



Corso di Digital Forensics

CdLM in Informatica

Università degli Studi di Salerno

Docente: Ugo Fiore

0 – Concetti di base

Le Origini dell'Investigazione Forense

1879

Alphonse Bertillon

Membro della Polizia di Parigi

1879

Alphonse Bertillon

Membro della Polizia di Parigi



1853-1914

Fonte:

https://it.wikipedia.org/wiki/Alphonse_Bertillon#/media/File:Bertillon_selfportrait.jpg

1879

Alphonse Bertillon

Membro della Polizia di Parigi

- Introduzione di un **processo di documentazione** di «*elementi*» (es. armi, oggetti, ecc.), in una **scena del crimine**
 - La documentazione avveniva mediante **fotografie**
- Bertillon affermava che la **scienza** e la **logica** dovrebbero essere utilizzate per **investigare** e **risolvere** il **crimine**
- Il lavoro scientifico di Bertillon ha notevolmente influenzato uno dei suoi seguaci: **Edmond Locard**

1879

Alphonse Bertillon

Membro della Polizia di Parigi

- Introduzione di un **processo di documentazione** di «*elementi*» (es. armi, oggetti, ecc.), in una **scena del crimine**
 - La documentazione avveniva mediante **fotografie**
- Bertillon affermava che la **scienza** e la **logica** dovrebbero essere utilizzate per **investigare** e **risolvere** il **crimine**
- Il lavoro scientifico di Bertillon ha notevolmente influenzato uno dei suoi seguaci: **Edmond Locard**

Edmond Locard

Principio di Scambio di Locard

1879

Alphonse Bertillon

Membro della Polizia di Parigi

- Introduzione di un **processo di documentazione** di «*elementi*» (es. armi, oggetti, ecc.), in una **scena del crimine**
 - La documentazione avveniva mediante **fotografie**
- Bertillon affermava che la **scienza** e la **logica** dovrebbero essere utilizzate per **investigare** e **risolvere** il **crimine**
- Il lavoro scientifico di Bertillon ha notevolmente influenzato uno dei suoi seguaci: **Edmond Locard**



Un'azione criminale di un individuo non può verificarsi senza lasciare un segno



Edmond Locard
Principio di Scambio di Locard

1879

Alphonse Bertillon

Membro della Polizia di Parigi

- Introduzione di un **processo di documentazione** di «*elementi*» (es. armi, oggetti, ecc.), in una **scena del crimine**
 - La documentazione avveniva mediante **fotografie**
- Bertillon affermava che la **scienza** e la **logica** dovrebbero essere utilizzate per **investigare** e **risolvere** il **crimine**
- Il lavoro scientifico di Bertillon ha notevolmente influenzato uno dei suoi seguaci: **Edmond Locard**

Edmond Locard

Principio di Scambio di Locard

- Principio forense fondamentale basato sullo **scambio comune** di **tracce fisiche** su una **scena del crimine**
- **Esempi di tracce fisiche**
 - Impronte digitali
 - Tracce di DNA
 - Residui di polvere da sparo
- Sebbene di natura circostanziale, le tracce, raccolte nella scena del crimine, aiutano a **ricostruire** quello che è successo ed **identificare** i presenti

1879

Alphonse Bertillon

Membro della Polizia di Parigi

- Introduzione di un processo di documentazione di «elementi» (es. armi, oggetti, ecc.), in una **scena del crimine**
 - La documentazione avveniva mediante **fotografie**
- Bertillon affermava che la **scienza** e la **logica** dovrebbero essere utilizzate per **investigare** e **risolvere** il crimine
- Il lavoro scientifico di Bertillon ha notevolmente influenzato uno dei suoi seguaci:
Edmond Locard

Edmond Locard

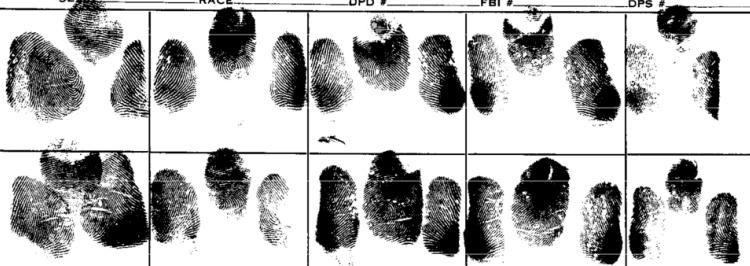
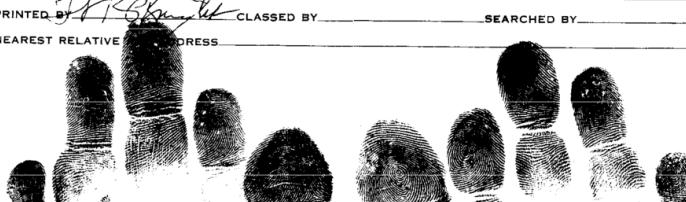
Principio di Scambio di Locard

- Principio forense fondamentale basato sullo **scambio comune** di **tracce fisiche** su una **scena del crimine**
- **Esempi di tracce fisiche**
 - Impronte digitali
 - Tracce di DNA
 - Residui di polvere da sparo
- Sebbene di natura circostanziale, le tracce, raccolte nella scena del crimine, aiutano a **ricostruire** quello che è successo ed **identificare** i presenti

- Ad oggi, le tecniche di analisi forense si sono **notevolmente evolute** dall'epoca di Bertillon e Locard
- Tuttavia, essi hanno introdotto **tre concetti fondamentali** che assistono gli investigatori e la giustizia penale:
 - Documentazione relativa alla scena del crimine
 - Identificazione di elementi utili per l'indagine (tracce)
 - Disciplina dell'analisi delle tracce

Le Impronte Digitali

- **Pietra miliare** nella scienza forense

11-23-63		5 4 0 1 8				
NAME LEE HARVEY OSWALD						
SEX	RACE	DPD #	FBI #	DPS #		
						
AGE	HT.	WT.	HAIR	EYES	COMP.	OCC.
DATE AND PLACE OF BIRTH _____						
PRESENT ADDRESS _____						
SCARS AND MARKS _____						
DATE OF ARREST _____		CHARGE _____				
SIGNATURE ARRESTED BY <i>JFK</i>	CLASSED BY			ARREST # _____		
PRINTED BY <i>JFK</i>				SEARCHED BY _____		
NEAREST RELATIVE	ADDRESS					
						



Le Impronte Digitali

- Pietra miliare nella scienza forense
- Inizialmente usate nei documenti legali cinesi, per secoli, come prova di identità e autenticità

1897

- Edward Henry inventò un valido **sistema di classificazione di impronte**
- Tale sistema venne **realizzato in India, nel 1897**

1902

- Nel 1901, il sistema di Edward Henry fu **presentato presso la polizia metropolitana di Londra**
- Nello stesso anno fu **adottato da New Scotland Yard**
- Nel **1902**, vi fu la **prima condanna giudiziaria grazie alle impronte digitali**

- Da notare, però, che l'affidabilità delle prove relative alle impronte digitali, è stata **recentemente contestata** in diverse giurisdizioni, con preoccupazioni per la **mancanza di standard validi per la valutazione di due impronte «imprese» su carta**

DNA

- Tramite l'**acido desossiribonucleico (DNA)** è possibile determinare le caratteristiche ereditarie di ogni persona
- Le tracce di DNA possono essere estratte da una serie di campioni di:
 - Saliva (es., da francobolli usati, buste, il filo interdentale)
 - Campioni ematici (es., da rasoi usati, i capelli, i vestiti, ecc.)

1987

- In Oregon, nel **1987**, le prove basate su DNA vengono **utilizzate per la prima volta**
- Nello specifico, sono state utilizzate per avere un risultato affidabile per la comparazione del DNA di un sospetto ed il DNA individuato nella scena del crimine
- Le prove ottenute dal DNA sono state **usate anche in "casi freddi"** (detti anche **cold case**, ovvero, casi irrisolti), dimostrando **l'innocenza di soggetti ingiustamente condannati**
- Da sottolineare che, data la complessità delle prove del DNA, **inizialmente, molte giurie hanno esitato in relazione a tali prove**
 - Con **l'evoluzione delle tecniche**, invece, tali prove **sono state maggiormente accettate** nelle corti



I Passi Fondamentali di un Esame Forense

Preservare la Scena del Crimine

- Preservare la scena del crimine è **fondamentale** ed è **importantissimo**
- Se l'evidenza è **contaminata, persa** o semplicemente **non identificata e/o trascurata**, tutto ciò che segue può avere un **valore limitato** per gli investigatori, i quali mettono insieme le prove del caso

I Passi Fondamentali di un Esame Forense

Preservare la Scena del Crimine

- Preservare la scena del crimine è **fondamentale** ed è **importantissimo**
- Se l'evidenza è **contaminata, persa** o semplicemente **non identificata e/o trascurata**, tutto ciò che segue può avere un **valore limitato** per gli investigatori, i quali mettono insieme le prove del caso

Riconoscere le Prove

- **Riconoscere le prove ed identificarle** risulta estremamente rilevante
- Individuare i punti in cui cercare può solo migliorare l'esito di un esame forense
- Una volta individuate, le prove devono essere **raccolte** e **classificate**

I Passi Fondamentali di un Esame Forense



Preservare la Scena del Crimine

- Preservare la scena del crimine è **fondamentale** ed è **importantissimo**
- Se l'evidenza è **contaminata, persa** o semplicemente **non identificata e/o trascurata**, tutto ciò che segue può avere un **valore limitato** per gli investigatori, i quali mettono insieme le prove del caso

Riconoscere le Prove

- **Riconoscere le prove ed identificarle** risulta estremamente rilevante
- Individuare i punti in cui cercare può solo migliorare l'esito di un esame forense
- Una volta individuate, le prove devono essere **raccolte** e **classificate**

Visione d'Insieme

- Le prove **non possono essere viste in maniera isolata**
- Dovrebbero essere **confrontate con altre prove** e dovrebbero essere identificate prove «effettive»
 - A tal punto, dovrebbe essere **descritte in termini scientifici**

Motivazioni e Nascita della Digital Forensics

Le Motivazioni | 1/3

- Negli ultimi anni, le **prove digitali** (o *digital evidence*) sono state sempre più utilizzate in ambito legale
- Sono stati individuati **profili specifici** con l'obiettivo di individuare le prove digitali, i quali effettuano analisi attendibili delle loro scoperte, in ambito digitale
- Il notevole incremento del **desktop computing** ha consentito la proliferazione anche della **criminalità informatica (cybercrime)**
- In risposta alla criminalità informatica e l'utilizzo di sistemi informatici come oggetto di un crimine, è emersa l'**investigazione forense digitale (digital forensics)**

Le Motivazioni | 2/3

- La **digital forensics** getta effettivamente le basi, come disciplina, negli anni '80
 - *Principali motivazioni*
 - Maggiore accessibilità dei computer
 - Sia economica sia nell'usabilità
 - Prime interconnessioni tra computer mediante reti locali
 - *Problematiche*
 - Obsolescenza delle leggi tradizionali e degli standard legali

Le Motivazioni | 2/3

- La **digital forensics** getta effettivamente le basi, come disciplina, negli anni '80
 - *Principali motivazioni*
 - Maggiore accessibilità dei computer
 - Sia economica sia nell'usabilità
 - Prime interconnessioni tra computer mediante reti locali
 - *Problematiche*
 - Obsolescenza delle leggi tradizionali e degli standard legali



Le Motivazioni | 2/3

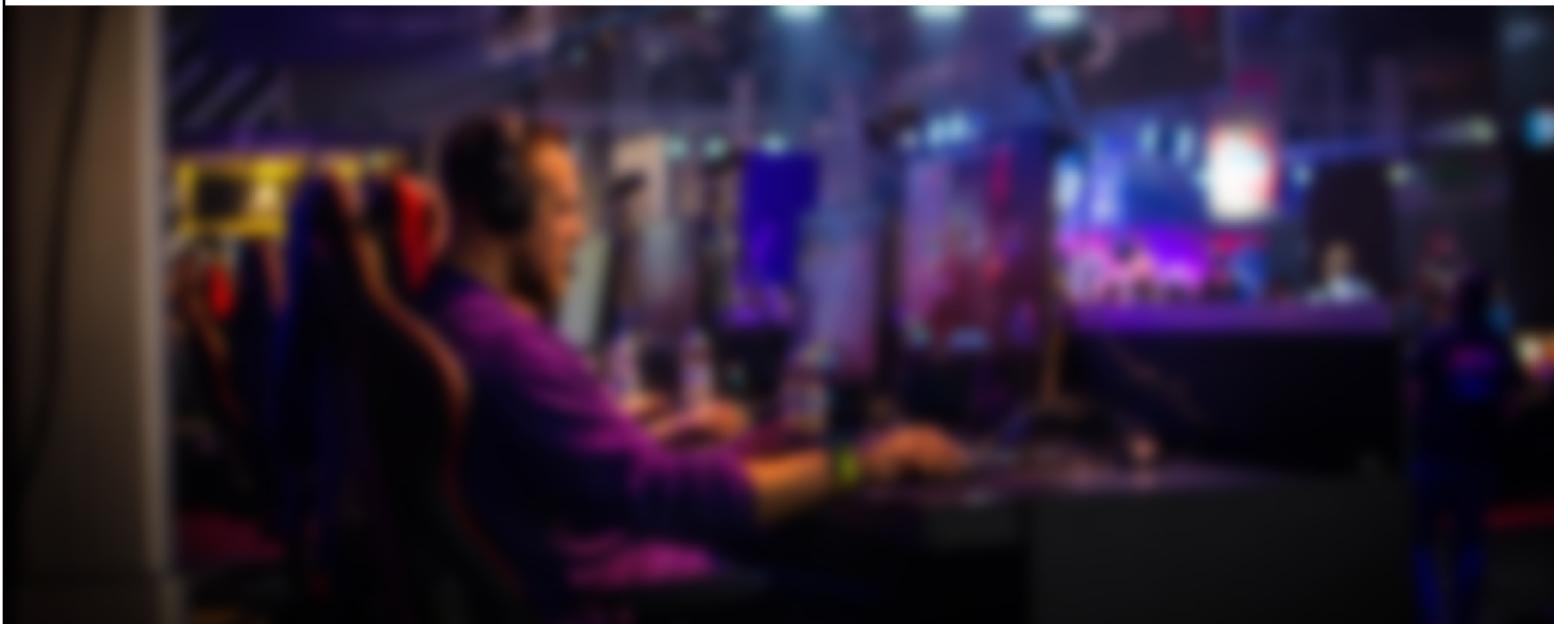
- **Esempi di Problematiche**

1. Il furto di un dispositivo informatico (computer, smartphone, ecc.) potrebbe essere confrontato con il furto di informazioni sensibili ottenute dal dispositivo stesso e utilizzate senza autorizzazione legale
2. Le informazioni possono rimanere sul dispositivo anche se ne è stata effettuata una copia (senza il permesso del proprietario)
 - In tal modo, il «ladro» assumerebbe permanente proprietà delle informazioni (anche se condivise con il proprietario)



Le Motivazioni | 3/3

- Le informazioni digitali sono memorizzate su dispositivi e possono essere sfruttate anche per attività non autorizzate
- I crimini informatici sono una versione «cibernetica» di crimini ben stabiliti nel mondo fisico



La Nascita | 1/2

- La nascita della **digital forensics** potrebbe risalire nell'anno 1984
- Un laboratorio dell'FBI ed altre agenzie di polizia, iniziarono a sviluppare software con l'obiettivo di esaminare le tracce informatiche

Curiosità

- Andrew Rosen ha scritto, per la Polizia Canadese, **il primo strumento, appositamente progettato, per l'investigazione forense digitale**
- Il tool era denominato *Desktop Mountie*

- In virtù dei crescenti attacchi a computer ed infrastrutture, varie organizzazioni hanno iniziato a realizzare e definire **politiche di sicurezza informatica e contromisure**
- Negli anni dal 1999 al 2007, vi sono state **notevoli evoluzioni** per quanto riguarda la **digital forensics**
 - Possibilità di individuare azioni del passato di un individuo, mediante tracce digitali, ad esempio:
 - File Cancellati
 - Note
 - E-Mail
 - Ecc.
 - La **digital forensics** era considerata principalmente una disciplina di nicchia
 - Al giorno d'oggi, invece, è oggetto di romanzi, fatti di cronaca, serie TV (es., C.S.I., ecc.)

