

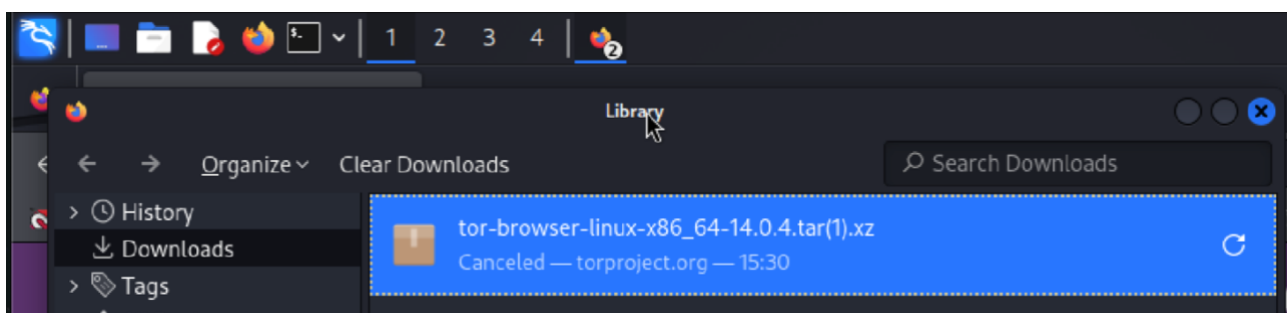
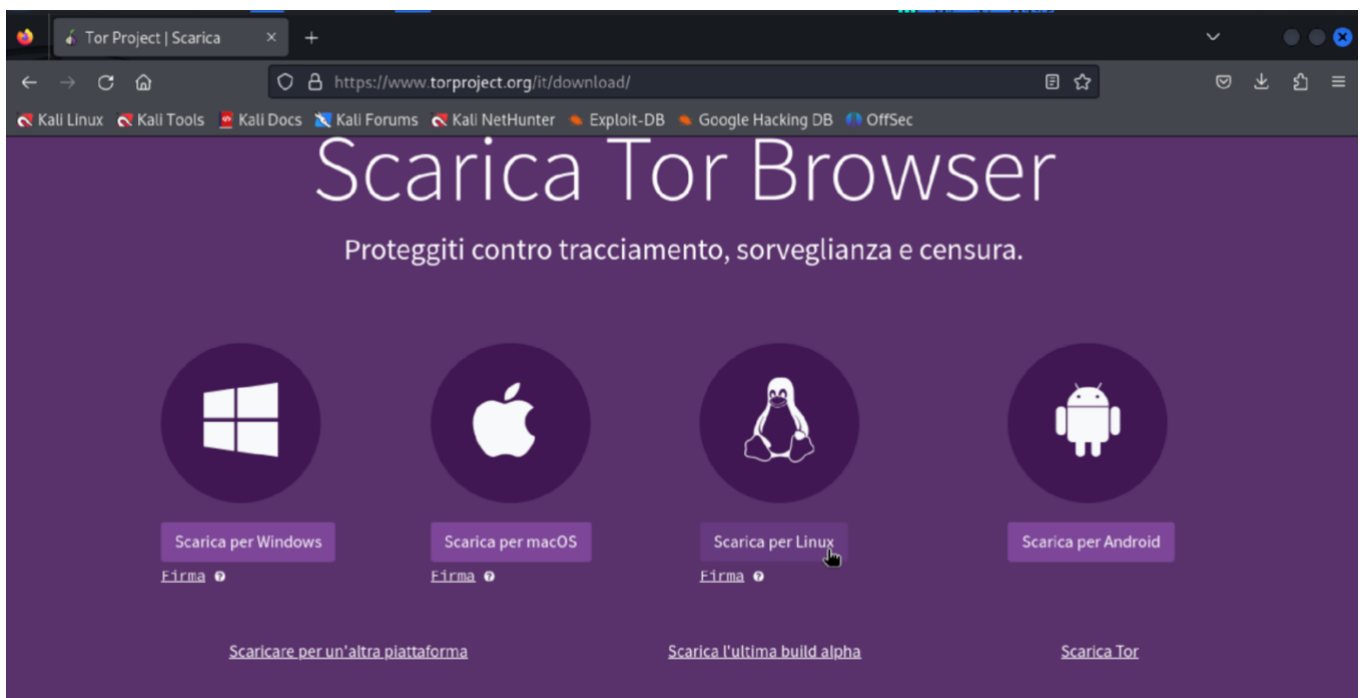
ESERCIZIO GIORNALIERO S7L4 (TOR)

Traccia:

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

Effettuare qualche navigazione sulla rete Tor ed effettuare screenshot per il report.

