Istruzioni e consigli per l'uso di Tor Browser (aggiornamento del 5 giugno 2015)

Cari compagni e sinceri democratici,

queste istruzioni hanno lo scopo di permettervi di non essere individuati quando operate su internet.

TOR permette di non essere individuati quando scambiate messaggi con altre persone: con la riserva che l'anonimato è garantito completamente solo se anche l'altra persona usa TOR. Prima di usare TOR dovete aver ben chiaro che siete anonimi nel senso che se inviate un messaggio chi spia non è in grado di sapere da dove parte e chi lo invia, ma se il messaggio non è criptato il suo contenuto è leggibile dagli spioni. Quindi è necessario imparare anche l'uso del sistema di criptazione PGP: sul sito del (n)PCI al link: http://www.nuovopci.it/corrisp/risp03.html trovate il manuale con istruzioni e consigli per l'uso del PGP.

Delle istruzioni che seguono, le cose importanti sono i consigli sull'uso di TOR. Una volta installato, il suo uso è semplice, ma solo seguendo i consigli qui dati evitate di rivelare la vostra identità.

Voler migliorare la società, cambiare lo stato delle cose è illegale per chi detiene il potere nelle cosiddette "democrazie occidentali". Quindi armatevi degli strumenti tecnici adatti a cambiare lo stato attuale delle cose.

Le istruzioni sono divise in capitoli. All'interno di ogni capitolo abbiamo numerato le istruzioni: questo perché ogni eventuale nostro corrispondente che ha osservazioni da fare su qualche istruzione, possa indicare facilmente a quale si riferisce.

INDICE

1. Procurarsi il programma per l'installazione di Tor Browser ____ **p. 1**

2. Installazione ____ **p. 2**

3. Perché siete anonimi ____ **p. 7**

4. Consigli per la navigazione anonima ____ **p. 7**

5. La posta anonima con TOR ____ **p. 9**

6. Usate un antivirus e aggiornate regolarmente Windows ____ **p. 10**

7. Ricordatevi che TOR protegge il vostro anonimato, non le informazioni che inviate ____ **p. 10**

8. Aggiornamento automatico di Tor Browser ____ **p. 10**

1. Procurarsi il programma per l'installazione di Tor Browser

1. All'indirizzo internet che segue trovate il programma per installare Tor Browser**(1)** per Windows.
   https://www.torproject.org/download/download-easy.html.en

(1) Tor Browser è un programma che integra Firefox e TOR e non ha bisogno di nessun altro programma accessorio per funzionare, né di impostazioni da parte di chi lo utilizza. Naturalmente TOR funziona anche su altri sistemi operativi (Mac OS e Linux).

2. Nella pagina che vi si presenta (come mostra la figura che segue) fate click sul tasto viola DOWNLOAD Tor Browser

Registrate il file **torbrowser-install-4.5.1_en-US.exe** (questa è la versione 4.5.1 in inglese di Tor Browser ed è l'ultimo aggiornamento nel momento in cui redigiamo queste istruzioni)

Nel manuale le indicazioni si riferiscono alla versione inglese, quindi vi consigliamo di scaricare la versione inglese impostando English nel campo di testo sotto il bottone viola.

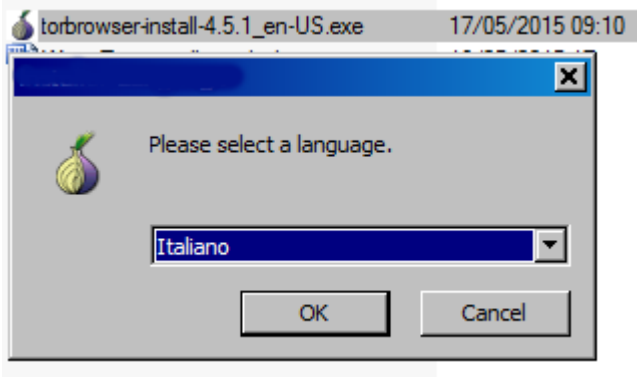
Se scaricate la versione italiana, considerate che i menu e le voci nei menu conservano la stessa posizione che hanno in quella inglese: non vi sarà quindi difficile capire a quale voce e menu ci riferiamo.

Noi usiamo la versione inglese e ne consigliamo l'uso perché, data la sua diffusione, garantisce meglio l'anonimato. Inoltre per chi volesse approfondire la conoscenza di TOR, offre maggiori possibilità.

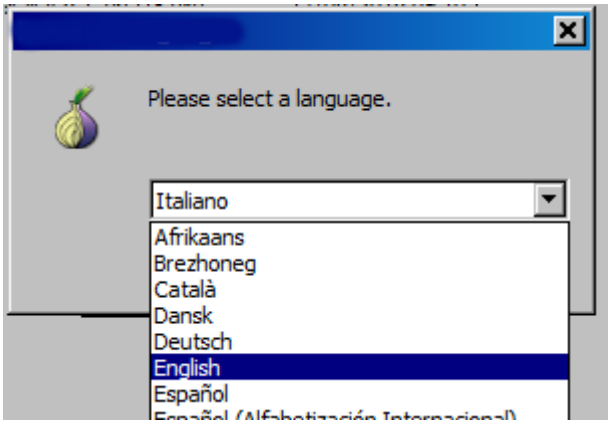
In questo breve manuale raccogliamo le informazioni minime indispensabili per iniziare a far funzionare TOR per la navigazione anonima su internet.

2. Installazione di Tor Browser

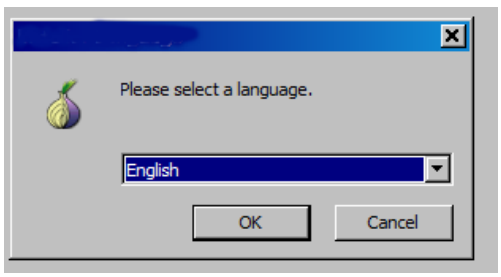
1. Avviate il programma "**torbrowser-install-4.5.1_en-US.exe**". Vi si presenta la finestra mostrata nella figura che segue.



2. Selezionate l'inglese: vi ricordiamo che in queste istruzioni ci riferiamo alla versione inglese dei menu.
   Per selezionare una lingua differente, fate click sul triangolino che punta verso il basso a destra del campo di testo che indica la lingua. Si apre la lista delle lingue disponibile, selezionate English (vedi figura che segue) .



