Anti-forensics for Internet Crime

Patrick Neumann, Tor Stian Borhaug,
Espen Winther Øyslebø, Odin Heitmann

Abstract

The time when you were anonymous online when using a pseudonym are long gone. People with both good and bad intentions are using Internet as their arena. How can a person with bad intentions use the Internet without the risk of getting caught by law enforcement agencies or being monitored by other government agencies? One solution is the use of several anti-forensics techniques, whereas use of the Onion Router and the Darknet are starting to become well-known.

Keywords

Anti-forensics;Internet Crime;Darknet;TOR

1.Introduction

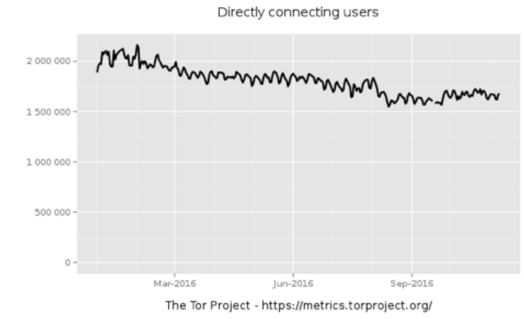
From year 2000 to 2015 the number of Internet users have increased from 400 million to 3.2 billion users worldwide. In the developed countries there is estimated that 8 out of 10 people households have Internet access, and that 8 out of 10 people are also using the Internet (ICT, 2015). If we estimate that only 1 out of 100 people use Internet for criminal activities that leaves us with 32 million potential criminals using the Internet for their activities. 32 million people are roughly the size of New York City and Paris combined. This number means we can expect that a great number of people use the Internet for illegal activities. But using the Internet for illegal activities is normally a bad idea if you do not cover your tracks to stay anonymous. There is a possibility that everything you do online will be logged somewhere. When you connect to the Internet through your Internet Service Provider (ISP) they can monitor which websites you access and all the data packets that go from and to your computer. Your IP address can be logged on every service you use, and Law Enforcement Agencies (LEA) and others can trace that IP address back to you. And what about people that live in regimes that suppress the freedom of speech, and whistleblowers that want to report issues without being traced? The “Panama Papers” (OCCRP, 2016) are a good example on how the Internet was used to share information from a whistleblower to a journalist, and how the whistleblower to this day remains anonymous. Without the possibility to remain anonymous the whistleblower’s life might be in danger, and that is why anti-forensics for Internet crime might not always be a bad thing. There are a lot of anti-forensics techniques available, a Google search for “Anti-Forensic techniques for internet” performed November 10th 2016 gave over 500.000 hits.

In this paper we will discuss some of the challenges, and possibilities, when facing Internet Crime when the users have actively used anti-forensics techniques. We will focus on the use of The Onion Router (TOR). To illustrate how TOR can be used as a anti-forensics technique we will create an online fake drug store. Luckily for LEA and other investigators anti-forensics techniques are not always 100% safe, and we will show how criminals have been caught despite having used anti-forensics techniques.

1.2. Online anonymity

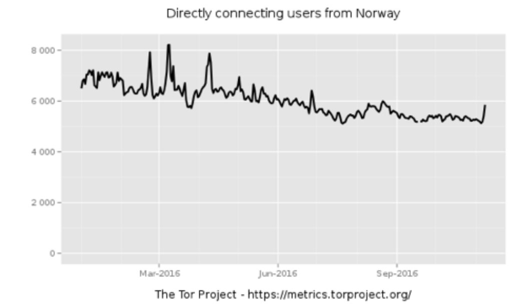
The time when you were anonymous online when using a pseudonym are long gone. Being anonymous online now can be described by the following seven dimensions of identity knowledge: Your legal name, location, pseudonyms that can be linked to your legal name or location, pseudonyms that provide clues to your identity, revealing patterns of behaviour, membership in social groups or information, items or skills that indicate personal characteristics (Kang, 2013). The pseudonym “OsloLawyer76” is a good example on how three dimensions of identity knowledge is revealed with location, profession and year of birth.

In the introduction we gave an example that 1 of 100 people used Internet for illegal activities, and got 32 million potential users. A study by Kang et. al (2013) showed that 53% of the interviewees had used online anonymity for illegal activities or engaged in socially undesirable activities online like visiting web pages containing violence and pornography. 93% of the interviewees had had anonymous social interaction online. An interesting aspect is that while online anonymity seems to be well-used, another study shows that 85% of the interviewees did not know how to surf the Internet anonymously (Conti, 2007) and that most people do not know who has, and can get, access to information about them (Kang, 2013). These numbers seems to make sense when searching for how many direct users TOR has had from January 1st to November 10th 2016. The number of users worldwide are between 1.5 to 2 million users. The number of Norwegian users are ranging from 5000 to 8000. The population of Norway was according to SSB 5,2 million on July 1st 2016. This means that around 0,15% of the Norwegian population have used TOR browser so far in 2016.



The Tor Project - https://metrics.torproject.org/

Fig. 1. Directly connecting users TOR clients, 01.01.16 to 10.11.16



The Tor Project - https://metrics.torproject.org/

Fig. 2. Directly connecting users TOR clients Norway, 01.01.16 to 10.11.16

1.3. The Onion Router

The basic onion routing principles was originally created by the United States Naval Research Laboratory in 1990s, and was further developed by the volunteer Tor group in 2001 (Tor Project, 2016). The main principle with onion routing is that you have layer on layer with encryption and re-routing so it should be extremely difficult to trace the origin of data packets. The data shared goes through a series of virtual tunnels instead of the normal direct connection we are used to when accessing the Internet. This is done so people and organizations can stay anonymous online. It is imperative to state that not only people with malicious intents are using onion routing. People living in countries with no freedom of speech or strict censorship can use TOR to broadcast information to people in other countries without being afraid of reprisals.

Tor is quite complex to explain without illustrations. The Tor Project have described it in an easy way, to show how the data flows from user through several nodes before it reaches the exit-node.

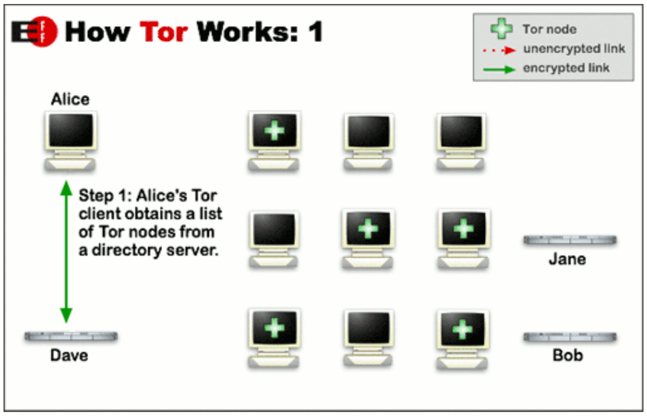

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

Fig.3. How Tor works 1/3.

