OFFICIAL (ISC)² CHAPTER

(ISC)² CHAPTER HELLENIC

The faces of Tor

Anonymity and Crime

Christos Ventouris
Cventouris papaki isc2 pavla chapter telia gr

5th InfoCom Security
April 1st, 2015

Why use Tor

- Internet surveillance threats user’s privacy
- Encryption alone does not work, since packet headers still reveal a great deal about users.
- The need from End-to-end anonymity.
  - Both sides (client and service offered)

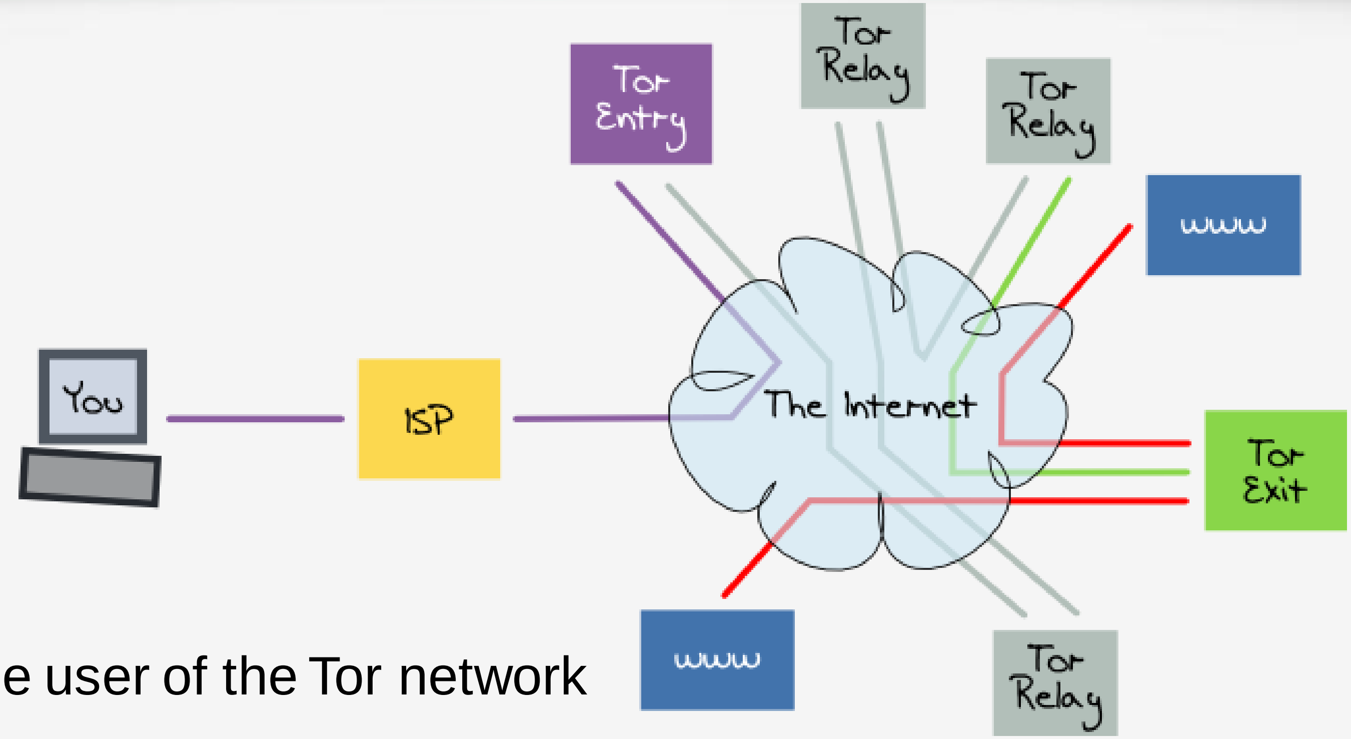
What is Tor

- Distributed anonymous communication service using an overlay network that allows people and groups to improve their privacy and security on the Internet.
- Individuals use Tor to keep websites from tracking them, or to connect to those internet services blocked by their local Internet providers.
- Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site.

