

DOCUMENTATION ON TOR: THE ONION ROUTER

Written By

A. K. M. Fahim Rahman (160215)

Mostofa Rakib Raihan (160220)

Introduction

Tor-The onion router is free and open source for enabling anonymous communication. This anonymity tool is used by user, who wants to stay private and uncensored during browsing. Tor directs Internet traffic through a free, worldwide network which consists of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance. It becomes more critical to trace user. Its intended use is to protect the personal privacy of users.

History

The basic idea of **Tor** -The Onion Routing was first proposed in 1995. The core principle of **Tor**, onion routing, was developed by United States Naval Research Laboratory employees. Tor enables its users to surf the Internet, chat and send instant messages anonymously. Though some websites restrict allowances through **Tor**. The software we know today as **Tor** becomes an open source from 2003.

Onion Routing

The main concept of Onion routing is inspired from Onion. It is implemented by encryption in the application layer of communication stack like the nested layers of an onion. Tor encrypts the data, including the next node destination IP Address, multiple times and sends it through a virtual circuit comprising successive, random-selection **Tor** relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it.

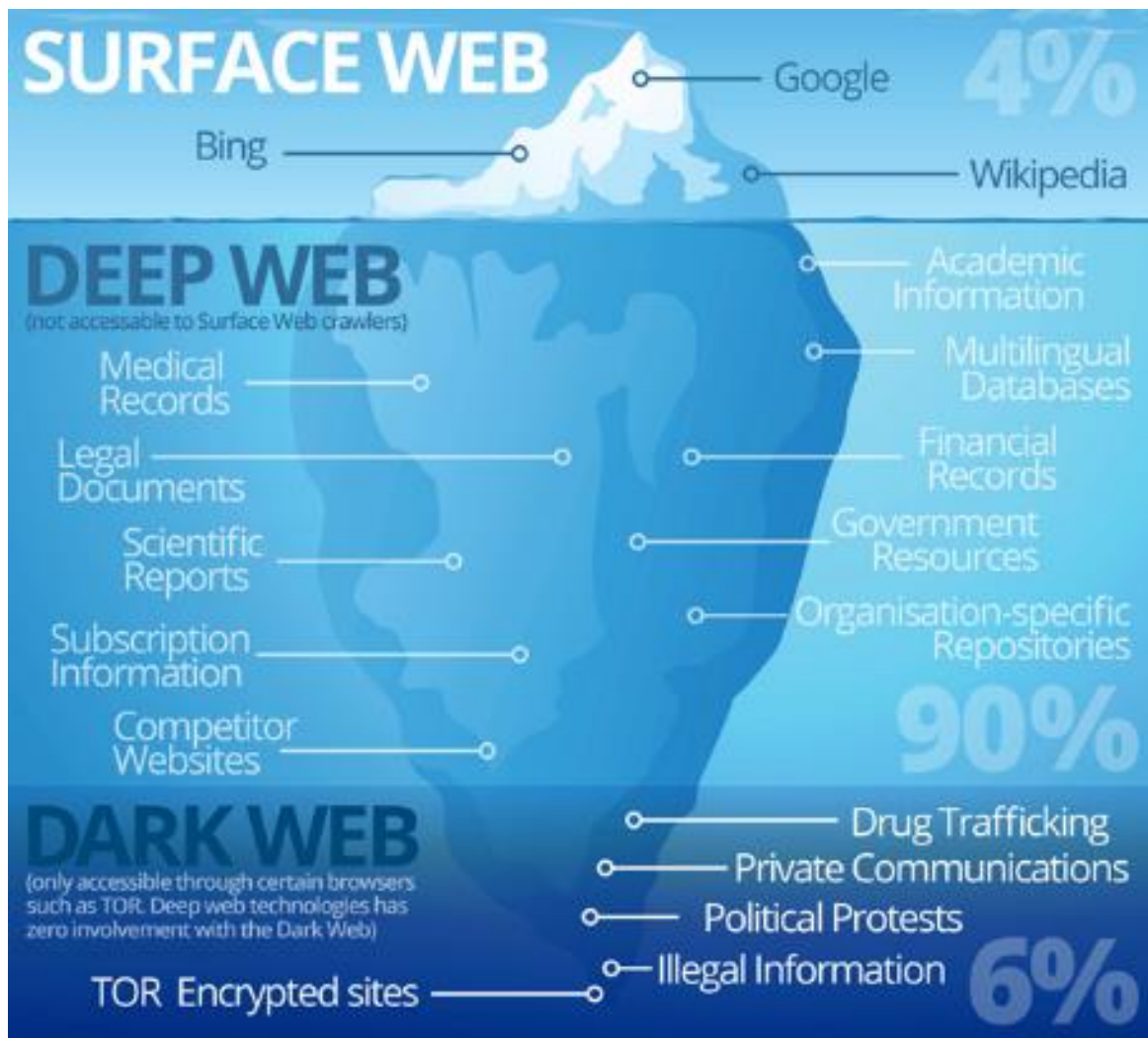
Tor browser

Tor browser is literally Firefox browser. Around 95% of its code comes from Firefox and the other 5% is modification and addition. The Firefox and **Tor** browser have collaborated for a long time. The **Tor** Browser team builds Tor browser by taking Firefox ESR (Firefox Extended Support) and applying some patches on it. As we know Firefox ESR is built by Firefox for large organizations. These changes add a huge and valuable privacy feature for the **Tor** users.

Why TOR?

We can classify the whole internet into three parts. The **Surface Web**, the **Deep Web** and the **Dark Web**. The surface web is that part of internet which is indexed in the search engines like Google, Bing etc. The rest of the internet is not indexed. As a result we have to know the exact address to access those parts. From that part there are some extreme contents like drug dealing, child abuses, animal abuses, TOR encrypted sites etc. which are generally hidden from the common people and is illegal around the globe.

To access the **Deep Web** and **Dark Web** we have to use onion network because firstly, the contents of it are in onion servers and secondly by using onion routing the identity can be classified.

