



# Corso di Digital Forensics

CdLM in Informatica

Università degli Studi di Salerno

Docente: Ugo Fiore

7 – Anti-forensics

# Anti-Forensics

## Definizione



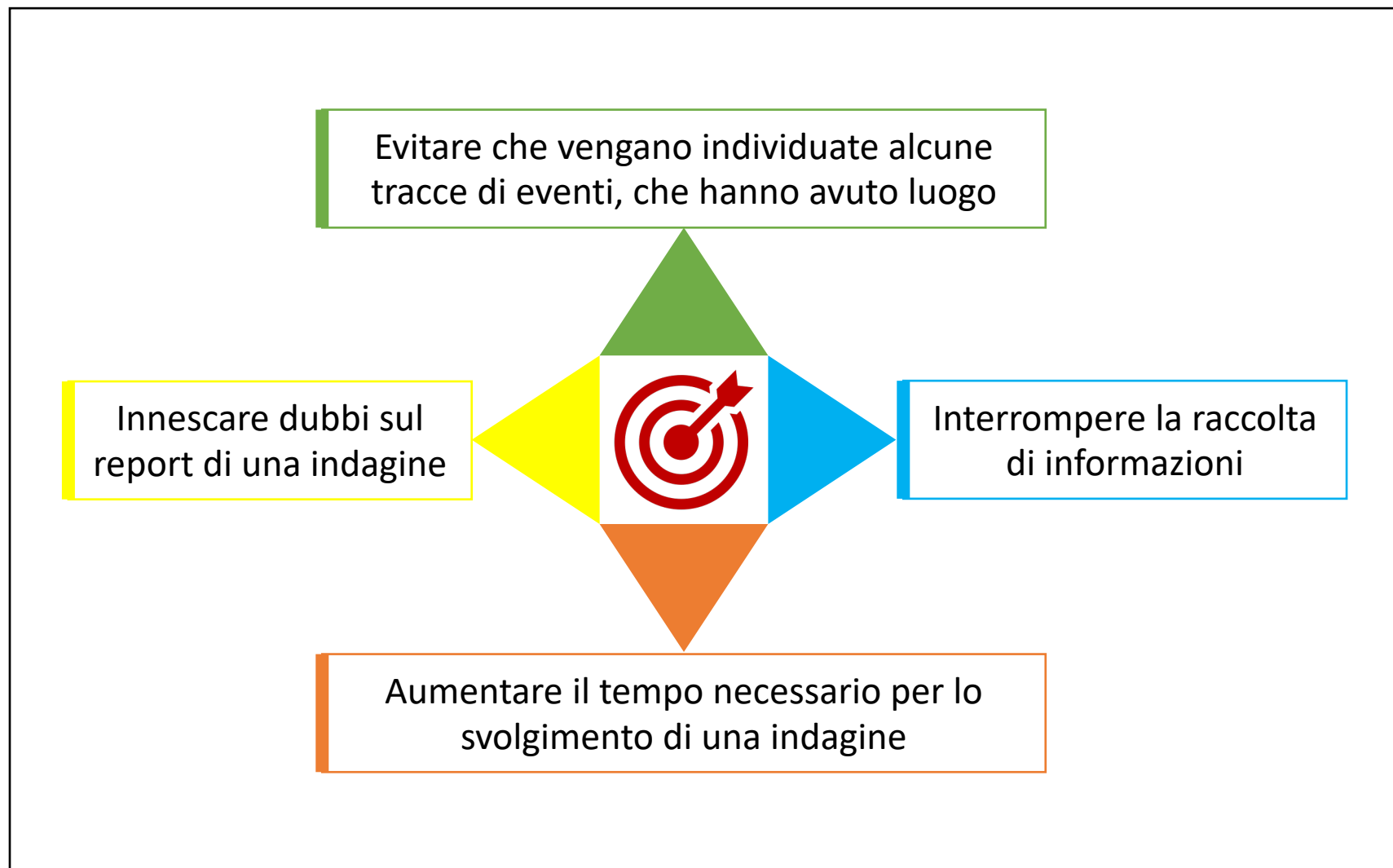
*L'Anti-Forensics (AF) è una collezione di strumenti e tecniche atte a mettere in difficoltà gli strumenti forensi, gli investigatori ed il normale svolgimento dell'indagine*



Definizione adattata da: **Anti-Forensics: Techniques, Detection and Countermeasures**  
(Riferimento completo nei Riferimenti Bibliografici)

# Anti-Forensics

## Obiettivi Principali



# Anti-Forensics

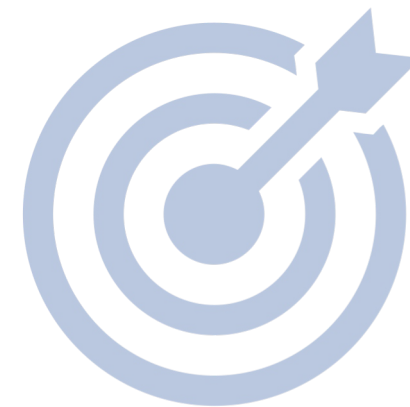
## Ulteriori Obiettivi

Forzare i tool forensi a rilevare la propria presenza

Sovvertire gli strumenti forensi (ovvero, utilizzarli come tool per l'anti-forensics)

Effettuare un attacco diretto all'investigatore forense

Non lasciare tracce dell'esecuzione di un tool per l'anti-forensics



# **Tecniche per l'Anti-Forensics**

## **Introduzione e Nozioni**

# Tecniche per l'Anti-Forensics

## Principali Categorie

Nascondere/Eliminare le Evidenze

Minimizzare le evidenze, provenienti dai tools per l'AF

Sfruttare bug dei tool per l'investigazione forense

Rilevare l'utilizzo di tool per l'investigazione forense

# Tecniche per l'Anti-Forensics

## Principali Categorie

### **Nascondere/Eliminare le Evidenze**

Minimizzare le evidenze, provenienti dai tools per l'AF

Sfruttare bug dei tool per l'investigazione forense

Rilevare l'utilizzo di tool per l'investigazione forense

# Tecniche per l'Anti-Forensics

## Nascondere/Eliminare le Evidenze

### Nascondere/Eliminare le Evidenze

#### *Esempi nel Mondo Fisico*

Nascondere/eliminare l'arma del delitto, pulire una superficie contenente impronte digitali, ecc.



# Tecniche per l'Anti-Forensics

## Nascondere/Eliminare le Evidenze

### Nascondere/Eliminare le Evidenze

- Sovrascrittura di Dati e Metadati
- Crittografia e Information Hiding

# Tecniche per l'Anti-Forensics

## Nascondere/Eliminare le Evidenze

### Nascondere/Eliminare le Evidenze

■ Sovrascrittura di Dati e Metadati

■ Crittografia e Information Hiding

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 1/4

- Esistono tool che permettono di sovrascrivere dati potenzialmente rilevanti per l'indagine
- In tal modo, tali informazioni vengono perse
- Questi tool operano tipicamente in tre modalità:
  1. Sovrascrittura dell'intero dispositivo di memorizzazione
  2. Sovrascrittura di singoli file
  3. Sovrascrittura dell'unallocated space, il quale potrebbe contenere file eliminati (ma ancora presenti sul dispositivo di memorizzazione)

# Nascondere/Eliminare le Evidenze

Sovrascrittura di Dati Metadata 1/4

Esempio | 1/2

dall'Argomento 2...

- La pulizia forense, di un disco fisso, prevede la sovrascrittura del contenuto di ciascun settore (di traccia), con valori nulli (zero) o con specifici pattern o con dati random

- Questi tool operano tipicamente in modalità:

1. **Sovrascrittura dell'intero dispositivo di memorizzazione**
2. Sovrascrittura di singoli file
3. Sovrascrittura dell'unallocated space, il quale potrebbe contenere file eliminati (ma ancora presenti sul dispositivo di memorizzazione)

# Nascondere/Eliminare le Evidenze

Sovrascrittura di Dati Metadata 1/4

*Esempio | 2/2*

- Es
  - pc
  - In
- Sovversione** di tool per la **pulizia forense** (ad esempio, il tool DC3DD), al fine di sovrascrivere l'intero dispositivo, per evitare che un investigatore forense possa individuarvi tracce e/o file eliminati (ad esempio, mediante tecniche di file recovery, ecc.)
- Questi tool operano tipicamente in modalità:
1. **Sovrascrittura dell'intero dispositivo di memorizzazione**
  2. Sovrascrittura di singoli file
  3. Sovrascrittura dell'unallocated space, il quale potrebbe contenere file eliminati (ma ancora presenti sul dispositivo di memorizzazione)

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 2/4

- Alcuni tool permettono di sovrascrivere i timestamp contenuti nei metadati del file system
  - Data/ora dell'ultimo accesso a un file
  - Data/ora di creazione di un file
  - Data/ora dell'ultima modifica a un file
  - Data/ora dell'ultima modifica ai metadati del file
- Tali metadati potrebbero essere utilizzati per la realizzazione di timeline tradizionali
  - In questo scenario, l'ordine degli eventi, riportati nella timeline, potrebbe risultare alterato
- Nelle prossime slide verrà mostrato un **tool** che permette di alterare i timestamp

# Nascondere/Eliminare le Evidenze

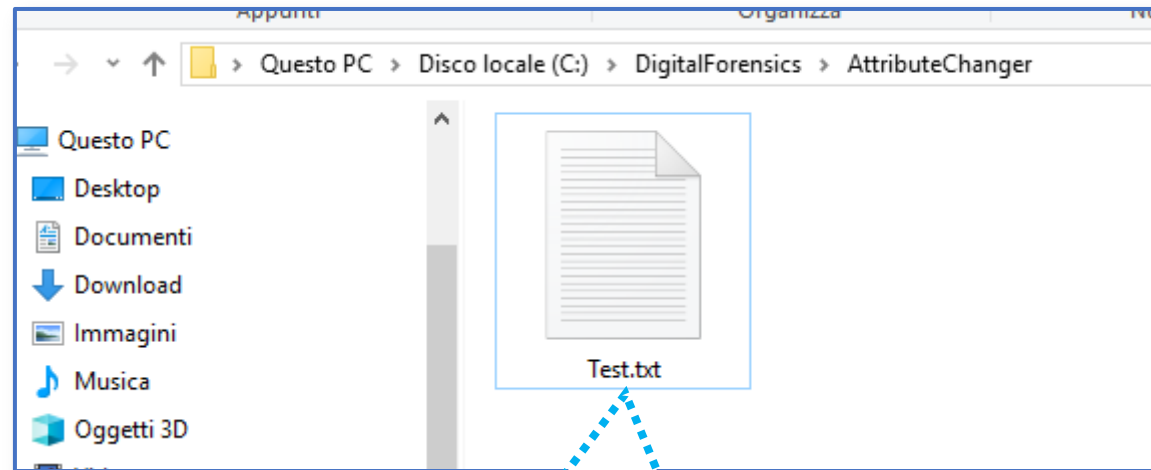
## Sovrascrittura di Dati e Metadati | 3/4

- Il tool **Attribute Changer** è un software gratuito
- Permette, in maniera semplice, di modificare i metadati di un file
- Si integra all'interno dell'interfaccia utente di Windows (Esplora Risorse)
  - Facendo click, con il tasto destro, su un certo file, verrà mostrato il relativo menu contestuale, il quale permetterà la **modifica dei metadati**
- È possibile mantenere un rapporto (*log*), in cui si tiene traccia di ogni modifica ai metadati di un certo file
  - Il log è esportabile in un foglio elettronico
- Link per ulteriori dettagli e download:
  - <https://www.petges.lu/>

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 1/12*



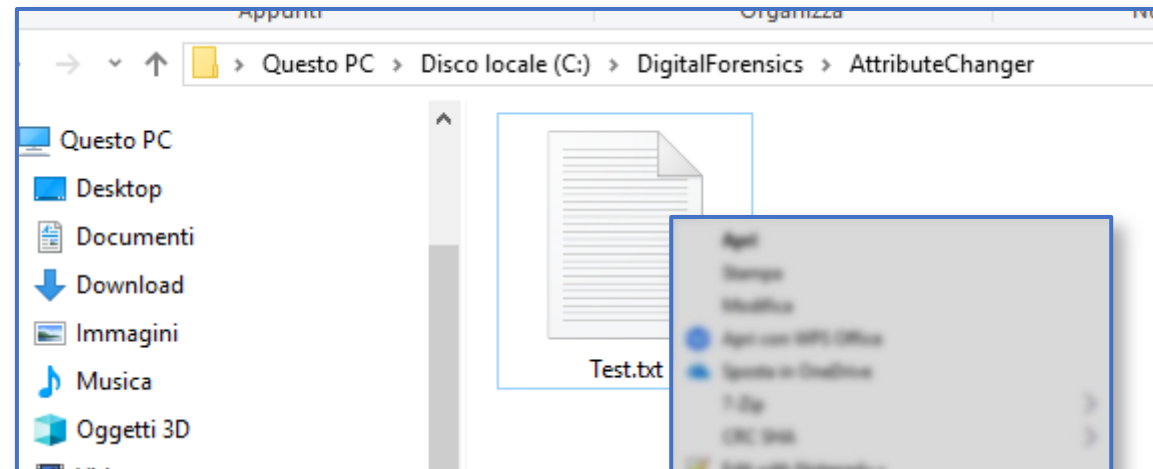
Cliccare con il tasto destro, su un file, per aprire il menu contestuale, relativo a tale file



# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 2/12*

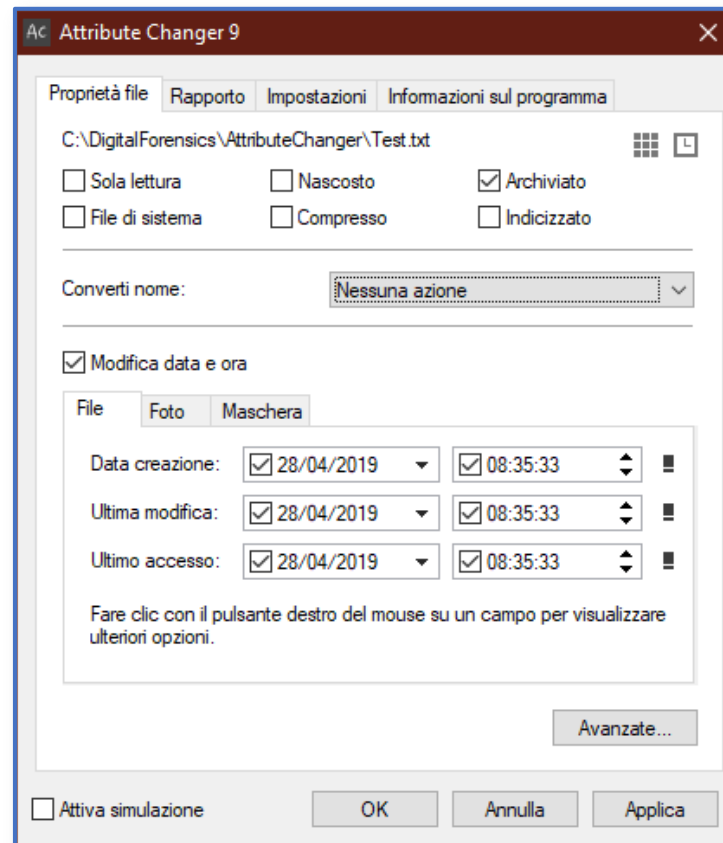


Cliccare sulla voce «**Cambia attributi...**», per alterare gli attributi del file selezionato

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 3/12*



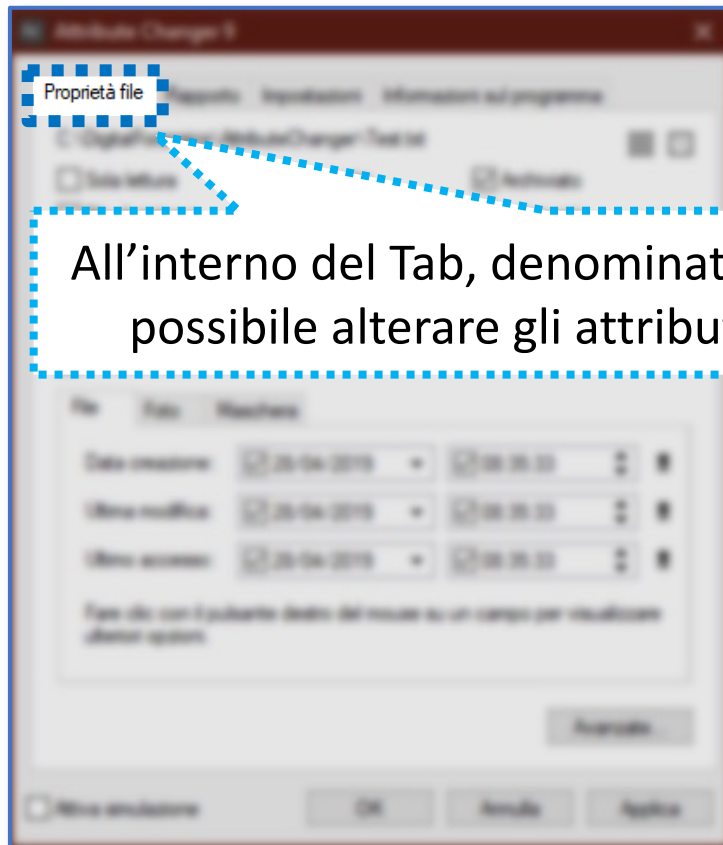
Interfaccia Utente di  
Attribute Changer

Versione Utilizzata: 9.10e  
(Build 2019.4.26)

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 4/12*

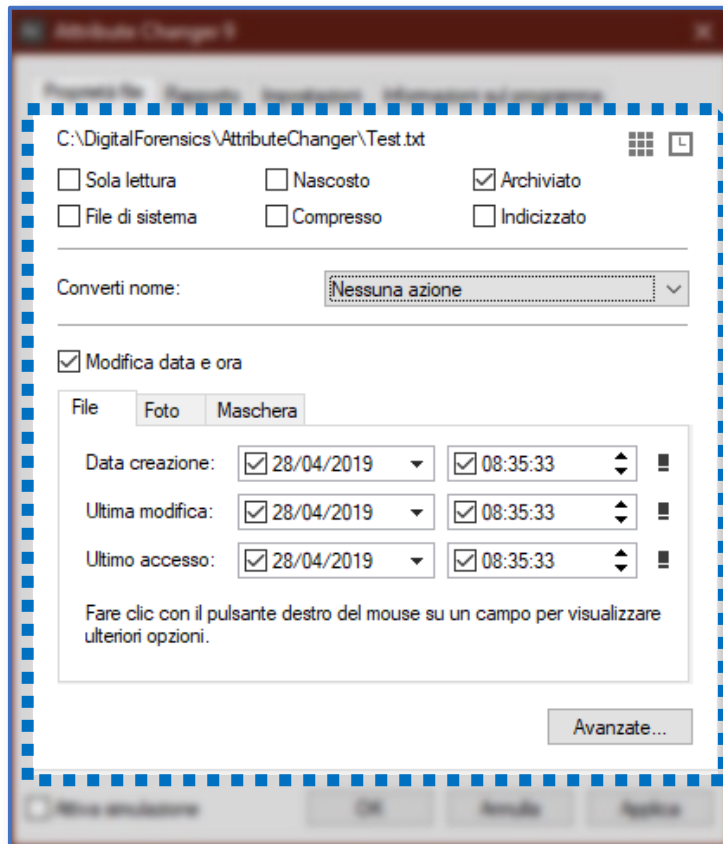


All'interno del Tab, denominato «**Proprietà file**», sarà possibile alterare gli attributi del file selezionato

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

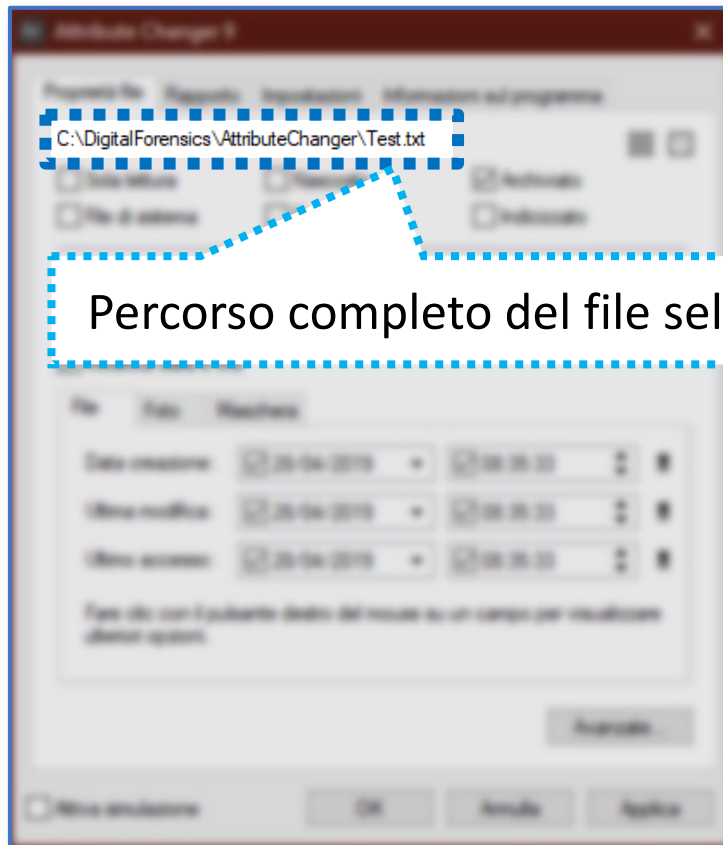
*Esempio di Utilizzo | Attribute Changer | 5/12*



# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 6/12*

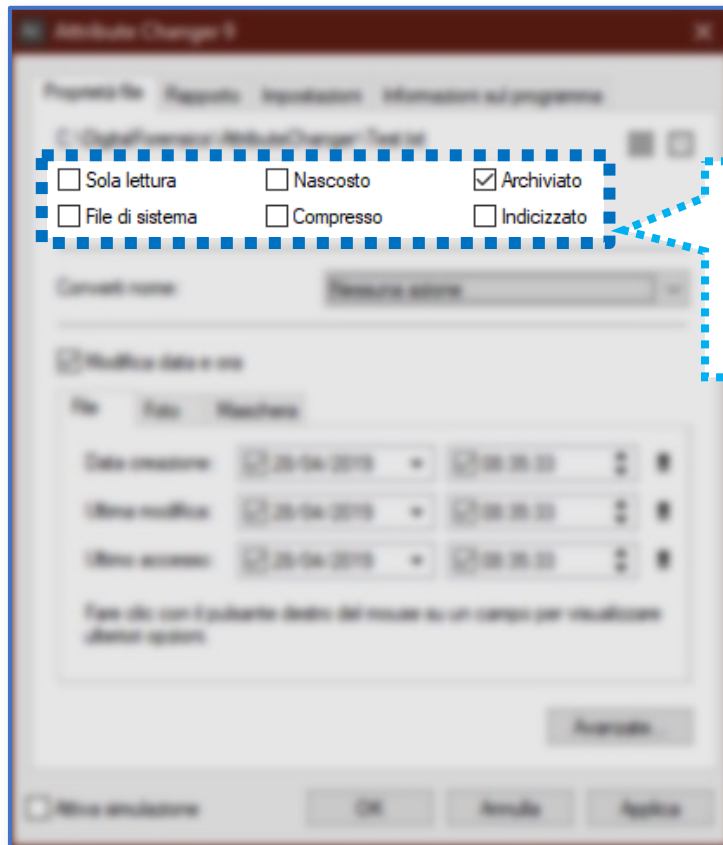


Percorso completo del file selezionato

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 7/12*

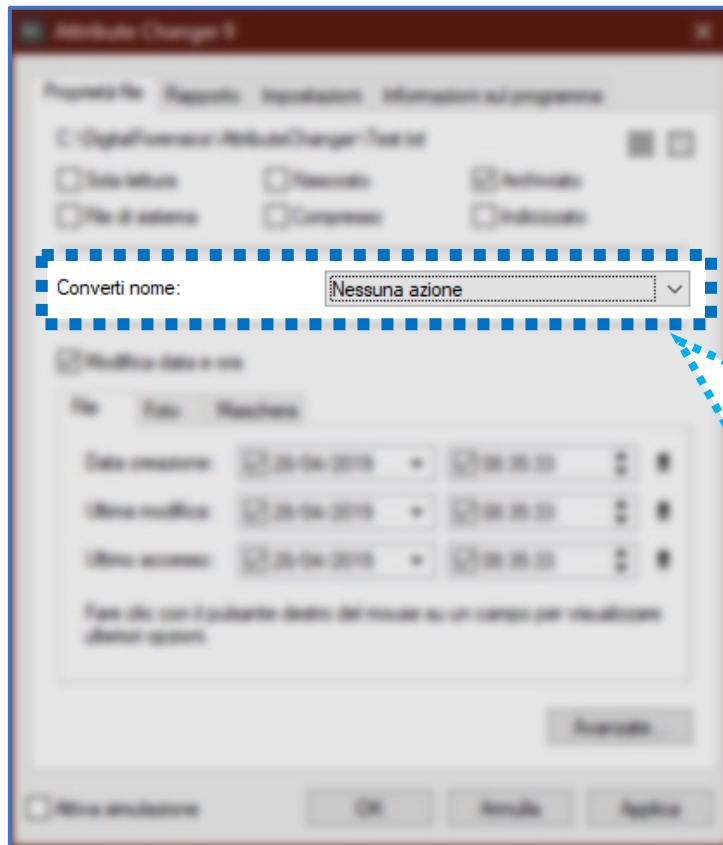


Possibilità di alterare alcuni attributi, relativi al file selezionato (ad esempio, file di sola lettura, nascosto, ecc.)

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 8/12*



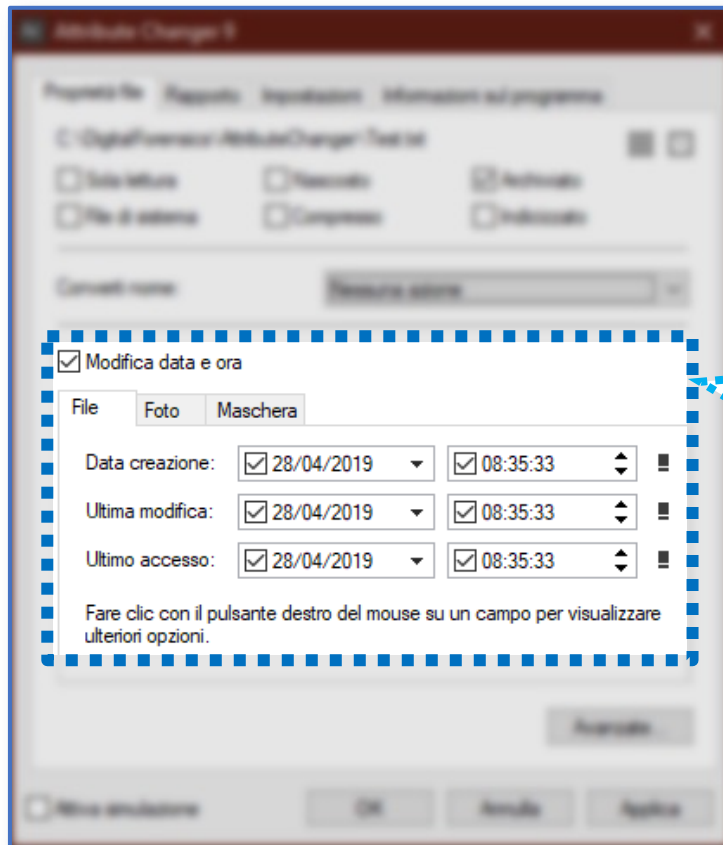
Possibilità di alterare il nome e  
l'estensione del file

- Nessuna azione
- Nessuna azione
- Nome IN MAIUSCOLO
- Estensione IN MAIUSCOLO
- Nome ed estensione IN MAIUSCOLO
- Nome IN MINUSCOLO
- Estensione IN MINUSCOLO
- Nome ed estensione IN MINUSCOLO
- Nome con MAIUSCOLA INIZIALE
- Estensione con MAIUSCOLA INIZIALE
- Nome ed est. con MAIUSCOLA INIZIALE

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 9/12*



Possibilità di alterare tutti i timestamp, del file selezionato



# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

☒ Modifica data e ora

File

Foto

Maschera

Data creazione:

☒ 28/04/2019 ▼

☒ 08:35:33 ▲▼

■

Ultima modifica:

☒ 28/04/2019 ▼

☒ 08:35:33 ▲▼

■

Ultimo accesso:

☒ 28/04/2019 ▼

☒ 08:35:33 ▲▼

■

Fare clic con il pulsante destro del mouse su un campo per visualizzare ulteriori opzioni.

