

Deep Vs. Dark web demystifying differences

Jurica Čular, M.Sc, MBA, CISA, CISSP
jcular@zsis.hr

Is there really a confusion?

- Ooh YES!



Ahmed Atia
@AMASEADA

 Follow

Clearing Up Confusion – Deep Web vs.
Dark Web | brightplanet.com/2014/03/cleari

...

   ...
4:16 AM - 11 Oct 2014



THINKIT DO! (It's taking longer than we thought)

ENTER KEYWORDS SEARCH

 Like 187  Tweet 36  Share 55

MS? **How can I access the deep, dark Web?**
February 8, 2013

Defs.

- Surface web – anything that can be indexed by a typical search engine like Google...



Defs.

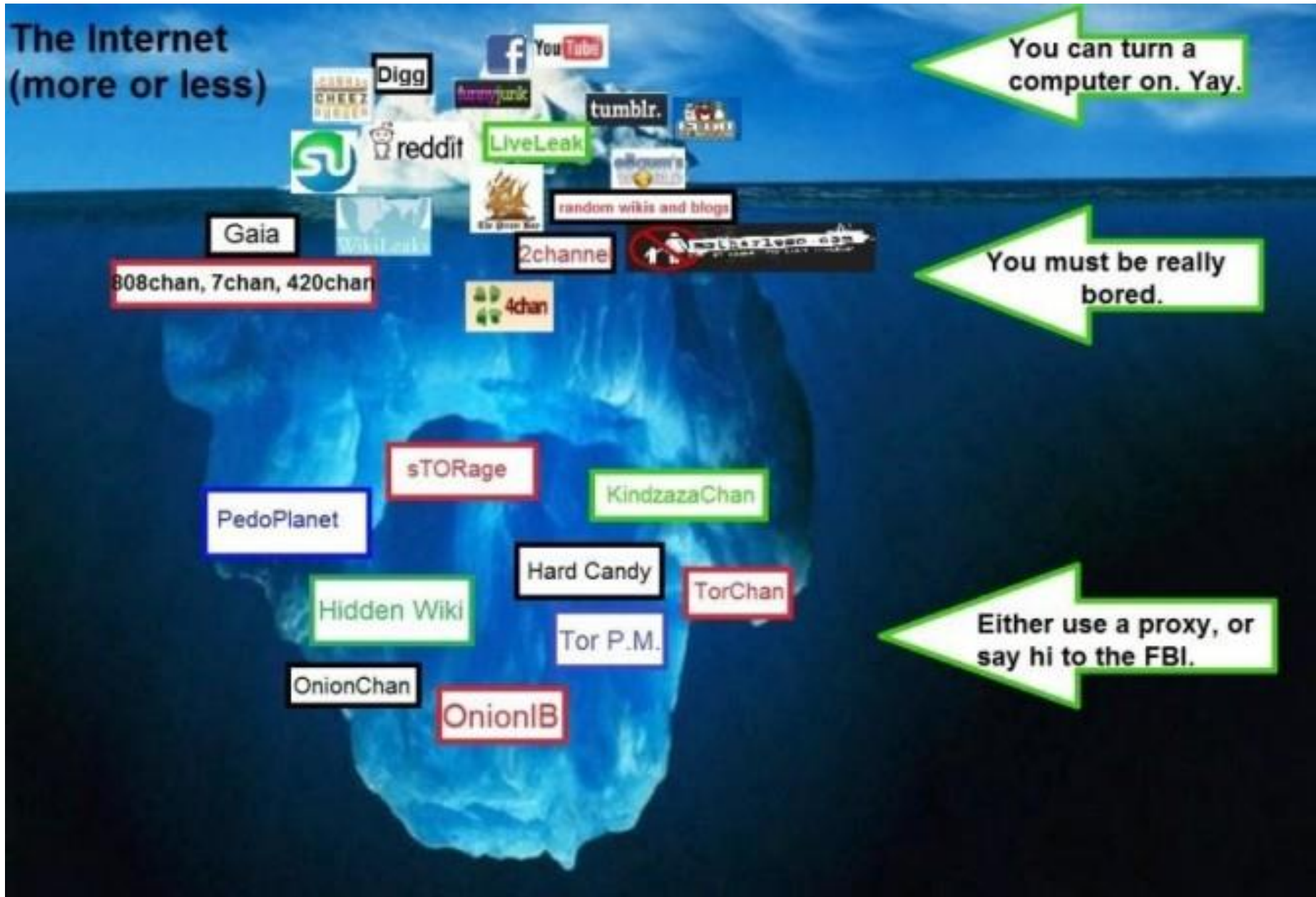
- Deep web – anything that CANNOT be found by search engine (purist)

The screenshot shows a web browser window with the Booking.com search results page for Ljubljana, Slovenia. The URL is www.booking.com/searchresults.en-gb.html?sid=ada660e49436d53b96ea281a78735109;dcid=4;checkin_monthday=12;checkin_year_month=2015-3;checkout_monthday=13;checkout_year_. The page features a navigation bar with the Booking.com logo, currency (€/\$), language (UK), and user options like 'Sign in' and 'Manage booking'. Below the navigation bar, there are breadcrumb links: home → slovenia (1,610 places to stay) → osrednjeslovenska (235 places to stay) → ljubljana (182 places to stay) → search results (Ljubljana, 2 adults, 1 night (12 Mar - 13 Mar) Change dates). A yellow banner highlights that Ljubljana is a top pick among travellers on the selected dates (39% reserved) and provides alternative date suggestions: 13 Mar — 14 Mar, 11 Mar — 12 Mar, and 10 Mar — 11 Mar. The main heading is 'Ljubljana: 111 of 182 properties available' with 3 reasons to visit: castles, old town and food. A filter sidebar on the left allows filtering by Price (per night), Cancellation policy, and Star rating. The main content area displays a list of hotels, with the first one being 'City Hotel' (3 stars, Value Deal, 597 bookmarks, Very good 8.4 score from 1689 reviews). The hotel listing includes a photo of a room, a description, and a 'Book now' button. The second hotel listed is 'Best Western Premier Hotel Slon' (4 stars, Value Deal, 483 bookmarks, Fabulous 8.7 score from 1480 reviews).

Defs.

- Dark web – small portion of deep web that has been intentionally hidden (...)

The Internet (more or less)



You can turn a computer on. Yay.

You must be really bored.

Either use a proxy, or say hi to the FBI.

