ISTAC Tor Overview

Andrew Lewman
andrew@torproject.org

November 3, 2010

The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy

What is Tor?

- online anonymity software and network

What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)

What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech

What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
- increasingly diverse toolset:
  Tor, Torbutton, Tor Browser Bundle, TA(I)LS LiveCD, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Torora, Tor Check, Arm, Nymble, Tor Control, Tor Wall, TorVM

estimated 500,000 daily users

Twitter in Iran: Good.

Iran Protests: Twitter, the Medium of the Movement

By **LEV GROSSMAN** Wednesday, Jun. 17, 2009

Related

Photos

Behind the Scenes with Mousavi

Stories

- In Iran, Rival Regime Factions Play a High-Stakes Game of Chicken
- Latest Tweets on Fallout from Iran's

MORE

Share The U.S. State Department doesn't usually take an interest in the maintenance schedules of dotcom start-ups. But over the weekend, officials there reached out to Twitter and asked them to delay a network upgrade that was scheduled for Monday night. The reason? To protect the interests of

From http://www.time.com/time/world/article/0,8599,1905125,00.html

Twitter in USA: Bad.

FBI Raids Queens Home in G20 Protest Twitter Crackdown

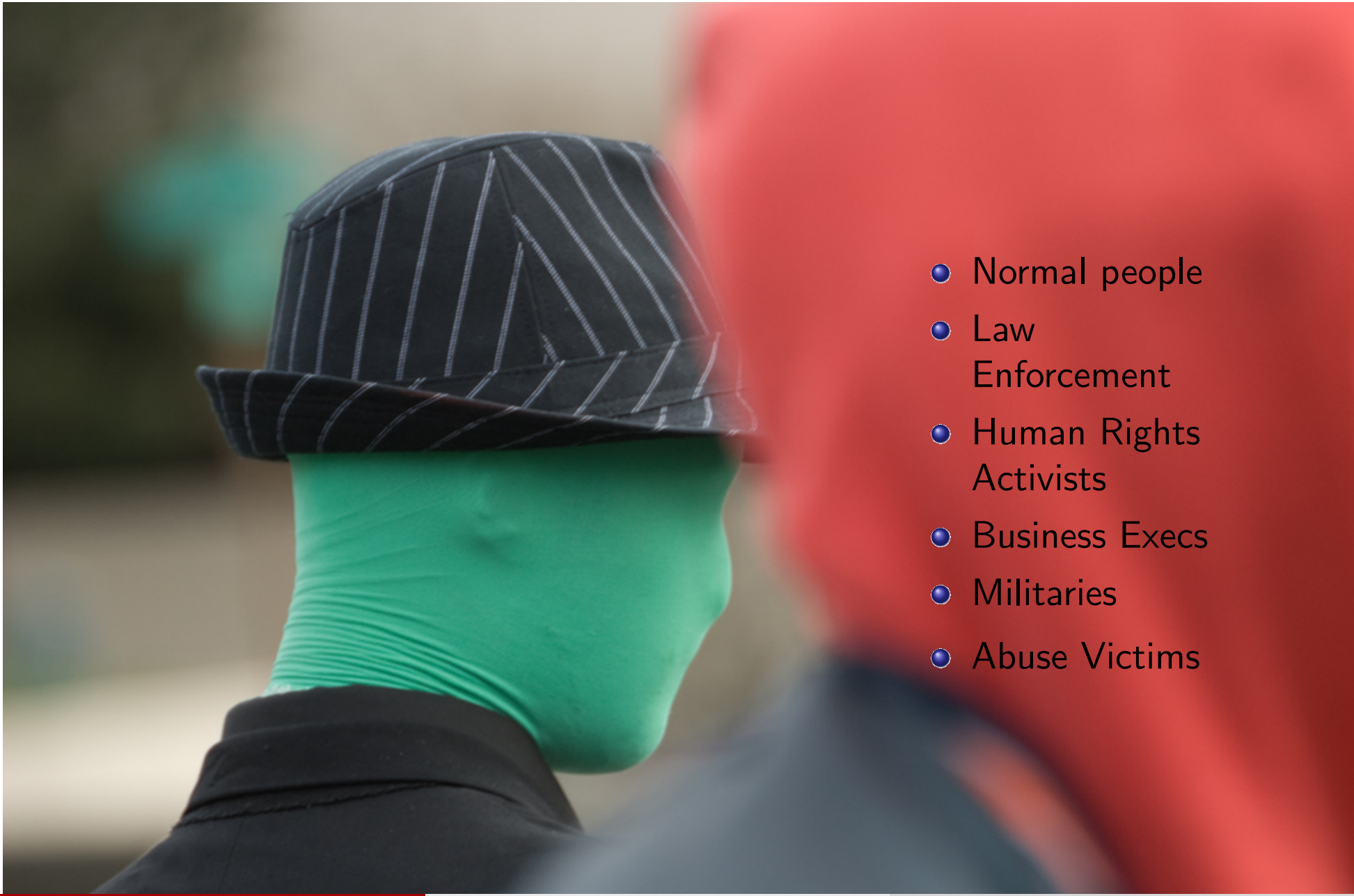
AP Photo/Matt Rourke

That's right, a Twitter crackdown. A lawyer for Jackson Heights social worker Elliot Madison, 41, says that the feds searched his client's house for 16 hours on Thursday after Madison was arrested on September 24th at a Pittsburgh hotel room with another man. What were they up to? Sitting at laptops sending Twitter messages advising G20 demonstrators about riot police activity in the streets. And yet *real* Twitter threats like Lindsay Lohan and Courtney Love remain at large.

Madison, a self-described anarchist, was in Pittsburgh volunteering for the Tin Can Comms Collective, a group that uses Twitter to send mass text messages during protests describing events observed on the streets or over police scanners; stuff like "SWAT teams rolling down 5th Ave." Tin Can was active during the St. Paul RNC protests, and the authorities are now on to them. Madison was charged with hindering apprehension or prosecution, criminal use of a communication facility and possession of instruments of crime; he's currently out on bail.

from http://gothamist.com/2009/10/05/fbi_raids_queens_home_in_g20_protes.php

Who uses Tor?



- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

Tor hides communication patterns by relaying data through volunteer servers

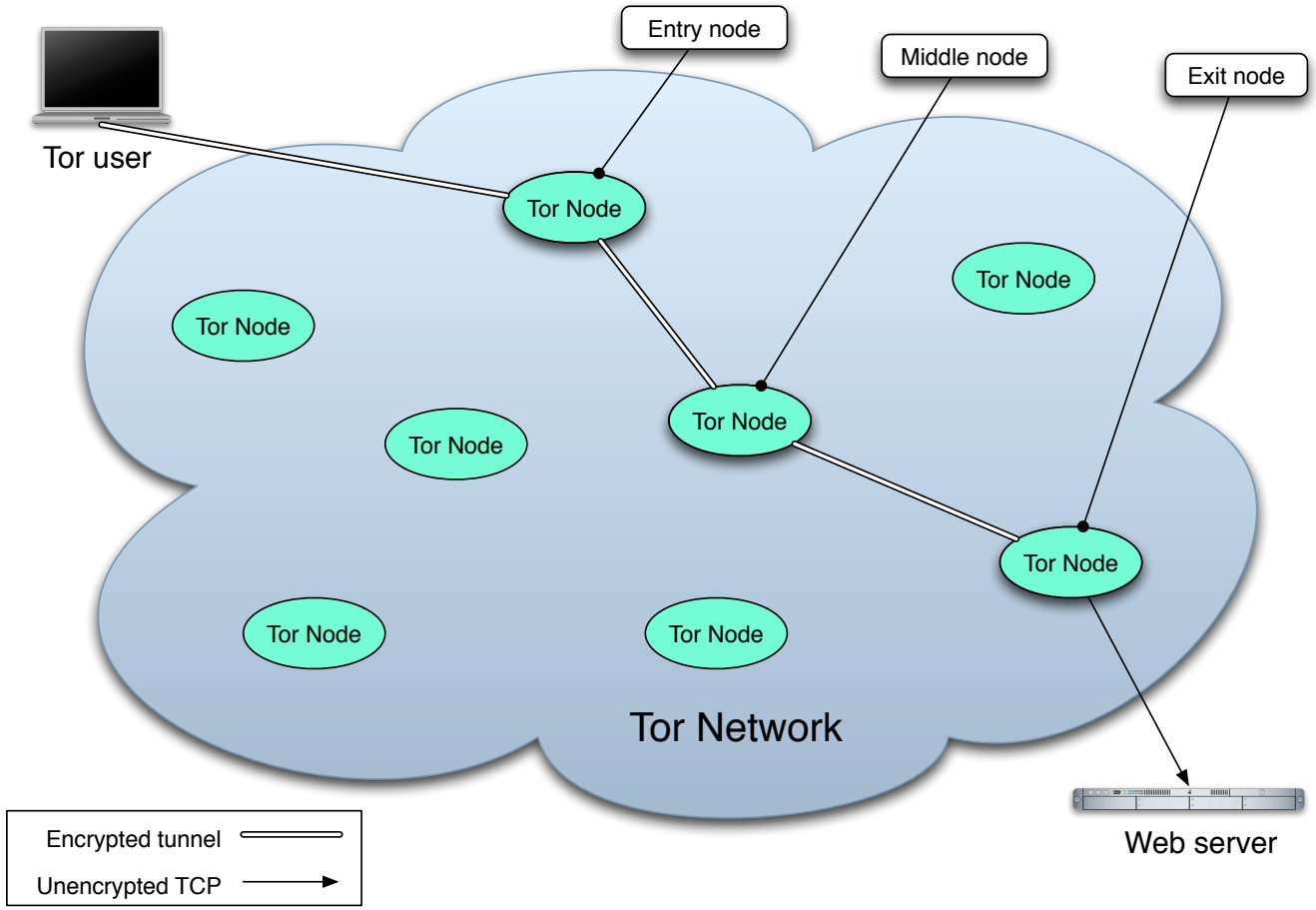
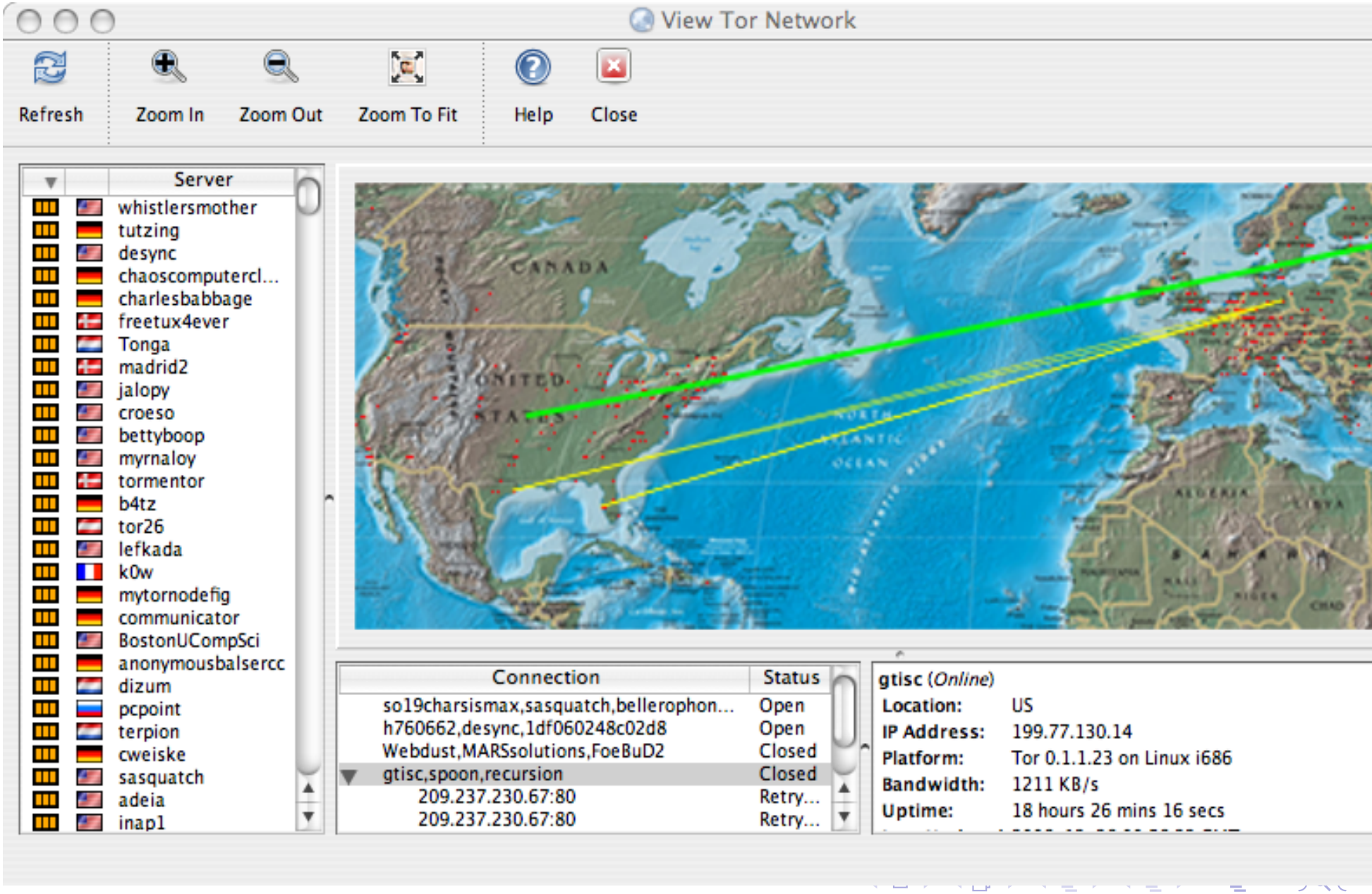


