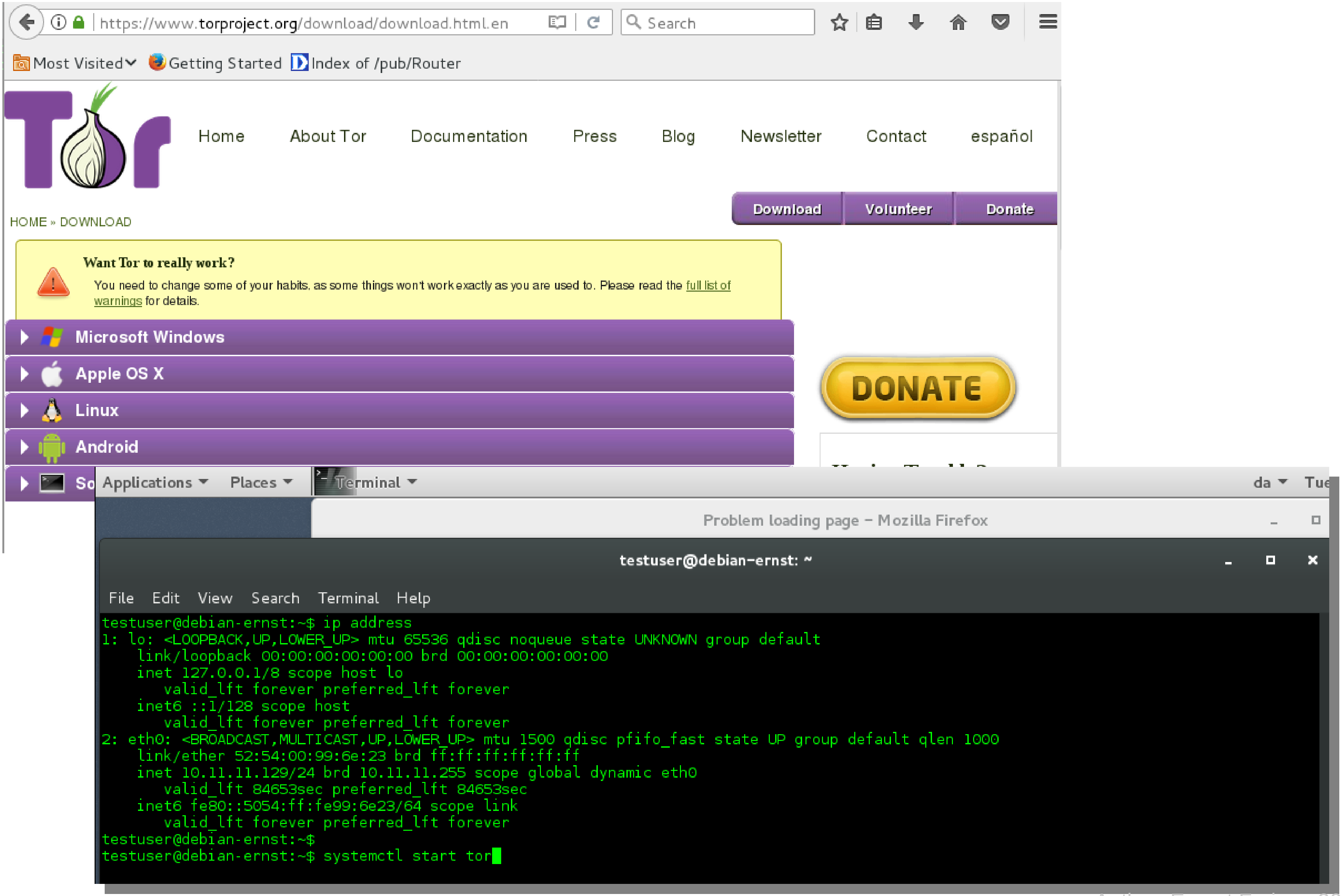
DarkNet - TOR

TOR stands for “The Onion Router” and it is called so because it uses the “Onion routing protocol” to hide information about user activity, allows users to browse the Web anonymously.