- Logos above water: Digg, YouTube, Facebook, reddit, LiveLeak, tumblr., Gaia, WikiLeak, random wikis and blogs, 2channe, 4chan, sTORage, KindzazaChan, Hard Candy, TorChan, Tor P.M., OnionChan, OnionIB, Hidden Wiki, PedoPlanet, 808chan, 7chan, 420chan.
- Logos below water: Gaia, WikiLeak, random wikis and blogs, 2channe, 4chan, sTORage, KindzazaChan, Hard Candy, TorChan, Tor P.M., OnionChan, OnionIB, Hidden Wiki, PedoPlanet, 808chan, 7chan, 420chan.

Search engine Vs. Deep Web Harvesting

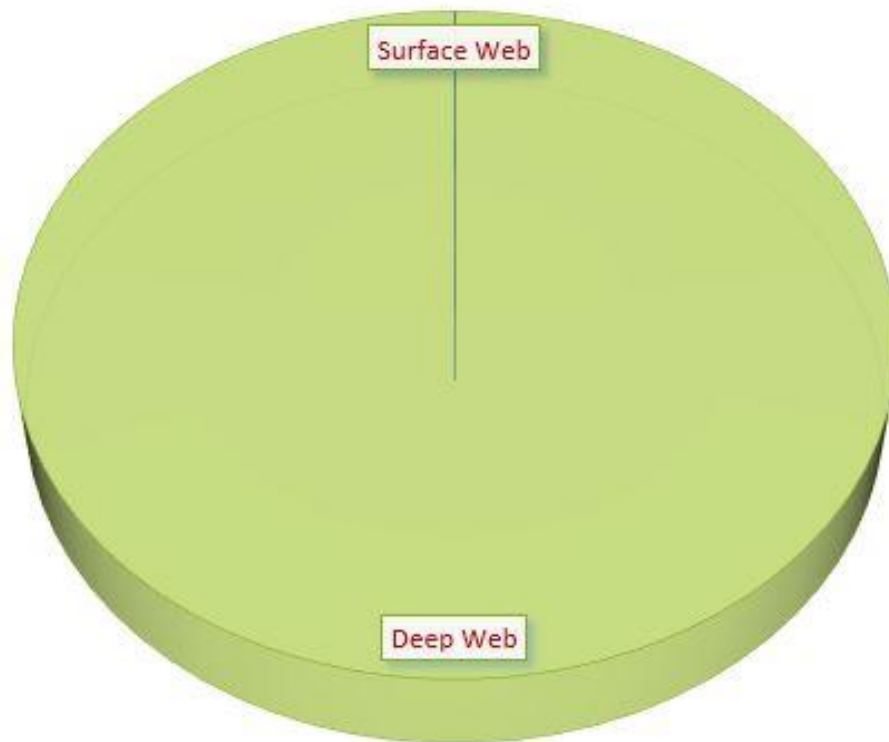
- Search engine(s)
- „What time does McDonalds close?“
- 90's
- Non commercial - research purpose

Search engine Vs. Deep Web Harvesting

- „What new info has been published on my competitors web site today?”
- Amount of data – metadata Vs. Full content
- BI or InfoSec?

Search engine Vs. Deep Web Harvesting

COMPARING THE SIZE OF THE DEEP & SURFACE WEB



Anonymity

- Anonymity...why?
- Def. – „unidentifiability within a set of subjects”
- New rules
- Many researches

Tor



[Home](#)

[About Tor](#)

[Docum](#)

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.



[Download Tor](#) ↓

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

- Encrypted content
- Encrypted content and routing info
- Relay networks

Tor – how Tor works?

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.



