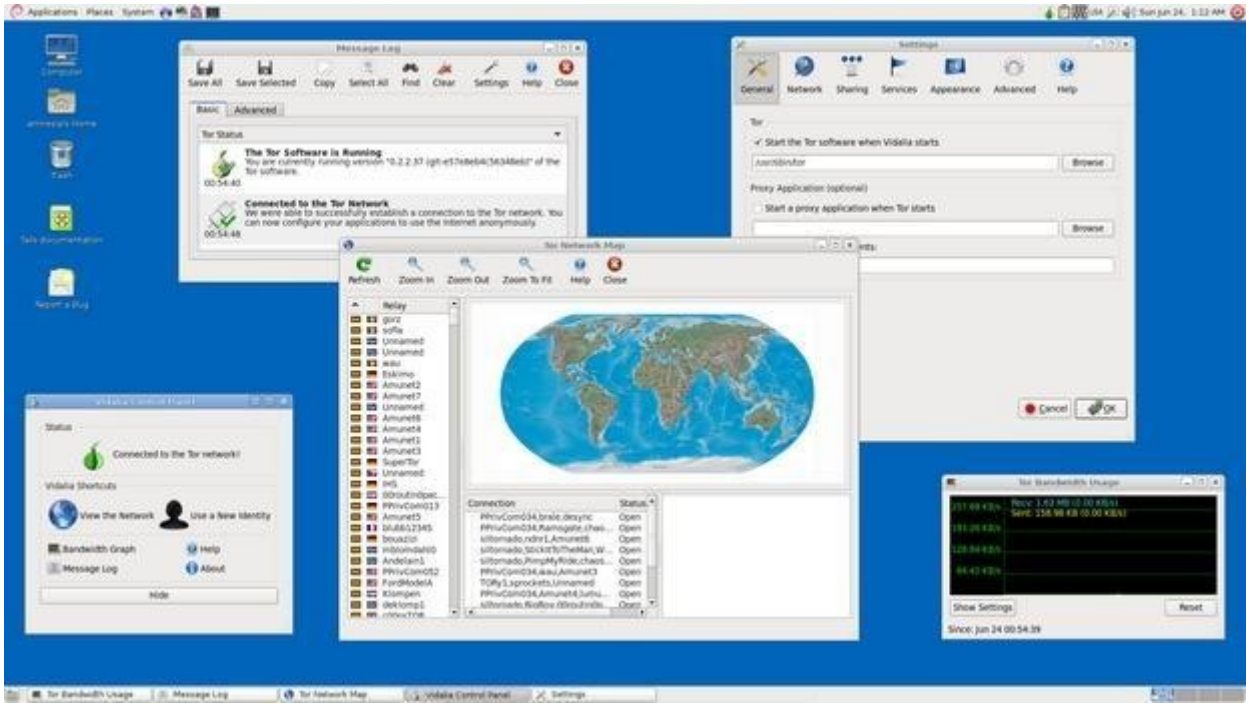
Tails, la distro Linux ultra-sicura

Esiste un sistema operativo che ci consente di utilizzare un computer in modo privato e anonimo? Per fortuna esiste. Si chiama Tails, una distribuzione Linux focalizzata sulla privatezza e l'anonimato, che è stata utilizzata da Edward Snowden per contattare i giornalisti che hanno scoperto lo scandalo dello spionaggio di massa della NSA.



Tails viene eseguito da un'unità flash USB, un DVD o una scheda SD e non lascia traccia sul computer su cui viene utilizzato. Tutti i dati e i file che gestisce sono crittografati e tutte le connessioni Internet sono crittografate e trasmesse attraverso la rete di anonimizzazione Tor, in modo che nessuno possa spiarle.

Ti mostreremo come funziona Tails, come installarlo e come usarlo su qualsiasi computer.

Che cos'è Tails?

L'"Amnesic Incognito Live System" o Tails, è una distro Linux basata su Debian , che è stata sviluppata per la privatezza e l'anonimato, come baluardi principali. È un sistema operativo amnesico perché funziona nella RAM, quindi non lascia traccia sul computer usato. Non c'è modo di rilevare che è stato usato. Viene definito anche

come sistema operativo in incognito perché crittografa tutti i dati e nasconde le connessioni Internet e l'ubicazione, quindi può essere utilizzato in modo anonimo.

In che modo Tails è un sistema operativo privato e anonimo?

