Mystery Shopping Inside the Ad Fraud Verification Bubble

A DHAR METHOD PUBLICATION

Authored by Shailin Dhar

"Advertisers, publishers, and everyone in between should pay attention to this report and take more aggressive and more detailed action against fraud -- don't assume someone else took care of it for you."

- Dr. Augustine Fou, Independent Ad Fraud Researcher

`

"I can't stress enough how important this research by Shailin and his team is. It shows clearly how easy it is to source sub-penny traffic that is specifically tailored to pass the filters of common ad fraud verification solutions."

- Mikko Kotila, Principal at botlab.io

TABLE OF CONTENTS

ABOUT THE AUTHOR SHAILIN DHAR

One of the few genuinely independent ad fraud consultants, Shailin is the author of *Uncommon Sense for Ad Tech,* an authoritative text on adtech, providing an unparalleled level of detail on the topic. Having worked years as a programmatic trader, and having gained first-hand experience in poorly understood, yet widely used practices of arbitrage and traffic sourcing, Shailin brings to the adtech industry a breadth of knowledge only few can claim. Ranging from meticulously thought out play-books for highly competitive media investment, to the dark arts of the adtech underbelly.

Shailin's consultancy, *The Dhar Method,* provides advisory and consultation on preventing advertising budgets from being spent on fraudulent sites and traffic. His unique method does not involve use of any technology, but focus on training your team in a way that guarantees true learning and understanding, together with sustainable results without reliance on 3rd-party technology partners. *The Dhar Method* services cover topics ranging from fundamental workings of programmatic advertising to every-day realities of billions of dollars of advertiser money being wasted on fake traffic and other forms of ad-fraud. *The Dhar Method* Services include staff training, supply and vendor audits, and various other buy-side focused evaluations.

Get more info about *The Dhar Method* from www.DharMethod.com or reach out to info@DharMethod.com.

DR. AUGUSTINE FOU
Ad Fraud Researcher

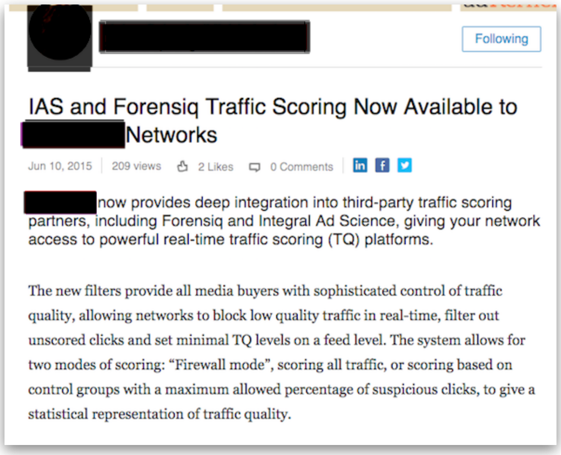
"This study is the 'smoking gun' and ballistics report that links the 'how' to the 'why'. We have long known the motive (huge profit) and opportunity (programmatic ad tech) for ad fraud. Shailin's experiment retraces the steps that cybercriminals take to make money from it. It shows just how easily they defeat widely used fraud detection mechanisms. Further, any "fraud free" guarantee is clearly a bad idea for both the party that offers it and the party that relies on it; 'fraud free' just means they couldn't detect it and block it; it's actually not fraud free.

MIKKO KOTILA
Principal @ botlab.io

"Since I started to research ad fraud in 2005, I've met only few people who have the level of understanding about ad fraud as Shailin does, and none of them work on the right side of the fight. Simply put, out of everyone out there working to make things better in the adtech industry, Shailin's understanding about ad fraud is a notch above the rest. "

MONETIZING FAKE TRAFFIC

The issue when a fraud detection vendor relying on proprietary technology becomes too widely used is that there is an incentive for sourced traffic vendors to reverse engineer the traffic profile needed to pass their filters and then sell that traffic to publishers who need to comply with demand from their buyers. For example, the PPC/CPC traffic market has traffic available for Integral Ad Science, Double Verify, MOAT, Forensiq, Pixalate. You can easily find people selling or seeking this traffic openly on LinkedIn; and you can find more with a web search. Example screenshots provided below:

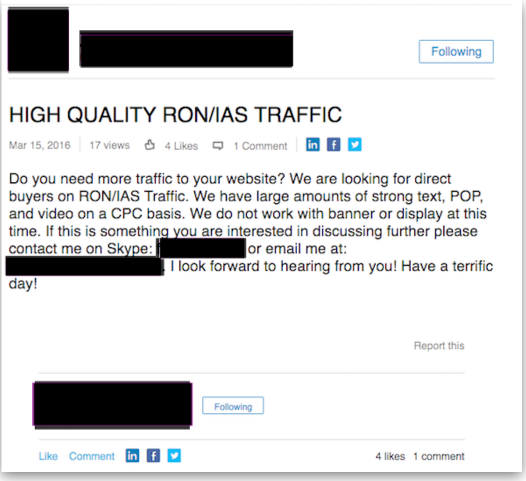

[redacted] [redacted]

IAS and Forensiq Traffic Scoring Now Available to [redacted]Networks

Jun 10, 2015 | 209 views | 2 Likes | 0 Comments

[redacted]now provides deep integration into third-party traffic scoring partners, including Forensiq and Integral Ad Science, giving your network access to powerful real-time traffic scoring (TQ) platforms.

The new filters provide all media buyers with sophisticated control of traffic quality, allowing networks to block low quality traffic in real-time, filter out unscored clicks and set minimal TQ levels on a feed level. The system allows for two modes of scoring: "Firewall mode", scoring all traffic, or scoring based on control groups with a maximum allowed percentage of suspicious clicks, to give a statistical representation of traffic quality.


[redacted] [redacted]

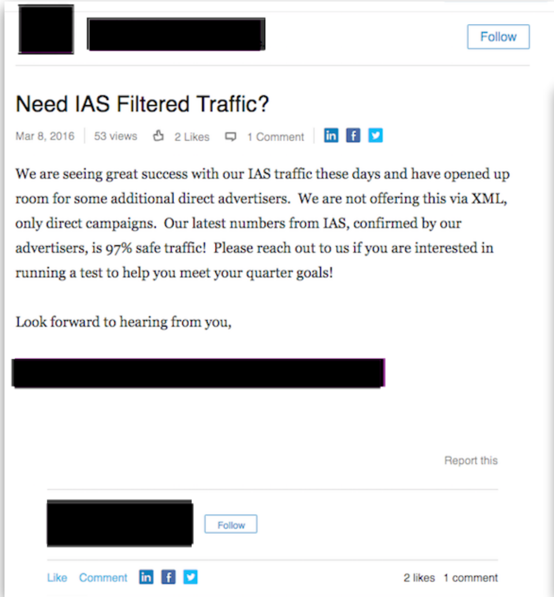
HIGH QUALITY RON/IAS TRAFFIC

Mar 15, 2016 | 17 views | 4 Likes | 1 Comment

Do you need more traffic to your website? We are looking for direct buyers on RON/IAS Traffic. We have large amounts of strong text, POP, and video on a CPC basis. We do not work with banner or display at this time. If this is something you are interested in discussing further please contact me on Skype: [redacted]or email me at: [redacted]. I look forward to hearing from you! Have a terrific day!

[redacted]

4 likes 1 comment


[redacted] [redacted]

Need IAS Filtered Traffic?

Mar 8, 2016 | 53 views | 2 Likes | 1 Comment

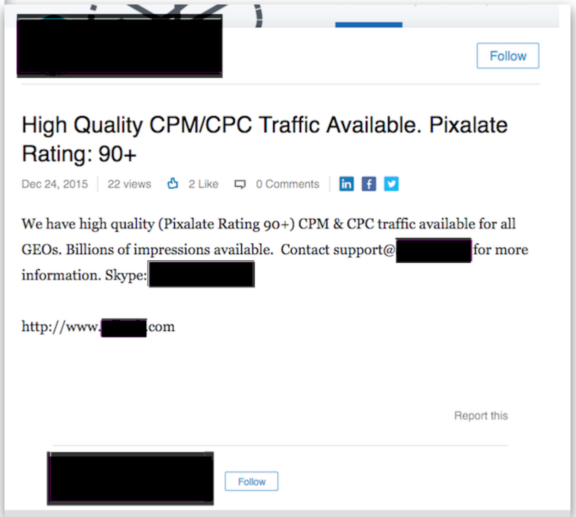
We are seeing great success with our IAS traffic these days and have opened up room for some additional direct advertisers. We are not offering this via XML, only direct campaigns. Our latest numbers from IAS, confirmed by our advertisers, is 97% safe traffic! Please reach out to us if you are interested in running a test to help you meet your quarter goals!