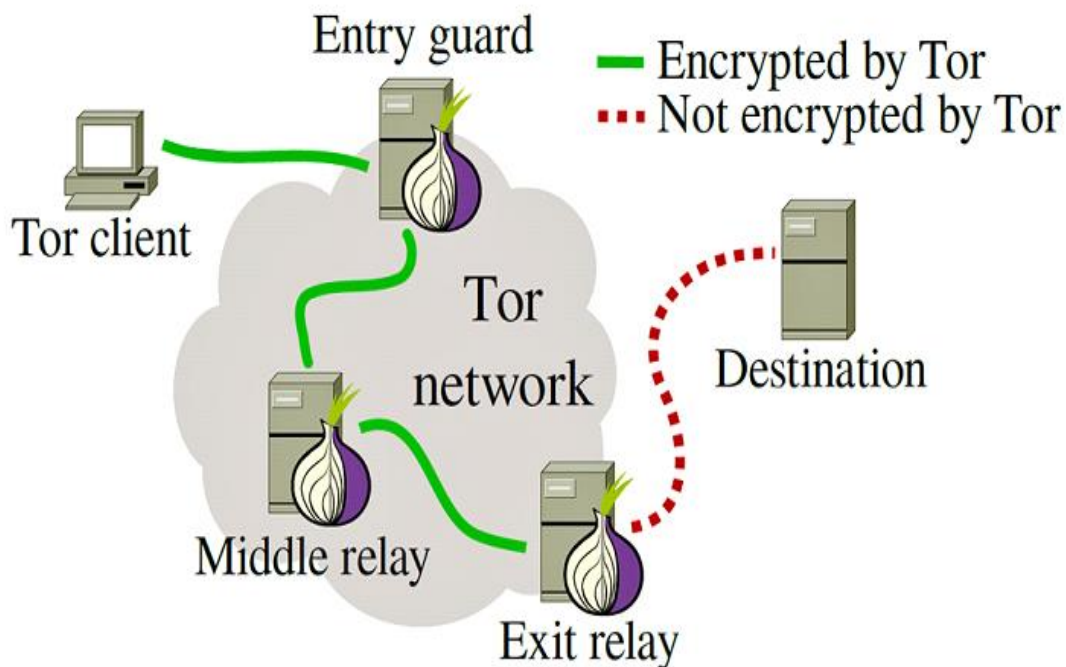


Why Tor browser is public:

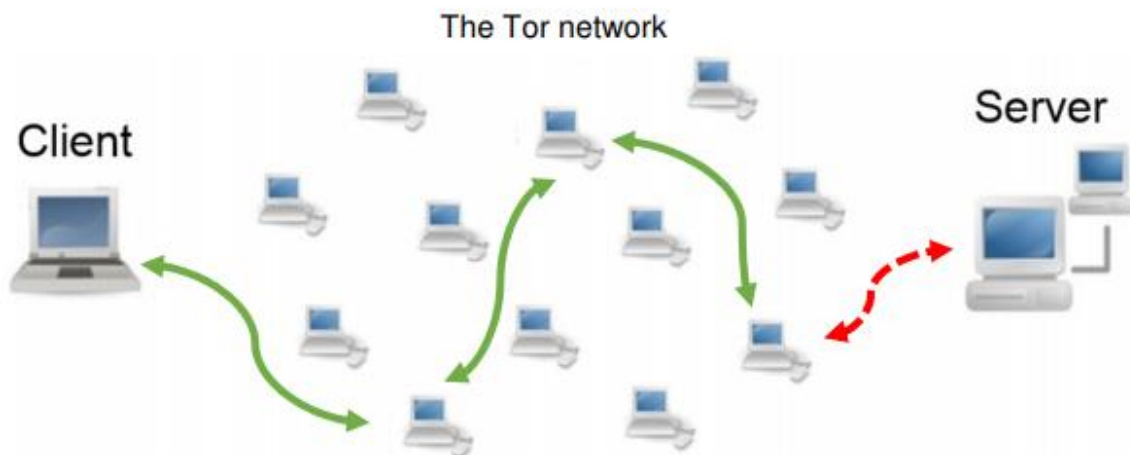
From the history we all know that tor was created with the support of US Naval Research Laboratory in suburban Maryland in Washington DC. If today TOR was only used by the US Navy, the ability to browse the open internet anonymously over tor would be useless. You still couldn't tell which tor user accessed which website, but if you see someone accessing TOR you would know it's a US agent, and if you see a website visited via the tor network you know it's visited by a US agent. The only other function of tor, hidden services, is much easier to achieve with a simple VPN if you only want to use it inside a single organization where anonymity isn't a primary concern. In short, TOR can only be useful for the navy because it's publicly available. An anonymity network used only by one group is useless for hiding that group's activities.

How does TOR works

The **Tor** network runs through the computer servers of thousands of volunteers spread throughout the world. Data is banded into an encrypted packet when it enters the Tor network. Tor strips away part of the packet's header, which is a part of the addressing information that could be used to gather idea about the sender. This is the step where Tor becomes distinguishable from normal Internet connections. And then, Tor encrypts the rest of the addressing information, called the packet wrapper. And once again regular Internet connections don't do this. The modified and encrypted data packet is then routed through many of these servers, called relays, on the way to its final destination. Each relay decrypts only enough of the data packet wrapper to know which relay the data came from, and which relay to send it to next. The relay then rewraps the package in a new wrapper and sends it on.



The layers of encrypted address information used to generate anonymous data packets sent through Tor are quite same as an onion.