- Chiunque può esaminare il codice per vedere com'è composto, e non contiene porte nascoste.
- Non utilizza il disco rigido o qualsiasi altra unità del computer in cui viene utilizzato, quindi non lascia traccia.
- Crittografa file, e-mail, messaggistica istantanea, documenti e qualsiasi altro dato gestito, in modo che nessuno possa spiarli o copiarli.
- Tutte le connessioni Internet sono crittografate e rese anonime attraverso la rete Tor. I dati rimbalzano su migliaia di computer volontari che nascondono l'IP.

Tails è supportato finanziariamente dal Tor Project e riceve anche il supporto del Debian Project, Mozilla e il Freedom of the Press Foundation. È in fase di sviluppo dal 2009 e lo scorso gennaio ha rilasciato un ottimo aggiornamento che aggiunge nuove funzionalità e prestazioni migliori. Questo è, quindi, il momento migliore per installare e utilizzare Tails.

Installazione e scaricamento di Tails

Vuoi sperimentare Tails? Può essere utilizzato su qualsiasi computer che soddisfi questi requisiti:

- Processore X86 prodotto dopo il 2005
- 2 GB di RAM
- 2 chiavette USB con almeno 4 GB di spazio e due porte USB.

Si può installare Tails su Windows, OS X, Debian o Ubuntu e altre distribuzioni Linux. È da tenere presente che ci riferiamo al sistema da cui abbiamo creato le chiavette USB; una volta creato si può usare su qualsiasi computer indipendentemente dal sistema operativo in cui è presente.

Tails funziona direttamente su un'unità flash, un disco DVD o una scheda SD. Ad esempio eseguiremo l'installazione più comune: da Windows, su un'unità flash USB. Questa procedura è simile in altri sistemi operativi. (per Linux vedere https://tails.boum.org/install/linux/index.it.html)

Sicuramente il fatto di avere come requisito, due chiavette USB avrà attirato l'attenzione. È per motivi di sicurezza. Innanzitutto viene eseguita un'installazione parziale in una chiavetta, e da essa l'installazione finale viene eseguita nella seconda chiavetta, evitando possibili intrusioni da parte di Windows.

Lo scaricamento

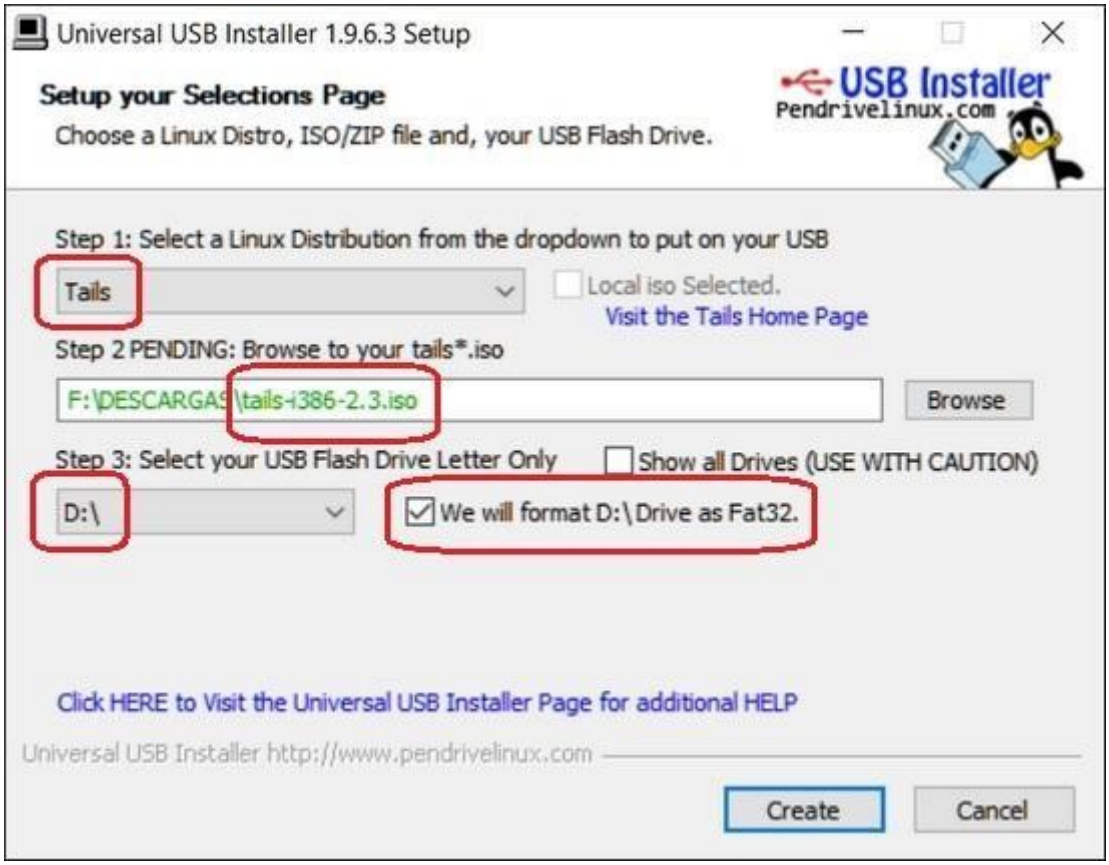
Il primo passo è scaricare Tails, che è memorizzato in un file .ISO. Per motivi di sicurezza, Tails consiglia di scaricare il file da Firefox con un'estensione speciale o da BitTorrent, poiché entrambi i metodi verificano l'integrità del file, per confermare che nessuno lo abbia modificato. Si può anche effettuare uno scaricamento diretto dal sito Web di Tails, ma questo sistema non verifica il file, quindi il malware potrebbe modificarlo. Utilizzando uno di questi metodi otterrai il file tails-i386-2.3.ISO o simile, che occupa 1,1 GB.

