freepto-docs - AvANa - Groups - we.riseup.net

Documentazione su freepto

- 1 Cos'e' freepto?
  - 1.1 Problemi comuni:
- 2 Come faccio ad avviare il sistema cifrato?
- 3 Cosa devo fare la prima volta che uso freepto?
  - 3.1 Modificare la passphrase di cifratura
  - 3.2 Modificare la password dell'utente paranoid
- 4 Tools installati
- 5 Come rendo anonima la mia navigazione sul web?
  - 5.1 Tor Browser Bundle
  - 5.2 TORtp
  - 5.3 VPN
  - 5.4 MAC Changer
- 6 Come proteggo le mie comunicazioni?
  - 6.1 Chat: Jabber + OTR
  - 6.2 Chat: IRC + TOR
  - 6.3 Mail: GnuPG
- 7 Come proteggo i miei dati?
  - 7.1 wipe
  - 7.2 MAT – Metadata Anonymisation Toolkit
  - 7.3 Bleachbit
  - 7.4 Truecrypt
  - 7.5 Tomb – The Crypto Undertaker
- 8 Accesso automatico agli Hidden Service TOR.
- 9 Avviare freepto su pc non fidati
- 10 Personalizzare freepto
- 11 Crea un nuova freepto
  - 11.1 1. scarica l'ultima versione di freepto:
  - 11.2 2. identifica la nuova pennetta usb:
  - 11.3 3. Installa freepto

Cos'e' freepto?

Freepto e' un sistema operativo live basato su Linux. Un sistema operativo live e' in grado di avviarsi direttamente da penna usb, senza toccare il disco del computer. Permette quindi di avere il proprio sistema operativo sempre in tasca, utilizzarlo sul sistema che si preferisce, senza bisogno di installare niente.

Esistono molti altri sistemi live, ma freepto si contraddistingue per l'attenzione alla sicurezza e all'usabilita', offrendo un sistema pensato per le necessita' dell'attivismo.

La pagina ufficiale del progetto la trovi qui: www.freepto.mx
h2. Come avvio freepto?

Per avviare freepto è necessario settare il proprio BIOS per effettuare il boot da USB.

Per selezionare il boot da USB, premere, subito dopo l'accensione del computer, il tasto `ESC`: questo dovrebbe far apparire un pannello di selezione del dispositivo di boot. Seleziona la penna usb!

Se questo non dovesse riuscire, si dovra' accedere al BIOS: solitamente è sufficiente durante l'avvio del computer premere uno di questi tasti: `ESC`, `F2`, `Canc` o `F10`. Purtroppo è impossibile indicare una procedura valida per tutti i casi, perchè ovviamente il menu del BIOS è differente da modello a modello. Quindi, almeno in questo caso, Google è tuo amico: cerca, ad esempio "boot usb" seguito dal modello / marca del tuo computer. Configurato il BIOS per l'avvio da USB, puoi semplicemente riavviare ed aspettare che freepto venga avviata.

Se tutto va per il verso giusto vedrai una schermata simile a questa:

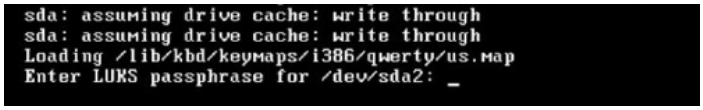
Problemi comuni:

- **Vedo la schermata con il logo, ma l'avvio si ferma subito per problemi con il tipo di cpu**

Stai usando un pc molto vecchio che non supporta il 64bit. Seleziona l'opzione `(486)` dal menu (nota: questa e' una novita' di freepto 0.1.2: prima non era possibile usare questi computer)

Come faccio ad avviare il sistema cifrato?

Durante la fase di boot di freepto ti verrà chiesto di inserire una passphrase per sbloccare la persistenza cifrata, con una stringa come questa:



E' possibile ignorare questa richiesta ed avviare freepto in modalità live, in questo modo però qualsiasi modifica fatta durante l'utilizzo di freepto verrà persa al successivo riavvio.

Montando la persistenza è invece possibile conservare i documenti creati e portarli con se in un sistema sicuro e cifrato.

