



Introduction to Tor

Information Security Inc.

Contents

- Tor
- DarkWeb vs DeepWeb
- Onion Sites
- References

Tor



- Online Anonymity
 - Open Source
 - Open Network
- Community of researchers, developers, users and relay operators.
- U.S. 501(c)(3) non-profit organization

Tor



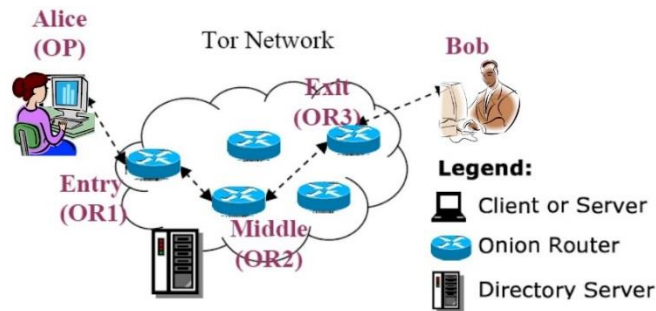
Tor

- The Onion Router
- Primary purpose => Anonymize Internet activity
- Series of routers that anonymously forward traffic



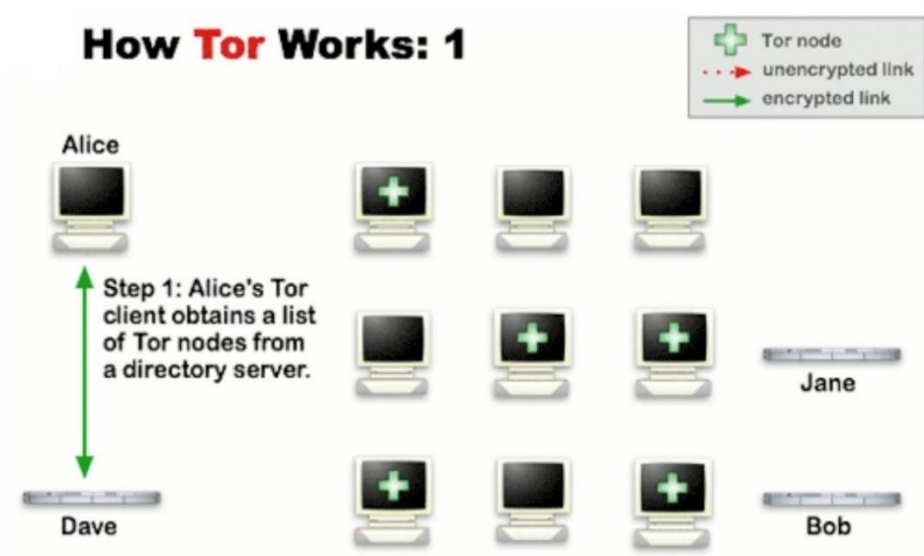
Tor

- Tor Components
- Client => the user of the Tor network
- Server => the target TCP applications (web servers)
- Tor (onion) router => the special proxy relays the application data
- Directory server => servers holding Tor router information



