

Le istruzioni per utilizzare Tor

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 (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, lo potete scaricare gratuitamente nella versione italiana al seguente indirizzo:

<http://www.mozillaitalia.it/archive/index.html#p1>

Vidalia, lo potete scaricare gratuitamente al seguente indirizzo:

<https://www.torproject.org/download.html.it>

Scegliete la versione per il vostro sistema operativo nella colonna “Scarica la versione stabile”. Nel momento in cui scriviamo la versione da scaricare (per Windows) è la seguente: **0.1.2.19**.

Il programma di installazione da scaricare (per il sistema operativo Windows) è il seguente:

<https://www.torproject.org/dist/vidalia-bundles/vidalia-bundle-0.1.2.19-0.0.16.exe>.

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 anche su altri sistemi operativi (Mac OS e Linux).

Le informazioni più dettagliate sono in inglese. Quindi ripassate le vostre nozioni d'inglese se volete utilizzare a fondo questo sito.

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

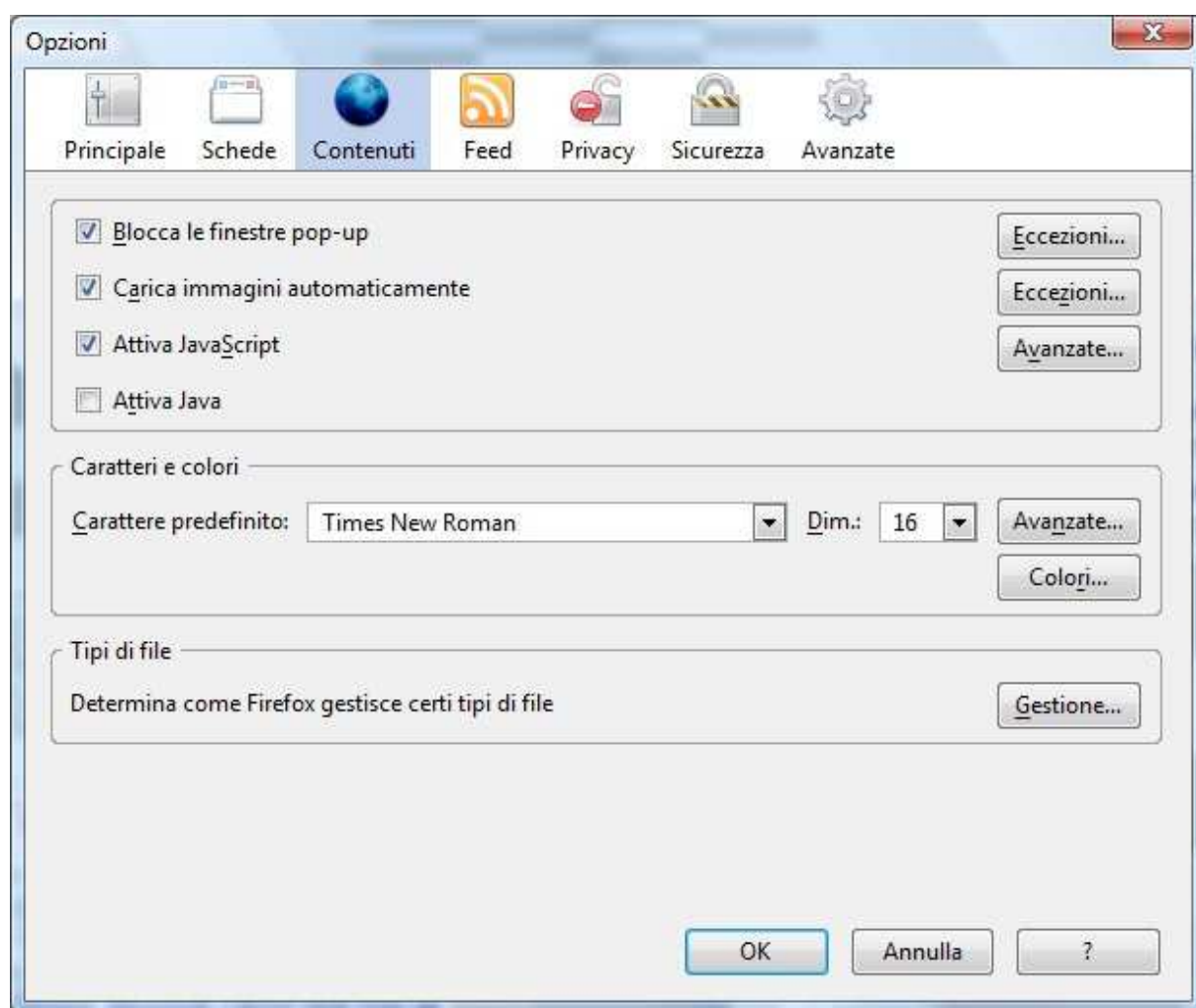
2. Installazione e configurazione

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.

