Piccola guida all'uso di TrueCrypt

Alle volte l'uso di nuovi programmi risulta un po' ostico perché la documentazione può risultare essere disponibile solo in inglese, perché il programma è abbastanza complesso, perché si ha timore di combinare il solito disastro oppure per la somma di una o più delle precedenti condizioni.

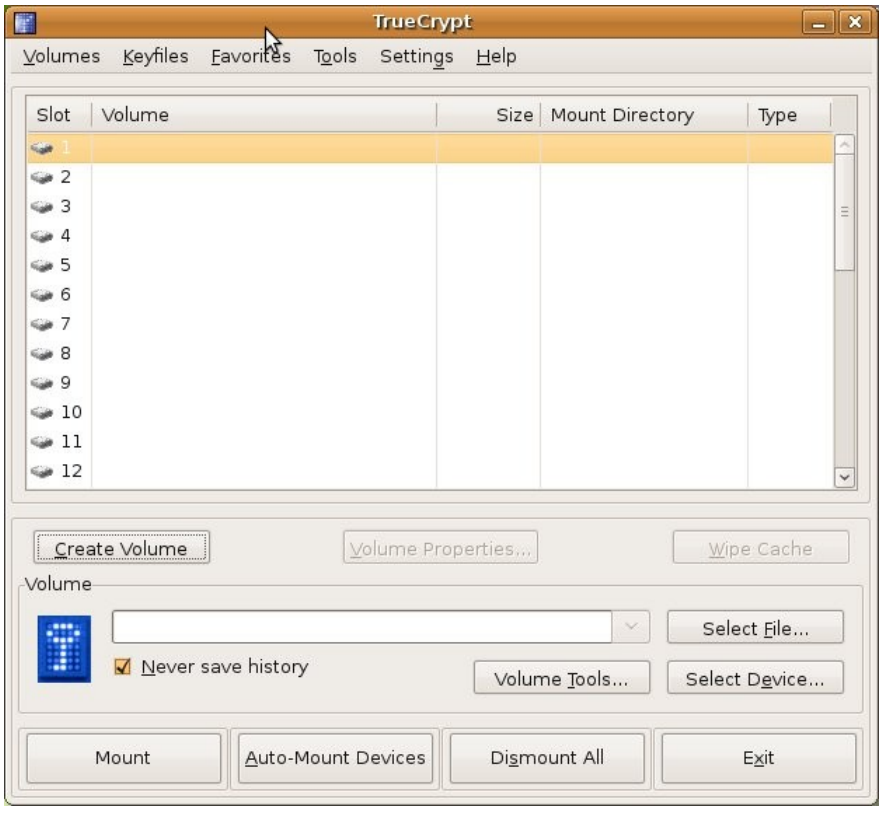
TrueCrypt è uno di questi applicativi: data l'importanza del compito che svolge e data la facilità con cui è possibile combinare il classico disastro (TrueCrypt può formattare anche intere partizioni), i nuovi utenti possono sentirsi un po' disorientati di fronte alla sua interfaccia.

Ho quindi pensato di scrivere una piccola guida per mostrare l'utilizzo delle funzioni base del programma: creeremo insieme un file contenitore cifrato che memorizzeremo su una chiavetta USB in modo da poter trasportare in tutta sicurezza i nostri dati.

La guida è stata scritta usando la versione Linux di TrueCrypt ma la si può adattare tranquillamente anche alla versione Windows dato che l'interfaccia del programma è identica (con la sola differenza della traduzione in italiano, che la versione per Linux ancora non supporta).

