Onionshare, trasferire i file in modo anonimo e sicuro sfruttando la rete TOR

Author : Antonio Sagliocca

Date : 30 Gennaio 2019

Quanti di noi utilizzano già la rete **Tor** (**The Onion Router**), che permette al momento la forma più sicura di anonimato per navigare in Internet, cercando così di **salvaguardare la propria privacy**? Ebbene, quello di cui vorrei parlavi oggi è un programma che consente di trasferire in modo sicuro e anonimo i file di qualsiasi dimensione utilizzando proprio la rete Tor. Possiamo trasferire un file a una persona remota senza dover utilizzare servizi di terze parti, come Cloud e Mailing che, se anche offrono un traffico cifrato, richiedono spesso la registrazione o comunque cercherebbero di profilarci e impicciarsi dei nostri affari.

RETE TOR E DEEP/DARK WEB

La rete Tor, per chi non la conoscesse, è però anche la rete che permette di navigare nel **Deep/Dark Web** (non è questa la sede per spiegare qual è la differenza tra i due), proprio grazie alla sua caratteristica di anonimato che consente così a malfattori di ogni tipo di portare avanti attività criminose forti del fatto di non poter essere individuati (ma questo non è sempre vero al 100%). Ma è anche la rete nella quale chi è vittima di censura nel proprio paese può invece esprimere le proprie idee ed aggiornarsi dei fatti che accadono nel mondo in modo critico e libero. Nel Deep Web, da vari anni, sono sbarcati progetti importanti proprio per poter raggiungere anche chi nel web tradizionale (definito Surface web) non può andarci.

ONIONSHARE

Attraverso il programma “**OnionShare**”, installato sul computer di chi trasferisce il file, viene avviato un **Server Web** accessibile in internet come servizio Tor Onion, viene quindi generato un link che va condiviso con chi deve scaricare il file e che da questo deve essere aperto attraverso il **Tor Browser**. A quel punto il destinatario non farà altro che scaricarsi il file, **prelevandolo direttamente dal computer del mittente** attraverso una connessione **peer-to-peer,** cifrata end-to-end, della rete Tor. Il destinatario non avrà bisogno di OnionShare, bensì solo del famoso Tor Browser. L’anonimato del Destinatario e quello del mittente sarà protetto da Tor.

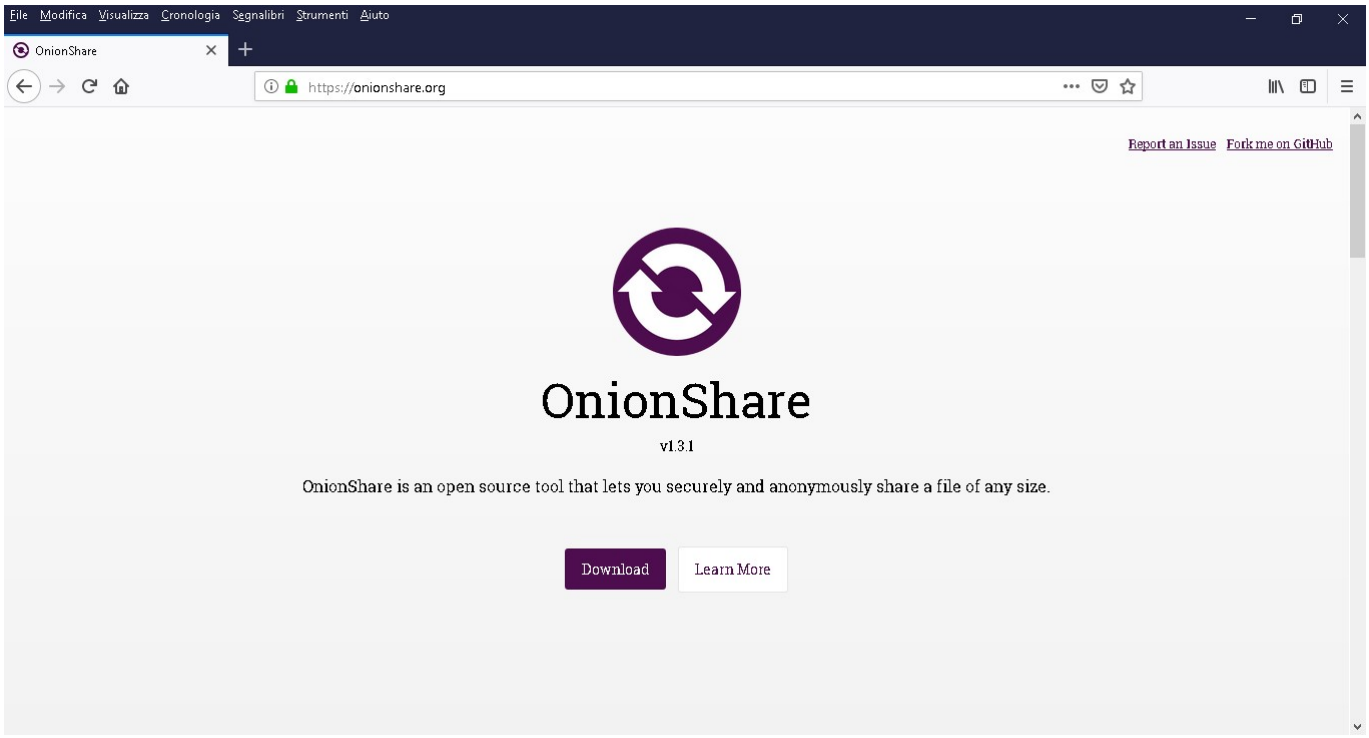
OnionShare è un software sviluppato da Micah Lee, un ingegnere informatico, sviluppatore software open source che si occupa di sicurezza e privacy. Si batte per la libertà di internet e delle informazioni, lavora per "The Intercept" l'organizzazione giornalistica pluripremiata nata dopo che gli informatori della NSA, tra cui **Edward Snowden**, hanno rivelato la sorveglianza di massa perpetrata dalla **NSA**. È inoltre membro di "Freedom of the Press Foundation" l'organizzazione no-profit che protegge, difende e potenzia il giornalismo di interesse pubblico nel 21° secolo. È conosciuto anche perché ha collaborato direttamente con Snowden nella fabbricazione di "Haven" l'**applicazione open source per Android** in grado di proteggerci dagli "spioni" (mentre scriviamo si trova sul Play Store con il nome "**Haven: Keep Watch (beta)**". Attraverso i sensori dello smartphone, quali microfono, rilevatore di luce e telecamere, che si attivano quando il proprietario si allontana, questa applicazione registra tutto ciò che accade, facendo da sentinella ai propri dati.

