UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

Informatica forense

INTRODUZIONE ALL'INFORMATICA FORENSE

Ugo LOPEZ

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Docente

Nome:	**Ugo LOPEZ**
Materie (LM CyberSecurity):	**Informatica forense**
	Sicurezza nelle reti e nei sistemi distribuiti
LinkedIn:	**Ugolopez.link/LinkedIn**
Email/Teams:	**ugo.lopez@uniba.it**
Telegram/Twitter:	**@ugolopez**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Introduzione all'informatica forense

- Brevi cenni storici sulla scienza forense
- Definizione di informatica forense
- Obiettivi dell'informatica forense
- Esempi di casi mediatici, diritto e giurisprudenza
- Principali rami dell'informatica forense
- Settori di applicazione dell'informatica forense
- Il metodo scientifico
- La prova digitale
- La catena di custodia
- Il processo di acquisizione della prova

Origini della moderna scienza forense

- Nel 1879 un impiegato di una questura francese, Alphonse BERTILLON, introduce un sistema di documentazione fotografica della scena del crimine
- Successivamente inventò l'**antropometria giudiziaria**, nota anche come il «*sistema Bertillon*»

Principio di Locard

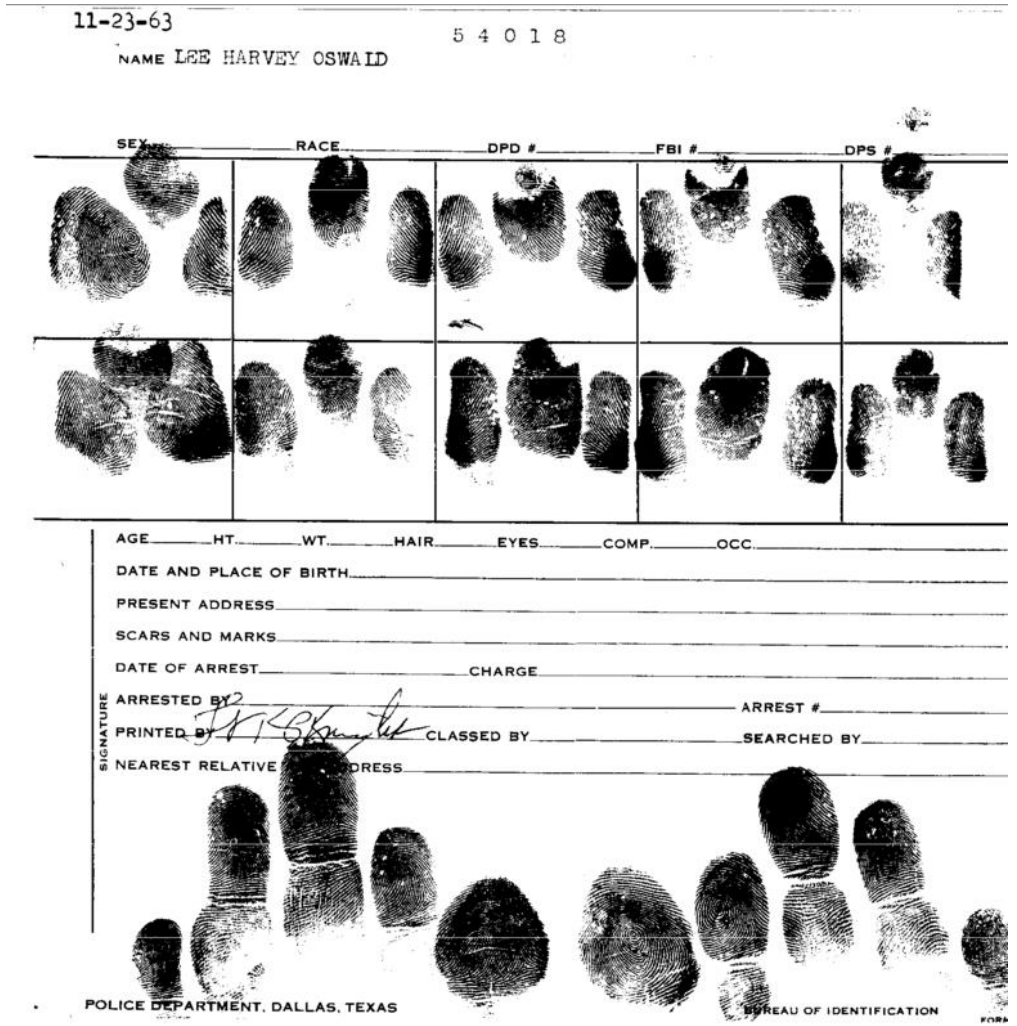
- Edmond Locard, padre della scienza forense come disciplina strutturata
- **Non si può entrare e/o uscire da un posto senza lasciare qualcosa di sè**

Definizione di scienza forense

La scienza forense è l'applicazione di tecniche e metodologie scientifiche alle tradizionali investigazioni di carattere giudiziario

