Meet Darknet, the hidden, anonymous underbelly of the searchable Web

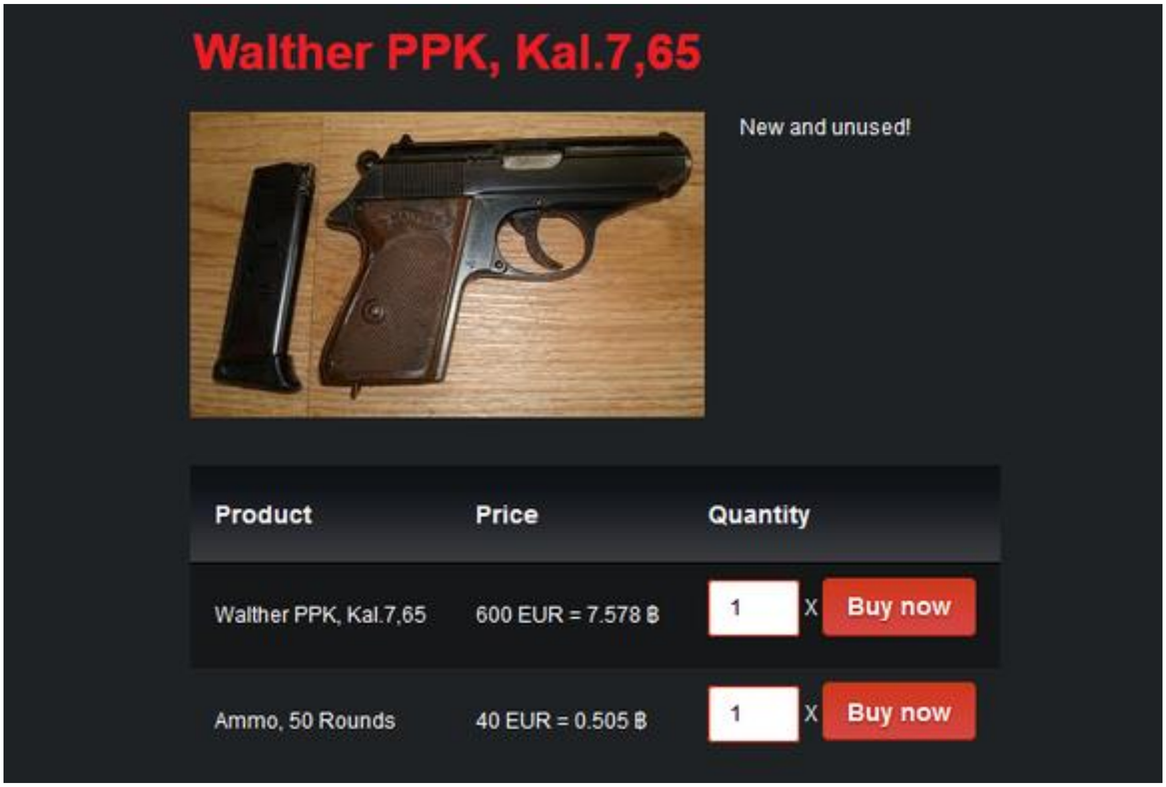
Brad Chacos @BradChacos

Aug 12, 2013 3:00 AM

There’s a place lurking beneath the Internet you use every day.

It’s a hidden underbelly, home to both rogues and political activists, and accessed only with the help of specially designed anonymizing software. It’s a secretive place, where Arab Spring dissidents can hide their digital tracks, a place where whistleblowers can reach out safely to scoop-seeking media outlets. And, yes, it’s also a dangerous place, where a lot of illicit, underground nastiness occurs.

There, you’ll find a society that lurks intentionally in the blind spots of search engines. Some call it the Darknet. All call it hard to reach—though it’s hardly impregnable, given last week’s news of security vulnerabilities, as well as site takedowns following the arrest of an alleged pornographer. Like a demilitarized zone or a lawless land, it’s not a place most people visit—nor should they. But by the time you’re done reading this article, you’ll know more about this shadowy, parallel online universe than Bing or Yahoo ever will.



Walther PPK, Kal.7,65

New and unused!

