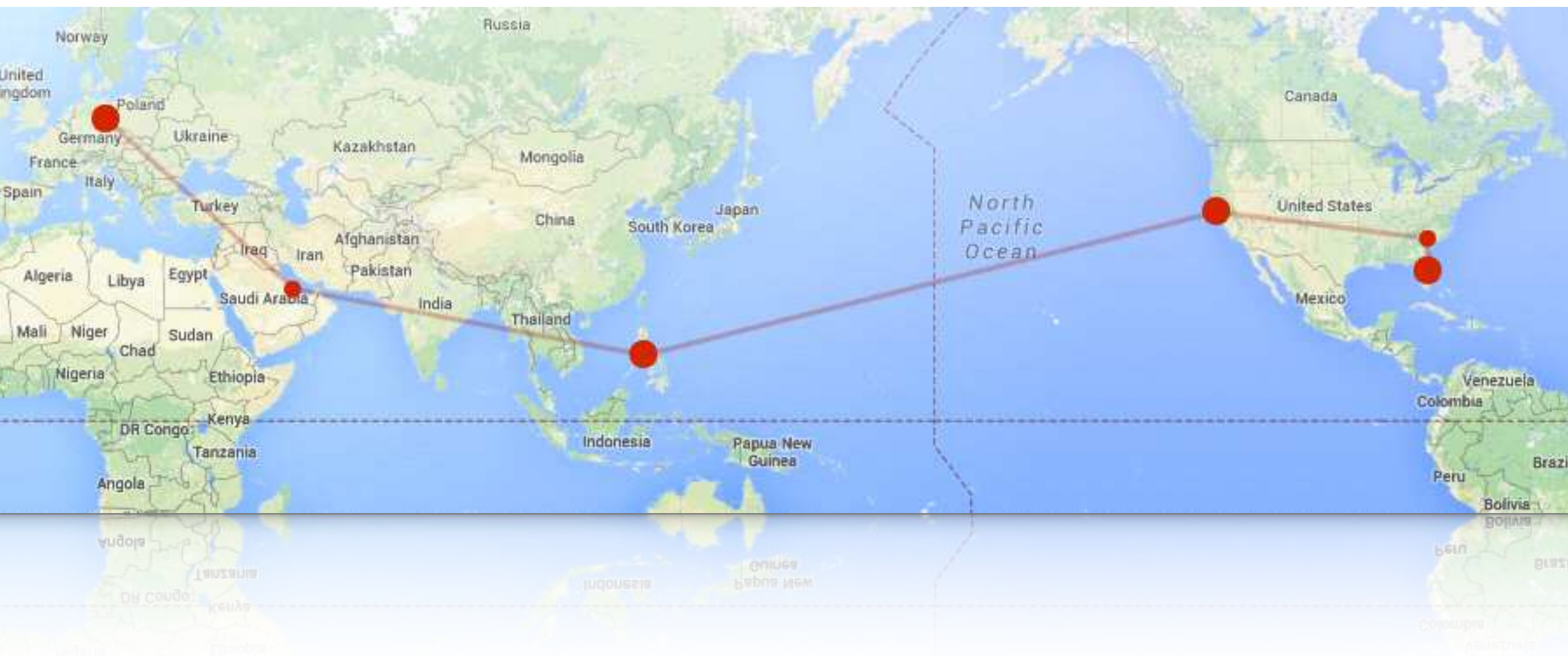


Hack Me, If You Can

Konstantin Haase
@konstantinhaase





rkh's lost bag

@rkh_bag

on my own adventures

location unknown

TWEETS

19

FOLLOWING

152

FOLLOWERS

151

 Follow

Tweets



rkh's lost bag @rkh_bag · Apr 1

Flight delayed. One more chance to get away!

