

DBan e la cancellazione sicura degli Hard Disk meccanici

Si applica a:	Hard Disk da dismettere		
Si richiede :	DBAN - Darik' Boot and Nuke - http://www.dban.org/		
Redatto da:	Euge aka "Den"		
File allegati:			
Cod. Agg. :	PWR	INF	1^ ed. 07/09/2006
Licenza		Alcuni diritti riservati. Puoi scaricare e condividere i lavori originali a condizione che non li modifichi né li utilizzi a scopi commerciali e sempre attribuendo la paternità dell'opera all'autore. Per il testo della licenza vedi: http://creativecommons.org/licenses/by-nc-nd/3.0/it/legalcode	
<p>Questo testo viene fornito "così come è" ("as is"). Per vari motivi, l'autore è impossibilitato a fornire assistenza e si limita solo a rendere disponibile questo testo. L'autore non è responsabile per i danni, problemi e/o malfunzionamenti che l'utilizzo di informazioni e/o procedure contenute e/o descritte in questo testo possono arrecare. Il contenuto di questo testo può essere derivato da test sperimentali effettuati che potrebbero essere stati non esaustivi e che potrebbero non aver fatto emergere conseguenze non desiderate o dannose. Prima di utilizzare le informazioni contenute in questo testo effettuare un backup del sistema. Tutti i marchi citati in questo testo sono di proprietà dei rispettivi proprietari.</p>			
Per questa e altra documentazione visitare il sito www.dentek.it			

1 - Introduzione

La necessità di cancellare efficacemente i supporti di memorizzazione dismessi in genere non è molto sentita perché normalmente non si considera che contengono molti dati personali e password. Si pensi però ad esempio ad un pc che è stato usato per l'home-banking quali informazioni può contenere.

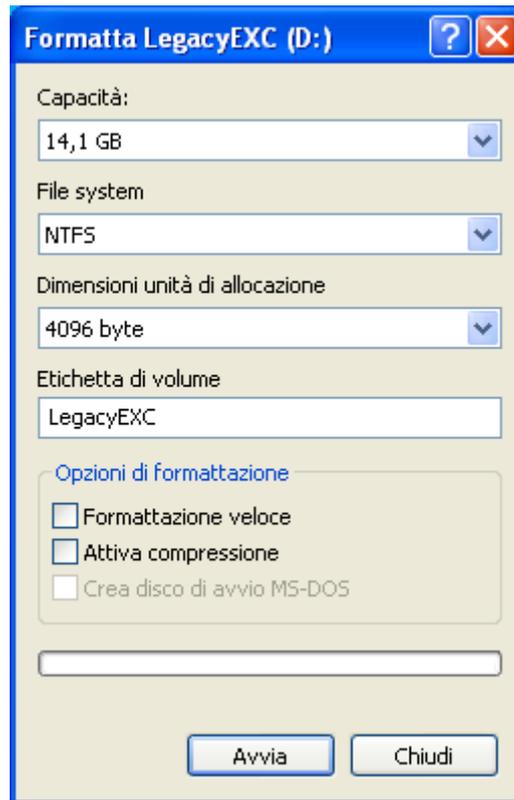
Dei ricercatori dell'università di Leicester hanno effettuato un test acquistando un certo numero di computer usati ed hanno riscontrato che in diversi casi gli hd contenevano ancora dati sensibili e i rimanenti erano stati solamente formattati (operazione non sufficiente a rendere illeggibili i dati memorizzati), rendendo i vecchi proprietari a rischio del cosiddetto furto d'identità.

ATTENZIONE: Questa procedura si riferisce esclusivamente agli hard disk meccanici; per altri tipi di memorie come hard disk SSD o ibridi, penne usb, flash memory o schede di memoria varie questa guida non si applica in quanto presentano problematiche diverse.

2 – La cancellazione sicura degli hard disk

Per "cancellazione sicura" di un hard disk si intende una cancellazione che non sia facilmente reversibile.

La normale formattazione degli Hard Disk, se viene effettuata in modalità veloce, non cancella il contenuto dei settori, ma si limita a farli "considerare" vuoti dal sistema operativo dandoli disponibili per il loro riutilizzo, non rimuovendo i dati scritti in essi.



Similmente avviene durante la normale cancellazione di file.

Conseguentemente anche dopo una cancellazione i dati sono ancora accessibili, (ad esempio con un editor esadecimale dei settori del disco fisso) e, quello che più conta, recuperabili. La minore o maggiore facilità con la quale i dati possono venir recuperati dipende dal file system utilizzato (fat, ntfs, ecc.) e dal metodo utilizzato per la cancellazione.

In pratica, se analizziamo un disco rigido in uso, potremmo riscontrare che sullo spazio non allocato a file esistenti ma assegnato in precedenza ad altri file poi cancellati, sono ancora presenti i dati di quest'ultimi; dati che saranno cancellati solo quando il sistema operativo utilizzerà quei settori per memorizzarvi un altro file la cui scrittura andrà a "ricoprire" i dati presenti.

