

The Digital Speakeasy: Secure and Anonymous Access to Your Website

Howdy!

**I'm an engineer at
Acquia**

Dustin Younse

@milsyobtaf

<https://github.com/milsyobtaf/prez>

What Is The Digital Speakeasy?



Browsing in Secret

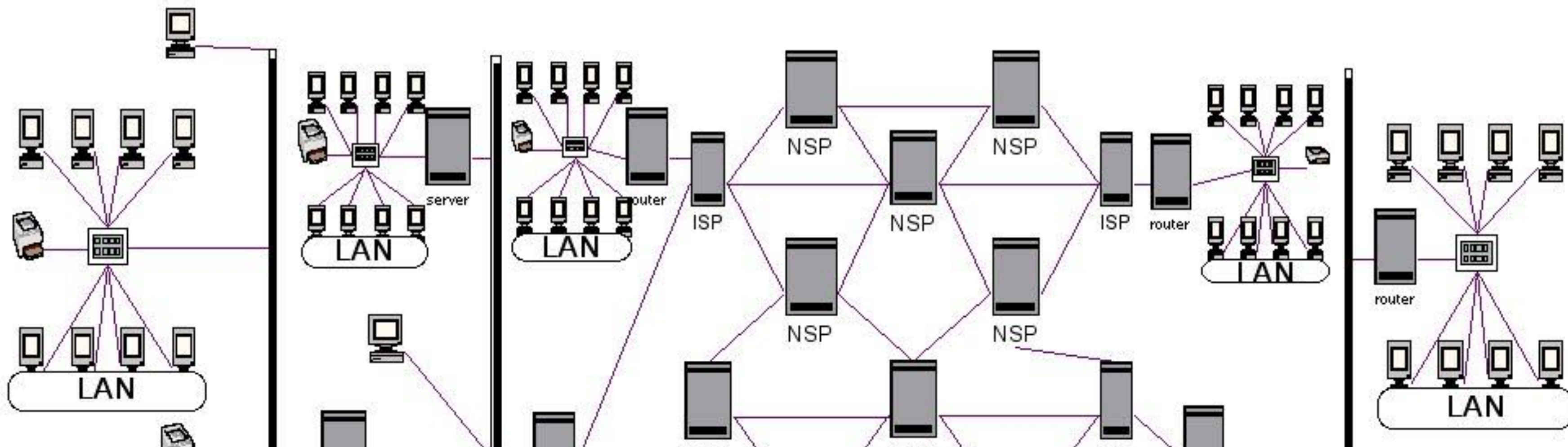
- Plain Text browsing





```
<!DOCTYPE html>
<html lang="en-US">
  <head>
    <meta charset="utf-8">
    <title>Web design, development, and strategy |
Four Kitchens</title>
    <meta name="viewport" content="width=device-
width, initial-scale=1.0, maximum-scale=1.0">
    <meta property="og:title" content="Web design,
development, and strategy">
<meta property="og:type" content="article">
<meta property="og:url" content="http://
fourkitchens.com/">
<link rel="canonical" href="http://
```

