The Digital Speakeasy: Secure and Anonymous Access to Your Website

php[world] 11/15/2017

Howdy!
I’m an engineer at Acquia

Dustin Younse
@milsyobtaf
https://github.com/milsyobtaf/prez

What Is The Digital Speakeasy?

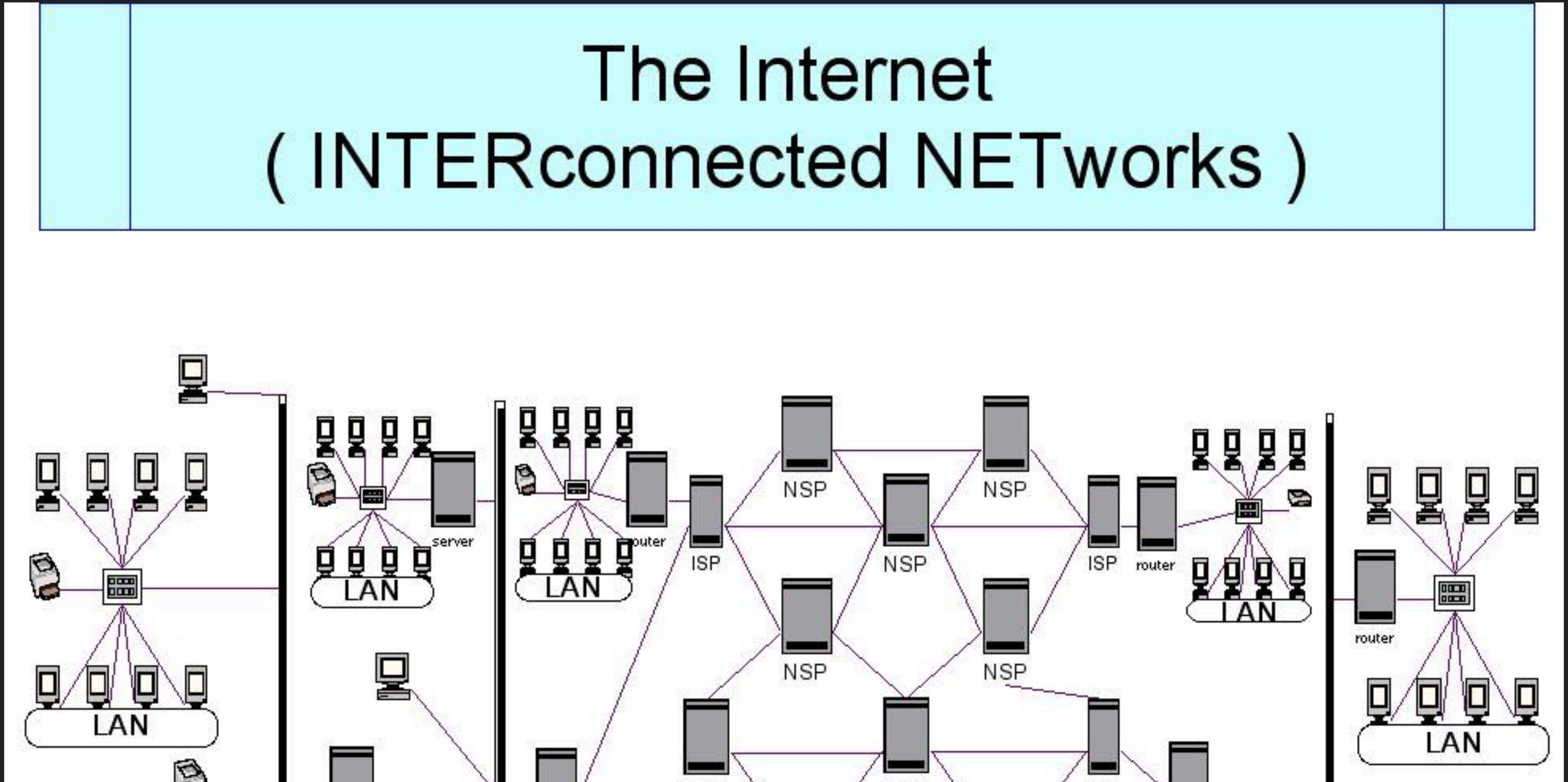
Browsing in Secret

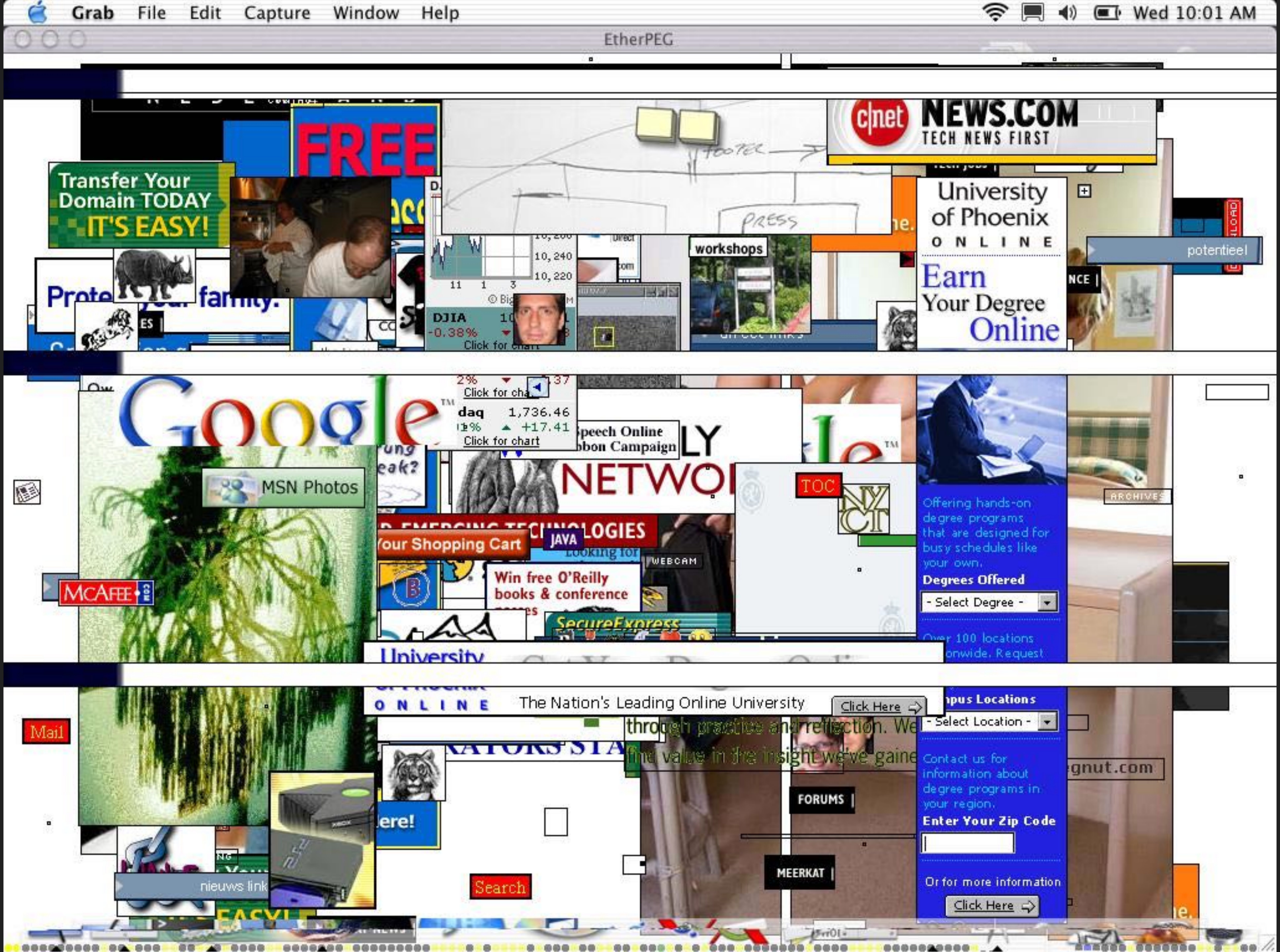
- Plain Text browsing

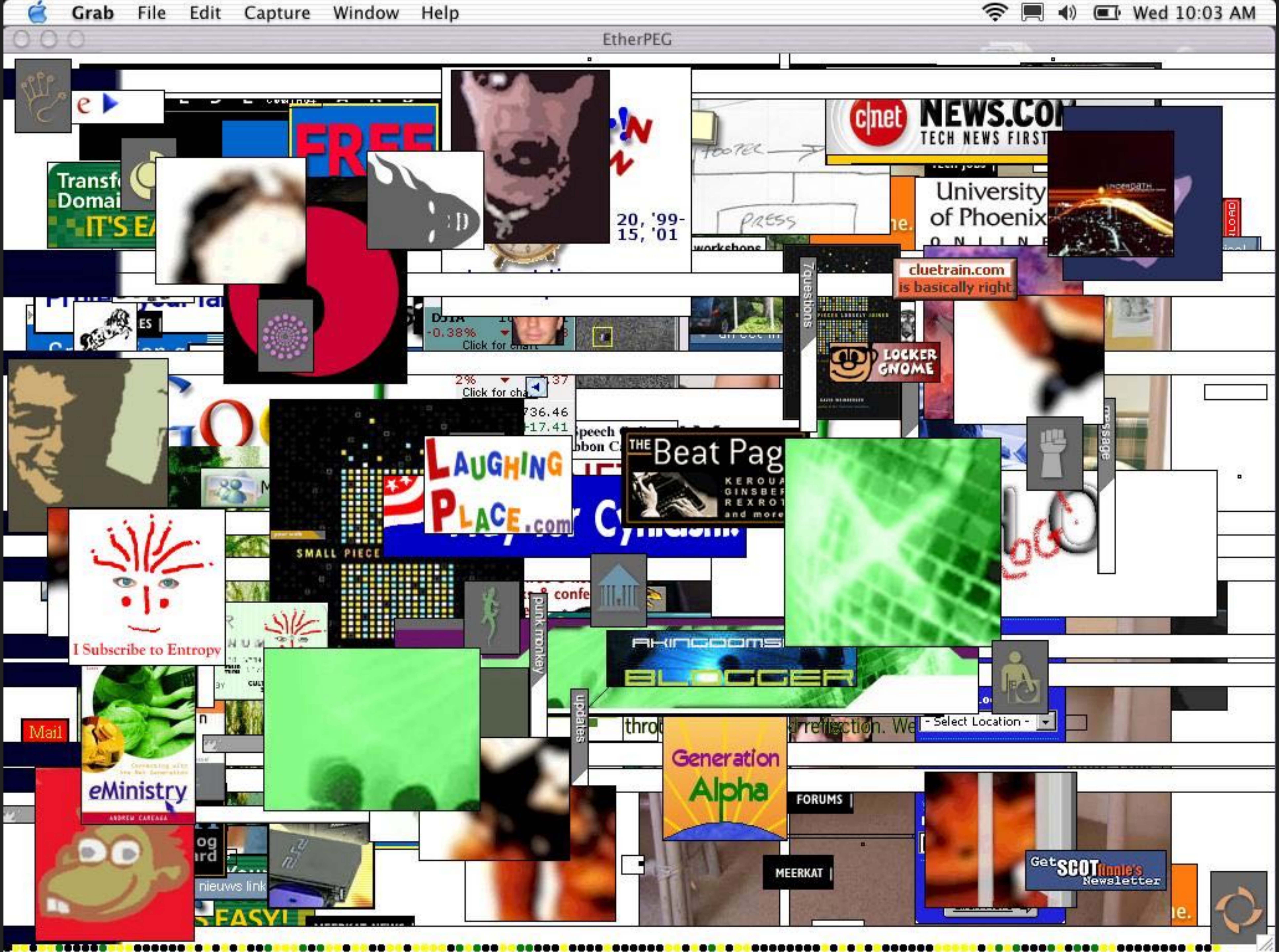
```
<!DOCTYPE html>
<html lang="en-US">
  <head>
    <meta charset="utf-8">
    <title>Web design, development, and strategy |
Four Kitchens</title>
    <meta name="viewport" content="width=device-
width, initial-scale=1.0, maximum-scale=1.0">
    <meta property="og:title" content="Web design,
development,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

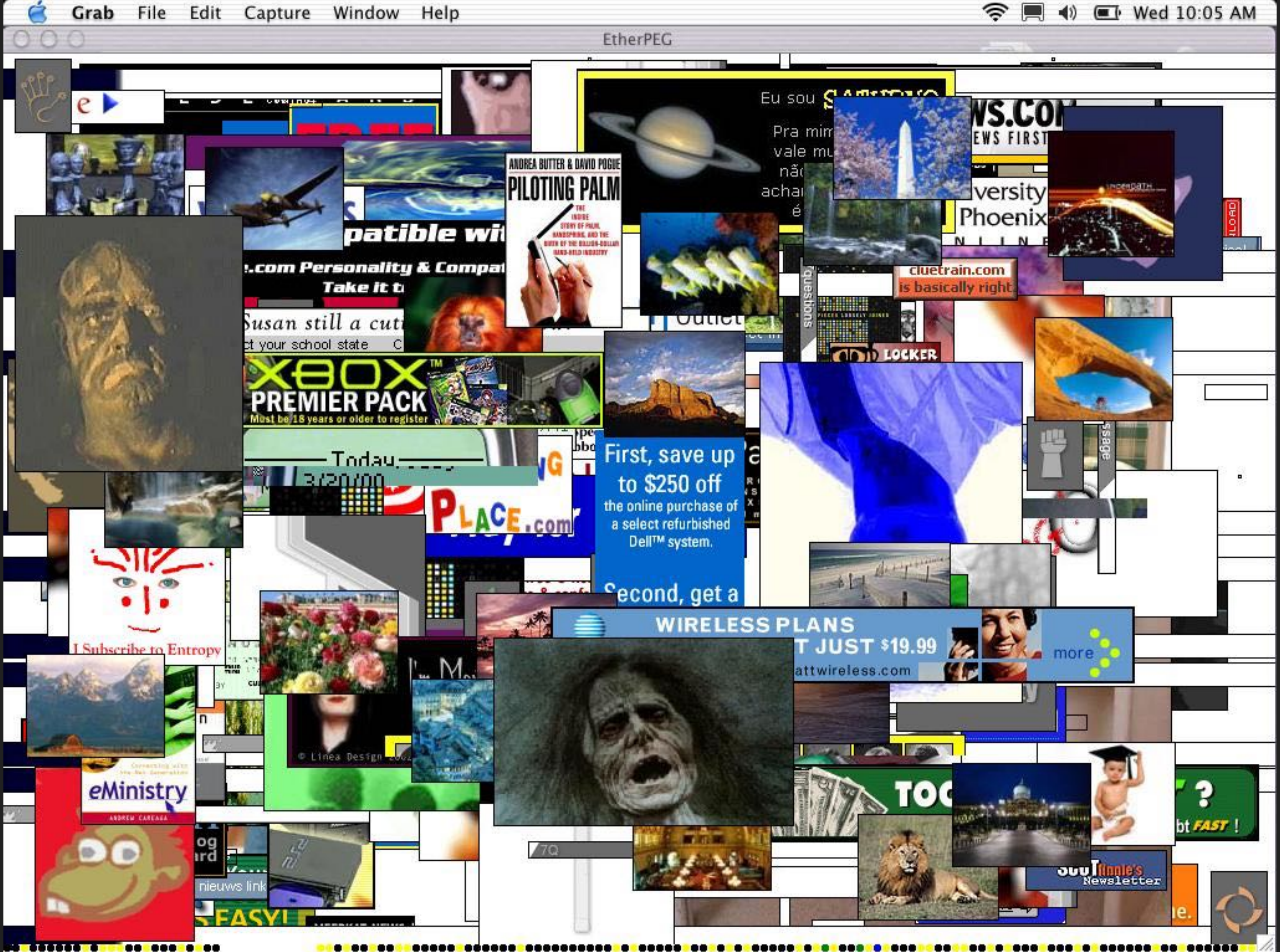
```
HTTP/1.1 200 OK
Server: nginx/1.6.1
Date: Sat, 20 Aug 2016 03:42:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 56595
Last-Modified: Wed, 17 Aug 2016 00:07:26 GMT
Connection: keep-alive
Vary: Accept-Encoding
ETag: "57b3aabe-dd13"
Expires: Sun, 21 Aug 2016 03:42:11 GMT
Cache-Control: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

The Internet Is Trusting By Default




Grab File Edit Capture Window Help
Wed 10:01 AM
EtherPEG
FREE
cnet NEWS.COM
TECH NEWS FIRST
Transfer Your Domain TODAY IT'S EASY!
FOOTER
PRESS
workshops
University of Phoenix ONLINE
Earn Your Degree Online
potentieel
DJIA -0.38%
Click for chart
daq 1,736.46 +17.41
Google
MSN Photos
Speech Online
bbon Campaign
NETWO
TOC
EMERGING TECHNOLOGIES
Your Shopping Cart
JAVA
WEBCAM
Win free O'Reilly books & conference
SecureExpress
McAFEE.COM
Offering hands-on degree programs that are designed for busy schedules like your own.
