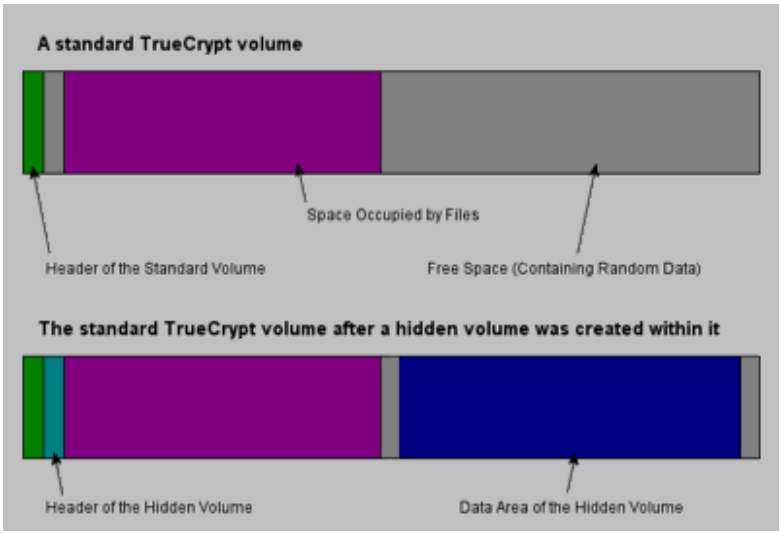
Manuale TrueCrypt



Versione 1.0.0 del 18/11/2013

TrueCrypt: installazione e considerazioni

In parte tratto dalla User Guide di TrueCrypt

TrueCrypt è un software per la creazione e il mantenimento di un volume criptato on-the-fly. Crittografia on-the-fly significa che i dati vengono automaticamente criptati giusto prima di venire salvati e viceversa decifrati solo dopo la lettura dal disco, senza l'intervento dell'utente. Non ci sono dati memorizzati in un volume crittografato che possano essere letti (decriptati) senza utilizzare la giusta password / keyfile(s) o chiavi di crittografia. Tutto il filesystem é criptato (per esempio, i nomi dei file, delle cartelle, dei contenuti di ogni file, spazio libero, meta dati, ecc.)

I file possono essere copiati da e per un volume TrueCrypt montato proprio come vengono copiati da e per qualsiasi disco normale (per esempio con semplici operazioni di drag-and-drop). I file vengono automaticamente decifrati al volo (in memoria RAM) mentre vengono letti o copiati da un volume TrueCrypt criptato. Allo stesso modo i file che vengono scritti o copiati nel volume TrueCrypt vengono automaticamente codificati al volo (giusto prima di essere scritti sul disco) nella RAM. Si noti che questo non significa che tutti i files che devono essere cifrati o decifrati debbano essere memorizzati in RAM prima di poter essere cifrati o decifrati. Non é necessaria memoria extra per TrueCrypt. Vediamo un esempio di come avviene tutto ciò.
Supponiamo che ci sia un file video Avi memorizzato in un volume TrueCrypt (quindi il file video é completamente criptato). L' utente fornisce la password corretta (e/o i keyfile(s)) e monta (apre) il volume TrueCrypt. Quando l'utente fa doppio-clic sull'icona del file video, il sistema operativo avvia l'applicazione associata al tipo di file, in genere un lettore multimediale. Il lettore multimediale inizia quindi il caricamento di una piccola porzione iniziale del file video, dal volume TrueCrypt cifrato alla RAM, al fine di riprodurlo. Mentre viene caricata quella parte, TrueCrypt la decripta automaticamente (in RAM) . La porzione decriptata del video (memorizzata in RAM) viene poi riprodotta dal lettore multimediale. Mentre viene riprodotta questa parte, il lettore multimediale inizia caricare un'altra piccola porzione del file video dal volume TrueCrypt cifrato alla RAM e il processo si ripete. Questo processo é chiamato on-the-fly encryption/decryption e funziona per tutti i tipi di file (non solo per i file video).
Si noti che TrueCrypt non memorizza mai i dati decriptati nel disco, li memorizza solo temporaneamente nella RAM. Anche quando il volume é montato, i dati memorizzati nel volume sono ancora crittografati. Quando si riavvia il S.O. o si spegne il computer, il volume verrà smontato ed i files memorizzati in esso saranno inaccessibili (perchè criptati). Anche se dovesse improvvisamente mancare l'alimentazione (senza adeguato sistema di continuità), i file memorizzati nel volume sarebbero inaccessibili e criptati. Per renderli fruibili é necessario montare il volume fornendo la password corretta e/o i file di chiavi).

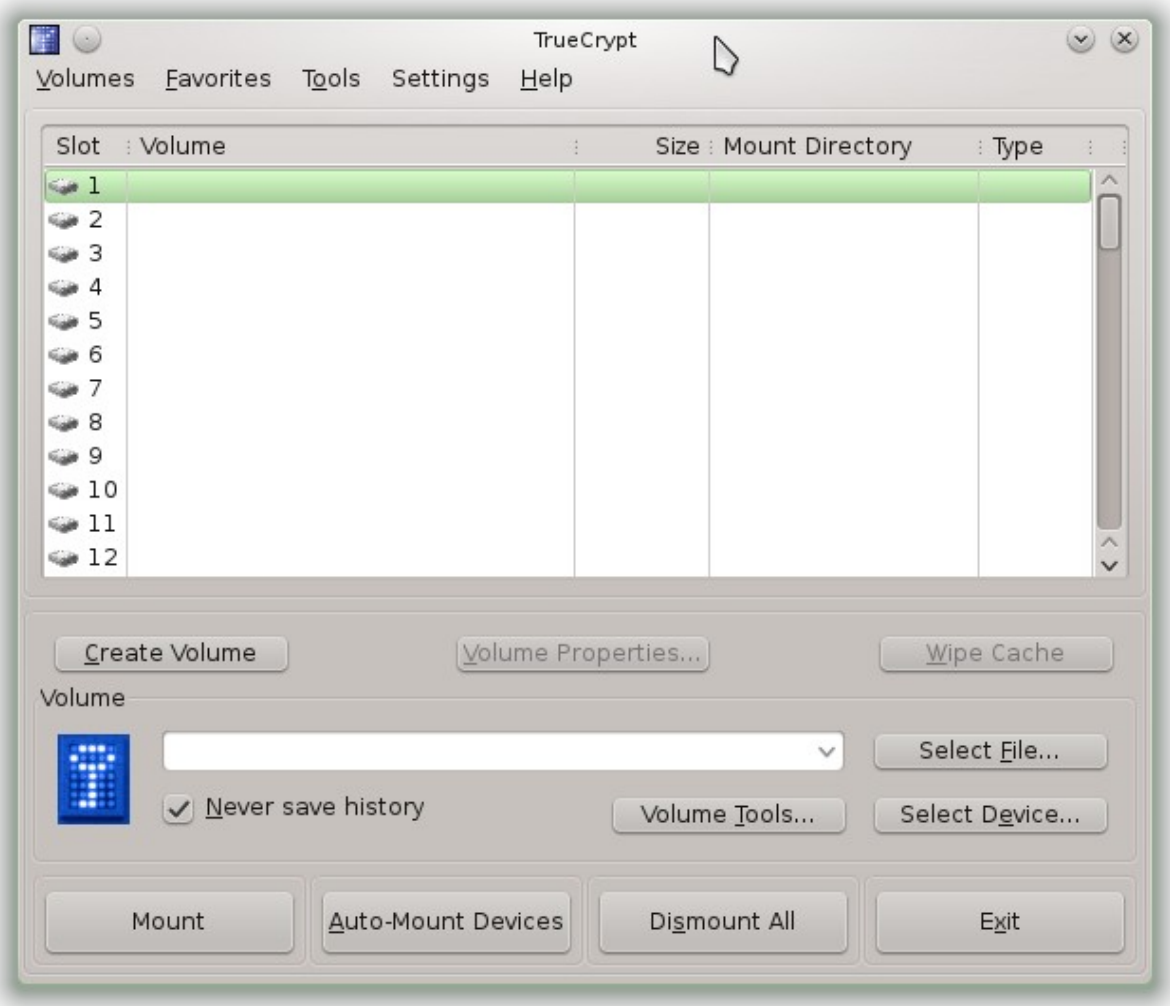
Come creare e utilizzare un contenitore TrueCrypt

Questo capitolo contiene le istruzioni passo-passo su come creare, montare e utilizzare un volume TrueCrypt . Si consiglia vivamente di leggere anche le altre sezioni di questo manuale , in quanto contengono importanti informazioni
E' consigliabile eseguire queste operazioni con l'utente che dovrà in seguito fruire del servizio di volume crittografato, per evitare alcuni problemi di proprietà dei files e delle directories che potrebbero sorgere, e di cui daremo conto più avanti.