Look forward to hearing from you,

[redacted]

[redacted]

2 likes 1 comment


[redacted]

High Quality CPM/CPC Traffic Available. Pixalate Rating: 90+

Dec 24, 2015 | 22 views | 2 Like | 0 Comments

We have high quality (Pixalate Rating 90+) CPM & CPC traffic available for all GEOs. Billions of impressions available. Contact support@[redacted]for more information. Skype:[redacted]

http://www.[redacted]com

[redacted]

Advertising fraud is a tricky issue. Different people accept that the industry is afflicted with very different levels of fraud. In addition, there are differences of opinion on how easy it is to commit fraud. Many people, including trade bodies such as the ANA, AAAA, and IAB seem to have accepted that the solution is to merely implement a 3rd-party fraud detection solution. A common theme in the industry seems to be mindlessly repeating findings of a given organization, without much regard to the validity of the findings. Every bot detection or fraud verification vendor in the ad-technology space have many engaging visuals and well thought out mission statements. Each of them seems to be on the virtuous hunt for new malicious botnets to which they give appropriate names, that instill a notion in us that it should be taken seriously. Botnet detection, without a doubt, takes a lot of intelligence and persistence, but it does not solve the problem of ad-fraud to the extent they would have us believe. Identifying or even mitigating botnets does not take away the financial motivation for companies that benefit from ad-fraud to turn a blind eye to it, or to actively perpetuate it.

Note that we are making the point about "companies" as the beneficiaries of ad-fraud; not hackers or cybercriminals. Those are the terms that have misled us to believe that fraud is an external issue that infiltrates our systems, rather than studying how exactly robotic traffic enters the supply chain and why it continues to eat up advertising budgets meant for reaching humans. When we think of fraud as an external force, it is easy to justify that the bot detection software is the reasonable safeguard layer of protection against it.

Some ad-tech companies seem to think that fraud is decreasing, at least within their systems, because of the use of a major detection software. The true state of the industry is that the amount of fraud is consistently rising, because it's actually getting easier to commit. It's getting easier because there is less human scrutiny on DSP's, SSP's, publishers and their traffic. As long as you pass the filter that is in place, you are golden.

The sole reliance on a proprietary 3rd-party software to tell you what is fraudulent and what is not, has contributed to the rise in fraudulent traffic plaguing online advertising budgets. Since we have softwares now that spit out a metric of what was robotic and what was human, we are living in a frightening false sense of security when it comes to fraudulent traffic.

I've personally attempted various methods of education to raise the awareness level of fraud in the industry. While usually being laughed off as a "fear monger" or someone misinformed about the topic, about 10% of people I've spoken to have taken my warnings seriously and supported the fight against the rampant complicit-ness to fraud in online advertising. These 10% have kept us motivated to continue fighting the good fight. Thank you to: William Rand, Daniel Layfield, John Drake, and last but most definitely not least, Mikko Kotila.

In order to show evidence of fraud being not only easy to commit, I decided to set up a fake site and monetize it by sending robotic traffic to it and find out if I get blocked or even detected. The following report covers my process in creating the site (with very little technical capabilities), monetizing it, and then using well-known 3rd-party verification solutions to tracking the levels of fraud.

LEGAL DISCLAIMER: though we initially wanted to show how to generate a profit with fraudulent traffic, our legal advisors forbade us from doing so, and advice we decided to follow together with capping the total investment to a small amount.This project in it's entirety has run a deficit of $500, not including the revenue generated as a results of the failure on behalf of the platforms we used to detect the robotic traffic we sourced for the experiment. We will not accept the said revenue from the monetization partner.

As the goals for this project I wanted to demonstrate to the industry at large, that:

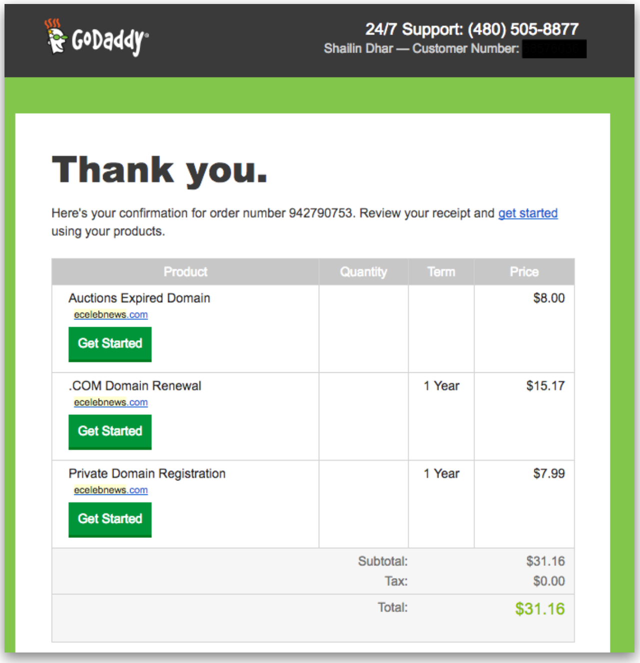
(1) **Traffic vendors sell traffic that is designed to and does pass major filters.**
(2) **The more widely used a filter is, the more widely it will be compromised. Buyers are not protected by the implementation of a verification software alone.**
(3) **Buyers should explore non-major-brand name fraud detection vendors as they are less likely to have traffic pre-engineered to bypass their filter.**
(4) **Fraud Detection vendors MUST be MORE cognizant of who all they are giving accounts to.**
(5) **We all MUST start taking fraud seriously. DO NOT UNDERESTIMATE the intelligence or motivation of people running fraudulent sites and operations.**

I sincerely hope you find this unique research useful,

Shailin Dhar
Independent Ad Fraud Consultant

THE WEBSITE - www.eCelebNews.com

The first step in this process is to create a site. We did this as simplistically as possible. On February 26, 2016 we went to GoDaddy auctions and searched the keyword "celeb."
The beautiful domain name of eCelebNews.com came up as available for $8.00. Then $15.17 for the yearly domain registration renewal. Then another $7.99 for private domain registration so nobody could tell that I was the one who owns the site.



24/7 Support: (480) 505-8877
Shailin Dhar — Customer Number: [redacted]

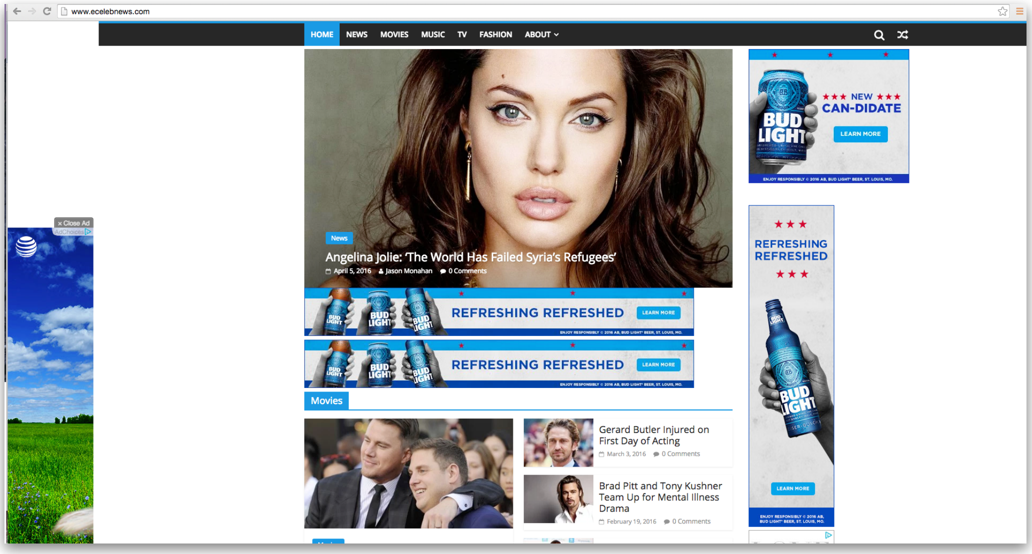
Thank you.

