Mascarea identităţii pe Internet

Browserul TOR

Setări importante pentru browserul TOR

Adăugarea de adrese la Bookmarks; salvarea şi restaurarea unor adrese

Precauţii elementare de luat pentru mărirea siguranţei navigării pe DarkNet

Sistemul de operare TAILS

Browserul TOR

Uneori ştim sau bănuim că adresa computerului/dispozitivului cu care navigăm pe Internet va fi înregistrată pe site-uri către care intenţionăm să navigăm cu browserul sau pe drumul până la acelea.

Aşadar, vrem să ascundem, să mascăm identitatea pe Internet:

- adresa IP (*I*nternet *P*rotocol) a dispozitivului – din care pot fi aflate:
  - ţara şi/sau locul (posibil până la nivel de clădire) a locului de unde accesăm site-urile
  - furnizorul de servicii pentru accesul la Internet

Aceasta se face prin salturi între aşa-zise noduri din reţeaua de anonimizare:

- numai primul nod va primi adresa IP reală
- în fiecare nod va fi schimbată adresa IP primită de la nodul precedent
- la destinaţie (site-ul vizitat) va fi observată adresa generată în ultimul nod de pe traseu

Astfel, putem naviga pe Internet din ţara X care pe traseul până la site va fi schimbată la ţara Y, ţara Z, ţara W şamd. până ce site-ul va considera că este vizitat din ţara H.

Adresa IP reală, cea cunoscută în sistemul de operare, nu va fi schimbată.
***Numai va apărea drept alta* în fiecare nod începând de la al doilea de pe traseu.**

O metodă folosită pe scară largă datorită simplităţii este navigarea pe Internet cu browserul TOR care derivă din browserul Firefox cu care este foarte asemănător.

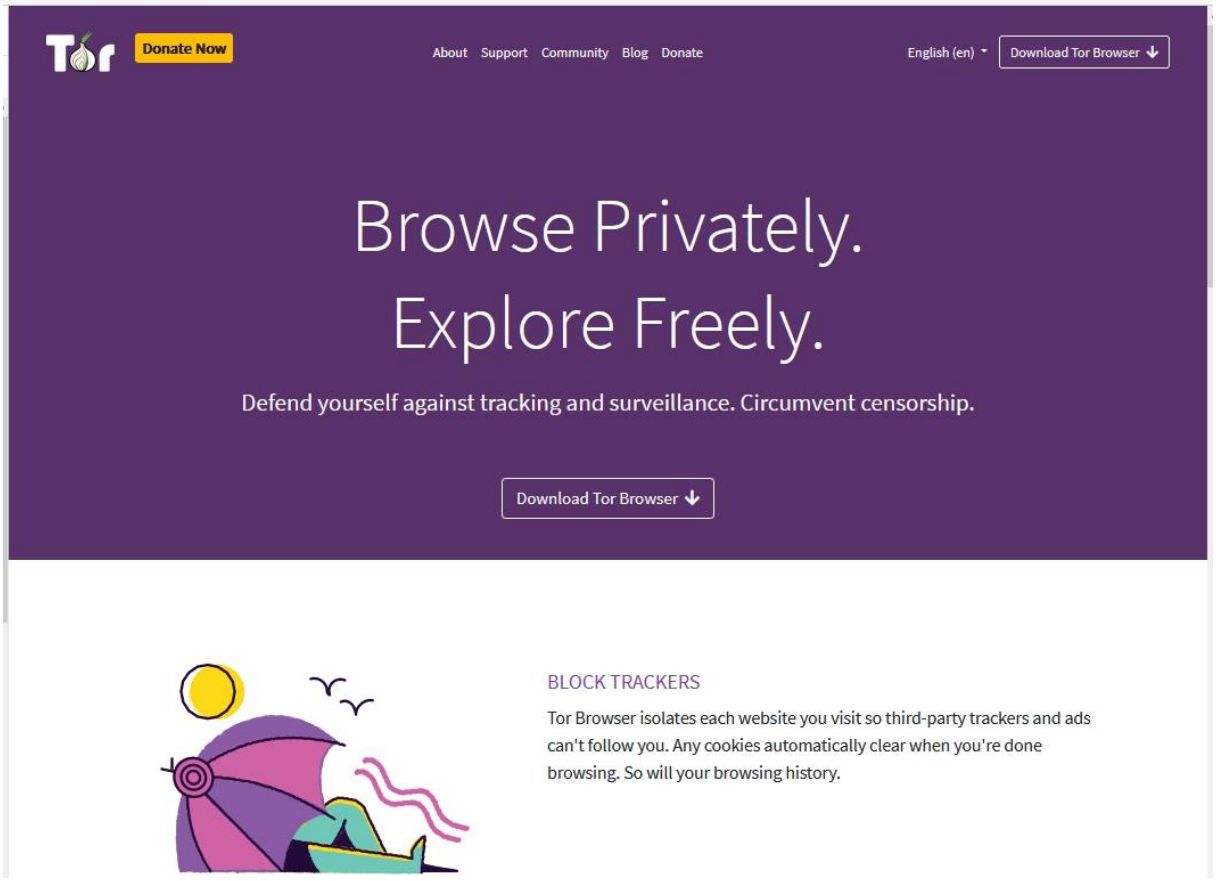
Pachetul de instalare poate fi preluat/descărcat gratis de pe site-ul:

https://www.torproject.org/

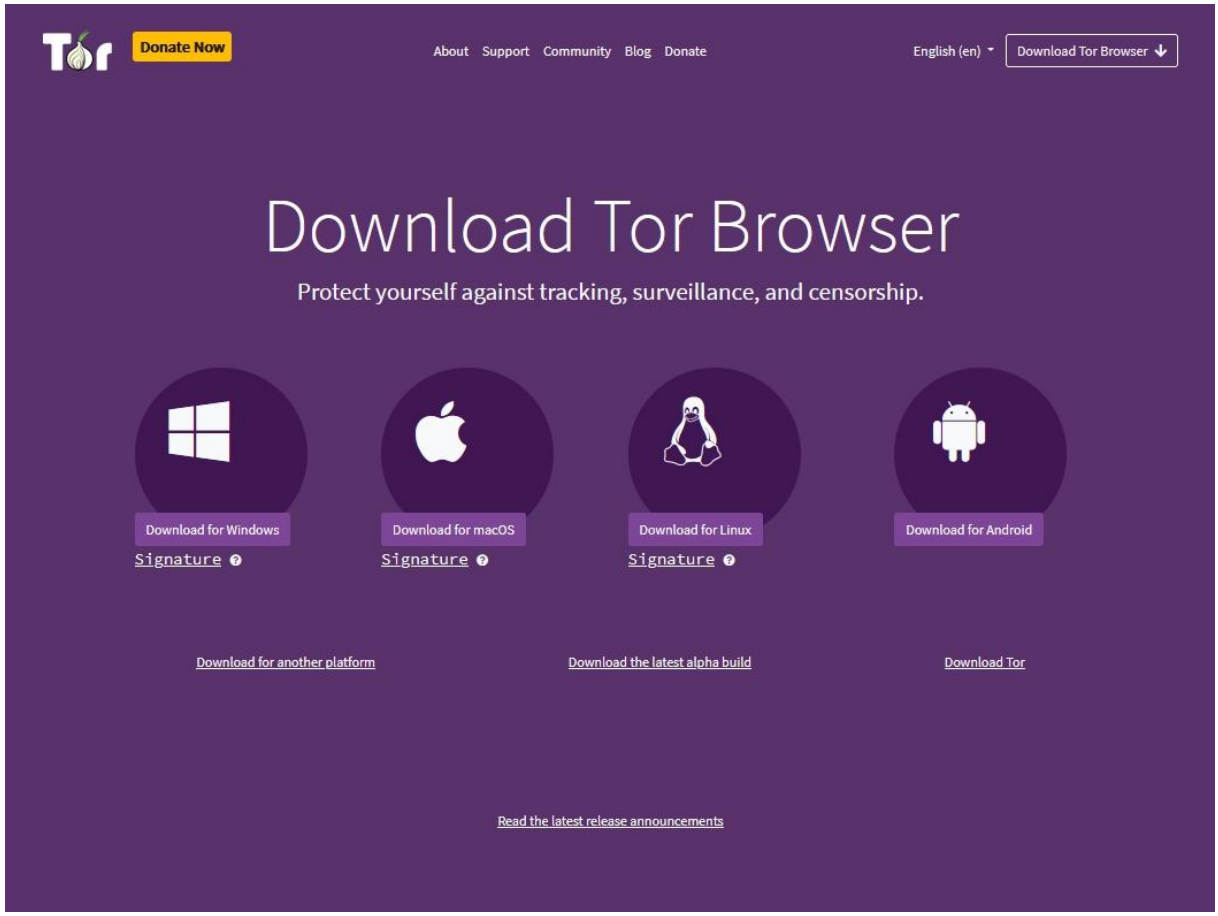
sau

http://www.torproject.org/

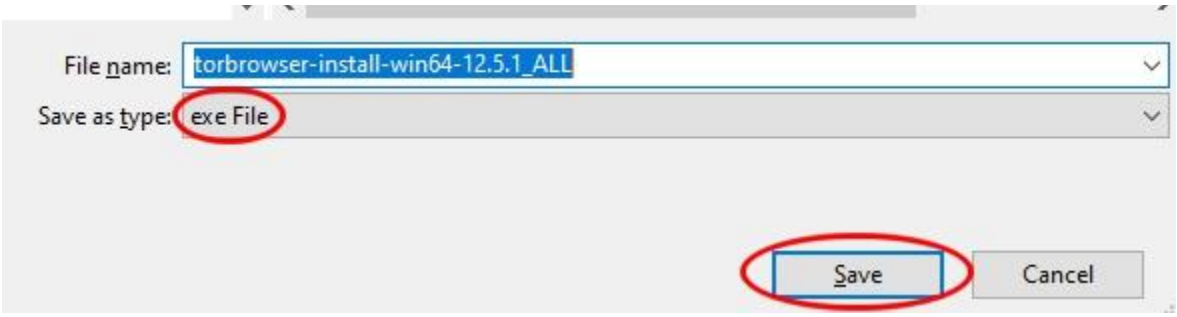
În luna iulie, 2023 pagina de întâmpinare pe acest site arăta astfel:
În dreapta-sus şi în centrul paginii se observă comanda/link-ul "*Download Tor Browser*"



Pentru a prelua/descărca pachete de instalare a browserului TOR pentru diverse sisteme de operare:
Click pe unul din acele linkuri:

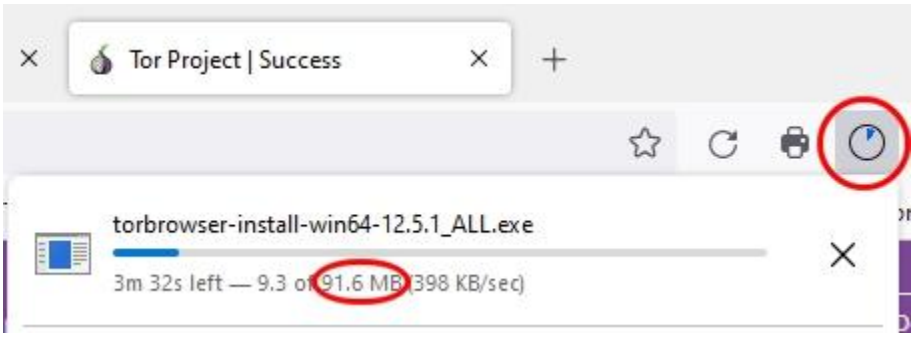


În exemplul acesta, descărcăm pachetul de instalare pentru sistemul de operare Windows:
Click pe linkul "Download for Windows"



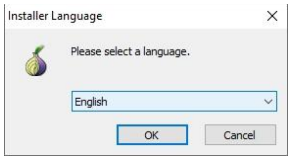
În imaginea următoare se vede zona din browserul *Firefox* cu care descărcăm pachetul respectiv:
La acele informaţii –
care prezintă progresia transferului de la site-ul torproject.org către computerul local –
se ajunge

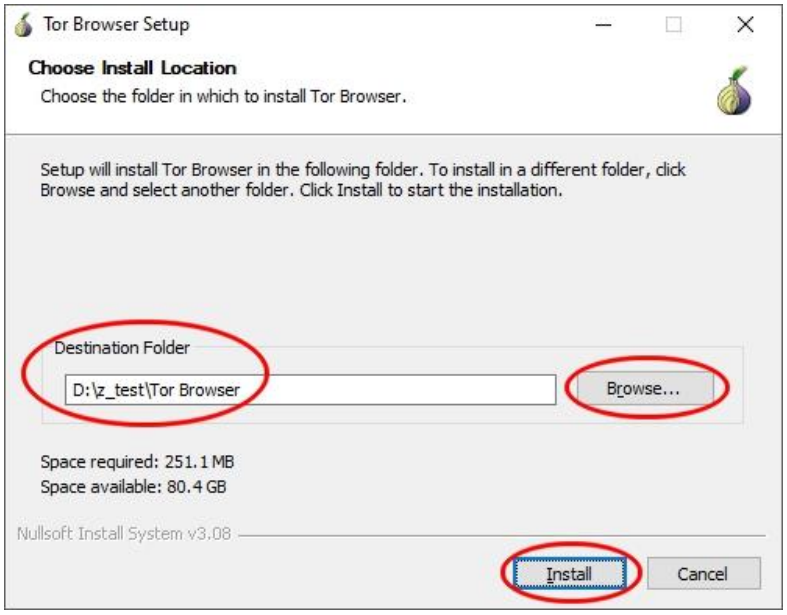
- fie cu click pe pictograma din imagine
- fie din meniul "Tools->Downloads" al *Firefox*
- fie cu tastele **Ctrl** şi **J** apăsate simultan



Odată descărcat acest pachet, ca fişier executabil cu extensia .exe,
purcedem la instalarea browserului, lansând acel executabil:

- fie dublu-click pe acel fişier
- fie click-dreapta pe el şi apoi alegerea comenzii "Open" sau similar, cu acelaşi înţeles



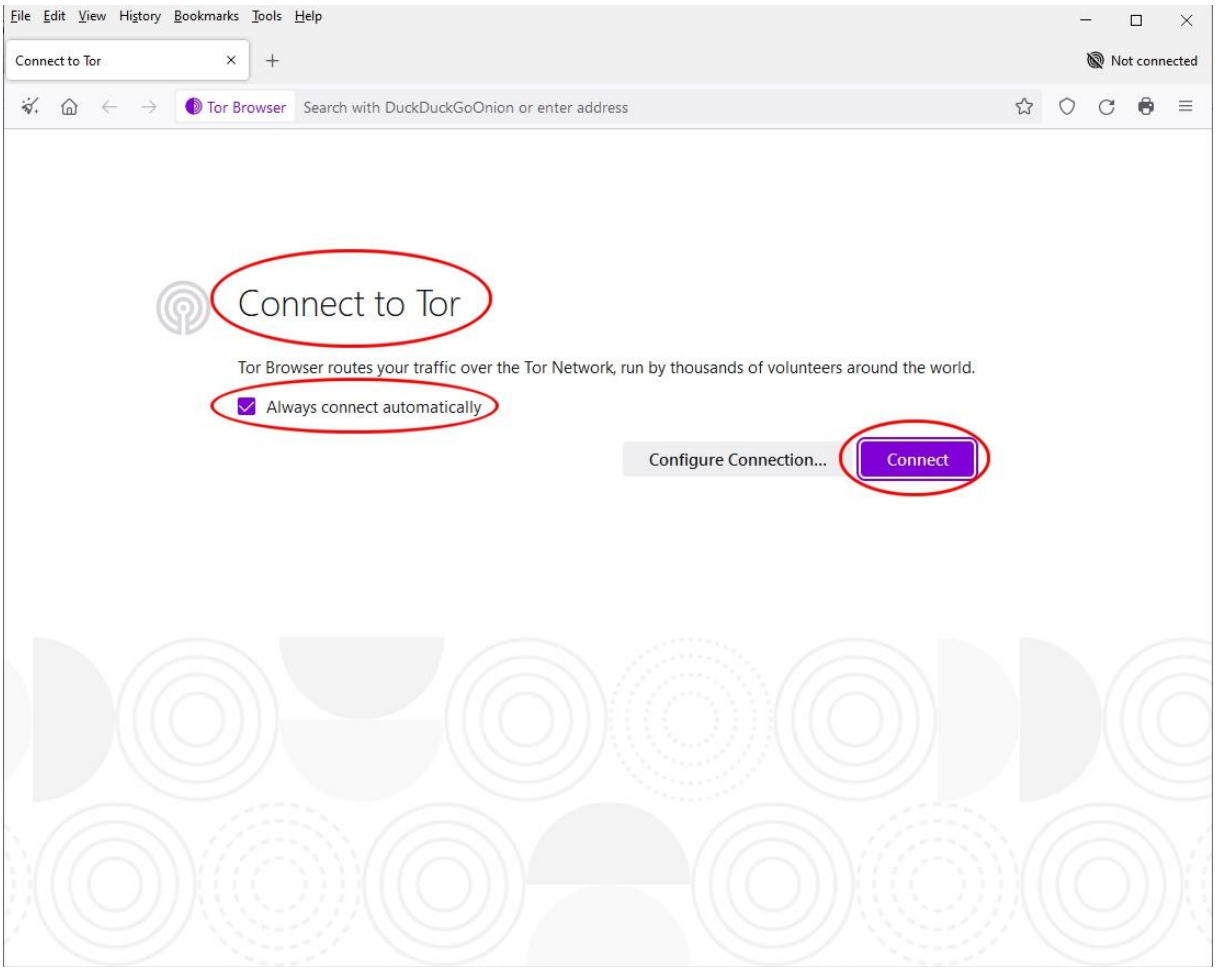


După instalare, pornim browserul TOR:

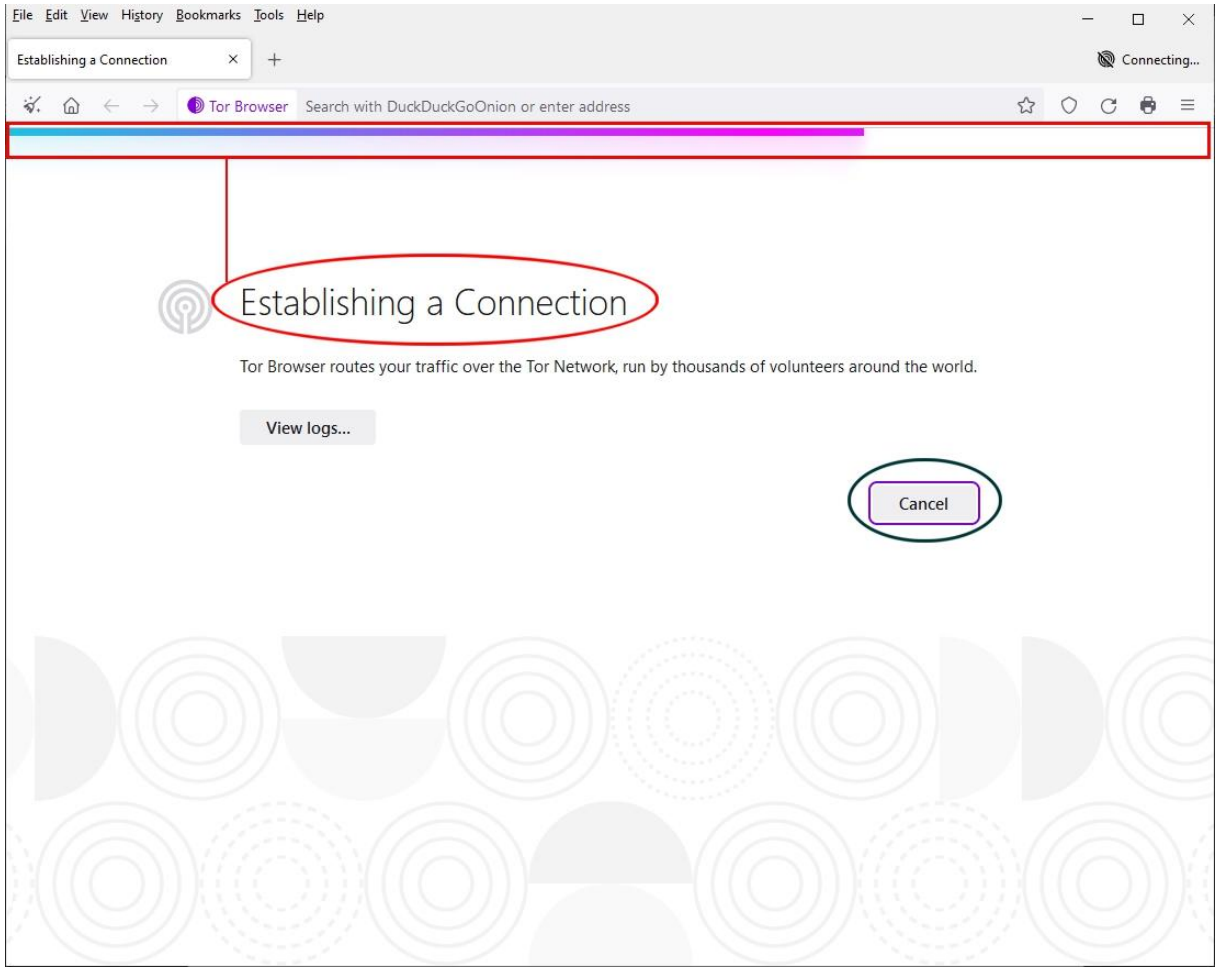
Este probabil să fie iniţiată automat conectarea la reţeaua de noduri.