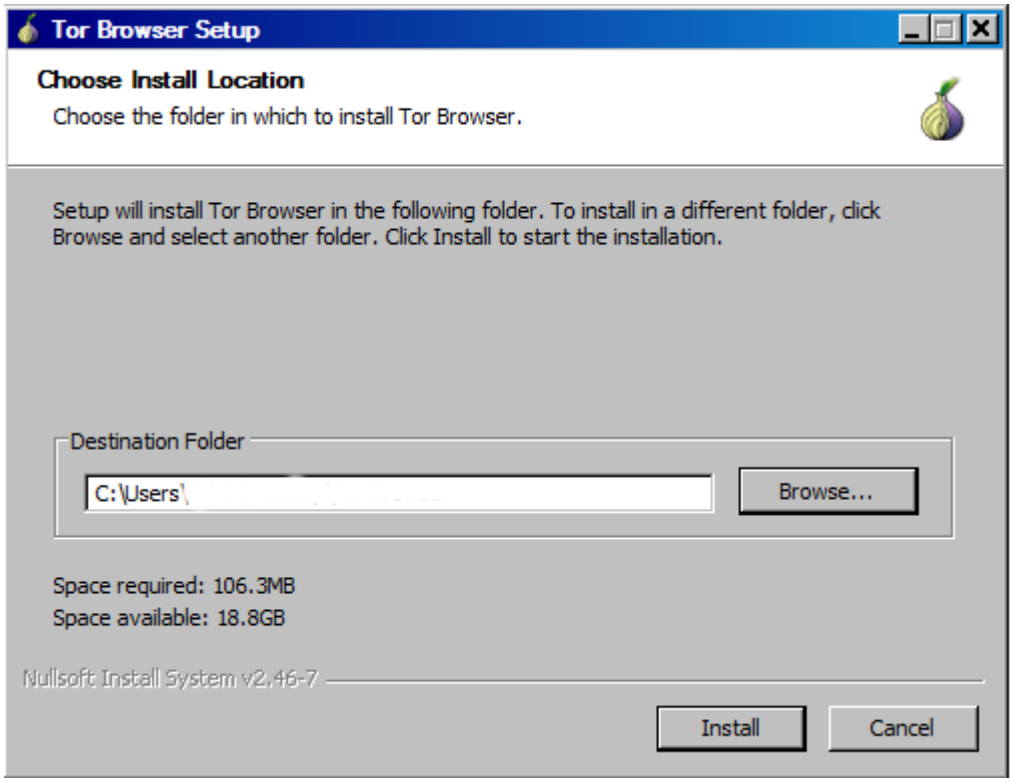
3. A questo punto la lingua selezionata è "English" (vedi figura che segue). Fate click sul tasto "OK" per avviare l'installazione.



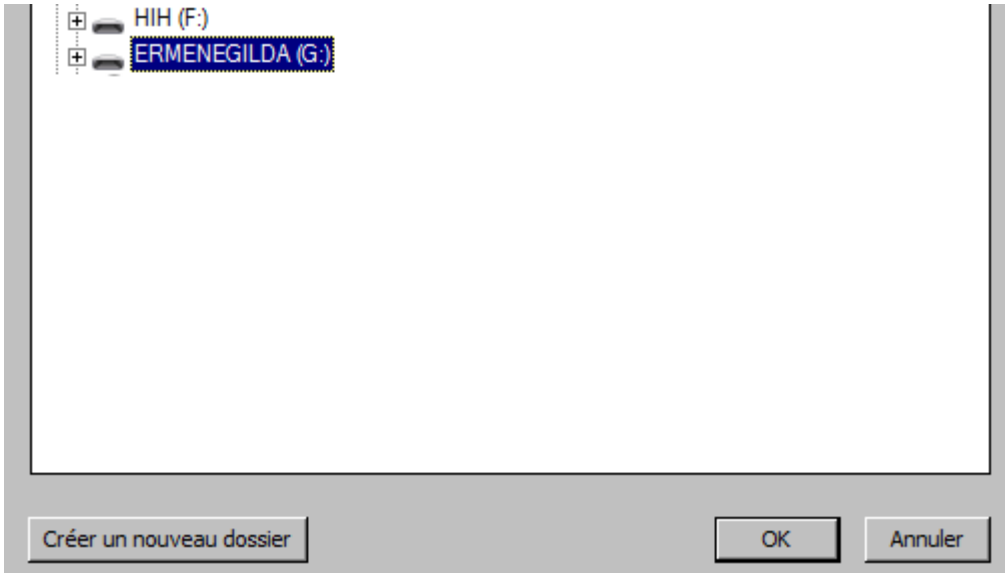
4. A questo punto si apre la finestra che vi permette di scegliere dove installare Tor Browser.

   Di seguito indichiamo al programma di installazione per mettere Tor Browser su una chiavetta USB, quindi se non l'avete già fatto inserite una chiavetta USB nel vostro computer.

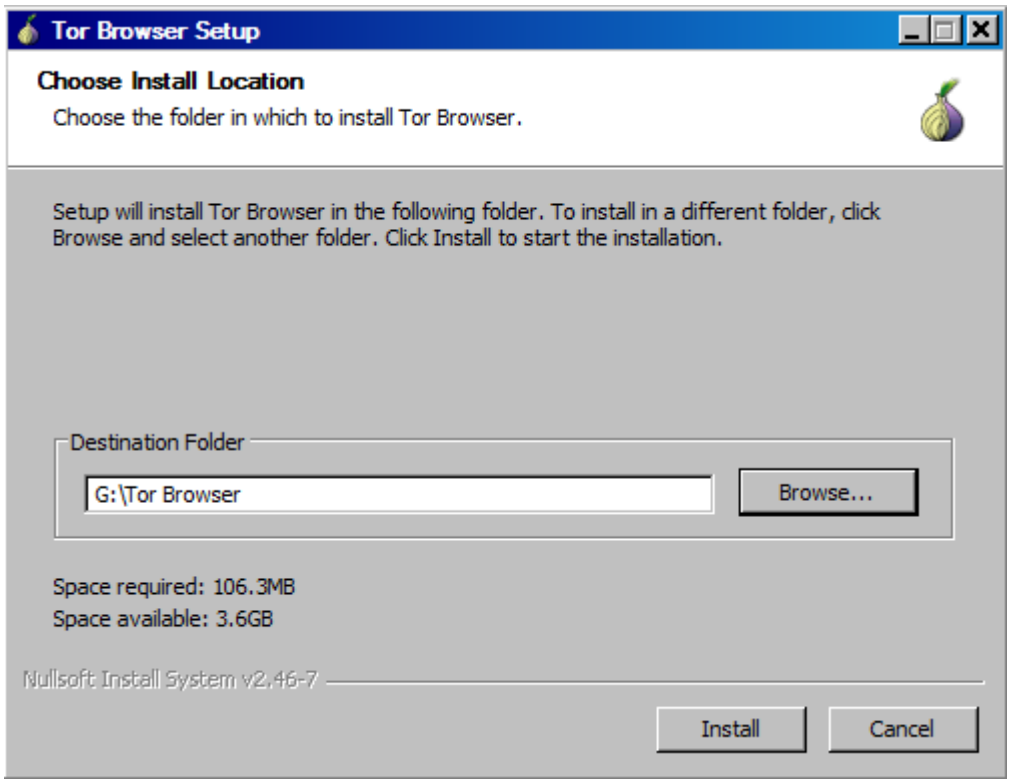
   Per scegliere la chiavetta USB su cui installare Tor Browser fate click sul bottone "Browse..." (vedi figura che segue).