Here's your confirmation for order number 942790753. Review your receipt and get started using your products.

Product	Quantity	Term	Price
Auctions Expired Domain ecelebnews.com Get Started			$8.00
.COM Domain Renewal ecelebnews.com Get Started		1 Year	$15.17
Private Domain Registration ecelebnews.com Get Started		1 Year	$7.99
	Subtotal: Tax:		$31.16 $0.00
	Total:		$31.16

Since we were going to be buying traffic to this site, we needed a hosting provider. Why not stick with GoDaddy basic for $8.99/month? The focus was not on making this profitable, but simply to show that even with all industry standards, it is possible to monetize extremely cheap bot traffic with little to no effort.

Once the domain was registered, we needed to make it look like a website. Wordpress is generally the easiest way to set such a site up and a free theme was chosen. The content was ripped from arbitrage sites like www.OMGpeople.com and www.TheMagicDress.com.
We now had a site that has been registered since January 18, 2015 since we bought it on the auction rather than a new registration, so it would not appear as a new site to detection software. The site was next populated with celebrity related content that could be said to attract users through social and native advertising channels.


www.ecelebnews.com
HOME
NEWS
MOVIES
MUSIC
TV
FASHION
ABOUT
× Close Ad
AdChoices
News
Angelina Jolie: 'The World Has Failed Syria's Refugees'
April 5, 2016
Jason Monahan
0 Comments
★★★ NEW ★★★
CAN-DIDATE
LEARN MORE
ENJOY RESPONSIBLY © 2016 AB, BUD LIGHT® BEER, ST. LOUIS, MO.
REFRESHING REFRESHED
LEARN MORE
ENJOY RESPONSIBLY © 2016 AB, BUD LIGHT® BEER, ST. LOUIS, MO.
REFRESHING REFRESHED
LEARN MORE
ENJOY RESPONSIBLY © 2016 AB, BUD LIGHT® BEER, ST. LOUIS, MO.
★★★
REFRESHING REFRESHED
★★★
LEARN MORE
ENJOY RESPONSIBLY © 2016 AB, BUD LIGHT® BEER, ST. LOUIS, MO.
Movies
Gerard Butler Injured on First Day of Acting
March 3, 2016
0 Comments
Brad Pitt and Tony Kushner Team Up for Mental Illness Drama
February 19, 2016
0 Comments

You can find the site at: http://www.ecelebnews.com/

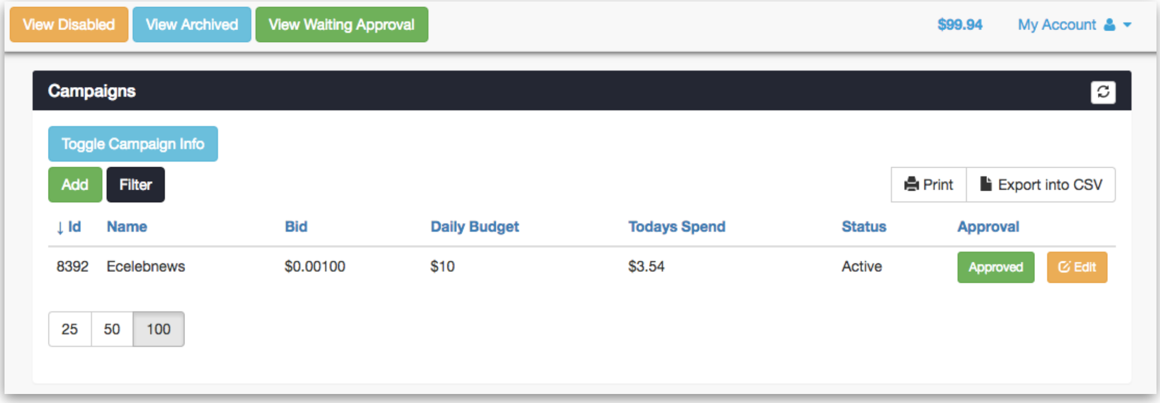
To any reasonable person, there is nothing attractive or interesting about the site. But when it comes to monetizing it with ad-technology, this site fits every criteria.

THE TRAFFIC - BUYING SOURCED TRAFFIC

Once we had the website up, it was time to start running traffic to the page while we went on to pick a monetization partner.

The one company we are NOT going to name in this report is the traffic vendor that provided us with the sourced traffic. Even though there will undoubtedly be people who will criticize this decision, there is no benefit from exposing a source of bot traffic as long as there is a demand for that type of traffic in the so-called legitimate market. If you close down one, another one will rise with a different name. Also as it had been already shown, such companies are very easy to find. As long as publishers, big and small, continue to buy traffic without concern whether it's human or bot, there will always be companies selling the traffic.

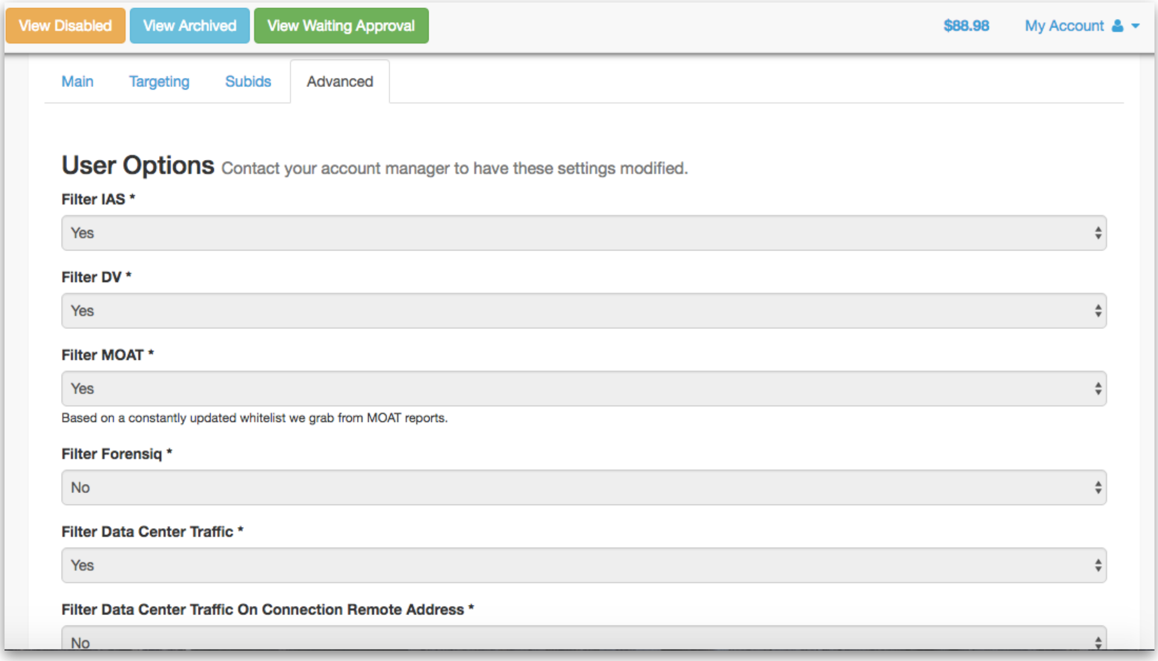
Through our traffic partner for this test, we set up a campaign in their platform to buy CPC traffic at $0.001 per click with a budget of $10 per day.



Campaigns

↓ Id	Name	Bid	Daily Budget	Todays Spend	Status	Approval
8392	Ecelebnews	$0.00100	$10	$3.54	Active	Approved Edit

Even at this low of a cost, this traffic was designed to pass Integral Ad Science, DoubleVerify, and MOAT filters. We'll get to how well it passed the filters and why in the sections below.