Dacă nu se întâmplă astfel, atunci apăsăm butonul "*Connect*", ca în imagine.

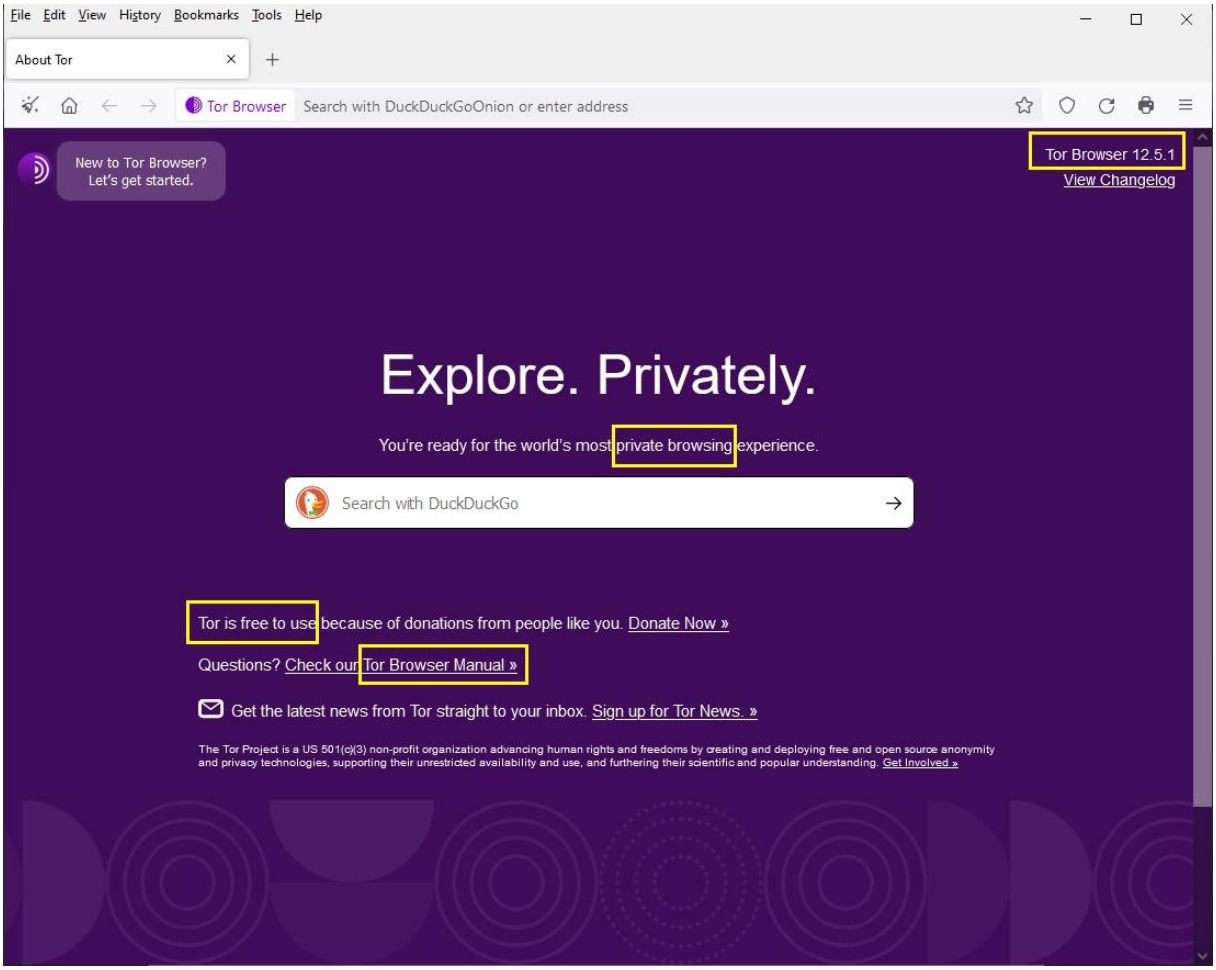
Apoi aşteptăm până când
- conectarea la reţeaua de anonomizare este realizată cu succes
  sau
- un mesaj de eroare anunţă eşecul încercării de conectare



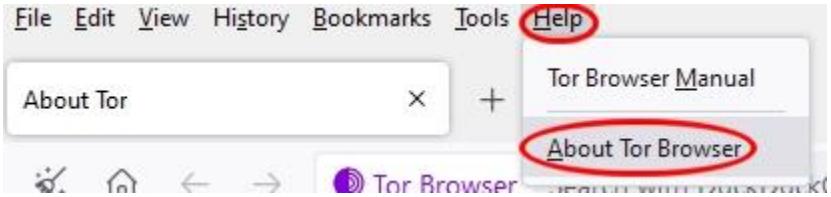
Putem anula procedura de conectare apăsând butonul "*Cancel*":

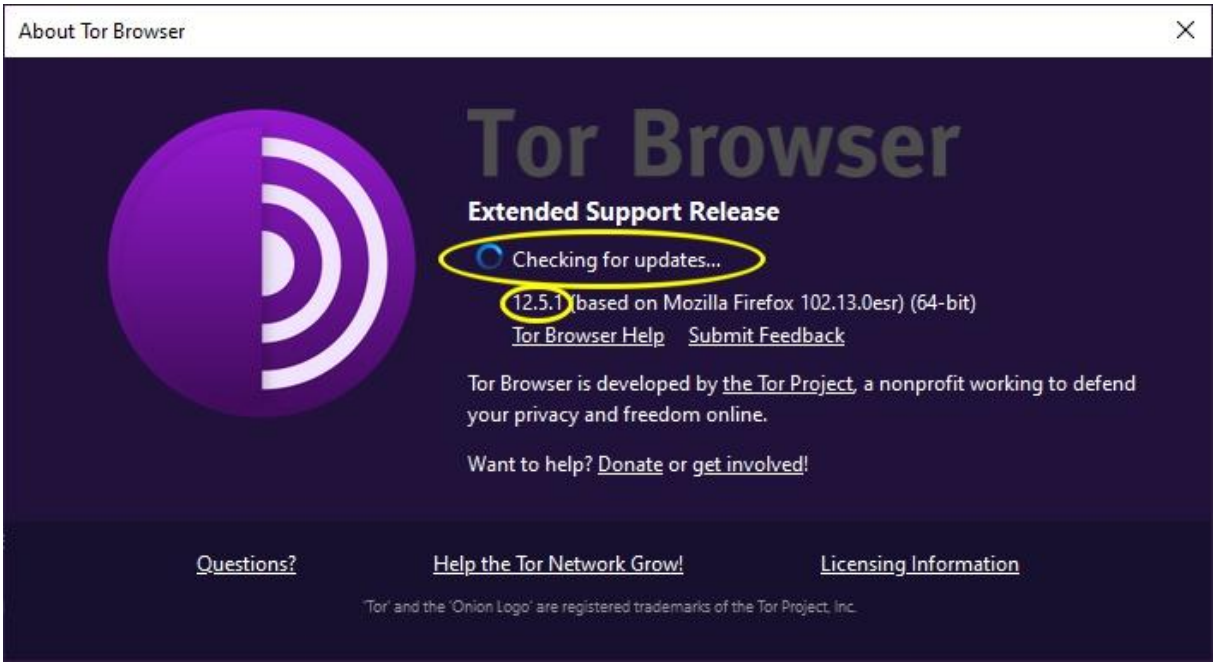


Conectarea la reţeaua de anonimizare este anunţată de pagina de pornire a browserului TOR:



Pentru a ne asigura că folosim cea mai recentă versiune, verificăm din meniul "*Help*":



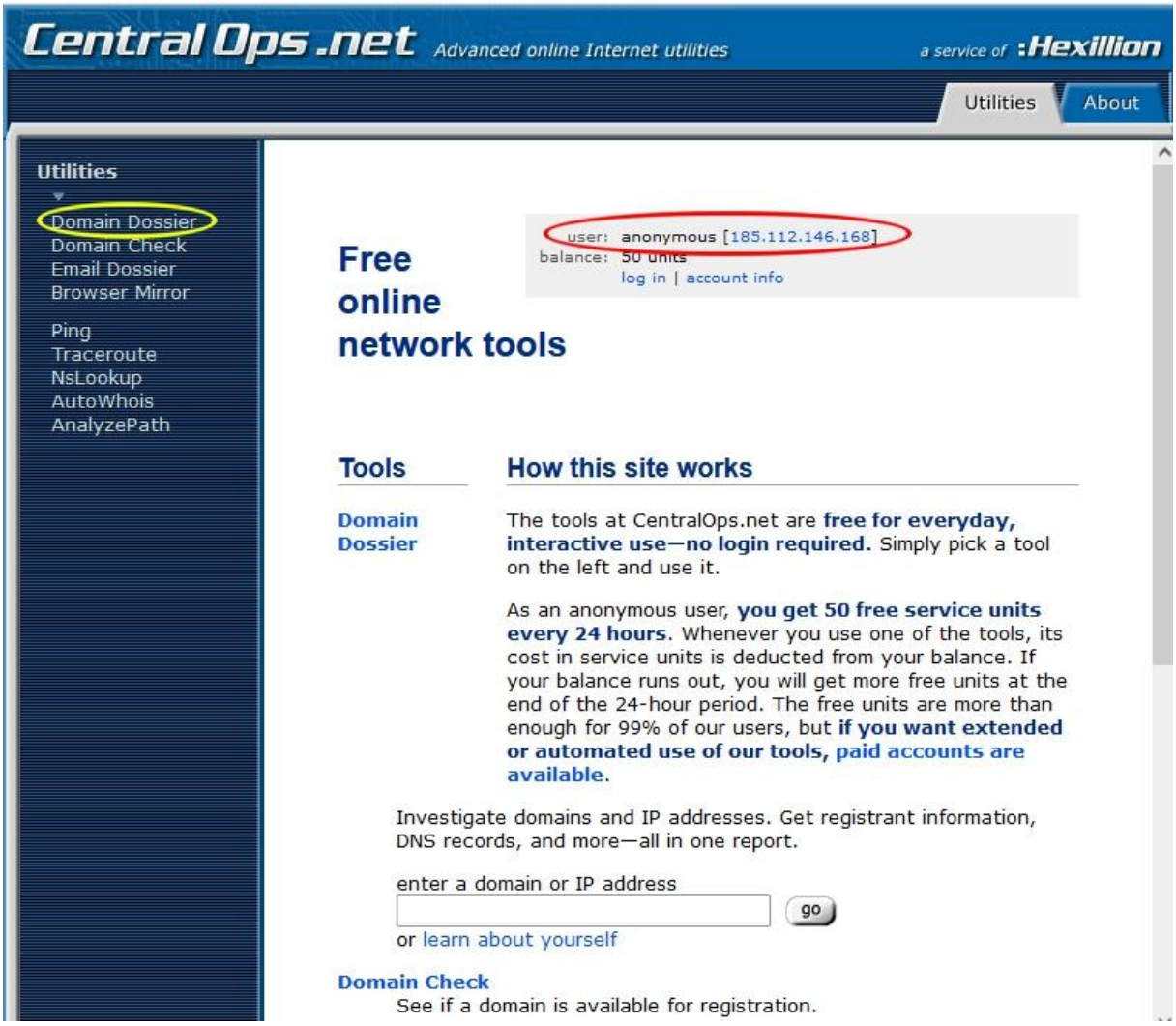


Să aflăm ce adresă IP ne-a fost atribuită:

Cu browserul TOR,
deci fiind deja "anonimi" deoarece ne-am conectat la reţeaua de anonimizare,
accesăm site-ul:

https://centralops.net/co/

unde putem afla informaţii detaliate despre "noi înşine ca adresă IP/identitate pe Internet"

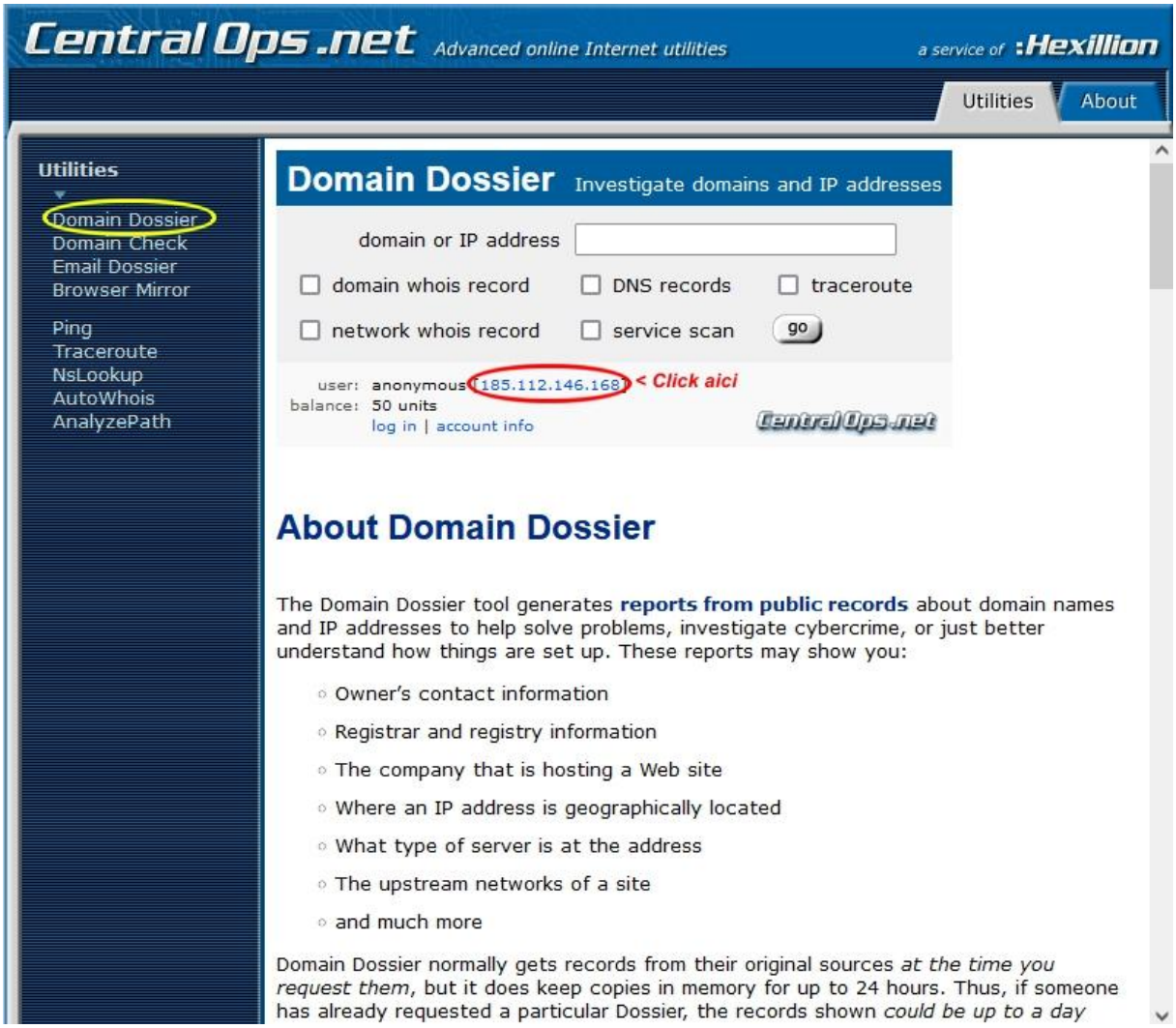


În imaginea precedentă observăm că adresa IP este alta decât cea reală.

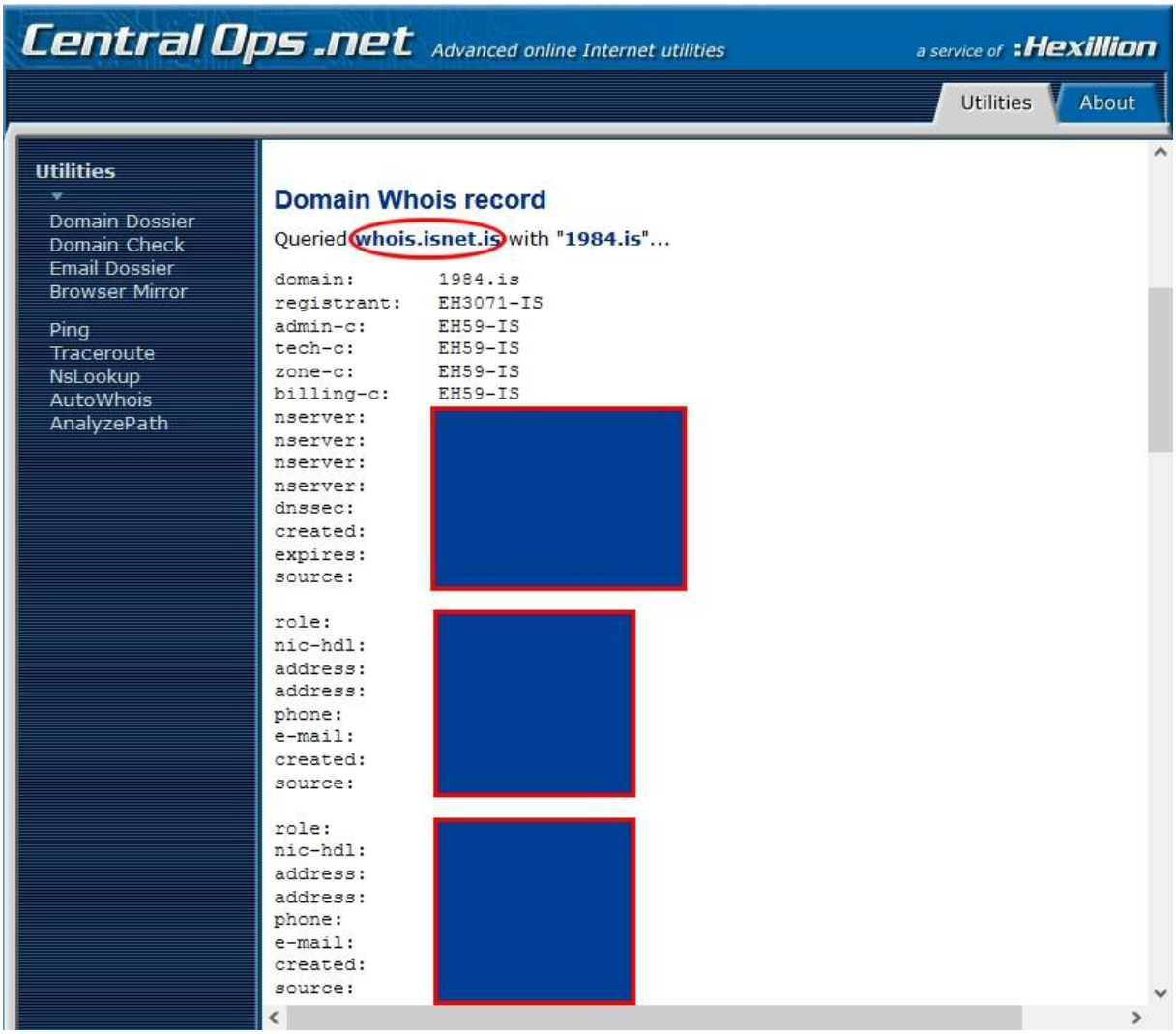
Pentru a afla cine anume suntem consideraţi:

- de către acest site
- şi de altfel de către orice site vizitat în această sesiune de lucru cu browserul TOR:

Apăsăm pe linkul "*Domain Dossier*"
după care sunt afişate acele informaţii detaliate despre "noi de la această adresă IP":



Click pe adresa IP din imaginea precedentă. Vor fi afişate informaţii detaliate despre adresa IP:



Observăm că adresa IP indică un domeniu de adrese din Islanda - ţară unde este posibil să nu ne aflăm, în realitate.

Fiecare site vizitat cu browserul TOR în această sesiune (adică, până îl închidem) va considera ca avem această adresă IP –
cea atribuită automat de trecerea prin nodurile reţelei de anonimizare.