Nel caso dei file, esiste anche il problema dello spazio rimanente in coda nell'ultimo settore della traccia utilizzato per la scrittura di un file di lunghezza non multipla alla dimensione del settore stesso.

Semplificando, se il supporto di memorizzazione magnetico e utilizza settori ad esempio di 512 Byte, se si scriverà un file ad es, da 1536 Byte, esso utilizzerà pienamente 3 settori ($512 \times 3 = 1536$), sovrascrivendo totalmente i tre settori che utilizzerà;

nel caso invece che il file da scrivere sul supporto sia di 1500 Byte, saranno utilizzati sempre tre settori del disco dove i primi due saranno utilizzati per la loro intera lunghezza ($512 \times 2 = 1024$), mentre nel terzo saranno utilizzati (e quindi sovrascritti) i rimanenti 472 Byte del file non andando ad interessare gli ultimi 40 Byte del settore ($512 - 472 = 40$) pertanto in questi ultimi 40 Byte saranno ancora presenti i valori del file che era stato memorizzato in precedenza in quel settore.

Tale spazio usualmente si definisce "slack".

Per completezza d'informazione, seppur con dispositivi particolari, anche nel caso di sovrascrittura di un settore si possono ancora recuperare i dati che sono stati sovrascritti.

Per questa ragione le norme di alcuni enti che regolano la modalità della cancellazione sicura dei supporti magnetici di memorizzazione prevedono più sovrascritture successive di valori numerici diversi provenienti da sequenze numeriche provenienti da algoritmi di generazione di numeri pseudo-casuali.

	DTK-KB-004-v0101 DBan e la cancellazione sicura degli Hard disk meccanici	28/04/2010
		Pag 3 di 20

Occorre aver cura di cancellare gli hard disk dei computer che vengono dismessi, in quanto possono contenere dati aventi carattere di riservatezza: occorre evitare che un eventuale terzo che prelevi il disco fisso dal pc dismesso possa accedere alle informazioni in esso contenute.

Mentre per quanto riguarda i floppy disk che possono essere formattati mediante un qualsiasi pc a disposizione con una formattazione “completa” che a differenza di quella “veloce” sovrascrive i dati presenti (anche se una volta sola e con un valore fisso) o possono essere facilmente distrutti fisicamente, per quanto riguarda gli hard disk il rendere non disponibili i dati presenti su di esso è un po’ meno agevole.

La difficoltà consiste nel fatto che il supporto da cancellare totalmente è lo stesso sul quale è installato il sistema operativo che deve effettuare la cancellazione e quindi normalmente avrà delle protezioni che eviteranno di cancellare parti necessarie per il suo funzionamento; inoltre non è detto che tale sistema operativo sia funzionante.

Occorrerebbe prelevare il disco fisso dal pc da dismettere, installarlo come disco dati (non di sistema) in un altro pc in parallelo a quello già presente e provvedere alla sua cancellazione utilizzando il sistema operativo normalmente utilizzato dal secondo pc.

Mentre questa procedura rimane l’unica nel caso che il pc da dismettere abbia problemi hardware e che di conseguenza non sia utilizzabile per eseguirvi alcun programma, negli altri casi è possibile utilizzare il tool Darik's Boot and Nuke ("DBAN"), attualmente distribuito nella versione 1.0.7 e prelevabile dal sito <http://www.dban.org/>. Detto programma è Open Source ed è distribuito sotto licenza GPL.

L’utilità consiste in un floppy avviabile contenente un sistema operativo minimo che provvederà, al termine del suo caricamento, al lancio dell’applicazione dban.

Il sistema operativo utilizzato è una versione minima di Linux, senza interfaccia grafica e con i moduli strettamente necessari al funzionamento di DBAN.

Nonostante il tutto sia contenuto in un floppy da 1,44 MB, contiene i driver per:

- controller dischi di tipo XT, IDE, Parallel-ATA, Serial-ATA e SCSI
- Bus ISA, MCA (Microchannel, utilizzato tempo fa su pc IBM serie PS2) e PCI

ed è utilizzabile su pc x86 basati su CPU a 16 bit e a 32 bit con una dotazione minima di 8 MByte di RAM .

I file system sui quali può operare sono:

- per i sistemi operativi Microsoft da DOS a Windows XP
 - FAT
 - VFAT
 - NTFS
- per i sistemi operativi Linux, FreeBSD, Open BSD, BeOS e QNX
 - EXT
 - ReiserFS
 - UFS

La versione attuale (1.0.7) non può cancellare dischi fissi collegati attraverso porte USB o Firewire.

3 - Creazione del floppy di boot di DBAN

ATTENZIONE:

Attualmente (aprile 2010) sul sito non è più disponibile il file per la creazione del floppy ma solo l'immagine .iso per cd relativa alla versione 2.0.0.beta del programma.

Tuttavia schermate relative all'utilizzo sono sostanzialmente uguali a quelle riportate per la versione utilizzata per la redazione di questa guida, che rimane utilizzabile.

Tenere presente che possono esserci state delle variazioni alla licenza d'uso del programma e delle sue caratteristiche; inoltre tale versione non cancella i dati sui dischi SSD: consultare il sito <http://www.dban.org> per gli aggiornamenti, anche riguardo all'efficacia dell'azione di cancellazione del programma.