Legislazione Italiana (*Cenni*)

Legislazione Italiana

Leggi e Best Practices | 1/18

Procedure per il trattamento delle **evidenze digitali, non regolamentate fino al 2008**

Legislazione Italiana

Leggi e Best Practices | 2/18

Procedure per il trattamento delle **evidenze digitali, non regolamentate fino al 2008**



Legge 18 marzo 2008, n. 48

Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla **criminalità informatica**, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (GU n. 80 del 4-4-2008 - Supplemento Ordinario n. 79)

Testo Completo: <http://www.parlamento.it/parlam/leggi/08048I.htm>

Legislazione Italiana

Leggi e Best Practices | 3/18



Legge 18 marzo 2008, n. 48

Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla **criminalità informatica**, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (GU n. 80 del 4-4-2008 - Supplemento Ordinario n. 79)

Testo Completo: <http://www.parlamento.it/parlam/leggi/08048I.htm>

Come indicato nel suddetto articolo, sono state inoltre apportate modifiche al **Codice Penale**, in merito alle evidenze digitali

Legislazione Italiana

Leggi e Best Practices | 4/18



Articolo 247 Codice di procedura penale (D.P.R. 22 settembre 1988, n. 447) Casi e forme delle perquisizioni

1-bis. Quando vi è fondato motivo di **ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico**, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, **adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.**

Legislazione Italiana

Leggi e Best Practices | 5/18



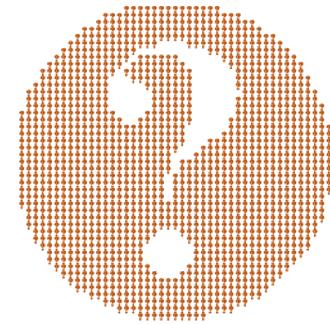
**Articolo 354 Codice di procedura penale
(D.P.R. 22 settembre 1988, n. 447)**

Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro

2. [parte omessa] In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità

Legislazione Italiana

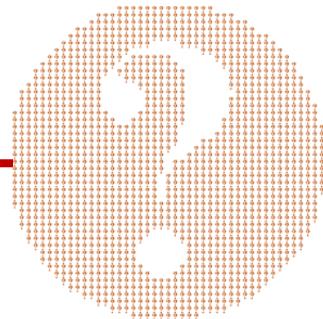
Leggi e Best Practices | 6/18



Legislazione Italiana

Leggi e Best Practices | 7/18

Quali sono le **caratteristiche** che devono avere le **misure tecniche**
(citeate negli articoli riportati nelle slide precedenti)

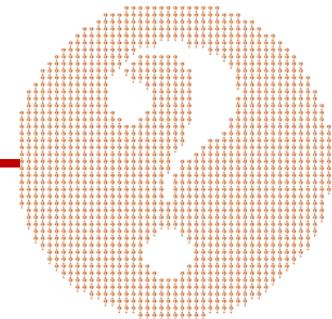


Legislazione Italiana

Leggi e Best Practices | 7/18

Quali sono le **caratteristiche** che devono avere le **misure tecniche**
(citeate negli articoli riportati nelle slide precedenti)

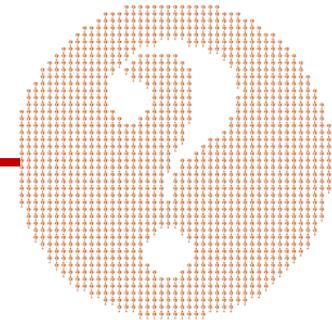
Nessun riferimento alla **metodologia** da adottare



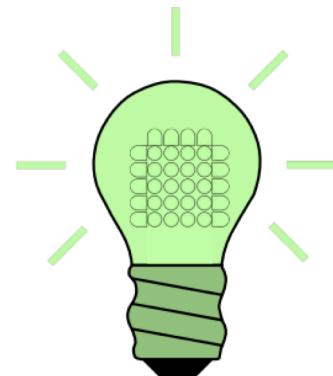
Legislazione Italiana

Leggi e Best Practices | 7/18

Quali sono le **caratteristiche** che devono avere le **misure tecniche**
(citate negli articoli riportati nelle slide precedenti)



Nessun riferimento alla **metodologia** da adottare



BEST PRACTICES

È saggio utilizzare le ***best practices***

Tecniche, metodologie, linee guida, ecc., raccolte dalle **esperienze più significative**, che si considera possano ottenere **risultati migliori**

Legislazione Italiana

Leggi e Best Practices | 8/18

Alcune Best Practices

- **Scientific Working Group on Digital Evidence (SWGDE)**
 - Best practices for Computer Forensics
 - Luglio 2006
 - www.swgde.org
- **RFC 3227, Guidelines for Evidence Collection and Archiving**
 - Febbraio 2002
- **UK Association of Chief Police Officers (ACPO)**
 - Good Practice Guide for Computer-Based Electronic Evidence, 2008
 - http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Legislazione Italiana

Leggi e Best Practices | 8/18

Alcune Best Practices

- **Scientific Working Group on Digital Evidence (SWGDE)**
 - Best practices for Computer Forensics
 - Luglio 2006
 - www.swgde.org
- **RFC 3227, Guidelines for Evidence Collection and Archiving**
 - Febbraio 2002
- **UK Association of Chief Police Officers (ACPO)**
 - Good Practice Guide for Computer-Based Electronic Evidence, 2008
 - http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Legislazione Italiana

Leggi e Best Practices | 9/18

Scientific Working Group on Digital Evidence (SWGDE)
Best practices for Computer Forensics
(Versione 1.0 novembre 2004, Versione 2.1 luglio 2006)

- 1.0 Seizing Evidence (*Presa in carico delle prove*)
 - 1.1 Evidence Handling
 - 1.1.1. Stand-alone computer (non-networked)
 - 1.1.2. Networked computer
 - 1.2 Servers
- 2.0 Equipment Preparation
- 3.0 Forensic Imaging
- 4.0 Forensic Analysis/Examination
 - 4.1 Forensic Analysis/Examination of Non-Traditional Computer Technologies
- 5.0 Documentation
- 6.0 Reports

Legislazione Italiana

Leggi e Best Practices | 10/18

Alcune Best Practices

- Scientific Working Group on Digital Evidence (SWGDE)
 - Best practices for Computer Forensics
 - Luglio 2006
 - www.swgde.org
- **RFC 3227, Guidelines for Evidence Collection and Archiving**
 - Febbraio 2002
- UK Association of Chief Police Officers (ACPO)
 - Good Practice Guide for Computer-Based Electronic Evidence, 2008
 - http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Legislazione Italiana

Leggi e Best Practices | 11/18

RFC 3227

Guidelines for Evidence Collection and Archiving

Pubblicata nel febbraio 2002, è ancora un *non smentito* punto di riferimento internazionale

Tra le altre cose consiglia:

- Documentare dettagliatamente ogni operazione svolta
- Chiari riferimenti temporali
- Indicazione di eventuali discrepanze
- Evitare tecniche invasive o limitare l'impatto all'irrinunciabile, preferendo strumenti ben documentabili
- Isolare il sistema da fattori esterni che possono modificarlo (attenzione: l'attività potrebbe essere rilevata)
- Nella scelta tra acquisizione e analisi, prima si acquisisce e poi si analizza
- Essere metodici e implementare automatismi (attenzione: arma a doppio taglio...)
- Procedere dalle fonti più volatili alle meno volatili
- Eseguire copie bit-level (bitstream image) e lavorare su esse

Legislazione Italiana

Leggi e Best Practices | 12/18

Alcune Best Practices

- Scientific Working Group on Digital Evidence (SWGDE)
 - Best practices for Computer Forensics
 - Luglio 2006
 - www.swgde.org
- RFC 3227, Guidelines for Evidence Collection and Archiving
 - Febbraio 2002
- **UK Association of Chief Police Officers (ACPO)**
 - Good Practice Guide for Computer-Based Electronic Evidence, 2008
 - http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Legislazione Italiana

Leggi e Best Practices | 13/18

UK Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence

Definizione di Quattro Principi | 1/2

- **Principio 1**
 - Nessuna azione intrapresa dalle forze dell'ordine o dai loro agenti dovrebbe modificare i dati conservati su un dispositivo digitale o supporti di memorizzazione che possono essere successivamente utilizzati in tribunale
- **Principio 2**
 - Nelle circostanze in cui una persona ritiene necessario accedere ai dati originali conservati su un dispositivo digitale o su supporti di memorizzazione, tale persona deve essere competente a farlo ed essere in grado di fornire prove che spieghino la rilevanza e le implicazioni delle proprie azioni

Legislazione Italiana

Leggi e Best Practices | 14/18

UK Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence

Definizione di Quattro Principi | 2/2

- **Principio 3**

- Dovrebbe essere creata e conservata una traccia documentativa o una registrazione di tutti i processi applicati alla prova elettronica basata su dispositivi digitali.
- Una terza parte indipendente dovrebbe essere in grado di esaminare tali processi e ottenere lo stesso risultato

- **Principio 4**

- Il responsabile dell'indagine (il funzionario) ha la responsabilità generale di assicurare che la legge e questi principi siano rispettati

Legislazione Italiana

Leggi e Best Practices | 15/18

Altre Best Practices

- **U.S. Department of Homeland Security**
 - Best Practices for Seizing Electronic Evidence v. 3
 - <http://www.forwardedge2.com/pdf/bestpractices.pdf>
- **US Department of Justice, National Institute of Justice**
 - Investigations Involving the Internet and Computer Networks (gennaio 2007)
 - <https://www.ncjrs.gov/pdffiles1/nij/210798.pdf>
 - Investigative Uses of Technology: Devices, Tools, and Techniques (ottobre 2007)
 - <http://www.ncjrs.gov/pdffiles1/nij/213030.pdf>
 - Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition” (aprile 2008)
 - <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>

Legislazione Italiana

Wokflow della Digital Forensics | 16/18



Legislazione Italiana

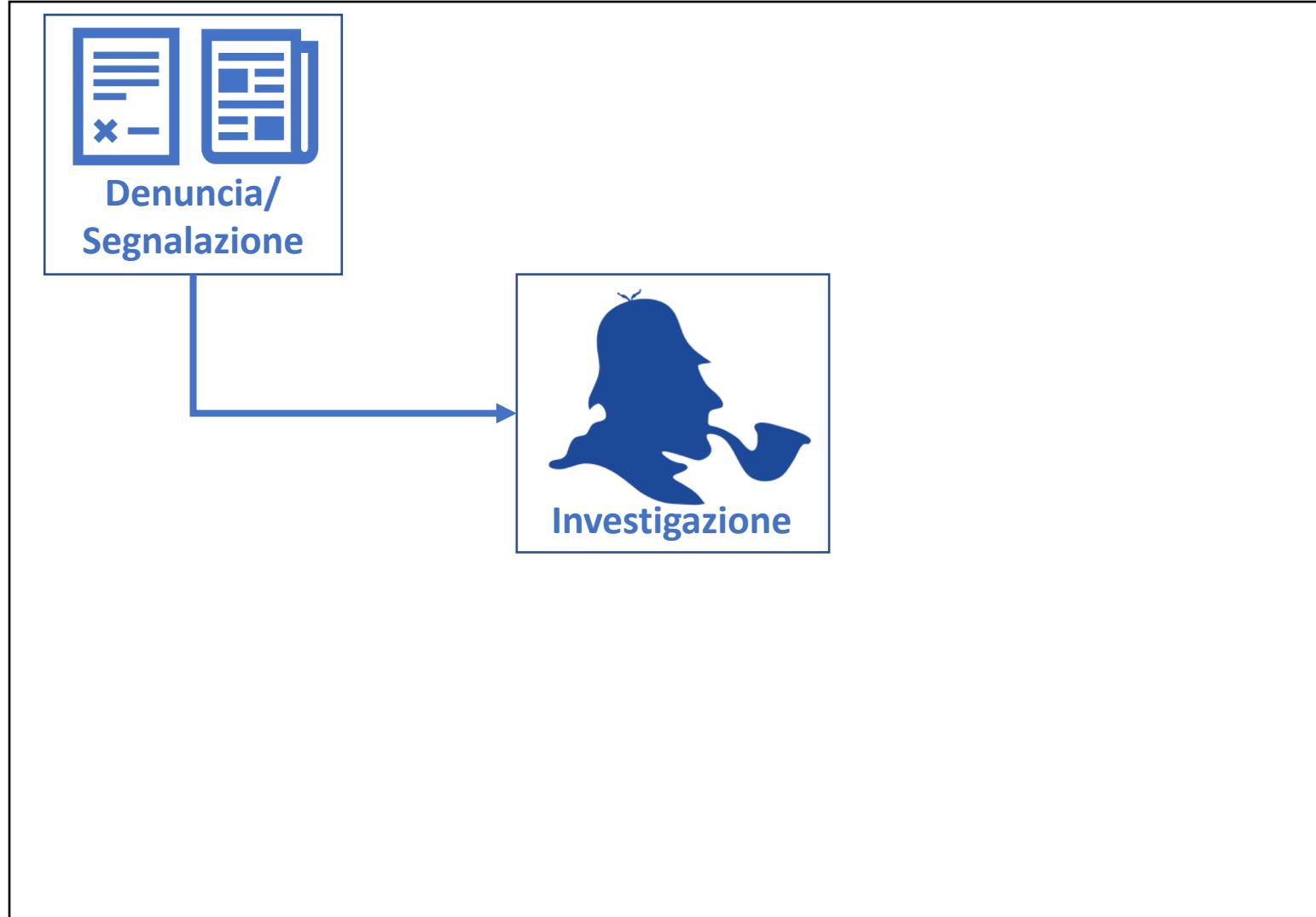
Workflow della Digital Forensics | 16/18