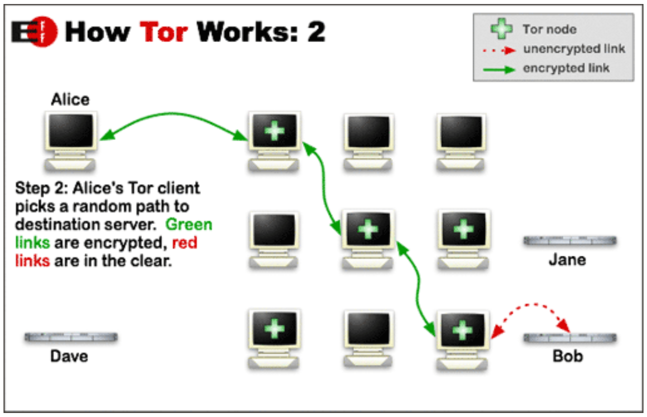

How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Fig.4. How Tor works 2/3.

As we see from fig. 4 the data flows through several nodes on the way from Alice to Bob, and all the data are encrypted except from the last node to Bob. If anyone wanted to monitor the content of the actual data they had to get between the last node and Bob. But they would not be able to trace the data back to Alice, at least not without going through a lot of nodes. Each node only see one hop, and eavesdropping would reveal nothing of nodes more than one hop away. The challenge with backtracking the data is that the path through nodes are randomized every time, and the number of nodes can be vast. As we mentioned earlier there are 1,5 to 2 million worldwide users of TOR, and as per October 2016 there are roughly 7000 relays up and running (Tor Project, 2016). Backtracking user can potentially lead through users from all the Continents in the World, where judicial law and cooperation between nations can make traditional tracing an impossible task.

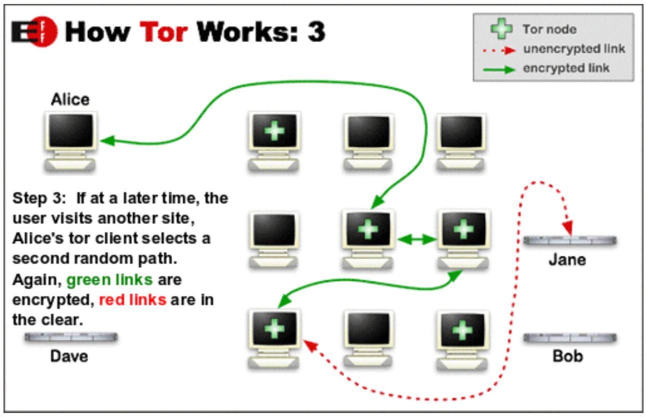
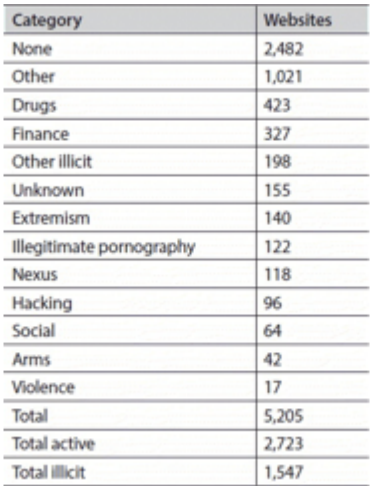

How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Fig.5. How Tor works 3/3.

Another part of the Tor networks security is that after ten minutes you will automatically use a new circuit. This is done to prevent others from analyzing your habits, and therefore be able to trace back activity to you.

1.4. What do people use TOR for?

Moore et. al (2016) did a survey of 5205 live websites from the TOR Darknet. The results clearly showed that the many of the web pages had illicit content. 8% of the pages on TOR were drug related, and 2% were related to illegitimate pornography.



Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Unknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

Fig.6. Classification of content, Moore et. al's survey of TOR Darknet web pages

1.5. Hidden web services on TOR

According to Shipley & Bowker (2014) the hidden services in Tor network is nothing new. They were introduced already in 2004, but was initially not for the technically faint of heart. With the release of a bundled browser in 2008, Tor became more user friendly and an increasing number of people started to use it. In turn, anonymous online markets have emerged, making it difficult for law enforcement to identify buyers and sellers. This has made the online markets very often specialize in black market goods, such as drugs, weapons and illegal pornography (Christin 2012).

Hidden services are run on a Tor client using special server software. The service is only available on the Tor network through a pseudo top-level domain of ".onion". When accessing this domain the traffic is routed through the Tor network without the use of IP-addresses. TorDir and Core.onion are examples of directories that lists a variety of sites on the Tor network. The hidden services is in fact not so "hidden", but you have to know how to get there. No traditional web crawlers like Google will show them.

As stated in the introduction, the majority of the hidden sites on Tor is used for illicit content. There is one interesting graph taken from www.gwern.net/Blackmarket%20survival#analysis that shows the life spans of some of the most famous black market web-shops on the dark web (see appendix). What the graph shows is that most of the services are short lived with an average lifetime from one to two years. Silk Road is one of the longer lived that emerged in 2011 and endures for almost 3 years before the FBI took it down in late 2013. Another interesting fact from the analysis is that from the 88 of markets mentioned, there have only been made arrest in five of them, e.g. Silk Road 1 and Silk Road 2.

We will in the following text take look at some real world examples of such illegal services hosted on Tor and how the law enforcement have used different tactics and techniques to close these services down. We will look at the commonalities and what approaches we, as digital forensic investigators can use from a tactical approach to the more technical spectre of it.

2. Examples where TOR web services have been investigated by law enforcement agencies

There have been several web services that have been investigated by law enforcement agencies. Some of them have been high-profile cases, like the black market store “Silkroad”. We’ll mention some of them.

2.1 Farmers market

The first web service we will look at started even before Silk Road. This was one of the first online black markets that emerged back in 2006 (Zetter, 2014). It connected buyers and sellers through an encrypted email service called Hushmail, but then moved over to the Tor network in 2010. The market hooked up buyers and sellers in 34 countries, and customers could pay for their drugs via services such as Western Union, PayPal or by cash.