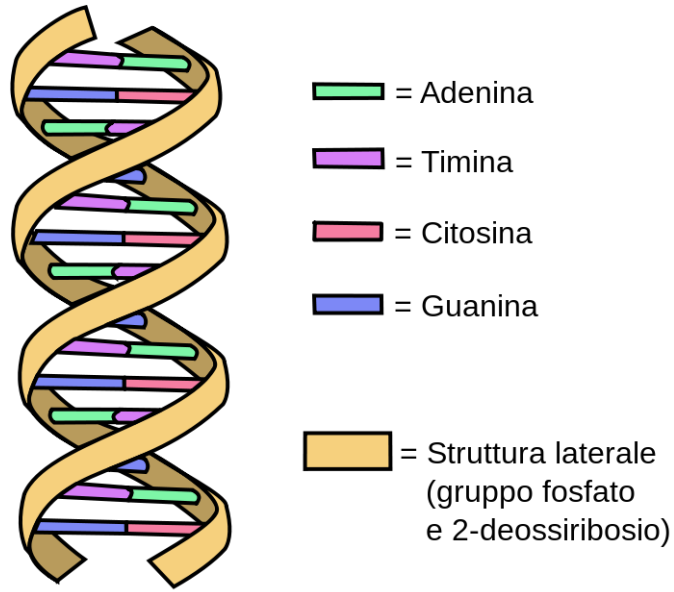
Impronte digitali

- Costituiscono il successivo “passaggio evolutivo” della scienza forense
- Usate sin dal 500 a.c. in Cina e Babilonia come firma personale
- Lo studio programmatico (**dattiloscopia**) risale invece alla fine del XII secolo
- *De externo tactus organo anatomica observatio* (1665) a cura di Marcello MALPIGHI
- Primo uso nelle scienze forensi nel 1880 (Henry Faulds)
- **Prima identificazione certa di un criminale (1892 – Francisca Rojas – Argentina)**



DNA

- Isolato da Friedrich Miescher nel 1869
- James Watson e Francis Crick presentarono il primo modello accurato nel 1953
- Nel 1984 Sir Alec Jeffreys sviluppa un metodo per l'identificazione di persone su scene del crimine (**fingerprinting genetico**)
- Il metodo fu usato per la prima volta nel 1988 per incriminare l'assassino Colin Pitchfork



DNA

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Informatica forense

- È attualmente la più giovane branca della scienza forense (anni ’80)
- Parallelamente, si sviluppa il concetto di **crimine informatico**
- Ad oggi usata non solo per il repertamento ma anche come mezzo d’indagine in senso lato

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Breve storia dell'informatica forense

- Nel 1984 l'FBI e altre agenzie governative americane iniziano a sviluppare programmi per reperire indizi all'interno dei computer
- Nasce il **Computer Analysis and Response Team** (**CART**) che, però, diventerà operativo solo nel 1991
- Andrew Rosen realizza per la polizia canadese **Desktop Mountie**, il primo strumento software per l'informatica forense
- Su questa falsariga, nasceranno poi **Expert Witness**, **Encase** e **Smart**
- Si sviluppa molto tra il 1997 ed il 2007, considerati gli "anni d'oro" dell'informatica forense

Chi è l'informatico forense?

"Digital forensics, also known as cyber forensics and computer forensics, is generally considered to consist of three roles in one: that of a cyber analyst familiar with the working of computer devices and networks, a detective with knowledge of investigating crime, and a lawyer with a sound understanding of the law and court procedures" (R. Boddington, "Practical Digital Forensics")

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Definizione di informatica forense

L'informatica forense (o *digital forensics*, prima nota col nome di *computer forensics*) è una branca della scienza forense legata alle prove acquisite da computer e altri dispositivi di memorizzazione digitale. Il suo scopo è quello di esaminare dispositivi digitali seguendo processi di analisi forense al fine di identificare, preservare, recuperare, analizzare e presentare fatti o opinioni riguardanti le informazioni raccolte

Crimini informatici

- Pedopornografia
- Cyberstalking
- Frodi informatiche
- Spionaggio
- Cyberbulling
- …

Computer Generated Evidence

L’informatica forense può essere utilizzata anche nel caso di reati non strettamente legati all’informatica (omicidi, stupri, etc.) nonché in contesti differenti (civile, amministrativo, tributario, arbitrale, stragiudiziale, etc.)

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

La sentenza Frye e i criteri Daubert

- **Sentenza Frye (1923)**: a partire da questo momento e per 70 anni vennero considerate attendibili solo le prove accettate dalla comunità scientifica di riferimento
- **Sentenza Daubert (1993)**: supera il «principio di Frye» ammettendo prove di segno opposto a quelle prodotte dalla comunità scientifica

Criteri Daubert (Del Pero, 2015)