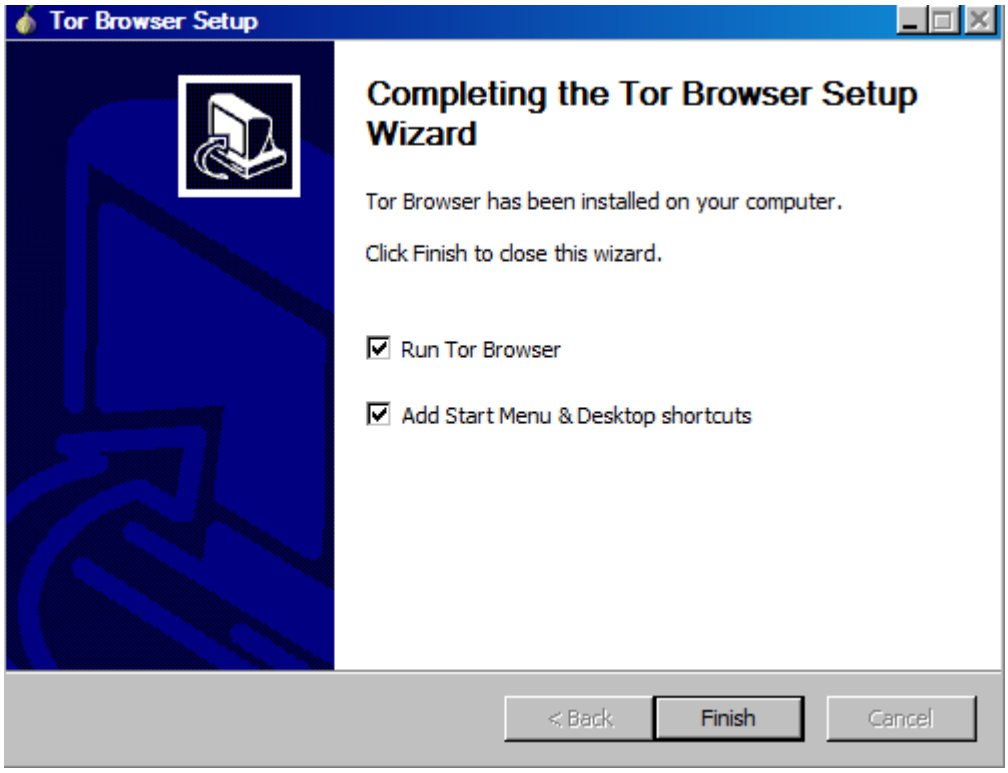
5. Si apre la finestra dove appaiono i dischi e le chiavette USB inseriti nel computer. Selezionate la chiavetta USB: nell'esempio si chiama "ERMENEGILDA" (vedi figura che segue).



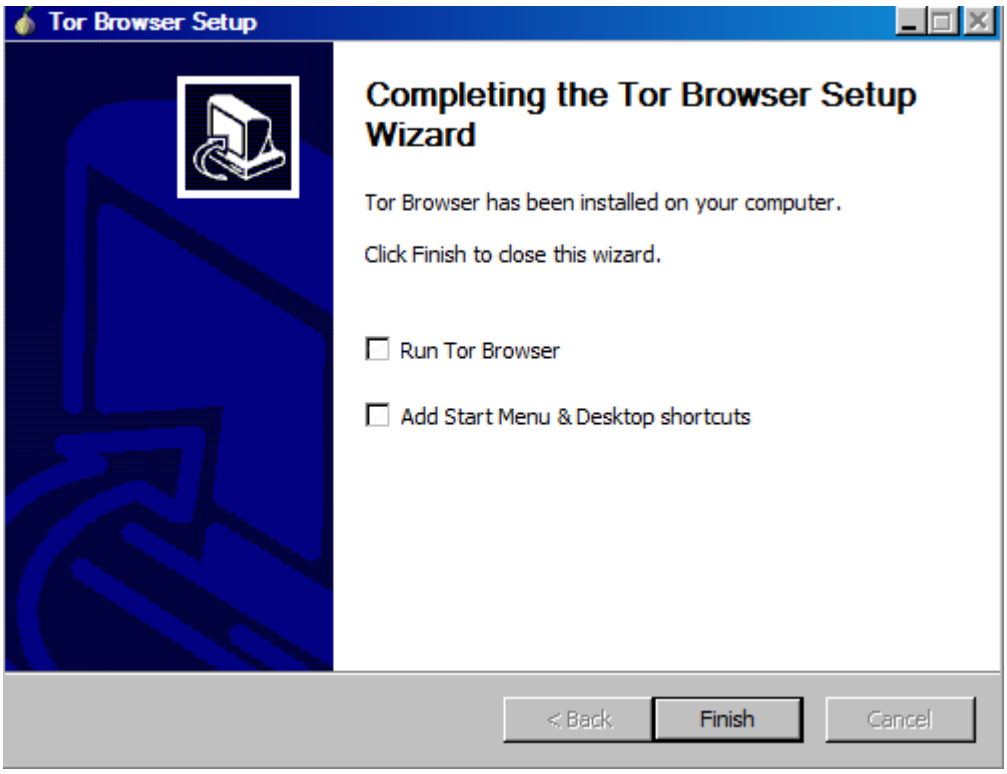
   Fate click su **OK**.



6. Ora nel campo “Destination Folder” (figura precedente) è selezionata la chiavetta USB. Fate click sul bottone “Install”. Alla fine dell’installazione sulla chiavetta “ERMENEGILDA” viene creata la cartella “Tor Browser” che conterrà il programma Tor Browser. La figura che segue mostra la finestra che appare alla fine dell’installazione.



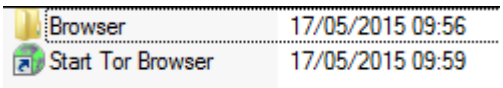
7. Deselezionate le due voci “Run Tor Browers” e “Add Start Menu & Desktop shortcuts”. La figura che segue mostra la finestra con le due voci deselezionate.



