati in memorie virtuali e file di swap
- History file dei browser
- History file in Internet
- File temporanei nelle reti telematiche
- Link di collegamento
- File di log
- Metadata
- File di informazioni
- Web based emails



Main Goal

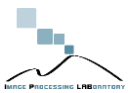
- Protect the suspect system
- Discover all files
- Recover deleted files
- Reveal contents of hidden files
- Access protected or encrypted files
- Use steganalysis to identify hidden data
- Analyze data in unallocated and slack space
- …
- Provide an opinion of the system layout
- Provide expert testimony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



Chain of Custody

- Handling of *e-evidence* must follow the *three C's of evidence*: **care, control, and chain of custody**

- Chain of custody procedures
  - Keep an **evidence log** that shows when evidence was received and seized, and where it is located
  - **Record dates** if items are released to anyone
  - **Restrict** access to evidence
  - Place original hard drive in an evidence **locker**
  - Perform all forensics on a **mirror-image** copy, never on the original data



Il Reperto informatico: le 5 fasi

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

Identificazione

- **Rilevare cosa è effettivamente utile per l'indagine**
  - Sistemi informatici
  - Sistemi di comunicazione
  - Supporti di memorizzazione esterna
  - Supporti non digitali e informazioni
    - Documenti, post-it…
    - Password, modalità di accesso a sistemi complessi…

Acquisizione

- **Duplicare le informazioni in maniera fedele all'originale**
  - Cloni
  - Immagini bit-a-bit
  - Immagini bit-a-bit compresse
- **Obiettivi**
  - Acquisire il maggior numero di dati (possibilmente tutti)
  - Rendere l'attività di acquisizione ripetibile
  - Limitare i tempi di inattività di server "importanti"

Acquisizione

- **Completa**
- **Accurata**
- **Incontaminata**

Acquisizione

Acquisizione

Chi effettua le indagini deve poter ottenere i dati in modo completo con interferenze minime sui dati originali sotto esame. Tali dati possono essere stampati e copiati, anche se questo porta a variazioni nei meta-dati associati, con la possibilità di creare vulnerabilità

Pertanto la tecnica più utilizzata per ottenere dati forense è quella dell'**imaging**.

Una **immagine bit-stream** di un dispositivo di memorizzazione digitale, ad es. hard disk o smart card, viene acquisita e creata in modo non invasivo includendovi le parti non occupate da dati di interesse

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

MD5

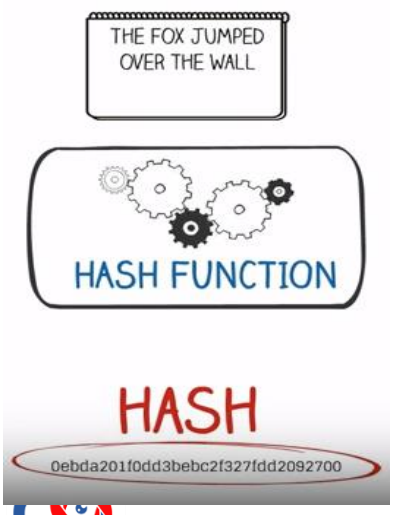
- A oggi, la disponibilità di algoritmi efficienti capaci di generare stringhe che collidono (ossia che producono in output lo stesso valore di hash) in un tempo ragionevole ha reso MD5 sfavorito rispetto ad altri algoritmi di hashing, sebbene la sua diffusione sia a tutt'oggi molto estesa (basti pensare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

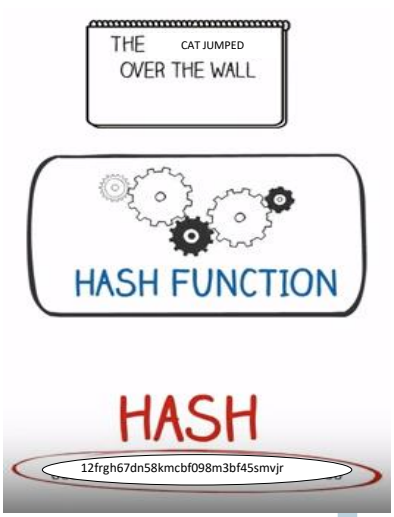
SHA (Secure Hash Algorithm)

- 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.

77





78

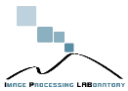
Example: MD5

The 128-bit (16-byte) MD5 hashes are typically represented as a sequence of 32 hexadecimal digits.

MD5("The quick brown fox jumps over the lazy dog") =
9e107d9d372bb6826bd81d3542a419d6

MD5("The quick brown fox jumps over the lazy dog**.**") =
e4d909c290d0fb1ca068ffaddf22cbd0

Even a small change in the message will (with overwhelming probability) result in a completely different hash!