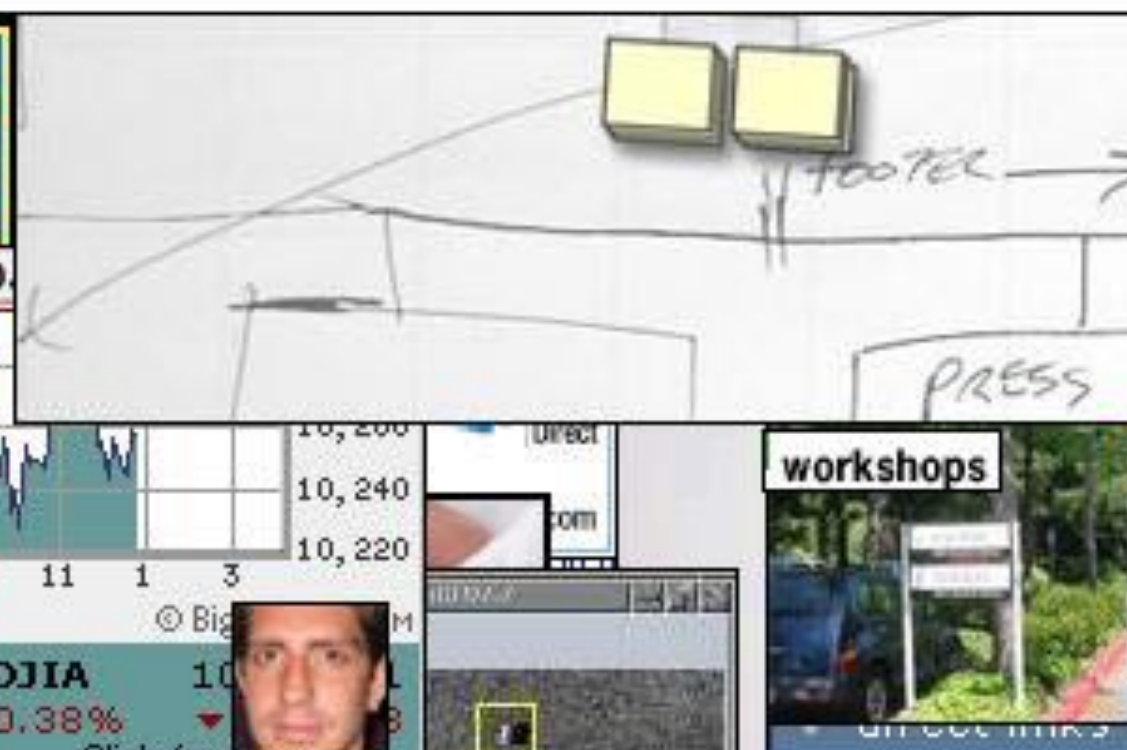


HTTP/1.1 200 OK
Server: nginx/1.6.1
Date: Sat, 20 Aug 2016 03:42:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 56595
Last-Modified: Wed, 17 Aug 2016 00:07:26 GMT
Connection: keep-alive
Vary: Accept-Encoding
ETag: "57b3aabe-dd13"
Expires: Sun, 21 Aug 2016 03:42:11 GMT
Cache-Control: max-age=86400
X-UA-Compatible: IE=Edge
Accept-Ranges: bytes

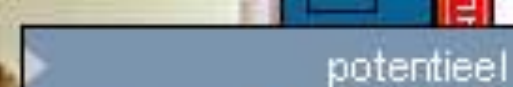


The Internet Is Trusting By Default

The Internet
(INTERconnected NETworks)

























Browsing in Secret

- Plain Text browsing
- HTTPS browsing

```
<!QBPGLCR ugzy>
<ugzy ynat="ra-HF">
  <urnq>
    <zrgn punefrg="hgs-8">
      <gvgyr>Jro qrfvta, qrirybczrag, naq fgengrtl |
Sbhe Xvgpuraf</gvgyr>
      <zrgn anzr="ivrjcbeg" pbagra="jvqgu=qrivpr-
jvqgu, vavgvny-fpnyr=1.0, znkvzhz-fpnyr=1.0">
      <zrgn cebcregl="bt:gvgyr" pbagra="Jro qrfvta,
qrirybczrag, naq fgengrtl">
<zrgn cebcregl="bt:glcr" pbagra="negvpyr">
<zrgn cebcregl="bt:hey" pbagra="uggc://
sbhexvgpuraf.pbz/">
<yvax ery="pnabavpny" uers="uggc://
```


HTTP/1.1 200 OK
Server: nginx/1.6.1
Date: Sat, 20 Aug 2016 03:49:34 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 56595
Last-Modified: Wed, 17 Aug 2016 00:07:26 GMT
Connection: keep-alive
Vary: Accept-Encoding
ETag: "57b3aabe-dd13"
Expires: Sun, 21 Aug 2016 03:49:34 GMT
Cache-Control: max-age=86400
X-UA-Compatible: IE=Edge
Accept-Ranges: bytes

Browsing in Secret

- Plain Text browsing
- HTTPS browsing
- Onion Router (gen 0 and gen 1)

David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. "Hiding Routing Information,"
Workshop on Information Hiding, Cambridge, UK, May, 1996.