Per eseguire questo esercizio, prima di tutto avvio la macchina kali e mi reco sul sito torproject.org, dal quale andrò a scaricare il file per installare Tor Browser.



Una volta scaricata la versione Linux, procedo con l'installazione.

Per farlo, dal terminale mi reco nella cartella Downloads, e una volta dentro posso procedere con il comando per l'estrazione del file scaricato, ovvero:

tar -xvf tor-browser-linux-x86_64-14.0.4.tar.xz

```
(francesco@kali)-[~]
$ cd Downloads

(francesco@kali)-[~/Downloads]
$ ls
Metasploitable_wr6h7y.pdf  Nessus-10.8.3-debian10_amd64.deb  starting_point_FrancescoZac.ovpn  tor-browser-linux-x86_64-14.0.4.tar.xz

(francesco@kali)-[~/Downloads]
$ tar -xvf tor-browser-linux-x86_64-14.0.4.tar.xz
tor-browser/
tor-browser/Browser/
tor-browser/Browser/.config/
tor-browser/Browser/.config/gtk-3.0/
tor-browser/Browser/.config/gtk-3.0/settings.ini
tor-browser/Browser/TorBrowser/
tor-browser/Browser/TorBrowser/Data/
tor-browser/Browser/TorBrowser/Data/Browser/
tor-browser/Browser/TorBrowser/Data/Browser/Caches/
tor-browser/Browser/TorBrowser/Data/Browser/profile.default/
tor-browser/Browser/TorBrowser/Data/Browser/profile.default/extensions/
tor-browser/Browser/TorBrowser/Data/Browser/profile.default/extensions/{73a6fe31-595d-460b-a920-fcc0f8843232}.xpi
tor-browser/Browser/TorBrowser/Data/Browser/profiles.ini
tor-browser/Browser/TorBrowser/Data/Tor/
tor-browser/Browser/TorBrowser/Data/Tor/geoip
tor-browser/Browser/TorBrowser/Data/Tor/geoip6
tor-browser/Browser/TorBrowser/Data/Tor/torrc
tor-browser/Browser/TorBrowser/Data/Tor/torrc-defaults
tor-browser/Browser/TorBrowser/Docs/
tor-browser/Browser/TorBrowser/Docs/ChangeLog.txt
tor-browser/Browser/TorBrowser/Docs/Licenses/
tor-browser/Browser/TorBrowser/Docs/Licenses/Firefox.txt
tor-browser/Browser/TorBrowser/Docs/Licenses/Libevent.txt
tor-browser/Browser/TorBrowser/Docs/Licenses/NoScript.txt
tor-browser/Browser/TorBrowser/Docs/Licenses/Noto-CJK-Font.txt
tor-browser/Browser/TorBrowser/Docs/Licenses/Noto-Fonts.txt
tor-browser/Browser/TorBrowser/Docs/Licenses/PluggableTransports/
tor-browser/Browser/TorBrowser/Docs/Licenses/PluggableTransports/LICENSE
tor-browser/Browser/TorBrowser/Docs/Licenses/PluggableTransports/LICENSE.CC0
tor-browser/Browser/TorBrowser/Docs/Licenses/PluggableTransports/LICENSE.GO
tor-browser/Browser/TorBrowser/Docs/Licenses/PluggableTransports/LICENSE.SNOWFLAKE

tor-browser/Browser/start-tor-browser
tor-browser/Browser/start-tor-browser.desktop
tor-browser/Browser/tbb_version.json
tor-browser/Browser/update-settings.ini
tor-browser/Browser/updater
tor-browser/Browser/updater.ini
tor-browser/Browser/vaapitest
tor-browser/start-tor-browser.desktop

(francesco@kali)-[~/Downloads]
$
```

Una volta completata l'estrazione, posso procedere con l'avvio:

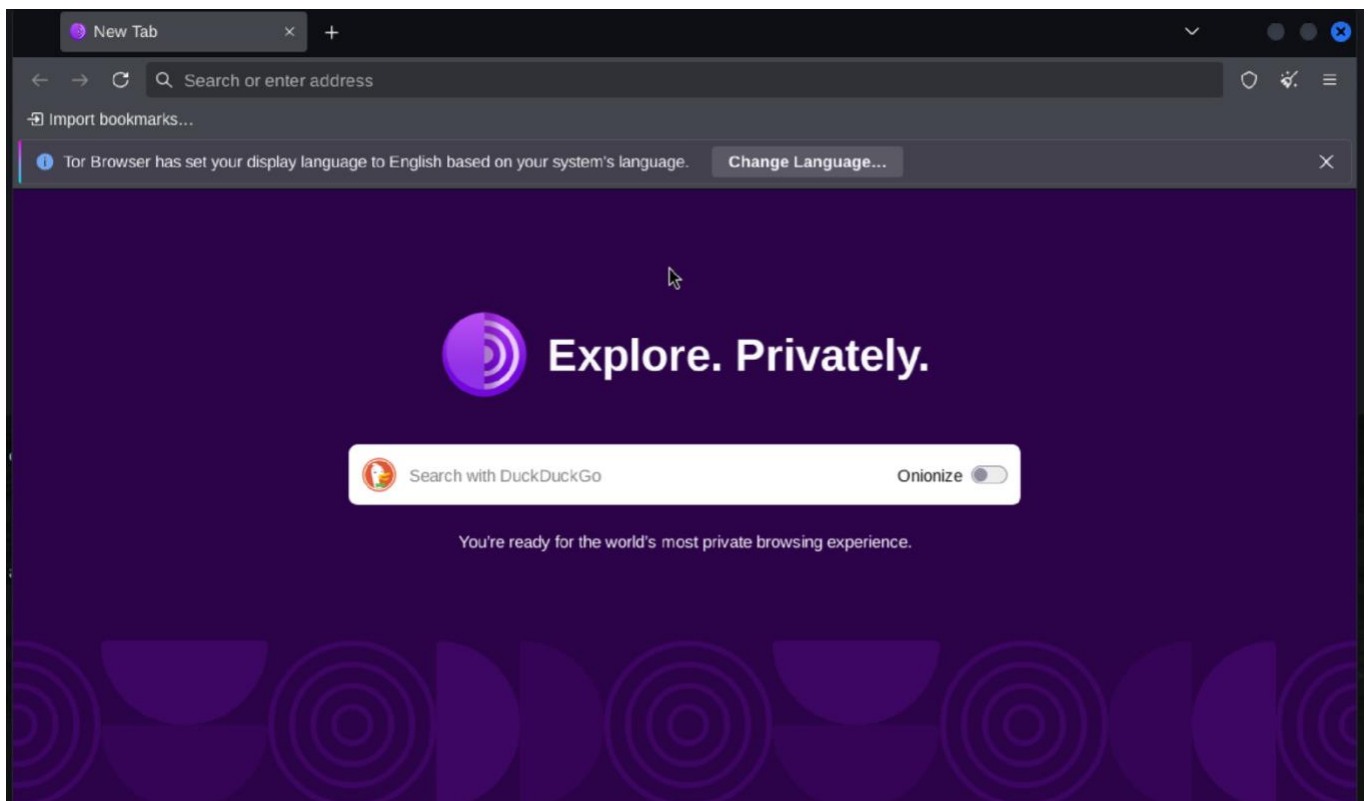
per farlo, mi reco all'interno della cartella nella quale è stato estratto il file:

cd Downloads

cd tor-browser

ed una volta entrato nella cartella, avvio il browser con il seguente comando:

./start-tor-browser.desktop

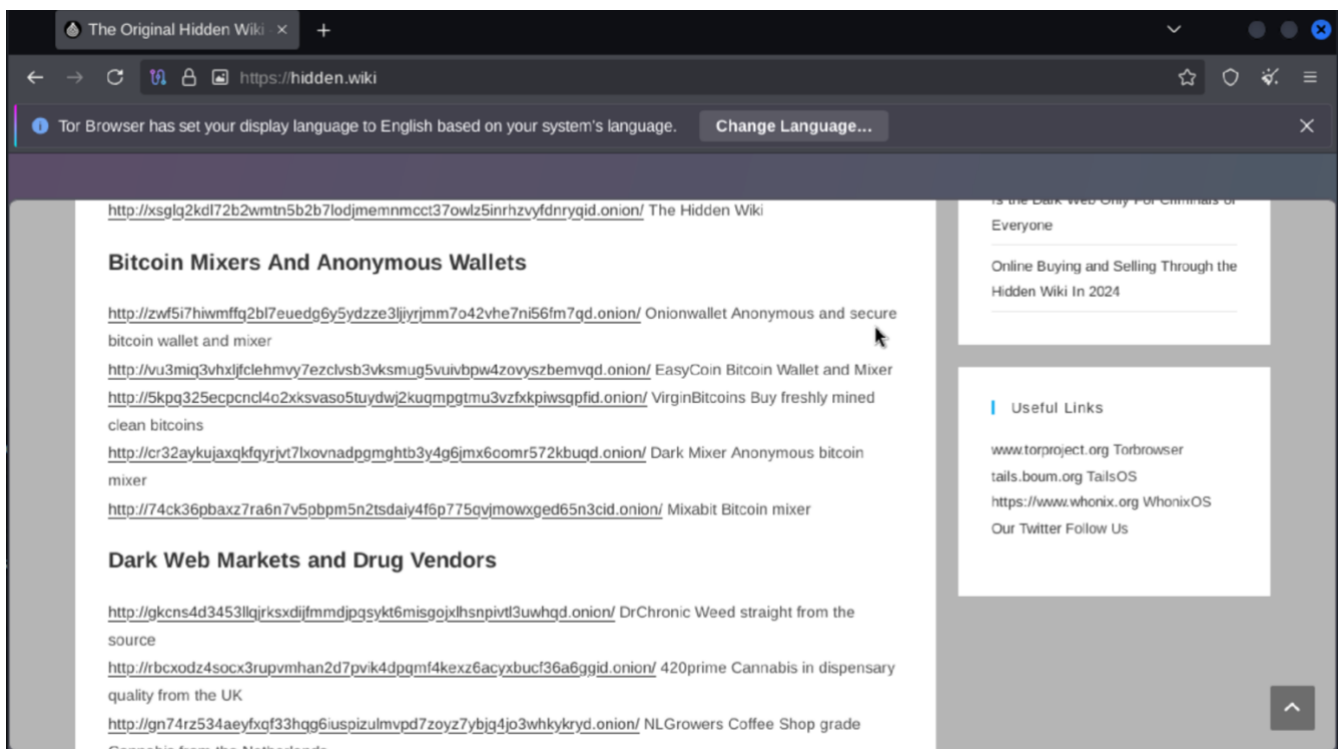
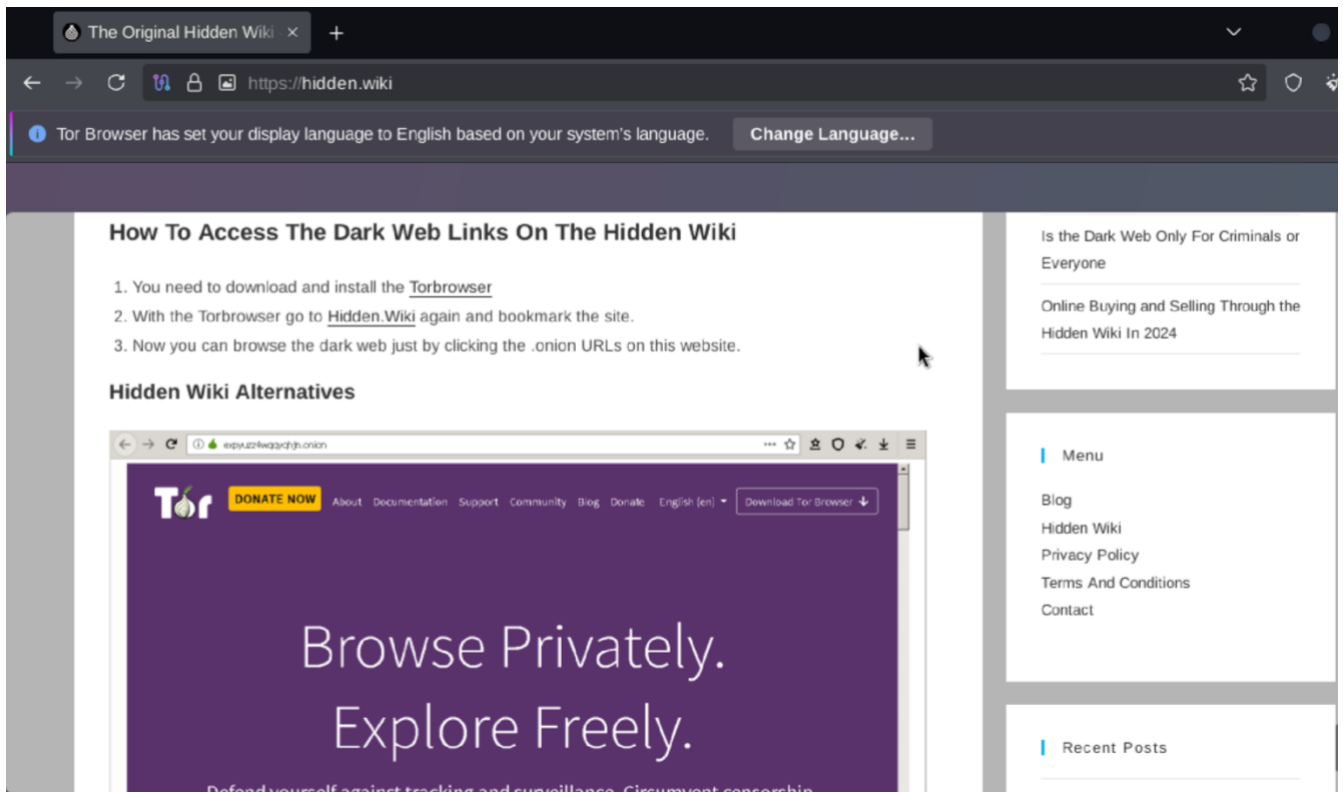


