



Avvocato Hacker

Strumenti per la cifratura, la cancellazione sicura e il backup dei dati e per la sicurezza degli Smart Phone

Sicurezza delle informazioni

- La **sicurezza delle informazioni** è un'esigenza che ha accompagnato la storia dell'uomo fin dalle antiche civiltà
- Il termine **Crittografia** deriva da **Kryptós + gráphein** = nascosto + scrivere: *l'arte di scrivere messaggi segreti*
- Erodoto (440 a.c.) racconta di un nobile persiano che fece tagliare a zero i capelli di uno schiavo fidato al fine di poter tatuare un messaggio sul suo cranio; una volta che i capelli furono ricresciuti, inviò lo schiavo alla sua destinazione, con la sola istruzione di tagliarseli nuovamente

Sicurezza delle informazioni

- Svetonio racconta che Giulio Cesare cifrava i messaggi **sostituendo ogni lettera con quella che nell'alfabeto segue di 3 posizioni**
- *«Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commute»*
(De vita duodecim Caesarum - Libri VIII)

Il Cifrario di Giulio Cesare

Testo in chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Testo cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Lo stesso si può fare con l'[alfabeto italiano](#):

Testo in chiaro	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
Testo cifrato	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

Per cifrare un messaggio, basta prendere ogni lettera del testo in chiaro e sostituirla con la corrispondente lettera della riga *testo cifrato*. Per decifrare, viceversa. Ecco un semplice esempio:

Testo in chiaro	attaccare gli irriducibili galli alla ora sesta
Testo crittato	DZZDFFDUH LON NUUNGA FNENON LDOON DOOD RUD VHVZD

Il Cifrario di Giulio Cesare

- Tutti i cifrari di questo tipo sono divenuti **molto semplici da rompere**: nessuno è adatto per comunicazioni sicure allo stato tecnologico attuale, né lo è stato negli ultimi 1000 anni!!
- Tuttavia....un rudimentale sistema di cifratura basato sul cifrario di Cesare è stato usato anche da **Bernardo Provenzano** per proteggere le informazioni scritte nei suoi famosi *pizzini*

I pizzini di Provenzano

"(...) Per una visita medica: avevo intenzione di contattare, con il tuo permesso, 1012234151512 14819647415218. Acquisto terreni: sono stato un po' disubbidiente su questo argomento in quanto sotto le feste mi sono visto con la persona interessata 512151522 191212154 e siamo rimasti che dopo le feste ci dovevamo vedere per discutere [...]"

- Le sequenze numeriche si ottengono rappresentando le lettere con dei numeri, in base all'ordine alfabetico (quindi A=1, B=2, ecc.) e poi sommando un valore prefissato – in questo caso 3

4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z

- Quindi
- "10 12 23 4 15 15 12" = "Givanni"
- "14 8 19 6 4 7 4 15 21 8" = "Mercadante"
- "5 12 15 15 22" = "Binnu"
- "19 12 12 15 4" = "Riina"

La sicurezza delle informazioni «moderna»

- Oggi buona parte del pianeta vive nella **società dell'informazione**, basata cioè sull'uso delle informazioni come parte integrante delle attività umane
- Qualunque programma che si occupi di preservare la sicurezza delle informazioni, persegue, in qualche misura, tre obiettivi fondamentali:
 - **Disponibilità**
 - **Integrità**
 - **Riservatezza**

Disponibilità

- La **disponibilità** è il **grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono**
- Per esempio:
 - Sistemi di **backup locale e remoto**
 - **Firewall e Intrusion Detection System**
 - **Gruppi di continuità**

Integrità

- L'integrità è il **grado di correttezza, coerenza e affidabilità delle informazioni** e il **grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche**
- Per esempio:
 - Procedure di **manutenzione e aggiornamenti** del sistema operativo e dei programmi applicativi
 - **Antimalware** (Virus, Trojan, Spyware, Worm,...)

Riservatezza

- La **riservatezza** consiste nel **limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate**
- Per esempio:
 - **Cifratura dei dati e delle comunicazioni**
 - **Cancellazione sicura dei dati digitali**
- Ma anche il fattore umano gioca il suo ruolo
 - **Scegliere in modo adeguato una password e tenerla segreta**
 - **Rifiutare informazioni a sconosciuti** (anche quando affermano di essere tecnici della manutenzione!!)

L'avvocato hacker

- Vediamo 4 possibili scenari reali:
 1. Utilizzo una chiavetta USB per conservare i dati di un cliente e la perdo...
 2. Devo cancellare un file che ho sul computer e non voglio che si possa recuperare...
 3. Devo dismettere il vecchio computer dello studio per regalarlo all'associazione cui sono iscritto e non voglio che i dati presenti siano recuperabili...
 4. Ho tutti i dati dello studio su un solo computer e si rompe in modo irrecuperabile l'hard disk...

Esempio 1: Cifratura di una chiavetta USB

- La cifratura della chiavetta USB è una possibile soluzione, a patto che:
 - Si utilizzino **tecniche consolidate e sicure** (ovvero algoritmi di cifratura affidabili e senza falle riconosciute, es. AES, Serpent, Twofish)
 - Si scelga una **password adeguata** (no parole di un dizionario, nomi propri, date di nascita, troppo corte, si frasi lunghe, ma per voi facili da ricordare con maiuscole, minuscole, numeri e simboli es. **@GenovaCiSono2Squadre (21 caratteri)**)
 - Potete utilizzare un calcolatore per il tempo di violazione della password disponibile online
<http://lastbit.com/pswcalc.asp>

Passo 1: Scarico TrueCrypt

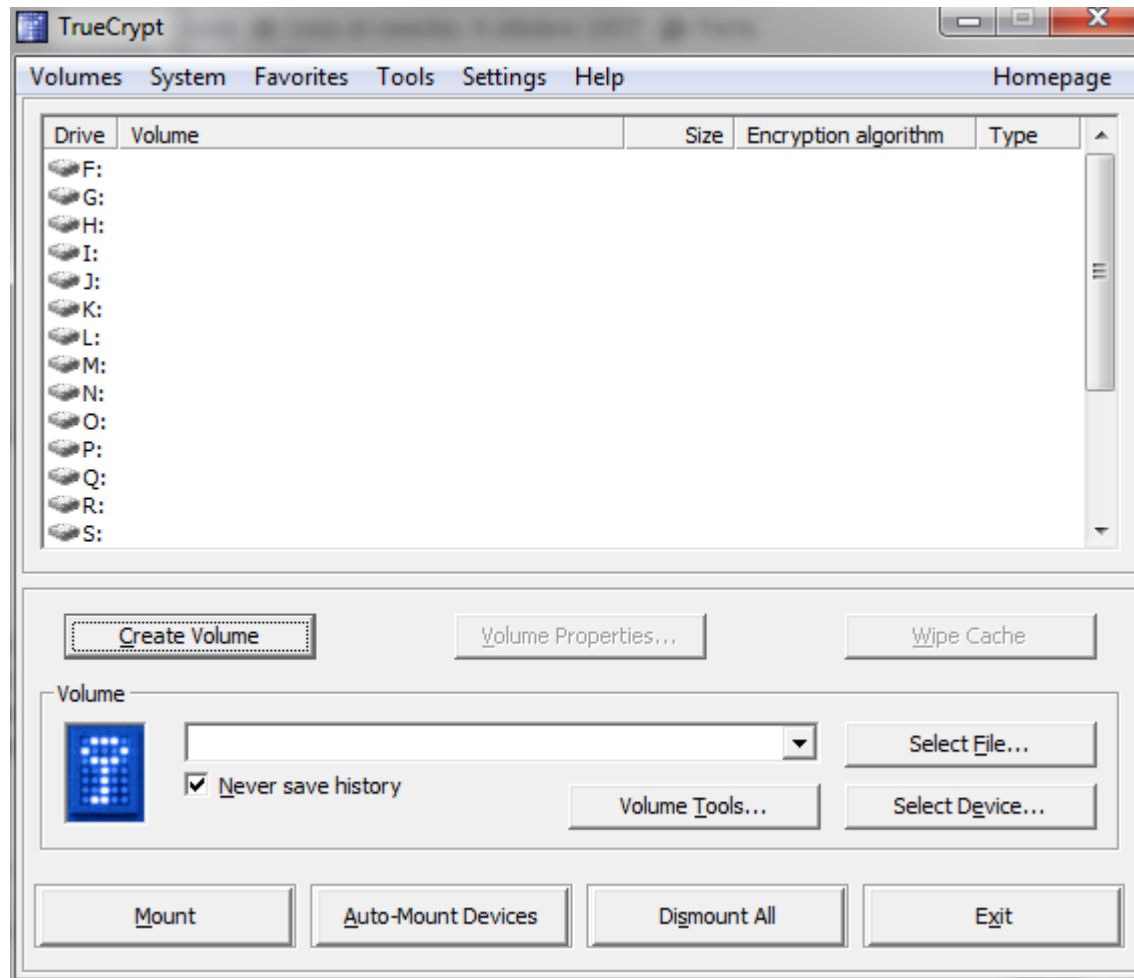
- Sito web: www.truecrypt.org
- Disponibile per Windows, Mac OS X e Linux