Expand

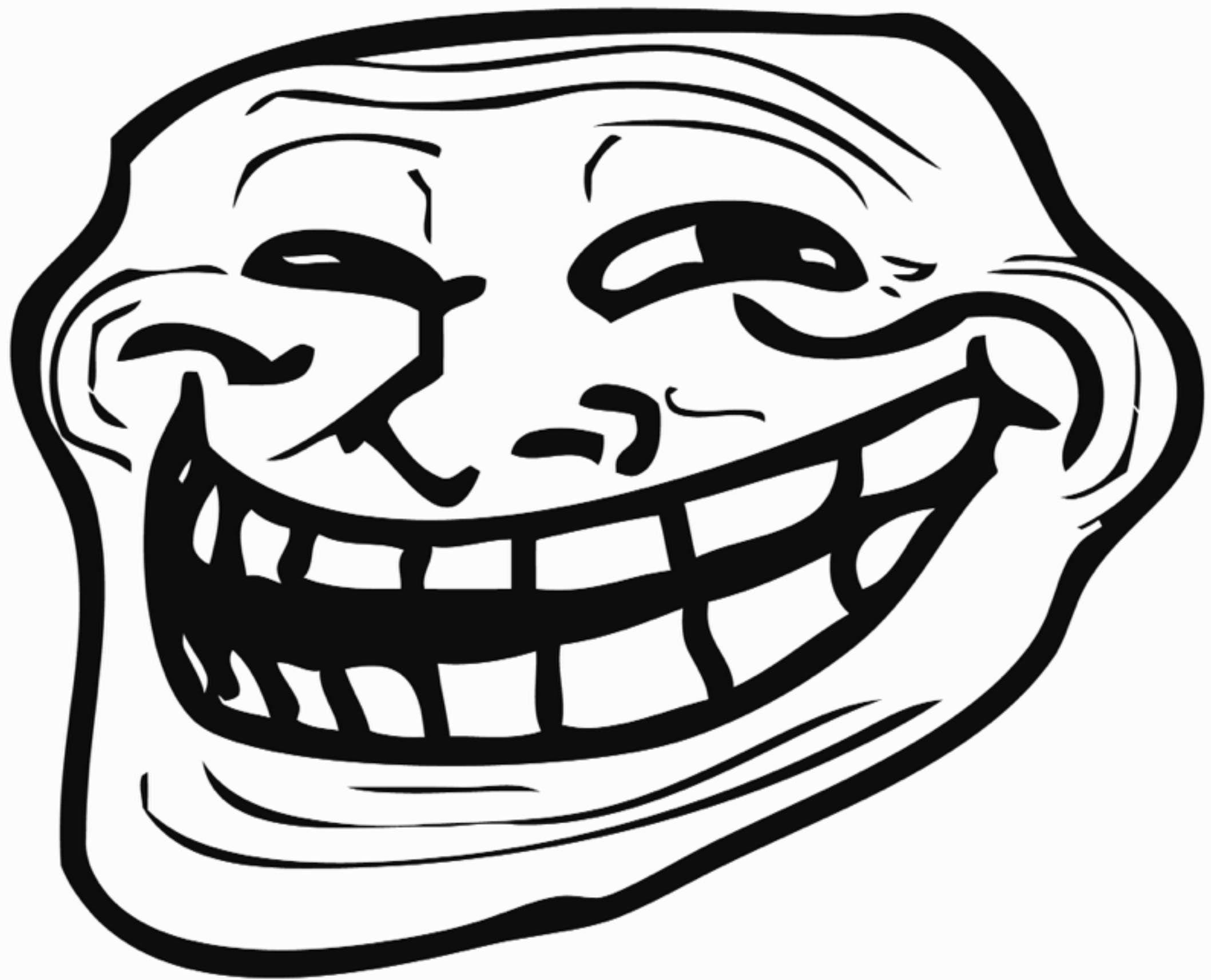
 Reply  Retweet  Favorite  Buffer ... More

Welcome to
St. Augustine,
the oldest city in
America

Three Things I'm good at

- History
- Geography
- Telling people they are wrong

	Settlement	City	Still Inhabited	European	European, Inhabited
America	Puerto Hormiga 4000 BC	Caral 2627 BC	Ticul 700 BC	Eystribyggð 985	Santo Domingo 1498
North America	Kaminaljuyu 1500 BC	Kaminaljuyu 1500 BC	Ticul 700 BC	Eystribyggð 985	Santo Domingo 1498
Mexico, US, Canada	Ticul 700 BC	Ticul 700 BC	Ticul 700 BC	L'Anse aux Meadows 1003	Veracruz 1519
US	Cahokia 650	Cahokia 650	Acoma Pueblo 1000	San Juan 1521	San Juan 1521
Continental US	Cahokia 650	Cahokia 650	Acoma Pueblo 1000	Pensacola 1559	Pensacola 1559





ALICE SENDS A MESSAGE TO BOB
SAYING TO MEET HER SOMEWHERE.

UH HUH.

BUT EVE SEES IT, TOO,
AND GOES TO THE PLACE.

WITH YOU SO FAR.

BOB IS DELAYED, AND
ALICE AND EVE MEET.

YEAH?



I'VE DISCOVERED A WAY TO GET COMPUTER
SCIENTISTS TO LISTEN TO ANY BORING STORY.

OH ALICE... YOU'RE
THE ONE FOR ME

BUT BOB... IN A
QUANTUM WORLD
HOW CAN WE BE SURE?

ψ^+ or ψ^- ?