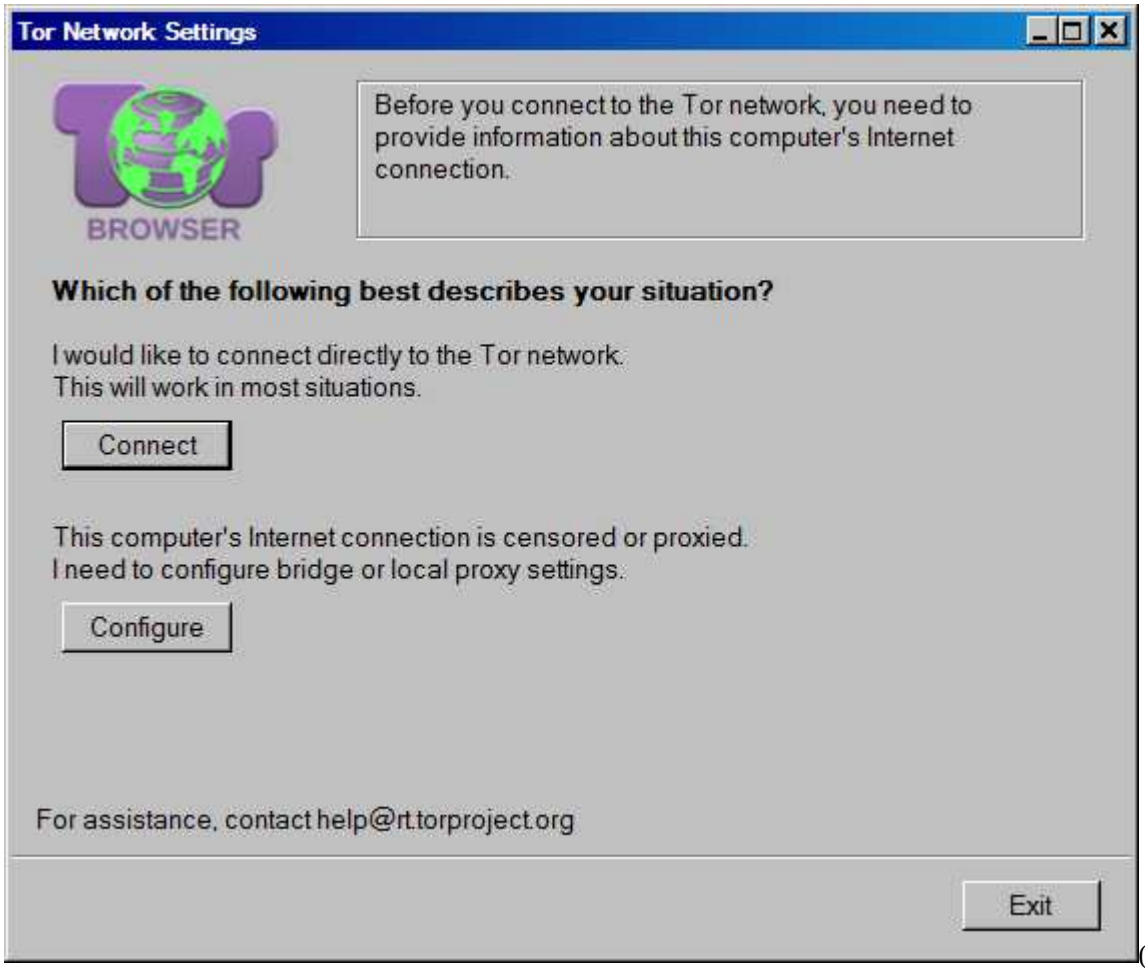
8. Fate click sul bottone “Finish”.
   L’installazione è terminata, ma prima di continuare una parentesi per spiegare perché diciamo di installare Tor Browser su una chiavetta USB.
   Il primo vantaggio è che Tor Browser sulla chiavetta non lascia traccia della sua presenza sul vostro computer. Secondo vantaggio, potete usare Tor Browser su qualsiasi altro computer Windows senza dover effettuare di nuovo l’installazione: basta introdurre la chiavetta USB in un altro computer e avviare Tor Browser dalla chiavetta.
   Questo è possibile perché il tipo di installazione eseguita è detta in gergo informatico “portable”. In pratica si tratta di un programma autosufficiente che non ha bisogno di appoggiarsi al sistema operativo di un computer specifico.

9. Per avviare Tor Browser aprite la chiavetta USB: troverete la cartella “Tor Browser”.

10. Aprite la cartella “Tor Browser”: al suo interno c’è l’icona con il “globo terrestre” (Start Tor Browser) che serve ad avviare Tor Browser (vedi figura che segue).

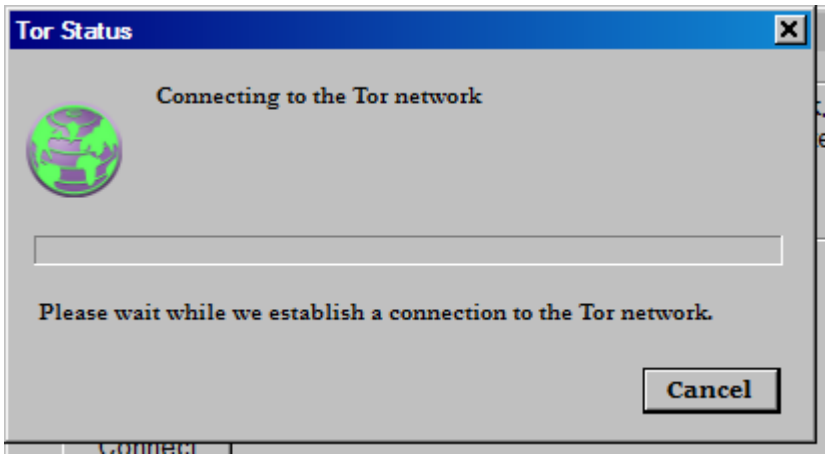


11. Facendo due click veloci si apre la finestre mostrata nella figura che segue.

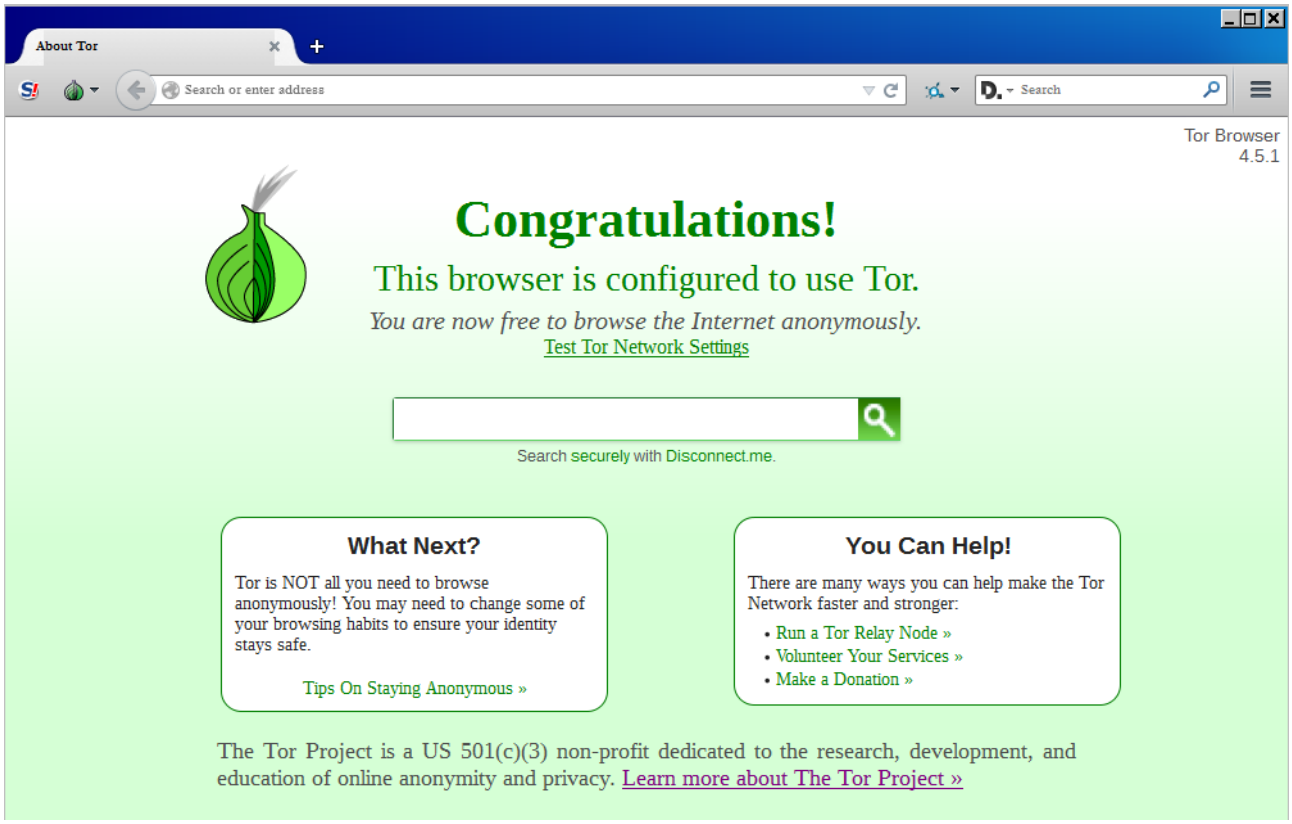


(*Figura A*)

12. Questa finestra (*Figura A*) vi appare solo la prima volta che avviate Tor Browser. La rivedrete eventualmente dopo che il programma Tor Browser si è interrotto in modo non corretto oppure nel caso non ci sia la connessione con la rete. Fate click sul bottone "Connect", vi appare la finestra mostrata nella figura che segue.