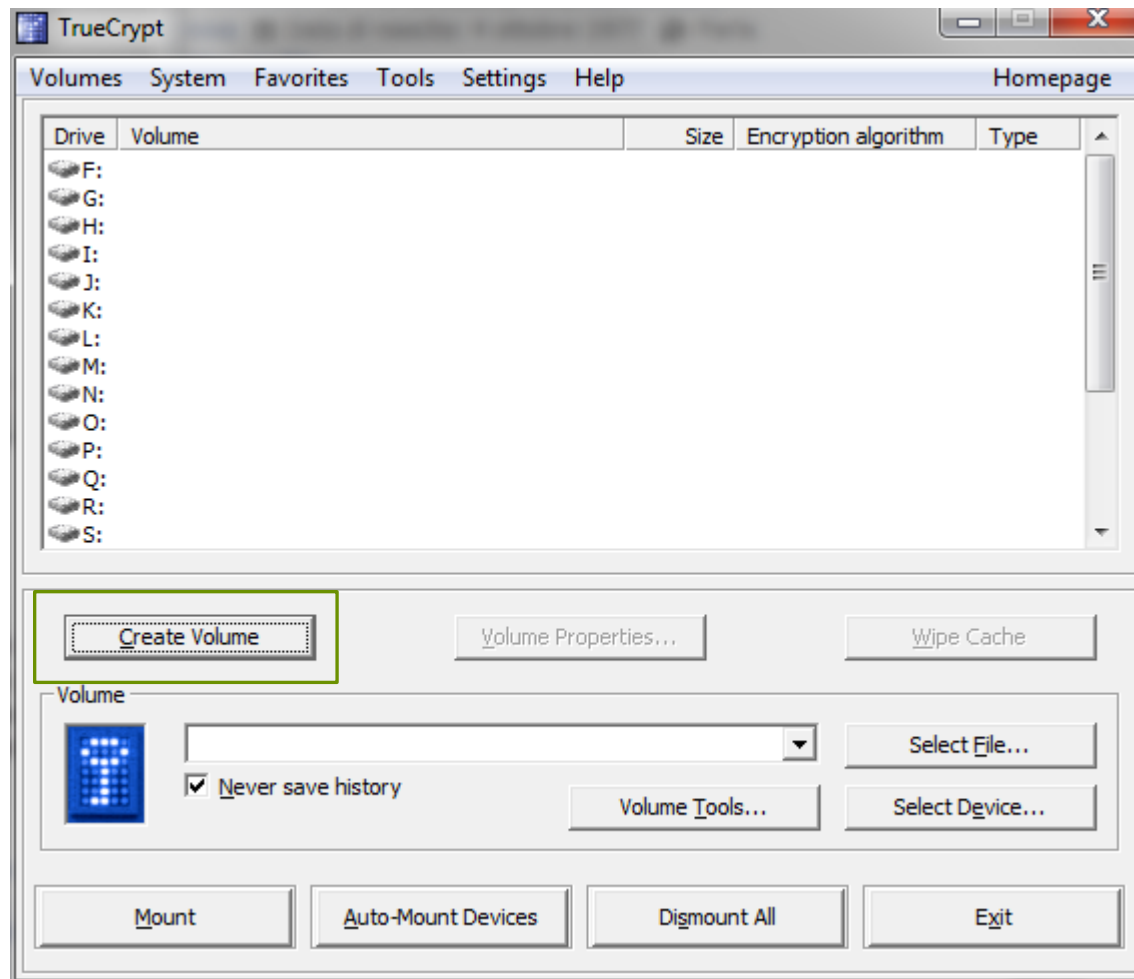
TrueCrypt

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

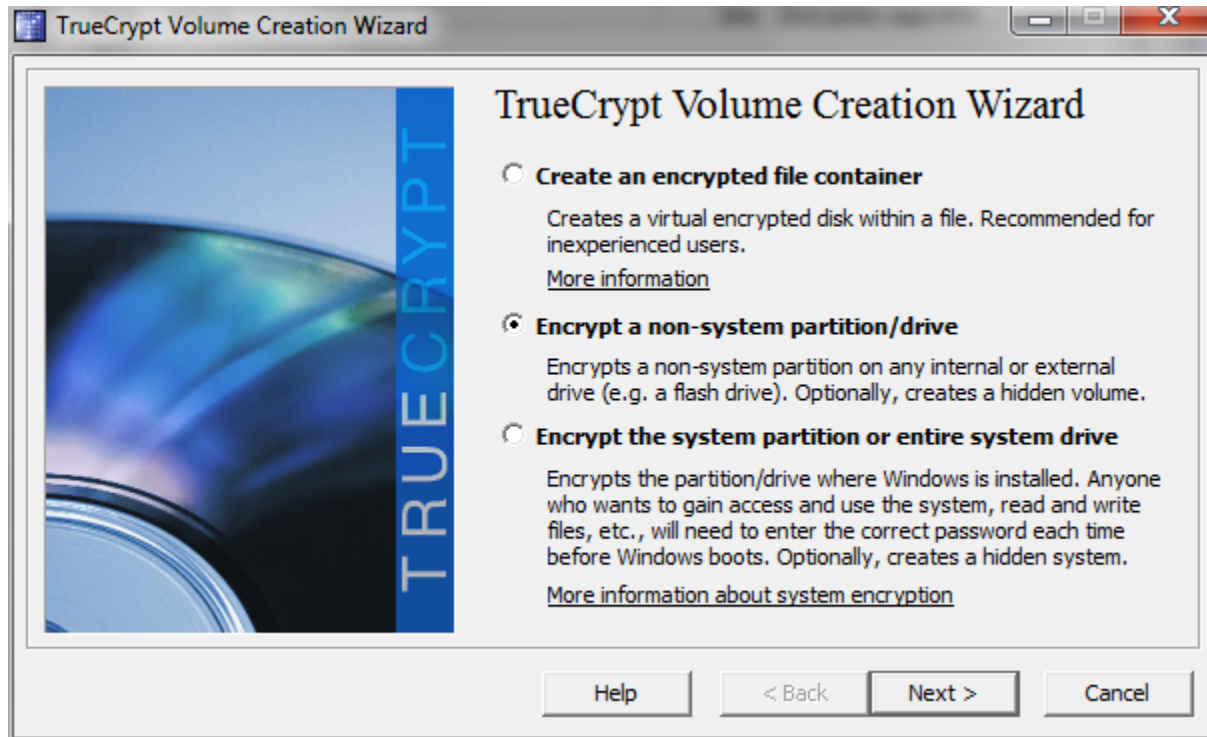
Passo 2: Eseguo il software



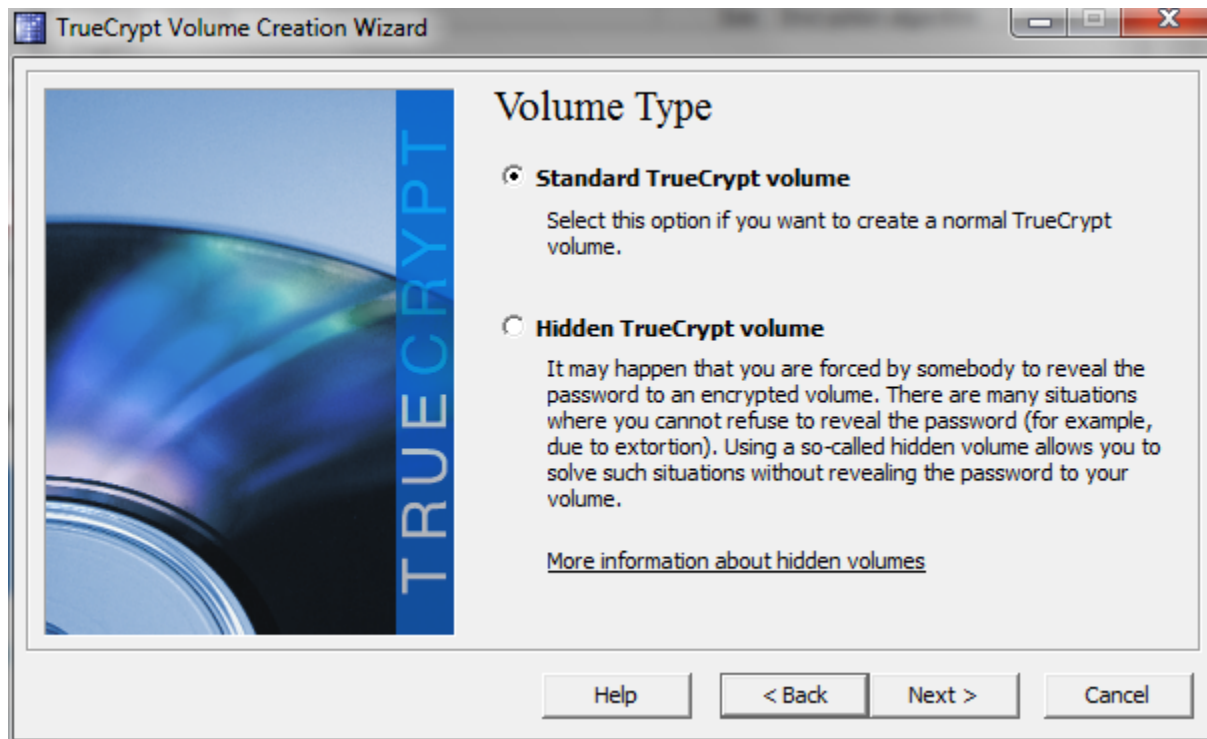
Passo 3: Creo il volume



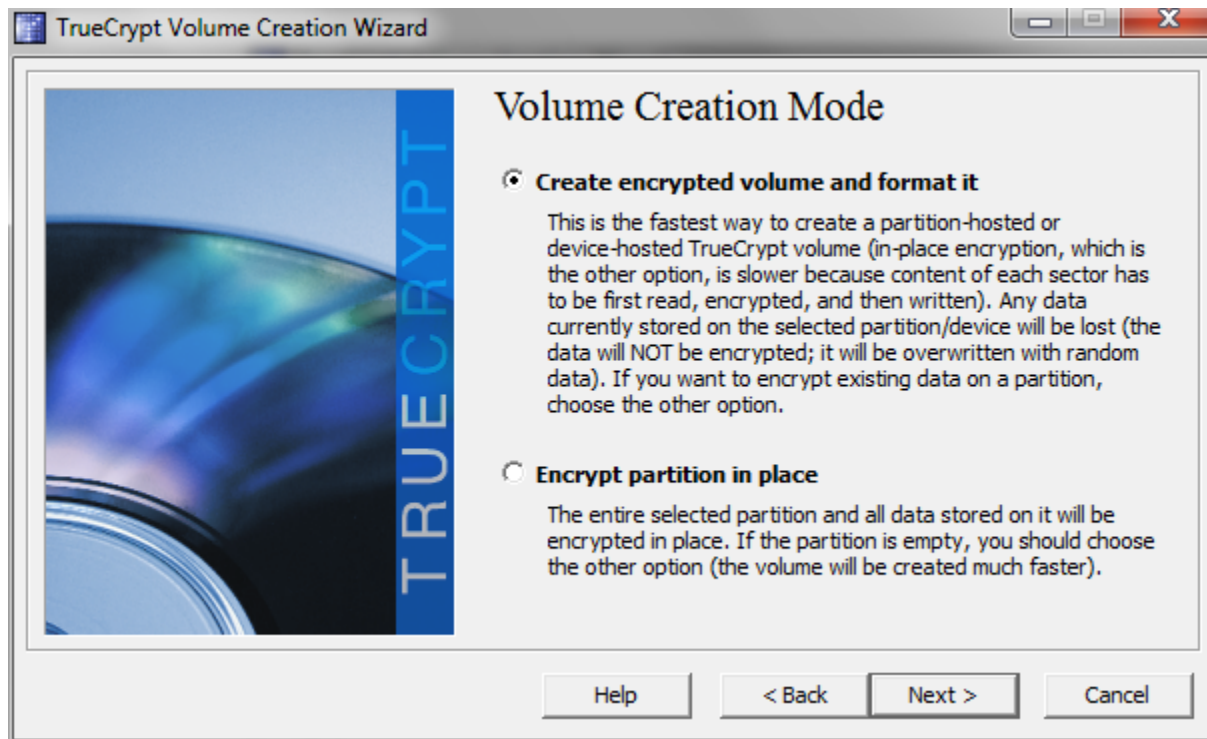