Degrees Offered
- Select Degree -
Over 100 locations nationwide. Request
ARCHIVES
The Nation's Leading Online University
Click Here
through practice and reflection. We
the value in the insight we've gained
Campus Locations
- Select Location -
Contact us for information about degree programs in your region.
Enter Your Zip Code
Or for more information
Click Here
Mail
FORUMS
MEERKAT
Search
nieuws link
gnut.com


Grab File Edit Capture Window Help
Wed 10:03 AM
EtherPEG
FREE
Transfer Domai IT'S EA
cnet NEWS.COM TECH NEWS FIRST
University of Phoenix ONLINE
cluetrain.com is basically right
20, '99-
15, '01
FOOTER
PRESS
workshops
7questions
DJIA -0.38% Click for chart
2% Click for chart
736.46
+17.41
LOCKER GNOME
LAUGHING PLACE.com
THE Beat Page KEROUAC GINSBERG REXROTH and more
SMALL PIECE
I Subscribe to Entropy
punk monkey
updates
message
conference
BLOGGER
- Select Location -
Generation Alpha
FORUMS
MEERKAT
Mail
eMinistry
nieuws link
EASY!
Get SCOT finnie's Newsletter


Grab
File
Edit
Capture
Window
Help
Wed 10:05 AM
EtherPEG
Eu sou
Pra mim
vale mu
não
achar
é
ws.com
EWS FIRST
versity
Phoenix
ANDREA BUTTER & DAVID POGUE
PILOTING PALM
THE INSIDE STORY OF PALM, HANDSPRING, AND THE BIRTH OF THE BILLION-DOLLAR HAND-HELD INDUSTRY
patible wi
.com Personality & Compat
Take it t
Susan still a cut
ct your school state
cluetrain.com
is basically right
Questions
LOCKER
XBOX
PREMIER PACK
Must be 18 years or older to register
Today
3/20/00
PLACE.com
First, save up to $250 off the online purchase of a select refurbished Dell™ system.
Second, get a
I Subscribe to Entropy
WIRELESS PLANS
T JUST $19.99
attwireless.com
more
© Linea Design
eMinistry
ANDREW CAREAGA
nieuws link
EASY!
TOO
Newsletter
bt FAST !