POWERED BY



GLOBAL SHARK TRACKER

Sharks

x All Sharks

Tracking Activity

All Activity x

Gender

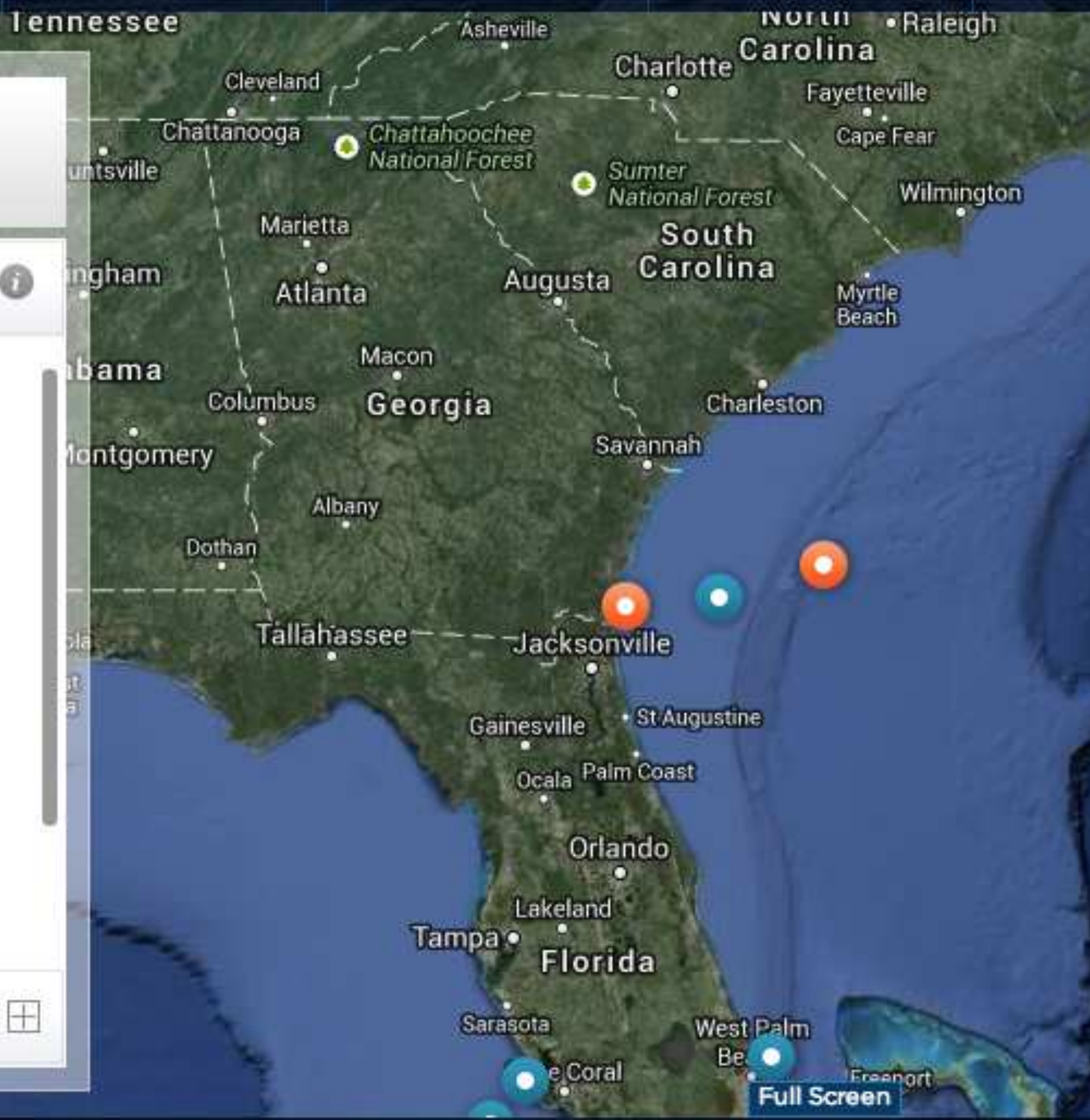
All Genders x

Stage of Life

All Stages of Life x

Tagged at

RECENT PINGS



XSS

Cross Site Scripting

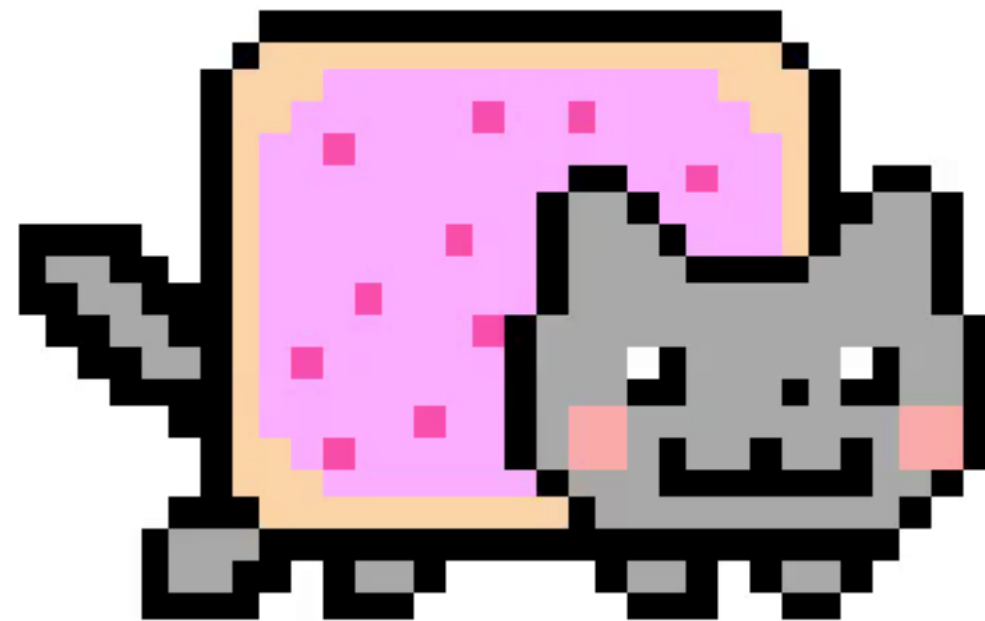
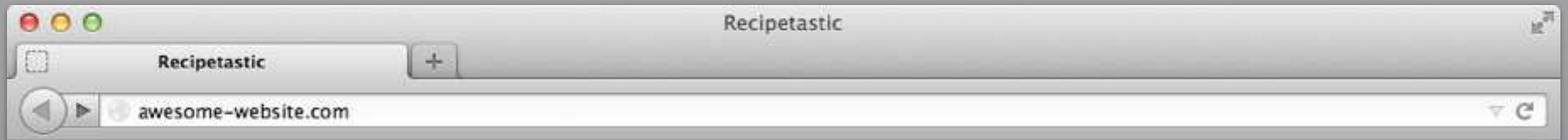
sanitize all user input