Se non ricordi la password, o non vuoi inserirla perche' l'ambiente non e' fidato (ad esempio se ci sono telecamere) puoi evitare di mettere la password e il sistema si avviera' ugualmente, ma in modalita' /live/: non vedrai i tuoi dati salvati, ne' potrai salvarne di nuovi. Potrai comunque usare il sistema di base senza problemi.

Cosa devo fare la prima volta che uso freepto?

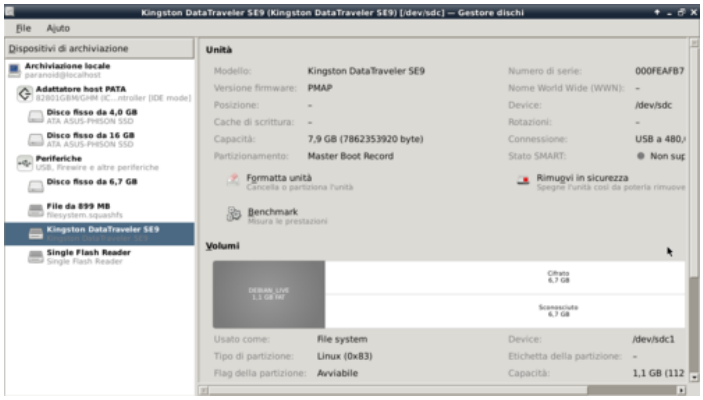
Modificare la passphrase di cifratura

Tutte le crypto-usb freepto hanno una passphrase di cryptseutp di default uguale per tutte ("freepto"), questo è necessario per permettere di automatizzare la procedura di installazione e distrbuire un sistema già installato e funzionante.

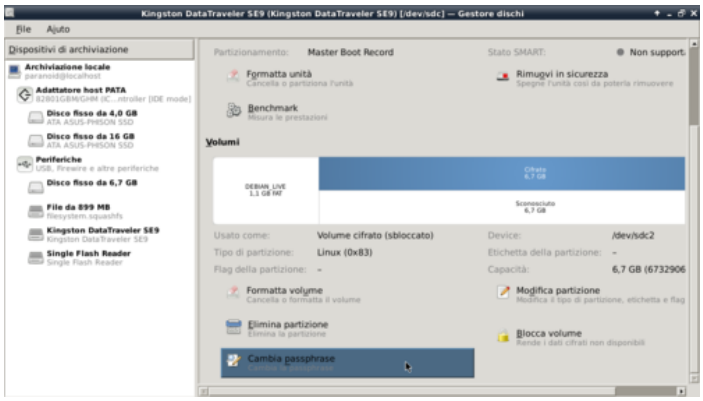
E' **ASSOLUTAMENTE NECESSARIO** modificare la passphrase di default, con una scelta da voi. Qui potete trovare alcune indicazioni su come scegliere una passphrase sicura.

Per cambiare passphrase bastano tre semplici passaggi

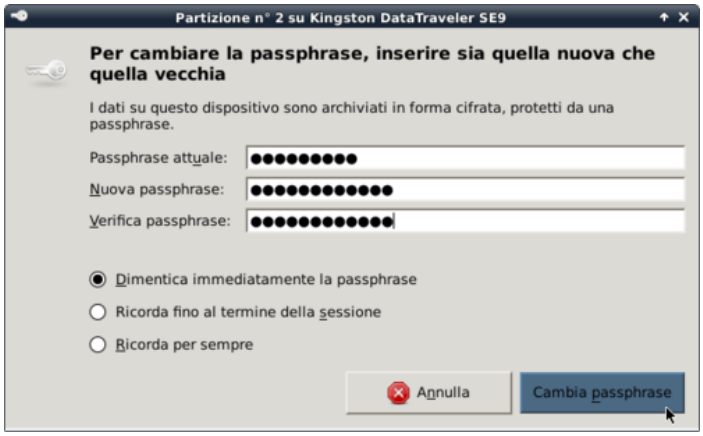
- 1. Aprire il menù delle applicazioni in alto a sinistra quindi "Accessori" —> "Gestore Dischi"



- 2. Selezionare la pennetta usb e poi la seconda partizione (cifrata)



- 3. Dal menù scegliere “modifica passphrase”



Modificare la password dell’utente paranoid

L’utenza configurata di default è la seguente:

- user: `paranoid`
- password: `live`

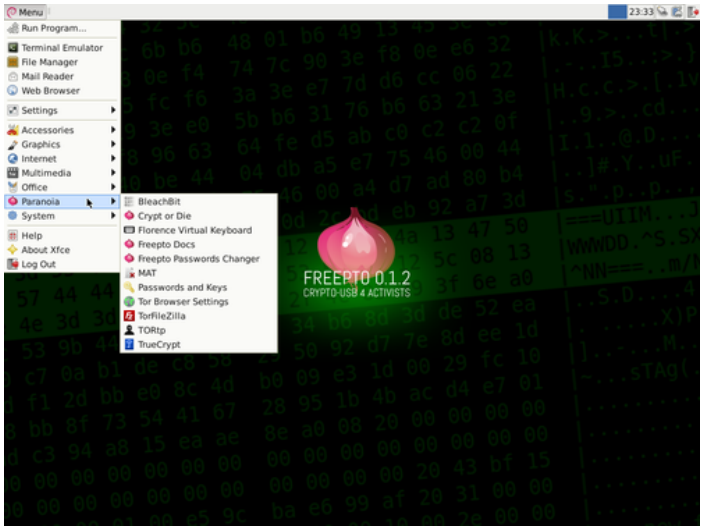
E’ bene cambiare la password con una piu’ sicura (Leggi alcune indicazioni su come scegliere una passphrase sicura).

Per farlo e’ sufficiente usare lo strumento `Freepto Password Changer`, che potete trovare nel menu `Paranoia`.

Tools installati

Nel classico menu delle applicazioni abbiamo voluto mettere in evidenza quelle piu' "particolari" per la tutela della sicurezza con un menu dedicato.

Tra di esse ci sono strumenti per la navigazione anonima, strumenti per la pulizia dei file temporanei, strumenti di cifratura. La descrizione di questi programmi e' approfondita piu' avanti.



Come rendo anonima la mia navigazione sul web?

Tutti i seguenti tool sono già installati di default su freepto

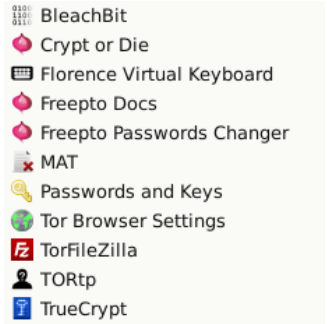
Tor Browser Bundle

Il Tor Browser è un software che integra Tor, Vidalia ed una versione modificata di firefox che migliora la sicurezza e l'anonimato della navigazione. Per maggiori informazioni, consulta la sezione dell'opuscolo dedicata

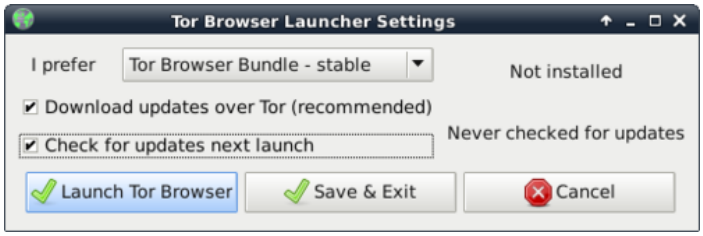
Gli obiettivi principali del TorBrowserBundle sono l'anonimato e la sicurezza della tua navigazione per questo motivo i suoi aggiornamenti da parte degli sviluppatori sono molto frequenti ed è molto importante per te avere sempre l'ultima versione disponibile.

Per questo motivo in Freepto TorBrowser non è installato di default, ma è presente torbrowser-launcher una sorta di gestore del TorBrowserBundle che si occupa di scaricare l'ultima versione disponibile e di avvisarvi quando ne è disponibile una nuova, in questo modo potete averne con pochi click sempre l'ultima versione disponibile.