User Options Contact your account manager to have these settings modified.

Filter IAS *
Yes

Filter DV *
Yes

Filter MOAT *
Yes
Based on a constantly updated whitelist we grab from MOAT reports.

Filter Forensiq *
No

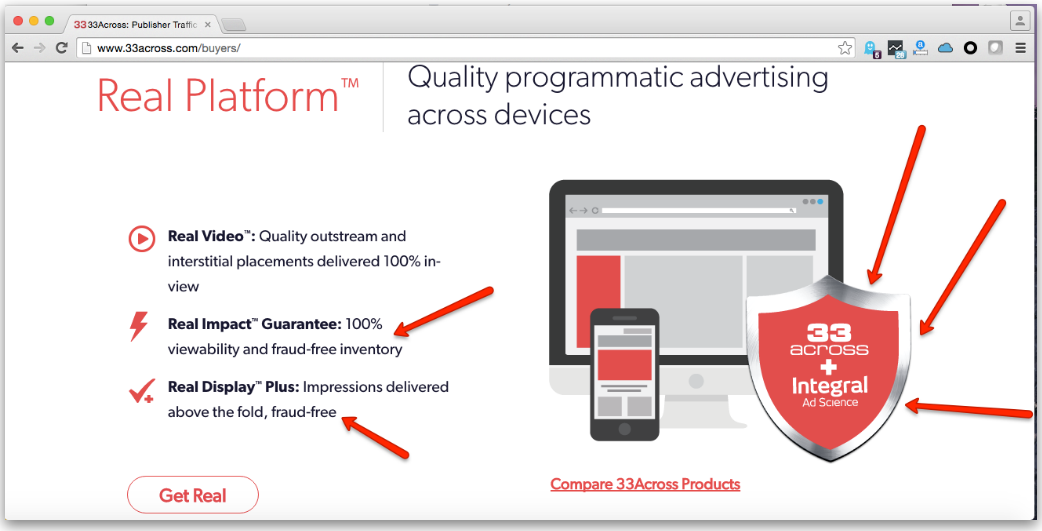
Filter Data Center Traffic *
Yes

Filter Data Center Traffic On Connection Remote Address *
No

MONETIZATION & INTEGRAL AD SCIENCE VERIFICATION

Now this was where it got tricky. Which company do we use as a method for monetizing this worthless robotic traffic we are buying at 1/1000 of what could be considered as a competitive price ($1 CPC)?

Instead of picking whichever major company was easiest to get approved in, we decided to make a point and choose an ad platform that is using a 3rd-party verification solution to provide a traffic quality guarantee to their buyers. 33Across was chosen because they guarantee "100% viewability and fraud-free inventory" through their partnership with Integral Ad Science, arguably the best known ad fraud verification company. 33Across focuses its website marketing communication on the guarantee it provides.



Real Platform™

Quality programmatic advertising across devices

Real Video™: Quality outstream and interstitial placements delivered 100% in-view

Real Impact™ Guarantee: 100% viewability and fraud-free inventory

Real Display™ Plus: Impressions delivered above the fold, fraud-free

The way they claim to use Integral Ad Science is that it acts like a protective wall to their ad server and does not allow any suspicious impressions through. In other words, the numbers you see in their reporting console will only include what they deem as non-fraudulent or human impressions.. In other words, any impression that would be registered in the 33Across console would have to pass the Integral Ad Science filter. We knew beforehand that all of the traffic was going to be robotic, so none of it should have become visible in the console.

We got approved within 2 days and there was absolutely no skepticism or doubt around the eCelebNews site, nor was there any skepticism when I said I'm buying all of my traffic.

The 33Across/Tynt tags are super easy to implement, which may be great for a legitimate publisher, but it makes them extremely attractive for a fraudulent player due to their easy of implementation, together with the low-friction no-questions-asked sign-up process

The standard floor prices to implement are $1 or $2 depending on the ad-units, and we went with whatever suggestions the account manager gave.

At no point were they made aware that all of this traffic was robotic nor that their technology was being put to test for its effectiveness. We were about to start the first "mystery shopping" experiment ever conducted on the topic of ad fraud verification.

VERIFICATION - MOAT

MOAT provided a trial account in order for us to see how their system measured the traffic sent to the page by the sourced traffic company we used for this test.

Initially there were a few implementation issues because MOAT wanted a pixel on every ad-tag but eventually I persuaded them to just provide a content-tag which only tracked traffic quality to the page. For the purposes of this experiment, there was no need for viewability metrics available through ad-tag level implementation.

While MOAT agreed to set up a trial account, at no point they were made aware that all of this traffic was robotic nor that their technology was being put to test for its effectiveness.

VERIFICATION - Oxford-BioChronometrics and DataDome

Since the traffic we were buying was designed to pass the Integral Ad Science and MOAT filters, it was the logical step that we would have agnostic bot-detection platforms track the traffic as well.

For this purpose two less known ad fraud verification companies based in Europe were selected.

Oxford-BioChronometrics (https://oxford-biochron.com/) is a Luxembourg based verification that company that does many things in addition to blocking fraudulent ad traffic; they also focus on user authentication and fighting phishing and spam.

DataDome (https://datadome.co/) is a Paris based bot-detection platform that focuses on web security and data fraud in addition to ad-fraud.

Both companies were gracious enough to participate in this study and offer their services complimentary to see how they detected the traffic.

The CMO of Oxford-BioChron, William Scheckel, who is also a professor of marketing at NYIT, was our contact at Oxford and facilitated the implementation which involved a single pixel being put in the header of our page.

A partner at DataDome, Benjamin Barrier, was our contact at DataDome and he facilitated the implementation of the tracking on the page which was a bit more complex from their side. They were very helpful and created a WordPress plugin for tracking just to help us deploy their tag.

The hypothesis in respect to these two trackers was that they would report a higher percentage of bots given that the traffic was not designed to pass their specific filters.

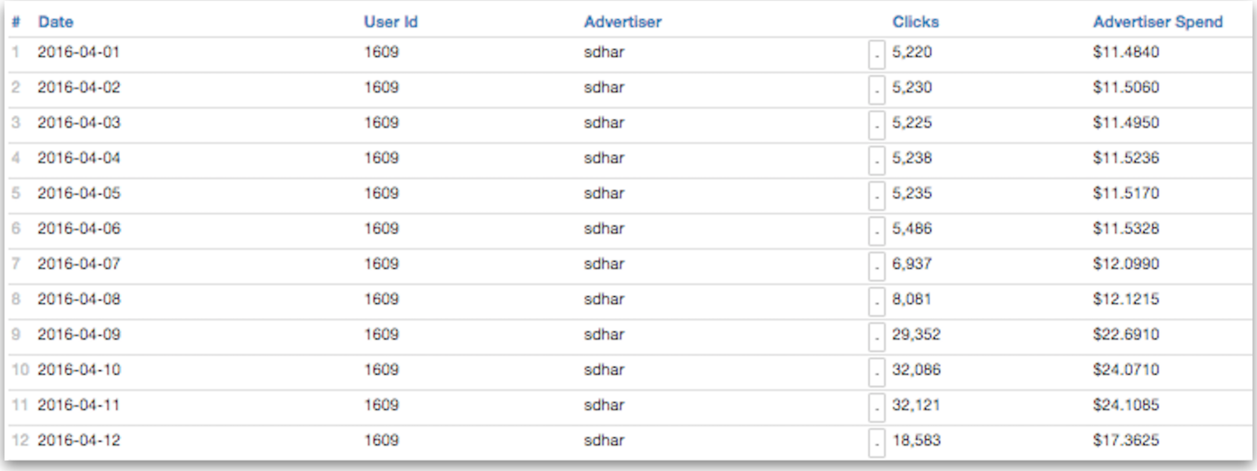
RESULTS

The main point of this paper, is that every company except the brand advertiser benefits from fraudulent traffic. This leads to many mixed incentives, the results of which are evidenced in this research. The purpose for the industry accepting that everyone but advertisers have benefited from fraudulent traffic is not for the sake of admitting guilt, but for the industry to approach ad fraud with the correct perspective, which is that ad fraud is an internal problem related with our behavior and underlying structure, not an external force afflicting the ecosystem.

