The Bieber Project

Ad Tech and Fraud 101

Mark Ryan Talabis, zvelo

zvelo
We categorize the Web

Introduction

- Chief Security Scientist, zvelo
  - Ad Tech Fraud Research
- Formerly, Cloud Email Threat Protection, Fireeye
- Alumni Member, Honeynet Project
  - Honeypots/Honeynets
- Author, Elsevier-Syngress
  - Information Security Analytics/Risk Management

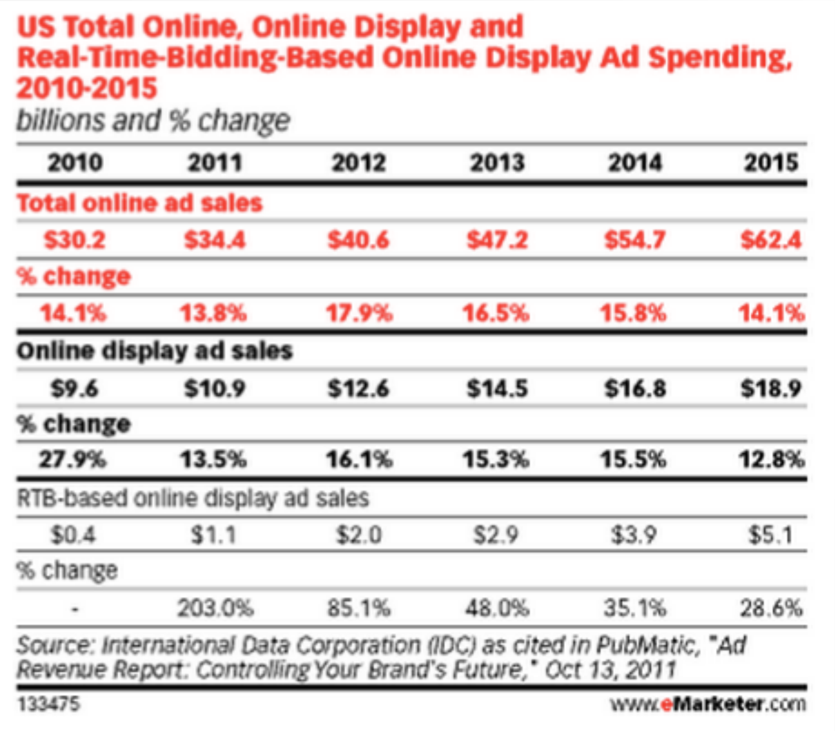
Main Topics

- The Business and Currency of Digital Advertising
- Ad Tech: The Ecosystem
- The Ad Fraud Problem
- Publisher-based Ad Fraud
- Non Human Traffic and the Bieber Project

The Business of Digital Advertising

Total digital ad spend is estimated to be

$60 billion in 2015



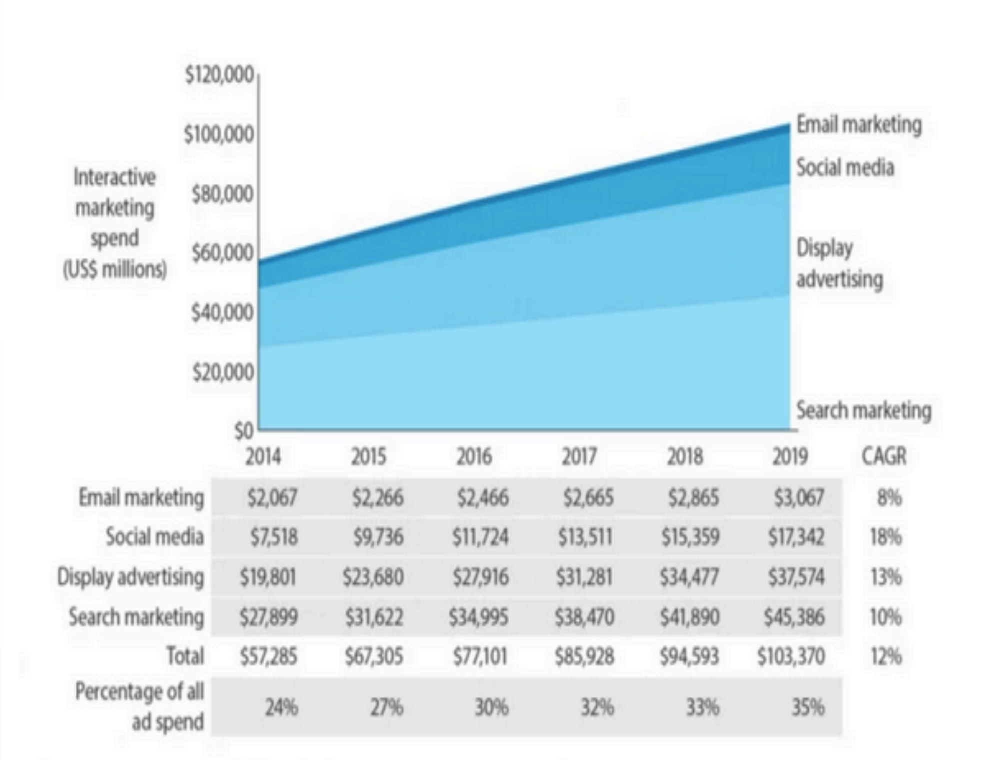
US Total Online, Online Display and Real-Time-Bidding-Based Online Display Ad Spending, 2010-2015

billions and % change

2010	2011	2012	2013	2014	2015
Total online ad sales					
$30.2	$34.4	$40.6	$47.2	$54.7	$62.4
% change					
14.1%	13.8%	17.9%	16.5%	15.8%	14.1%
Online display ad sales					
$9.6	$10.9	$12.6	$14.5	$16.8	$18.9
% change					
27.9%	13.5%	16.1%	15.3%	15.5%	12.8%
RTB-based online display ad sales					
$0.4	$1.1	$2.0	$2.9	$3.9	$5.1
% change					
-	203.0%	85.1%	48.0%	35.1%	28.6%

Source: International Data Corporation (IDC) as cited in PubMatic, "Ad Revenue Report: Controlling Your Brand's Future," Oct 13, 2011

133475 www.eMarketer.com



	2014	2015	2016	2017	2018	2019	CAGR
Email marketing	$2,067	$2,266	$2,466	$2,665	$2,865	$3,067	8%
Social media	$7,518	$9,736	$11,724	$13,511	$15,359	$17,342	18%
Display advertising	$19,801	$23,680	$27,916	$31,281	$34,477	$37,574	13%
Search marketing	$27,899	$31,622	$34,995	$38,470	$41,890	$45,386	10%
Total	$57,285	$67,305	$77,101	$85,928	$94,593	$103,370	12%
Percentage of all ad spend	24%	27%	30%	32%	33%	35%	

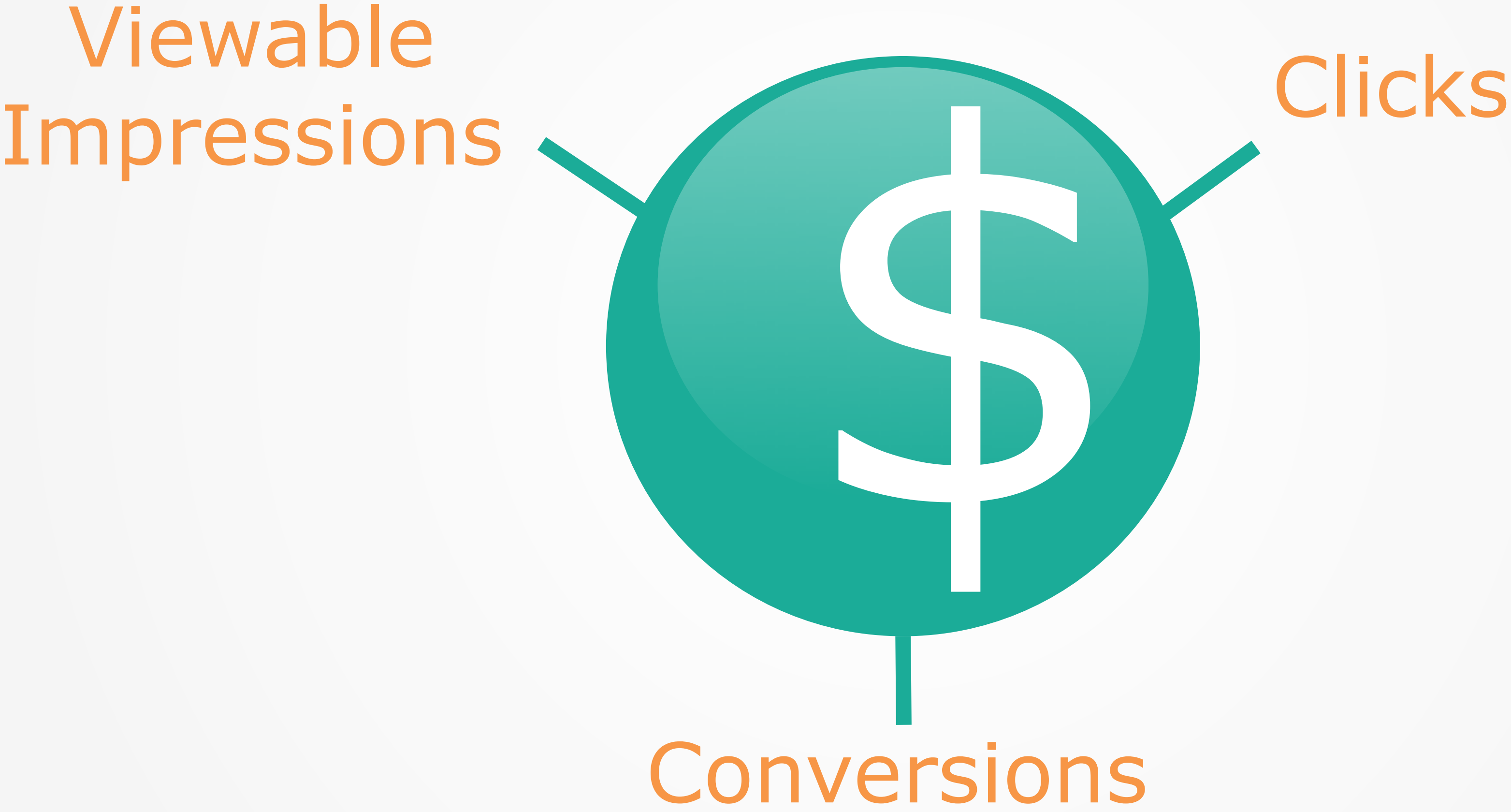
zvelo

We categorize the Web

The Currency of Digital Advertising

- Primary metric: the number of delivered, or served, impressions
- Primary problem: Not all online ads delivered actually have an opportunity to be seen
- Advertisers are obviously not interested in paying for ads that were never seen

