Le istruzioni per utilizzare TOR - Manuale

Queste istruzioni servono per navigare in maniera anonima su internet:

- accedere ai siti,
- copiare documenti,
- inviare o ricevere messaggi,
- gestire liste di distribuzione,
- gestire dei blog,
- inserire testi nei siti a condizione che possa essere fatto attraverso il programma Firefox di cui appresso.

In queste istruzioni non affrontiamo il problema né della creazione, né della gestione di un sito non gestibile con Firefox.

1. Procurarsi i programmi per l'installazione

Per iniziare ad utilizzare Tor dovete procurarvi Firefox 3.5.5 (il navigatore per internet che garantisce attualmente la maggiore sicurezza) e Vidalia (il programma che gestisce la connessione anonima a internet e contiene al suo interno Tor).

[*notate bene* le indicazioni che seguono sono riferite al sistema operativo Windows]

Firefox 3.5: lo potete scaricare gratuitamente nella versione inglese (quella descritta in queste istruzioni) al seguente indirizzo:

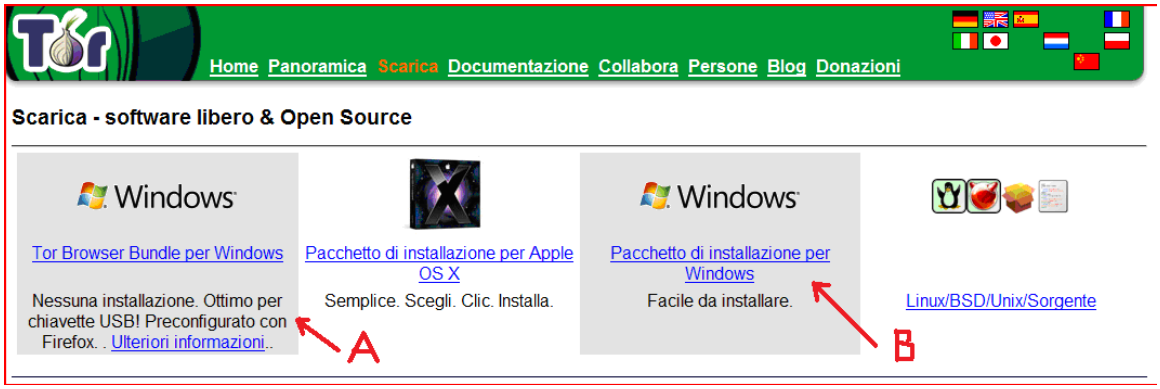
http://www.mozilla.com/en-US/

Ecco la zona della pagina web che si presenta. Fate click su **Download Firefox – Free** per ottenere il programma di installazione per il sistema Windows.

(La versione più aggiornata di *Firefox 3.5* nel momento in cui scriviamo è la 3.5.5)

Vidalia: lo potete scaricare gratuitamente al seguente indirizzo: **http://www.torproject.org/easy-download.html.it**

Ecco come vi appare la pagina per scaricare Vidalia.



Per ottenere la versione più recente fate click sul link "Pacchetto di installazione per Windows" **(zona B)**. Questa è la versione da installare sul vostro computer.

Nella **zona A** è disponibile un altro programma: il "Tor Browser Bundle per Windows". Questa versione di Vidalia vi permette di utilizzare Firefox per la navigazione anonima senza dover fare la minima regolazione e senza installazione. Potete tenere questo programma su una chiavetta USB, e usarlo da qualsiasi altro computer, senza doverlo installare.

È utile in vacanza e nei cyber caffè o su qualsiasi altro computer a cui abbiate accesso: scuola, ufficio, ecc. Questo programma non ha bisogno di installazione, il suo uso è più che discreto se si deve utilizzare la navigazione anonima quando si è in giro. Questa versione è quindi adatta ad un uso sporadico su computer diversi dal vostro, ma se non siete delle cime in computeristica o volete sperimentare subito la navigazione sicura, potete benissimo utilizzare questa versione anche sul vostro computer personale (le istruzioni dal sito ufficiale di TOR per l'installazione di questo programma le trovate facendo click su "Ulteriori informazioni" nella **zona A**).

Sul medesimo sito sono disponibili anche delle informazioni tecniche sul funzionamento di Vidalia al seguente indirizzo:

https://www.torproject.org/documentation.html.it.

Qui trovate indicazioni per installare e far funzionare Vidalia. Rispetto alle indicazioni del sito ufficiale, noi cerchiamo di indicarvi la procedura più rapida che garantisce contemporaneamente un grado di sicurezza adeguato alla navigazione anonima.

Naturalmente Vidalia funziona anche su altri sistemi operativi (Mac OS e Linux). Sempre sul sito all'indirizzo **https://www.torproject.org/download.html.it**, trovate programmi ed istruzioni anche per questi sistemi operativi.

Le informazioni più dettagliate sono in inglese. Quindi ripassate le vostre nozioni d'inglese se volete utilizzare a fondo questo sito per approfondire la conoscenza di Tor. Inoltre notate bene che le indicazioni per configurare Firefox 3.5 si riferiscono alla versione inglese. Se usate la versione italiana o in un'altra lingua, tenete conto che i menù e le voci sono comunque nella stessa posizione, cambiano solo le dizioni. Noi, per quanto possibile, vi indicheremo le coordinate dei menu e delle schede in modo da facilitarvi il lavoro di configurazione anche se avete una versione differente da quella inglese.

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

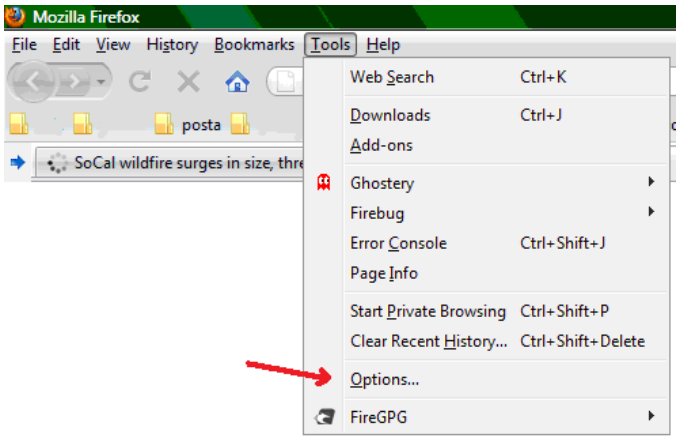
2. Installazione e configurazione

Il passaggio successivo è installare il navigatore Firefox e impostare le funzioni riguardanti la difesa della privacy descritte qui di seguito, che sono dei prerequisiti al corretto funzionamento di Tor.

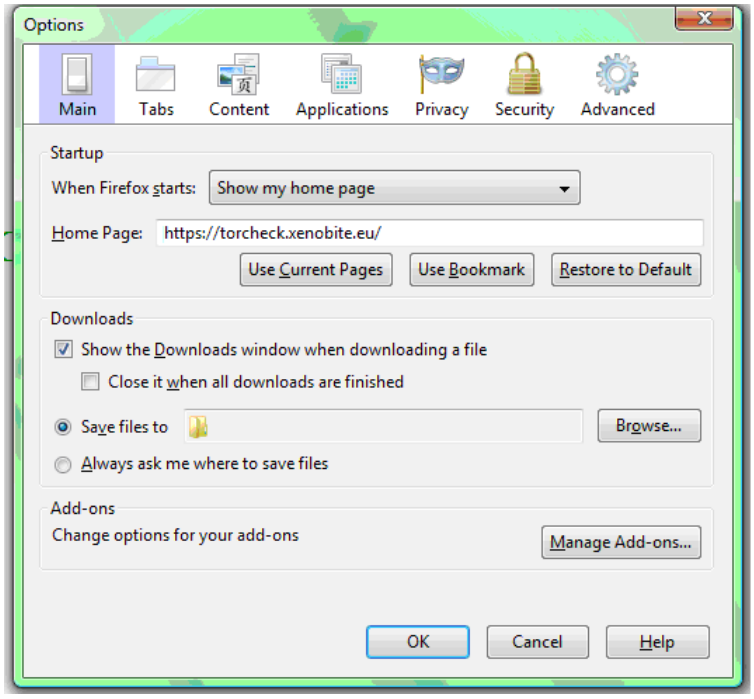
Per installare Firefox, utilizzate il programma indicato al punto 1. di queste istruzioni. Avviate il programma. Quando vi verranno richieste delle scelte, lasciate quelle proposte dal programma di installazione.

Firefox ha le stesse funzioni di Internet Explorer (IE). Dopo la sua installazione avrete a disposizione sul vostro computer entrambi i programmi: essi possono convivere tranquillamente. Vi consigliamo di usare IE per la navigazione normale (non anonima) e Firefox, impostato come vi descriveremo di seguito, per la navigazione anonima.

Dopo averlo installato, avviate Firefox e scegliete dal menu *Tools* la voce *Options*… .



Scegliete poi dalla finestra *Options* che si apre la scheda *Main*, come nella figura qui sotto.



Nel campo di testo *Home page:* inserite l'indirizzo internet: **https://torcheck.xenobite.eu/** come indicato nell'immagine soprastante.

È importante impostare l'*home page* a questo indirizzo perché è una pagina internet speciale che segnala se il sistema di navigazione anonima funziona correttamente ed è attivo. Più avanti descriveremo in dettaglio l'utilizzo di questa pagina.

Scegliete la cartella in cui volete registrare i file scaricati da internet con il pulsante che si trova a destra della voce *Save files to* . È importante definire questa cartella per ritrovare facilmente i dati riservati e poterli cancellare in modo adeguato[(1)].

Nota:

1. Per pulire tutto il vostri dati, dopo aver trasferito con l'operazione copia e incolla in un posto sicuro i dati da archiviare, usate **CCleaner** o **Eraser** per cancellare in modo definitivo i vostri file riservati rimasti sul computer. Solo utilizzando uno di questi due programmi di cancellazione ogni traccia del vostro lavoro viene effettivamente cancellata. **Non dovete mai buttare nel cestino** i file altrimenti possono essere recuperati da virus, troiani e poliziotti!

Non dovete mai fare operazioni di taglia incolla da un disco (o chiavetta) a un'altro.

