S7-L4
Tor

Emanuele Benedetti | 23 gennaio 2025

Consegna

Da Kali, scaricare e provare Tor Browser (senza modificare alcuna impostazione predefinita).

Effettuare qualche navigazione sulla rete tor ed effettuare screenshot per il report

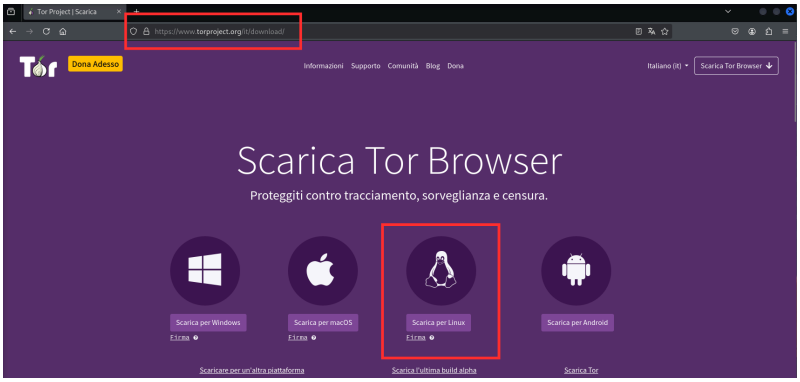
Bonus

Installare Tails OS su macchina virtuale

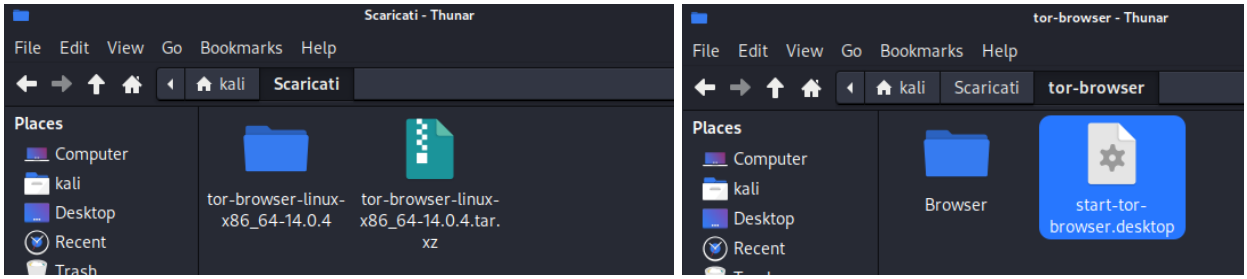
Svolgimento

Tor Browser è un browser che utilizza la rete Tor (The Onion Router) per cifrare il traffico e instradarlo attraverso una serie di nodi distribuiti nel mondo, rendendo difficile tracciare l'origine della connessione.

Per installarlo su Kali Linux sono andato sul sito ufficiale di Tor Project (https://www.torproject.org/it/download) ed ho selezionato "*Scarica per Linux*"



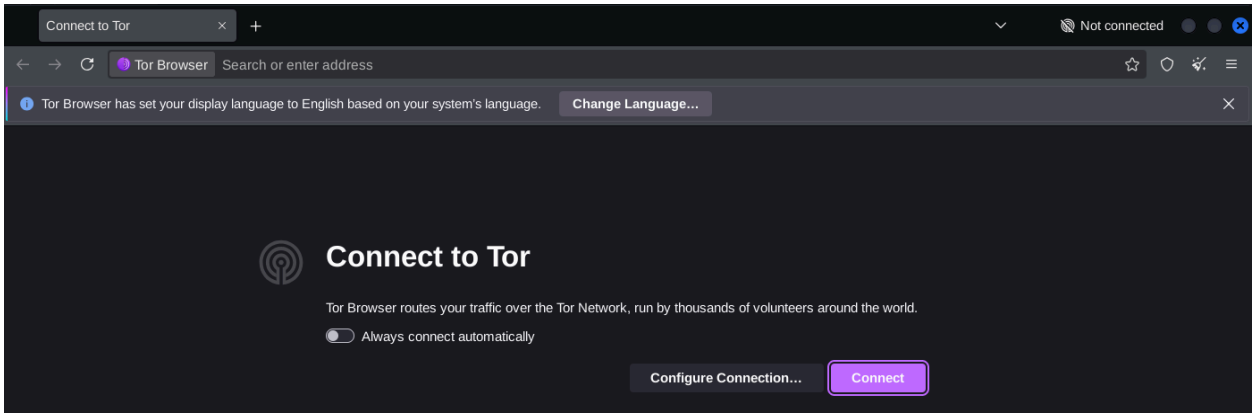
Entrando nella cartella estratta dal file scaricato, possiamo avviare il browser Tor.