Passo 1 - Download ed installazione

Se non lo si é ancora fatto , scaricare ed installare TrueCrypt.
Lo si può scaricare dal link: http://www.truecrypt.org/downloads scegliendo la release appropriata.
E' una buona idea verificare la firma PGP del file scaricato, scaricando anche quella e verificandola secondo le normali procedure descritte anche sul sito di download:
http://www.truecrypt.org/docs/digital-signatures#Y1139
Immaginando di aver scaricato il file truecrypt-7.1a-linux-x64.tar.gz esploderlo in una directory dove si abbia spazio per lavorare, con il comando "tar xvzf truecrypt-7.1a-linux-x64.tar.gz"
Ne risulterà un unico file: truecrypt-7.1a-setup-x64 che rappresenta l'installer. Mandarlo in esecuzione con il comando ./truecrypt-7.1a-setup-x64 L'installazione é rapidissima. Finita l'installazione il file truecrypt-7.1a-setup-x64 potrà anche essere cancellato. Poi bisognerà vedere a seconda della release di Linux in uso che riferimenti saranno stati installati per il suo lancio. Nella OpenSUSE 12.3 lo si trova sotto "Utilities --> More Programs". Eseguirlo.

Passo 2 - Inizio esecuzione



Viene visualizzata la finestra principale di TrueCrypt. Fare clic su Create Volume.

Passo 3 - Procedura guidata creazione volume

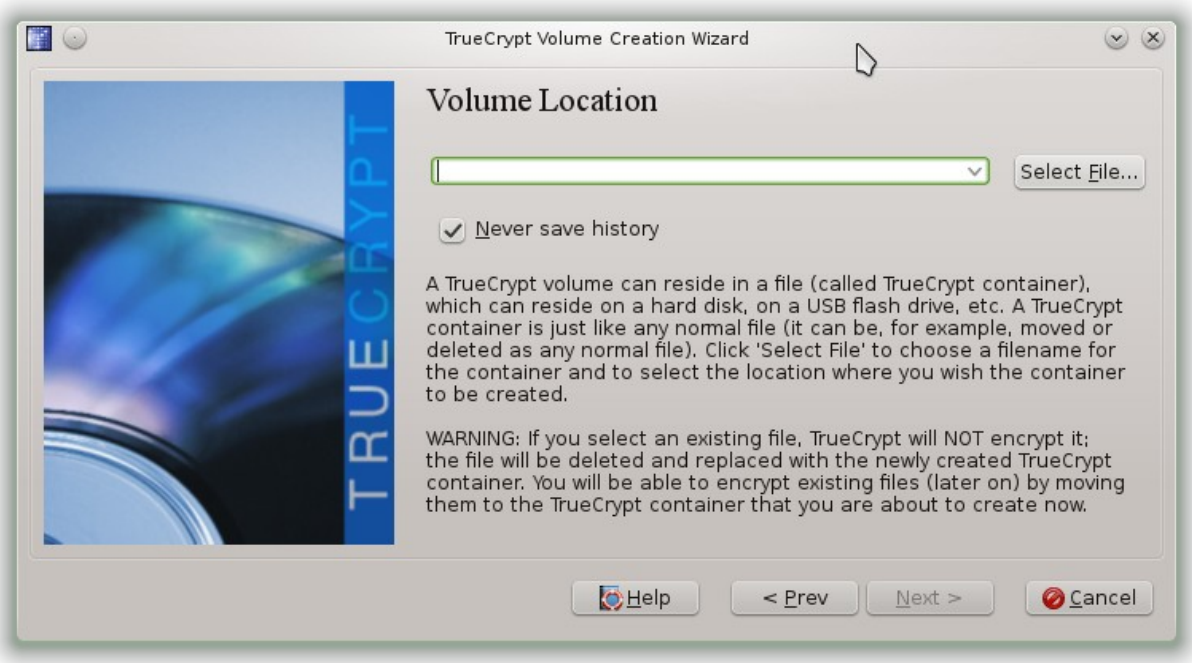
Viene visualizzata la finestra della procedura guidata di creazione del volume TrueCrypt.
In questo passaggio é necessario scegliere dove si desidera che risieda il volume TrueCrypt da creare. Un volume TrueCrypt può risiedere a scelta in un file, che viene chiamato anche contenitore, in una partizione o in un'unità disco completa. In questa fase del tutorial sceglieremo la prima opzione e creeremo un volume TrueCrypt all'interno di un file. Le altre opzioni sono similari.
Se state usando TrueCrypt sotto Windows sarà presente una terza scelta, quella di criptare la partizione di sistema o tutto il drive di sistema. Opzioni inerentemente pericolose e complesse per cui si rinvia alla versione originale del manuale, non essendo qui trattate.
Visto che l'opzione è selezionata per impostazione predefinita, si può semplicemente fare clic su Next .

Passo 4 - Scelta del tipo di volume

In questo passaggio é necessario scegliere se creare un volume TrueCrypt standard o nascosto. In questo tutorial sceglieremo la prima opzione e creeremo un volume TrueCrypt standard. Siccome l'opzione é selezionata per impostazione predefinita, si può semplicemente fare clic su Next .

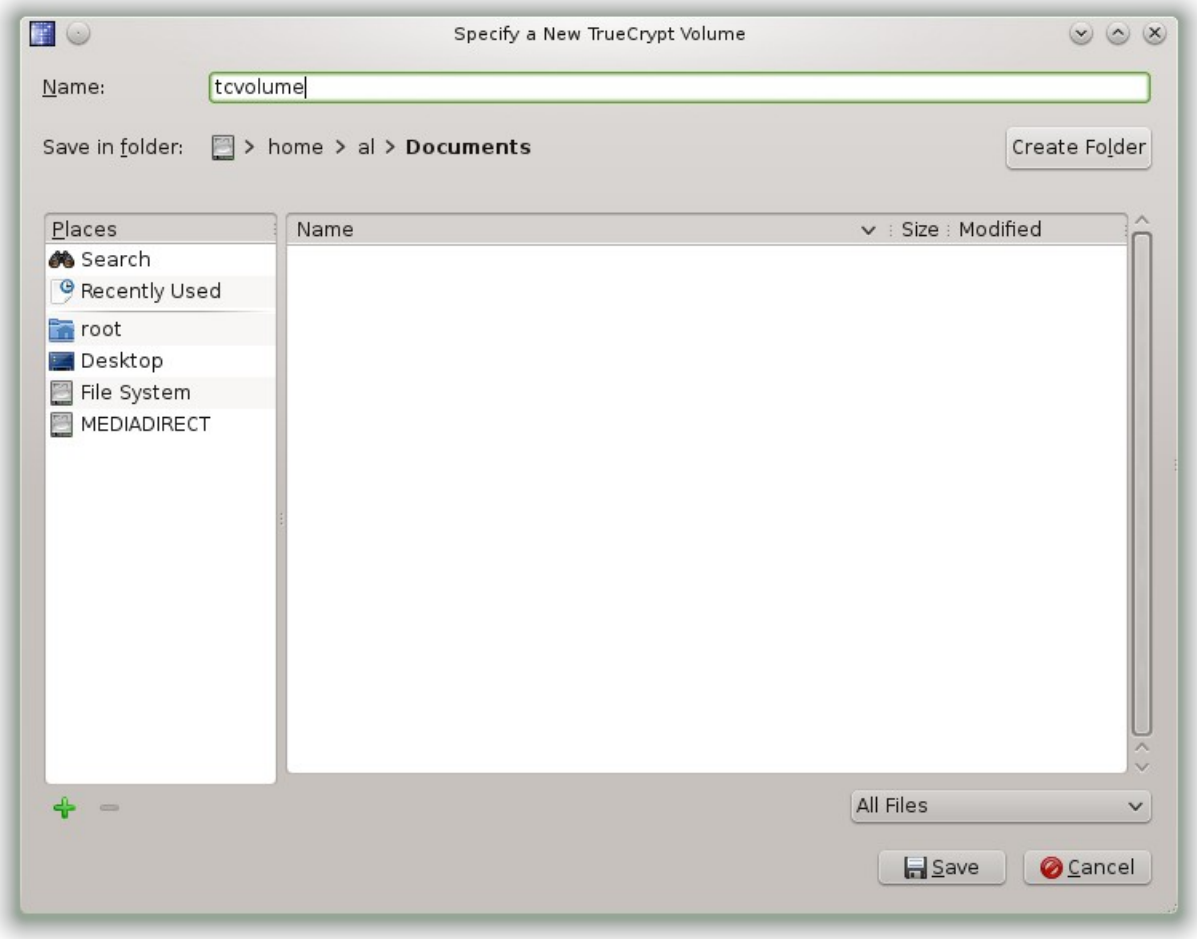
Passo 5 - Collocazione volume

In questo passaggio é necessario specificare dove si desidera che risieda il volume TrueCrypt (Contenitore) da creare . Si noti che un contenitore TrueCrypt é proprio come un normale file. Può essere, ad esempio, spostato o cancellato come un normale file. Ha anche bisogno di un nome di file, che potrete scegliere nella fase successiva .
Fare clic su Select File...