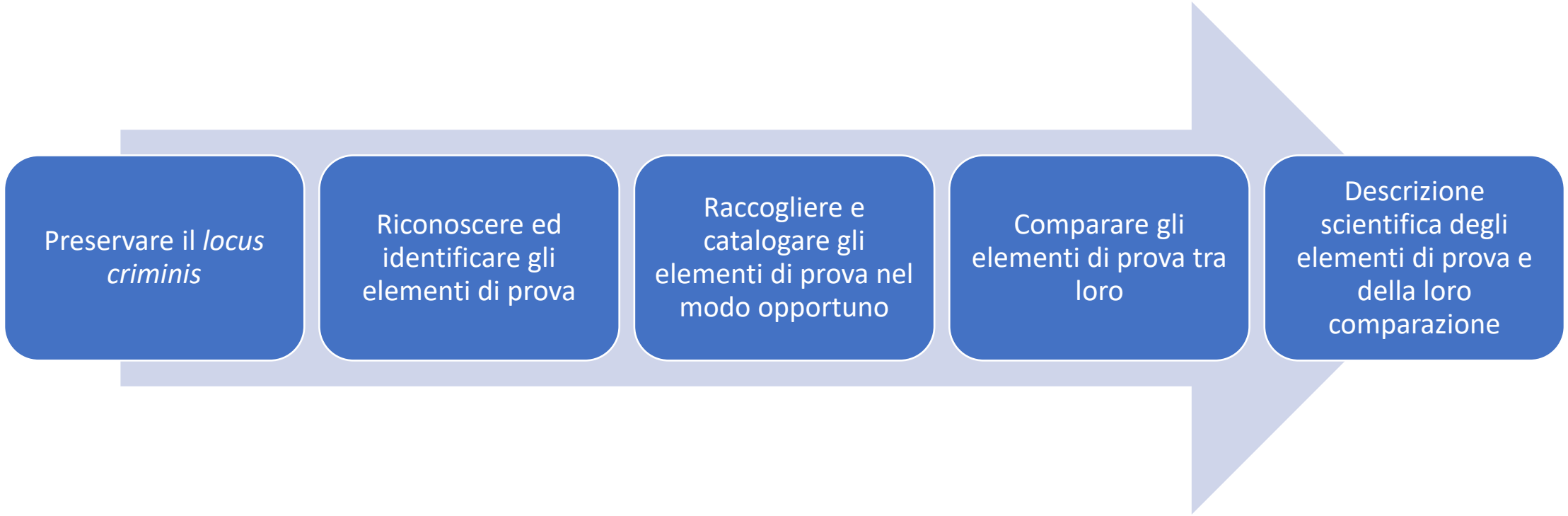
- Attendibilità (confronto tra ricerche analoghe)
- Validità (i risultati sono conformi all'esistente?)
- Generalizzabilità (applicabilità a casi analoghi)
- Credibilità (procedura e risultati affidabili)
- Falsificabilità (test con metodo scientifico)
- Blind Peer Review
- Accettabilità (risultati condivisi dalla comunità scientifica)
- Controllo metodologico (potenziale di errore)
- Affidabilità (stabilità in tempi diversi)
- Validità e validità incrementale (nuove informazioni)
- Sensitività (incidenza falsi positivi)
- Specificità (incidenza falsi negativi)

Sentenza Cozzini

- Introduce di fatto i «criteri Daubert» come forma di valutazione della scientificità di una prova anche nei tribunali italiani (Cass. Pen., sez. IV, n. 43786 del 17 settembre 2010)
- Ripresa più volte dalla giurisprudenza di merito e di legittimità (ad esempio la cd sentenza Fincantieri, in cui si ritiene inaffidabile la perizia di parte per esiguità del campione osservato, Cass. Pen. Sez. IV, sent. n. 33311/2012)

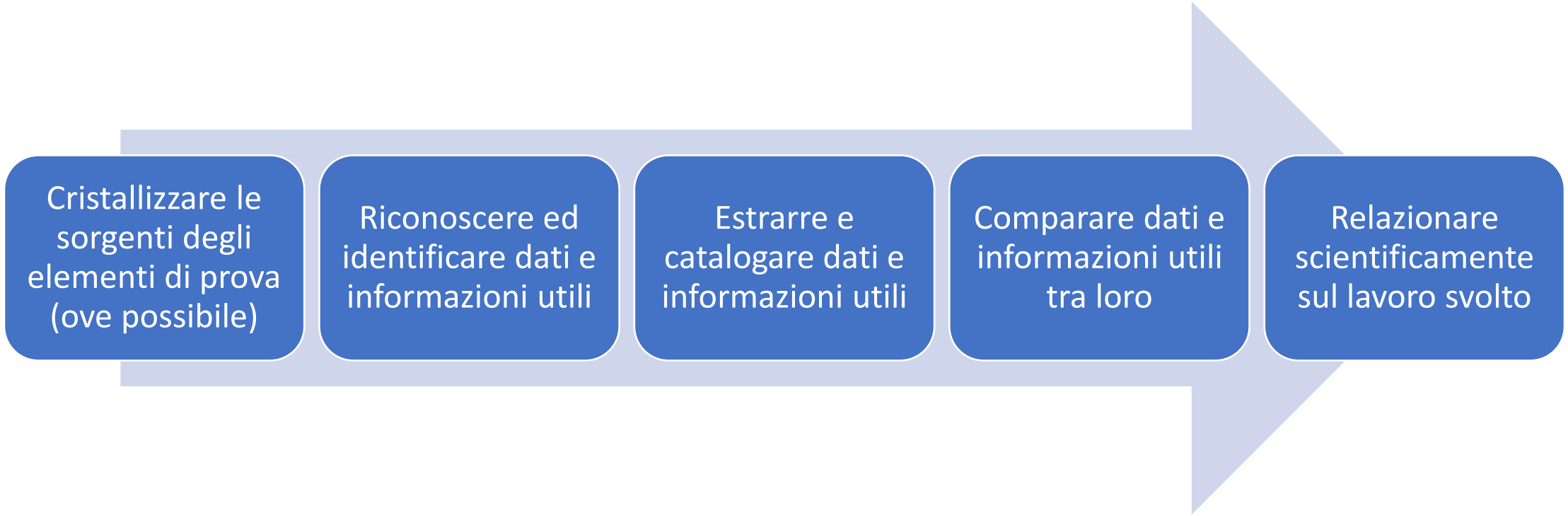
UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Obiettivi della scienza forense



