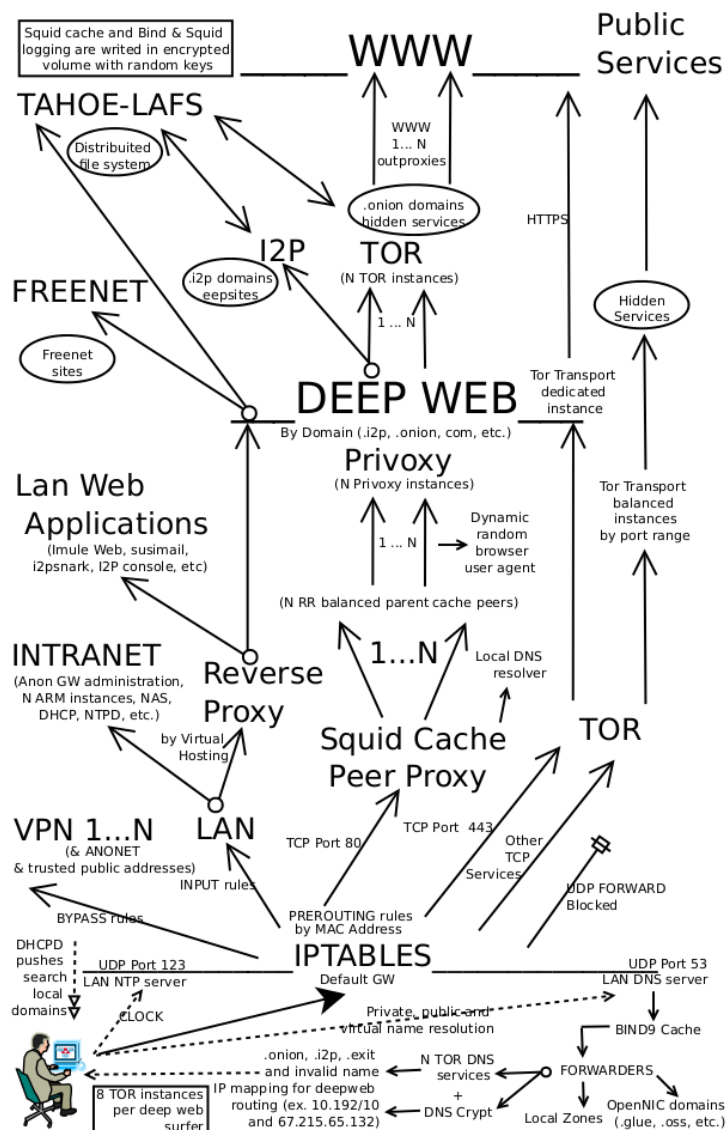


# Dark Web & Dark Market

- *Dark Web*
- *Open Source Intelligence OSINT and the Dark Web*
- *DeepDotWeb's DarkNet Dictionary Project*
- *Dark Net Markets Comparison Chart*

## Dark Web

Dark Web is actually the encrypted network that exists between Tor servers (or I2P servers) and their clients. If you want to access the Dark Web, you have to use certain anonymity tools and services.



Accessing tools:

## FreeLunch

FreeLunch.com®  
*Why Pay Anything?*

Moody's Analytics | Dismal Scientist

Email  Password

HOME FIND DATA VIEW MY BASKET HELP ABOUT FREELUNCH.COM

### Free Economic, Demographic & Financial Data

Finding and downloading economic data have never been this fast, simple or free!

Show me: ☒ FREE data only ☐ FREE & PREMIUM data

**A** Search for Economic Data

**B** Browse for Economic Data

**Consumer Markets**  
Auto Sales, Retail Sales

**Demographics**  
Households, Migration, Population

**Flow of Funds**  
Business, Households

**GDP**

**International Trade**  
Balance, Exports, Imports

**Labor markets**  
Employment, Unemployment

**Money, Credit & Interest rates**  
Consumer, Mortgage

**Prices**

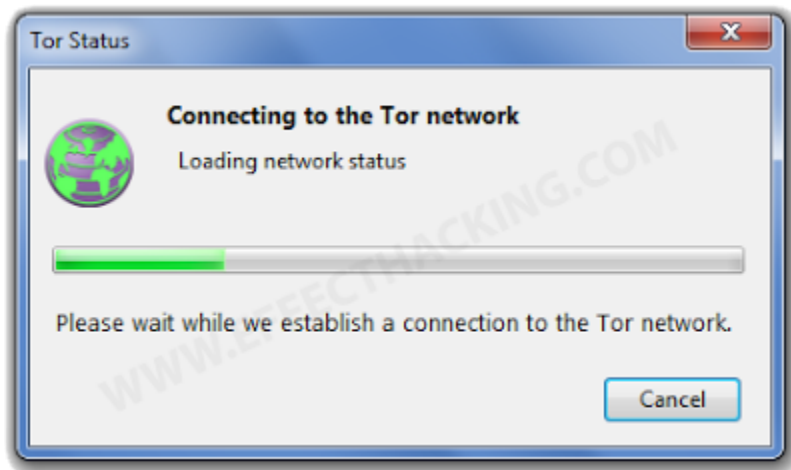
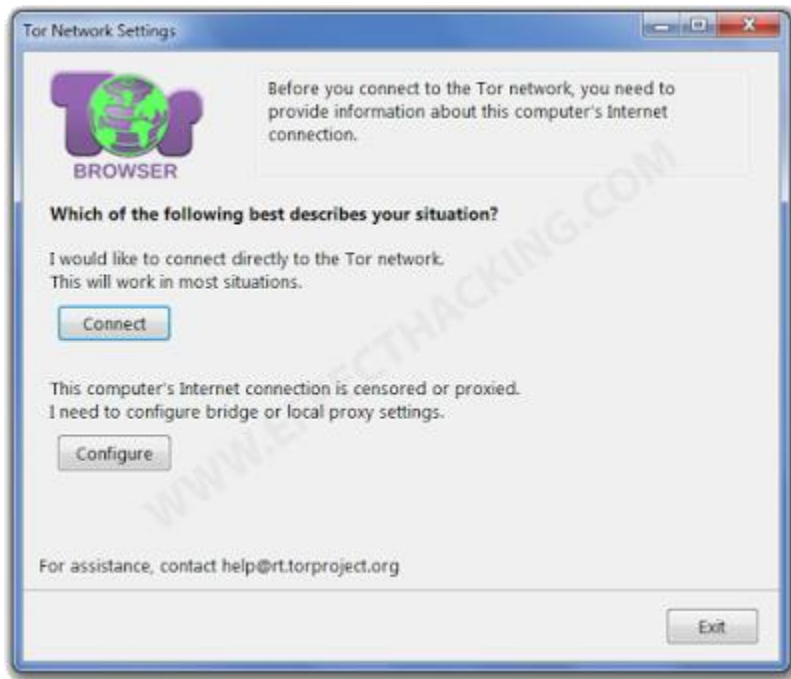
**Today's Top Downloads**

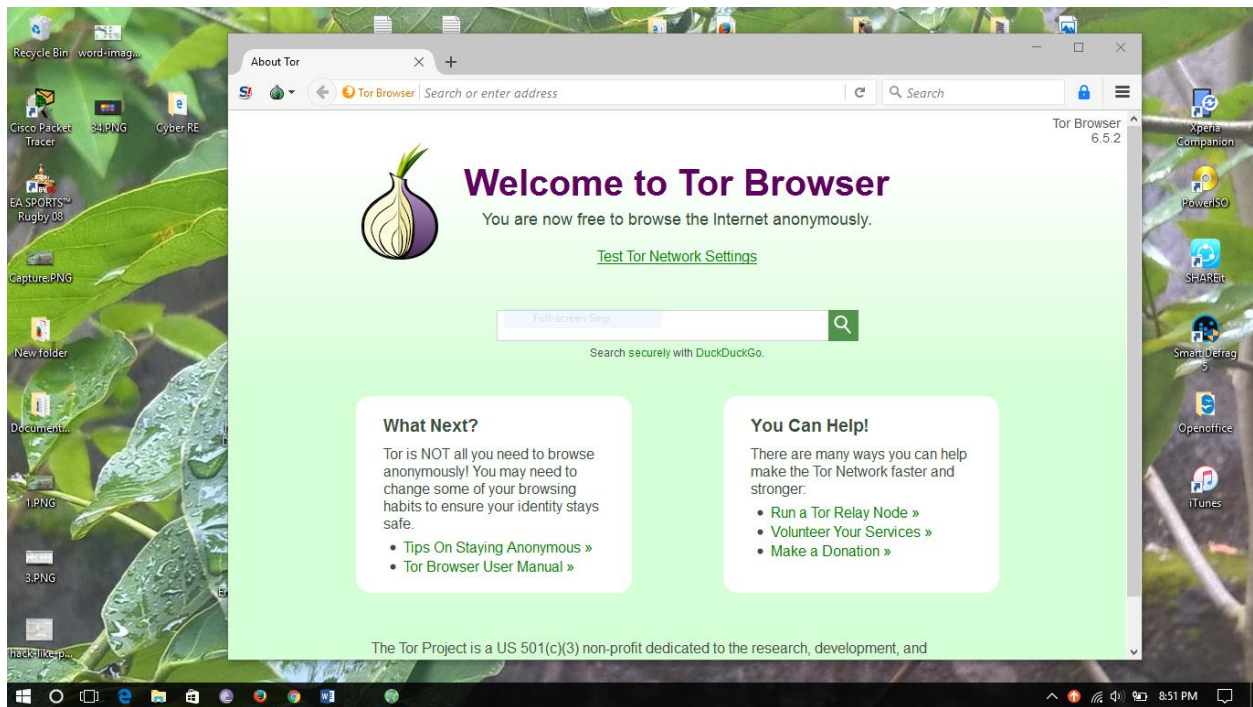
- Gross Domestic Product, (Bil. Ch. 2009 USD, SAAR) for United States
- Motor gasoline prices: Unleaded gasoline, (Cents per gal, NSA) for United States
- Personal Consumption Expenditures, (Bil. Ch. 2009 USD, SAAR) for United States
- CPI: Urban Consumer - All items, (Index 1982-84=100, SA) for United States
- Unemployment, (Ths. #, SA) for United States

**Today's Top Searches**

- GDP

## Tor Browser



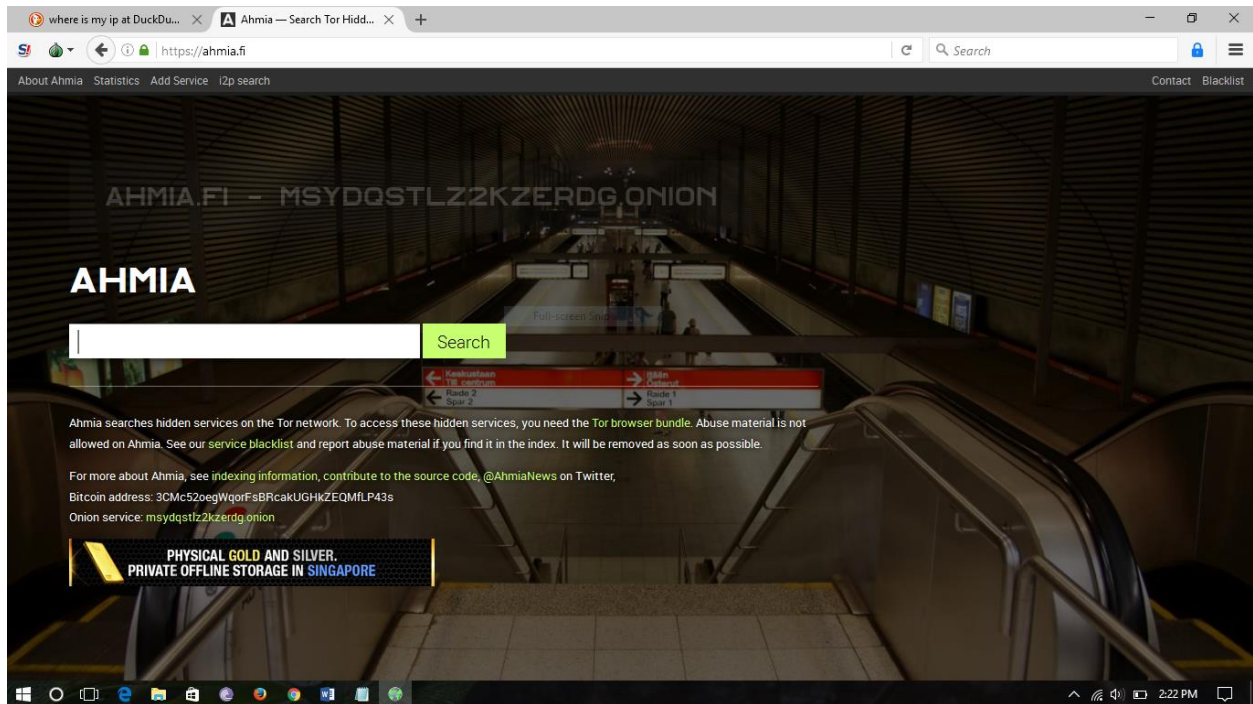


i2p



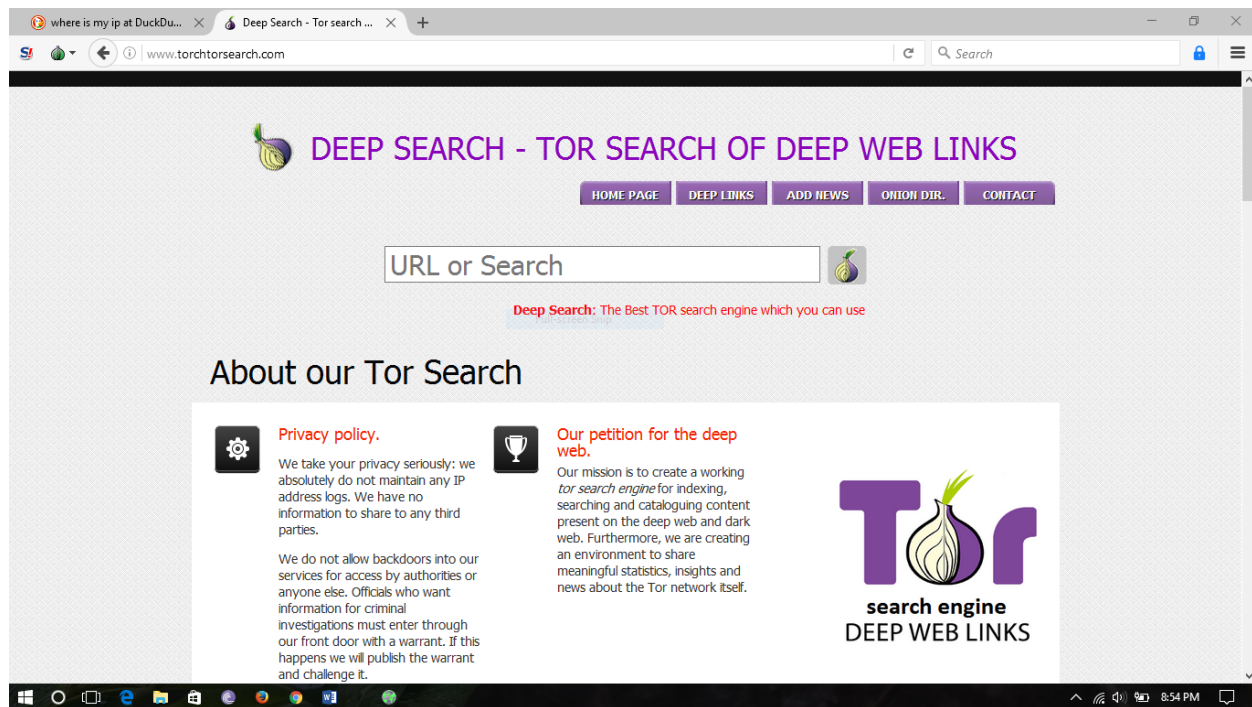
## Dark web search engines:

Ahmia.fi <https://ahmia.fi>

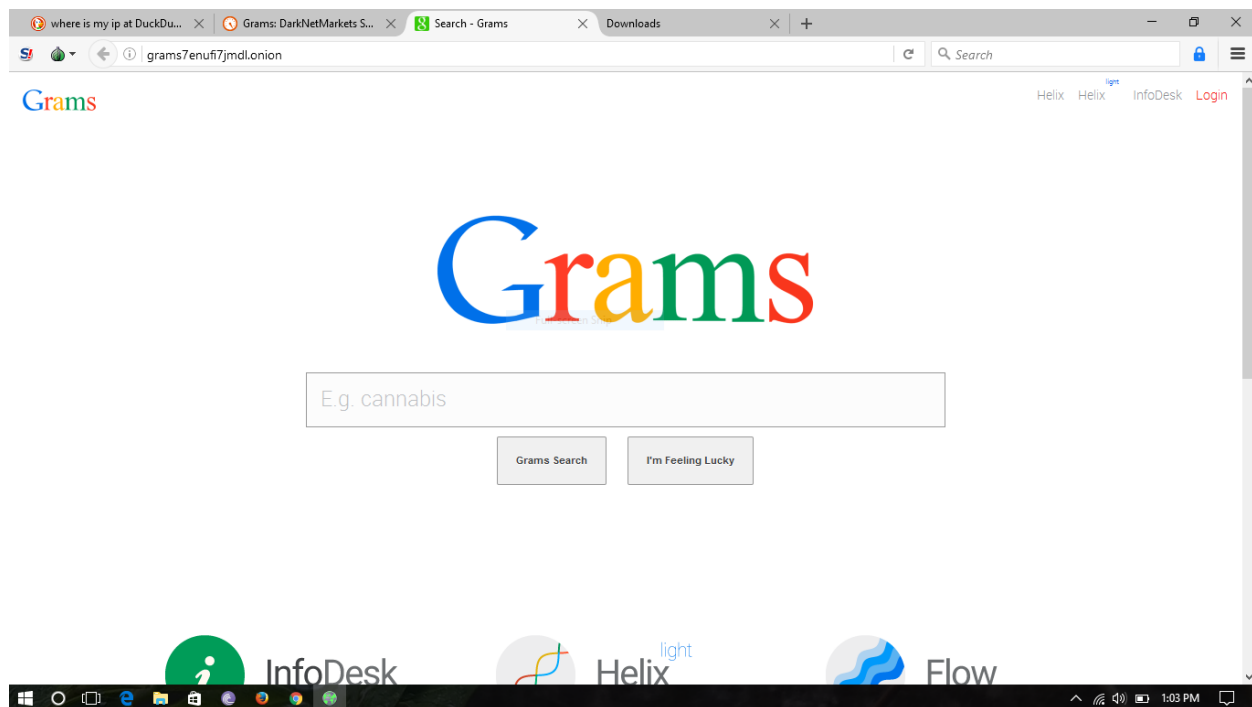


Tor engine <https://torchtorsearch.com>



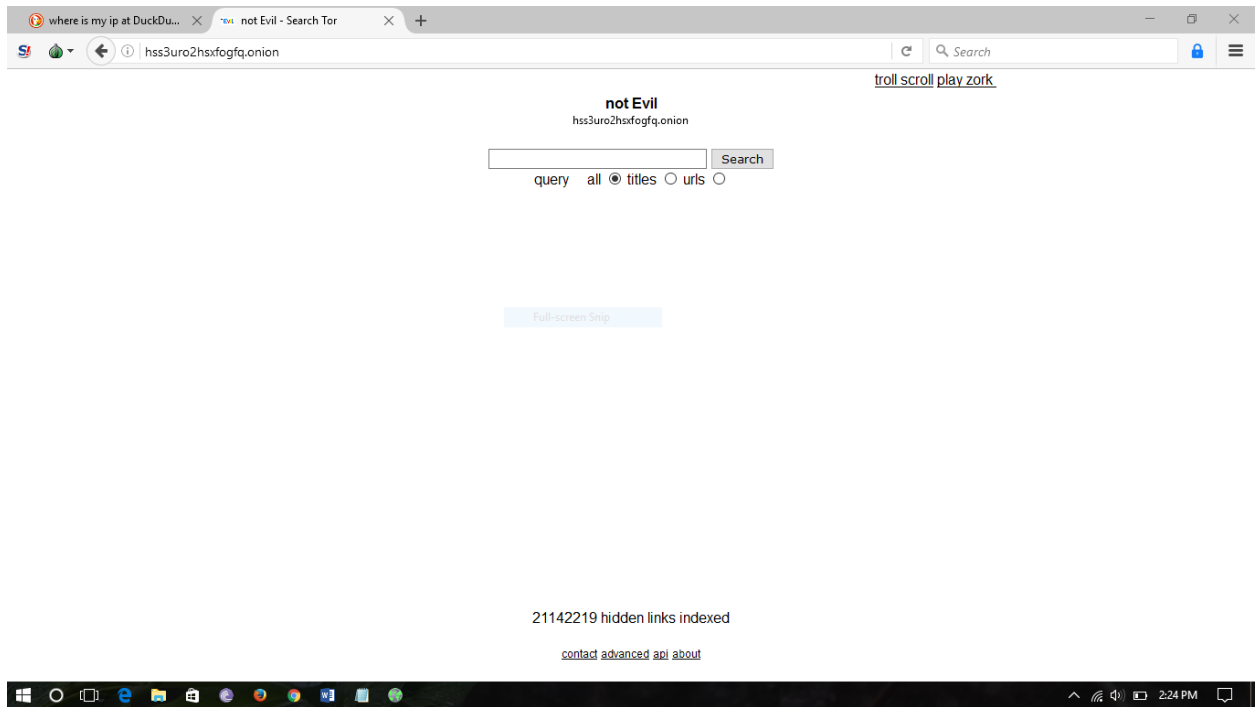


Grams <http://grams72tru2gdpl2.onion>



Not Evil <http://hss3uro2hsxfogfq.onion>





## Open Source Intelligence OSINT and the Dark Web

The dark web, the part of the deep web which is comprised of a number of darknets (e.g. Tor, Freenet, I2P...etc), provides individuals with an anonymous way to connect to the internet and publish information. Although this anonymous atmosphere is used to facilitate communications for legitimate purposes, it is also exploited for transforming information, services and goods for illegal purposes. Accordingly, Law Enforcement Agencies (LEAs) are interested in open source intelligence OSINT on many darknets, which would allow them to prosecute those involved in terrorist or criminal activities.

### What is Open Source Intelligence (OSINT)?

Open source intelligence OSINT represents intelligence derived from public sources. Across the intelligence community, “open” refers to public, or overt, sources, rather than private, or covert, sources. OSINT is not related by any means to public intelligence, or open source software.

OSINT depends on all forms of publicly available sources including:

- Media such as newspapers, radio, television....etc.
- Internet based communities such as social media sites, blogs, forums, video sharing sites...etc.
- Public documents including government official reports such as budgets, press conferences, demographics, contract awards...etc.
- Academic sources including papers, conferences, symposia...etc.
- Observations and reporting e.g. airplane spotters, UFO observers, radio monitors...etc.
- The deep web

### OSINT and the Challenges Faced By LEAs On the Dark Web:

LEAs around the world, including all major UK police forces, are currently investigating darknets, primarily Tor and I2P. The existence of other darknets is known and they are also considered to be of investigative interest, but, given their popularity, Tor and I2P (and Tor in particular) are believed to be used by the majority of dark web criminals, and therefore offer LEAs the best opportunities for investigating criminal activities on the dark web.

The main challenge faced by LEAs is the discovery of darknet nodes involved in illegal activities which would be of investigative interest to them. This is particularly challenging as darknet nodes are unreachable via regular search engines and existing dark web search engines are still far from supporting efficient searches. Once, though, a dark web node of interest has been discovered, the next major challenge is to identify the individual(s) involved in the illegal activities. Unlike ordinary websites however, dark web sites do not have an easily identifiable IP address, and the resolution of a Tor website, for example, firstly to an ISP and then to an individual becomes exponentially more difficult because of the complicated nature of data transfer across multiple nodes on Tor. To this end, LEAs have focused on the identification of the geographical location of such individuals. This has been successful

on the surface web where social posts are often geo-tagged (ranging from around 1.5 % on Twitter to around 20 % on Instagram and 50 % on Flickr, but on the dark web there are no social media that use geo-tagging and website owners do not normally advertise where they are located. Another method for geo-locating such individuals would be to examine the wording of their posts, biographies, or adverts. This has had limited success to date, as users on the dark web do not tend to give away such information, and any probing for further information by an investigator can end with them being “marked” as police.

The fact that geo-locating individuals engaging in criminal activities on the dark web is relatively problematic means that investigators have no way of initially knowing where a person is located, and invariably interact with a number of globally located criminals, before locating criminals that are domiciled within their own jurisdictions. Even though larger LEAs may be able to sustain a significant number of “false positives” before finding a vendor who is locally located, smaller LEAs may not, due to resourcing and budgetary constraints, and management may question the viability of continuing this type of work. To date, it is when an investigation moves from the digital world to the physical world, that most executive actions occur, e.g. during the delivery phase of an illegal commodity. This typically means that either a Covert Internet Investigator (CII) engages with an online criminal and coerces them to meet in real life, or that a criminal attempts to purchase some form of illegal commodity advertised by an LEA, and the LEA learns of a real shipping address that affords a surveillance opportunity. However, “de-confliction” appears to be a major issue for all LEAs, particularly in regard to dark web investigations as there is no central control mechanism in many countries for ensuring that “blue on blue” incidents do not occur.

Nevertheless, if an LEA was to take the step of advertising illegal items for sale in the hope of attracting criminals to their site, the investigators would have to have expert knowledge of non-generic or official names for certain items. For instance, Semtex has a chemical name that only people familiar with explosives would use, however people will search for the chemical name on darknets. As customers generally appear to search using very specific terminology, investigators would need to carefully “frame” specific items to attract the attention of the criminally minded. Online chatter between buyers and sellers is also commonplace and there is much negotiation on the price of the goods and/or shipping costs. Accordingly, good communication skills are undoubtedly required. Moreover, CIIs would need to ensure that their online presence looks realistic, e.g., by having a network of “friends” interacting with them. The dark web imposes major challenges for LEAs. Most OSINT investigators do not have a strong computer science/programming background and are largely self-taught when it comes to investigating darknets. This is a training issue that needs to be addressed, and LEAs may wish to start considering their recruitment policy for OSINT investigators, particularly with regard to the use of CIIs. To support them in such investigations, several technological solutions are currently being researched and developed, as discussed next.

## OSINT Techniques Used On The Dark Web By LEAs:

Discovering, collecting and monitoring information are the most significant processes for OSINT. Several different techniques (i.e., advanced search engine querying and crawling, social media mining and monitoring, restricted content access via cached results...etc.) are applied to surface web for retrieving content of interest from the intelligence perspective. On the other hand, the distinctive nature of the dark web, which requires special technical configuration for accessing it, while it also differentiates the way the network traffic is propagated for the sake of anonymity, dictates that the traditional OSINT techniques should be adapted to the rules, which govern the dark web.

### Search Engines:

As a result of the restricted nature of the dark web, requiring special software and/or configuration for being accessed, as well as of the volatility of the websites hosted in darknets (i.e. most websites in the dark web are hosted on machines that do not maintain a 24/7 uptime), conventional search engines do not index the content of the dark web. Nevertheless, a small number of search engines for the dark web exists, as well as directory listings with popular dark websites. The most stable and reliable such search tools are provided for Tor. Specifically, the most popular Tor search engine is DuckDuckGo (accessible both via a normal and an onion URL) emphasizing user privacy by avoiding tracking and profiling its users. DuckDuckGo may return results hosted in Tor onion sites, as well as results on the surface web based on partnerships with other search engines, such as Yahoo! and Bing.

On the other hand, Ahmia (accessible both via a normal and an onion URL) is a search engine returning only Tor-related results (after filtering out child pornography sites), and as of April 2016, it started indexing more than 5000 onion Web sites. Furthermore, Torch is also available only through its onion URL for retrieving results from Tor. Finally, several censorship-resistant directory listings, known as hidden wikis (e.g. The Hidden Wiki, Tor Links), containing lists of popular onion URLs are available and provide the user with an entry point to the world of Tor onion sites.

### Traffic Analysis and de-Anonymization of Users of the Dark Web:

The anonymity and the communication privacy provided on the dark web constitute the most significant incentive for attracting users wishing to hide their identity not only for avoiding government tracking and corporate profiling, but also for executing criminal activities. It is really important for LEAs to monitor the network traffic related to criminal activities, and to identify the actual perpetrators of these cybercrimes. Therefore LEAs are greatly interested in exploiting techniques which will allow them to determine with high degree of accuracy the identity of dark web users participating in criminal activities.

The de-anonymization of dark web users is accomplished either by exploiting the unique characteristics of every darknet, or based on data gathered through network traffic analysis of the communication taking place within such a darknet. In the former case, the de-anonymization process attempts to take advantage of potential weak points found across a darknet, whereas in the latter, the data collected is cross-referenced so as to identify the anonymous data source. As no existing darknet can guarantee perfect anonymity, several types of “attacks” have been proposed in the literature for de-anonymizing dark web users (especially Tor users) after taking advantage of vulnerabilities either existing inherently within the anonymity networks and the protocols used, or being caused by the user behavior. One of

the early research studies shows that information leakage and user de-anonymization in Tor is possible to occur either due to the intrinsic design of the http protocol or due to user behavior (i.e. users not following the Tor community instructions closely). A recent study proved that https is the best countermeasure for preventing de-anonymization for http over Tor.

Furthermore, another work proposes a collection of non-detectable attacks on Tor network based on the throughput of an anonymous data flow. It presents attacks for identifying Tor relays participating in a connection, while it also shows that the relationship between two flows of data can be uncovered by simply observing their throughput. Recent research efforts have also developed attacks for identifying the originator of a content message after taking advantage of Freenet design decisions. The proposed methodology requires deploying a number of monitoring nodes in Freenet for observing messages passing through the nodes. The main objective is to determine all the nodes having seen a specific message sent and identify the originating machine of the message when certain conditions are met. Moreover, a survey paper that discusses well-studied potential attacks on anonymity networks, which may compromise user identities, presents several mechanisms against user anonymity, either application-based, such as plug-ins able to bypass proxy settings, targeted DNS lookups, URI methods, code injection, and software vulnerabilities, or network-based, such as intersection, timing, fingerprinting, or congestion attacks. The effectiveness of these attacks was examined, by also considering the resources they require, and an estimate is provided in each case on whether it is plausible for each attack to be successful against modern anonymous networks with limited success.

## DeepDotWeb's DarkNet Dictionary Project

3DD – 3 Day delivery.

420 – From wikipedia: is a code-term used primarily in North America that refers to the consumption of cannabis and by extension, as a way to identify oneself with cannabis subculture or simply cannabis itself. Observances based on the number 420 include smoking cannabis around the time 4:20 p.m. (with some sources also indicating 4:20 a.m)

4/20 – 20th of april sale – also known as the special sale when the vendor Tony76 executed the most famous Scam on Silk road.

Administrator – In charge of a collection of services a year or two ago, including TorStatusNet, Hidden Image Board, a hosting service.

Altcoin – Any digital cryptocurrency other than Bitcoin, altcoin – any digital cryptocurrency other than Bitcoin.

Anonymity – This thing you want to have if you dont want to be found while using dark net markets.

AnonFiles – File upload site. You want to send a PDF/image/whatever to another user? Upload it to anonfiles, then you can share your custom link, and whoever you send it to can download your file anonymously.

Astrid – Creator and Moderator of /r/DarkNetMarkets, very promiscuous has had relations with all Moderators there, also is the CSS guru!

Avengers – A group of individuals who are well known for ordering LSD from many vendors back in the day of Silk Road 1.0, reagent testing it, consuming it, a writing reviews about the quality of the products. They currently can be found on the deep web on the Majestic Garden forum.

AYB – All You're Base, general Onionland portal

AYW – THW without the CP. Known formally as All You're Wiki. Most people use it now.

Backopy – The Administrator of Black Market Reloaded (BMR)

Bergie Web – The level of the internet hierarchy that comes between the “surface” and the “deep web,” if you are comparing the internet to an ocean. This includes porn, chans, and other sites that provide you with information on how to access the deep web. Peer-to-peer file sharing networks are also part of this level.

Bitcoinfog – “Wash” your bitcoins. Bitcoins can be traced, so let's say you received bitcoins from an illegal activity, those coins can be traced back to you if you use them on another website that is linked to your real identity (localbitcoins, paypal, bitstamp, MtGox etc). This handy website will erase all traces on your coins. the service is accessible here: <http://fogcore5n3ov3tui.onion>

Bitcoins – an open source, peer-to-peer payment network and pseudo-anonymous digital currency being used for almost all transaction on the darknet.

Black Market Reloaded – Also known as BMR, the oldest dark net market since Silk Road was shut down, the site is currently offline and planned to be back with a newer version.

Blockchain – Wikipedia Definition: A block chain is a transaction database shared by all nodes participating in a system based on the Bitcoin protocol

BotDW – Boss of the Deep Web

Buyers – Markplace user that is not a vendor. (duh)

Carding – The practice of stealing and selling credit card information

CD (Controlled Delivery) – The technique of controlled delivery is used when a consignment of illicit drugs is detected and allowed to go forward under the control and surveillance of law enforcement officers in order to secure evidence against the organizers of such illicit drug traffic.

Cirrus – A silk road forum moderator.

Chisquare/psi – Hugest faggot, avoid him more. Hosts numerous services. (Its not us who said this!)

Cipherspace – tor hidden services / i2p / freenet / any other anonymity network

Cold Storage – a secure offline wallet for your Bitcoins or other cryptocurrencies

CP – When mentioned in the context of the deep web – it usually mean Child pornography, something you should know and avoid at all cost when browsing around.

Cleartnet – regular internet (non TOR)

Cryptography – All the means of hiding and encrypting the data that you send over the internet.

Crypto News – (<http://wittvywowuxp35s6.onion>) is a hidden service for news about privacy, security, politics and technology. The owner only updates sporadically and focuses a lot on I2P.

Dark Net – A general term that describes the hidden websites hosted on the TOR / I2P and other networks that you cannot access with regular internet connection without using some special software or get crawled by Google and other search engines. more info can be found here

Dark Nexus – HTTP Refresh Chat

DarkNetMarkets – A sub Reddit meant for the discussion of the various Dark Net markets, can be found at this link.

DDOS Attack – Denial-of-service attack Form of an attack that is an attempt to make a machine or network resource unavailable to its intended users, was common on Silk road, some say it was used to locate the server location using a know tor vulnerability. Read the Wikipedia page for the technical explanation



DBAN – Darik’s Boot and Nuke software for wiping your harddrive from all information.

Deep Web – Synonymous with “Dark Net”.

DeepDotWeb – Us! The site where this list was created, can be found here:  
<http://www.deepdotweb.com> A Blog focusing on deepweb news.

Defcon – The alias of Silk Road 2.0 Admin. A person named Blake Benthall who was arrested During Operation Onymous is alleged to be him.

Dispute – In our context, this term is usually used to describe a disagreement between a buyer and a seller on the markets.

Digitalink – a/k/a Jacob Theodore George IV, according to Homeland Security Investigations (HSI) Digitalink was the first vendor on Silk Road selling illegal drugs to be arrested.

DoD / Coachella / HH (and some others) – A Well known scammer & troll, was eventually doxxed on some article and was not seen much since.

Domestic – A term that refers to making an order from a vendor who resides on the same country as the buyer.

Donations – You will encounter many requests for them on the darknet markets, will usually list a bitcoin address.

Doxx – The act of posting in a public forum the personally identifying information of a pseudonym used by an individual or the information posted therein.

Dread Pirate Roberts – The pseudonym used by the administrator of the original Silk Road market. It has been speculated that more than one person may have been using this pseudonym, but “Ross William Ulbricht” has been indicted by the FBI as being the sole owner.

DDG/Duck Duck Go – A search engine that respects privacy.

Emergency BTC Address — An address to be held on record to send all funds to in case of a market shutdown. This would ideally be a cold storage address with no information that could be used to connect the owner to their identity. This address would only be checked after a market was shut down in order to recover outstanding funds.

Encryption — Using secret information to make it infeasible without knowledge of said information to decipher the ‘cypher-text’ produced into a plain text message. This can take one of two forms, symmetric encryption which used a shared secret that both parties must know in advance, or public key cryptography where the information to encrypt the information differs from the secret needed to decrypt the information.

Escrow – the use of a neutral third party to ensure that a transaction payment will be made to a seller on completion of items sent to a buyer. Generally after a purchase is made, the funds are held ‘in escrow’ to be released when the buyer states the seller has met the terms of the purchase. Generally the third party will also offer arbitration in case of a dispute between the two parties.

Electrum plugin – Used on The Marketplace to create multi signature transactions with a click of a button – full usage instructions can be found in this tutorial.

Exit Scam – A term used to describe a situation where a market admin or a vendor wants to retire, and is doing so while taking as much money as possible from their users / buyers.

Vendors: usually by offering some great deal and abusing the reputation they gained so far by requiring people to not use the escrow protection and collecting as much money as possible (without sending out anything) before shutting down the store and running with as much BTC as they can.

Market admins: usually locking users funds on the market, just to shut it down completely soon after.

Fagmin/dgft – New Admin Of Torchan

FBI – the Federal Bureau of Investigation. This is the USA's state-wide police who prosecute violations of federal laws. They do not involve themselves in violations of state law.

FE -Finalize early. This is the release of escrow funds before the seller knows that the conditions of the contract have been met. This is used to reduce seller risk from BTC price fluxuation, and against market shutdown. This is also used to scam buyers as after the escrow has been released there is no recourse for the buyer if the seller does not deliver on their promises.

Feedback — a message left from a seller to the vendor, or vice versa, about how well a transactions went. It is considered good form to not reveal any information about the methods the seller used to ship the order nor the vendor's or seller's location or details. This is made publicly available to allow users of a site to determine if they should trust the vendor or seller

Flush (Curtis Green) — An individual the FBI accuses Dread Pirate Roberts of ordering to be murdered. This person is also accused of being 'Chronicpain' from the Silk Road Forums, and an employee of Silk Road. The details of the allegations can be read – [Here](#), [here](#) & [This](#) is a great resource.

Freedom Hosting – Huge free web provider. Some of its services hosted child porn. Busted by the feds around the same time SR was busted. SR also was hosted on it for a while before it switched to a dedi server.

Freenet – a peer-to-peer platform for censorship-resistant communication.

FUD – Fear, Uncertainty and Doubt

Galaxy Deep Web Social Network – (<http://hbjw7wjeoltskhol.onion/>) is the currently most active dark net chat, a great place to keep in touch with friends and vendors, share the newest FUD and fuck up your OPSEC while waiting for your order to be shipped.

Gawker — an online blog that reports on web trends. Notable for being one of the first major sites to report on the existence of the Silk Road on 2011-06-01 at <http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160>

GCHQ – British Government Communications Headquarters, equivalent to the NSA in the United States.

Grams – Cross Marketplace search engine for the DeepWeb (see the sidebar link here)

HackBB – Famous hacking phpBB board, also hosted downloads for files like zeuS.

Harry71 – Onion Spider Robot (<http://skunksworke2cg.onion/>) is a daily updated extensive list of Onion sites. The owner runs a crawler that checks if the sites are up, fetches the link and title and dumps it on his homepage. The site also contains some statistics about uptime and hosts.

Hidden Service – Another term for a .onion domain name. It can only be accessed through the Tor network, and cannot be seized by a government.

Honeypot – A hidden service or other website setup by law enforcement in attempt to attract and trap people who participate in illegal activities. Other cited uses include helping the military and government protect their secrets and the FBI defending large businesses.

Hushmail – An email provider that focuses on privacy and used industry standard protocols PGP and 256-bit AES encryption. It claims to be secure to the extent that not even company employees can read the contents your emails. Hushmail is known to cooperate with law enforcement by handing over encrypted emails.

Hidden Wiki – a ‘hidden service’ website on the Tor anonymous network that allows for open editing of subjects related to hidden services and activity in them. “You will never find a more wretched hive of scum and villainy. We must be cautious.”

Hub Forums – An Onion based platform for cross marketplace discussion, like DNM sub reddit, but forum based and fully anonymous – read the details here.

I2P — The ‘Invisible Internet Project’. Originally designed as a way to be able to use IRC anonymously, it has become one of the more popular anonymous networks. While similar to Tor, key differences include the fact that I2P focuses on gaining access to sites within the network, and not to the Internet at large. Not as much academic research has been done on this project as Tor. This service is very popular in Russia. About half the routers appear to be located there. Details can be found at <https://geti2p.net>

International – Outside of one’s own country. Some avoid international transactions because customs adds time and risk to an order. Some countries such as Australia are known for having customs that are extremely hard to get an order past.

ISP – Internet service provider.

IRC – Internet Relay Chat. A communication system allowing easy transfer of messages in the form of text. It is intended for group discussion in sessions called channels.

JB – See hard candy, except for teens.

Lavabit – A defunct email provider that shut down in August 2013 after being forced to hand over its SSL private keys to the US government.

LE / LEO’s / LEA’s – Law Enforcement / Law Enforcement Officers / Law Enforcement Agents

Library – Usually refers to Tor Library, the largest centralized eBook service on the Darknet.

Libertas — Pseudonym used by one of the original Silk Road forum administrators, and also used by one of the administrators of Silk Road 2. Arrest by the 'Garda Siochana' (Irish police). Details of the arrest may be found at this link.

Liberte – Another Linux distribution similar to TAILS and Whonix with the purpose of enabling anyone to communicate safely and covertly in hostile environments.

Litecoins — an alternative cryptocurrency, similar to bitcoin. The key difference is that while bitcoin uses hashcash-SHA256<sup>2</sup> at the 'proof of work', litecoin uses hashcash-Scrypt which is designed to use more memory and be less subject to custom hardware designed to solve the problem quickly. More details of this difference may be found at: <https://en.bitcoin.it/wiki/Hashcash>

LocalBitcoins — a site designed to allow over the counter trading of bitcoins. Famed for its anonymous nature people who sell on the site have been under constant pressure to avoid being prosecuted as unlicensed money traders. This extra risk and the extra work generally cause a significant price difference between the site and a more open (and regulated) exchange.

Love Letter – An official confiscation notice from the postal service sent to the recipient letting him know that his parcel was seized. In some cases, vendors sent fake love letters to create the false impression of a seized package and scam the buyer.

Lucyskyhigher – Reddit mod sexiest biotch on the always informative and largely humorous gathering place for all darknetmarkets, /r/Darknetmarkets

Marco Polo Task Force – A multi law enforcement agency task force based in Baltimore put together to investigate to investigate Silk Road and eventually included investigators from the FBI, DEA, DHS, the IRS, U.S. Postal Inspection, U.S. Secret Service, and the Bureau of Alcohol, Tobacco, Firearms and Explosives

Mariana's Web – Urban legend of a secret website in the deepweb.

Marketplaces – catch all term for web sites set up to allow trade between vendors and buyers. When used in the context of sale of illegal goods, these usually provide anonymity to the buyer and seller, a method of escrow to ensure to reduce risk from new vendors and sellers, and a method of advertising goods to be sold at a price so that a purchase may be initiated and paid for without involvement of the seller. Most markets are also set up as 'hidden services' under anonymity networks like tor, i2p, or freenet, although there do exist some 'clearnet' markets that operate over standard HTTP/HTTPS.

Mixie – First major service operator on Tor in 2007. Services include a basic message board on the home page, a PM service, a "create your own bbs-like board" system (anyone could create a community for free) called SnapBBS, and a few more features. Also hosted an OnionNet IRC server.

Molly – any damned thing you can shove into a gelcap and get somebody to buy. In theory, this is supposed to be MDMA in the gelcap, but more commonly you get something like methylone, BZP, a benzofuran, talc, or something potentially toxic like PMA. Test first before consuming, <http://dancesafe.org/health-and-safety/adulterant-screening-kit-instructions> is a good resource.

Monero – a newer more privacy focused cryptocurrency that's being accepted by some darknet markets.

MSM – Main Stream Media — Big news outlets designed for common consumption by the masses. These can range from more neutral sites like the BBC in the UK, Al Jazeera in the middle east, or The New York Times in the USA, to sites like the Daily Fail, Fox News, or Pravda which are not as known for being well vetting their news articles.

MtGox – Magic: The Gathering Online exchange. One of the first public exchanges for bitcoins to currencies such as USD. Because it was designed in haste, it has been plagued with issues of security. Widely considered to be completely insolvent, a lack of transparency has allowed constant rumour to circulate. They are no longer taking exchanges after claiming to be defrauded by outside parties taking advantages of quirks in the bitcoin protocol.

Multi Signature Escrow – Where an address is signed by both the buyer and the seller with their private keys. The buyer will send funds to the address and the seller ships the product. If both parties are happy they sign off on the address and release the funds in escrow, You can see example for such open source service [here](#).

Nameless – IRC server hosted by chi. No identities, all usernames randomly generated.

Nekro – Huge faggot, avoid him. (he said this, not us!)

MTLjohn – Was a funny Scammer on SR1 , kept popping again and again under different identities just to be exposed each by another vendor (LuckyLuciano) since he was so easy to provoke.

NDD – Next day delivery.

Onion – a hidden website using the Tor network. Name comes from the 'onion routing' used by tor. The url is composed of a hash of information used to identify the correct system, so most addresses are somewhat random. While creating an onion is easy, and the routing itself has few known weaknesses, securing such a site to leak no information is exceptionally difficult.

Onion Browser — A web browser like the Tor Browser Bundle (TBB). A web browser designed to work with the tor network to browse hidden services and normal websites anonymously, without leaking user information. While easier to use properly without leaking information, bugs in a browser can cause serious problems, such as the javascript bug that was used in part to shut down Freedom Hosting.

OnionForum – The original forum for Tor created by Legith in the early days of '05.

Onionland – A general term to describe tor hidden services

OnionNet – First real IRC network designed for Onionland. All IRC ops are pedophiles though. Long history but not many people use it anymore.

Onion Routing – A technique for anonymous communication over a computer network. Messages are repeatedly encrypted and send through multiple network nodes. The process is comparable to peeling an onion, each node removes a layer of encryption uncovering routing instructions for the following layer.

Onion patch – A saying for using the dnms on /r/drugs.

opDarknet – Campaign launched by Anonymous a couple years ago. Targeted child porn sites as well as Freedom Hosting.

Operation Onymous – A global crackdown on the darknet markets during November 2014, in which many sites were seized and several people arrested.

Optimus Crime/OC – Admin of HackBB.

OPSEC – Operation Security. The process of protecting little pieces of data that could be grouped together to form a bigger picture, or expose your identity.

OrBot – a mobile version of the tor router for Android. Can be found on the Google Play store. Designed to either work with it's own browser, or can be set up to work as proxy for any system that supports it. Can also be used on a rooted device to provide a transparent proxy that will force all apps to use tor for connecting.

OS – Operating system.

Pastebin – A website used to store text for a certain period of time. It is popular on the deep web because it is an easy way to anonymously share information.

Parallel construction – Parallel construction is a law enforcement process of building a parallel – or separate – evidentiary basis for a criminal investigation in order to conceal how the investigation began.

PGP/GPG – Pretty Good Privacy/ Gnu Privacy Guard. PGP was introduced in 1991, and was formalized with RFC 2440 and RFC 4880. Uses a combination of public-key and symmetric-key cryptography to ensure that messages can be delivered without a third party gaining access to the contents of the message. It also allows for a message to be signed so that the author of the message is indisputable. Many different algorithms can be used for the encryption, but the most commonly used methods are RSA for the public key crypto, and AES for the symmetric cypher. It is extremely important that the public key of any party be fully verified in order to know that the message is being delivered to the correct recipient or is from the correct sender. Here we have a simple usage guide for windows.

P2P Escrow – Most commonly used to refer transactions using 'P2SH' addresses as defined by BIP 016. A public key is provided by a seller, market, and vendor, and used to create an address which requires two of the three parties to sign in order to redeem. The buyer then pays to this address. Of extreme importance is the 'redeemScript' which details the information needed to redeem funds sent to the address, which is a hash of the redeemScript. The goal of this method is that no one party has enough information to take funds from these P2SH addresses. Even if the market is hacked or taken down, the funds cannot be seized, and a buyer and seller can, with the redeemsript, finalize a transaction outside of the market's involvement if they choose to.

Phishing – the act of using social engineering techniques to get private information such as user names and passwords. An example would be to send out a message claiming to be from an administrator asking for a password, or setting up a fraudulent website that looks to be well know market's site in order to gain user name and password information.

**Pidgin OTR** – Secured instant messaging software Pidgin is a free and open source client that lets you organize and manage your different Instant Messaging (IM) accounts using a single interface. The Off-the-Record (OTR) plug-in designed for use with Pidgin ensures authenticated and secure communications between Pidgin users.

**PIN Code** – Personal Identification Number Code. Uses as a secondary validation method to protect against loss of funds if the username and password are discovered. Generally it is only asked for during transfer of funds to outside the market or to confirm and finalize orders.

**PM / DM** – Personal message/ DM: Direct message.

**Processing Time** – time required by a market or vendor in order to complete a transaction. Generally this involves waiting for sufficient confirmations on the blockchain to ensure a deposit has been met, or to run funds through a bitcoin mixer on the market. Also used to for time required by a vendor once getting a transaction to put the goods into the post.

**Project Black Flag** – Market set up shortly after the fall of the original Silk Road. Widely suspected to be a scam, this was confirmed to be the case after a short period of time.

**Proxy** – Unlike a VPN, a proxy is a service that only changes the IP address websites can see within your web browser, rather than on all applications on your computer.

**RAT (Remote Administration Tool)** – A piece of software that allows a remote operator to control a system as if he has physical access to that system.

**RC (Research chemicals)** – From wikipedia, Research Chemical are chemical substances used by scientists for medical and scientific research purposes. One characteristic of a research chemical is that it is for laboratory research use only. A research chemical is not intended for human or veterinary use.

**Resolution** – Used when there is a dispute between a buyer and seller. This usually involves whatever market used to serve as an arbitrator to determine how funds are to be released from escrow.

**Reviews** – the corpus of feedbacks left on a site, along with more information information gained by outside channels. Used by buyers to determine if they should take a vendor or buyer as legitimate.

**Riseup / Safe-mail** – Excellent e-mail services.

**Ross Ulbricht** — Accused of the FBI of being the sole owner of the pseudonym ‘Dread Pirate Roberts’ and creator of the Silk Road. He was an Eagle Scout and in a known libertarian. The original Silk Road website went down after his arrest.

**Shadow Web** – A mythical part of the dark web that’s been perpetuated by creepypastas. Supposedly allows you to access an even darker network containing red rooms and cannibalism forums.

**Same Same But Different (SSBD)** – Peter Phillip Nash, Was arrested and accused in Australia for being on the Silk Road moderators You can read the full details about the moderators bust in this post.

**Samples** – In the context of a market, a free or low cost item sent to a well known buyer in order to establish legitimacy. This proves that at least the seller has access to a product and is capable of delivering it in as secure way. The receiving party is expected to leave public feedback regarding the quality of the products and how well it’s been packaged.



Satoshi Nakamoto – A pseudonym of the person or group of people who created Bitcoin and anonymously published its source code.

Shared Send – A free method to tumble Bitcoins provided by [blockchain.info](http://blockchain.info). It routes transactions through a shared wallet breaking the chain of transactions.

Scammer – One who would attempt to defraud either a vendor or seller. For a vendor this can take the form of simply not ever sending products, sending poor quality or misrepresented products, or ‘selective scamming’ (See other entry).

Selective Scamming– Where known individuals are sent product but large transactions or those from unknowns are not sent out. For a seller, this will mean that they claim to have not received goods that were delivered or that the goods were of poor quality/misrepresented.

Search (ability you must have) = <http://lmgty.com/?q=search>

Sheep – Second big online market to fail. Vendors flocked to the site citing its well polished vending design, and users followed. Disappeared without a trace taking all funds in escrow with it. Despite the manhunt that followed, it remains unclear if it was a deliberate scam, a result of being hacked, or a combination of the two.

Shipping – Process of a vendor packaging and sending goods. A source of extreme difficulty for vendors, and how many have been caught. Ideal methods will appear to be legitimate business to individual packages and correspondence. It is considered poor form to disclose any specifics of a shipment made, as it could be used to target a vendor.

Shilling – Creating accounts on Reddit / Forums for the sole intention of posting Positive / Negative post about someone or something while trying to make them look authentic.

Silk Road – ‘The ebay of illegal goods’. First reported to a wide audience by Gawker 2011-06-01, it flourished due to a large vendor and user base, and strict controls to weed out scammers. Taken down after the arrest of Ross Ulbricht at the start of October, 2013. While it was not the first nor the last market for illegal items, none have matched its popularity and trust level given by vendors and users.

SIGINT – Tor-based darknet email service that allows you to send email without revealing your location or identity. Its name is derived from SIGINT (“Signals Intelligence”), which refers to intelligence-gathering by interception of signals.

Silk Road 2.0 – The successor of the first Silk Road. Was seized during Operation Onymous, and Blake Benthall the alleged admin of the site (Defcon) was arrested.

SMAC – a tool that can change your MAC address

SMS4Tor – Self-destructing messages. Similar to Privnote but for Tor. I prefer this because it’s an onion address AND does not require javascript (Privnote requires JS). You type out a message on their site, create a custom link, and share it to another user. The link will only work once, and so whoever opens it first is the only one who can read it. A great alternative to PGP as it is much more user-friendly. Very

secure when combined with PGP encryption. \*This one's a little harder to find but if you google "self destruct message tor" you should be able to find it.

Stats (Buyer) – statistics used to determine legitimacy of buyers/sellers. Common are number of successful transactions, average reviews, and dollar amounts of successful transactions in total. These are usually imprecise in order to avoid anybody being profiled.

Stealth – Methods used by vendors during packaging to make them blend in with normal mail. Disclosing any particular method of stealth is considered extremely poor form. Examples of stealth methods include making the item appear to come from a legitimate, known business; hiding the product in another, nondescript looking item; and using moisture barrier bags or mylar to eliminate product odor from being emitted from the package. Ideally, you would be able to open the item and give a cursory inspection of all the contents and find nothing unusual, but in practice this can vary greatly.

Sub Reddits – one of the subforums from the popular reddit.com community. Many times shortened to r/subredditname in common discussion. A team of administrators that are usually not affiliated with reddit determines the content policy of the sub reddit, with the website taking a very hands off approach.

SQL injection – An database code injection technique, used to attack data driven applications in which malicious SQL statements are inserted into an entry field for execution, many markets got shut down or lost their money because of this type of attack.

Tails – Are you using just Tor Browser Bundle? Then consider TAILS, it's an operating system specially made for anonymous activities that you boot from a CD or usb stick. It leaves no traces on your computer and has plenty of built in tools that come in handy. \*Check out their website, search "Tails boum" and you should find it very easily.

Talk.masked/core.onion – 2 of the first major forums in Onionland besides Onionforum.

The Marketplace (i2p) – Market set up on the I2P network. Defined by use of an alternate anonymity network and the use of P2SH addresses to hold all funds in escrow during the ordering process. Tends to be either praised for its security or derided for the bugs and non-intuitiveness that it's model provides. You can find full usage guide [here](#).

Tony76 — Was a trusted vendor on SR1, than ran a massive "FE" scam you can read the full story [here](#), The FBI accuses DPR of placing a hit on the individual using this pseudonym. He scammed a large number of Silk Road users, but his true identity and the details of if he was killed or not are still in dispute.

Tor – The Onion Router. Uses 'onion routing' to provide anonymous access to the Internet by encrypting a message several times with each relay removing one layer before the final destination is reached. Funded heavily by the US government, it's security has been a focus of much academic research with no serious known issues or backdoors that have been discovered yet. Used by journalists, government censors, and more to hide their true location and identity.

Torchat – IM service that works by having each user set up a ‘hidden service’ that can be used to contact them via Tor. Somewhat similar in purpose to OTR, but messages do not have plausible deniability.

Torch – Tor Search Engine (<http://xmh57jrznw6insl.onion/>) is your light in the dark net. Make sure to bookmark it if you want to wander the depths beyond your favorite markets.

Tormarket – Another market to rise and fall after SR’s demise. Not as big as Sheep, but the timing made many very cautious about the reliability of new markets.

Tormail – Tor Mail was a Tor hidden service that allowed to send and receive email anonymously, to email addresses inside and outside the Tor network. The service was seized by the FBI as part of the Freedom Hosting bust in August 2013.

Tor Browser Bundle (TBB) – A modified version of Firefox that allows people to easily use the Tor anonymity network. It is compatible with Windows, OS X, and Linux.

Tor Exit Node – The last relay that data traveling from its originator (a computer) to the recipient (a web server) travels through before reaching the recipient. To the recipient, traffic appears to originate from the exit node.

Tor Node – A data relay, either a connection point, a redistribution point (middle node), or an endpoint (exit node).

TS/LS/OPVA/pthc/PB/ptsc/petersburg/anything relating to a child/swirlface/r@ygold – AVOID. CP keywords.

Tumble – a method to anonymize the source of your bitcoins.

TrueCrypt – Open source application used to encrypt storage devices such as hard drives and USB flash drives. It is also used to create encrypted virtual disks contained in a file that mount similarly to real storage devices.

Tx ID – Bitcoin transaction ID

Utopia marketplace – Market that had some connection to BMR (altho the nature of the connection is somewhat unclear). Had the advantage of being fully stocked with former BMR vendors at its public launch. Rapidly taken down by the Dutch police not long after it was unveiled to the public.

Vendors – Those who sell product on a market. This may be of an illegal nature, semi-legal nature, or completely legal nature. Because a vendor will be given a buyer’s full information to send the product to, any new vendor is under heavy scrutiny of being a scam or a ‘honeypot’ set up by law enforcement. Because of the difficult nature of the work, quality vendors tend to develop a cult following.










Vendors Roundtable – A vendor only discussion forum on Silk Road 1/2 forums. Used on a site to allow vendors to bring up issues about the market or buyers without raising alarm in the general populace.












VPN – Virtual Private Network. In the context of anonymous activity, this is usually a proxy that purports to be anonymous in nature to hide the end user’s identity. Generally either used to hide the fact that one is connecting to a anonymous network like Tor, or to hide the fact one is using an anonymous network like Tor (as many websites will block Tor outproxies). A VPN does not provide true security as there is no way to know if the operator is keeping logs.




Whonix – (<http://zo7fksnun4b4v4jv.onion>) is an Debian based operating system focused on anonymity, privacy and security by isolation. Whonix consists of two parts: One solely runs Tor and is called Gateway. The other, the Workstation, is on a completely isolated network. Only connections through Tor are possible.

Whistleblowing – The disclosure by a person, usually an employee in a government agency or private enterprise, to the public or to those in authority, of mismanagement, corruption, illegality, or some other wrongdoing.

## Dark Net Markets Comparison Chart

Market	Uptime Status	URL	Open registrati on?	Had Securit y Issues ?!	Activ e warni ngs	Vend or Bond	FE Allowed ?	Type	Ratings	Created
Alphabay	98.73%	<a href="http://pwoah7foa6au2pul.onion/register.php?aff=41211">http://pwoah7foa6au2pul.onion/register.php?aff=41211</a>	Open		None	200\$	Yes	Free Market	3.38 (887 reviews)	22-12-14
Dream Market	98.70%	<a href="http://lchudifyeqm4ldjj.onion/?ai=1675">http://lchudifyeqm4ldjj.onion/?ai=1675</a>	Open		None	0.25BTC	Yes	Market	4.16 (830 reviews)	15-11-13
Valhalla (Silkkitie)	97.99%	<a href="http://valhallaxmn3fydu.onion/register/E3we">http://valhallaxmn3fydu.onion/register/E3we</a>	Ref Only		None	1BTC	Yes	Market	3.39 (132 reviews)	1-10-13
Hansa Market	99.47%	<a href="http://hansamkt2rr6nfg3.onion/affiliate/110">http://hansamkt2rr6nfg3.onion/affiliate/110</a>	Open		None	0.3BTC	No	Market	4.31 (109 reviews)	18-07-15
Outlaw Market	98.91%	<a href="http://outfor6jwcztwbpd.onion/index.php?id=xx1">http://outfor6jwcztwbpd.onion/index.php?id=xx1</a>	Open		None	0.1 - 2BTC	Under Conditions	Market	3.78 (65 reviews)	29-12-13
Acropolis Market	99.77%	<a href="http://acropol4ti6ytzeh.onion/auth/register/BCBTNUERXY">http://acropol4ti6ytzeh.onion/auth/register/BCBTNUERXY</a>	Referral		None	100\$	Yes	Market	3.24 (21 reviews)	6-11-15
Tochka	97.42%	<a href="http://tochka3evlj3sxdv.onion/auth/register/563636d36ab740e4720f44e8328441d3">http://tochka3evlj3sxdv.onion/auth/register/563636d36ab740e4720f44e8328441d3</a>	Open		None	?	Yes	Market/Local	4.08 (71 reviews)	30-1-15
Apple Market	99.40%	<a href="http://254iloft5cheh2y2.onion/register.php?invite=3GmwV3P">http://254iloft5cheh2y2.onion/register.php?invite=3GmwV3P</a>	Open		None	0-1BTC	Yes	Market	3.13 (50 reviews)	18-2-16
House Of Lions	97.60%	<a href="http://leomarketjdridoo.onion/register/856aeda2b30778">http://leomarketjdridoo.onion/register/856aeda2b30778</a>	Referral		None	Free	Yes	Market	3.24 (31 reviews)	11-3-16

Market	Uptime Status	URL	Open registrati on?	Had Securit y Issues ?!	Activ e warni ngs	Vend or Bond	FE Allowed ?	Type	Ratings	Created
TradeRoute	99.72%	<a href="http://traderouteilbgzt.onion/?r=rvn50">http://traderouteilbgzt.onion/?r=rvn50</a>	Open		None	100USD	Yes	Market	4.48 (28 reviews)	16-7-16
Wall Street Market	99.80%	<a href="http://wallstyizjhkrvmj.onion/signup?ref=276">http://wallstyizjhkrvmj.onion/signup?ref=276</a>	Open		None	80\$ - Free For Trusted	lvl3 Vendors	Market	4.76 (21 reviews)	19-10-16
Zion Market	99.08%	<a href="http://zionshopusn6nopy.onion/_reg23">http://zionshopusn6nopy.onion/_reg23</a>	Open		None	Free	No	Market	4.75 (4 reviews)	28-11-16
Crypto Market	44.83%	<a href="http://cryptomktgxdn2zd.onion/">http://cryptomktgxdn2zd.onion/</a>	Open		None	0.12 - 0.4BTC	Yes	Market	3.68 (177 reviews)	22-12-14
Silk Road 3.0	87.73%	<a href="http://reloadedudjtjvxr.onion/">http://reloadedudjtjvxr.onion/</a>	Open		None	0.11 BTC	Yes	Market	2.80 (81 reviews)	13-10-14
The Majestic Garden	97.55%	<a href="http://bm26rwk32m7u7rec.onion">http://bm26rwk32m7u7rec.onion</a>	Open		None	By invite	Yes	Forum	3.36 (7 reviews)	?
Ramp (Russian Forum)	98.27%	<a href="http://ramp2bombkaddwvgz.onion">http://ramp2bombkaddwvgz.onion</a>	Open		None	?	Yes	Forum	3.92 (96 reviews)	?
Bloomsfield	58.64%	<a href="http://spr3udtjiegxevzt.onion">http://spr3udtjiegxevzt.onion</a>	Open		None	0.3BTC	Yes	Free Market	3.17 (12 reviews)	24-12-15
Darknet Heroes League	96.77%	<a href="http://darkheroesq46awl.onion/">http://darkheroesq46awl.onion/</a>	Open		None	Invited Vendors	Yes	Market	3.81 (53 reviews)	27-5-15
Minerva	99.88%	<a href="http://kp6yw42wb5wpsd6n.onion">http://kp6yw42wb5wpsd6n.onion</a>	Open		None	Free For now	Yes	Market	3.61 (9 reviews)	3-5-16
RsClub Market	98.73%	<a href="http://rsclubvwwcoovivi.onion/">http://rsclubvwwcoovivi.onion/</a>	Open		None	70\$	Yes	Market	3.07 (7 reviews)	11-7-16

Market	Uptime Status	URL	Open registration?	Had Security Issues ?!	Active warnings	Vendor Bond	FE Allowed ?	Type	Ratings	Created
PekarMarket	99.95%	<a href="http://pekarmarkfovqvlm.onion/">http://pekarmarkfovqvlm.onion/</a>	Open		None	?	No	Shell's Market	Not available	30-8-16
The Open Road	99.77%	<a href="http://kess3p7xv6y4mlsd.onion/">http://kess3p7xv6y4mlsd.onion/</a>	Open		None	?	Yes	Market	3.61 (9 reviews)	14-2-17
CGMC	100.00%	<a href="http://cgmcoopwhempo6a5.onion/">http://cgmcoopwhempo6a5.onion/</a>	Invite Only		None	None	No	Market	Not available	7-6-2016