Pentru a înţelege aceasta, iată diferenţa dintre adresele IP înregistrate pe acelaşi site vizitat cu browserul Firefox şi cu browserul TOR:

- accesare cu Firefox: adresa reală, nemodificată prin reţeaua de anonimizare:

rqip="78. 15" **rqpt**="WinNT" **rqbw**="Firefox115"

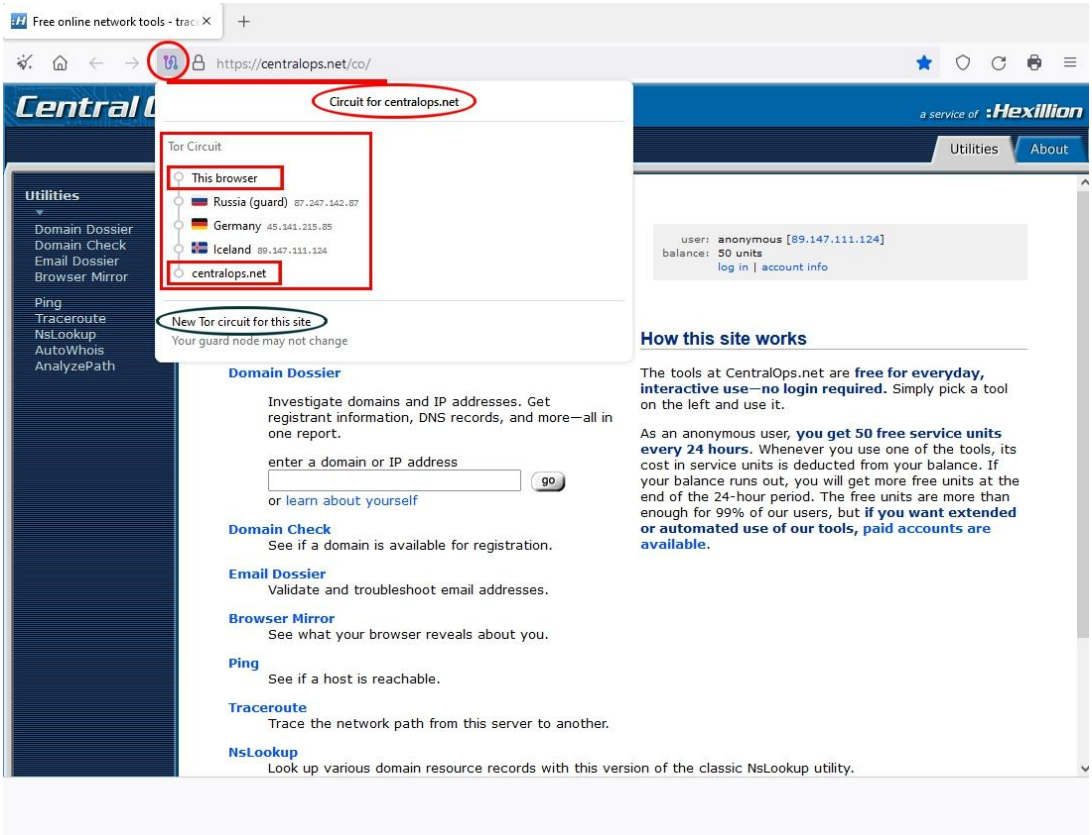
- accesare cu TOR: adresa falsă:

rqip="89. 33" **rqpt**="WinNT" **rqbw**="Firefox102"

Se observă cum browserul TOR este identificat drept o versiune a browserului Firefox, inferoară celei curente a aceluia.
De obicei, la un moment dat versiunea Firefox după care a fost proiectată cea curentă a TOR este mai mică decât cea mai recentă a Firefox – fiindcă TOR este dezvoltat după Firefox.

Totuşi, putem schimba circuitul/traseul pe care ajungem la un site:

Click pe pictograma din stânga adresei site-ului prezentat în această pagină:



Este prezentat circuitul pe care s-a mers

- de la acest computer/dispozitiv cu browserul TOR
- până la site (-ul destinaţie)

Circuitul poate fi schimbat astfel:

- click pe "***New Tor circuit for this site***"

Rezultatul va fi similar celui prezentat în imaginea următoare:



Mai mult - putem stabili manual ţara de unde intrăm în reţea şi pe cea de unde ieşim către site-uri pe Internet.

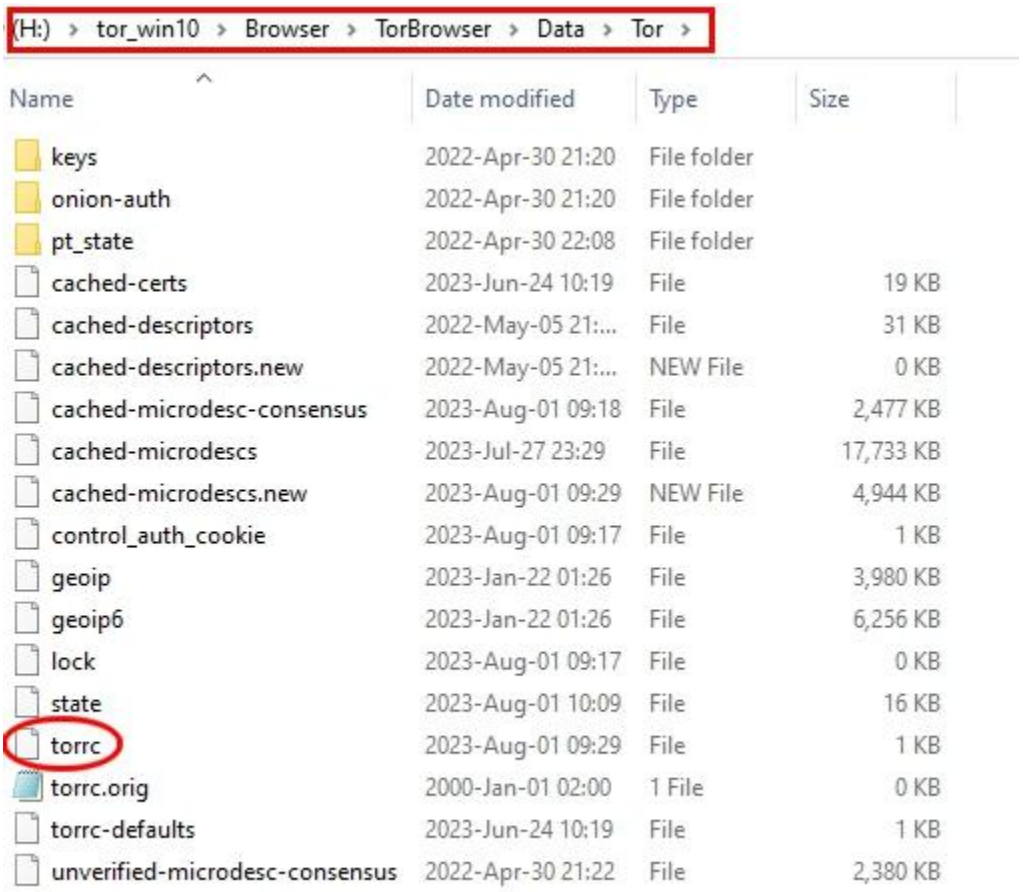
De exemplu, ca în imaginile precedente:

- vrem ca reţeaua de anonimizare să ne preia ca fiind în Rusia
- şi ca din ultimul nod al reţelei de anonimizare să ieşim cu identitate (ca loc) de Islanda

Aceasta se face editând un fişier din directorul/folderul unde am instalat browserul TOR, astfel:

Pornim un program de explorare a conţinutului computerului, de exemplu "Windows Explorer"/"My Computer"

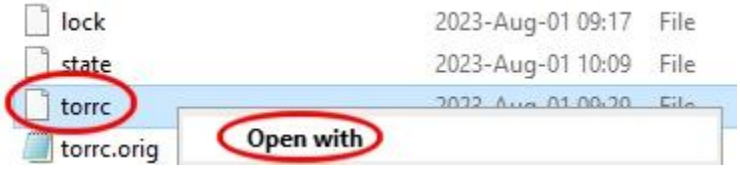
Mergem până în directorul/folderul unde am instalat Tor şi mai departe în subdirectoare până ce găsim fişierul "torrc" (nu are extensie), ca în imaginea următoare:



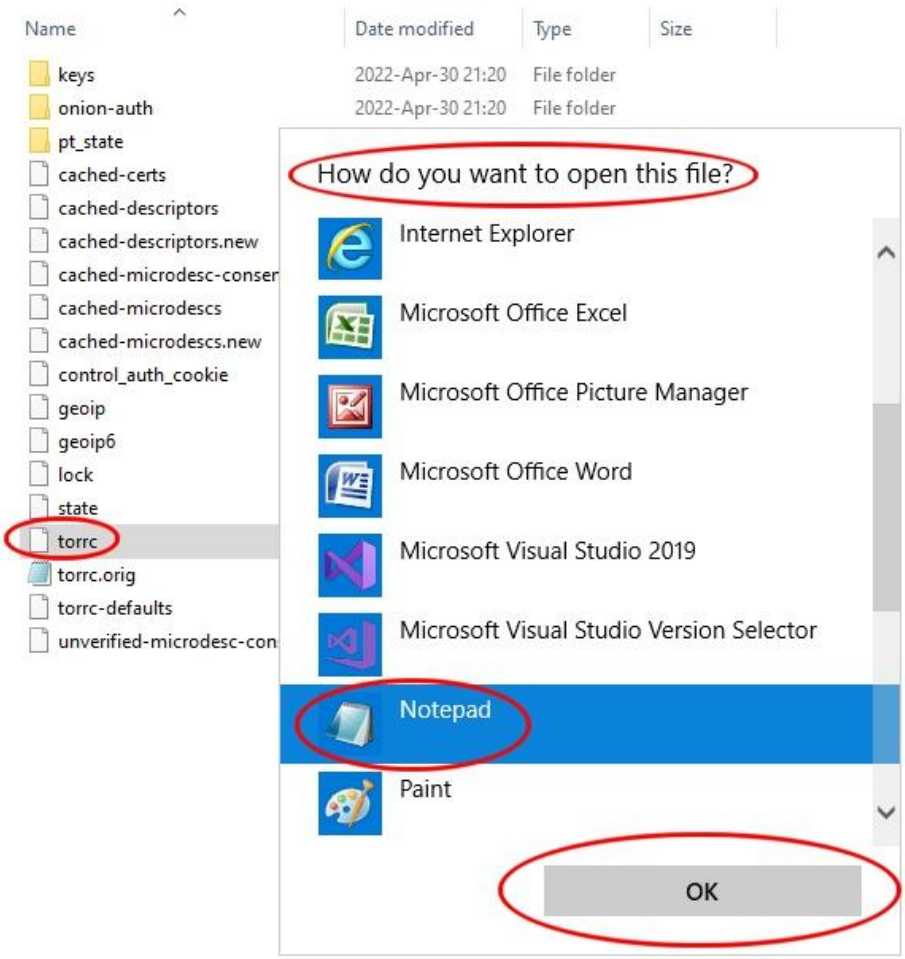
Deschidem pentru editare acest fişier.

În imaginea următoare, care ilustrează procedura din sistemul de operare *Windows 10*, aceasta se face astfel:

- click-dreapta pe numele acelui fişier
- se alege comanda "*Open with*"
    - fiindcă acest fişier nu are extensie, este probabil ca sistemul de operare să nu "ştie" cu ce program se poate deschide/edita în mod implicit acest tip de fişiere (fără extensie)

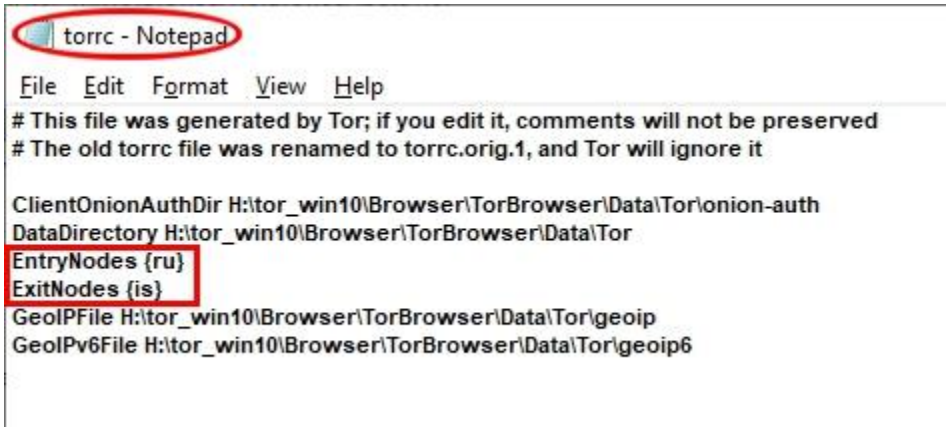


- se alege programul "*Notepad*"
    - deoarece fişierul "torrc" conţine text neformatat, încât acest program este suficient pentru a edita acel conţinut



După ce alegem "*Notepad*" apăsăm butonul "*OK*":

Fişierul va fi deschis şi îl putem edita/schimba:



Este recomandat să NU schimbăm nimic altceva din acest fişier, decât punctul de pornire şi de ieşire din reţeaua de anonimizare – anume:

EntryNodes
şi
ExitNodes

Acestea sunt proprietăţile folosite/solicitate de către browserul TOR
la intrarea şi la ieşirea din reţeaua de anonimizare.

Se vede cum în acest moment între acloladele corespunzătoare fiecărei proprietăţi se află, respectiv, indicativ ale ţărilor unde ne-am afla şi de unde am ieşi:

EntryNodes {**ru**}
"ru" indicând **Rusia**

ExitNodes {**is**}
"is" indicând **Islanda**

Aceste două indicative au fost citite şi folosite de către browser pentru a parcurge circuitul/traseul până la site(-urile) vizitat(e) în această sesiune.

Cele două ţări astfel indicate fiind ţările pe care le-am văzut adineauri în browserul Tor când am solicitat informaţii despre circuitul/traseul parcurs de la browser până la site-ul *CentralOps*.

Pentru a ne asuma altă identitate pe internet decât cea marcată de aceste două ţări

- schimbâm aceste indicative în fişierul "torrc"
- apoi salvăm (**Ctrl S**, în *Notepad*) fişierul "torrc"
- apoi închidem şi repornim browserul Tor
    - unde putem verifica noua identitate, cum s-a prezentat mai sus:
        - fie vizitând un site şi apoi solicitând informaţii despre circuitul/traseul până acolo cu click pe pictograma din stânga adresei site-ului
        - fie vizitând site-ul *CentralOps* unde sunt oferite informaţii detaliate despre adresa IP cu care ieşim din reţeaua de anonimizare şi deci cea care ne identifică la un site vizitat în această sesiune de navigare cu browserul TOR

Facem aceasta alegând din indicativele corespunzătoare ţărilor din lista următoare:

```
ASCENSION ISLAND                    {ac}
AFGHANISTAN                         {af}
ALAND                               {ax}
ALBANIA                             {al}
ALGERIA                             {dz}
ANDORRA                             {ad}
ANGOLA                              {ao}
ANGUILLA                            {ai}
ANTARCTICA                          {aq}
ANTIGUA AND BARBUDA                 {ag}
ARGENTINA REPUBLIC                  {ar}
ARMENIA                             {am}
ARUBA                               {aw}
AUSTRALIA                           {au}
AUSTRIA                             {at}
AZERBAIJAN                          {az}
BAHAMAS                             {bs}
BAHRAIN                             {bh}
BANGLADESH                          {bd}
BARBADOS                            {bb}
BELARUS                             {by}
BELGIUM                             {be}
BELIZE                              {bz}
BENIN                               {bj}
BERMUDA                             {bm}
BHUTAN                              {bt}
BOLIVIA                             {bo}
BOSNIA AND HERZEGOVINA              {ba}
BOTSWANA                            {bw}
BOUVET ISLAND                       {bv}
BRAZIL                              {br}
BRITISH INDIAN OCEAN TERR           {io}
BRITISH VIRGIN ISLANDS              {vg}
BRUNEI DARUSSALAM                   {bn}
BULGARIA                            {bg}
BURKINA FASO                        {bf}
BURUNDI                             {bi}
CAMBODIA                            {kh}
CAMEROON                            {cm}
CANADA                              {ca}
CAPE VERDE                          {cv}
```

CAYMAN ISLANDS	{ky}
CENTRAL AFRICAN REPUBLIC	{cf}
CHAD	{td}
CHILE	{cl}
PEOPLE'S REPUBLIC OF CHINA	{cn}
CHRISTMAS ISLANDS	{cx}
COCOS ISLANDS	{cc}
COLOMBIA	{co}
COMORAS	{km}
CONGO	{cg}
CONGO (DEMOCRATIC REPUBLIC)	{cd}
COOK ISLANDS	{ck}
COSTA RICA	{cr}
COTE D IVOIRE	{ci}
CROATIA	{hr}
CUBA	{cu}
CYPRUS	{cy}
CZECH REPUBLIC	{cz}
DENMARK	{dk}
DJIBOUTI	{dj}
DOMINICA	{dm}
DOMINICAN REPUBLIC	{do}
EAST TIMOR	{tp}
ECUADOR	{ec}
EGYPT	{eg}
EL SALVADOR	{sv}
EQUATORIAL GUINEA	{gq}
ESTONIA	{ee}
ETHIOPIA	{et}
FALKLAND ISLANDS	{fk}
FAROE ISLANDS	{fo}
FIJI	{fj}
FINLAND	{fi}
FRANCE	{fr}
FRANCE METROPOLITAN	{fx}
FRENCH GUIANA	{gf}
FRENCH POLYNESIA	{pf}
FRENCH SOUTHERN TERRITORIES	{tf}
GABON	{ga}
GAMBIA	{gm}
GEORGIA	{ge}
GERMANY	{de}
GHANA	{gh}
GIBRALTER	{gi}
GREECE	{gr}
GREENLAND	{gl}
GRENADA	{gd}
GUADELOUPE	{gp}
GUAM	{gu}
GUATEMALA	{gt}
GUINEA	{gn}
GUINEA-BISSAU	{gw}
GUYANA	{gy}
HAITI	{ht}
HEARD & MCDONALD ISLAND	{hm}

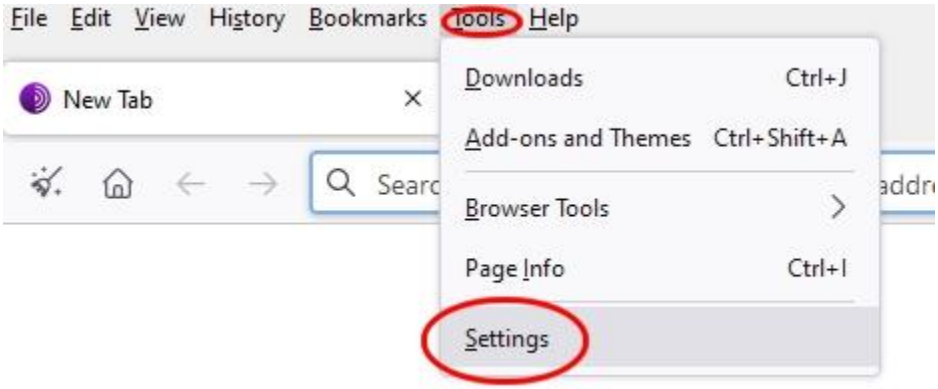
HONDURAS	{hn}
HONG KONG	{hk}
HUNGARY	{hu}
ICELAND	{is}
INDIA	{in}
INDONESIA	{id}
IRAN, ISLAMIC REPUBLIC OF	{ir}
IRAQ	{iq}
IRELAND	{ie}
ISLE OF MAN	{im}
ISRAEL	{il}
ITALY	{it}
JAMAICA	{jm}
JAPAN	{jp}
JORDAN	{jo}
KAZAKHSTAN	{kz}
KENYA	{ke}
KIRIBATI	{ki}
KOREA, DEM. PEOPLES REP OF	{kp}
KOREA, REPUBLIC OF	{kr}
KUWAIT	{kw}
KYRGYZSTAN	{kg}
LAO PEOPLE'S DEM. REPUBLIC	{la}
LATVIA	{lv}
LEBANON	{lb}
LESOTHO	{ls}
LIBERIA	{lr}
LIBYAN ARAB JAMAHIRIYA	{ly}
LIECHTENSTEIN	{li}
LITHUANIA	{lt}
LUXEMBOURG	{lu}
MACAO	{mo}
MACEDONIA	{mk}
MADAGASCAR	{mg}
MALAWI	{mw}
MALAYSIA	{my}
MALDIVES	{mv}
MALI	{ml}
MALTA	{mt}
MARSHALL ISLANDS	{mh}
MARTINIQUE	{mq}
MAURITANIA	{mr}
MAURITIUS	{mu}
MAYOTTE	{yt}
MEXICO	{mx}
MICRONESIA	{fm}
MOLDAVA REPUBLIC OF	{md}
MONACO	{mc}
MONGOLIA	{mn}
MONTENEGRO	{me}
MONTSERRAT	{ms}
MOROCCO	{ma}
MOZAMBIQUE	{mz}
MYANMAR	{mm}
NAMIBIA	{na}