Dopo qualche secondo di caricamento il browser si avvia correttamente e chiede di connettersi alla rete Tor. Alcuni vantaggi principali di Tor sono:

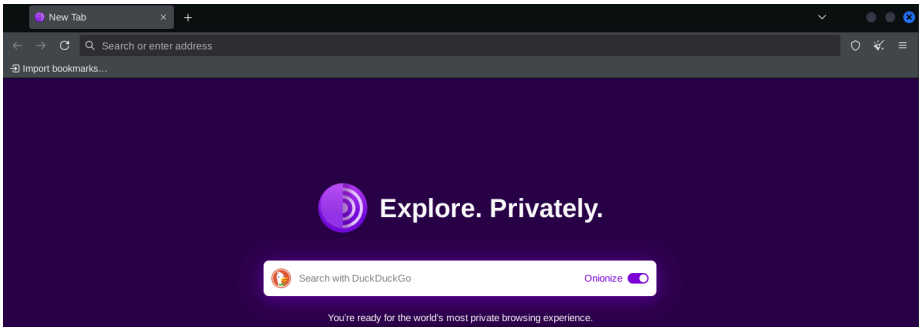
1. **Anonimato**: maschera l'indirizzo IP
2. **Crittografia**: i dati vengono cifrati durante il loro percorso attraverso la rete Tor, aumentando la sicurezza.
3. **Accesso a contenuti censurati**: in alcune regioni dove internet è censurato, Tor può aiutare ad aggirare queste restrizioni.

Tuttavia, è importante notare che non è completamente invulnerabile e che l'uso di Tor non garantisce sempre l'anonimato totale. Inoltre, la navigazione è più lenta rispetto ai browser tradizionali, dato che il traffico viene instradato attraverso più nodi e crittografato.

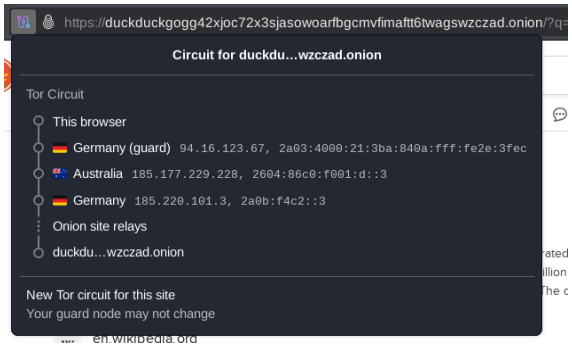


Connettiamo il browser alla rete Tor cliccando su "*connect*".

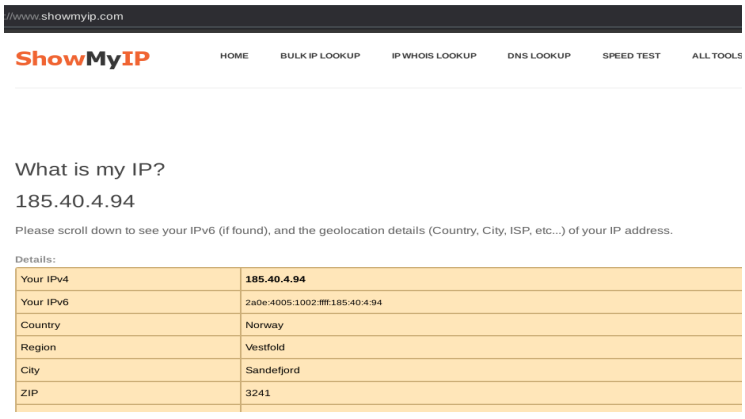
Nella schermata home possiamo selezionare il toogle “*Onionize*”, che permette di utilizzare la sua versione Onion di Duckduckgo garantendo maggiore privacy e anonimato.