Istallazione nella prima chiavetta

Inserire la prima unità flash USB nel computer. Da tenere presente che saranno formattate entrambe le chiavette che si intende utilizzare.

Scarica e avvia il programma di installazione USB universale (è consigliato da Tails, usare Etcher per Windows https://tails.boum.org/install/win/usb/index.it.html).

Nel campo Passaggio 1, cerca il sistema Tails. Nel passaggio 2 selezionare il file ISO scaricato nel passaggio precedente. Al passaggio 3 scegliere l'unità flash USB. Non commettere errori perché sarà formattato! Infine, seleziona la casella Formatte Drive come Fat32 e fare clic su Crea:



Messa in moto

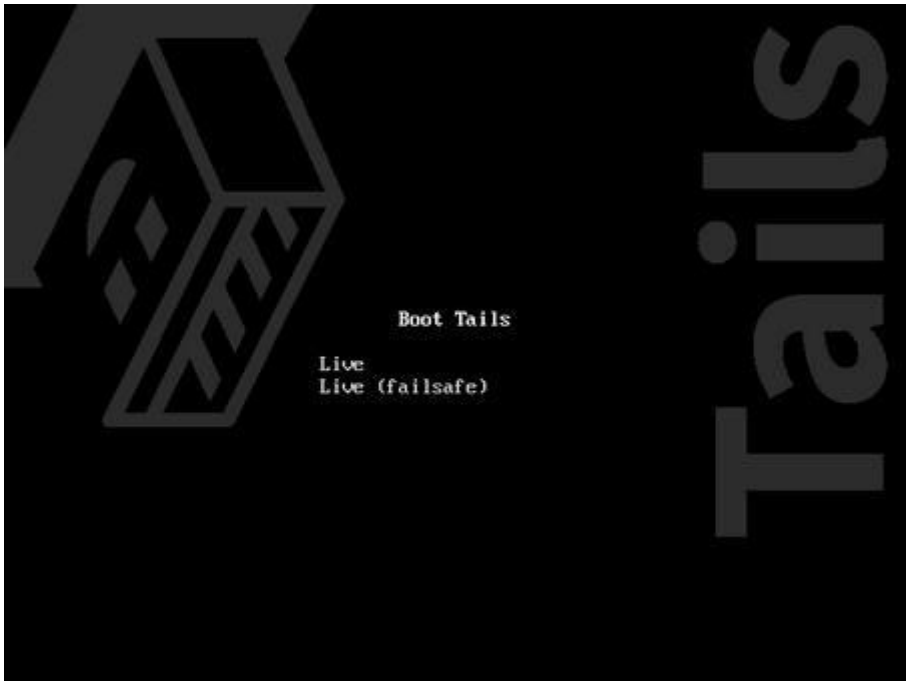
Abbiamo già Tails nella prima chiavetta, senza la maggior parte degli strumenti di sicurezza. Deve essere avviato per procedere con l'installazione finale.