Browsing in Secret

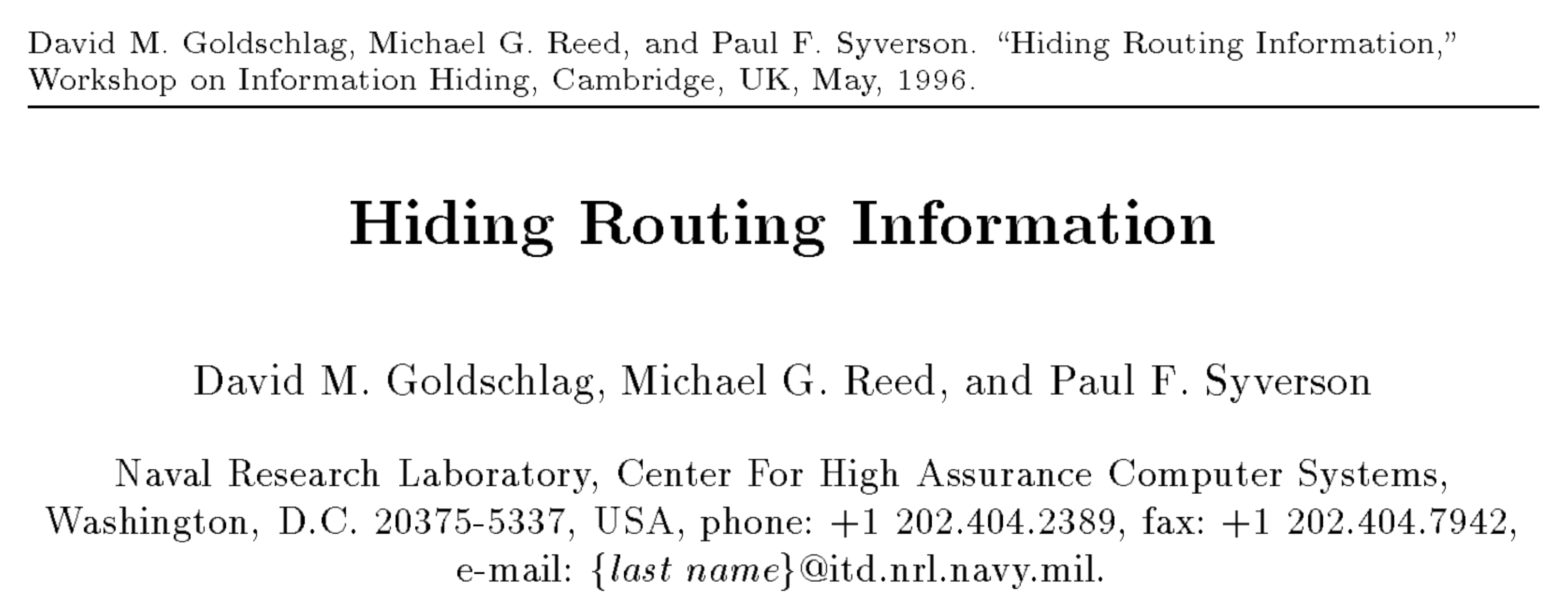
- Plain Text browsing
- HTTPS browsing

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

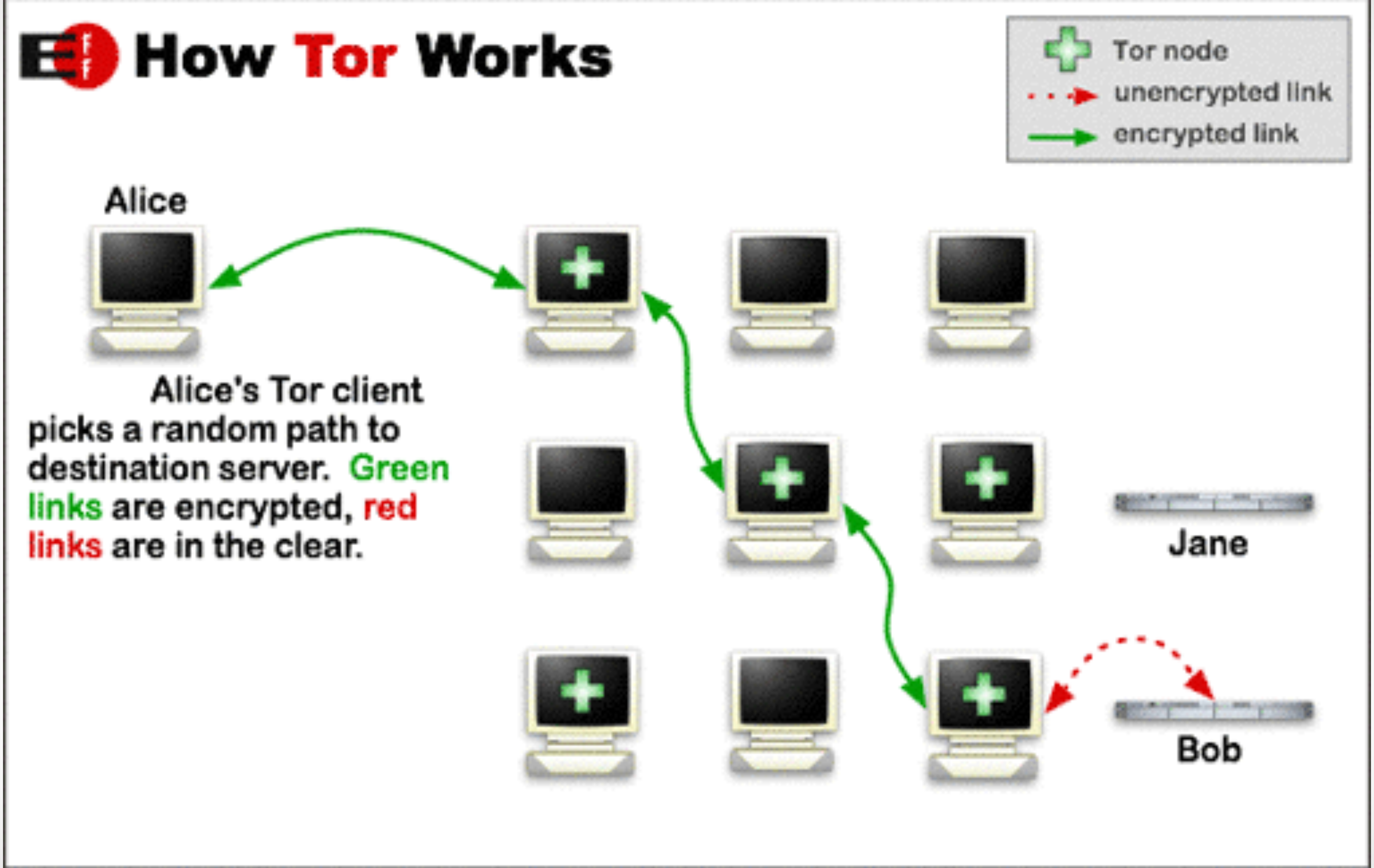
Hiding Routing Information

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

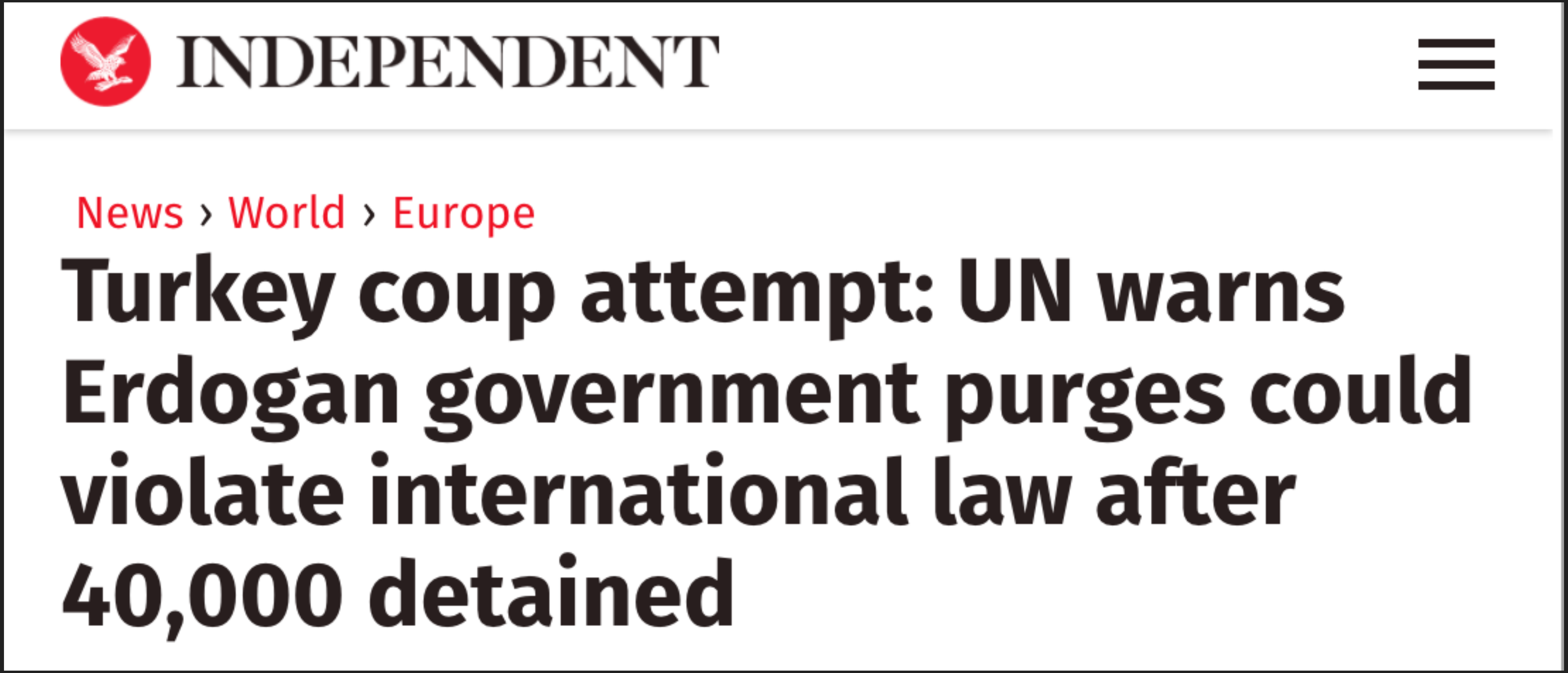
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

The Rule of Three

So Why Bother?