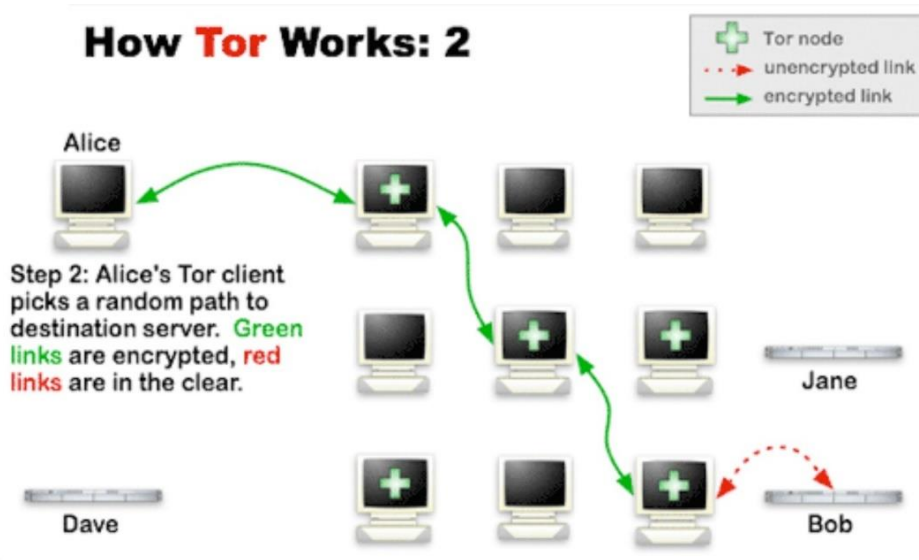
Tor

- Tor Operations



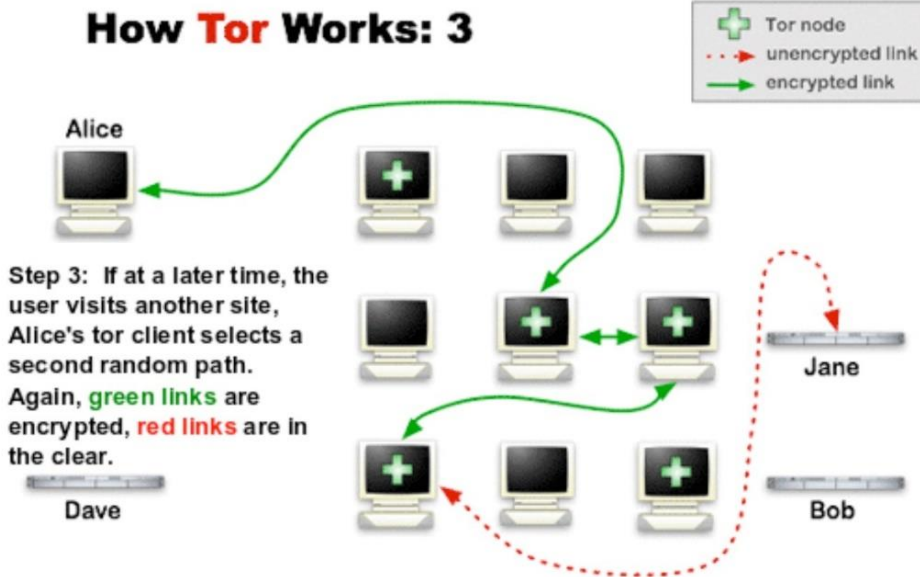
Tor

- Tor Operations



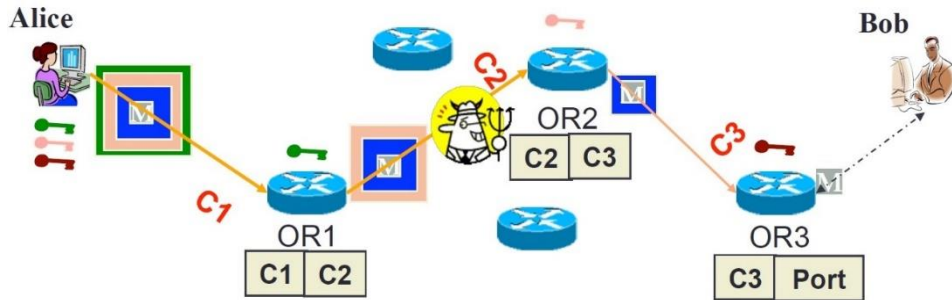
Tor

- Tor Operations



Tor

- A circuit is built incrementally one hop by one hop
- Onion-like encryption => Alice negotiates an AES key with each router; Messages are divided into equal sized cells; each router knows only its predecessor and successor; Only the exit router (OR3) can see the message



Tor

- Connect to the Tor Network
- 1) CLI Daemon => apt-get install tor

```
    # apt-get install tor
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libzstd1 tor-geoipdb torsocks
Suggested packages:
  mixmaster torbrowser-launcher tor-arm apparmor-utils obfs4proxy
The following NEW packages will be installed:
  libzstd1 tor tor-geoipdb torsocks
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,068 kB of archives.
After this operation, 11.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main amd64 libzstd1 amd64 1.3.3+dfsg-1 [190 kB]
Get:2 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main amd64 tor amd64 0.3.2.9-1 [1,668 kB]
Get:3 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main amd64 tor-geoipdb all 0.3.2.9-1 [1,138 kB]
Get:4 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main amd64 torsocks amd64 2.2.0-2 [73.1 kB]
Fetched 3,068 kB in 46s (66.3 kB/s)
Selecting previously unselected package libzstd1.
(Reading database ... 419475 files and directories currently installed.)
```