13. La prima volta è necessario aspettare alcuni minuti. Può capitare che non si avvii del tutto: in quel caso fate click su bottone "Cancel" e poi "Exit" dalla finestra mostrata nella *Figura A* e riavviate Tor Browser come sopra descritto. Quando la connessione è stabilita, viene avviato automaticamente Firefox. Si avvia mostrando la pagina di conferma della corretta configurazione per la navigazione in modo anonimo come mostrato nella figura che segue.



14. **A questo punto potete iniziare a navigare su internet.**

3. Perché siete anonimi

1. **Vi domanderete perché adesso che uso TOR sono anonimo. Lo siete perché tra il sito che visitate e il vostro computer si inserisce la rete TOR.** L'indirizzo IP**(2)** che è quello che vi identifica quando vi connettete a internet serve a collegarsi ad un computer della rete TOR, poi le informazioni viaggiano in modo criptato tra i computer della rete ed alla fine giungono al sito che volete consultare attraverso l'ultimo computer della catena della rete TOR. Quindi venite identificati con l'IP di quest'ultimo computer. Inoltre i dati scambiati tra voi e la rete TOR e tra computer e computer delle rete TOR sono criptati con il metodo PGP**(3)** in modo da rendere impossibile risalire al vostro indirizzo IP. Solo l'ultimo computer decripta i comandi e i dati che inviate al sito che state consultando.

4. Consigli per la navigazione anonima

1. **Prima di tutto un serie di avvertenze importanti.**

   Non dovete mai aggiungere estensioni e plug-in a Firefox. Se lo fate perdete l'anonimato.

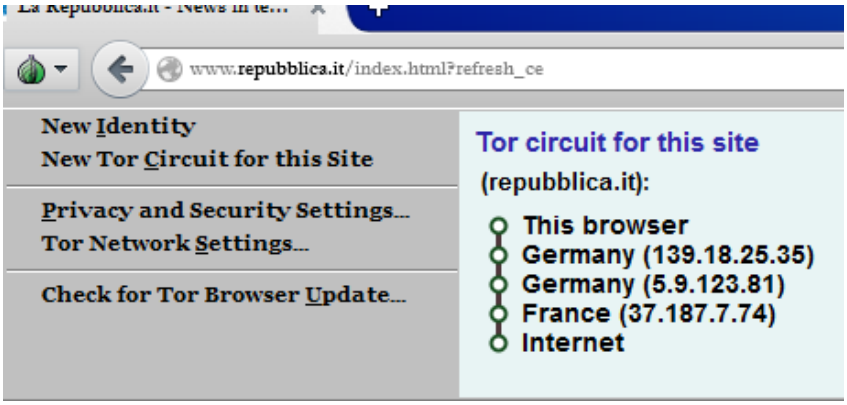
   Non dovete mai riempire moduli o richieste che contengano dati che si riferiscono a voi (lapalissiano, ma meglio ricordarselo).

M1. - **Non dovete mai fare il copia e incolla da Firefox a Word o Open Office** perché questi programmi quando ricevono i dati con il copia e incolla si collegano direttamente con internet per recuperarli **e lo fanno senza usare TOR**. Se vi interessa un testo di una pagina internet, usate dal menu "File" la voce "Save Page As..." di Tor Browser. Quando si apre la finestra per indicare dove salvare il file, in basso nel campo "Type" impostate "Web Page Complete...". Il recupero dei dati avverrà esclusivamente via la rete di TOR. Salvate la pagina che vi interessa su una chiavetta USB. In

seguito e **solo dopo essersi scollegati da internet,** potrete aprire la pagina salvata e recuperare testo e immagini facendo il copia e incolla o aprendo il file direttamente con Open Office o Word. **Notate Bene** che se siete inavvertitamente collegati ad internet e schiacciate un link presente nella pagina aperta con Word o Open Office, avviate la navigazione verso questo link attraverso il navigatore impostato come standard su Windows, cioè **senza l'anonimato garantito da Tor Browser**!

2. Per proteggere la vostra privacy, Tor Browser vi permette di **variare a piacimento il vostro indirizzo IP(2)**. Lo potete fare durante la sessione di navigazione attraverso le funzioni di TOR accessibili dall'icona a forma di cipolla in alto a sinistra (vedi figura che segue).

3. Per evitare di dare informazioni su di voi, cambiate il vostro IP. Quando ad esempio dovete consultare due webmail cambiate il vostro IP altrimenti qualcuno potrebbe dedurre un collegamento tra di esse e ricostruire la rete dei vostri contatti. Cambiate dunque l'IP dopo aver consultato la prima email facendo click sul simbolo della cipolla verde. Dal menu che appare (vedi figura che segue) selezionate la voce "New Identity". Firefox si chiude e si riapre ripulito di tutti i dati di navigazione precedenti: adesso potete consultare la seconda webmail.



4. Un altra voce utile in questo menu è "New Tor Circuit for this Site". Questa funzione torna utile anche quando un sito non viene visualizzato: cambiando l'IP a volte si ristabilisce il corretto funzionamento del sito da consultare.
   Per ritentare un collegamento recalcitrante, fate click sul simbolo della cipolla verde. Vi appare un menu (vedi figura precedente). Fate click sulla voce "New Tor Circuit for this Site". L'IP cambia e la pagina si riapre. A volte questa voce rimane inattiva. Vuol dire che TOR non ha ancora creato una nuova connessione con il sito. Normalmente dopo alcune decine di secondi questa voce diviene nuovamente attiva e potete di nuovo cambiare il vostro IP.

(2) L'indirizzo IP è un numero che viene assegnato ad ogni utente di internet e permette di identificarlo geograficamente. TOR si inserisce tra la vostra connessione e quella del sito finale: l'IP che vene riconosciuto dal sito consultato è differente dal vostro, inoltre i dati scambiati tra voi e la rete TOR sono criptati, in modo da rendere impossibile risalire al vostro indirizzo IP

5. Attenzione! La navigazione con TOR è lenta, a volte lentissima. Non cercate di vedere filmati in diretta. Questa è una caratteristica della navigazione a cui vi dovrete abituare. Se inviate una email con un allegato molto grande, dovete avere pazienza. A volte vi sembrerà che il sistema si è incastrato.