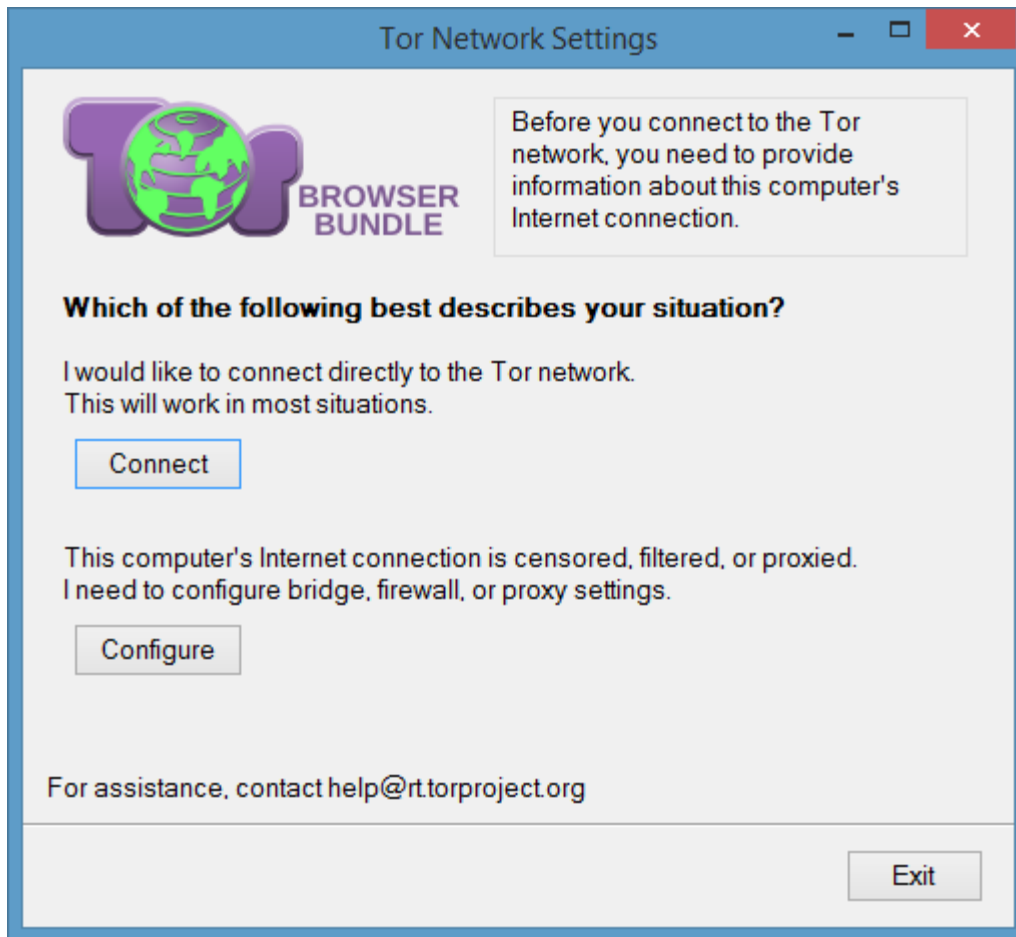


Websites that user visit only see the IP address of the Tor exit node (the last node in the **Tor** network that your traffic passes through), and not users actual IP. That way, a data packet's path through the **Tor** network cannot be fully traced.

How to setup and use the Tor Network

For windows/MAC we have to install **Tor Browser**. Tor nodes are published so anyone wishing to block Tor access on their network simply needs to block requests destined for these known nodes. A *bridge* is simply an unpublished Tor node; therefore connections to it likely will not be blocked because it's not a known node.

The Linux Tor browser is a single binary executable that has no installation process. We have to extract the zipped tar file and it will create a **tor-browser** directory. Run that file from the shell or double-click it in your file manager to launch the Tor Browser. This will launch the now-familiar first run process that will allow user to set up any bridges or proxies user may need, and connect to Tor.



Tor vs. VPN: the Differences

In this time of century everybody wants to surf internet without being acknowledged by the cybercriminals. And the best tool is available for privacy, are **Virtual Private Network (VPN)** and **Tor**.

A **Virtual Private Network (VPN)** connects a device through a secure tunnel to a remote server in a country of user's choice. This **masks the IP addresses**, making it appear as though the user is accessing the internet from the location of the remote server instead of your actual location. It provides an end-to-end encryption.

****Whereas Tor** doesn't provide end-to-end encryption, so unless user is accessing a website with HTTPS enabled, or using the dark web, the owner of the exit node the user use can see your data and its destination. Though VPN has some pitfalls also.

So, the best way to stay private will be combining Tor with VPN.

Tor Circuit

When user tries to enter a site which ended with .onion world the normal network declares it as invalid. But this site refers system that is used in Dark Web. When user tries to enter .onion domains. With no registrar, these domain names are actually a portion of a public key encryption of the address of the site. Tor browser knows how to expand one of these domains and it can figure out how to connect. A .onion domain name will always be 16 characters long and will only contain lowercase letters a to z and the digits 2 through 7.

If we try to visit uj3wazyk5u4hnavtk.onion this web site, the normal network will mention this as invalid. Because Chrome doesn't know how to interpret and decode.

This site can't be reached

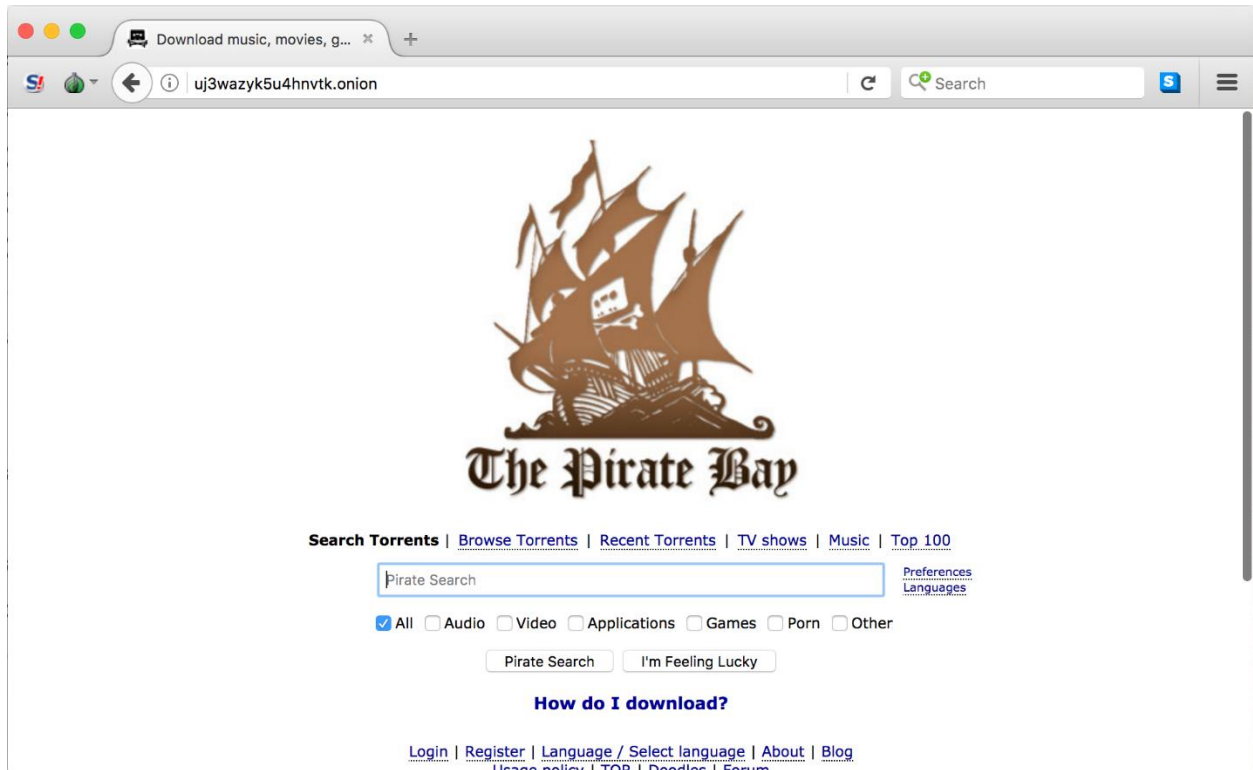
uj3wazyk5u4hnavtk.onion's server IP address could not be found.