Tor

- Connect to the Tor Network
- CLI Daemon Configs => /etc/tor/torsocks.conf, /etc/tor/torrc

```
/etc/tor# pwd
/etc/tor
/etc/tor# ls -alh
total 32K
drwxr-xr-x  2 root root 4.0K Feb  9 11:42 .
drwxr-xr-x 202 root root 12K Feb  9 11:42 ..
-rw-r--r--  1 root root 11K Jan 16 18:49 torrc
-rw-r--r--  1 root root 2.1K Aug  5 2017 torsocks.conf
```

Tor

- Connect to the Tor Network
- CLI Daemon Configs => Configure tor through /etc/tor/torrc (Set up hidden services, Set up the port to listen on, Setup basic access lists for allowing other systems to connect to tor through you)

```
## Configuration file for a typical Tor user
## Last updated 22 December 2017 for Tor 0.3.2.8-rc.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands; you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs/faq#torrc
##
## Tor opens a SOCKS proxy on port 9050 by default -- even if you don't
## configure one below. Set "SOCKSPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
#SOCKSPort 9050 # Default: Bind to localhost:9050 for local connections.
#SOCKSPort 192.168.0.1:9100 # Bind to this address:port too.
##
## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SOCKSPolicy is set, we accept
## all (and only) requests that reach a SOCKSPort. Untrusted users who
## can access your SOCKSPort may be able to learn about the connections
## you make.
#SOCKSPolicy accept 192.168.0.0/16
#SOCKSPolicy accept FC00::/7
#SOCKSPolicy reject *
##
## Logs go to stdout at level "notice" unless redirected by something
## else, like one of the below lines. You can have as many log lines as
## you want.
##
## We advise using "notice" in most cases, since anything more verbose
## may provide sensitive information to an attacker who obtains the logs.
##
## Send all messages of level 'notice' or higher to /var/log/tor/notices.log
log notice file /var/log/tor/notices.log
## Send every possible message to /var/log/tor/debug.log
log debug file /var/log/tor/debug.log
```

Tor

- Connect to the Tor Network
- CLI Daemon Configs => /etc/tor/torsocks.conf
- Using default settings

```
# torsocks.conf(5), torsocks(1) and torsocks(8) manpages.  
  
# Default Tor address and port. By default, Tor will listen on localhost for  
# any SOCKS connection and relay the traffic on the Tor network.  
TorAddress 127.0.0.1  
TorPort 9050
```

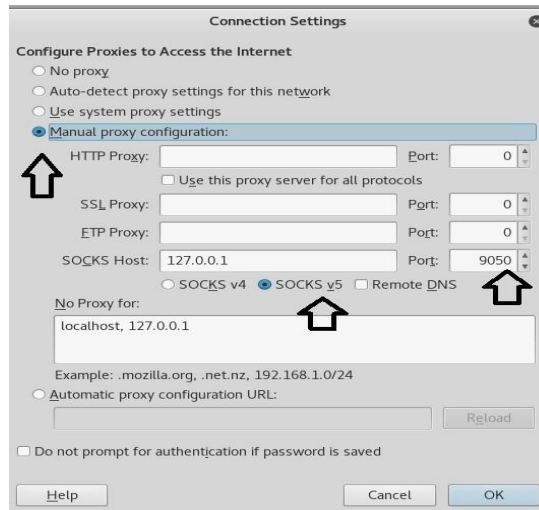
Tor

- Connect to the Tor Network
- Starting Tor proxy => /etc/init.d/tor start

```
/etc/tor# /etc/init.d/tor start
[ ok ] Starting tor (via systemctl): tor.service.
/etc/tor# netstat -anepl | grep tor
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN      0          69045      9845/tor
tcp        0      0 192.168.10.12:41774    217.182.198.95:443      ESTABLISHED 139        69073      9845/tor
tcp        0  543 192.168.10.12:36622    85.25.111.77:9001      ESTABLISHED 139        69201      9845/tor
tcp        0      0 192.168.10.12:35798    185.129.62.62:9001     ESTABLISHED 139        69059      9845/tor
tcp        0      0 192.168.10.12:54246    91.121.84.137:4052     ESTABLISHED 139        69062      9845/tor
tcp        0      0 192.168.10.12:36600    85.25.111.77:9001     ESTABLISHED 139        69075      9845/tor
tcp        0      0 192.168.10.12:53956    195.154.181.146:443    ESTABLISHED 139        69074      9845/tor
```

Tor

- Connect to the Tor Network
- Starting Tor proxy => Point browser to 9050



Tor

- Connect to the Tor Network
- Starting Tor proxy => Visit <https://check.torproject.org> for confirmation



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **91.219.237.244**

However, it does not appear to be Tor Browser.
[Click here to go to the download page](#)

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Atlas](#).