Come mostrato nella seguente immagine il browser ci mostra a quali nodi della rete siamo connessi, compresi gli indirizzi IP.



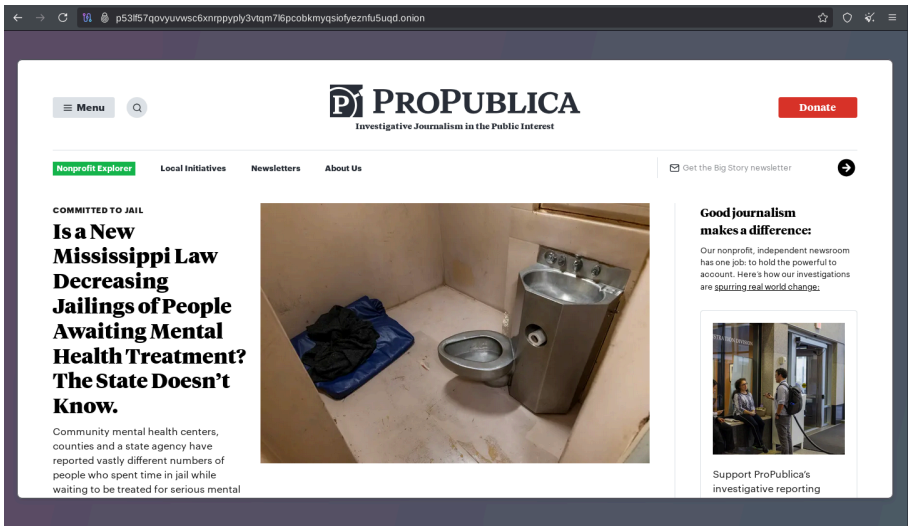
Possiamo verificare il nostro indirizzo tramite https://www.showmyip.com/



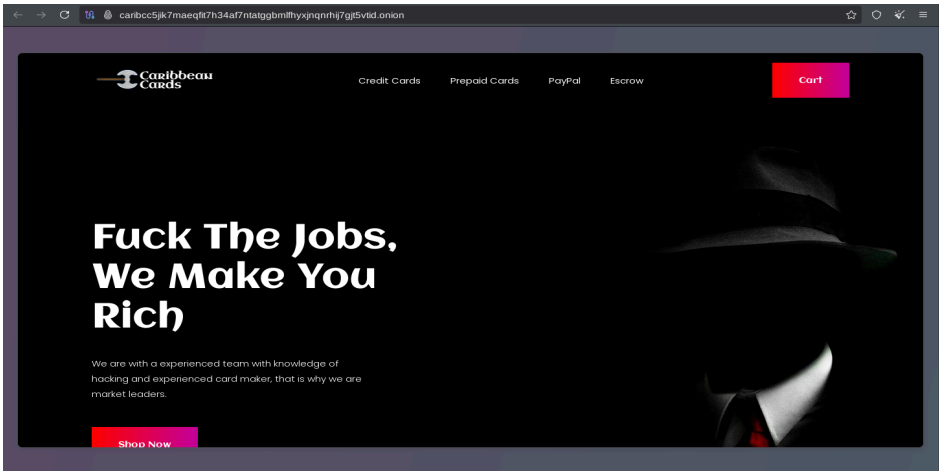
In questo caso il browser ha già ruotato il nostro IP che ora è localizzato in Norvegia

Possiamo effettuare una qualsiasi ricerca, come ad esempio su siti di informazione libera e/o indipendente presenti nel dark web. Poiché il dark web è popolato da attività illegali dobbiamo prestare attenzione ai risultati che otteniamo.

