Come criptare un disco di sistema con Veracrypt

https://turbolab.it/crittografia-945/come-criptare-disco-sistema-veracrypt-1190

https://www.linuxuprising.com/2018/10/how-to-encrypt-usb-drive-with-veracrypt.html

In questo articolo vediamo come criptare completamente un hard disk con tutto il sistema operativo e i dati personali. Se si cripta in questo modo Veracrypt crea un suo bootloader che sostituisce quello di Windows in modo che, quando si avvia il computer, compaia la richiesta della password di Veracrypt impostata in precedenza e, solo dopo averla inserita, si possa arrivare al sistema operativo vero e proprio.

Consigli importanti prima di cominciare

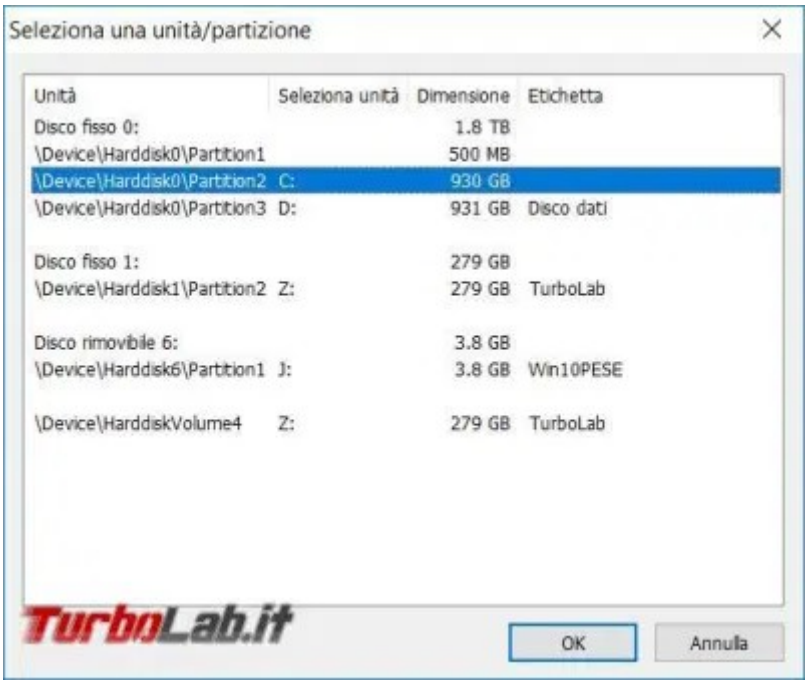
Dato che è sempre possibile che qualcosa vada storto durante le operazioni di criptazione, consiglio, prima di cominciare, di eseguire un backup dei dati importanti e anche l'immagine di sistema con programmi appositi.

VeraCrypt rallenta, e si mette in pausa, durante la criptazione. quando un altro programma scrive dei file sul disco fisso, chiudete quindi tutti i programmi e servizi attivi che possono causare problemi, quali antivirus o programmi di monitoraggio in tempo reale, il servizio Windows Search del sistema operativo, eventuali software di sincronizzazione, backup o deframmentazione. Se vedete che VeraCrypt rallenta troppo la criptazione aprite il task manager e provate a chiudere eventuali programmi che impegnano il disco fisso.

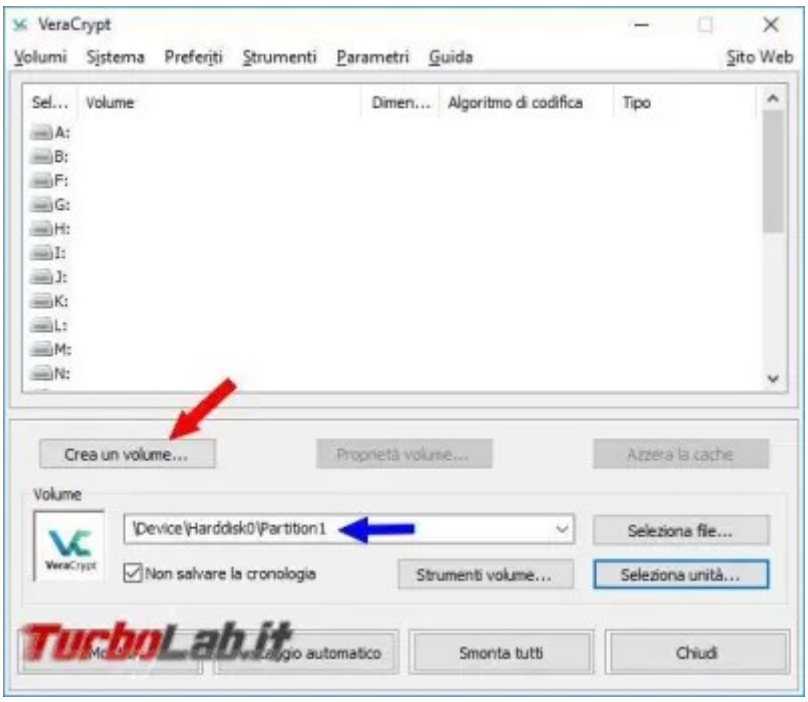
Funzionamento

Selezionate l'unità da criptare:

Potreste avere più di un hard disk/partizione, quindi indicate quello giusto da criptare.