Passo 4: Seleziono il tipo



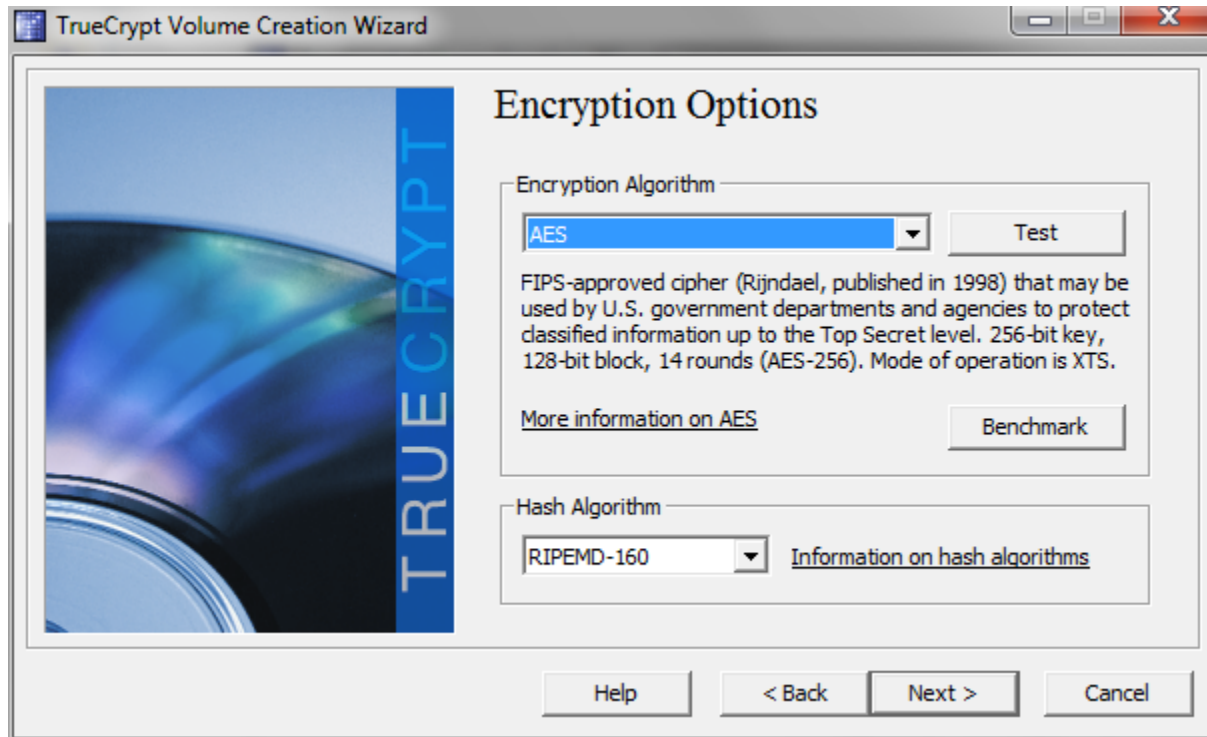
Passo 5: Seleziono il tipo



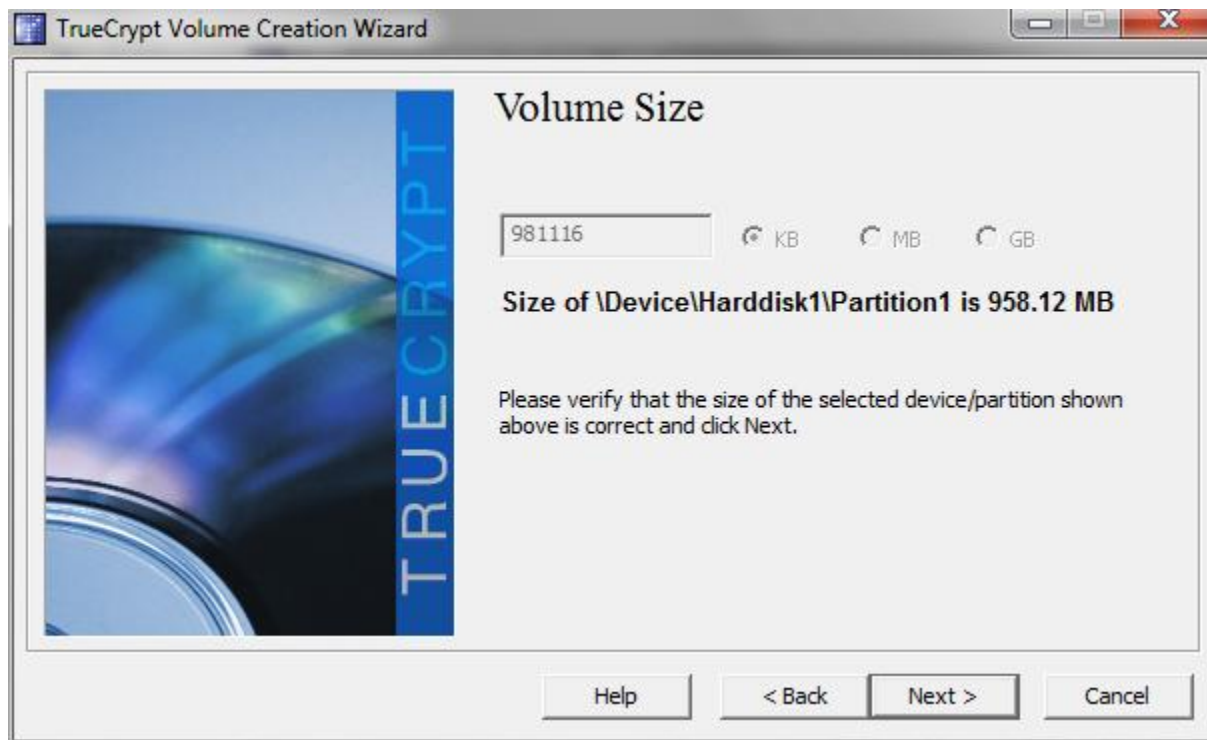
Passo 6: Scelgo la modalità



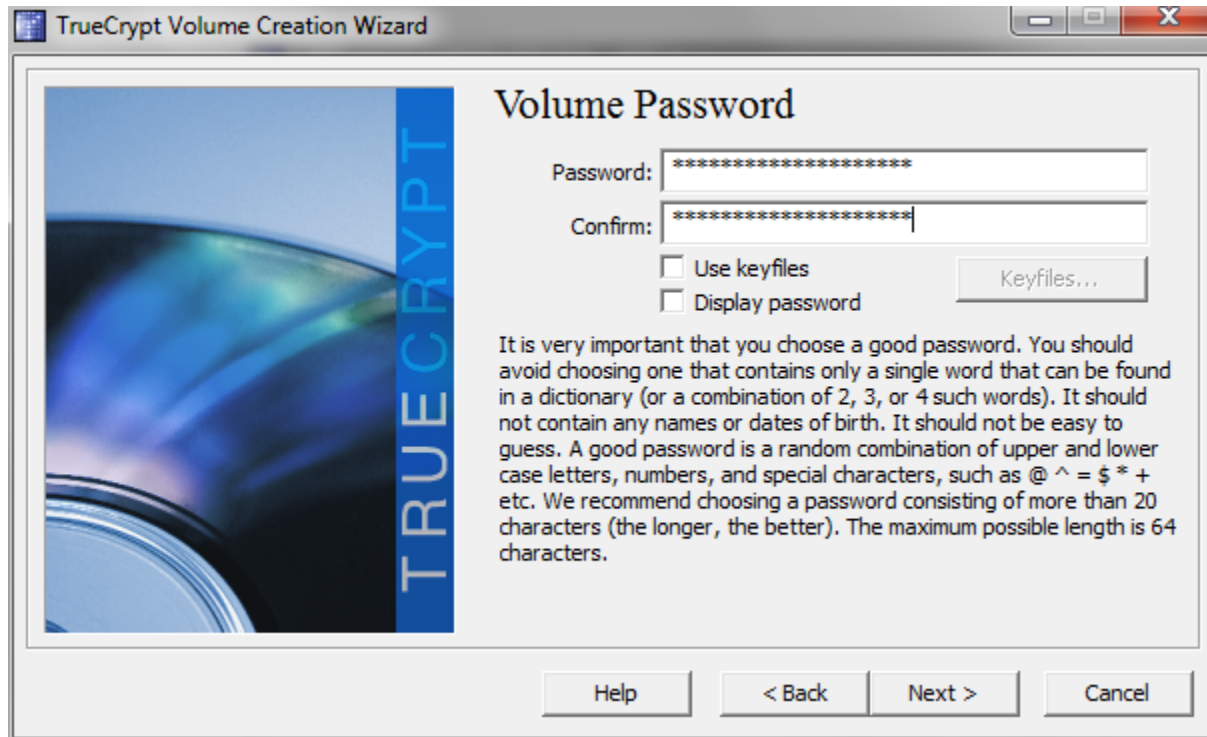
Passo 7: Scelgo l'algoritmo



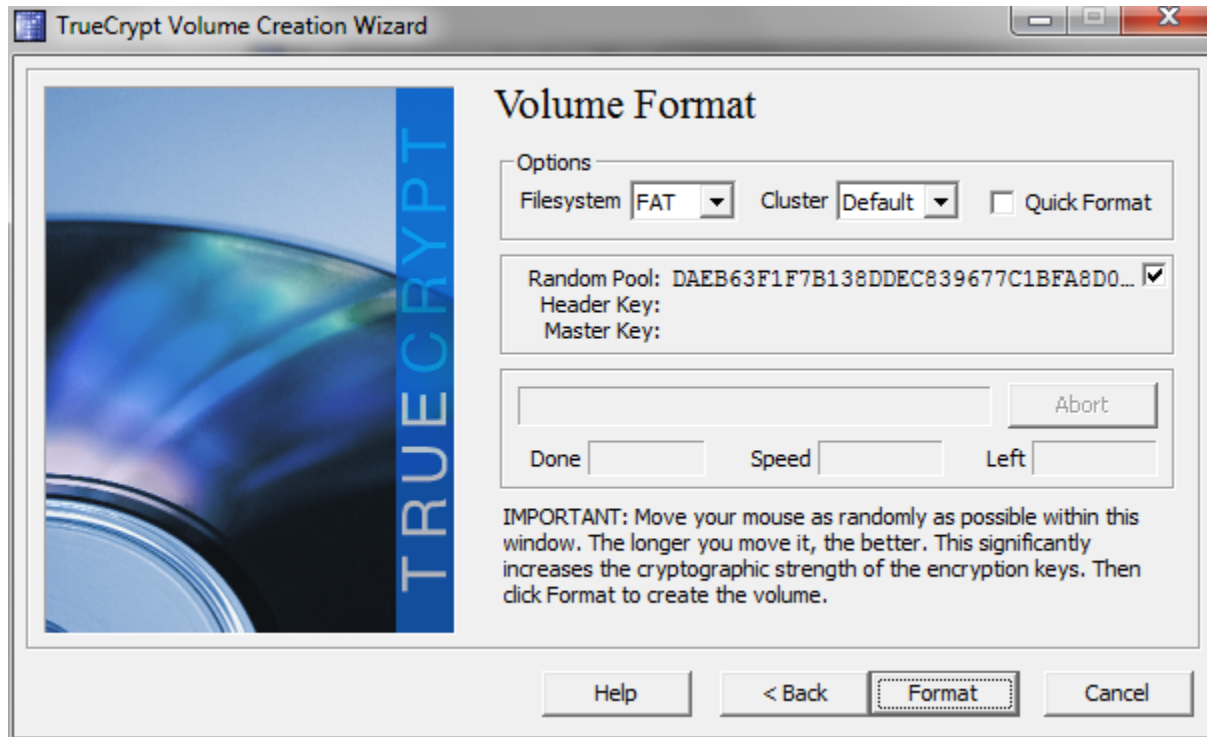