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 7.578 ฿	1 X Buy now
Ammo, 50 Rounds	40 EUR = 0.505 ฿	1 X Buy now

The Darknet ain’t your grandma’s Internet—but its depths hide both the noble and the treacherous.

Delving into the Darknet

Darknets are small niches of the “Deep Web,” which is itself a catch-all term for the assorted Net-connected stuff that isn’t discoverable by the major search engines. (BrightPlanet has a stellar Deep Web primer.)

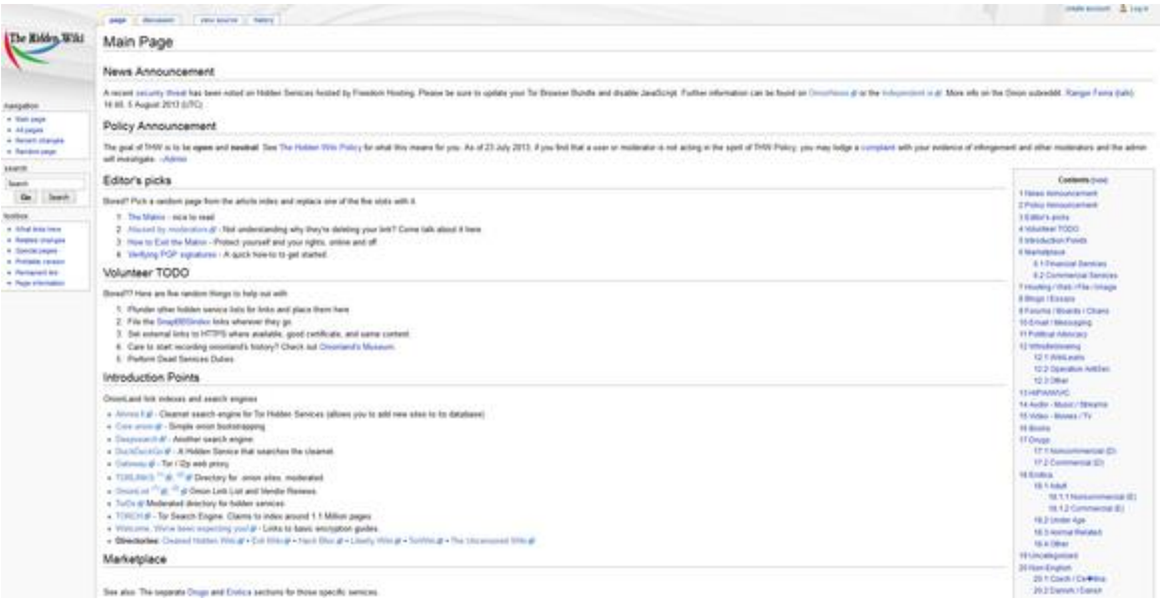
Most of the flotsam and jetsam found in the Deep Web are unintentional cast-offs: dynamic database queries and odd file formats that search engines aren’t equipped to deal with. Darknets, on the other hand, deliberately hide from the prying eyes of the searchable Web. They cloak themselves in obscurity with specialized software that guarantees encryption and anonymity between users, as well as protocols or domains that the average webizen will never stumble across.

Your chances of finding these clandestine networks, much less specific content on them, are virtually nil unless someone already in the know points you in the right direction.

And it’s no wonder why. Consider Onionland, the major Darknet hiding inside the anonymity-protecting Tor network, which was the focus of last week’s hubbub. (Fun fact: The Onionland name pays homage to Tor, which was originally an acronym for “The Onion Router.”)

Diving into Onionland—after you’ve installed the proper software and taken the proper safety precautions; more on that later—is awfully reminiscent of using the Surface Web of yesteryear. Since search engines don’t trawl the depths of the Darknet, the best guide to its realms are simple link directories.

Yes, the underbelly of the Web has yet to move beyond the old Yahoo days.



Main Page

News Announcement

A recent security threat has been noted on Hidden Services hosted by Freedom Hosting. Please be sure to update your Tor Browser Bundle and disable JavaScript. Further information can be found on OnionNews or the Independent.ie. More info on the Onion subreddit. Rangor Ferns (talk) 14:40, 5 August 2013 (UTC)

Policy Announcement

The goal of THW is to be **open** and **neutral**. See The Hidden Wiki Policy for what this means for you. As of 23 July 2013, if you find that a user or moderator is not acting in the spirit of THW Policy, you may lodge a complaint with your evidence of infringement and other moderators and the admin will investigate. --Admin

Editor's picks

Bored? Pick a random page from the article index and replace one of the five slots with it.