The Currency of Digital Advertising

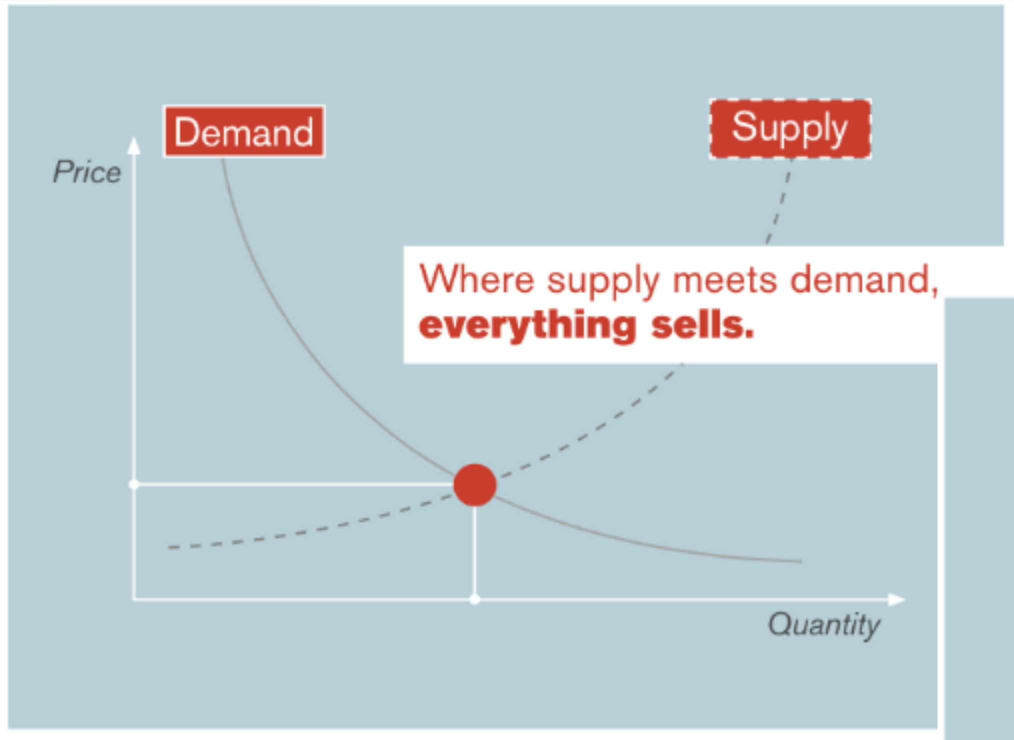


Viewable Impressions

Clicks

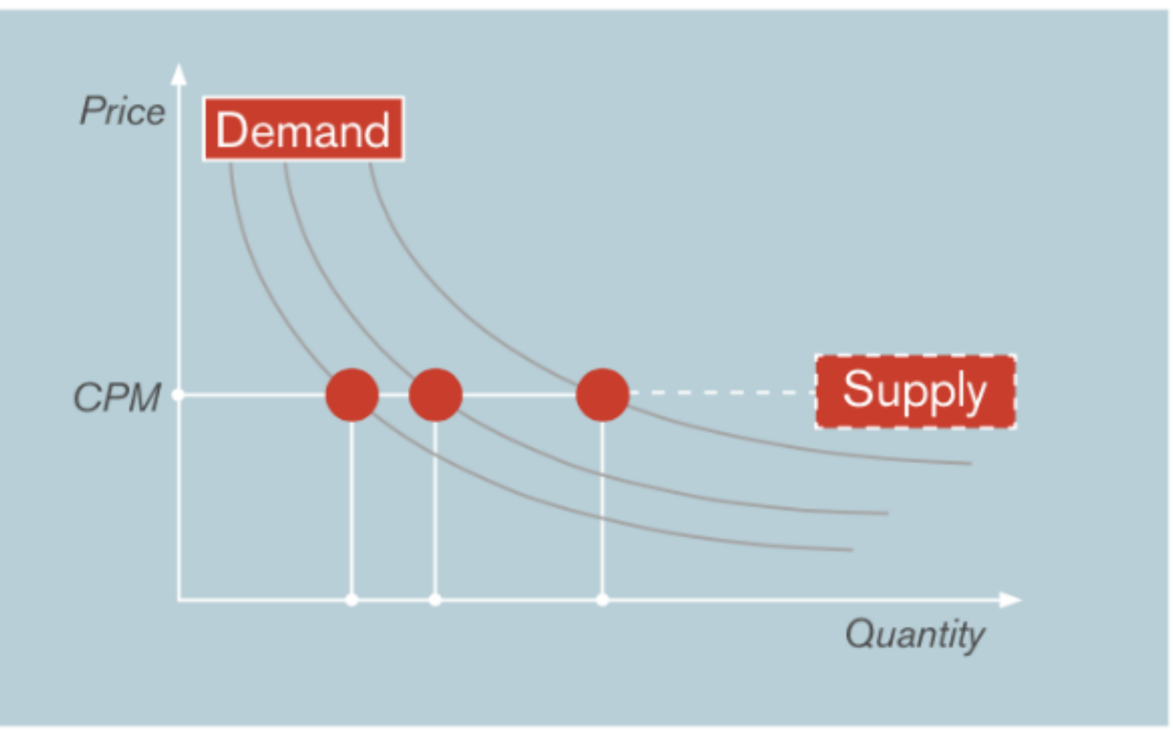
Conversions

The Business of Digital Advertising



Where supply meets demand, **everything sells.**

Supply and Demand



Reference: ComScore

The Business of Digital Advertising

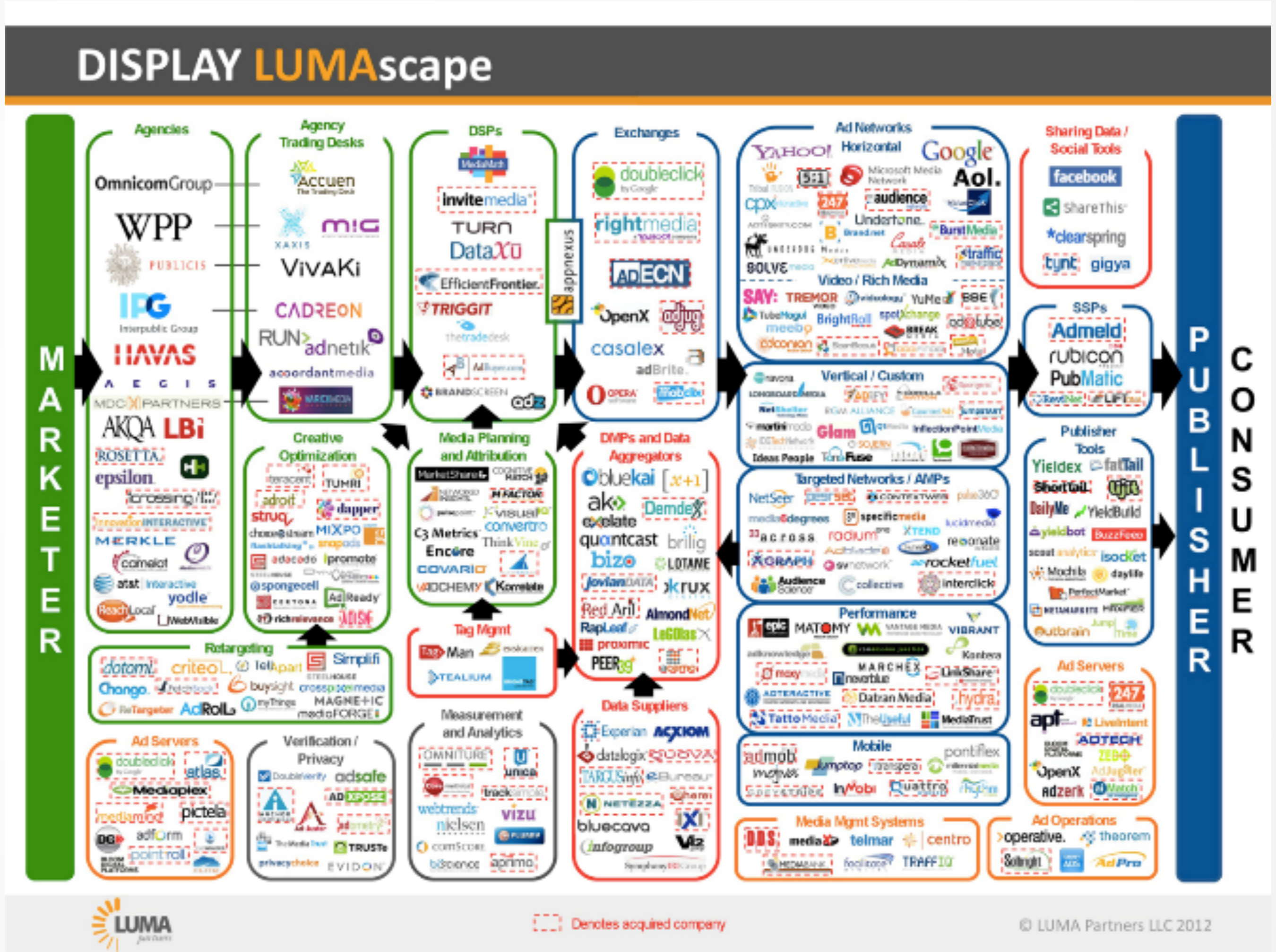
TV

VS

Online Advertising

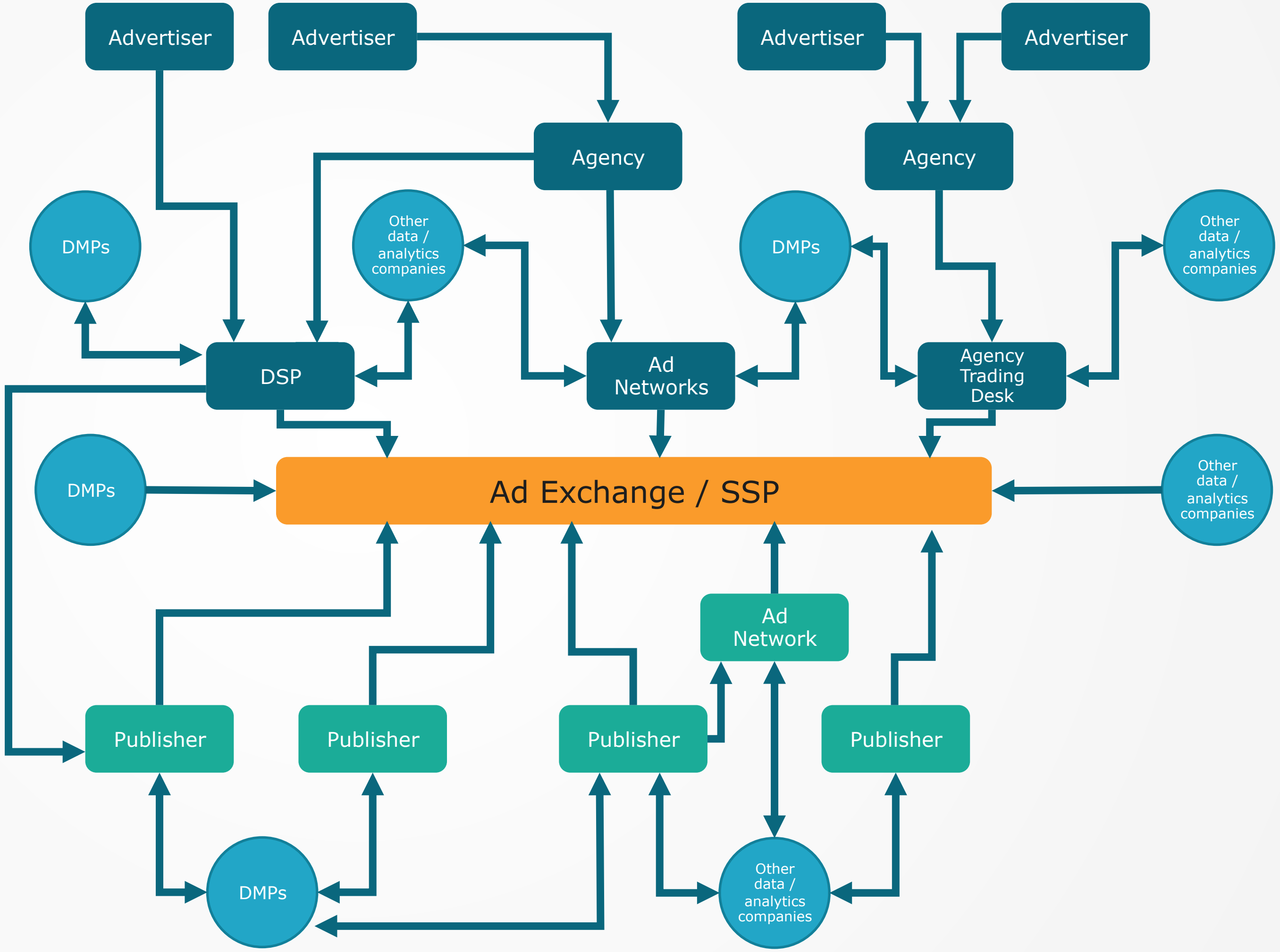
Ad Tech: The Ecosystem

Well, it’s a bit complicated…



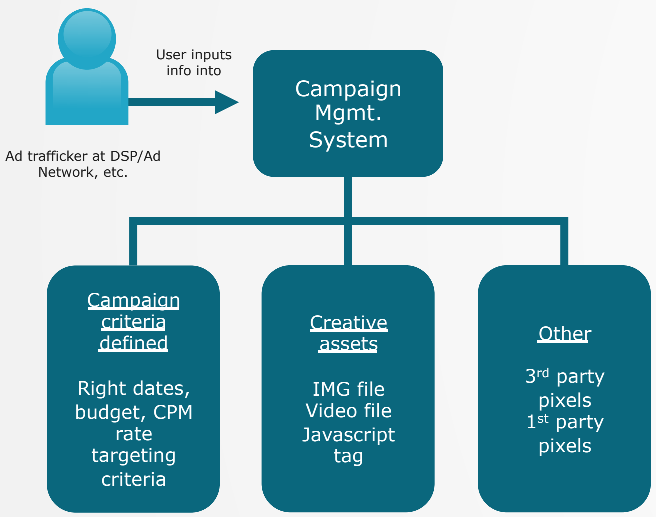
Ad Tech: The Ecosystem

Let's go through the 101 version…



Process of Serving an Ad

1. Campaign Setup



User inputs info into

Ad trafficker at DSP/Ad Network, etc.

Campaign Mgmt. System

Campaign criteria defined

Right dates, budget, CPM rate targeting criteria

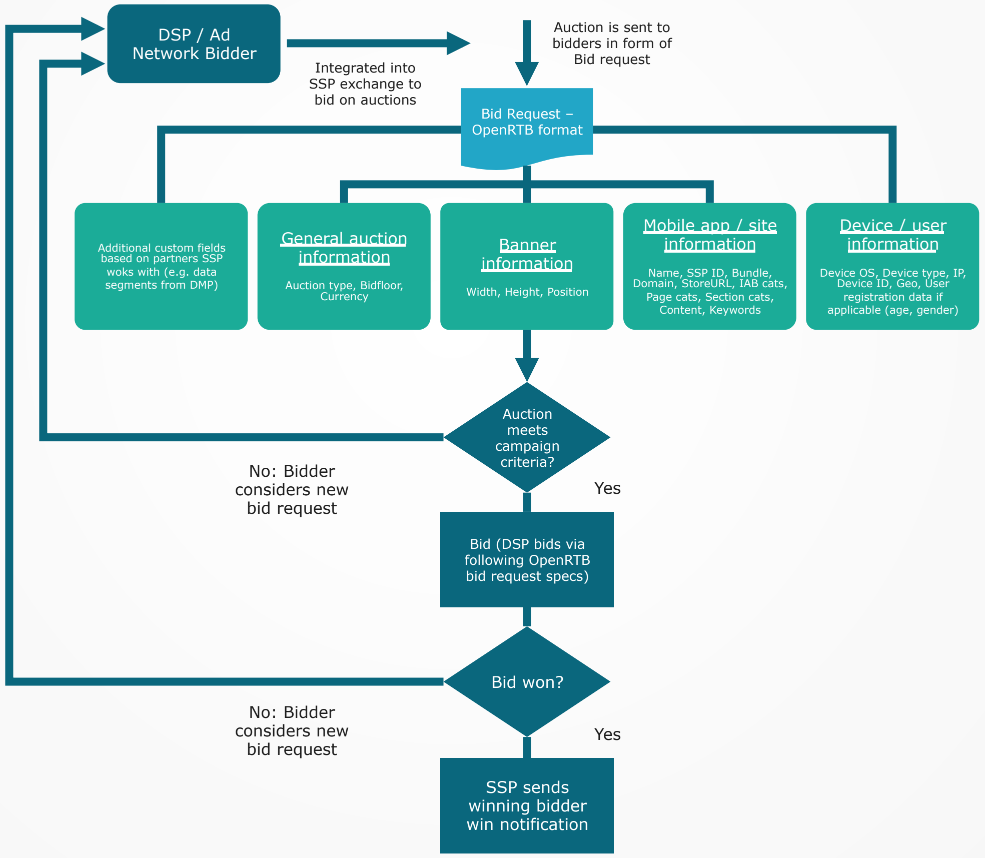
Creative assets

IMG file
Video file
Javascript tag

Other

3rd party pixels
1st party pixels

2. The Bidding Process



DSP / Ad Network Bidder

Integrated into SSP exchange to bid on auctions

Auction is sent to bidders in form of Bid request

Bid Request – OpenRTB format

Additional custom fields based on partners SSP woks with (e.g. data segments from DMP)

General auction information

Auction type, Bidfloor, Currency

Banner information

Width, Height, Position

Mobile app / site information

Name, SSP ID, Bundle, Domain, StoreURL, IAB cats, Page cats, Section cats, Content, Keywords

Device / user information

Device OS, Device type, IP, Device ID, Geo, User registration data if applicable (age, gender)

Auction meets campaign criteria?

No: Bidder considers new bid request

Yes

Bid (DSP bids via following OpenRTB bid request specs)

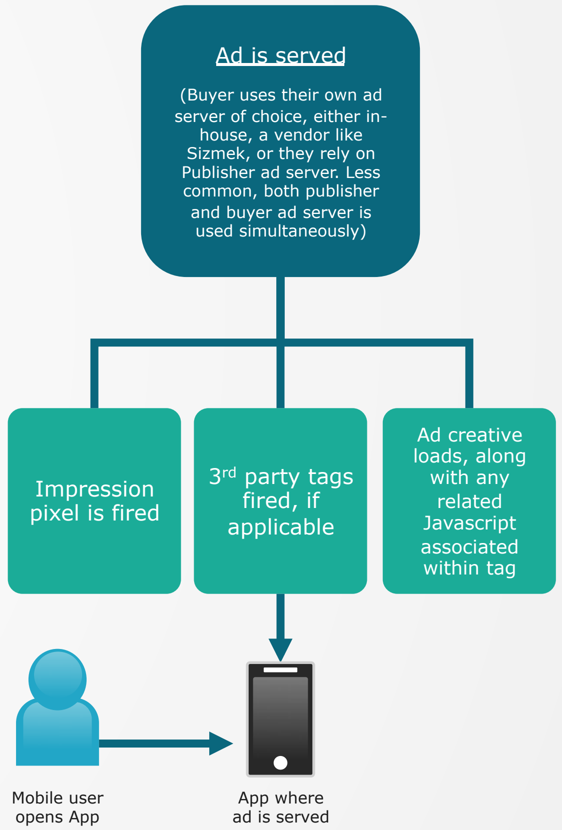
Bid won?

No: Bidder considers new bid request

Yes

SSP sends winning bidder win notification

3. Ad Serving



Ad is served

(Buyer uses their own ad server of choice, either in-house, a vendor like Sizmek, or they rely on Publisher ad server. Less common, both publisher and buyer ad server is used simultaneously)

Impression pixel is fired

3rd party tags fired, if applicable

Ad creative loads, along with any related Javascript associated within tag

Mobile user opens App

App where ad is served

zvelo
We categorize the Web

The Ad Fraud Problem

- Deliberate practice of attempting to serve ads that have no potential to be viewed by a human user
- Lots of varying statistics regarding the extent of the problem.
- Estimates range from 13% to as high as 60% of impressions served online were “suspicious”.
- What are we doing about it?

Interactive Advertising Bureau

- What is the IAB?
- Doing good things but sometimes a bit confusing to us people in security
- Released a Ad Fraud Taxonomy

IABs Ad Fraud Taxonomy

- Illegitimate and Non-Human Traffic Sources
  - Hijacked device
  - Crawler masquerading as a legitimate user
  - Data-center traffic
- Non-traditional / other traffic
  - Proxy traffic
  - Non-browser User-Agent header
  - Browser pre-rendering
- Hijacked Tags
  - Ad Tag Hijacking
  - Creative Hijacking
- Site Impression Attributes
  - Auto-Refresh
  - Ad Density
  - Hidden Ads
  - Viewability
  - Misappropriated Content
  - Falsely Represented
  - Non Brand Safe
  - Contains Malware
- Ad creative / other
  - Cookie Stuffing

101: What it Really Means

There are basically 3 main types of Ad Fraud:

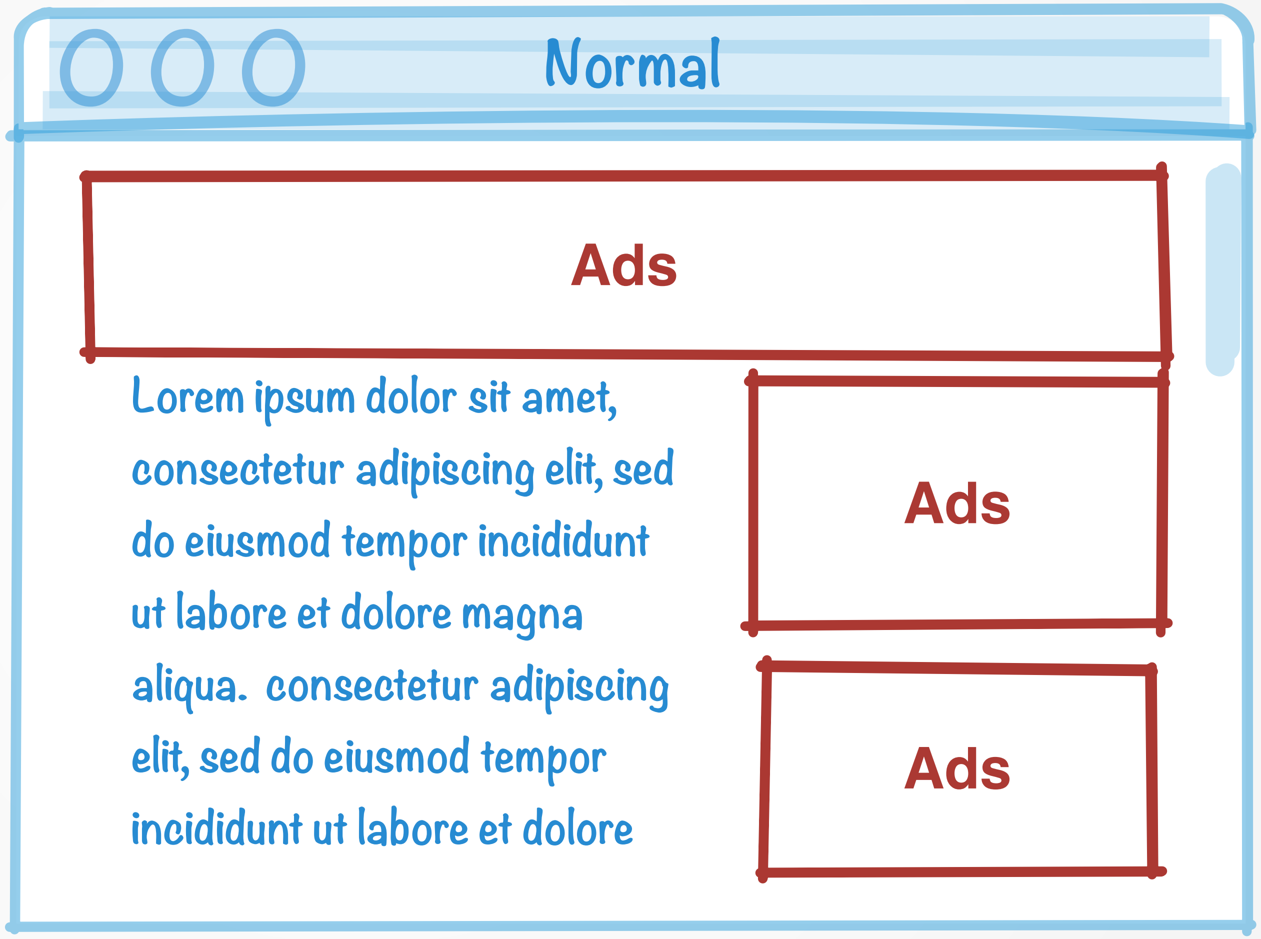
1. Publisher Tricks to Increase Impression Count
2. Illegal or Malicious Content
3. Use of Non Human Traffic to Increase Impressions

Publisher Tricks to Increase Impression Count

- Various techniques that publishers use to make 1 impression look like more!
- Some prominent examples are:
  - 1x1 Pixels
  - Ad Stacking
  - Gray Areas: Ad Clutter, Auto-play Videos

Publisher Tricks to Increase Impression Count

Typically advertisers will want to see this:



Normal

Ads

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore

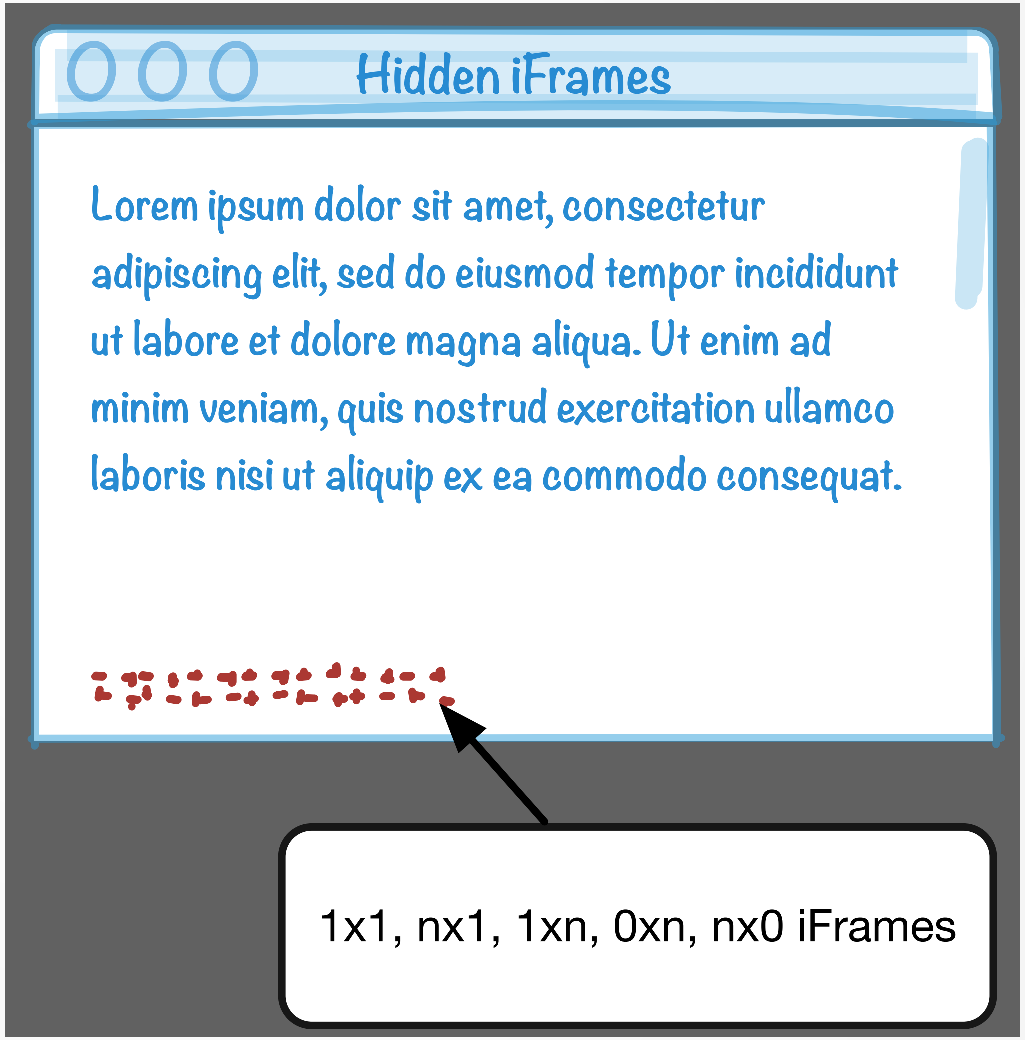
Ads

Ads

Publisher Tricks to Increase Impression Count

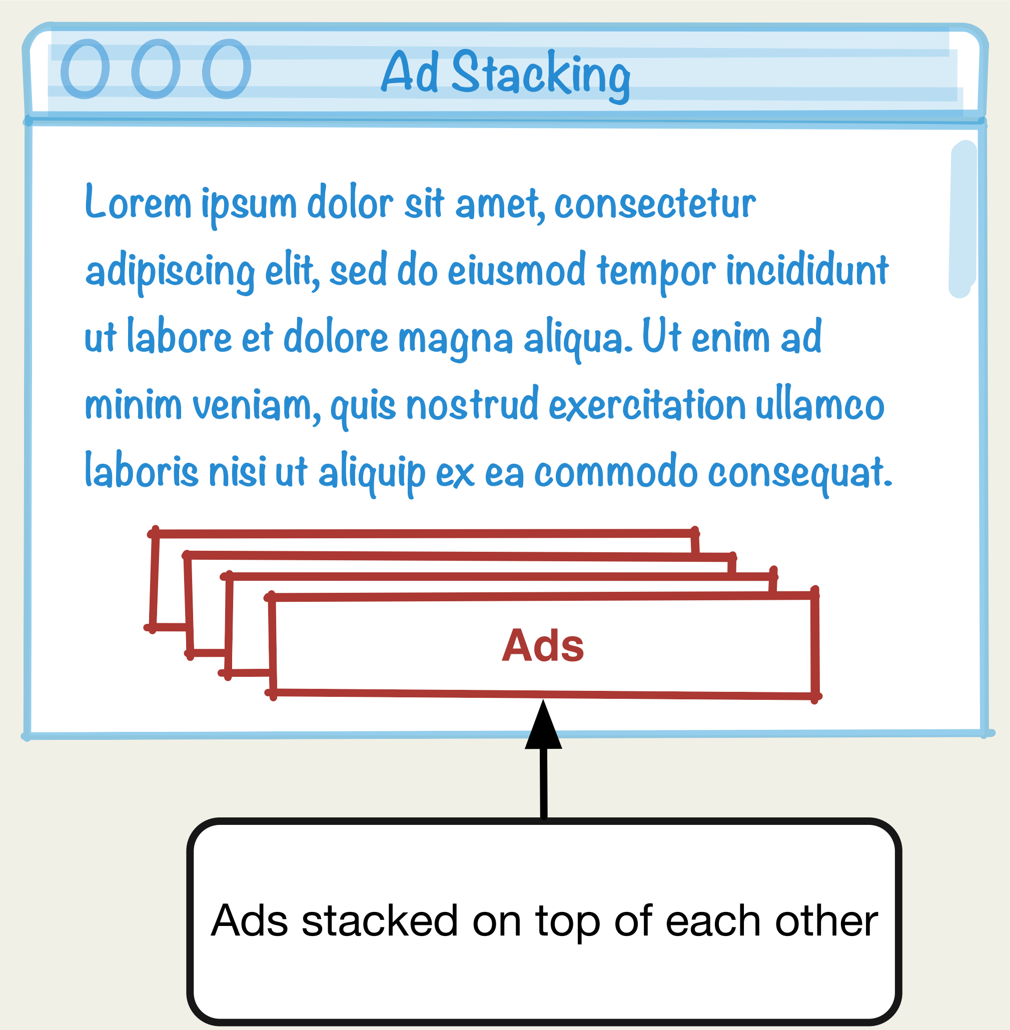
But some publishers will do this

(Hidden Ads):