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

Modifica dati e metadati

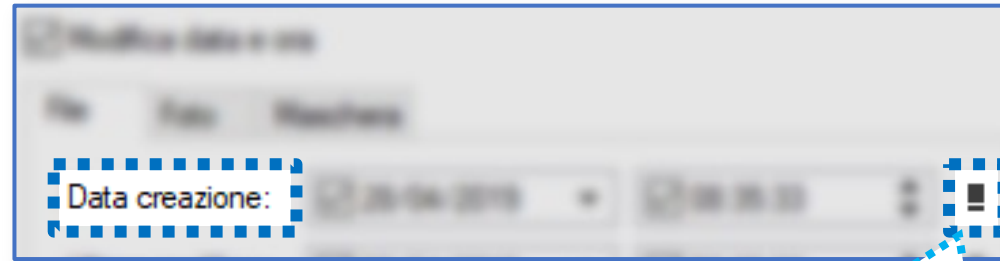
	Nome	Descrizione	Metadati
Data creazione:	<input checked="" type="checkbox"/> 28/04/2019 ▼	<input checked="" type="checkbox"/> 08:35:33 ▲▼	
Ultima modifica:	<input checked="" type="checkbox"/> 28/04/2019 ▼	<input checked="" type="checkbox"/> 08:35:33 ▲▼	
Ultimo accesso:	<input checked="" type="checkbox"/> 28/04/2019 ▼	<input checked="" type="checkbox"/> 08:35:33 ▲▼	

Tipi di dati: ☐ Metadati ☐ Dati del record ☐ Un campo per modificare

Possibilità di specificare, in maniera esplicita, la data e/o l'ora, per ciascun timestamp

# Nascondere/Eliminare le Evidenze

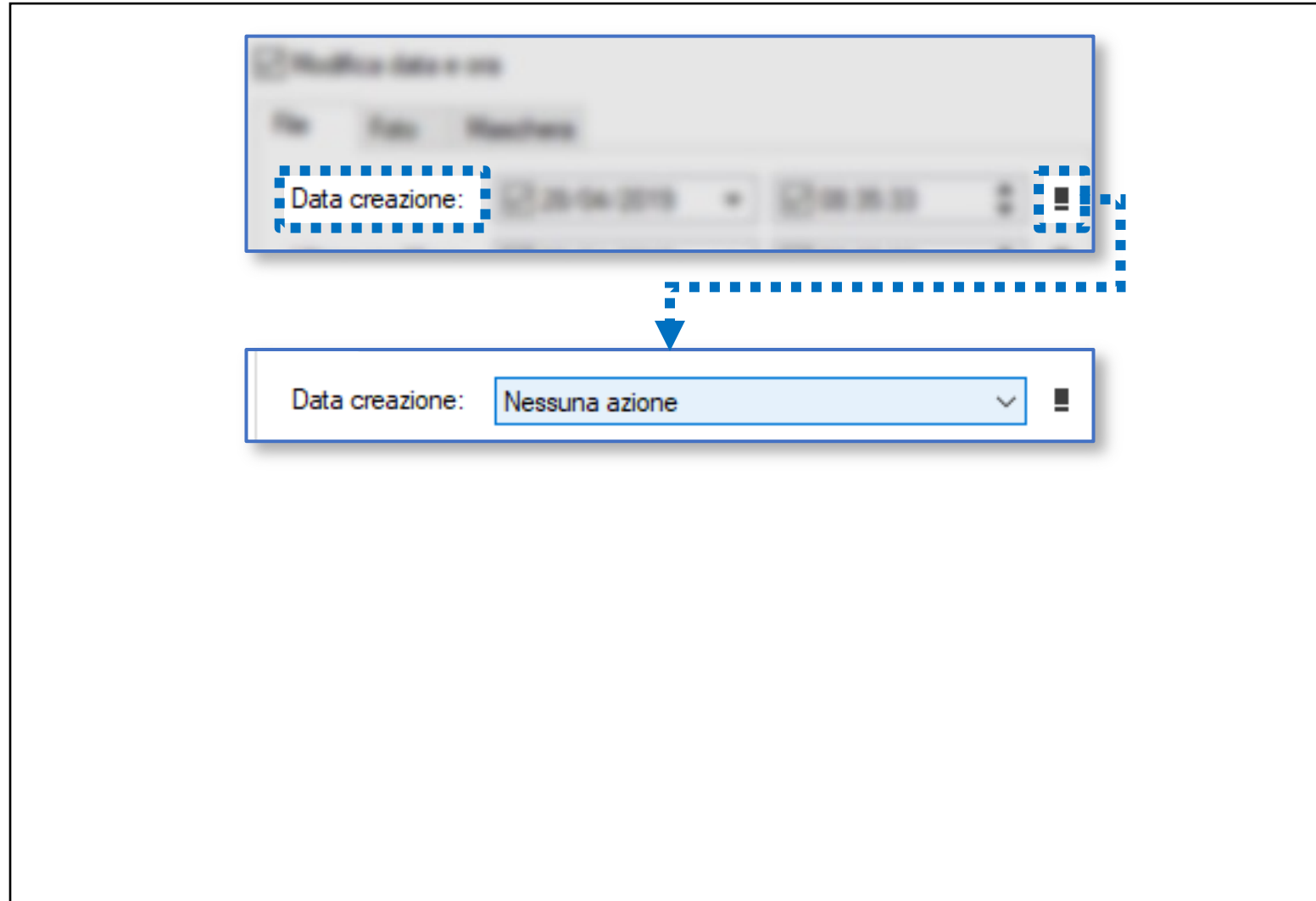
## Sovrascrittura di Dati e Metadati | 4/4



Alternativamente, cliccando su questo tasto, è possibile selezionare ulteriori opzioni per l'alterazione di un timestamp (in questo caso, si tratta del file relativo alla creazione del file)

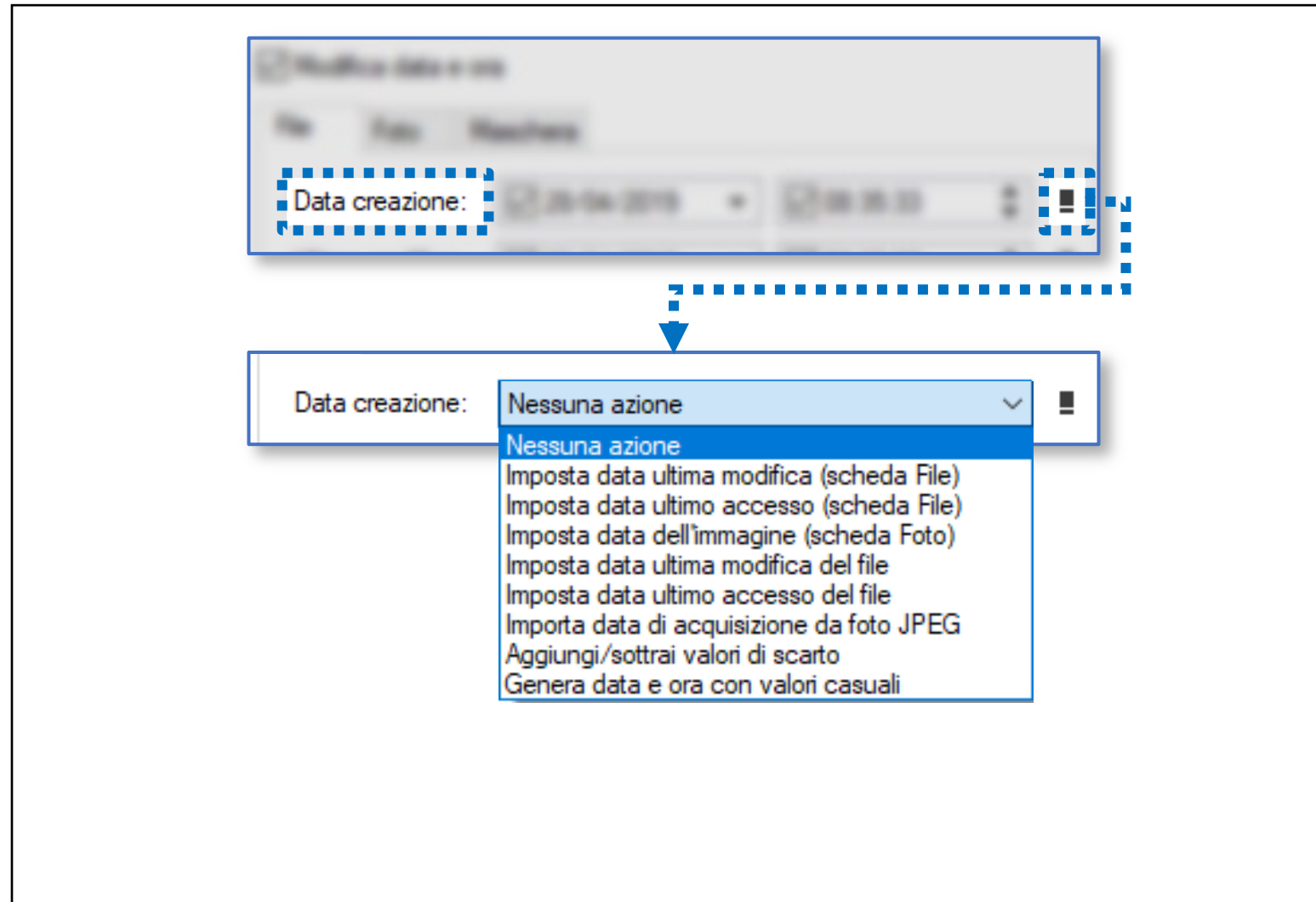
# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4



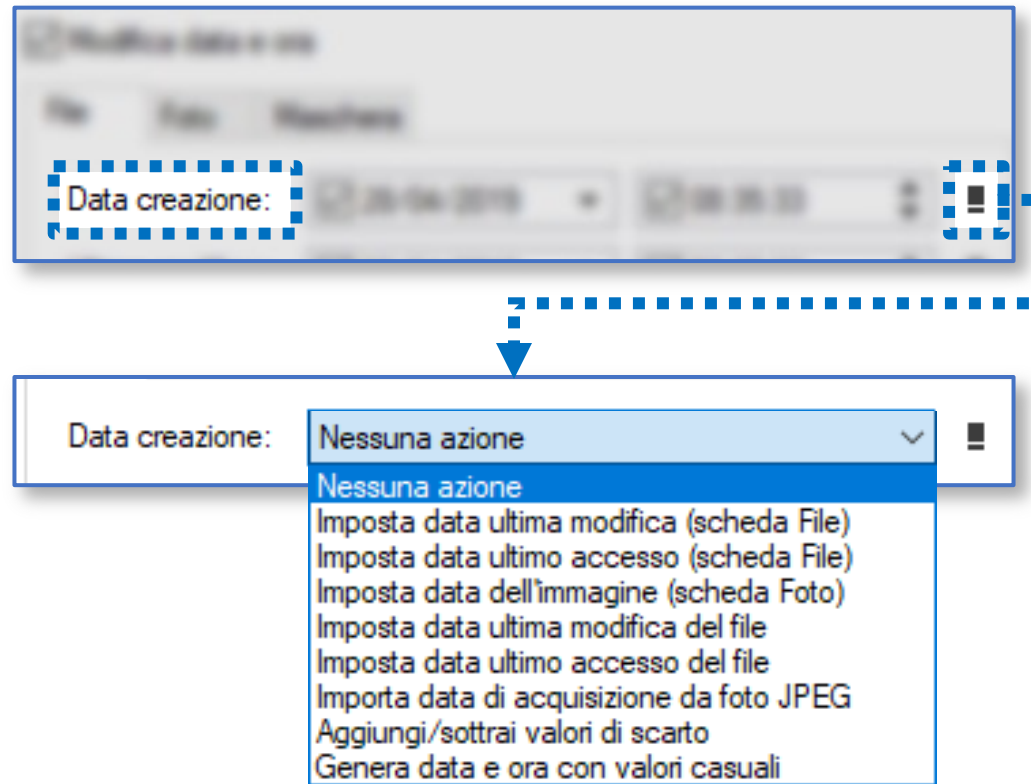
# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4



# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

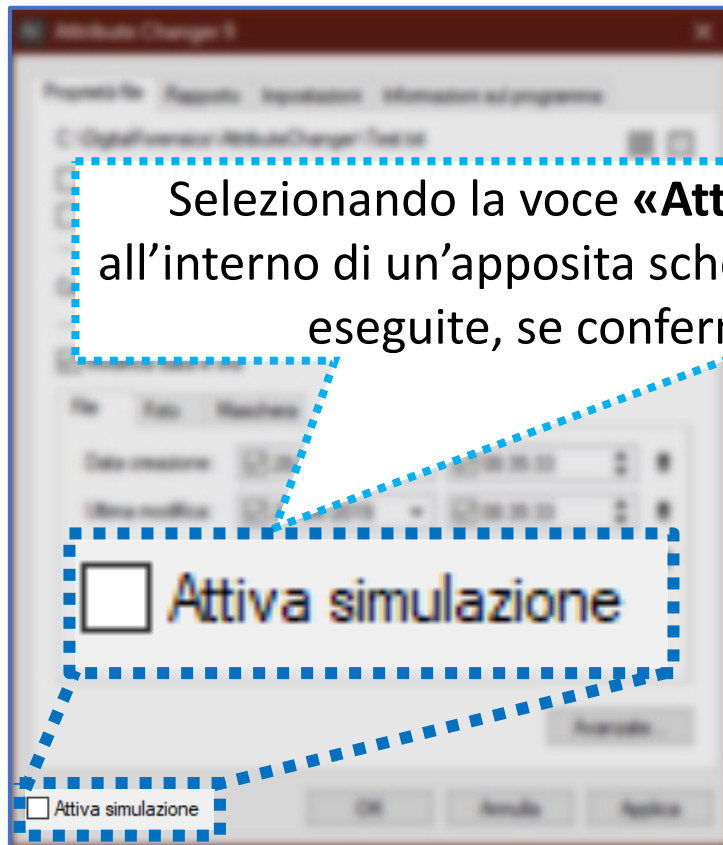


Le ulteriori opzioni disponibili per l'alterazione del timestamp (ad esempio, modificare la data e l'ora, in maniera casuale, da un range di date, che può essere indicato dall'utente)

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 10/12*



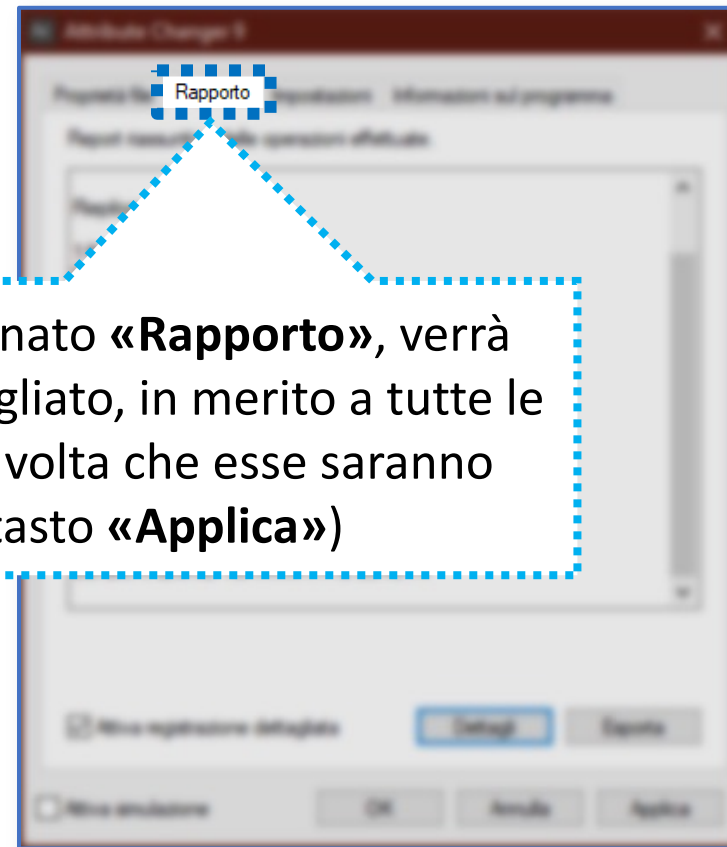
Selezionando la voce «**Attiva simulazione**», verranno mostrate, all'interno di un'apposita schermata, tutte le alterazioni, che verranno eseguite, se confermate, nella suddetta schermata

# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 11/12*

All'interno del Tab, denominato «**Rapporto**», verrà visualizzato il rapporto dettagliato, in merito a tutte le alterazioni effettuate, una volta che esse saranno confermate (con il tasto «**Applica**»)



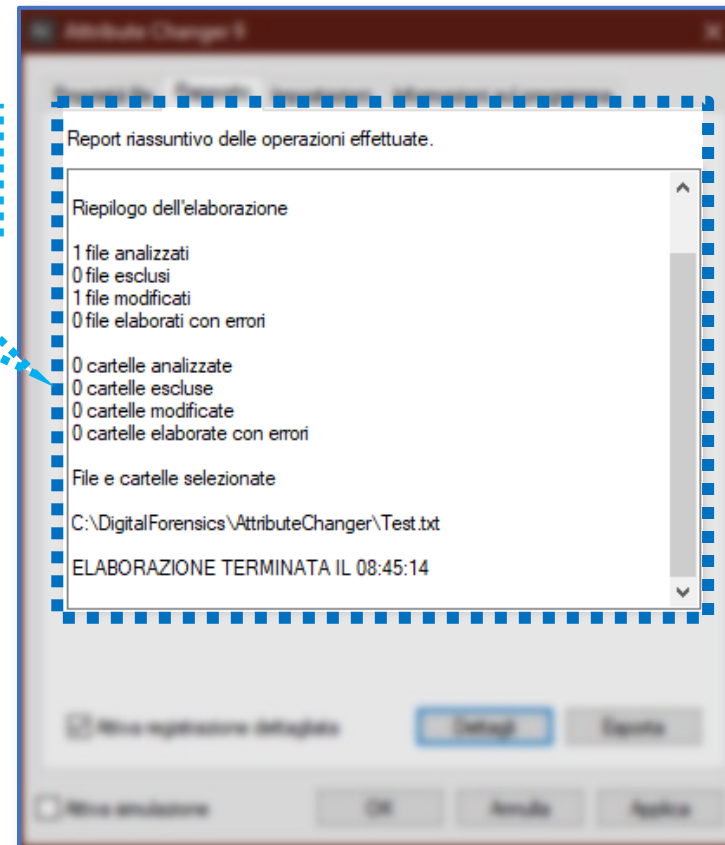


# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 12/12*

*Esempio di un Rapporto*

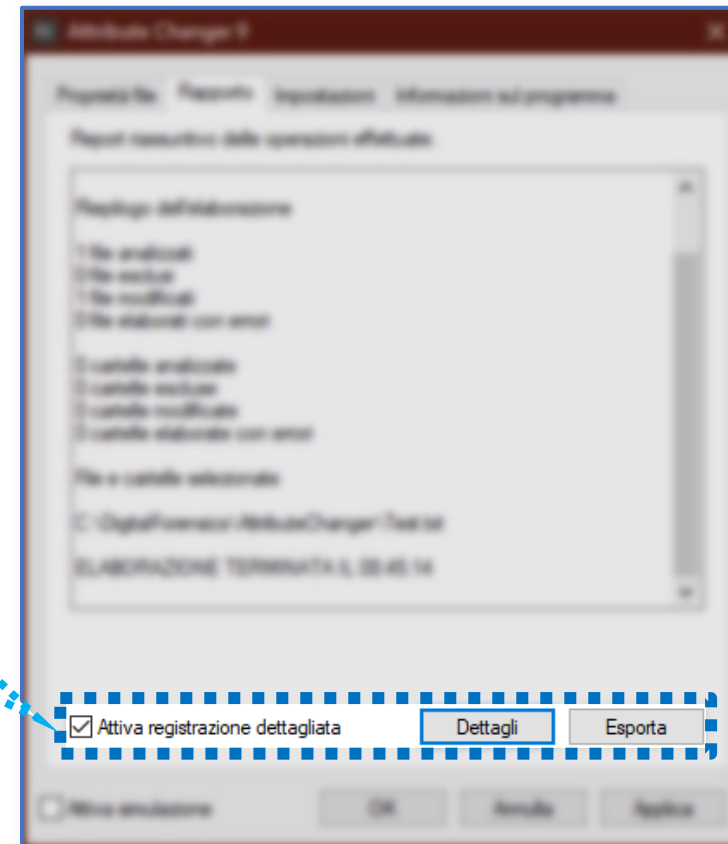


# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

*Esempio di Utilizzo | Attribute Changer | 12/12*

Possibilità di visualizzare eventuali ulteriori dettagli e/o di esportare, il rapporto in un foglio di calcolo



# Nascondere/Eliminare le Evidenze

## Sovrascrittura di Dati e Metadati | 4/4

- *Un altro tool per la Sovrascrittura di Metadati*
  - **Timestomp [Metasploit]**
    - Permette di sovrascrivere i metadati, relativi al file system NTFS
    - Link per approfondimenti:
      - <https://www.offensive-security.com/metasploit-unleashed/timestomp/>



# Tecniche per l'Anti-Forensics

## Nascondere/Eliminare le Evidenze

### Nascondere/Eliminare le Evidenze

- Sovrascrittura di Dati e Metadati
- Crittografia e Information Hiding

# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 1/10

- La **crittografia** e gli approcci di **information hiding** (occultamento di dati), possono essere utilizzati contro la maggior parte delle tecniche forensi
- La **crittografia** è particolarmente efficace per occultare dati
  - Tuttavia, i dati crittografati sono **facilmente rilevabili**
    - Infatti, i dati crittografati hanno un'entropia elevata
    - Inoltre, diversi tool per la crittografia inglobano metadati o header particolari all'interno dei file e ciò contribuisce a renderli riconoscibili

# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 1/10

- La **crittografia** e gli approcci di **information hiding** (occultamento di dati), possono essere utilizzati contro la maggior parte delle tecniche forensi

### OSSERVAZIONE IMPORTANTE

- Difficilmente, partendo da un file cifrato, è possibile recuperarne il contenuto originale

Tuttavia, il semplice fatto che la crittografia sia stata utilizzata potrebbe attirare l'attenzione dell'investigatore

- Inoltre, diversi tool per la crittografia, inglobano metadati o header particolari, all'interno dei file e ciò contribuisce a renderli riconoscibili

# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 2/10

- In questa categoria, possiamo individuare le seguenti tecniche per l'anti-forensics:
  - File System Crittografato
  - Protocolli di rete crittografati
  - Information Hiding

# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 3/10

- In questa categoria, possiamo individuare le seguenti tecniche per l'anti-forensics:
  - File System Crittografato
  - Protocolli di rete crittografati
  - Information Hiding



# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 4/10

- Un file system crittografato (detto anche **cryptographic file systems**) effettua la cifratura dei file
  - La cifratura viene effettuata quando i file vengono memorizzati sul dispositivo di memorizzazione
  - I file vengono decifrati solo quando vi è necessità di effettuare delle operazioni su di essi (ad esempio, lettura/scrittura del file, ecc.)
- Un investigatore, quindi, **non** può analizzare i file, contenuti in un file system siffatto, poiché essi sono cifrati

# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 5/10

- In questa categoria, possiamo individuare le seguenti tecniche per l'anti-forensics:
  - File System Crittografato
  - **Protocolli di rete crittografati**
  - Information Hiding

# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 6/10

- Il traffico di rete può essere crittografato
- Esistono diversi protocolli che permettono di crittografare il contenuto del traffico:
  - Secure Sockets Layer (SSL)
  - Secure SHell (SSH)
- L'idea di base è che i pacchetti vengono cifrati ed incapsulati
- Esiste poi l'**onion routing**, il quale fa uso di nod  
intermediari e cifratura telescopica grazie ai quali è  
possibile proteggere il traffico di rete da eventuali  
analisi

# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 7/10

- In questa categoria, possiamo individuare le seguenti tecniche per l'anti-forensics:
  - File System Crittografato
  - Protocolli di rete crittografati
  - Program Packers
  - **Information Hiding**

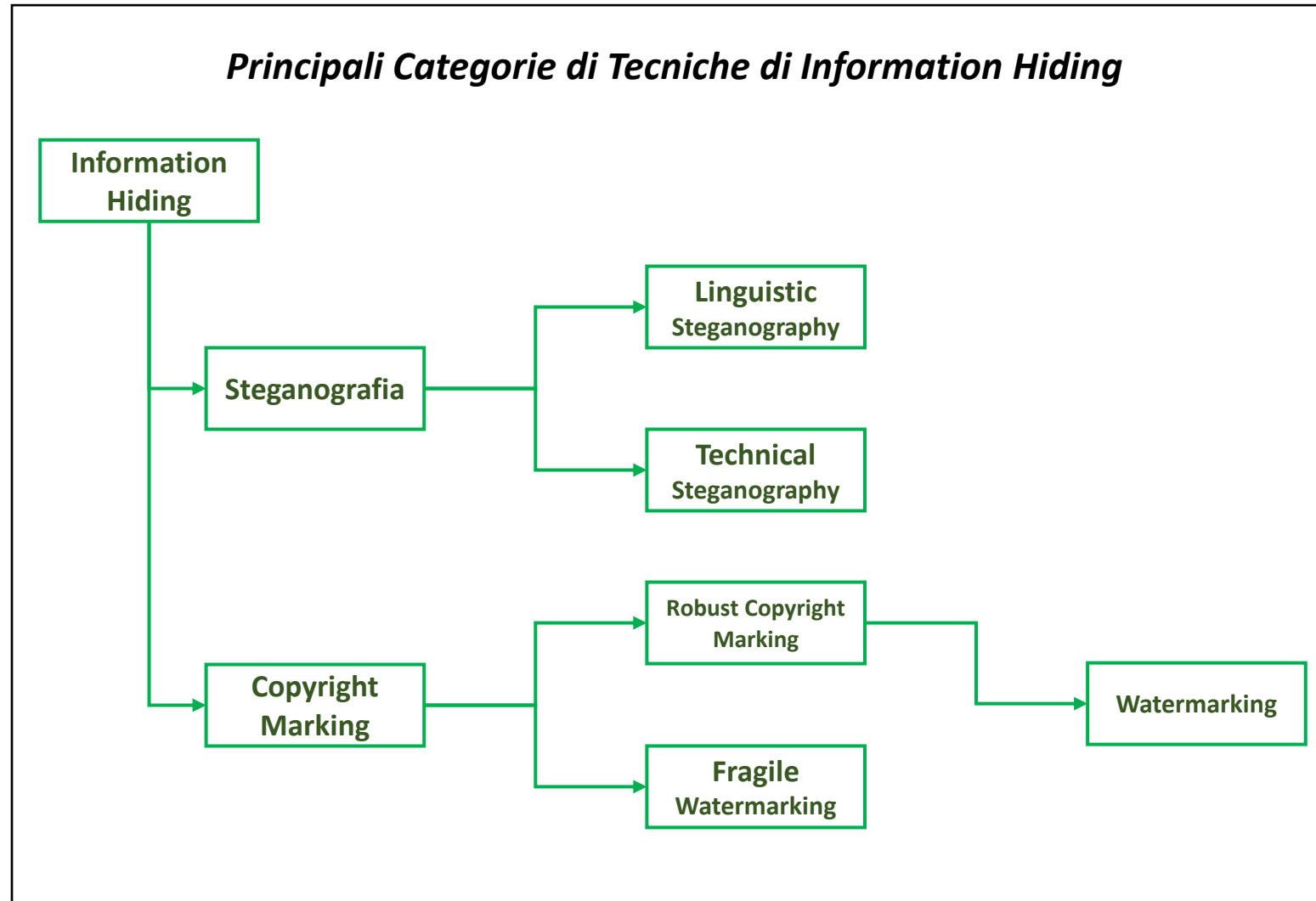
# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 8/10

- Mediante le tecniche di **information hiding** è possibile nascondere informazioni, in diverse tipologie di file:
  - Immagini
  - Audio
  - Video
  - Documenti
    - File di Testo Formattati
    - Presentazioni
    - Fogli di Calcolo
    - Portable Document Format (PDF)
  - Ecc.