[Donate to Support Tor](#)

[Tor Q&A Site](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)

Tor

- Connect to the Tor Network
- 2) TorBrowser => Simple Executable (launches portable Firefox browser)
- Download at <https://www.torproject.org/projects/torbrowser.html.en>



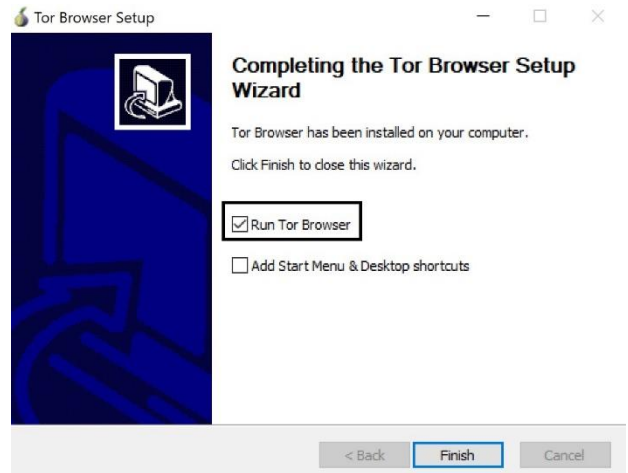
Tor

- Connect to the Tor Network
- TorBrowser => Simple Executable (launches portable Firefox browser)
- Install Tor Browser



Tor

- Connect to the Tor Network
- TorBrowser => Simple Executable (launches portable Firefox browser)
- Run Tor Browser

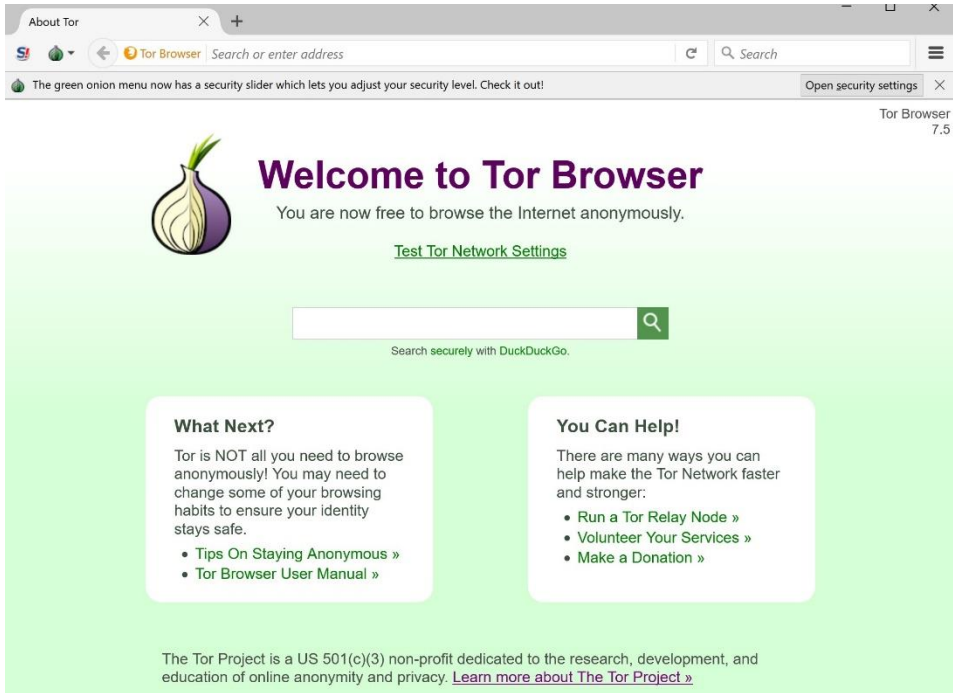


Tor

- Connect to the Tor Network
- TorBrowser => Simple Executable (launches portable Firefox browser)
- Connect



Tor




About Tor

Tor Browser | Search or enter address

The green onion menu now has a security slider which lets you adjust your security level. Check it out! [Open security settings](#)