Hidden iFrames
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
1x1, nx1, 1xn, 0xn, nx0 iFrames

Publisher Tricks to Increase Impression Count

Or this (Ad Stacking):


Ad Stacking
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
Ads

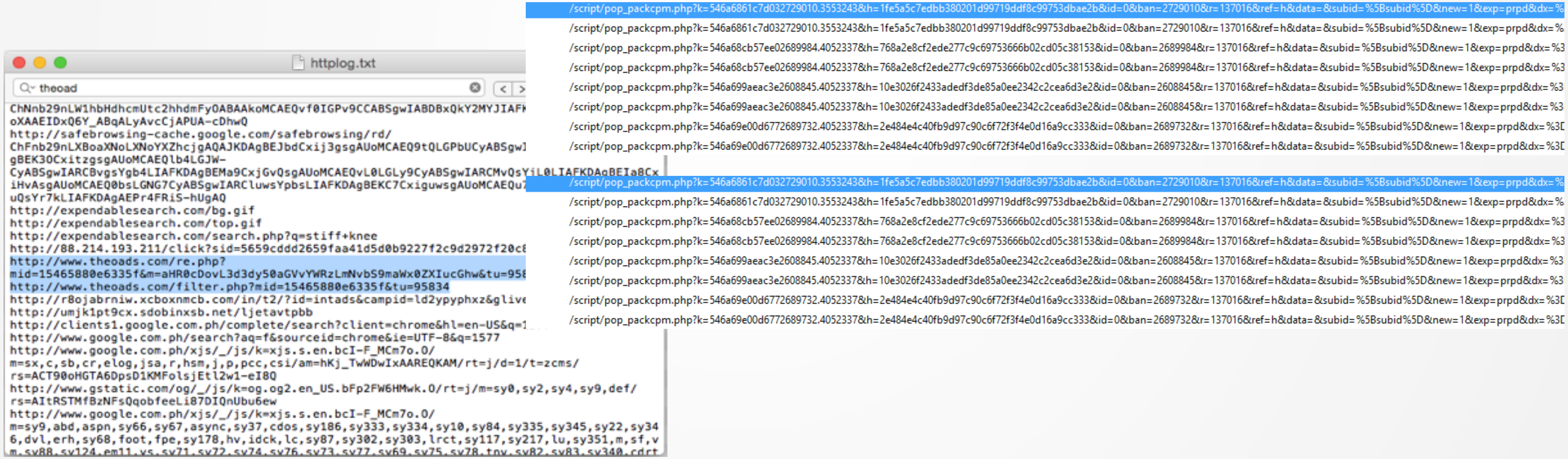
Ads stacked on top of each other

Illegal or Malicious Content

- There are times when fraud doesn’t directly mean increasing impressions (though it could end up that way)
- Some prominent examples are:
  - Serving malware or adware
  - Scams and Non Brand Safe

Illegal or Malicious Content

- Next few slides are from an investigation of malware-infected traffic exhibiting ad fraudish tendencies
- The Ad Network itself was serving "dirty" inventory or at the very least "low quality" content

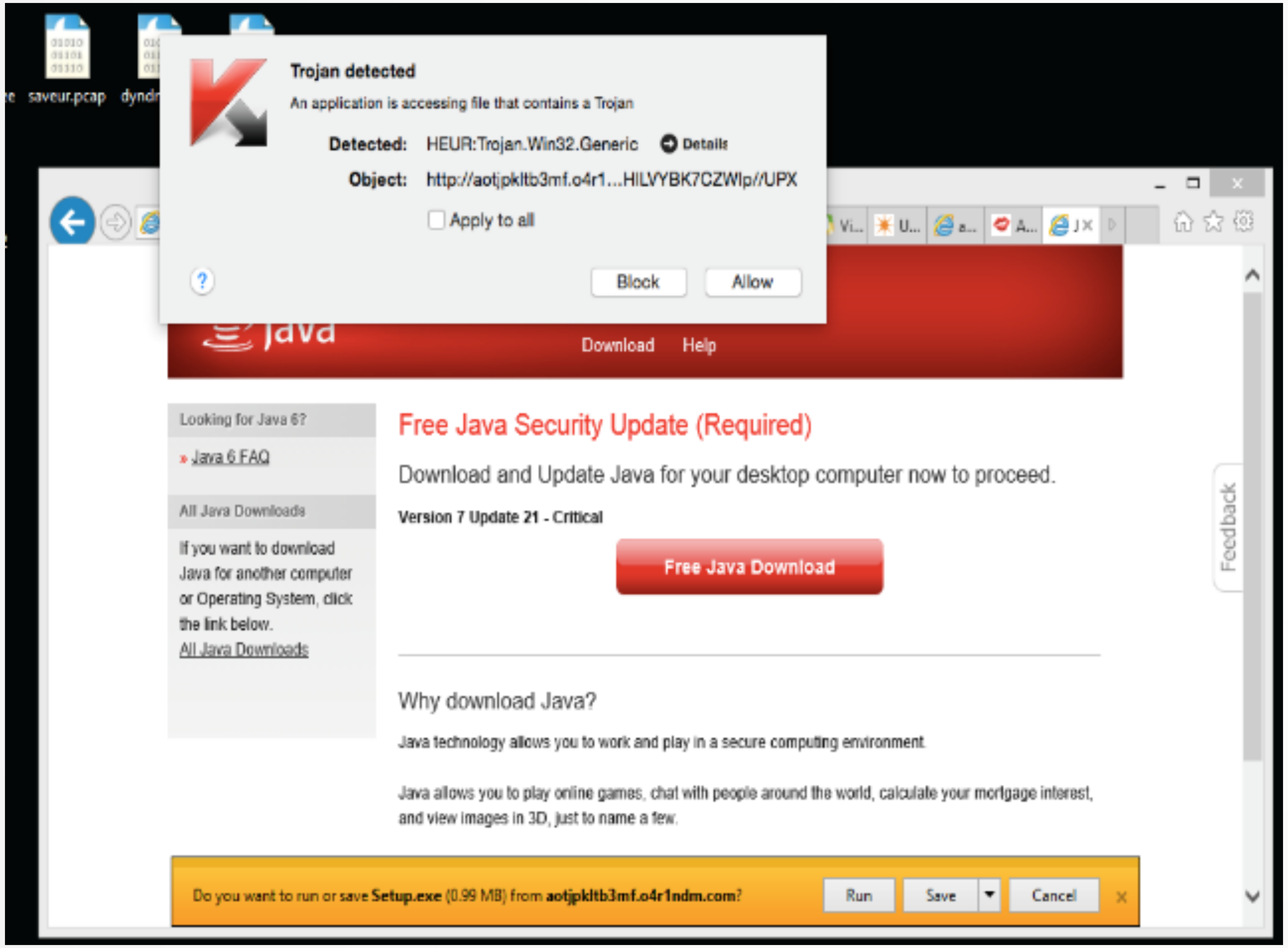


```
ChNnb29nLW1hbHdhcmUtc2hhdmFyOABAAkoMCAEQvf0IGPv9CCABSgwIABDBxQkY2MYJIAFK
oXAAEIDxQ6Y_ABqALyAvcCjAPUA-cDhwQ
http://safebrowsing-cache.google.com/safebrowsing/rd/
ChFnb29nLXBoaXNoLXNoYXZhcjgAQAJKDAgBEJbdCxij3gsgAUoMCAEQ9tQLGPbUCyABSgwI
gBEK3OCxitzgsgAUoMCAEQlb4LGJW-
CyABSgwIARCBvgsYgb4LIAFKDAgBEMa9CxjGvQsgAUoMCAEQvL0LGLy9CyABSgwIARCMvQsYiL0LIAFKDAgBEIa8Cx
iHvAsgAUoMCAEQ0bsLGNG7CyABSgwIARCluwsYpbsLIAFKDAgBEKC7CxiguwsgAUoMCAEQu7
uQsYr7kLIAFKDAgAEPr4FRiS-hUgAQ
http://expendablesearch.com/bg.gif
http://expendablesearch.com/top.gif
http://expendablesearch.com/search.php?q=stiff+knee
http://88.214.193.211/click?sid=5659cddd2659faa41d5d0b9227f2c9d2972f20c8
http://www.theoads.com/re.php?
mid=15465880e6335f&m=aHR0cDovL3d3dy50aGVvYWRzLmNvbS9maWx0ZXIucGhw&tu=958
http://www.theoads.com/filter.php?mid=15465880e6335f&tu=95834
http://r8ojabrniw.xcboxnmcb.com/in/t2/?id=intads&campid=ld2ypyphxz&glive
http://umjk1pt9cx.sdobinxsb.net/ljetavtpbb
http://clients1.google.com.ph/complete/search?client=chrome&hl=en-US&q=1
http://www.google.com.ph/search?aq=f&sourceid=chrome&ie=UTF-8&q=1577
http://www.google.com.ph/xjs/_/js/k=xjs.s.en.bcI-F_MCm7o.O/
m=sx,c,sb,cr,elog,jsa,r,hsm,j,p,pcc,csi/am=hKj_TwWDwIxAAREQKAM/rt=j/d=1/t=zcms/
rs=ACT90oHGTA6DpsD1KMFolsjEtl2w1-eI8Q
http://www.gstatic.com/og/_/js/k=og.og2.en_US.bFp2FW6HMwk.O/rt=j/m=sy0,sy2,sy4,sy9,def/
rs=AItRSTMfBzNFsQqobfeeLi87DIQnUbu6ew
http://www.google.com.ph/xjs/_/js/k=xjs.s.en.bcI-F_MCm7o.O/
m=sy9,abd,aspn,sy66,sy67,async,sy37,cdos,sy186,sy333,sy334,sy10,sy84,sy335,sy345,sy22,sy34
6,dvl,erh,sy68,foot,fpe,sy178,hv,idck,lc,sy87,sy302,sy303,lrct,sy117,sy217,lu,sy351,m,sf,v
m,sy88,sy124,em11,vs,sy71,sy72,sy74,sy76,sy73,sy77,sy69,sy75,sy78,tnv,sy82,sy83,sy340,cdrt
```

```
/script/pop_packcpm.php?k=546a6861c7d032729010.3553243&h=1fe5a5c7edbb380201d99719ddf8c99753dbae2b&id=0&ban=2729010&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%
/script/pop_packcpm.php?k=546a6861c7d032729010.3553243&h=1fe5a5c7edbb380201d99719ddf8c99753dbae2b&id=0&ban=2729010&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%
/script/pop_packcpm.php?k=546a68cb57ee02689984.4052337&h=768a2e8cf2ede277c9c69753666b02cd05c38153&id=0&ban=2689984&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a68cb57ee02689984.4052337&h=768a2e8cf2ede277c9c69753666b02cd05c38153&id=0&ban=2689984&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a699aeac3e2608845.4052337&h=10e3026f2433adedf3de85a0ee2342c2cea6d3e2&id=0&ban=2608845&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a699aeac3e2608845.4052337&h=10e3026f2433adedf3de85a0ee2342c2cea6d3e2&id=0&ban=2608845&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a69e00d6772689732.4052337&h=2e484e4c40fb9d97c90c6f72f3f4e0d16a9cc333&id=0&ban=2689732&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3D
/script/pop_packcpm.php?k=546a69e00d6772689732.4052337&h=2e484e4c40fb9d97c90c6f72f3f4e0d16a9cc333&id=0&ban=2689732&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3D
```

```
/script/pop_packcpm.php?k=546a6861c7d032729010.3553243&h=1fe5a5c7edbb380201d99719ddf8c99753dbae2b&id=0&ban=2729010&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%
/script/pop_packcpm.php?k=546a6861c7d032729010.3553243&h=1fe5a5c7edbb380201d99719ddf8c99753dbae2b&id=0&ban=2729010&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%
/script/pop_packcpm.php?k=546a68cb57ee02689984.4052337&h=768a2e8cf2ede277c9c69753666b02cd05c38153&id=0&ban=2689984&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a68cb57ee02689984.4052337&h=768a2e8cf2ede277c9c69753666b02cd05c38153&id=0&ban=2689984&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a699aeac3e2608845.4052337&h=10e3026f2433adedf3de85a0ee2342c2cea6d3e2&id=0&ban=2608845&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a699aeac3e2608845.4052337&h=10e3026f2433adedf3de85a0ee2342c2cea6d3e2&id=0&ban=2608845&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3
/script/pop_packcpm.php?k=546a69e00d6772689732.4052337&h=2e484e4c40fb9d97c90c6f72f3f4e0d16a9cc333&id=0&ban=2689732&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3D
/script/pop_packcpm.php?k=546a69e00d6772689732.4052337&h=2e484e4c40fb9d97c90c6f72f3f4e0d16a9cc333&id=0&ban=2689732&r=137016&ref=h&data=&subid=%5Bsubid%5D&new=1&exp=prpd&dx=%3D
```

Illegal or Malicious Content



Trojan detected

An application is accessing file that contains a Trojan

Detected: HEUR:Trojan.Win32.Generic

Object: http://aotjpkltb3mf.o4r1...HILVYBK7CZWlp//UPX

□ Apply to all

Free Java Security Update (Required)

Download and Update Java for your desktop computer now to proceed.

Version 7 Update 21 - Critical

Looking for Java 6?

» Java 6 FAQ

All Java Downloads

If you want to download Java for another computer or Operating System, click the link below.

All Java Downloads

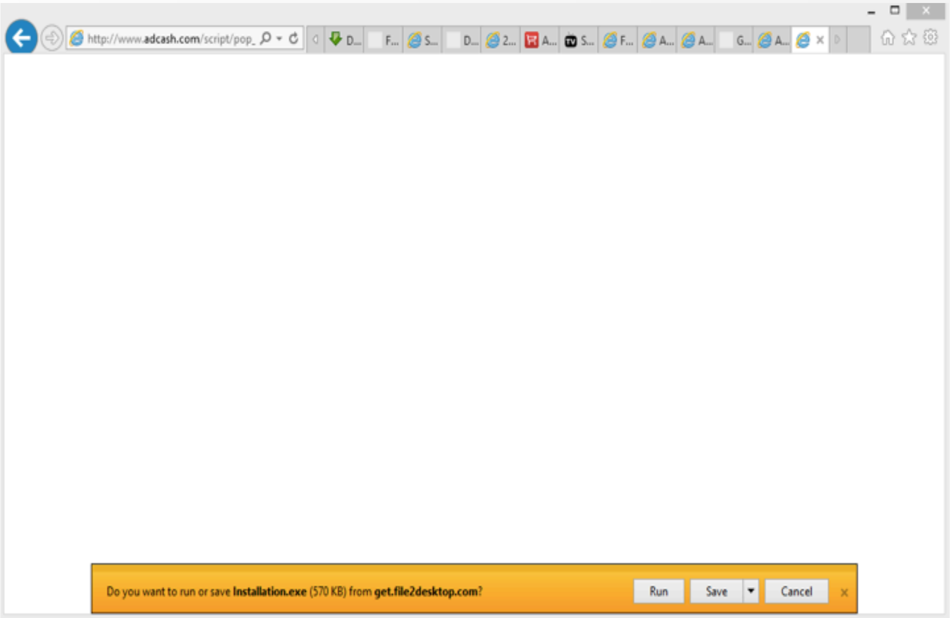
Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage interest, and view images in 3D, just to name a few.

Do you want to run or save **Setup.exe** (0.99 MB) from **aotjpkltb3mf.o4r1ndm.com**?

Ad network was serving malware!

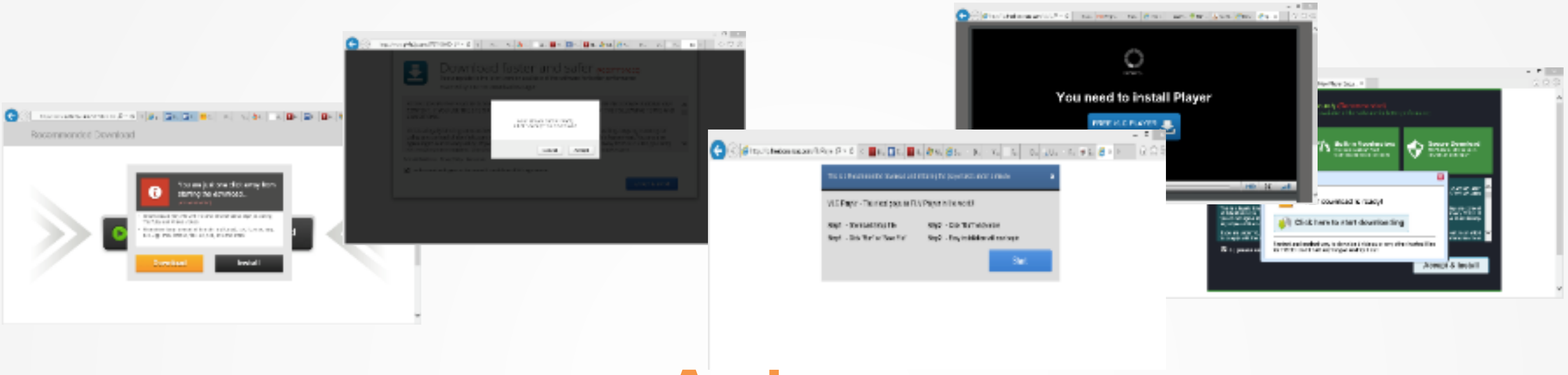


http://www.adcash.com/script/pop_

Do you want to run or save **Installation.exe** (570 KB) from **get.file2desktop.com**?