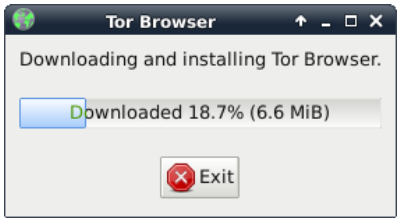
Dal menu `freepto` lancia `Tor Browser Settings`:



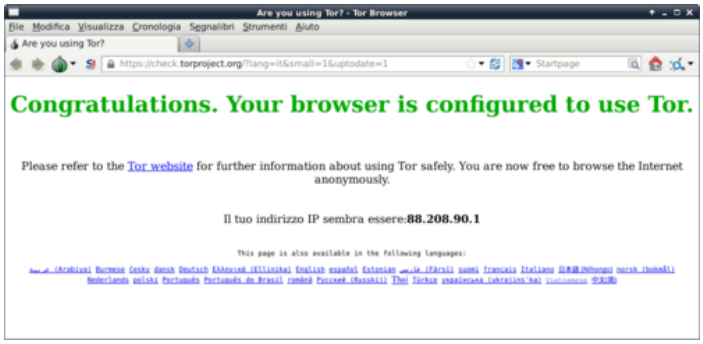
Seleziona come versione la `stable` e spunta `check for updates next launch`



A questo punto torbrowser-launcher scaricherà la versione più aggiornata di TorBrowser:



Al termine dell'instalazione si apre TorBrowser e potete inziare a navigare anonimamente:



TORtp

Puoi lanciarlo a partire dal menu "Freepto".

TORtp e' un semplice script che permette di redirigere tutto il traffico tcp generato dal tuo computer (oltre che tutte le richieste dns 53/udp) verso un transparent proxy TOR. In parole povere cioè significa che una volta attivato tutto il traffico del PC (che non è già configurato per usare TOR) viene forzato a passare verso TOR proteggendo in questo modo la tua identità.

Per una navigazione anonima nel web è probabilmente sufficiente l'utilizzo di Tor Browser Bundle già installato in freepto, ma se stai facendo qualcosa di particolarmente sensibile, allora è il caso di attivare TORtp.

Una volta lanciato, puoi attivarlo premendo il tasto **1** e disabilitarlo premendo il tasto **2**. Puoi uscire premendo il tasto **4**.

VPN

Su freepto è installato OpenVPN, un software che ti permette di utilizzare i servizi di vpn autogestiti da Riseup.net e Autistici/Inventati.

Per maggiori informazioni, consulta la sezione dell'opuscolo dedicata alle VPN.

MAC Changer

Il MAC Address è l'identificativo univoco della scheda di rete utilizzata dal tuo computer.
Potrebbe essere utile, soprattutto se ti connetti da WiFi pubbliche e aperte modificare il tuo MAC address. In questo modo sarà molto più difficile associare la tua attività online ad un computer fisico.

Per modificare il tuo mac-address puoi seguire questi semplici passaggi dal terminale:

```
sudo ifconfig eth0 down
sudo macchanger -A eth0
sudo ifconfig eth0 up
```

NB: dovrai sostituire ad eth0 il nome dell'interfaccia che stai utilizzando (con molta probabilità se si è connessi via wireless sarà "wlan0" se è connessi via cavo sarà "eth0").
Puoi vedere l'elenco di tutte le interfacce presenti sul tuo computer con questo comando:

```
sudo ifconfig -a
```

Come proteggo le mie comunicazioni?

Chat: Jabber + OTR

per le chat tra 2 persone, jabber+otr è il metodo più sicuro in assoluto.
Pidgin è il programma più adatto e semplice per farlo. Su freepto, lo troverete già configurato per l'uso di OTR.

Inoltre, pidgin userà tor in automatico: in questo modo nessuno saprà dove vi trovate, e chi controlla la vostra rete (università, access point pubblico, provider casalingo, datore di lavoro) non saprà nemmeno che state chattando.

Se avete già un account Riseup o A/I avete anche un account Jabber.

Per maggiori informazioni,consulta la sezione dell'opuscolo dedicata

Chat: IRC + TOR

Per conversazioni tra molti utenti, jabber può ancora essere usato, ma senza usare OTR: a questo punto la sicurezza dipende dall'affidabilità dei vostri gestori (ad esempio autistici.org è affidabile, gmail no).

Se la paranoia non è alta, IRC è un protocollo in cui le chat multi utente sono molto semplici da gestire. Il programma per usarlo è XChat, che su freepto è già configurato per usare TOR in modo da renderti più anonimo e connettersi ai server IRC di autistici/inventati in modo sicuro.