Diagram: Robert Watson

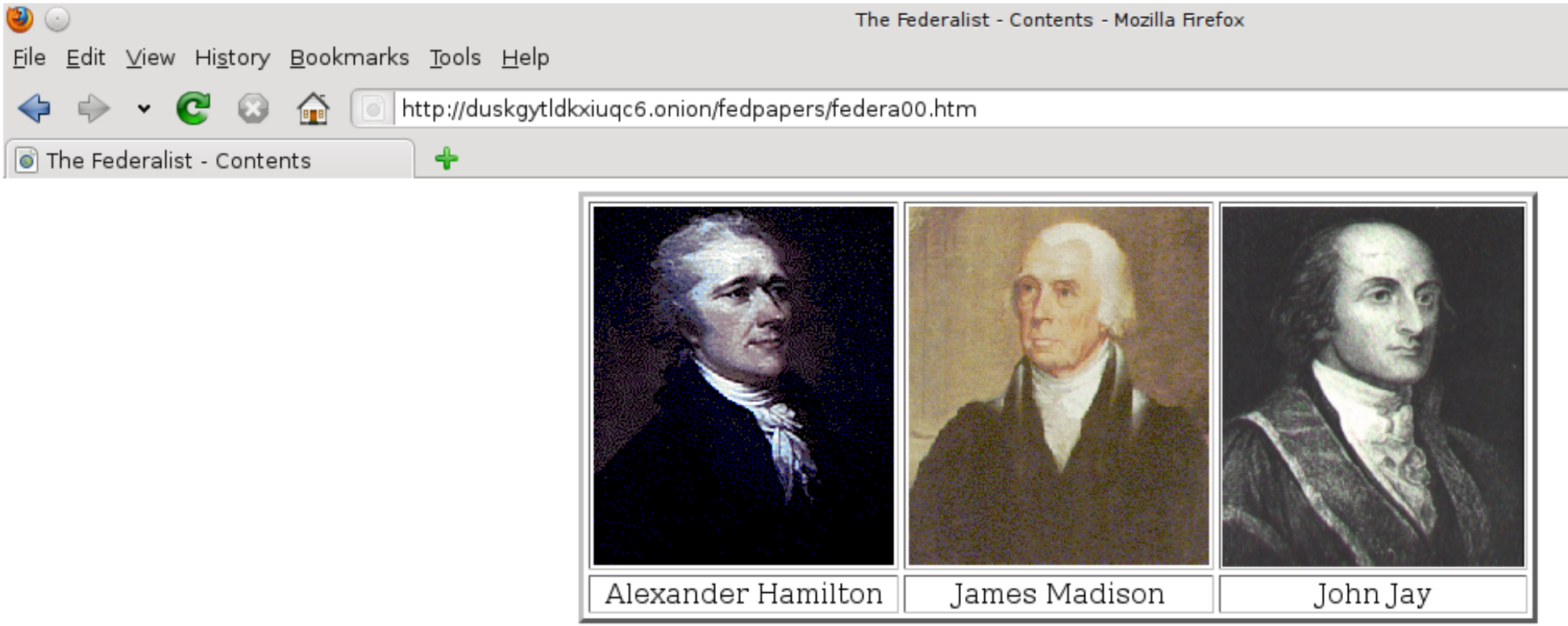
Tor


View Tor Network
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Server
whistlersmother
tutzing
desync
chaoscomputercl...
charlesbabbage
freetux4ever
Tonga
madrid2
jalopy
croeso
bettyboop
myrnaloy
tormentor
b4tz
tor26
lefkada
k0w
mytornodefig
communicator
BostonUCompSci
anonymousbalsercc
dizum
pcpoint
terpion
cweiske
sasquatch
adeia
inap1
CANADA
UNITED STATES
NORTH ATLANTIC OCEAN
Connection
Status
so19charsismax,sasquatch,bellerophon...
Open
h760662,desync,1df060248c02d8
Open
Webdust,MARSsolutions,FoeBuD2
Closed
gtisc,spoon,recursion
Closed
209.237.230.67:80
Retry...
209.237.230.67:80
Retry...
gtisc (Online)
Location:
US
IP Address:
199.77.130.14
Platform:
Tor 0.1.1.23 on Linux i686
Bandwidth:
1211 KB/s
Uptime:
18 hours 26 mins 16 secs

Metrics

- Measuring metrics anonymously
- NSF grant to find out
- Metrics portal:
  `https://metrics.torproject.org/`

Tor hidden services allow privacy enhanced hosting of services



Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my....

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?
- `http://www.decloak.net/` is a fine test

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are
- Orbot: Tor on Android. `http://openideals.com/2009/10/22/orbot-proxy/`
- iphone, maemo/meego, symbian, etc
- Tor on Windows CE, `http://www.gsmk.de` as an example.
- Guardian Project, `https://guardianproject.info/`

Ten things to look for in a circumvention tool

`https://www.torproject.org/press/`

Article originally prepared for the March 2010 “Index on Censorship”, then adapted for the July 2010 “China Rights Forum”.

Summary of Ten things...

- Has a diverse set of users

Summary of Ten things...

- Has a diverse set of users
- Works in your country

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy
- Has an open design