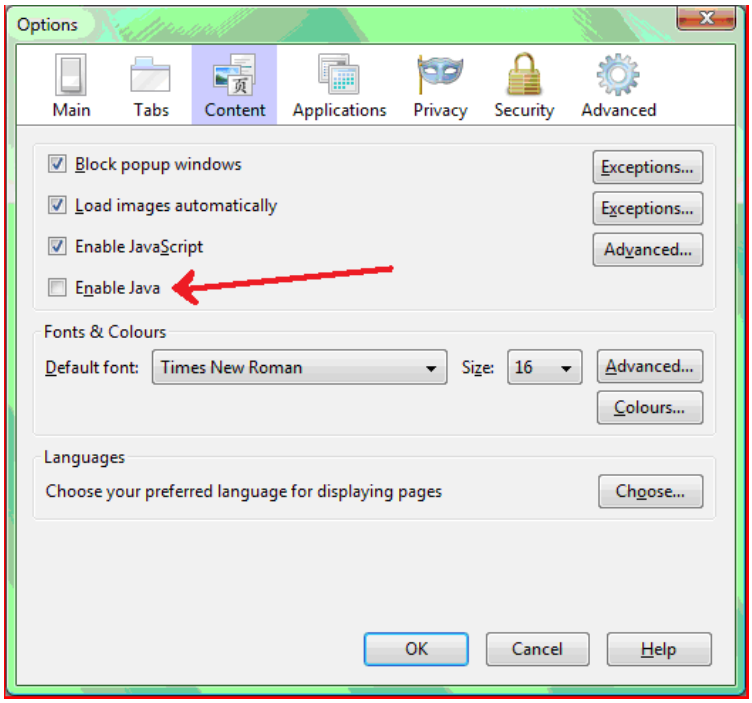
CCleaner è reperibile alla pagina internet:

http://www.filehippo.com/download_ccleaner/tech/

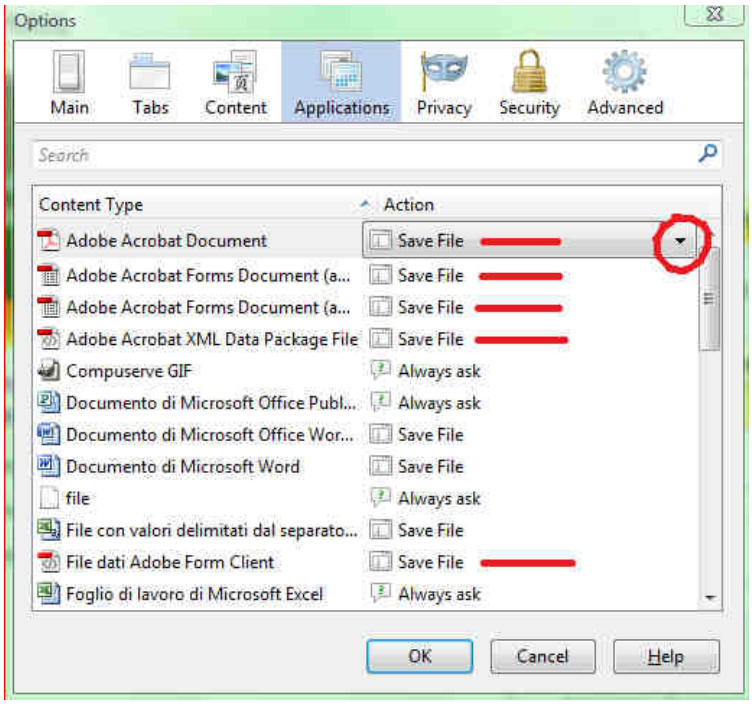
Eraser è reperibile alla pagina internet:

http://sourceforge.net/project/showfiles.php?group_id=37015

Sempre nella finestra *Options* selezionate la scheda *Content* e disattivate **Enabled Java**: la voce **Enabled Java** deve apparire sprovvista del segno di spunta. Fate click su OK per registrare la modifica. Bisogna impedire l'esecuzione di Java durante la navigazione, poiché Java scavalca la protezione di Tor. Java è usato soprattutto nei programmi di Chat e in alcuni casi come interfaccia per aggiornare i siti Web o trasferire i file. Comunque fate in modo che le impostazioni siano esattamente come le vedete nella figura sottostante.



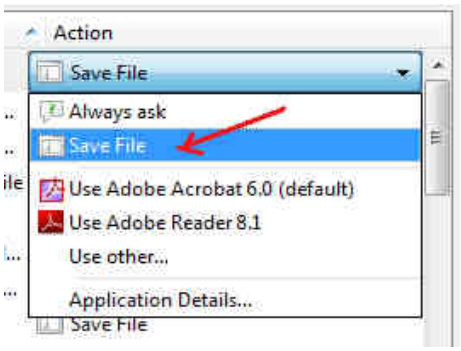
Sempre dalla finestra *Options* nella scheda *Applications* impostate *Save File* per tutti i file PDF e Microsoft Word come mostrato nell'immagine che segue.



I file PDF se aperti all'interno di Firefox, possono rivelare la vera identità di chi naviga. Scegliendo *Save File*, Firefox li registra anziché aprirli. Li potrete consultare alla fine della sessione di navigazione scollegandovi da internet.

Per impostare l'azione predefinita per ogni tipo di documento, evidenziate il tipo di documento, come nell'immagine soprastante.

Evidenziando il tipo di documento (qui ad esempio il tipo PDF) e facendo click sul triangolino nero a destra (nel cerchio rosso nell'immagine soprastante) appare il menù a discesa come nell'immagine che segue.

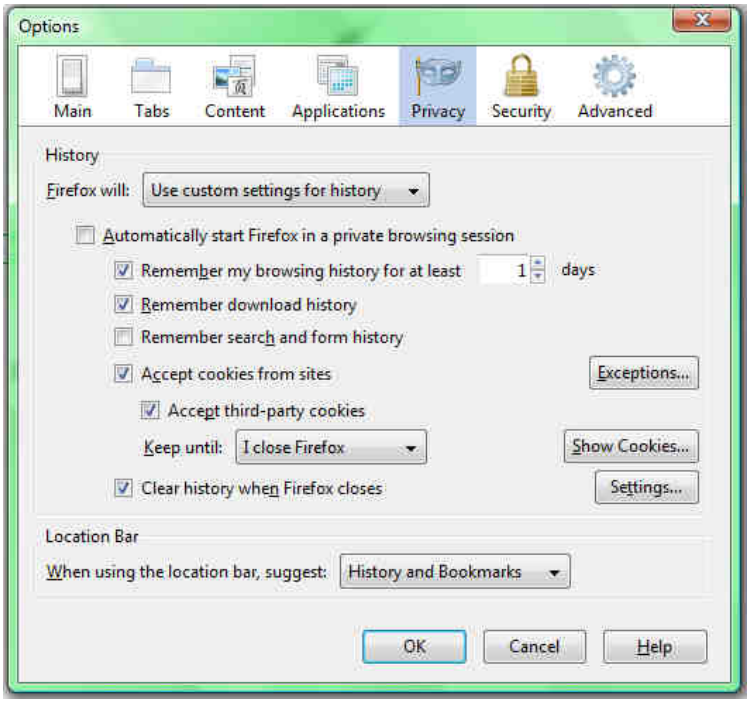


Vengono mostrate le possibili azioni da eseguire: scegliete "Save File". Ogni volta che nella navigazione aprirete un documento PDF, esso verrà registrato sul disco anziché essere visualizzato.

Per la visualizzazione dei file PDF è valido lo stesso discorso di Java. Adobe Acrobat Document (Acrobat Reader), il programma che visualizza i file PDF, se utilizzato all'interno di Firefox, può rivelare la vostra identità, soprattutto se viene utilizzato per riempire dei moduli. Impostando Firefox nella maniera indicata qui sopra, i file PDF vengono registrati sul disco del computer. Li potrete consultare tranquillamente alla fine del vostro collegamento con internet. Fate click sul bottone OK per registrare la modifica.

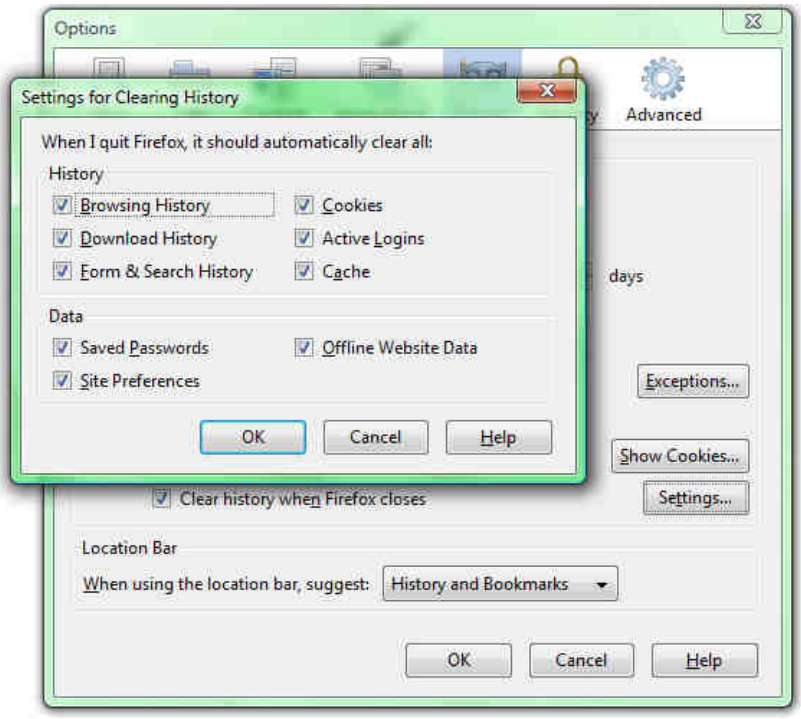
Sempre dalla finestra *Options* scegliete la scheda *Privacy*. Impostate i segni di spunta come nell'immagine che segue. Nella stessa scheda sotto la voce *Accept third-party cookies*, a destra di *keep until* (premendo sul triangolino vi vengono mostrate varie voci) impostate la voce *I close Firefox*. In questo modo siete sicuri di cancellare alla fine della sessione di lavoro le tracce della vostra navigazione. Molti siti funzionano attraverso l'utilizzo dei cookie. Disattivarli può significare l'impossibilità di utilizzarli. Ad esempio la maggior parte dei siti che gestiscono le email richiedono l'uso dei cookie.

Cancellando i cookie alla chiusura di Firefox ci garantiamo che se eventuali curiosi mettono le mani sul nostro computer, non sono in grado di risalire ai siti che consultiamo di frequente e a varie altre informazioni che possono costituire una manna per poliziotti & affini. Inoltre, quando iniziamo una nuova sessione, non abbiamo cookie già registrati che possono farci riconoscere dagli spioni.



Un'altra impostazione fondamentale per cancellare tutte le tracce della nostra navigazione e informazioni che possono identificarci, è l'attivazione della voce *Clear history when Firefox closes*, nella scheda *Privacy* (vedete immagine che segue). Deve essere presente il segno di spunta nella casella a sinistra di questa voce. Poi fate click sul bottone *Settings…*.

Vi si presenta la finestra "Setting for Cleating History". Rendete attive tutte le voci come mostrato nella figura seguente. Il segno di spunta deve essere visibile a sinistra di ogni voce e fate click su OK per registrare le vostre scelte.