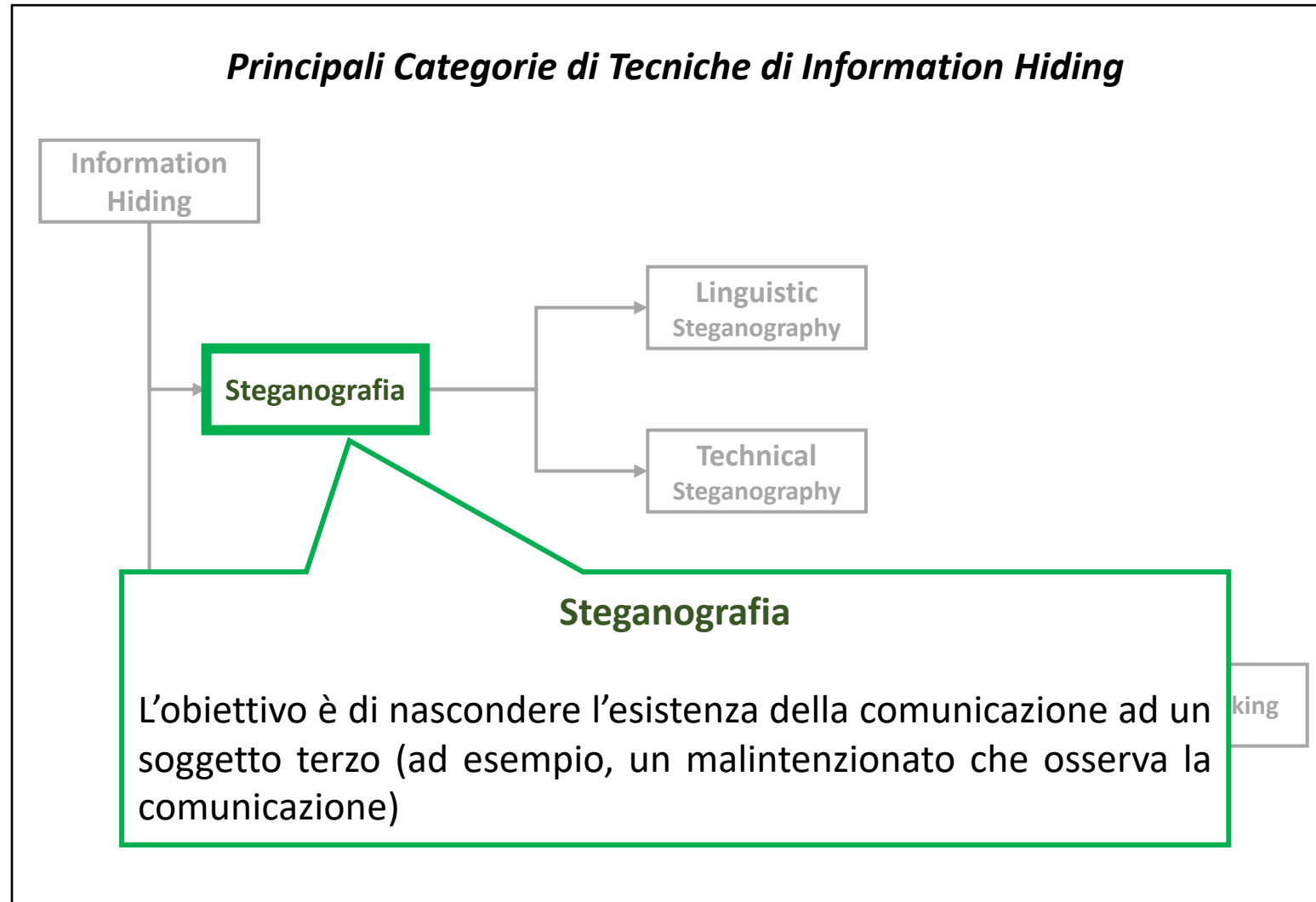
# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 9/10



# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 9/10



# Tecniche per l'Anti-Forensics

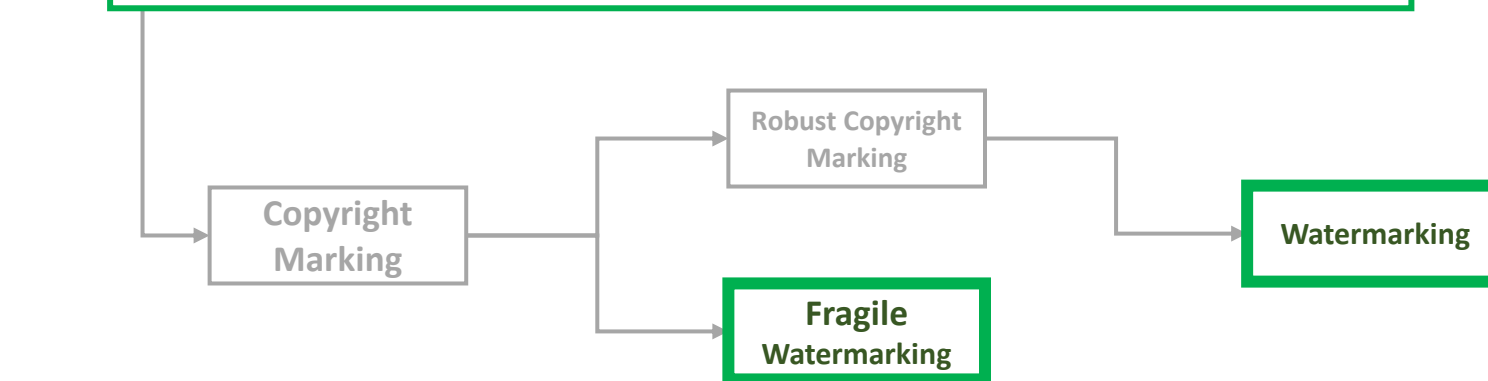
## Crittografia e Information Hiding | 9/10

### Watermarking | 1/3

Mediante le tecniche di watermarking, è possibile nascondere un «watermark» (o «*filigrana*»), all'interno di dati (generalmente, si tratta di dati multimediali, come, ad esempio, immagini, video, audio, ecc.)

Un watermark può essere una specifica sequenza di bit, una stringa, un semplice logo

Queste tecniche vengono principalmente impiegate per la protezione del copyright dei dati





# Tecniche per l'Anti-Forensics

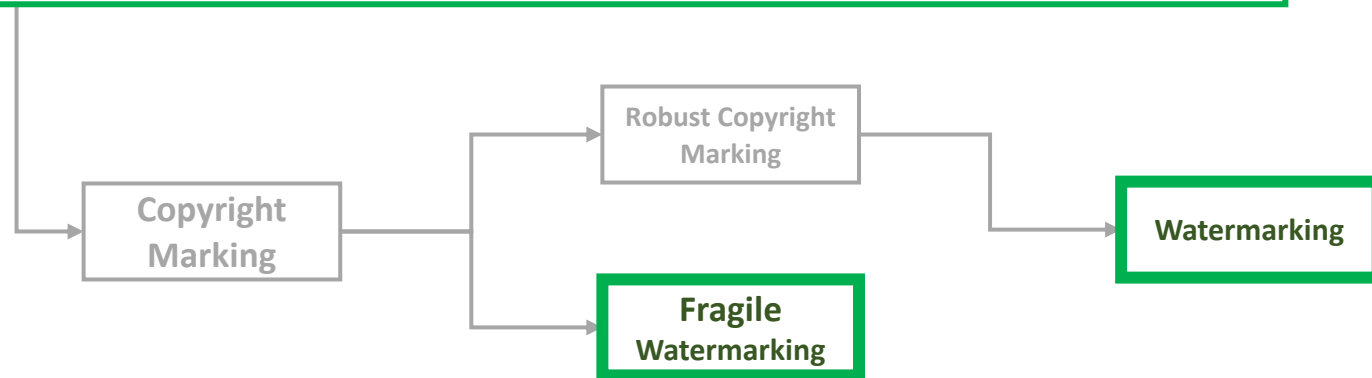
## Crittografia e Information Hiding | 9/10

### Watermarking | 2/3

Ad esempio, all'interno di una immagine, si nasconde un watermark (ad esempio, l'identificativo dell'autore di tale immagine, ecc.)

Da copia dell'immagine, utilizzata senza autorizzazione dell'autore, potrebbe essere estratta la «filigrana» suddetta sequenza di bit, dalla copia, e l'autore effettivo, potrebbe rivendicare la proprietà intellettuale (copyright) dell'immagine

Info  
H



# Tecniche per l'Anti-Forensics

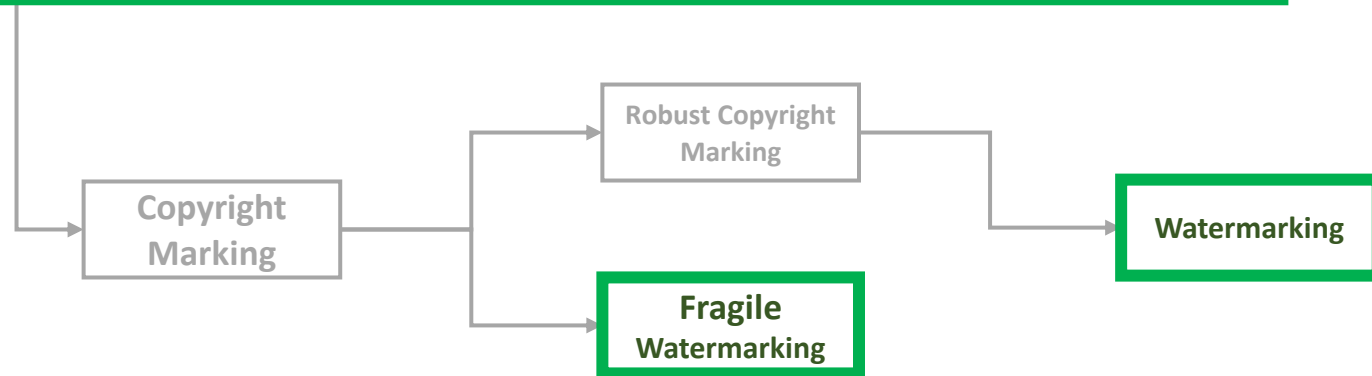
## Crittografia e Information Hiding | 9/10

### Watermarking | 3/3



*Esempio di Filigrana («non digitale»)  
in una Banconota da 20€*

Fonte: [https://upload.wikimedia.org/wikipedia/commons/8/82/Watermarks\\_20\\_Euro.jpg](https://upload.wikimedia.org/wikipedia/commons/8/82/Watermarks_20_Euro.jpg)



# Tecniche per l'Anti-Forensics

## Crittografia e Information Hiding | 10/10

- Esistono tool che permettono di nascondere dati, all'interno delle strutture del file system o del S.O.
- *Esempi*
  - **Slacker [Metasploit]**
    - È in grado di nascondere dati all'interno dello *slack space*, nel file system FAT oppure NTFS
      - Link per approfondimenti:
        - <https://www.bishopfox.com/resources/tools/other-free-tools/mafia/>
  - **StegoMFT**
    - È in grado di nascondere dati all'interno della Master File Table (MFT), del file system NTFS
      - Link per approfondimenti
        - <https://github.com/jschicht/StegoMft>

# Tecniche per l'Anti-Forensics

## Principali Categorie

Nascondere/Eliminare le Evidenze

**Minimizzare le evidenze, provenienti dai tools per l'AF**

Sfruttare bug dei tool per l'investigazione forense

Rilevare l'utilizzo di tool per l'investigazione forense

# Tecniche per l'Anti-Forensics

Minimizzare le evidenze, provenienti dai tools per l'AF

## Minimizzare le evidenze, provenienti dai tools per l'AF


- Memory Injection
- Live CD, Penne USB *bootable* e Virtual Machine
- Accessi anonimi e memorizzazioni anonime

# Tecniche per l'Anti-Forensics

Minimizzare le evidenze, provenienti dai tools per l'AF

## Minimizzare le evidenze, provenienti dai tools per l'AF

 Memory Injection

 Live CD, Penne USB *bootable* e Virtual Machine

 Accessi anonimi e memorizzazioni anonime

# Minimizzare le evidenze, provenienti dai tools per l'AF

## Memory Injection

- Sfruttando le vulnerabilità di **buffer overflow**, è possibile iniettare codice malevolo nello spazio di indirizzi di un programma «vittima» in esecuzione
  - In tal modo, il comportamento del programma «vittima» viene alterato
- Tradizionalmente, i buffer overflow sono utilizzati come **punto di ingresso in un sistema remoto**
  - In questo scenario, l'attaccante è in grado di memorizzare i tool per l'AF, sul sistema remoto

# Tecniche per l'Anti-Forensics

Minimizzare le evidenze, provenienti dai tools per l'AF

## Minimizzare le evidenze, provenienti dai tools per l'AF

Memory Injection

Live CD, Penne USB *bootable* e Virtual Machine

Accessi anonimi e memorizzazioni anonime



# Minimizzare le evidenze, provenienti dai tools per l'AF

## Live CD, Penne USB bootable e Virtual Machine | 2/6



Live CD



Penne USB  
*bootable*



Machine Virtuali

**Live CD, penne USB *bootable* e macchine virtuali** possono essere utilizzati come strumenti per l'anti-forensics

In genere, tali strumenti lasciano poche tracce

# Minimizzare le evidenze, provenienti dai tools per l'AF

## Live CD, Penne USB bootable e Virtual Machine | 3/6



**Live CD**



Penne USB  
*bootable*



Macchine Virtuali

Un Live CD è un supporto di memorizzazione di sola lettura (ad esempio, un CD-ROM, un DVD-ROM, ecc.)