Hiding Routing Information

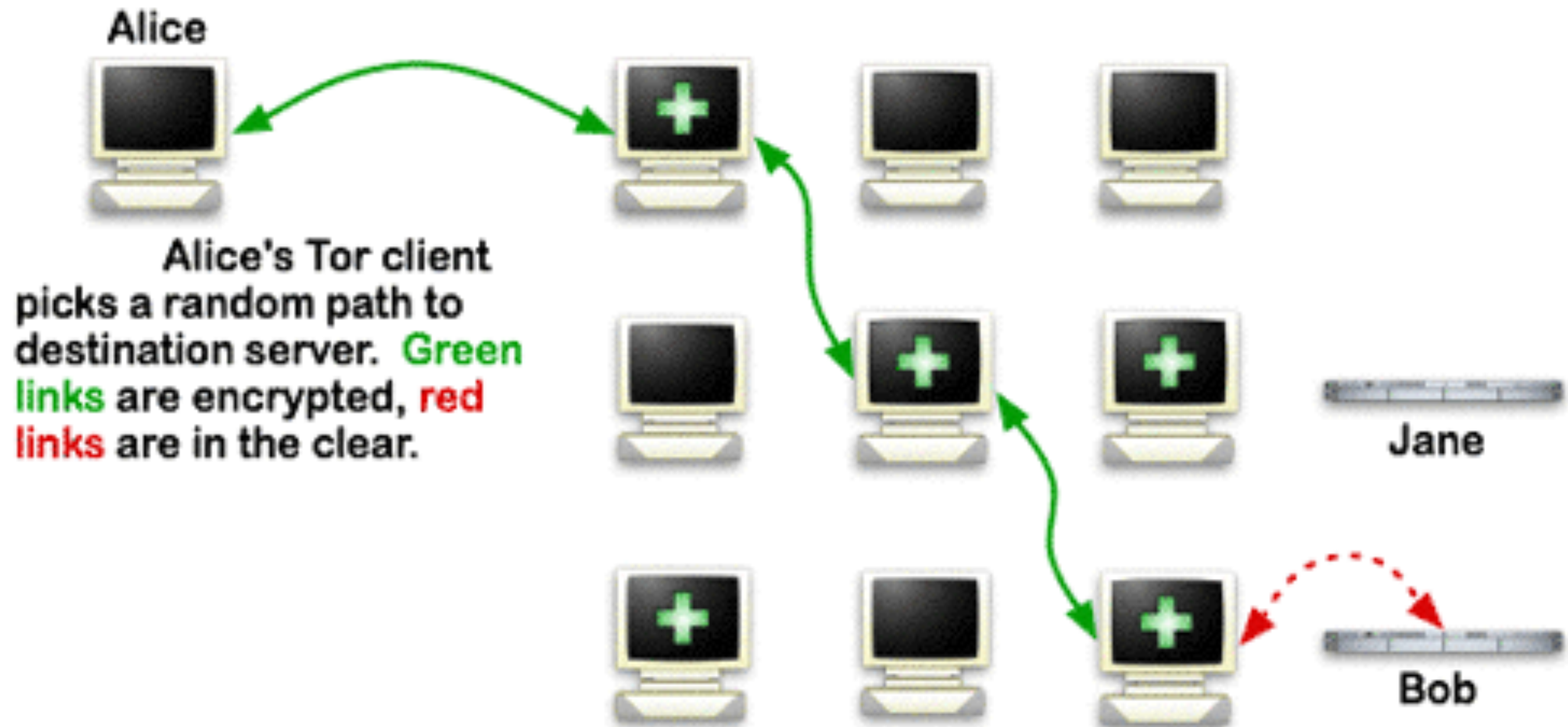
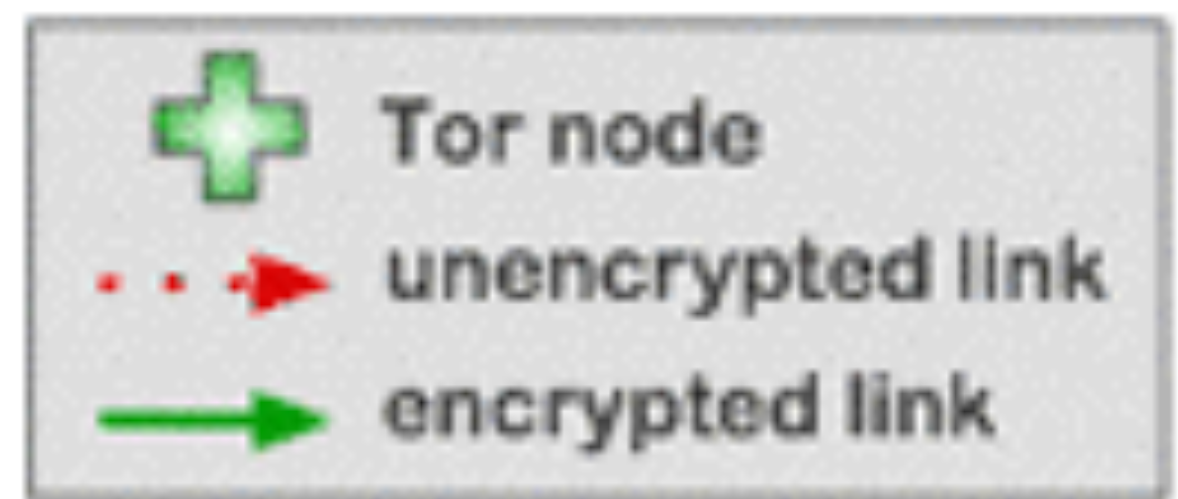
David M. Goldschlag, Michael G. Reed, and Paul F. Syverson

Naval Research Laboratory, Center For High Assurance Computer Systems,
Washington, D.C. 20375-5337, USA, phone: +1 202.404.2389, fax: +1 202.404.7942,
e-mail: {*last name*}@itd.nrl.navy.mil.

Browsing in Secret

- Plain Text browsing
- HTTPS browsing
- Onion Router (gen 1)
- Tor (The Onion Router, gen 2)

How Tor Works



The Rule of Three



So Why Bother?



The Importance of Privacy

- Not all governments are that forgiving
 - Arab Spring
 - Turkish Coup



INDEPENDENT



[News](#) > [World](#) > [Europe](#)

Turkey coup attempt: UN warns Erdogan government purges could violate international law after 40,000 detained

The Importance of Privacy

- Not all governments are that forgiving
 - Arab Spring
 - Turkish Coup
- Not all jobs are fully ethical
 - Edward Snowden
 - Chelsea Manning
- Your reading habits can have consequences
 - Open Societies Foundation

Soros hacked, thousands of Open Society Foundations files released online

Published time: 14 Aug, 2016 19:08



© 2016 PHOTO: GAGE SKIDMORE

TO THE TECHNOLOGY COMMUNITY:

Your threat model just changed.

Incoming President Donald Trump made campaign promises that, if carried out, threaten the free web and the rights of millions of people. He has praised attempts to undermine digital security, supported mass surveillance, and threatened net neutrality. He promised to identify and deport millions of your friends and neighbors, track people based on their religious beliefs, and suppress freedom of the press.

And he wants to use your servers to do it.

Today, we are calling on the technology community to unite with the Electronic Frontier Foundation in securing our networks against this threat.

ENCRYPT: Use HTTPS and end-to-end encryption for every user transaction, communication, and activity by default.

DELETE: Scrub your logs. You cannot be made to surrender data you do not have.

REVEAL: If you get a government request to monitor users or censor speech, tell the world.

RESIST: Fight for user rights in court, on Capitol Hill, and beyond.