L'idea di OnionShare è venuta a Lee nel 2013 quando **David Miranda**, un giornalista del "**The Guardian**", veniva perquisito e detenuto per nove ore all'aeroporto di Heathrow a Londra mentre stava cercando di imbarcarsi su un aereo per tornare a casa a Rio de Janeiro. Stava lavorando a un incarico giornalistico delicato e aveva con se una chiavetta USB cifrata che conteneva documenti governativi classificati. Per Lee doveva esistere un sistema più sicuro per trasferire documenti sensibili in tutto il mondo senza doverlo fare di persona rischiando così sia di perderli sia di farli cadere in mani sbagliate.

E del resto, non è un caso se dal 24 gennaio 2017 OnionShare è incluso nella distribuzione linux live "**Tails**", famosa perché ha come slogan "**Privacy per tutti dappertutto**" permettendo di utilizzare internet in modo anonimo e sicuro e non lasciando tracce (se non espressamente voluto) sul computer che viene utilizzato per navigare. Per chi non ha le conoscenze tecniche per configurare Tor sul proprio computer e non vuole così correre alcun rischio, Tails risulta la soluzione ideale.

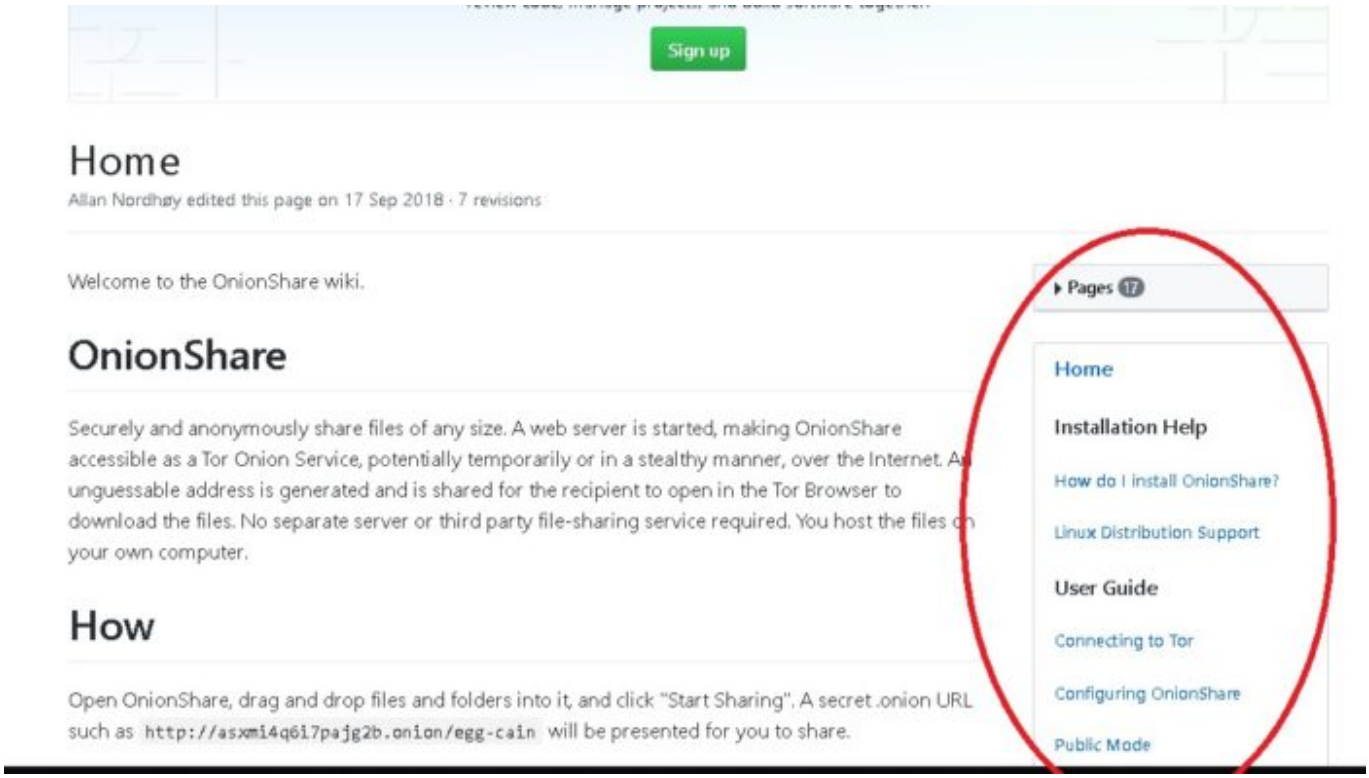
Conosciamo finalmente OnionShare, l'importante strumento di trasferimento dei file anonimo, utilizzato quotidianamente da centinaia di organizzazioni e professionisti che si occupano di libertà delle informazioni e da coloro che vogliono trasferire file all'altro capo del mondo in totale tranquillità, nonché utilizzato proprio dallo stesso Lee nella sua attività professionale. E conosciamone le caratteristiche più importanti.

La home page si presenta così ...



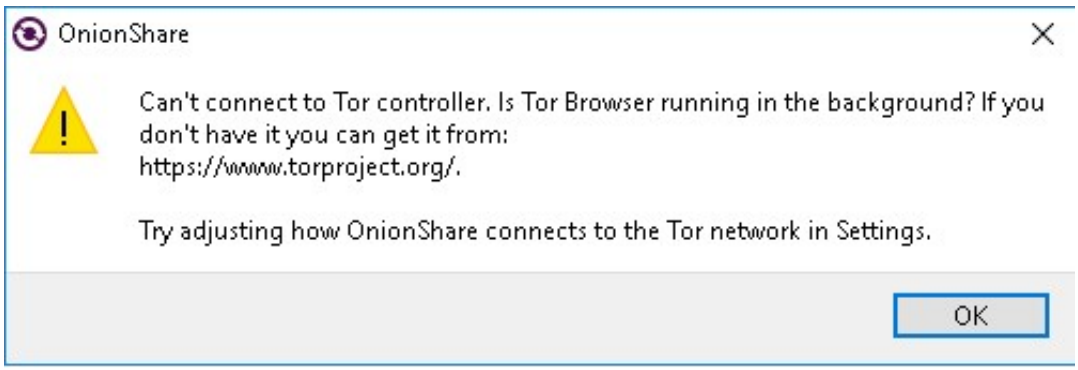
Premendo il bottone “**Download**” giungeremo dove si trovano le piattaforme per le quali il programma è progettato. Per MacOS e Windows scaricheremo i binari dell’installazione, per le varie distribuzioni linux, invece, troveremo i comandi da digitare per scaricarlo ed installarlo.