1. The Matrix - nice to read
2. Abused by moderators - Not understanding why they're deleting your link? Come talk about it here
3. How to Exit the Matrix - Protect yourself and your rights, online and off
4. Verifying PGP signatures - A quick how-to to get started.

Volunteer TODO

Bored?? Here are five random things to help out with

1. Plunder other hidden service lists for links and place them here
2. File the SnapBBSIndex links wherever they go
3. Set external links to HTTPS where available, good certificate, and same content
4. Care to start recording onionland's history? Check out Onionland's Museum.
5. Perform Dead Services Duties.

Introduction Points

OnionLand link indexes and search engines

- Ahmia.fi - Clearnet search engine for Tor Hidden Services (allows you to add new sites to its database)
- Core.onion - Simple onion bootstrapping
- Deepsearch - Another search engine
- DuckDuckGo - A Hidden Service that searches the clearnet
- Gateway - Tor / I2p web proxy
- TORLINKS [1], [2] Directory for .onion sites, moderated
- OnionList [1], [2] Onion Link List and Vendor Reviews
- TorDir Moderated directory for hidden services
- TORCH - Tor Search Engine. Claims to index around 1.1 Million pages
- Welcome, We've been expecting you! - Links to basic encryption guides
- **Directories**: Cleaned Hidden Wiki • Evil Wiki • Hack Bloc • Liberty Wiki • TorWiki • The Uncensored Wiki

Marketplace

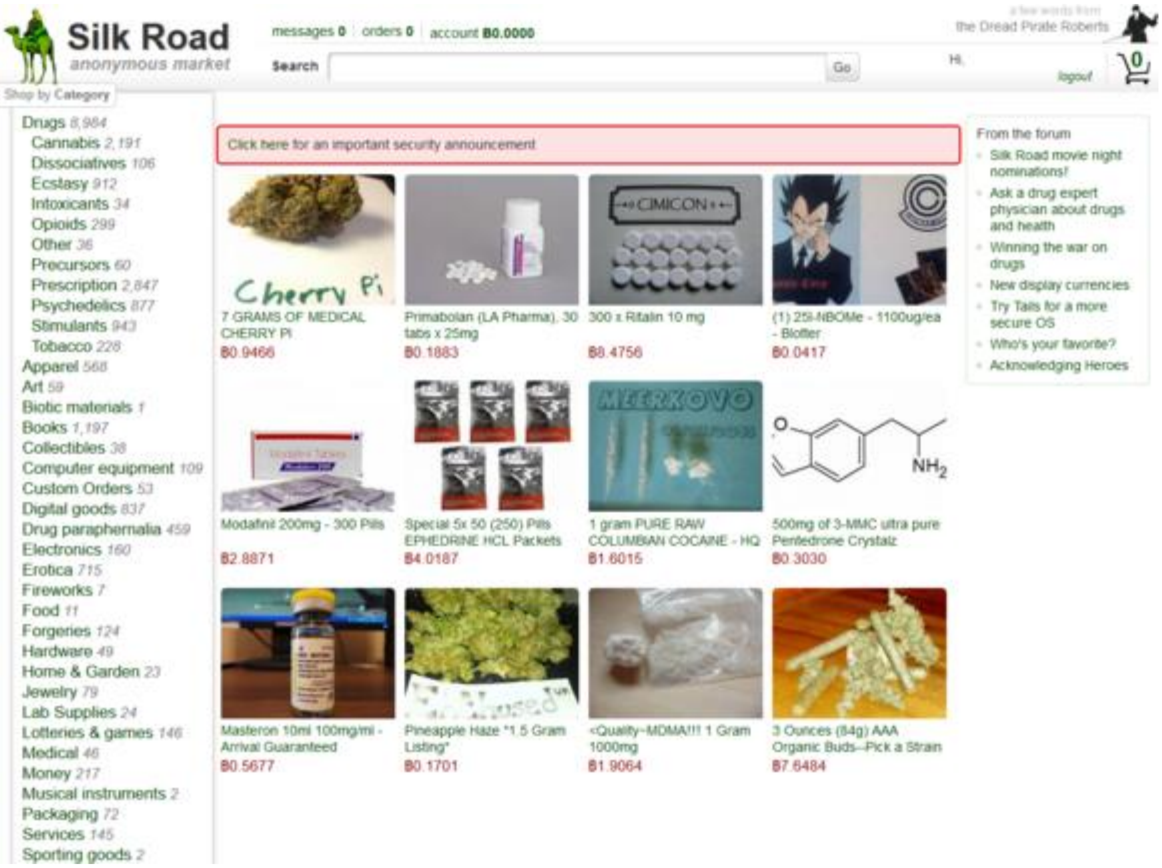
See also: The separate Drugs and Erotica sections for those specific services.