Considerate pero' che su irc gli utenti, di default, non sono "autenticati" e chiunque potrebbe chiamarsi col nome di chiunque altro senza alcun controllo. Ci sono dei metodi per ovviare a questo limite, ovvero la registrazione dei nick; in breve, IRC e' un'ottima piattaforma per chat con un livello di sicurezza medioalto e un utilizzo molto semplice.

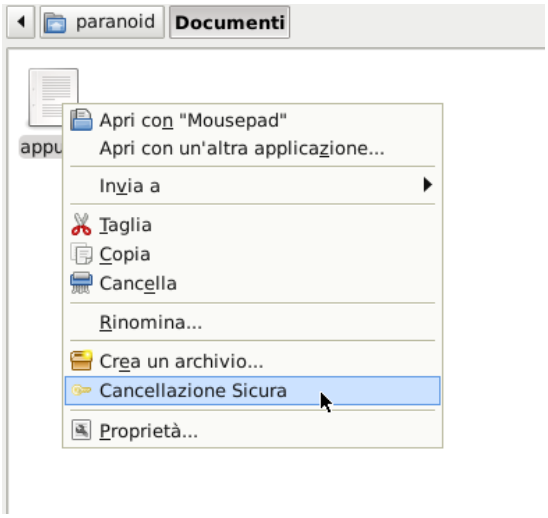
Mail: GnuPG

Per mandare le email in modo sicuro, GPG è il tool definitivo. In frepto abbiamo installato thunderbird+enigmail: in questo modo c'è un gestore di posta comodo e che permette di gestire tutto ciò che vi serve circa la cifratura di file e email con gpg.

Come proteggo i miei dati?

wipe

Il wipe sovrascrive il contenuto del file con dati casuali, prima di cancellare il file dall'indice. Infatti in genere quando si cancella un file si elimina solo la sua posizione in un indice, ma il suo contenuto rimane sul disco.
Per eseguire il wipe di un file e' sufficente clickare con il pulsante destro sul file e scegliere "cancella in modo sicuro"



il wipe del file e' piu' utile sui filesystem non cifrati che su quelli cifrati! :)

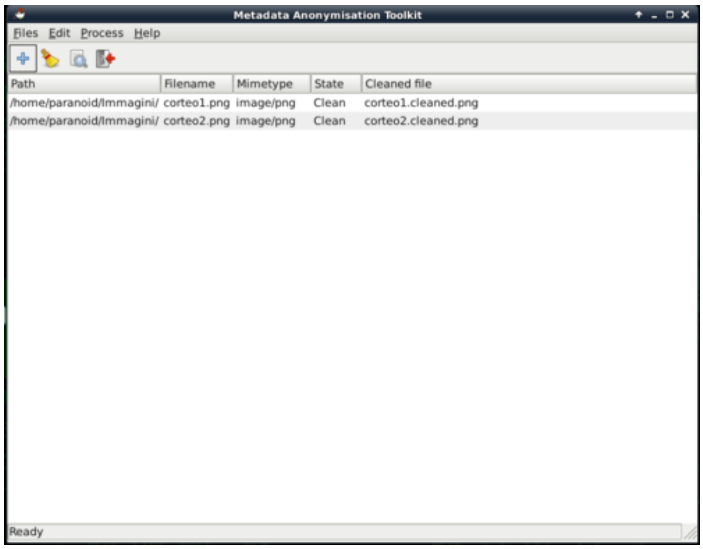
A partire da freepto 0.1.2, questo puo' essere fatto anche per intere directory: in questo modo si possono rapidamente cancellare in modo sicuro molti file semplicemente facendo tasto destro sulla directory e click.

MAT – Metadata Anonymisation Toolkit

La maggior parte dei file multimediali (file audio, immagini, video, pdf, documenti) contengono molti dati "nascosti" che potrebbero mettere a repentaglio l'anonimato; ad esempio, le immagini e i video contengono spesso il modello di camera utilizzato; e' quindi bene eliminare questi dati prima di diffondere questi file.

Per usarlo e' sufficiente aprire mat, cliccare su "Aggiungi" e scegliere i file da "pulire". A questo punto i file appariranno nella finestra di MAT e possiamo selezionarli e premere il pulsante "pulisci".

MAT creera', per ogni file, una versione `-cleaned`, mantenendo invece inalterato l'originale.



Bleachbit

BleachBit e' un programma integrato che esegue la cancellazione di una serie di dati potenzialmente sensibili di cui rimane traccia nelle cache del browser, in file temporanei generati da vari programmi e sul disco. Puoi vederlo come l'equivalente libero di CCleaner.

Truecrypt

Truecrypt è un software che permette la gestione di file o volumi cifrati.
Grazie a questo software potrai scambiare in sicurezza documenti con altre persone.

Maggiori informazioni possono essere trovate sul sito ufficiale: www.truecrypt.org

Tomb – The Crypto Undertaker

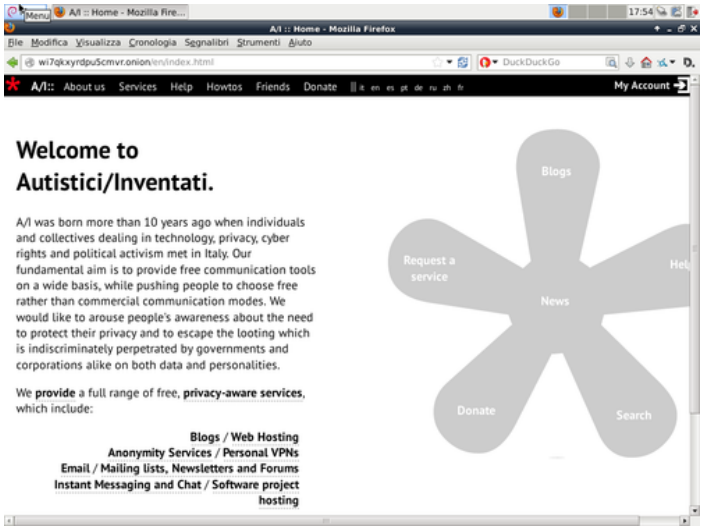
Tomb è un software opensource a riga di comando che permette la gestione di file cifrati.
L'assenza di un'interfaccia grafica lo rende adatto ad un'utenza più esperta.

Maggiori informazioni si possono trovare sul sito ufficiale: www.dyne.org/software/tomb

Accesso automatico agli Hidden Service TOR.

Su Freepto, Mozilla Firefox è configurato per utilizzare automaticamente Tor quando si tenta di accedere agli Hidden Service, ovvero tutte quelle URI che finiscono con ".onion". Questo è possibile grazie a FoxyProxy un plugin che permette di utilizzare proxy diversi a seconda della destinazione che vogliamo raggiungere.

In questo modo non è necessario abilitare TorBrowser ogni volta che si vuole visitare un hidden service (anche se per garantirsi un maggiora anonimato è comunque consigliato utilizzarlo), ma è sufficiente raggiungere il sito web ".onion" come si farebbe con qualsiasi altro sito:



Avviare freepto su pc non fidati

Se stai utilizzando freepto su un pc facilmente accessibile a chiunque (magari in un internet point, nell'auletta occupata di qualche università o in uno spazio occupato) considera che potrebbe esserci un keylogger (hardware) capace di registrare tutte le tue password.

Quindi evita, durante l'avvio di freepto, di inserire la password di cifratura perchè questo renderebbe del tutto vana la protezione del file system cifrato.

Puoi avviare freepto nella versione "live" (senza fornire la tua password di cifratura, quindi usando il sistema al suo stato originale) e successivamente potrai scrivere in sicurezza le tue password (per loggarti su webmail, etc) avendo l'accortezza di utilizzare Florence, una tastiera virtuale che ti permette di avere protezione dalla presenza di keylogger hardware.

Ovviamente Florence non ti protegge dalla presenza di telecamere o da occhi indiscreti, quindi evita di utilizzare postazioni controllabili da telecamere (e' successo che alcune password siano state captate in questo modo, quindi attenzione!)

Puoi avviare Florence attraverso il menu freepto ed avrai una finestre simile a questa:

Personalizzare freepto

Freepto e' un sistema operativo completo, quindi e' possibile aggiornarlo, installare nuovi programmi, personalizzarlo. Il modo migliore per installare nuovi programmi e' `synaptic`; dalla sua interfaccia e' possibile cercare "pacchetti" aggiuntivi, installarli, rimuoverli, aggiornarli. Al suo interno si trovano centinaia di programmi per fare qualsiasi cosa di cui abbiate bisogno: grafica, musica, presentazioni…

Crea un nuova freepto

Per creare freepto, purtroppo, e' necessario avere gia' un sistema Linux a disposizione. E' infatti necessario il programma `makefreepto`.