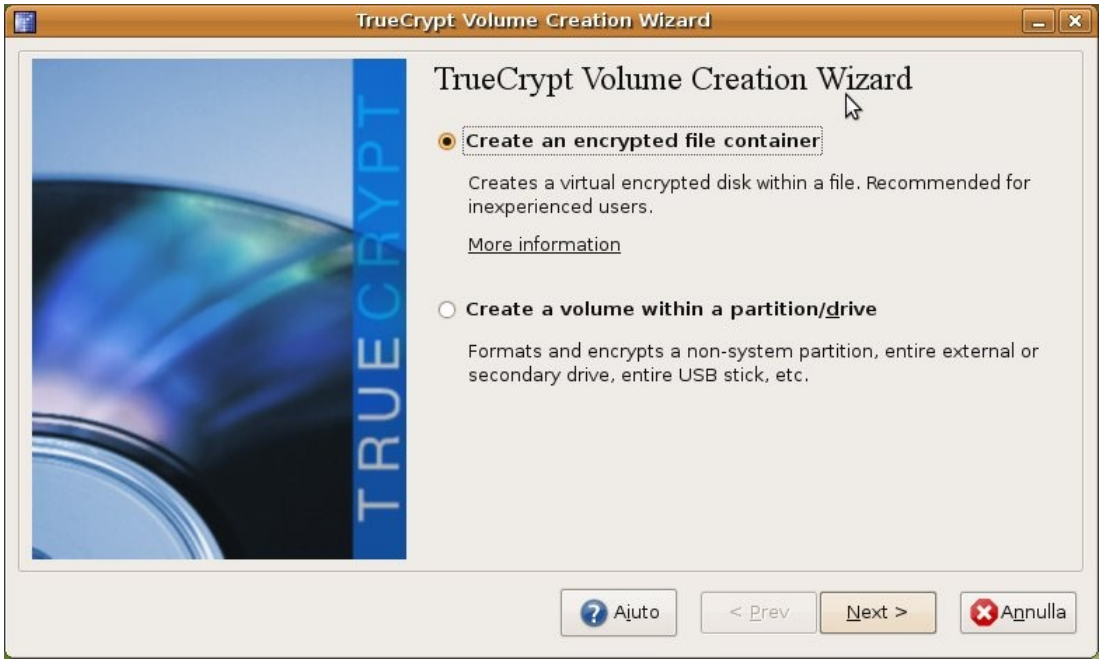
Per prima cosa è indispensabile installare il programma: la via più semplice è quella di utilizzare il gestore di pacchetti della propria distribuzione ma potrebbe capitare di ritrovarsi fra le mani una versione datata di TrueCrypt per cui il mio consiglio è quello di fare un salto sul sito ufficiale e prelevare la versione più recente disponibile ed installarla (qui non affronterò il problema: darò per scontato che si sappia come fare).

Una volta fatto questo, non resta che avviare il programma:



TrueCrypt appena avviato

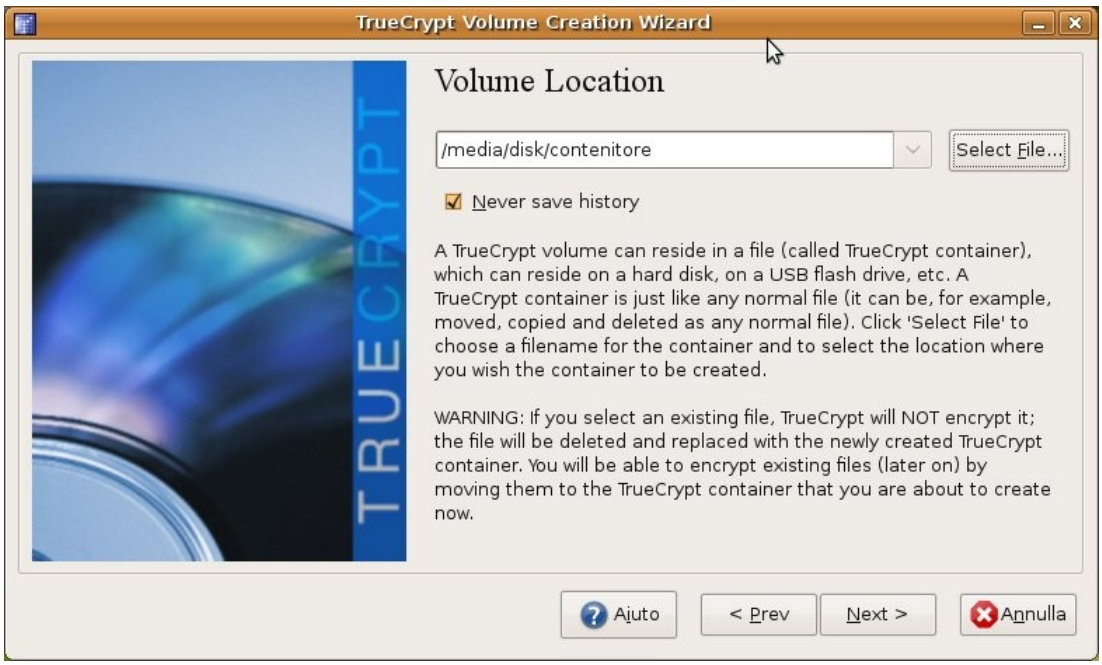
Adesso clicchiamo sul pulsante "***Create volume***". Si aprirà la finestra per la creazione di un nuovo volume cifrato. Per i nostri scopi scegliamo un **file contenitore cifrato**, così da poterlo copiare da e su una chiavetta USB senza problemi:



Scelta del tipo di volume

La scelta successiva è sul tipo di volume che vogliamo creare, se normale o nascosto. Spendiamo due parole su questo passaggio: TrueCrypt permette di creare anche un contenitore cifrato nascosto all'interno di un altro contenitore cifrato. Questo significa che l'accesso ai 2 file necessita di 2 password distinte e che il secondo contenitore non appare neanche se l'accesso al primo è avvenuto correttamente. Poniamo il caso che voi siate delle spie stile 007 e che stiate trasportando documenti segretissimi! Se, nella malaugurata ipotesi, foste catturati dalla polizia di uno Stato nemico e foste posti dinanzi all'ipotesi di essere torturati, potreste rivelare la password del volume visibile, onde far vedere ai nemici la vostra buona volontà: essi non troverebbero, però altro che dati insignificanti, e non sospetterebbero minimamente che il volume contiene in realtà un altro volume cifrato nascosto, che verrebbe alla luce solo in caso voi rivelereste la seconda password.

Detto questo, partiamo dal presupposto che non siate delle spie (non lo siete, vero?) e che il livello di sicurezza da voi ricercato è raggiunto con la creazione di un semplice volume cifrato (d'altronde, si tratta solo di non permettere ad altri di recuperare i vostri dati in caso smarriate la vostra chiavetta USB). Quindi, selezioniamo la prima voce e proseguiamo. Adesso dobbiamo scegliere il file contenitore: il mio consiglio è quello di crearlo sul disco rigido e poi ricopiarlo sulla chiavetta USB, onde evitare un'attesa più lunga durante la sua creazione. Se però la vostra chiavetta è abbastanza veloce (è del tipo USB 2.0), potete anche crearlo direttamente su di essa:

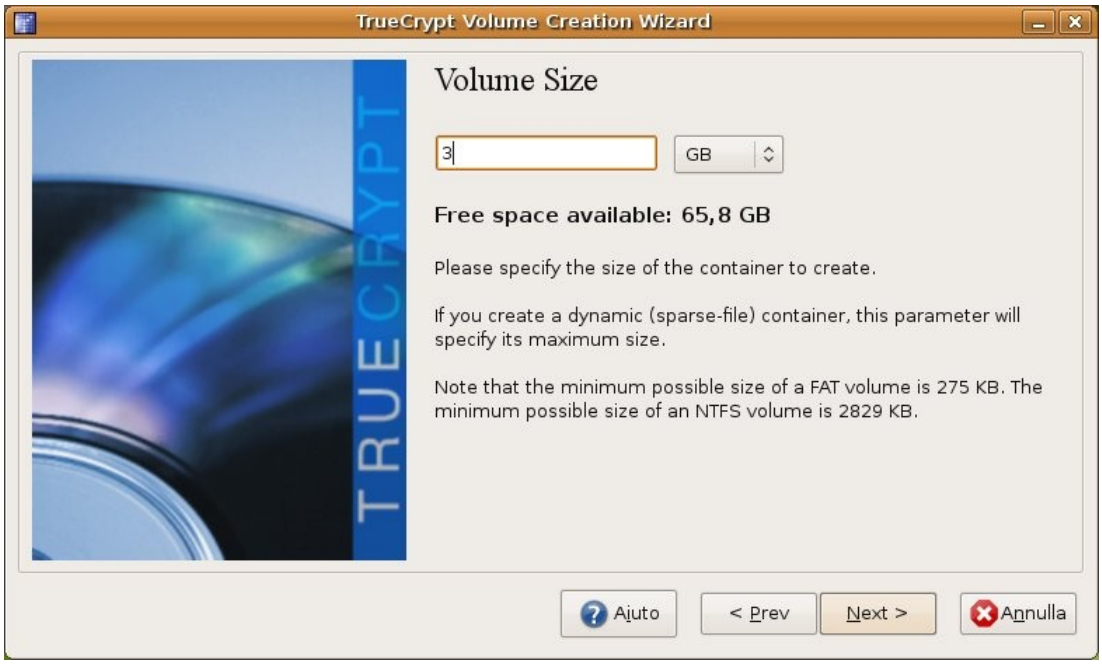


Scelta del file contenitore cifrato

Scegliamo adesso gli algoritmi crittografici. TrueCrypt 6.1 mette a disposizione 3 algoritmi crittografici a blocchi: **AES**, **Serpent** e **Twofish**, più alcune combinazioni di 2 o 3 di essi in cascata. Personalmente consiglio di scegliere fra gli algoritmi singoli ed evitare le combinazioni a cascata in quanto queste appesantiscono i calcoli necessari alla gestione dei dati cifrati senza aggiungere (mio modesto parere) nulla in più in quanto a sicurezza. Questo perché un buon algoritmo crittografico deve avere fra le sue proprietà la *confusione* e la *diffusione*: la prima serve a distruggere ogni relazione fra la chiave ed il testo cifrato; la seconda serve a distribuire le correlazioni statistiche del testo in chiaro lungo tutto il testo cifrato. Se l'algoritmo è sicuro, uno o due passaggi di esso non devono e non possono aggiungere nulla alla sicurezza del testo cifrato finale. Detto questo, la scelta è personale. Posso solo dire che l'AES è stato selezionato come nuovo standard crittografico dal governo americano e quindi è una scelta abbastanza sicura e testata. Il Serpent è arrivato secondo al processo di standardizzazione dell'AES: non è stato scelto non perché non fosse abbastanza sicuro (forse la sua struttura è più robusta di quella dello stesso AES) quanto perché è risultato più lento del suo rivale. Il Twofish, arrivato terzo al suddetto processo, è stato scritto da Bruce Schneier e Niels Ferguson, due nomi che in campo crittografico sono una garanzia: risulta un buon compromesso fra gli altri due. Io scelgo in genere l'AES perché è, fra i 3, l'algoritmo più studiato a livello internazionale.

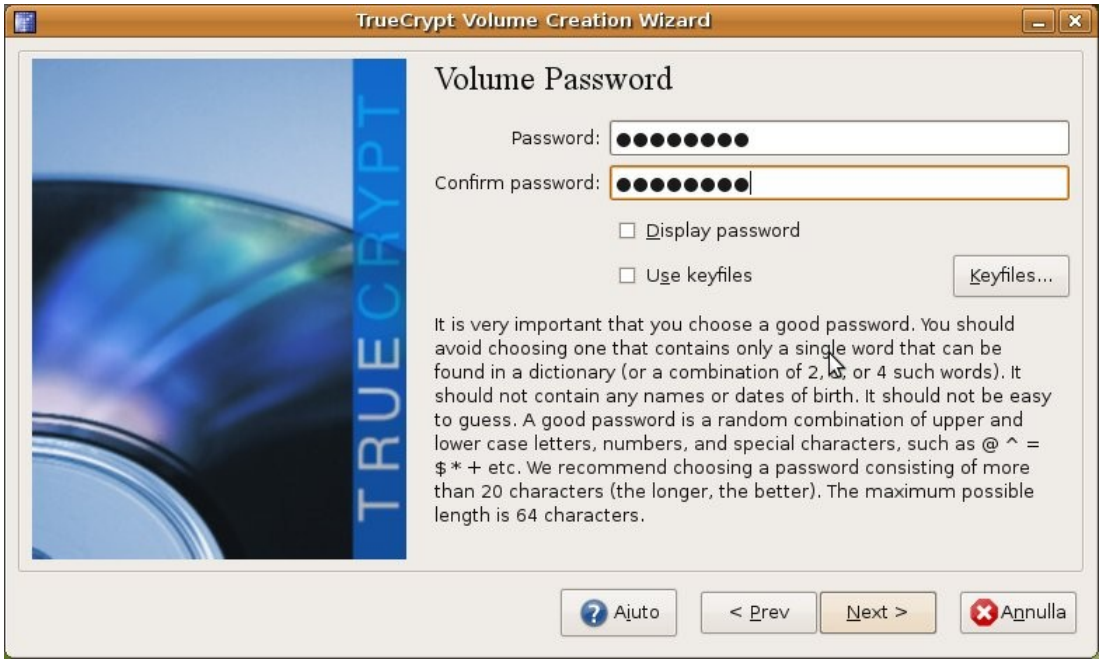
Non ci resta che scegliere, adesso, la funzione crittografica di hash. Anche qui ci sono 3 scelte: **RIPEMD-160**, **SHA-512** e **WHIRLPOOL**. Il primo è un algoritmo di provenienza europea sviluppato quale alternativa ai più noti algoritmi di origini transoceaniche quali MD5; l'SHA-512 è un membro dell'omonima famiglia di algoritmi di hash sviluppati dalla National Security Agency (NSA); infine, uno degli sviluppatori del WHIRLPOOL, Vincent Rijmen, è uno dei disegnatori dell'AES, per cui anche qui siamo di fronte, come nel caso del Twofish, a nobili origini. Dei 3, il RIPEMD-160 è l'unico a presentare un hash lungo solo 160 bit contro i 512 bit degli altri due: questo è il motivo principale per cui tendo a non consigliarlo. Tra l'SHA-512 ed il WHIRLPOOL io mi sento di suggerire l'utilizzo del primo perché anche qui siamo di fronte ad uno standard sviluppato da un ufficio governativo americano, l'NSA, di cui in genere ci si può fidare e perché, anche in questo caso, è un algoritmo molto studiato.