Classical Hashing on Images: Some Sources of Variability

Original

Rotation

Scale

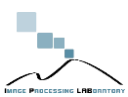
Crop

Light

Pose

Context

Image:	**MD5**
Original:	5972FB15A2FDFA7215134B5BACD4D032
Rotation:	6B0BC6F3DBD450EF3E9BE8CCBDB2480F
Scale:	D3CFFA588D5B4CF3395A69AC6EDAB4A5
Crop:	6CF3D1FD20388DE3F8D1858C4D7A53C7
Light:	38B5E48E46898E1E5E7207AEB4255518
Pose:	9030E506156664E0BBD6AA76F3CA1748
Context:	0F3055E092C73155690C822D6BA18BAD



Analisi

- Mettere in evidenza i dati con contenuto informativo importante per l'indagine
  - A favore
  - A sfavore
- Documentare il processo di analisi

L'analisi va eseguita su una copia (bit a bit) e deve essere RIPRODUCIBILE

Valutazione

- Interpretare i dati evidenziati in fase di analisi per sostenere le proprie tesi
  - A favore
  - A sfavore

Presentazione

- Documentare
  - Cosa è stato fatto
  - Come è stato fatto
  - Cosa è emerso
  - Che significato hanno i dati emersi
- Adattare il registro all'interlocutore
  - Tecnico
  - Giurista

83

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:

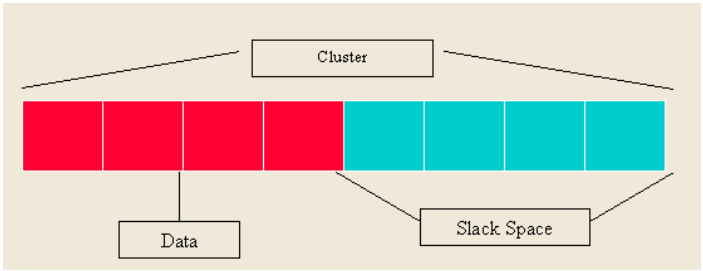
– Se effettuata da una applicazione standard rimuove solamente l'indirizzo dell'informazione associata a ogni blocco di dati, che logicamente connette i vari blocchi che costituiscono i contenuti dei file

– 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»

Slack Space

Area (compresa tra l'ultimo bit e la fine del settore) non utilizzata dal file che ha allocato lo spazio per ultimo



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/

Intro Image and Video Forensics

Prof. Sebastiano Battiato

A.A. 2023/2024

Corso di Laurea in Informatica
Università di Catania
Dipartimento di Matematica e Informatica

89

SWGIT

Scientific Working Group
Imaging Technology

"Forensics 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)

Image/Video Forensics (in practice)

- Enhancement/Restoration
- Interpretation and Content Analysis
  - Plate Recognition
  - Dynamic Reconstruction (car crashes, etc.)
  - Antropomethric issues
  - …

- **Source Identification**
- **Integrity/Authenticity**

Multimedia Forensics

Digital Forensics

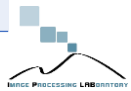
Authenticity VS Integrity

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

Digital Forensics

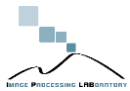


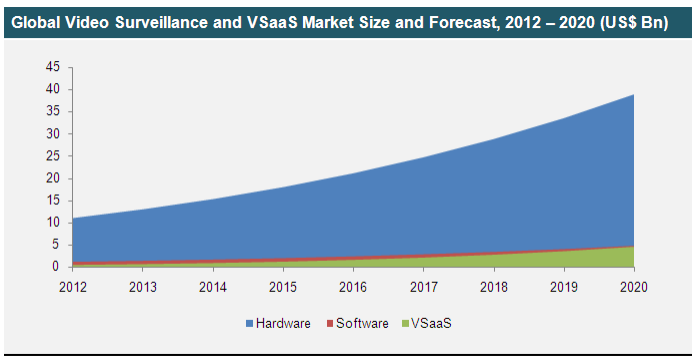
Original File: Special Cases

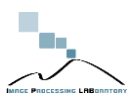
- **Recapture**: create a fake and then take a picture with the camera we want to pretend the picture was taken with

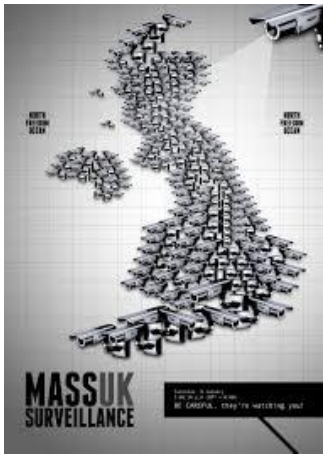
- **Staging**: the image file is authentic, but the content has been staged

In these cases an authentic file does not imply an authentic content.