In questo caso ho cercato il noto sito ProPublica, un'organizzazione giornalistica senza scopo di lucro che si concentra su inchieste investigative di grande impatto. Si occupa di temi come la corruzione, le disuguaglianze sociali e i diritti civili.

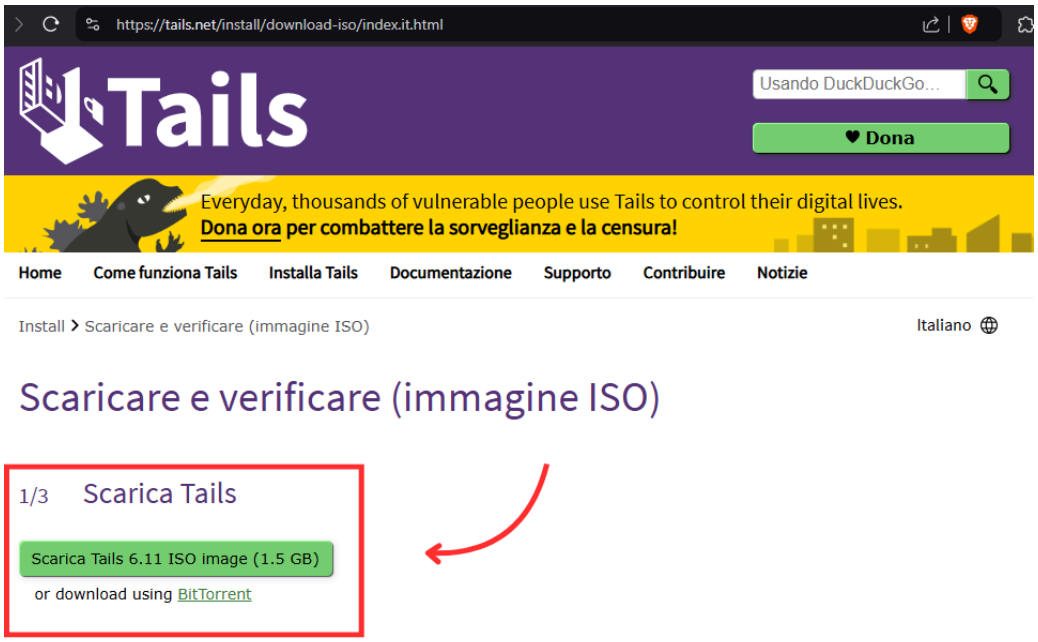


Potremmo anche avere accesso a siti per la vendita di materiale potenzialmente illegale, come quello mostrato nell'immagine che segue, che offre carte prepagate e carte di credito.