Who uses Tor

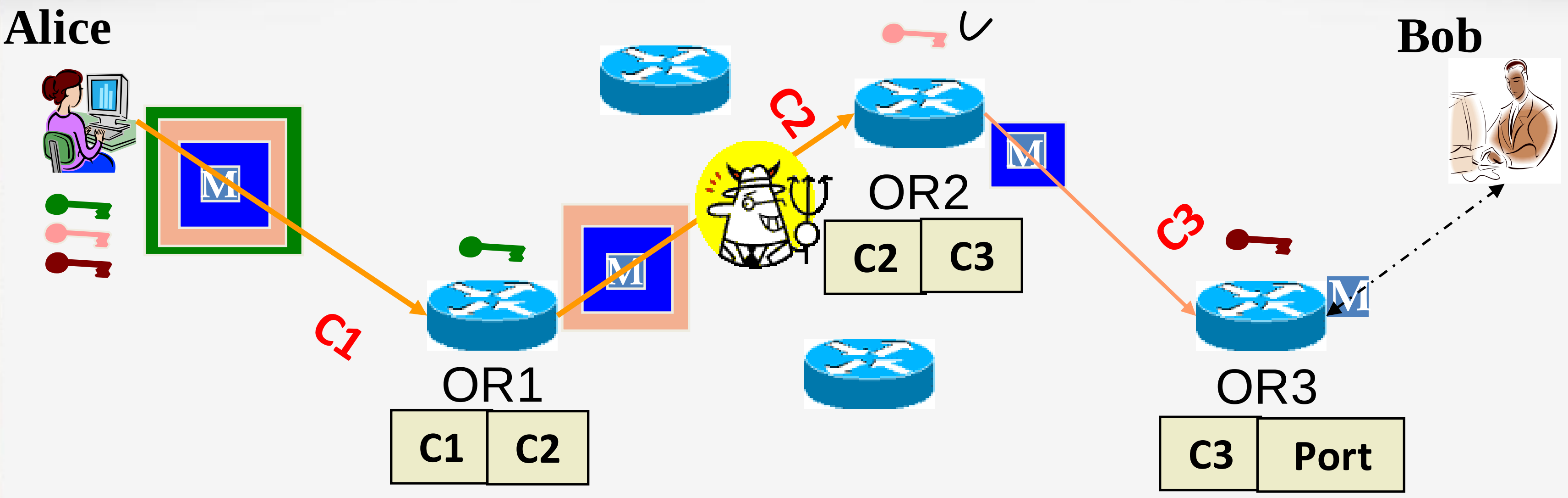
- Normal People
  - Privacy
  - Circumvent Censorship
- Journalists
  - Citizen Journalism
  - Communicate with tippers
- Law Enforcement
  - Tip Lines
  - Sting Operations
- Activists / Whistleblowers
- Military
- Bloggers

Components



- **You** : the user of the Tor network
- **www**: the target TCP applications such as www in our example
- **Tor Relay**: the special proxy relays the application data
- **Directory server**: servers holding Tor router information

The Onion Routing Concept



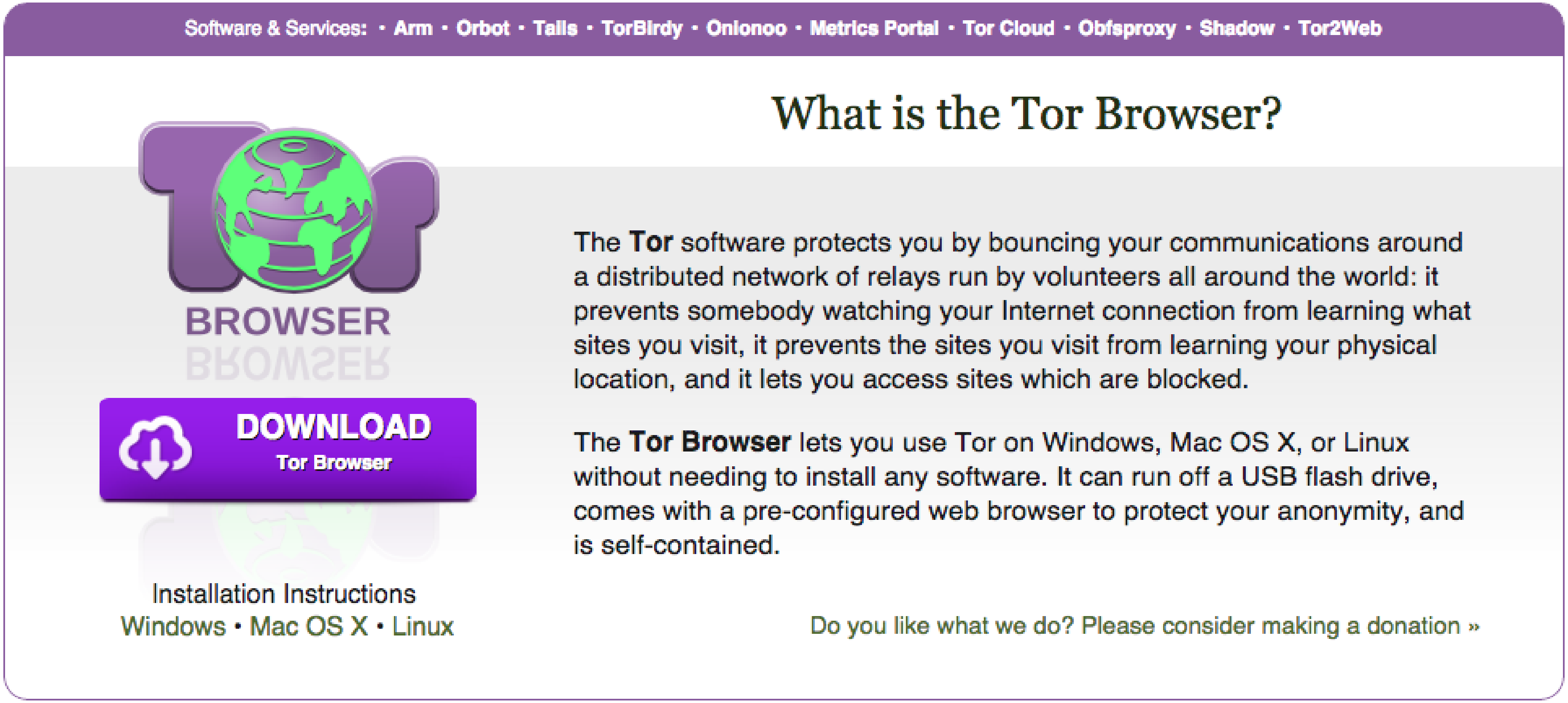
- The circuit is established hop by hop
  - Alice negotiates an AES key with each router
  - Messages are divided into equal sized cells
  - Each router knows only its predecessor and successor
  - Only the Exit router (OR3) can see the message, however it does not know where the message is from