L'innesto del workflow è la
denuncia o segnalazione di
un'attività illecita

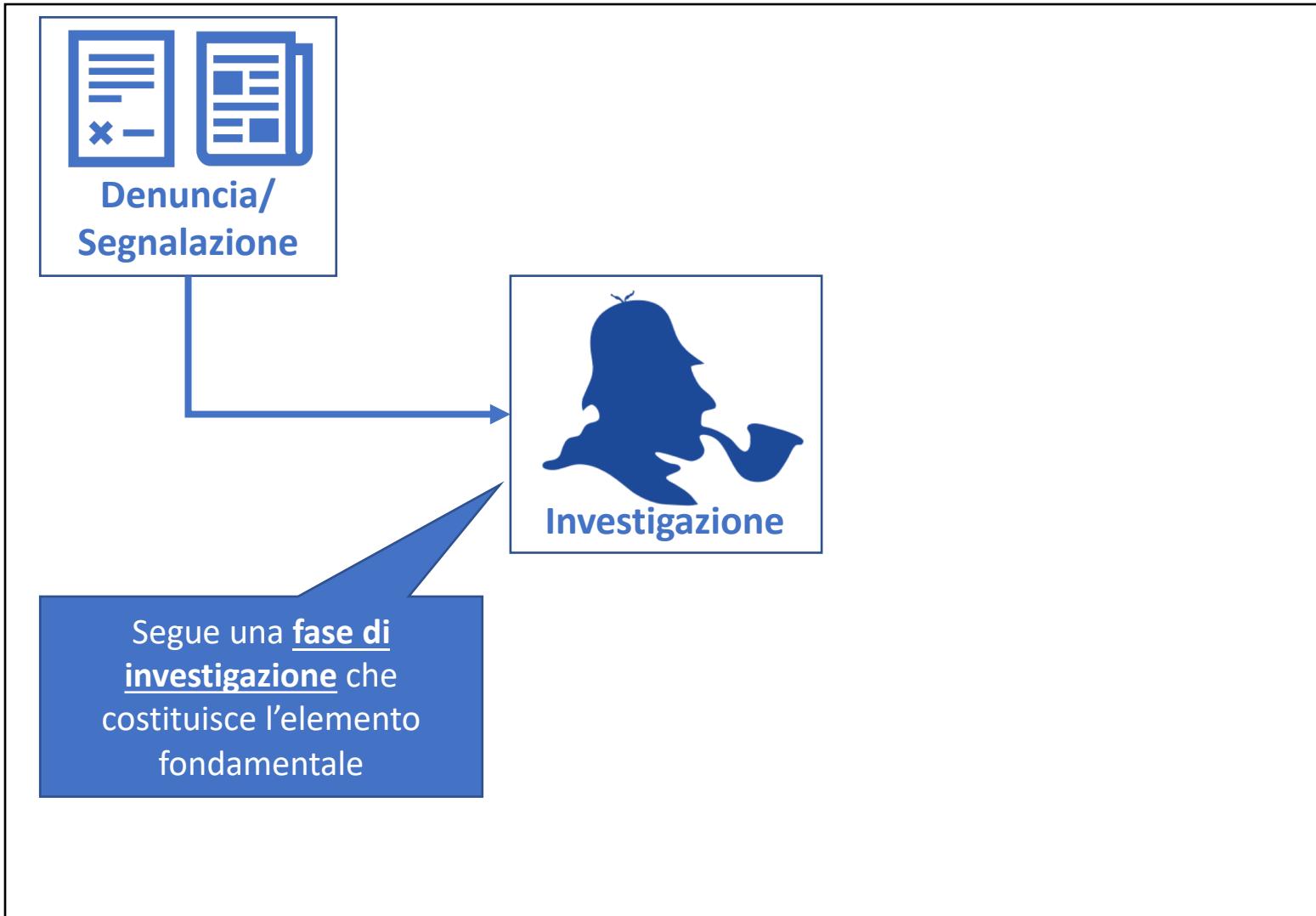
Legislazione Italiana

Wokflow della Digital Forensics | 17/18



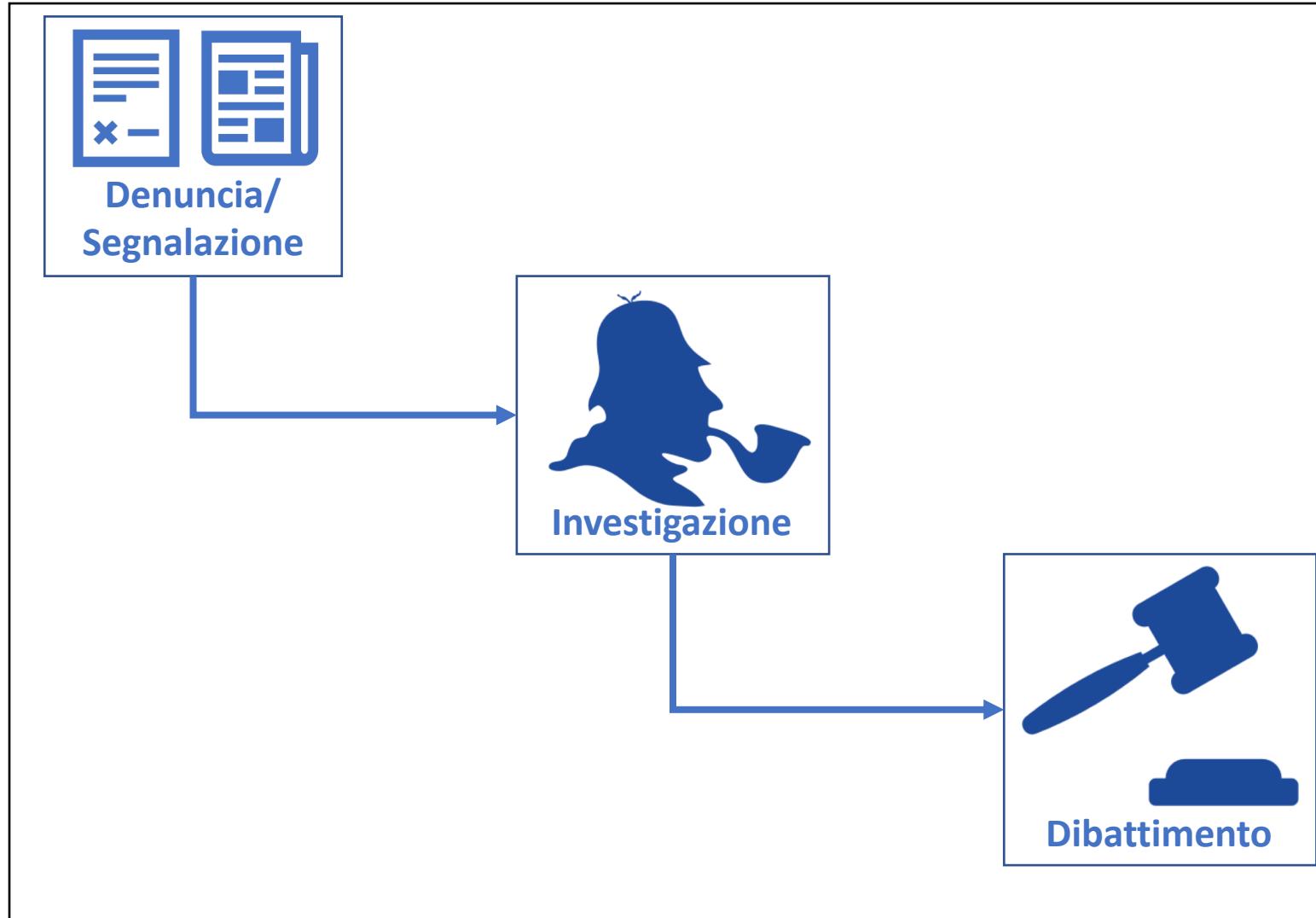
Legislazione Italiana

Wokflow della Digital Forensics | 17/18



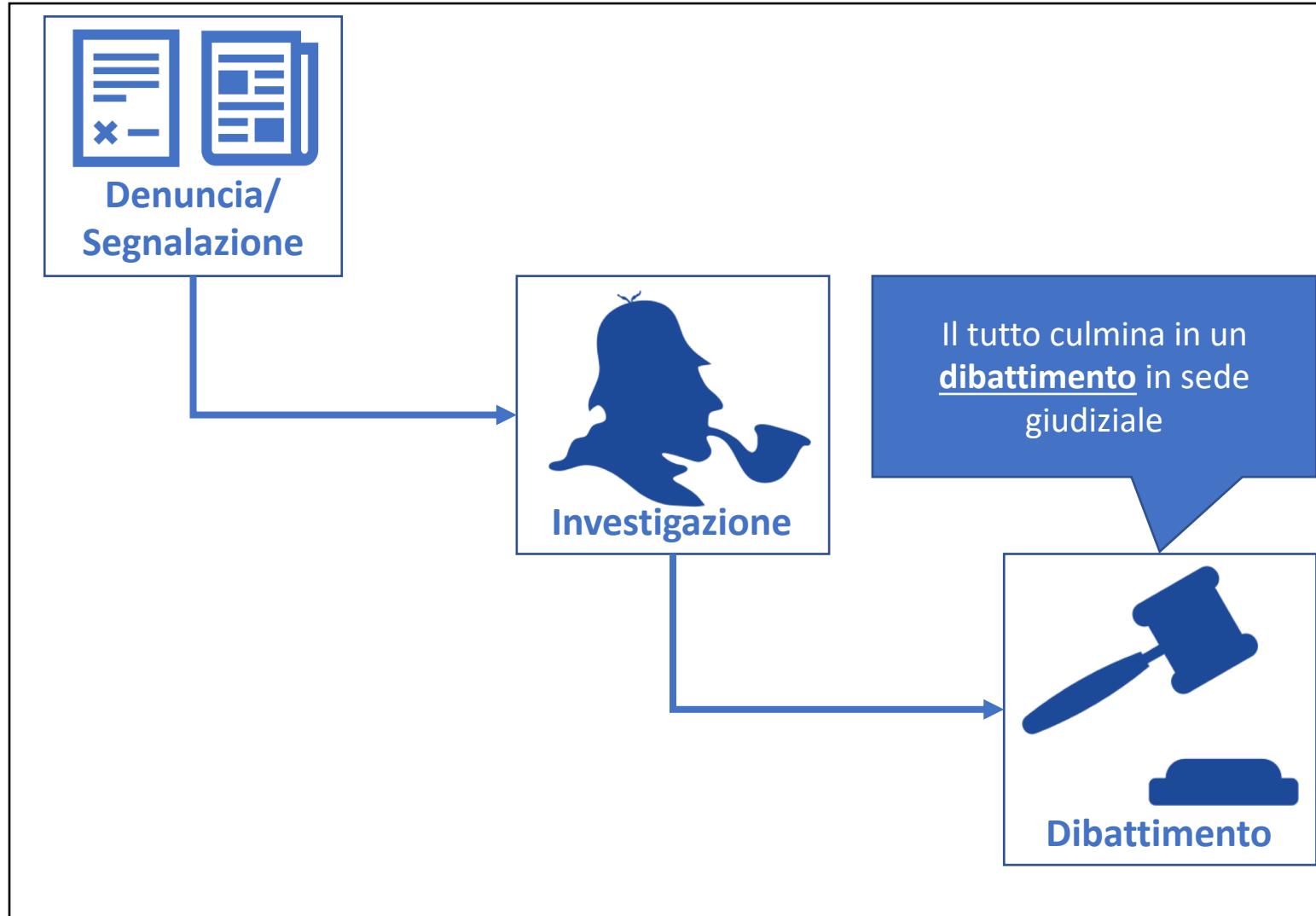
Legislazione Italiana

Wokflow della Digital Forensics | 18/18



Legislazione Italiana

Wokflow della Digital Forensics | 18/18



Fasi Principali dell'Investigazione

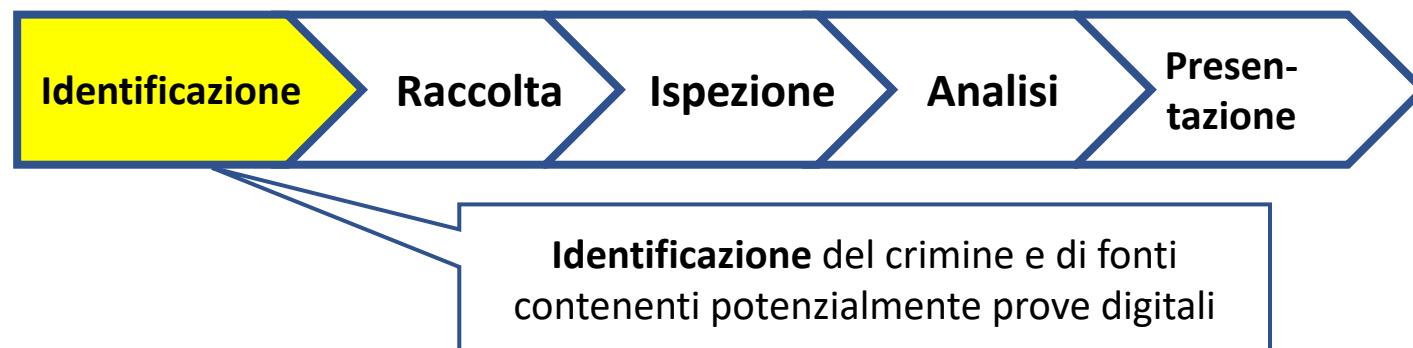
Fasi Principali

- Il processo di investigazione è articolato in cinque fasi principali consecutive:
 - Identificazione
 - Raccolta (o Acquisizione)
 - Ispezione
 - Analisi
 - Presentazione
- Fasi principali del processo di investigazione



Fasi Principali

- Il processo di investigazione è articolato in cinque fasi principali consecutive:
 - Identificazione
 - Raccolta (o Acquisizione)
 - Ispezione
 - Analisi
 - Presentazione
- Fasi principali del processo di investigazione



Fasi Principali

- Il processo di investigazione è articolato in cinque fasi principali consecutive:
 - Identificazione
 - Raccolta (o Acquisizione)
 - Ispezione
 - Analisi
 - Presentazione
- Fasi principali del processo di investigazione



Raccolta (o acquisizione) di dati *raw* («grezzi»), copiandoli, in maniera opportuna, dai dispositivi digitali

Fasi Principali

- Il processo di investigazione è articolato in cinque fasi principali consecutive:
 - Identificazione
 - Raccolta (o Acquisizione)
 - Ispezione
 - Analisi
 - Presentazione
- Fasi principali del processo di investigazione



Ispezione (examination) dei dati raccolti con l'obiettivo di realizzarne una struttura migliore ai fini dell'analisi e della comprensione

Fasi Principali

- Il processo di investigazione è articolato in cinque fasi principali consecutive:
 - Identificazione
 - Raccolta (o Acquisizione)
 - Ispezione
 - Analisi
 - Presentazione
- Fasi principali del processo di investigazione



Nella fase di **analisi**, si cerca di ottenere una migliore comprensione e si cerca di determinare i fatti di un evento o un'azione illegale

Fasi Principali

- Il processo di investigazione è articolato in cinque fasi principali consecutive:
 - Identificazione
 - Raccolta (o Acquisizione)
 - Ispezione
 - Analisi
 - Presentazione
- Fasi principali del processo di investigazione



Le prove digitali, individuate nelle fasi precedenti, vengono adeguatamente **presentate** nei tribunali e/o negli enti preposti

Fasi Principali

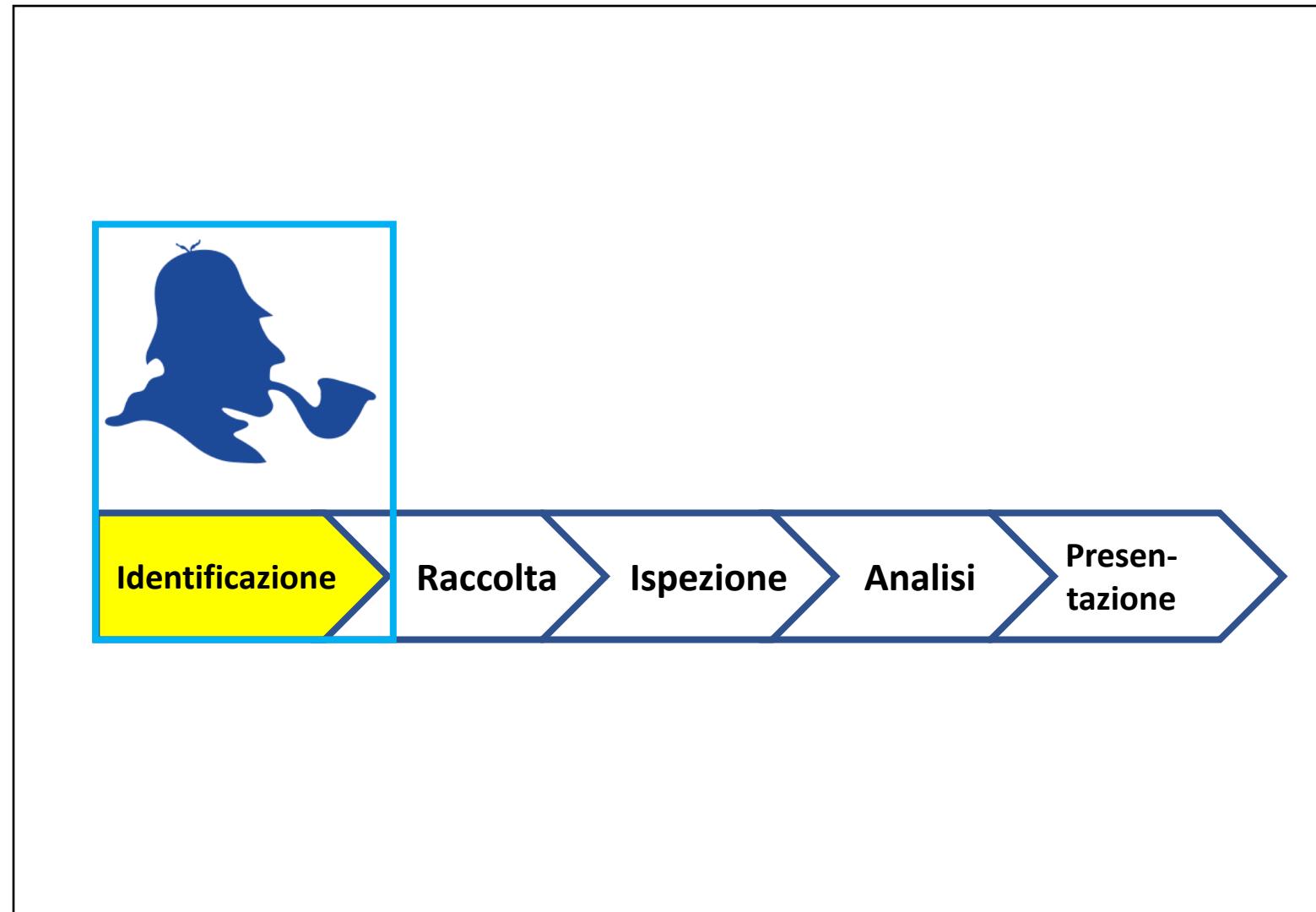
- Il processo di investigazione è articolato in cinque fasi principali consecutive:
 - Identificazione
 - Raccolta (o Acquisizione)
 - Ispezione
 - Analisi
 - Presentazione
- Fasi principali del processo di investigazione



OSSERVAZIONE

Durante il processo di investigazione forense, possono esservi diverse iterazioni di una o più fasi

Fasi Principali





Identificazione | 1/9

- Un crimine può essere identificato, basandosi su:
 - Segnalazioni/Reclami
 - Denunce
 - Allarmi
 - Indicazioni
 - Ecc.

Nella fase di **identificazione** si ha il compito di **rilevare, riconoscere e determinare** l'evento o il crimine da **investigare**

DEFINIZIONE



Identificazione | 2/9

- L'identificazione è una fase estremamente importante, poiché vengono **identificate informazioni o fonti di informazioni**
- Si identificano quindi anche i **dispositivi informatici** che potrebbero contenere **prove digitali**, ad esempio:
 - Computer desktop
 - Laptop/Notebook/PC 2-in-1
 - Tablet
 - Supporti di memorizzazione rimovibili
 - Penne USB, CD/DVD, ecc.
 - Supporti di memorizzazione non rimovibili
 - Dischi fissi interni, ecc.



Identificazione | 2/9

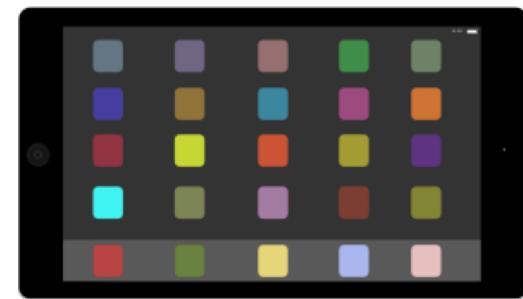
- L'identificazione è una fase estremamente importante, poiché vengono **identificate informazioni o fonti di informazioni**
- Si identificano quindi anche i **dispositivi informatici** che potrebbero contenere **prove digitali**, ad esempio:
 - Computer desktop
 - Laptop/Notebook/PC 2-in-1
 - Tablet
 - Supporti di memorizzazione rimovibili
 - Penne USB, CD/DVD, ecc.
 - Supporti di memorizzazione non rimovibili
 - Dischi fissi interni, ecc.
- **OSSERVAZIONE IMPORTANTE:** Le fonti di prove digitali NON sono sempre facili da identificare!



Identificazione Raccolta Ispezione Analisi Presen-
tazione

Identificazione | 2/9

Identificazione di Fonti con Potenziali Prove Digitali





Identificazione | 3/9

- Una corretta **pianificazione** e **preparazione** delle attività è una precondizione per una investigazione *efficace* ed *efficiente*
- La scelta degli strumenti e delle tecnologie da impiegare è strettamente dipendente dalla disponibilità di risorse, ecc.
 - La **solidità legale** dei suddetti strumenti deve essere **preventivamente valutata**, in quanto essi devono supportare i principi di **integrità**
- Nelle scene in cui sono **presenti dispositivi informatici**, è necessario effettuare una **fase di preparazione**, in cui si configurano adeguatamente **hardware** e **software** specifici per **l'analisi forense**



Identificazione | 4/9

First Responder | 1/2

- Nel momento in cui viene scoperto o sospettato un crimine, dovrebbe esserci un ***first responder*** (letteralmente, *primo soccorritore*), il quale deve allertare gli investigatori forensi e convocarli sulla scena del crimine
- In generale, il primo soccorritore ha competenze/conoscenze in relazione alle infrastrutture informatiche (reti, sistemi operativi, ecc.)
- Fra i primi soccorritori possiamo individuare
 - **Amministratori di Sistema**
 - **Amministratori di Rete**
 - **Amministratori/Responsabili della Sicurezza Informatica**
 - **Manager IT**



Identificazione | 4/9

First Responder | 2/2

- Anche se il primo soccorritore non dovesse avere competenze sufficienti, nell'ambito della digital forensics, dovrà comunque mettere in sicurezza i dati, le periferiche, i supporti di memorizzazioni, ecc., in modo che essi **non vengano utilizzati, alterati, rimossi da soggetti non autorizzati**
- Fra i doveri del primo soccorritore troviamo:
 - Effettuare le **prime valutazioni**
 - **Documentare la scena e la stanza integralmente:** il centro della stanza diviene il punto focale della descrizione
 - **Assicurare la scena da soggetti non autorizzati**
 - **Preservare e/o impacchettare le tracce per il trasporto**



Identificazione | 5/9

Documentazione e Preservazione delle Prove | 1/3

- La **documentazione della scena** dovrebbe essere effettuata dal primo soccorritore, al fine di **fornire maggiore supporto agli investigatori**
- La documentazione dovrebbe includere **fotografie, video, registrazioni audio** dei seguenti oggetti:
 - **Stanza** dove è allocato il dispositivo
 - Scrivania, entrata/uscita, finestre, prese elettriche, ecc.
 - **Stato del dispositivo**
 - Acceso/spento/luce di accensione lampeggiante
 - **Contenuto dello schermo** (se il device è avviato)
 - **Libri, annotazioni, pezzi di carta**
 - **Cavi connessi e cavi non connessi**



Identificazione | 5/9

Documentazione e Preservazione delle Prove | 2/3

- Il primo soccorritore dovrebbe avere con sé **diversi strumenti al fine di svolgere adeguatamente la documentazione e la preservazione delle stesse:**
 - Vestiti e occhiali protettivi
 - Braccialetti anti-statici
 - Etichette, adesivi, ecc.
 - Torce e lenti di ingrandimento
 - Contenitori, scatole, materiale per l'imballaggio, ecc.