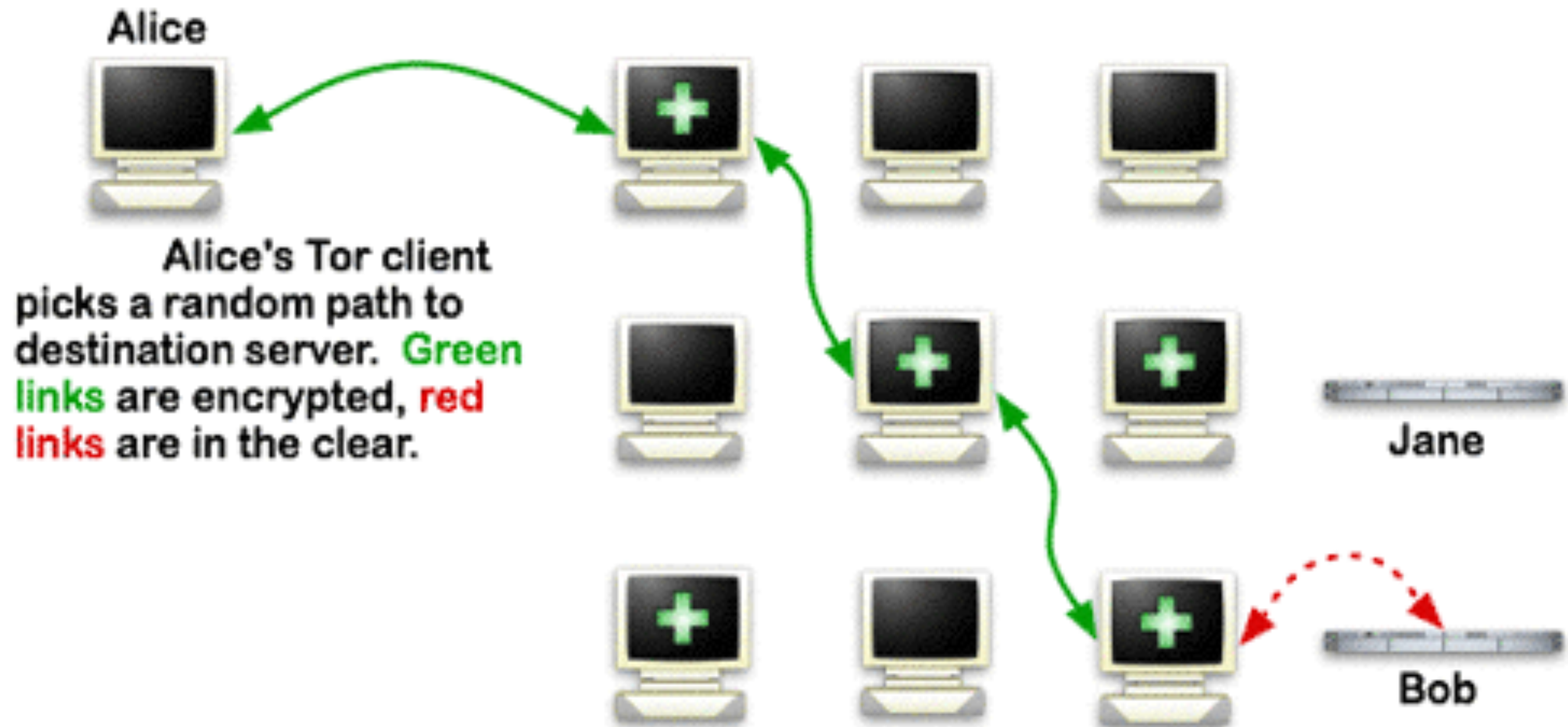
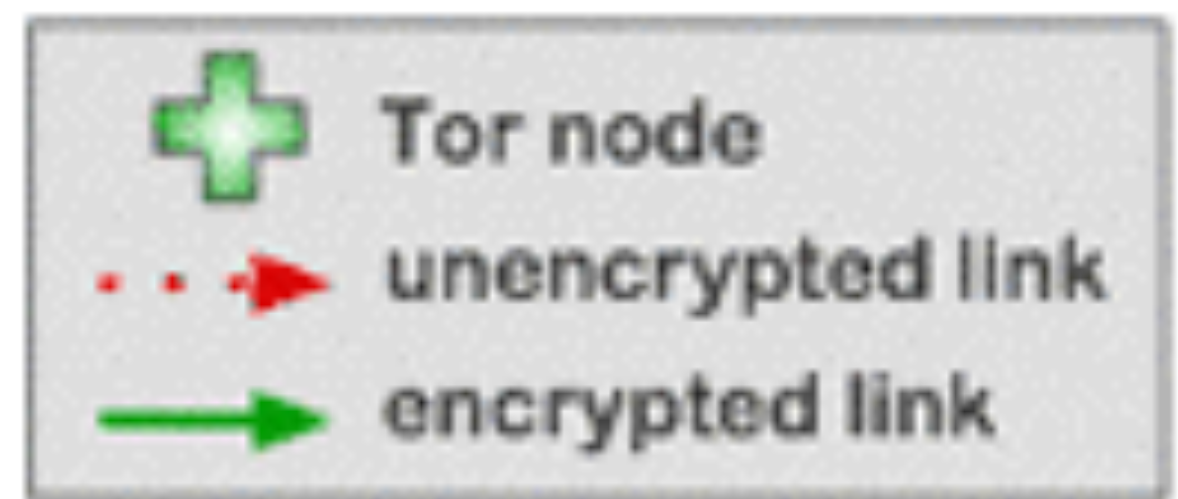
Well, Tor Seems Great!