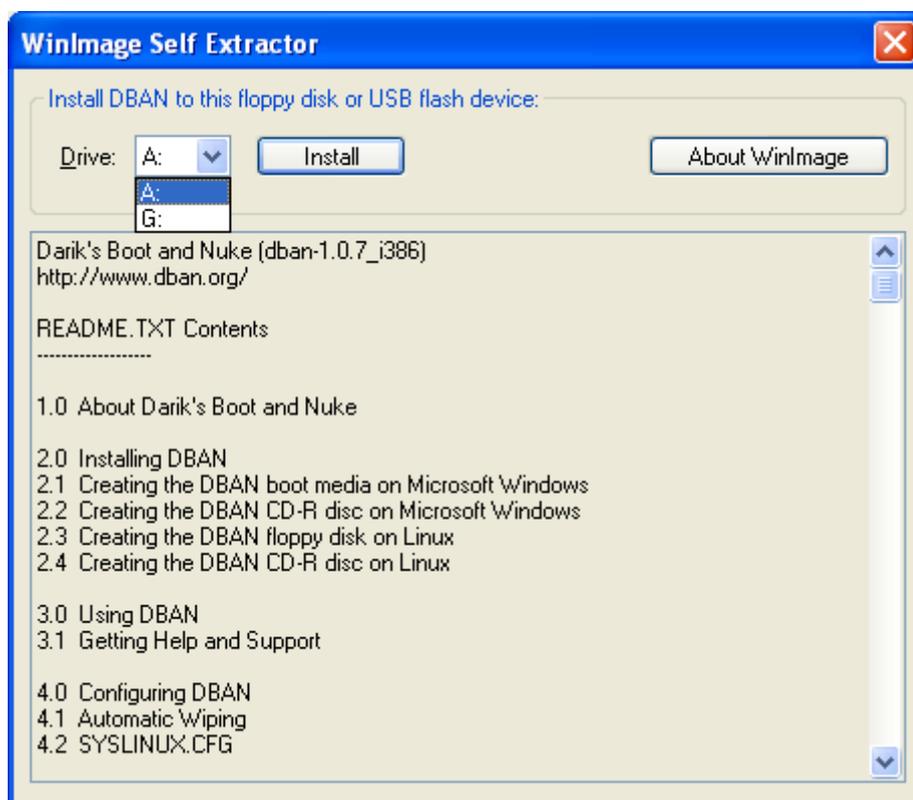
Per la creazione del floppy da ambiente Windows occorrerà, dopo averne effettuato il download dal sito

<http://www.dban.org>

provvedere all'esecuzione del file

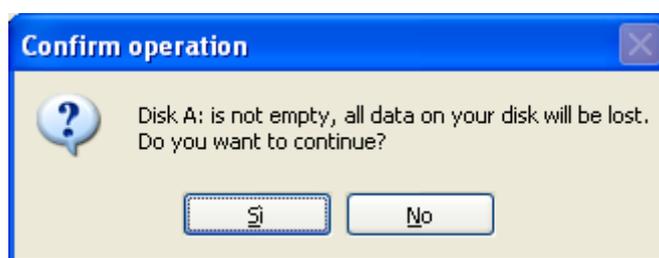
dban-1.0.7_i386.exe

o versione successiva (in questo caso si tratta della versione 1.0.7) con la conseguente visualizzazione della seguente finestra:

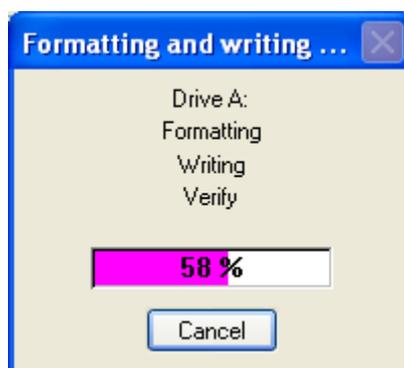


dalla quale selezionando il drive A: ed inserendo un floppy disk da 1,44 MB si inizierà la procedura di generazione facendo click su "Install"

Nel caso il floppy non fosse vuoto, verrà chiesta la conferma per proseguire in quanto il contenuto del floppy verrà sovrascritto.



Rispondendo “Si” inizierà la procedura di scrittura del floppy



alla fine della quale il floppy è pronto per essere utilizzato.

Per creare il floppy di DBAN potrebbe essere necessario essere loggati come membri del gruppo Administrator; inoltre anche alcuni antivirus o le policies di dominio potrebbero impedire la creazione del floppy.

In alternativa, è possibile installare l'utilità anche su una chiavetta usb, che verrà anch'essa resa avviabile. Nella figura precedente relativa alla scelta dell'unità di destinazione riportata in precedenza si può notare che è presente anche l'unità G: che corrisponde ad una chiavetta usb collegata al pc e che è stata correttamente rilevata dal programma di installazione.

Tuttavia non si consiglia tale soluzione in quanto solo i recenti pc possono effettuare il boot da periferiche usb e per alcuni occorre anche preventivamente settare alcune impostazioni del bios.