Tor Browser 7.5



Welcome to Tor Browser

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)

Search securely with DuckDuckGo.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

- [Tips On Staying Anonymous »](#)
- [Tor Browser User Manual »](#)

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

DarkWeb vs DeepWeb

- The “dark web” is the encrypted network that exists between Tor servers and their clients
- The “deep web” is simply the content of databases and other web services that for one reason or another cannot be indexed by conventional search engines



Onion Sites

- We are connected => Now what?
- Browse the Internet anonymously
- Fight Censorship
- Generally just stay anonymous
- Tor Hidden Services, they sometimes ends up like below

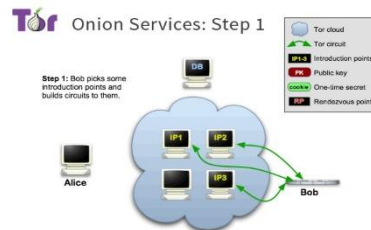


Onion Sites

- Tor Hidden Services
- Services that live only in the Tor Network => Turn Tor into a Darknet
- Services use .onion as TLD
- See => <https://www.torproject.org/docs/onion-services>

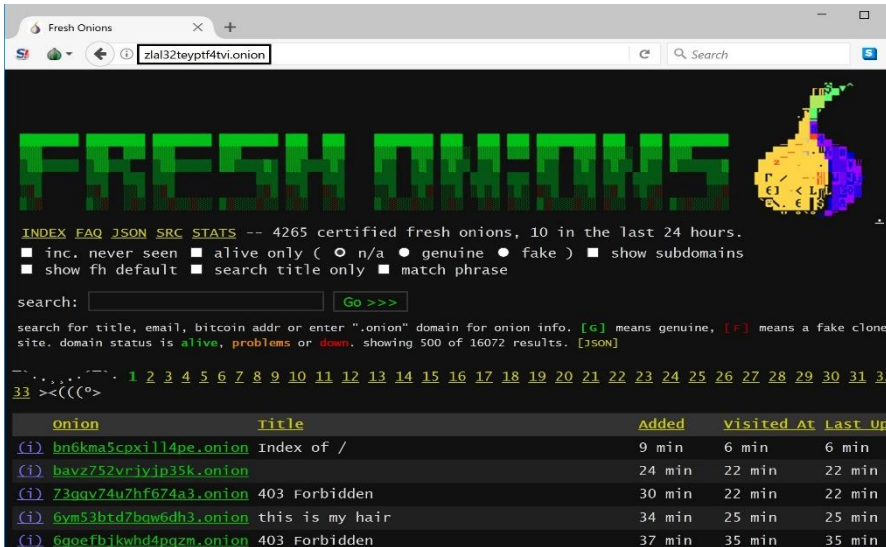


An onion service needs to advertise its existence in the Tor network before clients will be able to contact it. Therefore, the service randomly picks some relays, builds circuits to them, and asks them to act as introduction points by selling them its public key. Note that in the following figures the green links are circuits rather than direct connections. By using a full Tor circuit, it's hard for anyone to associate an introduction point with the onion server's IP address. While the introduction points and others are told the onion service's identity (public key), we don't want them to learn about the onion server's location (IP address).



Onion Sites

- The `http://zla132teyptf4tvi.onion` hidden service (tor hidden service crawler / spider and web site)



Fresh Onions

zla132teyptf4tvi.onion

FRESH ONIONS

INDEX FAQ JSON SRC STATS -- 4265 certified fresh onions, 10 in the last 24 hours.

■ inc. never seen ■ alive only (● n/a ● genuine ● fake) ■ show subdomains
■ show fh default ■ search title only ■ match phrase

search:

search for title, email, bitcoin addr or enter ".onion" domain for onion info. [G] means genuine, [F] means a fake clone site. domain status is **alive**, **problems** or **down**. showing 500 of 16072 results. [JSON]

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
33 ><(((^>

onion	title	Added	Visited At	Last Up
(i) bn6kma5cpxi114pe.onion	Index of /	9 min	6 min	6 min
(i) bavz752vrjyjp35k.onion		24 min	22 min	22 min
(i) 73qqv74u2hf674a3.onion	403 Forbidden	30 min	22 min	22 min
(i) 6vm53brd7baw6dh3.onion	this is my hair	34 min	25 min	25 min
(i) 6goefbjkwhd4pqzm.onion	403 Forbidden	37 min	35 min	35 min

Onion Sites

- The <http://z1al32teyptf4tvi.onion> hidden service (tor hidden service crawler / spider and web site)

z1al32teyptf4tvi.onion/?rep=n%2Fa&search=Hacker&submit=Go+>>>

FRESH ONIONS

INDEX FAQ JSON SRC STATS -- 4261 certified fresh onions, 10 in the last 24 hours.