Dovrebbe apparire il selettore di file standard (mentre la finestra della Creazione guidata volume TrueCrypt rimane aperta in background) .

Passo 6 - Finestra di scelta collocazione



In questo tutorial creeremo il nostro volume TrueCrypt nella cartella /home/al/Documents con nome **tcvolume** (come si può vedere nello screenshot sopra). Si può naturalmente scegliere qualsiasi altro nome di file e la posizione che ci piace (per esempio su una chiavetta di memoria USB). Si noti che il file **tcvolume** non esiste ancora, TrueCrypt lo creerà.

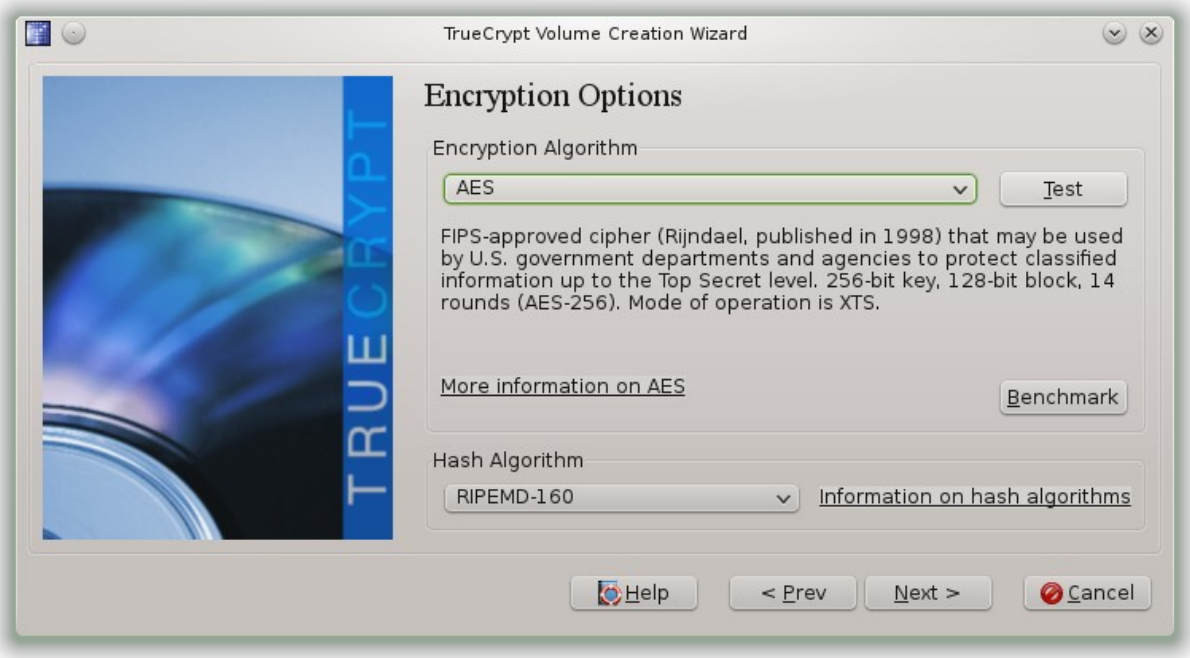
IMPORTANTE: Si noti che TrueCrypt non crittografa i file esistenti (durante la creazione di un contenitore di file TrueCrypt). Se si seleziona un file esistente in questo passaggio, verrà sovrascritto e sostituito con il volume appena creato (in questo modo é chiaro che il file sovrascritto verrà perso, non criptato). Sarete in grado di crittografare i file esistenti in seguito, spostandoli nel volume TrueCrypt che stiamo creando ora.

Selezionare il percorso desiderato (in cui si desidera creare il contenitore) nel selettore di file.
Digitare il nome voluto per il file nella casella Name:
Fare clic su Save.
Dovrebbe scomparire la finestra di selezione del file .

Passo 7 - Conclusione collocazione

Tornati a questa finestra cliccare Next

Passo 8 - Scelta parametri crittografici



In questa finestra potete scegliere i parametri crittografici di da applicare al volume. Siccome quelli predefiniti sono assolutamente ragionevoli potete cliccare su Next
Le alternative sono tutte valide, d'altronde TrueCrypt é un prodotto creato con la sicurezza sempre presente, qualunque algoritmo si scelga. Nel caso di più di un algoritmo in cascata, essendo le chiavi mutuamente indipendenti, otteniamo lo stesso effetto di avere una chiave lunga come la somma delle due o tre utilizzate. La robustezza aumenta a livelli veramente notevoli ma lo si paga in tempo di encryption/decryption, che nel caso di volumi di una certa dimensione può essere veramente fastidioso. Altrettanto sostanzialmente vale per l'agoritmo di hash: RIPEMD-160 é un ottimo algoritmo di hash ragionevolmente veloce, SHA-512 é piu' robusto non fosse altro per l'aumentata dimensione da 160 bit a 512 bit e Whirlpool é l'ultimo grido, lasciatemi dire, probabilmente il meglio che si può ottenere con 512 bit.

Passo 9 - Dimensioni Volume

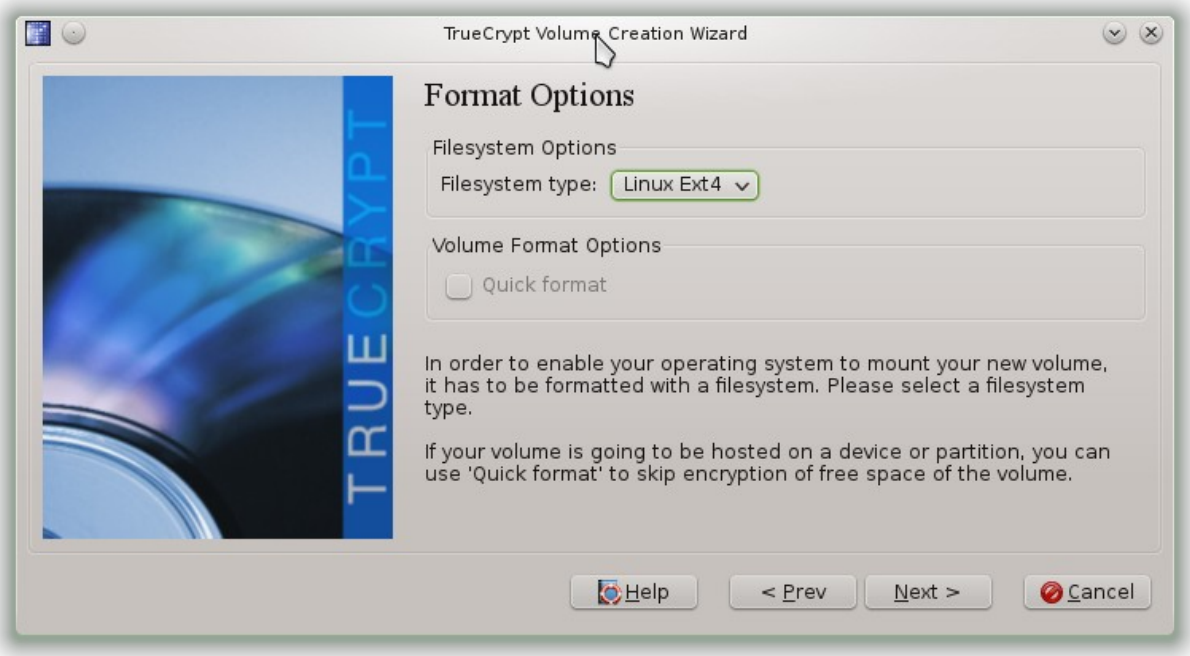
Qui abbiamo scelto di generare un volume di 100 Mbytes. La finestra ci avverte che non é possibile creare volumi di dimensioni inferiori a 292 Kbytes. Al termine fare click su Next