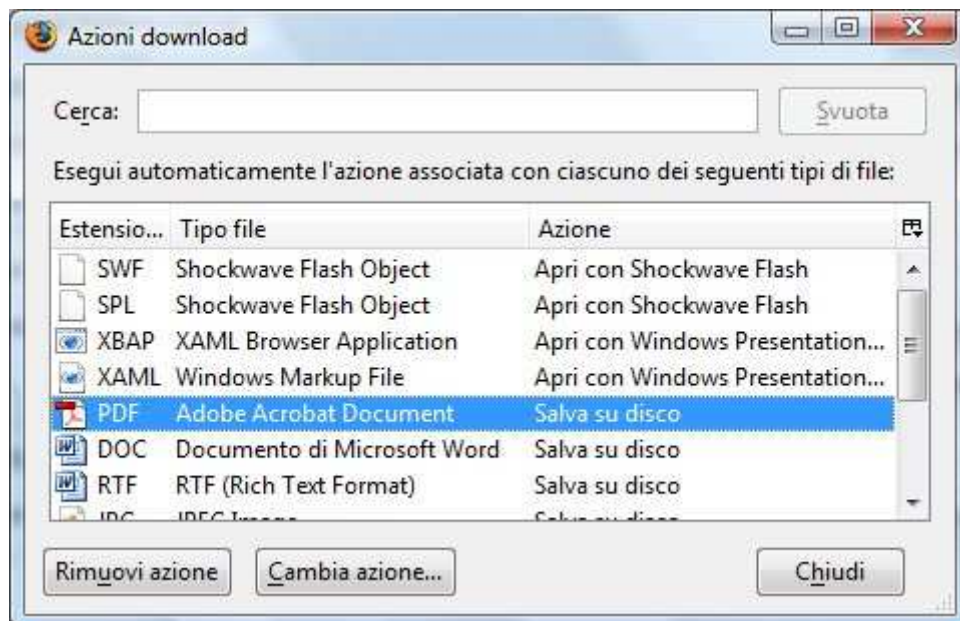
Dopo averlo installato, avviate Firefox e scegliete dal menu *Strumenti* la voce *Opzioni*. Scegliete poi dalla finestra che si apre l'area *Contenuti*, come nella figura qui sotto.



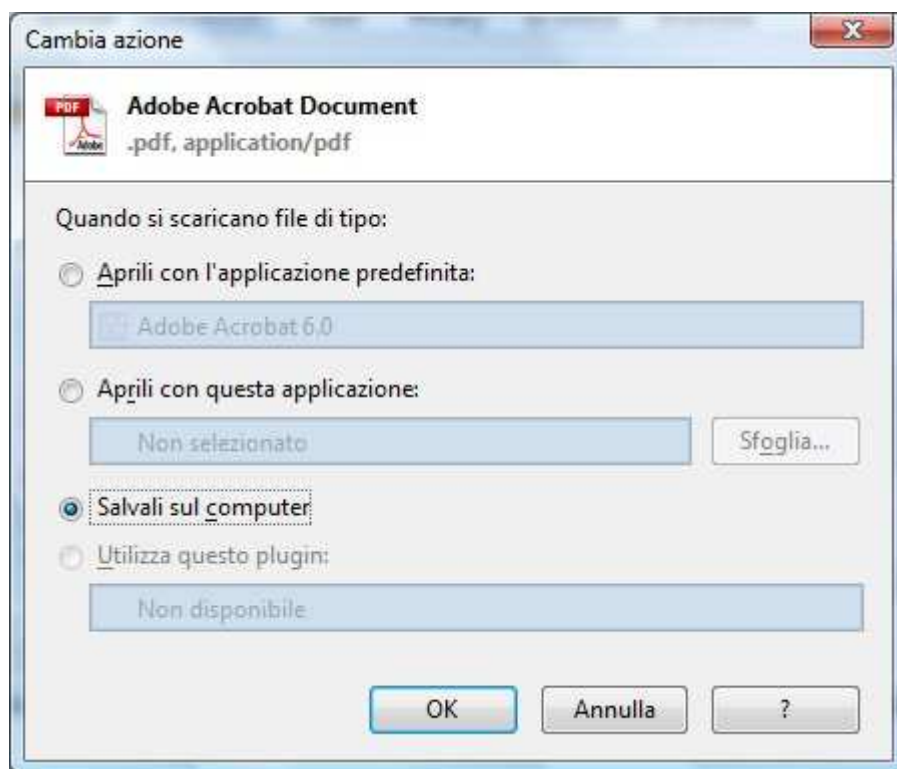
Disattivate Java: la voce *Attiva Java* deve apparire sprovvista del segno di spunta. Fate click su OK per registrare la modifica. Bisogna impedire l'esecuzione di Java durante la navigazione, poiché Java scavalca la protezione di Tor. Java è usato soprattutto nei programmi di Chat e in alcuni casi come interfaccia per aggiornare i siti Web o trasferire i file.

Sempre dall'area *Contenuti* fate click sul bottone *Gestione...* nella sezione *Tipi di file*.

Si apre la finestra mostrata nell'immagine qui sotto.



