

# LABORATORIO 23 GENNAIO 2025 S7-L4

## TOR BROWSER:

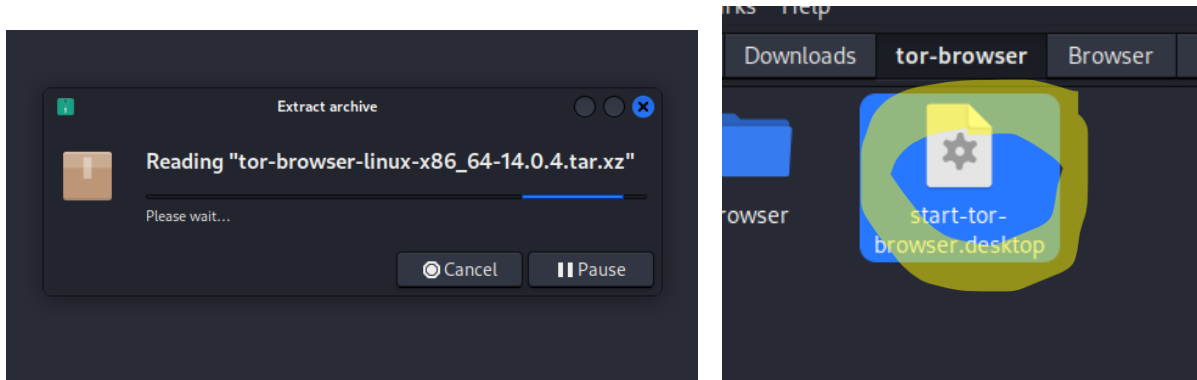
Da Kali, scaricare e provare Tor Browser (senza modificare alcuna impostazione predefinita). Effettuare qualche navigazione sulla rete Tor ed effettuare screenshot per il report.

Iniziamo avviando la macchina virtuale di Kali in Nat.

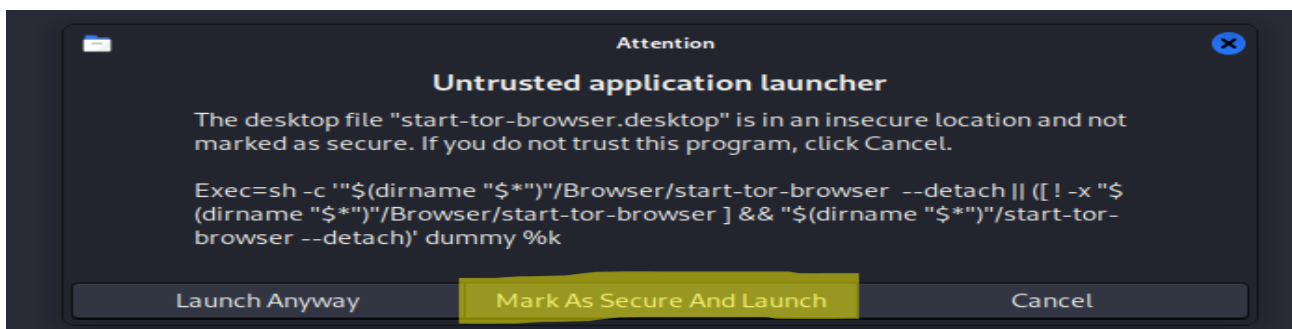
Una volta attivata, procediamo con il download e l'installazione di **Tor Browser**, comunemente chiamato “**the onion router**” in quanto sfogliando gli strati della cipolla possiamo navigare sempre più a fondo nel darkweb.