Dave

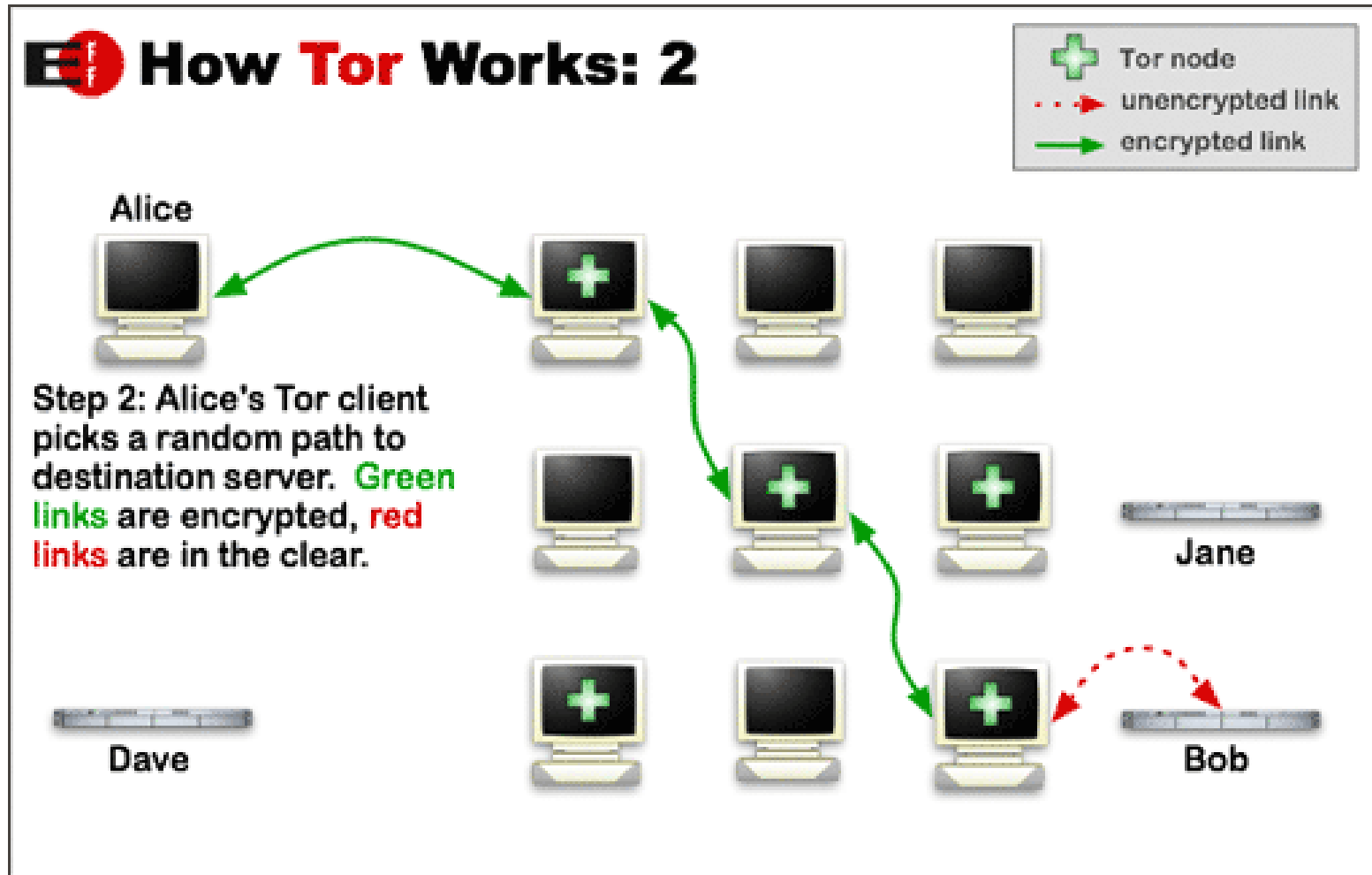


Jane



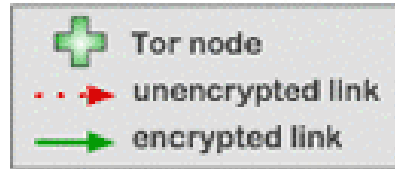
Bob

Tor – how Tor works?



Tor – how Tor works?

How Tor Works: 3



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.