Content-Security-Policy

```
default-src 'self';  
script-src 'self' https://apis.google.com;  
report-uri https://example.com/csp
```


CSRF

Cross Site Request Forgery



Is this awesome, y/n?

64

128

2

4096

32

64

512

8

Game over!

16

32

16

4

Try again



Tweet

71.4K

2

8

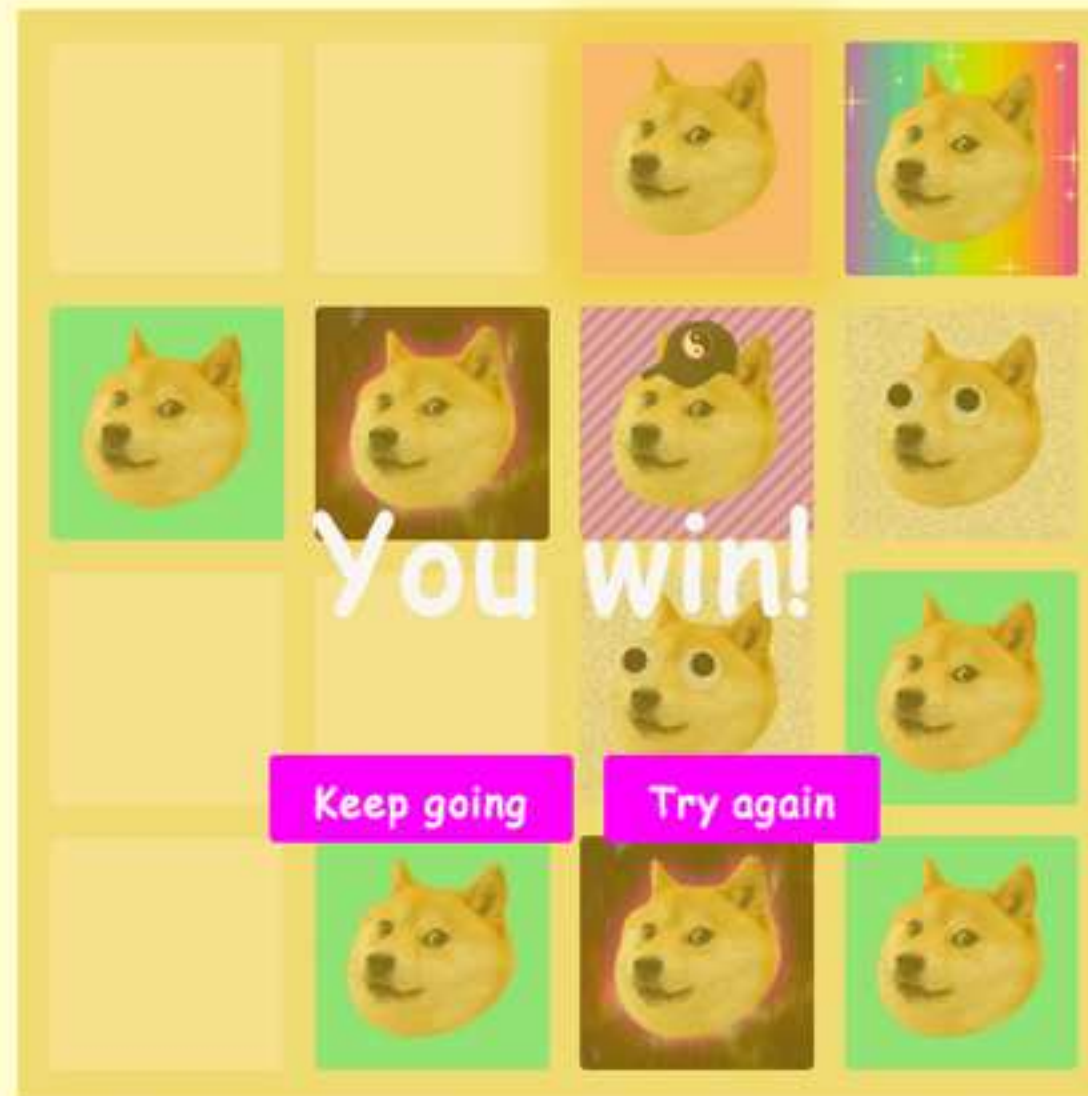
4

2

DOGE2048

SCORE
20596

BEST
20596



Keep going

Try again

Use your arrow keys or swipe to combine similar Doges and score points!