NAURU	{nr}
NEPAL	{np}
NETHERLANDS ANTILLES	{an}
NETHERLANDS, THE	{nl}
NEW CALEDONIA	{nc}
NEW ZEALAND	{nz}
NICARAGUA	{ni}
NIGER	{ne}
NIGERIA	{ng}
NIUE	{nu}
NORFOLK ISLAND	{nf}
NORTHERN MARIANA ISLANDS	{mp}
NORWAY	{no}
OMAN	{om}
PAKISTAN	{pk}
PALAU	{pw}
PALESTINE	{ps}
PANAMA	{pa}
PAPUA NEW GUINEA	{pg}
PARAGUAY	{py}
PERU	{pe}
PHILIPPINES (REPUBLIC OF THE)	{ph}
PITCAIRN	{pn}
POLAND	{pl}
PORTUGAL	{pt}
PUERTO RICO	{pr}
QATAR	{qa}
REUNION	{re}
ROMANIA	{ro}
RUSSIAN FEDERATION	{ru}
RWANDA	{rw}
SAMOA	{ws}
SAN MARINO	{sm}
SAO TOME/PRINCIPE	{st}
SAUDI ARABIA	{sa}
SCOTLAND	{uk}
SENEGAL	{sn}
SERBIA	{rs}
SEYCHELLES	{sc}
SIERRA LEONE	{sl}
SINGAPORE	{sg}
SLOVAKIA	{sk}
SLOVENIA	{si}
SOLOMON ISLANDS	{sb}
SOMALIA	{so}
SOMOA,GILBERT,ELLICE ISLANDS	{as}
SOUTH AFRICA	{za}
SOUTH GEORGIA, SOUTH SANDWICH ISLANDS	{gs}
SOVIET UNION	{su}
SPAIN	{es}
SRI LANKA	{lk}
ST. HELENA	{sh}
ST. KITTS AND NEVIS	{kn}
ST. LUCIA	{lc}
ST. PIERRE AND MIQUELON	{pm}

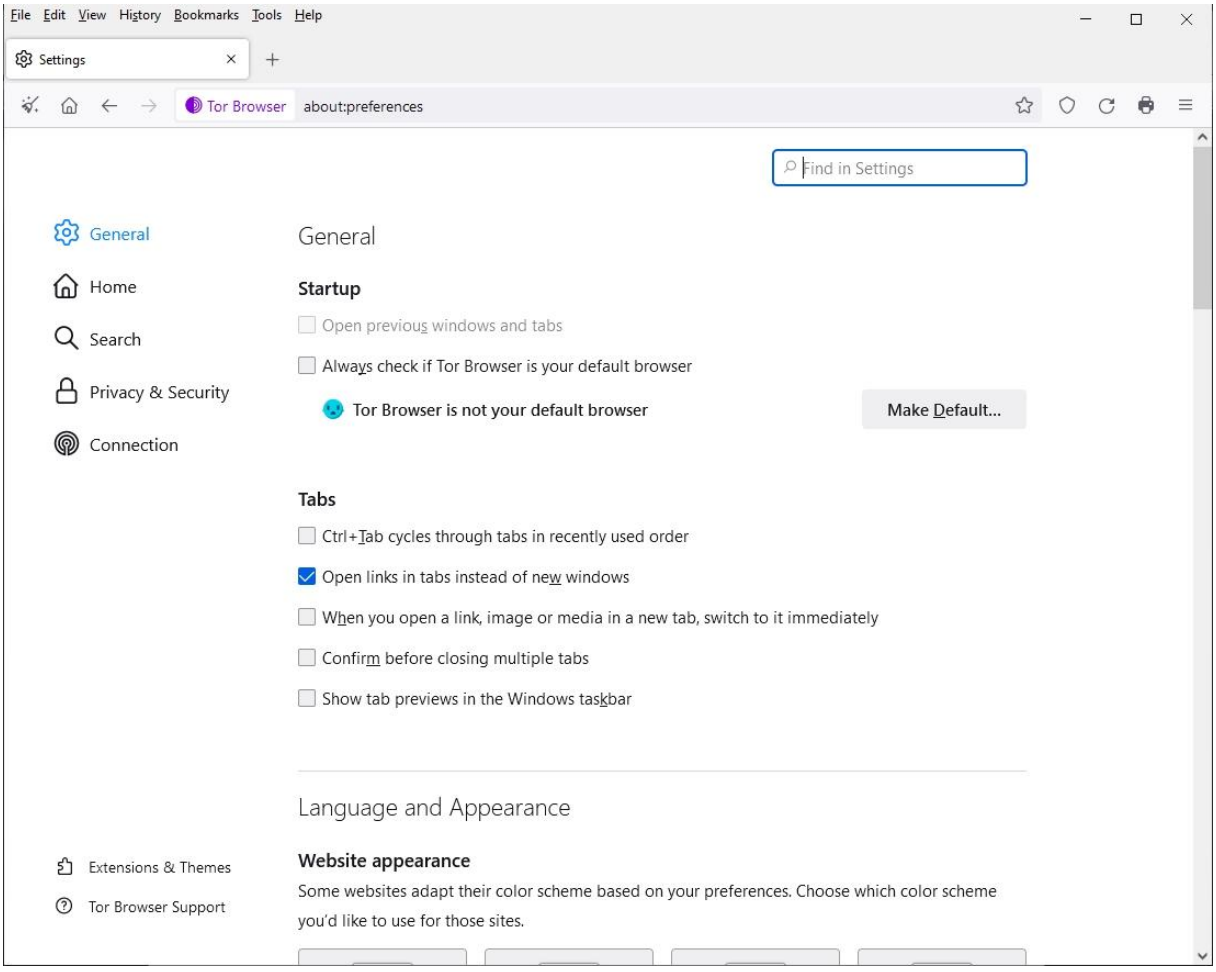
ST. VINCENT & THE GRENADINES	{vc}
SUDAN	{sd}
SURINAME	{sr}
SVALBARD AND JAN MAYEN	{sj}
SWAZILAND	{sz}
SWEDEN	{se}
SWITZERLAND	{ch}
SYRIAN ARAB REPUBLIC	{sy}
TAIWAN	{tw}
TAJIKISTAN	{tj}
TANZANIA, UNITED REPUBLIC OF	{tz}
THAILAND	{th}
TOGO	{tg}
TOKELAU	{tk}
TONGA	{to}
TRINIDAD AND TOBAGO	{tt}
TUNISIA	{tn}
TURKEY	{tr}
TURKMENISTAN	{tm}
TURKS AND CALCOS ISLANDS	{tc}
TUVALU	{tv}
UGANDA	{ug}
UKRAINE	{ua}
UNITED ARAB EMIRATES	{ae}
UNITED KINGDOM (no new registrations)	{gb}
UNITED KINGDOM	{uk}
UNITED STATES	{us}
UNITED STATES MINOR OUTL.IS.	{um}
URUGUAY	{uy}
UZBEKISTAN	{uz}
VANUATU	{vu}
VATICAN CITY STATE	{va}
VENEZUELA	{ve}
VIET NAM	{vn}
VIRGIN ISLANDS (USA)	{vi}
WALLIS AND FUTUNA ISLANDS	{wf}
WESTERN SAHARA	{eh}
YEMEN	{ye}
ZAMBIA	{zm}
ZIMBABWE	{zw}

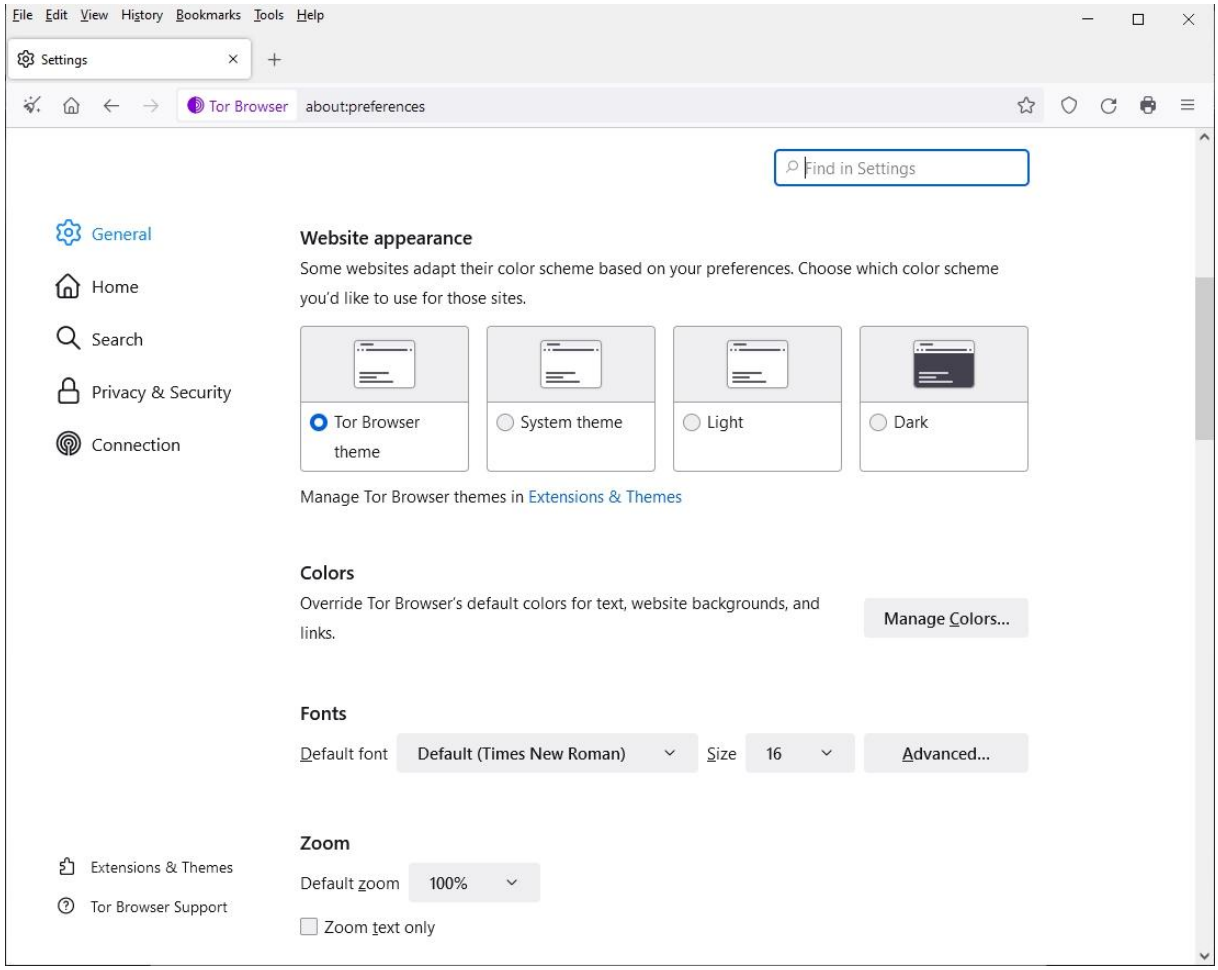
Setări importante pentru browserul TOR

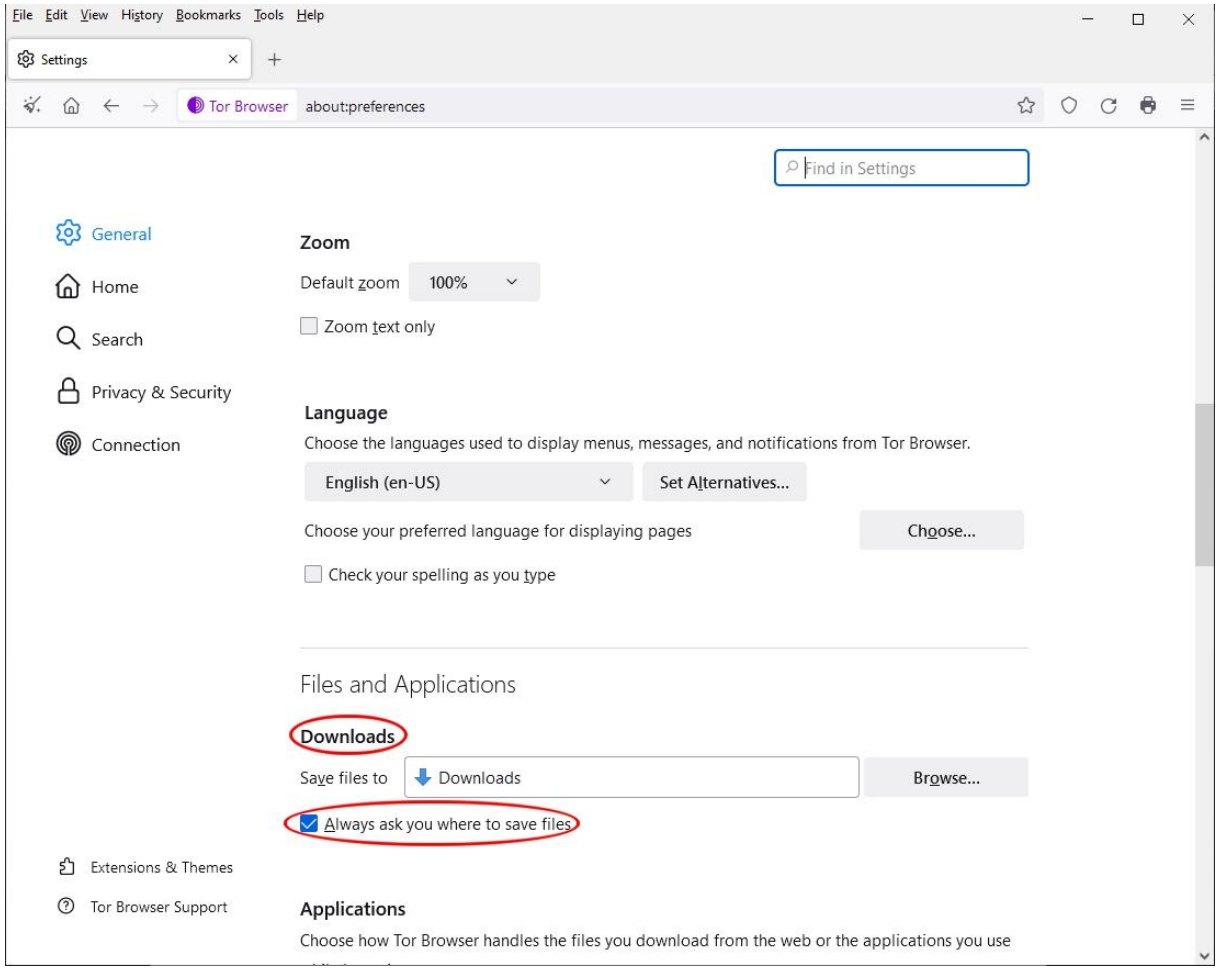
Unele proprietăţi importante ale browserului TOR pot fi accesate şi modificate din meniul "*Tools*", astfel:

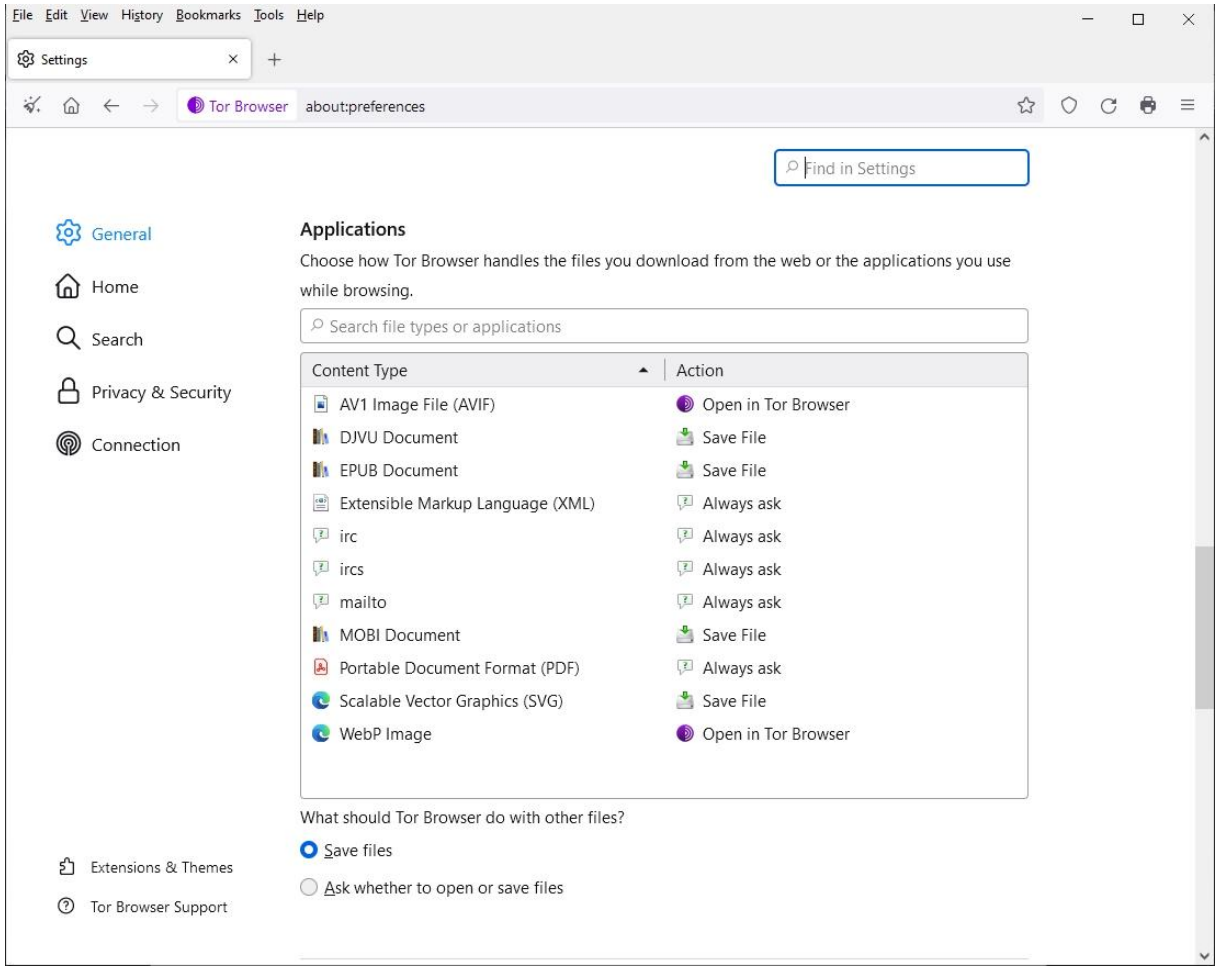


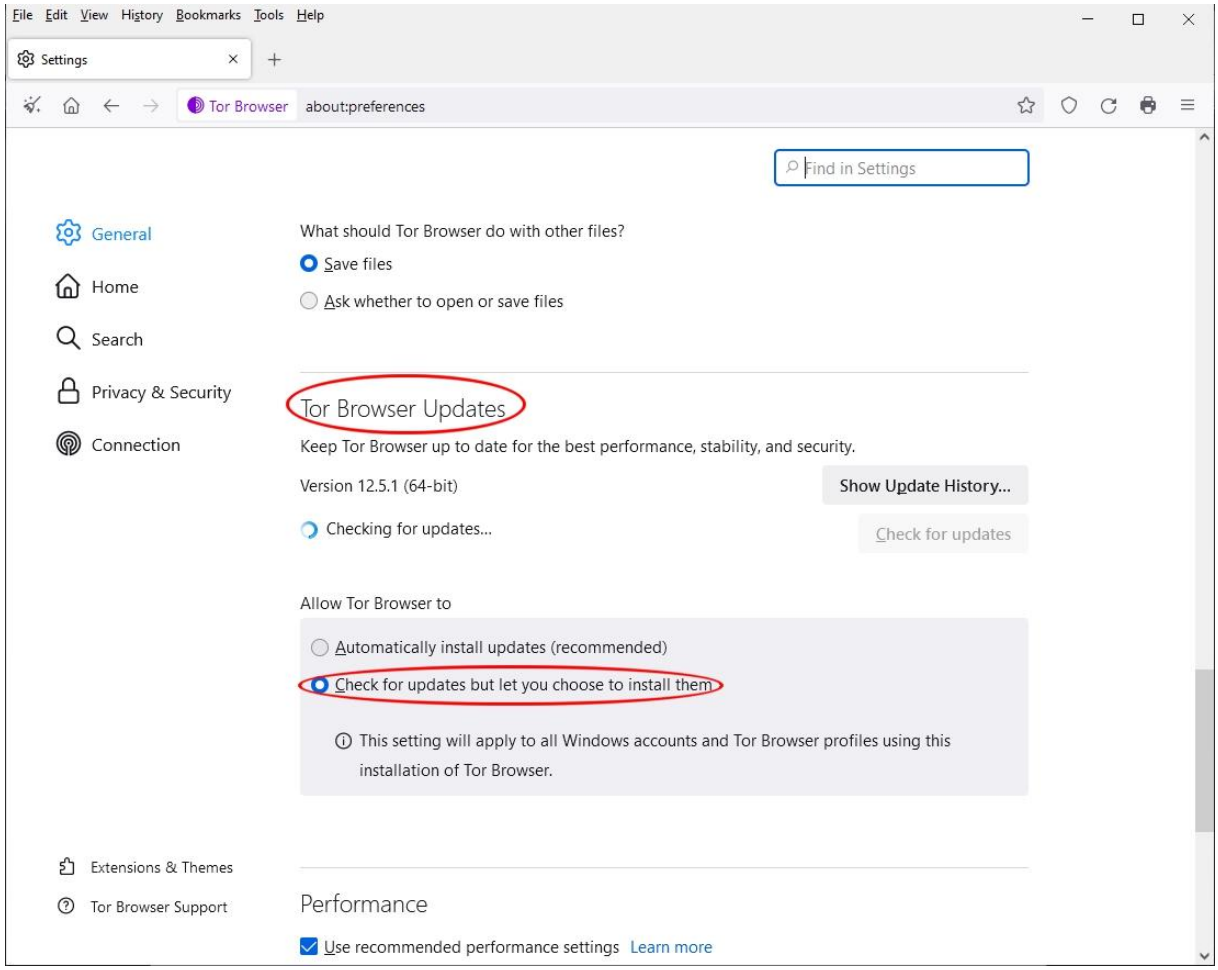
În pagina "*General*":