The Importance of Privacy

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



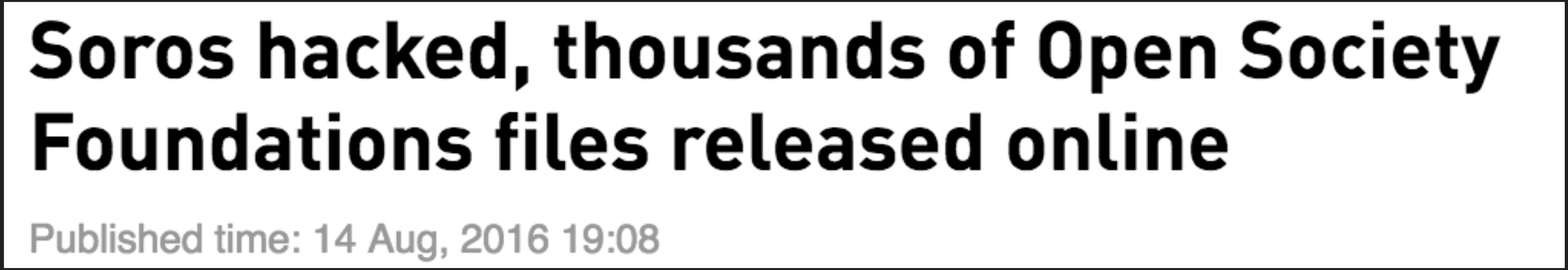
INDEPENDENT

News › World › Europe

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

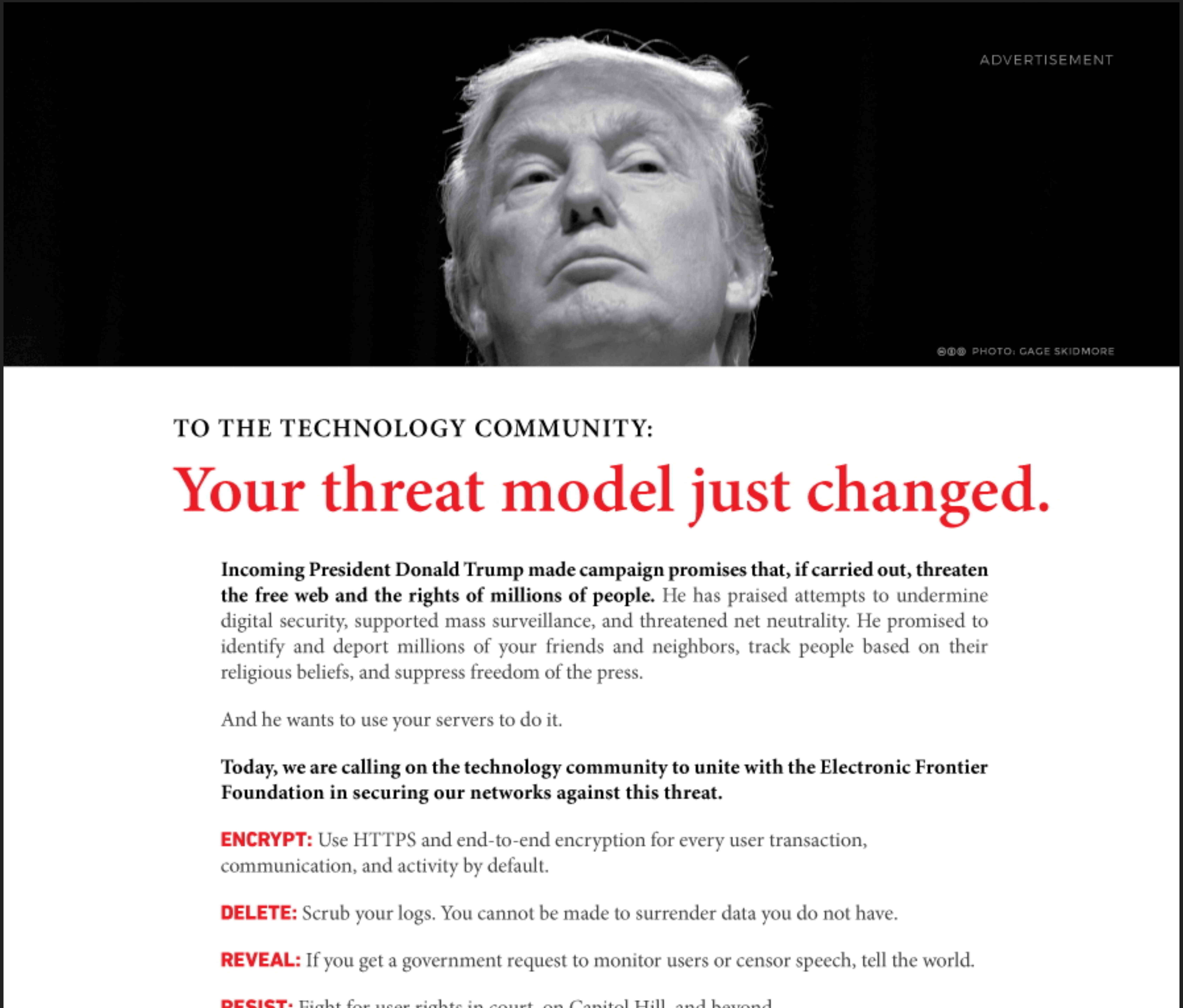
The Importance of Privacy

- 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



ADVERTISEMENT

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.