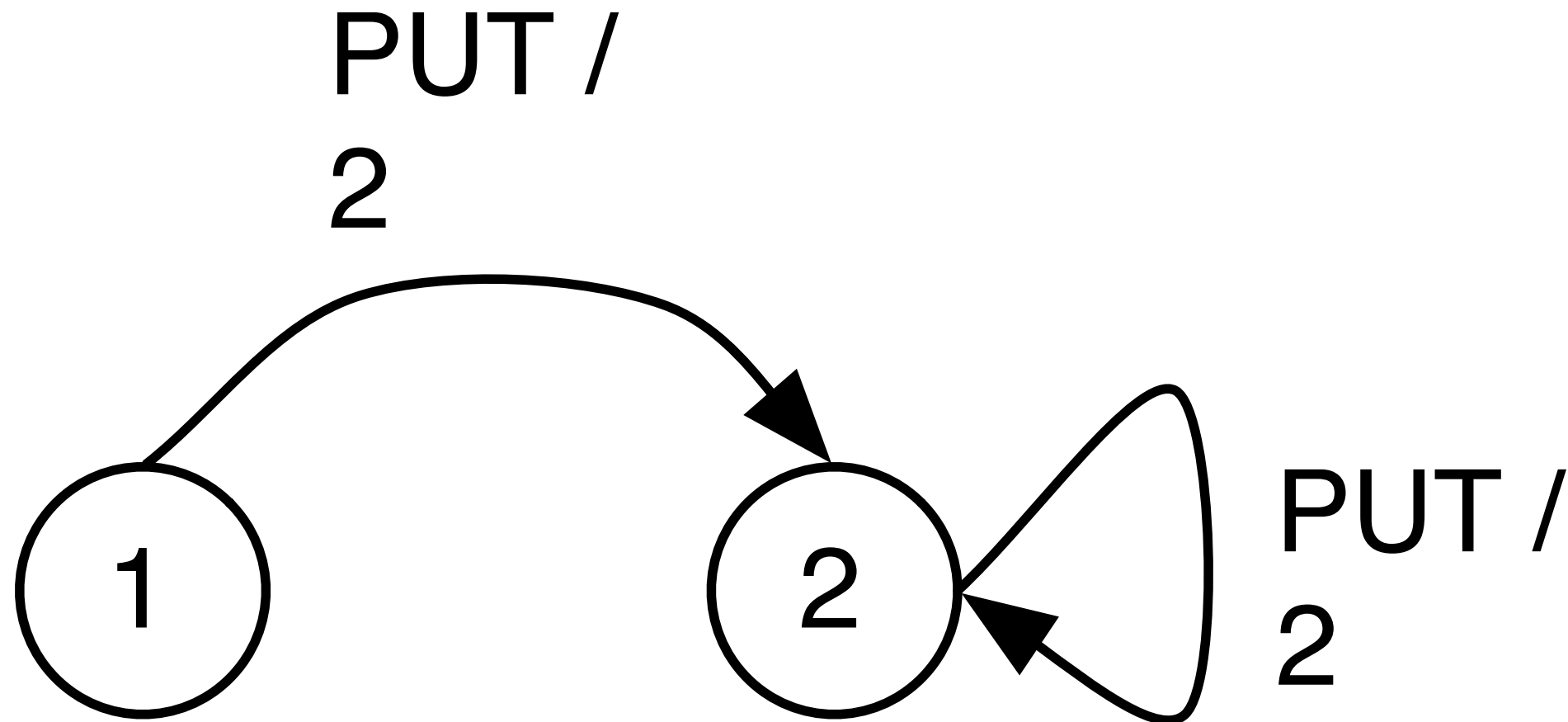
INFO

Like 25k Tweet 2,787

all requests include a
session cookie

embed URL as image

<https://speakerdeck.com/rkh/we-dont-know-http>



Repeatable! :)

State change! :(

Deterministic! :)

“safe” HTTP methods should
never change resource state

submit a hidden form


```
before do
  session[:csrf_token] ||= SecureRandom.hex(64)
  if session[:csrf_token] != params[:csrf_token]
    halt "access denied" unless request.safe?
  end
end
```