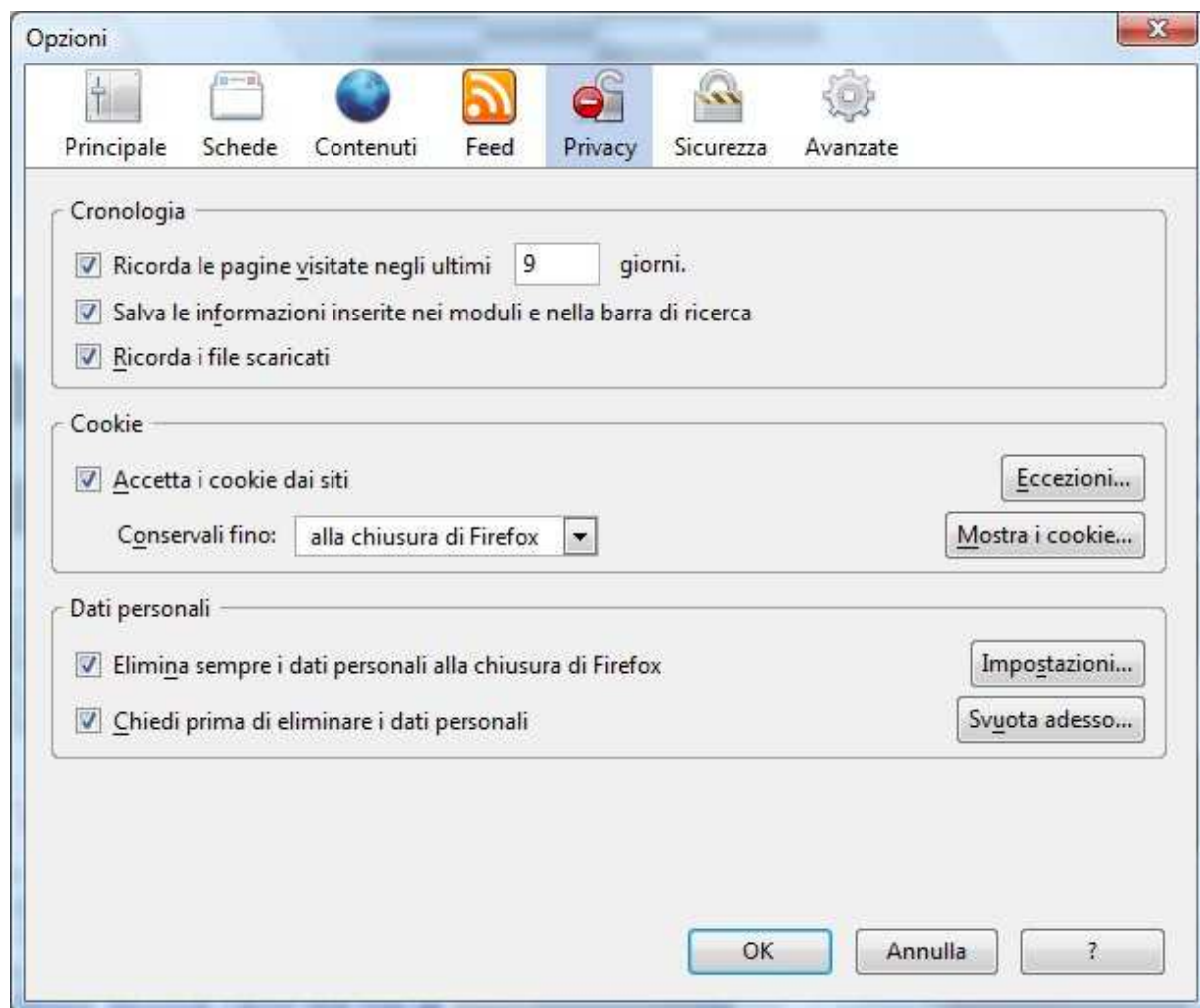
Scegliete *PDF* e poi fate click sul bottone *Cambia azione...*



Si apre un'ulteriore finestra, come quella mostrata qui sopra. Impostate *Salva sul computer*. 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 nella finestra *Cambia azione*, i file PDF vengono registrati sul disco del computer. Li potrete consultare tranquillamente alla fine del vostro collegamento con internet. Fate click su OK per registrare la modifica.

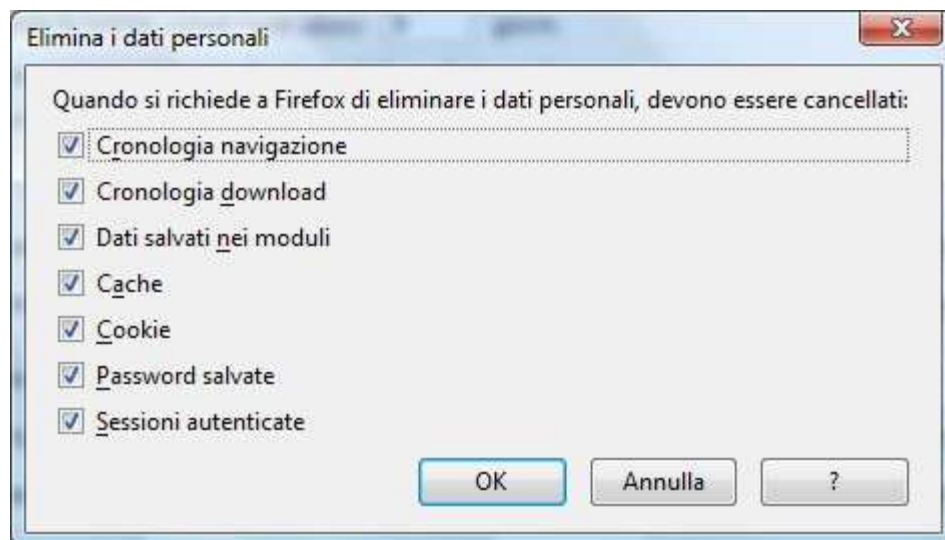
Sempre dalla finestra *Opzioni* scegliete l'area *Privacy* e impostate nella sezione *Cookie*, *Accetta i cookie dai siti* e impostate (premendo sul triangolino) accanto alla voce *Conservali fino*: la dizione *alla chiusura di Firefox*. In questo modo siete sicuri di cancellare alla fine della sessione di lavoro le tracce della vostra navigazione (vedi la figura in basso). 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.