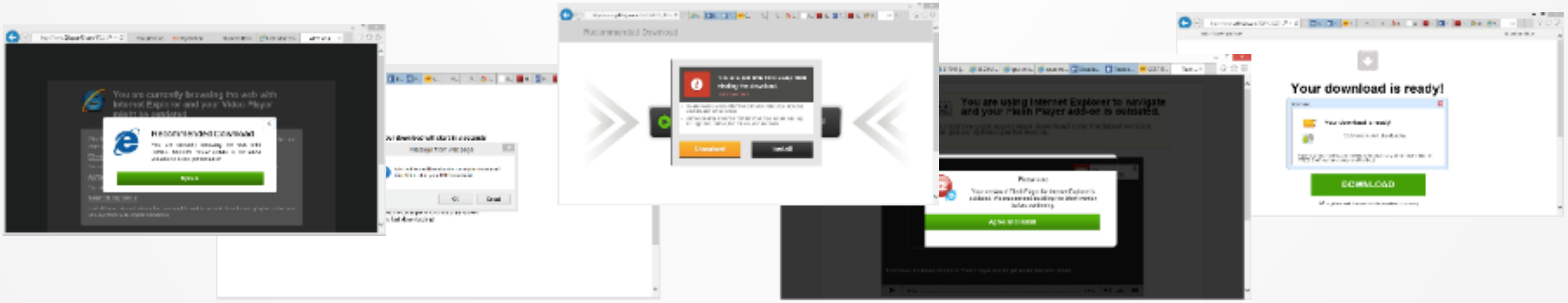
zvelo
We categorize the Web

Illegal or Malicious Content

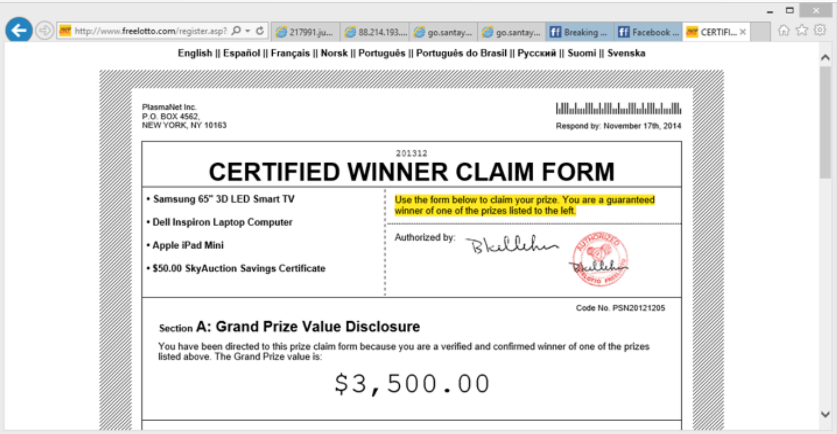

Recommended Download
Download faster and safer
Download
Install
You need to install Player
Click here to start downloading
Accept & Install

Adware

Ads that will serve you more Ads



Illegal or Malicious Content



English || Español || Français || Norsk || Português || Português do Brasil || Русский || Suomi || Svenska

PlasmaNet Inc.
P.O. BOX 4562,
NEW YORK, NY 10163

Respond by: November 17th, 2014

201312

CERTIFIED WINNER CLAIM FORM

- Samsung 65" 3D LED Smart TV
- Dell Inspiron Laptop Computer
- Apple iPad Mini
- $50.00 SkyAuction Savings Certificate

Use the form below to claim your prize. You are a guaranteed winner of one of the prizes listed to the left.

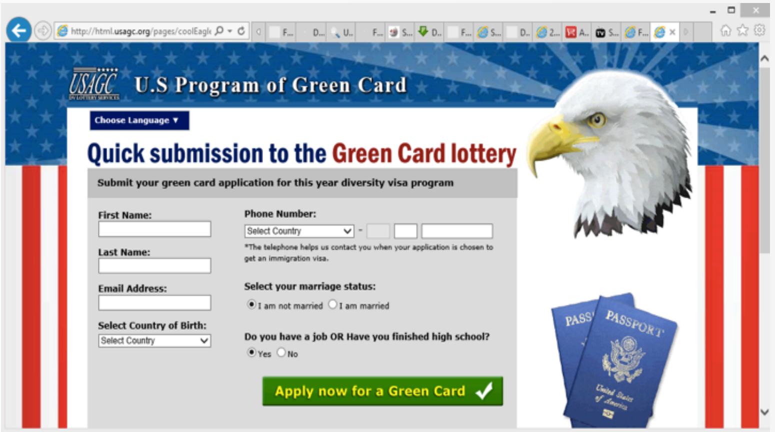
Authorized by:

Code No. PSN20121205

Section A: Grand Prize Value Disclosure

You have been directed to this prize claim form because you are a verified and confirmed winner of one of the prizes listed above. The Grand Prize value is:

$3,500.00



U.S Program of Green Card

Choose Language ▾

Quick submission to the Green Card lottery

Submit your green card application for this year diversity visa program

First Name:

Last Name:

Email Address:

Select Country of Birth: Select Country

Phone Number: Select Country

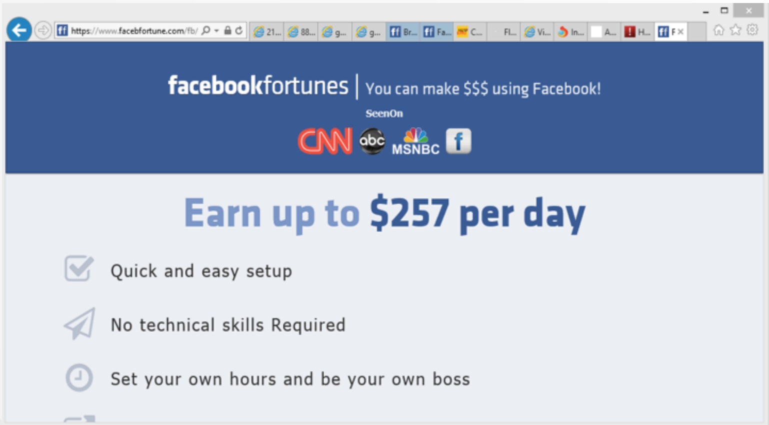
*The telephone helps us contact you when your application is chosen to get an immigration visa.

Select your marriage status:
● I am not married ○ I am married

Do you have a job OR Have you finished high school?
● Yes ○ No

Apply now for a Green Card ✓

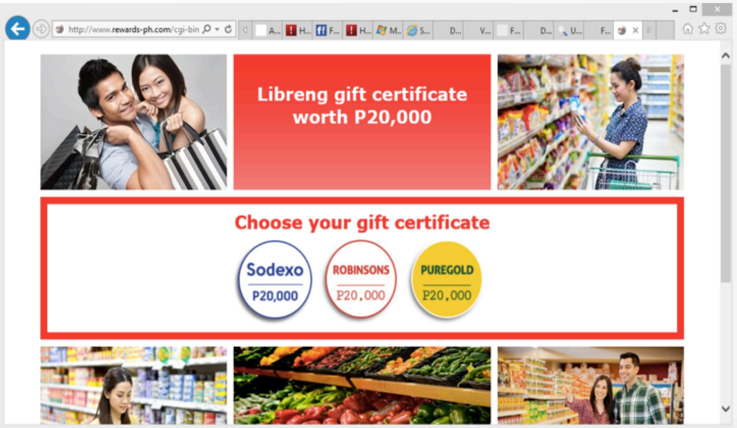
Scamvertising!



facebookfortunes | You can make $$$ using Facebook!

Earn up to $257 per day

- Quick and easy setup
- No technical skills Required
- Set your own hours and be your own boss



Libreng gift certificate worth P20,000

Choose your gift certificate

Sodexo P20,000

ROBINSONS P20,000

PUREGOLD P20,000

zvelo
We categorize the Web

Use of Non Human Traffic to Increase Impressions

- Bots! This is probably the most common thing that comes to mind.
- Non Human Traffic or NHT can be more than bots though.

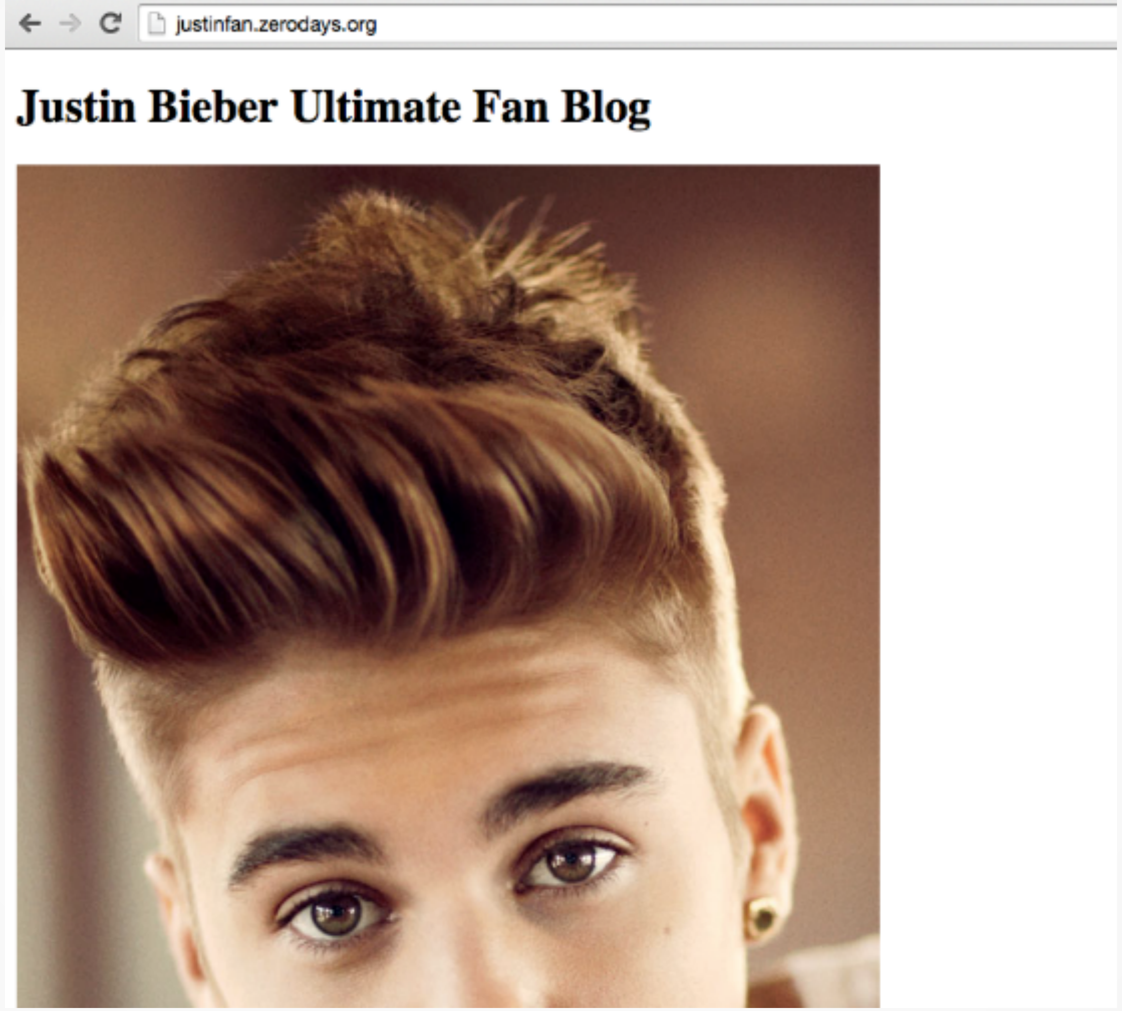
What is the best way to investigate this?

Buying Internet Traffic

What is Purchased Internet Traffic made of?

Can I buy internet traffic and get away with it?

The Bieber Project

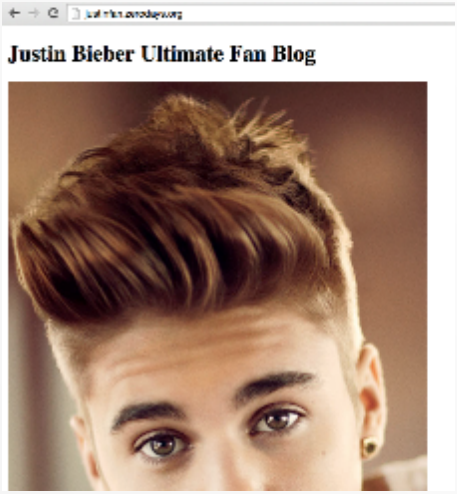


Justin Bieber Ultimate Fan Blog

Honeypot

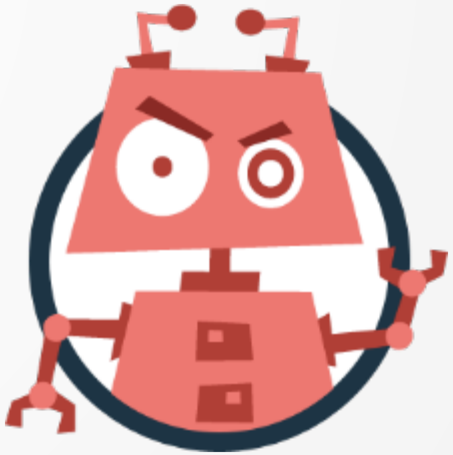
Collected Information

Bieber with a “Wire”

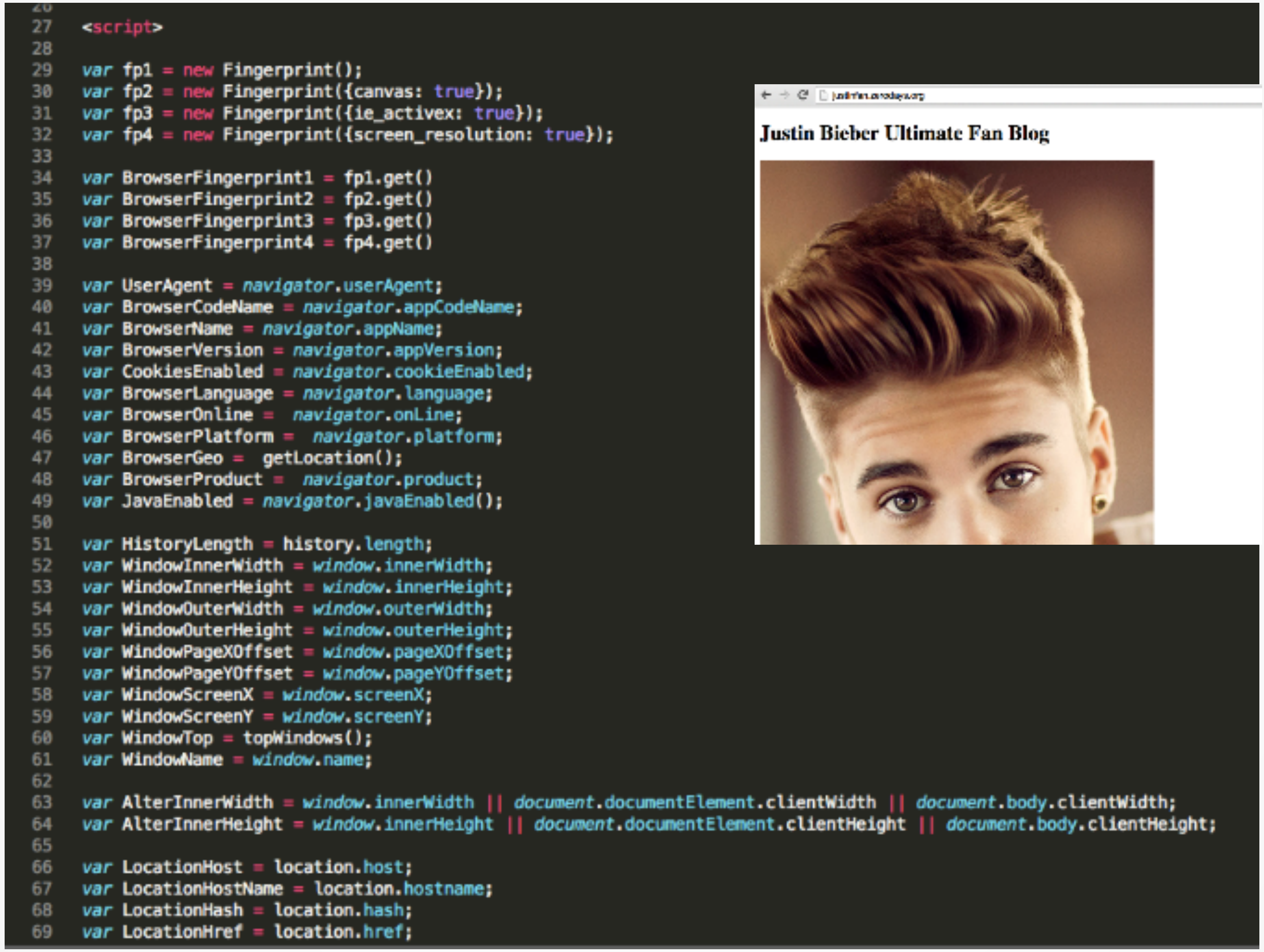


Justin Bieber Ultimate Fan Blog

Fraudulent Impressions?