Additional functionality

- Integrity checking
  - Only done at the edges of a stream
  - SHA-1 digest of data sent and received
  - First 4 bytes of digest are sent with each message for verification
- Congestion Control
  - OR-to-OR congestion might happen if too many users choose the same OR-to-OR connection.
  - Circuit Level throttling

Using Tor

https://www.torproject.org/projects/torbrowser.html.en



Software & Services: · Arm · Orbot · Tails · TorBirdy · Onionoo · Metrics Portal · Tor Cloud · Obfsproxy · Shadow · Tor2Web

What is the Tor Browser?

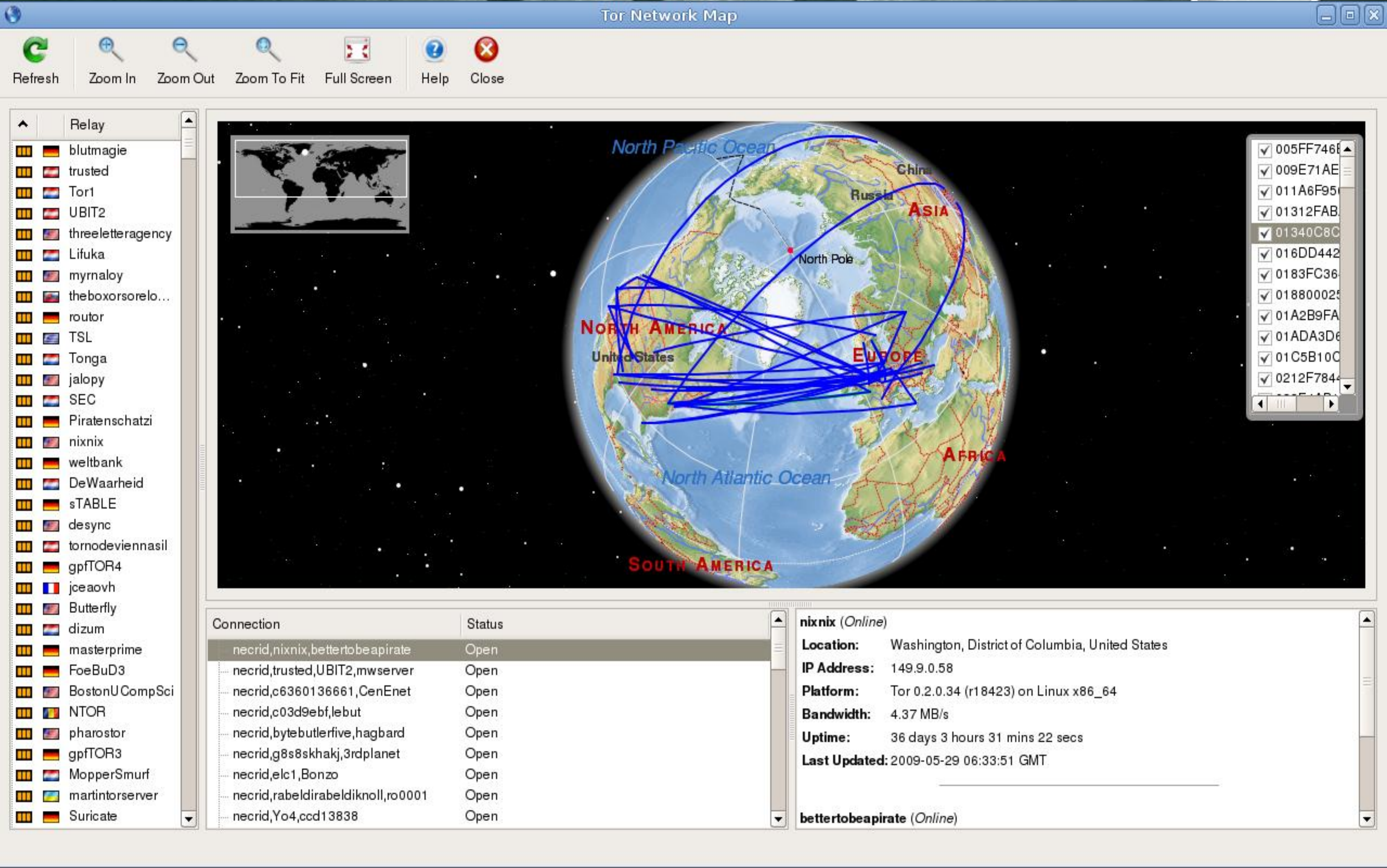
The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

The **Tor Browser** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.