Se l'operazione è bloccata, un sistema per sbloccarla consiste nel cambiare l'IP come sopra descritto. Un altro più drastico è terminare la sessione, selezionando la voce "New Identity" dal menu della cipolla verde (vedi figura precedente).

M2. - Nota importante per la sicurezza dei dati:

Per non lasciare traccia dei vostri dati, dopo aver criptato o trasferito con l'operazione copia e incolla in un posto sicuro i dati da archiviare, usate **Eraser(*)** per cancellare in modo definitivo i vostri file riservati rimasti sul computer. Solo con questo programma di cancellazione definitiva ogni traccia del vostro lavoro viene effettivamente cancellata.

Non dovete mai buttare nel cestino i file, altrimenti possono essere recuperati da virus, troiani e spioni. Cancellateli in modo definitivo con Eraser.

Non dovete mai fare operazioni di taglia / incolla da un disco (o chiavetta) a un'altro, perché il file originale viene messo nel cestino e non può più essere cancellato con Eraser. **Fate copia / incolla** del file su un altro supporto (chiavetta, disco esterno, ecc.) e poi cancellate con Eraser il file che è rimasto sul computer.

(*) Eraser è reperibile alla pagina internet:
http://eraser.heidi.ie/download.php

5. La posta anonima con TOR

1. Per l'invio e la ricezione della posta in modo anonimo con Tor Browser non si possono usare programmi tipo Outlook. Bisogna imperativamente usare le Webmail, cioè caselle email consultabili attraverso il navigatore Tor Browser. Naturalmente bisogna creare una casella nuova e non riconducibile a voi.
   Il principale problema che vi si presenterà sarà dato dal fatto che i principali provider di posta elettronica chiedono al momento dell'attivazione della casella un numero di cellulare, quindi provider tipo Yahoo, Google ecc. non possono essere utilizzati a questo scopo. Altri invece riconoscono che usate TOR e non permettono l'apertura di un email.
   Nel momento in cui scriviamo il migliore sistema per creare una casella email è disponibile sul sito di autistici.org al seguente link: https://www.autistici.org/services/
   Informazioni sul altri siti che offrono la possibilità di aprire in modo anonimo le webmail si trovano ai seguenti indirizzi:
   http://www.hacker10.com/category/internet-anonymity/
   http://www.hacker10.com/internet-anonymity/list-of-the-best-tor-email-hidden-services/
   http://mail2tor2zyjdctd.onion/register.php (qui potete aprire istantaneamente una email, testato il 21 maggio 2015)

2. Dopo aver aperto un email anonima, la potete usare per aprirne altre su siti tipo www.riseup.net o protonmail.ch che garantiscono l'anonimato, ma richiedono un email per inviarvi l'avviso di attivazione.

3. **ATTENZIONE - Basta una sola sessione di consultazione di una email senza l'uso di TOR per lasciare una traccia della vostra identità!**

4. **Un sistema alternativo alle email per la comunicazione anonima è we.riseup.net**
   Non è una casella email, è un spazio internet dove si depositano i documenti. Naturalmente li dovete criptare**(3)** prima di depositarli se volete salvare baracca e burattini. I corrispondenti devono controllare regolarmente il vostro spazio e ritirare il documento depositato. L'apertura dello spazio è immediata, nessuna necessità di dati.

Per aprire lo spazio su we.riseup.net, il modulo da compilare si trova all'indirizzo:

https://we.riseup.net/account/new .

NMB (Nota molto bene): l'email richiesta nel modulo è facoltativa, non occorre indicarla. Appena compilato il modulo lo spazio di scambio è subito disponibile.

(3) Per criptare i documenti dovete usare il sistema **PGP**. Per windows il programma lo trovate al seguente indirizzo:
http://www.gpg4win.org/download.html
Il manuale per il suo uso lo trovate al seguente indirizzo:
http://www.nuovopci.it/corrisp/risp03.html

6. Usate un antivirus e aggiornate regolarmente Windows

1. **È assolutamente necessario avere sempre un antivirus aggiornato**. Un antivirus gratuito ed efficace lo trovate al seguente indirizzo internet:

   https://www.avast.com/it-it/index
2. **Dovete eseguire regolarmente l'aggiornamento di Windows** perché gli spioni approfittano delle falle di sicurezza. Se non aggiornate Windows stendete un tappeto rosso a tutti gli spioni e le polizie!!!

7. Ricordatevi che TOR protegge il vostro anonimato, non le informazioni che inviate

1. ***Attenzione!*** Il sistema TOR protegge l'identità di chi invia o riceve un'informazione, ma non le informazioni che vengono inviate. Chi spia può intercettare il vostro messaggio. Se inviate: "L'assalto al Palazzo d'Inverno è domani alle 12.30", non aspettatevi nulla di buono. L'esempio è volutamente imbecille, proprio per non farvi scordare questa caratteristica di TOR e perché dovete imparare ad usare il sistema PGP**(3)** per criptare i dati da inviare.

Buon lavoro compagni e sinceri democratici!

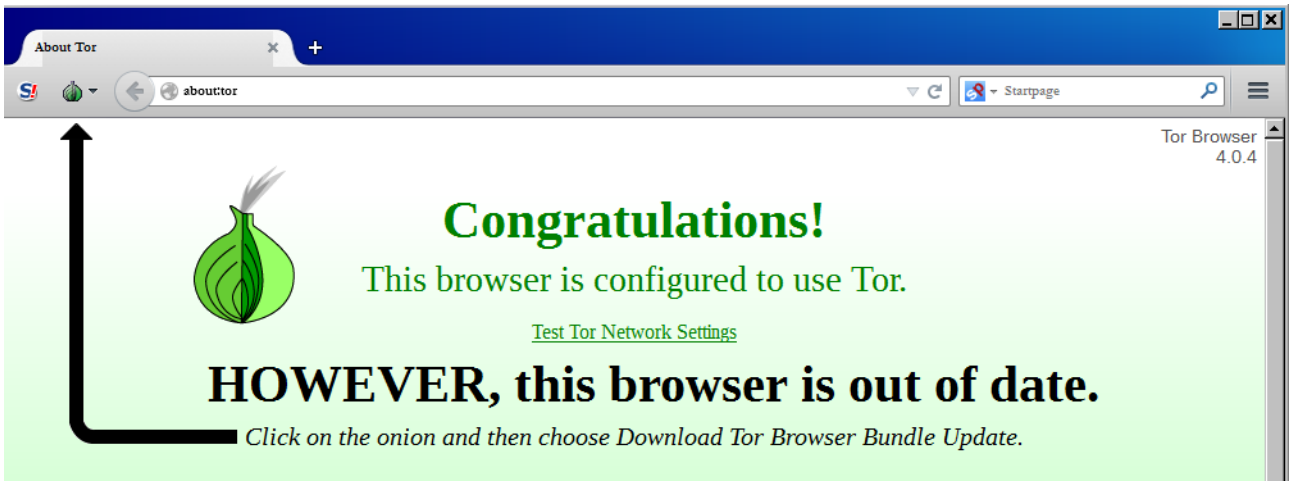
8. Aggiornamento automatico di Tor Browser

1. Dalla versione 4.0.3 e superiori di Tor Browser è stato introdotto l'aggiornamento automatico del programma.

   È necessario usare sempre la versione più aggiornata di Tor Browser: in ogni aggiornamento sono migliorate le difese contro gli spioni ed eliminati i difetti che possono compromettere l'anonimato.