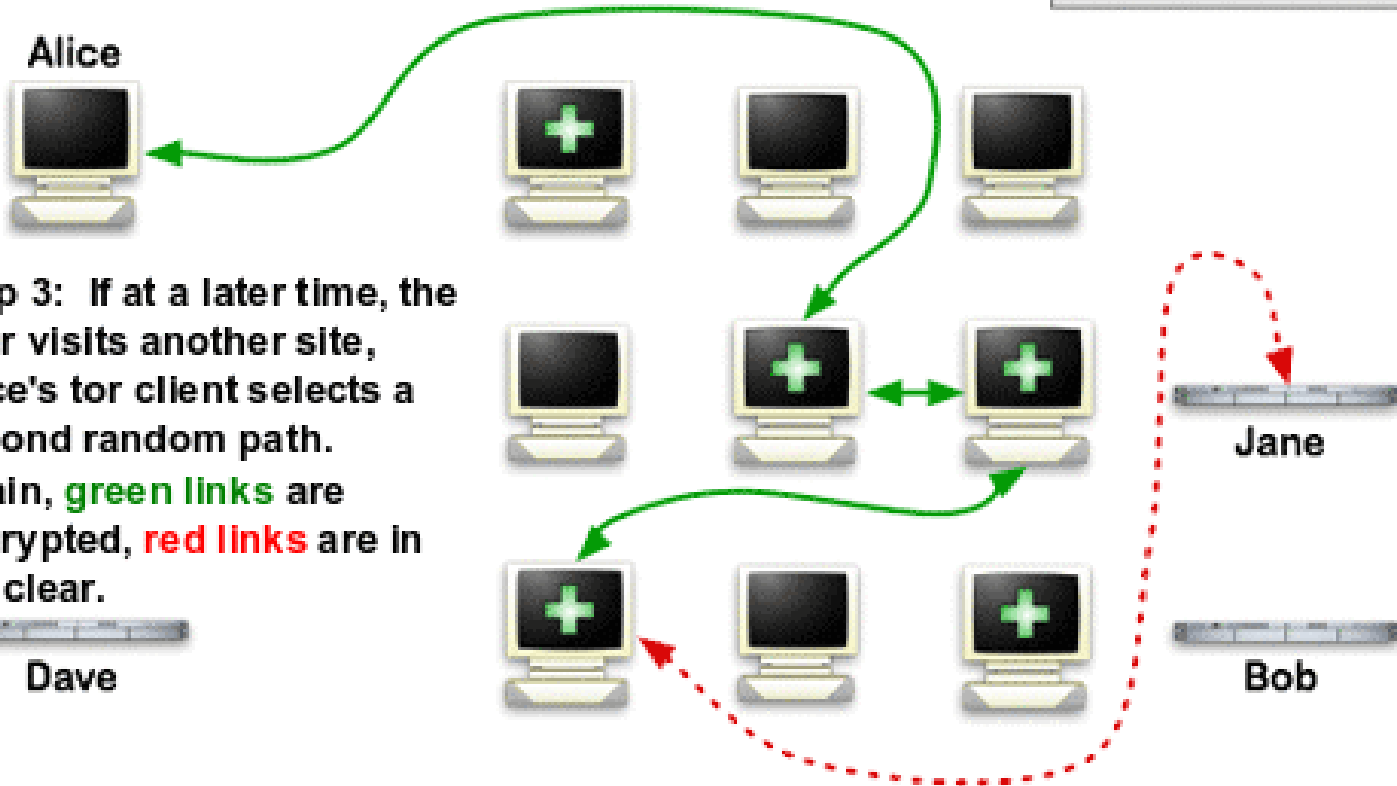
Dave



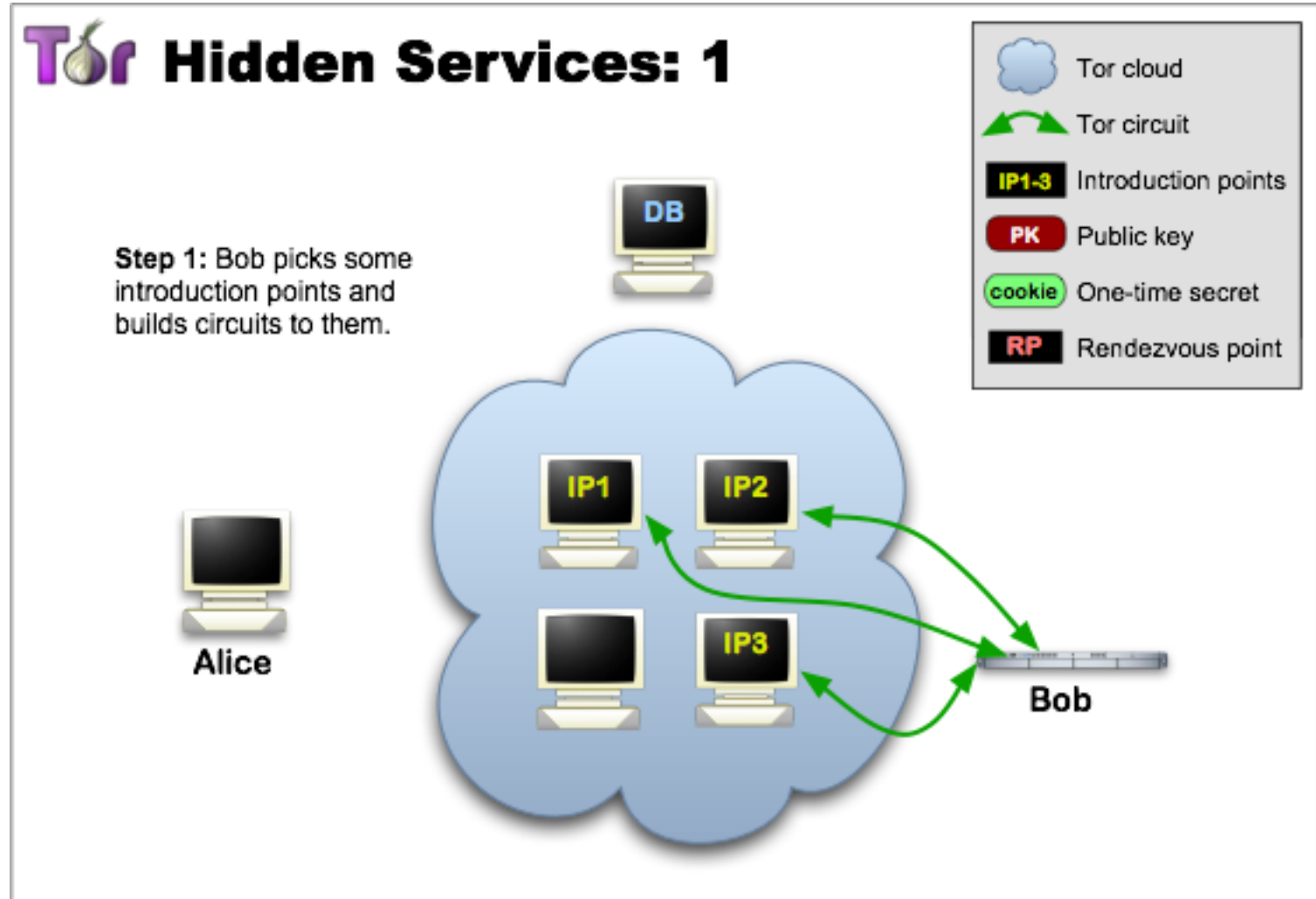
Jane



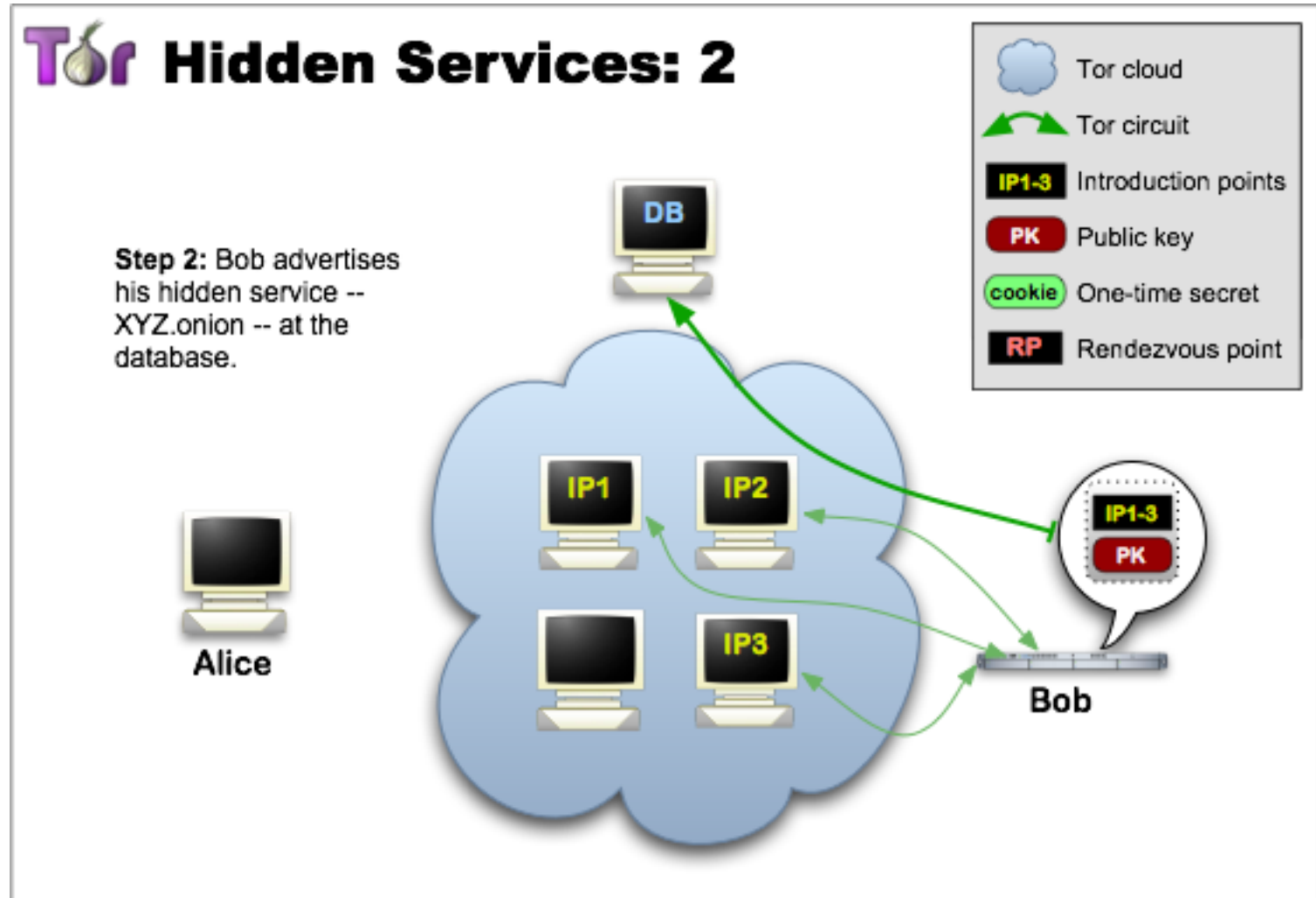