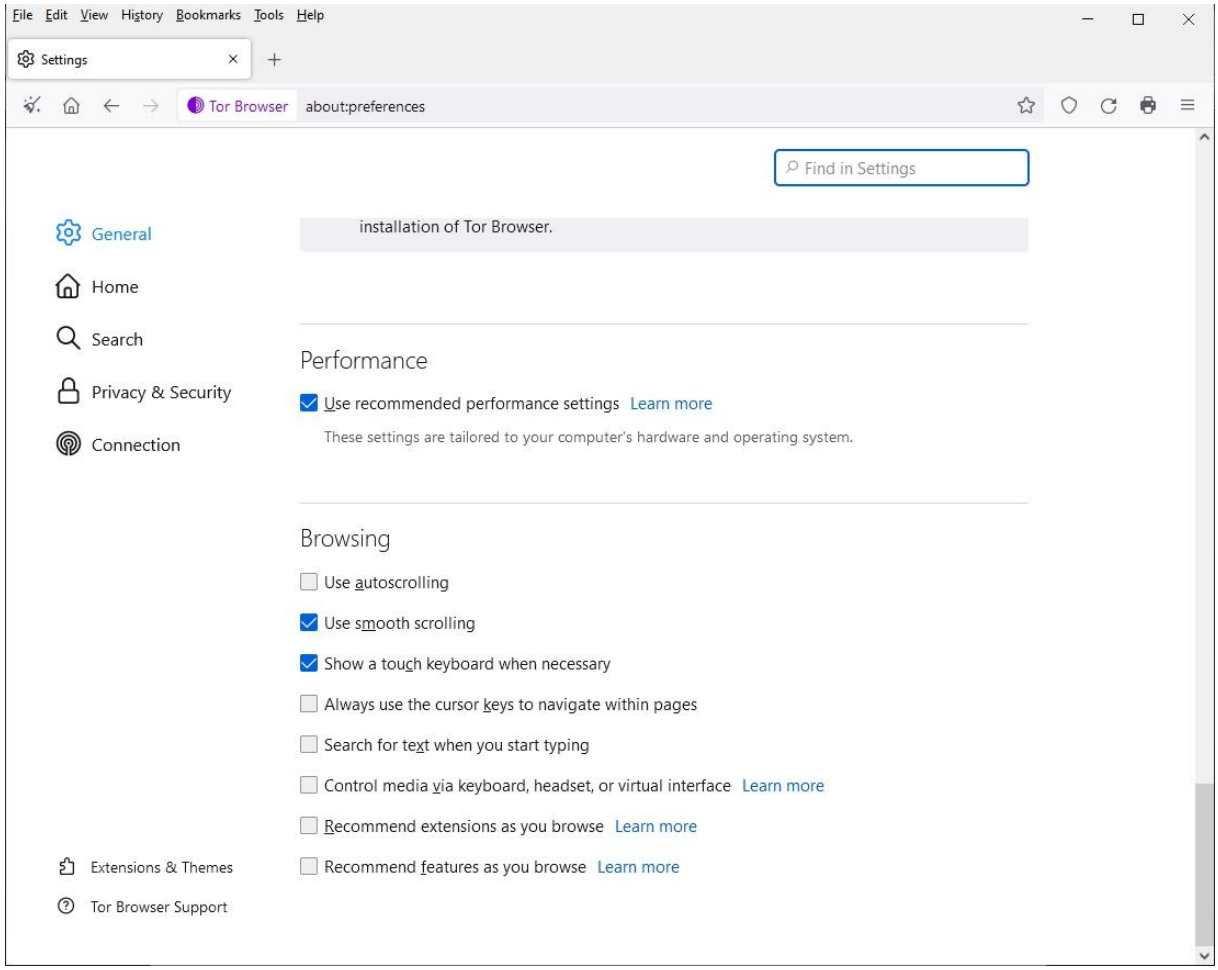



File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences
Find in Settings
General
Home
Search
Privacy & Security
Connection
Website appearance
Some websites adapt their color scheme based on your preferences. Choose which color scheme you'd like to use for those sites.
Tor Browser theme
System theme
Light
Dark
Manage Tor Browser themes in Extensions & Themes
Colors
Override Tor Browser's default colors for text, website backgrounds, and links.
Manage Colors...
Fonts
Default font
Default (Times New Roman)
Size
16
Advanced...
Zoom
Default zoom
100%
Zoom text only
Extensions & Themes
Tor Browser Support

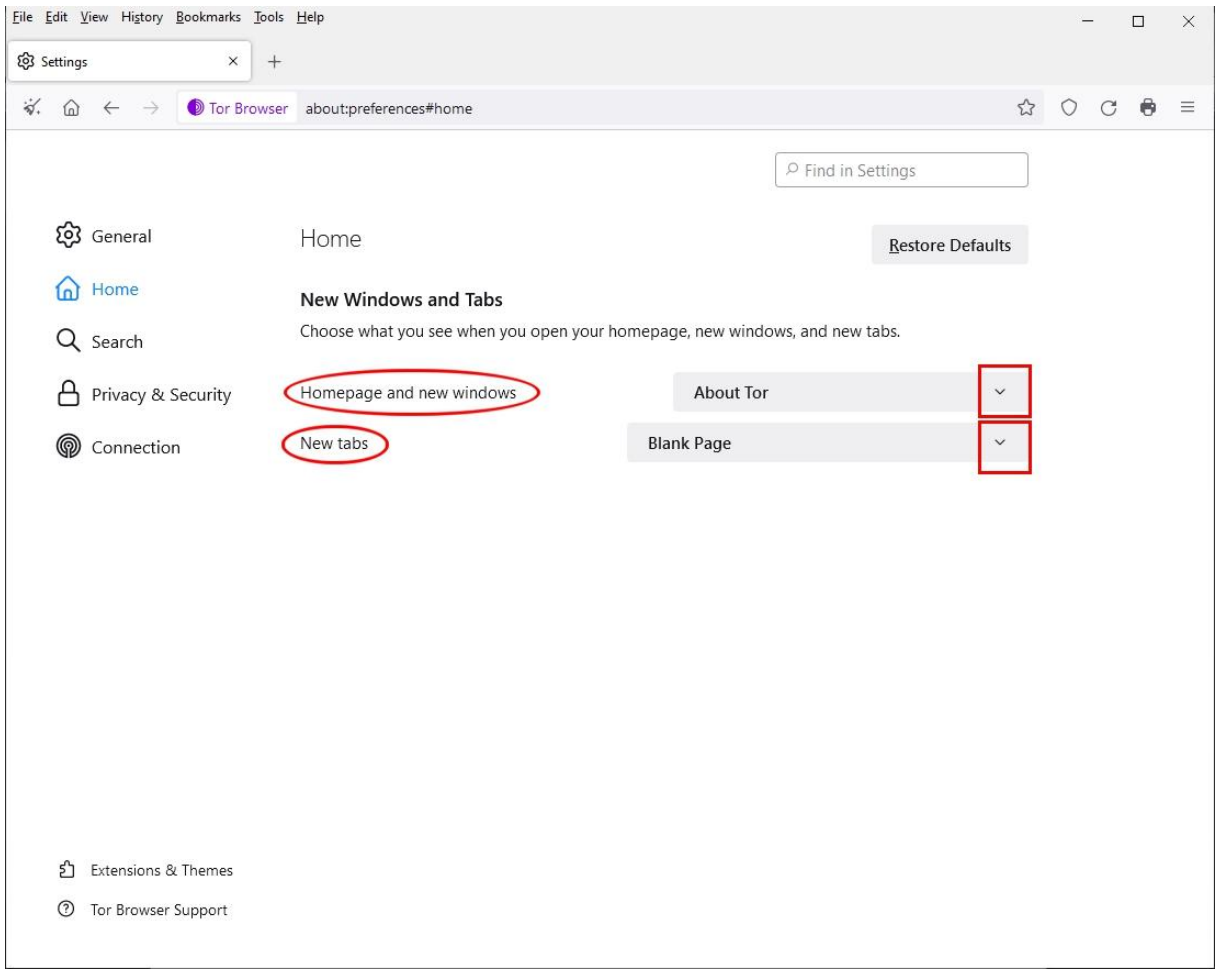

File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences
Find in Settings
General
Home
Search
Privacy & Security
Connection
Extensions & Themes
Tor Browser Support
Zoom
Default zoom
100%
Zoom text only
Language
Choose the languages used to display menus, messages, and notifications from Tor Browser.
English (en-US)
Set Alternatives...
Choose your preferred language for displaying pages
Choose...
Check your spelling as you type
Files and Applications
Downloads
Save files to
Downloads
Browse...
Always ask you where to save files
Applications
Choose how Tor Browser handles the files you download from the web or the applications you use


File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences
Find in Settings
General
Home
Search
Privacy & Security
Connection
Extensions & Themes
Tor Browser Support
Applications
Choose how Tor Browser handles the files you download from the web or the applications you use while browsing.
Search file types or applications
Content Type
Action
AV1 Image File (AVIF)
Open in Tor Browser
DJVU Document
Save File
EPUB Document
Save File
Extensible Markup Language (XML)
Always ask
irc
Always ask
ircs
Always ask
mailto
Always ask
MOBI Document
Save File
Portable Document Format (PDF)
Always ask
Scalable Vector Graphics (SVG)
Save File
WebP Image
Open in Tor Browser
What should Tor Browser do with other files?
Save files
Ask whether to open or save files

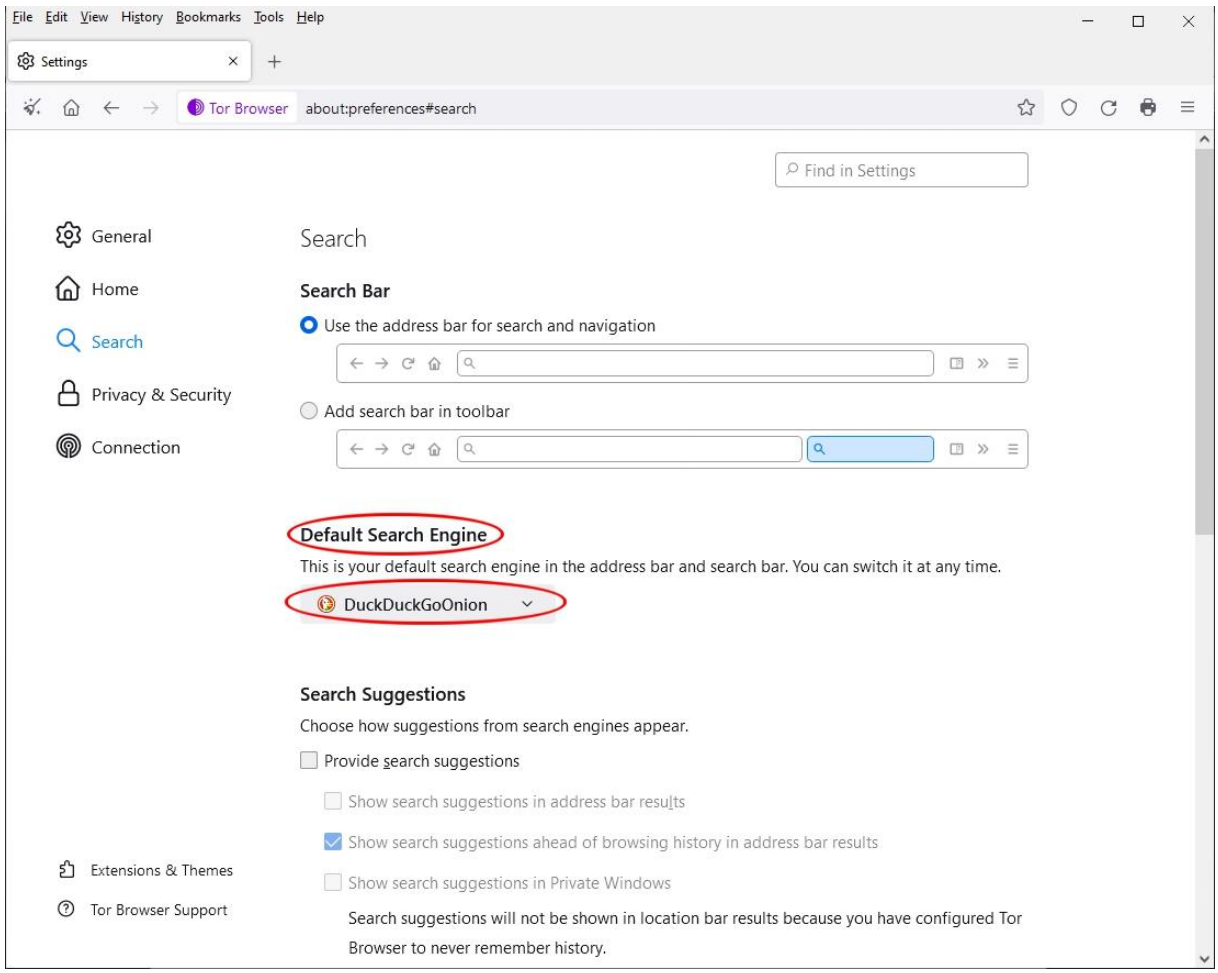

File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences
Find in Settings
General
Home
Search
Privacy & Security
Connection
What should Tor Browser do with other files?
Save files
Ask whether to open or save files
Tor Browser Updates
Keep Tor Browser up to date for the best performance, stability, and security.
Version 12.5.1 (64-bit)
Show Update History...
Checking for updates...
Check for updates
Allow Tor Browser to
Automatically install updates (recommended)
Check for updates but let you choose to install them
This setting will apply to all Windows accounts and Tor Browser profiles using this installation of Tor Browser.
Extensions & Themes
Tor Browser Support
Performance
Use recommended performance settings Learn more

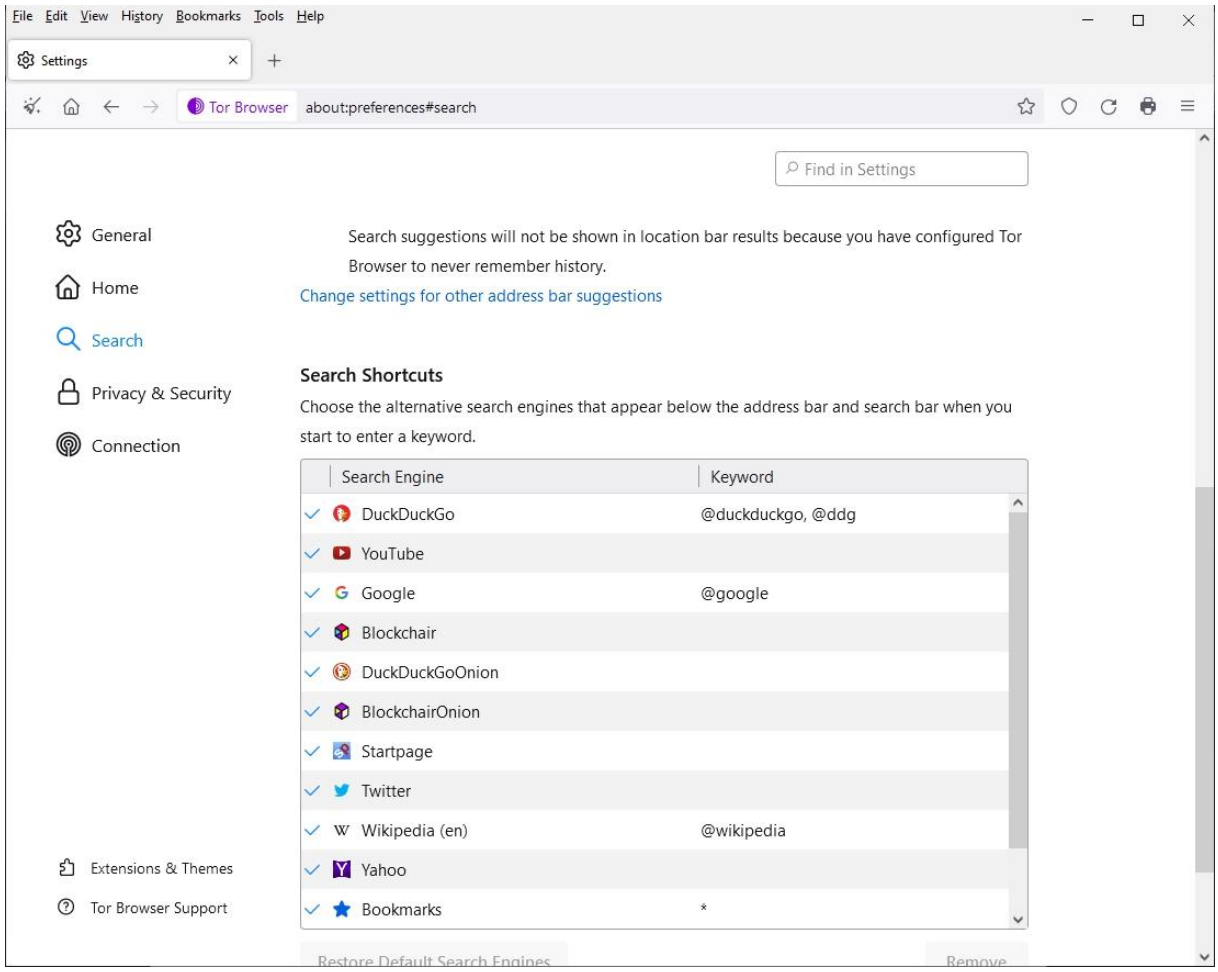

File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences
Find in Settings
General
Home
Search
Privacy & Security
Connection
Extensions & Themes
Tor Browser Support
installation of Tor Browser.
Performance
Use recommended performance settings Learn more
These settings are tailored to your computer's hardware and operating system.
Browsing
Use autoscrolling
Use smooth scrolling
Show a touch keyboard when necessary
Always use the cursor keys to navigate within pages
Search for text when you start typing
Control media via keyboard, headset, or virtual interface Learn more
Recommend extensions as you browse Learn more
Recommend features as you browse Learn more

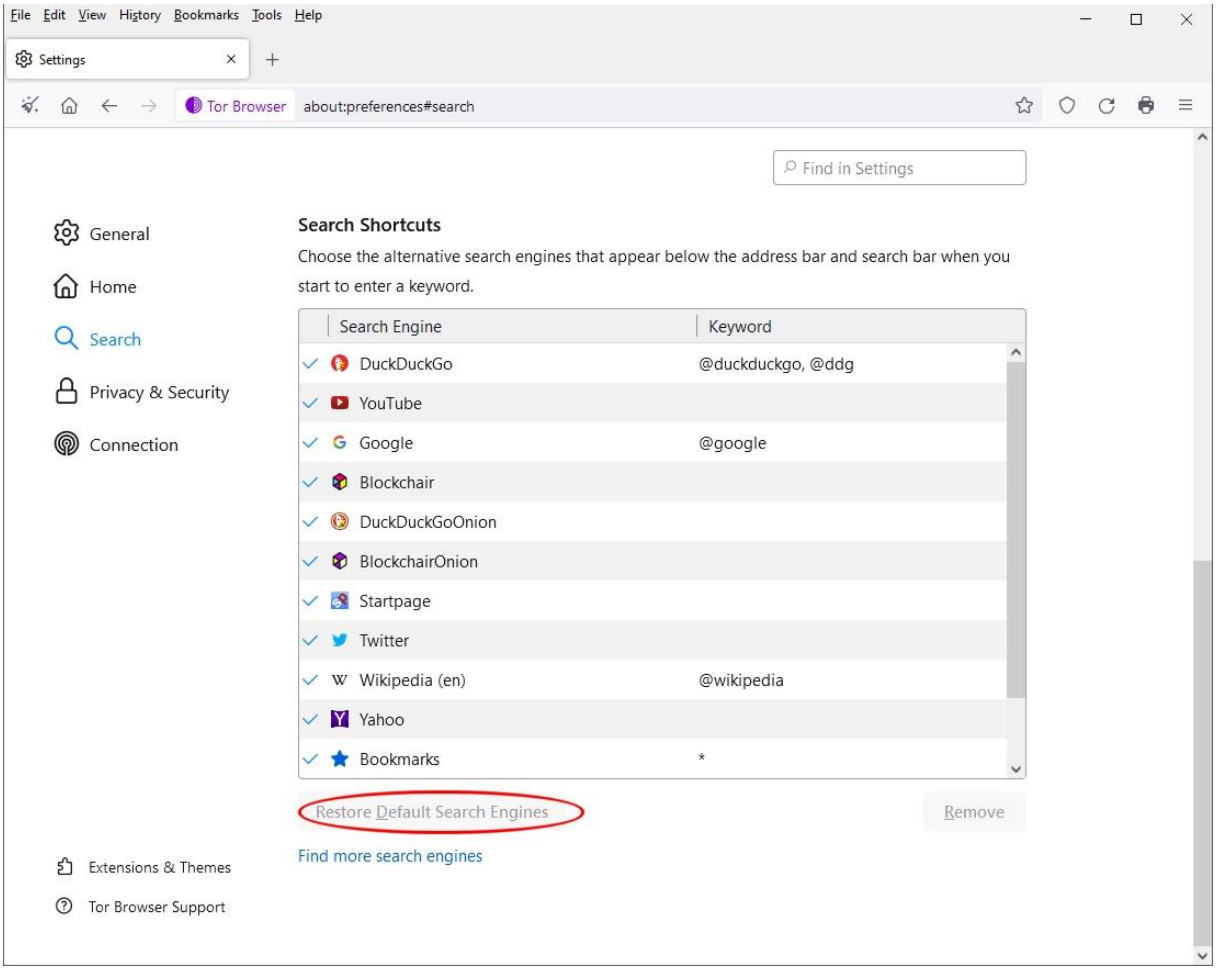
În pagina "*Home*":