Try:






- Checking the connection
- [Checking the proxy, firewall, and DNS configuration](#)
- [Running Network Diagnostics](#)

ERR_NAME_NOT_RESOLVED

But Tor browser can recognize and interpret this site. The screen shot is given below.



Tor Browser automatically uses the onion network to bounce all your queries from proxy server to proxy server given below:

<p>New Identity   U</p> <p>New Tor Circuit for this Site   L</p>	<p>Tor circuit for this site (uj3wazyk5u4hnavtk.onion):</p> <ul style="list-style-type: none">  This browser  Canada (159.89.32.215)  France (176.67.168.210)  United States (108.161.133.189)  (relay)  (relay)  (relay)  Onion site
<p>Security Settings...</p> <p>Tor Network Settings...</p>	
<p>Check for Tor Browser Update...</p>	

At first it bounces to Canada, France, back to the United States, through three relays, and then finally onto the Onion site (The Pirate Bay).

Clients can have anonymous communication to a server by proxying their traffic through a Circuit of three Tor relays. Tor is a volunteer-based network and anybody can run and advertise its own Tor relay. The number of Tor relays per one IP address should not exceed two.

Tor Content

The digital world is full of evil such as spammers, attackers, troll armies, digital marketing firms and many more whose only objective is to use our private data for their gain. Even governments are known to spy on people to meet their political needs. Many journalists, activists and researchers work has been exploited due to such a vulnerable structure.

Tor hidden services: Tor Hidden Services are a feature which adds responder anonymity to Tor. Specifically, hidden services allow running an Internet service such as a Web site so that the clients of the service do not know its actual IP address. When a client wants to communicate with the hidden service, he/ she needs to know not only its onion address, but also the public key and the list of introduction points. Due to this Bob generates two service descriptors which contain this information and uploads them to 6 hidden service directories.

Originating Traffic: Tor creates virtual circuits through the Tor network through which it can multiplex and onion-route that traffic to its destination. Once inside a Tor network, the traffic is sent from router to router along the circuit, ultimately reaching an exit node and is forwarded on to its original destination.

Guard nodes: In order to significantly reduce the probability of traffic confirmation attacks, Tor developers introduced the concept of entry guard nodes. A Tor client initially selects a set of three guard nodes from among Tor relays which have a Guard flag assigned to them. Whenever less than two guard nodes from the set are reachable, new guard nodes are chosen. A guard node remains in the set for a random duration between 30 and 60 days.

Deep Web Markets

Deep web market is a solution for all type legal or illegal products because these marketplaces offer security to both parties means seller or buyer, here you can use escrow service at a type to deals with any listed products. Drugs, Weapon, Digital products, Fraud, Services etc are available here.

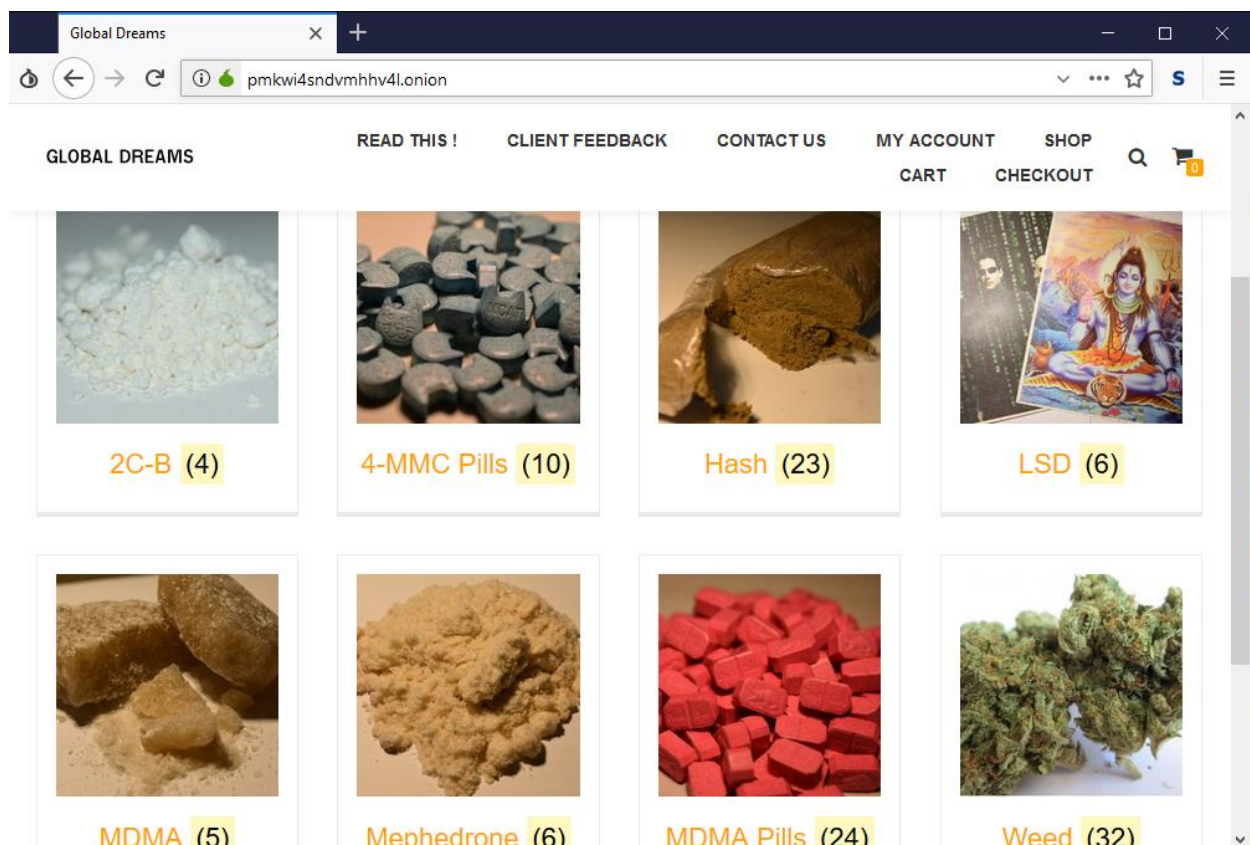
And Below listed marketplace and store only deal with Bitcoin and other crypto coins like Bitcoins cash, Monero, DASH, etc. Means if someone wants to deal with these marketplaces then he needs to any crypto coins which marketplace prefer for dealing (Bitcoins, Monero, Dash, LTC, etc).