Bob



Tor – hidden services



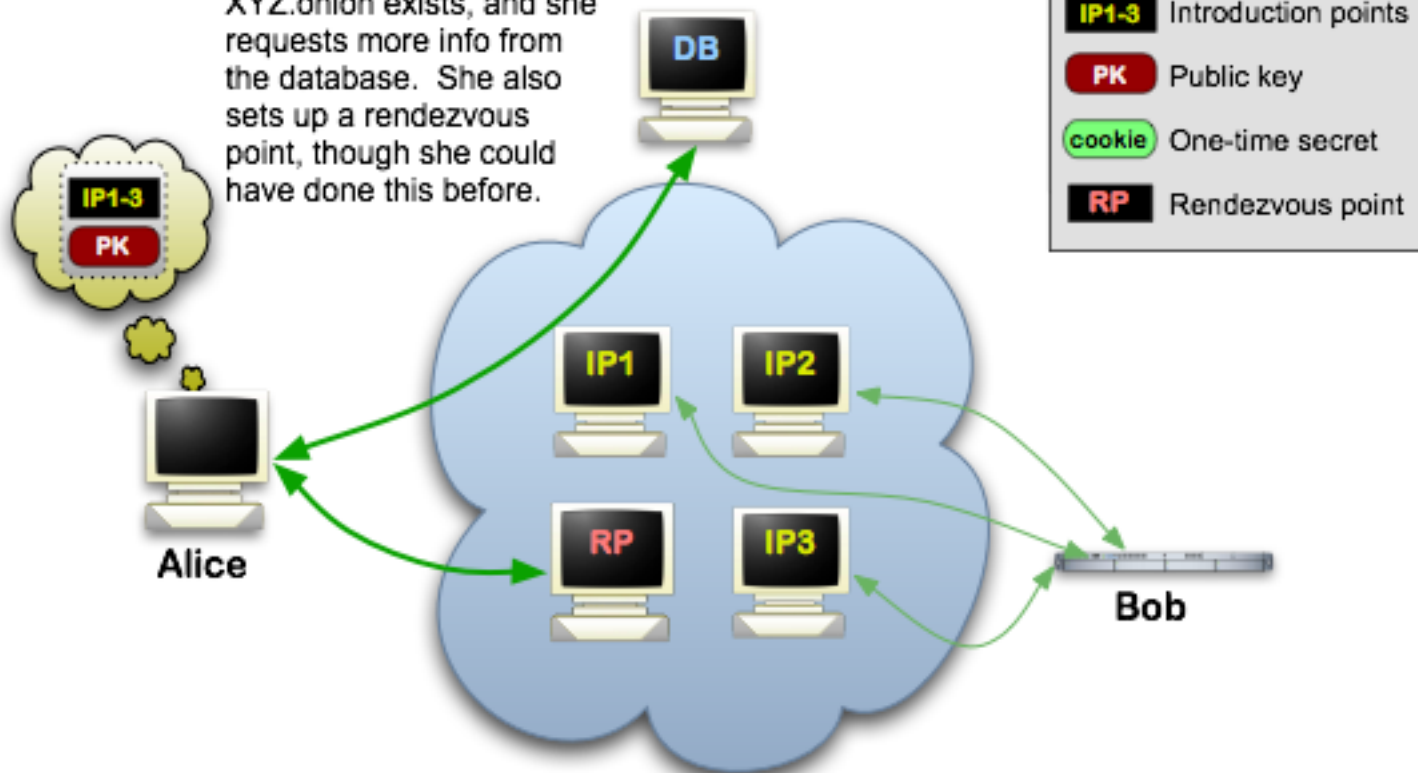
Tor – hidden services



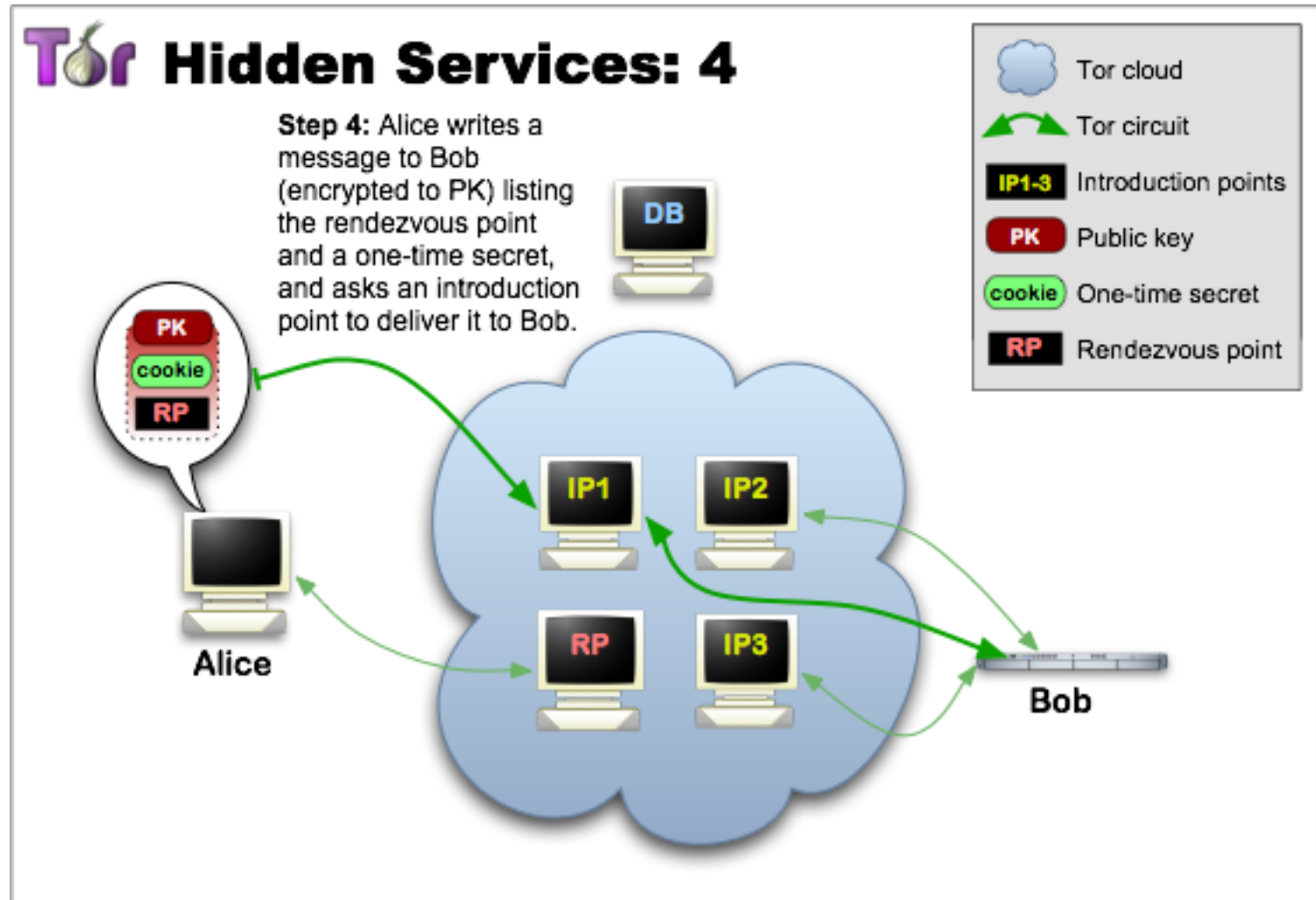