Se invece premessimo “**Learn More**” verremo trasportati sulla pagina “OnionShare Wiki” dell’autore. Questa pagina GitHub è molto importante in quanto qui possiamo trovare tutte le guide che potranno servirci, **le guide di installazione, di configurazione e di utilizzo del programma**.

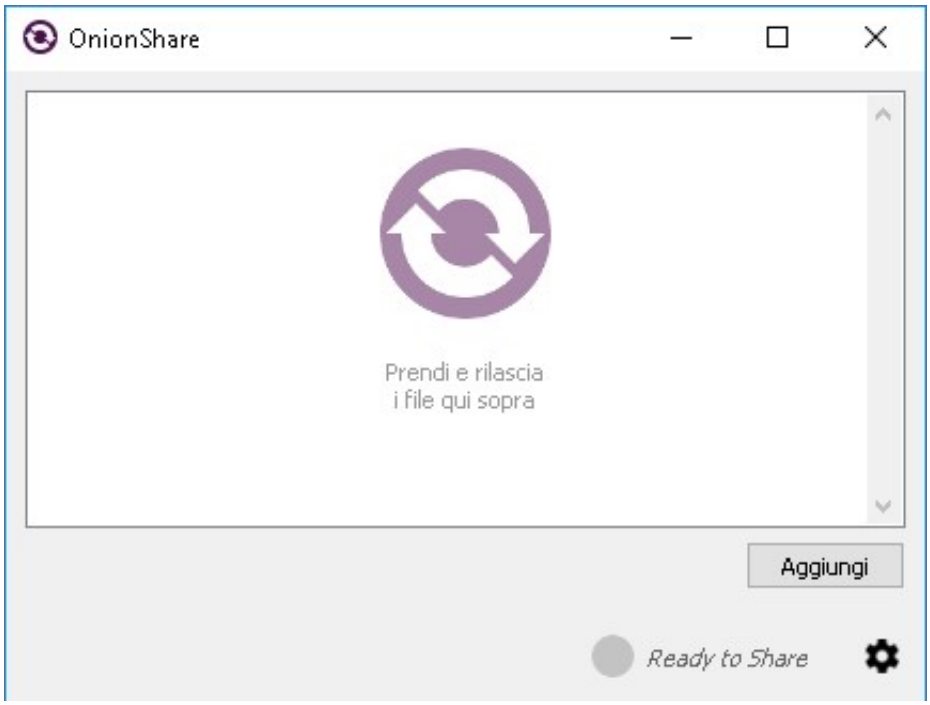


Per poter utilizzare OnionShare **è necessario essere collegati alla rete Tor** in quanto questa rappresenterà il canale di collegamento. Vedremo che ci saranno vari sistemi che questo strumento mette a disposizione per connettersi alla rete Tor. Quello scelto da noi è tramite il Tor Browser, quindi una volta scaricato e installato OnionShare, dovremo avviare il Tor Browser (supposto di averlo già presente sulla macchina) e lasciarlo aperto in background.

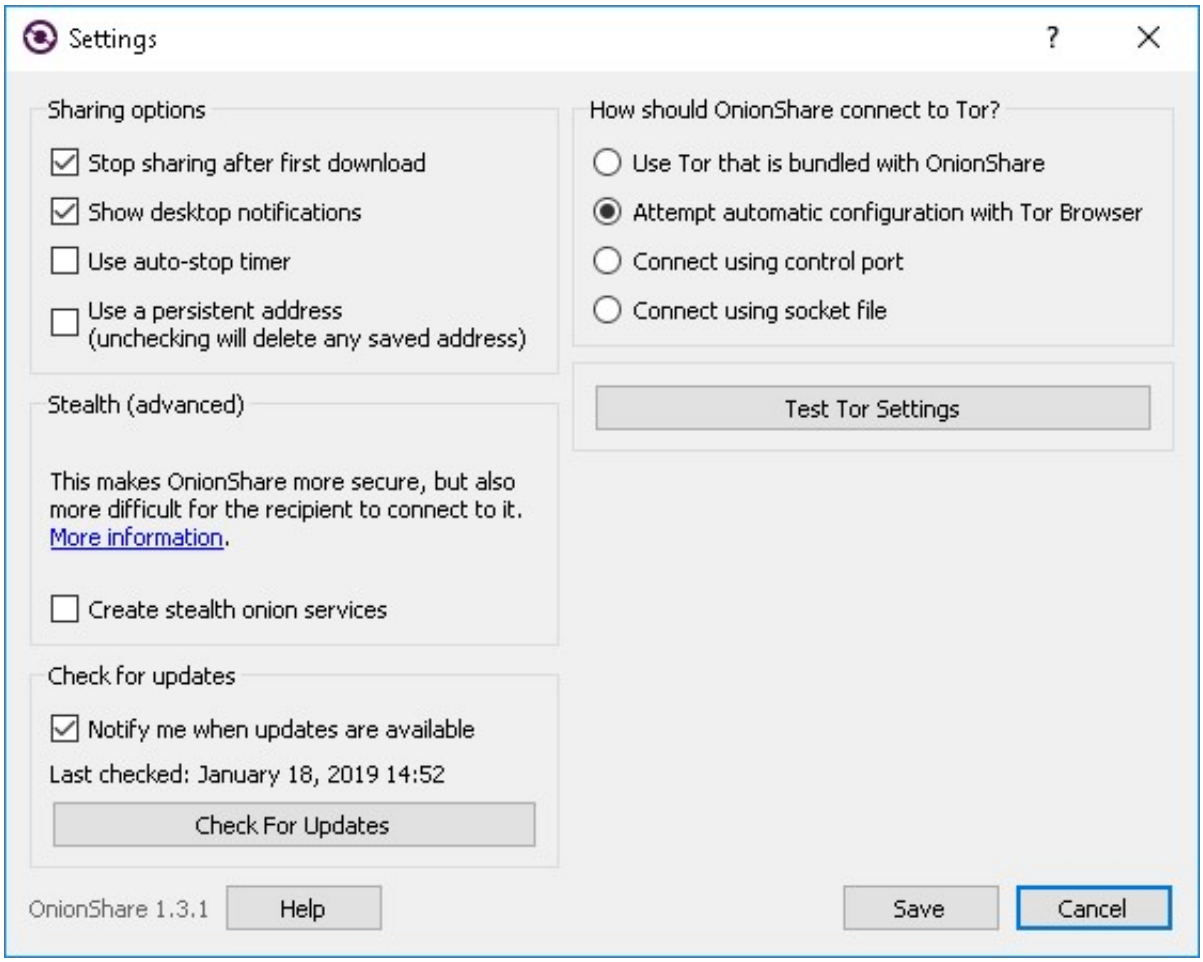
Se ci dimenticassimo di avviare il Tor Browser e provassimo ad aprire subito OnionShare, ci comparirebbe questo alert per ricordarcelo.