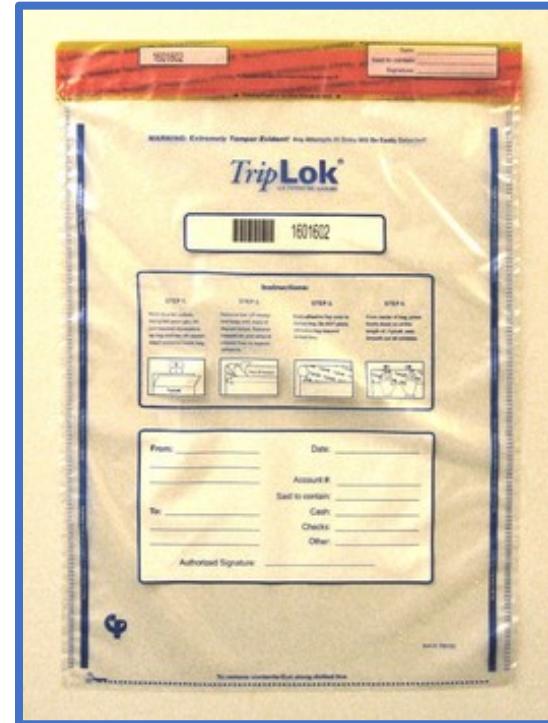
Identificazione | 5/9

Documentazione e Preservazione delle Prove | 3/3



Fonte:

https://en.wikipedia.org/wiki/Security_bag#/media/File:Mobiles.JPG



Fonte:

https://en.wikipedia.org/wiki/Security_bag#/media/File:Tamper_evident_currency_bag.jpg



Identificazione | 6/9

Live Systems

Denotiamo con *live system* un **sistema in fase di attività** che potenzialmente detiene prove, le quali sarebbero difficili da acquisire o potrebbero essere perse nel caso in cui il sistema venga spento

Dead Systems

Denotiamo con *dead system* un **sistema NON in fase di attività**; In tali sistemi, tutti i dati temporanei (memoria RAM, cache, ecc.) sono tipicamente persi



Identificazione | 6/9

Live Systems

Denotiamo con *live system* un **sistema in fase di attività** che potenzialmente detiene prove, le quali sarebbero difficili da acquisire o potrebbero essere perse nel caso in cui il sistema venga spento

Dead Systems

Denotiamo con *dead system* un **sistema NON in fase di attività**; In tali sistemi, tutti i dati temporanei (memoria RAM, cache, ecc.) sono tipicamente persi

Post Mortem Analysis e Live Analysis

L'analisi dei *dead systems* è denotata come **analisi post mortem (post mortem analysis)**, mentre l'analisi dei *live systems* è denotata come **live analysis**



Identificazione | 7/9

Live Systems | Caratteristiche | 1/2

- Per quanto riguarda i ***live system*** (**sistemi «attivi»**), è necessario prestare particolare attenzione a causa della **volatilità dei dati**
- In generale, è necessario ricordare che **fasi reboot** o **spegnimento** di un sistema, possono portare alla **sovrascrittura di dati** su un supporto di memorizzazione (ad esempio, un hard disk), perdita dei dati contenuti nella **memoria RAM** e perdita del **file di paging**
 - **IMPORTANTE:** Il **file di paging** è un file molto **importante** dal punto di vista della digital forensics (*maggiori dettagli nelle prossime slide*)



Identificazione | 7/9

Live Systems | Precauzioni | 2/2

- Alcune precauzioni da prendere quando si lavora con i live system:
 - **Muovere il mouse** o **spostare leggermente le dita sul touchpad** (nel caso di un notebook), per verificare se il **device** è in stato di **stand-by o in sospensione**
 - **OSSERVAZIONE:** Non si deve cliccare sui tasti del mouse (o touchpad), per evitare che si avviano programmi o si eseguano inavvertitamente operazioni
 - **Fotografare e registrare lo schermo del dispositivo**, considerando tutti i programmi visibili, data, ora e gli oggetti sul desktop
 - **Staccare la spina** su PC desktop o **rimuovere** (in caso di notebook e se possibile) **la batteria**
- È anche importante acquisire i dati contenuti nella RAM (*approfondimento nelle prossime lezioni*) e nel file di paging, cercando di effettuare il minor numero possibile di modifiche dei dati



Identificazione | 7/9

Dead Systems | Caratteristiche

- I ***dead system*** (*sistemi «inattivi» o «spenti»*) non dovrebbero mai essere riaccessi, se non da parte di un investigatore forense
- È necessario adottare **attenzioni particolari** al fine di garantire che i dati esistenti non vengano cancellati e che non vi sia sovrascrittura dei dati
 - È inoltre importante accertarsi che il sistema sia effettivamente spento e non sia in stato di stand-by/sospensione/ibernazione
- È comunque consigliato fotografare lo schermo e le porte del PC



Identificazione | 8/9

Importanza del File di Paging | 1/3

- I sistemi operativi hanno la possibilità di utilizzare una porzione del disco fisso come una estensione della memoria RAM: la **memoria virtuale** (o **virtual memory**)



Identificazione

Raccolta

Ispezione

Analisi

Presen-tazione

Identificazione | 8/9

Importanza del File di Paging | 1/3

- I sistemi operativi hanno la possibilità di utilizzare una porzione del disco fisso come una estensione della memoria RAM: la **memoria virtuale** (o **virtual memory**)

OSSERVAZIONE

Il disco fisso è certamente più lento, per quanto riguarda gli accessi (lettura/scrittura), rispetto alla memoria RAM

Tuttavia, in sistemi con **memoria RAM limitata** (ad esempio, notebook, ecc.), è **importante utilizzare la memoria virtuale** (tipicamente, memorizzata in un file speciale, detto **file di paging** o **file di swap**), in modo che al suo interno possano essere **memorizzati dati e processi** che vengono utilizzati di meno rispetto ad altri (lasciando così **più spazio nella memoria RAM**)



Identificazione | 8/9

Importanza del File di Paging | 1/3

- Come accennato precedentemente, nelle indagini forensi, il file di paging è molto importante
- Tale file **non è volatile quanto la memoria RAM**, proprio perché esso è memorizzato sul disco fisso
 - Nei sistemi operativi Microsoft Windows, si utilizza un file nascosto denominato *pagefile.sys*



Identificazione | 8/9

Importanza del File di Paging | 2/3

- Il file di paging dovrebbe essere sempre ispezionato, utilizzando appositi strumenti, poiché, poiché **potrebbe rivelare utilissime informazioni**
 - *Esempio*
 - Password
 - Informazioni sui siti visitati
 - Documenti aperti
 - Documenti stampati
 - Ecc.



Identificazione | 8/9

Importanza del File di Paging | 3/3

- I **dati** sulle unità meccaniche (come i dischi fissi) sono tipicamente **memorizzati in maniera frammentata**
- Il vantaggio del **file di paging** è che i suoi **dati** vengono tipicamente allocati in maniera contigua
MOTIVAZIONE: Fornire un **accesso più veloce** possibile ad essi
- Inoltre, è consigliabile sempre avere un file di paging di dimensioni pari a circa **una volta e mezzo** la dimensione totale della memoria RAM dell'elaboratore



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 1/5

- Procedura necessaria per poter tracciare lo stato di una prova (una volta identificata) e la relativa responsabilità in qualsiasi momento della sua esistenza
- Deve documentare chiaramente, in relazione alla prova:
 - Dove, quando e da chi è stata scoperta e acquisita
 - Dove, quando e da chi è stata custodita o analizzata
 - Chi l'ha avuta in custodia e in quale periodo
 - Come è stata conservata
 - Ad ogni passaggio di consegna, deve essere specificato dove, come e tra chi è stata trasferita (da qui, ***chain of custody*** o ***catena di custodia*** o, abbreviato, **CoC**)
- Gli accessi alla prova devono essere estremamente ristretti e chiaramente documentati



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 2/5

- Alcune informazioni contenute nella *chain of custody*:
 - Numero del caso
 - Azienda incaricata dell'investigazione
 - Investigatore assegnato al caso
 - Natura e breve descrizione del caso
 - Investigatore incaricato della duplicazione dei dati
 - Data e ora di inizio custodia
 - Luogo di rinvenimento del supporto
 - Produttore del supporto
 - Modello del supporto
 - Numero di serie del supporto



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 3/5

- Ogni volta che la prova è affidata ad un nuovo investigatore, nel documento bisogna aggiungere:
 - Nome dell'incaricato all'analisi
 - Data e ora di presa in carico del supporto
 - Data e ora di restituzione del supporto
- Tipicamente, la CoC è stampata direttamente sul contenitore della prova oppure è stampata su un'etichetta, la quale va allegata o attaccata al contenitore della prova



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 4/5

EVIDENCE			
Sottoposta dall'Ente/Autorità			
Data e Ora dell'Acquisizione			
Numero del Referto		Numero del Caso	
Acquisita Da			
Descrizione			
Luogo Acquisizione			
Tipo di Reato			
CHAIN OF CUSTODY			
Ceduta Da		Presa in Custodia Da	
Data e Ora			
Ceduta Da		Presa in Custodia Da	
Data e Ora			
Ceduta Da		Presa in Custodia Da	
Data e Ora			

Esempio di una CoC [NOTA: Adattamento da una CoC reale]



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 5/5

Esempio di Utilizzo

CHAIN OF CUSTODY			
Ceduta Da		Presa in Custodia Da	
Data e Ora			
Ceduta Da		Presa in Custodia Da	
Data e Ora			
Ceduta Da		Presa in Custodia Da	
Data e Ora			

Esempio di una Chain of Custody, relativa ad una certa evidenza, custodita inizialmente da Mario



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 5/5

Esempio di Utilizzo

CHAIN OF CUSTODY			
Ceduta Da	Mario	Presa in Custodia Da	Raffaele
Data e Ora	02/01/2019, 20:45		
Ceduta Da		Presa in Custodia Da	
Data e Ora			
Ceduta Da		Presa in Custodia Da	
Data e Ora			

I

I Passaggio di Custodia

Esempio di una Chain of Custody, relativa ad una certa evidenza, custodita inizialmente da *Mario*



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 5/5

Esempio di Utilizzo

CHAIN OF CUSTODY			
Ceduta Da	Mario	Presa in Custodia Da	Raffaele
Data e Ora	02/01/2019, 20:45		
Ceduta Da	Raffaele	Presa in Custodia Da	Antonio
Data e Ora	05/01/2019, 18:30		
Ceduta Da		Presa in Custodia Da	
Data e Ora			

Il Passaggio di Custodia

Esempio di una Chain of Custody, relativa ad una certa evidenza, custodita inizialmente da *Mario*



Identificazione | 9/9

Chain of Custody (*Catena di Custodia*) | 5/5

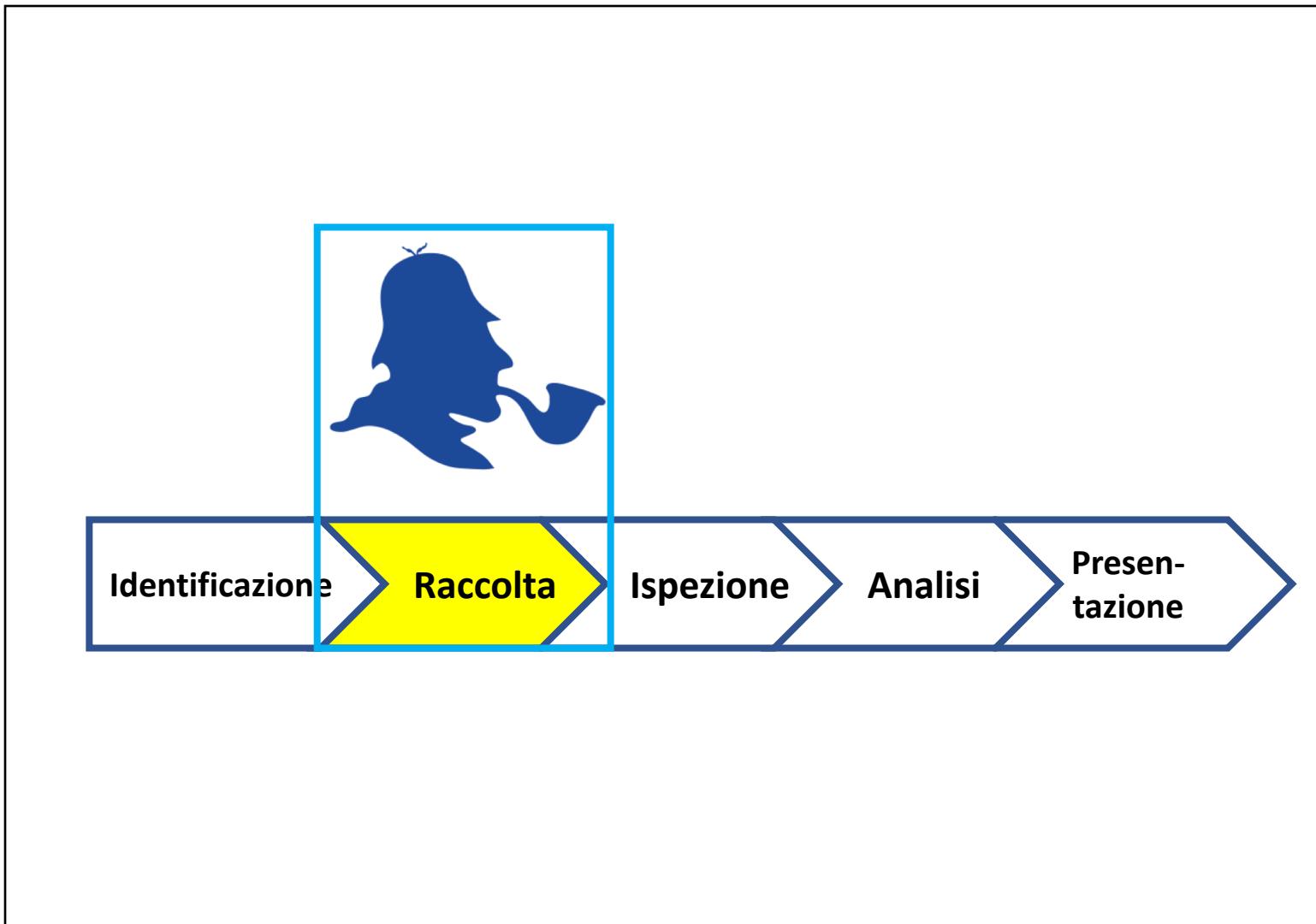
Esempio di Utilizzo

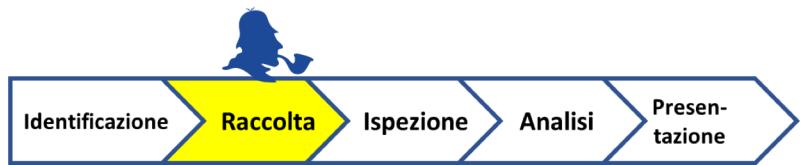
CHAIN OF CUSTODY			
Ceduta Da	Mario	Presa in Custodia Da	Raffaele
Data e Ora	02/01/2019, 20:45		
Ceduta Da	Raffaele	Presa in Custodia Da	Antonio
Data e Ora	05/01/2019, 18:30		
Ceduta Da	Antonio	Presa in Custodia Da	Giorgio
Data e Ora	07/01/2019, 10:15		

I
III Passaggio di Custodia

Esempio di una Chain of Custody, relativa ad una certa evidenza, custodita inizialmente da *Mario*

Fasi Principali





Raccolta | 1/11

- La fase di raccolta è riferita all'**acquisizione** e/o **copia** di dati digitali
- L'investigatore accede al dispositivo informatico, identificato come *rilevante* (nella fase di *identificazione*), contenente appunto i dati digitali utili per l'indagine
- Al fine di evitare eventuali compromissioni dei dati originali e, conseguentemente, compromettere le prove, è necessario lavorare su delle copie «esatte» dei dati (*maggiori dettagli in seguito*)

DEFINIZIONE

La fase di **raccolta** (o **acquisizione**) consiste nella copia di dati digitali, utilizzando appropriati ed adeguati strumenti e tecniche forensi



Raccolta | 3/11

Alcune Fonti di Prove Digitali



Hard Disk e Solid State Disk (SSD)



Memoria RAM



Infrastrutture di Rete



Identificazione **Raccolta** Ispezione Analisi Presen-
tazione

Raccolta | 3/11

Alcune Fonti di Prove Digitali

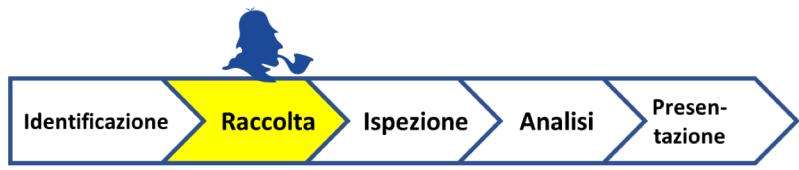


Hard Disk e Solid State Disk (SSD)

Memoria RAM



Infrastrutture di Rete



Raccolta | 3/11

- I dispositivi principali dove vengono memorizzate le informazioni sono i **dischi rigidi** (detti anche **Hard Disk Drive – HDD – o hard disk**)
- I dischi rigidi si sono iniziati a diffondere a partire dagli anni '50 ed è essenzialmente la **forma predominante di archiviazione digitale**
- Questo tipo di supporto è utile per individuare le prove, poiché i dati non sono convenienti da **eliminare definitivamente**
- Negli ultimi anni, tuttavia, si sono diffusi sempre più i **dischi a stato solido** (detti anche **Solid State Disk – SSD**)



Identificazione

Raccolta

Ispezione

Analisi

Presen-
tazione

Raccolta | 4/11

- Gli SSD sono più veloci ed hanno una logica di funzionamento generalmente complessa
- Gli SSD memorizzano tipicamente i dati in blocchi, suddivisi in «pagine» composte da grandi array di transistor, detti **Negative AND (NAND)**
- A causa della loro natura, gli SSD svolgono delle operazioni di pulizia «automatica», al fine di mantenere veloci gli SSD stessi e allungarne la vita
 - Ciò comporta, però, possibili difficoltà nel reperimento di tracce digitali



Identificazione **Raccolta** Ispezione Analisi Presen-
tazione

Raccolta | 3/11

Alcune Fonti di Prove Digitali



Hard Disk e Solid State Disk (SSD)

Memoria RAM



Infrastrutture di Rete



Identificazione

Raccolta

Ispezione

Analisi

Presen-
tazione

Raccolta | 5/11

- All'interno della memoria centrale (o **Random Access Memory – RAM**) vengono memorizzati, in binario, dati ed istruzioni
- Le istruzioni sono elaborate dalla **Central Processing Unit (CPU)**
- La RAM è una **memoria volatile**
- Fare una «istantanea» (***dump***) la RAM può essere importante, in quanto la RAM fornisce dettagli sull'uso più recente dell'elaboratore:
 - Processi
 - Alcune attività della tastiera
 - Ecc.
- Tuttavia, in alcuni casi, realizzare un *dump* della RAM può essere controproducente, in quanto può **contaminare il sistema**



Raccolta | 3/11

Alcune Fonti di Prove Digitali



Hard Disk e Solid State Disk (SSD)



Memoria RAM



Infrastrutture di Rete



Identificazione

Raccolta

Ispezione

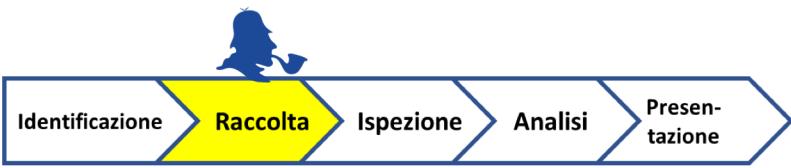
Analisi

Presen-
tazione

Raccolta | 6/11

- Qualora i dati dovessero essere memorizzati su server di **rete** (o altri apparati **interconnessi in rete**), l'accesso può essere fornito collegando un dispositivo alla medesima rete, specificando eventuali dettagli sull'autenticazione
- Tuttavia, in diversi casi, è preferibile creare «copie esatte» del server di rete invece di recuperare i dati tramite l'accesso (logico) al sistema operativo del server

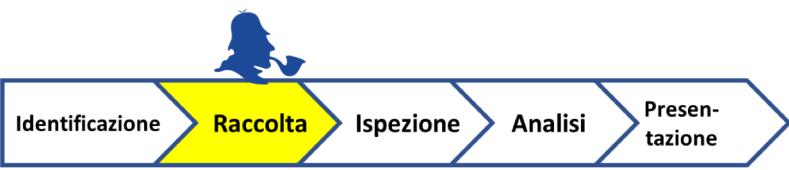




Raccolta | 7/11

Altre Fonti di Prove Digitali

- Central Processing Unit (CPU)
- Graphic Processing Unit (GPU)
- Dispositivi di memorizzazioni rimovibili
 - Pennette USB
 - DVD/CD/Blue-Ray
- Webcam
- Ecc.