Installation Instructions
Windows • Mac OS X • Linux

Do you like what we do? Please consider making a donation »

Using Tor



Relay
blutmagie
trusted
Tor1
UBIT2
threeletteragency
Lifuka
myrnaloy
theboxorsorelo...
routor
TSL
Tonga
jalopy
SEC
Piratenschatzi
nixnix
weltbank
DeWaarheid
sTABLE
desync
tornodeviennasil
gpfTOR4
jceaovh
Butterfly
dizum
masterprime
FoeBuD3
BostonUCompSci
NTOR
pharostor
gpfTOR3
MopperSmurf
martintorserver
Suricate

☑ 005FF746E
☑ 009E71AE
☑ 011A6F95
☑ 01312FAB
☑ 01340C8C
☑ 016DD442
☑ 0183FC36
☑ 01880002
☑ 01A2B9FA
☑ 01ADA3D6
☑ 01C5B10C
☑ 0212F784

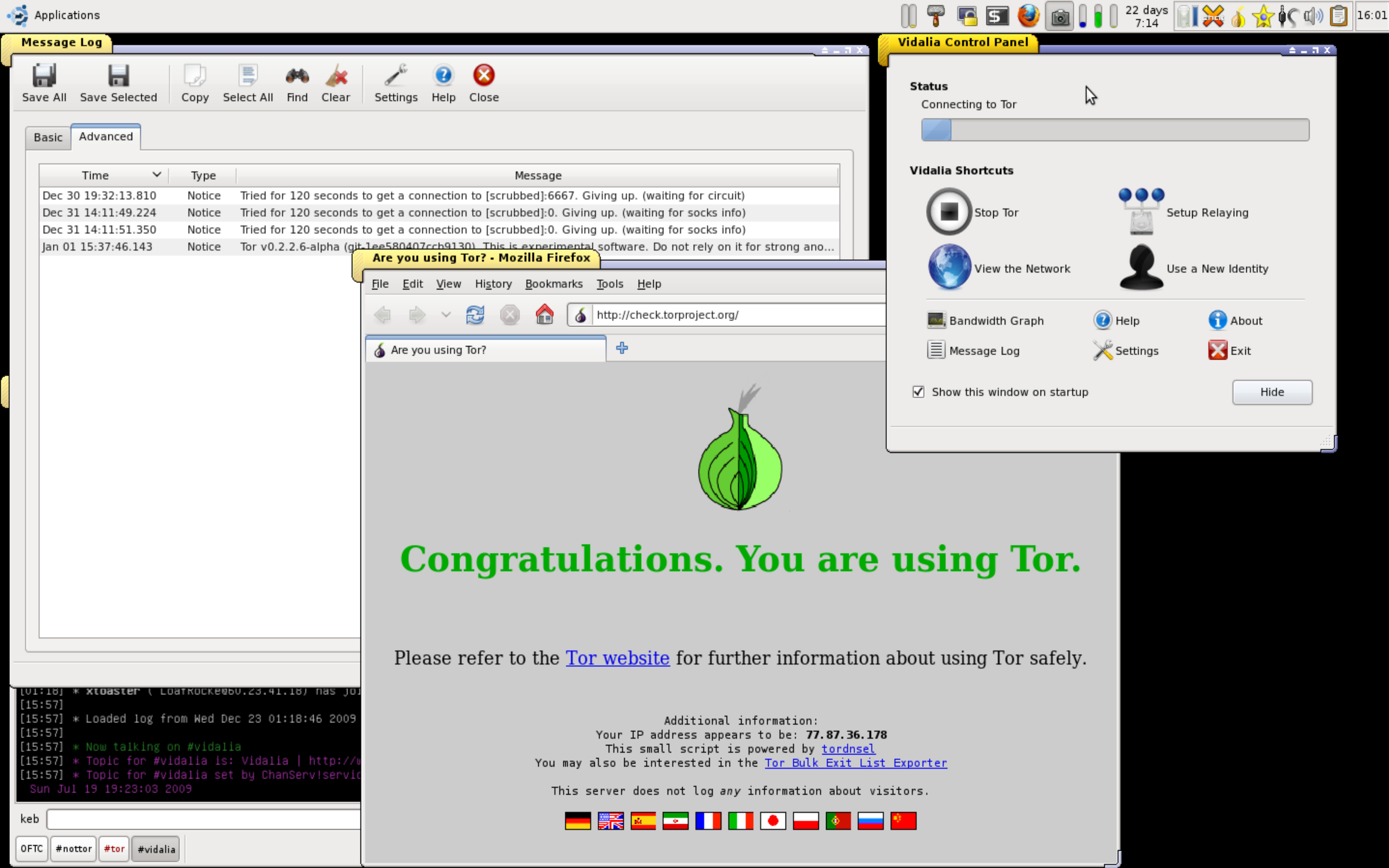
Connection	Status
necrid,nixnix,bettertobeapirate	Open
necrid,trusted,UBIT2,mwserver	Open
necrid,c6360136661,CenEnet	Open
necrid,c03d9ebf,lebut	Open
necrid,bytebutlerfive,hagbard	Open
necrid,g8s8skhakj,3rdplanet	Open
necrid,elc1,Bonzo	Open
necrid,rabeldirabeldiknoll,ro0001	Open
necrid,Yo4,ccd13838	Open

nixnix (*Online*)