■ inc. never seen ■ alive only (○ n/a ● genuine ● fake) ■ show subdomains
■ show fh default ■ search title only ■ match phrase

search:


search for title, email, bitcoin addr or enter ".onion" domain for onion info. [G] means genuine, [F] means a fake clone site. domain status is **alive**, **problems** or **down**. showing 500 of 10344 results. [JSON]

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 ><((°)

Onion	Title	Added
(i) auntwvpt2zktxwng.onion	Oniondir FACEBOOK HACKER EVER BEST FACEBOOK HACKER EVER BEST FACEBOOK HACKER EVER BEST FACEBOOK HACKER EVER BEST	2 wk
(i) ozawuyxtechnopol.onion	Revue de presse – TechnOpolis culture hacker » Dans le n° 904 (27 mars) des Inrockuptibles : « Hackers vaillants »	last mth
(i) fbcysyloegqzqcr.onion	Moneybook – HIRE THE REALIST HACKER . > HIRE THE REALIST HACKER . Full Version: HIRE THE REALIST HACKER . You're currently viewing a stripped	3 wk

Onion Sites

- DeepWeb List => <http://deepweblinks.org/>

deepweblinks.org  Search

TO BROWSE ONION DEEP WEB LINKS, INSTALL TOR BROWSER FROM [HTTP://TORPROJECT.ORG/](http://TORPROJECT.ORG/)

HIDDEN SERVICE LISTS AND SEARCH ENGINES

<http://3g2upl4pq8kufc4m.onion/> – DuckDuckGo Search Engine
<http://xmh57jzrnw6insl.onion/> – TORCH – Tor Search Engine
http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page – Uncensored Hidden Wiki
<http://32rfckwuorff4dlv.onion/> – Onion URL Repository
<http://e286a132vpuorbyg.onion/bookmarks.php> – Dark Nexus
<http://5plvrsgydwy2sgce.onion/> – Seeks Search
<http://2vlqpcqjllhmd5r2.onion/> – Gateway to Freenet
<http://nlmymchrnmlmbnll.onion/> – Is It Up?
<http://kpyynyvm6xq17wz2.onion/links.html> – ParaZite
<http://wiki5kauulhowqi5.onion/> – Onion Wiki
<http://kpvz7ki2v5agwt35.onion/> – The Hidden Wiki
<http://ldnxcnkne4qt176tg.onion/> – Tor Project: Anonymity Online
<http://torlinkbgs6aabns.onion/> – TorLinks
<http://jh32yv5zgyayyts3.onion/> – Hidden Wiki .Onion Urls
<http://wikitjerrta4qgz4.onion/> – Hidden Wiki – Tor Wiki
<http://xdagknwjc7aaytzh.onion/> – Anonet Webproxy
http://3fyb44wdhnd2ghhl.onion/wiki/index.php?title=Main_Page – All You're Wiki – clone of the clean hidden wiki that went down with freedom hosting
<http://3fyb44wdhnd2ghhl.onion/> – All You're Base
<http://j6im4v42ur8dpc3.onion/> – TorProject Archive
<http://p3igkncehackjtib.onion/> – TorProject Media
<http://kbpodhnxfl3clb4.onion/> – Tor Search
<http://cipollatnumrrahd.onion/> – Cipolla 2.0 (Italian)
<http://dppmfxaacucguzpc.onion/> – TorDir – One of the oldest link lists on Tor

MARKETPLACE FINANCIAL

<http://torbrokerge7zxxq.onion/> – TorBroker – Trade securities anonymously with bitcoin, currently supports nearly 1000 stocks and ETFs
<http://fogcore5n3ov3tui.onion/> – Bitcoin Fog – Bitcoin Laundry
<http://2vx83nyktk4kxbxb.onion/> – AUTOMATED PAYPAL AND CREDIT CARD STORE
<http://samsgdwtwz9hvjyud4.onion/> – Safe, Anonymous, Fast, Easy escrow service.
<http://easvcoinsav17p5l.onion/> – EasyCoin – Bitcoin Wallet with free Bitcoin Mixer