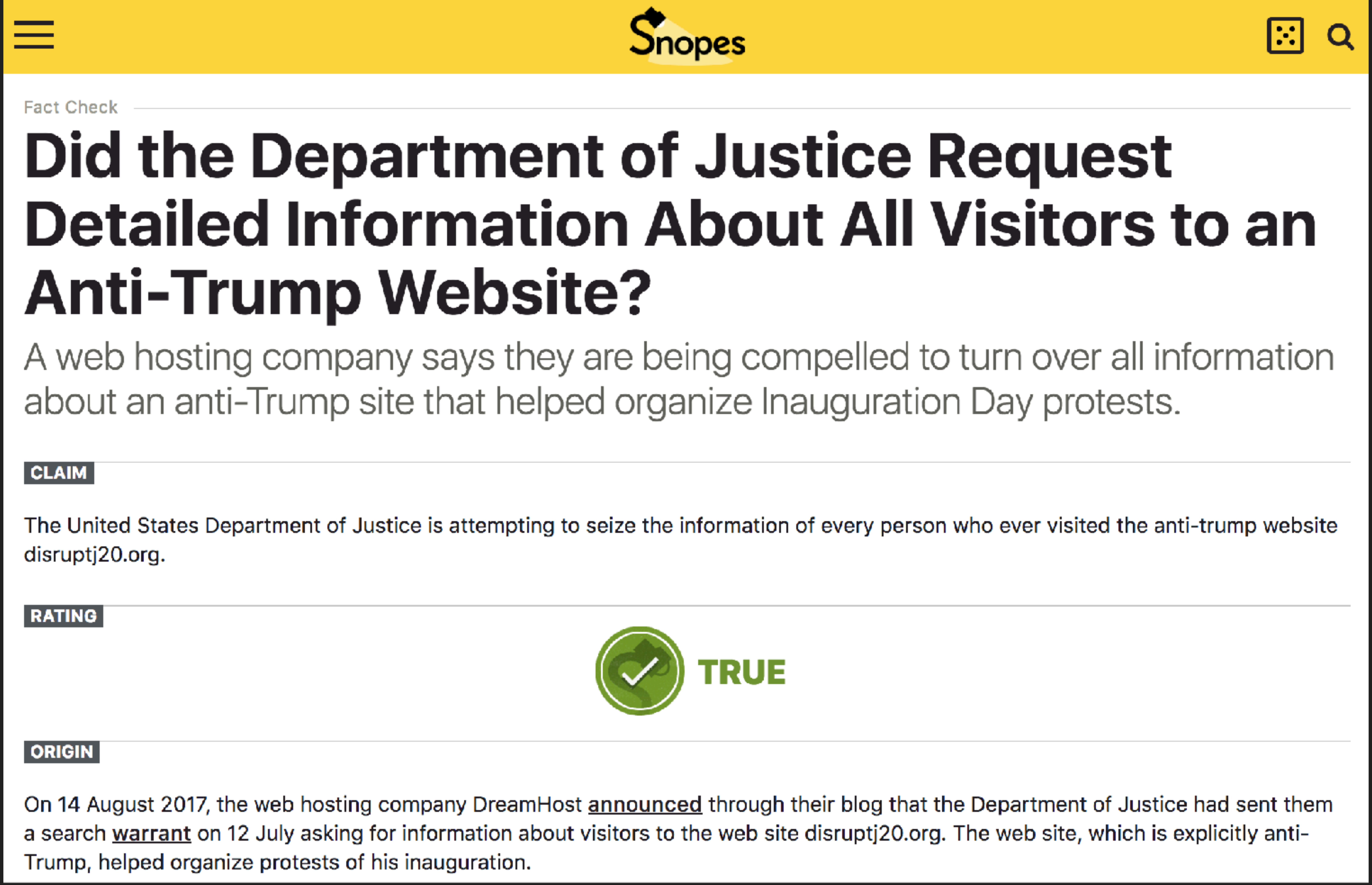
Today, we are calling on the technology community to unite with the Electronic Frontier Foundation in securing our networks against this threat.

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.



Snopes

Fact Check

Did the Department of Justice Request Detailed Information About All Visitors to an Anti-Trump Website?

A web hosting company says they are being compelled to turn over all information about an anti-Trump site that helped organize Inauguration Day protests.

CLAIM

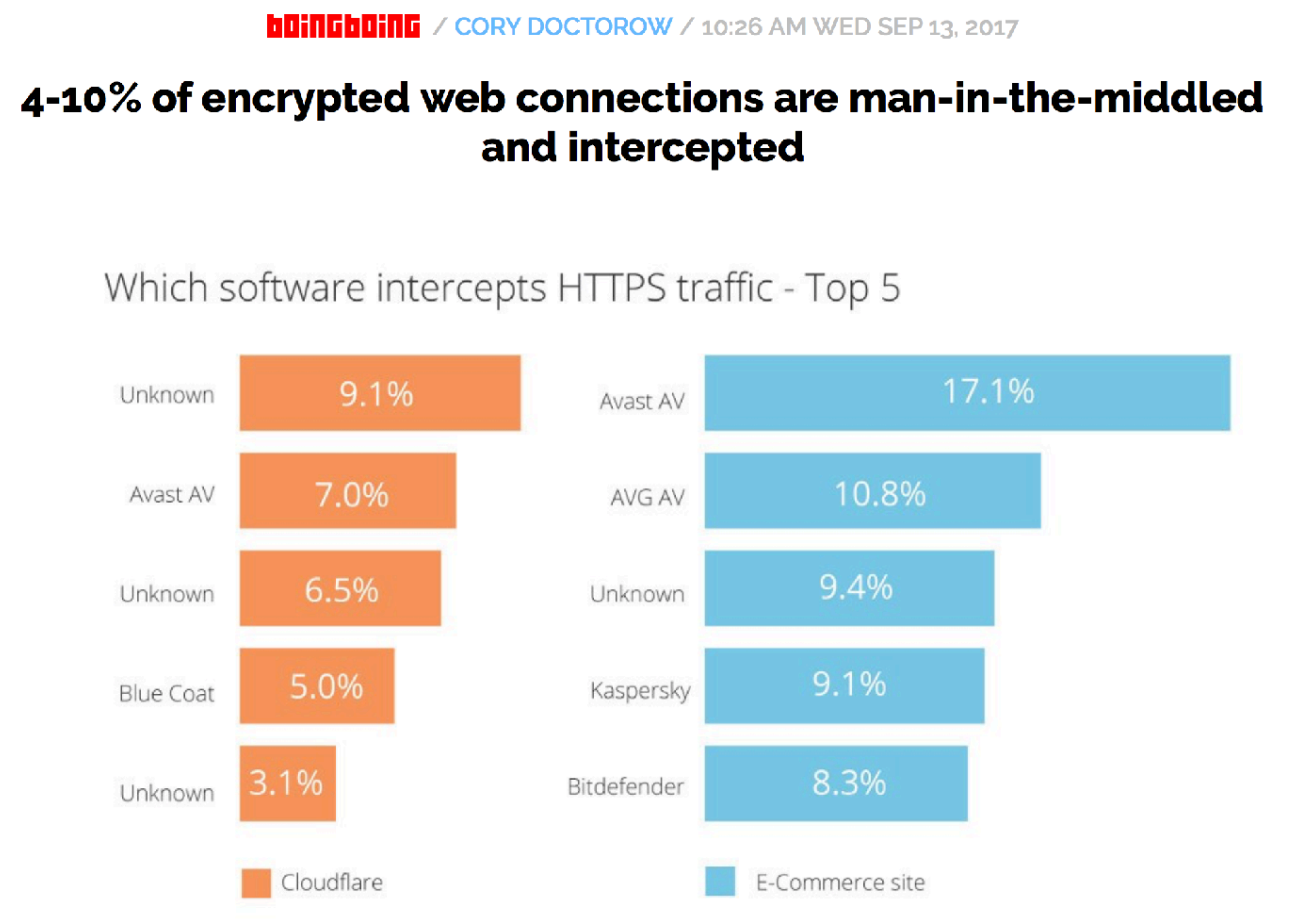
The United States Department of Justice is attempting to seize the information of every person who ever visited the anti-trump website disruptj20.org.

RATING

✓ TRUE

ORIGIN

On 14 August 2017, the web hosting company DreamHost announced through their blog that the Department of Justice had sent them a search warrant on 12 July asking for information about visitors to the web site disruptj20.org. The web site, which is explicitly anti-Trump, helped organize protests of his inauguration.