Study highlights potential impact of CCTV in police investigations (*)

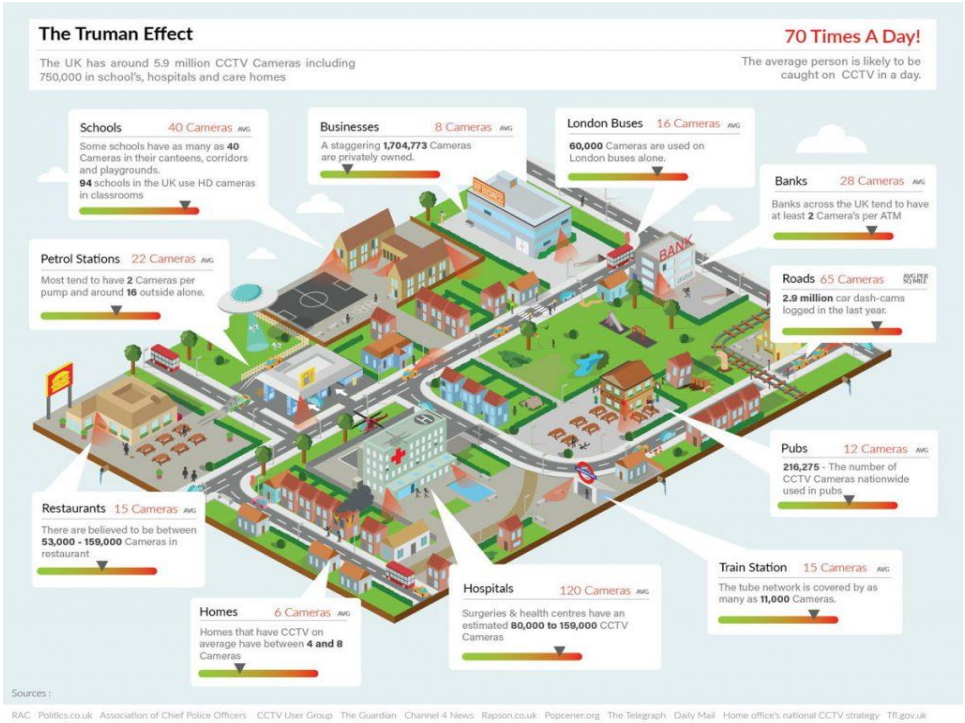
CCTV was available in the investigation of almost half of those crimes and proved useful in 65% of those cases (British Transport Police)

(*) M.P.J. Ashby - The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis – European Journal on Criminal Policy and Research – pp.1-19, 2017

CCTV is useful or not

Reason	Cases	%
CCTV not available and therefore not useful	134,819	54.7
incident location not covered by CCTV	72,042	29.2
recording not requested by officers	49,647	20.1
CCTV system faulty	5,891	2.4
recording over-written before it was retrieved	7,239	2.9
CCTV available but not useful	39,218	15.9
recording viewed but incident not shown	25,987	10.5
recording viewed but images of insufficient quality	12,055	4.9
wrong images requested or retrieved	1,176	0.5
CCTV useful	72,390	29.4

(*) M.P.J. Ashby - **The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis** – European Journal on Criminal Policy and Research – pp.1-19, 2017



97

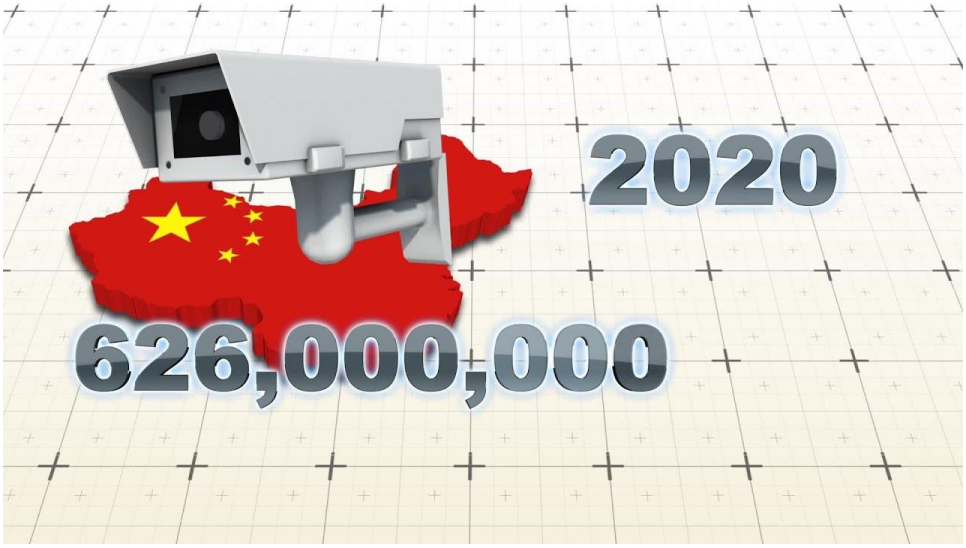
The Truman Effect

Area	Number of CCTV Cameras
Globally	245 million
USA	30 million
United Kingdom	5.9 million
France	>570,000
London	> 500,000
Greater Manchester	10,000
London's Tube Network	11,000
New York City Subway System	> 4,500.

Source: telegraph.co.uk, popularmechanics.com, manchestereveningnews.co.uk, itv.com, MTA, securitynewsdesk.com, swissinfo.ch

98

From 176M to 626M CCTV cameras!!!