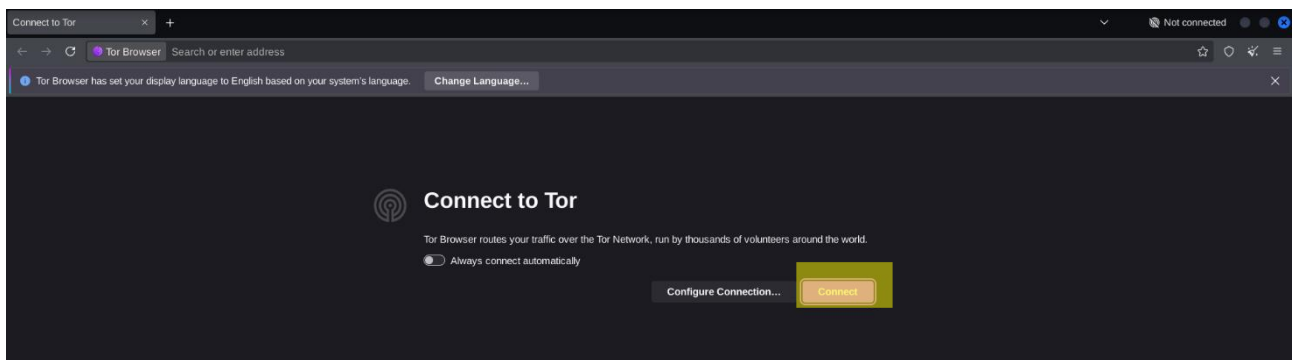
Scarichiamo la versione per Linux e andiamo ad estrarre il file che abbiamo ottenuto nella directory Downloads.



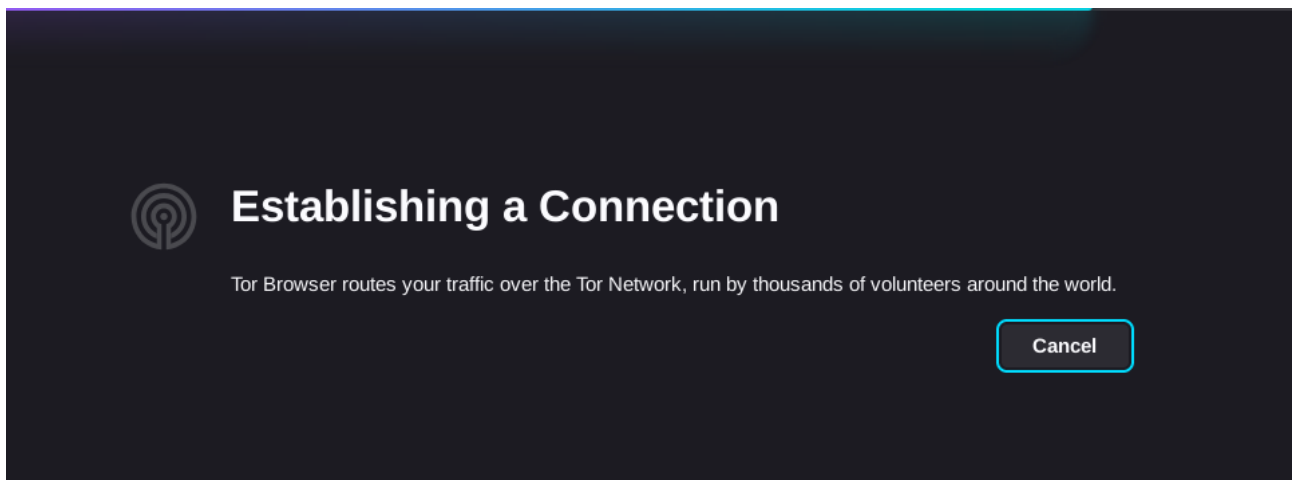
Avviamo il browser selezionando **mark as secure and launch**.