E' possibile anche generare un cd avviabile contenente l'utilità dban. Sul sito è infatti disponibile il file dban-1.0.7_i386.iso contenente un'immagine che è possibile scrivere su cd-r utilizzando un programma di masterizzazione in grado di gestire il formato .iso (ad es. CDBurnerXP).

Considerare però che i lettori di CD-ROM prodotti prima del 1998 possono avere nel leggere correttamente alcuni supporti CD-R; ancora più problematico è la compatibilità dei supporti CD-RW con i lettori non recenti.

Di conseguenza è consigliato, specie su vecchi computer, utilizzare DBAN da floppy disk mentre utilizzare DBAN da cd può essere comodo per operare su notebook recenti che non sono dotati di drive floppy incorporato.

4 - Uso di dban

Non è possibile eseguire dban dall'interno del DOS o di Windows.

Occorre effettuare il boot dal floppy (o da chiavetta usb o da cd) creato con la procedura riportata nel precedente capitolo e contenente l'utilità DBAN.

All'avvio verrà caricata una versione minima del sistema operativo Linux e successivamente verrà avviata l'utilità DBAN con la visualizzazione della schermata seguente

```

Darik's Boot and Nuke
=====

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied
warranty of merchantability or fitness for a particular purpose. In no event
shall the software authors or contributors be liable for any damages arising
from the use of this software. This software is provided "as is".

http://www.dban.org/

* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key for troubleshooting hints.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode.

boot:

```

Dalla quale proseguiremo premendo semplicemente il tasto <Enter> (<Invio>) per eseguire il programma in modalità interattiva.

Attenzione: se si scrivesse “autonuke” dban partirebbe in modo automatico cancellando automaticamente e senza ulteriori richieste tutti i supporti di memorizzazione da esso riconosciuti nel pc.

Il programma proseguirà con il caricamento dei moduli:

```

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied
warranty of merchantability or fitness for a particular purpose. In no event
shall the software authors or contributors be liable for any damages arising
from the use of this software. This software is provided "as is".

http://www.dban.org/

* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key for troubleshooting hints.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode.

boot:
Loading kernel.bzi.....
Loading initrd.gz.....
Ready.
Uncompressing Linux with LZMA...
Ok, booting the kernel. Please wait 60 seconds for DBAN to start...
If the computer hangs here, then reset it and read the DBAN
troubleshooting hints by pushing F4 at the boot prompt.

```

e dopo aver effettuato il riconoscimento dei supporti di memorizzazione presenti nel sistema visualizzerà l'interfaccia utente del programma:

```
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseme Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:
----- Disks and Partitions -----
▶ [ ] (IDE 0,0,0,-,-) Virtual HD

P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

Nota: nella schermata precedente ed in quelle seguenti viene visualizzata la presenza di un solo hard disk avente come etichetta "Virtual HD" in quanto per poter agevolmente memorizzare le schermate del programma, dban è stato lanciato su una macchina virtuale.

Nella sezione "Options" sono riportate le impostazioni correnti del programma, quali il generatore di numeri casuali in uso, il metodo di cancellazione usato, quando e se effettuare la verifica e il numero di rounds. Tali opzioni possono essere modificate utilizzando i comandi riportati nell'ultima riga della schermata.

Nella sezione "Disk and Partitions" sono visualizzati i dischi fissi rilevati e le relative partizioni.

Nella sezione "Statistics" saranno visualizzati i dati relativi all'avanzamento della procedura di cancellazione.

Nella riga in basso sono riportati i tasti mediante la pressione dei quali è possibile selezionare delle opzioni o impartire comandi; essendo possibile operare tramite tastiera è possibile usare il programma anche con sistemi obsoleti nei quali non è disponibile il mouse (ad es. mancata disponibilità di mouse seriale).

Nelle schermate ove si potranno scegliere i parametri è previsto l'uso dei seguenti tasti:

<Freccia Su> o <J> per evidenziare l'opzione precedente
<Freccia Giù> o <K> per evidenziare l'opzione successiva
<Spazio> per selezionare l'opzione evidenziata

Per deselezionare un'opzione precedentemente selezionata, posizionarsi nuovamente in corrispondenza di essa e premere nuovamente la barra spaziatrice.

I comandi disponibili sono i seguenti:

<P> - PRNG – per selezionare l’algoritmo di generazione delle sequenze di numeri pseudo-casuali; il Mersenne Twister, attivato per default, risulta più rapido rispetto il ISAAC.

```

Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Mersenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Pseudo Random Number Generator -----

                syslinux.cfg:  nuke="dwipe --prng twister"

▶ Mersenne Twister (mt19937ar-cok)
  ISAAC (rand.c 20010626)

The Mersenne Twister, by Makoto Matsumoto and Takuji Nishimura, is a
generalized feedback shift register PRNG that is uniform and
equidistributed in 623-dimensions with a proven period of 2^19937-1.

This implementation passes the Marsaglia Diehard test suite.