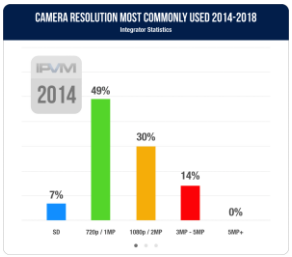


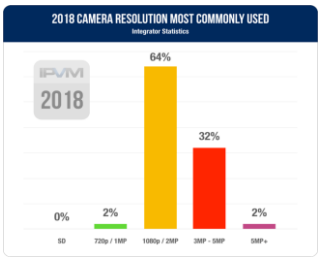
99

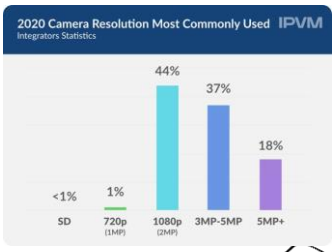
100

Resolution Statistics

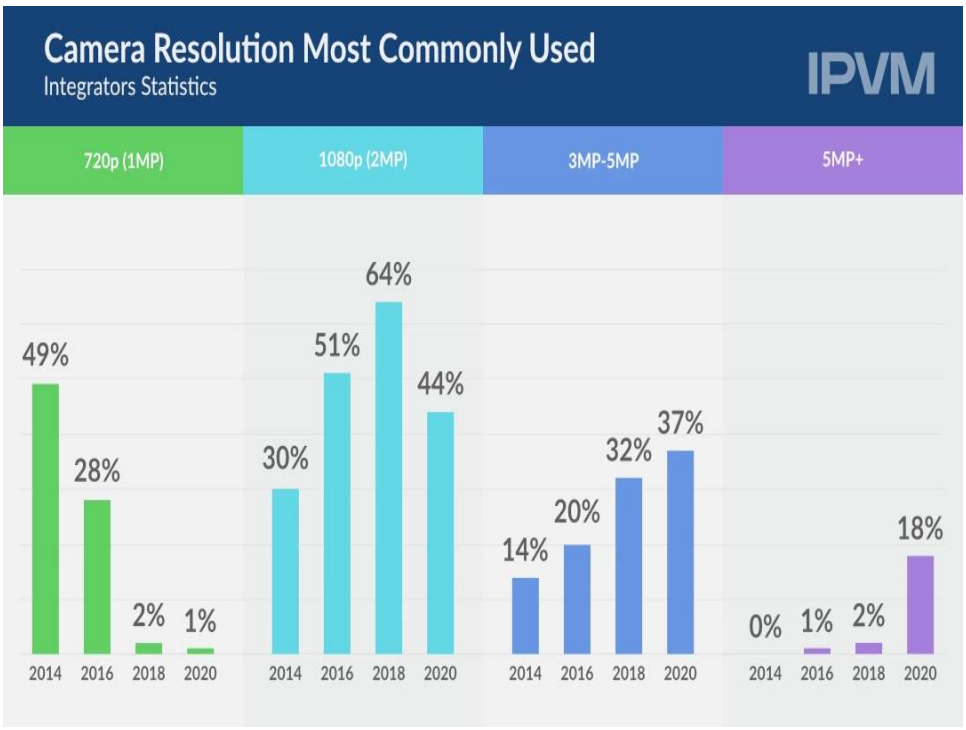
The average resolution used continues to grow modestly as our **Resolution Usage Statistics**, excerpted below, show:







101



102

- SWGDE Best Practices for Photographic Comparison for All Disciplines (Version: 1.1 2017)
- SWGDE Image Processing Guidelines (Version: 1.0 28/02/2016)
- SWGDE Proposed Techniques for Advanced Data Recovery from Security Digital Video Recorders (Version: 1.2 23/06/2016)
- SWGDE Training Guidelines for Video Analysis, Image Analysis and Photography (Version: 1.1 28/02/2016)
- SWGDE Recommendations and Guidelines for using Video Security Systems (Version: 1.0 29/05/2015)

Updated Versions

https://www.swgde.org/documents/swgit-document-archive

Project S-FIVE

(Standardisation of Forensic Image and Video Enhancement)