Un'altra impostazione fondamentale per cancellare tutte le tracce della nostra navigazione e informazioni che possono identificarci è l'attivazione nella sezione *Dati personali*, sempre nell'area *Privacy* (vedi immagine qui sopra), della voce *Elimina sempre i dati personali alla chiusura di Firefox*. Deve essere presente il segno di spunta nella casella a sinistra di questa voce. Poi fate click sul bottone *Impostazioni*....

Vi si presenta un'ulteriore finestra, come quella riportata qui di seguito. Rendete attive tutte le voci, 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 (*Cronologia di navigazione*), i file che scaricate (*Cronologia download*), i dati che avete immesso nei moduli (*Dati salvati nei moduli*), come quelli ad esempio utilizzati per mettere parole d'ordine o per aprire una email, ecc. Verrà cancellata la *Cache* che è una cartella in cui il navigatore registra le pagine visitate per rendere la loro visualizzazione più rapida, ma che si ricorda dei siti che frequentate con maggiore assiduità e costituisce una specie di profilo della vostra "personalità internet". In particolare controllate che siano attivate le due ultime voci, *Password salvate* e *Sessioni autenticate*, è importante per non permettere di far scoprire le password che usate ai programmi e virus spioni, qualora si insinuino nel vostro sistema.

Queste impostazioni cancellano le informazioni alla fine dell'utilizzo di Firefox. Potete però cancellare queste informazioni anche durante l'utilizzo di Firefox scegliendo dal menu *Strumenti* la voce *Elimina i dati personali*.... In questo modo potete collegarvi a più siti, senza lasciare traccia del vostro percorso. Sarà più difficile individuarvi nel corso della navigazione.

Non create segnalibri con i siti che possono caratterizzarvi. Create segnalibri con i siti più comuni come Virgilio, Yahoo, Google o ai giornali borghesi che non danno la minima informazione agli spioni.

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 siate 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-0.1.2.19-0.0.16.exe**.

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**, che è un programma aggiuntivo per Firefox che vi permetterà di gestire il vostro anonimato più facilmente.

Per il suo corretto funzionamento il programma deve installare i seguenti programmi: Vidalia, Privoxy, Tor.

4. L'impostazione di Vidalia (e Tor)

Quando avviate Vidalia, vi si presenta la finestra seguente:



Disattivate la voce *Mostra questa finestra all'avvio*. Il simbolo di Vidalia (La cipolla) è di color verde se tutto funziona regolarmente. Per funzionare Vidalia ha bisogno che sia in funzione anche Privoxy: a destra nella barra in basso di Windows, deve essere presente l'icona di Privoxy (di norma Privoxy viene installato in modo che si avvii automaticamente all'accensione del computer). Il simbolo di Privoxy è un disco blu con una P bianca al centro, come nella figura che segue. Se presente, indica che il programma è in funzione.