Contents [hide]

The Hidden Wiki is sometimes referred to as the front door of Onionland. Be careful what you click.

Even the major directories aren't completely reliable. Like a swamp, Onionland is constantly shifting, with Hidden Services appearing and vanishing on a daily basis. (Again, more on Hidden Services later.) A lot of sites listed on Onionland directories are simply gone now. Heck, even the directories themselves sometimes shift URLs, and you have to track down their new location, either within Onionland itself or on the .onion subreddit.

That said, three common Onionland starting points are The Hidden Wiki, TorDir, and TorLinks. All the directories in Onionland always point to Torch as a search engine of onions, but it never works properly. You can get to Torch's front page just fine, but individual searches time out. Every. Single. Time.



The infamous Silk Road.

Once you’re on a directory, one thing becomes overwhelmingly obvious: A lot of dirty, downright illegal stuff happens in Onionland. You’ll quickly find links to credit-card scammers, forged documents and currency, weapons dealers, gambling sites, marketplaces for every vice imaginable, hacker havens, the types of illegal and disgusting porn that get chased off the Surface Web, and even the notorious Silk Road trading post.

But wait! Don’t close your browser in disgust quite yet. *Do* be smart about your browsing—we have more security tips on the next page—and above all else, remember Onionland’s anarchistic nature.

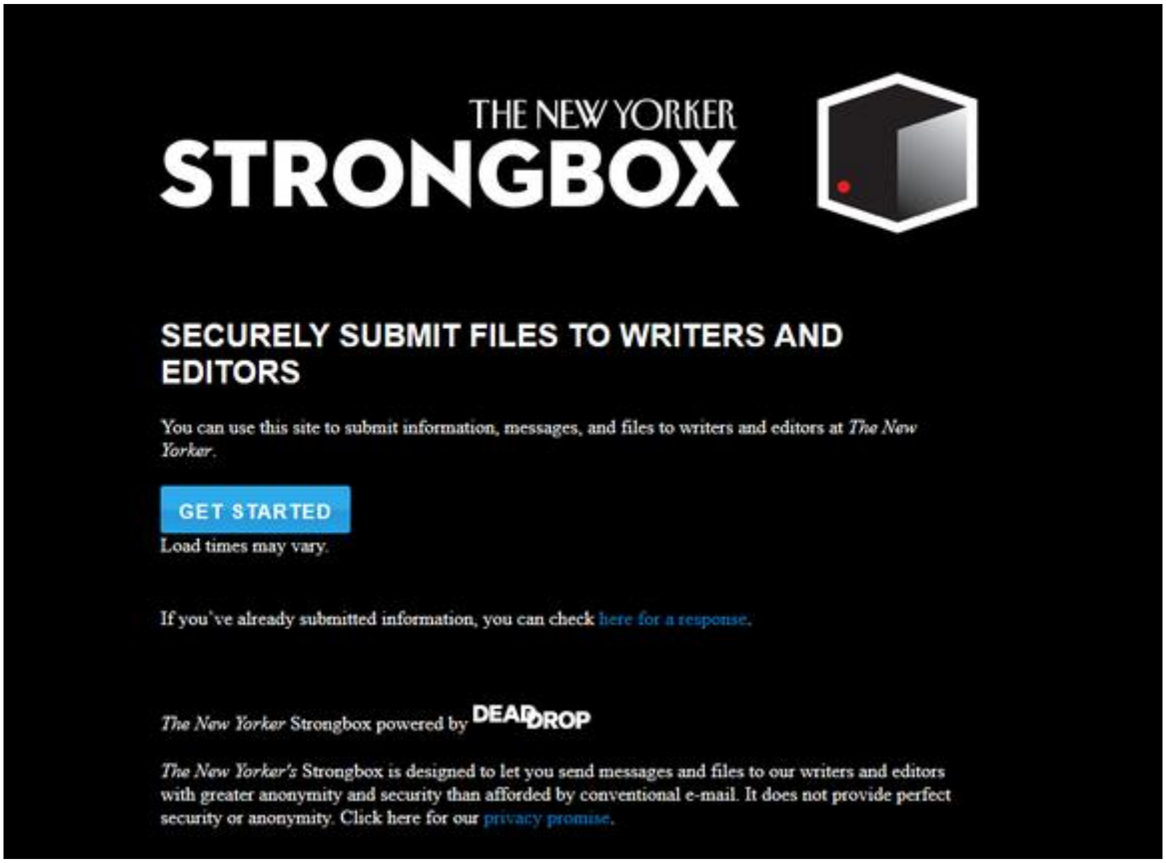
- **Tip #1:** You don’t have to click anything you don’t want to. You aren’t likely to stumble across questionable stuff unless you specifically seek it out.
- **Tip #2:** Remember that thanks to the underlying Tor technology, this Darknet is truly anonymous. If something for sale on the Darknet catches your eye, ask yourself: Are the services listed in this major Onionland wiki legit, or are they fronts for people looking to separate fools from their Bitcoins? Many of the scarier listings in directories are flat-out scams.