https://s-five.eu/

https://s-five.eu/FIVE_Best_Practice_Manual.htm

The final draft of the FIVE Best Practice Manual is publically available

Fantasy

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

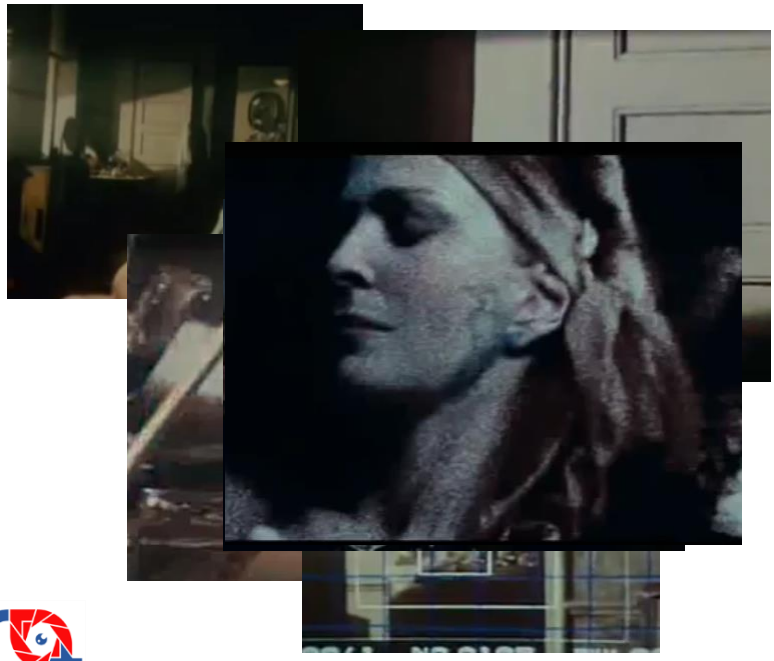
CSI




107

Esper Blade Runner

108

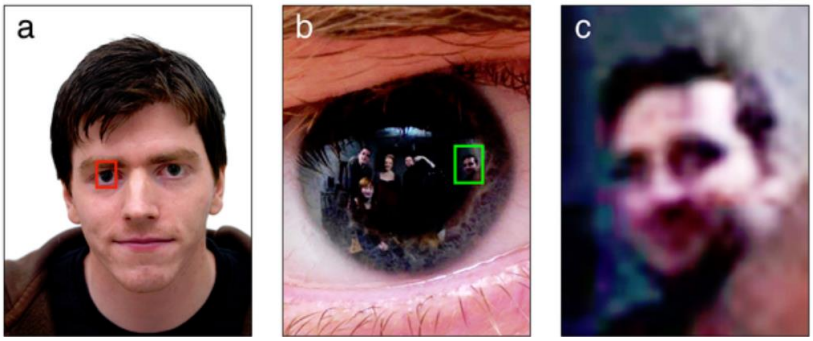


Fantasy

- Non si possono "creare" dal nulla informazioni che non ci sono…

- Si possono però enfatizzare ed estrarre informazioni che magari non si vedono, **ma comunque sono presenti!!!**

Fantasy



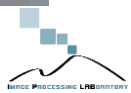
http://www.youtube.com/watch?feature=player_embedded&v=ey4UGvBIjy0

What about real resolution?

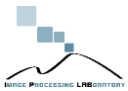
Credit Kurzwel Accelerating intelligence 2013

Realtà….

I Need That Plate! No Way...



I Need That Plate! No Way...



Failure Cases

115

Failure Cases

116

Bridge (2016)

Understand When It's Possible To Get Something

- What is the minimum quality for video? "Minimum quality" doesn't exist.
- The success of the enhancement depends on several factors:
  - ✓**Main goal** (video captured with an HD camera but the license plate we need to extract is too far away)
  - ✓**Technical related details**: Resolution of the area of interest, Level of compression, Presence of blur / focus, Number of available frames, Noise / brightness and contrast
- **It's important to understand which defects are present in order to apply the proper tools.**

Fattibilità del miglioramento

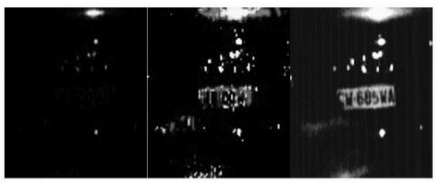
Esempi:

Da una singolo fotogramma in cui si vede una targa composta da tre pixel bianchi non sarà mai possibile ottenere nulla.

Per quanto riguarda il miglioramento di targhe, che è senza dubbio una delle richieste più comuni, l'esperienza ci consente di affermare che se la risoluzione verticale della targa non è almeno 12-15 pixel, non è possibile ottenere alcun miglioramento significativo.

Fattibilità del miglioramento

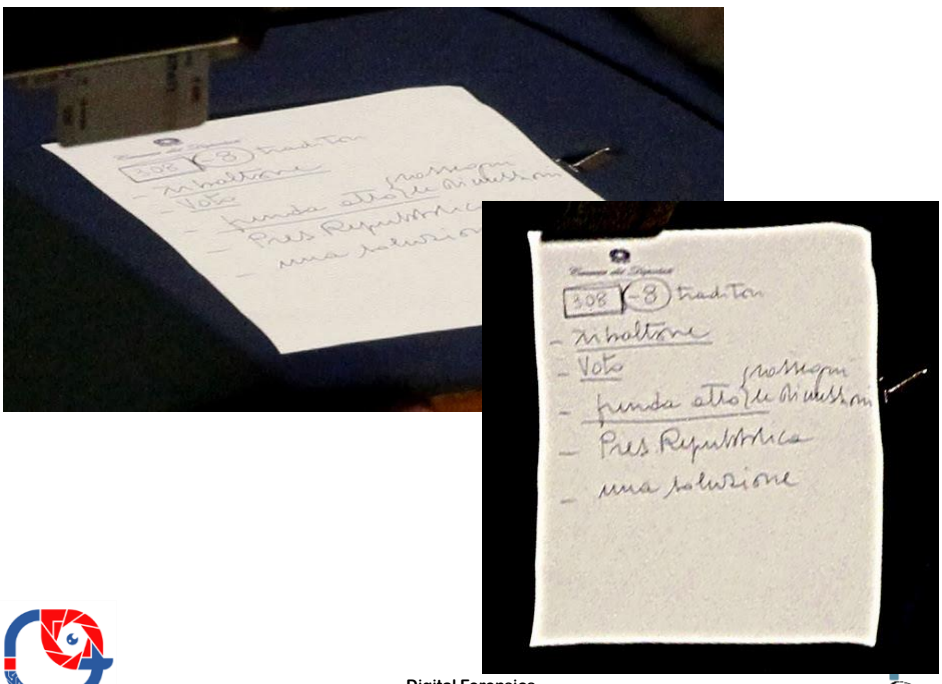
Da un video molto buio caratterizzato da un rumore elevato, spesso se si hanno a disposizione abbastanza fotogrammi è possibile recuperare un dettaglio.