Immettere la prima unità flash nel computer e riavviare. Premere il tasto F11 o quello richiesto dal BIOS per l'avvio da USB. Se non funziona e continua l'avvio in Windows, è necessario accedere al BIOS per modificare l'ordine di avvio. Riavvia nuovamente il computer e premi rapidamente il tasto F12 o Canc prima dell'avvio di Windows per accedere al BIOS.

L'opzione cambia in base al produttore, quindi accedi ai menu e cerca una sezione chiamata Inizio, Start, Boot o simili. Vedrai che il disco rigido è in prima posizione.

Utilizzare le frecce della tastiera e il tasto Invio, per modificare l'ordine di avvio del sistema dal connettore USB, quindi dal disco rigido. Salvare le modifiche nel BIOS e riavviare il computer.

Ora premi di nuovo F11 all’avvio, il computer dovrebbe avviarsi dalla chiavetta, avviando Tails. Vedrai un menu di avvio come questo:



Premi il tasto Invio per avviare Tails. Apparirà una finestra iniziale. Assicurati di cambiare la lingua in italiano nella barra in basso e premi Invio:

Istallazione finale

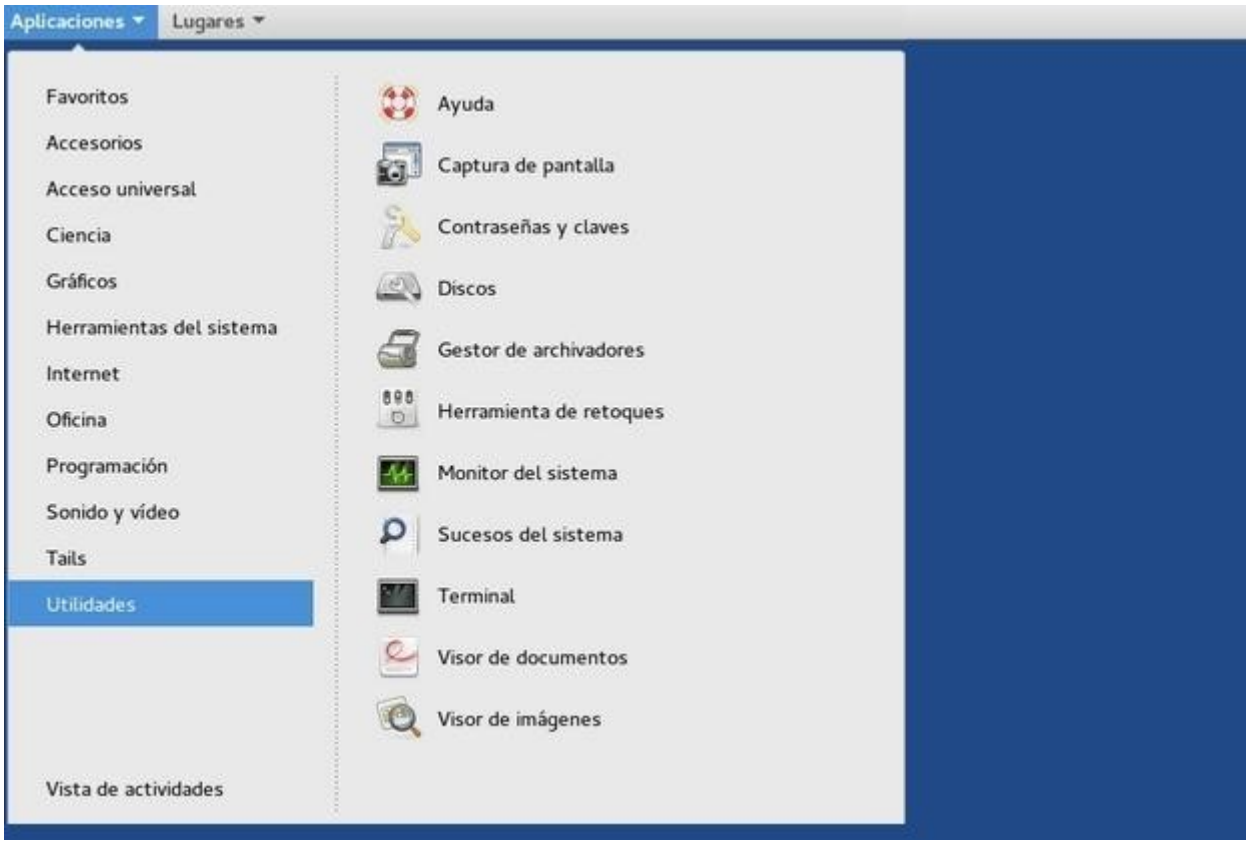
Ciò che abbiamo ora, è un’installazione parziale di Tails senza le misure di privatezza attivate. Andiamo a completare l’installazione finale.