Passo 8: Scelgo la dimensione



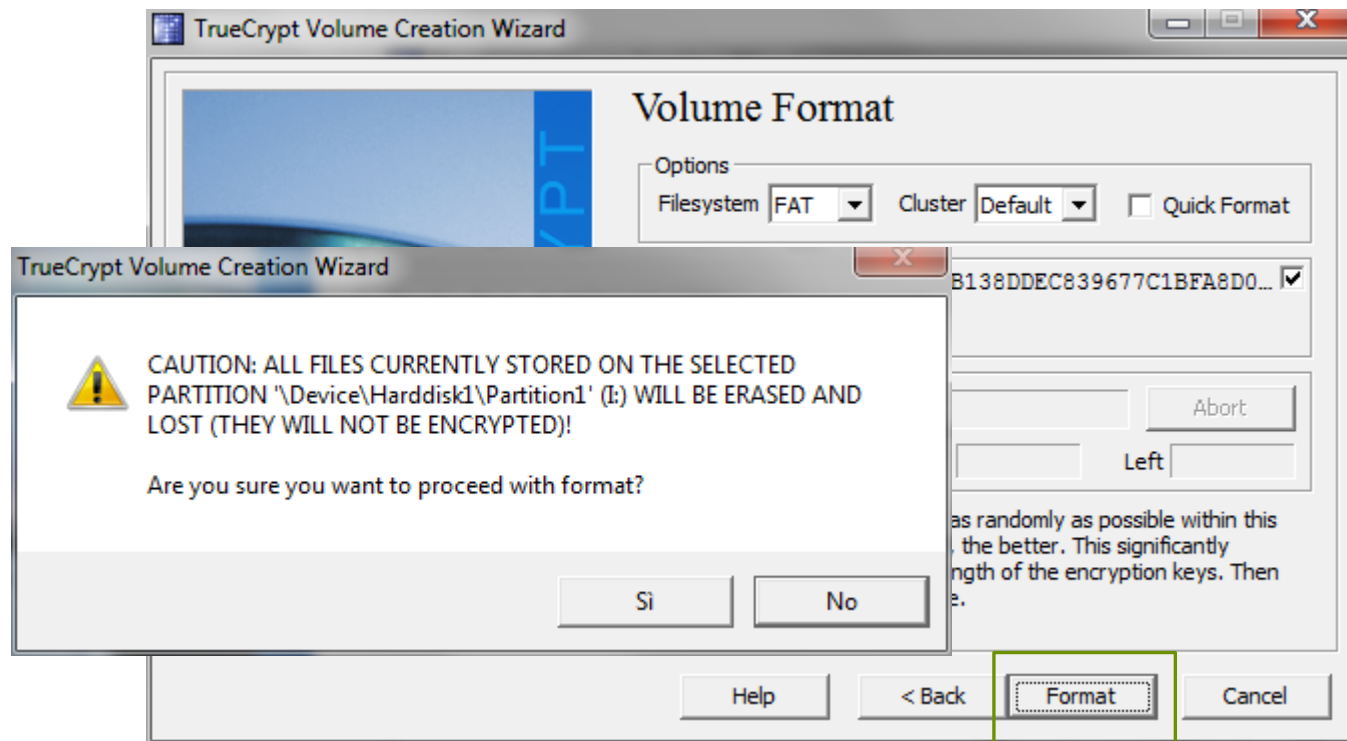
Passo 9: Scelgo la password



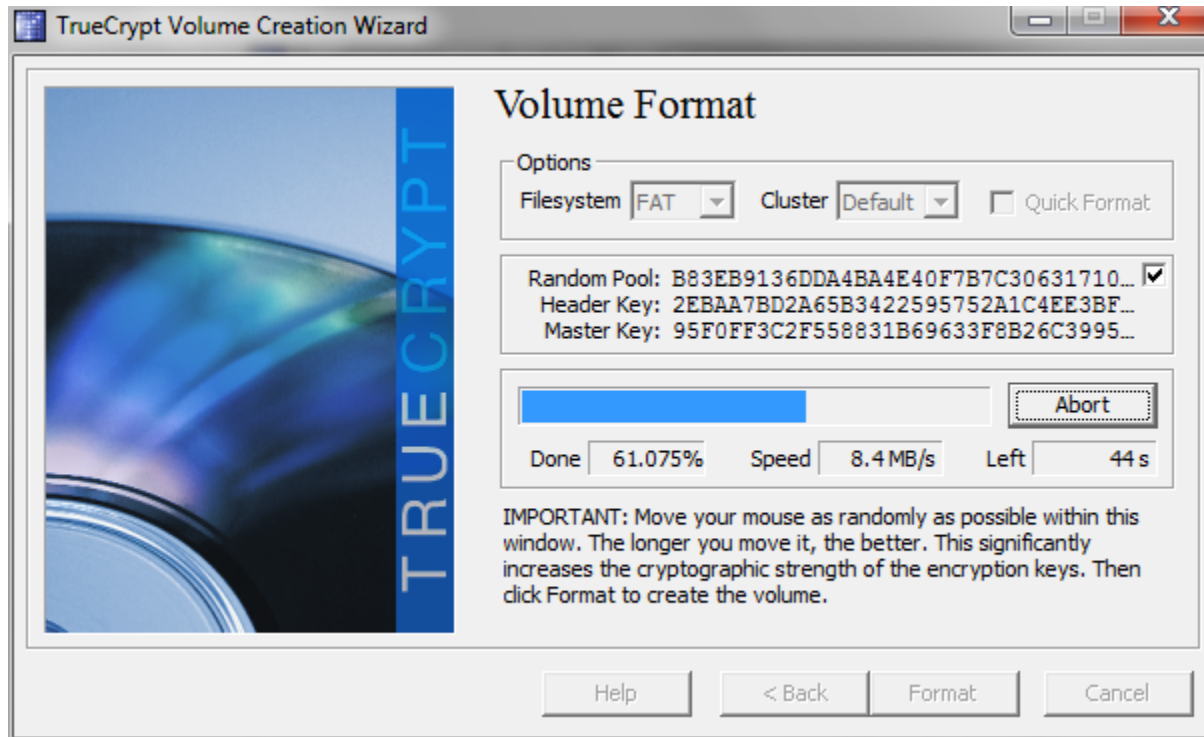
Passo 10: Scelgo il FileSystem



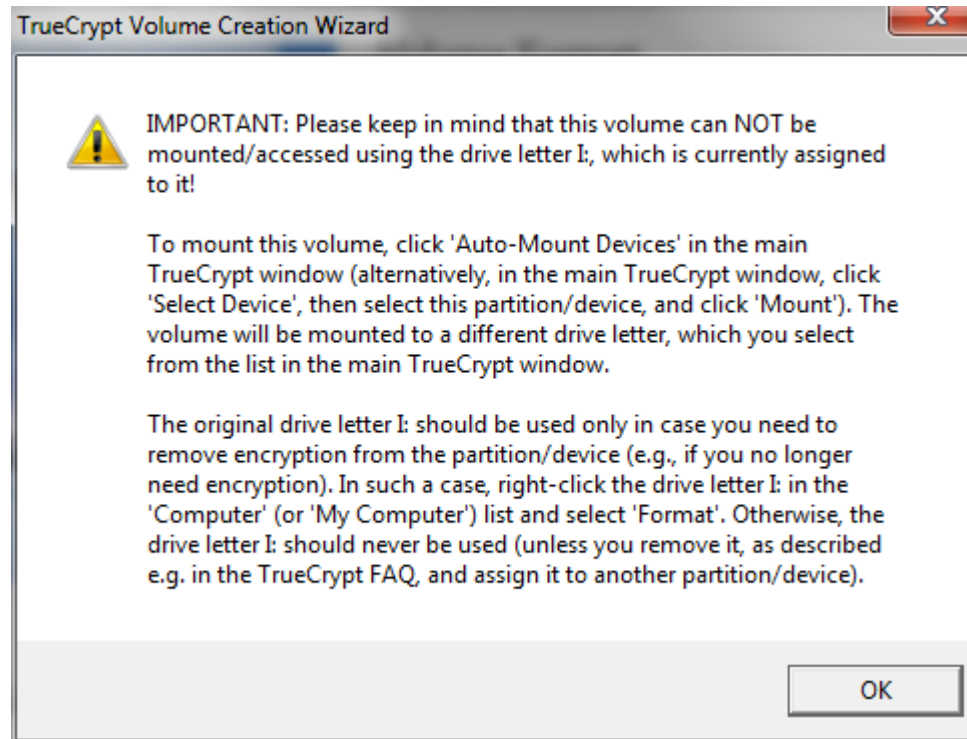
Passo 11: Formatto



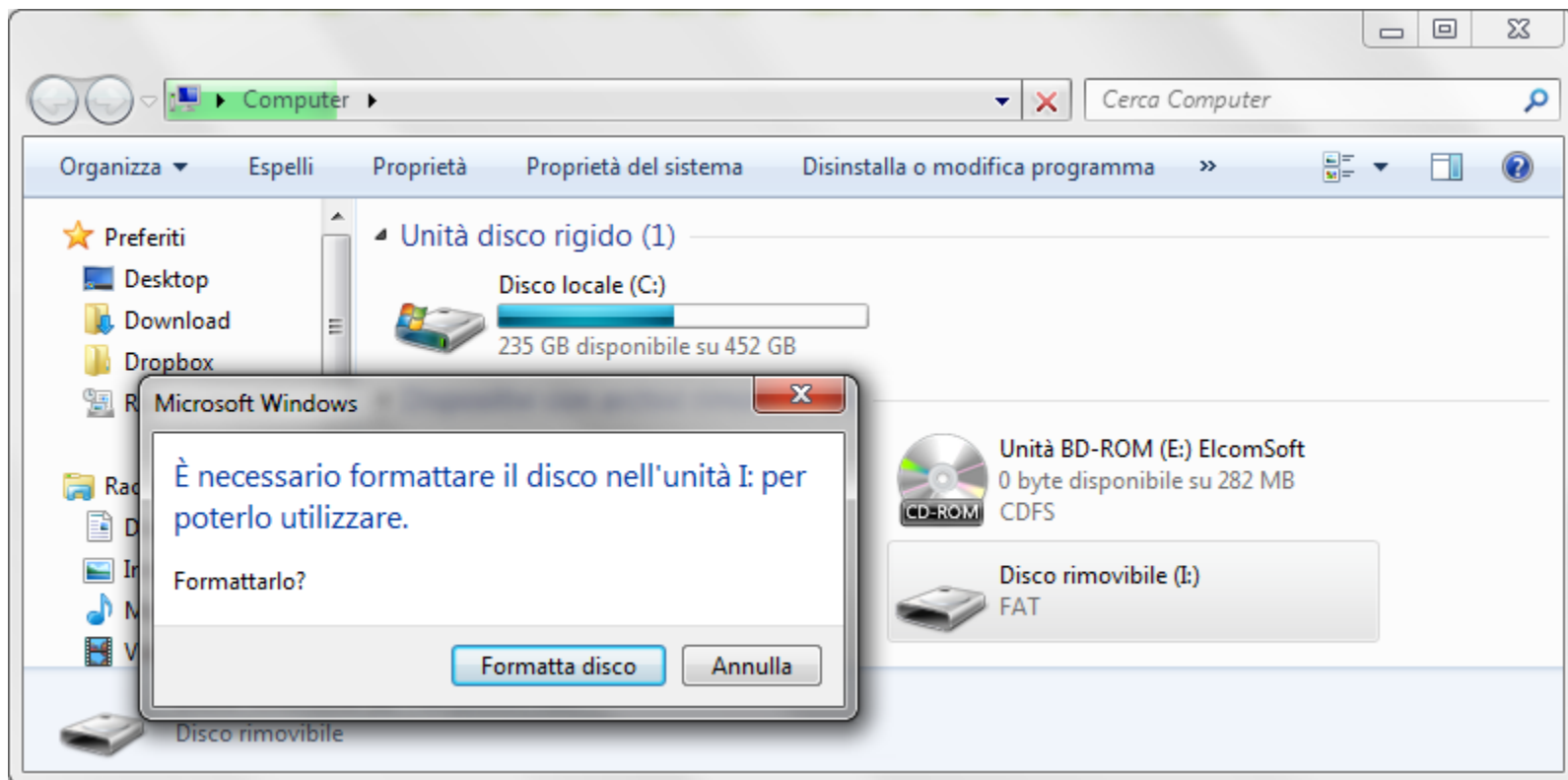
Passo 12: Attendo...