A two-year investigation led by the DEA (Drug Enforcement Administration) together with police in the Netherlands, Colombia and Scotland called "Operation Adam Bomb", involved undercover agents that infiltrated the network. The same year as the owners started using Hushmail, the mail provider announced a threat level in that they would not protect law violators being chased by the police and that they would eavesdrop on their users when presented with a court order.

So a combination of undercover work, traceable payment solutions and a mail provider that cooperated with the law enforcement led to the arrest and closure of the site in 2012.

2.2 Freedom Hosting

This was an anonymous hosting service and the most popular one on the Tor network since it was created in 2008. Freedom Hosting had servers that hosted the top sites on Tor. This included TorMail; that was considered the most secure anonymous email provider online, HackBB; a forum for hacking and fraud, the Hidden Wiki; which was the dark version of Wikipedia, and nearly all of the child pornography sites on the Tor network (O’Neill, 2013).

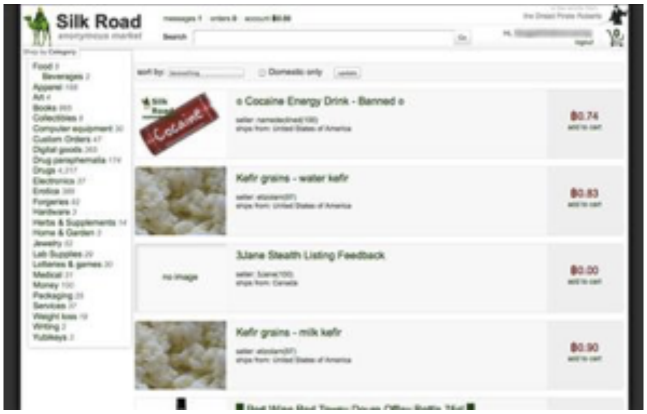
The first hit against Freedom Hosting actually came from the hacktivist group Anonymous in 2011. They launched a series of DDOS (Distributed Denial of Service) attacks against the child pornography sites hosted by Freedom Hosting. It was believed FBI was involved or at least knew of this since they had one profiling member as their informant at the time according to O'Neill (2013). However the sites went up again shortly after the DDOS.

The FBI managed to take over the servers of Freedom Hosting in 2013 and a couple of months later the sites under the hosting service began sending an error message with a hidden code embedded in the page. The embedded code exploited a security hole in Firefox to identify Tor users by reporting back to a mysterious server in Northern Virginia (Bowker, 2013).

2.3 Silk Road

The first online black market to use both Tor and the crypto currency Bitcoin was founded in 2011. It also used PGP (Pretty Good Privacy) encryption and was considered the safest place to buy drugs online. The site gained a lot of attention in the media and increased its user mass very rapidly.

The founder of the site called himself Dread Pirate Roberts and was later identified as Ross Ulbricht, actually by good old detective work according to an article in N.Y. Times (Popper, 2015). While FBI had no good clues to who Dread Pirate Roberts was, an IRS investigator working with the DEA found that Ulbricht was using his own personal e-mail account (rossulbricht at gmail dot com) in some early efforts to promote Silk Road. A person with the same name was asking for programming assistance on a message board for programmers and later changed his nick to "Frosty", which was the same name as the computer Dread Pirate Roberts had been logging onto the Silk Road with. The police got surveillance of Ulbricht, and when he logged onto his computer and just seconds after Dread Pirate Roberts logged onto Silk Road the detective work paid back.



Silk Road
anonymous market
Search
Go
the Dread Pirate Roberts
Shop by Category
Food 3
Beverages 2
Apparel
Art 4
Books
Collectibles 8
Computer equipment 30
Custom Orders 47
Digital goods
Drug paraphernalia
Drugs 4,217
Electronics 37
Erotica
Forgeries 42
Hardware 3
Herbs & Supplements 14
Home & Garden 3
Jewelry 62
Lab Supplies 29
Lotteries & games 30
Medical 31
Money
Packaging 25
Services 37
Weight loss 19
Writing 3
Yubikeys 2

sort by:
□ Domestic only

o Cocaine Energy Drink - Banned o
ships from: United States of America
฿0.74
add to cart

Kefir grains - water kefir
ships from: United States of America
฿0.83
add to cart

3Jane Stealth Listing Feedback
no image
ships from: Canada
฿0.00
add to cart

Kefir grains - milk kefir
ships from: United States of America
฿0.90
add to cart

Fig.7. Screenshot of Silk Road

Silk Road went online again just about a month after it was taken down. It re-emerged as Silk Road 2, but the FBI together with 17 other countries took it down again a year later. The bust was called Operation Onymous where 17 people was arrested and around 400 dark net domains closed. It is not known to the public how FBI was able to locate the sites and it raised questions to whether Law Enforcement had found new vulnerabilities in Tor

(Greenberg 2014). Nonetheless, the effort scared a lot of users from thinking Tor is perfectly safe.

3. Approaches to de-anonymize users on TOR

Online marketplaces where users connect to buy and sell drugs are mostly located on hidden services to make it harder for law enforcement to investigate. In this section we will look at ways to identify users of such services, and to find out where the hidden service is physically hosted.

3.1 Human error - our best bet?

In practice, the easiest way to achieve these goals is through traditional investigation techniques focusing on human error.

There is of course a possibility that the Law Enforcement in the US have found vulnerabilities in Tor, and we have heard stories of NSA's big scale surveillance of the Internet from the whistleblower Edward Snowden. It is not unlikely that the FBI or NSA are controlling parts of the Tor network, if you got the resources much is possible, but the most common reason why people get arrested is simply because they are human, human does mistakes.

One example is that several top Silk Road administrators were arrested because they gave proof of identity to Dread Pirate Roberts, data that was owned by the police when Ulbricht was arrested. They went in the undertow because police had access to the data. Further, dozens of dealers and customers were arrested for drug operations on the Darknet. The cause was not Tor itself, it was human error. Mail packages were caught and flagged, many had poor “stealth” for their orders, making them easily detected by postal workers and drug dogs (O'Neill 2014).

The exception from the examples I mentioned is the Freedom Hosting tracking exploit. But then, in the end this technique will be followed with tracing IP addresses and traditional investigative work to get the evidence needed for an arrest and conviction (Bowker 2013).

Shipley & Bowker (2014) writes that some of the best methods of identifying people online is the same tactic that hackers have used for years, *social engineering*. Social engineering is the act of manipulating people to do something or reveal information. It could be something as simple as a fake telephone call to the target stating that you are calling from the company's help desk and that you need their assistance with an issue. When working through a computer problem on the network the target is convinced that he must give his username and password to solve the problem.