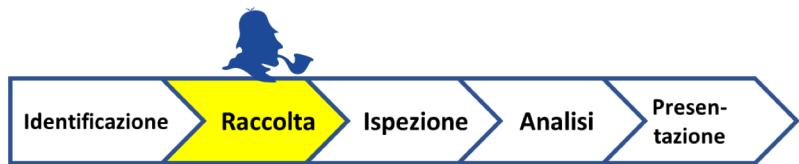
Raccolta | 7/11

Altre Fonti di Prove Digitali

- **Central Processing Unit (CPU)**
- **Graphic Processing Unit (GPU)**
- Dispositivi di memorizzazioni rimovibili
 - Pennette USB
 - DVD/CD/Blue-Ray
- Webcam
- Ecc.

OSSERVAZIONE

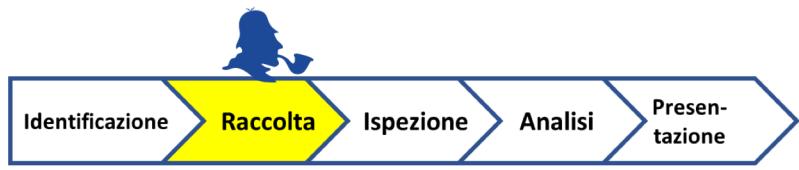
CPU e GPU potrebbero contenere informazioni memorizzate
all'interno delle rispettive cache



Raccolta | 8/11

Problemi relativi alle Fonti di Prove Digitali | 1/3

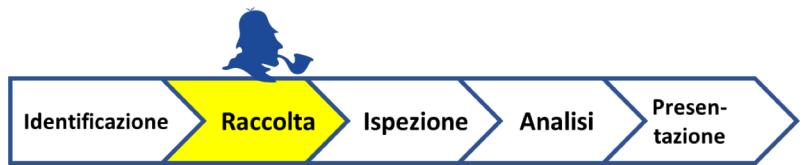
- I dati e/o i dispositivi hardware potrebbe essere alterati o danneggiati, in maniera:
 - Intenzionale
 - Al fine di rendere difficile l'acquisizione agli investigatori
 - Non intenzionale
 - Guasti meccanici (dovuti ad acqua, polvere, piccoli incendi, ecc.)
- Talvolta, quindi, vi è quindi necessità di ricostruire dati appunto da hardware/dati danneggiati



Raccolta | 8/11

Problemi relativi alle Fonti di Prove Digitali | 2/3

- È importante sottolineare che vi sono **più minacce per i dati digitali**, rispetto ai cosiddetti dati «cartacei»



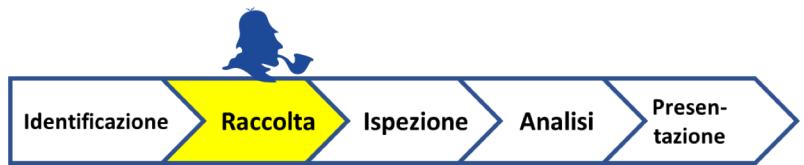
Raccolta | 8/11

Problemi relativi alle Fonti di Prove Digitali | 2/3

- È importante sottolineare che vi sono **più minacce per i dati digitali**, rispetto ai cosiddetti dati «cartacei»

Alcune Minacce per i dati «cartacei»

- Acqua
- Fuoco e Umidità
- Insetti
- Età
- Disastri naturali



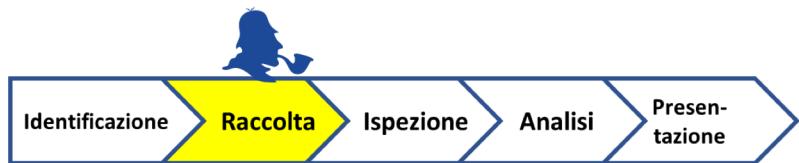
Raccolta | 8/11

Problemi relativi alle Fonti di Prove Digitali | 2/3

- È importante sottolineare che vi sono **più minacce per i dati digitali**, rispetto ai cosiddetti dati «cartacei»

Alcune Minacce per i dati digitali

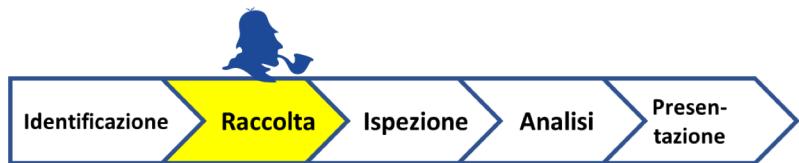
- | | |
|--|--|
| <ul style="list-style-type: none">• Errori Umani/Negligenze• Campi elettromagnetici e/o magnetici• Acqua e Condensa• Polvere• Calore | <ul style="list-style-type: none">• Impatti fisici• Voltaggio• Elettricità statica• Disastri naturali |
|--|--|



Raccolta | 9/11

Integrità delle Prove Digitali

- L'integrità di una prova è un aspetto centrale per quanto riguarda l'investigazione forense
- È importante che la prova non venga alterata durante la fase di raccolta (ad esempio, durante la copia di file, ecc.)
 - Ci sono dispositivi hardware e strumenti software che proteggono i dati originali da modalità diverse dalla lettura
- Per verificare se l'integrità delle prove è preservata, si utilizza il concetto di *digital fingerprint*, il quale si realizza mediante le funzioni crittografiche di hash (dette anche funzioni one-way)
 - *Esempi:* MD5, SHA-1, SHA-256, ecc.



Raccolta | 10/11

Ordine di Volatilità delle Prove Digitali

- In un'analisi digitale forense, si tiene conto di diverse fonti
- È necessario considerare che è impossibile ottenere alcuni dati da un sistema, senza modificarne lo stato
- Per questo motivo si definisce un ordine di volatilità (**Order Of Volatility – OOV**)
- I dati «*più volatili*» devono essere acquisiti prima dei dati «*meno volatili*»

DEFINIZIONE

L'**ordine di volatilità** definisce la priorità con la quale devono essere acquisiti i dati da dispositivi, in base alla volatilità dei dati stessi

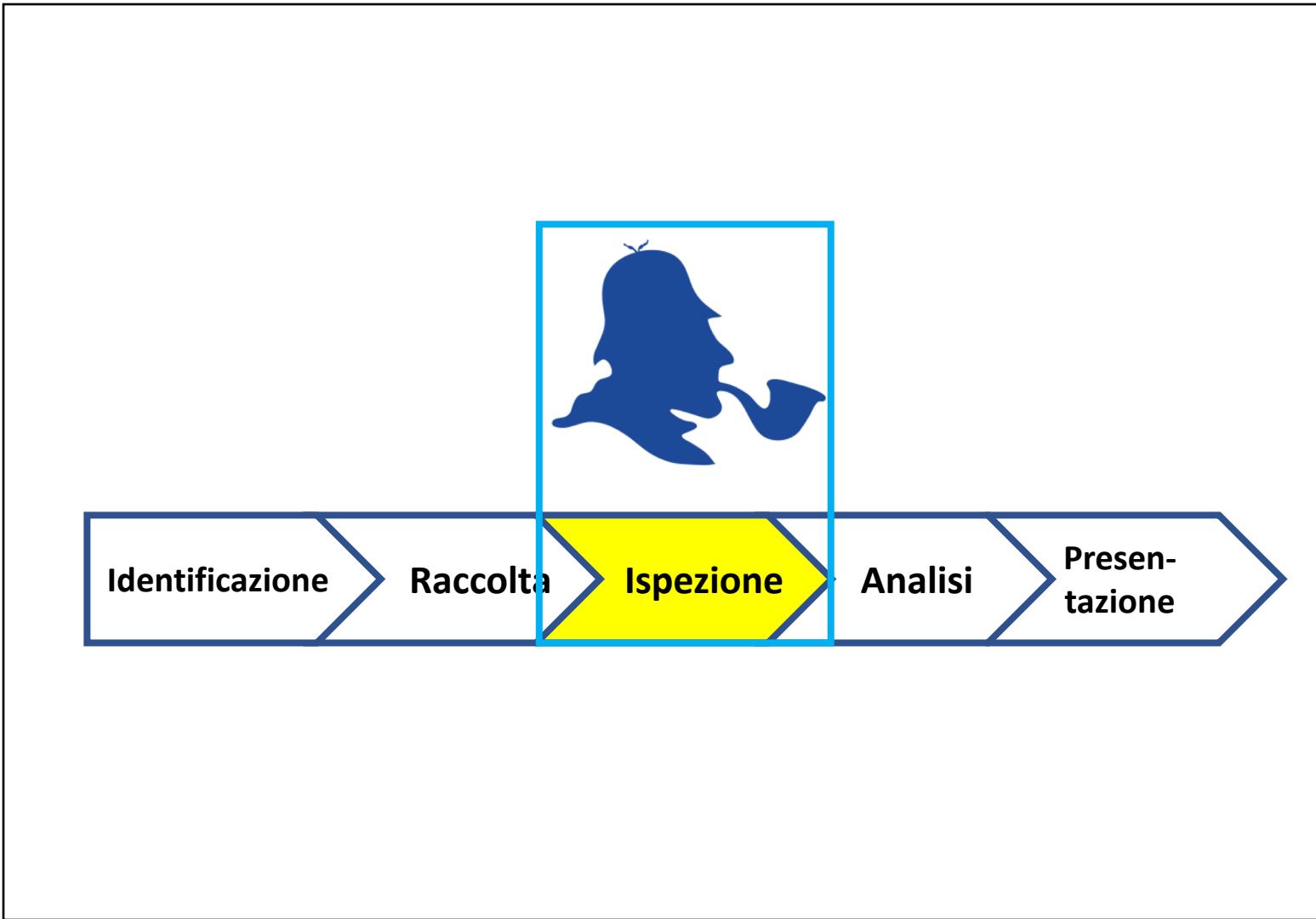


Raccolta | 11/11

Ordine di Volatilità delle Prove Digitali *Esempio*

- 
- Registri, memorie di periferiche, ecc.
 - Memoria RAM
 - Stato della Rete
 - Processi in Esecuzione
 - Disco Rigido
 - CD-ROM/DVD/Ecc.

Fasi Principali





Ispezione | 1/7

- L'**ispezione** richiede spesso la ristrutturazione, la riorganizzazione ed il processing dei dati grezzi
 - **OBIETTIVO:** Rendere tali dati più comprensibili agli investigatori
- Vengono tipicamente utilizzati strumenti forensi e appropriate tecniche per l'estrazione di informazioni rilevanti

Nella fase di **ispezione** vi è la preparazione e l'estrazione di potenziali prove digitali dai dati raccolti, nella fase precedente

DEFINIZIONE



Ispezione | 2/7

Ripristino (*Recovery*) dei Dati – 1/2

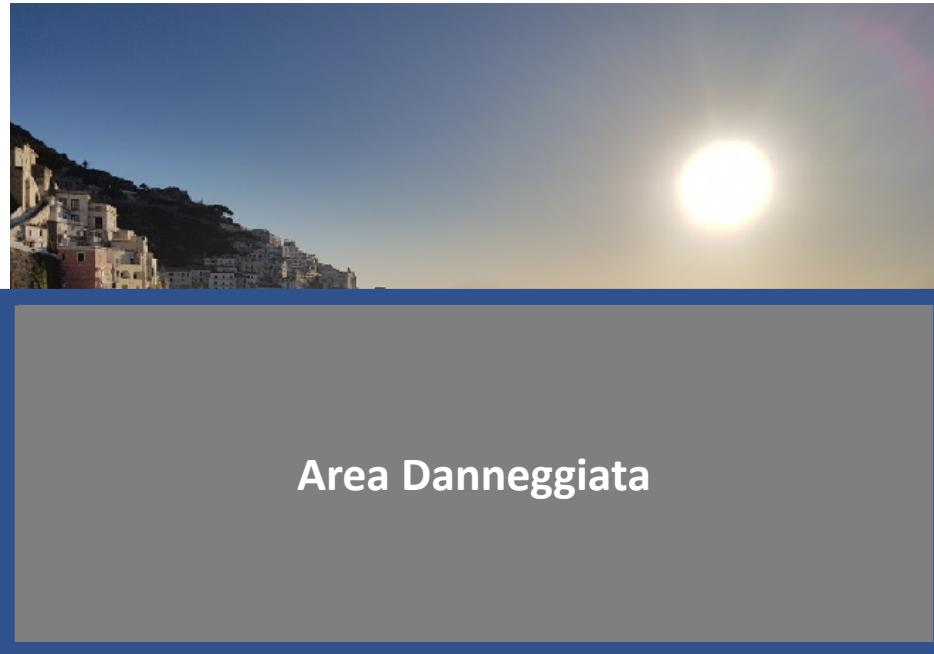
- I dispositivi informatici sono progettati affinché trattino i dati in maniera più efficiente possibile e forniscano una esperienza utente più gradevole possibile
- Tutto ciò, **in termini pratici**, si traduce, in genere, nei moderni sistemi operativi, nel trattare un *puntatore a un file*
- Quando un file viene eliminato, di fatto, solo il puntatore viene contrassegnato come *unallocated* (non allocato) o *available* (disponibile)
 - Questo significa che lo spazio, allocato per tale file, è disponibile, pertanto, può essere fisicamente sovrascritto da un nuovo file
- D'altro canto, un file può essere ripristinato (*recovered*), dal supporto di memorizzazione, se non è stato effettivamente sovrascritto da altri file



Ispezione | 3/7

Ripristino (*Recovery*) dei Dati – 2/2 Esempio

- *Simulazione di una Immagine Parzialmente Ripristinata*





Ispezione | 4/7

Riduzione e Filtraggio dei Dati Acquisiti – 1/2

- I dispositivi informatici analizzati dagli investigatori possono contenere **svariati terabytes di dati e miliardi di file**
- È pertanto impossibile fare una analisi completa su una siffatta mole di dati
- **SOLUZIONE:** Effettuare una fase di filtraggio dei dati (tramite strumenti forensi appositi), individuando quelli potenzialmente significativi
 - Ad esempio, i file relativi al Sistema Operativo risultano di scarso interesse, dal punto di vista forense (pertanto, possono essere parzialmente ignorati)



Ispezione | 5/7

Riduzione e Filtraggio dei Dati Acquisiti – 2/2

Dati Acquisiti

File di Interesse

Applicazioni

Driver

File Utente

File relativi al Sistema
Operativo



Ispezione | 6/7

Carving di File e Dati – 1/2

- I dati raccolti sono solitamente non strutturati e difficili da interpretare, da parte degli investigatori forensi
- Capita sovente di individuare file corrotti, cancellati, frammentati, ecc.
- Tramite appositi strumenti forensi è possibile categorizzare i suddetti file
 - I suddetti strumenti analizzano il contenuto dei file corrotti, ecc. ed individuano pattern o firme digitali, in modo da riuscire ad individuarne la tipologia

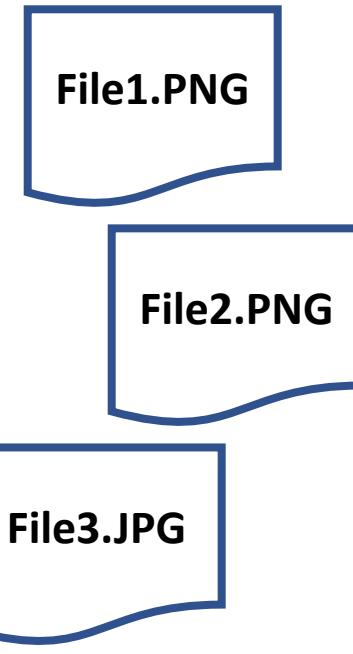


Ispezione | 7/7

Carving di File e Dati – 2/2

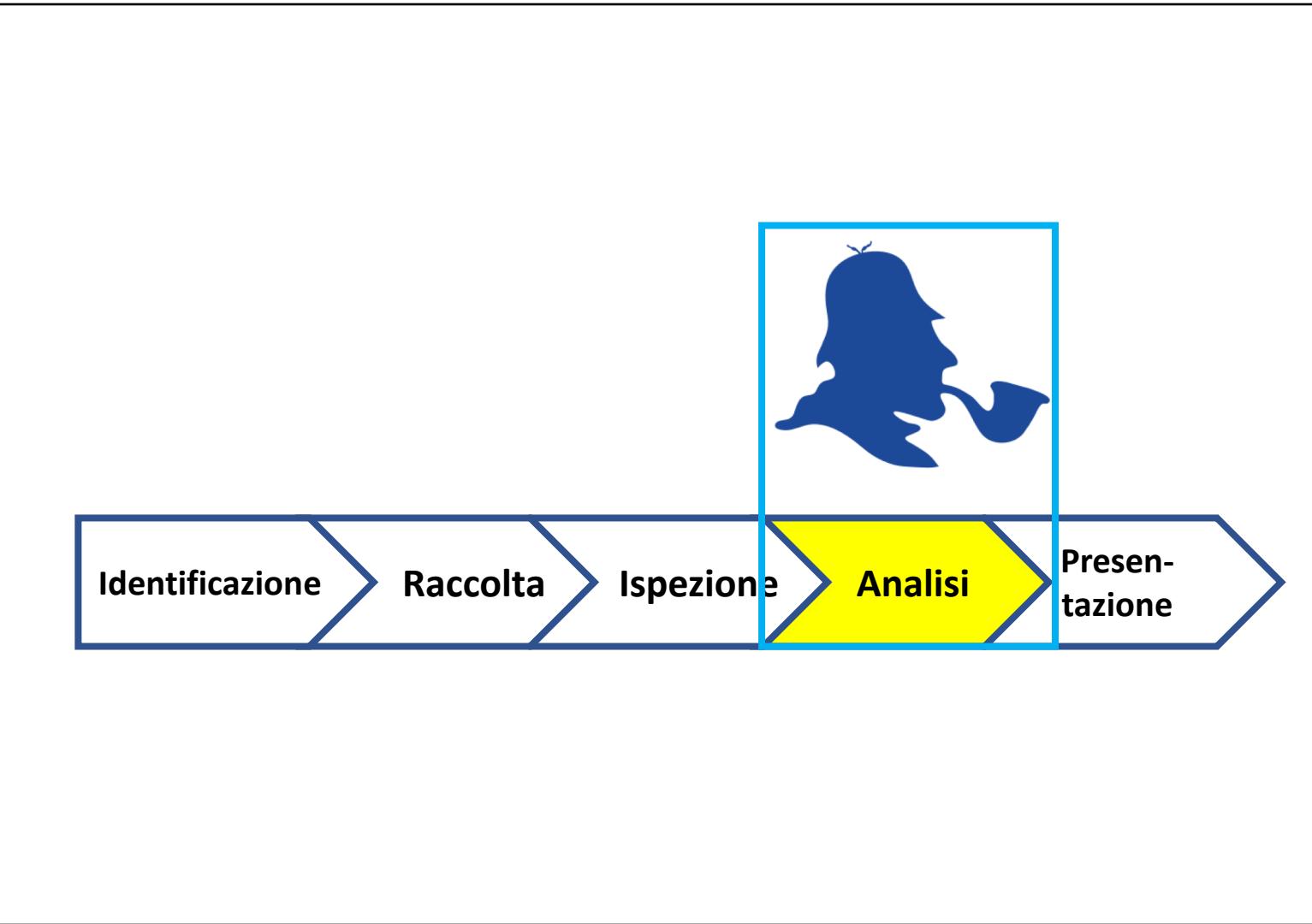


Input



Output

Fasi Principali





Analisi | 1/6

DEFINIZIONE

Nella fase di **analisi**, vengono processate le informazioni con gli obiettivi di determinare i *fatti*, in relazione ad un evento, e di determinare l'importanza e/o la significatività di una prova e il/i soggetto/i responsabile/i



Analisi | 1/6

DEFINIZIONE

Nella fase di **analisi**, vengono processate le informazioni con l'obiettivo di determinare i *fatti*, in relazione ad un evento, e di determinare l'importanza e/o la significatività di una prova e il/i soggetto/i responsabile/i

OSSERVAZIONE

La fase di analisi è un essa stessa un **processo iterativo**



Ricerca tramite Stringhe e Keyword – 1/2

- Ricerche mediante stringhe e keyword risultano utili nella fase di analisi, in quanto semplificano o comunque possono semplificare il lavoro dell'investigatore
- *Esempio*
 - In una analisi forense, si cercano informazioni di un individuo, di cui si conosce il nome e cognome o il soprannome
 - È possibile effettuare ricerche utilizzando proprio il *nome*, *cognome* e *soprannome* come parole chiave
- Le ricerche possono avvenire tramite pattern matching di stringhe, includendo espressioni regolari, ecc.