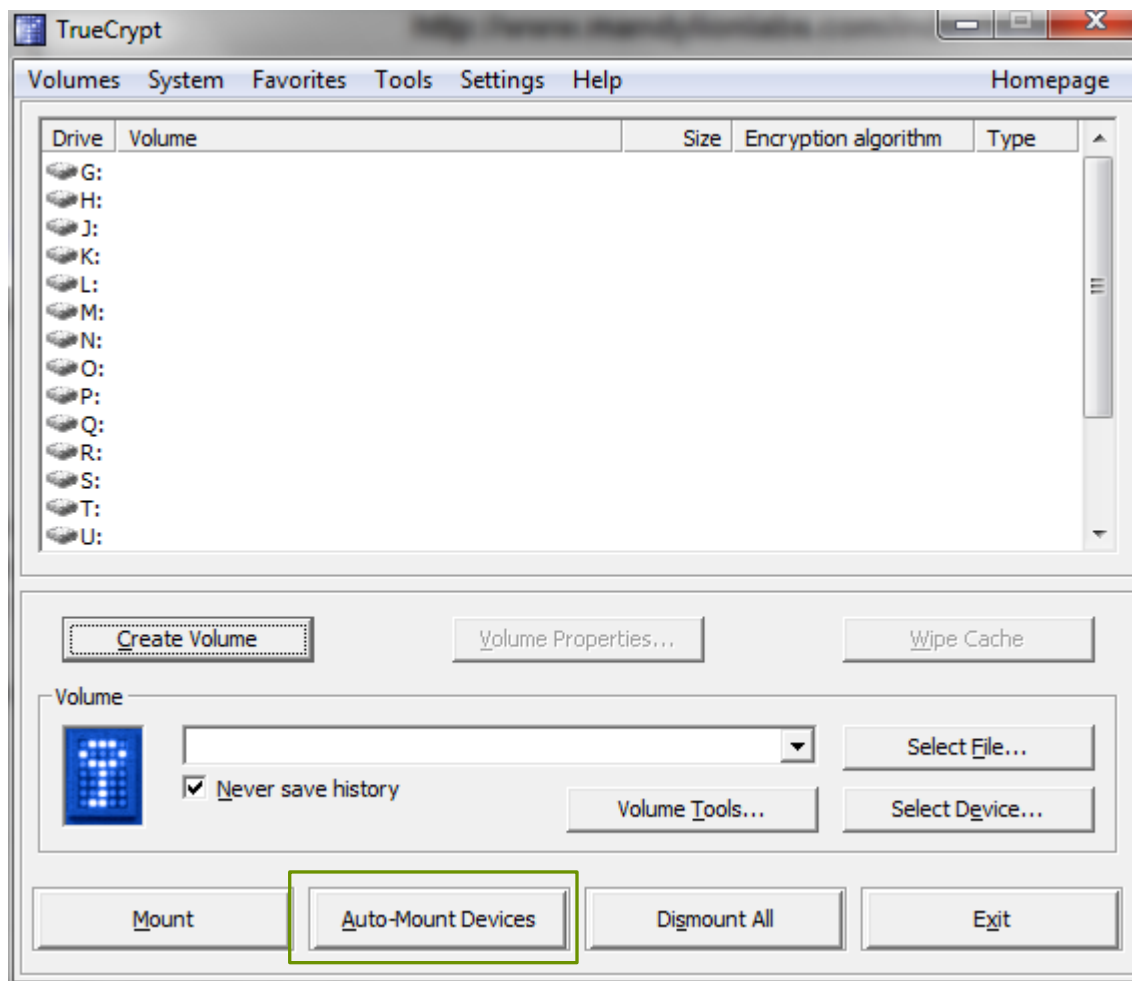
Passo 13: Leggo...



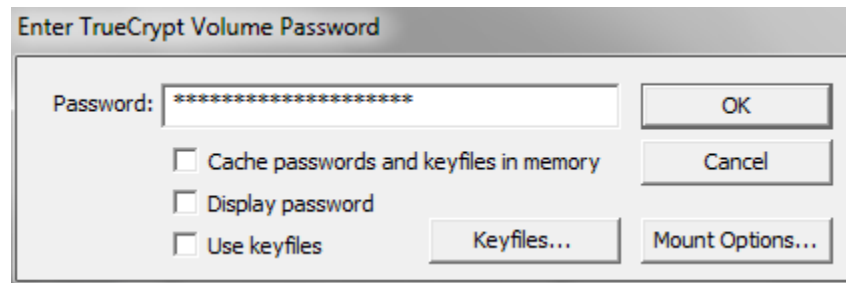
Come accedo al volume?



Passo 1: Monto la chiavetta



Passo 2: Inserisco la password



The image shows a screenshot of a Windows dialog box titled "Enter TrueCrypt Volume Password". The dialog box has a light gray background and a white border. At the top, the title "Enter TrueCrypt Volume Password" is displayed in a small, dark font. Below the title, there is a "Password:" label followed by a text input field containing a series of asterisks. To the right of the input field is an "OK" button. Below the input field, there are three checkboxes, each followed by a label: "Cache passwords and keyfiles in memory", "Display password", and "Use keyfiles". To the right of these checkboxes are two more buttons: "Cancel" and "Mount Options...". At the bottom of the dialog box, there are two buttons: "Keyfiles..." and "Mount Options...".