J=Up K=Down Space=Select

```

```

Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Mersenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Pseudo Random Number Generator -----

                syslinux.cfg:  nuke="dwipe --prng isaac"

  Mersenne Twister (mt19937ar-cok)
▶ ISAAC (rand.c 20010626)

ISAAC, by Bob Jenkins, is a PRNG derived from RC4 with a minimum period of
2^40 and an expected period of 2^8295.  It is difficult to recover the
initial PRNG state by cryptanalysis of the ISAAC stream.

J=Up K=Down Space=Select

```

<M> - Method – per selezionare la modalità con la quale cancellare il disco. Le modalità previste sono le seguenti:

Quick Erase	Cancellazione veloce; si limita nello scrivere il valore zero (una sola volta) in tutto il disco
RCMP TSSIT OPS-II	Metodo previsto dalla norma della Polizia Canadese a Cavallo Technical Security Standard for Information Technology – Appendix OPS-II – Media Sanitization; Paragrafo 2 sezione A
DoD Short	Metodo previsto dallo standard del Ministero della Difesa Americano Department of Defense 5220.22-M short wipe
DoD 5220.22-M	Metodo previsto dallo standard del Ministero della Difesa Americano Department of Defense 5220.22-M standard wipe
Gutmann Wipe	Metodo descritto da Peter Gutmann in “Secure Deletion of Data from Magnetic and Solid-State Memory”
PRNG Stream	Metodo che consiste nella scrittura di un flusso di valori numerici provenienti da un algoritmo PRNG di generazione di numeri casuali

I metodi sono elencati in ordine di sicurezza crescente, che in genere corrisponde anche ad un tempo di esecuzione maggiore.

Per alcuni metodi è possibile variare il numero delle passate di cancellazione al fine di aumentarne l'efficacia aumentandole.

```

Darik's Boot and Nuke 1.0.7
-----
Options                               Statistics
Entropy: Linux Kernel (urandom)        Runtime:
PRNG: Merseme Twister (mt19937ar-cok)  Remaining:
Method: DoD Short                       Load Averages:
Verify: Last Pass                       Throughput:
Rounds: 1                               Errors:

-----
Wipe Method
-----

Quick Erase                syslinux.cfg: nuke="dwipe --method dodshort"
RCMP TSSIT OPS-II         Security Level: Medium (3 passes)
▶ DoD Short
DoD 5220.22-M
Gutmann Wipe
PRNG Stream

The American Department of Defense 5220.22-M short wipe.
This method is composed of passes 1,2,7 from the standard wipe.

-----
J=Up K=Down Space=Select

```

<V> - Verify – dove impostare se eseguire la verifica o meno e se eseguirla ad ogni Rounds o solo alla fine

```
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseme Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Verification Mode -----

Verification Off          syslinux.cfg: nuke="dwipe --verify last"
▶ Verify Last Pass
Verify All Passes

Check whether the device is actually empty after the last pass fills the
device with zeros.

J=Up K=Down Space=Select
```

<R> - Rounds – dove si può impostare il numero di round da eseguire; digitare il numero voluto e premere <Invio>

```
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseme Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Rounds -----

> 1_

This is the number of times to run the wipe method on each device.

syslinux.cfg: nuke="dwipe --rounds 1"
```

In genere vanno bene tutti i valori di default proposti, ma dato che le procedure di cancellazione richiedono un po' di tempo, se la criticità dei dati contenuti nel disco fisso lo permette, si può considerare di utilizzare il metodo "Quick Erase" (cancellazione veloce) anziché il metodo "DoD Short" proposto di default e/o di non effettuare la verifica finale.

Per indicare quale hard disk (o su quale partizione di un hard disk) si vuole cancellare, occorre evidenziarlo con il triangolino spostandosi da una riga all'altra con i tasti già indicati in precedenza e selezionarlo premendo la barra spazio.

Gli hard disk e le partizioni che verranno cancellate saranno evidenziate dal testo "wipe" inserito tra le parentesi quadre, come nella schermata seguente che illustra un sistema con un solo hard disk nel quale è presente una sola partizione (nelle schermate seguenti gli hard disk sono denominati "Virtual HD" perché il DBAN è stato eseguito su hardware virtualizzato) :

```
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseme Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Disks and Partitions -----

▶ [wipe] (IDE 0,0,0,-,-) Virtual HD

P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

Nella seguente schermata invece è presente il seguente scenario:

- primo hd su bus ide contenente una sola partizione
- secondo hd su bus ide contenente due partizioni

```
Azione Modifica CD Disco floppy ?
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseme Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:
----- Disks and Partitions -----
▶ [ ] (IDE 0,0,0,-,-) Virtual HD
[ ] (IDE 0,0,0,-,1) Partition
[ ] (IDE 0,0,1,-,-) Virtual HD
[ ] (IDE 0,0,1,-,1) Partition
[ ] (IDE 0,0,1,-,2) Partition
P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

In tale scenario si vuole cancellare l'intero primo hd mentre nel secondo hd si vuole cancellare solo la prima partizione, come raffigurato nella seguente schermata:

```
Azione Modifica CD Disco floppy ?
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseme Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:
----- Disks and Partitions -----
[wipe] (IDE 0,0,0,-,-) Virtual HD
[*****] (IDE 0,0,0,-,1) Partition
[----] (IDE 0,0,1,-,-) Virtual HD
▶ [wipe] (IDE 0,0,1,-,1) Partition
[ ] (IDE 0,0,1,-,2) Partition
P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

. Per impostare ciò si è operato come di seguito:

- ci si è posizionati col triangolino bianco sulla prima riga (IDE 0,0,0,-,-) che identifica il primo hd e si è premuto la barra spazio: conseguentemente dban ha inserito la scritta "wipe" in corrispondenza di tale riga e ha provveduto a inserire "*****" nella seconda riga che corrisponde alla partizione contenuta in tale hd in modo da evidenziare che sarà cancellata

anch'essa; se il disco contenesse più di una partizione, sarebbero evidenziate tutte con gli asterischi e sarebbero tutte cancellate.

- Ci si è poi posizionati con il tasto <freccia giù> in corrispondenza della quarta riga, corrispondente alla prima partizione del secondo hd e si è premuto la barra spazio: dban ha inserito la scritta "wipe" solo in corrispondenza di tale riga, evidenziando che solo quella partizione verrà cancellata.

Premendo quindi il tasto <F10> inizierà il procedimento di cancellazione sicura sulle entità selezionate.

ATTENZIONE:

i dischi rigidi o le partizioni cancellate non saranno più recuperabili!
(che in effetti è proprio quello che si richiede al programma)

Al termine della procedura dban comunicherà l'avvenuta cancellazione e tenterà di scrivere sul floppy dal quale è stato lanciato un file di log anche se a volte tale operazione non va a buon segno e viene ritentata; è comunque possibile estrarre il floppy e spegnere il pc.

ATTENZIONE:

In alcuni casi, tentando di installare un nuovo sistema operativo su un hd cancellato con DBAN si ottiene un messaggio di errore riportante problemi alla piattina dati ide di collegamento o a un guasto del disco rigido.

Questo è indicativo dell'efficacia del programma DBAN.

In tal caso basta lanciare un programma di partizionamento dischi fissi (ad es. "Partition Magic") e creare una partizione: l'operazione reinizializzerà il disco fisso; dopo il riavvio si potrà installare normalmente il nuovo sistema operativo senza la comparsa di messaggi di errore.

In tutti i casi che si è riscontrato tale messaggio la procedura appena esposta ha funzionato correttamente e i pc sono in funzione da tempo senza problemi.

5 - Caratteristiche tecniche e piattaforme supportate del programma DBAN ver. 1.0.x

(tratto da <http://www.dban.org/>)

Darik's Boot and Nuke - Product Feature Checklist - DBAN version 1.0.x.

- Free.
- Fast. Rapid deployment in emergency situations.
- Easy. Start the computer with DBAN and press the ENTER key.
- Safe. Irrecoverable data destruction. Prevents most forensic data recovery techniques.

Price and Usage Restrictions

Open source code:

YES

User Rights:	<input checked="" type="checkbox"/> GPL PROTECTED
Wipe Methods	
Quick Erase	<input checked="" type="checkbox"/> YES
Canadian RCMP TSSIT OPS-II Standard Wipe	<input checked="" type="checkbox"/> YES
American DoD 5220-22.M Standard Wipe	<input checked="" type="checkbox"/> YES
Gutmann Wipe	<input checked="" type="checkbox"/> YES
PRNG Stream Wipe	<input checked="" type="checkbox"/> YES
Enhancements	
8/33/137 gigabyte disk size BIOS limit fix:	<input checked="" type="checkbox"/> YES
Fast PRNG (Mersenne Twister)	<input checked="" type="checkbox"/> YES
Entropy Seeding	<input checked="" type="checkbox"/> YES
Verification	<input checked="" type="checkbox"/> YES
Logging	<input checked="" type="checkbox"/> YES
Hardware Drivers	
Controllers: XT, IDE, PATA, SATA, SCSI	<input checked="" type="checkbox"/> ALL
Consoles: Serial, HGA, VGA	<input checked="" type="checkbox"/> ALL
Buses: ISA, MCA, PCI	<input checked="" type="checkbox"/> ALL

Platform Support

- Hardware
 - DBAN has *all* available drivers for SCSI disks.
 - DBAN has *all* available drivers for IDE, PATA, and SATA disks.
 - DBAN runs on *all* 32-bit x86-class computers (Athlon, Pentium, and others) with at least 8 megs of memory. If you find an incompatible machine, then please report it.
- Software

- DBAN supports all Microsoft platforms and securely destroys FAT, VFAT, and NTFS filesystems.
 - MS-DOS, Windows 3.1
 - Windows 95, Windows 98, Windows ME
 - Windows NT 3.0, Windows NT 3.1, Windows NT 3.5, Windows NT 4.0
 - Windows 2000, Windows XP
- DBAN supports all unix platforms and securely destroys ReiserFS, EXT, and UFS filesystems.
 - FreeBSD, NetBSD, OpenBSD
 - Linux
 - BeOS
 - QNX

6 – Istruzioni per DBan dal sito del Garante per la privacy

Successivamente alla prima versione di questa guida (settembre 2006), è stata pubblicata sul sito del Garante per la privacy una scheda informativa riguardante la cancellazione sicura dei dati indicando come strumento software proprio il programma DBan di cui fornisce anche le istruzioni per il suo uso; si riporta tale scheda per completezza d'informazione.