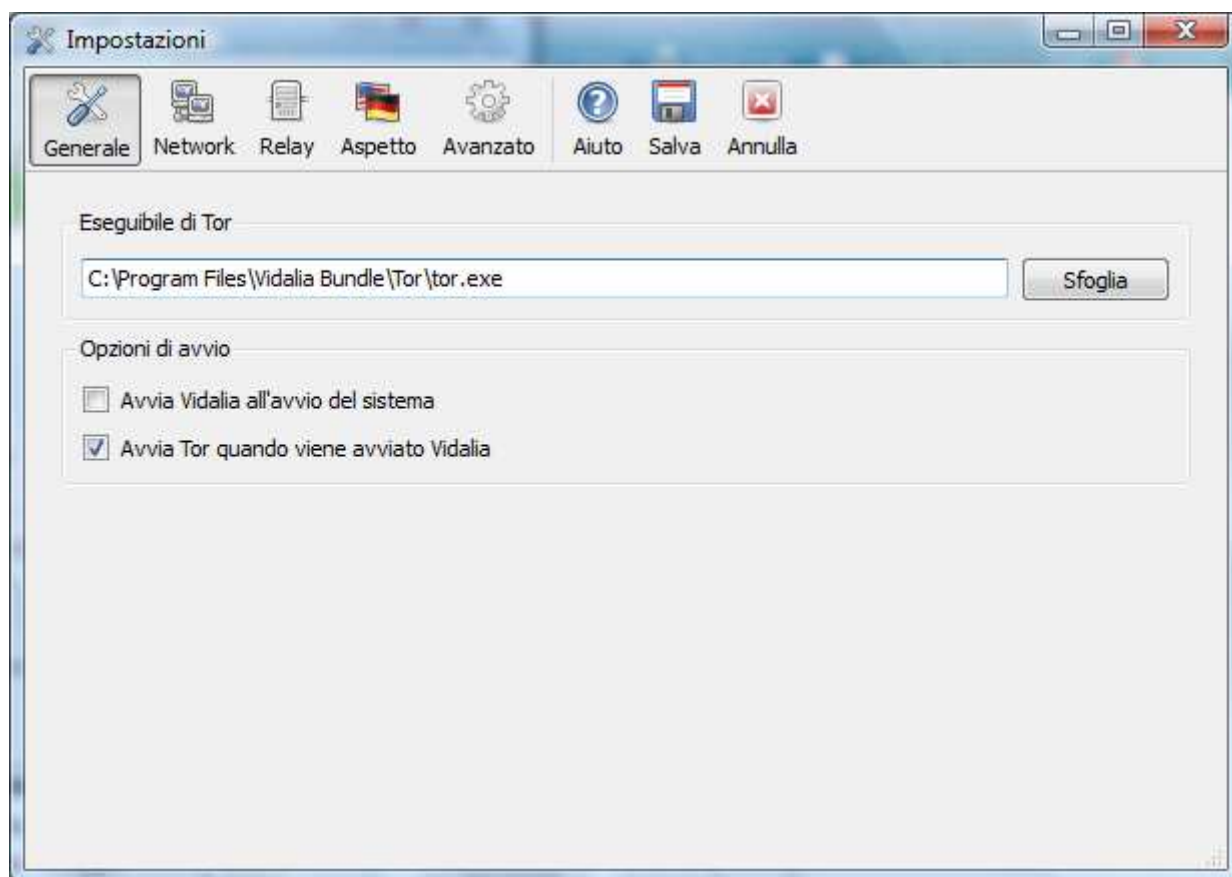


In questa immagine, c'è anche il simbolo di Vidalia (la cipolla), che indica, se è di color verde, il suo corretto funzionamento. Tor per funzionare ha bisogno che questi due programmi funzionino correttamente e contemporaneamente. Vidalia e Privoxy funzionano anche se non siete collegati a internet. Potete avviarli manualmente anche dopo che vi siete collegati a internet, attraverso il menu dei programmi di Windows.

Prima di continuare dovete fare le seguenti altre impostazioni.

Aprirete il *Pannello di Controllo Vidalia* (vedi figura in alto in questa pagina). Lo potete aprire facendo doppio click sul simbolo del programma, la cipolla nella barra in basso di Windows.

Fate click su *Impostazioni*. Vi appare la finestra seguente:



Selezionate l'area *Generale*. La voce *Avvia Tor quando viene avviato Vidalia* **deve essere imperativamente attivata**. La voce *Avvia Vidalia all'avvio del sistema*, consiglio di lasciarla disattivata e di avviare il programma manualmente solo quando dovete collegarvi in modo anonimo a internet. Fate click sul bottone a forma di dischetto *Salva*, per registrare la vostra scelta. Non attivate il *Relay*(1) se non siete capaci di gestire il firewall del router internet, pena il malfunzionamento al riavvio di Vidalia e la conseguente necessità di installare di nuovo Vidalia per correggere il malfunzionamento. Non variate le altre impostazioni. Quando sarete più esperti e vorrete installare il *Relay*, 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:

1. Attivare il *Relay* 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

Se non sono avviati, avviate Vidalia e Privoxy. Controllate sempre le icone nella barra in basso a destra per sapere se i programmi sono avviati. **Il solo fatto che i due programmi siano 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 dovreste 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.

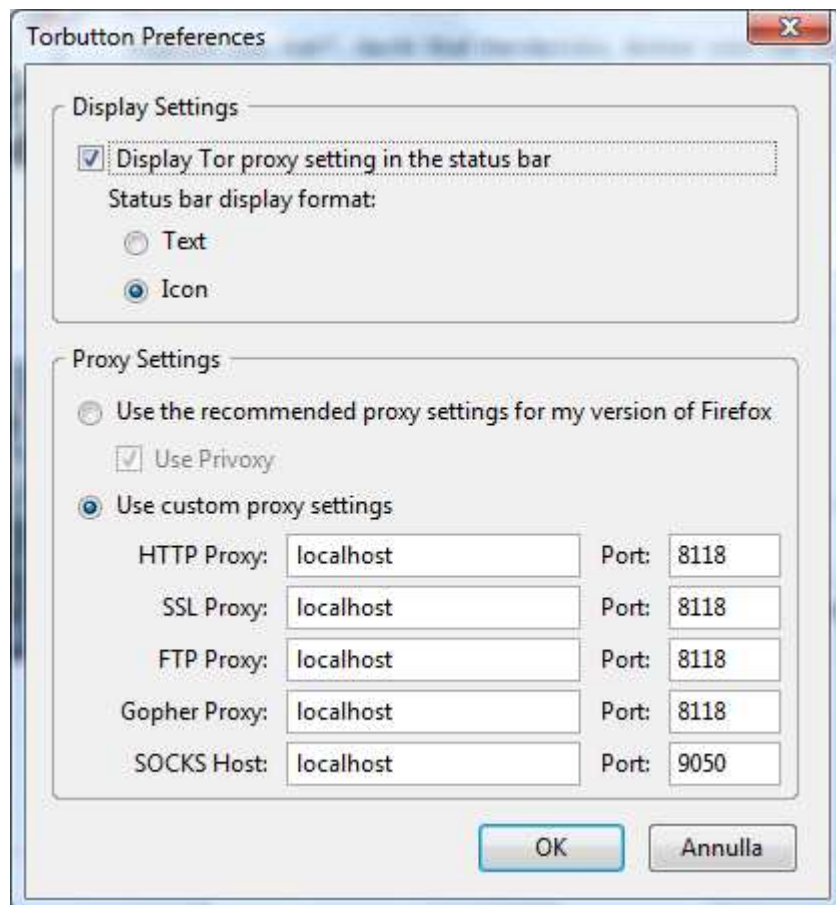
Avviamo Firefox. Se Vidalia si è correttamente installato, in basso a destra in Firefox deve essere presente, come nell'immagine che segue, la scritta in verde *Tor Enabled*.