Tor – hidden services

Tor Hidden Services: 3

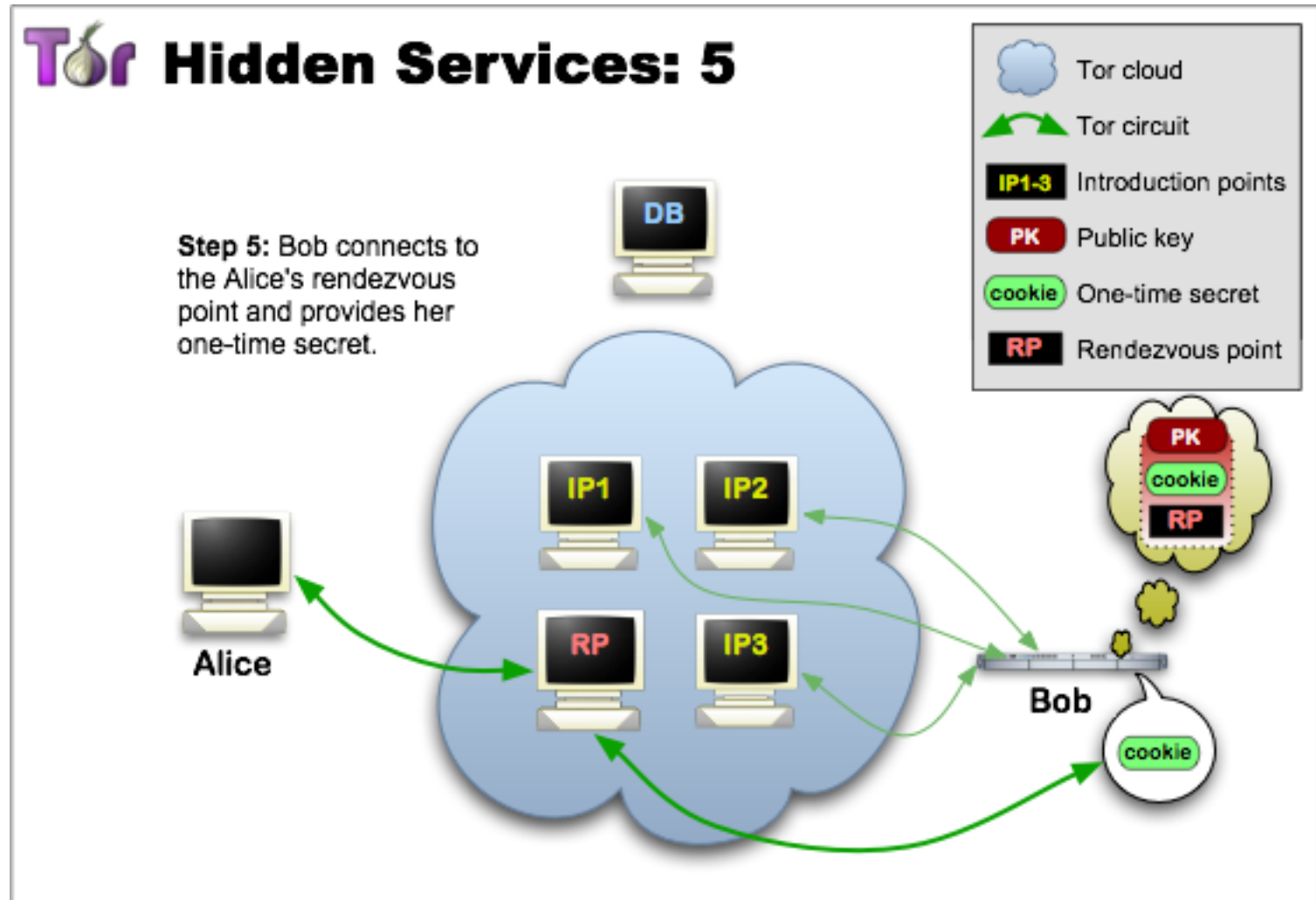
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