Passo 10 - Pass-phrase di protezione

Qui dovremo inserire la password di protezione del nostro volume. Sicuramente quella in esempio non é una buona password, o meglio pass-phrase, per la sua banalità. La scritta nella finestra recita:

E' importantissimo che scegliate una buona password. Dovreste evitare di sceglierne una costituita da una sola parola che possa essere trovata in un dizionario (o una combinazione di 2, 3 o 4 parole del genere). Non dovrebbe contenere nomi o date di nascita. Non dovrebbe essere facile da immaginare. Una buona password é una combinazione casuale di lettere maiuscole e minuscole, numeri e caratteri speciali come @ ^ = $ * + ecc. Noi raccomandiamo di scegliere una password di oltre i 20 caratteri (più é lunga e meglio é). La massima lunghezza possibile é di 64 caratteri.

Passo 11 - Scelta formattazione



In questa finestra scegliamo il tipo di filesystem che verrà utilizzato per il nostro contenitore. La scritta nella finestra recita:

Per far sì che il vostro sistema operativo sia in grado di montare il vostro nuovo volume, questi deve essere formattato con un filesystem. Scegliete il tipo di filesystem desiderato.

Se il vostro volume é costituito da un disco completo o una partizione, potete usare 'Quick Format' (ovvero Formattazione Veloce) per saltare l'operazione di encryption dello spazio vuoto del volume.

Passo 12 - Scelta tipo di mount

Dal momento che precedentemente abbiamo scelto un filesystem EXT4 che esiste solo sotto Linux, ci viene presentata questa finestra. In essa ci si chiede di scegliere se monteremo il volume su altre piattaforme (es. Windows) o solo Linux. Se scegliamo la prima ipotesi veniamo semplicemente avvertiti che non avendo scelto di formattare con un filesystem di tipo FAT potrebbe essere necessario installare altri drivers o altro software sulle piattaforme non Linux dove andremo a montarlo.

Click su Next.

Passo 13 - Formattazione

Come dice la scritta nella finestra é necessario muovere il mouse in modo casuale all'interno della finestra per "caricare" il generatore di numeri casuali. Più a lungo lo si fa e meglio é nel senso che le chiavi generate saranno veramente impredicibili. Quando si decide di averne abbastanza, fare click su Next ed inizia la formattazione. Se la formattazione termina con un errore del genere: *Failed to set up a loop device: ecc.* vuol dire che il modulo "loop" non é stato caricato automaticamente nel kernel e quindi prima di reiniziare la formattazione aprire una shell e digitare "modprobe loop" oppure "sudo modprobe loop" a seconda della distribuzione in uso. A formattazione terminata comparirà la finestra

Cliccare su OK

Passo 14 - Fine creazione volume

A questo punto abbiamo completato la generazione del nostro volume. Se non ne vogliamo creare altri useremo Exit altrimenti cliccheremo su Next

Creazione di un volume Hidden

Le prime fasi sono identiche a quelle della creazione di un volume **Standard**, fino al **Passo 4**

Passo 4h - Scelta volume hidden

A questo punto sceglieremo invece Hidden TrueCrypt Volume. La scritta recita:

Potrebbe capitare di essere costretti a rivelare la password di accesso ad un volume criptato. Ci sono molte situazioni in cui non potete rifiutarvi di rivelare la password (per esempio in caso di estorsione). L'utilizzo di un cosiddetto hidden volume (volume nascosto) vi permette di risolvere queste situazioni senza rivelare la password del volume (di interesse).

Click su Next

Passo 5h - Collocazione volume

Passo identico al precedente **Passo 5**

Passo 6h - Finestra di scelta collocazione

Passo identico al precedente **Passo 6**

Passo 7h - Conclusione collocazione contenitore

Passo identico al precedente **Passo 7**

Passo 8h - Scelta parametri crittografici volume esterno

Passo identico al precedente **Passo 8**

Passo 9h - Dimensioni volume esterno

In questo passo vi si chiede di stabilire le dimensioni del volume *esterno*, quello che conterrà quello *nascosto* più qualche file per renderlo verosimile, e che dovrà di conseguenza avere dimensioni maggiori di quello nascosto.

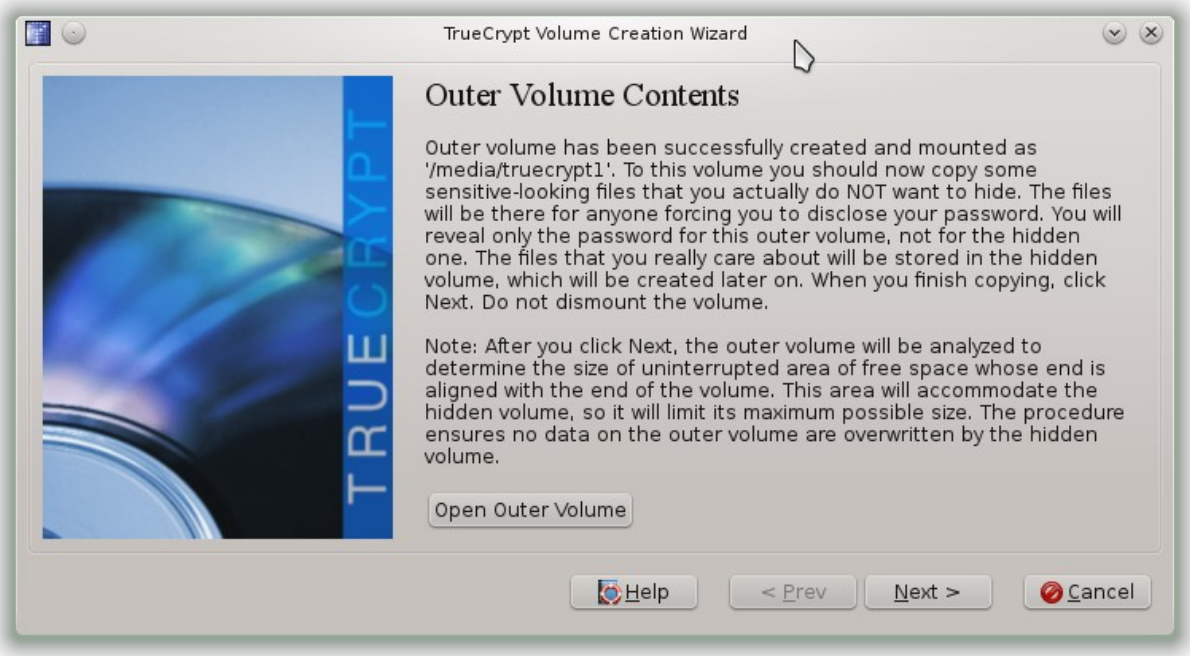
Passo 10h Pass-phrase protezione volume esterno

Questa sarà la password del volume *esterno*, quella che potremmo essere costretti a rivelare. Sceglietela decisamente differente da quella che utilizzerete per lo *hidden volume*

