Anti-forensics for Internet Crime

Group 13: Patrick Neumann, Tor Stian Borhaug, Espen Winther Øyslebø, Odin Heitmann

IMT4114 2016

Introduction

Number of Internet users 2000 > 2015: 400 million > 3.2 billion

8/10 people in developed countries use Internet

Our project:

We have created our “perfect” online drugstore on the darknet.

Research on real-life examples where criminals using anti-forensics techniques have been caught

Note: Not only criminals have the need for anonymity online. E.g. Snowden, Panama Papers..

Online anonymity

(Pseudonym is not enough)

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 pattern of behaviour
- Membership in social groups or information
- Items or skills that indicate personal characteristics

How about the pseudonym “OsloLaywer76”? Three dimensions revealed - not very smart..

Online anonymity

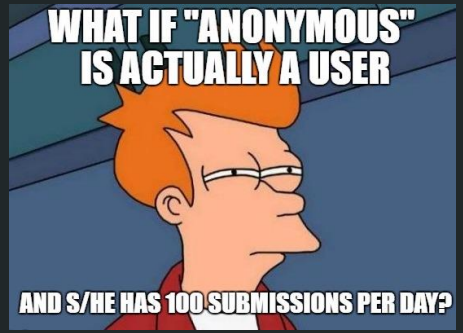
How good are the users?

A study showed that 53%(!) percent had:

- used online anonymity for illegal activities or,
- engaged in socially undesirable activities online like visiting webpages with violence or pornography

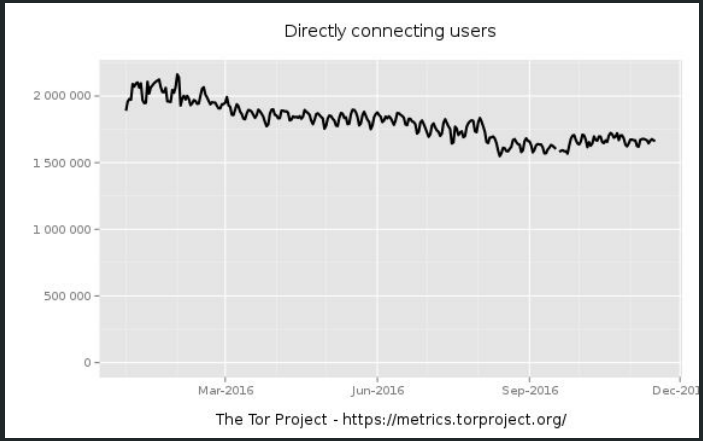
93% had had anonymous social interaction online.

But another study shows that only 15% knew how to surf the web anonymously.. (Were the 15% really anonymous...?)

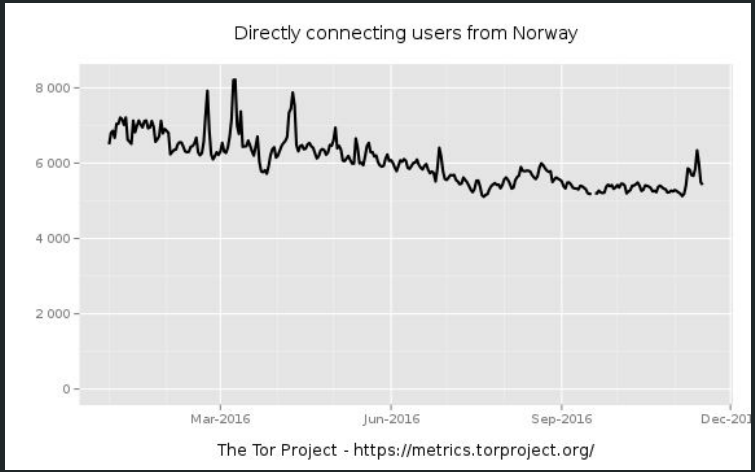


The Onion Router

(The users)



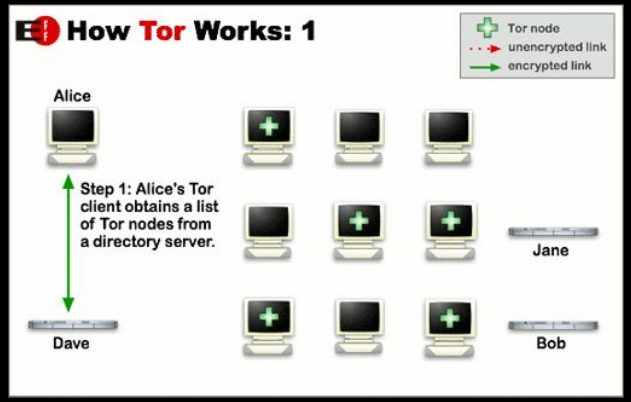
1,5 - 2 million users worldwide

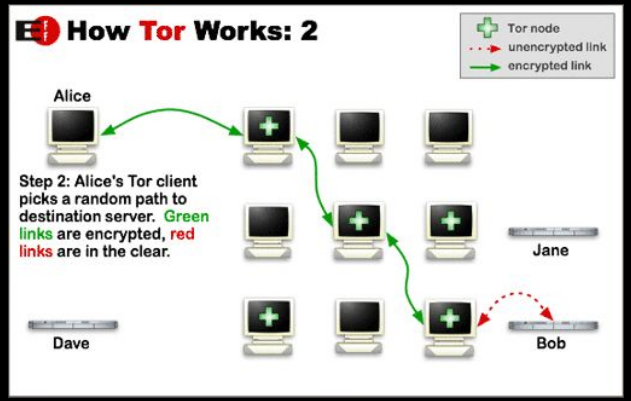


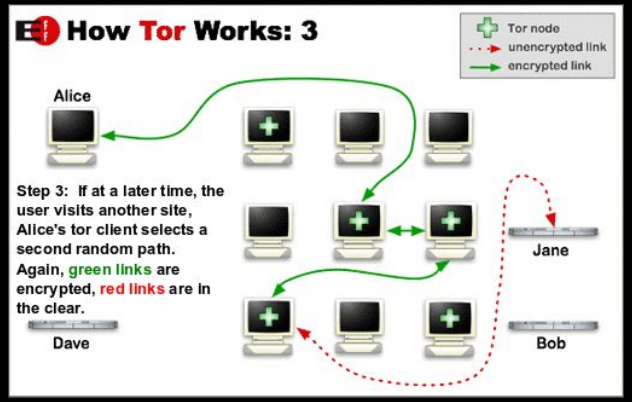
5000 - 8000 in Norway - are you one of them?

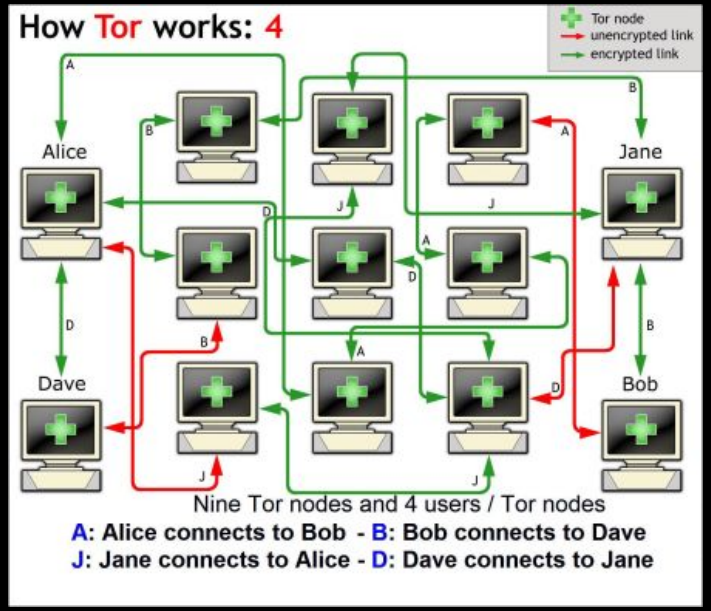
The Onion Router

(The basics)









The Onion Router

(What do people use TOR for?)

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

Hidden services

The underground of the dark web

- Only available through tor
- Mainly illicit content
- Limited life span

Hidden services

Investigations by law enforcement

- Farmers Market
- Freedom hosting
- Silk Road

Deanonymizing TOR

Methods to identify buyers and sellers on darknet markets

- Human Error
- Leaking sensitive information
- Unknown vulnerabilities
- Other attack vectors

Our “perfect” online drug store

Drugstore – Tor Browser

Drugstore

wws2ga5k5e33w27q.onion

Search

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 hyd
solution of baking soda and water, producing a very hard/brittle, off-white-to-brown colored, amorphous material that co
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)

1 Add to card

Drugstore – Tor Browser

Drugstore

wws2ga5k5e33w27q.onion/cart

Search

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

Hidden drugstore

Cart

<- Back to the calalog

Delete Cart

Quantity (Gramm)	Title	Price (Bitcoin)	Subtotal (Bitcoin)	Action
3	Hashish	0.010792	**0.032376**	Delete product
2	Crack (Cocaine)	0.093071	**0.186142**	Delete product
1	Crystal Meth	0.129291	**0.129291**	Delete product

Total: 0.347809 BTC

Checkout

Hint: the max of gramms per product per order is set at 10.

(c) 2016 - The Onion Root

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

Drugstore – Tor Browser

Drugstore

wws2ga5k5e33w27q.onion/checkout

Search

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

Hidden drugstore

Checkout

<- Back to the cart

Shipping Address:

Full Name:	Ian Fraser Kilmister
Address Line 1:	1265 Sunrise Highway
Address Line 2:	Suite 102
City:	Bay Shore NY
State/Province/Region:	
ZIP/Postal Code:	11706
Country:	United States of America
Email:	dont.forget.to@rock.and.roll

Place order

Some hints:

- **Fields with a bold red label are mandatory fields!**
- After successfully placing the order you will get a bitcoin address.
- Shipping will be done after you have proceeded a transaction to that address.
- Unpayed orders will be deleted in the database after the request expires (1 day).

(c) 2016 - The Onion Root

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

http://wws2ga5k5e33w27q.onion/

Supply

From our narrow selection:

1. Own production
2. Order and shipping to home
3. Smuggling

1. Too difficult
2. Gives the government the solution to track the way of the goods
3. Ordinary traders do not do it differently

That’s why we go with 3.

ISP (client side)

From our narrow selection:

1. (V-)DSL provider
2. UMTS/LTE
3. free WiFi

1. Not anonymous
2. Traceable
3. Only the MAC address could be the problem

(We will come to a decision later.)

OS (client side)

From our narrow selection:

1. ordinary Windows, ...
2. 1. + Tor-Browser
3. Tails

1. No anonymity
2. Anonymous browsing only
3. Everything (incl. Mail, SSH, ...) is routed through Tor

That's why we go with 3.

Also Tails is not perfect...

```
#!/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 "saver":
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
```

http://guidesj4g6kjznhj.onion/securityguide/Tails.html

ISP (server)

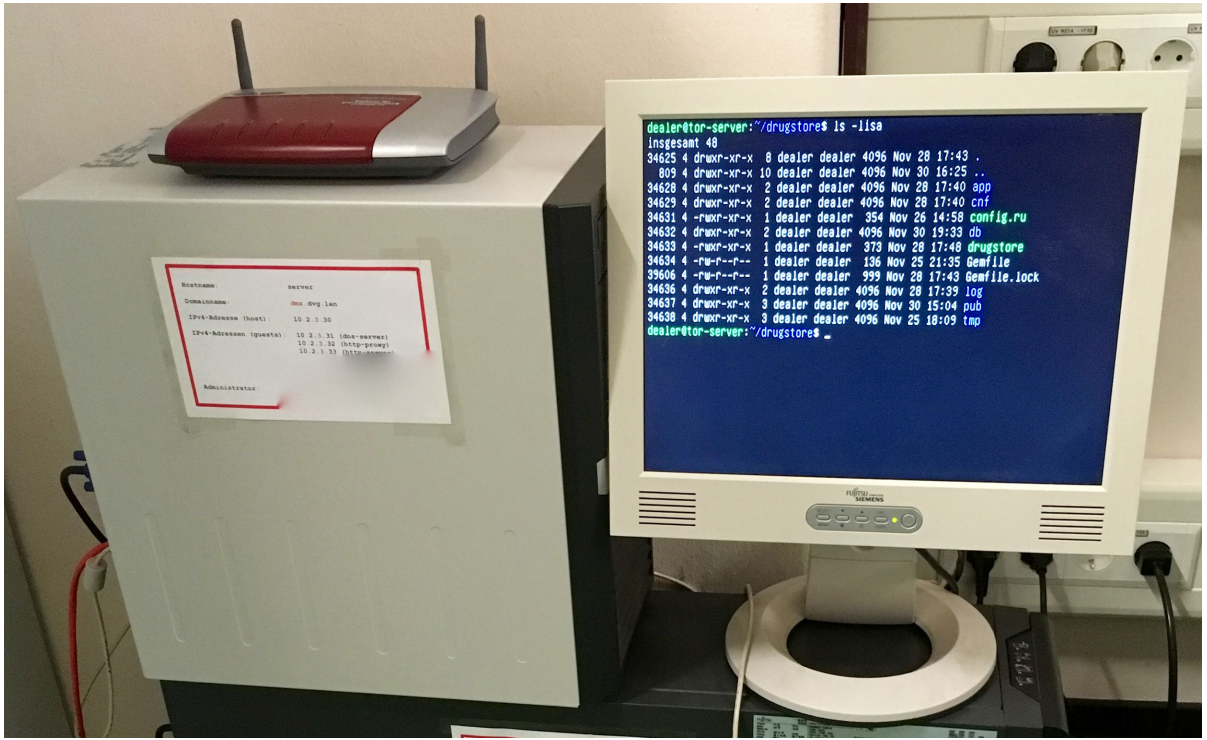
From our narrow selection:

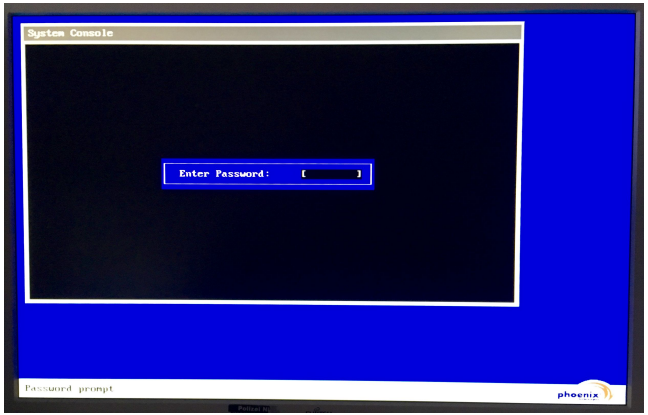
1. Data center
2. Virtual Server (cloud)
3. At home

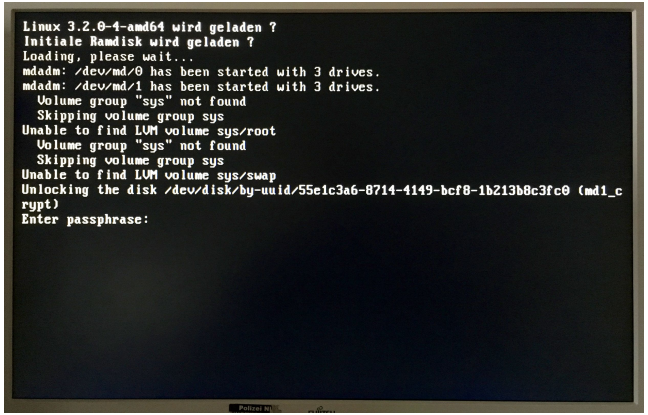
1. ISP does not accept anonymous payment/registration for a long running server
2. Lack of security
3. BIOS password and preboot authentication is possible

Because for a service the human is more less the source of errors we go with 3.

Would you like a little more than just theory?







OS (server)

From our narrow selection:

1. Microsoft Windows
2. Apple macOS
3. Linux

1. WAMP is not really suitable for production
2. To noble to corral it in a 19” rack
3. Able to use older hardware + production proofed

That’s why we go with 3.

(In special Debian/GNU Linux)

Some thoughts about configuration...

- disable booting from external devices in the BIOS
- protect the BIOS by a password
- because of reliability there should be two hard drives assembled as a software RAID 1
- only the boot partitions with the bootloader (incl. configuration), kernel image and initial ramdisk will be left unencrypted
- the raid for data will be encrypted
- to be able to connect the service to tor “tor” should be installed
- even though the system is encrypted it would be a good idea to deactivate logging as much as possible

THE WEBSHOP

From our narrow selection:

1. Apache + MySQL + PHP + Magento
2. Nginx + plain html + simplecardjs
3. Lighttpd + SQLite + ruby (selfmade)

1. To popular = to many Too many publicly known security holes
2. JavaScript is not really a secure solution for a webshop
3. We can skip unnecessary features, fake server signatures, … (We just need a little bit skill and time!)

That’s why we go with 3.

Would you like a little more than just theory?

drugstore

Suchen

Name	Änderungsdatum	Größe	Art
app	26.11.16, 01:15	--	Ordner
controllers.rb	Gestern, 20:51	3 KB	Ruby-Skript
models.rb	Gestern, 19:20	2 KB	Ruby-Skript
root.rb	28.11.16, 17:34	272 Byte	Ruby-Skript
views.rb	Gestern, 15:42	7 KB	Ruby-Skript
cnf	26.11.16, 13:18	--	Ordner
db.yml	28.11.16, 18:30	132 Byte	YAM...ment
thin.yml	26.11.16, 13:08	373 Byte	YAM...ment
config.ru	26.11.16, 14:58	354 Byte	Dokument
db	Gestern, 20:52	--	Ordner
drugstore.sqlite	Gestern, 20:52	131 KB	Dokument
drugstore	26.11.16, 13:08	346 Byte	Unix...table
Gemfile	25.11.16, 21:35	136 Byte	Text...ment
Gemfile.lock	25.11.16, 21:36	999 Byte	Dokument
log	25.11.16, 18:09	--	Ordner
pub	Gestern, 12:30	--	Ordner
favicon.ico	Gestern, 01:02	1 KB	Wind...lbild
img	Gestern, 11:31	--	Ordner
15zveKrrJWbp3BVpv36VWr1kPq3opNK6xf.png	Gestern, 11:00	4 KB	PNG-Bild
broken_cookies.jpg	Gestern, 11:31	29 KB	JPEG-Bild
dark_chocolate.jpg	Gestern, 11:31	9 KB	JPEG-Bild
salt_crystal.jpg	Gestern, 11:31	5 KB	JPEG-Bild
robots.txt	11.11.16, 22:10	26 Byte	Reiner Text
tmp	28.11.16, 17:54	--	Ordner

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>
```

aders Generator

HTTP Headers

http://wws2ga5k5e3

GET / HTTP/1.1
Host: wws2ga5k5e3
User-Agent: Mozilla
Accept: text/html,ap
Accept-Language: e
Accept-Encoding: g
Cookie: drugstore.s
Connection: keep-a

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 3111
Server: Microsoft-IIS/8.0
Date: Tue, 29 Nov 2016 13:17:19 GMT

Save All... Replay... Capture Clear Close

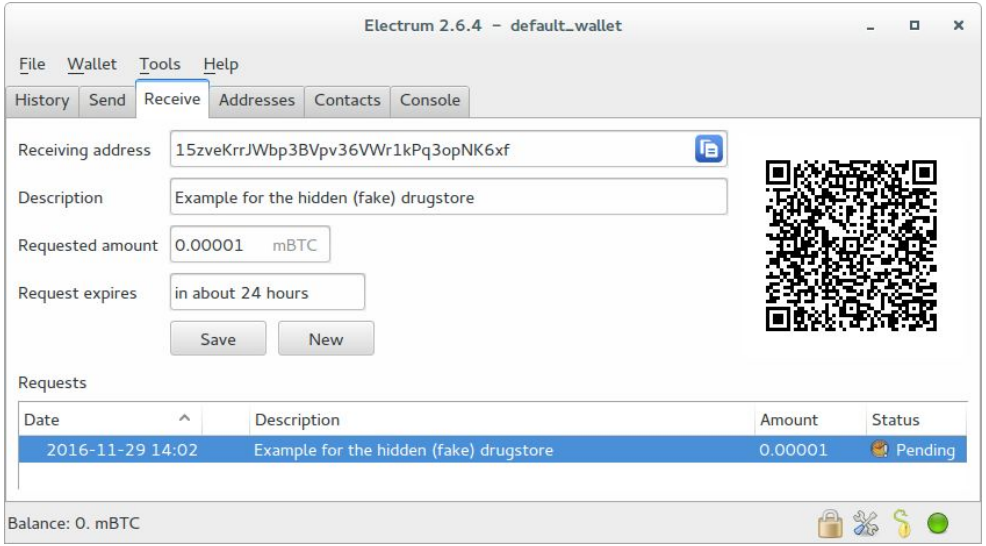
Payment

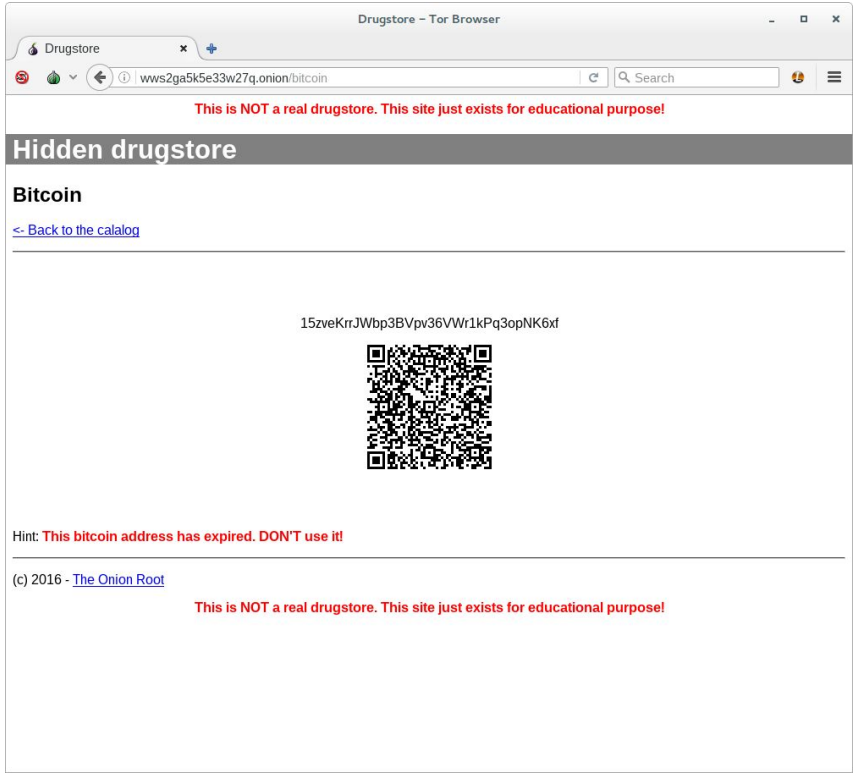
From our narrow selection:

1. Bank transfers
2. credit card or Paypal
3. Bitcoin

1. Leaves the possibility to track the way of the money
2. It’s difficult to have a 100% anonymous long running Paypal account
3. Is often used and relatively safe for anonymous payment

Would you like a little more than just theory?





Contact

From our narrow selection:

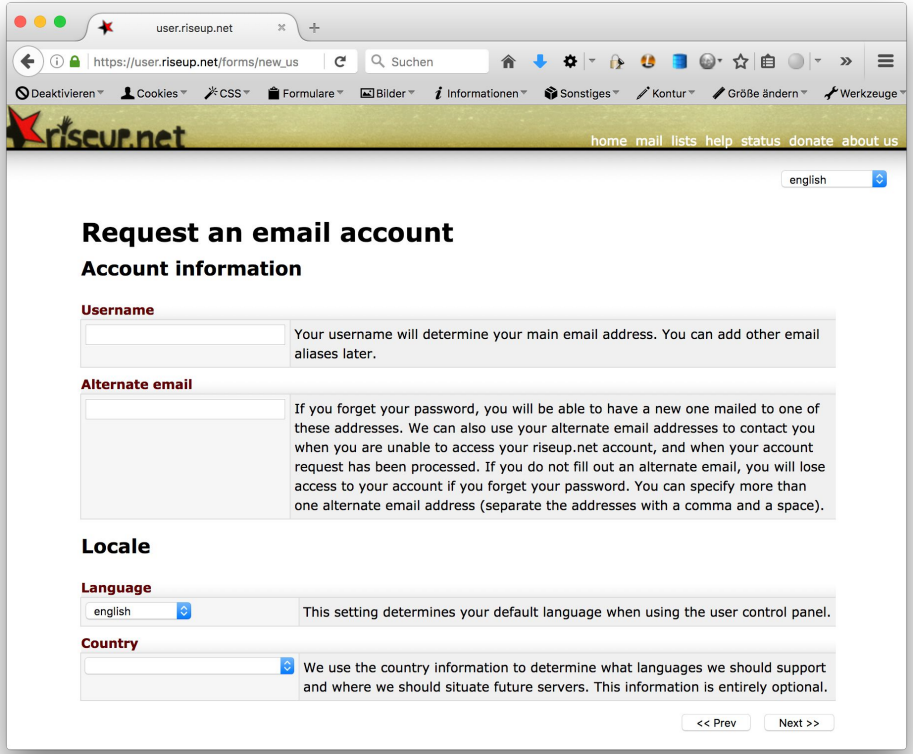
1. Regular email
2. Regular messenger
3. Anonymous email provider

1. Maybe cooperates really good with the government
2. ICQ messages goes through a Microsoft server and are observed by default
3. No questions while registrations, no logging, accessible through the tor network

That's why we go with 3.

(In special riseup.net)

Would you like a little more than just theory?




```
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)
```

Shipping

From our narrow selection:

1. Regular with cargo insurance and tracking
2. Just leave sender blank
3. leave sender blank and ship in letter size from different letter boxes

1. Maybe traceable to the sender (address)
2. Maybe traceable to the hometown
3. More distance between a lot of letter boxes and no fingerprints does not leave a lot for tracing

That’s why we go with 3.

Summary

- Smuggling
- Free WiFi (client)
- Tails (client)
  - Follow anti forensics guide
- Server at home
- Debian GNU/Linux (server)
  - A lot of configuration
- Lighttpd + SQLite + ruby + selfmade app
- Bitcoin
- Anonymous email provider (incl. Tor access)
- leave sender blank and ship in letter size from different letter boxes
- Never, never remove your gloves

What is the location of the server?

What person hides behind the-onion-root@riseup.net?