Scegliamo Crea un volume, poco più sotto vedrete l’indicazione del disco che avete appena selezionato:



Proseguiamo con Codifica la partizione o tutto il disco di sistema.

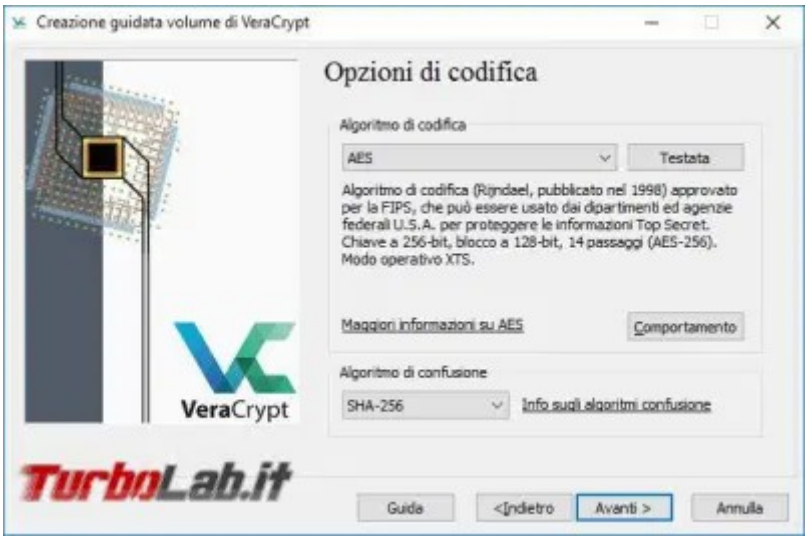
Andiamo avanti con Normale visto che non ho grossi segreti da nascondere.

Poi Codifica l’intero disco per avere una criptazione completa del disco fisso.

In molti computer di marca, a meno che non abbiate cancellato voi in precedenza il contenuto del disco fisso, spesso ci sono delle partizioni dedicate alla diagnostica e al ripristino della configurazione del sistema operativo. I comandi presenti in queste zone devono, in genere, poter agire prima che il sistema operativo si avvii, è bene quindi che non siano criptate.

Scegliete il tipo di boot, se singolo o multiplo, a seconda di quanti e quali sistemi operativi avete installato.

Se siete degli esperti di criptazione potete mettervi a modificare gli algoritmi di codifica e confusione, io non lo sono ed ho quindi lasciato quelli proposti. Se ne volete sapere di più, potete consultare questa pagina e tutte quelle ad essa collegate.

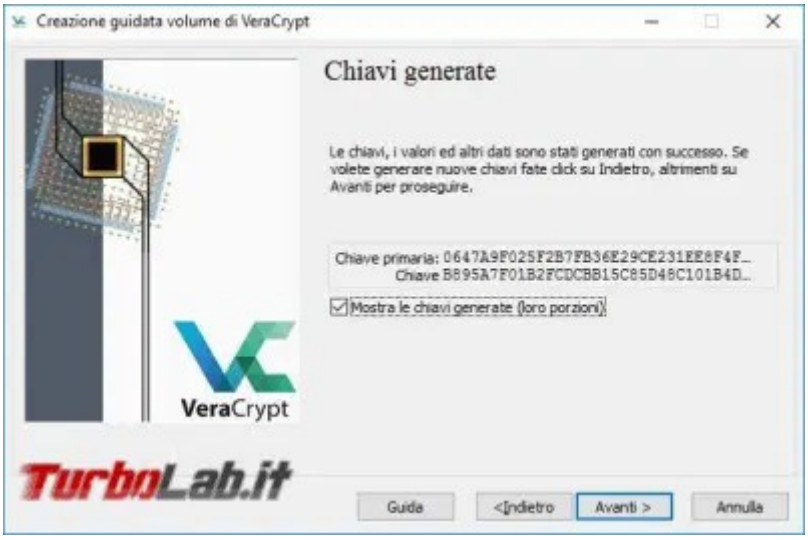


Inserite una password complessa con simboli, lettere maiuscole e numeri, vi consigliano di superare i venti caratteri, se avete buona memoria, ma accetta anche password più corte.

Una volta arrivati in questa schermata muovete il mouse in modo casuale per generare le chiavi di codifica, quando vi siete stancati di farlo premete Avanti.

Nei computer con UAC attivo chiederà conferma prima di procedere con determinate operazioni.

Una volta create le chiavi potete proseguire con Avanti.