Bieber with A Wire



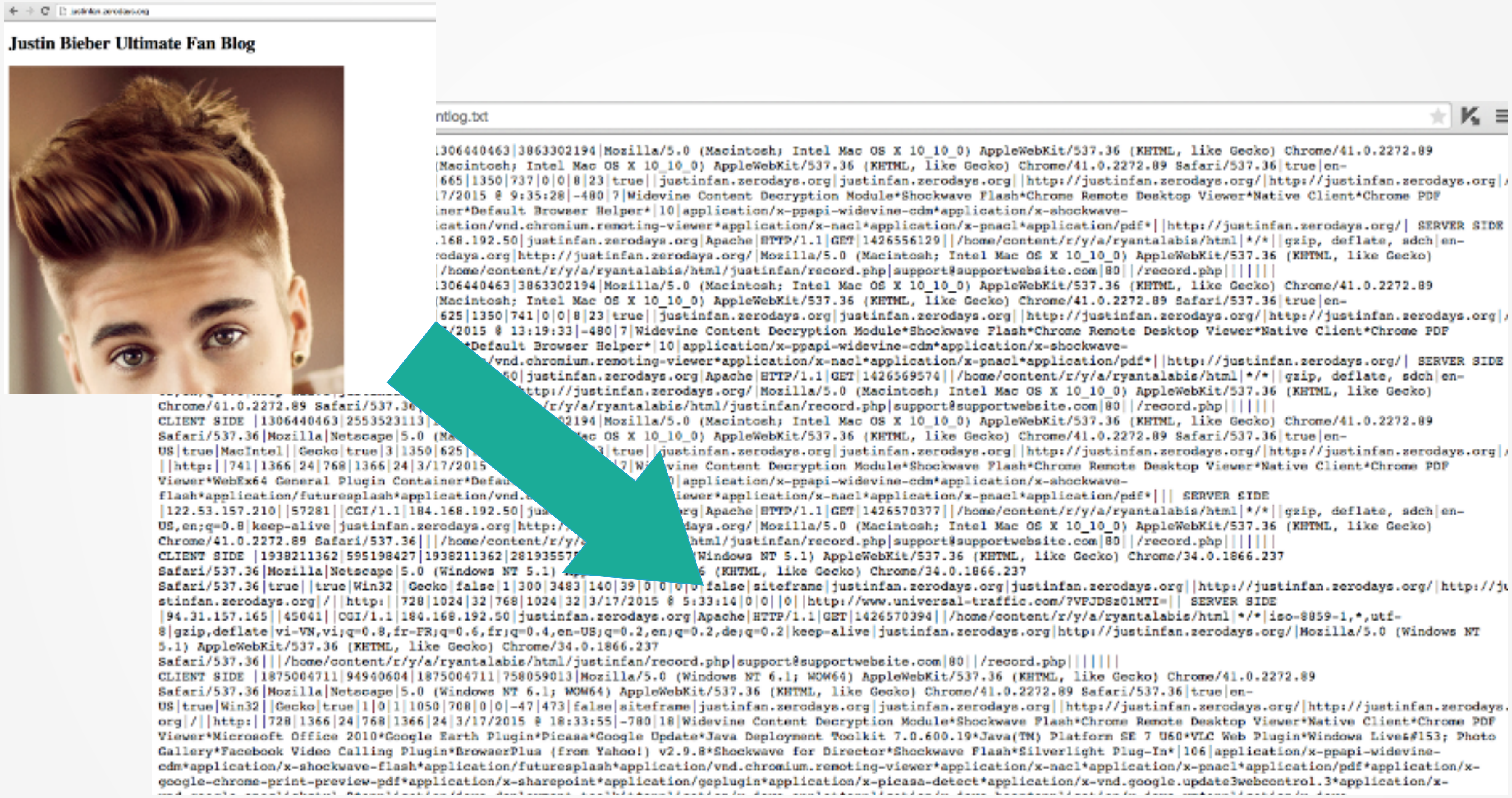
```
<script>

var fp1 = new Fingerprint();
var fp2 = new Fingerprint({canvas: true});
var fp3 = new Fingerprint({ie_activex: true});
var fp4 = new Fingerprint({screen_resolution: true});

var BrowserFingerprint1 = fp1.get()
var BrowserFingerprint2 = fp2.get()
var BrowserFingerprint3 = fp3.get()
var BrowserFingerprint4 = fp4.get()

var UserAgent = navigator.userAgent;
var BrowserCodeName = navigator.appCodeName;
var BrowserName = navigator.appName;
var BrowserVersion = navigator.appVersion;
var CookiesEnabled = navigator.cookieEnabled;
var BrowserLanguage = navigator.language;
var BrowserOnline =  navigator.onLine;
var BrowserPlatform =  navigator.platform;
var BrowserGeo =  getLocation();
var BrowserProduct =  navigator.product;
var JavaEnabled = navigator.javaEnabled();

var HistoryLength = history.length;
var WindowInnerWidth = window.innerWidth;
var WindowInnerHeight = window.innerHeight;
var WindowOuterWidth = window.outerWidth;
var WindowOuterHeight = window.outerHeight;
var WindowPageXOffset = window.pageXOffset;
var WindowPageYOffset = window.pageYOffset;
var WindowScreenX = window.screenX;
var WindowScreenY = window.screenY;
var WindowTop = topWindows();
var WindowName = window.name;

var AlterInnerWidth = window.innerWidth || document.documentElement.clientWidth || document.body.clientWidth;
var AlterInnerHeight = window.innerHeight || document.documentElement.clientHeight || document.body.clientHeight;

var LocationHost = location.host;
var LocationHostName = location.hostname;
var LocationHash = location.hash;
var LocationHref = location.href;
```

Justin Bieber Ultimate Fan Blog

zvelo

We categorize the Web

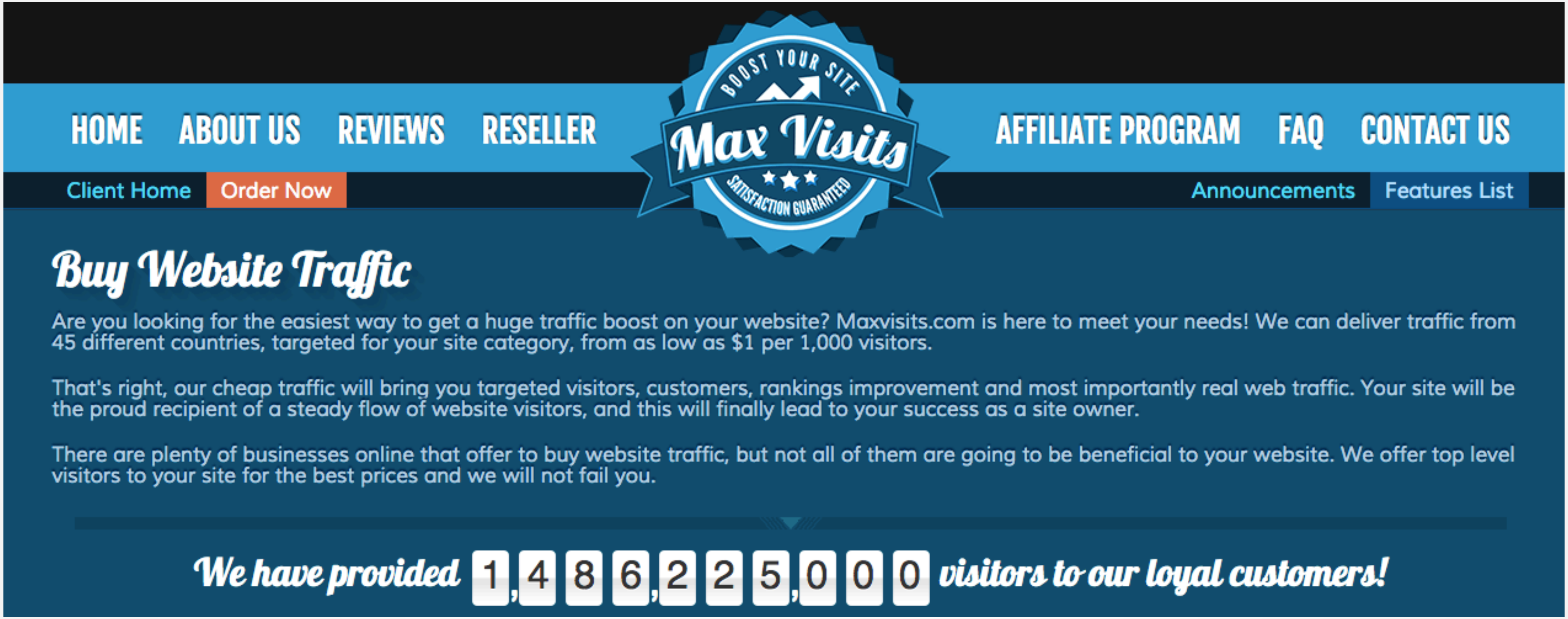
Data Stored for Analysis



Justin Bieber Ultimate Fan Blog

```
            306440463|3863302194|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89
            (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36|true|en-
            665|1350|737|0|0|8|23|true||justinfan.zerodays.org|justinfan.zerodays.org||http://justinfan.zerodays.org/|http://justinfan.zerodays.org|
            17/2015 @ 9:35:28|-480|7|Widevine Content Decryption Module*Shockwave Flash*Chrome Remote Desktop Viewer*Native Client*Chrome PDF
            iner*Default Browser Helper*|10|application/x-ppapi-widevine-cdm*application/x-shockwave-
            ication/vnd.chromium.remoting-viewer*application/x-nacl*application/x-pnacl*application/pdf*||http://justinfan.zerodays.org/| SERVER SIDE
            .168.192.50|justinfan.zerodays.org|Apache|HTTP/1.1|GET|1426556129||/home/content/r/y/a/ryantalabis/html|*/*||gzip, deflate, sdch|en-
            odays.org|http://justinfan.zerodays.org/|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko)
            |/home/content/r/y/a/ryantalabis/html/justinfan/record.php|support@supportwebsite.com|80||/record.php||||||
            306440463|3863302194|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89
            (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36|true|en-
            625|1350|741|0|0|8|23|true||justinfan.zerodays.org|justinfan.zerodays.org||http://justinfan.zerodays.org/|http://justinfan.zerodays.org|
             /2015 @ 13:19:33|-480|7|Widevine Content Decryption Module*Shockwave Flash*Chrome Remote Desktop Viewer*Native Client*Chrome PDF
             *Default Browser Helper*|10|application/x-ppapi-widevine-cdm*application/x-shockwave-
               /vnd.chromium.remoting-viewer*application/x-nacl*application/x-pnacl*application/pdf*||http://justinfan.zerodays.org/| SERVER SIDE
                 50|justinfan.zerodays.org|Apache|HTTP/1.1|GET|1426569574||/home/content/r/y/a/ryantalabis/html|*/*||gzip, deflate, sdch|en-
                   ttp://justinfan.zerodays.org/|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2272.89 Safari/537.36       /r/y/a/ryantalabis/html/justinfan/record.php|support@supportwebsite.com|80||/record.php||||||
CLIENT SIDE |1306440463|2553523113|       2194|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89
Safari/537.36|Mozilla|Netscape|5.0 (Ma     ac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36|true|en-
US|true|MacIntel||Gecko|true|3|1350|625|     3|true||justinfan.zerodays.org|justinfan.zerodays.org||http://justinfan.zerodays.org/|http://justinfan.zerodays.org|
||http:||741|1366|24|768|1366|24|3/17/2015     7|Wi  vine Content Decryption Module*Shockwave Flash*Chrome Remote Desktop Viewer*Native Client*Chrome PDF
Viewer*WebEx64 General Plugin Container*Defau     0|application/x-ppapi-widevine-cdm*application/x-shockwave-
flash*application/futuresplash*application/vnd.     iewer*application/x-nacl*application/x-pnacl*application/pdf*||| SERVER SIDE
|122.53.157.210||57281||CGI/1.1|184.168.192.50|ju     rg|Apache|HTTP/1.1|GET|1426570377||/home/content/r/y/a/ryantalabis/html|*/*||gzip, deflate, sdch|en-
US,en;q=0.8|keep-alive|justinfan.zerodays.org|http:/     days.org/|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2272.89 Safari/537.36|||/home/content/r/y/     html/justinfan/record.php|support@supportwebsite.com|80||/record.php||||||
CLIENT SIDE |1938211362|595198427|1938211362|28193555     Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1866.237
Safari/537.36|Mozilla|Netscape|5.0 (Windows NT 5.1)     6 (KHTML, like Gecko) Chrome/34.0.1866.237
Safari/537.36|true||true|Win32||Gecko|false|1|300|3483|140|39|0|0|0|0|false|siteframe|justinfan.zerodays.org|justinfan.zerodays.org||http://justinfan.zerodays.org/|http://ju
stinfan.zerodays.org|/||http:||728|1024|32|768|1024|32|3/17/2015 @ 5:33:14|0|0||0||http://www.universal-traffic.com/7VPJDSz01MTI=|| SERVER SIDE
|94.31.157.165||45041||CGI/1.1|184.168.192.50|justinfan.zerodays.org|Apache|HTTP/1.1|GET|1426570394||/home/content/r/y/a/ryantalabis/html|*/*|iso-8859-1,*,utf-
8|gzip,deflate|vi-VN,vi;q=0.8,fr-FR;q=0.6,fr;q=0.4,en-US;q=0.2,en;q=0.2,de;q=0.2|keep-alive|justinfan.zerodays.org|http://justinfan.zerodays.org/|Mozilla/5.0 (Windows NT
5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1866.237
Safari/537.36|||/home/content/r/y/a/ryantalabis/html/justinfan/record.php|support@supportwebsite.com|80||/record.php||||||
CLIENT SIDE |1875004711|94940604|1875004711|758059013|Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89
Safari/537.36|Mozilla|Netscape|5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36|true|en-
US|true|Win32||Gecko|true|1|0|1|1050|708|0|0|-47|473|false|siteframe|justinfan.zerodays.org|justinfan.zerodays.org||http://justinfan.zerodays.org/|http://justinfan.zerodays.
org|/||http:||728|1366|24|768|1366|24|3/17/2015 @ 18:33:55|-780|18|Widevine Content Decryption Module*Shockwave Flash*Chrome Remote Desktop Viewer*Native Client*Chrome PDF
Viewer*Microsoft Office 2010*Google Earth Plugin*Picasa*Google Update*Java Deployment Toolkit 7.0.600.19*Java(TM) Platform SE 7 U60*VLC Web Plugin*Windows Live&#153; Photo
Gallery*Facebook Video Calling Plugin*BrowserPlus (from Yahoo!) v2.9.8*Shockwave for Director*Shockwave Flash*Silverlight Plug-In*|106|application/x-ppapi-widevine-
cdm*application/x-shockwave-flash*application/futuresplash*application/vnd.chromium.remoting-viewer*application/x-nacl*application/x-pnacl*application/pdf*application/x-
google-chrome-print-preview-pdf*application/x-sharepoint*application/geplugin*application/x-picasa-detect*application/x-vnd.google.update3webcontrol.3*application/x-
```

Traffic Vendors



Buy Website Traffic

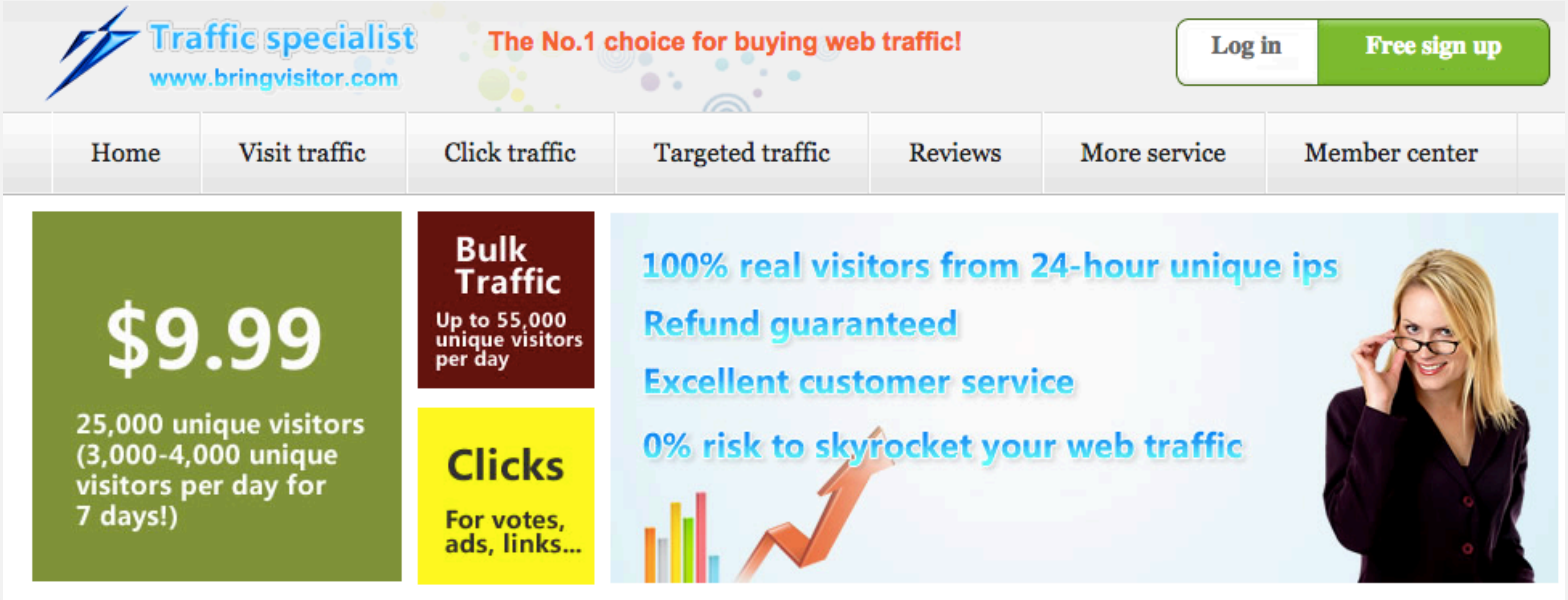
Are you looking for the easiest way to get a huge traffic boost on your website? Maxvisits.com is here to meet your needs! We can deliver traffic from 45 different countries, targeted for your site category, from as low as $1 per 1,000 visitors.

That's right, our cheap traffic will bring you targeted visitors, customers, rankings improvement and most importantly real web traffic. Your site will be the proud recipient of a steady flow of website visitors, and this will finally lead to your success as a site owner.

There are plenty of businesses online that offer to buy website traffic, but not all of them are going to be beneficial to your website. We offer top level visitors to your site for the best prices and we will not fail you.

We have provided 1,486,225,000 visitors to our loyal customers!

Traffic Vendors



Traffic specialist
www.bringvisitor.com

The No.1 choice for buying web traffic!

$9.99

25,000 unique visitors (3,000-4,000 unique visitors per day for 7 days!)

Bulk Traffic

Up to 55,000 unique visitors per day

Clicks

For votes, ads, links...

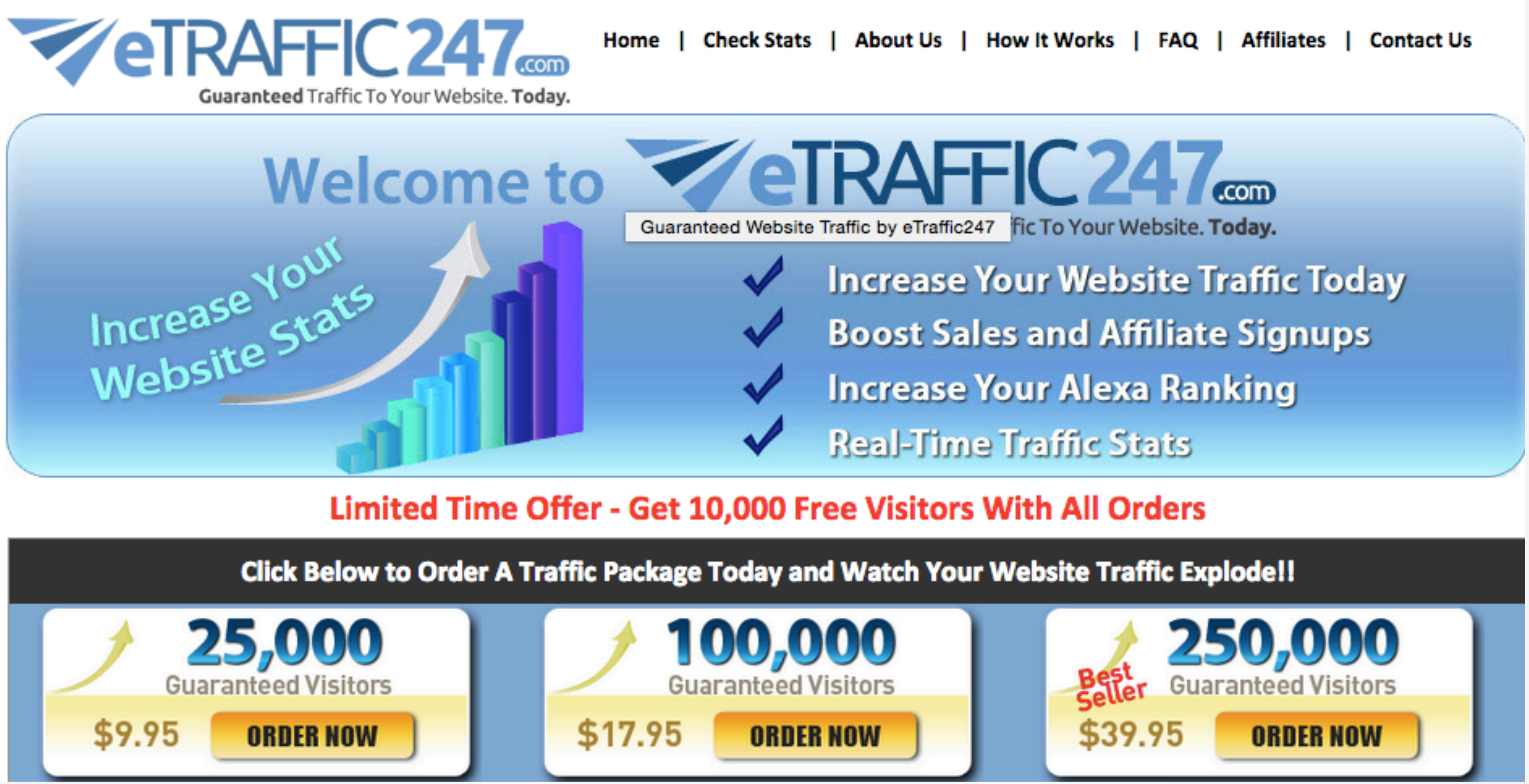
100% real visitors from 24-hour unique ips

Refund guaranteed

Excellent customer service

0% risk to skyrocket your web traffic

Traffic Vendors



eTRAFFIC247.com

Guaranteed Traffic To Your Website. Today.

Home | Check Stats | About Us | How It Works | FAQ | Affiliates | Contact Us

Welcome to eTRAFFIC247.com

Guaranteed Website Traffic by eTraffic247 fic To Your Website. Today.