But There's A Problem



How Tor Works



Hidden Services



<http://fkdheignoueupfmf.onion/>

<http://facebookcorewwi.onion/>

```
Cooking up some delicious scallions...
Using kernel optimized from file kernel.cl (Optimized4)
Using work group size 128
Compiling kernel... done.
Testing SHA1 hash...
CPU SHA-1: d3486ae9136e7856bc42212385ea797094475802
GPU SHA-1: d3486ae9136e7856bc42212385ea797094475802
Looks good!
LoopIteration:40 HashCount:671.09MH Speed:9.5MH/s Runtime:
00:01:10 Predicted:00:00:56 Found new key! Found 1 unique keys.
<XmlMatchOutput>
  <GeneratedDate>2014-08-05T07:14:50.329955Z</GeneratedDate>
  <Hash>prefix64kxpwmzdz.onion</Hash>
  <PrivateKey>-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCmYmTnwG0CpsP0qvs5mZQbIM1TTq0HK1r6zGvpk61ZaT7z2BCE
FPvdTdkZ4tQ3/95ufjhPx7EVDjeJ/JUbT0QAW/Yf1zUfFJuB1i0J2eUJzhhiHpC/
1d3rb6Uhnwvv3xSnfG8m7LeI/Ao3FLtyZFgGZPwsw3BZYyJn3sD1mJIJrQIEB/ZP
ZwKBgQCTU0TR4zcz65zS0fo9513YetVhfmAnYc00d8HTxqTqEsir00Xzw799ioTWt
```


But Drupal?



Drupal Hidden Services

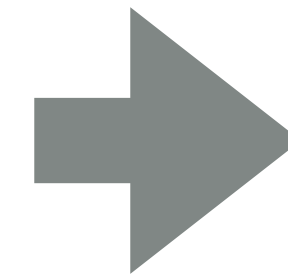
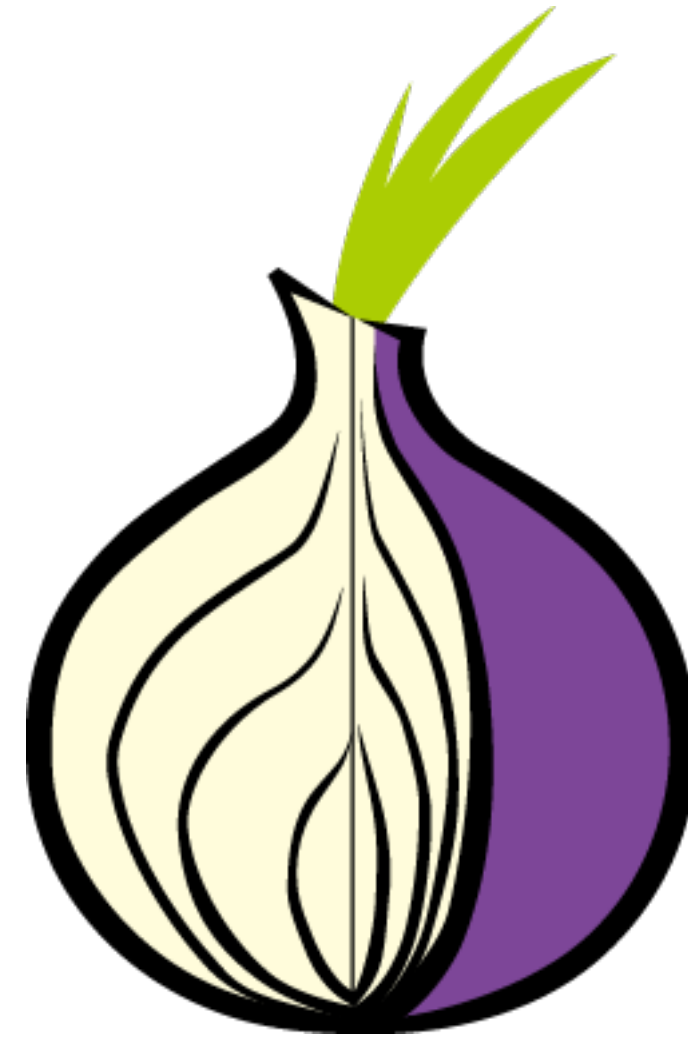
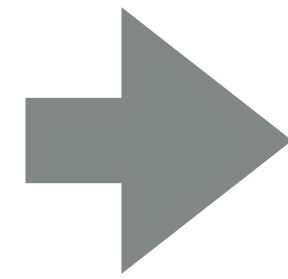
- Drupal Module (<http://dgo.to/tor>)
 - Very out of date, somewhat clunky
- Tor on Production Server
 - Complicates production server
 - Potential attack vectors
- Something else?