Enter TrueCrypt Volume Password

Password: *****

Cache passwords and keyfiles in memory

Display password

Use keyfiles

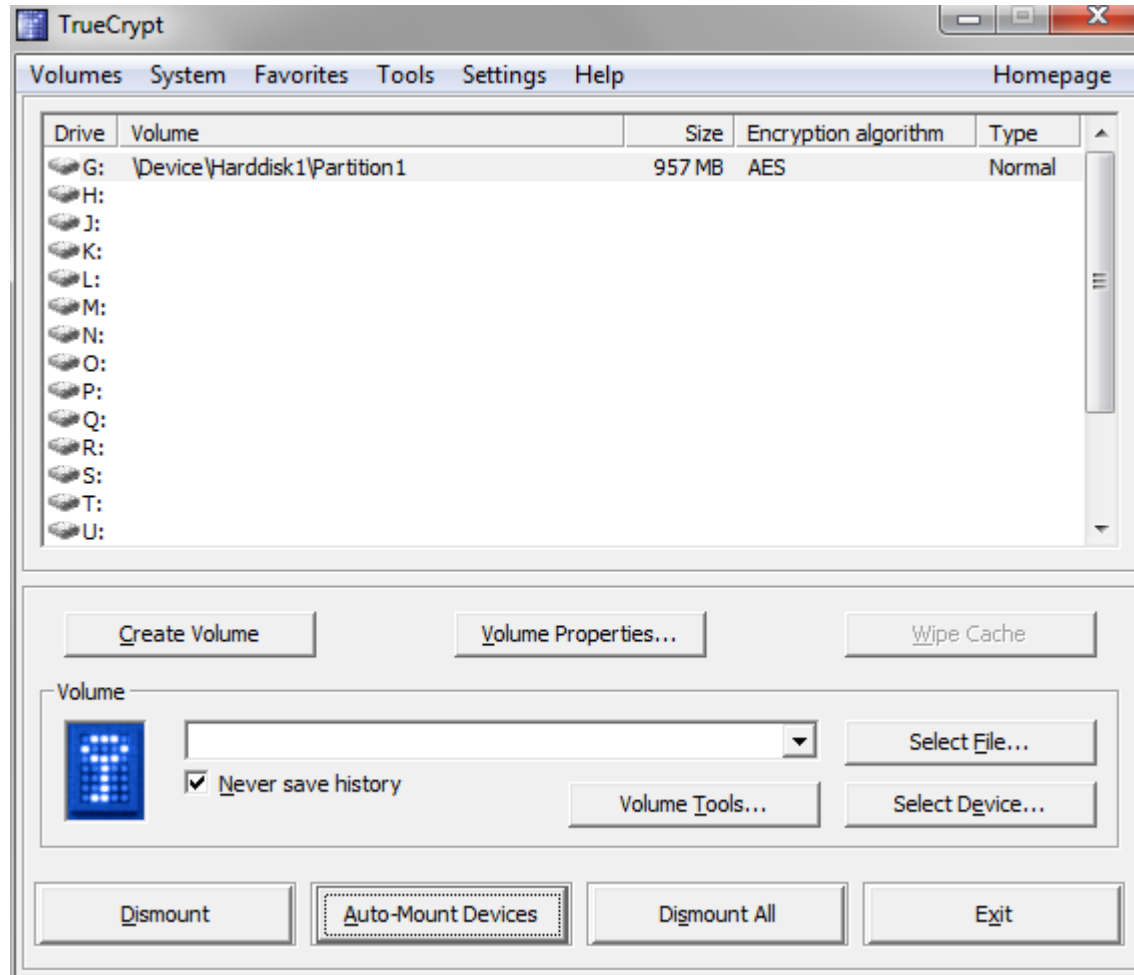
OK

Cancel

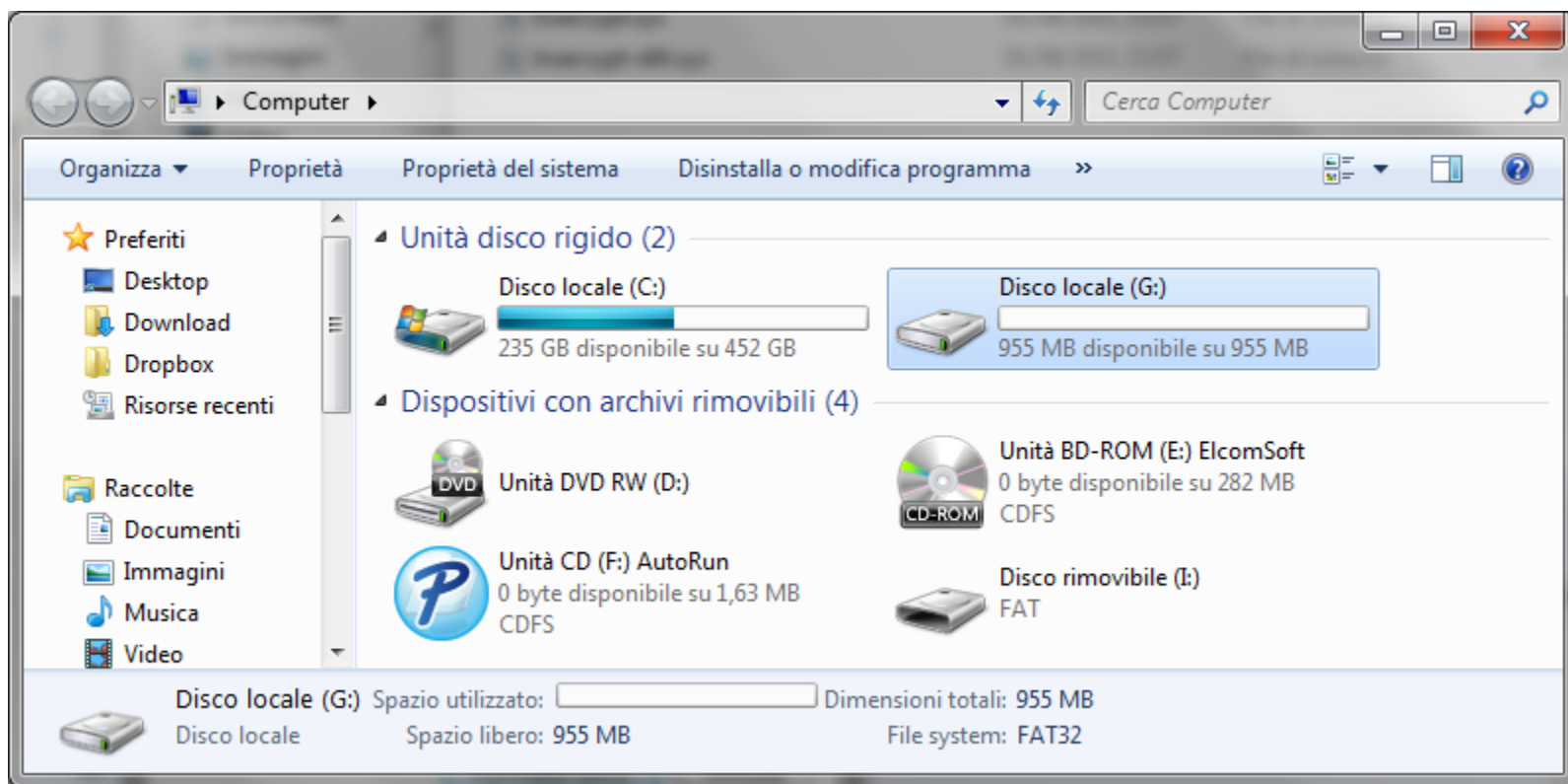
Keyfiles...

Mount Options...

Passo 3: Visualizzo...



Passo 4: Accedo...

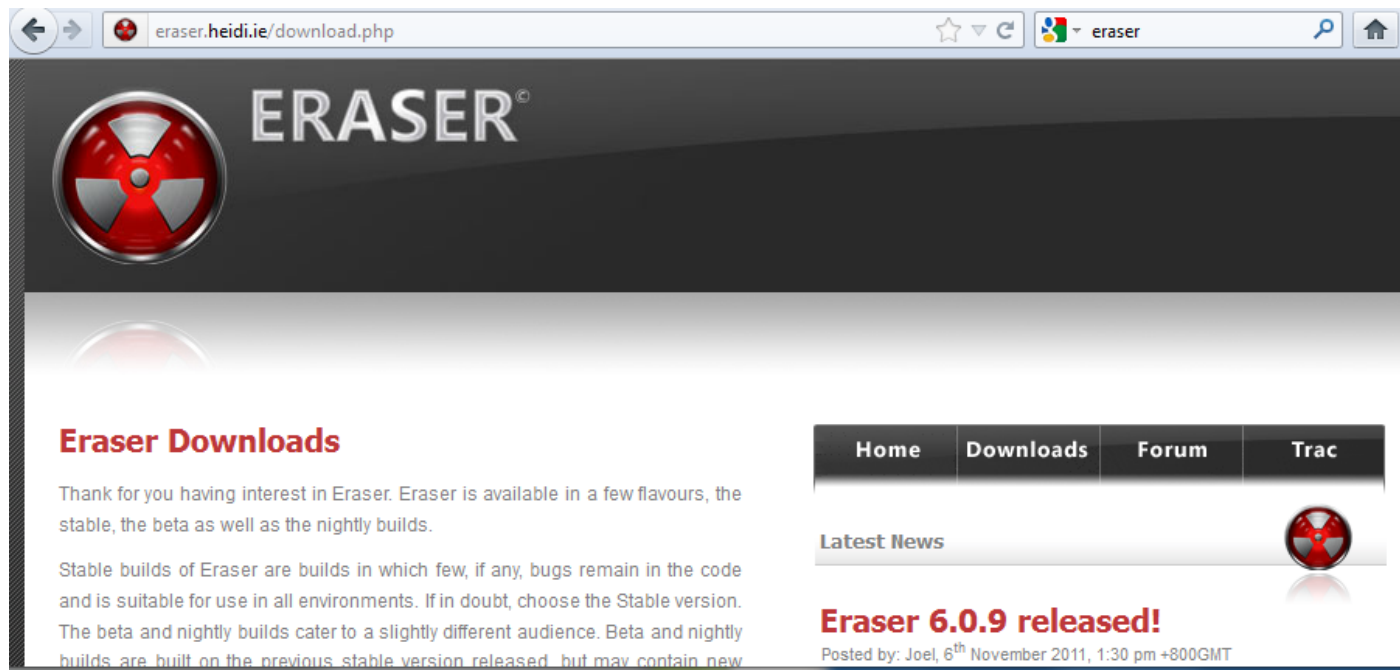


Esempio 2: Cancellazione sicura di un file

- La cancellazione di un file attraverso la funzione «Elimina» di un sistema operativo **non cancella in modo definitivo** il file
- E' come cancellare da un libro i riferimenti a un capitolo dell'indice e sperare che qualcuno che lo sfoglia tutto non si accorga del capitolo in più...
- Esistono diversi software di **data recovery** anche gratuiti per recuperare i file cancellati attraverso Windows (e in molti casi possono essere utilissimi...es. Recuva - <http://www.piriform.com/>)
- Per garantire una cancellazione sicura di un file devo **sovrascriverlo con sequenze di zeri oppure dati casuali**

Passo 1: Scarico Eraser

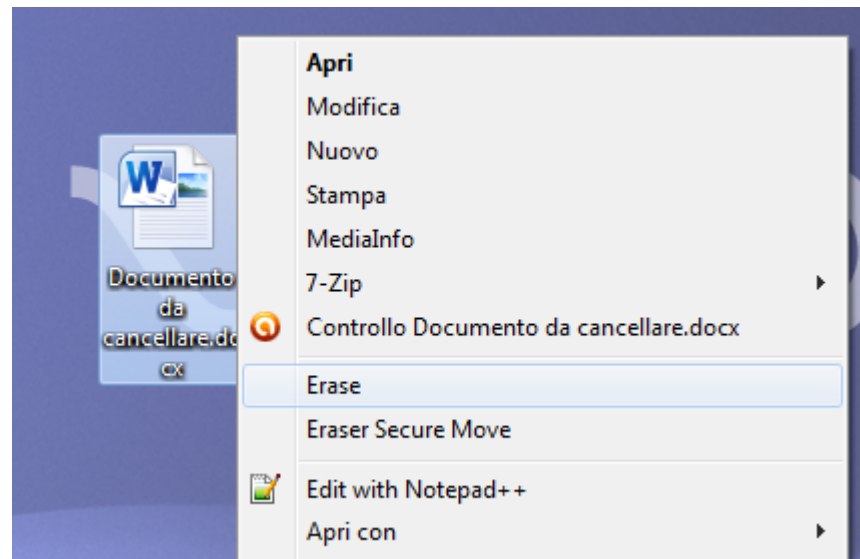
- Sito web: <http://eraser.heidi.ie/>
- Disponibile per Windows



The screenshot shows a web browser window with the address bar displaying "eraser.heidi.ie/download.php". The page features the Eraser logo, which is a red radiation symbol inside a circular frame, and the word "ERASER" in a bold, white, sans-serif font. Below the logo, the text "Eraser Downloads" is written in red. The main content area contains a paragraph of text: "Thank for you having interest in Eraser. Eraser is available in a few flavours, the stable, the beta as well as the nightly builds." followed by another paragraph: "Stable builds of Eraser are builds in which few, if any, bugs remain in the code and is suitable for use in all environments. If in doubt, choose the Stable version. The beta and nightly builds cater to a slightly different audience. Beta and nightly builds are built on the previous stable version released, but may contain new". To the right of the main content, there is a navigation menu with four buttons: "Home", "Downloads", "Forum", and "Trac". Below the navigation menu, there is a "Latest News" section with a small radiation symbol icon and a headline "Eraser 6.0.9 released!". The text below the headline reads "Posted by: Joel, 6th November 2011, 1:30 pm +800GMT".