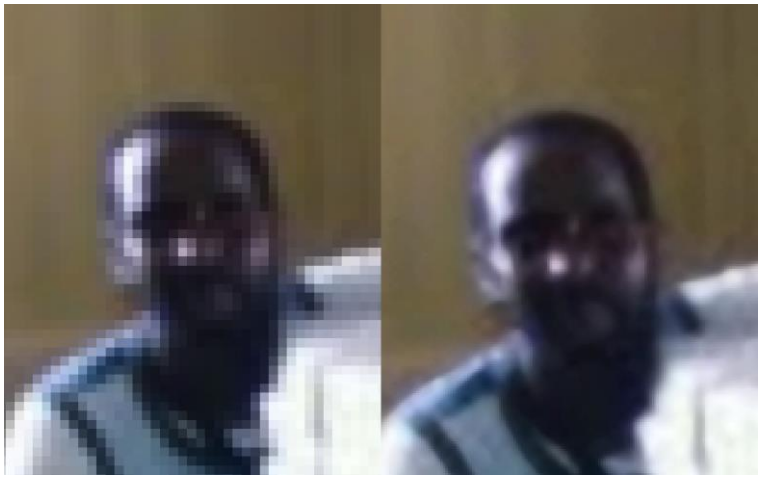
Se la risoluzione è adeguata e la compressione non eccessiva, anche con sfocature molto pesanti è possibile ottenere un'immagine nitida .

Correzione Prospettica

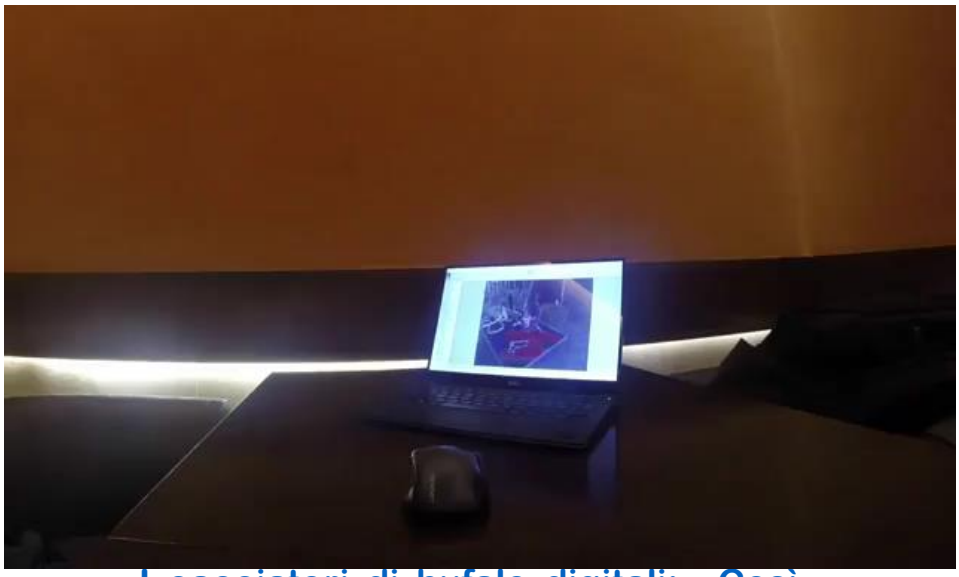
I pixel vengono «ridisegnati» mediante una opportuna trasformazione geometrica.



Super Resolution



(source Interpol)



[I cacciatori di bufale digitali: «Così staniamo i falsi»](#) - CorriereTV (2017)

125

Seeing isn't believing

126

127

English AI Anchor

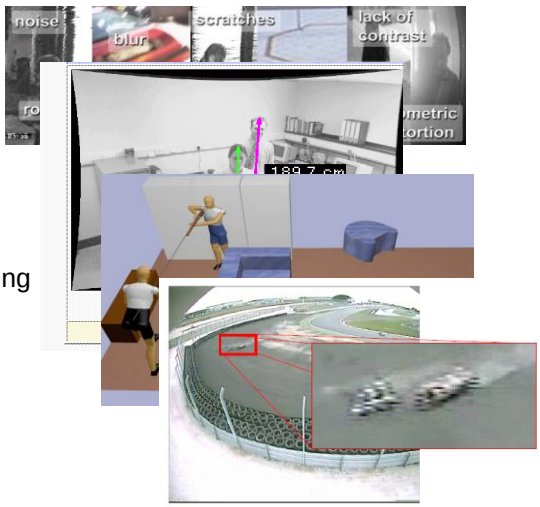
128

Seeing Isn't Believing

129

Esempi..