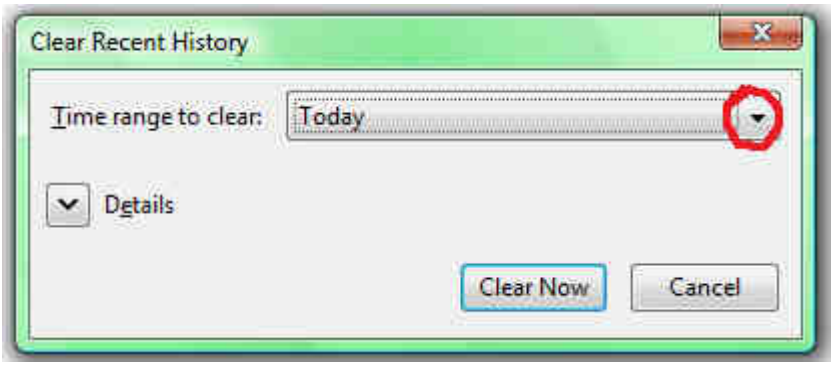
In questo modo sul vostro disco non verrà conservata la lista dei siti che visitate (*Browsing History*), i file che scaricate (*Download History*), i dati che avete immesso nei moduli (*Form & Search History*), come quelli ad esempio utilizzati per mettere parole d'ordine o per aprire una email, ecc. Verrà cancellata anche la *Cache*, che è una cartella in cui il navigatore registra le pagine visitate per rendere la loro visualizzazione più rapida, ma che lascia una traccia dei siti che frequentate con maggiore assiduità e costituisce una specie di profilo della vostra "personalità internet".

In particolare controllate che siano attivate le voci *Saved Passwords*, *Site preferences* e *Offline Website Data*, è importante per non permettere ai programmi e virus spioni, qualora si insinuino nel vostro sistema, di scoprire le password che usate.

Le impostazioni appena descritte cancellano le informazioni alla fine dell'utilizzo di Firefox. Potete però cancellare queste informazioni anche durante l'utilizzo di Firefox scegliendo dal menu *Tools* la voce *Clear Recent History…* .

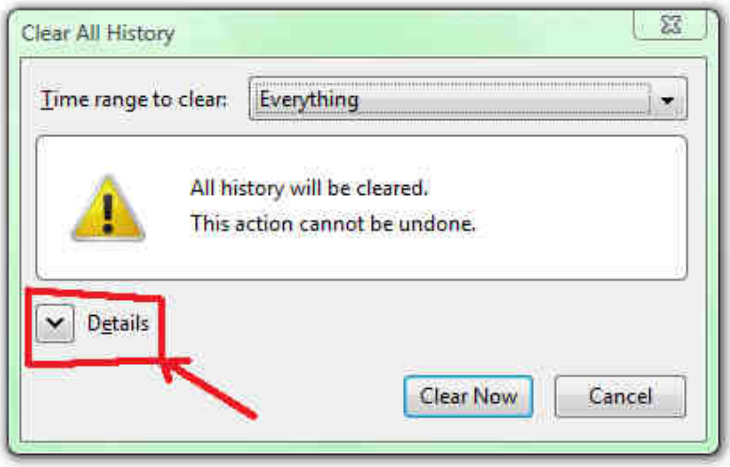
Però, prima di usare questa funzione, impostate cosa cancellare nel modo seguente.

Scegliendo dal menu *Tools* la voce *Clear Recent History…* si apre la finestra mostrata nell'immagine che segue.

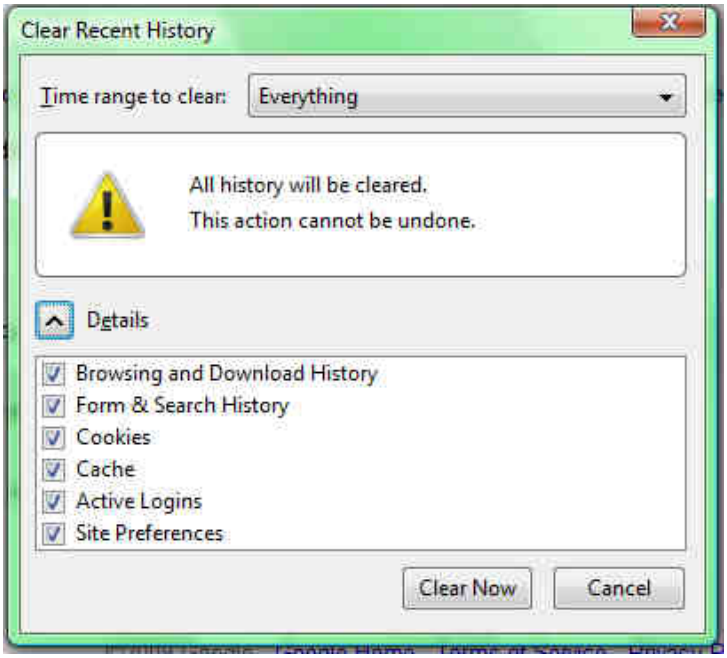


Fate click sul triangolino nero a sinistra della voce *Time range to clear:*. Vi appare un menu con varie voci. Scegliete la voce Everything (la voce indicata con A nell'immagine che segue).

Dopo la selezione la finestra prende l'aspetto dell'immagine che segue.



Fate click sulla freccina verso il basso di **Details**. Si apre un'area con diverse opzioni, come nell'immagine che segue.



Fate comparire il segno di spunta a sinistra di ogni voce e fate click sul bottone ***Clear Now***. Da questo momento in poi della navigazione le tracce della navigazione precedente non sono più registrate sul computer.

Non create segnalibri (indici dei siti usati più frequentemente, "Bookmarks" nella versione inglese di Firefox) con i siti che possono caratterizzarvi ai fini polizieschi (es. (n)PCI, ASP, CARC, ecc.). Create segnalibri solo per i siti comuni come Virgilio, Yahoo, Google o giornali borghesi.
Per i siti "sensibili" che usate spesso, create con il programma bloc-notes un file con l'elenco degl'indirizzi internet dei siti "sensibili" e copiateli in Firefox con il copia incolla invece di scriverli a mano. È il metodo più sicuro per tenere un elenco di siti che non possono essere letti dagli spioni durante la navigazione.

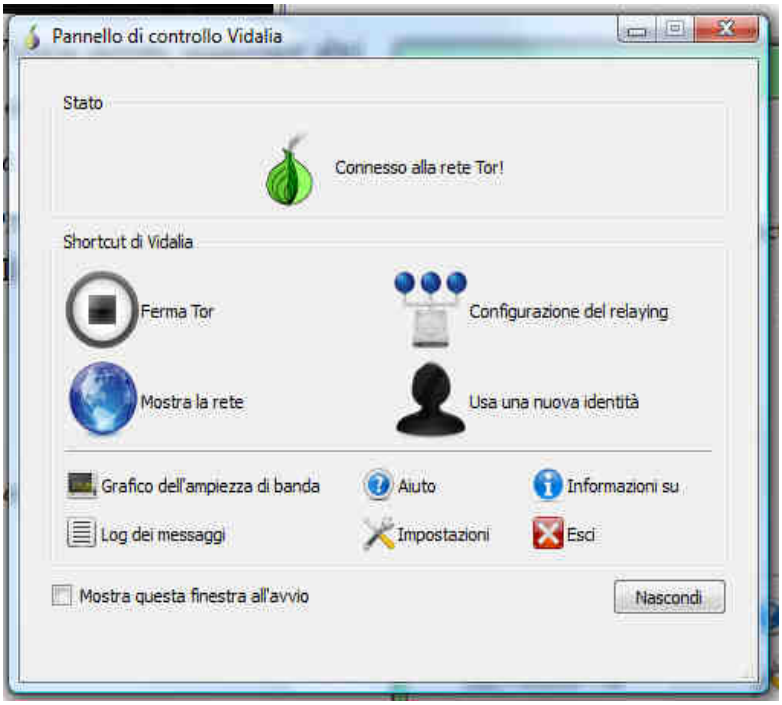
A questo punto avete terminato l'impostazione di Firefox e vi garantite un anonimato semplice ma efficace. Vale a dire che ogni volta che iniziate la navigazione su internet, è come se aveste il vostro documento di identità privo di informazioni.
La vostra individuazione è più difficile. Chi vi osserva non può sapere chi siete se non per il vostro identificativo di connessione, il famoso indirizzo IP, un numero che vi identifica sulla rete internet, paragonabile al numero di telefono di casa. **Tor è il software che vi permette di cancellare anche quest'ultima traccia e di impedire la vostra identificazione**.

3. L'installazione di Tor

L'installazione di Tor è molto semplice e avviene avviando il programma *vidalia-bundle-0.2.1.20-0.2.5.exe* (la versione più aggiornata nel momento in cui scriviamo) **che avete in precedenza scaricato come indicato al punto 1 di questo manuale**.
Quando si presenta la finestra con la scelta dei programmi da installare, lasciate le scelte che vi vengono proposte. **Controllate che nelle scelte sia attiva l'installazione di Torbutton:** è un programma aggiuntivo (Plugin) per Firefox **assolutamente** necessario per gestire il vostro anonimato.
Per il suo corretto funzionamento il programma TOR deve installare, oltre che se stesso, i seguenti programmi: Vidalia, Polipo e Torbutton.

4. L'impostazione di Vidalia (e Tor)

Quando avviate Vidalia per la prima volta, vi si presenta la finestra seguente:

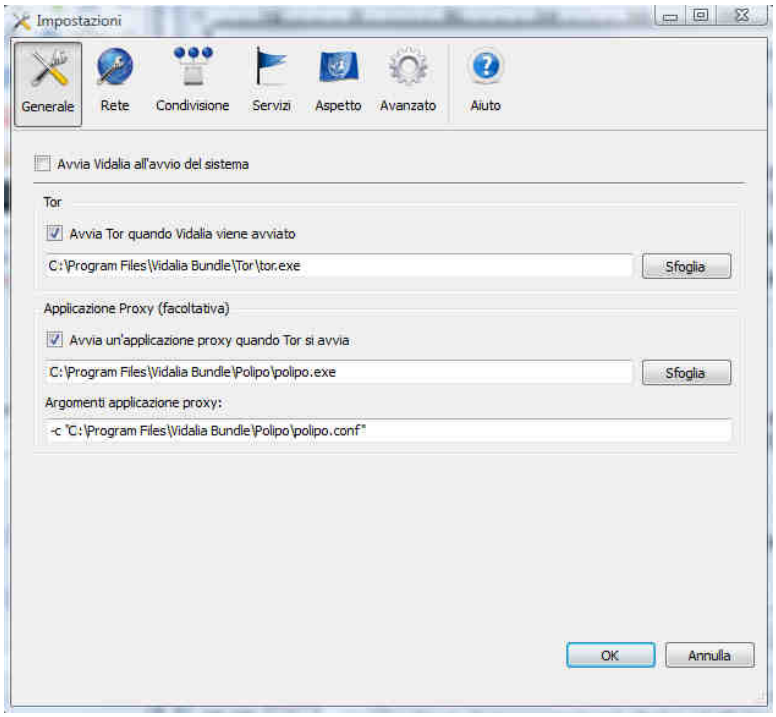


Se tutto funziona regolarmente e siete connessi a internet, il simbolo di Vidalia (la cipolla) deve apparire nella barra in basso di Windows di color verde.