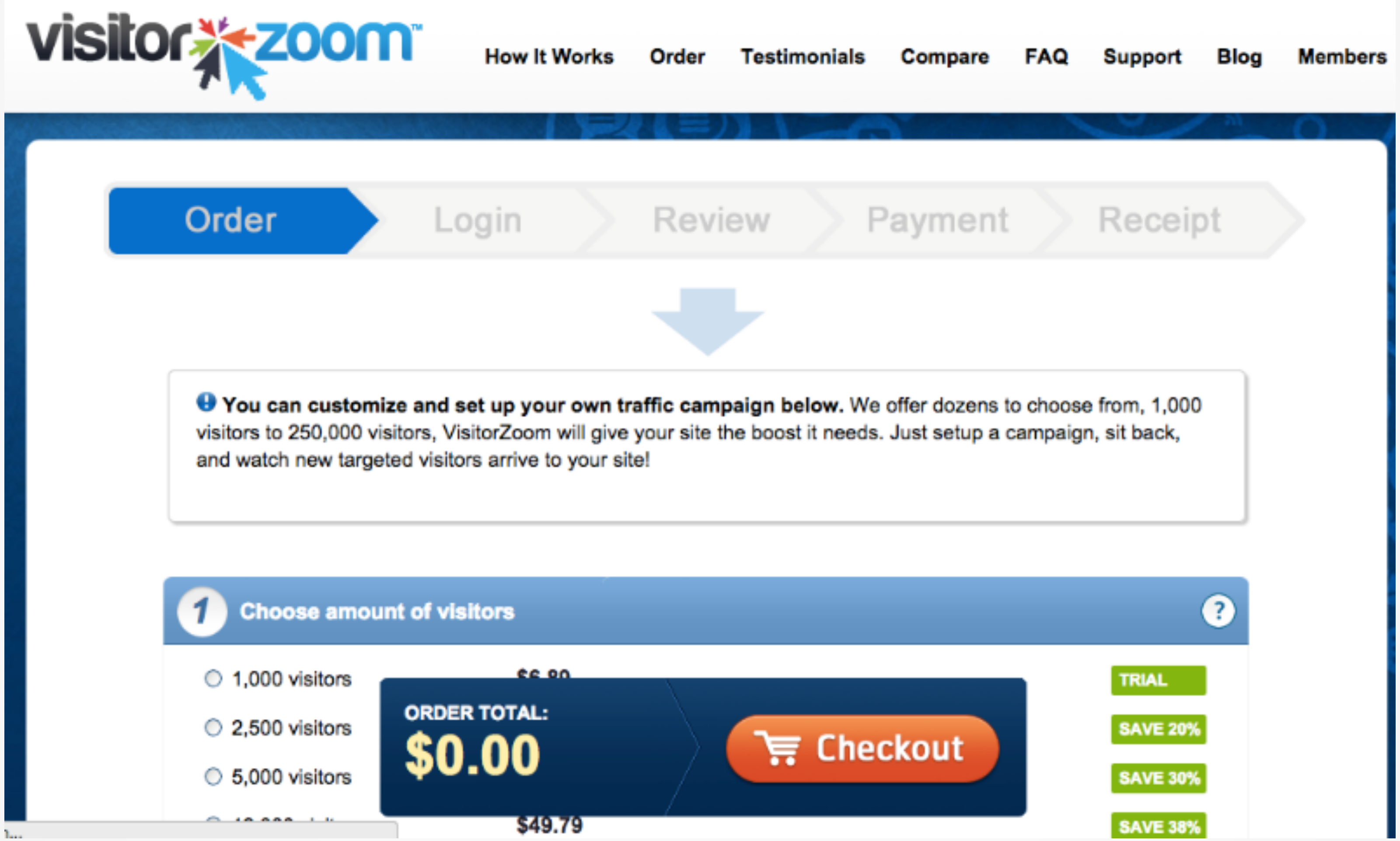
- ✓ Increase Your Website Traffic Today
- ✓ Boost Sales and Affiliate Signups
- ✓ Increase Your Alexa Ranking
- ✓ Real-Time Traffic Stats

Limited Time Offer - Get 10,000 Free Visitors With All Orders

Click Below to Order A Traffic Package Today and Watch Your Website Traffic Explode!!

25,000 Guaranteed Visitors $9.95 ORDER NOW	100,000 Guaranteed Visitors $17.95 ORDER NOW	Best Seller 250,000 Guaranteed Visitors $39.95 ORDER NOW

Traffic Vendors



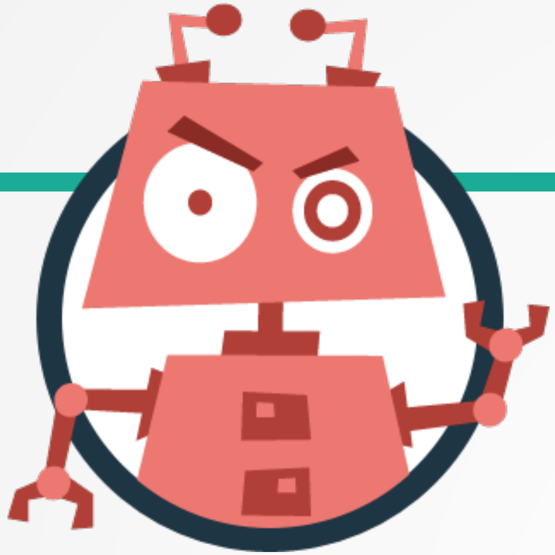
You can customize and set up your own traffic campaign below. We offer dozens to choose from, 1,000 visitors to 250,000 visitors, VisitorZoom will give your site the boost it needs. Just setup a campaign, sit back, and watch new targeted visitors arrive to your site!

1 Choose amount of visitors

○ 1,000 visitors	$6.80	TRIAL
○ 2,500 visitors		SAVE 20%
○ 5,000 visitors		SAVE 30%
	$49.79	SAVE 38%

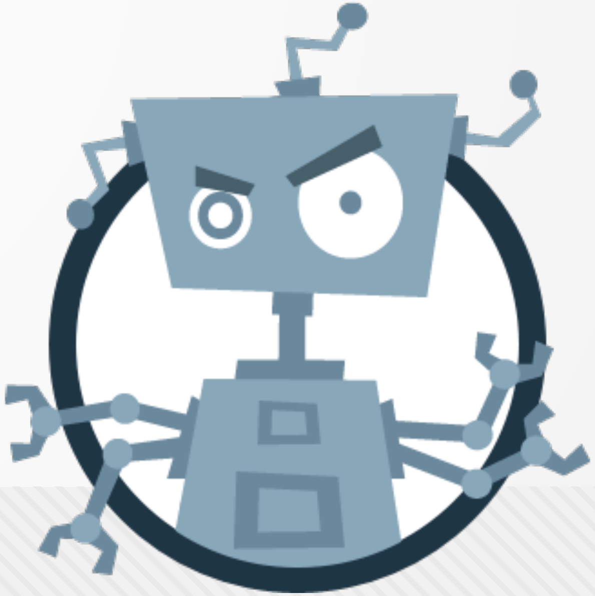
ORDER TOTAL:
$0.00

What is Purchased Internet Traffic Made Of?



Well..obviously **BOTS!**

(partly)

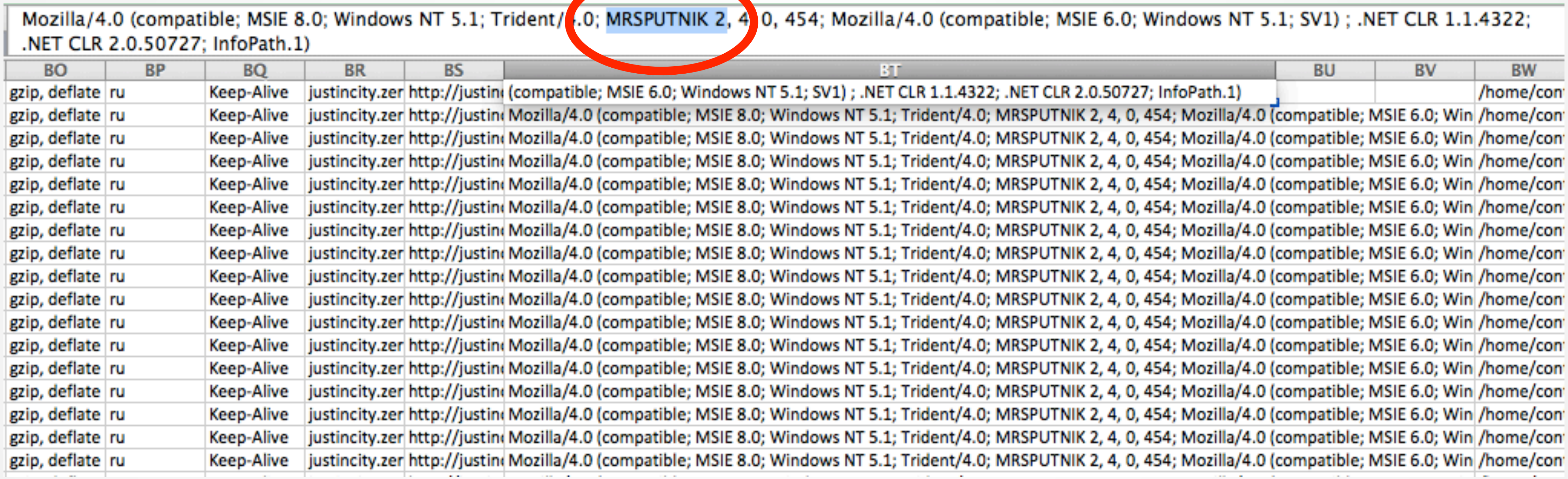


How do we know?

Clues are in the Impression…

What are the Clues…?

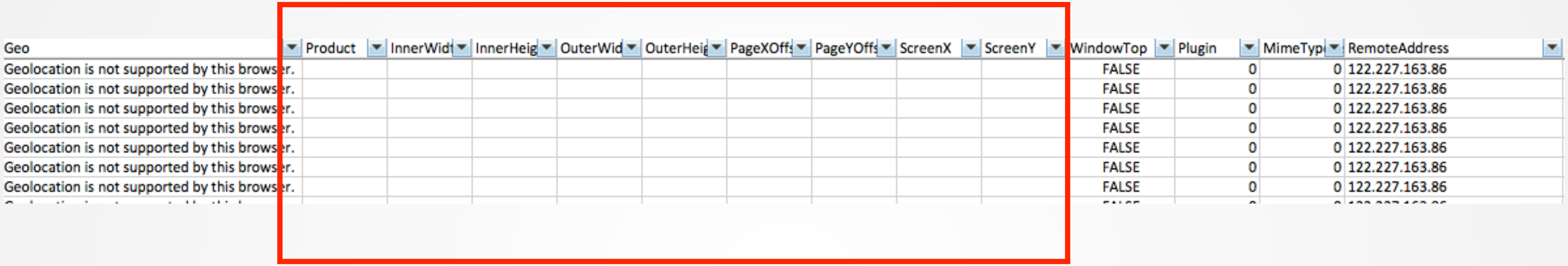
Browser has Suspicious User Agent…



Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)

BO	BP	BQ	BR	BS	BT	BU	BV	BW
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	(compatible; MSIE 6.0; Windows NT 5.1; SV1) ; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con
gzip, deflate	ru	Keep-Alive	justincity.zer	http://justin	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 454; Mozilla/4.0 (compatible; MSIE 6.0; Win			/home/con

What are the Clues…?

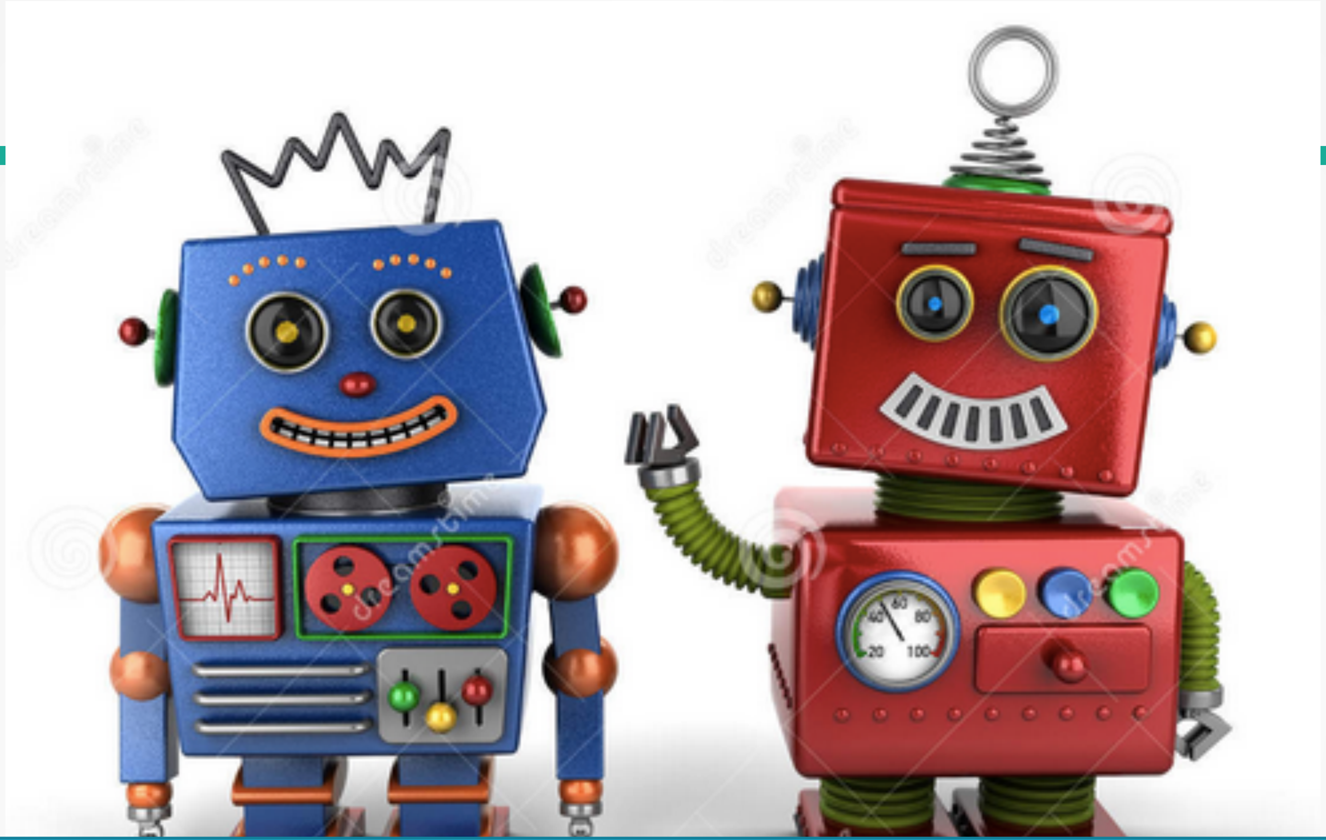


Geo	Product	InnerWidt	InnerHeig	OuterWid	OuterHeig	PageXOffs	PageYOffs	ScreenX	ScreenY	WindowTop	Plugin	MimeTyp	RemoteAddress
Geolocation is not supported by this browser.										FALSE	0	0	122.227.163.86
Geolocation is not supported by this browser.										FALSE	0	0	122.227.163.86
Geolocation is not supported by this browser.										FALSE	0	0	122.227.163.86
Geolocation is not supported by this browser.										FALSE	0	0	122.227.163.86
Geolocation is not supported by this browser.										FALSE	0	0	122.227.163.86
Geolocation is not supported by this browser.										FALSE	0	0	122.227.163.86
Geolocation is not supported by this browser.										FALSE	0	0	122.227.163.86

Lots of other suspicious information…

- No Plugins
- No Mime Types

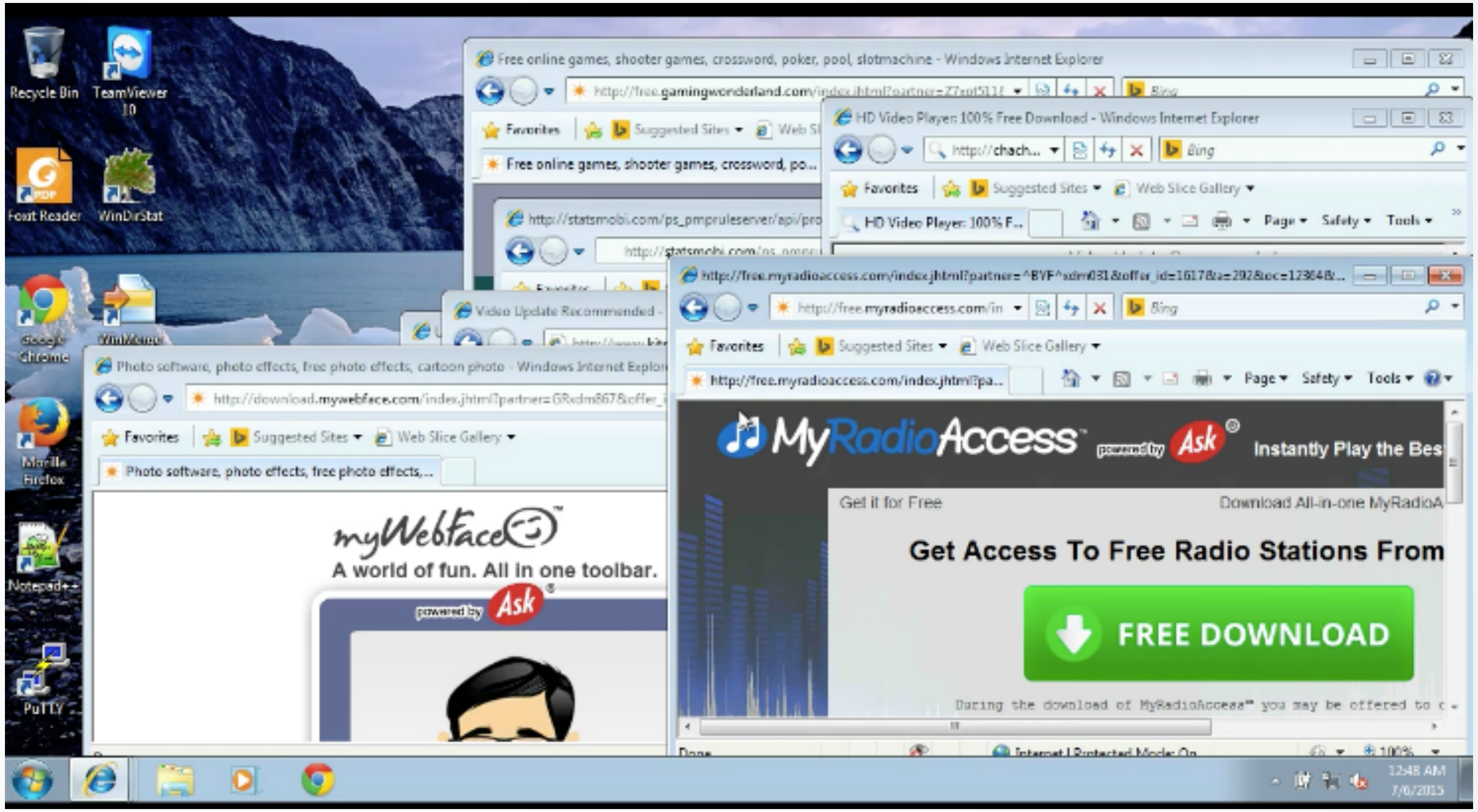
- Invisible Viewport Sizes
- Zero Page and Mouse Coordinates
- No Product Identifiers



It’s easy to catch “dumb” bots but what about the smarter ones?