Passo 11h - Formattazione volume esterno

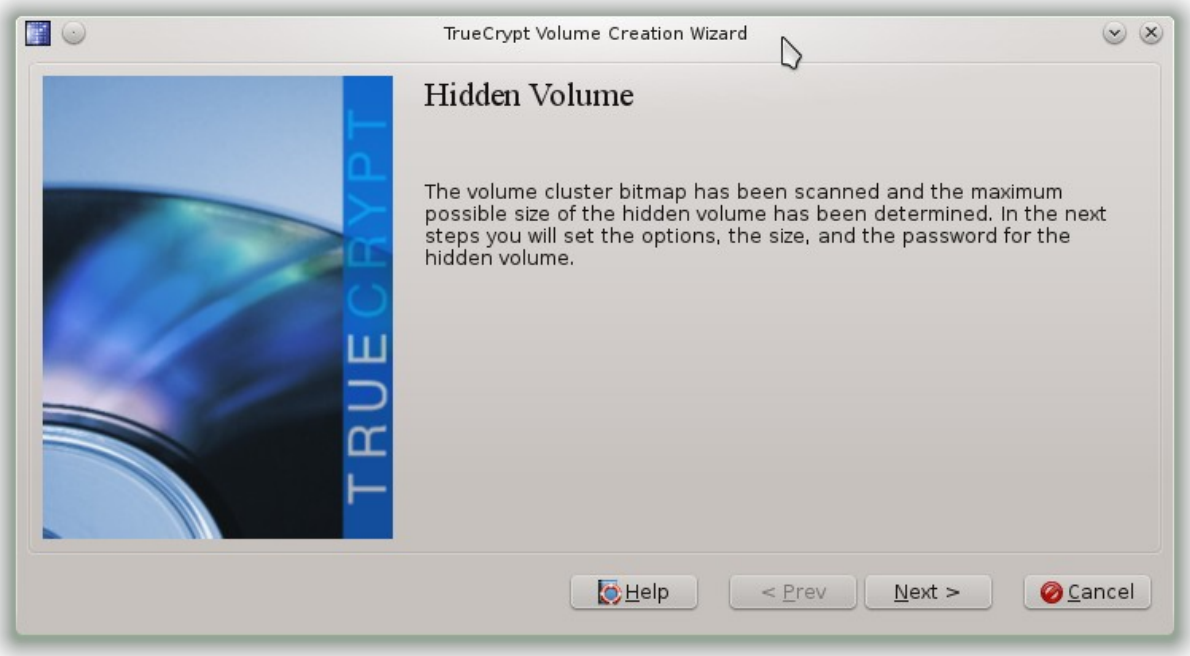
Anche qui muoveremo il mouse in modo casuale per un pò e poi cliccheremo Format

Passo 12h - Volume esterno completato

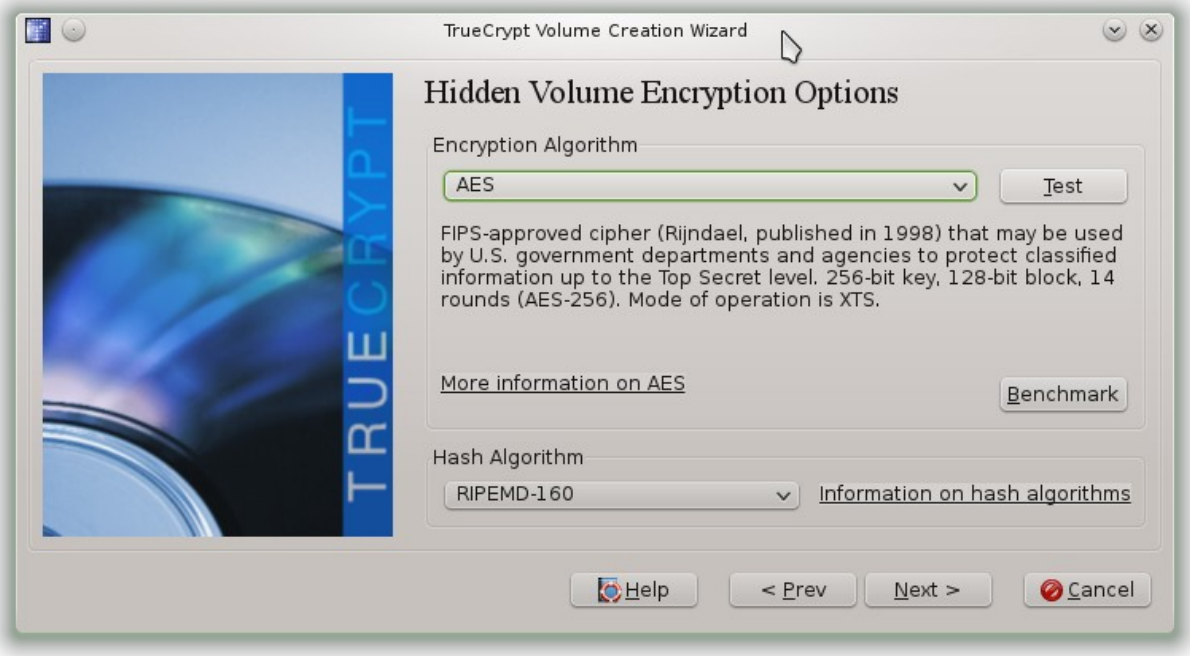


A questo livello il volume *esterno* é completato e montato. Possiamo aprirlo per depositarvi dei files ma essendo un'operazione fattibile anche in seguito consiglierei di rinviarla e cliccare su Next

Passo 13h - Inizio creazione volume hidden - opzioni crittografiche

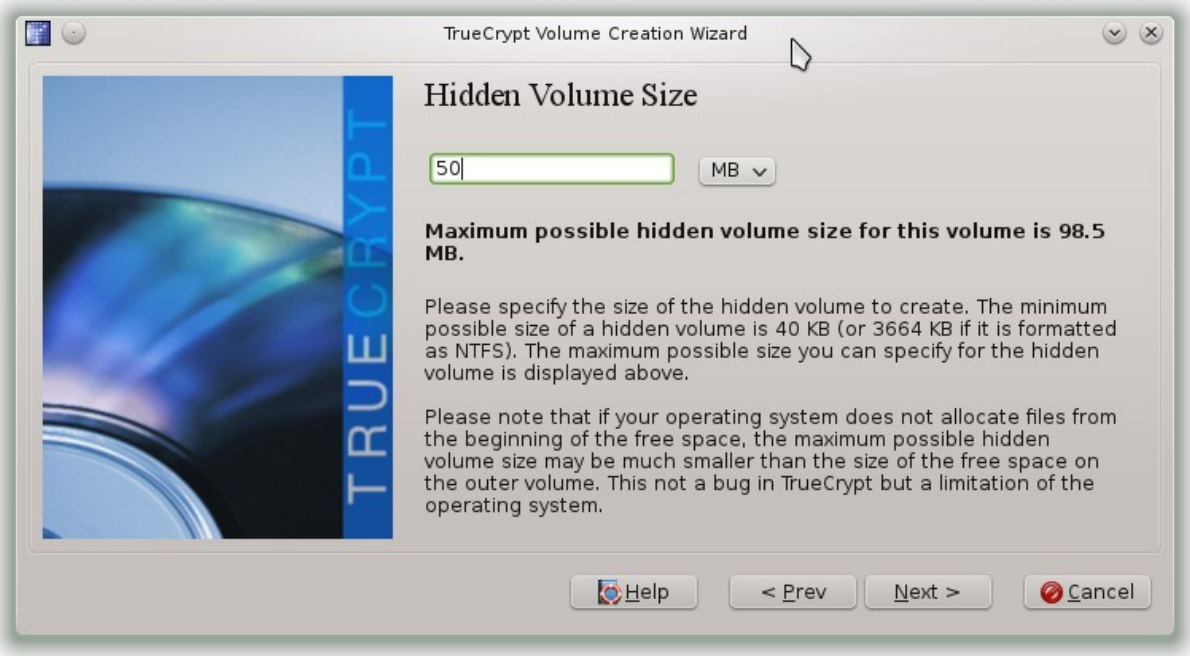


Inizio creazione *hidden volume*. Click su Next



Scelta dei parametri crittografici per lo *hidden volume*. Anche qui come nel precedente **Passo 8** i parametri preimpostati sono ragionevoli e quindi si può anche solo cliccare su Next