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Obiettivi dell'informatica forense



Precisazioni sulle linee guida dell'informatica forense

Data la giovane età della disciplina, possiamo provare a tracciare delle linee guida conformi al settore scientifico di riferimento ma, nei fatti, non esiste una piena standardizzazione dell'informatica forense le cui procedure, spesso, variano non solo sulla base dell'ordinamento nazionale ma, spesso, da Tribunale a Tribunale o, addirittura, all'interno dello stesso Tribunale, da Giudice a Giudice

Caso Garlasco

- Il 13 agosto 2007 Chiara Poggi, 26 anni, viene uccisa nella sua casa
- Il fidanzato, Alberto Stasi, 24 anni, viene arrestato 6 settimane dopo
- Alberto Stasi viene ritenuto colpevole il 12 dicembre 2015 dalla Corte di Cassazione
- La vicenda giudiziaria principale ed altre ad essa connesse presentano ancora degli strascichi

Caso Garlasco – Questione informatica

- Secondo la difesa, alla presunta ora del delitto Alberto STASI stava scrivendo la tesi sul suo computer
- 13.8.2007 – Delitto di Garlasco
- 14.8.2007 – I Carabinieri sequestrano il computer a Stasi
- 29.8.2007 – I Carabinieri consegnano il computer ai RIS
- Alberto STASI subisce un ulteriore procedimento per detenzione di materiale pedopornografico

Caso Garlasco – 14-29.8.2007

- Cosa hanno fatto i Carabinieri in questo periodo di tempo?
- «Da quel giorno e fino al 29 agosto sono 42 gli accessi fatti dai carabinieri prima della consegna ai colleghi del Ris di Parma. In quel periodo è stato acceso e spento più volte e questo potrebbe aver "alterato", sia a favore della difesa che a favore dell'accusa, quanto contenuto . Un dubbio sollevato nelle motivazioni, circa 15 pagine, scritte dal gup che ha replicato punto su punto alle eccezioni avanzate dalla difesa» (fonte «La Stampa»)

Caso Garlasco – Accuse di pedopornografia

“Non vi è prova di come quei frammenti di file siano pervenuti nel computer, nè che Stasi li abbia visionati e nemmeno che dai nomi dei frammenti di file emergesse il loro contenuto pedopornografico” (fonte «Il Giorno»)

Caso Vierika

Un virus informatico dal nome Vierika si diffonde molto rapidamente («in un solo giorno aveva infettato mille computer», fonte «La Repubblica)

Caso Vierika – Il «metodo» informatico

«La difesa dell'imputato sia nel corso dell'istruttoria, che nell'arringa finale ha reiteratamente posto in discussione la correttezza sia del metodo utilizzato dalla p.g. per estrarre i programmi dal computer del C., che di quello applicato dalla p.g. e dalle società Infostrada s.p.a. e Tiscali s.p.a. per individuare l'amministratore degli spazi web (uno dei quali contenente il secondo script del programma Vierika). **Il tema è, in termini generali, di non poco momento e certamente dovrà essere affrontato in maniera approfondita anche dalla giurisprudenza**» (Sentenza di primo grado)

Caso Vierika – Sentenza d’appello

Interessanti le motivazioni usate nel rigetto delle aggravanti che suggeriscono una interpretazione sistematica e non letterale dell’art. 615 ter c.p.

Caso Google-Vivi Down

Quattro dirigenti di Google vengono chiamati a rispondere di fronte al tribunale penale di Milano per violazione della privacy e concorso omissivo nel reato di diffamazione. Questo a causa di un video inserito (nel 2006) in YouTube (di Google), nel quale un bambino con sindrome di Down veniva picchiato e deriso dai suoi compagni di scuola (fonte “Il Fatto Quotidiano”)

Caso Google-Vivi Down – Pag. 31 sentenza di primo grado (Trib. Ord. Milano, Sent. n. 1972/10 del 24.2.2010)

"[...] veniva infine depositata [...] **la stampa degli oltre 60 commenti degli utenti al video in esame** [...]"