Location:	Washington, District of Columbia, United States
IP Address:	149.9.0.58
Platform:	Tor 0.2.0.34 (r18423) on Linux x86_64
Bandwidth:	4.37 MB/s
Uptime:	36 days 3 hours 31 mins 22 secs
Last Updated:	2009-05-29 06:33:51 GMT

bettertobeapirate (*Online*)

Using Tor



Time	Type	Message
Dec 30 19:32:13.810	Notice	Tried for 120 seconds to get a connection to [scrubbed]:6667. Giving up. (waiting for circuit)
Dec 31 14:11:49.224	Notice	Tried for 120 seconds to get a connection to [scrubbed]:0. Giving up. (waiting for socks info)
Dec 31 14:11:51.350	Notice	Tried for 120 seconds to get a connection to [scrubbed]:0. Giving up. (waiting for socks info)
Jan 01 15:37:46.143	Notice	Tor v0.2.2.6-alpha (git-1ee580407ccb9130). This is experimental software. Do not rely on it for strong ano...

```
[01:18] * xtoaster ( LoafRocke@60.23.41.18) has joi
[15:57]
[15:57] * Loaded log from Wed Dec 23 01:18:46 2009
[15:57]
[15:57] * Now talking on #vidalia
[15:57] * Topic for #vidalia is: Vidalia | http://v
[15:57] * Topic for #vidalia set by ChanServ!servic
  Sun Jul 19 19:23:03 2009
```

Congratulations. You are using Tor.

Please refer to the Tor website for further information about using Tor safely.

Additional information:
Your IP address appears to be: **77.87.36.178**
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log *any* information about visitors.