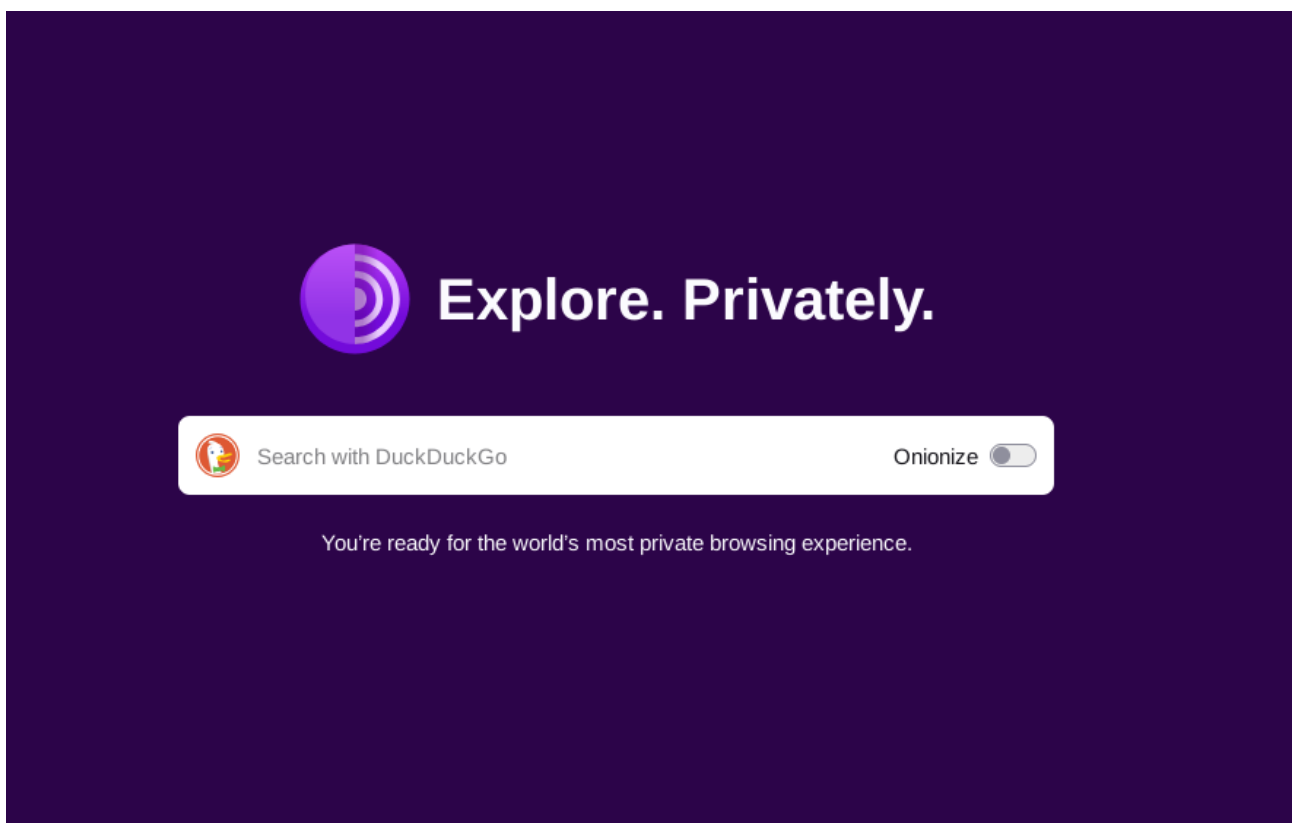
A questo punto si aprirà il browser. Lasciamo inalterate le impostazioni di default come la lingua e tutto il resto.



Clicchiamo quindi su **Connect** per stabilire una connessione.