HTTP/1.1 200 OK

Content-Type: text/html

Set-Cookie: csrf_token=XXX

```
<form action="/create" method="post">  
  <input name="content">  
  <input type="hidden" name="csrf_token"  
    value="XXX">  
</form>
```

Path Traversal


```
get('/:name' do  
  path = "public/#{params[:name]}.md"  
  send_file path  
end
```

%2e%2e%2f

Clickjacking

X-Frame-Options

Same Origin Policy

VBScript
CSRF

JSON

CSRF

Session authenticated JSON
endpoint

```
<script type=text/javascript>
function Array() {
    var obj = this;
    var ind = 0;
    var getNext = function(x) {
        obj[ind++] setter = getNext;
        if(x) document.write(x.toString() + "<br>");
    };
    this[ind++] setter = getNext;
}
</script>
```

<https://github.com/rkh/json-csrf>

Referrer Leak

[click here] ([http://
evil.com](http://evil.com))

GET / HTTP/1.1

Host: evil.com

Referer: http://good.com/?secret=foo

GET /?redirect_to=http://evil.com
Host: good.com
Referer: http://good.com/?secret=foo

GET / HTTP/1.1

Host: evil.com

Referer: http://good.com/?redirect_...

HTTP/1.1 301 Moved Permanently
Location: <http://evil.com>

Header Injection

HTTP/1.1 200 OK\n

Header: Value\n

Header: Value\n

\n

Body

HTTP/1.1 200 OK\n

Header: Val\rue\n

Header: Value\n

\n

Body



HTTP/1.1 200 OK\n

Header: Val\r

Injected: Value\n

Header: Value\n

\n

Body

HTTP/1.1 200 OK\n

Header: Val\r\r

Injected Body, OMG

<!--\n

Header: Value\n

\n

Body

```
GET /?redirect_to=%0dSet-Cookie:x=1
```

HTTP/1.1 301 Moved\n

Location: \r

Set-Cookie: x=1\n

\n

Capturing the Cookie

Mozilla Firefox

(Untitled)

Google

Firesheep

Stop Capturing

eric+google@codebutler.com

Google

Ian Gallagher

Facebook

neg9

Twitter

cdine

Flickr

facebook

Search

Ian Gallagher

Edit My Profile

News Feed

Messages

Events

Friends

Create Group...

News Feed

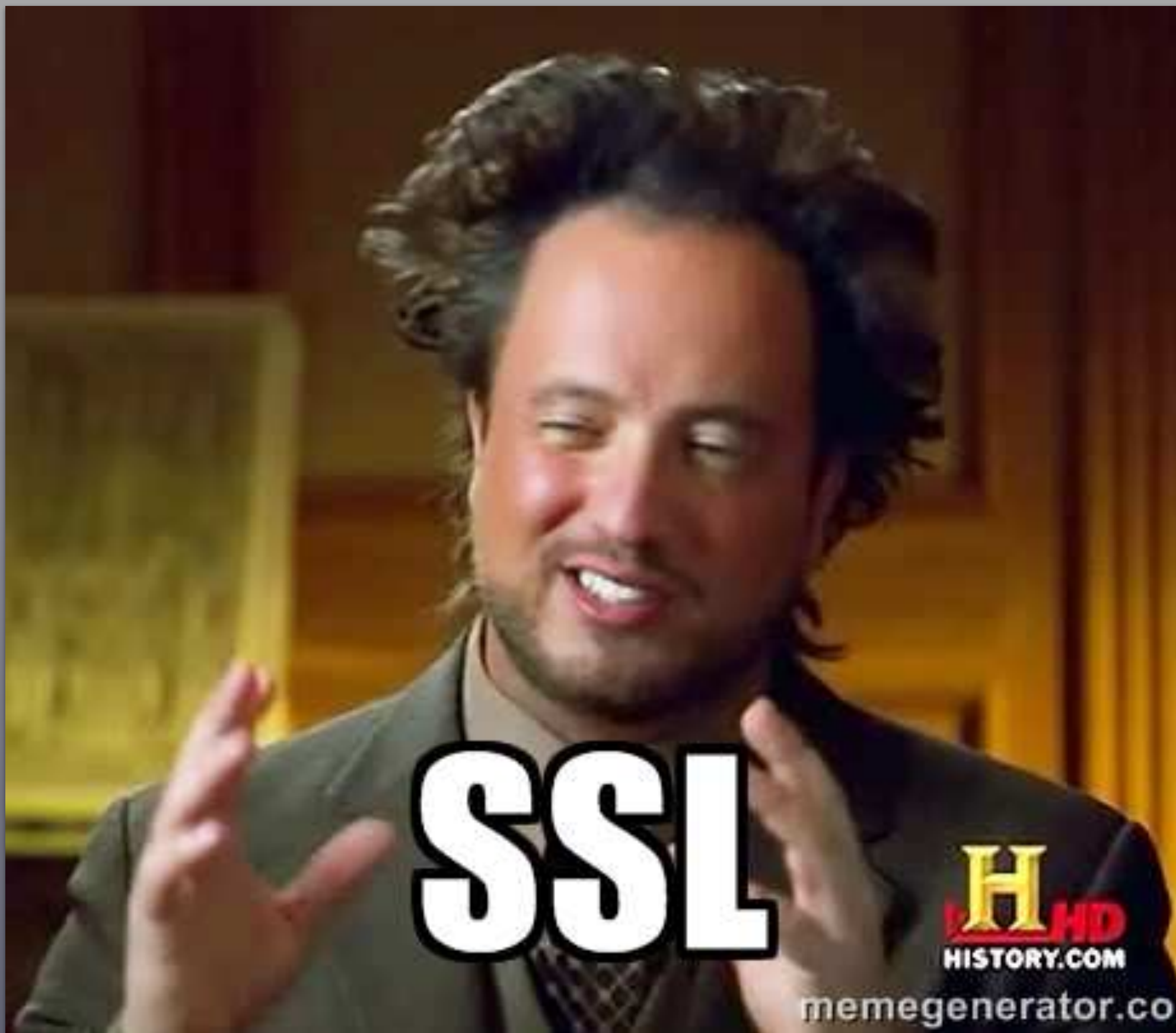
What's on your mind?