Drugs

The drugs are very sensitive products and one can't buy most of the illegal or legal drugs without a doctor prescription, but the dark web has multiple deep web drugs sites and stores that deal in all type legal or illegal drugs. (**Example**, Global Dreams is a Darknet Market which sells products such as Hash, Weed, and LSD.)

A list of some drug selling websites are –

1. **Global Dreams** – (<http://pmkwi4sndvmhvh4l.onion/>)
2. **TheBarKing Store** – (<http://tbkukxw3vpnrhbn.onion/>)
3. **DopeFarm** – (<http://dopefruggev5v4ul.onion/>)
4. **Onion Pharma** – (<http://pharma5jbbmwjoo3.onion/>)
5. **New Shit** – (<http://newshit5g5lc5coc.onion/>)
6. **People Drug Store** – (<http://drugszun7tvsgsaa.onion/>)
7. **The Pot Shop** – (<http://tdupp57f454vusnx.onion/>)



Porn and Rape

It has porn archive 10 times bigger than the normal network. Child porn, Gang rape, private video by hacking camera all are available here. Video of rape and murder, child porn, having intercourse with dead people. There are many live sites where people upload real life rape video. There are over millions of sites in this network.

A list of few onion websites for porn and sexual abuses:

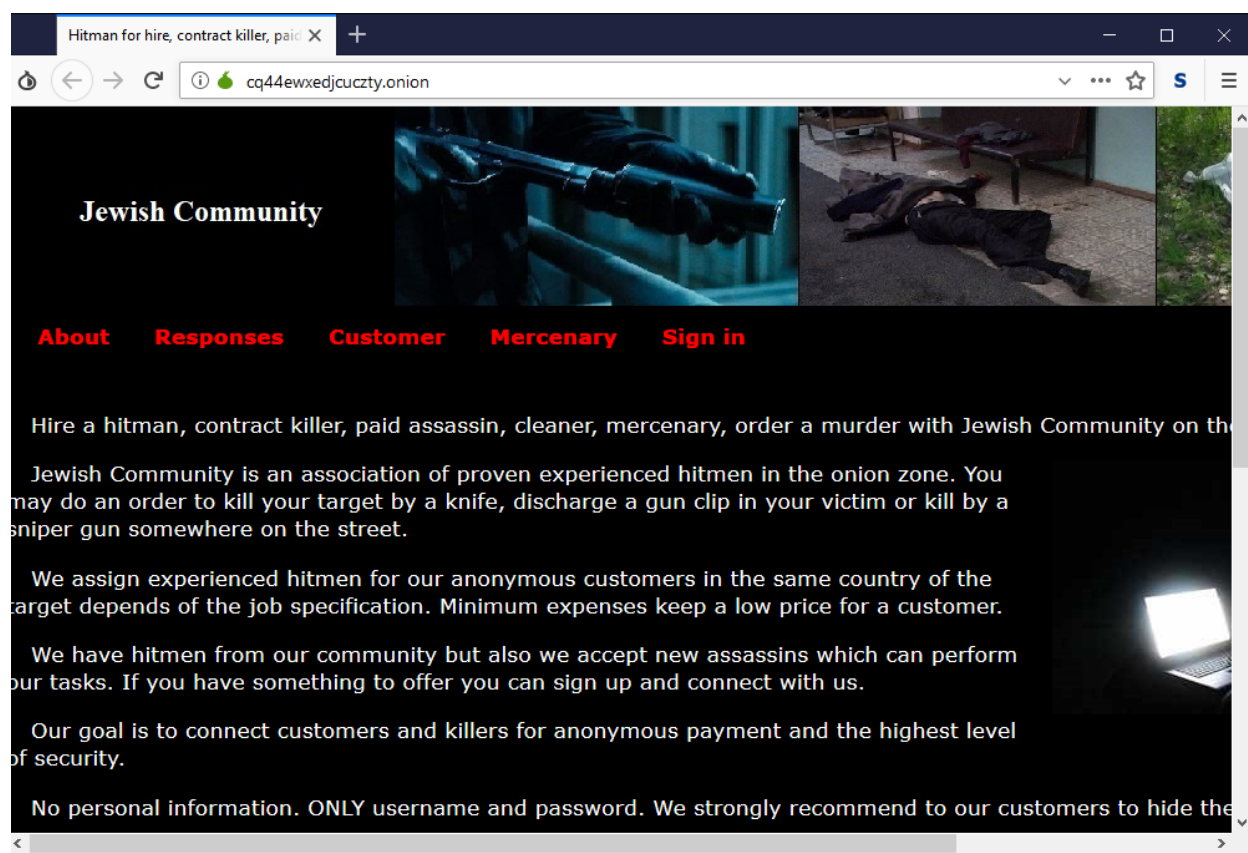
1. **Vault of Sex Dead** – (<http://5p6s4vkwdapnsiaw.onion/>)
2. **GermanGirls** – (<http://wirtin67ywc72piq.onion/>)
3. **xvideos** – (<http://xvideos24y74huqj.onion/>)
4. **Rape and Murder** – (<http://gigbztmown7d6usl.onion/>)
5. **Brutal. Onion** - (<http://xyx4fjc6bkz5fy4v.onion/>)
6. **Celebrity Underground** – (<http://iz56hciiqh5uh5u.onion/>)
7. **Dosug** - (<http://dosug4rea4kvnk5f.onion/>) [escort service]
8. **Blood and guts** – (<http://oxwugzccvk3dk6tj.onion/gore/index.html>)