a unified theory of the
web

david weinberger

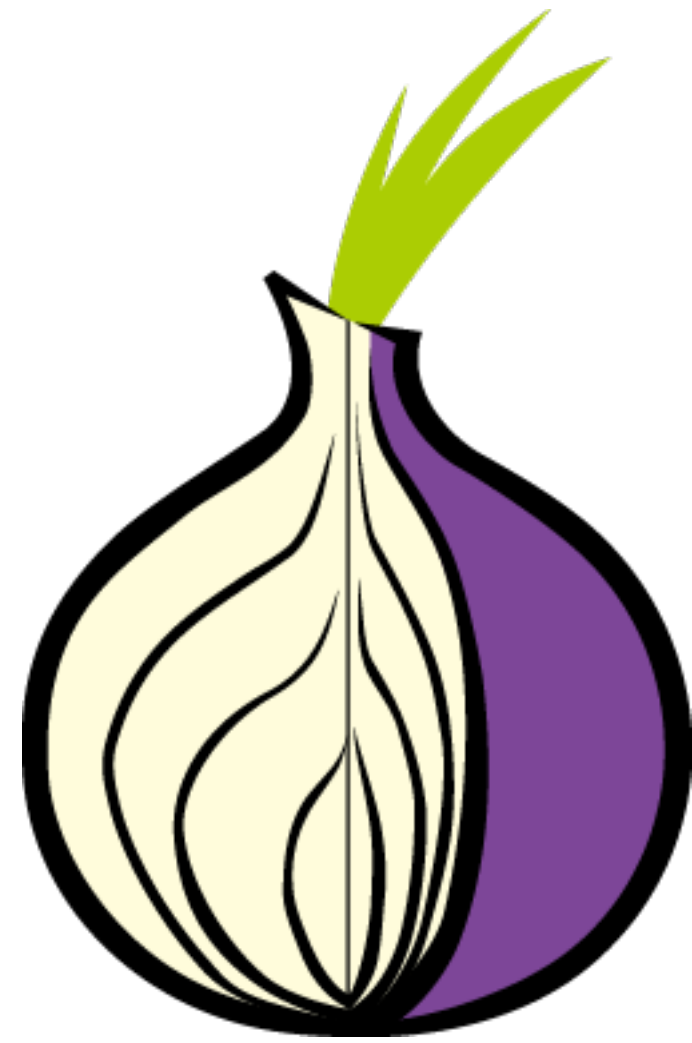
The Unix Way™



Reverse Proxy Setup

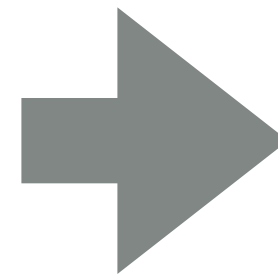
- Drupal server only accessed as standard web server
 - Can't blame Tor if the server white screens
- Drupal server can continue to collect logs normally
 - Tor server can be locked down and scrubbed