Passo 14h - Scelda dimensioni volume hidden



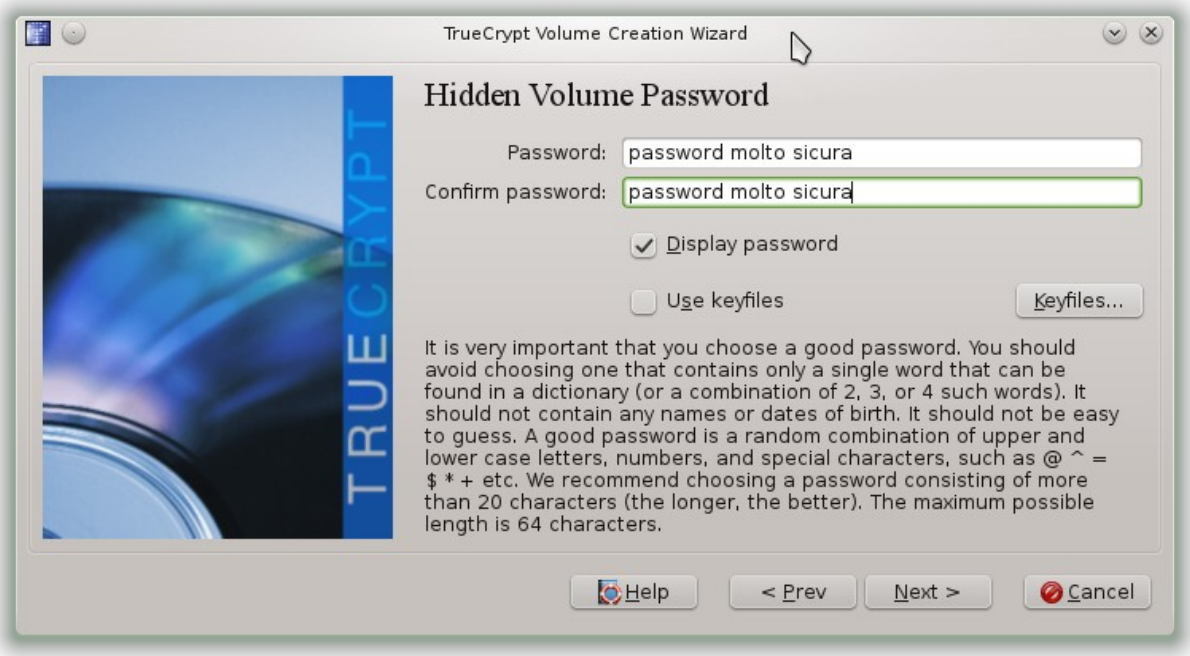
Qui scegliamo la dimensione dello *hidden volume*. Siccome vogliamo mettere dei files in quello *esterno* per la Plausible Deniability dovremo restare al di sotto della dimensione massima indicata in finestra, la cui scritta recita:

Specificare la dimensione dello *hidden volume* da creare. La dimensione minima possibile é di 40 KB (oppure 3664 KB se lo si formatta NTFS). La dimensione massima possibile che potete specificare é visualizzata qui sopra.

Notare che se il vostro sistema operativo non alloca i files dall'inizio dello spazio libero la dimensione massima possibile per lo *hidden volume* potrebbe essere molto inferiore allo spazio libero nel volume *esterno*. Questo non é un difetto di TrueCrypt ma una limitazione del sistema operativo.

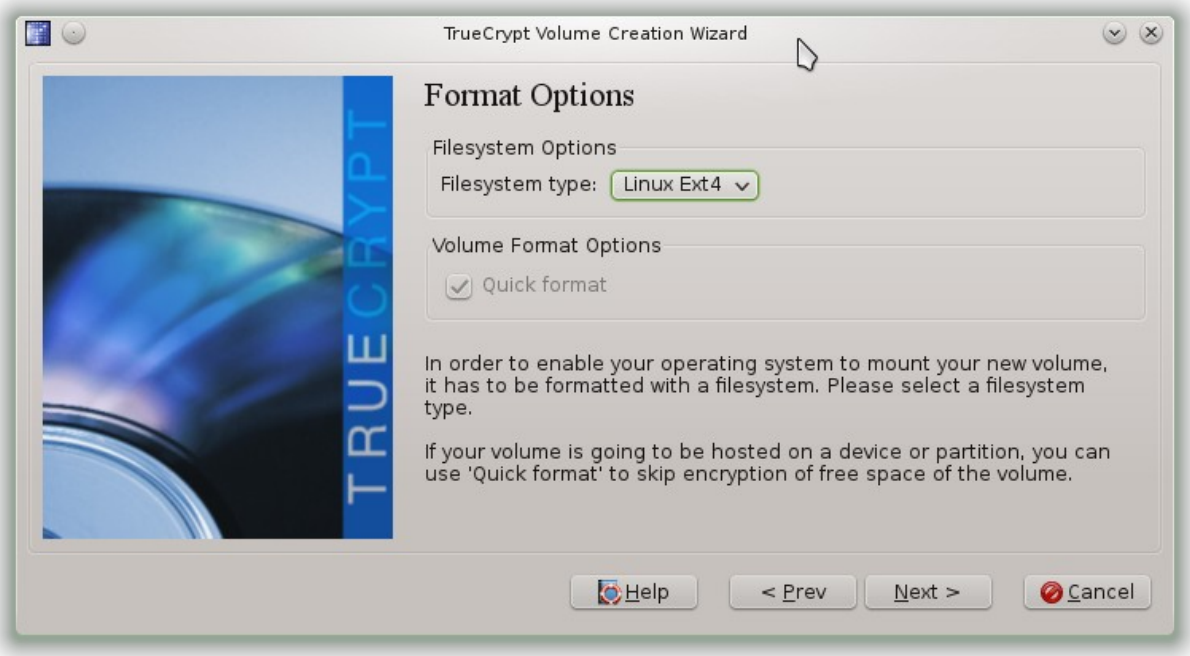
E questa é una buona ragione per creare prima lo *hidden volume* e poi mettere files in quello *esterno*.

Passo 15h - Pass-phrase protezione volume hidden



Qui si imposta la password/pass-phrase di protezione dello *hidden volume*. Valgono le stesse considerazioni espresse nel precedente **Passo 10**, compresa la traduzione della scritta nella finestra.

Passo 16h - Scelta filesystem volume hidden

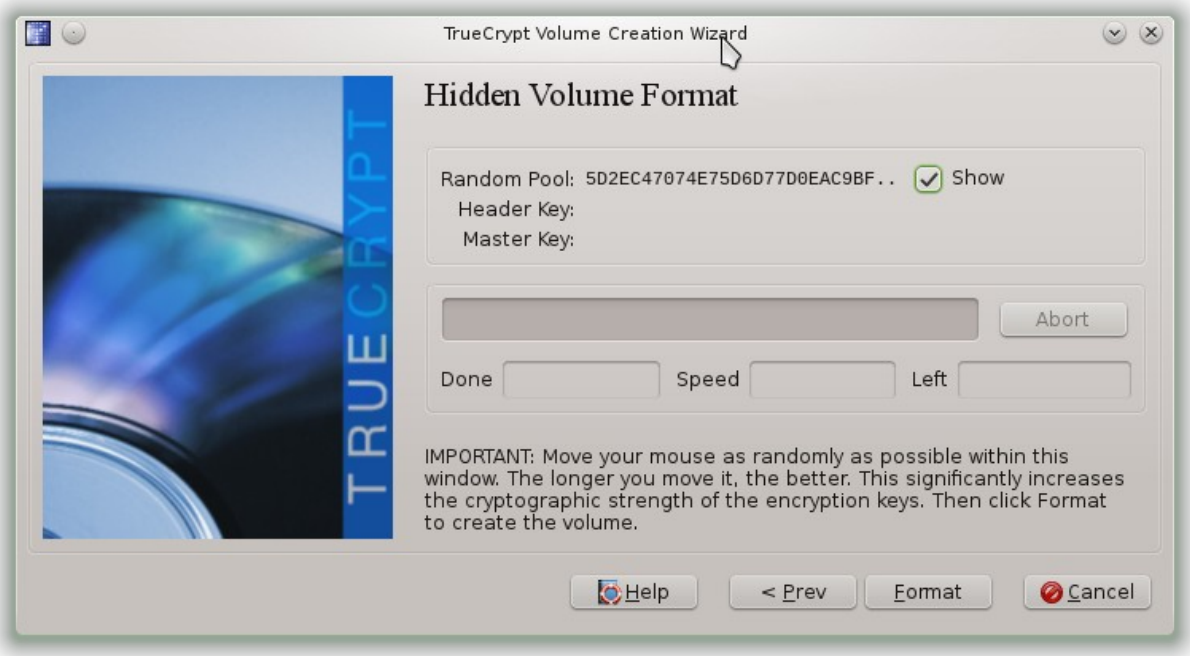


Qui scegliamo il tipo di filesystem da utilizzare per lo *hidden volume*. Stesse considerazioni e testo della finestra che nel precedente **Passo 11**

Passo 17h - Scelta mount volume hidden

Finestra di avviso come nel precedente **Passo 12** dovuta al fatto che non abbiamo formattato lo *hidden volume* con un filesystem tipo FAT

Passo 18h - Formattazione volume hidden



Formattazione *hidden volume*, stessa tecnica ed avvertenze del precedente **Passo 13** a cui si rinvia

Passo 19h - Fime creazione volume hidden

Fine della creazione dello *hidden volume*. La finestra recita:

Lo *hidden volume* TrueCrypt é stato correttamente creato ed é pronto per essere utilizzato. Se tutte le istruzioni, le precauzioni e le procedure descritte in "Requisiti di sicurezza e precauzioni relativi agli Hidden Volumes" sono state correttamente seguite dovrebbe essere impossibile provare l'esistenza dello *hidden volume*, anche se il volume *esterno* fosse montato.

