

«Back|Track-[IT]

[www.backtrack.it](http://www.backtrack.it)



(c) 2008 dr4kk4r  
[dr4kk4r@backtrack.it](mailto:dr4kk4r@backtrack.it)

# *La Catena di Custodia*



\*\*\*

**I**l primo e più importante passo che un forenser deve compiere prima di iniziare la sua investigazione, è quello di identificare la prova informatica e la sua possibile posizione.

Il secondo passo è la conservazione il forenser deve garantire l'integrità della prova informatica. Il dato originale non deve essere modificato e danneggiato e quindi si procede realizzandone una copia (bit-a-bit), su cui il forenser compie l'analisi. Dopo aver effettuato la copia è necessario verificarne la consistenza rispetto al dato originale: per questo motivo si firmano digitalmente il dato originale e la copia, che devono coincidere.

\*\*\*

**I**l dato originale deve essere protetto nella maniera più idonea a seconda del supporto su cui si trova. Le cause di alterazione di un supporto magnetico e di un supporto ottico, ad esempio, sono ben differenti. Si deve inoltre garantire una catena di custodia, ovvero un documento che dica quello che è stato fatto e quali persone fisiche hanno avuto accesso al dato originale e alle copie effettuate fino ad arrivare al giorno del processo.

\*\*\*

**L**e principali informazioni che possono essere contenute in questo documento sono:

- Numero del caso
- Società 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 in cui il supporto è stato rinvenuto
- Produttore del supporto
- Modello del supporto
- Numero di serie del supporto

\*\*\*

**O**gni volta che i supporti oggetto di indagini vengono affidati ad un nuovo investigatore, nella catena di custodia, dovrà essere aggiunta un'informazione contenente:

- Nome dell'incaricato all'analisi
- Data e ora di presa in carico del supporto
- Data e ora di restituzione del supporto



# www.backtrack.it

\*\*\*

*Questo documento è da ritenersi esclusivamente per scopi informativi / didattici, l' autore del testo e coloro che lo ospitano sul proprio spazio non sono responsabili delle azioni commesse da terze parti.*

\*\*\*

(c)2008 *brigante* for [backtrack.it](http://backtrack.it) published under [GNU/GPL-v3](http://www.gnu.org/licenses/gpl-3.0.html)