Now let's dig in to the results…

SOURCED TRAFFIC REPORT:

Below graphic illustrates the daily traffic and the total cost for the clicks that had been delivered by the traffic company.

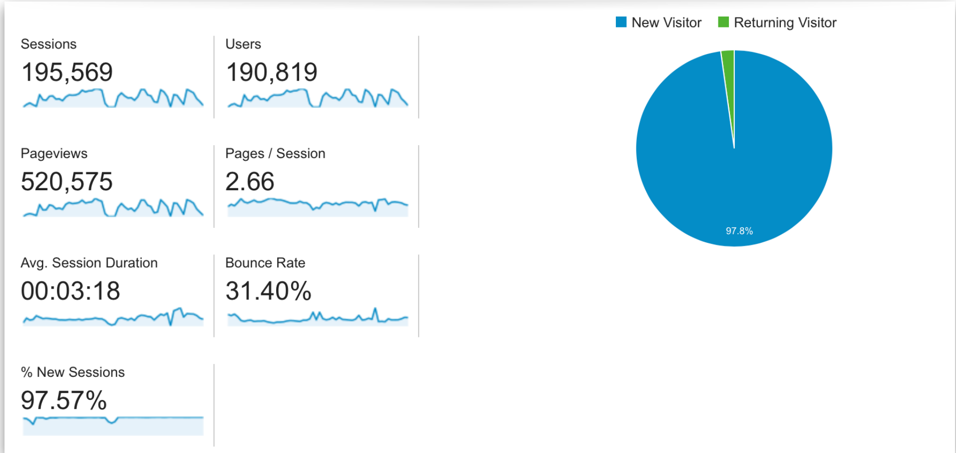


#	Date	User Id	Advertiser	Clicks	Advertiser Spend
1	2016-04-01	1609	sdhar	5,220	$11.4840
2	2016-04-02	1609	sdhar	5,230	$11.5060
3	2016-04-03	1609	sdhar	5,225	$11.4950
4	2016-04-04	1609	sdhar	5,238	$11.5236
5	2016-04-05	1609	sdhar	5,235	$11.5170
6	2016-04-06	1609	sdhar	5,486	$11.5328
7	2016-04-07	1609	sdhar	6,937	$12.0990
8	2016-04-08	1609	sdhar	8,081	$12.1215
9	2016-04-09	1609	sdhar	29,352	$22.6910
10	2016-04-10	1609	sdhar	32,086	$24.0710
11	2016-04-11	1609	sdhar	32,121	$24.1085
12	2016-04-12	1609	sdhar	18,583	$17.3625

You can find the full traffic purchase report here: http://screencast.com/t/0kxV600ZBk9O

GOOGLE ANALYTICS REPORTS:

For the time period of the test (20th of March to 14th of May), roughly 98% of the visitors were new and had a slightly lower than normal bounce rate 31.4% and 2.66 page-views per session. With the average session duration of +3 minutes, for a new site nothing seems to odd at this stage.



Sessions
195,569

Users
190,819

Pageviews
520,575

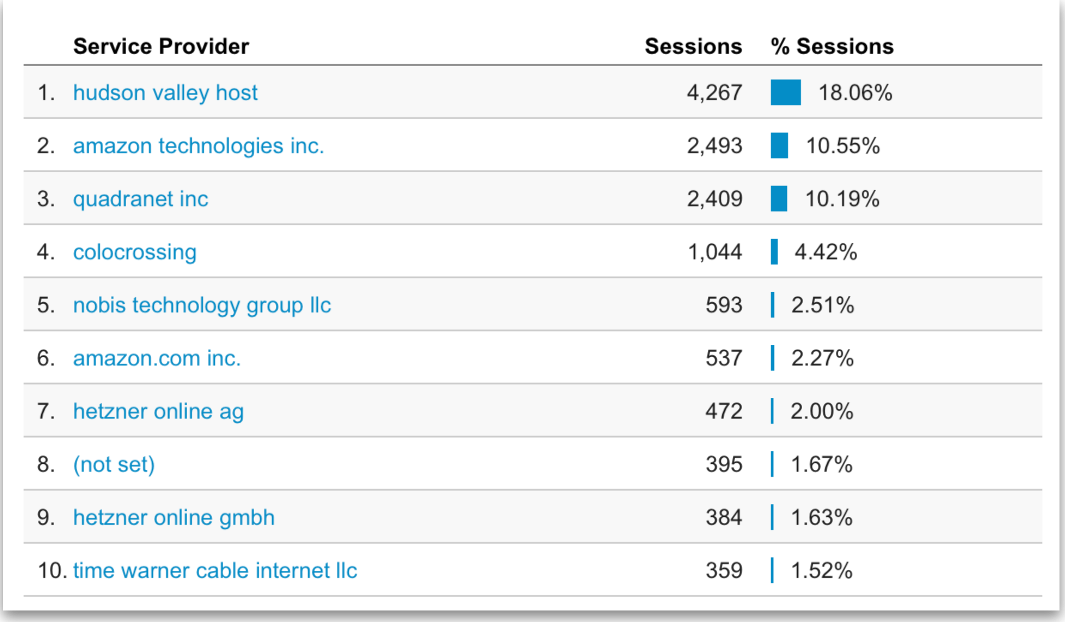
Pages / Session
2.66

Avg. Session Duration
00:03:18

Bounce Rate
31.40%

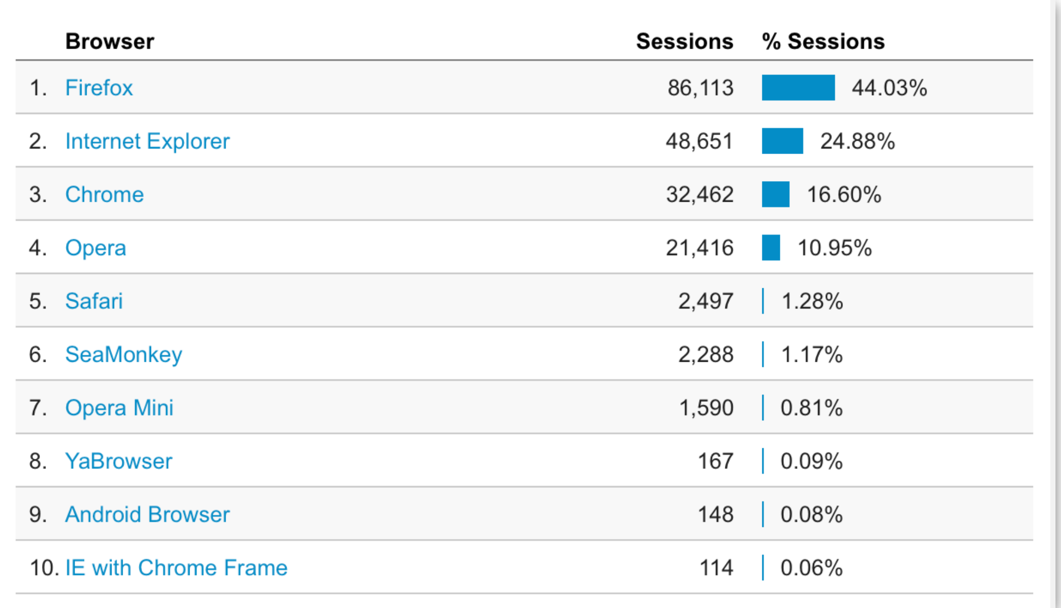
% New Sessions
97.57%

Where things start to get more obvious from the fraud detection standpoint, is traffic sources, and more specifically the Service Provider view. The great majority of all the traffic coming to the site is from hosting/cloud companies! Just Amazon's share is almost 1/8 of every visit, with another company Hudson Valley Host representing over 1/6 of every visit.