Ideal Setup



192.168.1.100

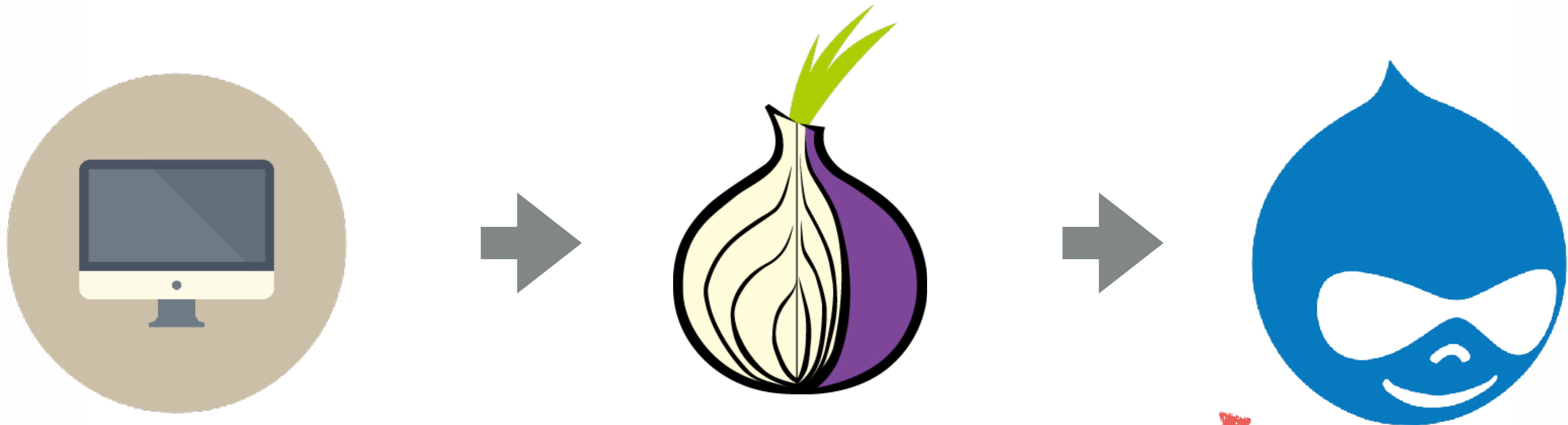
Private Networking



192.168.1.101

An Important Step

<http://fkdhaignoueupfmf.onion/>



<http://website.org/node/42>


```
### SUBS https://github.com/yaoweibin/
ngx_http_substitutions_filter_module ###
    # We're rewriting links, but we need to preserve
    rel=canonical for analytics.
    subs_filter "rel=\"canonical\" href=\"http://
www.website.org\" \"-----CANONICALHTTPfdgDOTORG-----\" i;
    subs_filter "rel=\"canonical\" href=\"https://
www.website.org\" \"-----CANONICALHTTPSfdgDOTORG-----\" i;
    # Keep links in .onion
    subs_filter (http:|https:)?//(www\.)?website.org //$server_name
gir;
    # Restore the rel="canonical" tag
    subs_filter "-----CANONICALHTTPfdgDOTORG-----"
"rel=\"canonical\" href=\"http://www.website.org\" i;
    subs_filter "-----CANONICALHTTPSfdgDOTORG-----"
"rel=\"canonical\" href=\"https://www.website.org\" i;
    ### /SUBS ###
```

```
g_=_p=_
    # We're rewriting links, but we need to preserve
rel=canonical for analytics.
    subs_filter "rel=\"canonical\" href=\"http://
www.website.org" "-----CANONICALHTTPfdgDOTORG-----" i;
    subs_filter "rel=\"canonical\" href=\"https://
www.website.org" "-----CANONICALHTTPSfdgDOTORG-----" i;
    # Keep links in .onion

subs_filter (http:|https:)?//
(www\.)?website.org // $server_name
gir;

    # Restore the rel="canonical" tag
    subs_filter "-----CANONICALHTTPfdgDOTORG-----"
"rel=\"canonical\" href=\"http://www.website.org" i;
    subs_filter "-----CANONICALHTTPSfdgDOTORG-----"
"rel=\"canonical\" href=\"https://www.website.org" i;
```



```
### HEADERS http://wiki.nginx.org/HttpHeadersMoreModule ###
    more_clear_headers "Age";
    more_clear_headers "Server";
    more_clear_headers "Via";
    more_clear_headers "X-From-Nginx";
    more_clear_headers "X-NA";
    more_clear_headers "X-Powered-By";
    more_clear_headers "X-Request-Id";
    more_clear_headers "X-Runtime";
    more_clear_headers "X-Varnish";
    more_clear_headers "Content-Security-Policy-Report-Only";
### /HEADERS ###

}
```

Ideal Setup





INDEPENDENT



[News](#) > [World](#) > [Europe](#)

Turkey coup attempt: UN warns Erdogan government purges could violate international law after 40,000 detained

It's only illegal if you *get caught*
- me, 1998

It's only secure if they can't
prove anything

- me, 2016

Ideal Setup

- All logging turned off
 - All log paths set to /dev/null
 - Belt and suspenders?
- Increase speed
 - One 🐒 instead of three?

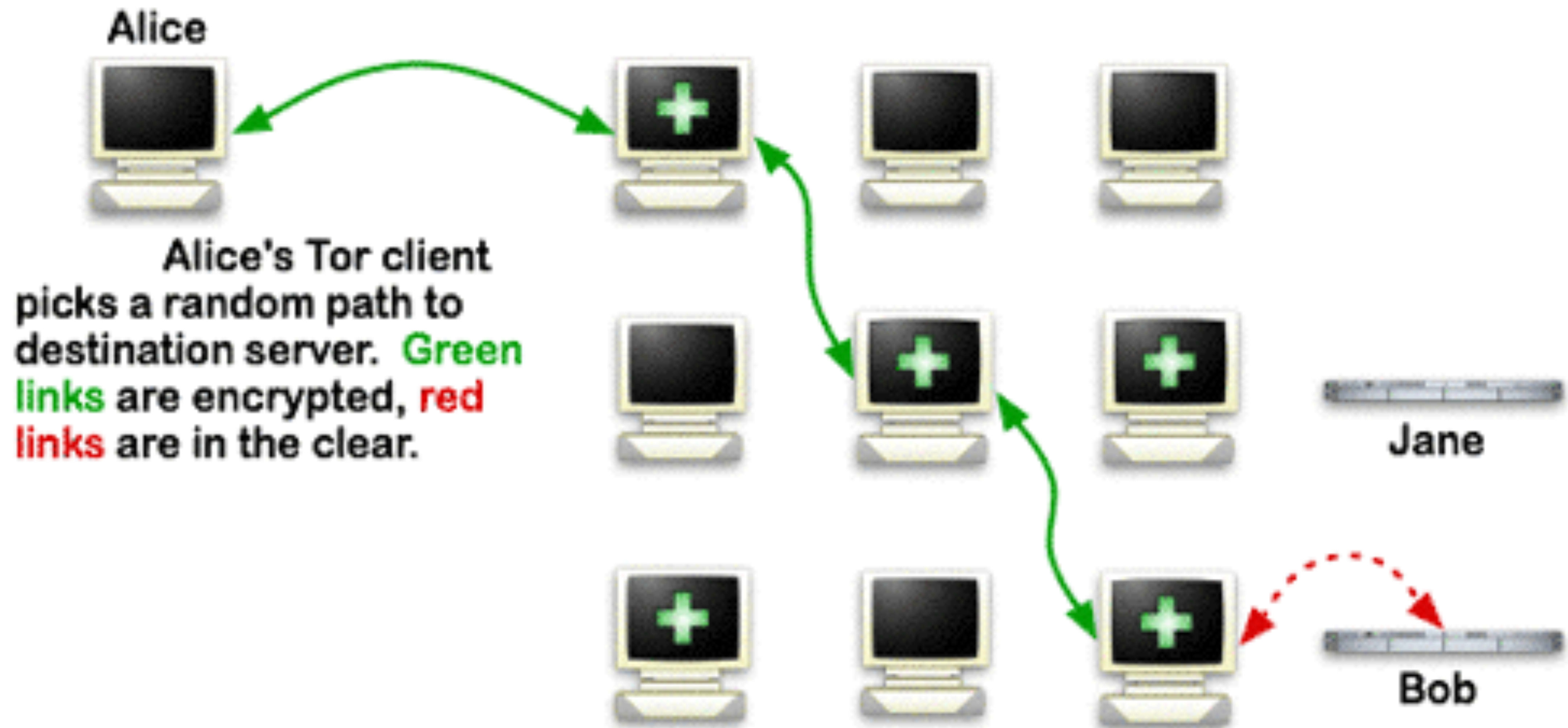
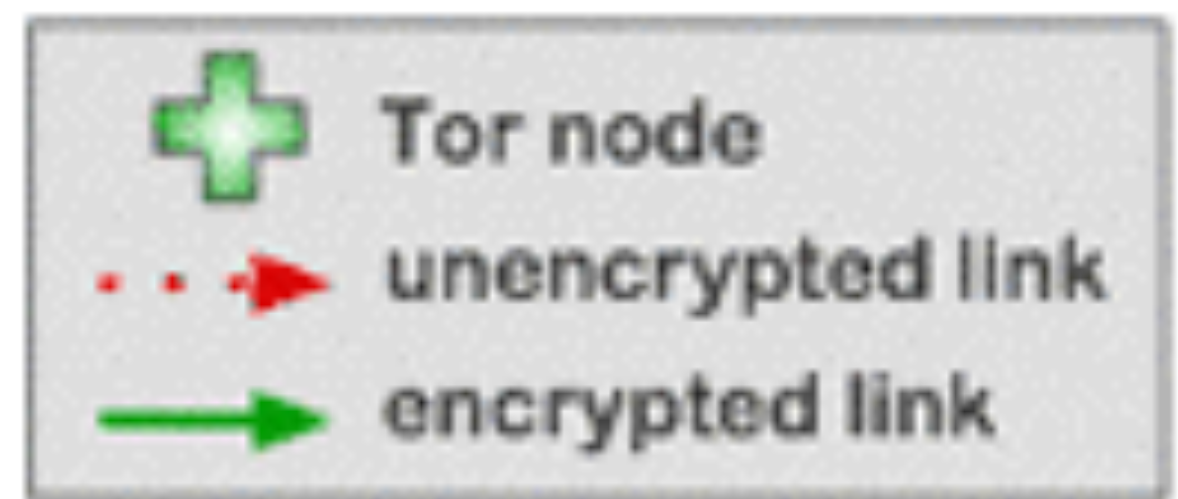
Future Improvements

