ELIMINAZIONE SICURA DEI FILES

Scritto da Matteo Giardino

E' molto diffusa la convinzione che l' eliminazione di un file dal cestino di Windows elimini definitivamente il file in questione dall' hard disk o dal supporto su cui si trova.
In realtà l' eliminazione di un file dal cestino di Windows comporta solo l' eliminazione del puntatore al file e non la cancellazione di esso dall' hard disk.
I files semplicemente cancellati dal cestino sono facilmente recuperabili e mediante l' impiego di software specifici come **Photorec**, **Recuva**, **Autopsy**, ecc.; in molti casi è possibile recuperare l' intero contenuto di essi.
In alcune situazioni il recupero non è però possibile: questo caso che si verifica generalmente quando i settori dell' hard disk dove risiedeva il file sono stati sovrascritti accidentalmente o mediante dei software appositi.

- METODI DI CANCELLAZIONE SICURA DEI FILES

DISTRUZIONE FISICA

Uno dei metodi più semplici ed efficaci è la **distruzione fisica** del supporto. Questo sistema è pressoche infallibile se eseguito correttamente.
Per i **CD** e i **DVD** si possono utilizzare degli appositi apparecchi, simili ai tritacarta, che polverizzano l' intero supporto, mentre, per distruggere un hard disk, è sufficiente aprire l' involucro protettivo e danneggiare i **piatti magnetici** utilizzando un qualsiasi oggetto appuntito o degli appositi punzonatori.
La distruzione fisica di un chiavetta USB consite nella distruzione meccanica del **circuito stampato** in essa contenuto mediante un martello o oggetto simile.

DEGAUSSING

Quando si deve dismettere un dispositivo di memoria che contiene dati personali e riservati è preferibile evitare l' uso di soluzione software, utilizzando la distruzione fisica e la **smagnetizzazione** (**degaussing**).

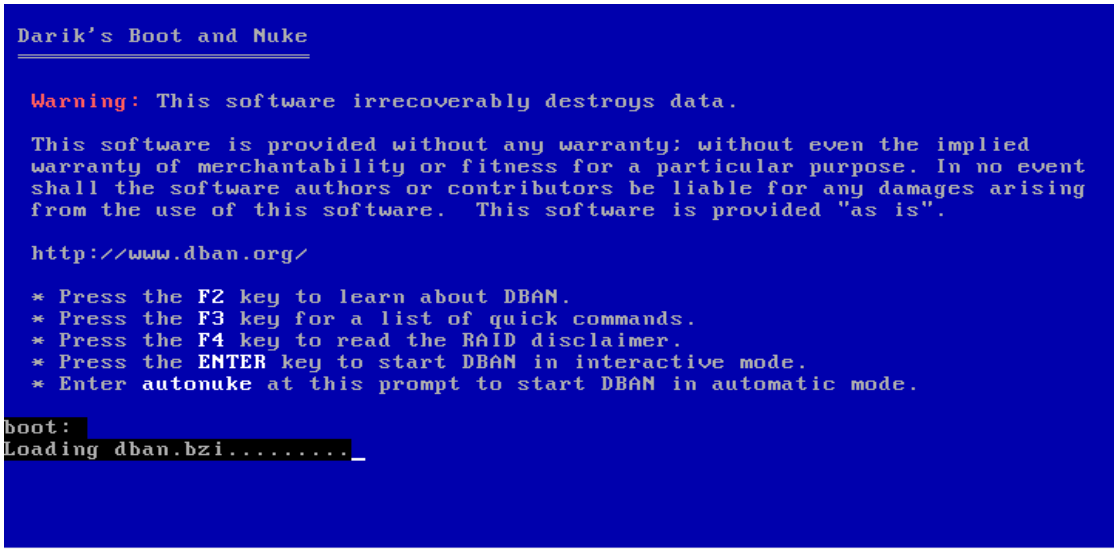
Il degaussing si basa sull' utilizzo di dispositivi detti **deguasser** che generano un campo magnetico con intensità sufficiente a smagnetizzare completamente il supporto di memoria da dismettere.
I degausser sono apparecchiature molto ingrombanti e pesanti (150-200 kg) che generano campi magnetici con intensità pari a circa **11500 Gauss** (circa 1,15 Tesla), più che sufficienti a smagnetizzare un hard disk di ultima generazione in poco più di 4 secondi.
Il campo generato dal degausser è però talmente forte che causa danni alla struttura interna del supporto rendendolo di fatto inutilizzabile. L' utilizzo di un degausser, su qualsiasi dispositivo magnetico, presuppone che questo venga dismesso dopo la procedura di degaussing in quanto reso inutilizzabile.
Questo procedimento non funziona sui supporti ottici come i CD e i DVD, sui quali l' unica procedura efficace è la distruzione fisica, mentre, funziona per tutti supporti magnetici (floppy, VHS, Mini-DV, ecc...)