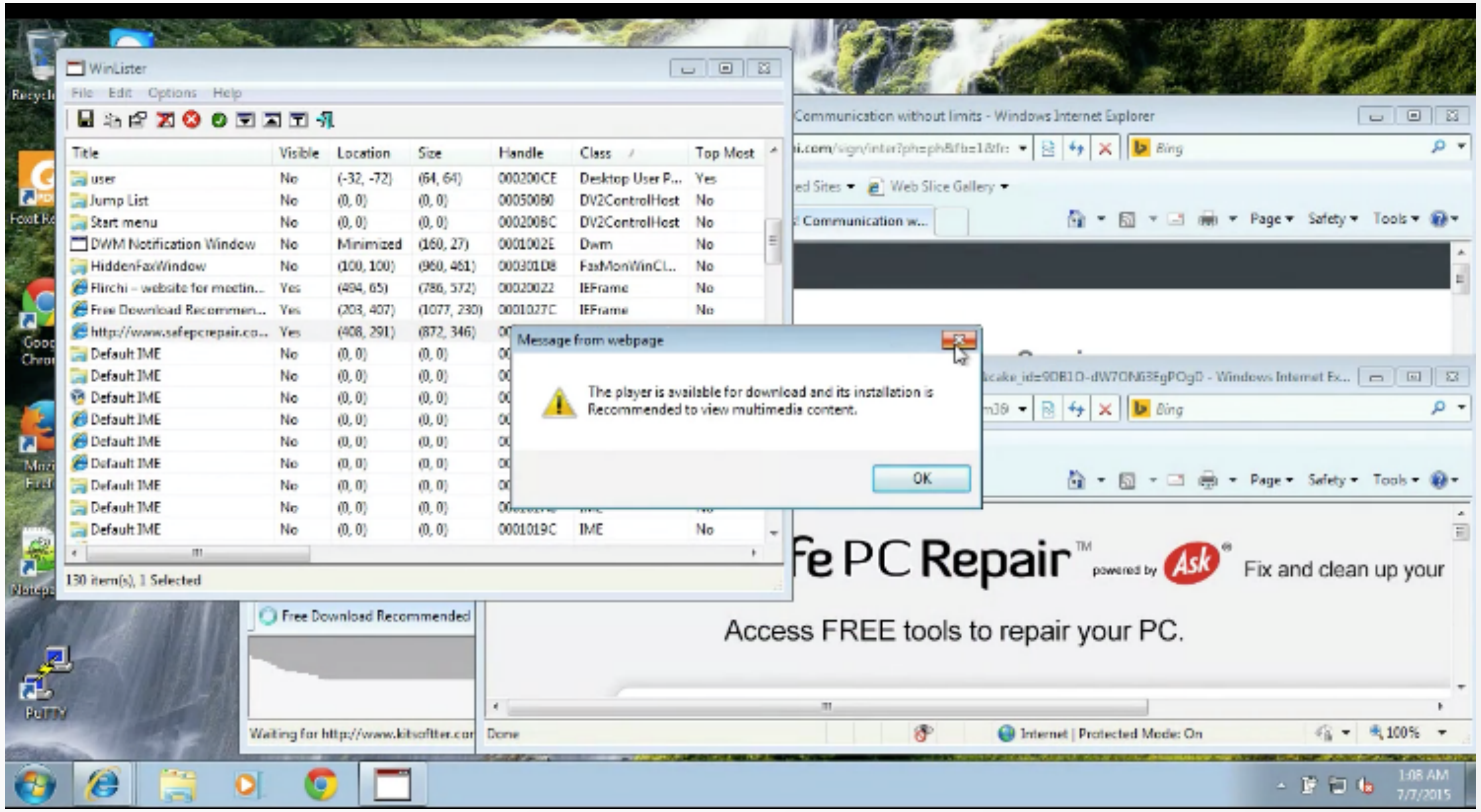
A Closer Look @ Smarter Bots

This is a video demonstration of a malware that hijacks a user's browser.


Recycle Bin
TeamViewer 10
Foxit Reader
WinDirStat
Google Chrome
WinMerge
Mozilla Firefox
Notepad++
PuTTY
Free online games, shooter games, crossword, poker, pool, slotmachine - Windows Internet Explorer
HD Video Player: 100% Free Download - Windows Internet Explorer
Photo software, photo effects, free photo effects, cartoon photo - Windows Internet Explorer
Video Update Recommended
http://free.myradioaccess.com/index.jhtml?partner=^BYF^xdm081&offer_id=1617&a=292&oc=12364&...
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Bing
myWebFace
A world of fun. All in one toolbar.
powered by Ask
MyRadioAccess
powered by Ask
Instantly Play the Bes
Get it for Free
Download All-in-one MyRadioA
Get Access To Free Radio Stations From
FREE DOWNLOAD
During the download of MyRadioAccess™ you may be offered to
Done
Internet | Protected Mode: On
100%
12:48 AM
7/6/2015

A Closer Look @ Smarter Bots

This is a video demonstration to show a stealthier ad fraud malware.


WinLister
File Edit Options Help
Communication without limits - Windows Internet Explorer
Web Slice Gallery
Page Safety Tools
Bing
Free Download Recommended
Waiting for http://www.kitsoftter.com
Done
Internet | Protected Mode: On
100%
OK
1:08 AM
7/7/2015

Title	Visible	Location	Size	Handle	Class	Top Most
user	No	(-32, -72)	(64, 64)	000200CE	Desktop User P...	Yes
Jump List	No	(0, 0)	(0, 0)	000500B0	DV2ControlHost	No
Start menu	No	(0, 0)	(0, 0)	000200BC	DV2ControlHost	No
DWM Notification Window	No	Minimized	(160, 27)	0001002E	Dwm	No
HiddenFaxWindow	No	(100, 100)	(960, 461)	000301D8	FaxMonWinCl...	No
Flirchi – website for meetin...	Yes	(494, 65)	(786, 572)	00020022	IEFrame	No
Free Download Recommen...	Yes	(203, 407)	(1077, 230)	0001027C	IEFrame	No
http://www.safepcrepair.co...	Yes	(408, 291)	(872, 346)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	[illegible]	[illegible]
Default IME	No	(0, 0)	(0, 0)	[illegible]	IME	No
Default IME	No	(0, 0)	(0, 0)	0001019C	IME	No

130 item(s), 1 Selected

Message from webpage

The player is available for download and its installation is Recommended to view multimedia content.

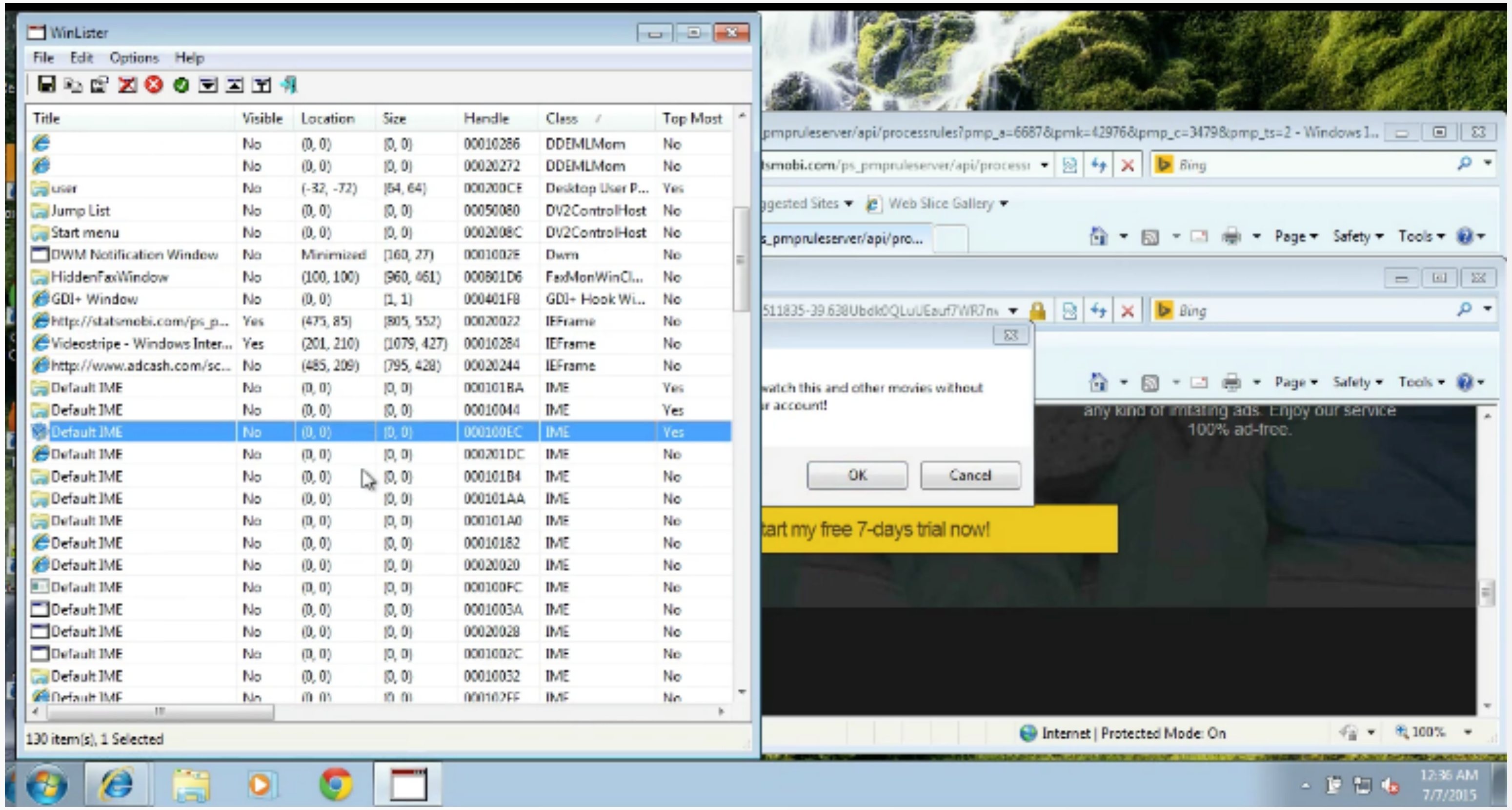
fe PC Repair™ powered by Ask® Fix and clean up your

Access FREE tools to repair your PC.

zvelo
We categorize the Web

A Closer Look @ Smarter Bots

This is a video demonstration showing a smarter malware that reproduces user events


WinLister
File
Edit
Options
Help
pmpruleserver/api/processrules?pmp_a=6687&pmk=42976&pmp_c=3479&pmp_ts=2 - Windows 1...
smobi.com/ps_pmpruleserver/api/processr
Bing
ggested Sites
Web Slice Gallery
s_pmpruleserver/api/pro...
Page
Safety
Tools
511835-39.638UbdkOQLuUEauf7WR7n
Bing
Page
Safety
Tools
OK
Cancel
tart my free 7-days trial now!
Internet | Protected Mode: On
100%
12:36 AM
7/7/2015

Title	Visible	Location	Size	Handle	Class	Top Most
	No	(0, 0)	(0, 0)	00010286	DDEMLMom	No
	No	(0, 0)	(0, 0)	00020272	DDEMLMom	No
user	No	(-32, -72)	(64, 64)	000200CE	Desktop User P...	Yes
Jump List	No	(0, 0)	(0, 0)	00050080	DV2ControlHost	No
Start menu	No	(0, 0)	(0, 0)	0002008C	DV2ControlHost	No
DWM Notification Window	No	Minimized	(160, 27)	0001002E	Dwm	No
HiddenFaxWindow	No	(100, 100)	(960, 461)	000801D6	FaxMonWinCl...	No
GDI+ Window	No	(0, 0)	(1, 1)	000401F8	GDI+ Hook Wi...	No
http://statsmobi.com/ps_p...	Yes	(475, 85)	(805, 552)	00020022	IEFrame	No
Videostripe - Windows Inter...	Yes	(201, 210)	(1079, 427)	00010284	IEFrame	No
http://www.adcash.com/sc...	No	(485, 209)	(795, 428)	00020244	IEFrame	No
Default IME	No	(0, 0)	(0, 0)	000101BA	IME	Yes
Default IME	No	(0, 0)	(0, 0)	00010044	IME	Yes
Default IME	No	(0, 0)	(0, 0)	000100EC	IME	Yes
Default IME	No	(0, 0)	(0, 0)	000201DC	IME	No
Default IME	No	(0, 0)	(0, 0)	000101B4	IME	No
Default IME	No	(0, 0)	(0, 0)	000101AA	IME	No
Default IME	No	(0, 0)	(0, 0)	000101A0	IME	No
Default IME	No	(0, 0)	(0, 0)	00010182	IME	No
Default IME	No	(0, 0)	(0, 0)	00020020	IME	No
Default IME	No	(0, 0)	(0, 0)	000100FC	IME	No
Default IME	No	(0, 0)	(0, 0)	0001003A	IME	No
Default IME	No	(0, 0)	(0, 0)	00020028	IME	No
Default IME	No	(0, 0)	(0, 0)	0001002C	IME	No
Default IME	No	(0, 0)	(0, 0)	00010032	IME	No
Default IME	No	(0, 0)	(0, 0)	000102FE	IME	No

130 item(s), 1 Selected

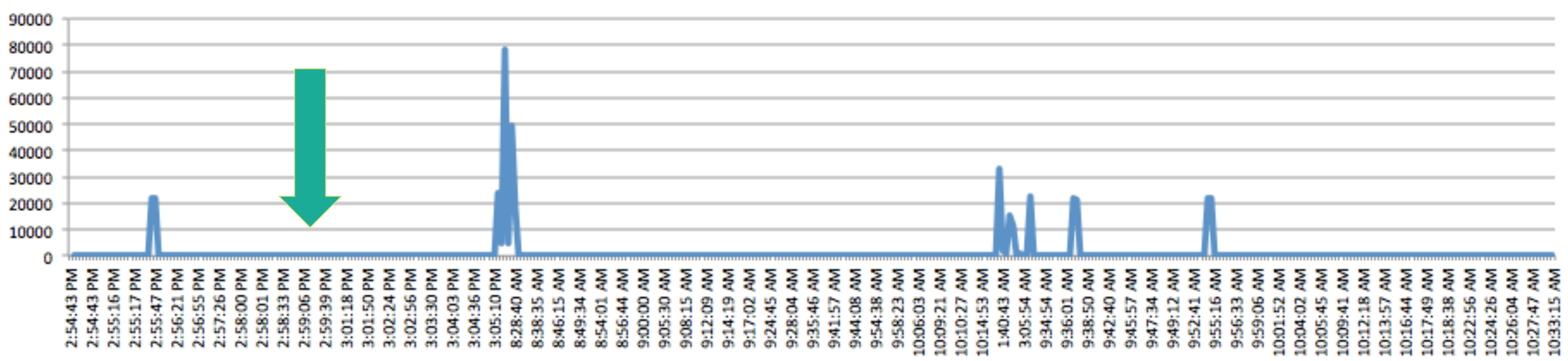
watch this and other movies without
r account!

any kind of irritating ads. Enjoy our service
100% ad-free.

What are the Clues…?

For hijacked machines, we need to do some trends analysis…

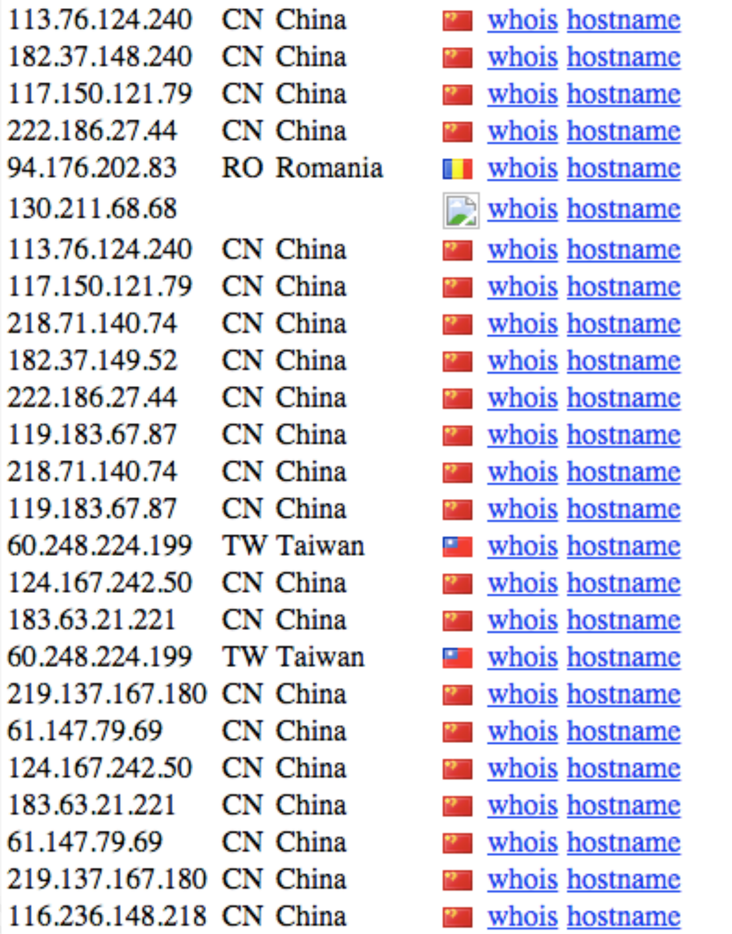
Example: Frequency between visits are too fast



zvelo
We categorize the Web

What are the Clues…?

You’ll need to look at broader patterns…

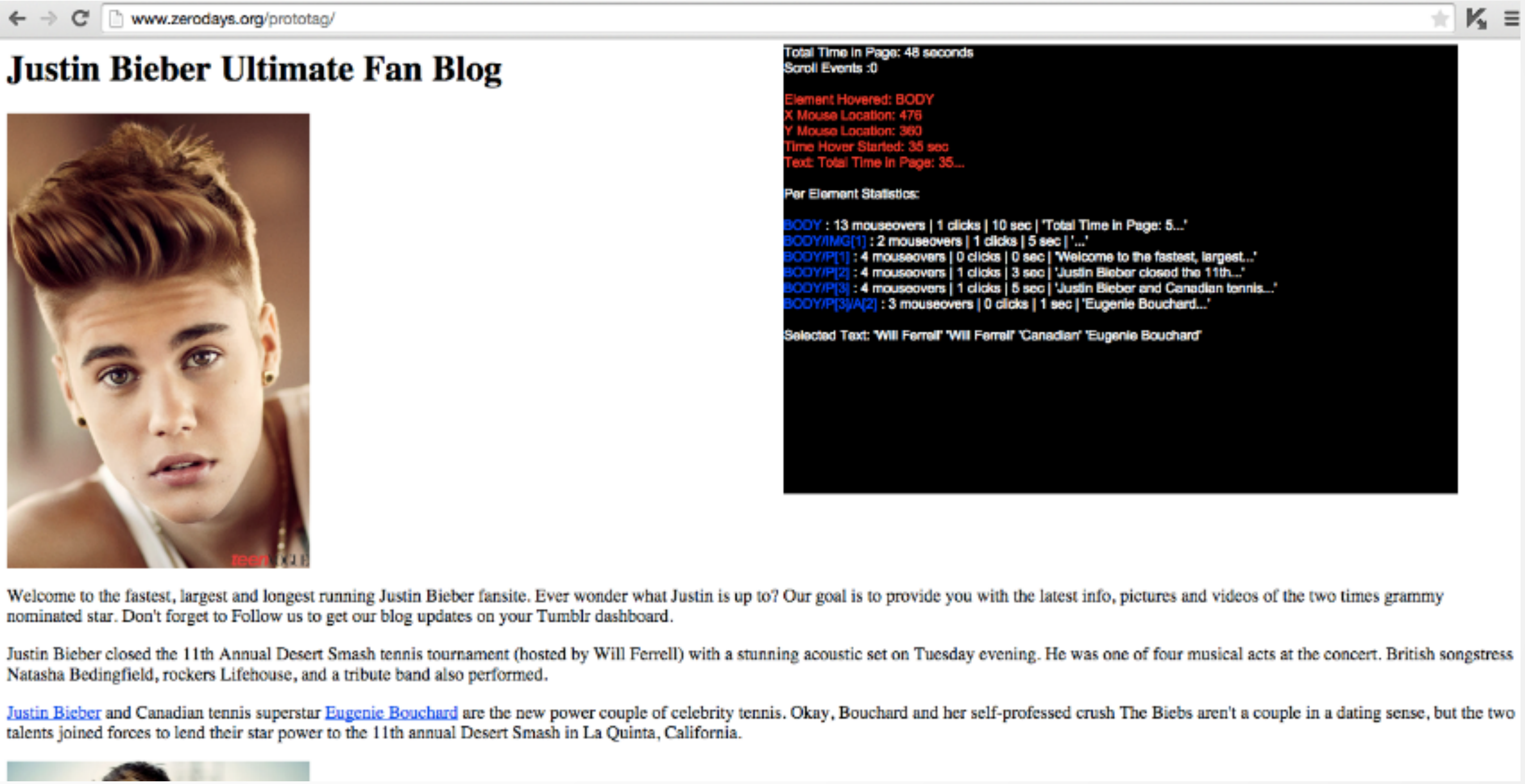


113.76.124.240	CN China	🇨🇳	whois	hostname
182.37.148.240	CN China	🇨🇳	whois	hostname
117.150.121.79	CN China	🇨🇳	whois	hostname
222.186.27.44	CN China	🇨🇳	whois	hostname
94.176.202.83	RO Romania	🇷🇴	whois	hostname
130.211.68.68			whois	hostname
113.76.124.240	CN China	🇨🇳	whois	hostname
117.150.121.79	CN China	🇨🇳	whois	hostname
218.71.140.74	CN China	🇨🇳	whois	hostname
182.37.149.52	CN China	🇨🇳	whois	hostname
222.186.27.44	CN China	🇨🇳	whois	hostname
119.183.67.87	CN China	🇨🇳	whois	hostname
218.71.140.74	CN China	🇨🇳	whois	hostname
119.183.67.87	CN China	🇨🇳	whois	hostname
60.248.224.199	TW Taiwan	🇹🇼	whois	hostname
124.167.242.50	CN China	🇨🇳	whois	hostname
183.63.21.221	CN China	🇨🇳	whois	hostname
60.248.224.199	TW Taiwan	🇹🇼	whois	hostname
219.137.167.180	CN China	🇨🇳	whois	hostname
61.147.79.69	CN China	🇨🇳	whois	hostname
124.167.242.50	CN China	🇨🇳	whois	hostname
183.63.21.221	CN China	🇨🇳	whois	hostname
61.147.79.69	CN China	🇨🇳	whois	hostname
219.137.167.180	CN China	🇨🇳	whois	hostname
116.236.148.218	CN China	🇨🇳	whois	hostname