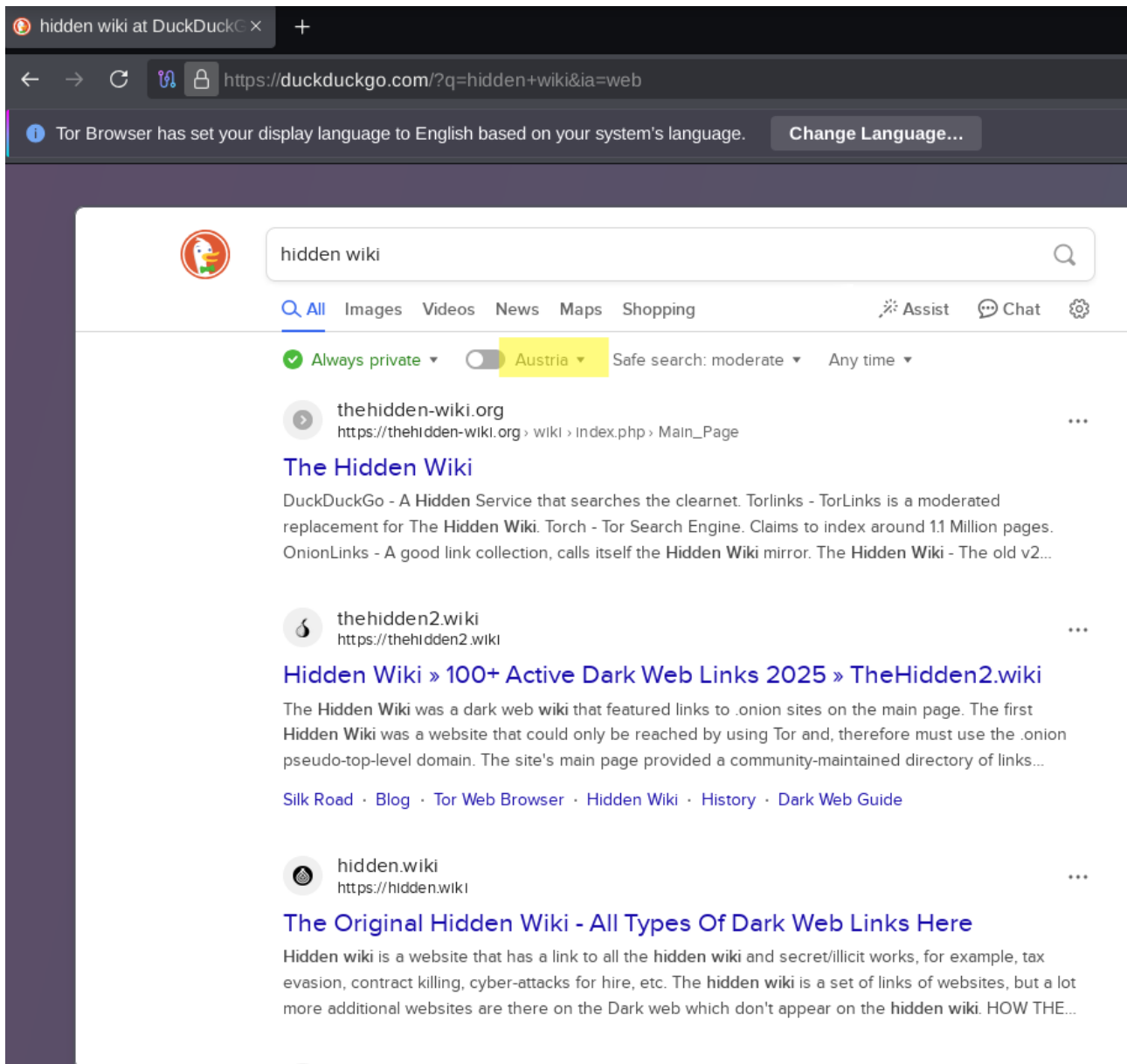


Dopo pochi secondi apparirà la schermata con il motore di ricerca DuckDuckGo all'interno della quale possiamo iniziare a cercare ciò di cui abbiamo bisogno.



Iniziamo a cercare **hidden wiki** che restituisce un numero considerevole di risultati contenenti link del DarkWeb.

Possiamo notare che siamo tracciati in Austria.



Continuando a navigare nel DarkWeb innanzitutto noteremo che cambierà sia l'IP sia lo stato in cui siamo localizzati. Facendo infatti una ricerca sul nostro indirizzo IP ci uscirà ora che siamo locati in Iran.

The screenshot shows the homepage of WhatIsMyIPAddress.com. The header includes the logo, a search bar, and navigation links (ABOUT, PRESS, PODCAST, SUPPORT). The main navigation bar has links for MY IP, IP LOOKUP, HIDE MY IP, VPNS, TOOLS, and LEARN. The main content area displays the following information:

- My IP Address is:**
  - IPv6: **2a0b:f4c2::15**
  - IPv4: **185.220.101.15**
- My IP Information:**
  - ISP: Stiftung Erneuerbare Freiheit
  - Services: [Network Sharing](#)
  - City: Mehriz
  - Region: Yazd Province
  - Country: Iran
- Are you using a Proxy?** (with a red button labeled **RATE YOUR PROXY**)
- [Show Complete IP Details](#)
- A map showing the location with a tooltip: "Click for more details about 2a0b:f4c2::15"
- Location not accurate? [Update My IP Location](#)

La nazione cambierà ad ogni nuova ricerca.