Another method is to use services like ReadyNotify.com or AnonymousSpeech.com where you send an e-mail to the target with some content added. When opened by the target it will track the target's IP address and reply it back.

3.2 Leaking IP address or other identifying information

TOR hidden services which are configured incorrectly may leak sensitive identifying information. For example, a web server running as a hidden service may leave a status page, logfile or error message visible. If the external IP address is part of this information, the location can be determined through contacting the ISP. The FBI testified that they found the IP address associated with a Silkroad server by examining an error message they got when trying to log in to the site.

Clients may also reveal their IP address or other sensitive information which can be used to uniquely identify the user, especially if not configured correctly. Using the TOR browser bundle or Tails mitigates some possible sources of such leaks.

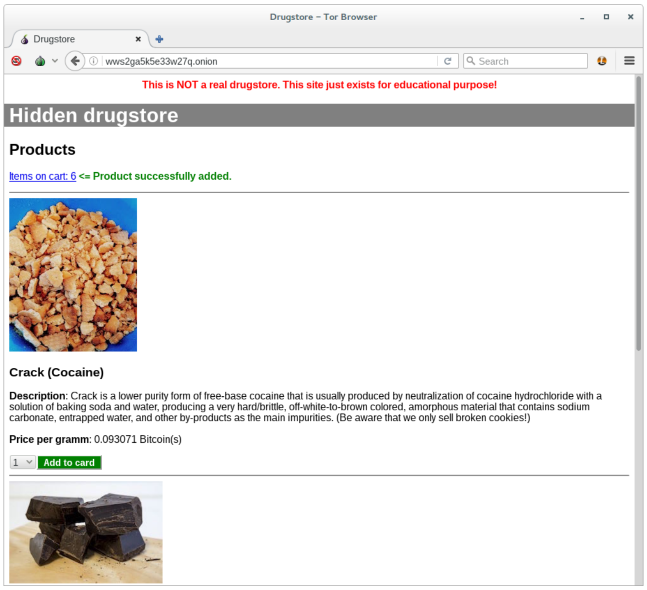
The simplest way in which a client can be identified is if it somehow leaks its IP address. Many client programs are not written with anonymity or TOR usage in mind, and plugins or external programs may access the Internet directly without going through TOR. Firefox resolve DNS addresses without going through TOR, unless configured not to. Bittorrent clients will often transmit their external IP address as part of the protocol, even when told to connect through TOR. Javascript, browser plugins, and software exploits are other potential ways in which the client may leak its IP address (Manils, 2010).

Obtaining the IP address through this method requires that the client connects to a service you control. This can be done by taking over control of a hidden service like the FBI did in the Freedom Hosting case, or by contacting users through direct messaging or forum posts and convincing them to follow links.

Even if a client does not leak its IP address, it may be fingerprinted by examining how the client or user behaves. A regular web browser will usually happily supply information about the screen resolution, installed plugins, installed fonts, timezone and other bits of information, and the combination of this information make the user relatively unique. This way, you may be able to track a user across different websites (Eckersley, 2010).

4. Case study - The “perfect” online drug store

The examples above with real-life stories show that human error is a large factor when online anonymity crumbles. Based on what we know from investigation and theory about online activity, we have created an online drug store using TOR. There were several key points that were crucial to create an online drug store, and we will discuss our thought about each factor.



This is NOT a real drugstore. This site just exists for educational purpose!

Hidden drugstore

Products

Items on cart: 6 <= Product successfully added.

Crack (Cocaine)

Description: Crack is a lower purity form of free-base cocaine that is usually produced by neutralization of cocaine hydrochloride with a solution of baking soda and water, producing a very hard/brittle, off-white-to-brown colored, amorphous material that contains sodium carbonate, entrapped water, and other by-products as the main impurities. (Be aware that we only sell broken cookies!)

Price per gramm: 0.093071 Bitcoin(s)

Fig.8. Screenshot of our online drug store, http://wws2ga5k5e33w27q.onion/.

4.1 Supply

The online drug stores we have seen have had several items in stock. We need to have a supply of drugs that do not get emptied. That would be bad for business. There are three ways that we can ensure that our supply is full.

1. Own production. Can be difficult to produce large amounts of “soft” drugs like cannabis and “hard” drugs like heroin,

cocaine, LSD etc., as the production requires a lot of equipment which again increases the risk for getting caught.

2. Order from other sellers and shipping to own home. Large risk that LEA's track the shipment, or that you get caught in the aftermath of another investigation, like e.g. SilkRoad.

3. Smuggling. As we see it this is the best solution to get a stock full of drugs. From our experience German dealer often travel to Amsterdam to fill up their stocks.

4.2 ISP (client side)

There are several possibilities for choosing internet connectivity from the client side, ranging from an ordinary DSL provider like AOL, a prepaid SIM bought with stolen ID and charging credits with cards from e.g. petrol stations or free WiFi from e.g. a library or an internet-cafè. As long as we use special software for staying anonymous, and keep the factor of human error out of the equation, each of the following methods should be safe. We have, however, chosen to go with free WiFi, as this will be the best solution for our OS.

4.3 Operating System (client side)

The OS on the client side can be Windows, OSX, Linux and other known OS. We need to have a Tor-browser installed. The browser leaves artefacts that can be found during an investigation. Another downside is that the factor of human error again can come into play if we are unaware and use e-mail or SSH from the same computer. We have found that Tails (https://tails.boum.org) is the best solution.

After we have installed Tails (https://tails.boum.org/install/clone/index.en.html) we have found a guide (http://guidesj4g6kjznhj.onion/securityguide/Tails.html) with additional hints in the Tor network. We used real hardware because virtual machines have unneeded additional bugs. We have added an encrypted Persistent Volume. We have written a quick and dirty script for more usability and stored it in the Persistent Volume:

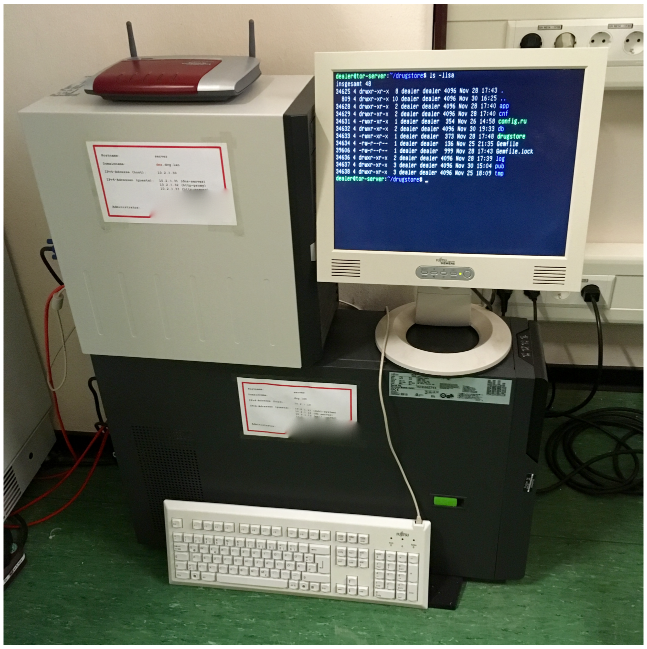
```
#!/bin/bash

# switch to another keyboard layout if needed:
readonly LANG="de"
setxkbmap "${LANG}"
gsettings set org.gnome.desktop.input-sources sources "[('xkb', '${LANG}')]"

# generate profile by first start of firefox:
/usr/local/bin/tor-browser &
sleep 10
pkill firefox

# make firefox more "safer":
cd ~/.tor-browser/profile.default/
echo 'user_pref("javascript.enabled", false);' >> ./prefs.js
echo 'user_pref("extensions.torbutton.saved.sendSecureXSiteReferrer", false);' >> ./
prefs.js
echo 'user_pref("network.http.sendRefererHeader", 0);' >> ./prefs.js
echo 'user_pref("network.http.sendSecureXSiteReferrer", false);' >> ./prefs.js
rm ~/.tor-browser/profile.default/extensions/\{d10d0bf8-f5b5-c8b4-a8b2-2b9879e08c5d\}

exit 0
```

Fig.9. Code from the script

Tails also supports "Mac Address Spoofing" per default. That feature does not make sense with your own router or mobile phone (tethering) in front of your Client with Tails. That is why we chose free WiFi (e. g. near/in a Restaurant, Hotel, ...) as our client side internet connection.

4.4 ISP (server)

When it comes to storage we can choose from a commercial datacenter like hetzer.de, a virtual server in the cloud like Amazon EC2 or a server in our own home. The main advantage with a commercial datacenter is reliability and performance of the server, but they do not accept anonymous payment and/or registration. We will not get physical access to the hardware, and will not be able to set bios password, change boot order (forbid booting from external media) or enter password for an encrypted partition. A virtual server is interesting because a deleted virtual server is not recoverable, and there is a lack of forensic interface for the government. Tails do not support virtual machines, so that would not work for us. That leaves us with the last option; a server in our own home.



```
dealer@tor-server:~/drugstore$ ls -lisa
insgesamt 48
34625 4 drwxr-xr-x  8 dealer dealer 4096 Nov 28 17:43 .
  809 4 drwxr-xr-x 10 dealer dealer 4096 Nov 30 16:25 ..
34628 4 drwxr-xr-x  2 dealer dealer 4096 Nov 28 17:40 app
34629 4 drwxr-xr-x  2 dealer dealer 4096 Nov 28 17:40 cnf
34631 4 -rwxr-xr-x  1 dealer dealer  354 Nov 26 14:58 config.ru
34632 4 drwxr-xr-x  2 dealer dealer 4096 Nov 30 19:33 db
34633 4 -rwxr-xr-x  1 dealer dealer  373 Nov 28 17:48 drugstore
34634 4 -rw-r--r--  1 dealer dealer  136 Nov 25 21:35 Gemfile
39606 4 -rw-r--r--  1 dealer dealer  999 Nov 28 17:43 Gemfile.lock
34636 4 drwxr-xr-x  2 dealer dealer 4096 Nov 28 17:39 log
34637 4 drwxr-xr-x  3 dealer dealer 4096 Nov 30 15:04 pub
34638 4 drwxr-xr-x  3 dealer dealer 4096 Nov 25 18:09 tmp
dealer@tor-server:~/drugstore$ _
```

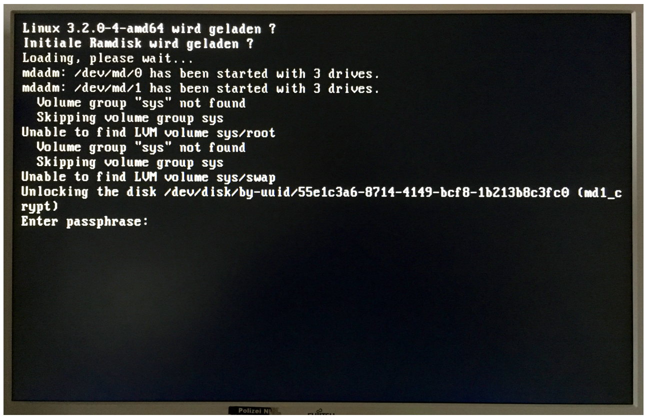
Fig.10. The "grey" machine is serving the hidden drugstore through the router on top of it. On the screen you can see the root of the application.

4.5 Configuration of server

Our experience with web development leaves us with a Linux distro.

To enhance security of the server there are several steps we will take:

- Disable booting from external devices in the bios
- Password-protect bios
- Two hard drives assembled as a software raid 1
- Only the boot partitions with the bootloader (including configuration), kernel image and initial ramdisk will be left unencrypted
- The raid for data will be encrypted (Fig 10.)
- To be able to connect to the service TOR we will install "TOR"
- Deactivate logging as much as possible. The system is encrypted, but better safe than sorry.



```
Linux 3.2.0-4-amd64 wird geladen ?
Initiale Ramdisk wird geladen ?
Loading, please wait...
mdadm: /dev/md/0 has been started with 3 drives.
mdadm: /dev/md/1 has been started with 3 drives.
  Volume group "sys" not found
  Skipping volume group sys
Unable to find LVM volume sys/root
  Volume group "sys" not found
  Skipping volume group sys
Unable to find LVM volume sys/swap
Unlocking the disk /dev/disk/by-uuid/55e1c3a6-8714-4149-bcf8-1b213b8c3fc0 (md1_c
rypt)
Enter passphrase:
```

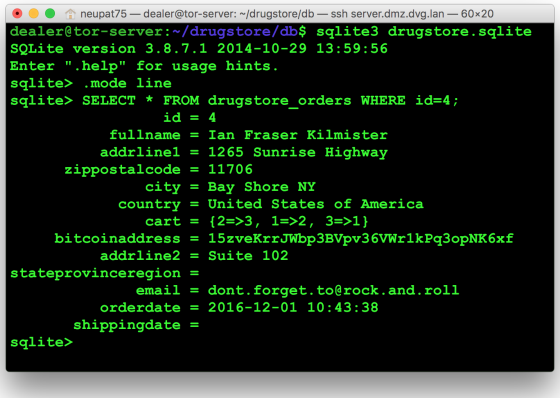
Fig.11. There is a passphrase required to start the machine with the hidden drugstore "in it". In addition you have to know a little bit about software raid and logical volume manager to investigate it. At least this photo shows that the suspect seems to be from Germany.