Create il file necessario per preparare un supporto di boot con cui avviare il computer in caso di problemi, per rimuovere la criptazione o riparare il bootloader di VeraCrypt, si può mettere il flag in Skip Rescue Disk verification per saltare la masterizzazione immediata del file ISO, in caso di pc con boot UEFI crea un file zip.

Potete conservare questi file e usarli solo nel momento del bisogno, se avete più di un computer criptato rinominate i file usando il nome del computer su cui sono stati creati.

In fondo all'articolo trovate spiegato come utilizzare questi importanti file.

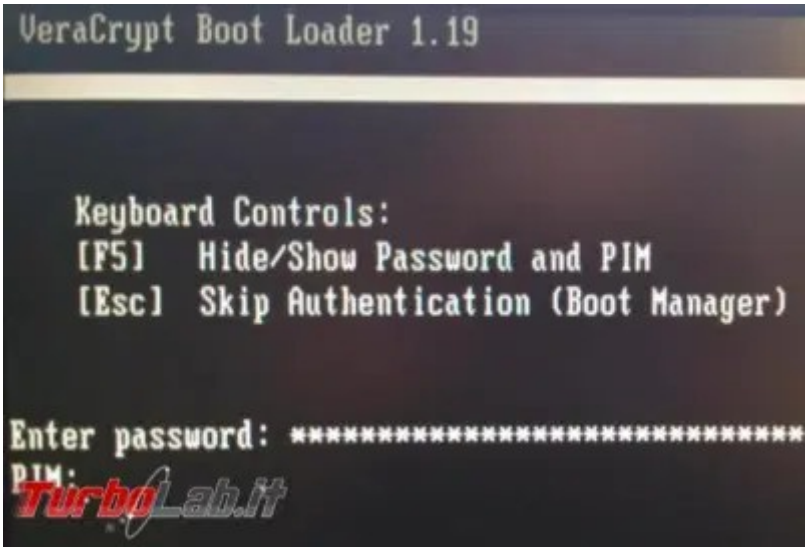
Ogni file ISO, o ZIP, è unico e personalizzato per quel computer dove è stato creato, se dovete rifare la criptazione dovete ricreare anche il file perché il vecchio non va più bene.

Decidete se sovrascrivere, io ho lasciato Nessuno come metodo di pulizia.

Arrivati a questo punto VeraCrypt deve eseguire un pre-test di codifica del sistema.

Alcune istruzioni per l'uso di VeraCrypt e poi bisogna riavviare il computer.

Al riavvio del computer comparirà un menu come quello che vedete nella foto, dovete inserire la password giusta per sbloccare il disco criptato, per il PIM basta premere invio.

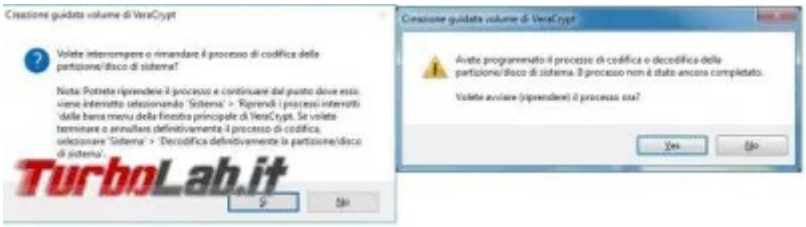


Il test si è concluso e possiamo dare il via alla vera e propria codifica del disco fisso.

Altre istruzioni per l'utilizzo di VeraCrypt.

Una volta avviata la codifica non resta che attendere alcune ore a seconda delle dimensioni del disco fisso.

Dato che l’operazione di criptazione impiega molte ore, e durante questo periodo sarebbe bene non utilizzare il computer per non rallentarla ulteriormente, la potete sospendere e riprendere quando volete, anche al successivo riavvio del sistema operativo.



Non rimane che armarsi di molta pazienza e attendere il raggiungimento del 100% della codifica.

Altro messaggio con traduzione non molto precisa, abbiamo appena finito di criptare il disco fisso, invece è scritto che è stato decriptato con successo.

Cosa fare se il volume criptato si blocca

Per quanto VeraCrypt possa essere affidabile, esiste sempre la possibilità che il bootloader di VeraCrypt, o qualche altro file importante, si danneggi e il sistema operativo non sia più in grado di avviarsi.

Per provare a ripristinare il bootloader di VeraCrypt, o decriptare un disco fisso, ci viene in aiuto il VeraCrypt Rescue Disk, o disco di ripristino, che viene creato durante l'installazione del programma.

In caso di computer con hard disk con boot mbr avrete un file ISO, che può essere masterizzato oppure trasferito su una pendrive, con un boot UEFI ci sarà un file zip il cui contenuto andrà estratto e masterizzato su un CD-Rom o copiato in una pendrive con cui avviare il computer.

Una volta avviato il computer con il supporto di boot che avete creato avrete un menu d'avvio simile a quello iniziale del boot loader di VeraCrypt dove, in più, ci sarà la voce [F8] Repair Options per accedere agli strumenti di ripristino.