Caso Google-Vivi Down – Dichiarazioni avv. VACIAGO

«…nel 2010 non dovrebbe essere più possibile produrre come prova in un processo penale un documento cartaceo di una pagina web corredato da un file digitale in formato word contenente il "copia e incolla" della medesima pagina web. Ci sono strumenti gratuiti e validissimi che permettono di garantire certezza nella fase dell’acquisizione di una prova digitale presente in Rete come ad esempio il software hashbot (http://www.hashbot.com/) che tra le altre cose è stato progettato da informatici italiani…»

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Caso Google-Vivi Down Esempio di acquisizione commenti

john
2 giorni fa
Che bella classe di dementi e minorati! E ovviamente non mi riferisco al p
crudelmente in giro. Complimenti ai genitori e agli insegnanti...

Anonimo
2 giorni fa
Vergogna...

gregorj
2 giorni fa
Complimenti: siete finiti su http://giornalettismo.ilcannocchiale.it

Anonimo
3 giorni fa
E' vergognoso! Andrebbe tolto immediatamente.

ummm
4-ott-2006
c'è più di un mongoloide in quella classe

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Cass. Sez. Lavoro n. 2912/04 del 2.12.2003

«…Va esclusa la qualità di documento in una copia su supporto cartaceo che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità a un ben individuato momento…»

Art. 20, I comma, DPR 445/2000 **abrogato nel 2005**

«…i duplicati, le copie, gli estratti del documento informatico**, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge se conformi alle disposizioni del presente testo unico** [*omissis*]
Le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato…»

Trib. Pescara – Sent. 1369/06 del 3 novembre 2006

Diffusione tramite sito web di immagini oscene – insufficienza a fini probatori della mera riproduzione a stampa operata dalla polizia giudiziaria – sussiste

(**la sentenza è precedente alla L. 48/2008**)

Motivazioni Sent. 1396/06 (1)

«il difensore dell’imputato ha contestato che le riproduzioni a stampa, di cui ha riferito il teste Bonifacio, consentano di stabilire inequivocamente autenticità, provenienza, data di pubblicazione e riferibilità all’imputato medesimo delle pagine web in contestazione»

Motivazioni Sent. 1396/06 (2)

«Disposta dunque perizia nel dibattimento, il perito ha dovuto concludere di essere impossibilitato ad ogni considerazione, non essendo riuscito ad acquisire le pagine web nel formato digitale, al fine di valutarne contenuto e caratteristiche tecniche; quindi censurando la mancata acquisizione di copia certificata dei documenti informatici, con eventuale sottoscrizione (firma digitale), come previsto dalla normativa tecnica già all'epoca emanata dall'AIPA (Autority per l'Informatica nella P.A., ora CNIPA centro Nazione per l'Informatica nella P.A.), in tema di creazione, diffusione e conservazione della documentazione informatica; sostanzialmente dunque confermando la scarsa valenza probatoria delle riproduzioni a stampa summenzionate (difficilmente classificabili, alla stregua della stessa normativa tecnica, quali "documenti analogici originali"), peraltro rimarcando come queste riportino diverse date di consultazione delle pagine all'indirizzo www.vallecupa.com, precisamente il 17.9.2002, 3.9.2002 e 29.7.2002, per giunta evidentemente successive all'epoca di contestazione del commesso reato»

Trib. Pen. xxx, Sent. n. xxx/19 del xx.x.2019 – Il CTP

«La correttezza della ricostruzione fattuale appena esposta è stata resa oggetto di critiche dal consulente xxx xxx, nominato difensore degli imputati, che ha sottolineato come i risultati degli accertamenti informatici effettuati nel corso delle indagini siano del tutto inaffidabili, **giacché ottenuti secondo modalità non forensi** e comunque non ripetibili, con conseguenti gravi lesioni sul piano del diritto di difesa costituzionalmente accordato ai soggetti attinti al processo penale»

Trib. Pen. xxx, Sent. n. xxx/19 del xx.x.2019 – Il Giudice

«…L'affidabilità dei risultati raggiunti è piena non soltanto con riferimento a quanto compiuto dall'autorità giudiziaria inquirente, terza e imparziale rispetto agli esiti della presente vicenda processuale, ma anche con riguardo alle attività di monitoraggio e prevenzione svolte dai tecnici di xxx xxx, **sia pure considerato l'interesse che tale società, oggi costituita parte civile**, possedeva già al tempo delle indagini quale persona offesa.[omissis]**non vi è alcun motivo per ritenere che tali risultati siano stati manomessi o alterati** per viziarne la portata probatoria…»

Rami dell'informatica forense

- Computer forensics
- Mobile forensics
- Network forensics
- Open Source Intelligence
- Cloud forensics
- Bitcoin forensics
- …

Computer Forensics

La computer forensics è il ramo della digital forensics che si occupa di identificare, acquisire, preservare e analizzare gli indizi digitali presenti su computer o similari a fini giuridici o giudiziari.