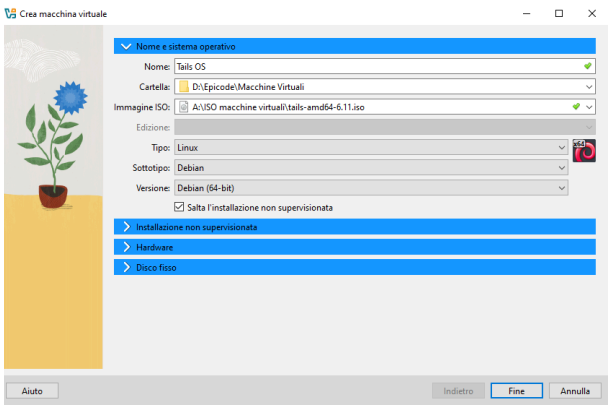


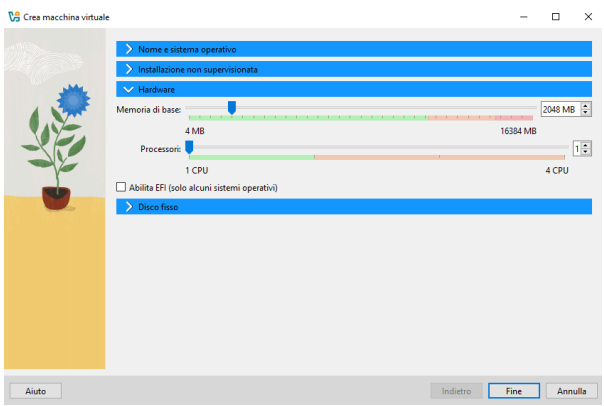
Bonus

Per installare Tails OS su macchina virtuale mi sono collegato al sito ufficiale https://tails.net/ ed ho selezionato il file .iso del sistema operativo, presente nella sezione download (https://tails.net/install/download-iso/index.it.html).

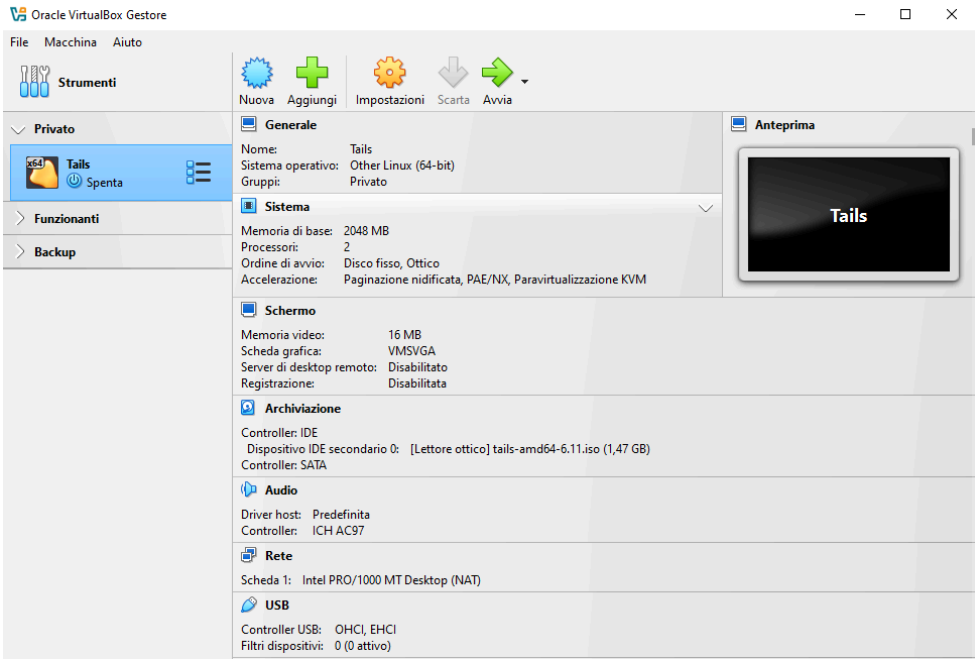


Dopo aver completato il download, ho avviato VirtualBox e creato una nuova macchina virtuale. Ho aggiunto nome della macchina, cartella di destinazione e il file .iso appena scaricato. Nella sezione hardware ho infine impostato la potenza della macchina in base alle necessità.





Poiché Tails è pensato per essere usato da una chiavetta USB o un DVD, in modo che non lasci tracce sul computer una volta spento, non è necessario creare ed aggiungere un disco fisso virtuale. Una volta completata la configurazione ho verificato dalla schermata principale che tutto fosse corretto ed avviato la macchina