4.6 Web shop

We considered three options for implementing the web shop.

- Apache + MySQL + PHP + Magento (www.magento.com)
- Nginx + plain html + simplecartsjs (http://simplecartjs.org/)
- A simple, self-made web application coded in Ruby at top of the micro framework "Camping" behind a lighttpd HTTP Server storing orders in a sqlite file without a backend accessible over HTTP.

A mainstream solution like "Magento" could be an attack vector and is often the reason why a suspect will code their own "closed" web applications. PHP is also well known as module of an Apache HTTP Server and there are periodical security issues. Attacking JavaScript will not affect the hidden service but it could be very easy to manipulate the interaction with the shop. A shopping cart solution in javascript is not a really secure idea (https://news.ycombinator.com/item?id=4820626). That is why we would go with the simple self made web application. If we administrate the server at home we could code a separate application as a backend of the shop that is only accessible over terminal or a port that is not routed to the internet and not through the tor network. If we have access to a terminal (local or remote) we just need a sqlite client to have access to the orders.



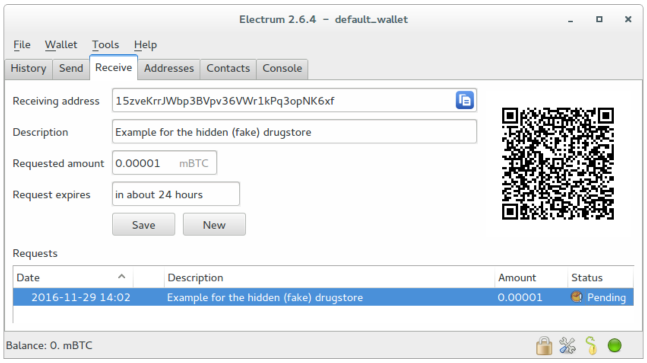
neupat75 — dealer@tor-server: ~/drugstore/db — ssh server.dmz.dvg.lan — 60×20

```
dealer@tor-server:~/drugstore/db$ sqlite3 drugstore.sqlite
SQLite version 3.8.7.1 2014-10-29 13:59:56
Enter ".help" for usage hints.
sqlite> .mode line
sqlite> SELECT * FROM drugstore_orders WHERE id=4;
               id = 4
         fullname = Ian Fraser Kilmister
        addrline1 = 1265 Sunrise Highway
    zippostalcode = 11706
             city = Bay Shore NY
          country = United States of America
             cart = {2=>3, 1=>2, 3=>1}
   bitcoinaddress = 15zveKrrJWbp3BVpv36VWr1kPq3opNK6xf
        addrline2 = Suite 102
stateprovinceregion =
            email = dont.forget.to@rock.and.roll
        orderdate = 2016-12-01 10:43:38
     shippingdate =
sqlite>
```

Fig.12. Screenshot of terminal and a sqlite3 query for orders.

4.7 Payment through cryptocurrencies

When buying or selling illicit goods online, traditional payment methods such as cash, credit cards and bank transfers are a poor choice because they are easily traceable. Bitcoin quickly got adopted as the de facto standard payment method for online marketplaces where illicit goods are sold because it is difficult to trace and operates outside of traditional financial systems.



Receiving address: 15zveKrrJWbp3BVpv36VWr1kPq3opNK6xf

Description: Example for the hidden (fake) drugstore

Requested amount: 0.00001 mBTC

Request expires: in about 24 hours

Requests

Date	Description	Amount	Status
2016-11-29 14:02	Example for the hidden (fake) drugstore	0.00001	Pending

Balance: 0. mBTC

Fig.13. With Electrum (pre-installed in Tails) it is just a click to generate a receive address.

Bitcoin is a cryptocurrency launched in 2009. Value is transferred from one address (account) to another through signed transactions, which are verified by miners. Miners verify transactions and are rewarded for maintaining network security through proof of work. Miner rewards are the only way new new units are added to the money supply, and this happens at a predictable and agreed upon rate (Nakamoto, 2008).

The bitcoin blockchain is a public ledger containing all historic transactions. Transactions contain information about all ingoing and outgoing addresses, and are therefore not anonymous but pseudonymous. Bitcoins can be followed from one address to another, but determining which real world identity controls the keys to an address can be challenging.

Ways to connect real world identities to bitcoin addresses include collecting information from open sources, through traditional investigation methods and through examining the blockchain. Except for the initial miner reward, all transactions are tainted by their history.

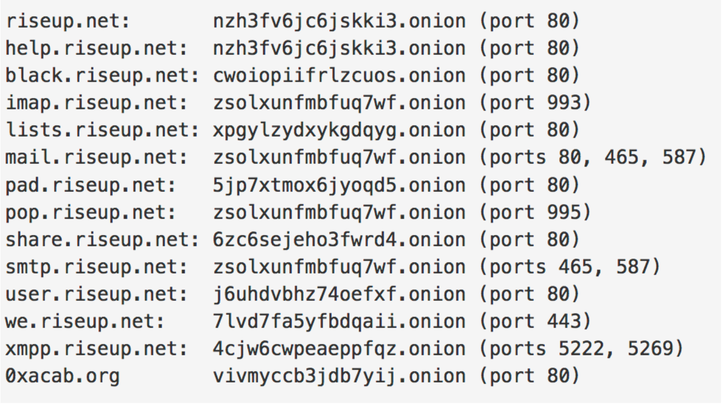
For example, if you know that an entity controls an address A, and you see a transaction which combines Bitcoin from address A and address B and sends it to address C, you can deduce that the entity also controls address B. Best practices to increase financial privacy are to use a new address for each transaction.

Discovering relationships between bitcoin addresses and real world identities is made difficult by the fact that a person can control more then one addresses, and multiple people may control one address through multi-signature transactions. Other challenges are the use of mixing services which obfuscate the transaction history. Mixing services can be explained using the analogy of exchanging a marked 100 dollar bill for a different 100 dollar bill by contacting someone with a large pool of 100 dollar bills.