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Scheda informativa - 12 dicembre 2008

Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori

Nel quadro delle proprie iniziative sulla protezione dei dati rispetto allo smaltimento, dismissione e cessione a qualunque titolo di apparecchiature elettriche ed elettroniche, l'Autorità intende fornire a utenti e operatori, a complemento del provvedimento che ha adottato il 13 ottobre 2008, alcuni suggerimenti pratici e facilitare la diretta consultazione di altre indicazioni provenienti dai principali fornitori e produttori che risultano operanti in questa tematica.

Pur non assumendo una diretta responsabilità in ordine all'efficacia di questi accorgimenti che l'esperienza dimostra al momento essere utili, l'Autorità ritiene comunque opportuno darne ulteriore pubblicità e richiamare l'attenzione di operatori e utenti a contribuire alla loro corretta applicazione e ogni loro integrazione o modifica, sulla base di approfondimenti e di altre esperienze applicative.

L'Autorità si riserva quindi di aggiornare periodicamente queste istruzioni.

Il Garante, nel sottolineare come non sia responsabile in alcun modo della correttezza delle

	DTK-KB-004-v0101 DBan e la cancellazione sicura degli Hard disk meccanici	28/04/2010
		Pag 16 di 20

istruzioni pubblicate in rete e a cui viene qui fatto riferimento, nonché delle conseguenze della loro messa in opera da parte degli utenti, assicura la propria disponibilità a integrare queste pagine, su richiesta di produttori diversi da quelli qui citati, con l'inserimento di nuovi riferimenti utili, nonché a provvedere all'aggiornamento di quelli già presenti.

La Cancellazione sicura delle informazioni

Il problema dell'e-waste riguarda chiunque mantenga memorizzati su dispositivi elettronici dati relativi a sé o a terzi: è infatti compito del loro possessore dati assicurare che questi non possano andare dispersi e acquisiti anche in modo incontrollato da estranei.

La semplice cancellazione dei file o la formattazione dell'hard disk, infatti, non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili.

Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze:

- preventivamente, con tecniche di memorizzazione sicura;
- immediatamente prima della cessione o dismissione dell'apparato elettronico, con strumenti software di cancellazione sicura (a condizione che l'apparato sia funzionante);
- al momento della cessione o dismissione, con la demagnetizzazione (degaussing), che azzerava tutte le aree di memoria elettronica e rende l'apparato inutilizzabile, o con la distruzione fisica del dispositivo di memorizzazione.

Per ciascuna delle opzioni citate si forniscono qui di seguito delle informazioni per la messa in pratica o per il reperimento di informazioni più dettagliate.

Memorizzazione sicura

La memorizzazione sicura dei file si può realizzare sui più diffusi sistemi operativi con l'attivazione di funzionalità crittografiche proprie del sistema, se disponibili, o con l'installazione di prodotti software aggiuntivi. Le concrete modalità dipendono fortemente dallo specifico sistema operativo utilizzato, e talvolta anche dalla sua versione o dall'applicazione di patch e aggiornamenti. I possessori di personal computer sono pertanto esortati a rivolgersi alle case produttrici del proprio hardware o del sistema operativo in uso per ottenere indicazioni dettagliate.

Si rinviano, in particolare, gli utenti di sistemi operativi Windows alla consultazione delle pagine informative predisposte, in lingua italiana, dalla casa produttrice Microsoft (<http://www.microsoft.com/italy/pmi/sicurezza/privacy/>).

Per i sistemi Apple, le pagine consultabili sul sito italiano del produttore illustrano le funzionalità [FileVault](#) disponibili nel sistema operativo Mac OS X per la protezione di intere directories o di volumi di dati.

Tra i sistemi "multiplatforma" (non dipendenti da uno specifico sistema operativo e perciò utilizzabili in ambiente Windows, MacOS, Unix, Linux...), è disponibile il software [TrueCrypt](#), che offre funzioni di cifratura con strong encryption di partizioni e interi dischi, comprese le partizioni "di sistema".

Cancellazione sicura

Gli utenti di sistemi operativi Microsoft Windows possono far riferimento alle già menzionate pagine informative pubblicate dal produttore

(<http://www.microsoft.com/italy/pmi/sicurezza/privacy/>), che illustrano nel dettaglio le modalità per affrontare il problema della cancellazione di interi volumi di dati qualora non sia stata preventivamente adottata la soluzione della memorizzazione sicura.

Gli utenti del sistema operativo Apple MacOS X, che incorpora una funzione di "svuotamento del cestino in modalità sicura", potranno trovare dettagliate informazioni sul sito del produttore www.apple.it oppure ricorrere a utility di tipo "open source" come Permanent Eraser, che consente di effettuare cancellazioni sicure con un algoritmo avanzato.