Permette l'avvio e l'esecuzione di un S.O., senza che il S.O. venga effettivamente installato sulla macchina

# Minimizzare le evidenze, provenienti dai tools per l'AF

## Live CD, Penne USB bootable e Virtual Machine | 4/6



Live CD



Penne USB  
*bootable*



Machine Virtuali

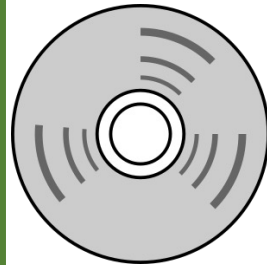
Analogamente ai Live CD, una penna USB bootable permette di avviare ed eseguire un S.O. senza che esso venga installato sulla macchina

La principale differenza consiste nel fatto che è possibile effettuare operazioni di scrittura in tali dispositivi

In tal modo, ad esempio, un attaccante potrebbe memorizzare dei file, creati direttamente sul S.O. che è stato avviato dalla penna USB

# Minimizzare le evidenze, provenienti dai tools per l'AF

## Live CD, Penne USB bootable e Virtual Machine | 5/6



**Live CD**



**Penne USB  
*bootable***



**Machine Virtuali**

Con un Live CD o una penna USB bootable, è possibile quindi utilizzare un certo PC, per effettuare eventuali attacchi, non lasciando alcuna traccia (o lasciandone pochissime) del suddetto attacco

# Minimizzare le evidenze, provenienti dai tools per l'AF

## Live CD, Penne USB bootable e Virtual Machine | 6/6



Live CD



Penne USB  
*bootable*



Macchine Virtuali

Si tratta di un S.O. «*client*», il quale viene eseguito in un programma (ad esempio, VMWare, Oracle VirtualBox, ecc.)

Il sistema che esegue il suddetto programma e, conseguentemente, il S.O. «*client*», viene detto sistema «*host*»

Sul sistema «*host*», vengono memorizzati gli «*stati*» del S.O. «*client*» ed un piccolo insieme di file (file di configurazione, ecc.)

# Minimizzare le evidenze, provenienti dai tools per l'AF

## Live CD, Penne USB bootable e Virtual Machine | 6/6



Live CD



Penne USB  
*bootable*



Macchine Virtuali

A seguito dello svolgimento di un attacco e/o di azioni malevole, sul S.O. «client», il malintenzionato dovrebbe solo cancellare in «*modo sicuro*» (minimizzando le tracce della cancellazione) i file associati alla macchina virtuale

# Tecniche per l'Anti-Forensics

Minimizzare le evidenze, provenienti dai tools per l'AF

## Minimizzare le evidenze, provenienti dai tools per l'AF

Memory Injection

Live CD, Penne USB *bootable* e Virtual Machine

Accessi anonimi e memorizzazioni anonime

# Minimizzare le evidenze, provenienti dai tools per l'AF

## Accessi anonimi e memorizzazioni anonime

- Un malintenzionato potrebbe **utilizzare diversi account «anonimi» o falsi**, su vari servizi di Cloud storage online
  - Al momento della creazione di un nuovo account, viene fornita una significativa quantità di spazio
- I malintenzionati potrebbero utilizzare lo spazio fornito dai suddetti account al fine di memorizzare dei tool per l'AF ed eventuali informazioni acquisite





# Tecniche per l'Anti-Forensics

## Principali Categorie

Nascondere/Eliminare le Evidenze

Minimizzare le evidenze, provenienti dai tools per l'AF

**Sfruttare bug dei tool per l'investigazione forense**

Rilevare l'utilizzo di tool per l'investigazione forense

# Tecniche per l'Anti-Forensics

## Sfruttare bug dei tool per l'investigazione forense

### Sfruttare bug dei tool per l'investigazione forense

- Mancato controllo dei dati di input
- Attacchi Denial of Service (DoS)
- Euristiche Fragili

# Tecniche per l'Anti-Forensics

## Sfruttare bug dei tool per l'investigazione forense

### Sfruttare bug dei tool per l'investigazione forense

- Mancato controllo dei dati di input
- Attacchi Denial of Service (DoS)
- Euristiche Fragili

# Sfruttare bug dei tool per l'investigazione forense

## Mancato controllo dei dati di input

- Allo stesso modo di qualsiasi altro software, anche i tool forensi **dovrebbero svolgere adeguati controlli sull'input**, onde evitare di incorrere in potenziali attacchi
  - Ad esempio, attacchi di *buffer overflow*, ecc.
- Gli attacchi ai suddetti tool potrebbero arrecare problemi ed errori durante lo svolgimento dell'indagine forense

# Tecniche per l'Anti-Forensics

## Sfruttare bug dei tool per l'investigazione forense

### Sfruttare bug dei tool per l'investigazione forense

- Mancato controllo dei dati di input
- **Attacchi Denial of Service (DoS)**
- Euristiche Fragili

# Sfruttare bug dei tool per l'investigazione forense

## Attacchi Denial of Service (DoS) | 1/2

- In alcuni casi, l'utilizzo di risorse (CPU, memoria RAM, spazio su disco, ecc.), da parte di alcuni tool forensi, è **dipendente dai dati di input**
  - In questi casi, le suddette risorse potrebbero essere soggette ad attacchi di tipo **DoS** (**D**enial-**o**f-**S**ervice)



# Sfruttare bug dei tool per l'investigazione forense

## Attacchi Denial of Service (DoS) | 2/2

*Esempio | 1/3*

*Attacco mediante tecniche Compressione Dati*

- Mediante tecniche di compressione dati, è possibile produrre un particolare attacco DoS, denominato ***compression bombs attack***
- In dettaglio, vengono realizzati particolari file compressi, denominati *compression bomb*
  - Analizzando questi file, alcuni tool forensi **devono utilizzare notevoli quantitativi di risorse**, soprattutto in termini di spazio del disco

# Sfruttare bug dei tool per l'investigazione forense

## Attacchi Denial of Service (DoS) | 2/2

*Esempio | 2/3*

*Attacco mediante tecniche Compressione Dati*

- Un esempio di compression bomb è il file denominato `42.zip`, di circa **44 KB**



# Sfruttare bug dei tool per l'investigazione forense

## Attacchi Denial of Service (DoS) | 2/2

*Esempio | 2/3*

*Attacco mediante tecniche Compressione Dati*

- Un esempio di compression bomb è il file denominato **42.zip**, di circa **44 KB**



Ulteriori dettagli e download al seguente link:

<https://www.unforgettable.dk/>

# Sfruttare bug dei tool per l'investigazione forense

## Attacchi Denial of Service (DoS) | 2/2

*Esempio | 2/3*

*Attacco mediante tecniche Compressione Dati*

- Il file 42.zip contiene 16 file zippati
  - Ciascuno di tali file contiene ancora 16 file zippati
    - Ciascuno di tali file contiene ancora 16 file zippati
      - Ciascuno di tali file contiene ancora 16 file zippati
        - Ciascuno di tali file contiene ancora 16 file zippati
          - Ciascuno di tali file contiene ancora 16 file zippati
            - Ciascuno dei quali contiene un file da **4.3 GB**

# Sfruttare bug dei tool per l'investigazione forense

## Attacchi Denial of Service (DoS) | 2/2

*Esempio | 3/3*

*Attacco mediante tecniche Compressione Dati*

Dimensione del file 42.zip, una volta estratti tutti i file al suo interno:

4.503.599.626.321.920 Byte → 4.5 PetaByte (PB)

# Tecniche per l'Anti-Forensics

## Sfruttare bug dei tool per l'investigazione forense

### Sfruttare bug dei tool per l'investigazione forense

- Mancato controllo dei dati di input
- Attacchi Denial of Service (DoS)
- Euristiche Fragili

# Tecniche per l'Anti-Forensics

## Euristiche Fragili | 1/2

- Alcuni tool forensi necessitano di **conoscere la tipologia di file**, al fine di permettere una elaborazione **efficiente** ed **efficace**
  - In genere, per identificare la tipologia di un file, i **tool si basano sull'header di un file**

# Tecniche per l'Anti-Forensics

## Euristiche Fragili | 2/2

- Alcuni tool forensi necessitano di conoscere la tipologia di file, al fine di permettere una elaborazione efficiente ed efficace
  - In genere, per identificare la tipologia di un file, i tool si basano sull'header di un file

**Conoscendo le euristiche** utilizzate, un attaccante può sfruttarle in maniera maliziosa

- Ad esempio, l'attaccante può alterare l'header di un file (prima di eliminarlo)
  - Probabilmente, tale file potrebbe non essere ripristinato dai tool di file recovery

# Tecniche per l'Anti-Forensics

## Principali Categorie

Nascondere/Eliminare le Evidenze

Minimizzare le evidenze, provenienti dai tools per l'AF

Sfruttare bug dei tool per l'investigazione forense

**Rilevare l'utilizzo di tool per l'investigazione forense**

# Tecniche per l'Anti-Forensics

## Rilevare l'utilizzo di tool per l'investigazione forense

### Rilevare l'utilizzo di tool per l'investigazione forense



Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T.



Contrastare la Network Forensics



# Tecniche per l'Anti-Forensics

## Rilevare l'utilizzo di tool per l'investigazione forense

### Rilevare l'utilizzo di tool per l'investigazione forense



Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T.



Contrastare la Network Forensics

# Tecniche per l'Anti-Forensics

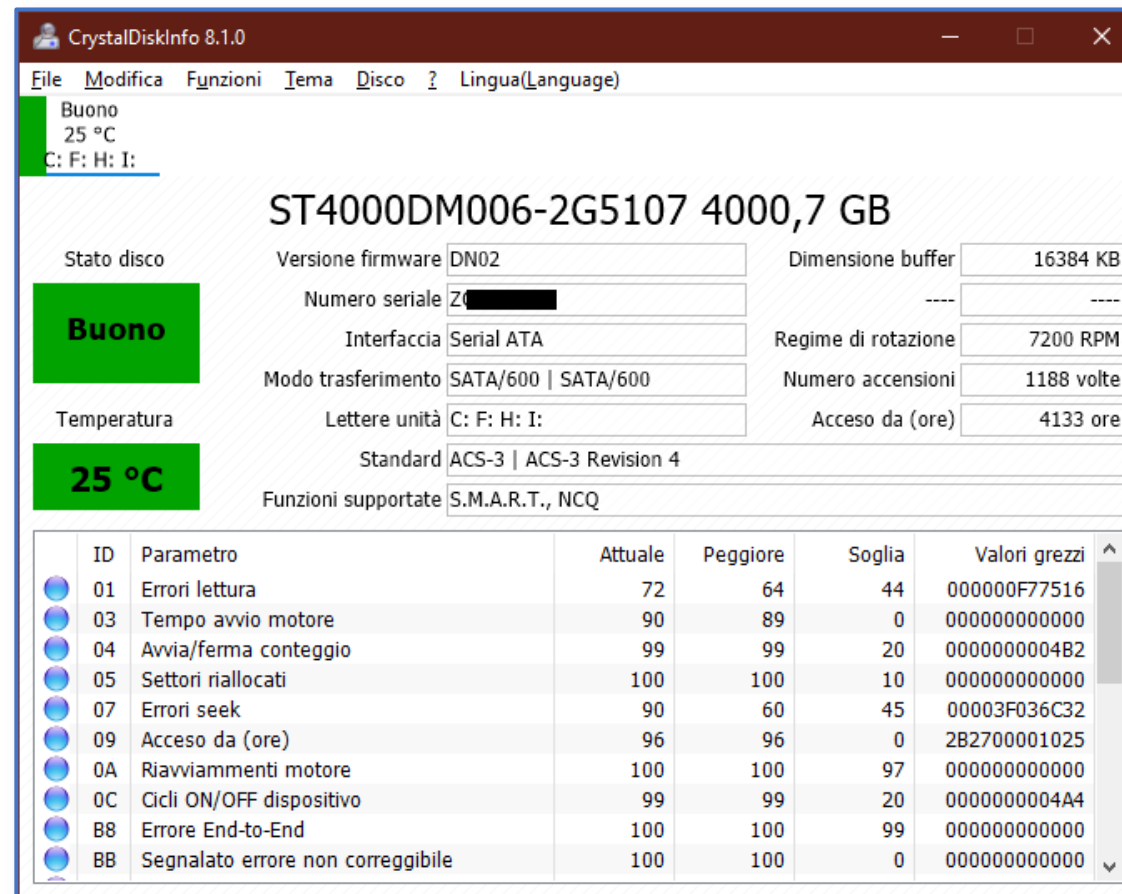
Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 1/4