The bright side of the Darknet

But the same anonymity that makes Onionland a haven for weapons dealers and perverts also makes it a bastion of a more noble cause: free speech.

Many countries lack the equivalent of the United States' First Amendment. Darknets grant everyone the power to speak freely without fear of censorship or persecution.According to the Tor Project, anonymizing Hidden Services have been a refuge for dissidents in Lebanon, Mauritania, and Arab Spring nations; hosted blogs in countries where the exchange of ideas is frowned upon; and served as mirrors for websites that attract governmental or corporate angst, such as GlobalLeaks, Indymedia, and Wikileaks.

The *New Yorker*'s Strongbox, which allows whistleblowers to securely and anonymously communicate with the magazine, is a Tor Hidden Service. The Tor Project says that authorities offer similarly secure tip lines, and that some militaries even use Hidden Services to create online secure command and control centers.



THE NEW YORKER
STRONGBOX

SECURELY SUBMIT FILES TO WRITERS AND EDITORS

You can use this site to submit information, messages, and files to writers and editors at *The New Yorker*.

Load times may vary.

If you've already submitted information, you can check here for a response.

The New Yorker Strongbox powered by DEADDROP

The New Yorker's Strongbox is designed to let you send messages and files to our writers and editors with greater anonymity and security than afforded by conventional e-mail. It does not provide perfect security or anonymity. Click here for our privacy promise.

The New Yorker's Strongbox whistleblower communication tool.

Delve deeper into the Darknet, and you'll find a veritable cornucopia of services dedicated to spreading the word: secure messaging and file-sharing tools, libraries chock-full of political literature, anonymous boards dedicated to intelligent debate, and much, much more. You'll even find a completely anonymous mirror for the DuckDuckGo search engine, in case you're worried about Google or Microsoft looking over your shoulder while you surf the Surface Web.

And those are all things that you can find from the major directories. Imagine the secrets flowing even deeper, beyond the signposts and outside links. None of Onionland's positive benefits—*none*—would be possible if it didn't offer a level of security that made the service so appealing to less savory types.

That's the rub about free speech: Sometimes people say and do things you don't like.

Intrigued? Read on to learn more about the technical aspects of Onionland, and the tools and precautions you'll need to visit the Darknet yourself.