TOR is the most common anonymizer service and an entry point to what is called ‘the dark net’ or ’deep web’. In addition to its privacy-enhancing features, TOR is also widely used for malicious and criminal activities such as black market trading, child pornography and to operate a Botnet...

DarkNet – Another use case

Get tor client



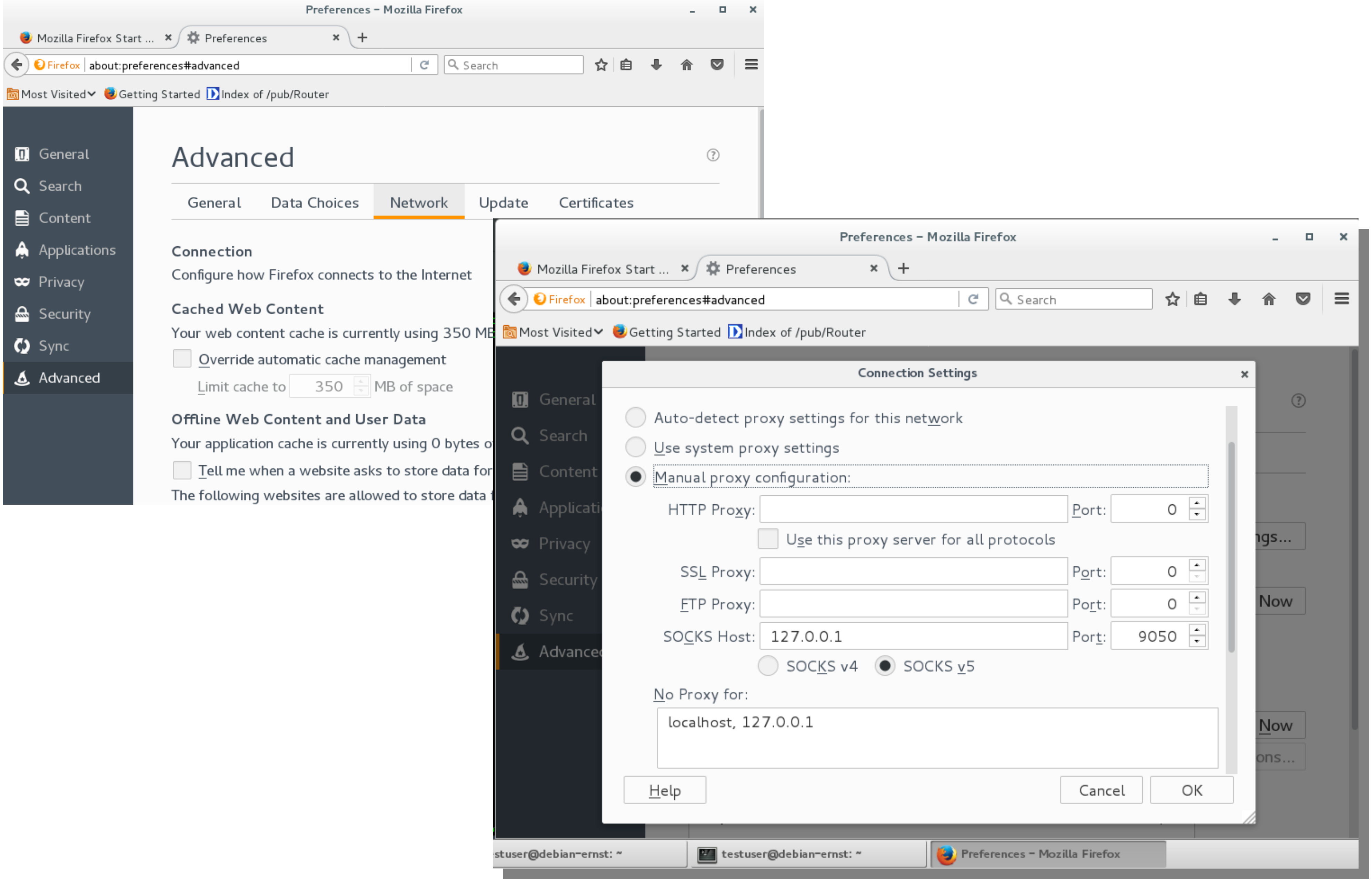
Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to. Please read the full list of warnings for details.

```
testuser@debian-ernst:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:99:6e:23 brd ff:ff:ff:ff:ff:ff
    inet 10.11.11.129/24 brd 10.11.11.255 scope global dynamic eth0
       valid_lft 84653sec preferred_lft 84653sec
    inet6 fe80::5054:ff:fe99:6e23/64 scope link
       valid_lft forever preferred_lft forever
testuser@debian-ernst:~$
testuser@debian-ernst:~$ systemctl start tor
```