- La maggior parte dei dischi fissi, integra una tecnologia chiamata S.M.A.R.T.
  - S.M.A.R.T. è l'acronimo di **S**elf-**M**onitoring, **A**nalysis and **R**eporting **T**echnology
- Mediante questa tecnologia, il disco fisso monitora sé stesso (self-monitoring), fornendo diverse informazioni diagnostiche:
  - Il numero totale di accensioni
  - Il tempo totale di attività (ovvero il tempo in cui il disco è stato utilizzato)
  - Eventuali temperature elevate raggiunte dal dispositivo
  - Altri attributi, specificati dal produttore
- Queste informazioni possono essere lette da specifici tool (*esempio nelle prossime slide*)

# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 2/4

*Esempio di informazioni S.M.A.R.T., fornite dal software gratuito  
CrystalDiskInfo (disponibile per S.O. Windows-based)*



The screenshot shows the CrystalDiskInfo 8.1.0 application window. The top menu bar includes File, Modifica, Funzioni, Tema, Disco, and Lingua(Language). The main display area shows the following information:

- Stato disco: **Buono**
- Temperatura: **25 °C**
- Modello: ST4000DM006-2G5107 4000,7 GB
- Versione firmware: DN02
- Numero seriale: Z0 [REDACTED]
- Interfaccia: Serial ATA
- Modo trasferimento: SATA/600 | SATA/600
- Lettere unità: C: F: H: I:
- Standard: ACS-3 | ACS-3 Revision 4
- Funzioni supportate: S.M.A.R.T., NCQ
- Dimensione buffer: 16384 KB
- Regime di rotazione: 7200 RPM
- Numero accensioni: 1188 volte
- Accesso da (ore): 4133 ore

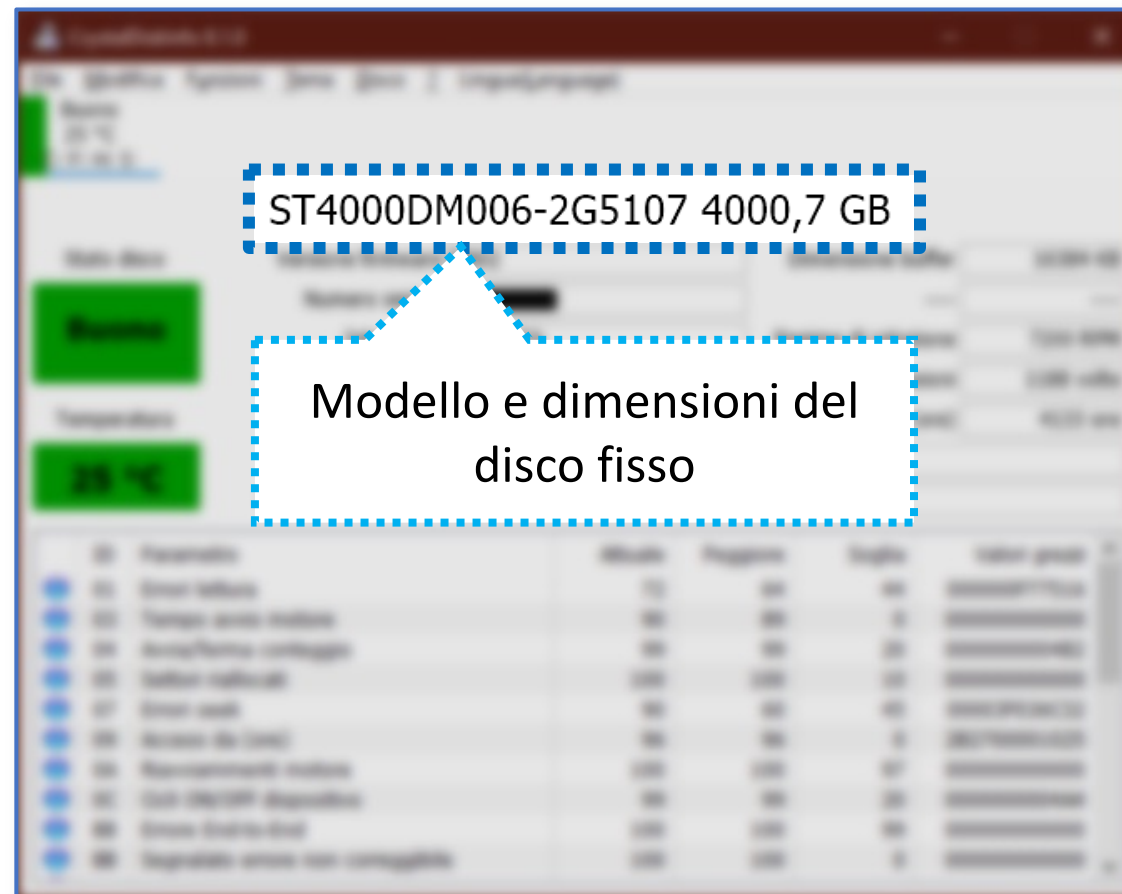
Below this information is a table of S.M.A.R.T. attributes:

ID	Parametro	Attuale	Peggior	Soglia	Valori grezzi
01	Errori lettura	72	64	44	000000F77516
03	Tempo avvio motore	90	89	0	000000000000
04	Avvia/ferma conteggio	99	99	20	0000000004B2
05	Settori riallocati	100	100	10	000000000000
07	Errori seek	90	60	45	00003F036C32
09	Accesso da (ore)	96	96	0	2B2700001025
0A	Riavviammenti motore	100	100	97	000000000000
0C	Cicli ON/OFF dispositivo	99	99	20	0000000004A4
B8	Errore End-to-End	100	100	99	000000000000
BB	Segnalato errore non correggibile	100	100	0	000000000000

# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 2/4

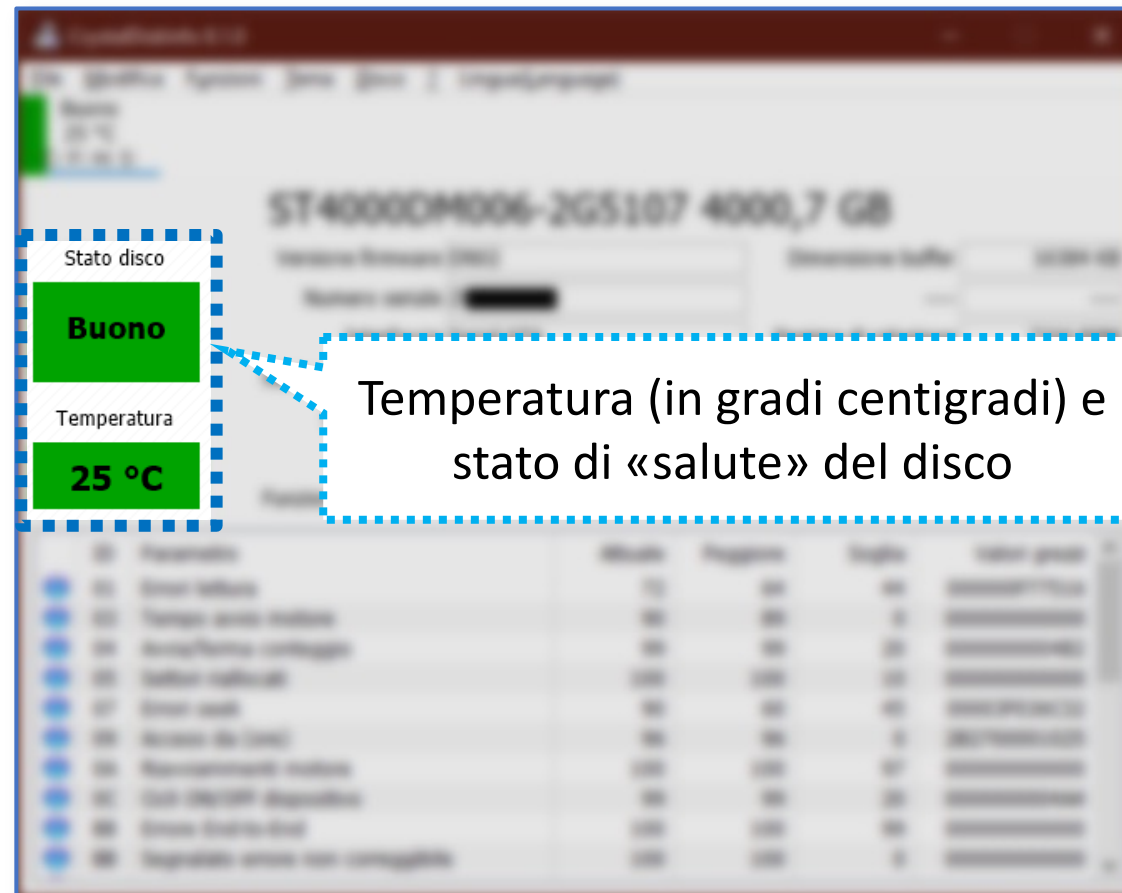
*Esempio di informazioni S.M.A.R.T., fornite dal software gratuito  
CrystalDiskInfo (disponibile per S.O. Windows-based)*



# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 2/4

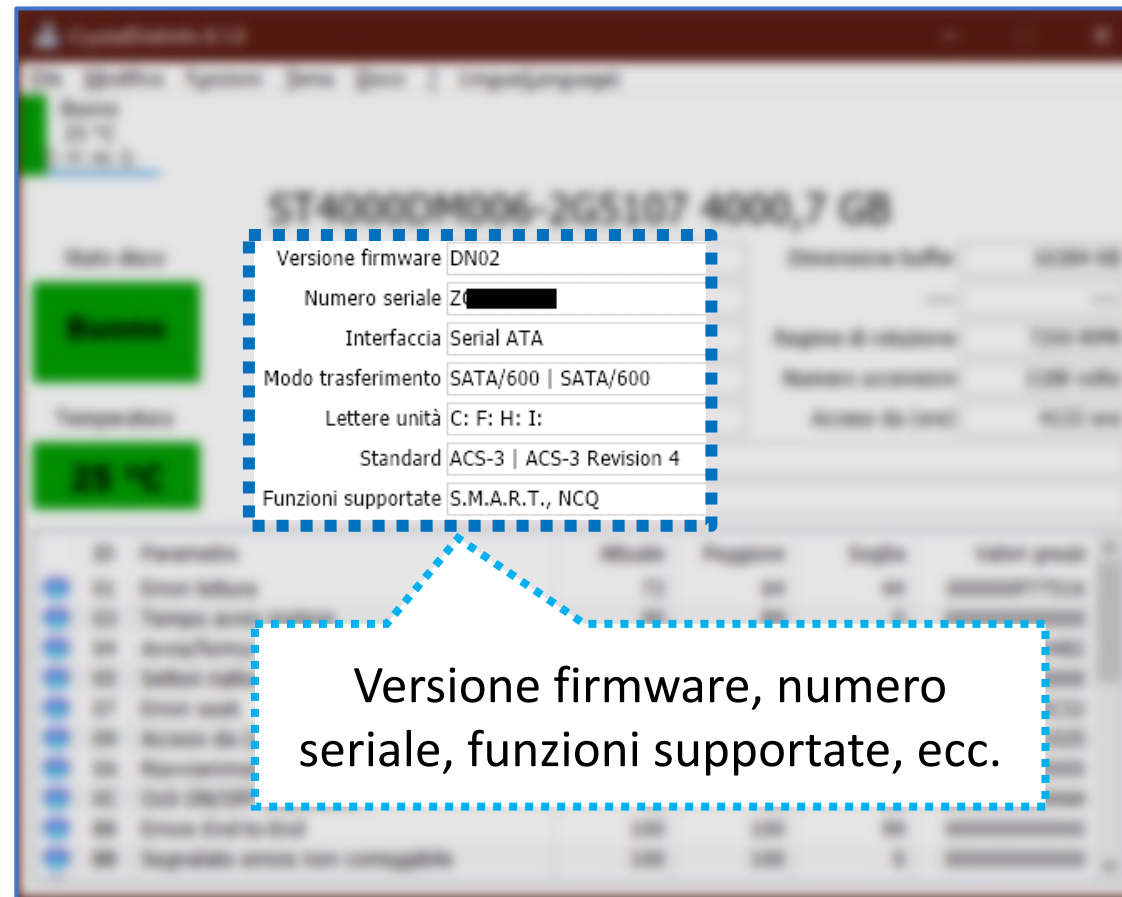
*Esempio di informazioni S.M.A.R.T., fornite dal software gratuito CrystalDiskInfo (disponibile per S.O. Windows-based)*



# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 2/4

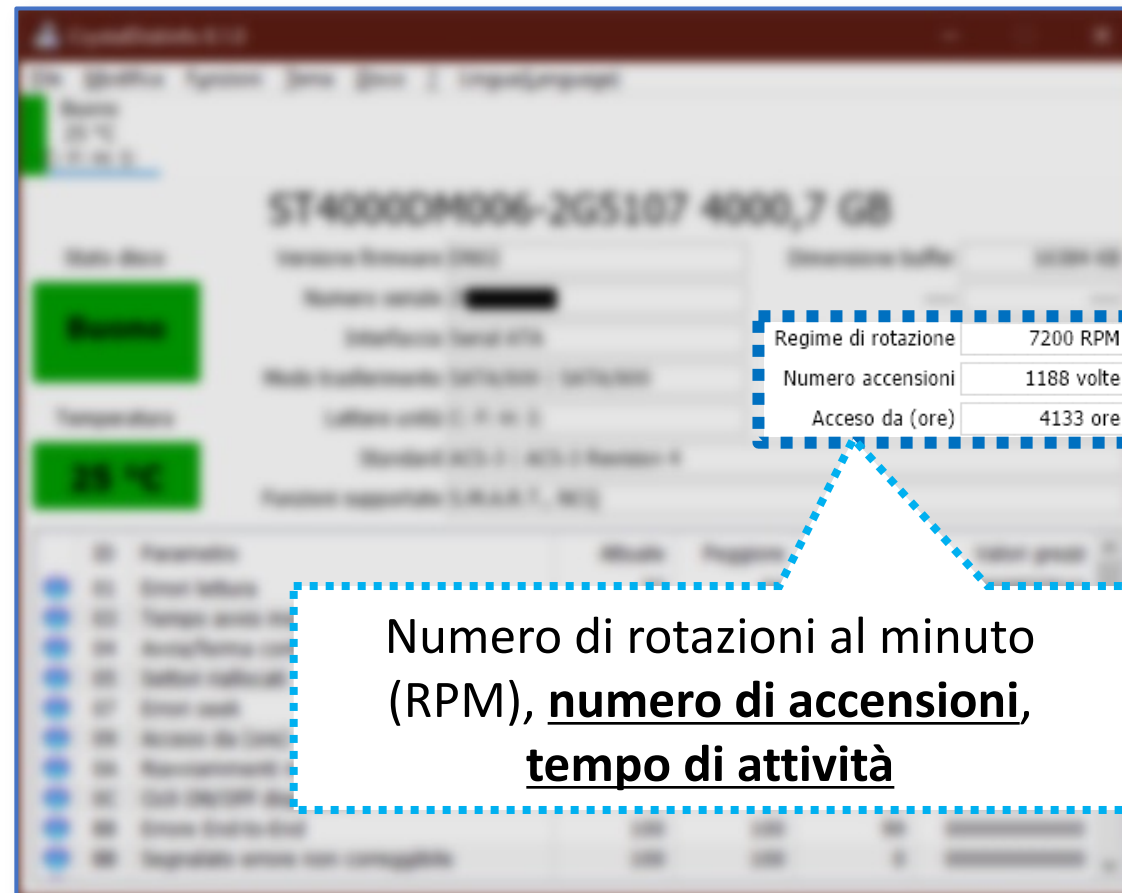
*Esempio di informazioni S.M.A.R.T., fornite dal software gratuito CrystalDiskInfo (disponibile per S.O. Windows-based)*



# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 2/4

*Esempio di informazioni S.M.A.R.T., fornite dal software gratuito CrystalDiskInfo (disponibile per S.O. Windows-based)*



The screenshot shows the CrystalDiskInfo application window. The main display shows the drive model 'ST4000DM006-2G5107' and its capacity '4000,7 GB'. On the right side, there is a table of SMART data. A blue dashed box highlights this table, and a blue dotted line points from it to a text box below.

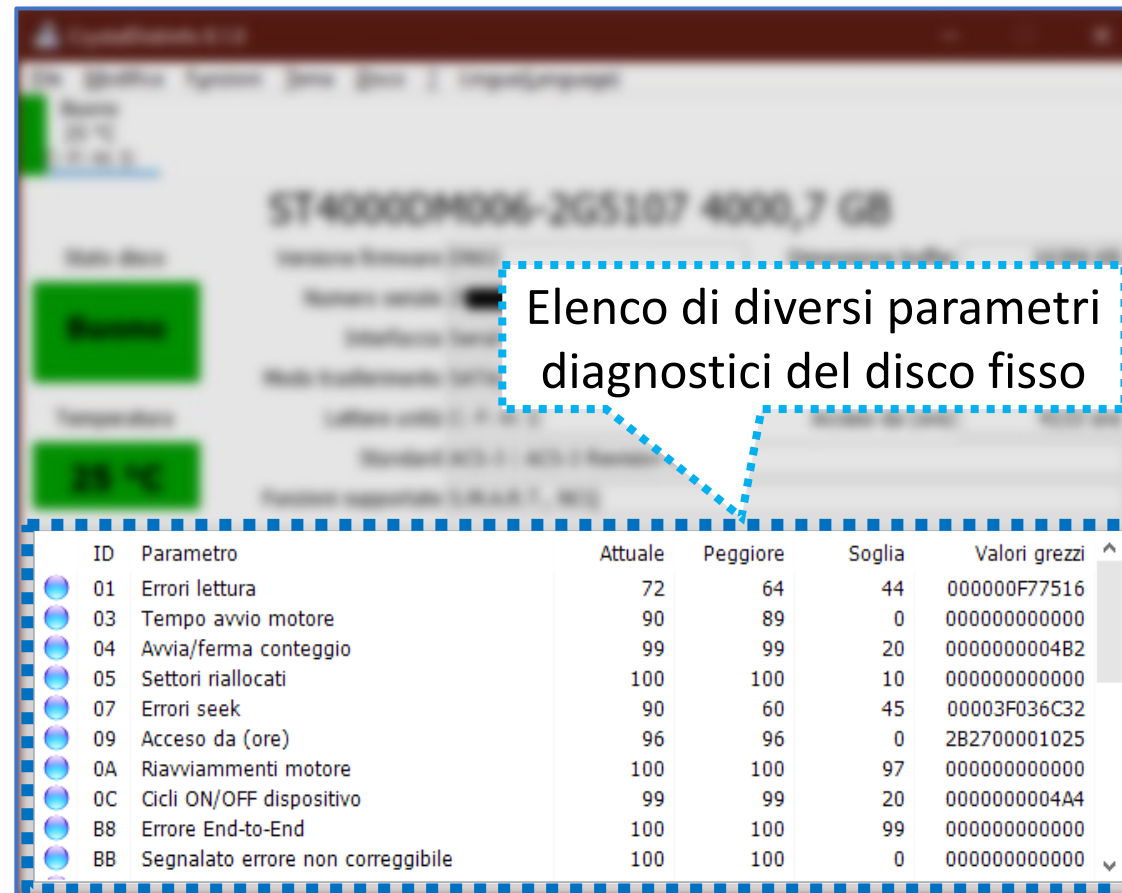
Regime di rotazione	7200 RPM
Numero accensioni	1188 volte
Acceso da (ore)	4133 ore

Numero di rotazioni al minuto (RPM), numero di accensioni, tempo di attività

# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 2/4

*Esempio di informazioni S.M.A.R.T., fornite dal software gratuito  
CrystalDiskInfo (disponibile per S.O. Windows-based)*



Elenco di diversi parametri diagnostici del disco fisso

ID	Parametro	Attuale	Peggior	Soglia	Valori grezzi
01	Errori lettura	72	64	44	000000F77516
03	Tempo avvio motore	90	89	0	000000000000
04	Avvia/ferma conteggio	99	99	20	0000000004B2
05	Settori riallocati	100	100	10	000000000000
07	Errori seek	90	60	45	00003F036C32
09	Acceso da (ore)	96	96	0	2B2700001025
0A	Riavviammenti motore	100	100	97	000000000000
0C	Cicli ON/OFF dispositivo	99	99	20	0000000004A4
B8	Errore End-to-End	100	100	99	000000000000
BB	Segnalato errore non correggibile	100	100	0	000000000000



# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 3/4

Non è possibile effettuare il reset delle informazioni,  
tracciate dalla tecnologia S.M.A.R.T.

- La tecnologia S.M.A.R.T. prevede un comando, denominato DISABLE, per disabilitare il tracciamento delle informazioni diagnostiche
  - Tuttavia, sperimentalmente, è stato osservato che solo alcuni modelli lo implementano
    - Inoltre, in alcuni casi, anche se tale comando è implementato e viene utilizzato, la tecnologia S.M.A.R.T. continua a tener traccia del tempo di attività e del numero di accensioni

# Tecniche per l'Anti-Forensics

Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T. | 4/4

- I tool per l'Anti-Forensics possono trarre beneficio dalle informazioni fornite dalla tecnologia S.M.A.R.T.
- Infatti, tramite tali informazioni, è possibile cercare di capire se sono già stati utilizzati determinati tool per l'analisi forense
  - Eventualmente, se non dovessero essere stati già utilizzati determinati tool forensi, l'attaccante potrebbe valutare l'utilizzo di strategie, per alterare il comportamento di questi ultimi
- *Esempio*
  - Un aumento significativo del tempo di attività del disco fisso, potrebbe indicare che è stato utilizzato un tool per l'acquisizione di una immagine forense

# Tecniche per l'Anti-Forensics

## Rilevare l'utilizzo di tool per l'investigazione forense

### Rilevare l'utilizzo di tool per l'investigazione forense



Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T.



**Contrastare la Network Forensics**

# Tecniche per l'Anti-Forensics

## Contrastare la Network Forensics

- Molti tool per la network forensics acquisiscono il traffico utilizzando un'interfaccia di rete in modalità promiscua
  - In questa modalità, l'interfaccia di rete è in grado di acquisire tutti i pacchetti sulla rete locale (non solo quelli indirizzati ad essa)
- In genere, gli host che effettuano il monitoring della rete non dovrebbero essere in grado di trasmettere sulla rete che stanno monitorando
  - Tuttavia, nella pratica, i suddetti host non sono spesso configurati correttamente
    - Pertanto, è possibile identificare (ed, eventualmente, attaccare) questi host, analizzando le loro risposte a pacchetti malformati

**Alcune Contromisure**

# Alcune Contromisure | 1/3

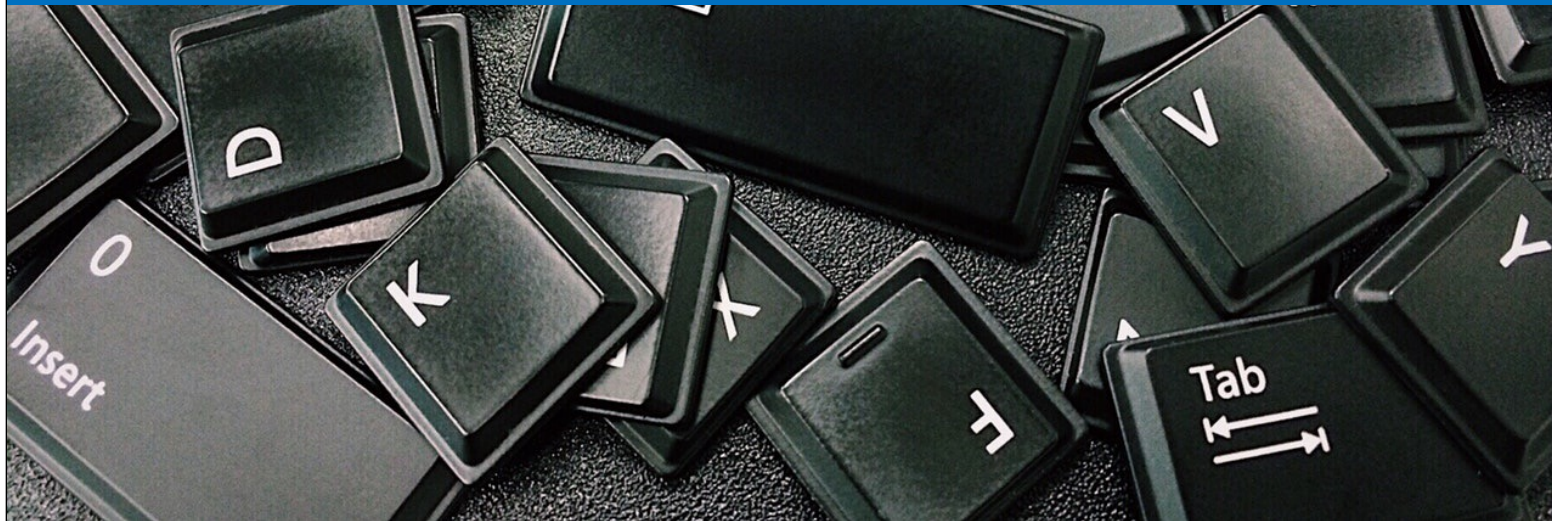
- Alcune delle tecniche anti-forensi possono essere semplicemente superate, migliorando i tool forensi
  - Ad esempio, utilizzando controlli più rigidi dell'input, ecc.
- Inoltre, è possibile mettere in difficoltà i tool per la sovrascrittura dei dati/metadati, memorizzando questi ultimi in supporti di sola lettura:
  - CD-ROM/DVD-ROM
  - Ecc.
- I suddetti supporti, ad esempio, un volta scritti, non possono essere alterati (si suppone, inoltre, che l'attaccante non vi abbia accesso fisico)

## Alcune Contromisure | 2/3

- Un'altra possibilità è quella di inviare dei log (relativi ai dati memorizzati nel file system) ad un host remoto (al quale si suppone che l'attaccante non abbia accesso)
- I *compression bombs attacks* potrebbero essere evitati
  - Un tool forense potrebbe avvisare l'investigatore di comportamenti potenzialmente anomali
  - *Possibili Esempi di tali Comportamenti*
    - Se la decompressione di un file richiede un tempo più lungo di una certa soglia
    - Se la dimensione dei dati estratti supera una certa soglia

## Alcune Contromisure | 3/3

- La crittografia dei file ed, in generale, i file system crittografati, sono, in generale, un problema per gli investigatori forensi
  - Tuttavia, in alcuni casi, è stato possibile recuperare password e/o chiavi crittografiche, utilizzando spyware, key logger e altre tecniche





# Riferimenti Bibliografici

- **Anti-Forensics: Techniques, Detection and Countermeasures, S. Garfinkel, Conference on i-Warfare and Security (ICIW) 2007**
- **Attribute Changer**
  - <https://www.petges.lu/>
- **File 42.zip**
  - <https://www.unforgettable.dk/>
- **CrystalDiskInfo**
  - <https://crystalmark.info/en/software/crystaldiskinfo/>