Hitman

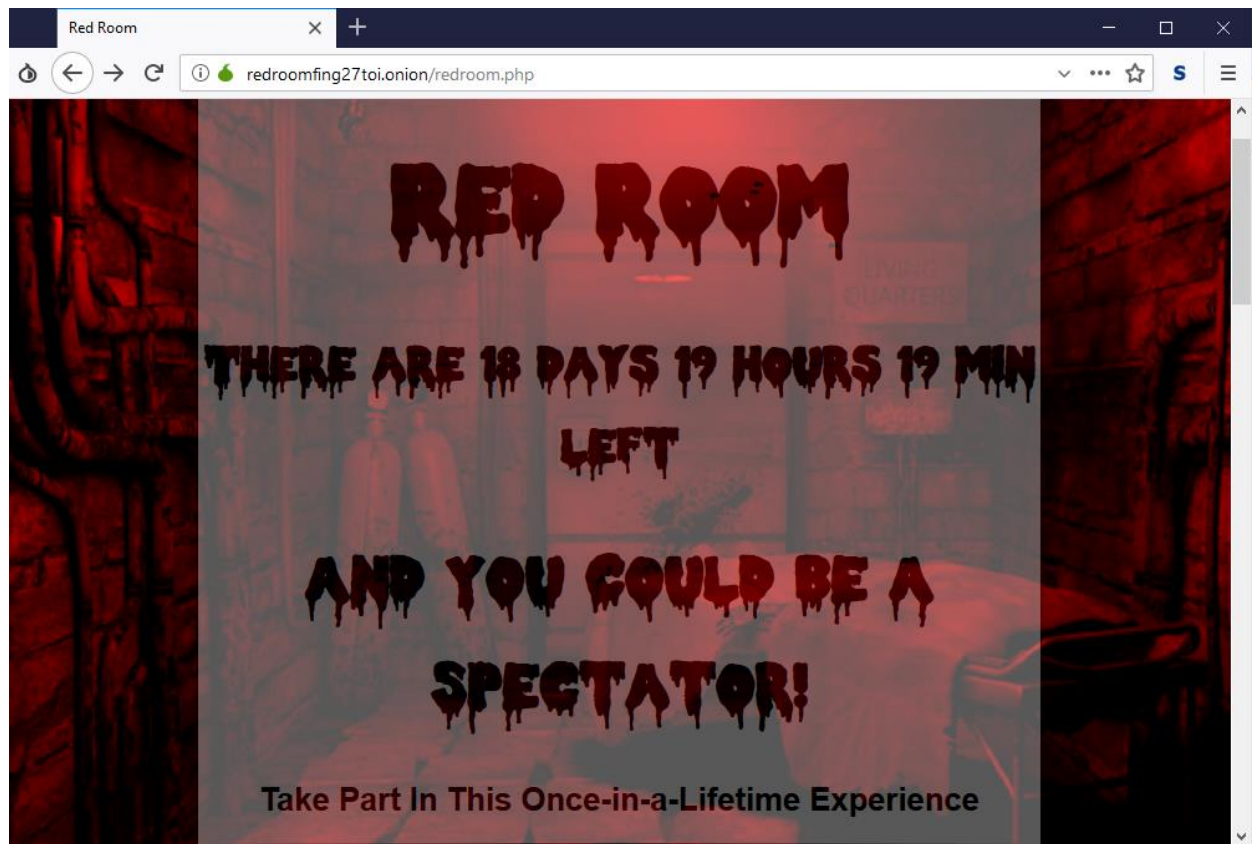
Deep web offering all type services like deep web hitman, Rent a Hitman, Rent a Hacker, Buying documents, Escrow. Jewish community is one of the oldest Hitmen-for-hire services on the Dark Web. Acts as an Escrow between people interested Payment is only released to the other party after a successful job, or else it's transferred to another Hitman or refunded. In their services, and experienced hitmen who can provide said services. Users create an anonymous account on the platform and make payments in BTC.

Most of the murders are done by usual mobsters who use handguns or knives and have hoods waiting for a victim near a house. Also they can offer you professional hitman with sniper guns. Cheapest killings start as low as USD \$6000, and then go up depending on the victim, method used to kill and so on. Has in in-built Bitcoin mixer to anonymize your coins further. Cheapest killings start as low as USD \$6000, and then go up depending on the victim, method used to kill and so on. Has in in-built Bitcoin mixer to anonymize your coins further.



Red Room

The modern version of the snuff movie, a **Red Room** is a live stream of the torture and murder of a person for the entertainment of others. When we explored dark web, we saw on the website homepage, the site offers snuff, death, gore, cry, Necro, Penalty type videos. They have very large snuff videos collections, which have blood, snuff, Torture, rape, etc. but videos available after premium subscription and fee will get by BTC.



Social Media

SecureShare, Raddle, Diaspora, Twitter Clone, Middle earth, OutBook, Reddit, Galaxy3, Dread etc. are social media of dark web.

Extra Deep web

Latest Deep web Updates and News, This Tor Link is a Part of not Evil Search Engine. **Confess your sins** is a web site where user who have lots of Sins and Want to confess but can't because users don't want to reveal your identity, Now solution available for user, here you can confess anything anonymously without revealing his identity.

Weapons

Every day, darknet performed more than thousands of weapons, warez, virus, and hacks related deals, and these numbers still growing day to day. Biggest deep web weapons marketplace which selling small or big type guns on the deep web, here you can buy Ammo, Guns. User can buy all type weapons by bitcoin.