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. In questa finestra 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.

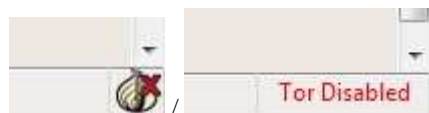
Ricopiate esattamente i valori impostati così come appaiono nell'immagine. Fate in modo che anche sul vostro computer siano impostati gli stessi valori.



Selezionate, nella sezione *Display setting*, *Icon* invece di *Text*. La scritta verde Tor Enabled in basso a destra verrà sostituita da un'icona più visibile come nell'immagine che segue



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

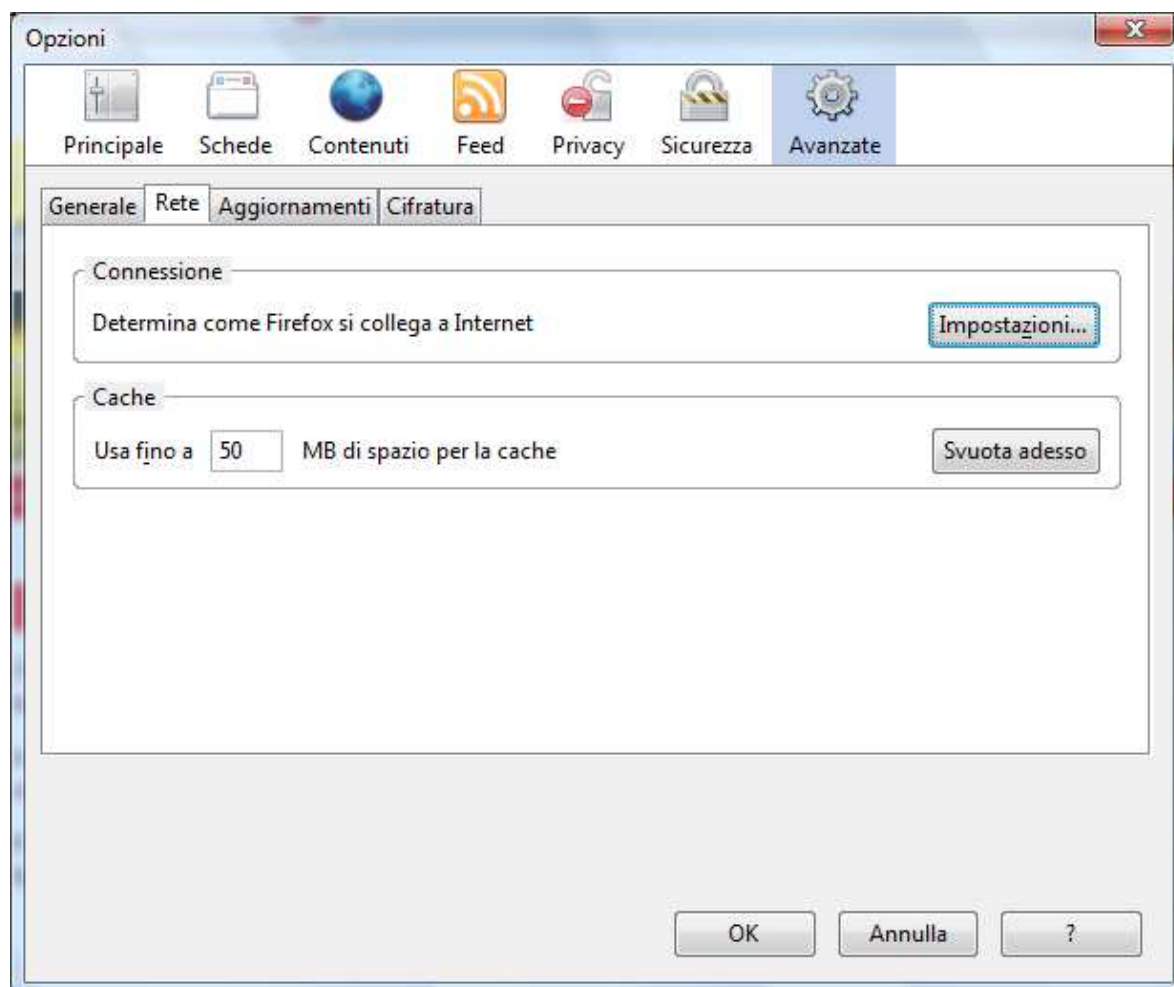


vuol dire che non avete scelto di attivare Tor per la navigazione. Fate click sull'icona o sulla scritta per attivare Tor. Quando Tor è in funzione la scritta deve essere verde oppure la cipolla non deve avere la X rossa, in questa condizione state navigando in modo anonimo.

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 di una sessione di navigazione anonima.