Una volta avviato, compare subito la pagina iniziale di tor browser, ma non vado a modificare nessuna impostazione come richiesto dall'esercizio.

Adesso, non resta altro che iniziare la navigazione su alcuni siti, ovviamente evitando procedure illegali.

Il primo sito che ho scelto di visitare è un sito già visto a lezione:

HiddenWiki:



Questo sito è una sorta di “indice” di vari servizi e siti sulla rete Tor.

Molti di questi siti, come si può notare dai titoli, si occupano di vendita di prodotti illegali, droghe ecc. Provo ad aprire alcuni link e vedo cosa viene fuori:


The Original Hidden Wiki x DrChronic - Weed straight x +

gkcns4d3453llqjrkxjdijfmdjpqsykt6misgojxlhspivt13uwhqd.onion

DrChronic

Products Login Registration

DrChronic - Shipping from USA



Straight from the source! We don't lose packages; your privacy and satisfaction is our top priority! Here at DrChronic we strive to meet and exceed customer expectations and always conduct our business professionally with integrity..

We currently ship MON,WED,FRI and all orders received before 12pm PST on those days will ship same day!
NO REFUND OR RESHIPMENT ON ORDERS THAT SHOW DELIVERED. Shipping is \$5, FREE for orders over \$200.

Product	Price	Quantity
SKUNK KUSH 1oz	120 USD = 0.00118 ₿	<input type="text" value="1"/> X Buy now
SKUNK KUSH 3oz	300 USD = 0.00294 ₿	<input type="text" value="1"/> X Buy now

Il primo link provato, mi porta subito ad un sito di vendita di cannabis, dove permette di selezionare la quantità e mostra il prezzo.

The Original Hidden Wiki x Apples 4 Bitcoin - Iphone: x DrChronic - Weed straight x +

awsrvr7occzj2yeyqevyrw7ji5ejuyofhfomidhh5qnuxpvwsucno7id.onion

Apples 4 Bitcoin

Login Register FAQs Products

Iphone

Brand new iPhones EU and US versions.
We ship from the EU and from the US, so there will be no import taxes!
All phones are factory unlocked and work internationally.
The iPhones are NOT reported as stolen!

Product	Price	Quantity
iPhone 15 Pro 1TB US Black	500 USD = 0.00490 ₿	1 x Buy now
iPhone 15 Pro 1TB US White	550 USD = 0.00539 ₿	1 x Buy now
iPhone 15 Pro 1TB EU Black	600 USD = 0.00588 ₿	1 x Buy now
iPhone 15 Pro 1TB EU White	600 USD = 0.00588 ₿	1 x Buy now
iPhone 15 Plus 512GB US Black	450 USD = 0.00441 ₿	1 x Buy now
iPhone 15 Plus 512GB EU Black	480 USD = 0.00471 ₿	1 x Buy now

Il secondo invece, vendita di Iphone.

SecureDrop:

Share and accept documents x +

https://securedrop.org

Tor Browser has set your display language to English based on your system's language.

Overview List o

SECUREDROP

Share and accept documents securely.