All’interno della disciplina possiamo trovare vari sottorami quali la **Windows Forensics**, la **Ubuntu Forensics** ed altri

Mobile forensics

La mobile forensics è il ramo della digital forensics che si occupa di identificare, acquisire, preservare e analizzare gli indizi digitali presenti su smartphone o similari a fini giuridici o giudiziari.

All'interno della disciplina possiamo trovare vari sottorami quali la **Android Forensics** e la **iPhone Forensics**

Network Forensics

La network forensics è il ramo della digital forensics che si occupa di identificare, acquisire, preservare e analizzare i dati che coinvolgono più sistemi informatici collegati tra loro all'interno di una rete di calcolatori

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Open Source INTelligence (OSINT)

La **Open Source INTelligence** è l'attività di raccolta d'informazioni mediante la consultazione di fonti di pubblico accesso (Wikipedia)

Cloud Computing

Definizione seria: «Il cloud computing è un modello che fornisce un accesso rapido e pratico on-demand via internet ad un gruppo di infrastrutture condivise e configurabili che può essere rilasciato rapidamente e con la minima interazione del fornitore» (NIST)

Definizione semiseria: «Il cloud è il computer di qualcun altro»

Cloud Forensics

La Cloud Forensics è il ramo della digital forensics che si occupa di identificare, acquisire, preservare e analizzare i dati reperiti in reti, computer e dispositivi di memorizzazione digitale impiegati in infrastrutture cloud

Bitcoin Forensics

La Bitcoin Forensics è il ramo della digital forensics che si occupa di identificare, acquisire, preservare e analizzare i dati in un sistema di criptovalute

Settori di applicazione dell'informatica forense

- Penale
- Civile
- Amministrativo
- Tributario
- Sportivo (e.g. caso Bracciali/Starace – Tennis scommesse)
- Arbitrale
- Stragiudiziale
- Analisi pre-giudiziali
- Spionaggio
- Controspionaggio
- …

Metodo scientifico

«Il metodo scientifico, o metodo sperimentale, è la modalità tipica con cui la scienza procede per raggiungere una **conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile**. Esso consiste, da una parte, nella raccolta di dati empirici sotto la guida delle ipotesi e teorie da vagliare; dall'altra, nell'analisi rigorosa, logico-razionale e, dove possibile, matematica di questi dati, associando cioè, come enunciato per la prima volta da Galilei, le «sensate esperienze» alle «dimostrazioni necessarie», ossia la sperimentazione alla matematica» (Wikipedia)