Analisi | 3/6

Ricerca tramite Stringhe e Keyword – 2/2

- Altre informazioni utili per la ricerca tramite stringhe e keyword possono essere:
 - Numero di telefono
 - Social Security Number (SSN)/Codice Fiscale (CF)
 - Indirizzi
 - *Virtuali*: IP, email, URL (es. indirizzi web)
 - *Fisici*: abitazione, ufficio
 - Religione, interessi culturali, ...
 - Ecc.



Analisi | 4/6

Tecniche Anti-Analisi Forense (*Cenni*)

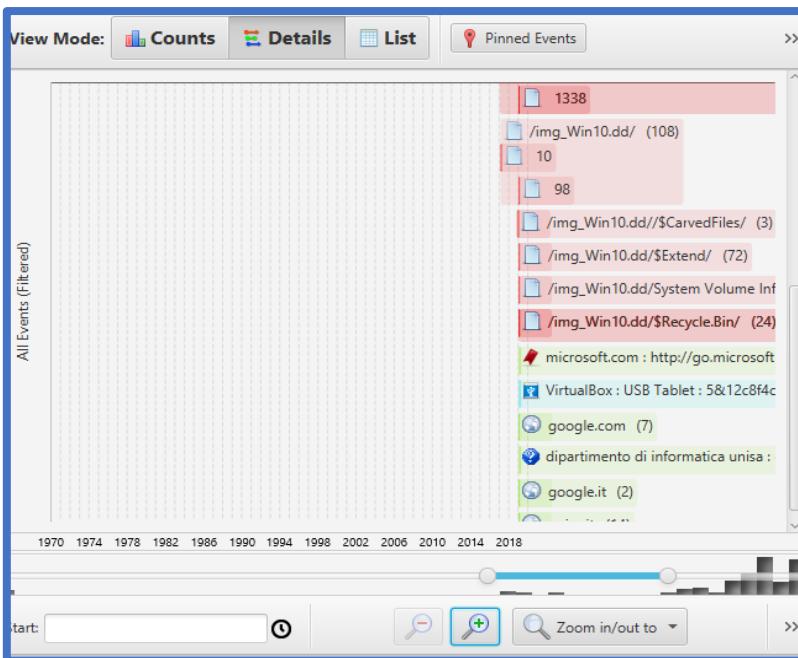
- Sono state sviluppate alcune tecniche note che sono deliberatamente attuate al fine di provare a rendere più difficile l'analisi forense:
 - Computer Media Wiping
 - Strumenti che fanno wiping (letteralmente: *pulizia*) con l'obiettivo di eliminare definitivamente i file
 - *Remote Wiping*: Utilizzato per la cancellazione remota di file su un dispositivo (ad esempio, un dispositivo rubato)
 - Cifratura e/o Offuscamento dei Dati
 - Alcuni malware tendono a offuscare/cifrare file di configurazione, ecc. (ad esempio, i ransomware)
 - È necessario individuare la motivazione relativa alla cifratura di un file (se per questioni di protezione di un file o cifratura effettuata da un malware)



Analisi | 5/6

Analisi delle Timeline degli Eventi

- È estremamente utile realizzare delle **timeline** di eventi (*esempio in figura*), basandosi sulle informazioni raccolte (ad esempio, la **struttura dei file**, le **date dell'ultimo accesso** relativa a file, ecc.)

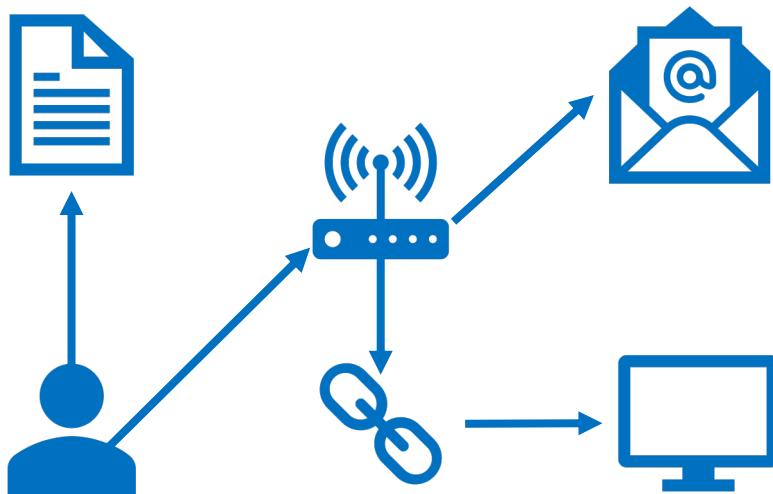




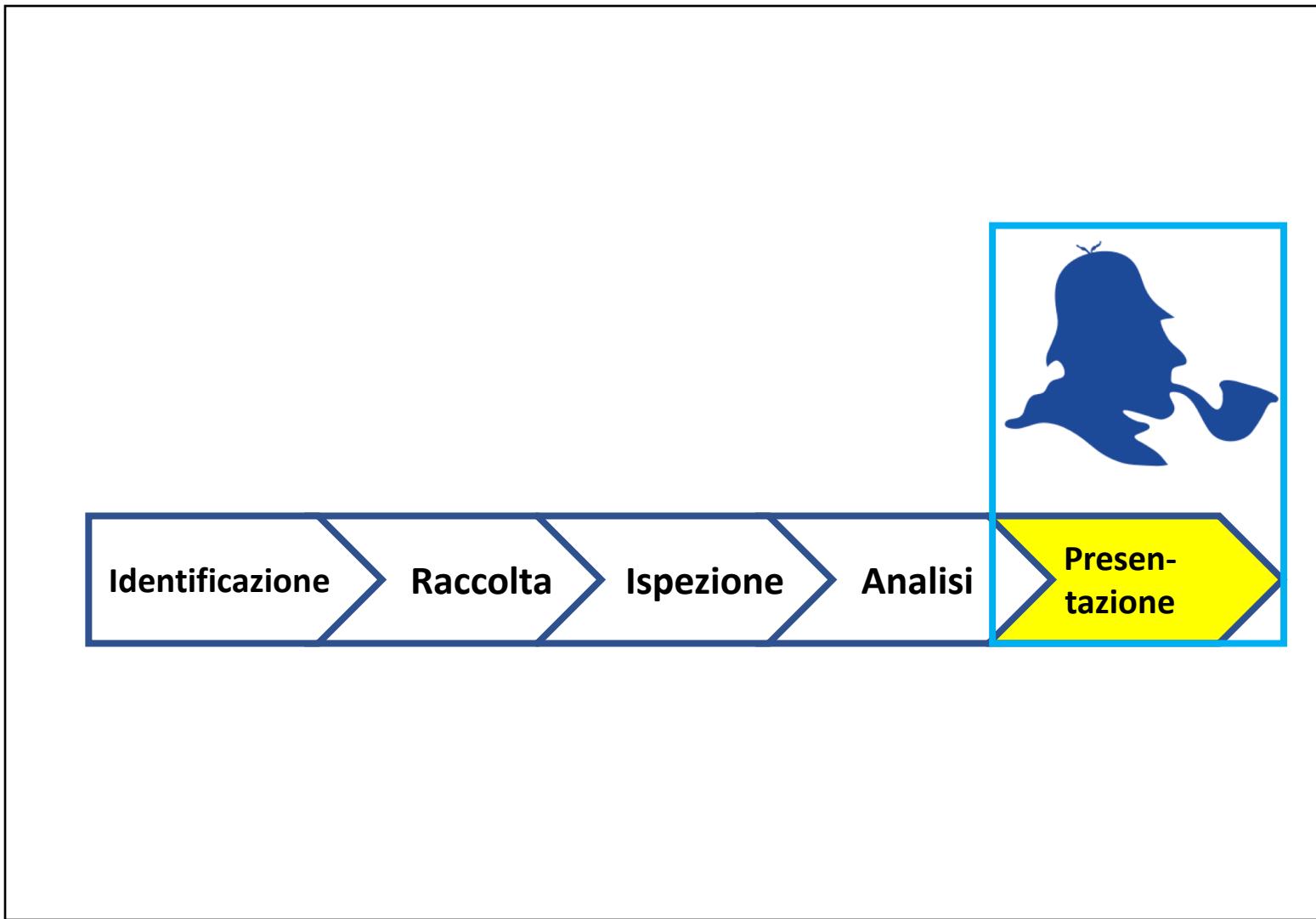
Analisi | 6/6

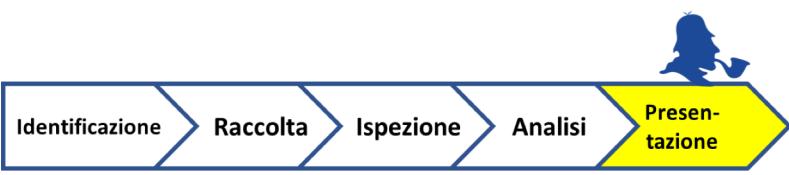
Analisi dei Collegamenti

- L'**analisi dei collegamenti** (*link analysis*) è una potente ed emergente disciplina, nell'ambito della digital forensics
- L'obiettivo principale è la costruzione di una **presentazione strutturata degli oggetti collegati ed interconnessi**, al fine di comprendere al meglio le associazioni e i collegamenti fra gli oggetti



Fasi Principali





Presentazione | 1/2

- La fase di **presentazione** è la fase in cui viene prodotta la documentazione finale relativa al risultato dell'investigazione
- Tale documentazione deve essere presentata in tribunale o negli uffici preposti

DEFINIZIONE

Nella fase di **presentazione**, l'investigatore condivide, alle parti interessate, i risultati dell'analisi, in forma di report

Identificazione

Raccolta

Ispezione

Analisi

Presentazione



Presentazione | 2/2

Esempio di report generato da un tool di analisi forense (Autopsy)

The screenshot shows a web browser displaying an Autopsy Forensic Report. The title bar reads "Autopsy Forensic Report". The address bar shows the URL "file:///C:/Users/Raffaele/Documents/Windows_10/Reports/Windows_10%20HTML%20Report%2002-26-2019-17-53-21/report.html".

Report Navigation:

- Case Summary
- EXIF Metadata (6)
- Encryption Suspected (8)
- Extension Mismatch Detected (5)
- Keyword Hits (1056)
- Operating System Information (2)
- Recent Documents (1)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- USB Device Attached (2)
- Web Bookmarks (1)
- Web Cookies (11)
- Web History (12)
- Web Search (1)

Autopsy Forensic Report
HTML Report Generated on 2019/02/26 17:53:21

Case: Windows_10
Case Number: 123456789
Examiner: Raffaele
Number of Images: 1

Image Information:

Win10.dd
Timezone: Europe/Berlin
Path: C:\Users\Raffaele\Plaso\Win10.dd

Software Information:

Autopsy Version: 4.10.0
Android Analyzer Module: 4.10.0

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | 1/12

- Sono state sviluppate **diverse distribuzioni Linux**, appositamente pensate per l'uso nell'ambito della digital forensics e che hanno caratteristiche interessanti
- Queste distribuzioni sono **gratuite** ed includono **diversi tool Open-Source**, ampiamente revisionati da community specializzate
 - Digital Evidence and Forensics Toolkit (DEFT) Linux
 - Computer Aided INvestigative Environment (CAINE)
 - Parrot Security Linux
 - Kali Linux

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | 2/12

- Sono state sviluppate **diverse distribuzioni Linux**, appositamente pensate per l'uso nell'ambito della digital forensics e che hanno caratteristiche interessanti
- Queste distribuzioni sono **gratuite** ed includono **diversi tool Open-Source**, ampiamente revisionati da community specializzate
 - **Digital Evidence and Forensics Toolkit (DEFT) Linux**
 - Computer Aided INvestigative Environment (CAINE)
 - Parrot Security Linux
 - Kali Linux

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 3/12

Digital Evidence and Forensics Toolkit (DEFT) Linux | 1/3

- **Progetto italiano**, nato nel 2005, non più aggiornato
- Esecuzione esclusivamente in RAM
 - Nessun meccanismo di swap, in modo da accedere a tutte le memorie secondarie in sola lettura, e non accedendovi mai in scrittura
- Basato su:
 - Xubuntu
- Maggiori dettagli:
 - <http://www.deftlinux.net/>

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 4/12

Digital Evidence and Forensics Toolkit (DEFT) Linux | 2/3

- Alcuni applicativi, per la digital forensics, preinstallati Open-Source:
 - The Sleuth Kit
 - Autopsy
 - Dhash, software per l'acquisizione e calcolo di hash su memorie di massa e file
 - Guymager
 - Linen, software per acquisizione memorie di massa fornito dalla Guidance Software
 - D3CDD
 - Tool per calcolo di hash (md5deep, sha1deep, e sha256deep)
 - Foremost
 - Ecc.
- Alcuni dei suddetti tool, verranno approfonditi nelle prossime lezioni

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 5/12

Digital Evidence and Forensics Toolkit (DEFT) Linux | 3/3

- *Screenshot di DEFT Linux | 1/3*

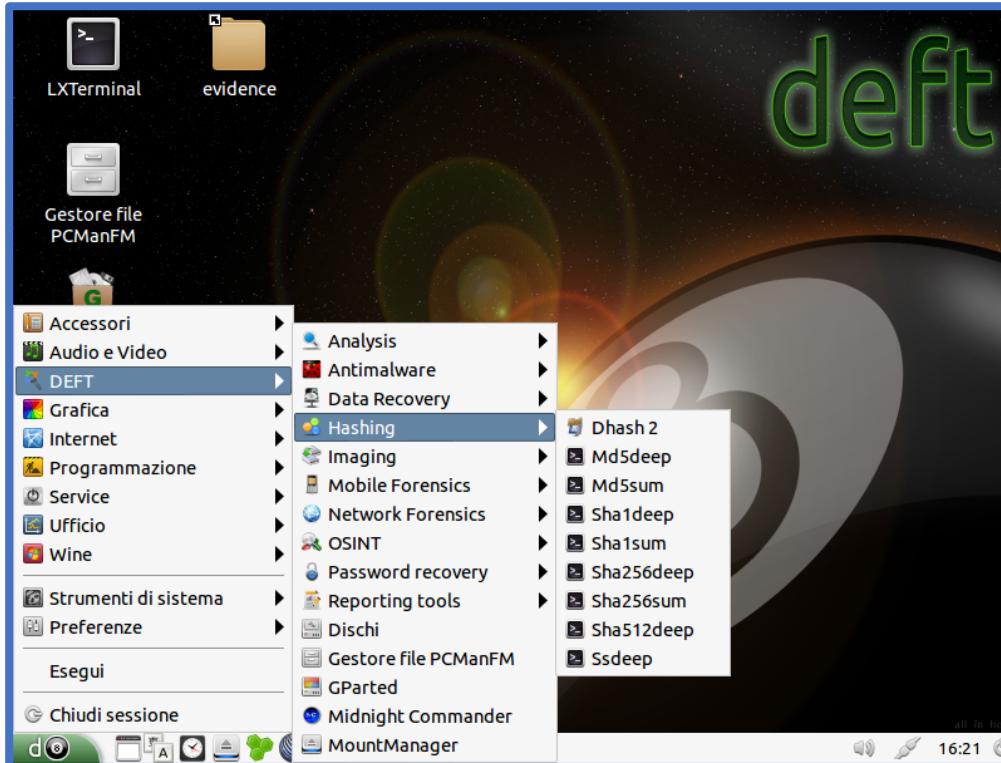


Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 5/12

Digital Evidence and Forensics Toolkit (DEFT) Linux | 3/3

- *Screenshot di DEFT Linux | 2/3*

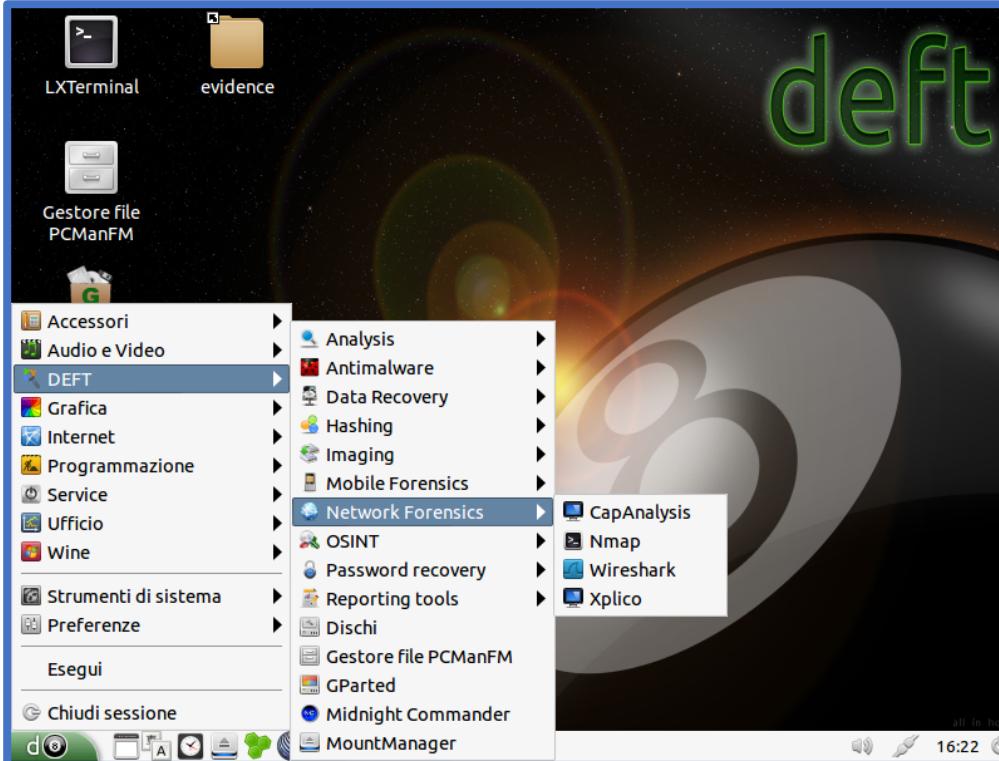


Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 5/12

Digital Evidence and Forensics Toolkit (DEFT) Linux | 3/3

- *Screenshot di DEFT Linux | 3/3*



Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | 6/12

- Sono state sviluppate **diverse distribuzioni Linux**, appositamente pensate per l'uso nell'ambito della digital forensics e che hanno caratteristiche interessanti
- Queste distribuzioni sono **gratuite** ed includono **diversi tool Open-Source**, ampiamente revisionati da community specializzate
 - Digital Evidence and Forensics Toolkit (DEFT) Linux
 - **Computer Aided INvestigative Environment (CAINE)**
 - Parrot Security Linux
 - Kali Linux