☒ Always private
 ☐ Romania
 Safe search: moc

Tornando su **hidden wiki** noteremo che i primi link siano in realtà fittizi e creati ad arte con ogni probabilità dalle autorità che cercando di “pescare” eventuali malviventi poco esperti che sono alla ricerca di droghe, armi o altre cose illegali o comunque da reperire illegalmente.

Proviamo ad esempio a “comprare” dati di carte di credito.

- [Cardshop](#) - High quality CCV and Drivers Licenses.  
 • [Cardshop](#) - Usa cvv know balance & Worldwide cc & cvv.

## USA CVV KNOWN BALANCE



You will get a High Quality known balance cc (100% live not some rubbish cards like my competitor ones) !  
You will get the current balance (how much is owed to bank by CH ) You will get available credit (so you know exactly how much to charge !  
You will also get last statement date /amount and next statement due /amount just so you get your head round it (in case your method takes a while you know exactly how to move around it.

You will receive the following card format:  
CC number | expiry | CVV | first name | last name | address | city | State | zipcode | email | phone number (where available) | current balance | available credit |

Cards designed for Paypal/stripe/square/venmo no more wasting time and money trying to find a card that works, with me you will hit first time guaranteed!  
Always bought cards not knowing how much to charge, and worried about charging too much and killing the card? NOT with my cards, you will know EXACTLY how much is in there so you can charge it without worrying !

Happy buying !

Product	Price	Quantity
10 x cards with credit from 1000 to 5000 USD	90 USD = 0.00088 ₿	Sold out
50 x cards with credit from 1000 to 5000 USD	350 USD = 0.00343 ₿	<input type="text" value="1"/> x <a href="#">Buy now</a>
10 x cards with credit from 5000 to 20000 USD	120 USD = 0.00118 ₿	Sold out
50 x cards with credit from 5000 to 20000 USD	450 USD = 0.00441 ₿	<input type="text" value="1"/> x <a href="#">Buy now</a>
10 x cards with credit from 20000 to 50000 USD	180 USD = 0.00177 ₿	<input type="text" value="1"/> x <a href="#">Buy now</a>
50 x cards with credit from 20000 to 50000 USD	650 USD = 0.00638 ₿	<input type="text" value="1"/> x <a href="#">Buy now</a>
10 x non verified by visa cards 5000 - 100000 USD	250 USD = 0.00245 ₿	<input type="text" value="1"/> x <a href="#">Buy now</a>

In questo caso abbiamo preso uno tra i primi link su hidden wiki e possiamo dedurre che sia un fake fatto ad arte dalle autorità come detto in precedenza.

Proviamo ora a **sfogliare la cipolla** di Tor per scavare più a fondo nel darkweb (ma senza esagerare!).

Per farlo dovremo effettuare ricerche a strati non soffermandoci su link “troppo belli per essere veri” e troppo in alto nei risultati delle nostre ricerche.

Cerchiamo quindi direttamente all'interno del darkweb e iniziamo una nuova ricerca su HiddenWiki su siti Onion. Stiamo sfogliando la cipolla.

The image shows two screenshots from a web browser. The top screenshot is a search results page for the term 'hidden' on the HiddenWiki site. It features a purple header with a 'Download Tor Browser' button. The search results list several links related to OnionLinks v3, another Hidden Wiki, Pug's Ultimate Dark Web Guide, and The Hidden Wiki. Below these, there are sections for 'Bitcoin Mixers And Anonymous Wallets' and 'Dark Web Markets and Drug Vendors', each with a list of links to various services like Onionwallet, EasyCoin, VirginBitcoins, and Mixabit. The bottom screenshot shows the OnionLinks website itself, which has a purple and white theme. It includes a navigation menu with links to Introduction Points, Financial Services, Commercial Services, Drugs, Chans, Privacy Services, Email Providers, Blogs And Personal Sites, Hacking, News Sites, Open Source Software, and Others. The website also displays a warning about the shutdown of v2 sites and provides links to the current v3 site and other related resources.