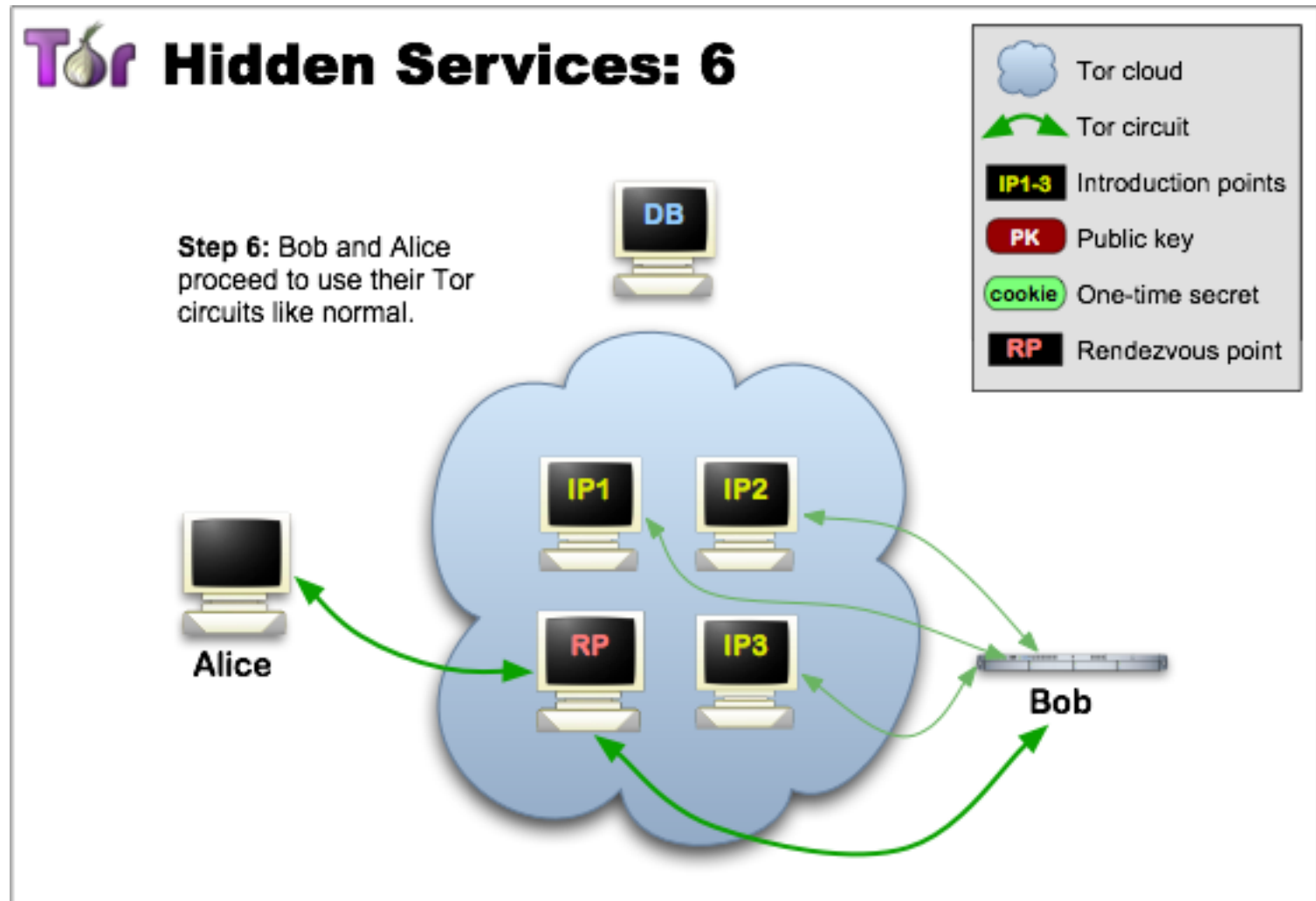
Tor – hidden services



Tor – hidden services



Tor – hidden services



Tor – users

Social Media

FOLLOW MASHABLE >

Tor Project Wins Award for Role in Middle East Revolutions

2.4k
SHARES



Share on Facebook



Share on Twitter



Tor – users

thehiddenwiki.org

1.4k
Like
26
Tweet
154
52
reddit

Marketplace Drugs

- <http://storesq3o5mfxiz.onion/> – Samsung StorE
- <http://sheep5u64f457aw.onion/> – Sheep Marketplace
- <http://n6juddp4as4gg.onion/betcoin.htm> – Tor BetCoin
- <http://qznixqwmep4p5b.onion/> – Tor Web Developer
- <http://f9nd6mieccqyit.onion/> – UK Passports
- <http://en35tuzqmn4lofbk.onion/> – US Fake ID Store
- <http://xfmwjig7ohypdq5r.onion/> – USA Citizenship
- <http://uybu3melulmofnd.onion/> – iLike Help Guy
- <http://dbmv5345pcv534x.onion/> – Network Consulting and Software Development
- <http://w4pk65choakk5ze.onion/raw4588/> – Quick Solution (Hitman)
- <http://n6juddp4as4gg.onion/tynermsr.htm> – Tyner MSR Store

Marketplace Drugs

- <http://rs04hullefireqf.onion/> – EuCanna – Medical Grade Cannabis Buds, Rick Simpson Oil, Ointments and Creams
- <http://newpdsuslmzqzvr.onion/> – Peoples Drug Store – The Darkweb's Best Online Drug Supplier
- <http://smoker32pk4qt3mx.onion/> – Smokeables – Finest Organic Cannabis shipped from the USA
- <http://fzqnlcvhkgbdw5.onion/> – CannabisUK – UK Wholesale Cannabis Supplier
- <http://kvbvbk4kddha2ht.onion/> – DaDope – German Weed and Hash shop. (Bitcoin)
- <http://s5q54hfw56ov2xc.onion/> – BitPharma – EU vendor for cocaine, speed, mdma, psychedelics and subscriptions
- <http://l6lardcivrlyq.onion/> – Brainmagic – Best psychedelics on the darknet
- <http://25ffhnaechtbzwf3.onion/> – NLGrowers – Coffee Shop grade Cannabis from the netherlands
- <http://fec33nz6mhzd54zj.onion/index.php> – Black Market Reloaded Forums
- <http://atlantisky4es5q.onion/> – Atlantis Marketplace
- <http://dke255bz267remj.onion/> – SR Road Forums

thehiddenwiki.org

1.4k
Like
26
Tweet
154
8+1
52
reddit

Erotic Hard Candy

- <http://k4jmdecpcnpsfe43c.onion/> – Girls Released – Some nice model pics
- <http://54dgeda4ik6iyui.onion/> – Gallery – Met-Art, FTVX etc sets
- <http://pinkmethuylenlz.onion/> – The Pink Meth (mirror)
- <http://2fgqzbb2ht7evom.onion/klxen/> – Klxen
- <http://orsxvca7glswuo7.onion/> – EroDir – Lots and lots of Hentai
- <http://mmgh3rqsrlgzdr.onion/> – VOR-COM

Erotic Hard Candy

- <http://lovezspampofiqul.onion/> – TLZ discussion board
- <http://tqjyhbso4mdcrvh.onion/sciclaycams/> – Sciclay Cams
- <http://iqinc7cbykhhufo.onion/> – LLL – Image and Video down- & upload
- <http://oglbv4c4kpoobkid.onion/oglb/> – Onion Girl Love Board – Private Board
- <http://bvunqhdbizxyuoe.onion/> – Boy Vids 4.0
- <http://girlbmame6evpw.onion/> – Girls and Boys
- <http://op4jvhn65pvj3slt.onion/> – PedoEmpire
- <http://7haz75ietjds3j.onion/> – All Natural Spanking
- <http://spofoh4ucwlc7zr6.onion/> – Safe Port Forum
- <http://tqjyhbso4mdcrvh.onion/forum/> – BL Forum
- <http://ftwebt6e3nb3lmw.onion/> – FTW Image Boards
- <http://tlz3gig7k46s4r66.onion/> – TLZ private forums
- <http://vkq6wz4ozmldscii.onion/> – Topic Links – A CP sites link list

Erotic Jailbait

- <http://66m4z7ukqobh4tc.onion/> – Some paradisebirds casev videos

Non-English

- <http://germanyhusicaysx.onion/> – Deutschland im Deep Web – German forum

Tor [background]

1995.