DarkNet – Another use case

Lets, move all my browser traffic over TOR :)



Advanced

General | Data Choices | Network | Update | Certificates

Connection

Configure how Firefox connects to the Internet

Cached Web Content

Your web content cache is currently using 350 ME

□ Override automatic cache management

Limit cache to 350 MB of space

Offline Web Content and User Data

Your application cache is currently using 0 bytes o

□ Tell me when a website asks to store data for

The following websites are allowed to store data f

Connection Settings

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: Port: 0

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: 127.0.0.1 Port: 9050

○ SOCKS v4 ● SOCKS v5

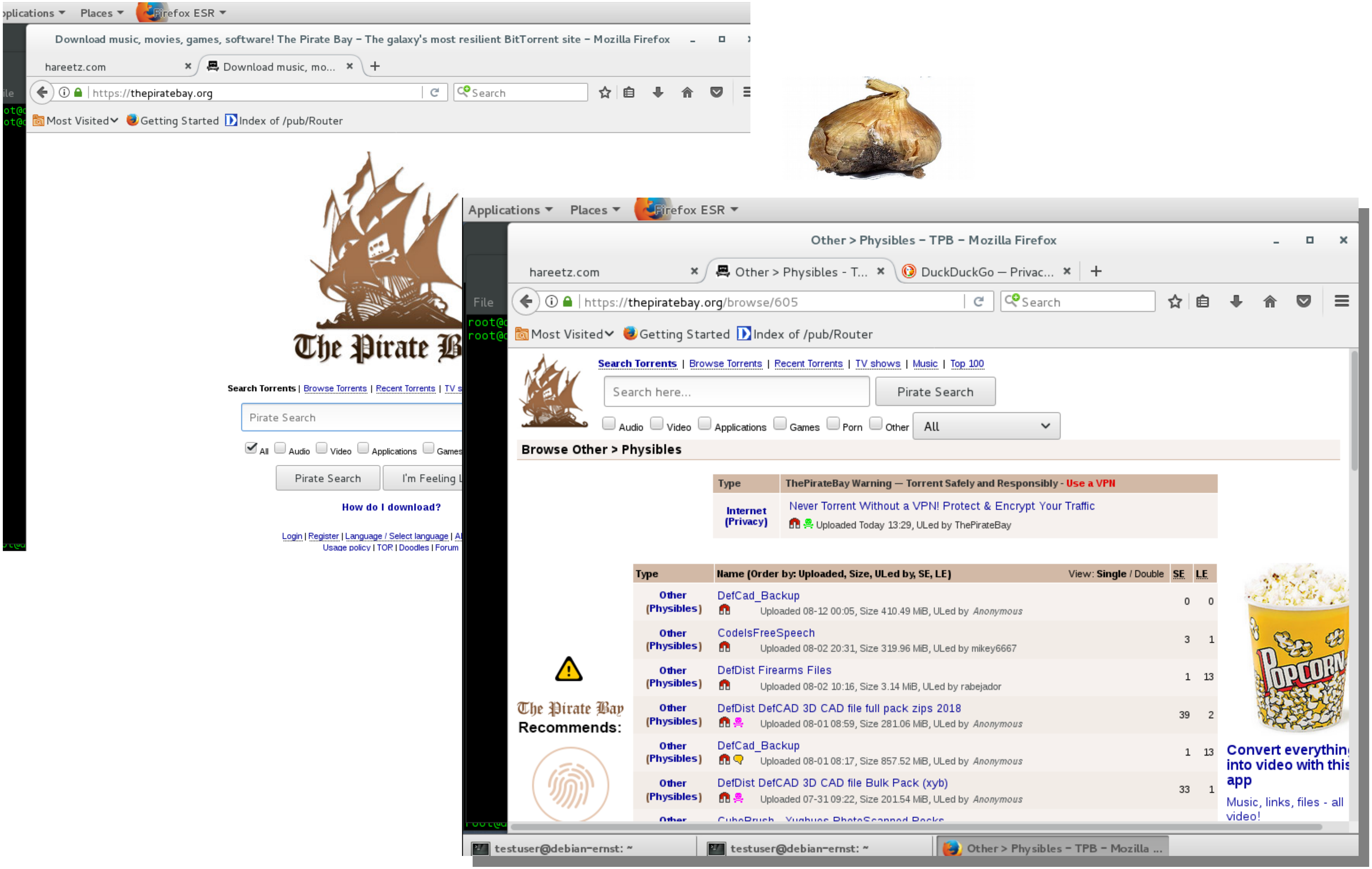
No Proxy for:

localhost, 127.0.0.1

Author: Ernest Farias - 2018

DarkNet – Another use case

It works!, from now on all browser traffic is hidden.



Download music, movies, games, software! The Pirate Bay – The galaxy's most resilient BitTorrent site – Mozilla Firefox

hareetz.com | Download music, mo...

https://thepiratebay.org

Search Torrents | Browse Torrents | Recent Torrents | TV s

Pirate Search

☑ All □ Audio □ Video □ Applications □ Games

How do I download?

Login | Register | Language / Select language | Al
Usage policy | TOR | Doodles | Forum

Other > Physibles – TPB – Mozilla Firefox

hareetz.com | Other > Physibles - T... | DuckDuckGo – Privac...

https://thepiratebay.org/browse/605

Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100

Search here...

□ Audio □ Video □ Applications □ Games □ Porn □ Other All

Browse Other > Physibles

Type	ThePirateBay Warning — Torrent Safely and Responsibly - Use a VPN
Internet (Privacy)	Never Torrent Without a VPN! Protect & Encrypt Your Traffic Uploaded Today 13:29, ULed by ThePirateBay

Type	Name (Order by: Uploaded, Size, ULed by, SE, LE) View: Single / Double	SE	LE
Other (Physibles)	DefCad_Backup Uploaded 08-12 00:05, Size 410.49 MiB, ULed by *Anonymous*	0	0
Other (Physibles)	CodeIsFreeSpeech Uploaded 08-02 20:31, Size 319.96 MiB, ULed by mikey6667	3	1
Other (Physibles)	DefDist Firearms Files Uploaded 08-02 10:16, Size 3.14 MiB, ULed by rabejador	1	13
Other (Physibles)	DefDist DefCAD 3D CAD file full pack zips 2018 Uploaded 08-01 08:59, Size 281.06 MiB, ULed by *Anonymous*	39	2
Other (Physibles)	DefCad_Backup Uploaded 08-01 08:17, Size 857.52 MiB, ULed by *Anonymous*	1	13
Other (Physibles)	DefDist DefCAD 3D CAD file Bulk Pack (xyb)	33	1
Other	CubeBrush - Yughues PhotoScanned Packs		

The Pirate Bay Recommends:

Convert everythin into video with this app

Music, links, files - all video!

DarkNet – Detection

The way to detect tor, is by catching the certificates xchanged, those will use same CN, starting with www. , and the host running tor will generate several ssl connections, being all them using diferents certificates but with the same CN pattern.

W/BRO and the x509 analyzer can accomplish this task.