Collegare la seconda chiavetta, che sarà anch’essa formattata.

Sulla scrivania di Tails, andare al menu Applicazioni, nell’angolo in alto a sinistra, e entrare in Tails. Avviare il programma di installazione di Tails:

Fare clic su Installa per la clonazione, selezionare la seconda unità flash USB e fare clic su Installa Tails per completare l’installazione. Dopo alcuni minuti la seconda chiavetta conterrà la versione finale di Tails. Rimuovere la prima, che è possibile utilizzare per altre cose, e riavviare il computer con la seconda unità flash. Ora si può usare Tails su qualsiasi computer semplicemente inserendo l’unità USB e avviandola da essa:

Nella barra in alto troverai l’accesso alla configurazione, i Luoghi (le unità di memoria) e le applicazioni installate:



Da tenere presente che, per motivi di sicurezza, non si avrà accesso ai dischi rigidi del computer, a meno che non vengano crittografati, Se si desidera archiviare qualcosa, utilizzare una chiavetta o un disco rigido esterno, che si collega al computer.

Per navigare, avvia il navigatore Tor, che rende anonimi l'ubicazione e l'identità. Tutto ciò che fai, viene eseguito nella RAM, quindi quando chiudi Tails non lascerai traccia di alcun tipo sul computer che hai utilizzato.

Logicamente, l'applicazione di numerosi livelli di sicurezza e crittografia fa funzionare più lentamente Windows o di altri sistemi. È il piccolo handicap da pagare per mantenere la privatezza e l'anonimato. Ma ne vale la pena!

¿Come funziona Tails?

Affinché un sistema operativo esegua operazioni come crittografare i file o rendere anonima la connessione, è necessario il supporto di programmi che eseguono queste attività. Tails include un gran numero di applicazioni gratuite create per garantire privatezza e anonimato. Questi sotto sono i più importanti:

Comunicazione

- Tor Browser: il navigatore Tor, si incarica di nascondere l'ubicazione e rendere anonimo tutto l'accesso alle pagine Web e ai servizi Internet.

- HTTPS Everywhere: crittografa la maggior parte dei siti Web visitati
- NoScript e Torbutton proteggono dagli attacchi Javascript.
- Adblock Plus: blocca la pubblicità intrusiva.
- Icedove (Thunderbirds): gestore di e-mail con opzioni di crittografia e privatezza aggiuntive.
- Gooby: editor di testo con opzione di lavoro di gruppo.
- Aircrack-ng: audit di sicurezza della connessione WiFi.
- I2P: Rete di anonimato alternativa a Tor.
- Electrum: Un client per usare Bitcoin.

Crittografia e privatezza

- LUKS:Crittografa dischi e unità USB.
- GnuPG: basato su OpenPNG, crittografa e-mail e file.
- PWGen: Generatore di password complesse.
- Florence: tastiera virtuale per immunizzare i keylogger.
- MAT: Anonimizza i metadati dei file.
- KeePassX: Gestore di password.

Applicazioni

- LibreOffice: Software Office compatibile con Office. Elaboratore di testi, foglio di calcolo, presentazioni, ecc.

  Gimp e Inkscape: Modifica delle immagini.

- Audacity: registrazione di audio multi-traccia, la loro modifica e il relativo mixaggio.
- PiTiVi: software di montaggio video non lineare.
- Brasero: software libero di masterizzazione di Cd e Dvd.
- È molti altri…

Naturalmente, puoi anche installare tutti i tipi di programmi Linux, a seconda delle tue esigenze.

Questo significa che Tails è sicuro al 100%, senza errori? Dipende dal computer che si utilizza. Tails può essere compromesso, se il computer utilizzato non è sicuro a livello hardware. Ad esempio, se hai un keylogger fisico installato o il BIOS o alcuni firmware sono stati hackerati. Ma su un computer pulito, Tails garantisce un elevato livello di privatezza e anonimato.