Status

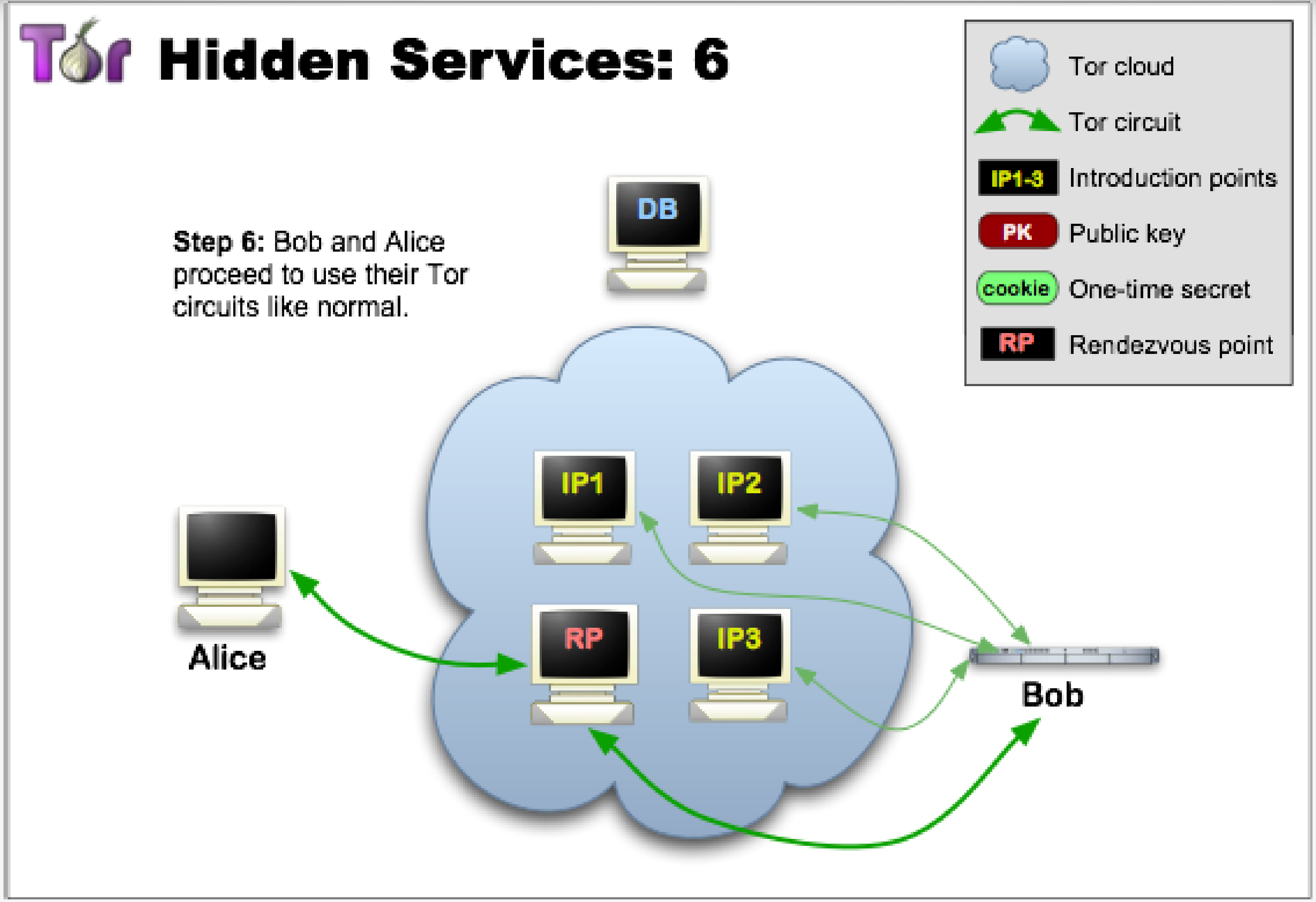
Connecting to Tor

☑ Show this window on startup

Hidden Services

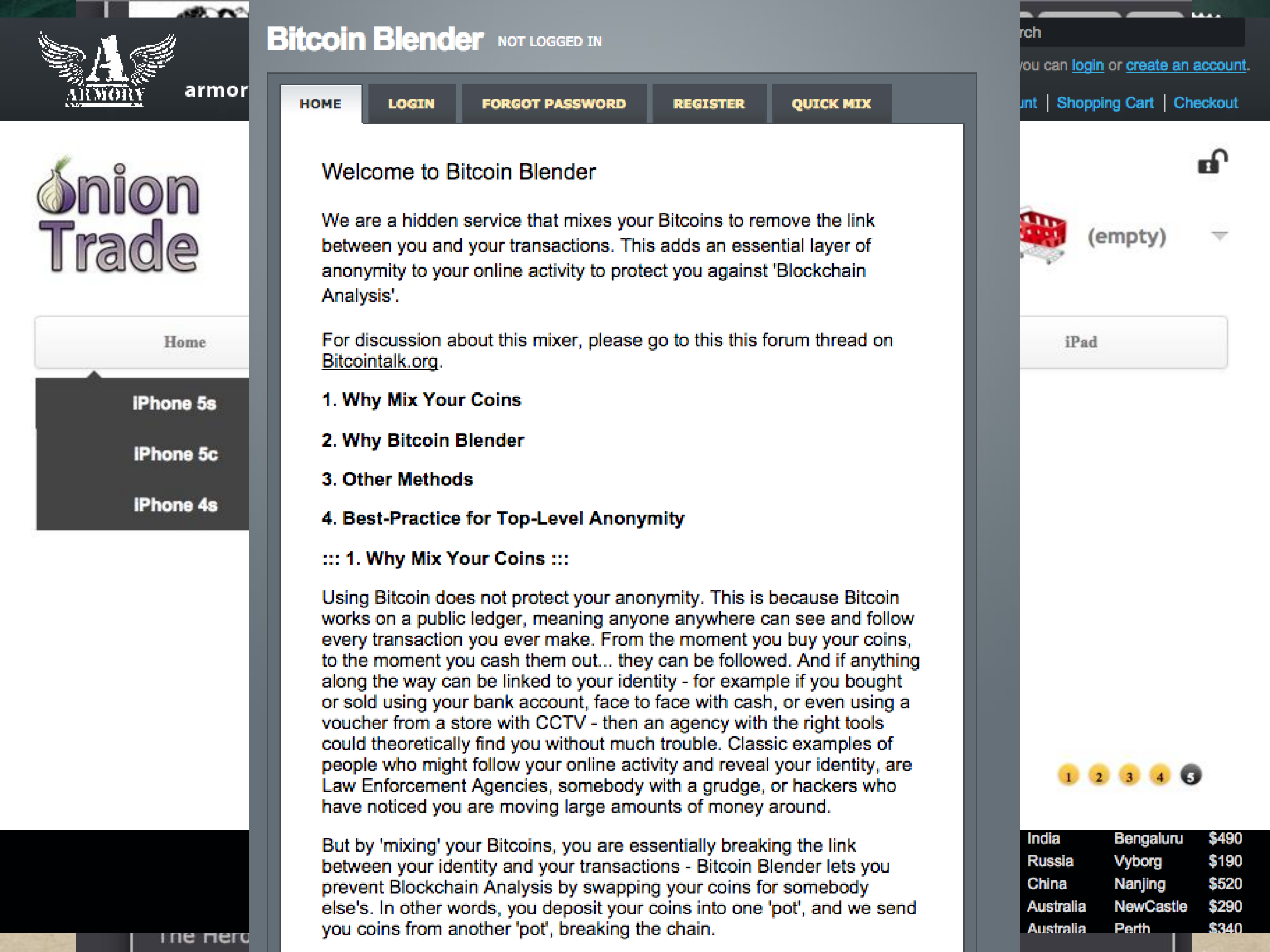
- Allows an online service to become anonymous
  - Domains in .onion resolved only by Tor Directory Servers.
  - Leverage “Rendezvous” points
  - Both clients and servers achieve anonymity.