- Image Enhancement
- Image Reconstruction
- Video Analysis
- 3D Reconstruction
- Steganografia e Self Embedding
- Image Forgery Identification
- Image Source Identification



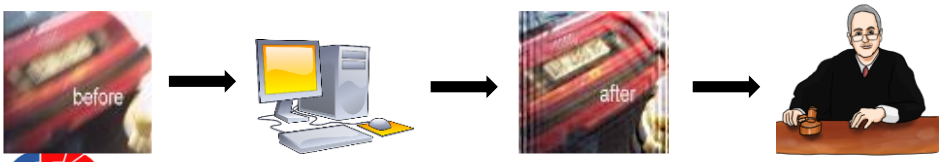
130

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

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.

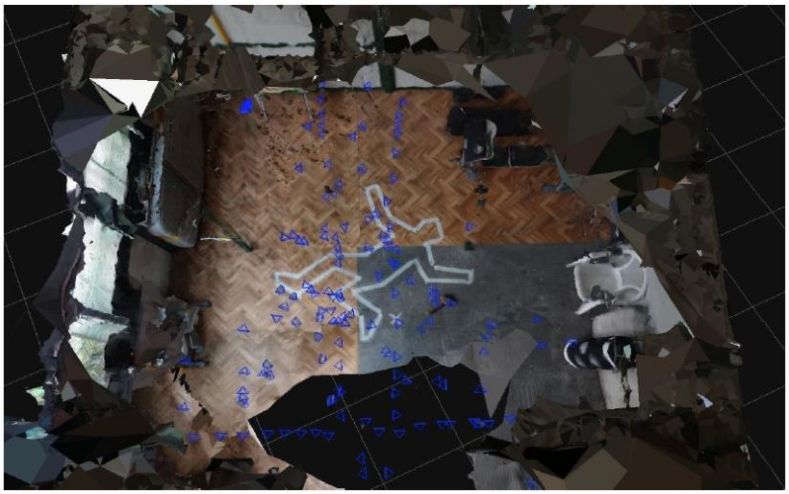
Per essere in grado di recuperare o di inferire delle evidenze di prova è comunque necessaria una adeguata competenza specifica che richiede uno studio sistematico dei **fondamenti della teoria dell'elaborazione delle immagini e dei video digitali**.

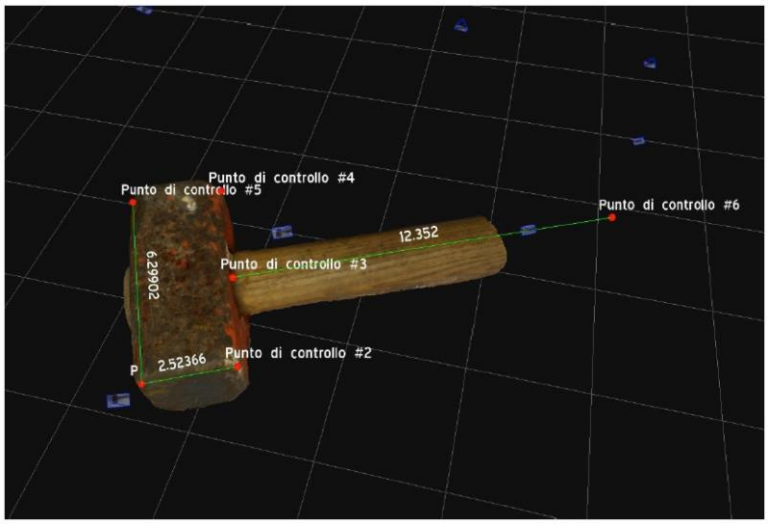
I software esistenti agevolano il lavoro degli investigatori ma non riescono per forza di cose ad automatizzare in maniera sistematica ed efficiente tali operazioni e richiedono l'ausilio di professionisti esperti.

Investigare su Immagini e Video

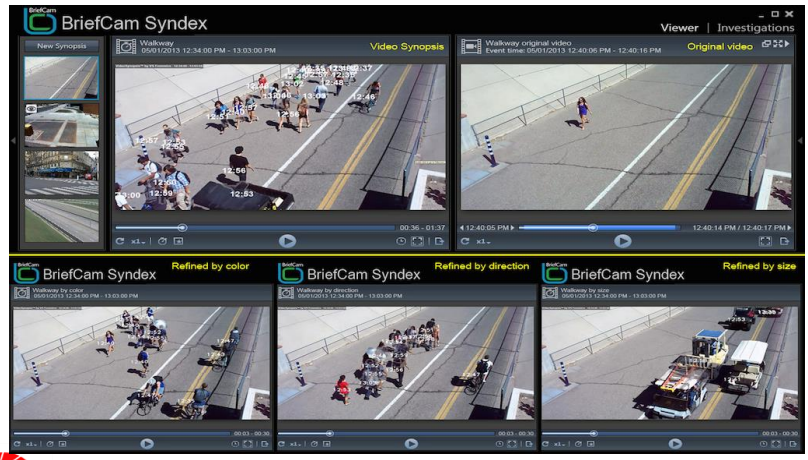
- Fondamenti di elaborazione delle immagini e dei video digitali
- La compressione dei dati
- Contraffazioni: casi famosi e non. Tecniche avanzate per l'identificazione delle contraffazioni: pixel-based, format-based, camera-based, physically-based, geometric based.
- Cenni di Steganografia
- Tip&tricks – 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