OnionShare, all'avvio, si presenterà come nell'immagine seguente (le maschere che si vedranno sono tratte da una installazione su Sistema Operativo Windows 10 e riguardano OnionShare versione 1.3.1).



Almeno la prima volta conviene aprire il pannello delle impostazioni premendo la rotellina in basso a destra in modo da configurare i parametri principali. Il pannello delle impostazioni appare come nell’immagine in basso.



Molte sono le impostazioni da poter regolare per ottimizzare il programma alle nostre esigenze.

Vediamo quali sono.

“**Stop Sharing After First Download**” Permette il download solo ad un utente, disabilitando la condivisione se un altro utente utilizza lo stesso link per scaricare. Ovviamente se vogliamo condividere il file a più utenti occorre disabilitare questo flag.

“**Show Desktop Notifications**” Fa comparire pop-up e notifiche sul computer quando un utente inizia, interrompe o completa un download.

“**Using the Auto Stop Timer**” Abilita una maschera nella finestra principale dell’applicazione dove è possibile impostare l’arresto della condivisione in base a data e ora. Per configurazioni particolari vedere l’OnionShare Wiki.

“**Use a Persistent address**” Di norma OnionShare fornisce un link da utilizzare per il download che vale solo una volta. Se si volesse riutilizzare il link per condivisioni successive occorre abilitare questo parametro. Questa impostazione è utile qualora si volesse organizzare una condivisione subito ma avviarla in data successiva, oppure se ci fossero problemi di connessione e poter continuare il download successivamente.

Deselezionando questo parametro si perderanno gli indirizzi persistenti eventualmente salvati in precedenza.
L'uso di questa impostazione salva la chiave privata nel file delle impostazioni di OnionShare. **Quindi attenzione a non smarrire tale file perché significherebbe permettere ad altri di accedere alla nostra condivisione.**

"**Create Stealth Onion Services**" Questa è una funzione che rende molto più sicuro OnionShare, ma anche molto più complesso il collegamento per chi dovrà ricevere il file. Normalmente, chiunque conosca il nostro indirizzo di condivisione Onion può collegarsi e quindi scaricare quanto stiamo pubblicando. **Ovviamente cercheremo di condividere tale indirizzo solo con chi è autorizzato a farlo**. Tuttavia, può succedere che nodi malevoli della rete Tor memorizzino il nostro indirizzo e provino a collegarsi ad esso così come un attaccante possa furtivamente venirne a conoscenza. Con la **procedura Stealth** invece, consigliata quando i file da trasferire sono davvero confidenziali, il ricevente dovrà inserire in un file di configurazione del proprio Tor Browser (nel file **torrc**) una determinata stringa che gli avremo fornito e in questo modo solo lui potrà scaricare il file anche se il link venisse a conoscenza di altri. Precise informazioni su come configurare questo servizio si possono trovare sulla pagina GitHub Wiki di Lee.

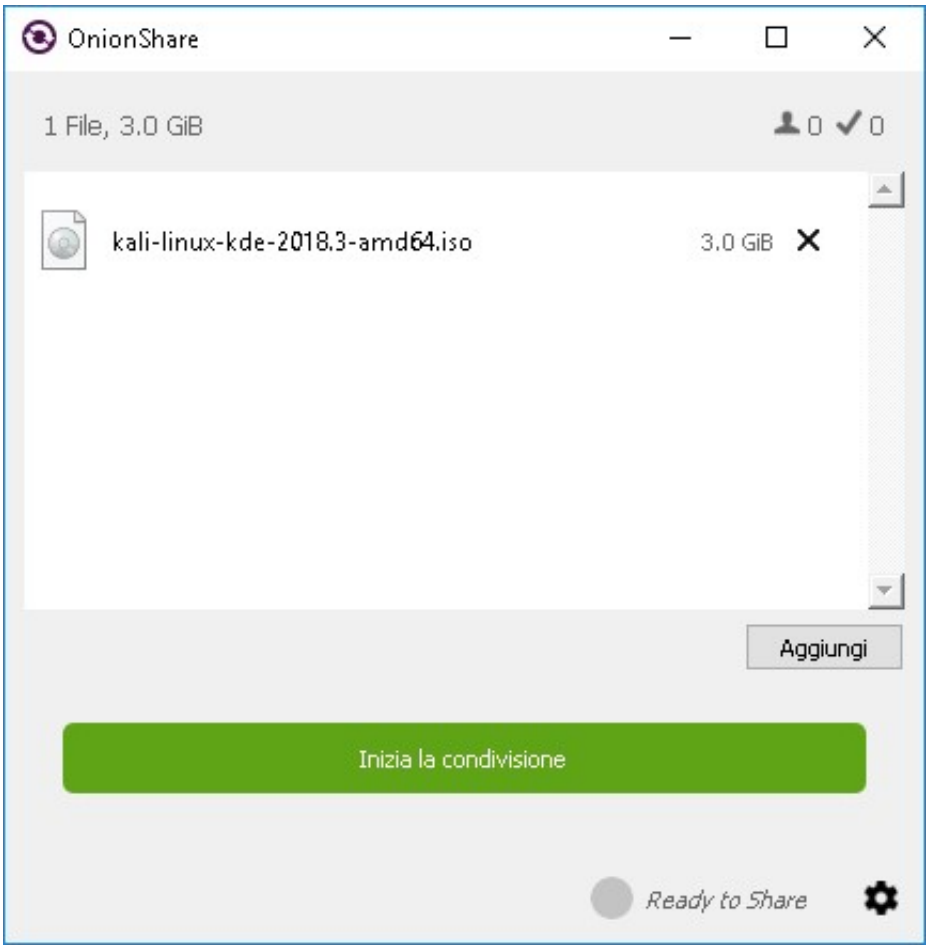
"**How Should Onionshare Connect to Tor?**" Qui è importante impostare come OnionShare si deve connettere alla rete Tor. Ricordiamo che è fondamentale essere connessi alla rete Tor perché il programma funzioni. Quattro sono le possibili scelte.