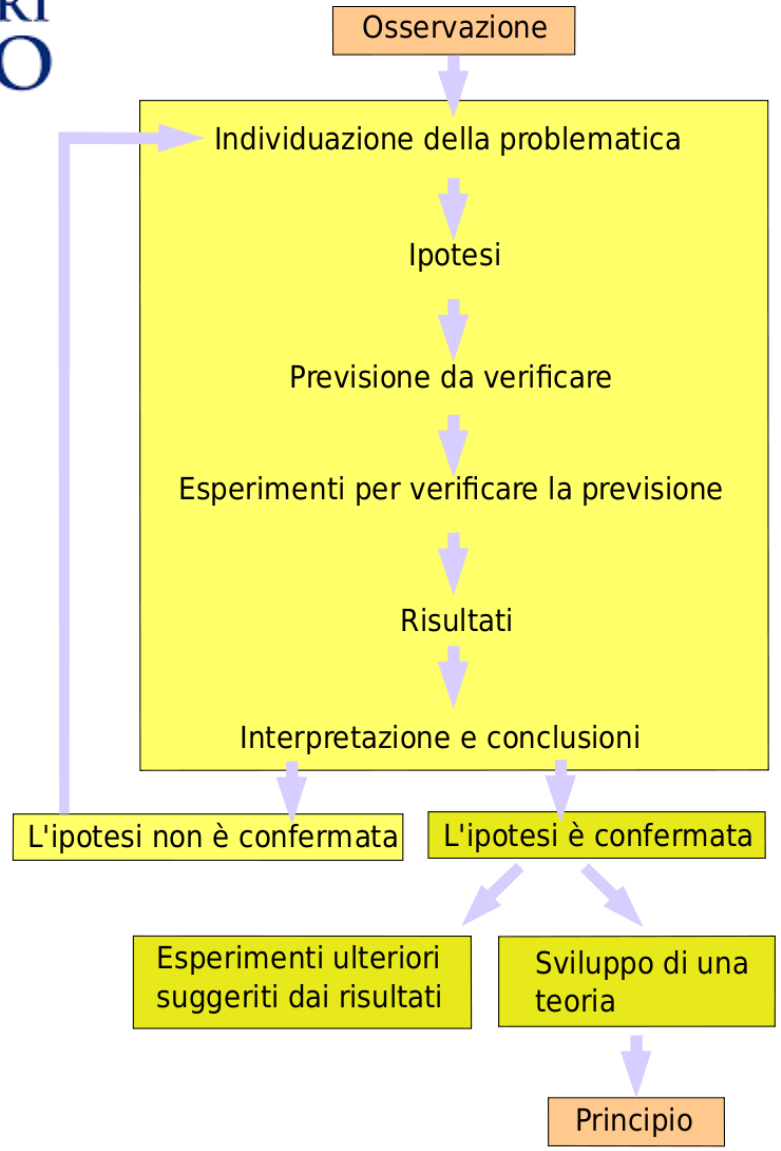
Storia del metodo scientifico

- Storicamente attribuito a Galileo GALILEI (tant'è che assume anche il nome di metodo galileiano) nell'attuale forma rigorosa
- Vi è traccia di approcci metodologici simili sin dall'antico Egitto
- Sviluppato successivamente da Kant nella Deduzione trascendentale
- Trova la sua massima espressione nella relatività generale di Einstein
- Formalizzato più recentemente da Popper, con cui viene sancita la superiorità del metodo deduttivo sul metodo induttivo

Massime

- «***Nissuna umana investigazione si può dimandare vera scienza, s'essa non passa per le matematiche dimostrazioni***» (L. Da Vinci)
- «**Max Planck non capiva nulla di fisica perché durante l'eclissi del 1919, è rimasto in piedi tutta la notte per vedere se fosse stata confermata la curvatura della luce dovuta al campo gravitazionale. Se avesse capito davvero la teoria avrebbe fatto come me e sarebbe andato a letto**» (A. Einstein)

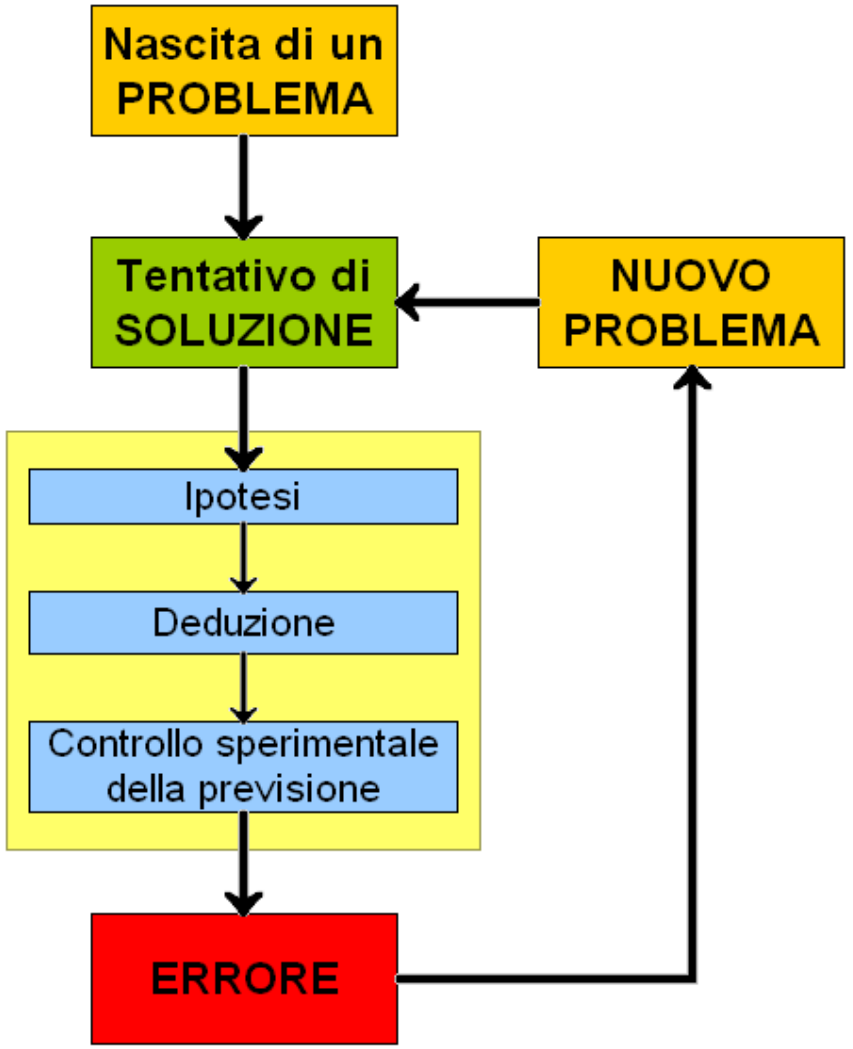
Il metodo induttivo



Limiti del metodo induttivo

Il paradosso del tacchino induttivista di Russell e Popper

Il metodo deduttivo



Il metodo come sostituto all'osservazione

Il paradosso di Achille e della tartaruga di Zenone: il problema dei quanti di materia risolto con 3000 anni di anticipo

Principio di falsificazione e ripetibilità

Il metodo deduttivo ben si adatta all'informatica forense, questo perché consente alle parti processuali, in ottemperanza al principio dispositivo, di provare a falsificare gli elementi di prova ripetendo gli esperimenti nelle medesime condizioni in cui sono stati effettuati dai periti/consulenti del Giudice o delle altre parti

Elemento di prova digitale

Nel 2020, la dimensione dei dati digitali prodotti da umani e macchine (e.g. periferiche IoT) supererà 44 zettabytes (1024^7 bytes) – Fonte EMC Corporation, “The Digital Universe of Opportunities,” 1.6.2018

La Digital Forensics consente di acquisire prove digitali (chiamate anche **Electronically Stored Information – ESI**) da vari dispositivi di memoria digitali (computer, smartphone, cellulari, tablet, hard disk interni ed esterni, schede di memoria, fotocamere e videocamere, DVR, etc.)