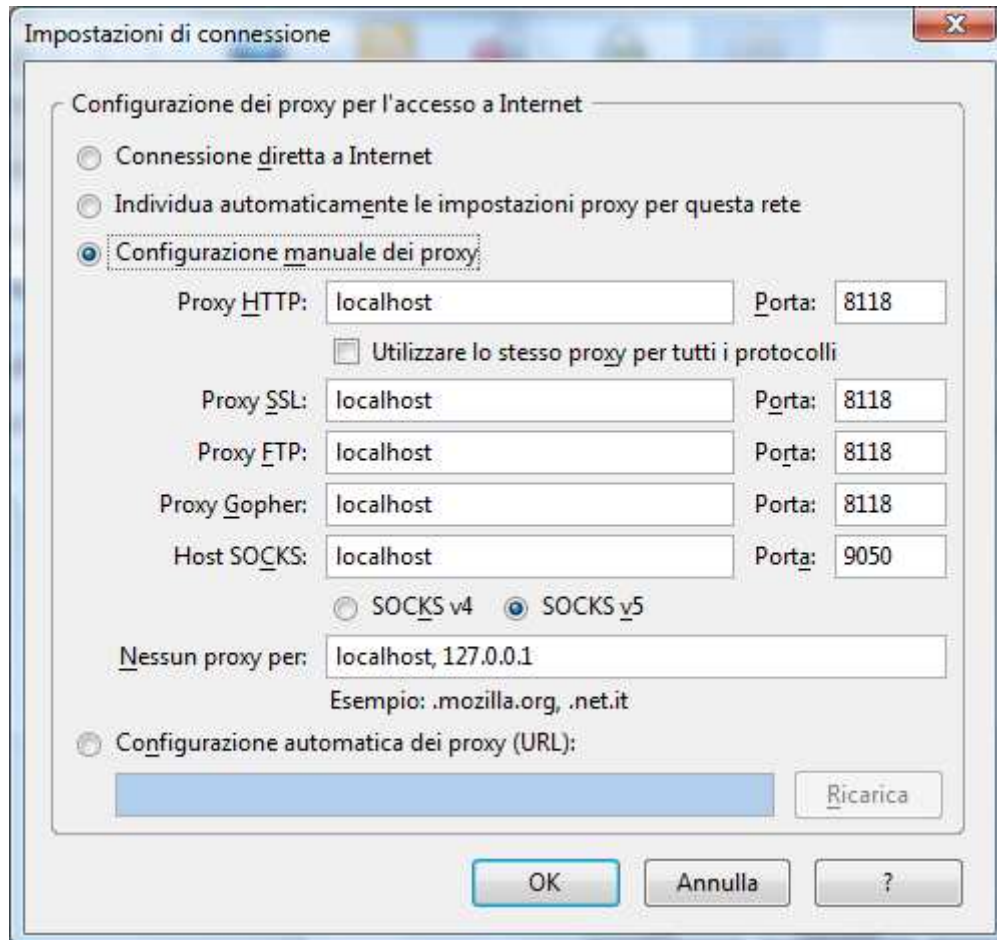
Se l'installazione di Tor non è riuscita a inserire in Firefox questa estensione (Torbutton), dovete impostare i valori per collegarvi a Tor attraverso il menu di Firefox.

In questo caso selezionate dal menu di Firefox - *Strumenti* la voce *Opzioni*, vi appare la finestra *Opzioni* (vedi qui sotto),



Selezionate l'area *Avanzate*. Selezionate la scheda *Rete* e fate click sul bottone *Impostazioni...* nella sezione *Connessione*.

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



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

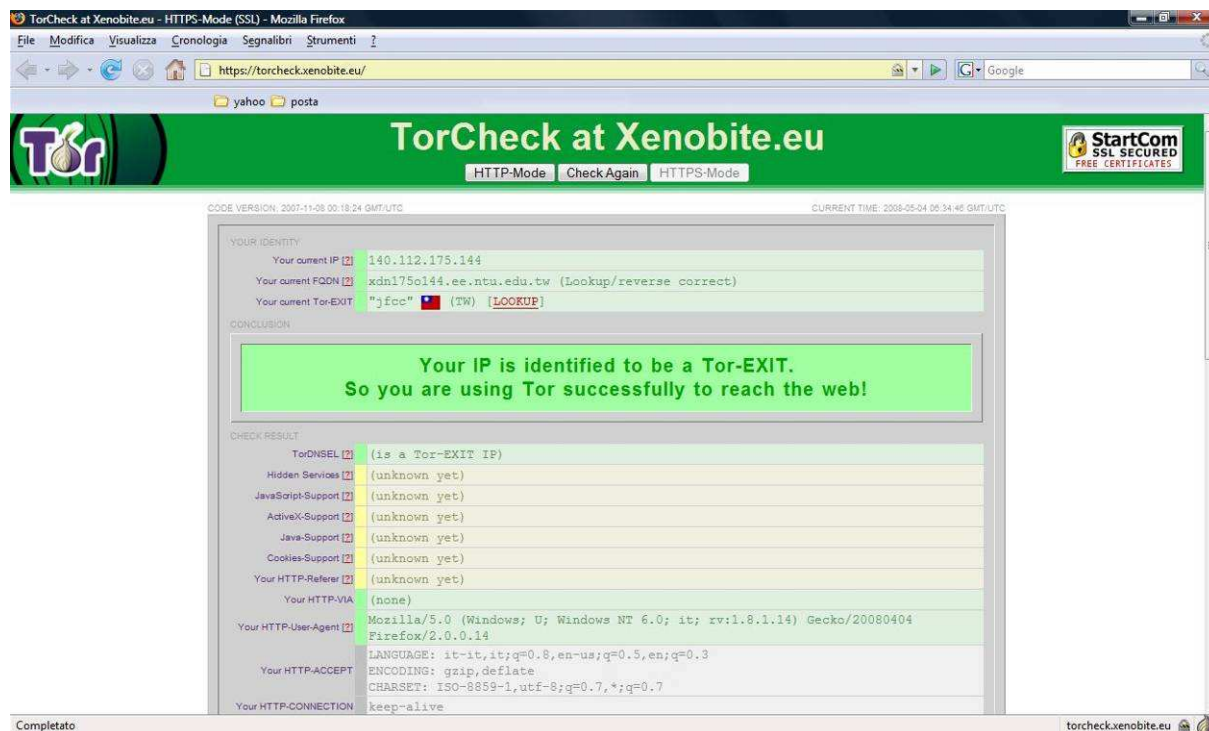
Queste sono le ultime impostazioni necessarie per la navigazione anonima con Firefox e Tor.