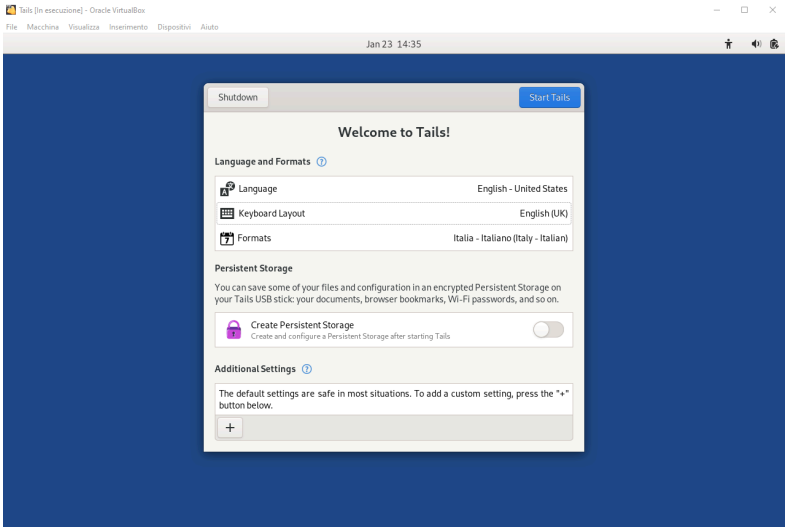


Come evidenziato sul sito di Tails, il sistema operativo è pensato per essere eseguito completamente su una chiavetta USB o un DVD. Poiché stiamo effettuando la configurazione su una macchina virtuale è bene ricordare che:

"*Eseguire Tails all'interno di una macchina virtuale comporta diverse implicazioni per la sicurezza. Se il sistema operativo ospite è compromesso da un software keylogger o altro malware, potrebbe compromettere le funzionalità di sicurezza di Tails. È probabile che vengano lasciate tracce della tua sessione di Tails sul disco rigido locale. Ad esempio, i sistemi operativi ospiti di solito utilizzano lo swapping (o paging), che copia parte della RAM sul disco rigido.*"

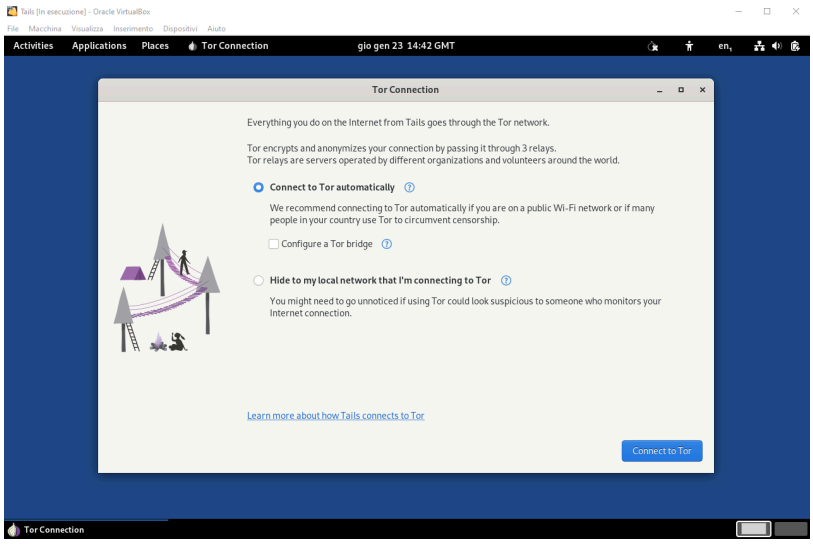
Dopo le dovute premesse possiamo continuare con l'avvio della macchina. Ad ogni avvio, il sistema mostrata una finestra di configurazione in cui è possibile selezionare la lingua e i formati ma soprattutto abilitare la memoria

persistente della macchina e l'utente root. Questo poiché Tails è pensato per essere eseguito su macchine diverse e in contesti potenzialmente rischiosi, garantendo privacy e sicurezza.



Ho selezionato le mie impostazioni e non ho abilitato la memoria persistente. In questo modo tutti i file e i dati presenti nella macchina al momento dello spegnimento verranno cancellati per sempre.

Avviamo la macchina con il tasto *Start Tails* e aspettiamo il caricamento del sistema. Tutto il traffico internet su Tails avviene tramite la rete Tor, pertanto ci viene subito chiesto in che modo vogliamo connetterci. Lasciamo la modalità automatica e clicchiamo su *Connect to Tor*.



A questo punto possiamo usare regolarmente il sistema, avviando ad esempio il browser Tor per eseguire le ricerche in maniera sicura.