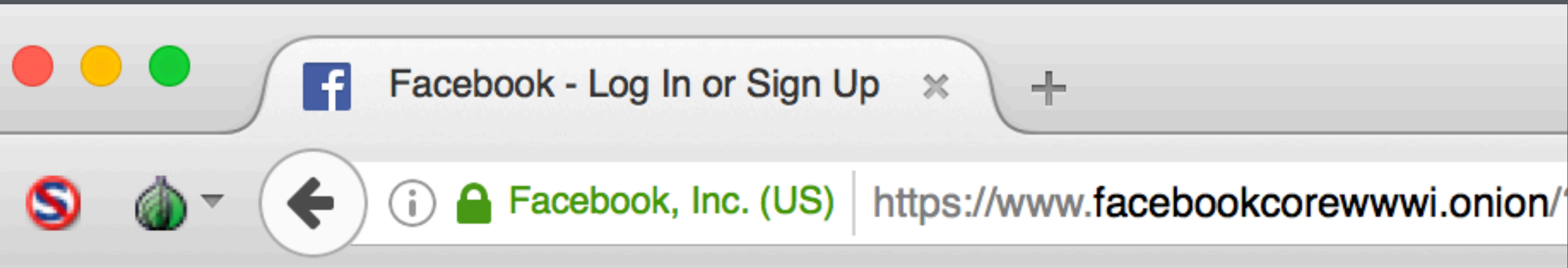
- Future Improvements
 - Single Onion Services - 1 hop server (🐒)
 - OnionBalance - load balancing
 - SSL Certificates

There Can Be Only One

- Hidden sites, by their nature, have unique and secure URLs
- It's still possible to be exposed to malicious Tor nodes
- Your browser might try to communicate to non-Onion addresses

How Tor Works





facebook

There Can Be Only One

- DigiCert
 - Only game in town, currently

September 11, 2015 by [Jeremy Rowley](#)+

Posted Under: [Browser](#), [Encryption](#), [News](#)

.Onion Officially Recognized as Special-Use Domain

.Onion now classified as a special-use, top-level domain by Internet Engineering Steering Group (IESG).

There Can Be Only One

- DigiCert
 - Only game in town, currently
 - Working to standardize .onion as a TLD

Extra Credit Assignments

- Generally secure networking - email, calendar, etc
- OnionShare filesharing
- Non-hidden but protected sharing (Tor + secret key)
 - A true speakeasy!
- DNS circumventing routing - share your localhost

Resource Links

General:

<https://www.torproject.org/about/overview.html.en>

<https://www.torproject.org/docs/hidden-services.html.en>

<https://www.eff.org/pages/tor-and-https>

ProPublica setup:

<https://www.propublica.org/nerds/item/a-more-secure-and-anonymous-propublica-using-tor-hidden-services>

<https://gist.github.com/mtigas/9a7425dfdacda15790b2>

HTTPS:

<https://www.cybersecureasia.com/blog/tor-ssl-onion-certificate-from-digicert>

Vanity URL:

<http://www.zdnet.com/article/facebook-sets-up-hidden-service-for-tor-users/>

Future Stuff:

<http://onionbalance.readthedocs.io/en/latest/>

<https://lists.torproject.org/pipermail/tor-dev/2015-October/009762.html>

<https://trac.torproject.org/projects/tor/ticket/17178>

<https://lists.torproject.org/pipermail/tor-dev/2015-October/009607.html>

@milsyobtaf

Thanks!
Questions?

@milsyobtaf

<https://github.com/milsyobtaf/prez>