   Qui di seguito spieghiamo come dovete fare per aggiornare in modo automatico Tor Browser.

   Se all'avvio di Tor Browser la prima finestra mostrata si presenta come nella figura che segue, vuol dire che è disponibile una versione più aggiornata di Tor Browser.

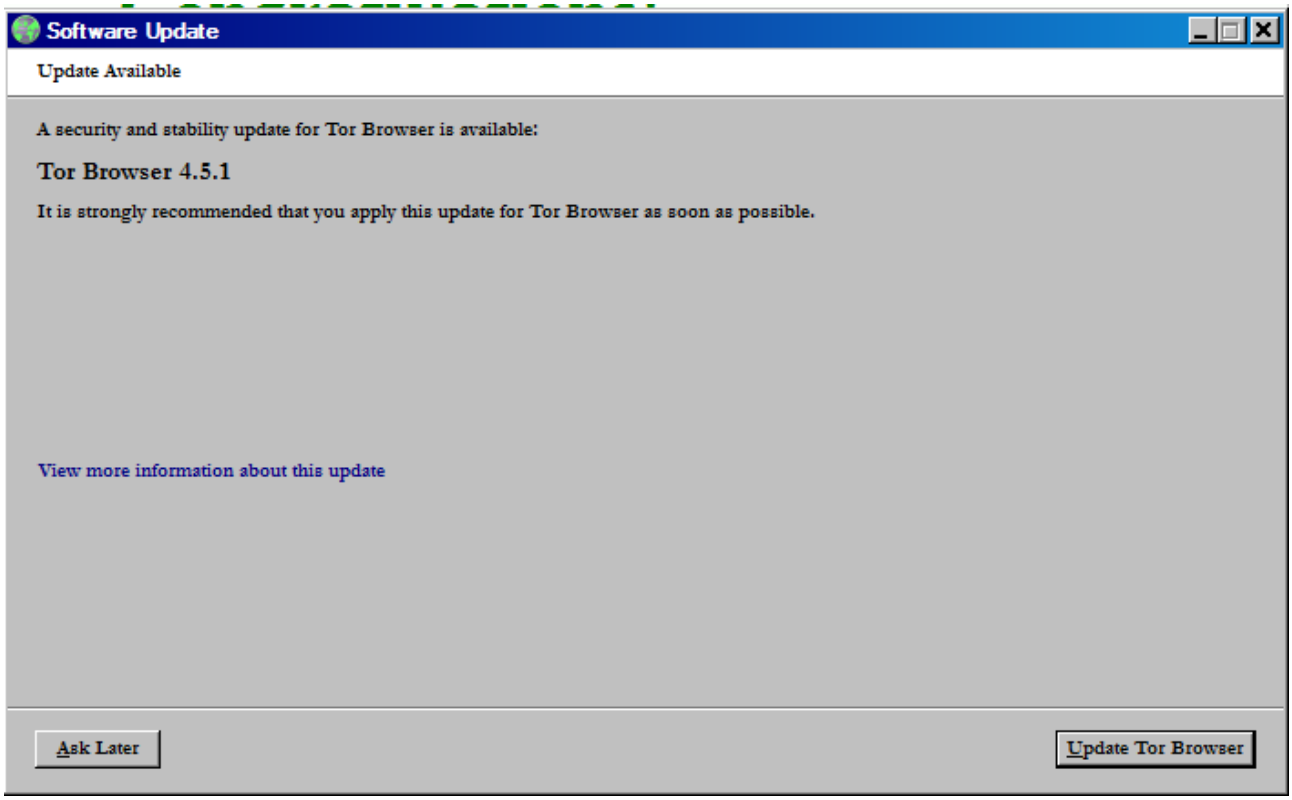


2. Contemporaneamente in basso a destra dello schermo del vostro computer vi appare la finestra mostrata nella figura che segue dove è indicata la nuova versione che verrà installa (nell'esempio "Tor Browser 4.5.1 available"): fate click su link **Download & Install...**.

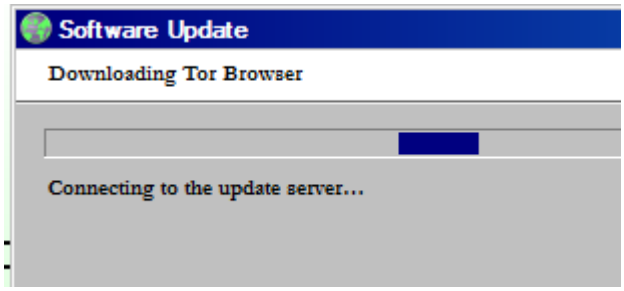
3. Questa finestra appare per pochi secondi. Se si chiude prima di aver fatto il click su **Download & Install...**, fermate Tor Browser e riavviatelo: vi riapparirà di nuovo questa finestra.

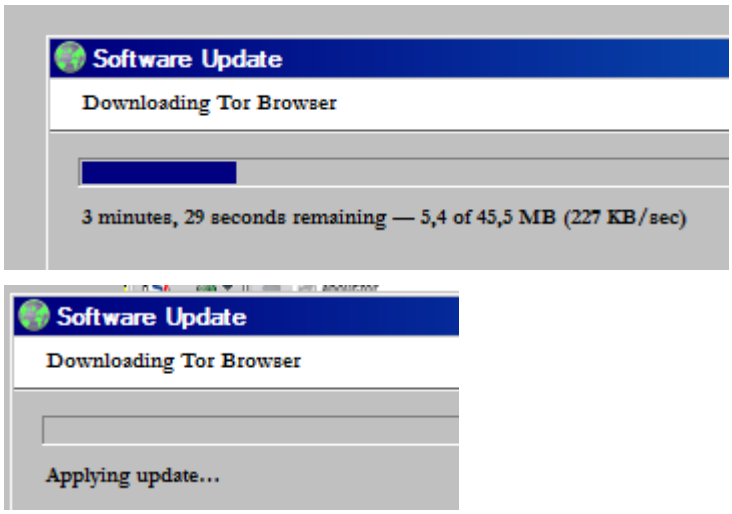
   Dopo aver fatto click su **Download & Install...** vi appare la finestra mostrata nella figura che segue.

   Per avviare l'aggiornamento automatico fate click sul bottone **Update Tor Browser**.