- Utilizzare il **servizo Tor che è incluso in OnionShare**. Questo è il modo predefinito e più semplice con cui OnionShare si connette a Tor. Aprendo OnionShare verrà avviato un processo Tor in background configurato appositamente per OnionShare. Sarà un processo indipendente da altri processi Tor presenti sul computer.
  Qualora per determinati motivi la connessione Tor non dovesse riuscire ci sarà la possibilità di impostare la modalità Bridges.

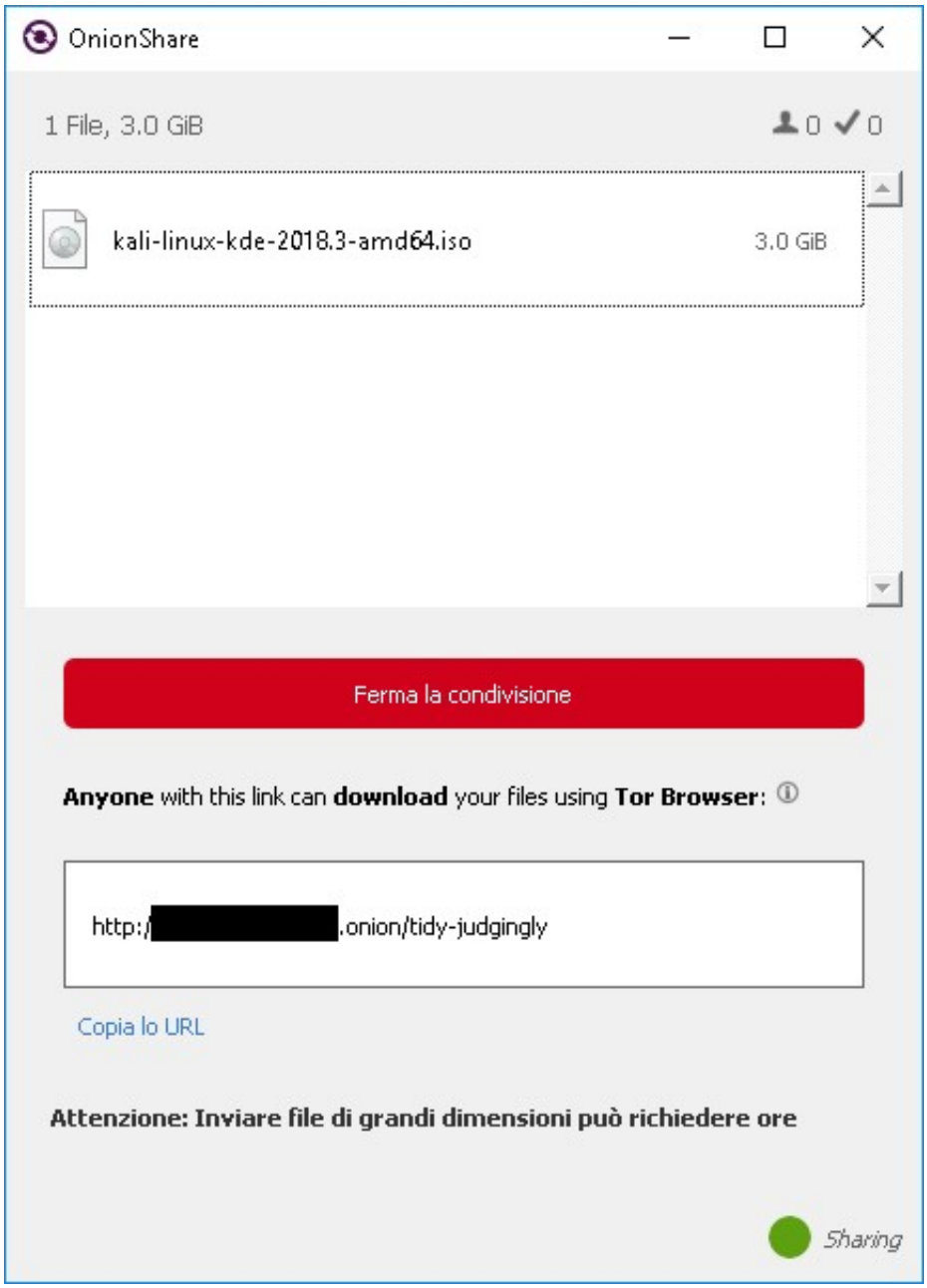
- Se abbiamo **Tor Browser installato sul computer** e vogliamo utilizzare questo per connetterci alla rete Tor basterà avviare Tor Browser prima di avviare OnionShare.
- Possiamo anche installare **Tor come servizio di sistema** e dire a OnionShare di connettersi a questo. Sarebbe anche possibile connettersi al servizio Tor presente su un sistema remoto. Sarà possibile quindi decidere se connettersi al servizio Tor utilizzando una "**control port**" o un "**socket file**". Per le configurazioni approfondite e per capire come installare Tor come servizio, l'OnionShare Wiki anche in questo caso sarà utilissimo.

Una volta che avremo configurato il programma e salvato le impostazioni, ci troveremo nuovamente sulla sua finestra principale e saremo pronti ad utilizzarlo. Nei passaggi seguenti vedremo il trasferimento di un grosso file (circa 3 Gb).