Nuove Tecnologie…




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

Video synopsis – Brief cam

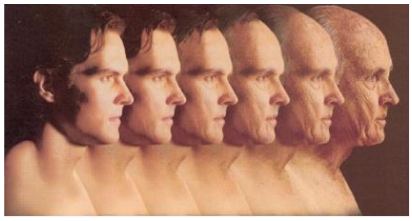


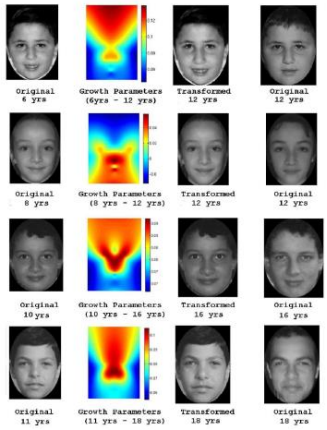
https://youtu.be/fISfDd35sXU

Video Fingerprint

- **Photo DNA (http://www.microsoftphotodna.com/)**
- **VideoGenome (http://v-nome.org/)**
- **Videntifier (http://www.eff2.net/)**

Riconoscimento ed Aging

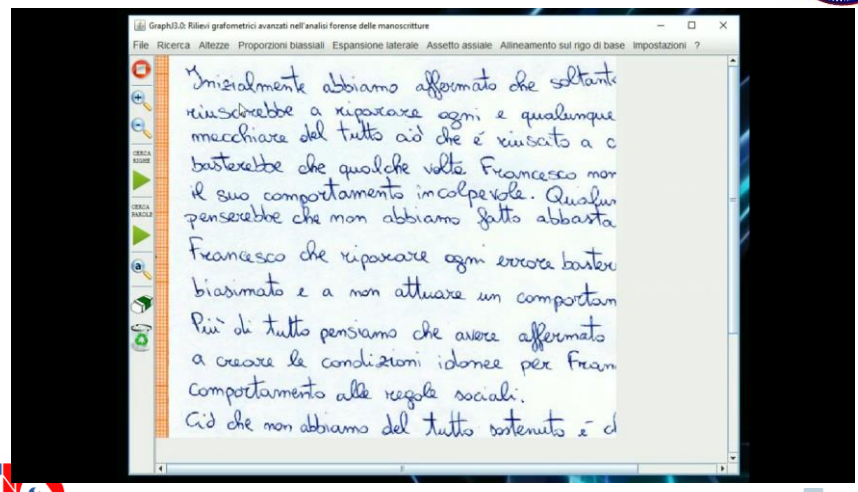




Digital Forensics

141

GraphJ: Analisi Manoscritture



http://iplab.dmi.unict.it/graphj/

Digital Forensics

142

Balistica Digitale



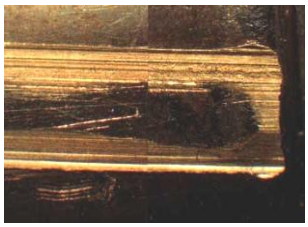
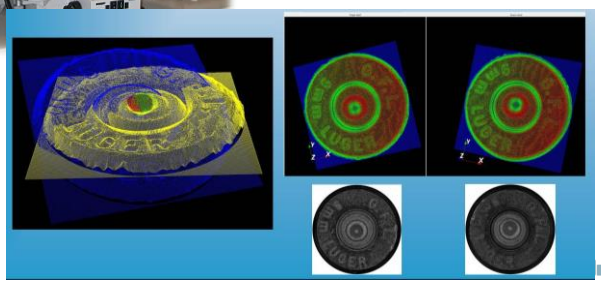



Image Forensics @IPLab
http://iplab.dmi.unict.it/mfs

- Support and technical advices to investigations, referring more precisely on multimedia contents analysis (Images, Videos, etc.).
- Applied and basic R&D in partnership with private and public institutions.
  - RIS (Reparto Investigativo Speciale) - Carabinieri Messina
  - Polizia di Stato – DAC e Polizia Scientifica (Roma)
  - IA- BPM – ENFSI
  - Presidenza del Consiglio di Ministri – Polo Tecnologico

  - IISFA
  - Forensics Group
  - Onlus (Telefono Arcobaleno, ecc.)
  - Ordini Professionali (Ingegneri, Avvocati, ecc.)

Contatti

Per ulteriori dettagli o info si visiti il sito

www.dmi.unict.it/~battiato/CF

Email

battiato@dmi.unict.it