Hidden Services



Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



Welcome to Bitcoin Blender

We are a hidden service that mixes your Bitcoins to remove the link between you and your transactions. This adds an essential layer of anonymity to your online activity to protect you against 'Blockchain Analysis'.

For discussion about this mixer, please go to this this forum thread on Bitcointalk.org.

1. Why Mix Your Coins

2. Why Bitcoin Blender

3. Other Methods

4. Best-Practice for Top-Level Anonymity

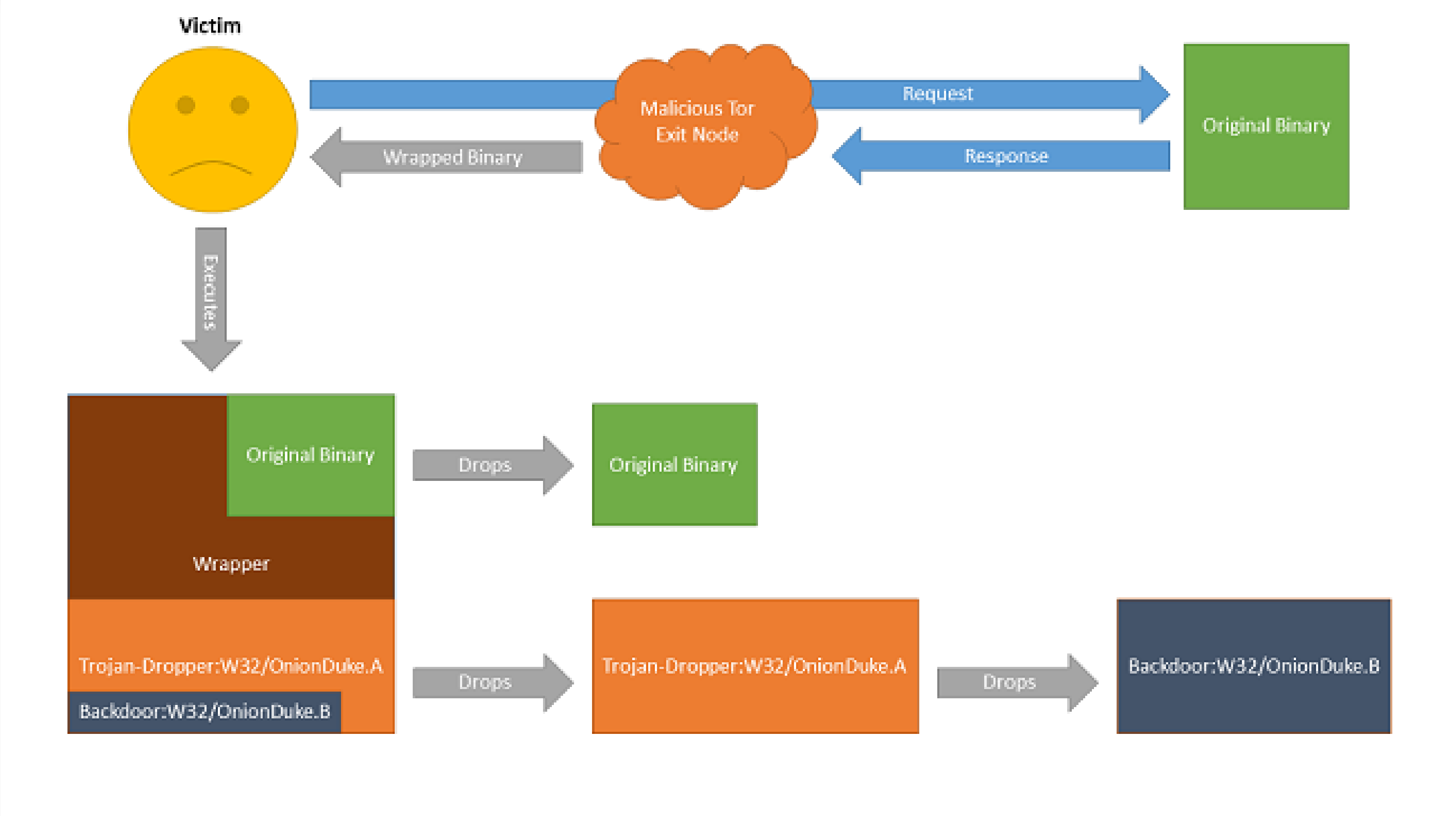
::: 1. Why Mix Your Coins :::

Using Bitcoin does not protect your anonymity. This is because Bitcoin works on a public ledger, meaning anyone anywhere can see and follow every transaction you ever make. From the moment you buy your coins, to the moment you cash them out... they can be followed. And if anything along the way can be linked to your identity - for example if you bought or sold using your bank account, face to face with cash, or even using a voucher from a store with CCTV - then an agency with the right tools could theoretically find you without much trouble. Classic examples of people who might follow your online activity and reveal your identity, are Law Enforcement Agencies, somebody with a grudge, or hackers who have noticed you are moving large amounts of money around.