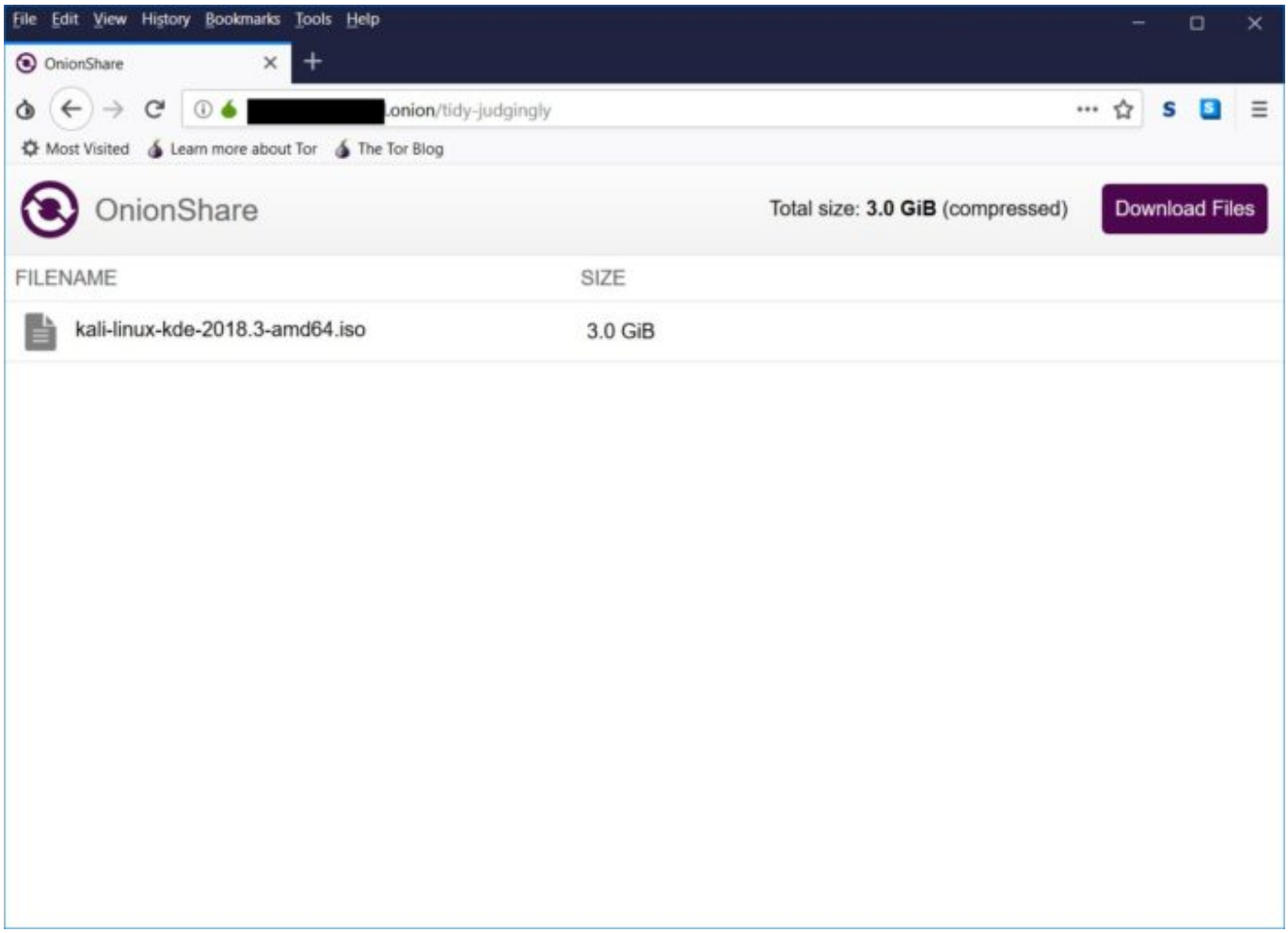
Il primo passo è quello di trascinare il file all'interno della maschera centrale di OnionShare oppure selezionarlo premendo il bottone "**Aggiungi**". Nel nostro esempio abbiamo aggiunto il file ISO di Kali Linux 2018.3 come si vede nell'immagine in basso.



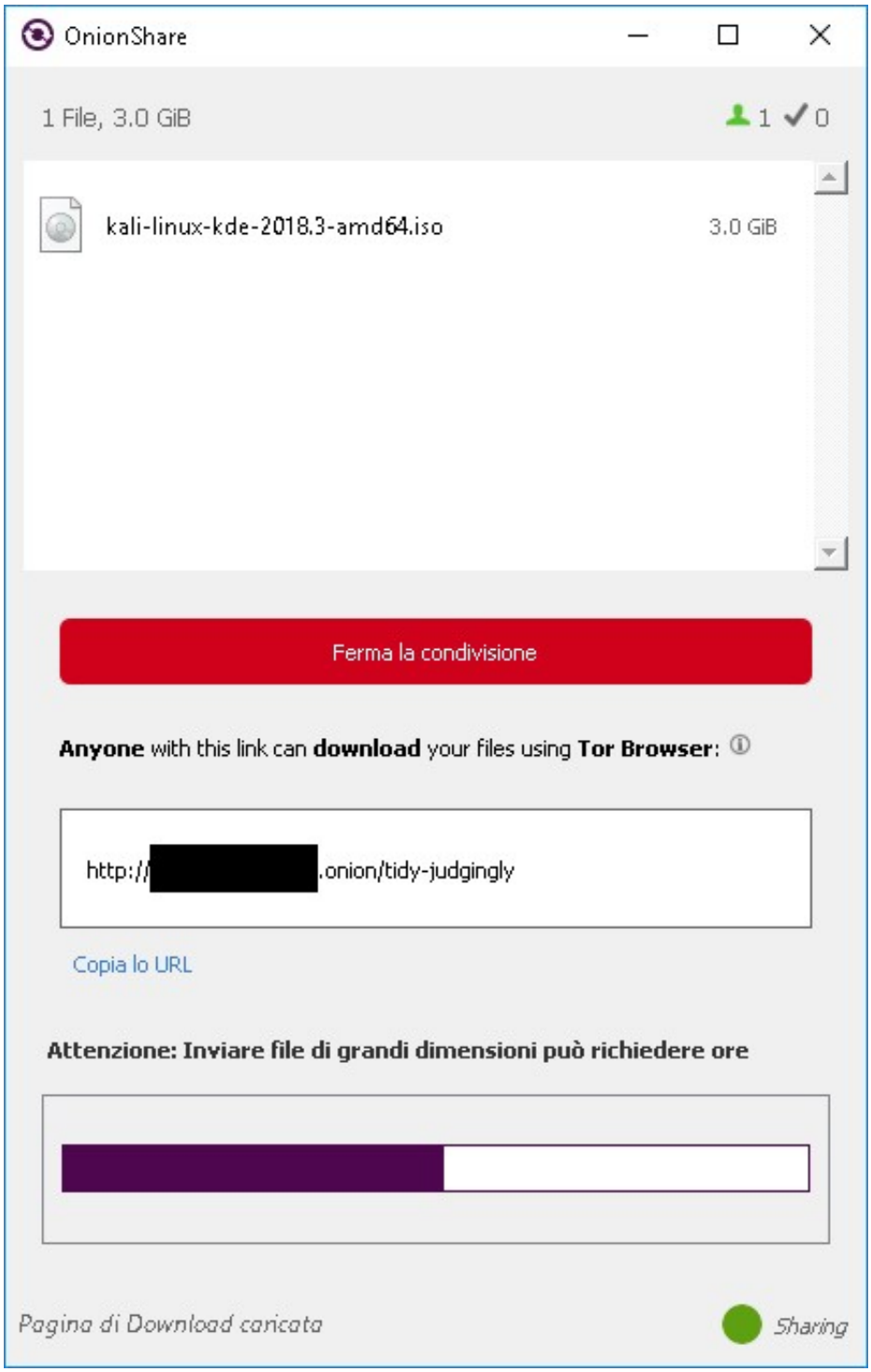
Ovviamente, anziché un file solo, avremmo potuto aggiungere più file utilizzando la stessa condivisione. A questo punto premiamo il grosso bottone verde che recita “**Inizia la condivisione**”. Dopo alcuni secondi, comparirà il link che dovremo fornire a chi dovrà ricevere il nostro file come vediamo nell’immagine seguente.