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 7/12

Computer Aided INvestigative Environment (CAINE) | 1/2

- **Insieme completo** di tool per l'analisi forense
- Ambiente di investigazione **affidabile**
- Interfaccia grafica e **user-friendly**
- **Report finale** dell'investigazione forense **completo** e generato in maniera **semi-automatizzata**
- Basato su:
 - Ubuntu
- Maggiori dettagli:
 - <https://www.caine-live.net/>

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 8/12

Computer Aided INvestigative Environment (CAINE) | 2/2

- *Screenshot di CAINE Linux | 1/2*

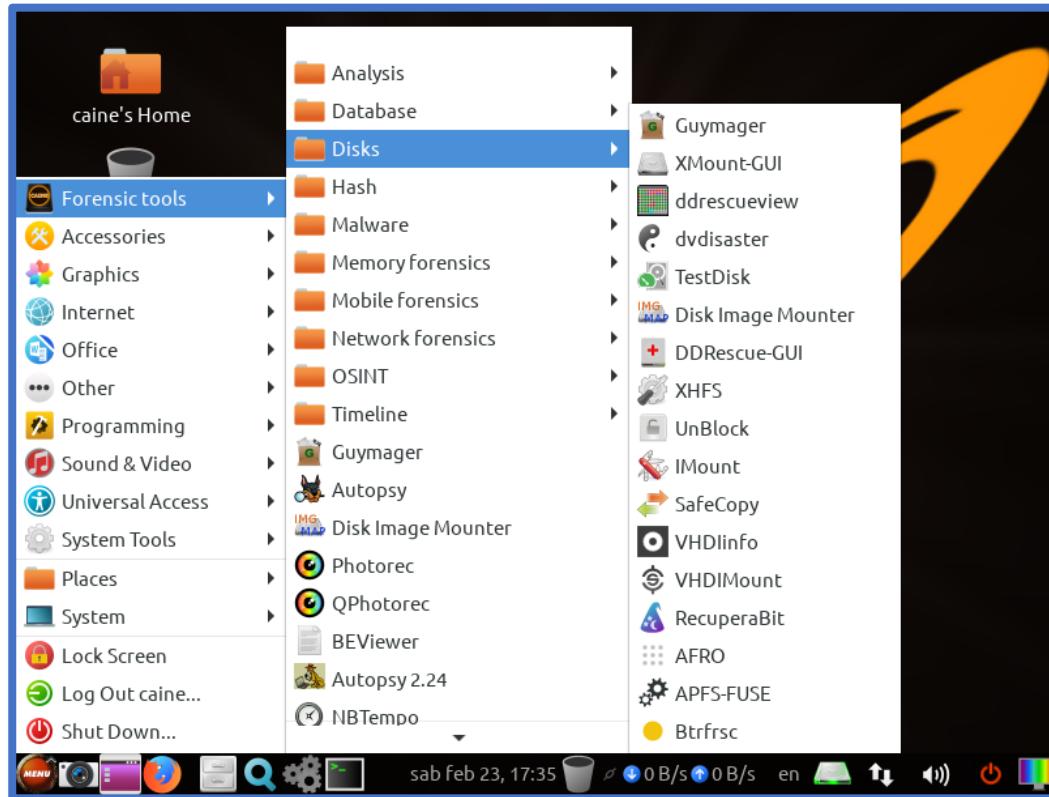


Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | DEFT Linux | 8/12

Computer Aided INvestigative Environment (CAINE) | 2/2

- *Screenshot di CAINE Linux | 2/2*



Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | 9/12

- Sono state sviluppate **diverse distribuzioni Linux**, appositamente pensate per l'uso nell'ambito della digital forensics e che hanno caratteristiche interessanti
- Queste distribuzioni sono **gratuite** ed includono **diversi tool Open-Source**, ampiamente revisionati da community specializzate
 - Digital Evidence and Forensics Toolkit (DEFT) Linux
 - Computer Aided INvestigative Environment (CAINE)
 - **Parrot Security Linux**
 - Kali Linux

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | Parrot Security Linux | 10/12

Parrot Security Linux | 1/2

- **Parrot Security Linux** è una distribuzione all-in-one, che contiene diversi tool, per varie attività, fra cui:
 - Penetration Testing
 - Privacy
 - Digital Forensics
 - Reverse Engineering
 - Sviluppo Applicazioni
- Basato su:
 - Debian
- Maggiori dettagli:
 - <https://www.parrotsec.org/>

Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | Parrot Security Linux | 11/12

Parrot Security Linux | 2/2

- *Screenshot di Parrot Security Linux | 1/3*

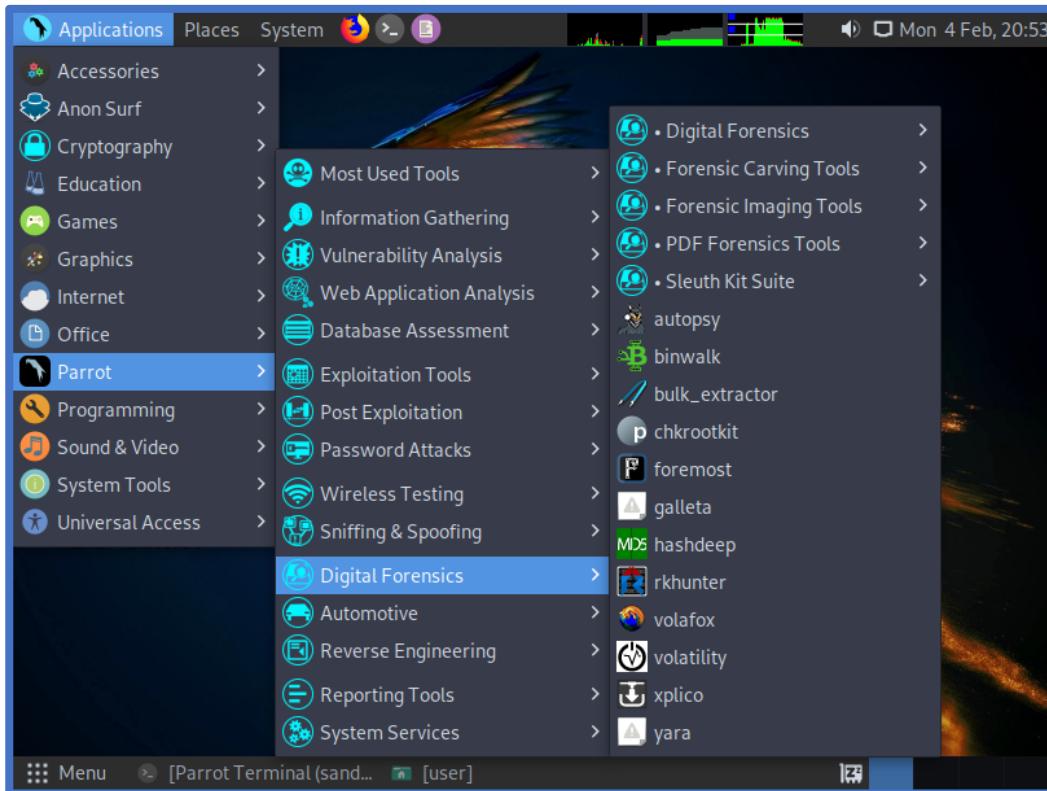


Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | Parrot Security Linux | 12/12

Parrot Security Linux | 2/2

- *Screenshot di Parrot Security Linux | 2/3*

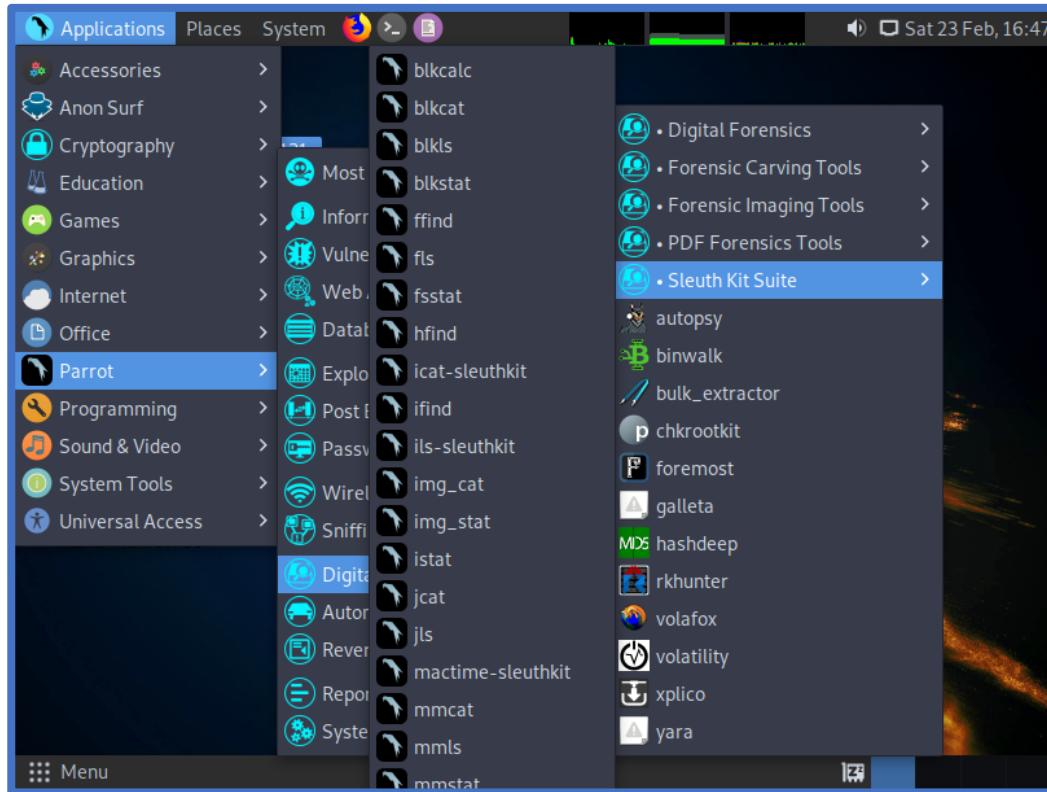


Distribuzioni Linux per la Digital Forensics

Distribuzioni Linux | Parrot Security Linux | 12/12

Parrot Security Linux | 2/2

- *Screenshot di Parrot Security Linux | 3/3*





Kali Linux

Kali Linux

Caratteristiche

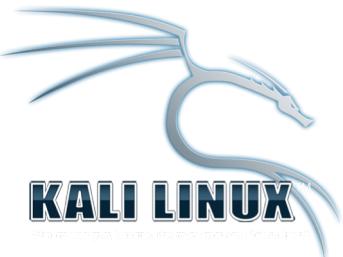
- Kali Linux è una distribuzione creata, inizialmente, per le attività relative al Penetration Testing
- Il nome iniziale era BackTrack, divenuto poi Kali Linux
- Analogamente alle altre tre distribuzioni Linux, viste precedentemente, Kali Linux può essere utilizzata in due modalità:
 - Modalità *live* (senza installazione)
 - Modalità *forense* (*maggiori dettagli nelle prossime slide*) dagli investigatori
 - Come un classico Sistema Operativo
- Basata su:
 - Debian
- Link per dettagli e download:
 - <https://www.kali.org/>



Kali Linux

Caratteristiche

- Kali Linux è una distribuzione creata, inizialmente, per le attività relative al Penetration Testing
- Il nome iniziale era BackTrack, diventato poi Kali Linux
- Analogamente a BackTrack, ha due modalità:
 - Moda
 - Moda
- dagli i
- Come
- Basata su:
 - Debian
- Link per dettagli e download:
 - <https://www.kali.org/>



La distribuzione Kali Linux sarà
utilizzata spesso come
riferimento, durante il Corso



Avvio di Kali Linux in Modalità Forense | 1/5

- Avviando Kali Linux da penna USB o da DVD-ROM, è possibile effettuare l'avvio, in modalità forense
- La modalità forense di Kali Linux permette di:
 - Lasciare intatti i supporti di memorizzazione del computer, su cui è stata avviata
 - Disabilita il *mounting* automatico di penne USB e altri dispositivi
 - Lascia inalterate le prove (supporti di memorizzazione del computer), durante la fase di indagine



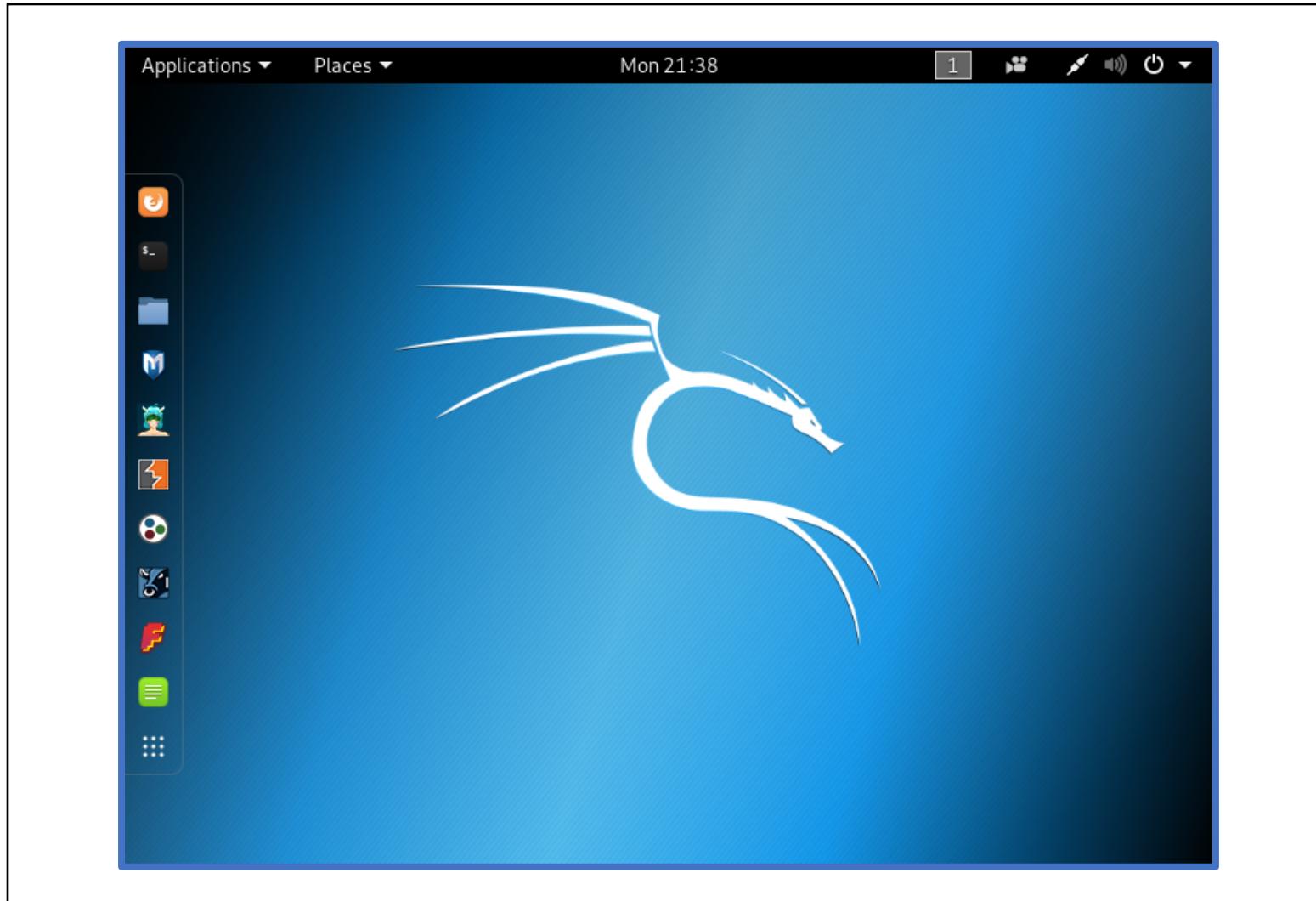
Avvio di Kali Linux in Modalità Forense | 2/5



All'avvio di Kali Linux (tramite DVD o penna USB), all'investigatore verrà presentata una schermata di scelta, dove è necessario selezionare l'opzione **Live (forensic mode)**, per l'avvio in modalità forense