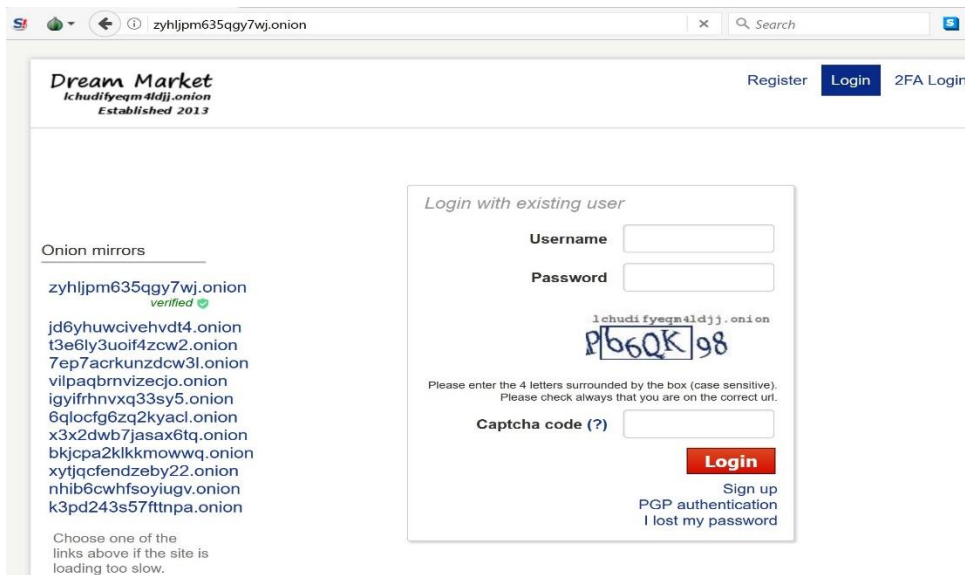
Onion Sites

- Hidden Wiki =>
http://kpvz7kpmcmne52qf.onion/wiki/index.php/Main_Page

The screenshot shows the main page of 'The Uncensored Hidden Wiki'. The browser address bar displays 'kpvz7kpmcmne52qf.onion/wiki/index.php/Main_Page'. The page features a navigation menu on the left with links to 'Main page', 'Recent changes', 'Random page', 'Censorship Policy', 'Wiki FAQ', and 'Help'. A search bar is also present. The main content area includes a 'Main Page' header, a pink banner stating 'Over 124 million page views and counting, TUHW est. 2014.', and a welcome message: 'Welcome to The Uncensored Hidden Wiki. The front page of the deep web! Currently 943 articles about anything and everything.' Below this, there are sections for 'Welcome!', 'Getting started...', 'Links and Editors Picks', and 'FEATURED ARTICLE'. The featured article is titled 'Hidden Answers' and describes a community project for collecting and cataloging uncensored information.

Onion Sites

- DreamMarket => <http://zyhlijpm635qgy7wj.onion/>



The screenshot shows a web browser window with the address bar displaying `zyhlijpm635qgy7wj.onion`. The website header includes the logo "Dream Market" with the tagline "Established 2013" and navigation links for "Register", "Login", and "2FA Login".

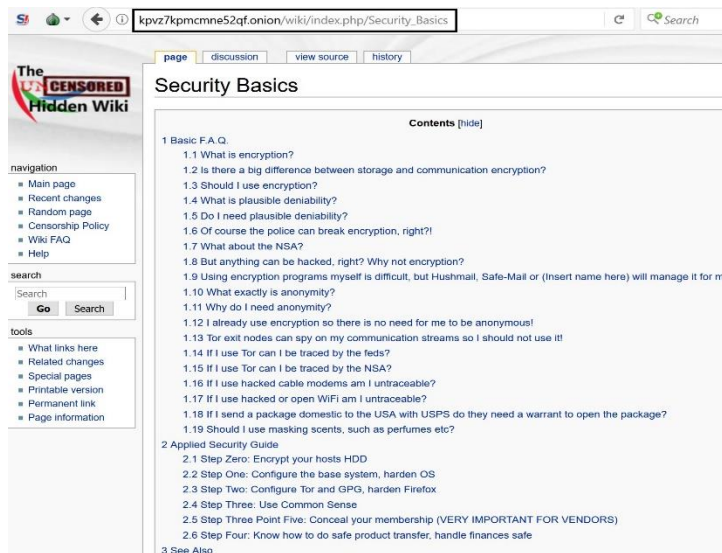
On the left side, there is a section titled "Onion mirrors" with a list of onion addresses. The first address is `zyhlijpm635qgy7wj.onion`, which is marked as "verified" with a green checkmark. Below it are several other onion addresses, including `jd6yhuwcivehvt4.onion`, `t3e6ly3uoif4zwcw2.onion`, `7ep7ackunzdcw3l.onion`, `vilpaqbrmvizecjo.onion`, `igyifrhvxq33sy5.onion`, `6qlocfg6zq2kyacl.onion`, `x3x2dwb7jasax6tq.onion`, `bkjcpa2klkkmowwq.onion`, `xytjcfendzeby22.onion`, `nhib6cwhfsoyiugv.onion`, and `k3pd243s57ftnpa.onion`.