bOiNGbOiNG / CORY DOCTOROW / 10:26 AM WED SEP 13, 2017

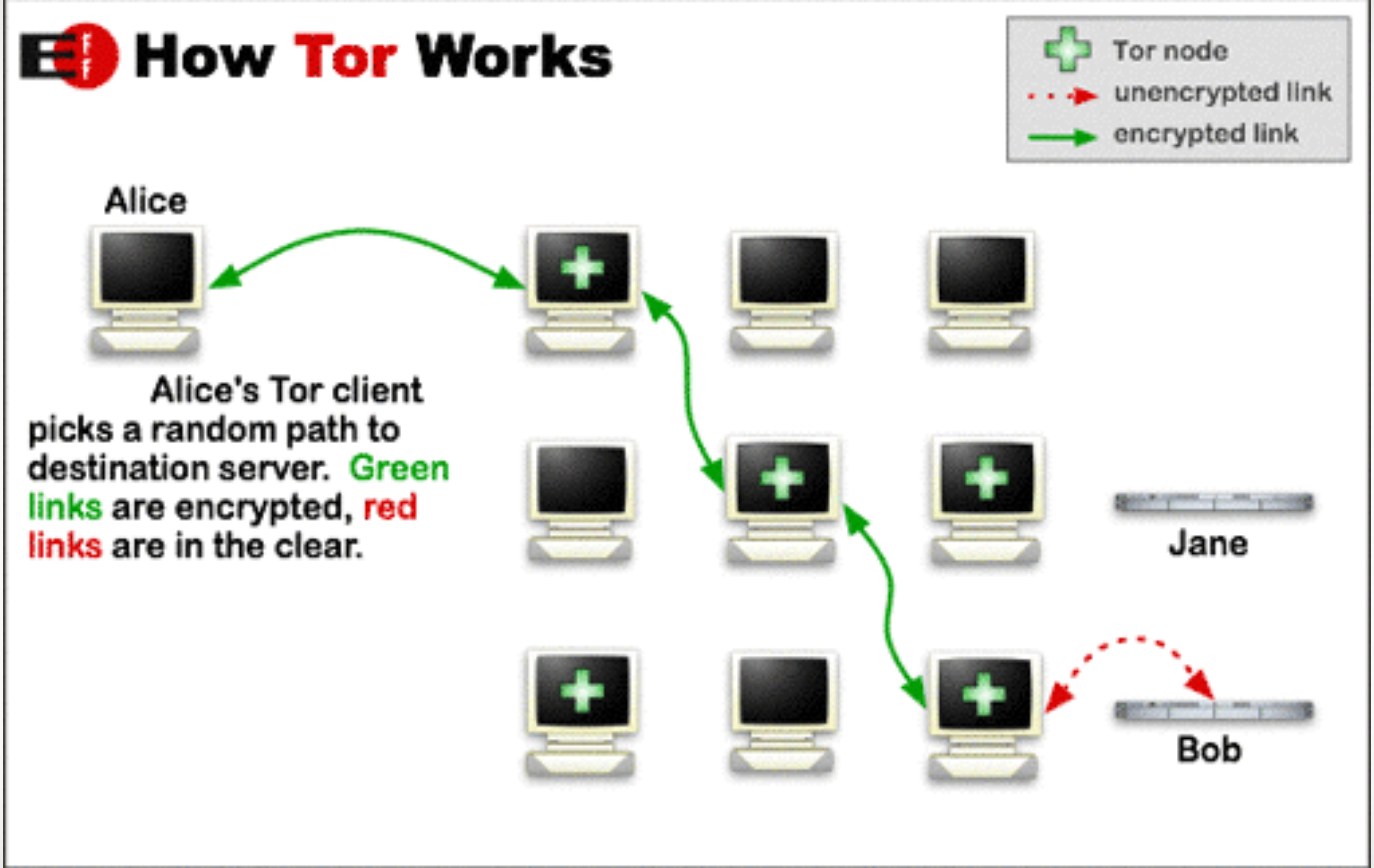
4-10% of encrypted web connections are man-in-the-middled and intercepted

Which software intercepts HTTPS traffic - Top 5

Well, Tor Seems Great!

But There's A Problem

How Tor Works



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

Hidden Services

http://fkdheignoueupfmf.onion/

http://facebookcorewwwi.onion/

http://www.nytimes3xbfgragh.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-----
MIICXAIBAAKBgQCmYmTnwGOCpsPOqvs5mZQbIM1TTqOHK1r6zGvpk61ZaT7z2BCE
FPvdTdkZ4tQ3/95ufjhPx7EVDjeJ/JUbT0QAW/YflzUfFJuBli0J2eUJzhhiHpC/
1d3rb6Uhnwvv3xSnfG8m7LeI/Ao3FLtyZFgGZPwsw3BZYyJn3sD1mJIJrQIEB/ZP
ZwKBgCTUOTR4zcz65zSOfo95l3YetVhfmApYcOOd8HTxqTqEsjr00XzW799joIWt
```

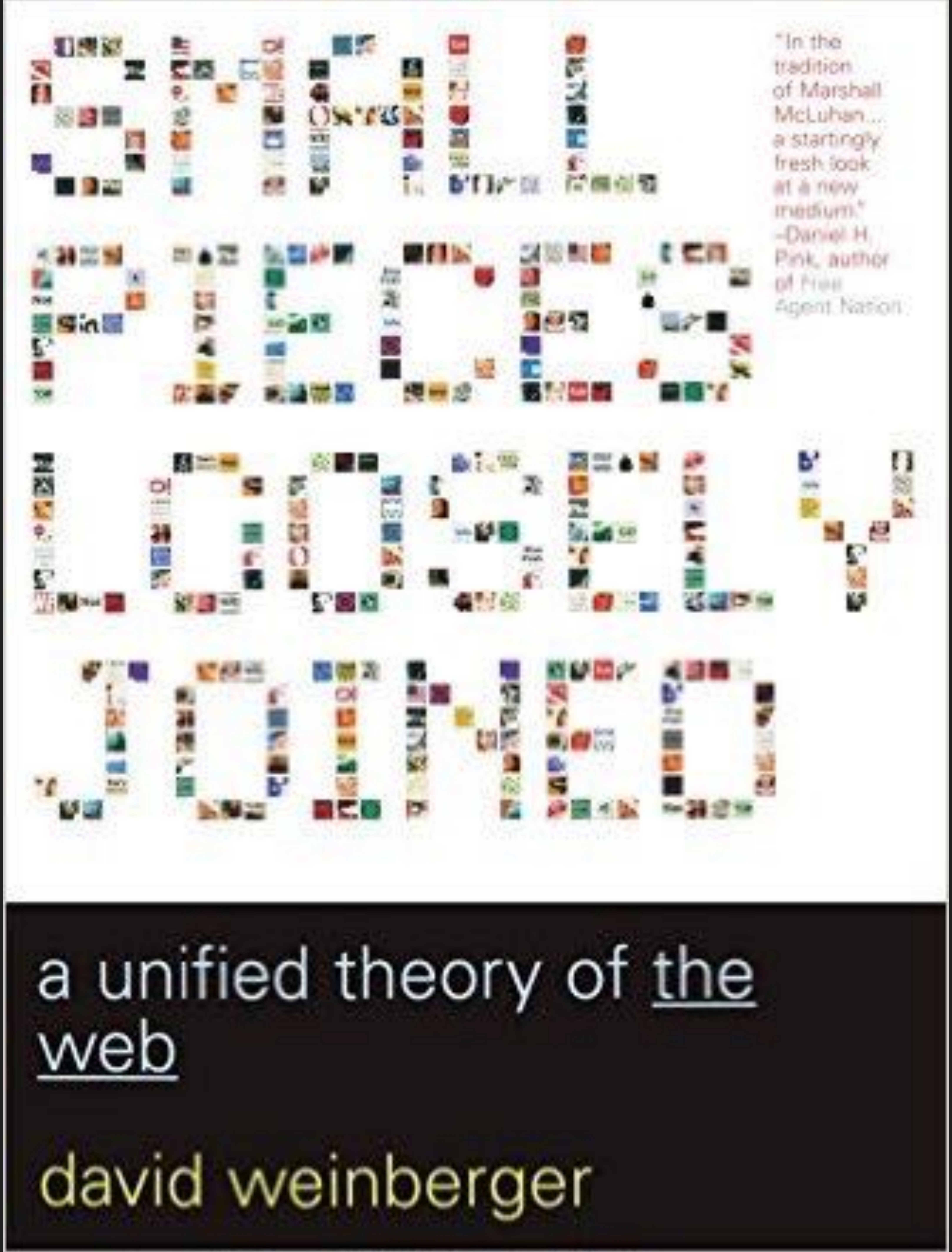
Caveat Typor

- Reduction of randomness per character
  - Loss of .onion domain
- Phishing attacks
  - **smspriv6fynj23u6**.onion vs **smsprivyevs6xn6z**.onion

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?



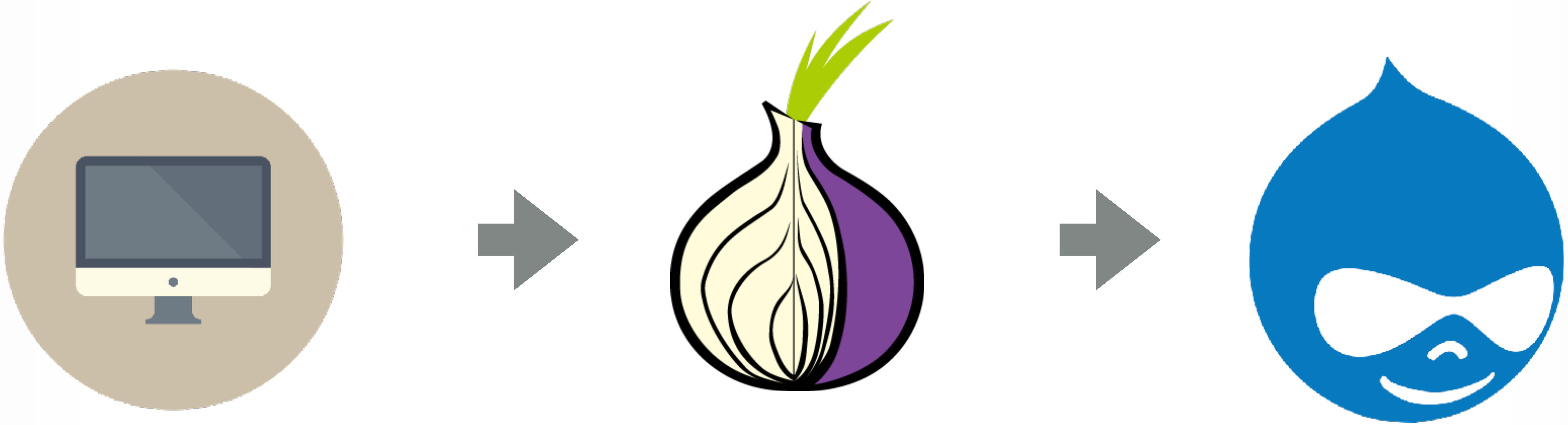
SMALL PIECES LOOSELY JOINED

"In the tradition of Marshall McLuhan... a startingly fresh look at a new medium." –Daniel H. Pink, author of *Free Agent Nation*

a unified theory of the web

david weinberger

The Unix Way™



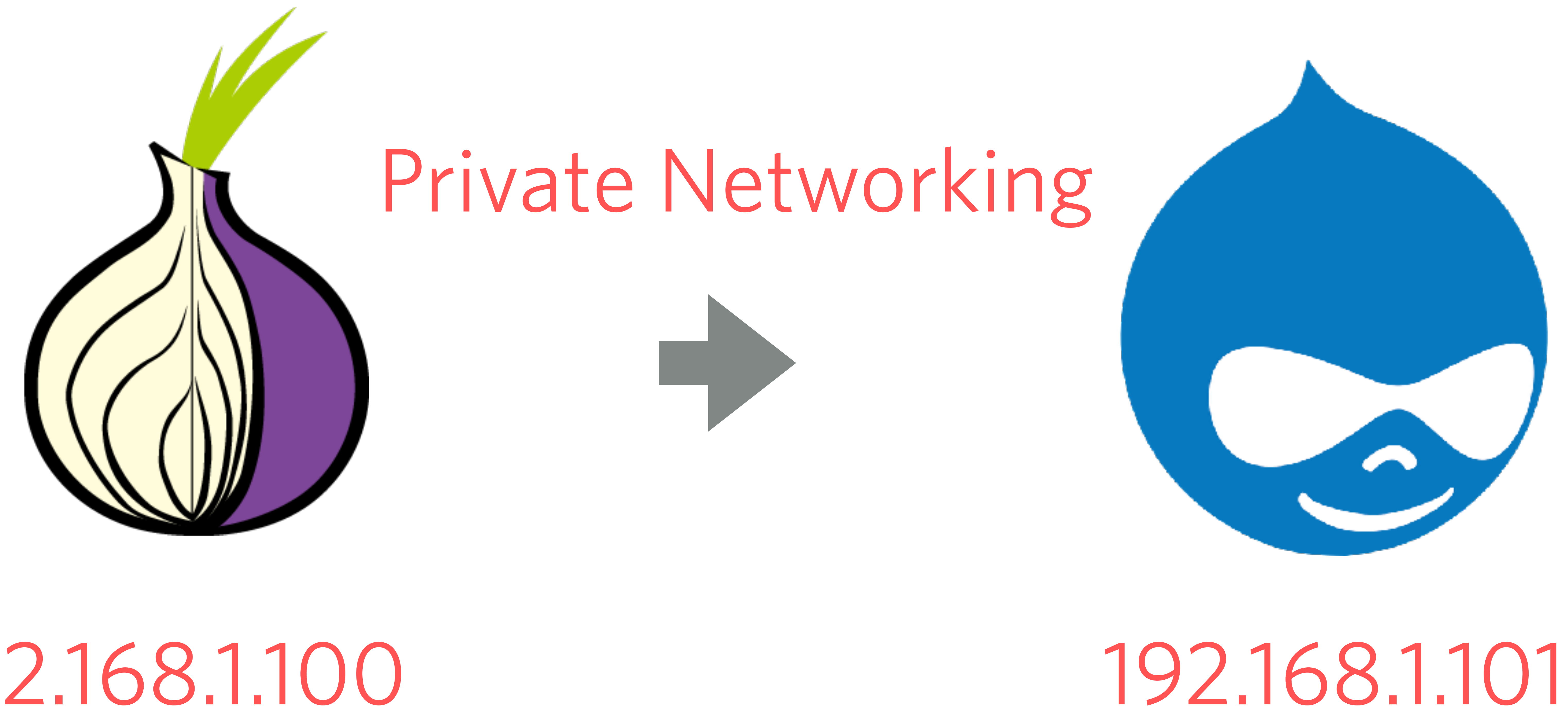
Reverse Proxy Setup

- 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