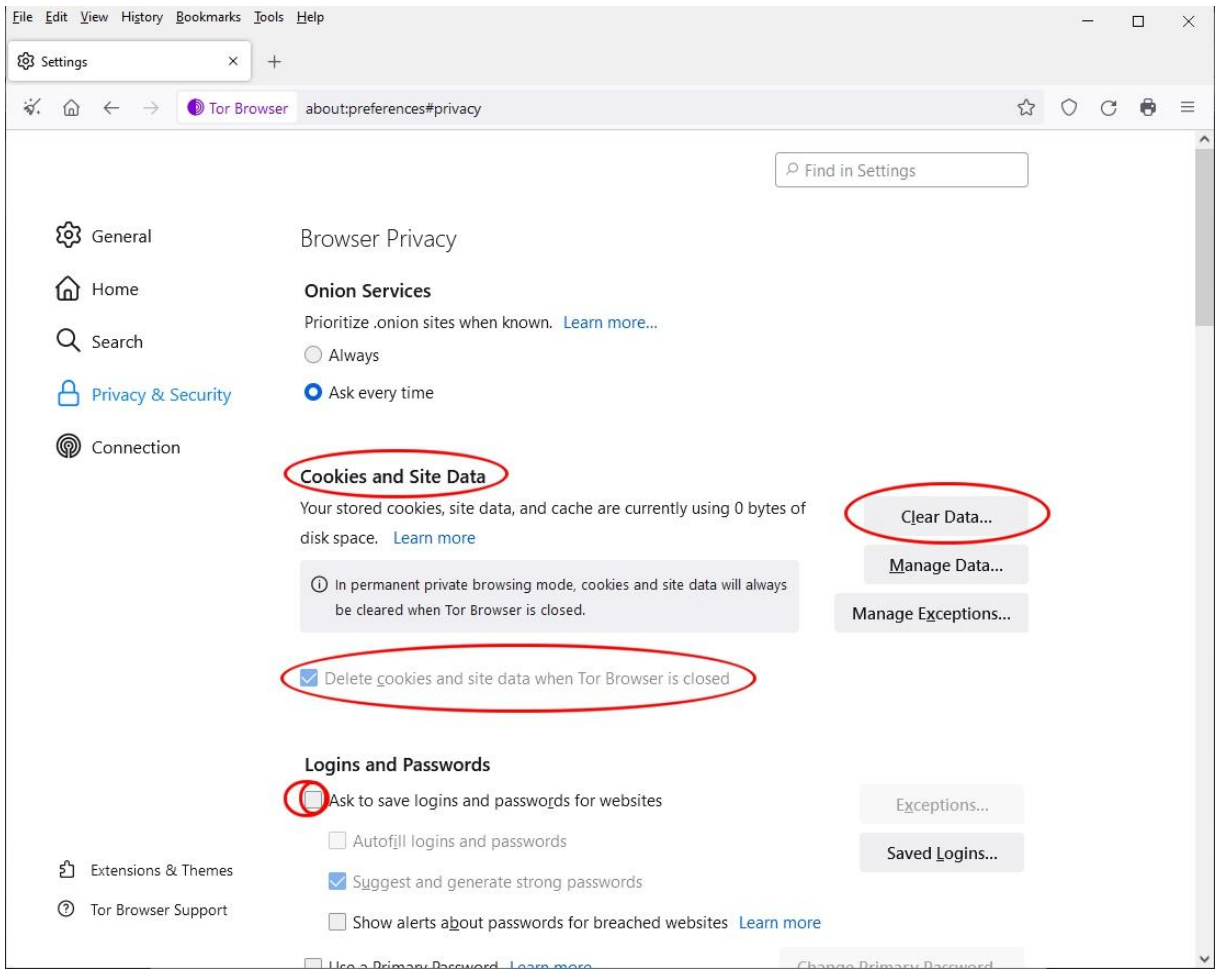
În pagina "*Search*":

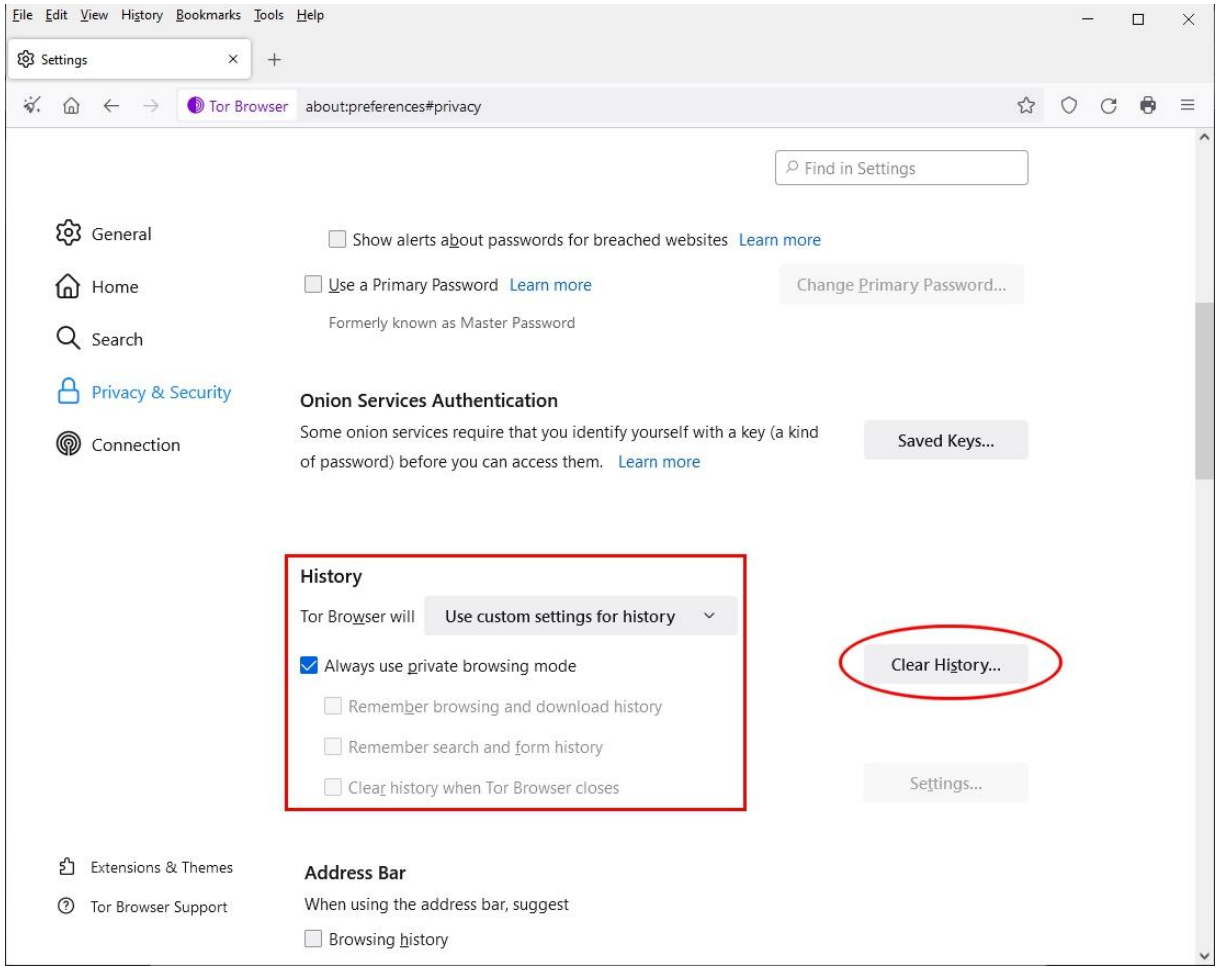


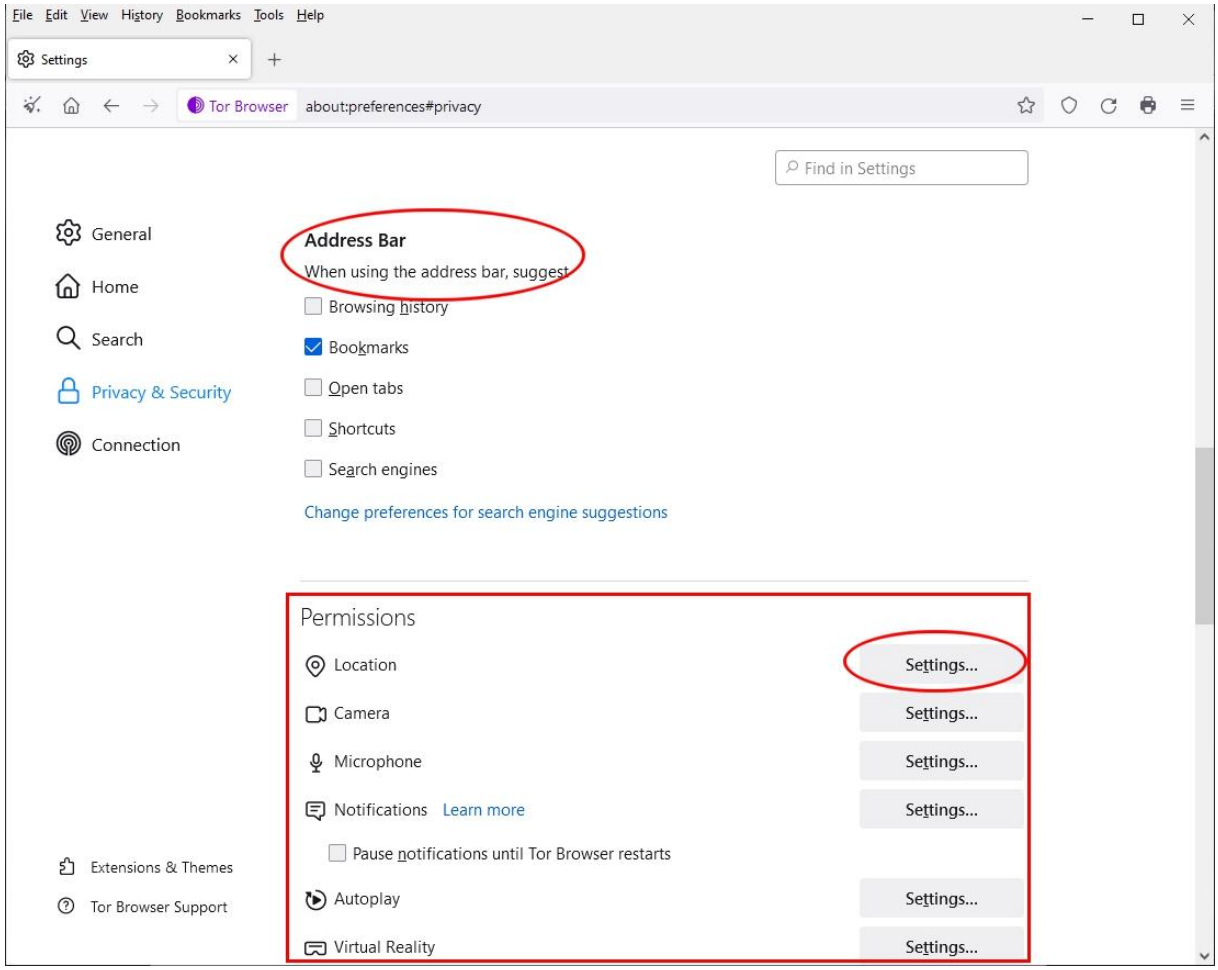

File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences#search
Find in Settings
General
Home
Search
Privacy & Security
Connection
Extensions & Themes
Tor Browser Support
Search suggestions will not be shown in location bar results because you have configured Tor Browser to never remember history.
Change settings for other address bar suggestions
Search Shortcuts
Choose the alternative search engines that appear below the address bar and search bar when you start to enter a keyword.
Search Engine
Keyword
DuckDuckGo
@duckduckgo, @ddg
YouTube
Google
@google
Blockchair
DuckDuckGoOnion
BlockchairOnion
Startpage
Twitter
Wikipedia (en)
@wikipedia
Yahoo
Bookmarks
*
Restore Default Search Engines
Remove

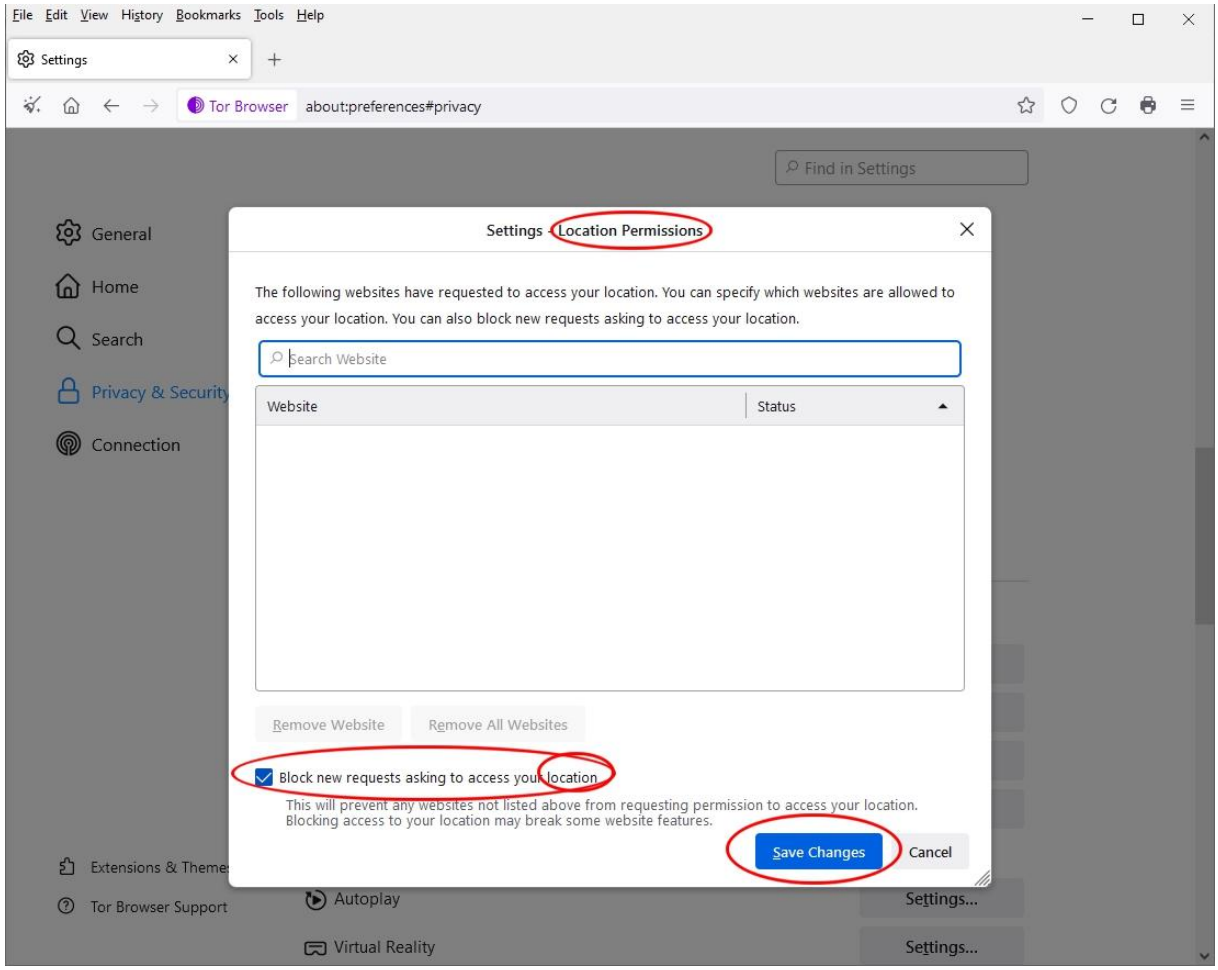

File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences#search
Find in Settings
General
Home
Search
Privacy & Security
Connection
Search Shortcuts
Choose the alternative search engines that appear below the address bar and search bar when you start to enter a keyword.
Search Engine
Keyword
DuckDuckGo
@duckduckgo, @ddg
YouTube
Google
@google
Blockchair
DuckDuckGoOnion
BlockchairOnion
Startpage
Twitter
Wikipedia (en)
@wikipedia
Yahoo
Bookmarks
*
Restore Default Search Engines
Remove
Find more search engines
Extensions & Themes
Tor Browser Support

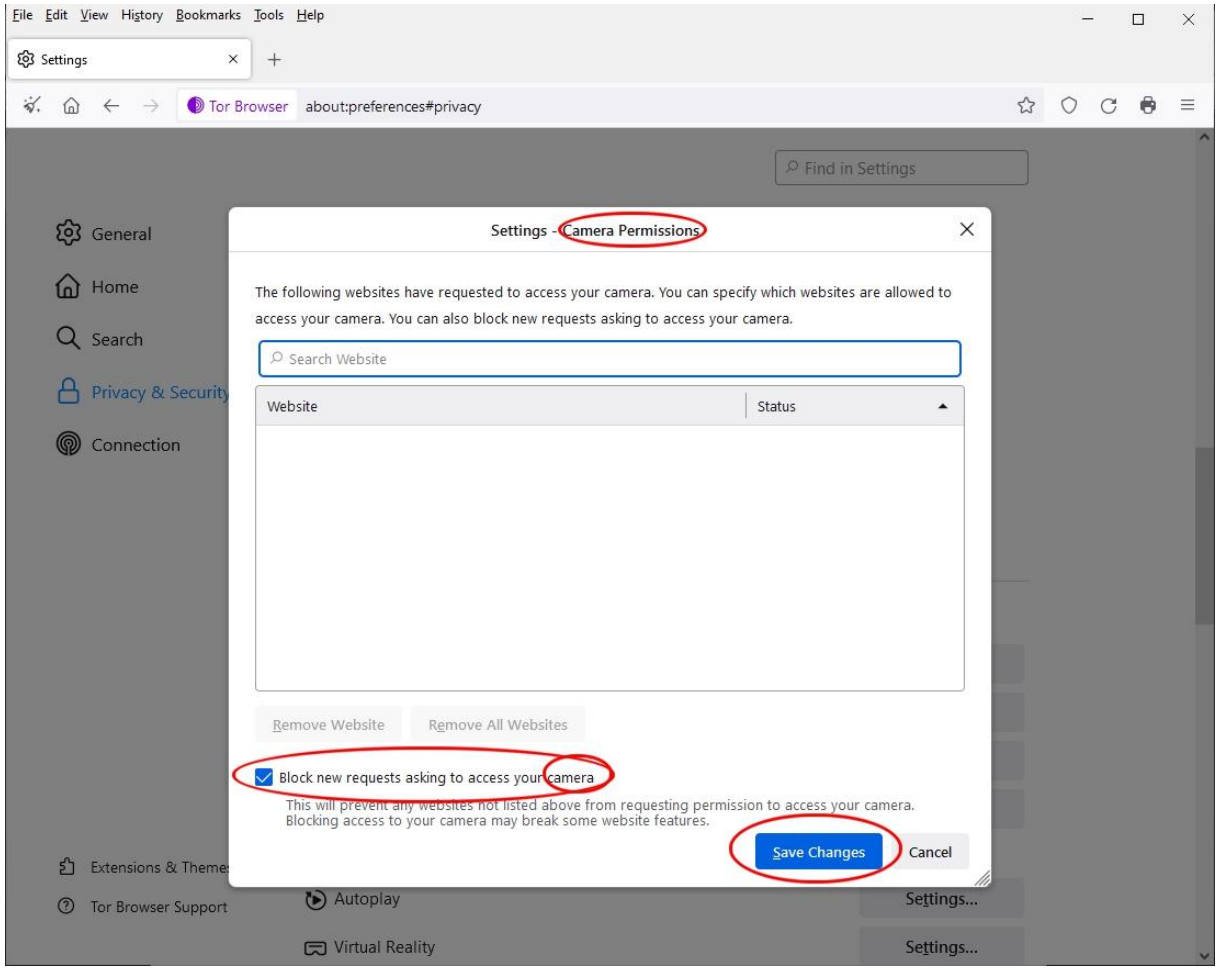
În pagina "*Privacy & Security*":