Download Tor Browser ↓

<http://jaz45aahn5vkemy4jkg4mi4syheisqn2wn2n4fsuitpcddackjwxplad.onion/> OnionLinks v3

<http://bj5hp4onm4tvpdb5rzt4zsbwoons67jnastvuxefe4s3v7kupjghg6gd.onion/> Another **Hidden** Wiki

<http://qrjtjevs5nxq6jvnrjyz5dasi3nbzx24mzmfmxuk2dnzhpphcmgoyd.onion/> Pug's Ultimate Dark Web Guide

<http://xsglg2kdl72b2wmt5b2b7lodjmemnmcc37owlz5inrhzyfdnrygid.onion/> The Hidden Wiki

**Bitcoin Mixers And Anonymous Wallets**

<http://zwf5i7hiwmffg2b7euedg6y5ydzze3ljyjrjmm7o42vhe7ni56fm7qd.onion/> Onionwallet Anonymous and secure bitcoin wallet and mixer

<http://vu3mig3vvhxijfclhmvy7ezclvsb3vksmug5vuiibpw4zovyszbemvgd.onion/> EasyCoin Bitcoin Wallet and Mixer

<http://5kpg325ecpcncl4o2xksvaso5tuydwj2kuqmpgtmu3vzfkpiwsgpfid.onion/> VirginBitcoins Buy freshly mined clean bitcoins



<http://cr32aykujaxqkfgyrjvt7lxovnadpgmgthb3y4g6jmx6oomr572kbugd.onion/> Dark Mixer Anonymous bitcoin mixer

<http://74ck36pbaxz7ra6n7v5pbpm5n2tsdaiy4f6p775qvmowxged65n3cid.onion/> Mixabit Bitcoin mixer

**Dark Web Markets and Drug Vendors**

[jaz45aahn5vkemy4jkg4mi4syheisqn2wn2n4fsuitpcddackjwxplad.onion](http://jaz45aahn5vkemy4jkg4mi4syheisqn2wn2n4fsuitpcddackjwxplad.onion/)

hidden ^ v Highlight All Match Case Match Diacritics Whole Words 12 of 41 matches

 **OnionLinks** 

**OnionLinks**

Short: onion v2 websites will stop working in October 2021. Bookmark OnionLinks or [DARKWEBLINKS.COM](http://DARKWEBLINKS.COM) for working v3 .onion sites!

**Navigation:**

- [Introduction Points](#)
- [Financial Services](#)
- [Commercial Services](#)
- [Drugs](#)
- [Chans](#)
- [Privacy Services](#)
- [Email Providers](#)
- [Blogs And Personal Sites](#)
- [Hacking](#)
- [News Sites](#)
- [Open Source Software](#)
- [Others](#)

**Introduction Points**

**OnionLinks** [jaz45aahn5vkemy4jkg4mi4syheisqn2wn2n4fsuitpcddackjwxplad.onion](http://jaz45aahn5vkemy4jkg4mi4syheisqn2wn2n4fsuitpcddackjwxplad.onion/)

**The Hidden Wiki** [swvugn3zqfhianshldcqp2u7olj3xext6i3ha3c5znpdcdnqn24nmd.onion](http://swvugn3zqfhianshldcqp2u7olj3xext6i3ha3c5znpdcdnqn24nmd.onion/)

hidden ^ v Highlight All Match Case Match Diacritics Whole Words 12 of 41 matches

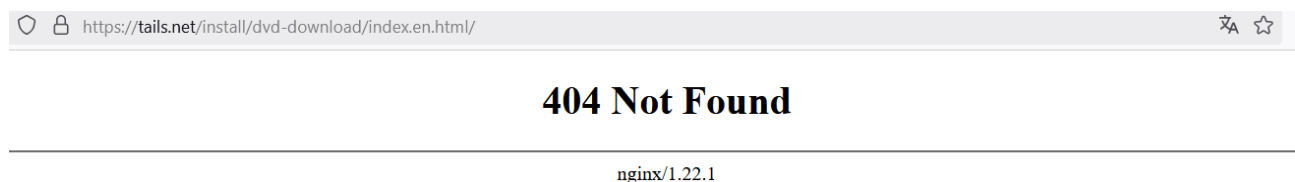
Qui troviamo numerosi link che potrebbero essere realmente siti dove reperire materiale illegale all'interno del darkweb.

Interrompiamo a questo punto la nostra ricerca per evitare di accedere a contenuti vietati.