ATTENZIONE: SE NON PROTEGGETE LO HIDDEN VOLUME (PER INFORMAZIONI SUL COME FARLO VEDERE OLTRE) NON SCRIVETE NEL VOLUME ESTERNO PERCHE' RISCHIERESTE DI SOVRASCRIVERE E DANNEGGIARE LO HIDDEN VOLUME.

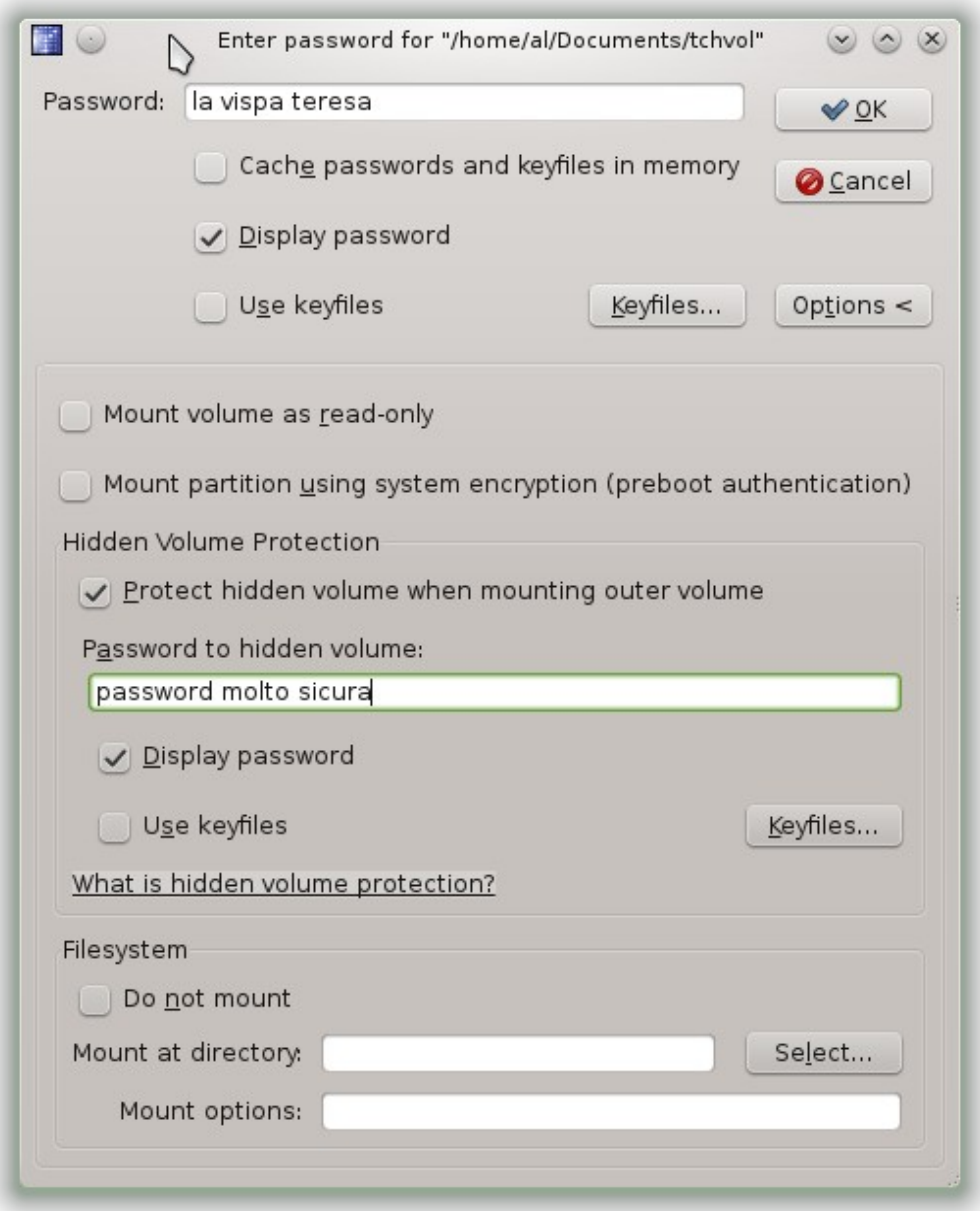
Passo 20h - Finestra finale

A questo punto a meno che non vogliate creare un altro contenitore cliccherete su Exit.

Protezione dei volumi nascosti dal danneggiamento

Se montate il volume *esterno* di un volume TrueCrypt contenente uno *hidden volume* e ne leggete i contenuti non correte nessun rischio. Ma se voi, o il sistema operativo, tentate di scrivervi, c'é il rischio di danneggiare lo *hidden volume*. Per prevenire questa eventualità dovete proteggerlo nel modo descritto più oltre.

Montando il volume esterno, dopo aver digitato la password, prima di cliccare OK cliccare Options



Ora é necessario specificare che si desidera la protezione dello hidden volume e fornirne la password. Fatto ciò potremo cliccare su OK

Entrambe le password debbono essere corrette, altrimenti non verrà montato nulla. Quando viene abilitata la protezione dello hidden volume, TrueCrypt non monta lo hidden volume. Ne decripta, in RAM, solamente lo header per ricavarne informazioni sullo spazio da lui occupato. Poi viene montato il volume esterno e viene bloccato ogni tentativo di scrittura nell'area occupata dallo hidden volume, almeno finchè non verrà smontato il volume esterno.

Consiglio di sperimentare un pò nel sorpassare la capacità reale del volume esterno: io ho notato in

almeno un paio di occasioni che "sembrava" che fossero stati scritti files per la capacità in eccesso pur non essendo stato toccato il volume hidden. Non ho provato a rileggerli ed immagino che contenessero garbage. In ogni caso non avrebbero che migliorato le cose dal punto di vista della plausible deniability.

Plausible Deniability

Nel caso siate forzati a rivelare la password, TrueCrypt fornisce e supporta due tipi di plausible deniability:

1. Volumi Nascosti (hidden volumes) e Sistemi Operativi Nascosti.
2. A meno che non vengano decriptati, una partizione o un disco TrueCrypt consistono di null'altro che dati casuali, ovvero non contengono alcun tipo di "firma". Pertanto e' impossibile **provare** che una partizione o un disco siano un volume TrueCrypt o che siano stati criptati, posto che siano state seguite le procedure e precauzioni descritte più avanti. Una possibile spiegazione plausibile dell'esistenza di una partizione o disco contenenti solo dati casuali potrebbe essere che ne avete fatto il "wipe" ovvero la "cancellazione sicura" con uno dei tools che lo fanno sovrascrivendo con dati casuali (in effetti TrueCrypt potrebbe essere usato per cancellare in modo sicuro una partizione o un disco creandovi un volume criptato vuoto. Comunque é necessario prevenire le fughe di dati, e notare che nel caso di encryption del sistema operativo la prima traccia contiene, in chiaro, il bootloader TrueCrypt che può essere facilmente identificato come tale, vanificando la plausible deniability. Quando si utilizza un sistema operativo criptato la plausible deniability può essere ottenuta creando un "sistema operativo nascosto" per i dettagli del quale si rinvia alla copia completa del manuale.

Nonostante i volumi TrueCrypt su file non contengano nessun genere di "firma" perchè finchè non sono decriptati sembrano contenere esclusivamente dati casuali, di per sè non permettono la plausible deniability perchè non esiste sostanzialmente nessuna spiegazione veramente plausibile all'esistenza di un file contenente solamente dati casuali. Mentre possiamo averla se creiamo al suo interno uno *hidden volume* (il volume esterno conterrà dati che ne giustificheranno l'esistenza).