```
# Try to run Tor more securely via a syscall sandbox.
# https://www.torproject.org/docs/tor-manual.html.en#Sandbox
Sandbox 1

# Disable the SOCKS port. Not like anything else on this box is using tor.
SocksPort 0

HiddenServiceDir /var/lib/tor/hidserv
#HiddenServicePort 80 127.0.0.1:80

HiddenServicePort 80  unix:/var/run/nginx-80.sock
#HiddenServicePort 443 unix:/var/lib/nginx/nginx-443.sock
```

```
server {
    server_name fdg22p3lmweopgho.onion;
    listen unix:/var/run/nginx-80.sock;
    allow "unix:";
    deny all;
    #listen 80;
    #allow 127.0.0.1;

    # Set cache on this nginx end so that we avoid fetching from
    # the real infrastructure when possible.
    proxy_cache tor;
    proxy_cache_valid any 5m;
    proxy_cache_revalidate on;
    proxy_cache_use_stale timeout updating;
    proxy_cache_key $request_uri;
    proxy_ignore_headers expires set-cookie;

    server_tokens off;
```

Ideal Setup



Private Networking

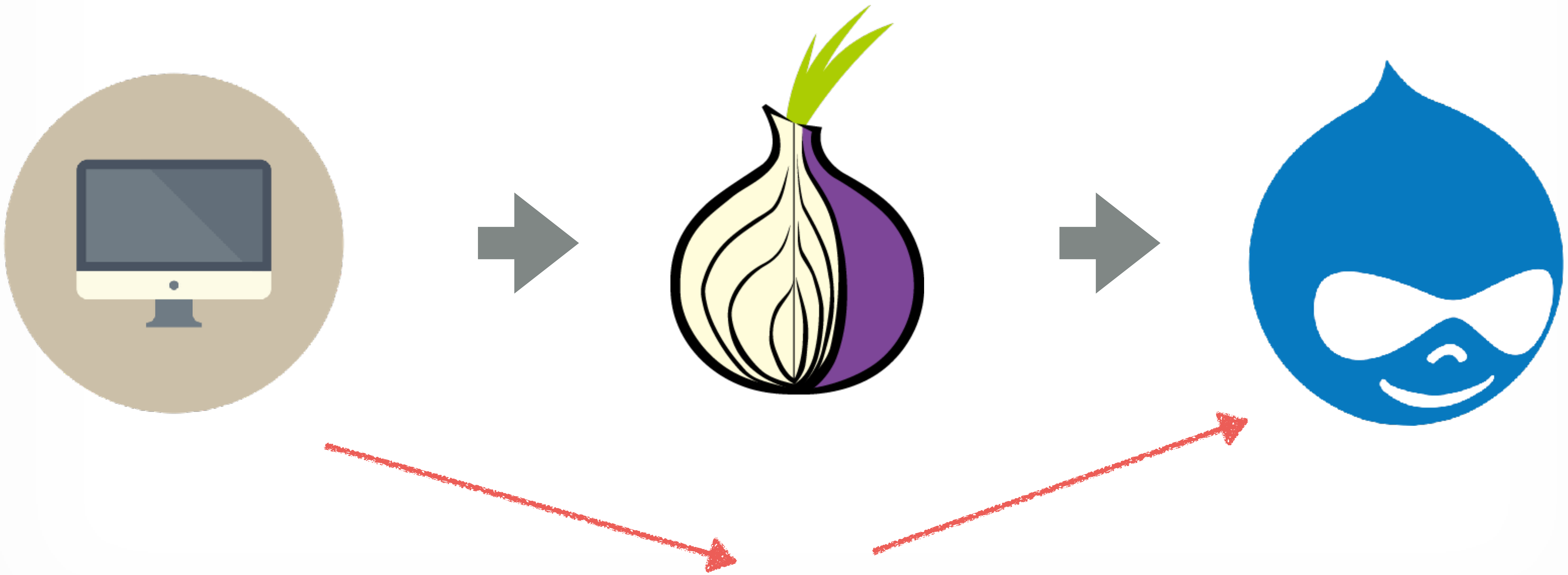
192.168.1.100

192.168.1.101

```
    location / {
        proxy_pass https://192.168.1.100;
        proxy_http_version 1.1;
        proxy_set_header Host "www.website.org";
        proxy_set_header  Connection      $connection_upgrade;
        proxy_set_header  Upgrade        $http_upgrade;
        #proxy_ssl_server_name on;
        proxy_read_timeout 30;
        proxy_connect_timeout 30;