Come nell'immagine qui di seguito:

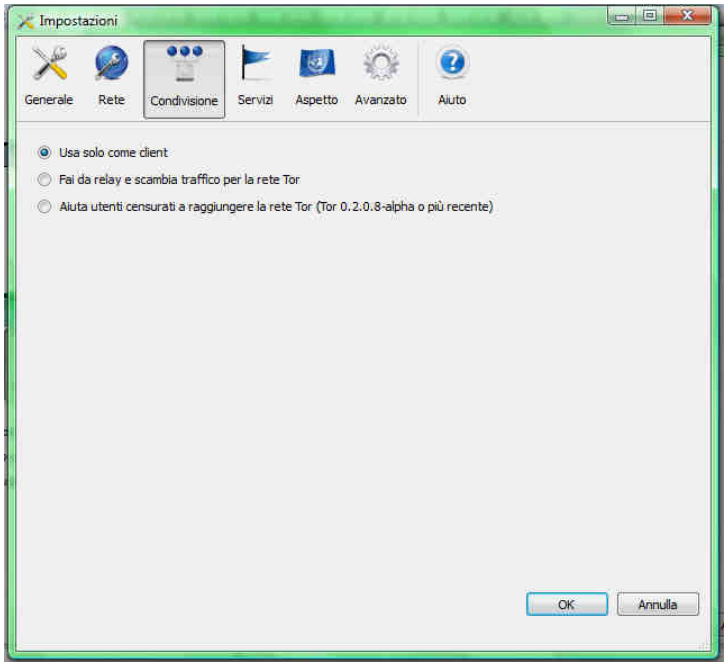
Prima di utilizzare Vidalia dovete impostare altri parametri come descritto di seguito. Aprite il *Pannello di Controllo Vidalia*. Apritelo facendo doppio click sul simbolo del programma: la cipolla nella barra in basso di Windows. Nella finestra che vi appare fate click su *Impostazioni*. (vedi immagine a sinistra)

Vi appare la finestra *Impostazioni* seguente:



Selezionate l'area *Generale*. La voce *Avvia Tor quando viene avviato Vidalia* **deve essere imperativamente attivata**. La voce *Avvia un'applicazione proxy quando Tor si avvia* **deve essere imperativamente attivata**. Lasciate le impostazioni che sono già inserite automaticamente nei campi di testo. Con queste impostazioni, ogni volta che dovete navigare in modo anonimo su internet dovete avviare manualmente Vidalia: una scelta dettata da questioni di riservatezza, la cipolla verde sul computer apparirà solamente quando voi lo deciderete. Fate click sul bottone ***OK*** per registrare la vostra scelta.

Selezionate la voce *Condivisione*. Lasciate attiva la voce *Usa solo come client* (vedi immagine seguente). Non variate le altre impostazioni. Quando sarete più esperti e vorrete installare il Relay[(2)], sarete costretti a modificare anche altre impostazioni. In queste istruzioni ci concentriamo solo sull'uso più semplice di Tor, cioè l'uso come Client (terminale) della rete Tor che non necessita di altre impostazioni.



Nota:

2. Attivare il "fai da Relay e scambia traffico per la rete Tor" (scambia traffico per la rete Tor) significa permettere al vostro computer di sostenere il traffico della rete Tor. Aumenterete le risorse della rete e la renderete più veloce. Questa attivazione richiede un'ulteriore sforzo di studio e sperimentazione. Se avete un vecchio computer che non utilizzate più, potete sperimentare l'installazione del Relay. L'installazione del Relay aumenta il vostro anonimato, nel senso che il vostro IP (identificativo su internet) verrà usato da migliaia di altre persone e quindi chi vorrà conoscere i vostri gusti e attività su internet, sarà costretto a cercare un ago nel pagliaio.

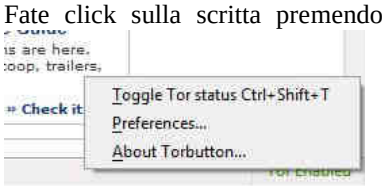
5. Come impostare Firefox per usufruire dell'anonimato attraverso Tor

Avviate Vidalia. Controllate sempre le icone nella barra in basso a destra per sapere se Vidalia è in funzione. **Il solo fatto che Vidalia sia in funzione non garantisce che la vostra navigazione sia anonima**. Bisogna impostare Firefox in modo da usufruire di Tor. Tenete ben presente che programmi che gestiscono la posta come Outlook o Thunderbird, non possono essere utilizzati con Tor. Per la posta dovrete quindi usare le email che si possono gestire attraverso il navigatore (le web email) tipo Yahoo, Google, Alice, Virgilio ecc. Ma su questo punto ritorneremo più avanti.

Vediamo adesso come impostare Firefox per indicargli di usare Tor durante la navigazione su internet.

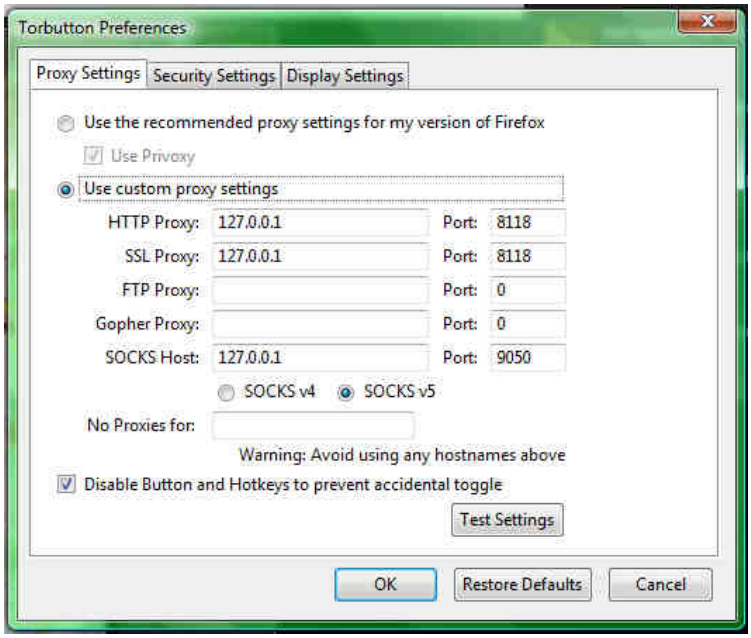
Avviamo Firefox. Se Vidalia si è correttamente installato aprendo Firefox vi viene richiesta l'installazione del plug-in di Torbutton. Confermate l'installazione e riavviate Firefox. Se tutto è andato bene, in basso a destra in Firefox deve essere presente, come nell'immagine che segue, la scritta in verde *Tor Enabled*.

Fate click sulla scritta premendo il tasto destro del mouse. Appare un menu. Scegliete la voce *Preferences…*

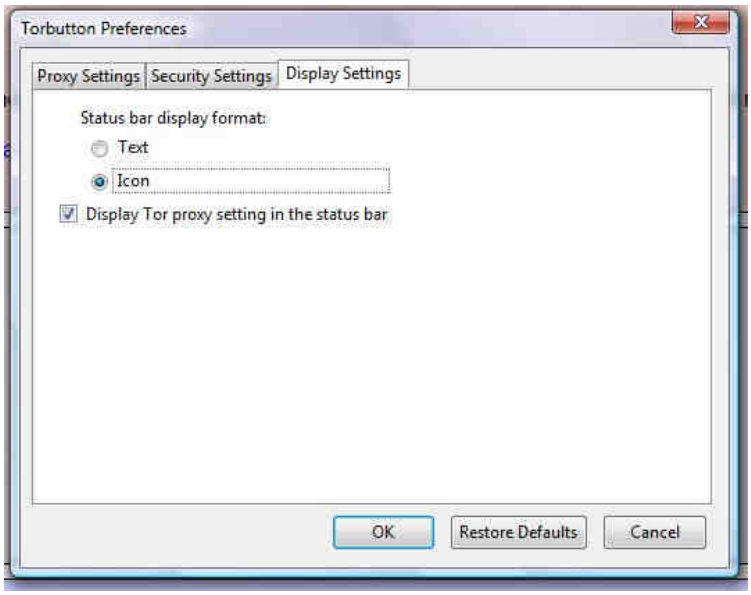


Appare la finestra *Torbutton Preferences* come nelle figura che segue. Selezionate la scheda *Proxy Setting*. In questa scheda dovete impostare i valori di connessione ad internet che permettono a Firefox di utilizzare Tor. Questa fase è essenziale per il corretto funzionamento di Firefox con Tor. Quindi prestate una cura particolare nell'impostazione dei parametri.

Fate click sul tasto *Restore Defaults* e ricopiate esattamente i valori impostati così come appaiono nell'immagine che segue. Fate in modo che anche sul vostro computer siano impostati gli stessi valori.



Sempre da questa finestra selezionate la scheda *Display Setting* e impostate *Icon* invece di *Text*.



Fate in modo che la vostre impostazioni siano uguali a quelle mostrate nella figura precedente. Confermate premendo il tasto *OK*.

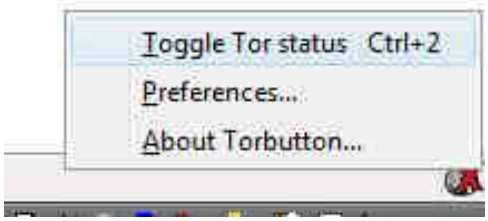
Impostando questi valori la scritta verde Tor Enabled in basso a destra verrà sostituita da un'icona più visibile come nell'immagine che segue.

 (la cipolla)

Se l'icona si presenta come nelle immagini che seguono:

vuol dire che non avete scelto di attivare Tor per la navigazione.

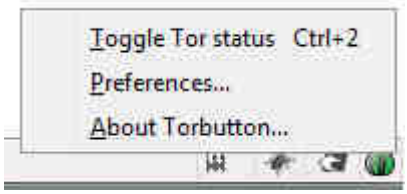
Per attivare Tor, fate click sull'icona o sulla scritta premendo il tasto destro del mouse e selezionate *Toggle Tor status* per avviare la navigazione anonima (vedi figura che segue).