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy
- Has an open design
- Has a decentralized architecture

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy
- Has an open design
- Has a decentralized architecture
- Keeps you safe from websites too

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy
- Has an open design
- Has a decentralized architecture
- Keeps you safe from websites too
- Doesn't promise to magically encrypt the entire Internet

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy
- Has an open design
- Has a decentralized architecture
- Keeps you safe from websites too
- Doesn't promise to magically encrypt the entire Internet
- Provides consistently good latency and throughput

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy
- Has an open design
- Has a decentralized architecture
- Keeps you safe from websites too
- Doesn't promise to magically encrypt the entire Internet
- Provides consistently good latency and throughput
- Makes it easy to get the software and updates

Summary of Ten things...

- Has a diverse set of users
- Works in your country
- Has a sustainable network and software development strategy
- Has an open design
- Has a decentralized architecture
- Keeps you safe from websites too
- Doesn't promise to magically encrypt the entire Internet
- Provides consistently good latency and throughput
- Makes it easy to get the software and updates
- Doesn't promote itself as a circumvention tool

Next steps

Visit `https://www.torproject.org/` for more information, links, and ideas.

Credits & Thanks

- who uses tor? `http://www.flickr.com/photos/mattw/2336507468/siz`, Matt Westervelt, CC-BY-SA.
- danger!, `http://flickr.com/photos/hmvh/58185411/sizes/o/`, hmvh, CC-BY-SA.
- 500k, `http://www.flickr.com/photos/lukaskracic/334850378/sizes/l/`, Luka Skracic, used with permission.