All about Tor

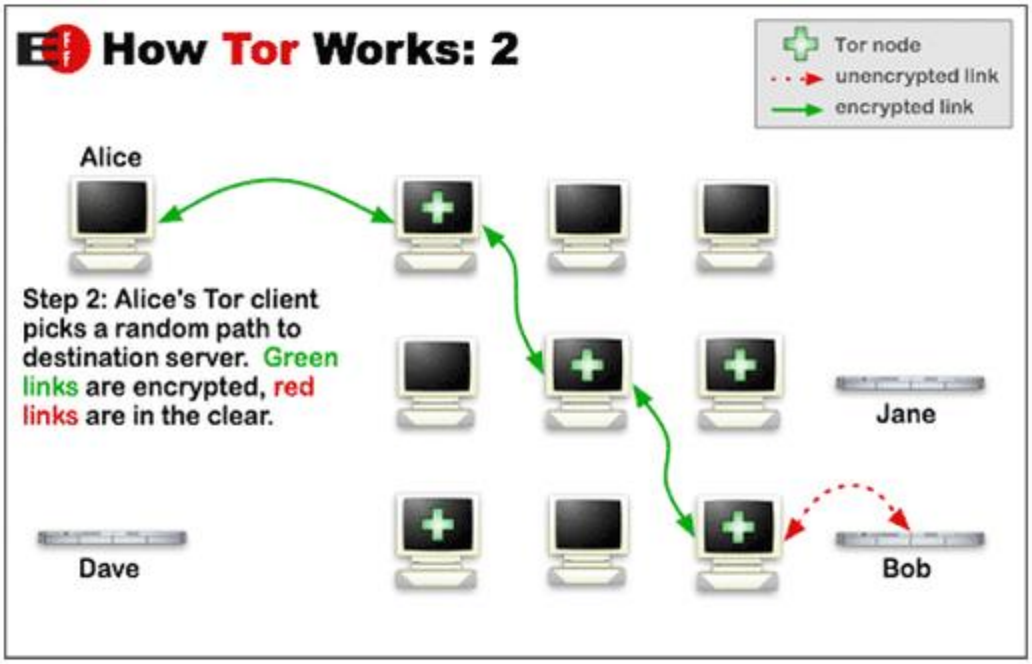
At the heart of Onionland lies Tor.

Ostensibly, Tor technology is designed to let you surf the Web anonymously, encrypting your connection requests and bouncing them through several in-network "nodes" before finally contacting the Web server that is your final destination. Each node knows only the identity of the nodes it directly connects to—*not* every connection between your PC and the Web server—and each "hop" between nodes gets its own set of encryption keys.

"The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you—and then periodically erasing your footprints," the Tor website explains.

Bouncing along so many connections makes browsing *slooooow*, but as long as you're smart enough to take some additional behavorial precautions, Tor is a particularly secure way to browse anonymously online.

Tor's network doesn't just offer anonymity to Web surfers, though; it also offers anonymity to Web servers, in the form of Hidden Services. They're the foundation that Onionland is built upon.


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

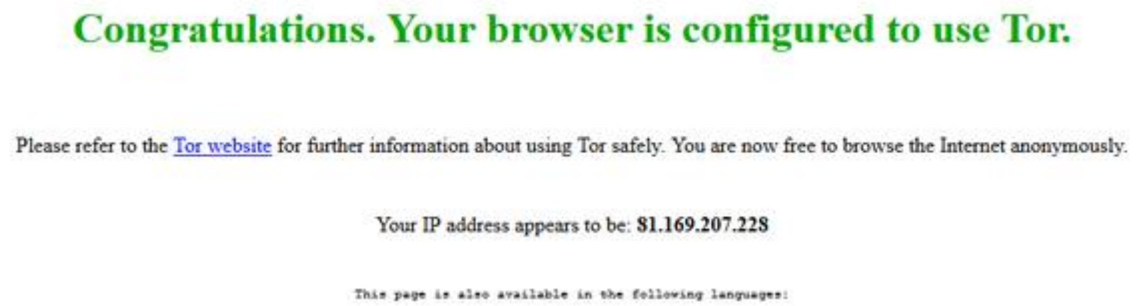
TOR PROJECT

The technology behind Tor Hidden Services is complex. In a nutshell, it allows websites to hide within the Tor network itself, rendering both server and servee completely anonymous. A website set up as a Tor Hidden Service is accessible only when you're connected to the Tor network. If you're not connected to Tor, you get nada. The Hidden Services pseudo-suffix, .onion, isn't resolvable by the Internet's core DNS servers, and Hidden Service URLs are a jumbled, 16-character alphanumeric mess autogenerated by a public cryptography key when the site is created.