Quando Tor è in funzione la scritta deve essere verde oppure la cipolla non deve avere la X rossa. In questa condizione state navigando in modo anonimo.

Ricordatevi di controllare sempre l'icona prima di iniziare una sessione di navigazione. È importante essere disciplinati per poter conservare l'anonimato. Dovete farvi una lista di cose da controllare e da fare prima di una sessione di navigazione anonima.

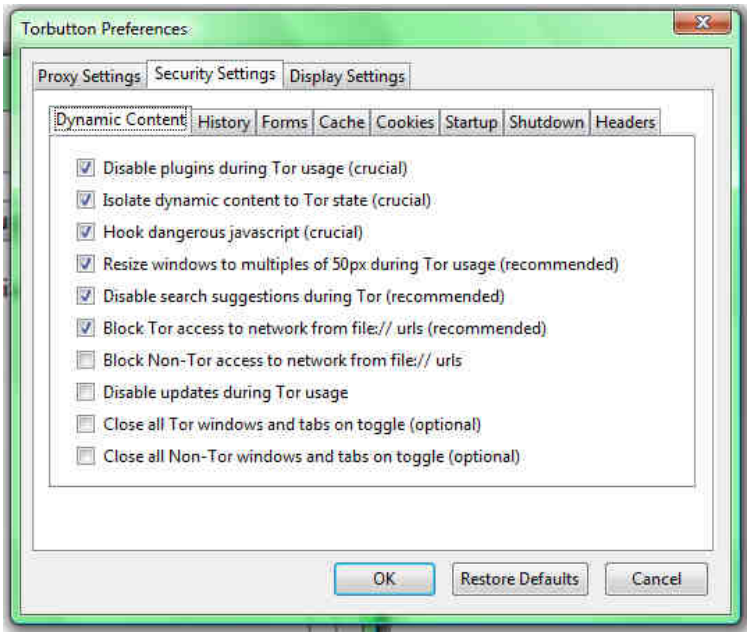
Fate click sulla cipolla premendo il tasto destro del mouse. Appare un menu. Scegliete la voce *Preferences…*

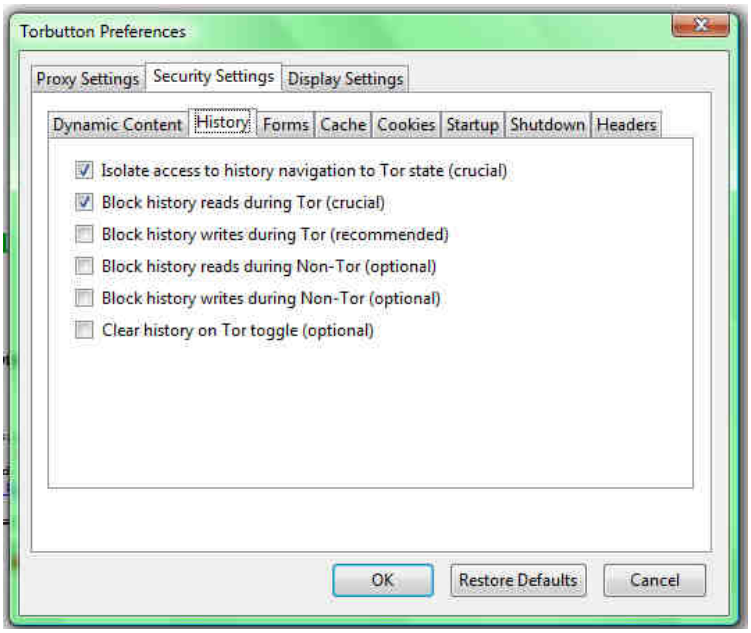


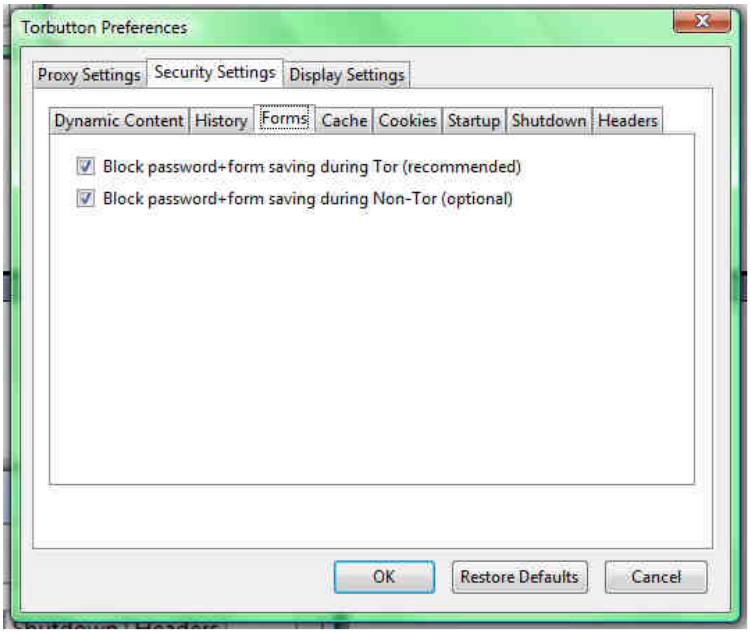
Si apre la finestra *Torbutton Preferences*. Scegliete la scheda *Security Setting*. All'apertura questa scheda vi mostra a sua volta una serie di schede. Le immagini che seguono vi mostrano come devono essere impostate le varie schede. Attenzione! Fate con pazienza questo lavoro e confermate le impostazioni con il tasto OK.

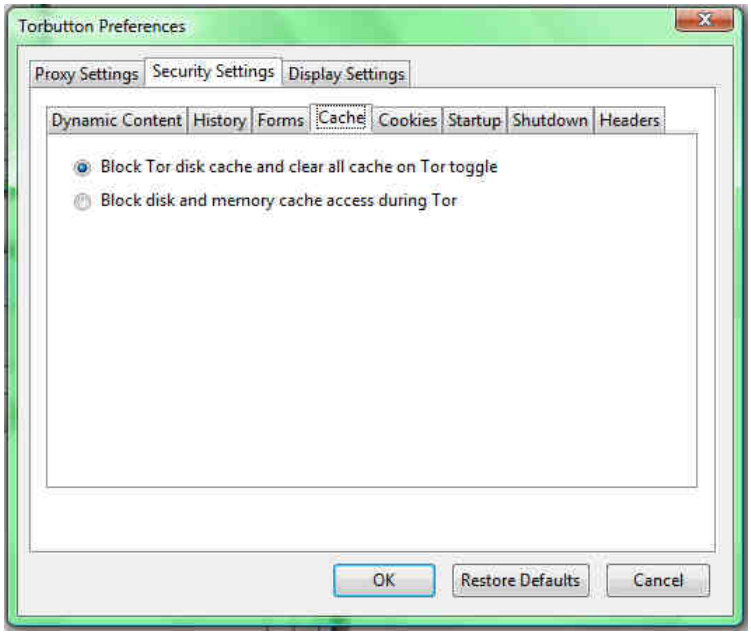
Riaprite la finestra *Torbutton Preferences* e ricontrollate le impostazioni confrontandole con la serie di immagini che seguono. Nessuna di queste impostazioni è secondaria. Vi raccomando di nuovo molta attenzione.

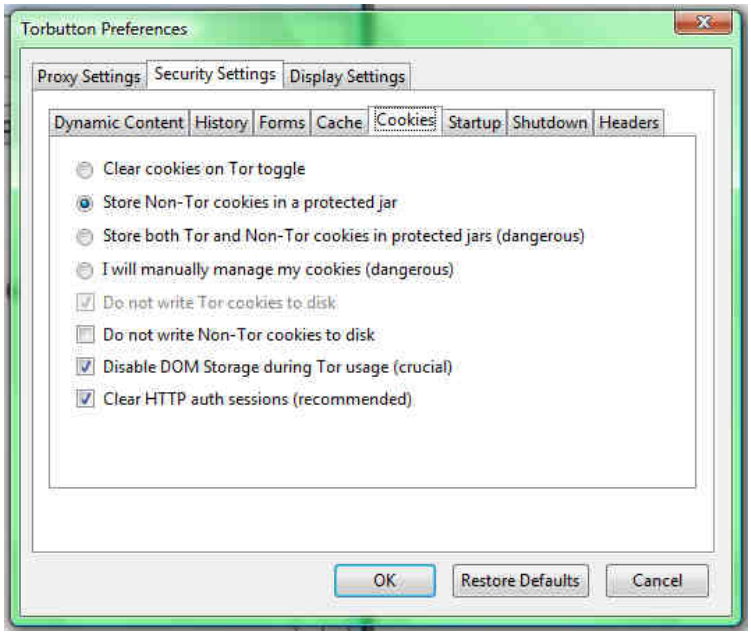
Ecco le immagini relative alla serie di sottoschede della scheda *Security Setting* e le **impostazioni corrette per ognuna di esse**.

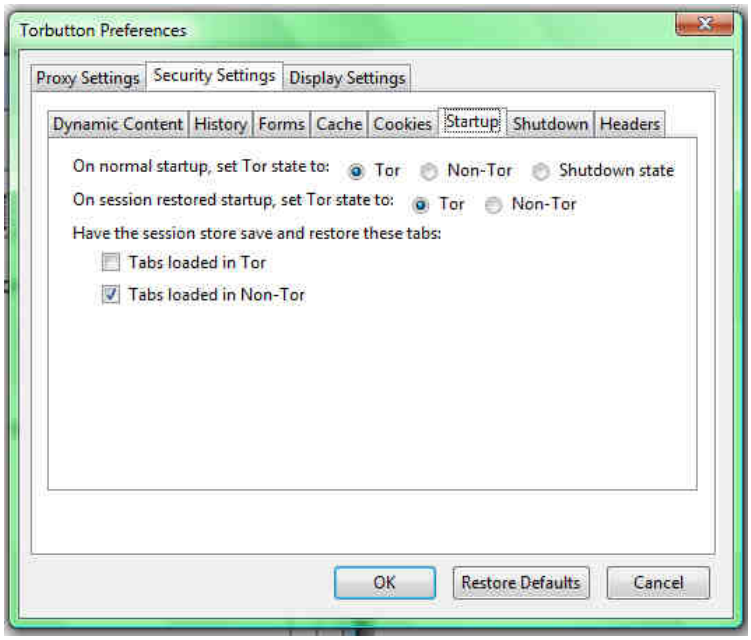

Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
Disable plugins during Tor usage (crucial)
Isolate dynamic content to Tor state (crucial)
Hook dangerous javascript (crucial)
Resize windows to multiples of 50px during Tor usage (recommended)
Disable search suggestions during Tor (recommended)
Block Tor access to network from file:// urls (recommended)
Block Non-Tor access to network from file:// urls
Disable updates during Tor usage
Close all Tor windows and tabs on toggle (optional)
Close all Non-Tor windows and tabs on toggle (optional)
OK
Restore Defaults
Cancel