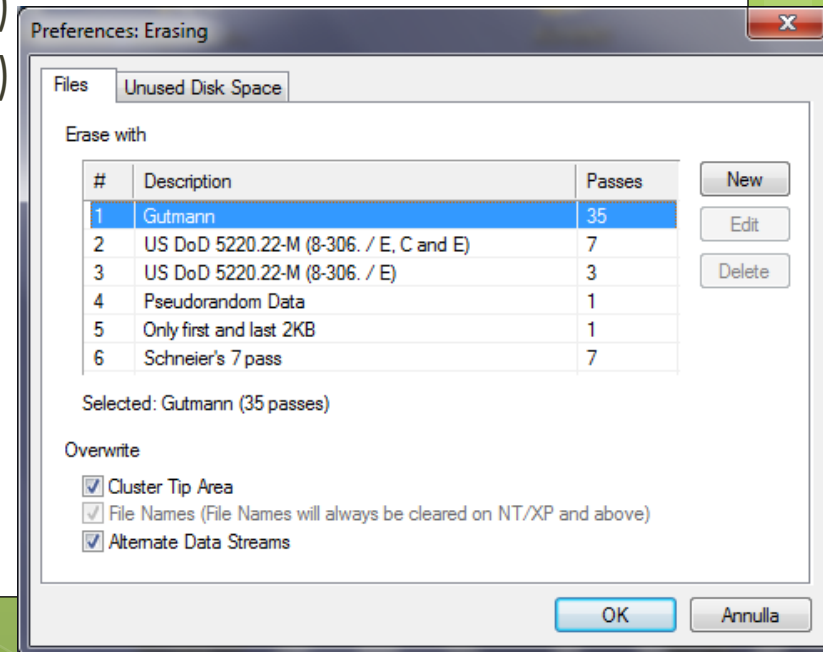
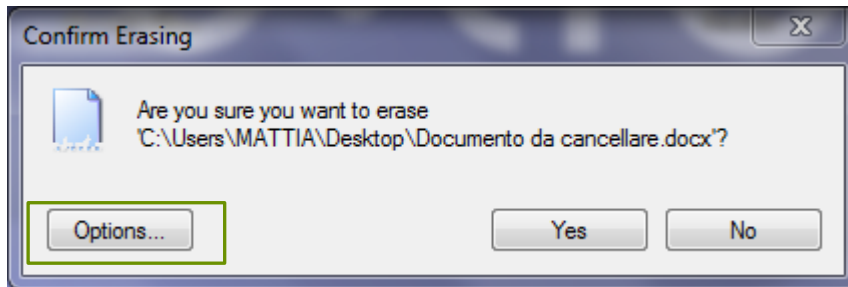
Passo 2: Cancellare in modo sicuro il file

- Click con il tasto destro sul file
- Scelgo la voce **Erase**

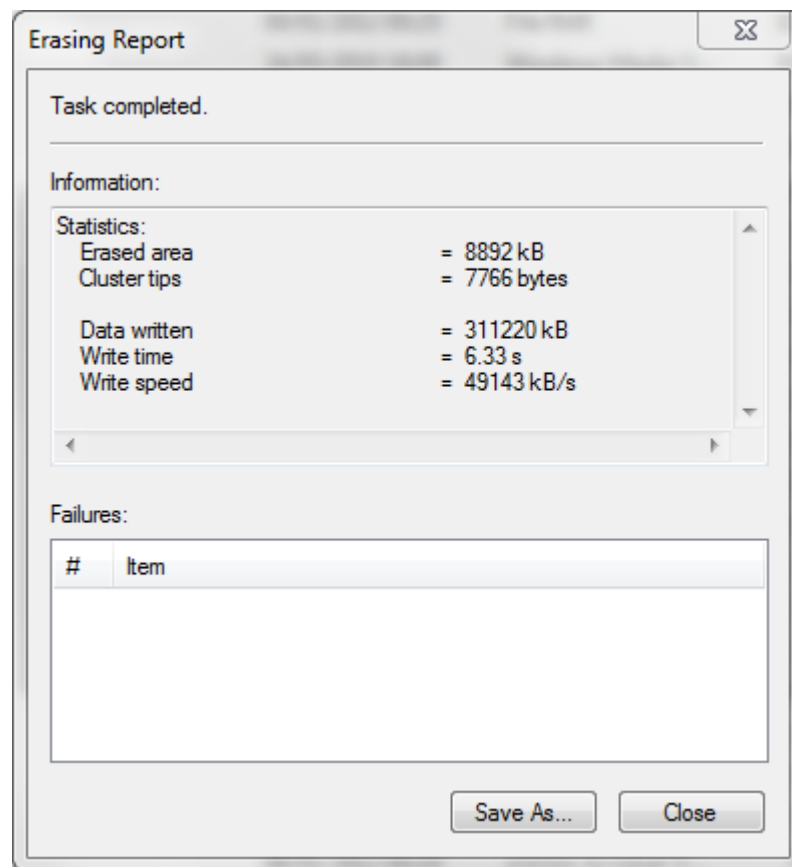
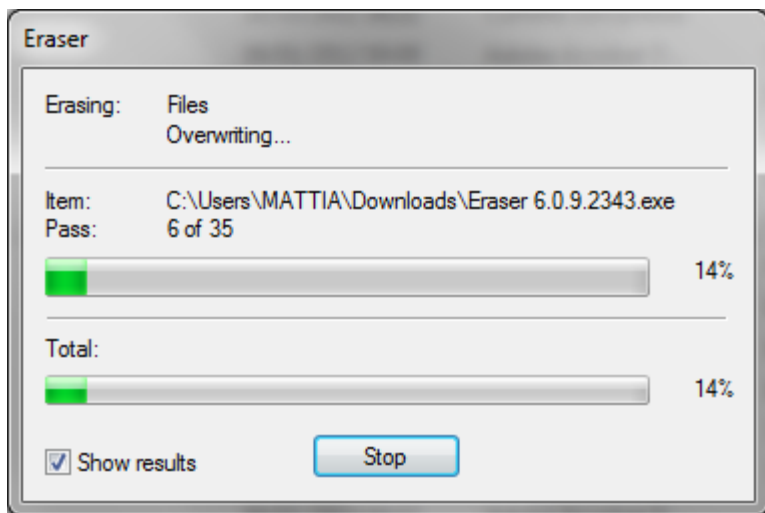


Passo 3: Scelgo le opzioni

- Nella schermata che compare faccio click sul tasto «Options»
- Scelgo l'algoritmo di cancellazione sicura
 - Dati casuali (1 passaggio)
 - US DoD 5220.22-M (3 passaggi)
 - US DoD 5220.22-M (7 passaggi)
 - Gutmann (35 passaggi)



Passo 4: Attendo...

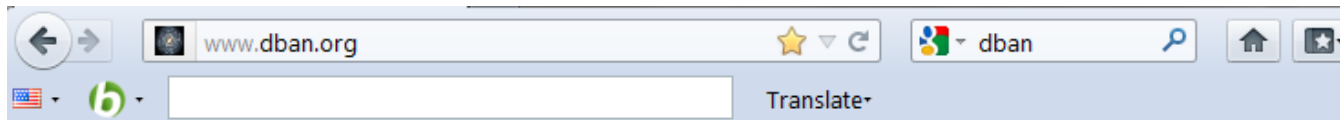


Esempio 3: Cancellazione sicura di hard disk

- Il principio è analogo a prima: cancellazione mediante sovrascrittura
- In questo caso non cancello un singolo file ma l'intero contenuto di un hard disk
- Diverse soluzioni gratuite per raggiungere il risultato:
 - Active Kill Disk for Windows (<http://www.killdisk.com/>)
 - DBAN (Darik's Boot and Nuke) (<http://www.dban.org/>)
 - DiskWipe (<http://www.diskwipe.org/>)

Passo 1: Scarico DBAN

- Sito web: <http://www.dban.org/>
- CD di avvio del computer per la cancellazione sicura



Darik's Boot And Nuke

[Download](#) | [Help](#) | [News](#) | [Contact](#) | [About DBAN](#)
[SourceForge Project Page](#) | [Development Status](#) | [Documentation](#)



About DBAN

Darik's Boot and Nuke ("DBAN") is a self-contained boot disk that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction. DBAN is a means of ensuring due diligence in computer recycling, a way of preventing identity theft if you want to sell a computer, and a good way to totally clean a Microsoft Windows installation of viruses and spyware.

Passo 2: Masterizzo su CD

- Utilizzo p.es. CD Burner XP (<http://cdburnerxp.se/>) e scelgo l'opzione «**Masterizza immagine ISO**»



Passo 2: Avvio il computer da CD

- Avvio il computer da cancellare con il CD appena creato

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 to read the RAID disclaimer.
- * Press the ENTER key to start DBAN in interactive mode.
- * Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _

Passo 3: Scelgo il metodo

- Al termine del caricamento premo il tasto «M» per scegliere il metodo di cancellazione sicura

```
Darik's Boot and Nuke 2.2.6 (beta)
----- 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:

----- 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.
```


Passo 4: Scelgo il disco

- Dalla schermata principale scelgo l'hard disk da cancellare e premo «spazio» per selezionarlo

```
Darik's Boot and Nuke 2.2.6 (beta)
----- 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:
----- Disks and Partitions -----
▶ [   ] ATA Disk VMware Virtual I 0000 40GB 00000000000000000001

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

Passo 5: Avvio la procedura

- Per avviare la procedura premo il tasto «F10» e attendo il completamento

```
Darik's Boot and Nuke 2.2.6 (beta)
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Merseenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1

----- Statistics -----
Runtime:    00:01:16
Remaining:  08:56:49
Load Averages: 1.08 0.46 0.19
Throughput: 6650 KB/s
Errors:     0