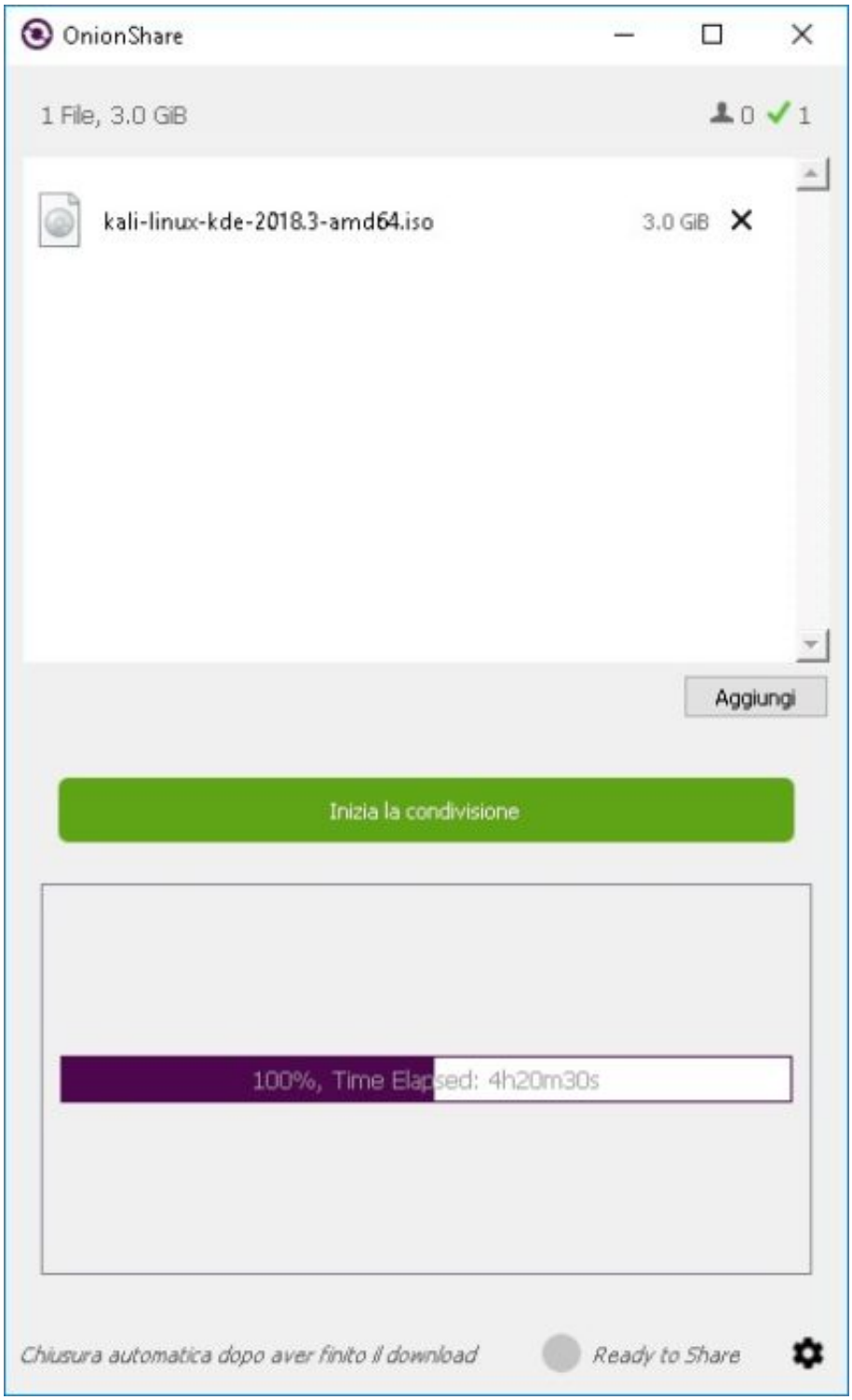
Il link fornito sarà costituito dal “**nome di dominio .onion / slug**” (dove slug sembrano essere parole generate automaticamente dalla pagina, leggibili dall’essere umano e che identificano la risorsa che si sta condividendo). Questo è il link che dovremo fornire al destinatario del file facendo attenzione, come è riportato sulla maschera del programma, che **chiunque conosca quell’indirizzo potrà fare il download del file**. **Pertanto sarà necessario comunicare questo indirizzo in modo sicuro**. Il destinatario del file quindi si collegherà attraverso il Tor Browser al link che ha ricevuto e visualizzerà quello che vogliamo trasferire.