Like TOR, bitcoin forensics is an ongoing field of research both in terms of how transactions can be tracked and how to increase anonymity.

4.8 Contact between us and buyer

A good web shop has a way of communicating with potential buyers. Regular e-mail like Gmail and Hotmail is farely easy to trace back to the user, and is not a good option. Messenger services like ICQ or Skype is also easy to track, even though more and more messenger services have implemented encryption as a standard the last year. If we will use e-mail Riseup (https://riseup.net/en) seems like a good alternative as Riseup is not logging. If you use the .onion address, the e-mail header does not contain your real ip-address (received entries). Riseup's IMAP and SMTP services can be used with Tails though the Tor network.



```
riseup.net:       nzh3fv6jc6jskki3.onion (port 80)
help.riseup.net:  nzh3fv6jc6jskki3.onion (port 80)
black.riseup.net: cwoiopiifrlzcuos.onion (port 80)
imap.riseup.net:  zsolxunfmbfuq7wf.onion (port 993)
lists.riseup.net: xpgylzydxykgdqyg.onion (port 80)
mail.riseup.net:  zsolxunfmbfuq7wf.onion (ports 80, 465, 587)
pad.riseup.net:   5jp7xtmox6jyoqd5.onion (port 80)
pop.riseup.net:   zsolxunfmbfuq7wf.onion (port 995)
share.riseup.net: 6zc6sejeho3fwrd4.onion (port 80)
smtp.riseup.net:  zsolxunfmbfuq7wf.onion (ports 465, 587)
user.riseup.net:  j6uhdvbhz74oefxf.onion (port 80)
we.riseup.net:    7lvd7fa5yfbdqaii.onion (port 443)
xmpp.riseup.net:  4cjw6cwpeaeppfqz.onion (ports 5222, 5269)
0xacab.org        vivmyccb3jdb7yij.onion (port 80)
```

Fig.14. List of Riseup's Tor hidden services.

4.9 Shipping

The last and crucial step is how we can get our product out to the customer. Regular shipping with cargo insurance and tracking is not a good idea, as we have to give some information if we want to track the shipment. We will leave sender blank, and ship in letter size envelopes from different mailboxes. We will also vary the size and brand of the envelope to make it harder for others to see a pattern in our shipment.

One possible issue with shipping is that you may leave fingerprints or DNA on packages you send which may later be used to convict you. Even using different mail offices for each package, it is possible that the postal service will become suspicious if you send enough packages. USPS confirmed that they photograph all letters and packages that are sent, so law enforcement can trace where a package was sent from (The New York Times, 2013).

5. Summary

The digital landscape of Internet and forensic techniques for Internet are changing rapidly. In order to beat anti-forensic techniques it is imperative that law enforcement agencies and other investigators continuously work to find flaws in the current technology. Our web store demonstrated in this paper might be safe (enough?) today, but tomorrow a flaw can be found which will make our web store unsafe. Luckily for LEA's the quote "Criminals have to be lucky each time; police has to be lucky only once" is quite describing. People using anti-forensics technology to hide illegal activity online can not afford to make a mistake. One mistake can be enough that they are caught, as we saw in the example with Silk road.

6. References

1. Bowker, Art (14.11.13) *Law Enforcement is on a Tor offensive*. http://scitechconnect.elsevier.com/law-enforcement-tor-offensive Retrieved 19.11.16
2. *Complete Anti-Forensics Guide* (2013) Unknown author. Retrieved from http://pastebin.com/TWsUpMnD
3. Conti, G. and Sobiesk, E. *An honest man has nothing to fear: user perceptions on web based information disclosure*. SOUPS, (2007), 112–121.
4. Eckersley, P. (2010, July). *How unique is your web browser?*. In International Symposium on Privacy Enhancing Technologies Symposium (pp. 1-18). Springer Berlin Heidelberg.
5. Greenberg, Andy (07.11.14). *Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains*. https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/ Retrieved 19.11.16.
6. *ICTFactsFigures2015*. (2015) Geneva: ICT Data and Statistics Division. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf
7. Kang, R., Brown, S., Kiesler, S. (2013) *Why Do People Seek Anonymity On the Internet?* Informing Policy and Design. Pittsburgh: Carnegie Mellon University. Retrieved from https://www.cs.cmu.edu/~kiesler/publications/2013/why-people-seek-anonymity-internet-policy-design.pdf
8. Krishnamurthy, B. and Wills, C.E. *Characterizing privacy in online social networks*. Proc. of the first workshop on Online social networks, (2008), 37–42.
9. Kwon, A., AlSabah, M., Lazar, D., Dacier, M., & Devadas, S. (2015). *Circuit fingerprinting attacks: Passive deanonymization of tor hidden services*. In 24th USENIX Security Symposium (USENIX Security 15) (pp. 287-302).
10. Manils, P., Abdelberri, C., Blond, S. L., Kaafar, M. A., Castelluccia, C., Legout, A., & Dabbous, W. (2010). *Compromising tor anonymity exploiting p2p information leakage*. arXiv preprint arXiv:1004.1461.
11. Moore, D., Rid, T. (2016) *Survival: Cryptopolitik and the Darknet*. IISS, volume 57 iss. 1.Retrieved from http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085
12. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.
13. Nicolas, C. (2012) *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*. https://arxiv.org/pdf/1207.7139v2.pdf Retrieved 18.11.16
14. Nixon, R. (02.08.13). *Postal Service Confirms Photographing All U.S. Mail*. http://www.nytimes.com/2013/08/03/us/postal-service-confirms-photographing-all-us-mail.html. Retrieved 03.12.2016
15. OCCRP. *Giant leak of offshore financial records exposes global array of crime and corruption*. OCCRP. The International Consortium of Investigative Journalists. April 3, 2016. Retrieved from https://www.occrp.org/en/panamapapers/overview/intro/
16. O'Neill, P. H. (04.08.13). *An in-depth guide to Freedom Hosting, the engine of the Dark Net*. http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/ Retrieved 18.11.16

17. O'Neill, P.H. (02.10.14). *The real problem with Tor's security.* http://kernelmag.dailydot.com/issue-sections/features-issue-sections/13606/tor-arrest-history/ Retrieved 19.11.16.

18. Popper, N. (25.12.15). *The Tax Sleuth Who Took Down a Drug Lord*. http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html Retrieved 19.11.16.