SOFTWARE SPECIFICI

L' unico procedura per la cancellazione dei files che non danneggia il supporto consiste nell' utilizzo di software specifici, detti **software di wiping**.
Tutti gli algoritmi di wiping prevedono la sovrascrittura dei settori dove si trova il file da cancellare per un certo numero di volte rendendo il suo recupero molto più complicato (e in determinati casi anche impossibile).
Esistono vari tipi di software: alcuni permettono la cancellazione di alcuni files o cartelle (come **wipe** e **secure-delete**) altri dell' intero hard disk (come **DBAN**).

- CANCELLARE UN HARD DISK CON DBAN

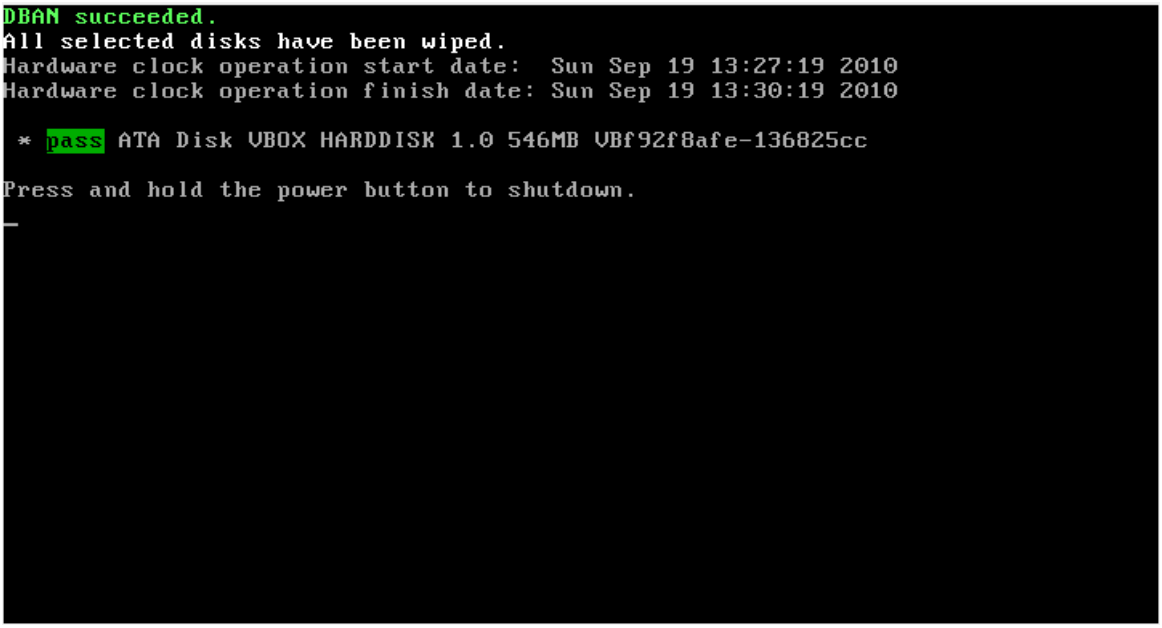
Scaricare l' immagine ISO di **DBAN** dal sito ufficiale www.dban.org e masterizzarla su un CD vergine utilizzando un programma apposito come **Brasero Disc Burner** (per Linux) o **CDBurnerXp** (per Windows).
Inserire il CD contenente DBAN nel lettore e avviare il computer impostando nel BIOS, il lettore CD come dispositivo di avvio.
Nella finestra che appare premere **ENTER** per avviare il wizard di cancellazione dell' hard disk.



Nella finestra che appare selezionare l' unità da cancellare utilizzando le frecce ↑ e ↓. Una volta posizionati sopra l' unità desiderata premere la barra spaziatrice per contrassegnarla come unità da cancellare.
Premere **M** per aprire la schermata di scelta del metodo di wiping, dove vengono proposti vari metodi tra i quali:

- DoDShort
- DoD5220.22-M
- Metodo Guttman

Selezionare il metodo desiderato e premere **ENTER**. Premere **F10** per iniziare la cancellazione del disco. Alla fine della procedura verrà mostrato un' avviso di conferma.