Il destinatario non farà altro che premere “**Download Files**” per iniziare il trasferimento. Si tratta, come già detto, di una **connessione Peer-to-Peer**. Il tempo di trasferimento attraverso la rete Tor sarà ovviamente più lungo rispetto ad un download classico in quanto come sappiamo la rete Tor è costituita da molti nodi sui quali viene dirottato il traffico. **Quindi file di grosse dimensioni potrebbero impiegare molto ad essere trasferiti**. Nel nostro esempio per trasferire il file da 3 Gb abbiamo impiegato oltre quattro ore. Quando il destinatario premerà il bottone download, l’operazione verrà notificata al mittente il quale visualizzerà nella maschera del programma una barra di avanzamento del trasferimento.

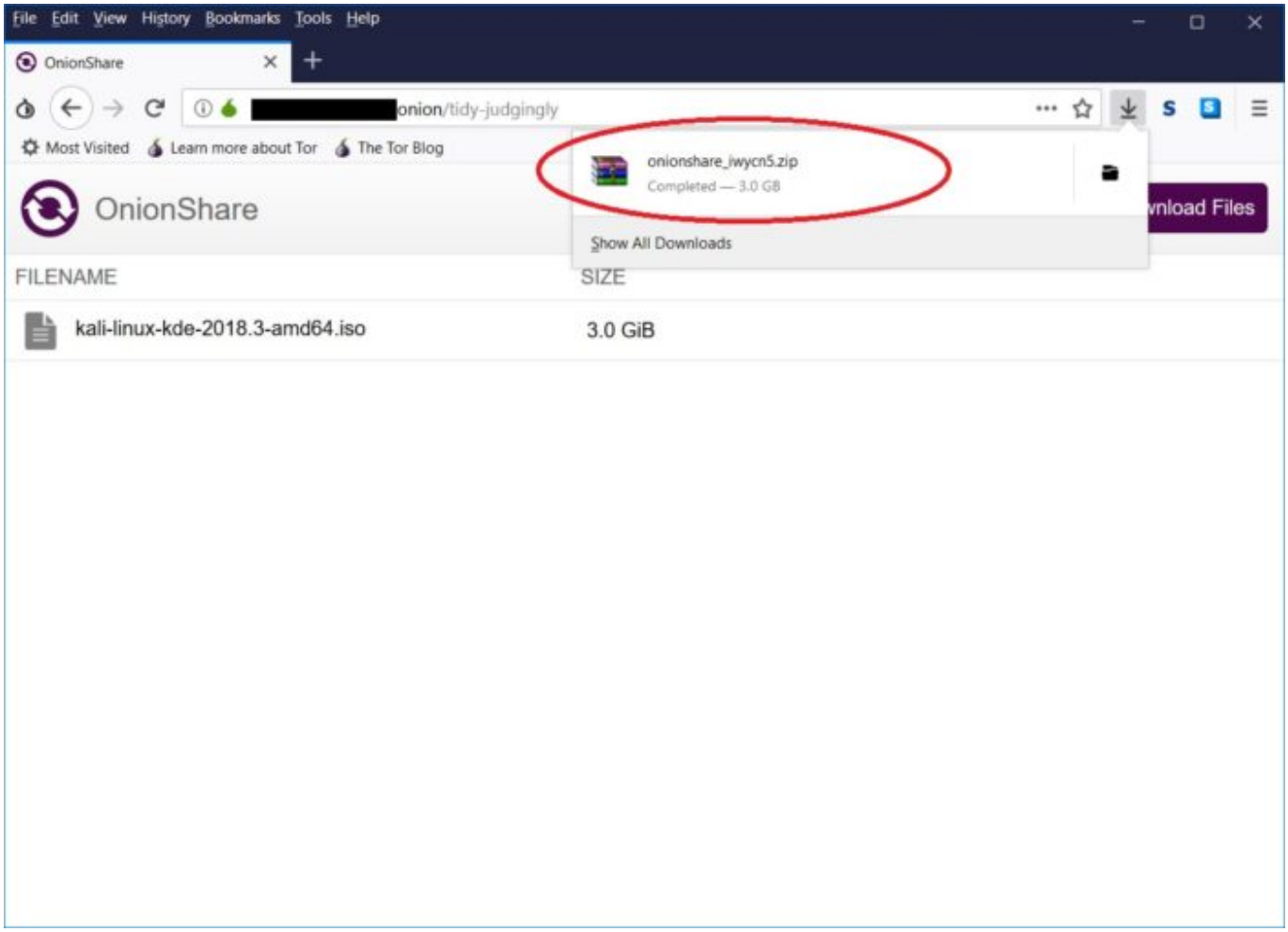


L’icona raffigurante un utente in alto indica il numero 1 perché un utente sta effettivamente scaricando il nostro file, mentre lo 0 sulla destra indica che nessun utente ha ancora completato il trasferimento. Quando il trasferimento sarà completato sulla maschera comparirà il 100% ed il tempo trascorso per scaricarlo tutto, come illustrato nell’immagine che segue.



OnionShare, ora che il trasferimento è terminato (la barra di avanzamento in questa versione non giunge fino alla fine), ha chiuso la condivisione perché nei parametri abbiamo lasciato il check su “**Stop Sharing After First Download**”. Essendoci stato già un download, il link che il programma ci aveva fornito non è più utilizzabile. Se volessimo trasferire nuovamente questo file dovremmo premere “**Inizia la condivisione**”, quindi OnionShare ci fornirebbe un nuovo link di condivisione.

Se ci spostiamo dal destinatario noteremo che questo non avrà ricevuto il file così come è stato condiviso (kali-linux-kde-2018.3-amd64.iso) perché, invece, è stato inserito durante il trasferimento in un archivio compresso .zip. Sia che si trasferiscano più file, sia che se ne trasferisca uno solo, il risultato sarà comunque un archivio compresso da OnionShare. Una volta scompattato l'archivio, il destinatario avrà esattamente quello che il mittente ha voluto trasmettergli e tutto è avvenuto in modo cifrato e anonimo.



In un mondo come quello attuale dove gravano su di noi forme diverse di sorveglianza di massa, conoscere un ulteriore strumento di difesa è importante. Ricordandoci però sempre che in internet, **non esiste garanzia di anonimato assoluto al 100%**. Molti sono i fattori che potrebbero inficiarlo, spesso causati dallo stesso utente.

Articolo a cura di **Antonio Sagliocca**