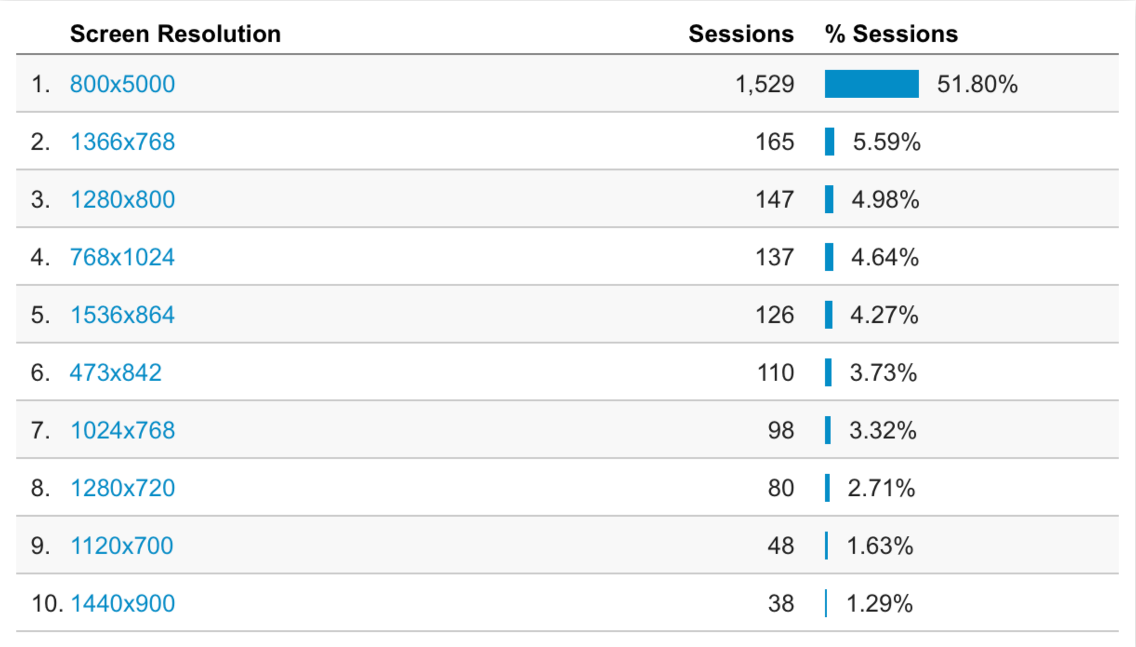
	Service Provider	Sessions	% Sessions
1.	hudson valley host	4,267	18.06%
2.	amazon technologies inc.	2,493	10.55%
3.	quadranet inc	2,409	10.19%
4.	colocrossing	1,044	4.42%
5.	nobis technology group llc	593	2.51%
6.	amazon.com inc.	537	2.27%
7.	hetzner online ag	472	2.00%
8.	(not set)	395	1.67%
9.	hetzner online gmbh	384	1.63%
10.	time warner cable internet llc	359	1.52%

The strong indicators for the fact that nothing but fake traffic was coming to this site continues with the Browser report where the data correlates very poorly with general share of browsers among internet users.



	Browser	Sessions	% Sessions
1.	Firefox	86,113	44.03%
2.	Internet Explorer	48,651	24.88%
3.	Chrome	32,462	16.60%
4.	Opera	21,416	10.95%
5.	Safari	2,497	1.28%
6.	SeaMonkey	2,288	1.17%
7.	Opera Mini	1,590	0.81%
8.	YaBrowser	167	0.09%
9.	Android Browser	148	0.08%
10.	IE with Chrome Frame	114	0.06%

One of the seemingly strangest things out of all the things that stood out, came from the Screen Resolution report, where we can find that over 50% of sessions came from a screen resolution of 800x5000. That is a really HIGH screen!



	Screen Resolution	Sessions	% Sessions
1.	800x5000	1,529	51.80%
2.	1366x768	165	5.59%
3.	1280x800	147	4.98%
4.	768x1024	137	4.64%
5.	1536x864	126	4.27%
6.	473x842	110	3.73%
7.	1024x768	98	3.32%
8.	1280x720	80	2.71%
9.	1120x700	48	1.63%
10.	1440x900	38	1.29%

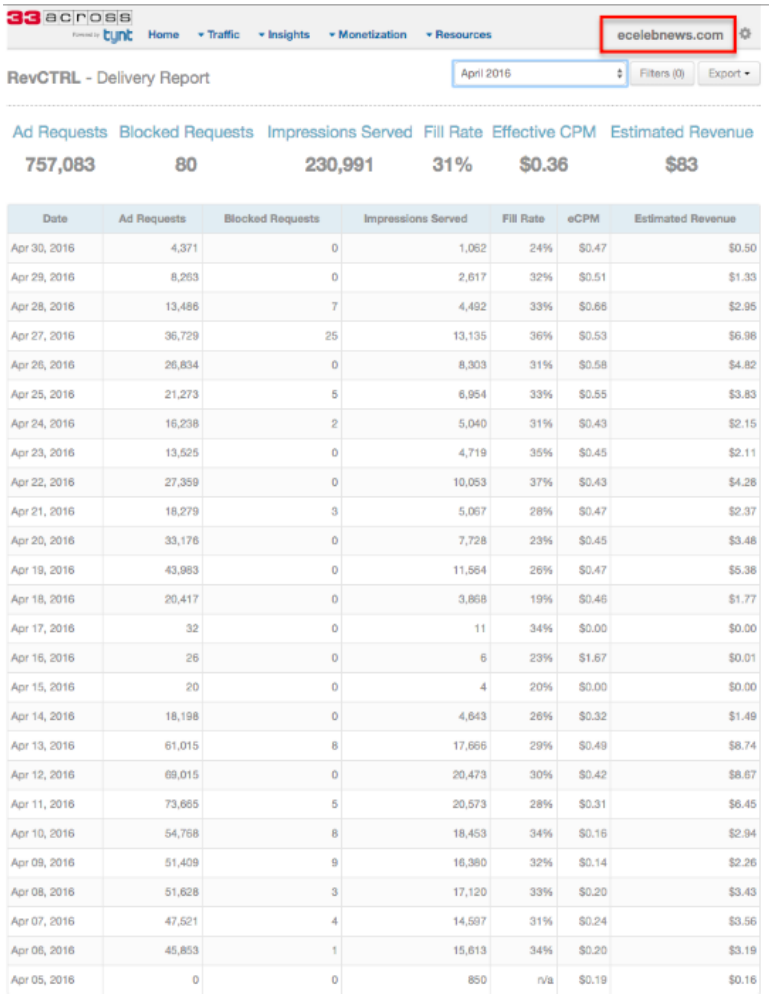
Without a doubt our favorite finding was from the Mobile Device report. Even though mobile traffic was less than 2% according to Google Analytics, we could not resist including in this report the most common mobile device, with over 50% share of all mobile traffic. And the winner is…Sagem my 721x, the device shown on the left.

More info about the device: http://www.inside-handy.de/img/tests/gal10358.jpg

In summary, it seems fair to argue that even without allegedly sophisticated ad fraud verification software in place, it would have been very easy to detect that most of the traffic coming to our fake site, was indeed fake traffic. Actually it's quite hard to find indications of human traffic within the web analytics data.