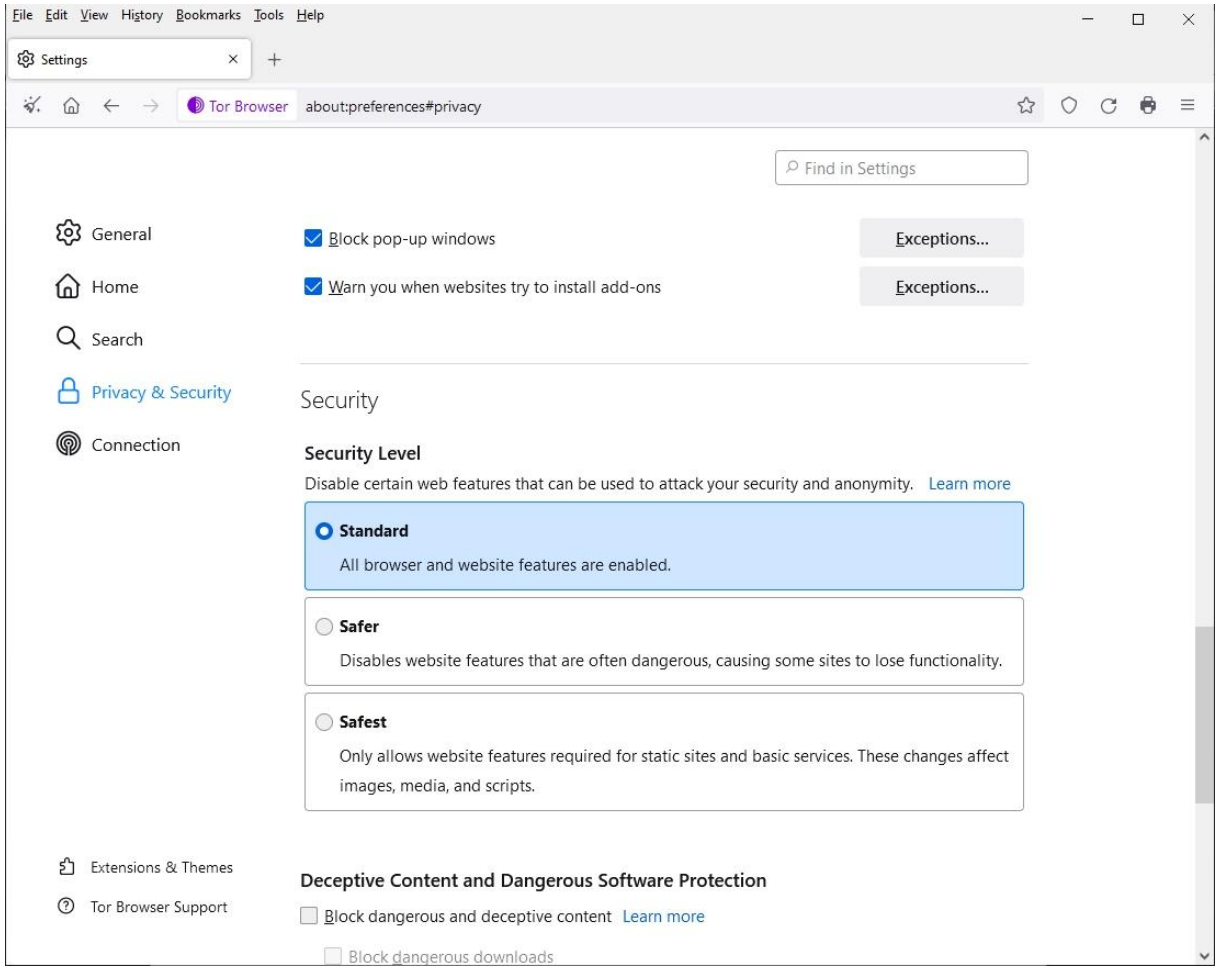

File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences#privacy
Find in Settings
General
Home
Search
Privacy & Security
Connection
Show alerts about passwords for breached websites Learn more
Use a Primary Password Learn more
Change Primary Password...
Formerly known as Master Password
Onion Services Authentication
Some onion services require that you identify yourself with a key (a kind of password) before you can access them. Learn more
Saved Keys...
History
Tor Browser will
Use custom settings for history
Always use private browsing mode
Remember browsing and download history
Remember search and form history
Clear history when Tor Browser closes
Clear History...
Settings...
Extensions & Themes
Tor Browser Support
Address Bar
When using the address bar, suggest
Browsing history

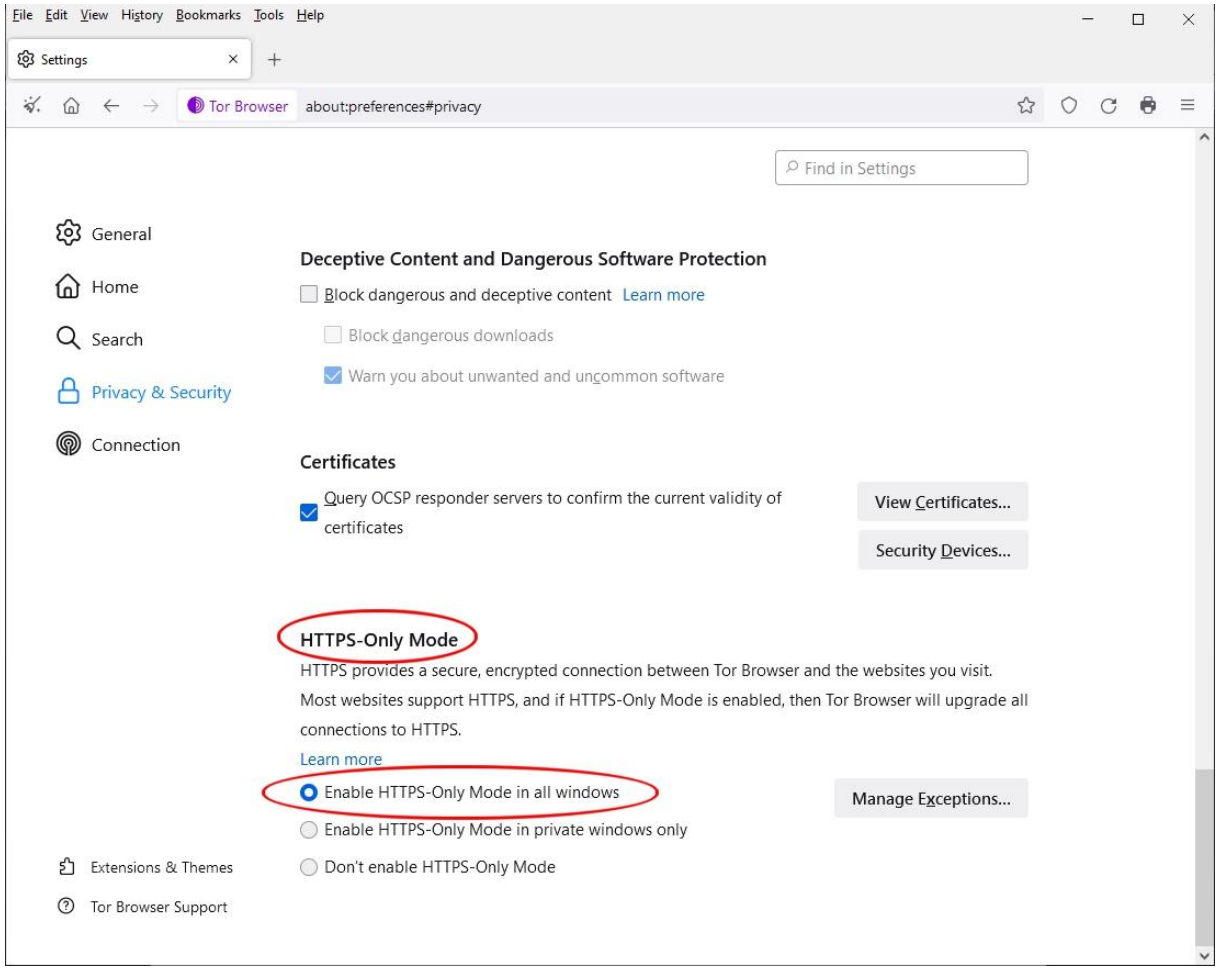

File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences#privacy
Find in Settings
General
Home
Search
Privacy & Security
Connection
Address Bar
When using the address bar, suggest
Browsing history
Bookmarks
Open tabs
Shortcuts
Search engines
Change preferences for search engine suggestions
Permissions
Location
Settings...
Camera
Settings...
Microphone
Settings...
Notifications
Learn more
Settings...
Pause notifications until Tor Browser restarts
Autoplay
Settings...
Virtual Reality
Settings...
Extensions & Themes
Tor Browser Support


File Edit View History Bookmarks Tools Help
Settings
Tor Browser about:preferences#privacy
Find in Settings
General
Home
Search
Privacy & Security
Connection
Settings - Location Permissions
The following websites have requested to access your location. You can specify which websites are allowed to access your location. You can also block new requests asking to access your location.
Search Website
Website
Status
Remove Website
Remove All Websites
Block new requests asking to access your location
This will prevent any websites not listed above from requesting permission to access your location. Blocking access to your location may break some website features.
Save Changes
Cancel
Extensions & Themes
Tor Browser Support
Autoplay
Settings...
Virtual Reality
Settings...

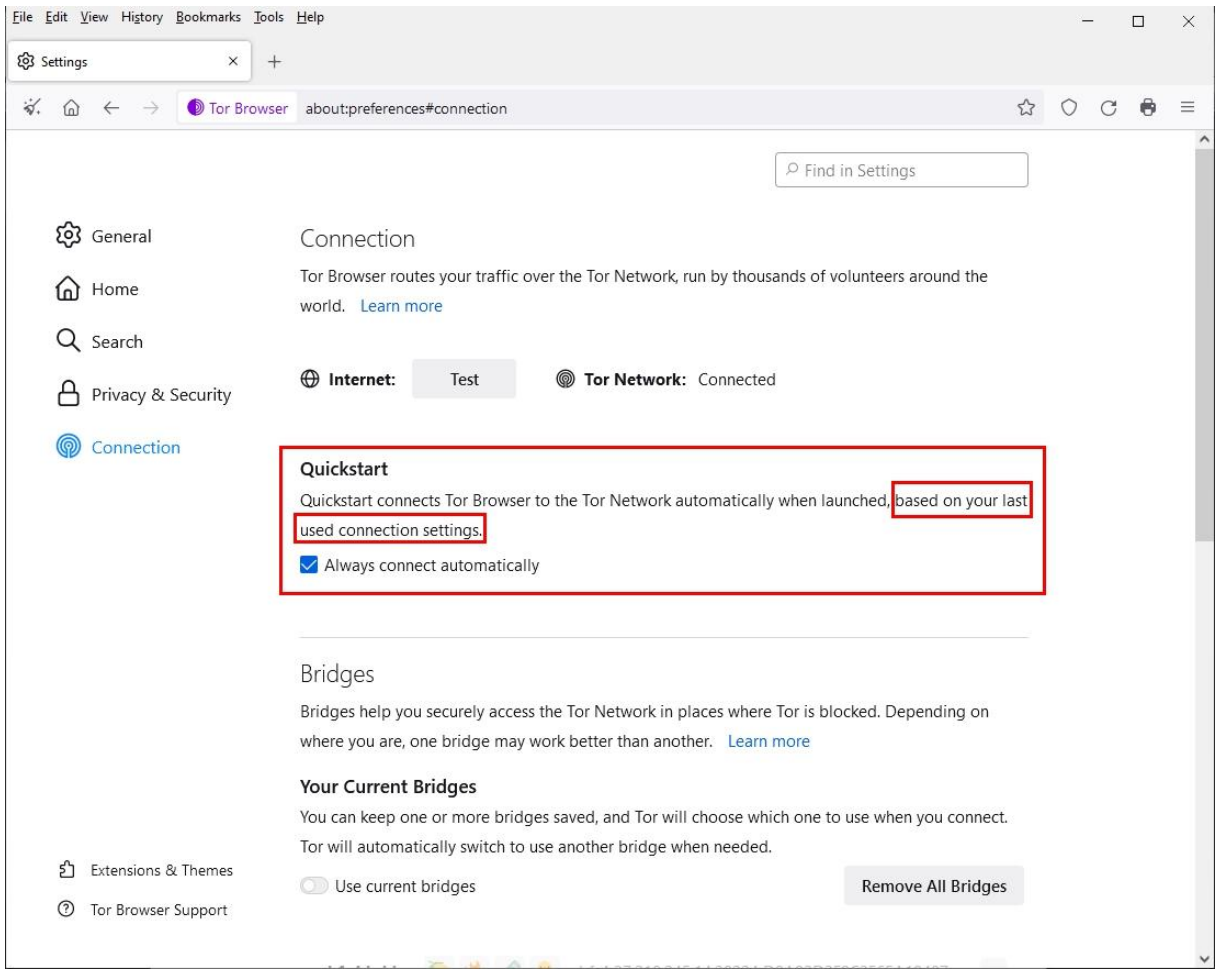


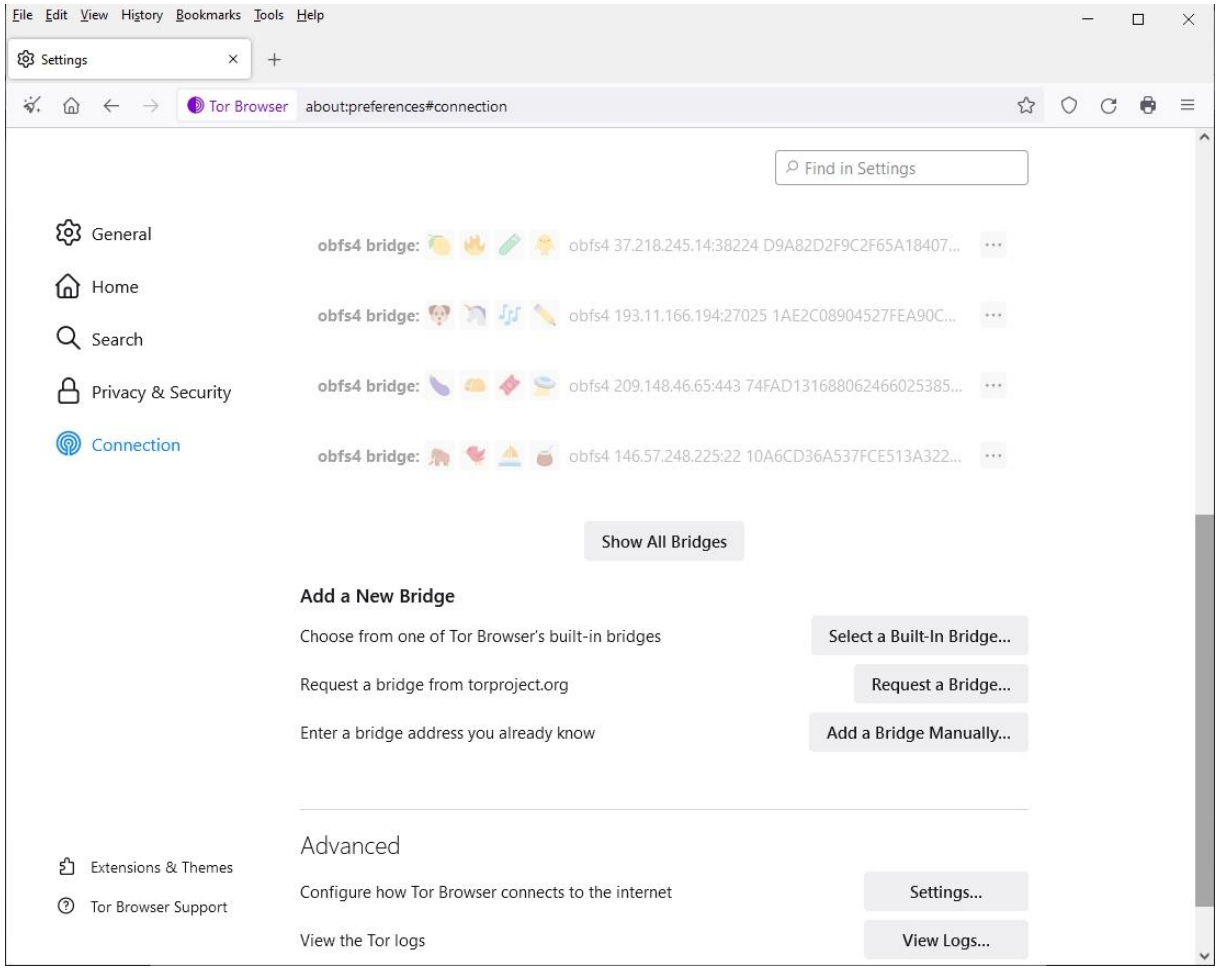
La fel – blocare/"Block" – se setează celelalte permisiuni.


File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences#privacy
Find in Settings
General
Home
Search
Privacy & Security
Connection
Extensions & Themes
Tor Browser Support
Block pop-up windows
Exceptions...
Warn you when websites try to install add-ons
Exceptions...
Security
Security Level
Disable certain web features that can be used to attack your security and anonymity. Learn more
Standard
All browser and website features are enabled.
Safer
Disables website features that are often dangerous, causing some sites to lose functionality.
Safest
Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content Learn more
Block dangerous downloads


File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences#privacy
Find in Settings
General
Home
Search
Privacy & Security
Connection
Extensions & Themes
Tor Browser Support
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content Learn more
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
HTTPS-Only Mode
HTTPS provides a secure, encrypted connection between Tor Browser and the websites you visit.
Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Tor Browser will upgrade all connections to HTTPS.
Learn more
Enable HTTPS-Only Mode in all windows
Enable HTTPS-Only Mode in private windows only
Don't enable HTTPS-Only Mode
Manage Exceptions...

În pagina "*Connection*":




File Edit View History Bookmarks Tools Help
Settings
Tor Browser
about:preferences#connection
Find in Settings
General
Home
Search
Privacy & Security
Connection
obfs4 bridge:
obfs4 37.218.245.14:38224 D9A82D2F9C2F65A18407...
obfs4 bridge:
obfs4 193.11.166.194:27025 1AE2C08904527FEA90C...
obfs4 bridge:
obfs4 209.148.46.65:443 74FAD1316880624660253 85...
obfs4 bridge:
obfs4 146.57.248.225:22 10A6CD36A537FCE513A322...
Show All Bridges
Add a New Bridge
Choose from one of Tor Browser's built-in bridges
Select a Built-In Bridge...
Request a bridge from torproject.org
Request a Bridge...
Enter a bridge address you already know
Add a Bridge Manually...
Advanced
Extensions & Themes
Tor Browser Support
Configure how Tor Browser connects to the internet
Settings...
View the Tor logs
View Logs...

TOR deschide accesul spre aşa-numitul "Internet întunecat/adânc" ("dark/deep web/net")
unde se află
inclusiv (adică, nu este o regulă implicită)
informaţii (ori, "conţinut") neplăcute, ilegale (în multe ţări/state/şamd.) şi/sau înşelătoare/false.

De regulă, site-urile accesibile ***numai*** cu browserul TOR sau cu unele similare acestuia
au adrese (ca text, cum este forma binecunoscută "www.site.com") terminate în "***.onion***"
de forma celei din continuare care la 1 august 2023 era adresa motorului de căutare *TORCH*:

http://torchdeedp3i2jigzjdmfpn5ttjhthh5wbmda2rr3jvqjg5p77c54dqd.onion/

Unele adrese .onion şi în general pe Dark Net se schimbă frecvent,
de aceea este bine
să adăugăm la "Bookmarks" în browserul TOR
adresepe care să le putem edita/modifica la nevoie astfel;
- ***click-dreapta pe Bookmark***
- ***alegerea comenzii "Edit Bookmark"***
- ***specificarea noii adrese.***

Site-uri cu adrese "obişnuite" pot fi accesate cu browserul TOR.

Dar de obicei, o adresă .onion
NU poate fi accesată
cu un browser "obişnuit" ca Firefox, Chrome, Edge
ci numai cu browserul TOR.