19. Riseup. *Tor - riseup.net*. Retrieved from https://riseup.net/en/security/network-security/tor#riseups-tor-hidden-services

20. Shipley, T. G., Bowker, Art (2014) *Investigating Internet Crimes*

21. Single, R. (11.07.07). *Encrypted E-Mail Company Hushmail Spills to Feds*. https://www.wired.com/2007/11/encrypted-e-mai/ Retrieved 18.11.16

22. Statistisk Sentralbyrå (2016). *Nøkkeltall for befolkning*. Retrieved 10.11.16 from https://www.ssb.no/befolkning/nokkeltall.

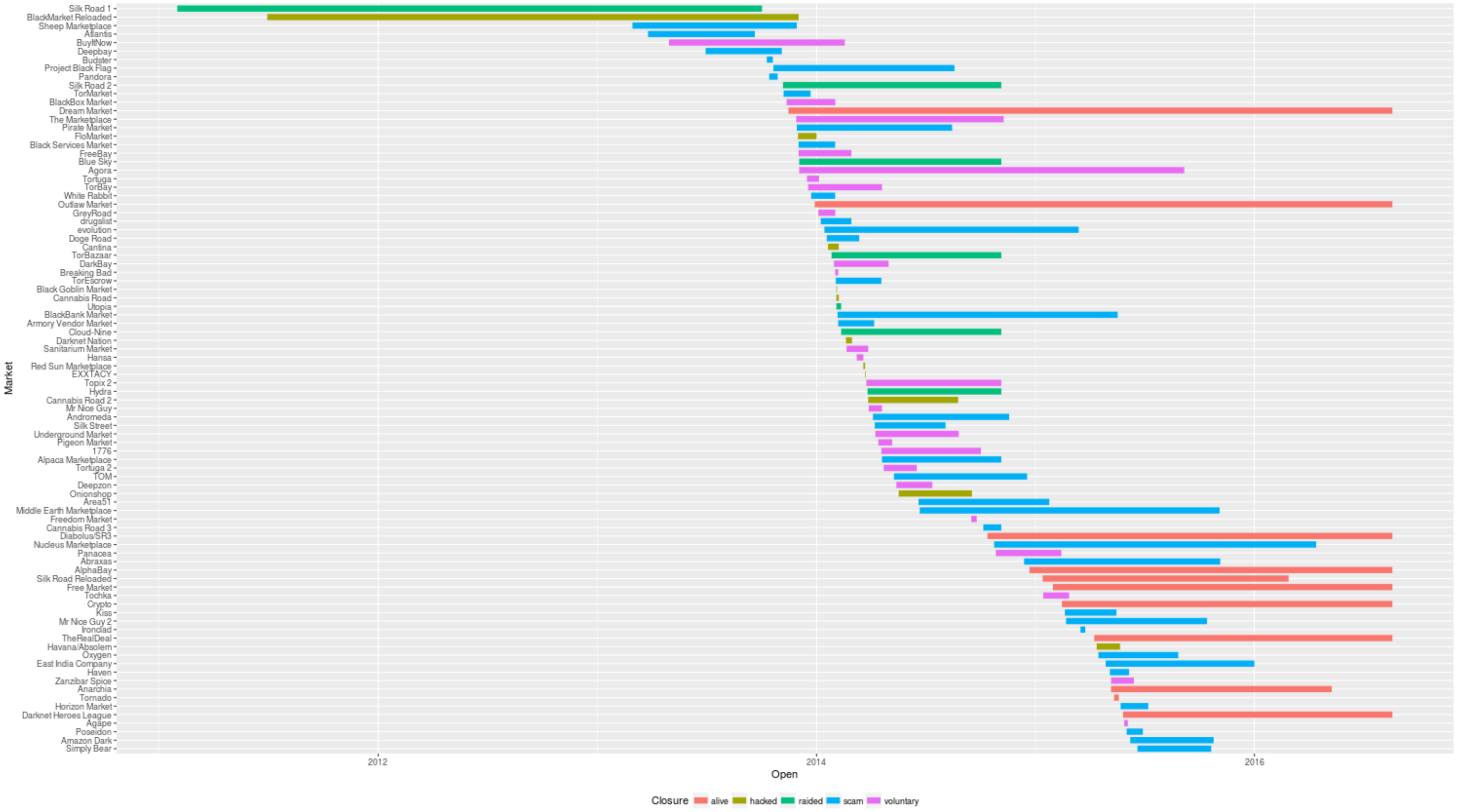
23. The Tor Project. *sida* | *The Tor Blog*. Retrieved 01.12.16 from https://blog.torproject.org/category/tags/sida

24. The Tor Project. *Tor Project: Overview*. Retrieved 01.12.16 from https://www.torproject.org/about/overview.html.en

25. Zetter, K. (16.04.14). *8 Suspects Arrested in Online Drug Market Sting*. https://www.wired.com/2012/04/online-drug-market-takedown/ Retrieved 18.11.16

A. Appendix

Appendix 1. Graph from https://www.gwern.net/Black-market%20survival#analysis


Silk Road 1
BlackMarket Reloaded
Sheep Marketplace
Atlantis
BuyItNow
Deepbay
Budster
Project Black Flag
Pandora
Silk Road 2
TorMarket
BlackBox Market
Dream Market
The Marketplace
Pirate Market
FloMarket
Black Services Market
FreeBay
Blue Sky
Agora
Tortuga
TorBay
White Rabbit
Outlaw Market
GreyRoad
drugslist
evolution
Doge Road
Cantina
TorBazaar
DarkBay
Breaking Bad
TorEscrow
Black Goblin Market
Cannabis Road
Utopia
BlackBank Market
Armory Vendor Market
Cloud-Nine
Darknet Nation
Sanitarium Market
Hansa
Red Sun Marketplace
EXXTACY
Topix 2
Hydra
Cannabis Road 2
Mr Nice Guy
Andromeda
Silk Street
Underground Market
Pigeon Market
Alpaca Marketplace
Tortuga 2
TOM
Deepzon
Onionshop
Area51
Middle Earth Marketplace
Freedom Market
Cannabis Road 3
Diabolus/SR3
Nucleus Marketplace
Panacea
Abraxas
AlphaBay
Silk Road Reloaded
Free Market
Tochka
Crypto
Kiss
Mr Nice Guy 2
Ironclad
TheRealDeal
Havana/Absolem
Oxygen
East India Company
Haven
Zanzibar Spice
Anarchia
Tornado
Horizon Market
Darknet Heroes League
Agape
Poseidon
Amazon Dark
Simply Bear
Market
Open
Closure
alive
hacked
raided
scam
voluntary