Questo appena passato era il punto decisionale più difficile da affrontare. Adesso le scelte rimaste sono abbastanza semplici, come ad esempio quella che riguarda la dimensione del contenitore cifrato:



Scelta della dimensione del file contenitore cifrato

Ricordatevi che se la chiavetta deve essere utilizzata anche su sistemi Windows ed è, perciò, formattata con il filesystem FAT32, la dimensione del file non può essere più grande di 4 GB. In genere, poi, è buona norma non utilizzare tutto lo spazio disponibile in quanto bisogna riservarne un po' per la memorizzazione degli eseguibili di TrueCrypt. Adesso è la volta di scegliere una password:



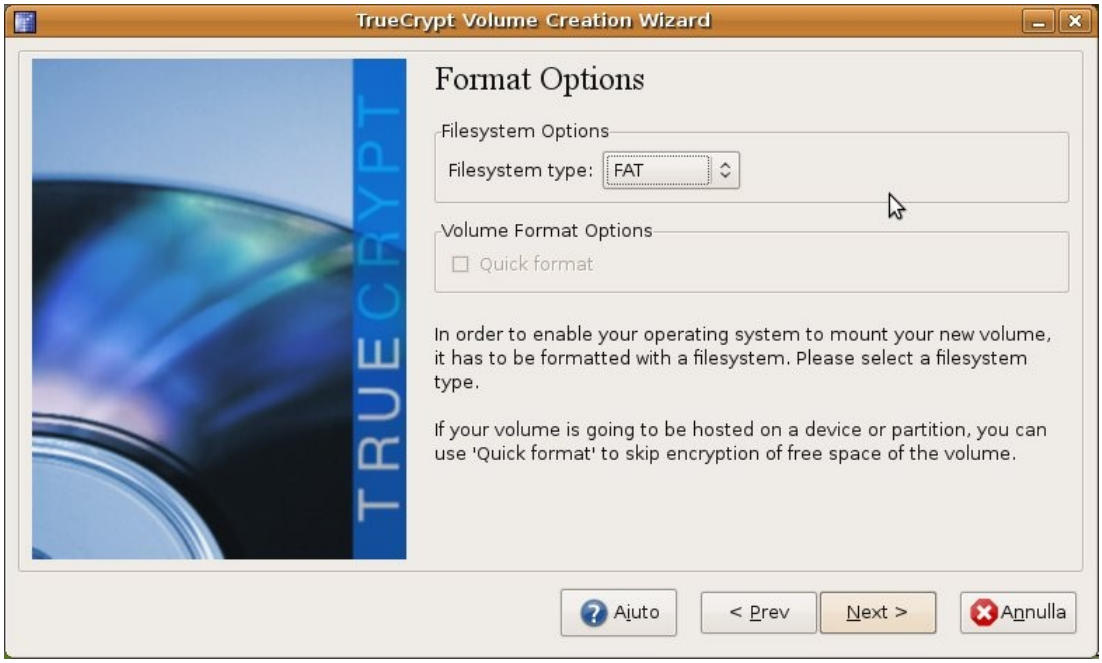
Scelta della password di cifratura

TrueCrypt suggerisce di utilizzare una password di almeno 20 caratteri alfanumerici, comprese lettere minuscole e maiuscole, numeri e segni di punteggiatura. Onestamente diventa però molto difficile tenere a mente una tale password per cui le scelte sono 2: o optate per una password più corta ma più facilmente ricordabile oppure scegliete di utilizzare un **keyfile**, vale a dire un file contenente la stringa di caratteri da usare come password. Questa seconda opzione pone un altro problema di sicurezza: mantenere tale file sicuro e sempre con voi, quindi su un'altra chiavetta o altro dispositivo di memorizzazione. Secondo me, a meno che non si debbano proteggere dati governativi segretissimi, l'uso di una password composta da una decina di caratteri è più che sufficiente: serviranno senz'altro diversi mesi prima di poterla violare, un tempo più che sufficiente per permettervi di cambiare i codici di accesso al vostro conto corrente...