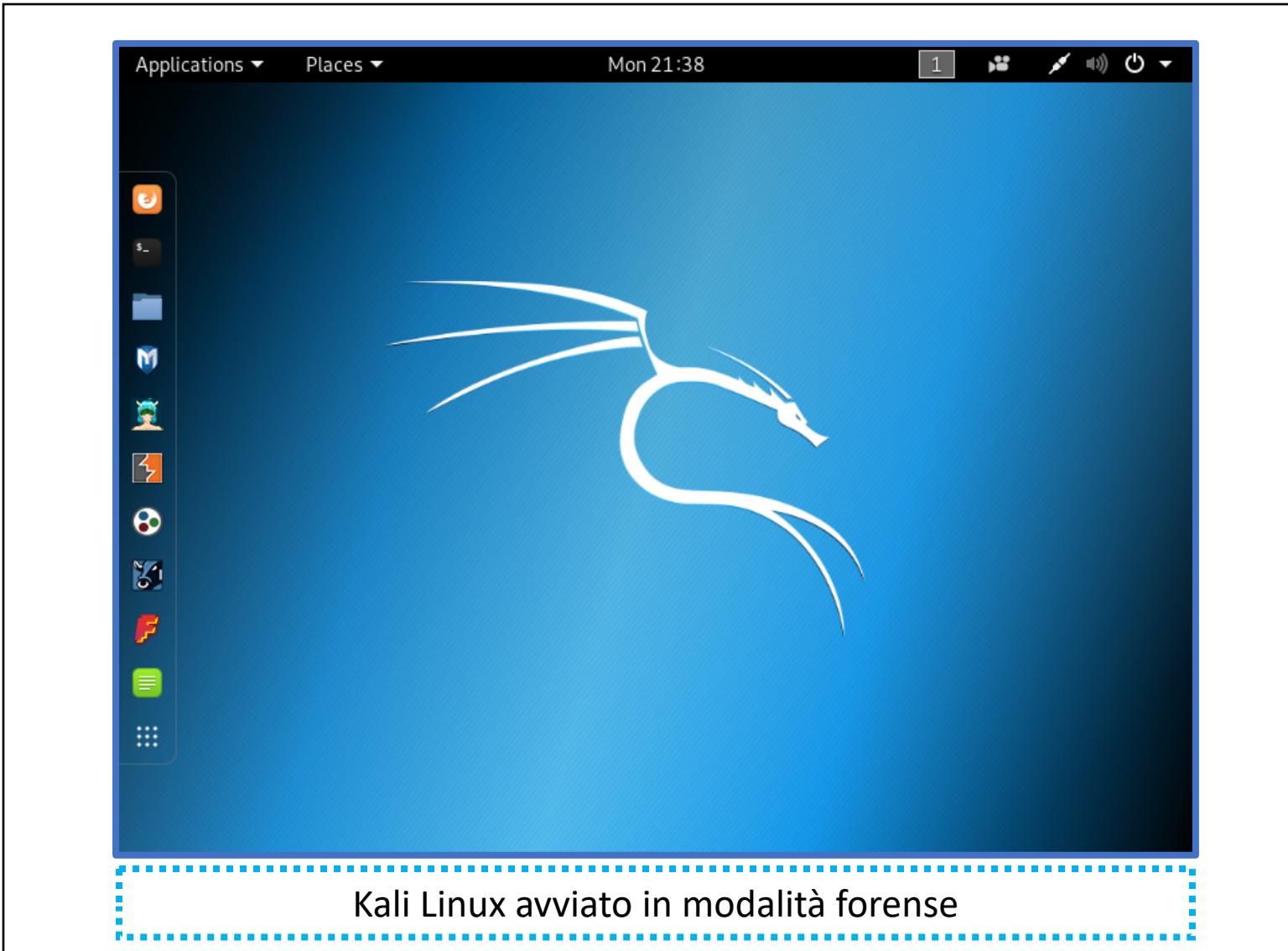
Kali Linux

Avvio di Kali Linux in Modalità Forense | 3/5



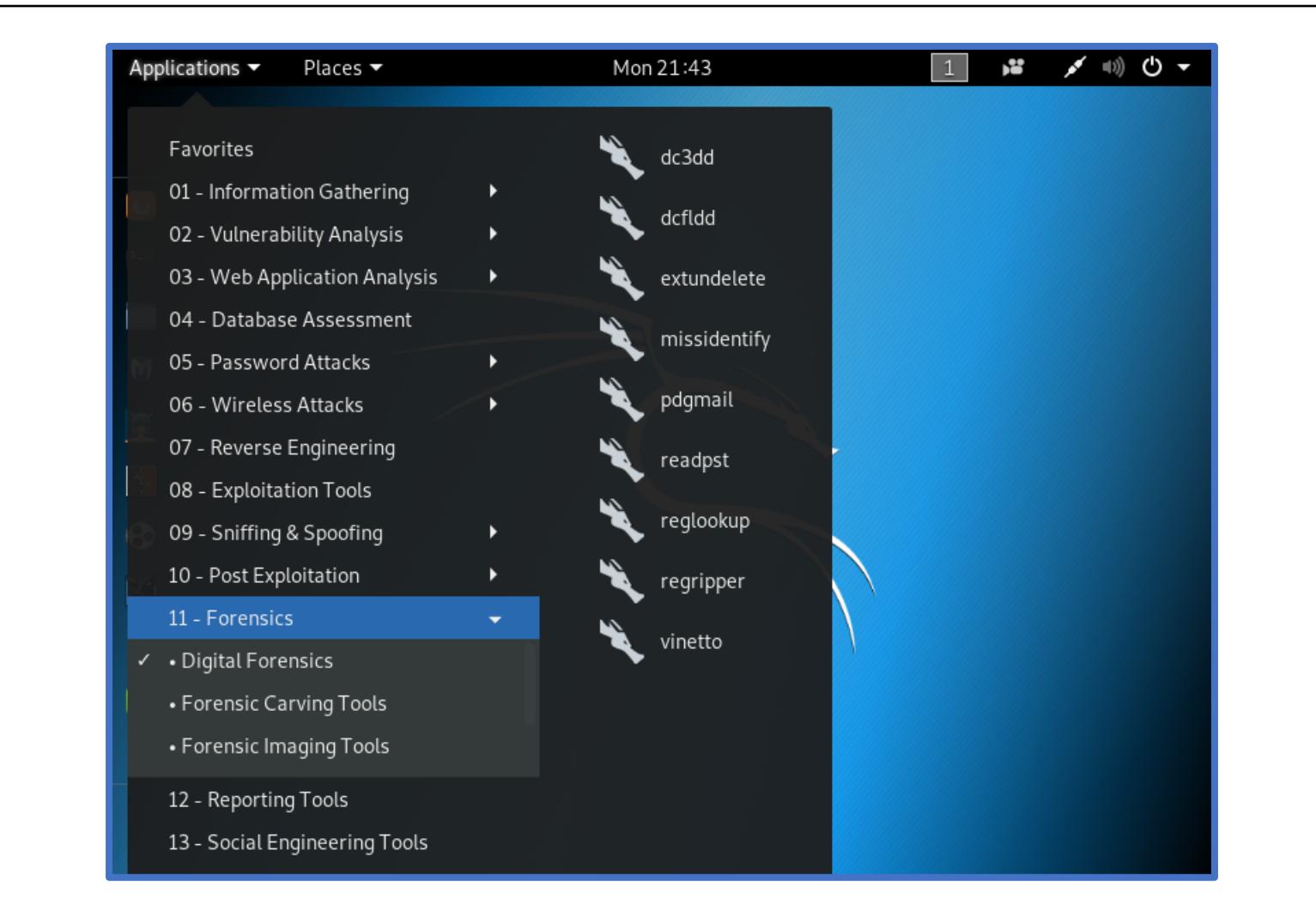
Kali Linux

Avvio di Kali Linux in Modalità Forense | 3/5



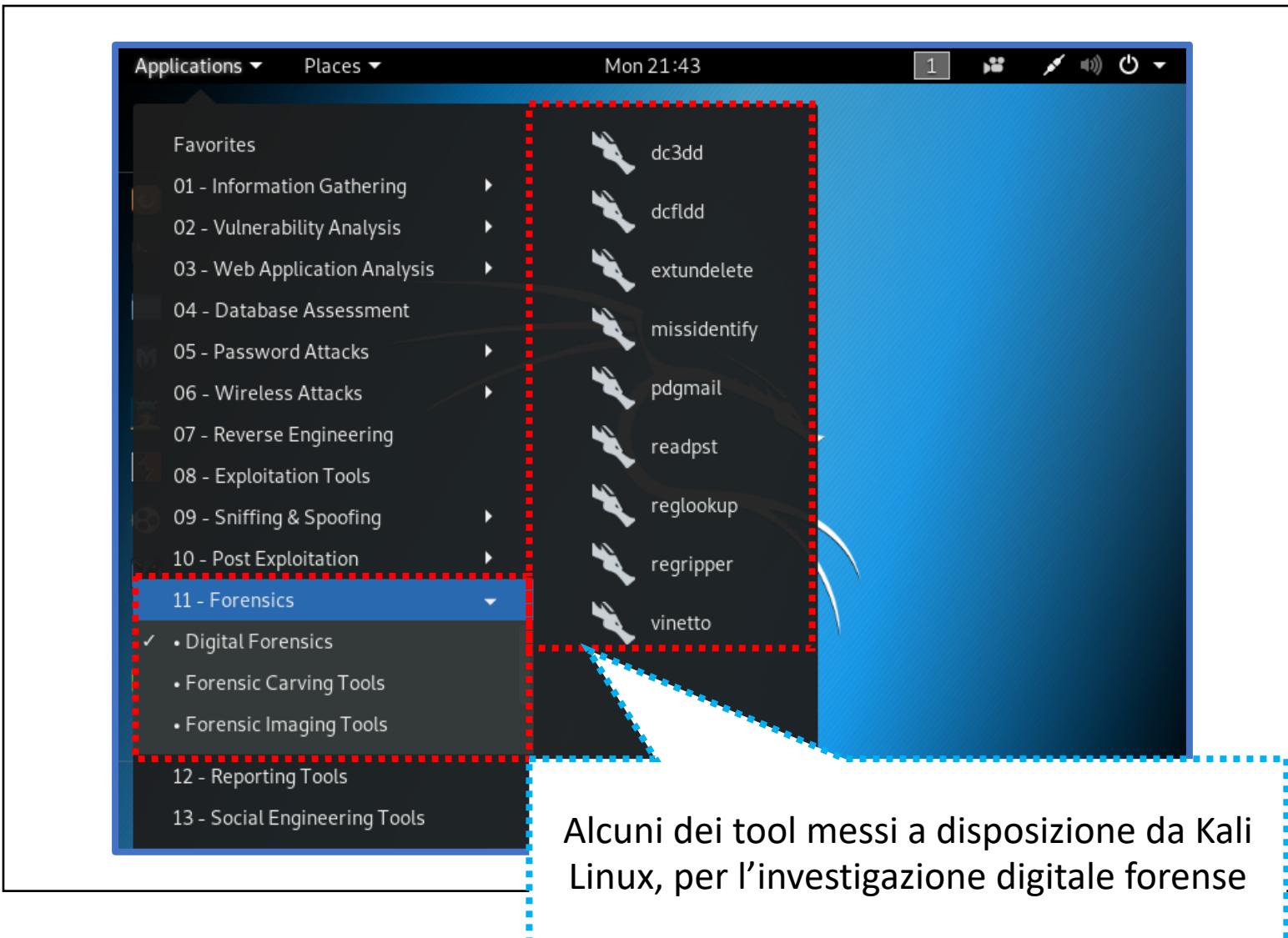
Kali Linux

Avvio di Kali Linux in Modalità Forense | 4/5



Kali Linux

Avvio di Kali Linux in Modalità Forense | 4/5



Avvio di Kali Linux in Modalità Forense | 5/5

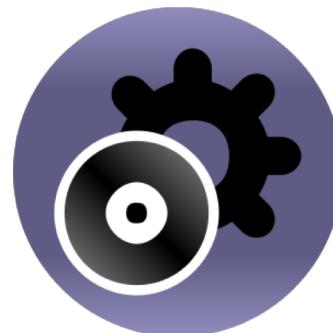
- La lista di tutti i tool, presenti in Kali Linux, è disponibile al seguente link:
 - <https://tools.kali.org/tools-listing>
- *Screenshot (Parziale)*

The screenshot shows the 'KALI TOOLS' website with a blue header bar containing the logo, 'Home', 'Tools Listing', 'Metapackages', and a search icon. Below the header is a main title 'Kali Linux Tools Listing'. Underneath, there are four main category sections: 'Information Gathering', 'Vulnerability Analysis', 'Wireless Attacks', and 'Web Applications', each with a list of tools.

Information Gathering	Vulnerability Analysis	Wireless Attacks	Web Applications
<ul style="list-style-type: none">• ace-voip• Amap• APT2• arp-scan• Automater	<ul style="list-style-type: none">• BBSQL• BED• cisco-auditing-tool• cisco-global-exploiter• cisco-ocs	<ul style="list-style-type: none">• Airbase-ng• Aircrack-ng• Airdecap-ng and Airdecoak-ng• Aireplay-ng• airgraph-ng	<ul style="list-style-type: none">• apache-users• Arachni• BBSQL• BlindElephant• Burp Suite

Installazione di Kali Linux su Virtual Machine | 1/6

- Software necessario per l'**installazione** di Kali Linux su Virtual Machine
 - Immagine ISO di Kali Linux
 - Software per la gestione di Virtual Machine
 - VirtualBox (Oracle)
 - VMWare (VMWare Inc.)
 - Ecc.



Installazione di Kali Linux su Virtual Machine | 1/6

- Software necessario per l'**installazione** di Kali Linux su Virtual Machine
 - Immagine ISO di Kali Linux
 - Software per la gestione di Virtual Machine
 - **VirtualBox (Oracle)**
 - **VMware (VMWare Inc.)**

Verrà utilizzato il software VirtualBox



Installazione di Kali Linux su Virtual Machine | 2/6

- Scaricare Oracle VirtualBox, dal seguente link:
 - <https://www.virtualbox.org/wiki/Downloads>



Installazione di Kali Linux su Virtual Machine | 3/6

- Installare VirtualBox sul proprio PC



Versione di riferimento: 6.0 (64 bit), per Microsoft Windows

Kali Linux

Installazione di Kali Linux su Virtual Machine | 4/6

- Scaricare la ISO di Kali Linux, dal seguente link:
 - <https://www.kali.org/downloads/>

The screenshot shows the 'Kali Linux Downloads' page. At the top, there's a navigation bar with links for Blog, Downloads, Training, and Documentation. Below the navigation, the page title 'Kali Linux Downloads' is centered. Underneath the title, there's a section titled 'Download Kali Linux Images'. A note below this section states: 'We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to [download Kali Linux](#) in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>.'. At the bottom of the page, there's a table listing three Kali Linux Light images:

Image Name	Download	Size	Version	sha256sum
Kali Linux Light 64 Bit	HTTP Torrent	867M	2018.4	ad63589f761a4344e930486e05e9d3652b8c8badb2e0f808951861ed489db1f6
Kali Linux Light Armhf	HTTP Torrent	630M	2018.4	4b409b7f0650741400b2c3c9076333f6c52211205c4a2828d677f1099d3e5d64
Kali Linux Light 32 Bit	HTTP Torrent	863M	2018.4	0659674f841d91b71bd2503e352ded588ec17d0e976c9fee4345dad35ace83b1

Kali Linux

Installazione di Kali Linux su Virtual Machine | 5/6



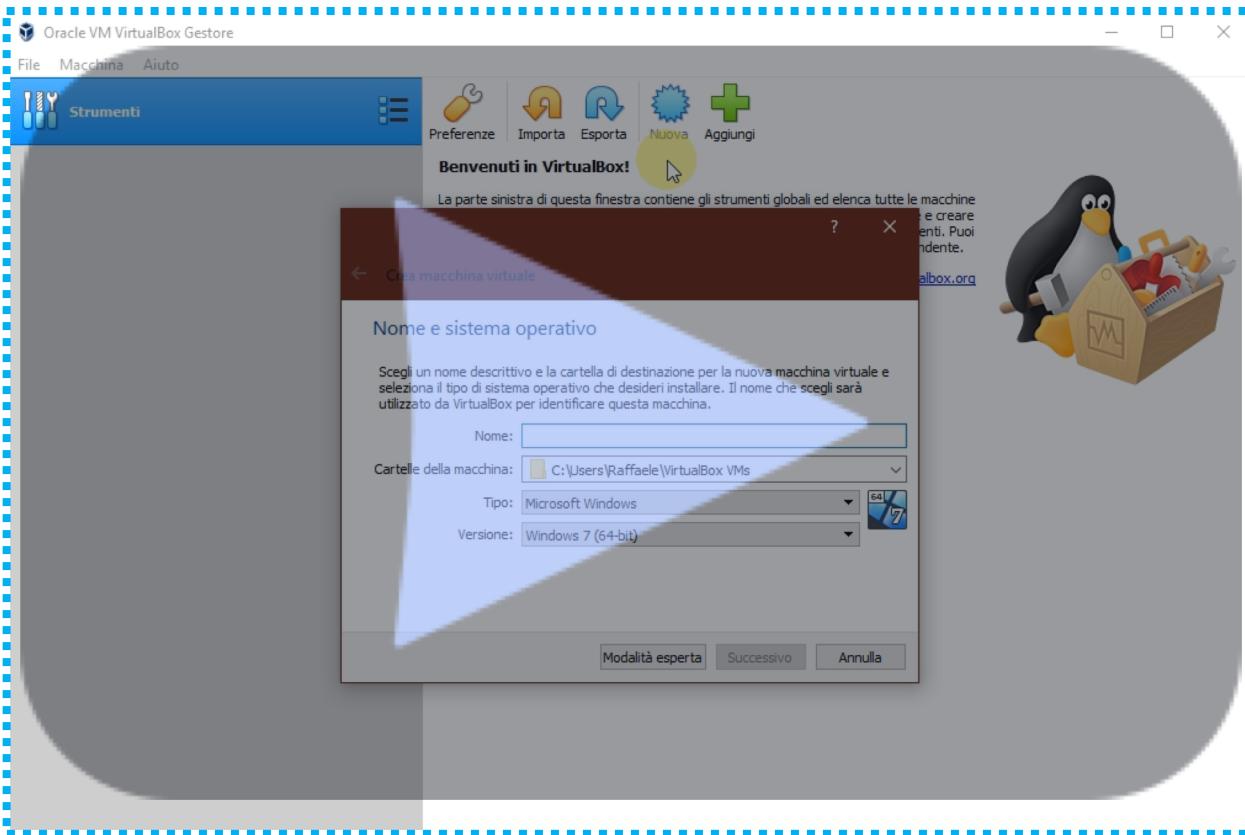
- *Versione di riferimento:* **2018.4** (64 bit)
 - Dimensione File: ~2,92 GB

Kali Linux

Installazione di Kali Linux su Virtual Machine | 6/6

DEMO Video Illustrativo

Installazione di Kali Linux su Virtual Machine



Video Disponibile al download anche sulla piattaforma e-Learning

Riferimenti Bibliografici

- **Boddington, Richard, Practical Digital Forensics, Packt Publishing Ltd, 2016**
 - Capitolo 1
- **André Årnes (editor), Digital Forensics, John Wiley & Sons, 2017**
 - Capitolo 1 (Solo definizioni Digital Forensics e Digital Evidence)
 - Capitolo 2
- **Digital Forensics with Kali Linux, Shiva V.N. Parasram, Packt Publishing, 2017**
 - Capitolo 1
 - Capitolo 2