Below the list, a note states: "Choose one of the links above if the site is loading too slow."

On the right side, there is a login form titled "Login with existing user". It contains fields for "Username" and "Password". Below these fields is a captcha image showing the text "1chudi fyegm4ldjj.onion" and a box containing the letters "Pb6QK98". Below the captcha, there is a text prompt: "Please enter the 4 letters surrounded by the box (case sensitive). Please check always that you are on the correct url." and a "Captcha code (?)" input field. At the bottom of the form, there is a red "Login" button and links for "Sign up", "PGP authentication", and "I lost my password".

Onion Sites

- SecurityBasics =>
http://kpvz7kpmcmne52qf.onion/wiki/index.php/Security_Basics



The screenshot shows a web browser window displaying the 'Security Basics' page on the 'The Censored Hidden Wiki'. The browser's address bar shows the URL 'kpvz7kpmcmne52qf.onion/wiki/index.php/Security_Basics'. The page features a navigation sidebar on the left with sections for 'navigation', 'search', and 'tools'. The main content area is titled 'Security Basics' and includes a 'Contents [hide]' section with a numbered list of topics. The list includes sections on 'Basic F.A.Q.' (covering encryption, deniability, NSA, and anonymity) and 'Applied Security Guide' (covering steps from host encryption to safe product transfer).

The Censored Hidden Wiki

Security Basics

Contents [hide]

- 1 Basic F.A.Q.
 - 1.1 What is encryption?
 - 1.2 Is there a big difference between storage and communication encryption?
 - 1.3 Should I use encryption?
 - 1.4 What is plausible deniability?
 - 1.5 Do I need plausible deniability?
 - 1.6 Of course the police can break encryption, right?!
 - 1.7 What about the NSA?
 - 1.8 But anything can be hacked, right? Why not encryption?
 - 1.9 Using encryption programs myself is difficult, but Hushmail, Safe-Mail or (insert name here) will manage it for me!
 - 1.10 What exactly is anonymity?
 - 1.11 Why do I need anonymity?
 - 1.12 I already use encryption so there is no need for me to be anonymous!
 - 1.13 Tor exit nodes can spy on my communication streams so I should not use it!
 - 1.14 If I use Tor can I be traced by the feds?
 - 1.15 If I use Tor can I be traced by the NSA?
 - 1.16 If I use hacked cable modems am I untraceable?
 - 1.17 If I use hacked or open WiFi am I untraceable?
 - 1.18 If I send a package domestic to the USA with USPS do they need a warrant to open the package?
 - 1.19 Should I use masking scents, such as perfumes etc?
- 2 Applied Security Guide
 - 2.1 Step Zero: Encrypt your hosts HDD
 - 2.2 Step One: Configure the base system, harden OS
 - 2.3 Step Two: Configure Tor and GPG, harden Firefox
 - 2.4 Step Three: Use Common Sense
 - 2.5 Step Three Point Five: Conceal your membership (VERY IMPORTANT FOR VENDORS)
 - 2.6 Step Four: Know how to do safe product transfer, handle finances safe
- 3 See Also

References

- Tor Hidden Services

<https://www.torproject.org/docs/onion-services>

- Tor

[https://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](https://en.wikipedia.org/wiki/Tor_(anonymity_network))

- Tor Download

<https://www.torproject.org/projects/torbrowser.html.en>

- List of Tor Hidden Services

https://en.wikipedia.org/wiki/List_of_Tor_hidden_services#Search_engines