Diversi applicativi software di tipo open source o comunque con licenze d'uso non commerciali sono poi disponibili per i sistemi Unix e Linux: tra questi, uno dei più noti ed efficaci è DBAN (www.dban.org), un sistema con cui è possibile creare un "disco di avvio" (boot disk) del proprio computer (sia in forma di floppy-disk che di CD-ROM o di USB flash storage). Si riportano qui di seguito le istruzioni per cancellare, con l'ausilio del software DBAN (Darik's Boot and Nuke), un hard-disk funzionante su un personal computer dotato di lettore di CD-ROM o di DVD.

Creazione del disco di avvio DBAN

Per prima cosa, occorre "scaricare" sul proprio computer il file immagine di DBAN, scegliendo quello adatto a essere "masterizzato" su CD o su DVD (<http://www.dban.org/download>). Il file dban-*_i386.iso va quindi salvato sul proprio computer e trasferito su CD (o DVD) utilizzando un software di masterizzazione. Il CD (o DVD) risultante sarà utilizzabile come "disco di avvio" del proprio computer.

Avvio della procedura di cancellazione sicura

Il computer che contiene il disco da cancellare dovrà essere avviato utilizzando il CD o DVD precedentemente creato, inserendo questo nel corrispondente lettore (drive) e procedendo al riavvio del sistema. Affinché il computer si avvii dal CD o DVD potrà rendersi necessario modificare l'ordine di scelta del dispositivo di avvio, tramite il cosiddetto BIOS setup solitamente accessibile poco dopo l'accensione del computer e prima che venga caricato il sistema operativo.

Cancellazione degli hard-disk con DBAN

Una volta avviato il computer con il disco di avvio DBAN, viene presentata una schermata di scelta tra diverse opzioni di avvio:

```
Darik's Boot and Nuke
-----
Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied
warranty of merchantability or fitness for a particular purpose. In no event
shall the software authors or contributors be liable for any damages arising
from the use of this software. This software is provided "as is".

http://www.dban.org/

* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key for troubleshooting hints.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

Figura 1: Avvio di DBAN

Premendo il tasto INVIO (RETURN) della tastiera si avvierà la procedura interattiva di cancellazione. Successivamente viene presentata la scelta del disco da cancellare, tra quelli installati nel computer e riconosciuti da DBAN.

```

Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Merseenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Disks and Partitions -----
▶ [wipe] (SCSI 1,0,0,0,-) VMware, VMware Virtual S
  [ 1] (IDE 0,0,1,-,-) VMware Virtual IDE Hard Drive

P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start

```

Figura 2: Scelta del disco da cancellare

Effettuata la scelta, occorrerà specificare quale metodo di cancellazione si vuole applicare. Per la maggior parte degli utilizzatori sarà sufficiente il cosiddetto "DoD short", derivato da standard militari USA: altri metodi, teoricamente ancora più sicuri, hanno lo svantaggio di richiedere tempi di elaborazione significativamente più lunghi, soprattutto se applicati a dischi di grande capacità.

```

Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Merseenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Wipe Method -----

Quick Erase          syslinux.cfg: nuke="dwipe --method dodshort"
RCMP TSSIT OPS-II   Security Level: Medium (3 passes)
▶ DoD Short
DoD 5220.22-M
Gutmann Wipe
PRNG Stream

The American Department of Defense 5220.22-M short wipe.
This method is composed of passes 1,2,7 from the standard wipe.

J=Up K=Down Space=Select

```

Figura 3: Scelta del metodo di cancellazione

Successivamente il programma mostrerà lo stato di avanzamento della cancellazione:

```

Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Mersenne Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime: 00:00:11
Remaining: 00:00:19
Load Averages: 0.33 0.09 0.02
Throughput: 18260 KB/s
Errors: 0

(SCSI 1,0,0,0,-) VMware, VMware Virtual S
[34.01%, round 1 of 1, pass 2 of 3] [writing] [18260 KB/s]

```

Figura 4: Cancellazione in corso

fino al suo completamento:

```

DBAN succeeded.
All selected disks have been wiped.
Remove the DBAN boot media and power off the computer.

Hardware clock operation start date: Sun Aug 13 15:24:36 2006
Hardware clock operation finish date: Sun Aug 13 15:27:00 2006
Saving log file to floppy disk... a floppy disk in DOS format was not found.
DBAN finished. Press ENTER to save the log file._

```

Figura 5: Fine della cancellazione con DBAN

A questo punto, si potrà spegnere il computer con sufficiente certezza di non aver lasciato dati sul disco, potendo così procedere alla sua integrale o parziale cessione o smaltimento.

Demagnetizzazione e distruzione

Nel caso in cui il dispositivo elettronico da sottoporre a smaltimento non sia più funzionante, e non

	DTK-KB-004-v0101	28/04/2010
	DBan e la cancellazione sicura degli Hard disk meccanici	Pag 20 di 20

siano pertanto applicabili le misure software, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi estranei occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione (degausser), o con la distruzione fisica.

I degausser permettono l'"azzeramento" delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo e causandone l'inutilizzabilità successiva.

In determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con appositi macchine analoghe ai "tritacarta" in uso negli uffici. Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori.