A TOUR THROUGH THE DARKSIDE OF THE INTERNET

Grifter and Metacortex

@grifter801

@metacortex

These
Guys

THESE GUYS

- Grifter (@grifter801)
  - DEF CON Goon
  - Multiple time DEF CON Speaker
  - DC801 Founder
  - Founder of 801 Labs Hacker Space in SLC

- Metacortex (@metacortex)
  - DC801 Organizer
  - Founder of the 801 Labs Hacker Space in SLC

- Seen us running around: DEF CON, Black Hat, BSides-SLC, SaintCON, ToorCon, ShmooCon

WARNING!!

- We **WILL** talk about some questionable content.
- We can not promise that you won't be offended.

- Content may include but not limited to
  - Drugs
  - Pornography
  - Counterfeit Material
  - Murder for Hire (hit men)
  - Money Laundering
  - Arms
  - Hacking
  - Cracking
  - Profanity

HERE IS WHAT WE WILL TALK ABOUT

- Tor
  - Connecting to it
  - Using it
  - Onion Sites
- Bitcoin
  - How Bitcoin works
  - How to use it
  - Mining bitcoin

HERE IS WHAT WE WILL TALK ABOUT

- How to find what you are interested in
  - Darknet Forums
    - Hacker/Carder Forums
  - Darknet Search Engines
  - Darknet Marketplaces

- Purchasing things you are interested in
  - How to stay anonymous when doing so

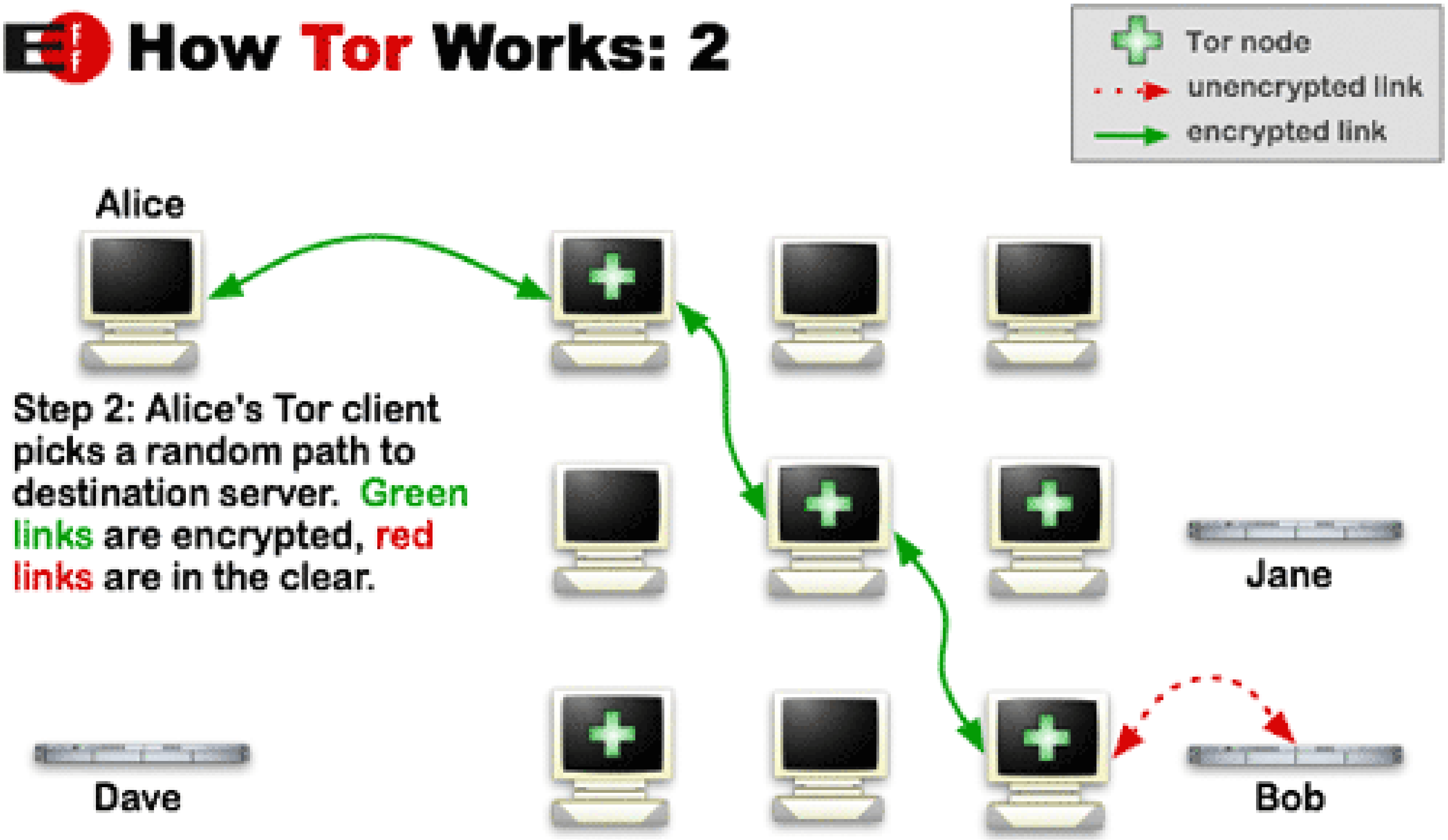
- Tips and tricks to be more anonymous and secure than nubs

TOR*

- The Onion Router
  - Primary Purpose: Anonymize Internet activity
  - Series of routers that anonymously forward traffic
    - Routers only knowledgeable about 1 hop in either direction

* Caution: Search of software classifies you as an “Extremist” in the eyes of the NSA, but honestly, what doesn’t?

How Tor Works: 2



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

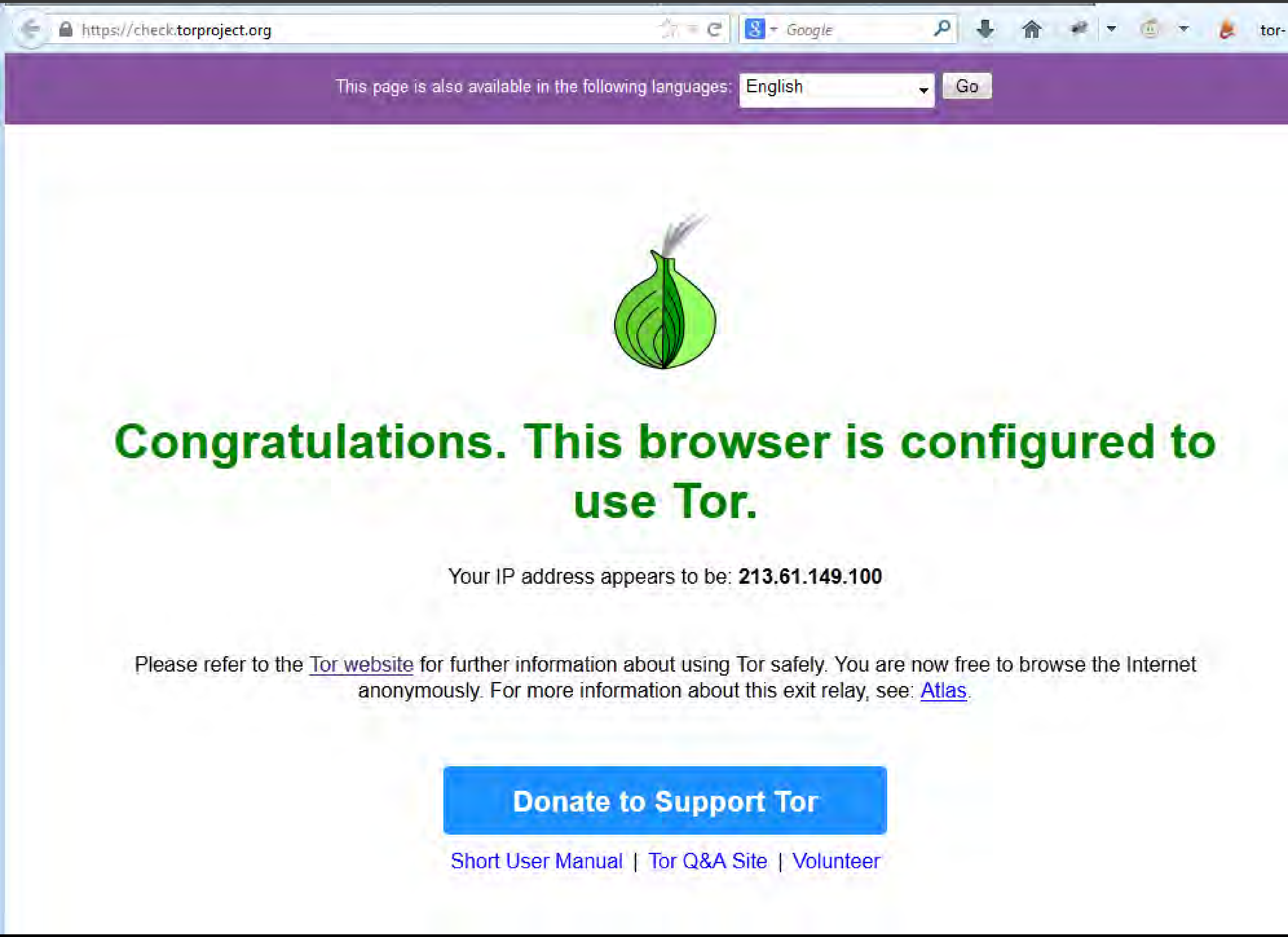
HOW DO YOU CONNECT TO THE TOR NETWORK

- CLI Daemon
  - apt-get install tor
    - /etc/tor/torrc
    - /etc/tor/tor-tsocks.conf
  - Starts socks5 proxy that you can point applications towards
    - Defaults to port 9050
- TorBrowser
  - Simple executable
  - Launches portable Firefox browser with select plugins

CLI CONNECTION

- /etc/init.d/tor start
  - Point Browser to 9050
  - Visit http://check.torproject.org for confirmation

- Configure tor through /etc/tor/torrc
  - Set up hidden services
  - Set up the port to listen on
  - Setup basic access lists for allowing other systems to connect to tor through you



https://check.torproject.org
Google
tor-

This page is also available in the following languages: English

Congratulations. This browser is configured to use Tor.

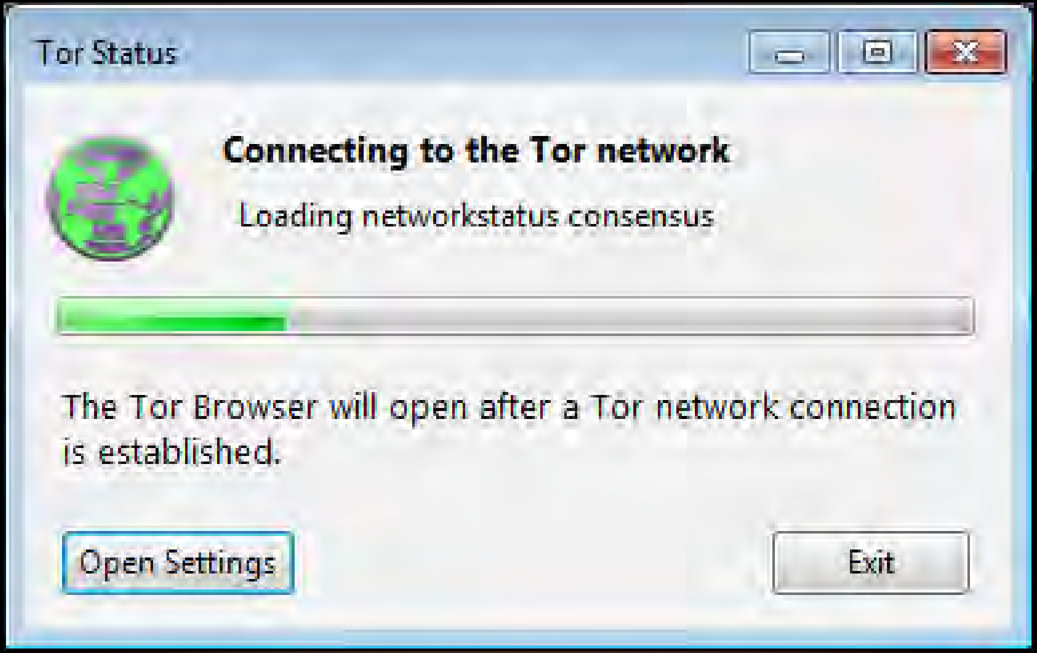
Your IP address appears to be: **213.61.149.100**

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Atlas.

Donate to Support Tor
Short User Manual | Tor Q&A Site | Volunteer

TORBROWSER

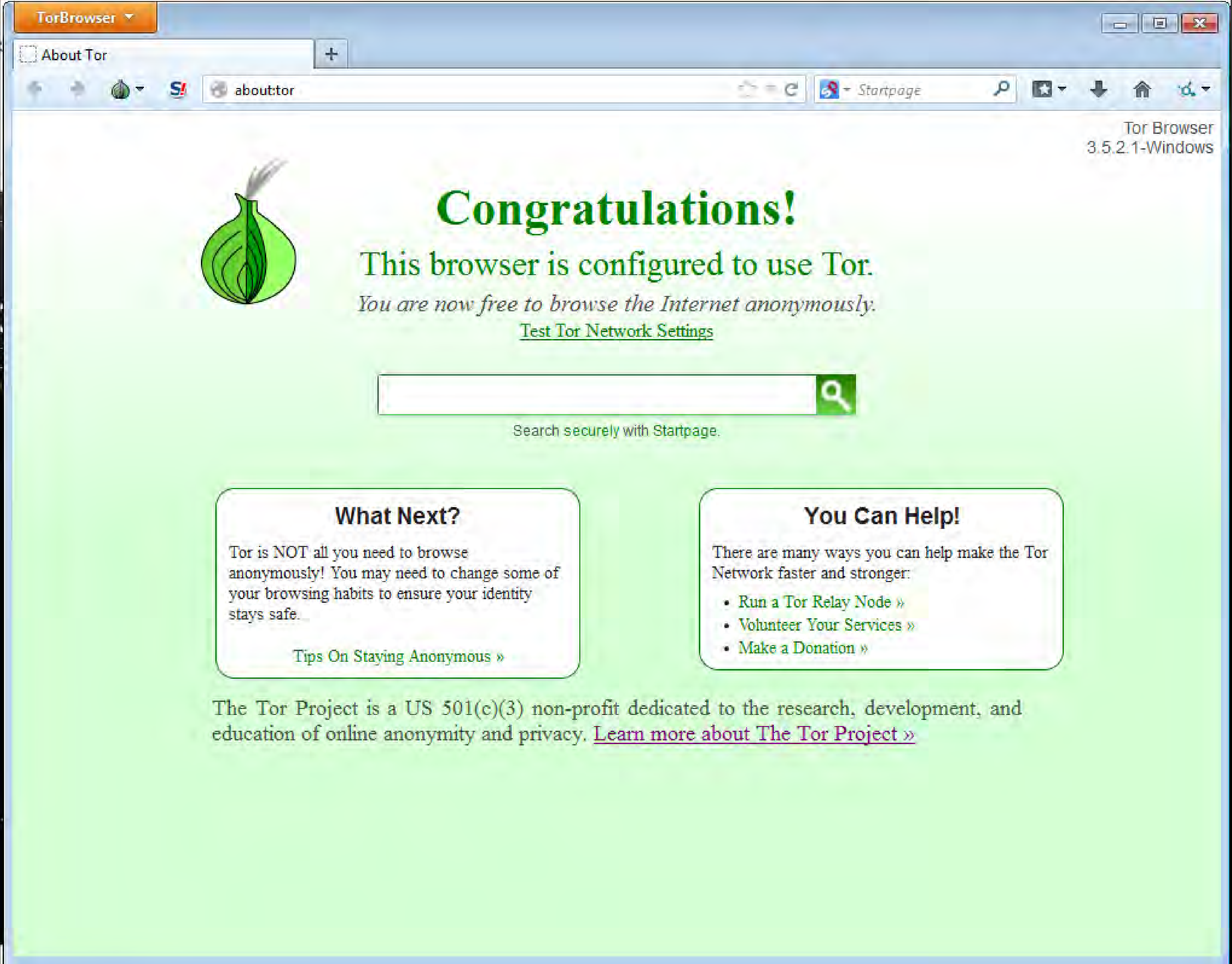
- Download at https://www.torproject.org/projects/torbrowser.html.en
  - Support for Windows, OSX, and Linux
- Run “Start Tor Browser.exe”



Connecting to the Tor network

Loading networkstatus consensus

The Tor Browser will open after a Tor network connection is established.



Tor Browser
3.5.2.1-Windows

Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

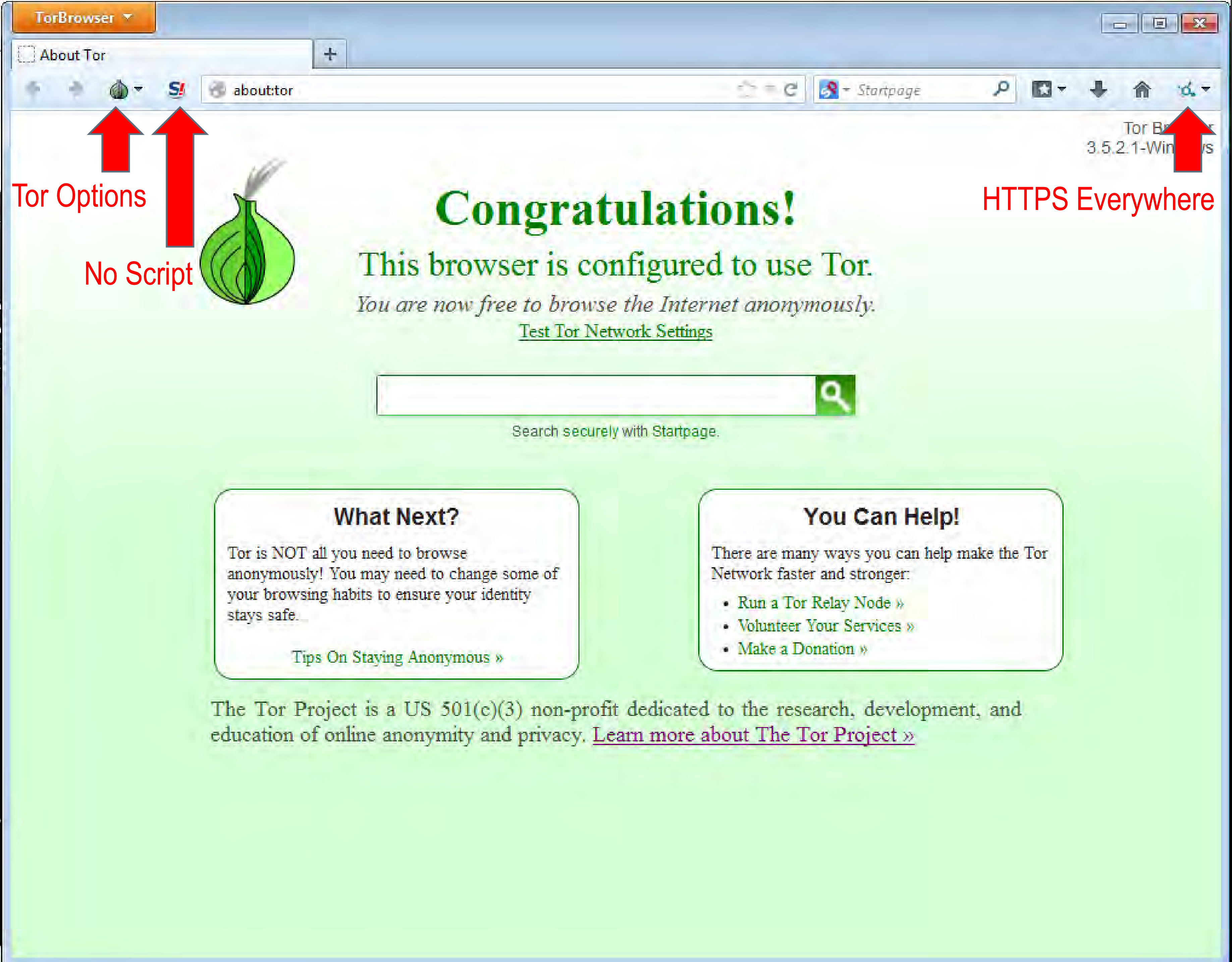
You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

DEMO CONNECTING TO TOR



Tor Options

No Script

HTTPS Everywhere

Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

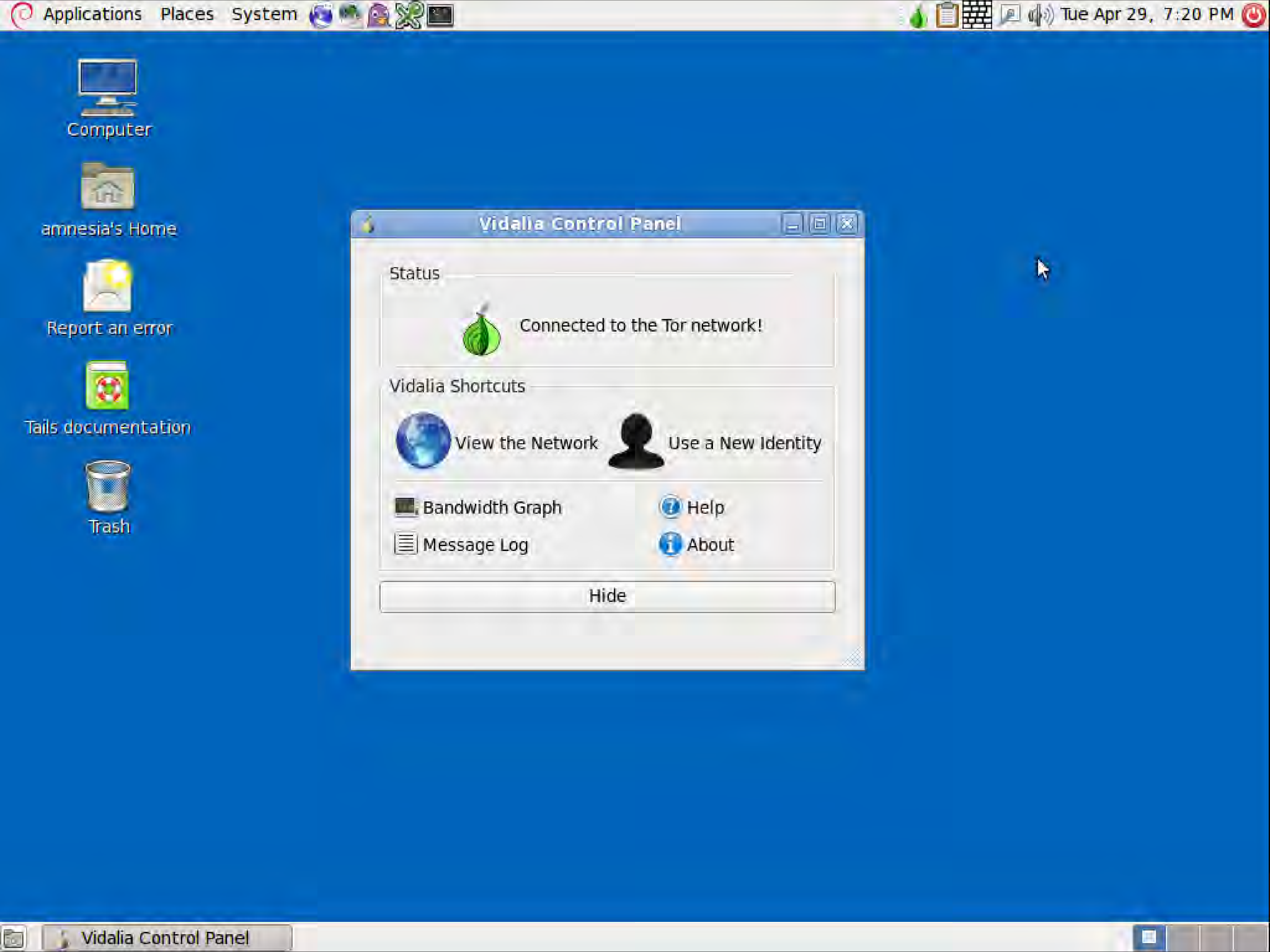
- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

TAILS*

- Linux Live distro (Debian) dedicated to staying anonymous.
- Forces all traffic through TOR
- Will not touch the hard disk (without a fight)
- Ability to disguise UI as Windows XP so it doesn't raise suspicions in public areas
- Comes with preinstalled software
  - HTTPS Everywhere plugin
  - OpenPGP
  - Pidgin OTR
  - Truecrypt
  - KeePassX

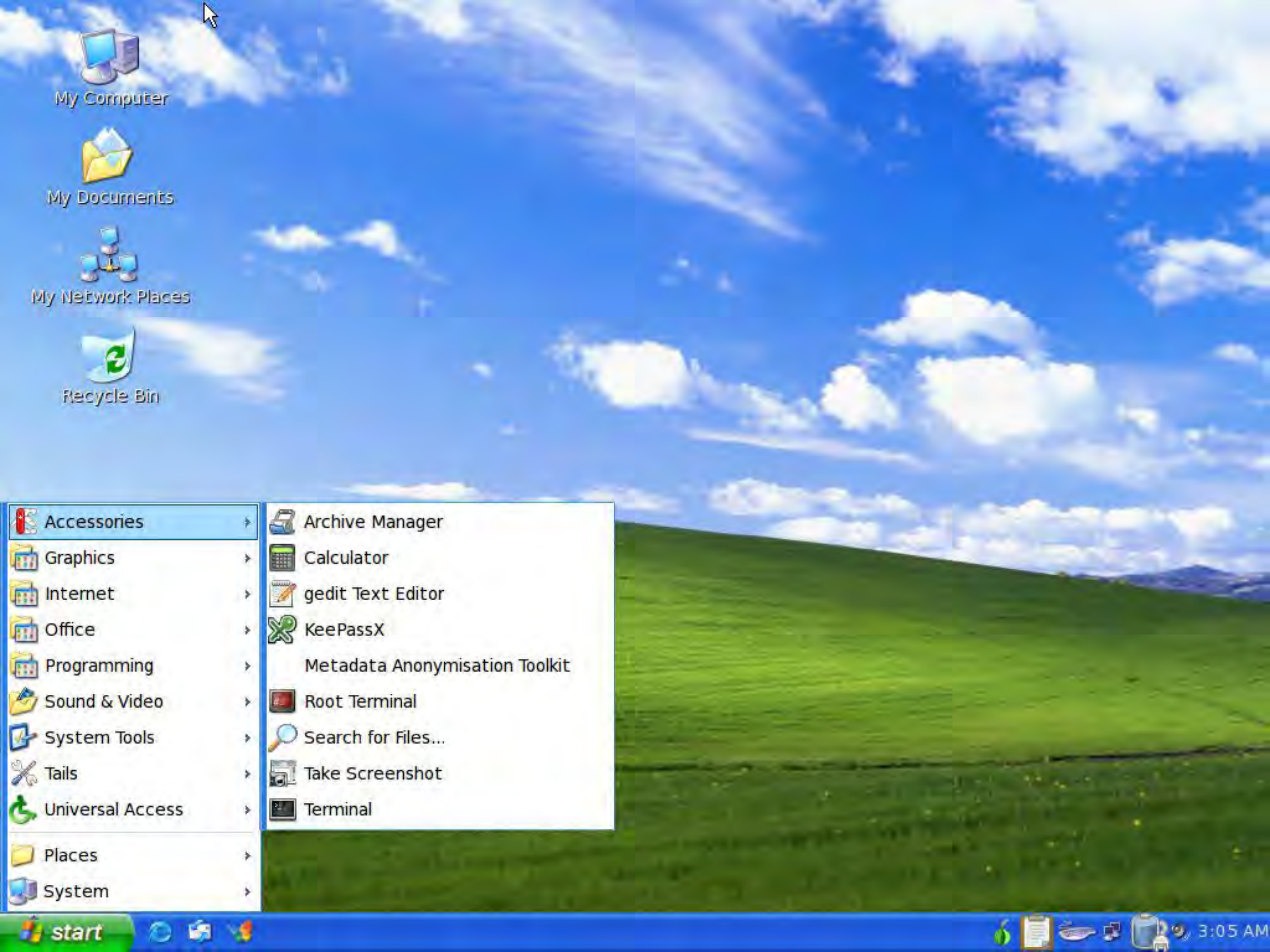
* Caution: Search of software classifies you as an "Extremist" in the eyes of the NSA



Vidalia Control Panel

Status

Connected to the Tor network!


My Computer
My Documents
My Network Places
Recycle Bin
Accessories
Graphics
Internet
Office
Programming
Sound & Video
System Tools
Tails
Universal Access
Places
System
Archive Manager
Calculator
gedit Text Editor
KeePassX
Metadata Anonymisation Toolkit
Root Terminal
Search for Files...
Take Screenshot
Terminal
start
3:05 AM

WE ARE CONNECTED…NOW WHAT?

- Browse the internet anonymously
- Tunnel out of restricted networks
- Fight Censorship
- Criticize Government/Government Officials
- Generally just stay anonymous
- Tor Hidden Services

TOR HIDDEN SERVICES

- Services that live only in the Tor Network
  - Turns Tor into a Darknet
- Services use .onion as TLD
- Put a pin in it mother fucker
- Fairly complex to explain how it still keeps anonymity so just see:
  - https://www.torproject.org/docs/hidden-services.html.en

FINDING HIDDEN SERVICES

- Hidden Wiki
  - http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- Torfind
  - http://ndj6p3asftxboa7j.onion/
- TorSearch
  - http://kbhpodhnfxl3clb4.onion/
- Grams – Google like search of the TOR darknet
  - http://grams7enufi7jmdl.onion/
- Deep Web Links ← NOT IN TOR
  - http://deepweblinks.org/
- Reddit ← NOT IN TOR
  - /r/onions
- Word of mouth

TORIFIED SITES/SITES OF INTEREST

- The Pirate Bay
  - http://jntlesnev5o7zysa.onion/
  - Caution:
    - Does no good if your Bittorrent client doesn’t go through Tor
- Assassination Market
  - http://www.assmkedzgorodn7o.onion/
  - Crowd Funded Assassinations
- Rent-A-Hacker
  - http://2ogmrlfzdthnwkez.onion/

HACKER FORUMS

- TCF – Tor Carding Forum
  - Trading CC's, CCV's, Identities
  - Some basic hacking info about RATS and shit
  - Requires ~ $50 purchase for access
  - http://6oa276dur6udwykp.onion/
- Intel Exchange
  - Mostly Trolling. Some decent information
  - http://rrcc5uuudhh4oz3c.onion
- HackBB
  - General Hacking/Tutorials/Nubs
  - http://jv7aqstbyhd5hqki.onion

MARKET PLACES

- What Tor Hidden Services are known for
- http://www.reddit.com/r/DarkNetMarkets
  - Most up to date listing in the sidebar
- Most Popular is Silkroad
  - Silkroad 2 is currently up after the takedown of the original
  - http://silkroad6ownowfk.onion/
- Agora
  - Decent selection of products
  - http://agorahooawayyfoe.onion
- Evolution
  - Our current favorite
  - http://k5zq47j6wd3wdvjq.onion

DEMO SILKROAD/EVOLUTION

CARDING SITES/FORUMS

- Tor Carding Forums (TCF).
  - http://6oa276dur6udwykp.onion
  - Requires ~ $50 purchase for access
- CC
  - http://carding2bil6j7ja.onion/cc

DEMO CARDING SITES

FAKE IDS

- Fake US Drivers Licenses
  - Scannable, Holograms, UV
  - http://en35tuzqmn4lofbk.onion/
- Fake Passports/Drivers Licenses
  - http://fakeidscpc4zz6c4.onion/
- Fake Passports
  - http://fakepasvv3holddd.onion/

- /r/fakeid
  - Not Tor specifically but you might want to use Tor

DEMO GRAMS

HOW DO YOU ACTUALLY GET ITEMS

- Bitcoin (BTC)
- Transfer BTC to the wallet on your marketplace account
  - Pay for items with that money
  - Money goes into Escrow
- Ship to pickup location
  - See the following OPSEC for further details

BITCOIN

- You’ve heard about it

- Online cryptocurrency
- You set up a digital wallet
  - Either local software or a web based wallet
    - I do not recommend a web based wallet.
- You can send up to 10 millionth of a bitcoin (8 decimal places or 0.00000001 BTC)
  - Not including fees
- You send to wallet addresses such as 146uk64ZP2iLsSBBPLzkY3xtCnuJg4yFsE

BUT REALLY

- BTC (or any cryptocurrency) boils down to a global transaction ledger maintained by the computational power of a P2P network.
  - The more people who participate in BTC the more secure it gets
  - Every transaction is logged by the peers in the P2P network
- Relies on PKI for authentication
  - Each wallet has a public and private key
  - When transactions are sent, they are signed with the private key

BITCOIN TUMBLING

- Tumbling or Mixing is the process of anonymizing bitcoin usage
    - Many parties put coins into communal pool
    - Pool distributes to different wallets
        - You get back the original amount of coins you put in (minus fee)

SOME CONSIDERATIONS FOR TOR

- Tor can in some cases reveal your true identity
  - Correlation
    - If someone owns both an entry and exit node, they can correlate between the two
  - Browser Exploits
    - Browser JavaScript engine
    - XSS
    - Pingbacks over non Tor connections

SOME CONSIDERATIONS FOR BITCOIN

- BTC is not a fully anonymous currency
  - Blockchain is PUBLIC
  - Use a tumbling service to further obfuscate the original source of your bitcoins
    - Don’t withdraw from a tumbler exactly what you put in
      - Spread out withdrawal amounts and send them to new wallet addresses

OPSEC

- Stay updated on the Tor Blog
  - https://blog.torproject.org
- Always keep Tor/TorBrowser updated
- Stay updated on status of current markets. The subreddit is FANTASTIC for that
- Browser segregation
  - Don’t be logging into social media sites in the same browser you don’t want to be tracked on
  - Use a VM specifically for Tor connections (Tails)
  - Even better:
    - Specifically boot into a trusted OS instead of VM as host OS has full VM visibility

OPSEC CONTINUED

- Receiving Items
  - Don’t send to your house
    - Send to PO Box or UPS Store.
      - UPS Store will sign for items on your behalf!
    - If you have access to an empty house/building, look into sending it there.
  - NEVER open questionable content anywhere you are visible by others
    - Wait till you get home
  - Try waiting a week or two to pick up an item
    - Foils stakeouts as no one will stakeout a Post Office 24/7 for 2 weeks
    - If you want, walk in and confirm item is there and come back later

EVEN MORE OPSEC!

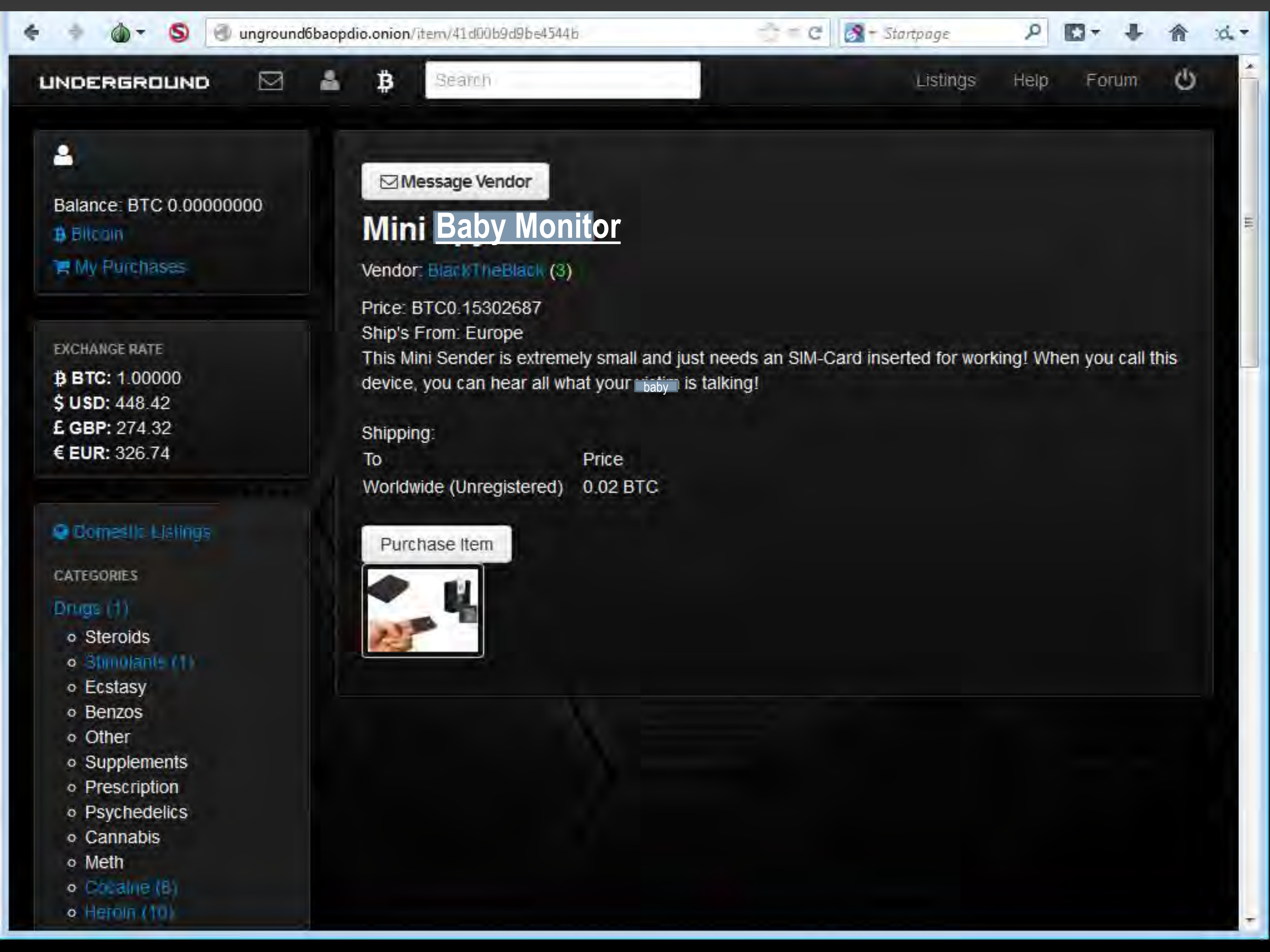
- Identities
    - Don’t reuse identities
    - Don’t reuse passwords
    - Use disposable emails
        - http://www.sharklasers.com/ & https://www.guerrillamail.com/

MAKING MAILBOXES MORE ANONYMOUS

- Purchase mailbox
- Buy fake ID using mailbox
- Burn mailbox
- Open new mailbox at different location using Fake ID
- Enjoy more anonymous receiving

WE BOUGHT SOME STUFF

- Mini Discreet…“Baby Monitor”
- Runs over the GSM network by inserting a sim card
- Call the associated number to instantly listen to the room
  - Or sms “1111” to turn on auto dial back
  - Sms “0000” to disable dial back



Balance: BTC 0.00000000

EXCHANGE RATE

₿ **BTC:**	1.00000
$ **USD:**	448.42
£ **GBP:**	274.32
€ **EUR:**	326.74

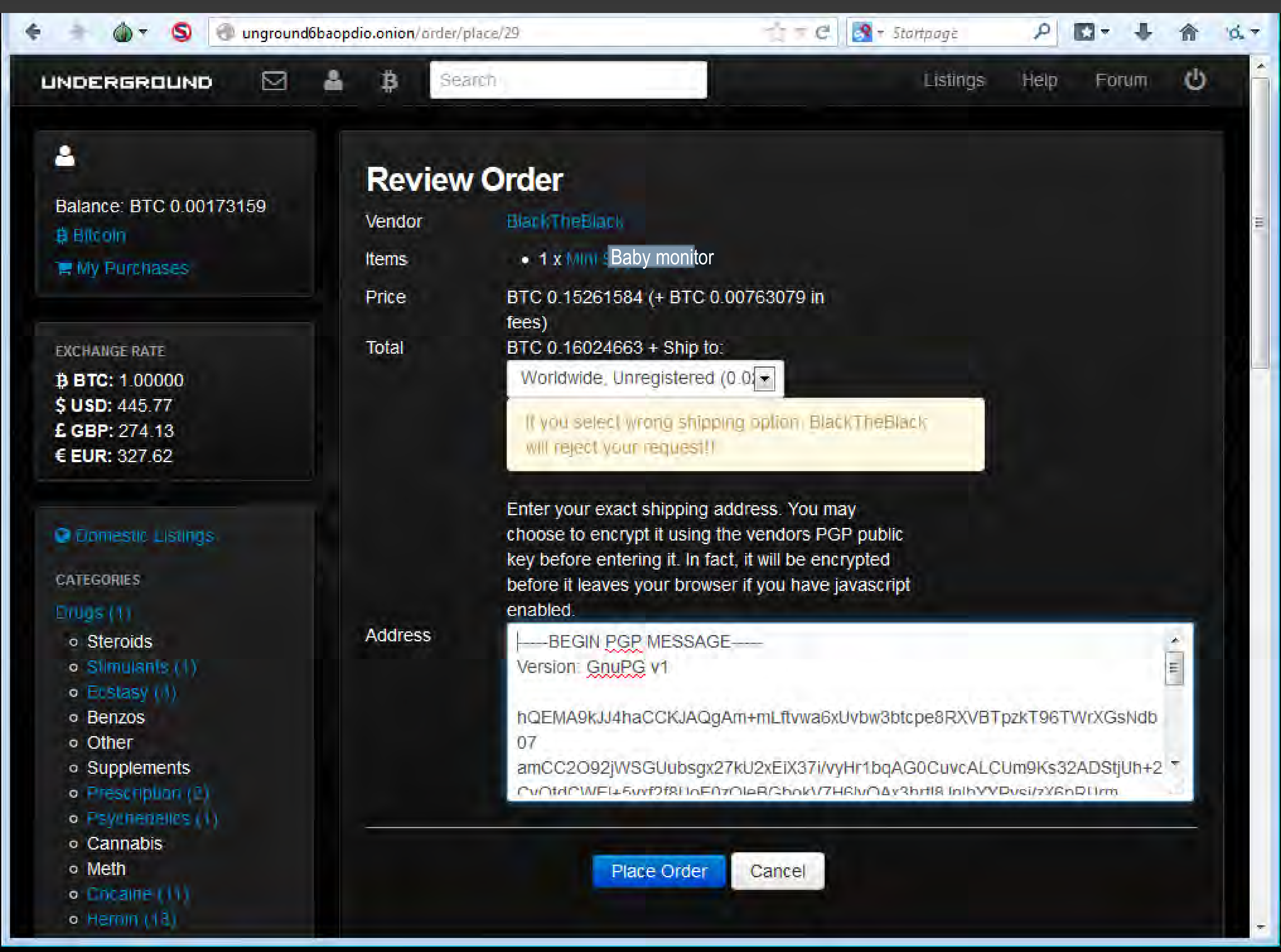
Mini Baby Monitor

Vendor: BlackTheBlack (3)

Price: BTC0.15302687
Ship's From: Europe
This Mini Sender is extremely small and just needs an SIM-Card inserted for working! When you call this device, you can hear all what your baby is talking!

Shipping:

To	Price
Worldwide (Unregistered)	0.02 BTC



Balance: BTC 0.00173159

EXCHANGE RATE

฿ **BTC:** 1.00000
$ **USD:** 445.77
£ **GBP:** 274.13
€ **EUR:** 327.62

Review Order

Vendor	BlackTheBlack
Items	• 1 x Mini S Baby monitor
Price	BTC 0.15261584 (+ BTC 0.00763079 in fees)
Total	BTC 0.16024663 + Ship to: Worldwide, Unregistered (0.0

If you select wrong shipping option, BlackTheBlack will reject your request!!

Enter your exact shipping address. You may choose to encrypt it using the vendors PGP public key before entering it. In fact, it will be encrypted before it leaves your browser if you have javascript enabled.

Address

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

hQEMA9kJJ4haCCKJAQgAm+mLftvwa6xUvbw3btcpe8RXVBTpzkT96TWrXGsNdb
07
amCC2O92jWSGUubsgx27kU2xEiX37i/vyHr1bqAG0CuvcALCUm9Ks32ADStjUh+2
CvOtdCWEl+5wf2f8UoF0zOleBGbokV7H6lvOAx3hrl8 InlbYYPysi/zX6pRUm
```

Hello

your item has been shipped to this address:

XXXXXXXX
Salt Lake City UT XXXXX
United States

Estimated delivery is between Wednesday, May. 14 and Thursday, May. 22

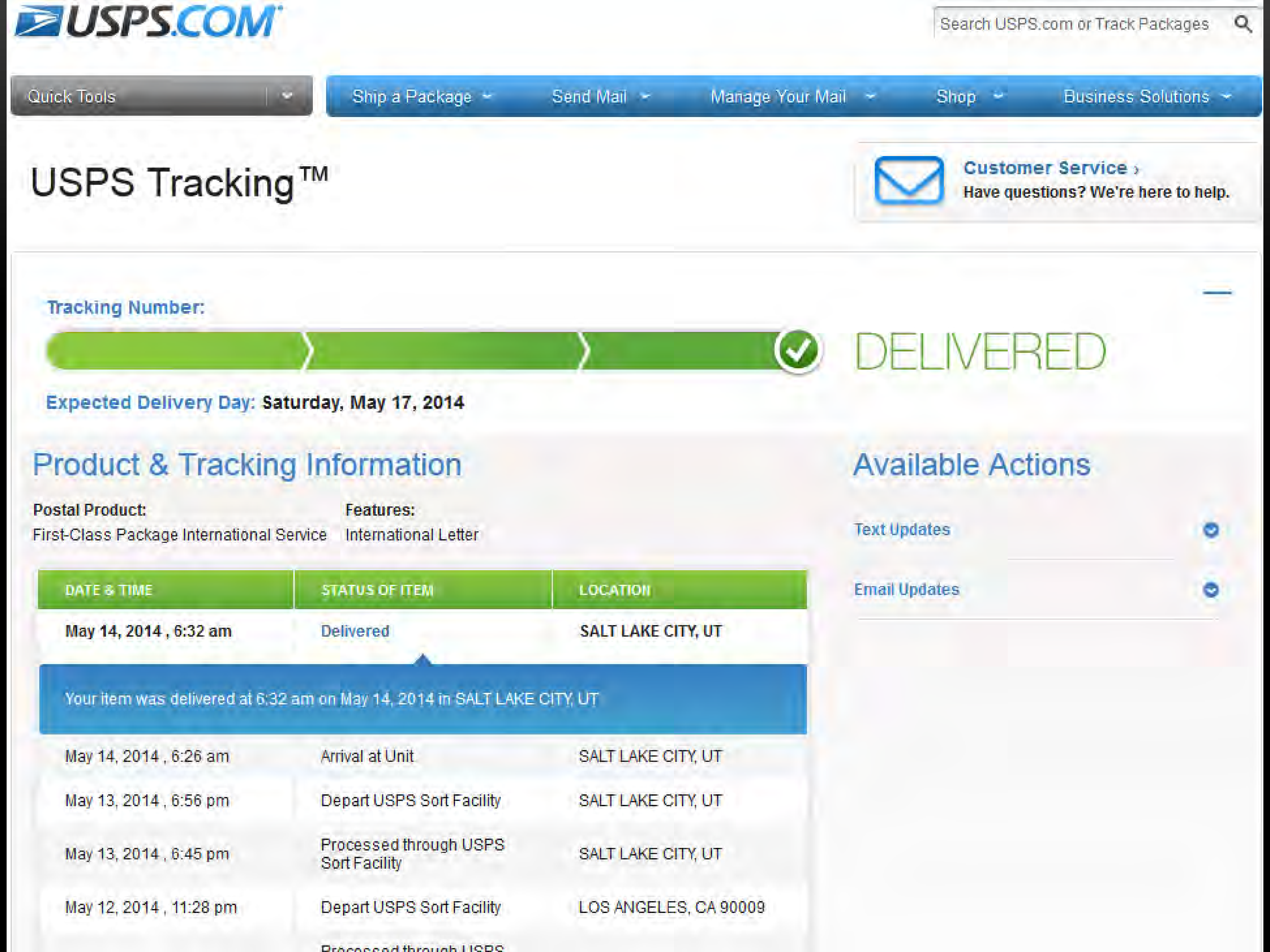
This is how you use the device:

- Open the back cover. Sim card into the deck will automatically boot.boot light is 3 seconds. after the lights go off you can dial the sim card number.
Installation:Please confirm the GSM network signal strength.So as not to affect the results cause can not be used

- Number of settings: call the sim card numer with mobilephone or telephone,hang up then setting success

- Voice feature:Send â1111â0000â

- The flash of red light indicates the SIM card is correctly inserted. SIM will completed initialization and maintain in stand-by status and the light will be off and it is ready to go



USPS Tracking™

Tracking Number:

DELIVERED

Expected Delivery Day: **Saturday, May 17, 2014**

Product & Tracking Information

Postal Product:
First-Class Package International Service

Features:
International Letter

DATE & TIME	STATUS OF ITEM	LOCATION
May 14, 2014 , 6:32 am	Delivered	**SALT LAKE CITY, UT**
Your item was delivered at 6:32 am on May 14, 2014 in SALT LAKE CITY, UT		
May 14, 2014 , 6:26 am	Arrival at Unit	SALT LAKE CITY, UT
May 13, 2014 , 6:56 pm	Depart USPS Sort Facility	SALT LAKE CITY, UT
May 13, 2014 , 6:45 pm	Processed through USPS Sort Facility	SALT LAKE CITY, UT
May 12, 2014 , 11:28 pm	Depart USPS Sort Facility	LOS ANGELES, CA 90009
	Processed through USPS	

Available Actions

PARTING THOUGHTS

- Clearly a lot of this talk falls into a gray area
- Darknets, like anything, can be use for “good” and “evil”
- These networks have legit purposes and not just for shady shit
- In our view, these networks are the future of how we will communicate online

SHAMELESS SELF PROMOTION

- Come visit us at 801 Labs and DC801 events
- Hit us up on twitter @dc801, @grifter801, and @metacortex
- Come hang out with us on IRC. #dc801 on the FreeNode network

DC801

801 LABS

APPENDIX A: BITCOIN MINING

- To cut down on computation of all the transactions globally, participants (nodes) group transactions unconfirmed transactions into “blocks” and suggests what the next block should be
- To keep too many people from creating blocks is to make them difficult to create.
  - Node creates block of grouped transactions and adds reference to previous block
    - SHA256 of the previous block
  - A “nonce” (random number) is appended to the block and hashed twice
    - SHA256(SHA254(block+nonce))
  - Each block hash has to be inferior to the current network difficulty
  - Once the hash of a block + nonce is less than the network difficulty, the block is submitted to the BlockChain (ledger of transactions)
- Mining is the process of brute forcing nonce’s in order to submit a block to the blockchain

APPENDIX A CONT: BITCOIN MINING REWARD

- Reward for successfully submitting a block to the blockchain is 25 BTC

APPENDIX A CONT2: BITCOIN MINING IS HARD

- In the very beginning people were mining on their CPU’s
    - Network difficulty started rising
- CUDA came around
    - People started mining on their Video Cards (much faster)
        - Network difficulty kept rising
- Mining Pools are created to share the computational load
- People started building big mining rigs of several Video Cards
    - Network difficulty continued to rise
- Custom BTC mining FPGA’s were created
    - Network difficulty is fairly high at this point
- Custom BTC mining ASIC’s are created

MORE APPENDIX A: CURRENT STATE OF MINING

- Unless you are running mid to high-end ASIC's you will be spending more in electricity than what you will gain back in BTC
- You will never submit a block to the blockchain on your own
  - Join a pool