SecureDrop is an open source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources. SecureDrop is available in 22 languages.

Get SecureDrop at your organization >

Try Onion Services

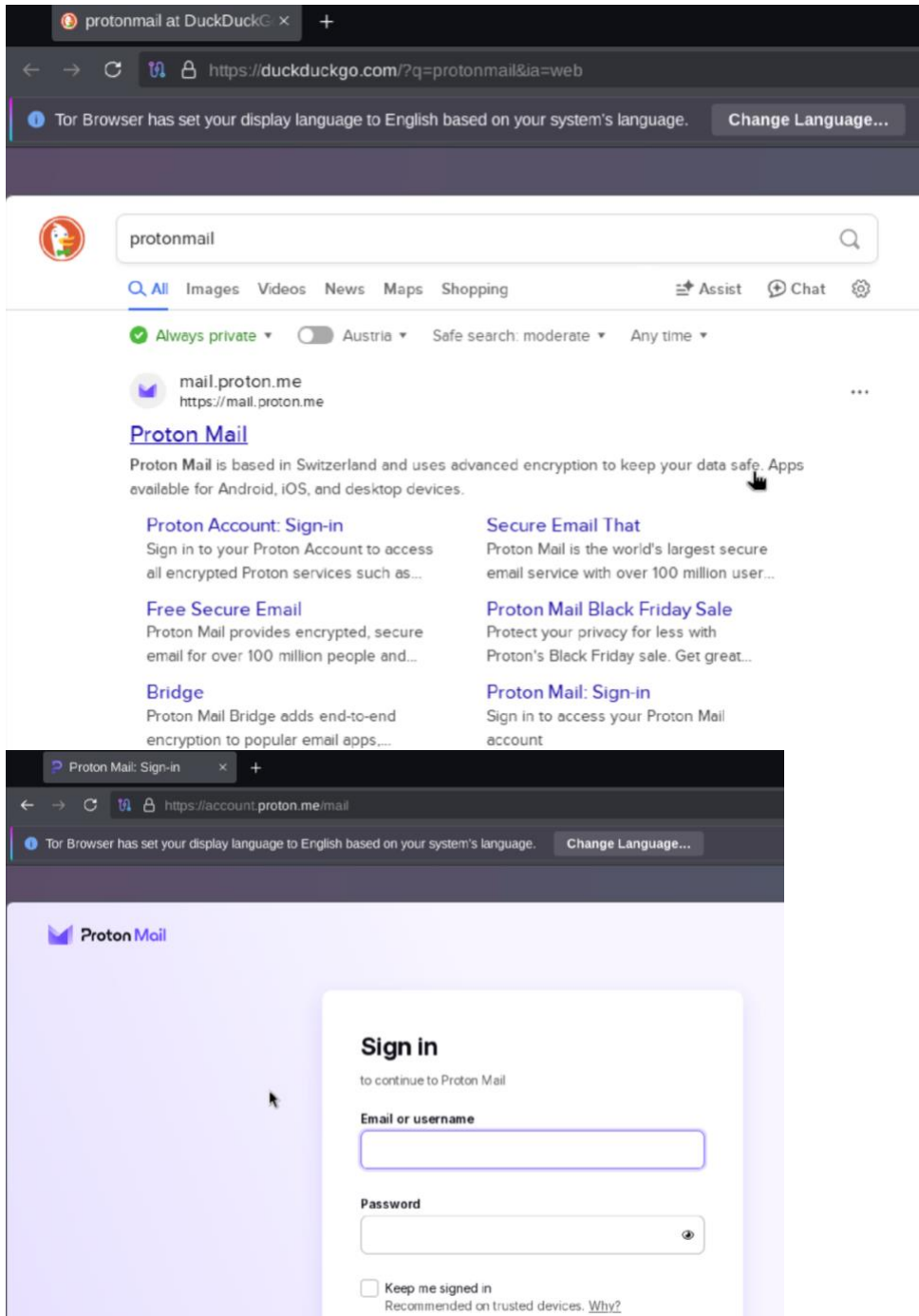
There's a more private and secure version of this site available over the Tor network via onion services. Onion services help website publishers and their visitors defeat surveillance and censorship.

Learn more

Not Now Visit the .onion

SecureDrop invece, è una piattaforma per la comunicazione sicura tra giornalisti e fonti anonime, molto interessante.

ProtonMail:



ProtonMail invece è un servizio di Posta elettronica sicura.