33ACROSS MONETIZATION

May 1-14: http://screencast.com/t/uZAwDC5koVV
April 1-30: http://screencast.com/t/NvaimJfJOM

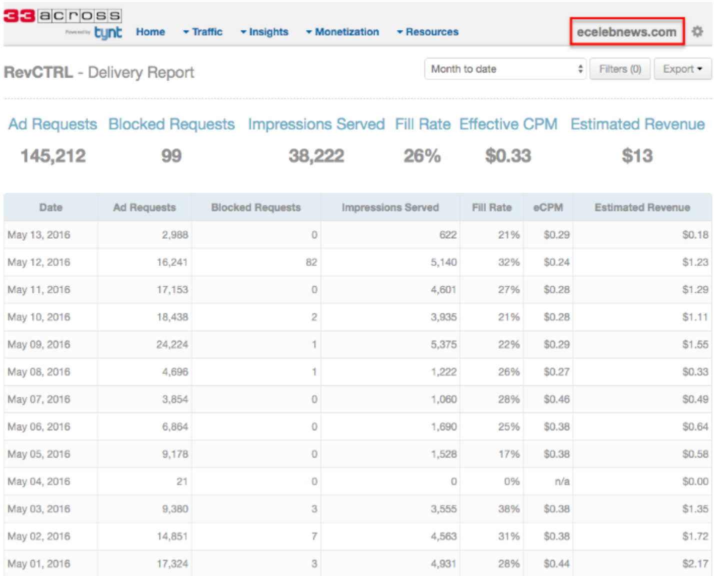


RevCTRL - Delivery Report

April 2016

Ad Requests	Blocked Requests	Impressions Served	Fill Rate	Effective CPM	Estimated Revenue
757,083	80	230,991	31%	$0.36	$83

Date	Ad Requests	Blocked Requests	Impressions Served	Fill Rate	eCPM	Estimated Revenue
Apr 30, 2016	4,371	0	1,062	24%	$0.47	$0.50
Apr 29, 2016	8,263	0	2,617	32%	$0.51	$1.33
Apr 28, 2016	13,486	7	4,492	33%	$0.66	$2.95
Apr 27, 2016	36,729	25	13,135	36%	$0.53	$6.98
Apr 26, 2016	26,834	0	8,303	31%	$0.58	$4.82
Apr 25, 2016	21,273	5	6,954	33%	$0.55	$3.83
Apr 24, 2016	16,238	2	5,040	31%	$0.43	$2.15
Apr 23, 2016	13,525	0	4,719	35%	$0.45	$2.11
Apr 22, 2016	27,359	0	10,053	37%	$0.43	$4.28
Apr 21, 2016	18,279	3	5,067	28%	$0.47	$2.37
Apr 20, 2016	33,176	0	7,728	23%	$0.45	$3.48
Apr 19, 2016	43,983	0	11,564	26%	$0.47	$5.38
Apr 18, 2016	20,417	0	3,868	19%	$0.46	$1.77
Apr 17, 2016	32	0	11	34%	$0.00	$0.00
Apr 16, 2016	26	0	6	23%	$1.67	$0.01
Apr 15, 2016	20	0	4	20%	$0.00	$0.00
Apr 14, 2016	18,198	0	4,643	26%	$0.32	$1.49
Apr 13, 2016	61,015	8	17,666	29%	$0.49	$8.74
Apr 12, 2016	69,015	0	20,473	30%	$0.42	$8.67
Apr 11, 2016	73,665	5	20,573	28%	$0.31	$6.45
Apr 10, 2016	54,768	8	18,453	34%	$0.16	$2.94
Apr 09, 2016	51,409	9	16,380	32%	$0.14	$2.26
Apr 08, 2016	51,628	3	17,120	33%	$0.20	$3.43
Apr 07, 2016	47,521	4	14,597	31%	$0.24	$3.56
Apr 06, 2016	45,853	1	15,613	34%	$0.20	$3.19
Apr 05, 2016	0	0	850	n/a	$0.19	$0.16



RevCTRL - Delivery Report

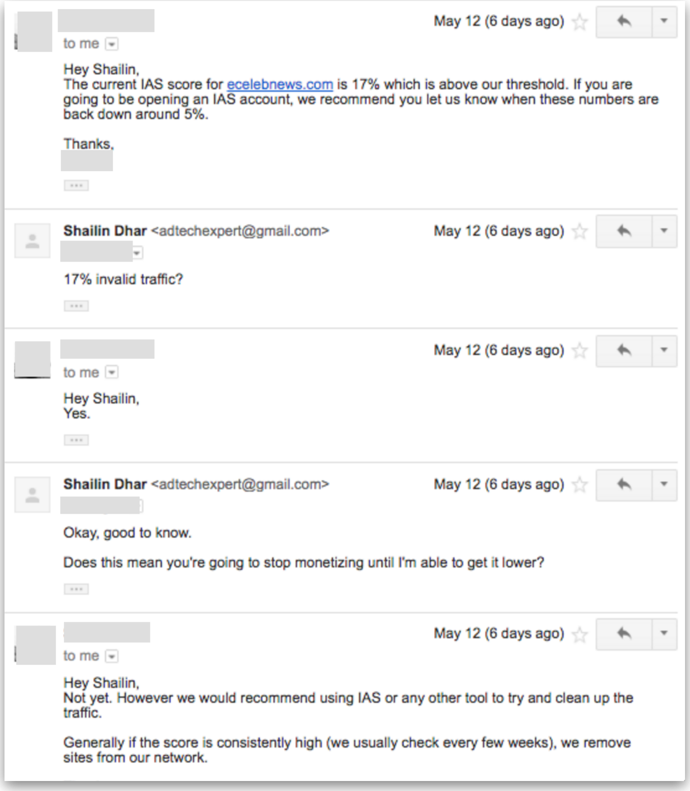
Month to date

Ad Requests	Blocked Requests	Impressions Served	Fill Rate	Effective CPM	Estimated Revenue
145,212	99	38,222	26%	$0.33	$13

Date	Ad Requests	Blocked Requests	Impressions Served	Fill Rate	eCPM	Estimated Revenue
May 13, 2016	2,988	0	622	21%	$0.29	$0.18
May 12, 2016	16,241	82	5,140	32%	$0.24	$1.23
May 11, 2016	17,153	0	4,601	27%	$0.28	$1.29
May 10, 2016	18,438	2	3,935	21%	$0.28	$1.11
May 09, 2016	24,224	1	5,375	22%	$0.29	$1.55
May 08, 2016	4,696	1	1,222	26%	$0.27	$0.33
May 07, 2016	3,854	0	1,060	28%	$0.46	$0.49
May 06, 2016	6,864	0	1,690	25%	$0.38	$0.64
May 05, 2016	9,178	0	1,528	17%	$0.38	$0.58
May 04, 2016	21	0	0	0%	n/a	$0.00
May 03, 2016	9,380	3	3,555	38%	$0.38	$1.35
May 02, 2016	14,851	7	4,563	31%	$0.38	$1.72
May 01, 2016	17,324	3	4,931	28%	$0.44	$2.17

A total of $96 of revenue was generated as part of this test ($564.93 spent on traffic - April 5 to May 14), with average fill rate around 30%. Filled RPM peaked at April 18 at $2.42.

Robotic traffic is being monetized at a $2.42 RPM without any optimization, which means the actual buyer is paying more, and then the end advertiser is paying even more. For showing an ad to a bot that will never buy their product or service.



[redacted] May 12 (6 days ago)
to me

Hey Shailin,
The current IAS score for ecelebnews.com is 17% which is above our threshold. If you are going to be opening an IAS account, we recommend you let us know when these numbers are back down around 5%.

Thanks,
[redacted]

Shailin Dhar <adtechexpert@gmail.com> May 12 (6 days ago)
[redacted]

17% invalid traffic?

[redacted] May 12 (6 days ago)
to me

Hey Shailin,
Yes.

Shailin Dhar <adtechexpert@gmail.com> May 12 (6 days ago)
[redacted]

Okay, good to know.

Does this mean you're going to stop monetizing until I'm able to get it lower?

[redacted] May 12 (6 days ago)
to me

Hey Shailin,
Not yet. However we would recommend using IAS or any other tool to try and clean up the traffic.

Generally if the score is consistently high (we usually check every few weeks), we remove sites from our network.

Given the overall amount of traffic is low, and we only generated about $100 (again, we will never accept the payment from 33Across that resulted from this test), this shows clearly how easy it is to monetize sub-penny bot traffic in a major ad-tech platform even when a "leading" ad fraud verification solution, such as Integral Ad Science is in use.