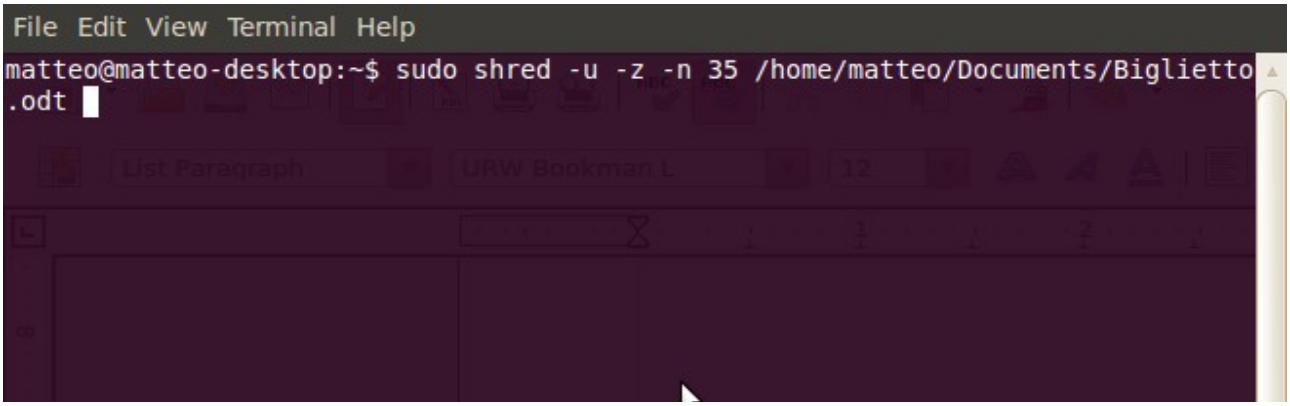


- CANCELLARE UN FILE CON SHRED

Aprire un finestra del terminale di Linux e acquisire i privilegi di amministratore digitando il comando **sudo su**.
Per cancellare un file digitare il seguente comando, seguito dalla pressione del tasto **Enter**:

sudo shred -u -z -n 35 nomefile

Ovviamente al posto di **nomefile** va inserito il percorso del file da cancellare, e al posto di 35 è possibile inserire il numero di passaggi di sovrascrittura da eseguire.



- ALGORITMI DI CANCELLAZIONE DEI FILES

METODO GUTTMAN

Il **metodo Guttman**, inventato dal professor **Peter Guttman** dell' università di Auckland, è probabilmente il metodo più sicuro per la cancellazione del files. Nella sua ricerca intitolata "**Secure Deletion of Data from Magnetic and Solid-State Memory**", Guttman afferma che mediante l' utilizzo di **microscopi elettronici** è possibile recuperare i dati contenuti in un determinato settore anche se questi sono stati cancellati con altri algoritmi (come il DoDShort o il DoD5220.22-M).
Guttman propone quindi una nuova soluzione che rende impossibile il recupero dei files anche con strumenti molto avanzati, come i microscopi elettronici.
Il metodo Guttamn prevede che il file da cancellare venga sovrascritto **35 volte** con sequenze di byte specifiche che permettono di ottenere una cancellazione assolutamente sicura. Le sequenze con cui sovrascrivere il file da cancellare non sono casuali: sono state studiate per attaccare la codifica dell' hard disk e cancellare il file definitivamente.

DoD5220.22-M

Il **DoD5220.22-M** è l' algoritmo utilizzato dal dipartimento della Difesa degli Stati uniti d' america. Questo sistema prevede **7 passaggi** di sovrascrittura: nel primo il viene sovrascritto con valori predefiniti, nel secondo con valori casuali, nel terzo con valori complementari a quelli usati nel primo e negli altri quattro con valori puramente casuali.

– *BIBLIOGRAFIA DELLE FONTI*

Peter Guttman, *"Secure Deletion of Data from Magnetic and Solid-State Memory"*, San Jose (California, USA) 1996

Dominik Hoferer, *"Cancellato? Forese..."*, da CHIP Computer & Communications (settembre 2010 n° 9/2010), Play media company

AA.VV., *"Mamma... ho perso il file!"*, da Win Magazine (giugno 2010 - anno XIII - n° 6), Edizioni Master

Contributori di Wikipedia, "Metodo Guttman", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Metodo_Guttman&oldid=32935500 (in data 20 settembre 2010).

http://www.vitedigitali.blogspot.com/2007/10/degausser-come-cancellare-i-dati.html

http://www.ontrackdatarecovery.it/degausser