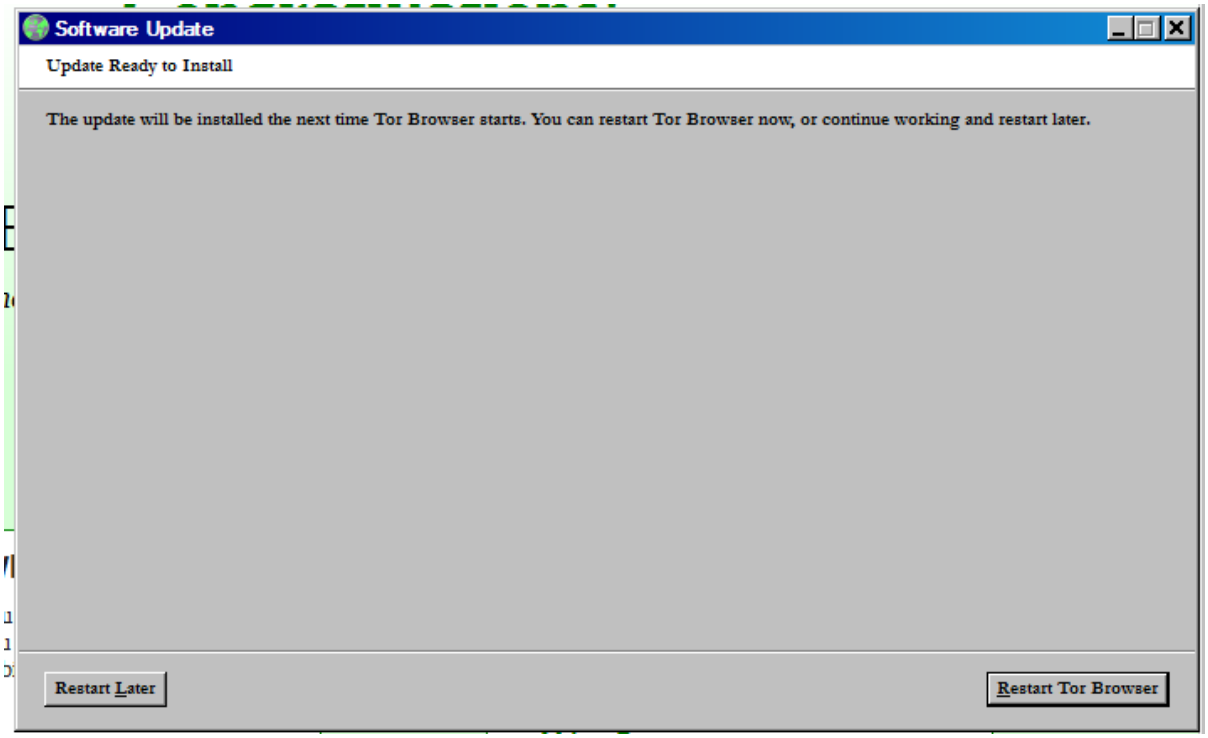


4. A questo punto si succedono varie fasi illustrate nell'ordine nelle figure che seguono.



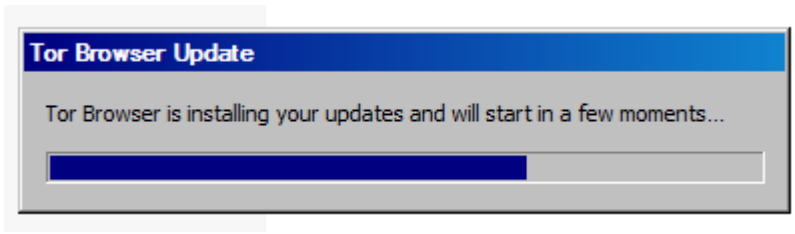


5. La figura precedente illustra l'ultima fase, dopo di essa vi appare la finestra mostrata nella figura che segue: fate click sul bottone **Restart Later**.

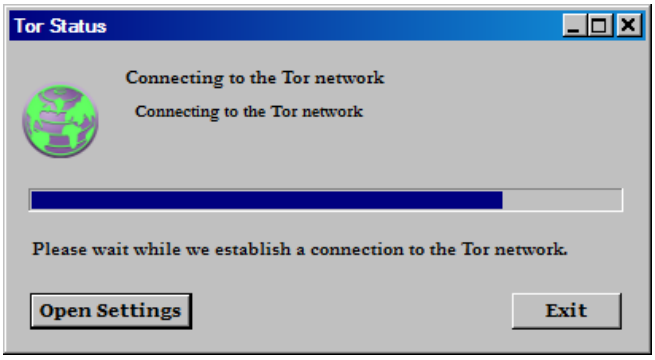


6. Fermate Tor Browser e riavviatelo.

   Al riavvio si apre la finestra mostrata nella figura che segue, che indica che sta avvenendo l'aggiornamento di Tor Browser e che al termine di esso il programma verrà avviato.



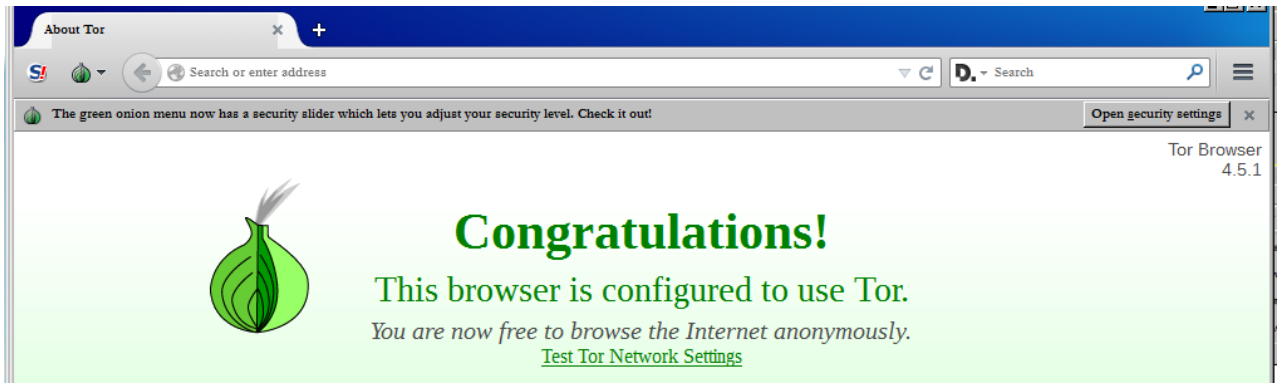
7. Alla fine dell'aggiornamento appare la finestra di avvio della connessione con internet attraverso Tor Browser (vedi la figura che segue).



8. Questa operazione può durare alcuni minuti, ma se la connessione non avviene fate click su bottone Exit e avviate di nuovo Tor Browser. Di solito al secondo tentativo la connessione si avvia rapidamente e vi appare la finestra di Firefox mostrata nella figura che segue.

   1. Noterete un barra orizzontale che contiene il bottone **Open security settings** (se fate click su questo bottone si apre una finestra per modificare le opzioni del livello di anonimato da mantenere durante la navigazione su internet, **non dovete modificarle!**) e subito a destra di esso una **X**: fate click sulla X per chiudere questa barra (questa barra è mostrata solo la prima volta dopo l'aggiornamento di Tor Browser).

   2. Noterete che nella finestra di Firefox in alto a destra c'è la scritta "Tor Browser - 4.5.1", che indica la versione di Tor Browser che state utilizzando. Se la confrontate con la prima figura di questo capitolo, noterete che prima la versione utilizzata era la "4.0.4".



9. Parallelamente a Firefox vi appare anche la finestra mostrata nella figura che segue che conferma che l'aggiornamento è stato eseguito correttamente: fate click sul bottone **OK** per chiuderla. Ora Tor Browser è aggiornato e protegge meglio il vostro anonimato.