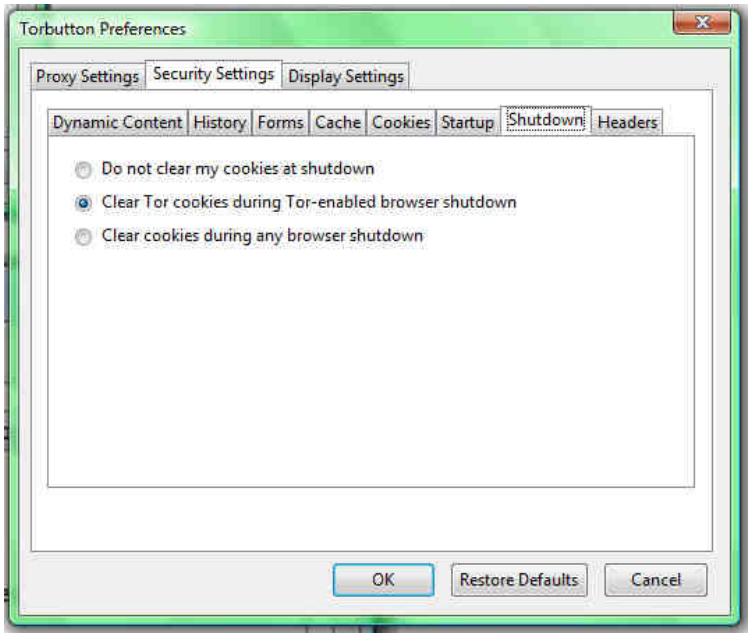

Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
Isolate access to history navigation to Tor state (crucial)
Block history reads during Tor (crucial)
Block history writes during Tor (recommended)
Block history reads during Non-Tor (optional)
Block history writes during Non-Tor (optional)
Clear history on Tor toggle (optional)
OK
Restore Defaults
Cancel

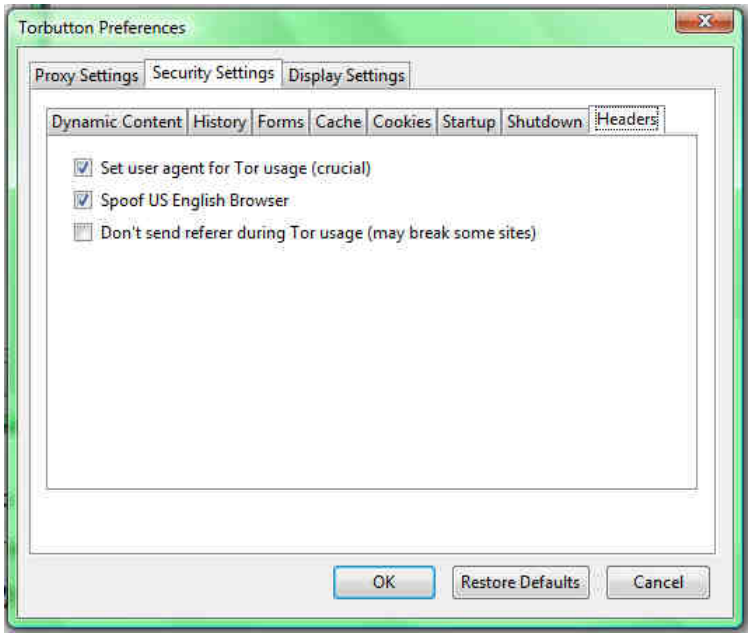

Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
Block password+form saving during Tor (recommended)
Block password+form saving during Non-Tor (optional)
OK
Restore Defaults
Cancel


Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
Block Tor disk cache and clear all cache on Tor toggle
Block disk and memory cache access during Tor
OK
Restore Defaults
Cancel


Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
Clear cookies on Tor toggle
Store Non-Tor cookies in a protected jar
Store both Tor and Non-Tor cookies in protected jars (dangerous)
I will manually manage my cookies (dangerous)
Do not write Tor cookies to disk
Do not write Non-Tor cookies to disk
Disable DOM Storage during Tor usage (crucial)
Clear HTTP auth sessions (recommended)
OK
Restore Defaults
Cancel


Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
On normal startup, set Tor state to:
Tor
Non-Tor
Shutdown state
On session restored startup, set Tor state to:
Tor
Non-Tor
Have the session store save and restore these tabs:
Tabs loaded in Tor
Tabs loaded in Non-Tor
OK
Restore Defaults
Cancel


Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
Do not clear my cookies at shutdown
Clear Tor cookies during Tor-enabled browser shutdown
Clear cookies during any browser shutdown
OK
Restore Defaults
Cancel

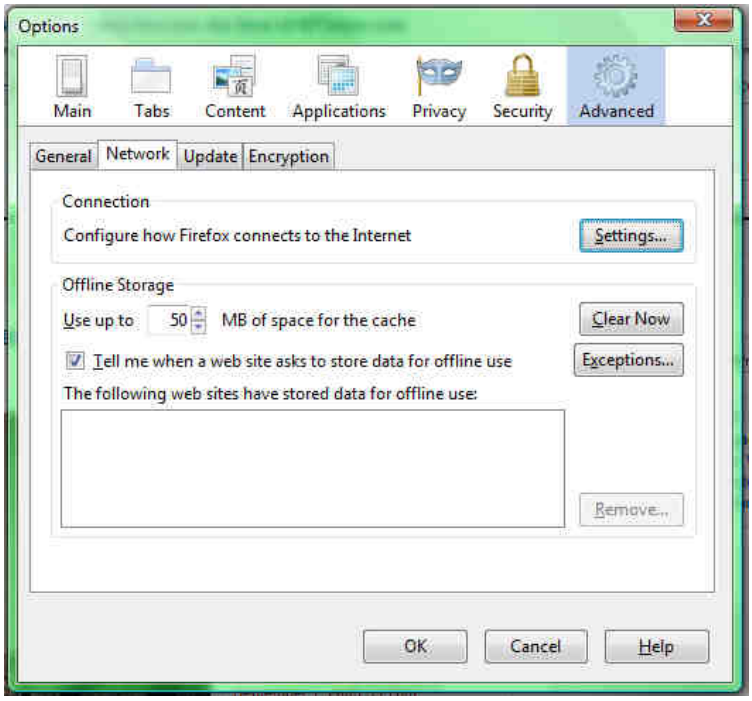

Torbutton Preferences
Proxy Settings
Security Settings
Display Settings
Dynamic Content
History
Forms
Cache
Cookies
Startup
Shutdown
Headers
Set user agent for Tor usage (crucial)
Spoof US English Browser
Don't send referer during Tor usage (may break some sites)
OK
Restore Defaults
Cancel

Torbutton è la base per l'impostazione e il corretto funzionamento di Firefox e Tor necessario per navigare in modo anonimo.

Se l'installazione di Torbutton non è riuscita, dovete impostare i valori per collegarvi a Tor attraverso il menu di Firefox.

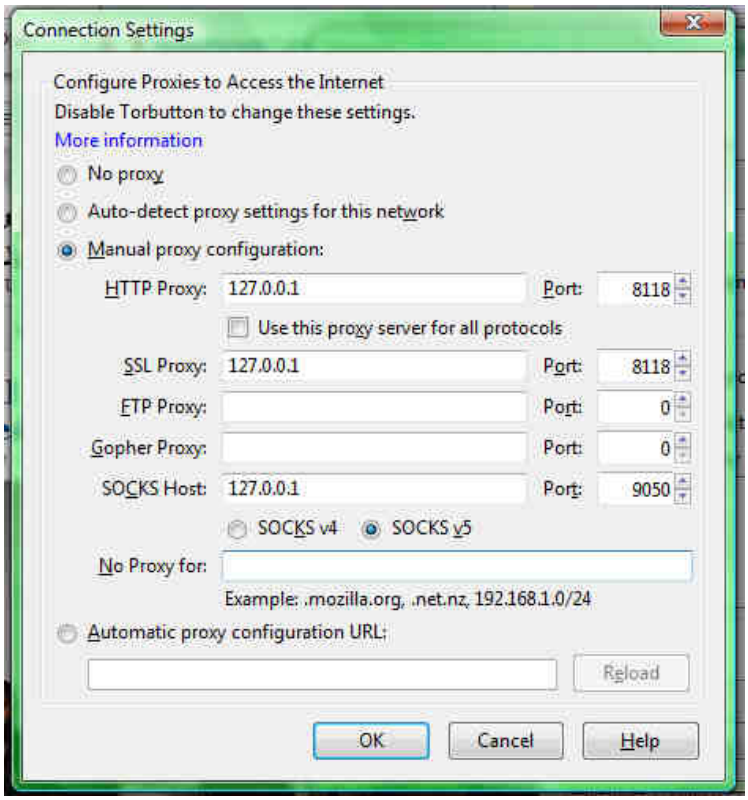
In questo caso selezionate dal menu di Firefox - *Tools* la voce *Options*.... Vi appare la finestra *Options* (vedi qui sotto).

Selezionate l'area *Advanced* e la scheda *Network.*



Fate click sul bottone *Settings…* nella sezione *Connection*.

Vi appare la seguente finestra: **impostate gli stessi valori sul vostro computer.**



Fate click sul bottone *OK* per registrare le impostazioni.