Dentro freepto questo programma e' gia' incluso, e può tornarti utile nel caso volessi creare una nuova freepto per qualcuno/a. Anche da un altro computer Linux, scaricarlo e' semplicissimo.

Non farti spaventare dal terminale bastano pochi semplici passaggi:

1. scarica l'ultima versione di freepto:

Tutte le versioni di freepto sono disponibili a partire da questo link: download.freepto.mx

Apri il terminale e copia-incolla il seguente comando (sostituendo alle X la versione che vuoi scaricare):

```
wget -c http://download.freepto.mx/makefreepto http://download.freepto.mx/freepto_vX.X.X/freepto-it_IT_X.X.X/freepto-it_IT_X.X.X.img
```

Questo scarichera' sia `makefreepto` che l'immagine effettiva.

2. identifica la nuova pennetta usb:

Inserisci la pennetta usb ed esegui il comando seguente per identificare il "device" a cui corrisponde.

Copia-incolla sul terminale il seguente comando:

```
dmesg | fgrep '[sd'
```

avrai un output simile a questo:

```
[ 3773.548418] sd 5:0:0:0: [sdc] 15625216 512-byte logical blocks: (8.00 GB/7.45 GiB)
[ 3773.550759] sd 5:0:0:0: [sdc] Write Protect is off
[ 3773.550763] sd 5:0:0:0: [sdc] Mode Sense: 03 00 00 00
[ 3773.551747] sd 5:0:0:0: [sdc] No Caching mode page present
[ 3773.551752] sd 5:0:0:0: [sdc] Assuming drive cache: write through
[ 3773.555490] sd 5:0:0:0: [sdc] No Caching mode page present
[ 3773.555496] sd 5:0:0:0: [sdc] Assuming drive cache: write through
[ 3773.562702] sd 5:0:0:0: [sdc] No Caching mode page present
[ 3773.562705] sd 5:0:0:0: [sdc] Assuming drive cache: write through
[ 3773.562708] sd 5:0:0:0: [sdc] Attached SCSI removable disk
```

La parte "importante" di tutto l'output è quella racchiusa tra le parentesi quadre, nell'esempio precedente il device è: `/dev/sdc`

ATTENZIONE: indicando il device sbagliato puoi rischiare di cancellare per sbaglio TUTTI I DATI PRESENTI SUL TUO COMPUTER!
Quindi se hai dei dubbi ripeti l'operazione per essere certo di aver individuato il device giusto.
Per essere piu' sicuri, puoi lanciare questo comando

```
sudo sh -c 'echo $(( $(blockdev --getsize64 /dev/sdX) / (1024*1024) ))'
```

ovviamente devi sostituire a `sdX` il nome del device che hai rilevato precedentemente.
Questo comando ti dira' la dimensione (in megabytes) del dispositivo; questo e' un buon metodo empirico per non confondere le pennine esterne (da pochi giga) con il disco del computer (da centinaia di giga).

3. Installa freepto

Dal terminale lancia il seguente comando (ovviamente devi sostiture a `sdX` il nome del device che hai rilevato precedentemente, ed a `freepto-it_IT_X.X.X.img` la versione che hai scaricato)

```
sudo bash makefreepto -i freepto-it_IT_X.X.X.img /dev/sdX
```

Otterrai un output simile a questo:

```
[+] Umount device /dev/sdb
[+] Remove all partition on /dev/sdb
[+] Starting copy
 with PID 4286
Writing 936M: 100%1914880+0 records in
1914880+0 records out
980418560 bytes (980 MB) copied, 358.496 s, 2.7 MB/s
./makefreepto: line 127: kill: (4286) - No such process
[+] Completed!
[+] Make encrypted persistent partition
Information: You may need to update /etc/fstab.

System is out of entropy while generating volume key.
Please move mouse or type some text in another window to gather some random events.
Generating key (50% done).
Generating key (75% done).
Generating key (87% done).
Generating key (100% done).
Command successful.
[+] Freepto is ready for use
```

Comments