Internetul "obişnuit" este cel unde se află - în general vorbind - site-urile pe care le accesăm în mod frecvent şi de care nu avem pretenţia de a ne ascunde.

Un site "obişnuit" ***poate avea şi*** o adresă de tipul **onion**, adică poate fi prezent ***şi*** pe Dark Net.

La aceeaşi dată din 2023, câteva adrese utile accesibile cu TOR erau:

(textul link-urilor afişate aici
- poate fi copiat după selectare cu mouse-ul şi **Ctrl C**
- apoi plasat în bara de adresă a browserului TOR, cu **Ctrl V**

Motorul de căutare *TORCH*, similar cu cele de la *Google*, *Yahoo*, *DuckDuckGo*, *Altavista* ş.a.:
http://torchdeedp3i2jigzjdmfpn5ttjhthh5wbmda2rr3jvqjg5p77c54dqd.onion/

Listă detaliată de linkuri: "The Hidden Wiki"
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

Listă de linkuri *.onion*: "General TOR Links"
http://fqr7fd4dmwxwpxn2355tnnj37x2hroxc2mr7uty4pwdflpt2bnbdiyqd.onion/

TorHidden.Wiki
http://darknetmdzfznq7zxywqzqnskp6b6thm3yy2uvuxqijrpzltvrdxuyyd.onion/dark-net-search-engines

TORDEX
http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onion/directory

TheDeepDarkNet
http://torlisthsxo7h65pd2po7kevpzkk4wwf3czylz3izcmsx4jzwabbopyd.onion/

Hidden Links
http://wclekwrf2aclunlmuikf2bopusjfv66jlhwtgbiycy5nw524r6ngioid.onion/

Bibliotecă online: Proiectul "Z-Library"
http://wiki5mmem2jh3n4rkqxpplia2wkulatppzshhoc3vrya4kmt2jhfd7ad.onion/

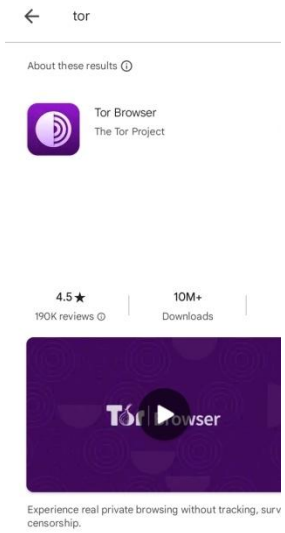
Bibliotecă online: "Just Another Library"
http://libraryfyuybp7oyidyya3ah5xvwgyx6weauoini7zyz555litmmumad.onion/

Acestea şi de altfel orice adrese pot fi puse în "*Bookmarks*" din browserul TOR, de unde să poată fi accesate cu un click pe mouse.
(este evident că în mod uzual nu este fezabil sau posibil să se reţină o astfel de adresă, pentru a fi scrisă fără greşeli/omisiuni pe bara adresei site-ului care trebuie vizitat)

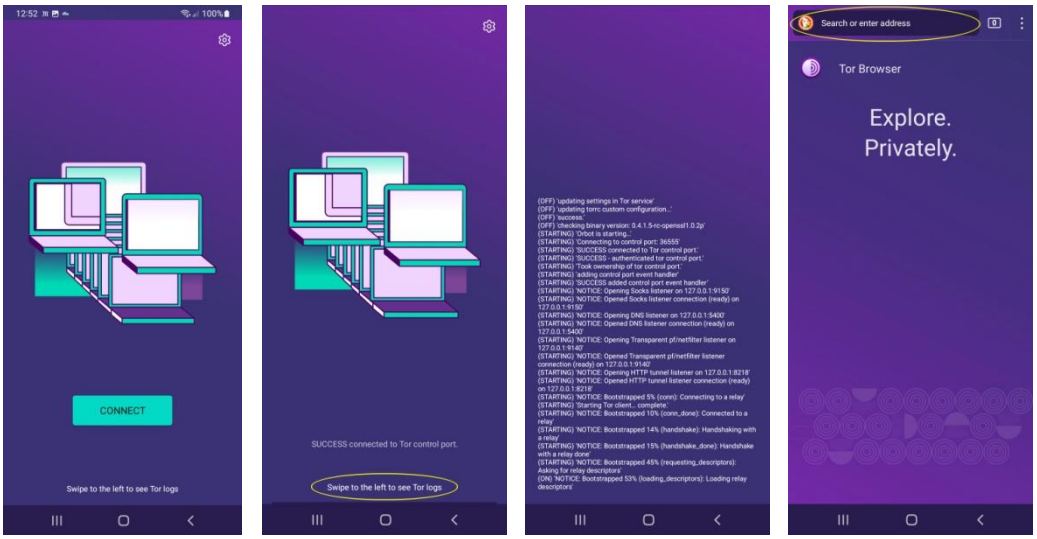
Instalarea browserului TOR pe smartphone sau tabletă cu sistemul de operare Android

În Play Store:

- se caută "tor"
- se instalează aplicaţia

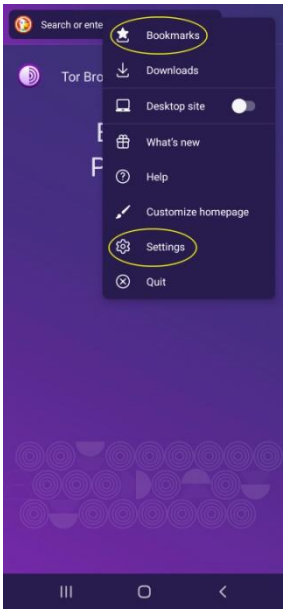


- se porneşte aplicaţia:



Click pe butonul din dreapta-sus desfăşoară meniul din care putem alege

- "Settings" – setările aplicaţiei
- "Bookmarks" – adresele salvate pentru accesre rapidă şi care pot fi atât "obişnuite", cât şi.onion



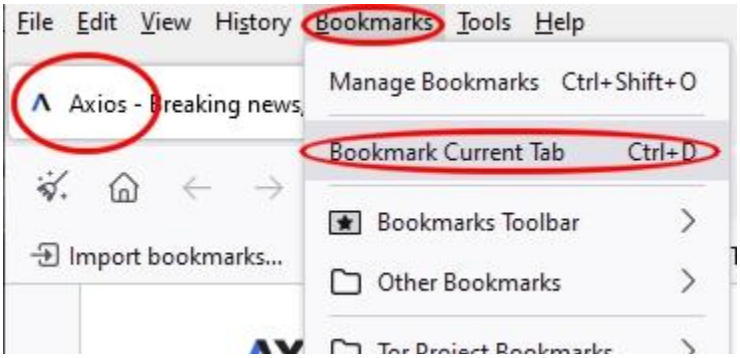
Adăugarea de adrese la Bookmarks; salvarea şi restaurarea unor adrese

Odată ce găsim drept demnă de revizitat o adresă pe Internet, o putem adăuga într-un browser la colecţia acestuia de adrese Favorite sau de semne-de-carte ("bookmarks").

În browserul TOR, la fel ca în Firefox, aceasta se face astfel:

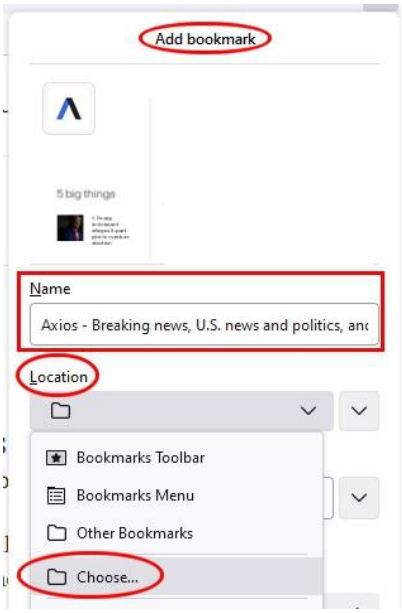
După ce este accesată adresa solicitată, specificată în bara adresei pe Internet a browserului:

Click pe meniul "Bookmarks"
Apoi se alege comanda "Bookmark current tab" –
adică, să se pună semn-de-carte
la adresa din pagina vizionată acum, în pagina ("tab") curentă a browserului
(în imaginea următoare, *titlul* paginii este "Axios...":



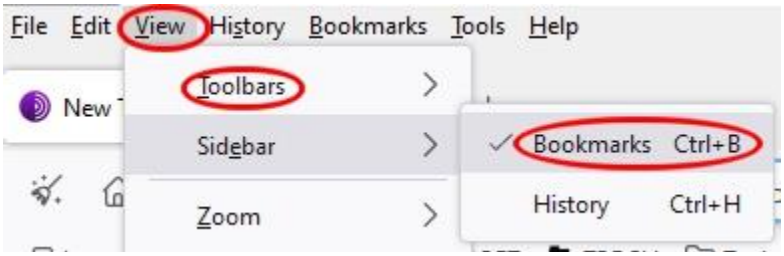
În dialogul care apare, specificăm:

- numele semnului-de-carte, în imagine fiind cel propus automat (*titlul* paginii)
- locaţia unde va fi salvat acest semn-de-carte: posibil, într-un grup de adrese Favorite:



Mai târziu, în orice sesiune de lucru cu ***acest browser*** (cel în care am adăugat adrese la *Bookmarks*), o adresă din cele salvate astfel poate fi accesată cu ***acest browser*** în două moduri:

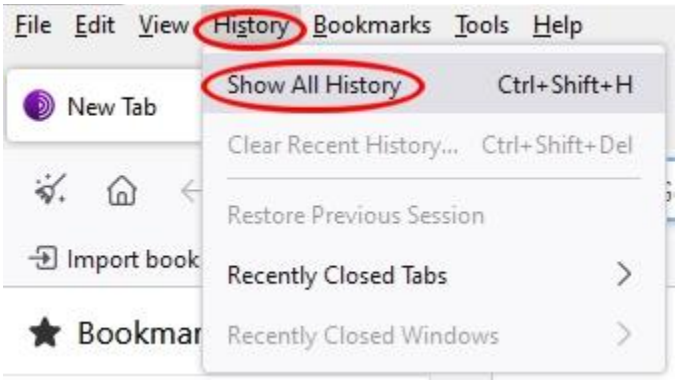
- fie apăsând simultan tastele **Ctrl** şi **B**
- fie din meniul "View -> Toolbars -> Bookmarks"



De obicei, lista semnelor-de-carte este afişată în stânga browserului.

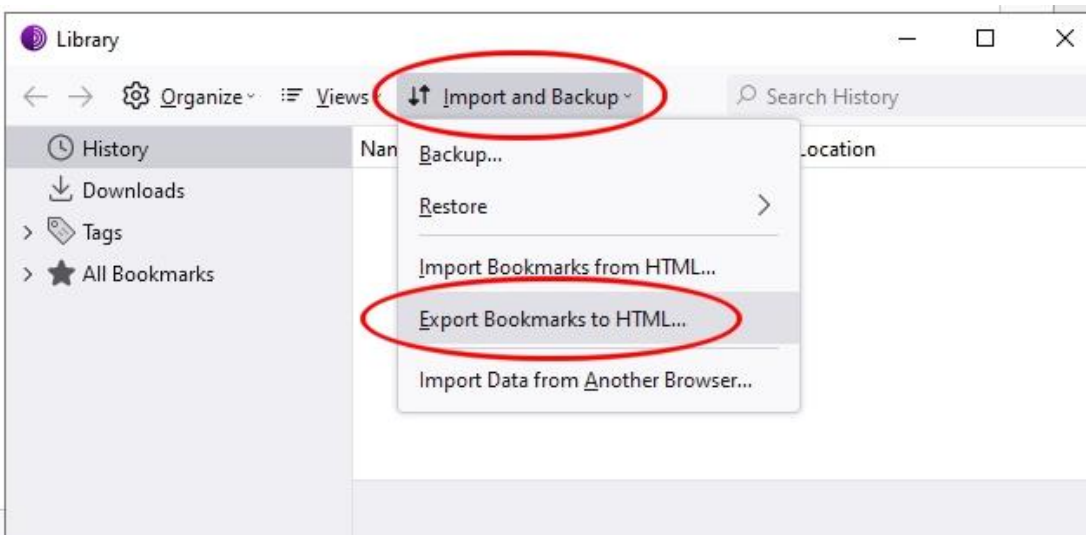
O astfel de listă a adreselor favorite poate fi salvată astfel:

Click pe meniul "History"
Apoi pe "Show All History"

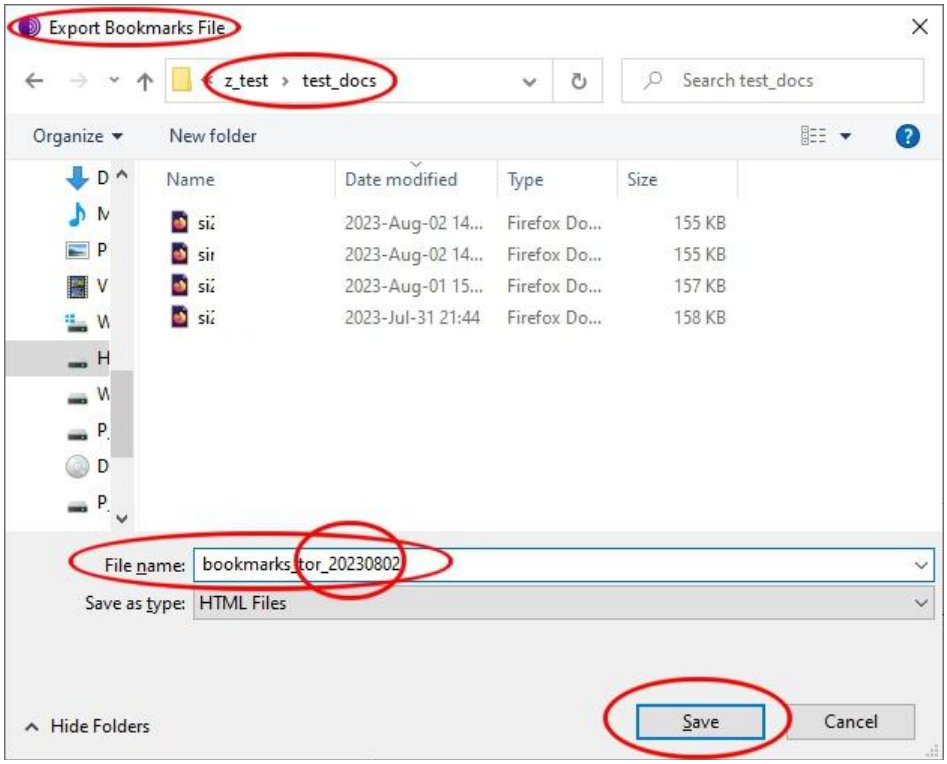


În dialogul care apare se acţionează ca în imaginea următoare:

- din secţiunea/meniul "Import and Backup"
- se alege comanda "Export Bookmarks to HTML..." – lista adreselor-semne-de-carte va fi salvată într-un fişier-text cu structură HTML, accesibilă pe scară largă:

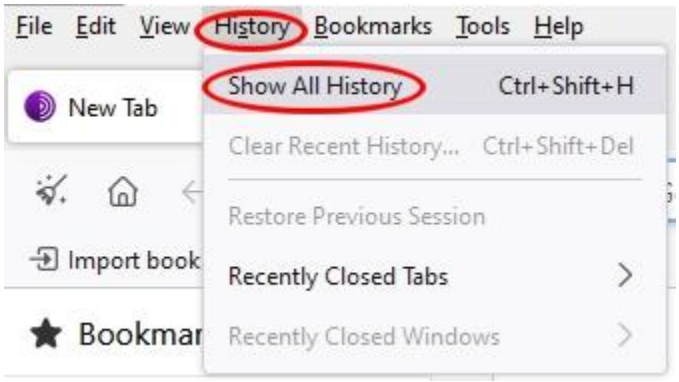


Apoi se specifică numele fişierului şi locaţia unde îl vom salva:
Este bine ca în nume să scriem data curentă, pentru a şti când anume erau valabile acele adrese:



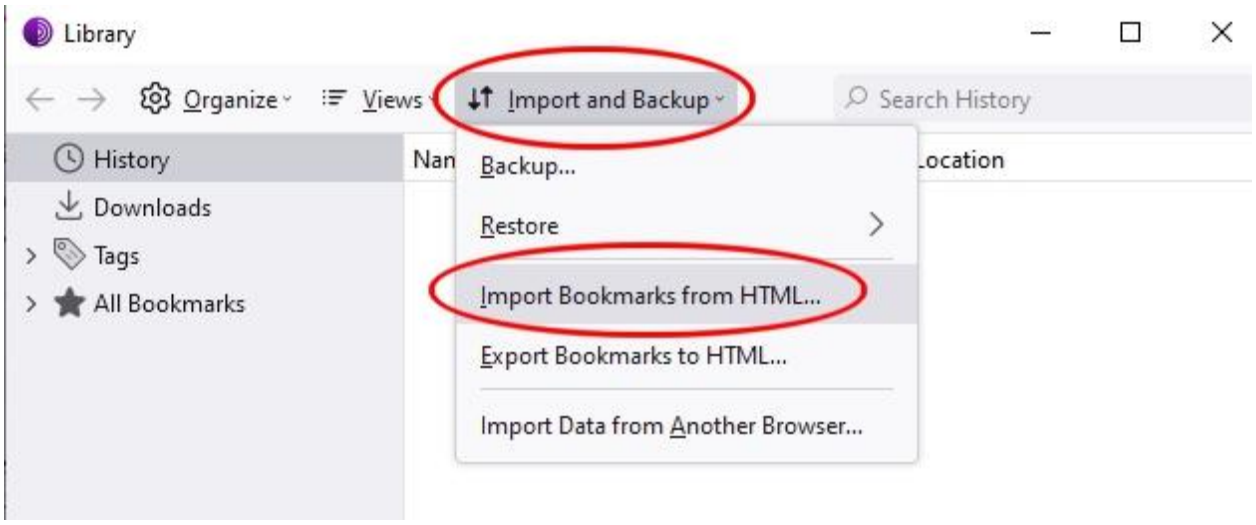
Putem recupera-încărca în acest browser
lista adreselor astfel salvate într-un fişier, astfel:

Click pe meniul "History"
Apoi pe "Show All History"



În dialogul care apare
se acţionează ca în imaginea următoare:

- din secţiunea/meniul "Import and Backup"
- se alege comanda "Import Bookmarks from HTML..." –
  - ***lista adreselor favorite-semne-de-carte va fi încărcată dintr-un fişier salvat anterior***
    - ***fie cu browserul TOR***
    - ***fie cu browserul Firefox (adică, pot fi folosite adresele folosite în Firefox):***



Apoi se alege fişierul unde sunt adresele Favorite, semne-de-carte
şi se afişează secţiunea *Bookmarks* pentru a putea naviga rapid (click) spre unele din acelea.

Precauţii elementare de luat pentru mărirea siguranţei navigării pe DarkNet

1. Trebuie evitate site-urile şi link-urile care se anunţă prin unele din aceste cuvinte, abrevieri şi coduri în limba engleză – lista nefiind completă, dar conţinând principalele particule de evitat şi vehiculate în această limbă fie de sine stătător, fie combinate (cu alte cuvinte):
   CP
   Child
   Pedo
   Bear
   Candy
   Fake (ID)
   Free/Cheap Money/Bitcoin/ş.a.
   Aceste cuvinte sau astfel de combinaţii urmate/precedate de semnul exclamării !

2. Nu trebuie accesate serviciile de e-mail cu care suntem obişnuiţi, de exemplu
- GMail
- Yahoo! Mail

3. Nu trebuie oferite informaţii personale cu specific financiar, de exemplu informaţii despre:
- cărţi de credit
- conturi în bancă

4. Nu trebuie oferite informaţii personale, de exemplu:
- Adresa
- Numele
- Locul de muncă
- Proprietăţi (avere)
- Informaţii despre rude şi prieteni apropiaţi

5. Nu trebuie descărcate/*download*-ate fişiere de tipuri/în formate care permit transportul de comenzi între computere/dispozitive de calcul, de exemplu:
- Documente de tip Microsoft Office, OpenOffice (https://www.openoffice.org/) şi LibreOffice (https://www.libreoffice.org/)
- Fişiere executabile şi module ale acestora,
  cu extensia din lista următoare - de asemenea incompletă:
  - .exe
  - .dll
  - .com
  - .ocx
  - .ctl
  - .js

De obicei, numele fişierului asociat unui link poate fi aflat plasând cursorul mouse-ului pe link şi citind în partea de jos a browserului (pe "bara de stare" – StatusBar) numele acelui fişier (poate fi pur şi simplu o pagină de internet, cu extensia .htm)

6. Trebuie evitată achiziţionarea de bunuri şi de servicii, oricât de ispititoare ar fi, deoarece:
- Pe circa 90% din "pieţe" (Market) se oferă falsuri
- Numeroase bunuri şi servicii sunt ilegale, sau folosirea lor în orice fel este ilegală în multe ţări/state/şamd.
- Majoritatea tranzacţiilor, sau unele din ele, sunt monitorizate