A seconda della dimensione del file contenitore da voi scelto, TrueCrypt potrebbe chiedervi se intendete memorizzare in tale contenitore file più o meno grandi di 4 GB (il limite della FAT32):

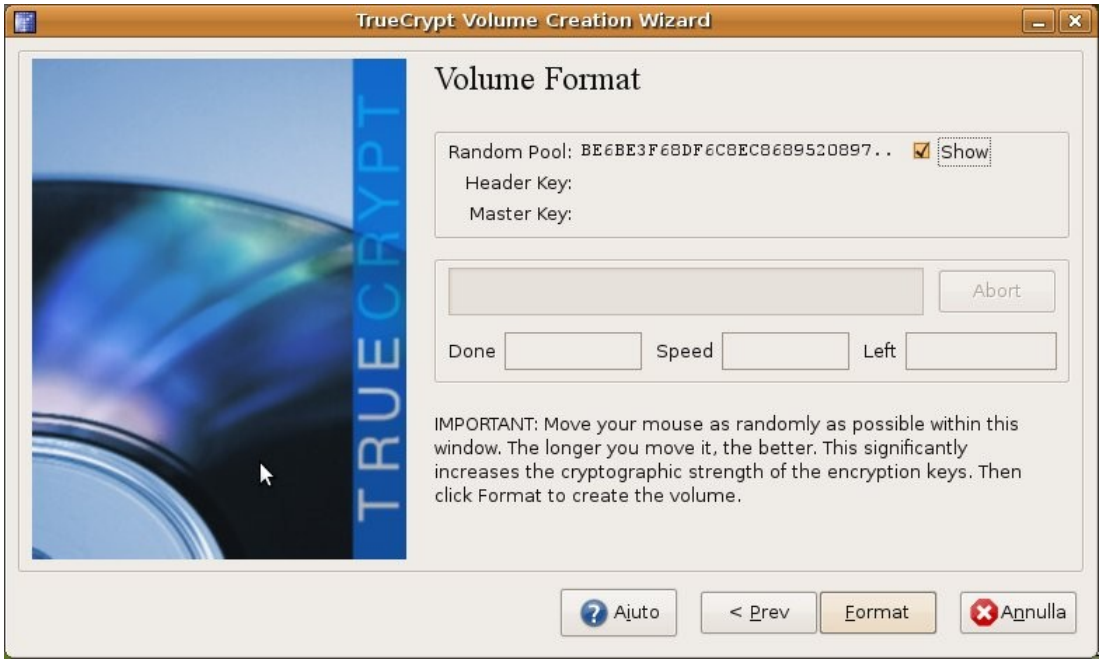
Si devono memorizzare file più grandi di 4 GB?

La scelta dipende ovviamente dalle necessità personali. Adesso è chiesto il filesystem da utilizzare per formattare il contenitore. Se questo dovrà essere letto da più sistemi, il consiglio è quello di usare ovviamente il tipo **FAT**, universalmente riconosciuto:



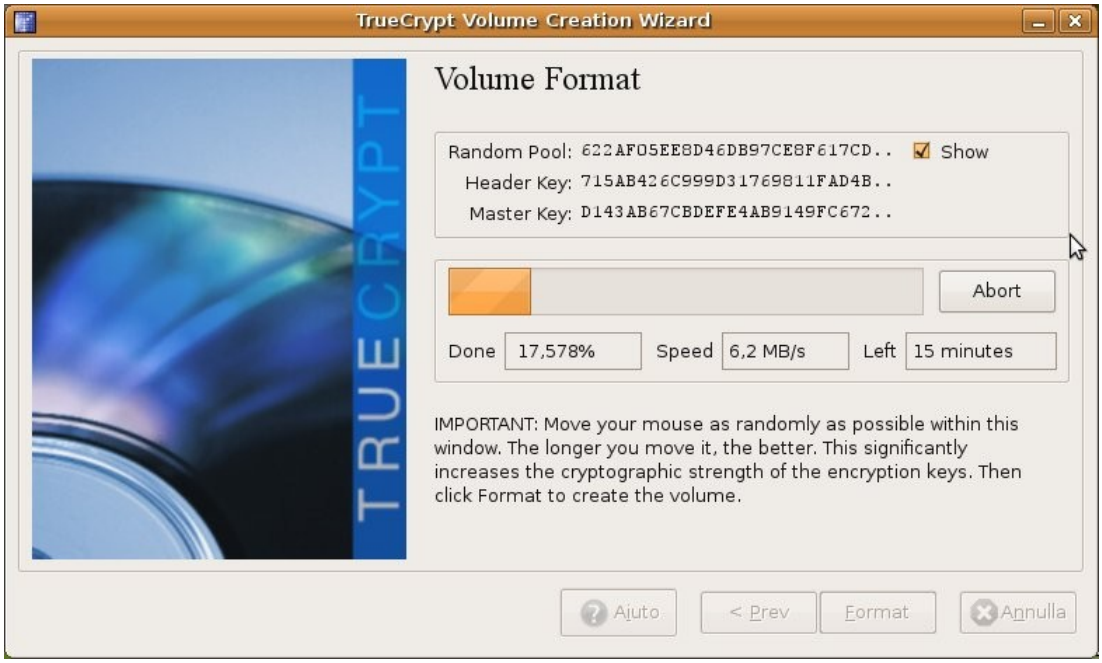
Scelta del filesystem

Siamo ad un passo dalla formattazione. TrueCrypt richiede ora che l'utente muova il puntatore del mouse sulla finestra del programma il più casualmente ed il più a lungo possibile onde permettere la collezione di una notevole quantità di entropia, necessaria a generare *keystream* (chiavi di cifratura derivate dalla password utente) molto robuste:



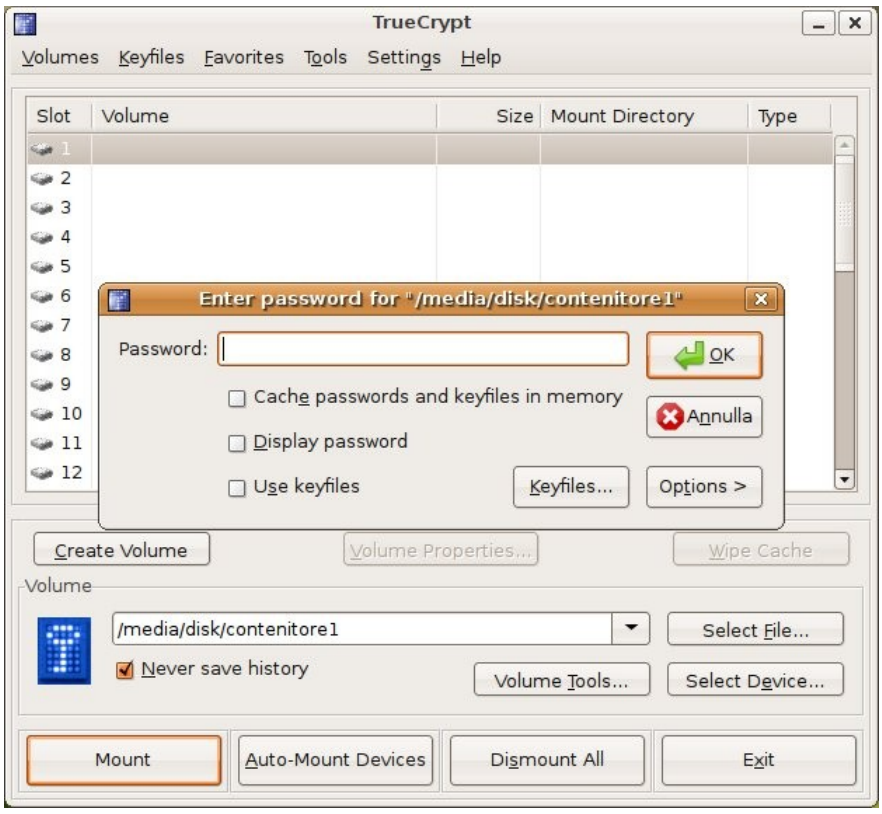
Collezione dell'entropia

Quando giudicheremo che l'entropia collezionata sarà sufficiente, potremo cliccare sul pulsante "***Format"*** per iniziare la formattazione del contenitore:



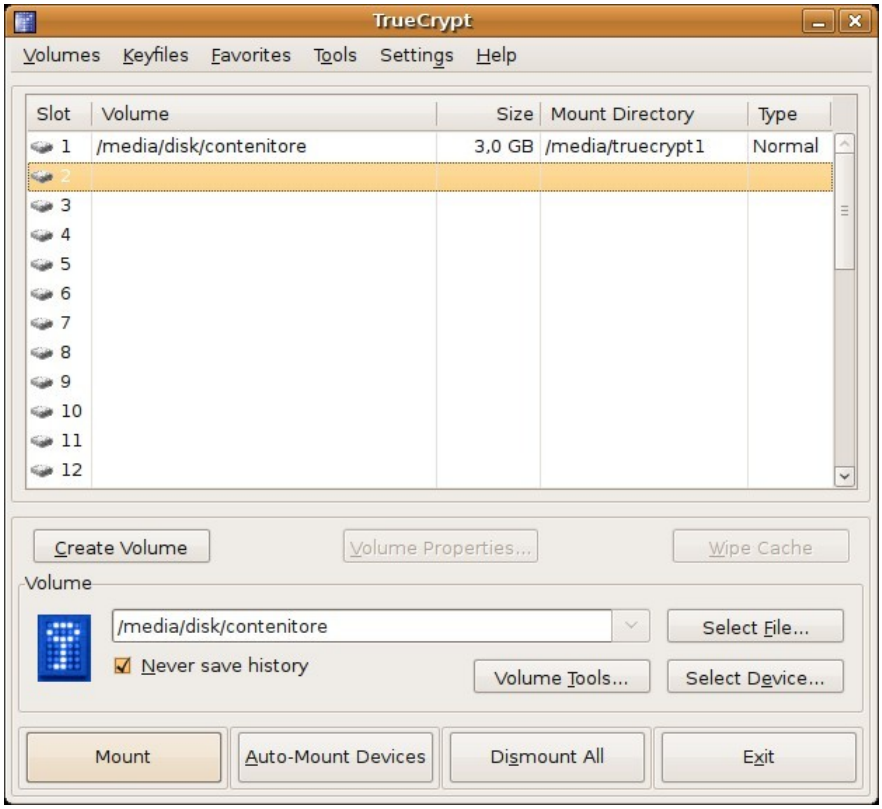
Formattazione del file contenitore cifrato

Terminata la formattazione, usciamo dalla creazione guidata e torniamo all'interfaccia di TrueCrypt per montare il file contenitore appena creato ("montare" significa far sì che il sistema operativo crei un collegamento logico fra il file residente sul disco ed il filesystem del sistema in modo che sia possibile accedervi come ad un qualsiasi altro disco). Per far ciò non resta che selezionare uno slot libero nella griglia di TrueCrypt, poi selezionare il file contenitore (se già non lo ha fatto in automatico il programma) ed infine cliccare sul pulsante ***Mount***. Verrà ora chiesta la password con cui abbiamo protetto il contenitore:



Montaggio del file contenitore cifrato

Su alcuni sistemi (ad esempio su Linux) verrà anche richiesta la password di amministratore per poter terminare la procedura di montaggio (senza di essa, non è possibile inserire il punto di montaggio del file contenitore cifrato nella tabella dei punti di montaggio del sistema). Fatto questo, nello slot selezionato apparirà il percorso che permetterà di accedere al file contenitore cifrato come fosse un qualsiasi altro dispositivo di memorizzazione del sistema: sarà TrueCrypt che effettuerà le operazioni di cifratura e decifratura in tempo reale ed "al volo" quando voi aprirete un file o ne salverete uno.



Visualizzazione del punto di montaggio

Come avete potuto vedere la creazione di un file contenitore cifrato è un'operazione tutt'altro che difficile: bastano pochi passaggi ed il vostro file cifrato è pronto a ricevere e proteggere i vostri dati. Ovviamente sarà possibile utilizzare tale contenitore sia su dispositivi fissi (dischi rigidi) che mobili (chiavette USB): basterà copiare il file contenitore sul supporto adeguato. Potete anche accedere al vostro file contenitore da più sistemi operativi: al riguardo si veda il mio precedente articolo TrueCrypt in 6.1 Traveler Mode anche su Linux. Che vi spiega come fare per poter creare una chiavetta USB con un contenitore cifrato apribile sia da Windows che da Linux senza la necessità che TrueCrypt sia installato sul computer.