Catena di custodia e sigillo digitale

Il termine catena di custodia (in inglese chain of custody) si riferisce alla documentazione cronologica o alla traccia cartacea che mostra il sequestro, la custodia, il controllo, il trasferimento, l'analisi, e la disposizione di elementi di prova, fisica o elettronica (Fonte – Wikipedia)

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Informazioni registrate nella catena di custodia

1. Cosa è l'elemento di prova digitale?
2. Dove è stato trovato?
3. Come è stato acquisito?
4. Come è stato trasportato, conservato e gestito?
5. Come è stato esaminato?
6. Quando, chi e come vi ha avuto accesso?
7. Come è stato usato durante l'investigazione?

Esempio di modelli NIST per la catena di custodia

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM
(Continued)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____ is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ ID#: _____ in my presence on (date) _____.

Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ ID#: _____ to

Name _____

Address: _____ City: _____ State: _____ Zip Code: _____

Telephone Number: (____) _____

Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Processo di acquisizione della prova

Fasi nel dettaglio

Come già accennato, il processo di acquisizione di un elemento di prova non è ancora standardizzato per cui, a parte le 4 macro fasi descritte, comunemente accettate, ogni consulente si regola sulla base della propria esperienza

Identificazione

Identificazione dei dati da analizzare e dei supporti da cui estrarli, nonché eventuale trasporto sicuro nel laboratorio forense

Acquisizione

Consiste nella duplicazione forense del supporto da analizzare (ove possibile) con cristallizzazione tramite funzioni di hash. È buona norma effettuare più copie forensi

Analisi

In questa fase, i contenuti delle copie forense vengono analizzati attraverso appositi strumenti possibilmente forensi

Presentazione

In questa fase, l’informatico forense produce un report dettagliato sulle ricerche effettuate e gli esiti raggiunti

Tentativi di standardizzare le procedure di informatica forense

- "Guide to Integrating Forensics Techniques into Incident Response" (NIST)
  - Contiene indicazioni di metodo forense dividend le investigazioni sulla base della sorgente dati (file, sistemi operativi, traffico di rete, operazioni)
- "Forensics Examination of Digital Evidence: A Guide for Law Enforcement" (US DoJ)
- "Electronic Crime Scene Investigation: A Guide for First Responders" (US DoJ)
- "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors" (US DoJ)
- "ACPO Good Practice Guide for Digital Evidence" (Association of Chief Police Officers)

Bibliografia

- “Practical Digital Forensics”, Richard Boddington, Packt Publishing, ISBN: 978-1-78588-710-9
- https://it.wikipedia.org/wiki/Scienza_forense
- https://it.wikipedia.org/wiki/Alphonse_Bertillon
- https://it.wikipedia.org/wiki/Edmond_Locard
- https://it.wikipedia.org/wiki/Impronta_digitale
- https://it.wikipedia.org/wiki/DNA
- https://it.wikipedia.org/wiki/Informatica_forense
- http://padova.movimentoforense.it/media/files/MF_Padova-Vicenza/slide-forensics-2.pdf
- http://www1.lastampa.it/redazione/cmsSezioni/cronache/200903articoli/41978girata.asp
- https://www.ilgiorno.it/pavia/cronaca/2014/03/05/1034891-Stasi-Pedopornografia.shtml
- http://www.penale.it/page.asp?mode=1&IDPag=182
- http://www.penale.it/page.asp?mode=1&IDPag=182
- https://www.repubblica.it/online/tecnologie_internet/zombie/vierika/vierika.html
- http://www.scintlex.it/documenti/%5bScintLex%5d%20Caso%20Vierika.pdf
- https://www.diritto.it/danneggiamento-dei-sistemi-informatici-ed-accesso-abusivo-ai-sensi-dell-art-615-ter-del-c-p/
- http://www.ilfattoquotidiano.it/2014/02/04/il-caso-vividown-e-lassoluzione-digoogle/868850/
- http://www.giurcost.org/casi_scelti/Google.pdf
- https://www.gennarocarotenuto.it/12914-caso-vividown-google-condannata-la-parola-alla-difesa/
- https://www.ricercagiuridica.com/sentenze/sentenza.php?num=428
- https://www.ictlex.net/?p=553
- https://it.wikipedia.org/wiki/Open_Source_Intelligence
- https://csrc.nist.gov/publications/detail/sp/800-145/final
- https://it.wikipedia.org/wiki/Metodo_scientifico
- https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm
- https://it.wikipedia.org/wiki/Catena_di_custodia
- https://www.nist.gov/document/sample-chain-custody-formdocx