The screenshot shows a web browser window with the address bar displaying "weapon5cd6o72mny.onion/shop.php". The page features three weapon listings, each with a green price tag at the top, an image of the weapon, a list of options, and a detailed description.

Weapon	Price (BTC)	Options
COLT LE6920 M4 AR-15 5.56NATO w/Optics	0.15525	1-2-3-4
TAVOR Mepro 21 SAR IDF Israel weapons Industry (IWI)	0.5822	1-2-3-4-5-6-7-8
FN PS90 w/Red-Dot 5.7X28	0.77626	1-2-3-4-5-6

COLT LE6920 M4 AR-15 5.56NATO w/Optics
Pre-Ban Pre-94 Bushmaster HBAR (heavy bull barrel) .223/5.56 Model XM15-E2S with 1-9 Twist 16" Barrel serial number L0470XX in "excellent" condition for its age and looks to be fired very little if at all! Comes with the EUROLUX 4X21 Scope

TAVOR Mepro 21 SAR IDF Israel weapons Industry (IWI)
The elite model TAVOR® SAR "IDF" model is the US civilian version in a semi-auto only configuration. It comes with a Meprolight® MEPRO 21 Day/Night Illuminated reflex sight mounted directly to the barrel, just as it is issued to the IDF


FN PS90 w/Red-Dot 5.7X28
the PS90 utilizes blowback operation and fires from a closed bolt for greater accuracy and reliability. The PS90 civilian legal 16.04 in cold hammer-forged MIL-SPEC barrel is equipped with an integrated muzzle brake to reduce recoil

Available some broad categories are Pistols, Assault Weapons, Full Auto Rifles, Submachine Guns, Sniper Rifles, Grenade Launchers, Walther PPK, Kal.7,65; Desert Eagle IMI, Kal.44; SIG Sauer P226 AL SO DAO, Kal. 9mm etc.

And it is quite a bit impossible to trace the buyer.


Fake Passport

Here user can easily buy fake passport. Criminal who is fleeing from law enforcement force can easily purchase passport of any country and can use it for multi-purpose.



Black Market - Guns Arms Ammo

weapon5cd6o72mny.onion/shop.php




European Fake ID
100% Realistic

European fake IDs perfectly manufactured. Seems real, already passed Customs and border in Italy, France, Spain, Switzerland without any problems.

Info

Specifications:
 Producer: EU Printer
 Delay: 5 days
 Quality: 100%

Price on market 3000\$




US Fake ID
100% Realistic

US fake IDs perfectly manufactured. Seems real, already passed Customs and border in USA, Canada, Mexico, Hawaii without any problems.

Info

Specifications:
 Producer: EU Printer
 Delay: 5 days
 Quality: 100%

Price on market 3000\$



Russian Fake ID
100% Realistic

Russian fake IDs perfectly manufactured. Seems real, already passed Customs and border in Moscow Airport, Belarus, Latvia without any problems.

Info

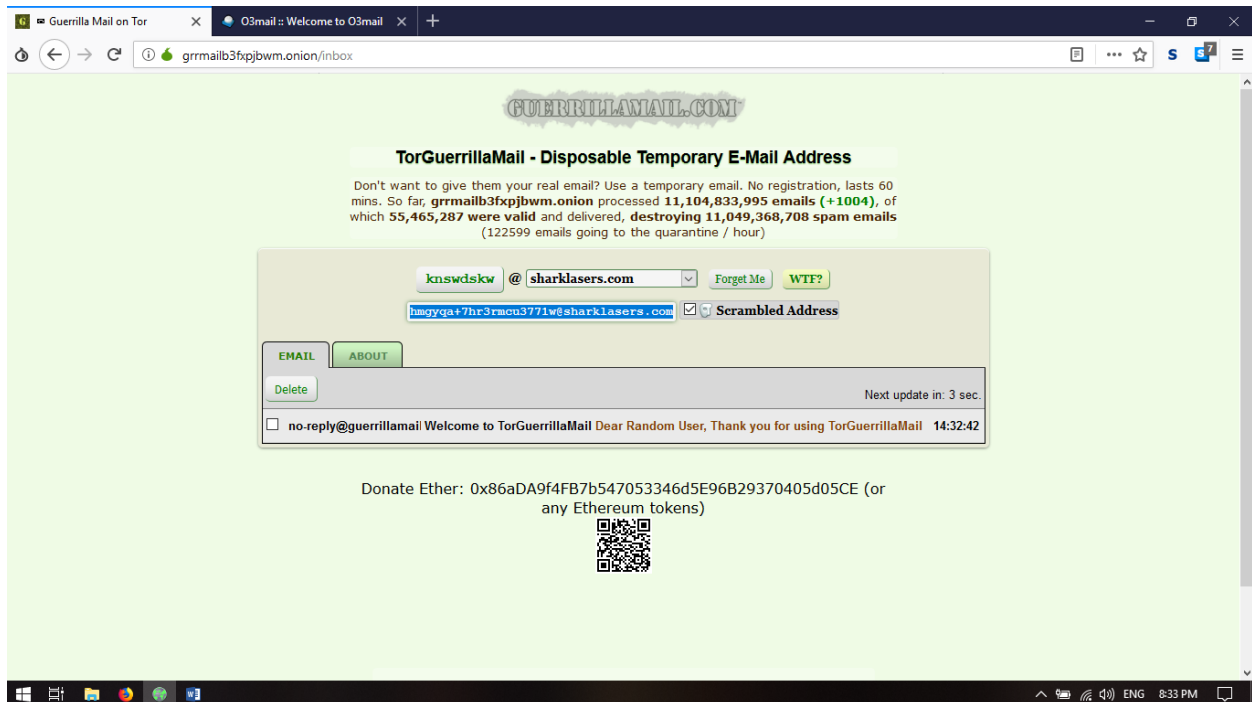
Specifications:
 Producer: RU Printer
 Delay: 5 days
 Quality: 100%

Price on market 3000\$

Email Services:

There are many email service provider in the onion network to provide people @onion email. Some of them are-

1. **ProtonMail** - (<https://protonirockerxow.onion/>)
2. **Adunanza OnionMail Server** - (<http://zrwxcayqc4jgggm.onion/>)
3. **Volatile** - (<http://vola7ileiax4ueow.onion/>)
4. **MSW (My Secrete World)** – (<http://mswmailgcjbye4sc.onion/>)
5. **Anonymous Says** - (<http://iwab42vsaitvzkf5.onion/>) [with 10 GB Disk Space, POP3, IMAP, SMTP access]
6. **Confidant Mail** – (<http://cwu7eglxcabwtzf.onion/>) [with 10 GB Disk Space, POP3, IMAP, SMTP access]
7. **TorGuerrillaMail** – (<http://grrmailb3fxpbwm.onion/>) [with 10 GB Disk Space, POP3, IMAP, SMTP access]



Torrent Service

TOR has a vast torrent websites. We can download/upload any torrent file like as surface web. All we need to have an onion mail id and the torrent file to upload or any torrent client to download torrent file.

Here given a list of Torrent Websites:

1. **The Pirates Bay** - (<http://uj3wazyk5u4hnvtk.onion/>)
2. **Rutor** - (<http://rutorc6mqdinc4cz.onion/>)
3. **TorrentGalaxy** - (<http://galaxy2gchufcb3z.onion/>)
4. **Anonymous Pirate** – (<http://smk4dw5cbxd6lttl.onion/>)
5. **NewsFileSearch.com** – (<http://wbyi72yt6itdcqd.onion/>)

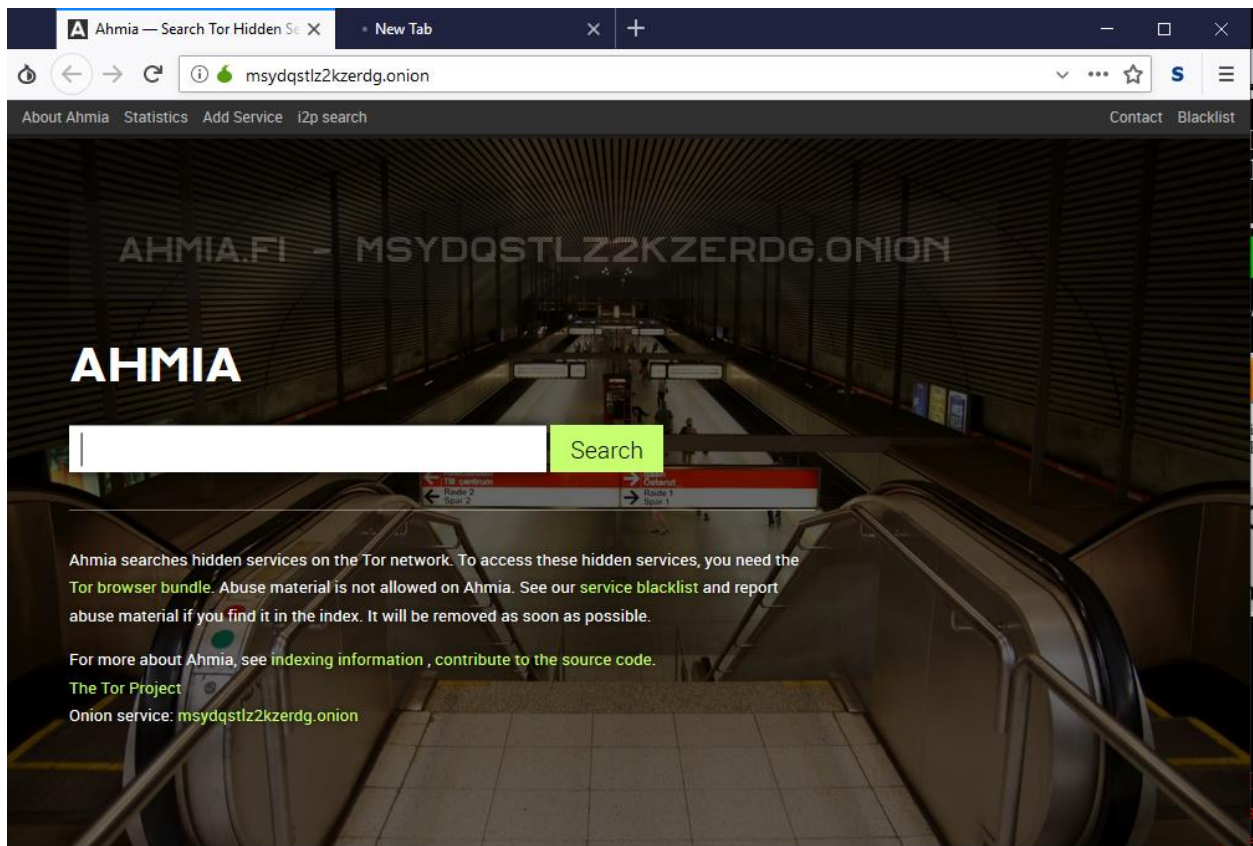
Tor Wiki:

There are some wiki available in both surface web and deep web contains many type of contents onion link. They can easily be found in search engines.

SEARCH ENGINE

There are many onion search engine to help people find their necessity. A list of few among them are –

1. DuckDuckgo - <https://3g2upl4pq6kufc4m.onion/>
2. NotEvil Tor Search engine - <http://hss3uro2hsxfogfq.onion/>
3. AHMIA - <http://msydstlz2kzerdg.onion>
4. Onionland Search engine - <http://3bbaaacczcbdddz.onion/>
5. Haystak - <http://haystakxad7wbk5.onion/>



The Hidden Wiki

The onion link is not too easy to remember. So there are wiki pages there are many onion link for different purpose. From their people can easily find many onion links and pages. It is easy to find any hidden wiki and from there all types of link can be found.

Security Concerns:

The network security experts suggest to cover up the web cam and the microphone of the laptop before open up the TOR browser. A VPN makes the guard node quite untraceable as the guard node has the real client's IP. Most of above the user must have to aware when they surf the deep or dark web as they contains miscellaneous types of content.

Conclusion

In this documentation we have tried to cover the whole TOR network into two parts. Firstly we explored about the TOR network, its history, its network type etc. In the latter part of this document we have explored the onion network. Here we have used some images and links which is given only for educational purpose. We have used several documents, webpages, wiki's to explore about this network.

--