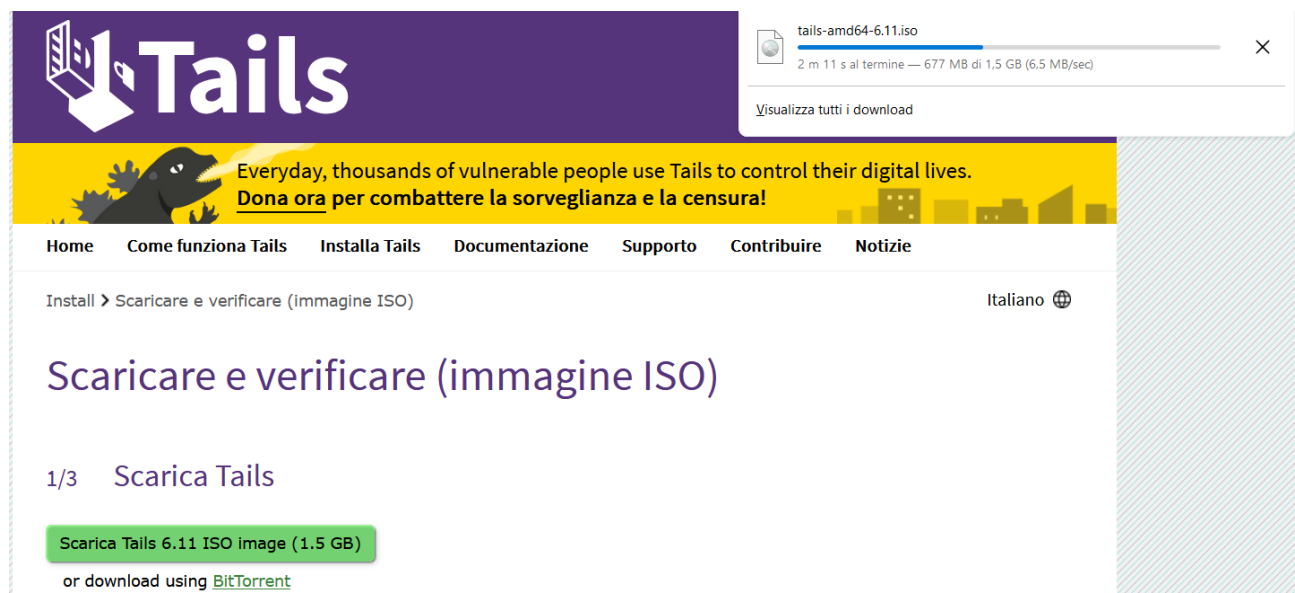
# ESERCIZIO BONUS:

## Installare Tails su macchina virtuale.

Per scaricare ed installare Tails ho cercato sul Web il link migliore in quanto quello che ci era stato fornito non era funzionante.



Trovo quindi un link corretto ed inizio a scaricare l'ISO di Tails.



A questo punto non ci resta che installare Tails su VirtualBox settando tutte le giuste configurazioni.



Iniziamo cliccando su nuova e specificando nome, tipo e versione. Carichiamo quindi l'immagine ISO appena scaricata.

The screenshot shows the 'Nome e sistema operativo' (Name and operating system) step of a virtual machine creation wizard. The fields are as follows:

- Nome:** Tails (with a green checkmark icon)
- Cartella:** C:\Users\home\VirtualBox VMs (with a folder icon)
- Immagine ISO:** C:\Users\home\OneDrive\Desktop\EPICODE\VIRTUAL MACHINE\tails-amd64-6.11.iso (with a green checkmark icon)
- Edizione:** (empty dropdown)
- Tipo:** Linux (with a dropdown arrow and an x64 icon)
- Sottotipo:** Debian (with a dropdown arrow)
- Versione:** Debian (64-bit) (with a dropdown arrow)
- ☐ Salta l'installazione non supervisionata

Below the fields are three blue buttons with white text and right-pointing arrows:

- Installazione non supervisionata
- Hardware
- Disco fisso

Assegniamo 2gb di Ram e 2 processori.