Quando si formatta una partizione come volume TrueCrypt la tabella delle partizioni, compresi gli ID delle partizioni, non vengono mai modificati (non viene scritta alcuna "firma" TrueCrypt nella tabella delle partizioni).

Esistono metodi per individuare files o dispositivi contenenti dati random, come appunto i volumi TrueCrypt. Questo però non tocca la plausible deniability in alcun modo. L'avversario non può comunque **provare** che la partizione o il dispositivo siano un volume TrueCrypt e soprattutto che il file, partizione o dispositivo contengano uno hidden volume, a patto che siano state seguite le procedure e le precauzioni opportune, descritte più avanti.

Qualche considerazione pratica: la plausible deniability si basa su un gioco *corretto* delle parti, se così vogliamo chiamarlo. Se l'avversario ha potere di coercizione sufficente potrà esercitarlo fino ad ottenere tutto ciò che esiste, o peggio ancora anche solo *sospettato* che esista. Pensate un pò ad un criminale interessato ai vostri dati, o a quanto lui presume voi conosciate, e sufficentemente determinato ad ottenerli... o a certi regimi repressivi in cui non si possa far conto sul rispetto della legalità da parte di nessuno...

Il termine *corretto* usato a proposito del gioco delle parti é da specificare bene. Non é corretto né morale per esempio tentare di nascondere alla giustizia le proprie "marachelle". Lo scopo di TrueCrypt non é nè può essere coprire le malefatte. Ma come ogni arma può danneggiare tanto un nemico come un amico così questo strumento può essere abusato. Pertanto é normale che la presenza di un contenitore criptato con TrueCrypt o altro prodotto che consente giochetti tipo hidden-volume susciti il sospetto del magistrato e la sua eventuale insistenza anche quando uno ha rivelato tutto cio' che c'era da rivelare. Quindi non usatelo per nascondere le lettere dell'amante...

Requisiti di sicurezza e precauzioni relativi agli Hidden Volumes

Voglio riportare una serie di consigli e precauzioni, senza pretesa di essere esaustivo. Nel manuale ufficiale si può trovare una trattazione abbondante ed accurata dell'argomento.

Qui voglio solo ricordare che ci sono altri modi con cui un avversario può venire a conoscenza dei nostri dati, o almeno di parte di essi ma quanto basti per spingerlo a mettere in atto azioni di costrizione per venire in possesso dei restanti.

Per esempio nei residui che rimangono sugli hard-disk dopo la cancellazione dei files, o nelle caches (browser, posta ecc.), o a causa di operazioni di compattazione e così via.

Quando si maneggiano dati che si vogliono assolutamente mantenere segreti, come linee guida di comportamento é bene che questi dati risiedano in modo "stabile", per così dire, ovvero siano archiviati, solo su volumi criptati *hidden*. Al di fuori di questi i dati debbono transitare solo per la RAM. Per ottenere ciò si può per esempio operare con una distribuzione "live" del sistema operativo ed un'installazione "portatile" di TrueCrypt sullo stesso supporto dei volumi criptati. In questo modo non c'é rischio di scrittura, anche solo temporanea, dei dati o di parte di essi al di fuori di supporti volatili (RAM).

Anche senza leakage vero e proprio di dati in chiaro talvolta la plausible deniability può venir danneggiata da altre circostanze. Per esempio se l'avversario é in grado di venire in possesso di copie del nostro volume criptato riferentisi a tempi differenti, nel cui intervallo siano state fatte scritture nel volume *hidden*, potrà notare che pur sembrando sempre garbage il contenuto di certi blocchi é cambiato, e chiedercene conto. In tal caso qualsiasi manovra sul volume *esterno* non provocherà variazioni di quegli specifici blocchi, a meno di non danneggiare, sovrascrivendolo, il volume *hidden*.

Aggiungo questa doverosa nota per richiamare l'attenzione sul fatto che TrueCrypt e' uno strumento potente e complesso, dalle molteplici implicazioni e sfaccettature. Il suo uso corretto non può prescindere dal possesso di sufficenti conoscenze informatiche con cui stabilire le modalità con cui eseguire le operazioni e quali operazioni eseguire. Questo manuale non può e non vuole essere una guida esaustiva ma uno stimolo ad interessarsi ad un prodotto particolare dalle applicazioni particolari. Pertanto non ci possiamo assumere responsabilità di alcun genere connesse all'utilizzo di questo prodotto.

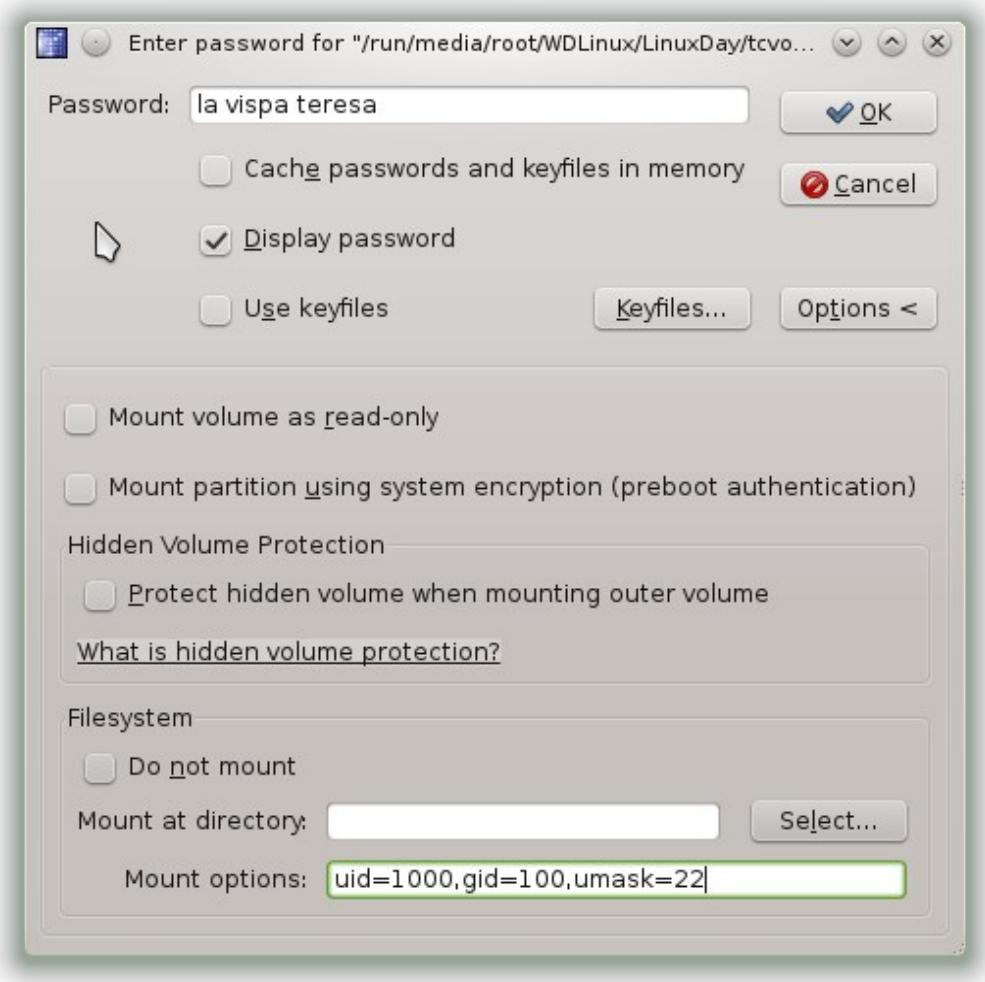
Problemi di ownership al mount

Se il volume Truecrypt é stato generato con un utente differente da quello che poi lo utilizzerà al momento di utilizzarlo si potrebbero incontrare problemi di autorizzazione all'accesso. Questi problemi sono i soliti dovuti alle protezioni messe in atto dal sistema operativo a livello filesystem.

La soluzione generica é quella di cambiare l'ownership del volume, dopo averlo montato con TrueCrypt. Il comando potrebbe essere **sudo chown -R miouser:miogruppo /path/del/mount**

Nel caso il volume fosse stato formattato con un filesystem FAT o NTFS, o altro che ammetta queste opzioni al comando mount, é possibile specificare come in figura:

uid=nnn,gid=mmm,umask=22 dove **nnn** ed **mmm** sono lo uid ed il gid numerici ricavabili dando il comando **id**



Sommario