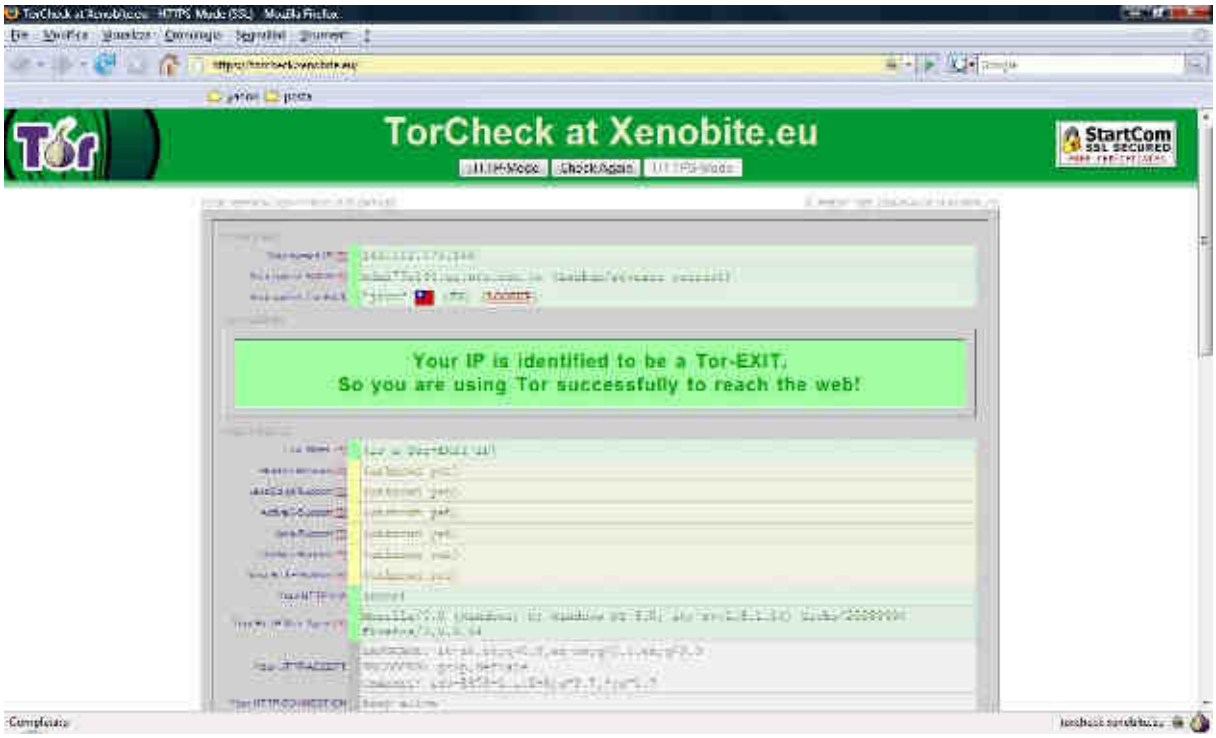
Queste sono le ultime impostazioni necessarie per la navigazione anonima con Firefox e Tor.

6. Verifica del funzionamento di Tor con Firefox

Questo capitolo è dedicato alla verifica del funzionamento della navigazione anonima.

La verifica avviene collegandosi al seguente indirizzo internet: https://torcheck.xenobite.eu/

Ecco come si presenta la pagina di questo sito:



Nella prima riga del modulo grigio (Your current IP) è mostrato il vostro numero identificativo internet che il sistema Tor vi attribuisce. Nella terza vi informa che in questo caso siete identificato come un taiwanese (Your current Tor-EXIT).

La seconda riga vi indica quale server della rete sta gestendo la navigazione sulla rete.

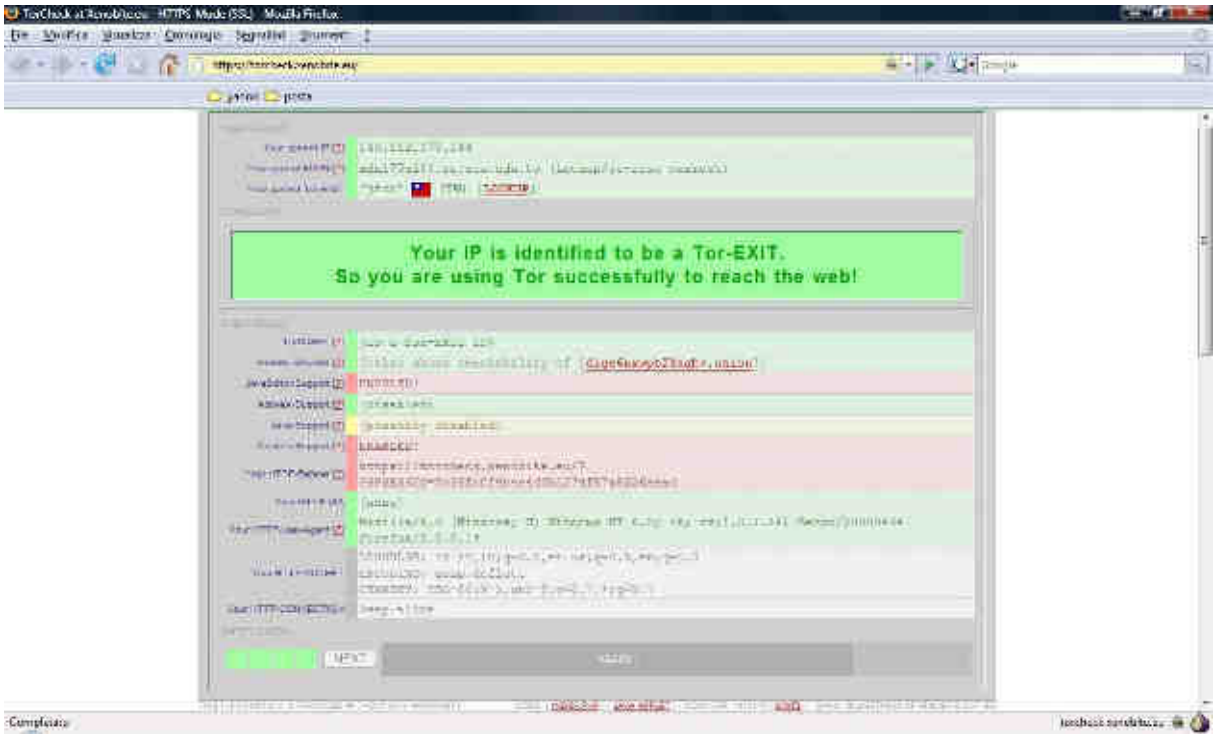
In grande sotto queste tre righe appare una scritta verde “Your IP is identified…”, questo vi indica che siete connesso in modo anonimo a internet.

Se non lo siete, appare la scritta seguente:

Controllate di nuovo che Tor sia attivo e le impostazioni corrette.

Questa pagina internet vi permette anche di controllare se Java è disabilitato e se le altre impostazioni del vostro navigatore sono sicure.

Ci sono altri controlli. Per avviarli, portatevi nella parte bassa del modulo e fate click sul bottone *START*. Poi fate click sullo stesso bottone che ora assume come testo *NEXT*, fino a che i quattro quadrati a sinistra del bottone diventano verdi, come nella figura della pagina seguente.



Quando i quattro quadrati sono verdi, vuol dire che tutti i controlli sono stati eseguiti.

Notate che dopo questi controlli le voci in verde indicano che Firefox è impostato correttamente per evitare di far conoscere la vostra identità. La voce più importante da controllare è Java-support. Il test ve la mostra in giallo: questo indica che Java non funziona, cioè è disabilitato. Non confondete Java con JavaScript, sono due cose molto diverse. Notate che JavaScript-support è segnalato in rosso.

Se ritornate al punto 2 di queste istruzioni, nella descrizione dell'installazione e della configurazione di Firefox, notate che non abbiamo detto a Firefox di non utilizzare JavaScript. Questa scelta volontaria dipende dal fatto che molti siti non funzionano senza l'utilizzo di JavaScript. Però JavaScript non può individuare il vostro identificativo (il vostro IP), ma solamente le informazioni legate all'impostazione di Firefox. Per questo abbiamo impostato Firefox per cancellare i Cookie, che contengono svariate informazioni sulle vostre abitudini e che JavaScript può esplorare e inviare agli spioni. Per evitare che JavaScript possa attingere alle informazioni contenute nei Cookie il rimedio consiste nella loro cancellazione durante la navigazione. Per cancellare i Cookie scegliete del menu *Tools* la voce *Clear Recent History…* e nella finestra che appare fate click sul bottone *Clear Now*. Fate questa operazione dopo aver visitato un sito "sensibile" o utilizzato una web mail "sensibile".

Se volete verificare l'efficacia della cancellazione dei Cookie, potete visitare una qualsiasi casella email, identificatevi, controllate la posta in arrivo, cancellate i Cookie attraverso la voce del menu *Tools* / *Clear Recent History…* mentre siete all'interno della vostra email. Constaterete che dopo la cancellazione sarete costretti a reidentificarvi perché le impostazioni legate a quella sessione di consultazione della email sono state cancellate, il gestore della web mail non vi riconosce più come legittimo utente.

Quindi non dovete disattivare JavaScript. La finestra mostrata sopra è corretta anche se presenta delle voci in rosso.

I Cookie sono necessari per consultare le caselle di posta Web, quindi non dovete disabilitarli. La cancellazione dei Cookie dopo ogni sessione di controllo della posta via web si impone, se si naviga a lungo. Uscendo da Firefox i Cookie vengono cancellati automaticamente. Quindi un buon sistema è uscire di frequente da Firefox. In questo modo si evita di far conoscere per esempio che due email differenti o due siti consultati sono legati ai vostri interessi personali.

Anche la voce Your http-referer è rossa. Per ovviare a questo inconveniente, basta impostare la pagina iniziale di Firefox su un sito ultra famoso come Google o Yahoo. Quando vi collegate al sito "caldo", l'eventuale informazione

che rivelate è che avete visitato un sito che altri milioni di internauti hanno visitato. Non visitate due siti "Caldi" uno di seguito all'altro. Uscite e rientrate da Firefox, se non volete mostrare che avete interessi per una certa area di siti. Queste istruzioni per il collaudo del funzionamento di Firefox e Tor le potete eseguire ad ogni inizio di sessione di navigazione se volete essere sicuri del buon funzionamento della navigazione anonima.

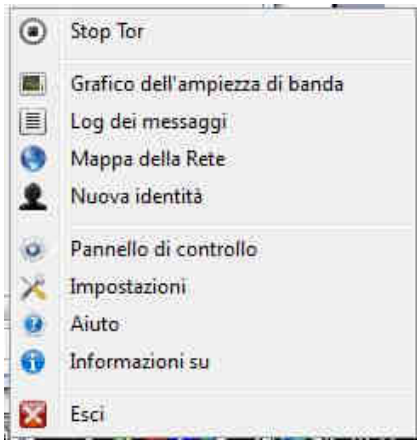
7. Consigli per la navigazione.

Superato il collaudo, potete iniziare la navigazione. Tenete presenti i consigli appena indicati per proteggere la vostra privacy. Tor vi permette di **variare a piacimento il vostro identificativo**.

Oltre ai consigli appena indicati, per evitare di dare informazioni sul vostro profilo, cambiate di tanto in tanto il vostro IP. Lo potete fare durante la sessione di navigazione attraverso le funzioni di Tor.

Fate click col tasto destro sul simbolo della cipolla verde nella barra in basso di Windows. Nel menu che vi viene mostrato (vedi sotto) fate click sulla voce Nuova identità. Sia che siate ancora in una sessione aperta di navigazione o che abbiate arrestato Firefox, l'IP cambia. La vostra nuova sessione si riapre, o continua, con una nuova identità.

A volte questa voce rimane inattiva. Vuol dire che Tor non ha ancora creato una nuova connessione. Normalmente dopo alcune decine di secondi questa voce diviene nuovamente attiva e potete di nuovo cambiare il vostro identificativo.