The screenshot shows the 'Hardware' step of the virtual machine creation wizard. The settings are as follows:

- Memoria di base:** A slider bar ranging from 4 MB to 12288 MB, with a blue arrow pointing to 2048 MB. The value '2048 MB' is displayed in a box on the right.
- Processori:** A slider bar ranging from 1 CPU to 8 CPU, with a blue arrow pointing to 2. The value '2' is displayed in a box on the right.
- ☐ Abilita EFI (solo alcuni sistemi operativi)

Below these settings is a blue button with a white right-pointing arrow labeled 'Disco fisso'.

Infine creiamo un disco fisso virtuale, assegniamo 20gb di memoria e VHD come tipo e variante del file di disco fisso con pre-allocazione a dimensione intera.

> Nome e sistema operativo

> Installazione non supervisionata

> Hardware

✓ Disco fisso

☒ Crea un disco fisso virtuale ora

Posizione e dimensione del file di disco fisso

C:/Users/home/VirtualBox VMs/Tails/Tails.vhd

4,00 MB 2,00 TB 20,00 GB

Tipo e variante del file di disco fisso

VHD (Virtual Hard Disk)

☒ Pre-allocazione a dimensione intera

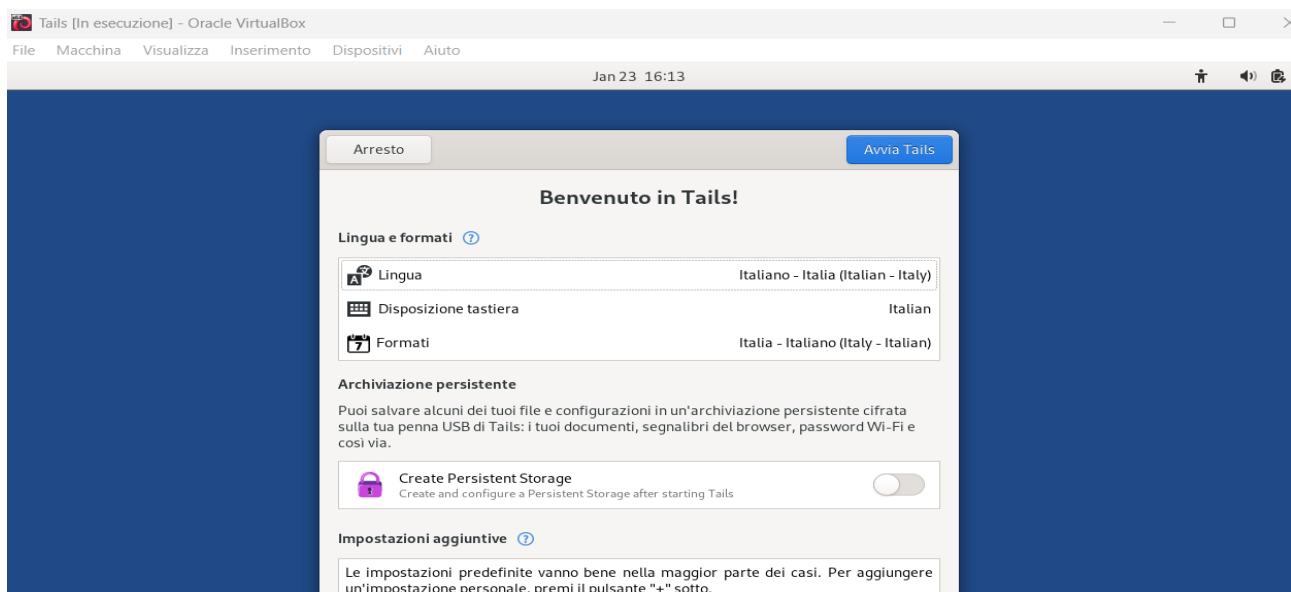
☐ Dividi in parti da 2GB

☐ Usa un file di disco fisso virtuale esistente

Parrot-security-6.2\_amd64-disk001.vdi (Normale, 64,00 GB)

☐ Non aggiungere un disco fisso virtuale

Una volta settate le impostazioni facciamo partire l'installazione della macchina. A questo punto facciamola partire e ne verifichiamo il giusto funzionamento.



Settiamo anche la lingua e la tastiera e siamo pronti all'avvio.