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.

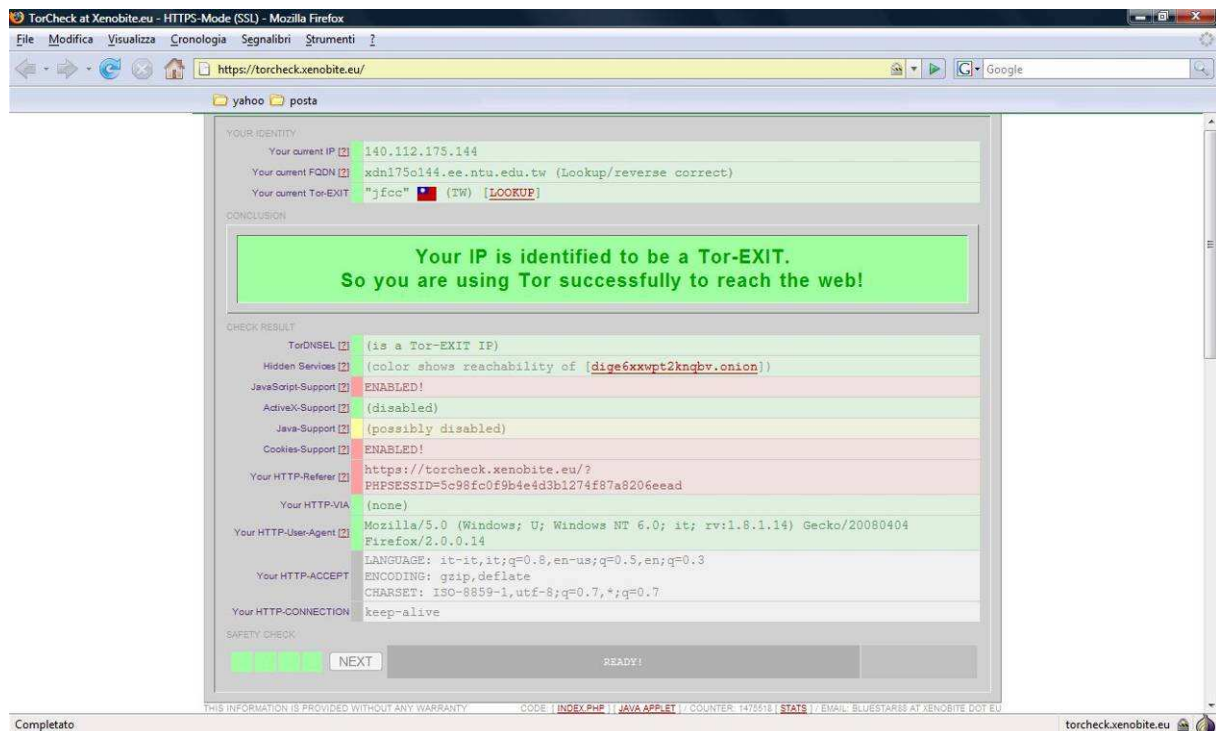
Se non lo siete, appare la scritta seguente:



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. Anche se il colore non è verde, questo indica che Java non funziona, che è disabilitato. Non confondete Java con JavaScript, sono due cose molto diverse. Notate che JavaScript-support è segnalato in rosso.

Se ritornate nel parte 2. in cui queste istruzioni descrivono l'installazione e la configurazione di Firefox, vedrete 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 inviare 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. Le contromisure sono la loro cancellazione anche durante la navigazione, attraverso la voce del menu *Strumenti / Elimina i dati personali...*

Se volete verificare l'efficacia della cancellazione dei Cookie, potete visitare una casella email di Yahoo, identificatevi, controllate la posta in arrivo, cancellate i Cookie mentre siete all'interno della vostra email. Constatere che dopo la cancellazione sarete costretti a reidentificarvi. Le impostazioni legate a quella sessione di consultazione della email sono state cancellate, Yahoo 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 modo da non presentarsi con eventuali informazioni personali quando si rivisitano le stesse pagine.

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 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 non dà segnali di vita. Un sistema per sbloccare operazioni troppo lunghe è cambiare l'identità come sopra descritto. Un'altra più drastica è terminare la sessione: arrestare Vidalia e farlo ripartire e reiniziare 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, quelle 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, manteniamo per esse l'anonimato. 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. Ricordatevi che Tor protegge il vostro anonimato, non le informazioni che inviate

Attenzione! Il sistema Tor protegge l'identità di chi invia 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 di questa caratteristica di Tor.

Buon lavoro compagni!