Ashley Winter
realized i really
for some fake r

indeed.

ABP

FoxyProxy: Disabled



SSL

H
HISTORY.COM

memegenerator.co

memegenerator.co

HISTORY.COM



BEAST

Browser Exploit Against
SSL/TLS

decrypt SSL via
injected plain text

fixed in TLS 1.1
(released in 2006)



NO
BALL
GAME

CRIME

Compression Ratio
Info-Leak Made Easy

GET /?user=**alice** HTTP/1.1

Cookie: user=**bob**

GET /?user=**bob** HTTP/1.1

Cookie: user=**bob**

*better
compression*



BREACH

Browser Reconnaissance
and Exfiltration via Adaptive
Compression of Hypertext

Browser

Reconnaissance

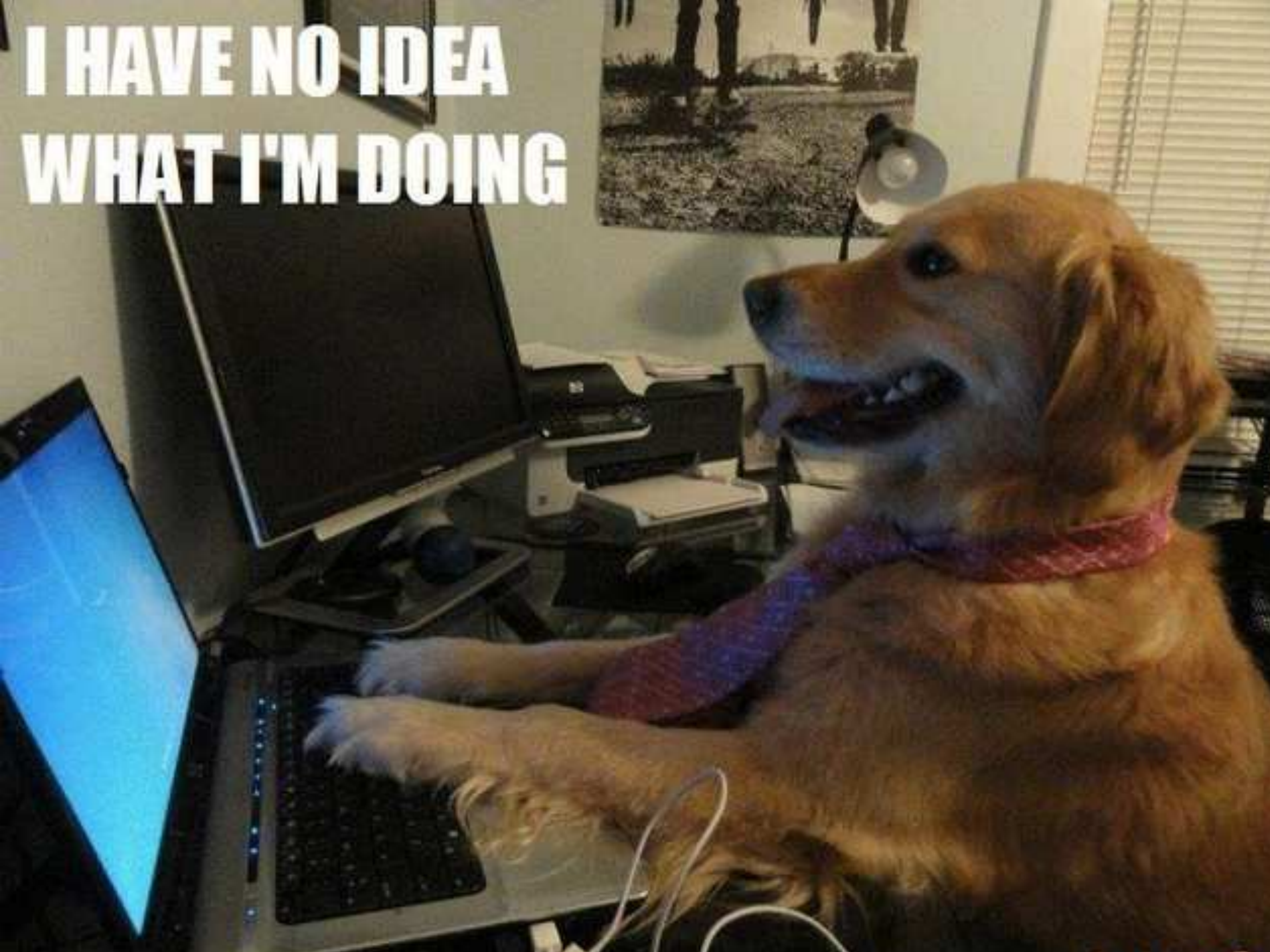
and
Exfiltration

via
Adaptive

Compression

of
Hypertext

**I HAVE NO IDEA
WHAT I'M DOING**





inject something in
the response

<http://www.recipetast.ic/search?q=XXX>

IF YOU THINK THIS HAS A HAPPY ENDING

**YOU HAVEN'T BEEN PAYING
ATTENTION**

Can we trust the
browser?

Can we trust the
browser plugins?



Cloud To Butt Plus

★★★★★ (45) | [Fun](#) | from Hank | 5,898 users

ADDED TO CHROME



OVERVIEW

DETAILS

REVIEWS

RELATED

+1

107

Read Blog Article

Tags: HP | to butt | People World Congress

Labels: HP | HP Butts | Mobile World Congress

Discover how HP Butt Maps can accelerate your ability to design and deploy butt services

Deepak Belani | March 6, 2013

[Post a Comment](#)

You have created your butt infrastructure, and now everything is in place—well almost. You have your service catalog online, but it is empty because you do not have any services to provision with. Traditionally you would have created these services yourself and they would have taken months of test to get them production ready. With HP Butt Maps now you can fast track building your application service catalogue in minutes!

Come discover how HP Butt Maps can accelerate your ability to design and deploy butt services. Come and see **Butt Maps Demo @ HP Booth: Industry Analyst Summit 2013** currently running in Boston, Westin Boston Waterfront Hotel.

Read Blog Article

Tags: application service catalog | Butt Service Automation | Service Providers

Labels: Butt Services | Butt Systems | Cloud Managed | HP Butt Maps

HP welcomes IBM's rhetoric around stronger OpenStack® support

Chris Percud | March 6, 2013

[Post a Comment](#)

Written by **Saar Gillai**, senior vice president and general manager of Converged Butts for Hewlett-Packard