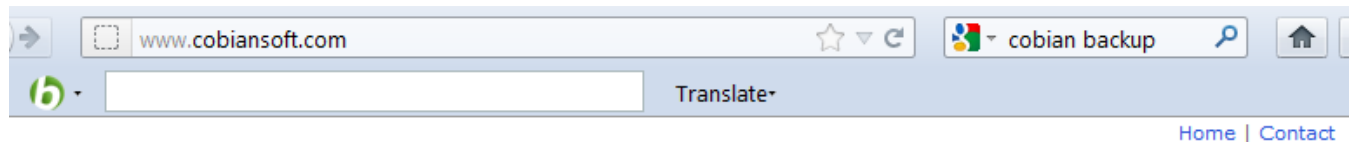
ATA Disk VMware Virtual I 0000 40GB 00000000000000000001
[00.24%, round 1 of 1, pass 1 of 3] [writing] [6650 KB/s]
```

Esempio 4: Backup dei dati

- Un backup consiste nella copia dei dati personali di un utente
- Richiede un supporto di storage diverso rispetto a quello che contiene i dati originali (p.es. CD/DVD, Chiavetta USB, Hard Disk esterno, NAS Server)
- E' inoltre necessario un software che **a intervalli predefiniti** copi il contenuto dell'origine sulla destinazione
- Diverse soluzioni gratuite:
 - Cobian Backup (<http://www.cobiansoft.com/>)
 - Uranium Backup (<http://www.uraniumbackup.com>)

Passo 1: Scarico Cobian

- Sito web: <http://www.cobiansoft.com/>



Navigation

Home

News

About

Personal

Pictures

Software

Cobian Backup

Cobian Poirot

Other software

Obsolete

Forum

Guest book

Hello and welcome to Cobian's site!

Welcome to Cobian's site, the home of [Cobian Backup](#). This is both a personal site and site about software development.

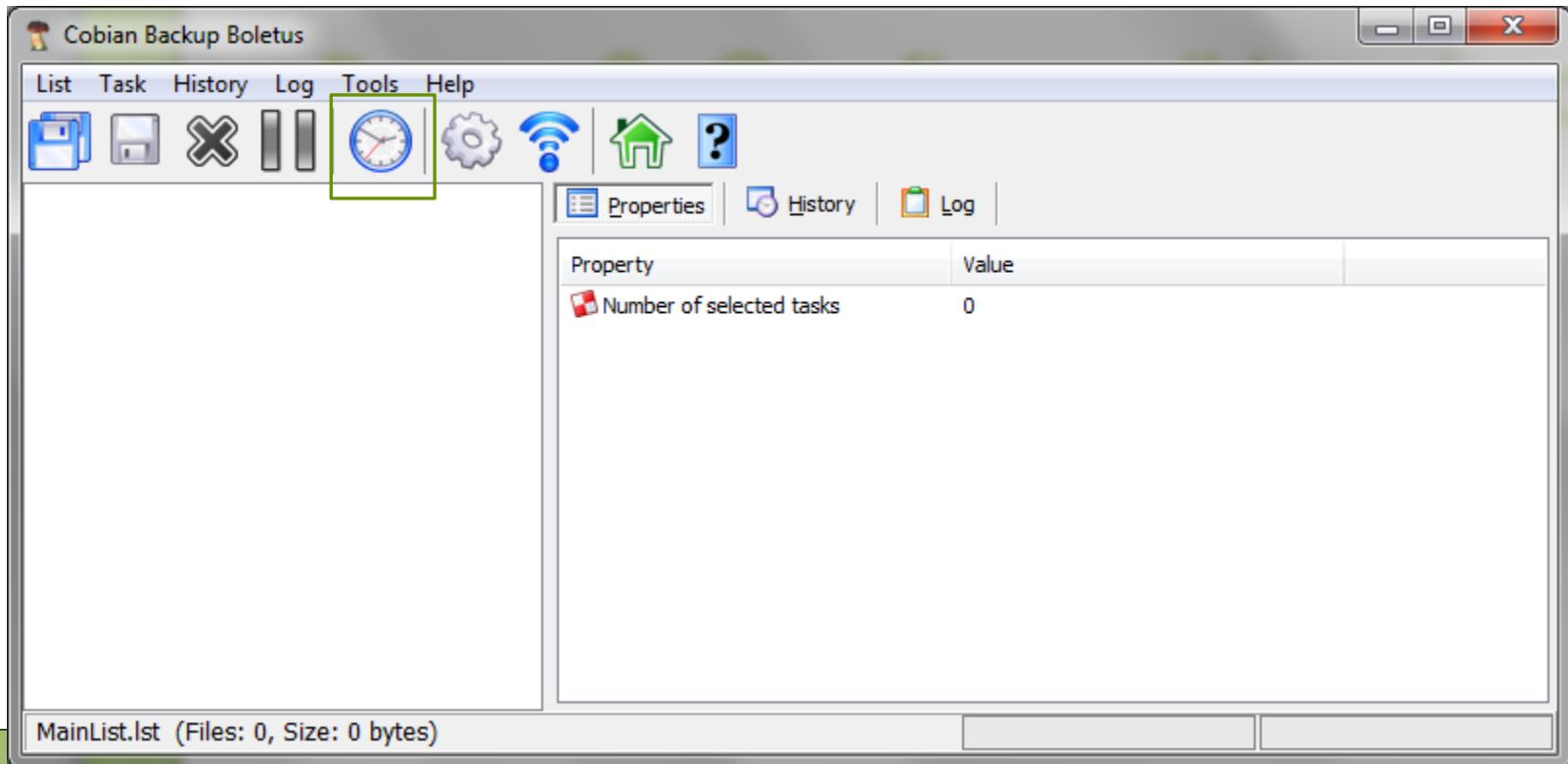
Please feel free to walk around my site and download any of my programs. Because of the popularity of Cobian Backup, which now is in its 9th version, I am actively supporting only that product. If you have some questions about Cobian Backup, please read the Help file and the FAQ first, and if you don't find the answer to your question there, post it to the [support forum](#) and I or other users will gladly try to help you.

Here you can download some other programs developed by me as well. Some useful utilities like Cobian Herald (a mailing list server), CobView (a multipurpose Windows Shell extension) and CobDDNS (a client updater for EditZone dynamic DNS) can be downloaded from [Other software](#).



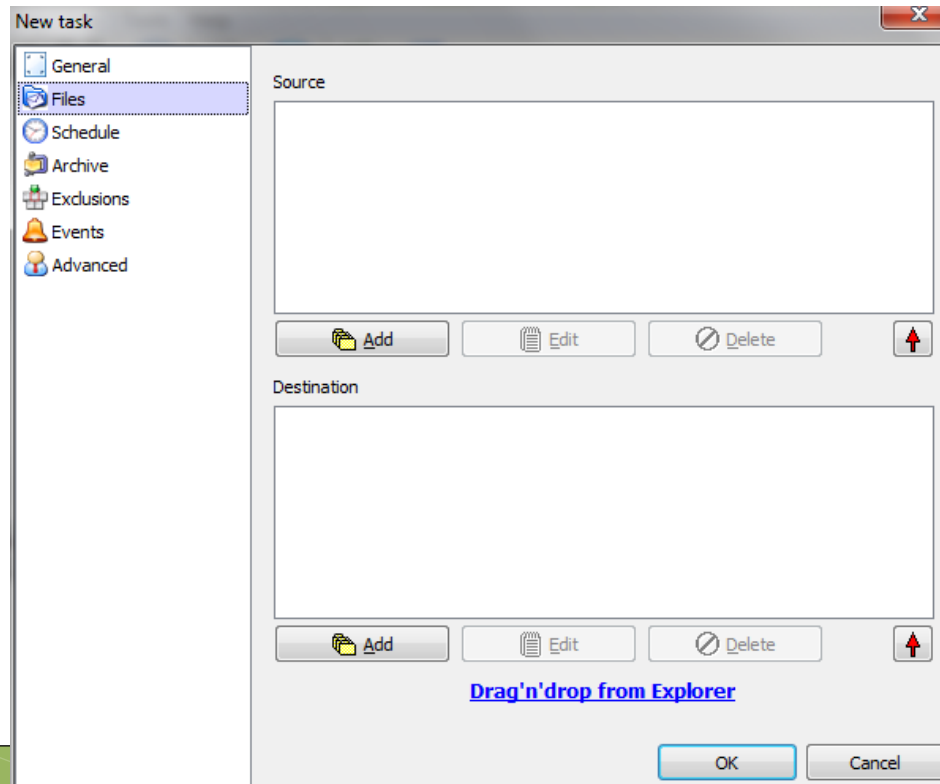
Passo 2: Configuro il backup

- Avvio il programma e seleziono la voce «New Task»



Passo 3: Scelgo file e cartelle

- Seleziono i file e le cartelle di cui effettuare il backup e la destinazione (es. hard disk esterno)



Passo 4: Scelgo lo scheduling

- Scelgo ogni quanto effettuare il backup (giornaliero, settimanale, mensile, annuale, manuale)

New task

General
Files
Schedule
Archive
Exclusions
Events
Advanced

Schedule type

Daily
Once
Daily
Weekly
Monthly
Yearly
Timer
Manually

Tuesday
 Thursday
 Friday
 Saturday
 Sunday

Date/Time

Date: 14/03/2012

Time: 16:26:45

Days of the month: 1

Month: January

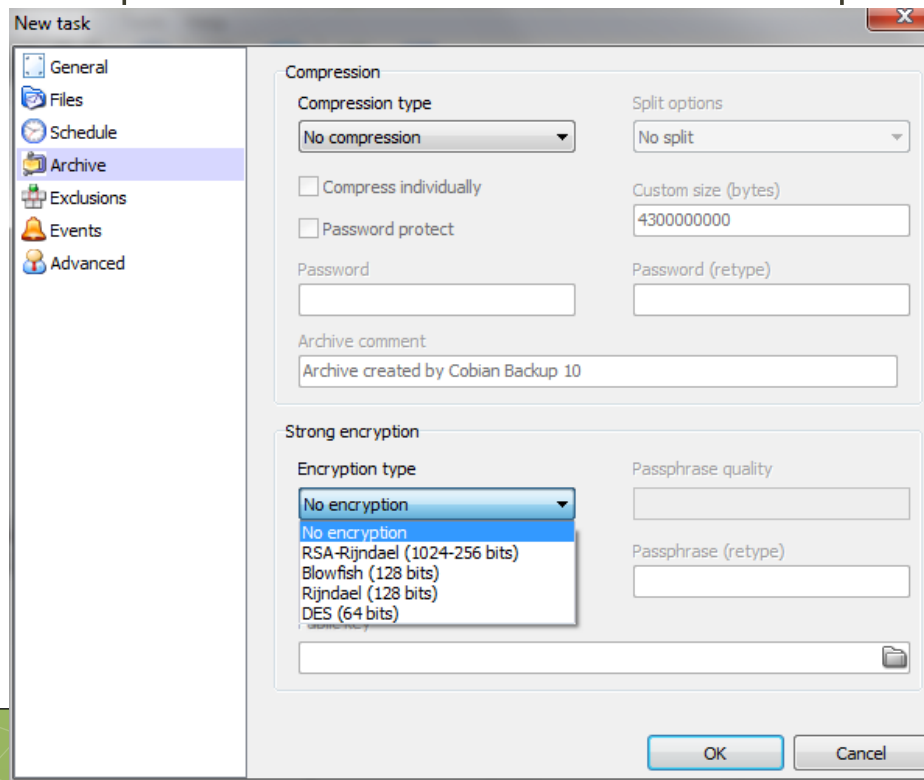
Timer (minutes): 180

From: 00:00:00 To: 23:59:59

OK Cancel

Passo 5: Scelgo lo cifratura

- Cifrare l'hard disk e poi avere un backup in chiaro non è molto intelligente
- Conviene quindi cifrare anche il backup



E se utilizzo Mac?

- Cifratura:
 - TrueCrypt
 - FileVault (integrato in Mac OS X)
- Backup
 - iBackup
 - TimeMachine (integrato in Mac OS X)
- Wiping
 - Permanent Eraser for Mac
 - Disk Utility (integrato in Mac OS X)

Le 7 regole d'oro per gli Smart Phone

- Non perdere il telefono...
- Limitare la conservazione di dati sensibili
- Impostare un **passcode di accesso complesso** (non i semplici 4 numeri...)
- Attivare le **procedure di cancellazione sicura dopo un certo numero di tentativi di inserimento di passcode errato**
- **Aggiornare il sistema operativo**
- **Disattivare bluetooth e wifi** quando non necessari
- **Attenzione alle applicazioni** che si installano

DFA (Digital Forensics Alumni)

- DFA è un'associazione nata nel **dicembre 2009**
- Idea di alcuni corsisti della prima e seconda edizione del **Corso di Perfezionamento in Computer Forensics e Investigazioni Digitali** presso l'Università degli Studi di Milano
- Obiettivo è la creazione di un **network tra gli ex alunni del corso e offrire strumenti per la collaborazione e il confronto tra le figure con una formazione tecnica** (periti e consulenti) e quelle con **formazione giuridica** (giudici, pubblici ministeri, avvocati, P.G.)

DFA (Digital Forensics Alumni)

- **Newsletter mensile** con aggiornamenti tecnici e legali in materia di Digital Forensics
- Per iscriversi
 - Visitare il nostro sito web www.perfezionisti.it oppure
 - Inviare una mail a info@perfezionisti.it

DFA (Digital Forensics Alumni)



Digital Forensics Alumni

Via Spallanzani, 16

20129 Milano

Fax.: +39 178 6071697

www.perfezionisti.it

info@perfezionisti.it



Mattia Epifani

Mail: mattia.epifani@digital-forensics.it

Web: <http://www.digital-forensics.it> - <http://blog.digital-forensics.it>

Linkedin: <http://www.linkedin.com/in/mattiaepifani>