But by 'mixing' your Bitcoins, you are essentially breaking the link between your identity and your transactions - Bitcoin Blender lets you prevent Blockchain Analysis by swapping your coins for somebody else's. In other words, you deposit your coins into one 'pot', and we send you coins from another 'pot', breaking the chain.

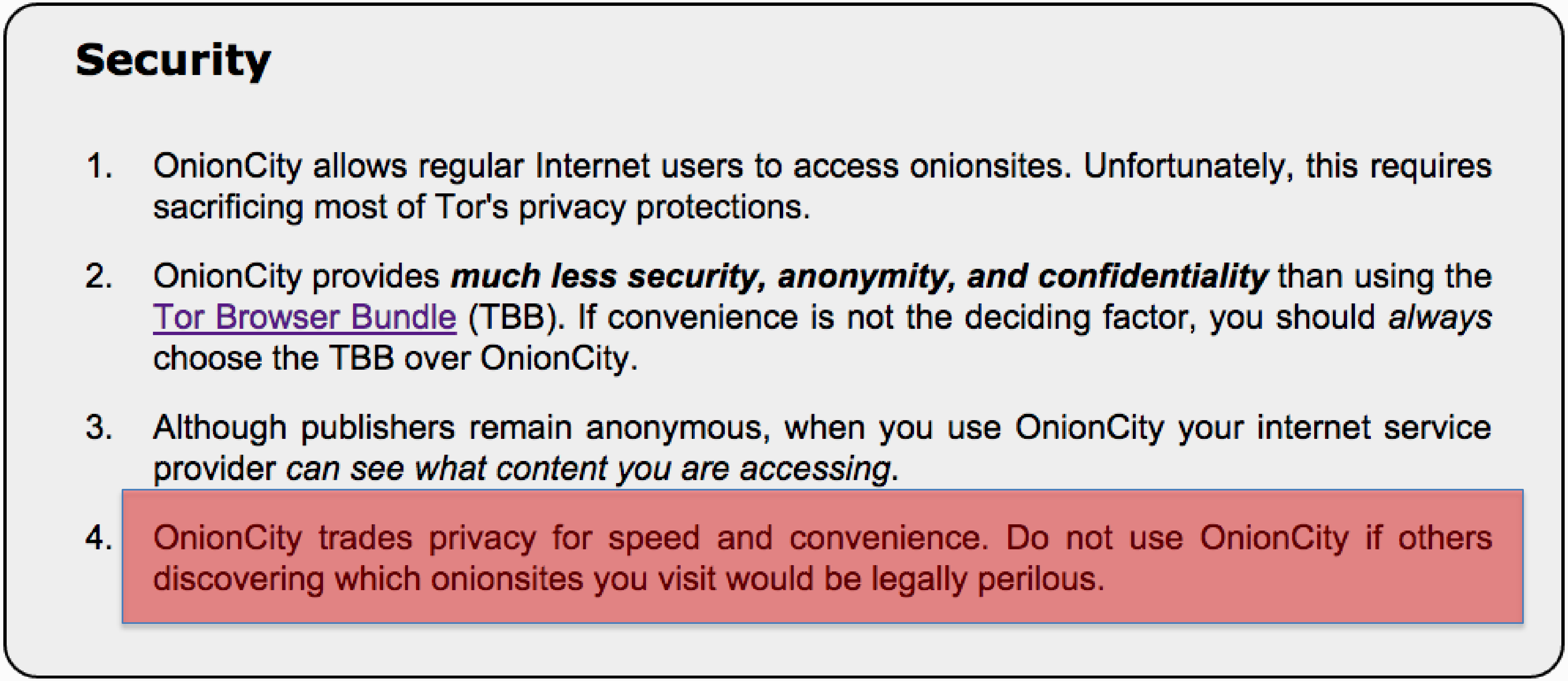
India	Bengaluru	$490
Russia	Vyborg	$190
China	Nanjing	$520
Australia	NewCastle	$290
Australia	Perth	$340

Malicious Attack over Tor



Tor for the lazy (and adventurous)

OnionCity



Security

1. OnionCity allows regular Internet users to access onionsites. Unfortunately, this requires sacrificing most of Tor's privacy protections.

2. OnionCity provides ***much less security, anonymity, and confidentiality*** than using the Tor Browser Bundle (TBB). If convenience is not the deciding factor, you should *always* choose the TBB over OnionCity.

3. Although publishers remain anonymous, when you use OnionCity your internet service provider *can see what content you are accessing*.

4. OnionCity trades privacy for speed and convenience. Do not use OnionCity if others discovering which onionsites you visit would be legally perilous.

Thank you

cventouris papaki isc2 pavla chapter telia gr