The growth and market acceptance of OpenStack has been a journey. One that HP has been closely involved with for nearly two years. Our decision to leverage OpenStack for our butt platform was not made lightly, and was based on our experience of deploying butt solutions for several years prior to our OpenStack participation. In fact, we have thousands of customers using our butt solutions and services, and those numbers are growing quickly.

Read Blog Article

launch, branding, and product marketing



Ken Henault



KenATHP
Sr Product Marketing Manager - Butts and Automation

15 years in the IT industry holding titles such as System Administrator, Professional Services Consultant, Technical Instructor, Solution Architect and Technical Product Marketing.



Mackey
Laura Mackey is an editor, writer and social media expert.



mikeslaw747
Director, Solutions Marketing in HP Software

Mike has been with HP for 30 years. Half of that time was in R&D, mainly as an architect. The other 15 years has been spent in product management and product marketing.



Rbg42
Chief Technologist - Strategic Enterprise Services

Roger has been trying to get out of Information Technology since programming COBOL on mainframes in the late '80's. But no matter in which continent he awoke, or whom employed him, his passion to enable people with technology was constant. So now he enables businesses to

Replaces the text 'the cloud' with 'my butt', as well as 'cloud' with 'butt' in certain contexts.

Slight improvements to Cloud-to-butt, found here:

<https://github.com/panicsteve/cloud-to-butt>

My repo: <https://github.com/hank/cloud-to-butt>

Changes occurrences of "cloud" or "the cloud" to "butt" or "my butt" respectively and only in proper context (not weather sites, if possible).

Social Engineering

So I hear you parse
YAML?

- !ruby/class 'Rack::Session::Cookie'

- !ruby/object:Gem::Requirement

requirements:

- !ruby/object:Rack::Session::Abstract::SessionHash

env:

HTTP_COOKIE: "a=BAhvOkBBY3RpdmVTdXBwb3J0OjpEZXBvZW5hdGlvdj06RGVw"

by: !ruby/object:Rack::Session::Cookie

coder: !ruby/object:Rack::Session::Cookie::Base64::Marshal {}

key: a

secrets: []

exists: true

Do you keep all this in
mind?

Next attack around the
corner?

Thank you!

@konstantinhaase