Example: Doesn’t help that almost all of the traffic was coming from one IP block from China…

User Events

Show video of user event collection…



Justin Bieber Ultimate Fan Blog

```
Total Time in Page: 48 seconds
Scroll Events :0

Element Hovered: BODY
X Mouse Location: 476
Y Mouse Location: 360
Time Hover Started: 35 sec
Text: Total Time in Page: 35...

Per Element Statistics:

BODY : 13 mouseovers | 1 clicks | 10 sec | 'Total Time in Page: 5...'
BODY/IMG[1] : 2 mouseovers | 1 clicks | 5 sec | '...'
BODY/P[1] : 4 mouseovers | 0 clicks | 0 sec | 'Welcome to the fastest, largest...'
BODY/P[2] : 4 mouseovers | 1 clicks | 3 sec | 'Justin Bieber closed the 11th...'
BODY/P[3] : 4 mouseovers | 1 clicks | 5 sec | 'Justin Bieber and Canadian tennis...'
BODY/P[3]/A[2] : 3 mouseovers | 0 clicks | 1 sec | 'Eugenie Bouchard...'

Selected Text: 'Will Ferrell' 'Will Ferrell' 'Canadian' 'Eugenie Bouchard'
```

Welcome to the fastest, largest and longest running Justin Bieber fansite. Ever wonder what Justin is up to? Our goal is to provide you with the latest info, pictures and videos of the two times grammy nominated star. Don't forget to Follow us to get our blog updates on your Tumblr dashboard.

Justin Bieber closed the 11th Annual Desert Smash tennis tournament (hosted by Will Ferrell) with a stunning acoustic set on Tuesday evening. He was one of four musical acts at the concert. British songstress Natasha Bedingfield, rockers Lifehouse, and a tribute band also performed.

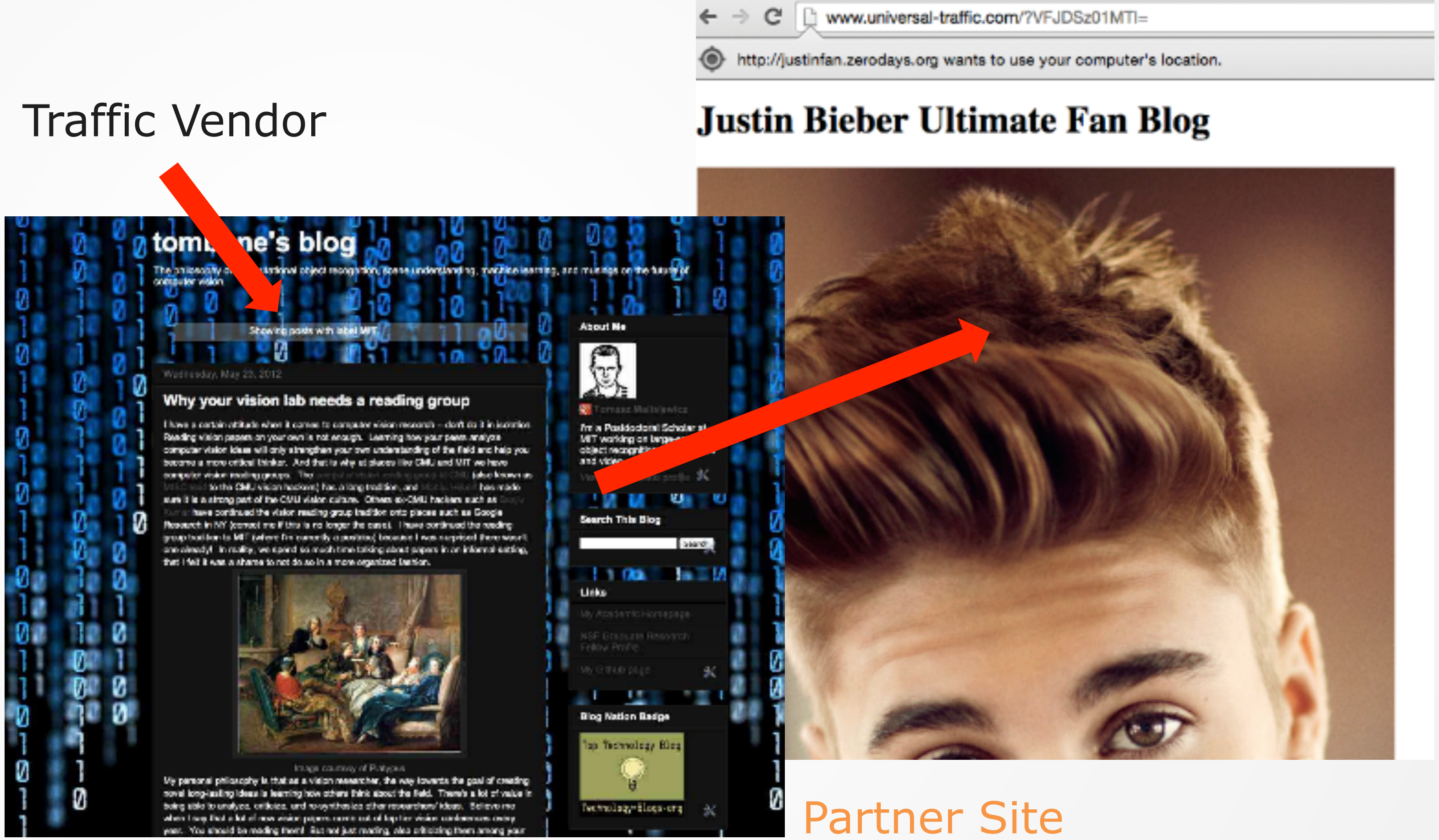
Justin Bieber and Canadian tennis superstar Eugenie Bouchard are the new power couple of celebrity tennis. Okay, Bouchard and her self-professed crush The Biebs aren't a couple in a dating sense, but the two talents joined forces to lend their star power to the 11th annual Desert Smash in La Quinta, California.

BUT it’s also made of HUMANS…

Who for all intents and purposes do not know they are visiting your site

Traffic is delivered to you through:

- Pop-unders
- Pop-ups
- Frames



Your Site

Traffic Vendor

Partner Site

www.universal-traffic.com/?VFJDSz01MTI=

http://justinfan.zerodays.org wants to use your computer's location.

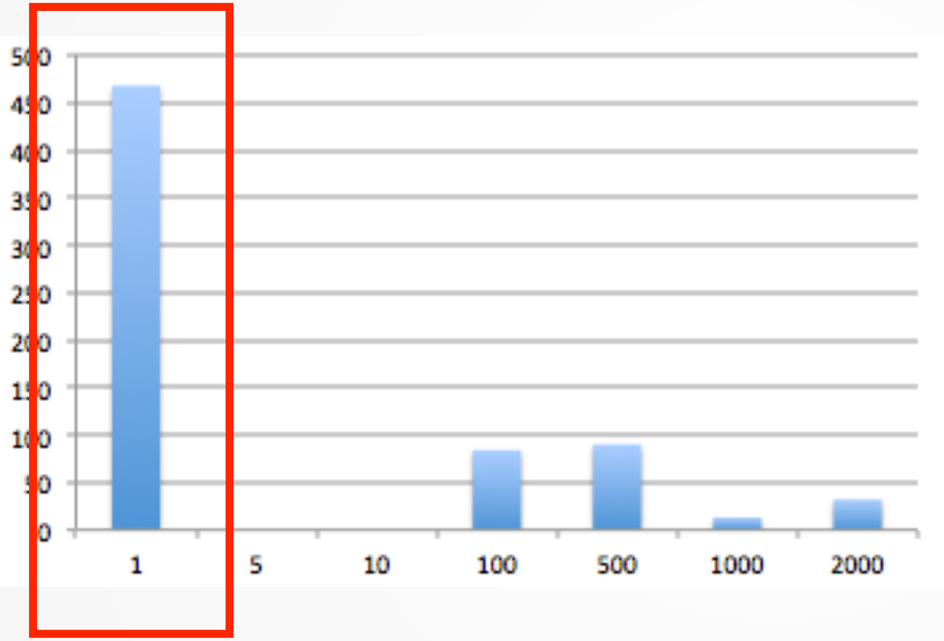
Justin Bieber Ultimate Fan Blog

tom ne's blog

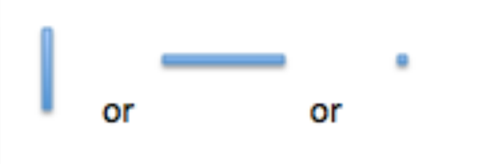
Why your vision lab needs a reading group

What are the Clues…?

70% of the viewports are 1 pixel!

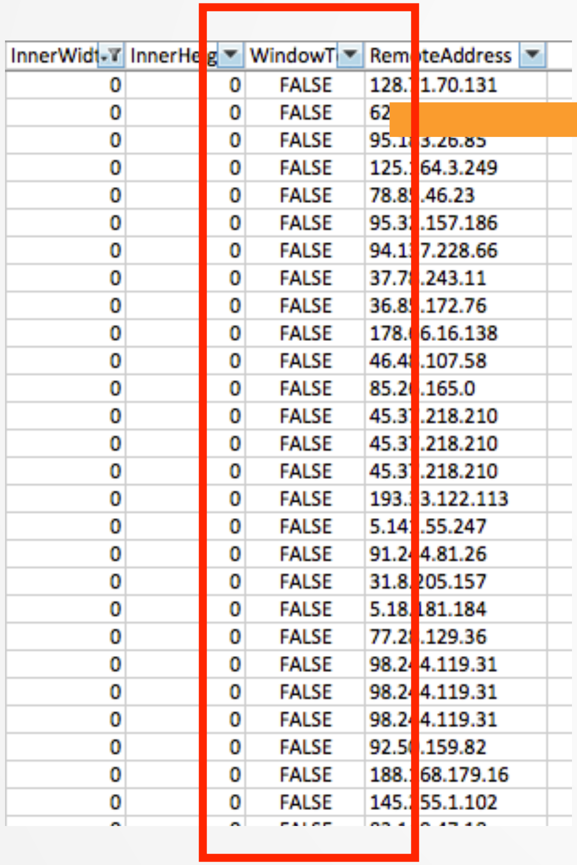


Meaning the size of the browsers viewing your site looks like this:

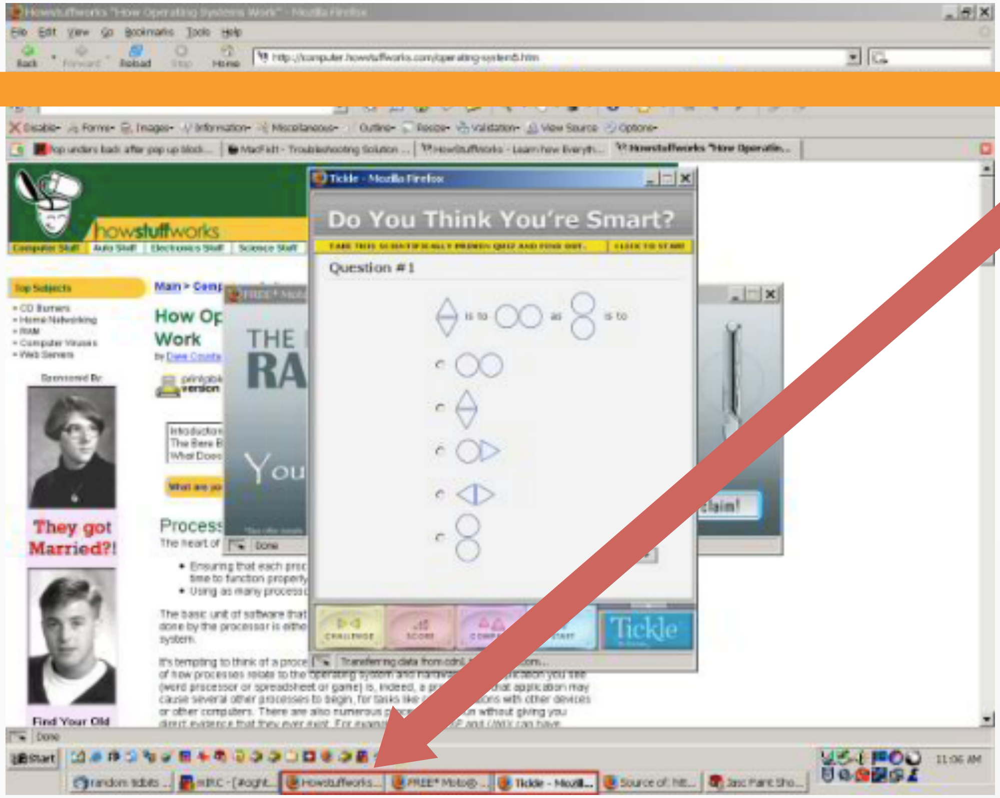


What are the Clues…?

The window is not the active window:



InnerWidt	InnerHeig	WindowT	RemoteAddress
0	0	FALSE	128.[illegible]1.70.131
0	0	FALSE	62[illegible]
0	0	FALSE	95.1[illegible]3.26.85
0	0	FALSE	125.[illegible]64.3.249
0	0	FALSE	78.8[illegible].46.23
0	0	FALSE	95.3[illegible].157.186
0	0	FALSE	94.1[illegible]7.228.66
0	0	FALSE	37.7[illegible].243.11
0	0	FALSE	36.8[illegible].172.76
0	0	FALSE	178.[illegible]6.16.138
0	0	FALSE	46.4[illegible].107.58
0	0	FALSE	85.2[illegible].165.0
0	0	FALSE	45.3[illegible].218.210
0	0	FALSE	45.3[illegible].218.210
0	0	FALSE	45.3[illegible].218.210
0	0	FALSE	193.[illegible]3.122.113
0	0	FALSE	5.14[illegible].55.247
0	0	FALSE	91.2[illegible]4.81.26
0	0	FALSE	31.8[illegible]205.157
0	0	FALSE	5.18[illegible]181.184
0	0	FALSE	77.2[illegible].129.36
0	0	FALSE	98.2[illegible]4.119.31
0	0	FALSE	98.2[illegible]4.119.31
0	0	FALSE	98.2[illegible]4.119.31
0	0	FALSE	92.5[illegible].159.82
0	0	FALSE	188.[illegible]68.179.16
0	0	FALSE	145.[illegible]55.1.102
0	0	FALSE	[illegible]


HowStuffWorks "How Operating Systems Work" - Mozilla Firefox
howstuffworks
Tickle - Mozilla Firefox
Do You Think You're Smart?
Question #1
Tickle
They got Married?!

Your site is here

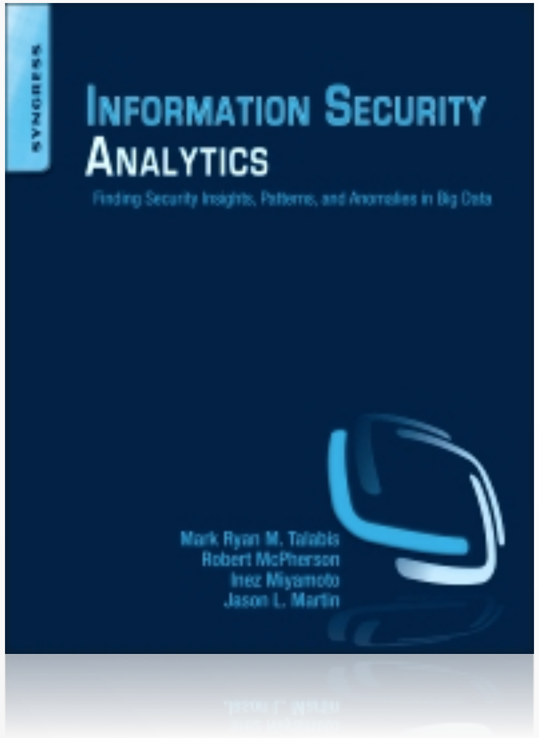
So…can I buy internet traffic and get away with it?

Depends.

- If an advertiser will audit the traffic and they know what to look for, you will get caught.
- If they don’t or if they don’t know what to look for, you won’t get caught.
- The “quality” of traffic is also directly proportional to how much you pay for it.
  - The lower prices, you’ll get bots.
  - They higher prices, you’ll get frames, popups or pop-unders.

If you liked my presentation

- Visit us at zvelo.com
- Check out my books: (available on Amazon)

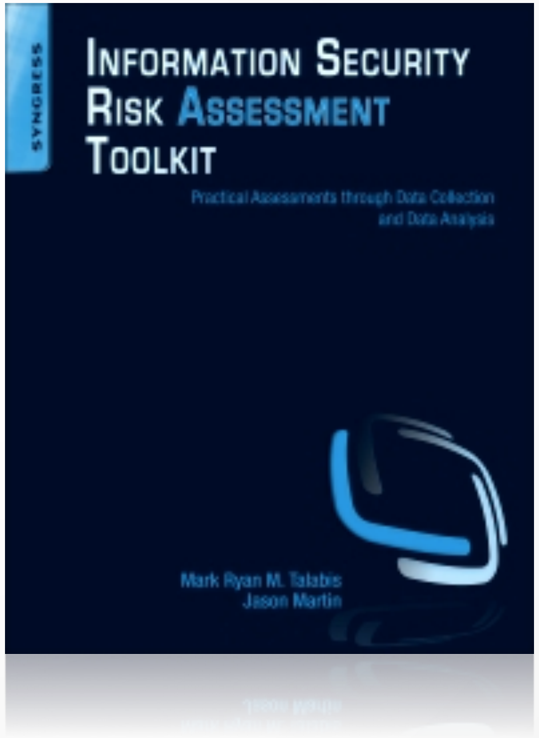


SYNGRESS

INFORMATION SECURITY ANALYTICS

Finding Security Insights, Patterns, and Anomalies in Big Data

Mark Ryan M. Talabis
Robert McPherson
Inez Miyamoto
Jason L. Martin



SYNGRESS

INFORMATION SECURITY RISK ASSESSMENT TOOLKIT

Practical Assessments through Data Collection and Data Analysis

Mark Ryan M. Talabis
Jason Martin

zvelo

We categorize the Web

www.zvelo.com