        # Don't compress data, since the subs module can't replace
        proxy_set_header Accept-Encoding "";

        # TODO: denying non-GET requests due to some bot-related
        #       abuse on some endpoints that poorly handle that.
        limit_except GET {
            deny all;
        }
```

An Important Step

http://fkdheignoueupfmf.onion/

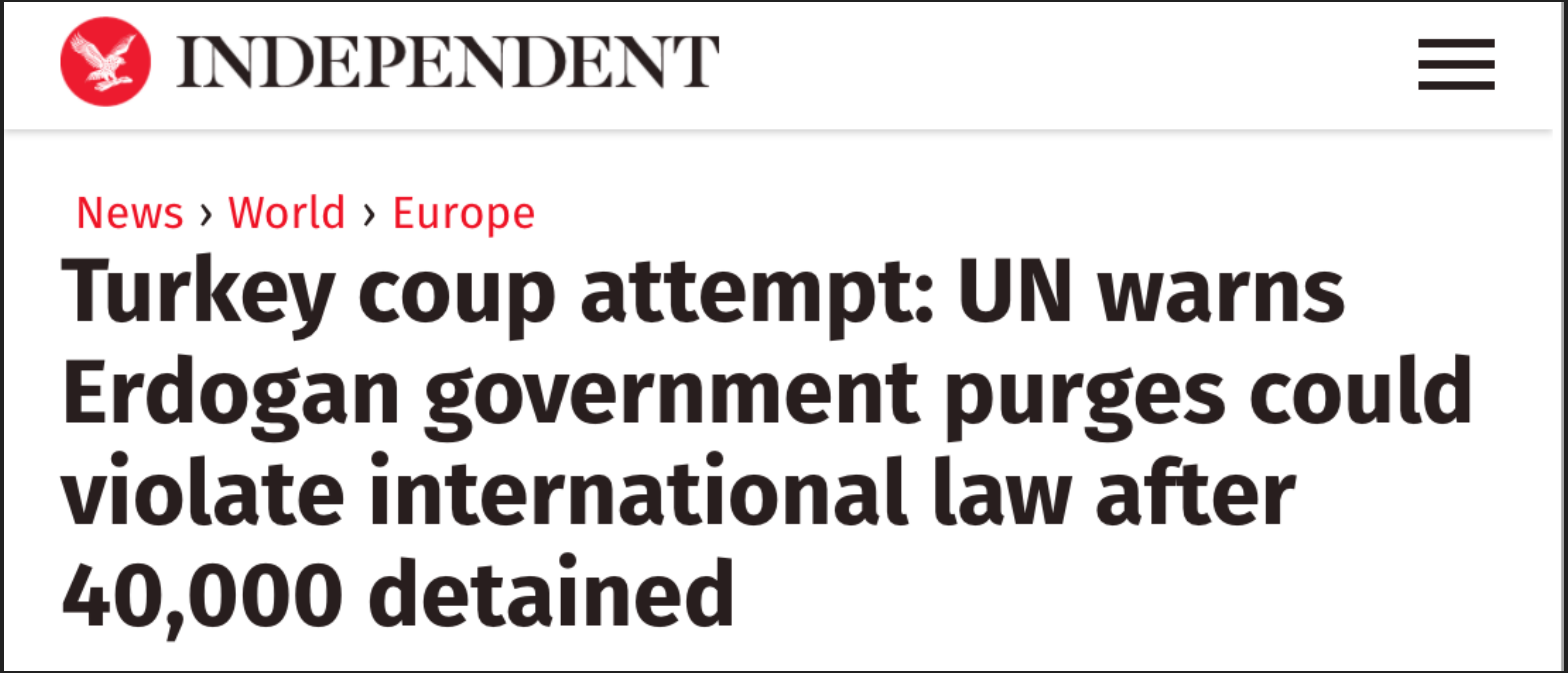


http://website.org/node/42

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

Press The Easy Button!

The Enterprise Onion Tool Kit

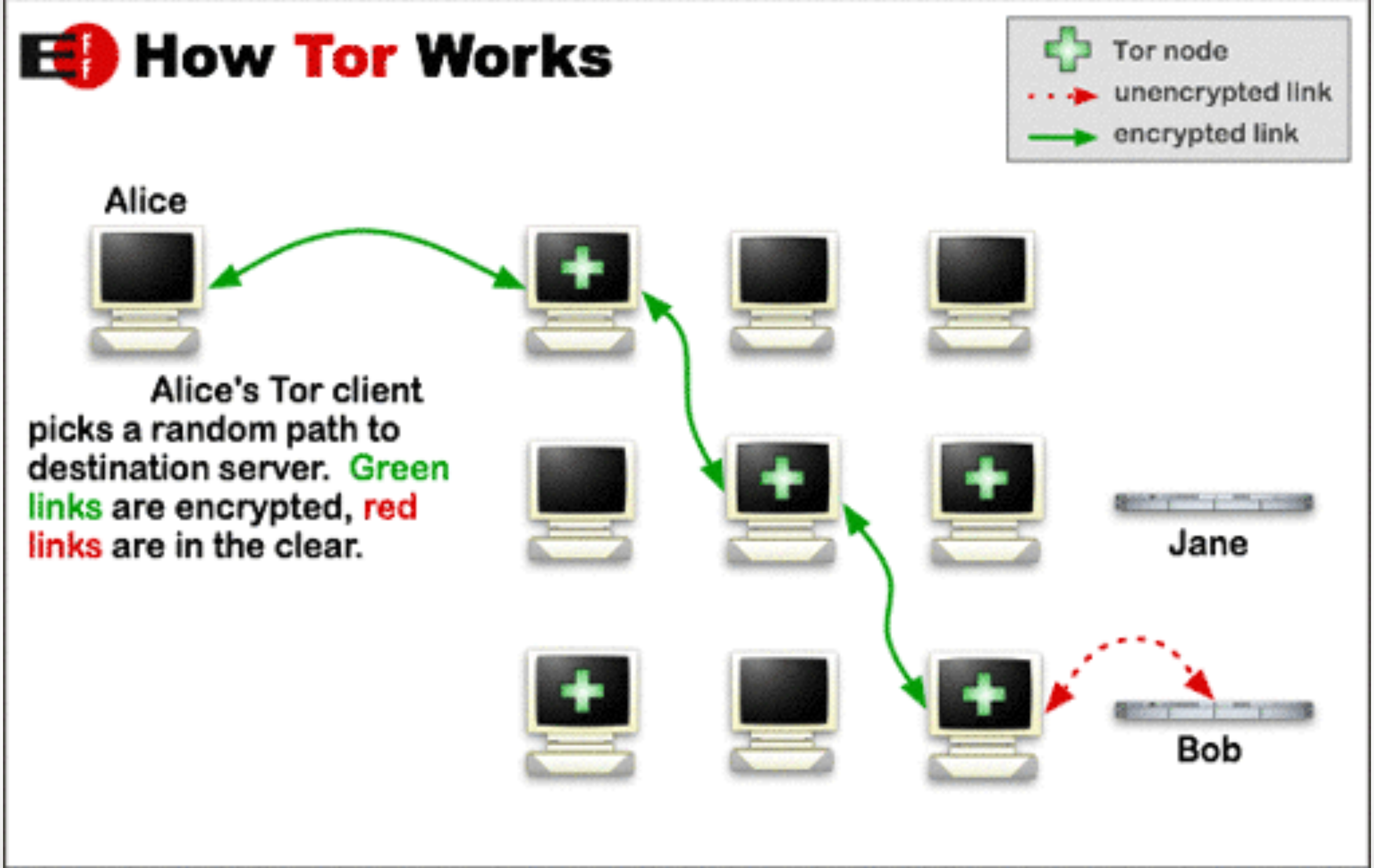
https://github.com/alecmuffett/eotk

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



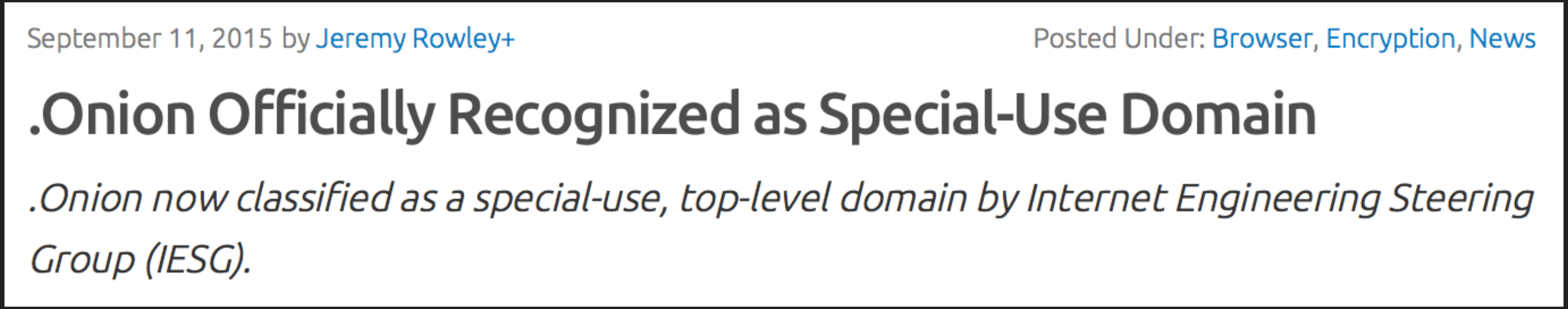
How Tor Works

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

Facebook - Log In or Sign Up
Facebook, Inc. (US)
https://www.facebookcorewwwi.onion/
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

- Put your site on the https://github.com/alecmuffett/onion-sites-that-dont-suck list
- Generally secure networking - email, calendar, etc
- OnionShare filesharing
- Hidden and 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

http://incoherency.co.uk/blog/stories/hidden-service-phishing.html

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:

https://github.com/alecmuffett/eotk

https://github.com/alecmuffett/onion-sites-that-dont-suck

https://onionshare.org

@milsyobtaf

Thanks!
Questions?

@milsyobtaf

https://github.com/milsyobtaf/prez