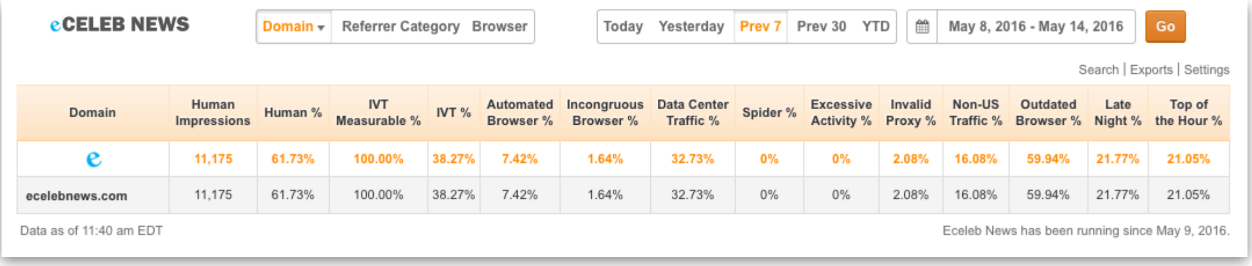
INTEGRAL AD SCIENCE DETECTION

33Across apparently does not share NHT (non-human traffic) or IVT (invalid traffic) data with their publishers because they claim that only verified human impressions are monetized. I had to ask several times to get the data which turned out to be 17% IVT. Meaning that 83% of the robotic traffic we purchased was considered human by the Integral Ad Science filter. When I informed the sourced traffic vendor that the rate was 17%, they said that the Integral Ad Science sampling got lucky because it's usually around 5%. Which is what 33Across and Integral Ad Science consider the healthy threshold for detected NHT for a publisher.

However, even though the healthy level is considered 5%, and the site used in this test was reporting a 17% IVT rate, there was no intention of stopping monetization or digging into why the rate was so high on behalf of 33Across. My guess as to why, since their filter samples the traffic, is that they just assume a certain level of fraudulent traffic across the board with every publisher.

MOAT DETECTION

MOATS's pixel was able to catch only 38.27% as invalid traffic, meaning that their technology verified 61.73% of the robotic traffic as being human. Around 10% of the traffic was detected as being from an automated browser. Surprisingly, 0% was flagged for having "excessive activity". Also peculiar was that 59.94% was detected as having an outdated browser.



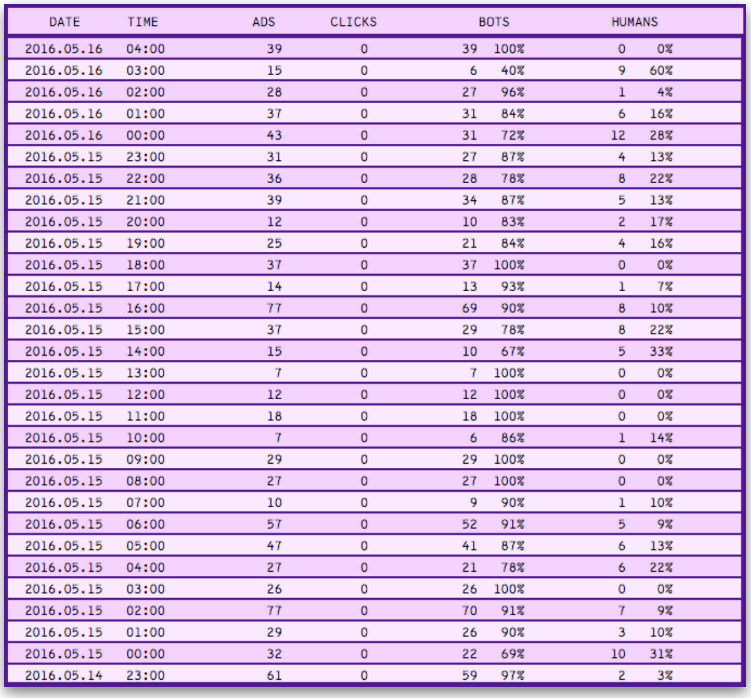
Domain	Human Impressions	Human %	IVT Measurable %	IVT %	Automated Browser %	Incongruous Browser %	Data Center Traffic %	Spider %	Excessive Activity %	Invalid Proxy %	Non-US Traffic %	Outdated Browser %	Late Night %	Top of the Hour %
e	11,175	61.73%	100.00%	38.27%	7.42%	1.64%	32.73%	0%	0%	2.08%	16.08%	59.94%	21.77%	21.05%
ecelebnews.com	11,175	61.73%	100.00%	38.27%	7.42%	1.64%	32.73%	0%	0%	2.08%	16.08%	59.94%	21.77%	21.05%

Data as of 11:40 am EDT

Eceleb News has been running since May 9, 2016.

OXFORD-BIOCHRONOMETRICS DETECTION

Oxford-BioChron detected a total of 373,874 unique "users", 90% of which was classified as bots, and 10% classified as humans. Clearly the best performing ad fraud detection solution in the test.



DATE	TIME	ADS	CLICKS	BOTS		HUMANS	
2016.05.16	04:00	39	0	39	100%	0	0%
2016.05.16	03:00	15	0	6	40%	9	60%
2016.05.16	02:00	28	0	27	96%	1	4%
2016.05.16	01:00	37	0	31	84%	6	16%
2016.05.16	00:00	43	0	31	72%	12	28%
2016.05.15	23:00	31	0	27	87%	4	13%
2016.05.15	22:00	36	0	28	78%	8	22%
2016.05.15	21:00	39	0	34	87%	5	13%
2016.05.15	20:00	12	0	10	83%	2	17%
2016.05.15	19:00	25	0	21	84%	4	16%
2016.05.15	18:00	37	0	37	100%	0	0%
2016.05.15	17:00	14	0	13	93%	1	7%
2016.05.15	16:00	77	0	69	90%	8	10%
2016.05.15	15:00	37	0	29	78%	8	22%
2016.05.15	14:00	15	0	10	67%	5	33%
2016.05.15	13:00	7	0	7	100%	0	0%
2016.05.15	12:00	12	0	12	100%	0	0%
2016.05.15	11:00	18	0	18	100%	0	0%
2016.05.15	10:00	7	0	6	86%	1	14%
2016.05.15	09:00	29	0	29	100%	0	0%
2016.05.15	08:00	27	0	27	100%	0	0%
2016.05.15	07:00	10	0	9	90%	1	10%
2016.05.15	06:00	57	0	52	91%	5	9%
2016.05.15	05:00	47	0	41	87%	6	13%
2016.05.15	04:00	27	0	21	78%	6	22%
2016.05.15	03:00	26	0	26	100%	0	0%
2016.05.15	02:00	77	0	70	91%	7	9%
2016.05.15	01:00	29	0	26	90%	3	10%
2016.05.15	00:00	32	0	22	69%	10	31%
2016.05.14	23:00	61	0	59	97%	2	3%

DATADOME DETECTION

DataDome detected that 52 % of the overall traffic during the test period came from bots. They had also noted that hits would not be considered bots unless they generate a higher volume of hits over the period, or fail a CAPTCHA (which they would, had we been blocking the bot traffic). Which means that detection could be easily overcome by distributing fake traffic across large number of IP addresses, as is often the case with botnet traffic.

CONCLUSIONS

- Leading ad fraud verification vendor Integral Ad Science detected 17% of easy-to-detect bot traffic mostly coming from hosting company IP addresses
- Moat detection verified 61.73% of the fake traffic as humans, but was able to identify some of the data center traffic and still significantly outperformed Integral-Ad-Science's detection result.
- DataDome detected roughly half of the fake traffic, where the traffic was not directly targeting to pass DataDome's detection.
- Oxford-BioChronometrics had by far the highest detection rate, at around 90%, where the traffic was not targeting to pass their detection.
- Ad fraud is very easy to commit, requires very low startup cost and no serious technical capabilities; anyone can start doing it today.
- Proprietary 3rd-party ad fraud verification solutions alone are not enough for media buyers to keep their media investment safe from fraud.
- The 100% fraud-free guarantee provided by 33Across is only about 17% true, given that according to comments by the company, the guarantee is solely based on the detection capability provided by Integral Ad Science.
- It is possible that other companies providing similar guarantees to buyers as 33Across is, are suffering from similar issues, where their customers (media buyers) are suffering significant losses due to false sense of security.

For questions, comments, concerns or if you would like to have access to the analytics account, please send a request to Info@DharMethod.com and we will get back to you according to your request.

THE DHAR METHOD