Have an example: http://idnxcnkne4qt76tg.onion/ For those using Tor, that link will lead to the Tor Project website. For everyone else: a dead end.

There's no chance that you—or Google—will stumble across that site by accident, or any of the secretive Darknets that have sprung up around technologies such as I2P orFreenet (which Alex Wawro touched upon in the August issue of PCWorld magazine).

A word about safety



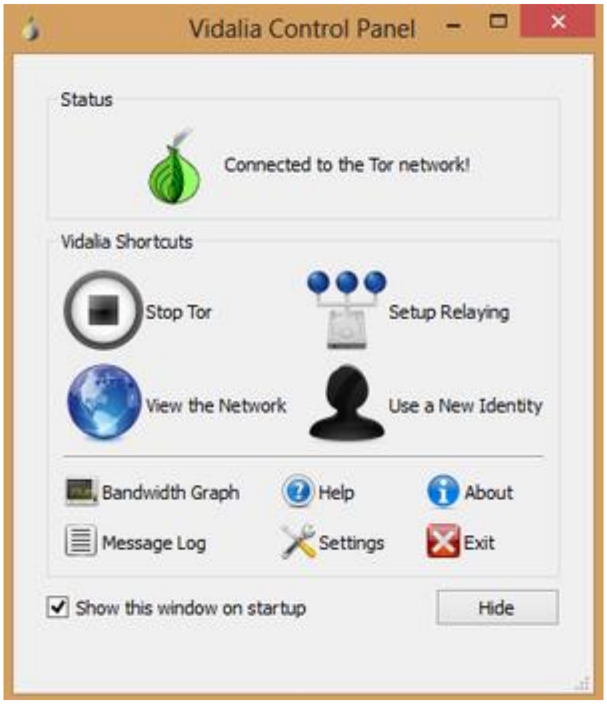
Congratulations. Your browser is configured to use Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

Your IP address appears to be: **81.169.207.228**

This page is also available in the following languages:

Once you’ve downloaded the Tor browser bundle, you have all you technically need to dive into Onionland, but let’s talk precautions first. You don’t want to delve the Darknet unprepared; a lot of computer-savvy, potentially malicious people are lurking out there. (You did see the parts of this article mentioning the guns and the drugs, right?)



Connected to the Tor network!

☑ Show this window on startup

The Tor browser’s Vidalia control panel.

First, realize that Tor alone isn’t enough to protect your privacy, as evidenced by a recent security exploit that embedded itself in many Onionland sites and sent crucial identifying information to a central server, destroying the anonymity that is central to the Darknet. Be sure to turn off JavaScript (click the *S* button next to the Tor browser’s address bar and select *Forbid scripts globally* from the drop-down menu) and *don't* configure the browser to accept cookies or to run add-ons.

And although this probably doesn't need to be said, don't share any personal information with anyone or any site on the Darknet. That includes reusing passwords you use on Surface Web sites, or divulging credit card information. Bitcoins are the preferred currency of this computerized Wild West for a reason.

Speaking of which, be very, very careful when slinging your digital dollars around. The anonymity of Bitcoins and the Darknet makes Onionland a haven for scammers.

Finally, consider visiting Onionland from a virtual machine to protect your actual PC from harm if you do manage to catch something nasty while trawling the depths. You could run a preview copy of Windows 8.1 or the Linux distribution of your choice in Virtualbox if you'd like, or you could (preferably) create a live disc of Tails, a Linux distro built around anonymity and the Tor browser.

Seriously: Don't muck around in the Dark without taking the proper security precautions. Got it? Good. Now go do it—or better yet, *don't*.

This is not for you

In all likelihood, you'll never need to venture into the Deep Web. The Surface Web contains all the services and tools the average person could ever want. You won't find any streaming video services or social networks or corporate websites or any other mainstream elements buried in the depths of the Deep Web, and the Darknet is fraught with bogeymen just waiting for you to let down your guard. Enjoy the novelty of an article like this, maybe scope out a directory or two, and then stay well away.

But if you ever *do* need the sanctity of secure communications and true anonymity—a level of protection that the Surface Web simply can't provide—then rest easy. Everyone has a voice in the Darknet, down in the depths where even Google's spiders fear to crawl.

http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html