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. Per controllare se un'operazione è attiva, potete consultare il *Grafico dell'ampiezza di banda* (vi si accedete dallo stesso menu appena descritto). La finestra vi mostra due andamenti, quello giallo dei dati inviati (quando allegate) e quello blu dei dati ricevuti (quando scaricate). Per esempio se andate sul sito di *La Voce* e provate a scaricare il file del *Manifesto Programma*, se l'attesa è molto lunga, potete controllare attraverso questo grafico se l'operazione è in corso oppure se non dà segnali di vita.

Se l'operazione è bloccata, un sistema per sbloccarla consiste nel cambiare l'identità come sopra descritto. Un altro più drastico è terminare la sessione: arrestare Vidalia e farlo ripartire e riiniziare la sessione di navigazione.

8. La posta anonima con Tor

Un piccolo ma importantissimo capitolo lo dedichiamo all'invio e alla ricezione della posta in modo anonimo. Come accennavamo all'inizio, con Tor non si possono usare i programmi Outlook e Thunderbird. Quindi le uniche possibilità che avete per essere anonimi è la gestione delle email via Web. Per intenderci le email che possono essere controllate e gestite attraverso Firefox sono gestibili in modo anonimo.

Creando nuove email su Yahoo, Google, ecc. con l'uso di Tor, non riveliamo la nostra identità. Consultandole e utilizzandole in seguito con Tor, le manteniamo anonime. L'importante è essere disciplinati e ordinati e collegarsi sempre con Tor sia nel momento della creazione che durante il loro utilizzo.

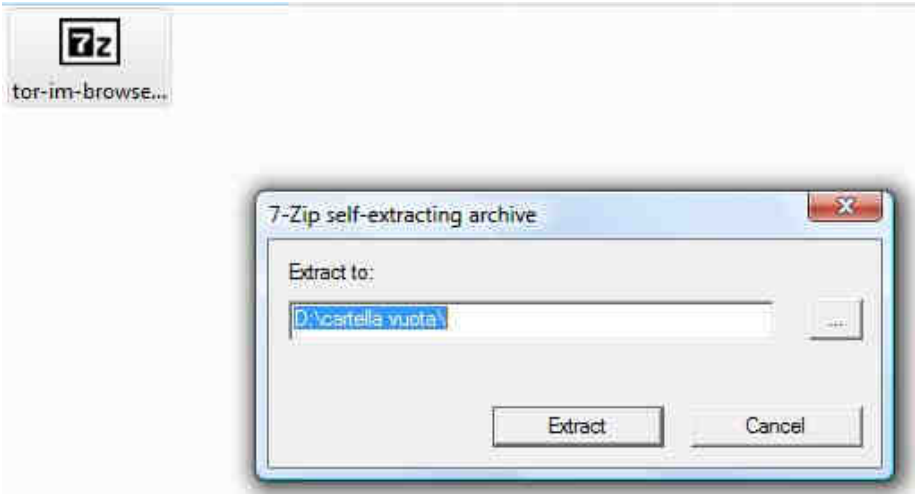
Basta una sola sessione di consultazione di una email senza l'uso di Tor per lasciare una traccia della vostra identità!

9. Uso del pacchetto Tor IM Browser per la navigazione anonima senza bisogno di installazione

Il programma **tor-im-browser-1.2.9_it.exe** (è la versione più aggiornata nel momento in cui scriviamo) lo potete scaricare, come mostrato nel punto 1 di questo manuale, dalla pagina **http://www.torproject.org/easy-download.html.it** . Questo programma, che qui chiameremo "Pacchetto Tor", è una versione di Tor in grado di funzionare subito senza essere installata. Questa versione crea una cartella che contiene tutti i programmi (compreso Firefox) già pronti per la navigazione anonima.

Copiate **tor-im-browser-1.2.9_it.exe** in una cartella del vostro computer vuota. Avviate questo programma.

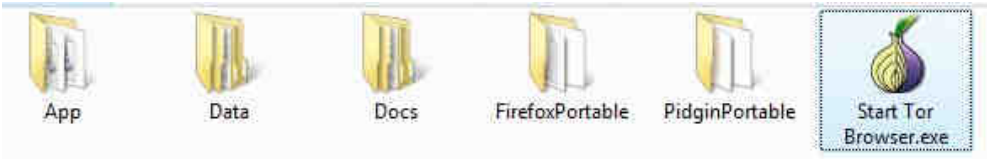
Vi appare una finestra in cui vi viene chiesto dove volete salvare il Pacchetto Tor. Vi viene proposta la stessa cartella in cui si trova il programma **tor-im-browser-1.2.9_it.exe**, (vedi immagine che segue). Fate click su *Extract*.



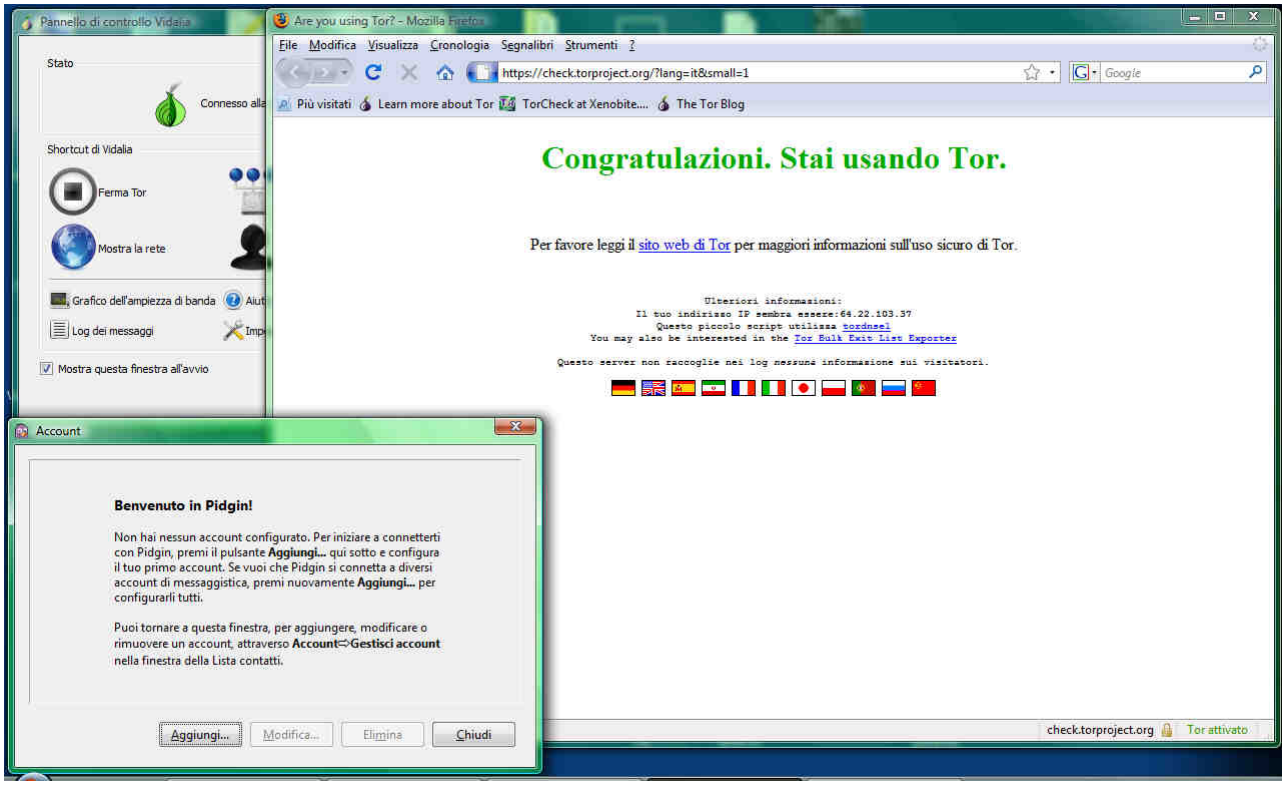
Dopo alcuni minuti verrà creata una cartella: "Tor Browser". Potete ora copiare la cartella su una chiavetta USB oppure lasciarla sul vostro computer, se ne fate un uso casalingo.

Per usare Tor, aprite la cartella "Tor Browser": all'interno troverete alcune cartelle e il programma **Start Tor Browser.exe**.

Fate partire questo programma. Dopo alcuni minuti partirà automaticamente Firefox.



Ecco cosa appare dopo aver avviato il programma *Start Tor Browser.exe*



La finestra *Pannello di controllo Vidalia* appare immediatamente dopo l'avvio. Poi appare la finestra *Account*. Infine si apre *Firefox*, una versione diversa da Firefox 3.5.5 .

La pagina iniziale di navigazione è già impostata sul sito di Tor in modo da controllare subito se state navigando in modo anonimo. La scritta in verde "Congratulazioni. Stai usando Tor." vi da la conferma che tutto funziona bene e potete proseguire la vostra sessione di navigazione anonima. La finestra Account serve a impostare il programma "Pidgin". In questo manuale non descriviamo l'utilizzo di questo programma. Pidgin è un programma che vi permette di comunicare direttamente (Instant Messenger) con altre persone collegate contemporaneamente ad internet.

Quindi come per la posta, è valido il discorso che siete anonimi, ma il contenuto della conversazione non è protetto. Sviluppate un buon linguaggio in codice e fatene un uso appropriato. Fate click sul tasto *Close* della finestra *Account* per chiudere Pidgin se non volete usarlo (se volete utilizzarlo documentatevi al seguente indirizzo: http://it.wikipedia.org/wiki/Pidgin_(software) o in inglese all'indirizzo: http://pidgin.im/about/).

Riprendo le considerazioni fatte all'inizio di queste istruzioni a proposito del "Pacchetto Tor".

Il "Pacchetto Tor" è importante perché vi permette di utilizzare Firefox in modo anonimo, senza dover fare la minima regolazione e senza installazione. Potete tenere questo programma su una chiavetta USB e usarlo da qualsiasi altro computer, senza doverlo installare. Utile in vacanza, nei cyber caffè o su qualsiasi altro computer a cui abbiate accesso: scuola, ufficio, ecc. Questo programma non ha bisogno di installazione, quindi non lascia traccia del suo uso, soprattutto se lo usate da una chiavetta USB. Queste caratteristiche lo rendono adatto soprattutto se si deve utilizzare la navigazione anonima quando si è in giro. Questa versione è quindi adatta ad un uso sporadico su computer diversi dal vostro, ma se non siete delle cime in computeristica o volete sperimentare subito la navigazione sicura potete benissimo utilizzare questa versione anche sul vostro computer personale. Le indicazioni generali sull'uso di Firefox 3.5 e Vidalia sono identiche per il **Pacchetto Tor**.

10. Ricordatevi che Tor protegge il vostro anonimato, non le informazioni che inviate

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.

Buon lavoro compagni!