“As military grade communication devices increasingly depend on the public communications infrastructure, it is important to use that infrastructure in ways that are resistant to traffic analysis. It may also be useful to communicate anonymously, for example when gathering intelligence from public databases”

Naval Research Labs Review, 1997

Tor [background]

- Technical solution not enough

“The United States government can’t simply run an anonymity system for everybody and then use it themselves only. Because then every time a connection came from it people would say, ‘Oh, it’s another CIA agent.’ If those are the only people using the network.”

Tor [background]

2004.

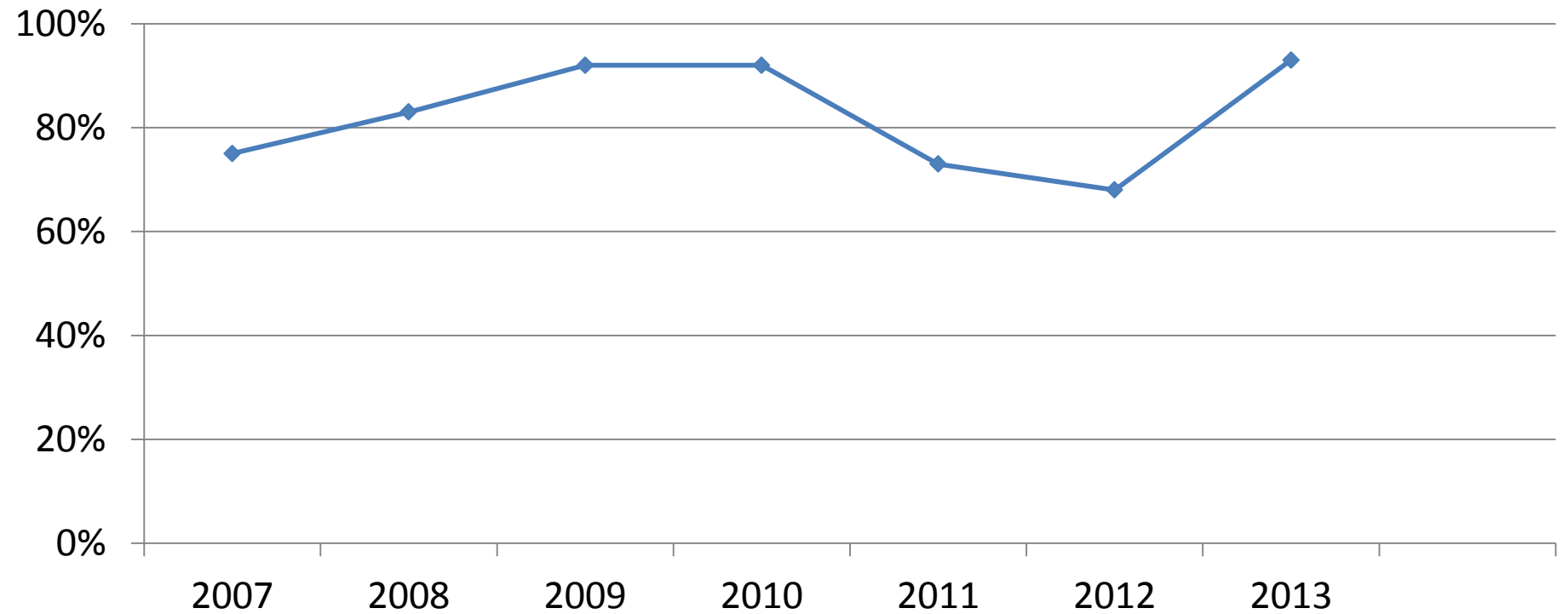
- TOR ready for deployment
- Released as Open Source
- Electronic Frontier Foundation



Tor [background]

2004.---

% revenue from US Government



Tor [background]

- Using, trying to „crack” and fund – at the same time!



- Running an exit node
- Big (expensive) nodes
- Washington DC

Tor [background]

- Fast nodes first
- 2005. „tricky design question”
- 2012. explanation

„(...) if we want to end up with a fast safe network, do we get there by having a slow safe network and hoping it'll get faster, or by having a fast less-safe network and hoping it'll get safer? We opted for the “if we don't stay relevant to the world, Tor will never grow enough” route.”

Famous takedowns

- Botnets /Adult sites /Black markets
- 2013.Freedom Hosting
- JavaScript & Firefox
- „One purpose” based malware

Famous takedowns

- 2013.Silk Road
- On-line store
- Island IP
- Surface web CAPTCHA
- Not likely!
- „economic” impacts

Famous takedowns

- 2015. Ulbricht convicted
- Lessons learned
 - just a platform
 - *“Silk Road was specifically and intentionally designed for the purpose of facilitating unlawful transactions,”*
 - money laundering
 - „Is BitCoin Money? Yes!”
 - Crack House Statute
 - *„This is not an ordinary dwelling, but a drug dealer’s ‘dream house.’”*

Famous takedowns

- Investigation legit?
 - Island territory
 - Ulbricht not owner
 - *„systems may be monitored for all lawful purposes, including to ensure that use is authorized.”*
- „Fourth Amendment”
 - “Because the SR Server was located outside the United States, the Fourth Amendment would not have required a warrant to search the server, whether for its IP address or otherwise,,”
- Catch 22
 - No possession, no privacy

Take aways

- Just to raise some questions
- Internet of things
- Popcorn and the front row!



GRACIAS
ARIGATO
SHUKURIA
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
DANKSCHEEN
TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
PALDIES
YOU
BOLZIN
MERCY
THANK
BIYAN
SHUKRIA
TINGKI
HATUR GI
EKOJU
SIKOMO
MAKETAI
MINMONCHAR
SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WADEEJA
MAITEKA
HUI
YUSPAGARATAM
DHANYABAAD
ANBIA
ATTO
MERSI
SPASIBO
DENKAUJA
NENACHALHYA
UNALCHEESH
BAIKA
MEDAWAGSE
TAVTAPUCH
BAIKO
SAKCO
MERASTAWHY
GAEJTHO
AGUYJE
FAKAAUE
KOMAPSUMNIDA
MAAKE
LAH